Citrix Endpoint Management

Machine translated content

Disclaimer

本内容的正式版本为英文版。部分 Cloud Software Group 文档内容采用了机器翻译，仅供您参考。Cloud Software Group 无法控制机器翻译的内容，这些内容可能包含错误、不准确或不合适的语言。对于从英文原文翻译成任何其他语言的内容的准确性、可靠性、适用性或正确性，或者您的 Cloud Software Group 产品或服务沿用了任何机器翻译的内容，我们均不作任何明示或暗示的保证，并且适用的最终用户许可协议或服务条款或者与 Cloud Software Group 签订的任何其他协议（产品或服务与已进行机器翻译的任何文档保持一致）下的任何保证均不适用。对于因使用机器翻译的内容而引起的任何损害或问题，Cloud Software Group 不承担任何责任。

Contents

Endpoint Management 3

新增功能 7

第三方声明 12

弃用 12

系统要求 21

Endpoint Management 兼容性 33

支持的设备操作系统 34

语言支持 35

FIPS 140-2 合规性 37

关于 **Endpoint Management** 38

Citrix Endpoint Management 与 **Microsoft Endpoint Manager** 的集成 51

载入和资源设置 65

Cloud Connector 的扩展和大小注意事项 75

准备注册设备并交付资源 76

证书和身份验证 89

上载、更新和续订证书 92

Citrix Gateway 和 **Endpoint Management** 103

域或域加安全令牌身份验证 113

客户端证书或证书加域身份验证 118

PKI 实体 138

凭据提供程序 152

APNs 证书 158

SAML 单点登录与 **Citrix Files** 166

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

通过 **Citrix Cloud** 使用 **Azure Active Directory** 进行身份验证 **176**

通过 **Citrix Cloud** 使用 **Okta** 进行身份验证 **179**

通过 **Citrix Cloud** 使用本地 **Citrix Gateway** 进行身份验证 **182**

用户帐户、角色和注册 **184**

注册配置文件 **199**

通知 **203**

使用 **RBAC** 配置角色 **209**

许可证 **225**

设备管理 **226**

Alexa for Business **248**

从设备管理迁移到 **Android Enterprise** **261**

Android Enterprise **265**

分发 **Android Enterprise** 应用程序 **310**

适用于 **Google Workspace**（以前称为 **G Suite**）客户的旧版 **Android Enterprise** **335**

Android OS **370**

Firebase Cloud Messaging **376**

Android SafetyNet **380**

Play Integrity API **384**

Samsung **387**

网络访问控制 **388**

iOS **394**

macOS **409**

通过 **Apple** 部署计划部署设备 **415**

批量注册 **Apple** 设备 **428**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

与 **Apple** 教育功能相集成 **433**

共用的 **iPad** **446**

分发 **Apple** 应用程序 **458**

网络访问控制 **482**

Windows Desktop 和 **Tablet** **488**

批量注册 **Windows** 设备 **495**

设备策略 **499**

AirPlay 镜像设备策略 **519**

AirPrint 设备策略 **521**

应用程序权限设备策略 **522**

APN 设备策略 **524**

应用程序访问设备策略 **526**

应用程序属性设备策略 **527**

应用程序配置设备策略 **528**

应用程序清单设备策略 **531**

应用程序防护设备策略 **533**

应用程序锁定设备策略 **535**

应用程序通知设备策略 **538**

应用程序限制设备策略 **540**

应用程序卸载设备策略 **542**

应用程序卸载限制设备策略 **543**

自动更新托管应用程序设备策略 **544**

BitLocker 设备策略 **545**

“蓝牙**”** 设备策略 **550**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

日历 **(CalDav)** 设备策略 **550**

手机网络设备策略 **552**

连接计划设备策略 **552**

联系人 **(CardDAV)** 设备策略 **554**

内容设备策略 **555**

凭据设备策略 **556**

自定义 **XML** 设备策略 **562**

Defender 设备策略 **565**

Device Guard 设备策略 **567**

设备运行状况证明设备策略 **568**

设备名称设备策略 **569**

教育配置设备策略 **570**

Endpoint Management 选项设备策略 **572**

Endpoint Management 卸载设备策略 **574**

Exchange 设备策略 **575**

文件设备策略 **579**

FileVault 设备策略 **581**

防火墙设备策略 **583**

字体设备策略 **585**

主屏幕布局设备策略 **586**

"导入设备配置**"** 设备策略 **588**

"导入 **iOS** 和 **macOS** 配置文件**"** 设备策略 **588**

键盘锁管理设备策略 **590**

网亭设备策略 **593**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Launcher 配置设备策略 **596**

LDAP 设备策略 **597**

位置设备策略 **598**

锁屏界面消息设备策略 **603**

邮件设备策略 **604**

托管书签设备策略 **606**

托管配置策略 **606**

托管域设备策略 **618**

最大常驻用户数设备策略 **620**

MDM 选项设备策略 **620**

网络设备策略 **621**

网络使用设备策略 **633**

Office 设备策略 **634**

组织信息设备策略 **635**

"操作系统更新**"** 设备策略 **635**

通行码设备策略 **646**

通行码锁定宽限期设备策略 **654**

个人热点设备策略 **655**

电源管理设备策略 **655**

"配置文件删除**"** 设备策略 **656**

预配配置文件设备策略 **657**

删除预配配置文件设备策略 **658**

代理设备策略 **658**

公共会话设备策略 **659**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

限制设备策略 **661**

漫游设备策略 **694**

SCEP 设备策略 **695**

Siri 和听写策略 **697**

SSO 帐户设备策略 **699**

应用商店设备策略 **700**

已订阅的日历设备策略 **700**

条款和条件设备策略 **701**

通道设备策略 **702**

VPN 设备策略 **703**

墙纸设备策略 **730**

Web 内容过滤器设备策略 **732**

Web 剪辑设备策略 **733**

Windows 代理设备策略 **734**

Windows GPO 配置设备策略 **738**

Windows Hello 企业版设备策略 **740**

添加应用程序 **741**

应用程序连接器类型 **783**

Citrix Launcher **784**

使用 **Apple** 批量购买功能添加应用程序 **787**

将 **Citrix Content Collaboration** 与 **Endpoint Management** 结合使用 **794**

适用于 **HDX** 应用程序的 **SmartAccess** **808**

升级 **MDX** 或企业应用程序 **825**

添加媒体 **827**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

部署资源 **831**

宏 **842**

自动化操作 **875**

监视和支持 **885**

连接检查 **892**

移动服务提供商 **896**

报告 **897**

REST API **904**

ActiveSync Gateway **906**

适用于 **Exchange ActiveSync** 的 **Endpoint Management** 连接器 **908**

适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器 **951**

高级概念 **963**

Endpoint Management 部署 **963**

管理模式 **964**

设备要求 **967**

安全性和用户体验 **968**

应用程序 **981**

用户社区 **987**

电子邮件策略 **992**

Endpoint Management 集成 **998**

与 **Citrix Gateway** 和 **Citrix ADC** 集成 **1004**

MDX 应用程序的 **SSO** 和代理注意事项 **1009**

身份验证 **1013**

服务器属性 **1024**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备和应用程序策略 **1036**

客户端属性 **1045**

用户注册选项 **1053**

应用程序预配和取消预配 **1056**

基于控制板的操作 **1058**

基于角色的访问控制和 **Endpoint Management** 支持 **1059**

Citrix 支持过程 **1060**

在 **Endpoint Management** 中发送组注册邀请 **1061**

为 **EWS** 配置基于证书的身份验证以接收 **Secure Mail** 推送通知 **1063**

配置本地设备运行状况证明服务器 **1066**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management

April 11, 2023

Citrix Endpoint Management 是一种解决方案，用于管理端点，以及提供移动设备管理 (MDM) 和移动应用程序管理 (MAM) 功能。借助 Endpoint Management，您可以管理设备和应用程序策略，并将应用程序交付给用户。您的企业信息将受严格的身份、设备、应用程序、数据和网络安全保护。

Citrix 职责与客户职责

Citrix Cloud Operations 部门负责处理各种体系结构和监视任务。因此，您可以重点关注用户体验以及管理设备、应用程序和策略。

Citrix 的职责：

- Endpoint Management 服务器节点
- Citrix Gateway（服务或本地）初始集成和配置
- Citrix Gateway 负载平衡器
- 数据库
- Cloud Connector 软件配置
- SAML 身份验证与 Citrix Content Collaboration 的集成
- Endpoint Management 站点监控：实例、数据库、企业连接 (LDAP)、VPN 通道（如果适用）、公共 SSL 证书、Endpoint Management 许可

客户的职责：

- Citrix Gateway（本地）管理和更新
- 安装了 Cloud Connector 和 Gateway Connector（适用于 Citrix Gateway 服务）的计算机
- LDAP/Active Directory
- DNS
- Citrix Content Collaboration：初始 Citrix Content Collaboration 配置、本地存储区域控制器安装、Citrix Files 更新
- Endpoint Management 配置：设备、策略、应用程序、交付组、操作和客户端证书

与 **Microsoft Endpoint Manager** 的集成

Endpoint Management 与 Microsoft Endpoint Manager (MEM) 集成。该集成在 Microsoft Edge 浏览器等 Microsoft Intune 感知应用程序中增加了 Endpoint Management Micro VPN 的价值。实现该集成后，您可以：

- 通过 Azure AD 进行有条件访问来确保 Secure Office 365 应用程序的安全。有关详细信息，请参阅与 Azure AD 条件访问集成。
- 通过 Intune 和 Citrix 封装自己的业务线应用，以在 Intune 移动应用程序管理 (MAM) 容器中提供 Micro VPN 功能。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 在一个容器中管理和交付 Office 365 应用程序、业务线应用和 Citrix Secure Mail。此管理方法提供终极安全性和高效工作。例如，您可以：
  - 阻止单个设备或操作系统
  - 基于设备、用户或用户组自定义 ActiveSync 策略
  - 在设备级别隔离
  - 监视单个连接或设备
  - 避免凭据和数据缓存的安全风险

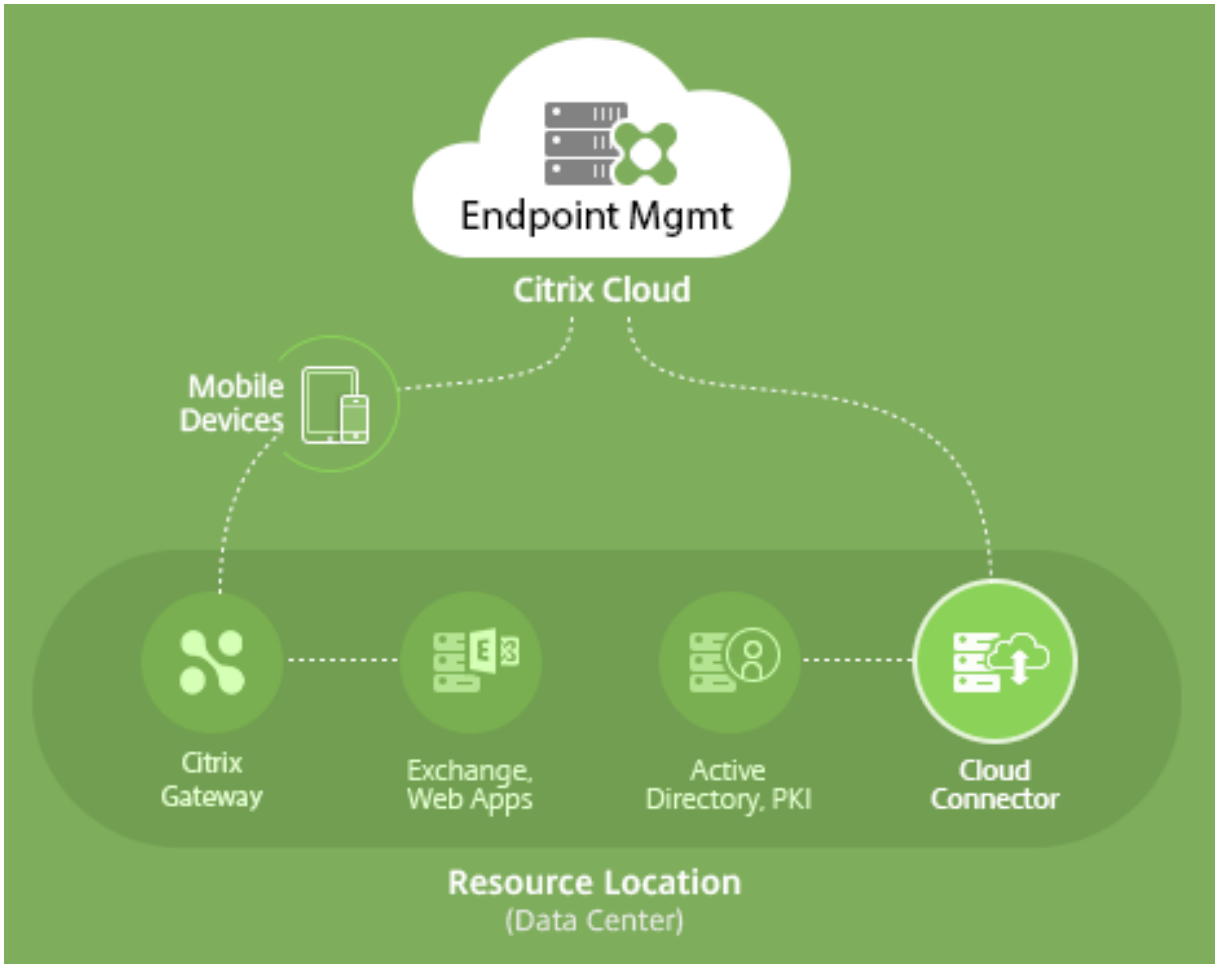
使用 Endpoint Management MDM+MAM 或 Intune MDM 来管理设备。有关详细信息，请参阅 Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成。

Cloud Connector 和资源位置

您可以通过 Cloud Connector 连接到 Endpoint Management。Cloud Connector 用作 Citrix Cloud 与您的资源位置之间的通信通道。借助 Cloud Connector，不需要诸如 VPN 或 IPsec 通道等任何复杂的网络连接或基础结构配置即可实现云管理。

资源位置拥有向订阅者提供服务所需的资源。对于 Endpoint Management，资源位置是 Citrix Gateway、LDAP、DNS 和 PKI 服务器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



有关 Cloud Connector 和资源位置的详细信息，请参阅关于 Endpoint Management。

开始使用 **Endpoint Management**

> 提示：
>
> XenMobile 迁移服务
>
> 如果您在本地使用 XenMobile Server，我们的 XenMobile 迁移服务可以帮助您开始使用 Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 不需要重新注册设备。
>
> 要了解详细信息，请联系您的本地 Citrix 销售人员、系统工程师或 Citrix Partner。
>
> 要了解与迁移服务有关的更多信息，请参阅 3 reasons to move to Citrix Endpoint Management service（迁移到 Citrix Endpoint Management 服务的 3 个原因）。
>
> 要了解迁移的原因、如何迁移以及迁移到 Citrix Endpoint Management 的好处，请访问 CEM 迁移服务课程目录或者参阅 Citrix Endpoint Management (CEM) 迁移服务指南。

当您评估或购买 Endpoint Management 时，Endpoint Management 运营团队会提供持续的入门帮助。运营团队还与您沟通，以确保核心 Endpoint Management 服务正在运行和配置正确。下图显示了入门步骤。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



要注册 Citrix 帐户并申请试用 Endpoint Management，请与您的 Citrix 销售代表联系。准备好继续操作时，请转至 https://onboarding.cloud.com。

有关 Endpoint Management 注册和配置的快速概览，请观看此视频。

这是一个嵌入式视频。单击链接观看视频

希望在开始之前了解更多信息吗？请尝试以下资源：

Endpoint Management 文档：提供从注册到初始配置再到高级配置的完整 Endpoint Management 文档。“新增功能”一文介绍了新增功能和修复。Citrix 在该文章可用于新版本时会向您发出通知。

Citrix Endpoint Management 入门手册：整合了有关 Endpoint Management 的所有可用信息，以便您可以继续顺利启用和启动 Endpoint Management。可以根据本文档来记录您的内部进程的变更以及记录您的高级设计和功能性设计。

Endpoint Management 部署手册：计划 Endpoint Management 部署涉及多个注意事项。本手册包括面向您的 Endpoint Management 环境的建议、常见问题和用例。

SalesIQ：面向我们的 Citrix Partner 的更多资源。

后续步骤

有关 Endpoint Management 注册过程的信息，请参阅载入和资源设置。

完成载入后，请参阅准备注册设备并交付资源。

弃用声明

有关正在逐步淘汰的 Citrix Endpoint Management 功能的高级通知，请参阅弃用。

Endpoint Management 支持

有关如何在 Endpoint Management 控制台中访问支持相关信息和工具的详细信息，请参阅监视和支持。

大约每隔 2 周，Endpoint Management 版本会进行一次滚动更新。对您（即客户）来说，此过程是透明的。初始更新仅应用于 Citrix 内部站点，然后逐步应用于客户环境。我们逐步提供更新，以提供产品质量并最大限度地提高可用性。

Endpoint Management 客户直接从 Endpoint Management Cloud Operations 团队接收更新和通信。通过这些更新，您可以了解最新的新增功能、已知问题、已修复的问题等信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud Operations 团队使用最新的 Endpoint Management 滚动修补程序维护 Endpoint Management 环境。要获取滚动补丁发布之前所需的特定补丁或修复程序，请联系 Citrix 技术支持。

如果您的环境存在任何问题，请联系 Citrix 技术支持或者您的 Citrix 帐户团队。此类问题可能包括移动设备注册、Endpoint Management 控制台访问或 Secure Mail 问题。

如果需要在 Cloud 或 Endpoint Management 中的 Citrix Gateway 上进行任何集成或更改，请通过 Citrix 技术支持提交请求。

可能会请求的更改示例如下：

- Citrix Files 与 Cloud 中的 Citrix Gateway 集成
- 更改 Citrix Gateway 身份验证类型
- 验证与客户数据中心资源的连接
- 更改 Micro VPN 的拆分通道配置
- 由于某些服务器配置更改，请重新启动 Endpoint Management 组件

服务级别协议

Citrix Endpoint Management 使用行业最佳做法来实现云级别的高度服务可用性。

有关 Citrix 对 Citrix Cloud 服务的可用性的承诺的完整详细信息，请参阅服务级别协议。

新增功能

August 8, 2023

Citrix 的目标是在推出了新增功能和产品更新时向 Endpoint Management 客户提供。新版本会带来更多的价值，应立即将更新告知客户。

- Endpoint Management 的滚动更新大约每两周发布一次。
- 这些更新不会导致您的实例或设备用户出现任何停机事件。
- 并非每个版本都有新功能，有些更新包括修复和性能性能增强。

对您（即客户）来说，此过程是透明的。我们仅将初始更新应用到 Citrix 内部站点，然后逐步应用到客户环境。分批递增更新有助于提供产品质量和最大限度地提高可用性。

您还可以直接从 Endpoint Management Cloud Operations 团队接收 Endpoint Management 更新和通信。通过这些更新，您可以了解最新的新增功能、已知问题、已修复的问题等信息。

有关更多详细信息，包括云规模和服务可用性，请参阅 Endpoint Management 服务等级协议。要监视服务中断情况和计划内维护，请参阅“服务运行状况” 控制板。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

继续支持 **Citrix ADC** 中已弃用的经典策略

Citrix 近期宣布自 Citrix ADC 12.0 Build 56.20 起弃用了一些基于经典策略的功能。Citrix ADC 弃用通知对与 NetScaler Gateway 的现有 Endpoint Management 集成没有影响。Citrix Endpoint Management 继续支持经典策略，无需执行任何操作。

在将端点升级到 **iOS 14.5** 之前的准备工作

在将任何端点升级到 iOS 14.5 之前，Citrix 建议您采取以下措施来缓解应用程序崩溃的情况：

- 将 Citrix Secure Mail 和 Secure Web 升级到 21.2.X 或更高版本。请参阅升级 MDX 或企业应用程序。
- 如果您使用 MDX Toolkit，请使用 MDX Toolkit 21.3.X 或更高版本打包所有第三方 iOS 应用程序，然后在 Endpoint Management 控制台中升级这些应用程序。请访问 MDX Toolkit 下载页面以获取最新版本。

在将本地 **Citrix ADC** 升级到 **13.0-64.35+** 之前的准备工作

如果您使用 Citrix ADC 的本地版本并升级到版本 13.0—64.35+：使用Endpoint Management 20.10.1 中的已知问题中描述的解决方法。

Endpoint Management 23.7.0

Play Integrity API。根据 Google 的弃用时间表，Play Integrity API 取代了即将弃用的 SafetyNet Attestation API。有关启用此 API 的更多信息和步骤，请参阅启用 Play Integrity API，请参阅此 Play Integrity API 文章。

Endpoint Management 23.6.0

此版本解决了多个有助于改进整体性能和稳定性的问题。未添加任何新功能。

Endpoint Management 23.4.0

此版本解决了多个有助于改进整体性能和稳定性的问题。未添加任何新功能。

当前已知问题

Endpoint Management 22.6.0 中的已知问题

间歇性地，在故障排除和支持 **>** 日志下选择要下载的所有三种日志类型（调试、管理员审核、用户审核）不起作用。仅下载调试日志。解决方法是，您可以单独下载每个日志，也可以通过选中所有三个复选框以隐身模式打开浏览器下载所有日志。[CXM-105334]

在 Android Enterprise 中创建网页链接时，尝试使用图标保存应用程序时会出错。这是 Google 的服务问题。解决方法是在不上传图标的情况下保存应用程序。[CXM-105395]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

即使已弃用，Samsung Knox/Safe 策略在已注册的设备上仍处于活动状态，并且无法禁用或配置。解决方法是取消注册并重新注册设备。[CXM-104303]

Endpoint Management 22.4.0 中的已知问题

在 **Monitor**（监视）选项卡上搜索已注册的 Active Directory 用户时，不会为该用户显示已注册的设备。您仍然可以从 “管理**”>“**设备” 中查看分配给用户的策略和应用程序，并使用所有安全操作。iOS 和 Android 注册的设备都会受到影响。[CXM-104283]

由于 Google 服务存在问题，私有应用程序无法使用 Android Enterprise 发布。问题解决后，我们将更新我们的文档。[CXM-103690]

Endpoint Management 21.12.0 中的已知问题

迁移到基于 Citrix Cloud 的 RBAC 后，在 Citrix Cloud 中拥有完全访问权限的管理员用户也可以在 CEM 中获得完全访问权限，即使他们在迁移之前具有自定义权限。解决方法：可以使用所需的访问权限在 Citrix Cloud“身份识别和访问管理” 页面上更新管理员权限。[CXM-102765]

在 2018 年之前注册的客户拥有控制台的本地管理员访问权限。具有添加或编辑本地用户权限的 CEM 管理员用户也可以在 Citrix Cloud 中添加或编辑本地用户。这包括更改本地用户的密码。要修复此问题，您可以致电支持部门，阻止本地管理员直接访问控制台，仅允许 Citrix Cloud 管理员访问。[CXM-102780]

Endpoint Management 21.11.0 中的已知问题

在仅在 MAM 下注册的 iOS 设备上，企业应用程序无法安装。[CXM-101852]

当 CEM 服务器升级到 21.11.0 时，使用适用于 Android Enterprise 版的自动更新托管应用程序策略无法在设备上应用。策略失败会影响设备上的应用程序更新。解决方法是，管理员可以编辑并保存策略以刷新默认值。[CXM-102446]

Endpoint Management 21.10.0 中的已知问题

VPN 设备策略在托管的 Windows 11 设备上无法正常工作。我们向 Microsoft 报告了此问题，并且正在与他们合作解决该问题。我们将提供任何进展的最新信息。

Endpoint Management 21.9.1 中的已知问题

在企业拥有的设备模式下注册工作配置文件的 Android 设备上：用户可能会看到错误消息，指出他们无法在个人配置文件中安装或搜索应用程序。如果用户看到这些错误，请更新 Google Play 应用商店应用程序并重试。[CXM-100678]

Endpoint Management 21.5.0 中的已知问题

如果用户有以下条件，则无法向 Azure Active Directory (AAD) 进行身份验证

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 使用 AAD 凭据在 Endpoint Management 中注册他们的设备。
2. 启动 Office 365 应用程序并完成 AAD 注册。
3. 从 Microsoft 身份验证器应用程序中删除他们的帐户。
4. 启动 Office 365 应用程序并注销。

解决方法：从 Endpoint Management 中取消注册设备并重新注册。[CXM-90235]

Endpoint Management 21.4.0 中的已知问题

如果尝试重新注册的用户与最初在设备上注册的用户不同的 Azure Active Directory 用户，则在 iOS 设备上重新注册失败。解决方法：重新注册之前，请从设备上的 Microsoft Authenticator 应用程序中取消注册原始用户。[CXM-90218]

Endpoint Management 21.2.0 中的已知问题

将 Secure Web 添加为适用于 Android Enterprise 的 MDX 应用时，托管 Google Play 无法使用应用标识符找到该应用程序。如果搜索 “Secure Web” 而非应用程序标识符，托管 Google Play 应用程序可以找到该应用程序。此问题属于 Google 缺陷。[CXM-91991]

导入 SSL 侦听器证书可能会失败。按照 CTX-297153 中的步骤重新打包证书密钥库。[XMHELP-3346]

Endpoint Management 20.10.1 中的已知问题

如果您将本地 Citrix ADC 升级到 13.0-64.35 或更高版本，并且 Endpoint Management 未启用 Workspace：单点登录 Citrix Files 或 ShareFile 域 URL 将导致出现错误。用户无法登录。此错误仅出现在具有 **Company Employee Sign in**（公司员工登录）选项的浏览器中。

要解决此问题：如果尚未从 Citrix Gateway 上的 ADC CLI 运行以下命令，请运行它们以启用全局 SSO：

```
set vpn parameter SSO ON

bind vpn vs <vsName> -portalTheme X1
```

有关详细信息，请参阅：

- Citrix ADC 版本
- 影响的 SSO 配置

执行完此解决方法后，用户可以在浏览器中使用公司员工登录选项通过 SSO 向 Citrix Files 或 ShareFile 域 URL 进行身份验证。[CXM-88400]

Endpoint Management 20.2.1 中的已知问题

在 Citrix Endpoint Management 控制台中使用 ShareFile URL 配置 Citrix Content Collaboration 后，单击测试连接按钮将导致出现错误。要解决此问题，请禁用针对 ShareFile 的多重身份验证。要了解有关此问题及其解决方法的更多信息，请参阅支持页面。[CXM-79240]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 20.1.0 中的已知问题

将用户添加到 Citrix Cloud 中的库时，Endpoint Management 会报告成功，但不会添加用户。[CXM-73726]

Endpoint Management 19.11.0 中的已知问题

MDX 和公共应用程序无法从控制台中删除。解决方法为，选择要删除的应用程序，然后单击编辑。取消选择 **Android Enterprise** 并从平台列表中选择任何其他平台。保存应用程序。然后，您可以删除该应用程序。[CXM-74468]

Endpoint Management 19.5.0 中的已知问题

注册 Citrix Ready Workspace Hub 设备时，请在允许列表中定义以太网 (eth0) MAC 地址，以避免注册失败。[CXM-43141]

Endpoint Management 19.4.1 中的已知问题

选项卡式浏览 Windows GPO 设备策略中的选项时，会跳过单选按钮和复选框。[CXM-58277]

Endpoint Management 19.2.1 中的已知问题

如果您通过通过 Google 管理控制台删除 Android Enterprise 来取消该企业的注册：尝试重新注册该企业可能会失败。请始终使用 Endpoint Management 控制台取消注册 Android Enterprise 企业，如取消注册 Android Enterprise 企业中所述。Google Workspace 客户，请按照取消注册 Android Enterprise 企业中的说明进行操作。[CXM-62709] [CXM-62950]

Endpoint Management 19.2.0 中的已知问题

在 Endpoint Management 10.18.3 中创建公共应用商店应用程序时：在 iPad 的“应用程序设置”页面上，如果单击返回而不搜索应用程序，然后单击下一步，则会出现以下问题。导航按钮显示无响应，并且不允许您搜索应用程序。为 iOS 或 Android 创建公共应用商店应用程序时会出现此问题。[CXM-46820]

Endpoint Management 10.19.1 中的已知问题

在设置 **> Android Enterprise** 页面上完成注册过程后，将显示以下错误消息：“发生配置错误。请重试”。关闭错误消息时，您的 Android Enterprise 配置将保存，但启用 **Android Enterprise** 设置为关。要解决此问题，请将应用程序类别的数量减少到 30 或更少。[CXM-60899]

Endpoint Management 10.18.5 中的已知问题

Chrome 应用程序配置为 Chrome OS 设备的必需应用程序时：用户可能需要注销并重新登录以安装该应用程序。此第三方问题为 Google 缺陷 ID #76022819。[CXM-48060]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 10.18.3 中的已知问题

删除具有已注册设备的 Citrix Cloud 管理员后：Endpoint Management 在管理员从 Secure Hub 应用程序或自助服务门户重新登录之前不更新 Endpoint Management 控制台中的用户角色。[CXM-45730]

Endpoint Management 10.7.4 中的已知问题

如果将 Endpoint Management 配置为使用具有 Azure Active Directory 的 Citrix 身份提供程序进行单点登录 (SSO)：Endpoint Management 管理员或用户重定向到 **Azure Active Directory** 登录屏幕时，该屏幕将包括消息 “Sign-in page for Citrix Secure Hub”（Citrix Secure Hub 的登录页面）。正确的消息为 “Sign-in page for Citrix Endpoint Management console”（Citrix Endpoint Management 控制台的登录页面）。[CXM-42309]

第三方声明

April 15, 2020

Citrix Endpoint Management 可能包含根据以下文档中定义的条款进行许可的第三方软件：

Citrix Endpoint Management 第三方声明

弃用

July 24, 2023

本文中的公告是关于正在逐渐淘汰的 Citrix Endpoint Management 功能的提前通知，以便您能够及时制定业务决策。Citrix 将监视客户使用情况和反馈以确定其退出时间。在后续版本中声明可能会有更改，可能不会包括每个弃用的特性或功能。有关产品生命周期支持的详细信息，请参阅 Product Lifecycle Support Policy（产品生命周期支持策略）一文。

> 重要：
>
> 感谢您使用 Endpoint Management Analyzer 工具，我们对此表示感谢。由于我们的发布节奏频繁且稳定，因此不再需要此工具。Citrix 已决定自 2023 年 3 月 31 日起停止这项服务。我们建议您使用 Citrix Endpoint Management 控制台或 Citrix NetScaler Gateway 中提供的连接检查功能。有关详细信息，请参阅连接检查。

弃用和删除

下面的列表显示了已弃用或已删除的 Citrix Endpoint Management 功能。

已弃用的项目不会立即删除。Citrix 将继续支持已弃用的项目，直到在将来的版本中将其删除为止。

在 Citrix Endpoint Management 中，已删除的项目已被删除或不再受支持。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

有关已达到生命周期结束的移动生产力应用程序的信息，请参阅 EOL 和已弃用的应用程序。

项目	说明	宣布弃用	已删除	备选
SafetyNet Attestation API	根据 Google 在此处发布的公告，已弃用对 Android SafetyNet Attestation 的支持。	2023 年 7 月	November 2023	播放完整性 API
Chrome OS	弃用了对 Chrome OS 的支持。	2022 年 7 月	2023 年 5 月	无备选
tvOS	弃用了对 tvOS 的支持。	2022 年 7 月	2023 年 5 月	无备选
Windows 信息保护 (WIP)	根据 Microsoft 在此处发布的公告，已弃用对 Windows Information Protection 的支持。	2022 年 8 月	2022 年 10 月	无备选
Endpoint Management Analyzer	已弃用对 Endpoint Management Analyzer 工具的支持。	2022 年 7 月	目标：2023 年 3 月 31 日	无备选
Workspace Hub 设备管理	已弃用对 Citrix Ready Workspace Hub 设备的支持。	2022 年 1 月	2022 年 6 月	无备选
适用于企业的 Microsoft Store	已弃用对适用于企业的 Microsoft Store 的支持。Microsoft 不再支持此平台。有关详细信息，请参阅 Microsoft 文档。	2021 年 7 月	目标：2023 年 3 月	无备选
Samsung SAFE	已弃用对 Samsung SAFE 的支持。	2022 年 1 月	2022 年 6 月	使用 Android Enterprise。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
适用于 Zebra 的自定义 XML	已弃用对 Zebra 设备上的自定义 XML 的支持。	2022 年 1 月	2022 年 6 月	使用 Android Enterprise 托管配置。
PKI 身份：Generic、Symantec PKI、DigiCert 和 Entrust	已弃用对 Generic, DigiCert 托管和 Entrust 适配器 PKI 实体的支持。	2021 年 6 月	2022 年 1 月	无备选
Android for Workspace	弃用了对 Android for Workspace 的支持	2022 年 1 月	April 2022	无备选
运营商 SMS 网关	已弃用对 Nexmo SMS 网关通知的支持	2022 年 1 月	April 2022	使用 SMTP 服务器通知
移动服务提供商 (MSP)	不建议使用 MSP 接口来查询 Blackberry 和其他 Exchange ActiveSync 设备以及发出操作	2022 年 1 月	April 2022	无备选
MDX Toolkit	弃用对支持移动应用程序管理 (MAM) SDK 的 MDX Toolkit 的支持。在过渡期间，您可以同时使用 MDX 打包的应用程序和 MAM SDK 开发的应用程序。	2020 年 3 月	2023 年 7 月	要继续管理您的企业应用程序，请使用 MAM SDK。
RBAC 角色 - 共享设备注册以及 COSU 设备注册人员	弃用对共享设备注册人员以及 COSU 设备注册人员的预定义的基于角色的访问控制设置的支持	2021 年 7 月	2021 年 12 月	通过 Apple 校园教务管理或 Apple 商务管理配置 iOS 设备。通过注册配置文件配置 Android COSU（专用）设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
Windows 设备的“允许自动连接到 Wi-Fi 感应热点”限制。	对于 Windows 10 设备，请删除对“允许自动连接到 Wi-Fi 感应热点”限制的支持。Windows 10 不再支持此功能。有关信息，请参阅 Microsoft 文档。	2021 年 10 月	2022 年 2 月	无备选
MDX：备用网关服务器	弃用了适用于 iOS 和 Android 设备的递升式身份验证。	2020 年 3 月	2021 年 9 月	无备选
MDX：Micro VPN（完整通道模式）	弃用了适用于 iOS 和 Android 设备的完整虚拟专用网络 (VPN) 通道。	2020 年 3 月	2021 年 9 月	使用 MAM SDK Web SSO 模式或使用 Citrix SSO 连接类型创建 PerApp VPN 策略。
MDX：PAC 文件支持	对 iOS 和 Android 设备的完整 VPN 通道部署使用代理自动配置 (PAC) 文件的支持已弃用。	2020 年 3 月	2021 年 9 月	使用 Citrix Gateway 通过代理服务器进行连接以访问内部网络。
MDX 共享设备支持	弃用了对 MDX 应用程序的共享设备支持。	2020 年 3 月	2021 年 9 月	对于 Android Enterprise，请使用注册为专用设备的共享设备。对于 iOS，请使用 Apple 校园教务管理或 GroundControl。
Android - Sony	弃用了对 Android Sony 设备和 Sony 特定的策略的支持。	2021 年 1 月	2022 年 2 月	使用 Android Enterprise
Android - HTC	弃用了对 Android HTC 设备和 HTC 特定的策略的支持。	2021 年 1 月	2022 年 2 月	使用 Android Enterprise

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
Android - Amazon	已弃用对 Android Amazon 设备和 Amazon 特定策略的支持。	2021 年 1 月	2022 年 2 月	使用 Android Enterprise
Knox Mobile Enrollment（旧版 DA）	已弃用在所有 Android 版本中的旧版设备管理员模式下对 Knox Mobile Enrollment (KME) 的支持。	2021 年 5 月 4 日	2021 年 9 月	使用 KME 在 Android Enterprise 模式下注册。Android 8、9、10、11 支持 Android Enterprise。
高安全性注册模式	弃用了对生成使用高安全性注册安全模式的注册邀请的支持。	2021 年 7 月	2022 年 2 月	请参阅注册邀请，获取受支持的注册安全模式列表。
派生凭据	弃用了对派生凭据和 Citrix Derived Credential Manager 应用程序的支持。	2021 年 3 月	2021 年 12 月	有关 iOS 支持的身份验证类型的列表，请参阅 iOS。
APNs 传出端口	Apple 对 APNs 旧版二进制文件协议的支持将于 2021 年 3 月 31 日结束。Apple 建议您改为使用基于 HTTP/2 的 APNs 提供程序 API。作为此更改的一部分，我们将弃用对用于向 `*.push.apple.com` 发送 APNs 通知的端口 2195 和 2196 的支持。	2020 年 10 月	2021 年 3 月	请改为使用端口 443。请参阅网络和防火墙要求。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
MDX Service	弃用了对支持移动应用程序管理 (MAM) SDK 的 MDX Service 的支持。在过渡期间，您可以同时使用通过 MDX Toolkit 进行的 MDX 打包的应用程序和 MAM SDK 开发的应用程序。	2020 年 3 月	2021 年 9 月	要继续封装您的企业应用程序，请使用 MDX Toolkit。
自助服务门户中的注册邀请设置	弃用了对用户从自助服务门户生成注册邀请的支持。	2021 年 7 月	2021 年 7 月	请与管理员联系，在 Endpoint Management 控制台中生成注册邀请。
注册邀请设置	弃用了对使用设备 IMEI、序列号和 UDID 创建注册邀请的支持。	2021 年 4 月	2021 年 7 月	创建注册邀请时，请在 Endpoint Management 控制台中的 **Manage**（管理）**> Enrollment Invitation**（注册邀请）下配置可用的设置。
基于证书的身份验证签名算法（非 FIPS 和弱密码）	已弃用对以下签名算法的支持：SHA1withRSA、SHA224withRSA、SHA1withECDSA、SHA224withECDSA、SHA1withDSA、RIPEMD160withRS RIPEMD128withRS RIPEMD256withRS	2020 年 5 月	2021 年 6 月	在 Endpoint Management 控制台（设置 **>** 凭据提供程序 **>** 证书签名请求）中为凭据提供程序创建 CSR 时，请选择较强的密码。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
适用于 Android 7.x 和 iOS 12.x 的 Citrix 移动应用程序和 Workspace 应用程序	弃用了对 Android 7.x 和 iOS 12.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持。	2021 年 4 月	2021 年 6 月	请每个主操作系统平台的当前版本和早期版本（最低版本）。较旧的设备保持注册状态。但是，Citrix 不测试也不支持旧设备。
适用于 Android 的 RSA 软令牌支持	弃用了对将 RSA 软令牌直接导入 Secure Hub for Android 的支持。	2021 年 1 月	2021 年 2 月	可以在 Google Play 中提供的 RSA Secure ID 应用程序中导入 RSA 软令牌。然后，可以使用该令牌进行 Citrix Gateway 身份验证。
Internet Explorer 11	已弃用支持 Internet Explorer 与 Endpoint Management 控制台一起使用。	2021 年 1 月	2021 年 1 月	请使用以下 Web 浏览器的最新版本：Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari
Endpoint Management Analyzer 中的网关配置检查	已弃用对网关配置检查选项的支持。	2020 年 11 月	2020 年 11 月	使用 Analyzer 中的 Citrix Insight Services 检查检查您的 Citrix ADC 配置是否准备好部署 Endpoint Management。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
在 Android Enterprise 设备上为旧版设备管理员模式发布的应用程序	我们不再将为旧版 DA 平台发布的应用程序发布到在 Android Enterprise 中注册的设备。	2020 年 10 月	2020 年 11 月	对于 Android Enterprise 设备，请发布适用于 Android Enterprise 平台的应用程序。要继续将旧版 DA 应用程序发布到 DA 模式下的设备，请为这些应用程序创建单独的交付组。
适用于 Android 10 设备的旧版设备管理员模式	Google 弃用了一些设备管理员 API。自升级到针对 Android API 级别 29 的 Citrix Secure Hub 起，Citrix 将不支持注册到设备管理员模式的 Android 10 设备。	2020 年 2 月	2020 年 11 月	将 Android 10 设备迁移到 Android Enterprise。
Android TouchDown	DigiCert 已停止支持 Android TouchDown。Citrix 从 Exchange 设备策略中删除了 Android TouchDown 平台页面。	2018 年 7 月	2020 年 11 月	建议：使用 Citrix Secure Mail。
适用于 Android 10 的新设备管理员注册	已禁用在 Android 10 设备上对新注册或重新注册到旧版设备管理员模式的支持。已注册的设备将继续工作。	2020 年 2 月	2020 年 9 月	将新 Android 10+ 设备注册到 Android Enterprise。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
MDX 加密	弃用了 Endpoint Management 控制台中的 MDX 加密和 MDX 加密功能。	2019 年 10 月	2020 年 9 月	使用我们的加密管理功能启用 iOS 或 Android 平台加密，并增加合规性检查。确保您已在 2020 年 7 月之前测试并计划从 MDX 加密迁移。
Windows Mobile/CE	弃用了对 Windows Mobile/CE 设备的支持。	2018 年 4 月	2020 年 9 月	使用 Windows 10 Desktop 和 Laptop。
Samsung SEAMS 容器	弃用了对 Samsung SEAMS 容器的支持。	2020 年 6 月	2020 年 8 月	使用 Android Enterprise。
远程支持	已弃用远程支持客户端。	2019 年 1 月	2020 年 8 月	无备选
适用于 Android 6.x 和 iOS 11.x 的 Citrix 移动应用程序和 Workspace 应用程序	弃用了对 Android 6.x 和 iOS 11.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持。	2020 年 4 月	2020 年 6 月	请每个主操作系统平台的当前版本和早期版本（最低版本）。较旧的设备保持注册状态。但是，Citrix 不测试也不支持旧设备。
适用于 iOS 的 Secure Hub 网络扩展	弃用了允许您为 iOS 设备自定义网络连接功能的网络扩展框架。Secure Hub 版本 20.3.0。	2018 年 10 月	2020 年 3 月	无备选
使用本地帐户的 API 登录	管理员将无法再使用本地帐户登录 REST API。	2020 年 10 月		管理员可以使用 Citrix Cloud 帐户登录。请参阅 REST API。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

项目	说明	宣布弃用	已删除	备选
自签名安全套接字层 (SSL) 证书	已弃用对所有设备平台的自签名 SSL 证书的支持。	2020 年 5 月		使用知名证书颁发机构 (CA) 颁发的可信 SSL 证书替换现有的自签名证书。

系统要求

May 8, 2023

等待 Citrix 预配 Endpoint Management 时，请务必通过安装 Cloud Connector 来为您的 Endpoint Management 部署做好准备。虽然 Citrix 托管和交付您的 Endpoint Management 解决方案，但是仍需要某些通信和端口设置。该设置将 Endpoint Management 体系结构连接到企业服务，例如 Active Directory。

Cloud Connector 要求

Citrix 使用 Cloud Connector 将 Endpoint Management 体系结构集成到您的现有体系结构中。Cloud Connector 通过端口 443 将以下资源位置安全地集成到 Endpoint Management 中：LDAP、PKI 服务器、内部 DNS 查询以及 Citrix Workspace 枚举。

- 至少两台加入到您的 Active Directory 域的专用 Windows Server 计算机。这些计算机可以是虚拟机，也可以是物理机。要安装 Connector 的计算机必须与 UTC 时间同步，才能正确安装和操作。有关最新要求的完整列表，请参阅您的 Citrix 帐户团队提供的部署资料。

  入门向导引导您完成在这些计算机上安装 Cloud Connector 的过程。

- 有关更多平台系统要求，请参阅 Citrix Cloud Connector。

支持的 **Active Directory** 功能级别

Citrix Cloud Connector 支持 Active Directory 中的以下林和域功能级别，以便与 Endpoint Management 结合使用。

林功能级别	域功能级别	支持的域控制器
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

林功能级别	域功能级别	支持的域控制器
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016

Citrix Gateway 要求

Endpoint Management 要求针对以下场景在您的资源位置中安装 Citrix Gateway：

- 您需要 Micro VPN 才能访问业务线应用的内部网络资源。这些应用程序通过 Citrix MDX 技术封装。Micro VPN 需要 Citrix Gateway 连接到内部后端基础结构。
- 您计划使用 Citrix 移动生产力应用程序，例如 Citrix Secure Mail。
- 您计划将 Endpoint Management 与 Microsoft Endpoint Manager 集成。

要求：

- 域 (LDAP) 身份验证
- Citrix Gateway 12.1 或更高版本，具有平台/通用许可证

有关详细信息，请参阅 许可。

- 公用 SSL 证书。

有关详细信息，请参阅在 Citrix ADC 设备上创建和使用 SSL 证书。

- Citrix Gateway 虚拟服务器的未使用公用 IP 地址
- Citrix Gateway 虚拟服务器的公共可解析完全限定域名 (FQDN)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 云托管 Endpoint Management 中间证书和根证书（在脚本包中提供）
- 代理负载平衡器 IP 的未使用内部专用 IP 地址
- 有关端口要求，请参阅本文后面的Citrix Gateway 端口要求 。
- Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成
- 在 Microsoft Azure 上部署 Citrix ADC VPX 实例

有关 Citrix Gateway 要求的信息，请参阅 Citrix 客户团队提供的部署材料。

有关 Android Enterprise 要求的信息，请参阅 Android Enterprise 部分。

Citrix Files 要求

Citrix Files 文件同步和共享服务在 Endpoint Management Premium 服务方案中可用。存储区域控制器通过向您的 Citrix Files 帐户提供私有数据存储来扩展 Citrix Files 软件即服务 (SaaS) 云存储。

存储区域控制器要求：

- 专用物理机或虚拟机
- Windows Server 2012 R2 或 Windows Server 2016
- 2 个 vCPU
- 4 GB RAM
- 50 GB 硬盘空间
- Web 服务器 (IIS) 的服务器角色：
  - 应用程序开发：ASP. NET 4.5.2
  - 安全性：基本身份验证
  - 安全性：Windows 身份验证

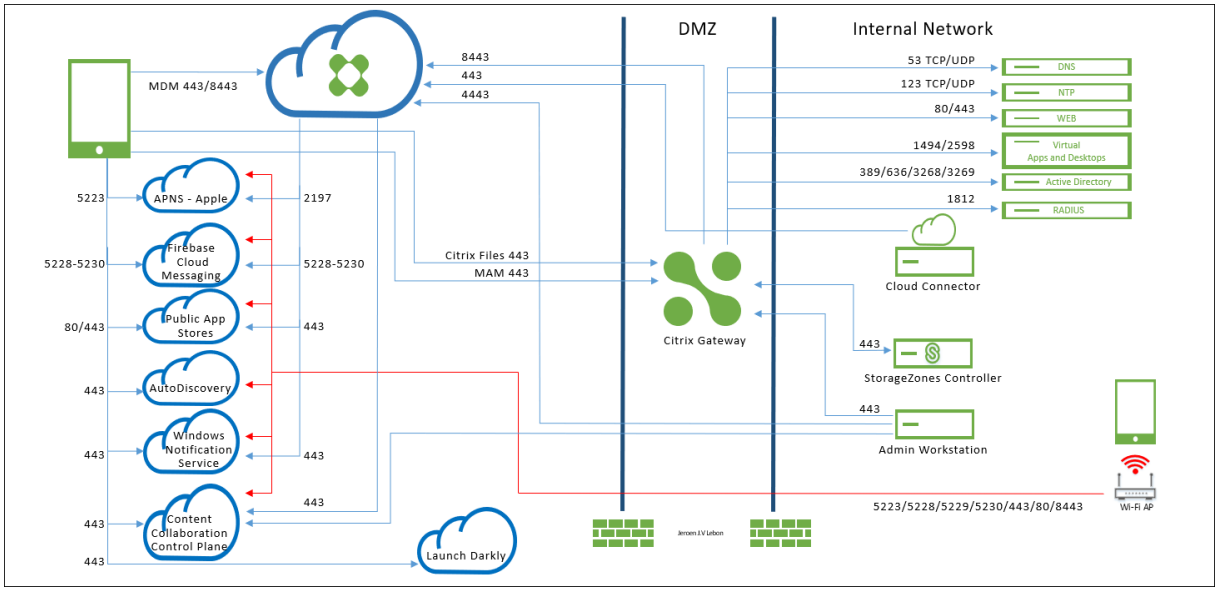
Citrix Files 平台要求：

- Citrix Files 安装程序要求在 Windows Server 上具有管理权限
- Citrix Files 管理员用户名

端口要求

要使设备和应用程序能够与 Endpoint Management 通信，应在防火墙中打开特定端口。下图显示了 Endpoint Management 的流量图。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



以下部分列出了必须打开的端口。有关移动生产力应用程序使用的 URL 的信息，请参阅 功能标志管理。

Citrix Gateway 端口要求

打开端口以允许用户通过 Citrix Gateway 从 Citrix Secure Hub 和 Citrix Workspace 连接到：

- Endpoint Management
- StoreFront
- 其他内部网络资源，例如 Intranet Web 站点

有关 Citrix Gateway 的更多信息，请参阅 Citrix Gateway 文档中的配置 Citrix Endpoint Management 环境的设置。有关 IP 地址的信息，请参阅 NetScaler Gateway 文档中的 NetScaler Gateway 如何使用 IP 地址。

TCP 端口	说明	源	目标
53（TCP 和 UDP）	用于 DNS 连接。	Citrix Gateway SNIP	DNS 服务器
80/443	Citrix Gateway 通过第二个防火墙将 Micro VPN 连接传递到内部网络资源。	Citrix Gateway SNIP	Intranet Web 站点
123（TCP 和 UDP）	用于网络时间协议 (NTP) 服务。	Citrix Gateway SNIP	NTP 服务器
389	用于非安全 LDAP 连接。	Citrix Gateway NSIP（或者 SNIP，如果使用负载平衡器）	LDAP 身份验证服务器或 Microsoft Active Directory

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	说明	源	目标
443	用于从 Citrix Workspace 到 Citrix Virtual Apps and Desktops 与 StoreFront 的连接。	Internet	Citrix Gateway
443	用于连接到 Endpoint Management 以实现 Web、移动和 SaaS 应用程序交付。	Internet	Citrix Gateway
443	用于 Cloud Connector 通信 – LDAP、DNS、PKI 和 Citrix Workspace 枚举	Cloud Connector 服务器	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.cloud.us (government), https://*.blob.core.windows.net/, https://*.servicebus.windows.net
443	用于通过浏览器访问 Endpoint Management 自助服务门户（如果已启用）。	访问点（浏览器）	Endpoint Management (https://<sitename>/zdm/shp)
636	用于安全 LDAP 连接。	Citrix Gateway NSIP（或者 SNIP，如果使用负载平衡器）	LDAP 身份验证服务器或 Active Directory
1494	用于与内部网络中基于 Windows 应用程序的 ICA 连接。Citrix 建议保持此端口处于打开状态。	Citrix Gateway SNIP	Citrix Virtual Apps and Desktops
1812	用于 RADIUS 连接。	Citrix Gateway NSIP	RADIUS 身份验证服务器

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	说明	源	目标
2598	用于使用会话可靠性连接到内部网络中基于 Windows 的应用程序。Citrix 建议保持此端口处于打开状态。	Citrix Gateway SNIP	Citrix Virtual Apps and Desktops
3269	用于 Microsoft Global Catalog 安全 LDAP 连接。	Citrix Gateway NSIP（或者 SNIP，如果使用负载平衡器）	LDAP 身份验证服务器或 Active Directory
4443	用于管理员通过浏览器访问 Endpoint Management 控制台。	访问点（浏览器）	Endpoint Management
8443	用于注册、应用商店和移动应用程序管理 (MAM)。	Citrix Gateway SNIP	Endpoint Management
8443	用于 Secure Mail 身份验证令牌的 Secure Ticket Authority (STA) 端口	Citrix Gateway SNIP	Endpoint Management

网络和防火墙要求

要使设备和应用程序能够与 Endpoint Management 通信，应在防火墙中打开特定端口。下表列出了这些端口。

打开从内部网络到 Citrix Cloud 的端口：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	源 IP	说明	目标	目标 IP
443		Cloud Connector	https://*.citrixworkspac.net, https://*.cloud.com (commercial), https://*.cloud.us (government), https://*.sharefile.com, https://cwsproduction.blob.core.wind ows.net/downloads, https://*.servicebus.windows.net	
443		管理控制台	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.cloud.us (government), https://*.citrix.com, https://cwsproduction.blob.core.windows.net/downloads	

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	源 IP	说明	目标	目标 IP
443		Endpoint Management 自助服务门户通过浏览器访问（如果启用了该门户）	Endpoint Management	
4443		通过浏览器访问 Endpoint Management 控制台	Endpoint Management	

打开从 Internet 到 DMZ 的端口：

TCP 端口	说明	源 IP	目标	目标 IP
443	Endpoint Management 客户端设备		Citrix Gateway IP	
443	Endpoint Management 客户端设备		Citrix Gateway VIP	
443	Citrix Files 公用 IP	CTX208318	Citrix Gateway VIP	

打开从 DMZ 到内部网络的端口：

TCP 端口	说明	源 IP	目标	目标 IP
389 或 636	Citrix Gateway NSIP		Active Directory IP	
53 (UDP)	Citrix Gateway NSIP		DNS 服务器 IP	
443	Citrix Gateway SNIP		Exchange (EAS) Server IP	
443	Citrix Gateway SNIP		内部 Web 应用程序/服务	

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	说明	源 IP	目标	目标 IP
443	Citrix Gateway SNIP		存储区域控制器 IP	

打开从内部网络到 DMZ 的端口：

TCP 端口	说明	源 IP	目标	目标 IP
443	管理客户端		Citrix Gateway NSIP	

打开从内部网络到 Internet 的端口：

TCP 端口	说明	源 IP	目标	目标 IP
443	Exchange (EAS) Server IP		Endpoint Management 推送通知侦听器 (1)	
443	存储区域控制器 IP		Citrix Files 控制平面	CTX208318

(1)us-east-1.mailboxlistener.xm.citrix.com, eu-west-1.mailboxlistener.xm.citrix.com, ap-southeast-1.mailboxlistener.xm.citrix.com

打开从企业 Wi-Fi 到 Internet 的端口：

TCP 端口	说明	源 IP	目标	目标 IP
8443 / 443	Endpoint Management 客户端设备		Endpoint Management	
5223	Endpoint Management 客户端设备		Apple APNS 服务器	17.0.0.0/8

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	说明	源 IP	目标	目标 IP
5228	Endpoint Management 客户端设备		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5229	Endpoint Management 客户端设备		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5230	Endpoint Management 客户端设备		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
443	Endpoint Management 客户端设备		Firebase Cloud Messaging	fcm.googleapis.com
443	Endpoint Management 客户端设备		Windows 推送通知服务	*.notify.windows.com
443 / 80	Endpoint Management 客户端设备		Apple iTunes App Store	ax.apps.apple.com, *.mzstatic.com, vpp.itunes.apple.com

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	说明	源 IP	目标	目标 IP
443 / 80	Endpoint Management 客户端设备		Google Play	play.google.com, android.clients.google.com, android.l.google.com, android.com, google-analytics.com
443 / 80	Endpoint Management 客户端设备		Microsoft 应用商店	login.live.com, *.notify.windows.com
443	Endpoint Management 客户端设备		适用于 iOS 和 Android 的 Endpoint Management 自动发现服务	discovery.cem.cloud.us
443	Endpoint Management 客户端设备		适用于 Windows 的 Endpoint Management 自动发现服务	enterpriseenrollment.mycompany.com, discovery.cem.cloud.us
443	存储区域控制器 IP		Citrix Files 控制平面	CTX208318
443	Endpoint Management 客户端设备		Google Mobile Management、Google API、Google Play 应用商店 API	*.googleapis.com

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

TCP 端口	说明	源 IP	目标	目标 IP
443	Endpoint Management 客户端设备		v470 之前的 CloudDPC 版本的连接性检查。自 NMR1 起的 Android 连接检查要求 `https://www.google.com/generate_204` 可访问，或者要求指定的 Wi-Fi 网络指向可访问的 PAC 文件）	`connectivitycheck.android.com`，`www.google.com`

自动发现服务连接的端口要求

此端口配置可确保从 Secure Hub for Android 连接的 Android 设备可以从内部网络访问 Endpoint Management 自动发现服务 (ADS)。下载通过 ADS 提供的任何安全更新时能够访问 ADS 非常重要。

> 注意：
>
> ADS 连接可能不支持您的代理服务器。在这种情况下，允许 ADS 连接跳过代理服务器。

如果您希望启用证书固定，请完成以下必备条件：

- 收集 **Endpoint Management** 服务器和 **Citrix Gateway** 证书：证书必须采用 PEM 格式，且必须是公有证书而不是私钥。
- 联系 **Citrix** 支持人员并请求启用证书锁定：在此过程中，系统会要求您提供证书。

证书固定功能要求设备先连接到 ADS，然后再注册。此要求确保 Secure Hub 可以使用最新的安全信息。为了 Secure Hub 注册设备，该设备必须访问 ADS。因此，在内部网络内开放 ADS 访问权限对于启用设备注册至关重要。

要允许访问适用于 Android/iOS 的 Secure Hub 的 ADS，请为以下 FQDN 打开端口 443：

FQDN	Port（端口）	IP 和端口用法
`discovery.cem.cloud.us`	443	Secure Hub - 通过 CloudFront 进行的 ADS 通信

有关支持的 IP 地址的信息，请参阅来自 AWS 的基于云的存储中心。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android Enterprise 网络要求

有关为 Android Enterprise 设置网络环境时要考虑的出站连接的信息，请参阅 Google 支持文章 Android Enterprise Network Requirements（Android Enterprise 网络要求）。

应用程序要求

Citrix Endpoint Management 支持添加和维护多达 300 个应用程序。超过此限制会导致您的系统变得不稳定。

Endpoint Management 兼容性

September 13, 2022

要使用新功能、修复和策略更新，Citrix 建议您安装以下组件的最新版本：

- Citrix 建议您将移动应用程序管理 (MAM) SDK 与企业级 iOS 和 Android 应用程序集成，以将 MDX 功能应用到这些应用程序。

  MDX Toolkit 计划于 2023 年 7 月达到生命周期已结束状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

- 移动生产力应用程序

本文概述了可以集成的受支持的 Endpoint Management 组件的版本。

最新版本的 Secure Hub、MDX Toolkit 和移动生产力应用程序与最新版本和前两个版本的 Endpoint Management 兼容。

移动生产力应用程序

用户从公共应用商店访问移动生产力应用程序。最新版本的移动生产力应用程序要求使用最新版本的 Secure Hub。这两个版本的应用程序与最新版本的 Secure Hub 兼容。

有关移动生产力应用程序两周一次的分阶段发布节奏的详细信息，请参阅发布时间表。有关支持详细信息，请参阅支持移动生产力应用程序。

MAM SDK

MAM SDK 提供了 iOS 和 Android 平台不涵盖的 MDX 功能。您可以在内部应用商店或公共应用商店中提供这些应用程序。请参阅 MDX 应用程序 SDK。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

MDX Toolkit

MDX Toolkit 计划于 2023 年 7 月达到生命周期已结束状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

Citrix 支持三个最新版本 (n.n.n) 的 MDX Toolkit。请参阅 MDX Toolkit 中的新增功能。

浏览器支持

Endpoint Management 控制台需要下列受支持的 Web 浏览器之一：

- Google Chrome 的最新版本
- Mozilla Firefox 的最新版本
- Microsoft Edge 的最新版本
- Apple Safari 的最新版本

支持的设备操作系统

July 24, 2023

本文介绍 Endpoint Management 支持的进行企业移动性管理的设备。由于平台限制和安全功能，Endpoint Management 并不在所有平台上支持所有功能。

有关移动生产力应用程序的最新版本，请参阅支持移动生产力应用程序。

> 注意：
>
> Citrix 支持每个主操作系统平台的当前版本和早期版本。某些 Endpoint Management 功能无法在较旧的平台版本上运行。
>
> 有关弃用通知，请参阅弃用。

操作系统支持列表

Citrix Endpoint Management 支持以下操作系统：

- **Android**： 10.x、11.x、12.x、13.x

  Citrix 建议先升级到 Android 10+，然后再使用 Android Enterprise。有关详细信息，请参阅Android 注意事项。

- **iOS**： 13.x、14.x、15.x、16.x

  Endpoint Management 和 Citrix 移动应用程序目前不支持 iOS 14.x、iOS 15.x 和 iOS 16.x 的所有新功能。

- **iPadOS**： 13.x、14.x

  Endpoint Management 和 Citrix 移动应用程序当前不支持 iPadOS 14.x 的所有新功能。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **macOS**： 10.13x、10.14x、10.15x、11.x、12.x、13.x

  Endpoint Management 和 Citrix 移动应用程序目前不支持 macOS 11、macOS 12 和 macOS 13 的所有新功能。

- **tvOS**： 10.2、11.x、12.x、13.x。需要使用 Apple 部署计划注册的第四代 Apple TV 设备。
- **Windows 10** 和 **Windows 11 Desktop** 和 **Tablet**：（仅限 MDM）
  - Windows 10 Professional 和 Windows 11 Professional
  - Windows 10 Enterprise 和 Windows 11 Enterprise
  - Windows 10 Education 和 Windows 11 Education
  - Windows IoT Enterprise

  有关特定操作系统的支持级别，请参阅 Microsoft 文档。

Android 注意事项

升级到 Android 10 或更高版本之前：有关弃用 Google 设备管理 API 如何影响运行 Android 10+ 的设备的信息，请参阅从设备管理迁移到 Android Enterprise。另请参阅此 Citrix 博客。

- Google 已弃用设备管理 API，这会影响运行 Android 10+ 的设备。在旧版设备管理模式下注册 Android 10+ 设备失败。Citrix 不支持在设备管理模式下注册 Android 设备。
- Citrix 建议在 Android 设备上使用 Android Enterprise。有关详细信息，请参阅从设备管理迁移到 Android Enterprise。
- Google API 更改不会影响在仅 MAM 模式下注册的设备。
- 另请参阅此 Citrix 博客。

升级之前：

- 确保您的服务器基础结构符合 subjectAltName (SAN) 扩展中包含匹配的主机名的安全证书的要求。
- 要验证主机名，服务器必须提供一个具有匹配 SAN 的证书。Citrix 仅信任包含与主机名匹配的 SAN 的证书。

语言支持

December 16, 2020

Citrix 移动生产力应用程序和 Endpoint Management 控制台已修改为可用于英语以外的其他语言。支持非英语字符和键盘输入，即使应用程序未本地化为用户的首选语言时也是如此。有关所有 Citrix 产品的全球支持的详细信息，请参阅 https://support.citrix.com/article/CTX119253。

本文列出了最新版本的 Endpoint Management 支持的语言。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 控制台和自助服务门户

- 法语
- 德语
- 西班牙语
- 日语
- 韩语
- 葡萄牙语
- 简体中文

Citrix 移动生产力应用程序

X 表示应用程序可在该特定语言中使用。

iOS 和 **Android**

语言	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
日语	X	X	X	X	X	X
简体中文	X	X	X	X	X	X
繁体中文	X	X	X	X	X	X
法语	X	X	X	X	X	X
德语	X	X	X	X	X	X
西班牙语	X	X	X	X	X	X
韩语	X	X	X	X	X	X
葡萄牙语	X	X	X	X	X	X
荷兰语	X	X	X	X	X	X
意大利语	X	X	X	X	X	X
丹麦语	X	X	X	X	X	X
瑞典语	X	X	X	X	X	X
希伯来语	X	X	X	X	X	仅限 iOS
阿拉伯语	X	X	X	X	X	X
俄语	X	X	X	X	X	X
土耳其语	X	X	仅限 Android	-	-	-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

语言	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
波兰语	X	X	X	-	-	-

对从右至左书写的语言的支持

下表概述了每个应用程序对中东语言文本的支持情况。X 指示功能是否对响应的平台可用。对于 Windows 设备，不支持从右向左排列的语言。

应用程序	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
QuickEdit	X	X

FIPS 140-2 合规性

December 3, 2021

美国国家标准和技术研究所 (US National Institute of Standards and Technologies, NIST) 发布了联邦信息处理标准 (Federal Information Processing Standard, FIPS)。FIPS 指定了安全系统中使用的加密模块的安全要求。FIPS 140-2 是此标准的第二版。有关 NIST 验证的 FIPS 140 模块的更多信息，请参阅 NIST 计算机安全资源中心。

iOS 上的所有静态数据和传输中数据加密操作都使用经过 FIPS 验证的加密模块。在 Android 上，所有静态数据加密操作都使用 Citrix 提供的经 FIPS 验证的加密模块或设备制造商提供的平台的加密模块。有关设备制造商的模块的详细信息，请与 Citrix 代表联系。

在受支持的 Windows 设备上，用于移动设备管理 (MDM) 的所有静态数据和传输中数据加密操作均使用 FIPS 验证的加密模块。

Citrix Endpoint Management MDM 的所有静态数据和传输中数据加密操作均使用经过 FIPS 验证的加密模块。MDM 流的所有静态数据和传输中数据在端到端传输时使用 FIPS 合规加密模块。该安全性包括上面介绍的移动设备加密操作，以及移动设备与 Citrix Gateway 之间的加密操作。

MDX Vault 使用 FIPS 验证的加密模块对 iOS 和 Android 设备上 MDX 包装的应用程序和关联的静态数据进行加密。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

关于 **Endpoint Management**

February 1, 2023

Citrix Endpoint Management 是一个统一的端点管理 (UEM) 解决方案，它将每个应用程序和端点集成到一个统一的视图中，从而提高安全性以及提升工作效率。有关 UEM 的概述，请参阅 Citrix Tech Zone 技术简要概述 Citrix Endpoint Management。

Endpoint Management 提供移动设备管理 (MDM) 和移动应用程序管理 (MAM)。

通过 Endpoint Management 的 MDM 功能，您可以：

- 部署设备策略和应用程序。
- 检索资产清单。
- 在设备上执行操作，例如设备擦除。

通过 Endpoint Management 的 MAM 功能，您可以：

- 保护 BYO 移动设备上应用程序和数据的安全。
- 交付企业移动应用程序。
- 锁定应用程序并擦除其数据。

结合使用 MDM 和 MAM 功能，您可以：

- 通过使用 MDM 来管理公司发放的设备
- 部署设备策略和应用程序
- 检索资产清单
- 擦除设备
- 交付企业移动应用程序
- 锁定应用程序并擦除设备上的数据

下表总结了 MDM、MAM 或 MDM+MAM 支持的 Endpoint Management 功能。

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
Android Enterprise:			
设备注册支持	是	是	是
域身份验证支持	是	否	是
域加安全令牌身份验证支持	否	否	是
客户端证书身份验证支持	否	是	是
客户端证书加域身份验证支持	否	否	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
客户端证书加安全令牌支持	否	否	是
Azure AD 身份提供程序支持	是	否	是
Okta 身份提供程序支持	是	否	是
单点登录到本机 SaaS 应用程序	是	否	是
面向企业应用程序的 Citrix 内容交付网络支持	是	是	是
面向 MDX 应用程序的 Citrix 内容交付网络支持	是	是	是
通过预配专用 Android Enterprise (COSU) 设备来支持共享设备	是	否	是
Android（旧版）：			
设备注册支持	是	是	是
域或域加安全令牌身份验证支持	否	否	是
客户端证书身份验证支持	否	是	是
客户端证书加域身份验证支持	否	否	是
客户端证书加安全令牌支持	否	否	是
Azure AD 和 Citrix 身份提供程序支持	是	否	是
Okta 身份提供程序支持	是	否	是
单点登录到本机 SaaS 应用程序	是	否	是
面向企业应用程序的 Citrix 内容交付网络支持	是	是	是
面向 MDX 应用程序的 Citrix 内容交付网络支持	是	是	是
Chrome：			

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
设备注册支持	是	否	是
用户名和密码身份验证支持	是	否	是
iOS:			
设备注册支持	是	是	是
域或域加安全令牌身份验证支持	否	否	是
客户端证书身份验证支持	否	是	是
客户端证书加域身份验证支持	否	否	是
Azure AD 和 Citrix 身份提供程序支持	是	否	是
Okta 身份提供程序支持	是	否	是
单点登录到本机 SaaS 应用程序	是	否	是
面向企业应用程序的 Citrix 内容交付网络支持	是	是	是
面向 MDX 应用程序的 Citrix 内容交付网络支持	是	是	是
Apple 教育集成	是	否	是
macOS:			
设备注册支持	是	否	否
域或域加一次性密码支持	是	否	否
邀请 URL 加一次性密码支持	是	否	否
Windows:			
设备注册支持	是	否	否
通过 Citrix Workspace 应用程序自动注册 Windows 10 和 Windows 11 设备	是	否	否

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
域或域加安全令牌身份验证支持	是	否	否
客户端证书身份验证支持	是	否	否
客户端证书加域身份验证支持	是	否	否
通过 Azure AD 或 Citrix 身份提供程序进行联合身份验证	是	否	否
面向企业应用程序的 Citrix 内容交付网络支持	是	否	否
Workspace Environment Management 集成 (3)	是	否	否

> 注意：
>
> (1) 部署排序仅适用于交付组中具有为 MDM 配置的注册配置文件的设备。
>
> (2) MAM 注册需要 Citrix Gateway。
>
> (3) Workspace Environment Management (WEM) 集成提供对各种 Windows 操作系统上的 MDM 功能的访问。

有关详细信息，请参阅管理模式.

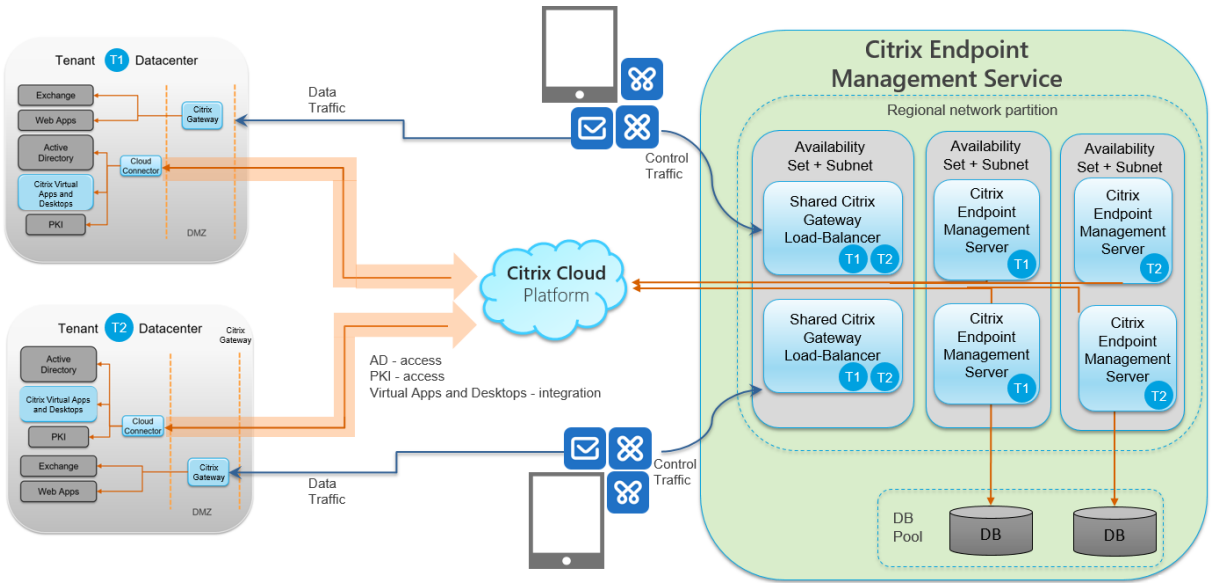
体系结构

贵组织的设备和应用程序管理要求决定您的 Endpoint Management 参考体系结构中的 Endpoint Management 组件。Endpoint Management 的组件为模块式，彼此在对方的基础之上构建。例如，您的部署包括 Citrix Gateway：

- Citrix Gateway 向用户授予对移动应用程序的远程访问权限以及跟踪用户设备类型。
- Endpoint Management 是您管理这些应用程序和设备的位置。

下图显示了 Endpoint Management 云部署的常规体系结构概览及其与您的数据中心的集成：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



下面各小节包含以下各项的参考体系结构图：

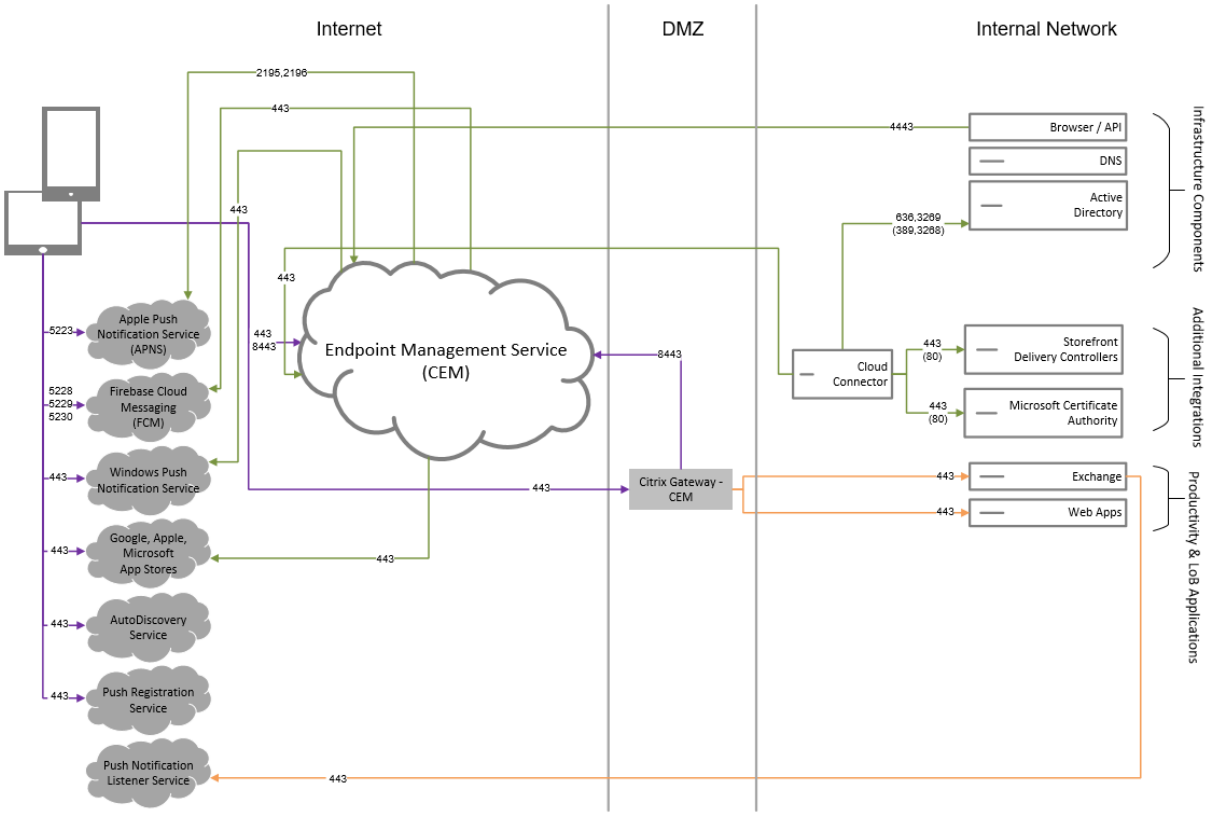
- Endpoint Management
- 可选组件，例如外部证书颁发机构、适用于 Exchange ActiveSync 的 Endpoint Management 连接器以及 Endpoint Management MDM+MAM 和 Intune MAM 通信流。

有关 Citrix ADC 和 Citrix Gateway 要求的详细信息，请参阅 Citrix 产品文档，网址为 https://docs.citrix.com/。

核心参考体系结构

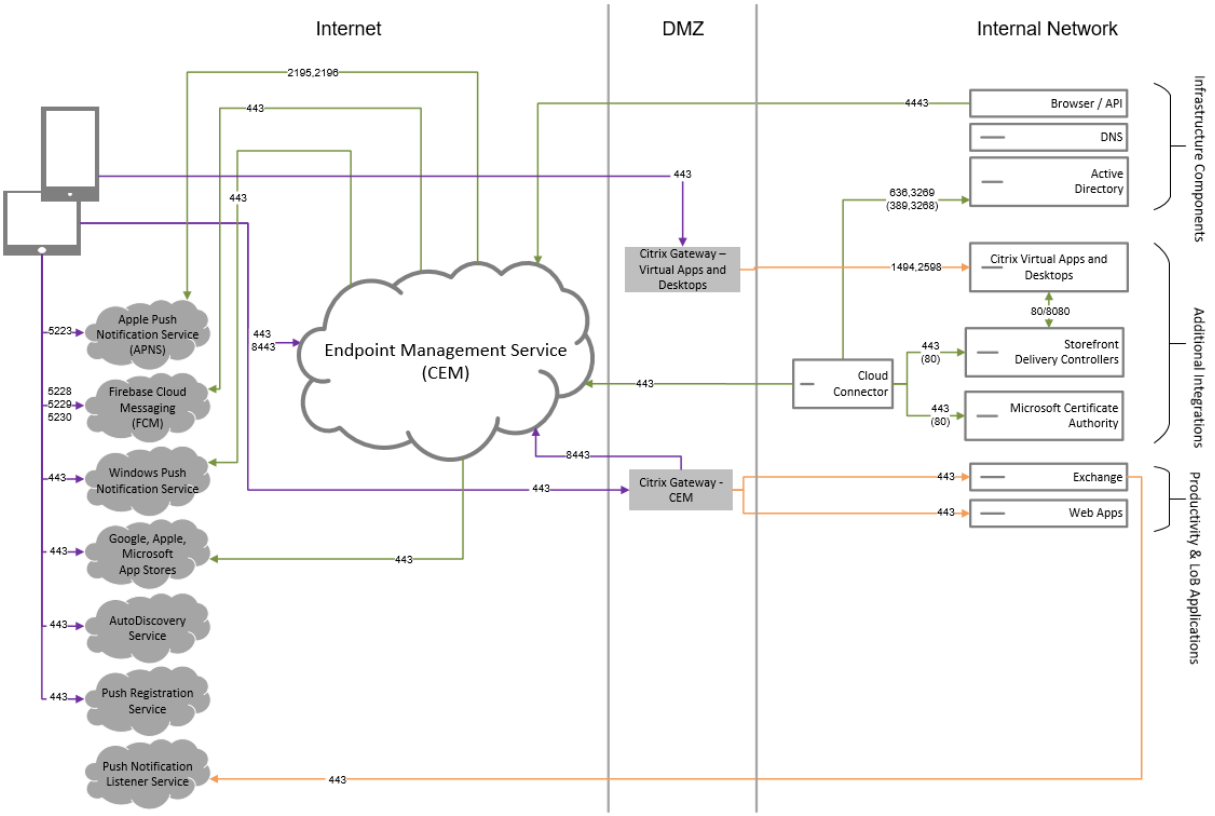
有关端口要求的详细信息，请参阅系统要求。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

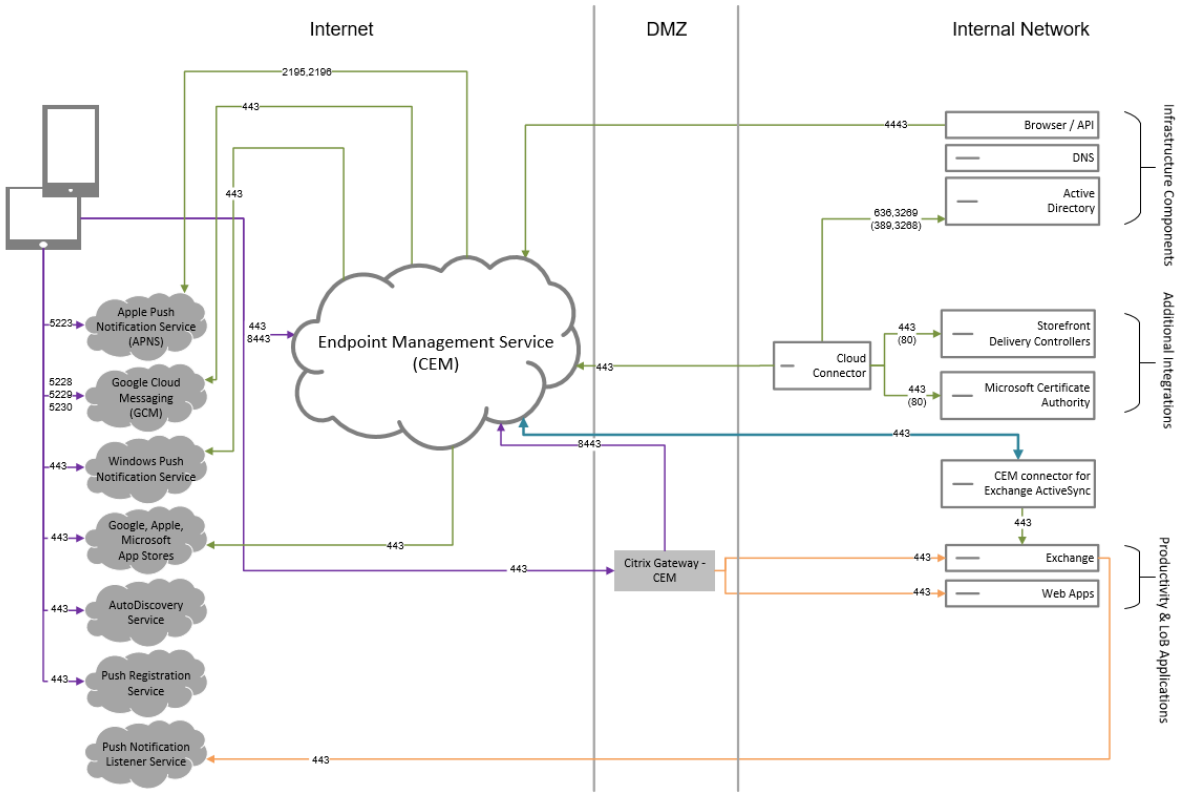


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

面向 **Citrix Virtual Apps and Desktops** 的参考体系结构

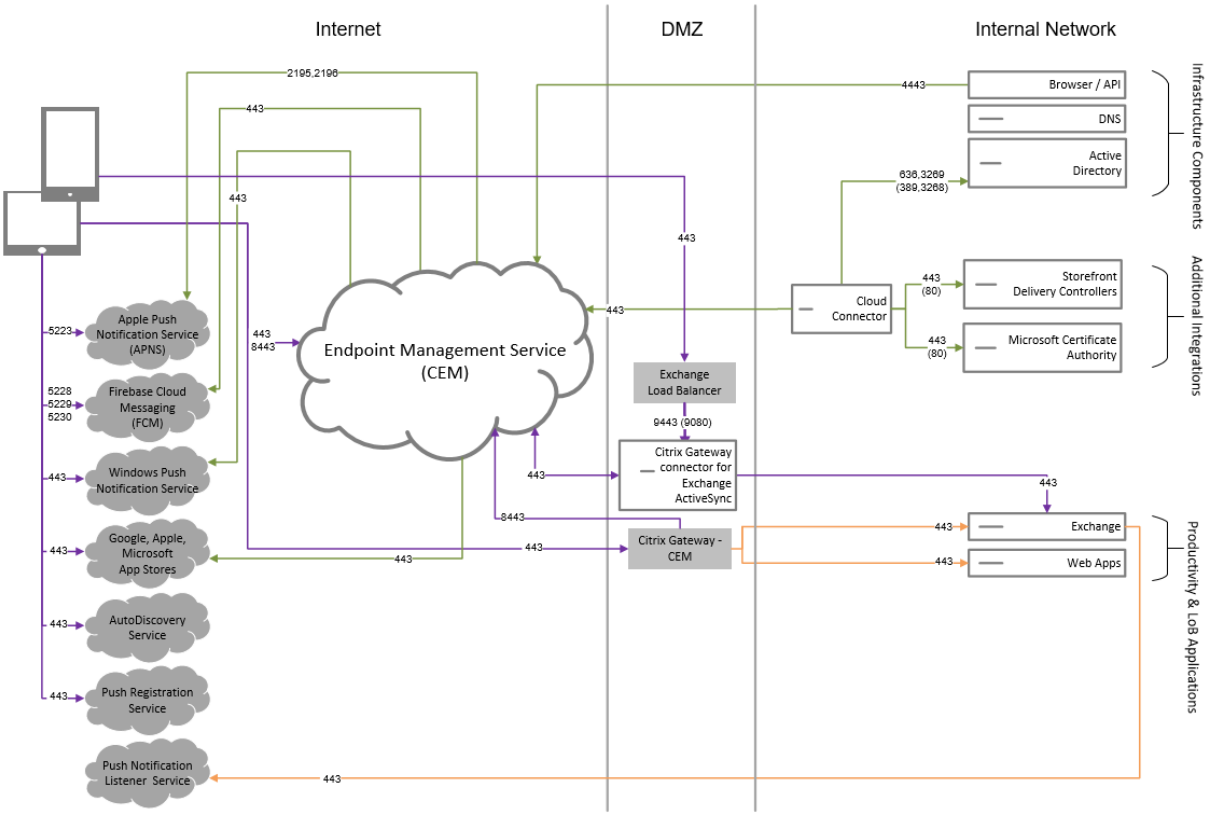

Internet
DMZ
Internal Network
2195,2196
443
443
443
443
443
443
8443
8443
443
443
443
443
443

面向适用于 **Exchange ActiveSync** 的 **Endpoint Management** 连接器的参考体系结构



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

面向适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的参考体系结构


Internet
DMZ
Internal Network
2195,2196
443
443
443

资源位置

请将资源位置放置在最能满足您的业务需求的位置。例如，公有云、分支机构、私有云或数据中心中。决定位置选择的因素包括：

- 与订阅者的临近程度
- 与数据的临近程度
- 规模要求
- 安全属性

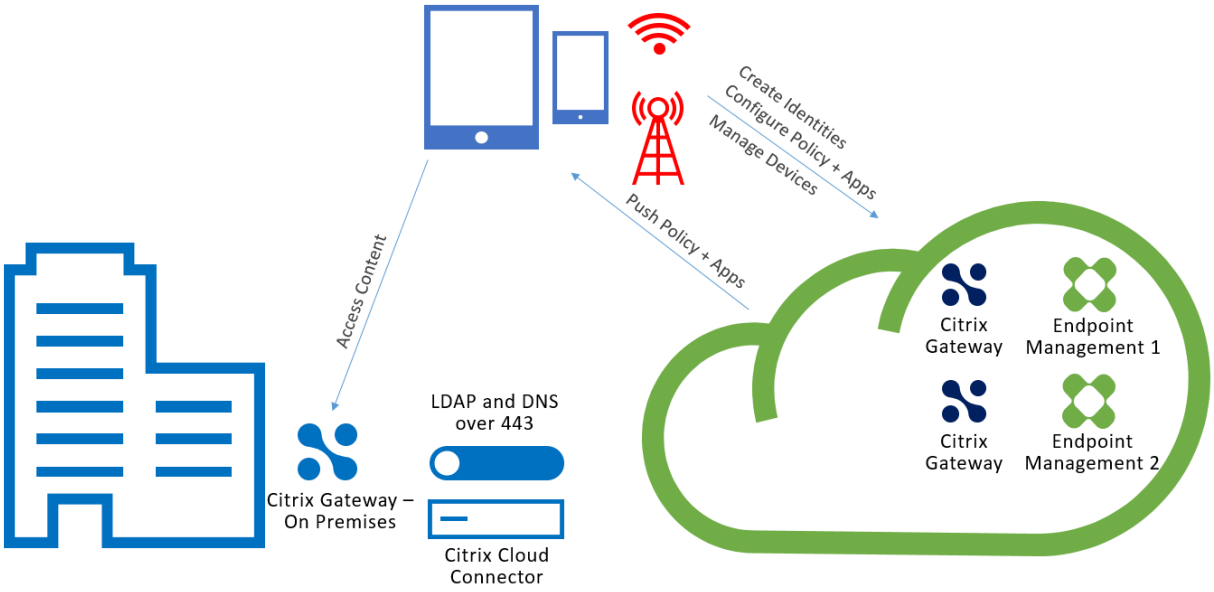
可以构建任意数量的资源位置。例如，您可以：

- 在您的数据中心中根据需要靠近数据的订阅者和应用程序为总部构建一个资源位置。
- 在公有云中为您的全局用户添加一个单独的资源位置。或者，在分支机构构建单独的资源位置，以提供能够提供最佳服务的靠近分支机构工作人员的应用程序。
- 在单独的网络中添加另一个提供受限制的应用程序的资源位置。此设置将提供对其他资源和订阅者的受限可见性，而不需要调整其他资源位置。

Cloud Connector

Cloud Connector 进行身份验证并加密 Citrix Cloud 与您的资源位置之间的所有通信。需要 Cloud Connector 才能访问以下服务：LDAP、IdP、PKI 服务器、内部 DNS 查询、Citrix Virtual Apps、Citrix Gateway、Citrix Workspace 和 Microsoft Endpoint Manager。

下图显示了 Cloud Connector 的流量图。



Cloud Connector 建立与 Citrix Cloud 的连接。Cloud Connector 不接受传入连接。

Cloud Connector 仅在设备注册期间低于负载。有关详细信息，请参阅 Cloud Connector 的扩展和大小注意事项。

包括移动应用程序管理 (MAM) 的解决方案需要本地 Citrix Gateway 提供的 Micro VPN。在此情景中：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 以下组件驻留在您的数据中心中：
  - Cloud Connector
  - Citrix Gateway
  - 适用于 Exchange、Web 应用程序、Active Directory 和 PKI 的服务器
- 移动设备与 Endpoint Management 和您的本地 Citrix Gateway 进行通信。

Endpoint Management 组件

Endpoint Management 控制台。可以使用 Endpoint Management 管理员控制台来配置 Endpoint Management。有关使用 Endpoint Management 控制台的详细信息，请参阅 Endpoint Management 下的文章。Citrix 会在更新了新版本的 Endpoint Management 的新增功能文章时向您发出通知。

请注意 Endpoint Management 服务与本地版本之间的以下差异：

- 远程支持客户端不可用于 Endpoint Management。
- Citrix 不支持在 Endpoint Management 中将 syslog 与本地 syslog 服务器相集成。相反，可以在 Endpoint Management 控制台中从故障排除和支持页面下载这些日志。执行此操作时，必须单击全部下载。

MAM SDK。MDX Toolkit 计划于 2023 年 7 月达到生命周期已结束状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

- 移动应用程序管理 (MAM) SDK 提供了 iOS 和 Android 平台不涵盖的 MDX 功能。可以启用 MDX 并保护 iOS 或 Android 应用程序。您可以在内部应用商店或公共应用商店中提供这些应用程序。请参阅 MDX 应用程序 SDK。

移动生产力应用程序。Citrix 开发的移动生产力应用程序提供了一套在 Endpoint Management 环境中使用的生产率和通信工具。贵公司的政策保护这些应用程序的安全。有关详细信息，请参阅移动生产力应用程序。

适用于 **Exchange ActiveSync** 的 **Endpoint Management** 连接器。适用于 Exchange ActiveSync 的 Endpoint Management 连接器为使用本机移动电子邮件应用程序的用户提供了安全的电子邮件访问权限。适用于 Exchange ActiveSync 的连接器在 Exchange 服务级别提供 ActiveSync 过滤功能。因此，过滤仅在邮件抵达 Exchange 服务时发生，而不是在其进入 Endpoint Management 环境时发生。连接器不需要使用 Citrix Gateway。可以部署连接器而不更改现有 ActiveSync 流量的路由。有关详细信息，请参阅适用于 Exchange ActiveSync 的 Endpoint Management 连接器。

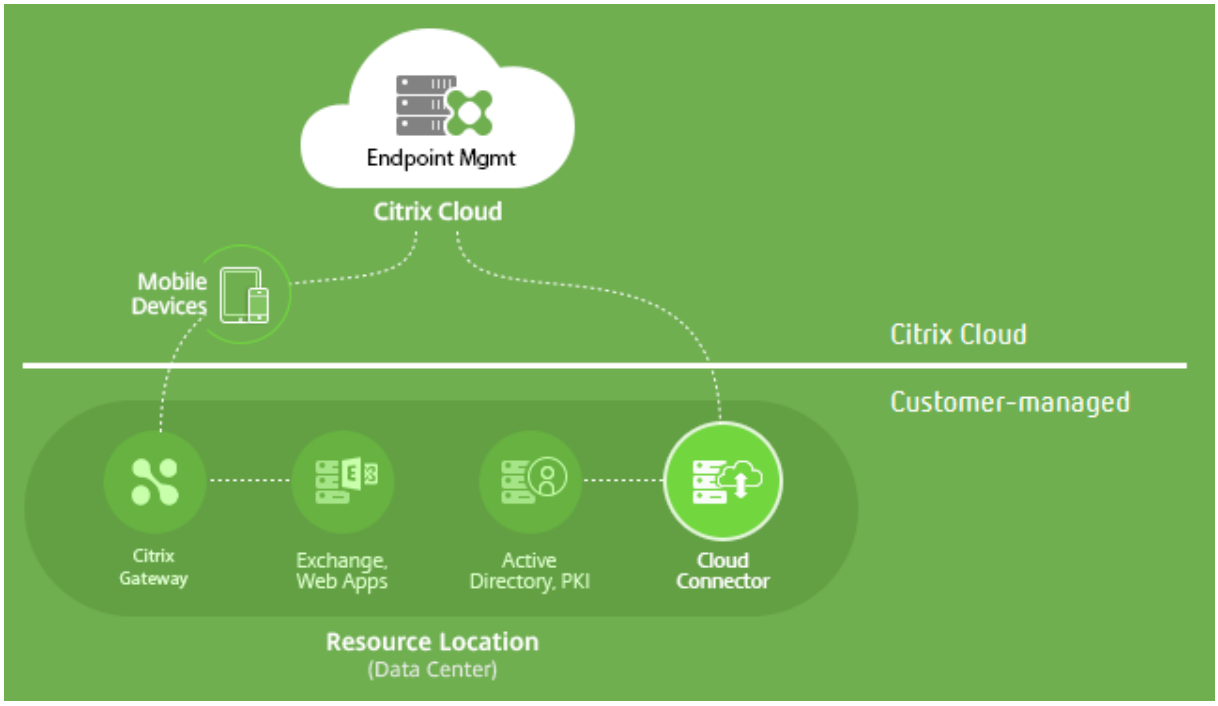
适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器。适用于 Exchange ActiveSync 的 Citrix Gateway 连接器为使用本机移动电子邮件应用程序的用户提供了安全的电子邮件访问权限。适用于 Exchange ActiveSync 的连接器在外围提供 ActiveSync 过滤功能。过滤功能使用 Citrix Gateway 作为 ActiveSync 流量的代理。因此，过滤组件位于邮件通信流的路径中，在邮件进入或离开环境时截获邮件。适用于 Exchange ActiveSync 的连接器将用作 Citrix Gateway 与 Endpoint Management 之间的中介。有关详细信息，请参阅适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 技术安全性概述

Citrix Cloud 管理 Endpoint Management 环境的控制平面。控制平面包括 Endpoint Management 服务器、Citrix ADC 负载平衡器和单租户数据库。云服务使用 Citrix Cloud Connector 与客户数据中心相集成。使用 Cloud Connector 的 Endpoint Management 客户通常在其数据中心中管理 Citrix Gateway。

下图说明了服务及其安全边界。



本部分包含以下信息：

- 提供 Citrix Cloud 的安全功能的简介。
- 定义在确保 Citrix Cloud 部署安全方面 Citrix 与客户之间的职责划分。
- 不是 Citrix Cloud 或其任何组件或服务的配置或管理指南。

有关 Endpoint Management 用于提供全面的端到端安全性的技术的信息，请参阅移动企业的安全性和生产力。

数据流

控制平面对用户和组对象具有有限的读取访问权限。这些对象驻留在您的目录、DNS 以及类似的服务中。控制平面通过安全 HTTPS 连接借助 Citrix Cloud Connector 访问这些服务。

公司数据（例如电子邮件、Intranet 和 Web 应用程序流量）通过 Citrix Gateway 直接在设备与应用程序服务器之间流动。Citrix Gateway 在客户数据中心中部署。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

数据隔离

控制平面存储管理用户设备及其移动应用程序所需的元数据。服务本身包含多租户组件和单租户组件的混合。但是，根据服务体系结构，客户元数据将始终为每个租户单独存储，并使用唯一的凭据来确保安全。

凭据处理

此服务处理以下四种类型的凭据：

- 用户凭据：用户凭据通过 HTTPS 连接从设备传输到控制平面。控制平面通过安全连接在客户目录中的某个目录中验证这些凭据。
- 管理员凭据：管理员针对 Citrix Cloud 进行身份验证，而 Citrix Cloud 使用 Citrix Online 开发的登录系统。此过程将生成一个一次性签名的 JSON Web 令牌 (JWT)，管理员通过该令牌访问服务。
- **Active Directory** 凭据：控制平面需要绑定凭据才能从 Active Directory 中读取用户元数据。这些凭据使用 AES-256 加密方法进行加密，并保存在每租户数据库中。

部署注意事项

Citrix 建议您查阅已发布的最佳做法文档，了解在您的环境中部署 Citrix Gateway 的相关信息。

更多资源

建议客户查看与其 Citrix 产品相关的安全公告。有关新的和更新的安全公告的信息，请参阅 Citrix 安全公告。另外，请考虑在警报设置下注册以接收警报。

有关更多安全信息，请参阅以下资源：

- Citrix 安全站点：https://www.citrix.com/security
- Citrix Cloud 文档：适用于 Citrix Cloud 平台的安全部署指南
- Citrix ADC 的安全部署指南

与 **Mobile Threat Defense** 软件集成

移动威胁防护 (MTD) 软件可检测、分析和帮助防止针对企业移动设备的高级网络攻击。MTD 和 Unified Endpoint Management (UEM) 的组合提高了组织的安全性和可见性。

MTD 软件提供 Endpoint Management 用于执行以下操作的威胁数据：

- 防止恶意软件、网络钓鱼、网络攻击和中间人攻击
- 确定设备合规性状态
- 确定风险水平
- 采取基于策略的操作来保护您的应用程序、数据、设备和移动网络

Citrix Endpoint Management 与以下 MTD 供应商集成：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Check Point
- 注意
- Wandera
- Zimperium

有关更多信息或请求演示，请联系我们的 MTD 合作伙伴或 Citrix 销售代表。

Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成

October 18, 2022

Endpoint Management 与 Microsoft Endpoint Manager (MEM) 的集成为 Microsoft Intune 感知应用程序（例如 Microsoft Edge 浏览器）增加了端点管理 Micro VPN 的价值。

要激活集成，请联系 Citrix Cloud Operations 团队。

此版本支持以下用例：

- Intune MAM 以及 Endpoint Management MDM+MAM。

  本文重点介绍了 Intune MAM + Endpoint Management MDM+MAM 用例。将 Citrix 添加为 MDM 提供程序后，请配置 Intune 托管应用程序以传送到设备。

  > 重要：
  >
  > 对于此用例，Secure Mail 不支持与 Intune 的集成。Secure Mail 仅适用于在 MDX 模式下注册的设备。

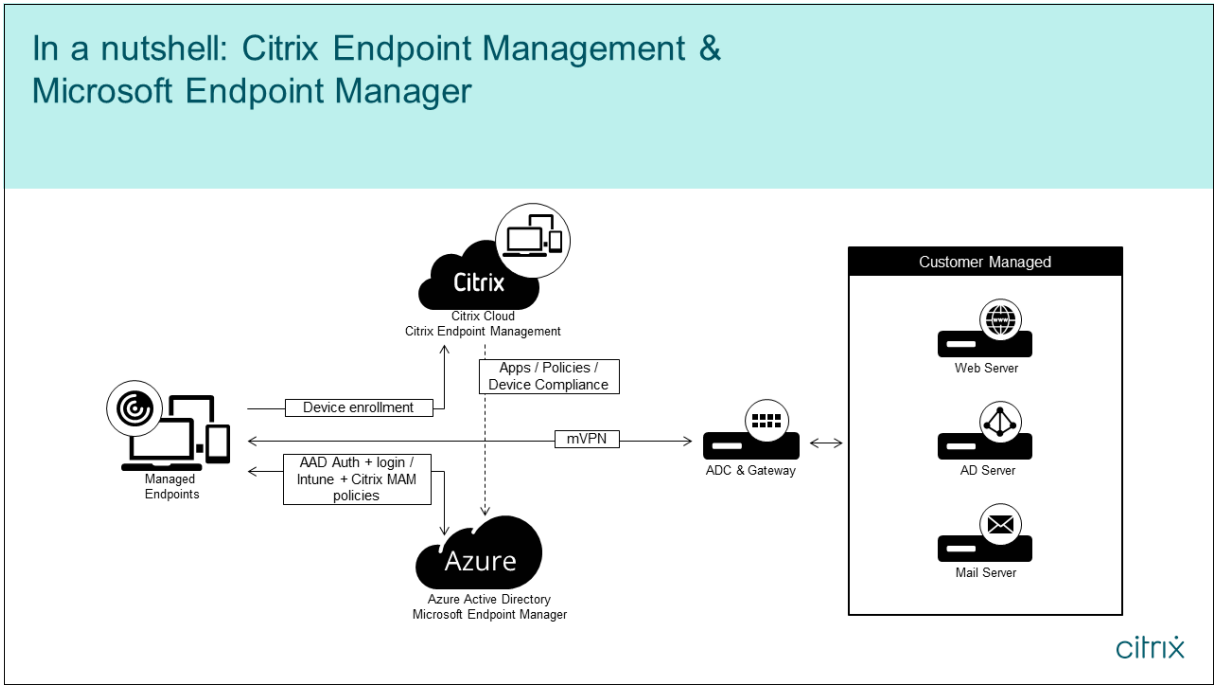
- Intune MAM 和 Endpoint Management MDM。
- Intune MAM。
- Intune MAM 和 Intune MDM。Secure Mail for iOS 支持在此用例中使用单点登录。

有关设置 Endpoint Management 与 MEM 的集成的简单易懂的图形指南，请参阅入门指南。

有关与 Azure AD 条件访问的集成有关的信息，请参阅与 Azure AD 条件访问集成。

下图概述 Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成的概述。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



系统要求

启用 **MDX**

- MAM SDK

  或

- MDX Toolkit

Microsoft

- Azure Active Directory (AD) 访问权限（具有租户管理权限）
- 启用了 Intune 的租户

防火墙规则

- 启用防火墙规则以允许 DNS 和 SSL 流量从 Citrix Gateway 子网 IP 传输到 `*.manage.microsoft.com`、`https://login.microsoftonline.com` 和 `https://graph.windows.net`（端口 53 和 443）

必备条件

- **Microsoft Edge** 浏览器：移动应用程序 SDK 集成在适用于 iOS 和 Android 的 Microsoft Edge 浏览器应用程序中。有关 Microsoft Edge 的详细信息，请参阅 Microsoft Edge 文档。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Citrix Cloud** 帐户：要注册 Citrix 帐户并申请试用 Citrix Endpoint Management，请与您的 Citrix 销售代表联系。准备好继续操作时，请转至 https://onboarding.cloud.com。有关申请 Citrix Cloud 帐户的详细信息，请参阅注册注册 Citrix Cloud。

  > 注意：
  >
  > 您提供的电子邮件必须是与 Azure AD 无关联的地址。可以使用任何免费的电子邮件服务。

- 适用于 **iOS** 的 **APNs** 证书：确保您配置了适用于 iOS 的 APNs 证书。要了解有关设置这些证书的详细信息，请参阅此 Citrix 博客文章：创建和导入 APNs 证书。
- **Azure AD** 同步：在 Azure AD 与本地 Active Directory 之间设置同步。请勿在域控制器计算机上安装 AD 同步工具。有关设置此同步的详细信息，请参阅 Azure Active Directory 上的 Microsoft 文档。

配置 **Citrix Gateway**

如果您要设置新的 Endpoint Management 部署，请安装以下 Citrix Gateway 设备之一：

- NetScaler Gateway VPX 3000 系列或更高版本
- NetScaler Gateway MPX 或专用 SDX 实例

要将 Citrix Gateway 与 MEM 集成的 Endpoint Management 结合使用，请执行以下操作：

- 使用管理接口和子网 IP 配置 Citrix Gateway。
- 对所有客户端到服务器的通信使用 TLS 1.2。有关为 Citrix Gateway 配置 TLS 1.2 的信息，请参阅 CTX247095。

如果您使用 Endpoint Management 与 MEM 集成以及 Endpoint Management MDM+MAM 部署，请配置两个 Citrix 网关。MDX 应用程序流量通过一个 Citrix Gateway 路由。Intune 应用程序流量通过其他 Citrix Gateway 路由。配置：

- 两个公用 IP。
- 或者，一个网络地址转换的 IP。
- 两个 DNS 名称。示例：`https://mam.company.com`。
- 两个公用 SSL 证书。配置与保留的公用 DNS 名称匹配的证书或使用通配符证书。
- 具有内部不可路由 RFC 1918 IP 地址的 MAM 负载平衡器。
- LDAP Active Directory 服务帐户。

同意委派权限提示

对于需要用户进行身份验证的托管应用程序，这些应用程序请求 Microsoft Graph 公开的应用程序权限。一旦同意这些权限提示，应用程序可以访问所需的资源和 API。某些应用程序需要得到 Microsoft Azure AD 的全球管理员的同意。对于这些委派权限，全局管理员必须向 Citrix Cloud 授予请求令牌的权限。然后，令牌将启用以下权限。有关更多详细信息，请参阅 Microsoft Graph 权限参考。

- 登录和读取用户配置文件：此权限允许用户登录并连接到 Azure AD。Citrix 无法查看用户凭据。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 读取所有用户的基本配置文件：该应用程序读取组织中用户的配置文件属性。属性包括组织中用户的显示名称、名字和姓氏以及电子邮件地址和照片。
- 读取所有组：此权限允许为应用程序和策略分配指定 Azure AD 组。
- 以已登录用户身份访问目录：此权限验证 Intune 订阅并启用 Citrix Gateway 和 VPN 配置。
- 读写 **Microsoft Intune** 应用程序：该应用程序可以读取和写入以下内容：
  - Microsoft 托管的属性
  - 组分配和应用程序的状态
  - 应用程序配置
  - 应用程序保护策略

此外，在 Citrix Gateway 配置期间，Azure AD 全局管理员必须：

- 批准为 Micro VPN 选择的 Active Directory。全局管理员还必须生成 Citrix Gateway 用于与 Azure AD 和 Intune 通信的客户端密钥。
- 没有 Citrix 管理员的角色。相反，Citrix 管理员将 Azure AD 帐户分配给具有适当 Intune 应用程序管理员权限的用户。然后，Intune 管理员担任 Citrix Cloud 管理员的角色，以从 Citrix Cloud 内部管理 Intune。

> 注意：
>
> Citrix 仅在安装过程中使用 Intune 全局管理员密码，并将身份验证重定向到 Microsoft。Citrix 无法访问密码。

配置 **Endpoint Management** 与 **MEM** 的集成

1. 登录到 Citrix Cloud 站点并申请 Endpoint Management 的试用版。
2. 销售工程师安排与您的入门会议。让他们知道您希望将 Endpoint Management 与 MEM 相集成。批准您的请求后，单击管理。
3. 在该站点，您可以单击站点右上角的齿轮，也可以单击配置站点。
4. 按照第一步中的链接进入身份识别和访问管理页面。
5. 单击连接以连接您的 Azure AD 安装。
6. 输入 Azure AD 管理员用于登录的唯一登录 URL，然后单击确认。
7. 添加 Azure AD 全局管理员帐户，然后接受权限申请。
8. 确认 Azure AD 实例已成功连接。要指示连接成功，未连接文本将更改为已启用。
9. 单击管理员选项卡，然后将您的 Azure AD Intune 管理员添加为 Citrix Cloud 管理员。从下拉菜单中选择“Azure AD”或“Citrix 身份”，然后搜索要添加的用户名。单击邀请，然后在单击发送邀请之前授予用户完全访问权限或自定义访问权限。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> Endpoint Management 需要针对自定义访问权限的以下规则：库和 Citrix Endpoint Management。

因此，Azure AD Intune 管理员会收到一封电子邮件邀请，以创建密码并登录到 Citrix Cloud。在管理员登录之前，请确保您注销了所有其他帐户。

Azure AD Intune 管理员必须遵循此过程中的其余步骤。

10. 使用新帐户登录后，在 **Endpoint Management** 下单击管理。如果您已正确配置所有内容，页面将显示 Azure AD 管理员已登录，并且您的 Intune 订阅有效。

为 **Micro VPN** 配置 **Citrix Gateway**

要将 Micro VPN 与 Intune 结合使用，必须将 Citrix Gateway 配置为对 Azure AD 进行身份验证。现有 Citrix Gateway 虚拟服务器不适用于此用例。

首先，将 Azure AD 配置为与本地 Active Directory 同步。此步骤是确保 Intune 和 Citrix Gateway 之间正确进行身份验证所必需的。

1. 在 Citrix Cloud 控制台的 **Endpoint Management** 下，单击管理。
2. 在 **Micro VPN** 旁边，单击配置 **Micro VPN**。
3. 输入 Micro VPN 服务的名称和 Citrix Gateway 的外部 URL，然后单击下一步。

   此脚本将 Citrix Gateway 配置为支持 Azure AD 和 Intune 应用程序。
4. 点击下载脚本。.zip 文件包括一个自述文件，其中包含实施脚本的说明。尽管您可以从此处保存并退出，但只有在 Citrix Gateway 安装中运行脚本后，Micro VPN 才会设置。

   > 注意：
   >
   > 完成 Citrix Gateway 配置过程后，如果看到“完成”以外的 OAuth 状态，请参阅“故障排除”部分。

配置设备管理

如果要管理除应用程序以外的设备，请选择一种设备管理方法。可以使用 Endpoint Management MDM+MAM 或 Intune MDM。

> 注意：
>
> 控制台默认为 Intune MDM。要使用 Intune 作为 MDM 提供程序，请参阅 Microsoft Intune 文档。

1. 在 Citrix Cloud 控制台的“Endpoint Management 与 MEM 的集成”下，单击管理。在设备管理 **-** 可选旁边，单击配置 **MDM**。
2. 输入唯一的站点名称，选择离您最近的云区域，然后单击“请求站点”。当您的网站准备就绪时，您会收到一封电子邮件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 单击确定关闭提示。选择要与您的站点关联的 Active Directory 位置或创建一个资源位置，然后单击下一步。
4. 单击下载 **Cloud Connector**，然后按照屏幕上的说明安装 Cloud Connector。安装后，单击测试连接以验证 Citrix Cloud 与 Cloud Connector 之间的连接。
5. 单击保存并退出以完成。此时将显示您的资源位置。单击完成将返回到设置屏幕。
6. 现在，您可以从站点磁贴访问 Endpoint Management 控制台。在这里，您可以执行 MDM 管理任务和分配设备策略。有关设备策略的详细信息，请参阅设备策略。

配置 **Intune** 托管应用程序以交付到设备

要配置 Intune 托管应用程序进行交付，请执行以下操作：

- 将应用程序添加到 Citrix Cloud 库
- 创建 Endpoint Management 设备策略以控制数据流
- 为应用程序和策略创建交付组

将 **Microsoft Intune** 应用程序添加到 **Citrix Cloud** 库

对于要添加的每个应用程序：

1. 在 Citrix Cloud 控制台中，单击菜单图标，然后单击 **Library**（库）。
2. 单击右上角的加号图标，然后单击 **Add a Mobile app**（添加移动应用程序）。
3. 如果您尚未在 Endpoint Management 控制台中配置 Android Enterprise，请在选择应用程序下选择 **Microsoft Intune Apps**（Microsoft Intune 应用程序）。选择要自定义的应用程序模板，或者单击 **Upload my own App**（上载我自己的应用程序）。

   Citrix 提供现有应用程序模板，每个模板都附带一组预配置的默认策略。对于客户上载的应用程序，以下策略适用：

   - **MDX** 文件：包括启用了 MAM SDK 的应用程序或 MDX 封装的应用程序，例如：
     - Intune 应用程序保护策略和软件包中的默认 MDX 策略
     - 公共应用商店应用程序，例如 Intune 应用程序保护策略和与捆绑包 ID 匹配的默认 MDX 策略
   - **IPA** 文件： Intune 应用程序保护策略。
   - **APK** 文件： Intune 应用程序保护策略。

   > 注意：
   >
   > 如果应用程序未使用 Intune 打包，则 Intune 应用程序保护策略不适用。

4. 单击 **Upload my own App**（上载我自己的应用程序）后，上载您的.mdx 或 Intune 封装的文件。
5. 输入应用程序的名称和说明，选择应用程序是可选应用程序还是必需应用程序，然后单击 **Next**（下一步）。
6. 配置应用程序设置。以下配置使 Endpoint Management 和 Intune 容器能够相互传输数据。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Allow apps to receive data from other apps**（允许应用程序接收来自其他应用程序的数据）：选择 **Policy managed apps**（策略托管的应用程序）。
- **Allow app to transfer data to other apps**（允许应用程序将数据传输到其他应用程序）：选择 **All apps**（所有应用程序）。
- **Restrict cut, copy, paste with other apps**（限制与其他应用程序的剪切、复制、粘贴操作）：选择 **Policy managed apps**（策略托管的应用程序）。

7. 为保存的数据配置存储库。在 **Select which storage services corporate data can be saved to**（选择可以将哪些存储服务企业数据保存到）中，选择 **LocalStorage**（本地存储）。
8. 可选：为应用程序设置数据重定位、访问权限和 PIN 策略。单击下一步。
9. 查看应用程序的摘要，然后单击完成。

   此应用程序配置过程可能需要几分钟时间。过程完成后，将显示一条消息，指示应用程序已发布到库。
10. 要将用户组分配给应用程序，请单击分配用户。
11. 在搜索框中，搜索用户组，然后单击以进行添加。无法添加单个用户。
12. 添加所需的所有组后，请通过单击 X 来关闭窗口。

    添加用户组时可能会看到一条错误。当用户组尚未同步到本地 Active Directory 时会出现此错误。

将 **Android Enterprise** 应用程序添加到 **Citrix Cloud** 库

要将 Android Enterprise 应用程序添加到 Citrix Cloud Library 并设置 Intune 应用程序保护策略，请使用以下内容配置您的云环境：

- 将 Citrix Cloud 与 Azure Active Directory (AAD) 帐户联合。请参阅将 Azure Active Directory 连接到 Citrix Cloud。
- 在 Endpoint Management 中配置 LDAP 和 Cloud Connector。
- 在 Endpoint Management 中设置 Android Enterprise。确保 Android Enterprise 设备在 MDM+MAM 中注册。要设置 Android Enterprise，请参阅 Android Enterprise。

以下过程将 Android Enterprise 应用程序同时添加到 Endpoint Management 控制台和 Intune 控制台。对于要添加的每个 Android Enterprise 应用程序：

1. 在 Citrix Cloud 控制台中，单击菜单图标，然后单击 **Library**（库）。
2. 单击右上角的加号图标，然后单击 **Add a Mobile app**（添加移动应用程序）。
3. 在选择应用程序下，选择 **Android Enterprise Apps**（Android Enterprise 应用程序）。
4. 在“Managed Google Play store”（托管 Google Play 应用商店）窗口中搜索应用程序并进行审批。关闭 Google 窗口后，单击下一步。
5. 添加应用程序详细信息，然后单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. 如果搜索并选择了一个 Citrix 移动生产力应用程序，则可以配置 Micro VPN 策略。配置这些策略后，单击下一步。
7. 配置 Intune 应用程序保护策略。单击下一步。
8. 配置应用程序设置。以下配置使 Endpoint Management 和 Intune 容器能够相互传输数据。
   - **Allow apps to receive data from other apps**（允许应用程序接收来自其他应用程序的数据）：选择 **Policy managed apps**（策略托管的应用程序）。
   - **Allow app to transfer data to other apps**（允许应用程序将数据传输到其他应用程序）：选择 **All apps**（所有应用程序）。
   - **Restrict cut, copy, paste with other apps**（限制与其他应用程序的剪切、复制、粘贴操作）：选择 **Policy managed apps**（策略托管的应用程序）。
9. 为保存的数据配置存储库。在 **Select which storage services corporate data can be saved to**（选择可以将哪些存储服务企业数据保存到）中，选择 **LocalStorage**（本地存储）。
10. 可选：为应用程序设置数据重定位、访问权限和 PIN 策略。单击下一步。
11. 查看应用程序的摘要，然后单击完成。

    此应用程序配置过程可能需要几分钟时间。过程完成后，将显示一条消息，指示应用程序已发布到库。该应用程序在 Endpoint Management 和 Intune 控制台中可用。在 Endpoint Management 控制台中，该应用程序属于新交付组的一部分，并标识为公共应用商店应用程序。
12. 要将用户组分配给应用程序，请单击分配用户。
13. 在搜索框中，搜索用户组，然后单击以进行添加。无法添加单个用户。
14. 添加所需的所有组后，请通过单击 X 来关闭窗口。

    添加用户组时可能会看到一条错误。当用户组尚未同步到本地 Active Directory 时会出现此错误。

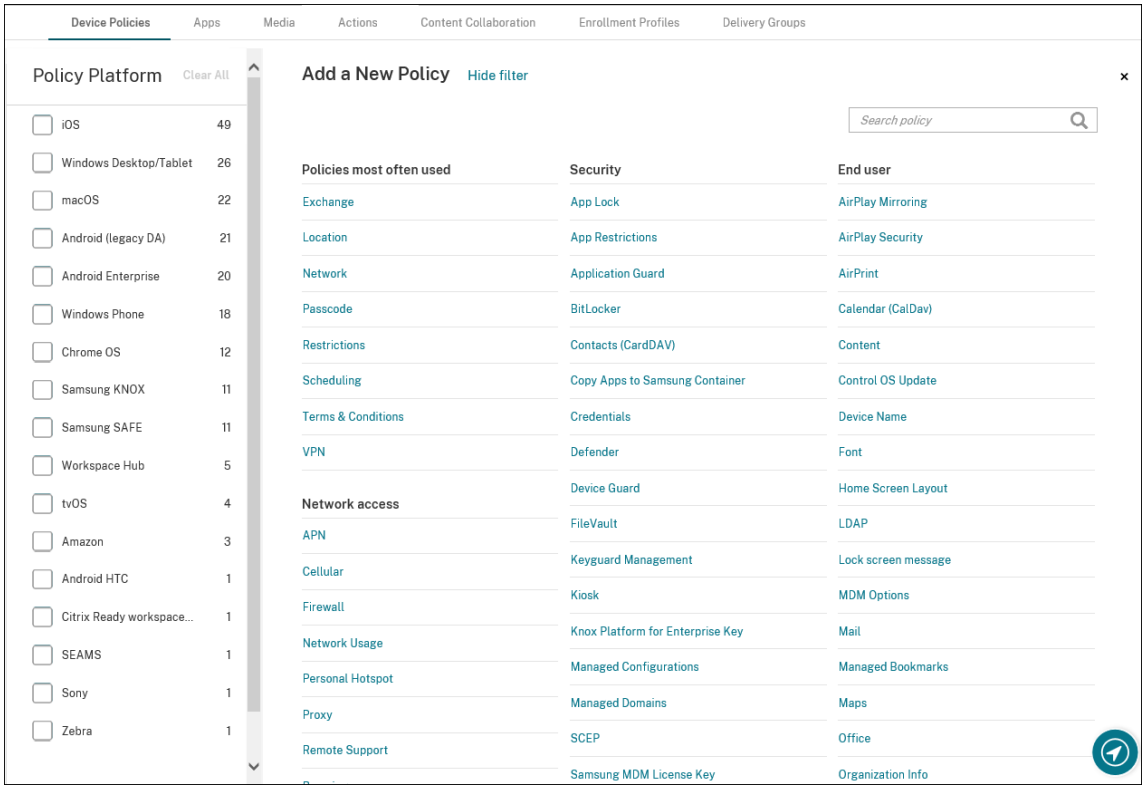
控制在托管应用程序之间传输的数据类型

控制可以使用 Endpoint Management 设备策略在 Endpoint Management 中的托管应用程序或 Intune 容器之间传输的数据类型。可以将“限制”策略配置为仅允许标记为“企业”的数据。配置“应用程序配置”策略以标记数据。

要配置“限制”设备策略，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击配置 **>** 设备策略。
2. 在设备策略页面上，单击添加。将显示添加新策略页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 单击策略列表中的限制。
4. 在策略信息页面上，键入策略的名称和说明（可选）。单击下一步。
5. 要为 iOS 应用程序创建设备策略，请在平台窗格中选择 **iOS**。
6. 在安全性 **-** 允许下，将在非托管应用程序中使用托管应用程序中的文档设置为关。将此设置设为关还会将非托管应用程序读取托管联系人和托管应用程序写入非托管联系人设置为关。单击下一步。
7. 单击下一步，直到出现保存按钮。单击保存。

为每个应用程序配置“应用程序配置”设备策略：

1. 在 Endpoint Management 控制台中，单击配置 **>** 设备策略。
2. 单击添加。将显示添加新策略页面。
3. 在策略列表中单击应用程序配置。
4. 在策略信息页面上，键入策略的名称和说明（可选）。单击下一步。
5. 要为 iOS 应用程序创建设备策略，请在平台窗格中选择 **iOS**。
6. 选择要配置的应用程序的标识符。
7. 对于 iOS 应用程序，请将以下文本添加到字典内容中：

```
1 <dict>
2     <key>IntuneMAMUPN</key>
```

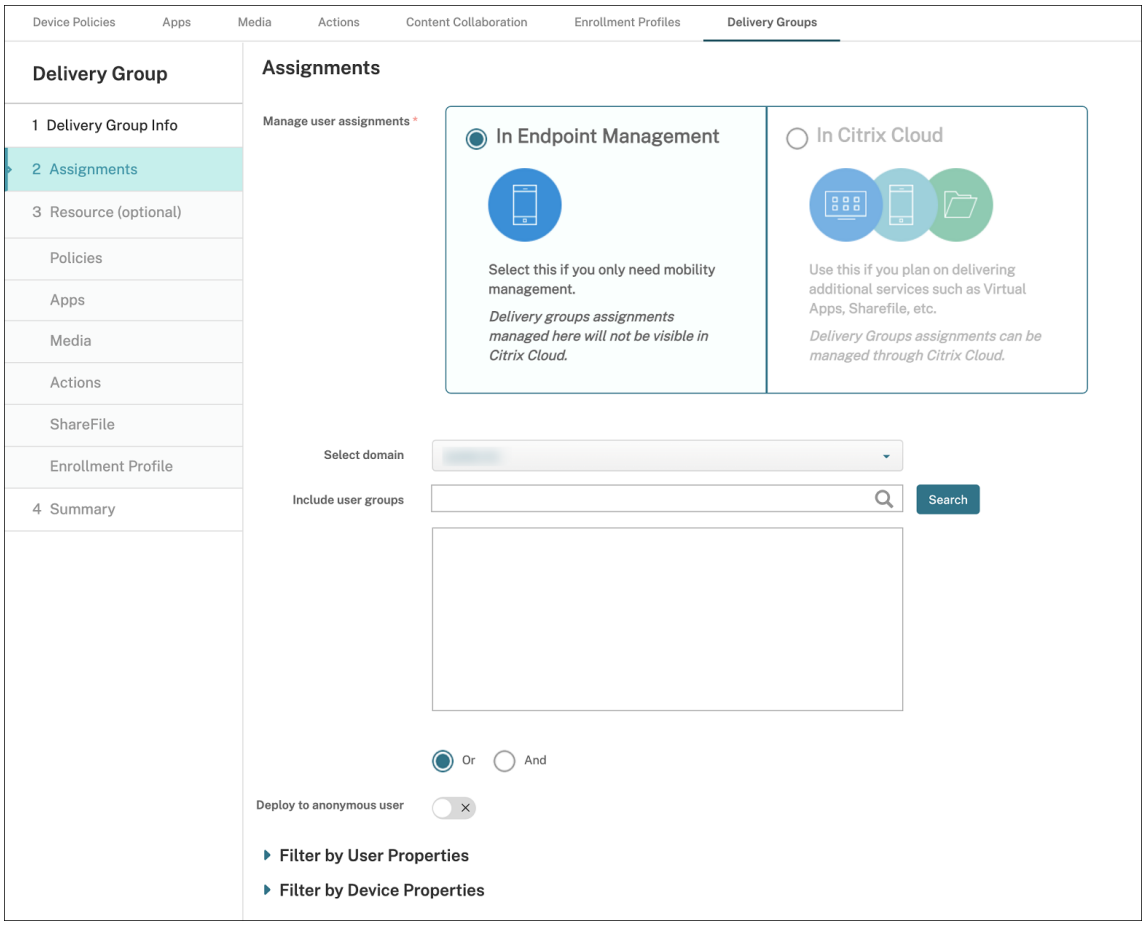
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
    <string>${
 user.userprincipalname }
 </string>
</dict>
<!--NeedCopy-->
```

8. 单击检查字典。
9. 单击下一步。
10. 单击保存。

为应用程序和设备策略配置交付组

1. 在 Endpoint Management 控制台中，单击配置 **>** 交付组。
2. 在交付组页面上，单击添加。此时将显示交付组信息页面。
3. 在交付组信息页面中，键入交付组的名称和说明（可选）。单击下一步。
4. 在分配页面上，指定部署交付组的方式：选择在 **Endpoint Management** 中或在 **Citrix Cloud** 中。



5. 如果您选择了 **Endpoint Management**：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 选择域：在列表中，选择要从中选择用户的域。
- 包括用户组：执行以下操作之一：
  - 在用户组列表中，单击要添加的组。选定的组将显示在选定用户组列表中。
  - 单击搜索以查看选定域中所有用户组的列表。
  - 在搜索框中键入完整或部分组名称，然后单击搜索以限制用户组列表。

  要从选定用户组列表中删除某个用户组，请执行以下操作之一：
  - 在选定用户组列表中，单击要删除的每个组旁边的 **X**。
  - 单击搜索以查看选定域中所有用户组的列表。滚动列表，并取消选中要删除的各个组旁边的复选框。
  - 在搜索框中键入完整或部分组名称，然后单击搜索以限制用户组列表。滚动列表，并取消选中要删除的各个组旁边的复选框。

6. 单击下一步。
7. 在策略页面中，从左到右拖动您创建的“限制”策略和“应用程序配置”策略。单击下一步。
8. 在应用程序页面中，将要提供的应用程序从页面左侧拖动到必需应用程序或可选应用程序。单击下一步。
9. （可选）配置媒体页面、操作页面和注册页面上的设置。或者接受每个页面上的默认值，然后单击下一步。
10. 在摘要页面上，查看交付组设置，然后单击保存以创建交付组。

在 Intune 控制台中发布应用程序时，选择强制管理应用程序。系统会提示使用未受监督的设备的用户允许管理此应用程序。如果用户接受该提示，应用程序将在设备上进行托管。如果用户拒绝提示，则该应用程序在设备上不可用。

配置 **Secure Mail**

Secure Mail 现在支持多种配置。可以在连接到本地 Exchange Server 的 Intune MAM 容器中封装 Secure Mail。可以将 Secure Mail 连接到托管 Exchange 或 Office 365 帐户。但是，此版本不支持基于证书的身份验证，因此改为使用 LDAP。

> 重要：
>
> 要在 MDX 模式下使用 Secure Mail，必须使用 Citrix Endpoint Management MDM+MAM。

Secure Mail 还会自动填充用户名。要启用此功能，必须先配置以下自定义策略：

1. 在 Endpoint Management 控制台中，转至设置 **>** 服务器属性，然后单击添加。
2. 在列表中，单击自定义键，然后在密钥字段中，键入 `xms.store.idpuser_attrs`。
3. 将该值设置为 **true**，然后在显示名称中键入 `xms.store.idpuser_attrs`。单击保存。
4. 单击客户端属性，然后单击添加。
5. 选择自定义密钥，然后在密钥字段中键入 **SEND_LDAP_ATTRIBUTES** 。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. `userPrincipalName=${ user.userprincipalname } ,email=${ user.mail } , displayname=${ user.displayname } ,sAMAccountName=${ user.samaccountname } ,aadupn=${ user.id_token.upn } ,aadtid=${ user.id_token.tid }` 在“值”字段中键入。输入描述，然后单击“保存”。

   以下步骤仅适用于 iOS 设备。

7. 转至配置 > 设备策略，单击“添加”，然后选择应用程序配置策略。
8. 输入策略名称，然后单击下一步。

   在“标识符”列表中，单击新增。在显示的文本框中，输入 Secure Mail 应用程序的捆绑包 ID。

9. 在字典内容框中，键入以下文本。

```
<dict>

<key>XenMobileUserAttributes</key>

<dict>

<key>userPrincipalName</key>

<string>${
 user.userprincipalname }
 </string>

<key>email</key>

<string>${
 user.mail }
 </string>

<key>displayname</key>

<string>${
 user.displayname }
 </string>

<key>sAMAccountName</key>

<string>${
 user.samaccountname }
 </string>

<key>aadupn</key>

```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
<string>${
 user.id_token.upn }
 </string>

<key>aadtid</key>

<string>${
 user.id_token.tid }
 </string>

</dict>

<key>IntuneMAMUPN</key>

<string>${
 user.id_token.upn }
 </string>

</dict>
```

10. 取消选中 **Windows Desktop/Tablet** 复选框，然后单击下一步。
11. 选择要将此策略部署到的用户组，然后单击保存。

故障排除

常规问题

问题：打开应用程序时，将显示以下错误消息：需要应用程序策略。

解决方案：在 Microsoft Graph API 中添加策略。

问题：您有策略冲突。

解决方案：仅允许为每个应用程序配置一个策略。

问题：您的应用程序无法连接到内部资源。

解决方法：确保正确的防火墙端口处于打开状态，您使用正确的租户 ID 等等。

Citrix Gateway 问题

下表列出了 Citrix Gateway 配置的常见问题及其解决方案。要进行故障排除，请启用更多日志并通过执行以下操作进行检查：

1. 在命令行界面中，运行以下命令：`set audit syslogParams -logLevel ALL`
2. 使用 `tail -f /var/log/ns.log` 从 shell 检查日志

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

问题	解决方案
为 Azure 上的网关应用程序配置所需的权限不可用。	检查是否有适当的 Intune 许可证可用。尝试使用 manage.windowsazure.com 门户来查看是否可以添加权限。如果问题仍然存在，请与 Microsoft 支持部门联系。
Citrix Gateway 无法访问 `login.microsoftonline.com` 和 `graph.windows.net`。	从 NS Shell 查看是否可以访问以下 Microsoft 网站：`curl -v -k https://login.microsoftonline.com`。然后，检查 Citrix Gateway 上是否配置了 DNS，以及防火墙设置是否正确（如果 DNS 请求有防火墙）。
配置 OAuthAction 后，ns.log 中会出现错误。	检查 Intune 许可是否已启用，以及 Azure 网关应用程序是否设置了适当的权限。
Sh OAuthAction 命令不会显示 OAuth 状态为完成。	检查 Azure Gateway 应用程序的 DNS 设置和配置权限。
Android 或 iOS 设备不显示双重身份验证提示。	检查双重设备 ID 登录架构是否绑定到身份验证虚拟服务器。

OAuth 错误情况和状态

状态	错误状况
COMPLETE	成功
AADFORGRAPH	密钥无效、URL 未解析、连接超时
MDMINFO	*manage.microsoft.com 已关闭或无法访问
GRAPH	图形端点已关闭，无法访问
CERTFETCH	由于 DNS 错误无法与令牌端点 `https://login.microsoftonline.com` 通信。要验证此配置，请转到 shell 并键入 `curl https://login.microsoftonline.com`。此命令必须验证。

限制

以下各项描述了将 MEM 与 Citrix Endpoint Management 结合使用的一些限制。

- 使用 Citrix 和 Intune 部署应用程序以支持 Micro VPN 时：当用户提供其用户名和密码以访问摘要站点时，即

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使其凭据有效，也会出现错误。[CXM-25227]

- 将拆分通道从开更改为关，并等待当前网关会话过期后：用户在完整 VPN 模式下启动内部站点之前，外部流量无需通过 Citrix Gateway 即可直接通过。[CXM-34922]
- 将“仅限 托管应用程序”的“打开”策略更改为“所有应用程序”后，用户在关闭并重新启动 Secure Mail 之前无法在非托管应用程序中打开文档。[CXM-34990]
- 在完整 VPN 模式下拆分通道设置为开，并且拆分 DNS 从本地更改为远程时，内部站点无法加载。[CXM-35168]

已知问题

禁用了 mVPN 策略启用 **http/https** 重定向 **(**使用 **SSO)** 时，Secure Mail 不起作用。[CXM-58886]

第三方已知问题

在 Secure Mail for Android 上，当用户轻按创建新事件时，不会显示新事件创建页面。[CXM-23917]

当您使用 Citrix 和 Intune 部署 Citrix Secure Mail for iOS 以支持 micro VPN 时：当用户将应用程序移至后台时，会遮盖 Secure Mail 屏幕的应用程序策略不会被强制执行。[CXM-25032]

载入和资源设置

May 8, 2023

如果您是 Citrix、Citrix Cloud 或 Endpoint Management 的新用户，本文将指导您完成入门过程。了解开始时所需的工作流程和详细信息。

- 我该从何处开始**?**
  - 如果您尚未购买 Endpoint Management 订阅，请参阅面向 Citrix 新客户。
  - 如果您有 Endpoint Management 订阅，请跳至“管理”按钮可用时。
  - 如果您已预配 Endpoint Management 站点，请跳至配置身份验证。
- 配置顺序是否重要？本文遵循推荐的配置顺序。您可以按不同的顺序工作。Endpoint Management 控制台通过“预配后设置”等消息，让您知晓是否缺少必备项。
- 载入后我该做什么？完成本文中介绍的入门和资源配置后，继续在 Endpoint Management 控制台中进行配置。有关接下来的步骤的信息，请参阅准备注册设备和交付资源。

面向 **Citrix** 新客户

对于新使用 Endpoint Management 的 Citrix Cloud 客户：

如果您已购买 Endpoint Management 订阅，请跳至“管理”按钮可用时。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

如果您尚未设置 Citrix Cloud 帐户，请参阅注册 Citrix Cloud。

如果您已设置 Citrix Cloud 帐户，但尚未购买 Endpoint Management，请申请服务演示版。

1. 使用 Citrix Cloud 管理员凭据登录到 Citrix Cloud 帐户。此时将显示 Citrix Cloud 主页。

   所有 Citrix Cloud 管理员帐户按如下所示进行创建：

   - Citrix Cloud 管理员默认为 Endpoint Management 管理员。
   - 创建的具有客户访问权限的 Citrix Cloud 管理员必须选择 Endpoint Management，才能管理 Endpoint Management。

2. 在 Citrix Cloud 主页上，找到 Endpoint Management 服务磁贴，然后单击申请演示版。
3. 填写并提交演示版申请表单。Endpoint Management 服务磁贴上的按钮更改为已申请演示版。

如果在处理申请之前单击 Endpoint Management 服务磁贴，则会显示一个屏幕，建议您与代表或合作伙伴联系。Citrix 销售代表可以提供有关服务的更多详细信息。

等待试用过程中，请务必通过检查系统要求来为您的 Endpoint Management 部署做好准备。虽然 Citrix 托管和交付您的 Endpoint Management 解决方案，但是您必须处理某些通信和端口要求。

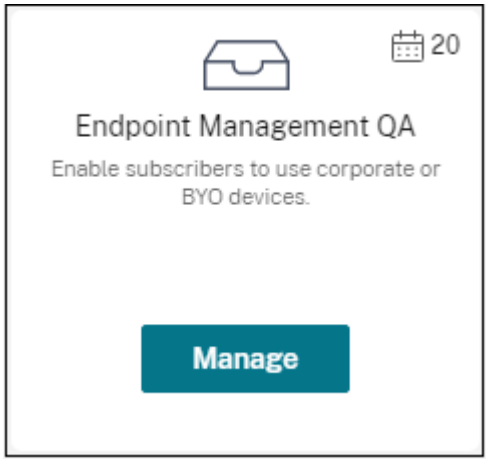
继续下一部分。

“管理”按钮可用时

此视频将指导您完成入门操作：

这是一个嵌入式视频。单击链接观看视频

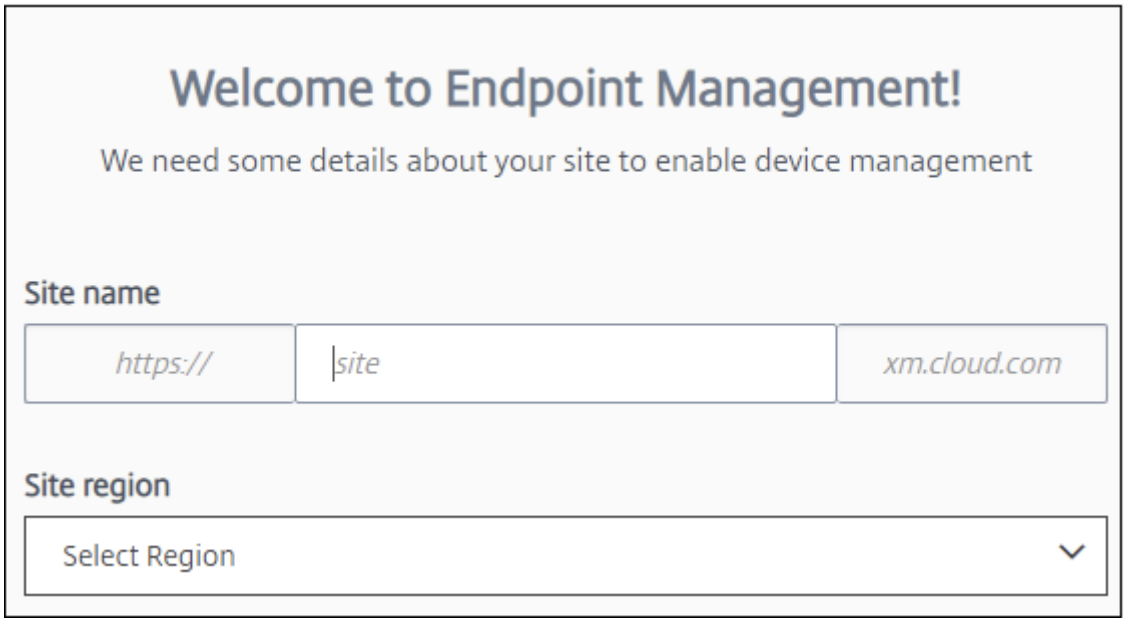
当您的 Endpoint Management 服务可用时，Endpoint Management 服务磁贴上的按钮将更改为管理。



要开始设置，请执行以下操作：

1. 使用 Citrix Cloud 管理员凭据登录您的 Citrix Cloud 帐户。
2. 单击 Endpoint Management 磁贴中的管理以访问 Endpoint Management 控制台。
3. 键入您的站点名称并选择一个区域。然后选择 **Save & Continue**（保存并继续）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



> 注意：
>
> 要请求允许使用的 IP，请联系 Citrix 支持代表。

Endpoint Management 控制台随后将打开，并显示一条消息，指出我们正在预配您的套件，并且某些 Endpoint Management 功能在预配期间处于锁定状态。

1. 在欢迎屏幕中，单击开始设置。
2. 选择要管理的端点，然后单击保存。可以随时添加或清除端点，以便在控制台中显示或隐藏这些端点。显示和隐藏端点不会影响您的配置。



在预配完成时，我们会向您发送一封电子邮件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

资源中心


单击资源中心图标可在不离开控制台的情况下观看操作方法视频。

在预配过程中

在我们预配 Endpoint Management 的同时，您可以开始配置。

配置资源位置

在为 Endpoint Management 配置轻型目录访问协议 (LDAP) 连接之前，您需要资源位置。资源位置包含向您的订阅者提供云服务所需的资源。每个域需要一个资源位置。要获取帮助，请参阅 Citrix Cloud 文章资源位置。

等待试用过程中，请务必通过检查系统要求来为您的 Endpoint Management 部署做好准备。虽然 Citrix 托管和交付您的 Endpoint Management 解决方案，但是仍需要某些通信和端口要求。该设置将 Endpoint Management 体系结构连接到企业服务，例如 Active Directory。必须提供的信息包括在 “Endpoint Management Trial Sales Engineer engagement”（Endpoint Management 试用版销售工程师参与情况）下的 Onboarding Handbook（入门手册）中。

授权您访问试用版后，**Endpoint Management** 对应的按钮将更改为 **Manage**（管理）。单击管理以打开 Citrix Endpoint Management 控制台。

配置身份验证

预配站点后，您可以继续进行配置。我们建议您设置一个云托管身份提供程序 (IdP) 或轻型目录访问协议 (LDAP) 以导入组、用户帐户和相关属性。

配置 **IdP**

Endpoint Management 支持使用身份提供程序（例如 Azure Active Directory、Okta 和本地 Citrix Gateway）进行身份验证。

在 Citrix Cloud 中配置一个 IdP 并为 Endpoint Management 设置该 IdP：

- 通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证
- 通过 Citrix Cloud 使用 Okta 进行身份验证
- 通过 Citrix Cloud 使用本地 Citrix Gateway 进行身份验证

配置 **LDAP**

可以在 Endpoint Management 中配置到一个或多个 LDAP 兼容目录的连接以进行基于域的身份验证。Endpoint Management 支持嵌套在 LDAP 中的组。嵌套组每天在本地时间上午 12 点同步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

作为配置 LDAP 的一部分，必须至少安装一个 Cloud Connector。

要了解快速概述，请观看此视频。

这是一个嵌入式视频。单击链接观看视频

要设置 LDAP，请执行以下操作：

1. 在设置页面上，滚动到 **LDAP** 磁贴，然后单击设置。
2. 按照屏幕上的指南下载并安装 Cloud Connector。在 Citrix Cloud 与您的资源之间启用通信需要 Cloud Connector。有关帮助，请参阅 Citrix Cloud Connector。

如果您具有 LDAP 配置并且添加了 Azure AD 或 Okta 作为身份提供程序，Endpoint Management 将同步 Endpoint Management 数据库中 Active Directory 组的特定于 IdP 的信息。此配置不会影响现有交付组和用户注册。但是，您以后将无法在 Endpoint Management 中添加 LDAP 设置。有关详细信息，请参阅身份提供程序身份验证。

如果在注册后通过更改域别名或用户搜索依据设置，用户必须重新注册。有关 LDAP 配置的详细信息，请参阅域或域加安全令牌身份验证。

设置 LDAP 后，您可以继续进行身份验证配置或设置特定平台。

配置 **Citrix Gateway**

与 Endpoint Management 集成后，Citrix Gateway 可提供对您的内部网络和资源的远程设备访问。

Endpoint Management 在以下场景中需要 Citrix Gateway：

- 您需要 Micro VPN 才能访问业务线应用的内部网络资源。这些应用程序通过 Citrix MDX 技术封装。Micro VPN 需要 Citrix Gateway 连接到内部后端基础结构。
- 您计划使用 Endpoint Management 来管理应用程序（MAM 或 MDM+MAM）。仅管理设备 (MDM) 不需要 Citrix Gateway。
- 您计划将 Endpoint Management 与 Microsoft Endpoint Manager 集成。（需要本地 Citrix Gateway。）

要了解快速概述，请观看此视频。

这是一个嵌入式视频。单击链接观看视频

下表汇总了本地 Citrix Gateway 解决方案支持的功能。

支持的功能	Citrix Gateway 本地
Secure Mail (STA)*	是
通道 - Web SSO (Web 单点登录)	是
完整 VPN（不适用于适用于 iOS 的 Citrix 移动生产力应用程序）	是
PerApp VPN	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

支持的功能	Citrix Gateway 本地
移动单点登录（访问控制）	否
高可用性	是 **
多 POP 部署	是 ***
代理支持	是
拆分通道	是
拆分 DNS	是

* Citrix Cloud Secure Ticket Authority (STA) 服务配置

** 本地配置

*** 全局服务器负载平衡配置

本地 **Citrix Gateway** 用例

在以下情况下，将一个或多个本地 Citrix Gateway 设备与 Endpoint Management 结合使用：

- 您需要 PerApp VPN 功能。
- 您需要完整通道、拆分通道、反向拆分通道或拆分 DNS。我们建议对通过客户端证书或端到端 SSL 与内部网络中的资源建立的连接使用完整 VPN 通道。
- 您使用 Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成。

使用本地 Citrix Gateway 涉及大量配置和维护工作。在 Endpoint Management 控制台中配置 LDAP 和 Citrix Gateway 后，可以从该控制台中导出脚本。然后，您可以在 Citrix Gateway 上运行该脚本。

1. 在设置页面上，滚动到 **Citrix Gateway** 磁贴，然后单击开始设置。
2. 选择 **Citrix Gateway (**本地**)** 作为类型。
3. 按照屏幕上的指导进行操作。有关信息，请参阅将本地 Citrix Gateway 配置为与 Endpoint Management 结合使用。

配置通知服务器

要发送通知，必须配置网关和通知服务器。通知服务器可确保最终用户与管理员之间通信的连接性和可能性。要在 Endpoint Management 中设置通知服务器，请参阅通知。

为 **Apple** 设备配置 **Apple** 推送通知服务 **(APNs)** 证书

Endpoint Management 需要 Apple 提供的 Apple 推送通知服务 (APNs) 证书来注册和管理 Apple 设备。如果您打算使用适用于 Apple 的 Secure Mail 的推送通知，Endpoint Management 还需要 APNs 证书。有关 Endpoint

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Management 和 APNs 的信息，请参阅 Secure Mail for iOS 的推送通知。

要从 Apple 获取证书，需要 Apple ID 和开发者帐户。有关详细信息，请参阅 Apple Developer Program（Apple 开发者计划）Web 站点。

要了解快速概述，请观看此视频。

这是一个嵌入式视频。单击链接观看视频

要使用 Citrix 证书签名请求配置 APN，请执行以下操作：

1. 在设置页面上，展开 **Apple** 磁贴。
2. 在 **APNs** 证书磁贴上，单击设置，然后按照屏幕上的指导进行操作。

有关详细信息，请参阅证书和身份验证。

配置 **Android Enterprise**

Endpoint Management 在您创建交付组并通过 Cloud 库向交付组分配用户后完全配置。自此之后，Endpoint Management 管理将在 Citrix Cloud 中进行。组合后的界面简化了在 Citrix Cloud 与 Endpoint Management 之间切换的过程。

可以使 Google Play 或 Google Workspace 为 Endpoint Management 设置 Android Enterprise。

1. 如果贵组织不使用 **Google Workspace**：您可以使用托管 Google Play 将 Citrix 注册为 EMM 提供商。如果使用托管 Google Play，您将为设备和最终用户预配托管 Google Play 帐户。托管 Google Play 帐户提供对托管 Google play 的访问，以允许用户安装和使用您提供的工作应用程序。如果贵组织使用第三方身份服务，您可以将托管 Google Play 帐户与您的现有身份帐户链接。

   由于这种类型的企业未绑定到域，因此，您可以为单个组织创建多个企业。例如，组织中的每个部门或区域都可以注册为不同的企业。通过该设置，您可以使用不同的企业来管理单独的设备和应用程序集合。

2. 如果贵组织尚未使用 **Google Workspace** 向用户提供对 **Google Apps** 的访问权限：您可以使用 Google Workspace 将 Citrix 注册为 EMM。如果贵组织使用 Google Workspace，它将具有现有企业 ID 和用户的现有 Google 帐户。要将 Endpoint Management 与 Google Workspace 配合使用，请使用 Google Directory API 与 LDAP 目录同步并从 Google 检索 Google 帐户信息。

   这种类型的企业与现有域相关联。因此，每个域只能创建一个企业。要在 Endpoint Management 中注册设备，每个用户都必须使用其现有的 Google 帐户手动登录。该帐户允许用户通过 Google Workspace 计划访问托管 Google Play 和其他 Google 服务。

要了解快速概述，请观看此视频。

这是一个嵌入式视频。单击链接观看视频

要开始，请执行以下操作：

1. 在设置页面上，展开 **Android** 磁贴。
2. 在 **Android Enterprise** 磁贴上，单击设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 根据您为用户提供 Google Play 应用程序访问权限的方法，选择 **Google Play** 或 **G Suite**。
   如果您之前使用 Google Play 配置了 Android Enterprise 平台，UI 会将您带到 Google Play 应用商店以重新注册。单击重新注册，返回到 CEM 控制台，然后刷新页面。
4. 按照屏幕上的指导进行操作。

请参阅：

- 创建 Android Enterprise 帐户

配置 **Firebase Cloud Messaging**

Citrix 建议使用 Firebase Cloud Messaging (FCM) 来控制将 Android 设备连接到 Endpoint Management 的方式和时间。Endpoint Management 将连接通知发送到针对 FCM 启用的 Android 设备。任何安全操作或部署命令都将触发推送通知，以提示用户重新连接到 Endpoint Management。请参阅 Firebase Cloud Messaging。

与 **Microsoft Endpoint Manager** 集成

Endpoint Management 与 Microsoft Endpoint Manager 的集成将 Endpoint Management Micro VPN 的值增加到 Microsoft Intune 感知应用程序，例如 Microsoft Edge 浏览器。

Endpoint Management 与 MEM 的集成还允许企业通过 Intune 和 Citrix 封装自己的业务线应用。应用程序封装在 Intune 移动应用程序管理 (MAM) 容器内提供 Micro VPN 功能。借助 Endpoint Management Micro VPN，您的应用程序能够访问本地资源。可以在一个容器中管理和交付 Office 365 应用程序、业务线应用和 Citrix Secure Mail。单个容器可提供极致的安全性和生产力。

- Citrix Cloud 管理员默认为 Endpoint Management 管理员。
- 创建的具有客户访问权限的 Citrix Cloud 管理员必须选择 Endpoint Management，才能管理 Endpoint Management。

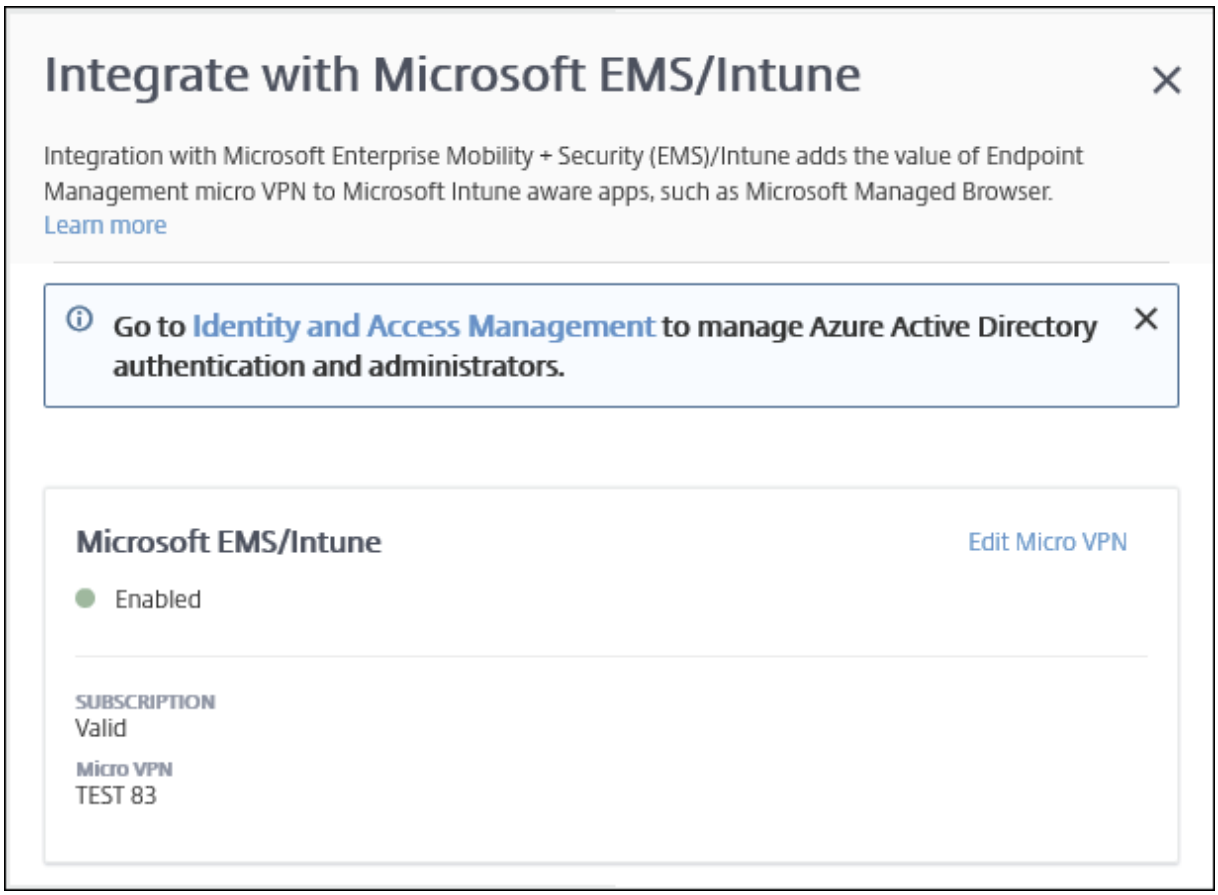
在 Endpoint Management 控制台中，只能更改用户的角色和成员关系。要随时更改角色，请从 Citrix Cloud 控制板访问 Endpoint Management 控制台。转到管理选项卡并单击用户。选择特定用户，然后单击编辑以更改角色。有关详细信息，请参阅使用 RBAC 配置角色。

要与 MEM 集成，请参阅 Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成。

在 Citrix Cloud 中完成配置后，返回到 Endpoint Management 控制台，如下所示：转到 Citrix Cloud 主页，然后单击 **Endpoint Management** 磁贴上的管理。然后，您可以验证是否已使用 Azure Active Directory 帐户登录 Endpoint Management。

1. 在设置页面上，滚动到 与 **Microsoft EMS/Intune** 集成磁贴。
2. 单击查看更多。UI 将指示您是否已成功启用连接。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



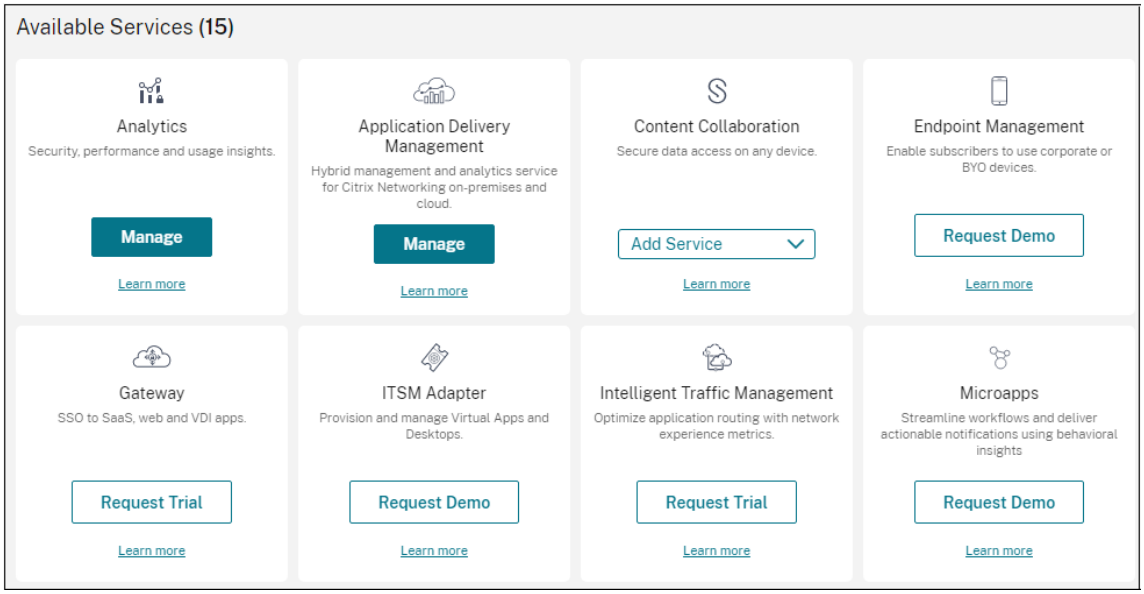
在 Citrix Cloud 控制台中，也可以更改用户名或密码，以及删除或编辑本地用户。请参阅身份识别和访问管理。

将现有 **Citrix Content Collaboration** 帐户链接到 **Citrix Cloud**

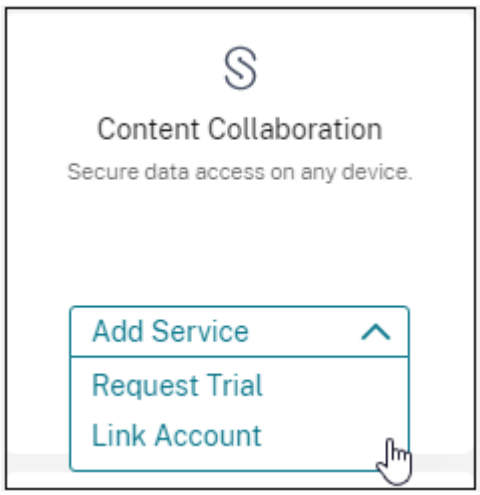
如果您有在注册 Citrix Cloud 之前已存在的 Citrix Content Collaboration 帐户，则必须将该帐户链接到 Citrix Cloud。要链接帐户，您的电子邮件地址必须是 Citrix Content Collaboration 帐户的管理员。当您准备好继续操作时，请访问 https://onboarding.cloud.com。

1. 登录后，将显示如下所示的屏幕。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

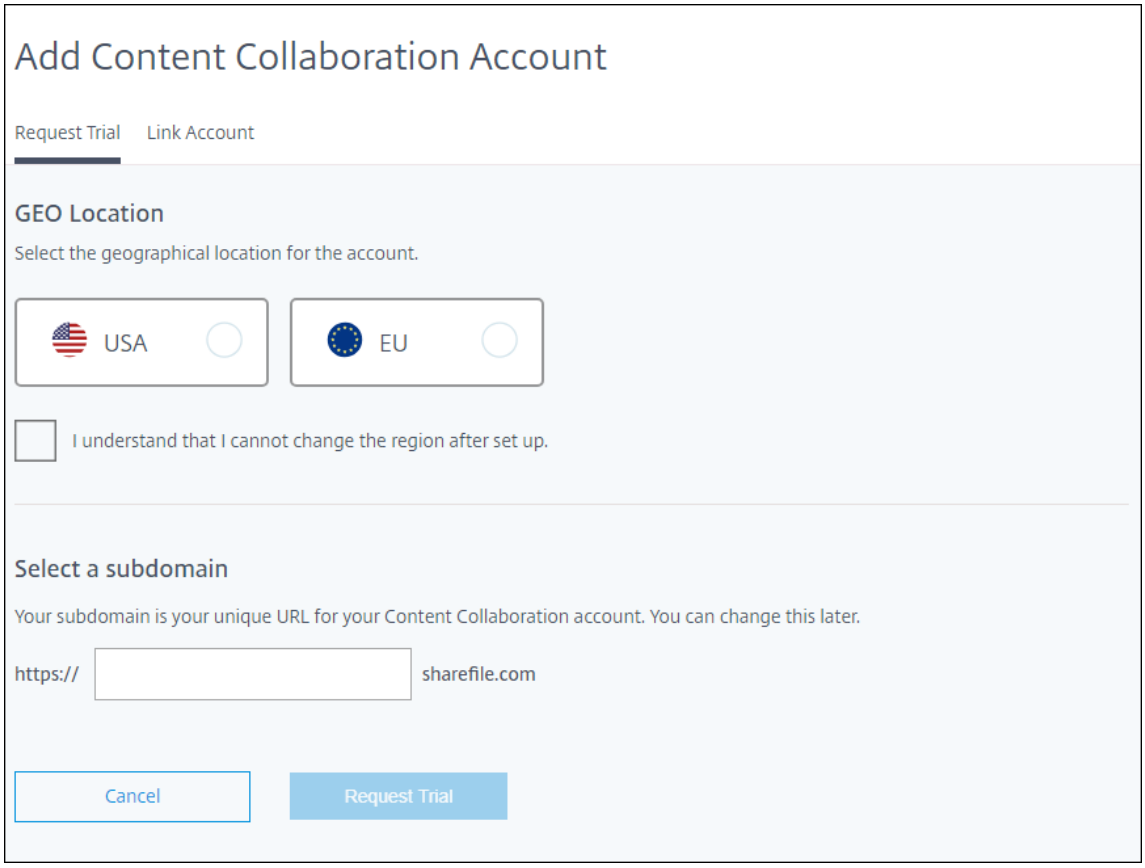


2. 在 **Citrix Content Collaboration** 磁贴中，选择链接帐户。



3. 确认 Citrix Content Collaboration 帐户后，将显示以下页面：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 单击 **Link Account**（链接帐户）选项卡完成此过程。可以立即从 Citrix Cloud 管理您的 Citrix Content Collaboration 帐户。

Cloud Connector 的扩展和大小注意事项

December 3, 2021

在评估 Citrix Endpoint Management 服务的大小和可扩展性时，请根据您的特定要求研究和测试 Cloud Connector 的配置。Cloud Connector 仅在设备注册期间低于负载。缩小计算机大小会对系统性能产生负面影响。

Citrix 需要每个资源位置配备两个 Cloud Connector。在不与任何其他组件或产品共享责任的专用服务器上安装 Cloud Connector。在我们的测试中，Cloud Connector 部署在高可用性集中（它们的负载不平衡）。

测试配置

- 两个专用 Windows Server 2019，2 个 vCPU，4 GB 内存
- Android 和 iOS 设备注册到 MDM +MAM 中，在 8 小时内均匀拆分
- Endpoint Management 配置为每 1000 台设备每小时注册 125 台设备
  - 1000 台设备（每小时注册 125 台设备）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 5000 台设备（每小时注册 625 台设备）
- 10000 台设备（每小时注册 1250 台设备）
- 20000 台设备（每小时注册 2500 台设备）

测试结果

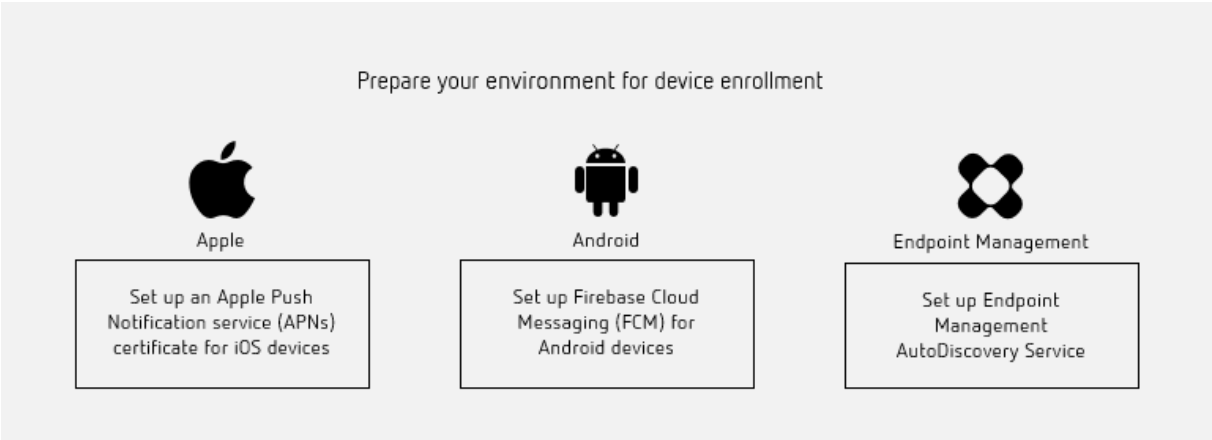
Cloud Connector	1000 台设备	5000 台设备	10000 台设备	20000 台设备
CPU 平均值	2%	2%	4%	4%
CPU 最大值	8%	8%	10%	11%
内存平均值	73%	73%	75%	75%
最大内存	76%	76%	76%	79%

准备注册设备并交付资源

July 24, 2023

> 重要：
>
> 在继续操作之前，请务必完成载入和资源设置中描述的所有任务。
>
> 让您的用户了解即将发生的变更。请参阅欢迎使用 Citrix User Adoption Kit。

Endpoint Management 支持各种注册选项。本文介绍了启用要注册的所有受支持的设备所需的基本设置。下图概要介绍了基本设置。



有关支持的设备列表，请参阅支持的设备操作系统。

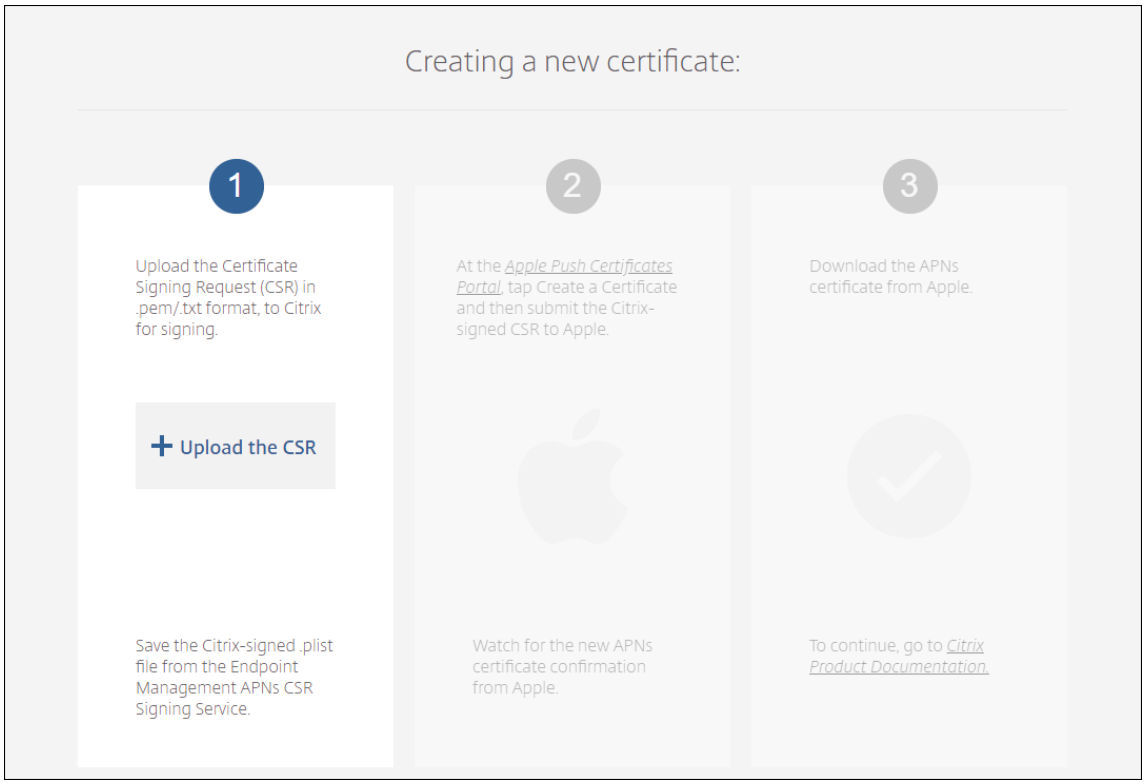
为 **iOS** 设备设置 **Apple** 推送通知服务 **(APNs)** 证书

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> Apple 对 APNs 旧版二进制文件协议的支持将于 2021 年 3 月 31 日结束。Apple 建议您改为使用基于 HTTP/2 的 APNs 提供程序 API。自版本 20.1.0 起，Citrix Endpoint Management 支持基于 HTTP/2 的 API。有关更多信息，请参阅 https://developer.apple.com/ 中的新闻更新 “Apple 推送通知服务更新”。有关检查与 APN 的连接的帮助，请参阅连接检查。

Endpoint Management 需要 Apple 提供的 Apple 推送通知服务 (APNs) 证书来注册和管理 iOS 设备。Endpoint Management 还需要 APNs 证书才能接收 Secure Mail for iOS 推送通知。

- 要从 Apple 获取证书，需要 Apple ID 和开发者帐户。有关详细信息，请参阅 Apple Developer Program（Apple 开发者计划）Web 站点。
- 要获取 APNs 证书并将其导入 Endpoint Management，请参阅 APNs 证书。



- 有关 Endpoint Management 和 APNs 的详细信息，请参阅 Secure Mail for iOS 的推送通知。

为 **Android** 设备设置 **Firebase Cloud Messaging (FCM)**

Firebase Cloud Messaging (FCM) 控制 Android 设备连接到 Endpoint Management 服务的方式和时间。任何安全操作或部署命令都将触发推送通知。通知会提示用户重新连接到 Endpoint Management。

- FCM 设置要求您配置 Google 帐户。要创建 Google Play 凭据，请参阅管理您的开发者帐户信息。还可以使用 Google Play 可添加、购买和审批应用程序，以便部署到设备上的 Android Enterprise 工作区。可以使用 Google Play 部署您的私有 Android 应用程序、公共应用程序和第三方应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 要设置 FCM，请参阅 Firebase Cloud Messaging。

设置 **Endpoint Management** 自动发现服务

自动发现服务通过基于电子邮件的 URL 发现简化用户的注册过程。自动发现服务还为 Citrix Workspace 客户提供注册验证、证书固定以及其他优势等功能。该服务托管在 Citrix Cloud 中，是许多 Endpoint Management 部署的重要组成部分。

使用自动发现服务，用户可以：

- 可以使用公司网络凭据注册其设备。
- 不需要输入有关 Endpoint Management 服务器地址的详细信息。
- 以用户主体名称 (UPN) 格式输入其用户名。例如，`user@mycompany.com`。

我们建议您在高安全性环境中使用自动发现服务。自动发现服务支持公钥证书固定，以防范中间人攻击。证书固定功能可确保 Citrix 客户端在与 Endpoint Management 通信时使用贵企业签名的证书。要为 Endpoint Management 站点配置证书固定，请联系 Citrix 支持。有关证书固定的信息，请参阅证书固定。

要访问自动发现服务，请导航到 https://adsui.cloud.com（商用）或 https://adsui.cem.cloud.us（政府）。

必备条件

- Citrix Cloud 中的新自动发现服务需要最新版本的 Secure Hub：
  - 对于 iOS，Secure Hub 版本 21.6.0 或更高版本
  - 对于 Android，Secure Hub 版本 21.8.5 或更高版本

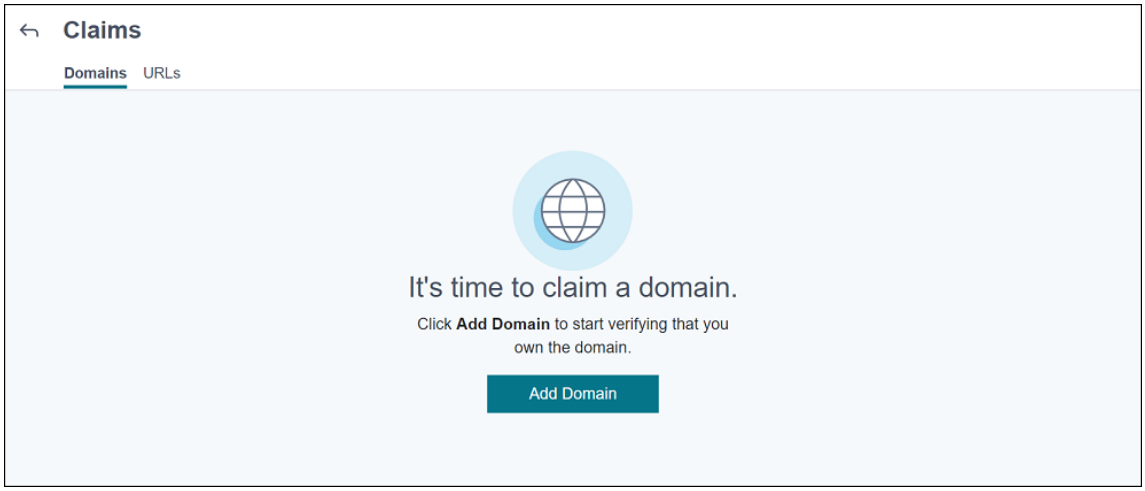
    在 Secure Hub 早期版本上运行的设备可能会遇到服务中断的情况。
- 您必须拥有具有完全访问权限的 Citrix Cloud 管理员帐户，才能访问新的自动发现服务。自动发现服务不支持具有自定义访问权限的管理员帐户。如果您没有帐户，请参阅注册 Citrix Cloud。

  Citrix 在不中断服务的情况下将所有现有的自动发现记录迁移到 Citrix Cloud。迁移的记录不会自动显示在新控制台中。必须在新的自动发现服务中回收域才能证明所有权。有关详细信息，请参阅 CTX312339。
- 在开始将自动发现服务用于 Endpoint Management 部署之前，请验证并声明您的域。最多可以声明 10 个域。该声明将已验证的域与自动发现服务相关联。要声明超过 10 个域，请开立 SRE 票证或联系 Citrix 技术支持。
- 请使用 MAM 端口设置（而非 Citrix Gateway FQDN）将 MAM 流量定向到您的数据中心。如果输入完全限定的域名以及 Citrix Gateway 的端口，客户端设备将使用 **MAM** 端口设置中的配置。
- 如果广告拦截程序阻止打开站点，请确保您为整个 Web 站点禁用了广告拦截程序。

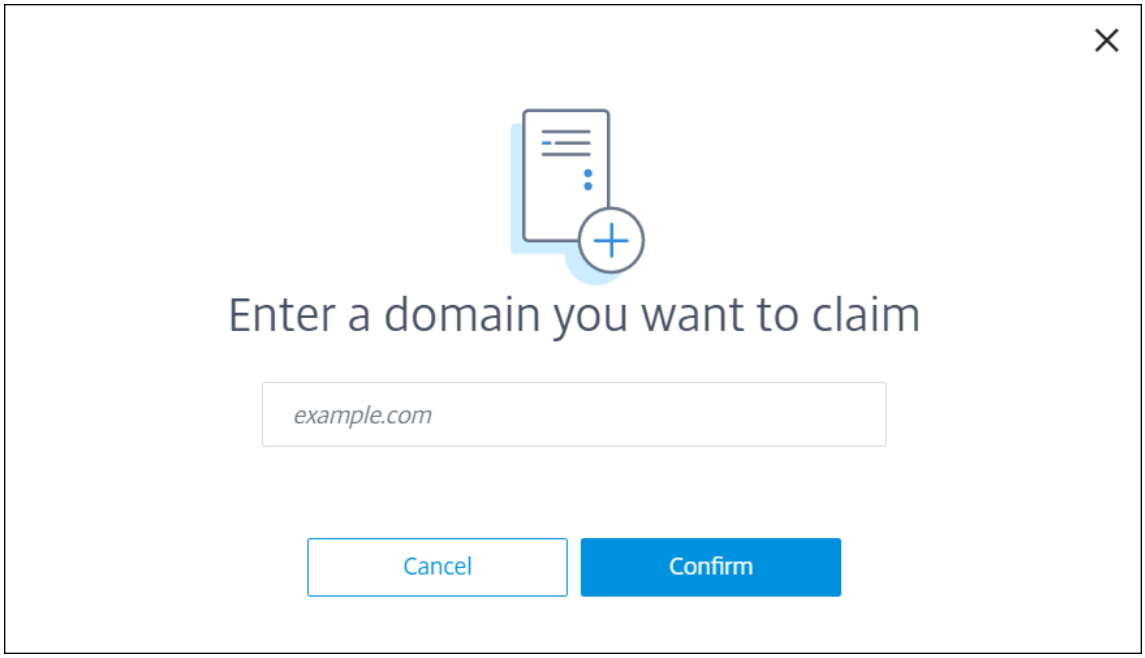
申领域

1. 在声明 **>** 域选项卡上，单击添加域。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

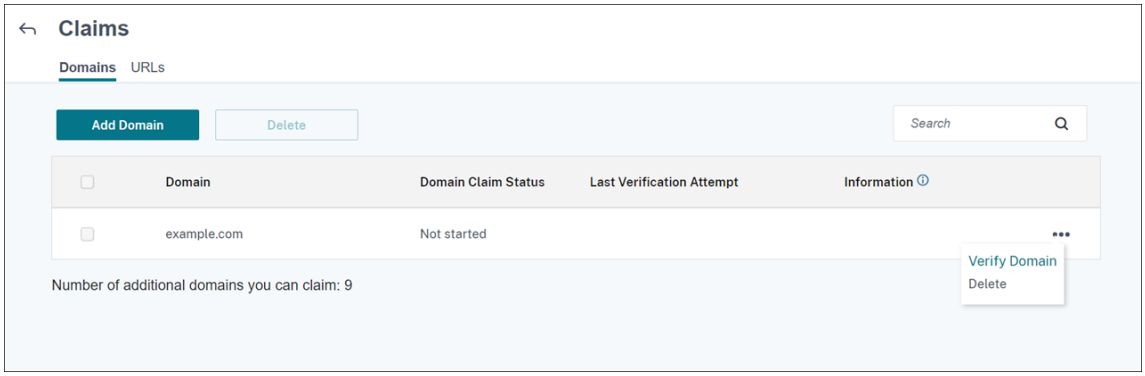


2. 在出现的对话框中，输入 Endpoint Management 环境的域名，然后单击 确认。您的域名将显示在声明 **>** 域中。

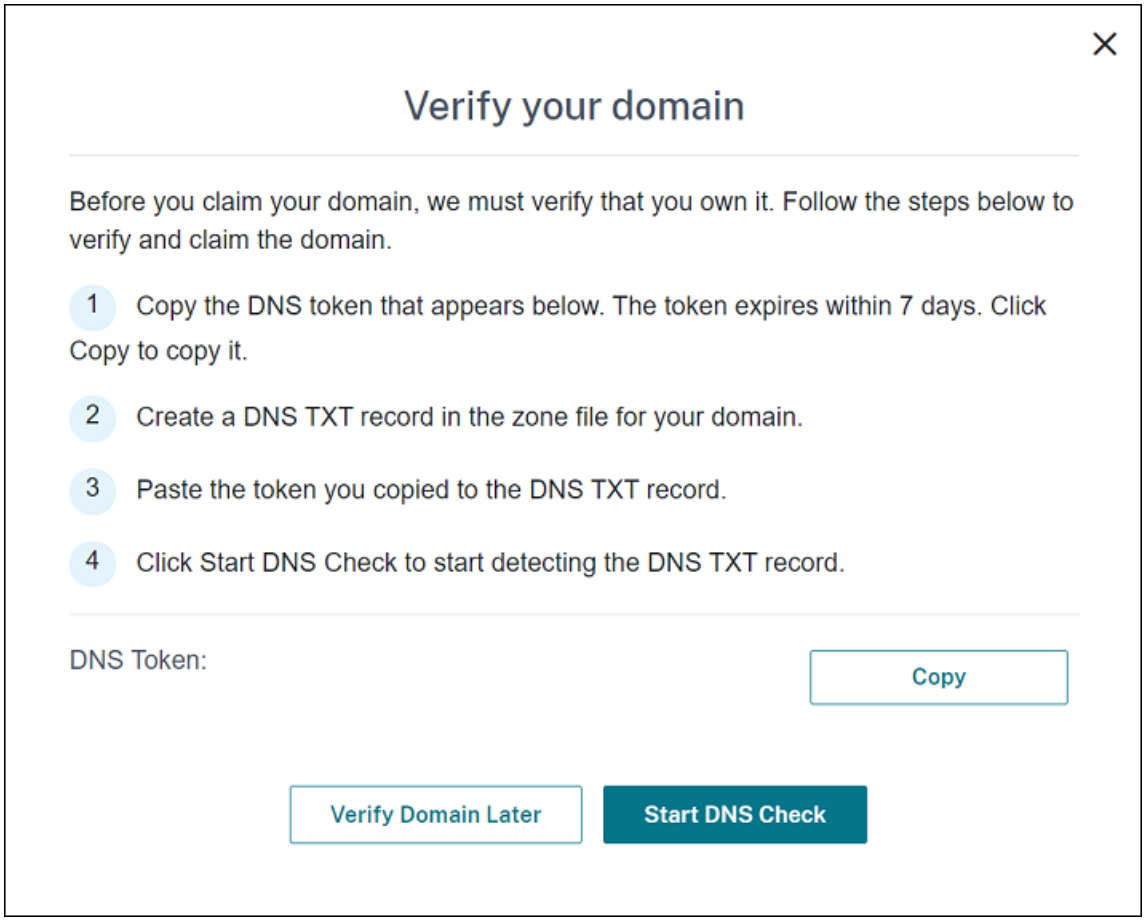


3. Verify Domain 在添加的域中，单击省略号菜单，然后选择 **Verify Domain**（验证域）以开始验证过程。此时将显示验证您的域页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 在 **Verify your domain**（验证您的域）页面上，按照说明进行操作以验证您是否拥有该域。

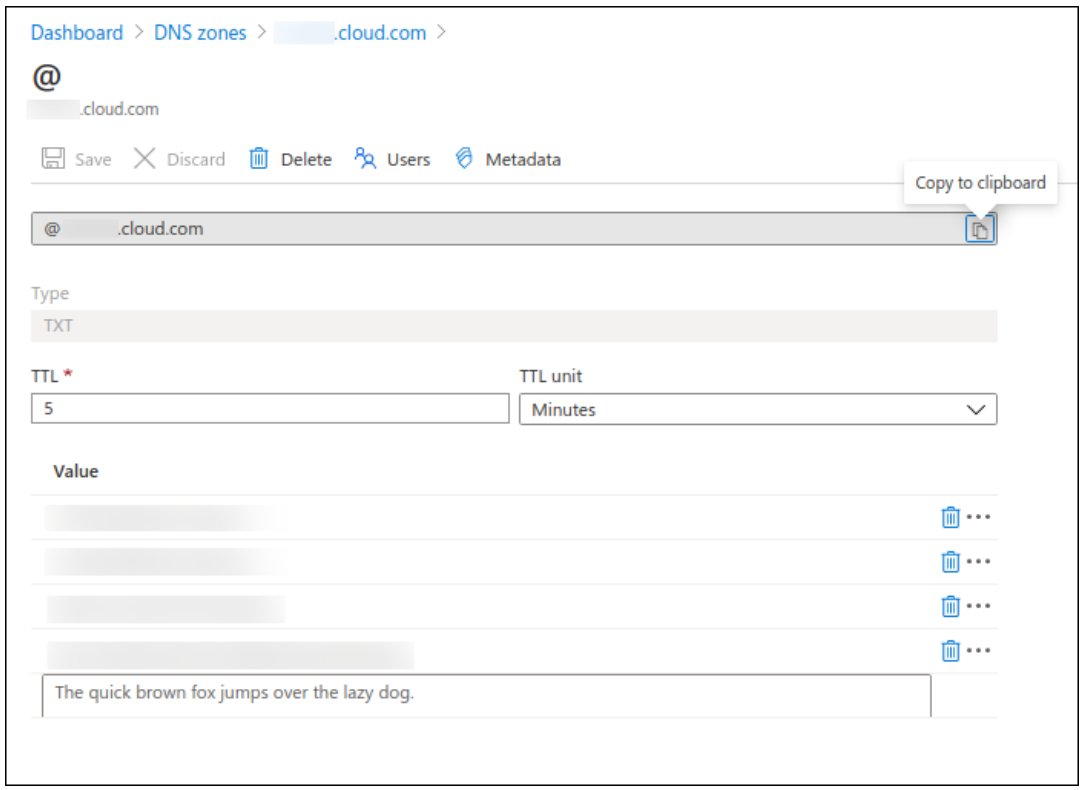


a) 单击 **Copy**（复制）将 DNS 令牌复制到剪贴板。

b) 在区域文件中为您的域创建 DNS TXT 记录。为此，请转到托管提供商门户网站的域并添加您复制的 DNS 令牌。

下面的屏幕截图显示了托管提供商门户网站的域。您的门户可能看起来有所差别。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



c) Start DNS Check 在 Citrix Cloud 中，在 **Verify your domain**（验证您的域）页面上，单击 **Start DNS Check**（启动 DNS 检查）以开始检测 DNS TXT 记录。如果要在以后验证域，请单击 **Verify Domain Later**（以后验证域）。

验证过程通常需要大约一个小时。但是，最多可能需要两天才能返回响应。在状态检查期间，您可以注销并重新登录。

配置完成后，域的状态将从挂起更改为已验证。

5. 声明您的域后，请提供自动服务的相关信息。单击您添加的域上的省略号菜单，然后单击添加 **Endpoint Management** 信息。此时将显示 **AutoDiscovery Service Information**（自动发现服务信息）页面。
6. 输入以下信息，然后单击保存。
   - **Endpoint Management** 服务器 **FQDN**：输入 Endpoint Management 服务器的完全限定域名。例如：`example.xm.cloud.com`。此设置用于 MDM 和 MAM 控制流量。
   - **Citrix Gateway FQDN**：输入 Citrix Gateway 的完全限定域名，格式为 FQDN 或 FQDN:port。例如：`example.com`。此设置用于将 MAM 流量定向到您的数据中心。对于仅限 MDM 部署，请将此字段留空。

     > 注意：
     >
     > Citrix 建议您使用 **MAM** 端口设置而非 **Citrix Gateway FQDN** 来控制 MAM 流量。如果输入完全限定的域名以及 Citrix Gateway 的端口，客户端设备将使用 **MAM** 端口设置中的配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 实例名称：输入您在上面配置的 Endpoint Management 服务器的实例名称。如不确定实例名称，请保留默认值 **zdm**。
- **MDM** 端口：输入用于 MDM 控制流量和 MDM 注册的端口。对于基于云的服务，默认值为 443。
- **MAM** 端口：输入用于 MAM 控制流量、MAM 注册、iOS 注册和应用程序枚举的端口。对于基于云的服务，默认值为 8443。

请求 **Windows** 设备的自动发现

如果计划注册 Windows 设备，请执行以下操作：

1. 与 Citrix 支持部门联系并创建支持请求以启用 Windows 自动发现。
2. 获取适用于 `enterpriseenrollment.mycompany.com` 的公开签名的非通配符 SSL 证书。`mycompany.com` 部分是包含用户用于注册的帐户的域。将.pfx 格式的 SSL 证书及其密码附加到在上一步中创建的支持请求。

   要使用多个域注册 Windows 设备，还可以使用具有以下结构的多域证书：

   - SubjectDN，包含用于指定所服务的主域的 CN（例如 enterpriseenrollment.mycompany1.com）。
   - 适用于其余域的恰当 SAN（例如 enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.com 等）。
3. 在您的 DNS 中创建一条规范名称 (CNAME) 记录，并将 SSL 证书的地址 (enterpriseenrollment.mycompany.com) 映射到 autodisc.xm.cloud.com。

   当 Windows 设备用户使用 UPN 注册时，Citrix 注册服务器：

   - 提供 Endpoint Management 服务器的详细信息。
   - 指示设备从 Endpoint Management 请求有效证书。

此时，您可以注册所有受支持的设备。继续下一部分，准备向设备提供资源。

与 **Azure AD** 条件访问集成

你可以将 Endpoint Management 配置为将 Azure AD 条件访问支持应用于 Office 365 应用程序。此功能允许您在部署 Office 365 应用程序时为设备用户部署零信任方法。您可以使用设备状态、风险评分、位置和设备保护功能来应用自动操作，并定义对托管 Android Enterprise 和 iOS 设备上 Office 365 应用程序的访问权限。

要强制实施 Azure AD 设备合规性，必须为各个 Office 365 应用程序配置条件访问策略。您可以限制用户对不受管理和不合规设备上的特定 Office 365 应用程序的访问权限，并仅允许在受管设备和合规设备上访问单个应用程序

必备条件

- 对于此集成，你必须拥有有效的 Azure AD 高级订阅，包括 Intune 和 Microsoft Office 365 许可证。
- Secure Hub 21.4.0 及更高版本

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 在 Citrix Cloud 中将 Azure AD 配置为身份提供商 (IdP)，然后将 Citrix 身份设置为 Endpoint Management 的 IdP 类型。有关信息，请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。
- 同意使用 Citrix 多租户 AAD 应用程序以允许移动应用程序对 AAD 客户端应用程序进行身份验证。仅在 Azure 全局管理员将 **Users can register applications**（用户可以注册应用程序）的值设置为否时必需。在 Azure 门户中的 **Azure Active Directory >** 用户 **>** 用户设置下配置此设置。要同意，请参阅配置 Endpoint Management 以实现 Azure AD 合规性管理。
- 在开始 Azure AD 设备注册过程之前，在设备上安装 Microsoft Authenticator 应用程序。
- 对于 Android Enterprise 平台，请将 Web 浏览器应用程序配置为必需的公共商店应用程序。
- 禁用 Azure AD 控制台中的 安全默认设置。启动 Azure AD 配置时，将用更精细的 Azure AD 条件访问策略替换安全默认设置。有关安全默认设置的详细信息，请参阅 Microsoft 文档。

通过 **Azure AD** 条件访问策略配置设备合规性

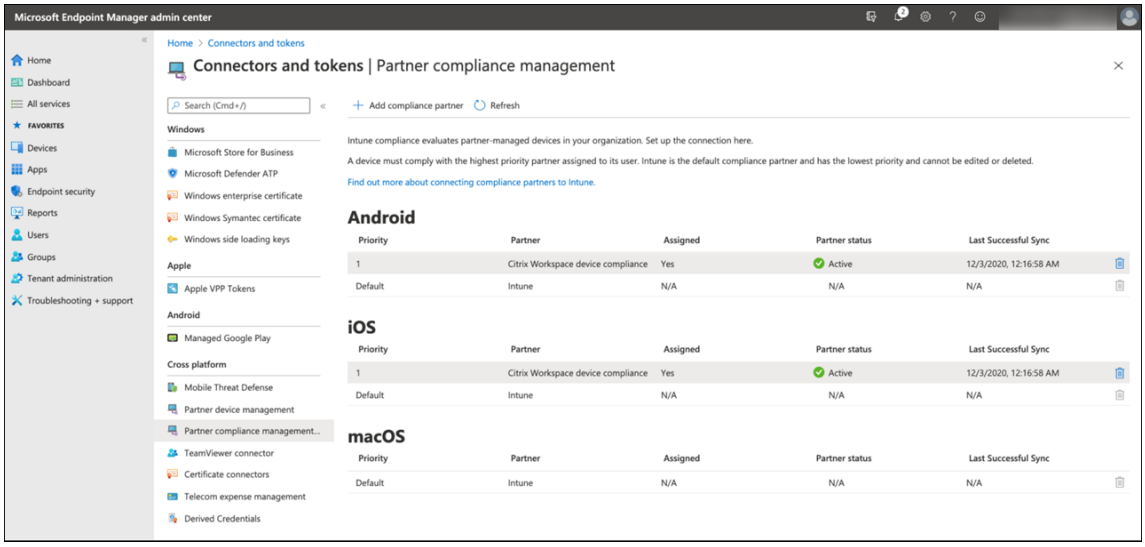
通过 Azure AD 条件访问策略配置设备合规性的一般步骤如下：

1. **Endpoint Management** 配置：
   - 在 Microsoft 端点管理器管理中心中，将 **Citrix Workspace** 设备合规性添加为每个设备平台的合规性合规性合作伙伴并分配用户组。
   - 在 Endpoint Management 中，同步来自 Microsoft 端点管理器管理中心的信息。
2. **Azure AD** 配置：在 Azure AD 门户中，为各个 Office 365 应用程序设置条件访问策略。
3. **Endpoint Management** 配置：为 Office 365 应用程序配置条件访问策略后，在 Endpoint Management 中添加 Microsoft Authenticator 应用程序和 Office 365 应用程序作为公共应用商店应用程序。将这些公共应用程序分配给交付组并将其设置为必需的应用程序。

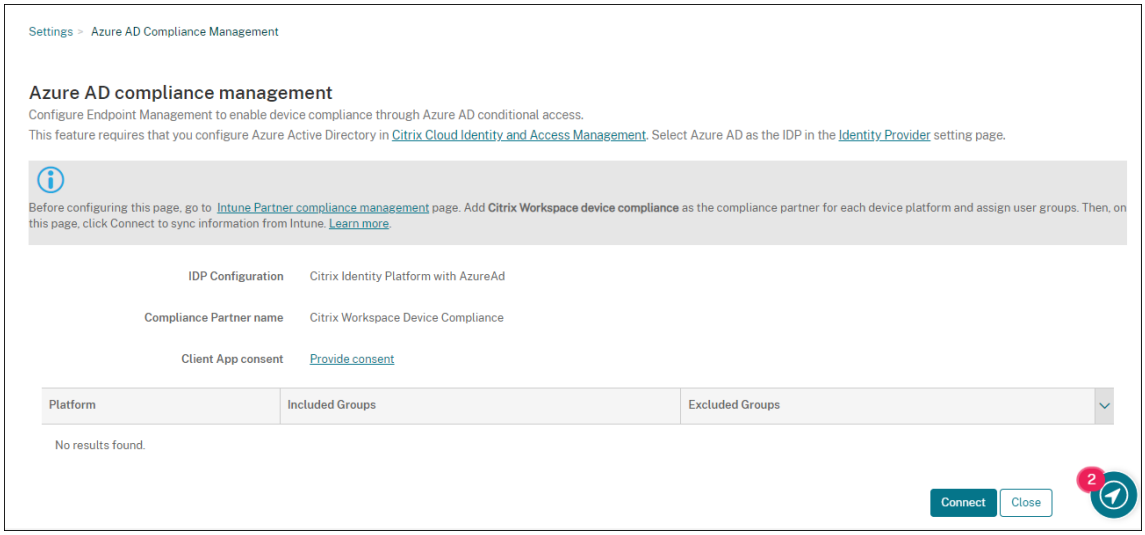
为 **Azure AD** 合规性管理配置 **Endpoint Management**

1. 登录 Microsoft Endpoint Manager admin center（Microsoft Endpoint Manager 管理中心），导航到 **Tenant administration**（租户管理）**> Connectors and token**（连接器和令牌）**> Device compliance management**（设备合规性管理）。单击 添加合规性合作伙伴，然后选择 **Citrix Workspace** 设备合规性作为每个设备平台的合规性然后分配用户组。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

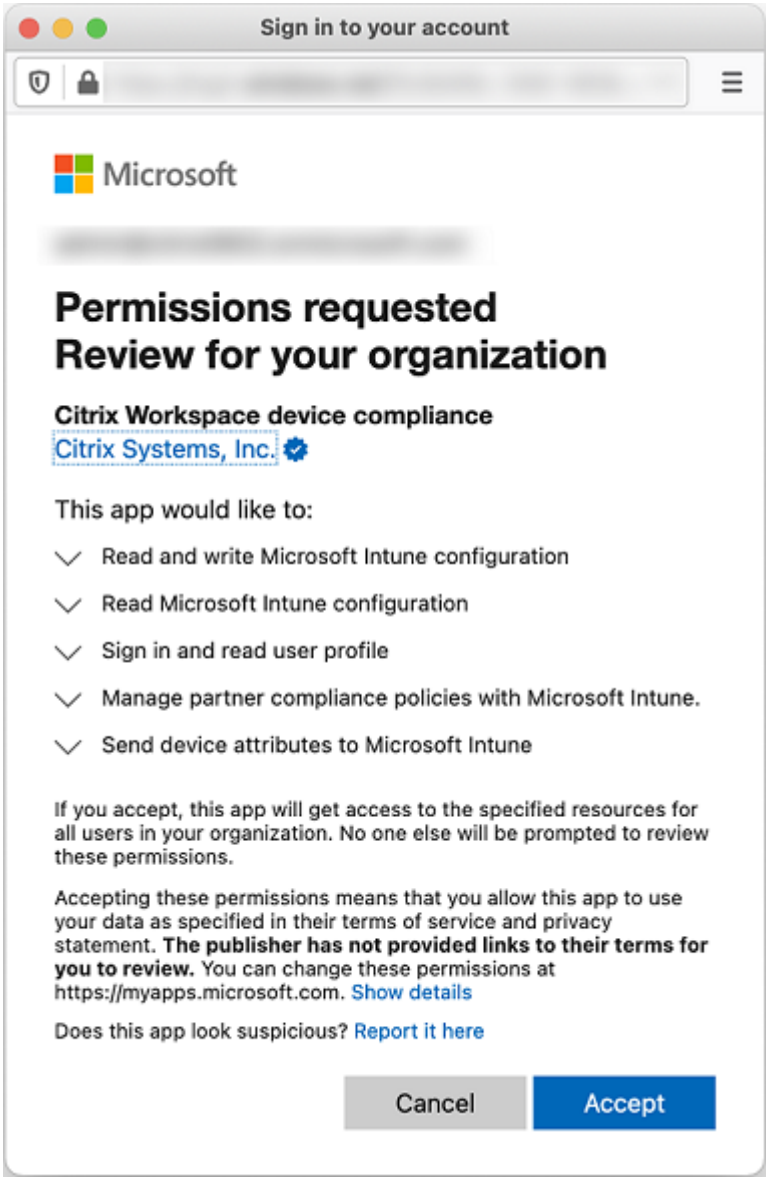


2. 在 Endpoint Management 中，转到 **Settings**（设置）**> Azure AD compliance management**（**Azure AD** 合规性管理）。
3. （可选）设置全局同意，以便用户不需要在每个设备上提供同意。在 **Client App consent**（客户端应用程序同意）旁边，单击 **Provide consent**（提供同意）。输入您的全局管理员 Azure AD 凭据并按照提示提供客户端应用程序的全局同意。
4. 单击 连接以同步来自 Microsoft 端点管理器管理中心的信息。



将出现一个对话框，提示您接受此配置的权限。单击 **Accept**（接受）。配置完成后，同步的设备平台将显示在列表中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



在 **Azure AD** 中配置条件访问策略

在 Azure AD 门户中，为 Office 365 应用程序配置条件访问策略以强制设备合规性。转至 **Devices**（设备）**> Conditional Access**（条件访问）**> Policies**（策略）**> New policy**（新建策略）。有关详细信息，请参阅 Microsoft 文档。

要为 Intune 托管应用配置设备合规性：

- 配置 Intune 托管应用程序以交付到设备
- 需要批准的客户端应用程序
- 需要应用程序保护策略和批准的用于云应用程序访问的客户端应用程序

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在 **Endpoint Management** 中配置应用

为 Office 365 应用程序配置条件访问策略后，在 Endpoint Management 中添加 Microsoft Authenticator 应用程序和 Office 365 应用程序作为公共应用商店应用程序。将这些公共应用程序分配给交付组并将其设置为必需的应用程序。有关信息，请参阅添加公共应用商店应用程序。

用户验证工作流

1. 新用户必须使用 Azure AD 凭据将设备注册到 Endpoint Management 中。以前使用 Azure AD 凭据注册的用户无需重新注册其设备。
2. Endpoint Management 将 Microsoft Authenticator 和配置的 Office 365 应用程序作为必需的应用程序推送到设备。如果您将 Web 浏览器应用程序配置为 Android 平台所需的公共商店应用程序，那么 Endpoint Management 也会将其推送到用户设备。
3. Secure Hub 自动安装和显示通过 Endpoint Management 管理的所有应用程序。
4. 当用户尝试登录任何可用的 Office 365 应用程序时，设备会提示用户点击 **Azure AD** 注册链接以启动注册过程。
5. 用户点击注册链接后，Microsoft 身份验证器应用程序将打开。用户输入 Azure AD 凭据并同意设备注册条款。然后微软身份验证器应用程序关闭并重新打开 Secure Hub。
6. Secure Hub 显示 Azure AD 设备注册已完成的消息。用户现在可以使用微软应用程序访问他们的云资源。

   注册完成后，Azure AD 会在控制台中将设备标记为托管并合规。

默认设备策略和移动生产力应用程序

如果您自 Endpoint Management 19.5.0 或更高版本开始使用，我们会预先配置一些设备策略和移动生产力应用程序。该配置使您能够：

- 立即将基本功能部署到设备
- 收钱执行建议的安全工作区的基准配置

对于 Android、Android Enterprise、iOS、macOS 和 Windows Desktop/Tablet 平台，您的站点包含以下预配置的设备策略：

- 密码设备策略：密码设备策略设置为开，启用所有默认的密码设置。
- 应用程序清单设备策略：应用程序清单设备策略设置为开。
- 限制设备策略：限制设备策略设置为开，启用所有默认限制设置。

这些策略位于 **AllUsers** 交付组中，该交付组包含所有 Active Directory 和本地用户。我们建议您仅将 AllUsers 交付组用于初始测试。然后，创建交付组并禁用 AllUsers 交付组。可以在交付组中重复使用预配置的设备策略和应用程序。

所有 Endpoint Management 设备策略都记录在设备策略下。该文章包含有关如何使用控制台编辑设备策略的信息。有关某些常用设备策略的信息，请参阅设备策略和用例行为。

对于 iOS 和 Android 平台，您的站点包含以下预配置的移动生产力应用程序：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Secure Mail**
- **Secure Web**
- **Citrix Files**

这些应用程序位于 **AllUsers** 交付组中。

有关详细信息，请参阅关于移动生产力应用程序。

继续执行 **Endpoint Management** 配置

完成设备注册的基本设置后，配置 Endpoint Management 的方式因您的用例而有很大差异。例如：

- 您有哪些安全要求？您希望如何平衡这些要求与用户体验？
- 您支持哪些设备平台？
- 用户是否拥有其设备或使用公司拥有的设备？
- 您希望向设备推送哪些设备策略？
- 您为用户提供哪些类型的应用程序？

本部分通过引导您查看此文档集中的文章，帮助您浏览许多配置选项。

在第三方站点中完成配置时，请记下信息及其位置，以便在配置 Endpoint Management 控制台设置时参考。

- 安全性和身份验证。Endpoint Management 使用证书创建安全连接并对用户进行身份验证。Citrix 为您的 Endpoint Management 实例提供通配符证书。
  - 有关按安全级别对身份验证组件和推荐的配置的讨论，请参阅“高级概念”文章身份验证。另请参阅安全性和用户体验。
  - 有关 Endpoint Management 操作期间使用的身份验证组件的概述，请参阅证书和身份验证。
  - 可以从以下身份验证类型中进行选择。配置身份验证包括 Endpoint Management 和 Citrix Gateway 控制台中的任务。
    - 域或域加安全令牌身份验证
    - 客户端证书或证书加域身份验证
  - 要向用户提供证书，请配置：
    - PKI 实体
    - 凭据提供程序
  - 设备注册安全模式。设备注册安全模式指定凭据类型，并使用用户在 Endpoint Management 中注册设备所需的注册步骤。有关信息，请参阅配置注册安全模式。
  - 要允许用户使用 Azure Active Directory 凭据进行身份验证，请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。
- 设备注册
  - 计划可用于注册大量设备：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 通过 Apple 部署计划部署设备
    * Apple 设备的批量注册
    * 批量注册 Windows 设备
  - 要注册 Android 设备，请创建 Android Enterprise 管理员帐户。请参阅 Android Enterprise。或者，请参阅适用于 Google Workspace 客户的旧版 Android Enterprise。
  - 要注册 Citrix Ready Workspace Hub，请参阅 Workspace Hub 设备管理
  - 您可以使用注册邀请或发送注册通知。
    * 注册邀请。
    * 通知。
  - 有关注册的详细信息，请参阅设备管理以及该节点下的文章。
- 设备策略和管理
  - 设备 (MDM) 策略。所有 Endpoint Management 设备策略都记录在设备策略下。有关某些常用设备策略的信息，请参阅设备策略和用例行为。
  - 客户端属性。客户端属性包含用户设备上直接提供给 Secure Hub 的信息。请参阅客户端属性和 Endpoint Management 客户端属性。
  - 交付组。有关与交付组有关的示例用例，请参阅用户社区和添加交付组。
- 准备应用程序以进行部署
  - 有关 Endpoint Management 支持的应用程序的信息，请参阅添加应用程序。
  - 可以使用 Apple 批量购买管理 iOS 应用程序许可。有关信息，请参阅 Apple 批量购买。
  - 可以使用 Endpoint Management 部署您通过 Apple 批量购买获取的 iBooks。请参阅添加媒体。
  - Citrix 提供移动生产力应用程序，包括 Secure Mail 和 Secure Web。请参阅关于移动生产力应用程序。
  - 作为 Secure Mail 的替代方案，您可以将本机邮件传递到设备。请参阅：
    * 电子邮件策略
    * 适用于 Exchange ActiveSync 的 Endpoint Management 连接器
    * 适用于 Exchange ActiveSync 的 Citrix Gateway 连接器
  - 要允许用户将文档和数据安全地传输给 Microsoft Office 365 应用程序，请参阅允许与 Office 365 应用程序的安全交互和 Office 设备策略。
  - 有关应用程序策略的常规信息，请参阅应用程序策略和用例场景。
  - MDX Toolkit 是应用程序封装技术，用于将企业应用程序准备好用于 Endpoint Management 安全部署。MAM SDK 取代了 MDX Toolkit。MDX Toolkit 计划于 2023 年 7 月达到生命周期已结束状态。

    有关 MAM SDK 的信息，请参阅 MAM SDK 概述。
  - 有关应用程序的详细信息，请参阅添加应用程序下的其他文章。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 通过 Endpoint Management 中基于角色的访问控制 (RBAC) 功能，可以向用户和组分配预定义的角色（或称权限集）。这些权限控制用户对系统功能的访问级别。有关信息，请参阅使用 RBAC 配置角色。
- 在 Endpoint Management 中创建自动化操作以指定对事件、某些设置或用户设备上存在应用程序做出反应。有关信息，请参阅自动化操作。

证书和身份验证

March 16, 2022

在 Endpoint Management 操作期间，若干组件都会参与身份验证：

- **Endpoint Management**： Endpoint Management 服务器是您定义注册安全性和注册体验的位置。用于加入用户的选项包括：
  - 向所有用户开放注册还是仅对收到邀请的用户开放注册。
  - 要求执行双重身份验证还是三重身份验证。Endpoint Management 客户端属性允许您启用 Citrix PIN 身份验证以及配置 PIN 复杂性和过期时间。
- **Citrix Gateway**： Citrix Gateway 为 Micro VPN SSL 会话提供终止服务。Citrix Gateway 还提供网络在途安全，并允许您定义用户每次访问应用程序时的身份验证体验。
- **Secure Hub**：注册期间，Secure Hub 与 Endpoint Management 协同工作。Secure Hub 是设备上可以与 Citrix Gateway 通信的实体：会话过期时，Secure Hub 会从 Citrix Gateway 获取身份验证票证，并将该票证传递给 MDX 应用程序。Citrix 建议使用证书固定，以防范中间人攻击。有关详细信息，请参阅 Secure Hub 文章中的证书固定部分。

  Secure Hub 还有助于使用 MDX 安全容器：Secure Hub 会推送策略，在应用程序超时后与 Citrix Gateway 建立会话，以及定义 MDX 超时和身份验证体验。Secure Hub 还可执行越狱检测、地理定位检查以及您应用的所有策略。
- **MDX** 策略： MDX 策略会在设备上创建数据保管库。MDX 策略会将 Micro VPN 连接引导回 Citrix Gateway，强制执行脱机模式限制，以及强制执行超时等客户端策略。

Citrix Endpoint Management 使用以下身份验证方法对用户进行身份验证以访问其资源：

- 移动设备管理 (MDM)
  - 云托管身份提供程序 (IdP)
  - 轻型目录访问协议 (LDAP)
    - 邀请 URL + PIN
    - 双重身份验证
- 移动应用程序管理 (MAM)
  - LDAP
  - 证书

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 安全令牌
  MAM 身份验证需要使用 Citrix Gateway。

有关其他配置详细信息，请参阅以下文章：

- 上载、更新和续订证书
- Citrix Gateway 和 Endpoint Management
- 域或域加安全令牌身份验证
- 客户端证书或证书加域身份验证
- PKI 实体
- 凭据提供程序
- APNs 证书
- 如果您的站点未启用 Workspace：用于单点登录 Citrix Files 的 SAML
- 通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证
- 通过 Citrix Cloud 使用 Okta 进行身份验证
- 通过 Citrix Cloud 使用本地 Citrix Gateway 进行身份验证
- 要对 Wi-Fi 服务器进行身份验证，请将证书发送到设备：网络设备策略
- 要推送未用于身份验证的唯一证书，例如内部根证书颁发机构 (CA) 证书或特定策略（证书设备策略），请执行以下操作：

证书

Endpoint Management 在安装过程中生成自签名安全套接字层 (SSL) 证书，用于确保与服务器之间的通信流安全。使用知名证书颁发机构发布的可信 SSL 证书替换此 SSL 证书。

Endpoint Management 还使用自己的公钥基础结构 (PKI) 服务或从客户端证书的 CA 获取证书。所有 Citrix 产品均支持通配符和使用者备用名称 (SAN) 证书。对于大多数部署，仅需两个通配符或 SAN 证书。

客户端证书身份验证为移动应用程序提供了一个额外的安全层，允许用户无缝访问 HDX 应用程序。配置了客户端证书身份验证时，用户将键入其 Citrix PIN 以对启用了 Endpoint Management 的应用程序进行单点登录 (SSO) 访问。Citrix PIN 还简化了用户身份验证体验。Citrix PIN 用于确保客户端证书的安全或在设备本地保存 Active Directory 凭据。

要在 Endpoint Management 中注册并管理 iOS 设备，应设置并创建 Apple 提供的 Apple 推送通知服务 (APNs) 证书。有关步骤，请参阅 APNs 证书。

下表显示了每个 Endpoint Management 组件的证书格式和类型：

Endpoint Management 组件	证书格式	必需的证书类型
Citrix Gateway	PEM (BASE64)、PFX (PKCS #12)	SSL、根证书（Citrix Gateway 自动将 PFX 转换为 PEM。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 组件	证书格式	必需的证书类型
Endpoint Management	.p12（在基于 Windows 的计算机上为.pfx）	SSL、SAML、APNs（Endpoint Management 还在安装过程中生成完全 PKI。）重要： Endpoint Management 不支持扩展名为.pem 的证书。要使用.pem 证书，请将.pem 文件拆分为证书和密钥，并将各自导入到 Endpoint Management 中。
StoreFront	PFX (PKCS #12)	SSL、根证书

Endpoint Management 支持位长度为 4096 和 2048 的客户端证书。

对于 Citrix Gateway 和 Endpoint Management，Citrix 建议从公共 CA（如 Verisign、DigiCert 或 Thawte）获取服务器证书。您可以从 Citrix Gateway 或 Endpoint Management 配置实用程序创建证书签名请求 (CSR)。创建 CSR 后，将其提交到 CA 进行签名。CA 返回已签名证书后，即可在 Citrix Gateway 或 Endpoint Management 上安装该证书。

> 重要：
>
> iOS、iPadOS 和 macOS 中的可信证书的要求
>
> Apple 对 TLS 服务器证书有新要求。验证所有证书都符合 Apple 的要求。请参阅 Apple 出版物 https://support.apple.com/en-us/HT210176。
>
> Apple 正在缩短 TLS 服务器证书的最长允许生命周期。此更改仅影响 2020 年 9 月之后颁发的服务器证书。请参阅 Apple 出版物 https://support.apple.com/en-us/HT211025。

LDAP 身份验证

Endpoint Management 支持对一个或多个（与轻型目录访问协议 (LDAP) 兼容的）目录执行基于域的身份验证。LDAP 是一个软件协议，用于提供对与组、用户帐户和相关属性有关的信息的访问权限。有关详细信息，请参阅域或域加安全令牌身份验证。

身份提供程序身份验证

可以通过 Citrix Cloud 配置身份提供程序 (IdP) 以注册和管理用户设备。

IdP 支持的用例：

- Azure Active Directory（通过 Citrix Cloud）
  - Workspace 集成是可选的

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 配置为进行基于证书的身份验证的 Citrix Gateway
  - Android Enterprise（预览版。支持 BYOD、完全托管设备和增强的注册配置文件）
  - iOS（适用于 MDM+MAM 和 MDM 注册）
  - 适用于 Apple 商务管理的 iOS 和 macOS 注册
  - 旧版 Android (DA)

  Apple 校园教务管理等自动注册功能目前不受支持。

- 通过 Citrix Cloud 进行的 Okta

  - Workspace 集成是可选的
  - 配置为进行基于证书的身份验证的 Citrix Gateway
  - Android Enterprise（预览版。支持 BYOD、完全托管设备和增强的注册配置文件）
  - iOS（适用于 MDM+MAM 和 MDM 注册）
  - 适用于 Apple 商务管理的 iOS 和 macOS 注册
  - 旧版 Android (DA)

  Apple 校园教务管理等自动注册功能目前不受支持。

- 本地 Citrix Gateway（通过 Citrix Cloud）

  - 配置为进行基于证书的身份验证的 Citrix Gateway
  - Android Enterprise（预览版。支持 BYOD、完全托管设备和增强的注册配置文件）
  - iOS（适用于 MDM+MAM 和 MDM 注册）
  - 目前不支持 Apple 部署计划等旧版 Android (DA)
    自动注册功能。

上载、更新和续订证书

October 18, 2022

我们建议您列出 Endpoint Management 部署所需的证书。使用该列表可跟踪证书过期日期和密码。本文将帮助您在整个生命期内管理客户端证书。

您的环境中可能包含以下证书：

- Endpoint Management 服务器

  - 用于 MDM FQDN 的 SSL 证书（从 XenMobile Server 迁移到 Endpoint Management 时需要此证书；否则，Citrix 将负责管理此证书）
  - SAML 证书（适用于 Citrix Files）
  - 用于以上证书和任何其他内部资源（StoreFront/代理等）的根证书和中间 CA 证书
  - 用于 iOS 设备管理的 APNs 证书
  - 用于连接到 PKI 的 PKI 用户证书（如果您的环境需要基于证书的身份验证，则需要此证书）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- MDX Toolkit
  - Apple 开发人员证书
  - Apple 预配配置文件（按应用程序）
  - Apple APNs 证书（用于 Citrix Secure Mail）
  - Android 密钥库文件

  MAM SDK 不封装应用程序，因此不需要证书。
- Citrix Gateway
  - 用于 MDM FQDN 的 SSL 证书
  - 用于网关 FQDN 的 SSL 证书
  - 用于 ShareFile SZC FQDN 的 SSL 证书
  - 用于 Exchange 负载平衡（卸载配置）的 SSL 证书
  - 用于 StoreFront 负载平衡的 SSL 证书
  - 用于上述证书的根和中间 CA 证书

> 注意：
>
> 客户端设备必须具有所需的根/中间证书，才能与颁发服务器证书的证书颁发机构建立信任。否则，您可能会收到 SSL 错误 61。要解决此问题，请执行以下操作：
>
> 1. 下载或获取由您的 SSL 证书提供商颁发的 SSL 根/中间证书文件（.crt 或.cer）。通常，根/中间/服务器证书存在于您的 SSL 服务提供商提供的证书包中。
> 2. 在客户端设备上安装根/中间证书。
> 3. 如果客户端设备上安装了防病毒软件，请确保防病毒软件信任证书。

上载证书

您上载的每个证书在证书表中都有一个条目，其中包括其内容摘要。配置需要证书的 PKI 集成组件时，请选择满足该条件的服务器证书。例如，您可能希望将 Endpoint Management 配置为与 Microsoft 证书颁发机构 (CA) 集成。与 Microsoft CA 的连接必须通过使用客户端证书进行身份验证。

Endpoint Management 可能不会处理给定证书的私钥。同样，Endpoint Management 可能不需要上载的证书的私钥。

本节介绍了上载证书的常规过程。有关创建、上载和配置客户端证书的详细信息，请参阅客户端证书或证书加域身份验证。

您有两个用于上载证书的选项：

- 将证书单独上载到控制台。
- 使用 REST API 执行证书的批量上载。此选项仅适用于 iOS 设备。

将证书上载到控制台时，您可以：

- 导入密钥库。然后，您在密钥库存储库中找出要安装的条目，除非您要上载 PKCS #12 格式。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 导入证书。

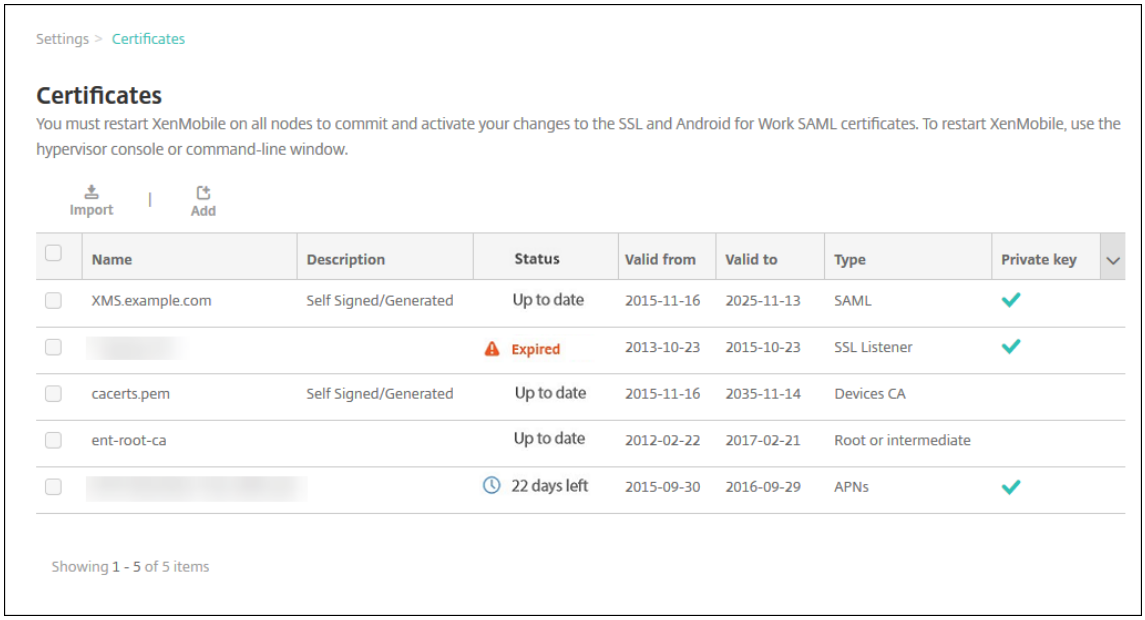
您可以上载 CA 用于对请求进行签名的 CA 证书（不带私钥）。您还可以上载用于客户端身份验证的 SSL 客户端证书（带私钥）

在配置 Microsoft CA 实体时，您指定 CA 证书。您从属于 CA 证书的所有服务器证书列表中选择 CA 证书。同样，配置客户端身份验证时，您可以从包含 Endpoint Management 具有私钥的所有服务器证书的列表中进行选择。

导入密钥库

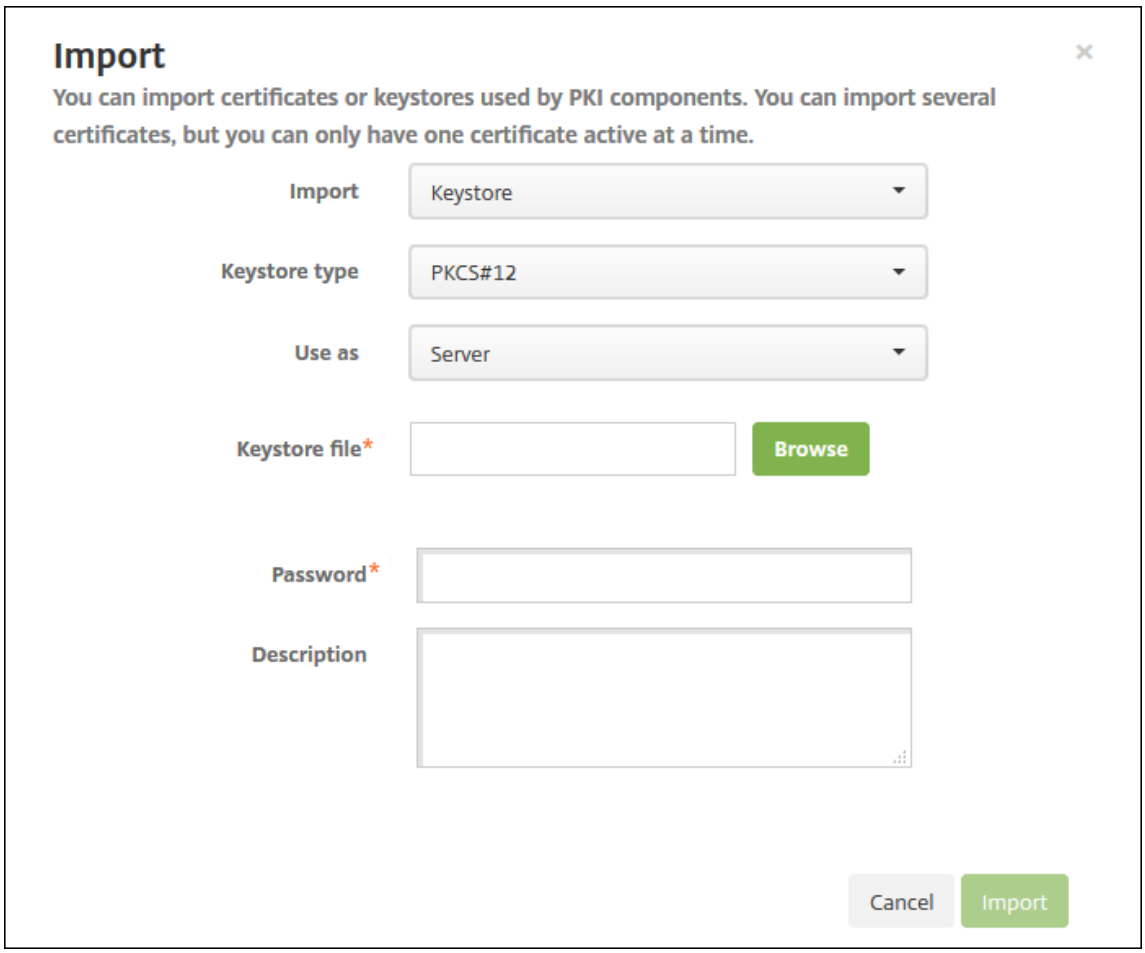
密钥库是安全证书的存储库。按照设计，密钥库可以包含多个条目。从密钥库加载时，必须指定用于识别要加载的条目的条目别名。如果未指定别名，则将加载库中的第一个条目。由于 PKCS #12 文件通常仅包含一个条目，当选择 PKCS #12 作为密钥库类型时，不会显示别名字段。

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。使用搜索栏可查找并打开证书设置。



2. 单击导入。此时将显示导入对话框。
3. 配置以下设置：
    - 导入：选择密钥库。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 密钥库类型：在列表中，单击 **PKCS #12**。
- 用作：在列表中，单击您计划使用证书的方式。可用选项如下：
  - 服务器：服务器证书是 Endpoint Management 功能上使用的证书。将服务器证书上载到 Endpoint Management Web 控制台。这些证书包括 CA 证书、RA 证书以及用于您基础结构其他组件的客户端身份验证的证书。此外，您还可以使用服务器证书来存储您要部署到设备的证书。此用法特别适用于在设备上建立信任所使用的 CA。
  - **SAML**：安全声明标记语言 (SAML) 认证允许您提供对服务器、Web 站点和应用程序的 SSO 访问权限。
  - **APNs**：利用 Apple 提供的 APNs 证书可通过 Apple 推送网络进行移动设备管理。
  - **SSL** 侦听器：安全套接字层 (SSL) 侦听器向 Endpoint Management 通知 SSL 加密活动。
- 密钥库文件：浏览以查找要导入的密钥库。密钥库是一个.p12 或.pfx 文件。选择文件，然后单击打开。
- 密码：键入分配给证书的密码。
- 说明：（可选）键入密钥库的说明，以帮助您将其与其他密钥库区分开。

4. 单击导入。密钥库将添加到证书表中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

导入证书

导入证书时，Endpoint Management 将尝试基于输入内容构建证书链。Endpoint Management 将导入某个链中的所有证书来为每个证书创建一个服务器证书条目。仅当文件或密钥库条目中的证书形成链时，才可执行此操作。证书链中的每个后续证书都必须是前一个证书的颁发者。

您可以为导入的证书添加可选说明。此说明将仅附加到链中的第一个证书上。可在以后更新提醒说明。

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。使用搜索栏可查找并打开证书设置。
2. 在证书页面上，单击导入。此时将显示导入对话框。配置以下设置：
   - 导入：单击证书。
   - 用作：选择您计划使用证书的方式。可用选项如下：
     - 服务器：服务器证书是 Endpoint Management 功能上使用的证书。将服务器证书上载到 Endpoint Management Web 控制台。这些证书包括 CA 证书、RA 证书以及用于您基础结构其他组件的客户端身份验证的证书。此外，您还可以使用服务器证书来存储您要部署到设备的证书。此选项特别适用于在设备上建立信任所使用的 CA。
     - **SAML**：安全声明标记语言 (SAML) 认证允许您提供对服务器、Web 站点和应用程序的单点登录 (SSO) 访问权限。
     - **SSL** 侦听器：安全套接字层 (SSL) 侦听器向 Endpoint Management 通知 SSL 加密活动。
   - 证书导入：浏览以查找要导入的证书。选择文件，然后单击打开。
   - 私钥文件：浏览以查找证书的可选私钥文件。私钥用于与证书一起使用以便进行加密和解密。选择文件，然后单击打开。
   - 说明：键入证书的说明（可选），以帮助您将其与其他证书区分开。
3. 单击导入。证书将添加到证书表中。

使用 **REST API** 批量上载证书

有时一次上载一个证书并不合理。在这些情况下，请使用 REST API 执行证书的批量上载。此方法支持.p12 格式的证书。有关 REST API 的详细信息，请参阅 REST API。

1. 以 `device_identity_value.p12` 格式重命名每个证书文件。`device_identity_value` 可以是每个设备的 IMEI、序列号或 MEID。

   例如，您选择使用序列号作为标识方法。一台设备具有序列号 `A12BC3D4EFGH`，因此将您希望在该设备上安装的证书文件命名为 `A12BC3D4EFGH.p12`。

2. 创建一个文本文件以存储.p12 证书的密码。在该文件中，在新行中键入每个设备的设备标识符和密码。使用格式 `device_identity_value=password`。请参阅以下内容：

```
A12BC3D4EFGH.p12=password1!
A12BC3D4EFIJ.p12=password2@
A12BC3D4EFKL.p12=password3#
<!--NeedCopy-->
```

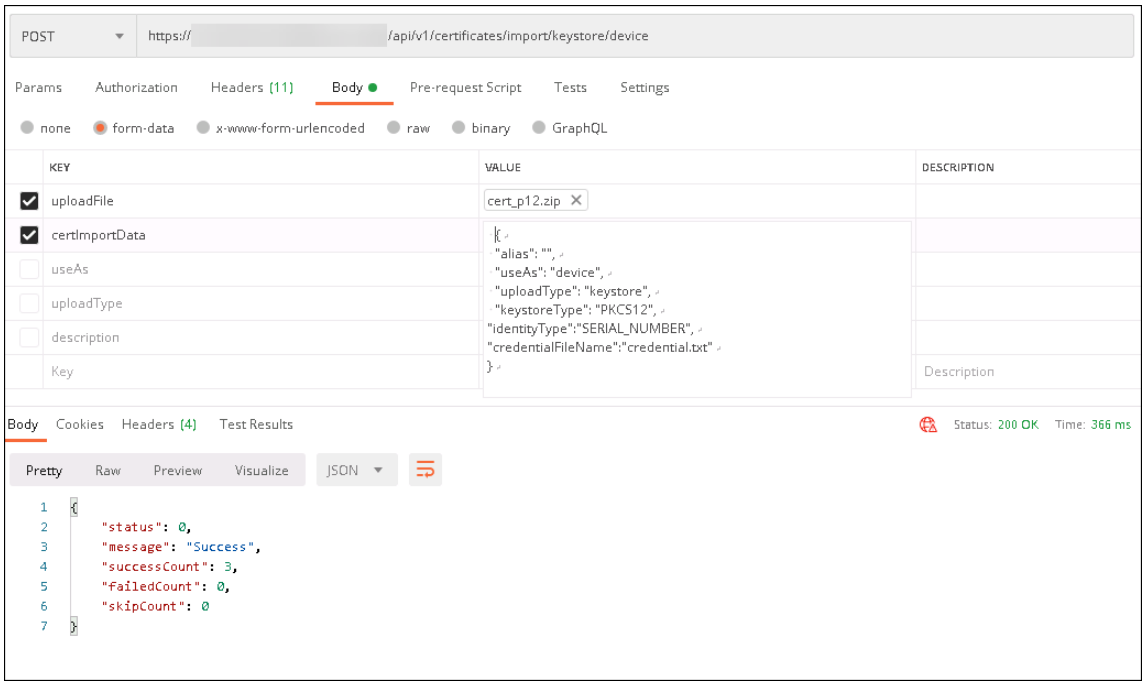
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 将所有证书和您创建的文本文件打包到.zip 文件中。
4. 启动 REST API 客户端，登录 Endpoint Management，然后获取身份验证令牌。
5. 导入您的证书，确保您将以下内容放入消息正文中：

```
{

    "alias": "",
    "useAs": "device",
    "uploadType": "keystore",
    "keystoreType": "PKCS12",
    "identityType":"SERIAL_NUMBER",         # identity type can be
       "SERIAL_NUMBER","IMEI","MEID"
    "credentialFileName":"credential.txt"    # The credential file
       name in .zip
 }

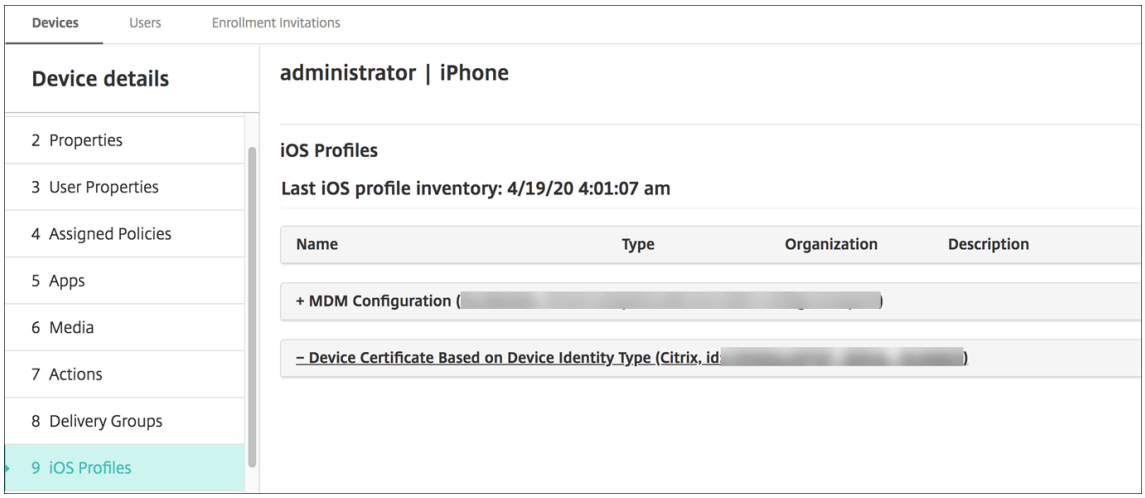
<!--NeedCopy-->
```



6. 使用凭据类型 **Always on IKEv2**（始终启用 IKEv2）和设备身份验证方法基于设备标识的设备证书创建 VPN 策略。选择您的证书文件名中使用的设备标识类型。请参阅 VPN 设备策略。
7. 注册 iOS 设备并等待部署 VPN 策略。通过检查设备上的 MDM 配置来确认证书安装。还可以在 Endpoint Management 控制台中检查设备详细信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.





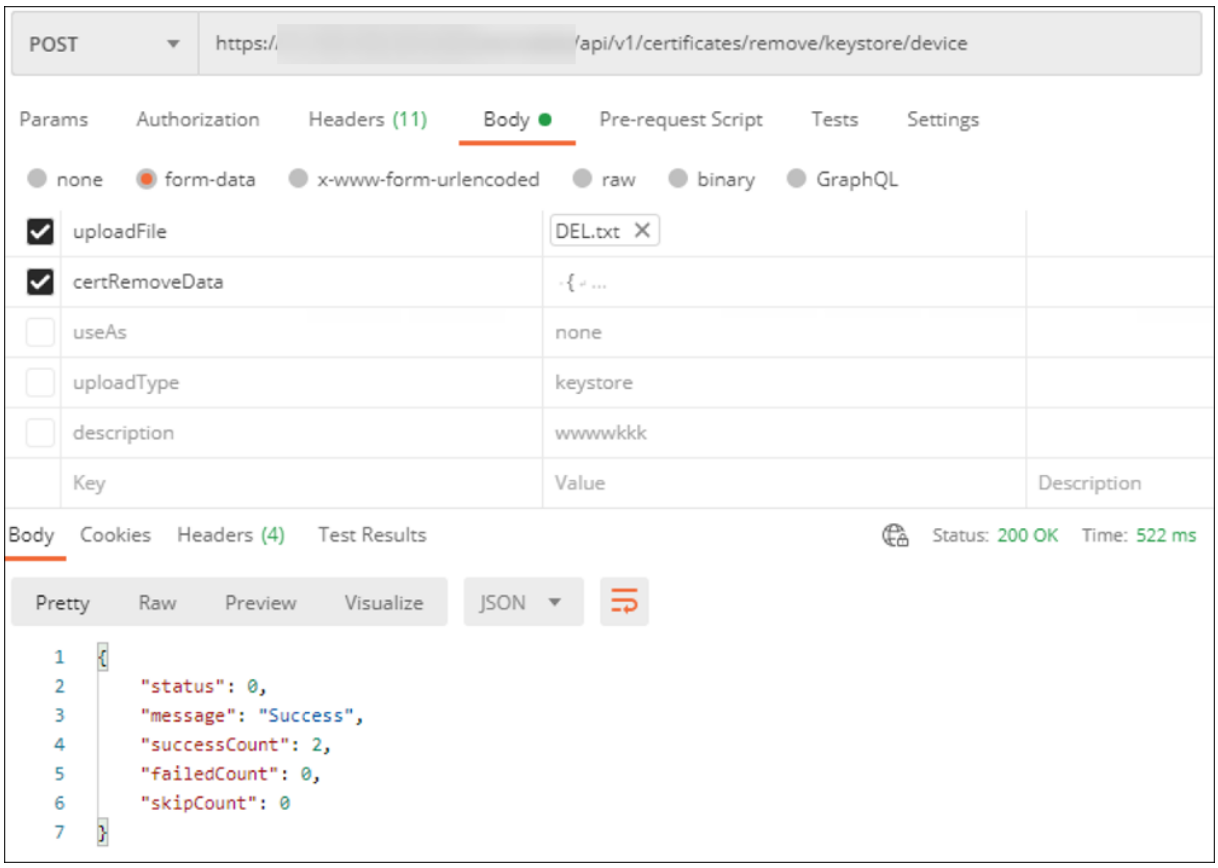
还可以通过创建一个包含为每个要删除的证书列出的 `device_identity_value` 的文本文件来批量删除证书。在 REST API 中，调用删除 API 并使用以下请求，将 `device_identity_value` 替换为适当的标识符：

```
```
{

    "identityType"="device_identity_value"
 }

<!--NeedCopy--> ```
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved. 
```



更新证书

Endpoint Management 只允许系统中每个公钥一次存在一个证书。如果尝试为已导入证书的同一密钥对导入证书，您可以：

- 替换现有条目。
- 删除条目。

上载新证书以替换旧证书后，无法删除旧证书。配置 PKI 实体设置时，两个证书都存在于 **SSL** 客户端证书菜单中。列表中较新的证书位于旧证书下方。

更新证书

1. 按照客户端证书或证书加域身份验证中的步骤创建替换证书。

   > 重要：
   >
   > 请勿使用该选项创建使用现有私钥的证书。创建证书以更新过期证书时，私钥也必须是新的。

2. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。使用搜索栏可查找并打开证书设置。
3. 在导入对话框中，导入新证书。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

当更新服务器证书时，使用先前证书的组件将自动切换到使用新证书。同样，如果已经在设备上部署服务器证书，证书将在下一次部署时自动更新。

要更新 APNs 证书，请执行创建证书的步骤，然后转到 Apple Push Certificates Portal。有关详细信息，请参阅续订 APNs 证书。

如果您的 Citrix Gateway 设置为进行 SSL 卸载，请确保使用新的 cacert.pem 来更新您的负载平衡器。

> 注意：
>
> 如果您已从 XenMobile 本地迁移到 Endpoint Management，并且正在更新证书，请在完成上述步骤后与 Citrix 支持部门联系。您需要向他们提供新证书的副本（PFX 格式），包括证书密码。Citrix 支持将更新云端 NetScaler 并重启租户节点以完成证书更新过程。

更新 **PKI** 服务证书颁发机构 **(CA)**

可以请求 Citrix Cloud Operations 团队在您的 Endpoint Management 部署中刷新或重新生成内部 PKI 证书颁发机构 (CA)。为这些请求打开一个技术支持案例。

```
When the new CAs are available, Cloud Operations lets you know that you
    can proceed with renewing the device certificates for your users.
```

续订设备证书

如果设备上的证书过期，证书将变得无效。您不能再在您的环境中运行安全事务，也不能访问 Endpoint Management 资源。证书颁发机构 (CA) 会在过期日期之前提示您续订 SSL 证书。执行上述步骤以更新证书，然后在已注册的设备上启动证书续订。

对于受支持的 iOS、macOS 和 Android 设备，可以通过安全操作（证书续订）启动证书续订。可以从 Endpoint Management 控制台或公用 REST API 续订设备证书。对于注册的 Windows 设备，用户必须重新注册其设备才能接收新的设备证书颁发机构 (CA)。

下次设备连接回 Endpoint Management 时，Endpoint Management 服务器会根据新 CA 颁发新的设备证书。

使用控制台续订设备证书

1. 转到管理 **>** 设备，然后选择要为其续订设备证书的设备。
2. 单击安全，然后单击证书续订。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

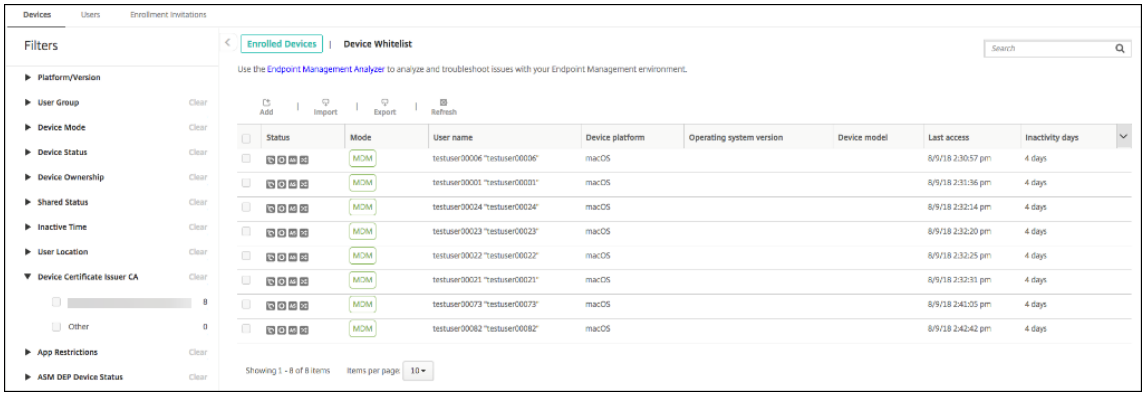


已注册的设备继续运行而不会中断。Endpoint Management 在设备重新连接到服务器时颁发设备证书。

要查询特定设备证书颁发者 CA 组中的设备，请执行以下操作：

1. 在管理 **>** 设备中，展开过滤器窗格。
2. 在过滤器窗格中，展开设备证书颁发者 **CA**，然后选择要续订的颁发者 CA。

   在设备表中，将显示所选颁发者 CA 的设备。



使用 **REST API** 续订设备证书

Endpoint Management 在内部将以下证书颁发机构 (CA) 用于 PKI：根 CA、设备 CA、服务器 CA。这些 CA 是一个逻辑组并具有组名称。在 Endpoint Management 预配过程中，服务器会生成三个 CA，并为其指定组名称 “default”。

CA 颁发以下 API 来管理和续订设备证书。已注册的设备继续运行而不会中断。Endpoint Management 在设备重新连接到服务器时颁发设备证书。有关详细信息，请下载 Public API for REST Services（用于 REST 服务的公共 API）PDF。

- 返回仍在使用旧 CA 的设备的列表（请参阅 “适用于 REST 的公共 API 服务”PDF 中的第 3.16.2 节）
- 续订设备证书（请参阅第 3.16.58 节）
- 获取所有 CA 组（请参阅第 3.23.1 节）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用于 **Citrix Secure Mail** 的 **APNs** 证书

Apple 推送通知服务 (APNs) 证书每年都会过期。请务必在 APNs SSL 证书过期之前创建该证书，并在 Citrix 门户中进行更新。如果证书过期，用户会面临 Secure Mail 推送通知不一致的情况。此外，您不能再为您的应用程序发送推送通知。

用于 **iOS** 设备管理的 **APNs** 证书

要在 Endpoint Management 中注册和管理 iOS 设备，应设置和创建 Apple 提供的 APNs 证书。如果证书过期，用户将不能在 Endpoint Management 中注册，而您不能管理其 iOS 设备。有关详细信息，请参阅 APNs 证书。

可以通过登录 Apple Push Certificates Portal 来查看 APNs 证书状态和过期日期。请务必以创建证书的同一用户身份登录。

在过期日期之前 30 天和 10 天，您还会收到 Apple 发送的电子邮件通知。通知包含以下信息：

```
The following Apple Push Notification Service certificate, created for
    Apple ID CustomerID will expire on Date. Revoking or allowing this
    certificate to expire will require existing devices to be re-
    enrolled with a new push certificate.

Please contact your vendor to generate a new request (a signed CSR),
    then visit https://identity.apple.com/pushcert to renew your Apple
    Push Notification Service certificate.

Thank You,

Apple Push Notification Service
<!--NeedCopy-->
```

MDX Toolkit（**iOS** 分发证书）

在物理 iOS 设备上运行的应用程序（Apple App Store 中的应用程序除外）具有以下签名要求：

- 使用预配配置文件为应用程序签名。
- 使用相应的分发证书为应用程序签名。

要验证您的 iOS 分发证书是否有效，请执行以下操作：

1. 从 Apple 企业开发人员门户中，为您计划用 MDX 封装的每个应用程序创建一个显式应用程序 ID。可接受的应用程序 ID 示例：`com.CompanyName.ProductName`.
2. 从 Apple 企业开发人员门户中，转到 **Provisioning Profiles**（预配配置文件）**> Distribution**（分发），并创建一个内部预配配置文件。对在上一步中创建的每个应用程序 ID 重复此步骤。
3. 下载所有预配配置文件。有关详细信息，请参阅封装 iOS 移动应用程序。

要确认所有 Endpoint Management 服务器证书是否有效，请执行以下操作：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在 Endpoint Management 控制台中，单击设置 **>** 证书。
2. 检查包括 APNs、SSL 侦听器、根和中间证书在内的所有证书是否有效。

Android 密钥库

密钥库是指包含用于为您的 Android 应用程序签名的证书的文件。当您的密钥有效期过期后，用户不能再无缝地升级到应用程序的新版本。

Citrix Gateway

有关如何处理 Citrix Gateway 的证书过期的详细信息，请参阅 Citrix 支持知识中心中的 How to handle certificate expiry on NetScaler（如何处理 NetScaler 的证书过期）。

如果 Citrix Gateway 证书过期，用户将无法注册和访问应用商店。过期的证书还会阻止用户使用 Secure Mail 时连接到 Exchange Server。此外，用户不能枚举和打开 HDX 应用程序（具体取决于哪个证书过期）。

Expiry Monitor 和 Command Center 可以帮助您跟踪 Citrix Gateway 证书。Center 会在证书过期时通知您。这些工具可以协助监视以下 Citrix Gateway 证书：

- 用于 MDM FQDN 的 SSL 证书
- 用于网关 FQDN 的 SSL 证书
- 用于 ShareFile SZC FQDN 的 SSL 证书
- 用于 Exchange 负载平衡（卸载配置）的 SSL 证书
- 用于 StoreFront 负载平衡的 SSL 证书
- 用于上述证书的根和中间 CA 证书

Citrix Gateway 和 Endpoint Management

December 3, 2021

与 Endpoint Management 集成后，Citrix Gateway 可提供对您的内部网络和资源的远程设备访问。Endpoint Management 在设备上的应用程序与 Citrix Gateway 之间创建一个 Micro VPN。

可以使用 Citrix Gateway 服务（预览版）或本地 Citrix Gateway（又称为 NetScaler Gateway）。有关两种 Citrix Gateway 解决方案的概述，请参阅将 Citrix Gateway 与 Endpoint Management 结合使用。

配置身份验证以便远程设备能够访问内部网络

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **Citrix Gateway**。此时将显示 **Citrix Gateway** 页面。在以下示例中，存在一个 Citrix Gateway 实例。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

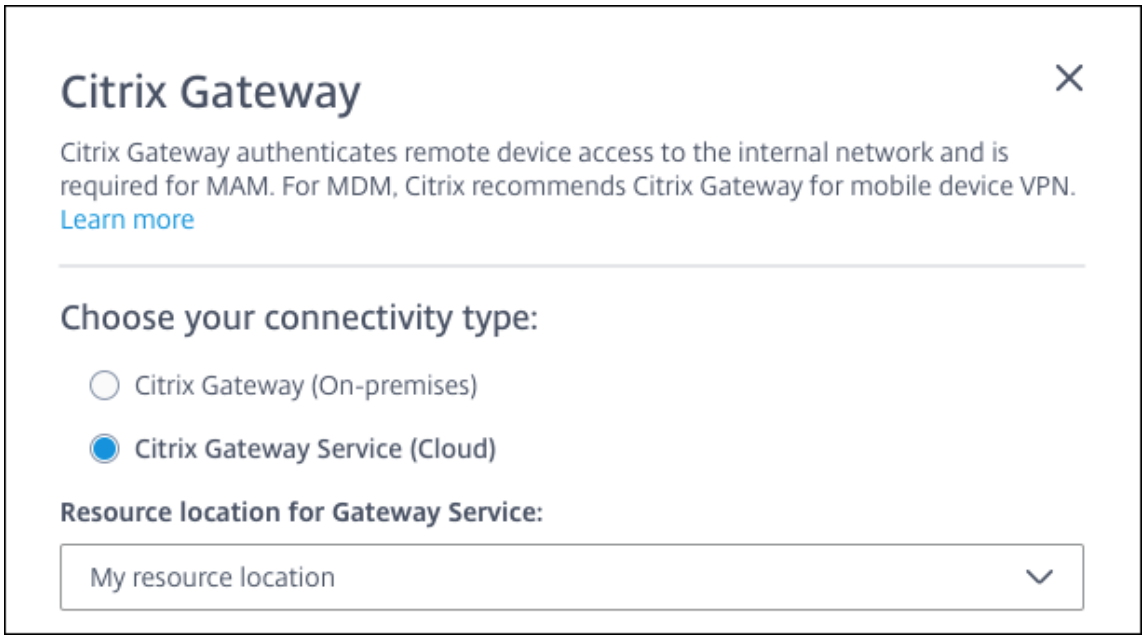


3. 配置以下设置：
   - 身份验证：选择是否启用身份验证。默认值为开。
   - 向用户提供用于身份验证的证书：选择是否希望 Endpoint Management 与 Secure Hub 共享身份验证证书。共享证书使 Citrix Gateway 能够处理客户端证书身份验证。默认值为关。
   - 凭据提供程序：在列表中，单击要使用的凭据提供程序。有关更多信息，请参阅 凭证提供程序。
4. 单击保存。

添加 **Citrix Gateway** 服务实例（预览版）

保存身份验证设置后，请向 Endpoint Management 中添加一个 Citrix Gateway 实例。

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将打开设置页面。
2. 在 设置页面上，滚动到 Citrix Gateway 磁贴，然后单击 开始安装程序。此时将显示 **Citrix Gateway** 页面。
3. 选择 **Citrix Gateway service (cloud)**（Citrix Gateway 服务 (云)）并指定网关服务的资源位置。



   - **Resource location for Gateway service**（网关服务的资源位置）：如果您使用的是 Secure Mail，此选项为必填项。指定 STA 服务的资源位置。资源位置必须包括已配置的 Citrix Gateway。如果稍后要删除为网关服务配置的资源位置，请更新此设置。

   完成这些设置后，单击连接以建立连接。新 Citrix Gateway 已添加。**Citrix Gateway service (cloud)**（Citrix Gateway 服务 (云)）磁贴将显示在设置页面上。要编辑实例，请单击查看更多。如果网关连接器在所选资源位置中不可用，请单击 **Add Gateway Connector**（添加网关连接器）。按照屏幕上的指导安装网关连接器。也可以稍后添加网关连接器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

4. 单击 **Save and Export Script**（保存并导出脚本）。

   - **Save and Export Script**（保存并导出脚本）。单击按钮保存您的设置并导出配置捆绑包。可以将脚本从捆绑包上载到 Citrix Gateway，以便使用 Endpoint Management 设置对其进行配置。有关信息，请参阅这些步骤后面的 “配置本地 Citrix Gateway 以与 Endpoint Management 配合使用”。

   您已添加新 Citrix Gateway。**Citrix Gateway** 磁贴将显示在设置页面上。要编辑实例，请单击查看更多。

将本地 **Citrix Gateway** 配置为与 **Endpoint Management** 结合使用

要配置本地 Citrix Gateway 以与 Endpoint Management 配合使用，请执行下面各部分中详细介绍的以下常规步骤：

1. 确认您的环境是否满足必备条件。
2. 从 Endpoint Management 控制台导出脚本捆绑包。
3. 从捆绑包中提取文件。如果您仅在 Citrix Gateway 上使用经典策略，并且运行的是 Citrix ADC 13.0 或更早版本，请在文件名中使用带 “Classic” 的脚本。如果您正在使用任何高级策略或者运行 Citrix ADC 13.1 或更高版本，请在文件名中使用带 “Advanced” 的脚本。
4. 在 Citrix Gateway 上运行相应的脚本。请参阅脚本附带的自述文件了解最新的详细说明。
5. 测试配置。

这些脚本配置 Endpoint Management 所需的以下 Citrix Gateway 设置：

- MDM 和 MAM 需要的 Citrix Gateway 虚拟服务器
- Citrix Gateway 虚拟服务器的会话策略
- Endpoint Management 服务器详细信息
- 用于证书验证的代理负载平衡器
- Citrix Gateway 虚拟服务器的身份验证策略和操作。这些脚本描述了 LDAP 配置设置。
- 代理服务器的流量操作和策略
- 无客户端访问配置文件
- Citrix Gateway 上的静态本地 DNS 记录
- 其他绑定：服务策略、CA 证书

这些脚本不处理以下配置：

- Exchange 负载平衡
- Citrix Files 负载平衡
- ICA 代理配置
- SSL 卸载

使用 **Citrix Gateway** 配置脚本的必备条件

Endpoint Management 要求：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 请先完成 Endpoint Management 中的 LDAP 和 Citrix Gateway 配置，然后再导出脚本捆绑包。如果更改设置，请再次导出脚本捆绑包。

Citrix Gateway 要求：

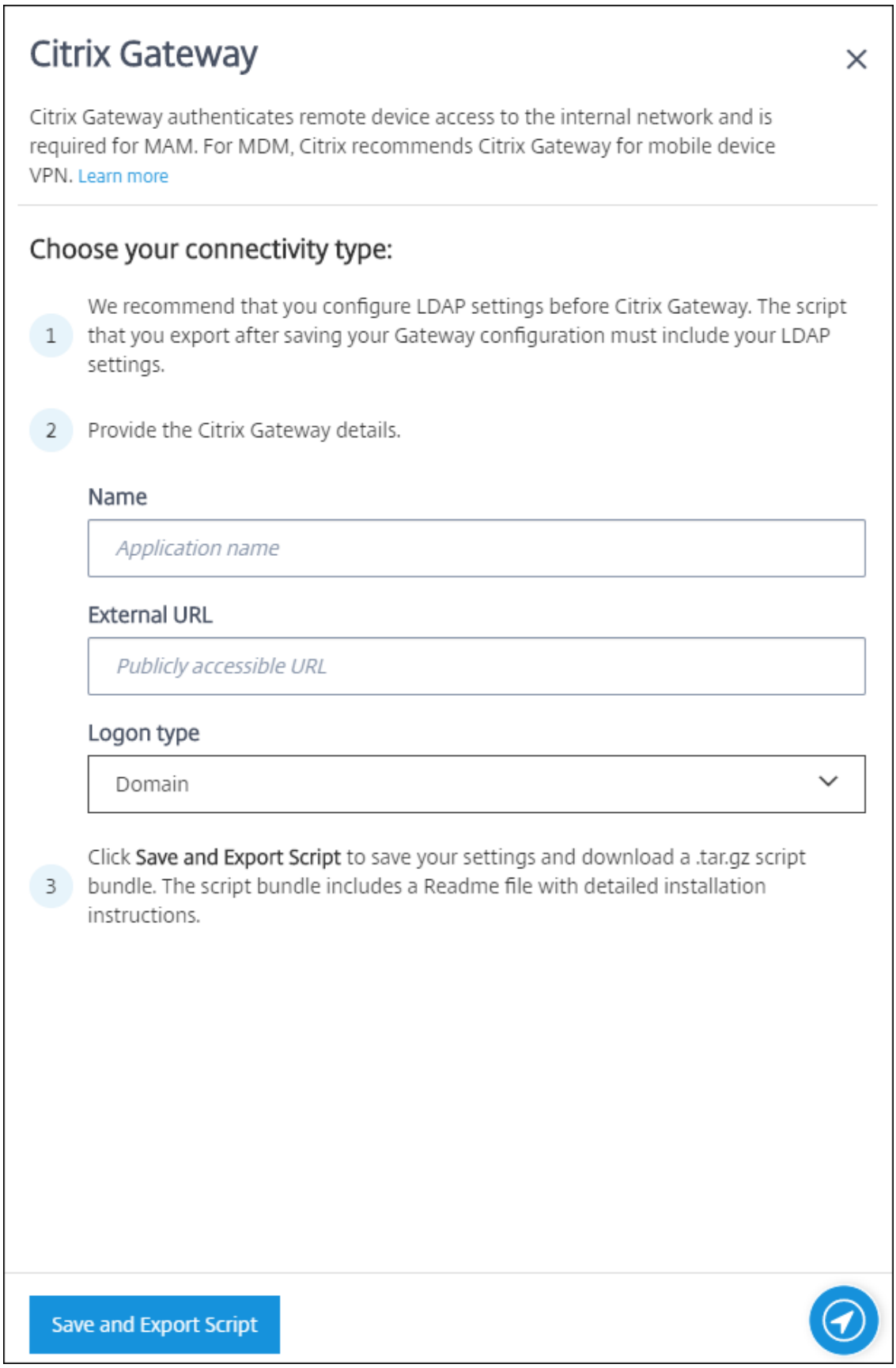
- 在 Citrix Gateway 上使用基于证书的身份验证时，必须在 Citrix ADC 设备上创建 SSL 证书。请参阅在 Citrix ADC 设备上创建和使用 SSL 证书。
- Citrix Gateway（最低版本 11.0，内部版本号 70.12）。
- Citrix Gateway IP 地址已配置并且连接到 LDAP 服务器（平衡了 LDAP 的负载时除外）。
- Citrix Gateway 子网 (SNIP) IP 地址已配置，连接到必需的后端服务器，并且能够通过端口 8443/TCP 访问公用网络。
- DNS 可以解析公共域。
- Citrix Gateway 已通过平台/通用许可证或试用版许可证获得许可。有关信息，请参阅 https://support.citrix.com/article/CTX126049。

从 **Endpoint Management** 中导出脚本包

保存身份验证设置后，请向 Endpoint Management 中添加一个 Citrix Gateway 实例。

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将打开设置页面。
2. 在 设置页面上，滚动到 Citrix Gateway 磁贴，然后单击 开始安装程序。此时将显示 **Citrix Gateway** 页面。
3. 选择 **Citrix Gateway (**本地**)** 并配置以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 名称：键入 Citrix Gateway 实例的名称。
- 外部 **URL**：键入 Citrix Gateway 的可公开访问的 URL。例如，`https://receiver.com`。
- 登录类型：选择登录类型。类型包括域、仅限安全令牌、域和安全令牌、证书、证书和域以及证书和安全令牌。默认值为域。

如果您有多个域，请使用证书和域。有关详细信息，请参阅为多个域配置身份验证。

Citrix Gateway 上的基于证书的身份验证需要额外的配置。例如，必须将根 CA 证书上载到您的 Citrix ADC 设备。请参阅在 Citrix ADC 设备上创建和使用 SSL 证书。

有关详细信息，请参阅部署手册中的身份验证。

4. 单击 **Save and Export Script**（保存并导出脚本）。
   - **Save and Export Script**（保存并导出脚本）。单击按钮保存您的设置并导出配置捆绑包。可以将脚本从捆绑包上载到 Citrix Gateway，以便使用 Endpoint Management 设置对其进行配置。有关信息，请参阅这些步骤后面的 “配置本地 Citrix Gateway 以与 Endpoint Management 配合使用”。

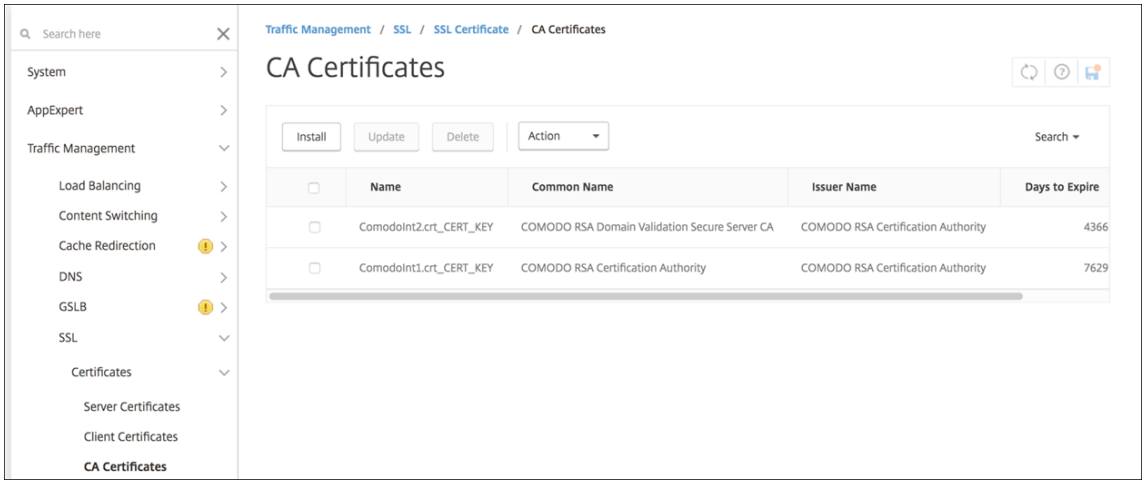
   您已添加新 Citrix Gateway。**Citrix Gateway** 磁贴将显示在设置页面上。要编辑实例，请单击查看更多。

在您的环境中安装脚本

脚本包中包括以下内容。

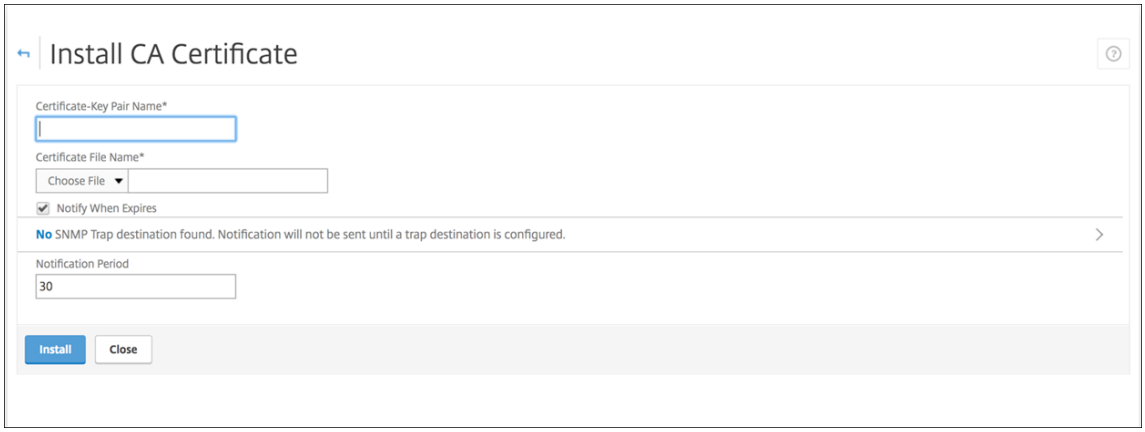
- 包含详细说明的 readme 文件
- 包含用于在 NetScaler 中配置所需组件的 NetScaler CLI 命令的脚本
- 公用根 CA 证书和中间 CA 证书
- 包含用于删除 NetScaler 配置的 NetScaler CLI 命令的脚本

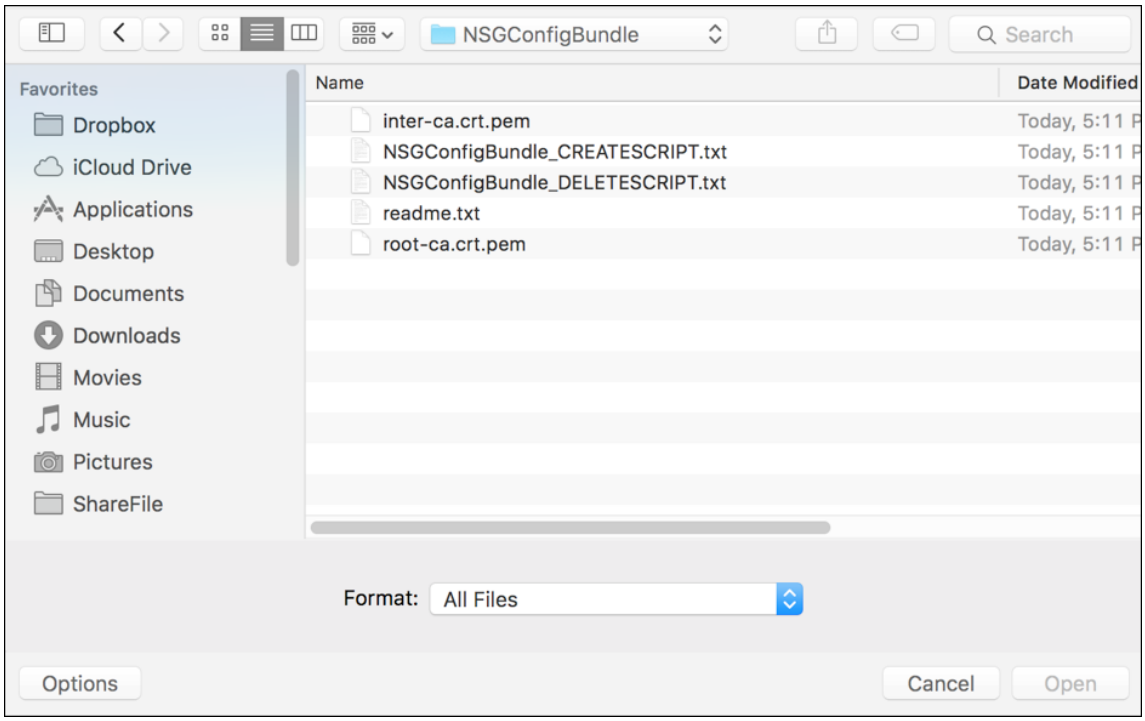
1. 将证书文件（在脚本包中提供）上载并安装在 Citrix ADC 设备上的 /nsconfig/ssl/ 目录中。请参阅在 Citrix ADC 设备上创建和使用 SSL 证书。

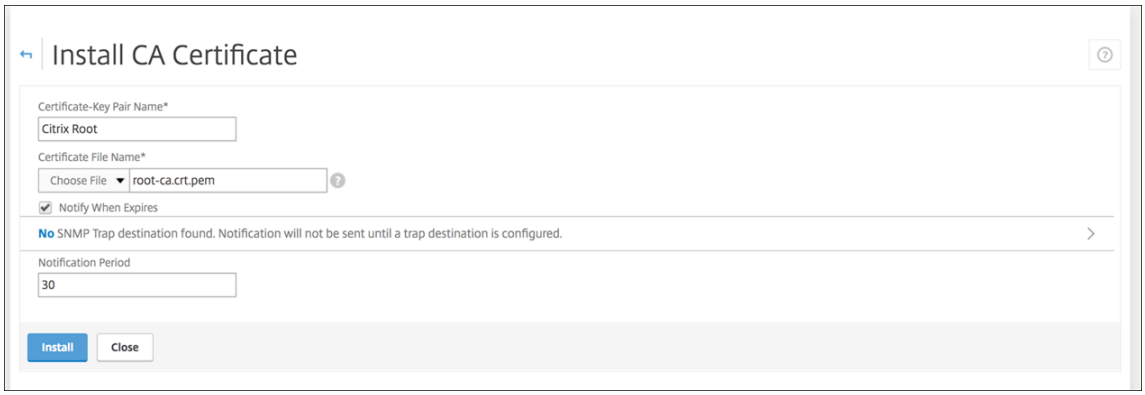


以下示例显示了如何安装根证书。

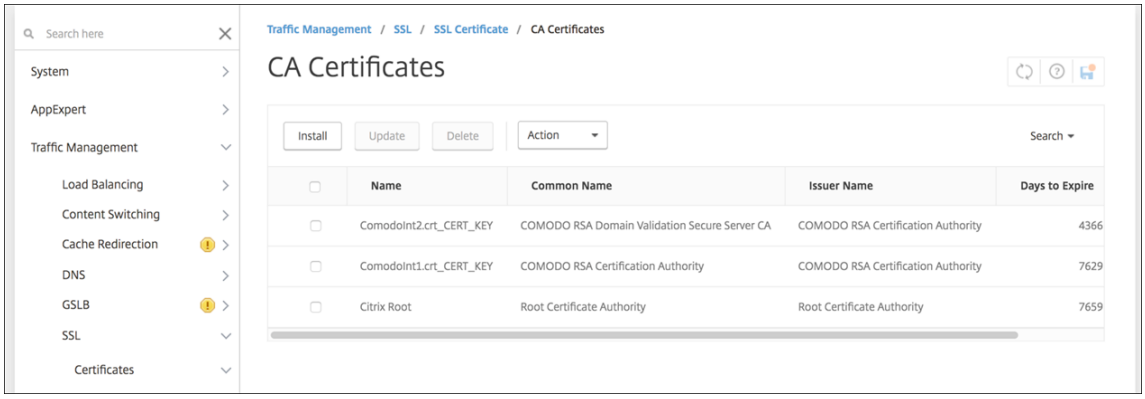
© 1999–2023 Cloud Software Group, Inc. All rights reserved.







© 1999–2023 Cloud Software Group, Inc. All rights reserved.



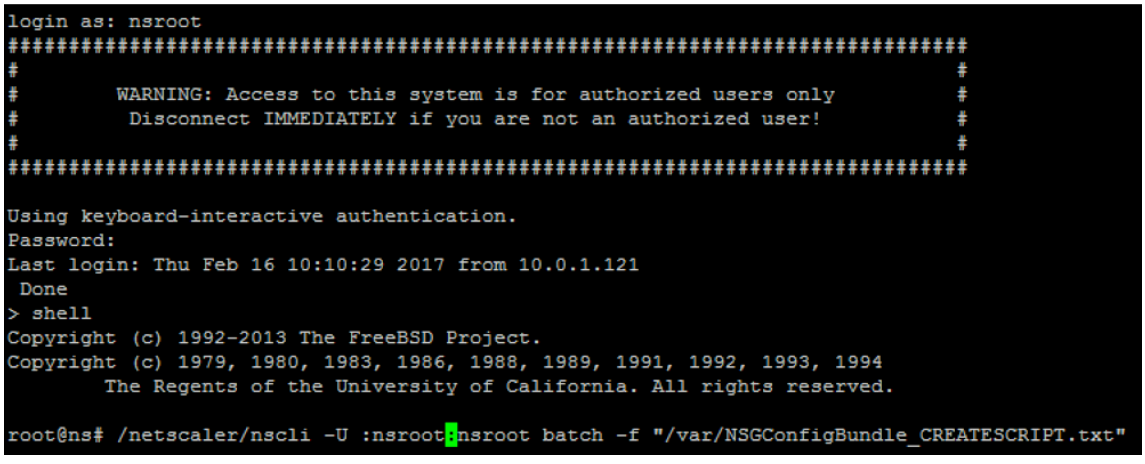
请务必同时安装根证书和中间证书。

2. 编辑脚本(ConfigureCitrixGatewayScript_Classic.txt 或 ConfigureCitrixGatewayScript_Advanced.txt)，以便用环境中的详细信息替换所有占位符。

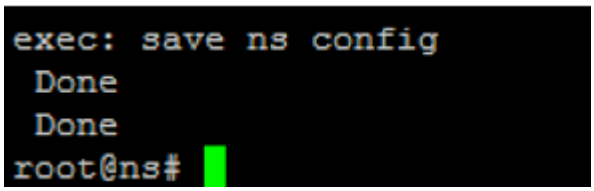
```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. 按照脚本包附带的自述文件所述，在 NetScaler bash shell 中运行编辑后的脚本。例如：

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/OfflineNSGConfigtBundle_CREATESCRIPT.txt"
```



脚本完成后，将显示以下行。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

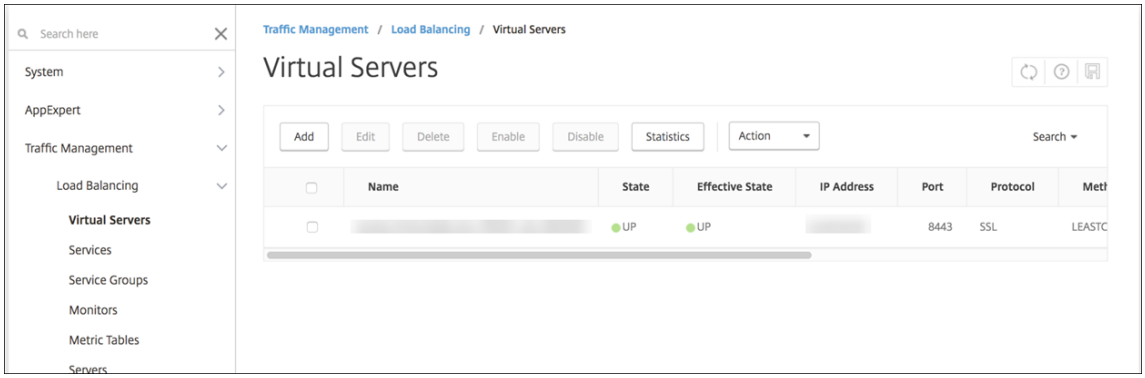
测试配置

要验证配置，请执行以下操作：

1. 验证 Citrix Gateway 虚拟服务器显示的状态是否为运行。



2. 验证代理负载平衡虚拟服务器显示的状态是否为运行。



3. 打开 Web 浏览器，连接到 Citrix Gateway URL，并尝试进行身份验证。如果身份验证成功，您将被重定向到“HTTP 状态 404 - 未找到”消息。
4. 注册设备，并确保其获取 MDM 和 MAM 注册。

为多个域配置身份验证

如果您有多个 Endpoint Management 实例（例如，用于测试、开发和生产环境），请手动为其他环境配置 Citrix Gateway。（只能运行一次 NetScaler for XenMobile 向导。）

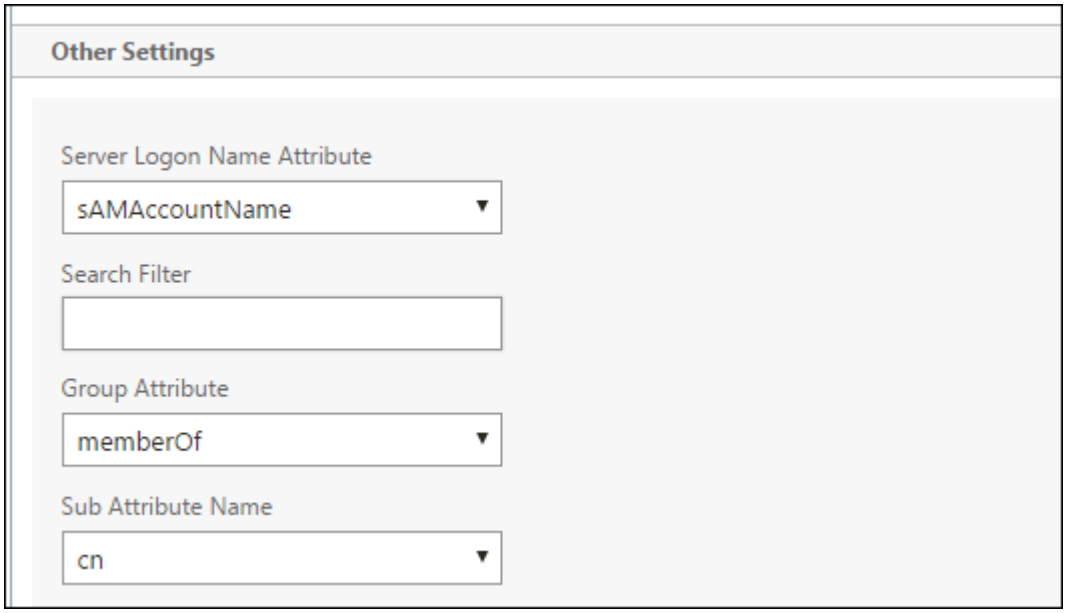
Citrix Gateway 配置

要为多域环境配置 Citrix Gateway 身份验证策略和会话策略，请执行以下操作：

1. 在 Citrix Gateway 配置实用程序中的配置选项卡上，展开 **Citrix Gateway >** 策略 **>** 身份验证。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 在导航窗格中，单击 **LDAP**。
3. 单击后即可编辑 LDAP 配置文件。将服务器登录名称属性更改为 **userPrincipalName** 或您想要用于执行搜索操作的属性。记下您指定的属性。在 Endpoint Management 控制台中配置 LDAP 设置时，请提供该属性。

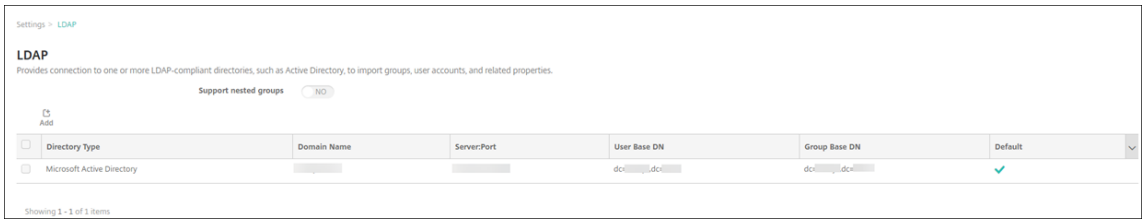


4. 针对每个 LDAP 策略重复以上步骤。每个域均需要一个单独的 LDAP 策略。
5. 在绑定到 Citrix Gateway 虚拟服务器的会话策略中，导航到编辑会话配置文件 **>** 已发布的应用程序。请确保单点登录域为空。

Endpoint Management 配置

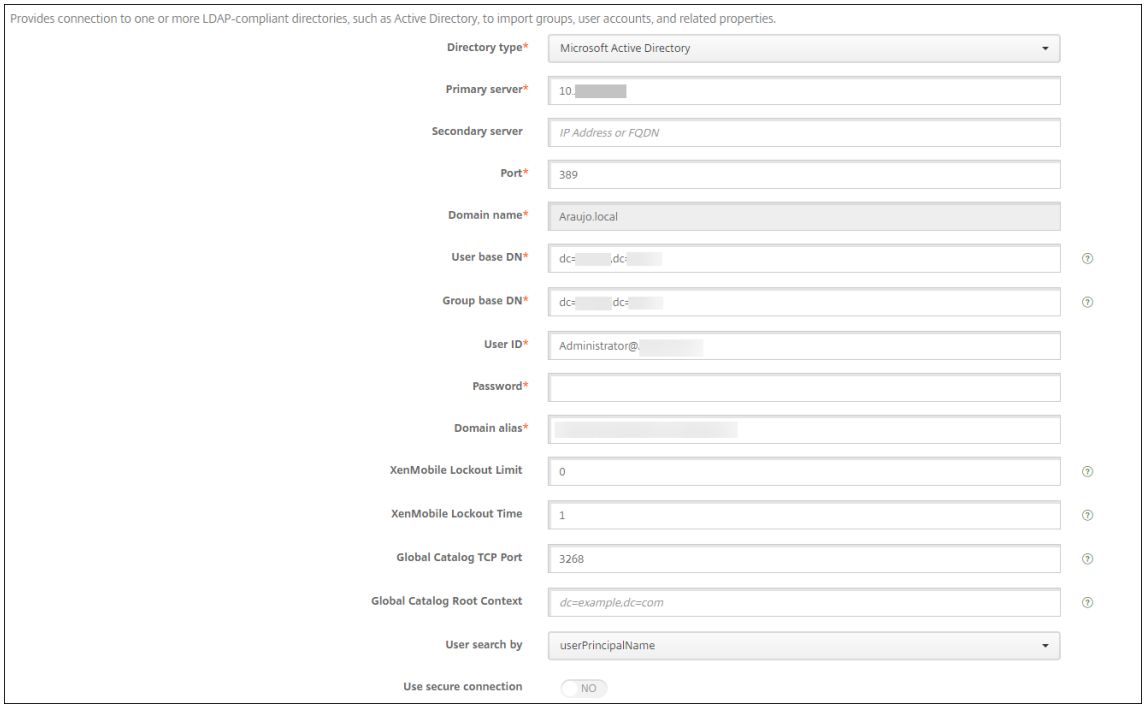
要为多域环境配置 Endpoint Management LDAP，请执行以下操作：

1. 在 Endpoint Management 控制台中，转至设置 **> LDAP** 并添加或编辑一个目录。



2. 提供相关信息。
   - 在域别名中，指定要用于执行用户身份验证的每个域。用逗号分隔这些域，并且在域之间不要使用空格。例如：domain1.com,domain2.com,domain3.com
   - 请确保用户搜索依据字段与在 Citrix Gateway LDAP 策略中指定的服务器登录名称属性保持一致。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



删除对特定 **URL** 的入站连接请求

如果您的环境中的 Citrix Gateway 是为 SSL 卸载配置的，您可能希望网关删除对特定 URL 的入站连接请求。如果您更喜欢这种额外的安全性，请联系 Citrix Cloud Operations 部门，并请求他们允许将您的 IP 添加到您的本地数据中心白。

域或域加安全令牌身份验证

December 3, 2021

Endpoint Management 支持对一个或多个（与轻型目录访问协议 (LDAP) 兼容的）目录执行基于域的身份验证。可以在 Endpoint Management 中配置到一个或多个目录的连接。Endpoint Management 使用 LDAP 配置导入组、用户帐户和相关属性。

> 重要提示：
>
> 用户在 Endpoint Management 中注册设备后，Endpoint Management 不支持将身份验证模式从一种身份验证模式更改为其他身份验证模式。例如，在用户注册后，您无法将身份验证模式从 域身份验证更改为域 + 证书。

关于 **LDAP**

LDAP 是一个独立于供应商的开源应用程序协议，用于通过 Internet 协议 (IP) 网络访问和维护分布式目录信息服务。目录信息服务用于共享通过网络可用的用户、系统、网络、服务和应用程序信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

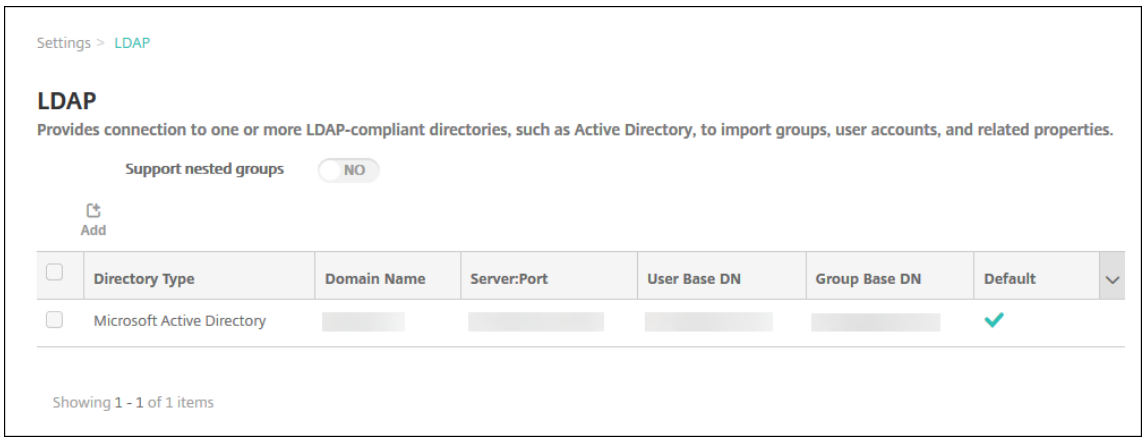
LDAP 的常见用处是为用户提供单点登录 (SSO)，即每个用户在多项服务之间共享一个密码。通过单点登录，用户登录一次公司 Web 站点，可对公司 Intranet 进行经过身份验证访问。

客户端通过连接到 LDAP 服务器（称为目录系统代理程序 (Directory System Agent, DSA)）启动 LDAP 会话。然后，客户端向服务器发送操作请求，服务器通过相应的身份验证进行响应。

在 **Endpoint Management** 中添加或编辑 **LDAP** 连接

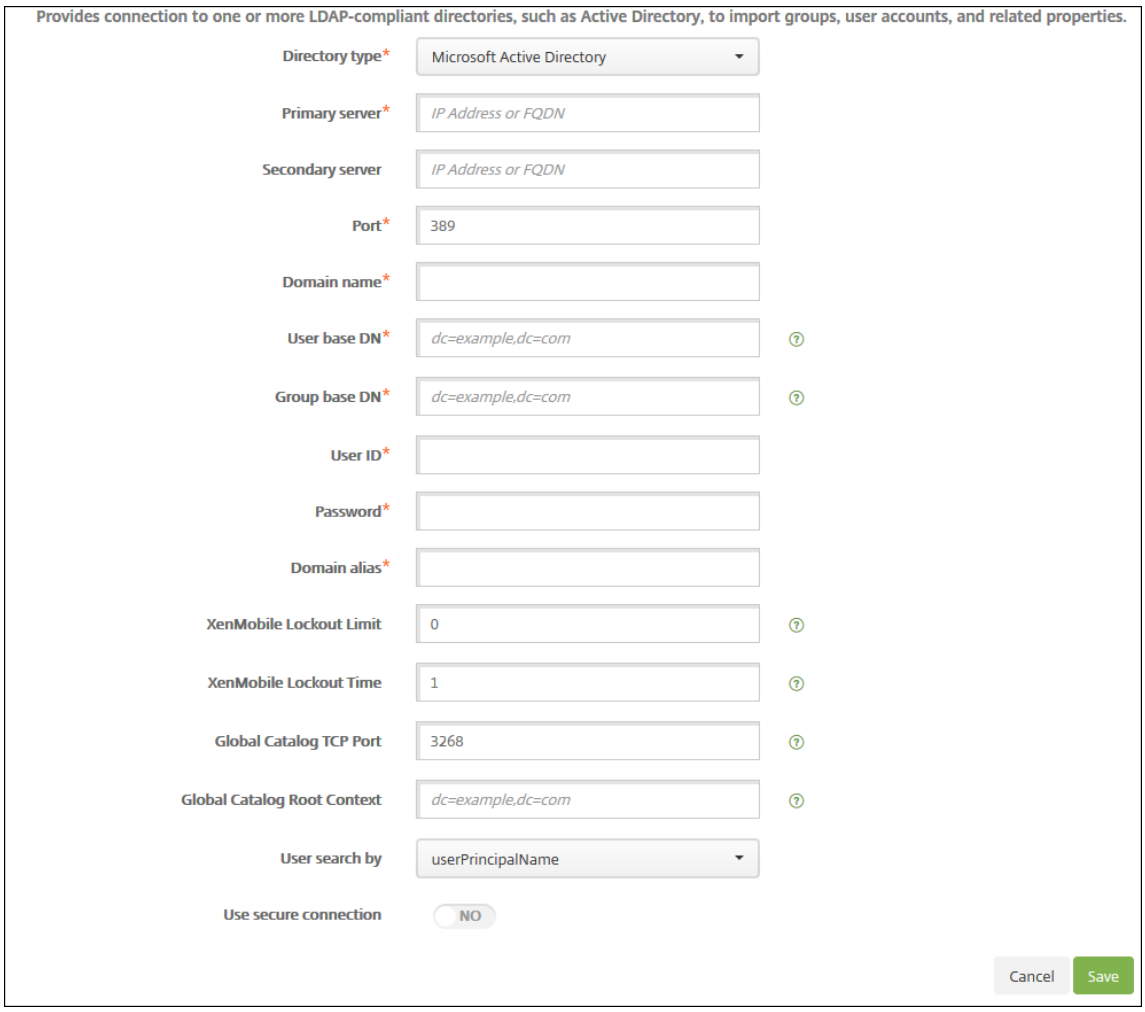
您通常在加入 Endpoint Management 时配置 LDAP 连接，如 配置 LDAP中所述。如果您在该部分中显示的屏幕可用之前加载，请使用本部分中的信息添加 LDAP 连接。

1. 在 Endpoint Management 控制台中，转到设置 **> LDAP**。
2. 在服务器下方，单击 **LDAP**。此时将显示 **LDAP** 页面。



3. 在 **LDAP** 页面上，单击 添加或 编辑。此时将显示 添加 **LDAP** 或编辑 **LDAP** 页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 配置以下设置：

   - 目录类型：在列表中，单击相应的目录类型。默认值为 **Microsoft Active Directory**。
   - 主服务器：键入用于 LDAP 的主服务器；可以输入 IP 地址或完全限定的域名 (FQDN)。
   - 辅助服务器：（可选）如果配置了辅助服务器，请输入辅助服务器的 IP 地址或 FQDN。此服务器是故障转移服务器，在无法访问主服务器时使用。
   - 端口：键入 LDAP 服务器使用的端口号。默认情况下，对于不安全的 LDAP 连接，端口号设置为 **389**。对安全的 LDAP 连接使用端口号 **636**，对 Microsoft 不安全 LDAP 连接使用 **3268**，或者对 Microsoft 安全 LDAP 连接使用 **3269**。
   - 域名：键入域名。
   - 用户基础 **DN**：通过唯一标识符在 Active Directory 中键入用户的位置。语法示例包括：`ou=users`、`dc=example` 或 `dc=com`。
   - 组基础 **DN**：在 Active Directory 中键入组的位置。例如 `cn=users`，`dc=domain`，`dc=net`，其中 `cn=users` 表示组的容器名称，`dc` 表示 Active Directory 的域组件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 用户 **ID**：键入与 Active Directory 帐户关联的用户 ID。
- 密码：键入与用户关联的密码。
- 域别名：键入域名的别名。如果在注册后更改域别名设置，用户必须重新注册。
- **Endpoint Management** 锁定限制：键入 **0** 到 **999** 之间的数字，表示失败登录尝试次数。值为 **0** 表示 Endpoint Management 从不根据失败登录尝试次数锁定用户。默认值为 **0**。

  请注意将此锁定限制设置为低于 LDAP 锁定策略的值。如果 Endpoint Management 无法向 LDAP 服务器进行身份验证，这样做有助于防止用户锁定。例如，如果 LDAP 锁定策略设置为 5 次尝试，请将此锁定限制配置为 **4** 或更低的值。
- **Endpoint Management** 锁定时间：键入 **0** 到 **99999** 之间的数字，表示用户超过锁定限制后必须等待的分钟数。值为 **0** 表示不强制用户在锁定后等待。默认值为 **1**。
- 全局目录 **TCP** 端口：键入全局目录服务器的 TCP 端口号。默认情况下，TCP 端口号设置为 **3268**；对于 SSL 连接，使用端口号 **3269**。
- 全局目录根上下文：（可选）键入用于在 Active Directory 中启用全局目录搜索的全局根上下文值。此搜索是除标准 LDAP 搜索之外的方法，可在任何域中使用，无需指定实际的域名。
- 用户搜索依据：选择 Endpoint Management 用于搜索此目录中的用户的用户名或用户 ID 的格式。用户在注册时以此格式输入其用户名或用户 ID。如果在注册后通过设置更改用户搜索，用户必须重新注册。

  如果选择 **userPincipalName**，则用户以下格式输入用户主体名称 (UPN)：

  – 用户名 @ 域

  如果选择 **sAMAccountName**，则用户将输入以下格式之一的安全帐户管理员 (SAM) 名称：

  – 用户名 @ 域
  – 域\用户名
- 使用安全连接：选择是否使用安全连接。默认值为否。

5. 单击保存。

删除 **LDAP** 兼容目录

1. 在 **LDAP** 表中，选择要删除的目录。

   可以通过选中每个属性旁边的复选框，选择多个要删除的属性。
2. 单击删除。此时将显示确认对话框。再次单击删除。

配置域加安全令牌身份验证

可以将 Endpoint Management 配置为要求用户通过 RADIUS 协议使用其 LDAP 凭据以及一次性密码进行身份验证。

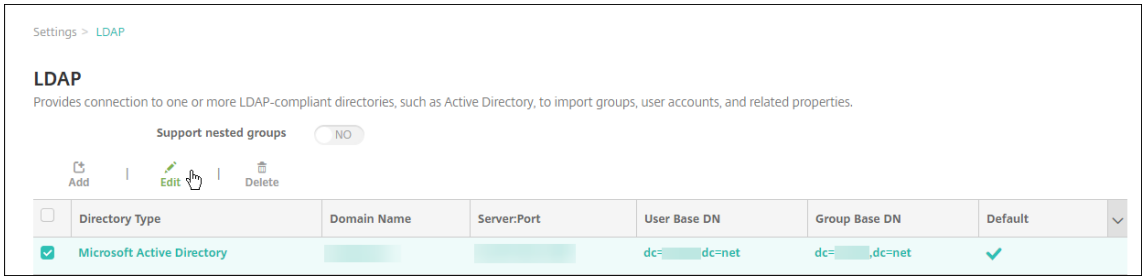
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要实现最佳可用性，可以将此配置与 Citrix PIN 和 Active Directory 密码缓存组合在一起。采用该配置时，用户不需要重复输入其 LDAP 用户名和密码。用户在注册、密码过期和帐户锁定时输入用户名和密码。

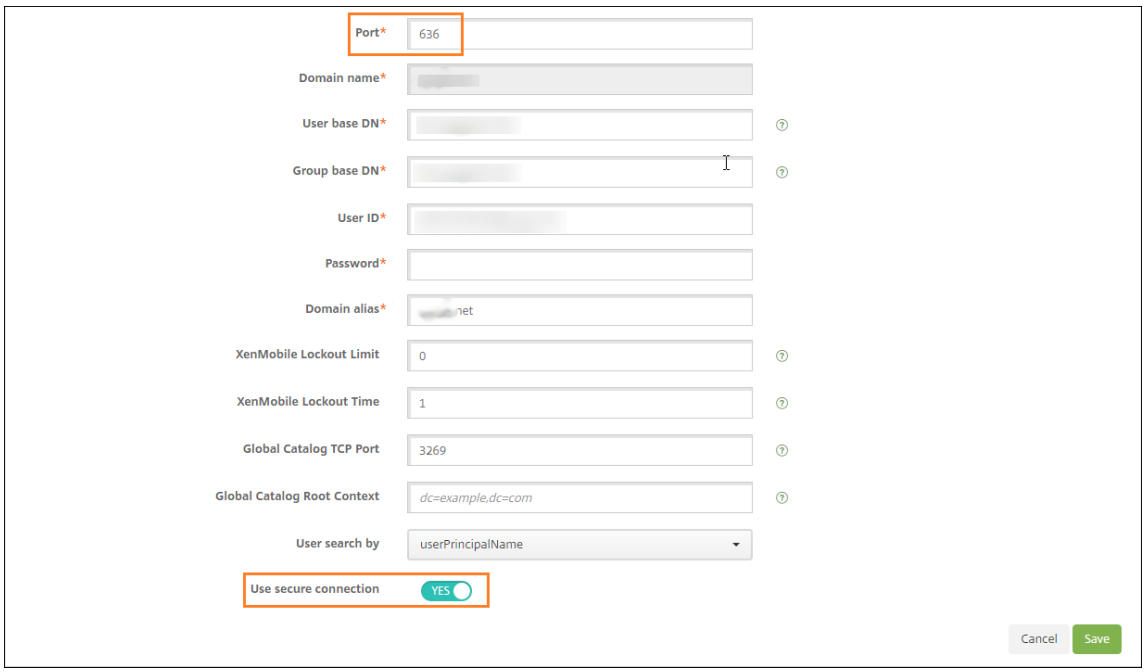
配置 **LDAP** 设置

使用 LDAP 进行身份验证要求您在 Endpoint Management 上安装证书颁发机构颁发的 SSL 证书。有关信息，请参阅 上传证书。

1. 在设置中，单击 **LDAP**。
2. 选择 **Microsoft Active Directory**，然后单击编辑。



3. 确认“端口”为 **636**（用于安全 LDAP 连接）还是 **3269**（用于 Microsoft 安全 LDAP 连接）。
4. 将使用安全连接更改为是。



配置 **Citrix Gateway** 设置

以下步骤假定您已向 Endpoint Management 中添加 Citrix Gateway 实例。要添加 Citrix Gateway 实例，请参阅 Citrix Gateway 和 Endpoint Management。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在设置中，单击 **Citrix Gateway**。
2. 选择 Citrix Gateway，然后单击编辑。
3. 在登录类型中，选择域和安全令牌。

启用 **Citrix PIN** 和用户密码缓存

要启用 Citrix PIN 和用户密码缓存，请转至设置 **>** 客户端属性，然后选中这些复选框：启用 **Citrix PIN** 身份验证和启用用户密码缓存。有关详细信息，请参阅客户端属性。

配置 **Citrix Gateway** 以进行域和安全令牌身份验证

为与 Endpoint Management 配合使用的虚拟服务器配置 Citrix Gateway 会话配置文件和策略。有关信息，请参阅 Citrix Gateway 文档。

客户端证书或证书加域身份验证

February 14, 2022

Endpoint Management 的默认配置是用户名和密码身份验证。要为 Endpoint Management 环境中的注册和访问再增加一个安全层，请考虑使用基于证书的身份验证。在 Endpoint Management 环境中，此配置是用于实现安全性和用户体验的最佳组合。证书加域身份验证通过 Citrix Gateway 进行的双重身份验证可提供最佳 SSO 选择和安全性。

要实现最佳可用性，可以将证书加域身份验证与 Citrix PIN 和 Active Directory 密码缓存组合在一起。因此，用户不需要重复输入其 LDAP 用户名和密码。用户在注册、密码过期和帐户锁定时输入用户名和密码。

> 重要：
>
> 用户在 Endpoint Management 中注册设备后，Endpoint Management 不支持将身份验证模式从域身份验证更改为某些其他身份验证模式。

如果禁用了 LDAP 并且不希望使用智能卡或类似方法，配置证书可代替智能卡来访问 Endpoint Management。用户随后使用 Endpoint Management 生成的唯一 PIN 进行注册。用户获取访问权限后，Endpoint Management 随后创建和部署后续用来在 Endpoint Management 环境中执行身份验证的证书。

使用 Citrix Gateway 仅证书身份验证或证书加域身份验证时，可以使用 NetScaler for XenMobile 向导设置 Endpoint Management 所需的配置。只能运行一次 NetScaler for XenMobile 向导。

在高度安全的环境中，在组织外的公共或不安全网络中使用 LDAP 凭据会被视为组织面临的首要安全威胁。对于高度安全的环境，可以选择使用客户端证书和安全令牌的双重身份验证。有关信息，请参阅 为证书和安全令牌身份验证配置 Endpoint Management。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

客户端证书身份验证适用于在 MAM 和 MDM+MAM 中注册的设备。必须依次配置 Microsoft 服务器、Endpoint Management 和 Citrix Gateway，才能对这些设备使用客户端证书身份验证。执行本文所述的如下常规步骤。

在 Microsoft 服务器上：

1. 向 Microsoft 管理控制台中添加证书管理单元。
2. 向证书颁发机构 (CA) 中添加模板。
3. 从 CA 服务器创建 PFX 证书。

在 Endpoint Management 中：

1. 将证书上载到 Endpoint Management。
2. 为基于证书的身份验证创建 PKI 实体。
3. 配置凭据提供程序。
4. 将 Citrix Gateway 配置为提供用于进行身份验证的用户证书。

有关 Citrix Gateway 配置的信息，请参阅 Citrix ADC 文档中的以下文章：

- 客户端身份验证
- SSL 配置文件基础结构
- 配置和绑定客户端证书身份验证策略。

必备条件

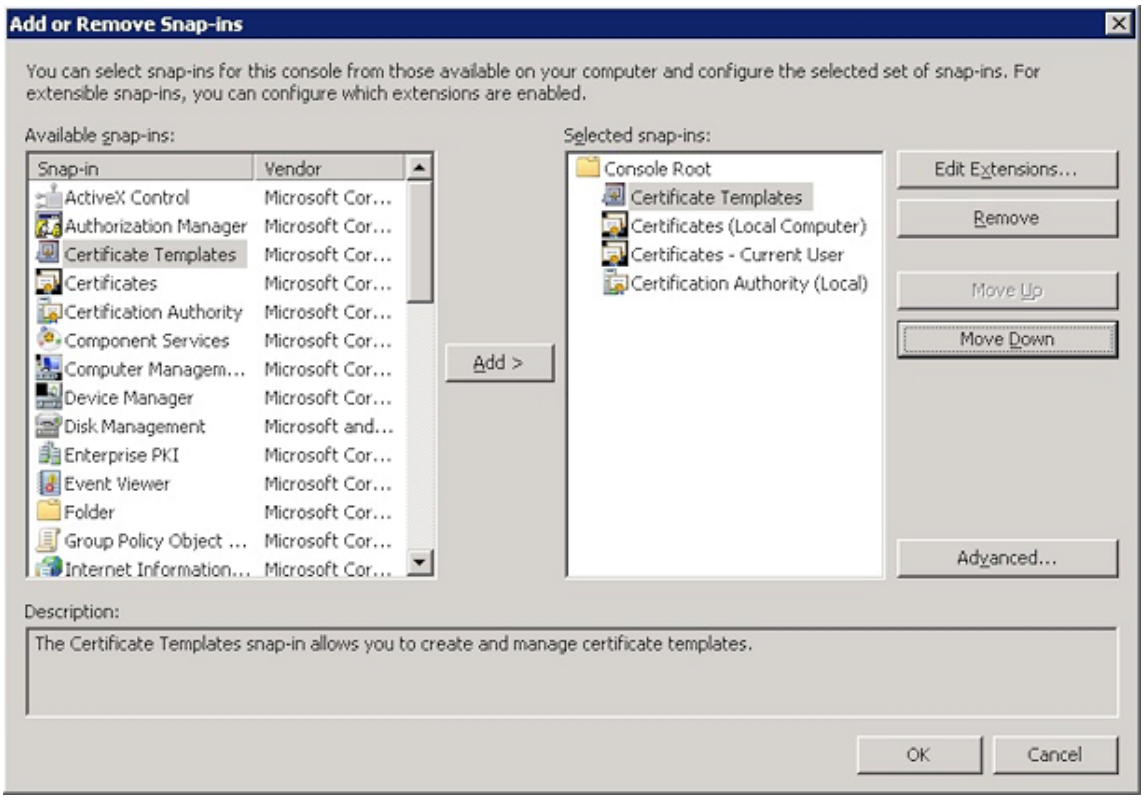
- 创建 Microsoft 证书服务实体模板时，通过排除特殊字符来避免已注册的设备可能会出现的身份验证问题。例如，请勿在模板名称中使用以下字符：`: ! $ ()## % + * ~ ? | { } []`
- 要为 Exchange ActiveSync 配置基于证书的身份验证，请参阅有 关 Exchange Server 的微软文档。为 Exchange ActiceSync 配置证书颁发机构 (CA) 服务器站点以要求客户端证书。
- 如果使用专用服务器证书来确保流向 Exchange Server 的 ActiveSync 流量安全，请确保移动设备具有所有根证书/中间证书。否则，在 Secure Mail 中设置邮箱时，基于证书的身份验证将失败。在 Exchange IIS 控制台中，必须执行以下操作：
  - 添加一个 Web 站点以供 Endpoint Management 和 Exchange 使用，并绑定 Web 服务器证书。
  - 使用端口 9443。
  - 对于该 Web 站点，必须添加两个应用程序，一个用于 Microsoft-Server-ActiveSync，一个用于 EWS。对于这两个应用程序，请在 **SSL Settings**（SSL 设置）下方选择 **Require SSL**（需要 SSL）。

向 **Microsoft** 管理控制台添加证书管理单元

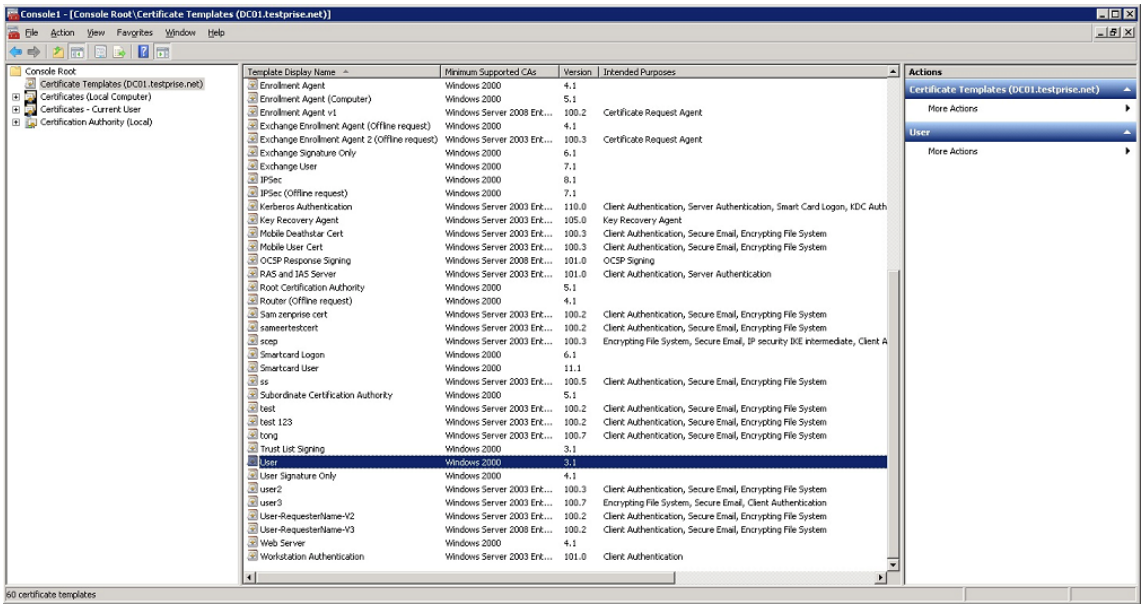
1. 打开该控制台，然后单击添加/删除管理单元。
2. 添加以下管理单元：
   - 证书模板
   - 证书 (本地计算机)

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 证书 - 当前用户
- 证书颁发机构 (本地)

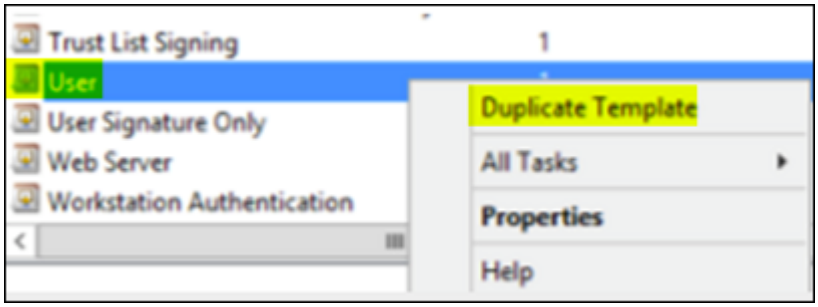


3. 展开证书模板。



4. 依次选择用户模板和复制模板。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



5. 提供模板显示名称。

   > 重要：
   >
   > 仅在必要时选中在 **Active Directory** 中发布证书复选框。如果选中了此选项，则将在 Active Directory 中创建所有用户客户端证书，这可能会导致您的 Active Directory 数据库混乱不堪。

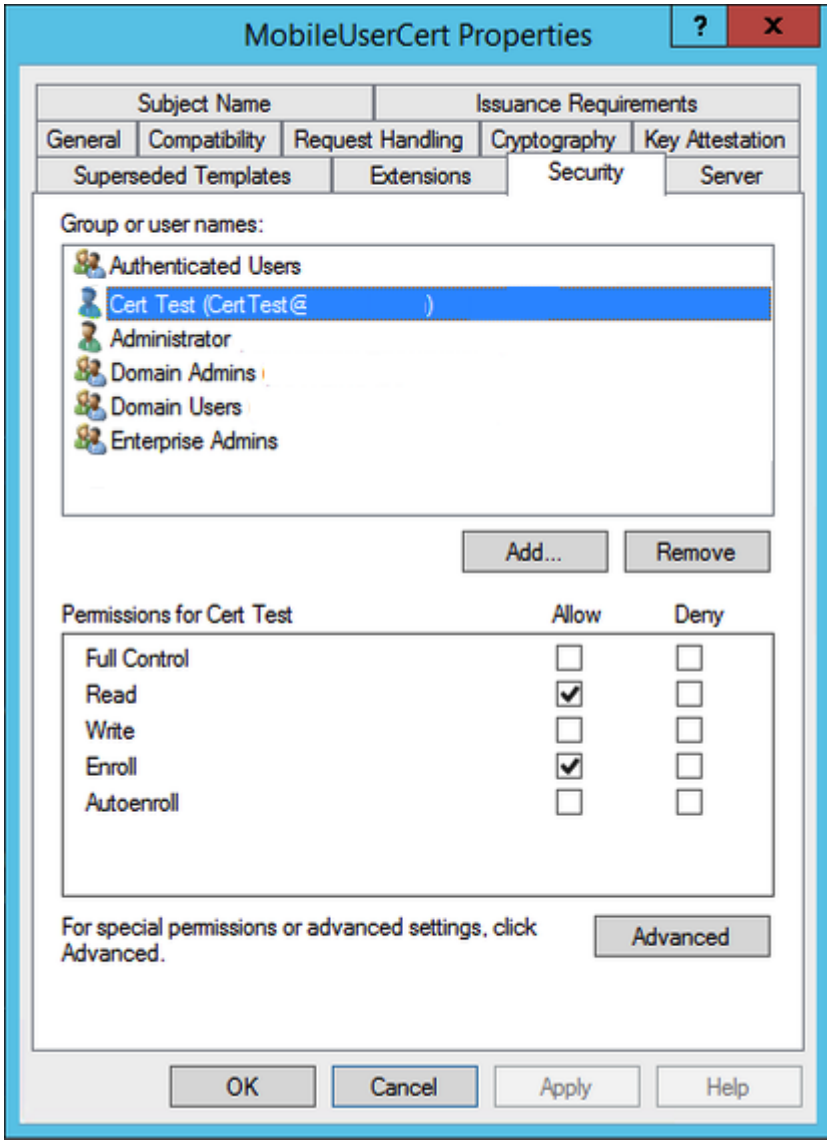
6. 选择 **Windows 2003 Server** 作为模板类型。在 Windows 2012 R2 Server 中，在兼容性下选择证书颁发机构，然后设置接受方 **Windows 2003**。

7. 在安全下，单击添加，然后选择 Endpoint Management 将用于生成证书的 AD 用户帐户。

   > 重要提示：
   >
   > 在此处仅添加服务帐户用户。请仅将注册权限添加到此 AD 用户帐户。

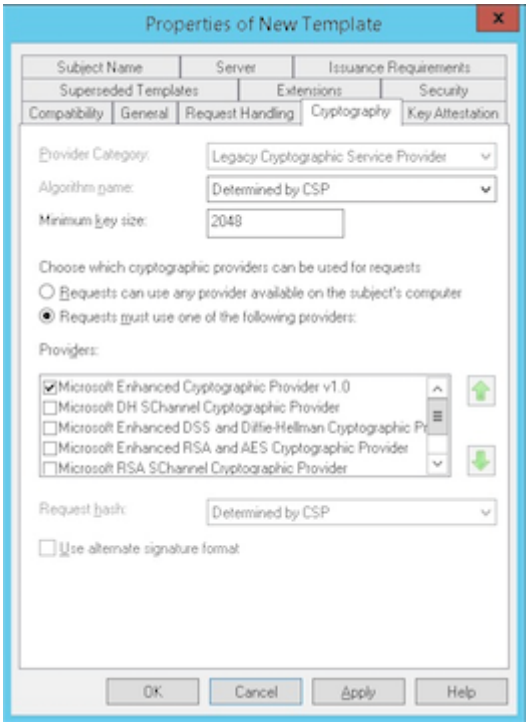
   如本文后面所述，您将使用服务帐户创建用户.pfx 证书。有关信息，请参阅从 CA 服务器创建 PFX 证书。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

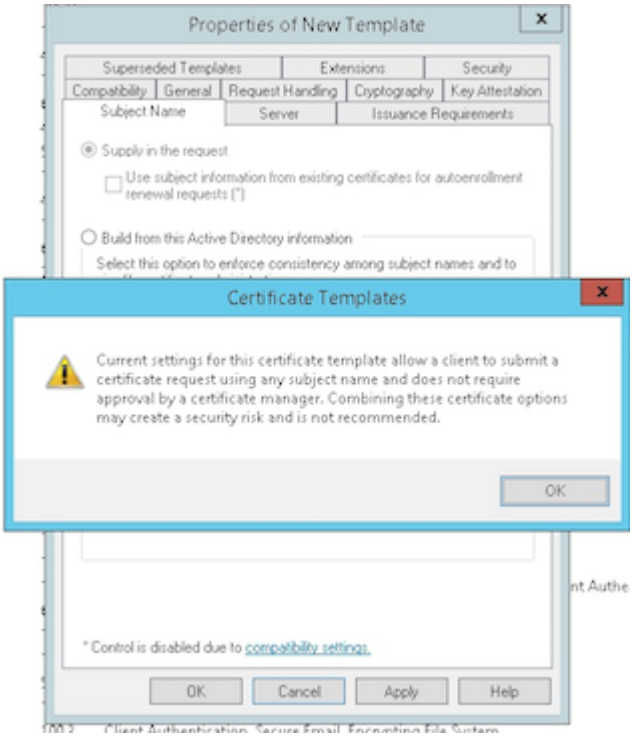


8. 在加密下方，务必提供密钥大小。以后可在 Endpoint Management 配置过程中输入密钥大小。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



9. 在使用者名称下方，选择在请求中提供。应用更改并保存。

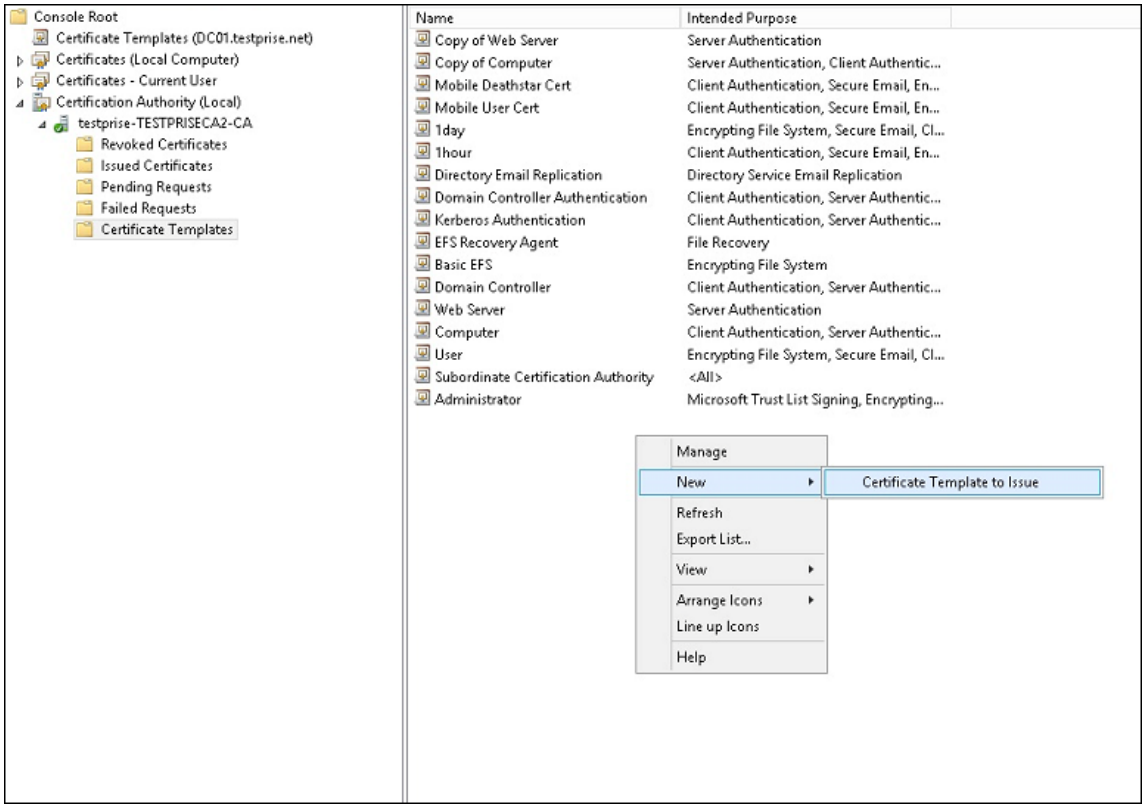


向证书颁发机构添加模板

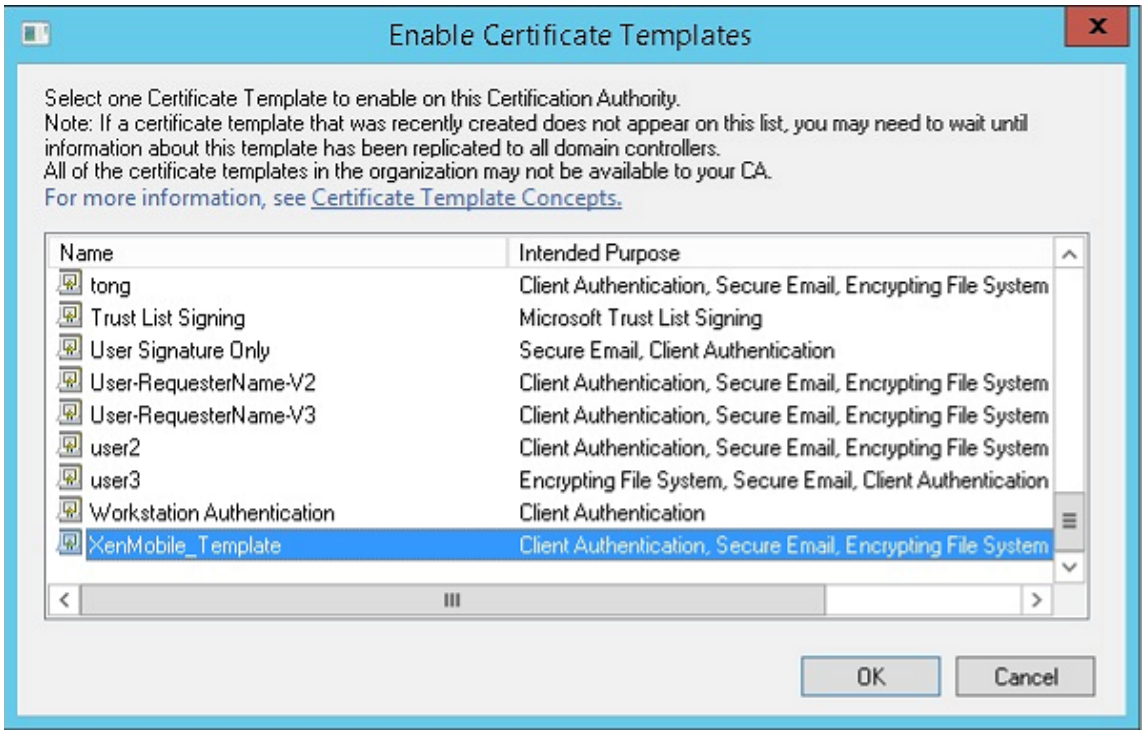
1. 转至证书颁发机构并选择证书模板。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 在右侧窗格中单击鼠标右键，然后选择新建 **>** 要颁发的证书模板。



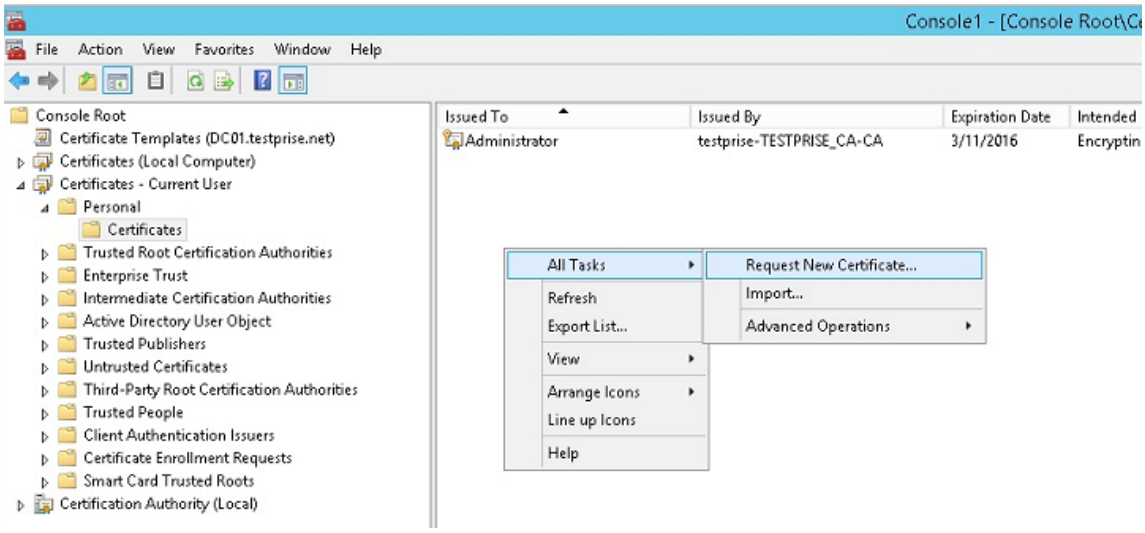
3. 选择在上一步中创建的模板，然后单击确定将其添加到证书颁发机构。



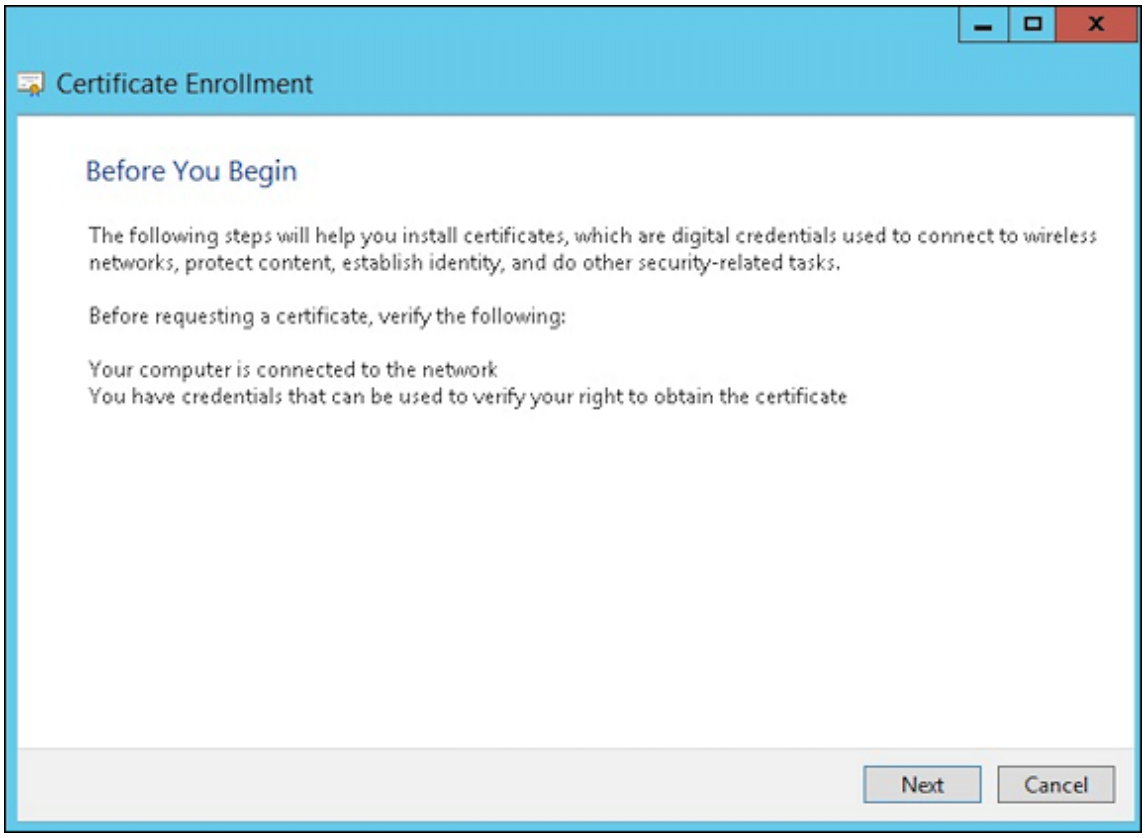
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

从 **CA** 服务器创建 **PFX** 证书

1. 使用登录时使用的服务帐户创建用户.pfx 证书。.pfx 会上传到 Endpoint Management，然后端点管理将代表注册其设备的用户请求用户证书。
2. 在当前用户下方，展开证书。
3. 在右侧窗格中单击鼠标右键，然后单击申请新证书。

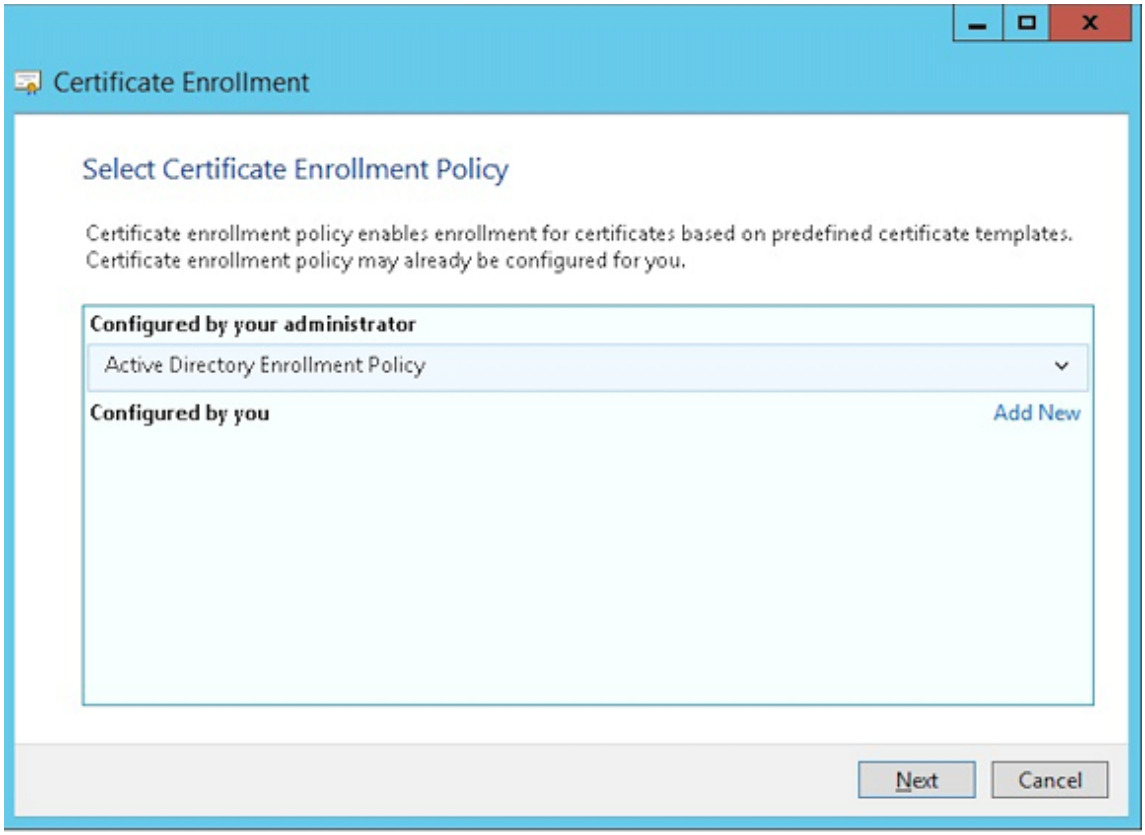


4. 此时将显示证书注册屏幕。单击 **Next**（下一步）。



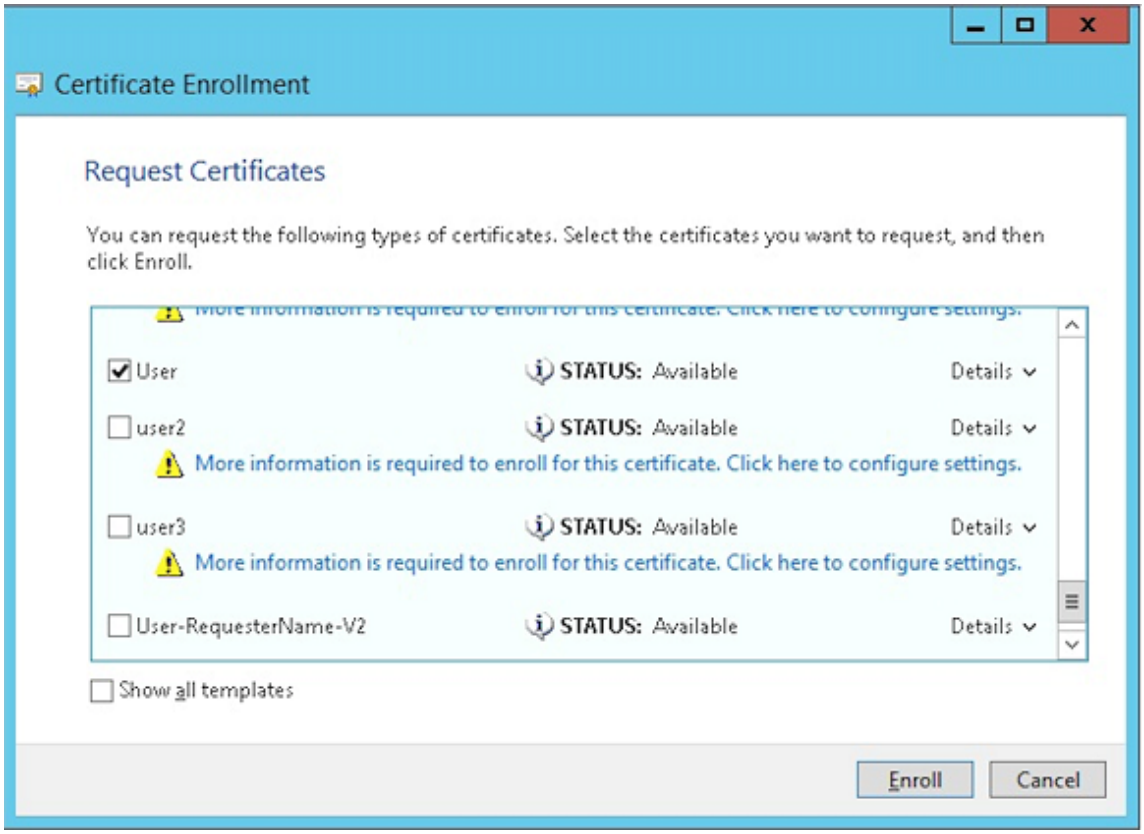
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 选择 **Active Directory** 注册策略，然后单击下一步。

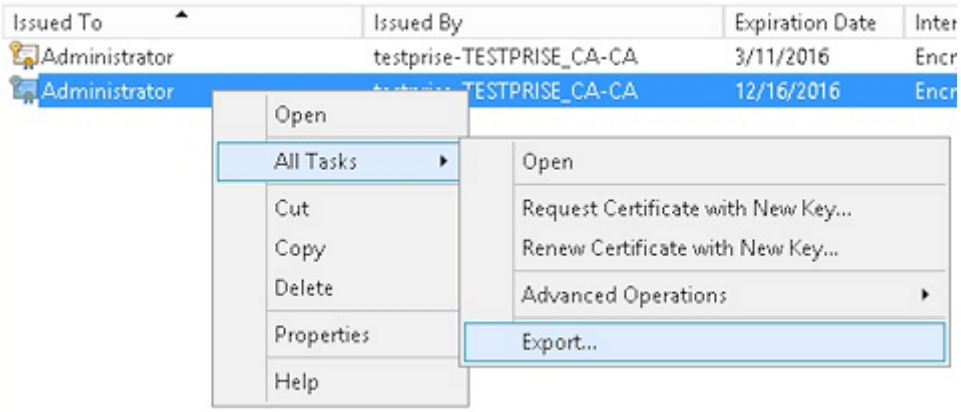


6. 选择用户模板，然后单击注册。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

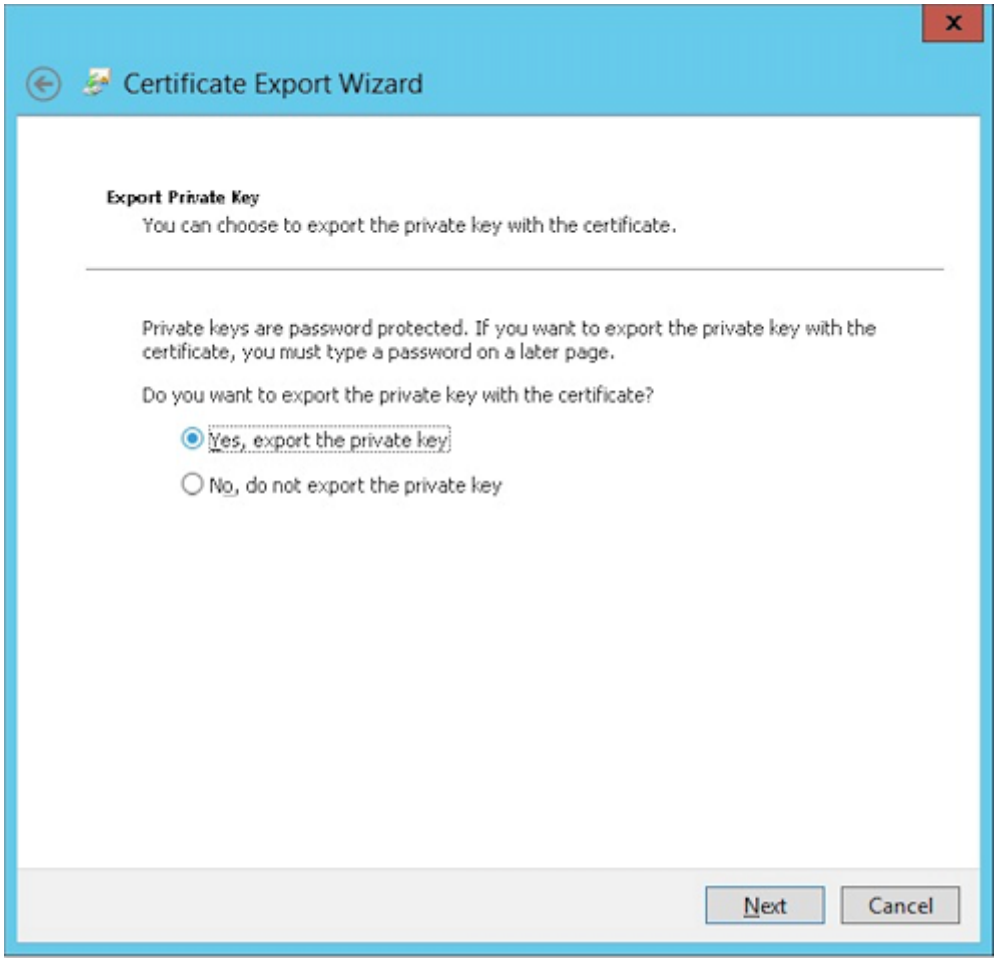


7. 导出在上一步中创建的.pfx 文件。



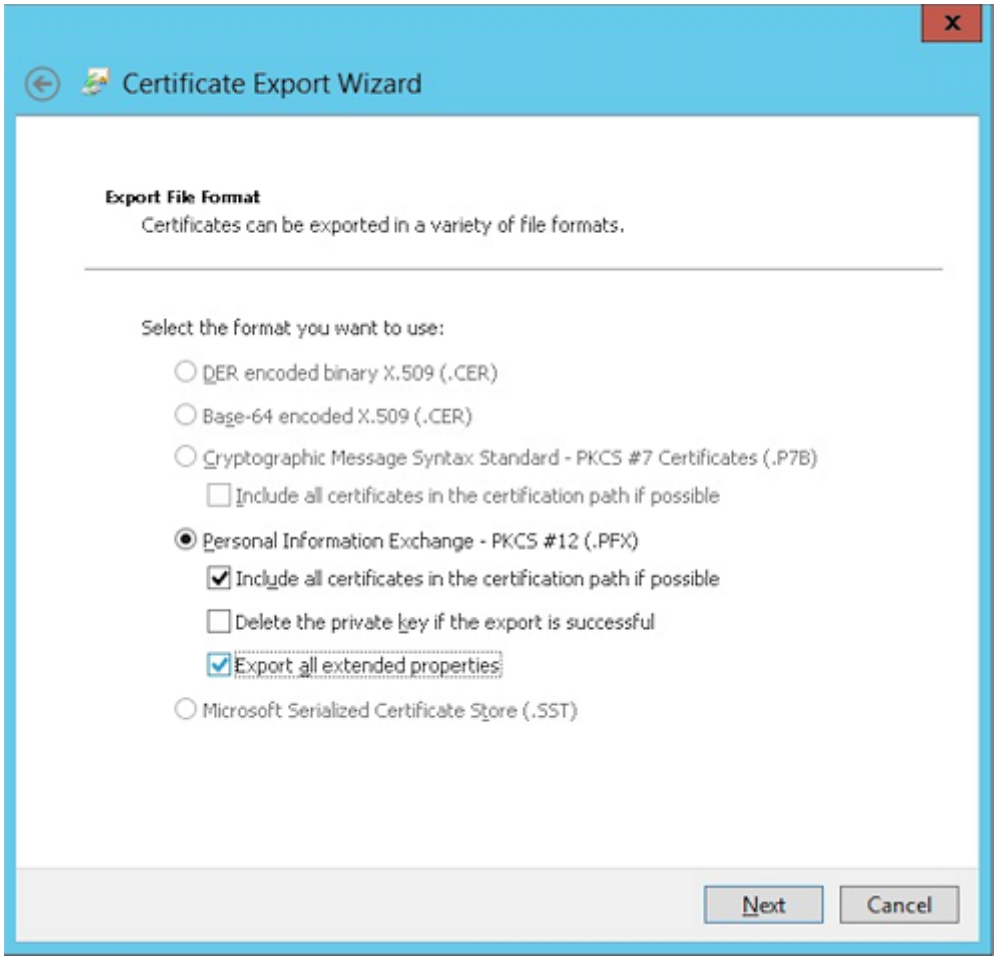
8. 单击是，导出私钥。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



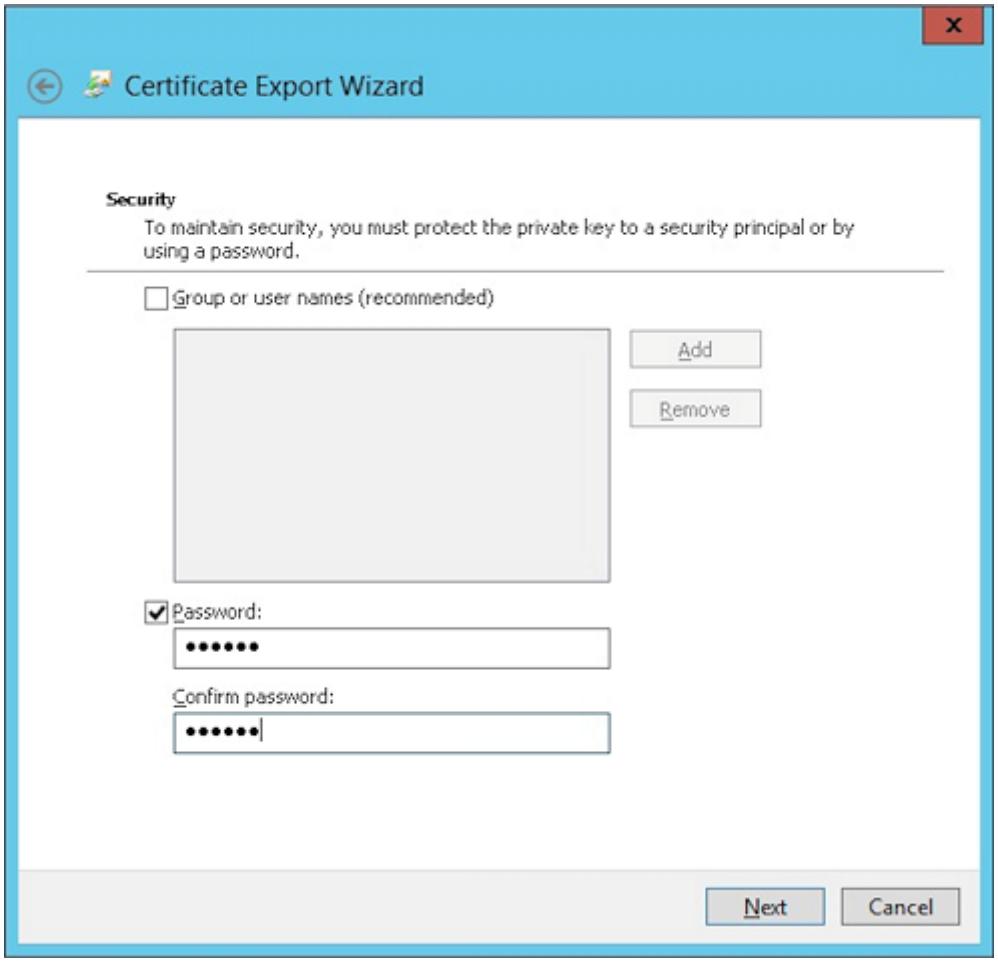
9. 选中如果可能，则包括证书路径中的所有证书和导出所有扩展属性复选框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



10. 设置在将此证书上载到 Endpoint Management 中时要使用的密码。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

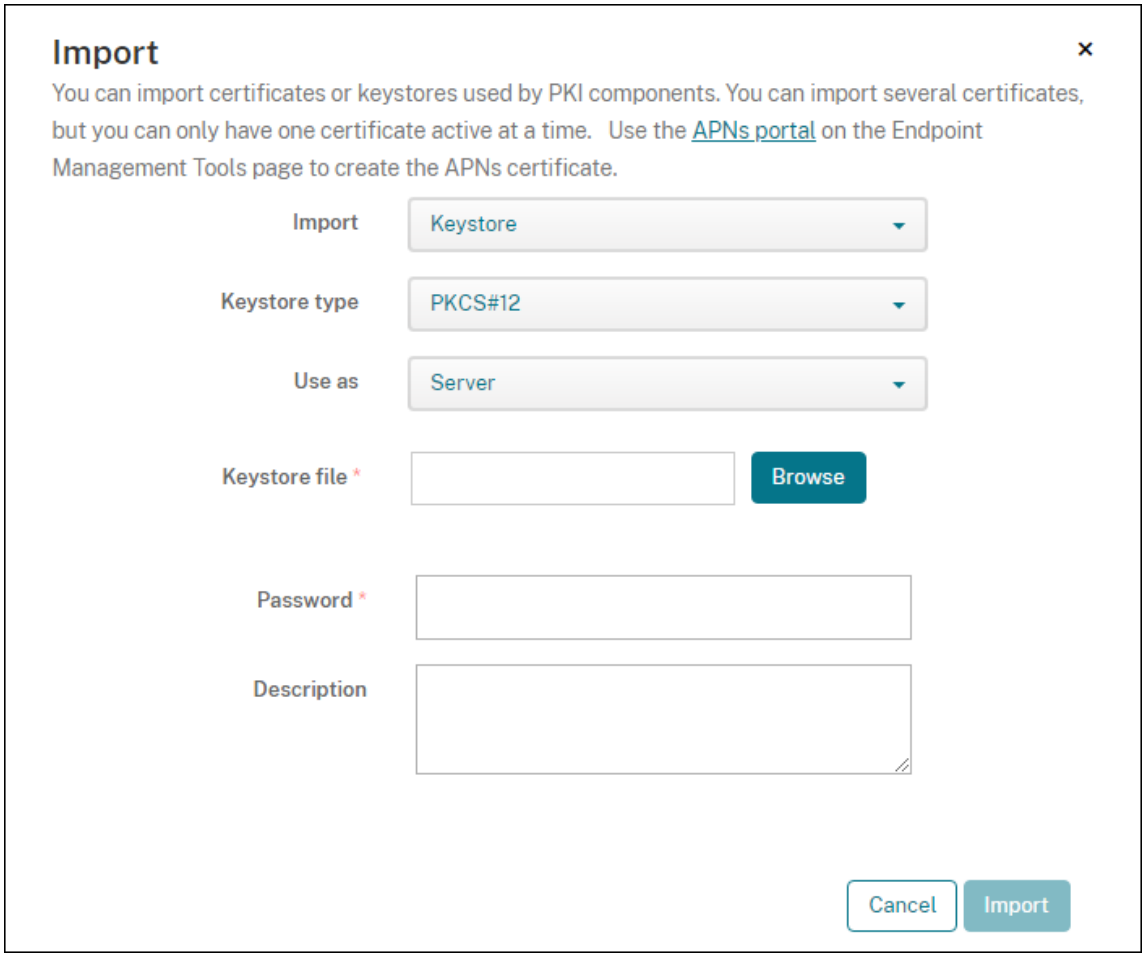


11. 将证书保存到您的硬盘驱动器。

将证书上载到 **Endpoint Management**

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置屏幕。
2. 依次单击证书和导入。
3. 输入以下参数：
    - 导入：密钥库
    - 密钥库类型： PKCS #12
    - 用作：服务器
    - 密钥库文件：单击“浏览”选择刚刚创建的.pfx 证书。
    - 密码：输入为此证书创建的密码。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

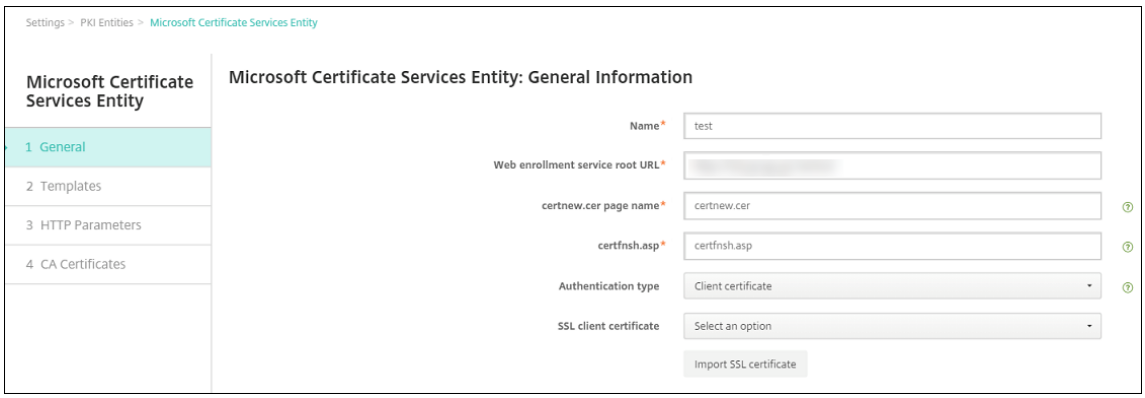


4. 单击导入。
5. 验证是否已正确安装证书。正确安装的证书将显示为用户证书。

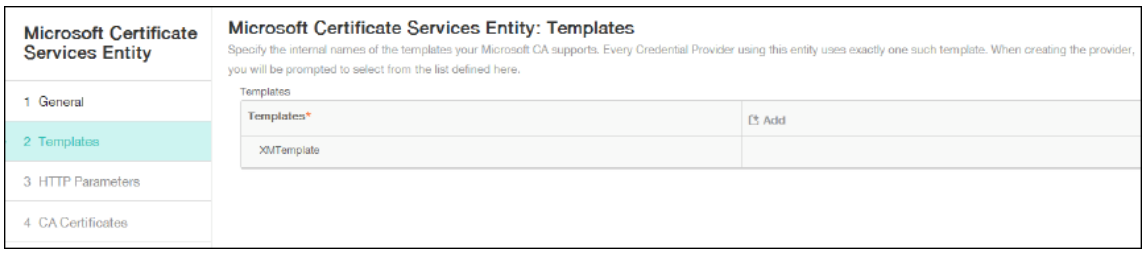
为基于证书的身份验证创建 **PKI** 实体

1. 在设置中，转至更多 **>** 证书管理 **> PKI** 实体。
2. 依次单击添加和 **Microsoft** 证书服务实体。此时将显示 **Microsoft** 证书服务实体**:** 常规信息屏幕。
3. 输入以下参数：
   - 名称：键入任意名称。
   - **Web** 注册服务根 **URL**： `https://RootCA-URL/certsrv/` （请务必在 URL 路径结尾添加一个斜杠 /。）
   - **certnew.cer** 页面名称： certnew.cer（默认值）
   - **certfnsh.asp**： certfnsh.asp（默认值）
   - 身份验证类型：客户端证书
   - **SSL** 客户端证书：选择用于颁发 Endpoint Management 客户端证书的用户证书。如果不存在证书，请按照上一节中的步骤上传证书。

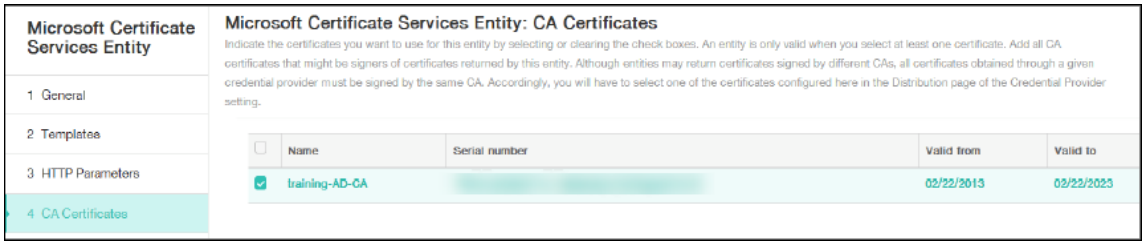
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 在模板下方，添加配置 Microsoft 证书时创建的模板。请勿添加空格。



5. 跳过“HTTP 参数”，然后单击 **CA** 证书。
6. 选择与您的环境对应的根 CA 名称。此根 CA 属于从 Endpoint Management 客户端证书中导入的链的一部分。

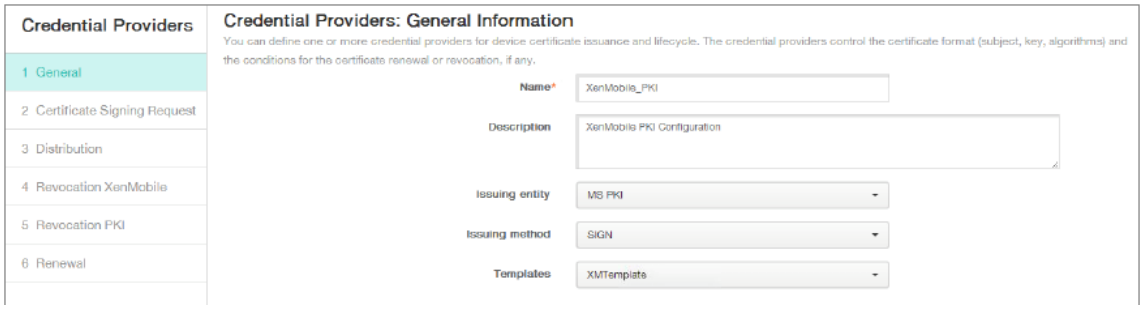


7. 单击保存。

配置凭据提供程序

1. 在设置中，转至更多 **>** 证书管理 **>** 凭据提供程序。
2. 单击添加。
3. 在常规下方，输入以下参数：
   - 名称：键入任意名称。
   - 说明：键入任意说明。
   - 颁发实体：选择之前创建的 PKI 实体。
   - 颁发方法：签名
   - 模板：选择在“PKI 实体”下方添加的模板。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

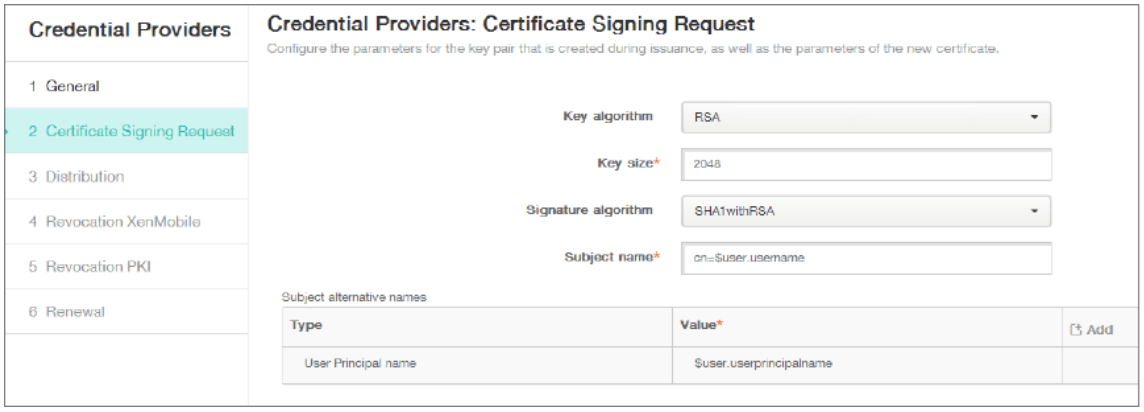


4. 单击证书签名请求，然后输入以下参数：

   - 密钥算法： RSA
   - 密钥大小： 2048
   - 签名算法： SHA256withRSA
   - 使用者名称： `cn=$user.username`

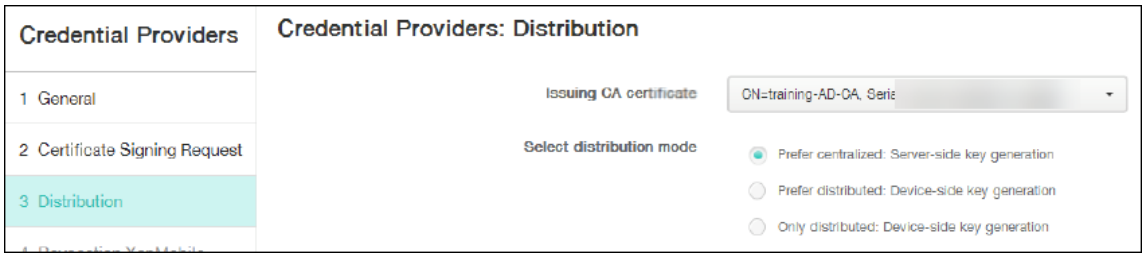
   对于使用者备用名称，请单击添加，然后输入以下参数：

   - 类型：用户主体名称
   - 值： `$user.userprincipalname`



5. 单击分发并输入以下参数：

   - 颁发 **CA** 证书：选择签署了 Endpoint Management 客户端证书的颁发 CA。
   - 选择分发模式：选择首选集中式**:** 服务器端密钥生成。

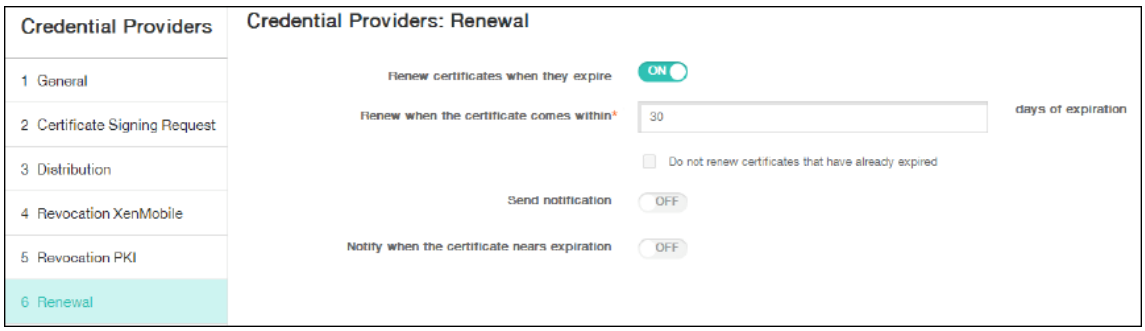


6. 对于后两个部分（吊销 **Endpoint Management** 和吊销 **PKI**），根据需要设置参数。在此示例中，跳过这两个选项。

7. 单击续订。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

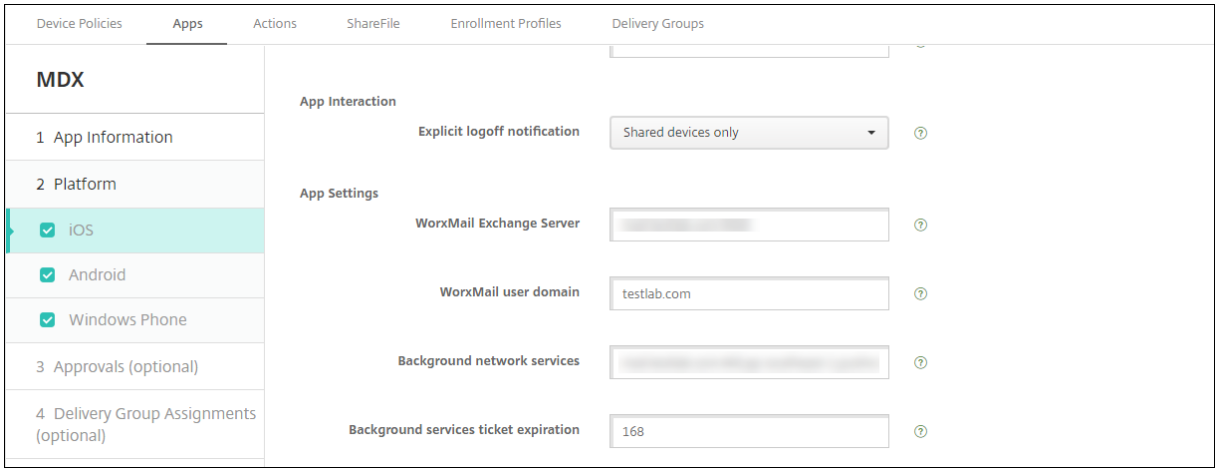
8. 在证书过期时启用续订。
9. 让所有其他设置保留为默认设置，或者根据需要进行更改。



10. 单击保存。

将 **Secure Mail** 配置为使用基于证书的身份验证

将 Secure Mail 添加到 Endpoint Management 时，请务必在应用程序设置下方配置 Exchange 设置。

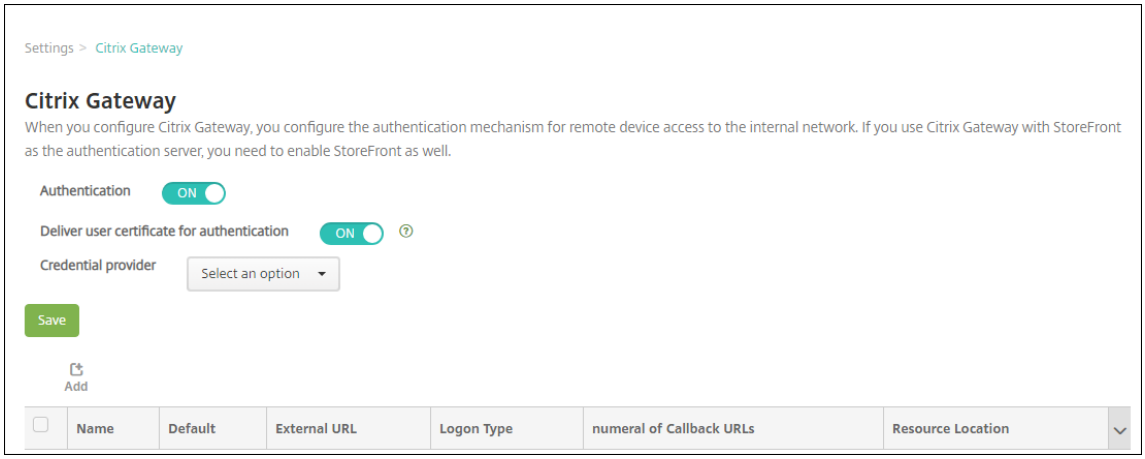


在 **Endpoint Management** 中配置 **Citrix Gateway** 证书传递

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置屏幕。
2. 在服务器下方，单击 **Citrix Gateway**。
3. 如果尚未添加 Citrix Gateway，请单击添加并指定以下设置：
   - 名称：设备的描述性名称。
   - 别名：设备的可选别名。
   - 外部 **URL**：`https://YourCitrixGatewayURL`
   - 登录类型：选择证书和域
   - 需要密码：关
   - 设置为默认值：开

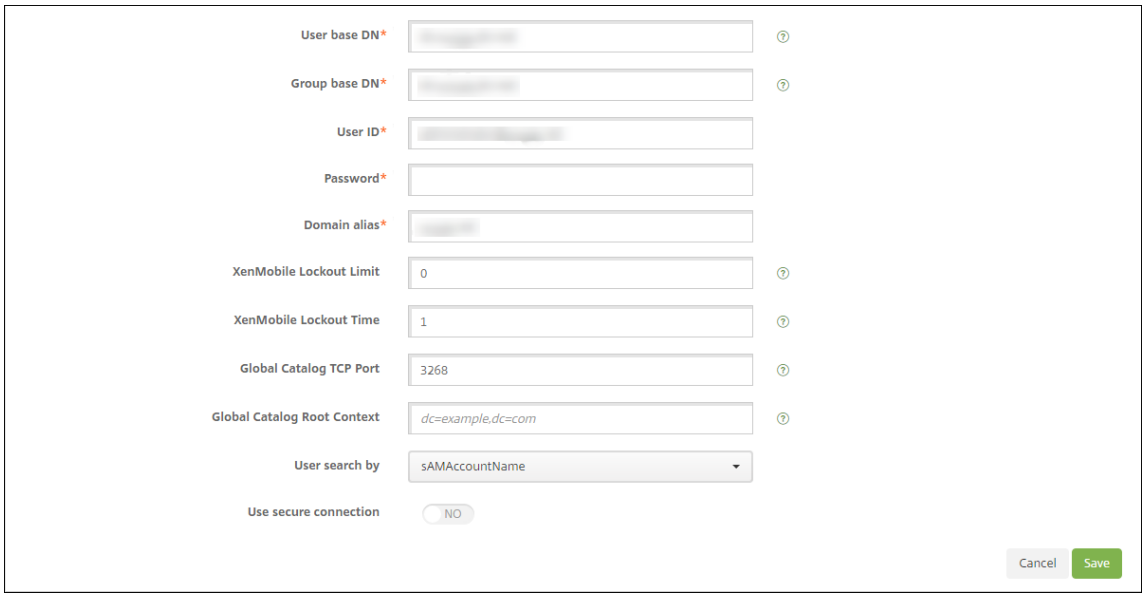
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

4. 对于身份验证和向用户提供用于身份验证的证书，选择开。



5. 对于凭据提供程序，选择一个提供程序，然后单击保存。

6. 要使用用户证书中的 sAMAccount 属性作为用户主体名称 (UPN) 的备用名称，请按如下所示在 Endpoint Management 中配置 LDAP 连接器：转至设置 **> LDAP**，选择目录并单击编辑，然后在用户搜索依据中选择 **sAMAccountName**。



启用 **Citrix PIN** 和用户密码缓存

要启用 Citrix PIN 和用户密码缓存，请转至设置 **>** 客户端属性，然后选中这些复选框：启用 **Citrix PIN** 身份验证和启用用户密码缓存。有关详细信息，请参阅客户端属性。

客户端证书配置故障排除

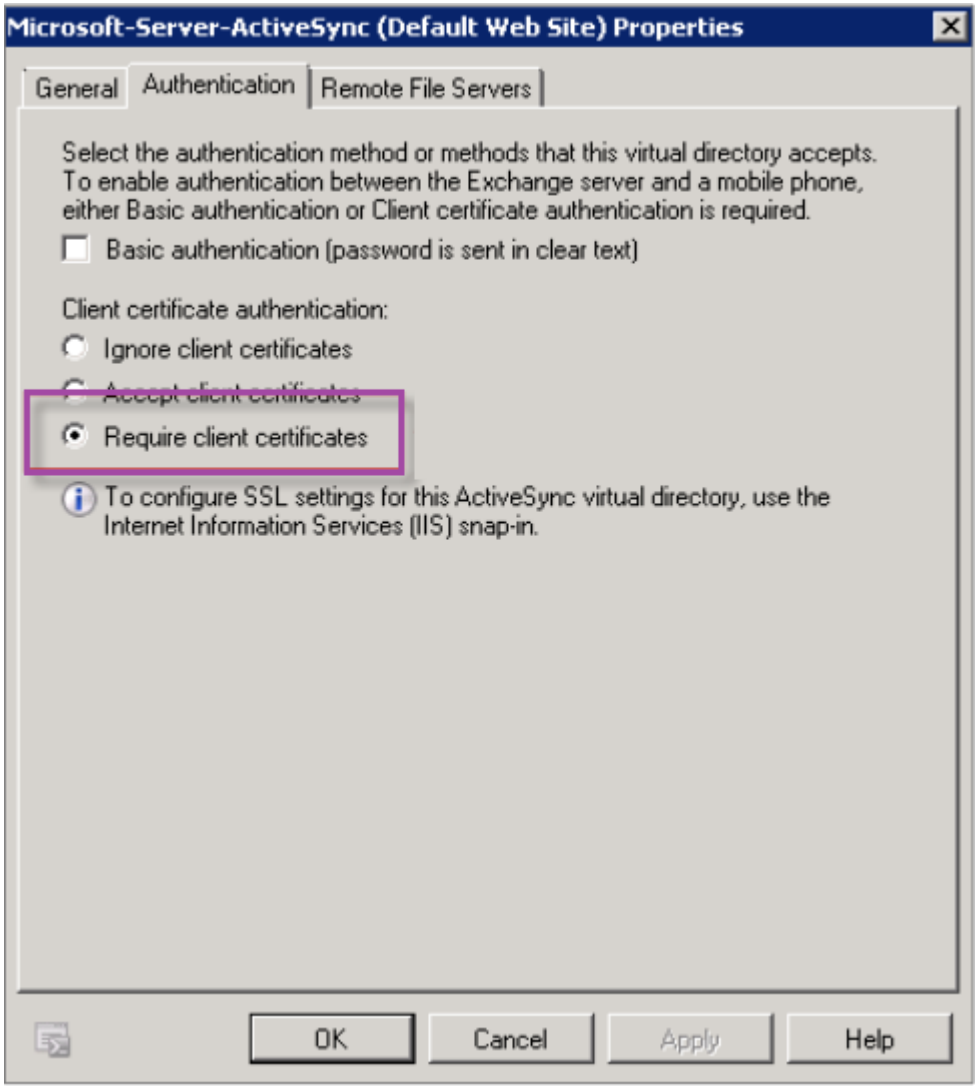
成功配置前述配置及 Citrix Gateway 配置后，用户工作流如下：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 用户注册其移动设备。
2. Endpoint Management 会提示用户创建 Citrix PIN。
3. 随后用户被重定向到应用商店。
4. 用户启动 Secure Mail 时，Endpoint Management 不提示其提供用户凭据以用于邮箱配置。相反，Secure Mail 将从 Secure Hub 请求客户端证书，并将其提交给 Microsoft Exchange Server 以进行身份验证。如果 Endpoint Management 在用户启动 Secure Mail 时提示用户提供凭据，请检查您的配置。

如果用户能够下载并安装 Secure Mail，但邮箱配置过程中 Secure Mail 无法完成配置：

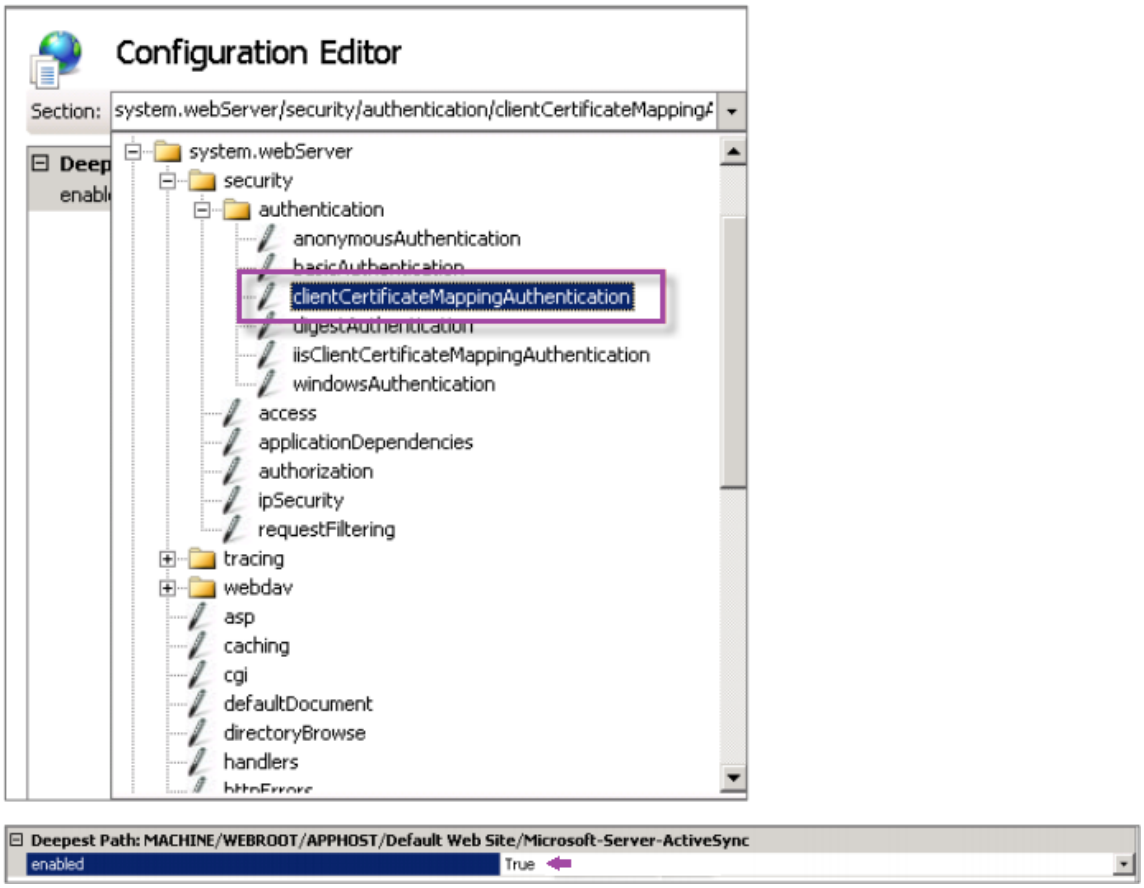
1. 如果 Microsoft Exchange Server ActiveSync 使用专用 SSL 服务器证书来确保流量安全，请验证是否已在移动设备上安装根证书/中间证书。
2. 验证为 ActiveSync 选择的身份验证类型是否为要求提供客户端证书。



3. 在 Microsoft Exchange Server 上，检查 **Microsoft-Server-ActiveSync** 站点以验证是否已启用客户端证书映射身份验证。默认情况下，客户端证书映射身份验证处于禁用状态。此选项位于配置编辑器 **>** 安全 **>** 身份

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

验证下方。



选择 **True** 后，请务必单击应用以使更改生效。

4. 在 Endpoint Management 控制台中检查 Citrix Gateway 设置：确保向用户提供用于身份验证的证书设置为开，并且为凭据提供程序选择了正确的配置文件。

确定是否已向移动设备提供客户端证书

1. 在 Endpoint Management 控制台中，转至管理 **>** 设备，然后选择设备。
2. 单击编辑或显示更多。
3. 转至交付组部分，并搜索以下条目：

   Citrix Gateway Credentials: Requested credential, CertId=

验证是否已启用客户端证书协商

1. 运行以下 `netsh` 命令以显示 IIS Web 站点上绑定的 SSL 证书配置：

   ```
   netsh http show sslcert
   ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 如果 **Negotiate Client Certificate**（协商客户端证书）的值为 **Disabled**（已禁用），请运行以下命令将其启用：

```
netsh http delete sslcert ipport=0.0.0.0:443
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={
 app_id } certstorename=store_name verifyclientcertrevocation=Enable
 VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable
clientcertnegotiation=Enable
```

例如：

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdfhaf98rhkjqf9823rkjhd
 appid={ 123asd456jd-a12b-3c45-d678-123456lkjhgf } certstorename=
ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCached
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

如果无法通过 Endpoint Management 向 Windows Phone 8.1 设备提供根证书/中间证书，请执行以下操作：

- 通过电子邮件将根证书/中间证书 (.cer) 文件发送到 Windows Phone 8.1 设备并直接安装。

如果无法在 Windows Phone 8.1 上成功安装 Secure Mail，请验证以下项：

- 应用程序注册令牌（.AETX 文件）是否已使用企业中心设备策略通过 Endpoint Management 提供。
- 创建应用程序注册令牌时使用的证书提供程序提供的企业证书是否与用于封装 Secure Mail 并为 Secure Hub 应用程序签名的企业证书相同。
- 是否使用相同的发布者 ID 签名并封装 Secure Hub、Secure Mail 和应用程序注册令牌。

PKI 实体

October 18, 2022

Endpoint Management 公钥基础结构 (PKI) 实体配置代表执行实际 PKI 操作（颁发、吊销和状态信息）的组件。这些组件是 Endpoint Management 的内部组件或外部组件。内部组件称为自主组件。外部组件属于企业基础结构的组成部分。

Endpoint Management 支持以下类型的 PKI 实体：

- Microsoft 证书服务
- 任意证书颁发机构 (CA)

Endpoint Management 支持以下 CA 服务器：

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Windows Server 2016
- Windows Server 2019

常见 **PKI** 概念

无论何种类型，每个 PKI 实体均拥有下列功能的子集：

- 签名：基于证书签名请求 (CSR) 颁发新证书。
- 提取：恢复现有证书和密钥对。
- 吊销：吊销客户端证书。

关于 **CA** 证书

配置 PKI 实体时，请向 Endpoint Management 指明哪个 CA 证书将成为该实体所颁发（或从该实体恢复）的证书的签署者。该 PKI 实体可以返回任意多个不同 CA 签名（提取或新签名）的证书。

请在 PKI 实体配置过程中提供其中每个颁发机构的证书。为此，请将证书上载到 Endpoint Management，然后在 PKI 实体中引用这些证书。对于任意 CA，证书实际上是签名 CA 证书。对于外部实体，必须手动指定该证书。

> 重要：
>
> 创建 Microsoft 证书服务实体模板时，为避免已注册的设备可能会出现的身份验证问题：请勿在模板名称中使用特殊字符。例如，请勿使用：`! : $ ( )## % + * ~ ? | { } [ ]`

Microsoft 证书服务

Endpoint Management 通过其 Web 注册界面与 Microsoft Certificate Services 交互。Endpoint Management 仅支持通过该接口颁发新证书。如果 Microsoft CA 生成 Citrix Gateway 用户证书，Citrix Gateway 将支持续订和吊销这些证书。

要在 Endpoint Management 中创建 Microsoft CA PKI 实体，必须指定证书服务 Web 界面的基本 URL。如果选择此项，则使用 SSL 客户端身份验证保护 Endpoint Management 与证书服务 Web 界面之间的连接。

添加 **Microsoft** 证书服务实体

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标，然后单击 **PKI** 实体。
2. 在 **PKI** 实体页面上，单击添加。

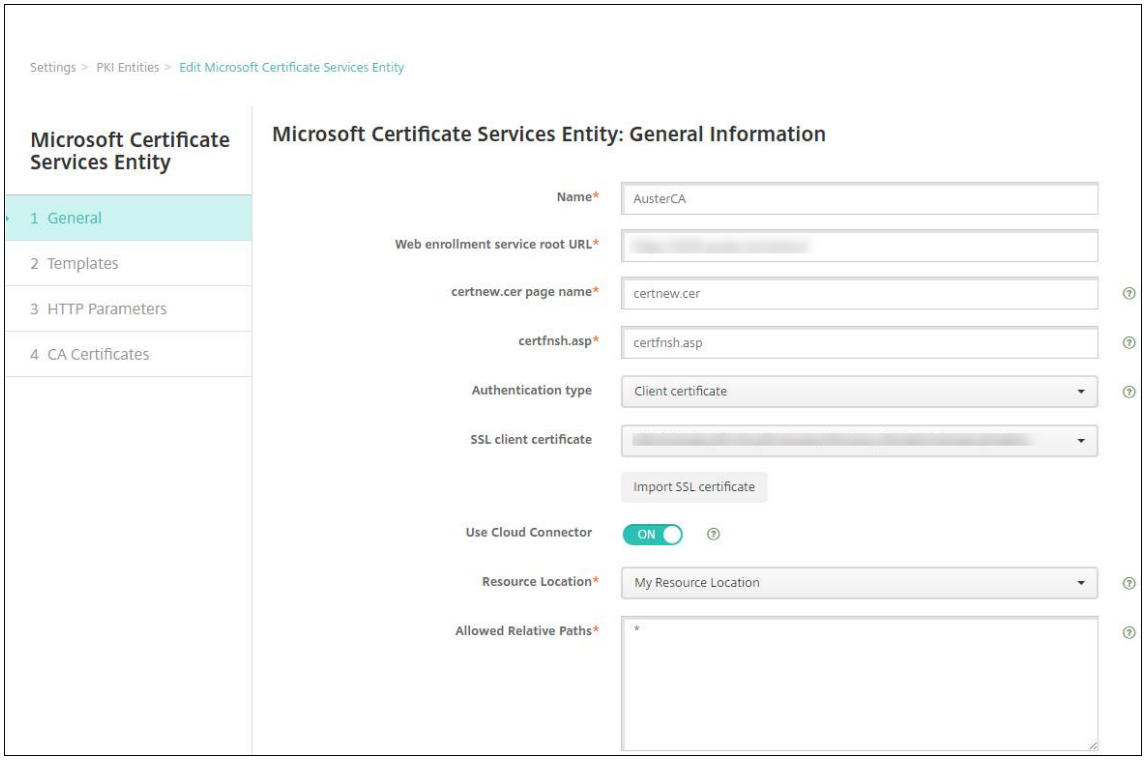
   此时将显示一个 PKI 实体类型菜单。
3. 单击 **Microsoft** 证书服务实体。

   此时将显示 **Microsoft** 证书服务实体**:** 常规信息页面。
4. 在 **Microsoft** 证书服务实体**:** 常规信息页面上，配置以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 名称：为新实体键入名称，此名称以后将用于指代该实体。实体名称必须唯一。
- **Web** 注册服务根 **URL**：键入 Microsoft CA Web 注册服务的基本 URL。例如：`https://192.0.0.1/certsrv/`。该 URL 可使用纯 HTTP 或 HTTP-over-SSL。
- **certnew.cer** 页面名称： certnew.cer 页面的名称。若非因为某些原因重命名了此页面，请使用默认名称。
- **certfnsh.asp**： certfnsh.asp 页面的名称。若非因为某些原因重命名了此页面，请使用默认名称。
- 身份验证类型：选择要使用的身份验证方法。
  - 无
  - **HTTP Basic**：键入连接所需的用户名和密码。
  - 客户端证书：选择正确的 SSL 客户端证书。
- 使用 **Cloud Connector**：选择开可使用 Cloud Connector 连接到 PKI 服务器。然后，指定资源位置以及连接的允许使用的相对路径。
  - 资源位置：从在 Citrix Cloud Connector 中定义的资源位置进行选择。
  - 允许使用的相对路径：允许为指定资源位置使用的相对路径。每行请指定一个路径。可以使用星号 (*) 通配符。

    假定资源位置为 `https://www.ServiceRoot/certsrv`。要提供对该路径中的所有 URL 的访问权限，请在允许使用的相对路径中输入 `/*`。



5. 单击测试连接以确保服务器可以访问。如果不可访问，则会显示一条消息，指出连接失败。请检查配置设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. 单击下一步。

   此时将显示 **Microsoft** 证书服务实体**:** 模板页面。在此页面上，指定 Microsoft CA 所支持模板的内部名称。创建凭据提供程序时，从此处定义的列表中选择模板。使用此实体的每个凭据提供程序仅使用一个此类模板。

   有关 Microsoft 证书服务模板的要求，请参阅您的 Microsoft Server 版本对应的 Microsoft 文档。除了证书中注明的证书格式外，Endpoint Management 对其分发的证 书没有要求。

7. 在 **Microsoft** 证书服务实体**:** 模板页面上，单击添加，键入模板的名称，然后单击保存。为要添加的每个模板重复执行此步骤。

8. 单击下一步。

   此时将显示 **Microsoft** 证书服务实体**: HTTP** 参数页面。在此页面上，您可以指定自定义参数以供 Endpoint Management 添加到向 Microsoft Web 注册界面发送的 HTTP 请求。自定义参数仅对 CA 上运行的自定义脚本有用。

9. 在 **Microsoft** 证书服务实体**: HTTP** 参数页面上，单击添加，键入要添加的 HTTP 参数的名称和值，然后单击下一步。

   此时将显示 **Microsoft** 证书服务实体**: CA** 证书页面。在此页面上，必须将系统通过此实体获取的证书的签署者告知 Endpoint Management。续订 CA 证书后，将在 Endpoint Management 中对其进行更新。Endpoint Management 以透明方式将更改应用于实体。

10. 在 **Microsoft** 证书服务实体**: CA** 证书页面上，选择要用于此实体的证书。

11. 单击保存。

    实体将显示在 PKI 实体表格中。

Citrix Gateway 证书吊销列表 **(CRL)**

Endpoint Management 仅支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，Endpoint Management 将使用 Citrix Gateway 管理吊销。

配置基于客户端证书的身份验证时，请考虑是否要配置 Citrix Gateway 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh**（启用 CRL 自动刷新）。此步骤可确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证。

Endpoint Management 将重新颁发新证书，因为吊销用户证书后，Endpoint Management 不会限制用户生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

任意 **CA**

向 Endpoint Management 提供 CA 证书及关联的私钥时，将创建任意 CA。Endpoint Management 将根据您指定的参数，在内部处理证书颁发、吊销和状态信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置任意 CA 时，可以为该 CA 激活联机证书状态协议 (OCSP) 支持。如果您启用了 OCSP 支持，CA 将向该 CA 颁发的证书中添加 `id-pe-authorityInfoAccess` 扩展。该扩展指向以下位置处的 Endpoint Management 内部 OCSP 响应者：

```
https://<server>/<instance>/ocsp
```

配置 OCSP 服务时，请为相关任意实体指定 OCSP 签名证书。可以将 CA 证书本身用作签署者。要避免 CA 私钥的不必要暴露（建议避免），请创建一个由 CA 证书签名并包含 `id-kp-OCSPSigning extendedKeyUsage` 扩展的委派 OCSP 签名证书。

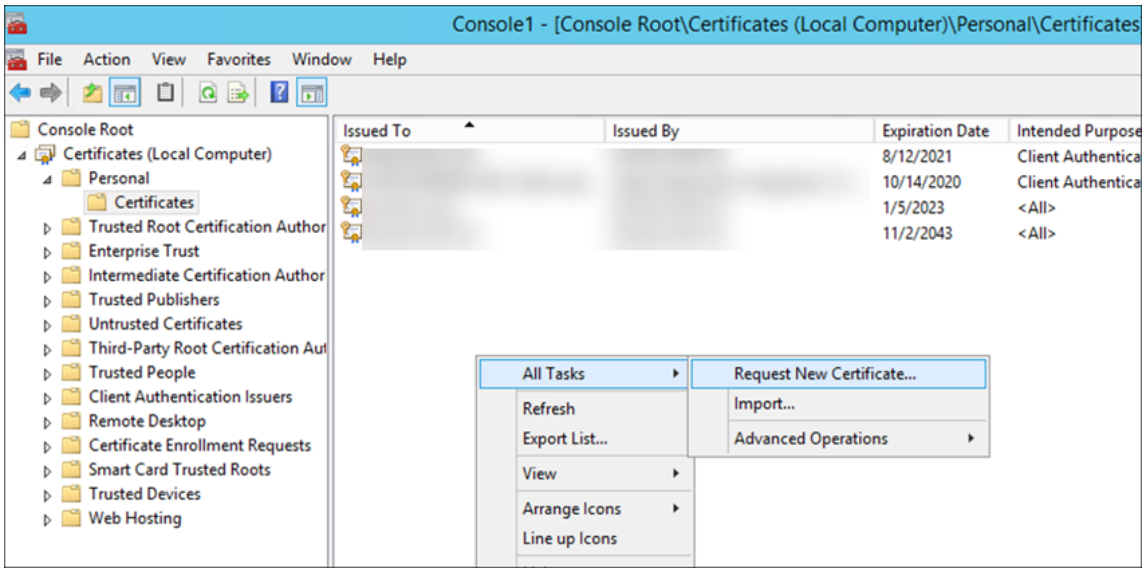
Endpoint Management OCSP Responder Service 支持在请求中使用基本 OCSP 响应及以下散列算法：

- SHA-256
- SHA-384
- SHA-512

响应通过 SHA-256 及签名证书的密钥算法（DSA、RSA 或 ECDSA）进行签名。

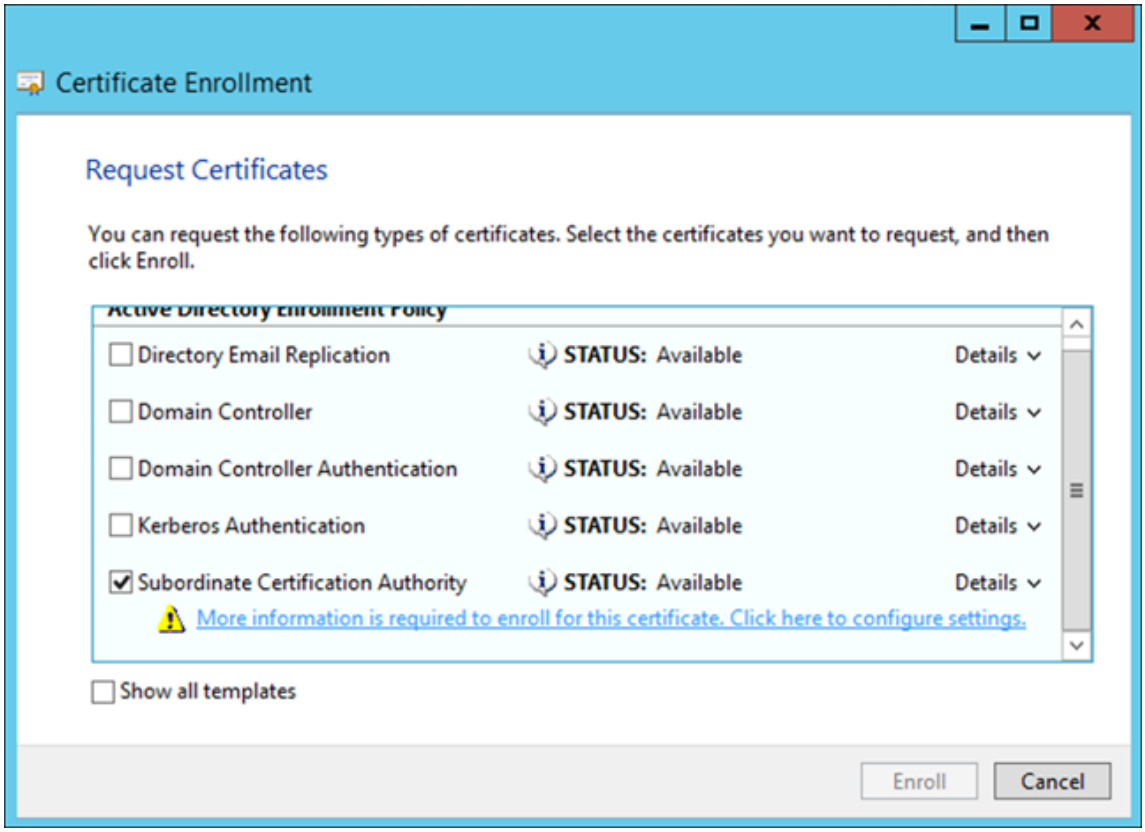
为您的 **CA** 生成和导入证书

1. 在服务器上，使用本地系统帐户打开 Microsoft 管理控制台 (MMC)，然后打开证书管理单元。在右侧窗格中，右键单击，然后单击 所有任务 **>** 请求新证书。



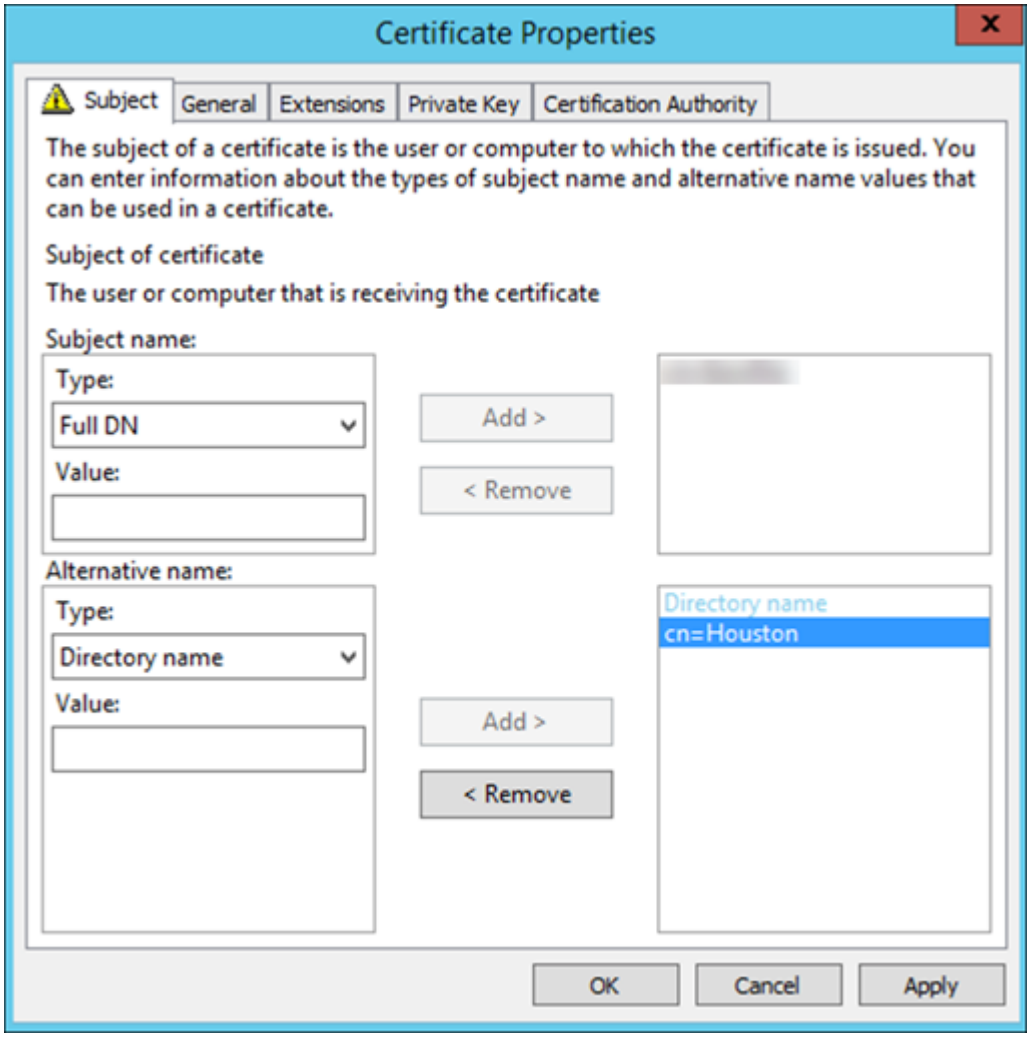
2. 在打开的向导中，单击 下一步两次。在 请求证书列表中，选择 从属证书颁发机构，然后单击 更多信息链接。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



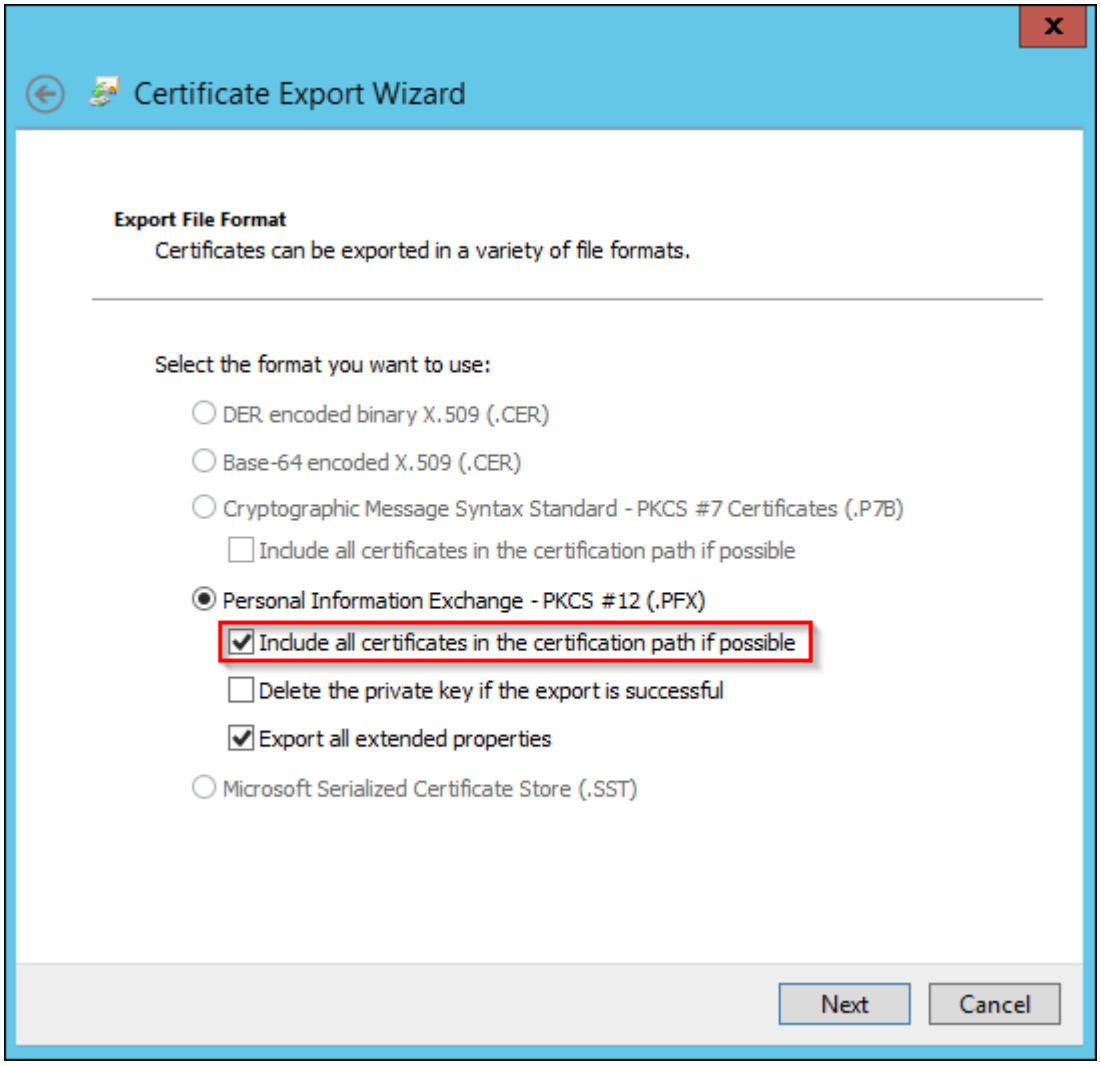
3. 在窗口中，键入 主题名称和 替代名称。单击确定。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

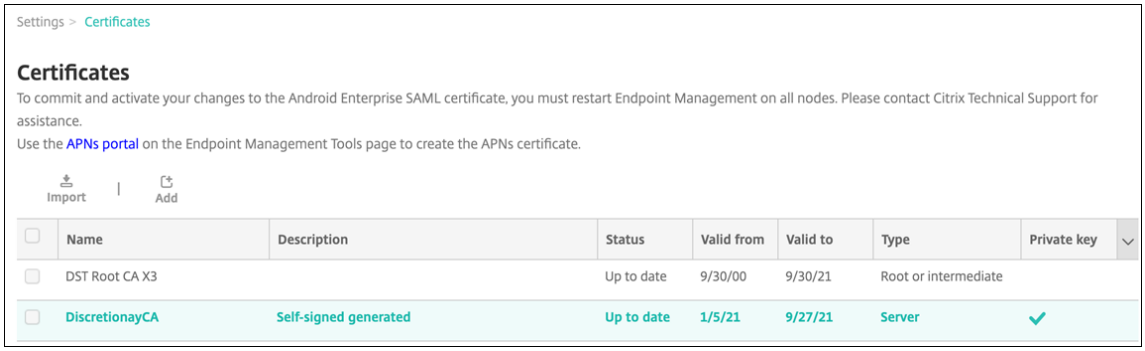


4. 单击 注册，然后单击 完成。
5. 在 MMC 中，右键单击您创建的证书。单击 所有任务 **>** 导出。将证书导出为带有私钥的.pfx 文件。如果可能，请选择在证书路径中包含所有证书的选项。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

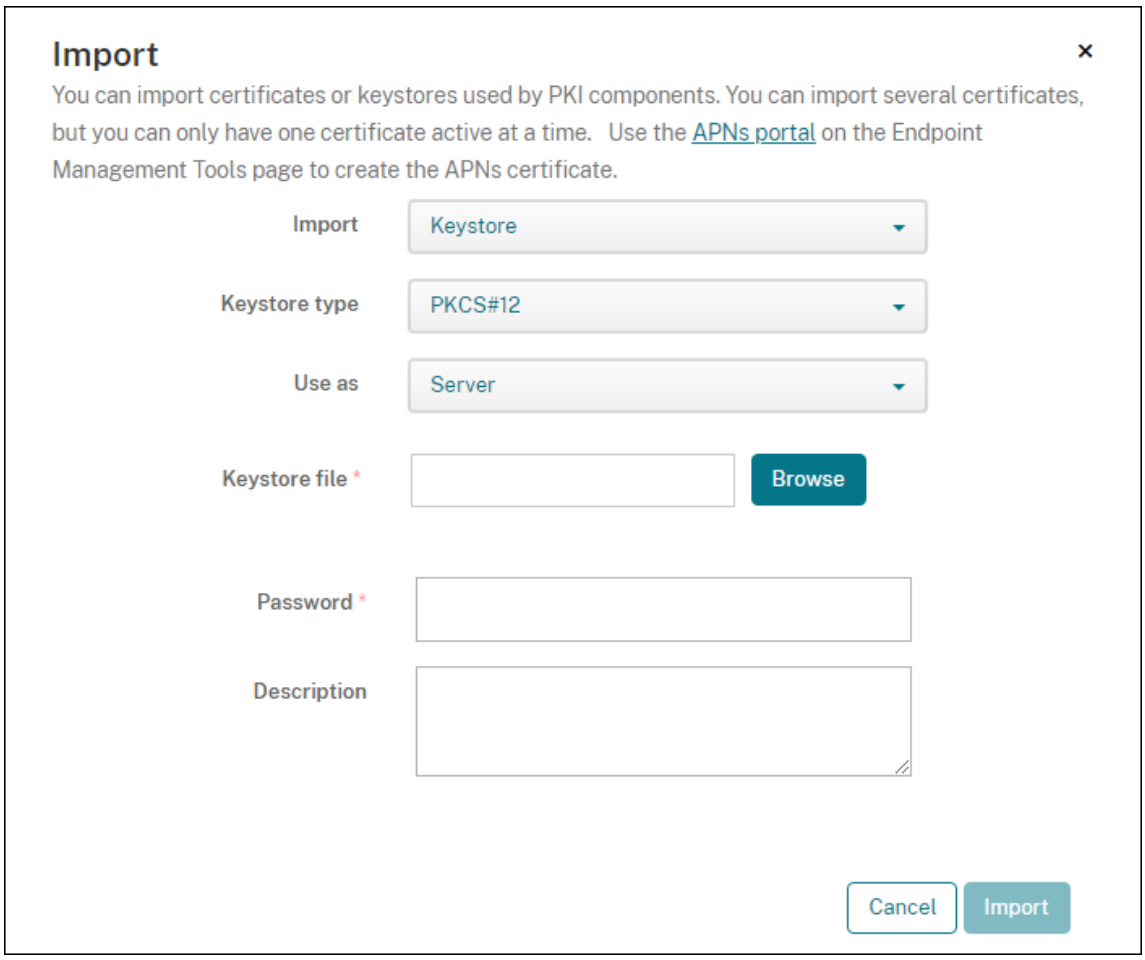


6. 在 Endpoint Management 控制台中，导航到 设置 **>** 证书。



7. 单击导入。在打开的窗口中，浏览以前导出的证书和私钥文件。

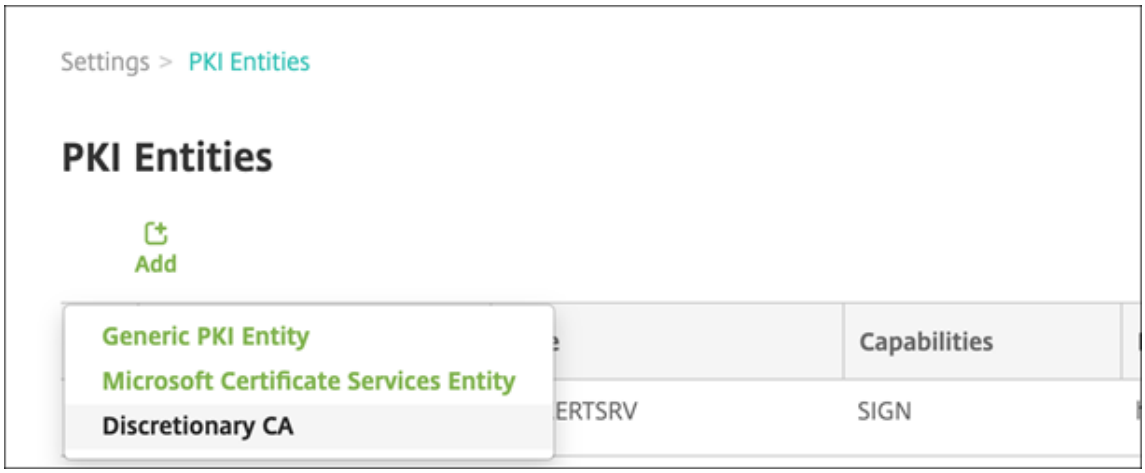
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



8. 单击导入。证书将添加到表中。

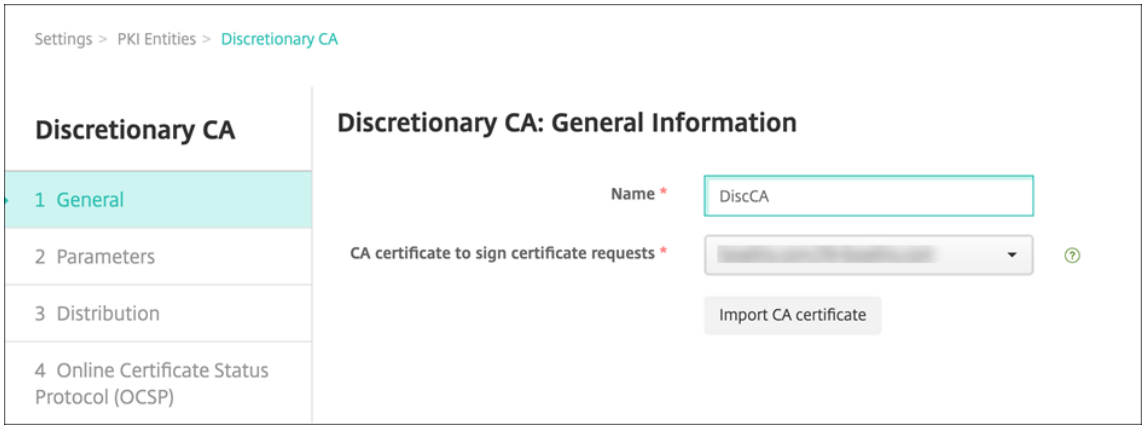
添加任意 **CA**

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标，然后单击更多 **> PKI** 实体。
2. 在 **PKI** 实体页面上，单击添加。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 单击任意 **CA**。

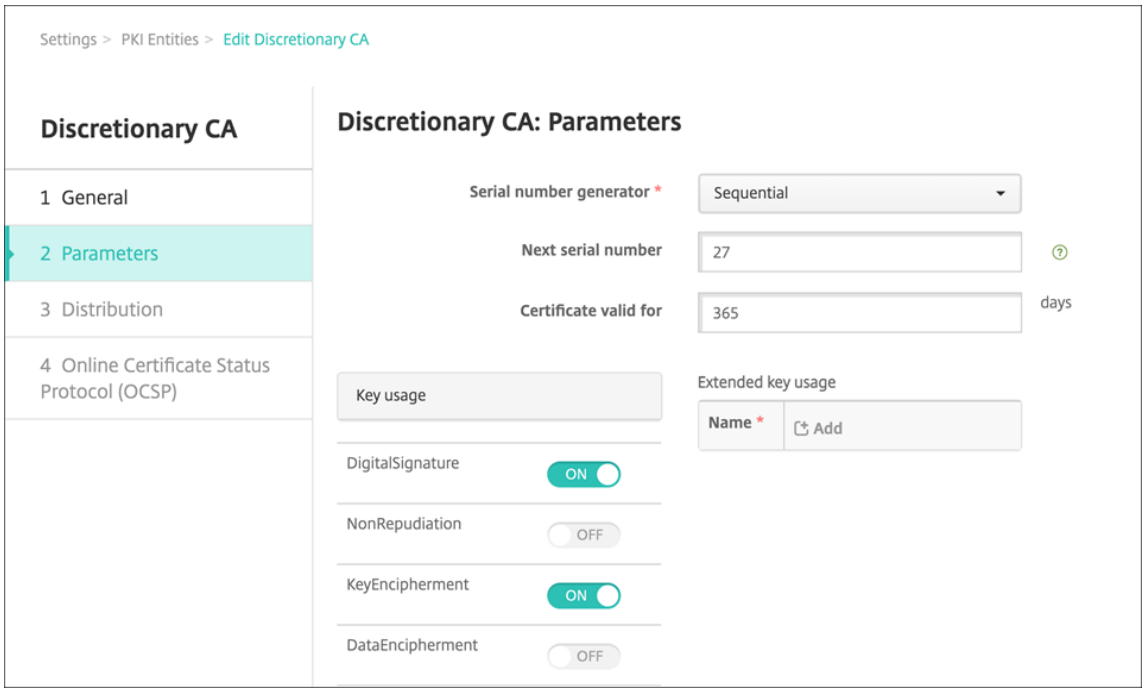


4. 在“ 自由裁量 **CA**：常规信息”页面上，配置以下内容：

   - 名称：键入任意 CA 的描述性名称。
   - 用于对证书请求进行签名的 **CA** 证书：单击任意 CA 用于为证书请求签名的证书。

     此证书列表是根据您通过配置 **>** 设置 **>** 证书上载到 Endpoint Management 的 CA 证书（带私钥）生成的。

5. 单击下一步。



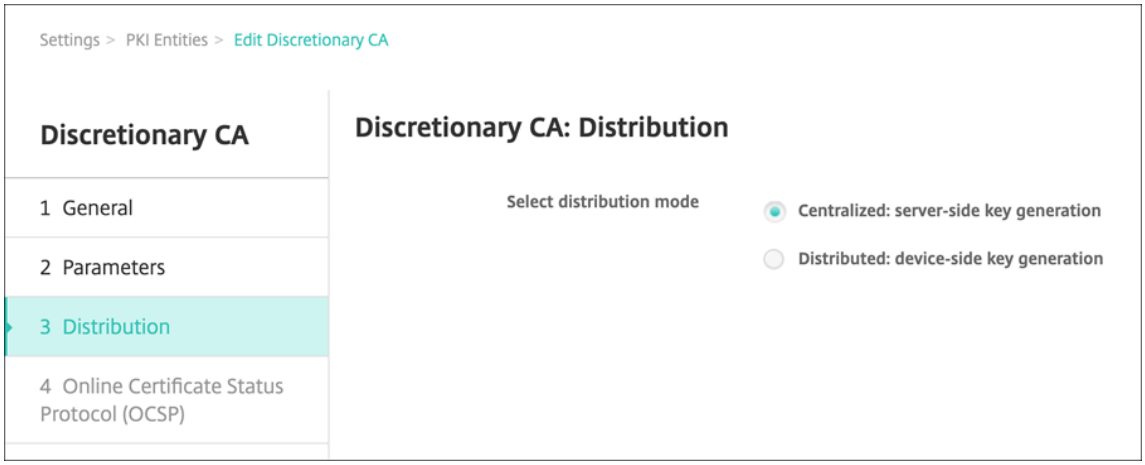
6. 在“ 自由 **CA**：参数”页面上，配置以下内容：

   - 序列号生成器：任意 CA 为其颁发的证书生成序列号。从此列表中，单击按顺序或不按顺序以确定序列号的生成方式。
   - 下一个序列号：键入一个用于确定颁发的下一个序列号的值。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 证书有效期：键入证书有效的天数。
- 密钥用法：通过将相应的密钥设置为开，标识任意 CA 所颁发证书的目的。一旦设置，CA 仅限于为此目的颁发证书。
- 扩展密钥用法：要添加更多参数，请单击添加，键入密钥名称，然后单击保存。

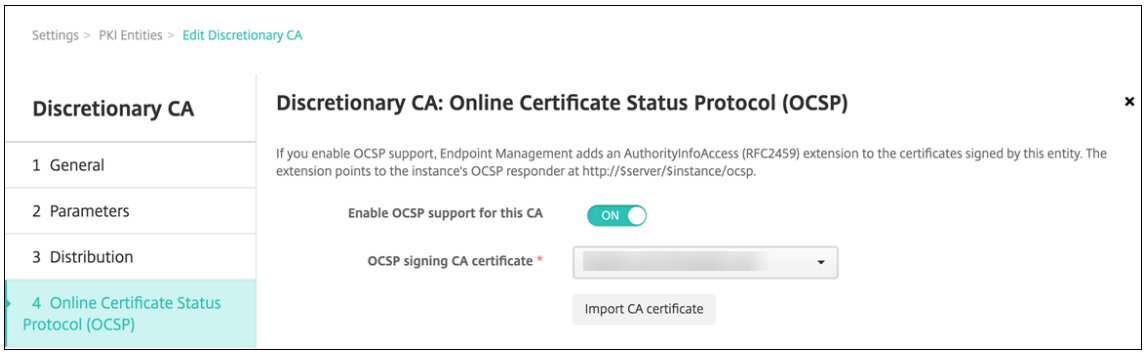
7. 单击下一步。



8. 在任意 **CA:** 分发页面上，选择分发模式：

- 集中式**:** 服务器端密钥生成。Citrix 建议使用集中选项。在服务器上生成并存储私钥，然后分发到用户设备。
- 分布式**:** 设备端密钥生成。私钥在用户设备上生成。此分布式模式使用 SCEP 并需要采用 **keyUsage keyEncryption** 扩展名的 RA 加密证书和采用 **KeyUsage digitalSignature** 扩展名的 RA 签名证书。同一个证书可以同时用于加密和签名。

9. 单击下一步。



10. 在 “ 自由授权 **CA**：在线证书状态协议 **(OCSP)** ” 页面上，配置以下内容：

- 如果要向此 CA 签名的证书添加 `AuthorityInfoAccess` (RFC2459) 扩展，请将为此 **CA** 启用 **OCSP** 支持设置为开。此扩展指向位于 `https://<server>/<instance>/ocsp` 的 CA OCSP 响应者。
- 如果启用了 OCSP 支持，请选择 OSCP 签名 CA 证书。此证书列表使用您上载到 Endpoint Management 的 CA 证书生成。

启用该功能使 Citrix ADC 有机会检查证书的状态。Citrix 建议您启用此功能。

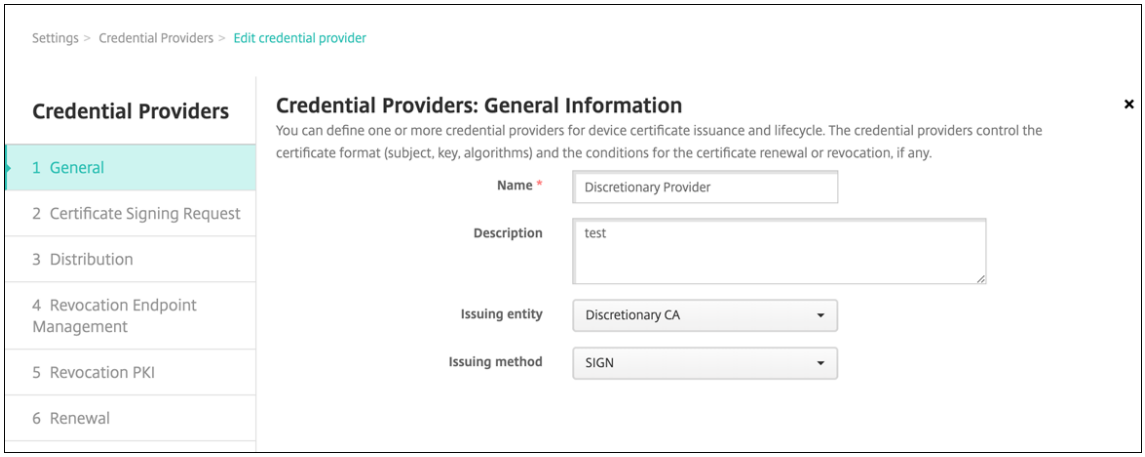
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

11. 单击保存。

    任意 CA 将显示在 PKI 实体表格中。

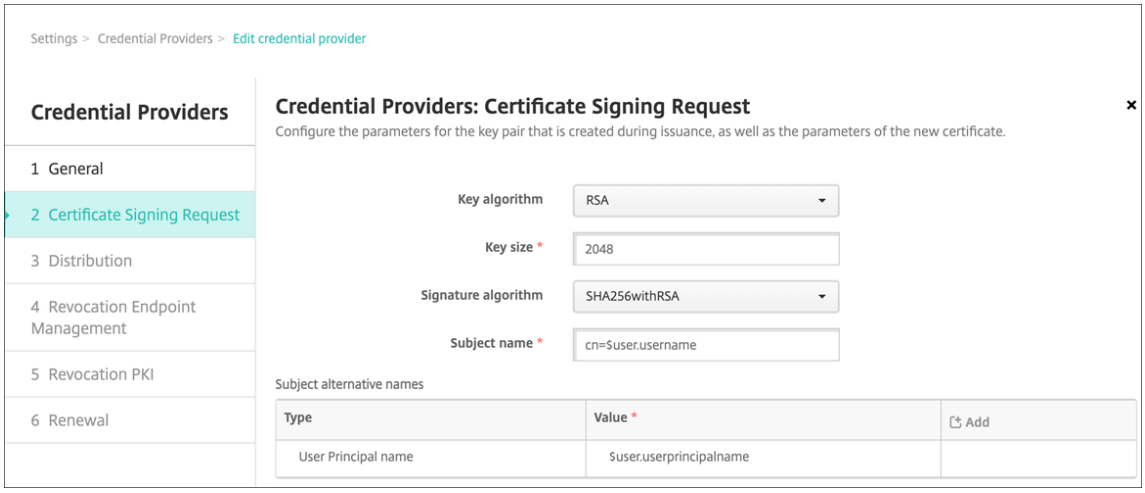
配置凭据提供程序

1. 在 Endpoint Management 控制台中，导航到 设置 **>** 凭据提供程序，然后单击 添加。
2. 在 凭据提供程序：常规信息页面上，配置以下内容：



   - 名称：为新提供程序配置键入唯一名称。此名称之后将用于在 Endpoint Management 控制台的其他部分标识该配置。
   - 说明：凭据提供程序的说明。尽管此字段为可选字段，但说明可以提供有关此凭据提供程序的有用详细信息。
   - 发行实体：选择 自行授权 **CA**。
   - 颁发方法：单击签名或提取以选择系统用于从已配置的实体获取证书的方法。对于客户端证书身份验证，请使用签名。

3. 单击下一步。在凭据提供程序**:** 证书签名请求页面上，根据您的证书配置来配置以下各项：



   - 密钥算法：选择用于获取新密钥对的密钥算法。可用值为 **RSA**、**DSA** 和 **ECDSA**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

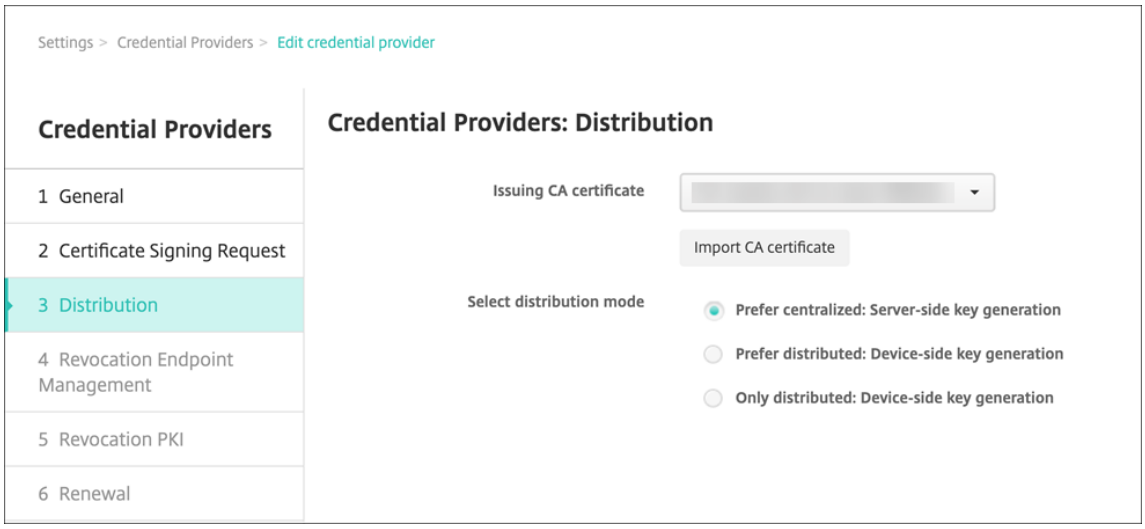
- 密钥大小：键入密钥对的大小（以位为单位）。此字段为必填字段。Citrix 建议使用 **2048** 位。
- 签名算法：单击用于新证书的值。值取决于密钥算法。Citrix 建议使用 **SHA256withRSA**。
- 使用者名称：必填。键入新证书使用者的标识名 (DN)。使用 `CN=${ user.username }` 作为用户名或 `CN=${ user.samaccountname }` 以使用 samAccountName。
- 要向使用者备用名称表中添加新条目，请单击添加。选择备用名称的类型，然后在第二列中键入一个值。

  添加以下内容：

  - 类型：用户主体名称
  - 值：`$user.userprincipalname`

  与主题名称一样，您可以在值字段中使用 Endpoint Management 宏。

4. 单击下一步。在 凭据提供程序：分发页面上，配置以下内容：

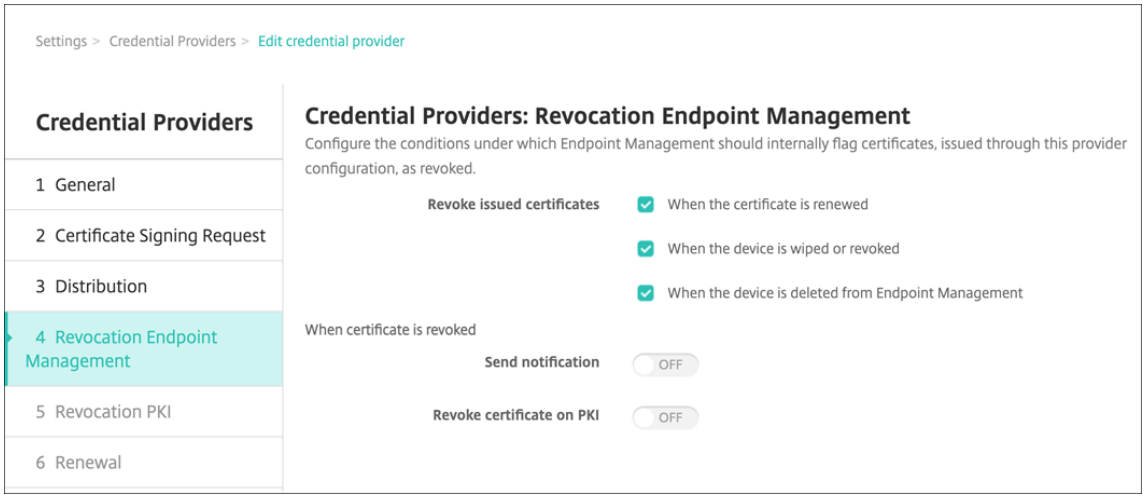


- 颁发 **CA** 证书：选择之前添加的自行授权 CA 证书。
- 选择分发模式：选择以下生成和分发密钥的方法之一：
  - 首选集中式**:** 服务器端密钥生成： Citrix 建议采用此集中式选项。它支持 Endpoint Management 支持的所有平台，并且在使用 Citrix Gateway 身份验证时也需要使用此模式。在服务器上生成并存储私钥，然后分发到用户设备。
  - 首选分布式**:** 设备端密钥生成：在用户设备上生成并存储私钥。此分布式模式使用 SCEP 并需要采用 keyUsage keyEncryption 的 RA 加密证书和采用 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可以同时用于加密和签名。
  - 仅分布式：设备端密钥生成：此选项与 “ 首选分布式：设备端密钥生成” 相同，但是如果设备端密钥生成失败或不可用，则没有选项可用。

  如果选择首选分布式**:** 设备端密钥生成或仅限分布式**:** 设备端密钥生成，请单击 RA 签名证书和 RA 加密证书。同一个证书可用于这两个目的。此时将显示有关这些证书的新字段。

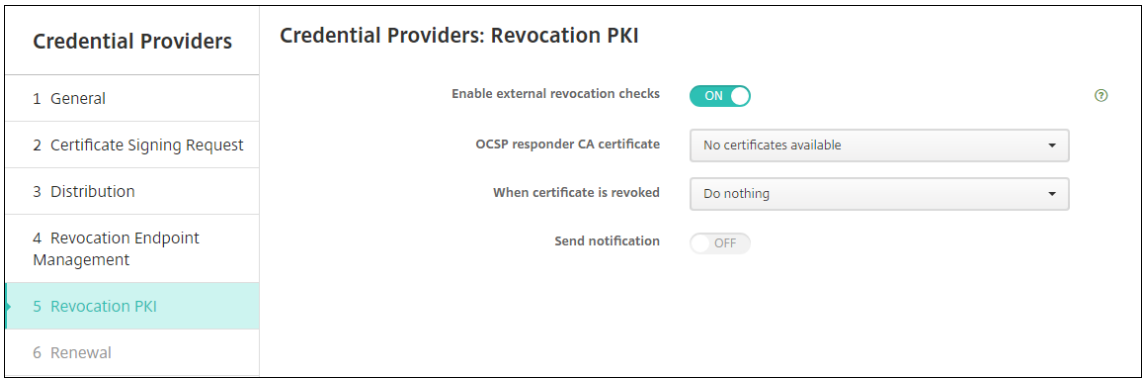
5. 单击下一步。在 凭据提供程序：吊销 **Endpoint Management** 页面上，配置 Endpoint Management 内部将通过此提供程序配置颁发的证书标记为已撤销的条件。配置以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 在吊销已颁发的证书中，选择一个表明何时应吊销证书的选项。
- 要指示 Endpoint Management 在吊销证书时发送通知，请将发送通知的值设置为开并选择通知模板。
- 使用 Endpoint Management 作为自行决定 **PKI** 时，撤销 **PKI** 上的证书不起作用。

6. 单击下一步。在 凭据提供程序：吊销 **PKI** 页面上，确定如果证书被吊销，应对 PKI 采取哪些操作。您还可以选择创建通知消息。配置以下设置：



- 启用外部撤销检查：打开此 设置。此时将显示更多与吊销 PKI 相关的字段。
- 在 **OCSP** 响应方 **CA** 证书列表中，选择证书主题的判别名称 (DN)。

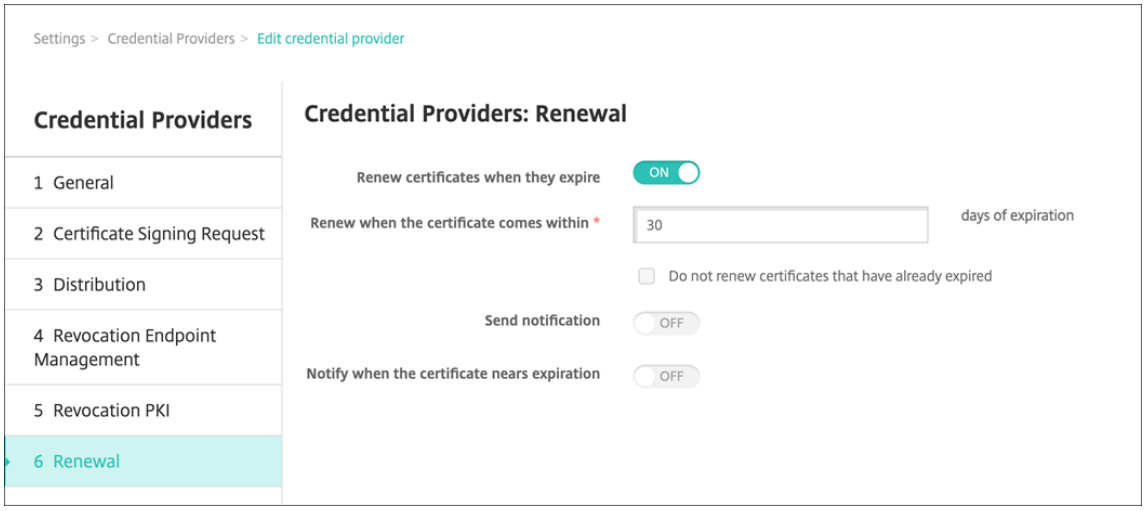
  可以为 DN 字段值使用 Endpoint Management 宏。例如：`CN=${ user.username } , OU =${ user.department } , O=${ user.companyname } , C=${ user.c } \ endquotation`
- 在吊销证书时列表中，单击吊销证书时对 PKI 实体执行的以下操作之一：
  - 不执行任何操作。
  - 续订证书。
  - 吊销和擦除设备。
- 要指示 Endpoint Management 在吊销证书时发送通知，请将发送通知的值设置为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可以从两个通知选项中选择：

- 如果选择选择通知模板，则可以选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
- 如果选择输入通知详细信息，则可以自行编写通知消息。除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

7. 单击下一步。在 凭据提供商：续订页面上，配置以下内容：



将 证书过期时续订设置为 开。此时将显示更多字段。

- 在证书在此时间内提供时续订字段中，键入在过期前多少天续订证书。
- （可选）选择不续订已过期的证书。在此情况下，“已过期”表示证书的“`NotAfter`”日期在过去，不是指证书已被吊销。在内部吊销证书后，Endpoint Management 不会续订这些证书。

要指示 Endpoint Management 在续订证书时发送通知，请将发送通知设置为开。要指示 Endpoint Management 在证书接近过期时发送通知，请将证书即将过期时通知设置为开。

对于其中任一选择方式，可以从两个通知选项中选择：

- 选择通知模板：选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
- 输入通知详细信息：自行编写通知消息。提供收件人电子邮件地址、消息和频率，以便发送通知。

8. 单击保存。

凭据提供程序

May 19, 2022

凭据提供程序是在 Endpoint Management 系统的各个部分中使用的实际证书配置。凭据提供程序定义证书的来源、参数和生命周期。无论这些证书是设备配置的一部分还是独立的配置（即，按原样推送到设备），都是这样。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备注册约束证书生命周期。也就是说，Endpoint Management 在注册前不颁发证书，尽管 Endpoint Management 可能会在注册的过程中颁发某些证书。此外，在某个注册环境下从内部 PKI 颁发的证书会在注册被吊销时吊销。管理关系终止后，不保留任何有效证书。

一个凭据提供程序配置可用于多个位置，从而达到通过一个配置同时控制任意多个证书的效果。这时，其唯一性在于部署资源和部署。例如，如果凭据提供程序 P 作为配置 C 的一部分部署到设备 D：P 的颁发设置将决定部署到 D 的证书。同样，在更新 C 时将应用 D 的续订设置。并且，删除 C 或吊销 D 时将应用 D 的吊销设置。

根据这些规则，Endpoint Management 中的凭据提供程序配置确定以下各项：

- 证书的来源。
- 获取证书的方法：签发新证书还是提取（恢复）现有证书和密钥对。
- 用于颁发或恢复的参数。例如，密钥大小、密钥算法和证书扩展名等证书签名请求 (CSR) 参数。
- 将证书交付给设备的方式。
- 吊销条件。尽管在管理关系终止后 Endpoint Management 中的所有证书都将被吊销，但该配置可以指定在更早时间吊销。例如，配置可以指定在删除关联设备配置时吊销证书。此外，在某些情况下，Endpoint Management 中关联证书的吊销可能会发送给后端公钥基础结构 (PKI)。也就是说，在 Endpoint Management 中吊销证书可能导致在 PKI 上吊销证书。
- 续订设置。通过指定凭据提供程序获取的证书可以在即将过期时自动续订。或者采用与之不同的方式，在接近过期时由系统发送通知。

配置选项的可用性主要取决于为凭据提供程序选择的 PKI 实体的类型和颁发方法。

证书颁发方法

可以通过签名获得证书，也就是所谓的颁发方法。

利用此方法，颁发包括创建新私钥、创建 CSR 和将 CSR 提交给证书颁发机构 (CA) 进行签名。Endpoint Management 支持 MS 证书服务实体和任意 CA 实体的签名方法。

凭据提供程序使用签名颁发方法。

证书交付

Endpoint Management 中可用的证书交付模式共有两种：集中和分散。分布式模式使用简单证书注册协议 (SCEP)，并且只有在客户端支持该协议时方可使用（仅限 iOS）。在某些情况下，必须采用分布式模式。

对于支持分散式（SCEP 辅助）交付的凭据提供程序，需要特殊的配置步骤：设置注册机构 (RA) 证书。需要 RA 证书是因为，使用 SCEP 协议时，Endpoint Management 充当实际证书颁发机构的委派者（注册者）。Endpoint Management 必须向客户端证实自己有权执行此类操作。通过向 Endpoint Management 上载上述证书，可以建立该机构。

需要两种不同的证书角色（尽管同一证书即可满足这两项要求）：RA 签名和 RA 加密。这些角色的限制如下：

- RA 签名证书必须拥有 X.509 密钥用法数字签名。
- RA 加密证书必须拥有 X.509 密钥用法密钥加密。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要配置凭据提供程序的 RA 证书，请先将证书上载到 Endpoint Management，然后在凭据提供程序中链接到这些证书。

仅当凭据提供程序为证书角色配置了证书时，才可将凭据提供程序视为支持分散式交付。可以将每个凭据提供程序配置为首选集中式模式、首选分布式模式或要求分布式模式。实际结果取决于具体环境：如果环境不支持分布式模式，但是凭据提供程序要求使用该模式，部署将失败。同样，如果环境要求使用分布式模式，但凭据提供程序不支持该模式，部署也将失败。在所有其他情况下，将会应用首选设置。

下面显示了 SCEP 在整个 Endpoint Management 的分布：

上下文	支持 SCEP	需要 SCEP
iOS 配置文件服务	是	是
iOS 移动设备管理注册	是	否
iOS 配置文件	是	否
SHTP 注册	否	否
SHTP 配置	否	否
Windows Tablet 注册	否	否
Windows Tablet 配置	不可以，但 Windows 10 和 Windows 11 版本支持的网络设备策略除外	否

证书吊销

有三种类型的吊销。

- 内部吊销：内部吊销影响由 Endpoint Management 维护的证书状态。重新评估提供的证书时，或者提供证书的 OCSP 状态信息时，Endpoint Management 会考虑此状态。凭据提供程序配置决定在各种条件下此状态受到的影响。例如，凭据提供程序可以指定从设备中删除证书后将这些证书标记为已吊销。
- 外部传播的吊销：又称 “吊销 Endpoint Management”，这种类型的吊销适用于从外部 PKI 获取的证书。在凭据提供程序配置定义的条件下，Endpoint Management 在内部吊销证书时也会在 PKI 上吊销该证书。
- 外部引起的吊销：又称 “吊销 PKI”，这种类型的吊销也仅适用于从外部 PKI 获取的证书。每次 Endpoint Management 评估指定证书的状态时，Endpoint Management 都将向 PKI 查询该状态。如果证书已吊销，Endpoint Management 将在内部吊销该证书。此机制使用 OCSP 协议。

这三种类型并不互斥，而是可以一起应用。外部吊销或独立查询结果可能会导致内部吊销。内部吊销会潜在影响外部吊销。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

证书续订

证书续订由吊销现有证书和颁发另一个证书两个过程组成。

Endpoint Management 将首先尝试获取新证书，然后再吊销之前的证书，以避免在颁发失败时造成服务中断。如果采用分散式（支持 SCEP）交付，仅当证书成功安装到设备后再进行吊销。否则，将在新证书发送给设备之前进行吊销。这种吊销与证书是否安装成功无关。

配置吊销时，需要指定特定的持续时间（天）。如果设备已连接，服务器将验证证书的“`NotAfter`”日期是否晚于当前日期减去指定的持续时间。如果证书满足该条件，Endpoint Management 将尝试续订该证书。

创建凭据提供程序

凭据提供程序的配置方式有多种，主要取决于为其选择的颁发实体和颁发方法。可以将使用内部实体或外部实体的凭据提供程序区分开来：

- 任意实体属于内部实体，位于 Endpoint Management 内部。任意实体的颁发方法始终为签名。签名意味着，在执行每个颁发操作时，Endpoint Management 都将使用为该实体选择的 CA 证书给新密钥对签名。该密钥对是在设备上生成还是在服务器上生成取决于所选的分发方法。
- 外部实体包括 Microsoft CA，属于您的企业基础结构的一部分。

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标，然后单击设置 **>** 凭据提供程序。
2. 在凭据提供程序页面上，单击添加。

   此时将显示凭据提供程序**:** 常规信息页面。
3. 在凭据提供程序**:** 常规信息页面上，执行以下操作：
   - 名称：为新提供程序配置键入唯一名称。此名称之后将用于在 Endpoint Management 控制台的其他部分标识该配置。
   - 说明：凭据提供程序的说明。尽管此字段为可选字段，但说明可以提供有关此凭据提供程序的有用详细信息。
   - 颁发实体：单击凭据颁发实体。
   - 颁发方法：单击签名或提取以选择系统用于从已配置的实体获取证书的方法。对于客户端证书身份验证，请使用签名。
   - 如果模板列表可用，请为凭据提供程序选择您在 PKI 实体下添加的模板。

     在设置 **> PKI** 实体中添加 Microsoft 证书服务实体时，这些模板将变为可用。
4. 单击下一步。

   此时将显示凭据提供程序**:** 证书签名请求页面。
5. 在凭据提供程序**:** 证书签名请求页面上，根据您的证书配置来配置以下各项：
   - 密钥算法：选择用于获取新密钥对的密钥算法。可用值为 **RSA**、**DSA** 和 **ECDSA**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 密钥大小：键入密钥对的大小（以位为单位）。此字段为必填字段。

  允许的值取决于密钥类型。例如，DSA 密钥的最大大小为 2048 位。为避免出现错误的负值（取决于基础硬件和软件），Endpoint Management 不强制实施密钥大小。应始终先在测试环境中测试凭据提供程序配置，然后在生产环境中激活这些配置。

- 签名算法：单击用于新证书的值。值取决于密钥算法。

- 使用者名称：必填。键入新证书使用者的标识名 (DN)。例如：
  `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

  For example, for client certificate authentication, use these settings:

  - **Key algorithm:** RSA
  - **Key size:** 2048
  - **Signature algorithm:** SHA256withRSA
  - **Subject name:** `cn=$user.username`

- 要向使用者备用名称表中添加新条目，请单击添加。选择备用名称的类型，然后在第二列中键入一个值。

  对于客户端证书身份验证，请指定以下设置：

  - 类型：用户主体名称
  - 值：`$user.userprincipalname`

    与“使用者名称”相同，可以在值字段中使用 Endpoint Management 宏。

6. 单击下一步。

   此时将显示凭据提供程序**:** 分发页面。

7. 在凭据提供程序**:** 分发页面上，执行以下操作：

   - 在颁发 **CA** 证书列表中，单击提供的 CA 证书。由于凭据提供程序使用任意 CA 实体，因此该凭据提供程序的 CA 证书将始终为在该实体上配置的 CA 证书。CA 证书在此显示是为了与使用外部实体的配置保持一致。
   - 在选择分发模式中，单击以下生成和分发密钥方式中的一种：
     - 首选集中式**:** 服务器端密钥生成： Citrix 建议采用此集中式选项。它支持 Endpoint Management 支持的所有平台，并且在使用 Citrix Gateway 身份验证时也需要使用此模式。在服务器上生成并存储私钥，然后分发到用户设备。
     - 首选分布式**:** 设备端密钥生成：在用户设备上生成并存储私钥。此分布式模式使用 SCEP 并需要采用 keyUsage keyEncryption 的 RA 加密证书和采用 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可以同时用于加密和签名。
     - 仅限分布式**:** 设备端密钥生成：此选项与“首选分布式: 设备端密钥生成”的工作方式相同，但是此选项是“仅限”而非“首选”，当设备端生成密钥失败或不可用时，没有其他选项可用。

   如果选择首选分布式**:** 设备端密钥生成或仅限分布式**:** 设备端密钥生成，请单击 RA 签名证书和 RA 加密证书。同一个证书可用于这两个目的。此时将显示有关这些证书的新字段。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

8. 单击下一步。

   此时将显示凭据提供程序**:** 吊销 **Endpoint Management** 页面。在此页面上，配置 Endpoint Management 在内部将通过此提供程序配置颁发的证书标记为吊销的条件。

9. 在凭据提供程序**:** 吊销 **Endpoint Management** 页面上，执行以下操作：

   - 在吊销已颁发的证书中，选择一个表明何时应吊销证书的选项。
   - 要指示 Endpoint Management 在吊销证书时发送通知，请将发送通知的值设置为开并选择通知模板。
   - 要在从 Endpoint Management 吊销证书后在 PKI 上吊销该证书，请将吊销 **PKI** 上的证书设置为开，并在实体列表中，单击某个模板。实体列表将显示具有吊销功能的所有可用实体。从 Endpoint Management 吊销证书后，吊销调用将发送给在实体列表中选择的 PKI。

10. 单击下一步。

    此时将显示凭据提供程序**:** 吊销 **PKI** 页面。请在此页面上指出吊销证书时应对 PKI 执行的操作。您还可以选择创建通知消息。

11. 在凭据提供程序**:** 吊销 **PKI** 页面上，如果要从 PKI 吊销证书，请执行以下操作：

    - 将启用外部吊销检查设置更改为开。此时将显示更多与吊销 PKI 相关的字段。
    - 在 **OCSP** 响应者 **CA** 证书列表中，单击证书使用者的标识名 (DN)。

      可以为 DN 字段值使用 Endpoint Management 宏。例如：`CN=${ user.username } , OU =${ user.department } , O=${ user.companyname } , C=${ user.c } \ endquotation`

    - 在吊销证书时列表中，单击吊销证书时对 PKI 实体执行的以下操作之一：
      - 不执行任何操作。
      - 续订证书。
      - 吊销和擦除设备。
    - 要指示 Endpoint Management 在吊销证书时发送通知，请将发送通知的值设置为开。

      可以从两个通知选项中选择：

    - 如果选择选择通知模板，则可以选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
    - 如果选择输入通知详细信息，则可以自行编写通知消息。除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

12. 单击下一步。

    此时将显示凭据提供程序**:** 续订页面。在此页面上，可以将 Endpoint Management 配置为执行以下操作：

    - 续订证书。可以选择在续订时发送通知，以及选择从操作中排除已过期的证书。
    - 为即将过期的证书发送通知（续订前通知）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

13. 在凭据提供程序**:** 续订页面上，如果要在证书过期时进行续订，请执行以下操作：

    将在证书过期时续订设置为开。此时将显示更多字段。

    - 在证书在此时间内提供时续订字段中，键入在过期前多少天续订证书。
    - （可选）选择不续订已过期的证书。在此情况下，“已过期”表示证书的“NotAfter”日期在过去，不是指证书已被吊销。在内部吊销证书后，Endpoint Management 不会续订这些证书。

    要指示 Endpoint Management 在续订证书时发送通知，请将发送通知设置为开。要指示 Endpoint Management 在证书接近过期时发送通知，请将证书即将过期时通知设置为开。
    对于其中任一选择方式，可以从两个通知选项中选择：

    - 选择通知模板：选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
    - 输入通知详细信息：自行编写通知消息。提供收件人电子邮件地址、消息和频率，以便发送通知。

    在证书在此时间内提供时通知字段中，键入在证书过期前多少天发送通知。

14. 单击保存。

    凭据提供程序将显示在“凭据提供程序”表中。

APNs 证书

July 7, 2023

要在 Endpoint Management 中注册并管理 Apple 设备，请设置 Apple 提供的 Apple 推送通知服务 (APNs) 证书。该证书通过 Apple 推送网络实现移动设备管理。

工作流程摘要：

步骤 **1**：通过以下任一方法创建证书签名请求 (CSR)：

- 在 macOS 上使用钥匙串访问创建 CSR （Citrix 推荐）
- 使用 Microsoft IIS 创建 CSR
- 使用 OpenSSL 创建 CSR

步骤 **2**：在 Endpoint Management 工具中签署 CSR

步骤 **3**：将签名的 CSR 提交给 Apple 以获取 APNs 证书

步骤 **4**：使用执行步骤 1 的同一台计算机，完成 CSR 并导出 PKCS #12 文件：

- 在 macOS 上使用钥匙串访问创建 PKCS #12 文件
- 使用 Microsoft IIS 创建 PKCS #12 文件
- 使用 OpenSSL 创建 PKCS #12 文件

步骤 **5**：将APNs 证书导入 Endpoint Management

步骤 **6**： 续订 APNs 证书

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

创建证书签名请求

我们建议您在 macOS 上使用钥匙串访问来创建 CSR。还可以通过 Microsoft IIS 或 OpenSSL 创建 CSR。

> 重要：
>
> - 对于用于创建证书的 Apple ID：
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.
>   - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device re-enrollment.
> - 如果您无意或有意吊销了该证书，则无法管理自己的设备。
> - 如果使用 iOS Developer Enterprise Program 创建移动设备管理器推送证书：请务必在 Apple Push Certificates Portal 中处理面向迁移的证书的任何操作。

在 **macOS** 上使用钥匙串访问创建 **CSR**

1. 在运行 macOS 的计算机上，在应用程序 **>** 实用工具下方，启动钥匙串访问应用程序。
2. 打开钥匙串访问菜单，然后单击证书助理 **>** 从证书颁发机构请求证书。
3. “证书助理”将提示您输入以下信息：
   - 电子邮件地址：管理证书的个人或角色帐户的电子邮件地址。
   - 常用名称：管理证书的个人或角色帐户的公用名称。
   - **CA** 电子邮件地址：证书颁发机构的电子邮件地址。
4. 选择存储到磁盘和让我指定密钥对信息选项，然后单击继续。
5. 输入 CSR 文件的名称，在您的计算机上保存此文件，然后单击保存。
6. 指定密钥对信息：选择密钥大小 2048 位以及 **RSA** 算法，然后单击继续。作为 APNs 证书流程的一部分，CSR 文件已可供上载。
7. 证书助理完成 CSR 流程后，单击完成。
8. 要继续，请签署 CSR。

使用 **Microsoft IIS** 创建 **CSR**

生成 APNs 证书请求的第一步是创建证书签名请求 (CSR)。对于 Windows，请通过使用 Microsoft IIS 生成 CSR。

1. 打开 Microsoft IIS。
2. 双击 IIS 的服务器证书图标。
3. 在服务器证书窗口中，单击创建证书申请。
4. 键入适当的唯一判别名 (DN) 信息。例如，您可以键入 Endpoint Management 服务器的完全限定域名 (FQDN)，例如 `www.domain.com`。然后，单击下一步。
5. 为加密服务提供程序选择 **Microsoft RSA SChannel Cryptographic Provider**，并为位长度选择 **2048**，然后单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. 输入文件名并指定 CSR 的保存位置，然后单击完成。
7. 要继续，请签署 CSR。

使用 **OpenSSL** 创建 **CSR**

如果无法使用 macOS 设备或 Microsoft IIS 生成 CSR，请使用 OpenSSL。可以从 OpenSSL Web 站点下载并安装 OpenSSL。

1. 在安装 OpenSSL 的计算机上，通过命令提示符或 shell 运行以下命令。

```
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.
csr -newkey rsa:2048
```

2. 此时将显示以下要求证书命名信息的消息。根据请求输入信息。

```
1  You are about to be asked to enter information that will be
       incorporated into your certificate request.
2  What you are about to enter is what is called a Distinguished Name
       or a DN.
3  There are quite a few fields but you can leave some blank
4  For some fields there will be a default value,
5  If you enter '.', the field will be left blank.
6  -----
7  Country Name (2 letter code) [AU]:US
8  State or Province Name (full name) [Some-State]:CA
9  Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
       Customer
11 Organizational Unit Name (eg, section) [:Marketing
12 Common Name (eg, YOUR name) []:John Doe
13 Email Address []:john.doe@customer.com
14 <!--NeedCopy-->
```

3. 在下一条消息中，输入 CSR 私钥的密码。

```
1  Please enter the following 'extra' attributes
2  to be sent with your certificate request
3  A challenge password []:
4  An optional company name []:
5  <!--NeedCopy-->
```

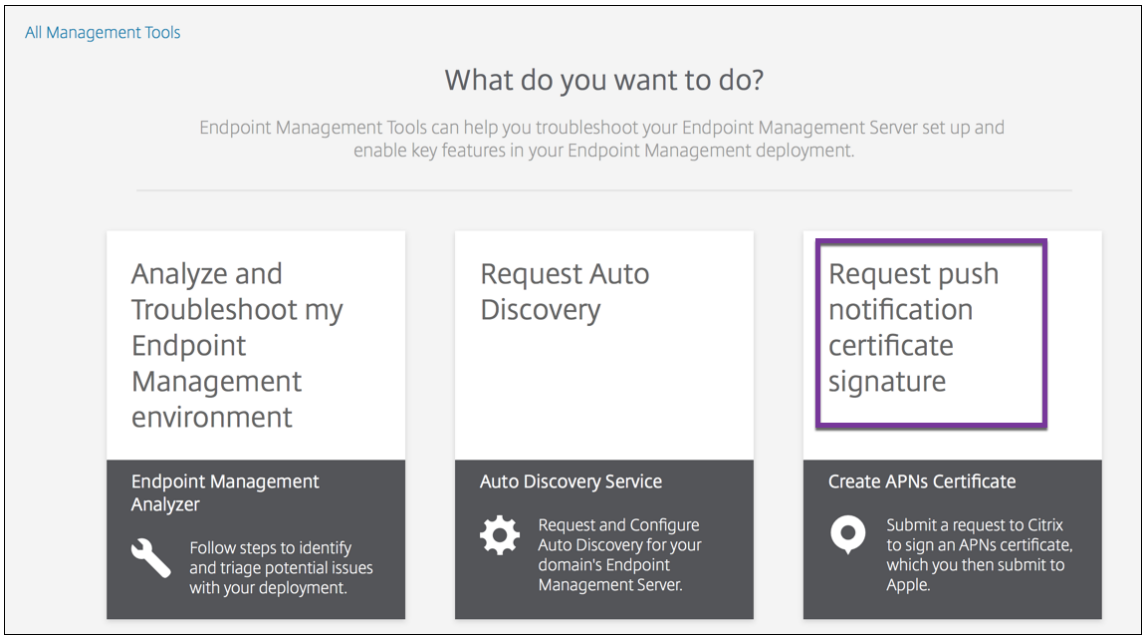
4. 要继续，请按照下一节中的说明为 CSR 签名。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

为 **CSR** 签名

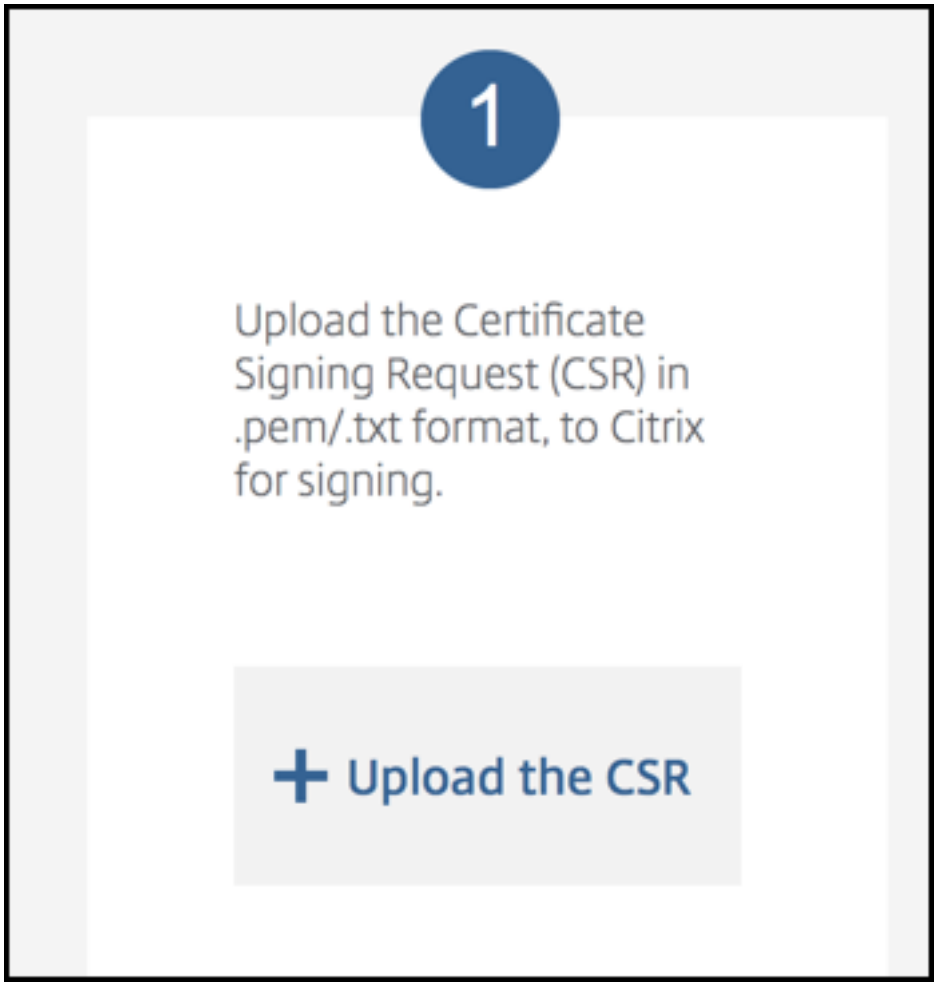
要将证书与 Endpoint Management 一起使用，必须将其提交给 Citrix 进行签名。Citrix 使用其移动设备管理签名证书给 CSR 签名并返回 `.plist` 格式的已签名文件。

1. 在浏览器中，转到 Endpoint Management 工具 网站，然后单击 请求推送通知证书签名。



2. 在创建新证书页面上，单击上载 **CSR**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 浏览并选择证书。

   > 重要：
   >
   > 证书必须为.pem/txt 格式。如果需要，通过右键单击并重命名该文件，将证书的文件扩展名更改为.pem 或.txt。

4. 在 **Endpoint Management APNs CSR Signing**（Endpoint Management APNs CSR 签名）页面上，单击 **Sign**（签名）。将为 CSR 签名并将签名后的 CSR 自动保存到已配置的下载文件夹。

5. 要继续，请按照下一节中的说明提交签名的 CSR。

将签名后的 **CSR** 提交给 **Apple** 以获取 **APNs** 证书

收到 Citrix 签名的证书签名请求 (CSR) 后，将 CSR 提交给 Apple 以获取导入 Endpoint Management 所需的 APNs 证书。

> 注意：
>
> 有些用户报告登录 Apple 推送门户时遇到问题。作为替代方法，您可以登录 Apple 开发者门户。然后，您可以按

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 照以下步骤进行操作：

1. 在浏览器中，转到 Apple 推送证书门户。
2. 单击 **Create a Certificate**（创建证书）。
3. 首次使用 Apple 创建证书：选中 **I have read and agree to these terms and conditions**（我已阅读并同意这些条款和条件）复选框，然后单击 **Accept**（接受）。
4. 单击 **Choose File**（选择文件），浏览到计算机上已签名的 CSR，然后单击 **Upload**（上载）。此时将显示一条确认消息，指示上载成功。
5. 单击 **Download**（下载）以检索.pem 证书。
6. 要继续，请完成 CSR 并导出 PKCS #12 文件，如下一节中所述。

完成 **CSR** 并导出 **PKCS #12** 文件

收到 Apple 提供的 APNs 证书后，返回到钥匙串访问、Microsoft IIS 或 OpenSSL 以将证书导出到 PCKS #12 文件中。

PKCS #12 文件包含 APNS 证书文件和您的私钥。PFX 文件的扩展名通常为.pfx 或.p12。可以互换使用.pfx 和.p12 文件。

> 重要：
>
> Citrix 建议您保存或导出本地系统中的个人密钥和公钥。您需要密钥来访问 APNs 证书以便重复使用。如果没有相同的密钥，您的证书无效，您必须重复执行整个 CSR 和 APNs 过程。

在 **macOS** 上使用钥匙串访问创建 **PKCS #12** 文件

> 重要：
>
> 在此任务中使用的 macOS 设备应与生成 CSR 时使用的 macOS 设备相同。

1. 在设备上，找到从 Apple 收到的生产标识 (.pem) 证书。
2. 启动钥匙串访问应用程序并导航到登录 **>** 我的证书选项卡。将产品标识证书拖放到打开的窗口中。
3. 单击证书并展开左箭头以验证证书是否包含关联的私钥。
4. 要开始将证书导出到 PCKS #12 (.pfx) 证书中，请选择证书和私钥，单击鼠标右键，然后选择导出 **2** 个项目。
5. 使用唯一的名称为证书文件命名，以便在 Endpoint Management 中使用。请勿在名称中包含空格字符。然后，为保存的证书选择一个文件夹位置，选择.pfx 文件格式，然后单击保存。
6. 输入用于导出证书的密码。Citrix 建议使用具有唯一性的强密码。还要确保证书和密码的安全性，以供以后使用和引用。
7. 钥匙串访问应用程序将提示您输入登录密码或选定的钥匙串。键入密码，然后单击确定。保存的证书现在即可用于 Endpoint Management 服务器。
8. 要继续，请参阅将APNs 证书导入 Endpoint Management。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使用 **Microsoft IIS** 创建 **PKCS #12** 文件

> 重要：
>
> 在此任务中使用的 IIS 服务器应与生成 CSR 时使用的 IIS 服务器相同。

1. 打开 Microsoft IIS。
2. 单击服务器证书图标。
3. 在服务器证书窗口中，单击完成证书申请。
4. 浏览至来自 Apple 的 Certificate.pem 文件。然后，键入友好名称或证书名称，并单击确定。请勿在名称中包含空格字符。
5. 选择在步骤 4 中找到的证书，然后单击导出。
6. 指定.pfx 证书的位置和文件名以及密码，然后单击确定。

   您需要证书的密码才能将其导入 Endpoint Management。
7. 将.pfx 证书复制到计划安装 Endpoint Management 的服务器上。
8. 要继续，请参阅将APNs 证书导入 Endpoint Management。

使用 **OpenSSL** 创建 **PKCS #12** 文件

如果您使用 OpenSSL 创建 CSR，还可以使用 OpenSSL 创建.pfx APNs 证书。

1. 在命令提示符或 shell 下，运行以下命令。`Customer.privatekey.pem` 是来自您的 CSR 的私钥。`APNs_Certificate.pem` 是您刚刚从 Apple 收到的证书。

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey
   .pem -out apns_identity.pfx
   ```
2. 输入.pfx 证书文件的密码。记住此密码，因为在将证书上载到 Endpoint Management 时要再次使用该密码。
3. 记下.pfx 证书文件的位置。然后，将该文件复制到 Endpoint Management 服务器中，以便可以使用控制台上载文件。
4. 要继续，请将 APNs 证书导入 Endpoint Management，如下一节中所述。

将 **APNs** 证书导入 **Endpoint Management**

在收到新 APNs 证书后：将 APNs 证书导入 Endpoint Management，以便首次添加该证书或者替换证书。

1. 在 Endpoint Management 控制台中，转至设置 **>** 证书。
2. 单击导入 **>** 密钥库。
3. 在用作中，选择 **APNs**。
4. 浏览到计算机上的.pfx 或.p12 文件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 输入密码，然后单击导入。

有关 Endpoint Management 中证书的更多信息，请参阅 证书和身份验证。

续订 **APNs** 证书

> 重要：
>
> 如果您在续订过程中使用其他 Apple ID，则必须重新注册用户设备。

要续订 APNs 证书，请执行创建证书的步骤，然后前往 Apple 推送证书门户。使用该门户上载新证书。登录后，将显示您的现有证书或者从您之前的 Apple 开发人员帐户导入的证书。

在 Certificates Portal 中，续订证书的唯一区别是要单击 **Renew**（续订）。您必须在 Certificates Portal 上拥有开发人员帐户才能访问该站点。要续订证书，请使用相同的组织名称和 Apple ID。

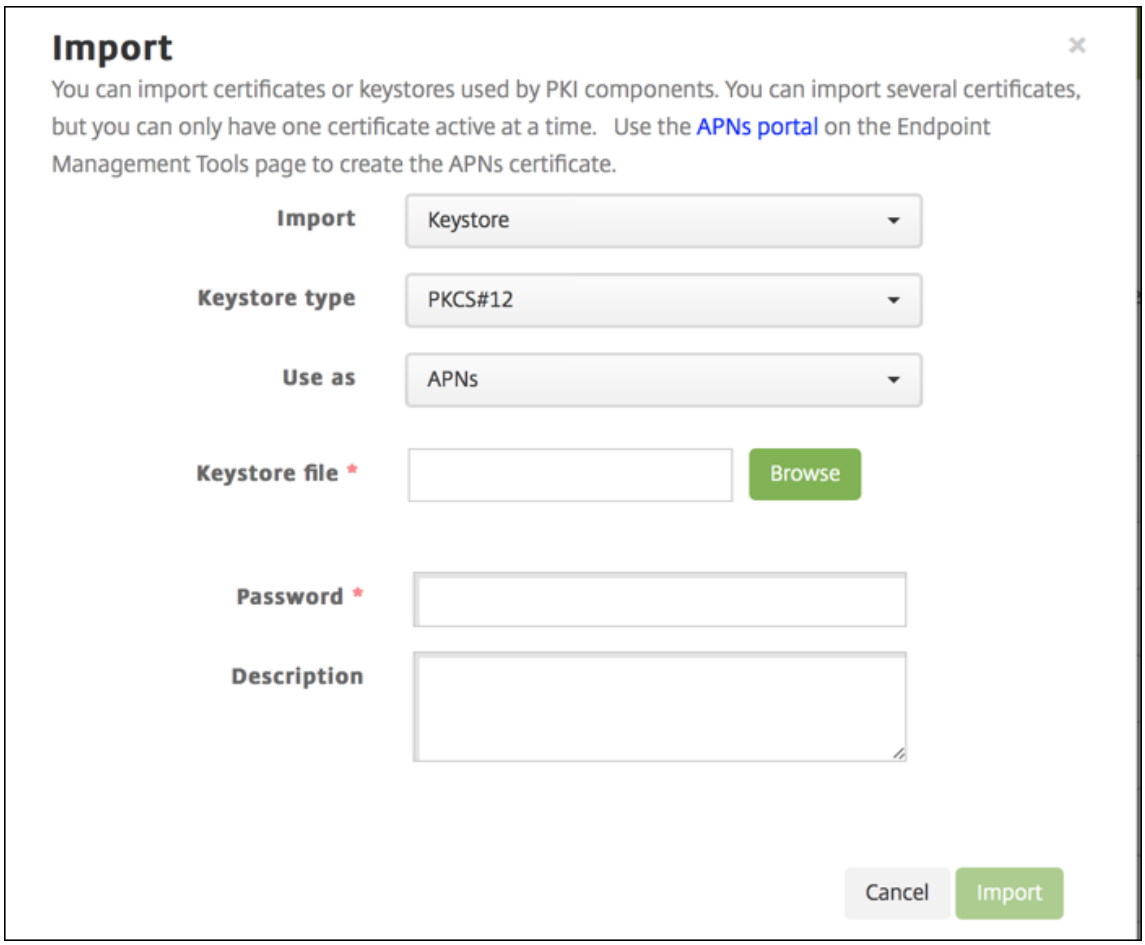
要确定 APNs 证书的过期时间，请在 Endpoint Management 控制台中转至设置 **>** 证书。如果证书过期，请不要吊销。

1. 使用 Microsoft IIS、钥匙串访问 (macOS) 或 OpenSSL 生成 CSR。有关生成 CSR 的更多信息，请参阅创建证书签名请求。
2. 在浏览器中，转到 Endpoint Management 工具。然后，单击 **Request push notification certificate signature**（申请推送通知证书签名）。
3. 单击 **+ Upload the CSR**（+ 上载 CSR）。
4. 在对话框中，导航到 CSR，单击 **Open**（打开），然后单击 **Sign**（签名）。
5. 收到 `.plist` 文件时，将其保存。
6. 在步骤 3 标题中，单击 **Apple Push Certificates Portal** 并登录。
7. 选择要续订的证书，然后单击 **Renew**（续订）。
8. 上载 `.plist` 文件。您将收到输出文件.pem。保存.pem 文件。
9. 使用该.pem 文件完成 CSR（根据您在步骤 1 中创建 CSR 时使用的方法）。
10. 将证书导出为.pfx 文件。

在 Endpoint Management 控制台中，导入.pfx 文件并按如下所示完成配置：

1. 转到设置 **>** 证书 **>** 导入。
2. 在导入菜单中，选择密钥库。
3. 从 密钥库类型菜单中，选择 **PKCS #12**。
4. 在用作中，选择 **APNs**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



5. 对于密钥库文件，单击浏览并导航到该文件。
6. 在密码中，键入证书密码。
7. 键入可选说明。
8. 单击导入。

Endpoint Management 将您重定向回证书页面。名称、状态、有效期开始时间和有效期结束时间字段将更新。

SAML 单点登录与 Citrix Files

November 26, 2021

> 重要：
>
> 本文仅适用于未启用 Workspace 的 Endpoint Management 环境。在启用了 Workspace 的环境中，Content Collaboration 直接与 Citrix Workspace 集成。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可以将 Endpoint Management 和 Content Collaboration 配置为使用安全声明标记语言 (SAML) 来提供对 Citrix Files 移动应用程序的单点登录 (SSO) 访问。此功能包括：

- 使用 MDX Toolkit 启用或封装 MAM SDK 的 Citrix Files 应用程序
- 未封装的 Citrix Files 客户端，例如 Web 站点、Outlook 插件或同步客户端
- 对于封装的 **Citrix Files** 应用程序：登录到 Citrix Files 的用户将被重定向到 Secure Hub 以进行用户身份验证并获取 SAML 令牌。成功进行身份验证后，Citrix Files 移动应用程序会将 SAML 令牌发送到 Content Collaboration。初始登录后，用户可以通过 SSO 访问 Citrix Files 移动应用程序。还可以将附件从 Content Collaboration 附加到 Secure Mail 邮件，而不需要每次都登录。
- 对于非封装的 **Citrix Files** 客户端：使用 Web 浏览器或其他 Citrix Files 客户端登录到 Citrix Files 的用户将被重定向到 Endpoint Management。Endpoint Management 对用户进行身份验证，然后用户获取发送到 Content Collaboration 的 SAML 令牌。初始登录后，用户可以通过 SSO 访问 Citrix Files 客户端，而不需要每次都登录。

要将 Endpoint Management 作为 SAML 身份提供程序 (IdP) 用于 Content Collaboration，必须将 Endpoint Management 配置与 Enterprise 帐户结合使用，如本文中所述。或者，可以将 Endpoint Management 配置为只与存储区域连接器一起使用。有关详细信息，请参阅 Content Collaboration 与 Endpoint Management 结合使用。

有关详细的参考体系结构图，请参阅体系结构。

必备条件

先完成以下必备条件，才能对 Endpoint Management 和 Citrix Files 应用程序配置 SSO：

- MAM SDK 或兼容版本的 MDX Toolkit（适用于 Citrix Files 移动应用程序）。

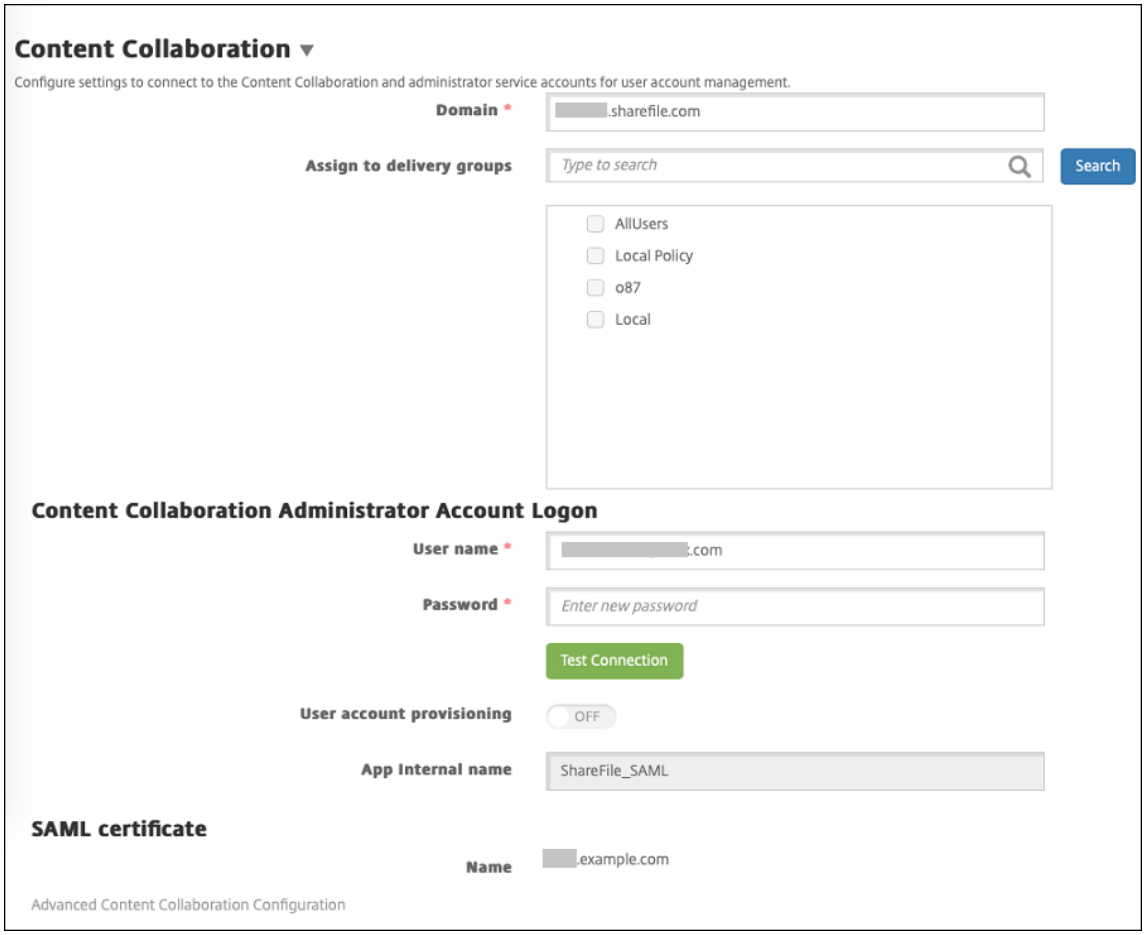
  有关详细信息，请参阅 Endpoint Management 兼容性。
- 兼容版本的 Citrix Files 移动应用程序和 Secure Hub。
- Content Collaboration 管理员帐户。
- 通过验证的 Endpoint Management 与 Content Collaboration 之间的连接。

配置 **Content Collaboration** 访问权限

在为 Content Collaboration 设置 SAML 之前，请按以下方式提供 Content Collaboration 访问信息：

1. 在 Endpoint Management Web 控制台中，单击配置 **> Content Collaboration**。此时将显示 **Content Collaboration** 配置页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 配置以下设置：
   - 域：键入您的 Content Collaboration 子域名。例如：`example.sharefile.com`。
   - 分配给交付组：选择或搜索希望能够对 ShareFile 使用 SSO 的交付组。
   - **Content Collaboration** 管理员帐户登录
   - 用户名：键入 Content Collaboration 管理员用户名。此用户必须具有管理员权限。
   - 密码：键入 Content Collaboration 管理员密码。
   - 用户帐户预配：保留此设置处于禁用状态。使用 Citrix Content Collaboration 用户管理工具进行用户预配。请参阅预配用户帐户和通讯组。
3. 单击测试连接按钮以确认 Content Collaboration 管理员帐户的用户名和密码是否可以向指定的 Content Collaboration 帐户进行身份验证。
4. 单击保存。
   - Endpoint Management 将与 Content Collaboration 同步并更新 Content Collaboration 设置 **ShareFile** 颁发者/实体 **ID** 和登录 **URL**。
   - 配置 **> Content Collaboration** 页面将显示应用程序内部名称。您需要该名称才能完成后面在修改 Citrix Files.com SSO 设置中介绍的步骤。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

为封装的 **Citrix Files MDX** 应用程序设置 **SAML**

对于包含通过 MAM SDK 准备的 Citrix Files 应用程序的单点登录配置，您无需使用 Citrix Gateway。要为未封装的 Citrix Files 客户端（例如 Web 站点、Outlook 插件或同步客户端）配置访问权限，请参阅为其他 Citrix Files 客户端配置 Citrix Gateway。

要为封装的 Citrix Files MDX 应用程序配置 SAML，请执行以下操作：

1. 下载适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。请参阅 Citrix.com 下载。
2. 通过 MAM SDK 准备 Citrix Files 移动应用程序。有关详细信息，请参阅 MAM SDK 概述。
3. 在 Endpoint Management 控制台中，上载准备的 Citrix Files 移动应用程序。有关上载 MDX 应用程序的信息，请参阅将 MDX 应用程序添加到 Endpoint Management。
4. 验证 SAML 设置：使用在前面配置的管理员用户名和密码登录 Content Collaboration。
5. 确认为 Content Collaboration 和 Endpoint Management 配置了相同的时区。确保 Endpoint Management 按配置的时区显示正确时间。如果不正确，SSO 可能会失败。

验证 **Citrix Files** 移动应用程序

1. 在用户设备上，安装和配置 Secure Hub。
2. 从应用商店下载并安装 Citrix Files 移动应用程序。
3. 启动 Citrix Files 移动应用程序。Citrix Files 将启动，但不提示输入用户名和密码。

使用 **Secure Mail** 验证

1. 在用户设备上，如果尚未安装和配置 Secure Hub，请进行安装和配置。
2. 从应用商店下载、安装并设置 Secure Mail。
3. 打开新的电子邮件窗体，并轻按从 **ShareFile** 附加。此时将显示可以附加到电子邮件中的文件，但不提示输入用户名或密码。

为其他 **Citrix Files** 客户端配置 **Citrix Gateway**

要配置对未封装的 Citrix Files 客户端（例如 Web 站点、Outlook 插件或同步客户端）的访问，请将 Citrix Gateway 配置为支持将 Endpoint Management 用作 SAML 身份提供程序，如下所示。

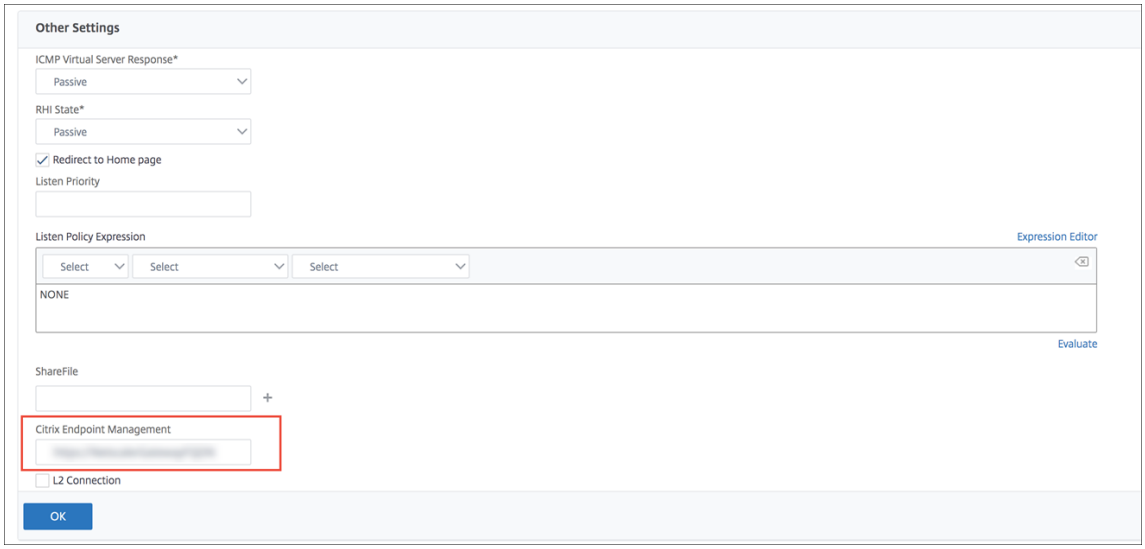
- 禁用主页重定向。
- 创建 Citrix Files 会话策略和配置文件。
- 在 Citrix Gateway 虚拟服务器上配置策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

禁用主页重定向

对通过 /cginfra 路径发出的请求禁用默认行为。执行该操作后，用户将看到最初请求的内部 URL，而非配置的主页。

1. 编辑用于 Endpoint Management 登录的 Citrix Gateway 虚拟服务器的设置。在 Citrix Gateway 中，转至 **Other Settings**（其他设置），然后取消选中标签为 **Redirect to Home Page**（重定向到主页）的复选框。



2. 在 **ShareFile**（现在称为 Content Collaboration）下方，键入 Endpoint Management 内部服务器的名称和端口号。
3. 在 **Citrix Endpoint Management** 下，键入您的 Endpoint Management URL。

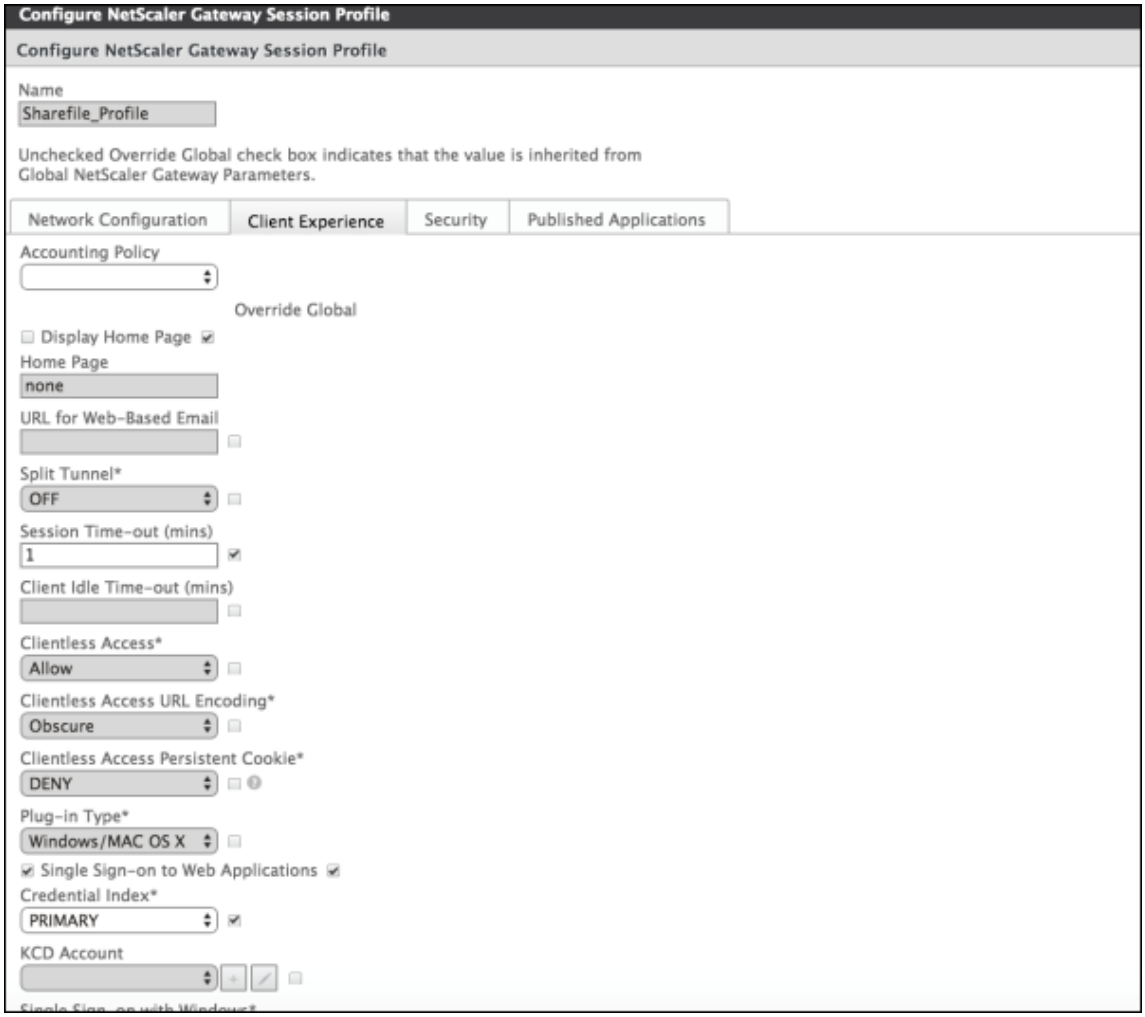
   此配置授权您向通过 /cginfra 路径输入的 URL 发送请求。

创建 **Citrix Files** 会话策略并请求配置文件

请配置以下设置以创建 Citrix Files 会话策略并请求配置文件：

1. 在 Citrix Gateway 配置实用程序的左侧导航窗格中单击 **NetScaler Gateway > Policies**（策略）**> Session**（会话）。
2. 创建会话策略。在 **Policies**（策略）选项卡上，单击 **Add**（添加）。
3. 在 **Name**（名称）字段中，键入 **ShareFile_Policy**。
4. 单击 **+** 按钮创建操作。此时将显示 **Create NetScaler Gateway Session Profile**（创建 NetScaler Gateway 会话配置文件）页面。

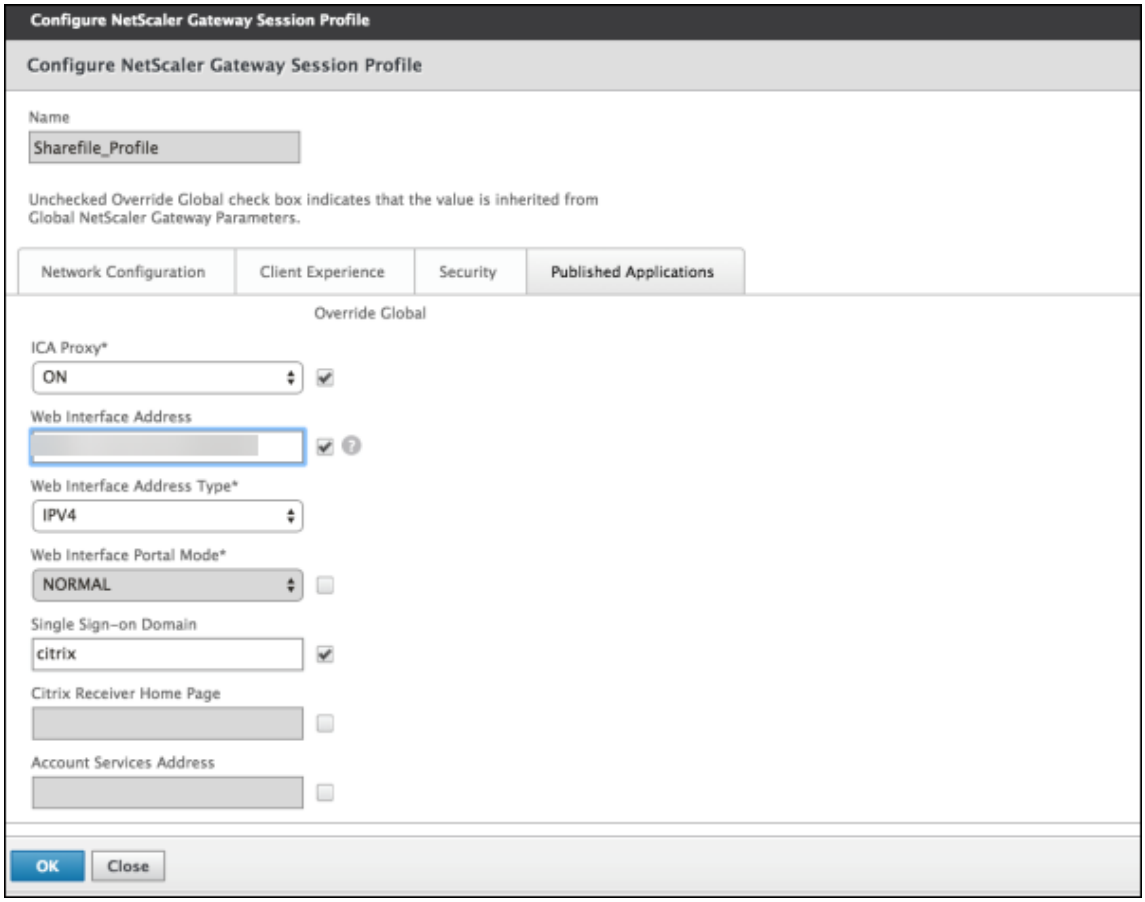
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



配置以下设置：

- **Name**（名称）：键入 **ShareFile_Profile**。
- 单击 **Client Experience**（客户端体验）选项卡，然后配置以下设置：
  - **Home Page**（主页）：键入 **none**（无）。
  - **Session Time-out (mins)**（会话超时 **(**分钟**)**）：键入 **1**。
  - **Single Sign-on to Web Applications**（单点登录到 **Web** 应用程序）：选择此设置。
  - **Credential Index**（凭据索引）：单击 **PRIMARY**（主要）。
- 单击 **Published Applications**（已发布的应用程序）选项卡。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



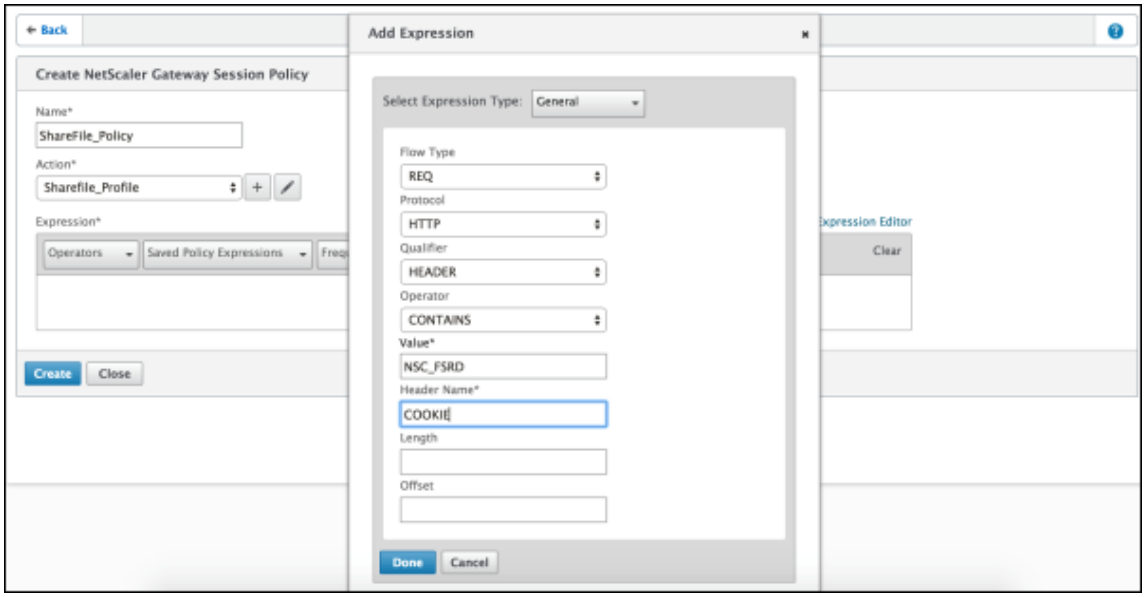
配置以下设置：

- **ICA Proxy**（ICA 代理）：单击 **ON**（开）。
- **Web Interface Address**（**Web Interface** 地址）：键入 Endpoint Management 服务器的 URL。
- **Single Sign-on Domain**（单点登录域）：键入 Active Directory 的域名。

  配置 Citrix Gateway 会话配置文件时，**Single Sign-on Domain**（单点登录域）的域后缀必须与在 LDAP 中定义的 Endpoint Management 域别名匹配。

5. 单击 **Create**（创建）以定义会话配置文件。
6. 单击 **Expression Editor**（表达式编辑器）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



配置以下设置：

- **Value**（值）：键入 **NSC_FSRD**。
- **Header Name**（标头名称）：键入 **COOKIE**。

7. 单击 **Create**（创建），然后单击 **Close**（关闭）。



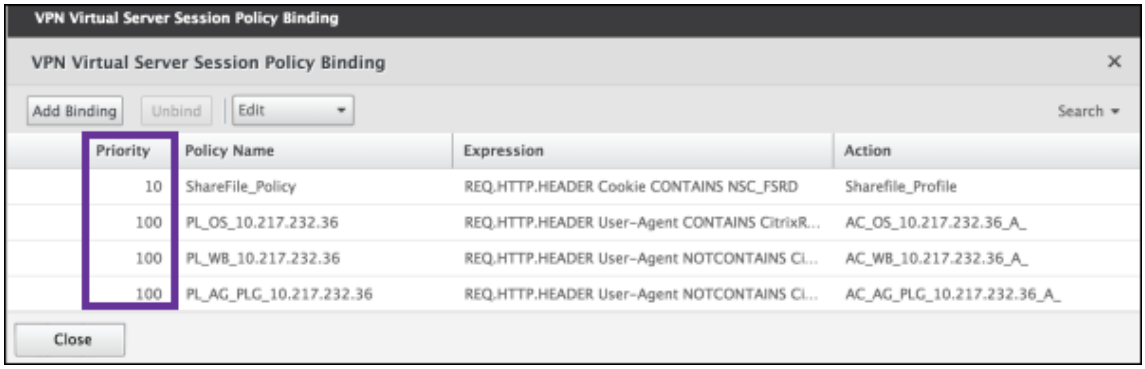
在 **Citrix Gateway** 虚拟服务器上配置策略

在 Citrix Gateway 虚拟服务器上配置以下设置。

1. 在 Citrix Gateway 配置实用程序的左侧导航窗格中单击 **NetScaler Gateway > Virtual Servers**（虚拟服务器）。
2. 在 **Details**（详细信息）窗格中，单击 Citrix Gateway 虚拟服务器。
3. 单击编辑。
4. 单击 **Configured policies**（已配置的策略）**> Session policies**（会话策略），然后单击 **Add binding**（添加绑定）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 选择 **ShareFile_Policy**。
6. 编辑为选定策略自动生成的 **Priority**（优先级）编号，以便与列出的任何其他策略相比，其优先级最高（编号最小）。例如：



7. 单击 **Done**（完成），然后保存运行的 Citrix Gateway 配置。

修改 **Citrix Files.com SSO** 设置

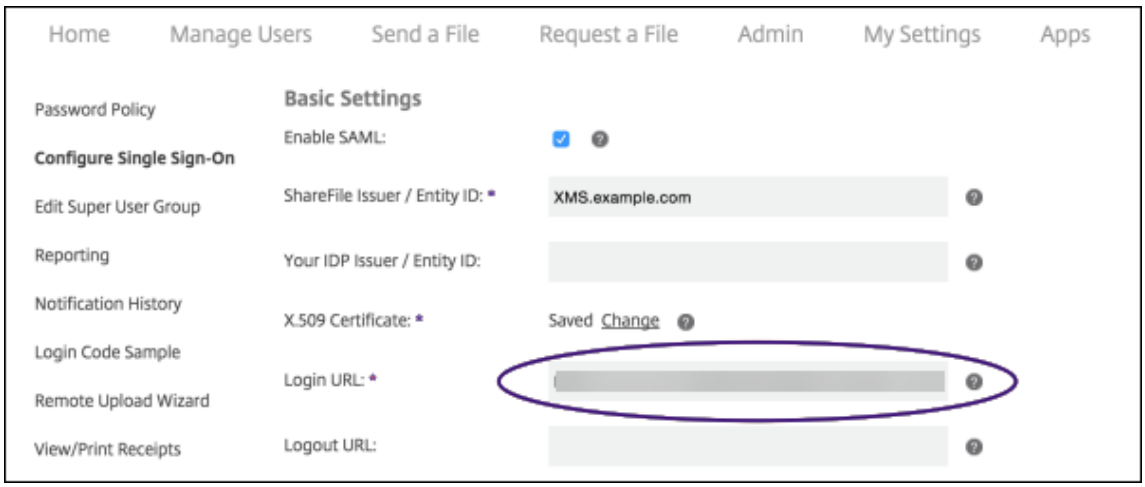
针对 MDX 和非 MDX Citrix Files 应用程序进行以下更改。

> 重要：
>
> 内部应用程序名称后附加了一个新编号：
>
> - 每次编辑或重新创建 Citrix Files 应用程序时
> - 每次在 Endpoint Management 中更改 Content Collaboration 设置时
>
> 因此，您还必须在 Citrix Files Web 站点中更新登录 URL，以反映更新后的应用程序名称。

1. 以 Content Collaboration 管理员身份登录到您的 Content Collaboration 帐户 (`https://<subdomain>.sharefile.com`)。
2. 在 Content Collaboration Web 界面中，单击 **Admin**（管理），然后选择 **Configure Single Sign-on**（配置单点登录）。
3. 按如下所示编辑 **Login URL**（登录 URL）：

   下面是编辑之前的 **Login URL**（登录 URL）示例：`https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 在 Endpoint Management 服务器 FQDN 前面插入 Citrix Gateway 虚拟服务器的外部 FQDN 和 **/cginfra/https/**，然后在 Endpoint Management FQDN 后面添加 **8443**。

  下面是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

- 将参数 &`app=ShareFile_SAML_SP` 更改为内部 Citrix Files 应用程序名称。默认情况下，内部名称为 `ShareFile_SAML`。但是，每次更改配置时，都会向内部名称附加一个数字（`ShareFile_SAML_2`、`ShareFile_SAML_3` 等）。可以在配置 **> Content Collaboration** 页面上查找应用程序内部名称。

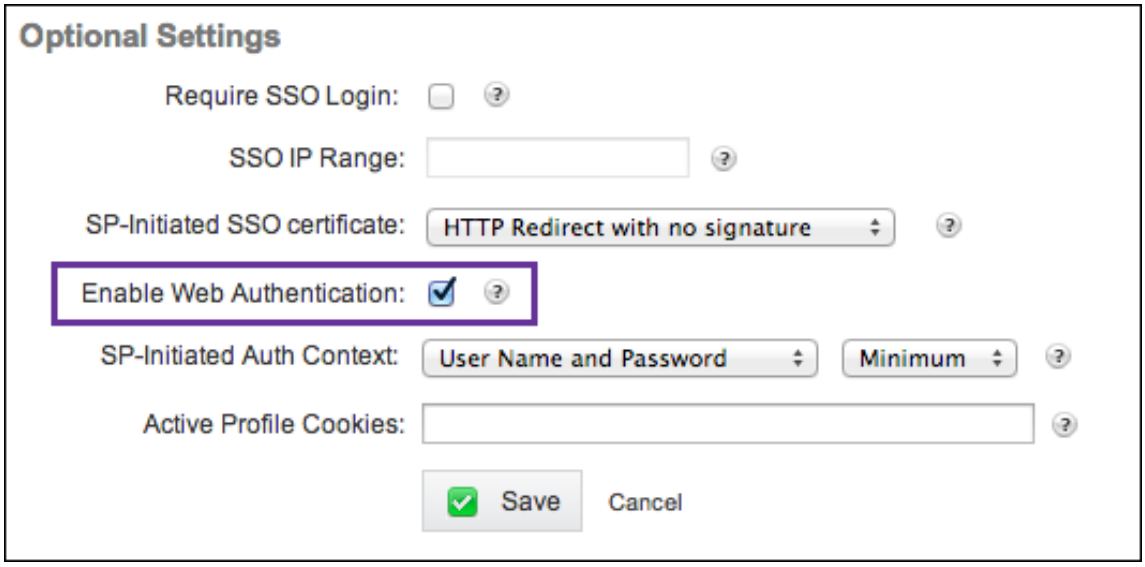
  下面是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- 向 URL 的末尾添加 &`nssso=true`。

  下面是最终 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`。

4. 在 **Optional Settings**（可选设置）下方，选中 **Enable Web Authentication**（启用 Web 身份验证）复选框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



验证配置

请执行以下配置以验证设置。

1. 在浏览器中访问 `https://<subdomain>sharefile.com/saml/login`。

   系统会将您重定向到 Citrix Gateway 登录表单。如果未被重定向，请验证前面的配置设置。

2. 输入所配置的 Citrix Gateway 和 Endpoint Management 环境的用户名和密码。

   此时将在 `<subdomain>.sharefile.com` 下显示您的 Citrix Files 文件夹。如果未显示您的 Citrix Files 文件夹，请确保您输入了正确的登录凭据。

通过 **Citrix Cloud** 使用 **Azure Active Directory** 进行身份验证

October 18, 2022

Endpoint Management 支持通过 Citrix Cloud 使用 Azure Active Directory (Azure AD) 凭据进行身份验证。此身份验证方法仅适用于通过 Citrix Workspace 应用程序或 Citrix Secure Hub 注册 MDM 的用户。如果 Endpoint Management 已启用工作区，则用户可从 Citrix Workspace 应用程序访问资源。如果您未启用 Citrix Workspace 与 Citrix Endpoint Management 的集成，则用户可以从 Secure Hub 访问资源。

在 MAM 中注册的设备无法通过 Citrix Cloud 使用 Azure AD 凭据进行身份验证。要将 Secure Hub 与 MDM+MAM 结合使用，请将 Endpoint Management 配置为使用 Citrix Gateway 进行 MAM 注册。有关更多信息，请参阅 Citrix Gateway 和 Endpoint Management。

Endpoint Management 使用 Citrix Cloud 服务、Citrix 身份与 Azure Active Directory 联盟。Citrix 建议您使用 Citrix 身份提供程序来代替与 Azure Active Directory 直接连接。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 支持以下平台使用 Azure AD 进行身份验证：

- 未在 Apple 商务管理或 Apple 校园教务管理中注册的 iOS 和 macOS 设备
- 在 Apple 商务管理中注册的 iOS 和 macOS 设备
- 适用于 BYOD 和完全托管模式的 Android Enterprise 设备（预览版）

通过 Citrix Cloud 使用 Azure AD 进行身份验证具有以下限制：

- 不适用于 Endpoint Management 本地帐户。
- 不支持通过 Azure AD 对注册邀请进行身份验证。如果您向用户发送了一个包含注册 URL 的注册邀请，用户将通过 LDAP 进行身份验证，而非通过 Azure AD。

必备条件

- Azure Active Directory 用户凭据
- Active Directory 中的用户组必须与 Azure Active Directory 中的用户组匹配。
- Active Directory 中的用户名和电子邮件地址必须与 Azure Active Directory 中的用户名和
- Citrix Cloud 帐户，安装了用于目录服务同步的 Citrix Cloud Connector。
- Citrix Gateway。Citrix 建议您启用基于证书的身份验证以实现完整的单点登录体验。如果您在 Citrix Gateway 上使用 LDAP 身份验证进行 MAM 注册，最终用户在注册期间会遇到双身份验证提示。有关详细信息，请参阅客户端证书或证书加域身份验证。
- 如果 Endpoint Management 未启用 Workspace，则为 Secure Hub。
- 如果 Endpoint Management 已启用 Workspace，则 Citrix Workspace 应用程序。有关启用 Citrix Workspace 集成的信息，请参阅 Workspace 配置。
- 在 Android Enterprise 的注册配置文件中，将 允许用户拒绝设备管理设置为 关闭。如果用户拒绝设备管理，则无法使用身份提供商注册进行身份验证。有关详细信息，请参阅 注册安全性。

可以在启用或不启用 Workspace 的情况下配置此功能。

如果 **Endpoint Management** 启用了 **Workspace**，则配置

如果将 Endpoint Management 与 Citrix Workspace 集成，则通过 Citrix Cloud 使用 Azure AD 配置身份验证的一般步骤如下：

1. 将 Citrix Cloud 配置为使用 Azure AD 作为身份提供程序。
2. 将 Azure AD 配置为 Citrix Workspace 的身份验证方法。

如果 **Endpoint Management** 未启用 **Workspace**，则配置

如果未为 Endpoint Management 启用 Citrix Workspace，则通过 Citrix Cloud 使用 Azure AD 配置身份验证的一般步骤如下：

1. 将 Citrix Cloud 配置为使用 Azure AD 作为身份提供程序。
2. 将 Citrix 身份配置为 Endpoint Management 的 IdP 类型。

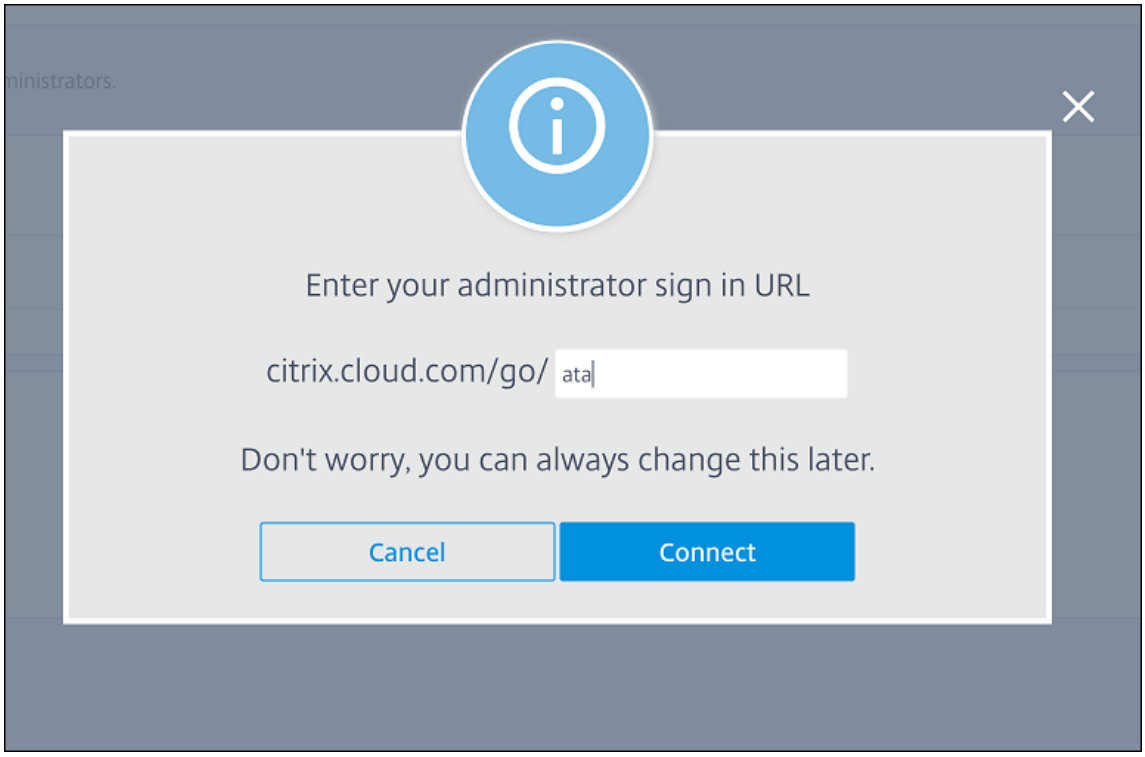
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

完成该配置后，已加入域的 Secure Hub 用户可以使用 Secure Hub 使用其 Azure AD 凭据登录。Secure Hub 对 MAM 设备使用客户端证书身份验证。

将 **Citrix Cloud** 配置为使用 **Azure Active Directory** 作为您的身份提供程序

要将此服务设置为与 Citrix Workspace 应用程序和 Secure Hub 配合使用，请在 Citrix Cloud 中配置 Azure Active Directory。

1. 转到 https://citrix.cloud.com 并登录到您的 Citrix Cloud 帐户。
2. 在 Citrix Cloud 菜单中，转至身份识别和访问管理页面并连接到 Azure Active Directory。
3. 键入您的管理员登录 URL，然后单击连接。



4. 登录后，您的 Azure Active Directory 帐户将连接到 Citrix Cloud。身份识别和访问管理 **>** 身份验证页面显示哪些帐户用于登录您的 Citrix Cloud 和 Azure AD 帐户。
5. 要为通过 Citrix Workspace 应用程序和 Secure Hub 注册的用户启用 Azure AD 的身份验证，请在 工作区配置 **>** 身份验证下，选择 **Azure Active Directory**。完成配置后，您可以通过 Citrix Workspace 应用程序和 Secure Hub 注册用户设备。

将 **Citrix** 身份配置为适用于 **Endpoint Management** 的 **IdP** 类型

此配置仅适用于通过 Secure Hub 注册的用户。在 Citrix Cloud 中配置 Azure Active Directory 后，请按如下所示配置 Endpoint Management。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在 Endpoint Management 控制台中，转至设置 **>** 身份提供程序 **(IDP)**，然后单击添加。
2. 在 身份提供程序 **(IDP)** 页面上，配置以下内容：
   - **IDP** 名称：键入唯一名称以标识您正在创建的 IdP 连接。
   - **IDP** 类型：选择 **Citrix** 身份平台。
   - 身份验证域：选择 **Azure Active Directory**。此域对应于 Citrix Cloud **Workspace** 配置 **>** 身份验证页面上的身份提供程序域。
3. 单击下一步。在 **IDP** 声明使用情况页面上，配置以下内容：
   - 用户标识符类型：默认情况下，此字段设置为 **userPrincipalName**。确保在本地活动目录和 Azure Active Directory Active Directory 中为所有用户配置相同的标识符。Endpoint Management 使用此标识符将身份提供商上的用户与本地 Active Directory 用户映射。
   - 用户标识符字符串：此字段自动填充。
4. 单击下一步，检查摘要页面，然后单击保存。

   Secure Hub 用户、Endpoint Management 控制台和自助服务门户用户现在可以使用其 Azure Active Directory 凭据登录。

Secure Hub 身份验证流程

Endpoint Management 使用以下流程在通过 Secure Hub 注册的设备上使用 Azure AD 作为 IdP 对用户进行身份验证：

1. 用户开始使用 Secure Hub。
2. Secure Hub 将身份验证请求传递到 Citrix 身份，该身份再将请求传递到 Azure Active Directory。
3. 用户键入 Azure Active Directory 用户名和密码。
4. Azure Active Directory 验证用户并将某个代码发送到 Citrix 身份。
5. Citrix 身份将该代码发送到 Secure Hub，后者再将该代码发送到 Endpoint Management 服务器。
6. Endpoint Management 通过使用代码和密码获取 ID 令牌，然后验证 ID 令牌中的用户信息。Endpoint Management 返回会话 ID。

通过 **Citrix Cloud** 使用 **Okta** 进行身份验证

October 18, 2022

Endpoint Management 支持通过 Citrix Cloud 使用 Okta 凭据进行身份验证。此身份验证方法仅适用于通过 Citrix Workspace 应用程序或 Citrix Secure Hub 注册 MDM 的用户。如果 Endpoint Management 已启用工作区，则用户可从 Citrix Workspace 应用程序访问资源。如果您未启用 Citrix Workspace 与 Citrix Endpoint Management 的集成，则用户可以从 Secure Hub 访问资源。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在 MAM 中注册的设备无法通过 Citrix Cloud 使用 Okta 凭据进行身份验证。要将 Secure Hub 与 MDM+MAM 结合使用，请将 Endpoint Management 配置为使用 Citrix Gateway 进行 MAM 注册。有关更多信息，请参阅 Citrix Gateway 和 Endpoint Management。

Endpoint Management 使用 Citrix Cloud 服务、Citrix 身份与 Okta 联合。Citrix 建议您使用 Citrix 身份提供程序来代替与 Okta 直接连接。

Endpoint Management 支持以下平台使用 Okta 进行身份验证：

- 未在 Apple 商务管理或 Apple 校园教务管理中注册的 iOS 和 macOS 设备
- 在 Apple 商务管理中注册的 iOS 和 macOS 设备
- 适用于 BYOD 和完全托管模式的 Android Enterprise 设备（预览版）

通过 Citrix Cloud 使用 Okta 进行身份验证有以下限制：

- 不适用于 Endpoint Management 本地帐户。
- 不支持通过 Okta 进行注册邀请的身份验证。如果您向用户发送了一个包含注册 URL 的注册邀请，用户将通过 LDAP 进行身份验证，而非通过 Okta。

必备条件

- Okta 用户凭据
- Active Directory 中的用户组必须与 Okta 中的用户组匹配。
- 活动目录中的用户名和电子邮件地址必须与 Okta 中的用户名和电子邮件地址相匹配。
- Citrix Cloud 帐户，安装了用于目录服务同步的 Citrix Cloud Connector
- Citrix Gateway。Citrix 建议您启用基于证书的身份验证以实现完整的单点登录体验。如果您在 Citrix Gateway 上使用 LDAP 身份验证进行 MAM 注册，最终用户在注册期间会遇到双身份验证提示。有关详细信息，请参阅客户端证书或证书加域身份验证。
- 如果 Endpoint Management 未启用 Workspace，则为 Secure Hub。
- 如果 Endpoint Management 已启用 Workspace，则 Citrix Workspace 应用程序。有关启用 Citrix Workspace 集成的信息，请参阅 Workspace 配置。
- 在 Android Enterprise 的注册配置文件中，将 允许用户拒绝设备管理设置为 关闭。如果用户拒绝设备管理，则无法使用身份提供商注册进行身份验证。有关详细信息，请参阅 注册安全性。

可以在启用或不启用 Workspace 的情况下配置此功能。

如果 **Endpoint Management** 启用了 **Workspace**，则配置

如果将 Endpoint Management 与 Citrix Workspace 集成，则通过 Citrix Cloud 使用 Okta 配置身份验证的一般步骤如下：

1. 将 Citrix Cloud 配置为使用 Okta 作为您的身份提供商。
2. 将 Okta 配置为 Citrix Workspace 的身份验证方法。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要将 Citrix Cloud 配置为使用 Okta 作为身份提供程序并将 Okta 设置为 Citrix Workspace 的身份验证方法，请参阅 将 Okta 作为身份提供程序连接到 Citrix Cloud。

完成配置后，您可以通过 Citrix Workspace 应用程序注册用户设备。

如果 **Endpoint Management** 未启用 **Workspace**，则配置

如果未为 Endpoint Management 启用 Citrix Workspace，则通过 Citrix Cloud 配置使用 Okta 进行身份验证的常规步骤为：

1. 将 Citrix Cloud 配置为使用 Okta 作为您的身份提供商。
2. 将 Citrix 身份配置为 Endpoint Management 的 IdP 类型。

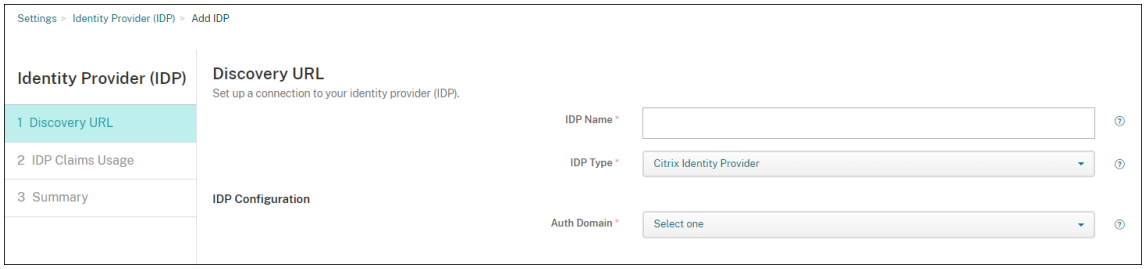
将 **Citrix Cloud** 配置为使用 **Okta** 作为您的身份提供程序

要在 Citrix Cloud 中配置 Okta，请参阅 将 Okta 作为身份提供商连接到 Citrix Cloud。

将 **Citrix** 身份配置为适用于 **Endpoint Management** 的 **IdP** 类型

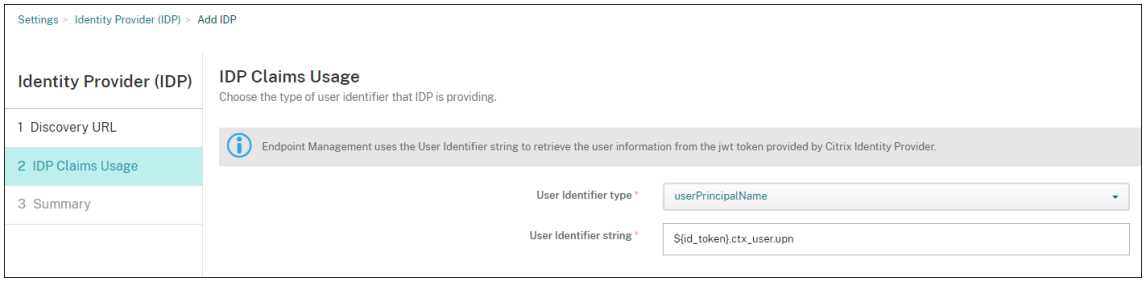
此配置仅适用于通过 Secure Hub 注册的用户。在 Citrix Cloud 中配置 Azure Active Directory 后，请按如下所示配置 Endpoint Management。

1. 在 Endpoint Management 控制台中，转至设置 **>** 身份提供程序 **(IDP)**，然后单击添加。
2. 在 身份提供程序 **(IDP)** 页面上，配置以下内容：



   - **IDP** 名称：键入用于识别要创建的 IdP 连接的唯一名称。
   - **IDP** 类型：选择 **Citrix** 身份提供商。
   - 身份验证域：选择 Citrix Cloud 域。如果不确定要选择哪一个，则您的域将显示在 Citrix Cloud 身份和访问管理 **>** 身份验证页面上。
3. 单击下一步。在 **IDP** 声明用法页面中，配置以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 用户标识符类型：此字段设置为 **userPrincipalName**。确保在本地 Active Directory 和 Okta 中为所有用户配置相同的标识符。Endpoint Management 使用此标识符将身份提供商上的用户与本地 Active Directory 用户映射。
- 用户标识符字符串：此字段自动填充。

完成此配置后，已加入域的 Secure Hub 用户可以使用 Secure Hub 使用其 Okta 凭据登录。Secure Hub 对 MAM 设备使用客户端证书身份验证。

Secure Hub 身份验证流程

Endpoint Management 使用以下流程在通过 Secure Hub 注册的设备上使用 Okta 作为 IdP 的用户进行身份验证：

1. 用户开始使用 Secure Hub。
2. Secure Hub 将身份验证请求传递给 Citrix 身份，然后 Citrix 身份将请求传递给 Okta。
3. 用户键入其用户名和密码。
4. Okta 验证用户并向 Citrix 身份发送代码。
5. Citrix 身份将该代码发送到 Secure Hub，后者再将该代码发送到 Endpoint Management 服务器。
6. Endpoint Management 通过使用代码和密码获取 ID 令牌，然后验证 ID 令牌中的用户信息。Endpoint Management 返回会话 ID。

通过 **Citrix Cloud** 使用本地 **Citrix Gateway** 进行身份验证

October 18, 2022

Endpoint Management 支持通过 Citrix Cloud 使用本地 Citrix Gateway 进行身份验证。此身份验证方法仅适用于通过 Citrix Workspace 应用程序或 Citrix Secure Hub 注册 MDM 的用户。如果 Endpoint Management 已启用工作区，则用户可从 Citrix Workspace 应用程序访问资源。如果您未启用 Citrix Workspace 与 Citrix Endpoint Management 的集成，则用户可以从 Secure Hub 访问资源。

在 MAM 中注册的设备无法通过 Citrix Cloud 使用本地 Citrix Gateway 凭据进行身份验证。要将 Secure Hub 与 MDM+MAM 结合使用，请将 Endpoint Management 配置为使用 Citrix Gateway 进行 MAM 注册。有关更多信息，请参阅 Citrix Gateway 和 Endpoint Management。

Endpoint Management 支持通过 Citrix Cloud 对以下平台使用本地 Citrix Gateway 进行身份验证：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- iOS 设备
- 适用于 BYOD 和完全托管模式的 Android Enterprise 设备

> 注意：
>
> Endpoint Management 不支持使用本地 Citrix Gateway 进行身份验证以便通过 Citrix Cloud 发送注册邀请。如果您向用户发送包含注册 URL 的注册邀请，则用户将通过 LDAP 而非本地 Citrix Gateway 作为身份提供程序进行身份验证。

Citrix 建议您启用基于证书的身份验证以实现完整的单点登录体验。如果您在 Citrix Gateway 上使用 LDAP 身份验证进行 MAM 注册，最终用户在注册期间会遇到双身份验证提示。有关详细信息，请参阅客户端证书或证书加域身份验证。

必备条件

- Citrix Gateway。Citrix 建议您启用基于证书的身份验证以实现完整的单点登录体验。如果您在 Citrix Gateway 上使用 LDAP 身份验证进行 MAM 注册，则最终用户在注册过程中会遇到双重身份验证提示。有关详细信息，请参阅客户端证书或证书加域身份验证。
- 安装了 Citrix Cloud Connector 的 Citrix Cloud 帐户以进行目录服务同步。
- Secure Hub 20.5.0 及更高版本（如果 Endpoint Management 未启用工作区）。
- 如果 Endpoint Management 已启用 Workspace，则 Citrix Workspace 应用程序。有关启用 Citrix Workspace 集成的信息，请参阅 Workspace 配置。

可以在启用或不启用 Workspace 的情况下配置此功能。

如果 **Endpoint Management** 启用了 **Workspace**，则配置

如果将 Endpoint Management 与 Citrix Workspace 集成，则通过 Citrix Cloud 使用本地 Citrix Gateway 配置身份验证的一般步骤如下：

1. 将 Citrix Cloud 配置为使用 Citrix Gateway 作为您的身份提供商。
2. 将 Citrix Gateway 配置为 Citrix Workspace 的身份验证方法。

要将 Citrix Cloud 配置为使用 Citrix Gateway 作为身份提供程序，并将 Citrix Gateway 设置为 Citrix Workspace 的身份验证方法，请参阅 将本地 Citrix Gateway 作为身份提供程序连接到 Citrix Cloud。

完成配置后，您可以通过 Citrix Workspace 应用程序注册用户设备。

如果 **Endpoint Management** 未启用 **Workspace**，则配置

如果未为 Endpoint Management 启用 Citrix Workspace，则通过 Citrix Cloud 使用本地 Citrix Gateway 配置身份验证的一般步骤如下：

1. 将 Citrix Cloud 配置为使用 Citrix Gateway 作为您的身份提供商。
2. 将 Citrix 身份配置为 Endpoint Management 的 IdP 类型。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

将 **Citrix Cloud** 配置为使用 **Citrix Gateway** 作为您的身份提供程序

要在 Citrix Cloud 中设置 Citrix Gateway 身份验证，请参阅 将本地 Citrix Gateway 作为身份提供程序连接到 Citrix Cloud。

将 **Citrix** 身份提供程序配置为适用于 **Endpoint Management** 的 **IdP** 类型

此配置仅适用于通过 Secure Hub 注册的用户。在 Citrix Cloud 中配置 Citrix Gateway 后，请按如下所示配置 Endpoint Management。

1. 在 Endpoint Management 控制台中，转至设置 **>** 身份提供程序 **(IDP)**，然后单击添加。
2. 在 身份提供程序 **(IDP)** 页面上，配置以下内容：
   - **IDP** 名称：键入唯一名称以标识您正在创建的 IdP 连接。
   - **IDP** 类型：选择 **Citrix** 身份提供商。
   - 身份验证域：选择 **Citrix Gateway**。此域对应于 Citrix Cloud **Workspace** 配置 **>** 身份验证页面上的身份提供程序域。
3. 单击下一步。在 **IDP** 声明使用情况页面上，配置以下内容：
   - 用户标识符类型：默认情况下，此字段设置为 **userPrincipalName**。
   - 用户标识符字符串：此字段自动填充。
4. 单击下一步，检查摘要页面，然后单击保存。

   现在，您可以使用本地 Citrix Gateway 作为身份提供程序通过 Secure Hub 注册用户设备。

Secure Hub 身份验证流程

Endpoint Management 使用以下流程在通过 Secure Hub 注册的设备上使用本地 Citrix Gateway 作为 IdP 对用户进行身份验证：

1. 用户开始使用 Secure Hub。
2. Secure Hub 将身份验证请求传递给 Citrix 身份，后者会将请求传递给本地 Citrix Gateway。
3. 用户键入其用户名和密码。
4. 本地 Citrix Gateway 会验证用户并向 Citrix 身份发送代码。
5. Citrix 身份将该代码发送到 Secure Hub，后者再将该代码发送到 Endpoint Management 服务器。
6. Endpoint Management 通过使用代码和密码获取 ID 令牌，然后验证 ID 令牌中的用户信息。Endpoint Management 返回会话 ID。

用户帐户、角色和注册

October 18, 2022

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

您可以在 Endpoint Management 控制台的管理选项卡和设置页面上执行用户配置任务。除非另有说明，否则本文提供完成以下任务的步骤。

- 注册安全模式和邀请
  - 从设置 > 注册，配置最多七种注册安全模式并发送注册邀请。每种注册安全模式都有自己的安全级别和用户注册设备所必须采取的步骤数。
- 用户帐户和组的角色
  - 从设置 > 基于角色的访问控制，向用户和组分配预定义角色或权限集合。这些权限控制用户对系统功能的访问级别。有关详细信息，请参阅使用 RBAC 配置角色。
  - 从设置 > 通知模板，创建或更新用于自动化操作、注册和发送给用户的标准通知消息的通知模板。可以将通知模板配置为通过两个不同的通道来发送消息：Secure Hub 或 SMTP。有关更多信息，请参阅：创建和更新通知模板。
- 用户帐户和组：
  - 从管理 > 用户中，手动添加用户帐户或使用.csv 预配文件导入帐户并管理本地组。但是，大多数 Endpoint Management 部署都连接到 LDAP 以获取用户和组信息。在以下用例中，您可能希望在本地创建用户帐户：
    - 在零售等环境中，设备是共用的，而不是由单个用户专用。
    - 如果您使用不受支持的目录，例如 Novell eDirectory。
  - 从设置 > 工作流，使用工作流对用户帐户的创建和删除进行管理。

关于用户帐户

Endpoint Management 用户帐户适用于本地、Active Directory 或云用户。

- 云用户：云用户是 Citrix Cloud 在将管理员添加到您的 Citrix Cloud 客户帐户时创建的特殊用户帐户。云用户帐户使用与 Citrix Cloud 上的管理员帐户相同的用户名，并且默认为管理员角色。云用户帐户提供单点登录并执行其他管理功能。

  要向 Citrix Cloud 帐户添加管理员，请参阅 邀请新管理员。

对于云用户：

- 您可以通过 Citrix Cloud 控制台更改云用户的角色和用户属性。请参阅 管理 Citrix Cloud 管理员。
- 要更改密码，请参阅 管理员。
- 要删除云用户，请在 Citrix Cloud 中转到 身份和访问管理 > 管理员。单击用户行末尾的省略号，然后选择 删除管理员。
- 您无法将云用户添加到本地组。

配置注册安全模式

您可以配置设备注册安全模式，以便在 Endpoint Management 中为设备注册指定安全级别和通知模板。

Endpoint Management 提供六种注册安全模式，每种模式都有自己的安全级别以及用户注册设备必须采取的步骤。您可以从管理 > 注册 邀请页面在 **Endpoint Management** 控制台中配置注册安全模式。有关信息，请参阅 注册邀

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

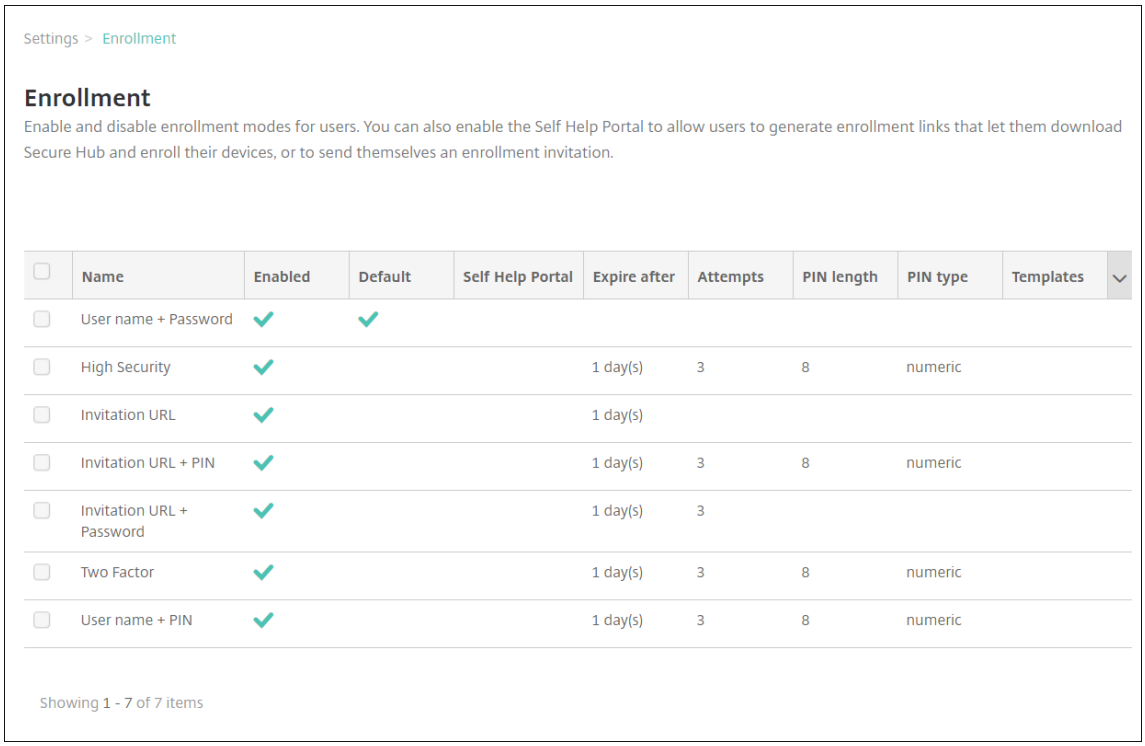
请。

> 注意：
>
> 如果计划使用自定义通知模板，则必须先设置模板，然后再配置注册安全模式。有关通知模板的详细信息，请参阅创建或更新通知模板。

1. 在 Endpoint Management 控制台上，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击注册。此时将显示注册页面，其中包含所有可用注册安全模式的表格。默认情况下，启用所有注册安全模式。
3. 在列表中选择任何注册安全模式以对其进行编辑。然后，将模式设置为默认模式或禁用该模式。

   选中注册安全模式旁边的复选框以查看选项菜单。或者，单击列表中的其他任意位置可查看列表右侧的选项菜单。

   > 提示：
   >
   > 编辑注册安全模式时，可以指定过期截止日期，在截止日期之后，用户将无法注册其设备。有关信息，请参阅本文中的编辑注册安全模式 。此值显示在用户和组注册邀请配置页面。



   根据您的平台，您可以选择以下注册安全模式：

   - 用户名 + 密码
   - 邀请 URL
   - 邀请 URL + PIN
   - 邀请 URL + 密码
   - 双重
   - 用户名 + PIN

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

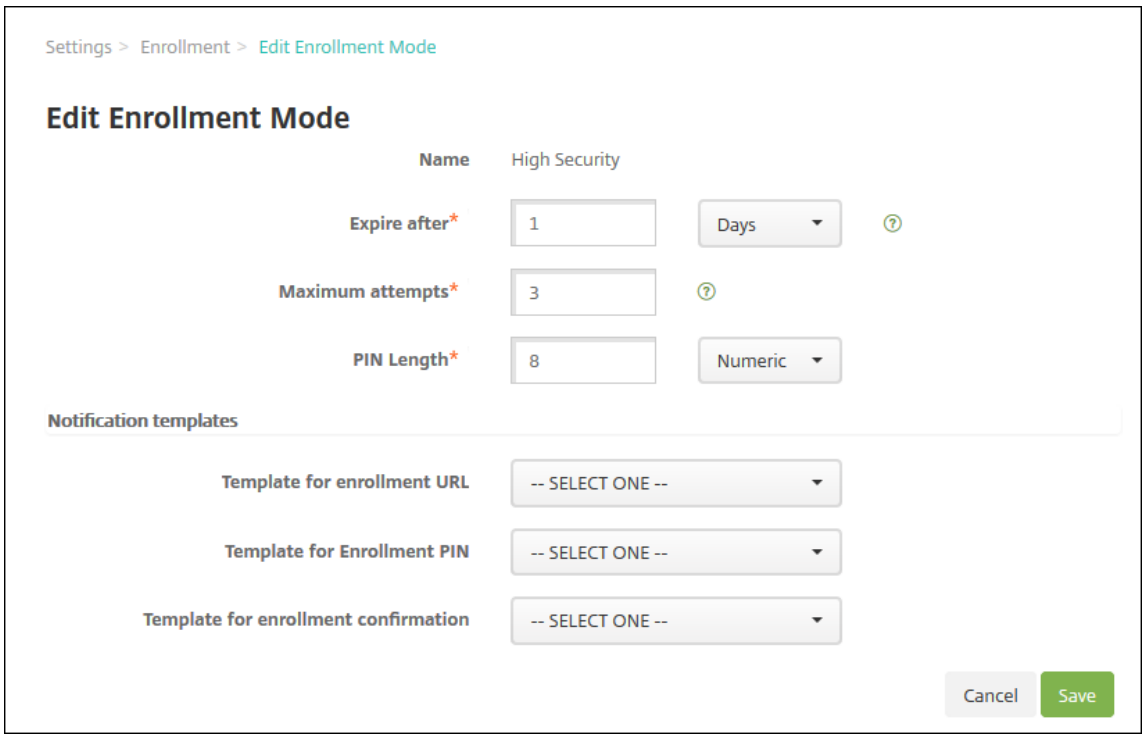
有关特定于平台的注册安全模式的信息，请参阅 各平台的注册安全模式。

可以将注册邀请用作限制为特定用户或组注册的功能的有效方式。要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。对于使用用户名 **+** 密码、双重身份验证或用户名 **+ PIN** 注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

您可以使用一次性 PIN（有时又称为 OTP）注册邀请作为双重身份验证解决方案。一次性 PIN 注册邀请控制用户可以注册的设备数量。OTP 邀请不适用于 Windows 设备。

编辑注册安全模式

1. 在注册列表中，选择注册安全模式，然后单击编辑。此时将显示编辑注册模式页面。根据所选择的模式，您可能会看到不同的选项。



2. 适当更改以下信息：

   - 此时间后过期：键入过期期限，过了此期限后用户将无法注册其设备。此值显示在用户和组注册邀请配置页面。

     键入 **0** 可防止邀请过期。

   - 天：在列表中，单击天或小时，对应于您在此时间后过期中输入的过期期限。
   - 最大尝试次数：键入用户可以尝试注册的次数，超出此次数后用户将被锁定，无法进行注册过程。此值显示在用户和组注册邀请配置页面。

     键入 **0** 表示尝试次数不受限制。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **PIN** 长度：键入用于设置生成的 PIN 的长度的数字。
- 数字：在列表中，单击数字或字母数字以选择 PIN 类型。
- 通知模板：
  - 注册 **URL** 模板：在列表中，单击用于注册 URL 的模板。例如，注册邀请模板向用户发送电子邮件。有关通知模板的详细信息，请参阅 创建或更新通知模板。
  - 注册 **PIN** 模板：在列表中，单击用于注册 PIN 的模板。
  - 注册确认模板：在列表中，单击用于向用户通知已成功注册的模板。

3. 单击保存。

将注册安全模式设为默认模式

除非您选择不同的注册安全模式，否则默认注册安全模式用于所有设备注册请求。如果没有将注册安全模式设置为默认模式，则必须为每个设备注册创建注册请求。

1. 如果未启用要用作默认值的注册安全模式，请选择它并单击 启用。唯一可以用作默认的注册安全模式是用 户名 **+** 密码、双因素或用 户名 **+ PIN** 码。
2. 选择注册安全模式，然后单击 默认。所选模式现已成为默认模式。如果将任何其他注册安全模式设为默认模式，此模式将不再作为默认模式。

禁用注册安全模式

禁用注册安全模式将使此模式不可供用户使用，既不可用于组注册邀请，也不可在自助服务门户中提供。您可以通过禁用一种注册安全模式并启用另一种注册安全模式来更改允许用户注册设备的方式

1. 选择注册安全模式。

   不能禁用默认注册安全模式。如果要禁用默认注册安全模式，必须首先删除其默认状态。

2. 单击禁用。注册安全模式不再处于启用状态。

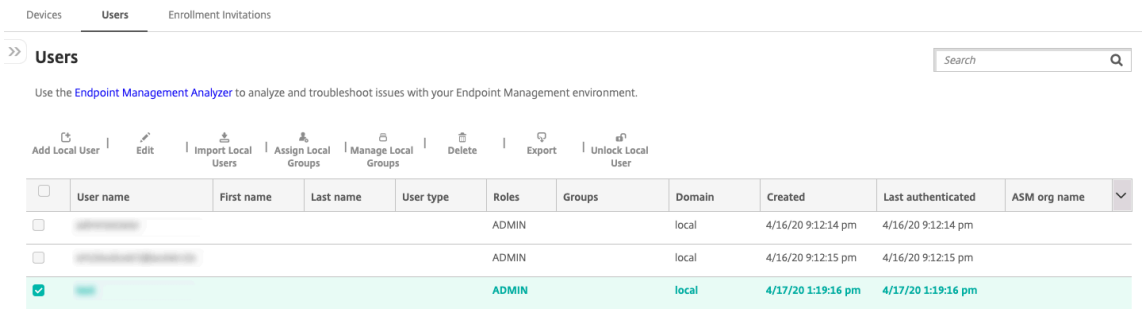
添加、编辑、解锁或删除本地用户帐户

可以手动向 Endpoint Management 中添加本地用户帐户，也可以使用预配文件导入帐户。有关从置备文件导入用户帐户的步骤，请参阅导入用户帐户。

所有 Citrix Cloud 管理员都是作为 Endpoint Management 管理员创建的。如果创建具有自定义访问权限的 Citrix Cloud 管理员，请确保访问包括 Endpoint Management。有关添加 Citrix Cloud 管理员的信息，请参阅 添加管理员。

1. 在 Endpoint Management 控制台中，单击管理 **>** 用户。此时将显示用户页面。

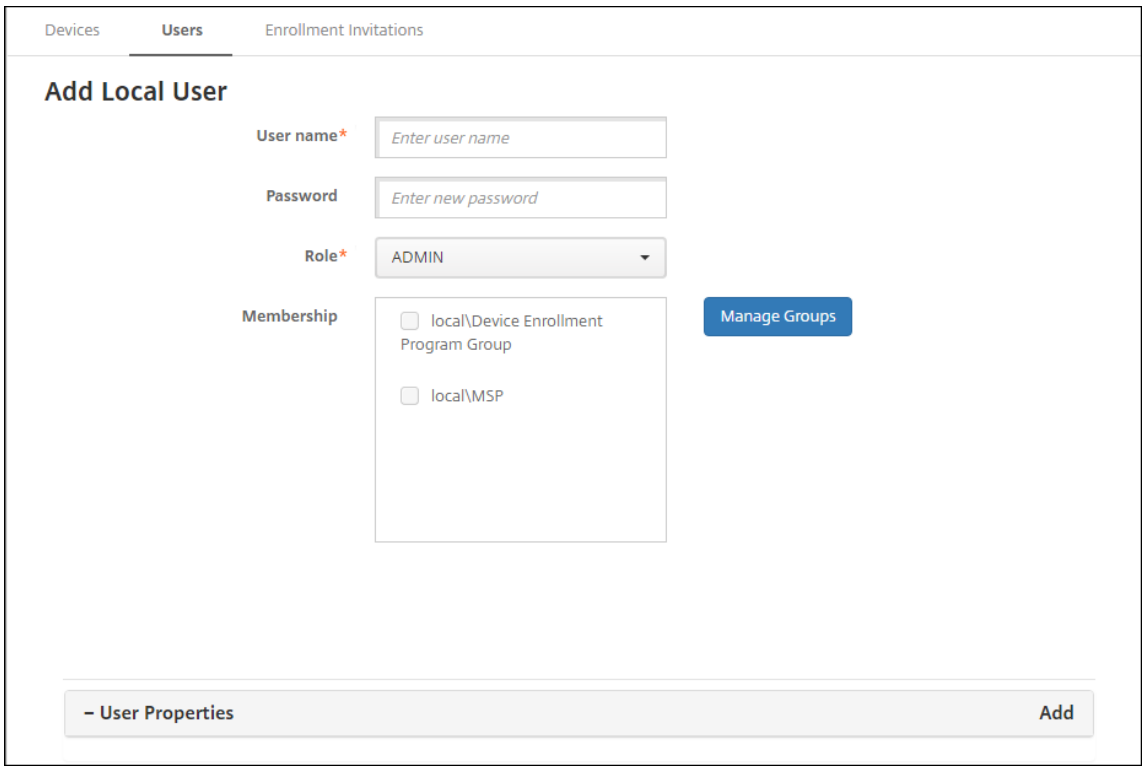
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 单击显示过滤器以过滤列表。

添加本地用户帐户

1. 在用户页面上，单击添加本地用户。此时将显示添加本地用户页面。



2. 配置以下设置：

   - 用户名：键入名称，这是必填字段。您可以在名称中包括以下内容：空格、大写字母和小写字母。
   - 密码：键入可选用户密码。密码的长度至少为 14 个字符，并且必须满足以下全部条件：
     - 至少包含两个数字
     - 至少包含一个大写字母和一个小写字母
     - 至少包含一个特殊字符
     - 不要包含字典单词或限制单词，例如 Citrix 用户名或电子邮件地址。
     - 不要包含三个以上的连续字符和重复字符或键盘模式，例如 1111、1234 或 asdf

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 角色：在列表中，单击用户角色。有关角色的更多信息，请参阅使用 RBAC 配置角色。可能的选项包括：
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- 成员身份：在列表中，单击要添加此用户的一个或多个组。
- 用户属性：添加可选用户属性。对于要添加的每个用户属性，单击添加，然后执行以下操作：
  - 用户属性：在列表中，单击某个属性，然后在该属性旁边的字段中键入用户属性。
  - 单击完成保存用户属性或单击取消。

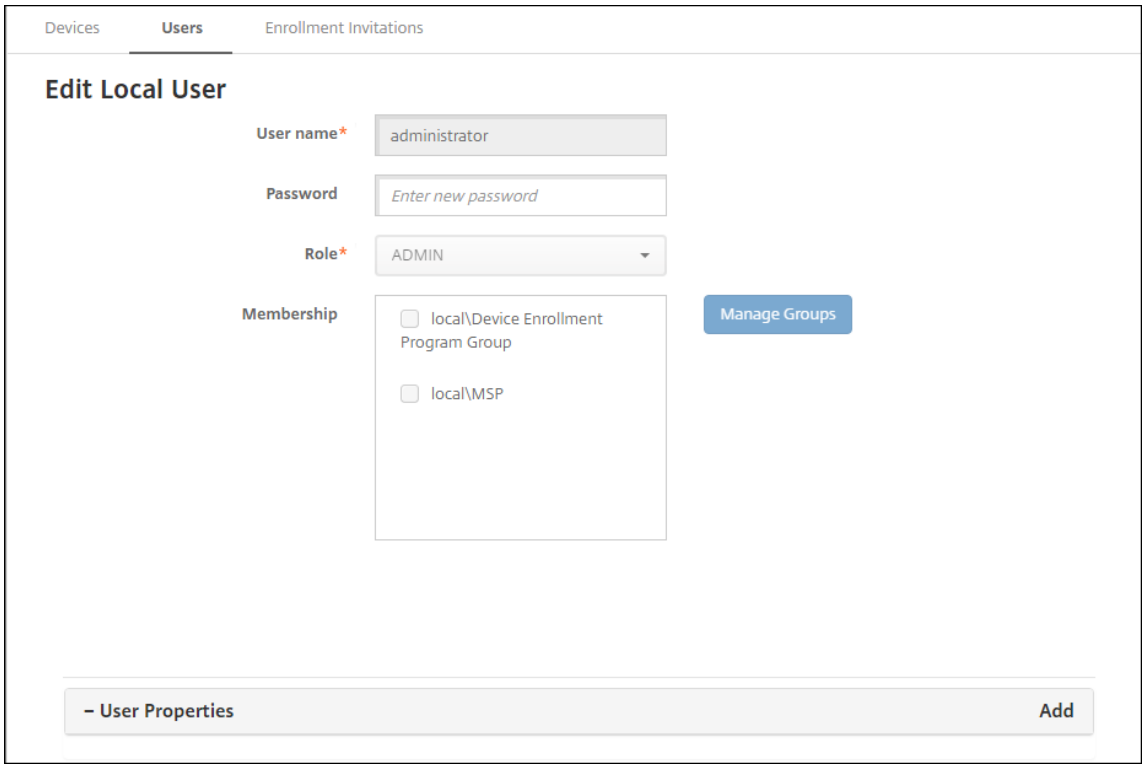
要删除现有用户属性，请将鼠标悬停在包含该属性的行上方，然后单击右侧的 **X** 。属性立即被删除。

要编辑现有用户属性，请单击属性并进行更改。单击完成保存更改后的列表，或者单击取消保留列表不变。

3. 单击保存。创建用户后，本地用户帐户的用户类型字段将保留为空。

编辑本地用户帐户

1. 在用户页面上的用户列表中，通过单击选择某个用户，然后单击编辑。此时将显示编辑本地用户页面。



2. 适当更改以下信息：
   - 用户名：无法更改用户名。
   - 密码：更改或添加用户密码。
   - 角色：在列表中，单击用户角色。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 成员身份：在列表中，单击要添加或编辑用户帐户的一个或多个组。要从组中删除用户帐户，请取消选中组名称旁边的复选框。
- 用户属性：请执行以下操作之一：
  - 对于您要更改的各个用户属性，请单击属性并进行更改。单击完成保存更改后的列表，或者单击取消保留列表不变。
  - 对于要添加的每个用户属性，单击添加，然后执行以下操作：
    * 用户属性：在列表中，单击某个属性，然后在该属性旁边的字段中键入用户属性。
    * 单击完成保存用户属性或单击取消。
  - 对于要删除的每个现有用户属性，请将鼠标悬停在包含此属性的行上，然后单击右侧的 **X**。属性立即被删除。

3. 单击保存以保存您所做的更改，或者单击取消保留用户不变。

解锁本地用户帐户

根据以下服务器属性，本地用户帐户被锁定：

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

  有关详细信息，请参阅 服务器属性定义。

当本地用户帐户被锁定时，您可以从 Endpoint Management 控制台解锁该帐户。

1. 在用户页面上的用户帐户列表中，通过单击选择某个用户帐户。
2. 单击解锁用户。此时将显示确认对话框。
3. 单击解锁以解锁用户帐户，或者单击取消保持用户不变。

无法从 Endpoint Management 控制台解锁 Active Directory 用户。锁定的 Active Directory 用户必须联系其 Active Directory 技术支持重置密码。

删除本地用户帐户

1. 在用户页面上的用户帐户列表中，通过单击选择某个用户帐户。

   可以通过选中每个用户帐户旁边的复选框，选择多个要删除的用户帐户。
2. 单击删除。此时将显示确认对话框。
3. 单击删除以删除用户帐户或单击取消。

删除 **Active Directory** 用户

要一次删除一个或多个 Active Directory 用户，请选择这些用户，然后单击删除。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

如果要删除的用户具有已注册的设备，而您希望重新注册这些设备，请先删除这些设备，然后再重新注册。要删除某个设备，请转至管理 > 设备，选择该设备，然后单击删除。

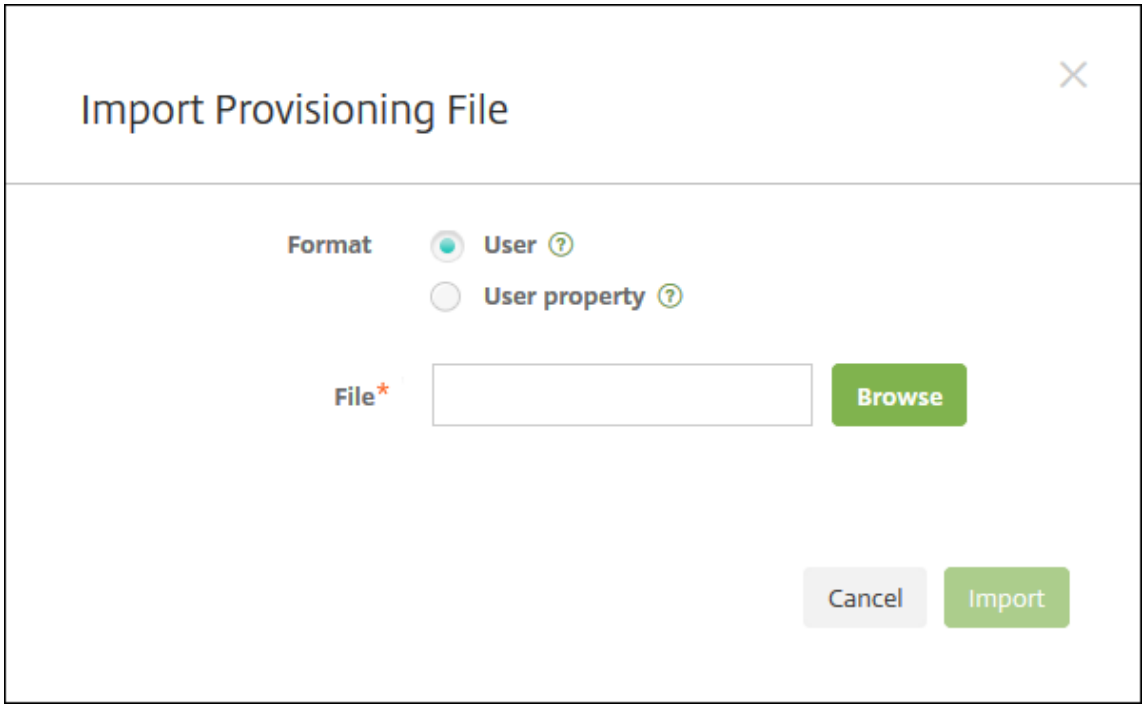
导入用户帐户

您可以从称为预配文件的.csv 文件导入本地用户帐户和属性，该文件可以手动创建。有关设置预配文件格式的详细信息，请参阅预配文件的格式。

> 注意：
>
> - 对于本地用户，请使用域名以及导入文件中的用户名。例如，指定 username@domain。如果在 Endpoint Management 中将创建或导入的本地用户用于托管域，则用户无法使用对应的 LDAP 凭据进行注册。
> - 如果将用户帐户导入到 Endpoint Management 内部用户目录，请禁用默认域以加快导入过程的速度。请注意，禁用域会影响注册。您可以在内部用户导入完成后重新启用默认域。
> - 本地用户可以采用用户主体名称 (UPN) 格式。但是，Citrix 建议您不要使用托管域。例如，如果 example.com 处于托管状态，请勿使用以下 UPN 格式创建本地用户：user@example.com。

准备好预配文件后，请按照以下步骤将此文件导入到 Endpoint Management 中。

1. 在 Endpoint Management 控制台中，单击管理 > 用户。此时将显示用户页面。
2. 单击导入本地用户。此时将显示导入预配文件对话框。



3. 对于要导入的预配文件的格式，选择用户或属性。
4. 通过单击浏览并导航到要使用的预配文件所在位置，选择此文件。
5. 单击导入。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

预配文件的格式

可以创建预配文件，并用其将用户帐户和属性导入 Endpoint Management。对预配文件使用以下格式之一：

- 用户置备文件字段： `user;password;role;group1;group2`
- 用户属性置备文件字段： `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> 注意：
>
> - 使用分号 (;) 分隔预配文件中的字段。如果某个字段的某一部分包含分号，请使用反斜杠字符 () 进行转义。例如，在预配文件中，按照 **propertyV;test;1;2** 格式键入属性 **propertyV; test;1;2**。
> - 角色的有效值为预定义的角色 USER、ADMIN、SUPPORT 和 DEVICE_PROVISIONING 以及您定义的任何其他角色。
> - 使用句点字符 (.) 作为分隔符来创建组层次结构。请勿在组名称中使用句点。
> - 属性预配文件中的属性使用小写。数据库区分大小写。

用户预配内容示例

条目 `user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` 表示：

- 用户： user01
- 密码： pwd; 01
- 角色： USER
- 组：
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

另一个示例 `AUser0;1.password;USER;ActiveDirectory.test.net` 表示：

- 用户： AUser0
- 密码： 1.password
- 角色： USER
- 组： ActiveDirectory.test.net

用户属性预配内容示例

条目 `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` 表示：

- 用户： user01
- 属性 **1**
  - 名称： propertyN
  - 值： propertyV;test;1;2

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

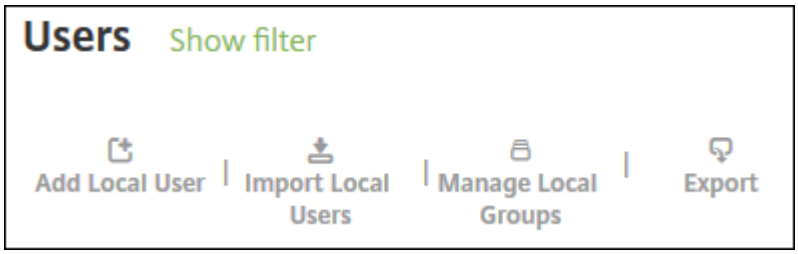
- 属性 **2**:
  - 名称： prop 2
  - 值： prop2 value

添加或删除组

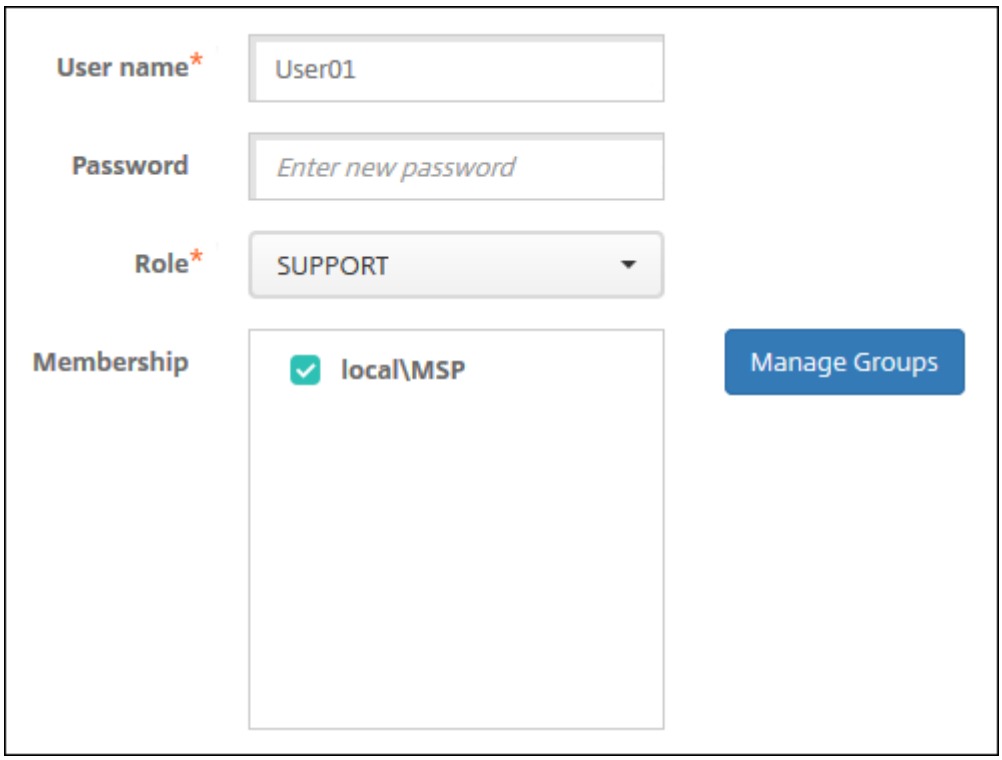
在 Endpoint Management 控制台中的以下页面上的管理组对话框中管理组：用户、添加本地用户或编辑本地用户。没用组编辑命令。

添加本地组

1. 执行以下操作之一：
   - 在用户页面上，单击管理本地组。

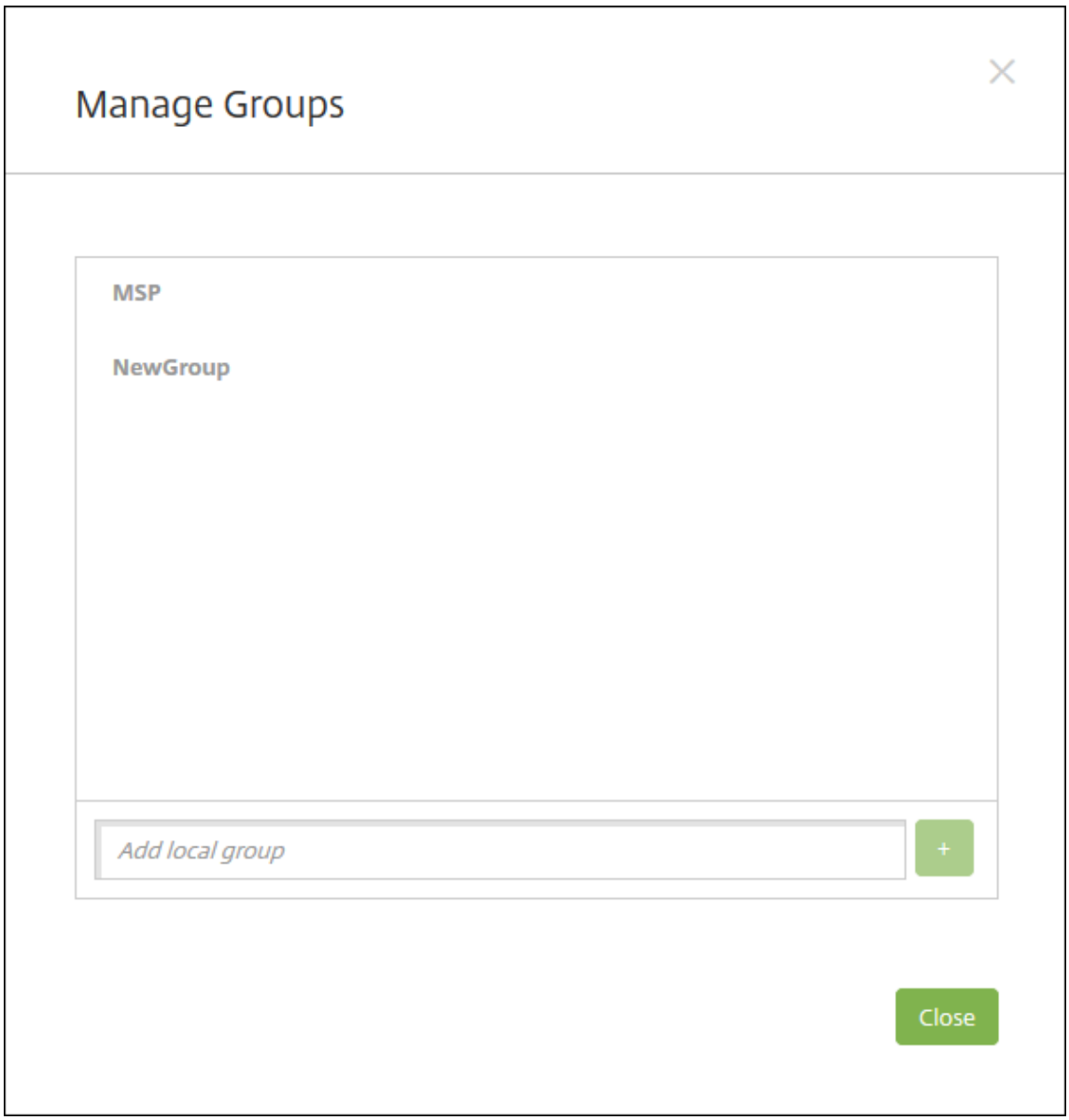


   - 在添加本地用户页面或编辑本地用户页面上，单击管理组。



   此时将显示管理组对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 在组列表下方，键入组名称，然后单击加号 (**+**)。用户组已添加到列表中。
3. 单击关闭。

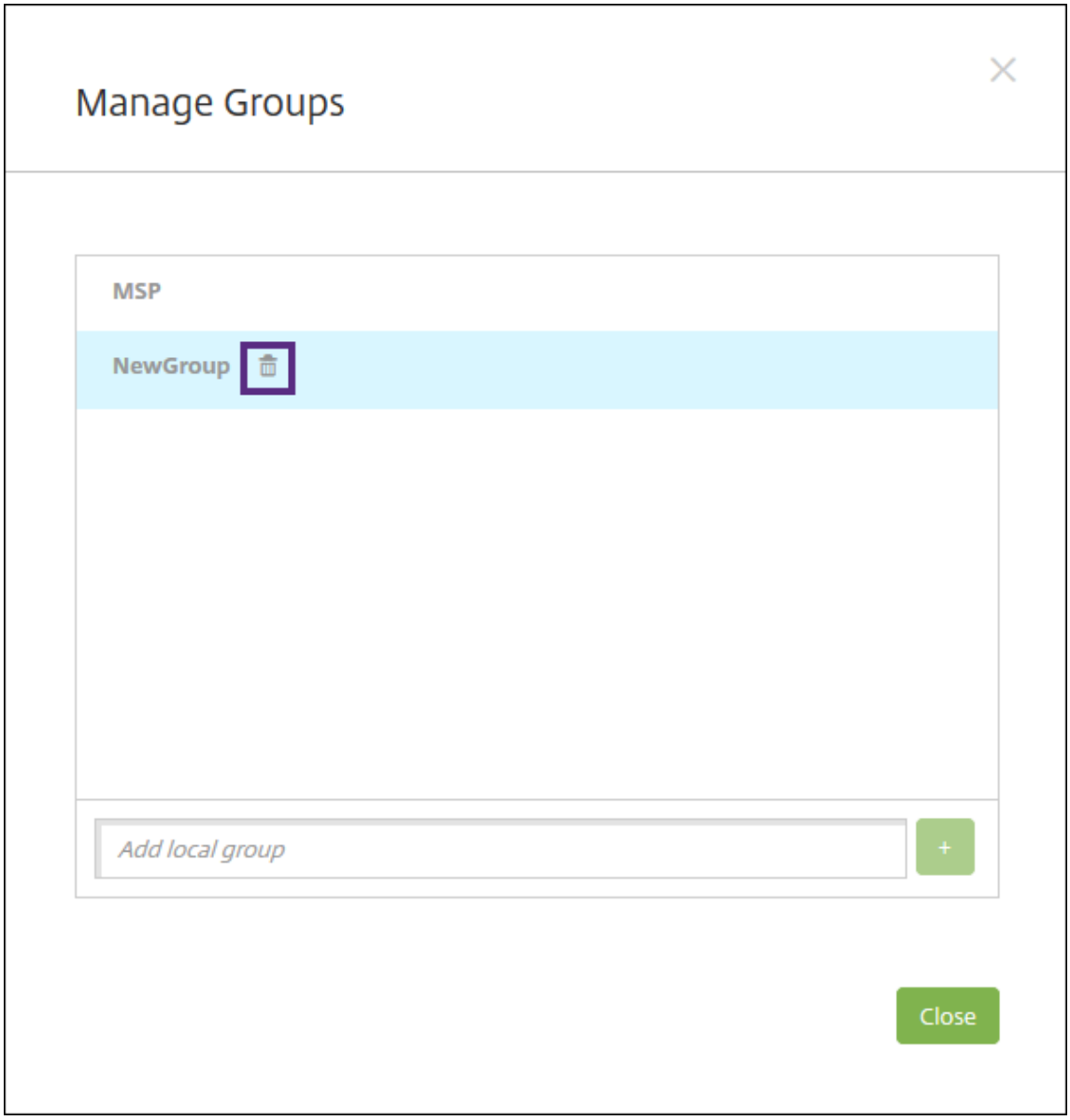
删除组

删除组不会影响用户帐户。相反，删除组将仅删除用户与该组的关联。用户还会丧失该组关联的交付组提供的应用程序或配置文件的访问权限。但是，任何其他组关联仍保持不变。如果用户不与任何其他本地组关联，这些用户将在顶层关联。

1. 执行以下操作之一：
   - 在用户页面上，单击管理本地组。
   - 在添加本地用户页面或编辑本地用户页面上，单击管理组。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

此时将显示管理组对话框。



2. 在管理组对话框上，单击要删除的组。
3. 单击组名称右侧的垃圾桶图标。此时将显示确认对话框。
4. 单击删除以确认操作并删除该组。

   > 重要：
   >
   > 此操作无法撤消。

5. 在管理组对话框上，单击关闭。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

创建和管理工作流

可以使用工作流对用户帐户的创建和删除进行管理。应先确定组织中有权批准用户帐户请求的人员，才能创建工作流。然后，使用工作流模板创建和批准用户帐户请求。

首次设置 Endpoint Management 时，要配置工作流电子邮件设置，您必须先配置此设置才能使用工作流。随时可以更改工作流电子邮件设置。这些设置包括电子邮件服务器、端口、电子邮件地址以及创建用户帐户的请求是否需要进行审批。

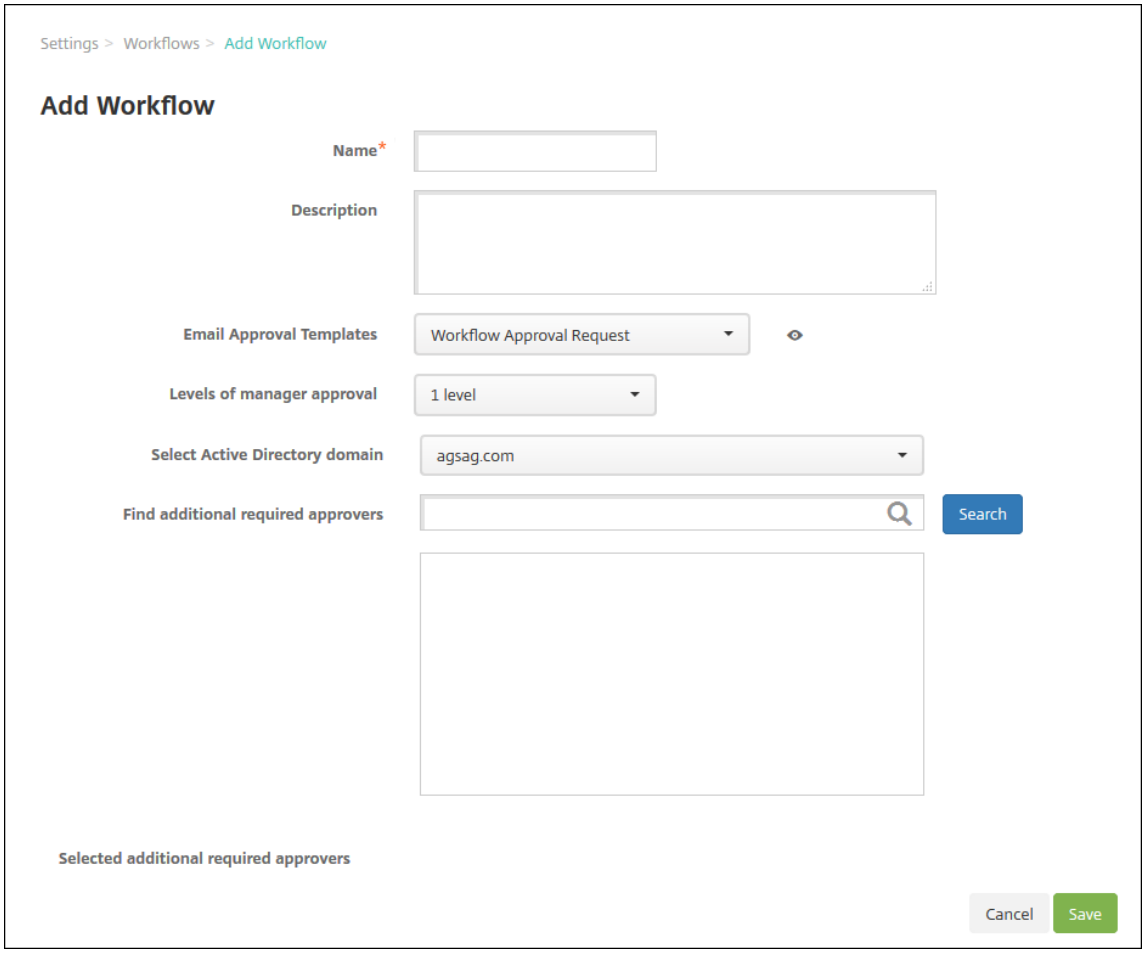
可以在 Endpoint Management 中的两个位置配置工作流：

- 在 Endpoint Management 控制台的设置 **>** 工作流页面中。在工作流页面上，可以配置多个用于应用程序配置的工作流。在“工作流”页面上配置工作流时，可以在配置应用程序时选择工作流。
- 配置应用程序连接器时，请在应用程序中提供工作流名称，然后配置审批用户帐户请求的人员。请参阅 添加应用。

可以为用户帐户分配最多三个经理审批级别。如果需要其他人员批准用户帐户，可以使用其姓名或电子邮件地址搜索和选择这些人员。Endpoint Management 找到相应的人员时，您可以将其添加到工作流中。工作流中的所有人员都将收到电子邮件，以批准或拒绝新用户帐户。

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击工作流。此时将显示工作流页面。
3. 单击添加。此时将显示添加工作流页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 配置以下设置：

   - 名称：键入工作流的唯一名称。
   - 说明：（可选）键入工作流的说明。
   - 电子邮件审批模板：在列表中，选择要指定的电子邮件审批模板。在 Endpoint Management 控制台中设置下方的通知模板部分创建电子邮件模板。单击此字段右侧的眼睛图标，即可预览正在配置的模板。
   - 经理审批级别：在列表中，选择此工作流所需的经理审批级别数。默认值为 **1** 级。可能的选项包括：
     - 不需要
     - 1 级
     - 2 级
     - 3 级
   - 选择 **Active Directory** 域：在列表中，选择用于工作流的合适 Active Directory 域。
   - 查找所需的其他审批者：在搜索字段中键入姓名，然后单击搜索。源于 Active Directory 的姓名。
   - 姓名显示在此字段中后，选中姓名旁边的复选框。姓名和电子邮件地址显示在选定的其他所需审批者列表中。
     - 要从列表中删除某个姓名，请执行以下操作之一：
       * 单击搜索以查找选定域中的所有人员列表。
       * 在搜索框中键入完整姓名或部分姓名，然后单击搜索以限制搜索结果。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

* 在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。滚动列表，并取消选中要删除的各个姓名旁边的复选框。

5. 单击保存。已创建的工作流显示在工作流页面上。

创建工作流后，您可以查看工作流详细信息，查看与工作流相关的应用程序，或者删除工作流。工作流创建后无法进行编辑。如果需要使用不同审批级别或审批者的工作流，请创建另一个工作流。

查看详细信息和删除工作流

1. 在工作流页面上的现有工作流列表中，选择一个特定的工作流。为此，请单击列表中的行，或者选中工作流旁边的复选框。
2. 要删除工作流，请单击删除。此时将显示确认对话框。再次单击删除。

> 重要：
>
> 此操作无法撤消。

注册配置文件

August 10, 2022

注册配置文件指定以下内容：

- 适用于 Android、iOS 和 Windows 设备的设备管理注册选项。
- 适用于 Android 和 iOS 设备的应用程序管理注册选项。
- 其他注册选项：
  - 是否限制用户可以注册的设备数量。
    如果达到设备限制，则将显示一条错误消息，通知用户已超出设备注册限制。
  - 是否允许用户拒绝设备管理。

可以使用注册配置文件在单个 Endpoint Management 控制台中合并多个用例和设备迁移路径。一些用例包括：

- 移动设备管理（仅 MDM）
- MDM+ 移动应用程序管理 (MAM)
- 仅 MAM
- 公司拥有的注册
- BYOD 注册（选择退出 MDM 注册的功能）
- 将 Android 设备管理员注册迁移到 Android Enterprise 注册（完全托管、工作配置文件、专用设备）
- 通过适用于 Windows 的工作区应用程序自动注册 Windows 10 和 Windows 11 设备（预览版）

如果您的当前站点为仅 MDM，并且您要添加 MAM，必须配置 Citrix Gateway。有关更多信息，请参阅 Citrix Gateway 要求。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

创建交付组时，可以使用名为 Global 的默认注册配置文件或者指定不同的注册配置文件。

按平台划分的注册配置文件功能包括以下内容。

- 对于 **Android** 设备：您可以指定管理模式和设备所有者模式。例如：公司拥有的设备，使用工作配置文件进行完全管理，以及 BYOD 工作配置文件。

  默认情况下，新设备在 Android Enterprise 中注册。可以选择使用旧版 Android 设备管理员 (DA) 模式管理设备。默认情况下，新设备也会在应用程序管理中注册。

  有关指定安全级别和所需注册步骤的信息，请参阅用户帐户、角色和注册。

- 对于 **iOS** 设备：您可以指定设备管理类型：**Apple** 用户注册、**Apple** 设备注册或 不管理设备。此 **Apple** 用户注册模式可作为公共预览版使用。要启用此功能，请联系您的支持团队。

  如果选择 Apple 用户注册，则可以选择为托管 Apple ID 使用自定义域并配置该域。

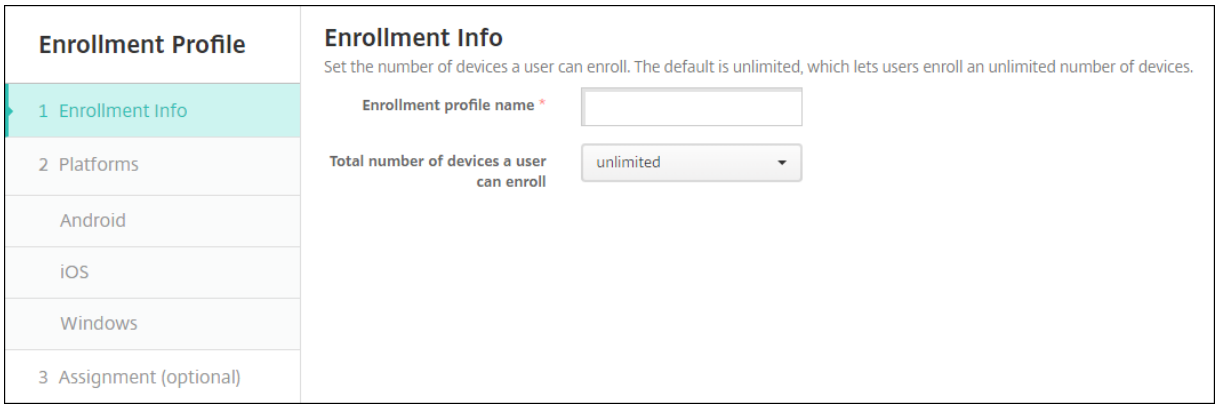
  默认情况下，新设备在 Apple 设备管理中注册。默认情况下，新设备也会在应用程序管理中注册。

- 对于 **Windows 10** 和 **Windows 11** 设备：您可以指定是否使用适用于 Windows 的 Citrix 设备管理。默认情况下，新设备在设备管理中注册。

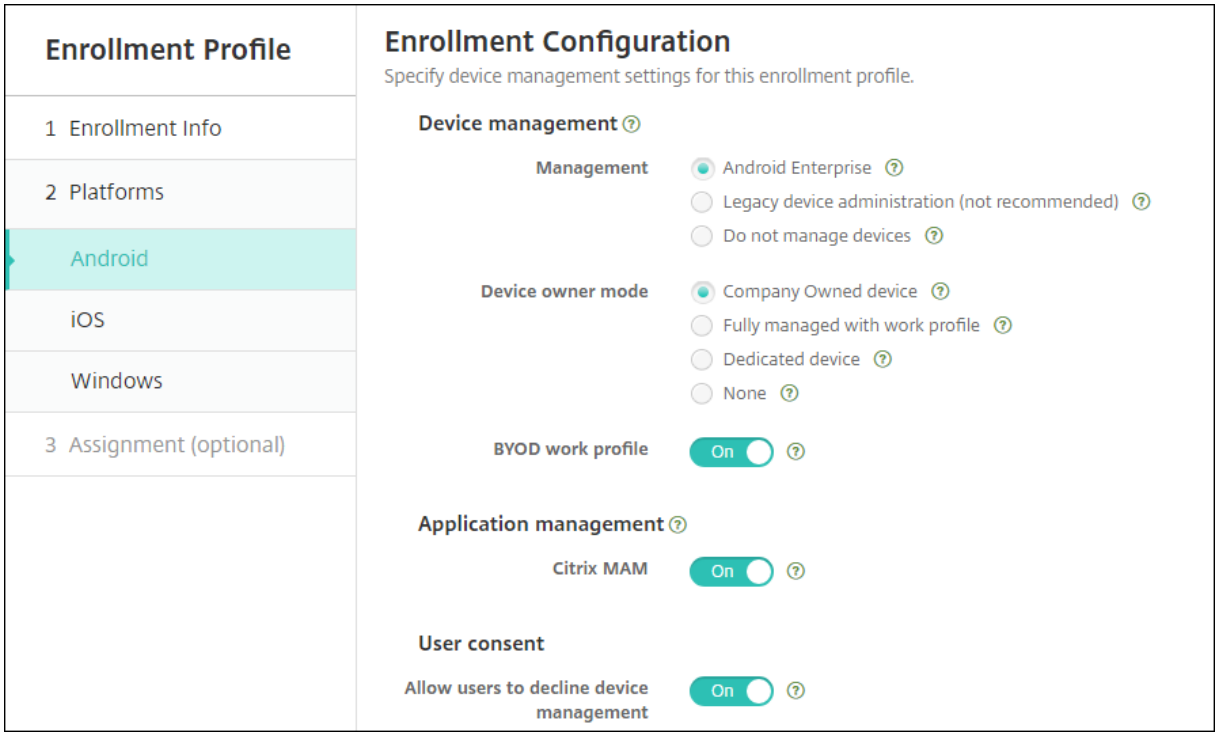
全局注册配置文件

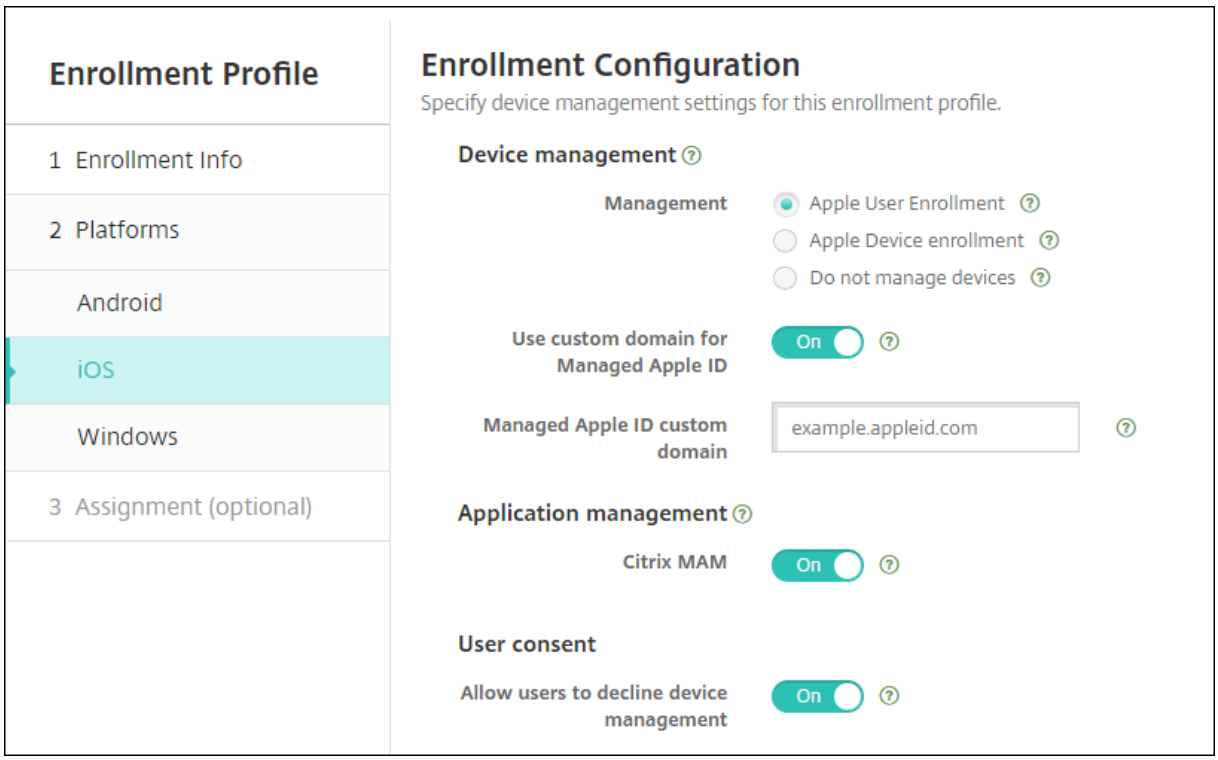
默认注册配置文件的名称为 Global。在您有机会创建注册配置文件之前，全局配置文件对测试非常有用。

如果您开始使用 Endpoint Management 20.2.1 或更高版本，则全局注册配置文件将具有预定义的设置。以下屏幕截图显示了全局注册配置文件的默认设置。只有 MAM 的部署才会显示这些选项的一部分。

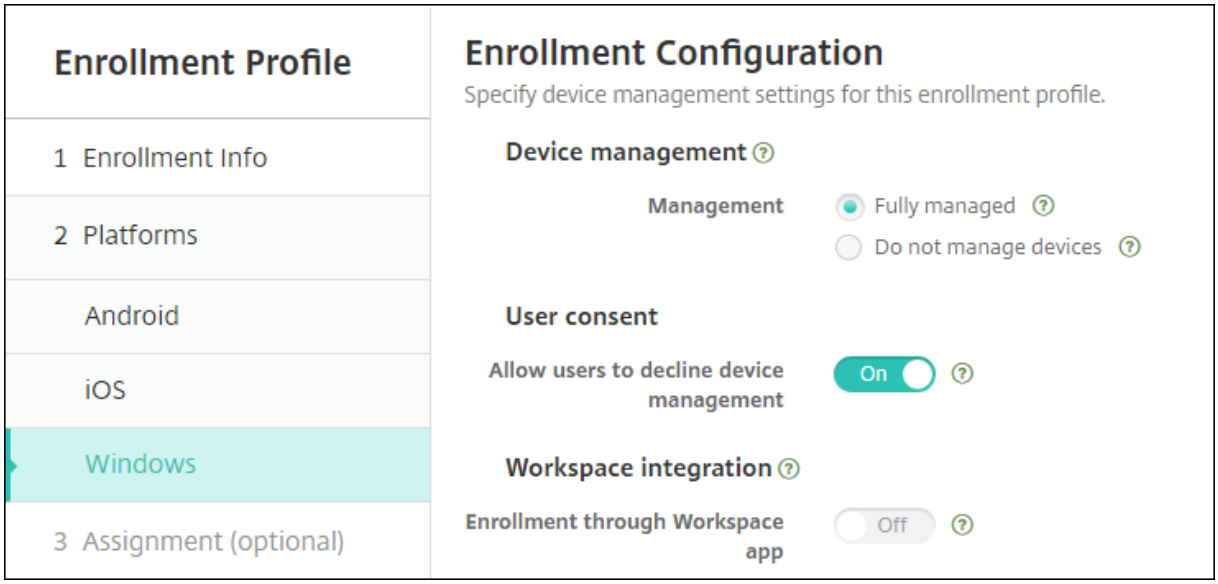


© 1999–2023 Cloud Software Group, Inc. All rights reserved.





© 1999–2023 Cloud Software Group, Inc. All rights reserved.



注册配置文件、交付组和注册

注册配置文件和交付组按如下所示进行交互：

- 可以将注册配置文件附加到一个或多个交付组。
- 如果用户属于具有不同注册配置文件的多个交付组，该交付组的名称决定使用的注册配置文件。Endpoint Management 选择按字母顺序排列的交付组列表中最后显示的交付组。例如，假设您有以下对象：
  - 两个注册配置文件，名为 “EP1” 和 “EP2”。
  - 两个交付组，名为 “DG1” 和 “DG2”。
  - “DG1” 与 “EP1” 相关联。
  - “DG2” 与 “EP2” 相关联。

  如果注册用户同时位于 “DG1” 和 “DG2” 交付组中，Endpoint Management 将使用 “EP2” 注册配置文件来确定用户的注册类型。
- 部署顺序仅适用于交付组中具有为 MDM（设备管理）配置的注册配置文件的设备。
- 设备注册后，对注册配置文件所做的某些更改需要重新注册：
  - 更改配置以将设备从 MDM+MAM 降级为 MAM 或 MDM 注册。更新注册配置文件或将设备移动到其他交付组时可能会发生降级。
  - 将 MAM 添加到为 MDM 配置的注册配置文件。
  - 将 MDM 添加到为 MAM 配置的注册配置文件。
- 切换到其他注册配置文件不会影响现有的已注册设备。但是，用户必须先取消注册然后重新注册这些设备，才能使更改生效。

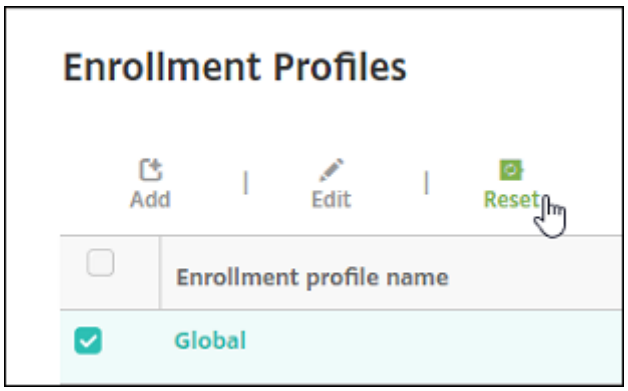
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

创建注册配置文件

1. 在 Endpoint Management 控制台中，转到配置 **>** 注册配置文件。
2. 在注册信息页面上，键入配置文件的描述性名称。默认情况下，用户可以注册的设备数不受限制。选择一个值以限制每个用户的设备数量。此限制适用于用户注册的 MAM 或 MDM 托管 Android、iOS 和 Windows 设备的总和。
3. 完成平台页面。有关特定于平台的注册设置的信息，请参阅：
   - Android Enterprise：创建注册配置文件
   - iOS：支持的注册方法
   - Windows 桌面和平板电脑：支持的注册方法
4. 在分配页面上，将一个或多个交付组附加到注册配置文件。

   用户可能属于具有不同注册配置文件的多个交付组。在这种情况下，交付组的名称决定使用的注册配置文件。Endpoint Management 选择按字母顺序排列的交付组列表中最后显示的交付组。要创建交付组，请转到配置 **>** 交付组。

您的注册配置文件列表显示在配置 **>** 注册配置文件页面上。要编辑全局配置文件或将其重置为原始默认设置，请选择全局配置文件对应的行，然后单击重置。您无法删除全局配置文件。



通知

June 9, 2022

可以将 Endpoint Management 中的通知用于以下目的：

- 与选择的用户组通信以使用多个系统相关功能。也可以将这些通知发送给特定用户。例如，使用 iOS 设备的所有用户、设备不合规的用户、使用员工自带设备的用户等。
- 注册用户及其设备
- 满足某些条件时自动通知用户（使用自动化操作）。例如：
  - 由于合规性问题阻止用户设备访问企业域时

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 设备已被越狱或获得 Root 权限时

有关自动操作的详细信息，请参阅 自动操作。

要使用 Endpoint Management 发送通知，必须配置网关和通知服务器。您可以在 Endpoint Management 中设置通知服务器来配置 SMTP 服务器。这些服务器向用户发送电子邮件通知。您可以使用通知通过 SMTP 发送邮件。

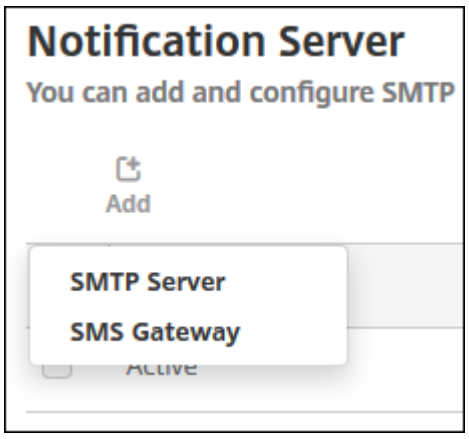
- SMTP 是一种面向连接的基于文本的协议，其中邮件发件人与邮件接收人进行通信。邮件发件人发出命令字符串并提供必要的数据，通常通过 TCP 连接。SMTP 会话包括来自 SMTP 客户端（邮件发送人员）的命令和来自 SMTP 服务器的相应响应。

必备条件

- 可配置 SMTP 通知服务器以向用户发送消息。如果此服务器托管在内部服务器上，请联系系统管理员以获取配置信息。如果此服务器是托管的邮件服务，请在服务提供商的 Web 站点上查找适当的配置信息。
- 您只能使用一个活动的 SMTP 服务器。此通信通道只允许一个活动配置。
- 从位于网络的 DMZ 中的 Endpoint Management 打开端口 25 以指回内部网络上的 SMTP 服务器。这样，Endpoint Management 能够成功发送通知。

配置 **SMTP** 服务器

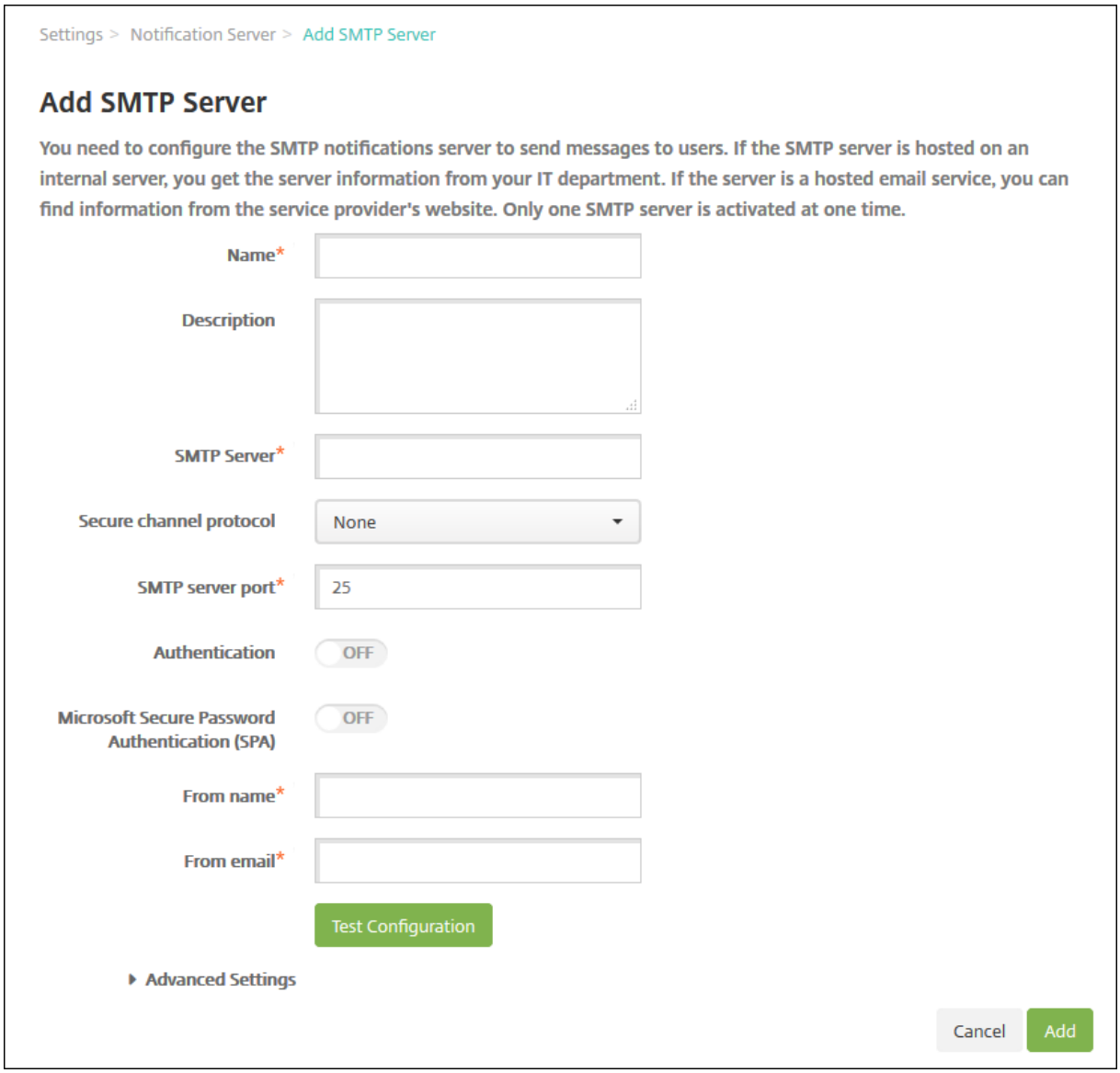
1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在通知下方，单击通知服务器。此时将显示通知服务器页面。
3. 单击添加。出现一个菜单，其中包含用于配置 SMTP 服务器的选项。



- 要添加 SMTP 服务器，请单击 **SMTP** 服务器，然后参阅添加 SMTP 服务器 以了解配置此设置的步骤。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

添加 **SMTP** 服务器



1. 配置以下设置：

   - 名称：键入与此 SMTP 服务器帐户关联的名称。
   - 说明：（可选）输入服务器的说明。
   - **SMTP** 服务器：键入服务器的主机名。指定完全限定域名 (FQDN) 或 IP 地址。
   - 安全通道协议：在列表中，单击 **SSL**、**TLS** 或无选择服务器使用的安全通道协议（如果服务器配置为使用安全身份验证）。默认值为无。
   - **SMTP** 服务器端口：键入 SMTP 服务器使用的端口。默认情况下，此端口设置为 25。如果 SMTP 连接使用 SSL 安全通道协议，请将端口设置为 465。
   - 身份验证：选择开或关。默认值为关。
   - 如果启用身份验证，请配置以下设置：
     - 用户名：键入进行身份验证时使用的用户名。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 密码：键入身份验证用户的密码。
- **Microsoft** 安全密码身份验证 **(SPA)**：如果 SMTP 服务器使用的是 SPA，请单击开。默认值为关。
- 发件人姓名：键入客户端接收来自此服务器的通知电子邮件时，显示在发件人框中的姓名。例如，公司 IT。
- 发件人电子邮件：键入电子邮件收件人回复 SMTP 服务器发送的通知时使用的电子邮件地址。

2. 单击测试配置以发送测试电子邮件通知。
3. 展开高级设置，然后配置以下设置：
   - **SMTP** 重试次数：键入 SMTP 服务器发送邮件失败的重试次数。默认值为 5。
   - **SMTP** 超时：键入发送 SMTP 请求时等待的持续时间（秒）。如果频繁出现因超时导致消息发送失败的情况，请增加此值。降低此值时请格外小心，以避免增加超时次数和未送达的消息。默认值为 30 秒。
   - **SMTP** 收件人数量上限：键入 SMTP 服务器发送的每封电子邮件的收件人数量上限。默认值为 100。
4. 单击添加。

创建和更新通知模板

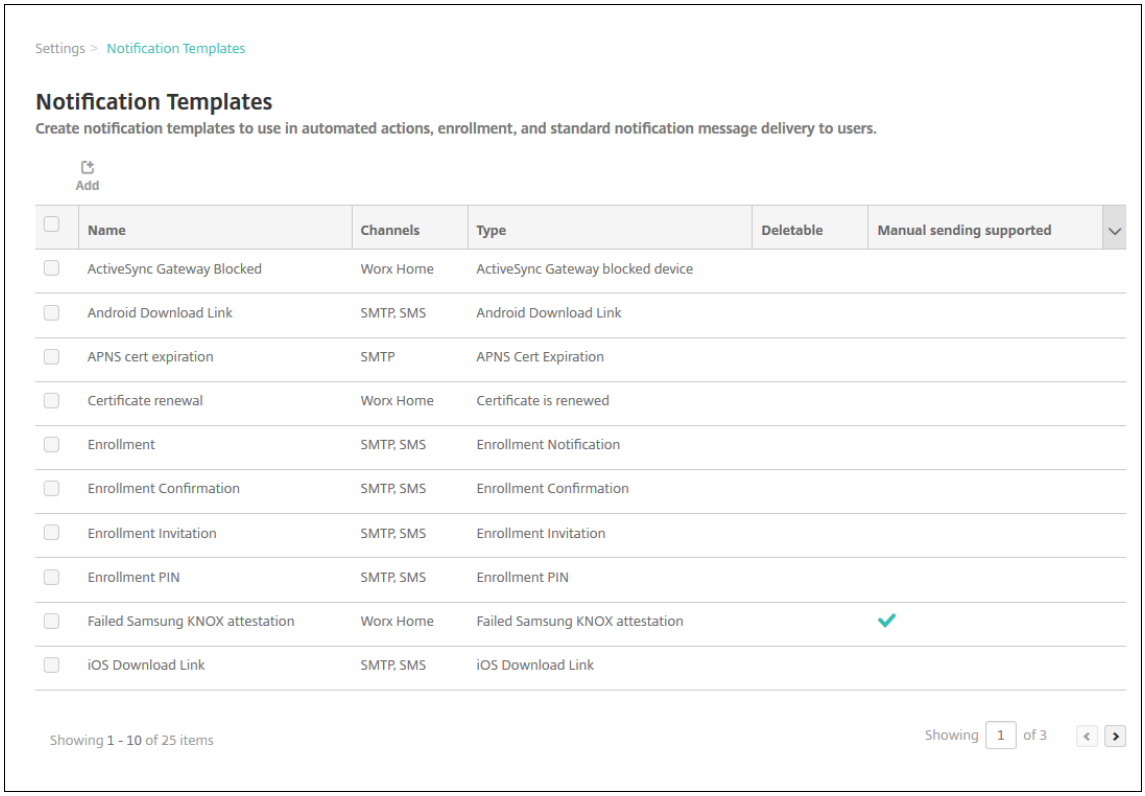
可以在 Endpoint Management 中创建或更新用于自动化操作、注册和发送给用户的标准通知消息的通知模板。可以将通知模板配置为通过两个不同的通道来发送消息：Secure Hub 或 SMTP。

Endpoint Management 包括许多预定义的通知模板。这些模板反映了 Endpoint Management 为系统中的每个设备自动响应的不同类型的事件。

> 注意：
>
> 如果您计划使用 SMTP 通道向用户发送通知，则必须先设置通道，然后才能激活它们。如果尚未设置通道，当添加通知模板时，Endpoint Management 会提示您设置通道。

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击通知模板。此时将显示通知模板页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



添加通知模板

1. 单击添加。如果未设置 SMTP 服务器，则会显示有关使用 SMTP 通知的消息。您可以选择立即设置 SMTP 服务器或稍后设置。

   如果您选择立即设置 SMTP 服务器设置，则会将您重定向到“设置”页面上的“通知服务器”页面。设置了要使用的通道后，可以返回通知模板页面，继续添加或修改通知模板。

   > 重要：
   >
   > 如果您选择稍后设置 SMTP 服务器设置，则在添加或编辑通知模板时将无法激活这些通道。因此，这些通道不可用于发送用户通知。

2. 配置以下设置：

   - 名称：键入模板的描述性名称。
   - 说明：键入模板的说明。
   - 类型：在列表中，单击通知类型。仅显示选定类型支持的通道。仅允许一个 APNS 证书过期模板，此为预定义模板。您无法添加此类型的模板。

   > 注意：
   >
   > 对于某些模板类型，类型的下面会显示短语“支持手动发送”。这些模板类型可以在控制板和设备的通知列表页面上找到。可以从这些位置手动向用户发送通知。在“主题”或“消息”字段中使用以下宏的任何模板

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 在任何通道上均不可以使用手动发送。

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

> 注意：
>
> Endpoint Management 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

3. 在通道下方，配置用于此通知的每个通道的信息。可以选择任何通道或所有通道。您选择的通道取决于您希望发送通知的方式。

   - 如果选择 **Secure Hub**，则仅 iOS 和 Android 设备接收通知，通知将显示在设备的通知托盘中。
   - 如果选择 **SMTP**，使用其电子邮件地址注册的用户将收到该邮件。

   Secure Hub：

   - 激活：单击以启用通知通道。
   - 消息：键入要发送给用户的消息。如果使用的是 Secure Hub，此字段为必填字段。有关在消息中使用宏的信息，请参阅宏。
   - 声音文件：在列表中，单击用户收到通知时听到的通知声音。

   SMTP：

   - 激活：单击以启用通知通道。

     只能在设置 SMTP 服务器后，才能激活 SMTP 通知。

   - 发件人：键入通知的可选发件人，可以是姓名或/和电子邮件地址。
   - 收件人：此字段包含除临时通知以外的所有通知的预置宏，以确保通知发送到正确的 SMTP 收件人地址。Citrix 建议您不要修改模板中的宏。可以通过在此字段中添加其地址来添加更多收件人（例如公司管理员）。使用分号 (;) 分隔宏与其他地址。要发送临时通知，可以输入特定收件人，也可以从管理 **>** 设备页面选择设备并从此处发送通知。有关详细信息，请参阅 设备。
   - 主题：键入通知的描述性主题。此字段为必填字段。
   - 消息：键入要发送给用户的消息。有关在消息中使用宏的信息，请参阅宏。

4. 单击添加。正确配置所有通道后，它们将按以下顺序显示在“通知模板”页面上：SMTP 和 Secure Hub。未正确配置的通道将在经过正确配置后显示。

编辑通知模板

1. 选择通知模板。此时将显示特定于该模板的编辑页面。可以编辑模板（类型字段除外）以及激活或停用通道。
2. 单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

删除通知模板

您只能删除自己添加的通知模板。不能删除预定义的通知模板。

1. 选择现有通知模板。
2. 单击删除。此时将显示确认对话框。
3. 单击删除以删除通知模板，或单击取消以取消删除通知模板。

使用 **RBAC** 配置角色

July 24, 2023

Endpoint Management 中基于角色的访问控制 (RBAC) 功能允许您为用户和组分配角色。角色是一组权限，用于控制用户对系统功能的访问级别。

Endpoint Management 附带以下默认用户角色。可以将默认角色用作您自定义的用于创建自己的用户角色的模板。

- 管理员：授予完整系统访问权限。
- 用户：允许用户注册设备和访问自助服务门户。

可以使用 Endpoint Management 中的 RBAC 功能执行以下操作：

- 创建和编辑用户角色。
- 将角色分配给本地用户组和 Active Directory (AD) 组。
- 通过 **Identity and Access Management**（身份和访问管理）**> Administrators**（管理员）将角色分配给 Citrix Cloud 中的管理员。请参阅向 Citrix Cloud 管理员添加角色。

使用 **RBAC** 功能

可以将角色分配给本地用户、云管理员（在 Citrix Cloud 中）以及本地用户组和 Active Directory 组。

- 本地用户：使用管理 **>** 用户向本地用户分配角色。只能为本地用户分配一个角色。要更改角色，可以手动编辑用户帐户。或者，也可以为本地用户创建一个组，并为该组分配一个角色。
- 云管理员：云管理员是 Citrix Cloud 在将管理员添加到您的 Citrix Cloud 客户帐户时创建的一个特殊用户帐户。云管理员帐户使用与 Citrix Cloud 上的管理员帐户相同的用户名。在 Endpoint Management 控制台中创建 RBAC 角色，并在 Citrix Cloud 中通过 **Identity and Access Management**（身份和访问管理）**> Administrators**（管理员）向这些用户分配角色。
- **Active Directory** 组： Active Directory 组中的所有用户都具有相同的权限。如果用户属于多个 Active Directory 组，所有权限将合并以定义该用户的权限。例如，假设 ADGroupA 用户可以定位经理的设备，而 ADGroupB 用户可以擦除员工的设备。属于两个组的用户可以找到并擦除经理和员工的设备。如果用户属于具有冲突权限的组，则以允许的权限为准。

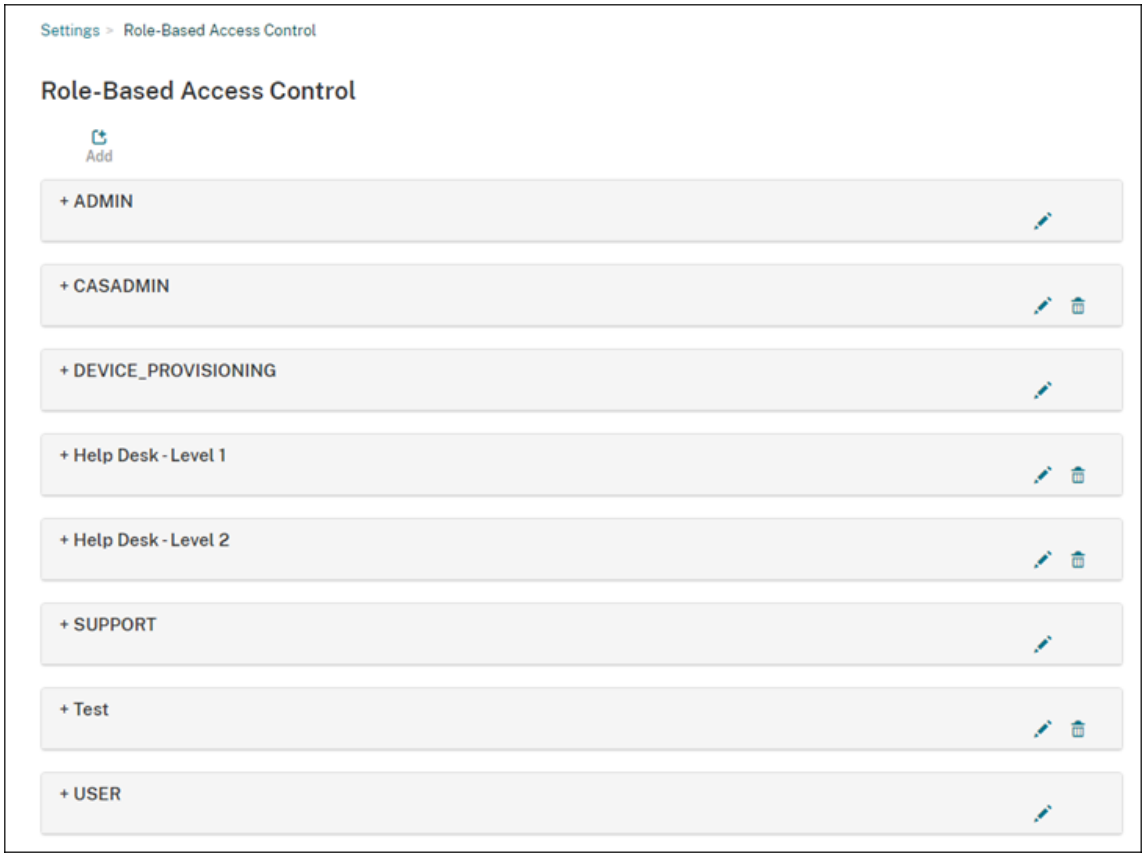
有关详细信息，请参阅关于用户帐户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

创建或编辑角色

1. 在 Endpoint Management 控制台中，要访问设置页面，请单击右上角的齿轮图标。
2. 单击基于角色的访问控制。基于角色的访问控制页面显示默认用户角色以及您添加的任何角色。

   单击某个角色旁边的加号 (+) 可查看该角色的所有权限。



3. 要添加角色，请单击添加。或者，要编辑某个角色，请单击现有角色右侧的笔。

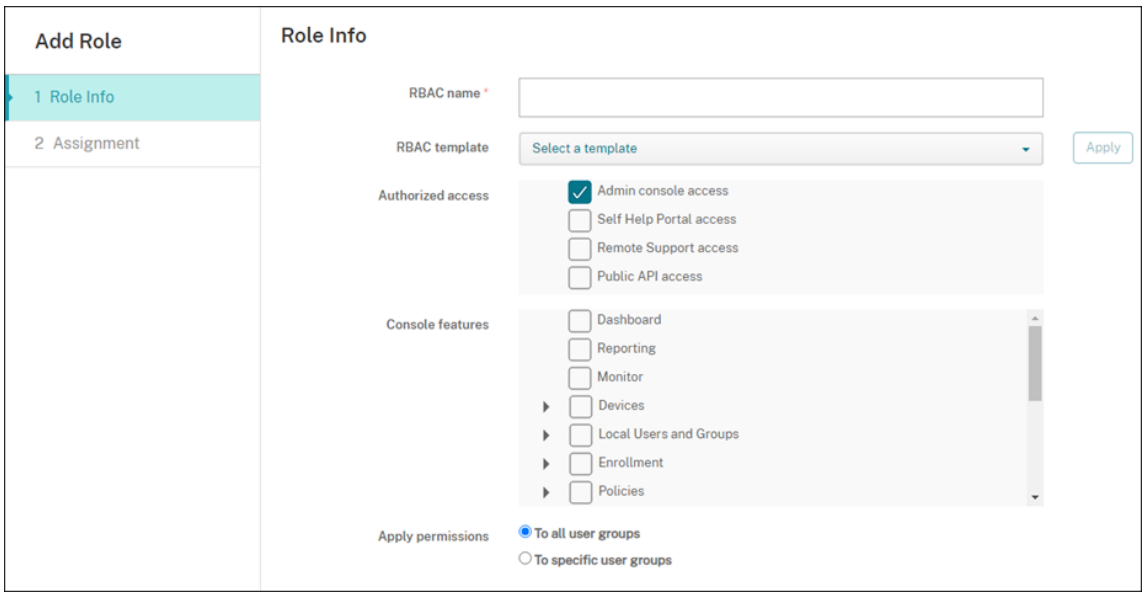
   > 注意：
   >
   > 可以通过单击您定义的角色右侧的垃圾桶来删除角色。无法删除默认用户角色。

4. 在添加角色页面上，输入以下信息：

   - **RBAC** 名称：输入新用户角色的描述性名称。无法更改现有角色的名称。
   - **RBAC** 模板：（可选）选择某个模板以将其作为新角色的起点。（编辑角色时，无法选择或更改模板。）RBAC 模板是用于定义系统功能访问权限的默认用户角色。

   单击应用按钮以填充授权访问和控制台功能复选框。Endpoint Management 使用选定模板的预定义访问权限和功能权限填充这些字段。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



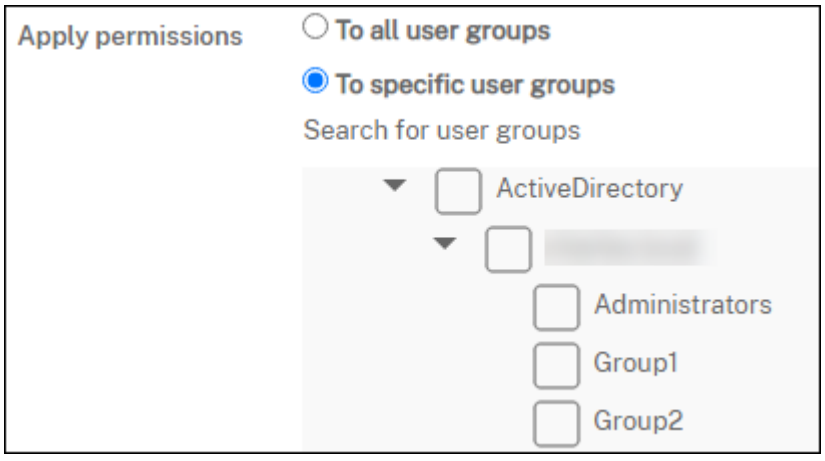
5. 要自定义角色，请选中或取消选中授权访问和控制台功能中的复选框。

   单击控制台功能旁边的三角形可显示并选择该功能特定的权限。单击顶层的复选框不会选择各个权限。请展开顶层权限后选择各个选项。

6. **Apply permissions**（应用权限）：单击 **To specific user groups**（至特定用户组）以对选择的组应用权限。

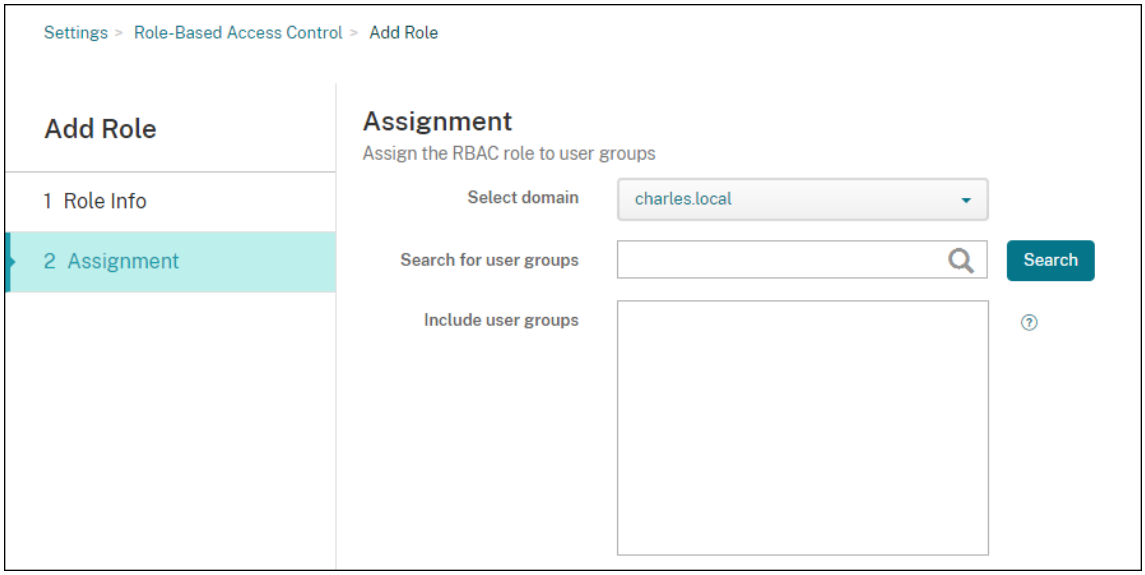
   例如，如果 RBAC 管理员具有 ActiveDirectory 用户组的权限：

   - 管理员只能访问 ActiveDirectory 组中的用户的信息。
   - 管理员无法查看任何其他本地或 AD 用户。管理员可以查看属于这些组的子组成员的用户。
   - 管理员可以发送邀请至：
     - 权限组及其子组
     - 属于权限组及其子组的成员的用户



7. 单击下一步，输入以下信息，以将角色分配给用户组。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 选择域：在列表中，选择一个域。
- 搜索用户组：单击搜索可查看所有可用组的列表。键入完整组名称或部分组名称以缩小搜索范围。
- 包括用户组：在显示的列表中，选择要向其分配角色的用户组。

8. 单击保存。

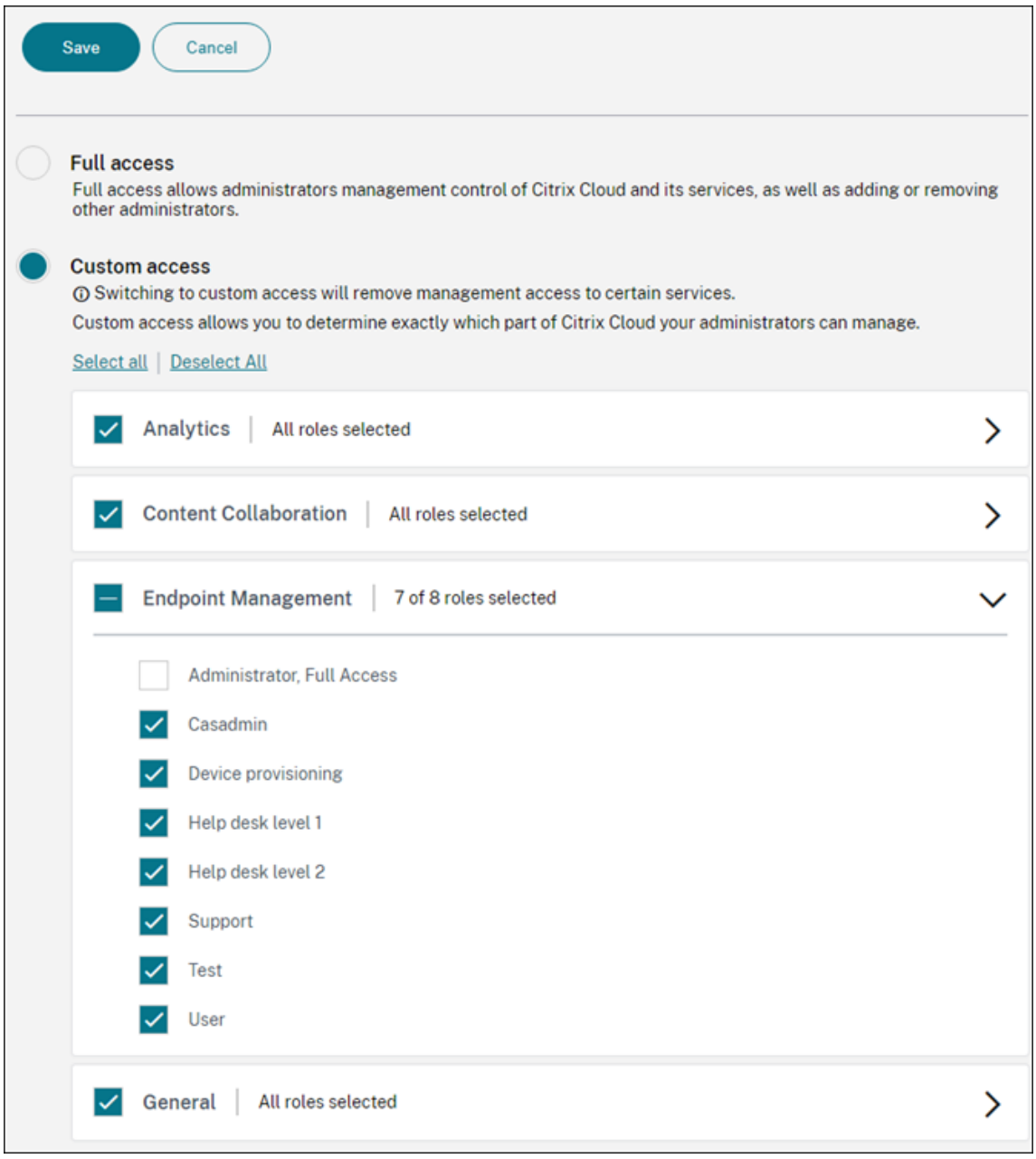
向 **Citrix Cloud** 管理员添加角色

无需通过 Endpoint Management 控制台向 Citrix Cloud 管理员分配 RBAC 角色，而应从 Citrix Cloud 控制台分配角色。

1. 在 Citrix Cloud 控制台中，导航到 **Identity and Access Management**（身份和访问管理）**> Administrators**（管理员）。
2. 选择身份提供程序，然后键入电子邮件地址以添加管理员。单击 **Invite**（邀请）。

   单击现有管理员行结尾的 **...** 可编辑这些权限。
3. 单击 **Custom access**（自定义访问权限）。向管理员分配权限时，可以选择在 Endpoint Management 控制台中创建的 RBAC 角色。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 单击 **Send Invite**（发送邀请）以向新管理员发送邀请，或者单击 **Save**（保存）完成对管理员的编辑。

预定义的角色

每个预定义的 RBAC 角色都具有某些关联的访问权限和功能权限。以下各表介绍了管理员角色和用户角色的每种权限。不能删除或编辑预定义的角色。

- 要获取每个内置角色的默认权限的完整列表，请下载基于角色的访问控制默认设置
- 有关 Endpoint Management 用户帐户的信息，请参阅关于用户帐户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 在“设置”权限下，RBAC 权限向管理员用户授予完全访问权限，包括分配自己的权限的能力。请仅向打算提供控制 Endpoint Management 系统中的所有对象的功能的用户授予此访问权限。

管理角色

预定义的管理员角色在 Endpoint Management 中提供特定的访问权限。默认情况下，启用授权访问（自助服务门户除外）、控制台功能以及应用权限。

，可以使用 **Manage**（管理）**> Users**（用户）更改分配了管理员角色的本地用户的角色。对于具有管理员角色的云用户，请使用 Citrix Cloud 控制台更改角色。默认情况下，具有管理员角色的云和本地用户具有完全访问权限。

管理员的授权访问权限

管理控制台访问	管理员可以访问 Endpoint Management 控制台上的所有功能。
自助门户访问	默认情况下，管理员无法访问自助服务门户。（具有用户角色的用户只能访问自助服务门户。）
远程支持访问	管理员可以访问远程支持功能。
公共 API 访问	管理员可以访问公共 API，以便以编程方式执行可以在 Endpoint Management 控制台上执行的操作。这些操作包括管理证书、应用程序、设备、交付组和本地用户。

面向管理员的控制台功能

管理员对 Endpoint Management 控制台具有不受限制的访问权限。

控制板	控制板是管理员在登录 Endpoint Management 控制台后看到的第一个页面。控制板显示有关通知和设备的基本信息。
报告	分析 **>** 报告页面提供预定义的报告，您可以利用这些报告分析应用程序和设备部署情况。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备	在管理 **>** 设备页面中，可以管理用户设备。可以在此页面上逐个添加设备，也可以通过导入设备预配文件一次添加多个设备。
本地用户和组	在管理 **>** 用户页面中，可以添加、编辑或删除本地用户和本地用户组。
注册	在管理 **>** 注册邀请页面中，可以管理如何邀请用户在 Endpoint Management 中注册其设备。
策略	“ 配置**” > “**设备策略” 页面是管理设备策略（例如 VPN 和网络）的位置。
应用程序	在配置 **>** 应用程序页面中，可以管理用户能够在其设备上安装的各种应用程序。
媒体	在配置 **>** 媒体页面中，可以管理用户能够在其设备上安装的各种媒体。
操作	在配置 **>** 操作页面中，可以管理触发事件的响应。
交付组	在配置 **>** 交付组页面中，可以管理交付组以及与其关联的资源。
注册配置文件	在配置 **>** 注册配置文件页面中，可以配置用户如何注册其设备。
Alexa for Business	在设置页面中，可以管理您的 Alexa for Business 配置文件。
设置	在设置页面中，可以管理系统设置，例如，客户端和服务器属性、证书和凭据提供程序。重要：这些设置包括 RBAC 权限。RBAC 权限向管理员授予完全访问权限，包括分配自己的权限的能力。请仅向打算提供控制 Endpoint Management 系统中的所有对象的功能的用户授予此访问权限。
支持	在故障排除和支持页面中，可以执行运行诊断和生成日志等故障排除活动。

面向管理员的设备限制

管理员可以通过设置设备限制、设置并向设备发送通知、管理设备上的应用程序等操作，访问控制台各处的设备功能。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

完全擦除设备	擦除设备上的所有数据和应用程序，包括内存卡（如果设备具有内存卡）。
清除限制	删除一项或多项设备限制。
选择性擦除设备	擦除设备上的所有公司数据和应用程序，保留个人数据和应用程序。
查看位置	查看设备的位置以及在设备上设置地理区域限制。包括：定位设备、跟踪设备。
锁定设备	远程锁定设备，使用户无法使用设备。
解锁设备	远程解锁设备，使用户可以使用设备。
锁定容器	远程锁定设备上的企业容器。
解锁容器	远程解锁设备上的企业容器。
重置容器密码	重置企业容器密码。
启用 ASM/绕过激活锁	启用激活锁时，在受监督的 iOS 设备上存储绕过码。要擦除该设备，请使用此代码自动清除激活锁。
获取常驻用户	列出在当前设备上具有活动帐户的用户。此操作将强制在设备与 Endpoint Management 控制台之间进行同步。
注销常驻用户	强制注销当前用户。
删除常驻用户	删除特定用户的当前会话。该用户可以重新登录。
使设备响铃	远程使 Windows 设备以最高音量响铃 5 分钟。
重新启动设备	从 Endpoint Management 控制台重新启动 Windows 设备。
部署到设备	向设备发送应用程序、通知、限制和其他资源。
编辑设备	更改设备上的设置。
通知设备	向设备发送通知。
添加/删除设备	在 Endpoint Management 中添加或删除设备。
设备导入	通过文件向 Endpoint Management 导入一组设备。
导出设备表	从“设备”页面收集设备信息，并将其导出到.csv 文件。
吊销设备	禁止设备连接到 Endpoint Management。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序锁定	拒绝访问设备上的所有应用程序。在 Android 上，此限制会阻止用户登录到 Endpoint Management。在 iOS 中，用户可以登录，但无法访问应用程序。
应用程序擦除	在 Android 上，此限制将删除用户的 Endpoint Management 帐户。在 iOS 上，此限制将删除用户访问 Endpoint Management 功能所需的加密密钥。
查看软件清单	查看设备上安装的软件。
请求使用 AirPlay 镜像	请求启动 AirPlay 流。
停止使用 AirPlay 镜像	停止 AirPlay 流。
启用丢失模式	在管理 **>** 设备页面上，可以将受监督的设备置于丢失模式，以阻止锁屏界面上的受监督设备。然后，您可以在设备丢失或被盗时找到设备。
禁用丢失模式	在管理 **>** 设备页面上，可以禁用设置为丢失模式的设备的丢失模式。
操作系统更新设备	可以将“操作系统更新”设备策略部署到设备。
关闭设备	从 Endpoint Management 控制台关闭 iOS 设备。
重新启动设备	从 Endpoint Management 控制台重新启动 iOS 设备。
续订设备注册证书	续订设备 CA 证书。

本地用户和组

管理员在 Endpoint Management 中的管理 **>** 用户页面上管理本地用户和本地用户组。

添加本地用户
删除本地用户
编辑本地用户
导入本地用户
导出本地用户
本地用户组
获取本地用户锁 ID

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

删除本地用户锁

注册

管理员可以添加和删除注册邀请、向用户发送通知以及将注册表导出到.csv 文件。

添加/删除注册	添加或删除向一个或一组用户发送的注册邀请。
通知用户	向一个或一组用户发送注册邀请。
导出注册邀请表	从“注册”页收集注册信息并将其导出到.csv 文件。

策略

添加/删除策略	添加或删除设备策略或应用程序策略。
编辑策略	更改设备策略或应用程序策略。
上载策略	上载设备策略或应用程序策略。
克隆策略	复制设备策略或应用程序策略。
禁用策略	禁用现有应用程序策略。
导出策略	从“设备策略”页面收集设备策略信息，并将其导出到.csv 文件。
分配策略	将设备策略分配给一个或多个交付组。

应用程序

管理员在 Endpoint Management 中的配置 **>** 应用程序页面上管理应用程序。

添加/删除应用商店或企业应用程序	添加或删除公共应用商店应用程序或企业应用程序（未启用 MDX）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

编辑应用商店或企业应用程序	更改公共应用商店应用程序或企业应用程序（未启用 MDX）。
添加/删除 MDX、Web 和 SaaS 应用程序	在 Endpoint Management 中添加或删除启用了 MDX 的应用程序、内部网络中的应用程序（Web 应用程序）或公共网络中的应用程序 (SaaS)。
添加 MDX、Web 和 SaaS 应用程序	更改启用了 MDX 的应用程序、内部网络中的应用程序（Web 应用程序）或从公共网络（SaaS）连接到 Endpoint Management 的应用程序。
添加/删除类别	添加或删除应用程序在应用商店中可以归属的类别。
将公共/企业应用程序分配给交付组	将公共应用商店应用程序或启用了 MDX 的应用程序分配给交付组以便部署。
将 MDX/WebLink/SaaS 应用程序分配给交付组	将启用了 MDX、不需要单点登录 (WebLink) 或来自公共网络 (SaaS) 的应用程序分配给交付组。
导出应用程序表	从“应用程序”页收集应用程序信息并将其导出到.csv 文件。

媒体

管理来自公共应用商店的媒体或批量购买许可证。

添加/删除应用商店或企业书籍
将公共/企业书籍分配给交付组
编辑应用商店或企业书籍

操作

添加/删除操作	添加或删除由触发器和关联响应定义的操作。触发器是事件、设备或用户属性或已安装的应用程序名称。
编辑操作	更改由触发器和关联响应定义的操作。触发器是事件、设备或用户属性或已安装的应用程序名称。
将操作分配给交付组	将操作分配给交付组以便部署到用户设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

导出操作	从“操作”页收集操作信息并将其导出到.csv 文件。

交付组

管理员在配置 **>** 交付组页面上管理交付组。

添加/删除交付组	创建或删除交付组，即添加指定用户和可选策略、应用程序和操作。
编辑交付组	更改现有交付组，即修改用户和可选策略、应用程序和操作。
部署交付组	使交付组可供使用。
导出交付组	从“交付组”页收集交付组信息并将其导出到.csv 文件。

注册配置文件

管理注册配置文件。

添加/删除注册配置文件
编辑注册配置文件
将注册配置文件分配给交付组

Alexa for Business

管理 Alexa for Business 配置文件。

添加/删除/编辑会议室
添加/删除/编辑会议室配置文件
添加/删除/编辑技能组

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

面向管理员的设置

管理员在设置页面上配置各种设置。

RBAC	RBAC 分配。重要：此权限向管理员授予完全访问权限，包括分配自己的权限的能力。请仅向打算提供控制 Endpoint Management 系统中的所有对象的功能的用户授予此访问权限。
LDAP	管理一个或多个 LDAP 兼容目录（例如 Active Directory），以导入组、用户帐户和相关属性。
注册	为用户和自助门户启用注册安全模式。
发布管理	查看当前安装的版本。包括：发布管理更新
Certificates（证书）	编辑 APNS 证书
通知模板	创建要在自动执行的操作、注册以及对用户的标准通知消息交付中使用的通知模板。
工作流	管理用于应用程序配置的用户帐户的创建、审批和删除。
凭据提供程序	添加一个或多个授权颁发设备证书的凭据提供程序。凭据提供程序控制证书格式以及续订或吊销证书的条件。
PKI 实体	管理公钥基础结构实体（通用、Microsoft Certificate Services 或任意 CA）。
测试 PKI 连接	使用设置 **> PKI** 实体页面上的测试连接按钮可确保服务器可访问。
客户端属性	管理用户设备上的各种属性，例如通行码类型、长度和过期日期。
客户端支持	设置用户联系支持服务的方式（电子邮件、电话或支持票证电子邮件）。
客户端外观方案	为应用商店创建自定义的应用商店名称和默认应用商店视图。添加显示在应用商店或 Secure Hub 中的自定义徽标。
运营商 SMS 网关	设置运营商 SMS 网关以配置 Endpoint Management 通过运营商 SMS 网关发送的通知。
通知服务器	设置用于向用户发送电子邮件的 SMTP 网关服务器。
ActiveSync Gateway	通过规则和属性，管理用户对用户和设备的访问权限。
Google Chrome	配置 Endpoint Management 以与您的 Google Workspace 帐号进行通信。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Apple 部署计划	将 Apple 部署计划帐户添加到 Endpoint Management。
Apple Configurator 设备注册	在 Endpoint Management 控制台中配置 Apple Configurator 设置。
iOS/批量购买设置	添加 Apple 批量购买帐户。
NetScaler Gateway	在 Endpoint Management 中配置 NetScaler Gateway（现已重命名为 Citrix Gateway）设置。
网络访问控制	设置确定设备不兼容的条件，以使其无法访问网络。
服务器属性	添加或修改服务器属性。需要在所有节点上重新启动 Endpoint Management。
Virtual Apps and Desktops	允许用户通过 Citrix Workspace 添加 Citrix Virtual Apps and Desktops。
Citrix Files	将 Endpoint Management 与 Enterprise 帐户结合使用时：配置连接到 Content Collaboration 帐户和管理员服务帐户以管理用户帐户的设置。需要使用现有 Citrix Files 域和管理员凭据。在 Endpoint Management 中使用存储区域连接器时：将 Endpoint Management 配置为指向在存储区域连接器中定义的网络共享和 SharePoint 位置。
Android Enterprise	配置 Android Enterprise 服务器设置
身份提供程序 (IdP)	配置身份提供程序。
Endpoint Management 工具	“访问 Endpoint Management 工具” 页面。
Windows 批量注册	配置 Windows 批量注册设置。

支持

管理员可以执行各种支持任务。

NetScaler Gateway 连接检查	通过 IP 地址执行 NetScaler Gateway 的各种连接检查。需要用户名和密码。
Endpoint Management 连接性检查	为选定的 Endpoint Management 功能（例如数据库、DNS、Google Plan）执行连接检查。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix 产品文档	访问公共 Citrix Endpoint Management 文档站点。
Citrix 知识中心	访问 Citrix 支持站点以搜索知识库文章。
日志	查看和下载文件。
宏	在配置文件、策略、通知或注册模板的文本字段中填充用户或设备属性数据。配置一个策略并将其部署到较大的用户群，并为每个目标用户显示特定于用户的值。
PKI 配置	导入和导出 PKI 配置信息。
APNS 签名实用程序	提交 Apple 推送网络签名 (Apple Push Network signing, APNs) 证书请求，或上载适用于 iOS 的 Secure Mail APNs 证书。
Citrix Insight Services	将日志上载到 Citrix Insight Services (CIS)，以帮助解决各种问题。
发送到适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的设备状态	向 Endpoint Management 查询发送到适用于 Exchange ActiveSync 的连接器的设备状态。查询基于设备 ActiveSync ID。

限制组访问

管理员用户可以应用所有用户组的权限。

用于设备预配的控制台功能

设备预配用户具有 Endpoint Management 控制台的以下有限访问权限。默认情况下，以下各功能均处于启用状态。

设备限制

编辑设备	更改设备上的设置。
添加/删除设备	在 Endpoint Management 中添加或删除设备。

设备预配设置

设备预配用户可以访问设置页面，但无权配置功能。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用户角色

具有用户角色的用户具有 Endpoint Management 的以下有限访问权限。

授权用户访问权限

自助服务门户	仅向用户提供访问 Endpoint Management 中的自助门户的权限。

面向用户的控制台功能

用户具有 Endpoint Management 控制台的以下有限访问权限。

面向用户的设备限制访问

完全擦除设备	擦除设备上的所有数据和应用程序，包括内存卡（如果设备具有内存卡）。
选择性擦除设备	擦除设备上的所有公司数据和应用程序，保留个人数据和应用程序。
查看位置	查看设备的位置以及在设备上设置地理区域限制。包括：定位设备、查看设备的位置、跟踪设备、跟踪设备位置随时间的变化。
锁定设备	远程锁定设备，使其无法使用。
解锁设备	远程解锁设备，使其可以使用。
锁定容器	远程锁定设备上的企业容器。
解锁容器	远程解锁设备上的企业容器。
重置容器密码	重置企业容器密码。
启用 ASM/绕过激活锁	启用激活锁时，在受监督的 iOS 设备上存储绕过码。要擦除该设备，请使用此代码自动清除激活锁。
获取常驻用户	列出在当前设备上具有活动帐户的用户。此操作将强制在设备与 Endpoint Management 控制台之间进行同步。
注销常驻用户	强制注销当前用户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

删除常驻用户	删除特定用户的当前会话。该用户可以重新登录。
使设备响铃	远程使 Windows 设备以最高音量响铃 5 分钟。
重新启动设备	重新启动 Windows 设备。
应用程序锁定	拒绝访问设备上的所有应用程序。在 Android 上，用户无法登录 Endpoint Management。在 iOS 中，用户可以登录，但无法访问应用程序。
应用程序擦除	在 Android 上，此限制将删除用户的 Endpoint Management 帐户。在 iOS 上，此限制将删除用户访问 Endpoint Management 功能所需的加密密钥。
查看软件清单	查看设备上安装的软件。

面向用户的注册限制

添加/删除注册	添加或删除向一个或一组用户发送的注册邀请。
通知用户	向一个或一组用户发送注册邀请。

限制所有角色的组访问权限

对于默认角色，此权限在默认情况下设置，并且可应用于所有用户组。您无法编辑此角色。

许可证

October 18, 2022

有关 Citrix 许可证使用情况的信息，请参阅：

- 监视云服务的许可证和活动使用情况
- 监视 Endpoint Management 的许可证和活动使用情况

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备管理

July 7, 2023

Citrix Endpoint Management 可以在单个管理控制台中预配和管理各种设备类型、保护其安全以及将其列入清单。

- 使用一组通用的设备策略可管理受支持的设备。要按平台快速查看可用的设备策略，请执行以下操作：
  1. 转到 Endpoint Management 控制台并导航到配置 **>** 设备策略。
  2. 单击添加，然后选择要查看的平台。

     有关详细信息，请参阅过滤已添加的设备策略列表。
- 保护企业信息，以严格保护身份信息、公司拥有的设备和 BYO 设备、应用程序、数据和网络的安全。指定用于对设备进行身份验证的用户身份。配置如何在设备上分开保存企业数据和个人数据。
- 向最终用户交付任何应用程序，无论设备或操作系统如何。在应用程序级别保护您的信息，并提供企业级移动应用程序管理。
- 使用预配和配置控制来设置设备。这些控制包括设备注册、策略应用程序和访问权限。
- 使用安全和合规性控制创建可自定义的安全基线和可操作的触发。例如，在违反界定的合规性标准时锁定、擦除设备或在设备上发出通知。
- 使用操作系统更新控制来阻止或强制执行操作系统更新。此功能对于抵御有针对性的操作系统漏洞以防止数据丢失至关重要。

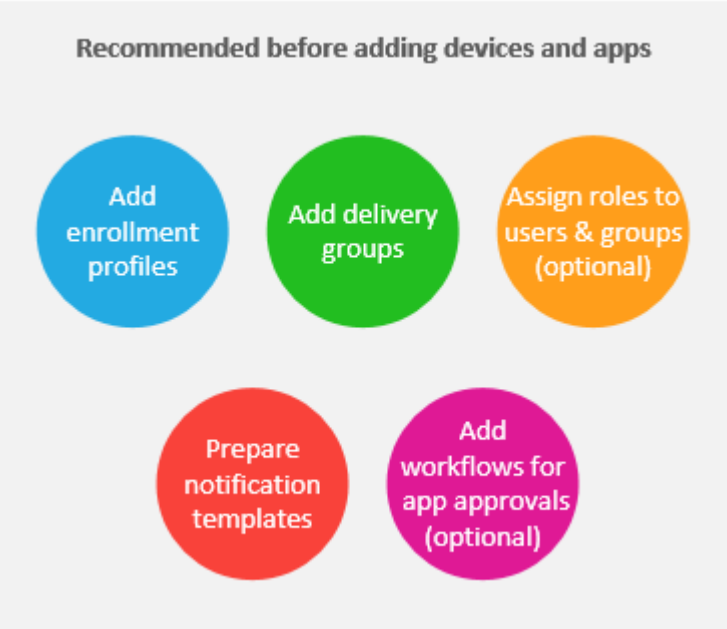
要访问有关每个受支持平台的文章，请展开内容列表中的“设备管理”部分。这些文章提供了特定于每个设备平台的详细信息。本文的其余部分介绍如何执行一般设备管理任务。

设备管理工作流程

本节中的工作流程图为设备管理任务提供了建议顺序。

1. 建议添加设备和应用程序前必须满足的必备条件：提前执行以下设置可以无中断地配置设备和应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



请参阅：

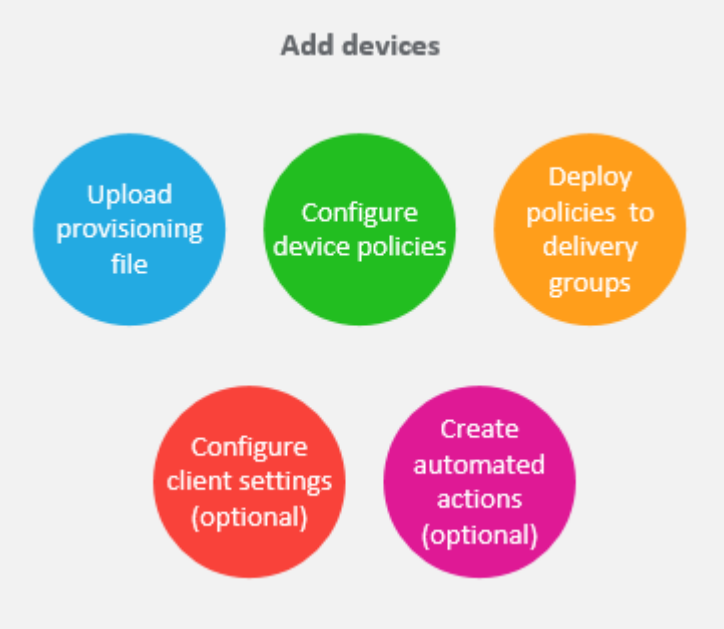
部署资源

使用 RBAC 配置角色

创建和更新通知模板

创建和管理工作流

2. 添加设备：



请参阅：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

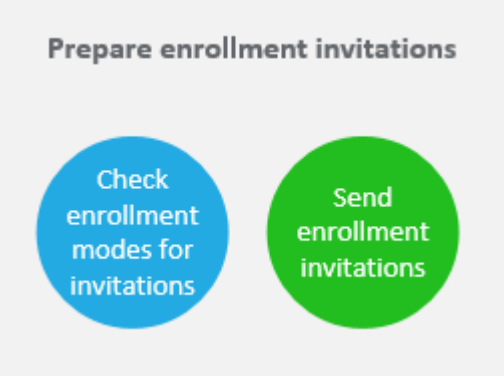
准备注册设备并交付资源

设备策略

部署到交付组

自动化操作

3. 准备注册邀请：可以向使用 iOS、iPadOS、macOS、Android Enterprise 或旧版 Android 设备的用户发送注册邀请。如果您计划使用注册邀请，请执行以下操作。



请参阅：

配置注册安全模式

向设备发送通知

4. 添加应用程序：



请参阅：

MAM SDK

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

添加应用程序

关于应用程序类别

应用工作流

部署到交付组

5. 执行持续的设备和应用程序管理：除了使用 Endpoint Management 控制板外，我们还鼓励您查看每个版本的新增功能内容。“新增功能”提供有关任何所需操作的信息，例如配置新设备策略。



请参阅：

监视和支持

报告

安全操作

新增功能

设备策略

注册邀请

为了安全地远程管理用户设备，请在 Endpoint Management 中注册用户设备。将 Endpoint Management 客户端软件安装在用户设备上并验证用户的身份。然后，安装 Endpoint Management 和用户配置文件。有关受支持设备平台的注册详细信息，请参阅本部分下的设备文章。

在 Endpoint Management 控制台中：

- 可以向使用 iOS、iPadOS、macOS、Android Enterprise 或旧版 Android 设备的用户发送注册邀请。注册邀请不适用于 Windows 设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 可以向使用 iOS、iPadOS、Android Enterprise 或旧版 Android 设备的用户发送邀请 URL。邀请网址不适用于 Windows 设备。

注册邀请的发送方式如下所示：

- 如果 Active Directory 用户在 Active Directory 中有电子邮件地址，他们将收到邀请。本地用户通过用户属性中指定的电子邮件接收邀请。

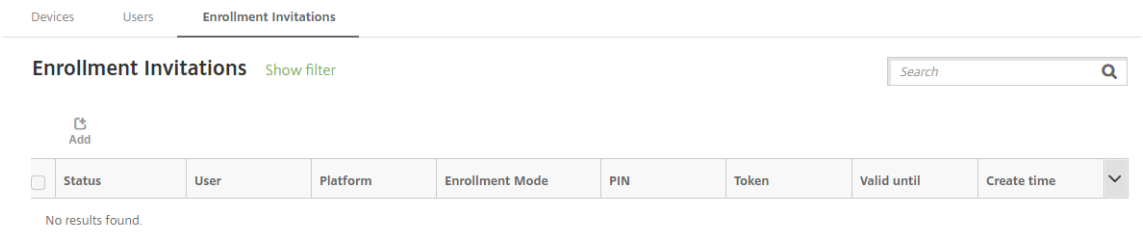
用户注册后，其设备在管理 **>** 设备上将显示为托管设备。邀请 URL 的状态显示为已兑换。

必备条件

- 已配置 LDAP
- 如果使用本地组和本地用户：
  - 一个或多个本地组。
  - 分配给本地组的本地用户。
  - 交付组与本地组相关联。
- 如果使用 Active Directory：
  - 交付组与 Active Directory 组相关联。

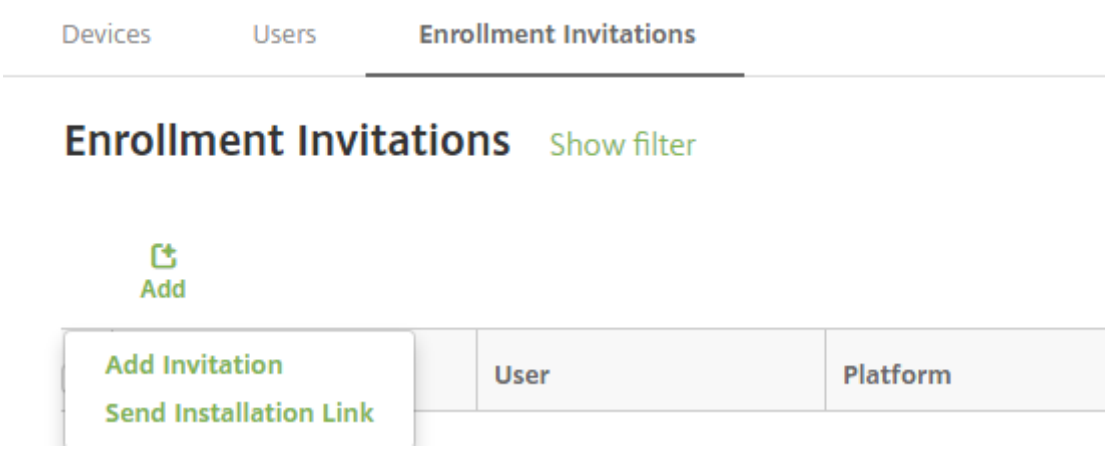
创建注册邀请

1. 在 Endpoint Management 控制台中，单击管理 **>** 注册邀请。此时将显示注册邀请页面。



2. 单击添加。此时将显示一个注册选项菜单。

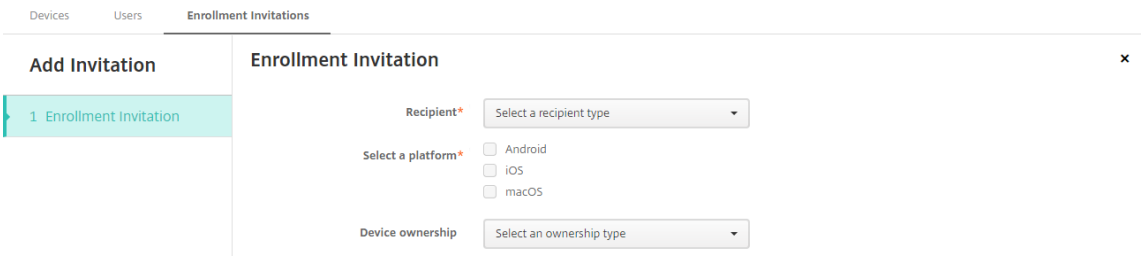
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 要向用户或组发送注册邀请，请单击添加邀请。
- 要通过 SMTP 向收件人列表发送注册安装链接，请单击“发送安装链接”。

如何发送注册邀请和安装链接将在这些步骤之后进行介绍。

3. 单击添加邀请。将显示注册邀请屏幕。



4. 配置以下设置：

   - 收件人：选择组或用户。
   - 选择平台：如果收件人为组，则默认选择所有平台。可以更改所选平台。如果收件人为用户，则不选择任何平台。选择平台。

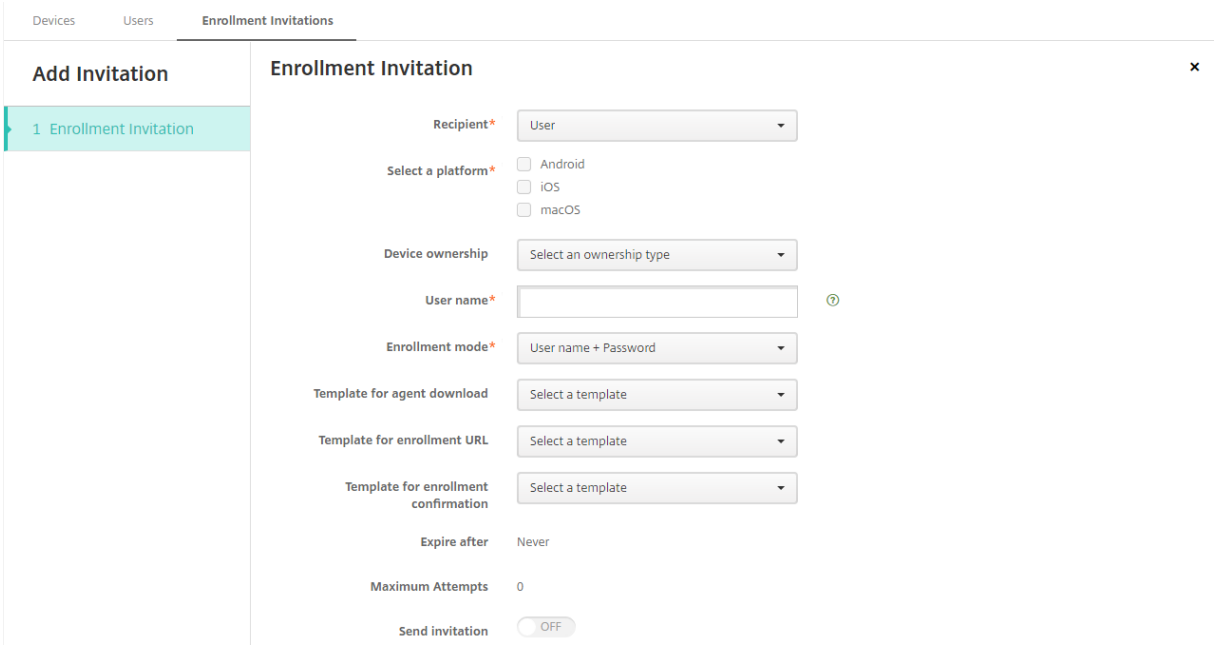
     要为 Android Enterprise 设备创建注册邀请，请选择 **Android**。

   - 设备所有权：选择公司或员工。

此时将显示用户或组的设置，如以下各节中所述。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

向用户发送注册邀请



1. 配置以下用户设置：

   - 用户名：键入用户名。用户必须作为本地或 Active Directory 用户身份存在于 Endpoint Management 中。如果用户是本地用户，请设置用户的电子邮件属性，以便能够向该用户发送通知。如果用户在 Active Directory 中，前提是配置了 LDAP。
   - 电话号码：如果您选择多个平台或仅选择 macOS，则不会显示此设置。（可选）键入用户的电话号码。
   - 运营商：如果您选择多个平台或仅选择 macOS，则不会显示此设置。选择要与用户的电话号码关联的运营商。
   - 注册模式：为用户选择注册安全模式。默认值为用户名 **+** 密码。下面某些选项不对所有平台可用：
     - 用户名 **+** 密码
     - 邀请 **URL**
     - 邀请 **URL + PIN**
     - 邀请 **URL +** 密码
     - 双重
     - 用户名 **+ PIN**

   我们弃用了对高安全性注册模式的支持。要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。对于使用用户名 **+** 密码、双重或用户名 **+ PIN** 注册的设备，用户必须下载 Secure Hub 并手动输入其凭据。

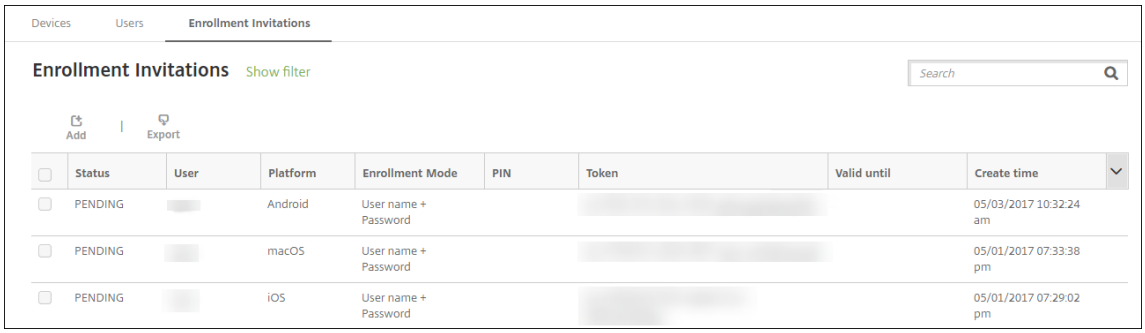
   有关详细信息，请参阅注册安全模式（按平台）。用于注册的 PIN 又称为一次性 PIN。此类 PIN 仅在用户注册时有效。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 当您选择包含 PIN 的任何注册安全模式时，将显示 注册 **PIN** 的模板字段。单击注册 **PIN**。

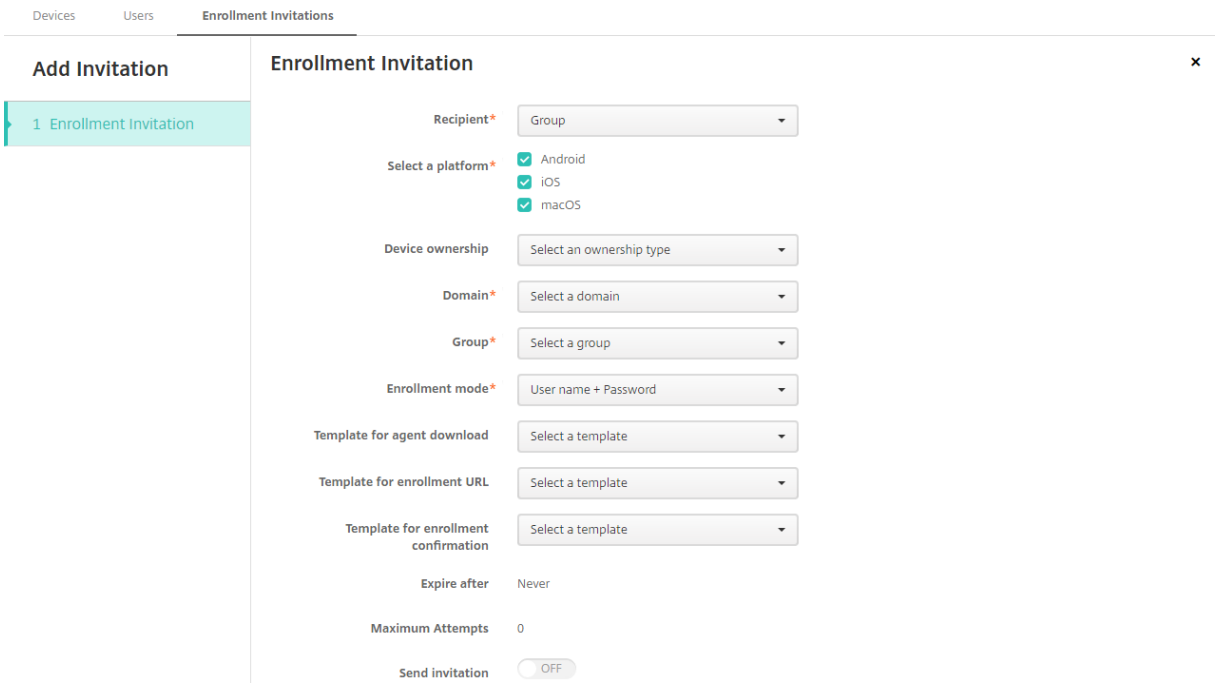
- 代理下载模板：选择名为下载链接的下载链接模板。该模板适用于受支持的所有平台。
- 注册 **URL** 模板：选择注册邀请。
- 注册确认模板：选择注册确认。
- 此时间后过期：在配置注册安全模式时设置此字段，并指示注册何时到期。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- 最大尝试次数：此字段在配置注册安全模式时设置，并指示注册过程发生的最大次数。
- 发送邀请：选择开将立即发送邀请。选择关将向注册邀请页面上的表格中添加邀请，但不发送。

2. 如果已启用发送邀请，请单击保存并发送。否则，请单击保存。邀请将显示在注册邀请页面上的表格中。



向组发送注册邀请

下图中显示了用于配置向组发送的注册邀请的设置。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 配置以下设置：

   - 域：选择要接收邀请的组的域。
   - 组：选择要接收邀请的组。Endpoint Management 从 Active Directory 获取用户列表。该列表包括姓名中包含特殊字符的用户。
   - 注册模式：选择希望组中的用户采用的注册方式。默认值为用户名 + 密码。下面某些选项不对所有平台可用：
     - 用户名 + 密码
     - 邀请 **URL**
     - 邀请 **URL + PIN**
     - 邀请 **URL** + 密码
     - 双重
     - 用户名 + **PIN**

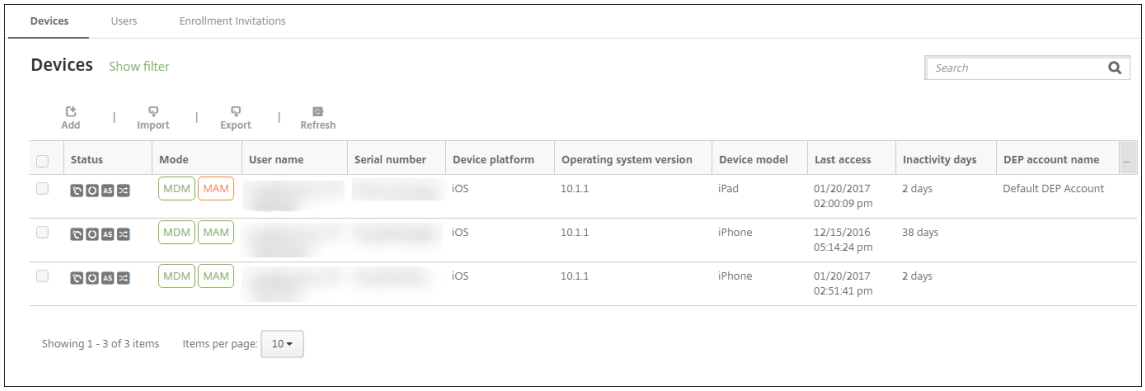
   我们弃用了对高安全性注册模式的支持。要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL** + 密码注册安全模式。对于使用用户名 + 密码、双重或用户名 + **PIN** 注册的设备，用户必须下载 Secure Hub 并手动输入其凭据。

   仅显示对每个选定的平台有效的注册安全模式。有关详细信息，请参阅注册安全模式（按平台）。

   > 注意：
   >
   > 当您选择包含 PIN 的任何注册安全模式时，将显示 注册 **PIN** 的模板字段。单击注册 **PIN**。

   - 代理下载模板：选择名为下载链接的下载链接模板。该模板适用于受支持的所有平台。
   - 注册 **URL** 模板：选择注册邀请。
   - 注册确认模板：选择注册确认。
   - 此时间后过期：在配置注册安全模式时设置此字段，并指示注册何时到期。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
   - 最大尝试次数：此字段在配置注册安全模式时设置，并指示注册过程发生的最大次数。
   - 发送邀请：选择开将立即发送邀请。选择关将向注册邀请页面上的表格中添加邀请，但不发送。

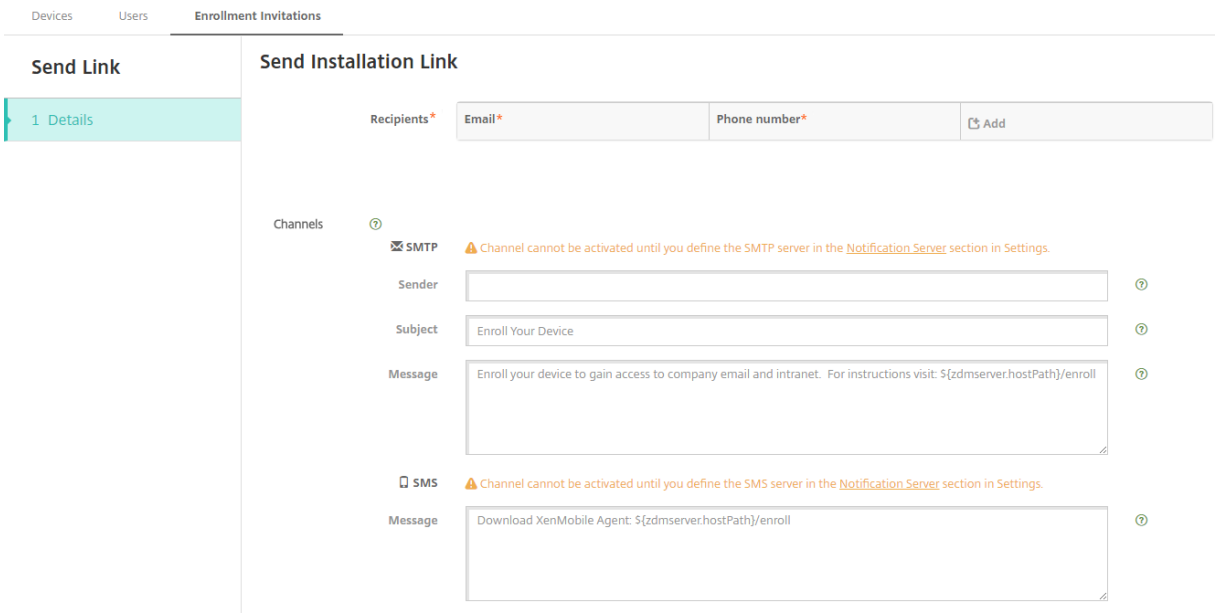
2. 如果已启用发送邀请，请单击保存并发送。否则，请单击保存。邀请将显示在注册邀请页面上的表格中。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

发送安装链接

在发送注册安装链接之前，必须从“设置”页面在通知服务器上配置通道 (SMTP)。有关详细信息，请参阅通知



1. 配置这些设置，然后单击保存。

   - 收件人：对于要添加的每个收件人，单击添加，然后执行以下操作：
     - 电子邮件：键入收件人的电子邮件地址。此字段为必填字段。
     - 电话号码：键入收件人的电话号码。此字段为必填字段。

     > 注意：
     >
     > 要删除收件人，请将鼠标悬停在包含列表的行上，然后单击右侧的垃圾图标。此时将显示确认对话框。单击删除以删除列表，或单击取消以保留列表。
     >
     > 要编辑收件人，请将鼠标悬停在列表所在行上。然后，单击右侧的笔图标。更新列表，然后单击保存以保存更改后的列表，或单击取消以保留列表不变。

   - 通道：选择用于发送注册安装链接的通道。您可以通过 **SMTP** 发送通知。在通知服务器的设置页面上配置服务器设置后，才能激活这些通道。有关详细信息，请参阅通知。
   - **SMTP**：配置以下可选设置。如果不在这些字段中键入任何内容，将使用为所选平台配置的通知模板中指定的默认值：
     - 发件人：键入可选发件人。
     - 主题：键入消息的可选主题。例如，“注册您的设备”。
     - 消息：键入要发送给收件人的可选消息。例如，“注册您的设备以获取组织应用程序和电子邮件的访问权限。”

2. 单击发送。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 如果您的环境使用 sAMAccountName：在用户收到邀请并单击链接后，必须编辑用户名才能完成身份验证。用户名以 sAMAccountName@domainname.com 的形式显示。用户必须删除 @domainname.com 部分。

按平台分类注册安全模式

下表显示了可用于注册用户设备的安全模式。在该表中，是表示哪些设备平台支持使用不同注册配置文件的特定注册和管理模式。

MDM 注册安全模式	Citrix Gateway 上的 MAM 注册安全模式	管理模式	支持不同的注册配置文件	Android（旧版）	Android Enterprise	iOS（用户注册模式）	iOS	macOS	Windows
Azure AD 和 Okta 可通过 Citrix Cloud 作为身份提供程序	客户端证书	MDM+MA 或 MDM	是	是	是	是	是	否	否
用户名 + 密码	LDAP、LDAP + 客户端证书和仅客户端证书	MDM+MAM MDM 或 MAM（仅 MAM 模式在 Citrix Gateway 上不支持客户端证书）	是	是	是	是	是	是	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

MDM 注册安全模式	Citrix Gateway 上的 MAM 注册安全模式	管理模式	支持不同的注册配置文件	Android（旧版）	Android Enterprise	iOS（用户注册模式）	iOS	macOS	Windows
邀请 URL	客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	否	否
邀请 URL + PIN	客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	否	否
邀请 URL + 密码	LDAP、LDAP + 客户端证书和仅客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	否	否
双重身份验证（用户名 + 密码 + PIN）	LDAP、LDAP + 客户端证书和仅客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	是	否
用户名 + PIN	客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	是	否

下面介绍了注册安全模式在 iOS、Android 和 Android Enterprise 设备上的行为方式：

- 用户名 **+** 密码（默认设置）
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Secure Hub 将打开。然后，用户键入用户名和密码以将设备注册到 Endpoint Management 中。
- 邀请 **URL**
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Secure Hub 将打开。此时将显示 Endpoint Management 服务器名称和是，注册按钮。用户轻按是，注册以在 Endpoint Management 中注册设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 邀请 **URL + PIN**
  - 向用户发送以下电子邮件：
    - 包含注册 URL 的电子邮件，该邮件允许用户通过 Secure Hub 在 Endpoint Management 中注册设备。
    - 包含一次性 PIN（用户在注册设备时必须键入该 PIN）以及用户的 Active Directory（或本地）密码的电子邮件。
  - 在此模式下，用户只能通过使用通知中的注册 URL 进行注册。如果用户丢失了通知邀请，用户将无法注册。但是，您可以发送其他邀请。
- 邀请 **URL +** 密码
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Secure Hub 将打开。此时将显示 Endpoint Management 服务器名称，以及允许用户键入密码的字段。
- 双重
  - 向用户发送包含注册 URL 和一次性 PIN 码的单个通知。当用户单击 URL 时，Secure Hub 将打开。将显示 Endpoint Management 服务器名称，以及允许用户键入密码和 PIN 的两个字段。
- 用户名 **+ PIN**
  - 向用户发送以下电子邮件：
    - 包含注册 URL 的电子邮件，该邮件允许用户下载并安装 Secure Hub。Secure Hub 打开后，系统将提示用户键入用户名和密码，以便在 Endpoint Management 中注册设备。
    - 包含一次性 PIN（用户在注册设备时必须键入该 PIN）以及用户的 Active Directory（或本地）密码的电子邮件。
  - 如果用户丢失了通知邀请，用户将无法注册。但是，您可以发送其他邀请。

下面介绍了注册安全模式在 macOS 设备上的行为方式：

- 用户名 **+** 密码
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Safari 浏览器将打开。此时将显示一个登录页面，提示用户键入用户名和密码，以便在 Endpoint Management 中注册设备。
- 双重
  - 向用户发送包含注册 URL 和一次性 PIN 码的单个通知。当用户单击 URL 时，Safari 浏览器将打开。将出现一个登录页面，其中显示两个字段，允许用户键入密码和 PIN。
- 用户名 **+ PIN**
  - 向用户发送以下电子邮件：
    - 包含注册 URL 的电子邮件。当用户单击 URL 时，Safari 浏览器将打开。此时将显示一个登录页面，提示用户键入用户名和密码，以便在 Endpoint Management 中注册设备。
    - 包含一次性 PIN（用户在注册设备时必须键入该 PIN）以及用户的 Active Directory（或本地）密码的电子邮件。
  - 如果用户丢失了通知邀请，用户将无法注册。但是，您可以发送其他邀请。

您无法向 Windows 设备发送注册邀请。Windows 用户直接通过其设备注册。有关注册 Windows 设备的信息，请参阅 Windows 设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

安全操作

您可以从“管理”>“设备”页面执行设备和应用程序安全操作。设备操作包括吊销、锁定、解锁及擦除。应用程序安全操作包括应用程序锁定和应用程序擦除。

- 激活锁绕过：设备激活之前从受监督的 iOS 设备中删除激活锁。此命令不需要用户的个人 Apple ID 或密码。
- 应用程序锁定：拒绝访问设备上的所有应用程序。在 Android 上，应用程序锁定后，用户将无法登录 Endpoint Management。在 iOS 中，用户可以登录，但无法访问任何应用程序。
- 应用程序擦除：从 Secure Hub 中删除用户帐户并取消注册设备。在您使用 应用程序取消擦除操作之前，用户无法重新注册。
- **ASM** 部署计划激活锁：为在 Apple 校园教务管理中注册的 iOS 设备创建激活锁绕过码。
- 证书续订：对于支持的 iOS、macOS 和 Android 设备，证书续订安全操作会启动证书续订。下次设备连接回 Endpoint Management 时，Endpoint Management 服务器会根据新证书颁发机构颁发新的设备证书。
- 清除限制：在受监督的 iOS 设备上，此命令允许 Endpoint Management 清除用户配置的限制密码和限制设置。
- 启用/禁用丢失模式：将受监督的 iOS 设备置于丢失模式，并向设备发送消息、电话号码和脚注以供显示。第二次发送此命令将使设备脱离丢失模式。
- 启用跟踪：在 Android 或 iOS 设备上，此命令允许 Endpoint Management 以您定义的频率轮询特定设备的位置。要在地图上查看设备坐标和位置，请转到管理 > 设备，选择一个设备，然后单击编辑。设备信息位于安全下的常规选项卡上。使用启用跟踪可持续跟踪设备。Secure Hub 会在设备运行时定期报告位置。
- 完全擦除：立即从设备中（包括从任何内存卡中）擦除所有数据和应用程序。擦除的设备保留在管理 > 设备页面上的设备列表中，用于审核。可以从设备列表中删除擦除的设备。
  - 对于 Android 设备，此请求还可以包括用于擦除内存卡的选项。
  - 对于带有工作配置文件的完全托管的 Android Enterprise 设备（COPE 设备），您可以在选择性擦除删除工作配置文件后进行完全擦除。
  - 对于 iOS、macOS 和 tvOS 设备，擦除操作会立即进行，即使设备处于锁定状态亦如此。

    对于 iOS 11 和 iPadOS 12 设备（最低版本）：确认完全擦除时，可以选择在设备上保留手机网络流量套餐。

    对于 iOS 11.3 设备（最低版本）：确认完全擦除后，将阻止 iOS 设备进行近距离设置。设置新的 iOS 设备时，用户通常可以使用已配置的 iOS 设备来设置自己的设备。您可以阻止在由 Endpoint Management 管理并已擦除的设备上进行邻近感应设置。
  - 如果设备用户在删除内存卡内容之前关闭了设备，用户可能仍然对设备数据具有访问权限。
  - 可以在将擦除请求发送到设备之前取消该请求。
- 定位：在管理 > 设备页面上的设备详细信息 > 常规下定位设备并报告设备位置（包括地图）。定位是一次性操作。使用“定位”显示执行操作时的当前设备位置。要在一段时间内持续跟踪设备，请使用启用跟踪。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 将此操作应用到 Android（Android Enterprise 除外）设备或 Android Enterprise（企业拥有或 BYOD）设备时，请注意以下行为：
    * 定位要求用户在注册期间授予位置权限。用户可以选择不授予定位权限。如果用户在注册期间没有授予权限，则 Endpoint Management 会在发送 定位命令时再次请求位置权限。
  - 将此功能应用到 iOS 或 Android Enterprise 设备时，请注意以下限制：
    * 对于 Android Enterprise 设备，除非位置设备策略已将设备的位置模式设置为高精度或省电，否则此请求将失败。
    * 对于 iOS 设备，只有当设备处于 MDM 丢失模式时，命令才会成功。

- 锁定：远程锁定设备。如果设备被盗且必须锁定，则锁定很有用。Endpoint Management 随之生成一个 PIN 代码并在设备中进行设置。要访问设备，用户需要键入该 PIN 代码。使用取消锁定可从 Endpoint Management 控制台中删除锁定。
- 锁定并重置密码：远程锁定设备并重置密码。
  - 不支持以下设备：
    * 在工作配置文件模式下在 Android Enterprise 中注册的设备，以及
    * 运行 Android 7.0 之前的 Android 版本的设备
  - 在工作配置文件模式下于 Android Enterprise 中注册且运行 Android 7.0 或更高版本的设备上：
    * 密码锁定工作资料。设备不会被锁定。
    * 如果未发送通行码，或者发送的通行码不符合要求，并且工作配置文件没有通行码：设备将被锁定。
    * 如果未发送通行码，或者发送的通行码不符合要求，但工作配置文件有通行码：工作配置文件将被锁定，但设备不锁定。
- 通知 **(**响铃**)**：在 Android 设备上播放声音。
- 重新启动：重新启动 Windows 10 和 Windows 11 设备。对于 Windows Tablet 和 PC，将显示一条有关等待重新启动的消息。重新启动将在五分钟后发生。
- 请求使用**/**停止使用 **AirPlay** 镜像：在受监督的 iOS 设备上启动和停止 AirPlay 镜像。
- 重新启动**/**关闭：立即重新启动或关闭受监督的设备。tvOS 支持重新启动，但不支持关闭。
- 吊销：禁止设备连接到 Endpoint Management。
- 吊销**/**授权：执行与 “选择性擦除” 相同的操作。吊销后，可以重新向设备授权以进行重新注册。
- 响铃：如果设备处于丢失模式，响铃将在受监督的 iOS 设备上播放声音。声音将持续播放，直至您将设备从丢失模式中删除或者用户禁用声音。
- 轮换个人恢复密钥：如果您启用了 FileVault 设备策略，则此操作会生成一个新的个人恢复密钥并将旧密钥替换为这个新密钥。可以在请求尚未处理的情况下取消此请求。为此，请单击 **Cancel Rotate personal recovery key**（取消轮换个人恢复密钥）。
- 选择性擦除：擦除设备上的所有公司数据和应用程序，保留个人数据和应用程序。执行选择性擦除操作后，使用授权操作重新授权设备，以便用户可以重新注册设备。擦除的设备保留在管理 **>** 设备页面上的设备列表中，用于审核。可以从设备列表中删除擦除的设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 选择性擦除 Android 设备不会断开设备与 Device Manager 及企业网络的连接。要阻止设备访问 Device Manager，还必须吊销设备证书。
  - 选择性擦除 Android 设备也会吊销设备。只有在重新授权设备或从控制台中删除设备后，才能重新注册设备。
  - 对于使用工作配置文件（COPE 设备）的 Android Enterprise 完全托管设备，您可以在选择性擦除操作删除工作配置文件后执行完全擦除。或者，也可以使用相同的用户名重新注册设备。重新注册设备会重新创建工作配置文件。
  - 对于 iOS 和 macOS 设备，此命令将删除通过 MDM 安装的任何配置文件。
  - 在 Windows 设备上执行的选择性擦除还将删除当时已登录的任何用户的配置文件文件夹的内容。选择性擦除不会删除您通过配置向用户提供的任何 Web 剪辑。要删除 Web 剪辑，用户需要手动取消注册其设备。不能重新注册选择性擦除的设备。

- 解锁：清除设备被锁定时向其发送的通行码。此命令不解锁设备。

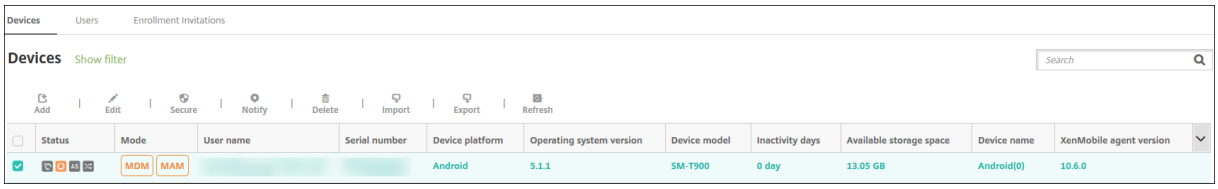
在管理 **>** 设备中，设备详细信息页面还将列出设备安全属性。这些属性包括“强 ID”、“锁定设备”、“激活锁绕过”以及平台类型的其他信息。完全擦除设备字段包括用户的 PIN 代码。擦除设备后，用户必须输入该代码。如果用户忘记了该代码，您可以在此处查找。

您可以自动执行某些操作。有关详细信息，请参阅自动化操作。

从 **Endpoint Management** 控制台中删除设备

> 重要：
>
> 当您从 Endpoint Management 控制台中移除设备时，托管应用程序和数据将保留在设备上。要从设备中删除托管应用程序和数据，请参阅本文后面的“删除设备”部分。

要从 Endpoint Management 控制台中删除某个设备，请转至管理 **>** 设备，选择一个托管设备，然后单击删除。



选择性擦除设备

1. 转至管理 **>** 设备，选择一个托管设备，然后单击安全。
2. 在安全操作中，单击选择性擦除。
3. 仅限 Android 设备：要断开设备与企业网络的连接，请在擦除设备后，在安全操作中，单击吊销。

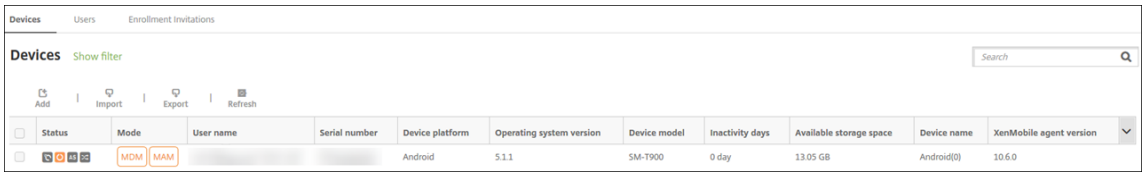
   要在擦除之前撤回选择性擦除请求，请在安全操作中，单击取消选择性擦除。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

删除设备

此过程将从该设备中删除托管应用程序和数据，并从 Endpoint Management 控制台的“设备”列表中删除该设备。可以使用 Endpoint Management 公共 REST API 批量删除设备。

1. 转至管理 **>** 设备，选择一个托管设备，然后单击安全。
2. 单击选择性擦除。系统提示时，单击执行选择性擦除。
3. 要验证擦除命令是否成功，请刷新管理 **>** 设备。在模式列中，琥珀色的 MDM 和 MAM 指示擦除命令成功。



4. 在管理 **>** 设备中，选择该设备，然后单击删除。系统提示时，再次单击删除。

锁定、解锁、擦除或取消擦除应用程序

1. 转至管理 **>** 设备，选择一个托管设备，然后单击安全。
2. 在安全操作中，单击应用程序操作。

   还可以使用安全操作对话框检查已禁用或从 Active Directory 中删除其帐户的用户的设备状态。如果存在“应用程序解锁”操作或“应用程序取消擦除”操作，则表明应用程序已被锁定或擦除。

应用程序擦除和取消擦除

1. 转至管理 **>** 设备。选择一台设备。
2. 应用程序擦除
   - 单击安全 **>** 应用程序擦除。出现一个包含以下消息的对话框：是否确实要对此设备执行应用程序擦除**?** 单击应用程序擦除。
3. 应用程序取消擦除
   - 单击安全 **>** 应用程序取消擦除。出现一个包含以下消息的对话框：是否确实要对此设备执行应用程序取消擦除**?** 单击设备应用程序取消擦除。
4. 以相同模式以同一用户身份重新注册设备。
5. 从我的应用程序页面启动 MDX 应用程序。
6. 启动 Secure Hub。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

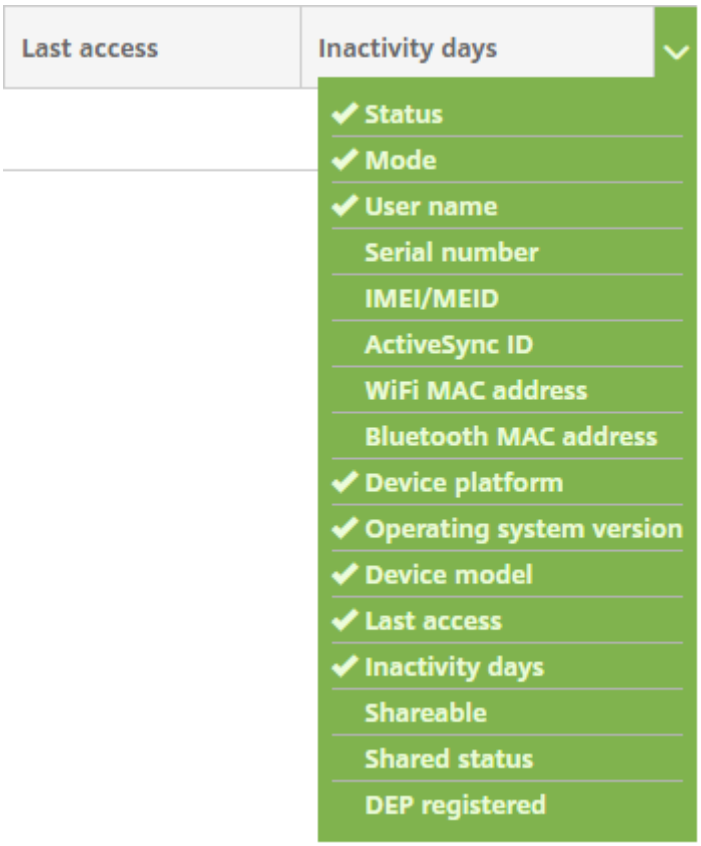
获取有关设备的信息

Endpoint Management 数据库用于存储移动设备的列表。要将设备填充到 Endpoint Management 控制台中，可以手动添加设备或从文件导入设备列表。有关设备预配文件格式的详细信息，请参阅本文中稍后介绍的设备预配文件格式。

Endpoint Management 控制台中的管理 **>** 设备页面将列出每个设备以及以下信息：

- 状态：图标指示设备是否已越狱、是否托管、ActiveSync Gateway 是否可用以及部署状态。
- 模式：指示设备模式，如 MDM 或 MDM+MAM。
- 与设备有关的其他信息，例如用户名、设备平台、上次访问时间和不活动天数。这些标题是显示的默认标题。

要自定义设备表，请单击最后一个标题上的向下箭头。然后选择要在表格中查看的其他标题，或者清除要将其删除的所有标题。



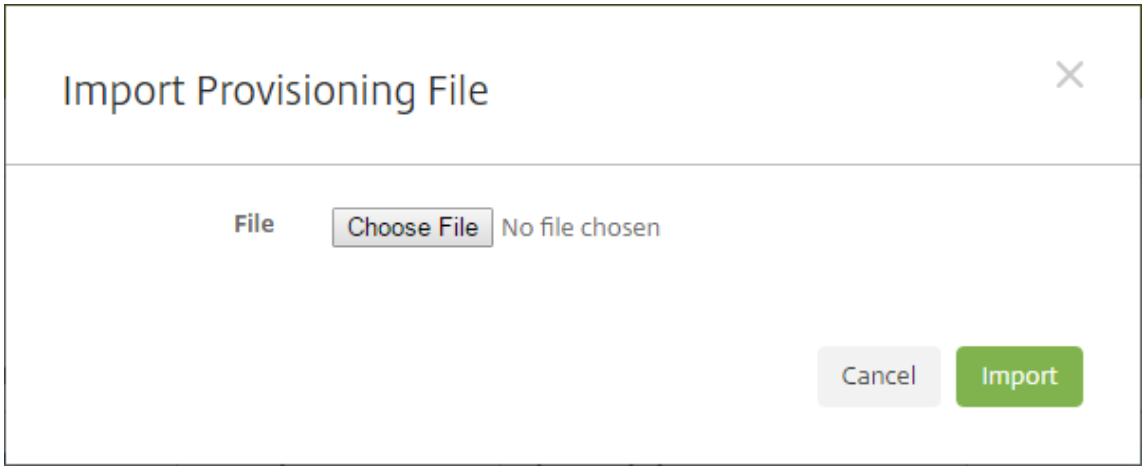
您可以手动添加设备、从设备配置文件导入设备、编辑设备详细信息、自定义 Active Directory 用户属性、执行安全操作以及向设备发送通知。还可以将所有设备表数据导出到.csv 文件，以创建自定义报告。服务器将导出所有设备属性。如果应用过滤器，Endpoint Management 会在创建.csv 文件时使用过滤器。

从预配文件导入设备

您可以导入移动运营商或设备制造商支持的文件，或创建自己的设备预配文件。有关详细信息，请参阅本文中后面的设备预配文件格式。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

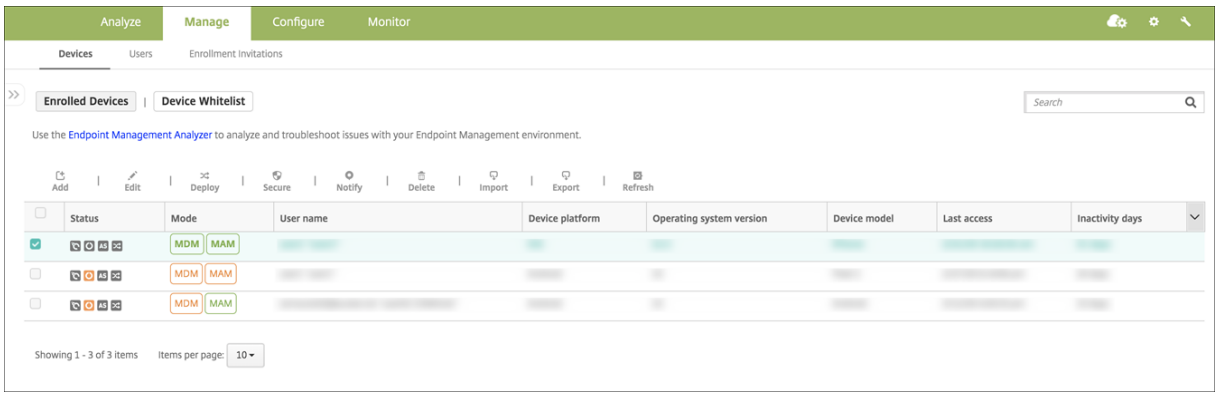
1. 转至管理 > 设备，然后单击导入。此时将显示导入预配文件对话框。



2. 单击选择文件，然后导航到要导入的文件。
3. 单击导入。设备表将列出导入的文件。
4. 要编辑设备信息，请将其选中，然后单击编辑。有关设备详细信息页面的信息，请参阅获取有关设备的信息。

部署到设备

可以强制一个或多个设备与 Endpoint Management 建立连接。所选设备立即接收资源，而无需等待下一次计划签入。



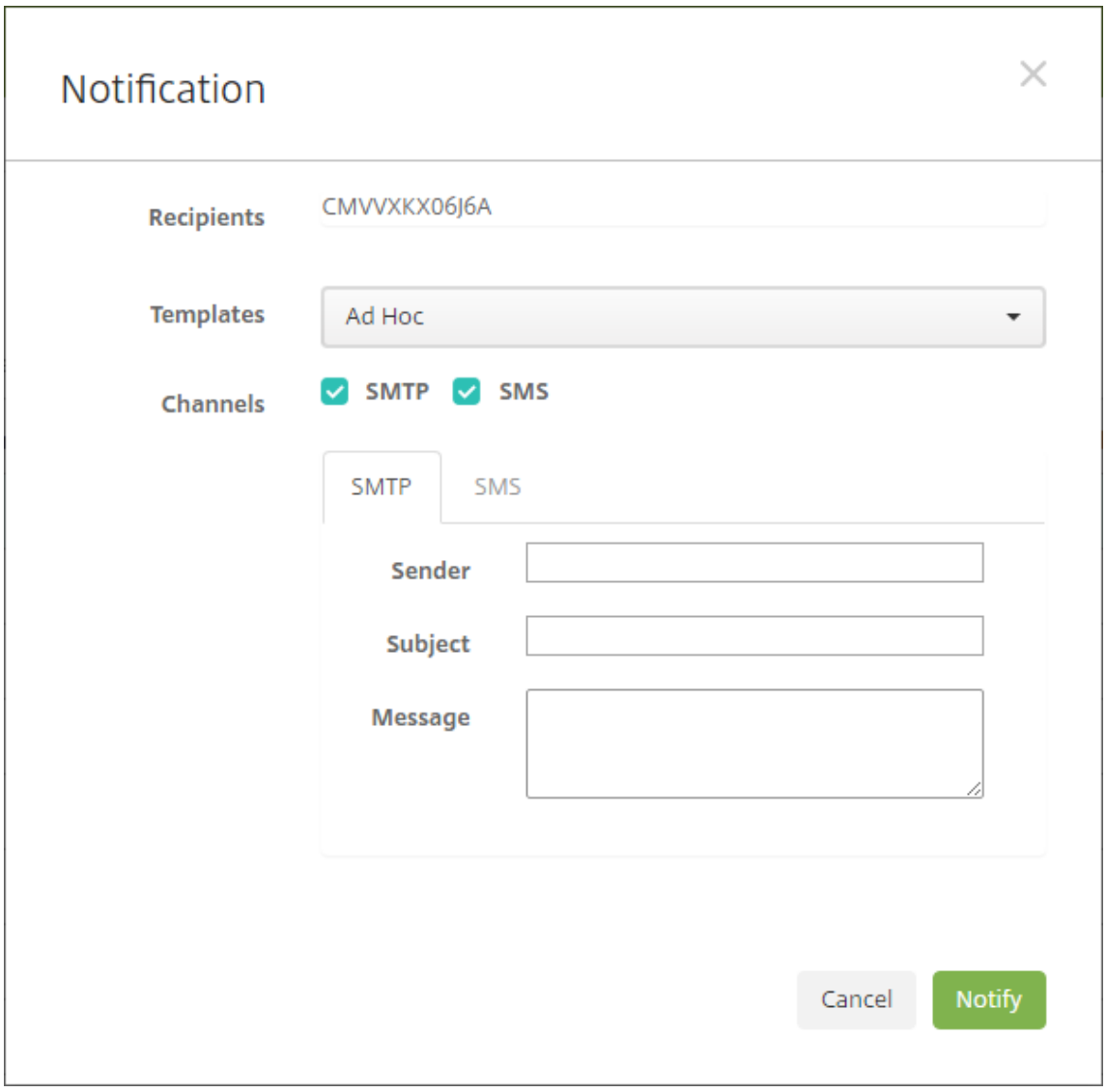
1. 转到管理 > 设备，选择 MDM 或 MDM+MAM 托管设备，然后单击部署。
2. 在对话框中，单击部署以确认您的操作。

向设备发送通知

您可以从设备页面向设备发送通知。有关通知的详细信息，请参阅通知。

1. 在 管理 > 设备页面上，选择要向其发送通知的一个或多个设备。
2. 单击通知。将显示通知对话框。收件人字段列出要接收通知的所有设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 配置以下设置：
    - 模板：在列表中，单击要发送的通知类型。对于除临时外的每个模板，主题和消息字段将显示为所选模板配置的文本。
    - 通道：选择消息的发送方式。默认值为 **SMTP**。单击选项卡以查看每个通道的消息格式。
    - 发件人：输入可选发件人。
    - 主题：输入临时消息的主题。
    - 消息：输入临时消息的消息。
4. 单击通知。

导出设备表

1. 根据您希望在导出文件中显示的内容过滤设备表。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 单击设备表上方的导出按钮。Endpoint Management 将提取过滤后的设备表中的信息，并将其转换为.csv 文件。
3. 系统提示时，打开或保存.csv 文件。

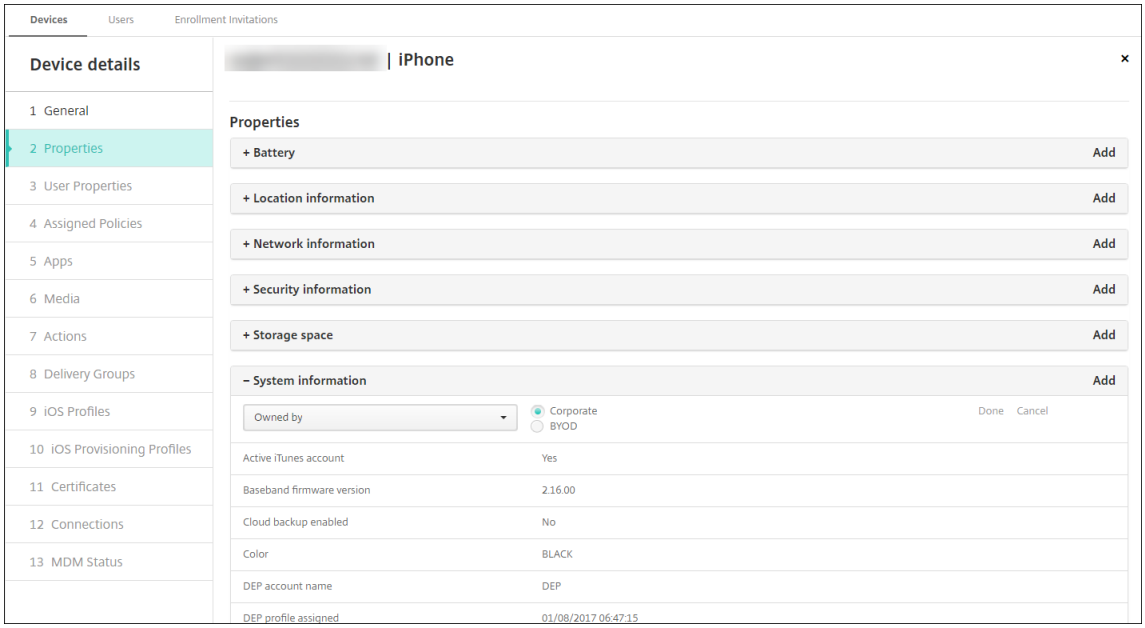
手动标记用户设备

您可以在 Endpoint Management 中通过以下方式手动标记设备：

- 在基于邀请的注册过程中。
- 在自助服务门户注册过程中。
- 通过添加设备所有权作为设备属性

您可以选择将设备标记为公司拥有或员工拥有。使用自助服务门户自助注册设备时，可以将设备标记为公司拥有或员工拥有。也可以手动标记设备，如下所示。

1. 在 Endpoint Management 控制台中，从设备选项卡向设备添加属性。
2. 添加名为所有者的属性，然后选择公司或 **BYOD**（员工拥有）。



自定义 **Active Directory** 用户属性

您可以自定义某些 Active Directory 用户属性，以定义 Endpoint Management 创建用户帐户时能够访问的属性。

要查看属性列表，请将 `optional.user.identity.attributes` 服务器属性作为自定义键添加到设置 **>** 服务器属性中。在值字段中，可以删除并稍后还原 Endpoint Management 默认提供的可选 Active Directory 用户属性。有关详细信息，请参阅服务器属性。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

编辑默认值列表并保存更改后，可以在管理 **>** 设备 **>** 用户属性中查看更新的 Active Directory 用户属性。Endpoint Management 会在用户登录到设备后或下次计划的设备签入期间更新控制台。如果您出现拼写错误或添加了不受支持的值，Endpoint Management 将忽略您的更改。

删除可选 Active Directory 用户属性可能会影响以下功能：

- 预配用户帐户：如果删除名字和姓氏值，Endpoint Management 将无法为 Citrix Content Collaboration 和 Salesforce 预配用户帐户。
- 注册邀请：如果删除用户的电子邮件或移动电话详细信息，用户将无法收到注册邀请。
- 设备通知操作：如果删除用户的电子邮件详细信息，用户将无法通过 SMTP 接收通知。
- 单点登录到 **Secure Mail**：如果删除显示名称值，用户将无法使用单点登录登录 Secure Mail。
- 用户属性和部署规则：如果删除用于配置用户属性和部署规则的任何可选属性，可能会影响现有配置。
- 操作：如果删除在配置 **>** 操作中用于设置自动操作的任何可选属性，可能会影响现有配置。
- 自定义报告：如果删除自定义报告中使用的任何可选属性，可能会影响现有配置。

搜索设备

为了进行快速搜索，默认搜索范围包括以下设备属性：

- 序列号
- IMEI
- Wi-Fi MAC 地址
- 蓝牙 MAC 地址
- Active Sync ID
- 用户名

可以通过服务器属性 **include.device.properties.during.search** 配置搜索范围，其默认值为 **false**。要在设备搜索中包括所有设备属性，请转至设置 **>** 服务器属性并将该设置更改为 **true**。

设备预配文件格式

许多移动运营商或设备制造商都会提供授权移动设备的列表。可以使用这些列表来避免手动输入长长的移动设备列表。Endpoint Management 支持以下受支持的设备类型通用的导入文件格式：Android、iOS 和 Windows。

手动创建的预配文件必须采用以下格式：

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;
propertyName2;propertyValue2; ... propertyNameN;propertyValueN
```

请紧急以下几点：

- 有关每个属性的有效值，请参阅 PDF 设备属性名称和值。
- 使用 UTF-8 字符集。
- 使用分号 (;) 分隔预配文件中的字段。如果字段的一部分有分号，请使用反斜杠字符 (\) 对其进行转义。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

例如，对于此属性：

```
propertyV;test;1;2
```

按如下所示对其进行转义：

```
propertyV\;test\;1\;2
```

- 对于 iOS 设备，必须提供序列号，因为序列号是 iOS 设备标识符。
- 对于其他设备平台，必须包括序列号或 IMEI。
- **OperatingSystemFamily** 的有效值为 **WINDOWS**、**ANDROID** 或 **iOS**。

设备预配文件示例：

```
`1050BF3F51730108161006551059039l;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F51730108161006551059039l;25244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F51730108161006551059039l;35244201625379903;iOS;test;
4050BF3F51730108161006551059039l;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

文件中的每行都描述一个设备。该示例中第一个条目的含义如下：

- 序列号：1050BF3F51730108161006551059039l
- IMEI：15244201625379901
- 操作系统系列：WINDOWS
- 属性名称：propertyN
- 属性值：propertyV\;test\;1\;2;prop 2

Alexa for Business

December 3, 2021

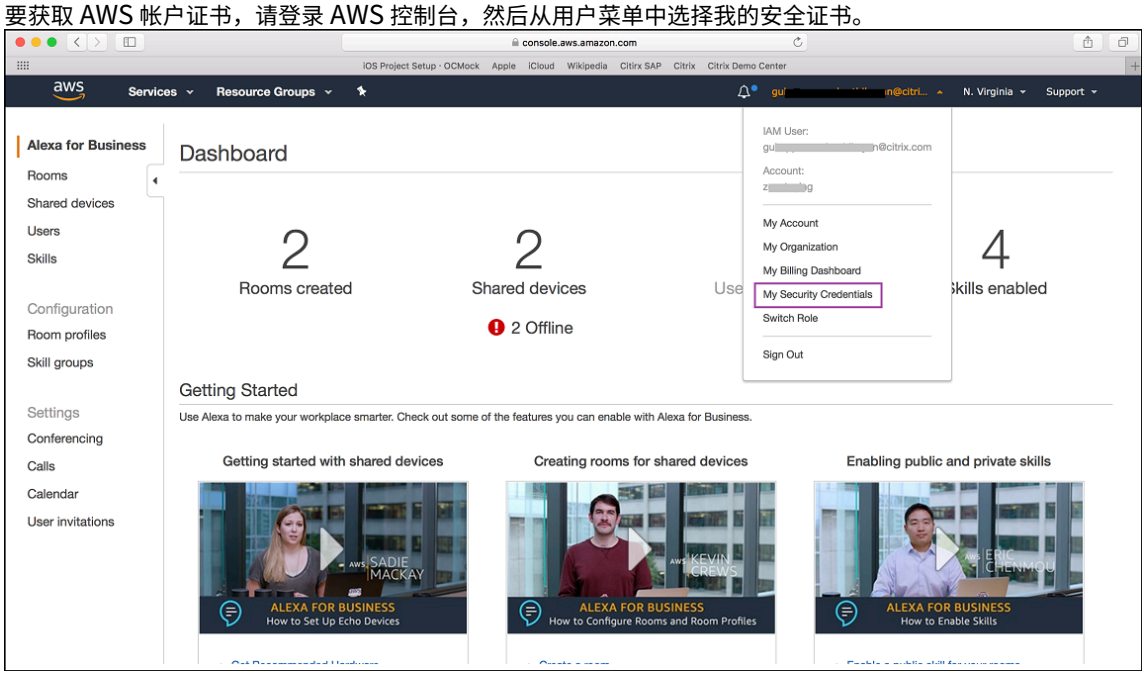
Amazon Web Services (AWS) 的 Alexa for Business 服务允许您管理大量支持 Alexa 的设备，以供企业使用，例如会议室协助。Endpoint Management 允许您在 Endpoint Management 控制台中配置和管理这些设备。Endpoint Management 不会将策略直接部署到 Alexa 设备。相反，Endpoint Management 会更新 AWS 服务，AWS 将配置交付给 Alexa 设备。

有关将 Alexa 用于企业版的信息，请参阅《适用 于企业管理的 Alexa 指南》。

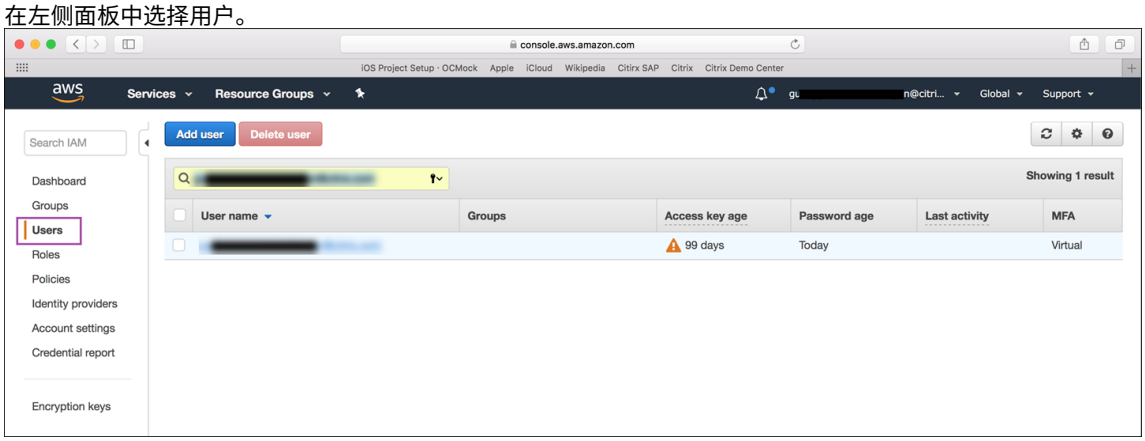
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

向 **Endpoint Management** 验证您的 **AWS** 帐户

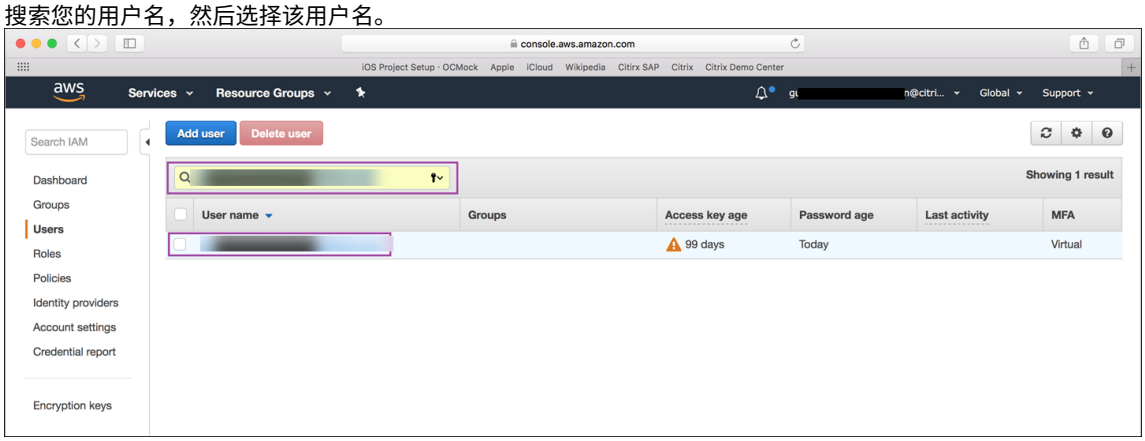
1. 要获取 AWS 帐户证书，请登录 AWS 控制台，然后从用户菜单中选择我的安全证书。



2. 在左侧面板中选择用户。

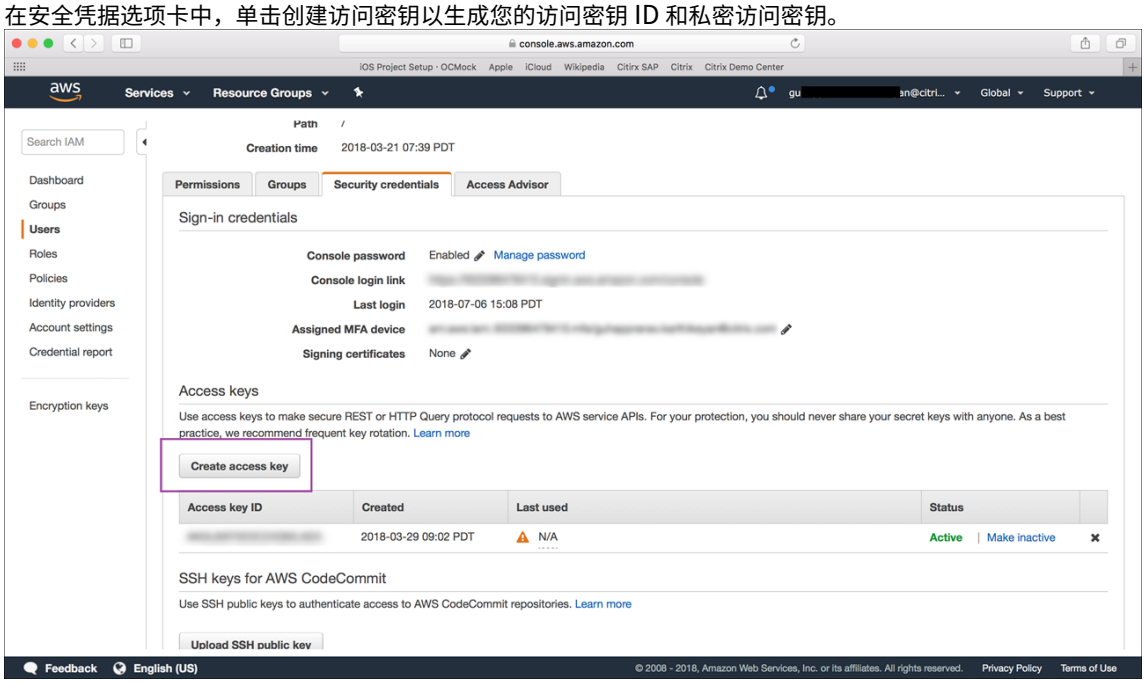


3. 搜索您的用户名，然后选择该用户名。

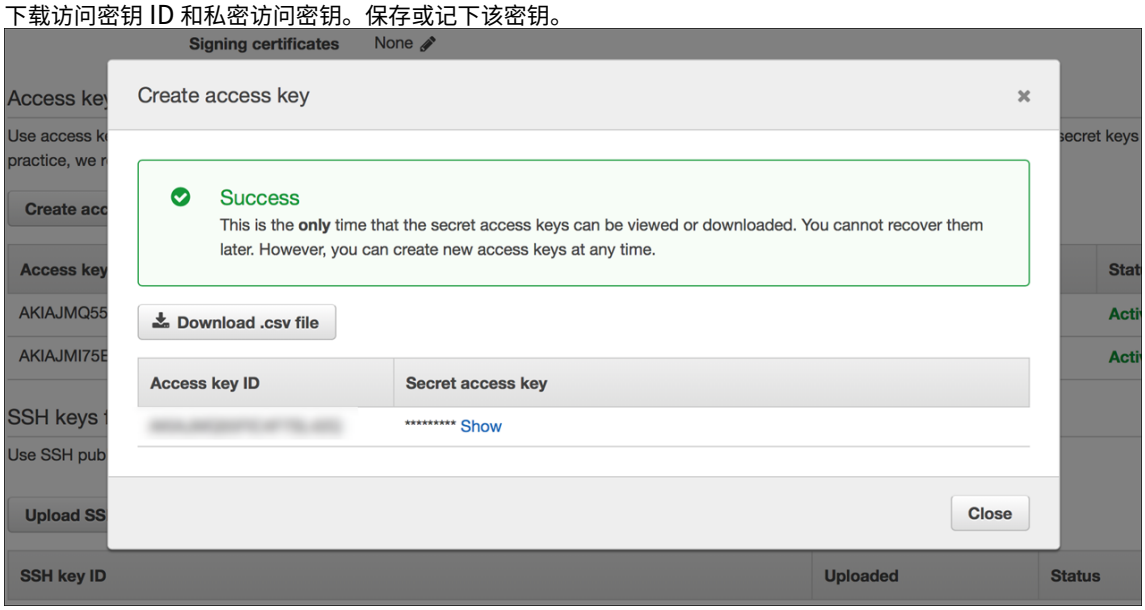


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

4. 在安全凭据选项卡中，单击创建访问密钥以生成您的访问密钥 ID 和私密访问密钥。



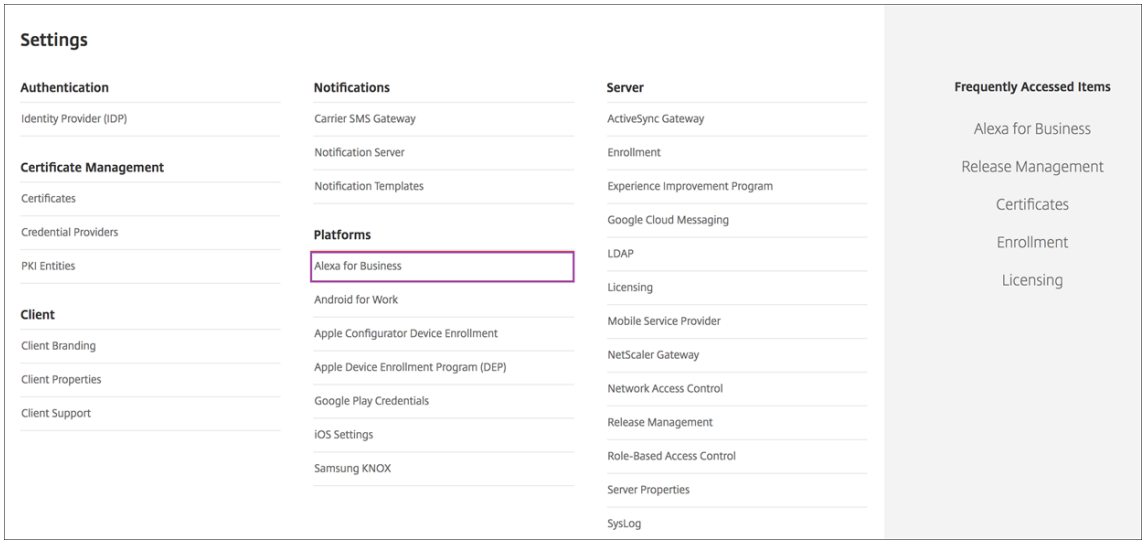
5. 下载访问密钥 ID 和私密访问密钥。保存或记下该密钥。



6. 在 Endpoint Management 控制台中，单击齿轮图标以转到设置。

7. 在平台下，选择 **Alexa for Business**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



8. 输入您的访问密钥 ID 和私密访问密钥。单击保存。



在 **Endpoint Management** 上配置 **Alexa for Business**

Endpoint Management 允许您配置：

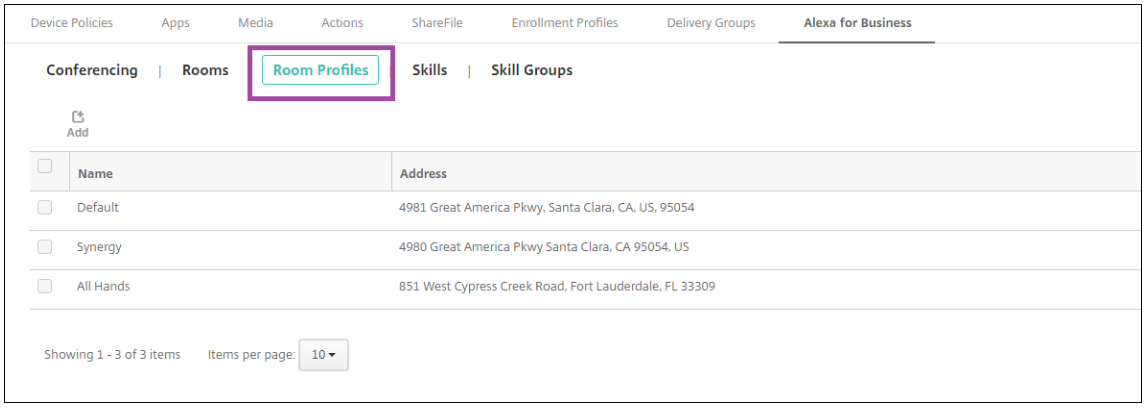
- 您应用到包含 Alexa 设备的房间的设置的房间配置文件
- 代表包含设备的物理房间的房间
- 分配给房间或设备的技能组
- Alexa 技能库中可添加到技能组的 Alexa 技能
- 通过会议功能，您可以选择会议提供商，以及控制人们在房间中安排和加入会议的方式

配置房间配置文件

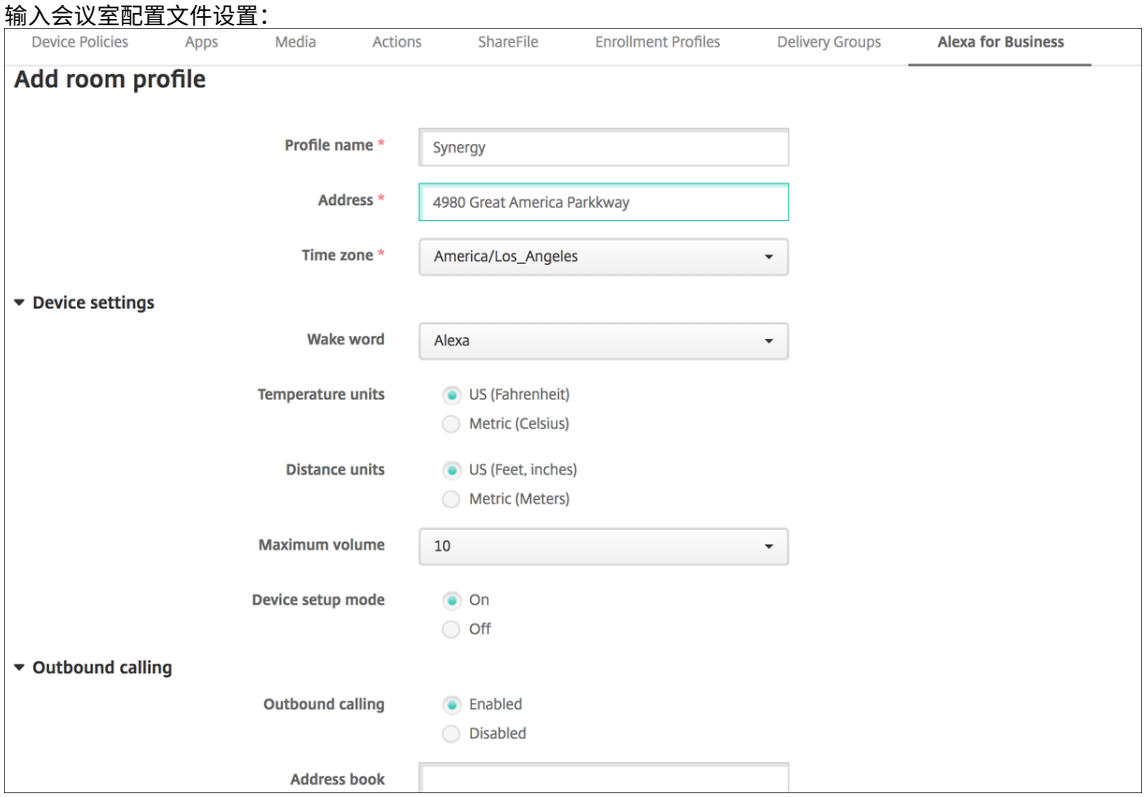
房间配置文件是一组常见配置，可应用于包含 Alexa 设备的房间集合。可以添加、编辑和删除房间配置文件。

1. 在 Endpoint Management 控制台中，选择配置 **> Alexa for Business >** 房间配置文件。此时将显示可用房间配置文件列表。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 要添加房间配置文件，请单击添加。要编辑房间配置文件，请选择要编辑的房间配置文件，然后单击编辑。
3. 输入会议室配置文件设置：



- 配置文件名称：键入配置文件的名称。
- 地址：键入包含 Alexa 设备的房间的建筑物的物理（街道）地址。
- 时区：选择地点的时区。
- 唤醒词：选择 Alexa 设备响应的唤醒词。
- 温度单位：选择 Alexa 设备报告温度的单位。
- 距离单位：选择 Alexa 设备报告距离的单位。
- 最大音量：为 Alexa 选择最大音量设置。
- 设备设置模式：通过强制 Alexa 设备进入设备设置模式，选择是否可以重新配置 Alexa 设备。
- 拨出电话：启用或禁用 Alexa 设备的拨出电话功能。
- 通讯簿：设置 Alexa 设备的通讯簿配置。

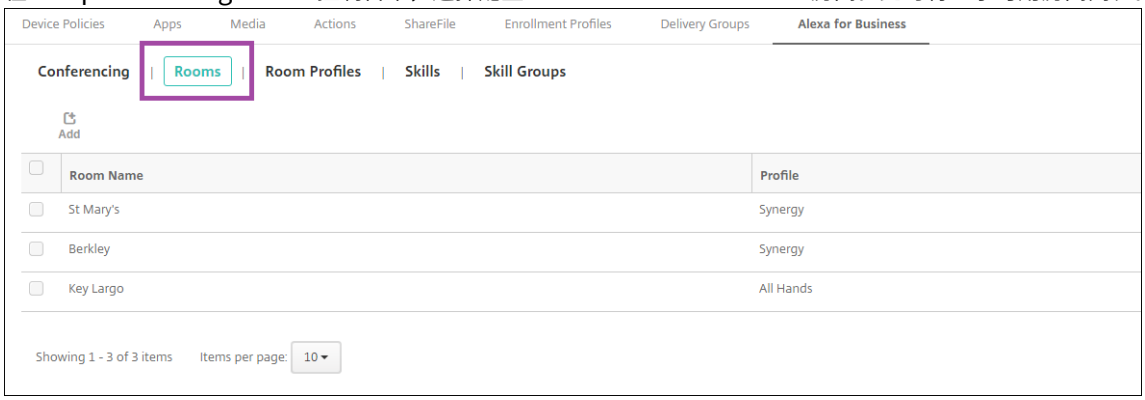
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

4. 单击保存。

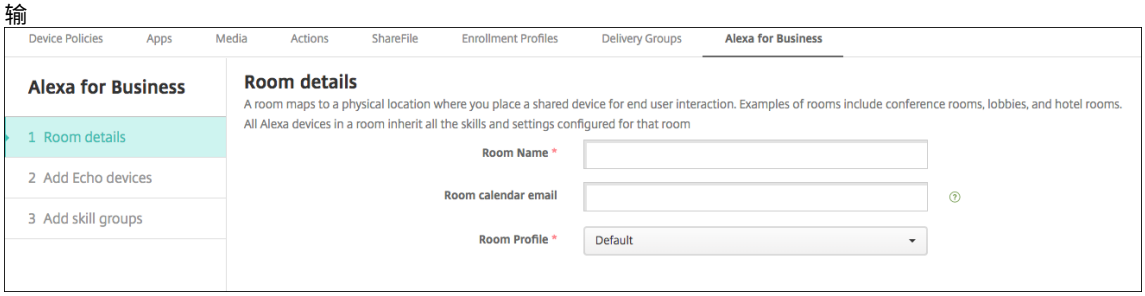
配置房间

您在 Endpoint Management 控制台中配置的房间代表建筑物中的物理房间、会议室和其他房间。配置房间时，您可以将 Alexa 设备与该房间相关联，并将技能组添加到该设备中。可以添加、编辑和删除房间。

1. 在 Endpoint Management 控制台中，选择配置 **> Alexa for Business >** 房间。此时将显示可用房间列表。



2. 要添加房间，请单击添加。要编辑房间，请选择要编辑的房间，然后单击编辑。
3. 输

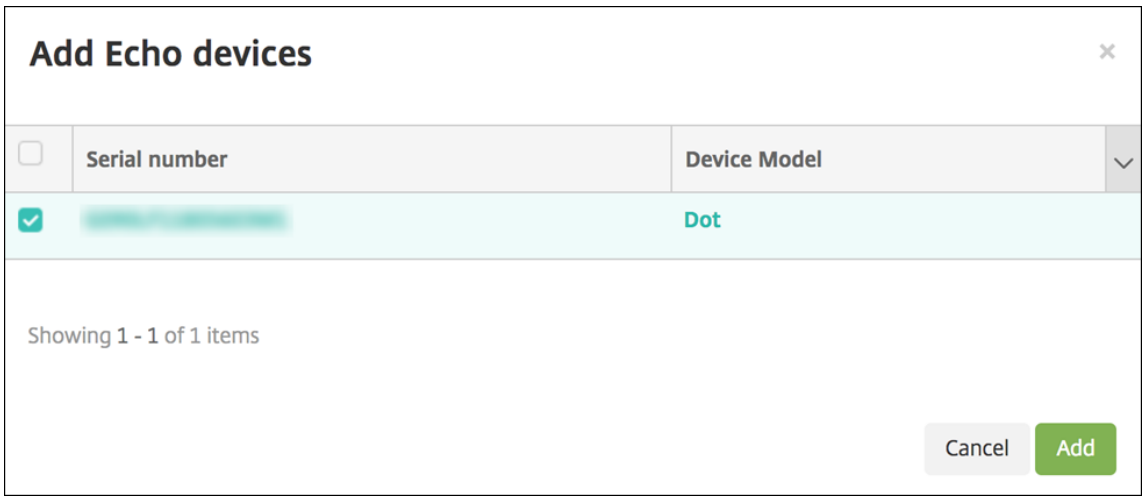


-会议 室名称：键入会议室、会议室或其他会议室的名称。

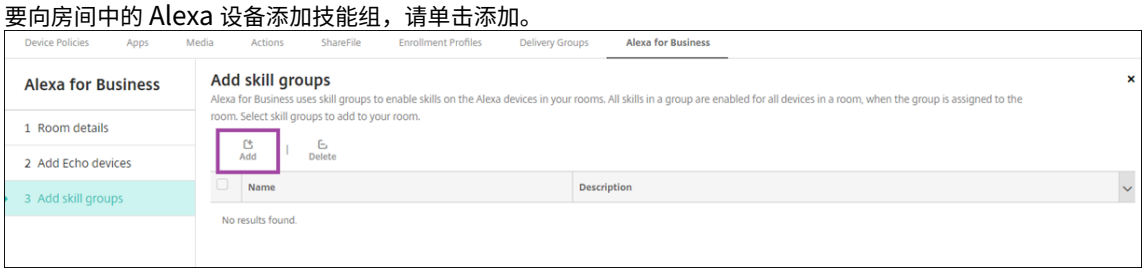
- 房间日历电子邮件：键入房间的日历电子邮件地址。
- 房间配置文件：选择房间的房间配置文件配置的名称。

4. 单击下一步。
5. 要将 Alexa 设备与房间关联，请单击添加。
6. 选择一个设备，然后单击添加。选定的设备将显示在添加回声设备页面中。

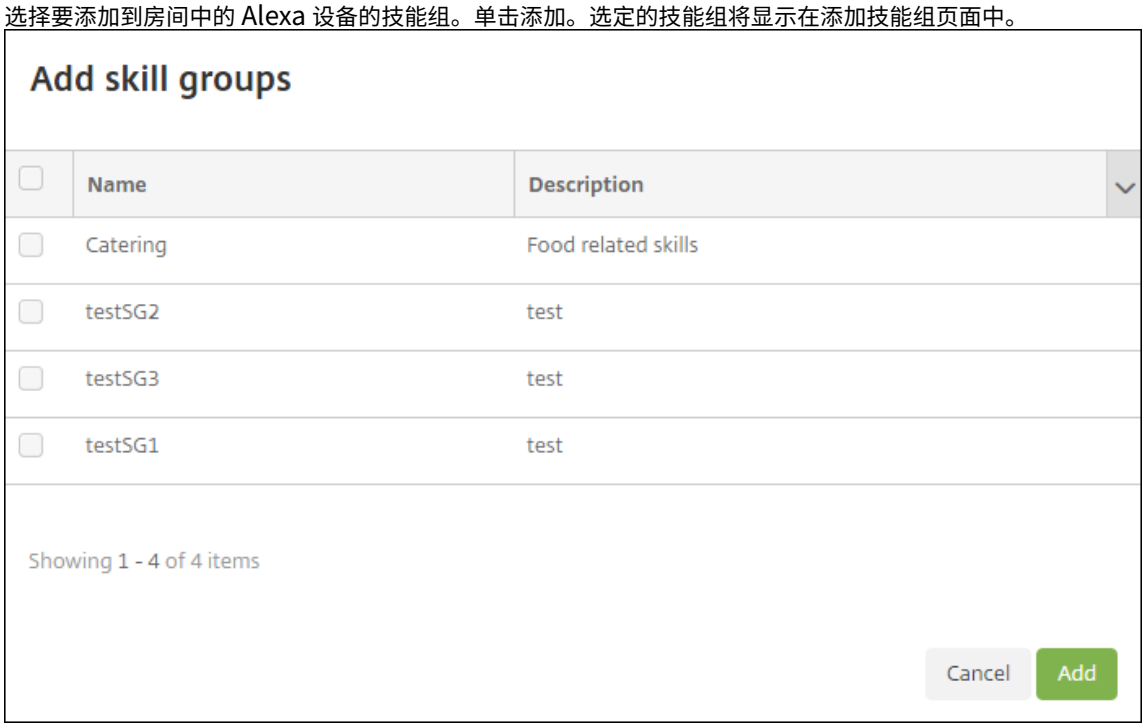
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



7. 单击下一步。
8. 要向房间中的 Alexa 设备添加技能组，请单击添加。



9. 选择要添加到房间中的 Alexa 设备的技能组。单击添加。选定的技能组将显示在添加技能组页面中。



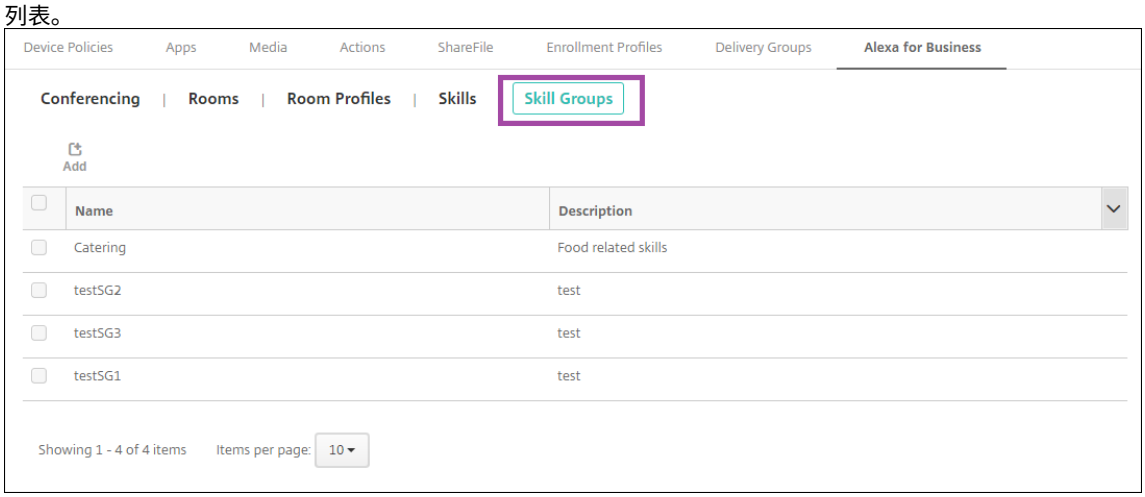
10. 单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

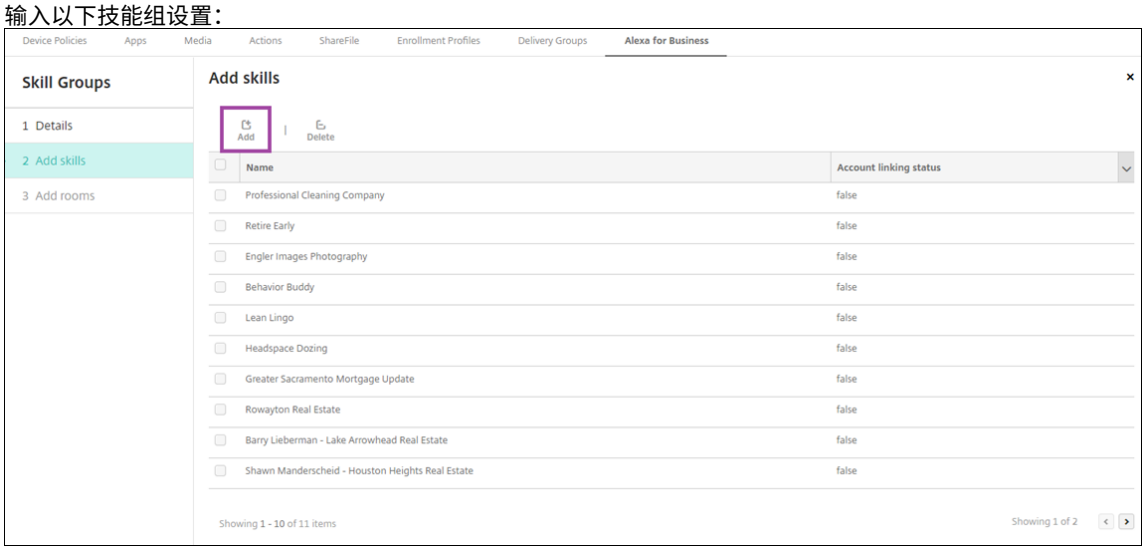
配置技能组

技能组是可应用于房间的技能集合。可以创建技能组，然后将其分配给房间。通过技能，您可以使用 Alexa 设备执行诸如启动和结束在线会议或查看议程项目列表之类的操作。可以添加、编辑和删除技能组。

1. 在 Endpoint Management 控制台中，选择配置 **> Alexa for Business >** 技能组。此时将显示可用技能组列表。

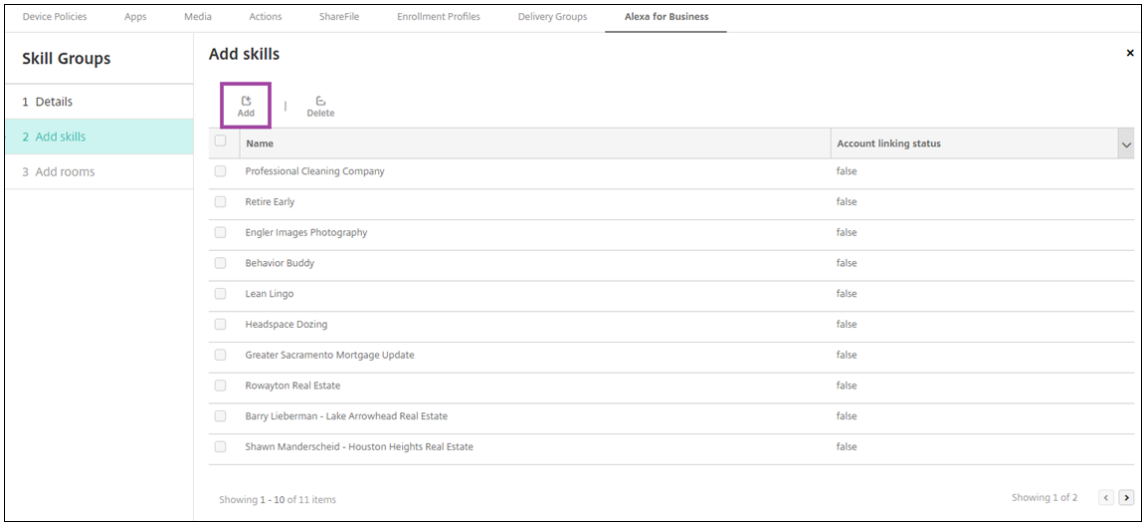


2. 要添加技能组，请单击添加。要编辑技能组，请选择要编辑的技能组，然后单击编辑。
3. 输入以下技能组设置：

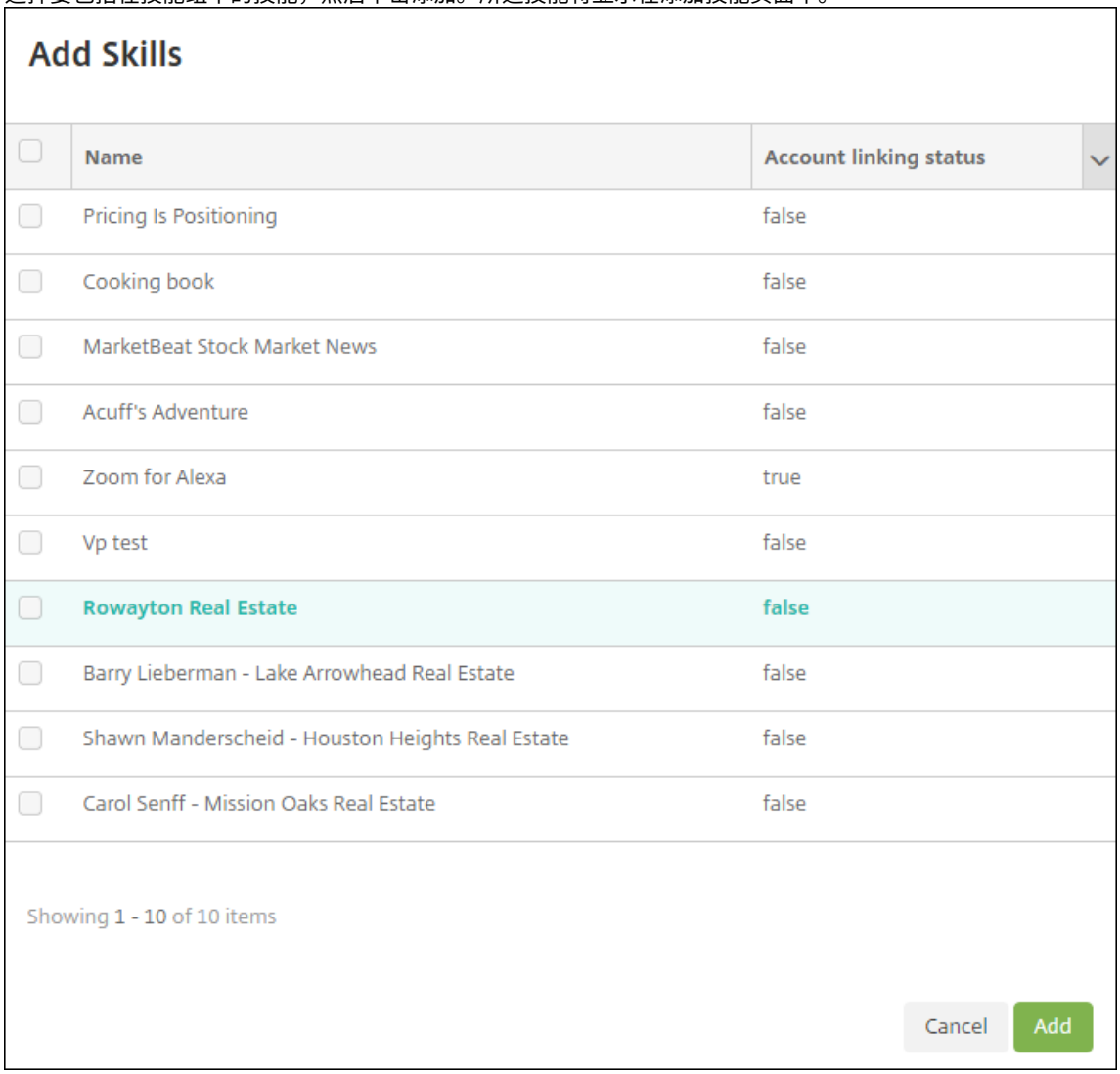


   - 名称：键入技能组的名称。
   - 说明：键入技能组的简要说明。
4. 单击下一步。
5. 要向技能组中添加技能，请单击添加。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

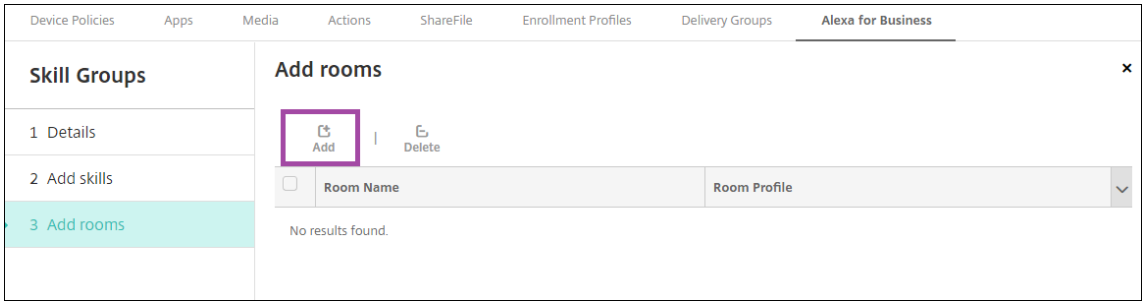


6. 选择要包括在技能组中的技能，然后单击添加。所选技能将显示在添加技能页面中。

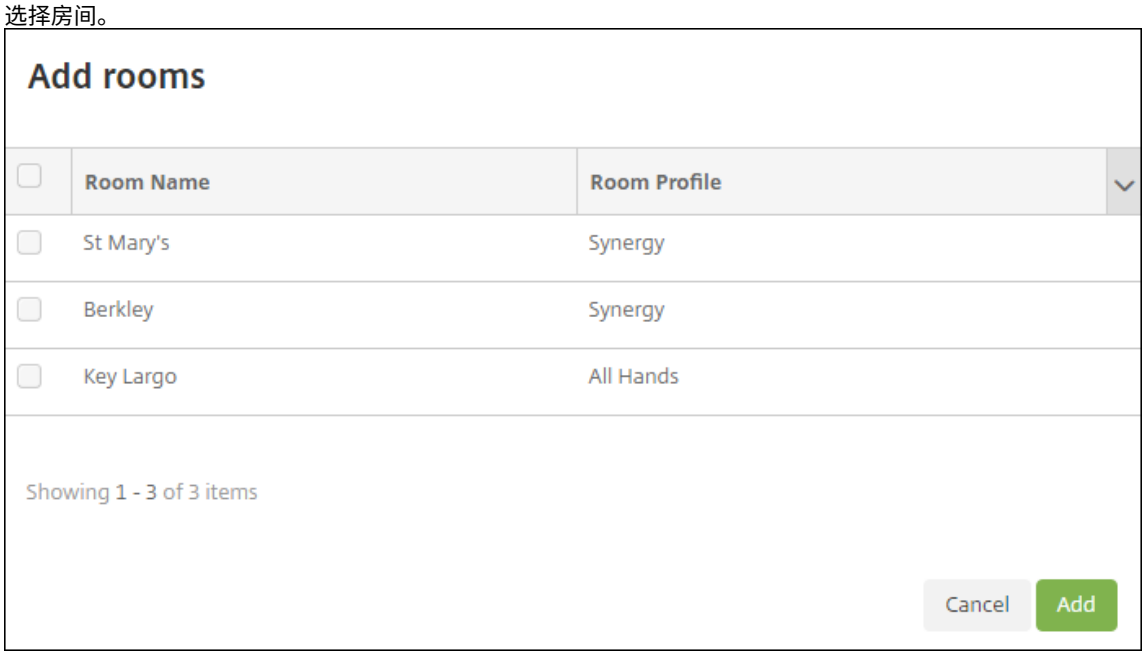


7. 要将技能组添加到指定房间中的 Alexa 设备，请单击添加。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



8. 选择房间。



9. 单击保存。

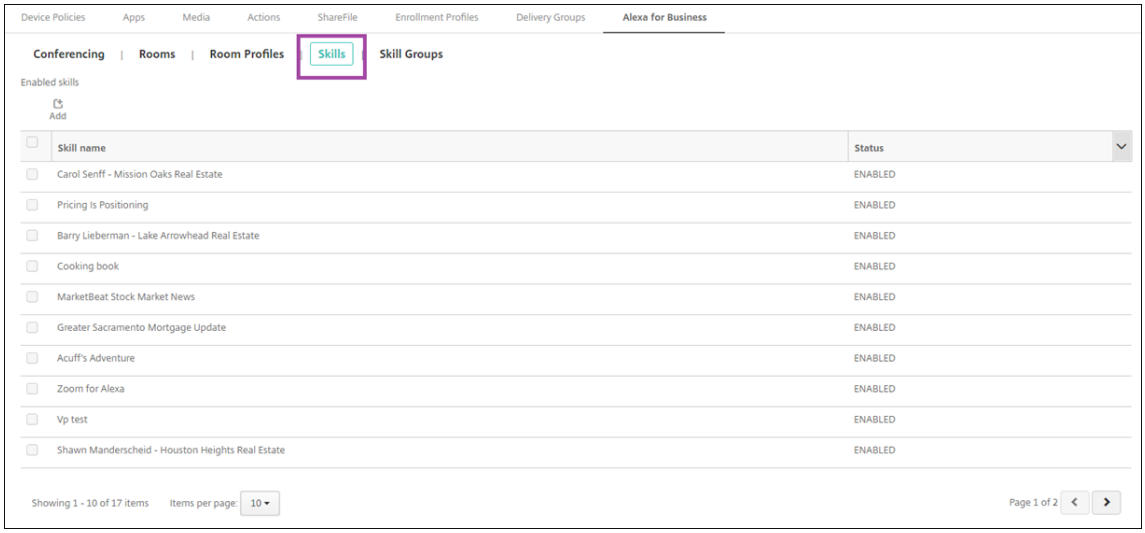
使技能可用于技能组

可以配置您的 Alexa for Business 组织中可包含在技能组中的 Alexa 技能列表。这些技能来自公共 Alexa 技能库或为贵组织发布的专用技能。

向贵组织添加技能

1. 在 Endpoint Management 控制台中，选择配置 **> Alexa for Business >** 技能。此时将显示已启用的技能列表。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 要添加技能，请单击添加。
3. 要查看更多 Alexa 技能，请选择一种类别，然后单击显示更多。单击显示更多可将多达 10 种技能添加到贵组织中的可用技能列表中。再次单击显示更多可添加更多技能。

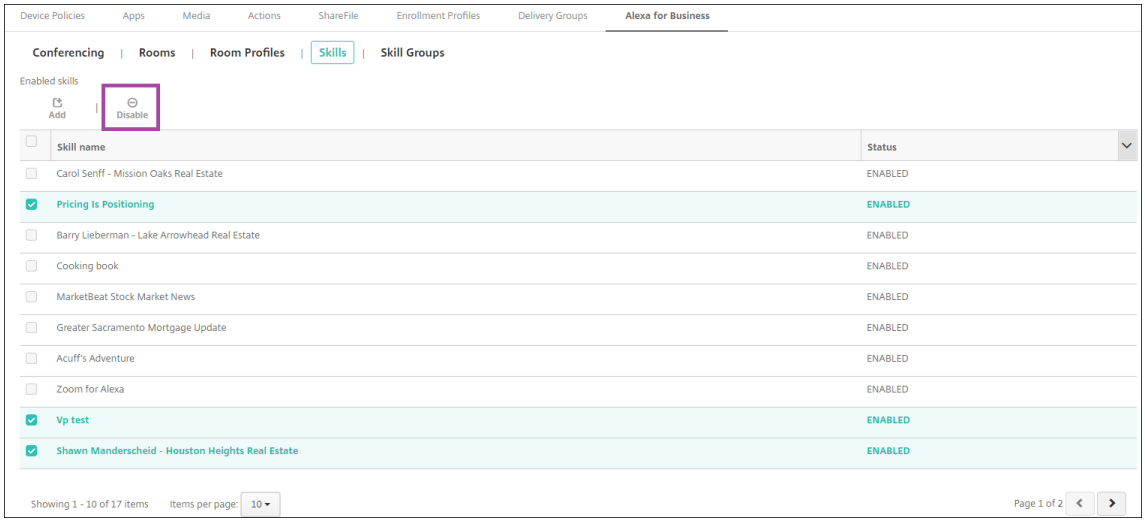


4. 选择要添加到贵组织的技能。
5. 单击保存。

删除贵组织中的技能

1. 在 Endpoint Management 控制台中，选择配置 **> Alexa for Business >** 技能。此时将显示已启用的技能列表。
2. 选择要从贵组织中删除的技能。
3. 单击禁用。

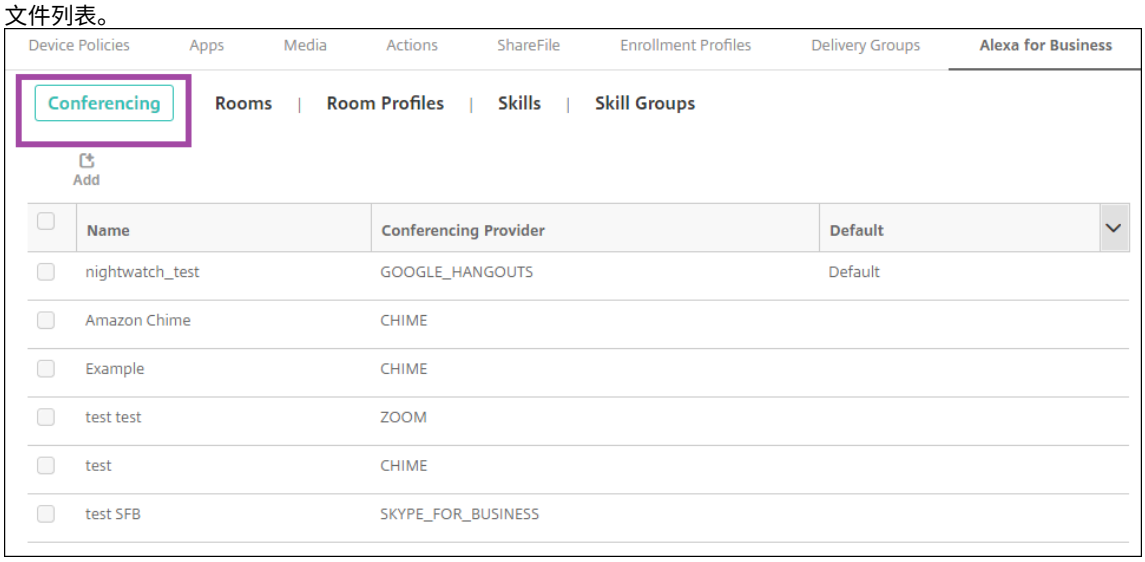
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



配置会议

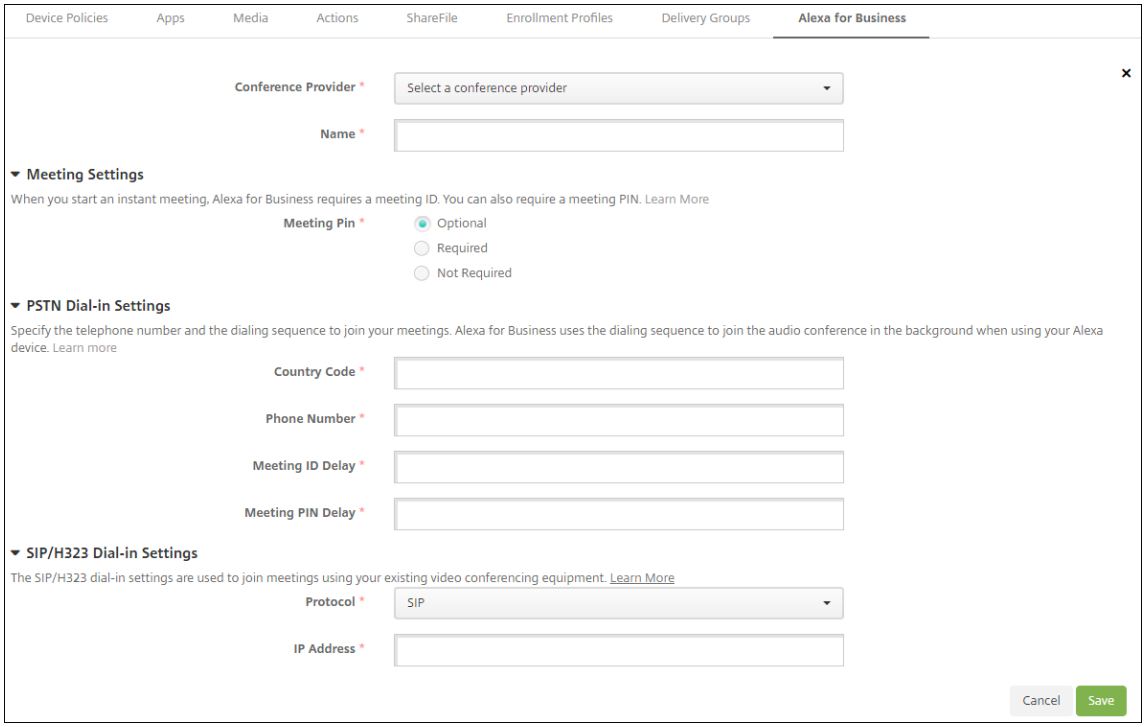
通过会议功能，您可以配置会议提供提供程序（例如 Google Hangout 或 Amazon Chime），这些提供程序控制用户在包含 Alexa 设备的会议室中加入会议的方式。可以添加、编辑和删除会议提供程序。还可以设置默认会议提供程序。

1. 在 Endpoint Management 控制台中，选择配置 **> Alexa for Business >** 会议。此时将显示可用房间配置文件列表。



2. 要添加会议提供程序，请单击添加。要编辑会议提供程序，请选择要编辑的房间配置文件，然后单击编辑。
3. 输入会议室配置文件设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 会议提供程序：从列表中选择会议提供程序。
- 名称：键入要为会议提供程序指定的名称。
- 会议 **PIN**：指定是否需要 PIN 码才能加入会议。
- **PSTN** 拨入设置
  - 国家/地区代码：键入国家/地区代码。
  - 电话号码：键入电话号码。
  - 会议 **ID** 延迟：指定发送会议 ID 之前的秒数。
  - 会议 **PIN** 延迟：指定发送 PIN 码之前的秒数。
- **SIP/H323** 拨入设置 SIP/H323 拨入设置用于使用您的现有视频会议设备加入会议。
  - 协议：选择协议。
  - **IP** 地址：键入 IP 地址。

4. 单击保存。

如果配置了多个会议提供程序，请设置默认提供程序。

1. 在 Endpoint Management 控制台中，选择配置 **> Alexa for Business >** 会议。此时将显示可用房间配置文件列表。
2. 选择要设置为默认会议提供程序的提供程序。
3. 单击设置默认值。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

从设备管理迁移到 **Android Enterprise**

December 3, 2021

本文探讨了从旧版 Android 设备管理迁移到 Android Enterprise 的注意事项和建议。Google 即将弃用 Android 设备管理 API。该 API 支持 Android 设备上的企业应用程序。Android Enterprise 是 Google 和 Citrix 推荐的现代化管理解决方案。

Endpoint Management 正在更改为 Android Enterprise 作为 Android 设备的默认注册方法。Google 弃用 API 后，在设备管理模式下 Android Q 设备的注册将失败。

Android Enterprise 支持完全托管和工作配置文件设备模式。谷歌出版物 Android 企业迁移蓝皮书详细解释了旧设备管理和 Android Enterprise 之间的区别。我们建议您阅读 Google 提供的迁移信息。

我们建议您还参阅 Citrix Tech Zone 文章 “ 使用 Citrix Endpoint Management 从 Android 设备管理员迁移到 Android Enterprise”。

设备管理弃用的影响

Google 已弃用设备管理员 API，自 2020 年 11 月 2 日起将不再支持这些 API。在我们将 Citrix Secure Hub 升级到目标 Android API 级别 29 后，这些 API 将无法在运行 Android 10+ 的设备上运行：

- 禁用相机头：控制对设备相机的访问。
- 键盘锁功能：控制与设备锁定有关的功能，例如生物识别和图案。
- 密码过期：强制用户在可配置的时间段后更改密码。
- 限制密码：设置限制性密码要求。

要求和建议

- 如果您可以将设备升级到 Android 10+，则必须在 Android Enterprise 中注册该设备。
  - 必须将 Android 11 设备注册到 Android Enterprise。
  - 截至 2020 年 9 月，对于 Android 10 设备：Citrix 不支持进入设备管理模式的新注册或设备重新注册。如上一部分中所述，已注册的设备将继续运行至 2020 年 11 月 2 日。
- 对于运行 Android 9 及更低版本的设备，我们支持旧设备管理模式。但是，我们建议尽快将这些设备移动到 Android Enterprise。
- 对于在 Citrix 仅 MAM 模式下注册的新设备或现有设备，无需执行任何操作。弃用的 Google API 不会对仅 MAM 模式下的设备产生任何影响。但是，随着向平台加密的迁移，我们强烈建议从仅 MAM 模式迁移到 Android Enterprise 工作配置文件模式 (BYOD)。工作配置文件模式提供 MAM 功能，但在设备上的容器中提供。

分析

迁移的分析阶段包括：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 了解您的旧版 Android 设置
- 记录您的旧版设置，以便您可以将旧版功能映射到 Android Enterprise 功能

建议的分析

1. 在 Endpoint Management 上评估 Android Enterprise：完全托管，通过工作配置文件、专用设备、工作配置文件 (BYOD) 进行完全托管。
2. 根据 Android Enterprise 分析您当前的设备管理功能。
3. 记录您的设备管理用例。

要记录您的设备管理用例，请执行以下操作：

1. 在 Endpoint Management 控制台中创建电子表格并列出当前的策略组。
2. 基于现有策略组创建单独的用例。
3. 对于每个用例，请记录以下内容：
    - 名
    - 企业所有者
    - 用户身份模型
    - 设备要求
        - 安全
        - 管理
        - 可用性
    - 设备清单
        - 制造商和型号
        - 操作系统版本
    - 应用程序
4. 对于每个应用程序，请列出：
    - 应用程序名称
    - 软件包名称
    - 托管方法
    - 应用程序是公用还是专用
    - 应用程序是否具有强制性 (true/false)

要求映射

根据完成的分析，确定您的 Android Enterprise 功能要求。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

建议的要求映射

1. 确定管理模式和注册方法：
    - 工作配置文件 (BYOD)：需要重新注册。无需重置出厂设置。
    - 完全托管：需要恢复出厂设置。使用 QR 码、近场通信 (NFC) 碰撞、设备策略控制器 (DPC) 标识符、零触摸方式注册设备。
2. 创建应用程序迁移策略。
3. 将用例要求映射到 Android Enterprise 功能。记录与要求最匹配的每个设备要求及其相应的 Android 版本的功能。
4. 根据功能要求（7.0、8.0、9.0）确定最低 Android 操作系统。
5. 选择身份模型：
    - 建议：托管 Google Play 帐户
    - 仅当您是谷歌云身份识别客户时才使用 Google Workspace 帐号
6. 创建设备策略：
    - 无操作：如果设备满足最低操作系统级别
    - 升级：如果设备支持且可以更新到支持的操作系统
    - 替换：如果设备无法更新到支持的操作系统级别

推荐的应用程序迁移策略

完成需求映射后，将应用程序从 Android 平台移动到 Android Enterprise 平台。有关发布应用的详细信息，请参阅添加应用。

- 公共应用商店应用程序
    1. 选择要迁移的应用程序，然后编辑应用程序以清除 Google Play 设置，然后选择 **Android Enterprise** 作为平台。
    2. 选择交付组。如果某个应用程序是必需的，请将该应用程序移动到交付组中的必需应用程序列表。

    保存应用程序后，该应用程序将显示在 Google Play 应用商店中。如果您有工作配置文件，应用程序将显示在工作配置文件中的 Google Play 应用商店中。
- 专用（企业）应用程序

    专用应用程序由内部开发人员或第三方开发人员开发。我们建议您使用 Google Play 发布专用应用程序。
    1. 选择要迁移的应用程序，然后编辑应用程序以选择 **Android Enterprise** 作为平台。
    2. 上载 APK 文件，然后配置应用程序设置。
    3. 将应用程序发布到所需的交付组。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- MDX 应用程序

  1. 选择要迁移的应用程序，然后编辑应用程序以选择 **Android Enterprise** 作为平台。
  2. 上载 MDX 文件。完成应用程序审批流程。
  3. 选择 MDX 策略。

  对于企业 MDX 应用程序，我们建议将其更改为 MDX SDK 模式打包的应用程序：

  - 选项 1：使用专门分配给贵组织的开发人员帐户在 Google Play 中托管 APK。在 Endpoint Management 中发布 MDX 文件。
  - 选项 2：从 Endpoint Management 发布应用程序作为企业应用程序。在 Endpoint Management 中发布 APK，并为 MDX 文件选择平台 **Android Enterprise**。

Citrix 设备策略迁移

对于同时适用于 **Android (**旧版 **DA)** 和 **Android Enterprise** 平台的策略：请编辑策略并选择平台 **Android Enterprise**。

- 对于 Android Enterprise，请考虑设备注册方法。某些策略选项仅适用于处于工作配置文件模式或完全托管模式的设备。请参阅配置 Android Enterprise 设备和应用程序策略。
- 如果您对旧式 DA 设备使用 Exchange 设备策略，请改为创建托管配置策略设备策略以配置电子邮件设置。
- 为确保使策略针对预期设备（Android Enterprise 与旧版 DA），请向策略中添加部署规则。例如，对于旧版 DA 平台，请使用以下部署规则：

```
Limit by known device property name Android Enterprise
Enabled Device? Isn' t equal to true
<!--NeedCopy-->
```

该部署规则将检查设备是否未针对 Android Enterprise 启用，并将策略和应用程序一起提供给为旧版 DA 启用的设备。

概念证明

将应用程序迁移到 Android Enterprise 后，可以设置迁移测试以验证功能是否按预期运行。

推荐的概念证明设置

1. 设置部署基础结构：
   - 为您的 Android Enterprise 测试创建交付组。
   - 在 Endpoint Management 中配置 Android Enterprise。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 设置用户应用程序。
3. 配置 Android Enterprise 功能。
4. 将策略分配给 Android Enterprise 交付组。
5. 测试和确认功能。
6. 完成每个用例的设备设置流程。
7. 记录用户设置步骤。

部署

现在，您可以部署 Android Enterprise 设置并准备用户进行迁移。

建议的部署策略

Citrix 推荐的部署策略是为 Android Enterprise 测试所有生产系统，然后在以后完成设备迁移。

- 在这种情况下，用户继续使用旧设备与其当前配置。可以为 Android Enterprise 管理设置新设备。
- 请仅在需要升级或更换时迁移现有设备。
- 在常规生命周期结束时将现有设备迁移到 Android Enterprise 管理中。或者，在这些设备因丢失或损坏而需要更换时，迁移这些设备。

Android Enterprise

April 11, 2023

Android Enterprise 是一套由 Google 提供的作为 Android 设备的企业管理解决方案工具和服务。借助 Android Enterprise：

- 可以使用 Endpoint Management 管理公司拥有的 Android 设备以及携带自己的 (BYOD) Android 设备。
- 可以管理整个设备或设备上的单独配置文件。这一单独的配置文件将企业帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。
- 还可以管理专用于单一用途的设备，例如库存管理。有关 Google 对 Android Enterprise 的功能的概述，请参阅 Android Enterprise 管理。

资源：

- 有关与 Android Enterprise 相关的术语和定义的列表，请参阅 Google Android Enterprise 开发人员指南文章 Android Enterprise terminology（Android Enterprise 术语）。Google 经常更新这些术语。
- 有关 Endpoint Management 支持的 Android 操作系统列表，请参阅支持的设备操作系统。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 有关为 Android Enterprise 设置网络环境时要考虑的出站连接的信息，请参阅 Google 支持文章 Android Enterprise Network Requirements（Android Enterprise 网络要求）。
- 有关部署 Android Enterprise 的信息，请参阅部署资源)。

Android Enterprise 入门

> 重要：
>
> 设备管理模式不再受支持。如果您的用户的设备采用设备管理模式，则请参阅从设备管理迁移到 Android Enterprise。将设备迁移到 Android Enterprise 后，请按照以下步骤设置 Android Enterprise 设备。



一次性设置

1. 创建托管 Google Play 帐户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

请参阅将托管 Google Play 与 Endpoint Management 结合使用和要求。

2. 将您的 Google Play 帐户绑定到 Endpoint Management。

   请参阅将 Endpoint Management 连接到 Google Play。

3. 规划您希望管理设备的方式。

   请参阅设备部署方案和配置文件。

4. 规划用户设备的注册安全性。

   请参阅注册安全性。

5. 准备交付启用了 MDX 的应用程序。

   使用 MAM SDK 开发应用程序。或者，如果您尚未准备好过渡到新 SDK，请使用基于命令行的 MDX Toolkit 来封装应用程序。

   请参阅 MAM SDK 概述。

此时，您已准备好使用应用程序和设备策略、注册配置文件以及应用程序来配置 Android Enterprise 设备。有关指导，请参阅以下部分。

配置设备

1. 创建交付组。

   控制哪些用户获得哪些资源以及何时获得资源。请参阅部署资源。

   我们将停止向注册了 Android Enterprise 的设备提供为传统 DA 平台发布的应用程序。对于 Android Enterprise 设备，请发布适用于 Android Enterprise 平台的应用程序。要继续将旧版 DA 应用程序发布到 DA 模式下的设备，请为这些应用程序创建单独的交付组。请参阅弃用。

2. 添加应用程序。可以直接从 Endpoint Management 控制台审批 Google Play 中的应用程序。

   请参阅 Google 支持文章 Manage apps in your organization（管理贵组织中的应用程序）。

3. 创建注册配置文件。

   指定设备和应用程序管理注册选项。请参阅设备部署方案和配置文件和创建注册配置文件。

   - 将 Android Enterprise 公共应用商店应用程序部署给 Android 设备用户时，该用户将自动在 Android Enterprise 中注册。
   - 零接触注册允许您将设备配置为在首次开机时自动注册。请参阅零接触注册。

4. 配置设备和应用程序策略。

   在企业安全性与用户隐私和用户体验之间取得平衡。请参阅配置 Android Enterprise 设备和应用程序策略。

5. 分发 Apple 应用程序。

   使用托管 Google Play 可添加、购买和审批应用程序，以便部署到设备上的 Android Enterprise 工作区。用户只能安装您为其提供的托管 Google Play 中的应用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

请参阅：

- 分发 Android Enterprise 应用程序
- 托管配置策略
- 应用程序权限策略

6. 配置安全操作以监控和提供合规性。

   请参阅安全操作。

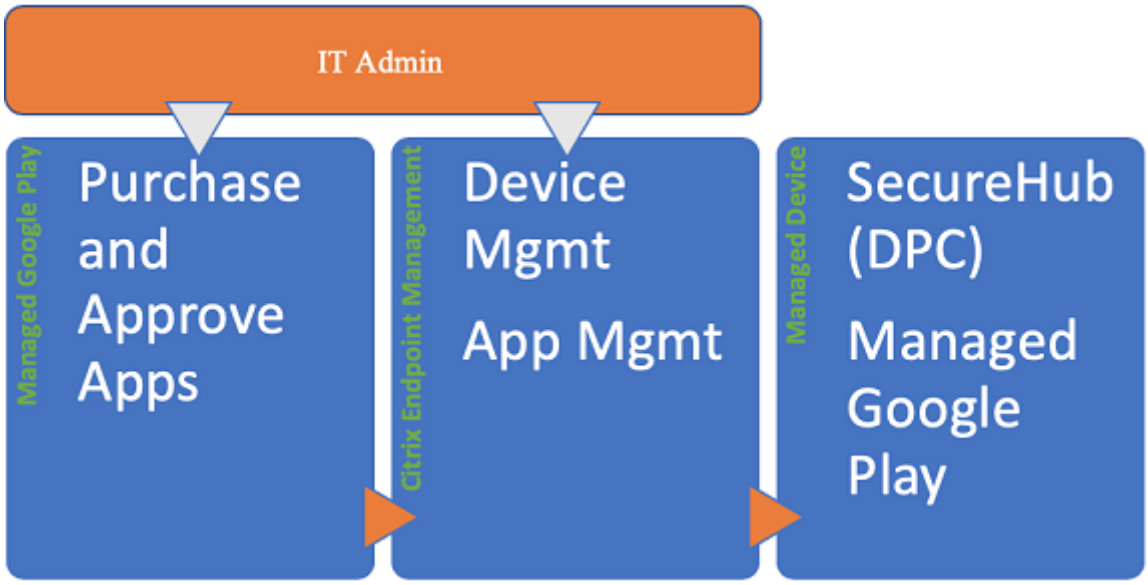
将托管 **Google Play** 与 **Endpoint Management** 结合使用

将 Endpoint Management 与托管 Google Play 相集成以使用 Android Enterprise 时，可以创建一个企业。Google 将企业定义为组织与企业移动管理 (EMM) 解决方案之间的绑定。组织通过您的解决方案管理的所有用户和设备都属于其企业。

适用于 Android Enterprise 的企业有三个组件：EMM 解决方案、设备策略控制器 (DPC) 应用程序和 Google 企业应用程序平台。当您将 Endpoint Management 与 Android Enterprise 相集成时，完整的解决方案包含以下组件：

- **Citrix Endpoint Management**： Citrix EMM。Endpoint Management 是用于安全数字工作区的统一端点管理。Endpoint Management 为 IT 管理员提供了为其组织管理设备和应用程序的方法。
- **Citrix Secure Hub**：Citrix DPC 应用程序。Secure Hub 是 Endpoint Management 的启动板。Secure Hub 在设备上强制执行策略。
- 托管 **Google Play**：与 Endpoint Management 集成的 Google 企业应用程序平台。Google Play EMM API 设置应用程序策略并分发应用程序。

下图显示了管理员如何与这些组件进行交互，以及组件之间如何交互：



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 可以使用托管 Google Play 或 Google Workspace（以前称为 G Suite）将 Citrix 注册为您的 EMM 提供商。本文讨论了使用 Android Enterprise 与托管 Google Play。如果贵组织使用 Google Workspace 提供对应用程序的访问权限，您可以将其用于 Android Enterprise。请参阅适用于 Google Workspace 客户的旧版 Android Enterprise。

使用托管 Google Play 时，请为设备和最终用户预配托管 Google Play 帐户。托管 Google Play 帐户提供对托管 Google play 的访问，以允许用户安装和使用您提供的应用程序。如果贵组织使用第三方身份服务，您可以将托管 Google Play 帐户与您的现有身份帐户链接。

由于这种类型的企业未绑定到域，因此，您可以为单个组织创建多个企业。例如，组织中的每个部门或区域都可以注册为不同的企业。使用不同的企业可以管理单独的设备和应用程序的集合。

对于 Endpoint Management 管理员，托管 Google Play 将 Google Play 的用户体验和应用商店功能与一组专为企业设计的管理功能相结合。使用托管 Google Play 可添加、购买和审批应用程序，以便部署到设备上的 Android Enterprise 工作区。可以使用 Google Play 部署您的公共应用程序、专用应用程序和第三方应用程序。

对于托管设备的用户，托管 Google Play 是企业应用商店。用户可以浏览应用程序、查看应用程序详细信息以及安装这些应用程序。与 Google Play 的公共版本不同，用户只能从您为其提供的托管 Google Play 安装应用程序。

设备部署方案和配置文件

设备部署方案是指谁拥有您所部署的设备以及如何管理这些设备。设备配置文件是指 DPC 如何在设备上管理和强制执行策略。

工作配置文件将企业帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。工作配置文件和个人配置文件在操作系统级别分隔。有关工作配置文件的更多详细信息，请参阅 什么是工作配置文件。

> 重要：
>
> 当 Android Enterprise 设备更新到 Android 11 时，Google 将作为“使用工作配置文件的完全托管”进行托管的设备迁移到新的安全性增强的工作配置文件体验。新注册模式称为”企业拥有的设备上的工作配置文件“。有关详细信息，请参阅使用工作配置文件进行完全托管的 Android Enterprise 的未来更改。
> 有关 Android 12 设备的信息，请参阅工作配置文件的安全性和隐私增强功能。

设备管理	用例	工作配置文件	个人资料	备注
公司拥有的设备（完全托管）	仅供工作使用的公司拥有的设备	否	否	仅适用于新设备或恢复出厂设置的设备。请参阅预配 Android Enterprise 完全托管设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备管理	用例	工作配置文件	个人资料	备注
具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备	供工作和个人使用的公司拥有的设备	是	是。两个 DPC 副本在这些设备上运行：一个在设备所有者模式下管理设备，另一个在配置文件所有者模式下管理工作配置文件。您可以将单独的策略应用到设备和工作配置文件。	请参阅预配具有工作配置文件或企业拥有的设备上的工作配置文件的 Android Enterprise 完全托管设备。
专用设备 *	为单个用例配置的公司拥有的设备，例如数字标牌或票证打印	否	否	请参阅预配专用 Android Enterprise 设备。
BYOD 工作配置文件 **	通过工作配置文件管理注册的个人设备（又称为配置文件所有者模式）	是	是。DPC 仅管理工作配置文件，不管理整个设备。	这些设备不需要是新设备或恢复出厂设置的设备。请参阅预配 Android Enterprise 工作配置文件设备。

* 用户可以共享专用设备。当用户登录到专用设备上的应用程序时，其工作状态与应用程序一致，而非与设备一致。

** Endpoint Management 不像在 BYOD 工作配置文件模式下一样支持 Zebra 设备。Endpoint Management 支持 Zebra 设备作为使用 Android Enterprise 的完全托管设备。

注册安全性

注册配置文件确定 Android 设备在 MAM、MDM 还是 MDM+MAM 中注册，并提供供用户选择退出 MDM 的选项。

有关指定安全级别和所需注册步骤的信息，请参阅用户帐户、角色和注册。

Endpoint Management 支持对在 MDM 或 MDM+MAM 中注册的 Android 设备使用以下身份验证方法。有关信息，请参阅以下文章：

- 域或域加安全令牌身份验证
- 客户端证书或证书加域身份验证
- 身份提供程序：
  - 通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证（预览版）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 通过 Citrix Cloud 使用 Okta 进行身份验证（预览版）

一种罕见的身份验证方法是客户端证书加安全令牌。有关信息，请参阅 https://support.citrix.com/article/CTX215200。

要求

在开始使用 Android Enterprise 之前，您需要：

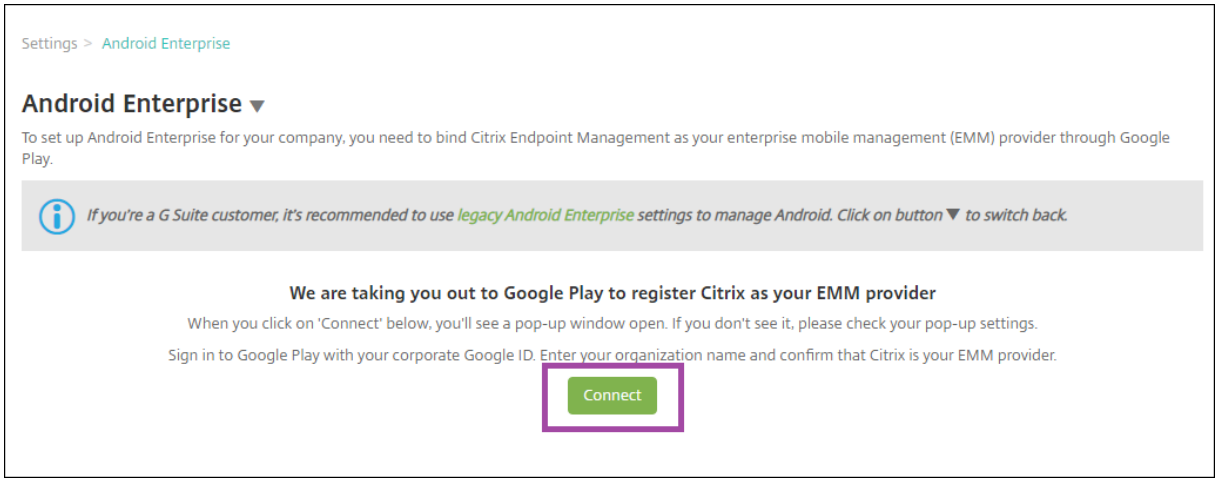
- 帐户和凭据：
  - 要通过托管 Google Play 设置 Android Enterprise，则需要企业 Google 帐户
  - 要下载最新的 MDX 文件，则需要 Citrix 客户帐户
- Firebase Cloud Messaging (FCM) 和为 Endpoint Management 配置的连接计划设备策略。请参阅 Firebase Cloud Messaging 和连接计划设备策略。

将 **Endpoint Management** 连接到 **Google Play**

要为贵组织设置 Android Enterprise，请通过托管 Google Play 将 Citrix 注册为 EMM 提供商。该设置将托管 Google Play 连接到 Endpoint Management，并在 Endpoint Management 中为 Android Enterprise 创建一个企业。

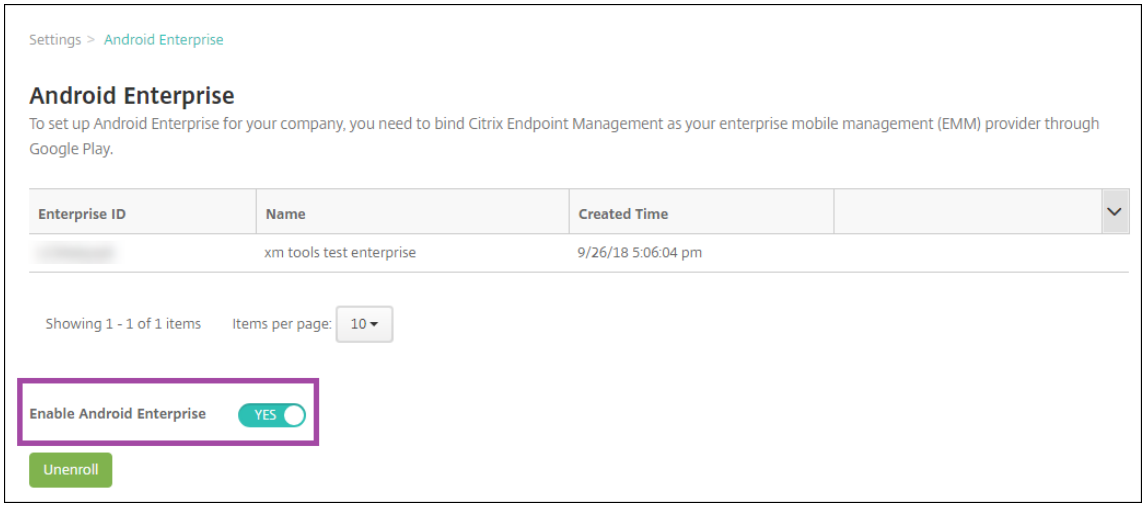
您需要一个企业 Google 帐户才能登录 Google Play。

1. 在 Endpoint Management 控制台中，转到设置 **> Android Enterprise**。
2. 单击连接。Google Play 将打开。

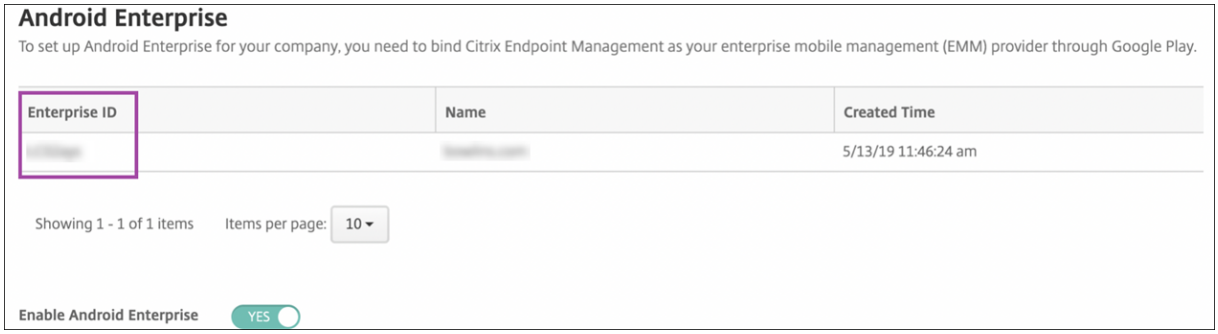


1. 使用您的企业 Google 帐户凭据登录 Google Play。输入贵组织的名称并确认 Citrix 是您的 EMM 提供商。
2. 将为 Android Enterprise 添加企业 ID。要启用 Android Enterprise，请将启用 **Android Enterprise** 滑动到是。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



您的企业 ID 将显示在 Endpoint Management 控制台中。



您的环境已连接到 Google，可以管理设备。您现在可以为用户提供应用程序。

Endpoint Management 可以为用户提供 Citrix 移动生产力应用程序、MDX 应用程序、公共应用商店应用程序、Web 和 SaaS 应用程序、企业应用程序和 Web 链接。有关向用户提供这些类型的应用程序的更多信息，请参阅 分发 Android Enterprise 应用程序。

下面的部分介绍了如何提供移动生产力应用程序。

向 **Android Enterprise** 用户提供 **Citrix** 移动生产力应用程序

向 Android Enterprise 用户提供 Citrix 移动生产力应用程序需要以下步骤。

1. 将应用程序发布为 MDX 应用程序。请参阅将应用程序配置为 MDX 应用程序。
2. 为用户用于访问其设备上的工作配置文件的安全质询配置规则。请参阅配置安全质询策略。

您发布的应用程序可用于在 Android Enterprise 企业中注册的设备。

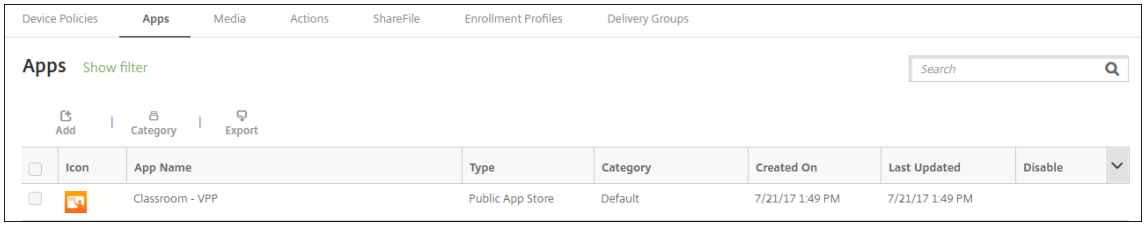
> 注意：
>
> 将 Android Enterprise 公共应用商店应用程序部署给 Android 用户时，该用户将自动在 Android Enterprise 中注册。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

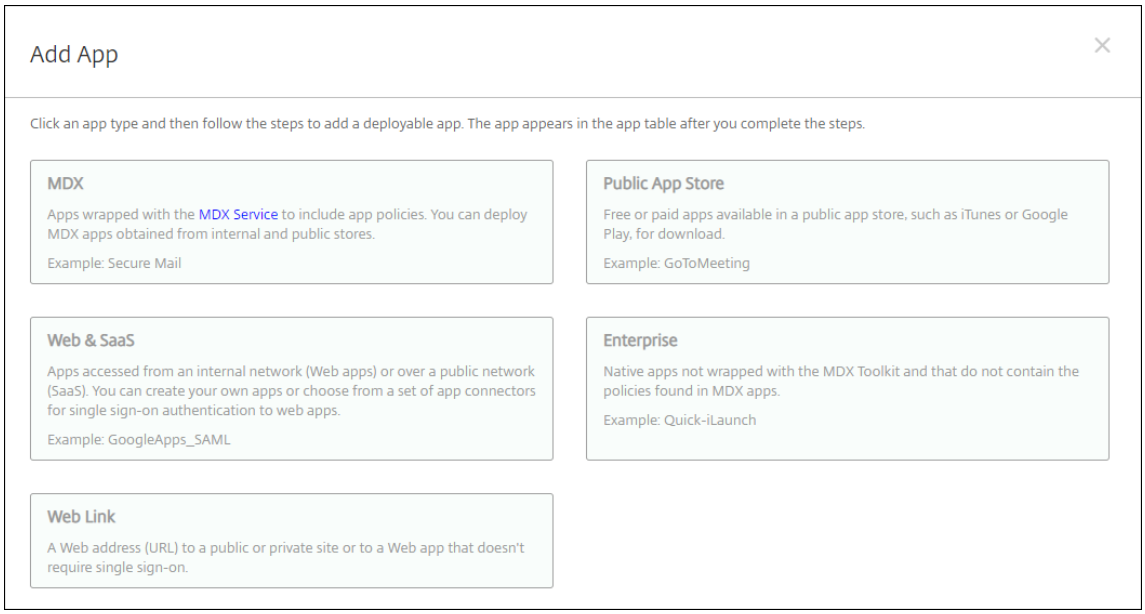
将应用程序配置为 **MDX** 应用程序

要将 Citrix 生产力应用程序配置为适用于 Android Enterprise 的 MDX 应用程序，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序。此时将显示应用程序页面。

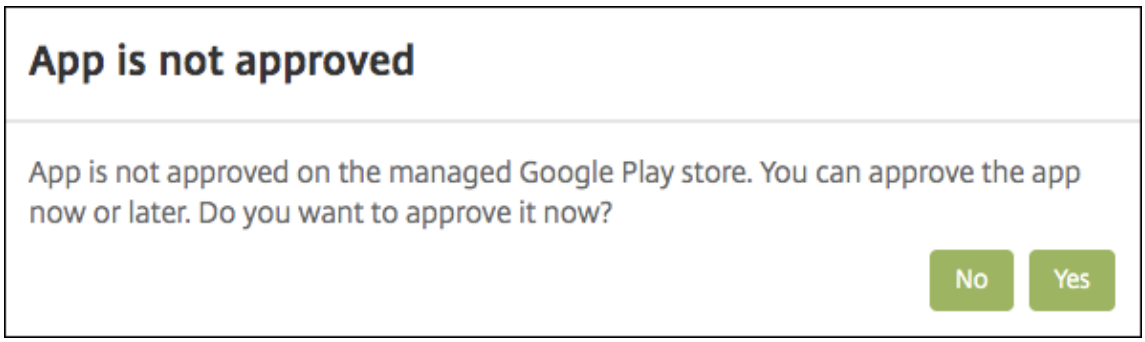


2. 单击添加。此时将显示添加应用程序对话框。

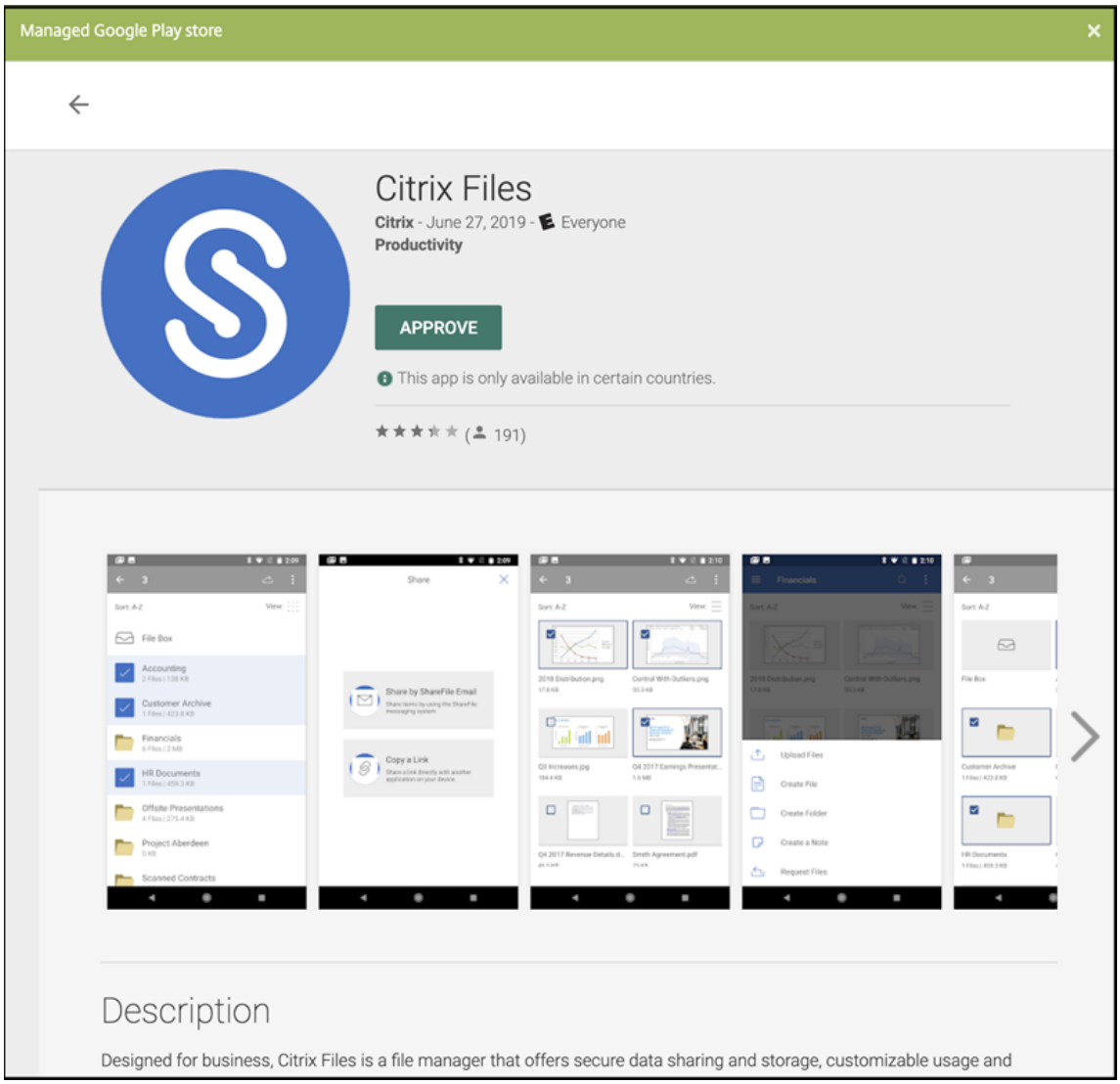


3. 单击 **MDX**。此时将显示应用程序信息页面。
4. 在页面左侧，选择 **Android Enterprise** 作为平台。
5. 在应用程序信息页面中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在应用程序表中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
6. 单击下一步。此时将显示 **Android Enterprise MDX** 应用程序页面。
7. 单击上载并导航到应用程序的.mdx 文件的文件位置。选择该文件，然后单击打开。
8. UI 会通知您附加的应用程序是否需要从托管 Google Play 应用商店获得批准。要在不离开 Citrix Endpoint Management 控制台的情况下审批应用程序，请单击是。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

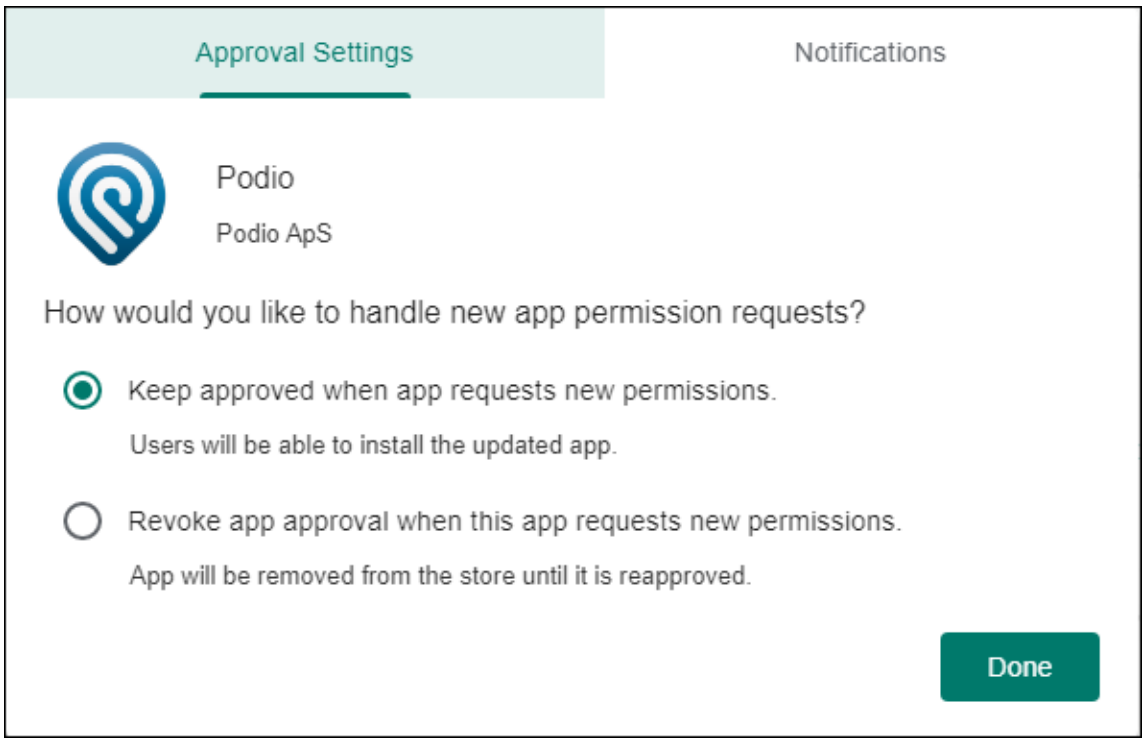


9. 当托管 Google Play 应用商店页面打开时，单击批准。



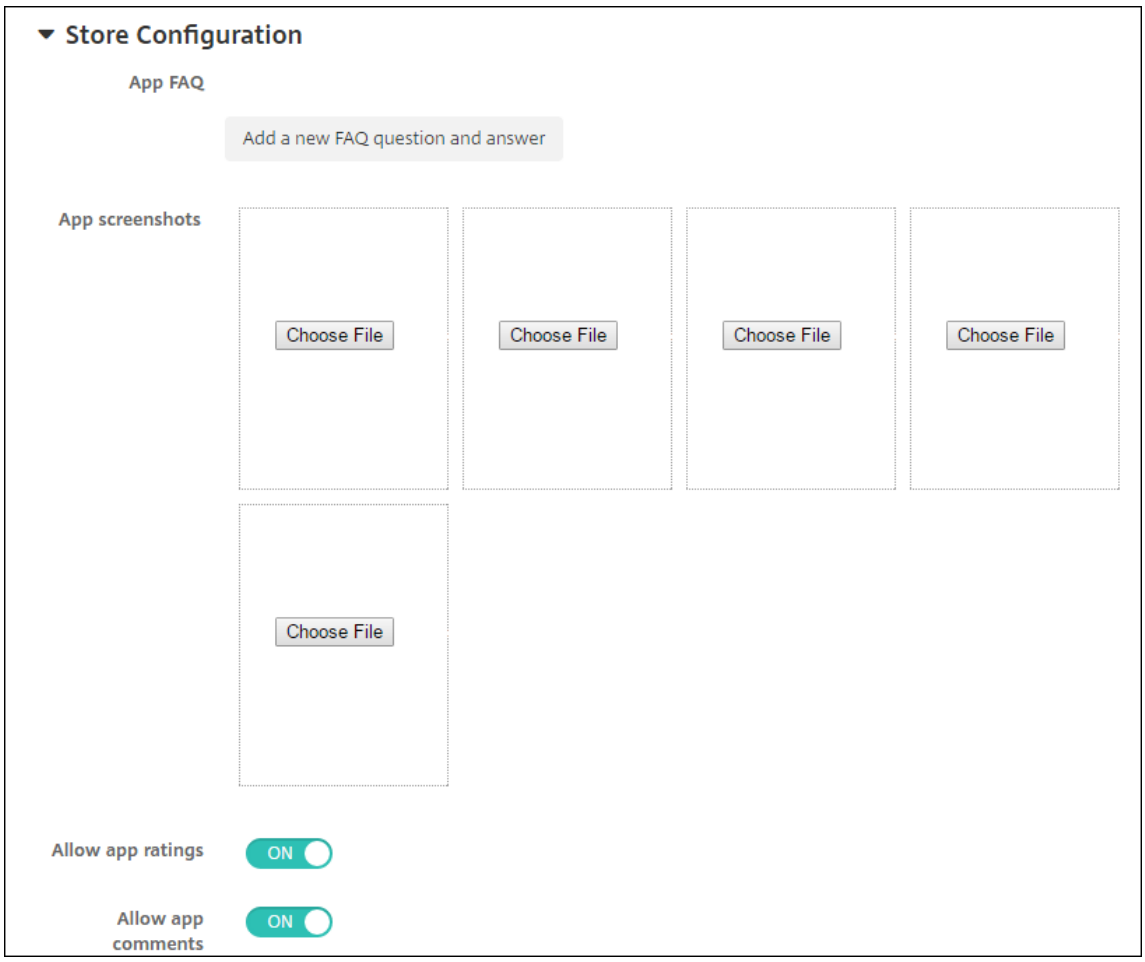
10. 再次单击 **Approve**（批准）。
11. 选择 **Keep approved when app requests new permissions**（在应用程序请求新权限时保持已批准）。单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



12. 当应用程序获得批准并保存后，页面上会显示更多设置。配置以下设置：
    - 文件名：键入与应用程序关联的文件名。
    - 应用程序说明：键入应用程序的说明。
    - 产品轨迹：指定要推送到用户设备的产品轨迹。如果您有一个专为测试而设计的轨迹，则可以选择并将其分配给您的用户。默认值为生产。
    - 应用程序版本：（可选）键入应用程序版本号。
    - 软件包 **ID**： Google Play 应用商店中的应用程序的 URL。
    - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
    - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
    - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
13. 配置 **MDX** 策略。有关 MDX 应用程序的应用程序策略的详细信息，请参阅 MDX 策略概览和 MAM SDK 概览。
14. 配置部署规则。有关信息，请参阅部署资源。
15. 展开应用商店配置。此设置不适用于仅出现在托管 Google Play 中的 Android Enterprise 应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



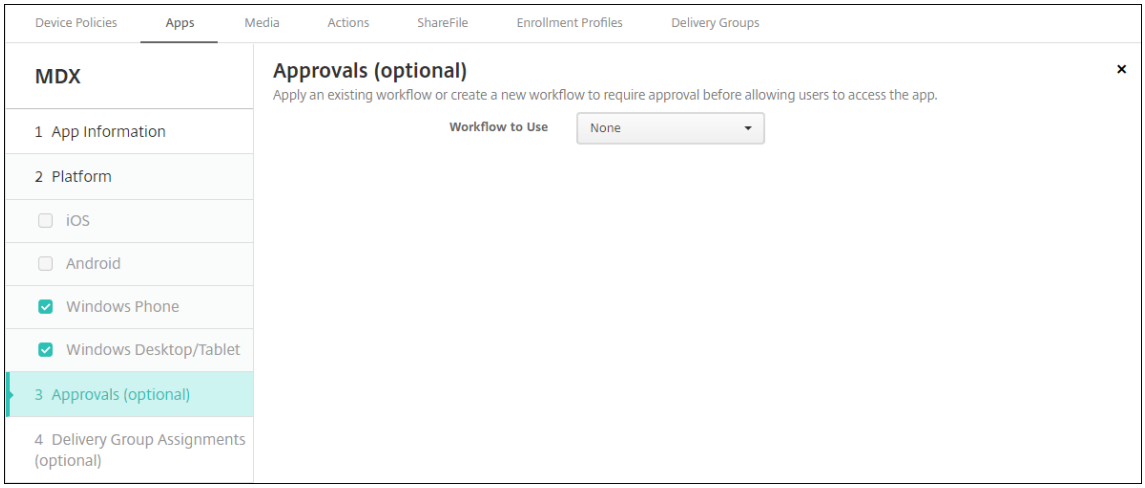
（可选）可以添加应用程序的常见问题解答或显示在应用商店中的屏幕截图。还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - 应用程序常见问题解答：添加应用程序的常见问题和答案。
  - 应用程序屏幕截图：添加屏幕截图以帮助在应用商店中对应用程序进行分类。上载的图形必须为 PNG 格式。您无法上传 GIF 或 JPEG 图像。
  - 允许应用程序评级：选择是否允许用户对应用程序进行评级。默认为“开”。

    允许应用程序评论：选择是否允许用户对所选应用程序发表评论。默认为“开”。

16. 单击下一步。此时将显示审批页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



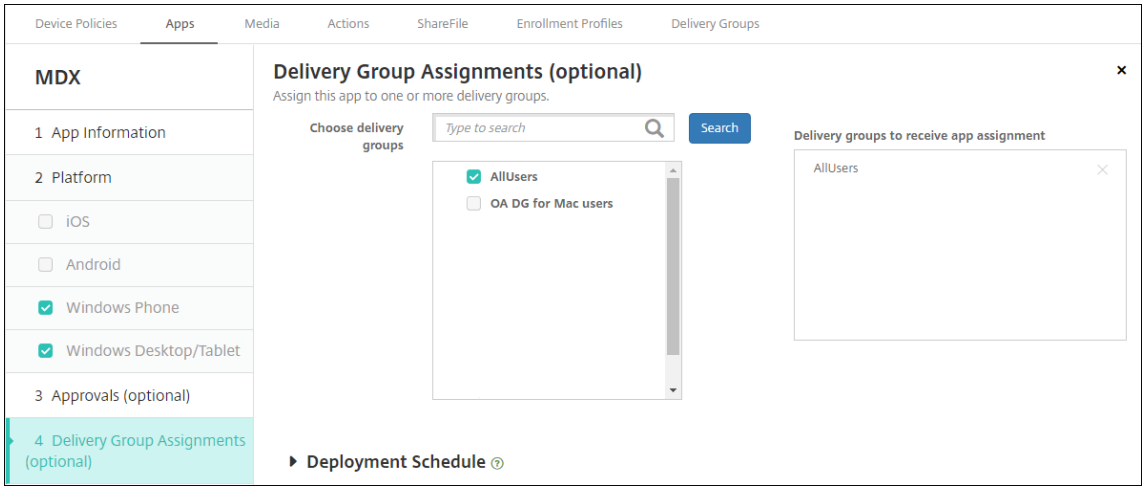
创建用户帐户时如果需要审批则使用工作流。如果不想设置审批工作流，可以跳至步骤 15。

要指定或创建工作流，请配置以下设置：

- 要使用的工作流：在此列表中，单击现有工作流或单击创建新工作流。默认值为无。
- 如果选择创建新工作流，请配置以下设置。有关详细信息，请参阅创建和管理工作流。
- 名称：键入工作流的唯一名称。
- 说明：（可选）键入工作流的说明。
- 电子邮件审批模板：在列表中，选择要指定的电子邮件审批模板。单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
- 经理审批级别：在列表中，选择此工作流所需的经理审批级别数。默认值为 1 级。可能的选项包括：
  - 不需要
  - 1 级
  - 2 级
  - 3 级
- 选择 **Active Directory** 域：在列表中，选择用于工作流的合适 Active Directory 域。
- 查找所需的其他审批者：在搜索字段中键入其他所需人员的姓名，然后单击搜索。名称源于 Active Directory。
- 姓名显示在此字段中后，选中姓名旁边的复选框。姓名和电子邮件地址显示在选定的其他所需审批者列表中。
  - 要从选定的其他所需审批者列表中删除人员，请执行以下操作之一：
    * 单击搜索以查找选定域中的所有人员列表。
    * 在搜索框中键入完整姓名或部分姓名，然后单击搜索以限制搜索结果。
    * 在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。滚动列表，并取消选中要删除的各个姓名旁边的复选框。

17. 单击下一步。此时将显示交付组分配页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



18. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。
19. 展开部署计划，然后配置以下设置：
    - 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。
    - 在“部署计划”旁边，单击立即或稍后。默认选项为立即。
    - 如果单击以后，请单击日历图标，然后选择部署的日期和时间。
    - 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
    - 在“部署以实现始终开启的连接”旁边，确保选中“关闭”。默认选项为关。对于在 10.18.19 或更高版本中开始使用 Endpoint Management 的客户，Android Enterprise 无法使用永远在线的连接。我们不建议开始使用 10.18.19 版之前的 Endpoint Management 的客户使用这些连接。

      当您在“设置”>“服务器属性”中配置了计划后台部署密钥时，此选项适用。

      配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。
20. 单击保存。

为每个移动生产力应用程序重复上述步骤。

配置安全质询策略

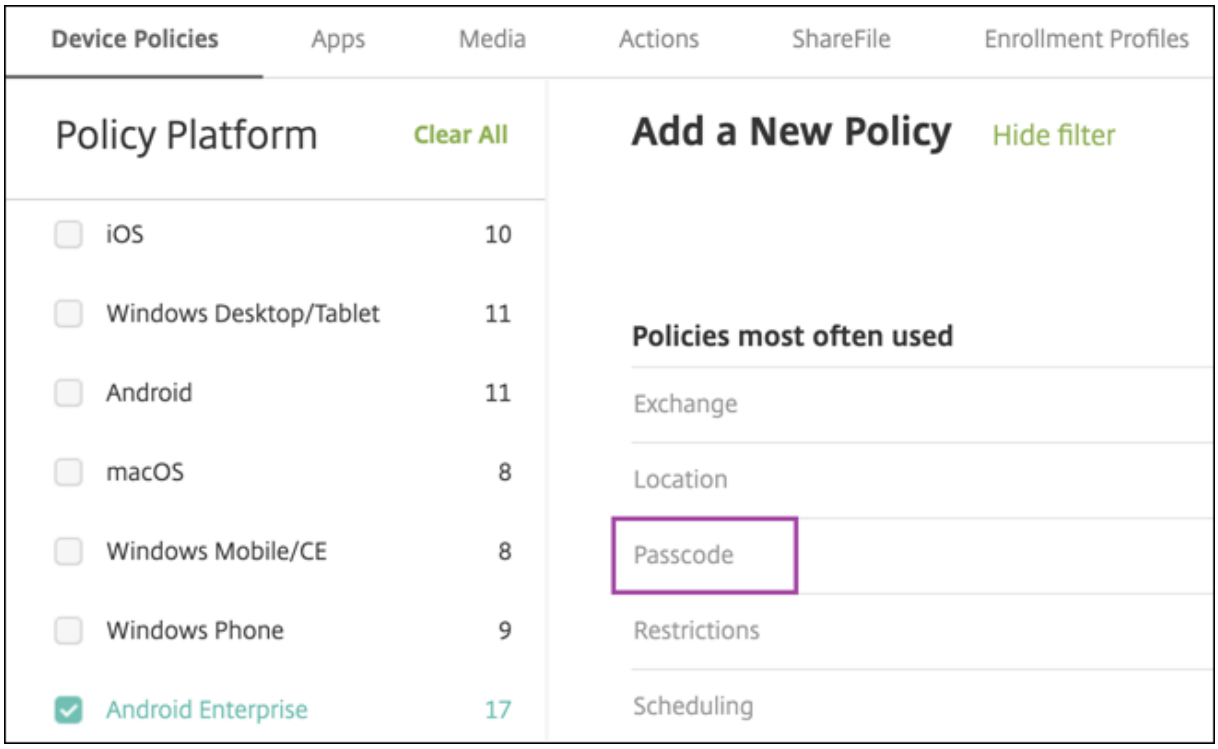
Endpoint Management 通行码设备策略将配置安全质询规则。当用户访问其设备或其设备上的 Android Enterprise 工作配置文件时，会出现这些质询。安全质询可能是通行码或生物特征识别。有关通行码策略的详细信息，请参阅通行码设备策略。

- 如果您的 Android Enterprise 部署包含 BYOD 设备，请为工作配置文件配置通行码策略。
- 如果您的部署包括公司拥有的完全托管设备，请为设备本身配置通行码策略。
- 如果您的部署包括两种类型的设备，请配置两种类型的通行码策略。

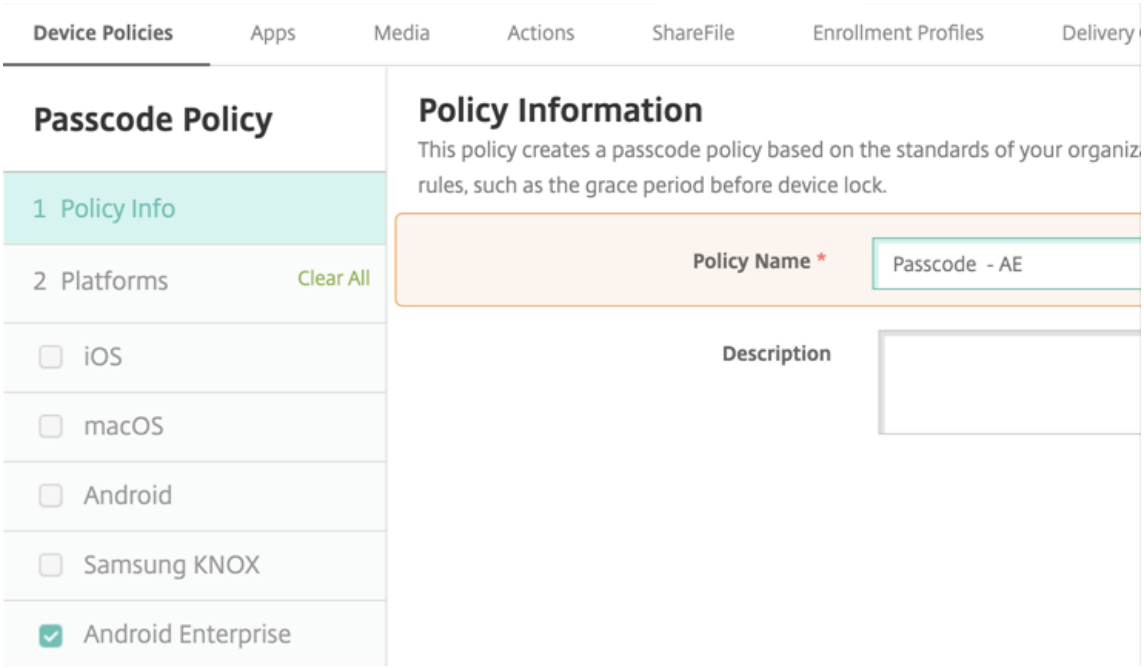
要配置通行码策略，请执行以下操作：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在 Endpoint Management 控制台中，单击配置 **>** 设备策略。
2. 单击添加。
3. 单击显示过滤器以显示策略平台窗格。在策略平台窗格中，选择 **Android Enterprise**。
4. 单击右侧窗格上的通行码。



1. 输入策略名称。单击下一步。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 配置通行码策略设置。
    - 将需要设备通行码设置为开，以查看设备本身的安全质询可用的设置。
    - 将工作配置文件安全质询设置为开，以查看可用于工作配置文件安全质询的设置。
3. 单击下一步。
4. 将策略分配给一个或多个交付组。
5. 单击保存。

创建注册配置文件

如果为 Endpoint Management 部署启用了 Android Enterprise，注册配置文件可以控制 Android 设备的注册方式。创建注册配置文件以注册 Android Enterprise 设备时，可以配置注册配置文件以将新设备和重置为出厂设置的设备注册为：

- 完全托管设备
- 专用设备
- 具有工作配置文件的完全托管设备/企业拥有的设备上的工作配置文件

还可以配置其中每个 Android Enterprise 注册配置文件以将 BYOD Android 设备注册为工作配置文件设备。

如果为您的 Endpoint Management 部署启用了 Android Enterprise，则所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。默认情况下，全局注册配置文件会将新的和恢复出厂设置的 Android 设备注册为完全托管设备，并将 BYOD Android 设备注册为企业拥有的设备上的工作配置文件。

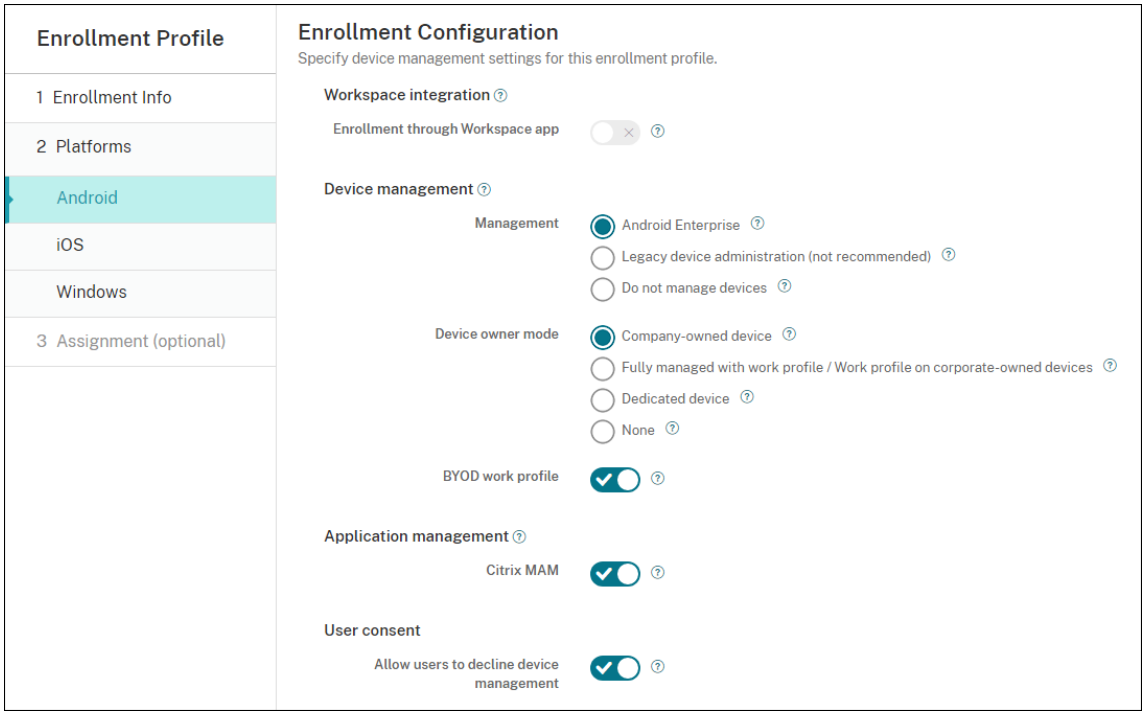
创建注册配置文件时，需要为其分配交付组。如果用户属于具有不同注册配置文件的多个交付组，该交付组的名称决定使用的注册配置文件。Endpoint Management 选择按字母顺序排列的交付组列表中最后显示的交付组。有关详细信息，请参阅注册配置文件。

为完全托管设备添加注册配置文件

默认情况下，全局注册配置文件将注册完全托管设备，但您可以创建更多注册配置文件以注册完全托管设备。

1. 在 Endpoint Management 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置使用此配置文件的成员可以注册的设备数量。
4. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。
5. 将管理设置为 **Android Enterprise**。
6. 将设备所有者模式设置为公司拥有的设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



7. **BYOD** 工作配置文件允许您配置注册配置文件以将 BYOD 设备注册为工作配置文件设备。将新设备和重置为出厂设置的设备注册为完全托管设备。将 **BYOD** 工作配置文件设置为开，以允许将 BYOD 设备注册为工作配置文件设备。将 **BYOD** 工作配置文件设置为关，以限制对完全托管设备的注册。默认值为开。
8. 选择是否在 Citrix MAM 中注册设备。
9. 如果将 **BYOD** 工作配置文件设置为开，请配置用户同意书。要允许 BYOD 工作配置文件设备的用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。

   如果 **BYOD** 工作配置文件设置为开，则允许用户拒绝设备管理的默认值为开。如果 **BYOD** 工作配置文件设置为关，则禁用允许用户拒绝设备管理。
10. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
11. 请选择包含注册完全托管设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

    此时将显示“注册配置文件”页面，其中包含您添加的配置文件。

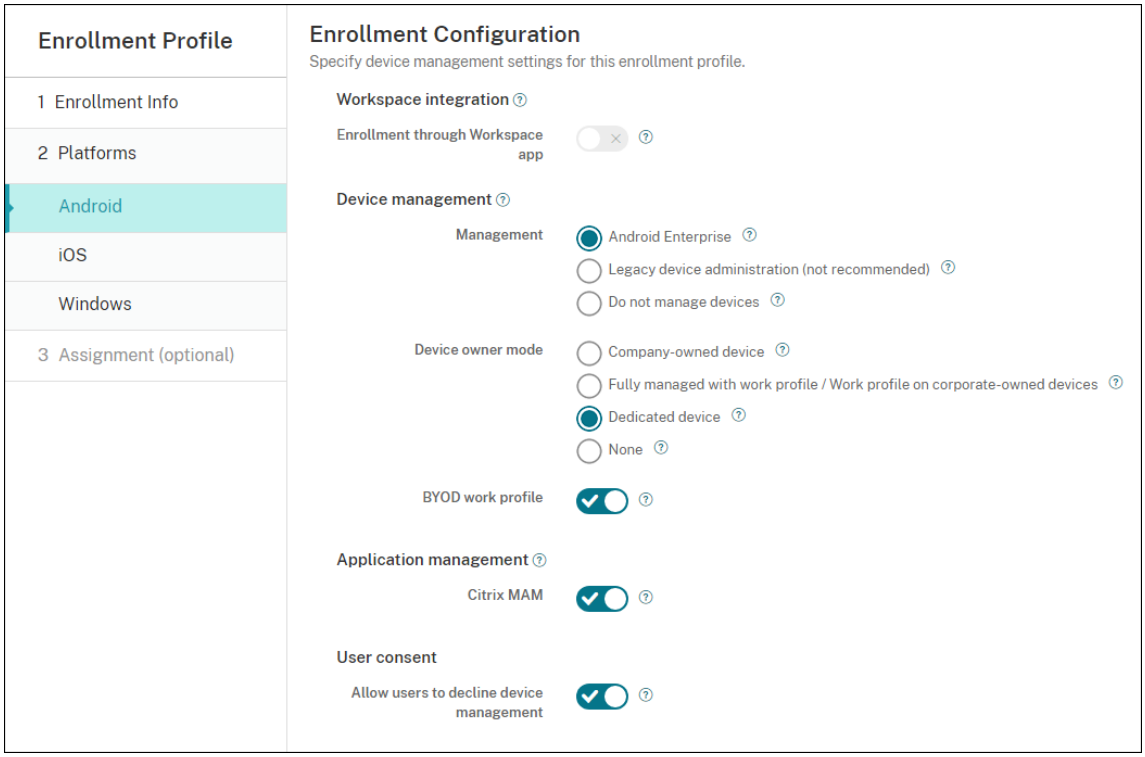
添加专用的注册配置文件

当 Endpoint Management 部署包括专用设备时，单个 Endpoint Management 管理员或一小组管理员会注册多个专用设备。为确保这些管理员可以注册所需的所有设备，请为他们创建注册配置文件，允许每个用户使用无限制的设备。

1. 在 Endpoint Management 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。设置为无限制（使用此配置文件的成员可以注册的设备数量）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。
4. 将管理设置为 **Android Enterprise**。
5. 将设备所有者模式设置为专用设备。



6. **BYOD** 工作配置文件允许您配置注册配置文件以将 BYOD 设备注册为工作配置文件设备。将新设备和重置为出厂设置的设备注册为专用设备。将 **BYOD** 工作配置文件设置为开，以允许将 BYOD 设备注册为工作配置文件设备。将 **BYOD** 工作配置文件设置为关，以限制对公司拥有的设备的注册。默认值为开。
7. 选择是否在 Citrix MAM 中注册设备。
8. 如果将 **BYOD** 工作配置文件设置为开，请配置用户同意书。要允许 BYOD 工作配置文件设备的用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。

   如果 **BYOD** 工作配置文件设置为开，则允许用户拒绝设备管理的默认值为开。如果 **BYOD** 工作配置文件设置为关，则禁用允许用户拒绝设备管理。
9. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
10. 请选择包含注册专用设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

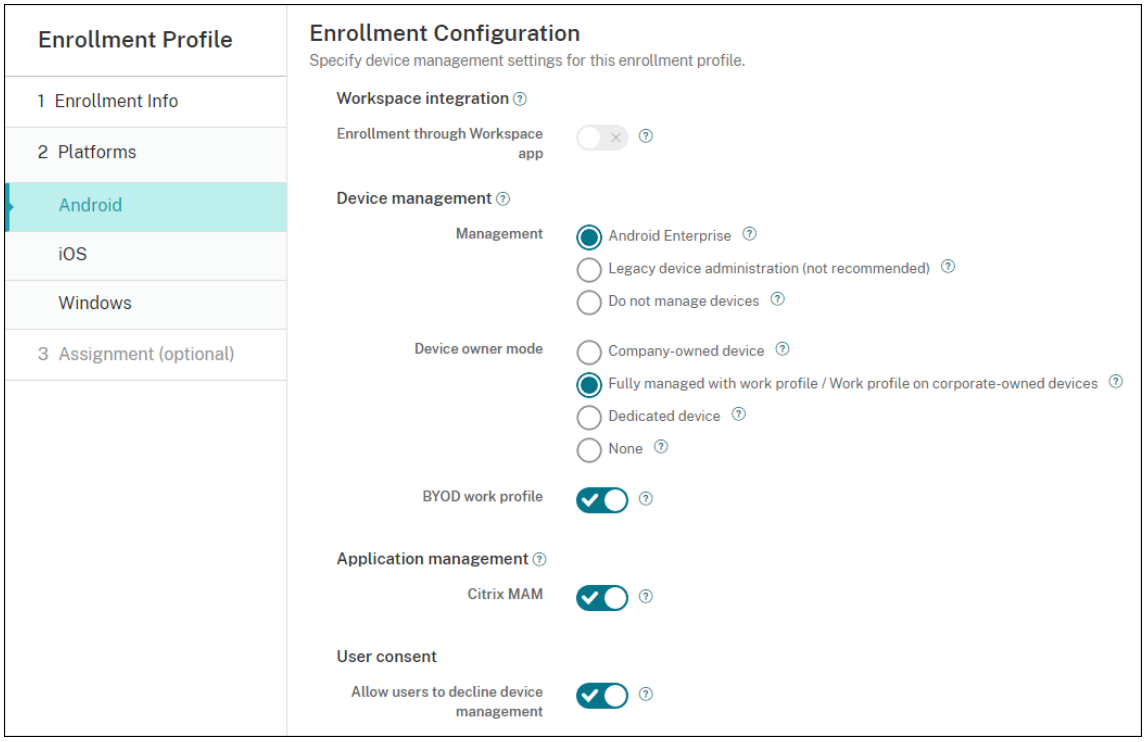
    此时将显示“注册配置文件”页面，其中包含您添加的配置文件。

为具有工作配置文件**/**企业拥有的设备上的工作配置文件的完全托管设备添加注册配置文件

1. 在 Endpoint Management 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 设置使用此配置文件的成员可以注册的设备数量。
4. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。
5. 将管理设置为 **Android Enterprise**。将设备所有者模式设置为具有个人配置文件/企业拥有的设备上的工作配置文件的完全托管。



6. **BYOD** 工作配置文件允许您配置注册配置文件以将 BYOD 设备注册为工作配置文件设备。新设备和重置为出厂设备的设备注册为使用工作配置文件的完全托管设备。将 **BYOD** 工作配置文件设置为开，以允许将 BYOD 设备注册为工作配置文件设备。将 **BYOD** 工作配置文件设置为关，以限制对专用设备的注册。默认设置为关。
7. 选择是否在 Citrix MAM 中注册设备。
8. 如果将 **BYOD** 工作配置文件设置为开，请配置用户同意书。要允许 BYOD 工作配置文件设备的用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。

   如果 **BYOD** 工作配置文件设置为开，则允许用户拒绝设备管理的默认值为开。如果 **BYOD** 工作配置文件设置为关，则禁用允许用户拒绝设备管理。
9. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
10. 请选择包含注册使用工作配置文件的完全托管设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

    此时将显示“注册配置文件”页面，其中包含您添加的配置文件。

为旧版设备添加注册配置文件

Google 弃用了设备管理的设备管理员模式。Google 鼓励客户在设备所有者模式或配置文件所有者模式下管理所有 Android 设备。【请参阅 Google Android Enterprise 开发人员指南中的 Device admin deprecation（设备管理

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

员弃用)。】

要支持此更改，请执行以下操作：

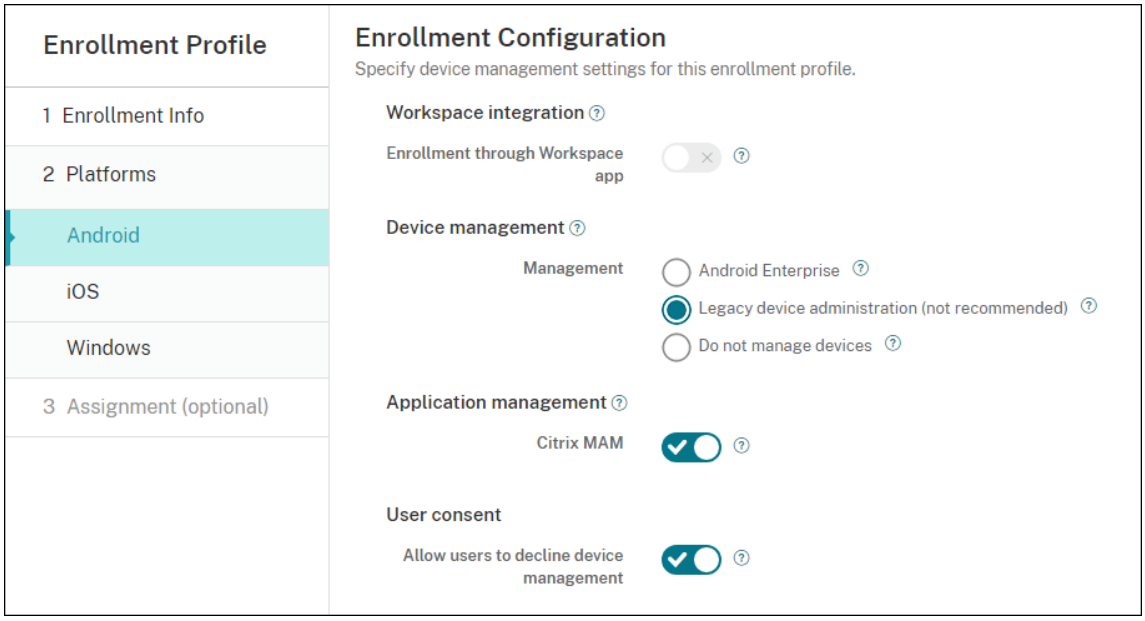
- Citrix 将 Android Enterprise 设置为 Android 设备的默认注册选项。
- 如果为您的 Endpoint Management 部署启用了 Android Enterprise，则所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。

贵组织可能尚未准备好开始使用 Android Enterprise 管理旧版 Android 设备。在这种情况下，您可以继续在设备管理员模式下进行管理。对于已在设备管理员模式下注册的设备，Endpoint Management 将继续以设备管理员模式管理这些设备。

为旧版设备创建注册配置文件，以允许新 Android 设备注册使用设备管理员模式。

要为旧版设备创建注册配置文件：

1. 在 Endpoint Management 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置使用此配置文件的成员可以注册的设备数量。
4. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。
5. 将管理设置为旧版设备管理 **(**不推荐**)**。单击下一步。



6. 选择是否在 Citrix MAM 中注册设备。
7. 要允许用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。默认值为开。
8. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
9. 请选择包含注册专用设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

此时将显示“注册配置文件”页面，其中包含您添加的配置文件。

要在设备管理员模式下继续管理旧版设备，请使用此配置文件注册或重新注册这些设备。通过让用户下载 Secure Hub 并提供注册服务器 URL，您可以注册与工作配置文件设备类似的设备管理员设备。

预配 **Android Enterprise** 工作配置文件设备

Android Enterprise 工作配置文件设备在配置文件所有者模式下注册。这些设备不需要是新设备或恢复出厂设置的设备。BYOD 设备作为工作配置文件设备注册。注册体验与 Endpoint Management 中的 Android 注册体验相似。用户将从 Google Play 下载 Secure Hub 并注册其设备。

默认情况下，当您在 Android Enterprise 中将设备注册为工作配置文件设备时，设备上的 **USB** 调试和未知来源设置将被禁用。

在 Android Enterprise 中将设备注册为工作配置文件设备时，将始终转至 Google Play。在该应用商店中，允许 Secure Hub 在用户的个人配置文件中显示。

预配 **Android Enterprise** 完全托管设备

可以在前面的部分中设置的部署中注册完全托管设备。完全托管设备是公司拥有的设备，在设备所有者模式下注册。在设备所有者模式下，只能注册新设备或恢复出厂设置的设备。

可以使用以下任何注册方法在设备所有者模式下注册设备：

- **DPC** 标识符令牌：如果使用此注册方法，用户在设置设备时将输入字符`afw##xenmobile`。`afw##xenmobile` 为 Citrix DPC 标识符令牌。此令牌将设备标识为由 Endpoint Management 托管并从 Google Play 应用商店下载 Secure Hub。请参阅使用 Citrix DPC 标识符令牌注册设备。
- 近场通信 **(NFC)** 碰撞： NFC 碰撞注册方法通过在两个设备之间使用近场通信来传输数据。蓝牙、Wi-Fi 和其他通信模式在新设备或恢复出厂设置的设备上处于禁用状态。NFC 是此状态下设备可以使用的唯一通信协议。请参阅通过 NFC 碰撞注册设备。
- **QR** 代码： QR 代码注册可用于注册不支持 NFC 的分布式设备队列（例如平板电脑）。QR 代码注册方法通过扫描设置向导中的 QR 代码来设置并配置设备配置文件模式。请参阅使用 QR 代码注册设备。
- 零接触：零接触注册允许您将设备配置为在首次开机时自动注册。某些运行 Android 9.0 或更高版本的 Android 设备支持零触摸注册。请参阅零接触注册。
- **Google** 帐号：用户输入自己的 Google 帐号凭据以开始配置流程。此选项适用于使用 Google Workspace 的企业。

使用 **Citrix DPC** 标识符令牌注册设备

用户在打开新设备或恢复出厂重置的设备以进行初始设置后输入 Google 帐户时输入 `afw##xenmobile`。此操作将下载并安装 Secure Hub。用户随后将按照 Secure Hub 设置提示进行操作，完成注册过程。

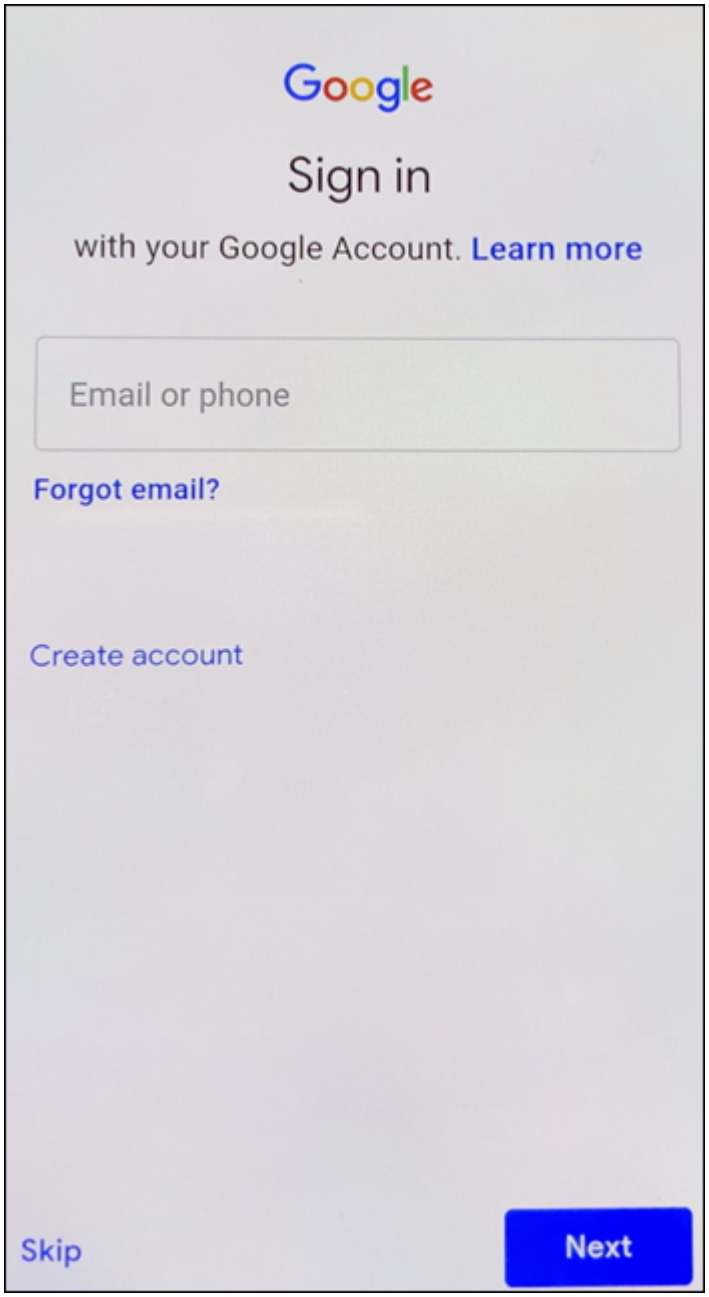
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

系统要求

- 在运行 Android OS 的所有 Android 设备上均受支持。

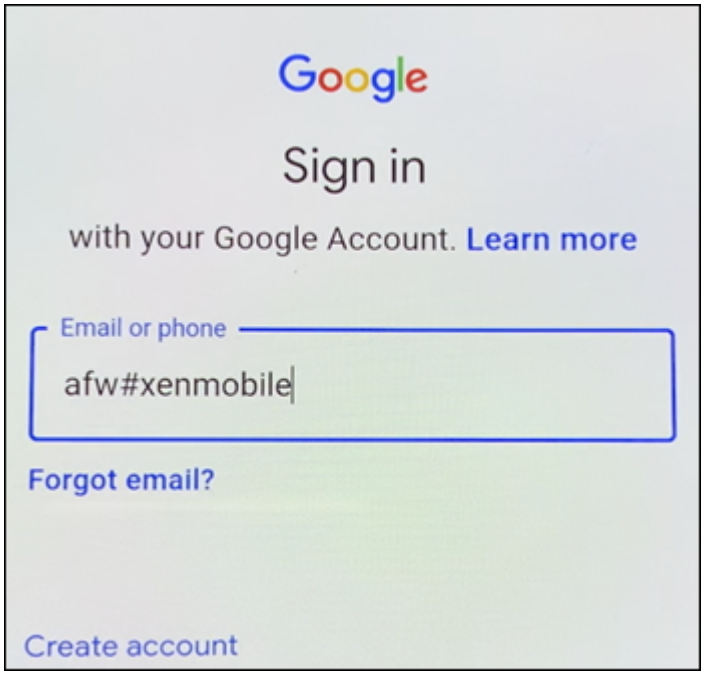
注册设备

1. 打开新设备或恢复出厂设置的设备的电源。
2. 初始设备设置加载并提示您输入 Google 帐户。如果设备加载设备的主屏幕，请检查通知栏中是否显示完成设置通知。



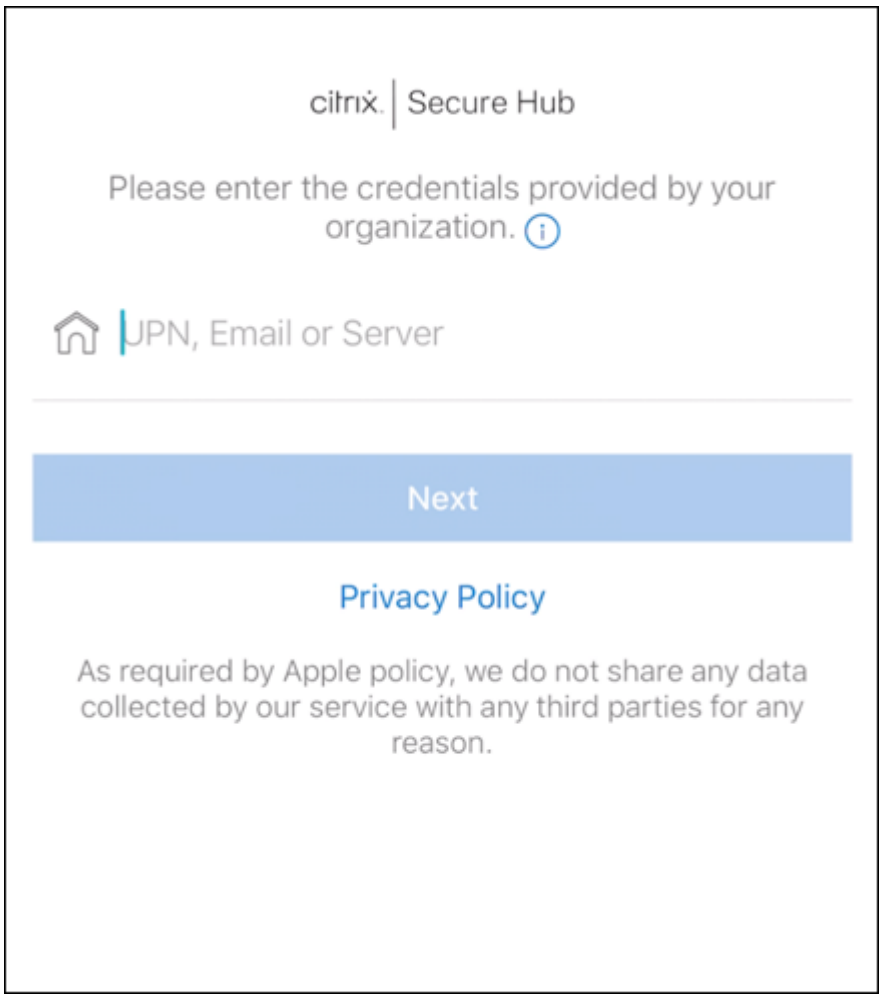
3. 在电子邮件或电话字段中输入 `afw##xenmobile`。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



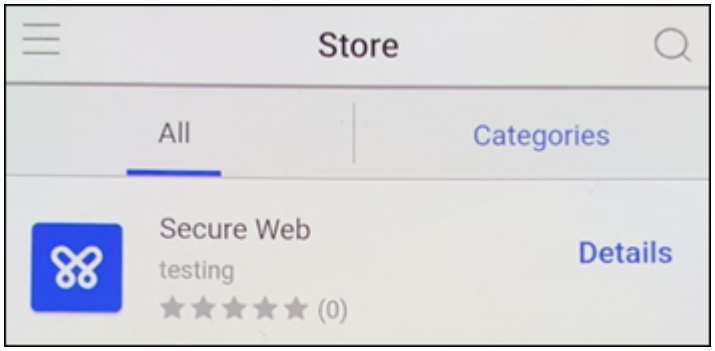
4. 在 Android Enterprise 屏幕上轻按安装，提示安装 Secure Hub。
5. 在 Secure Hub 安装程序屏幕上轻按安装。
6. 对所有应用程序权限申请轻按允许。
7. 轻按接受并继续以安装 Secure Hub 并允许其管理设备。
8. Secure Hub 现在已安装，并位于默认注册屏幕上。在此示例中，未设置自动发现。如果是，用户可以输入其用户名/电子邮件，并为其找到一个服务器。相反，请输入环境的注册 URL，然后轻按下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

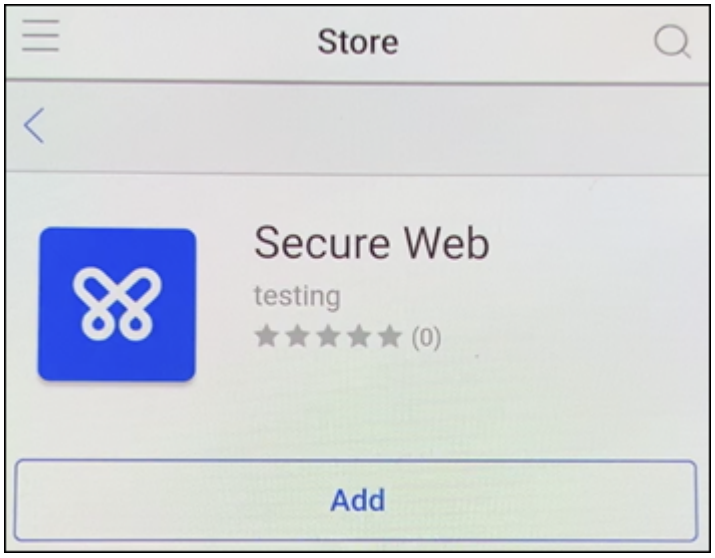


9. Endpoint Management 的默认配置允许用于选择其使用 MAM 还是 MDM+MAM。如果以这种方式提示，请轻按是，注册以选择 MDM+MAM。
10. 输入用户电子邮件地址和密码，然后轻按下一步。
11. 系统将提示用户配置设备通行码。轻按设置并输入通行码。
12. 系统会提示用户配置工作配置文件解锁方法。在此示例中，轻按密码，轻按 **PIN**，然后输入 PIN。
13. 设备现在位于 Secure Hub 我的应用程序登录屏幕上。轻按从应用商店中添加应用程序。
14. 要添加 Secure Web，请轻按 **Secure Web**。

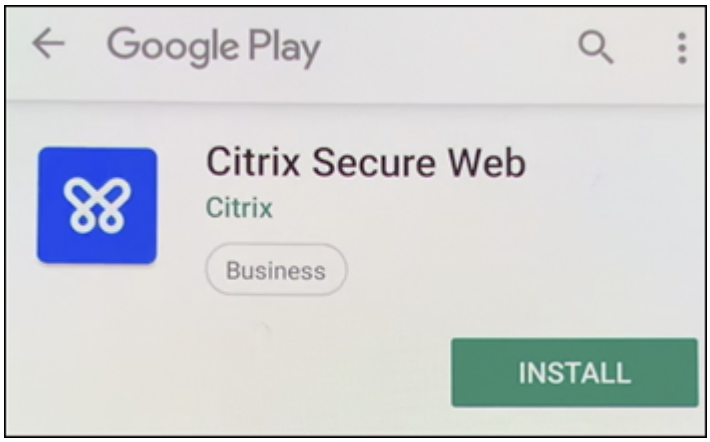
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



15. 轻按添加。

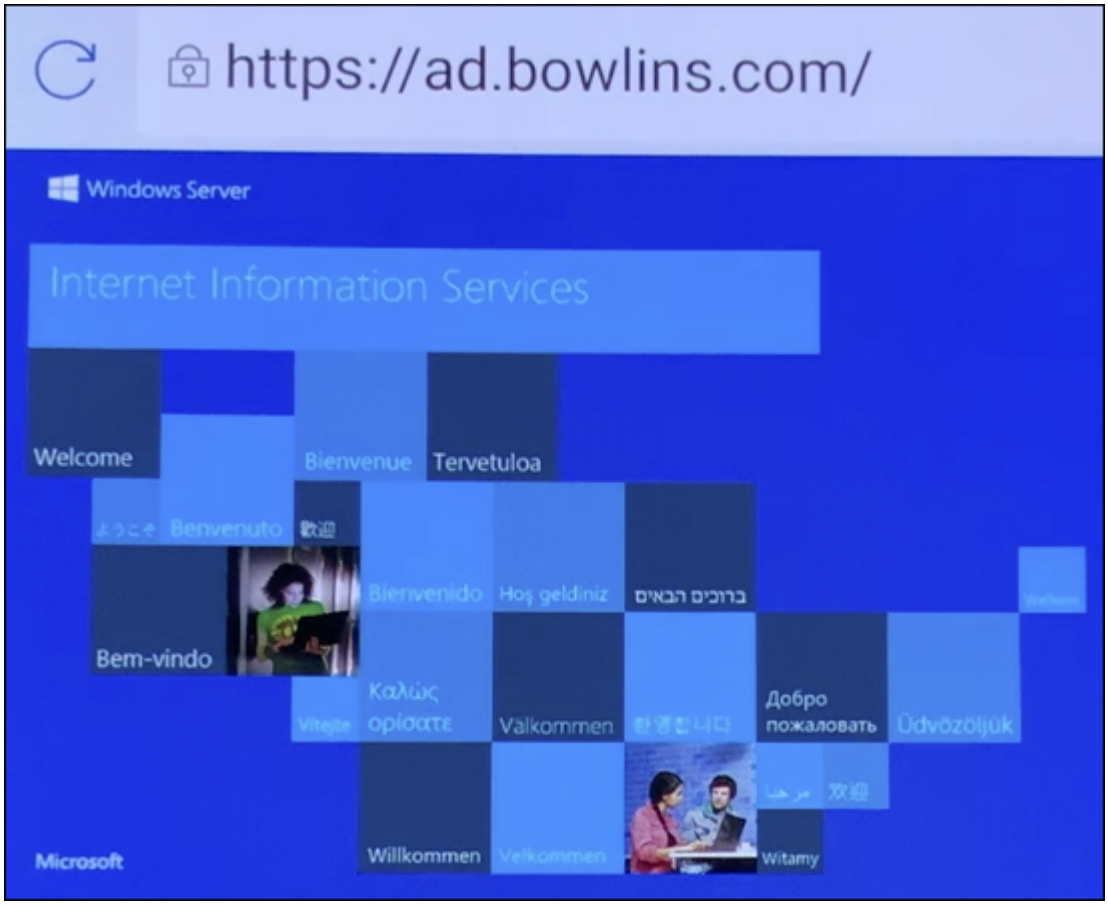


16. Secure Hub 引导用户访问 Google Play 应用商店以安装 Secure Web。轻按安装。



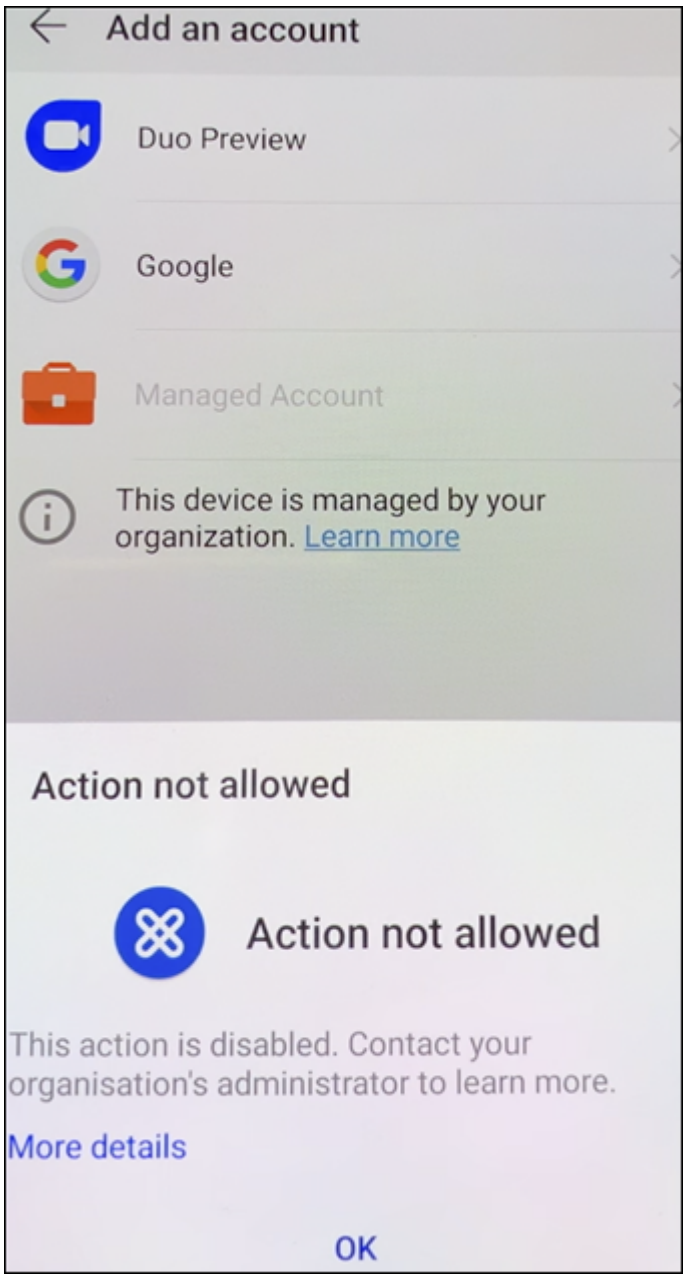
17. 安装 Secure Web 后，轻按打开。在地址栏中输入来自内部站点的 URL，并验证页面是否加载。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



18. 转到设备上的设置 **>** 帐户。注意无法修改托管帐户。用于共享屏幕或远程调试的开发人员选项也被阻止。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



通过 **NFC** 碰撞注册设备

要使用 NFC 碰撞功能将设备注册为完全托管设备，需要两个设备：一个已恢复出厂设置的设备，以及一个运行 Endpoint Management Provisioning Tool 的设备。

系统要求和必备条件

- 支持的 Android 设备。
- 具有 NFC 功能的新设备或恢复出厂设置的设备，作为完全托管设备配置为 Android Enterprise。请参阅预配 Android Enterprise 完全托管设备中的相应部分。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 另一台具有 NFC 功能、运行配置的 Provisioning Tool 的设备。Provisioning Tool 在 Secure Hub 或 Citrix 下载页面上提供。

每台设备只能有一个 Android Enterprise 配置文件。在这种情况下，配置文件适用于托管 Secure Hub。尝试添加第二个 DPC 应用程序会删除已安装的 Secure Hub。

通过 **NFC** 碰撞传输数据

预配恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以初始化 Android Enterprise：

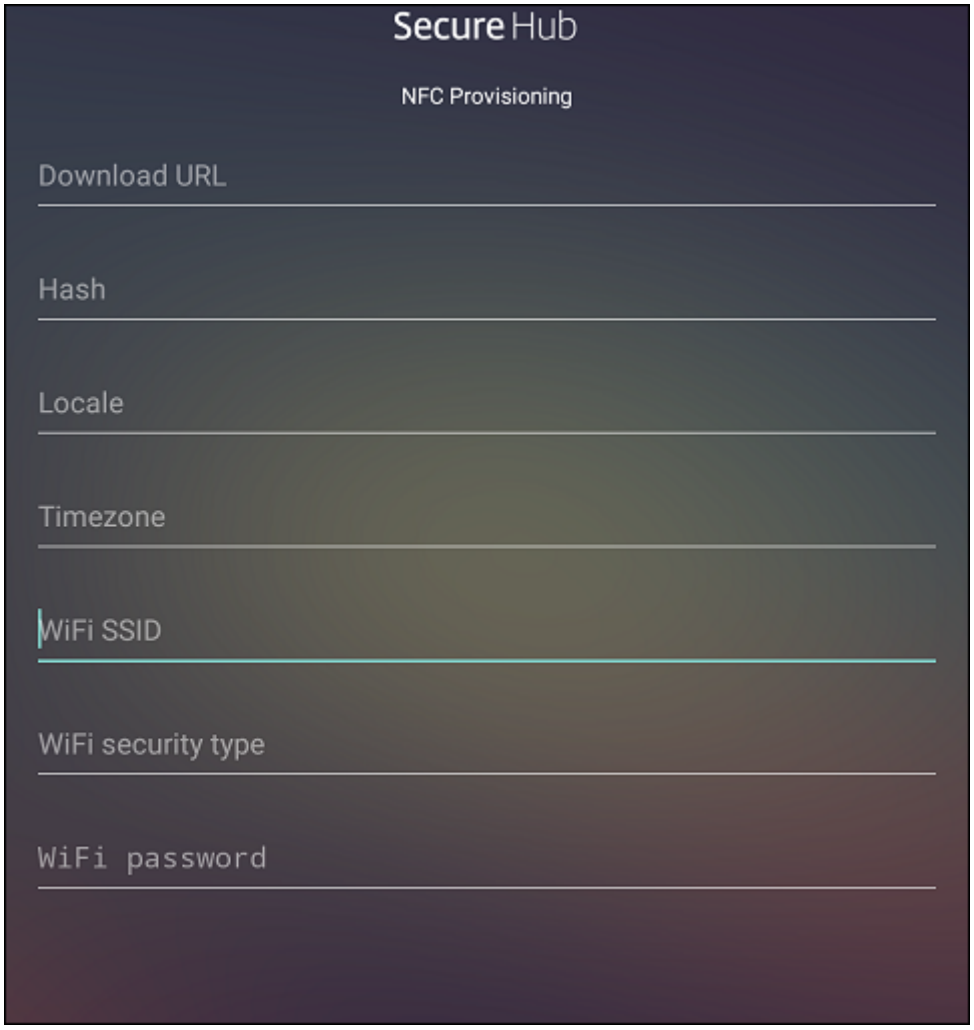
- 要作为设备所有者（在此示例中为 Secure Hub）的 DPC 应用程序的包名称。
- 设备可以从中下载 DPC 应用程序的 Intranet/Internet 位置。
- 用于验证下载是否成功的 DPC 应用程序的 SHA-256 哈希。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备能够连接和下载 DPC 应用程序。注意：Android 现在不支持在此步骤中使用 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

碰撞两个设备时，来自 Provisioning Tool 的数据将发送到恢复出厂设置的设备。该数据随后用于下载使用管理员设置的 Secure Hub。如果未输入时区和位置值，Android 将在新设备上自动配置值。

配置 **Endpoint Management Provisioning Tool**

执行 NFC 碰撞之前，必须配置 Provisioning Tool。此配置随后在 NFC 碰撞过程中被传输到恢复出厂设置的设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



可以将数据键入到必填字段中，或者使用文本文件进行填充。下一个过程中的步骤介绍了如何配置文本文件，并包含每个字段的说明。键入后，该应用程序将不保存信息，因此，您可能希望创建一个文本文件以保留该信息供将来使用。

使用文本文件配置 **Provisioning Tool**

将文件命名为 nfcprovisioning.txt 并将其放置在设备的 SD 卡中的 /sdcard/ 文件夹下。该应用程序随后可以读取文本文件并填充值。

文本文件必须包含以下数据：

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>

此行为 EMM 提供程序应用程序的 Intranet/Internet 位置。恢复出厂设置的设备在进行 NFC 碰撞后连接到 Wi-Fi 之后，该设备必须有权访问此位置才能进行下载。该 URL 为常规 URL，不需要特殊格式。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>

此行是 EMM 提供程序应用程序的校验和。此校验和用于验证下载是否成功。本文稍后将讨论获取校验和的步骤。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

此行是运行 Provisioning Tool 的设备的已连接 Wi-Fi SSID。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

支持的值为 WEP 和 WPA2。如果 Wi-Fi 未受保护，此字段必须留空。

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

如果 Wi-Fi 未受保护，此字段必须留空。

android.app.extra.PROVISIONING_LOCALE=<locale>

输入语言和国家/地区代码。语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请键入 en_US 表示在美国所讲的英语。如果未输入任何代码，则会自动填充国家/地区和语言。

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

设备运行时所在的时区。键入区域/位置的数据库名称。例如，键入 **America/Los_Angeles** 表示太平洋时间。如果未键入名称，时区将自动填充。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

不需要此数据，因为值 Secure Hub 被硬编码到应用程序中。在本文中提及的目的只是为了保持完整性。

如果使用 WPA2 保护 Wi-Fi，则完整的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

如果有未受保护的 Wi-Fi，则已完成的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

获取 **Citrix Secure Hub** 的校验和

Secure Hub 的校验和是一个常数值：qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM。要下载适用于 Secure Hub 的 APK 文件，请使用以下 Google Play 应用商店链接：https://play.google.com/managed/downloadManagingApp?identifier=xenmobile。

获取应用程序校验和

必备条件：

- 来自 Android SDK Build Tools 的 **apksigner** 工具
- OpenSSL 命令行

要获取任何应用程序的校验和，请按照下列步骤进行操作：

1. 从 Google Play 应用商店下载应用程序的 APK 文件。
2. 在 OpenSSL 命令行中，导航到 **apksigner** 工具：android-sdk/build-tools/<version>/apksigner 并键入以下内容：

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

   该命令返回有效的校验和。

3. 要生成 QR 码，请在 PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM 字段中输入校验和。例如：

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
9       }
10
11    }
12
13  <!--NeedCopy-->
```

使用的库

Provisioning Tool 在其源代码中使用以下库：

- Google 遵循 Apache License 2.0 提供的 v7 `appcompat` 库、Design Support 库以及 v7 Palette Support 库

  有关信息，请参阅 Support Library Features Guide（支持库功能指南）。

- Jake Wharton 遵循 Apache License 2.0 提供的 Butter Knife

使用 **QR** 代码注册设备

用户可以使用您为完全托管设备生成的 QR 代码注册这些设备。

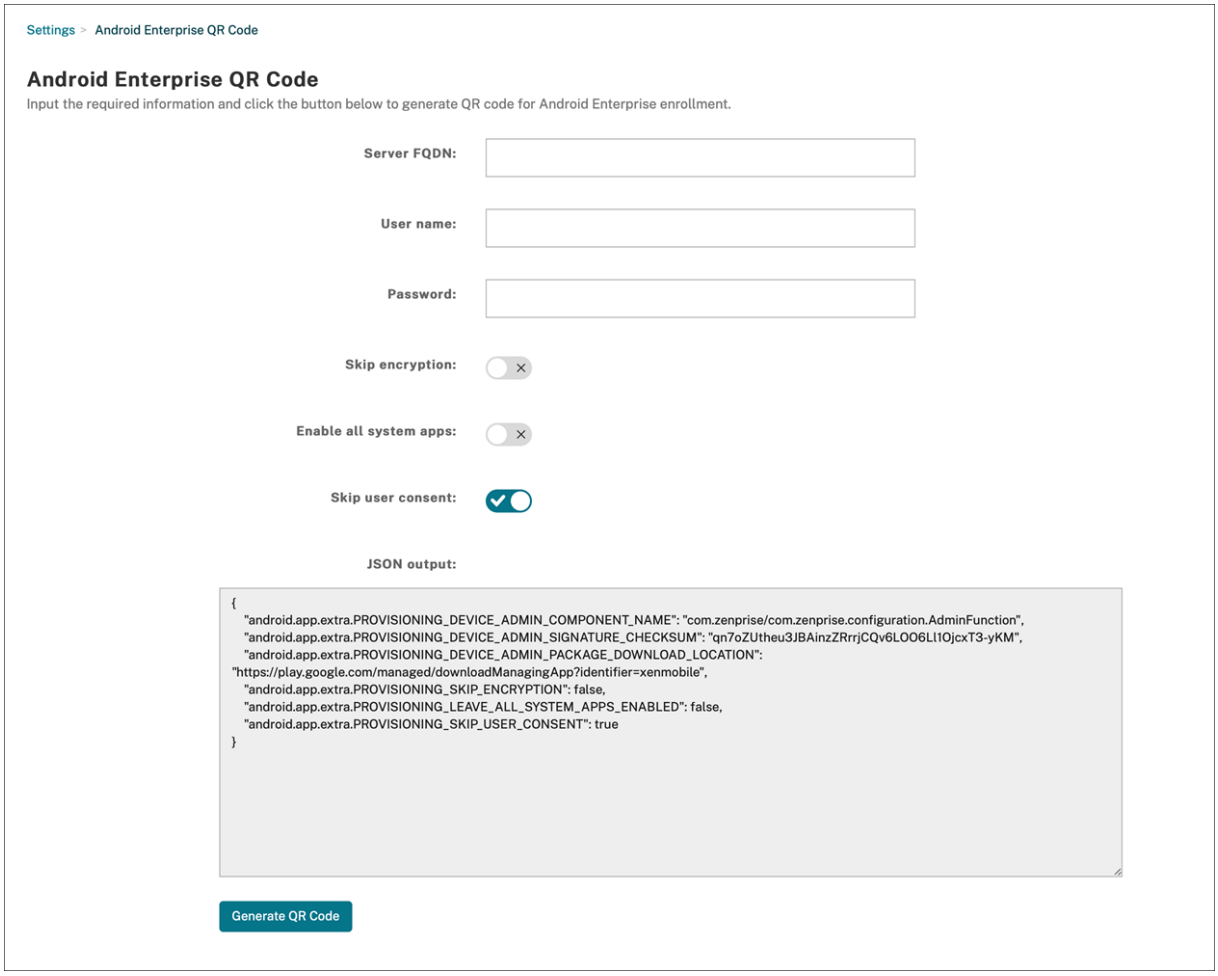
系统要求

运行 Android 7.0 或更高版本的 Android 设备。

创建 **QR** 代码

您根据需要通过指定注册信息生成 QR 代码。生成 QR 代码后，请在本地保存 QR 代码。Endpoint Management 不存储该代码。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



1. 导航到 **Settings**（设置）**> Android Enterprise QR Code**（**Android Enterprise QR** 代码）。
2. 如果需要，请指定以下注册信息：
   - **Server FQDN**（服务器 FQDN）：键入 Endpoint Management 服务器的 FQDN（例如 `example.cem.cloud.com`）。此字段为可选字段。如果留空，用户必须在注册时填充此信息。
   - **User name**（用户名）：键入用于注册的用户名。如果您计划将二维码分发给多个用户，我们建议将此字段留空。使用用户名和密码配置 QR 代码对注册 Kiosk 设备非常有用。如果将此字段留空，用户必须在注册时填充此信息。
   - **Password**（密码）：键入与所键入的用户名相关联的密码。如果将此字段留空，用户必须在注册时填充此信息。
   - **Skip encryption**（跳过加密）：如果设置为 **On**（开），注册期间将不加密设备。默认值为关。
   - **Enable all system apps**（启用所有系统应用程序）：如果设置为 **On**（开），则允许访问设备上的所有系统应用程序。默认值为关。
   - **Skip user consent**（跳过用户同意）：如果设置为 **Off**（关），用户可以选择退出设备管理。默认值为关。

   JSON output（JSON 输出）框显示与指定的信息对应的 JSON 内容。
3. 要添加更多注册信息，请编辑 **JSON output**（JSON 输出）框中的 JSON 内容。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

4. 单击 **Generate QR Code**（生成 QR 代码）。QR 代码在 JSON 输出的右侧显示。
5. 右键单击 QR 代码图像并保存。
6. 将该图像发送给用户以便进行设备注册。

恢复出厂设置的设备将扫描此 QR 代码以注册为完全托管设备。

注册设备

打开新设备或恢复出厂设置的设备的电源后：

1. 在欢迎屏幕上轻按该屏幕六次以启动 QR 代码注册流程。
2. 系统提示时，连接到 Wi-Fi。QR 代码中 Secure Hub 的下载位置可以通过此 Wi-Fi 网络访问。

   设备成功连接到 Wi-Fi 后，将从 Google 下载一个 QR 代码读取器并启动摄像头。
3. 将摄像头对准 QR 代码以扫描该代码。

   Android 将从 QR 代码中的下载位置下载 Secure Hub，验证签名证书的签名，安装 Secure Hub 并将其设置为设备所有者。

有关详细信息，请参阅此面向 Android EMM 开发人员的 Google 指南：https://developers.google.com/android/work/prov-devices#qr_code_method。

零接触注册

零接触注册允许您将设备设置为在首次开机时将其自身配置为完全托管的设备。

您的设备经销商在 Android 零触摸门户网站上为您创建一个帐户，这是一个可让您将配置应用到设备的联机工具。使用 Android 零接触门户，创建一个或多个零接触注册配置，并将配置应用于分配给您帐户的设备。当用户为这些设备打开电源时，这些设备将自动注册到 Endpoint Management 中。分配给设备的配置定义了其自动注册过程。

系统要求

- 对零触摸注册的支持自 Android 9.0 开始。

您的经销商提供的设备和帐户信息

- 符合零接触注册条件的设备是从企业经销商或 Google 合作伙伴处购买的。有关 Android Enterprise 零触摸合作伙伴的列表，请参阅 Android website（Android Web 站点）。
- 由您的经销商创建的 Android Enterprise 零触摸门户帐户。
- Android Enterprise 零触摸门户帐户登录信息，由您的经销商提供。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

创建零触摸配置

创建零触摸配置时，请包含一个自定义 JSON 以指定配置的详细信息。

使用此 JSON 可配置要在指定的 Endpoint Management 服务器上注册的设备。在本示例中，将服务器的 URL 替换为 “URL”。

```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL"
7            }
8
9         }
10
11  <!--NeedCopy-->
```

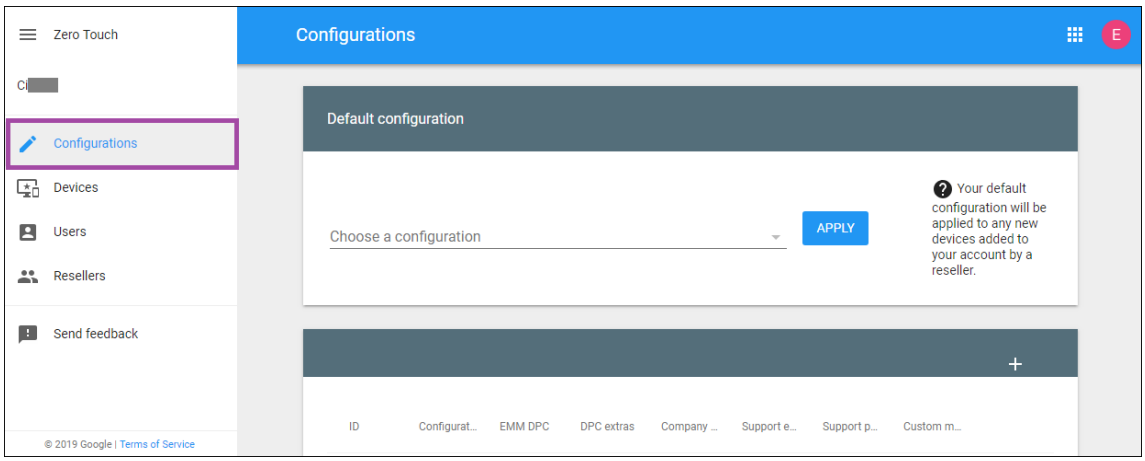
可以使用具有更多参数的可选 JSON 来进一步自定义您的配置。此示例指定 Endpoint Management 服务器以及使用此配置的设备用于登录服务器的用户名和密码。

```
1       {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4            {
5
6                "serverURL":"URL",
7                "xm_username":"username",
8                "xm_password":"password"
9             }
10
11              }
12
13    <!--NeedCopy-->
```

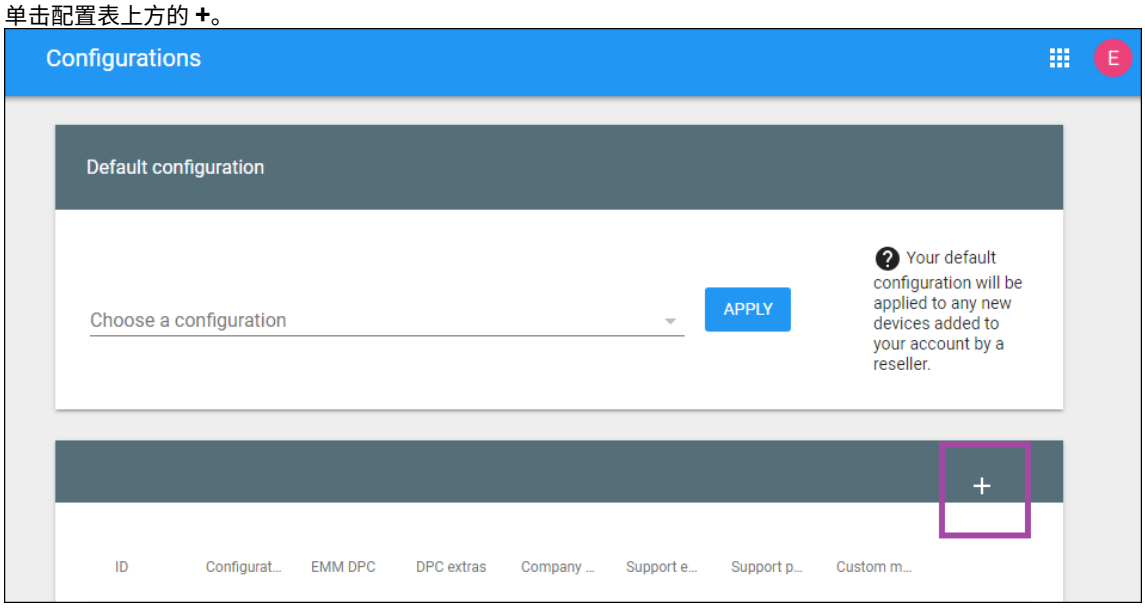
> 重要：
>
> 要在企业拥有的设备上的工作配置文件模式下注册设备，请将 { "desiredProvisioningMode": "managedProfile"} 添加到 PROVISIONING_ADMIN_EXTRAS_BUNDLE 下的自定义 JSON。

1. 转至 Android 零触摸门户，网址为 https://partner.android.com/zerotouch。使用您的零触摸设备经销商提供的帐户信息登录。
2. 单击配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

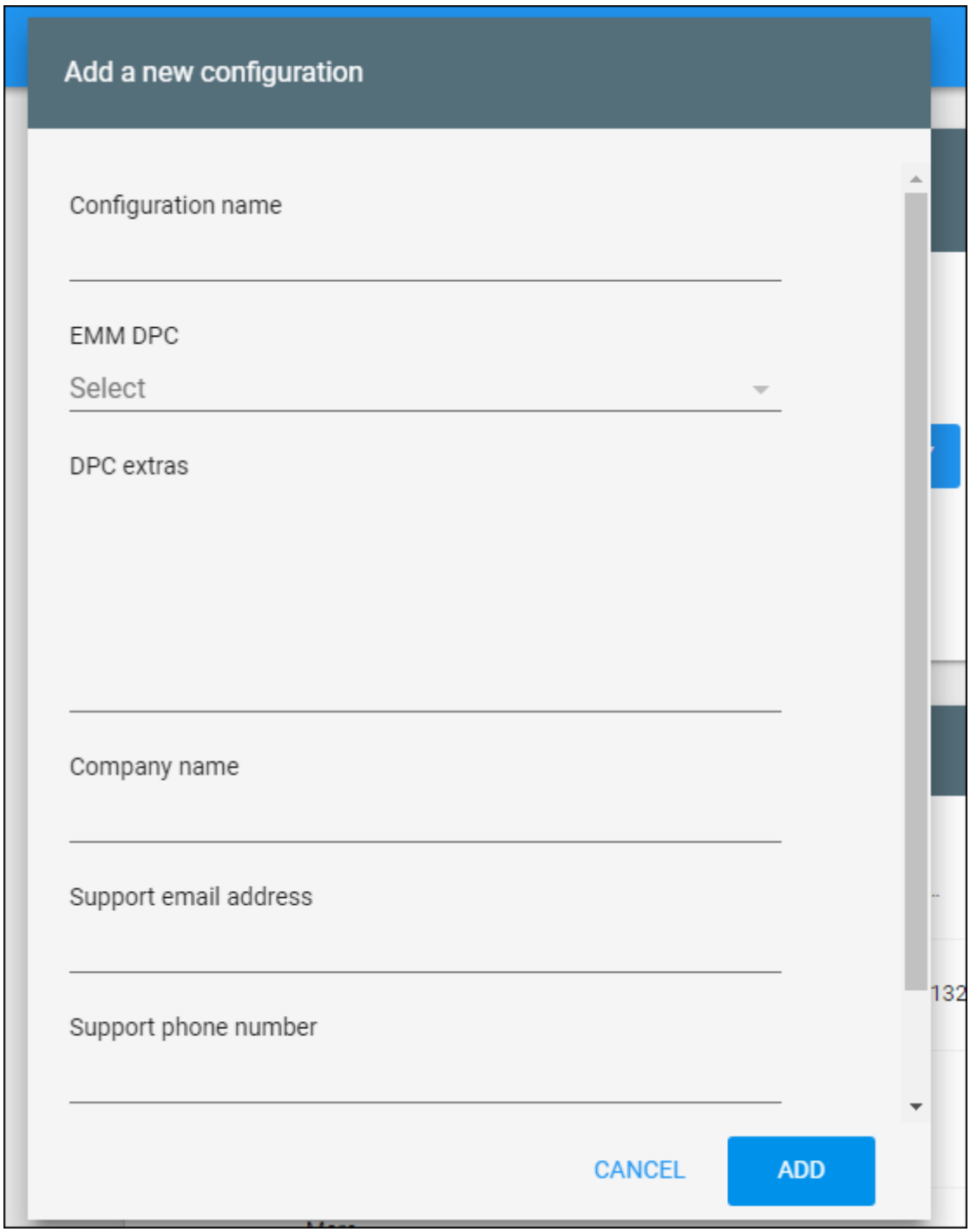


3. 单击配置表上方的 **+**。



4. 在显示的配置窗口中输入您的配置信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

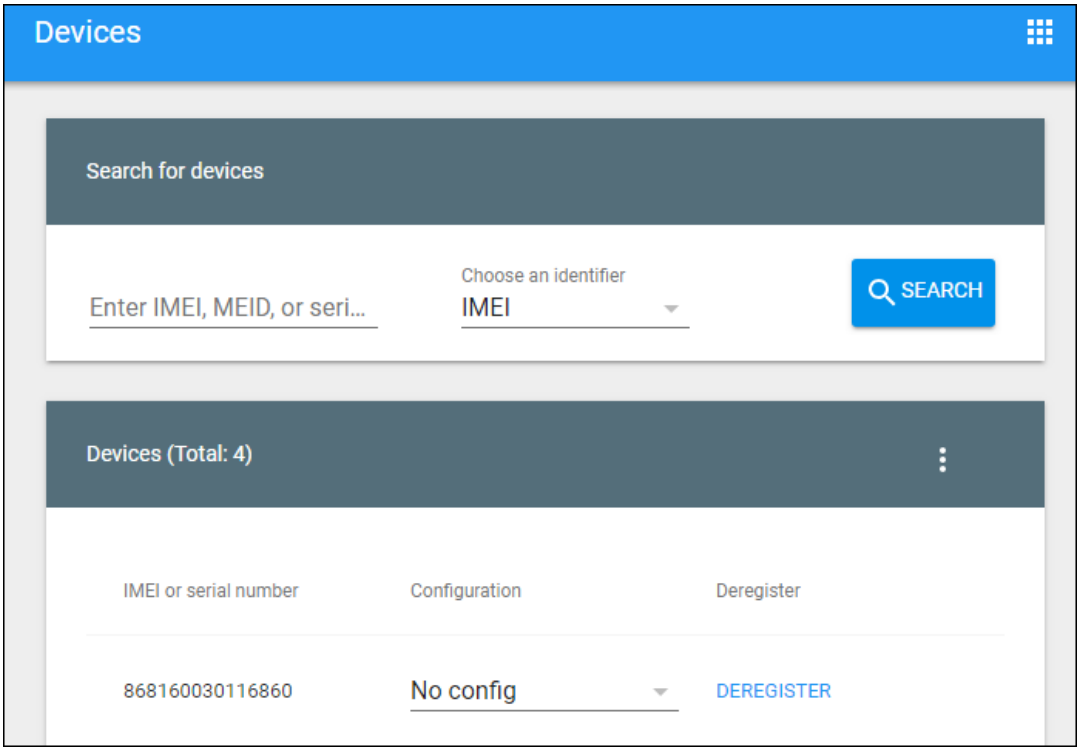


- 配置名称：键入您为此配置选择的名称。
- **EMM DPC**：选择 **Citrix Secure Hub**。
- **DPC** 附加程序：在此字段中粘贴您的自定义 JSON 文本。
- 公司名称：键入您希望在设备配置期间在 Android Enterprise 零接触设备上显示的名称。
- 支持电子邮件地址：键入用户可以联系以寻求帮助的电子邮件地址。此地址会在设备预配之前显示在 Android Enterprise 零触摸设备上。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 支持电话号码：键入您的用户可以联系以寻求帮助的电话号码。设备预配之前，此电话号码会显示在 Android Enterprise 零触摸设备上。
- 自定义消息：（可选）添加一个或两个句子，以帮助您的用户与您联系，或者为其提供有关其设备发生的情况的更多详细信息。此自定义消息会在设备预配之前显示在 Android Enterprise 零触摸设备上。

5. 单击添加。
6. 要创建更多配置，请重复步骤 2 到 4。
7. 要将配置应用到设备，请执行以下操作：
   a) 在 Android 零触摸门户中，单击设备。
   b) 在设备列表中找到设备，然后选择要向其分配的配置。



   c) 单击更新。

可以使用 CSV 文件将配置应用到许多设备。

有关如何将配置应用于多台设备的信息，请参阅 IT 管理员零接触注册。此 Android Enterprise 主题提供了有关如何管理配置并将其应用于设备的更多信息。

预配专用 **Android Enterprise** 设备

专用 Android Enterprise 设备属于完全托管设备，专门用于满足单个用例。您将这些设备限制为执行此用例所需任务所需的一个应用程序或一小部分应用程序。您还可以阻止用户启用其他应用程序或在设备上执行其他操作。

使用用于其他完全托管设备的任何注册方法注册专用设备，如预配 Android Enterprise 完全托管设备。预配专用设备需要在注册之前进行更多设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要预配专用设备，请执行以下操作：

- 为允许在您的 Endpoint Management 部署中注册专用设备的 Endpoint Management 管理员创建注册配置文件。请参阅创建注册配置文件。
- 要使专用设备能够访问应用程序，请将其添加到允许列表中。
- 或者，将允许运行的应用程序设置为允许锁定任务模式。当某个应用程序处于锁定任务模式时，用户打开时该应用程序将固定到设备屏幕。此时将不显示任何主页按钮，并且返回按钮处于禁用状态。用户使用编程到该应用程序中的一项操作退出该应用程序，例如注销。
- 在您添加的注册配置文件中注册每台设备。

系统要求

- 对注册专用设备的支持自 Android 6.0 起启用。

允许运行应用程序并设置锁定任务模式

展台设备策略允许您允许运行应用程序以及设置锁定任务模式。默认情况下，Secure Hub 和 Google Play 服务都在允许列表中。

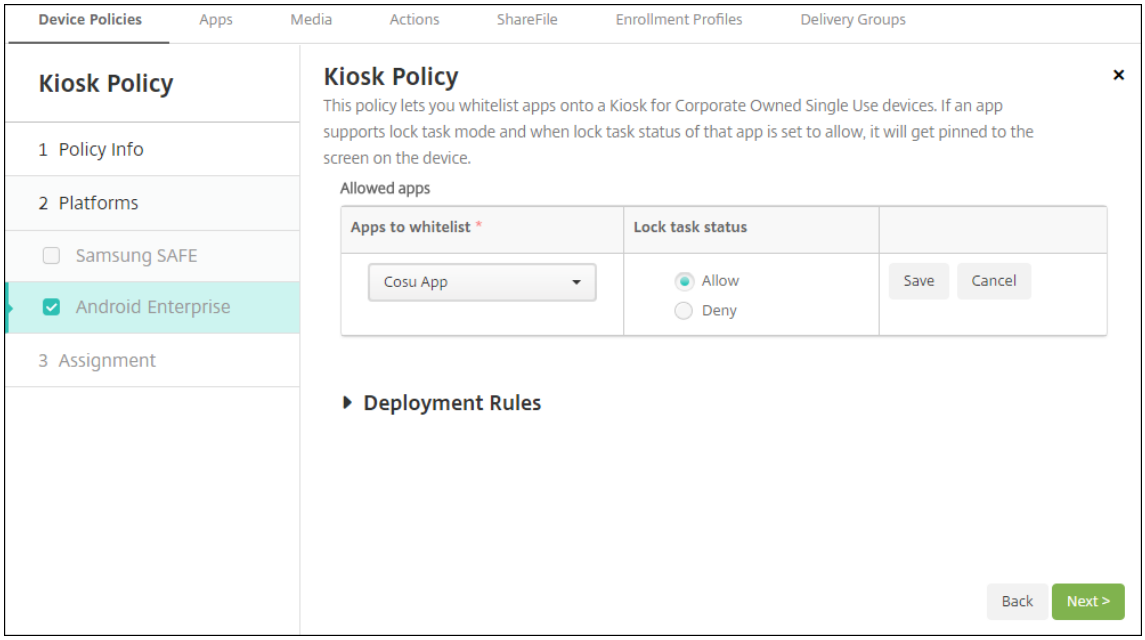
要添加展台策略，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击配置 **>** 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在“安全性”下，单击展台。此时将显示展台策略页面。
4. 在“平台”下，选择 **Android Enterprise**。清除其他平台。
5. 在“策略信息”窗格中，键入策略名称和可选说明。
6. 单击下一步，然后单击添加。
7. 要允许运行某个应用程序并允许或拒绝该应用程序的锁定任务模式，请执行以下操作：

   从列表中选择要允许的应用程序。

   选择允许可设置要在用户启动应用程序时固定到设备屏幕的应用程序。选择拒绝可设置不固定的应用程序。默认设置为允许。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



8. 单击保存。
9. 要允许运行另一个应用程序并允许或拒绝该应用程序的锁定任务模式，请单击添加。
10. 配置部署规则并选择交付组。有关详细信息，请参阅设备策略。

预配具有工作配置文件或企业拥有的设备上的工作配置文件的 **Android Enterprise** 完全托管设备

运行 Android 9.0-10.x 的设备注册为“具有工作配置文件的完全托管”。自 Android 11+ 起，设备注册为“企业拥有的设备上的工作配置文件”。所有这些设备都是公司拥有的设备，用于工作和个人目的。贵组织负责管理整个设备。可以将一组策略应用到设备，另一组策略应用到工作配置文件。

在 Endpoint Management 控制台中，使用工作配置文件的完全托管设备将显示以下术语：

- 设备所有权为“企业”。
- 设备 Android Enterprise 安装类型为“企业所有者但由个人使用”。

系统要求

- 支持注册具有工作配置文件的完全托管设备从 Android 9.0 开始。

注册设备

新设备和重置为出厂设备的设备注册为使用工作配置文件的完全托管设备。这些设备使用用于其他完全托管设备的任何注册方法，如预配 Android Enterprise 完全托管设备中所述。运行 Android 11 的设备可以使用 QR 代码或该部分中所述的零触摸注册注册方法在企业拥有的设备上的工作配置文件模式下注册。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 使用 QR 代码方法在企业拥有的设备上的工作配置文件模式下注册设备时，请将以下内容添加到 `serverURL` 字段上方的 JSON 输出中：
>
> `"desiredProvisioningMode": "managedProfile",`

JSON output

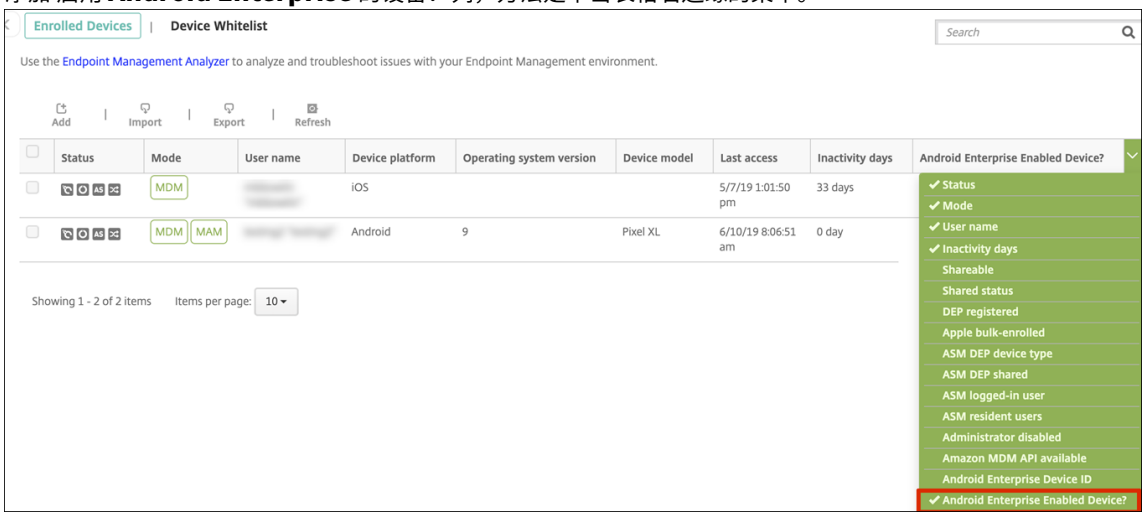
```
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
    "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
    "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
    "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "desiredProvisioningMode": "managedProfile",
        "serverURL": "https://testServer.xmqa.cloud.com",
        "username": "username",
        "password": "password"
    }
```

非新设备或恢复出厂设置的设备将注册为工作配置文件设备，如预配 Android Enterprise 工作配置文件设备中所述。

在 **Endpoint Management** 控制台中查看 **Android Enterprise** 设备

要查看 Android Enterprise 完全托管设备、专用设备和使用工作配置文件的完全托管设备，请执行以下操作：

1. 在 Endpoint Management 控制台中，转到管理 **>** 设备。
2. 添加 启用 **Android Enterprise** 的设备？列，方法是单击表格右边缘的菜单。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 要查看可用的安全操作，请选择完全托管设备，然后单击安全。当设备处于完全托管状态时，“完全擦除”操作可用，但 选择性擦除不可用。该差别是因为设备仅允许来自托管 Google Play 应用商店的应用程序。用户无法选择从公共商店安装应用程序。贵组织负责管理设备上的所有内容。



配置 **Android Enterprise** 设备和应用程序策略

有关在设备和应用程序级别控制的策略的概述，请参阅 Android Enterprise 支持的设备策略和 MDX 策略。

关于策略需要了解以下内容：

- 设备限制：数十种设备限制允许您控制以下功能：
  - 使用设备摄像头
  - 在工作配置文件与个人配置文件之间使用复制和粘贴
- **PerApp VPN**：使用“托管配置”设备策略为 Android Enterprise 配置 VPN 配置文件。
- 电子邮件策略：我们建议使用“托管配置”设备策略来配置应用程序。

设备策略

下表列出了适用于 Android Enterprise 设备的所有设备策略。

> 重要：
>
> 对于在 Android Enterprise 中注册并使用 MDX 应用程序的设备：可以通过 MDX 和 Android Enterprise 控制某些设置。对 MDX 使用限制性最低的策略设置，并通过 Android Enterprise 控制策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序权限	应用程序清单	应用程序卸载
自动更新托管应用程序	连接计划	凭据
自定义 XML	Endpoint Management 选项	文件
键盘锁管理	Kiosk	Launcher 配置
位置	托管配置	网络
操作系统更新	通行码	限制

适用于具有工作配置文件的完全托管设备的设备策略（**COPE** 设备）

对于具有工作配置文件的完全托管设备，可以使用某些设备策略将单独的设置应用到整个设备和工作配置文件。可以使用其他设备策略将设置仅应用到整个设备或仅应用到具有工作配置文件的完全托管设备的工作配置文件。对于在企业拥有的设备上的工作配置文件模式下注册的设备，策略仅适用于工作配置文件，不适用于整个设备。

策略	适用对象
应用程序权限	工作配置文件
应用程序清单	工作配置文件
应用程序卸载	工作配置文件
自动更新托管应用程序	工作配置文件
连接计划	工作配置文件
凭据	工作配置文件
自定义 XML	不适用
Endpoint Management 选项	工作配置文件
文件	工作配置文件
键盘锁管理	设备和工作配置文件
Kiosk	不适用
Launcher 配置	设备和工作配置文件
位置	设备（仅限定位模式）
托管配置	工作配置文件
网络	设备
操作系统更新	不适用

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

策略	适用对象
通行码	设备和工作配置文件
限制	设备和工作配置文件（为设备和工作配置文件创建单独的策略）
VPN	不适用

另请参阅 Android Enterprise 支持的设备策略和 MDX 策略和 MAM SDK 概述。

安全操作

Android Enterprise 支持以下安全操作。有关每个安全操作的说明，请参阅安全操作。

安全操作	工作配置文件	完全托管
证书续订	是	是
完全擦除	是（选择性擦除后）	是
查找	是	是
锁定	是	是
锁定并重置密码	否	是
通知（响铃）	是	是
吊销	是	是
选择性擦除	是	是

安全操作说明

- 除非“位置”设备策略将设备的位置模式设置为高精度或电池节能，否则定位安全操作将失败。请参阅位置设备策略。
- 在运行 Android 9.0 之前版本的 Android 的工作配置文件设备上：
  - 不支持锁定和重置密码操作。
- 在 Android 9.0 或更高版本的工作配置文件设备上：
  - 发送的密码将锁定工作配置文件。设备本身不锁定。
  - 如果未在工作配置文件上设置通行码：
    - 如果未发送通行码或发送的通行码不符合通行码要求：设备处于锁定状态。
  - 如果在工作配置文件上设置了通行码：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

* 如果未发送通行码，或者发送的通行码不符合通行码要求：工作配置文件将锁定，但设备本身不锁定。

取消注册 **Android Enterprise** 企业

如果您不想再使用 Android Enterprise 企业，则可以取消注册该企业。

> 警告：
>
> 取消注册企业后，通过其注册的设备上的 Android Enterprise 应用程序将重置为其默认状态。Google 不再管理设备。如果您注册到新的 Android Enterprise 企业，则必须从托管 Google Play 审批新组织的应用程序。然后，您可以从 Endpoint Management 控制台更新应用程序。

取消注册 Android Enterprise 企业后：

- 通过企业注册的设备和用户会将 Android Enterprise 应用程序重置到其默认状态。以前应用的托管配置策略不再影响操作。
- Endpoint Management 负责管理通过企业注册的设备。从 Google 角度来看，这些设备是非托管设备。您不能添加新的 Android Enterprise 应用程序。无法应用托管配置策略。可以将其他策略（例如“计划”、“密码”和“限制”）应用到这些设备。
- 如果您尝试在 Android Enterprise 中注册设备，则这些设备将注册为安卓设备，而不是 Android 企业设备。

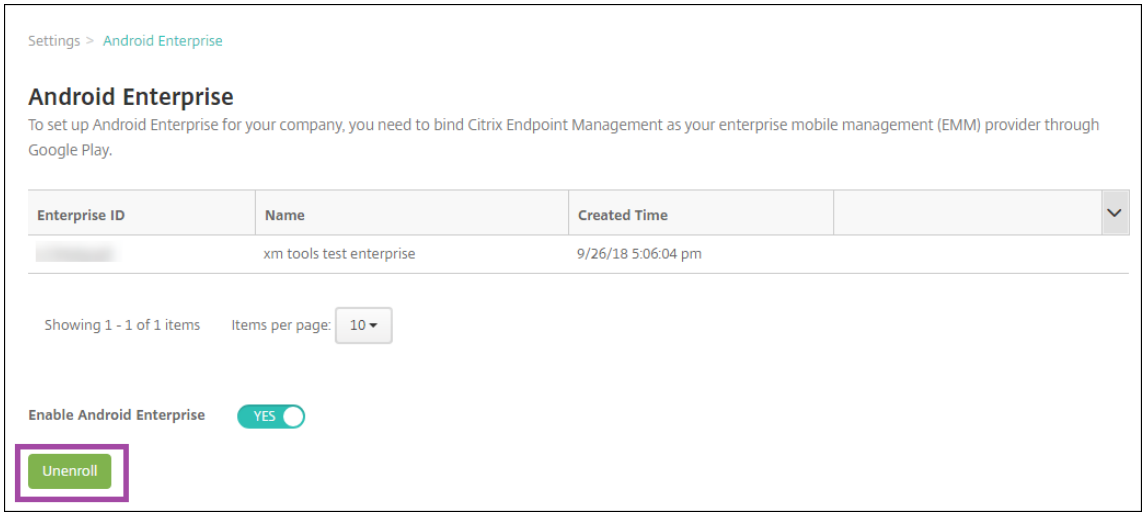
使用 Endpoint Management 服务器控制台和 Endpoint Management Tools 取消注册 Android Enterprise 企业。

执行此任务时，Endpoint Management 会打开一个工具弹出窗口。在开始之前，请确保您的浏览器有权打开弹出窗口。某些浏览器（例如 Google Chrome）要求禁用弹出窗口阻止功能并将 Endpoint Management 站点的地址添加到弹出窗口允许列表中。

要取消注册 Android Enterprise 企业，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在“设置”页面上，单击 **Android Enterprise**。
3. 单击取消注册。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



分发 **Android Enterprise** 应用程序

July 24, 2023

Endpoint Management 管理部署到设备的应用程序。可以组织和部署以下类型的 Android Enterprise 应用程序。

- 托管应用商店应用：这些应用包括托管 Google Play 商店中提供的免费应用。例如，GoToMeeting。
- **MDX**：使用 MAM SDK 准备的应用程序或使用 MDX Toolkit 封装的应用程序。这些应用程序包括 MDX 策略。您可以从内部来源和公共应用商店获取 MDX 应用程序。将 Citrix 移动生产力应用程序作为 MDX 应用程序部署。
- 企业：您开发或从其他来源获取的专用应用程序。可以通过托管 Google Play 应用商店向用户提供这些应用程序。托管 Google Play 应用商店是 Google 企业应用商店。
- **MDX-enabled private apps**（启用了 MDX 的专用应用程序）：使用 MAM SDK 准备或通过 MDX Toolkit 封装的企业应用程序。

可以通过两种不同的方式添加企业应用程序和启用了 MDX 的专用应用程序。

- 将应用程序作为企业应用程序添加到 Endpoint Management 控制台，如本文中的企业应用程序和启用了 MDX 的专用应用程序部分中所述。
- 使用您的 Google 开发者帐号将应用程序直接发布到托管 Google Play 应用商店。然后将应用程序作为托管应用商店应用程序添加到 Endpoint Management 控制台。请参阅托管应用商店应用程序。

如果您使用 Google 开发者帐户发布应用程序，然后切换到使用 Endpoint Management 控制台，则应用程序的所有权会有所不同。在这种情况下，您需要在两个位置管理应用程序。Citrix 建议使用一种或另一种方法添加应用程序。

如果您需要从托管 Google Play 应用商店中删除自助管理的应用程序，请向 Google 开立一个票证。开发者可以禁用但不能删除托管 Google Play 应用商店中的应用程序。

以下各部分内容提供了有关 Android Enterprise 应用程序配置的详细信息。有关分发应用程序的信息，请参阅添加应用程序。该文包含：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 用于添加 Web 和 SaaS 应用程序或 Web 链接的一般工作流程
- 面向企业和公共应用商店应用程序的必需应用程序工作流
- 如何通过适用于企业应用程序的 Citrix 内容交付网络 (CDN) 交付企业应用程序

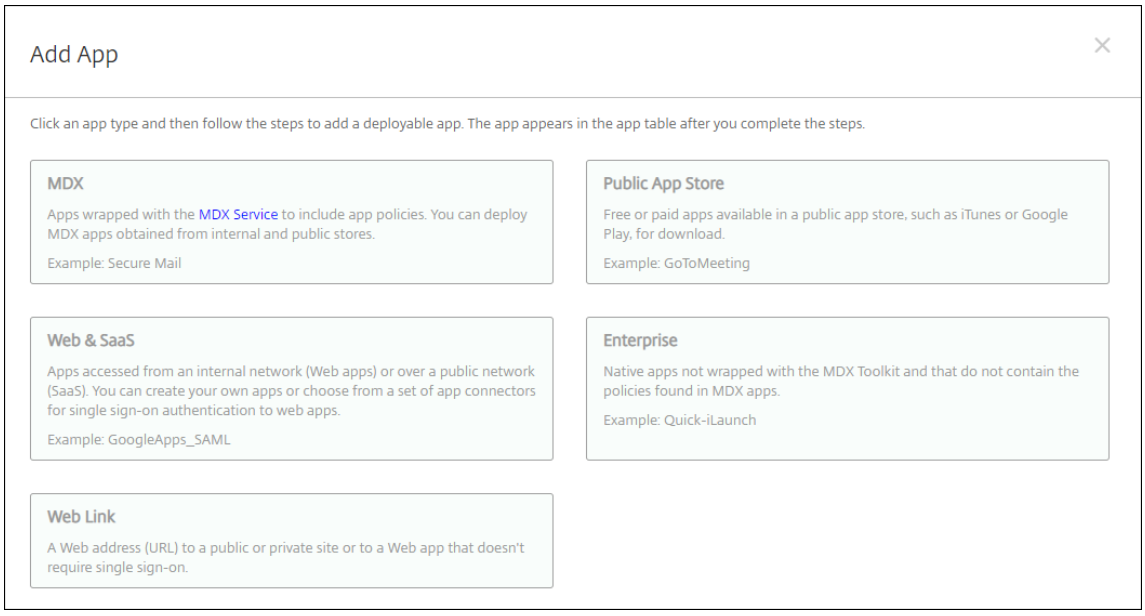
托管应用商店应用程序

您可以将托管 Google Play 商店中提供的免费应用程序添加到 Citrix Endpoint Management 中。

> 注意：
>
> 要使可从托管 Google Play 访问的 Google Play 应用商店中的所有应用程序，请使用访问托管 **Google Play** 应用商店中的所有应用程序服务器属性。请参阅服务器属性。将此属性设置为 **true** 会允许所有 Android Enterprise 用户访问公共 Google Play 应用商店应用程序。然后，您可以使用限制设备策略来控制对这些应用程序的访问。

步骤 **1**：添加和配置应用程序

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击公共应用商店。

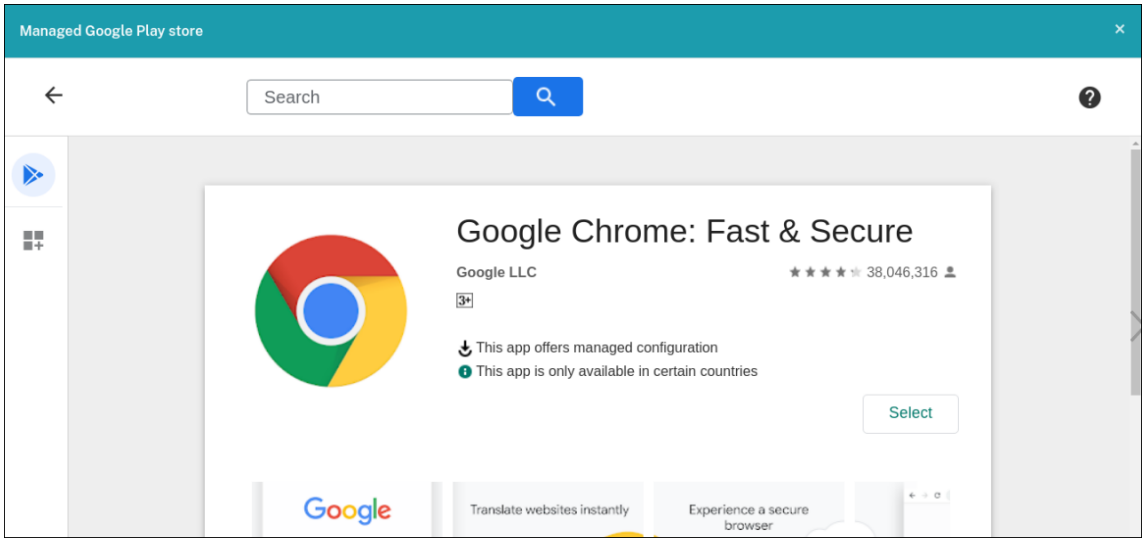


3. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。该名称显示在应用程序表格中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
4. 选择 **Android Enterprise** 作为平台。
5. 在搜索框中键入应用程序名称或软件包 ID，然后单击搜索。可以在 Google Play 应用商店中找到软件包 ID。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

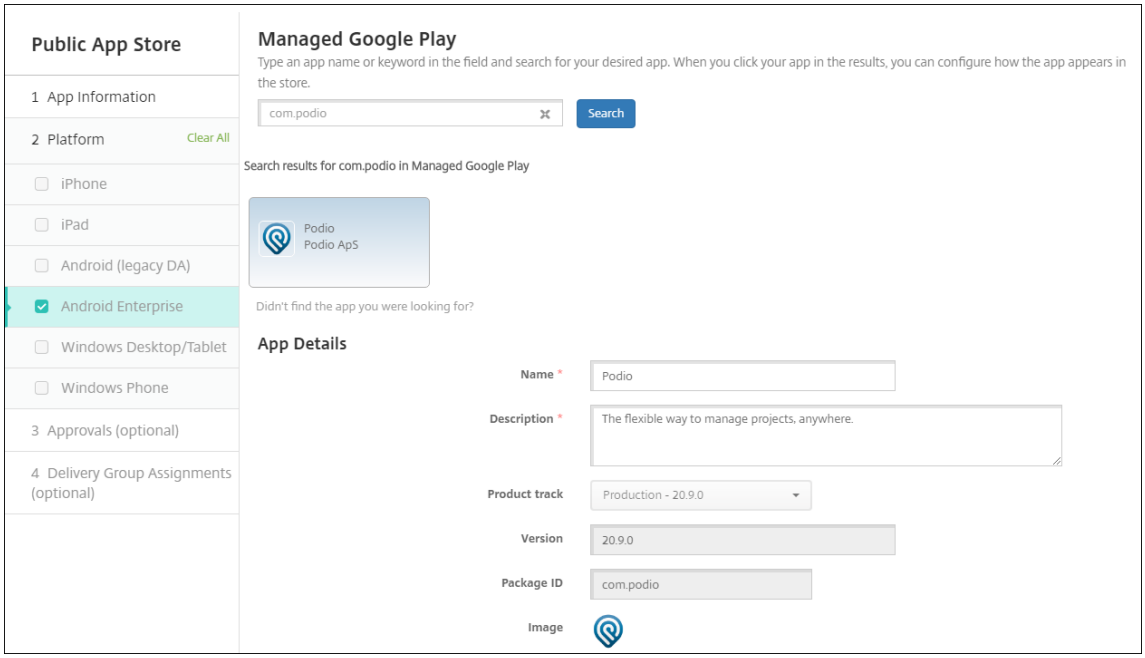
该 ID 位于应用程序的 URL 中。例如，`com.Slack` 为 `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US` 中的软件包 ID。

6. 此时将显示符合搜索条件的应用程序。单击所需的应用程序，然后单击 “选择”。



7. 再次单击 “选择”。

8. 单击应用程序图标并配置应用程序名称和说明。



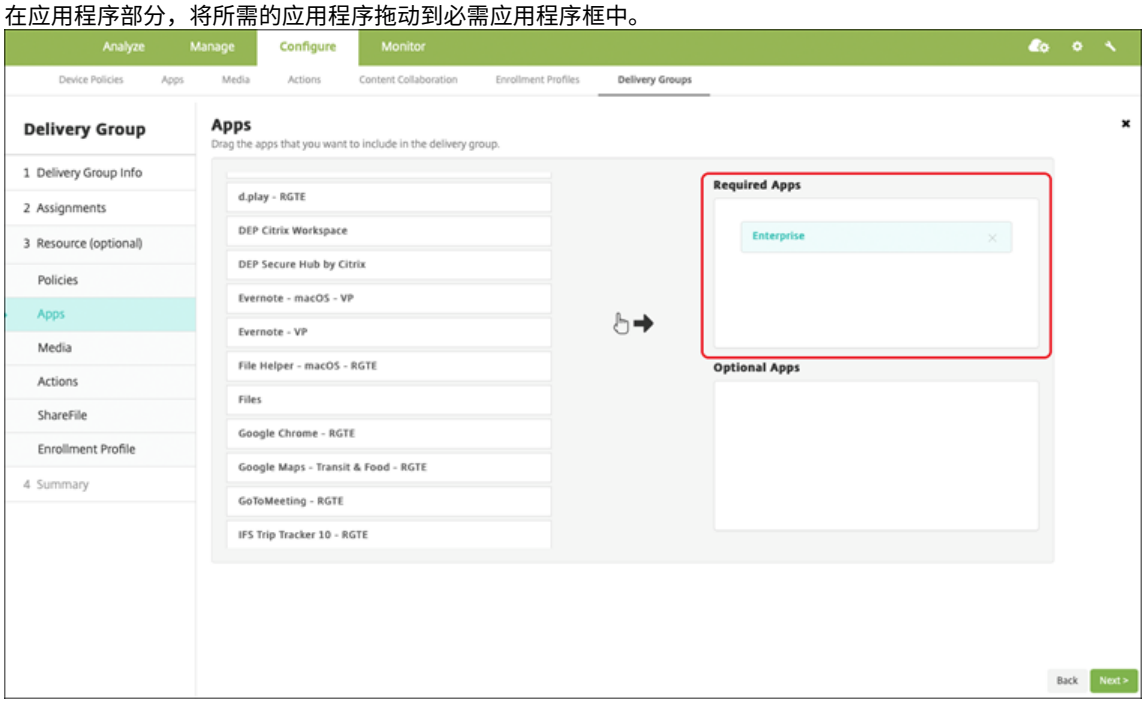
9. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

步骤 **2**：配置应用程序部署

1. 导航到配置 **>** 交付组，然后选择您配置的交付组。单击编辑。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



3. 在摘要页面上，单击保存。
4. 在交付组页面上，选择交付组，然后单击部署。

MDX 应用程序

将 MDX 文件添加到 Endpoint Management 并配置应用程序详细信息和策略设置。要为 Android Enterprise 配置 Citrix 移动生产力应用程序，请将其添加为 MDX 应用程序。有关每种设备平台类型可用的应用程序策略的信息，请参阅：

- MAM SDK 概述
- MDX 策略概览

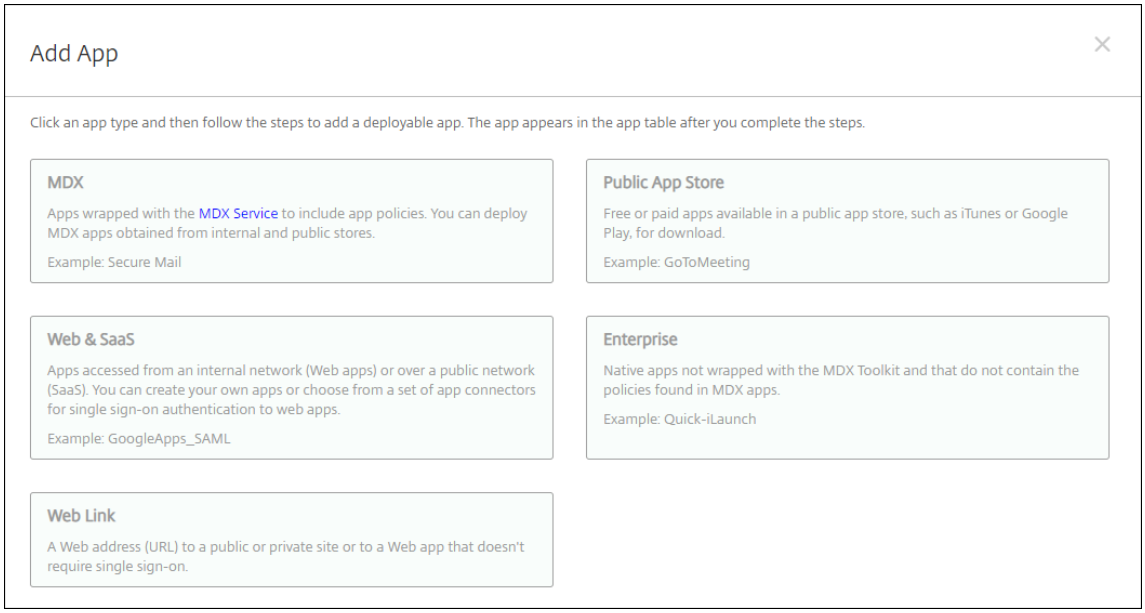
步骤 **1**：添加和配置应用程序

1. 对于 Citrix 移动生产力应用程序，请下载公共应用商店 MDX 文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management** 生产力应用程序。

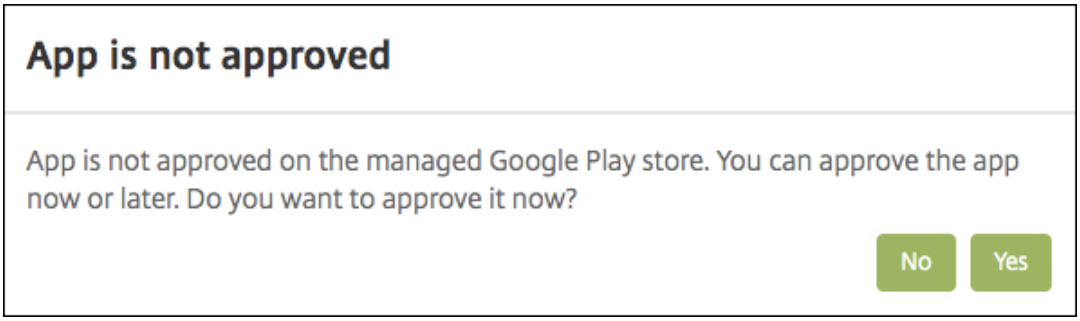
   对于其他类型的 MDX 应用程序，请获取 MDX 文件。

2. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序。单击添加。此时将显示添加应用程序对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

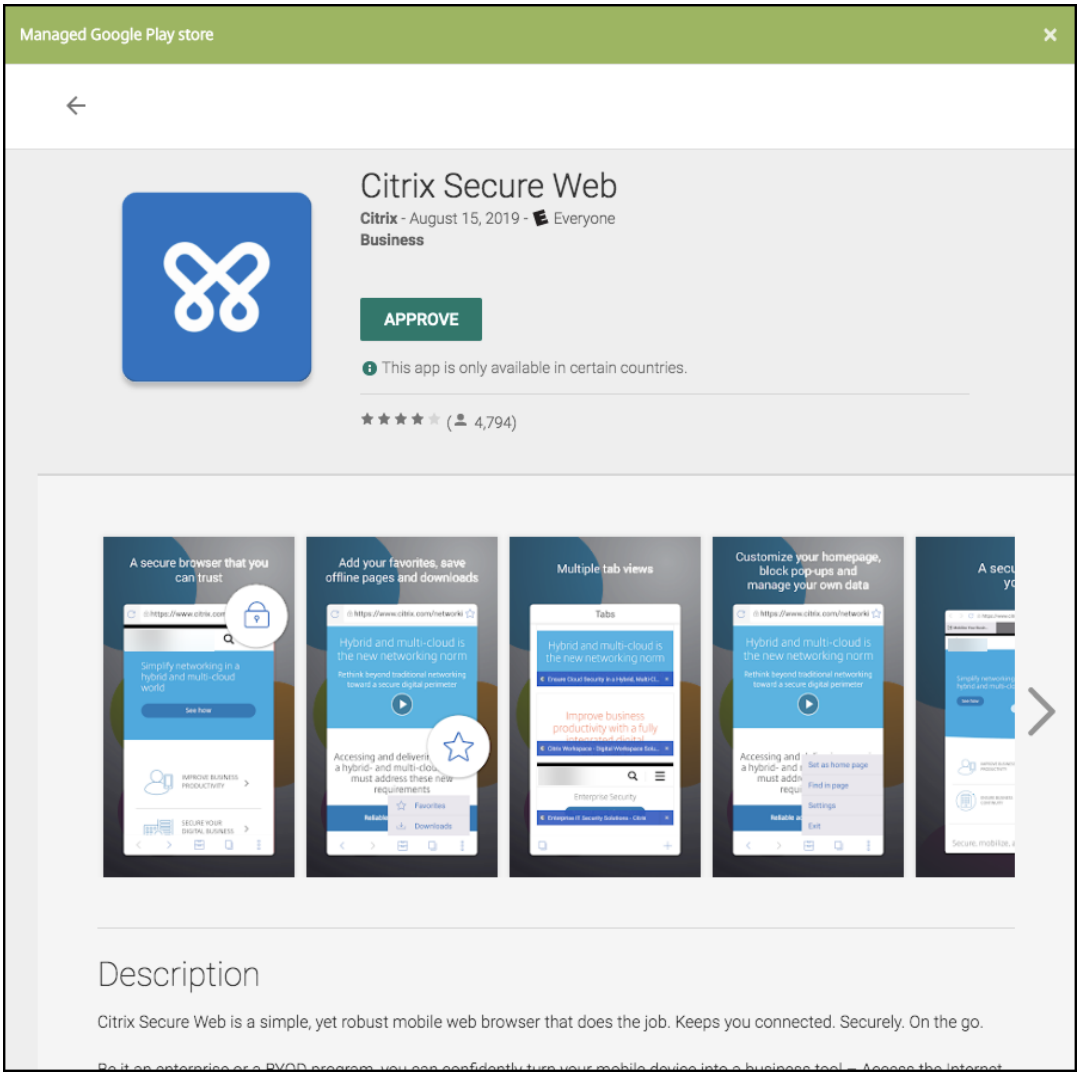


3. 单击 **MDX**。此时将显示 **MDX** 应用程序信息页面。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。该名称显示在应用程序表格中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
4. 选择 **Android Enterprise** 作为平台。
5. 单击上载并导航到 MDX 文件。Android Enterprise 仅支持使用 MAM SDK 或 MDX Toolkit 准备的应用程序。
   - UI 会通知您附加的应用程序是否需要从托管 Google Play 应用商店获得批准。要在不离开 Citrix Endpoint Management 控制台的情况下审批应用程序，请单击是。

     在托管 Google Play 应用商店打开后，按照说明审批并保存应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



成功添加应用程序后，将显示应用程序详细信息页面。

6. 配置以下设置：

   - 文件名：键入与应用程序关联的文件名。
   - 应用程序说明：键入应用程序的说明。
   - 应用程序版本：（可选）键入应用程序版本号。
   - 软件包 **ID**：键入从托管的 Google Play 商店获取的应用程序包 ID。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。

7. 配置 **MDX** 策略。MDX 策略因平台而异，并且包含面向策略区域的选项，包括身份验证、设备安全和应用程序限制。在控制台中，每种策略都具有介绍此策略的提示。有关每种设备平台类型可用的应用程序策略的信息，请参阅：

   - MAM SDK 概述

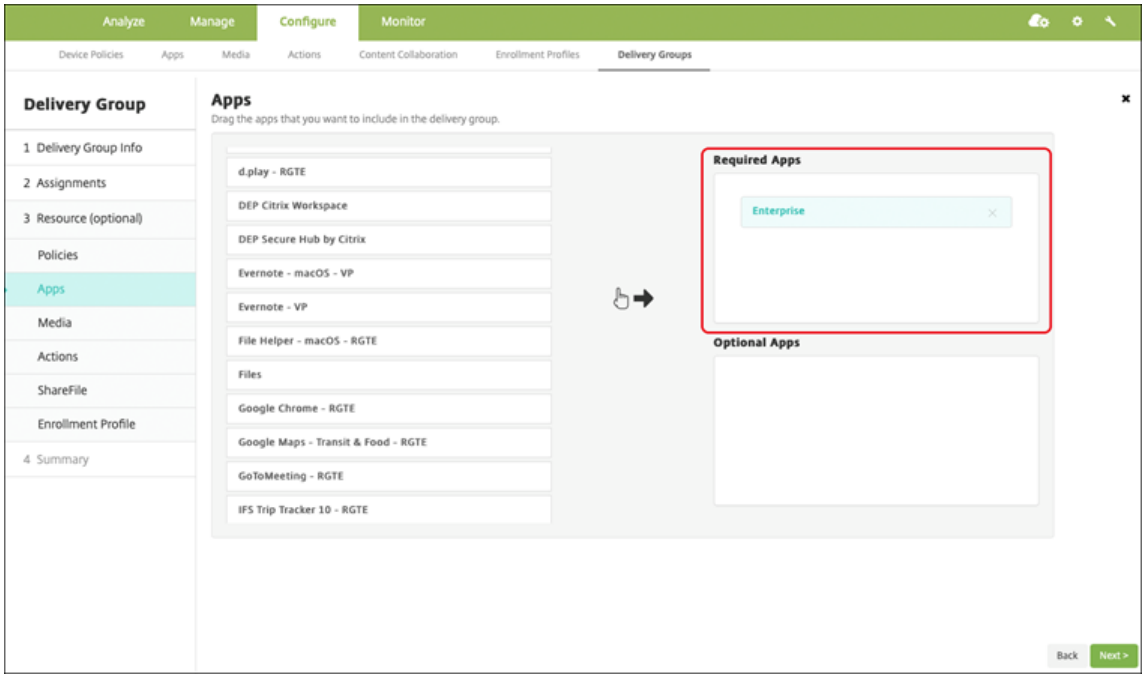
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- MDX 策略概览

8. 配置部署规则和应用商店配置。
9. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

步骤 **2**：配置应用程序部署

1. 导航到配置 **>** 交付组，然后选择您配置的交付组。单击编辑。
2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



3. 在摘要页面上，单击保存。
4. 在交付组页面上，选择交付组，然后单击部署。

企业应用程序

XenMobile 应用程序表示未使用 MAM SDK 或 MDX Toolkit 准备的专用应用程序。可以自己开发这些应用程序或直接从其他来源获取。要添加企业应用程序，您需要与该应用程序关联的 APK 文件。请务必关注 Google Best practices for private apps（专用应用程序的最佳实践）。

观看此视频以了解更多：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



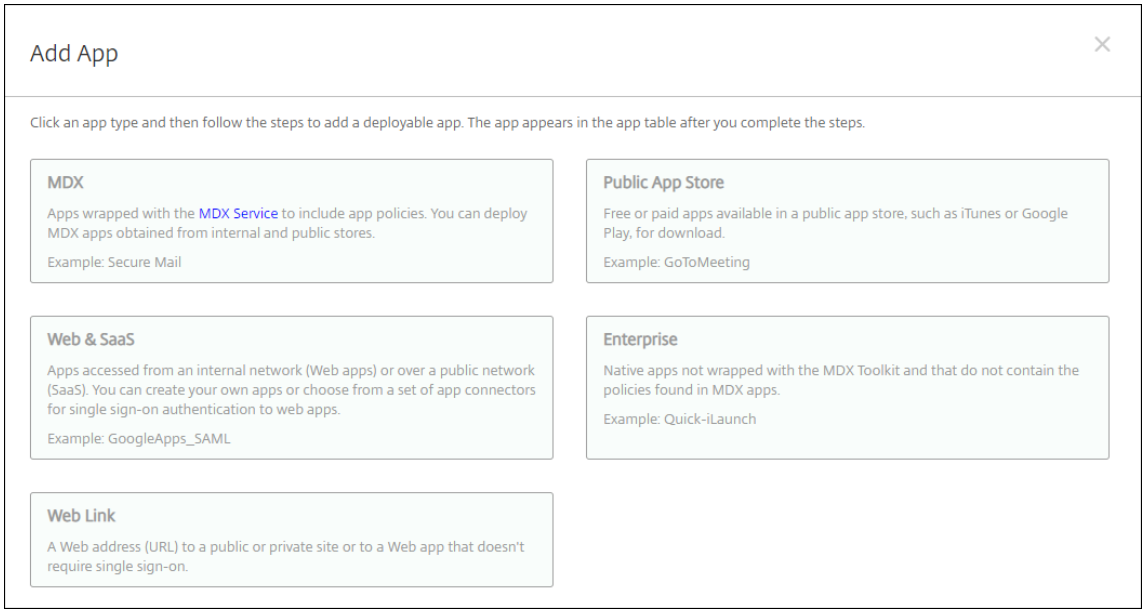
步骤 **1**：添加和配置应用程序

通过以下两种方法之一添加应用程序：

- 将应用程序直接发布到托管 Google Play 应用商店，然后将其作为托管 Play 应用商店应用程序添加到 Endpoint Management 控制台。参照 Google 文档，了解如何发布专用应用程序，然后按照托管应用商店应用程序部分中的步骤进行操作。
- 将应用程序作为企业应用程序添加到 Endpoint Management 控制台。请执行以下步骤：

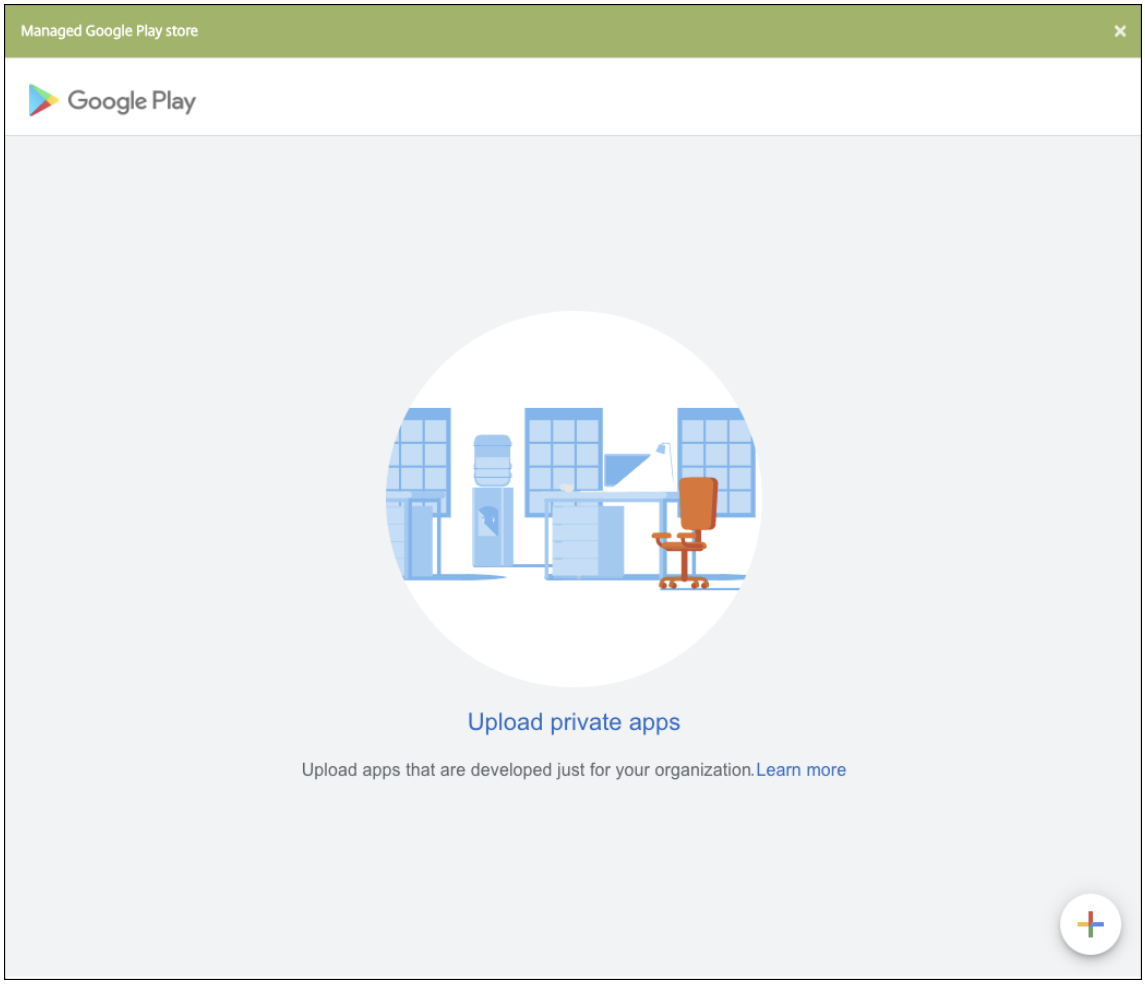
1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序。单击添加。此时将显示添加应用程序对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



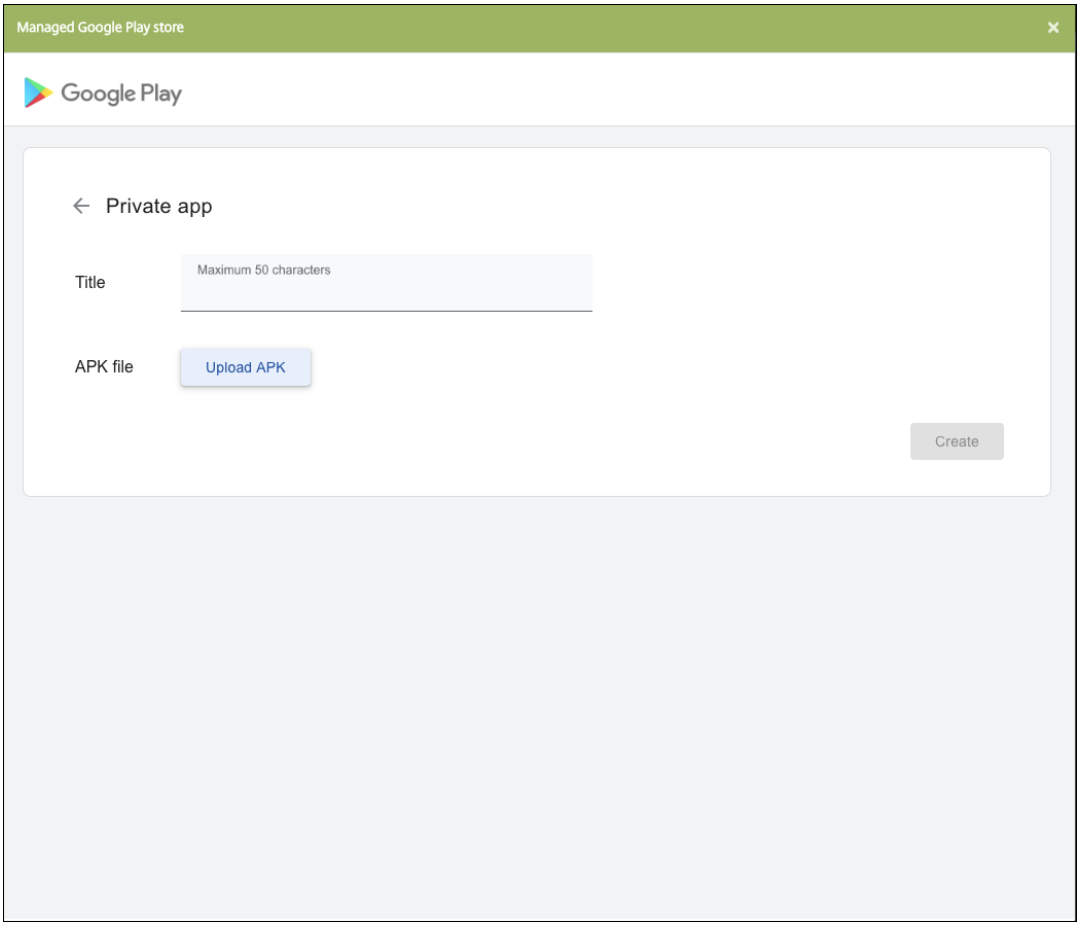
2. 单击企业。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
3. 选择 **Android Enterprise** 作为平台。
4. 上载按钮将打开托管 Google Play 应用商店。您无需注册开发者帐户即可发布专用应用程序。单击右下角的加号图标以继续。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



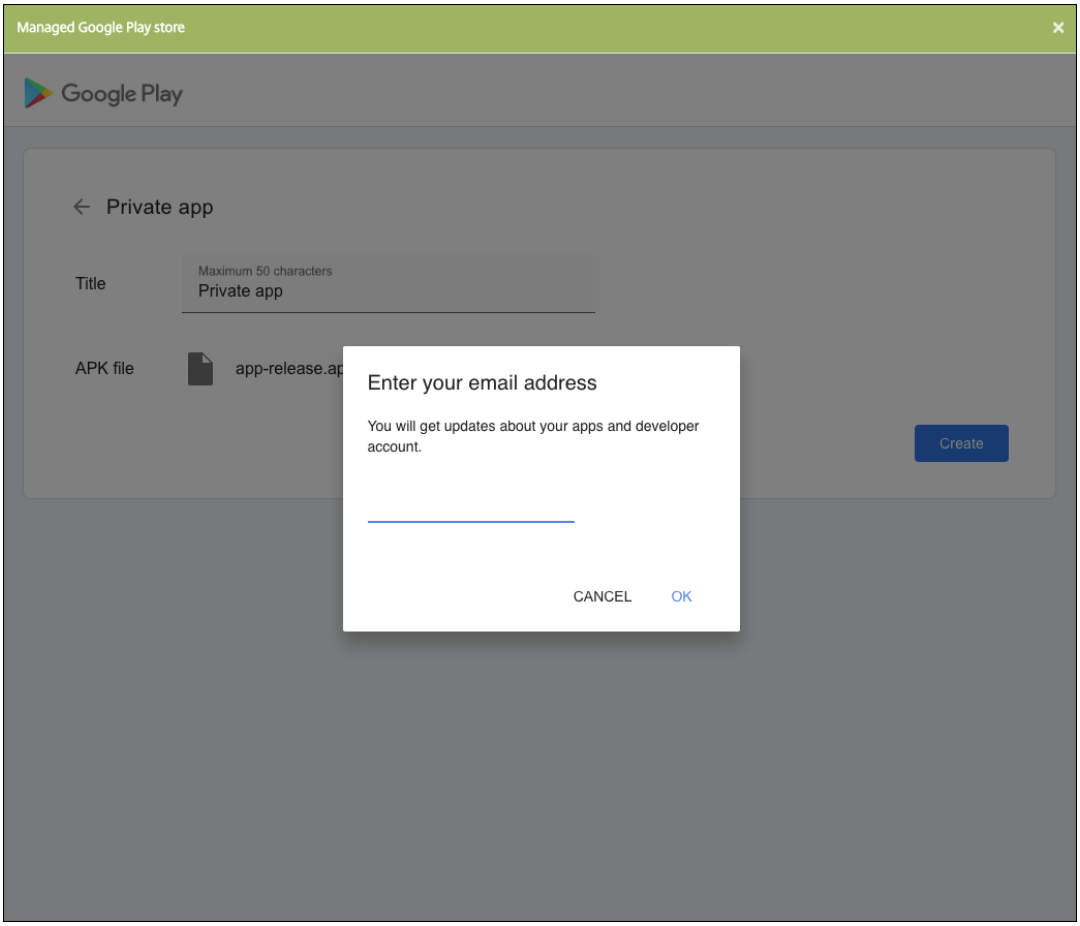
a) 键入应用程序的名称并上载.apk 文件。完成后，单击创建。您的专用应用程序最多可能需要 10 分钟才能发布。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



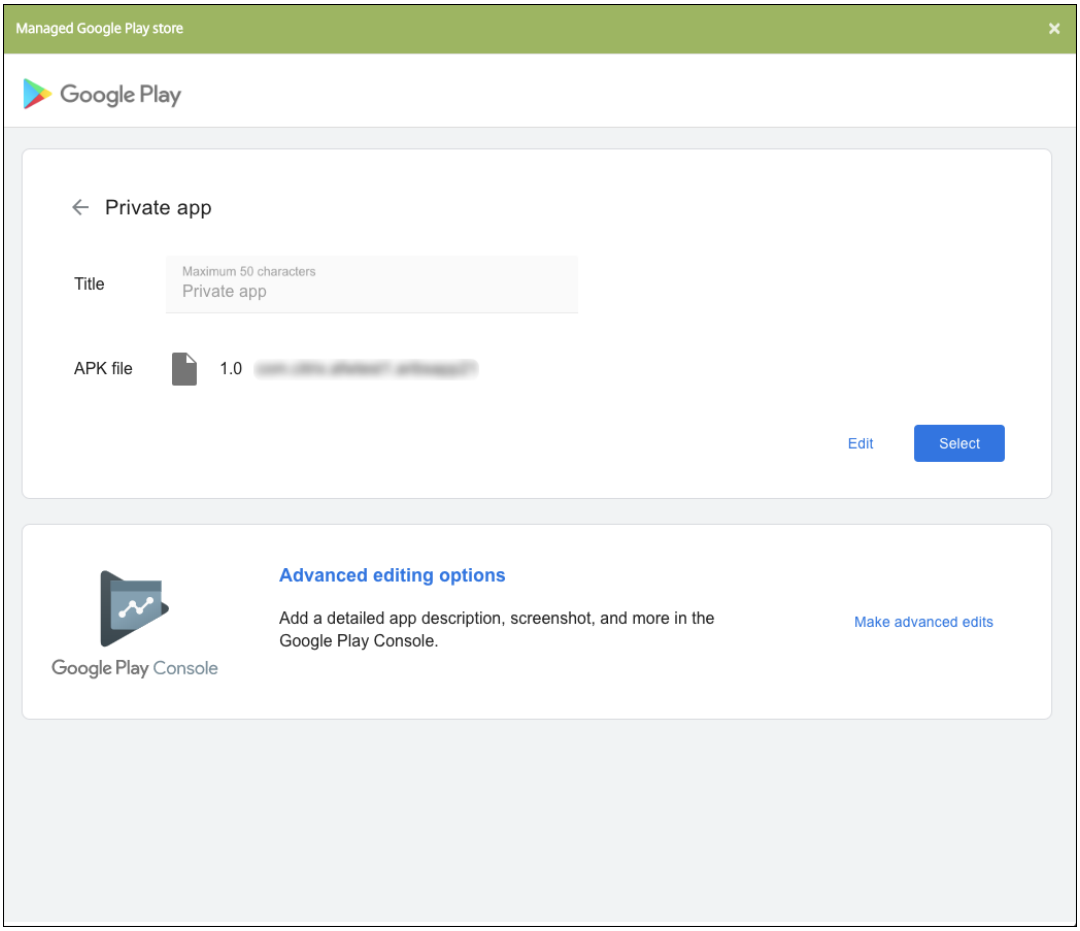
b) 输入电子邮件地址以获取有关您的应用程序的更新。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



c) 发布应用程序后，单击专用应用程序的图标。如果要添加应用程序说明、更改应用程序图标以及执行其他操作，请单击 **Make advanced edits**（进行高级编辑）。否则，请单击选择以打开应用程序信息页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

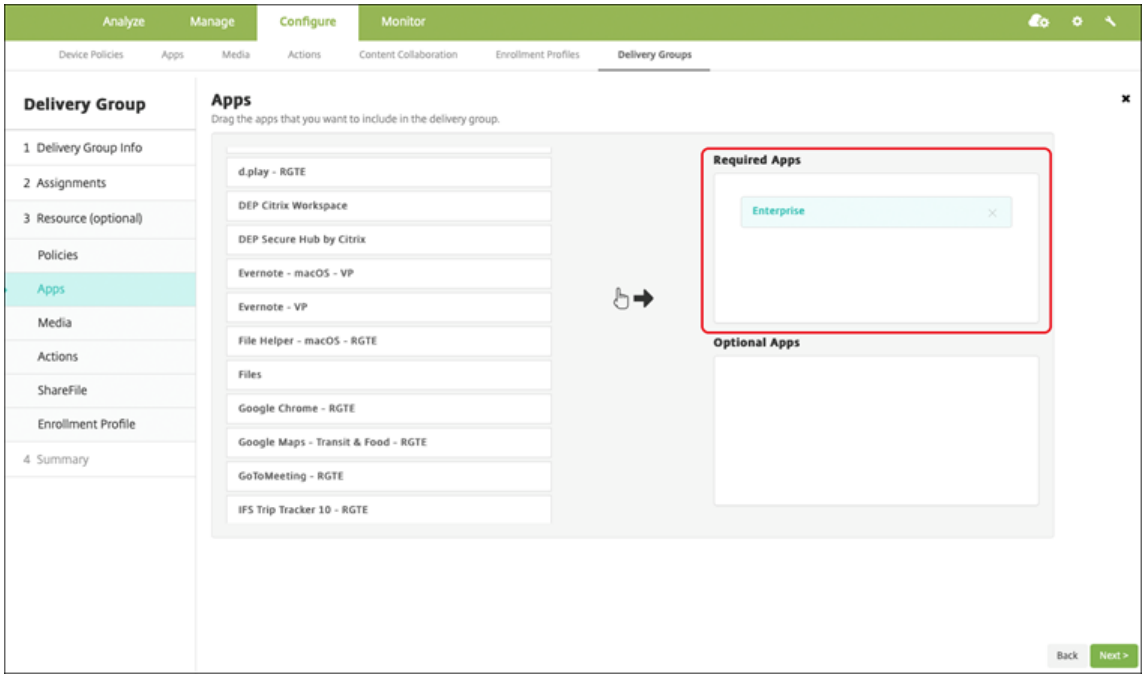


5. 单击下一步。此时将显示平台的应用程序信息页面。
6. 为平台类型配置设置，例如：
   - 文件名：（可选）键入应用程序的新名称。
   - 应用程序说明：（可选）键入应用程序的新说明。
   - 应用程序版本：无法更改此字段。
   - 软件包 **ID**：应用程序的唯一标识符。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
7. 配置部署规则和应用商店配置。
8. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

步骤 **2**：配置应用程序部署

1. 导航到配置 **>** 交付组，然后选择您配置的交付组。单击编辑。
2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 在摘要页面上，单击保存。
4. 在交付组页面上，选择交付组，然后单击部署。

启用了 **MDX** 的专用应用程序

要将 Android Enterprise 应用程序添加为启用了 MDX 的企业应用程序，请执行以下操作：

1. 创建专用 Android Enterprise 应用程序并为应用程序启用 MDX。
2. 将应用程序上载到 Endpoint Management 控制台。
   - 在托管 Google Play 应用商店中托管和发布应用程序。
   - 将应用程序作为企业应用程序添加到 Endpoint Management 控制台。
3. 将 MDX 文件添加到 Endpoint Management 中。

如果您决定通过 Google Play 应用商店托管和发布应用程序，请不要选择使用 Google 证书签名。请使用用于通过 MDX 启用应用程序的相同证书对应用程序进行签名。有关发布应用程序的详细信息，请参阅 Publishing your app（发布您的应用程序）和 Signing your app（对您的应用程序进行签名）上的 Google 文档。MAM SDK 不封装应用程序，因此它不需要用于开发应用程序的证书以外的证书。

有关通过 Google Play 控制台发布专用应用程序的详细信息，请参阅有关如何从 Play 控制台发布专用应用程序的 Google 文档。

要通过 Endpoint Management 发布应用程序，请参阅以下部分。

准备 **Android Enterprise** 应用程序

在创建 Android Enterprise 应用程序时，请务必遵循 Google 专用应用程序的最佳实践。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

创建 Android Enterprise 应用程序后，请将 MAM SDK 与应用程序集成，或者使用 MDX Toolkit 封装应用程序。然后，将生成的文件添加到 XenMobile。

可以通过上载更新后的.apk 文件来更新应用程序。以下步骤介绍了通过 MDX Toolkit 封装应用程序的过程。

1. 创建 Android Enterprise 应用程序并生成签名的.apk 文件。
2. 以下示例文件包含所有已知策略，其中一些策略可能不适用于您的环境。任何不可用的设置都将被忽略。使用以下参数创建 XML 文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
            NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
        <ActivePollPeriod>60</ActivePollPeriod>
        <PublicFileAccessLimitsList/>
        <CutAndCopy>Unrestricted</CutAndCopy>
        <Paste>Unrestricted</Paste>
        <DocumentExchange>Unrestricted</DocumentExchange>
        <OpenInExclusionList/>
        <InboundDocumentExchange>Unrestricted</
            InboundDocumentExchange>
        <InboundDocumentExchangeWhitelist/>
        <connectionSecurityLevel>TLS</connectionSecurityLevel>
        <DisableCamera>false</DisableCamera>
        <DisableGallery>false</DisableGallery>
        <DisableMicrophone>false</DisableMicrophone>
        <DisableLocation>false</DisableLocation>
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
35          <DisableSms>false</DisableSms>
36          <DisableScreenCapture>false</DisableScreenCapture>
37          <DisableSensor>false</DisableSensor>
38          <DisableNFC>false</DisableNFC>
39          <BlockLogs>false</BlockLogs>
40          <DisablePrinting>false</DisablePrinting>
41          <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
               MvpnNetworkAccess>
42          <MvpnSessionRequired>False</MvpnSessionRequired>
43          <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44          <DisableLocalhostConnections>false</
               DisableLocalhostConnections>
45          <CertificateLabel/>
46          <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47          <DefaultLoggerLevel>15</DefaultLoggerLevel>
48          <MaxLogFiles>2</MaxLogFiles>
49          <MaxLogFileSize>2</MaxLogFileSize>
50          <RedirectSystemLogs>false</RedirectSystemLogs>
51          <EncryptLogs>false</EncryptLogs>
52          <GeofenceLongitude>0</GeofenceLongitude>
53          <GeofenceLatitude>0</GeofenceLatitude>
54          <GeofenceRadius>0</GeofenceRadius>
55          <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56          <Authentication>OfflineAccessOnly</Authentication>
57          <ReauthenticationPeriod>480</ReauthenticationPeriod>
58          <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59      </Policies>
60  </MobileAppPolicies>
61  <!--NeedCopy-->
```

3. 使用 MDX Toolkit 封装应用程序。有关使用 MDX Toolkit 的信息，请参阅封装 Android 移动应用程序。

   将 **apptype** 参数设置为 **Premium**。在下面介绍的命令中使用上一步中的 XML 文件。

   如果您知道应用程序的应用商店 URL，请将 **storeURL** 参数设置为应用商店 URL。发布应用程序后，用户将从应用商店 URL 下载应用程序。

   下面是用于封装名为 SampleAEapp 的应用程序的 MDX Toolkit 命令的示例：

```
1  ```
2   java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
       Duser.variant
3   -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
4   -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
5   -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
6   -MinPlatform 5.0
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
  -keystore /MyKeystore
  -storepass mystorepwd123
  -keyalias key0
  -keypass mykeypwd123
  -storeURL "https://play.google.com/store/apps/details?id=
     SampleAEappPackage"
  -appType Premium
  -premiumMdxPolicies <Path to Premium policy XML>
<!--NeedCopy--> ```
```

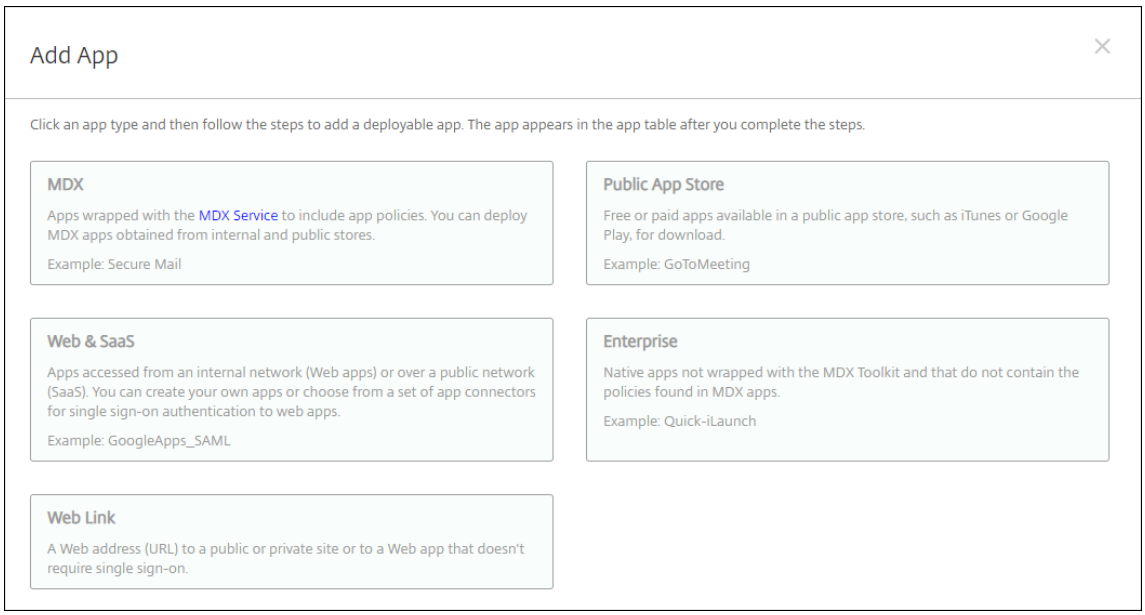
封装应用程序会生成一个封装的.apk 文件和一个.mdx 文件。

添加封装的**.apk** 文件

通过以下两种方法之一添加应用程序：

- 将应用程序直接发布到托管 Google Play 应用商店，然后将其作为托管 Play 应用商店应用程序添加到 Endpoint Management 控制台。参照 Google 文档，了解如何发布专用应用程序，然后按照托管应用商店应用程序部分中的步骤进行操作。
- 将应用程序作为企业应用程序添加到 Endpoint Management 控制台。请执行以下步骤：

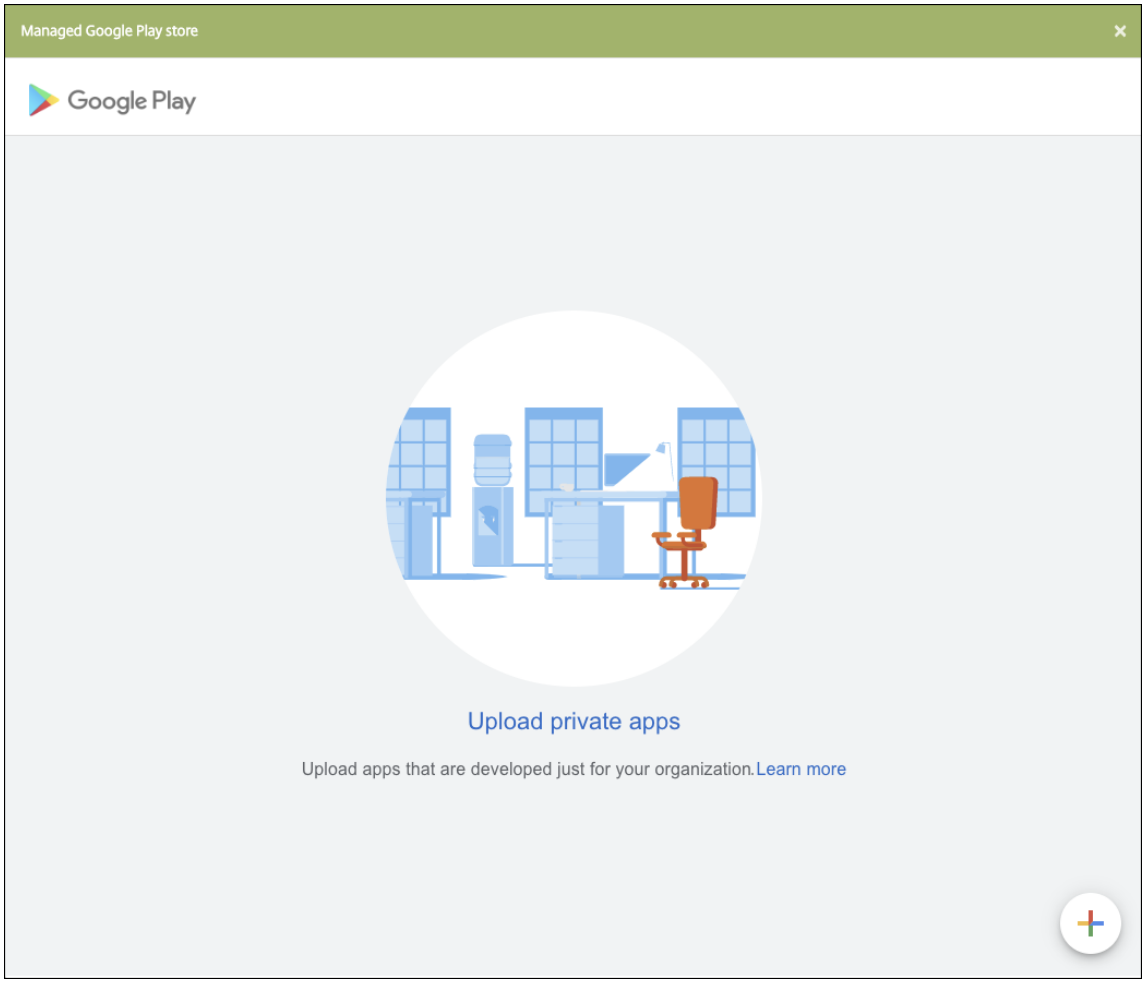
1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序。此时将打开应用程序页面。
2. 单击添加。此时将显示添加应用程序对话框。



3. 单击企业。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。

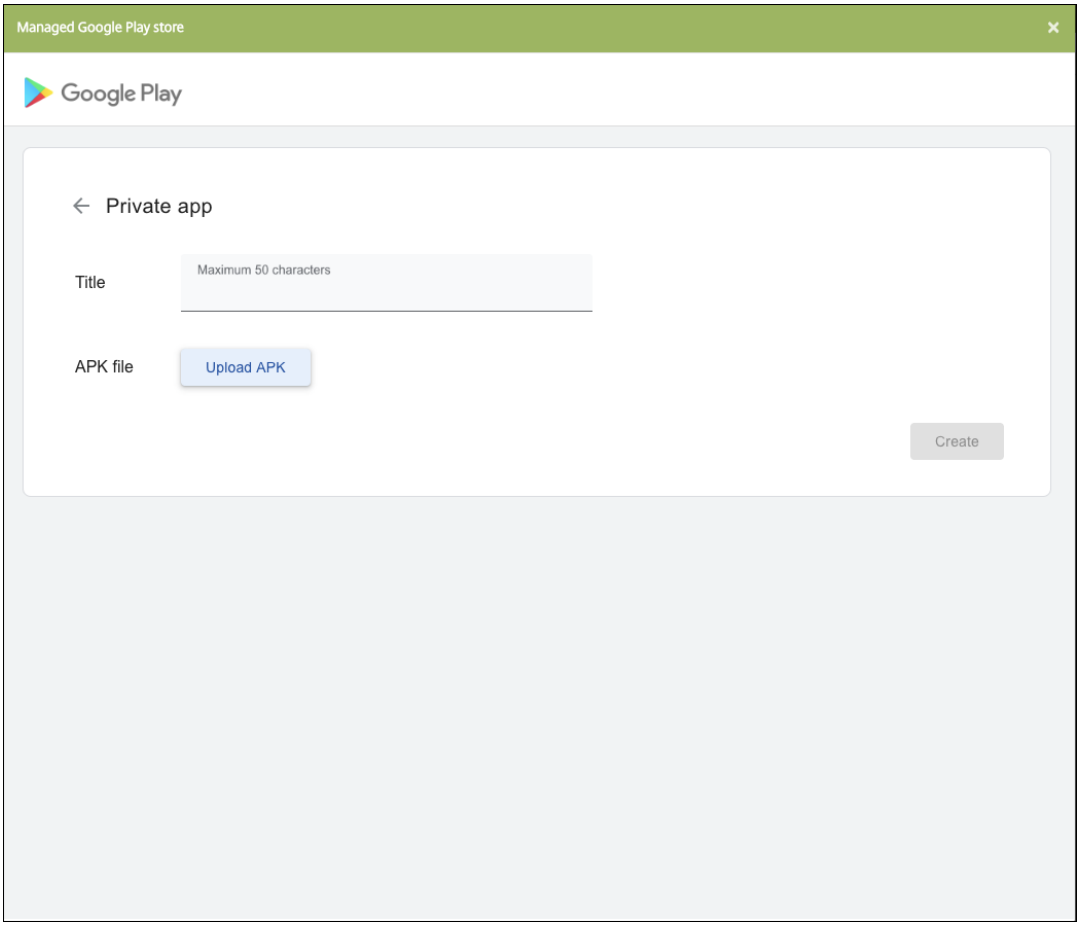
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

4. 选择 **Android Enterprise** 作为平台。
5. 上载按钮将打开托管 Google Play 应用商店。您无需注册开发者帐户即可发布专用应用程序。单击右下角的加号图标以继续。



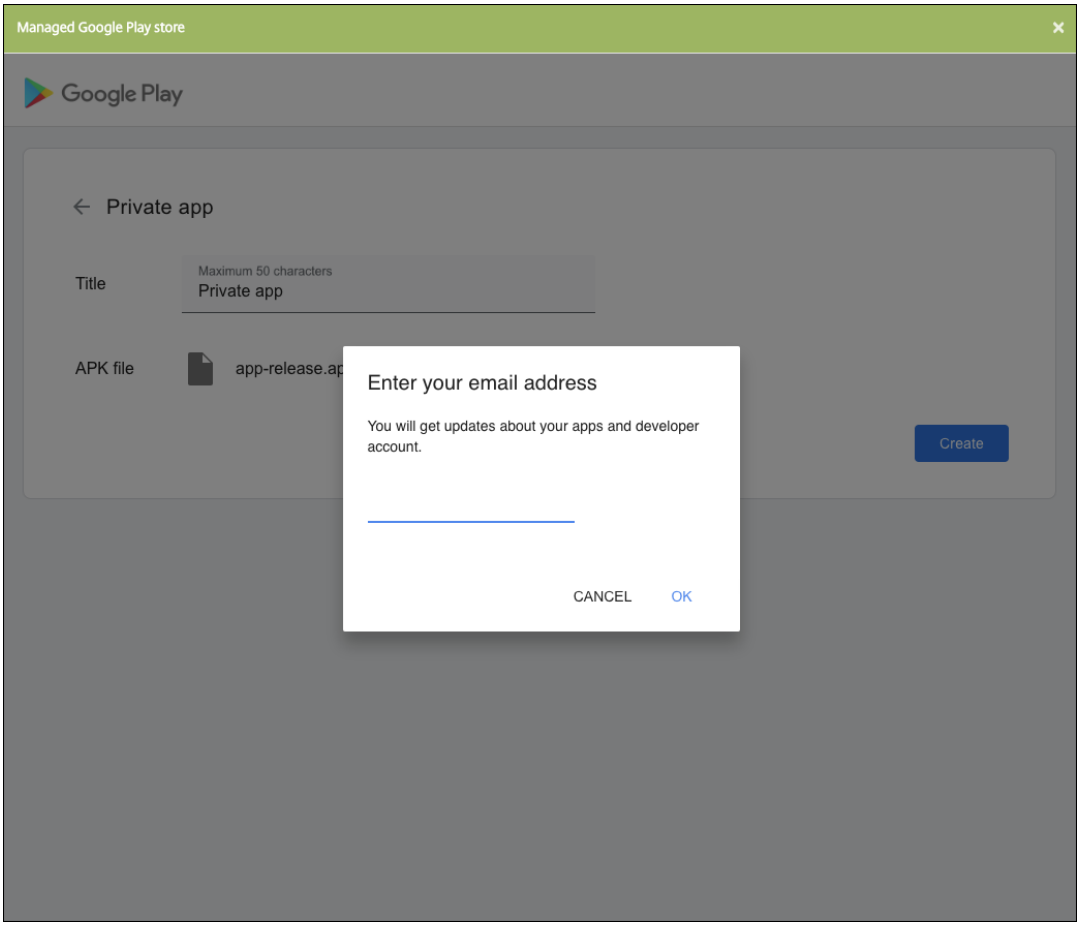
a) 键入应用程序的名称并上载.apk 文件。完成后，单击创建。您的专用应用程序最多可能需要 10 分钟才能发布。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



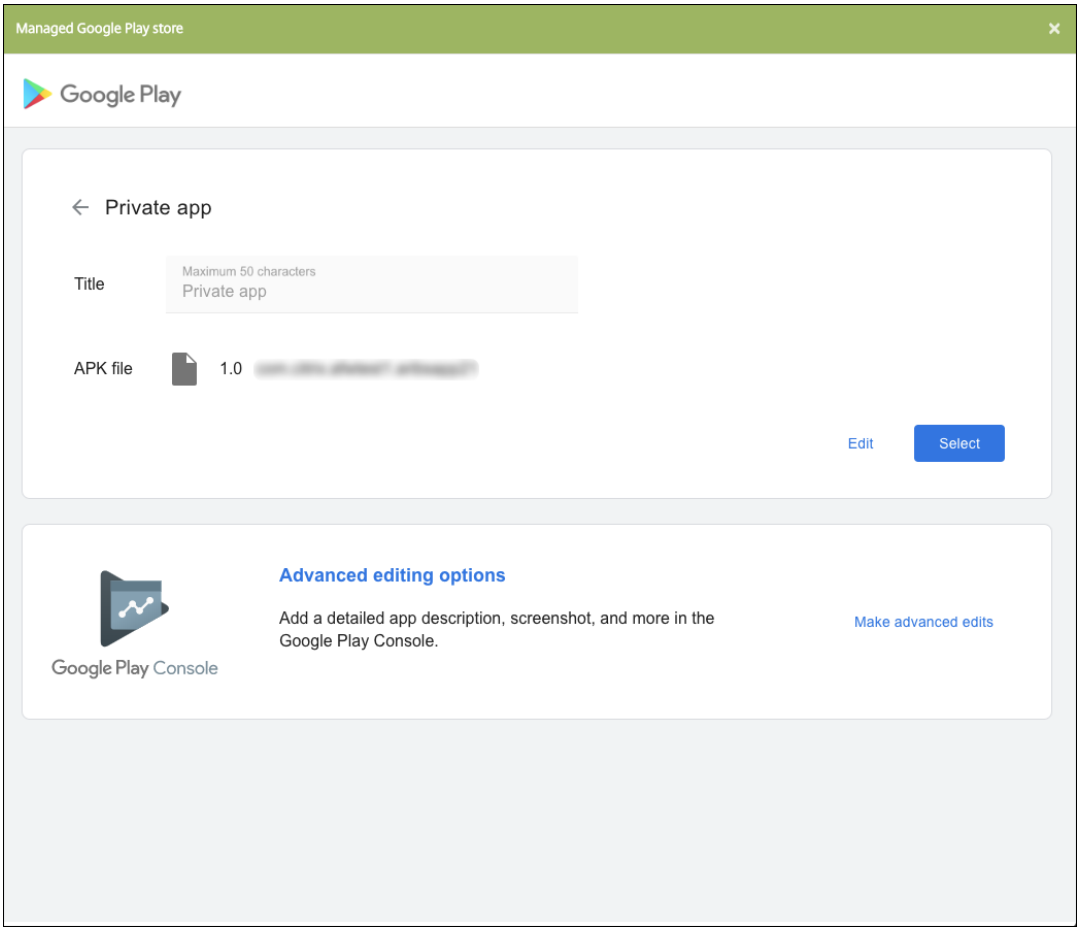
b) 输入电子邮件地址以获取有关您的应用程序的更新。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



c) 发布应用程序后，单击私有应用程序的图标，然后单击 选择以打开应用程序信息页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 单击下一步。此时将显示平台的应用程序信息页面。
7. 为平台类型配置设置，例如：
   - 文件名：（可选）键入应用程序的新名称。
   - 应用程序说明：（可选）键入应用程序的新说明。
   - 应用程序版本：无法更改此字段。
   - 软件包 **ID**：应用程序的唯一标识符。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
8. 配置部署规则和应用商店配置。
9. 在 企业应用程序页面中，单击 下一步。此时将显示审批页面。

   要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果无需审批工作流，可以跳至步骤 13。
10. 单击下一步。
11. 此时将显示交付组分配页面。无需在此页面上执行任何操作。添加.mdx 文件时，可以为此应用程序配置交付组

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

和部署计划。单击保存。

可选：添加或更改应用商店 **URL**

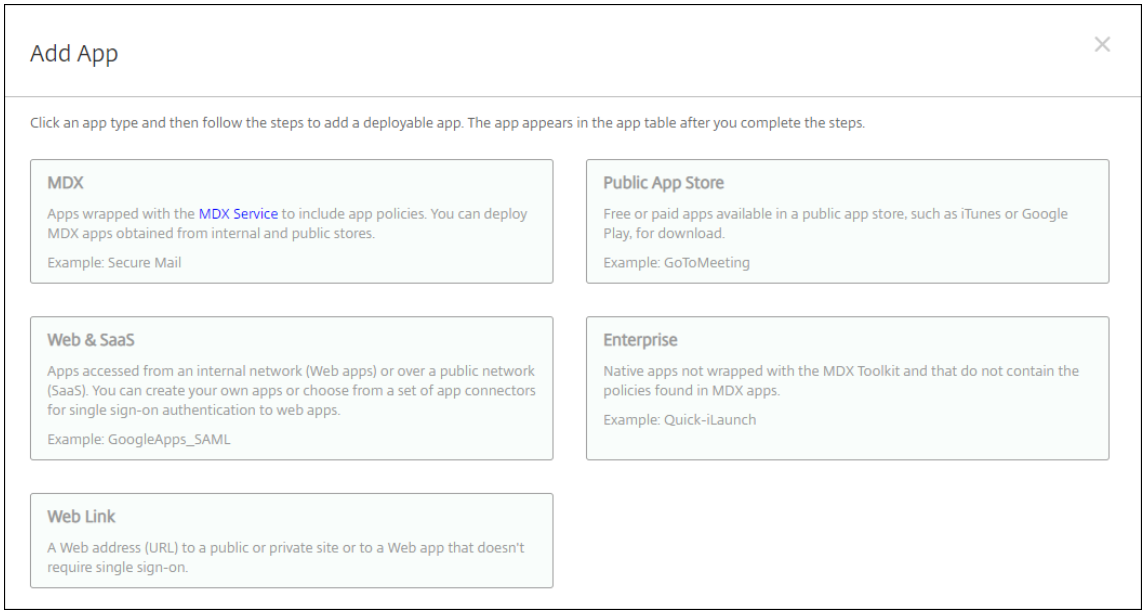
如果您在封装应用程序时不知道应用商店 URL，请立即添加应用商店 URL。

1. 查看托管 Google Play 应用商店中的应用程序。选择应用程序时，应用商店 URL 将显示在浏览器的地址栏中。从 URL 表单中复制应用程序的软件包名称。例如：`https://play.google.com/store/apps/details?id=SampleAEappPackage`。您复制的 URL 可能以 `https://play.google.com/work/` 开头。确保将 `work` 更改为 `store`。
2. 使用 MDX Toolkit 将应用商店 URL 添加到.mdx 文件中：

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
<!--NeedCopy-->
```

添加**.mdx** 文件

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序。单击添加。此时将显示添加应用程序对话框。

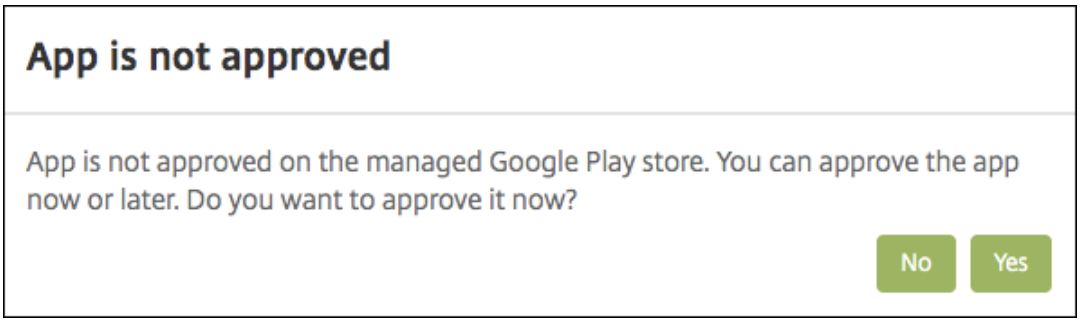


2. 单击 **MDX**。此时将显示 **MDX** 应用程序信息页面。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。该名称显示在应用程序表格中的应用程序名称下。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

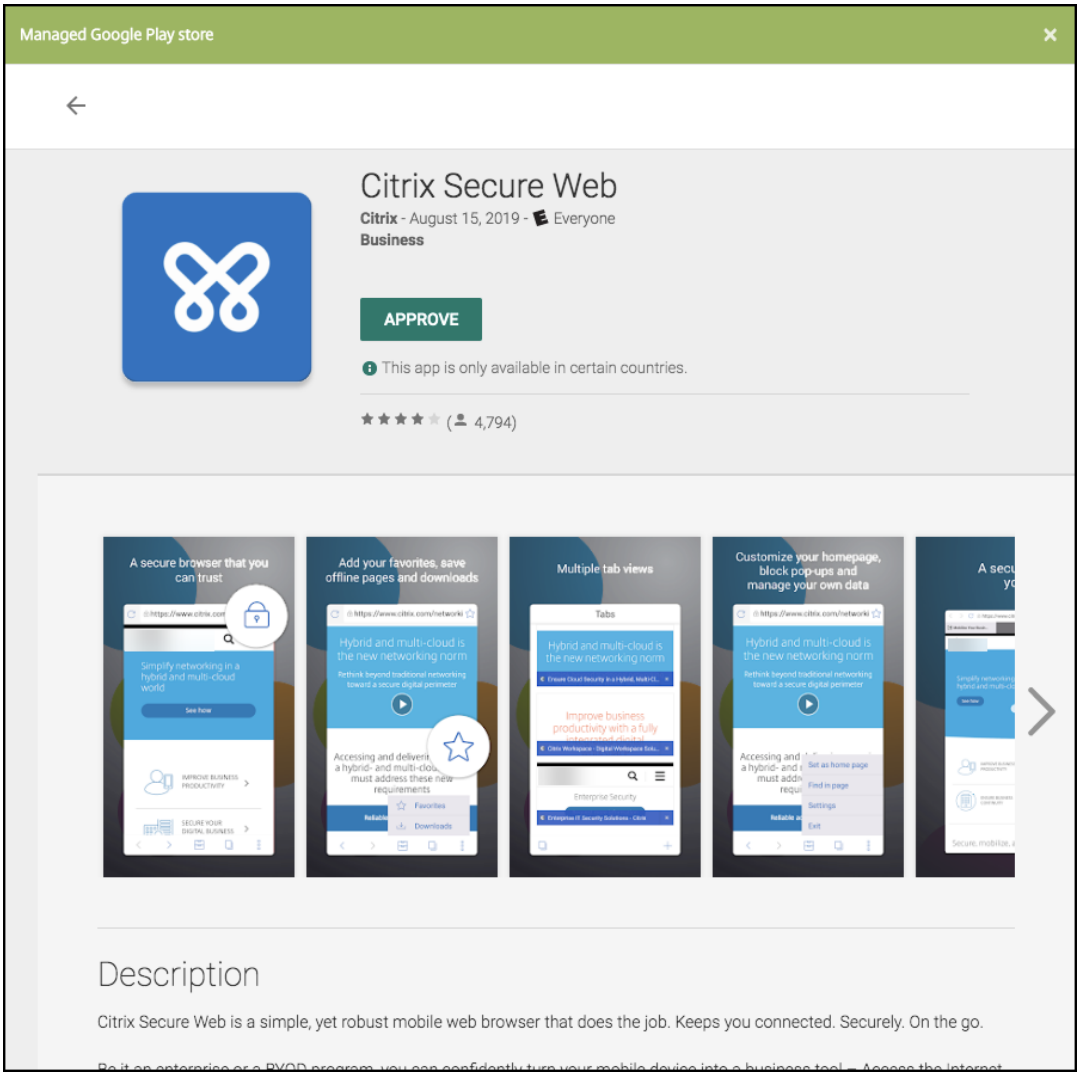
- 说明：键入应用程序的可选说明。

3. 选择 **Android Enterprise** 作为平台。
4. 单击上载并导航到 MDX 文件。Android Enterprise 仅支持使用 MDX Toolkit 封装的应用程序。
   - UI 会通知您附加的应用程序是否需要从托管 Google Play 应用商店获得批准。要在不离开 Citrix Endpoint Management 控制台的情况下审批应用程序，请单击是。



   在托管 Google Play 应用商店打开后，按照说明审批并保存应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



成功添加应用程序后，将显示应用程序详细信息页面。

5. 配置以下设置：

   - 文件名：键入与应用程序关联的文件名。
   - 应用程序说明：键入应用程序的说明。
   - 应用程序版本：（可选）键入应用程序版本号。
   - 软件包 **ID**：键入从托管的 Google Play 商店获取的应用程序包 ID。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。

6. 配置 **MDX** 策略。MDX 策略因平台而异，并且包含面向策略区域的选项，包括身份验证、设备安全和应用程序限制。在控制台中，每种策略都具有介绍此策略的提示。有关每种设备平台类型可用的应用程序策略的信息，请参阅：

   - MAM SDK 概述

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- MDX 第三方应用程序策略概览

7. 配置部署规则和应用商店配置。

   如果在设置 > 服务器属性中配置了计划后台部署密钥，则为始终启用的连接部署适用。

   始终启用选项：

   - 不适用于 iOS 设备
   - 不适用于开始使用版本 10.18.19 或更高版本的 Endpoint Management 的 Android 和 Android Enterprise 客户
   - 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用

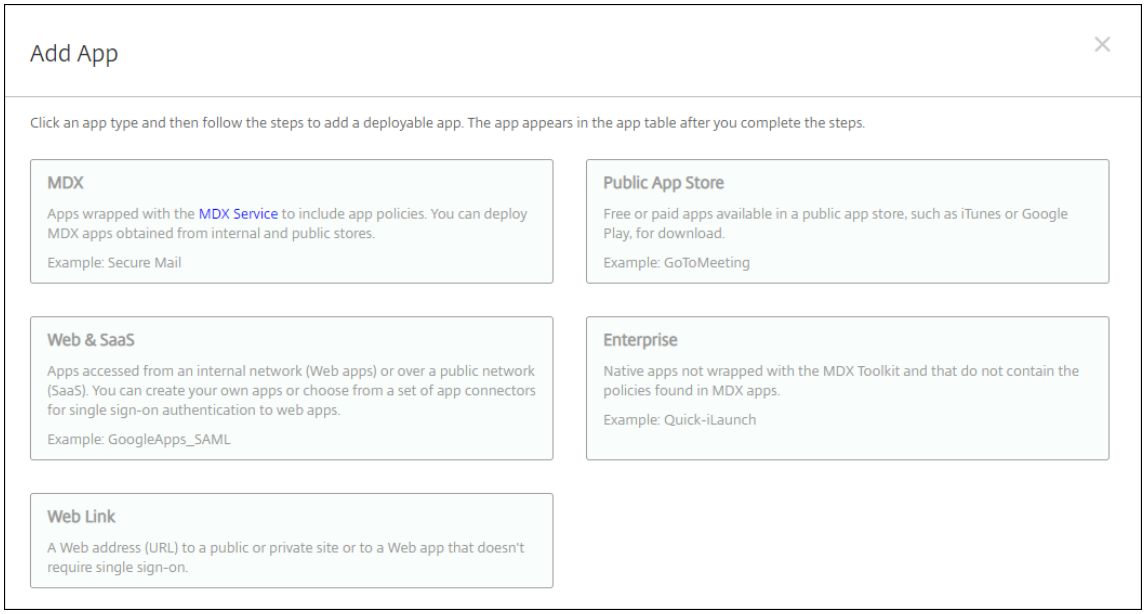
   配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

8. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

更新应用程序

要更新 Android Enterprise 应用程序，请封装并上载更新后的.apk 文件：

1. 使用 MAM SDK 或 MDX Toolkit 封装更新后的应用程序的.apk 文件。
2. 在 Endpoint Management 控制台中，单击配置 > 应用程序。此时将打开应用程序页面。

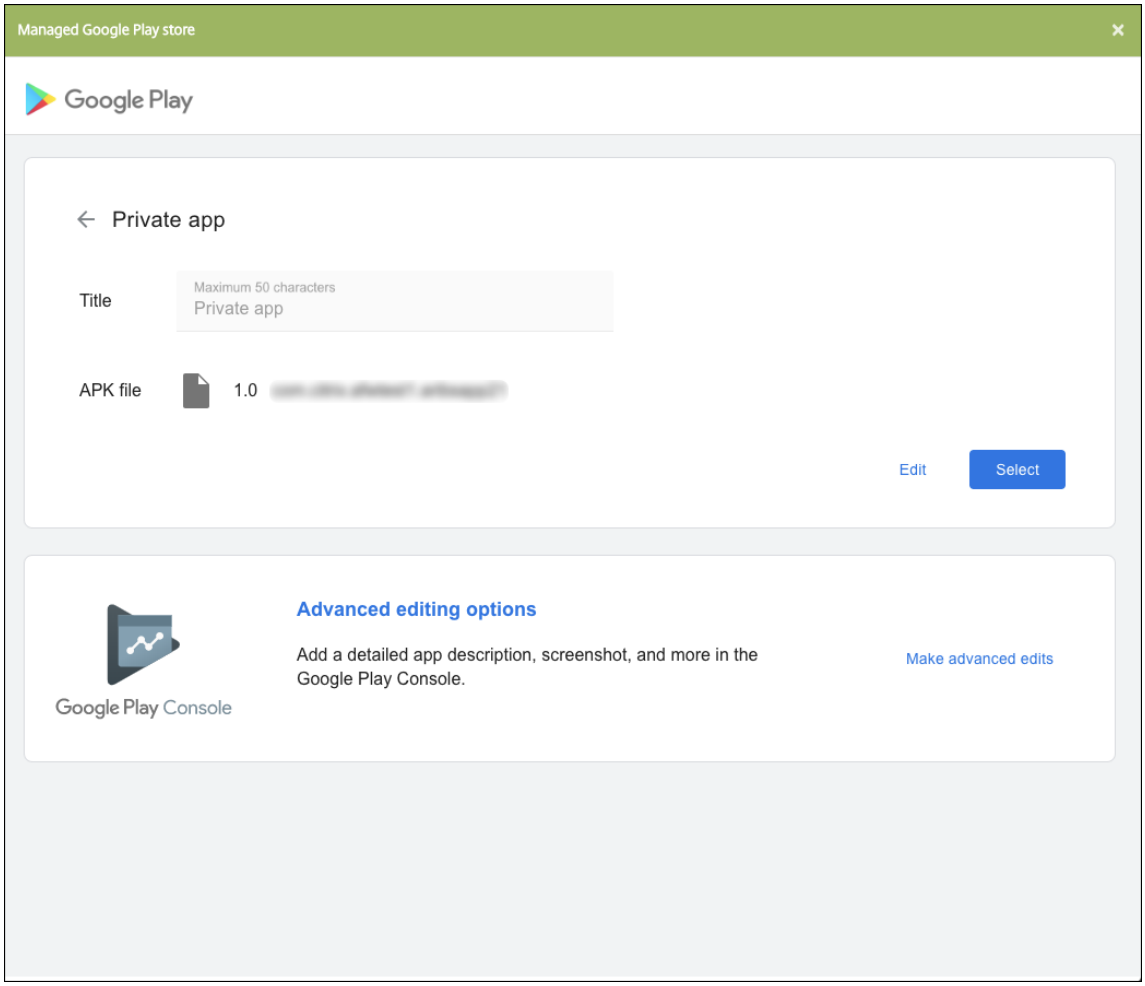


3. 单击添加。此时将显示添加应用程序对话框。
4. 单击企业。在应用程序信息窗格中，键入以下信息：

   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 选择 **Android Enterprise** 作为平台。
6. 单击下一步。将显示 企业应用程序页面。
7. 单击上载。
8. 在托管 Google Play 应用商店页面中，选择要更新的应用程序。
9. 在应用程序信息页面中，单击.apk 文件名旁边的编辑。



10. 导航到新.apk 文件并上载该文件。
11. 在托管 Google Play 应用商店页面中，单击保存。

适用于 **Google Workspace**（以前称为 **G Suite**）客户的旧版 **Android Enterprise**

December 3, 2021

谷歌 Workspace 客户必须使用旧版 Android Enterprise 版设置来配置旧版 Android Enterprise 版。谷歌最近将 G Suite 重命名为 Google Workspace。

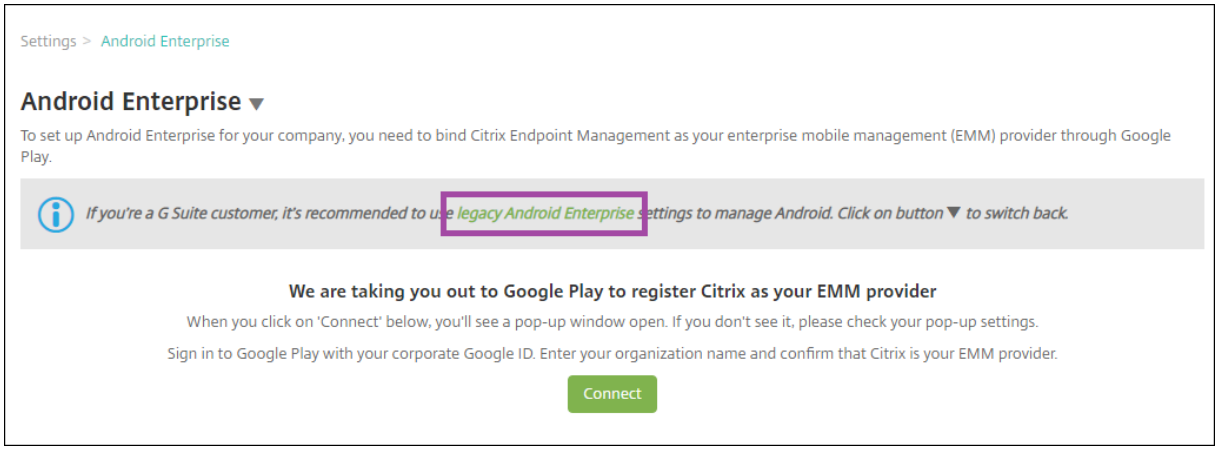
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

如果您的组织已使用 Google Workspace 向用户提供对谷歌应用的访问权限，则可以使用 Google Workspace 将 Citrix 注册为 EMM。如果您的组织使用 Google Workspace，则该组织拥有现有的企业 ID 和现有的用户 Google 帐号。要将 Endpoint Management 与 Google Workspace 结合使用，您可以与 LDAP 目录同步，然后使用谷歌目录 API 从谷歌检索谷歌帐户信息。由于这种类型的企业绑定到现有域，因此，每个域只能创建一个企业。要在 Endpoint Management 中注册设备，每个用户都必须使用其现有的 Google 帐户手动登录。除了您的 Google Workspace 套餐提供的任何其他谷歌服务之外，该帐户还允许他们访问托管的 Google Play。

旧版 Android Enterprise 的要求：

- 可公开访问的域
- Google 管理员帐户
- 具有托管配置文件支持的 Android 设备
- 安装了 Google Play 的 Google 帐户
- 用户设备上设置的工作配置文件

要开始配置旧版 Android Enterprise，请单击 Endpoint Management“设置” 的 **Android Enterprise** 页面中的旧版 **Android Enterprise**。



创建 **Android Enterprise** 帐户

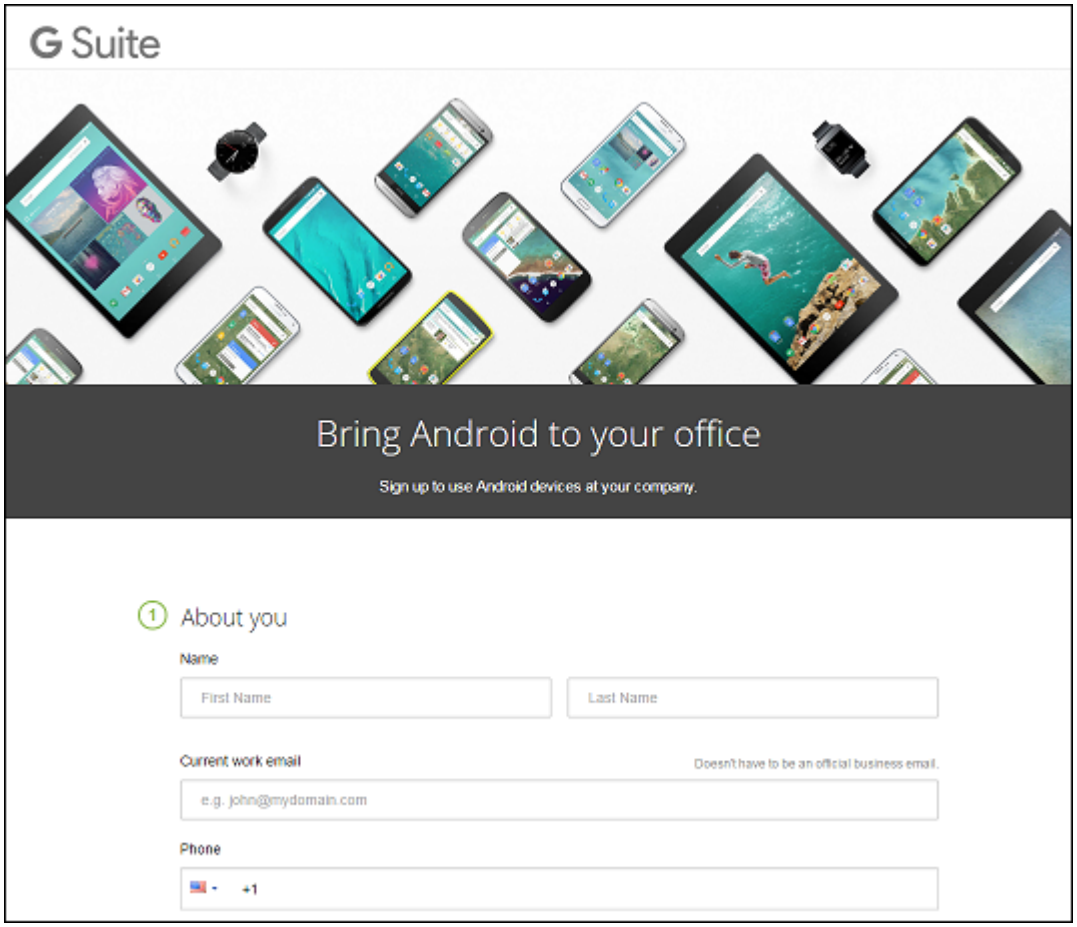
要设置 Android Enterprise 帐户，必须向 Google 验证您的域名。

如果已向 Google 验证您的域名，可以跳至此步骤：设置 Android Enterprise 服务帐户并下载 Android Enterprise 证书。

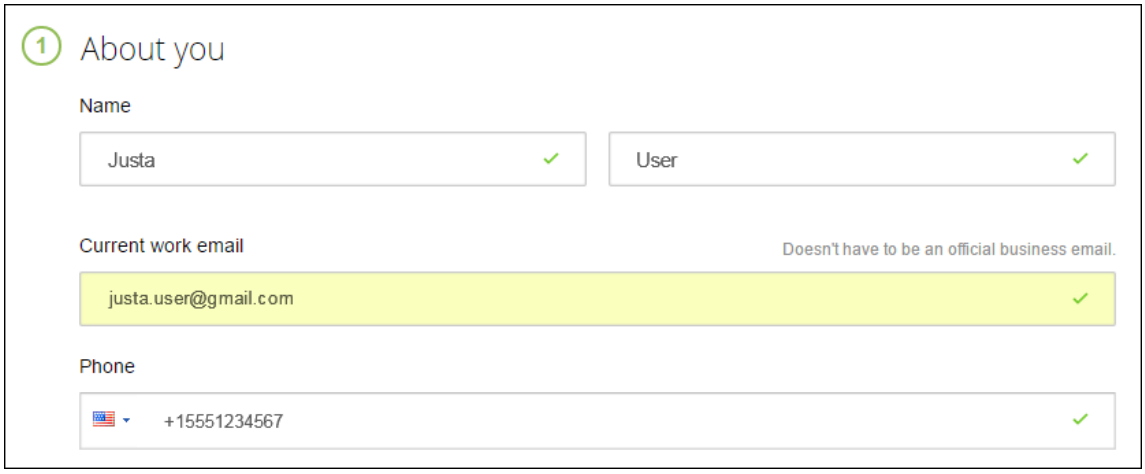
1. 导航到 https://gsuite.google.com/signup/basic/welcome。

   此时将显示以下页面，您可以在此页面中键入管理员和公司信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

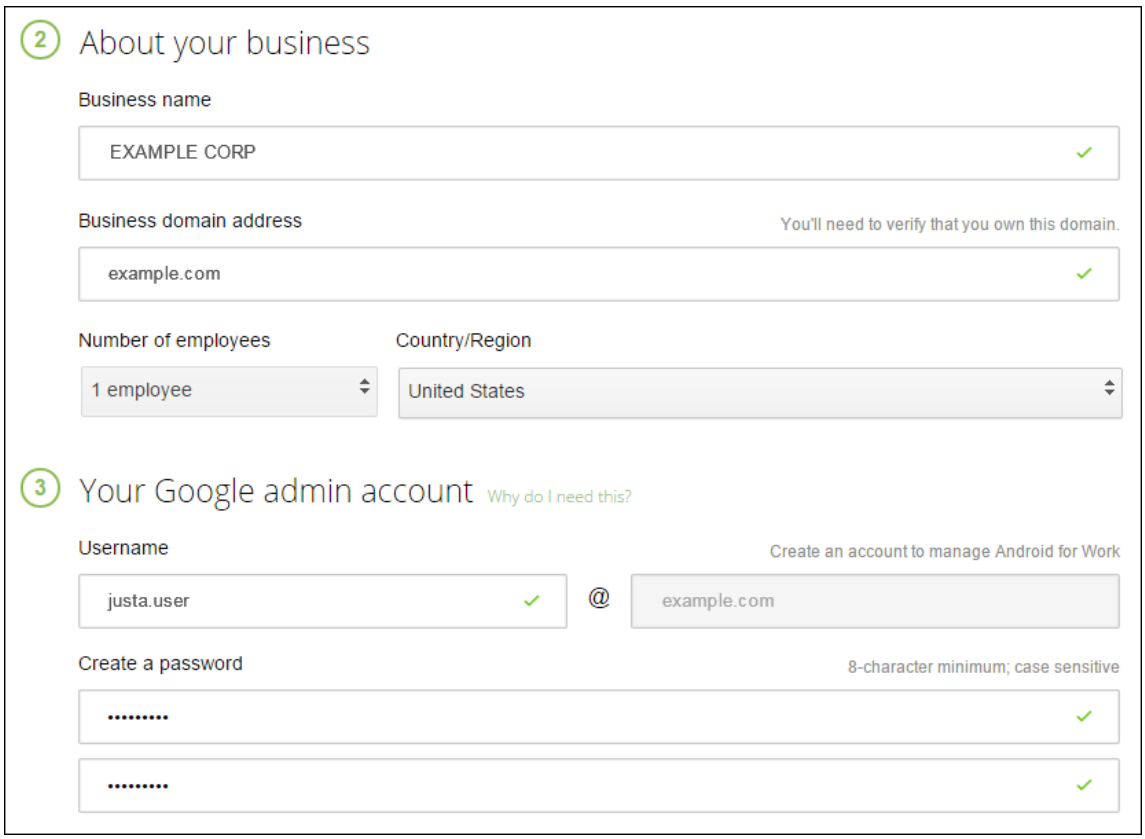


2. 键入管理员用户信息。



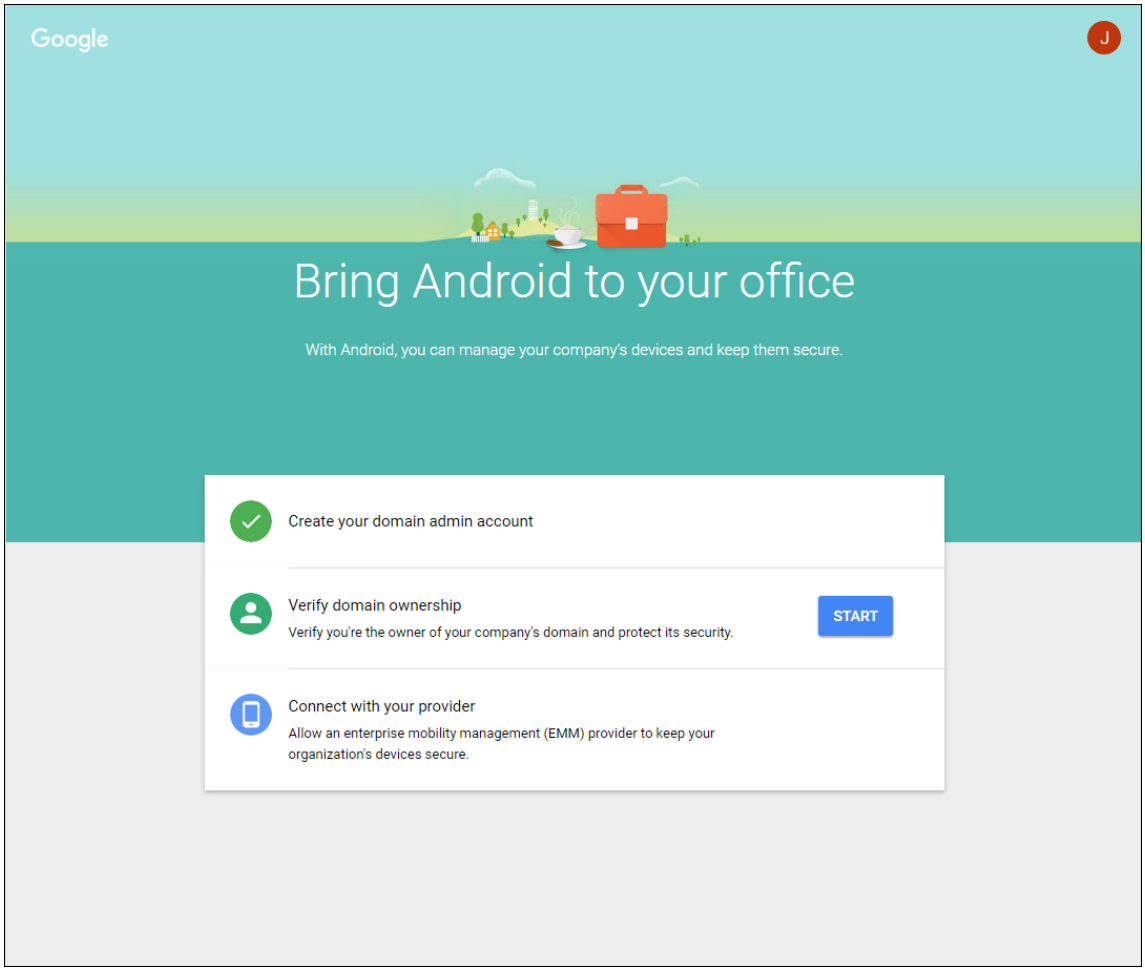
3. 键入您的公司信息（管理员帐户信息除外）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



此过程中的第一个步骤已完成，请继续查看下面的页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



验证域所有权

允许 Google 通过以下方式之一验证您的域：

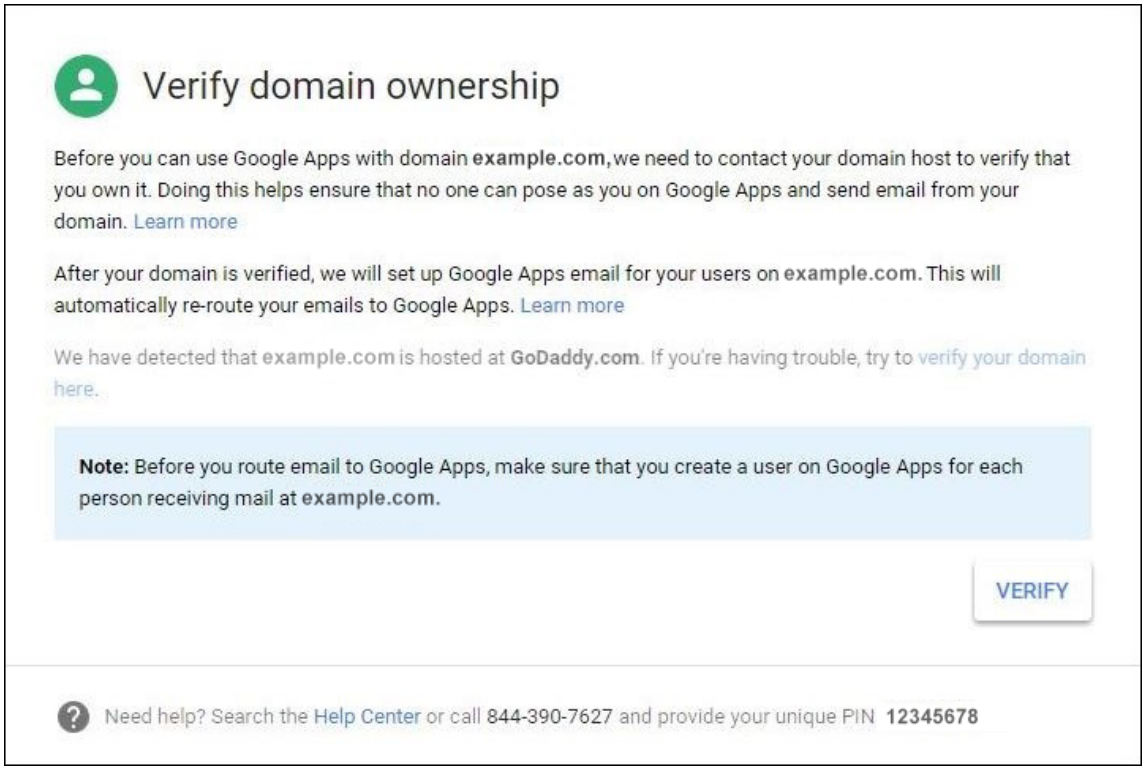
- 将 TXT 或 CNAME 记录添加到域主机的 Web 站点。
- 向域的 Web 服务器上载 HTML 文件。
- 向您的主页添加 `<meta>` 标记。Google 建议使用第一种方法。本文不包含验证域所有权的步骤，但您可以从以下网址找到所需的信息：https://support.google.com/a/answer/6248925。

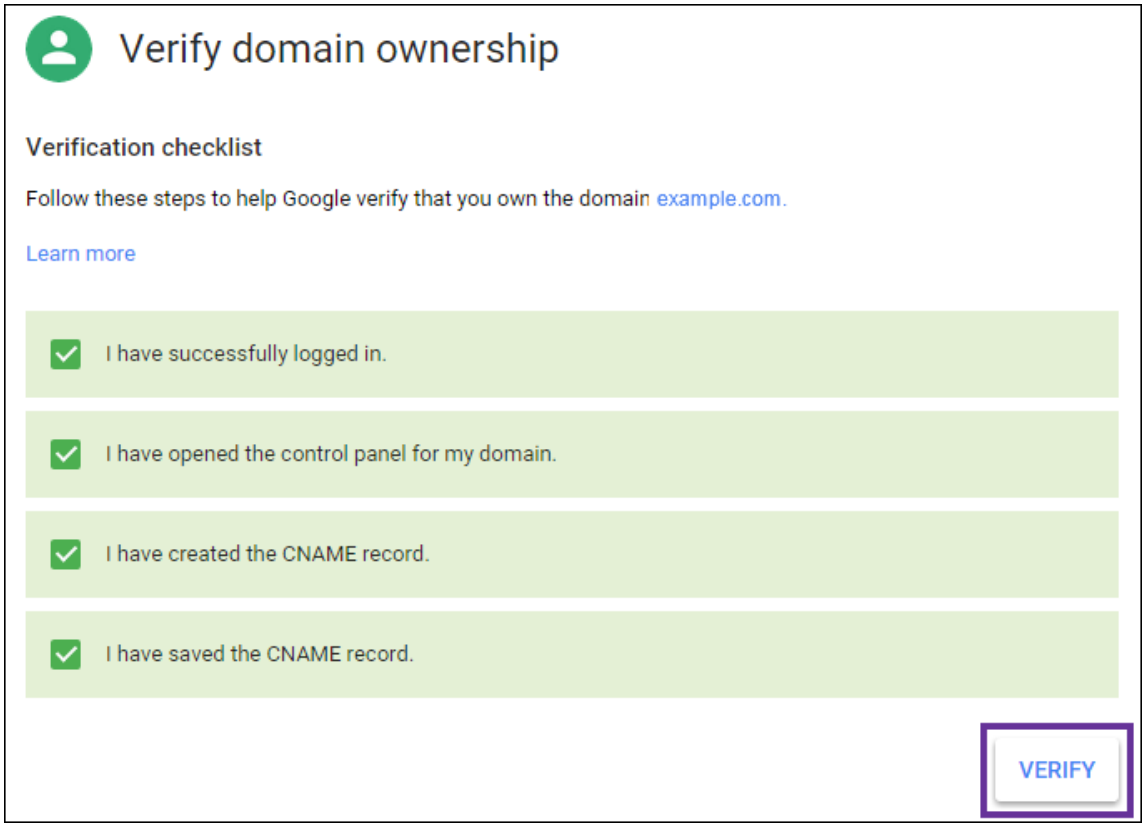
1. 单击 **Start**（开始）开始验证您的域。

   此时将显示 **Verify domain ownership**（验证域所有权）页面。请按照此页面上显示的说明验证您的域。

2. 单击 **Verify**（验证）。

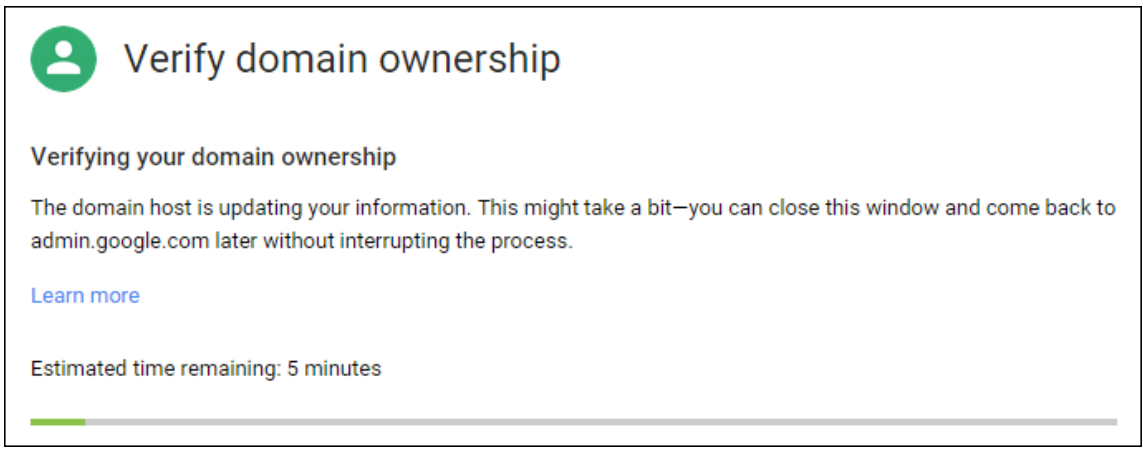
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



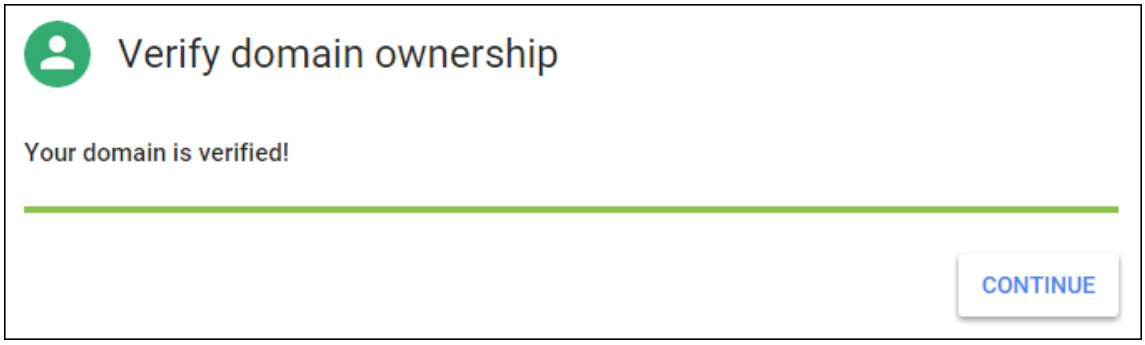


3. Google 验证您的域所有权。

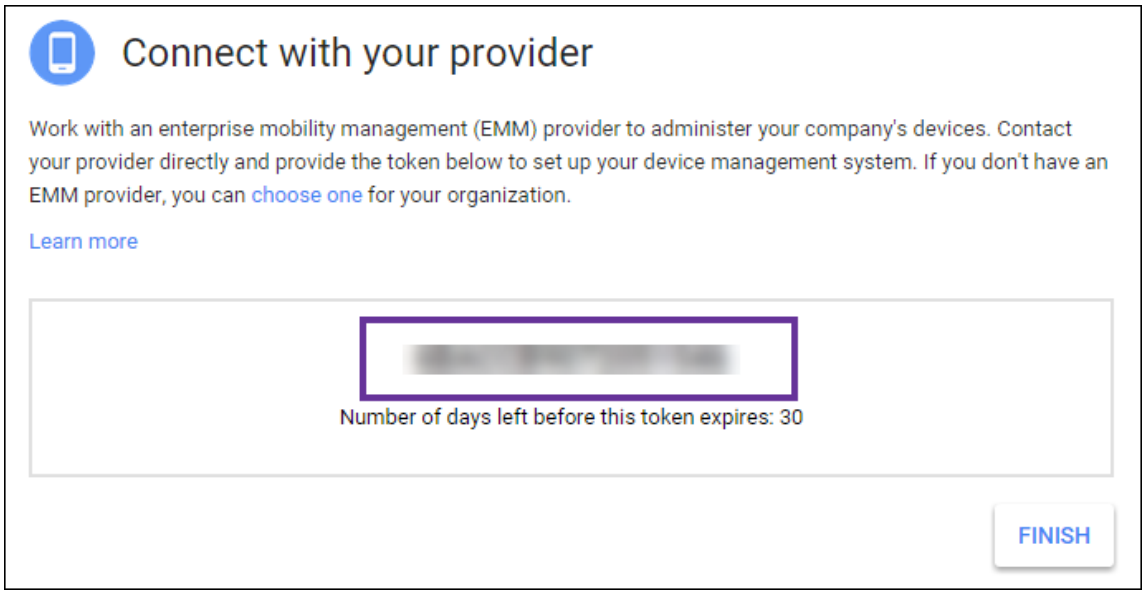
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 成功验证后，将显示以下页面。单击继续。



5. Google 创建一个需要向 Citrix 提供的 EMM 绑定令牌，您在配置 Android Enterprise 设置时需要使用该令牌。复制并保存该令牌；稍后的设置过程中需要使用该令牌。



6. 单击 **Finish**（完成）以完成 Android Enterprise 设置。此时将显示一个页面，指示您已成功验证您的域。

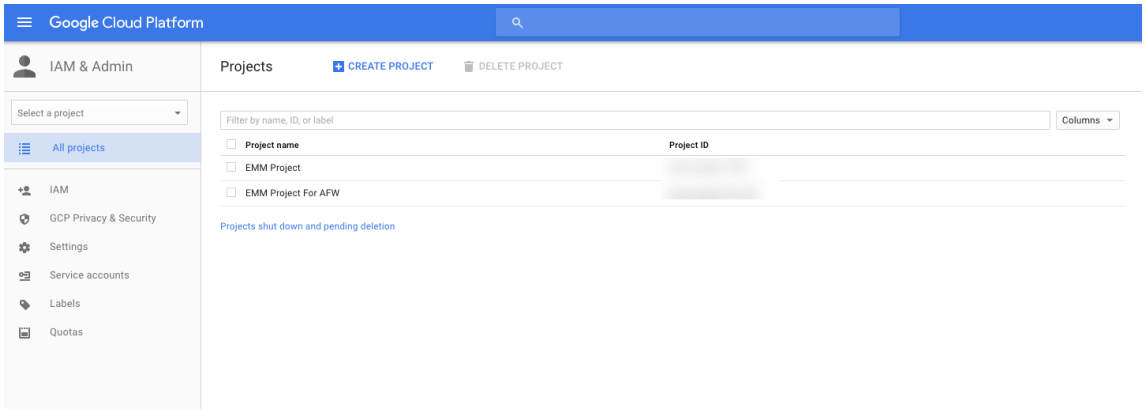
创建 Android Enterprise 服务帐户后，可以登录 Google 管理控制台管理您的移动性管理设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

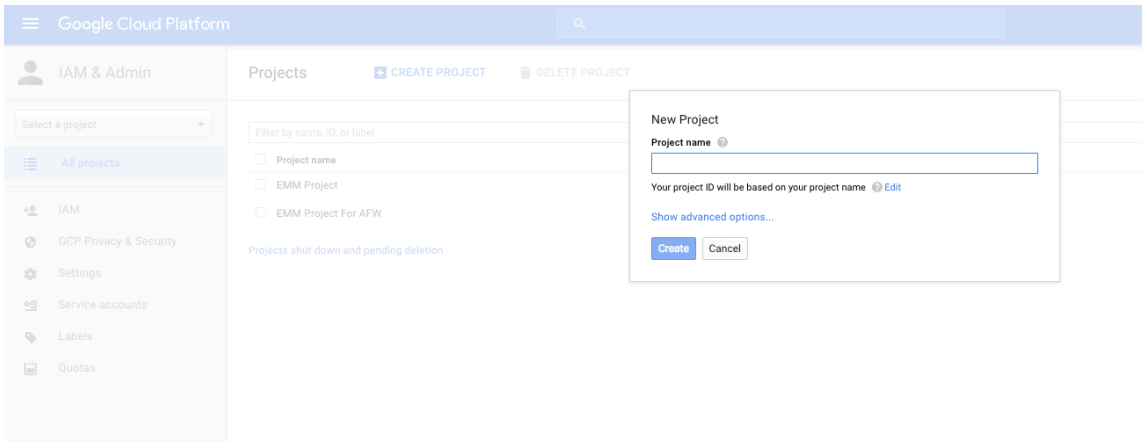
设置 **Android Enterprise** 服务帐户并下载 **Android Enterprise** 证书

要允许 Endpoint Management 联系 Google Play 和 Directory 服务，必须使用面向开发人员的 Google 项目门户创建新服务帐户。此服务帐户用于 Endpoint Management 与适用于 Android 的 Google 服务之间的服务器至服务器通信。有关使用的身份验证协议的详细信息，请访问 https://developers.google.com/identity/protocols/OAuth2ServiceAccount。

1. 在 Web 浏览器中，访问 https://console.cloud.google.com/project 并使用您的 Google 管理员凭据登录。
2. 在“项目”列表中，单击“创建项目”。

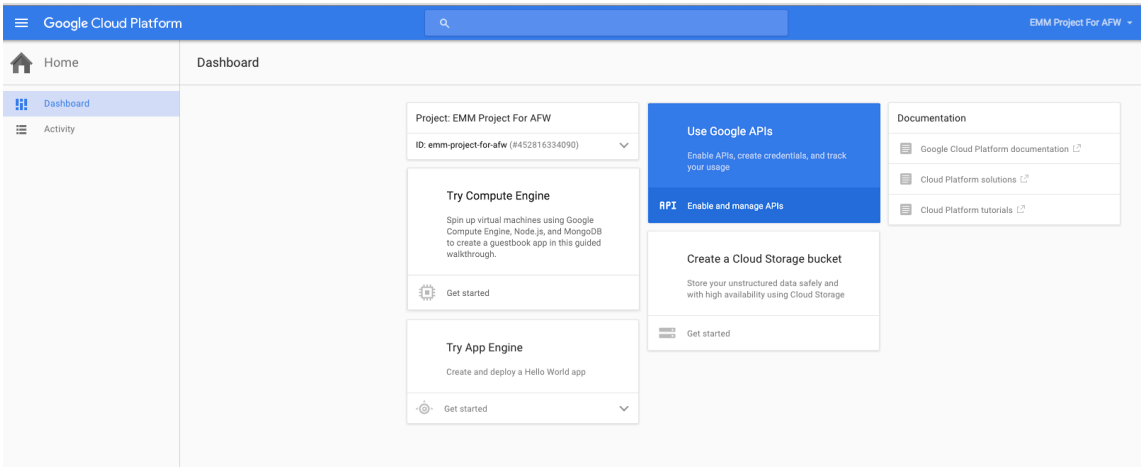


3. 在 **Project name**（项目名称）中，键入项目的名称。

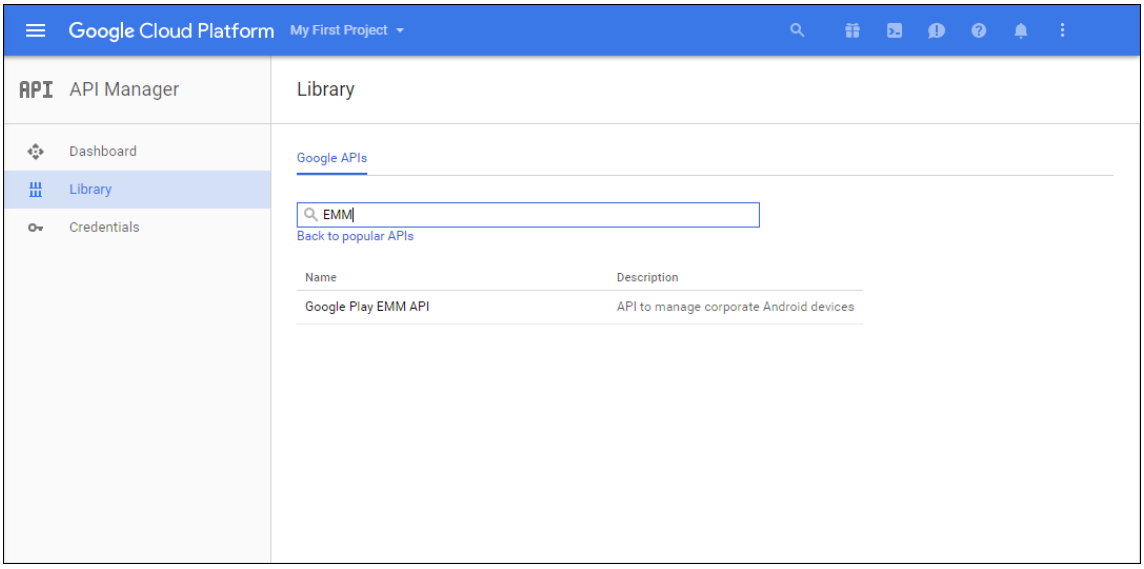


4. 在“Dashboard”（控制板）上，单击 **Use Google APIs**（使用 Google API）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

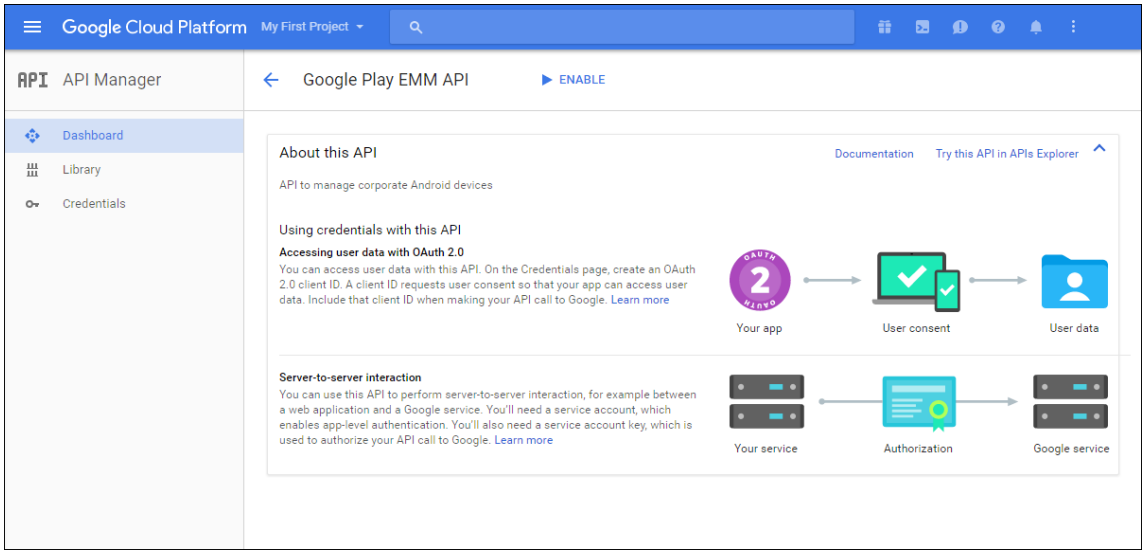


5. 单击 **Library**（库），在 **Search**（搜索）中，键入 **EMM**，然后单击搜索结果。

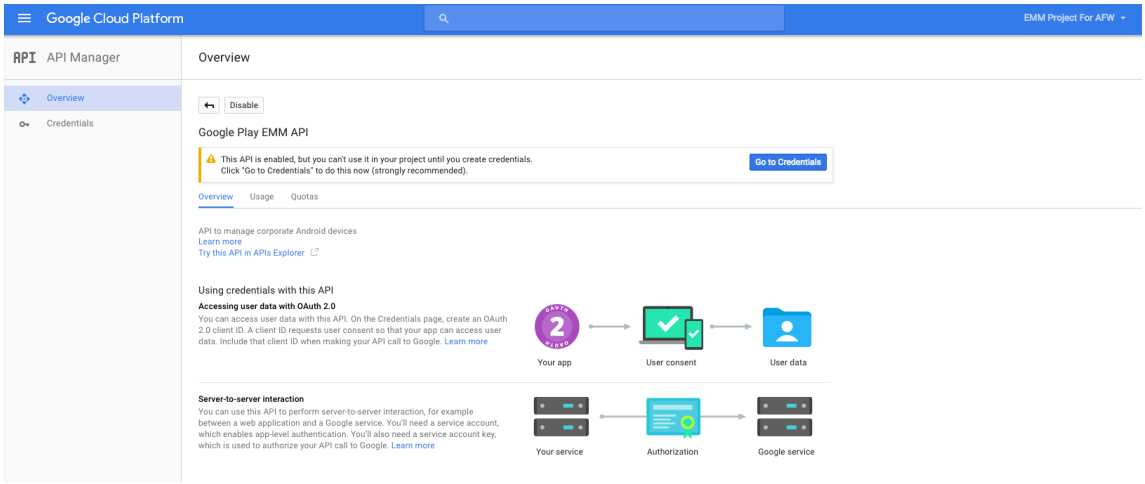


6. 在 **Overview**（概览）页面上，单击 **Enable**（启用）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

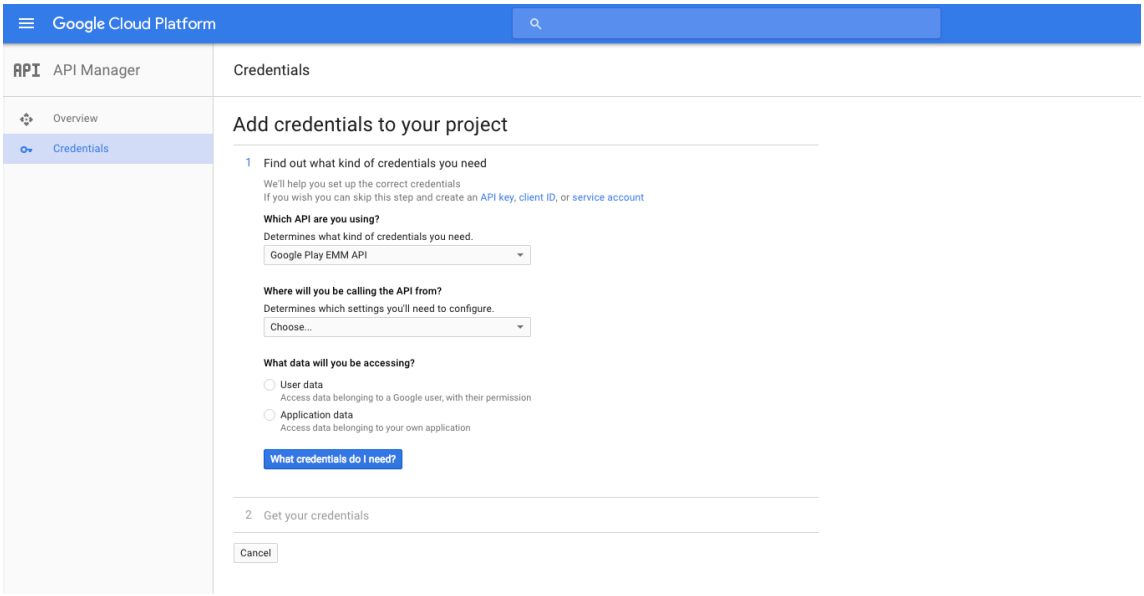


7. 在 **Google Play EMM API** 旁边，单击 **Go to Credentials**（转至凭据）。

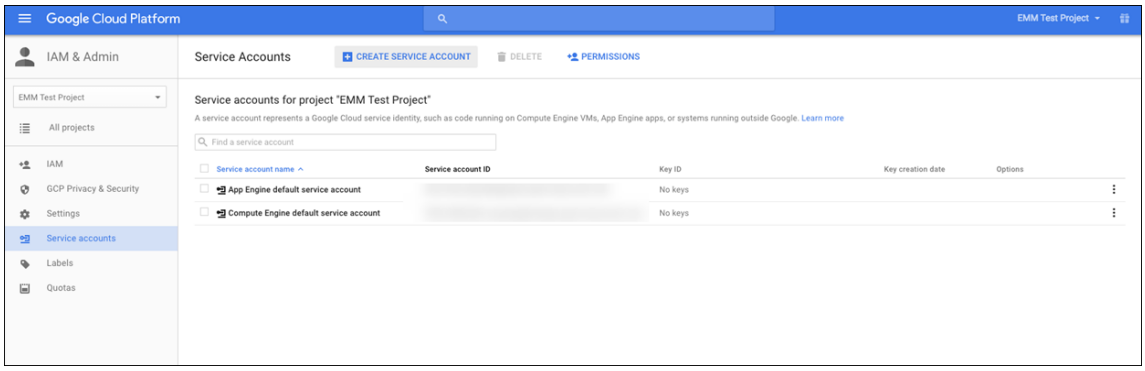


8. 在 **Add credentials to our project**（向我们的项目中添加凭据）列表中，在步骤 1 中单击 **service account**（服务帐户）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

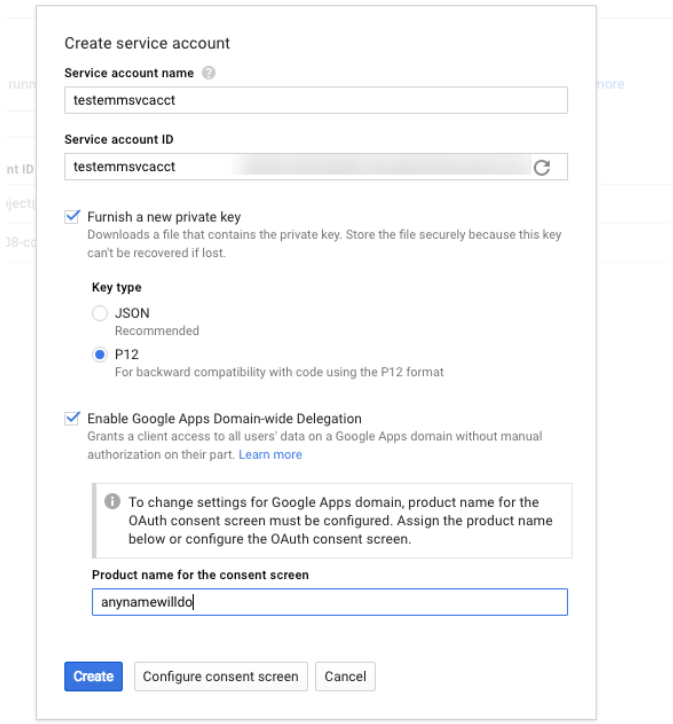


9. 在 **Service Accounts**（服务帐户）页面上，单击 **Create Service Account**（创建服务帐户）。



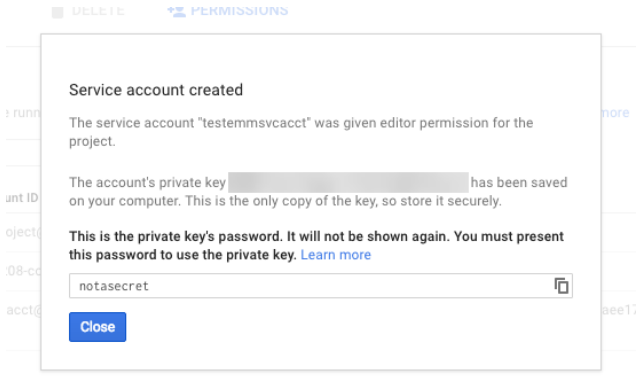
10. 在 **Create service account**（创建服务帐户）中，命名该帐户，然后选中 **Furnish a new private key**（提供新私钥）复选框。单击 **P12**，选中 启用 **Google Apps** 域范围内的委派复选框，然后单击 创建。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

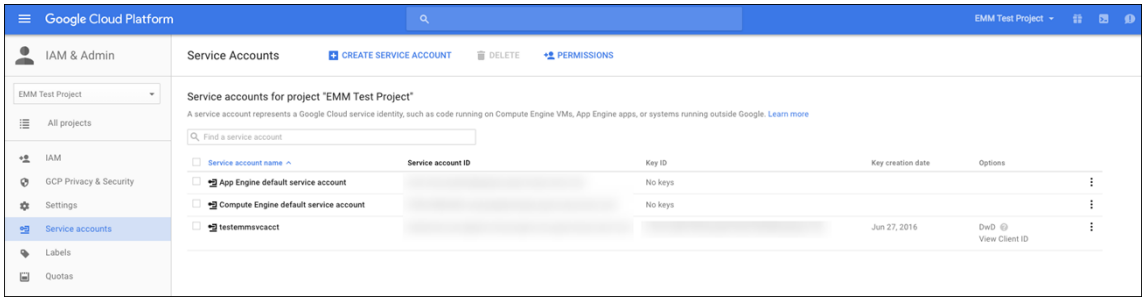


证书（P12 文件）将下载到您的计算机。请务必将该证书保存到一个安全的位置。

11. 在 **Service account created**（已创建服务帐户）确认屏幕上，单击 **Close**（关闭）。

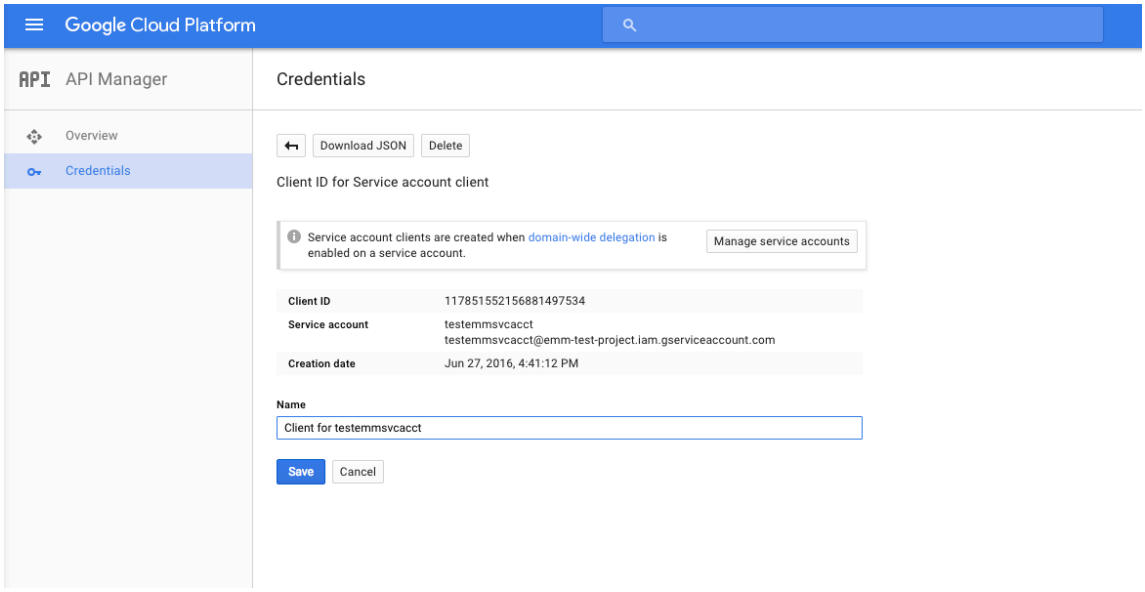


12. 在 **Permissions**（权限）中，单击 **Service accounts**（服务帐户），然后在您的服务帐户对应的 **Options**（选项）下方，单击 **View Client ID**（查看客户端 ID）。

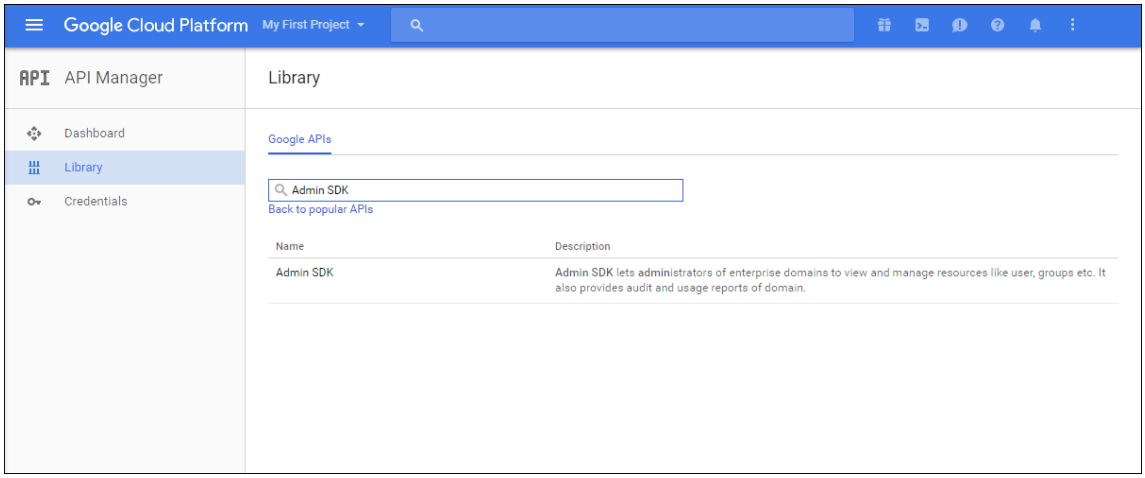


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

13. 此时将显示 Google 管理控制台上的帐户授权所需的详细信息。将 **Client ID**（客户端 ID）和 **Service account**（服务帐户）ID 复制到以后能够从中检索该信息的位置。需要提供此信息以及域名，才能发送给 Citrix 技术支持以添加到允许列表。

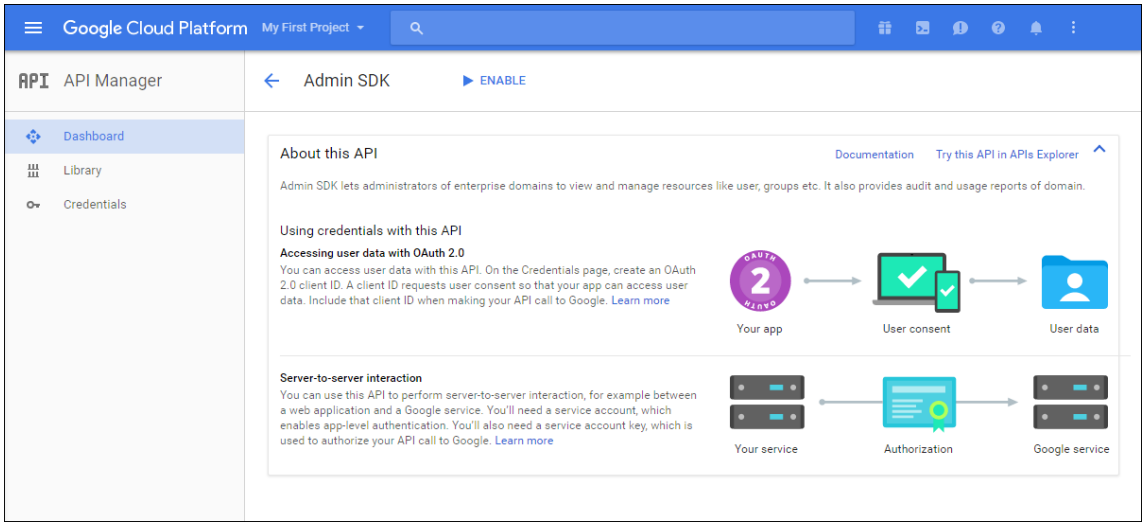


14. 在 **Library**（库）页面上，搜索 **Admin SDK**（管理 SDK），然后单击搜索结果。

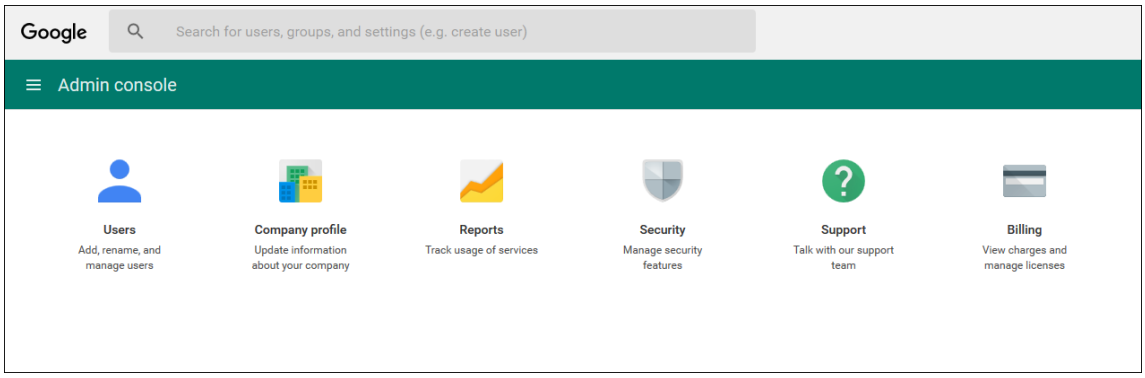


15. 在 **Overview**（概览）页面上，单击 **Enable**（启用）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

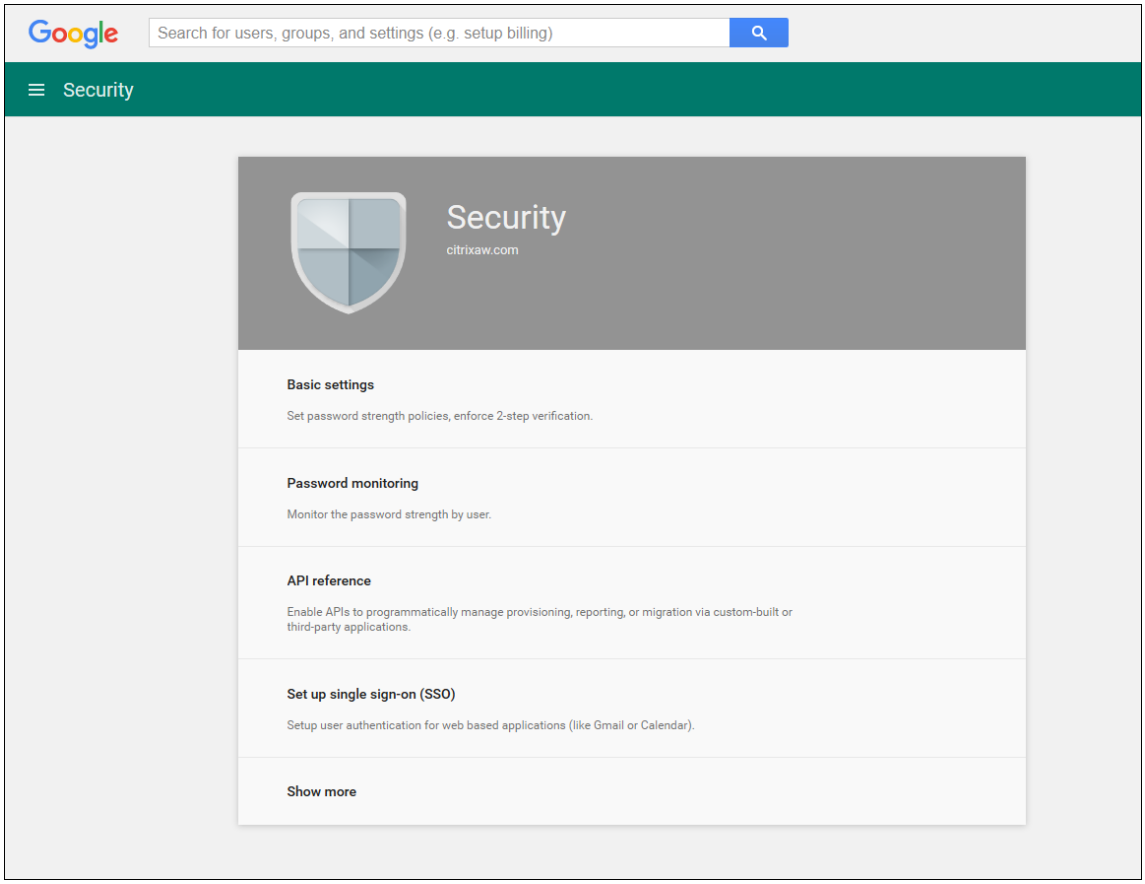


16. 打开您的域对应的 Google 管理控制台，然后单击 **Security**（安全）。

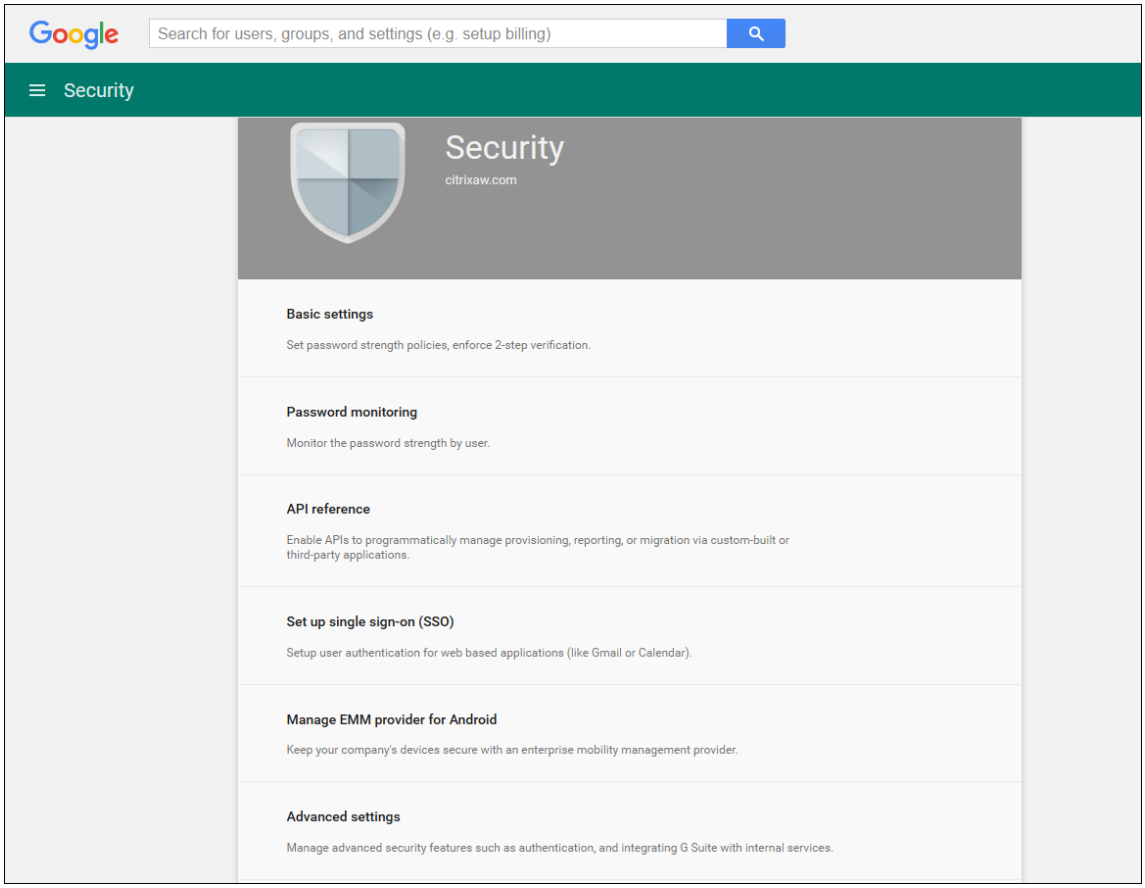


17. 在 **Settings**（设置）页面上，单击 **Show more**（显示更多），然后单击 **Advanced settings**（高级设置）。

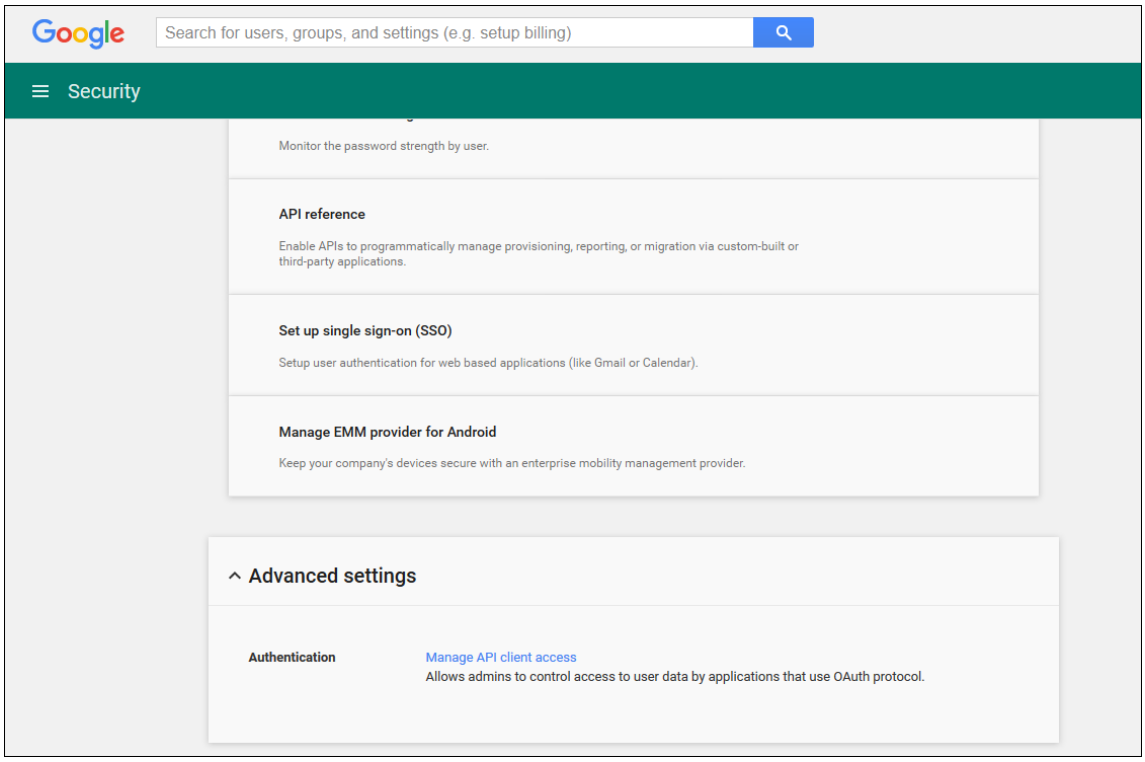
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

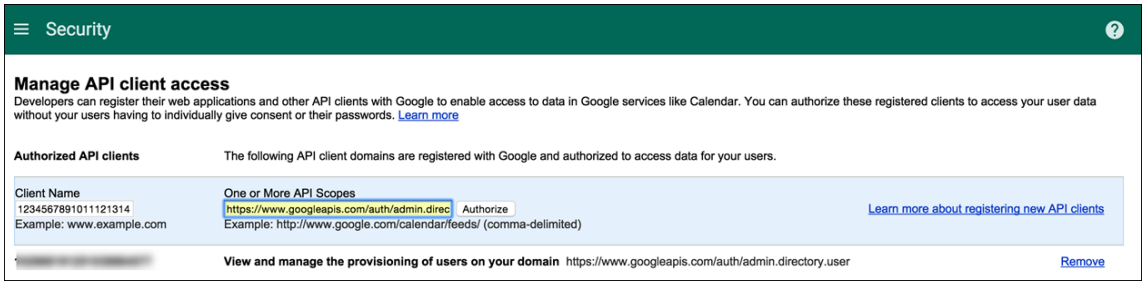


18. 单击 **Manage API client Access**（管理 API 客户端访问）。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

19. 在 **Client Name**（客户端名称）中，输入您之前保存的客户端 ID，在 **One or More API Scopes**（一个或多个 API 作用域）中，键入 `https://www.googleapis.com/auth/admin.directory.user`，然后单击 **Authorize**（授权）。



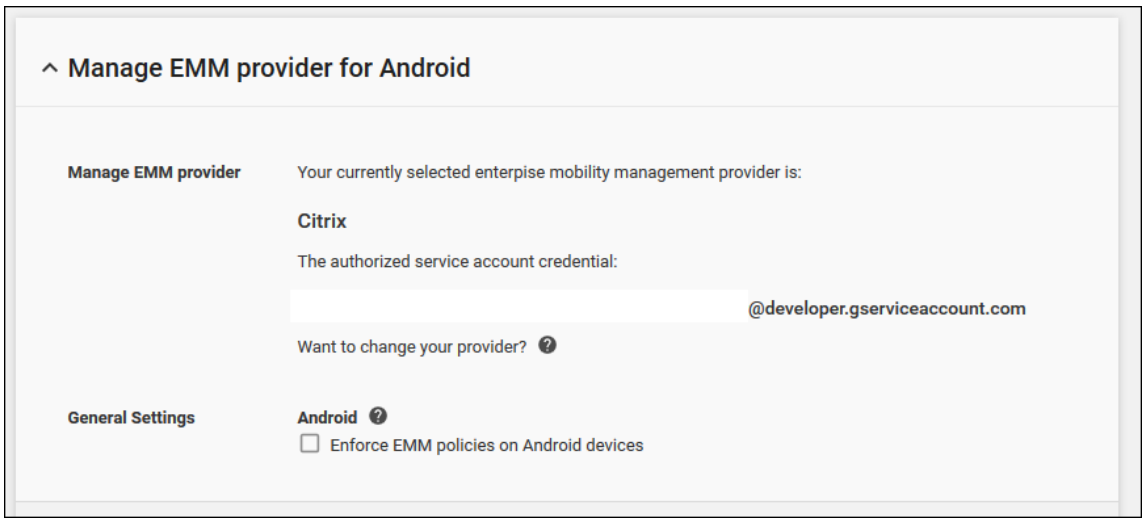
绑定到 **EMM**

必须先联系 Citrix 技术支持并提供您的域名、服务帐户和绑定令牌，才能使用 Endpoint Management 管理您的 Android 设备。Citrix 会将该令牌绑定到 Endpoint Management 作为企业移动性管理 (EMM) 提供程序。有关 Citrix 技术支持的联系信息，请参阅 Citrix 技术支持。

1. 要确认绑定，请登录 Google 管理门户，然后单击 **Security**（安全）。
2. 单击 **Manage EMM provider for Android**（管理适用于 Android 的 EMM 提供程序）。

   您将看到自己的 Google Android Enterprise 帐户绑定到 Citrix，用作 EMM 提供程序。

   确认令牌绑定后，可以开始使用 Endpoint Management 控制台管理您的 Android 设备。导入在步骤 14 中生成的 P12 证书。设置 Android Enterprise 服务器设置，启用基于 SAML 的单点登录 (SSO)，并至少定义一个 Android Enterprise 设备策略。

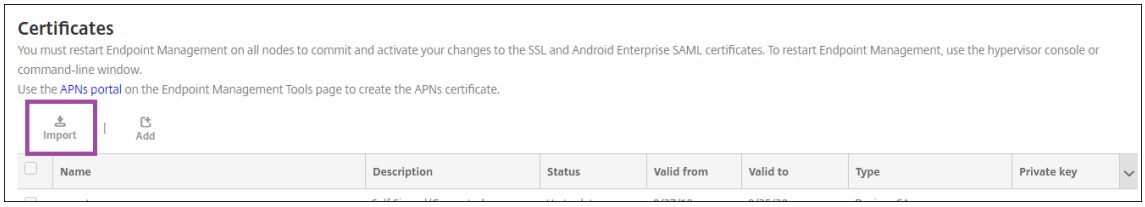


导入 **P12** 证书

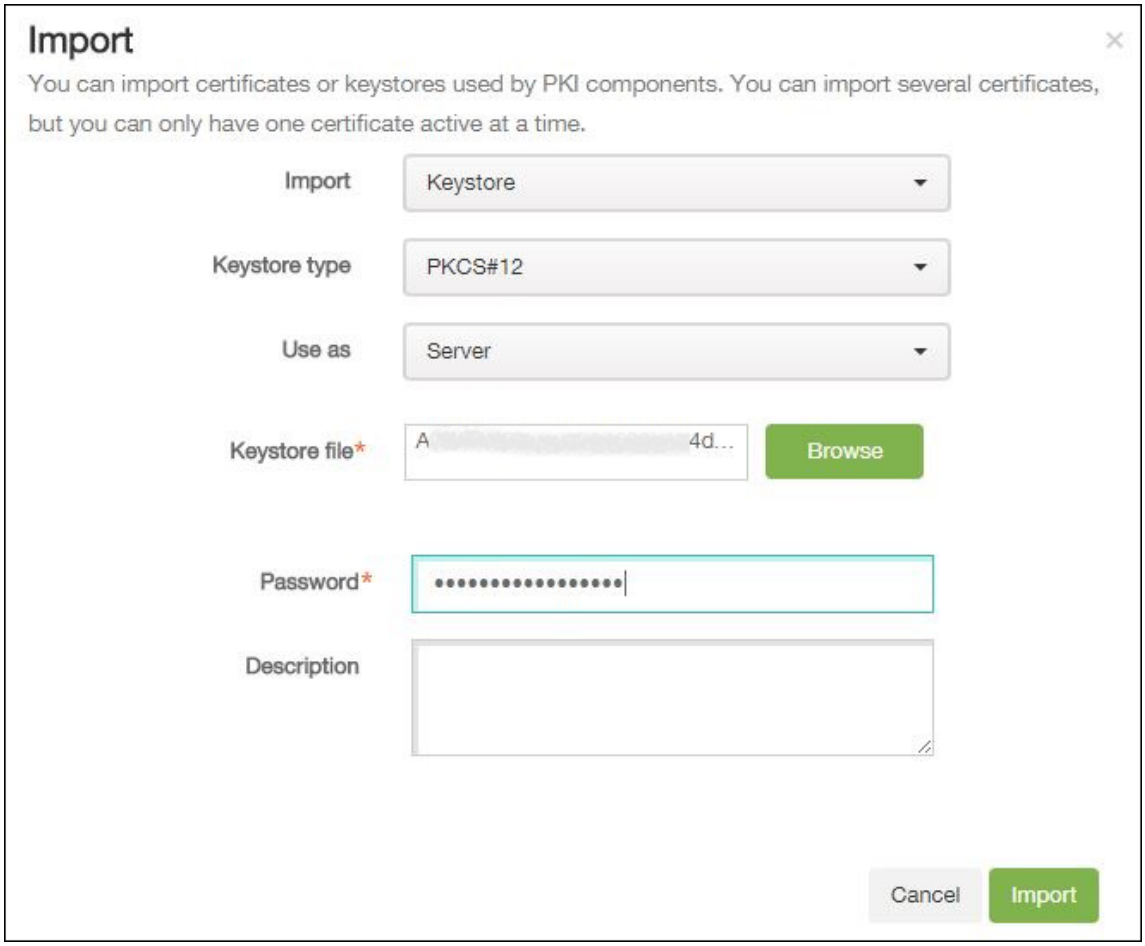
请按照以下步骤导入 Android Enterprise P12 证书：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标以打开设置页面，然后单击证书。此时将显示证书页面。



2. 单击导入。此时将显示导入对话框。



配置以下设置：

- 导入：在列表中，单击密钥库。
- 密钥库类型：在列表中，单击 **PKCS#12**。
- 用作：在列表中，单击服务器。
- 密钥库文件：单击浏览，然后导航到 P12 证书。
- 密码：键入证书密码。这是您在设置 Android Enterprise 帐户时创建的私钥密码。
- 说明：（可选）键入证书的说明。

3. 单击导入。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置 **Android Enterprise** 服务器设置

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在平台下，单击 **Android Enterprise**。此时将显示 **Android Enterprise** 页面。

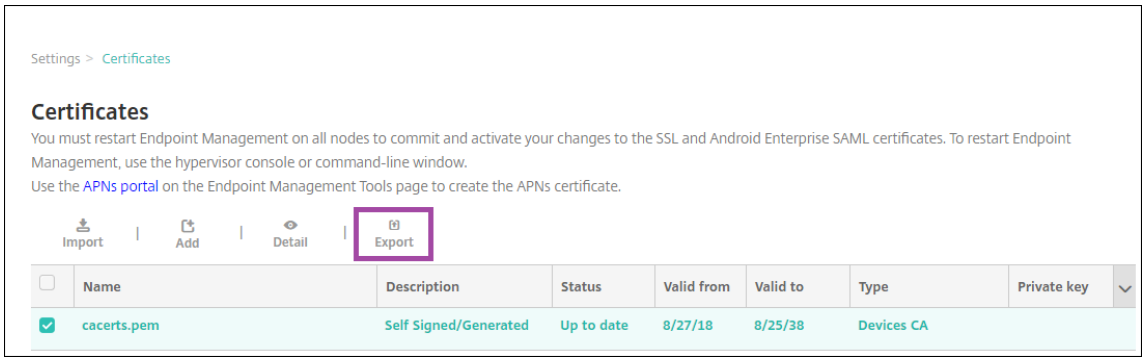


配置以下设置，然后单击 保存。

- 域名：键入您的 Android Enterprise 域名，例如 domain.com。
- 域管理员帐户：键入您的域管理员的用户名，例如，用于 Google 开发人员门户的电子邮件帐户。
- 服务帐户 **ID**:键入您的服务帐户 ID,例如,Google 服务帐户中关联的电子邮件 (`serviceaccountemail@xxxxxxx.iam.gserviceaccount.com`)。
- 客户端 **ID**：键入您的 Google 服务帐户的数字客户端 ID。
- 启用 **Android Enterprise**：选择启用或禁用 Android Enterprise。

启用基于 **SAML** 的单点登录

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击证书。此时将显示证书页面。

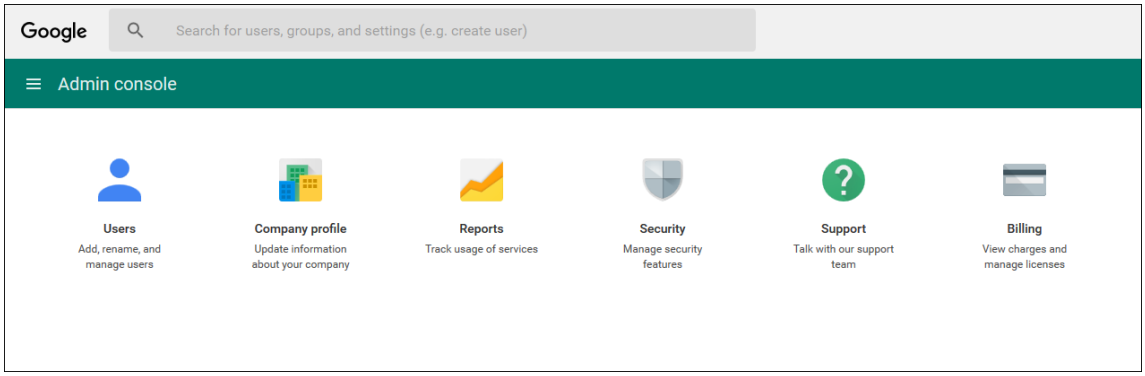


3. 在证书列表中，单击 SAML 证书。
4. 单击导出并将证书保存到您的计算机。

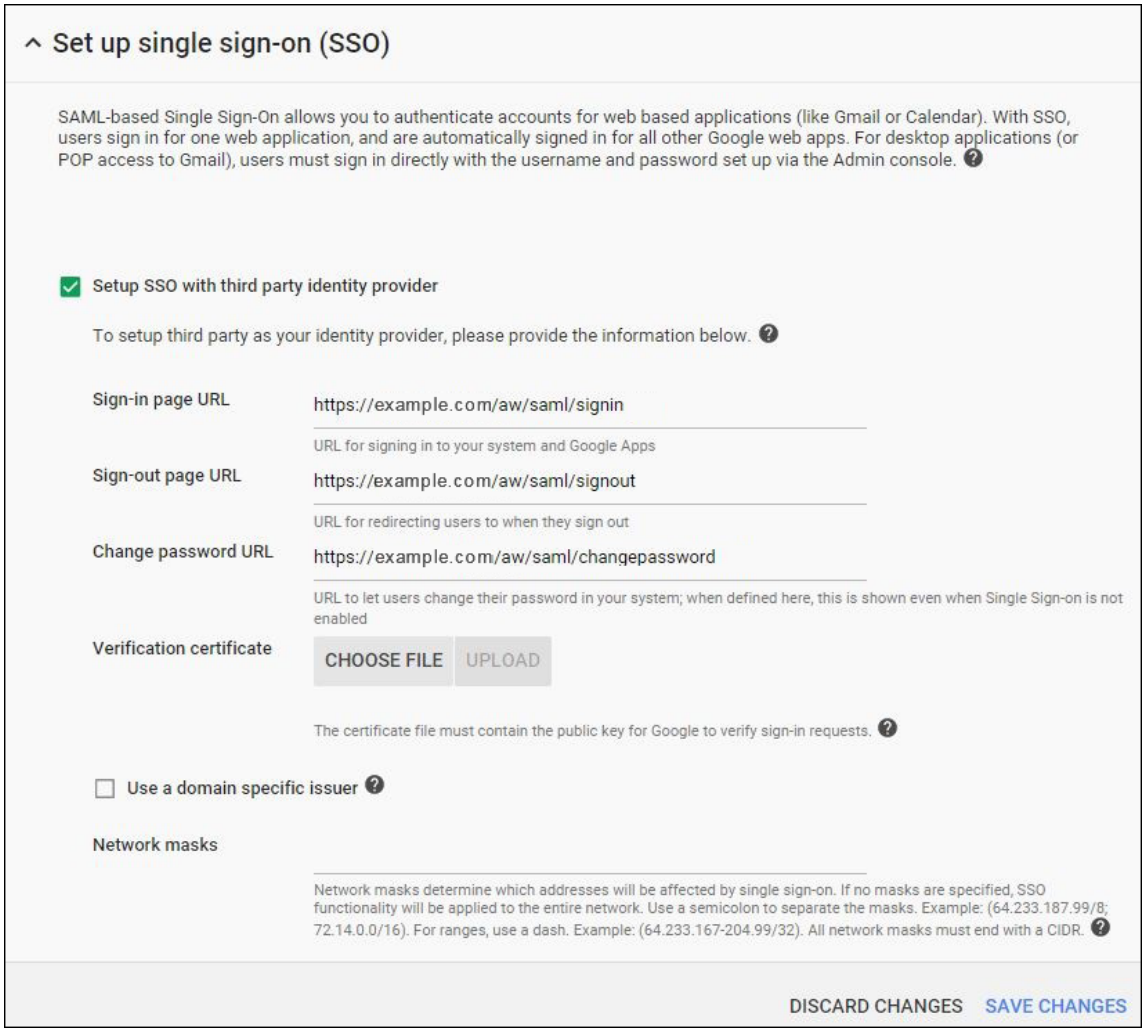
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 使用您的 Android Enterprise 管理员凭据登录 Google 管理门户。有关门户的访问权限，请参阅 Google 管理门户。

6. 单击 **Security**（安全）。



7. 在 **Security**（安全）下方，单击 **Set up single sign-on** (SSO)（设置单点登录 (SSO)），然后配置以下设置。



- **Sign-in page URL**（登录页面 **URL**）：键入用户登录您的系统和 Google Apps 使用的 URL。例如：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

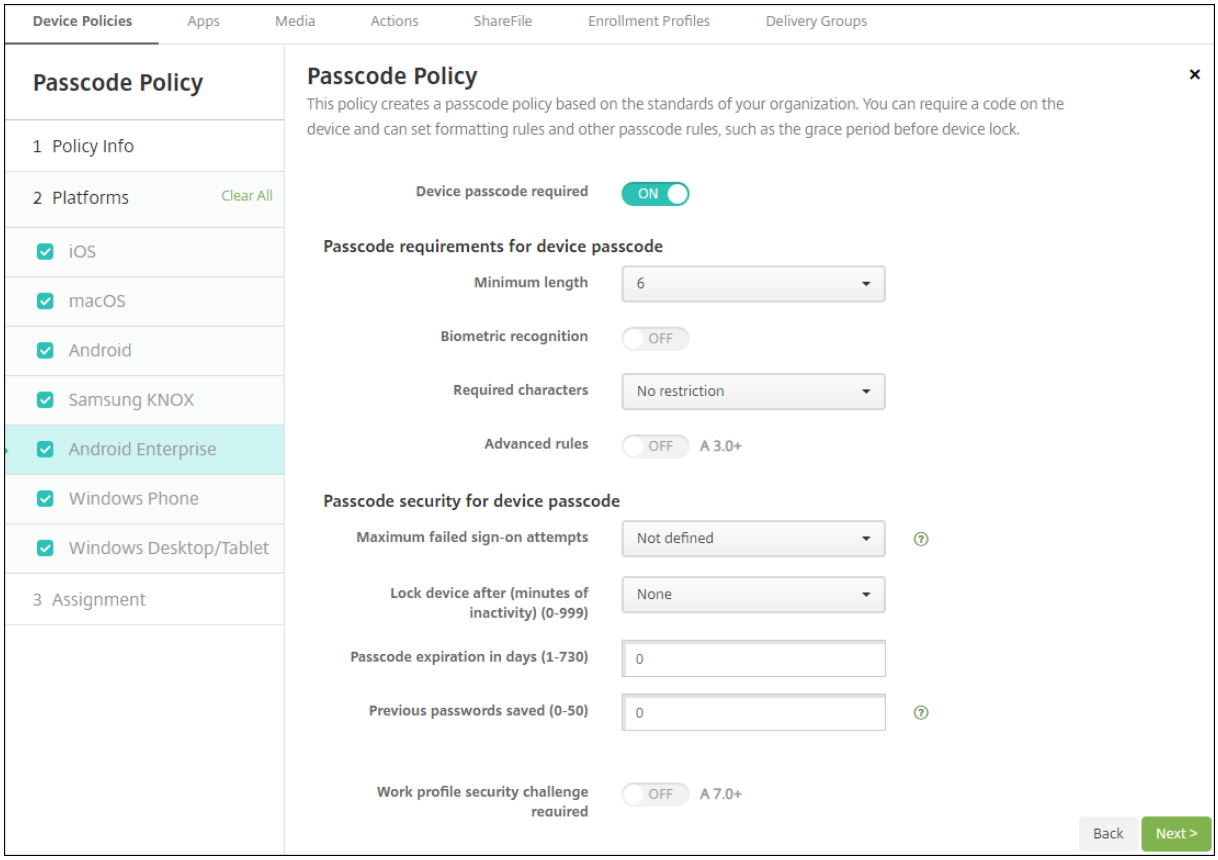
https://<Xenmobile-FQDN>/aw/saml/signin。

- **Sign out page URL**（注销页面 **URL**）：键入用户注销时被定向到的 URL。例如：https://<Xenmobile-FQDN>/aw/saml/signout。
- **Change password URL**（更改密码 **URL**）：键入 URL 以允许用户更改其系统中的密码。例如：https://<Xenmobile-FQDN>/aw/saml/changepassword。如果定义了此字段，用户将看到此提示，即使 SSO 不可用时也是如此。
- **Verification certificate**（验证证书）：单击 **CHOOSE FILE**（选择文件），然后导航到从 Endpoint Management 导出的 SAML 证书。

8. 单击 **SAVE CHANGES**（保存更改）。

设置 **Android Enterprise** 设备策略

设置通行码策略，以便用户在首次注册时必须在其设备上创建通行码。



设置任何设备策略的基本步骤如下。

1. 在 Endpoint Management 控制台中，单击配置，然后单击设备策略。
2. 单击添加，然后在添加新策略对话框中选择要添加的策略。在此示例中，请单击通行码。
3. 完成策略信息页面。
4. 单击 **Android Enterprise** 并配置策略设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 将策略分配到交付组。

配置 **Android Enterprise** 帐户设置

必须在 Endpoint Management 中设置 Android Enterprise 域和帐户信息，才能开始管理设备上的 Android 应用程序和策略。首先，请在 Google 上完成 Android Enterprise 设置任务以设置域管理员，并获取服务帐户 ID 和绑定令牌。

1. 在 Endpoint Management Web 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在平台下，单击 **Android Enterprise**。此时将显示 **Android Enterprise** 配置页面。



1. 在 **Android Enterprise** 页面上，配置以下设置：
   - 域名：键入域名。
   - 域管理员帐户：键入您的域管理员用户名。
   - 服务帐户 **ID**：键入您的 Google 服务帐户 ID。
   - 客户端 **ID**：键入您的 Google 服务帐户的客户端 ID。
   - 启用 **Android Enterprise**：选择是否启用 Android Enterprise。
2. 单击保存。

设置 **Google Workspace** 合作伙伴访问 **Endpoint Management**

Chrome 的一些 Endpoint Management 功能使用谷歌合作伙伴 API 在 Endpoint Management 和您的 Google Workspace 域之间进行通信。例如，Endpoint Management 要求对管理隐身模式和来宾模式等 Chrome 功能的设备策略使用 API。

要启用合作伙伴 API，请在 Endpoint Management 控制台中设置 Google Workspace 域，然后配置您的 Google Workspace 帐户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

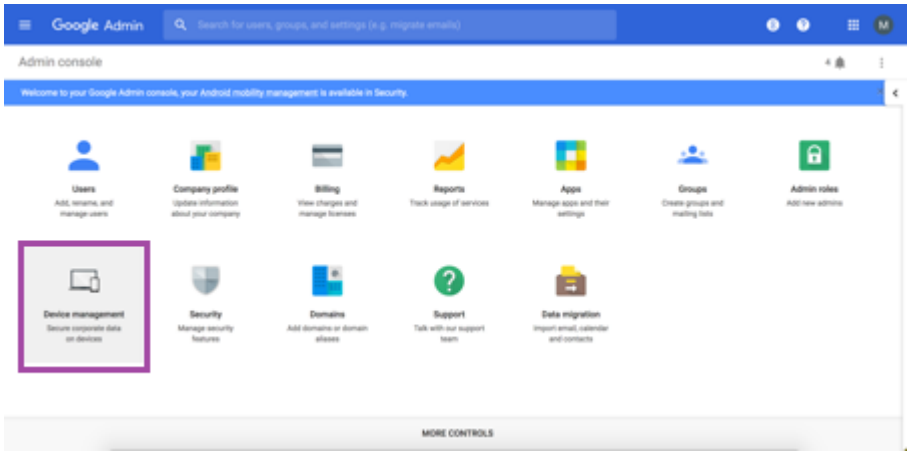
在 **Endpoint Management** 中设置您的 **Google Workspace** 域

要启用 Endpoint Management 与 Google Workspace 域中的 API 进行通信，请前往 **“设置” > “谷歌 Chrome 配置”** 并配置设置。

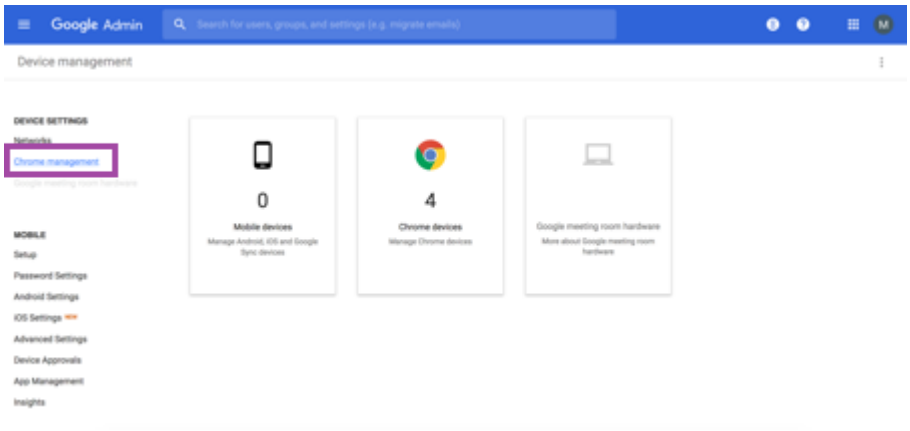
- **Google Workspace** 域：托管 Endpoint Management 所需的 API 的 Google Workspace 作空间域。
- **Google Workspace** 管理员帐户：您的 Google Workspace 域的管理员帐户。
- **Google Workspace** 客户端 **ID**： Citrix 的客户端 ID。请使用此值为您的 Google Workspace 域配置合作伙伴访问权限。
- **Google Workspace** 企业 **ID**：您帐号的企业 ID，由您的 Google 企业帐号填写。

启用对您的 **Google Workspace** 域中的设备和用户的合作伙伴访问权限

1. 登录 Google 管理控制台：https://admin.google.com
2. 单击 **Device Management**（设备管理）。

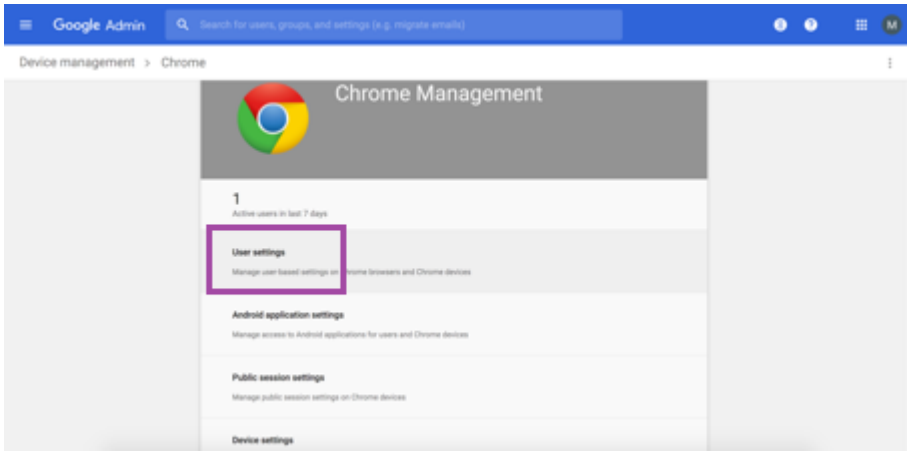


3. 单击 **Chrome management**（Chrome 管理）。



4. 单击 **User settings**（用户设置）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

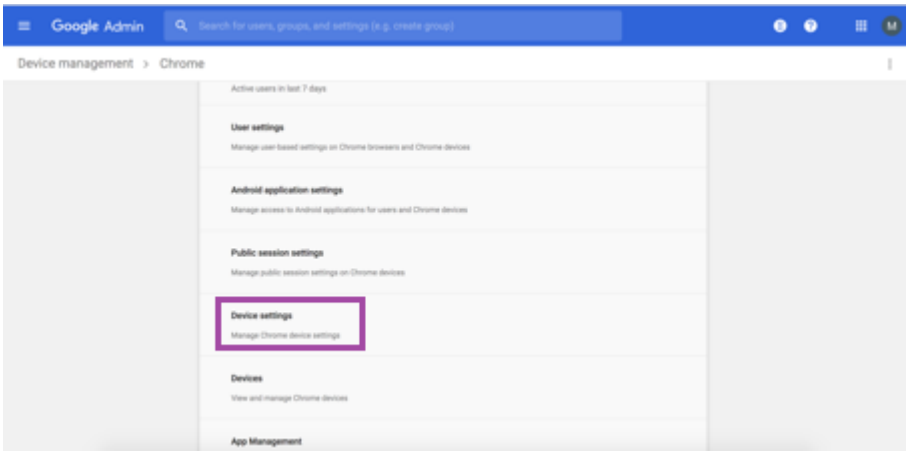


5. 搜索 **Chrome Management - Partner Access**（Chrome 管理 - 合作伙伴访问权限）。

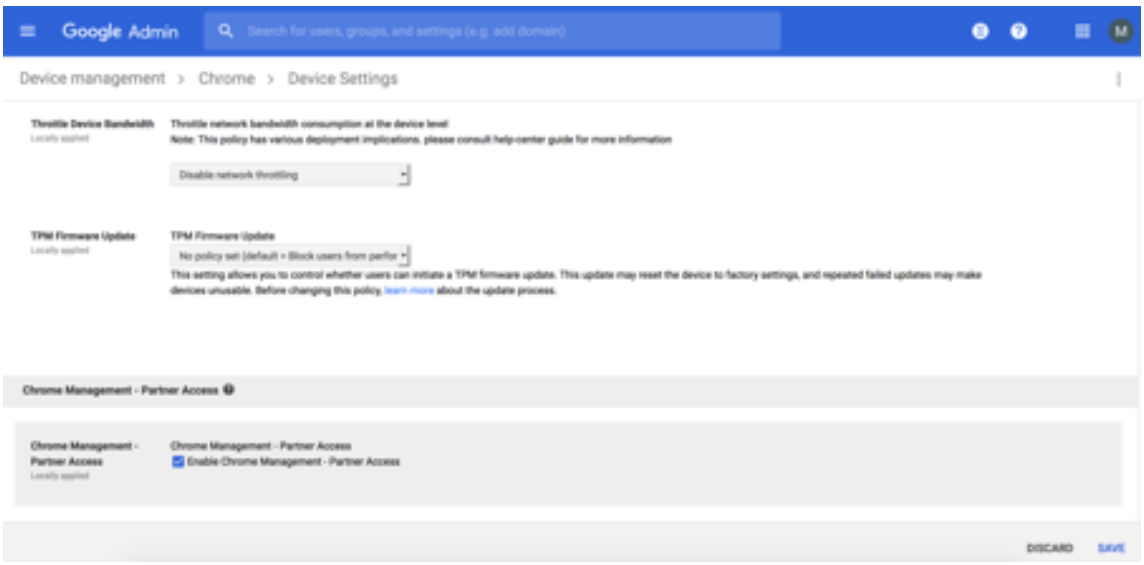


6. 选中 **Enable Chrome Management - Partner Access**（启用 Chrome 管理 - 合作伙伴访问权限）复选框。
7. 同意您理解并希望启用合作伙伴访问权限。单击保存。
8. 在 Chrome 管理页面中，单击 **Device Settings**（设备设置）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



9. 搜索 **Chrome Management - Partner Access**（Chrome 管理 - 合作伙伴访问权限）。

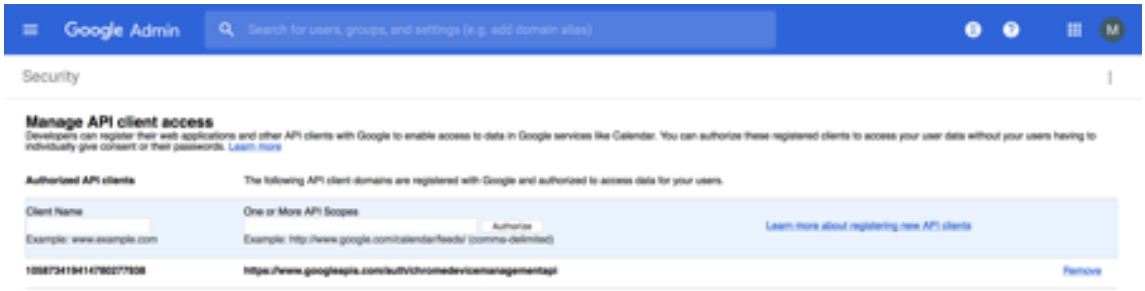


10. 选中 **Enable Chrome Management - Partner Access**（启用 Chrome 管理 - 合作伙伴访问权限）复选框。
11. 同意您理解并希望启用合作伙伴访问权限。单击保存。
12. 转至 **Security**（安全）页面，然后单击 **Advanced Settings**（高级设置）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



13. 单击 **Manage API client Access**（管理 API 客户端访问）。
14. 在 Endpoint Management 控制台中，转至设置 **> Google Chrome** 配置并复制 G Suite 客户端 ID 的值。然后，返回到 **Manage API client Access**（管理 API 客户端访问）页面并将复制的值粘贴到 **Client Name**（客户端名称）字段中。
15. 在 **One or More API Scopes**（一个或多个 API 范围）中，添加 URL：`https://www.googleapis.com/auth/chromedevicemanagementapi`



16. 单击 **Authorize**（授权）。

    此时将显示消息 “Your settings have been saved”（已保存您的设置）。

注册 **Android Enterprise** 设备

如果您的设备注册过程要求用户输入用户名或用户 ID，接受的格式取决于将 Endpoint Management 服务器配置为按用户主体名称 (UPN) 还是 SAM 帐户名称来搜索用户。

如果 Endpoint Management 服务器配置为按 UPN 搜索用户，用户必须按以下格式输入 UPN：

- 用户名 @ 域

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

如果 Endpoint Management 服务器配置为按 SAM 搜索用户，用户必须按以下格式之一输入 SAM：

- 用户名 @ 域
- 域\用户名

要确定为您的 Endpoint Management 服务器配置的用户名类型，请执行以下操作：

1. 在 Endpoint Management 服务器控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击 **LDAP** 以查看 LDAP 连接的配置。
3. 在靠近页面底部的位置，查看用户搜索依据字段：
    - 如果设置为 **userPrincipalName**，Endpoint Management 服务器将设置为按 UPN 搜索。
    - 如果设置为 **sAMAccountName**，Endpoint Management 服务器将设置为按 SAM 搜索。

取消注册 **Android Enterprise** 企业

可以使用 Endpoint Management 服务器控制台和 Endpoint Management Tools 取消注册 Android Enterprise 企业。

执行此任务时，Endpoint Management 服务器将打开 Endpoint Management Tools 的弹出窗口。开始之前，请确保 Endpoint Management 服务器有权在您使用的浏览器中打开弹出窗口。某些浏览器（例如 Google Chrome）要求禁用弹出窗口阻止功能并将 Endpoint Management 站点的地址添加到弹出窗口允许列表中。

> 警告：
>
> 取消注册企业后，通过其注册的设备上的 Android Enterprise 应用程序将重置到其默认状态。这些设备将不再由 Google 托管。如果未进一步进行配置，在 Android Enterprise 企业中重新注册这些设备可能不会恢复以前的功能。

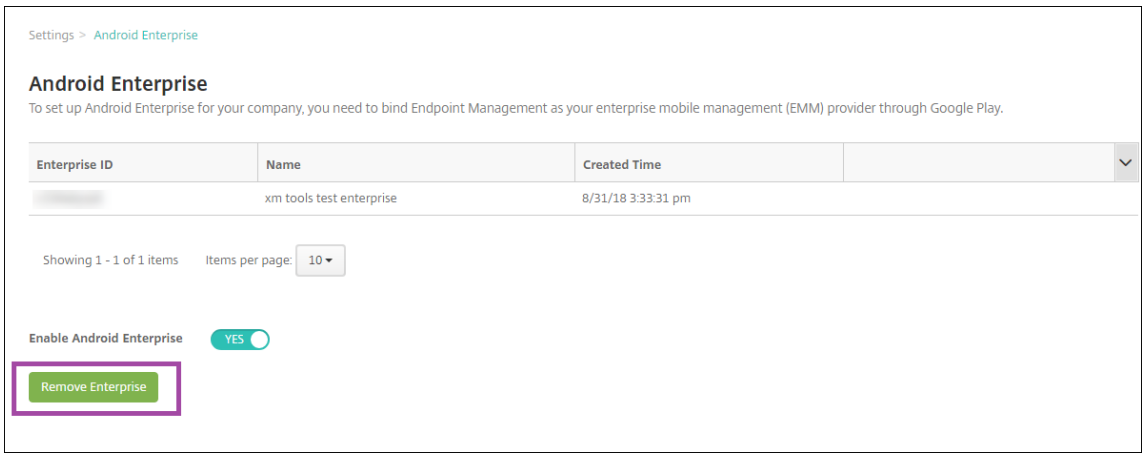
取消注册 Android Enterprise 企业后：

- 通过企业注册的设备和用户会将 Android Enterprise 应用程序重置到其默认状态。之前应用的应用程序权限和托管配置策略不再有效果。
- 通过企业注册的设备由 Endpoint Management 托管，但在 Google 看来未托管。无法添加任何新的 Android Enterprise 应用程序。不能应用应用程序权限或托管配置策略。仍然可以将其他策略（例如“计划”、“密码”和“限制”）应用于这些设备。
- 如果尝试在 Android Enterprise 中注册设备，这些设备将注册为 Android 设备，而非 Android Enterprise 设备。

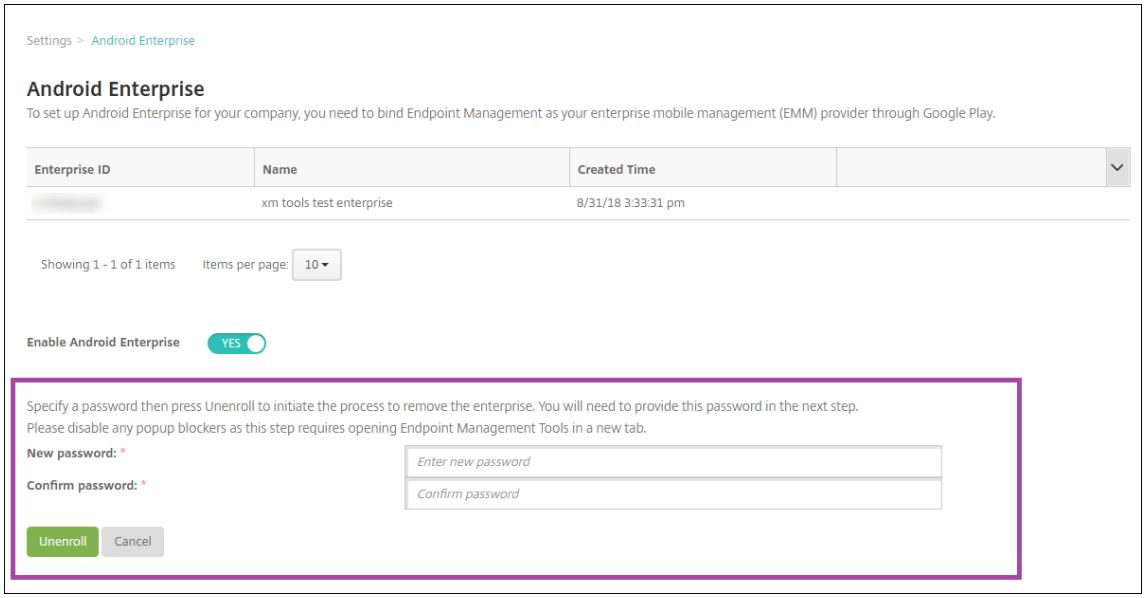
要取消注册 Android Enterprise 企业，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在“设置”页面上，单击 **Android Enterprise**。
3. 单击删除企业。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

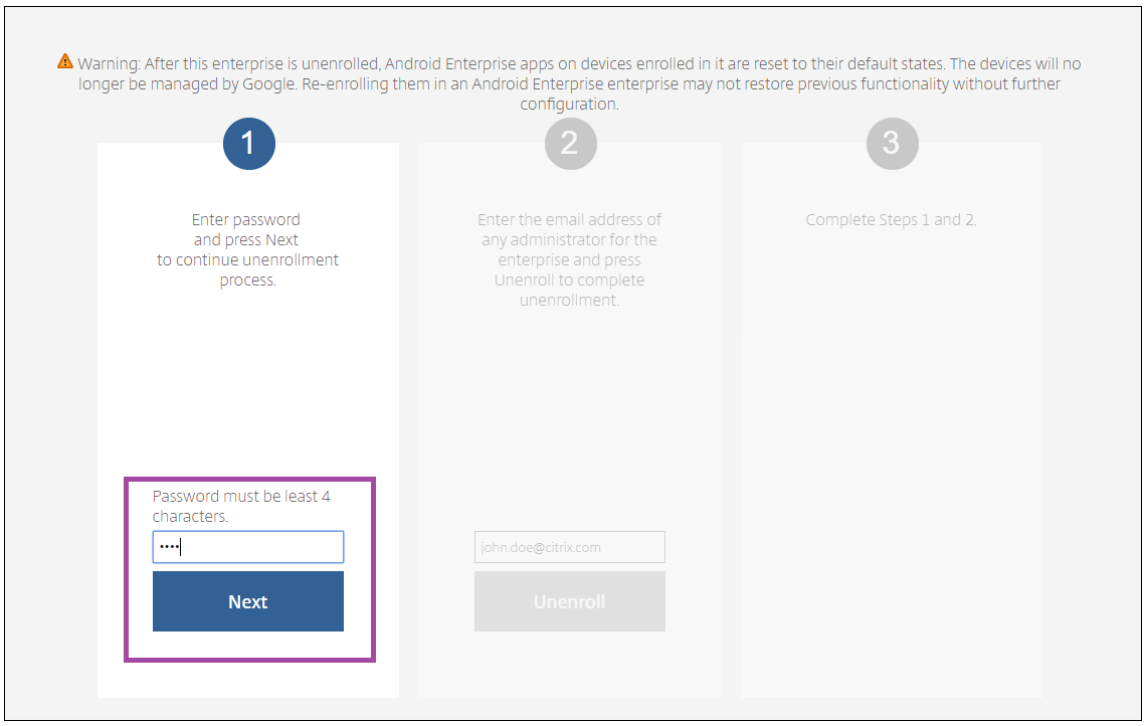


4. 指定一个密码。您在执行下一步骤时需要此密码才能完成取消注册操作。然后单击取消注册。

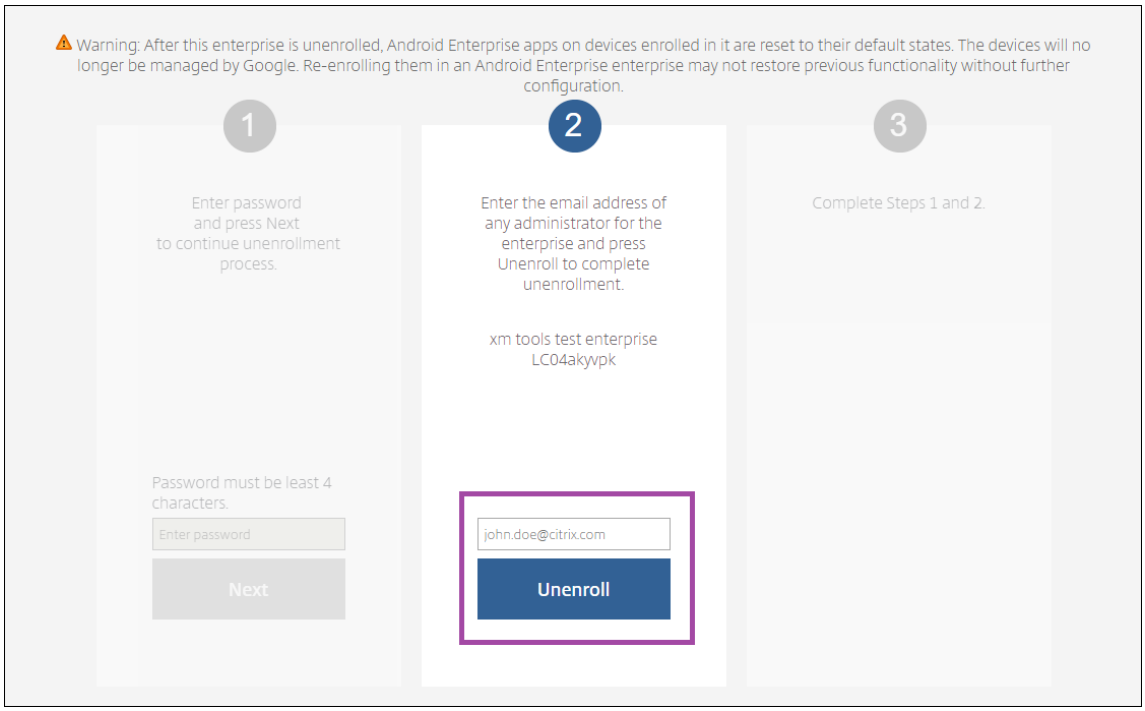


5. “Endpoint Management Tools” 页面打开时，请输入您在上一步骤中创建的密码。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 单击取消注册。



在 **Android Enterprise** 中预配完全托管设备

只有公司拥有的设备可以是 Android Enterprise 中的完全托管设备。在完全托管设备上，整个设备（而不仅仅是工作配置文件）由公司或组织控制。完全托管设备也称为工作托管设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 支持对完全托管设备使用以下注册方法：

- **afw#xenmobile**：如果使用此注册方法，用户在设置设备时将输入字符 `afw##xenmobile`。此令牌将设备标识为由 Endpoint Management 托管并下载 Secure Hub。
- **QR** 代码：QR 代码预配是预配不支持 NFC 的分布式设备队列（例如平板电脑）的简便方式。可以在已恢复出厂设置的队列设备上使用 QR 代码注册方法。QR 代码注册方法通过扫描设置向导中的 QR 代码来设置并配置完全托管设备。
- 近场通信 **(NFC)** 碰撞：可以在已重置为出厂设置的队列设备上使用 NFC 碰撞注册方法。NFC 碰撞通过在两个设备之间使用近场通信来传输数据。蓝牙、Wi-Fi 和其他通信模式在恢复出厂设置的设备上处于禁用状态。NFC 是此状态下设备可以使用的唯一通信协议。

afw#xenmobile

此注册方法在打开新设备或恢复出厂设置的设备以便进行初始设置后使用。系统提示输入 Google 帐户时，用户输入 `afw##xenmobile`。此操作将下载并安装 Secure Hub。用户随后将按照 Secure Hub 设置提示进行操作，完成注册过程。

对于大多数客户，建议使用此注册方法，因为是从 Google Play 应用商店下载最新版本的 Secure Hub。与其他注册方法不同，您不用提供要从 Endpoint Management 服务器下载的 Secure Hub。

必备条件：

- 在运行 Android OS 的所有 Android 设备上均受支持。

QR 代码

要使用 QR 代码在设备模式注册设备，请通过创建一个 JSON 并将该 JSON 转换为 QR 代码来生成 QR 代码。将使用设备相机扫描 QR 代码以注册设备。

必备条件：

- 在运行 Android 7.0 及更高版本的所有 Android 设备上均受支持。

从 JSON 创建 QR 代码

创建包含以下字段的 JSON。

以下字段均为必填项：

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

值：com.zenprise/com.zenprise.configuration.AdminFunction

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

值：qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

值：https://play.google.com/managed/downloadManagingApp?identifier=xenmobile

以下字段为选填字段：

- **android.app.extra.PROVISIONING_LOCALE**：输入语言和国家/地区代码。

  语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请输入 en_US 表示在美国所讲的英语。

- **android.app.extra.PROVISIONING_TIME_ZONE**：设备运行时所在的时区。

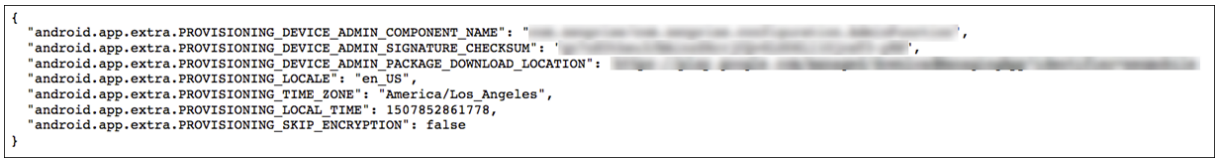
  键入区域/位置的数据库名称。例如，键入 **America/Los_Angeles** 表示太平洋时间。如果未键入名称，时区将自动填充。

- **android.app.extra.PROVISIONING_LOCAL_TIME**：从 Epoch 开始经过的时间（毫秒）。

  Unix epoch（或 Unix 时间、POSIX 时间或 Unix 时间戳）是指从 1970 年 1 月 1 日（午夜，UTC/GMT）开始经过的秒数。该时间不包括闰秒（在 ISO 8601 中为：1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION**：设置为 **true** 将在配置文件创建期间跳过加密。设置为 **false** 将在配置文件创建期间强制加密。

典型的 JSON 如下：



使用任意 JSON 验证工具（例如 https://jsonlint.com）验证创建的 JSON。然后使用任意联机 QR 代码生成器将该 JSON 字符串转换为 QR 代码。

恢复出厂设置的设备将扫描此 QR 代码以将设备注册为完全托管设备。

注册设备

要将设备注册为完全托管设备，该设备必须处于已恢复出厂设置状态。

1. 在欢迎屏幕上轻按该屏幕六次以启动 QR 代码注册流程。
2. 系统提示时，连接到 Wi-Fi。QR 代码（JSON 编码）中 Secure Hub 的下载位置可以通过此 Wi-Fi 网络访问。

   设备成功连接到 Wi-Fi 后，将从 Google 下载一个 QR 代码读取器并启动摄像头。

3. 将摄像头对准 QR 代码以扫描该代码。

   Android 将从 QR 代码中的下载位置下载 Secure Hub，验证签名证书的签名，安装 Secure Hub 并将其设置为设备所有者。

有关使用 QR 码方法预配设备的更多信息，请参阅面向 Android EMM 开发人员的 Google API 文档。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

NFC 碰撞

要使用 NFC 碰撞功能将设备注册为完全托管设备，需要两个设备：一个已恢复出厂设置的设备，以及一个运行 Endpoint Management Provisioning Tool 的设备。

必备条件：

- 支持的 Android 设备
- 为 Android Enterprise 启用 Endpoint Management
- 新的或恢复出厂设置的设备，为 Android Enterprise 预配为完全托管设备。可以在本文中查找完成此必备条件的步骤。
- 另一个设备具有 NFC 功能，运行已配置的 Provisioning Tool。Provisioning Tool 在 Secure Hub 或 Citrix 下载页面上提供。

每个设备只能配备一个 Android Enterprise 配置文件，通过企业移动性管理 (EMM) 应用程序管理。在 Endpoint Management 中，Secure Hub 为 EMM 应用程序。仅允许在每个设备上配备一个配置文件。尝试添加第二个 EMM 应用程序将删除第一个 EMM 应用程序。

通过 NFC 碰撞传输数据

预配恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以初始化 Android Enterprise：

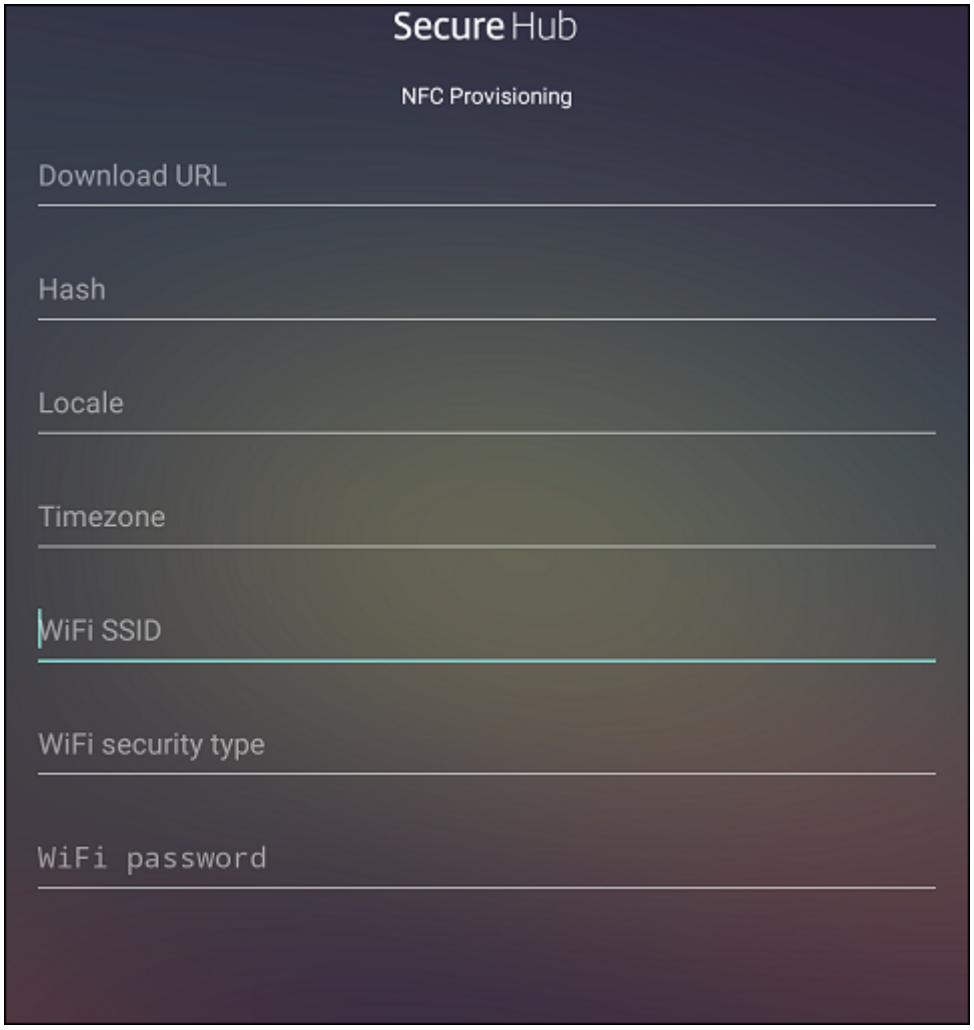
- 要作为设备所有者（在此示例中为 Secure Hub）的 EMM 提供程序应用程序的包名称。
- 设备可以从中下载 EMM 提供程序应用程序的 Intranet/Internet 位置。
- EMM 提供商应用程序的 SHA-256 哈希值，以验证下载是否成功。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备能够连接和下载 EMM 提供程序应用程序。注意：Android 现在不支持在此步骤中使用 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

碰撞两个设备时，来自 Provisioning Tool 的数据将发送到恢复出厂设置的设备。该数据随后用于下载使用管理员设置的 Secure Hub。如果未输入时区和位置值，Android 将在新设备上自动配置值。

配置 Endpoint Management Provisioning Tool

执行 NFC 碰撞之前，必须配置 Provisioning Tool。此配置随后在 NFC 碰撞过程中被传输到恢复出厂设置的设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



可以将数据键入到必填字段中，或者通过文本文件进行填充。下一个过程中的步骤介绍了如何配置文本文件，并且包含每个字段的说明。键入后，该应用程序将不保存信息，因此，您可能希望创建一个文本文件以保留该信息供将来使用。

使用文本文件配置 **Provisioning Tool**

将文件命名为 nfcprovisioning.txt，然后将该文件放在设备 SD 卡上的 **/sdcard/** 文件夹中。该应用程序随后可以读取文本文件并填充值。

文本文件必须包含以下数据：

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

此行为 EMM 提供程序应用程序的 Intranet/Internet 位置。恢复出厂设置的设备在进行 NFC 碰撞后连接到 Wi-Fi 之后，该设备必须有权访问此位置才能进行下载。该 URL 为常规 URL，不需要特殊格式。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

此行是 EMM 提供程序应用程序的校验和。此校验和用于验证下载是否成功。本文中后面的内容介绍了获取校验和的步骤。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

此行是运行 Provisioning Tool 的设备的已连接 Wi-Fi SSID。

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

支持的值为 WEP 和 WPA2。如果 Wi-Fi 未受保护，此字段必须留空。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

如果 Wi-Fi 未受保护，此字段必须留空。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

输入语言和国家/地区代码。语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请键入 en_US 表示在美国所讲的英语。如果未输入任何代码，则会自动填充国家/地区和语言。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

设备运行时所在的时区。键入区域/位置的数据库名称。例如，键入 **America/Los_Angeles** 表示太平洋时间。如果未键入名称，时区将自动填充。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

不需要此数据，因为值 Secure Hub 被硬编码到应用程序中。在本文中提及的目的只是为了保持完整性。

如果存在通过使用 WPA2 保护的 Wi-Fi，完整的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

如果存在不受保护的 Wi-Fi，完整的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

获取 **Citrix Secure Hub** 的校验和

Secure Hub 的校验和是一个常数值：`qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。要下载适用于 Secure Hub 的 APK 文件，请使用以下 Google Play 应用商店链接：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

获取应用程序校验和

必备条件：

- 来自 Android SDK Build Tools 的 **apksigner** 工具
- OpenSSL 命令行

要获取任何应用程序的校验和，请按照下列步骤进行操作：

1. 从 Google Play 应用商店下载应用程序的 APK 文件。
2. 在 OpenSSL 命令行中，导航到 **apksigner** 工具：`android-sdk/build-tools/<version>/apksigner` 并键入以下内容：

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
    (?<=SHA-256 digest:) .* }
    '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   <!--NeedCopy-->
   ```

   该命令返回有效的校验和。

3. 要生成 QR 码，请在 `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` 字段中输入校验和。例如：

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
7
8         "serverURL": "https://supportablility.xm.cloud.com"
9       }
10
11    }
12
13  <!--NeedCopy-->
```

使用的库

Provisioning Tool 在其源代码中使用以下库：

- v7 `appcompat` 库、Design Support 库以及 v7 Palette Support 库

  有关信息，请查看 Android 开发人员文档中的支持库功能指南。

- Jake Wharton 遵循 Apache License 2.0 提供的 Butter Knife

在 **Android Enterprise** 中预配工作配置文件设备

在 Android Enterprise 中的工作配置文件设备上，您安全地分隔了设备上的企业区域与个人区域。例如，BYOD 设备可以是工作配置文件设备。工作配置文件设备的注册体验与 Endpoint Management 中的 Android 注册体验相似。用户将从 Google Play 下载 Secure Hub 并注册其设备。

默认情况下，如果某个设备在 Android Enterprise 中注册为工作配置文件设备，USB 调试和未知来源设置在该设备上将处于禁用状态。

> 提示：
>
> 在 Android Enterprise 中将设备注册为工作配置文件设备时，将始终转至 Google Play。在该应用商店中，允许 Secure Hub 在用户的个人配置文件中显示。

Android OS

November 7, 2022

> 注意：
>
> 本文不适用于使用 Android Enterprise 管理的设备。有关这些设备的信息，请参阅本部分中的其他文章。

Endpoint Management 还支持不通过 Android 或 Samsung 企业程序管理的 Android 操作系统设备。要控制 Android 设备连接到 Endpoint Management 服务的方式和时间，请使用 Firebase Cloud Messaging (FCM)。有关信息，请参阅 Firebase Cloud Messaging。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

注册配置文件确定 Android 设备在 MAM、MDM 还是 MDM+MAM 中注册，并提供供用户选择退出 MDM 的选项。Endpoint Management 支持对 MDM+MAM 中的 Android 设备使用以下身份验证类型。有关信息，请参阅以下文章：

- 域或域加安全令牌身份验证
- 客户端证书或证书加域身份验证
- 身份提供程序：
  - 通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证
  - 通过 Citrix Cloud 使用 Okta 进行身份验证

另一种罕见的身份验证方法是客户端证书加安全令牌。有关信息，请参阅 https://support.citrix.com/article/CTX215200。

启动 Android 设备管理的一般工作流程如下：

1. 完成登录流程。请参阅载入和资源设置和准备注册设备并交付资源。
2. 选择并配置注册方法。请参阅支持的注册方法。
3. 配置 Android 设备策略。
4. 注册 Android 设备。
5. 设置设备和应用程序安全操作。请参阅安全操作。

有关支持的操作系统，请参阅支持的设备操作系统。

支持的注册方法

下表列出了 Endpoint Management 支持的 Android 设备的注册方法：

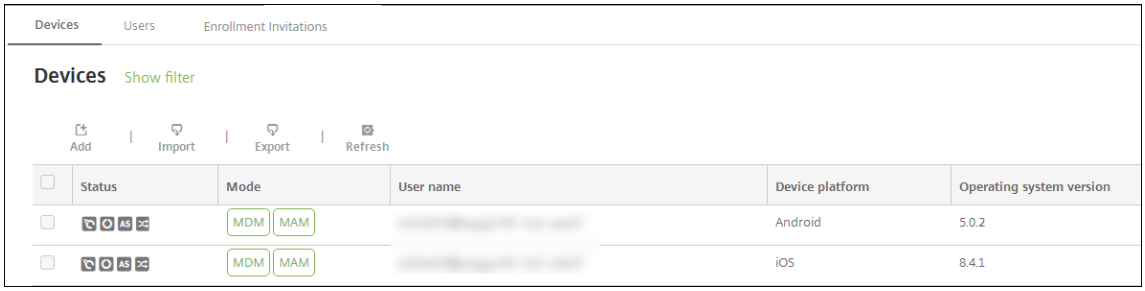
方法	支持
批量注册	否
手动注册	是
注册邀请	是

手动添加 **Android** 设备

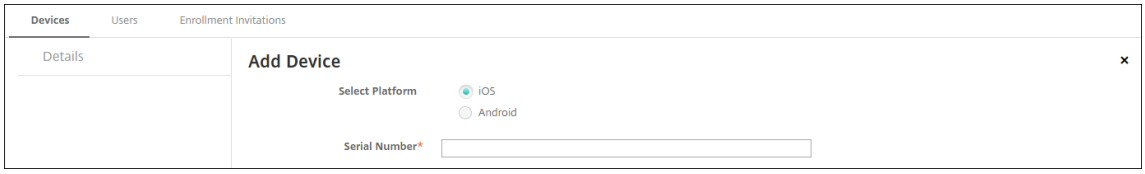
如果您想手动添加 Android 或 iOS 设备（例如用于测试目的），请按照以下步骤进行操作。

1. 在 Endpoint Management 控制台中，单击管理 **>** 设备。此时将显示设备页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 单击添加。此时将显示添加设备页面。



3. 配置以下设置：

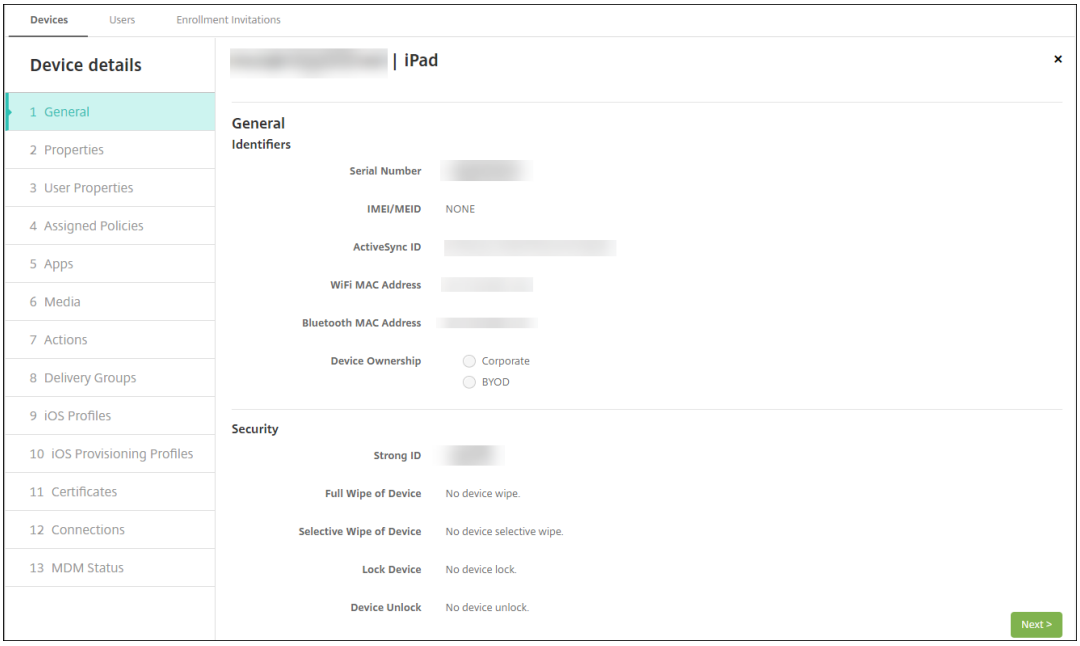
   - 选择平台：单击 **Android**。
   - 序列号：键入设备序列号。
   - **IMEI/MEID**：（可选）键入设备的 IMEI/MEID 信息。

4. 单击添加。设备将添加到所显示设备表的列表底部。要查看并确认设备详细信息，请执行以下操作：选择已添加的设备，然后在显示的菜单中，单击编辑。

   > 注意：
   >
   > 选中某个设备旁边的复选框时，选项菜单将在设备列表上方显示。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。

   - 已配置 LDAP
   - 如果使用本地组和本地用户：
     - 一个或多个本地组。
     - 分配给本地组的本地用户。
     - 交付组与本地组相关联。
   - 如果使用 Active Directory：
     - 交付组与 Active Directory 组相关联。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



5. 常规页面列出设备标识符，例如，序列号和平台类型的其他信息。对于设备所有权，请选择公司或 **BYOD**。

   常规页面还列出了设备安全属性，例如，强 ID、锁定设备、激活锁绕过和平台类型的其他信息。完全擦除设备字段包括用户的 PIN 代码。擦除设备后，用户必须输入该代码。如果用户忘记了该代码，您可以在此处查找。

6. 属性页面列出了 Endpoint Management 要预配的设备属性。此列表显示了用于添加设备的预配文件中包含的任何设备属性。要添加属性，请单击添加，然后从列表中选择一种属性。有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

   添加属性时，它最初将显示在添加了该属性的类别下方。单击下一步，然后返回属性页面后，属性将显示在相应列表中。

   要删除某个属性，请将鼠标悬停在列表上方，然后单击右侧的 **X**。Endpoint Management 会立即删除该项目。

7. 其余的设备详细信息部分包含设备的摘要信息。

   - 用户属性：显示用户的 RBAC 角色、组成员身份、托管 Google Play 帐户和属性。可以从此页面中停用托管 Google Play 帐户。
   - 已分配的策略：显示已部署、挂起和失败的策略数量。提供每个策略的策略名称、类型和上次部署信息。允许您将部署状态重置为挂起，然后重新部署用户删除的策略。
   - 应用程序：显示上一个清单的已安装、挂起和失败的应用程序部署数量。提供应用程序名称、标识符、类型和其他信息。有关 iOS 和 macOS 清单密钥（例如 **HasUpdateAvailable**）的说明，请参阅移动设备管理 (MDM) 协议。
   - 媒体：显示上一个清单的已部署、挂起和失败的媒体部署数量。
   - 操作：显示已部署、挂起和失败的操作数量。提供上一个部署的操作名称和时间。
   - 交付组：显示成功、挂起和失败的交付组数量。对于每个部署，提供交付组的名称和部署时间。选择一个交付组以查看更多详细信息，包括状态、操作以及通道或用户。
   - **iOS** 配置文件：显示上一个 iOS 配置文件清单，包括名称、类型、组织和说明。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **iOS** 预配配置文件：显示企业分发预配配置文件信息，例如 UUID、过期日期以及托管状态。
- 证书：显示有效证书、已过期证书或已吊销证书信息，例如，类型、提供程序、颁发者、序列号、过期之前的剩余天数。
- 连接：显示第一个连接状态和最后一个连接状态。提供每个连接的用户名、倒数第二次身份验证和上次身份验证时间。
- **MDM** 状态：显示 MDM 状态、上次推送时间以及上次设备答复时间等信息。

配置 **Android** 设备策略

使用这些策略可配置 Endpoint Management 与运行 Android 的设备的交互方式。下表列出了适用于 Android 设备的所有设备策略。

APN	应用程序访问	应用程序清单
应用程序锁定	应用程序卸载	凭据
Endpoint Management 选项	Endpoint Management 卸载	文件
Launcher 配置	位置	网络
通行码	限制	计划
应用商店	条款和条件	通道
VPN	Web 剪辑	

注册 **Android** 设备

1. 在 Android 设备上转到 Google Play 应用商店，下载 Citrix Secure Hub 应用程序，然后轻按该应用程序。
2. 系统提示安装应用程序时，单击下一步，然后单击安装。
3. 安装 Secure Hub 后，轻按打开。
4. 对于运行 Android 6.0 及更高版本的设备，请接受所需的权限：
   - 是否允许 Secure Hub 拨打和管理电话？（必需）
   - 是否允许 Secure Hub 访问设备上的照片、媒体和文件？（必需）
   - 是否允许 Secure Hub 访问此设备的位置？（可选）
5. 输入您的企业凭据，例如 Endpoint Management 服务器名称、用户主体名称 (UPN) 或电子邮件地址。然后，单击下一步。
6. 选择如何注册您的设备：
   - 要在 MDM+MAM 中注册，请轻按是，注册。
   - 要在 MAM 中注册，请轻按否。
7. 在 **Activate device administrator**（激活设备管理员）屏幕中，轻按激活。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

8. 输入公司密码，然后轻按登录。
9. 系统可能会要求您创建一个 Citrix PIN，具体取决于 Endpoint Management 的配置方式。可以使用该 PIN 登录 Secure Hub 或其他启用了 Endpoint Management 的应用程序，例如 Secure Mail 和 Citrix Files。请输入 Citrix PIN 两次。在 **Create Citrix PIN**（创建 Citrix PIN）屏幕上，输入一个 PIN。
10. 重新输入 PIN。此时会打开 Secure Hub。这时即可访问应用商店来查看您可以安装在 Android 设备上的应用程序。
11. 如果您在注册后将 Endpoint Management 配置为自动向设备推送应用程序，系统将提示用户安装这些应用程序。此外，您在 Endpoint Management 中配置的策略将部署到设备。轻按安装以安装应用程序。

取消注册和重新注册 **Android** 设备

用户可以从 Secure Hub 内部取消注册。用户通过以下过程取消注册时，设备将仍然在 Endpoint Management 控制台的设备清单中显示。但您无法在设备上执行操作。例如，您无法跟踪设备或监视设备合规性。

1. 轻按以打开 Secure Hub 应用程序。
2. 执行以下操作，具体取决于您拥有的是手机还是平板电脑：

   在手机上：

   - 从屏幕左侧轻扫以打开设置窗格。
   - 依次轻按首选项、帐户和删除帐户。

   在平板电脑上：

   - 轻按右上角的电子邮件地址旁边的箭头。
   - 依次轻按首选项、帐户和删除帐户。
3. 在删除帐户**?** 窗口中，轻按是，删除。
   Secure Hub 将取消注册您的设备。请按照屏幕上的说明重新注册设备。

安全操作

Android 支持以下安全操作。有关每个安全操作的说明，请参阅安全操作。

应用程序锁定	应用程序擦除	证书续订
完全擦除	查找	锁定
锁定并重置密码	通知	吊销
选择性擦除		

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 对于运行 Android 6.0 及更高版本的设备，定位安全操作要求用户在注册过程中授予位置权限。用户可以选择不授予定位权限。如果用户在注册过程中不授予该权限，Endpoint Management 会在发送定位命令时再次申请定位权限。

Firebase Cloud Messaging

July 19, 2022

> 注意：
>
> Firebase Cloud Messaging (FCM) 的前称为 Google Cloud Messaging (GCM)。某些 Endpoint Management 控制台标签和消息使用 GCM 术语。

Citrix 建议使用 Firebase Cloud Messaging (FCM) 来控制将 Android 设备连接到 Endpoint Management 的方式和时间。配置为使用 FCM 时，Endpoint Management 会将连接通知发送到针对 FCM 启用的 Android 设备。任何安全操作或部署命令都将触发推送通知，以提示用户重新连接到 Endpoint Management。

完成本文中的配置步骤且某个设备签入后，该设备将注册到 Citrix Endpoint Management 中的 FCM 服务。该连接允许通过使用 FCM 在 Endpoint Management 服务与您的设备之间实现近乎实时的通信。FCM 注册适用于新设备注册和以前注册的设备。

当 Endpoint Management 需要启动与设备的连接时，它将连接到 FCM 服务。然后，FCM 服务将通知该设备进行连接。这种类型的连接与 Apple 用于其推送通知服务的连接类似。

必备条件

- 最新版本 Secure Hub 客户端
- Google 开发人员帐户凭据
- 在启用了 FCM 的 Android 设备上安装的 Google Play 服务

防火墙端口

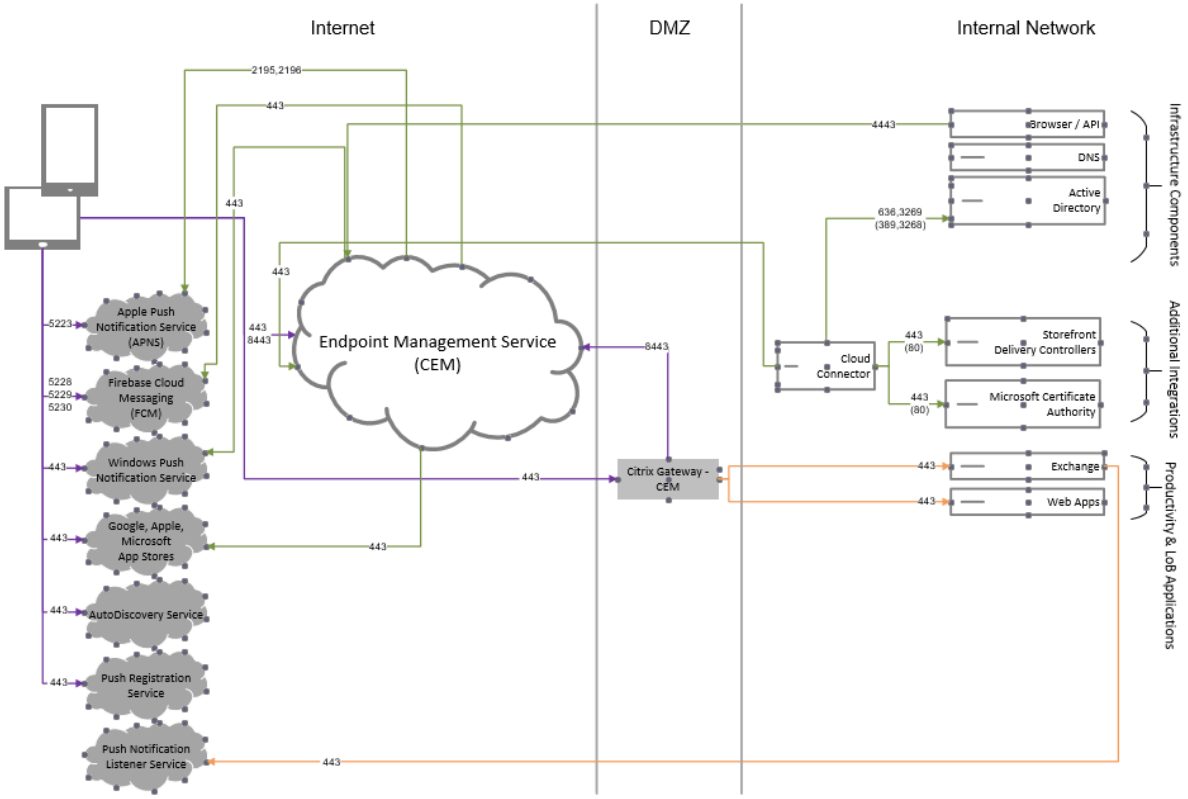
- 将 Endpoint Management 上的端口 443 打开到 `fcm.googleapis.com` 和 `Google.com`。
- 在端口 5228、5229 和 5230 上为设备 Wi-Fi 打开传出 Internet 通信。
- 要允许传出连接，FCM 建议将端口 5228 到 5230 添加到允许列表，且无任何 IP 限制。但是，如果您需要 IP 限制，FCM 建议将 IPv4 和 IPv6 块中的所有 IP 地址添加到允许列表。这些块将在 Google ASN 15169 中列出。每月更新该列表。

有关详细信息，请参阅端口要求。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

体系结构

此图显示了外部和内部网络中 FCM 的通信流。



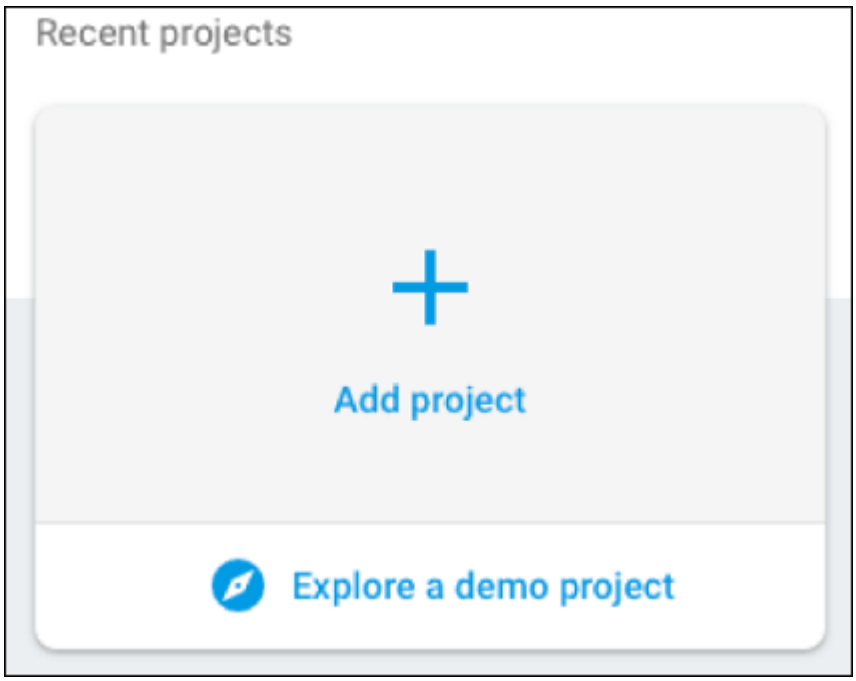
为 **FCM** 配置 **Google** 帐户

1. 使用您的 Google 开发人员帐户凭据登录以下 URL：

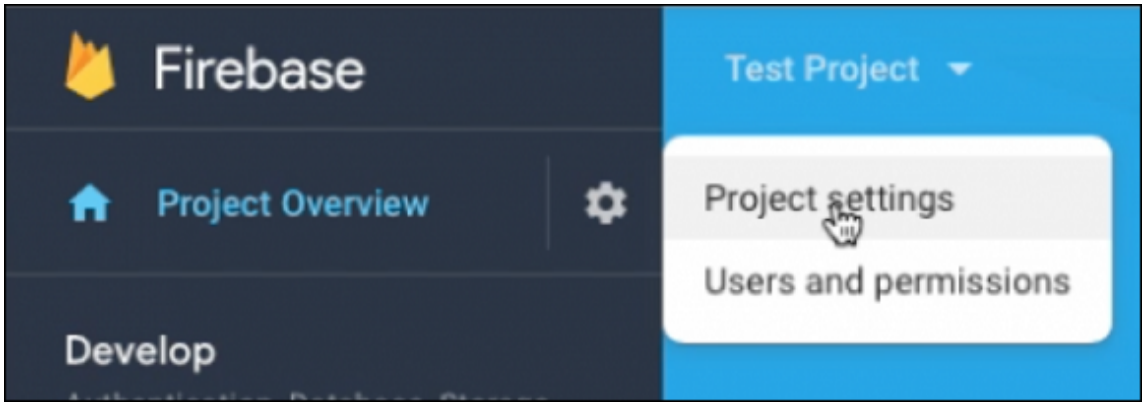
   https://console.firebase.google.com/

2. 单击添加项目。

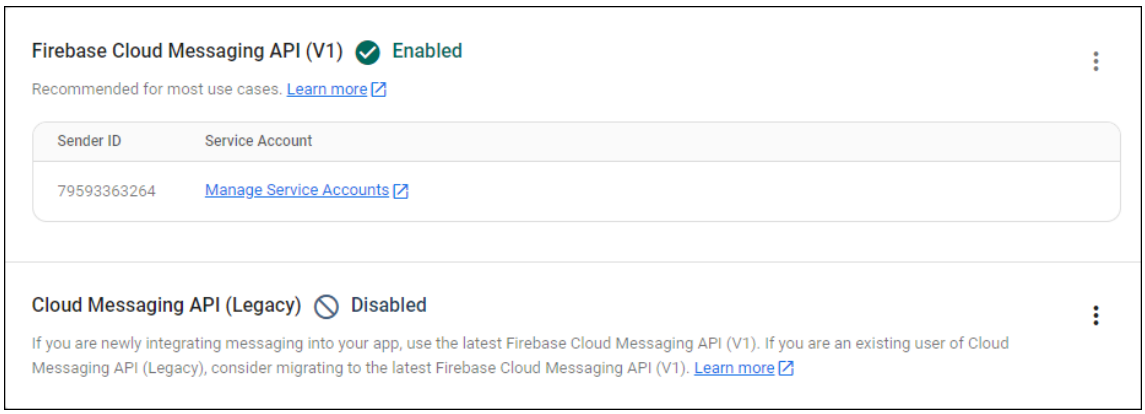
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 创建项目后，单击项目设置。



4. 单击 **Cloud Messaging** 选项卡。确认已启用 Firebase Cloud Messaging API，然后单击管理服务帐户。



5. 复制密钥和 **OAuth 2** 客户端 **ID** 字段中的值。如果您未列出密钥，请单击操作下的省略号以添加新密钥。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

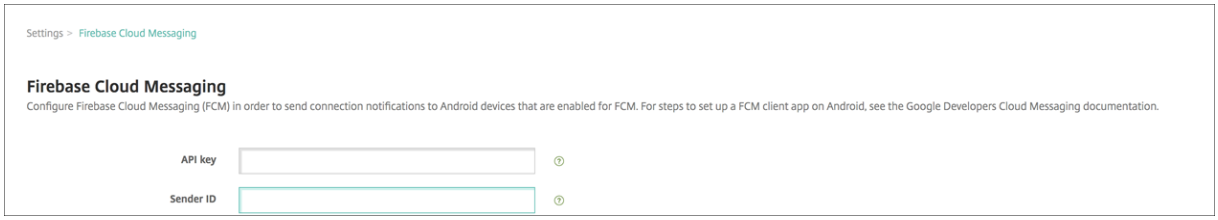


有关在 Android 上设置 FCM 客户端应用程序的步骤，请参阅此 Google Developers Cloud Messaging 文章：https://firebase.google.com/docs/cloud-messaging/android/client。

为 **FCM** 配置 **Endpoint Management**

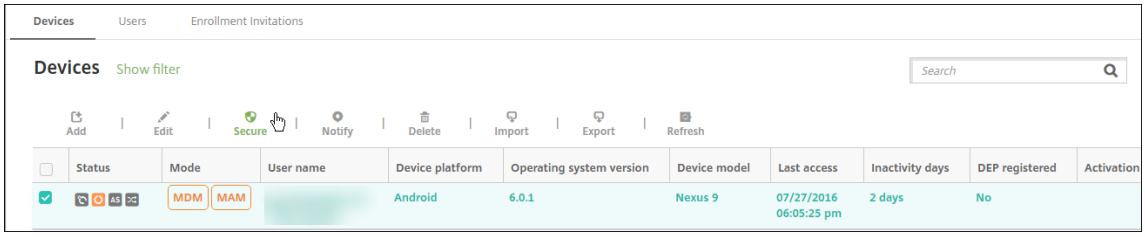
在 Endpoint Management 控制台中，转至设置 **> Firebase Cloud Messaging**。

- 编辑 **API** 密钥，然后键入您在 Firebase Cloud Messaging 配置的最后一步中复制的 Firebase Cloud Messaging 密钥。
- 编辑发件人 **ID**，然后键入您在上一步骤中复制的 **OAuth 2** 客户端 **ID** 值。



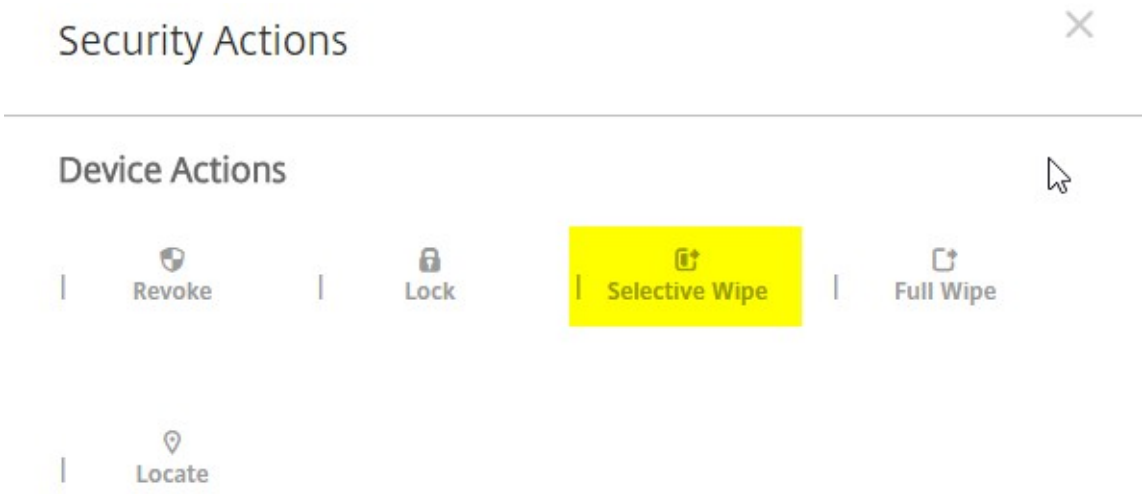
测试您的配置

1. 注册 Android 设备。
2. 保持设备在一段时间内处于空闲状态，以使其与 Endpoint Management 断开连接。
3. 在 Endpoint Management 控制台中，单击管理，选择 Android 设备，然后单击安全。



4. 在设备操作下方，单击选择性擦除。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



成功配置后，即可在设备上执行选择性擦除。

Android SafetyNet

December 3, 2021

您可以配置 Android SafetyNet 功能来评估安装了 Secure Hub 的 Android 设备的兼容性和安全性。Android SafetyNet 不适用于 MAM 部署。

启用此功能后，SafetyNet Attestation API 会检查设备上的软件和硬件信息，以创建该设备的配置文件。然后，API 在已通过 Android 兼容性测试的设备型号列表中查找相同的配置文件。API 还使用此信息确定 Secure Hub 是否已由未知来源修改。

启用 Android SafetyNet 功能后，Secure Hub 会向 Google Play 服务发送 SafetyNet Attestation API 请求，并将结果报告回 Endpoint Management。然后，Endpoint Management 将使用证明结果更新设备信息。可以设置使用证明结果触发设备上的操作的自动操作。

有关 SafetyNet 认证 API 如何工作的更多信息，请参阅 Android 开发人员文档。

预估您需要多少个 **SafetyNet Attestation API** 请求

发送 SafetyNet Attestation API 请求：

- 在 Endpoint Management 中注册设备时。
- 发生 Secure Hub 联机身份验证时。服务器会话过期时或用户注销服务器然后重新登录时会发生联机身份验证。Secure Hub 将提示用户提供凭据以通过服务器进行身份验证。
- 重新启动设备时。
- 按定期循环时间间隔配置，介于 24 到 1000 小时之间。

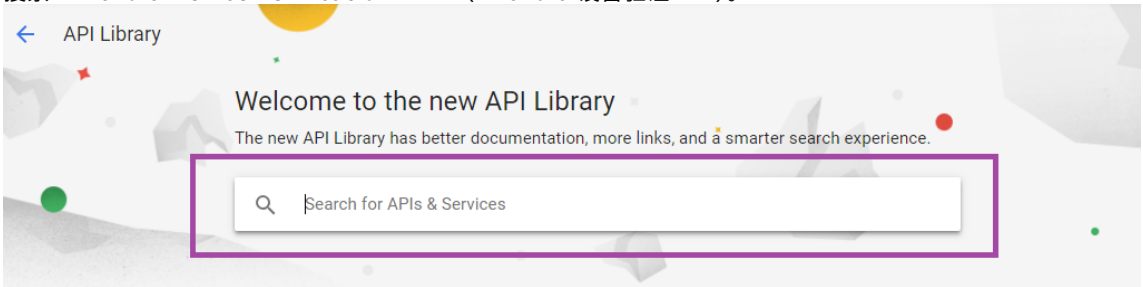
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

如果您的 Endpoint Management 部署每天发出超过 10,000 个请求，请 填写此配额申请表。

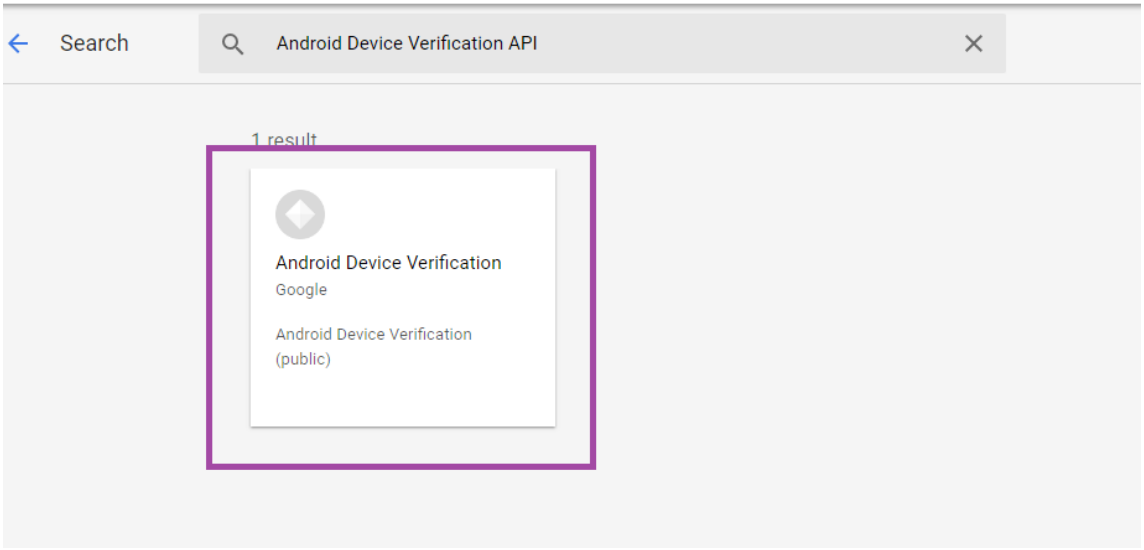
获取 **SafetyNet API** 密钥

要在 Endpoint Management 中启用 Android SafetyNet，您需要 SafetyNet API 密钥。

1. 使用您的 Google 管理员帐户凭据登录到 Google API 控制台。
2. 转到 “Library”（库）页面。
3. 搜索 “Android Device Verification API”（Android 设备验证 API）。

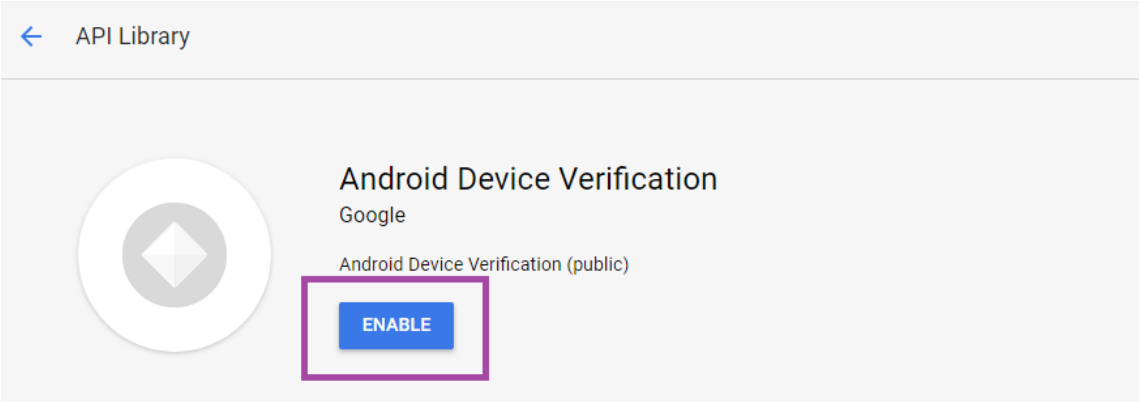


4. 单击 **Android Device Verification API**（Android 设备验证 API）。

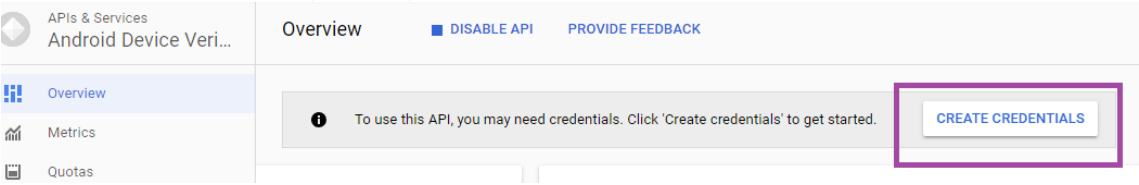


5. 如果 API 尚未启用，请单击 **Enable**（启用）。

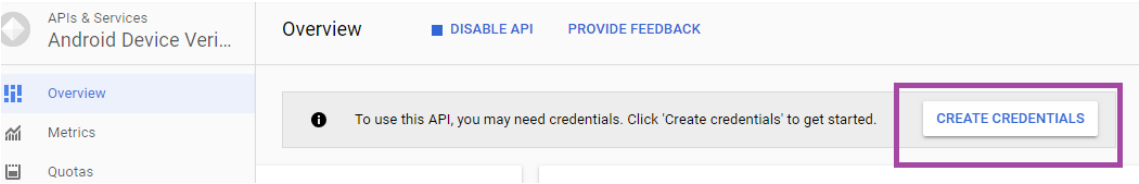
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



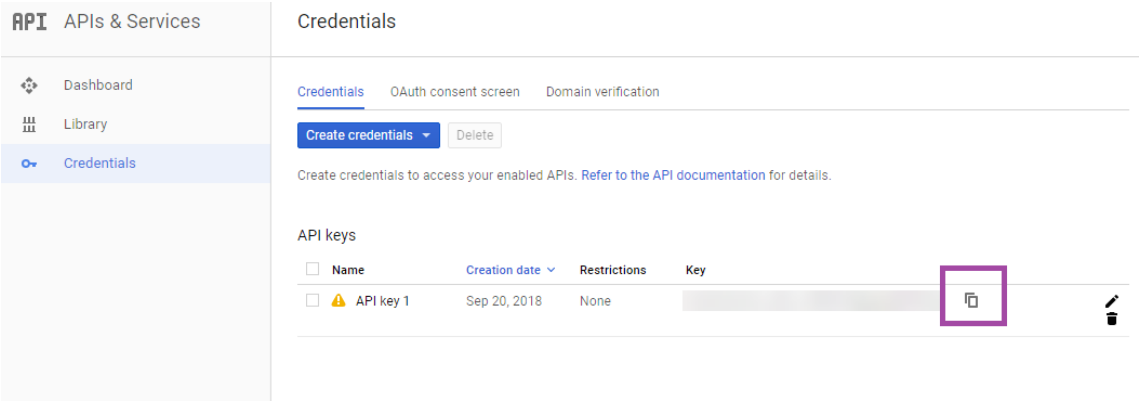
6. 单击管理。
7. 单击 **Create Credentials**（创建凭据）以生成 API 密钥。



8. 选择 **Android Device Verification**（Android 设备验证）单击 **What credentials to I need**（我需要什么凭据）。然后单击 **Done**（完成）。



9. 在 **Credentials**（凭据）页面中，单击密钥旁边的复制图标以复制密钥。



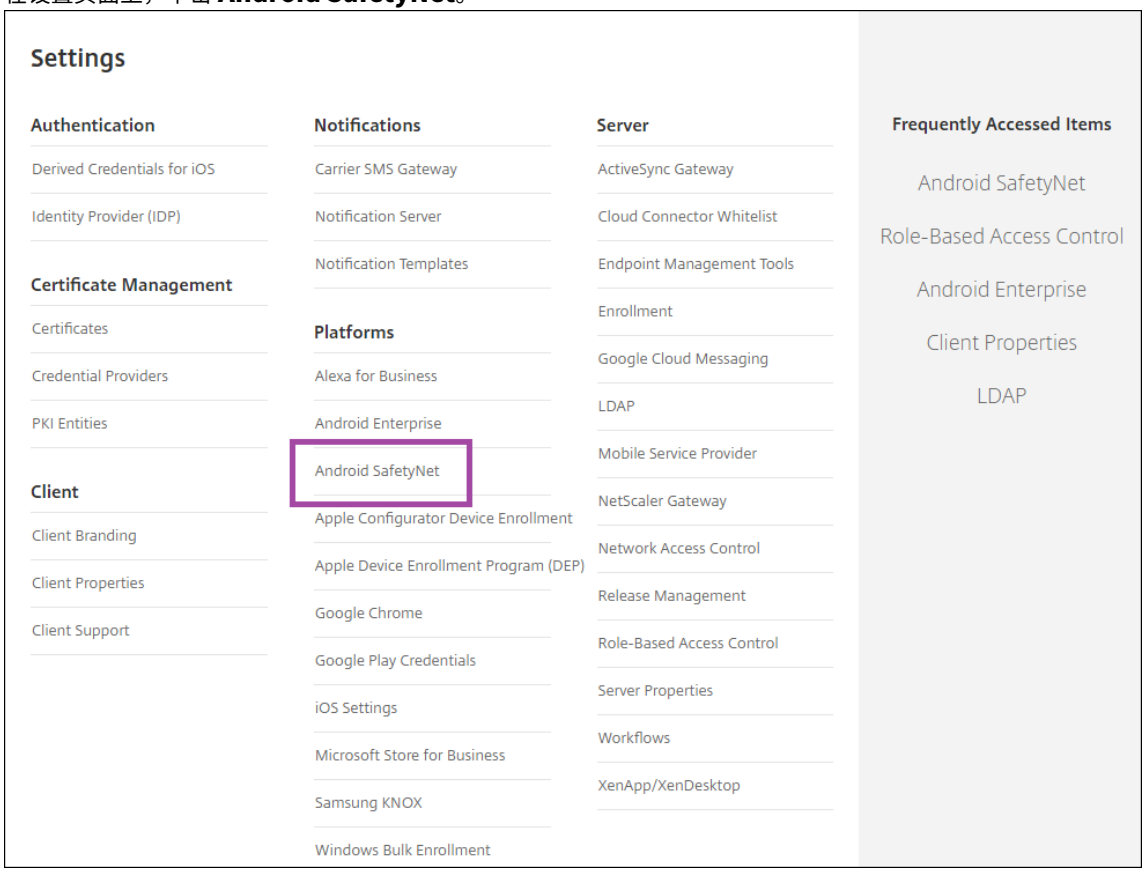
10. 保存密钥，以便您能够在启用 Android SafetyNet 时将其粘贴到 Endpoint Management 控制台中。

启用 **Android SafetyNet**

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。

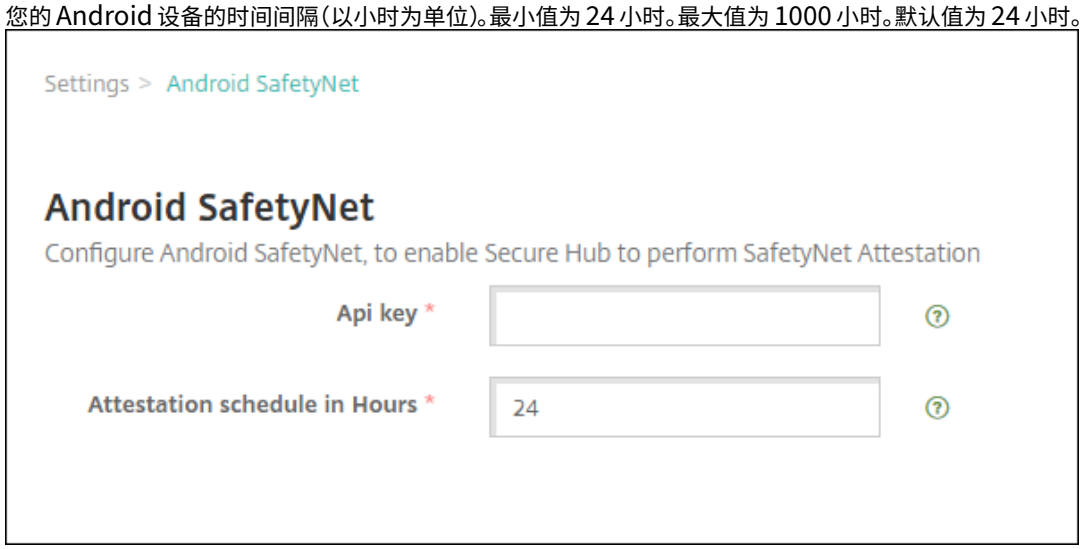
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 在设置页面上，单击 **Android SafetyNet**。



3. 配置以下设置：

   - **API** 密钥。粘贴从 Google API 控制台获取的 SafetyNet API 密钥。
   - **Attestation schedule in hours**（证明时间表 (小时)）。键入 SafetyNet Attestation API 评估您的 Android 设备的时间间隔(以小时为单位)。最小值为 24 小时。最大值为 1000 小时。默认值为 24 小时。



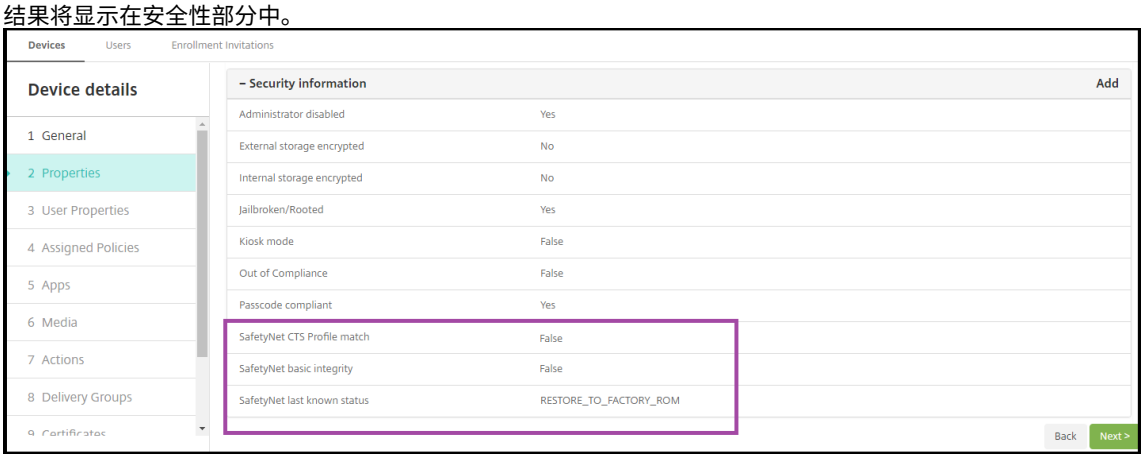
4. 单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

查看 **Android SafetyNet** 结果

要查看设备的 SafetyNet Attestation API 评估结果，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击管理 **>** 设备。
2. 选择 Android 设备以查看 SafetyNet Attestation API 结果。然后单击显示更多。
3. 在设备详细信息页面中，选择属性。
4. 结果将显示在安全性部分中。



SafetyNet Attestation API 为每个设备返回以下状态：

- **SafetyNet CTS profile match**（SafetyNet CTS 配置文件匹配）：如果此值设置为 **True**，则设备具有与已通过 Android 兼容性测试套件 (CTS) 的测试的配置文件匹配。如果此值设置为 **False**，则设备没有与已通过 Android CTS 测试的配置文件匹配的配置文件。
- **SafetyNet basic integrity**（SafetyNet 基本完整性）：如果此值设置为 **True**，则 SafetyNet Attestation API 未发现设备上的 Secure Hub 已被未知来源修改的证据。如果此值设置为 **False**，则设备上的 Secure Hub 已被未知来源修改。
- **SafetyNet last known status**（SafetyNet 上次已知状态）：此值显示设备的上次已知 SafetyNet 状态：
  - **Success**（成功）：SafetyNet Attestation API 未发现设备上的 Secure Hub 已被未知来源修改的证据。
  - **LOCK_BOOTLOADER**：用户应锁定设备的引导装载程序。设备上的 Secure Hub 已被未知来源修改。
  - **RESTORE_TO_FACTORY_ROM**：用户应将设备恢复到干净的出厂 ROM。设备上的 Secure Hub 已被未知来源修改。

Play Integrity API

August 8, 2023

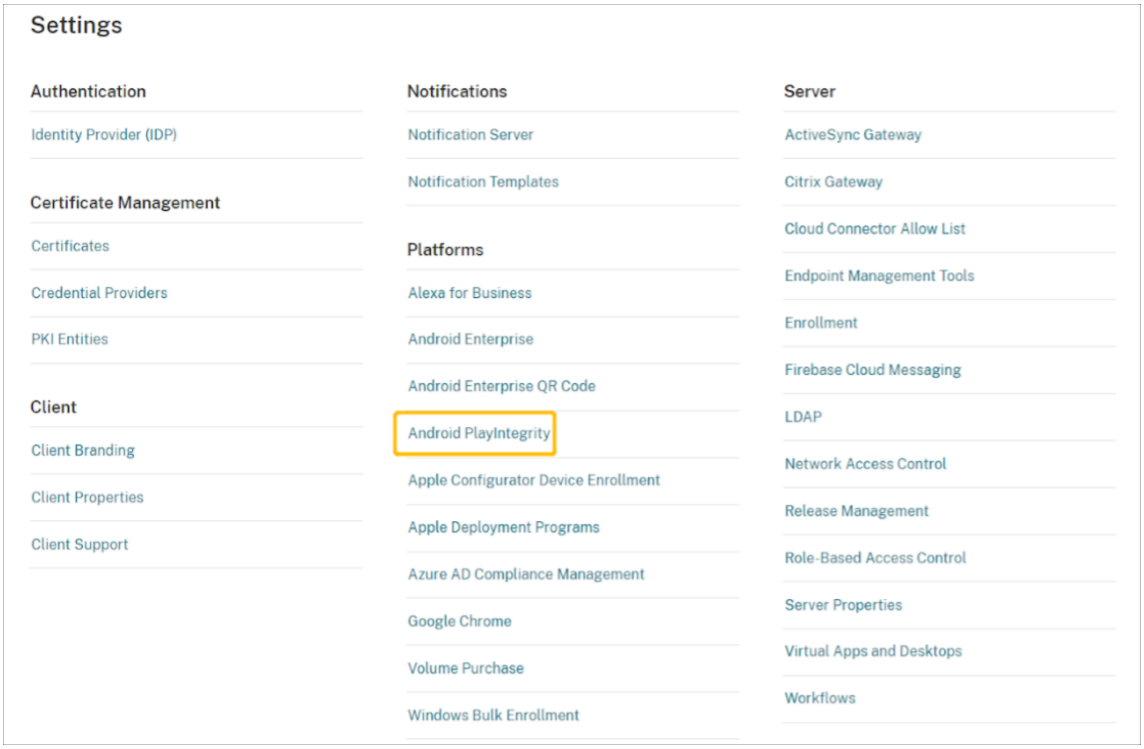
Play Integrity API 有助于保护您的应用程序和游戏免受潜在风险和欺诈性互动（例如作弊和未经授权的访问）的侵害，使您能够采取适当的措施来防止攻击并减少滥用。有关更多信息，请参阅 Play Integrity API。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

启用 **Play Integrity API**

请按照以下步骤切换到 Play Integrity API。

1. 打开 *afw.safetynet.attestation.api*。指定 Citrix Endpoint Management 服务器的弃用功能标志。
2. 在 Endpoint Management 控制台上，从设置页面中选择 **Android PlayIntegrity**。

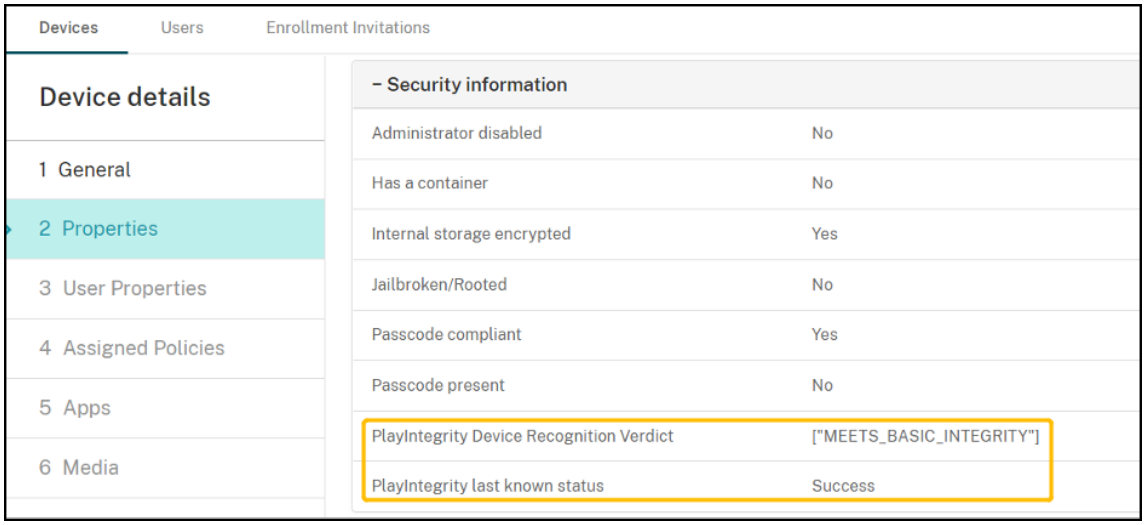


3. 在认证时间表的工时字段中输入一个值。这是 PlayIntegrity Attestation API 评估您的设备的间隔时间。最小值为 24 小时，最大值为 1000 小时。默认值为 24 小时。单击保存。
4. 升级到 Secure Hub Android 版本 23.7.0。从您的设备注销，然后登录 Citrix Secure Hub，以通过 Play Integrity API 触发认证。

查看和分析 **Play Integrity API** 认证结果

1. 在 Endpoint Management 控制台上，转到管理 **>** 设备。
2. 选择要查看 Play Integrity API 认证结果的设备。单击显示更多。
3. 在设备选项卡中，选择属性。结果显示在安全信息部分中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. Play Integrity API 认证返回以下状态：

   - 如果 **PlayIntegrity** 设备识别判决字段包含 **“MEETS_BASIC_INTEGRITY”**，则表示在设备上运行的 Secure Hub 至少通过了基本的系统完整性。
   - 如果 **PlayIntegrity** 设备识别判决字段不包含 **“MEETS_BASIC_INTEGRITY”**，则表示设备上的 Secure Hub 可能在无法识别的 Android 版本中运行，可能有解锁的引导加载程序，或者可能没有经过制造商的认证。
   - 如果 **PlayIntegrity** 的最后已知状态为成功，则表示 PlayIntegrity API 认证已成功运行。
   - 如果 **PlayIntegrity** 的最后已知状态为失败，则表示 PlayIntegrity API 认证无法运行。

> 注意：
>
> 在 SafetyNet Attestation 的最后一次关闭之前（2023 年 11 月底），管理员可以清除允许您使用 SafetyNet 的功能标志。

限制

1. 新注册的 COSU 设备和 DO 设备会被标记为不合规，即使这些设备符合要求也是如此。

   Play Integrity API 在 DO 注册期间首次认证时返回空白，这会使设备看起来不合规。这是 Google 发布的已知问题，DPC Support Lib 20230418 是为了修复这个问题而发布的。

   此修复可从 23.9.0 版本中获得。在此之前，请使用以下步骤作为解决方法：

   - 清除功能标志，继续使用 SafetyNet API 以继续使用 SafetyNet Attestation API。
   - 注册后注销并重新登录即可触发认证。您也可以等待下一次定期认证，默认时间为 24 小时。

   此问题仅在注册期间出现。Play Integrity API 注册后运行良好。

2. 即使设备符合要求，新注册的 WPCOD 设备也会被标记为不合规。Google 正在审查这个问题。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Samsung

December 20, 2022

Samsung 提供了与 Citrix Endpoint Management 兼容的几种解决方案。

要控制 Android 设备连接到 Endpoint Management 服务的方式和时间，请使用 Firebase Cloud Messaging (FCM)。有关信息，请参阅 Firebase Cloud Messaging。

注册配置文件确定 Android 设备在 MAM、MDM 还是 MDM+MAM 中注册，并提供供用户选择退出 MDM 的选项。Endpoint Management 支持对在 MDM+MAM 中注册的 Android 设备使用以下身份验证类型。有关信息，请参阅以下文章：

- 域或域加安全令牌身份验证
- 客户端证书或证书加域身份验证
- 身份提供程序：
  - 通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证
  - 通过 Citrix Cloud 使用 Okta 进行身份验证

另一种罕见的身份验证方法是客户端证书加安全令牌。有关信息，请参阅 https://support.citrix.com/article/CTX215200。

启动 Android 设备管理的一般工作流程如下：

1. 完成登录流程。请参阅载入和资源设置和准备注册设备并交付资源。
2. 选择并配置注册方法。请参阅支持的注册方法。
3. 部署三星许可证密钥。
4. 配置三星设备策略。
5. 设置设备和应用程序安全操作。请参阅安全操作。

有关支持的操作系统，请参阅支持的设备操作系统。

支持的注册方法

下表列出了 Endpoint Management 支持的 Android 设备的注册方法：

方法	支持
手动注册	是
注册邀请	是

有关注册设备的信息，请参阅 注册 Android 设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

部署 **Samsung** 许可证密钥

Samsung 拥有 Enterprise License Management (ELM) 密钥。您从 Samsung 购买 Samsung 许可证。

配置 **Samsung** 设备策略

设备策略：

应用程序限制	应用程序卸载	浏览器
将应用程序复制到 Samsung 容器	Exchange	通行码
限制	VPN	

安全操作

Android 支持以下安全操作。有关每个安全操作的说明，请参阅安全操作。

应用程序锁定	应用程序擦除	证书续订
完全擦除	查找	锁定
锁定并重置密码	通知	吊销
选择性擦除		

> 注意：
>
> 对于运行 Android 6.0 及更高版本的设备，定位安全操作要求用户在注册过程中授予位置权限。用户可以选择不授予定位权限。如果用户在注册过程中不授予该权限，Endpoint Management 会在发送定位命令时再次申请定位权限。

网络访问控制

November 7, 2022

可以使用网络访问控制 (NAC) 解决方案扩展 Android 和 Apple 设备的 Endpoint Management 设备安全评估。您的 NAC 解决方案使用 Endpoint Management 安全评估帮助制定和处理身份验证决策。配置 NAC 设备后，将强制执行在 Endpoint Management 中配置的设备策略和 NAC 过滤器。

将 Endpoint Management 与 NAC 解决方案结合使用可提高 QoS，并对网络内部的设备进行更精细的控制。有关

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

将 NAC 与 Endpoint Management 集成的优势的摘要，请参阅 访问控制。

Citrix 支持以下与 Endpoint Management 集成的解决方案：

- Citrix Gateway
- ForeScout

Citrix 不保证其他 NAC 解决方案的集成。

使用网络中的 NAC 设备：

- Endpoint Management 支持 NAC 作为 iOS、Android Enterprise 和 Android 设备的端点安全功能。
- 可以在 Endpoint Management 中启用过滤器，以便根据规则或属性将设备设置为对 NAC 合规或不合规。例如：
  - 如果 Endpoint Management 中的托管设备不符合指定的条件，Endpoint Management 会将该设备标记为不合规。NAC 设备会阻止网络中的不合规设备。
  - 如果 Endpoint Management 中的托管设备安装了不合规的应用程序，NAC 过滤器可以阻止建立 VPN 连接。因此，不合规的用户设备无法通过 VPN 访问应用程序或 Web 站点。
  - 如果将 Citrix Gateway 用于 NAC，则可以启用拆分隧道，以防止 Citrix Gateway 插件向 Citrix Gateway 发送不必要的网络流量。有关拆分隧道的详细信息，请参阅配置拆分隧道。

支持的 **NAC** 合规性过滤器

Endpoint Management 支持以下 NAC 合规性过滤器：

匿名设备：检查设备是否处于匿名模式。如果在设备尝试重新连接时 Endpoint Management 无法重新对用户进行身份验证，则可以执行此检查。

禁止的应用程序：检查设备是否具有应用程序访问策略中定义的禁止的应用程序。有关该策略的更多信息，请参阅 应用程序访问设备策略。

不活动设备：按照服务器属性中 **Device Inactivity Days Threshold**（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。有关详细信息，请参阅服务器属性。

缺少所需的应用程序：检查设备是否缺少在应用程序访问策略中定义的任何所需的应用程序。

非推荐应用程序：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码：检查用户密码是否合规。在 iOS 和 Android 设备上，Endpoint Management 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。例如，在 iOS 设备上，如果 Endpoint Management 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规设备”属性检查设备是否不合规。通常情况下，使用 Endpoint Management API 的自动操作或第三方会更改该属性。

吊销状态：检查设备证书是否已吊销。再次授权之前，已吊销的设备无法重新注册。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

已获得 **root** 权限的 **Android** 设备和已越狱的 **iOS** 设备：检查 Android 设备或 iOS 设备是否已被越狱。

非托管设备：检查 Endpoint Management 是否正在管理设备。例如，在 MAM 下注册的设备或已取消注册的设备为非托管设备。

> 注意：
>
> “隐式合规/不合规”过滤器仅在 Endpoint Management 管理的设备上设置默认值。例如，任何安装了阻止的应用程序或未注册的设备都将被标记为“不合规”。NAC 设备会阻止您的网络中的这些设备。

配置概述

我们建议您按照列出的顺序配置 NAC 组件。

1. 配置设备策略以支持 NAC：

   对于 **iOS** 设备：请参阅配置 VPN 设备策略以支持 NAC。

   对于 **Android Enterprise** 设备：请参阅为 Citrix SSO 创建 Android Enterprise 托管配置。

   对于 **Android** 设备：请参阅 配置适用于 Android 的 Citrix SSO 协议。

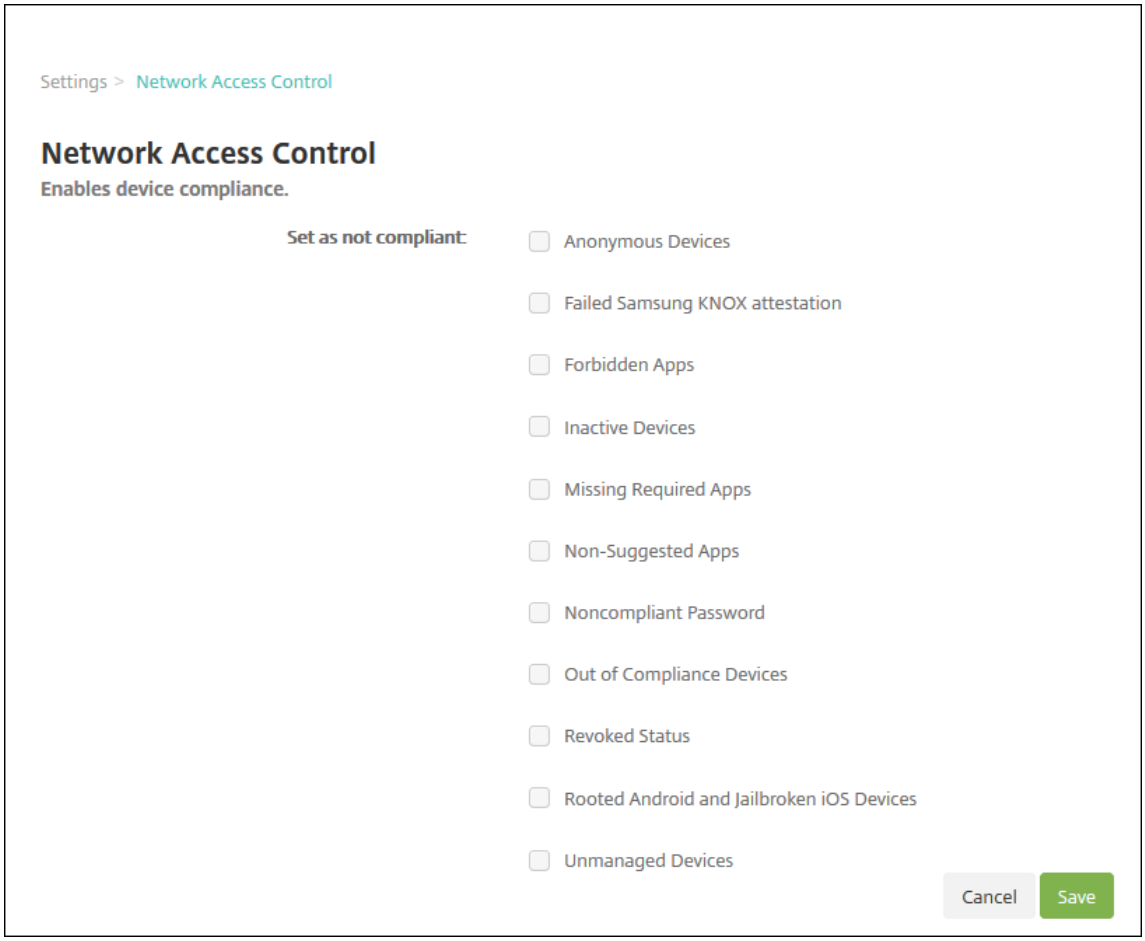
2. 在 Endpoint Management 中启用 NAC 筛选器。
3. 配置 NAC 解决方案：
   - Citrix Gateway，详见更新 Citrix Gateway 策略以支持 NAC。

     要求您在设备上安装 Citrix SSO。请参阅 Citrix Gateway 客户端。
   - ForeScout：请参阅 ForeScout 文档。

在 **Endpoint Management** 中启用 **NAC** 过滤器

1. 在 Endpoint Management 控制台中，转到设置 **>** 网络访问控制。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 选中要启用的设为不合规过滤器旁边的复选框。
3. 单击保存。

更新 **Citrix Gateway** 策略以支持 **NAC**

必须在 VPN 虚拟服务器上配置高级（非传统）身份验证和 VPN 会话策略。

以下步骤使用以下任一特性更新 Citrix Gateway：

- 与 Endpoint Management 集成。
- 或者，为 VPN 进行设置，而非作为 Endpoint Management 环境的一部分，并且可以访问 Endpoint Management。

在您的虚拟 VPN 服务器上，从控制台窗口中执行以下操作：命令和示例中的 FQDN 和 IP 地址是虚构的。

1. 如果要在您的 VPN 虚拟服务器上使用经典策略，请删除并取消绑定所有经典策略。要进行检查，请键入：

   ```
   show vpn vserver <VPN_VServer>
   ```

   删除包含单词 Classic 的所有结果。例如：`VPN Session Policy Name: PL_OS_10.10.1.1 Type : Classic Priority: 0`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要删除策略，请键入：

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. 请通过键入以下命令创建相应的高级会话策略。

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

例如：`add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. 请通过键入以下命令将策略绑定到您的 VPN 虚拟服务器。

```
bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
```

4. 请通过键入以下命令创建身份验证虚拟服务器。

```
add authentication vserver <authentication vserver name> <service type>
 <ip address>
```

例如：`add authentication vserver authvs SSL 0.0.0.0`
在此示例中，`0.0.0.0` 表示身份验证虚拟服务器不面向公众开放。

5. 请通过键入以下命令将 SSL 证书与虚拟服务器绑定在一起。

```
bind ssl vserver <authentication vserver name> -certkeyName <Webserver
certificate>
```

例如：`bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. 请从 VPN 虚拟服务器将身份验证配置文件关联到身份验证虚拟服务器。首先，请通过键入以下命令创建身份验证配置文件。

```
add authentication authnProfile <profile name> -authnVsName <authentication
 vserver name>
```

例如：

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. 请通过键入以下命令将身份验证配置文件与 VPN 虚拟服务器关联。

```
set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
```

例如：

```
set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
```

8. 请通过键入以下命令检查从 Citrix Gateway 到设备的连接。

```
curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/
Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
```

例如，此查询通过获取在环境中注册的第一台设备 (`deviceid_1`) 的合规性状态来验证连接性：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
```

成功的结果与以下示例类似。

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. 上一个步骤成功时，请创建对 Endpoint Management 的 Web 身份验证操作。首先，请创建一个策略表达式以从 iOS VPN 插件中导出设备 ID。键入以下命令。

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. 请通过键入以下命令向 Endpoint Management 发送请求。在此示例中，Endpoint Management IP 是 10.207.87.82，FQDN 为 example.em.cloud.com:4443。

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
    ```

    Endpoint Management NAC 的成功输出为 HTTP status 200 OK。X-Citrix-Device-State 标头的值必须为 Compliant。

11. 请通过键入以下命令创建一个要将操作关联到的身份验证策略。

    ```
    add authentication Policy <policy name> -rule <rule> -action <web authentication action>
    ```

    例如：add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac

12. 请通过键入以下命令将现有 LDAP 策略转换为高级策略。

    ```
    add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>
    ```

    例　　如：add authentication Policy ldap_xm_test_pol -rule **true** -action 10.10.1.1_LDAP

13. 请通过键入以下命令添加要将 LDAP 策略关联到的策略标签。

    ```
    add authentication policylabel <policy_label_name>
    ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

例如：`add authentication policylabel ldap_pol_label`

14. 请通过键入以下命令将 LDAP 策略关联到策略标签。

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol
 -priority 100 -gotoPriorityExpression NEXT
```

15. 请连接合规设备以执行 NAC 测试，以确认成功的 LDAP 身份验证。键入以下命令。

```
bind authentication vserver <authentication vserver> -policy <web
authentication policy> -priority 100 -nextFactor <ldap policy label> -
gotoPriorityExpression END
```

16. 添加 UI 以与身份验证虚拟服务器相关联。请键入以下命令以检索设备 ID。

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -
action lschema_single_factor_deviceid
```

17. 请通过键入以下命令绑定身份验证虚拟服务器。

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority
 100 -gotoPriorityExpression END
```

18. 创建 LDAP 高级身份验证策略以启用 Secure Hub 连接。键入以下命令。

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority
110 -gotoPriorityExpression NEXT
```

iOS

February 14, 2022

要在 Endpoint Management 中管理 iOS 设备，应设置 Apple 提供的 Apple 推送通知服务 (APNs) 证书。有关信息，请参阅 APNs 证书。

注册配置文件确定 iOS 设备是否在 MDM+MAM 模式下注册，并带有用户可选择退出移动设备管理 (MDM) 的选项。Endpoint Management 支持对 MDM+MAM 中的 iOS 设备使用以下身份验证类型。有关信息，请参阅以下文章：

- 域或域加安全令牌身份验证
- 客户端证书或证书加域身份验证
- 身份提供程序：
  - 通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证
  - 通过 Citrix Cloud 使用 Okta 进行身份验证

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **iOS 13** 中对可信证书的要求：
>
> Apple 对 TLS 服务器证书有新的要求。验证所有证书都符合 Apple 的新要求。请参阅 Apple 出版物 https://support.apple.com/en-us/HT210176。有关管理证书方面的帮助，请参阅上载证书。

启动 iOS 设备管理的一般工作流程如下：

1. 完成登录流程。请参阅载入和资源设置和准备注册设备并交付资源。
2. 选择并配置注册方法。请参阅支持的注册方法。
3. 配置 iOS 设备策略。
4. 注册 iOS 设备。
5. 设置设备和应用程序安全操作。请参阅安全操作。

有关支持的操作系统，请参阅支持的设备操作系统。

iOS 14 兼容性

Endpoint Management 和 Citrix 移动应用程序与 iOS 14 兼容，但目前不支持新的 iOS 14 功能。

对于受监督的 iOS 设备，您最多可以将软件升级延迟 90 天。在适用于 iOS 的“限制”设备策略中，请使用以下设置：

- 强制执行延迟的软件更新
- 强制执行软件更新延迟

请参阅 iOS 设置。这些设置不适用于用户注册模式或非监督（完全 MDM）模式下的设备。

必须保持公开状态的 Apple 主机名

某些 Apple 主机名必须保持打开状态，以确保 iOS、macOS 和 Apple App Store 的正常运行。阻止这些主机名可能会影响以下对象的安装、更新和正确操作：iOS、iOS 应用程序、MDM 操作以及设备和应用程序注册。有关详细信息，请参阅 https://support.apple.com/en-us/HT201999。

支持的注册方法

可以在注册配置文件中指定如何管理 iOS 设备。可以在以下注册设置之间进行选择：

- **Apple User Enrollment**（Apple 用户注册）：对于 BYOD 设备，请为个人数据的隐私性和企业数据的安全性提供一个平衡点。此注册模式作为公共预览版提供。要启用此功能，请联系您的支持团队。
- **Apple Device Enrollment**（Apple 设备注册）：对于受监督的 iOS 设备，请在设备上安装单独的个人配置文件和公司配置文件。
- **Do not manage devices**（请勿管理设备）：如果只希望管理应用程序，请从 MDM 中排除这些设备。

有关创建注册配置文件的详细信息，请参阅注册配置文件。

Endpoint Management 支持对 iOS 设备使用以下注册方法：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

方法	支持
Apple 商务管理	是
Apple 校园教务管理	是
Apple Configurator	是
手动注册	是
注册邀请	是

Apple 部署计划包括适用于企业组织的 Apple 商务管理 (ABM) 和适用于教育组织的 Apple 校园教务管理 (ASM)。有关详细信息，请参阅通过 Apple 部署计划部署设备。

Apple 校园教务管理的类型为教育 Apple 部署类型。请参阅与 Apple 教育功能相集成。

请使用 Apple 部署计划批量注册 iOS、iPadOS、macOS 和 tvOS 设备。可以直接从 Apple 、参与计划的 Apple 授权经销商或运营商处购买这些设备。无论您是否直接从 Apple 购买 iOS 设备，都可以使用 Apple Configurator 注册这些设备。请参阅批量注册 Apple 设备。

托管 **Apple ID**

用户注册与托管 Apple ID 紧密集成。可以使用 ABM/ASM 手动创建托管 Apple ID，或者通过 Azure Active Directory (AAD) 动态创建托管 Apple ID。

对于非联合身份验证，请使用 ABM/ASM 创建托管 Apple ID 以添加帐户。有关在 ABM/ASM 中添加帐户的信息，请参阅网址为 `https://support.apple.com/guide/apple-business-manager/welcome/web` 的 Apple 文档和网址为 `https://support.apple.com/guide/apple-school-manager/welcome/web` 的 ASM。我们建议您在用户注册时执行以下操作以避免执行额外的步骤：

- 在创建托管 Apple ID 时，请使用与公司电子邮件地址匹配的电子邮件。
- 将用户角色设置为员工。
- 要求用户在注册之前手动更改密码。请告知用户，我们建议您使用与企业帐户相同的密码。

要动态创建托管 Apple ID，请将 Citrix Cloud 配置为使用 AAD 作为其身份提供程序。有关将 Citrix Cloud 配置为使用 AAD 的详细信息，请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。此外，请在 ABM/ASM 中配置联合身份验证。要了解有关在 ABM 或 ASM 中配置联合身份验证的更多信息，请参阅《Apple 商务管理用户指南》和《Apple 校园教管理用户指南》。

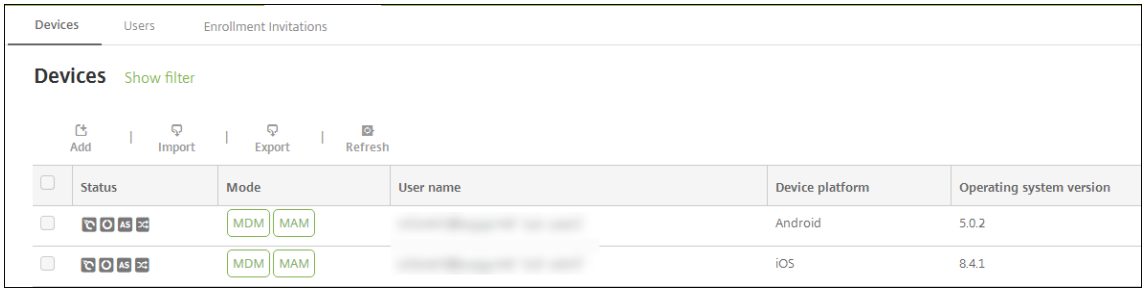
手动创建托管 Apple ID 时，可以配置自定义域来代替默认域使用。您配置的自定义域将替换现有域。例如，您的企业电子邮件地址采用格式 `first.last@company.com`，但您希望改为使用 `mycompany.website.com` 作为托管 Apple ID 的域。在 ABM/ASM 上创建托管 Apple ID 时，电子邮件地址将变为 `first.last@mycompany.website.com`。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

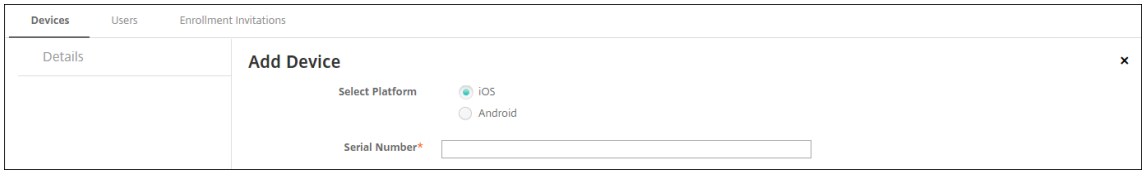
手动添加 **iOS** 设备

如果要手动添加 iOS 设备（例如用于测试目的），请按照以下步骤进行操作。

1. 在 Endpoint Management 控制台中，单击管理 **>** 设备。此时将显示设备页面。



2. 单击添加。此时将显示添加设备页面。



3. 配置以下设置：

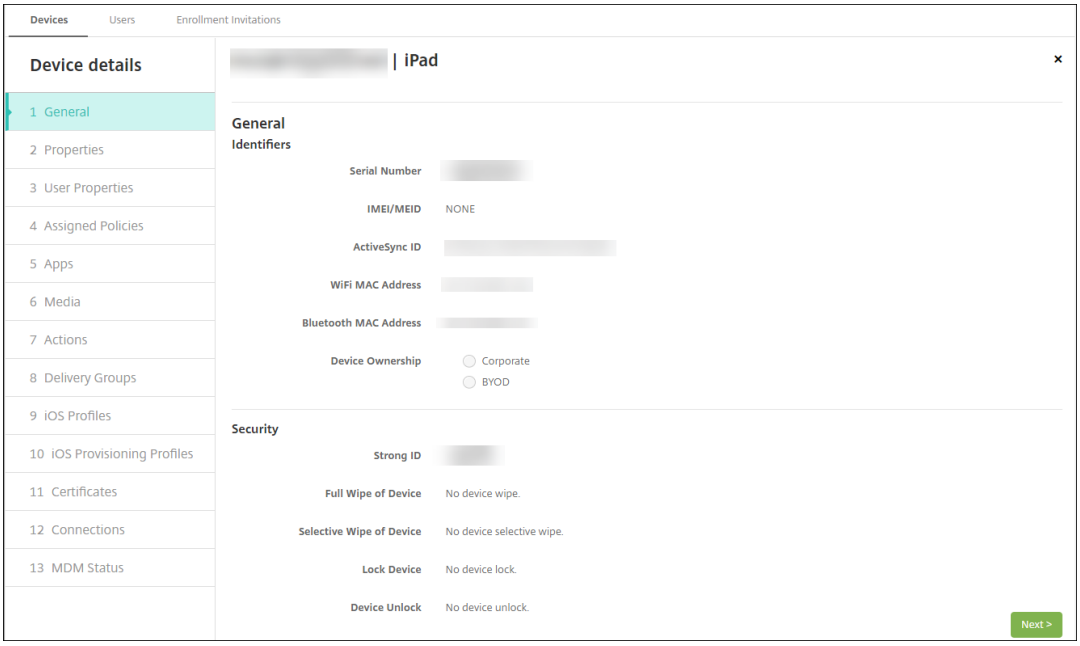
   - 选择平台：单击 **iOS**。
   - 序列号：键入设备序列号。

4. 单击添加。设备将添加到所显示设备表的列表底部。要查看并确认设备详细信息，请执行以下操作：选择已添加的设备，然后在显示的菜单中，单击编辑。

   > 注意：
   >
   > 选中某个设备旁边的复选框时，选项菜单将在设备列表上方显示。如果单击列表中的其他任意位置，选项菜单将在列表右侧显示。

   - 已配置 LDAP
   - 如果使用本地组和本地用户：
     - 一个或多个本地组。
     - 分配给本地组的本地用户。
     - 交付组与本地组相关联。
   - 如果使用 Active Directory：
     - 交付组与 Active Directory 组相关联。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



5. 常规页面列出设备标识符，例如，序列号和平台类型的其他信息。对于设备所有权，请选择公司或 **BYOD**。

   常规页面还列出了设备安全属性，例如，强 ID、锁定设备、激活锁绕过和平台类型的其他信息。完全擦除设备字段包括用户的 PIN 代码。擦除设备后，用户必须输入该代码。如果用户忘记了该代码，您可以在此处查找。

6. 属性页面列出了 Endpoint Management 预配的设备属性。此列表显示了用于添加设备的预配文件中包含的任何设备属性。要添加属性，请单击添加，然后从列表中选择一种属性。有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

   添加属性时，它最初将显示在添加了该属性的类别下方。单击下一步，然后返回属性页面后，属性将显示在相应列表中。

   要删除某个属性，请将鼠标悬停在列表上方，然后单击右侧的 **X**。Endpoint Management 会立即删除该项目。

7. 其余的设备详细信息部分包含设备的摘要。

   - 用户属性：显示用户的 RBAC 角色、组成员身份、批量购买帐户和属性。可以从此页面停用批量购买帐户。
   - 已分配的策略：显示已部署、挂起和失败的策略数量。提供每个策略的策略名称、类型和上次部署信息。允许您将部署状态重置为挂起，然后重新部署用户删除的策略。
   - 应用程序：显示上一个清单的已安装、挂起和失败的应用程序部署数量。提供应用程序名称、标识符、类型和其他信息。有关 iOS 和 macOS 清单密钥（例如 **HasUpdateAvailable**）的说明，请参阅移动设备管理 (MDM) 协议。
   - 媒体：显示上一个清单的已部署、挂起和失败的媒体部署数量。
   - 操作：显示已部署、挂起和失败的操作数量。提供上一个部署的操作名称和时间。
   - 交付组：显示成功、挂起和失败的交付组数量。对于每个部署，提供交付组的名称和部署时间。选择一个交付组以查看更多详细信息，包括状态、操作以及通道或用户。
   - **iOS** 配置文件：显示上一个 iOS 配置文件清单，包括名称、类型、组织和说明。
   - **iOS** 预配配置文件：显示企业分发预配配置文件信息，例如 UUID、过期日期以及托管状态。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 证书：显示有效证书、已过期证书或已吊销证书信息，例如，类型、提供程序、颁发者、序列号、过期之前的剩余天数。
- 连接：显示第一个连接状态和最后一个连接状态。提供每个连接的用户名、倒数第二次身份验证和上次身份验证时间。
- **MDM** 状态：显示 MDM 状态、上次推送时间以及上次设备答复时间等信息。

配置 iOS 设备策略

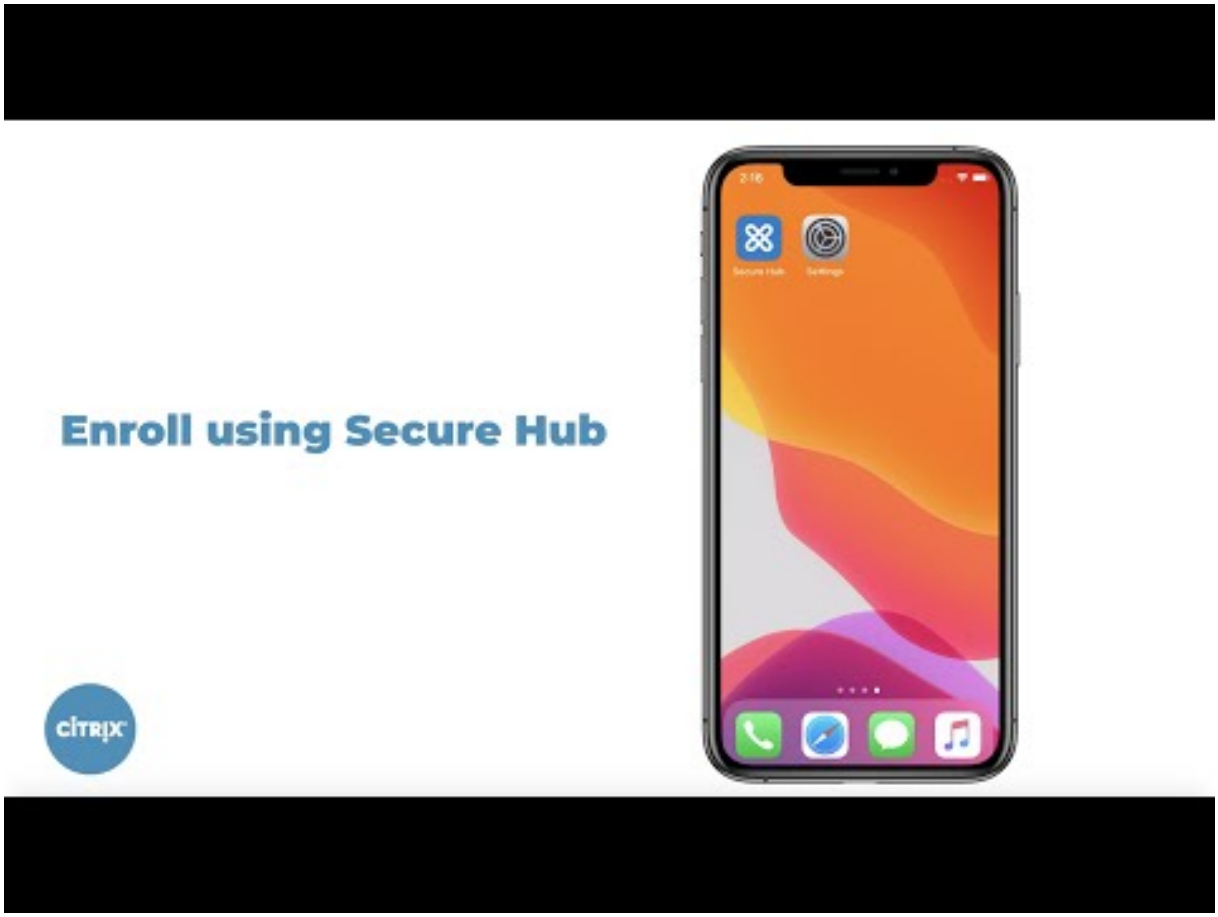
使用这些策略可配置 Endpoint Management 与运行 iOS 或 iPadOS 的设备的交互方式。下表列出了适用于 iOS 和 iPadOS 设备的所有设备策略。

AirPlay 镜像	AirPrint	APN
应用程序访问	应用程序属性	应用程序配置
应用程序清单	应用程序锁定	应用程序卸载
应用程序通知	蓝牙	日历 (CalDav)
手机网络	联系人 (CardDAV)	凭据
设备名称	教育配置	Exchange
字体	主屏幕布局	导入 iOS 和 macOS 配置文件
LDAP	位置	锁屏界面消息
邮件	托管域	最大常驻用户数
MDM 选项	网络	网络使用情况
组织信息	操作系统更新	通行码
通行码锁宽限期	个人热点	配置文件删除
预配配置文件	删除预配配置文件	代理
限制	漫游	SCEP
SSO 帐户	存储	已订阅的日历
条款和条件	VPN	壁纸
Web 内容过滤器	Web 剪辑	

注册 iOS 设备

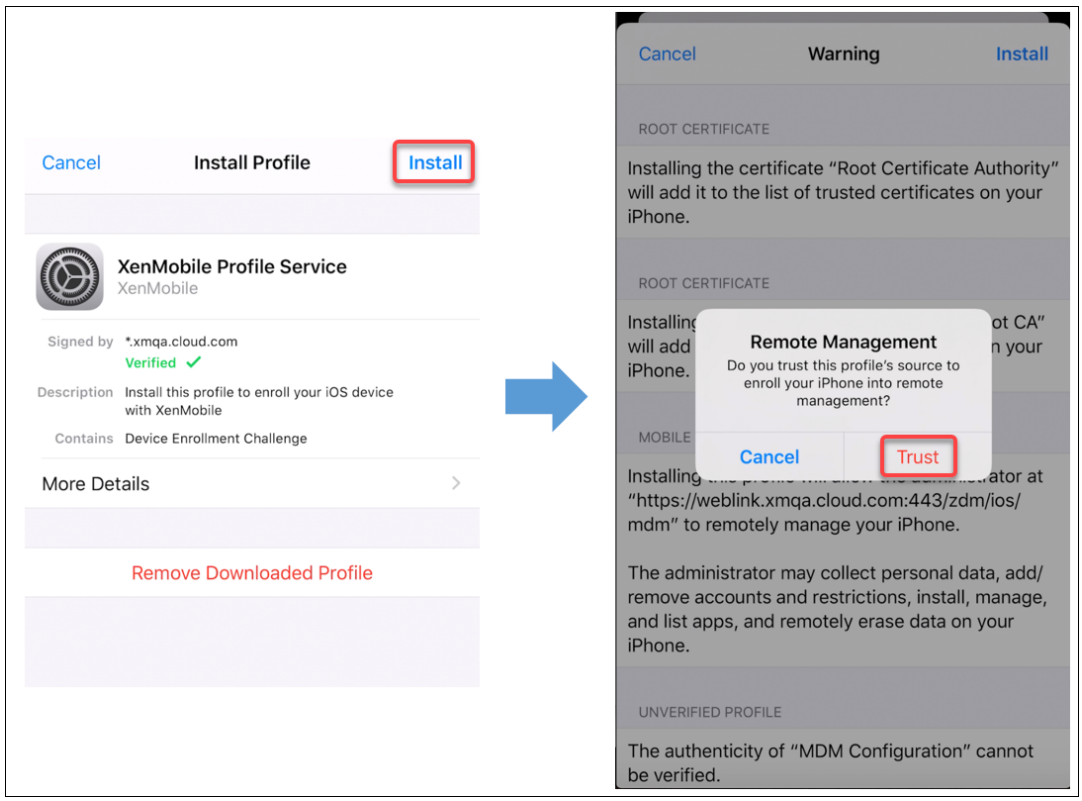
本部分内容介绍用户如何将 iOS 设备（12.2 或更高版本）注册到 Endpoint Management。有关 iOS 注册的详细信息，请观看以下视频：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



1. 在 iOS 设备上转到 Apple 应用商店，下载 Citrix Secure Hub 应用程序，然后轻按该应用程序。
2. 当系统提示安装应用程序时，轻按下一步，然后轻按安装。
3. 安装 Secure Hub 后，轻按打开。
4. 输入您的企业凭据，例如 Endpoint Management 服务器名称、用户主体名称 (UPN) 或电子邮件地址。然后，单击下一步。
5. 轻按是，注册以注册 iOS 设备。
6. 此时将显示 Endpoint Management 收集的数据列表。单击下一步。显示组织如何使用该数据的说明。单击下一步。
7. 键入凭据后，在出现提示时轻按允许以下载配置文件。下载配置文件后，轻按关闭。
8. 在设备设置中，安装 XenMobile 配置文件。
    - 转到设置 **>** 常规 **>** 配置文件 **> XenMobile** 配置文件服务，然后轻按安装以添加配置文件。
    - 在通知窗口中，轻按信任，将您的设备注册到远程管理中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



9. 注册成功后，打开 Secure Hub。如果要注册到 MDM+MAM：验证凭据后，在出现提示时创建并确认您的 Citrix PIN。
10. 工作流程完成后，注册设备。随后即可访问应用商店来查看您安装在 iOS 设备上的应用程序。

安全操作

iOS 的设备注册支持以下安全操作。有关每个安全操作的说明，请参阅安全操作。

- 激活锁绕过
- 应用程序锁定
- 应用程序擦除
- ASM 激活锁
- 证书续订
- 清除限制
- 启用/禁用丢失模式
- 启用/禁用跟踪
- 完全擦除
- 查找
- 锁定
- 响铃
- 请求使用/停止使用 AirPlay 镜像
- 重新启动/关闭

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 吊销/授权
- 选择性擦除
- 解锁

iOS 的用户注册支持以下安全操作：

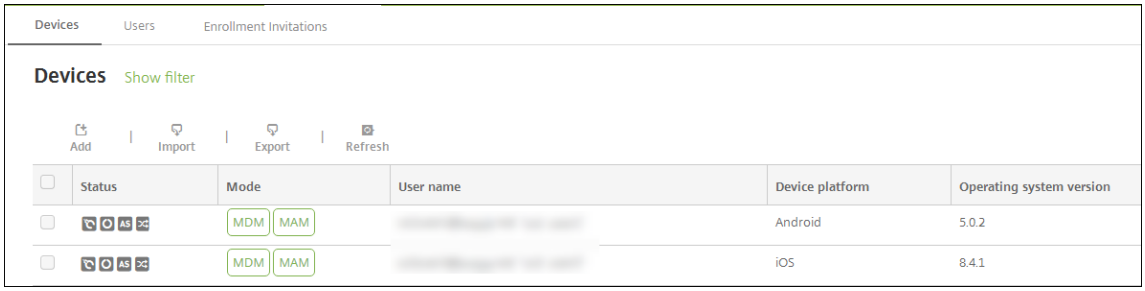
- 吊销
- 锁定
- 选择性擦除
- 证书续订

锁定 **iOS** 设备

您可以锁定丢失的 iOS 设备，同时在设备锁屏界面上显示消息和电话号码。

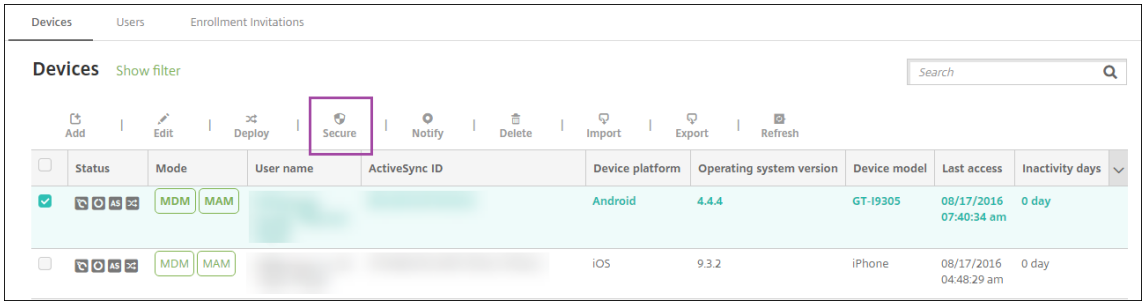
要在锁定的设备上显示消息和电话号码，请在 Endpoint Management 控制台中将通行码策略设置为 **true**。用户可以改为手动在设备上启用通行码。

1. 单击管理 **>** 设备。此时将显示设备页面。

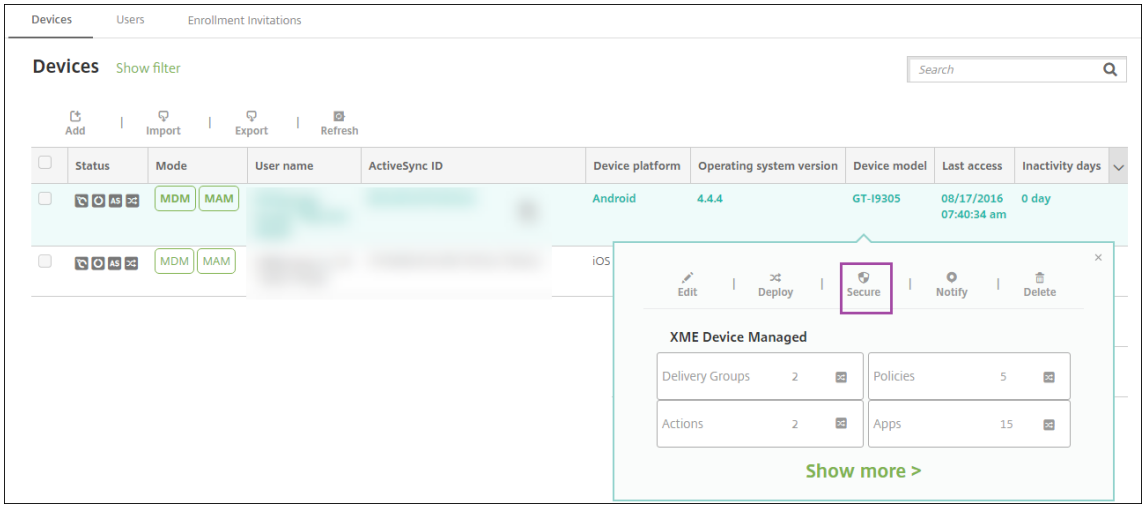


2. 选择要锁定的 iOS 设备。

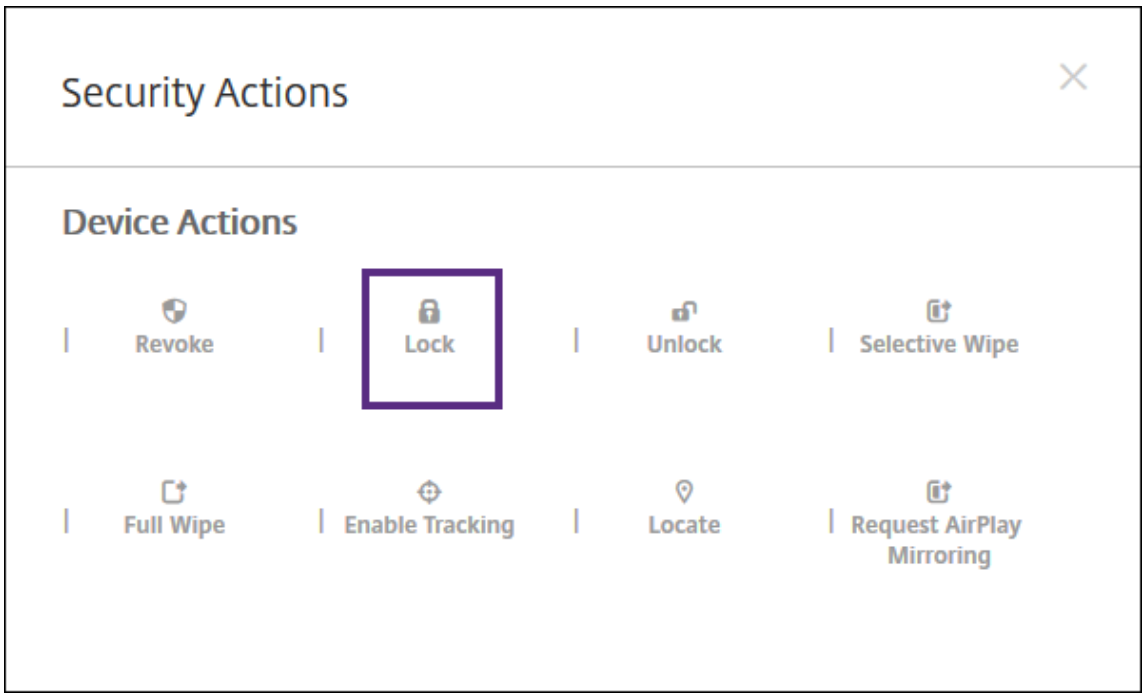
   选中设备旁边的复选框以显示设备列表上方的选项菜单。单击列表中的其他任意位置可在列表右侧显示选项菜单。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

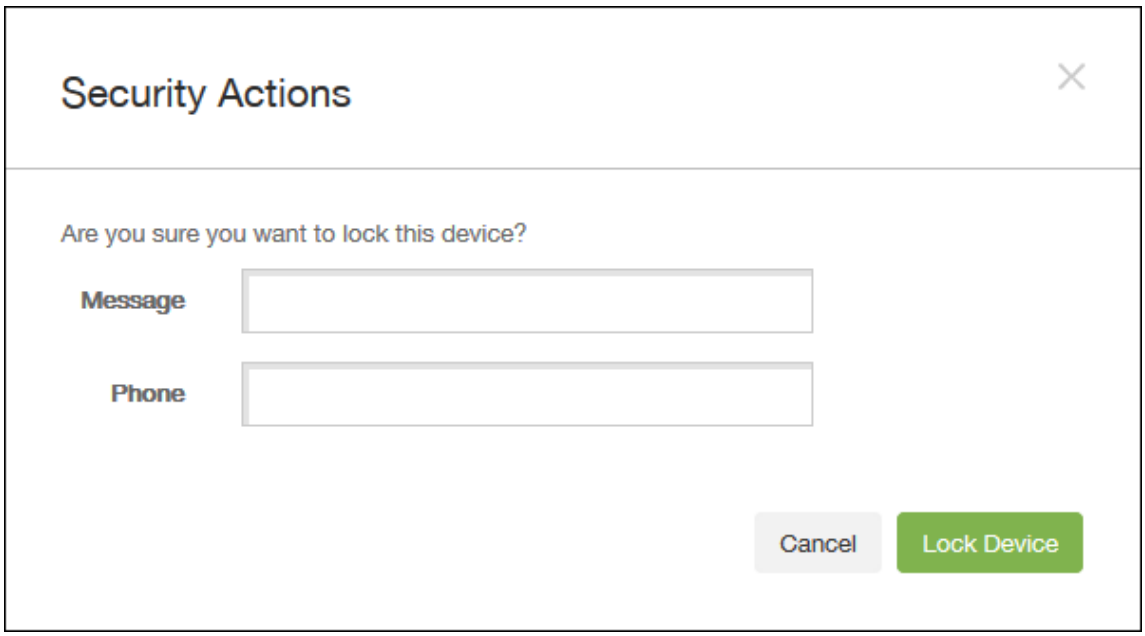


3. 在选项菜单中，选择安全。此时将显示安全操作对话框。



4. 单击锁定。此时将显示安全操作确认对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



5. （可选）键入将显示在设备锁屏界面上的消息和电话号码。

   iOS 会将 “丢失的 iPad” 字样附加到您在消息字段中键入的内容后。

   如果将消息字段留空，并提供电话号码，Apple 将在设备锁屏界面上显示消息 “呼叫所有者”。

6. 单击锁定设备。

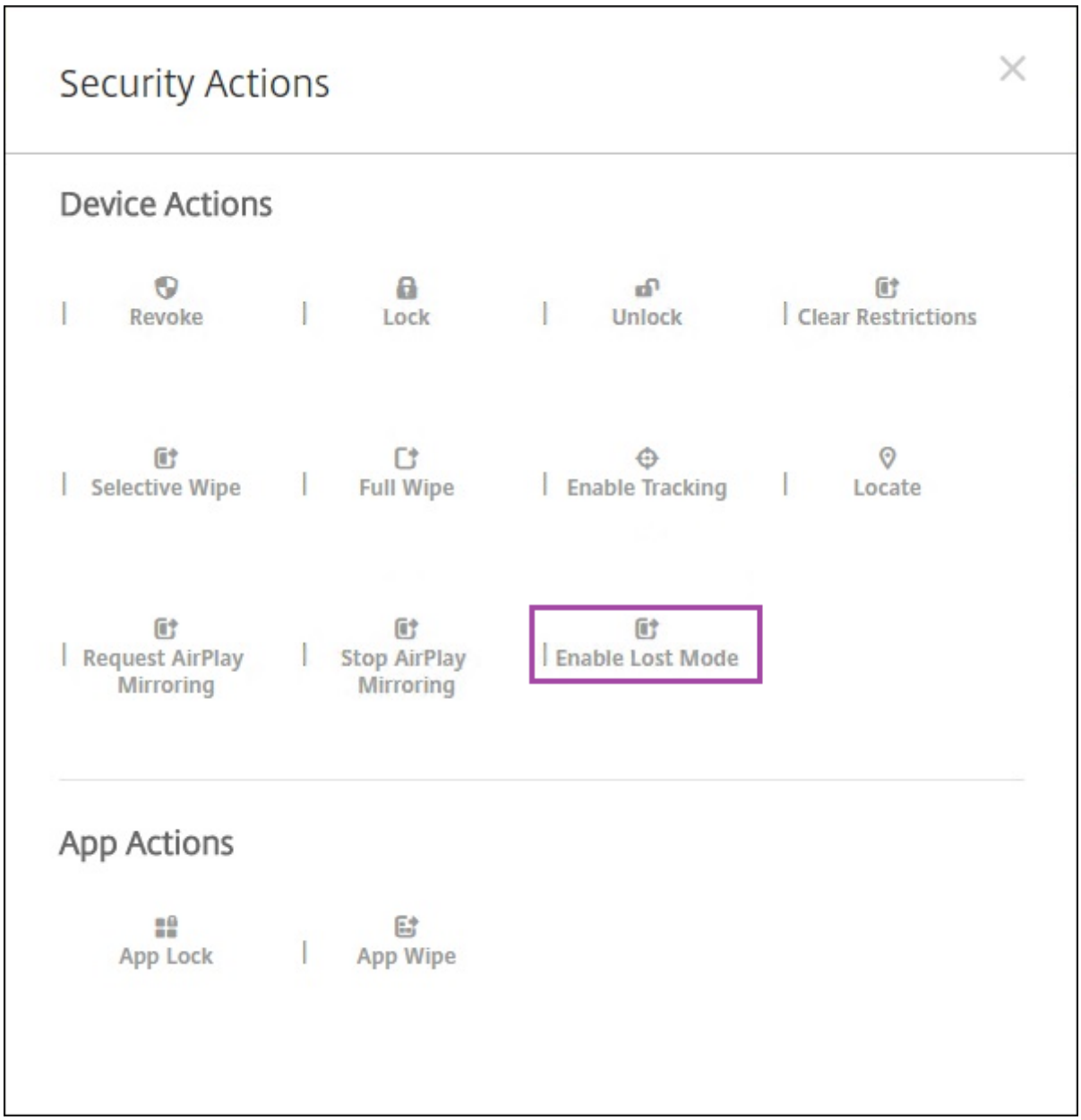
将 **iOS** 设备置于丢失模式

Endpoint Management 丢失模式设备属性将 iOS 设备置于丢失模式。与 Apple 托管丢失模式不同，Endpoint Management 丢失模式不要求用户执行以下任一操作来启用定位其设备：配置查找我的 **iPhone/iPad** 设置或为 Citrix Secure Hub 启用定位服务。

在 Endpoint Management 丢失模式下，只有 Endpoint Management 可以解锁设备。（与此相反，如果您使用 Endpoint Management 设备锁定功能，用户可以使用您提供的 PIN 代码直接解锁设备。

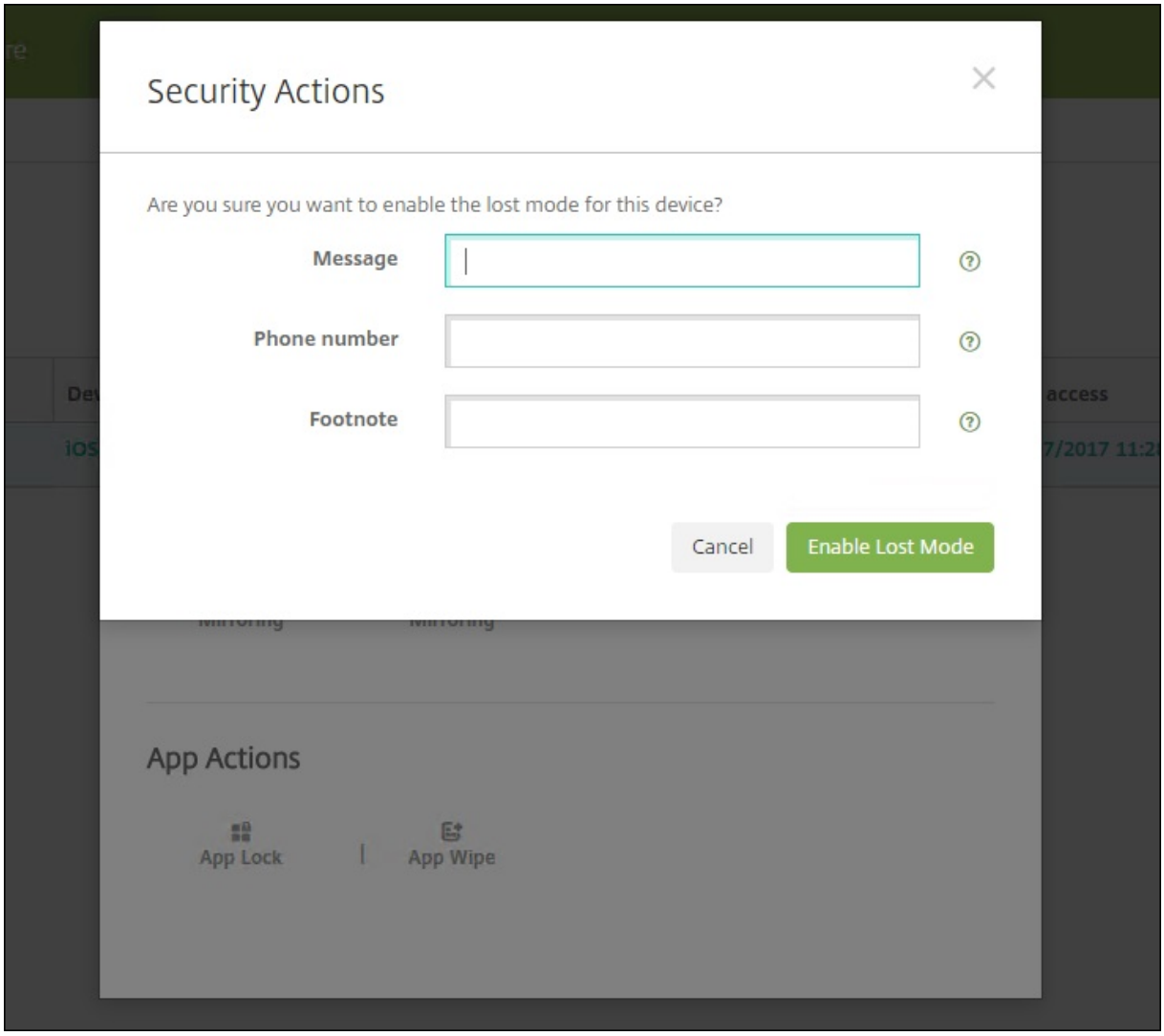
要启用或禁用丢失模式，请转至管理 **>** 设备，选择受监督的 iOS 设备，并单击安全。然后，单击启用丢失模式或禁用丢失模式。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



如果单击启用丢失模式，请键入设备处于丢失模式时要在设备上显示的信息。

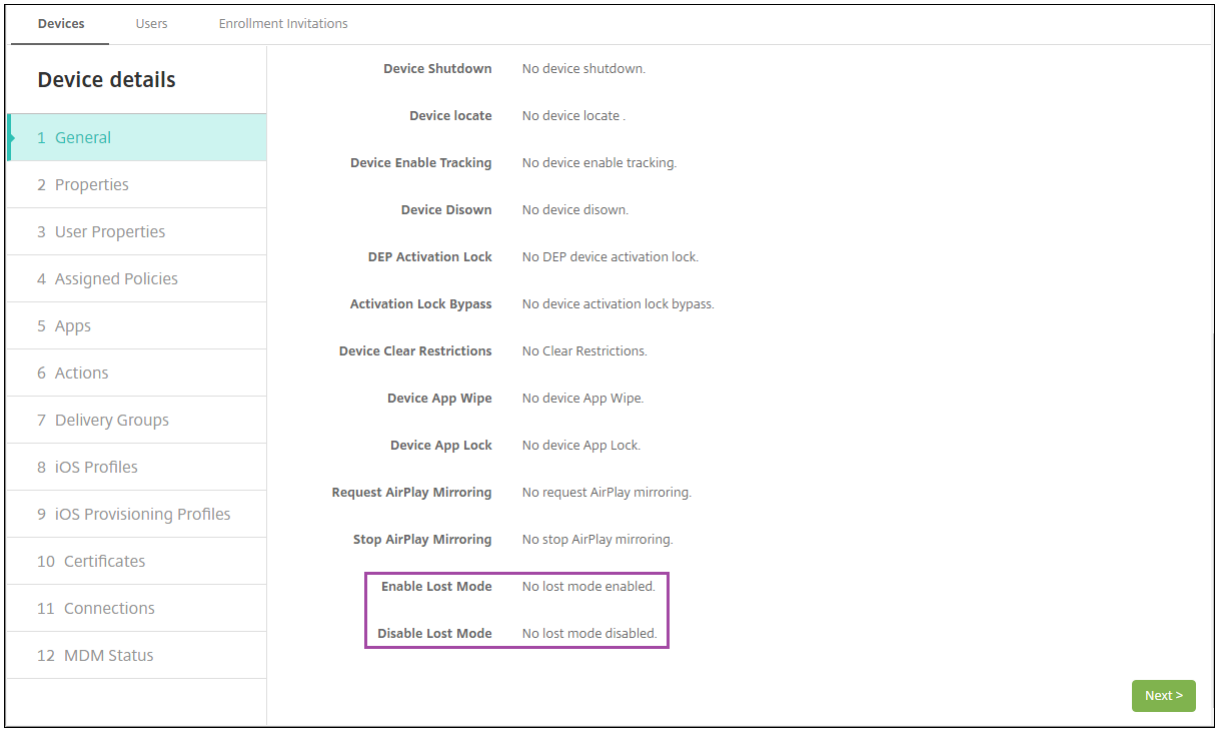
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



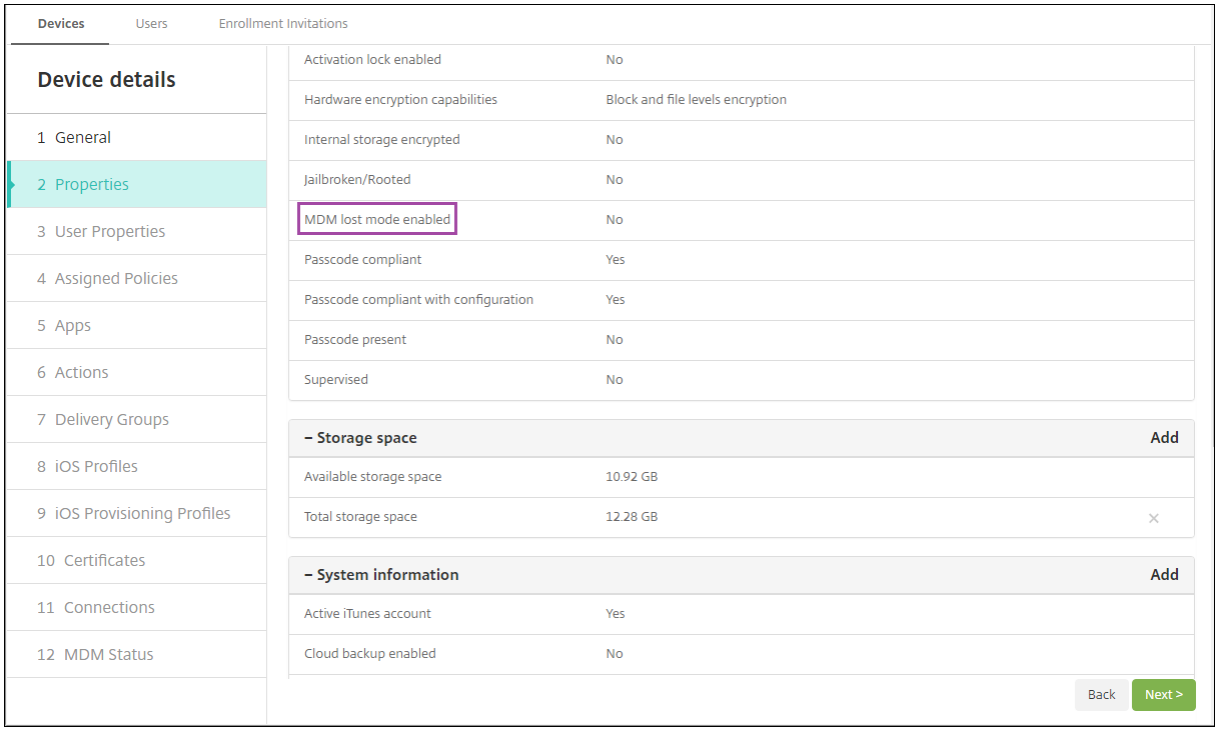
可使用以下任何方法来检查丢失模式状态：

- 在安全操作窗口中，确认按钮是否为禁用丢失模式。
- 在管理 **>** 设备中常规选项卡上的安全下方，查看最后一次“启用丢失模式”或“禁用丢失模式”操作。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 在管理 **>** 设备中的属性选项卡上，确认已启用 **MDM** 丢失模式设置的值是否正确。



如果在 iOS 设备上启用了 Endpoint Management 丢失模式，Endpoint Management 控制台还会按如下所示进行更改：

- 在配置 **>** 操作中，操作列表不包括这些自动化操作：吊销设备、选择性擦除设备和完全擦除设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 在管理 **>** 设备中，安全操作列表不再包括吊销和选择性擦除设备的操作。您仍可以根据需要使用安全操作来执行完全擦除操作。

iOS 会将 “丢失的 iPad” 字样附加到您在安全操作屏幕的消息中输入的内容后。

如果将消息留空，并提供电话号码，Apple 将在设备锁屏界面上显示消息 “呼叫所有者”。

绕过 **iOS** 激活锁

激活锁是一项 “查找我的 iPhone/iPad” 功能，用于阻止重新激活丢失或被盗的受监督设备。激活锁需要用户的 Apple ID 和密码，之后用户才能执行以下操作：关闭 “查找我的 iPhone/iPad”、擦除设备或重新激活设备。对于组织拥有的设备，绕过激活锁是（例如）重置或重新分配设备的必要操作。

要启用激活锁，请配置并部署 Endpoint Management MDM 选项设备策略。之后可以从 Endpoint Management 控制台管理设备，而不需要用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 Endpoint Management 控制台发出 “激活锁绕过” 安全操作。

例如，如果用户在执行完全擦除操作之前或之后归还了丢失的手机或设置了设备：手机提示输入 Apple App Store 帐户凭据时，请通过发出 “激活锁绕过” 安全操作来绕过该设置。

激活锁绕过的设备要求

- 通过 Apple Configurator 或 Apple 部署计划进行监督
- 配置了 iCloud 帐户
- 已启用 “查找我的 iPhone/iPad”
- 已在 Endpoint Management 中注册
- “MDM 选项” 设备策略（启用了激活锁）已部署到设备

要在发出设备的完全擦除操作之前绕过激活锁，请执行以下操作：

1. 转至管理 **>** 设备，选择设备，单击安全，然后单击激活锁绕过。
2. 擦除设备。激活锁屏幕在设备设置过程中不显示。

要在发出设备的完全擦除操作之后绕过激活锁，请执行以下操作：

1. 重置或擦除设备。激活锁屏幕在设备设置过程中显示。
2. 转至管理 **>** 设备，选择设备，单击安全，然后单击激活锁绕过。
3. 轻按设备上的 “返回” 按钮。此时将显示主屏幕。

请紧急以下几点：

- 建议您的用户不要关闭 “查找我的 iPhone/iPad”。请勿从设备执行完全擦除操作。在这些情况下，系统将提示用户输入 iCloud 帐户密码。验证帐户后，用户在擦除所有内容和设置后将看不到 “激活 iPhone/iPad” 屏幕。
- 对于具有生成的激活锁绕过码并且启用了激活锁的设备：如果在执行完全擦除操作后无法绕过 “激活 iPhone/iPad” 页面，则不需要从 Endpoint Management 中删除设备。您或用户可以联系 Apple 技术支持人员来直接解锁设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 确认硬件清单过程中，Endpoint Management 将查询设备中是否存在激活锁绕过码。如果绕过码可用，设备会将其发送到 Endpoint Management。之后，要从设备中删除绕过码，请从 Endpoint Management 控制台发送“激活锁绕过”安全操作。此时，Endpoint Management 和 Apple 将具有解锁设备所需的绕过码。
- “激活锁绕过”安全操作依赖 Apple 服务的可用性。如果该操作无法运行，您可以使用以下方法之一解锁设备：
  - 在设备上，手动输入 iCloud 帐户的凭据。
  - 将“用户名”字段留空，并在“密码”字段中键入绕过码。要查找绕过码，请转至管理 **>** 设备，选择设备，单击编辑，然后单击属性。激活锁绕过码显示在安全信息下。

macOS

December 3, 2021

要在 Endpoint Management 中管理 macOS 设备，应设置 Apple 提供的 Apple 推送通知服务 (APNs) 证书。有关信息，请参阅 APNs 证书。

Endpoint Management 将 macOS 设备注册到 MDM 中。Endpoint Management 支持对 MDM 中的 macOS 设备使用以下注册身份验证类型。

- 域
- 域名加一次性密码
- 邀请 URL 加一次性密码

> **macOS 15** 中对可信证书的要求：
>
> Apple 对 TLS 服务器证书有新的要求。验证所有证书都符合 Apple 的新要求。请参阅 Apple 出版物 https://support.apple.com/en-us/HT210176。有关管理证书方面的帮助，请参阅上载证书。

启动 macOS 设备管理的一般工作流程如下：

1. 完成登录流程。请参阅载入和资源设置和准备注册设备并交付资源。
2. 选择并配置注册方法。请参阅支持的注册方法。
3. 配置 macOS 设备策略。
4. 注册 macOS 设备。
5. 设置设备和应用程序安全操作。请参阅安全操作。

有关支持的操作系统，请参阅支持的设备操作系统。

必须保持公开状态的 **Apple** 主机名

某些 Apple 主机名必须保持打开状态，以确保 iOS、macOS 和 Apple App Store 的正常运行。阻止这些主机名可能会影响以下对象的安装、更新和正确操作：iOS、iOS 应用程序、MDM 操作以及设备和应用程序注册。有关详细信息，请参阅 https://support.apple.com/en-us/HT201999。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

支持的注册方法

下表列出了 Endpoint Management 支持的 macOS 设备的注册方法：

方法	支持
Apple 部署计划	是
Apple 校园教务管理	是
Apple Configurator	否
手动注册	是
注册邀请	是

Apple 制定了面向企业和教育帐户的设备注册计划。对于企业帐户，需要在 “Apple 部署计划” 中注册才能使用 Apple 部署计划在 Endpoint Management 中注册和管理设备。该程序适用于 iOS、macOS 和 Apple TV 设备。请参阅通过 Apple 部署计划部署设备。

对于教育帐户，需要创建一个 Apple 校园教务管理帐户。Apple 校园教务管理统一了部署计划和批量购买。Apple 校园教务管理的类型为教育 Apple 部署类型。请参阅与 Apple 教育功能相集成。

可以使用 Apple 部署计划批量注册 iOS、macOS 和 Apple TV 设备。可以直接从 Apple 、参与计划的 Apple 授权经销商或运营商处购买这些设备。

配置 **macOS** 设备策略

使用这些策略可配置 Endpoint Management 与运行 macOS 的设备的交互方式。下表列出了适用于 macOS 设备的所有设备策略。

AirPlay 镜像	应用程序清单	应用程序卸载
日历 (CalDav)	联系人 (CardDAV)	凭据
设备名称	Exchange	FileVault
防火墙	字体	导入 iOS 和 macOS 配置文件
LDAP	邮件	网络
操作系统更新	通行码	配置文件删除
限制	SCEP	VPN
Web 剪辑		

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

注册 **macOS** 设备

Endpoint Management 提供两种方法来注册运行 macOS 的设备。这两种方法都使 macOS 用户能够直接从其设备无线注册。

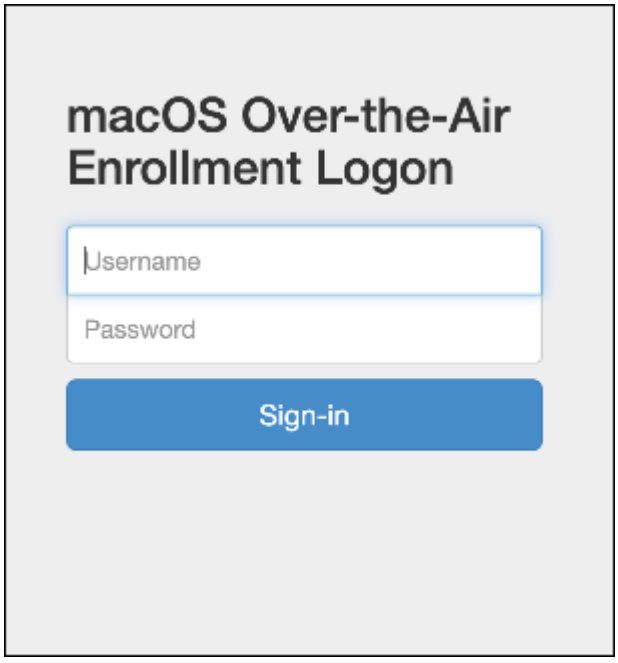
- 向用户发送注册邀请：此注册方法允许您为 macOS 设备设置以下任意注册安全模式：
  - 用户名 + 密码
  - 用户名 + PIN
  - 双重身份验证

  用户按照注册邀请中的说明进行操作时，将显示一个填写了用户名的登录屏幕。
- 向用户发送注册链接：此注册方法适用于 macOS 设备，向用户发送一个注册链接，用户可以在 Safari 或 Chrome 浏览器中打开该链接。用户随后通过提供其用户名和密码进行注册。

  要阻止对 macOS 设备使用注册链接，请将服务器属性启用 **macOS OTAE** 设置为 **false**。因此，macOS 用户只能使用注册邀请进行注册。

向 **macOS** 用户发送注册邀请

1. 添加面向 macOS 用户注册的邀请。请参阅注册邀请。
2. 用户收到邀请并单击链接后，以下屏幕将在 Safari 浏览器中显示。Endpoint Management 填充用户名。如果您为注册安全模式选择双重，则将显示另一个字段。



3. 用户根据需要安装证书。用户是否会收到安装证书的提示取决于您是否为 macOS 配置了以下证书：公众信任的 SSL 证书和公众信任的数字签名证书。有关证书的信息，请参阅证书和身份验证。
4. 用户提供请求的凭据。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

安装 Mac 设备策略。现在即可以像管理移动设备一样使用 Endpoint Management 管理 macOS 设备。

向 **macOS** 用户发送安装链接

1. 发送注册链接 `https://serverFQDN:8443/instanceName/macos/otae`，用户可以在 Safari 或 Chrome 浏览器中打开该链接。
   - **serverFQDN** 是运行 Endpoint Management 的服务器的完全限定域名 (FQDN)。
   - 端口 **8443** 为默认安全端口。如果已配置其他端口，请使用该端口替换 8443。
   - **instanceName**（通常显示为 `zdm`）为在服务器安装过程中指定的名称。

   有关发送安装链接的详细信息，请参阅发送安装链接。
2. 用户根据需要安装证书。如果您为 iOS 和 macOS 配置了公众信任的 SSL 证书和数字签名证书，用户将看到安装证书的提示。有关证书的信息，请参阅证书和身份验证。
3. 用户登录其 Mac 设备。

   安装 Mac 设备策略。现在即可以像管理移动设备一样使用 Endpoint Management 管理 macOS 设备。

安全操作

macOS 支持以下安全操作。有关每个安全操作的说明，请参阅安全操作。

吊销	锁定	选择性擦除
完全擦除	证书续订	轮换个人恢复密钥

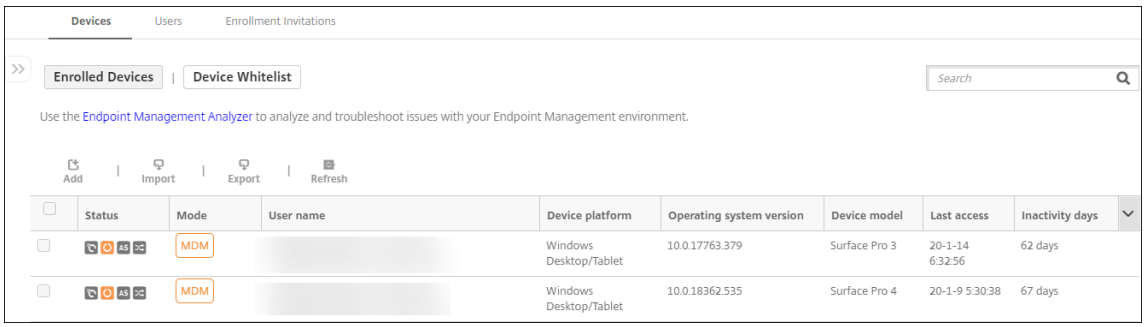
锁定 **macOS** 设备

可以远程锁定丢失的 macOS 设备。Endpoint Management 锁定设备它随之生成一个 PIN 代码并在设备中进行设置。要访问设备，用户需要键入该 PIN 代码。使用取消锁定可从 Endpoint Management 控制台中删除锁定。

可以使用通行码设备策略配置与 PIN 代码关联的更多设置。有关详细信息，请参阅 macOS 设置。

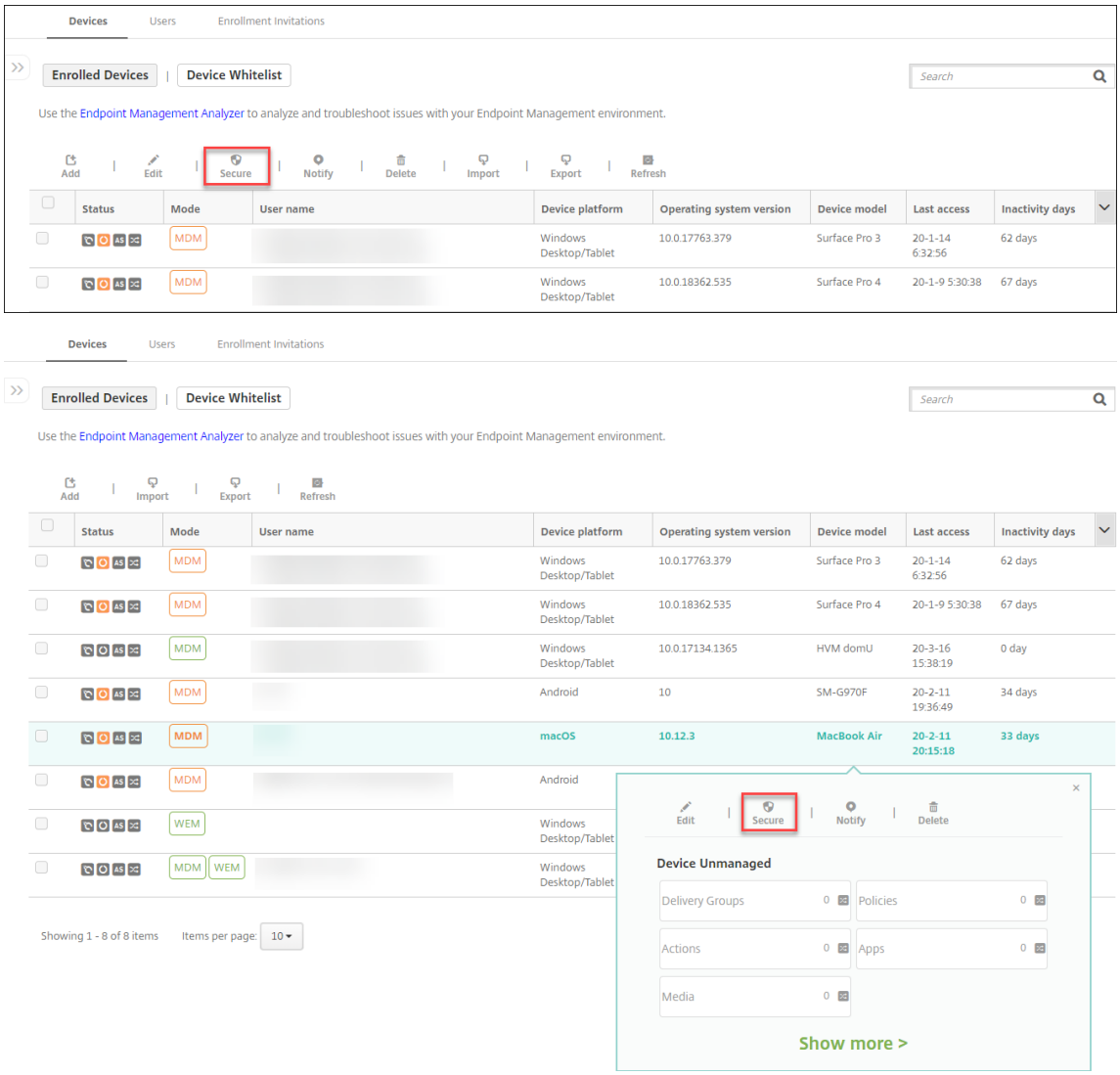
1. 单击管理 **>** 设备。此时将显示设备页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 选择要锁定的 macOS 设备。

   选中设备旁边的复选框以显示设备列表上方的选项菜单。也可以单击列出的项目上的其他任何位置，以在此列表的右侧显示选项菜单。

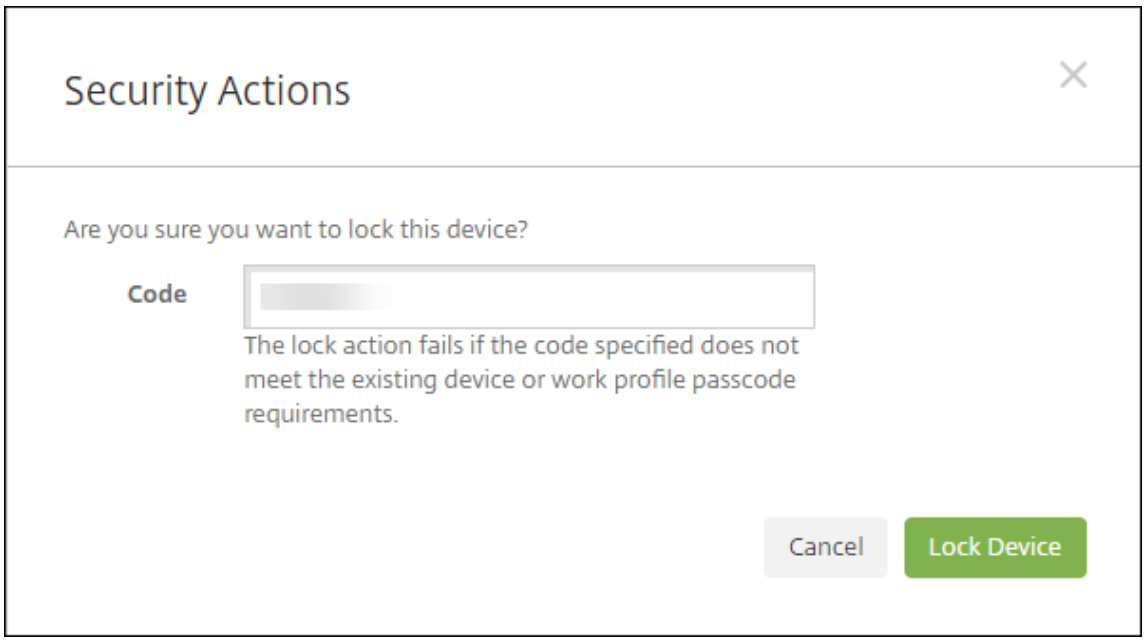


3. 在选项菜单中，选择安全。此时将显示安全操作对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 单击锁定。此时将显示安全操作确认对话框。



5. 单击锁定设备。

> 重要：
>
> 还可以指定密码，而不是使用 Endpoint Management 生成的代码。如果指定的代码不符合设备或现有工作配置文件的代码要求，锁定操作将失败。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

引导程序令牌

引导程序令牌可帮助您在登录到 macOS 设备时向帐户授予 SecureToken macOS 属性。SecureToken 从一个可信帐户向下传递到另一个帐户。启用了 SecureToken 的帐户可以在设备上执行加密操作。如果没有引导程序令牌，您需要在添加单个用户帐户之前，按照复杂的工作流程进行操作，在该设备上创建帐户。

Endpoint Management 支持对通过 Apple 部署计划注册的 macOS 设备使用托管引导程序令牌。您使用 Apple 部署计划注册您直接从 Apple、Apple 授权经销商或运营商处购买的 macOS 设备。有关在 Apple 部署计划中注册的信息，请参阅通过 Apple 部署计划部署设备。

引导程序令牌在设置助理工作流程期间生成。具体而言，它们都是在本地用户帐户创建期间生成的。设置助理在用户首次启动其设备时运行。这些令牌保存在 Endpoint Management 数据库中，您和最终用户不可见。从 Endpoint Management 站点删除设备会删除这些令牌。执行出厂重置不会将其删除。

必备条件：

- macOS 11.0 或更高版本
- 配备 Apple T2 安全芯片的 macOS 设备
- 通过 Apple 部署计划注册的 macOS 设备

在 Endpoint Management 中托管引导程序令牌的一个优势是，可以为 FileVault 启用远程帐户以及能够解锁 FileVault 卷。有关 FileVault 的信息，请参阅 FileVault 策略。

通过 **Apple** 部署计划部署设备

October 18, 2022

Apple 部署计划 (ADP) 允许您自动在 Endpoint Management 中注册 Apple 设备，而不需要在用户获取设备之前触摸或准备这些设备。用户拆箱并激活设备后，设备将自动在 Endpoint Management 中注册，并且所有管理设置、应用程序和书籍都可随时供用户使用。

这些 ADP 包括适用于企业组织的 Apple 商务管理 (ABM) 和适用于教育组织的 Apple 校园教务管理 (ASM)。ABM 和 ASM 适用于 iOS、iPadOS、macOS 和 tvOS 设备。有关设备资格的详细信息，请参阅《Apple 商务管理用户指南》和《Apple 校园教管理用户指南》。

> 注意：
>
> ABM 和 ASM 组合了 Apple 提供的先前的设备注册计划和批量购买计划。

本文将引导您完成 ABM 或 ASM 常规部署工作流程：

1. 在 ABM 或 ASM 中注册
2. 将 ABM 或 ASM 帐户连接到 Endpoint Management
3. 订购设备
4. 将设备分配给 Endpoint Management

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 批量购买内容并将其与 Endpoint Management 同步
6. 配置设备策略和应用程序的部署规则
7. 添加包含向其分配的用户和资源的交付组

完成此部署过程后，设备即准备好拆箱并激活，以执行自动设备注册。

必备条件

打开所需的端口，以便在 Endpoint Management 和 Apple 之间建立连接。有关详细信息，请参阅端口要求。

在 **ABM** 或 **ASM** 中注册

要开始在 Apple 中部署设备，请在 ABM 或 ASM 中进行注册。

ABM 和 ASM 适用于组织，不适用于个人。您必须提供许多组织详细信息和信息才能创建帐户。可能需要一些时间才能完成帐户申请并收到帐户审批结果。

注册 **ABM**

要在 ABM 中注册，请转至 business.apple.com。单击立即注册申请新帐户。

最佳做法是使用贵组织的电子邮件地址，例如 deployment@company.com。注册过程可能需要几天时间。收到登录凭据后，请按照 ABM 中提供的步骤创建帐户。

注册 **ASM**

要创建 Apple 校园教务管理帐户，请转至 Apple 校园教务管理并按照说明进行注册。首次登录 ASM 时，设置助手将打开。

- 有关 ASM 必备条件、设置助手和管理任务的信息，请参阅 Apple School Manager User Guide（《Apple 校园教务管理用户指南》）。
- 设置 ASM 用户帐户时，请使用与 Active Directory 的域名不同的域名。例如，请在 ASM 的域名中添加 `appleid` 之类的前缀。
- 将 ASM 连接到您的名单数据时，ASM 将为教师和学生创建管理式 Apple ID。名单数据包括教师、学生和班级。有关向 ASM 添加名单数据的信息，请参阅此列表中前文链接的 “Apple School Manager User Guide”（《Apple 校园教务管理用户指南》）。
- 可以为您的机构自定义管理式 Apple ID 格式，如此列表中前文链接 “Apple School Manager User Guide”（《Apple 校园教务管理用户指南》）中所述。

  > 重要：
  >
  > 将 ASM 信息导入 Endpoint Management 后，请勿更改托管的 Apple ID。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

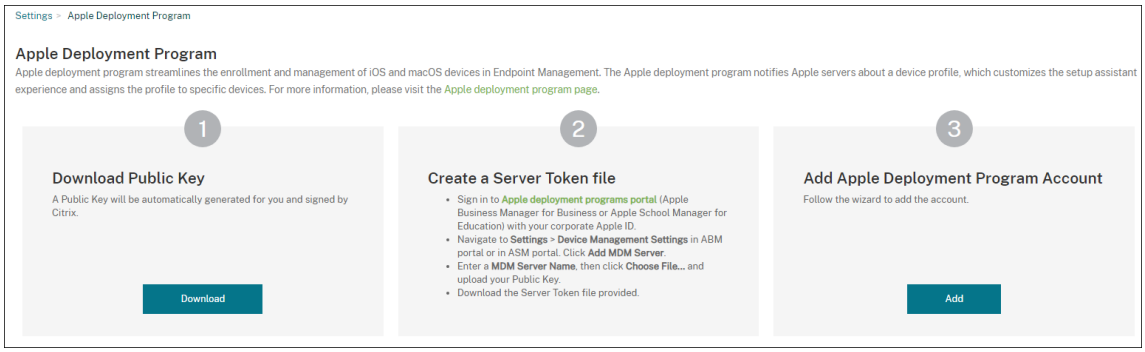
- 如果您是通过经销商或运营商购买的设备，请将这些设备链接到 Apple ASM。有关信息，请参阅此列表中前文链接的 “Apple School Manager User Guide”（《Apple 校园教务管理用户指南》）。

将 **ABM** 或 **ASM** 帐户连接到 **Endpoint Management**

创建 ABM 或 ASM 帐户后，将其与 Endpoint Management 服务器部署相连接。

步骤 **1**：从 **Endpoint Management** 服务器下载公钥

1. 在 Endpoint Management 控制台中，转至设置 **> Apple** 部署计划。



2. 在下载公钥下，单击下载。

步骤 **2**：在您的 **Apple** 帐户中创建并下载服务器令牌文件

1. 使用管理员或设备注册管理员帐户登录到 Apple 商务管理或 Apple 校园教务管理。
2. 在边栏底部，单击设置，然后单击设备管理设置 **>** 添加 **MDM** 服务器。
3. 在 **MDM** 服务器名称设置中，键入 Endpoint Management 服务器的名称。键入的服务器名称仅供参考。它不是服务器的 URL 或名称。
4. 在 **Upload Public Key**（上载公钥）下，单击 **Choose File**（选择文件）。上载您从 Endpoint Management 下载的公钥，并保存所做的更改。
5. 单击 **Download Token**（下载令牌）以将服务器令牌文件下载到您的计算机。

   将 ABM 或 ASM 帐户添加到 Endpoint Management 时，可以上载服务器令牌文件。导入令牌文件后，您的令牌信息将在 Endpoint Management 控制台中显示。
6. 在 **Default Device Assignment**（默认设备分配）下，单击 **Change**（更改）。选择设备的分配方式，然后提供所需的信息。有关详细信息，请参阅《ABM 用户指南》或《Apple 校园教管理用户指南》。

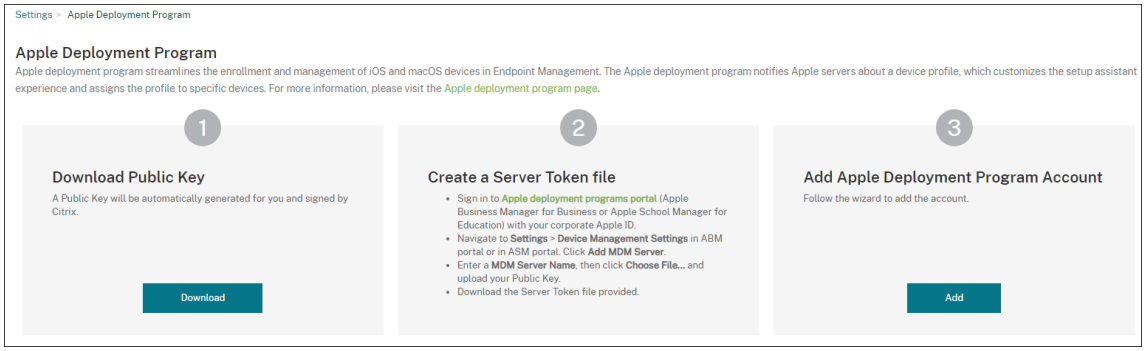
步骤 **3**：将您的帐户添加到 **Endpoint Management**

可以将多个 ABM 或 ASM 帐户添加到 Endpoint Management。有了此功能，可以按国家/地区和部门等使用不同的注册设置和设置助理选项。然后将 ABM 或 ASM 帐户与不同的设备策略相关联。

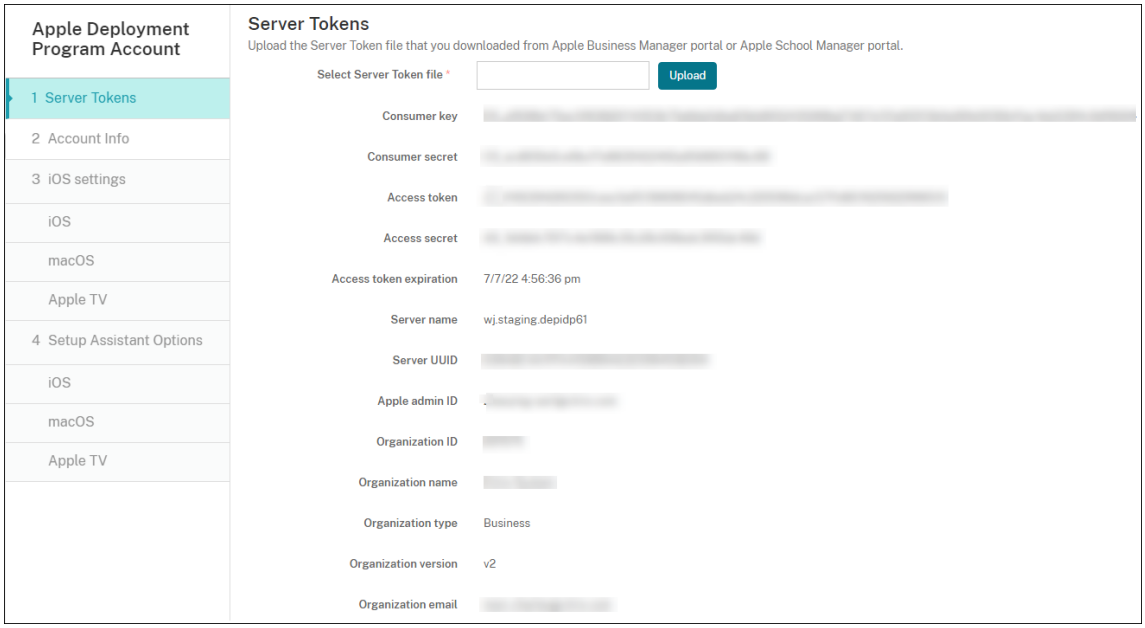
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

例如，可以将来自不同国家/地区的所有 ABM 或 ASM 帐户集中在同一 Endpoint Management 服务器上，以导入和监督所有 ABM 或 ASM 设备。您首先按部门、组织层级结构或其他结构来自定义注册设置和设置助理选项。然后配置策略以在整个组织中提供合适的功能，并允许用户获得适当的帮助。

1. 在 Endpoint Management 控制台中，前往设置 **> Apple** 部署计划，然后在添加 **Apple** 部署计划帐户下，单击添加。



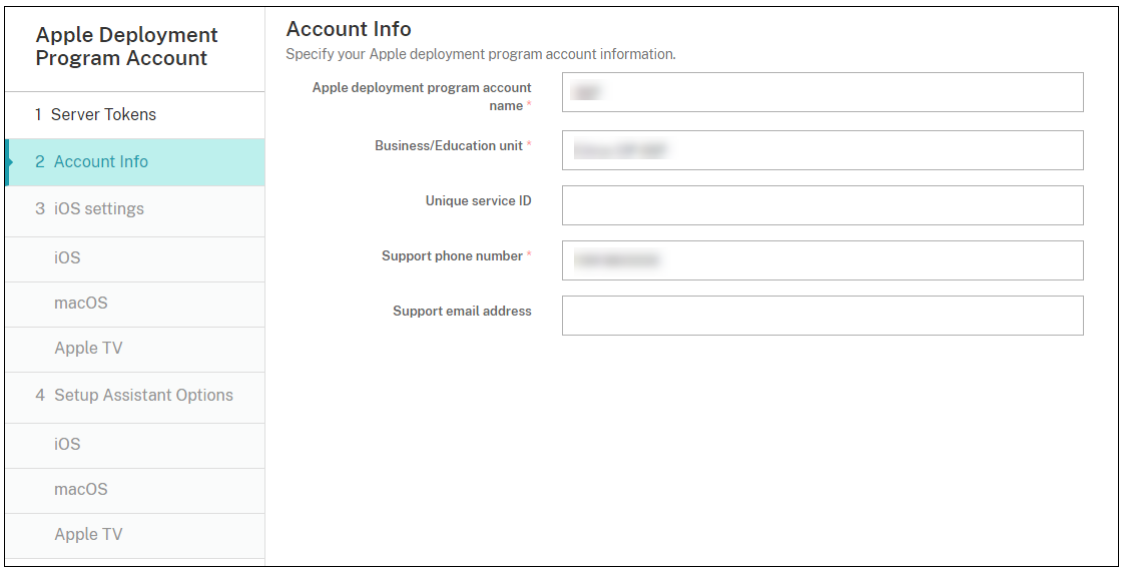
2. 在服务器令牌页面中，指定您的服务器令牌文件，然后单击上载。



此时将显示您的服务器令牌信息。

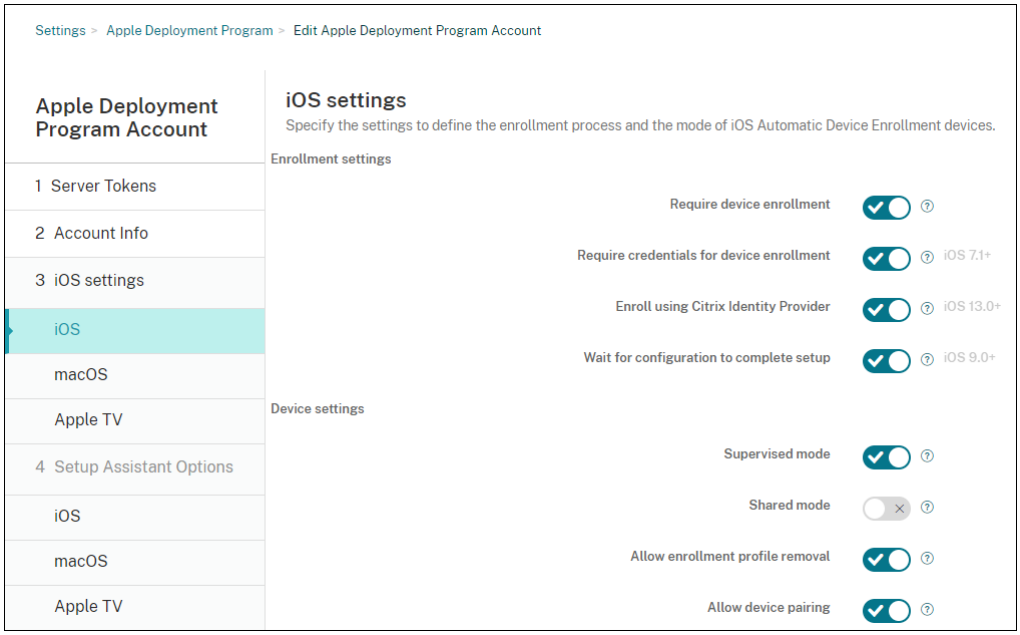
3. 在帐户信息页面中，指定以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- **Apple** 部署计划帐户名称：此 ADP 帐户的唯一描述性名称，标识按国家/地区或组织层级结构等对象组织 ADP 帐户的方式。
- 业务/教育单位：将设备分配到的业务单位或部门。此字段为必填字段。
- 唯一服务 **ID**：有助于您进一步识别帐户的可选唯一 ID。
- 支持电话号码：支持电话号码，用户在设置期间拨打此号码寻求帮助。此字段为必填字段。
- 支持电子邮件地址：向最终用户提供的可选支持电子邮件地址。
- 教育后缀：适用于 ASM 帐户。键入分配给通过此帐户注册的设备的后缀。

4. 在 **iOS** 设置中，指定以下设置：



注册设置：

- 要求设备注册：是否要求用户注册其设备。默认值为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 需要提供凭据才能完成设备注册： ABM 和 ASM 设置过程中是否需要用户输入其凭据。我们建议您要求所有用户在设备注册期间输入其凭据，仅允许授权用户注册设备。默认值为开。

  如果您在首次设置之前启用 ABM 或 ASM 但不选择此选项，Endpoint Management 将创建 ABM 组件。此创建包括用户、Secure Hub、软件清单和部署组等组件。如果选择了此选项，Endpoint Management 将不创建这些组件。因此，如果您在以后清除此选项，则尚未输入其凭据的用户将无法在 ABM 或 ASM 中注册，因为这些组件不存在。在这种情况下，要添加 ABM 或 ASM 组件，在这种情况下，请禁用并启用 ABM 或 ASM 帐户。

- 使用 **Citrix** 身份提供程序注册：是否使用 Citrix 身份提供程序进行注册。此设置仅适用于 ABM 帐户。如果设置为 开，启用 ADP 的 iOS 设备只能使用 Citrix 身份提供程序进行注册。默认值为关。

  要打开该设置，必须首先将 Citrix 身份提供程序配置为身份提供程序。转到 设置 **>** 身份提供程序 **(IDP)**，单击 添加，然后选择 **Citrix** 身份提供程序。

  如果此设置为“开”，请注意以下注意事项：

  - 您无法在 设置 **>** 身份提供程序 **(IDP)** 页面上删除相应的 **Citrix** 身份提供程序配置。
  - 编辑相应的 Citrix 身份提供程序配置时，无法切换到其他身份提供程序。

- 等待完成配置设置：是否要求用户的设备一直保持在“设置助理”模式，直到将所有 MDM 资源部署到设备。此设置适用于处于受监督模式的设备。默认值为关。

- Apple 文档指出，当设备处于“设置助手”模式时，以下命令可能无法使用：

  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

设备设置：

- 受监督模式：如果要使用 Apple Configurator 管理注册的设备或启用了等待完成配置设置，必须设置为开。默认值为开。有关将 iOS 设备置于受监督模式的详细信息，请参阅使用 Apple Configurator 2 部署设备。
- 允许删除注册配置文件：是否允许设备使用能够远程删除的配置文件。默认值为关。
- 允许设备配对：您是否能够通过 Apple Music 和 Apple Configurator 管理已注册的设备。默认值为关。

监督身份

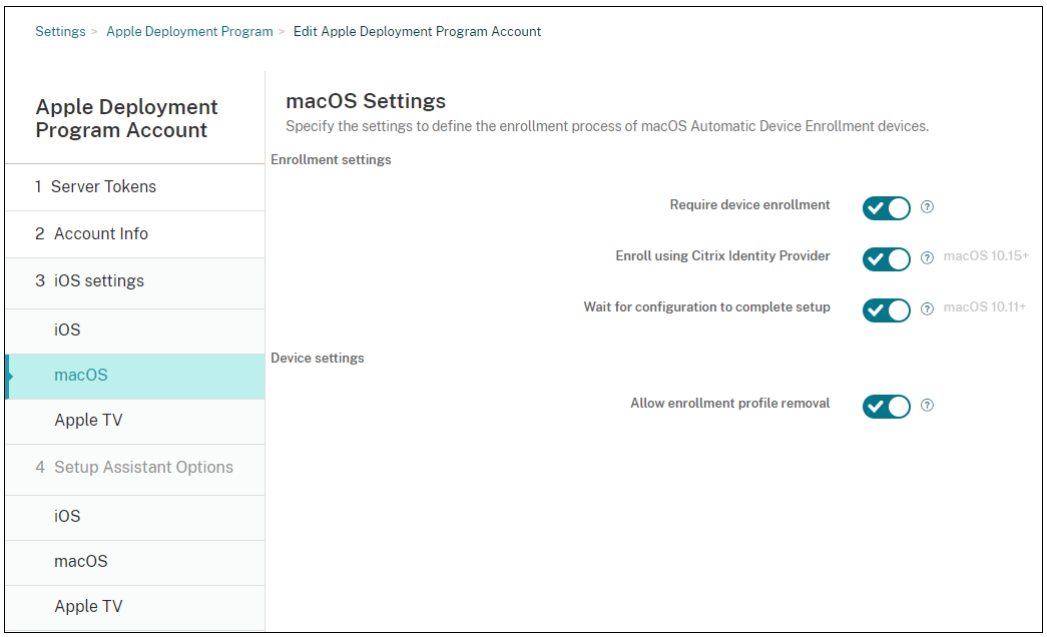
如果使用 GroundControl 工具，则可以添加证书以执行以下操作：

- 覆盖配对限制，以避免显示“信任此主机”提示。
- 通过 USB 上报托管设备操作以执行配置文件安装等活动，而无需用户交互。这样做将允许 GroundControl 启用单应用程序模式和设备锁定以进行签出。
- 将备份还原到 ABM 或 ASM 设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

有关 GroundControl 的详细信息，请参阅 GroundControl Web 站点。

5. 在 **macOS** 设置中，指定以下设置：



注册设置：

- 要求设备注册：是否要求用户注册其设备。默认值为开。
- 使用 **Citrix** 身份提供程序注册：是否使用 Citrix 身份提供程序进行注册。此设置仅适用于 ABM 帐户。如果设置为 开，启用 ADP 的 macOS 设备只能使用 Citrix 身份提供程序进行注册。默认值为关。

  要打开该设置，必须首先将 Citrix 身份提供程序配置为身份提供程序。转到 设置 **>** 身份提供程序 **(IDP)**，单击 添加，然后选择 **Citrix** 身份提供程序。

  如果此设置为“开”，请注意以下注意事项：

  - 您无法在 设置 **>** 身份提供程序 **(IDP)** 页面上删除相应的 **Citrix** 身份提供程序配置。
  - 编辑相应的 Citrix 身份提供程序配置时，无法切换到其他身份提供程序。
- 等待完成配置设置：如果选择否，macOS 设备将不继续在“设置助理”下操作，直到将 MDM 资源通行码部署到设备。该部署在创建本地帐户之前进行。此设置适用于 macOS 10.11 及更高版本的设备。默认值为关。

设备设置：

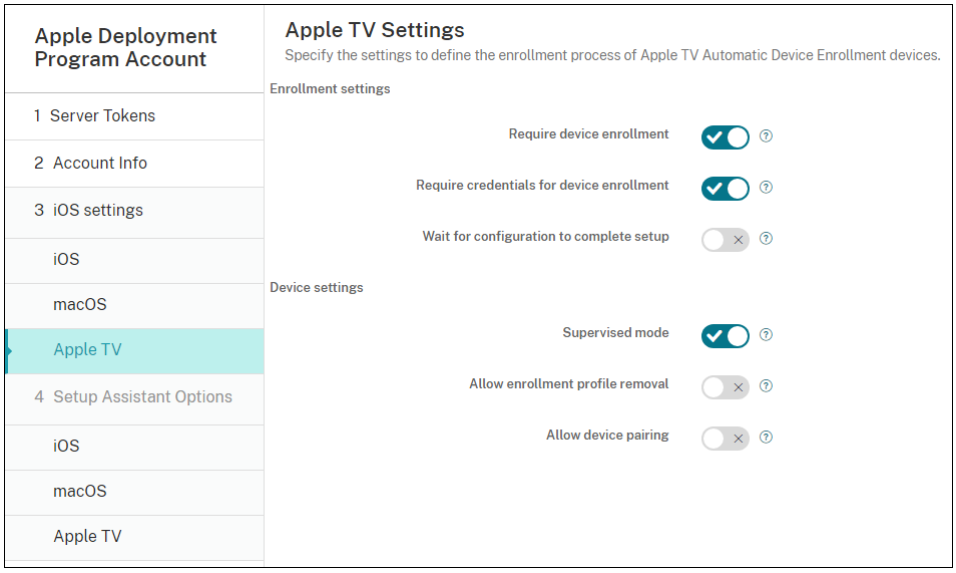
- 允许删除注册配置文件：是否允许设备使用能够远程删除的配置文件。默认值为关。

6. 在 **Apple TV** 设置中，指定以下设置：

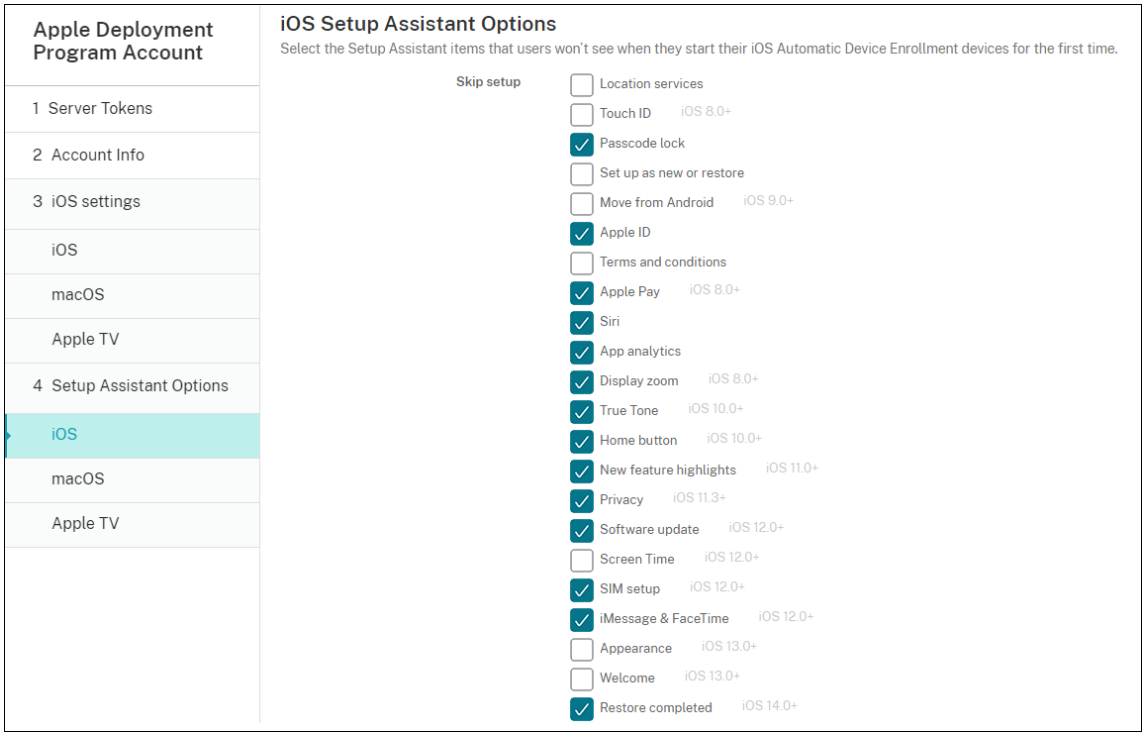
- 要求注册设备：阻止用户跳过注册过程。
- 需要提供凭据才能完成设备注册：注册过程中对凭据的质询。关闭此设置时，Apple TV 将注册为默认“设备注册计划用户”。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 等待完成配置设置：设备在设置助理屏幕中等待，直至所有资源都部署完毕。
- 受监督模式：配置限制过程中向管理员提供更多功能。
- 允许删除注册配置文件：允许用户删除注册配置文件。
- 允许设备配对：允许通过 Apple 工具（例如 Apple App Store 和 Apple Configurator）管理通过设备注册计划注册的设备。



7. 在 **iOS** 设置助手选项中，选择用户在首次启动其设备时 iOS 设置助手跳过的步骤。跳过屏幕时，相关功能将使用默认设置。用户可以在设置完成后配置已跳过的功能，除非您完全限制对这些功能的访问。有关限制对功能的访问的信息，请参阅限制设备策略。所有项目的默认设置为未选中。以下说明解释了选择某项设置时发生的情况。



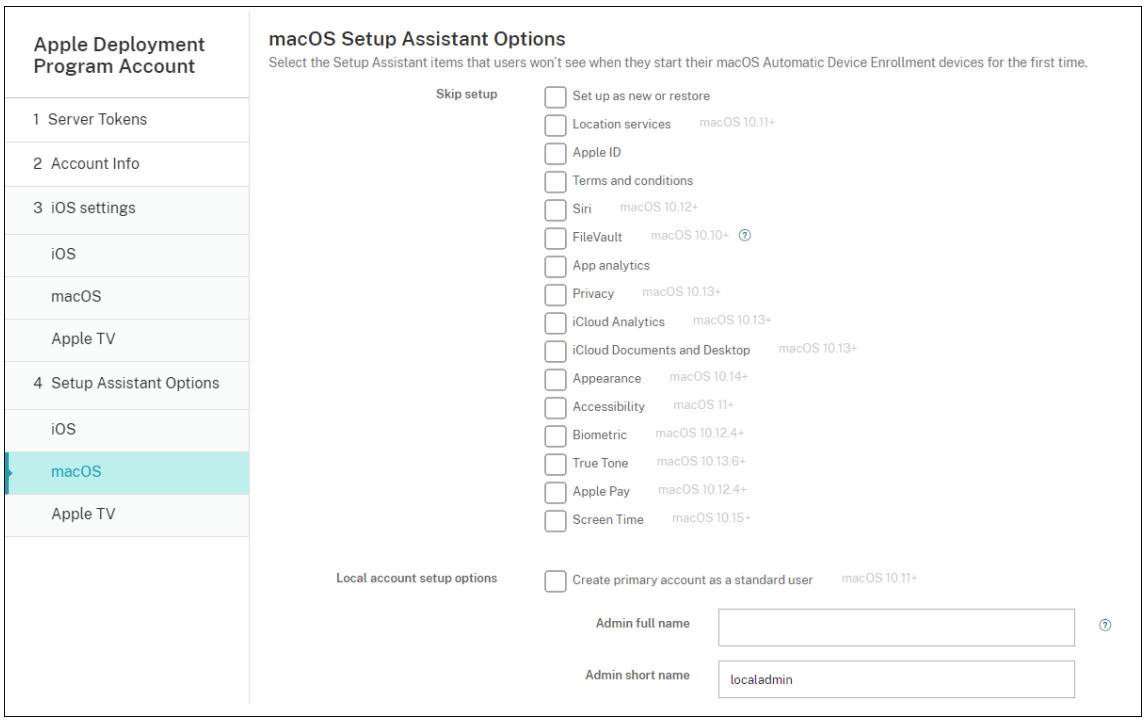
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 定位服务：阻止用户在设备上设置定位服务。
- **Touch ID**：阻止用户在 iOS 设备上设置 Touch ID 或面容 ID。
- 通行码锁定：阻止用户为设备设置通行码。如果不存在通行码，用户将无法使用 Touch ID 或 Apple Pay。
- 设置为新设备或还原：阻止用户将设备设置为新设备或从 iCloud 或 Apple App Store 备份还原。
- 从 **Android** 移动：阻止用户将数据从 Android 设备传输到 iOS 设备。此选项仅在已选择设置为新对象或还原时可用（即跳过相应步骤）。
- **Apple ID**：阻止用户为设备设置托管 Apple ID 帐户。
- 条款和条件：阻止用户阅读并接受条款和条件以使用设备。
- **Apple Pay**：阻止用户设置 Apple Pay。如果清除此设置，用户必须设置 Touch ID 和 Apple ID。请确保清除这些设置。
- **Siri**：阻止用户配置 Siri。
- 应用程序分析：阻止用户设置是否与 Apple 共享崩溃数据和使用情况统计信息。
- 显示缩放：阻止用户在 iOS 设备上设置显示分辨率（标准或缩放）。
- 原彩：阻止用户设置四通道传感器以动态调整显示器的白平衡。
- 主页按钮：阻止用户设置反馈的主页按钮样式。
- 新功能亮点：阻止用户看到显示 Apple 软件新增功能信息的屏幕。
- 隐私：阻止用户看到数据和隐私窗格。适用于 iOS 11.3 及更高版本。
- 软件更新：阻止用户将 iOS 更新到最新版本。适用于 iOS 12.0 及更高版本。
- 屏幕时间：阻止用户启用屏幕时间。适用于 iOS 12.0 及更高版本。
- **SIM** 设置：阻止用户设置手机网络套餐。适用于 iOS 12.0 及更高版本。
- **iMessage** 和 **FaceTime**：阻止用户启用 iMessage 和 FaceTime。适用于 iOS 12.0 及更高版本。
- 外观：阻止用户选择外观模式。适用于 iOS 13.0 及更高版本。
- 欢迎：阻止用户看到入门屏幕。适用于 iOS 13.0 及更高版本。
- 已完成还原：阻止用户看到还原是否在设置过程中完成。适用于 iOS 14.0 及更高版本。
- 已完成更新：阻止用户看到软件更新是否在设置过程中完成。适用于 iOS 14.0 及更高版本。
- 应用商店：阻止用户设置应用商店。适用于 iOS 11.1 及更高版本。

该帐户显示在设置 **> Apple** 部署计划上。

8. 在 **macOS** 设置助手选项中，选择用户在首次启动其设备时 macOS 设置助手跳过的步骤。跳过屏幕时，相关功能将使用默认设置。用户可以在设置完成后配置已跳过的功能，除非您完全限制对这些功能的访问。有关限制对功能的访问的信息，请参阅限制设备策略。所有项目的默认设置为未选中。以下说明解释了选择某项设置时发生的情况。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 设置为新设备或还原：阻止用户将设备设置为新设备或从“时间机器”备份还原或执行系统迁移。
- 定位服务：阻止用户在设备上设置定位服务。适用于 macOS 10.11 及更高版本。
- **Apple ID**：阻止用户为设备设置托管 Apple ID 帐户。
- 条款和条件：阻止用户阅读并接受条款和条件以使用设备。
- **Siri**：阻止用户配置 Siri。适用于 macOS 10.12 及更高版本。
- **FileVault**：使用 FileVault 加密启动磁盘。如果系统具有一个本地用户帐户并且该帐户已登录到 iCloud 时，Endpoint Management 才应用 FileVault 设置。

  可以使用 macOS FileVault 磁盘加密功能通过加密系统卷的内容 (https://support.apple.com/en-us/HT204837) 来保护系统卷。如果您在未打开 FileVault 功能的新型便携式 Mac 上运行设置助理，系统可能会提示您打开此功能。该提示在新系统以及升级到 OS X 10.10 或 10.11 的系统中显示，但仅当系统具有一个本地管理员帐户并且该帐户已登录到 iCloud 时显示。
- 应用程序分析：阻止用户设置是否与 Apple 共享崩溃数据和使用情况统计信息。
- 隐私：阻止用户看到数据和隐私窗格。适用于 macOS 10.13 及更高版本。
- **iCloud** 分析：阻止用户选择是否向 Apple 发送诊断 iCloud 数据。适用于 macOS 10.13 及更高版本。
- **iCloud** 文档和桌面：阻止用户设置 iCloud 桌面和文档。适用于 macOS 10.13 及更高版本。
- 外观：阻止用户选择外观模式。适用于 macOS 10.14 及更高版本。
- 辅助功能：阻止用户自动聆听旁白。仅在设备连接到以太网时可用。适用于 macOS 11 及更高版本。
- 生物特征识别：阻止用户设置 Touch ID 和面容 ID。适用于 macOS 10.12.4 及更高版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 原彩：阻止用户设置四通道传感器以动态调整显示器的白平衡。适用于 macOS 10.13.6 及更高版本。
- **Apple Pay**：阻止用户设置 Apple Pay。如果清除此设置，用户必须设置 Touch ID 和 Apple ID。确保清除 **Apple ID** 和生物特征识别设置。
- 屏幕时间：阻止用户启用屏幕时间。适用于 macOS 10.15 及更高版本。
- 应用商店：阻止用户设置应用商店。适用于 macOS 11.1 及更高版本。
- 使用 **Apple Watch** 解锁：防止用户使用 Apple Watch 解锁 Mac。适用于 macOS 12 及更高版本。
- 本地帐户设置选项：指定在设备上创建帐户的设置。Endpoint Management 首先使用您在此处指定的信息创建本地管理员帐户。用户激活其设备时，将创建一个用户帐户作为主帐户。创建主帐户作为标准用户选项决定主帐户是否具有管理员权限。

> 重要：
>
> 只能在 **macOS** 设置页面上将等待完成配置设置设置为开后，才能选择创建主帐户作为标准用户。

- 创建主帐户作为标准用户：选中时，Endpoint Management 将创建具有标准权限的用户，而非授予用户对设备的管理员权限。如果要向用户授予对设备的管理员权限，请跳过此选项。默认不选择此选项。
- 管理员全名：键入系统为管理员帐户显示的名称。
- 管理员短名称：键入设备为主文件夹显示的名称和在 shell 中显示的名称。
- 管理员密码：键入管理员帐户的安全密码。
- 显示用户和组中的管理员帐户：如果清除此选项，管理员帐户不会显示在 macOS 设置中的用户和组中。如果您创建主帐户作为标准用户，请启用此设置以隐藏 Endpoint Management 首先创建的管理员帐户。

为增强安全性，Endpoint Management 将检查是否每天轮转管理员帐户的密码。默认情况下，Endpoint Management 每 7 天轮转一次密码。要更改默认值，请更新 `mac.dep.admin.passwd.rotate` 服务器属性。有关详细信息，请参阅服务器属性。

为了增强密码强度和安全性，Endpoint Management 将按如下所示生成密码：

- 长度为 12 个字符
- 3 个大写字母
- 3 个小写字母
- 3 个数字
- 3 个特殊字符：`! \@ \## \$ % \^ \* ? + = -`

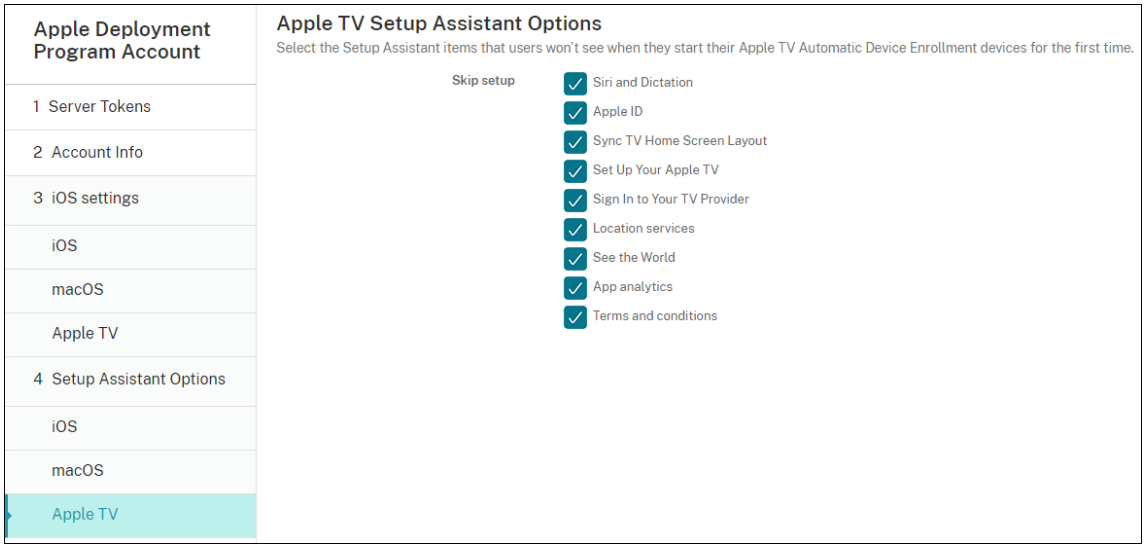
要查看设备的以前的密码、当前密码和密码更改状态，请转至管理 **>** 设置。单击该设备，单击显示更多，然后查看设备详细信息 **>** 常规页面。安全部分显示以下内容：

- **Previous administrator password**（以前的管理员密码）：允许您查看以前的密码。Endpoint Management 仅显示最后一个密码。单击显示密码以查看密码。
- **Current administrator password**（当前的管理员密码）：允许您查看当前的密码。
- **Change administrator password**（更改管理员密码）：允许您查看密码更改状态。可能会显示以下信息，具体取决于实际状态：

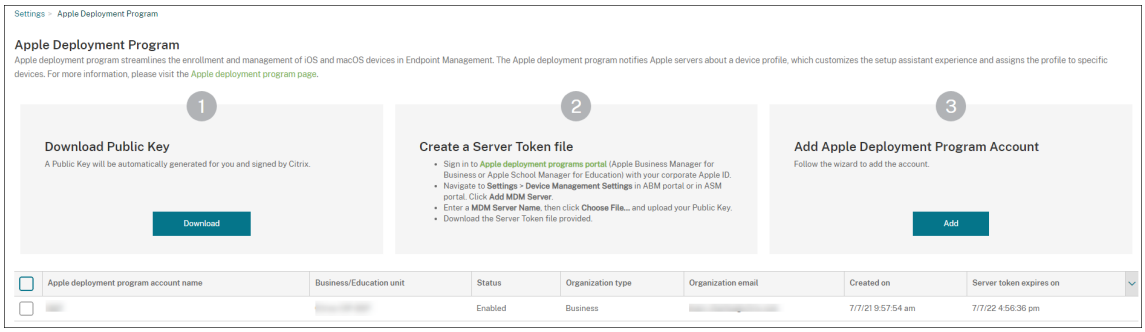
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 请求在 < 指定的时间值 > 更改密码。指定的时间值 >
- 密码已于 < 指定的时间值 > 更改。指定的时间值 >
- 尝试在 < 指定的时间值 > 更改密码失败。指定的时间值 >
- 密码尚未更改。

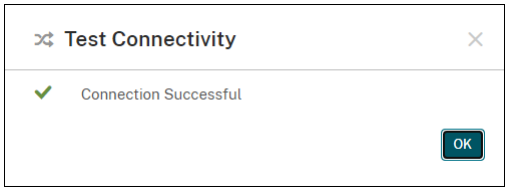
9. 在 **Apple TV** 设置助手选项中，选择您的用户在首次启动其设备时跳过的 Apple TV 设置助手步骤。所有项目的默认设置为未选中。保存更改。



10. 该帐户显示在设置 **> Apple** 部署计划上。要测试 Endpoint Management 与 Apple 之间的连接，请选择该帐户并单击测试连接。



此时将显示一条状态消息。



订购设备

可以直接从以下渠道订购设备：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Apple。向卖方提供 Apple 客户编号。
- 参与的 Apple 授权经销商或运营商。向卖方提供您的组织 ID，并获取其经销商 ID。

有关管理设备供应商的信息，请参阅《Apple 商务管理用户指南》或《Apple 校园教务管理用户指南》。

订单发货后，您购买的 Apple 设备将添加到您的 ABM 或 ASM 帐户中。

将设备分配给 **Endpoint Management**

在 ABM 或 ASM 门户中，搜索订单编号并使用该编号将此订单中的设备分配给 Endpoint Management。也可以使用 Apple Configurator 2 将 iPhone、iPad、iPod touch 和 Apple TV 设备添加到 ABM 或 ASM 中，而无论设备是从何处购买的。

有关详细信息，请参阅《Apple 商务管理用户指南》或《Apple 校园教务管理用户指南》。

批量购买内容，并将其同步到 **Endpoint Management**

ABM 和 ASM 允许您从单个组织帐户批量购买、分发和管理应用程序和书籍的许可证。为使 Endpoint Management 能够与 ABM 或 ASM 通信以获得要分发的许可证信息，请完成以下步骤：

1. 在 ABM 或 ASM 门户中，从 **Apps and Books**（应用程序和书籍）中购买公共应用程序和书籍，从 **Custom Apps**（自定义应用程序）中购买针对 Endpoint Management 开发的自定义应用程序。

   > 注意：
   >
   > 如果 Endpoint Management 与 Citrix Workspace 相集成，请购买 **Workspace** 应用程序，然后将其配置为 Endpoint Management 中的必需应用程序。

2. 在 ABM 或 ASM 门户中，下载分配给 Endpoint Management 的内容令牌。

   有关步骤 1 和 2 的详细信息，请参阅《Apple 商务管理用户指南》或《Apple 校园教务管理用户指南》。

3. 在 Endpoint Management 控制台中，根据您下载的内容令牌创建一个批量购买帐户。

   有关详细信息，请参阅通过 Apple 批量购买添加应用程序。

   创建批量购买帐户后，您购买的应用程序和书籍将显示在管理 > 应用程序中，分配给 Endpoint Management 服务器的设备将显示在管理 **>** 设备中。

配置设备策略和应用程序的部署规则

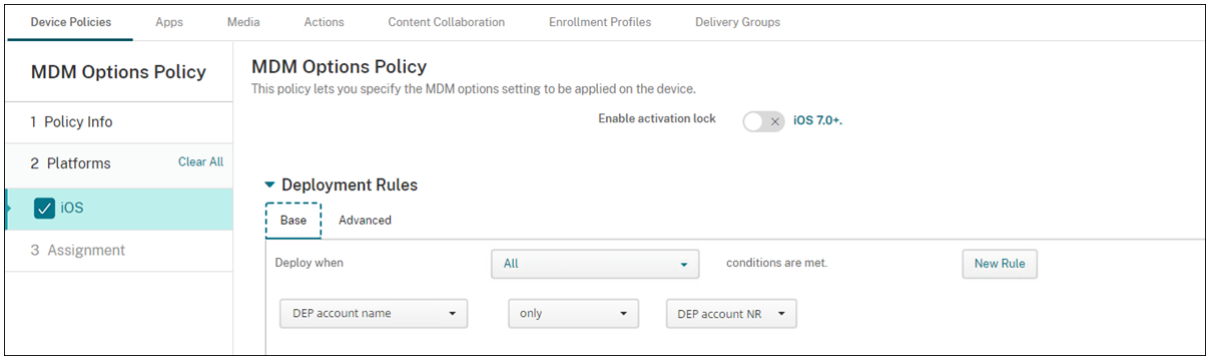
配置设备策略和应用程序时，可以将 ABM 或 ASM 帐户与不同的设备策略和应用程序关联。

1. 在配置 **>** 设备策略和配置 **>** 应用程序页面上，展开部署规则。
2. 为特定的 ABM 帐户或除所选帐户以外的所有 ABM 帐户指定策略或应用程序部署。

ABM 帐户的列表仅包括状态为已启用或已禁用的帐户。如果 ABM 帐户已禁用，ABM 设备将不属于该帐户。因此，Endpoint Management 不会将应用程序或策略部署到该设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在以下示例中，设备策略仅针对 ABM 帐户名称为 “ABM Account NR” 的设备进行部署。



批量注册 **Apple** 设备

September 13, 2022

您可以通过两种方式在 Endpoint Management 中注册大量 iOS、iPadOS、macOS 和 tvOS 设备：

- 使用 Apple 部署计划 (ADP) 注册您直接从 Apple 或从参与计划的 Apple 授权经销商或运营商处购买的 Apple 设备。

  有关部署启用 ADP 的设备的更多信息，请参阅 通过 Apple 部署计划部署设备。本文介绍用户如何注册启用了 ADP 的设备以及如何重新注册这些设备。

- 无论你是否直接从 Apple 购买 iOS 设备，都可以使用 Apple Configurator 2 注册 iOS 设备。

本文介绍了如何使用 Apple Configurator 2 批量部署设备。

关于批量注册

ADP 包括面向企业的 Apple 商务管理 (ABM) 和面向教育的 Apple 校园教务管理 (ASM)。通过 ADP 进行批量注册具有以下功能：

- 你不必触摸或准备设备。
- 在 Endpoint Management 中完成部署设置后，您可以将设备提供给可以立即开始使用它们的用户。
- 您可以通过省去一些设置助手步骤来简化用户的设置过程。
- 有关设置 ABM 和 ASM 的更多信息，请参阅 Apple 商务管理和 [Apple 校园教](https://school.apple.com/)务管理提供的文档。

通过 Apple Configurator 2 进行批量注册具有以下功能：

- 你可以将 iOS 设备连接到运行 macOS 10.7.2 或更高版本的 Mac 和 Apple Configurator 2 应用程序。您可以通过 Apple 配置器 2 准备 iOS 设备并配置策略。
- 设备在设置过程中自动注册 Endpoint Management。设置完成后，Endpoint Management 会将策略、应用程序和其他资源推送到设备。您之后可以开始管理设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 有关使用 Apple Configurator 2 的更多信息，请参阅 Apple Configurator 帮助。

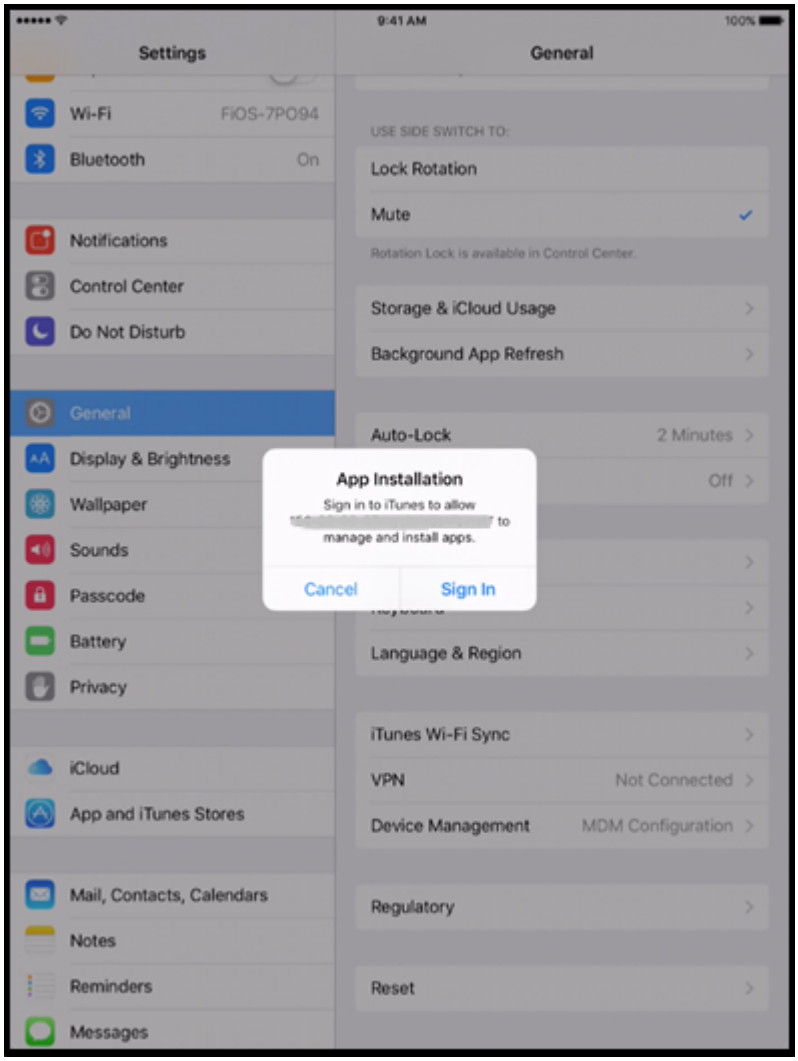
用户如何注册启用 **ADP** 的设备

用户按如下方式在 Endpoint Management 中注册其设备：

1. 用户启动他们的设备。
2. Endpoint Management 将您在 “设置” **> “Apple** 部署计划**”** 页面上配置的 ADP 设置传送到设备。
3. 用户在其设备上配置初始设置。
4. 该设备将自动启动 Endpoint Management 设备注册过程。
5. 如果将 Endpoint Management 与 Citrix Workspace 集成，部署计划的部署软件包中将包括 Workspace 应用程序作为必需应用程序。在这种情况下，Secure Hub 会提示用户先在 Citrix Workspace 中注册设备，然后在 Endpoint Management 中注册。
6. 用户继续在其设备上配置其他初始设置。
7. 在主屏幕中，可能会提示用户登录苹果应用商店，以便他们可以下载 Citrix Secure Hub。

   > 注意：
   >
   > 如果将 Endpoint Management 配置为使用基于设备的批量购买应用程序分配来部署 Secure Hub 应用程序，则此步骤是可选步骤。在这种情况下，你无需创建 Apple App Store 帐户或使用现有帐户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



8. 用户打开 Secure Hub 并键入其凭据。如果策略要求，系统可能会提示用户创建并验证 Citrix PIN。

   Endpoint Management 将任何其余必备应用程序部署到设备。

重新注册启用 **ADP** 的设备

启用 ADP 的设备在恢复出厂设置的情况下注册。要重新注册启用了 ADP 的设备，必须首先完成完全擦除才能取消注册设备。详细步骤如下所示：

1. 在 管理 **>** 设备页面上，选择设备。
2. 单击 **Security**（安全）。
3. 单击 “ 完全擦除” 以将设备取消注册到恢复出厂设置状态。
4. 启动设备。

> 重要：
>
> 请勿使用 选择性擦除来取消注册启用了 ADP 的设备，因为 ADP 注册要求设备处于恢复出厂设置状态。

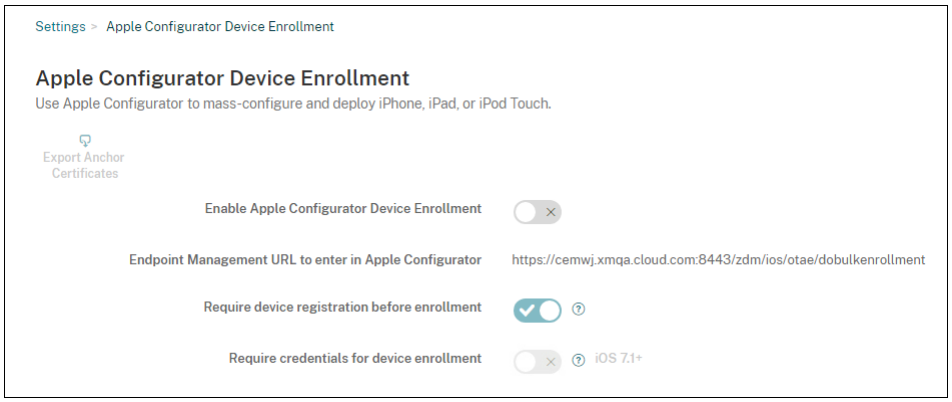
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使用 **Apple Configurator 2** 部署设备

你可以使用 Apple Configurator 2 部署包含设置、应用和数据的大量设备，并在 Endpoint Management 中注册这些设备。

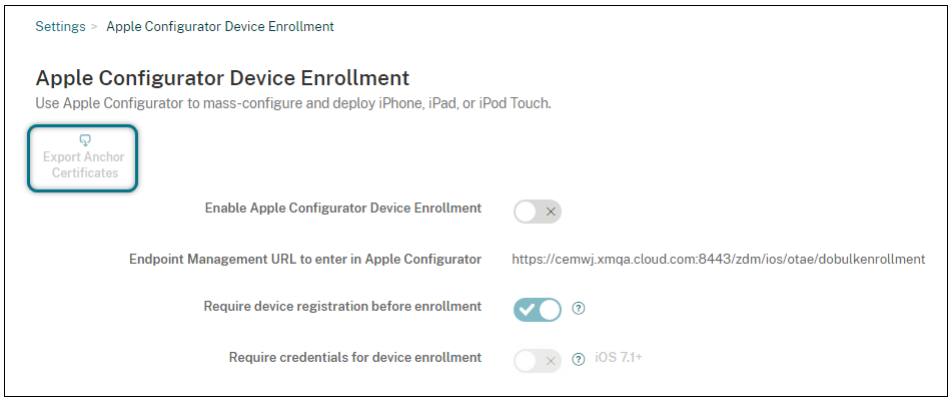
步骤 **1**：在 **Endpoint Management** 中配置设置

1. 在 Endpoint Management 控制台中，转至设置 **> Apple Configurator** 设备注册。



2. 将启用 **Apple Configurator** 设备注册设置为是。
3. 复制 注册 **URL** 以在 **Apple Configurator** 设置中输入，然后在 Apple 配置器 2 中配置设置时粘贴此 URL。此设置提供与 Apple 通信的 Endpoint Management 服务器的 URL。注册 URL 是 Endpoint Management 服务器完全限定域名 (FQDN)，例如 `mdm.server.url.com`，或 IP 地址。
4. 要防止注册未知设备，请将要求在注册之前注册设备设置为是。注意：如果此设置为是，必须先在 Endpoint Management 中手动或通过 CSV 文件将配置的设备添加到管理 **>** 设备，然后再进行注册。
5. 请将需要提供凭据才能完成设备注册设置为是，才能要求使用 iOS 设备的用户在注册时输入其凭据。默认值为否。

> 注意：
>
> 如果 Endpoint Management 服务器使用的是受信任的 SSL 证书，请跳过此步骤。单击导出锚点证书，然后将 certchain.pem 文件保存到 macOS 钥匙串中（登录或系统）。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

步骤 **2**：在 **Apple Configurator 2** 中配置设置

1. 准备一台运行 macOS 10.7.2 或更高版本并安装了 Apple Configurator 2 的 Mac。
2. 使用 Dock 连接器转 USB 电缆将 Apple 设备连接到 Mac。最多可以同时配置 30 台已连接的设备。如果没有基座接口，请使用一个或多个有源 USB 2.0 高速集线器连接设备。
3. 启动 Apple Configurator 2。该配置器会显示您能够准备监督的任何设备。
4. 准备设备以进行监督：
   - 如果您打算通过定期重新应用配置来保留对设备的控制权，请选择 **Supervise devices**（监督设备）。单击下一步。

     > 重要：
     >
     > 将设备置于受监督模式时，系统将会在设备上安装所选版本的 iOS，同时完全擦除设备上以前存储的任何用户数据或应用程序。

   - 在 iOS 中，单击 **Latest**（最新），获取您要安装的最新版本的 iOS。
5. 在在 **MDM** 服务器中注册中，选择 MDM 服务器。要添加服务器，请单击 “ 下一步”。
6. 在 定义 **MDM** 服务器中，提供服务器的名称，然后从 Endpoint Management 控制台粘贴 MDM 服务器 URL。
7. 在分配给组织中，选择要监督设备的组织。

   有关通过 Apple Configurator 2 准备设备的详细信息，请参阅 Apple Configurator 帮助页面准备设备。
8. 在配置每个设备的过程中，请将其打开以启动 iOS 设置助理，以便为首次使用准备好设备。

使用 **Apple Configurator 2** 将设备添加到 **ABM** 或 **ASM**

您可以使用 Apple Apple Configurator 2 将 iPhone、iPad 和 Apple TV 设备添加到您的 ABM 或 ASM 帐户，无论这些设备是在哪里购买的。
添加设备后，它们将显示在 “ 设备” 部分中。这些设备不再包含通过 Apple Configurator 2 分配的注册设置。有关详细信息，请参阅《Apple 商务管理用户指南》或《Apple 校园教务管理用户指南》。

续订 **ADP** 令牌

当您的 ADP 令牌过期时，Endpoint Management 会显示许可证过期警告。替换来自 ASM 或 ABM 的令牌。

步骤 **1**：从 **Endpoint Management** 服务器下载公钥

1. 在 Endpoint Management 控制台中，转至设置 **> Apple** 部署计划计划以下载新公钥。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

步骤 **2**：在您的 **Apple** 帐户中创建并下载服务器令牌文件

1. 登录 ABM 以下载令牌。
2. 打开设置并选择需要令牌的服务器。单击编辑。
3. 在 **MDM** 服务器设置下，上传从 Endpoint Management 下载的新公钥并保存更改。
4. 单击下载令牌以下载新令牌。

步骤 **3**：在 **Endpoint Management** 中上载服务器令牌文件

1. 在 Citrix Endpoint Management 中，转到设置 **> Apple** 部署计划。
2. 选择部署计划帐户，单击编辑，然后上载您的服务器令牌文件。
3. 单击下一步保存更改。

与 **Apple** 教育功能相集成

July 7, 2023

在使用 Apple 教育功能的环境中，可以使用 Endpoint Management 作为您的移动设备管理 (MDM) 解决方案。Endpoint Management 支持包括 Apple 校园教务管理 (ASM) 和面向 iPad 的课堂应用程序。Endpoint Management 的教育配置设备策略配置教师和学生的设备以供 Apple 教育功能使用。

您负责向教师和学生提供预配置并且受监督的 iPad。该配置包括 Endpoint Management 中的 ASM 注册、配置了新密码的管理式 Apple ID 帐户以及必需的批量购买应用程序和 iBooks。

有关 Apple 教育功能的更多信息，请参阅 Apple 教育 网站和来自同一站点的 Apple 教育部署指南。

Apple 校园教务管理

请按照以下常规步骤将 Endpoint Management 与 ASM 集成。

1. 在 ASM 中为您的机构创建一个账户，以便在 ASM 中注册您的机构。
2. 为 Apple 校园管理员配置教育批量购买账户。
3. 为 Apple 校园教务管理用户添加密码。
4. 规划资源和交付组并将其添加到 Endpoint Management 中。
5. 测试教师和学生设备注册情况。
6. 向教师和学生提供预配置的设备。
7. 管理教师、学生和班级数据
8. 如果设备丢失或被盗，您可以锁定并找到设备。

有关注册 ASM 以及将账户连接到 Endpoint Management 的信息，请参阅 通过 Apple 部署计划部署设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

必备条件

- Citrix Gateway
- 为 MDM+MAM 配置的注册配置文件。
- 安装了 iOS 9.3（最低版本）的 Apple iPad 第三代（最低版本）或 iPad Mini

> 注意：
>
> Endpoint Management 不针对 LDAP 或 Active Directory 验证 ASM 用户帐户。但是，可以将 Endpoint Management 连接到 LDAP 或 Active Directory 以便管理与 ASM 教师或学生无关的用户和设备。例如，可以使用 Active Directory 将 Secure Mail 和 Secure Web 提供给其他 Apple ASM 成员，例如 IT 管理员和经理。
>
> 由于 Apple ASM 教师和学生都是本地用户，因此，不需要向其设备部署 Citrix Secure Hub。
>
> 包括 Citrix Gateway 身份验证的 MAM 注册不支持本地用户（仅支持 Active Directory 用户）。因此，Endpoint Management 仅向教师和学生设备部署必需的批量购买应用程序和 iBooks。

适用于 **iPad** 的 **“课堂”** 应用程序

通过适用于 iPad 的 “课堂” 应用程序，教师可以连接到学生的设备以及对其进行管理。可以查看设备屏幕、打开 iPad 上的应用程序、共享并打开 Web 链接以及在 Apple TV 上呈现学生的屏幕。

“课堂” 应用程序在 App Store 中免费提供。您将应用程序上载到 Endpoint Management 控制台。随后使用教育配置设备策略配置 “课堂” 应用程序（将该应用程序部署到教师的设备）。

有关如何部署课堂应用的更多信息，请参阅 分发 Apple 应用程序。

有关课堂应用要求、设置和功能的更多信息，请参阅 Apple 支持网站上的 课堂用户指南 。

为 **Apple** 校园教务管理用户添加密码

添加 ASM 帐户后，Endpoint Management 将从 ASM 导入类和用户。Endpoint Management 将班级视为本地组，并在控制台中使用术语 “组”。如果某个班级在 ASM 中具有组名称，Endpoint Management 会将该组名称分配给班级。否则，Endpoint Management 将为组名称使用源系统 ID。Endpoint Management 不为班级名称使用课程名称，因为 ASM 中的课程名称不唯一。

Endpoint Management 使用管理式 Apple ID 创建用户类型为 **ASM** 的本地用户。这些用户属于本地用户，因为 ASM 创建的凭据与所有外部数据源都无关。因此，Endpoint Management 不使用目录服务器对这些新用户进行身份验证。

ASM 不会向 Endpoint Management 发送临时用户密码。可以从 CSV 文件导入或手动添加这些密码。要导入临时用户密码，请执行以下操作：

1. 获取 ASM 在创建管理式 Apple ID 临时密码时生成的 CSV 文件。
2. 编辑 CSV 文件，将临时密码替换为用户在 Endpoint Management 中注册时提供的新密码。为实现这一目的，不对密码类型设置任何限制。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

CSV 文件中的条目格式如下所示：`user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

其中：

用户：`user@appleid.citrix.com`

名字：`Firstname`

中间名：`Middle`

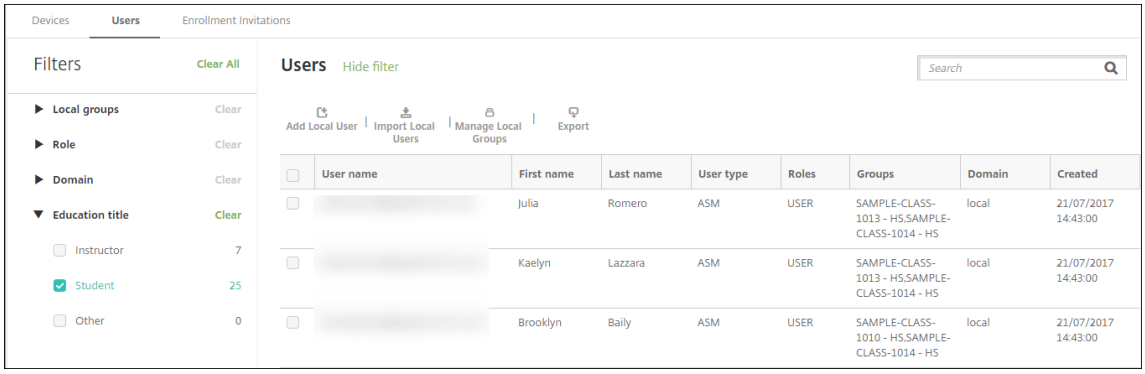
姓氏：`Lastname`

密码：`Password123!`

3. 在 Endpoint Management 控制台中，单击管理 **>** 用户。此时将显示用户页面。

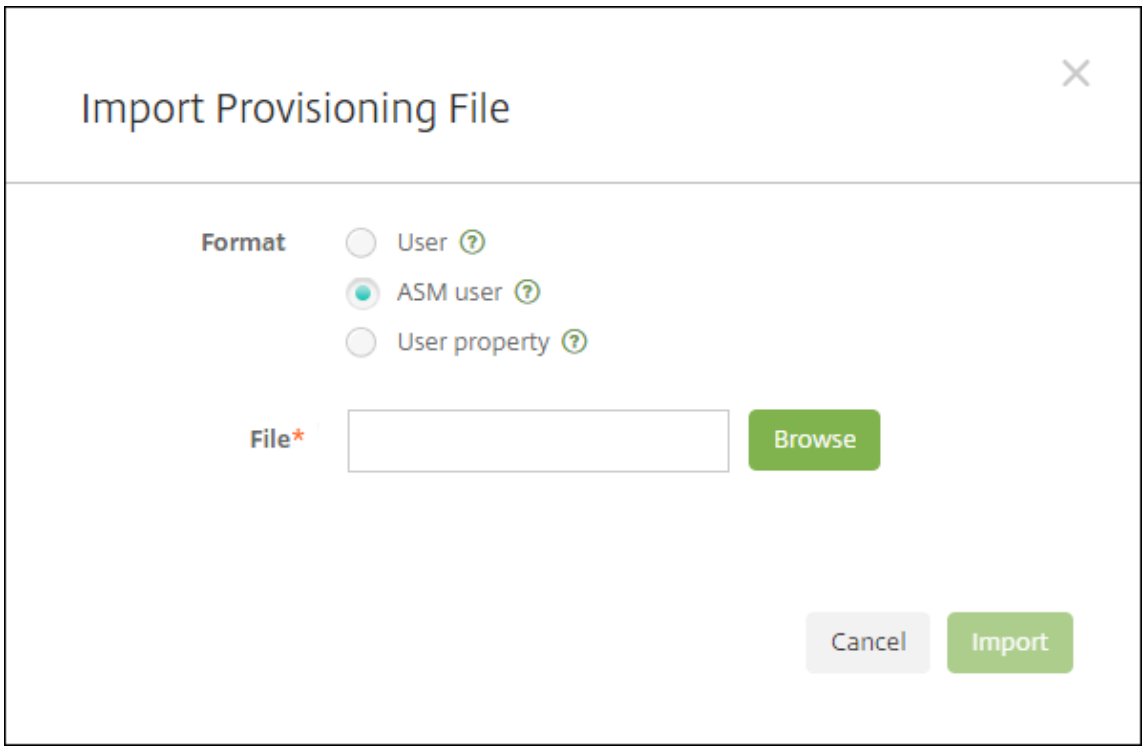
   下面的管理 **>** 用户屏幕示例显示了从 ASM 中导入的用户的列表。在用户列表中：

   - 用户名显示管理式 Apple ID。
   - 用户类型为 **ASM**，指示源自 ASM 的帐户。
   - 组显示班级。

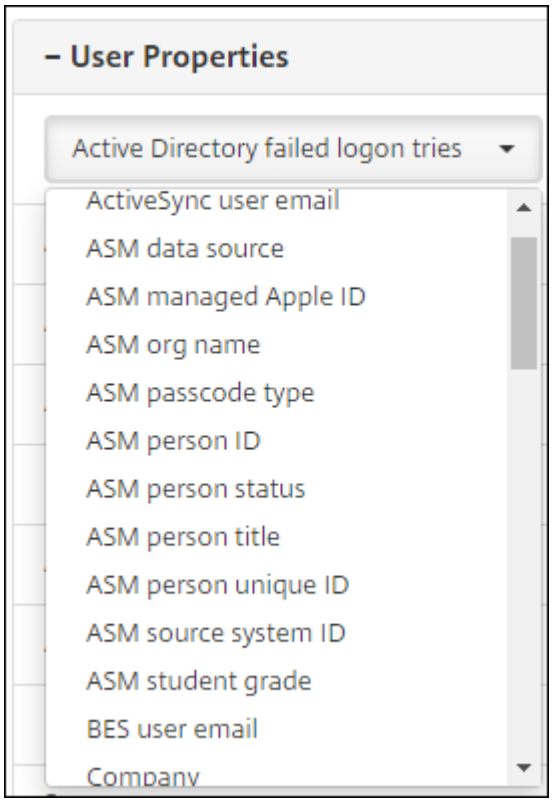


4. 单击导入本地用户。此时将显示导入预配文件对话框。
5. 对于格式，请选择 **ASM** 用户，导航到您在步骤 2 中准备的 CSV 文件，然后单击导入。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 要查看某个本地用户的属性，请选择该用户，然后单击编辑。



除名称属性外，还可以使用以下 ASM 属性：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **ASM** 数据源：班级的数据源，例如 **CSV** 或 **SFTP**。
- **ASM** 管理式 **Apple ID**：管理式 Apple ID 可能包括您的机构名称和 `appleid`。例如，该 ID 可能类似于 johnappleseed@appleid.myschool.edu。Endpoint Management 需要使用管理式 Apple ID 进行身份验证。
- **ASM** 组织名称：您在 Endpoint Management 中为帐户指定的名称。
- **ASM** 通行码类型：人员的密码策略：复杂（包含 8 个或更多数字和字母的非学生用密码）、**four**（4）（数字）或 **six**（6）（数字）。
- **ASM** 人员的唯一 **ID**：用户的标识符。
- **ASM** 人员状态：指定管理式 Apple ID 的状态为活动还是不活动。用户提供其管理式 Apple ID 帐户的新密码后，此状态将变为活动。
- **ASM** 人员职称：“教师”、“学生”或“其他”。
- **ASM** 人员的唯一 **ID**：用户的唯一标识符。
- **ASM** 源系统 **ID**：系统源的标识符。
- **ASM** 学生年级：学生的年级信息（教师不使用）。

规划资源和交付组并将其添加到 **Endpoint Management**

交付组指定要部署到各类别的用户的资源。例如，可以为教师和学生创建一个交付组。或者，可以创建多个交付组，以便您能够自定义发送给不同教师或学生的应用程序、媒体和策略。可以为每个班级创建一个或多个交付组。还可以为管理员（教育机构中的其他员工）创建一个或多个交付组。

部署到用户设备的资源包括设备策略、批量购买应用程序和 iBooks。

- 设备策略：

  如果教师使用“课堂”应用程序，则需要配置教育配置设备策略。请务必检查其他设备策略，以确定您希望如何配置和限制教师和学生的 iPad。

- 批量购买应用程序：

  Endpoint Management 要求您将批量购买应用程序部署为教育用户的必需应用程序。Endpoint Management 不支持将此类批量购买应用程序作为可选应用程序进行部署。

  如果您使用 Apple“课堂”应用程序，请仅将其部署到教师的设备。

  部署要提供给教师或学生的任何其他应用程序。此解决方案不使用 Citrix Secure Hub 应用程序，因此，不需要为教师或学生部署。

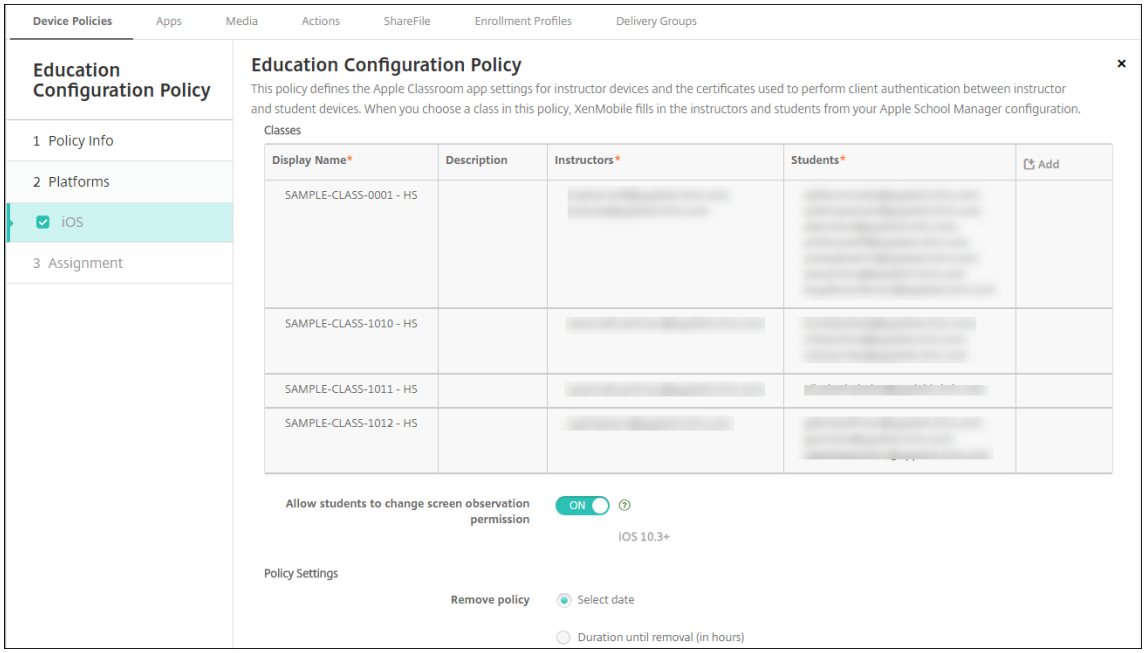
- 批量购买 iBooks：

  Endpoint Management 连接到您的 ASM 帐户后，您购买的 iBooks 将显示在 Endpoint Management 控制台的配置 **>** 媒体中。该页面上列出的 iBooks 可以添加到交付组中。Endpoint Management 仅支持将 iBooks 添加为所需媒体。

为教师和学生规划资源和交付组后，可以在 Endpoint Management 控制台中创建这些项目。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 创建要为教师或学生设备部署的任何设备策略。有关教育配置设备策略的信息，请参阅教育配置设备策略。

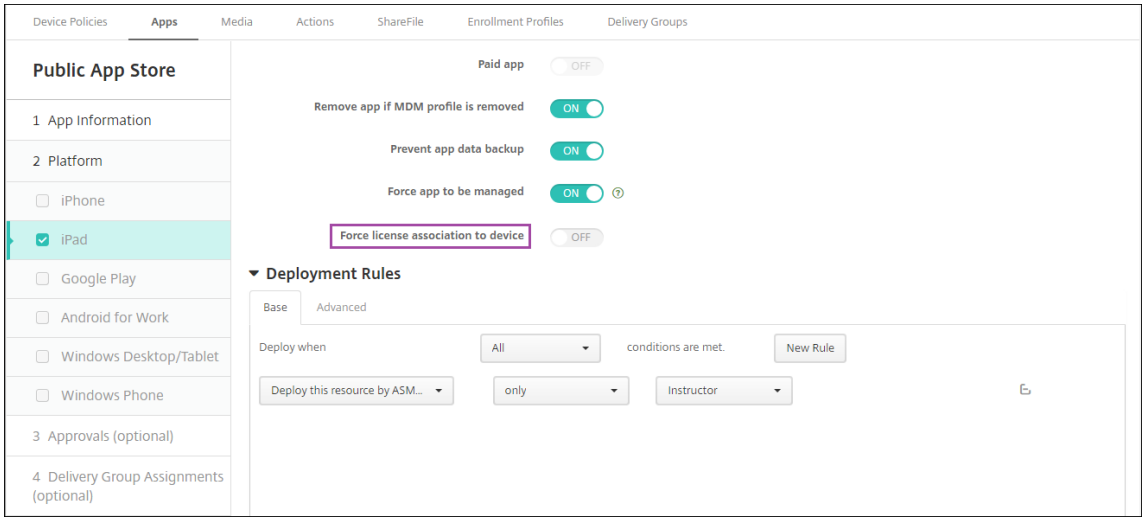


有关设备策略的信息，请参阅设备策略以及各策略文章。

2. 配置应用程序（配置 > 应用程序）和 iBooks（配置 > 媒体）：

   - 默认情况下，Endpoint Management 在用户级别分配应用程序和 iBooks。首次部署过程中，教师和学生将收到一条提示注册参加 ASM 的提示。接受邀请后，用户会在接下来的部署中（6 个小时内）收到其 ASM 应用程序和 iBooks。Citrix 建议您强制为新 ASM 用户部署应用程序和 iBooks。为此，请选择交付组并单击部署。

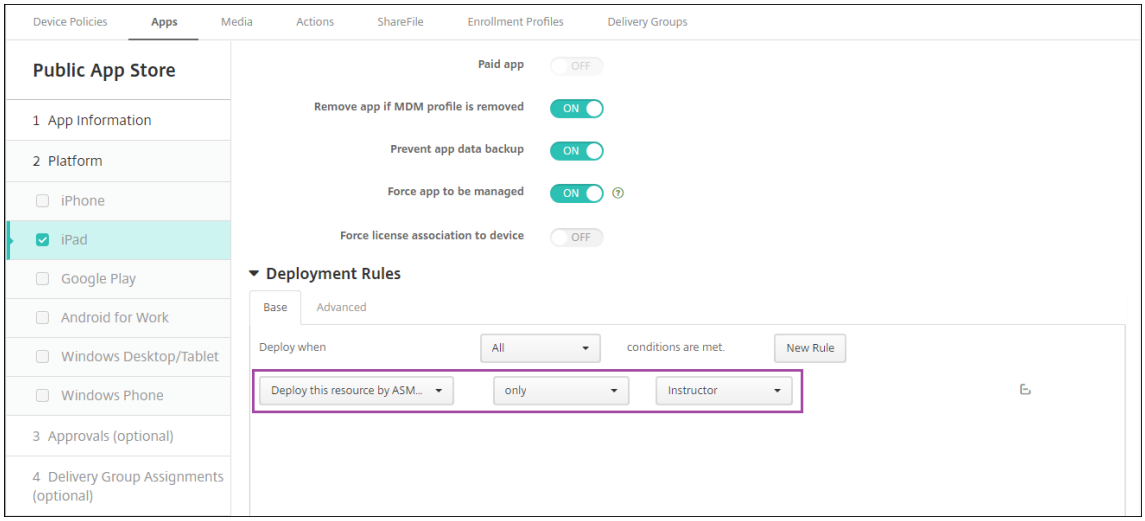
     可以选择在设备级别分配应用程序（而非 iBooks）。为此，请将强制与设备建立许可证关联设置更改为开。在设备级别分配应用程序时，用户不会收到加入批量购买计划的邀请。



   - 要仅为教师部署应用程序，请选择仅包括教师的交付组，或者使用以下部署规则：

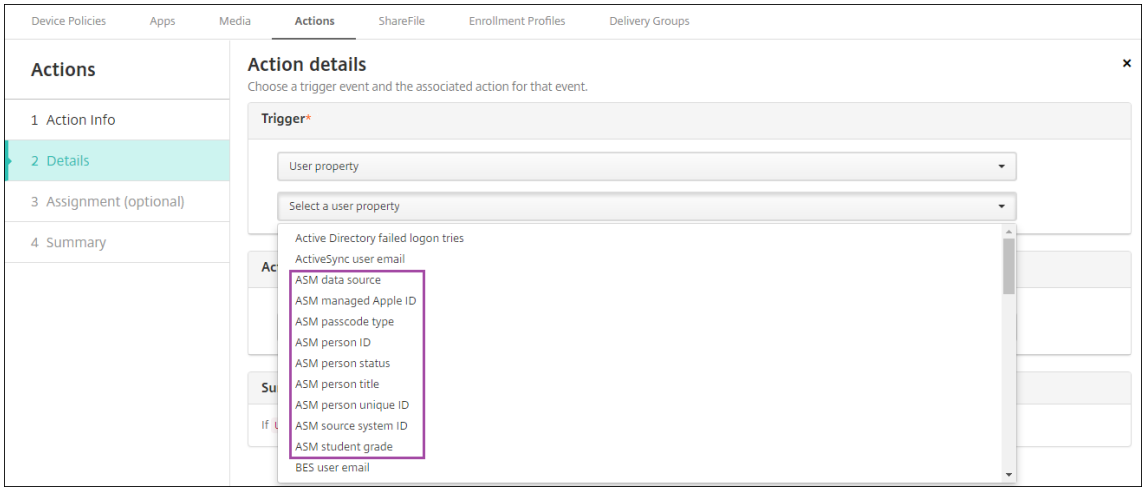
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
Deploy this resource by ASM device type
only
Instructor
<!--NeedCopy-->
```



- 有关添加批量购买应用程序的帮助，请参阅 添加公共应用商店应用程序。

3. 可选。根据 ASM 用户属性创建操作。例如，您可能会创建在新应用程序安装时向学生设备发送通知的操作。或者，可以创建用户属性触发的操作，如以下示例中所示。



要创建操作，请转至配置 > 操作。有关配置操作的信息，请参阅自动化操作。

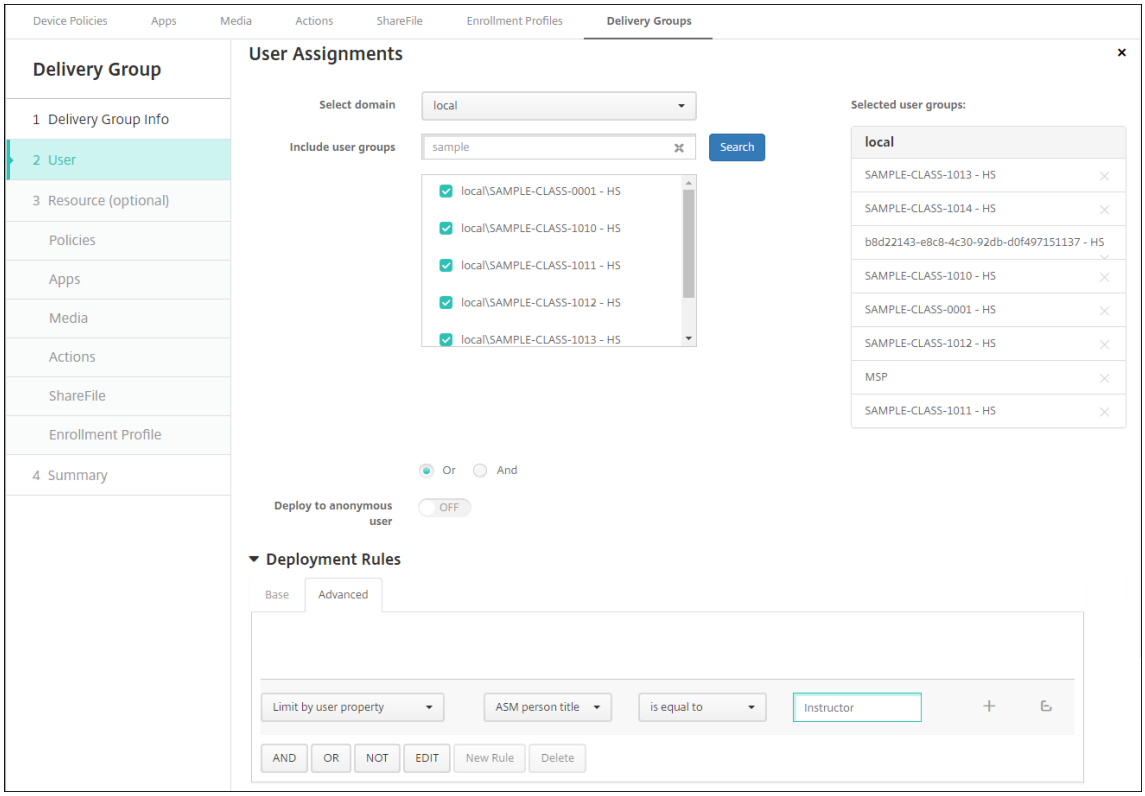
4. 在配置 > 交付组中，为教师和学生创建交付组。选择从 ASM 中导入的班级。此外，请为教师和学生创建部署规则。

   例如，以下用户分配针对教师。部署规则为：

```
Limit by user property
ASM person title
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

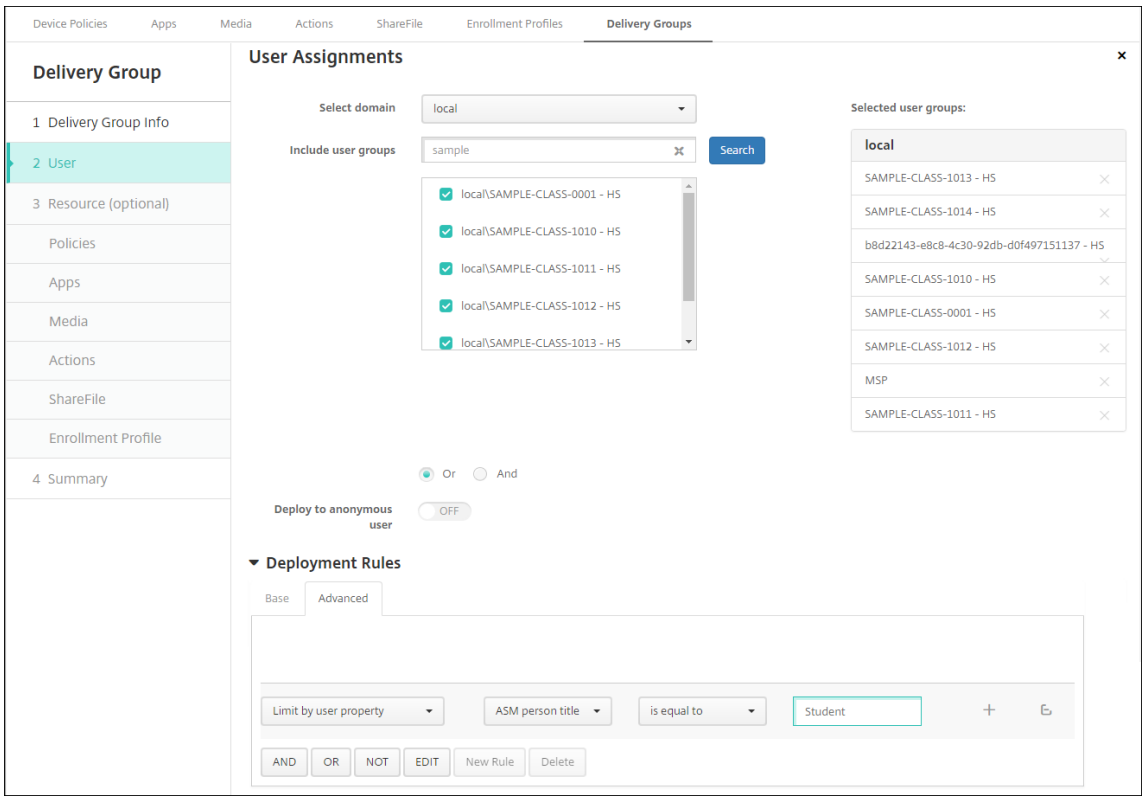
```
is equal to
Instructor
<!--NeedCopy-->
```



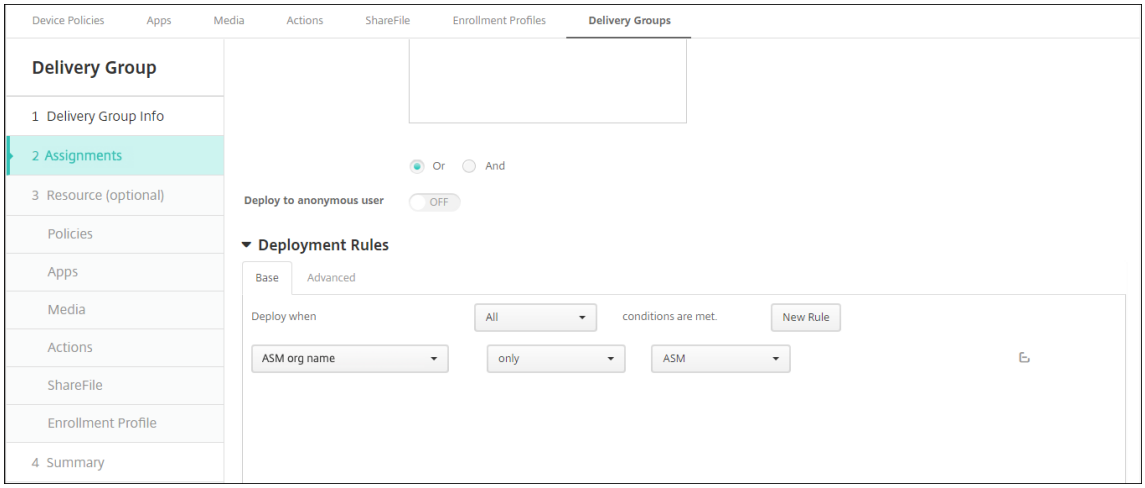
以下用户分配针对学生。部署规则为：

```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

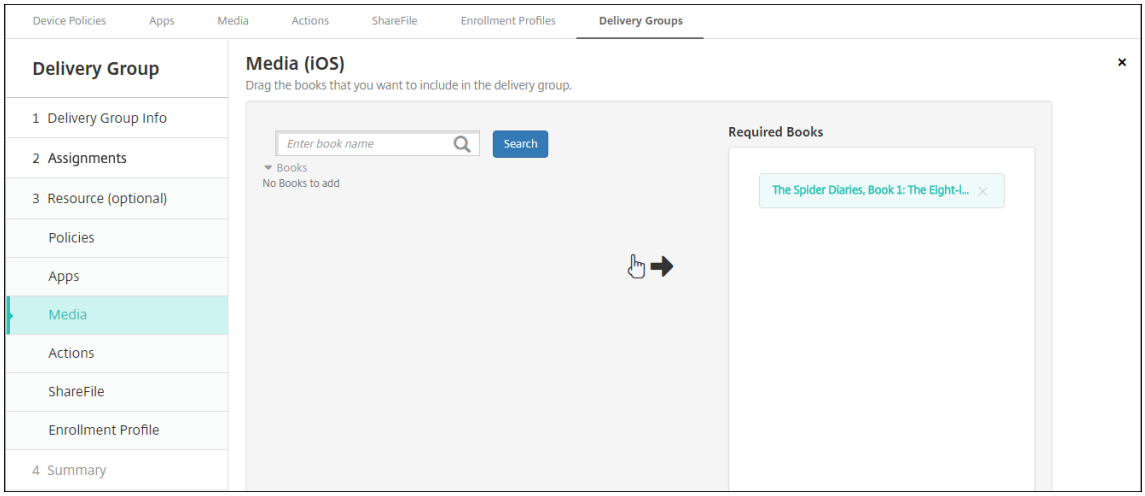


还可以使用基于 ASM 组织名称的部署规则过滤交付组。

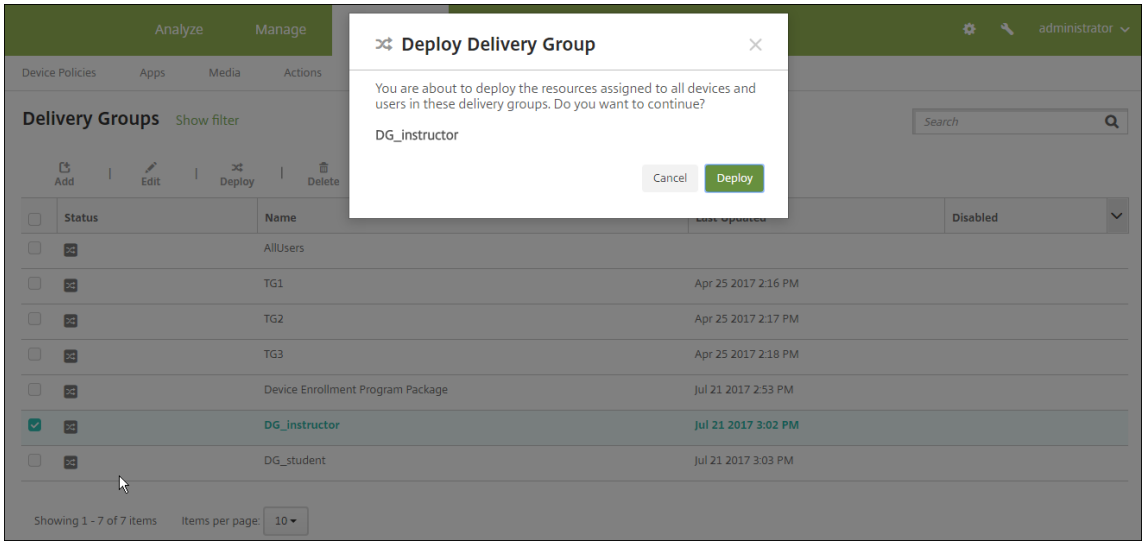


5. 将资源分配给交付组。以下示例显示了交付组中包含的 iBook。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



以下示例显示了在您选择交付组并单击部署时显示的确认对话框。



有关详细信息，请参阅部署资源中的“编辑交付组”和“部署到交付组”。

测试教师和学生设备注册

可以通过以下方法之一注册设备：

- 学校管理员可以使用您能够在 Endpoint Management 控制台中设置的用户密码注册教师和学生设备。因此，可以向用户提供设置了应用程序和媒体的设备。
- 收到设备时，用户使用您向其提供的用户密码进行注册。注册完成后，Endpoint Management 将向设备发送设备策略、应用程序和媒体。

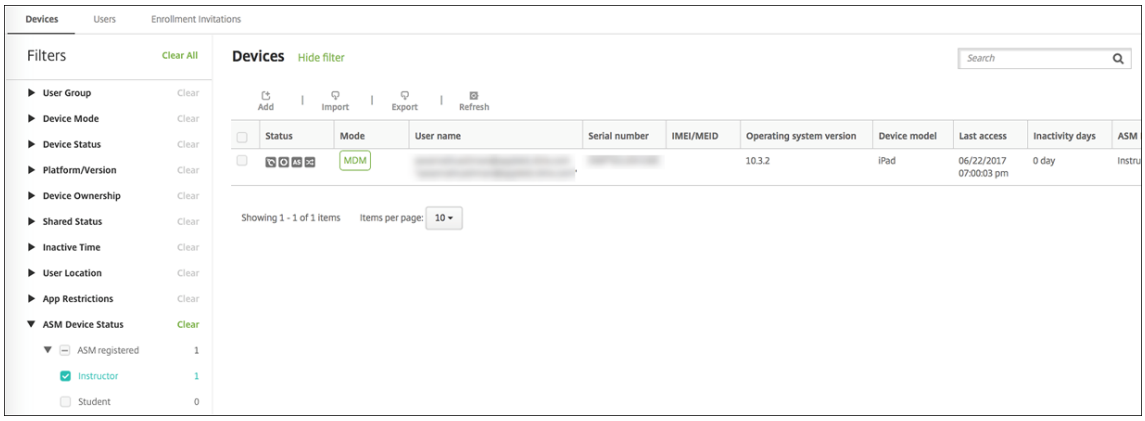
要测试注册，请使用链接到 ASM 的 Apple 部署计划设备。

1. 如果设备未链接到 ASM，请通过执行硬重置来擦除设备内容和设置。
2. 将 ASM 设备注册给教师。然后，将 ASM 设备注册给学生。

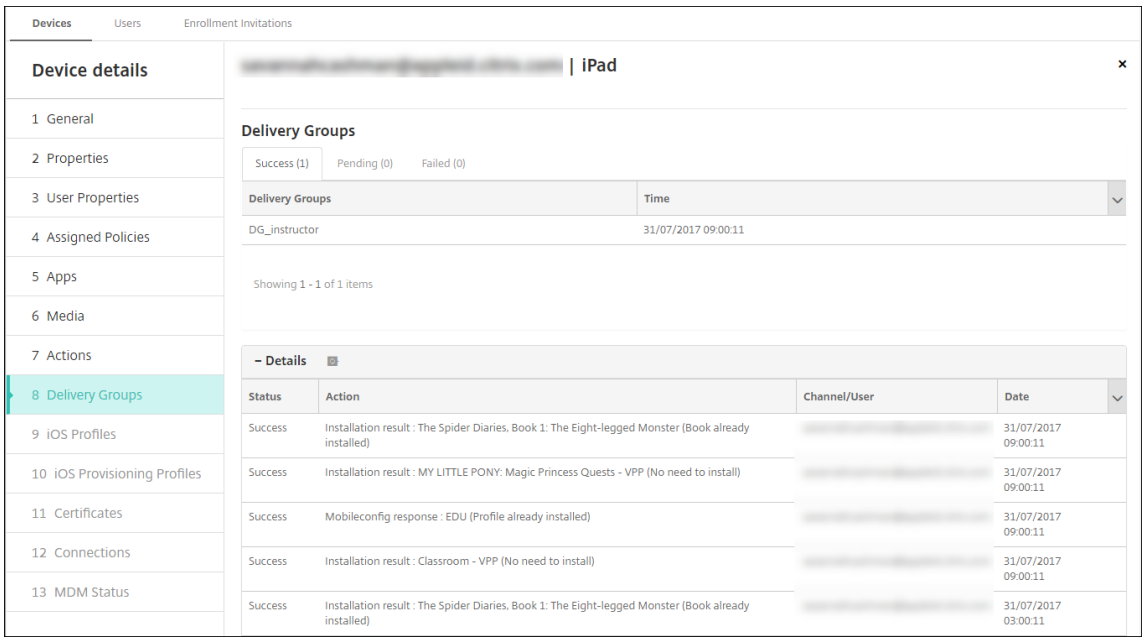
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 在管理 **>** 设备页面中，检查 ASM 设备是否在仅 MDM 模式下注册。

   可以按 ASM 设备状态过滤设备页面：已注册 **ASM**、已共享 **ASM**、教师和学生。



4. 要验证是否为每个设备正确部署了 MDM 资源，请执行以下操作：选择设备，单击编辑，然后检查各页面。



分发设备

Apple 建议您举办活动，以便能够将设备分发给教师和学生。

如果未分发预注册的设备，还需要向这些用户提供以下各项内容：

- 用于注册的 Endpoint Management 密码
- 管理式 Apple ID 的 ASM 临时密码。

首次用户体验如下所示。

1. 用户在硬重置后首次启动其设备时，Endpoint Management 将在注册屏幕中提示用户注册其设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 用户提供其管理式 Apple ID 和 Endpoint Management 密码，用于对 Endpoint Management 进行身份验证。
3. 在 Apple ID 设置步骤中，设备将提示用户提供其管理式 Apple ID 和 ASM 的临时密码。这些项目将对 Apple 服务验证用户的身份。
4. 设备提示用户为其管理式 Apple ID 创建密码，用于保护 iCloud 中的数据。
5. 在设置助手结束时，Endpoint Management 将开始向设备中安装策略、应用程序和媒体。对于在用户级别分配的应用程序和 iBooks，设置助手将提示教师和学生注册参加批量购买。接受邀请后，用户会在接下来的部署中（6 个小时内）收到其批量购买应用程序和 iBooks。

管理教师、学生和班级数据

管理教师、学生和班级数据时，请注意以下事项：

- 将 ASM 信息导入 Endpoint Management 后，请勿更改托管的 Apple ID。Endpoint Management 还使用 ASM 用户标识符来标识用户。
- 如果您在创建一个或多个“教育配置”设备策略后在 ASM 中添加或更改了班级数据，请编辑策略，然后重新部署这些策略。
- 如果班级的教师在您部署教育配置设备策略后发生了变化，请检查策略以确保其在 Endpoint Management 控制台进行了更新，然后重新部署该策略。
- 如果您在 ASM 门户中更新了用户属性，Endpoint Management 还将在控制台中更新这些属性。但是，Endpoint Management 不通过与接收其他属性相同的方式接收 ASM 人员职务属性，即“教师”、“学生”或“其他”。因此，如果您在 ASM 中更改了 ASM 人员职务，请完成以下步骤以在 Endpoint Management 中反映该更改。

要管理数据，请执行以下操作：

1. 在 ASM 门户中，更新学生年级并清除教师年级。
2. 如果您将学生帐户更改为教师帐户，请将该用户从班级中的学生列表中删除。然后，将该用户添加到同一班级或其他班级中的教师列表中。

   如果您将教师帐户更改为学生帐户，请将该用户从班级中删除。然后，将该用户添加到同一班级或其他班级中的学生列表中。您的更新将在下次同步时在 Endpoint Management 控制台中显示（默认时间间隔为每隔 5 分钟）或提取（默认时间间隔为每隔 24 小时）。
3. 编辑教育配置设备策略以应用更改并重新部署。
   - 如果从 ASM 门户中删除用户，Endpoint Management 还会在提取后从 Endpoint Management 控制台中删除该用户。

     可以通过更改以下服务器属性值来缩短两个基线之间的时间间隔：**bulk.enrollment.fetchRosterInfoDelay**（默认值为 **1440** 分钟）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 部署资源后：如果学生加入了某个班级，请创建仅包含该学生的交付组，并为该学生部署资源。
- 如果某个学生或教师丢失了临时密码，请其联系 ASM 管理员。管理员可以提供临时密码或生成一个新密码。

管理丢失或被盗的设备

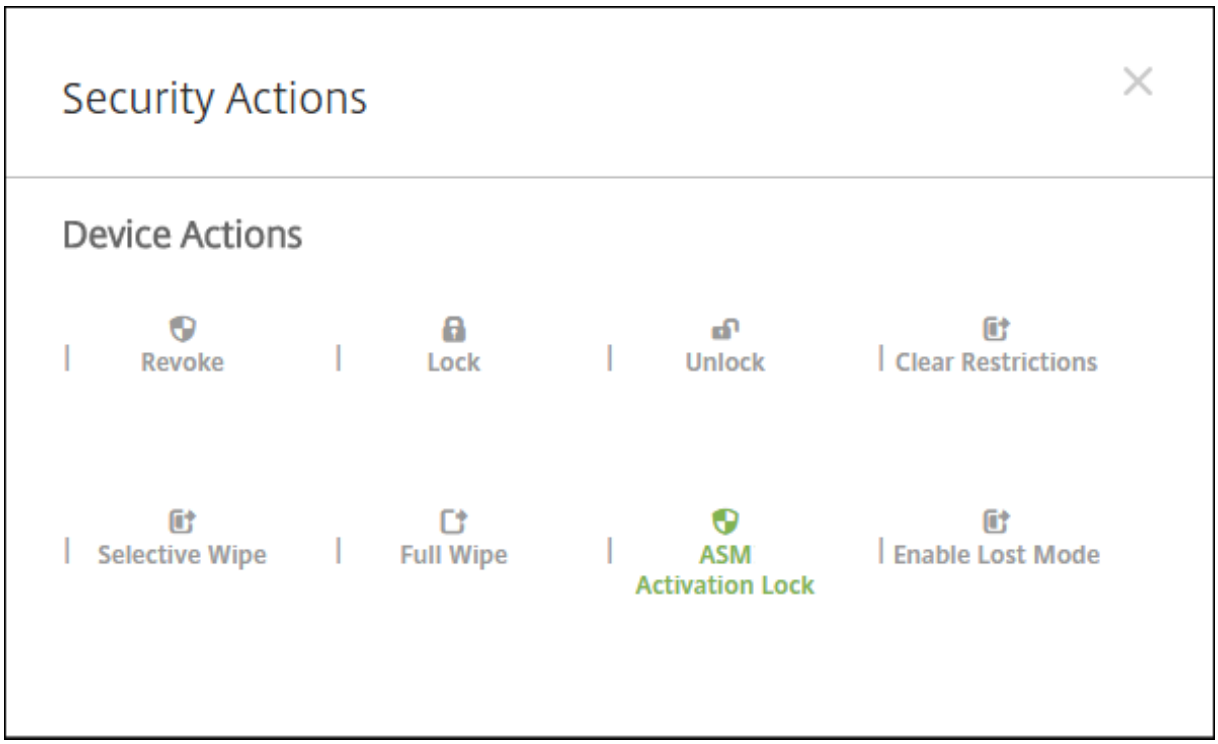
Apple 的“查找我的 iPhone/iPad”服务包括激活锁功能。激活锁可防止未授权的用户使用或转售在 Apple 部署计划中注册的丢失或被盗设备。

Endpoint Management 包括 **ASM** 激活锁安全操作，使您能够将锁定代码发送到已注册 ASM Apple 部署计划的设备。

使用 **ASM** 激活锁安全操作时，Endpoint Management 不需要用户启用“查找我的 iPhone/iPad”服务即可定位设备。ASM 设备被硬重置或完全擦除后，用户需要提供其管理式 Apple ID 和密码才能解锁该设备。

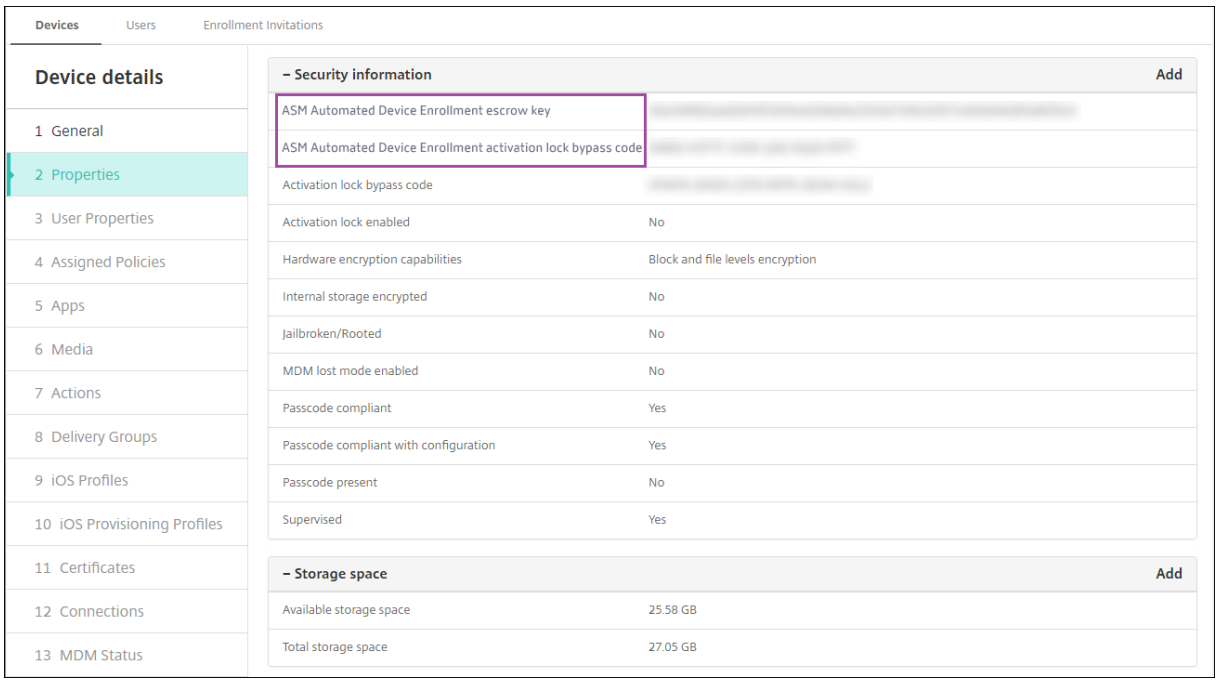
要从控制台中释放锁定，请单击安全操作激活锁绕过。有关绕过激活锁的信息，请参阅 绕过 iOS 激活锁。用户还可以将登录保留为空，并键入 **ASM** 激活锁绕过码作为密码。该信息在属性选项卡上的设备详细信息中提供。

要设置激活锁，请转至管理 **>** 设备，选择设备，单击安全性，然后单击 **ASM** 激活锁。

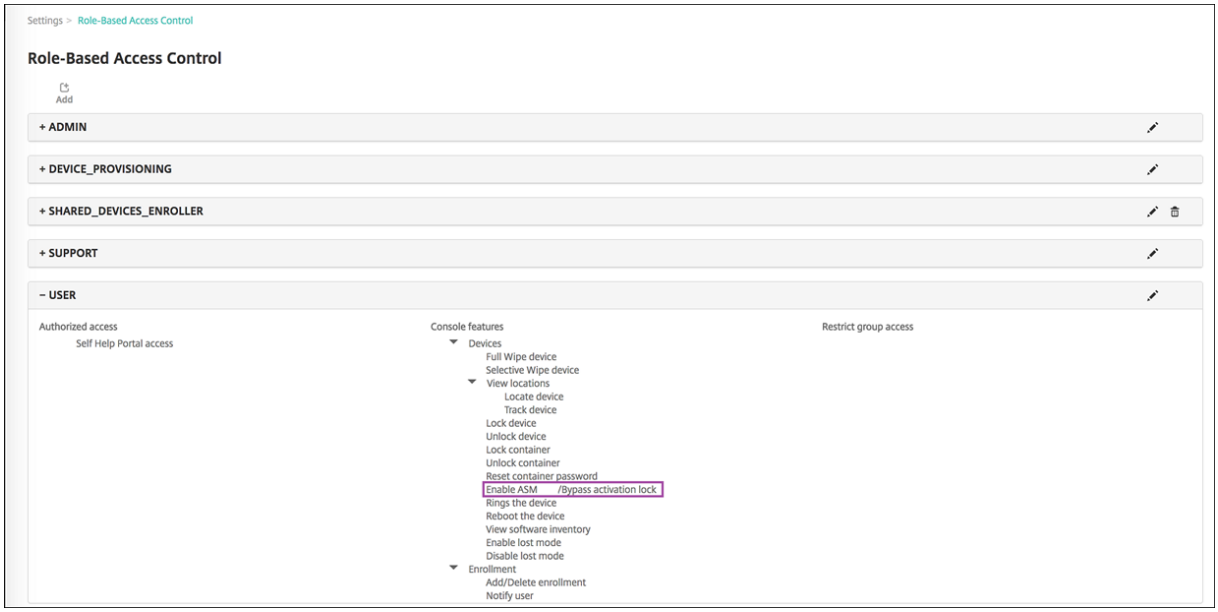


属性 **ASM** 托管密钥和 **ASM** 激活锁绕过码显示在设备详细信息中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



ASM 激活锁的 RBAC 权限为设备 **>** 启用 **ASM** 绕过激活锁。



共用的 **iPad**

April 11, 2023

共享的 iPad 功能允许多个用户使用 iPad。即使设备是共享的，也可以个性化用户体验。您可以将共享的 iPad 用于教育或商业。除了 Apple 商务管理 (ABM) 支持的角色之外，Apple 校园教务管理 (ASM) 还支持教师和学生角色。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

共用的 **iPad** 的必备条件

- Apple 校园教务或 Apple 商务管理
- Citrix Endpoint Management
- 任意 iPad Pro、iPad 第五代、iPad Air 2 或更高版本以及 iPad mini 4 或更高版本
- 至少 32 GB 存储空间
- 受监督设备

配置共用的 **iPad**

多名学生或员工可以出于不同的目的共享 iPad。

您或设备所有者注册 Shared iPad，然后将设备策略、应用程序和媒体部署到设备上。之后，用户提供他们的托管 Apple ID 凭据以登录共享 iPad。如果您以前为学生部署了“教育配置”策略，这些学生将不再以“其他用户”身份登录共享设备。

Endpoint Management 为共享 iPad 使用两个通信渠道：设备所有者（教师或主管）的系统频道和当前常驻用户（学生或员工）的用户频道。Endpoint Management 使用这些通道为 Apple 支持的资源发送恰当的 MDM 命令。

通过系统通道部署的资源如下：

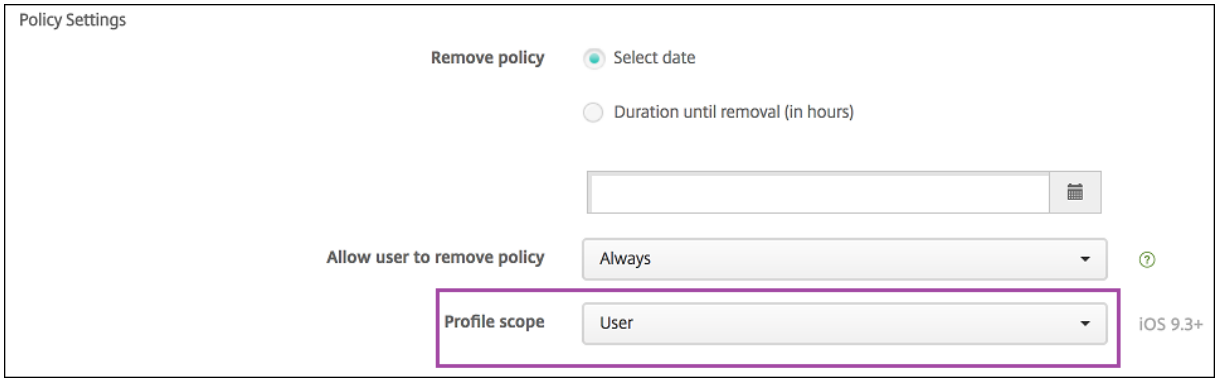
- 设备策略，例如 教育配置、锁屏消息、最大常驻用户数和 密码锁定宽限期
- 基于设备的批量购买应用程序
  Apple 不支持共享 iPad 上的企业应用程序或基于用户的批量购买应用。共用的 iPad 上安装的应用程序是设备的全局应用程序，不基于用户。
- 基于用户的批量购买 iBooks
  Apple 支持在共享 iPad 上分配基于用户的批量购买 iBooks。

通过用户通道部署的资源如下：

- 设备策略：应用程序通知、主屏幕布局、限制和 Web 剪辑。

  Endpoint Management 仅支持通过用户通道部署这些设备策略。

配置设备策略时，可以在策略设置配置文件作用域中指定部署通道。



要删除通过用户通道部署的设备策略，请务必为“配置文件删除”策略选择部署范围为用户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

常规工作流程

通常，您向设备所有者提供预配置和受监督的共享 iPad。然后，这些人将设备分发给学生或员工。如果您没有分发预注册的共享 iPad：请务必向设备所有者提供他们的 Endpoint Management 服务器密码，以便他们可以注册自己的设备。

配置和注册共用的 iPad 的常规工作流程如下。

1. 使用 Endpoint Management 服务器控制台添加启用了 共享模式的 ASM 或 ABM 帐户（设置 **> Apple** 部署计划）。有关更多信息，请参阅接下来的“管理共享 iPad 的帐户”。
2. 如本部分内容中所述，请向 Endpoint Management 中添加所需的设备策略、应用程序和媒体。将这些资源分配给交付组。
3. 让设备所有者在共享 iPad 上执行硬重置。此时将显示面向注册的“远程管理”屏幕。
4. 设备所有者注册共享 iPad。
   Endpoint Management 将所配置的资源部署到每个已注册的共用的 iPad。自动重启后，设备所有者可以与用户共享设备。iPad 上将显示一个登录页面。
5. 设备用户输入他们的托管 Apple ID 和临时 ASM 密码。
   共享 iPad 会向 ASM 进行身份验证，并提示用户创建 ASM 密码。对于下次登录共享 iPad，设备用户将提供新的 ASM 密码。
6. 然后，共享 iPad 的另一个设备用户可以通过重复上一步进行登录。

管理共享 **iPad** 的账户

如果您已经在 Apple 教育或 Apple Business 中使用了 Endpoint Management：在 Endpoint Management 中为未共享的设备（例如设备所有者使用的设备）配置了现有的 ASM/ABM 帐户。对于共享设备和非共享设备，您可以使用相同的 ASM/ABM 帐户和同一 Endpoint Management 服务器。

将共用的 **iPad** 组织整理到设备组中

ASM/ABM 允许您通过创建多个 MDM 服务器将设备组织成组。将共享 iPad 分配给 MDM 服务器时，请为每组共享 iPad 创建一个设备组：

- 共用的 iPad 组 1 > 设备组 1 MDM 服务器
- 共用的 iPad 组 2 > 设备组 2 MDM 服务器
- 共用的 iPad 组 N > 设备组 N MDM 服务器

为每个设备组添加 **ASM** 帐户

当您从 Endpoint Management 服务器控制台创建多个 ASM/ABM 账户时，您会自动导入共享 iPad 组：

- 设备组 1 MDM 服务器 > 设备组 1 帐户
- 设备组 2 MDM 服务器 > 设备组 2 帐户
- 设备组 N MDM 服务器 > 设备组 N 帐户

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

共用的 iPad 的特定要求如下：

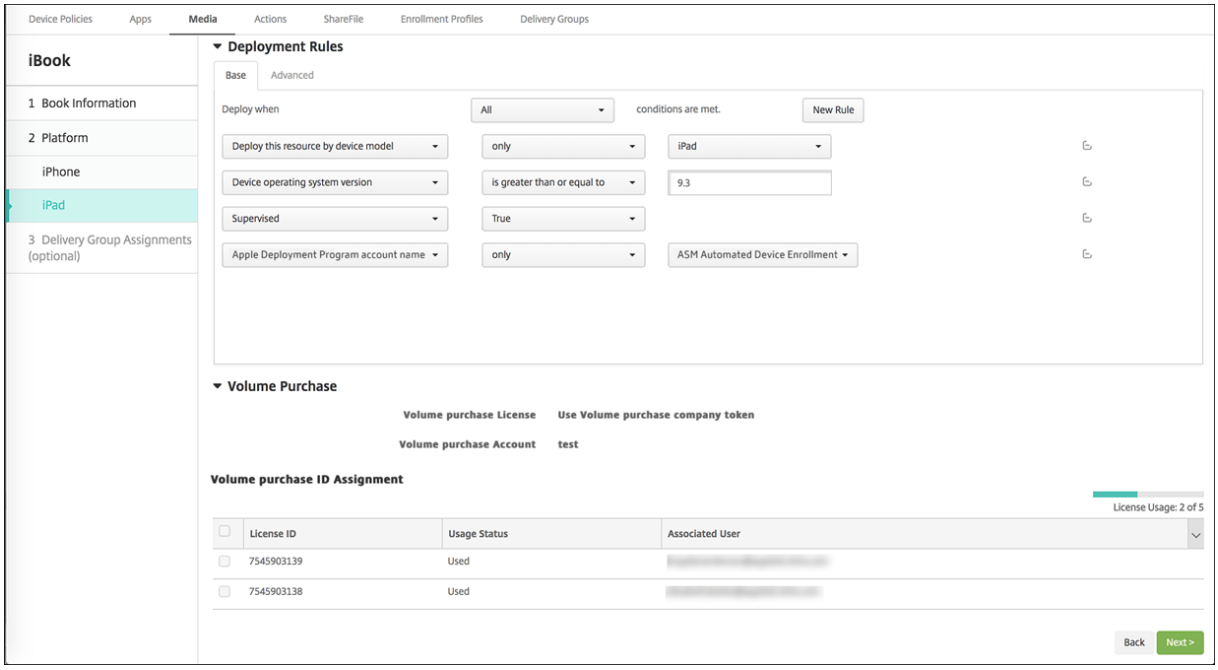
- 启用以下设置的每个设备组都有一个 ASM/ABM 账户：
  - 要求注册设备
  - 受监督模式
  - 共享模式
- 对于指定的教育机构，请务必为所有 ASM 帐户使用相同的教育后缀。

共用的 **iPad** 的应用程序

共用的 iPad 支持分配基于设备的批量购买应用程序。在共享 iPad 上部署应用之前，Endpoint Management 向 Apple 批量购买服务器发送请求，向设备分配批量购买许可证。要检查批量购买分配，请转至配置 **>** 应用程序 **> iPad** 并展开批量购买。

共用的 **iPad** 的媒体

共用的 iPad 支持分配基于用户的批量购买 iBook。在共享 iPad 上部署 iBooks 之前，Endpoint Management 向 Apple 批量购买服务器发送请求，向用户分配批量购买许可证。要检查批量购买分配，请转至配置 **>** 媒体 **> iPad** 并展开批量购买。



共用的 **iPad** 的部署规则

对于共享 iPad 部署，交付组级别的规则不适用，因为它们与用户属性相关。要为每个设备组过滤策略、应用程序和媒体，请执行以下操作：根据帐户名称为资源添加部署规则。例如：

- 对于设备组 1 帐户，请设置此部署规则：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```

- 对于设备组 2 帐户，请设置此部署规则：

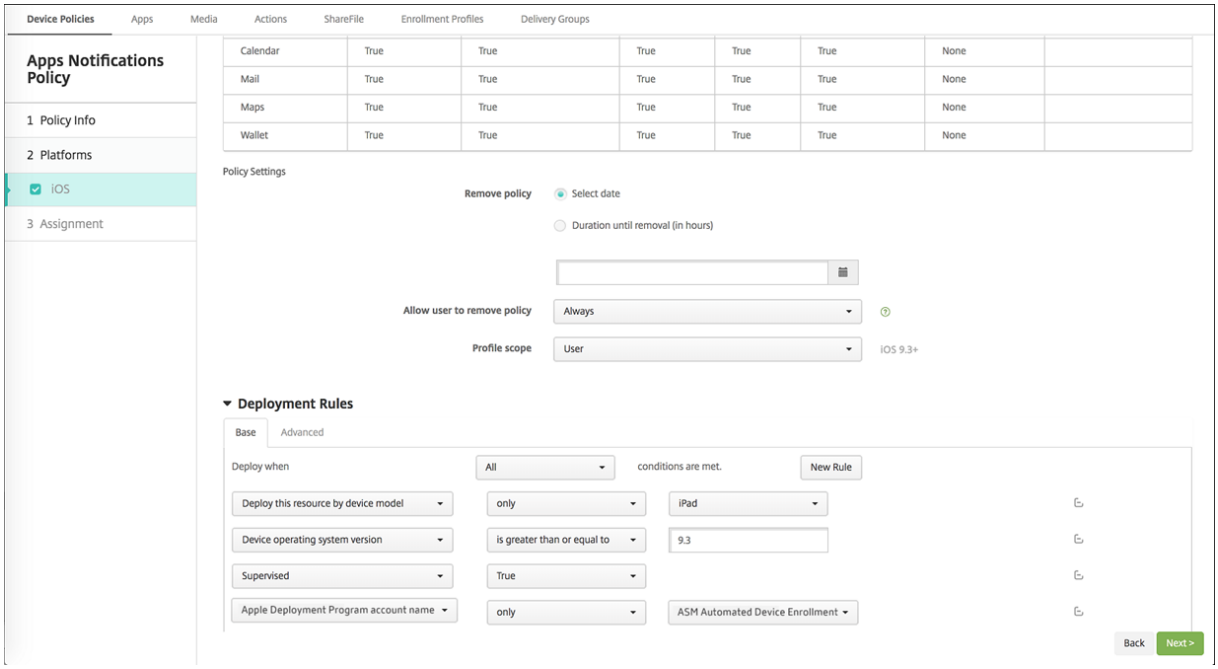
```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- 对于设备组 N 帐户，请设置此部署规则：

```
Apple Deployment Program account name
Only
Device Group N account

<!--NeedCopy-->
```



要仅向设备所有者部署 Apple 课堂应用程序（使用非共享的 iPad），请使用以下部署规则按 ASM 共享状态筛选资源：

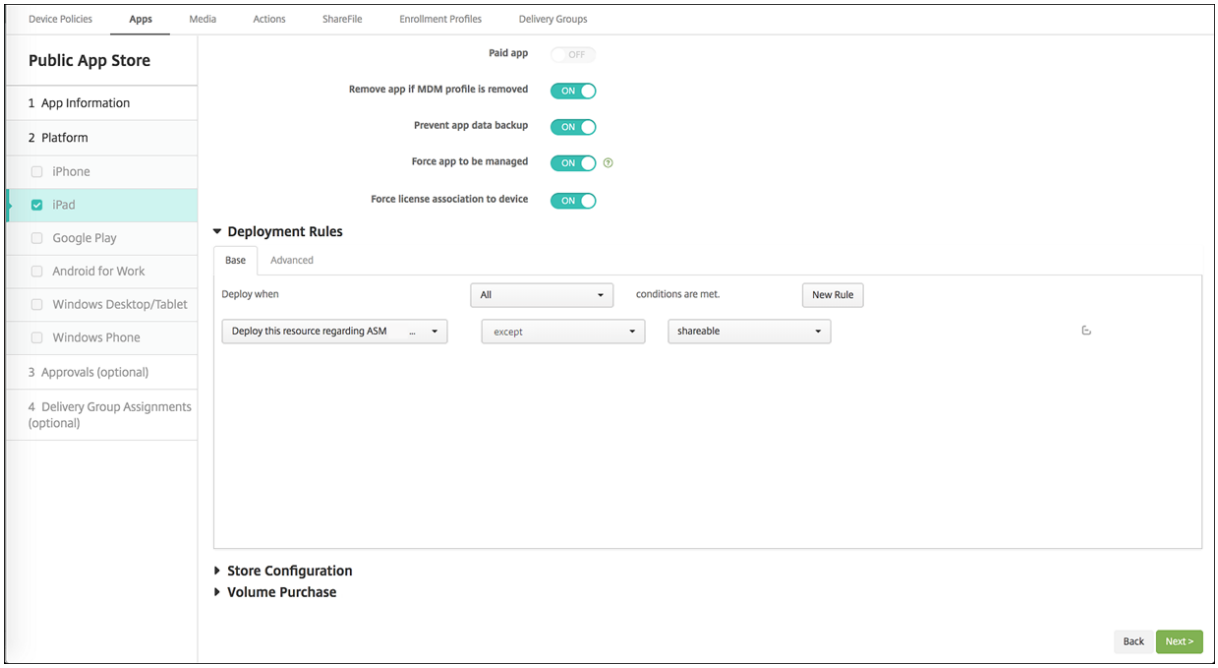
```
Deploy this resource regarding ASM/ABM shared mode
only
unshared
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
4
5  <!--NeedCopy-->
```

或：

```
1  Deploy this resource regarding ASM/ABM shared mode
2  except
3  shareable
4
5  <!--NeedCopy-->
```

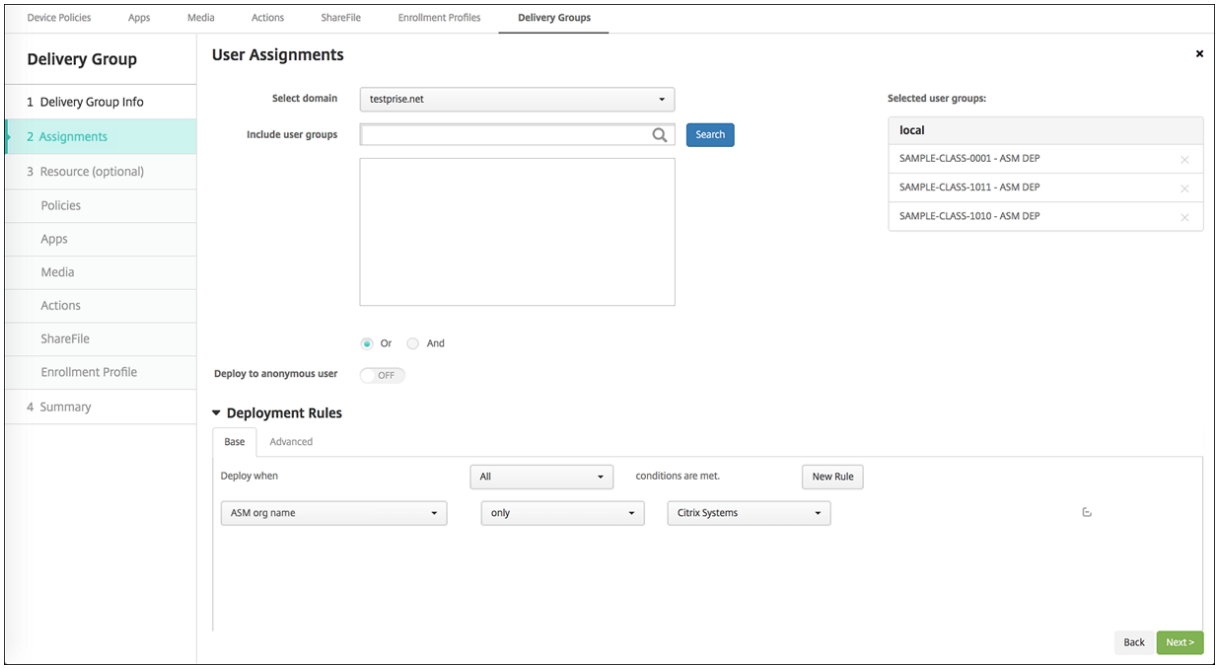


共用的 **iPad** 的交付组

对于设备组：

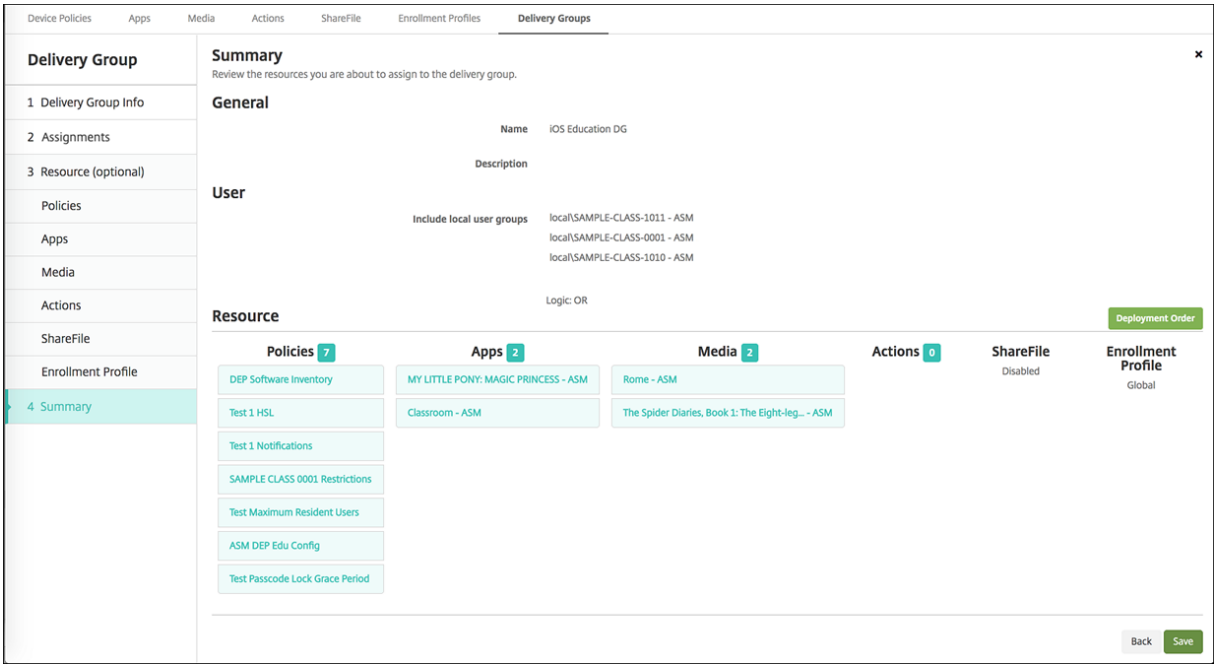
- 配置一个交付组。对于教师，请分配教育配置策略定义的所有课程。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 该交付组必须包括以下 MDM 资源：
  - 设备策略：
    - 教育配置（适用于 ASM）
    - 锁屏界面消息
    - 应用程序通知
    - 主屏幕布局
    - 限制
    - 最大常驻用户数
    - 通行码锁宽限期
  - 必需的批量购买应用程序
  - 必须的批量购买 iBooks

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

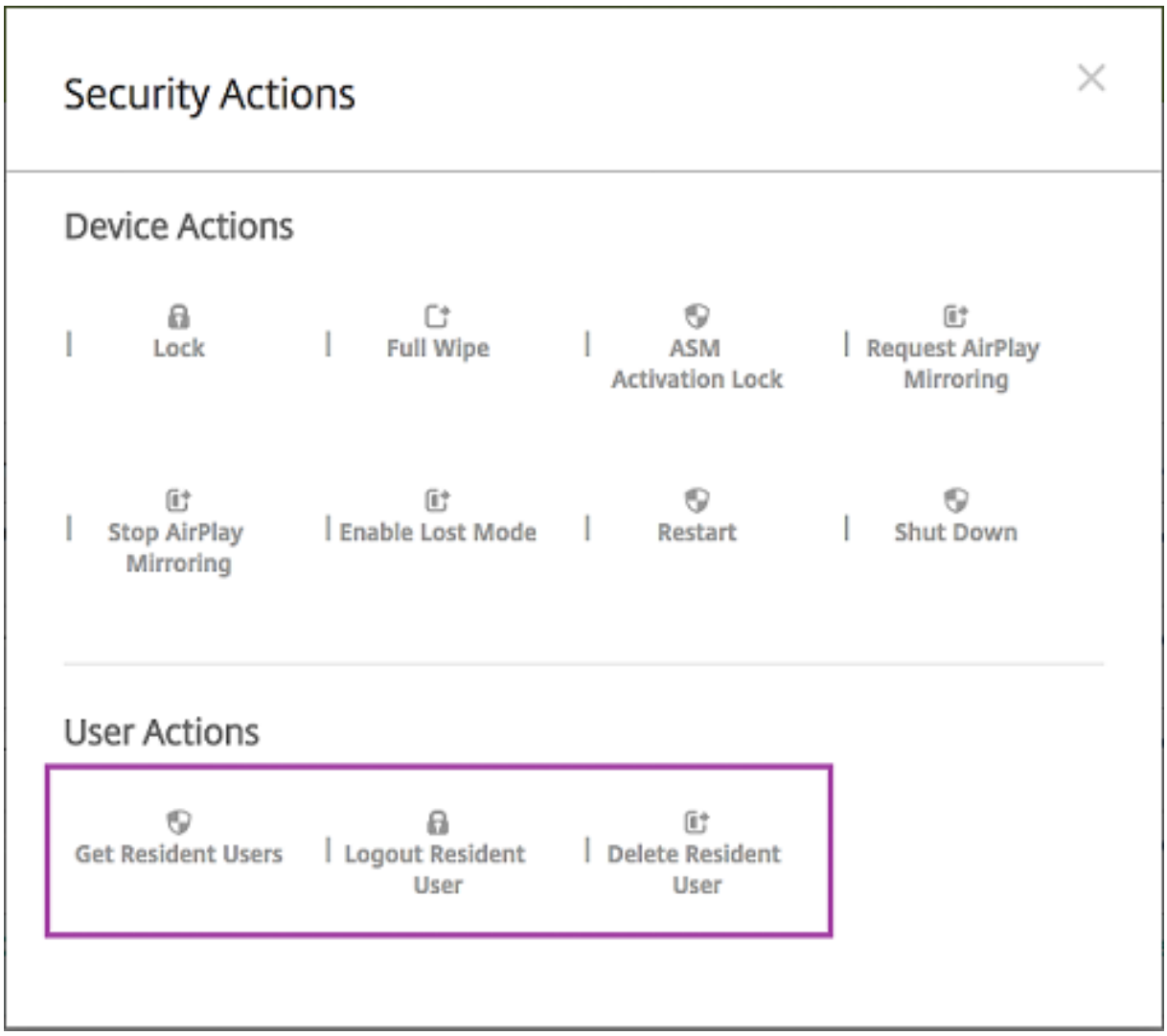


共用的 **iPad** 的安全操作

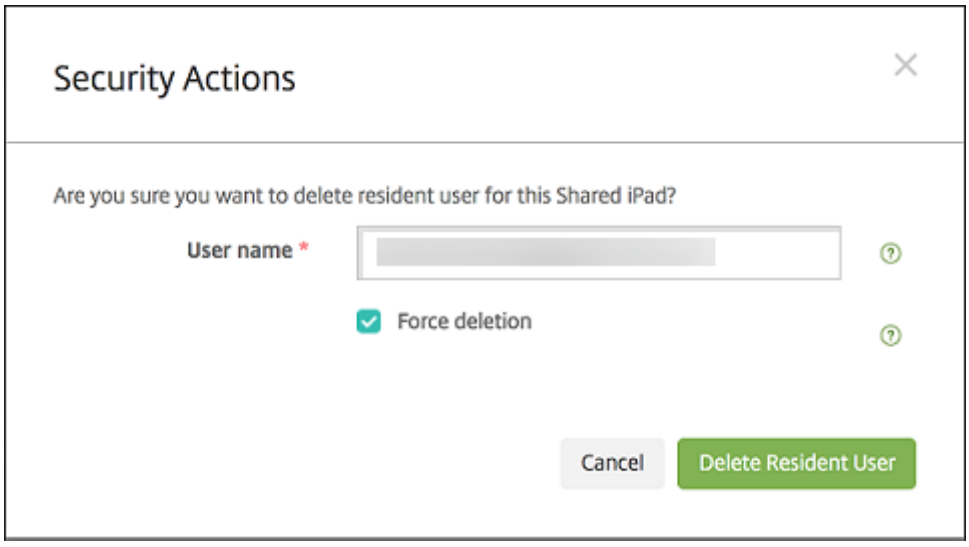
除现有安全操作外，可以对共用的 iPad 使用以下安全操作：

- 获取常驻用户：列出在当前设备上具有活动帐户的用户。此操作将强制在设备与 Endpoint Management 控制台之间进行同步。
- 注销常驻用户：强制注销当前用户。
- 删除常驻用户：删除特定用户的当前会话。该用户可以重新登录。
- 删除所有用户：删除设备上的所有用户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



单击删除常驻用户后，可以指定用户名。



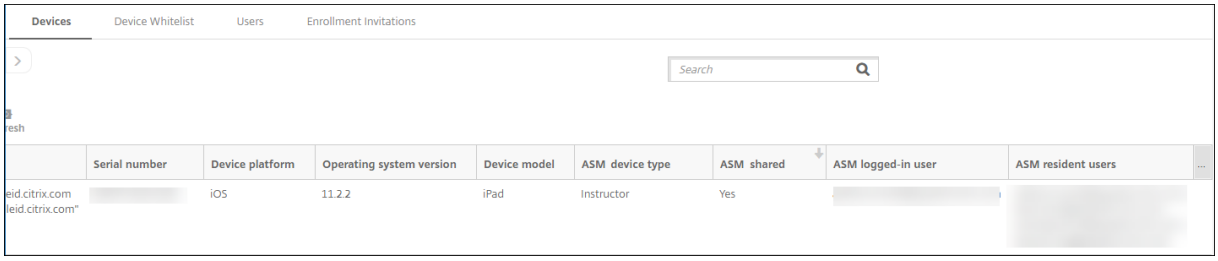
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

安全操作的结果在管理 > 设备 > 常规和管理 > 设备 > 交付组页面上显示。

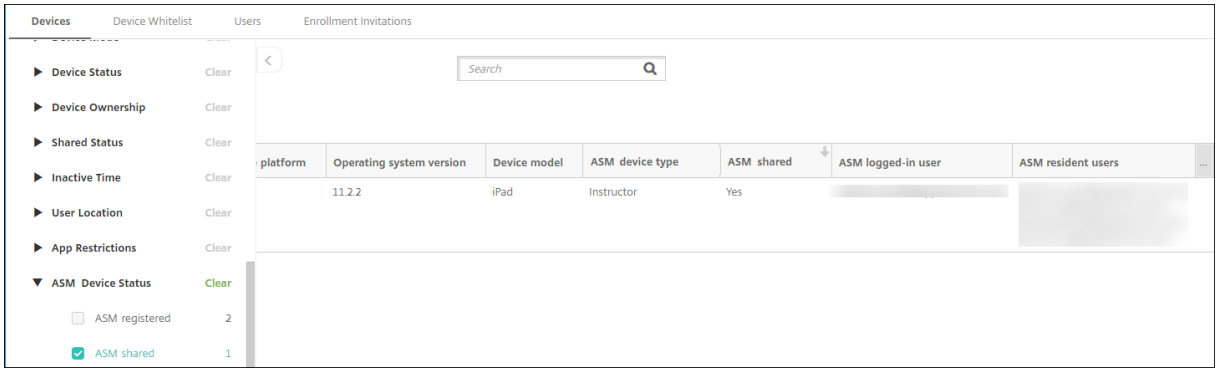
获取与共用的 **iPad** 有关的信息

请在管理 > 设备页面上查找共用的 iPad 特有的信息：

- 请查找：
  - 设备是否共享（**ASM/ABM** 共享）
  - 谁登录到共享设备（**ASM/ABM** 已登录用户）
  - 分配给共享设备的所有用户（**ASM/ABM** 常驻用户）

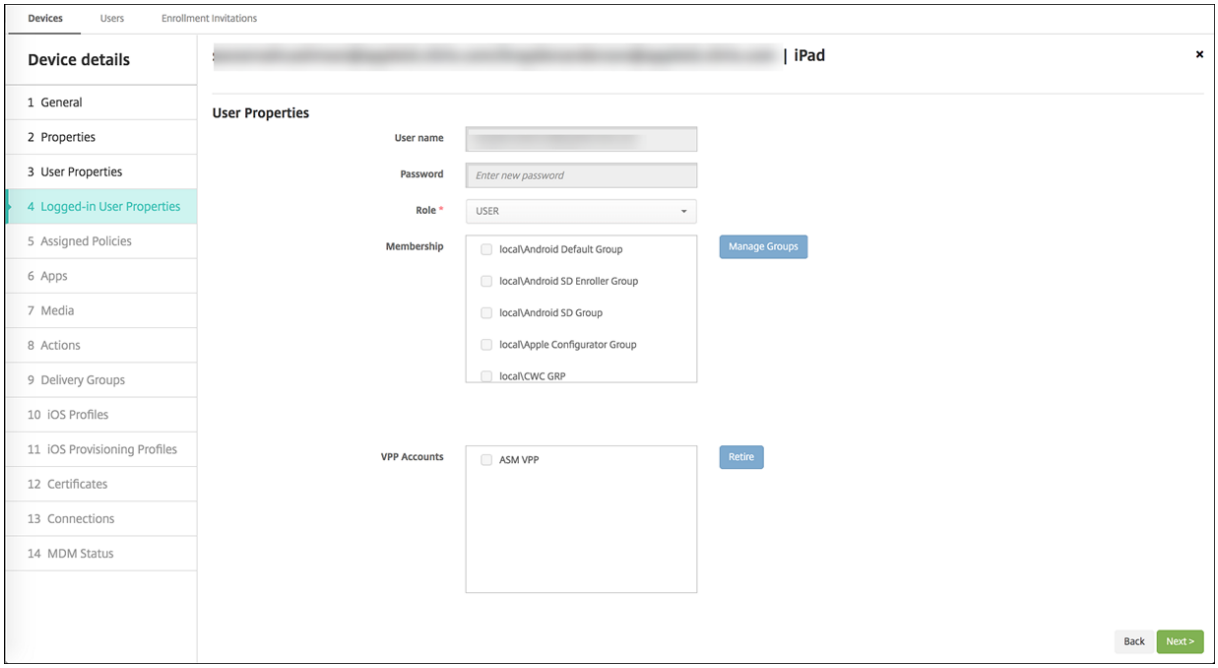


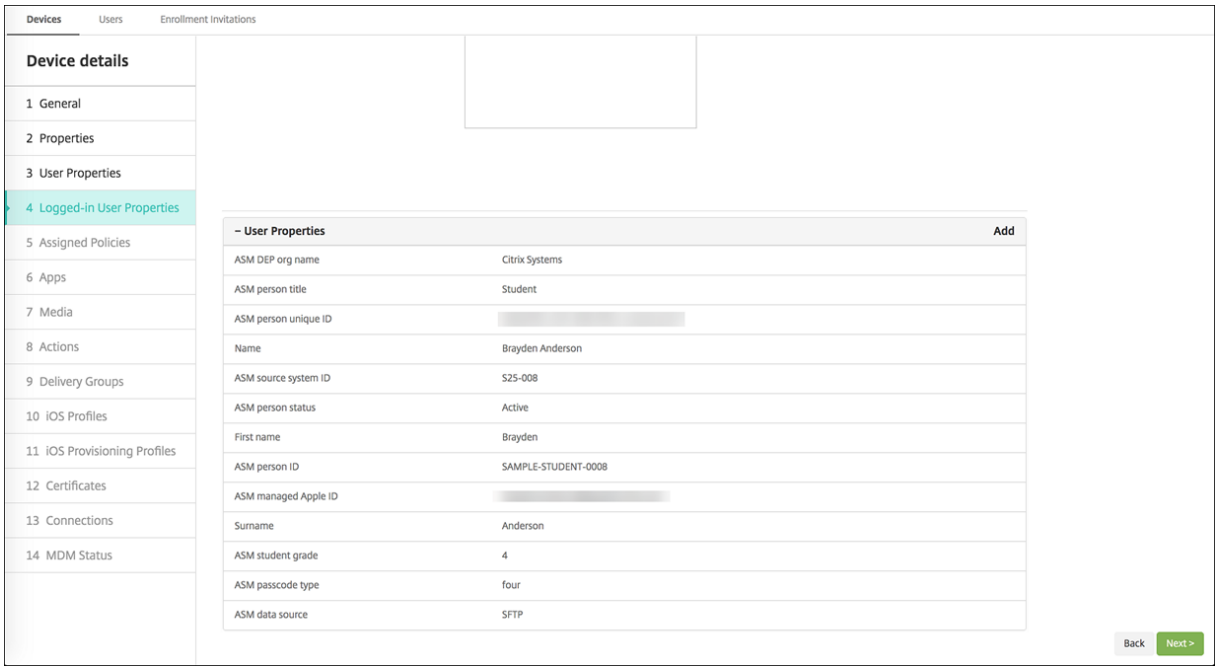
- 按 **ASM/ABM** 设备状态筛选设备列表：



- 在管理 > 设备 > 已登录用户的属性页面上查看与登录到共用的 iPad 的用户有关的详细信息。

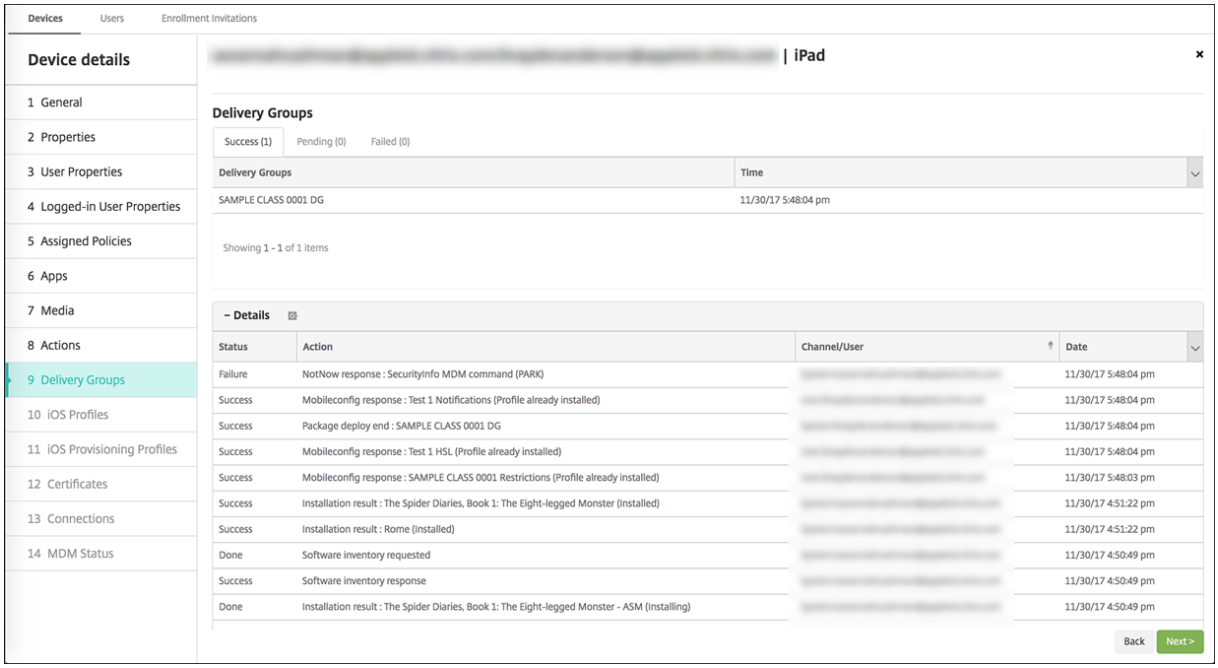
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



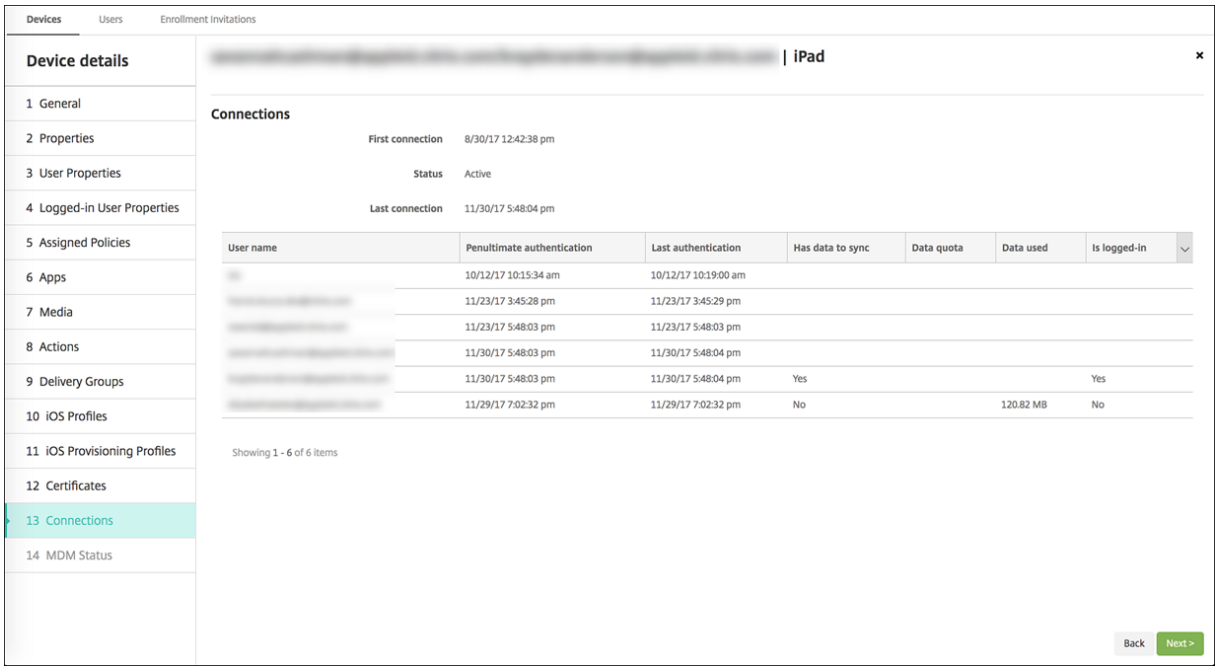


- 在 管理 **>** 设备 **>** 交付组页面上，查看用于向交付组中的设备所有者和用户部署资源的渠道。渠道/用户列显示类型（系统或 用户）和收件人。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

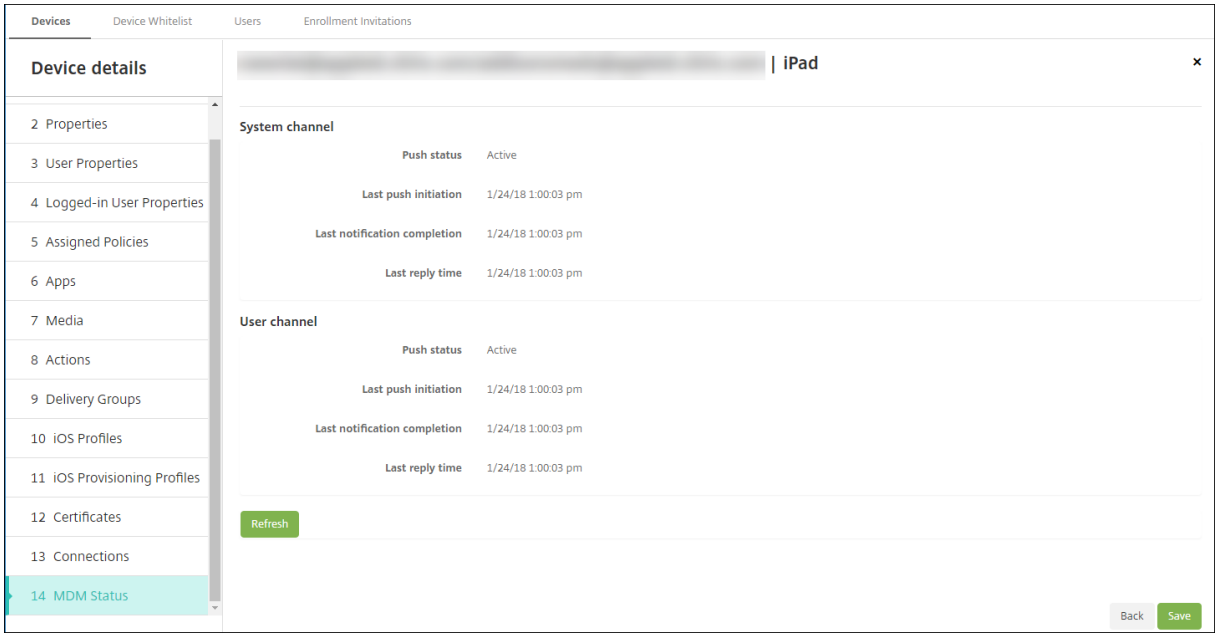


- 获取与常驻用户有关的信息：
  - 有要同步的数据：用户是否具有要同步到云的数据。
  - 数据配额：为用户设置的数据配额，单位为字节。如果用户配额暂时关闭或不强制对用户实施，配额可能不会显示。
  - 已使用的数据：用户使用的数据量，单位为字节。如果系统收集信息过程中出现错误，值可能不会显示。
  - 已登录：用户是否已登录设备。



- 查看两个通道的推送状态。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



分发 **Apple** 应用程序

November 26, 2021

Endpoint Management 管理部署到设备的应用程序。您可以组织和部署以下类型的 iOS/iPadOS 和 macOS 应用程序。

- 公共应用商店 **(**仅限 **iOS/iPadOS)**：这些应用程序包括公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。例如，GoToMeeting。
- 企业 **(iOS/iPadOS/macOS)**：未启用 MDX 且不包含与 MDX 应用程序关联的策略的本机应用程序。
- **MDX (**仅限 **iOS/iPadOS)**：使用 MAM SDK 准备的应用程序或使用 MDX Toolkit 封装的应用程序。这些应用程序包括 MDX 策略。您可以从内部来源和公共应用商店获取 MDX 应用程序。
- 批量购买 **(iOS/iPadOS/macOS)**：具有通过 Apple 批量购买计划管理的许可证的应用程序。
- **iOS** 自定义应用程序 **(**仅限 **iOS/iPadOS)**：在内部或第三方开发的专有企业对企业应用程序。

有关不同类型的应用程序的详细信息，请参阅添加应用程序。

某些部署需要 Apple 商务管理 (ABM) 或 Apple 校园教务管理 (ASM) 帐户。有关详细信息，请参阅以下部分。

对于每种类型的应用程序和分发方法，Citrix 建议采用一组配置实践。有关为其他平台分发应用程序的信息，请参阅添加应用程序。以下各部分内容提供了有关 iOS 应用程序配置的详细信息。

应用程序分发的一般步骤

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

场景	步骤 1：链接帐户	步骤 2：添加和配置应用程序	步骤 3：配置交付组并部署应用程序
公共应用商店应用程序，包括 Citrix 移动应用程序	不适用	在 **Endpoint Management** 中：在配置 **>** 应用程序中，添加适用于 iPhone 或 iPad 的公共应用商店应用程序。配置应用程序并将其分配给交付组。	在 **Endpoint Management** 中：使用交付组配置和部署应用程序。
通过 Apple 批量购买提供的公共应用商店应用程序，包括 Citrix 移动应用程序	在 Apple 部署计划中注册在 **Endpoint Management** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 或 **ASM** 中：从“应用程序”和“书籍”购买和添加应用程序。在 **Endpoint Management** 中：转到配置 **>** 应用程序，配置应用程序，然后将其分配给交付组。	在 **Endpoint Management** 中：使用交付组配置和部署应用程序。
企业应用程序	不适用	在 **Endpoint Management** 中：转到配置 **>** 应用程序。单击添加，然后单击企业。上载 IPA 文件。配置应用程序并将其分配给交付组。	在 **Endpoint Management** 中：使用交付组配置和部署应用程序。
MDX 应用程序	不适用	在 **Endpoint Management** 中：转到配置 **>** 应用程序。单击添加，然后单击 **MDX**。确保您为平台选择了 **iPad**/**iPhone**。上载 MDX 文件。配置应用程序并将其分配给交付组。	在 **Endpoint Management** 中：使用交付组配置和部署应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

场景	步骤 1：链接帐户	步骤 2：添加和配置应用程序	步骤 3：配置交付组并部署应用程序
使用 Apple 批量购买分发的 MDX 应用程序	在 Apple 部署计划中注册在 **Endpoint Management** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 中：从“应用程序”和“书籍”购买和添加 MDX 应用程序。将应用程序链接到您的 ABM 帐户。在 **Endpoint Management** 中：转到配置 **>** 应用程序，配置应用程序，然后将其分配给交付组。	在 **Endpoint Management** 中：使用交付组配置和部署应用程序。
自定义应用程序	在 Apple 部署计划中注册在 **Endpoint Management** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 中：将您的应用程序作为私人应用程序添加到应用商店中。请将应用程序链接到您的 ABM 帐户。在 **Endpoint Management** 中：转到配置 **>** 应用程序，配置应用程序，然后将其分配给交付组。	在 **Endpoint Management** 中：使用交付组配置和部署应用程序。
启用了 MDX 的自定义应用程序	在 Apple 部署计划中注册在 **Endpoint Management** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 中：将您的应用程序作为私人应用程序添加到应用商店中。请将应用程序链接到您的 ABM 帐户。在 **Endpoint Management** 中：转到配置 **>** 应用程序并上载 MDX 文件。配置应用程序并将其分配给交付组。	在 **Endpoint Management** 中：使用交付组配置和部署应用程序。

公共应用商店应用程序

可以将 App Store 中提供的免费和付费应用程序添加到 Citrix Endpoint Management 中。

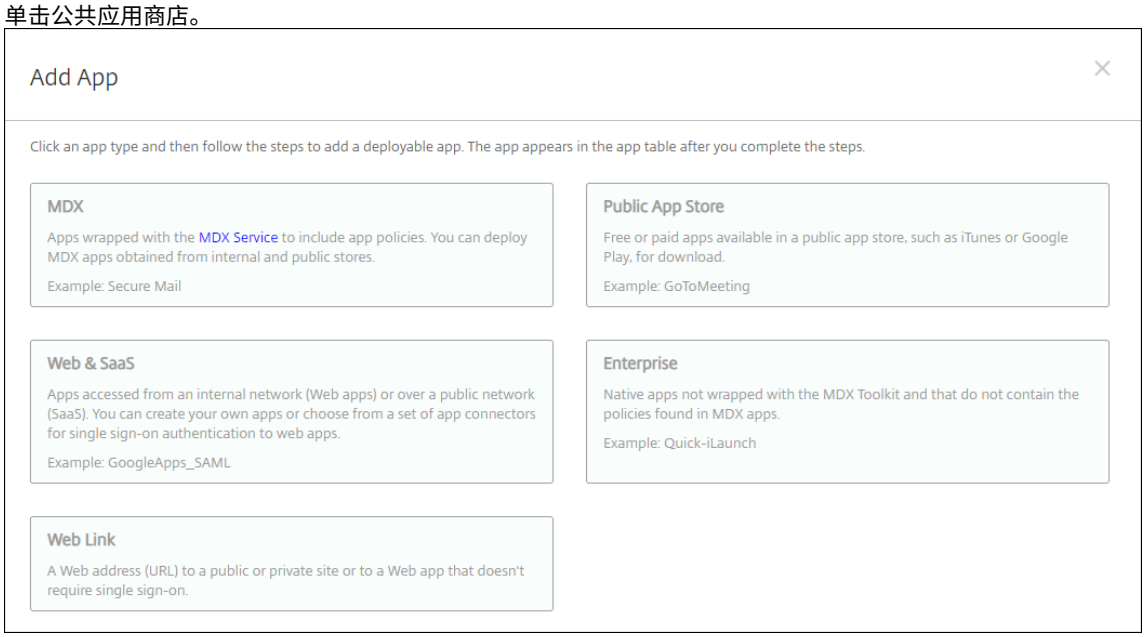
功能可用性	
需要监督设备	否
适用于用户注册模式	否

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

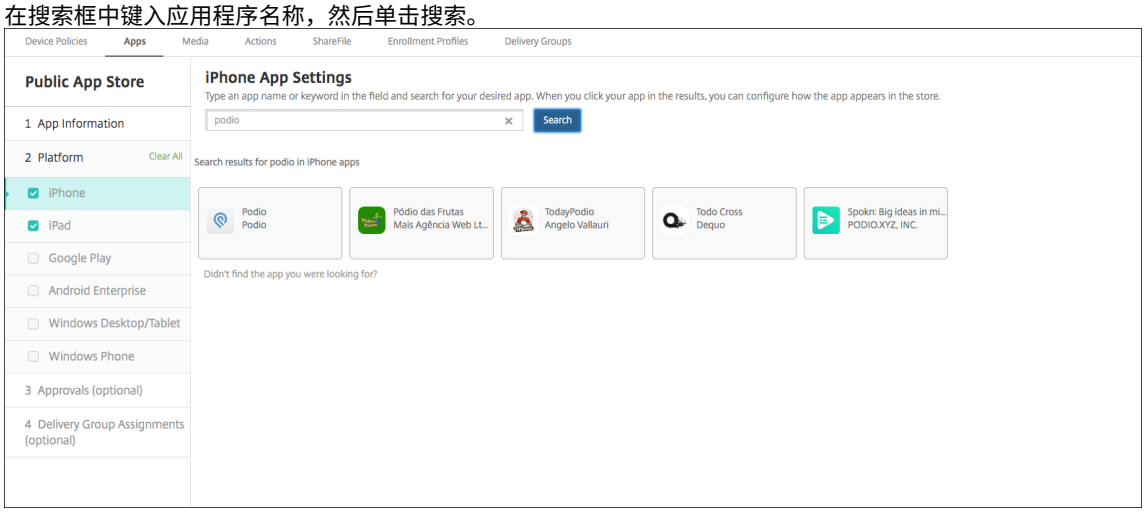
功能可用性	
有效日期	iOS/iPadOS

步骤 **1**：添加和配置应用程序

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击公共应用商店。



3. 为平台选择 **iPhone** 或 **iPad**
4. 在搜索框中键入应用程序名称，然后单击搜索。

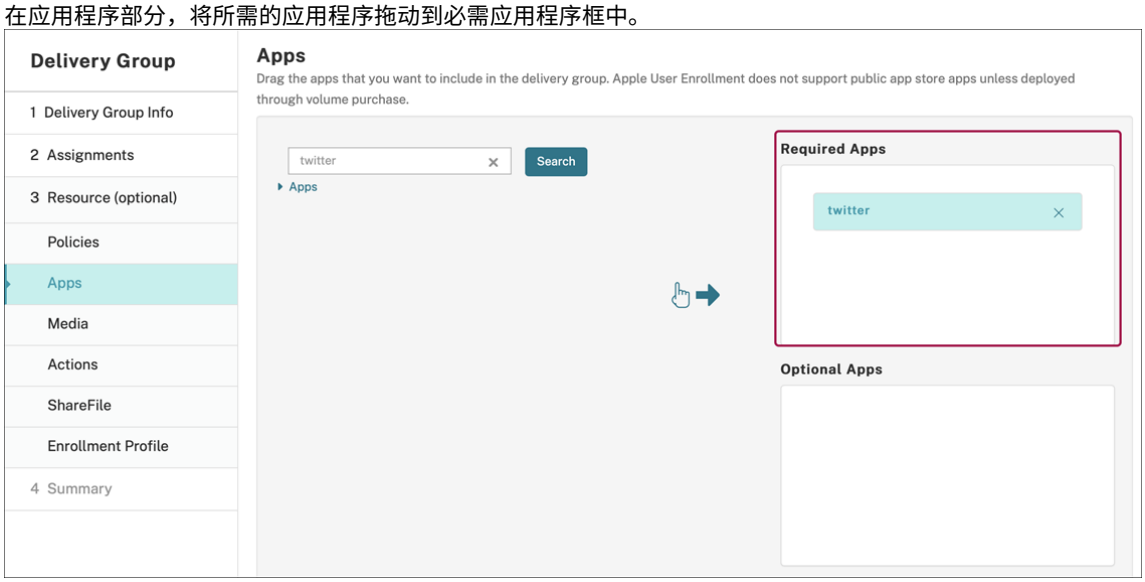


5. 此时将显示符合搜索条件的应用程序。单击所需的应用程序。
6. 将交付组分配给应用程序，然后单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

步骤 **2**：配置应用程序部署

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。
2. 选择要配置的应用程序，然后单击编辑。
3. Citrix 建议启用强制管理应用程序功能。
4. 分配任何交付组，然后单击保存。
5. 导航到配置 **>** 交付组，然后单击添加。
6. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



7. 导航回配置 **>** 交付组。
8. 选择交付组并单击部署。
9. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



通过 **Apple** 批量购买提供的公共应用商店应用程序

可以通过 Apple 批量购买计划管理 iOS/iPadOS 应用程序许可证。请按照以下步骤将批量购买应用程序添加到 Endpoint Management。

功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS/macOS

步骤 **1**：链接帐户

1. 设置 Apple 商务管理 (ABM) 或 Apple 校园教务管理 (ASM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 Endpoint Management 链接起来。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用程序会自动更新。如果应用程序启用了强制管理应用程序设置，则会更新而不提示用户。无论应用程序是必需应用程序还是可选应用程序，都会更新。

要使用强制管理应用程序和应用程序自动更新设置，请启用 `apple.app.force.managed` 服务器属性。请参阅服务器属性。

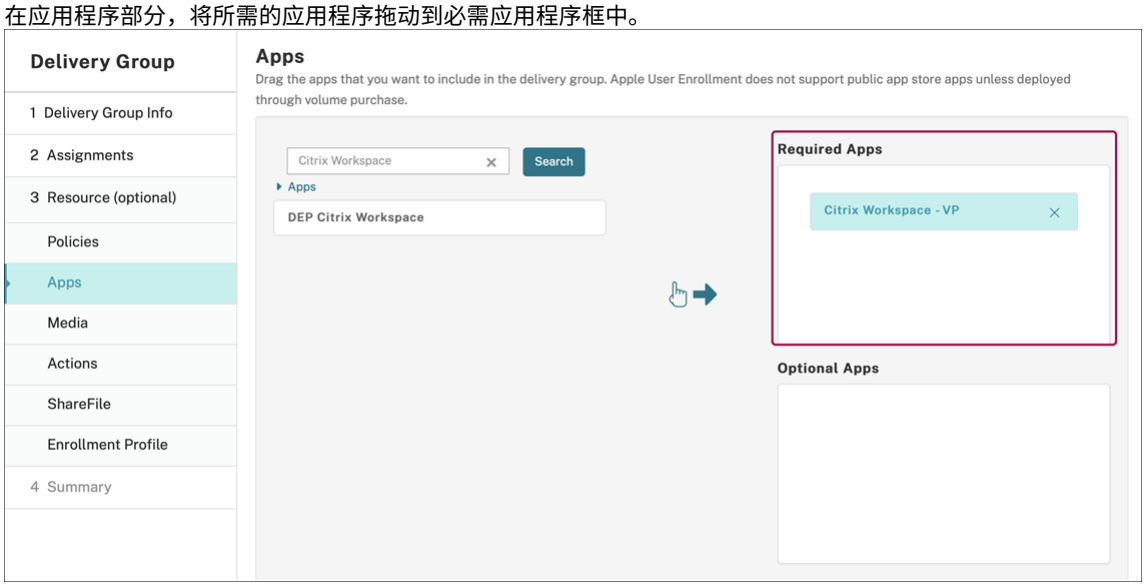
步骤 **2**：从 **Apple** 获取应用程序和许可证

在 ABM/ASM 帐户中购买应用程序。可以在 Apple 书籍（仅适用于 iOS/iPadOS）和 Apple App Store 中进行购买。请记住，您必须购买所有应用程序，即使它们是免费的亦如此。在 ABM/ASM 上购买许可证后，Endpoint Management 将自动显示该应用程序。

有关如何使应用程序可供您的企业使用的信息，请参阅 Apple 文档。

步骤 **3**：配置应用程序部署

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。
2. 选择要配置的批量购买应用程序，然后单击编辑。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. Citrix 建议启用强制管理应用程序功能（仅限 iOS/iPadOS）。
5. 分配任何交付组，然后单击保存。
6. 导航到配置 **>** 交付组，然后单击添加。
7. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



8. 导航回配置 **>** 交付组。
9. 选择交付组并单击部署。
10. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



企业应用程序

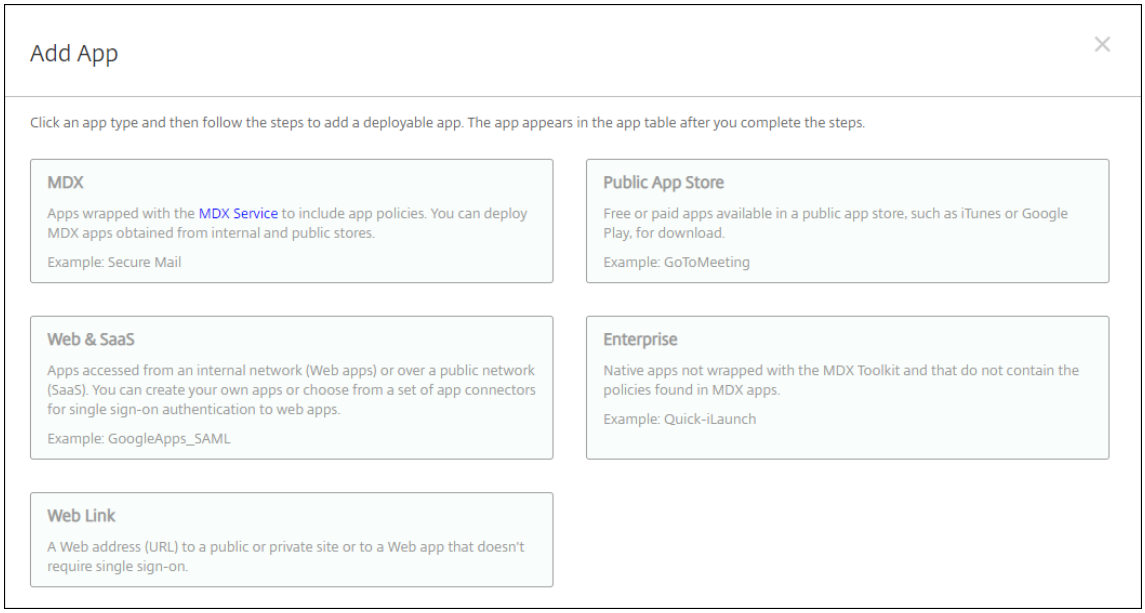
还可以添加没有关联任何 MDX 策略的本机应用程序。请按照以下步骤添加 App Store 上不存在的应用程序。

功能可用性	
需要监督设备	否
适用于用户注册模式	是
操作系统	iOS/iPadOS/macOS

步骤 **1**：添加和配置应用程序

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击企业。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 在应用程序信息页面上，配置以下设置：

   - 名称：键入应用程序的描述性名称。该名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中，单击要将应用程序添加到的类别。

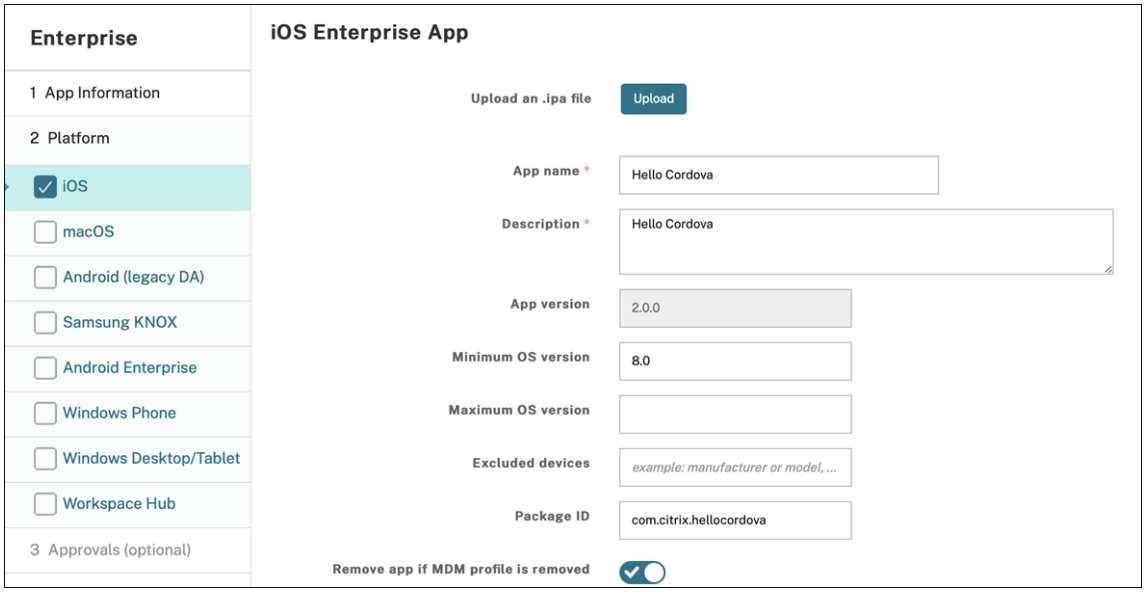
4. 单击下一步。此时将显示应用程序平台页面。
5. 选择平台：**iPhone**、**iPad** 或 **macOS**。
6. 上载 IPA 文件 (iOS/iPadOS) 或上载 PKG 文件 (macOS)
7. 单击下一步。此时将显示应用程序详细信息页面。
8. 配置以下设置：

   - 文件名：（可选）键入应用程序的新名称。
   - 应用程序说明：（可选）键入应用程序的新说明。
   - 应用程序版本：无法更改此字段。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
   - 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否从设备中删除应用程序。默认值为“开”。（仅限 iOS/iPadOS）
   - 阻止备份应用程序数据：选择是否阻止应用程序备份数据。默认值为“开”。（仅限 iOS/iPadOS）
   - 强制管理应用程序：安装非托管应用程序时，如果希望不受监督设备上的用户看到允许管理应用程序的提示，请选择开。如果用户接受提示，则将托管应用程序。如果应用程序启用了强制管理应用程序设置，则会更新而不提示用户。无论应用程序是必需应用程序还是可选应用程序，都会更新。（仅限 iOS/iPadOS）

要使用强制管理应用程序和应用程序自动更新设置，请启用 `apple.app.force.managed` 服务器属性。请

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

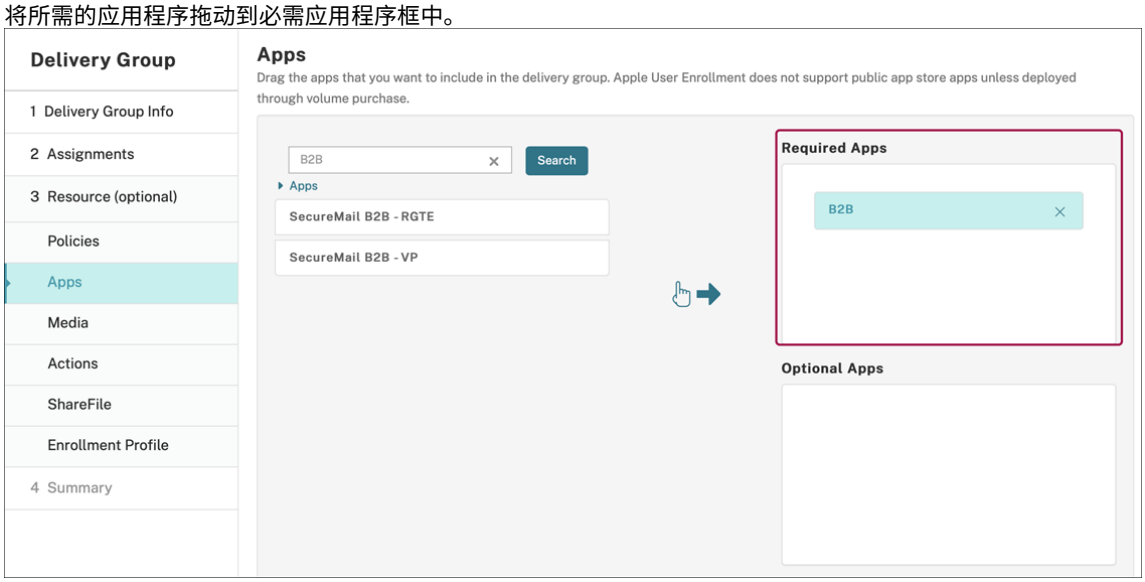
参阅服务器属性。



9. 将交付组分配给应用程序，然后单击保存。

步骤 **2**：配置应用程序部署

1. 在 Endpoint Management 控制台中，导航到配置 **>** 交付组。选择要配置的交付组，然后单击应用程序页面。
2. 将所需的应用程序拖动到必需应用程序框中。



3. 导航到配置 **>** 交付组。
4. 选择交付组并单击部署。
5. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



MDX 应用程序

要使用 MDX 策略和安全功能，请添加启用了 MAM SDK 或 MDX 封装的应用程序。可以使用批量购买或不使用批量购买来部署 MDX 应用程序。

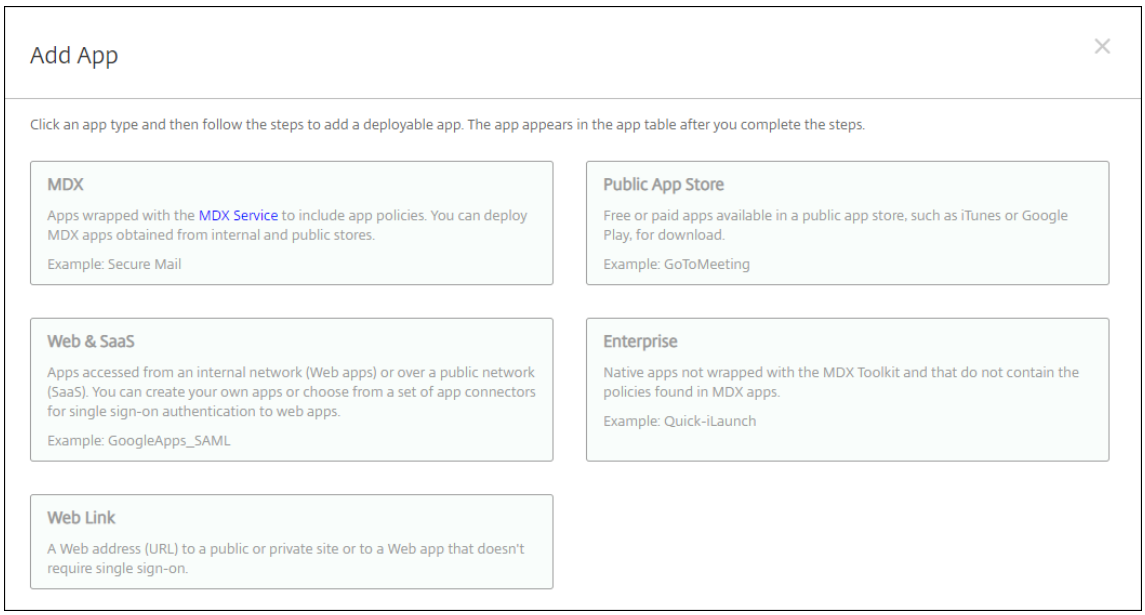
功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

要添加公共应用商店应用程序的 MDX 版本，请按照公共应用商店应用程序下的步骤进行操作，然后按照本部分中的步骤进行操作。

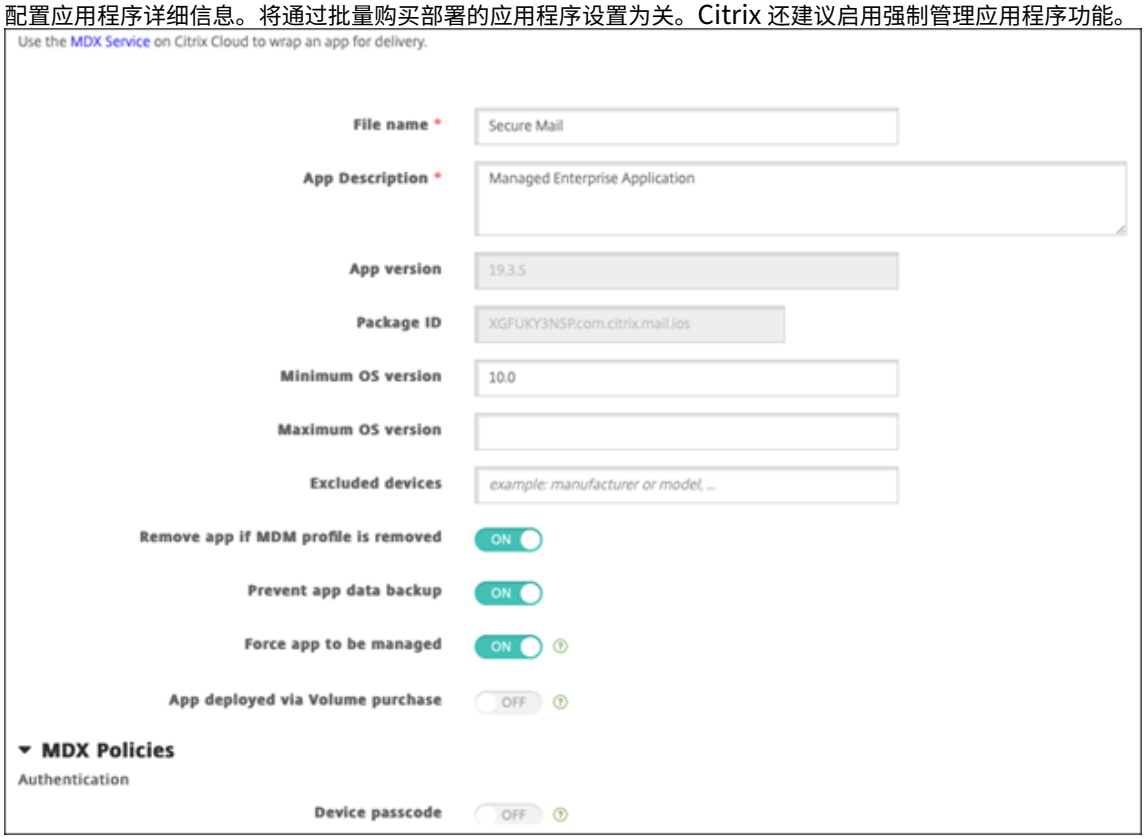
步骤 **1**：添加和配置应用程序

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击 **MDX**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

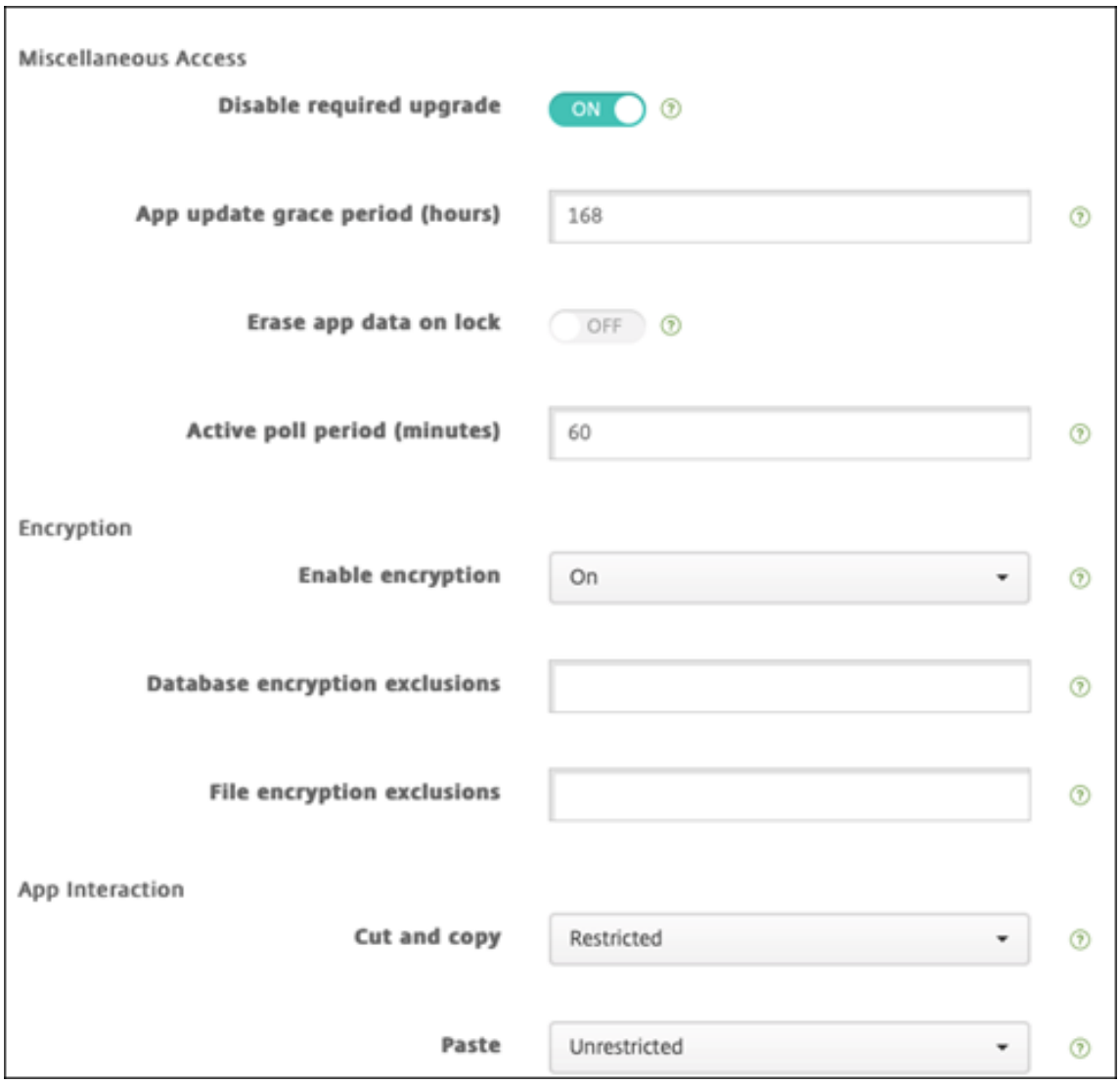


3. 为平台选择 **iPhone** 或 **iPad**。
4. 上载 MDX 文件。
5. 配置应用程序详细信息。将通过批量购买部署的应用程序设置为关。Citrix 还建议启用强制管理应用程序功能。



6. 配置 MDX 策略。将禁用所需的升级设置为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

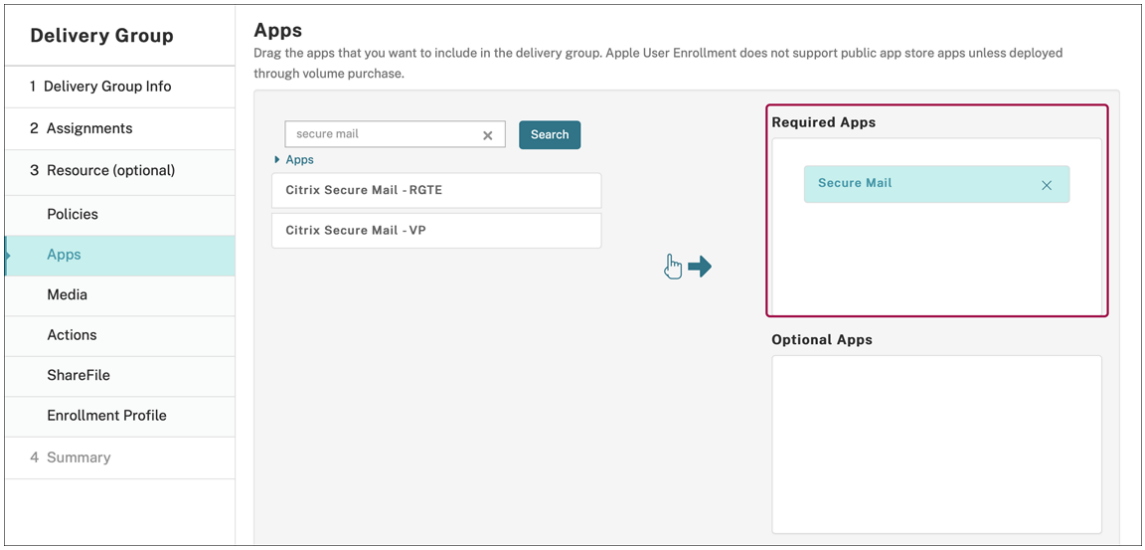


7. 将交付组分配给应用程序，然后单击保存。

步骤 **2**：配置应用程序部署

1. 在 Endpoint Management 控制台中，导航到配置 **>** 交付组，然后单击添加。
2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 导航到配置 **>** 交付组。
4. 选择交付组并单击部署。
5. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。



使用 **Apple** 批量购买分发的 **MDX** 应用程序

要使用 MDX 策略和安全功能，请添加启用了 MAM SDK 或 MDX 封装的应用程序。要使用批量购买部署应用程序，这些应用程序必须存在于应用商店中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

步骤 **1**：链接帐户

1. 设置 Apple 商务管理 (ABM) 或 Apple 校园教务管理 (ASM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 Endpoint Management 链接起来。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应用程序会自动更新。如果应用程序启用了强制管理应用程序设置，则会更新而不提示用户。无论应用程序是必需应用程序还是可选应用程序，都会更新。

   要使用强制管理应用程序和应用程序自动更新设置，请启用 `apple.app.force.managed` 服务器属性。请参阅服务器属性。

步骤 **2**：从 **Apple** 获取应用程序和许可证

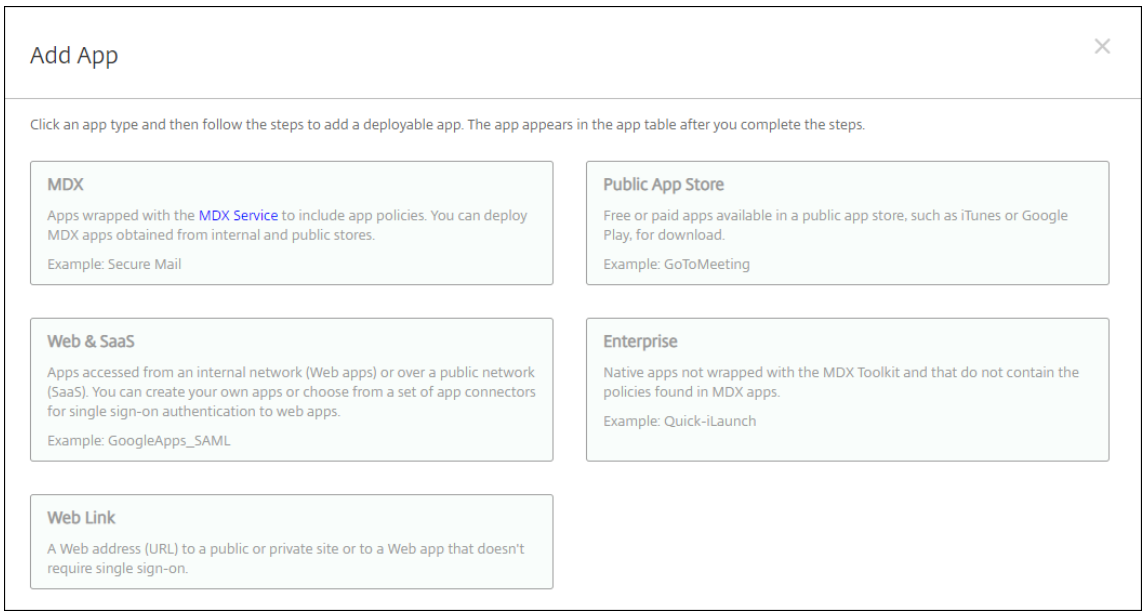
在 ABM/ASM 帐户中购买应用程序。可以在 Apple 书籍（仅适用于 iOS/iPadOS）和 Apple App Store 中进行购买。请记住，您必须购买所有应用程序，即使它们是免费的亦如此。在 ABM/ASM 上购买许可证后，Endpoint Management 将自动显示该应用程序。

有关如何使应用程序可供您的企业使用的信息，请参阅 Apple 文档。

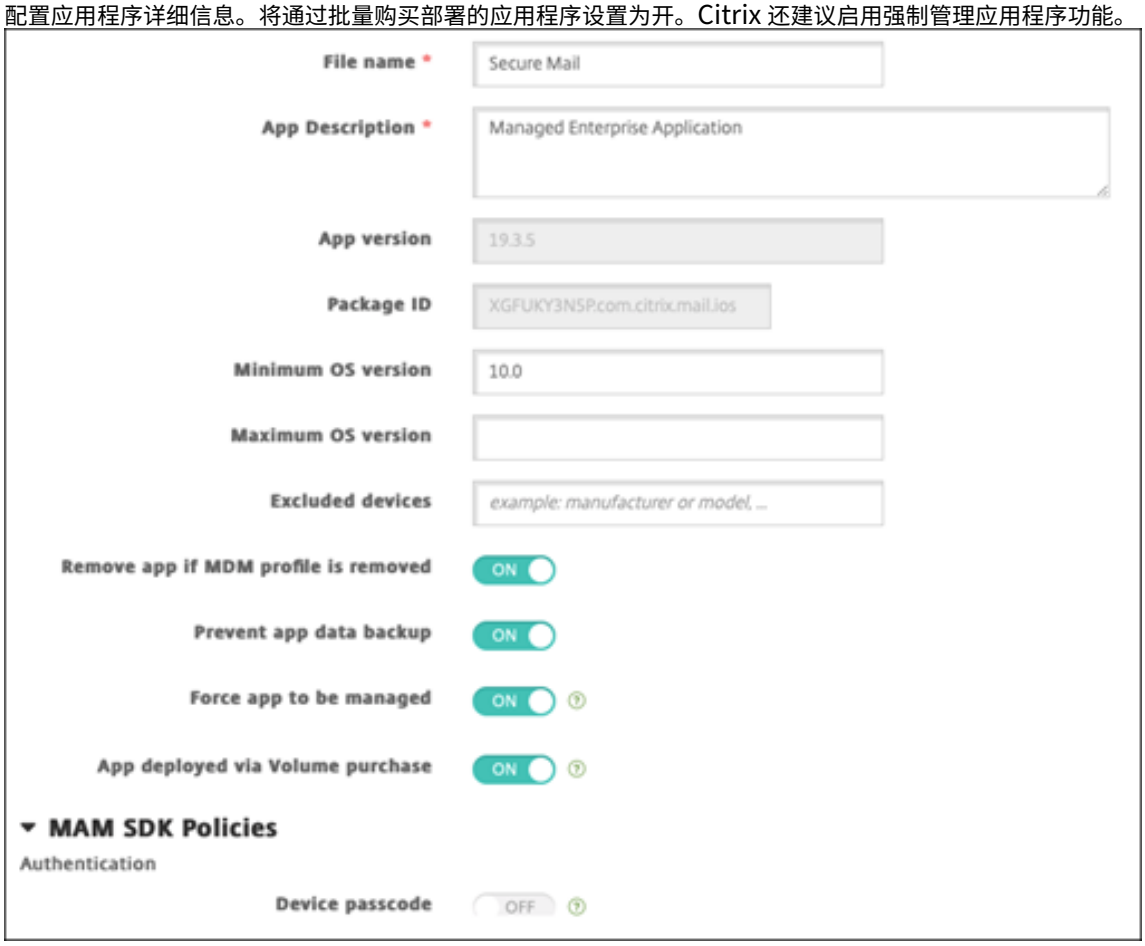
步骤 **3**：添加和配置应用程序

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击 **MDX**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

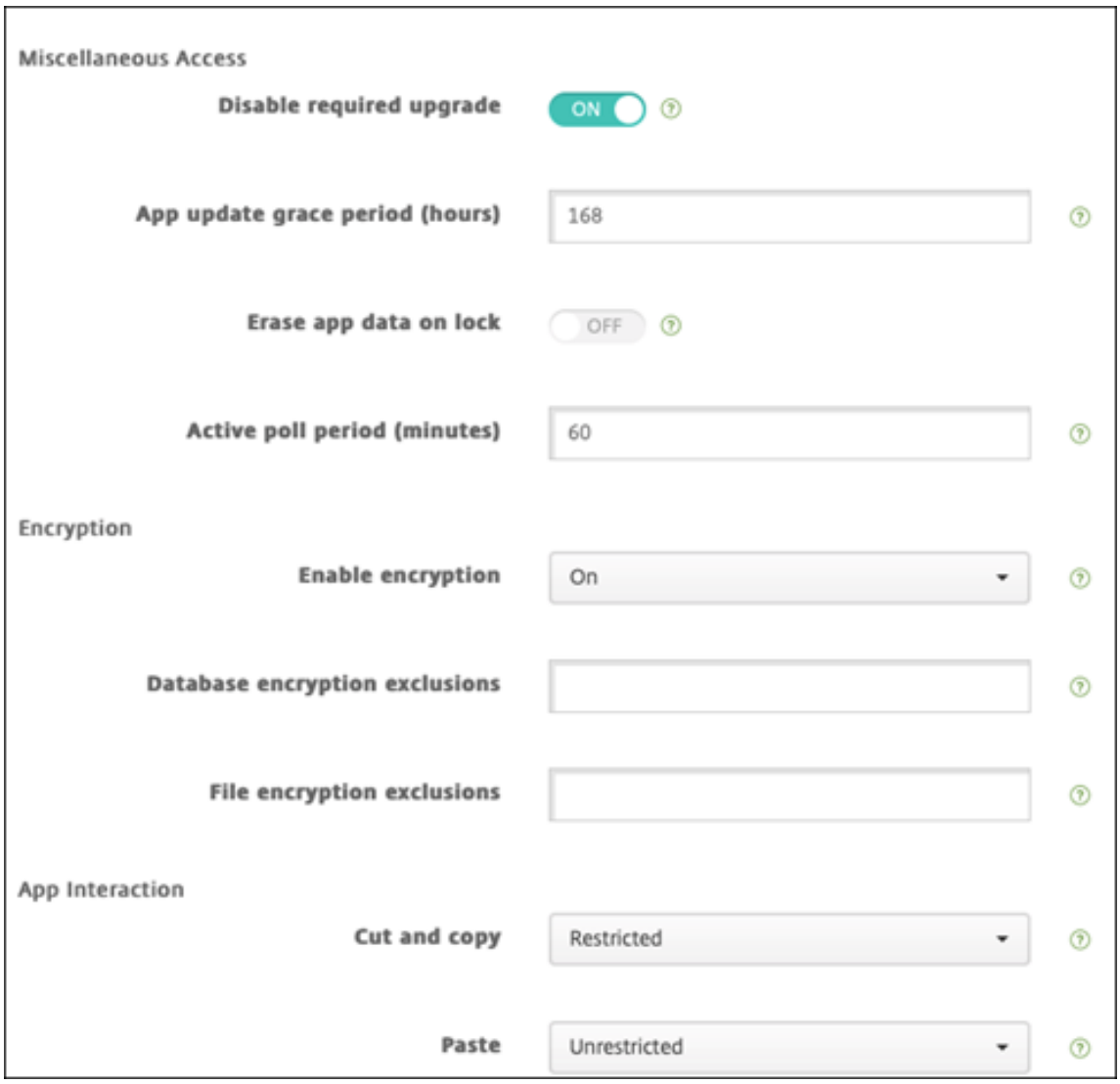


3. 为平台选择 **iPhone** 或 **iPad**。
4. 上载 MDX 文件。
5. 配置应用程序详细信息。将通过批量购买部署的应用程序设置为开。Citrix 还建议启用强制管理应用程序功能。



6. 配置 MDX 策略。将禁用所需的升级设置为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



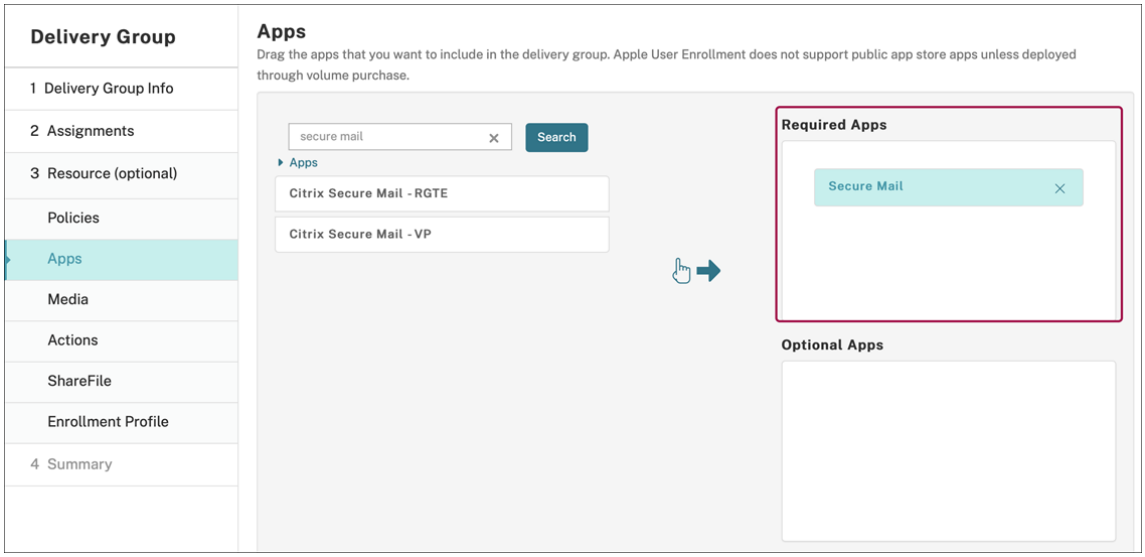
7. 将交付组分配给每个平台的应用程序，然后单击保存。

此配置将导致在应用程序列表中为此应用程序列出两个条目。选择要配置的应用程序时，请选择类型为 **MDX** 的应用程序。

步骤 **4**：配置应用程序部署

1. 在 Endpoint Management 控制台中，导航到配置 **>** 交付组，然后单击添加。
2. 在应用程序部分，将所需的 MDX 应用程序拖动到必需应用程序框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 导航到配置 > 交付组。
4. 选择交付组并单击部署。
5. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。



自定义应用程序

自定义应用程序是专有的企业对企业应用程序。可以使用 Endpoint Management 和 Apple 批量购买来私下安全地分发专有应用程序。可以将应用程序分发给特定的合作伙伴、客户、特许经营商和内部员工。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

自定义应用程序的要求

- Apple 商务管理或 Apple 校园教务管理帐户
- Apple 批量购买帐户（需要安装了 iOS 7 或更高版本的设备）
- 使用以下 Apple 注册模式之一在 Endpoint Management 中注册设备：
  - 自动化设备注册
  - 设备注册
  - 用户注册

步骤 **1**：链接帐户

要使用批量购买部署自定义应用程序，请将批量购买帐户链接到 Endpoint Management。

1. 设置 Apple 商务管理 (ABM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 Endpoint Management 链接起来。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应用程序会自动更新。如果应用程序启用了强制管理应用程序设置，则会更新而不提示用户。无论应用程序是必需应用程序还是可选应用程序，都会更新。

   要使用强制管理应用程序和应用程序自动更新设置，请启用 `apple.app.force.managed` 服务器属性。请参阅服务器属性。

步骤 **2**：在 **ABM** 上配置应用程序

在 ABM 帐户中添加应用程序。可以上载和分发您自己的自定义应用程序，或者从其他组织购买自定义应用程序的许可证。有关在 ABM 上添加和启用自定义应用程序的详细信息，请参阅 Apple 文档。

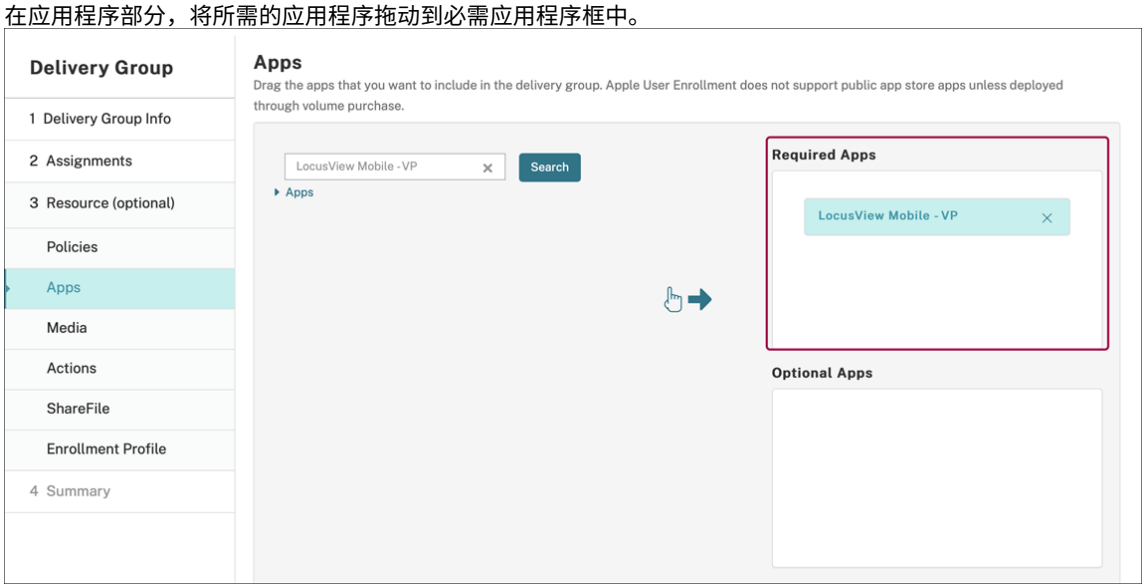
步骤 **3**：在 **Endpoint Management** 中添加和配置应用程序

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。批量购买应用程序将显示在应用程序列表中。
2. 选择要配置的应用程序。单击编辑。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. 选择要向其分发应用程序的交付组。单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

步骤 **4**：配置应用程序部署

1. 在 Endpoint Management 控制台中，导航到配置 **>** 交付组，然后单击添加。
2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



3. 导航回配置 **>** 交付组。
4. 选择要部署的交付组，然后单击部署。
5. 用户会收到部署应用程序的请求。应用程序在用户接受后在后台安装。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

启用了 **MDX** 的自定义应用程序

要使用 MDX 策略和安全功能，请添加启用了 MAM SDK 或 MDX 封装的自定义应用程序。

功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

步骤 **1**：链接帐户

要使用批量购买部署自定义应用程序，请将批量购买帐户链接到 Endpoint Management。

1. 设置 Apple 商务管理 (ABM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 Endpoint Management 链接起来。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应用程序会自动更新。如果应用程序启用了强制管理应用程序设置，则会更新而不提示用户。无论应用程序是必需应用程序还是可选应用程序，都会更新。

   要使用强制管理应用程序和应用程序自动更新设置，请启用 `apple.app.force.managed` 服务器属性。请参阅服务器属性。

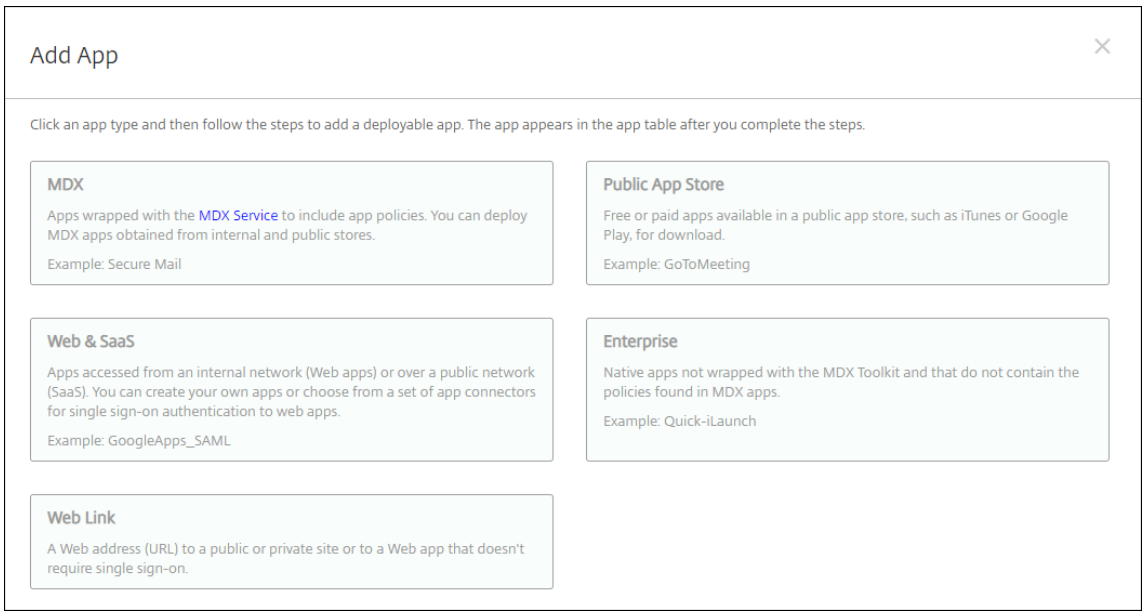
步骤 **2**：在 **ABM** 上配置应用程序

在 ABM 帐户中添加应用程序。可以上载和分发您自己的自定义应用程序，或者从其他组织购买自定义应用程序的许可证。有关在 ABM 上添加和启用自定义应用程序的详细信息，请参阅 Apple 文档。

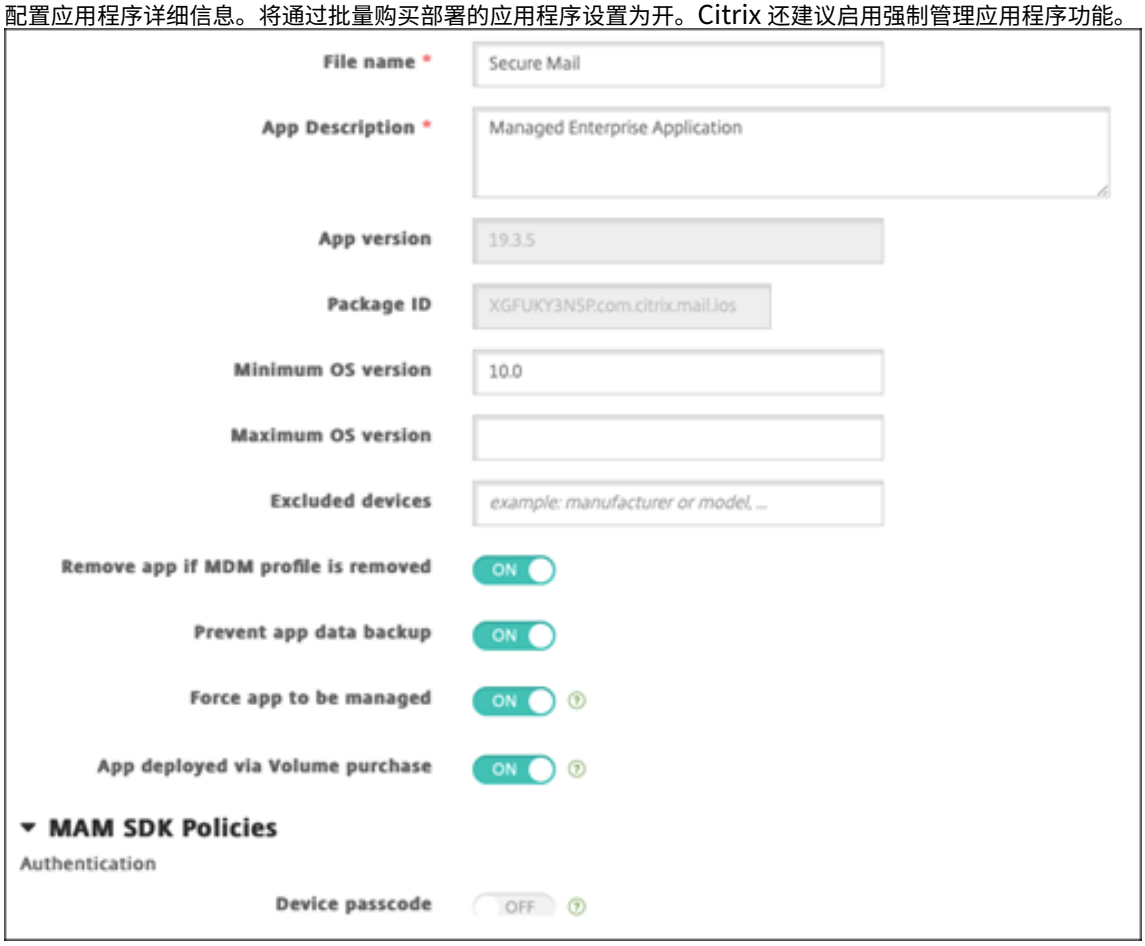
步骤 **3**：在 **Endpoint Management** 中添加和配置应用程序

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击 **MDX**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

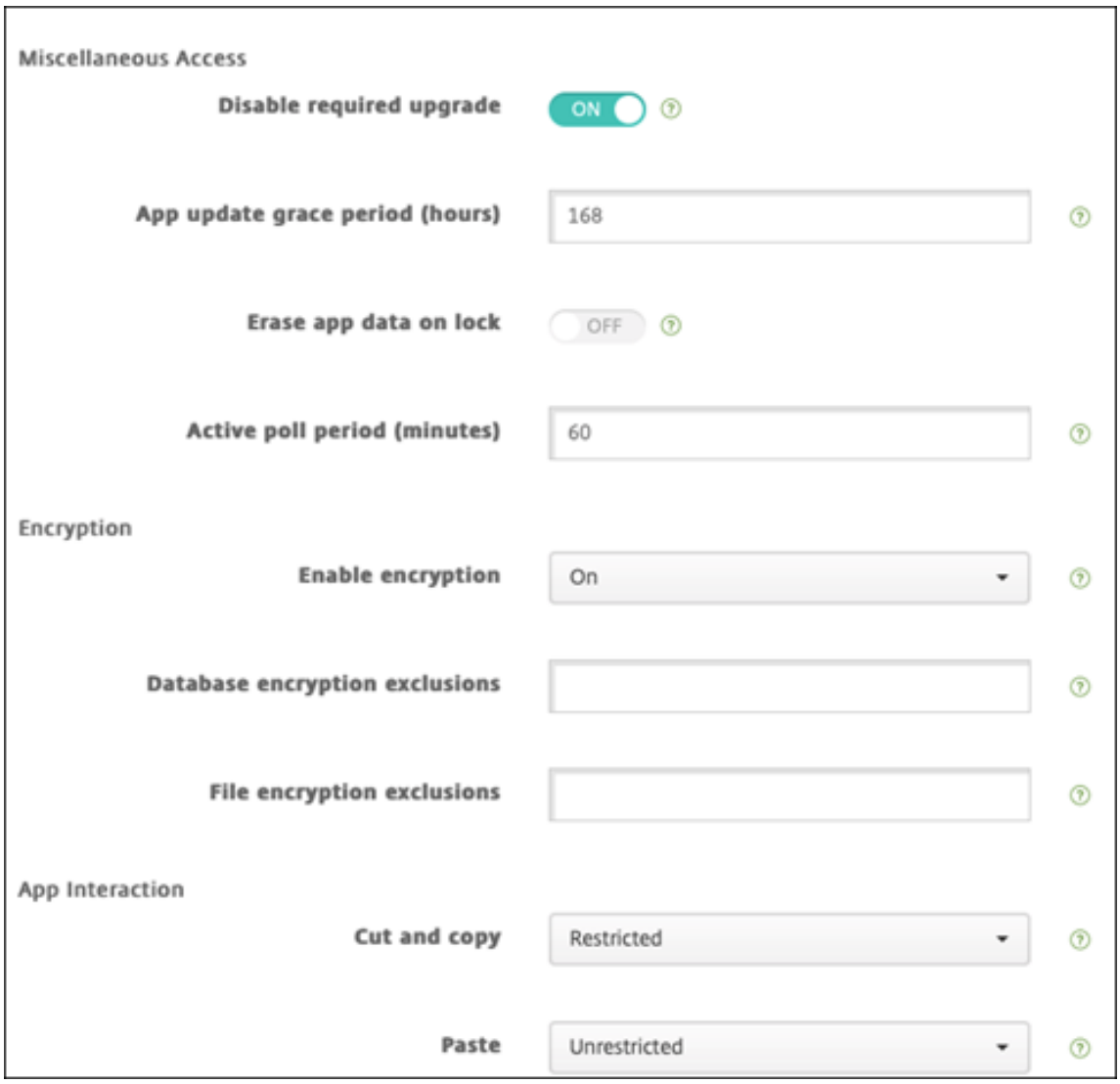


3. 选择 **iPhone** 或 **iPad** 平台。
4. 上载要添加的应用程序的 MDX 文件。
5. 配置应用程序详细信息。将通过批量购买部署的应用程序设置为开。Citrix 还建议启用强制管理应用程序功能。



6. 配置 MDX 策略。将禁用所需的升级设置为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



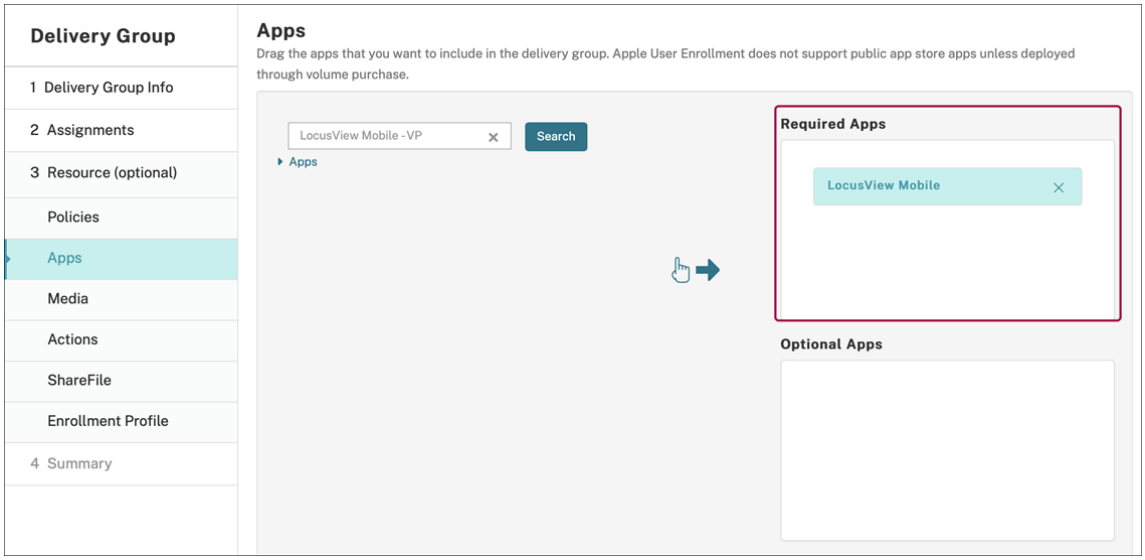
7. 将交付组分配给应用程序，然后单击保存。

此配置将导致在应用程序列表中为此应用程序列出两个条目。选择要配置的应用程序时，请选择类型为 **MDX** 的应用程序。

步骤 **4**：配置应用程序部署

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。批量购买应用程序将显示在应用程序列表中。
2. 选择要配置的应用程序。单击编辑。
3. 选择要在每个平台上向其分发应用程序的交付组。单击保存。
4. 导航到配置 **>** 交付组，然后单击添加。
5. 在应用程序部分，将所需的 MDX 应用程序拖动到必需应用程序框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 导航回配置 **>** 交付组。
7. 选择要部署的交付组，然后单击部署。
8. 用户会收到部署应用程序的请求。应用程序在用户接受后在后台安装。



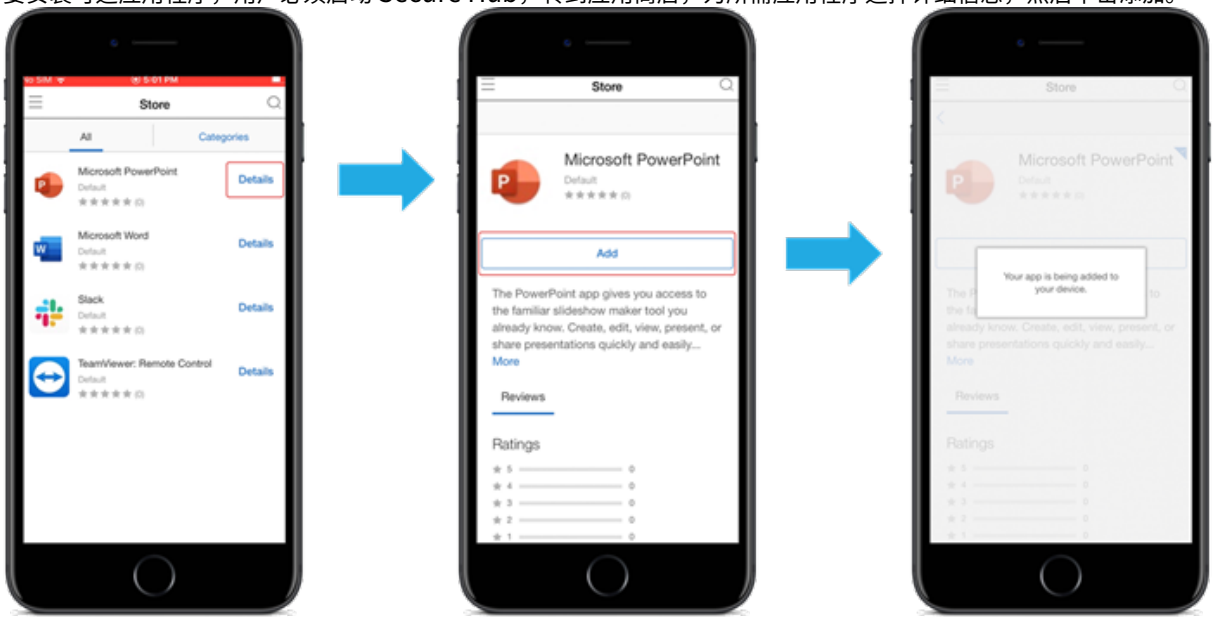
可选应用程序（仅限 **iOS/iPadOS**）

Citrix 建议根据需要部署应用程序。所需的应用程序以无提示方式安装在用户设备上，从而最大限度地减少交互。启用此功能还将允许应用程序自动更新。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可选应用程序允许用户选择要安装的应用程序，但用户必须通过 Secure Hub 手动启动安装。

要安装可选应用程序，用户必须启动 Secure Hub，转到应用商店，为所需应用程序选择详细信息，然后单击添加。



网络访问控制

November 7, 2022

可以使用网络访问控制 (NAC) 解决方案扩展 Android 和 Apple 设备的 Endpoint Management 设备安全评估。您的 NAC 解决方案使用 Endpoint Management 安全评估帮助制定和处理身份验证决策。配置 NAC 设备后，将强制执行在 Endpoint Management 中配置的设备策略和 NAC 过滤器。

将 Endpoint Management 与 NAC 解决方案结合使用可提高 QoS，并对网络内部的设备进行更精细的控制。有关将 NAC 与 Endpoint Management 集成的优势的摘要，请参阅 访问控制。

Citrix 支持以下与 Endpoint Management 集成的解决方案：

- Citrix Gateway
- ForeScout

Citrix 不保证其他 NAC 解决方案的集成。

使用网络中的 NAC 设备：

- Endpoint Management 支持 NAC 作为 iOS、Android Enterprise 和 Android 设备的端点安全功能。
- 可以在 Endpoint Management 中启用过滤器，以便根据规则或属性将设备设置为对 NAC 合规或不合规。例如：
  - 如果 Endpoint Management 中的托管设备不符合指定的条件，Endpoint Management 会将该设备标记为不合规。NAC 设备会阻止网络中的不合规设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 如果 Endpoint Management 中的托管设备安装了不合规的应用程序，NAC 过滤器可以阻止建立 VPN 连接。因此，不合规的用户设备无法通过 VPN 访问应用程序或 Web 站点。
- 如果将 Citrix Gateway 用于 NAC，则可以启用拆分隧道，以防止 Citrix Gateway 插件向 Citrix Gateway 发送不必要的网络流量。有关拆分隧道的详细信息，请参阅配置拆分隧道。

支持的 **NAC** 合规性过滤器

Endpoint Management 支持以下 NAC 合规性过滤器：

匿名设备：检查设备是否处于匿名模式。如果在设备尝试重新连接时 Endpoint Management 无法重新对用户进行身份验证，则可以执行此检查。

禁止的应用程序：检查设备是否具有应用程序访问策略中定义的禁止的应用程序。有关该策略的更多信息，请参阅 应用程序访问设备策略。

不活动设备：按照服务器属性中 **Device Inactivity Days Threshold**（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。有关详细信息，请参阅服务器属性。

缺少所需的应用程序：检查设备是否缺少在应用程序访问策略中定义的任何所需的应用程序。

非推荐应用程序：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码：检查用户密码是否合规。在 iOS 和 Android 设备上，Endpoint Management 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。例如，在 iOS 设备上，如果 Endpoint Management 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规设备”属性检查设备是否不合规。通常情况下，使用 Endpoint Management API 的自动操作或第三方会更改该属性。

吊销状态：检查设备证书是否已吊销。再次授权之前，已吊销的设备无法重新注册。

已获得 **root** 权限的 **Android** 设备和已越狱的 **iOS** 设备：检查 Android 设备或 iOS 设备是否已被越狱。

非托管设备：检查 Endpoint Management 是否正在管理设备。例如，在 MAM 下注册的设备或已取消注册的设备为非托管设备。

> 注意：
>
> “隐式合规/不合规”过滤器仅在 Endpoint Management 管理的设备上设置默认值。例如，任何安装了阻止的应用程序或未注册的设备都将被标记为“不合规”。NAC 设备会阻止您的网络中的这些设备。

配置概述

我们建议您按照列出的顺序配置 NAC 组件。

1. 配置设备策略以支持 NAC：

   对于 **iOS** 设备：请参阅配置 VPN 设备策略以支持 NAC。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

对于 **Android Enterprise** 设备：请参阅为 Citrix SSO 创建 Android Enterprise 托管配置。

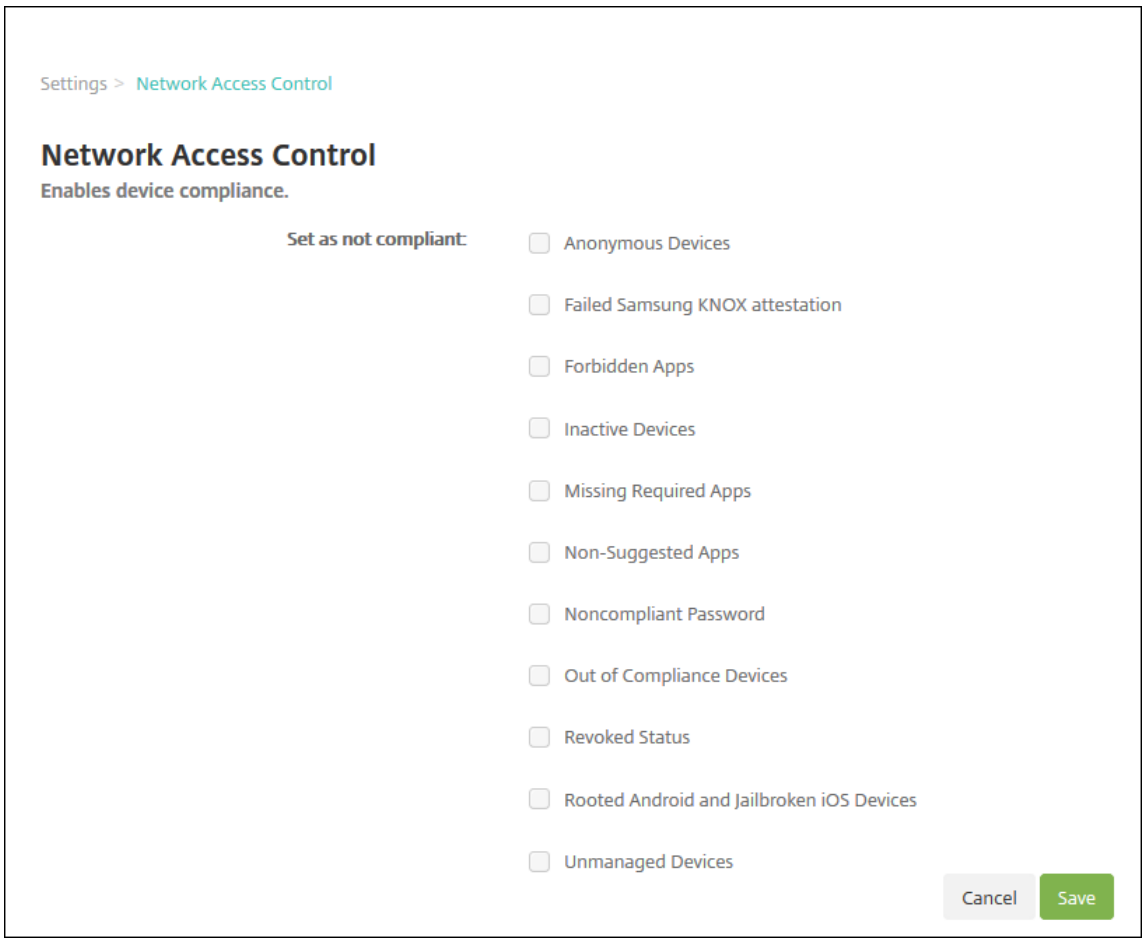
对于 **Android** 设备：请参阅 配置适用于 Android 的 Citrix SSO 协议。

2. 在 Endpoint Management 中启用 NAC 筛选器。
3. 配置 NAC 解决方案：
   - Citrix Gateway，详见更新 Citrix Gateway 策略以支持 NAC。

     要求您在设备上安装 Citrix SSO。请参阅 Citrix Gateway 客户端。
   - ForeScout：请参阅 ForeScout 文档。

在 **Endpoint Management** 中启用 **NAC** 过滤器

1. 在 Endpoint Management 控制台中，转到设置 **>** 网络访问控制。



2. 选中要启用的设为不合规过滤器旁边的复选框。
3. 单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

更新 **Citrix Gateway** 策略以支持 **NAC**

必须在 VPN 虚拟服务器上配置高级（非传统）身份验证和 VPN 会话策略。

以下步骤使用以下任一特性更新 Citrix Gateway：

- 与 Endpoint Management 集成。
- 或者，为 VPN 进行设置，而非作为 Endpoint Management 环境的一部分，并且可以访问 Endpoint Management。

在您的虚拟 VPN 服务器上，从控制台窗口中执行以下操作：命令和示例中的 FQDN 和 IP 地址是虚构的。

1. 如果要在您的 VPN 虚拟服务器上使用经典策略，请删除并取消绑定所有经典策略。要进行检查，请键入：

   ```
   show vpn vserver <VPN_VServer>
   ```

   删除包含单词 Classic 的所有结果。例如：`VPN Session Policy Name: PL_OS_10.10.1.1 Type : Classic Priority: 0`

   要删除策略，请键入：

   ```
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. 请通过键入以下命令创建相应的高级会话策略。

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   例如：`add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. 请通过键入以下命令将策略绑定到您的 VPN 虚拟服务器。

   ```
   bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
   ```

4. 请通过键入以下命令创建身份验证虚拟服务器。

   ```
   add authentication vserver <authentication vserver name> <service type>
    <ip address>
   ```

   例如：`add authentication vserver authvs SSL 0.0.0.0`
   在此示例中，`0.0.0.0` 表示身份验证虚拟服务器不面向公众开放。

5. 请通过键入以下命令将 SSL 证书与虚拟服务器绑定在一起。

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver
   certificate>
   ```

   例如：`bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. 请从 VPN 虚拟服务器将身份验证配置文件关联到身份验证虚拟服务器。首先，请通过键入以下命令创建身份验证配置文件。

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication
    vserver name>
   ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

例如：

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. 请通过键入以下命令将身份验证配置文件与 VPN 虚拟服务器关联。

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   例如：

   ```
   set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
   ```

8. 请通过键入以下命令检查从 Citrix Gateway 到设备的连接。

   ```
   curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/
   Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   例如，此查询通过获取在环境中注册的第一台设备 (deviceid_1) 的合规性状态来验证连接性：

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-
   Citrix-VPN-Device-ID: deviceid_1"
   ```

   成功的结果与以下示例类似。

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   5 <!--NeedCopy-->
   ```

9. 上一个步骤成功时，请创建对 Endpoint Management 的 Web 身份验证操作。首先，请创建一个策略表达式以从 iOS VPN 插件中导出设备 ID。键入以下命令。

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
   TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. 请通过键入以下命令向 Endpoint Management 发送请求。在此示例中，Endpoint Management IP 是 10.207.87.82，FQDN 为 example.em.cloud.com:4443。

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
     4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "
    Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+
    xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.
    RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ
    (\"Compliant\")"
    ```

    Endpoint Management NAC 的成功输出为 HTTP status 200 OK。X-Citrix-Device-State 标头的值必须为 Compliant。

11. 请通过键入以下命令创建一个要将操作关联到的身份验证策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
add authentication Policy <policy name> -rule <rule> -action <web
authentication action>
```

例如：`add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER (\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. 请通过键入以下命令将现有 LDAP 策略转换为高级策略。

```
add authentication Policy <policy_name> -rule <rule> -action <LDAP
action name>
```

例　　如：`add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 请通过键入以下命令添加要将 LDAP 策略关联到的策略标签。

```
add authentication policylabel <policy_label_name>
```

例如：`add authentication policylabel ldap_pol_label`

14. 请通过键入以下命令将 LDAP 策略关联到策略标签。

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol
 -priority 100 -gotoPriorityExpression NEXT
```

15. 请连接合规设备以执行 NAC 测试，以确认成功的 LDAP 身份验证。键入以下命令。

```
bind authentication vserver <authentication vserver> -policy <web
authentication policy> -priority 100 -nextFactor <ldap policy label> -
gotoPriorityExpression END
```

16. 添加 UI 以与身份验证虚拟服务器相关联。请键入以下命令以检索设备 ID。

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -
action lschema_single_factor_deviceid
```

17. 请通过键入以下命令绑定身份验证虚拟服务器。

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority
 100 -gotoPriorityExpression END
```

18. 创建 LDAP 高级身份验证策略以启用 Secure Hub 连接。键入以下命令。

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority
110 -gotoPriorityExpression NEXT
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop 和 Tablet

November 7, 2022

Endpoint Management 在 MDM 中注册 Windows 10 和 Windows 11 设备。Endpoint Management 支持对在 MDM 中注册的 Windows 10 和 Windows 11 设备使用以下身份验证类型。

- 基于域的身份验证
  - Active Directory
  - Azure Active Directory
- 身份提供程序：
  - Azure Active Directory
  - Citrix 身份提供程序

有关受支持的身份验证类型的详细信息，请参阅证书和身份验证。

启动 Windows 10 或 Windows 11 设备管理的一般工作流程如下：

1. 完成登录流程。请参阅载入和资源设置和准备注册设备并交付资源。

   如果计划使用自动发现服务注册 Windows 设备，则必须配置 Citrix 自动发现服务。请求 Citrix 技术支持提供帮助。有关详细信息，请参阅请求 Windows 设备的自动发现。

2. 选择并配置注册方法。请参阅支持的注册方法。
3. 配置 Windows Desktop 和 Tablet 设备策略。
4. 用户注册 Windows 10 和 Windows 11 设备。
5. 设置设备和应用程序安全操作。请参阅安全操作。

有关支持的操作系统，请参阅支持的设备操作系统。

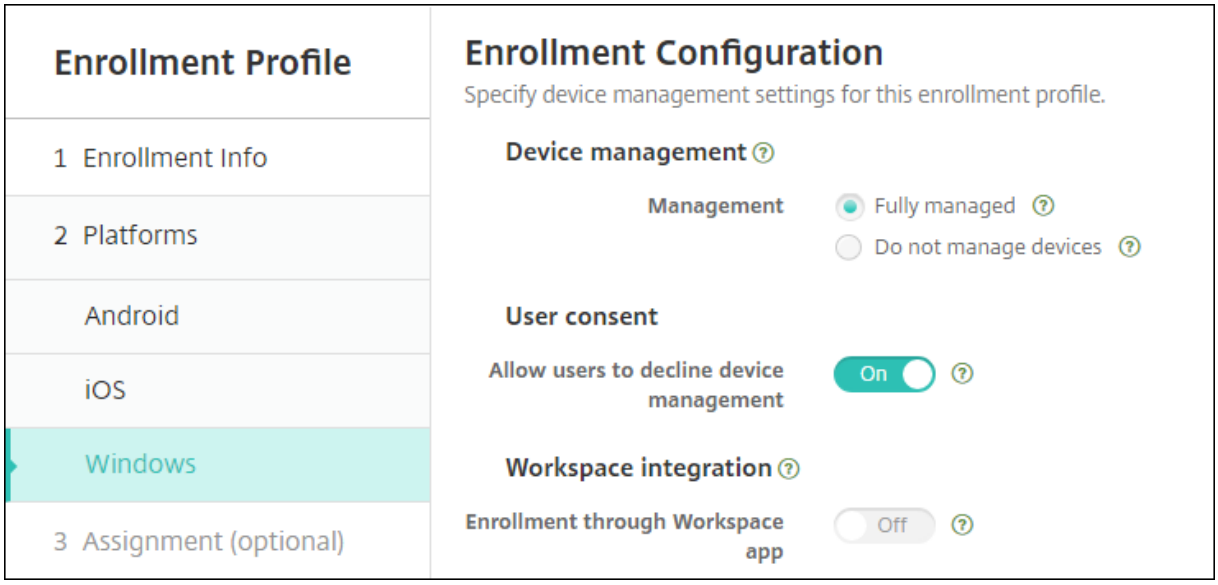
支持的注册方法

可以在注册配置文件中指定如何管理 Windows 10 和 Windows 11 设备。有两个选项可用：

- 完全托管（MDM 注册）
- 不管理设备（未注册 MDM）

要为 Windows 10 和 Windows 11 设备配置注册设置，请转到配置 **>** 注册配置文件 **> Windows**。有关注册配置文件的详细信息，请参阅注册配置文件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



下表列出了 Endpoint Management 支持的 Windows 10 和 Windows 11 设备的注册方法：

方法	支持
Azure Active Directory 注册	是
自动发现服务注册	是
Windows 批量注册	是
手动注册	是
注册邀请	否

> 注意：
>
> - 手动注册要求用户输入 Endpoint Management 服务器的完全限定域名 (FQDN)。我们不建议使用手动注册。相反，请使用其他方法以简化用户的注册过程。
> - 您不能向 Windows 设备发送注册邀请。Windows 用户直接通过其设备注册。

配置 **Windows Desktop** 和 **Tablet** 设备策略

使用这些策略可配置 Endpoint Management 与运行 Windows 10 或 Windows 11 的 Desktop 和 Tablet 设备的交互方式。此表列出了适用于 Windows Desktop 和 Tablet 设备的所有设备策略。

应用程序配置	应用程序清单	应用程序锁定
应用程序卸载	应用程序防护	BitLocker
凭据	自定义 XML	Defender

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Device Guard	设备运行状况证明	Exchange
防火墙	Kiosk	网络
办公网络	操作系统更新	通行码
限制	应用商店	条款和条件
VPN	Web 剪辑	Windows 代理
Windows GPO 配置	Windows Hello for Business

通过 **Azure Active Directory** 注册 **Windows 10** 和 **Windows 11** 设备

> 重要：
>
> 必须先在 Azure 中配置 Azure Active Directory (AD) 设置，然后配置 Endpoint Management，用户才能注册。有关详细信息，请参阅将 Endpoint Management 连接到 Azure AD。

Windows 10 和 Windows 11 设备可以通过 Azure 注册作为 AD 身份验证的联合方式。此注册需要 Azure AD Premium 订阅。

可以使用以下任一方法将 Windows 10 和 Windows 11 设备加入到 Microsoft Azure AD 中：

- 对于公司拥有的设备：
  - 在设备首次打开电源以将该设备加入 Azure AD 时在 MDM 中注册。在这种情况下，用户按 https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx 一文中所述完成注册。

    对于使用此方法注册的 Windows 设备，可以使用 Windows AutoPilot 设置和预配置设备。有关详细信息，请参阅使用 Windows AutoPilot 设置和配置设备。
  - 在配置设备后，从 Windows 设置页面将设备加入 Azure AD 时，请注册 MDM。在这种情况下，用户按配置设备后加入 Azure AD 时在 MDM 中注册中所述完成注册。
- 对于个人设备（BYOD 或移动设备）：
  - 在向 Windows 中添加 Microsoft 工作帐户同时注册到 Azure AD 时在 MDM 中注册。在这种情况下，用户按注册到 Azure AD 时在 MDM 中注册中所述完成注册。

配置设备后加入 **Azure AD** 时在 **MDM** 中注册

1. 在设备上，从“开始”菜单导航到设置 **>** 帐户 **>** 访问工作单位或学校，然后单击连接。
2. 在设置工作或学校帐户对话框的替代操作下，单击将此设备加入 **Azure Active Directory**。
3. 输入 Azure AD 凭据，然后单击登录。
4. 接受组织要求的条款和条件。
   - 如果用户单击拒绝，则设备既不加入 Azure AD，也不在 Endpoint Management 中注册。
5. 单击加入继续完成注册过程。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. 单击完成以完成注册过程。

注册到 **Azure AD** 时在 **MDM** 中注册

1. 在设备上，从“开始”菜单导航到设置 **>** 帐户 **>** 访问工作单位或学校，然后单击连接。
2. 在设置工作或学校帐户对话框中，输入 Azure AD 凭据，然后单击登录。
3. 接受组织要求的条款和条件。该设备已注册到 Azure AD 并在 Endpoint Management 中注册。
    - 如果用户单击拒绝，则设备将注册到 Azure AD，但不注册到 Endpoint Management 中。帐户上没有信息按钮。
4. 单击加入继续完成注册过程。
5. 单击完成以完成注册过程。

使用自动发现服务注册 **Windows** 设备

要为 Windows 设备配置自动发现服务，请向 Citrix 技术支持部门寻求帮助。有关详细信息，请参阅请求 Windows 设备的自动发现。

> 注意：
>
> SSL 侦听器证书必须是公用证书，才能注册 Windows 设备。自签名 SSL 证书的注册失败。

用户执行以下步骤以完成注册：

1. 在设备上，从“开始”菜单导航到设置 **>** 帐户 **>** 访问工作单位或学校，然后单击仅在设备管理中注册。
2. 在设置工作或学校帐户对话框中，输入公司电子邮件地址，然后单击下一步。

    要注册为本地用户，请输入带有正确域名的不存在的电子邮件地址（例如 `foo\@mydomain.com`）。该步骤允许用户绕过已知的 Microsoft 限制，其中 Windows 上的内置设备管理负责执行注册。在正在连接到服务对话框中，输入与本地用户关联的用户名和密码。然后，设备会发现 Endpoint Management 服务器并启动注册过程。
3. 输入凭据，然后单击继续。
4. 在使用条款对话框中，同意托管您的设备，然后轻按接受。

如果域策略禁用 MDM 注册，通过自动发现服务注册加入了域的 Windows 设备将失败。用户可以改为使用以下方法之一：

- 从域中删除设备，注册，然后重新加入这些设备。
- 输入 Endpoint Management 服务器的 FQDN 以继续。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows 批量注册

启用 Windows 批量注册后，可以为 MDM 服务器设置多个不需要重新映像设备就可管理的设备。可以对 Windows 10 和 Windows 11 Desktop 和便携式计算机设备的批量注册使用预配包。有关信息，请参阅批量注册 Windows 设备。

安全操作

Windows 10 和 Windows 11 设备支持以下安全操作。有关每个安全操作的说明，请参阅安全操作。

查找	锁定	重新启动
吊销	选择性擦除	擦除

将 Endpoint Management 连接到 Azure AD

Windows 10 和 Windows 11 设备可以在 Azure 中注册。在 Azure AD 中创建的用户可以访问这些设备。Endpoint Management 作为 MDM 服务部署在 Microsoft Azure 中。将 Endpoint Management 连接到 Azure AD 将使用户能够在将设备注册到 Azure AD 时自动将其设备注册到 Endpoint Management 中。

要将 Endpoint Management 连接到 Azure AD，请执行以下步骤：

1. 在 Azure 门户中，导航到 **Azure Active Directory >** 移动性 **(MDM** 和 **MAM) >** 添加应用程序，然后单击本地 **MDM** 应用程序。
2. 提供应用程序的名称，然后单击添加。
3. （可选）Azure 不允许将未经验证的域（例如 cloud.com）用于 IDP 配置。如果您的 Endpoint Management 注册 FQDN 包括 cloud.com，请联系 Citrix 技术支持，向其提供来自 Azure 的 TXT 记录。Citrix 技术支持人员会验证子域，允许您继续进行配置。如果您的 FQDN 在您自己的域下，您可以在 Azure 中进行正常验证。
4. 选择您创建的应用程序，配置以下设置，然后单击保存。
   - **MDM** 用户范围。选择全选。
   - **MDM** 使用条款 **URL**。以 `https://<Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou` 格式输入。
   - **MDM** 发现 **URL**。以 `https://<Endpoint Management Enrollment FQDN>:8443/zdm/wpe` 格式输入。
5. 单击本地 **MDM** 应用程序设置。
   - 在属性窗格中，设置格式为 `https://< Endpoint Management Enrollment FQDN >:8443` 的应用程序 **ID URI**。此应用程序 ID URI 是您不能在任何其他应用程序中再次使用的唯一 ID。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 在所需权限窗格中，选择 **Microsoft Graph** 和 **Windows Azure Active Directory**。
- 在密钥窗格中，创建身份验证密钥。单击保存查看键值。键值仅显示一次。保存密钥以供以后使用。您需要步骤 7 中的密钥。

6. 在 Endpoint Management 控制台中，转至设置 **>** 身份提供程序 **(IDP)**，然后单击添加。
7. 在发现 **URL** 页面上，配置以下设置，然后单击下一步。
   - **IDP** 名称。键入用于识别要创建的 IdP 连接的唯一名称。
   - **IDP** 类型。选择 **Azure Active Directory**。
   - 租户 **ID**。Azure 中的目录 **ID**。在 Azure 中导航到 **Azure Active Directory >** 属性时，您将看到该信息。
8. 在 **Windows MDM** 信息页面上，配置以下设置，然后单击下一步。
   - 应用程序 **ID URI**。您在 Azure 中键入的应用程序 ID URI 值。
   - 客户端 **ID**。您在 Azure 中的属性窗格中看到的应用程序 ID。
   - 键。您在上面的步骤 4 中创建和保存的键值。
9. 在 **IDP** 声明用法页面中，配置以下设置并单击“下一步”。
   - 用户标识符类型。选择 **userPrincipalName**。
   - 用户标识符字符串。输入 `${ id_token } .upn`。
10. 单击保存。
11. 将 Azure AD 用户添加为本地用户，并将其分配给本地用户组。
12. 创建条款和条件设备策略以及包括该本地用户组的交付组。

与 **Workspace Environment Management** 集成时的设备管理

仅使用 Workspace Environment Management (WEM)，MDM 部署是不可能的。仅使用 Endpoint Management，您只能管理 Windows 10 和 Windows 11 设备。通过集成两者，WEM 可以访问 MDM 功能，并且您可以通过 Endpoint Management 管理范围更广的 Windows 操作系统。该管理采取配置 Windows GPO 的形式。目前，管理员将 ADMX 文件导入 Citrix Endpoint Management，并将其推送到 Windows 10 和 Windows 11 Desktop 和 Tablet 以配置特定应用程序。使用 Windows GPO 配置设备策略，可以配置 GPO 并将更改推送到 WEM 服务。然后，WEM 代理将 GPO 应用到设备及其应用程序。

MDM 管理不是 WEM 集成的要求。WEM 支持的任何设备都可以向其推送 GPO 配置，即使 Endpoint Management 本身不支持该设备亦如此。

有关支持的设备列表，请参阅操作系统要求。

接收 Windows GPO 配置设备策略的设备在名为 WEM 的新 Endpoint Management 模式下运行。在已注册设备的管理 **>** 设备列表中，WEM 管理的设备的模式列中列出了 **WEM**。

有关详细信息，请参阅 Windows GPO 配置设备策略。

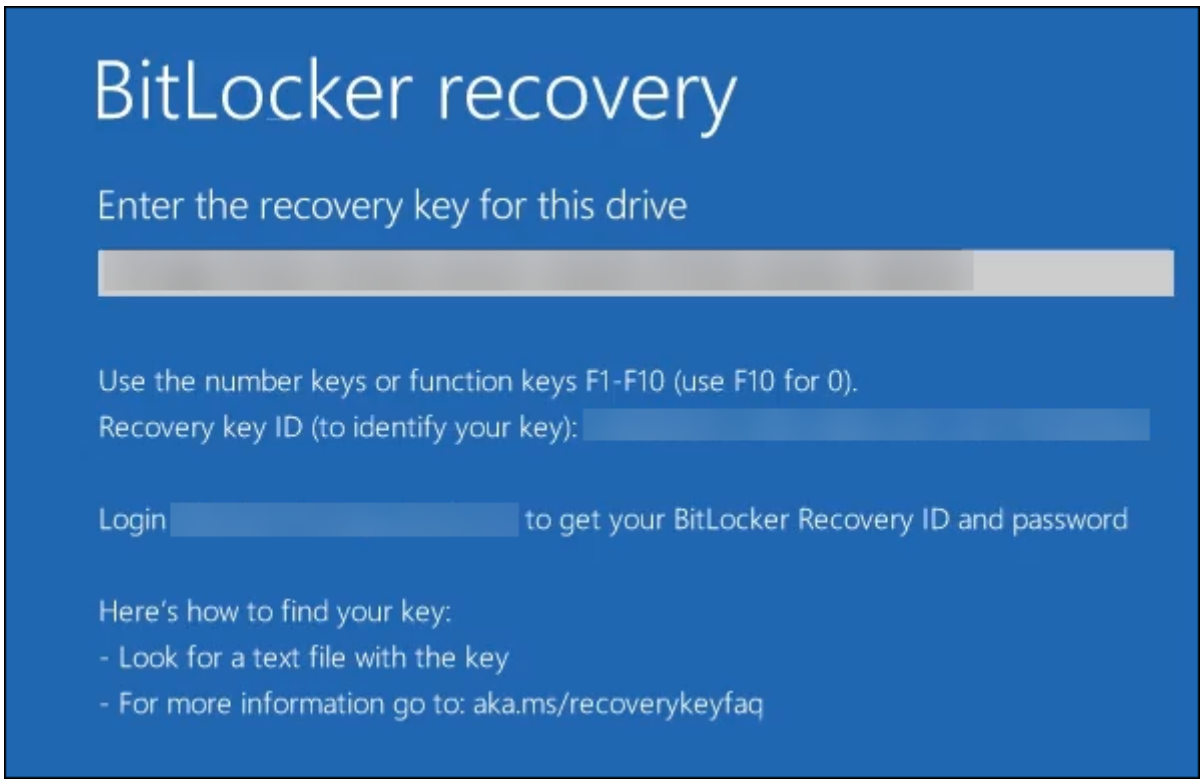
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

BitLocker 恢复密钥

使用 BitLocker 加密磁盘是一项非常有用的安全功能。但是，如果用户丢失了其 BitLocker 恢复密钥，解锁设备可能是一个难题。Endpoint Management 现在可以自动、安全地为用户保存 BitLocker 恢复密钥。用户可以在自助服务门户网站上找到自己的 BitLocker 恢复密钥。要启用和查找 BitLocker 恢复密钥，请执行以下操作：

1. 在 Endpoint Management 控制台中，导航到设置 **>** 服务器属性。
2. 搜索 `shp` 并启用 `shp.console.enable` 功能。确保 `enable.new.shp` 仍处于禁用状态。有关启用自助服务门户的详细信息，请参阅配置注册安全模式。
3. 导航到配置 **>** 设备策略。找到您的 BitLocker 策略或创建一个策略，然后启用 **BitLocker Recovery backup to Endpoint Management**（BitLocker 恢复备份到 Endpoint Management）设置。

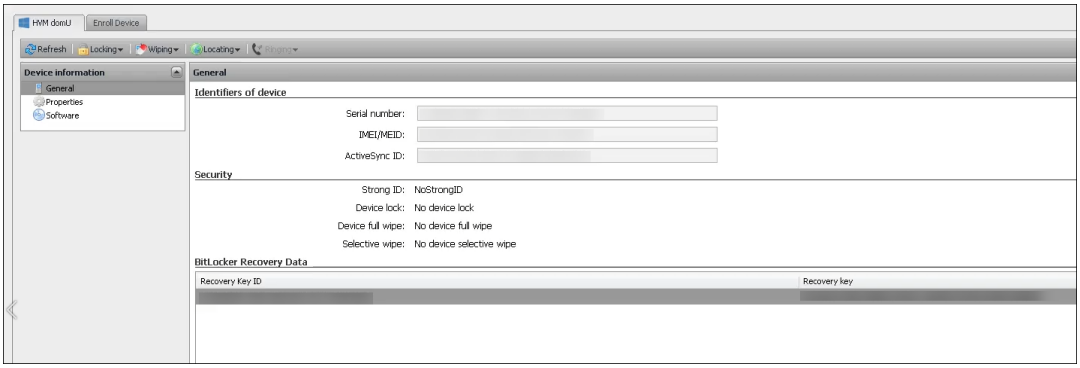
解锁设备时，最终用户会看到一条消息，要求其输入密钥。此消息还显示恢复密钥 ID。



要查找其 BitLocker 恢复密钥，用户可以导航到自助服务门户。

1. 在常规详细信息下，请查看 **BitLocker** 恢复数据。
   - 恢复密钥 **ID**：用于加密磁盘的 BitLocker 恢复密钥的标识符。此 ID 必须与上一条消息中给出的密钥 ID 匹配。
   - 恢复密钥：用户为解锁其磁盘而必须输入的密钥。在解锁提示符处输入此密钥。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



有关 BitLocker 设备策略的详细信息，请参阅 BitLocker 设备策略。

批量注册 **Windows** 设备

June 9, 2022

Endpoint Management 支持批量注册 Windows 10 和 Windows 11 台式机和平板电脑设备。通过批量注册，您可以设置许多设备供 Endpoint Management 管理，而无需重新映像设备。可以对批量注册使用预配包。

批量注册 Windows 10 和 Windows 11 设备的一般工作流程如下所示：

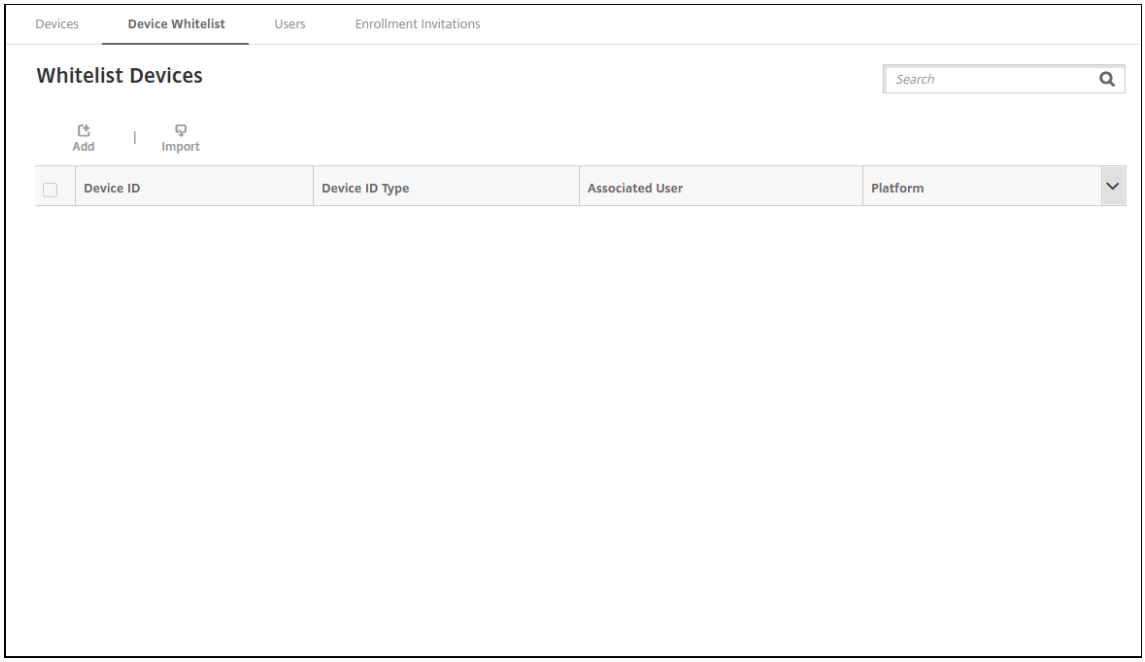
1. 分配设备。可以根据每个设备分配设备，也可以批量分配。
2. 配置批量注册。
3. 创建一个预配包并按设备应用该包。

在运行批量注册之前，请务必将所有设备分配给正确的用户。请通过根据每个设备添加或批量添加设备来执行此分配。

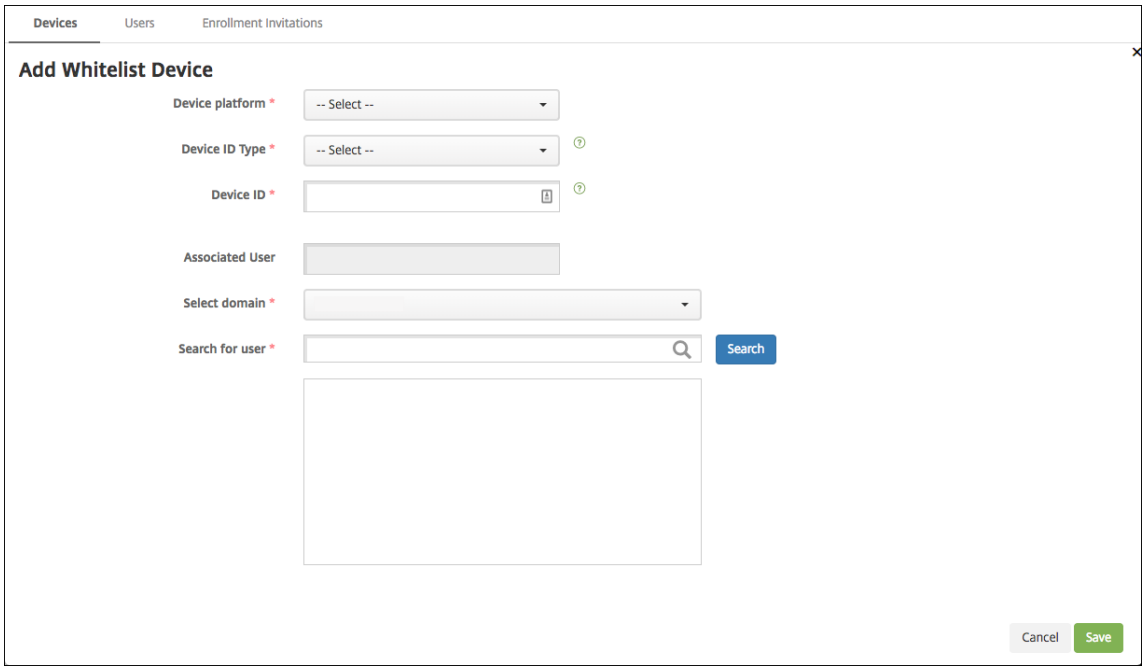
根据每个设备分配设备

1. 在 Endpoint Management 控制台中，导航到管理 **>** 设备 **>** 设备允许列表。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 要添加每个设备，请单击添加。



3. 键入以下信息：

   - 设备平台：选择 **Windows**。
   - 设备 **ID** 类型：选择用于标识设备的 ID。Endpoint Management 支持 Windows 设备的硬件 **ID** 和设备名称。
   - 设备 **ID**：键入与之前为设备选择的类型对应的 ID。
   - 关联用户：显示此设备的关联用户。此字段将自动填充您选择的用户。

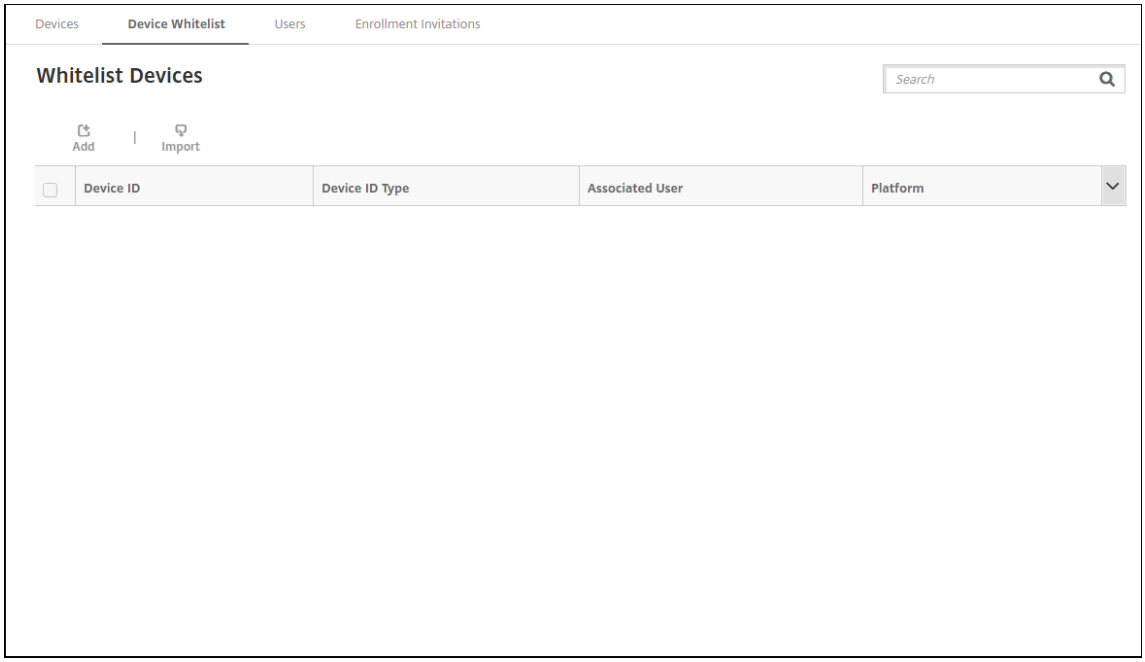
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 选择域：选择要从中搜索关联用户的域。
- 搜索用户在此字段中键入完整或部分用户名，然后单击搜索以查找要与此设备关联的用户。

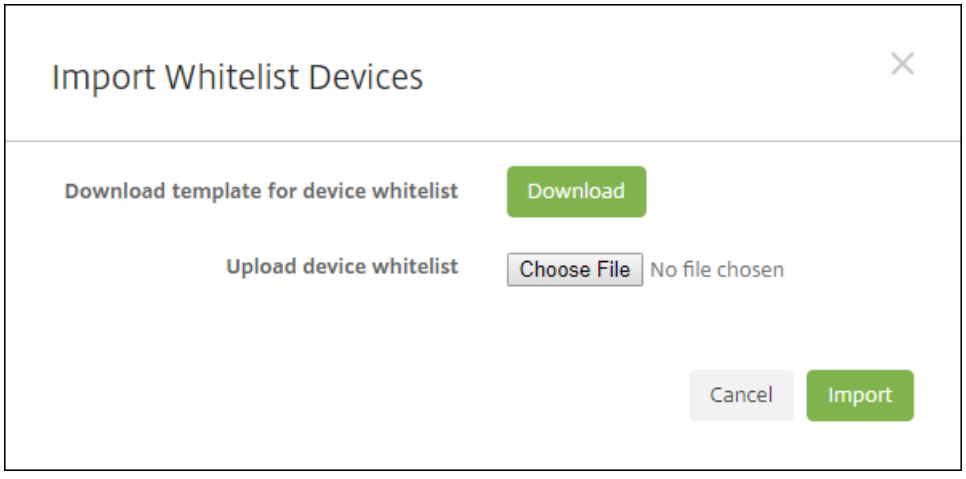
4. 单击保存。

批量添加设备

1. 在 Endpoint Management 控制台中，导航到管理 **>** 设备 **>** 设备允许列表。



2. 单击导入。

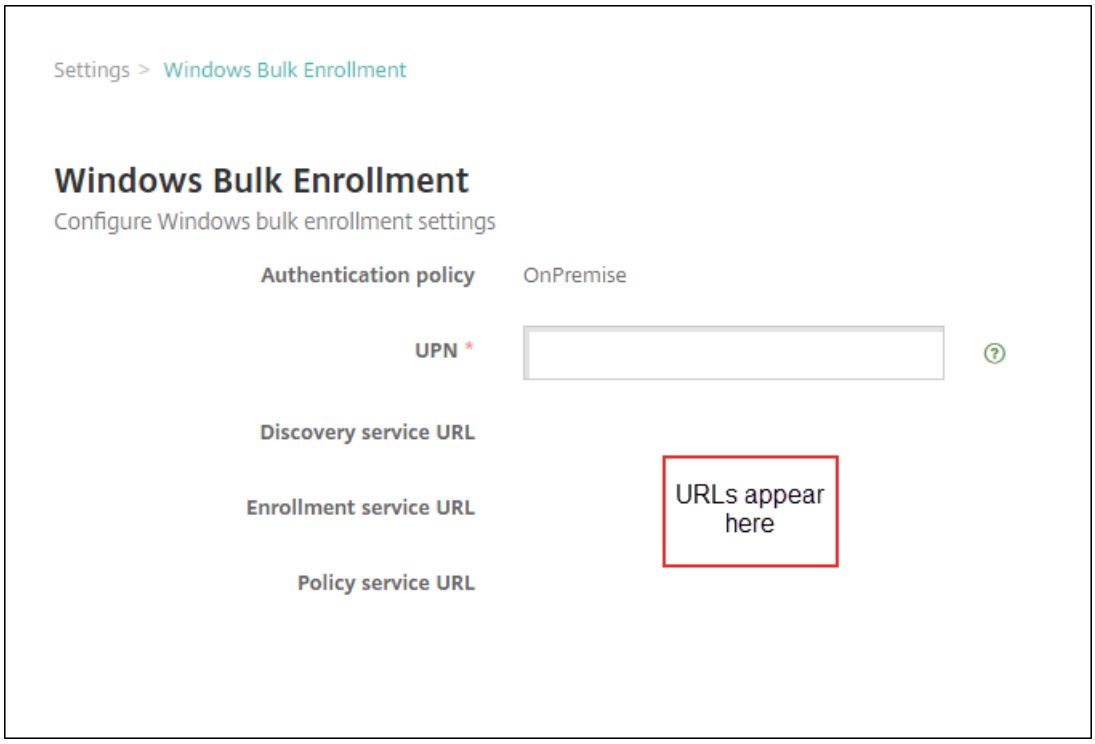


3. 单击下载下载设备允许列表的模板（电子表格）。填写该电子表格，然后使用选择文件和导入上载电子表格。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置批量注册

1. 在 Endpoint Managementr 控制台中，导航到设置 **> Windows** 批量注册。
2. 在 **UPN** 字段中，键入用于部署所有设备的用户名。UPN 必须是 Endpoint Management 中具有注册权限的有效用户。可以提供与之前选择的关联用户不同的 UPN。



   在 Windows 配置设计器中创建预配包时，您需要 URL。

3. 单击保存。

创建和应用预配包

要批量置备设备，请从 Microsoft 应用商店下载 Windows 配置设计器。Windows 配置设计器将创建用于创建设备映像的预配包。作为这些预配包的一部分，可以包括 Endpoint Management 批量注册配置设置，以便预配的设备自动注册到 Endpoint Management 中。

有关使用预配包的信息，请参阅https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool。按照该文档中 *Create and apply a provisioning package for on-premises authentication*（创建和应用预配包用于本地身份验证）部分中描述的步骤进行操作。可以按照这些步骤将以下 Endpoint Management 批量注册配置设置包括在内，并将该软件包应用到每个设备。

- 发现服务 **URL**。
- 注册服务 **URL**。
- 策略服务 **URL**。
- 密码。UPN 的密码。您之前在 UPN 字段中键入了用户名。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

批量注册设备开箱即用

Endpoint Management 支持开箱即用的 Windows 设备批量注册。请按照以下步骤进行操作，设置并执行批量注册：

1. 使用 Endpoint Management 控制台添加设备（根据每个设备添加或批量添加）并配置批量注册。有关更多信息，请参阅 批量添加设备 和 配置批量注册。
2. 创建置备包，如 创建并应用置备包中所述。

   > 注意：
   >
   > 创建预配包时，需要为每个设备配置设备名称。为此，请在 Windows 配置设计器中导航到运行时设置 **>** 帐户 **>** 计算机帐户 **>** 计算机名称，然后指定设备的名称。为每个设备指定的设备名称必须与导入允许列表设备时使用的名称一致。

3. 将该预配包放置在 USB 记忆棒中。
4. 用户首次打开目标设备时，请将该 USB 记忆棒插入设备。

   Windows 设备会自动发现 USB 记忆棒上的预配包 (.ppkg)。有关详细说明，请参阅有关如何在 初始设置期间应用置备包的 Microsoft 文档。

该设备将自动注册到 Endpoint Management 中。

对于运行 Windows 10（2004 或更高版本）或 Windows 11 的设备，可以通过仅创建一个预配包来简化注册过程。该软件包之后可应用到所有设备。因此，您不再需要在每设备基础上创建预配包。

要简化注册过程，请在创建预配包时执行以下步骤：

1. 在 Windows 配置设计器中，导航到运行时设置 **>** 帐户 **>** 计算机帐户 **>** 计算机名称。
2. 在计算机名称字段中，包括以下字符串作为设备名称的一部分：`%SERIAL%`。例如：`Surface-%SERIAL%`。字符串扩展为每个设备的 BIOS 序列号。

设备策略

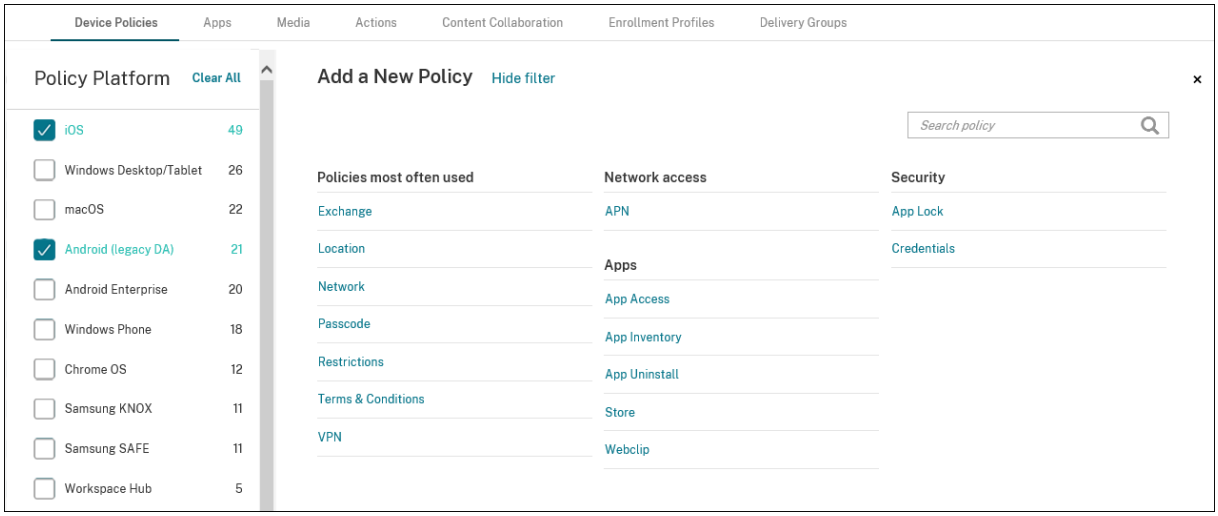
July 24, 2023

您可以通过创建策略来配置 Endpoint Management 与您的设备交互的方式。尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。因此，您可能会发现平台之间的差异，甚至 Android 设备的不同制造商之间的差异。

要查看对每个平台可用的策略，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击配置 **>** 设备策略。
2. 单击添加。
3. 每个设备平台显示在策略平台窗格中的列表中。如果该窗格未打开，请单击显示过滤器。
4. 要查看适用于某个平台的所有策略的列表，请选择该平台。要查看适用于多个平台的策略的列表，请选择所有这些平台。仅当策略适用于选择的每个平台时，才会显示在列表中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



有关每个设备策略的摘要说明，请参阅本文中的设备策略摘要。

> 注意：
>
> 如果您的环境配置了组策略对象 (GPO)：
>
> 为 Windows 10 和 Windows 11 配置 Endpoint Management 设备策略时，请记住以下规则。如果已注册的一台或多台设备上的某个策略冲突，则优先应用与 GPO 对应的策略。

要查看 Android Enterprise 容器支持的策略，请参阅 Android Enterprise。

必备条件

- 创建计划使用的交付组。
- 安装所有必需的 CA 证书。

添加设备策略

创建设备策略的基本步骤如下：

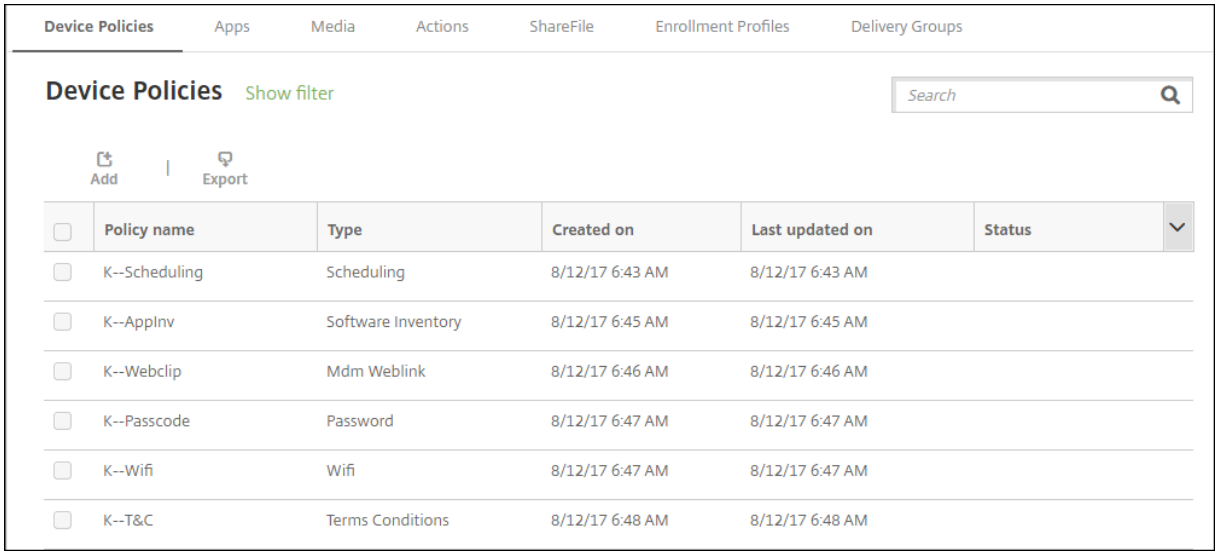
1. 为策略命名并添加说明。

   > 重要：
   >
   > 请勿在策略名称中使用正斜杠 (/)。如果执行此操作，以后编辑策略时可能会出现错误。

2. 为一个或多个平台配置策略。
3. 创建部署规则（可选）。
4. 将策略分配到交付组。
5. 配置部署计划（可选）。

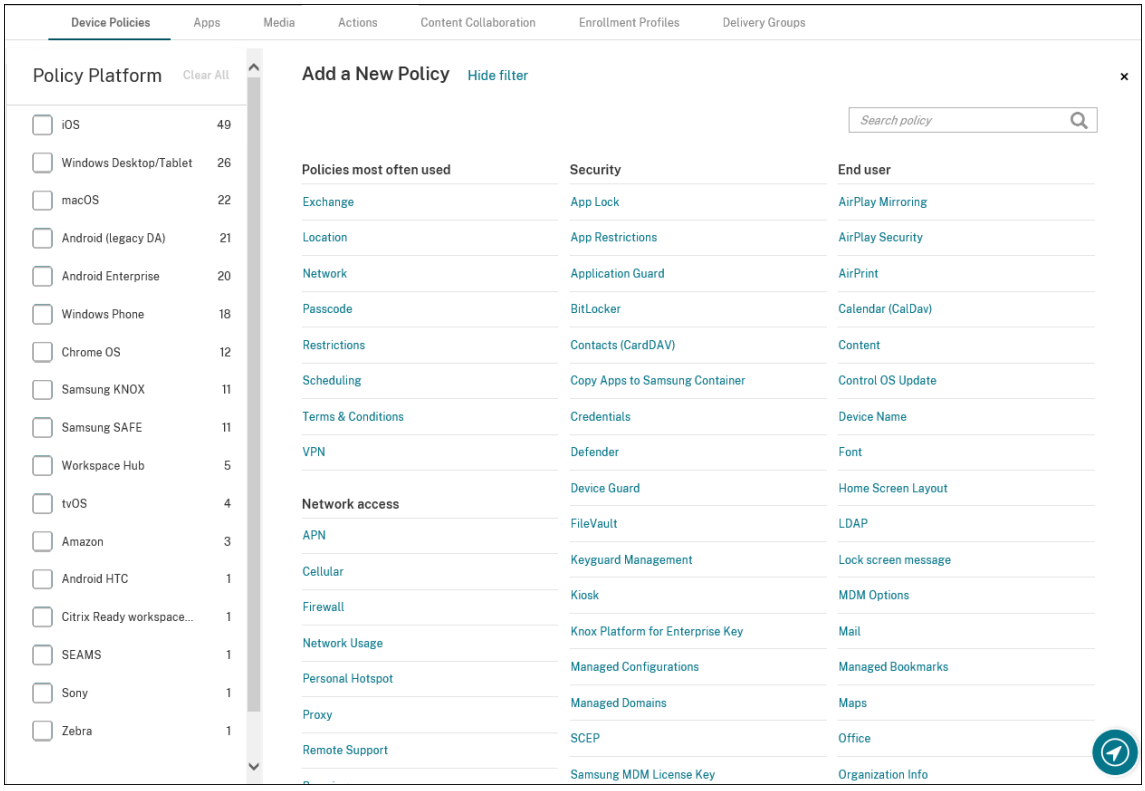
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要创建和管理设备策略，请转到配置 > 设备策略。



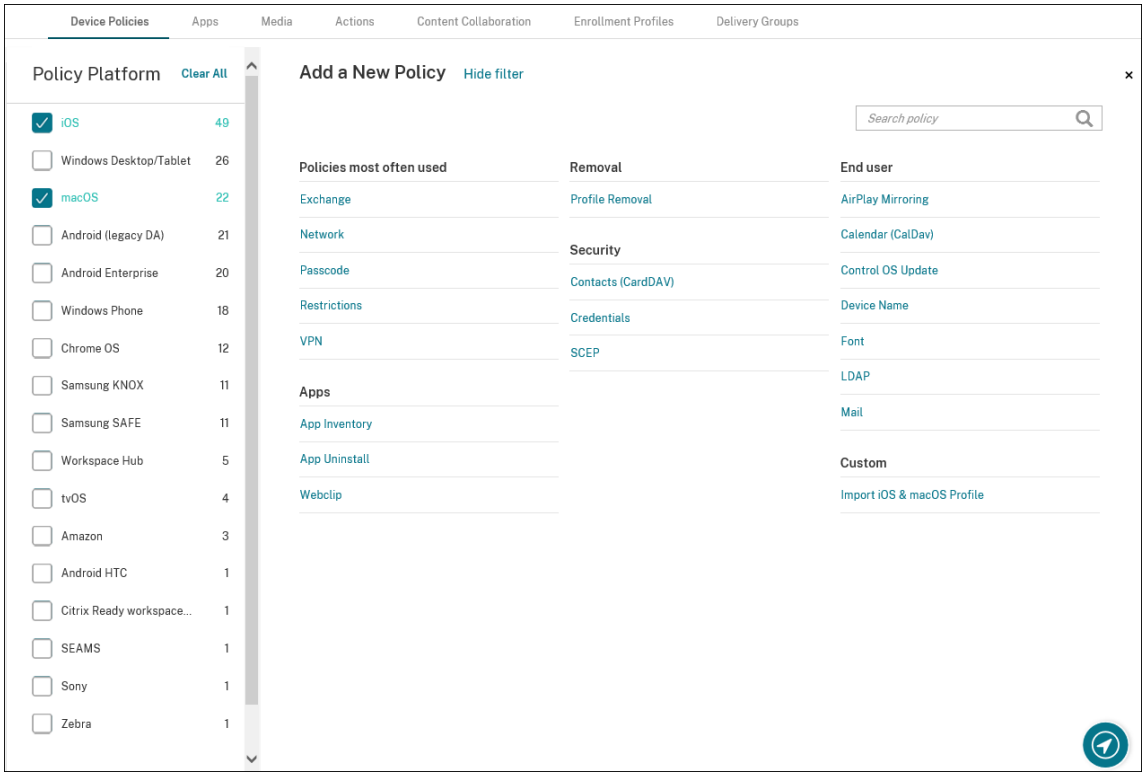
要添加策略，请执行以下操作：

1. 在设备策略页面上，单击添加。将显示添加新策略页面。



2. 单击一个或多个平台可查看适用于选定平台的设备策略的列表。单击某个策略名称可继续添加该策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



还可以在搜索框中键入策略的名称。随着键入，将显示可能的匹配项。如果列表中存在您的策略，请单击此策略。只有选中的策略保留在结果中。单击此策略以打开其策略信息页面。

3. 选择要包含在策略中的平台。选定平台的配置页面显示在步骤 5 中。
4. 完成策略信息页面，然后单击下一步。策略信息页面收集策略名称等信息，以帮助您识别和跟踪自己的策略。此页面在所有策略之间相似。
5. 完成平台页面。显示在步骤 3 选择的每个平台的平台页面。这些页面因策略而异。策略可能会因平台而异。并非所有策略都适用于所有平台。

   一些页面包括项目表。要删除现有项目，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾桶图标。在确认对话框中，单击删除。

   要编辑现有项目，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。

配置部署规则、分配和计划

有关配置部署规则的详细信息，请参阅部署资源。

1. 在平台页面上，展开部署规则，然后配置以下设置。默认情况下将显示基础选项卡。
   - 在列表中，单击选项以指定部署条件。可以选择在满足全部条件时部署策略，或在满足任意条件时部署策略。默认选项为全部。
   - 单击新建规则以定义条件。
   - 在列表中，单击条件，例如设备所有权和 **BYOD**。

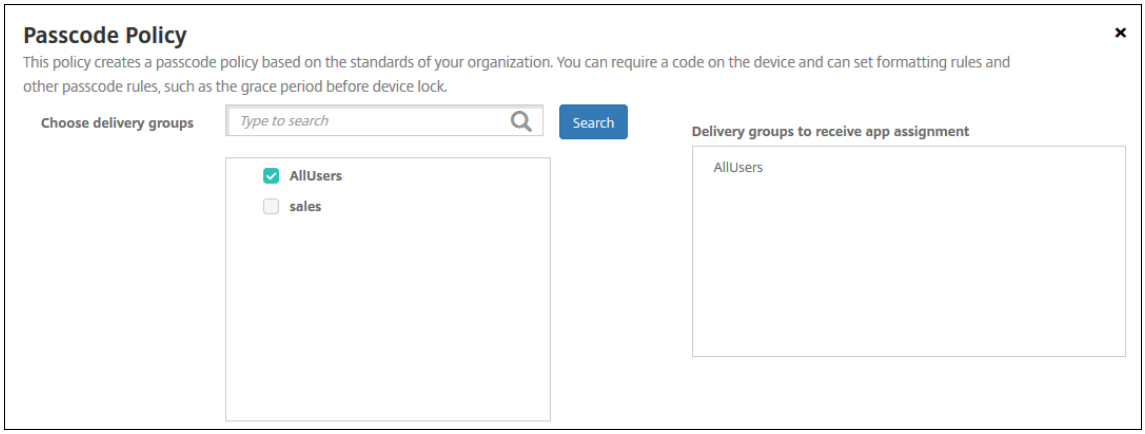
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。

2. 单击高级选项卡以使用布尔选项组合规则。此时将显示您在基础选项卡上选择的条件。
3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   - 单击与、或或非。
   - 在列表中，选择要添加到规则的条件。然后单击右侧的加号 (+) 向规则添加条件。

     您随时可以单击以选择某个条件，然后单击编辑或删除。
   - 单击新建规则添加其他条件。
4. 单击下一步移到下一个平台页面，或者在完成所有平台页面后移到分配页面。
5. 在分配页面上，选择要应用策略的交付组。如果单击某个交付组，此组将显示在用于接收应用程序分配的交付组框中。

   用于接收应用程序分配的交付组在您选择某个交付组之后才显示。

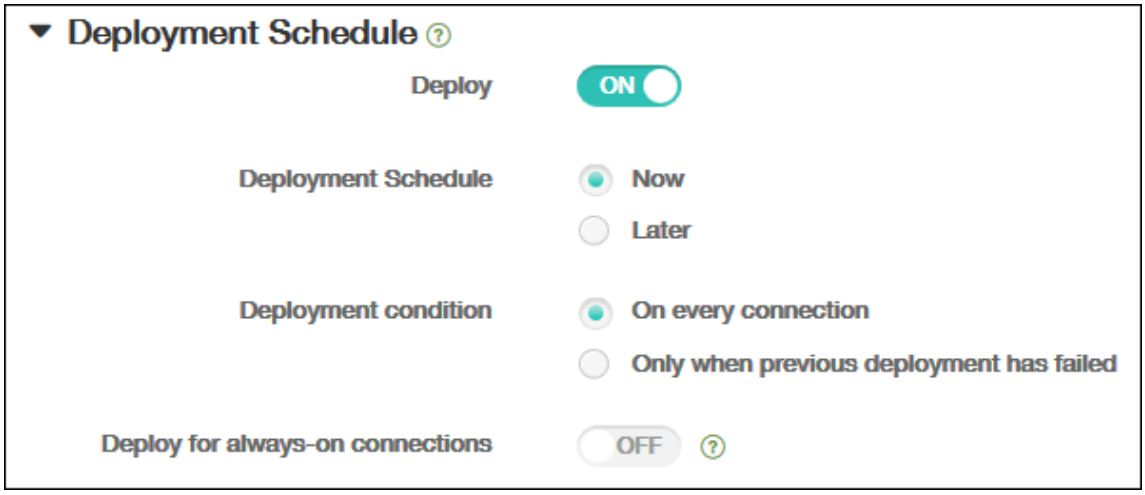


6. 在分配页面上，展开部署计划，然后配置以下设置：
   - 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。
   - 在部署计划旁边，单击立即或稍后。默认选项为立即。
   - 如果单击以后，请单击日历图标，然后选择部署的日期和时间。
   - 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
   - 在为始终启用的连接部署旁边，单击开或关。默认选项为关。

     > 注意：
     >
     > 如果在设置 > 服务器属性中配置了计划后台部署密钥，则适用此选项。
     >
     > 始终启用选项：
     >
     > - 不适用于 iOS 设备
     > - 不适用于开始使用版本 10.18.19 或更高版本的 Endpoint Management 的 Android 和

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> Android Enterprise 客户
> – 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用
>
> 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。



7. 单击保存。

   该策略显示在设备策略表中。

从设备中删除设备策略

从设备中删除设备策略的步骤取决于平台。

- Android

  要从 Android 设备中删除设备策略，请使用 Endpoint Management 卸载设备策略。有关信息，请参阅 Endpoint Management 卸载设备策略。

- iOS 和 macOS

  要从 iOS 或 macOS 设备中删除设备策略，请使用“配置文件删除”设备策略。在 iOS 和 macOS 设备上，所有策略都属于 MDM 配置文件的一部分。因此，可以仅针对要删除的策略创建“配置文件删除”设备策略。策略和配置文件的其余部分仍保留在设备上。有关信息，请参阅“配置文件删除”设备策略。

- Windows 10 和 Windows 11

  不能直接从 Windows Desktop 或 Tablet 设备中删除设备策略。但是，可以使用以下方法之一：

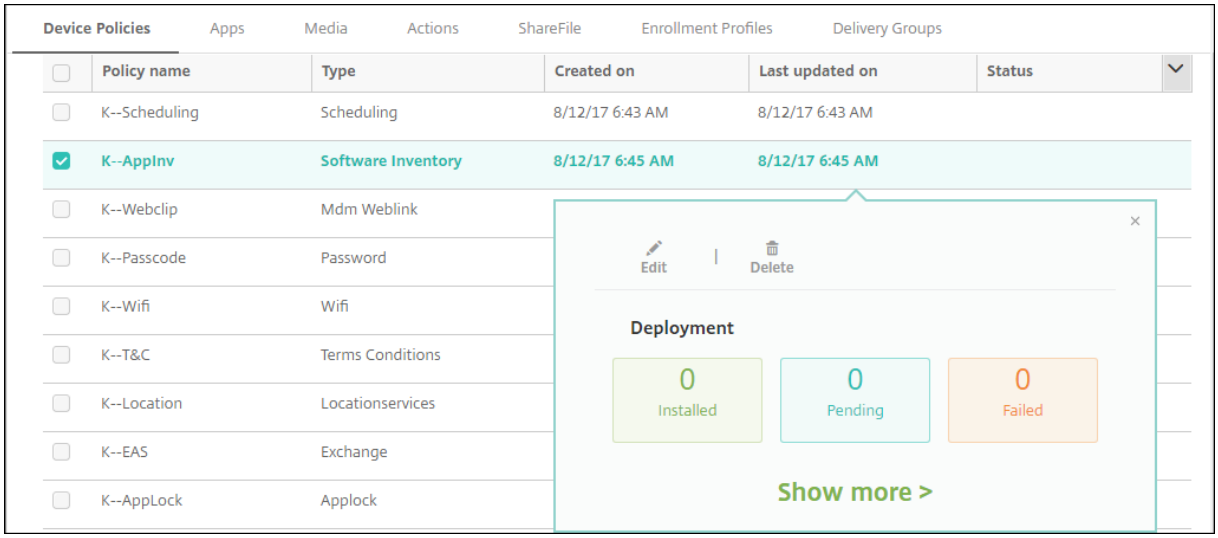
  – 取消注册设备，然后将新的一组策略推送到设备。用户随后将重新注册以继续。

  – 推送安全操作以选择性擦除特定设备。该操作将从设备中删除所有企业应用程序和数据。然后从仅包含该设备的交付组中删除设备策略，并将该交付组推送给设备。用户随后将重新注册以继续。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

编辑设备策略

要编辑策略，请选中策略旁边的复选框。选项菜单显示在策略列表上方。或者，单击列表中的策略以显示更多控件。



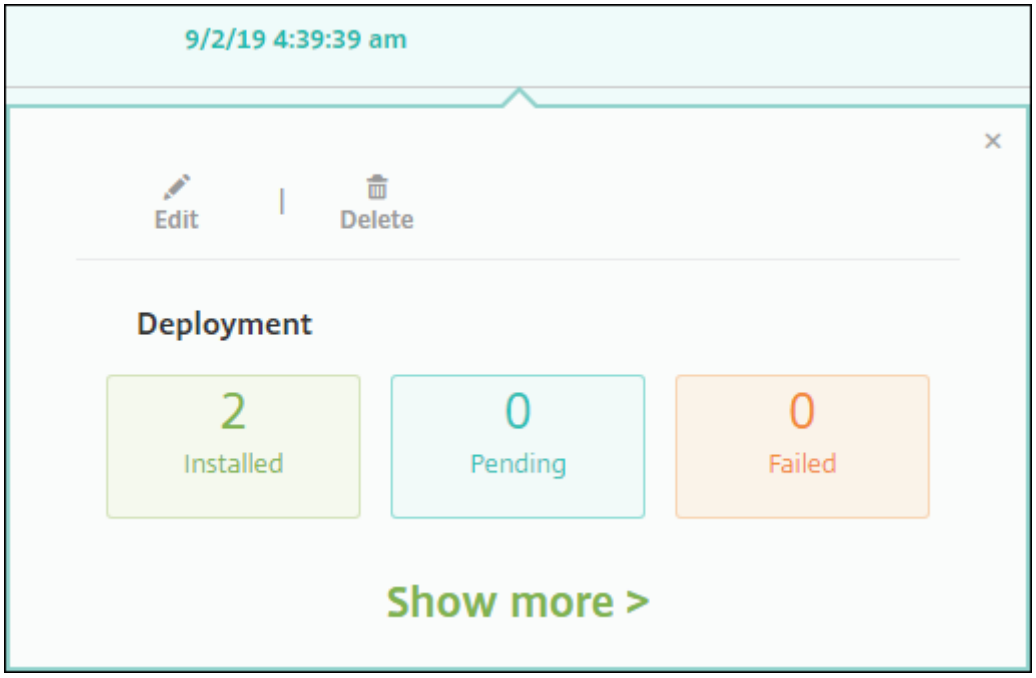
要查看策略详细信息，请单击显示更多。

要编辑某个设备策略的所有设置，请单击编辑。

如果单击删除，将显示确认对话框。再次单击删除以删除策略。

检查策略部署状态

单击配置 **>** 设备策略页面上的策略行以检查其部署状态。

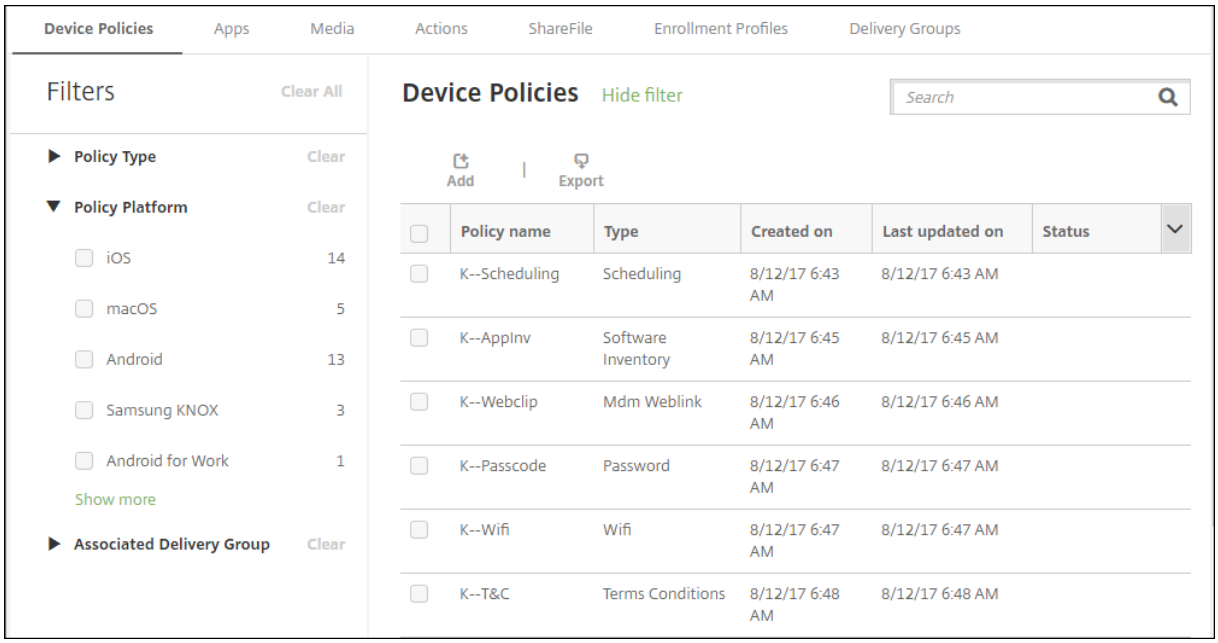


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

当策略部署处于挂起状态时，用户可以通过轻按首选项 > 设备信息 > 刷新策略从 Secure Hub 刷新策略。

过滤已添加的设备策略列表

可以按策略类型、平台和关联的交付组过滤已添加的策略列表。在配置 > 设备策略页面上，单击显示过滤器。在列表中，选择您要查看的项对应的复选框。



单击保存此视图以保存过滤器。之后过滤器的名称显示在保存此视图按钮下面的一个按钮中。

设备策略摘要

设备策略名称	设备策略说明
AirPlay 镜像	将特定 AirPlay 设备（例如 Apple TV 或其他 Mac 计算机）添加到 iOS 设备。还可以将设备添加到受监督设备的允许列表中。该选项仅将用户限制到允许列表中的 AirPlay 设备。
隔空打印	将 AirPrint 打印机添加到 iOS 设备上的 AirPrint 打印机列表。通过此策略可以更加轻松地为打印机和设备位于不同子网的环境提供支持。
APN	确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。大多数新式电话中已定义此设置。如果贵组织不使用使用者 APN 从移动设备连接到 Internet，请使用此策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略名称	设备策略说明
应用程序访问	定义设备上的必需、可选或受阻止应用程序的列表。然后，可以创建自动化操作，以使设备符合此应用程序列表。
应用程序属性	为 iOS 设备指定各种属性，例如托管应用程序捆绑包 ID 或 PerApp VPN 标识符。
应用程序配置	远程配置支持托管配置的应用程序的各种设置和行为。为此，您要将 XML 配置文件（称为属性列表或 `plist`）部署到 iOS 设备。或者，将键/值对部署到 Windows 10 台式机或平板电脑设备。
应用程序清单	收集托管设备上的应用程序清单。然后，Endpoint Management 会将清单与部署到这些设备的任何应用程序访问策略进行比较。这样一来，便可以检测允许列表或阻止列表中的应用程序以便进行应用程序访问，然后采取相应的操作。
应用程序锁定	定义用户可以或无法在 iOS 或某些 Android 设备上运行的应用程序列表。可以将 iPad 转变为 kiosk。
应用权限	配置对工作配置文件内部的 Android Enterprise 应用程序的请求如何处理 Google 称作 “危险” 权限的权限。
应用程序限制	为您想要阻止用户在 Chrome OS 设备上安装的应用程序创建阻止列表。还可以创建允许用户安装的应用程序的允许列表。
应用程序卸载	从用户设备中删除应用程序。
应用程序卸载限制	指定用户可以或无法卸载的应用程序。
应用程序防护	仅对于 Microsoft Edge 浏览器，此策略会指定 Windows Defender 应用程序防护设置。设置包括是否阻止企业站点上的外部内容。
应用程序通知	控制 iOS 用户如何从指定的应用程序接收通知。
自动更新托管应用程序	控制 Android Enterprise 设备上安装的托管应用程序的更新方式。
BitLocker	配置在 Windows 10 和 Windows 11 设备上的 BitLocker 界面中可用的设置。
蓝牙	在 iOS 设备上启用或禁用蓝牙。
浏览器	定义用户设备是否可以使用浏览器或设备可以使用的浏览器功能。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略名称	设备策略说明
日历 (CalDav)	将日历 (CalDAV) 帐户添加到 iOS 或 macOS 设备。使用 CalDAV 帐户，用户可以将计划数据与支持 CalDAV 的任何服务器同步。
手机网络	配置手机网络设置。
连接计划	Android 设备必须重新连接到 Endpoint Management，才能进行 MDM 管理、应用程序推送和策略部署。如果不向设备发送此策略并且未启用 Google FCM，设备将无法重新连接回服务器。
联系人 (CardDAV)	将 iOS 联系人 (CardDAV) 帐户添加到 iOS 或 macOS 设备。使用 CardDAV 帐户，用户可以将联系人数据与支持 CardDAV 的任何服务器同步。
内容	控制 Chrome 操作系统的各种 Web 内容选项，包括要显示的主页以及如何处理弹出窗口。
凭据	启用使用 Endpoint Management 中的 PKI 配置进行集成身份验证。例如，使用 PKI 实体、密钥库、凭据提供程序或服务器证书。
自定义 XML	自定义功能，例如预配设备、启用设备功能、配置设备和管理故障。
Defender	配置适用于台式机和平板电脑的 Windows 10 和 Windows 11 的 Windows Defender 设置。
Device Guard	启用安全启动、UEFI 锁和虚拟化等安全功能。
设备运行状况证明	需要 Windows 10 和 Windows 11 设备报告其运行状况的状态。为此，它们向 Health Attestation Service (HAS) 发送特定数据和运行时信息以供分析。HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 Endpoint Management。Endpoint Management 收到运行状况证明证书后，会根据该证书的内容，部署您配置的自动操作。
设备名称	在 iOS 和 macOS 设备上设置名称，以便您可以轻松识别设备。可以使用宏、文本或二者的组合定义设备名称。
教育配置	配置教师和学生的设备以供 Apple 教育使用。如果教师使用“课堂”应用程序，则需要配置教育配置设备策略。支持 iOS (iPadOS) 设备。
Endpoint Management 选项	配置从 Android 设备连接到 Endpoint Management 时的 Secure Hub 行为。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略名称	设备策略说明
Endpoint Management 卸载	从 Android 设备卸载 Endpoint Management。部署后，此策略将从部署组中的所有设备中删除 Endpoint Management。
Exchange	为设备上的本机电子邮件客户端启用 ActiveSync 电子邮件。
文件	将为用户执行某些功能的脚本文件添加到 Endpoint Management。或者，您可以添加您希望 Android 设备用户能够在其设备上访问的文档文件。添加文件时，还可以指定设备上要存储该文件的目录。
FileVault	此策略允许您在已注册的 macOS 设备上启用 FileVault 设备加密。还可以控制用户在登录过程中可以跳过 FileVault 设置的次数。适用于 macOS 10.7 或更高版本。
防火墙	配置防火墙设置。提供要在设备上允许或阻止的 IP 地址、端口和主机名。还可以配置代理和代理重新路由设置。
字体	在 iOS 和 macOS 设备上添加字体。字体必须是 TrueType (.TTF) 字体或 OpenType (.OFT) 字体。Endpoint Management 不支持字体集合（.TTC、.OTC）。
主屏幕布局	指定受监督的 iOS 设备上的 iOS 主屏幕的应用程序和文件夹布局。
导入设备配置	从 Workspace Hub 设备导入模板配置文件。
导入 iOS 和 macOS 配置文件	将 iOS 和 macOS 设备的设备配置 XML 文件导入 Endpoint Management 中。此文件包含您通过使用 Apple Configurator 准备的设备安全策略和限制。
键盘锁管理	控制用户在解锁设备键盘锁和工作质询键盘锁之前可用的功能。还可以控制完全托管设备和专用设备的设备键盘锁功能。例如，您可以禁用锁屏功能，例如指纹解锁、信任代理和通知。
Launcher 配置	指定 Android 设备上的 Citrix Launcher 的设置，例如允许的应用程序以及 Launcher 图标的自定义徽标图像。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略名称	设备策略说明
LDAP	提供与要用于 iOS 设备的 LDAP 服务器有关的信息，包括任何必要的帐户信息（例如 LDAP 服务器主机名）。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。
位置	允许您在地图上对设备进行地理定位（假定该设备已为 Secure Hub 启用 GPS）。将此策略部署到设备后，您可以从 Endpoint Management 发送定位命令。之后设备会返回其位置坐标。Endpoint Management 还支持地理包围栏和跟踪策略。
锁屏界面消息	将消息设置为当设备丢失时在以下设备上显示：共用的 iPad 的登录窗口和受监督 iOS 设备的锁屏界面。
邮件	在 iOS 或 macOS 设备上配置电子邮件帐户。
托管书签	将书签文件夹部署到 Chrome 操作系统设备。
托管配置	控制 Android Enterprise 设备的各种应用配置选项和应用程序限制。
托管域	定义应用于电子邮件和 Safari 浏览器的托管域。托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护公司数据。对于受监督的 iOS 设备，可以指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。
最大常驻用户数	指定共用的 iPad 的最大用户数。支持 iOS 和 iPadOS 设备。
MDM 选项	在受监督的 iOS 设备上管理 “查找我的 iPhone” 和 “iPad 激活锁”。
网络	允许管理员将 Wi-Fi 路由器详细信息部署到托管设备。路由器详细信息包括 SSID、身份验证数据和配置数据。
网络使用情况	设置网络使用规则，以指定 iOS 设备上托管应用程序如何使用网络（例如手机网络数据网络）。规则仅适用于托管应用程序。托管应用程序是指您通过 Endpoint Management 部署到用户设备的应用程序。
办公网络	将 Microsoft Office 应用程序部署到运行 Windows 10（版本 1709 或更高版本）或 Windows 11 的设备上。
组织信息	指定 Endpoint Management 部署到 iOS 设备的警报消息的组织信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略名称	设备策略说明
OS 更新	将最新的操作系统更新部署到受支持且受监督的设备。
通行码	在托管设备上强制使用 PIN 代码或密码。您可以为设备上的通行码设置复杂性和超时。
通行码锁宽限期	指定共用的 iPad 屏幕保持锁定的分钟数，之后用户必须输入通行码才能解锁屏幕。支持 iOS 和 iPadOS 设备。
个人热点	允许用户不在 Wi-Fi 网络的范围内时连接到 Internet。用户通过其 iOS 设备上手机网络数据连接并使用个人热点功能进行连接。
电源管理	控制 Chrome 操作系统设备在使用交流电或电池电源时如何响应空闲时间。
配置文件删除	从 macOS 设备中删除应用程序配置文件。
预配配置文件	指定要发送到设备的企业分发预配配置文件。在开发 iOS 企业应用程序以及为其进行代码签名时，通常会包括预配配置文件。Apple 要求应用程序的配置文件在 iOS 设备上运行。如果预配配置文件缺失或已过期，用户轻按应用程序以将其打开时，应用程序将崩溃。
删除预配配置文件	删除 iOS 预配配置文件。
代理	为运行 iOS 的设备指定全局 HTTP 代理设置。只能为每个设备部署一个全局 HTTP 代理策略。
公开会话	将 Chrome 操作系统设备配置为在客户机模式下充当公用设备。
限制	提供在托管设备上执行锁定和控制功能的数百种选项。限制选项示例：禁用相机或麦克风、强制执行漫游规则以及强制访问第三方服务（例如应用商店）。
漫游	配置在 iOS 设备上是否允许语音和数据漫游。如果禁用语音漫游，会自动禁用数据漫游。
Samsung MDM 许可证密钥	指定必须部署到设备的内置 Samsung Enterprise License Management (ELM) 密钥。Endpoint Management 还支持 Samsung Enterprise Firmware-Over-The-Air (E-FOTA) 服务。
SCEP	将 iOS 和 macOS 设备配置为从外部 SCEP 服务器检索证书。您还可以使用 SCEP 从连接到 Endpoint Management 的 PKI 向设备交付证书。为此，请在分布式模式下创建 PKI 实体和 PKI 提供程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略名称	设备策略说明
单点登录 (SSO) 帐户	创建 SSO 帐户，以便用户只需登录设备一次，即可访问 Endpoint Management 和内部公司资源。用户无需在设备上存储任何凭据。Endpoint Management 跨应用程序（包括 App Store 中的应用程序）使用 SSO 帐户的企业用户凭据。此策略与 Kerberos 身份验证兼容。适用于 iOS。
存储加密	加密内部和外部存储。对于某些设备，此策略可防止用户在其设备上使用存储卡。
存储	指定应用商店 Web 剪辑是否显示在用户设备的主屏幕上。
已订阅的日历	将订阅的日历添加到 iOS 设备上的日历列表。请务必先订阅某个日历，才能将其添加到用户设备上已订阅的日历列表中。
条款和条件	要求用户接受贵公司控制与企业网络的连接的特定策略。当用户在 Endpoint Management 中注册其设备时，必须接受条款和条件才能注册其设备。拒绝这些条款和条件会取消注册过程。
通道	在任何移动设备应用程序的客户端组件和应用服务器组件之间定义代理参数。
VPN	提供对使用传统 VPN 网关技术的后端系统的访问权限。此策略用于提供可以部署到设备的 VPN 网关连接的详细信息。Endpoint Management 支持多个 VPN 提供商，包括 Cisco AnyConnect，Juniper 和 Citrix VPN。如果您的 VPN 网关支持此选项，您可以将此策略链接到 CA 并按需启用 VPN。
墙纸	添加.png 或.jpg 文件，以设置 iOS 设备锁屏界面、主屏幕或二者的墙纸。要在 iPad 和 iPhone 上使用不同的墙纸，请创建不同的墙纸策略并将其部署到相应的用户。
Web 剪辑	在 Web 站点中放置快捷方式或 Web 剪辑，以便其与应用程序一起出现在用户设备上。您可以指定自己的图标来表示 iOS、macOS 和 Android 设备的 Web 剪辑。Windows 平板电脑只需要一个标签和一个 URL。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略名称	设备策略说明
Web 内容过滤器	过滤 iOS 设备上的 Web 内容。Endpoint Management 使用 Apple 自动过滤功能和您添加到允许列表和阻止列表中的站点。仅适用于受监督的 iOS 设备。
Windows 代理	启用此策略以在 Windows 桌面版和平板电脑版上运行上载的 PowerShell 脚本。
Windows GPO 配置	为受 Citrix Workspace Environment Management 支持的任何 Windows 设备配置组策略对象 (GPO)。
Windows Hello 企业版	启用 Windows 功能，以便用户可以在其设备上预配 Windows Hello 企业版。此策略还允许您配置通行码限制和其他安全功能。

设备策略（按平台）

策略	iOS	macOS	Android Enterprise	Android（旧版 DA）	Chrome OS	Windows Desktop/Tablet	其他
AirPlay 镜像设备策略	X	X					
AirPrint 设备策略	X						
APN 设备策略	X			X			
应用程序访问设备策略	X			X			
应用程序属性设备策略	X						
应用程序配置设备策略	X					X	
应用程序清单设备策略	X	X	X	X		X	
应用程序锁定设备策略	X			X		X	

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

策略	iOS	macOS	Android Enterprise	Android（旧版 DA）	Chrome OS	Windows Desktop/Tablet	其他
应用程序权限设备策略			X				
应用程序限制设备策略					X		
应用程序卸载设备策略	X	X	X	X			
应用程序卸载限制设备策略							X
应用程序防护设备策略						X	
应用程序通知设备策略	X						
自动更新托管应用程序			X				
BitLocker 设备策略						X	
“蓝牙”设备策略	X						
浏览器设备策略							X
日历 (CalDav) 设备策略	X	X					
手机网络设备策略	X						
连接计划设备策略			X	X	X		
联系人 (CardDAV) 设备策略	X	X					

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

策略	iOS	macOS	Android Enterprise	Android（旧版 DA）	Chrome OS	Windows Desktop/Tablet	其他
内容设备策略					X		
将应用程序复制到 Samsung 容器设备策略							X
凭据设备策略	X	X	X	X	X	X	
自定义 XML 设备策略			X			X	
Defender 设备策略						X	
Device Guard 设备策略						X	
设备运行状况证明设备策略						X	
设备名称设备策略	X	X					
教育配置设备策略	X						
Endpoint Management 选项设备策略			X	X			
Endpoint Management 卸载设备策略				X			

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

策略	iOS	macOS	Android Enterprise	Android（旧版 DA）	Chrome OS	Windows Desktop/Tablet	其他
Exchange 设备策略	X	X	X	X		X	
文件设备策略			X	X			
FileVault 设备策略		X					
防火墙设备策略		X				X	
字体设备策略	X	X					
主屏幕布局设备策略	X						
“导入设备配置”设备策略							X
“导入 iOS 和 macOS 配置文件”设备策略	X	X					
键盘锁管理设备策略			X				
网亭设备策略			X		X	X	
Launcher 配置设备策略			X	X			
LDAP 设备策略	X	X					
位置设备策略	X		X	X			
锁屏界面消息设备策略	X						

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

策略	iOS	macOS	Android Enterprise	Android（旧版 DA）	Chrome OS	Windows Desktop/Tablet	其他
邮件设备策略	X	X					
托管书签设备策略					X		
托管配置设备策略			X				
托管域设备策略	X						
最大常驻用户数设备策略	X						
MDM 选项设备策略	X						
网络设备策略	X		X	X	X		
网络使用设备策略	X						
Office 设备策略						X	
组织信息设备策略	X						
“操作系统更新”设备策略	X	X	X		X	X	
通行码设备策略	X	X	X	X		X	
通行码锁定宽限期设备策略	X						
个人热点设备策略	X						
电源管理设备策略					X		

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

策略	iOS	macOS	Android Enterprise	Android（旧版 DA）	Chrome OS	Windows Desktop/Tablet	其他
“配置文件删除”设备策略	X	X					
预配配置文件设备策略	X						
删除预配配置文件设备策略	X						
代理设备策略	X						
公共会话设备策略					X		
限制设备策略	X	X		X	X	X	
漫游设备策略	X						
Samsung MDM 许可证密钥设备策略			X				
SCEP 设备策略	X	X					
Siri 和听写策略	X						
SSO 帐户设备策略	X						
存储加密设备策略							
应用商店设备策略	X			X		X	
已订阅的日历设备策略	X						

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

策略	iOS	macOS	Android Enterprise	Android（旧版 DA）	Chrome OS	Windows Desktop/Tablet	其他
条款和条件设备策略	X			X		X	
通道设备策略				X			
VPN 设备策略	X	X		X	X	X	
墙纸设备策略	X						
Web 剪辑设备策略	X	X		X		X	
Web 内容过滤器设备策略	X						
Windows 代理设备策略						X	
Windows GPO 配置设备策略						X	
Windows Hello 企业版设备策略						X	

AirPlay 镜像设备策略

March 31, 2022

Apple AirPlay 功能允许用户通过 Apple 电视采用流技术将 iOS 设备中的内容无线推送到电视屏幕，或将设备上显示的内容精确显示到电视屏幕或其他 Mac 计算机上。

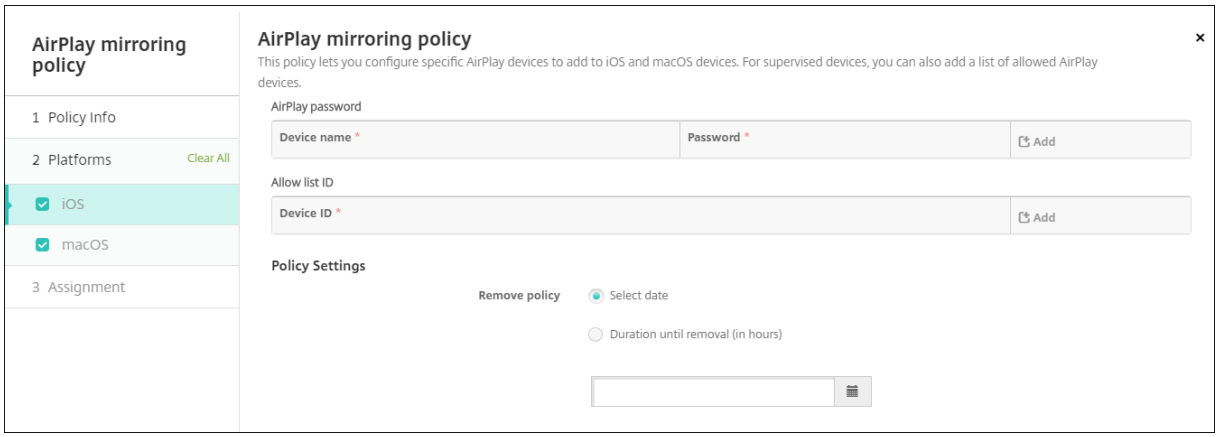
可以在 Endpoint Management 中添加一个设备策略，用于将特定 AirPlay 设备（例如 Apple 电视或其他 Mac 计算机）添加到 iOS 设备。您还可以将设备添加到受监督设备的允许列表，这将限制用户仅使用这些 AirPlay 设备。有关将设备置于受监督模式的信息，请参阅使用 Apple Configurator 2 部署设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 继续操作前，请确保您具有要添加的所有设备的设备 ID 和任何密码。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

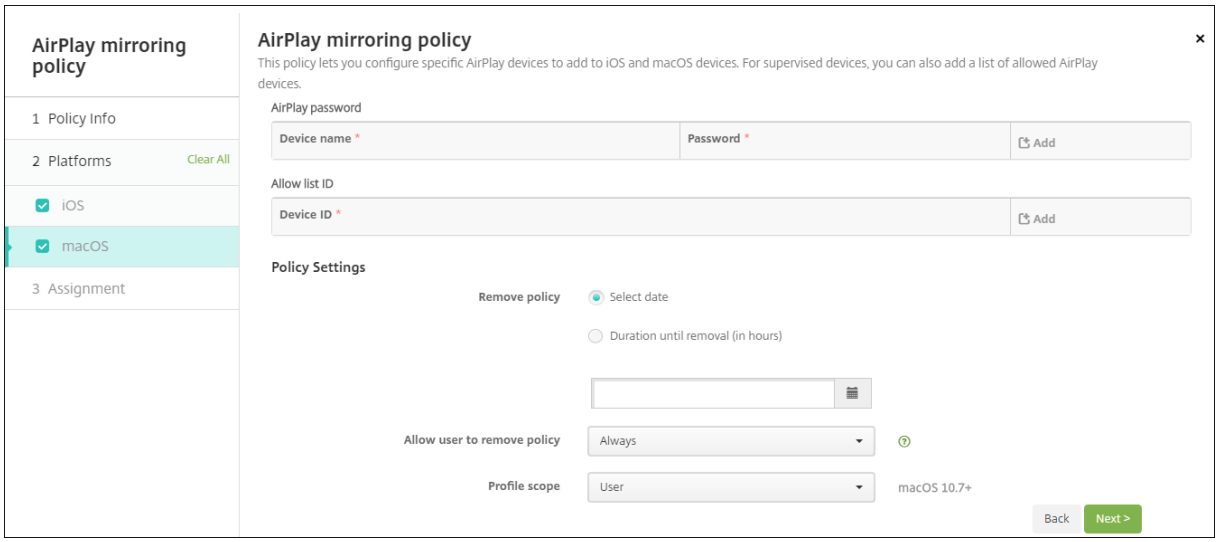
iOS 设置



- **AirPlay** 密码：对于要添加的每个设备，单击添加，然后执行以下操作：
  - 设备名称：以 xx:xx:xx:xx:xx:xx 格式输入硬件地址（Mac 地址）。此字段不区分大小写。
  - 密码：输入设备的可选密码。
  - 单击添加以添加设备，或单击取消以取消添加设备。
- 允许列表 **ID**：对于未受监督的设备，忽略此列表。此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。对于要添加到列表的每个 AirPlay 设备，单击添加，然后执行以下操作：
  - 设备 **ID**：以 xx:xx:xx:xx:xx:xx 格式键入设备 ID。此字段不区分大小写。
  - 单击添加以添加设备，或单击取消以取消添加设备。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

macOS 设置



- **AirPlay** 密码：对于要添加的每个设备，单击添加，然后执行以下操作：
  - 设备名称：以 xx:xx:xx:xx:xx:xx 格式输入硬件地址（Mac 地址）。此字段不区分大小写。
  - 密码：输入设备的可选密码。
  - 单击添加以添加设备，或单击取消以取消添加设备。
- 允许列表 **ID**：对于未受监督的设备，忽略此列表。此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。对于要添加到列表的每个 AirPlay 设备，单击添加，然后执行以下操作：
  - 设备 **ID**：以 xx:xx:xx:xx:xx:xx 格式键入设备 ID。此字段不区分大小写。
  - 单击添加以添加设备，或单击取消以取消添加设备。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

AirPrint 设备策略

March 31, 2022

AirPrint 设备策略将 AirPrint 打印机添加到 iOS 设备上的 AirPrint 打印机列表。通过此策略可以更加轻松地为打印机和设备位于不同子网的环境提供支持。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 要配置 AirPrint 设备策略，您需要每台打印机的 IP 地址和资源路径。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- **AirPrint** 目标：对于您要添加的各个 AirPrint 目标，单击添加，然后执行以下操作：
  - **IP** 地址：输入 AirPrint 打印机 IP 地址。
  - 资源路径：输入与打印机关联的资源路径。此值与 `_ipps.tcp` Bonjour 记录的参数相对应。例如，`printers/Canon_MG5300_series` 或 `printers/Xerox_Phaser_7600`。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 或更高版本。

应用程序权限设备策略

May 6, 2022

对于工作配置文件中的 Android Enterprise 应用程序：您可以配置对这些应用程序的请求如何处理 Google 称作 “危险” 权限的权限。您负责控制是否提示用户授予或拒绝来自应用程序的权限申请。此功能适用于运行 Android 7.0 及更高版本的设备。

Google 将危险权限定义为以下权限：

- 授予应用程序对涉及用户隐私信息的数据或资源的访问权限。
- 或者，可能会影响用户存储的数据或其他应用程序的操作。例如，读取用户联系人的能力属于危险权限。

您可以配置全局状态来控制所有危险权限请求的行为。此配置的作用域是工作配置文件中的 Android Enterprise 应用程序。还可以针对每个应用程序控制单个权限组的危险权限申请的行为，如 Google 所定义。这些单个设置将覆盖全局状态。

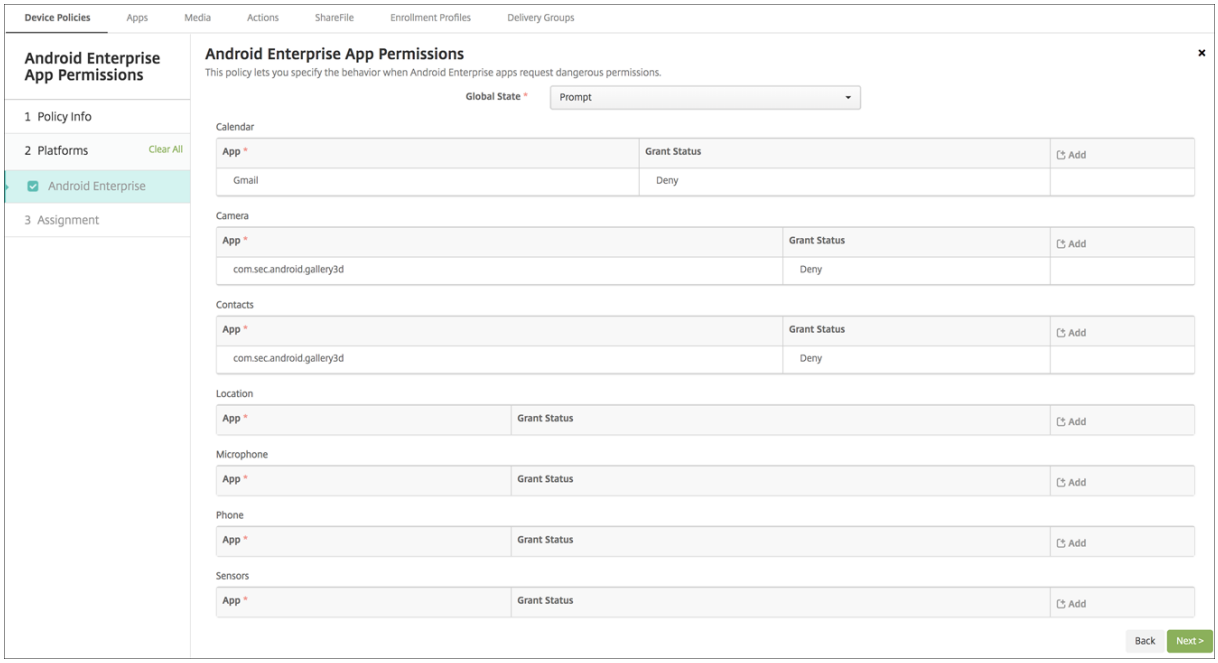
有关 Google 如何定义权限组的信息，请参阅 Android developers guide（《Android 开发人员指南》）。

默认情况下，系统将提示用户授予或拒绝危险权限申请。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android Enterprise 设置



- 全局状态：控制所有危险权限申请的行为。在列表中，单击提示、授予或拒绝。
  - 提示：系统提示用户授予或拒绝危险权限申请。
  - 授予：授予所有危险权限申请。系统不提示用户。
  - 拒绝：拒绝所有危险权限申请。系统不提示用户。

  默认值为提示。
- 针对每个应用程序设置每个权限组的单个行为。要配置某个权限组的行为，请单击添加，然后在应用程序下方从列表中选择一个应用程序。如果配置 Android Enterprise 系统应用程序，请单击新增功能，然后在“限制”设备策略中输入启用的应用程序包名称。在“授予状态”下，选择提示、授予或拒绝。此授予状态将替代全局状态。
  - 提示：系统提示用户针对此应用程序授予或拒绝来自此权限组的危险权限申请。
  - 授予：针对此应用程序授予来自此权限组的危险权限申请。系统不提示用户。
  - 拒绝：针对此应用程序拒绝来自此权限组的危险权限申请。系统不提示用户。

  默认值为提示。
- 单击应用程序和授予状态旁边的保存。
- 要为权限组添加更多应用程序，请再次单击添加并重复执行这些步骤。
- 设置完权限组的授予状态后，单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

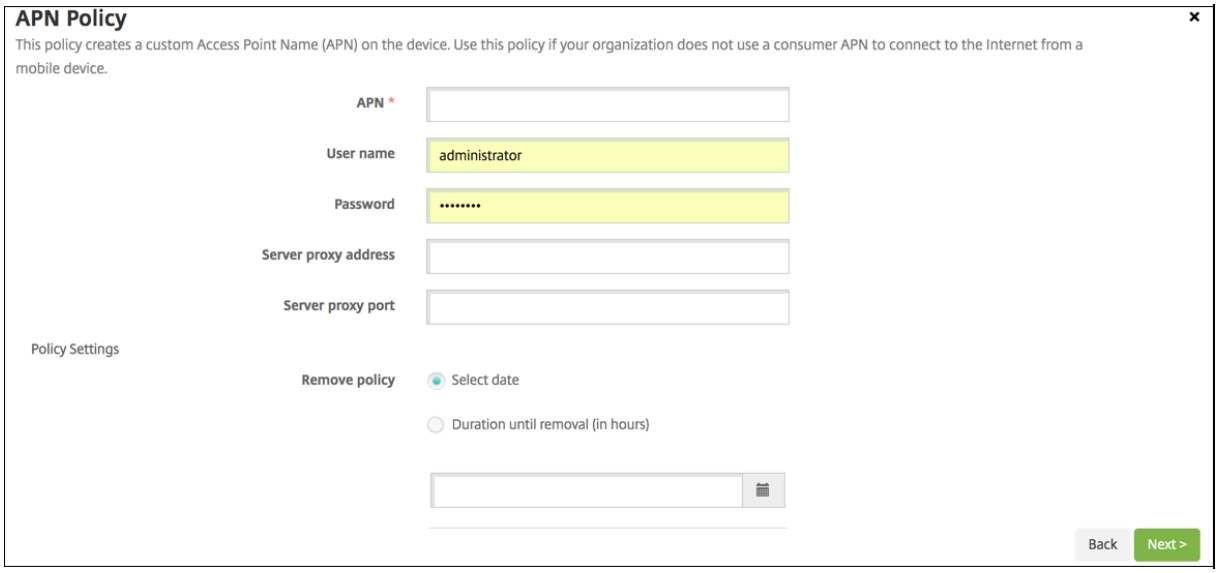
APN 设备策略

March 31, 2022

可以为 iOS 和 Android 设备添加接入点名称 (APN) 设备策略。如果贵组织不使用客户 APN 从移动设备连接到 Internet，可以使用此策略。APN 策略确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。大多数新式电话中已经定义此设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

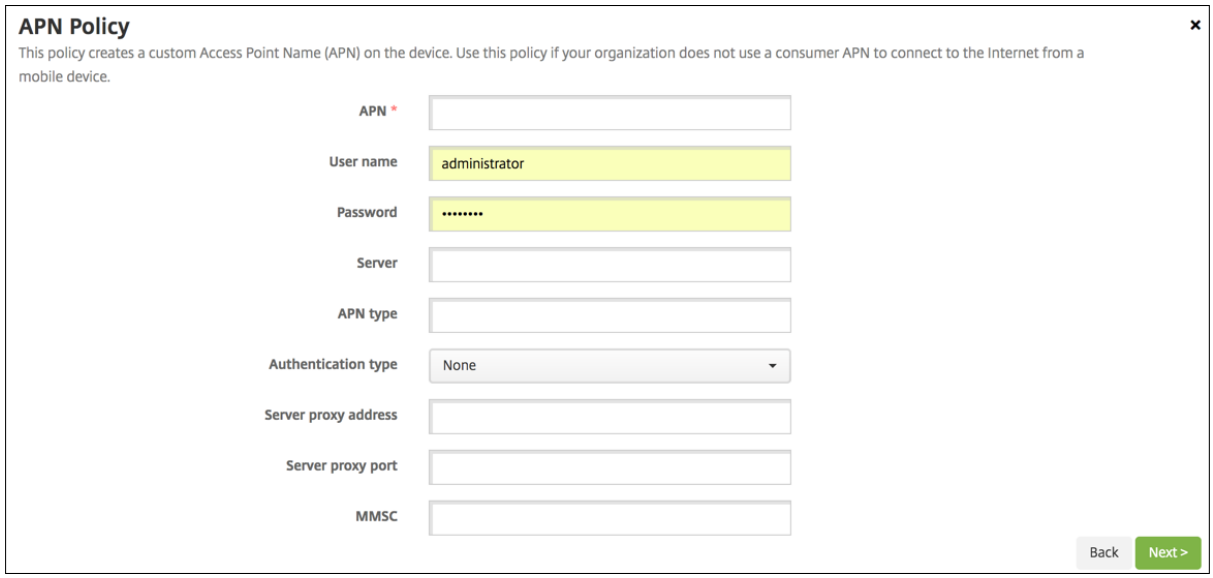
iOS 设置



- **APN**：键入接入点的名称。名称必须与接受的 iOS APN 匹配，否则策略将不起作用。
- 用户名：此字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- 密码：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- 服务器代理地址： APN 代理的 IP 地址或 URL。
- 服务器代理端口： APN 代理的端口号。如果输入了服务器代理地址，则需要端口号。
- 在策略设置下方的删除策略旁边，单击选择日期或删除前的持续时间 **(**小时**)**。
  - 对于选项选择日期，请单击日历以选择具体删除日期。
  - 对于需要密码选项，请键入密码。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 或更高版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android 设置



- **APN**：键入接入点的名称。名称必须与接受的 Android APN 匹配，否则策略将不起作用。
- 用户名：此字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- 密码：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- 服务器：此设置在智能手机之前出现，通常为空。它是指无法访问或呈现标准 Web 站点的手机的无线应用协议 (WAP) 网关服务器。
- **APN** 类型：此设置必须匹配运营商的接入点用途。它是 APN 服务说明符的逗号分隔字符串，必须与无线运营商的发布定义匹配。示例包括：
  - `\*`：所有流量均通过此接入点。
  - `mms`：多媒体流量通过此接入点。
  - **`default`**：包括多媒体在内的所有流量均通过此接入点。
  - `supl`：与 GPS 关联的安全用户层面定位 (Secure User Plane Location)
  - `dun`：拨号网络已过时，很少使用。
  - `hipri.`：高优先级网络。
  - `fota`：无线固件升级用于接收固件更新。
- 身份验证类型：在列表中，单击要使用的身份验证类型。默认值为 “无”。
- 服务器代理地址：运营商的 APN HTTP 代理的 IP 地址或 URL。
- 服务器代理端口： APN 代理的端口号。如果已输入服务器代理地址，则此端口为必填项。
- **MMSC**：运营商提供的 MMS 网关服务器地址。
- 多媒体消息服务器 **(MMS)** 代理地址： MMS 流量的多媒体消息服务服务器的地址。MMS 使得 SMS 可以发送包含多媒体内容（如图片或视频）的大型消息。这些服务器需要特定的协议（如 MM1、... MM11)。
- **MMS** 端口：用于 MMS 代理的端口。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序访问设备策略

March 31, 2022

应用程序访问设备策略允许您定义必须安装、可以安装或不得安装的应用程序的列表。如果设备上的应用程序与此策略冲突，Endpoint Management 会将该设备标记为不合规。然后，您可以创建自动操作来对该设备的合规性做出反应。

> 重要：
>
> 应用程序访问设备策略不会阻止用户安装禁止的应用程序或者卸载必需的应用程序。

一次只能配置一种类型的访问策略。每个策略都包含必需的应用程序、建议的应用程序或禁止的应用程序的列表，但不包含同一应用程序访问策略中的混合列表。如果为每种列表类型创建一个策略，请谨慎地为每个策略命名，以便于了解哪项策略适用于哪种应用程序列表。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 和 **Android**（旧版 **DA**）设置

- 访问策略：选择要为此策略配置的列表类型。
  - **Required**（必需）：应用程序必须存在于设备上。如果应用程序不存在，设备将被标记为不合规。**Required**（必需）为默认选项。
  - **Forbidden**（禁止）：设备上不得存在该应用程序。如果该应用程序确实存在，设备将被标记为不合规。
- 要向列表中添加一个或多个应用程序，请执行以下操作：
  1. 单击添加，然后配置以下各项：
     - 应用程序名称：输入应用程序的名称。
     - 应用程序标识符：输入可选的应用程序标识符。
  2. 单击保存。
  3. 对要添加的每个应用程序重复这些步骤。

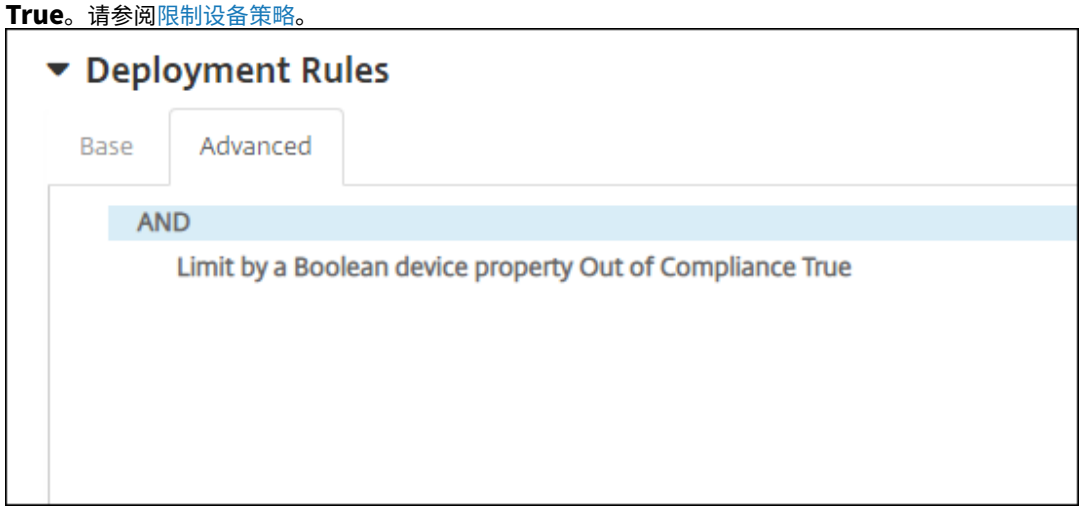
根据应用程序访问合规性配置自动化操作

1. 添加应用程序访问策略以要求或禁止应用程序。
2. 根据有问题的应用程序是必需的还是禁止的，配置两个自动化操作：
   - 必需
     - 如果设备上不存在必需的应用程序，则将该设备标记为不合规。
     - 安装必需的应用程序后，将设备标记为合规。
   - 禁止
     - 如果设备上存在禁止的应用程序，则将该设备标记为不合规。
     - 一旦不再安装禁止的应用程序，则将设备标记为合规。

     有关设置自动化操作的信息，请参阅自动化操作。
3. 使用要在不合规设备上实施的设置创建限制策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

a) 作为限制策略的一部分，添加一条高级部署规则，其中包含选项通过布尔设备属性进行限制、不合规和 **True**。请参阅限制设备策略。



4. 创建配置文件删除策略，以便在设备恢复合规性后删除限制策略。
5. 添加一条高级部署规则，其中包含选项通过布尔设备属性进行限制、不合规和 **False**。请参阅“配置文件删除”设备策略。

应用程序属性设备策略

March 31, 2022

在应用程序属性设备策略中，您可以为 iOS 设备上的应用程序指定属性。通过配置此类型的策略，您可以完成以下操作：

- 为应用程序分配 PerApp VPN。
- 阻止用户卸载任务关键型应用程序。适用于 iOS 14 及更高版本。
- 如果启用了关联域功能，请指定要添加到应用程序的关联域。适用于 iOS 13 及更高版本。

  有关详细信息，请参阅关于关联域。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

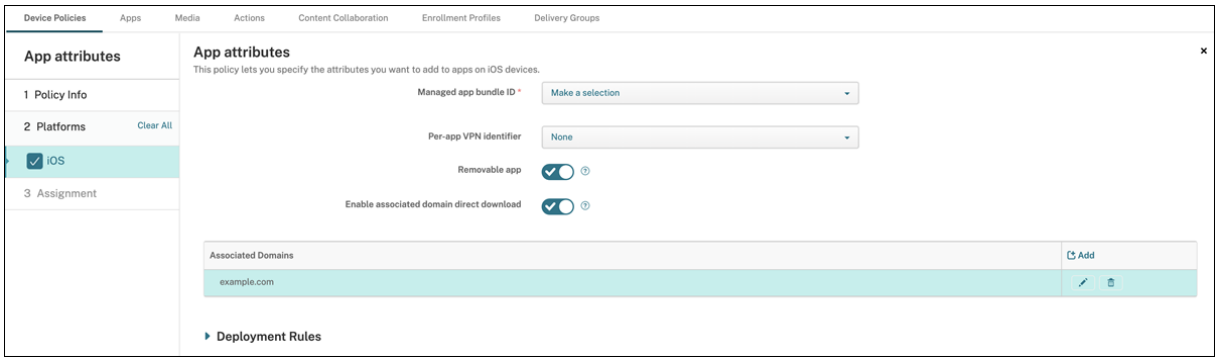
关于关联域

通过关联域，您可以在域与应用程序之间建立安全关联，以便可以从您的 Web 站点共享凭据或提供应用程序中的功能。例如，启用此功能后，您可以在贵组织的应用程序与 Web 站点之间共享数据以及登录凭据。

有关如何启用此功能的信息，请参阅 Apple Web 站点上的 Supporting Associated Domains（支持关联域）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 设置



- 托管应用程序捆绑包 **ID**：请按以下方式指定应用程序：
  - 选择应用程序捆绑包 ID。选项仅在您启用了应用程序清单设备策略后可用，该策略将收集托管设备上的应用程序的清单。
  - 选择 **“Add new**（新增），然后键入应用程序捆绑包 ID。
    要查找应用程序捆绑包 ID，请参阅在应用商店中查找应用程序的捆绑包 ID。
- **PerApp VPN** 标识符：（可选）为此应用程序选择 PerApp VPN。选项包括在设备策略 **> VPN** 策略页面上配置的 PerApp VPN 连接。Per-app VPN identifier
  有关详细信息，请参阅配置 PerApp VPN。
- **Removable app**（可删除的应用程序）：（可选）指定当此应用程序是托管应用程序时，用户是否可删除此应用程序。要阻止用户卸载此应用程序，请将此选项设置为关。默认值为开。
- **Enable associated domain direct download**（启用关联域直接下载）：（可选）默认为开，表示此应用程序直接在域上执行声明站点关联验证，而非在 Apple 服务器上执行。对于无法访问 Internet 的域，请仅将此选项设置为开。
- **Associated Domains**（关联域）：（可选）要添加此应用程序的关联域，请单击 **Add**（添加），然后键入其完全限定域名 (FQDN)。

在应用商店中查找应用程序的捆绑包 ID

1. 在 App Store 中找到应用程序，然后复制 URL 末尾的编号。例如，363501921 是 Citrix Workspace 应用程序的应用程序 ID。
2. 转到 `https://itunes.apple.com/lookup?id=` 并粘贴该 URL 后的编号。TXT 文件自动下载到您的计算机。
3. 在 TXT 文件中，搜索 `bundleId` 并获取应用程序的捆绑包 ID。示例：Citrix Workspace 应用程序的捆绑包 ID 为 `com.citrix.ReceiveriPad`。

应用程序配置设备策略

September 23, 2022

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

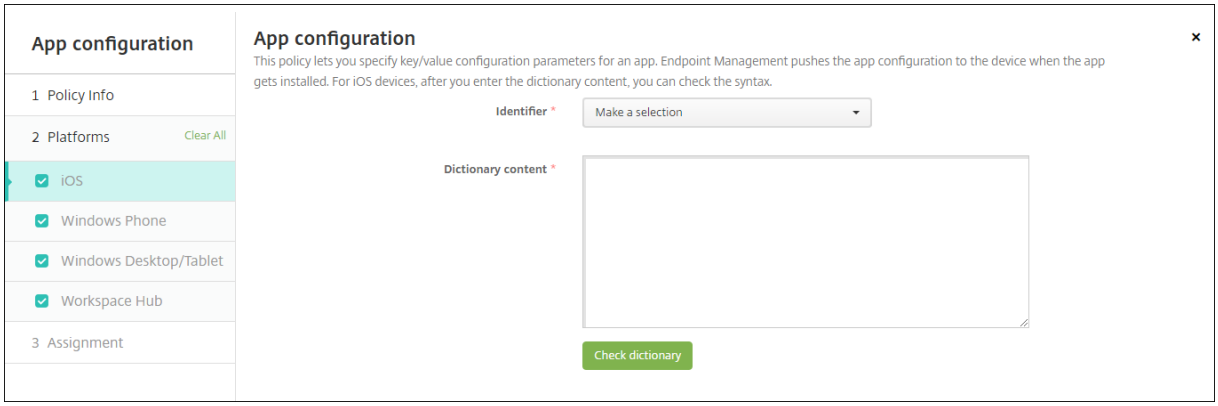
您可以执行以下操作来远程配置支持托管配置的应用程序：

- 将 XML 配置文件（.plist，又称为属性列表）部署到 iOS 设备
- 运行 Windows 10 或 Windows 11 的 Phone、Desktop 或 Tablet 设备的键/值对
- Citrix Workspace 到 Workspace Hub 设备的连接信息

配置指定应用程序中的各种设置和行为。Endpoint Management 在用户安装应用程序时将配置推送到设备。可以配置的实际设置和行为取决于应用程序，不在本文的探讨范围之内。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- 标识符：在列表中，单击要配置的应用程序，或单击新增向列表中添加应用程序。
  - 如果单击新增，请在显示的字段中键入应用程序标识符。
- 字典内容：键入或复制并粘贴 XML 属性列表 (.plist) 配置信息。
- 单击检查字典。Endpoint Management 将验证 XML。如果没有错误，内容框下面将显示有效 **XML**。如果内容框下面显示语法错误，必须纠正这些错误，然后才能继续操作。

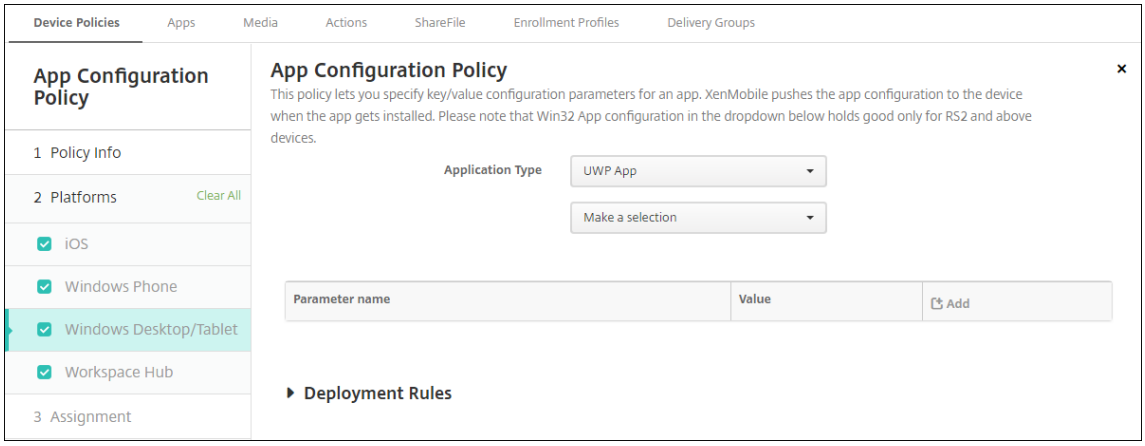
Windows Desktop/Tablet 设置

可以配置通用 Windows 平台 (UWP) 应用程序或 Win32 应用程序。要导入 Microsoft 管理模板 (ADMX) 策略设置，请配置 Win32 应用程序。

> 注意：
>
> 应用程序配置设备策略支持第三方应用程序（例如 Office）的第三方 ADMX 文件。不支持在 %SystemRoot%\PolicyDefinitions<!--NeedCopy--> 下作为操作系统组策略提供的适用于 Windows 的 Microsoft ADMX 模板。

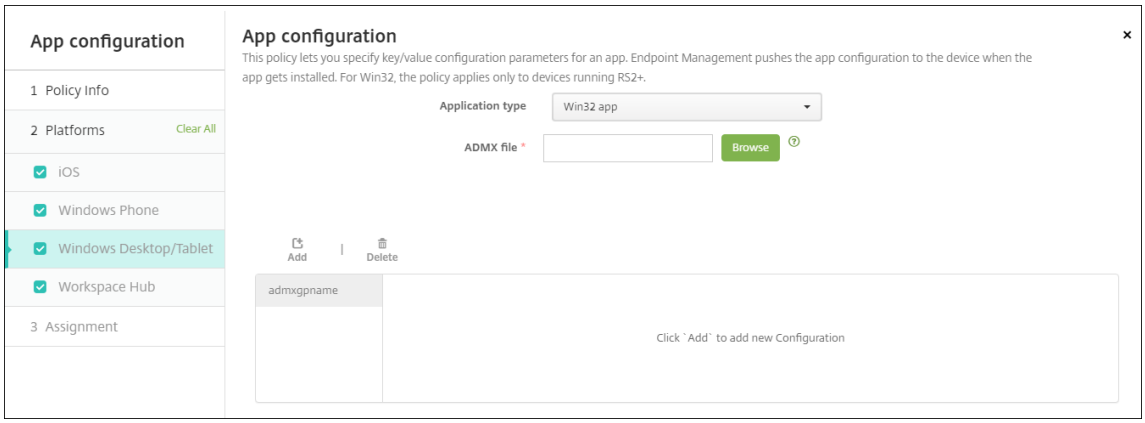
- 如果选择 **UWP** 应用程序：在做出选择列表中，单击要配置的应用程序，或单击新增向列表中添加应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



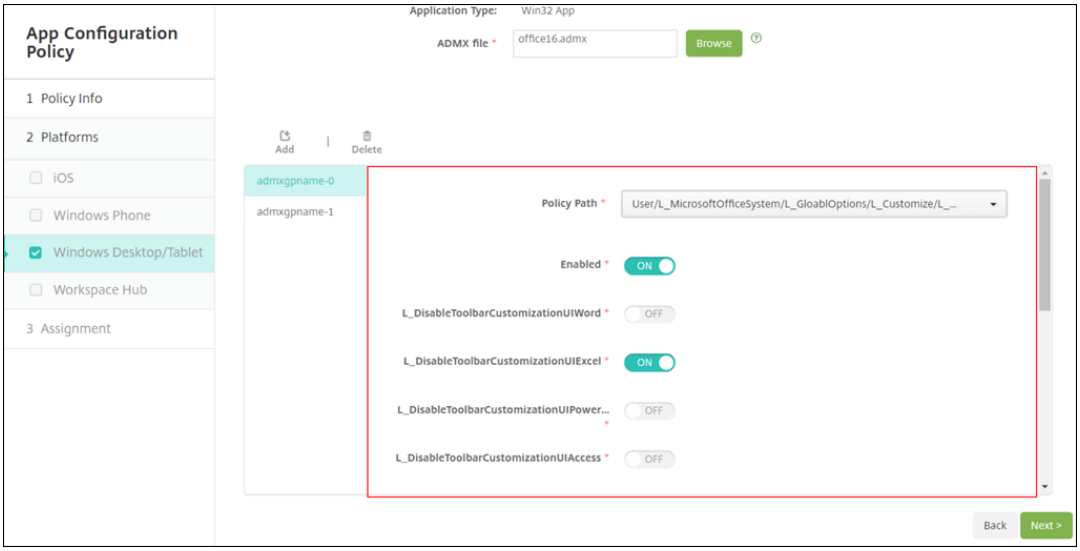
- 如果单击新增，请在显示的字段中键入软件包系列名称。
- 对于要添加的每个配置参数，单击添加，然后执行以下操作：
  - 参数名称：为 Windows 设备输入应用程序设置的键名称。有关 Windows 应用程序设置的信息，请参阅 Microsoft 文档。
  - 值：输入指定参数的值。
  - 单击添加以添加参数，或单击取消以取消添加参数。

- 如果选择 **Win32** 应用程序：单击浏览并导航到要用于配置策略的 ADMX 文件。



- 单击添加。ADMX 文件中的配置选项将在页面右侧显示。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 选择策略路径。如果多次选择相同的路径，则将强制选择与最新版本相关联的配置。
- 将启用设置为开。
- 输入所需的任何列表元素值作为键-值对。使用文本字符串 **&#xF000** 分隔每个键-值对与值对中的值和键。
- 包含小数的元素值可能需要特定范围内的值。

应用程序清单设备策略

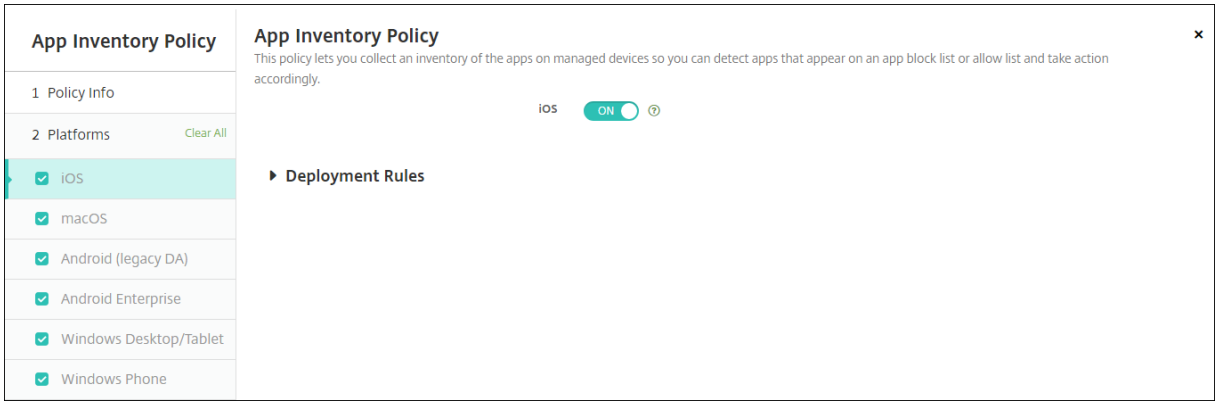
March 31, 2022

应用程序清单策略用于收集托管设备上的应用程序清单。然后，Endpoint Management 可以将清单与部署到这些设备的任何应用程序访问策略进行比较。这样一来，便可以检测应用程序允许列表或阻止列表中的应用程序，然后采取相应操作。使用应用程序访问策略可定义允许或阻止列表。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS、macOS、Android（旧版 DA）、Android Enterprise 和 Windows Desktop/Tablet



- 对于所选的每个平台，保留默认设置或将设置更改为关。默认值为开。

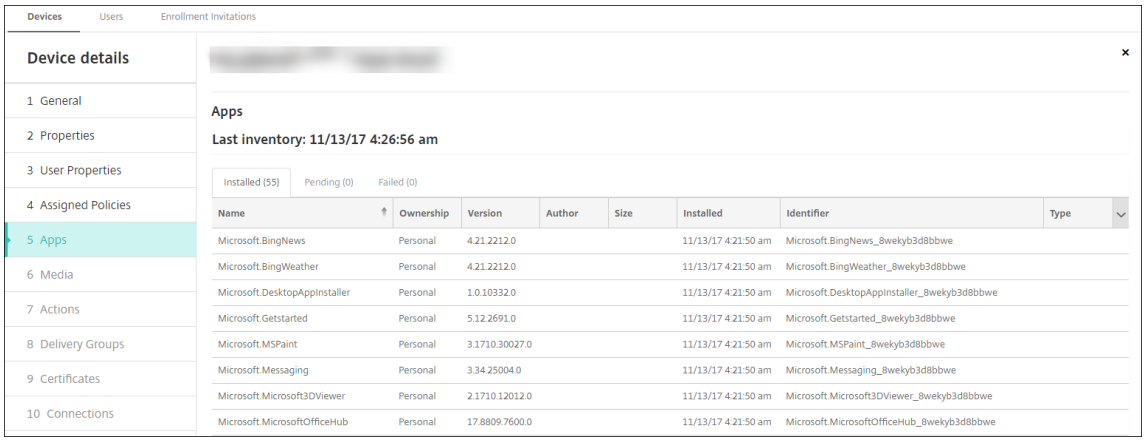
清单和删除 Win32 应用程序

您可以确定用户设备上的 Win32 应用程序是否遵守“应用程序访问”设备策略。要查看托管的 Windows 10 和 Windows 11 Desktop 和 Tablet 设备上 Win32 应用程序的清单，请执行以下操作：

1. 转至配置 > 设备策略并为 **Windows Desktop/Tablet** 平台添加“应用程序清单”策略。部署该策略。
2. 转至管理 > 设备，选择要查看的 Windows 10 和 Windows 11 设备，单击编辑，然后单击应用程序选项卡。

   此时将显示清单的结果。

   > 注意：
   >
   > 如果您正在配置 Windows 11 设备，则必须等待长达 24 小时才能获得 Microsoft 设计的准确清单结果。



3. 将应用程序清单与您的“应用程序访问”设备政策进行比较。如果设备安装了阻止列表中的应用程序，可以将其从设备中删除。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

不正确的产品代码导致的应用程序安装和卸载问题

如果为 Win32 应用程序配置了不正确的产品代码，该应用程序最初将安装，但 Microsoft 不会将应用程序状态返回到 Endpoint Management。因此：

- “应用程序卸载” 设备策略不卸载该应用程序。
- Endpoint Management 将继续部署该应用程序，因为服务器没有确认该应用程序已安装。每次部署后，设备都将生成一个错误代码，因为该应用程序已安装。管理 **>** 设备 **>** 交付组详细信息中显示的错误为：`Msi Application received: Reporting:AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

要更正产品代码，请执行以下操作：

1. 从设备中手动删除该应用程序。
2. 在 Endpoint Management 控制台中，转至配置 **>** 应用程序并更正 Win32 应用程序的产品代码。
3. 部署该 Win32 应用程序。

应用程序防护设备策略

March 30, 2022

应用程序防护策略指定 Windows Defender 应用程序防护设置。此设置包括是否启用应用程序防护和剪贴板行为的控件。

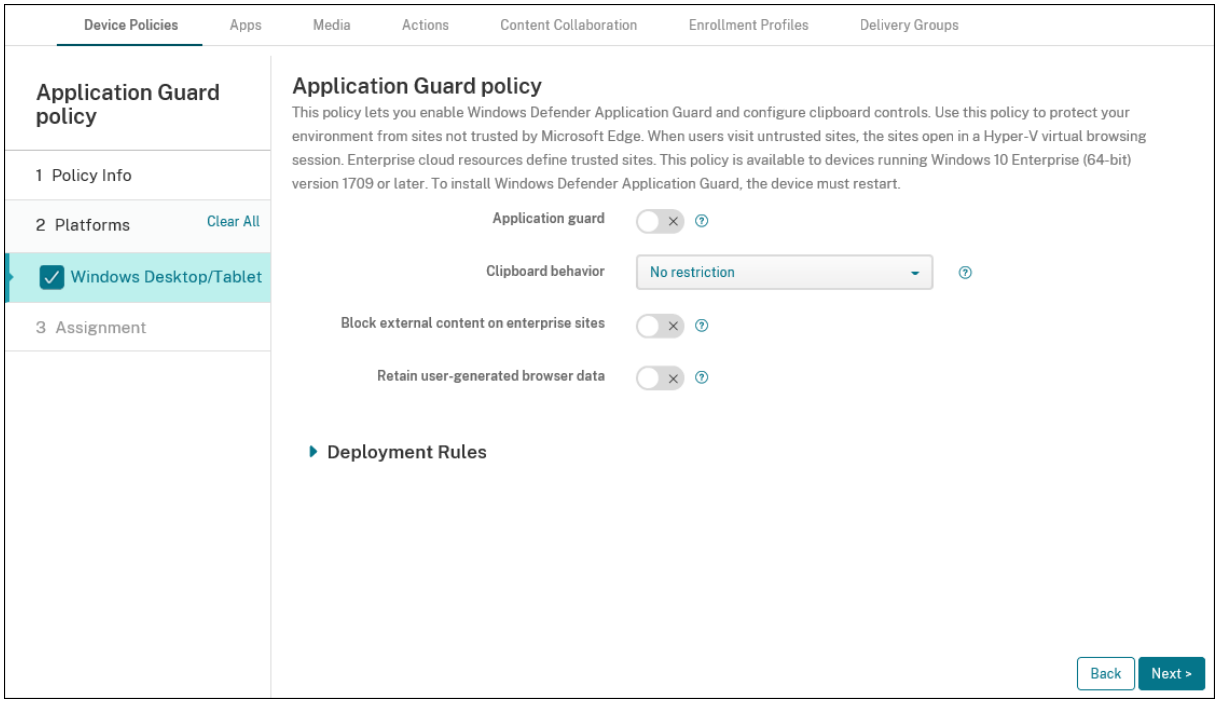
Windows Defender 应用程序防护将保护您的环境免受尚未定义为贵组织信任的站点所影响。用户访问未在您的隔离网络边界中列出的站点时：这些站点将在 Hyper-V 中的虚拟浏览会话中打开。企业云资源定义可信站点。

要求

- 运行 Windows 10 Enterprise（64 位）或 Windows 11 Enterprise（64 位）的设备。需要重新启动设备才能安装 Windows Defender 应用程序防护。
- Microsoft Edge 浏览器

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop 和 Tablet 设置



- 应用程序防护：启用应用程序防护。默认设置为关。
  - 企业云资源：逗号分隔的企业云域列表。
- 剪贴板行为：控制能够复制并粘贴的路线内容。这些选项如下所示：
  - 未配置
  - 仅允许从浏览器复制并粘贴到 **PC**：仅允许用户将内容从其浏览器复制并粘贴到 PC。
  - 仅允许从 **PC** 复制并粘贴到浏览器：仅允许用户将内容从其 PC 复制并粘贴到浏览器。
  - 允许在 **PC** 与浏览器之间复制并粘贴：允许用户在其 PC 与浏览器之间自由复制并粘贴内容。
  - 阻止在 **PC** 与浏览器之间复制并粘贴：不允许用户在其 PC 与浏览器之间复制并粘贴内容。
- 剪贴板内容：控制用户可以复制并粘贴的内容。这些选项如下所示：
  - 无限制
  - 允许复制文本：仅允许用户复制文本。
  - 允许复制图像：仅允许用户复制图像。
  - 允许同时复制文本和图像：允许用户同时复制文本和图像。
- 阻止企业站点上的外部内容：如果设置为开，Windows Defender 应用程序防护功能将阻止在企业站点上加载来自未审批站点的内容。默认设置为关。
- 保留用户生成的浏览器数据：如果设置为开，则允许保存在应用程序防护虚拟浏览会话期间创建的用户数据。此数据包括密码、收藏夹和 cookie 等内容。默认设置为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序锁定设备策略

March 31, 2022

应用程序锁定设备策略定义了以下任一应用程序的列表：

- 允许在设备上运行。
- 阻止在设备上运行。

策略的确切运行方式因支持的每个平台而异。例如，不能阻止在 iOS 设备上运行多个应用程序。

同样，对于 iOS 设备，每个策略只能选择一个 iOS 应用程序。用户只能使用其设备运行单个应用程序。在强制执行应用程序锁定设备策略时，用户无法在设备上执行除您明确允许的选项之外的任何其他活动。

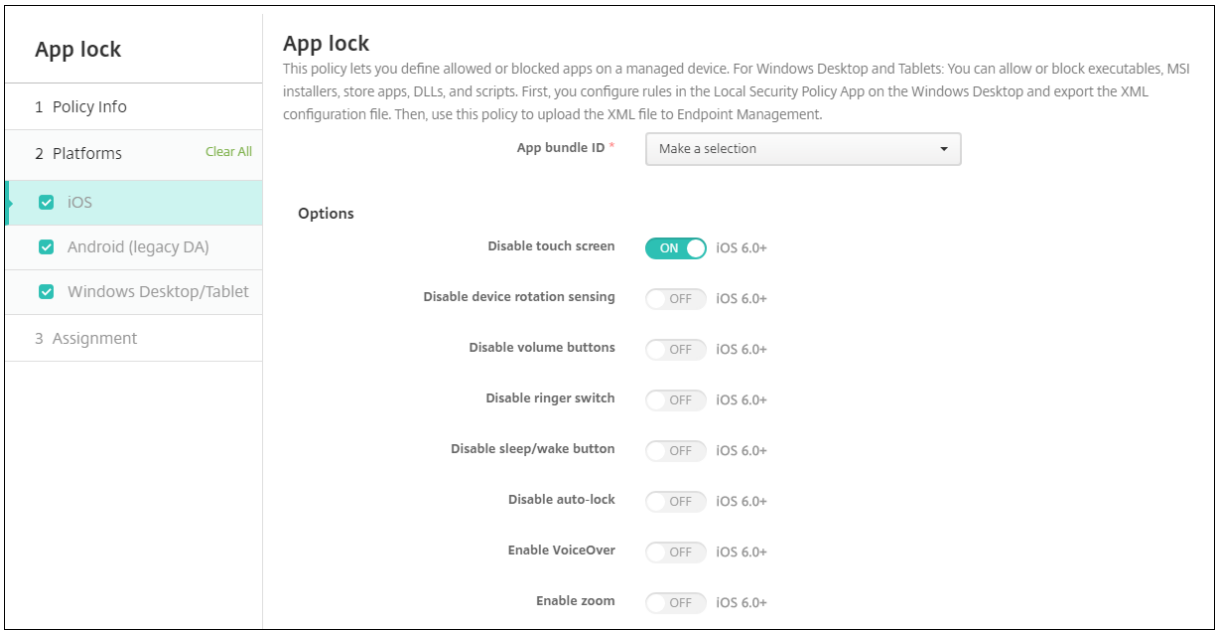
此外，必须监督 iOS 设备才能推送应用程序锁定策略。

虽然设备策略适用于大多数 Android L 和 M 设备，但是，应用程序锁定不适用于 Android N 或更高版本的设备。它不起作用，因为 Google 弃用了所需的 API。

对于托管 Windows Desktop 和 Tablet，您可以创建一个应用程序锁定设备策略，该策略定义允许列表和阻止列表中的应用程序列表。可以允许或阻止可执行文件、MSI 安装程序、应用商店应用程序、DLL 和脚本。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- 应用程序捆绑包 **ID**：在列表中，单击应用此策略的应用程序，或单击新增向列表中添加应用程序。如果选择新增，请在显示的字段中键入应用程序名称。
- 选项：对于每个选项，除禁用触摸屏默认值为开之外，默认值均为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 禁用触摸屏
  - 禁用设备旋转感应
  - 禁用音量按钮
  - 禁用铃声开关

    禁用铃声开关设置为开时，铃声行为取决于首次禁用时开关所处的位置。
  - 禁用睡眠/唤醒按钮
  - 禁用自动锁定
  - 禁用 VoiceOver
  - 启用缩放
  - 启用反转颜色
  - 启用 AssistiveTouch
  - 启用朗读所选内容
  - 启用单声道音频
  - 启用语音控制
- 用户已启用的选项：对于每个选项，默认值为关。
  - 允许 VoiceOver 调整
  - 允许缩放调整
  - 允许反转颜色调整
  - 允许 AssitiveTouch 调整
  - 允许语音控制调整
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 或更高版本。

将 **iPad** 配置为网亭

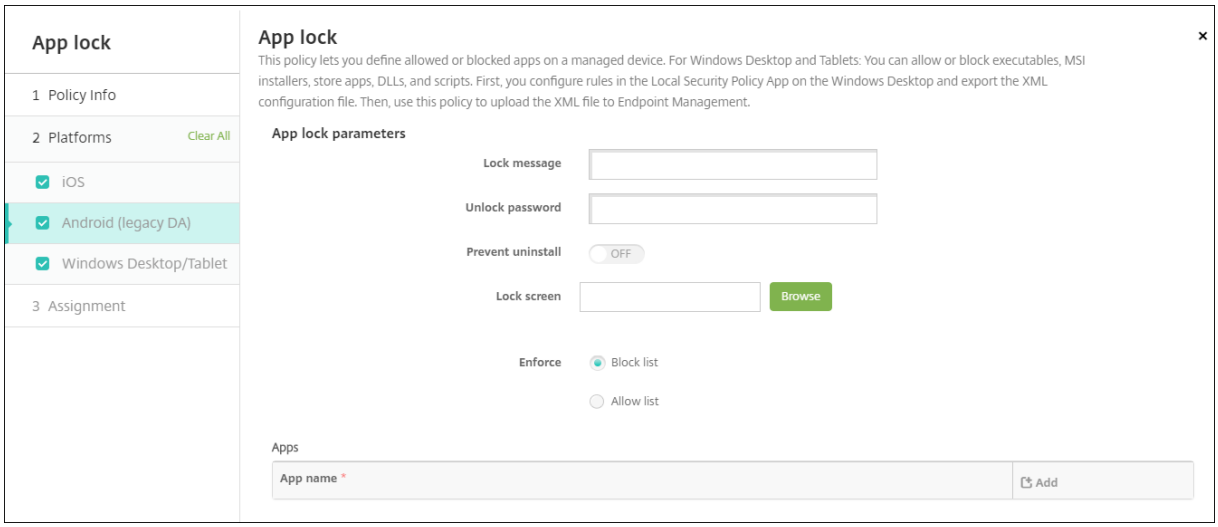
可以使用应用程序锁定设备策略运行受监督的 iPad 作为网亭。Apple 将此功能称为单应用模式。有关此功能的详细信息，请参阅 Apple 文档。在部署此策略之前，请务必部署要运行的应用程序。

1. 导航到配置 **>** 设备策略，然后单击添加。
2. 选择应用程序锁定策略。
3. 键入策略名称和可选说明。
4. 仅选择 **iOS** 平台。
5. 对于应用程序捆绑包 **ID**，请选择要在 iPad 上运行的应用程序。
6. 如前所述，配置所需的任何选项并保存策略。
7. 将策略添加到与 iPad 相同的交付组，然后部署策略。

Android（旧版 **DA**）设置

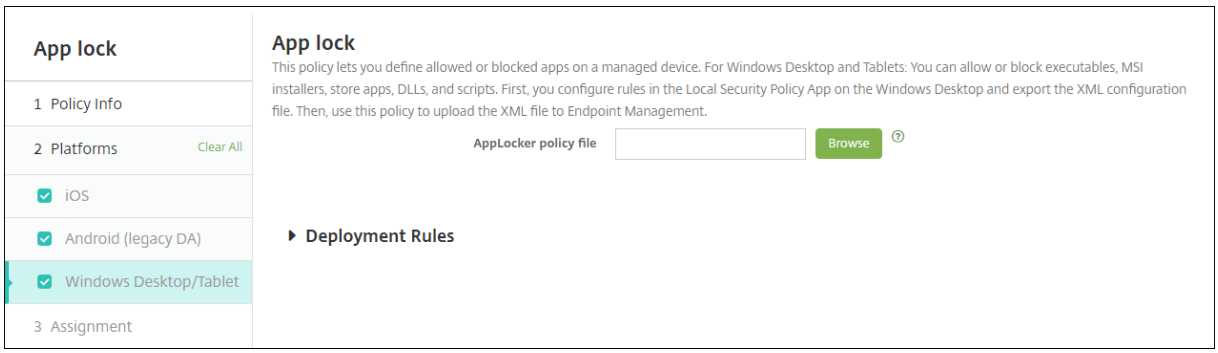
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 不能使用“应用程序锁定”设备策略阻止 Android 的“设置”应用程序。



- 应用程序锁定参数
  - 锁定消息：键入用户尝试打开锁定的应用程序时看到的消息。
  - 解锁密码：键入用于解锁应用程序的密码。
  - 阻止卸载：选择是否允许用户卸载应用程序。默认值为关。
  - 锁定屏幕：单击浏览并导航到显示在设备锁屏界面上的图像文件所在位置，选择此图像。
  - 强制执行：单击阻止列表创建不允许在设备上运行的应用程序列表。单击允许列表创建允许在设备上运行的应用程序列表。
- 应用程序：单击添加，然后执行以下操作：
  - 应用程序名称：在列表中，单击要添加到允许或阻止列表中的应用程序的名称。或者，单击新增将应用程序添加到可用应用程序列表中。
  - 如果选择新增，请在显示的字段中键入应用程序名称。
  - 单击保存或取消。
  - 为要添加到允许列表或阻止列表中的每个应用程序重复执行这些步骤。

Windows Desktop 和 Tablet 设置



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序锁定的必备条件

- 在 Windows 中，在 Windows 10 或 Windows 11 桌面上的本地安全策略编辑器中配置规则。
- 导出策略 XML 文件。Citrix 建议您在 Windows 中创建默认规则，以避免锁定默认配置或导致设备上出现问题。
- 然后，使用应用程序锁定设备策略将 XML 文件上载到 Endpoint Management。有关创建规则的详细信息，请参阅此 Microsoft 文章：https://docs.microsoft.com/en-us/windows/security/threat-protection/applocker/applocker-overview

从 **Windows** 配置和导出策略 **XML** 文件

> 重要：
>
> 通过 Windows 策略编辑器配置策略 XML 文件时，请使用“仅审核”模式。

1. 在 Windows 计算机中，启动本地安全策略编辑器。单击启动，键入本地安全策略，然后单击本地安全策略。
2. 在控制台树中，展开应用程序控制策略。
3. 单击 **AppLocker**，然后在中心窗格中，单击 **Configurerule enforcement**（配置规则强制执行）。
4. 选择已配置，然后选择强制规则。启用了某个规则时，**Enforce rules**（强制执行规则）为默认值。
5. 右键单击 **AppLocker**，单击 **Export Policy**（导出策略），然后保存 XML 文件。

> 注意：
>
> 可以创建 **Executable Rules**（可执行规则）、**Windows Installer Rules**（Windows 安装程序规则）、**Script Rules**（脚本规则）和 **Packaged App Rules**（封装应用程序规则）。为此，请右键单击文件夹，然后单击 **Create New Rule**（创建新规则）。

将策略 **XML** 文件导入 **Endpoint Management**

创建应用程序锁定策略。在应用程序锁定策略文件设置中，单击浏览并导航到 XML 文件。

停止应用 **“应用程序锁定”** 策略

在 Endpoint Management 中部署“应用程序锁定”策略后：要停止应用该“应用程序锁定”策略，请创建一个空 XML 文件。然后，创建另一个“应用程序锁定”策略，上载文件并部署该策略。启用了“应用程序锁定”的设备不受影响。首次接收该测 uede 设备未设置“应用程序锁定”策略。

应用程序通知设备策略

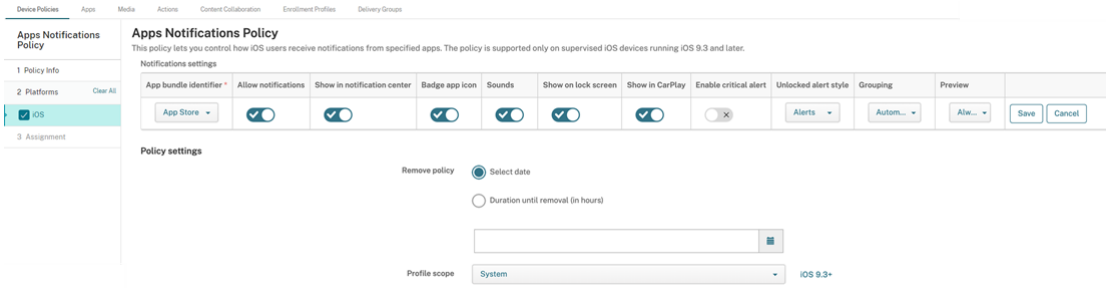
March 31, 2022

通过应用程序通知策略，您可以控制 iOS 用户如何从指定的应用程序接收通知。此策略仅在运行 iOS 9.3 或更高版本的受监督的 iOS 设备上受支持。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- **App bundle identifier**（应用程序捆绑包标识符）：指定要管理通知设置的应用程序：
  - 选择应用程序捆绑包 ID。选项仅在您启用了应用程序清单设备策略后可用，该策略将收集托管设备上的应用程序的清单。
  - 选择 **“Add new**（新增），然后键入应用程序捆绑包 ID。
    要查找应用程序捆绑包 ID，请参阅在应用商店中查找应用程序的捆绑包 ID。
- 允许通知：选择开将允许通知。
- 在通知中心中显示：选择开将在用户设备的通知中心显示通知。
- 徽章应用程序图标：选择开将在通知中显示徽章应用程序图标。
- 声音：选择开将在通知中包含声音。
- 在锁屏界面中显示：选择开将在用户设备的锁屏界面中显示通知。
- 在 **CarPlay** 中显示：选择开将在 Apple CarPlay 中显示通知。适用于 iOS 12 及以上版本。默认值为开。
- 启用严重警报：选择开，应用程序可将通知标记为忽略“请勿打扰”和铃声设置的关键通知。适用于 iOS 12 及以上版本。默认设置为关。
- 解锁的警报样式：选择无、横幅或警报来配置解锁的警报的外观。
- 预览：选择设备如何显示应用程序的通知预览。适用于 iOS 14 及更高版本。
  - **Always**（始终）：在设备锁定或解锁时显示通知预览。
  - **When Unlocked**（解锁时）：仅在设备解锁时显示通知预览。
  - **Never**（从不）：在设备上关闭通知预览。
- **Grouping**（分组）：选择设备如何对来自应用程序的通知进行分组。适用于设备 iOS 12 及更高版本。
  - **Automatic**（自动）：将通知分组到应用程序指定的组中。
  - **By app**（按应用程序）：将来自应用程序的通知分组为一个组中。
  - **Off**（关）：关闭应用程序的通知分组。设备按顺序显示所有通知。
- 策略设置
  - 删除策略：选择计划删除策略的方法。选项包括以下内容：
    * 选择日期：单击日历可选择具体删除日期。
    * 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。适用于 iOS 6.0 或更高版本。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。适用于 iOS 9.3 及更高版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序限制设备策略

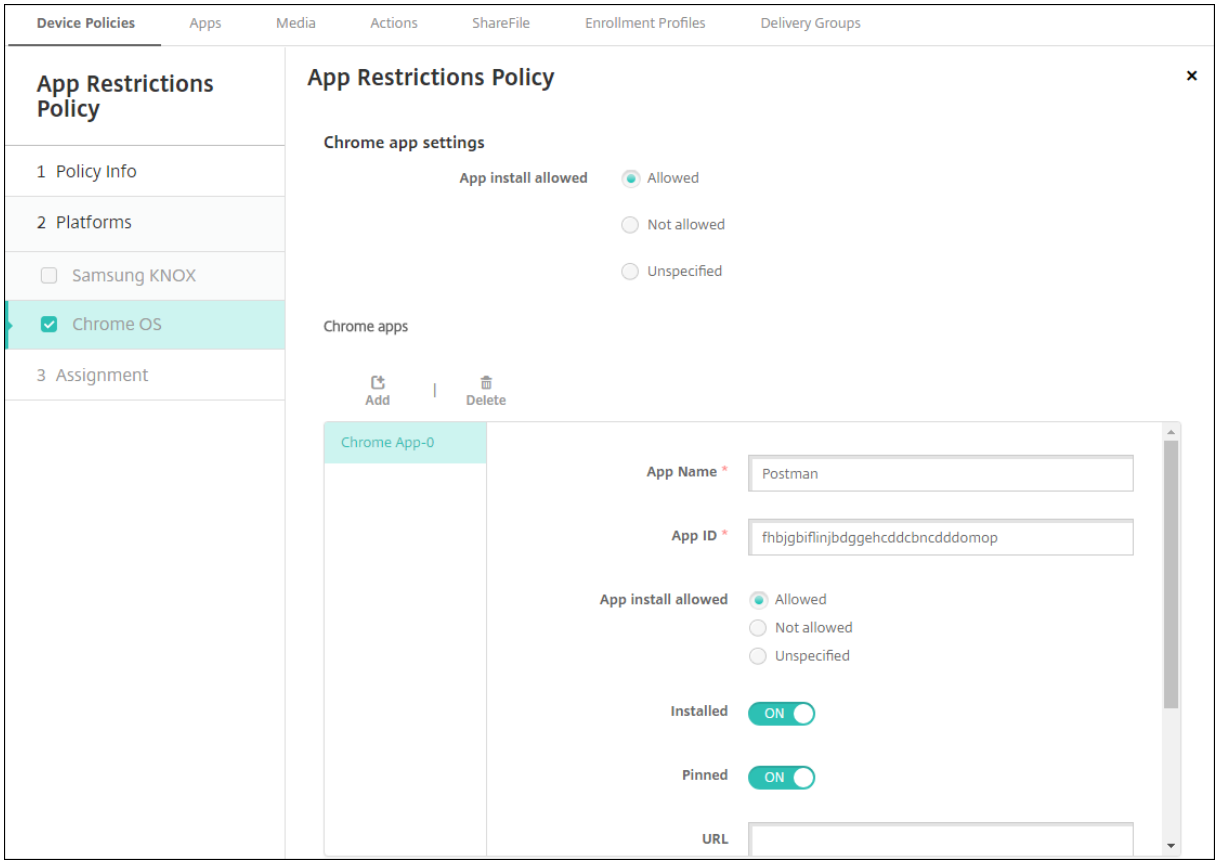
November 7, 2022

您可以使用“应用程序限制”设备策略来指定允许或阻止的 Chrome 应用程序，以及在 Chrome OS 应用程序上运行的 Android 应用程序。如果在“限制”设备策略中启用了 App Runtime for Chrome (ARC)，请在“应用程序限制”设备策略中的 **Android** 应用程序下配置 Android 应用程序限制。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Chrome 应用程序设置

Chrome 应用程序同时属于应用程序和扩展。



- 允许安装的应用程序：允许或阻止在 Chrome OS 设备上安装所有 Chrome 应用程序的一项全局设置。如果选择允许，则可以创建特定阻止应用程序的列表。如果选择不允许，则可以创建特定允许应用程序的列表。为此，请单击 **Chrome** 应用程序下的添加。要使用在您的 Chrome 帐户中指定的设置，请选择未指定。默认值为允许。
- **Chrome** 应用程序：要添加作为允许安装的应用程序设置选项的例外的 Chrome 应用程序，请单击添加，然后指定以下设置：
  - 应用程序名称：用于在 Endpoint Management 控制台中标识应用程序的名称。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 应用程序 **ID**：Chrome 应用程序的唯一标识符。请勿包括前缀 “app:”。

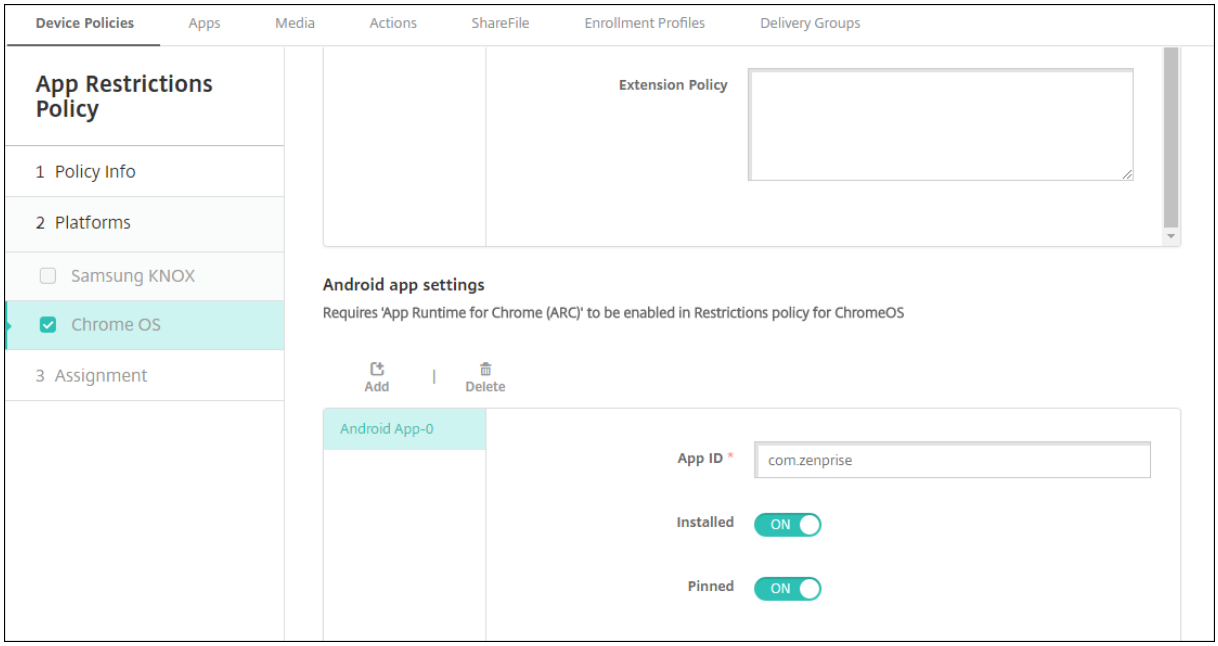
要查找 Chrome 应用程序 ID，请访问 Chrome 网上应用店。然后，搜索该应用程序。单击该应用程序以在地址栏中查看 URL 和应用程序 ID。地址的最后一个部分为应用程序 ID。例如，如果 URL 为 `https://chrome.google.com/webstore/detail/example/abcdefghijkl`，则应用程序 ID 为 `abcdefghijkl`。

只能从 Chromebook 中查找 Chrome 应用程序。可以从任何平台中查找 Chrome 扩展。

- 允许安装的应用程序**:** 创建上述全局设置的例外。此设置允许或阻止指定的 Chrome 应用程序。
- 已安装：如果设置为开，则强制为已注册的 Chrome OS 设备用户安装 Chrome 应用程序。如果设置为关，并且某个应用程序已安装，则将卸载该应用程序。如果设置为关，并且该应用程序不再通过策略配置，则该应用程序将保持安装。默认设置为关。
- 已固定：如果设置为开，则将该应用程序固定到 Chromebook 任务栏。默认设置为关。
- **URL**：指定用户可以从中下载未在 Chrome 网上应用店中托管的应用程序的 URL。
- 扩展策略：以 JSON 格式定义此应用程序定义的应用程序特定策略。有关信息，请参阅存储区域的清单。

Android 应用程序设置

要允许已注册的 Chrome OS 设备用户运行 Android 应用程序，请按下部分内容 “允许已注册的 Chrome OS 设备用户运行 Android 应用程序” 中所述配置 “限制” 设备策略。要配置 ARC 应用程序限制，请在 Android 应用程序下单击添加，然后指定以下设置。



- 应用程序 **ID**：Chrome OS 上运行的 Android 应用程序的唯一应用程序标识符。例如：com.android.camera。请勿包括前缀 “app:”。

  要查找 Android 应用程序 ID，请访问 Google Play 应用商店。然后，搜索该应用程序。单击该应用程序以在地址栏中查看应用程序 ID。**id=** 后面的部分为应用程序 ID。例如，如果 URL 为 `https://play.google.com/store/apps/details?id=com.citrix.mail`，则应用程序 ID 为 **id=com.citrix.mail**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 已安装：指定是否强制为已注册的 Chrome OS 设备用户安装 Android 应用程序。如果设置为关，并且某个应用程序已安装，则将卸载该应用程序。如果设置为关，并且该应用程序不再通过策略配置，则该应用程序将保持安装。默认设置为关。
- 已固定：如果设置为开，则将 Android 应用程序固定到 Chromebook 任务栏。默认设置为关。

允许已注册的 **Chrome OS** 设备用户运行 **Android** 应用程序

要允许已注册的 Chrome OS 设备用户运行 Android 应用程序，请执行以下操作：转至配置 **>** 设备策略，然后为启用了设置启用 **App Runtime for Chrome (ARC)** 的 Chrome OS 添加“限制”设备策略。

- 启用 **App Runtime for Chrome (ARC)**：如果设置为开，则允许已注册的 Chrome OS 设备用户运行 Android 应用程序。在“应用程序限制”设备策略中指定 ARC 应用程序。需要 Google Workspace Chrome 配置。如果在当前用户会话中启用了短暂模式或多点登录，ARC 将不可用。如果设置为关，企业 Chrome OS 设备用户将无法运行 Android 应用程序。默认值为开。

应用程序卸载设备策略

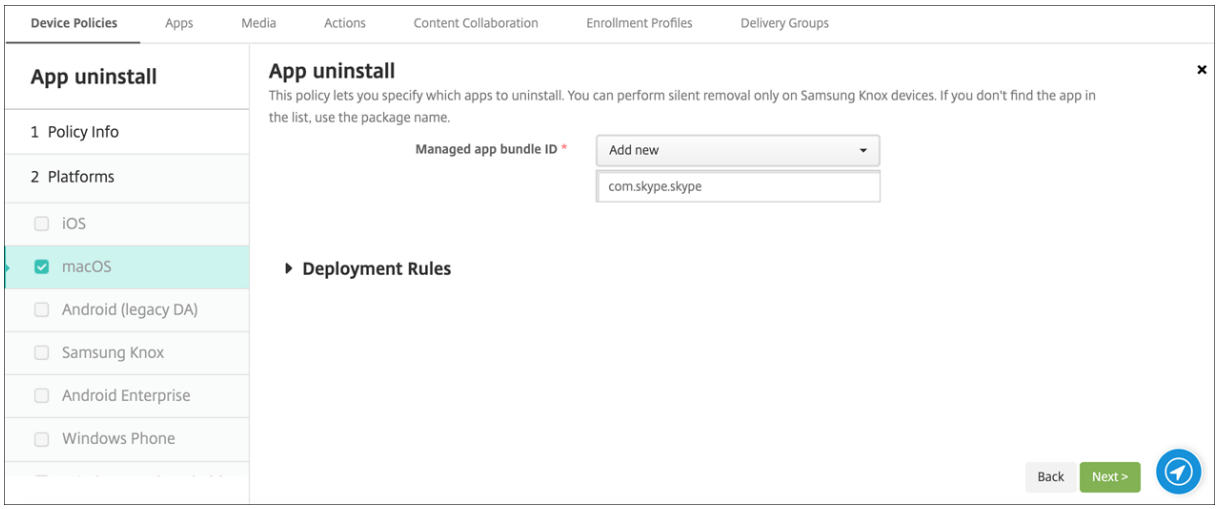
November 7, 2022

“应用程序卸载”策略允许您从用户设备中删除应用程序。如果您不想再支持某个应用程序，或者希望将其替换为来自其他供应商的类似应用程序，则可以将其删除。

将此策略部署到用户设备时，用户会收到卸载应用程序的提示，然后删除该应用程序。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 和 **macOS** 设置



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 托管应用程序捆绑包 **ID**：在列表中，选择现有的托管应用程序或者添加新应用程序。如果没有为此平台配置任何应用程序，则列表为空，您必须添加新的托管应用程序。选择 **Add new**（新增）时，将出现一个字段，您可以在其中键入托管应用程序的名称。适用于 iOS 5.0 及更高版本以及 macOS 11.0 及更高版本。

Android（旧版 **DA**）、**Android Enterprise** 和 **Windows Desktop/Tablet** 设置

- 要卸载的应用程序：对于您要添加的每个应用程序，单击添加，然后执行以下操作：
  - 应用程序名称：在列表中，单击现有应用程序，或单击新增输入新的应用程序名称。如果此平台没有配置应用程序，该列表是空的，您必须添加新的应用程序。
  - 单击添加以添加应用程序，或单击取消以取消添加应用程序。

对于 Android Enterprise 应用程序，还可以启用应用程序清单设备策略。请参阅应用程序清单设备策略。

在安装相应的公共应用商店应用程序后自动卸载企业应用程序

可以将 Endpoint Management 配置为在安装公共应用商店版本时删除 Citrix 应用程序的企业版本。此功能可防止用户设备在安装公共应用商店版本后具有两个相同的应用程序图标。

“应用程序卸载”设备策略的部署条件将触发 Endpoint Management 在安装新版本时从用户设备中删除较旧的应用程序。此功能仅适用于在企业模式 (XME) 下连接到 Endpoint Management 服务器的托管 iOS 设备。

要通过“已安装应用程序的名称”条件配置一条部署规则，请执行以下操作：

- 指定企业应用程序的托管应用程序捆绑包 **ID**。
- 添加规则：单击新建规则，然后（如示例中所示）选择已安装应用程序的名称和等于。键入公共应用商店应用程序的应用程序捆绑包 ID。

在示例中，公共应用商店应用程序 (com.citrix.mail.ios) 安装在指定交付组中的设备上时，Endpoint Management 将删除企业版本 (com.citrix.mail)。

应用程序卸载限制设备策略

July 8, 2022

可以指定用户可以或不能在 Amazon 设备上卸载的应用程序。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Amazon 设置

- 应用程序卸载限制设置：对于要添加的每个应用程序规则，单击添加，然后执行以下操作：
  - 应用程序名称：在列表中，单击某个应用程序，或单击新增以添加新应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

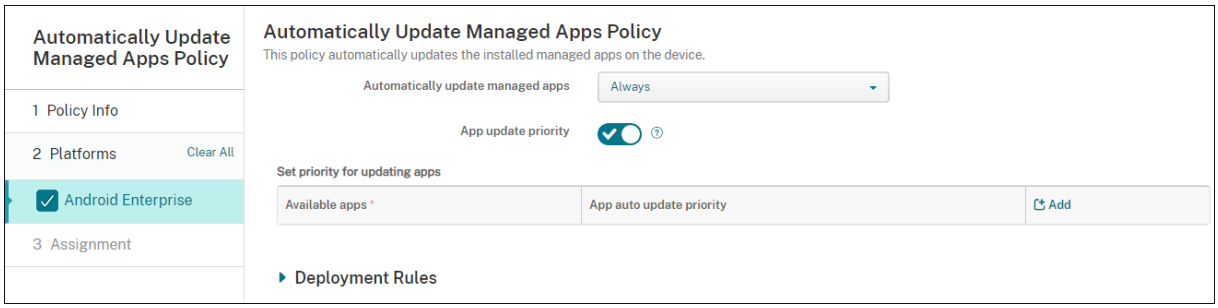
- 规则：选择用户是否可以卸载应用程序。默认值为允许卸载。
- 单击保存或取消。

自动更新托管应用程序设备策略

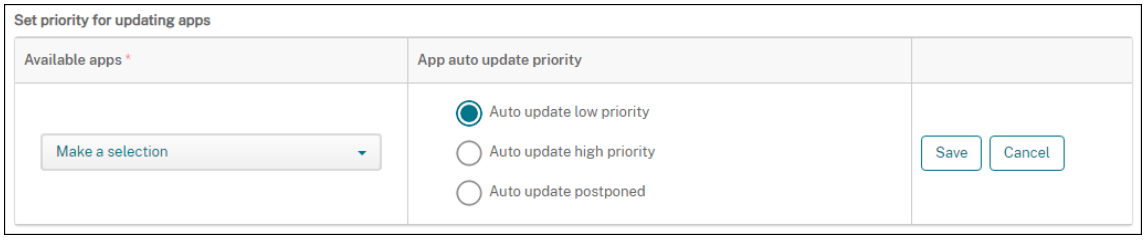
May 6, 2022

此策略控制 Android Enterprise 设备上安装的托管应用程序的更新方式。可以限制用户允许自动更新其设备上的应用程序的能力。如果您允许用户控制其设备上的应用程序的自动更新，这些用户会在托管 Google Play 应用商店中设置自动应用程序更新策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。



- 自动更新托管应用程序
  - 始终：启用自动应用程序更新。始终为默认设置。
  - 允许用户配置策略：允许用户在托管 Google Play 应用商店中为设备配置自动应用程序更新策略。
  - 从不：禁用自动应用程序更新。
  - 仅当设备连接到 **Wi-Fi** 时：仅当设备连接到 Wi-Fi 时，才允许自动更新应用程序。
- **App update priority**（应用程序更新优先级）：如果设置为开，则可以为每个托管应用程序配置更新优先级。
- **Set priority for updating apps**（设置更新应用程序的优先级）：单击 **Add**（添加）可配置应用程序的更新优先级。



（应用程序更新优先级配置）

  - **Available apps**（可用应用程序）：从菜单中选择一个应用程序以配置更新优先级。
  - **App auto-update priority**（应用程序自动更新优先级）：从以下选项中选择更新优先级：
    - **Auto update low priority**（自动更新低优先级）：当设备正在充电（而非主动使用）并连接到不按流量计费的网络时，应用程序将更新。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * **Auto update high priority**（自动更新高优先级）：应用程序在没有限制的情况下尽快更新。
    * **Auto update postponed**（自动更新已推迟）：在新版本可用后最长 90 天内，不会自动更新应用程序。90 天后，应用程序以低优先级自动更新。应用程序更新后，在另一个 90 天内该应用程序不会自动更新。用户可以随时手动更新应用程序。
  - 完成时单击 **Save**（保存）。可以通过单击铅笔图标编辑配置。通过单击垃圾桶删除配置。

BitLocker 设备策略

March 31, 2022

Windows 10 和 Windows 11 中包括一项名为 BitLocker 的磁盘加密功能，该功能提供针对丢失或被盗的 Windows 设备的未授权访问的额外文件和系统保护。要获取更多保护，可以对受信任的平台模块 (TPM) 芯片版本 1.2 或更高版本使用 BitLocker。TPM 芯片处理加密操作、生成和存储加密密钥以及限制对加密密钥的使用。

自 Windows 10 Build 1703 起，MDM 策略可以控制 BitLocker。可以在 Endpoint Management 中使用 BitLocker 设备策略配置在 Windows 10 和 Windows 11 设备上的 BitLocker 向导中可用的设置。例如，在启用了 BitLocker 的设备上，BitLocker 会提示用户使用多个选项：

- 希望如何在启动时解锁其设备
- 如何备份其恢复密钥
- 如何解锁固定驱动器。

BitLocker 设备策略还配置是否：

- 在没有 TPM 芯片的设备上启用 BitLocker。
- 在 BitLocker 界面中显示恢复选项。
- 拒绝在未启用 BitLocker 时对固定驱动器或可移动驱动器的写入访问。
- 安全地保存加密的 BitLocker 恢复密钥，以便用户在忘记或放错密钥时访问该密钥。此密钥可在自助门户网站上找到。

> 注意
>
> BitLocker 加密在设备上启动后，您将无法通过部署更新后的 BitLocker 设备策略来更改设备上的 BitLocker 设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

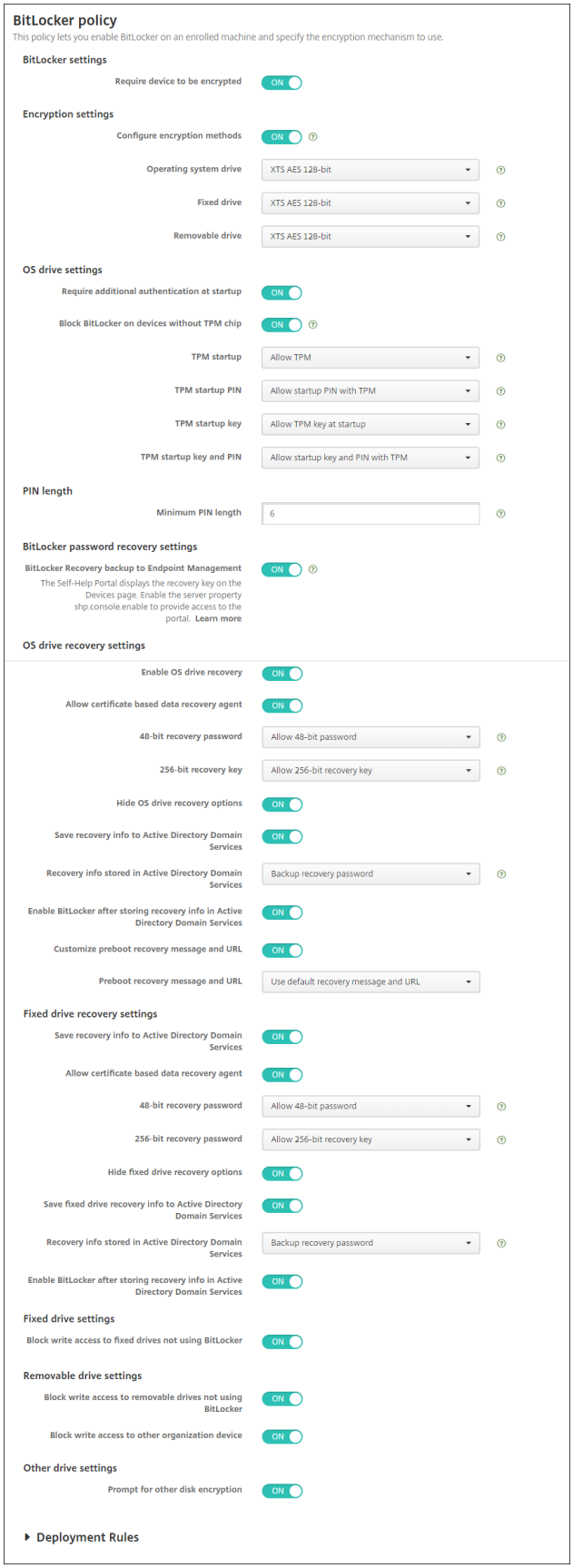
要求

- BitLocker 设备策略需要 Windows 10 Enterprise 或 Windows 11 Enterprise Edition。
- 部署 BitLocker 设备策略之前，请准备您的环境以便使用 BitLocker。有关 Microsoft 提供的详细信息（包括 BitLocker 系统要求和设置），请参阅 BitLocker 中的文章。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop 和 Tablet 设置



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Bitlocker** 设置
  - 要求加密设备：确定是否提示用户在 Windows Desktop 或 Tablet 上启用 BitLocker 加密。如果设置为开，设备将在注册完成后显示一条消息，指出企业要求设备加密。如果设置为关，系统将不提示用户，并且 BitLocker 将使用策略设置。默认值为关。
- 加密设置
  - 配置加密方法：确定要对特定设备类型使用的加密方法。如果设置为关，BitLocker 向导将提示设备用户指定要对某种驱动器类型使用的加密方法。所有驱动器的加密方法都默认为 XTS-AES 128 位。可移动驱动器的加密方法默认为 AES-CBC 128 位。如果设置为开，BitLocker 将使用在策略中指定的加密方法。如果设置为开，将显示以下额外的设置：操作系统驱动器、固定驱动器和可移动驱动器。选择每种驱动器类型的默认加密方法。默认值为关。
- 操作系统驱动器设置
  - 启动时需要额外的身份验证：指定在设备启动过程中需要额外进行一次身份验证。此外，还指定是否允许在没有 TPM 芯片的设备上启用 BitLocker。如果设置为关，没有 TPM 的设备将无法使用 BitLocker 加密。有关 TPM 的信息，请参阅 Microsoft 文章 Trusted Platform Module Technology Overview（受信任的平台模块技术概览）。如果设置为开，将显示以下额外的设置。默认值为关。
  - 在没有 **TPM** 芯片的设备上阻止 **BitLocker**：在没有 TPM 芯片的设备上，BitLocker 要求用户创建解锁密码或启动密钥。启动密钥存储在 USB 驱动器中，用户必须在启动之前将该驱动器连接到设备。解锁密码最少包含 8 个字符。默认值为关。
  - **TPM** 启动：在配备了 TPM 的设备上，存在四种解锁模式：“仅 TPM”、“TPM + PIN”、“TPM + 密钥”以及“TPM + PIN + 密钥”。TPM 启动面向“仅 TPM”模式，在该模式下，加密密钥存储在 TPM 芯片中。此模式不要求用户提供额外的解锁数据。用户设备在重新启动过程中使用 TPM 芯片中的加密密钥自动解锁。默认值为允许 **TPM**。
  - **TPM** 启动 **PIN**：此设置为“TPM + PIN”解锁模式。PIN 最多可以包含 20 个数字。使用最小 **PIN** 长度设置可指定最小 PIN 长度。用户将在 BitLocker 设置过程中配置 PIN，并在设备启动过程中提供 PIN。
  - **TPM** 启动密钥：此设置为“TPM + 密钥”解锁模式。启动密钥存储在 USB 或其他可移动驱动器中，用户必须在启动之前将该驱动器连接到设备。
  - **TPM** 启动密钥和 **PIN**：此设置为“TPM + PIN + 密钥”解锁模式。

    如果解锁成功，操作系统将开始加载。否则，设备将进入恢复模式。
- **PIN** 长度
  - 最小 **PIN** 长度：TPM 启动 PIN 的最小长度。默认值为 **6**。
- **BitLocker** 密码恢复设置
  - **BitLocker Recovery backup to Endpoint Management**（BitLocker 恢复备份到 Endpoint Management）：如果启用了此选项，必须解锁其设备的用户可以在自助门户网站上找到其 BitLocker 恢复密钥。Endpoint Management 管理员看不到用户的 BitLocker 恢复密钥。有关查看 BitLocker 恢复密钥的详细信息，请参阅 BitLocker 恢复密钥。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 操作系统驱动器恢复设置：为用户配置用于 BitLocker 加密的固定驱动器的恢复选项。
  - 启用操作系统驱动器恢复：如果解锁步骤失败，BitLocker 将提示用户提供已配置的恢复密钥。此设置将配置对用户可用的操作系统驱动器恢复选项（如果用户没有解锁密码或 USB 启动密钥）。默认设置为关。
  - 允许基于证书的数据恢复代理：指定是否允许启用基于证书的数据恢复代理。从公钥策略中添加数据恢复代理，该代理位于组策略管理控制台 (GPMC) 或本地组策略编辑器中。有关数据恢复代理的详细信息，请参阅 Microsoft 文章 BitLocker Group Policy settings（BitLocker 组策略设置）。默认设置为关。
  - **48** 位恢复密码：指定是否允许或要求用户使用恢复密码。BitLocker 生成密码并将其存储在文件中或 Microsoft 云帐户中。默认值为允许 **48** 位密码。
  - **256** 位恢复密钥：指定是否允许或要求用户使用恢复密钥。恢复密钥为 BEK 文件，该文件存储在 USB 驱动器中。默认值为允许 **256** 位恢复密钥。
  - 隐藏操作系统驱动器恢复选项：指定在 BitLocker 界面中显示还是隐藏恢复选项。如果设置为开，则不在 BitLocker 界面中显示任何恢复选项。在这种情况下，请将设备注册到 Active Directory 中，将恢复选项保存到 Active Directory 中，并将将恢复信息保存到 **AD DS** 中设置为开。默认设置为关。
  - 将恢复信息保存到 **Active Directory** 域服务中：指定是否将恢复选项保存到 Active Directory 域服务中。默认设置为关。
  - 存储在 **Active Directory** 域服务中的恢复信息：指定在 Active Directory 域服务中存储 BitLocker 恢复密码还是恢复密码和密钥包。存储密钥包将支持从物理损坏的驱动器中恢复数据。默认值为备份恢复密码。
  - 将恢复信息存储到 **Active Directory** 域服务后启用 **BitLocker**：指定是否阻止用户启用 BitLocker，但设备已连接到域，并且 BitLocker 恢复信息已成功备份到 Active Directory 时除外。如果设置为开，设备必须在启动 BitLocker 之前加入域。默认设置为关。
  - 预引导恢复消息和 **URL**：指定 BitLocker 是否在恢复屏幕上显示自定义的消息和 URL。如果设置为开，将显示以下额外的设置：使用默认恢复消息和 **URL**、使用空恢复消息和 **URL**、使用自定义恢复消息、使用自定义恢复 **URL** 和使用 **Endpoint Management** 恢复消息和 **URL**。如果设置为关，将显示默认恢复消息和 URL。默认设置为关。
- 固定驱动器恢复设置：为用户配置用于 BitLocker 加密的固定驱动器的恢复选项。BitLocker 不向用户显示与固定驱动器加密有关的消息。要在启动过程中解锁驱动器，用户需要提供密码或智能卡。用户在固定驱动器上启用了 BitLocker 加密时，启动解锁设置（不在此策略中）将在 BitLocker 界面上显示。有关相关设置的信息，请参阅此列表中前面部分的配置操作系统驱动器恢复。默认设置为关。
- 固定驱动器设置
  - 阻止对不使用 **BitLocker** 的固定驱动器进行写入访问：如果设置为开，则仅当固定驱动器通过 BitLocker 加密时，用户才能向这些驱动器写入数据。默认设置为关。
- 可移动驱动器设置
- 阻止对不使用 **BitLocker** 的可移动驱动器进行写入访问：如果设置为开，则仅当可移动驱动器通过 BitLocker 加密时，用户才能向这些驱动器写入数据。请根据贵组织是否允许在其他组织可移动的驱动器上具有访问权限来

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置此设置。默认设置为关。

- 阻止对其他组织设备进行写入访问：如果设置为开，则用户无法写入其组织中的其他设备，例如网络驱动器。
- 其他驱动器设置
- 其他磁盘加密提示：允许您禁用对设备上的其他磁盘加密的警告提示。默认值为关。

“蓝牙”设备策略

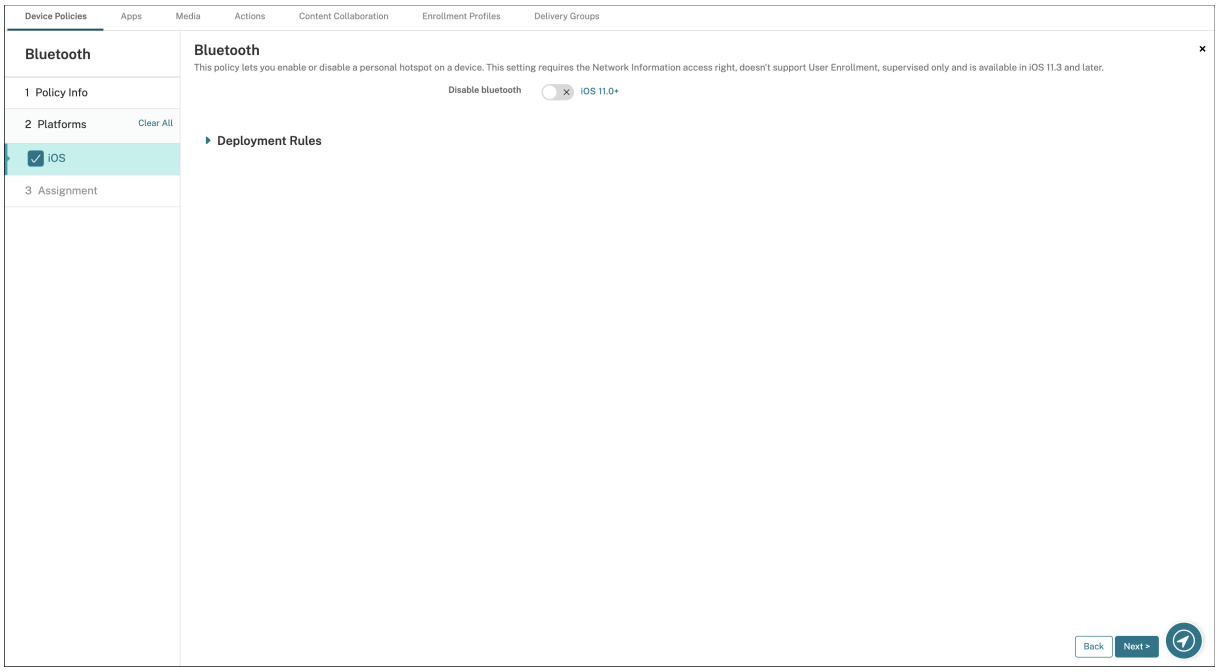
March 31, 2022

可以在受监督的 iOS 设备上配置蓝牙策略以启用或禁用蓝牙。

此设置需要“网络信息”访问权限，不支持用户注册，并且在 iOS 11.3 及更高版本中可用。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- **Disable Bluetooth**（禁用蓝牙）：允许您在受监督的设备上禁用或启用蓝牙。

日历 **(CalDav)** 设备策略

March 31, 2022

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可以在 Endpoint Management 中添加一个设备策略，用于向用户的 iOS 或 macOS 设备添加日历 (CalDAV) 帐户，使用户可以将其计划数据与任何支持 CalDAV 的服务器同步。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CalDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CalDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。
- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 或更高版本。

macOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CalDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CalDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。
- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

手机网络设备策略

March 31, 2022

此策略允许您在 iOS 设备上配置手机网络设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

可以在非字符串字段（例如代理服务器端口）中使用宏。

例如，您可以使用 `${ device.xyz }` 或 `${ setting.xyz }` 等宏，这将扩展到整数。还可以通过 “导入 iOS 和 macOS 配置文件” 设备策略在您导入到 Endpoint Management 的设备配置 XML 文件中使用宏。

- 附加 **APN**
  - 名称：此配置的名称。
  - 身份验证类型：在清单上，单击 “质询握手身份验证协议” (**CHAP**) 或密码身份验证协议 (**PAP**)。默认值为 **PAP**。
  - 用户名和密码：用于身份验证的用户名和密码。
- **APN**
  - 名称：接入点名称 (APN) 配置的名称。
  - 身份验证类型：在列表中，单击 **CHAP** 或 **PAP**。默认值为 **PAP**。
  - 用户名和密码：用于身份验证的用户名和密码。
  - 代理服务器：代理服务器网络地址。
  - 代理服务器端口：代理服务器端口。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。

连接计划设备策略

July 24, 2023

> 重要：
>
> Citrix 建议您使用 Firebase Cloud Messaging (FCM) 来控制从 Android 和 Android Enterprise 设备到 Endpoint Management 的连接。有关使用 FCM 的信息，请参阅 Firebase Cloud Messaging。

如果选择不使用 FCM，可以创建连接计划策略，用于控制用户设备如何及何时连接到 Endpoint Management。如果选择使用 FCM，还必须创建连接计划策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可以指定用户需要手动连接其设备或设备在定义的时间范围内进行连接。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Android 和 **Android Enterprise** 设置

- 需要连接设备：单击要为此计划设置的选项。
  - 从不：手动进行连接。用户必须从其设备上的 Endpoint Management 启动连接。Citrix 建议不要对生产部署使用此选项，因为这会阻止您将安全策略部署到设备，这意味着用户绝不会收到任何新应用程序或策略。默认情况下，从不选项处于启用状态。
  - 每隔：按照指定间隔进行连接。如果此选项生效，则当您发送锁定或擦除等安全策略时，Endpoint Management 将在下次设备连接时在设备上处理该操作。选择此选项后，将显示每隔 **N** 分钟连接一次字段，您必须在其中输入设备必须进行重新连接的间隔分钟数。默认值和最小值为 **120**。
  - 定义计划：用户设备上的 Endpoint Management 尝试在网络连接断开后重新连接到 Endpoint Management 服务器。Endpoint Management 通过在您定义的时间范围内定期传输控制数据包来监视连接。有关如何定义连接时间范围的信息，请参阅下文中的 “定义连接的时间范围”。
    - 要求每个范围内存在一个连接：在定义的任一时间范围内用户设备必须至少连接一次。
    - 使用本地设备时间而非 **UTC**：将定义的时间范围与本地设备时间而非协调世界时 (UTC) 同步。

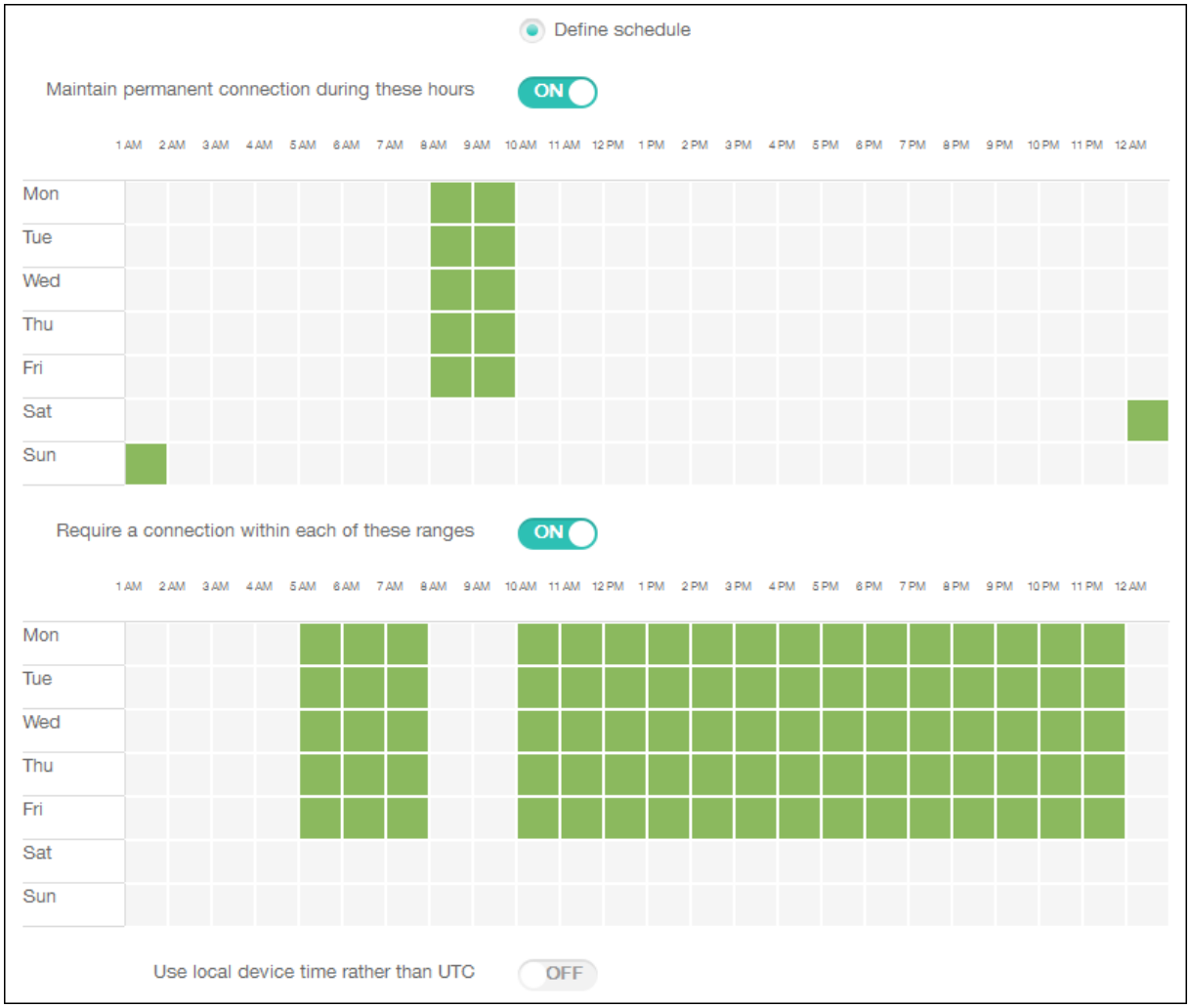
定义连接的时间范围

启用下列选项时，将显示一个时间表，您可以利用此时间表设置所需的时间范围。您可以启用其中一个选项，也可以同时启用两个选项，以满足在指定时间需要永久连接或在特点时限内需要连接的需求。时间线中的每个方块为 1 小时。要指定在每个工作日的上午 8:00 到上午 9:00 之间连接，请单击时间表中每个工作日上午 8:00 到上午 9:00 之间的正方形。

例如，下图中的两个时间线需要：

- 每个工作日上午 8:00 至上午 10:00 之间的永久连接
- 星期六凌晨 1:00 至星期日凌晨 2:00 之间的永久连接
- 每个工作日凌晨 5:00 至上午 8:00 或上午 10:00 至正午 12:00 之间至少建立一个连接

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



联系人 **(CardDAV)** 设备策略

March 31, 2022

可以在 Endpoint Management 中添加一个设备策略，用于向用户的 iOS 或 macOS 设备添加 iOS 联系人 (CardDAV) 帐户，使用户可以将其联系人数据与任何支持 CardDAV 的服务器同步。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CardDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CardDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。

macOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CardDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CardDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。
- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

内容设备策略

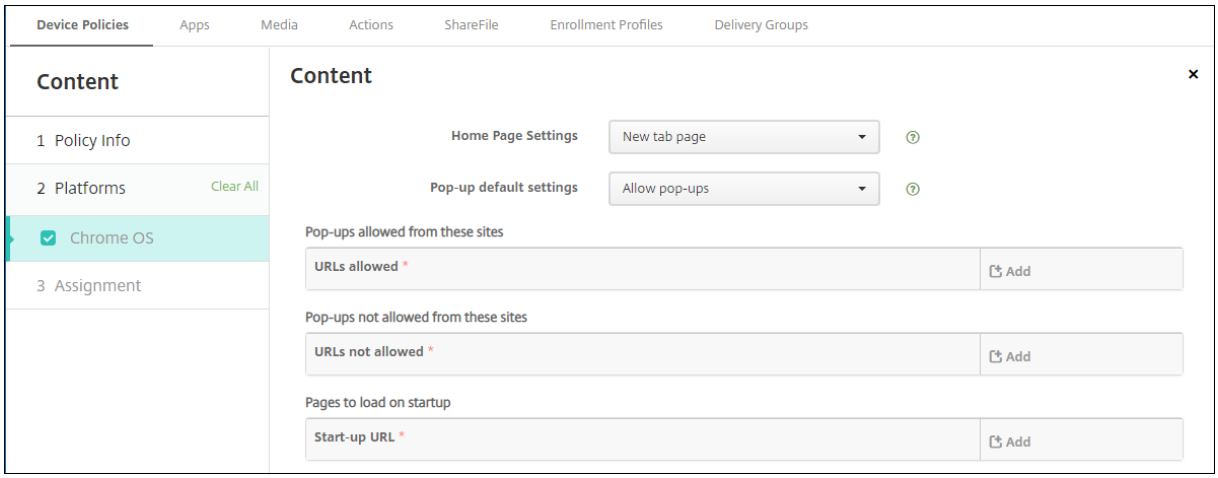
March 31, 2022

您可以控制 Chrome 操作系统的各种 Web 内容选项，包括要显示的主页以及如何处理弹出窗口。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Chrome OS 设置



- **Home Page Settings**（主页设置）：选择主页应为新选项卡还是指定的 URL。
- **Homepage URL**（主页 URL）：如果您为主页设置选择了主页 URL，请在此处键入 URL。
- **Pop-up default settings**（弹出窗口默认设置）：选择默认情况下是允许还是阻止弹出窗口。然后，您可以允许或阻止特定 URL 打开弹出窗口。
- **Pop-ups allowed from these sites**（允许来自这些站点的弹出窗口）：指定允许打开弹出窗口的 URL 列表。
- **Popup not allowed from these sites**（不允许来自这些站点的弹出窗口）：指定阻止打开弹出窗口的 URL 列表。
- **Pages to load on startup**（启动时要加载的页面）：指定要在浏览器启动时打开的 URL 列表。

凭据设备策略

July 24, 2023

凭据设备策略指向在 Endpoint Management 中配置的 PKI。例如，您的 PKI 配置可能包括 PKI 实体、密钥库、凭据提供程序或服务器证书。有关凭据的详细信息，请参阅证书和身份验证。

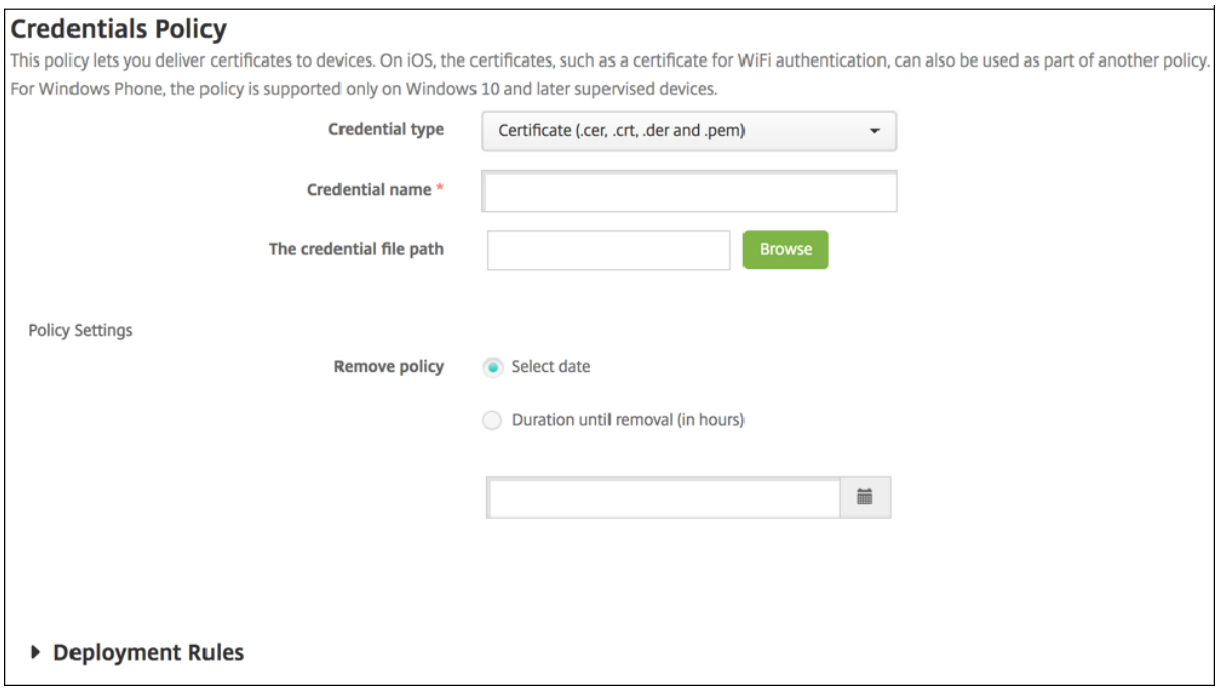
每个受支持的平台都需要一组不同的值，本文将对此进行介绍。

> 注意：
>
> 创建此策略前，需要具有计划用于各平台的凭据信息，以及任何证书和密码。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 和 tvOS 设置

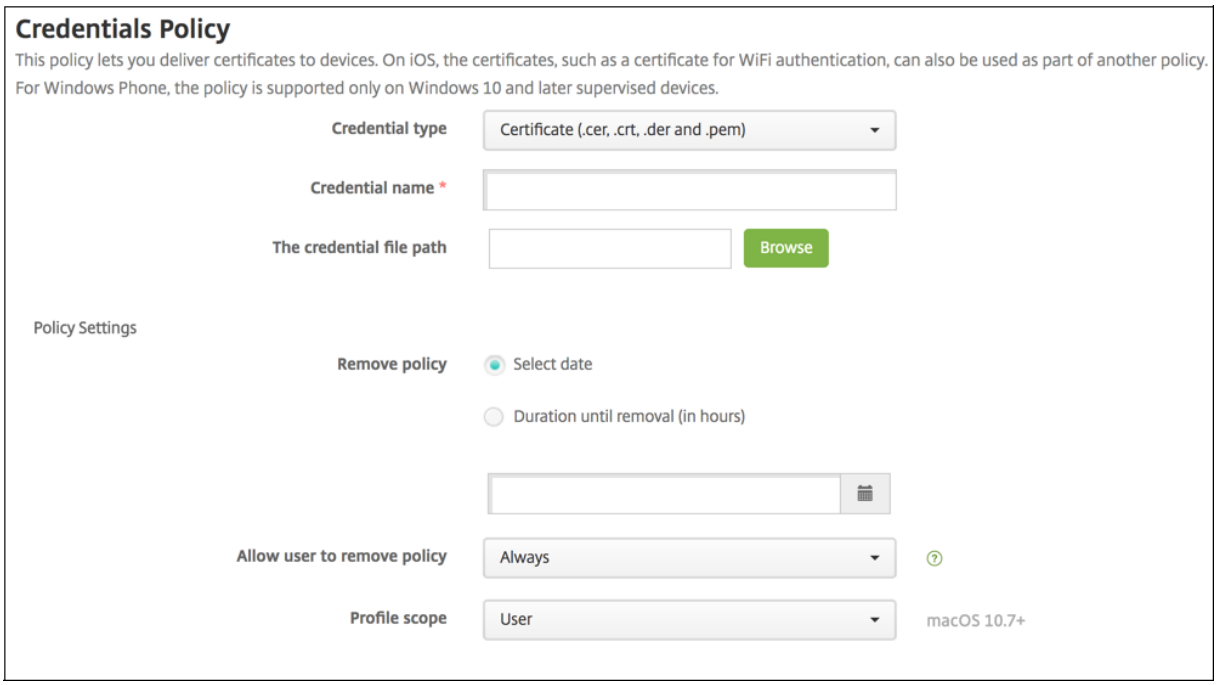


配置以下设置：

- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：通过单击浏览并导航到该凭据文件的位置来选择凭据文件。
  - 密钥库
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：通过单击浏览并导航到该凭据文件的位置来选择凭据文件。
    - 密码：输入凭据的密钥库密码。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。不适用于 iOS。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

macOS 设置

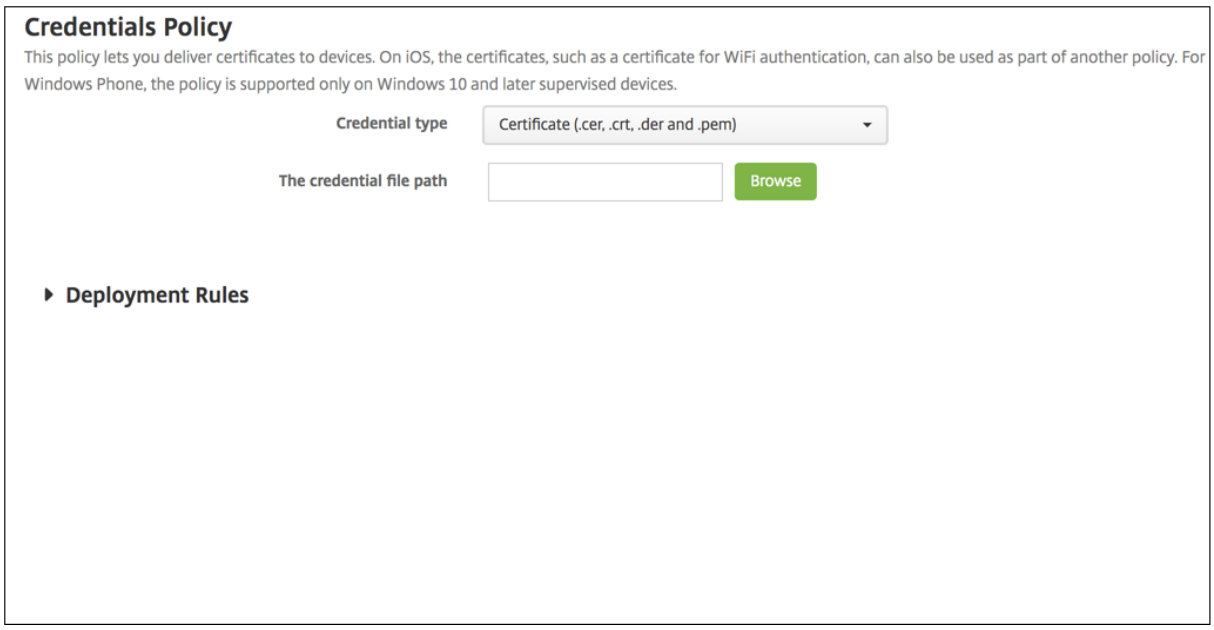


配置以下设置：

- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
  - 密钥库
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
    - 密码：输入凭据的密钥库密码。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android 设置

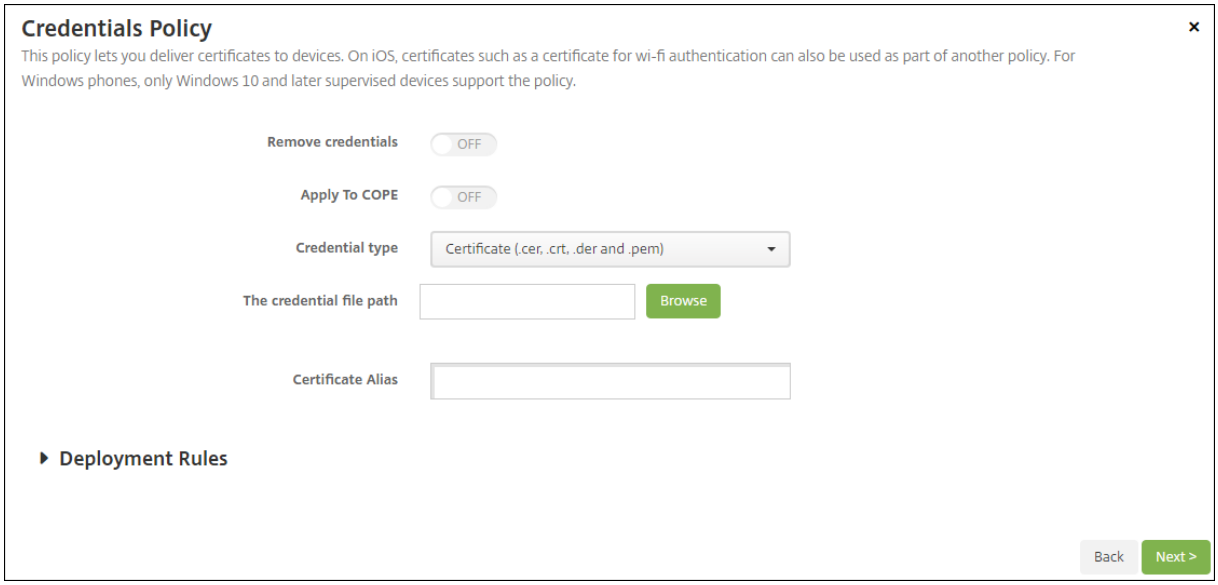


配置以下设置：

- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：通过单击浏览然后导航到文件的位置来选择凭据文件。
  - 密钥库
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
    - 密码：键入凭据的密钥库密码。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android Enterprise 设置



配置以下设置以确定如何应用凭据设置：

- 删除凭据：设置为开可配置以下设置。默认设置为关。
  - 删除用户凭据：从托管密钥库中删除证书。默认设置为关。
  - 删除受信任的根证书：卸载所有非系统 CA 证书。默认设置为关。
- 应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备：允许您为具有工作配置文件的完全托管设备配置凭据策略设置。当此设置为 开时，选择以下设置之一。此策略仅适用于设备上的工作配置文件。

配置凭据设置：

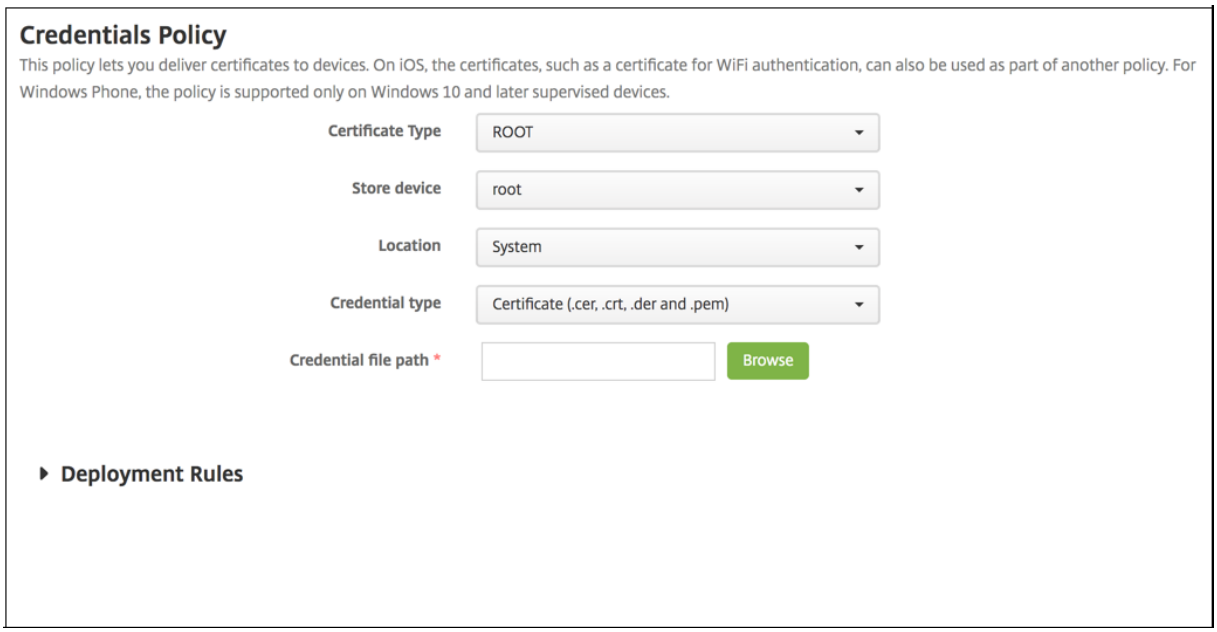
- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
  - 密钥库
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
    - 密码：键入凭据的密钥库密码。
    - 证书别名：证书别名使应用程序能够更轻松地访问证书。在 “Android Enterprise 托管配置” 设备策略中配置证书别名。然后，在 “凭据” 设备策略中的证书别名字段中键入别名。应用程序将检索证书并对 VPN 进行身份验证，而无需用户执行任何操作。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。
    - 要使用证书的应用程序：指定对来自此提供程序的凭据具有静默访问权限的应用程序：单击添加，选

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

择一个应用程序，然后单击保存。

* 证书别名：证书别名使应用程序能够更轻松地访问证书。在 “Android Enterprise 托管配置” 设备策略中配置证书别名。然后，在 “凭据” 设备策略中的证书别名字段中键入别名。应用程序将检索证书并对 VPN 进行身份验证，而无需用户执行任何操作。

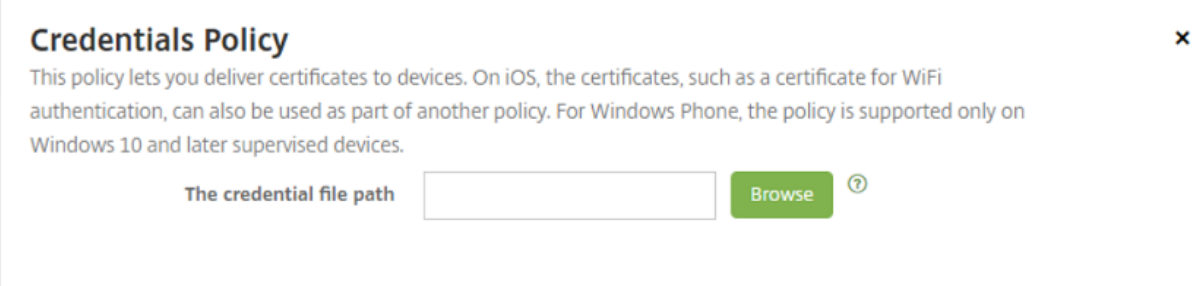
Windows Desktop/Tablet 设置



- 证书类型：在列表中，单击根证书或客户端证书。
- 如果单击根证书，则配置以下设置：
  - 存储设备：在列表中，单击根、我的或 **CA** 以选择凭据的证书存储位置。如果选择我的，则证书将存储在用户的证书存储中。
  - 位置：对于 Windows 10 和 Windows 11 平板电脑，系统是唯一的位置。
  - 凭据类型：对于 Windows 10 和 Windows 11 平板电脑，证书是唯一的凭据类型。
  - 凭据文件路径：单击浏览并导航到证书文件所在位置，选择此证书文件。
- 如果单击客户端证书，则配置以下设置：
- 位置：对于 Windows 10 和 Windows 11 平板电脑，系统是唯一的位置。
- 凭据类型：对于 Windows 10 和 Windows 11 平板电脑，密钥库是唯一的凭据类型。
- 凭据名称：键入凭据的名称。此字段为必填字段。
- 凭据文件路径：单击浏览并导航到证书文件所在位置，选择此证书文件。
- 密码：键入与凭据关联的密码。此字段为必填字段。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Workspace Hub 设置



- 凭据文件路径：浏览包含要上载的证书的 CA 证书文件或.zip 文件。此策略支持.cer、.crt、.pem 和.der 证书文件。

自定义 XML 设备策略

July 24, 2023

您可以在 Endpoint Management 中创建自定义 XML 策略，以便在支持的 Windows 设备上自定义以下功能：

- 预配，包括配置设备以及启用或禁用功能
- 设备配置，包括允许用户更改设置和设备参数
- 软件升级，包括提供要加载到设备中的新软件或缺陷修复（包括应用程序和系统软件）
- 故障管理，包括接收来自设备的错误和状态报告

> 注意：
>
> 创建 XML 内容时，请谨慎使用% 字符。% 字符是 XML 保留字符，仅用于转义 XML 特殊字符。要在名称中使用%，请将其编码为%25。

对于 Windows 设备：可以在 Windows 中使用 Open Mobile Alliance Device Management (OMA DM) API 创建自己的自定义 XML 配置。本主题中不介绍如何使用 OMA DM API 创建自定义 XML。有关使用 OMA DM API 的详细信息，请参阅 Microsoft Developer Network 站点上的 OMA DM protocol support（OMA DM 协议支持）。

对于 Android Enterprise 设备：可以使用 MX Management System (MXMS) 创建自定义 XML 配置。使用 MXMS API 创建自定义 XML 不在本文的探讨范围之内。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

Windows Desktop/Tablet 设置

XML 内容：键入或剪切并粘贴要添加到策略的自定义 XML 代码。

单击下一步后，Endpoint Management 将检查 XML 内容语法。内容框下将显示所有语法错误。请先修复所有错误，然后再继续操作。

如果没有语法错误，将显示自定义 **XML** 策略分配页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使用 **Windows AutoPilot** 设置和配置设备

Windows AutoPilot 是用于设置和预先配置新设备的技术的集合，将这些设备准备好用于生产。可以使用 Windows AutoPilot 重置设备、改变设备用途以及还原设备。AutoPilot 有助于移除当前操作系统部署的部分复杂性。使用 AutoPilot 会将任务缩减到一组能够使您的设备准备好快速有效使用的简单设置和操作。

有关将 Windows AutoPilot 与 Endpoint Management 结合使用的简要概述，请观看此视频。

这是一个嵌入式视频。单击链接观看视频

必备条件

- 在 Azure Active Directory 门户中配置的公司外观方案。
- 公司具有 Azure Active Directory Premium P1 或 P2 订阅。
- 将 Azure Active Directory 配置为适用于 Endpoint Management 的 IdP 类型在 Endpoint Management 控制台中，转至设置 **>** 身份提供程序 **(IDP)**。
- 与 Windows AutoPilot 使用的云服务的网络连接。
- 预装了 Windows 10 专业版、企业版或教育版（版本 1703 或更高版本）或 Windows 11 专业版、企业版或教育版的设备。
- 设备能够访问 Internet。

有关配置必备项的详细信息，请参阅 AutoPilot 上的 Microsoft Windows 文档：https://docs.microsoft.com。

要在 **Endpoint Management** 中为 **AutoPilot** 设备配置 **Windows** 自动重新部署功能，请执行以下操作

1. 按照以下步骤进行操作，在自定义 XML 设备策略中添加自定义 XML 策略。在 **XML** 内容中添加以下内容：

```
<Add>
<CmdID>\_cmdid\_</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
   DisableAutomaticReDeploymentCredentials</LocURI>
</Target>
<Meta>
<Format xmlns="syncml:metinf">int</Format>
</Meta>
<Data>0</Data>
</Item>
</Add>

<!--NeedCopy-->
```

2. 在 Windows 锁屏界面上，键入键击 **Ctrl + Windows** 键 **+ R**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 使用 Azure Active Directory 帐户登录。
4. 设备将验证该用户是否有权重新部署设备。设备随后将重新部署。
5. 使用 AutoPilot 配置更新设备后，用户随后可以登录全新配置的设备。

在 **Windows 11** 设备上部署单应用程序自助服务终端

> 注意：
>
> Windows 11 设备仅支持单应用程序信息亭模式。

在 **XML** 内容文本框中，复制并粘贴以下 XML 脚本，然后将以下字符串替换为您的设置：

- `your_username_here`（两个实例）：要在设备上创建的用户名。为两个实例保持相同的设置。
- `your password_here`：用户的密码。
- `your_UWP_app_id_here`：要在设备上部署的 UMP 应用程序的 AUMID。

XML 脚本：

```
<Add>
    <CmdID>\_cmdid\_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/Accounts/Users/
               your_username_here/Password</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>your_password_here</Data>
    </Item>
</Add>
<Replace>
    <CmdID>\_cmdid\_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</
               LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data><![CDATA[<AssignedAccessConfiguration
        xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
        xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/
           config">
            <Profiles>
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
                <Profile Id="{
AFF9DA33-AE89-4039-B646-3A5706E92957 }
">
                    <KioskModeApp AppUserModelId="your_UWP_app_id_here"
                        />
                </Profile>
            </Profiles>
            <Configs>
                <Config>
                    <Account>your_username_here</Account>
                    <DefaultProfile Id="{
AFF9DA33-AE89-4039-B646-3A5706E92957 }
"/>
                </Config>
            </Configs>
        </AssignedAccessConfiguration>]]></Data>
    </Item>
</Replace>
<!--NeedCopy-->
```

Defender 设备策略

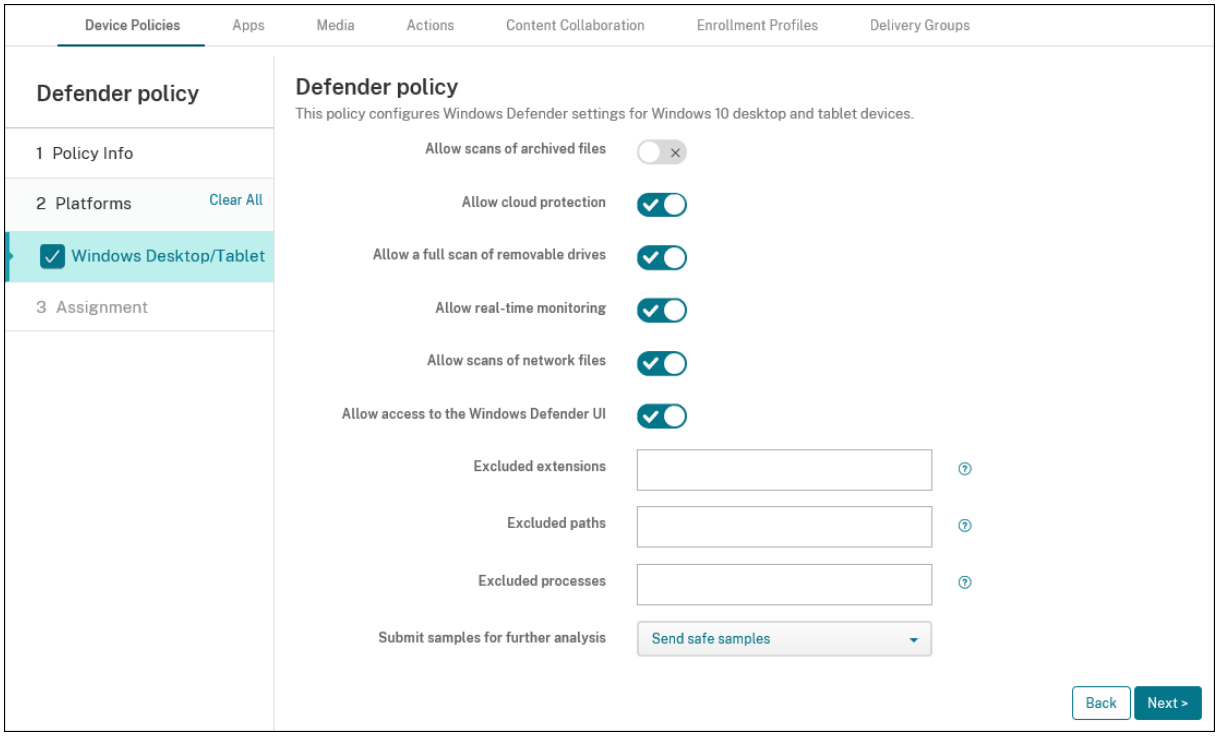
March 31, 2022

Windows Defender 是 Windows 10 和 Windows 11 附带的恶意软件防护功能。可以使用 Endpoint Management 设备策略 Defender 为 Windows 10 和 Windows 11 Desktop 和 Tablet 设备配置 Microsoft Defender 策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop 和 Tablet 设置



- **Allow scanning of archived files**（允许扫描存档的文件）：允许或阻止 Defender 扫描存档的文件。默认值为关。
- 允许启用云保护：允许或阻止 Defender 向 Microsoft 发送有关恶意软件活动的信息。默认值为开。
- 允许完全扫描可移动驱动器：允许或阻止 Defender 扫描可移动驱动器，例如 U 盘。默认值为开。
- **Allow real-time monitoring**（允许实时监视）：默认值为 **On**（开）。
- 允许扫描网络文件：允许或阻止 Defender 扫描网络文件。默认值为开。
- 允许访问 **Windows Defender UI**：指定用户是否可以访问 Windows Defender 用户界面。此设置在下次启动用户设备时生效。如果此设置设为关，则用户不会收到任何 Windows Defender 通知。默认值为开。
- 排除的扩展名：要从实时扫描或计划的扫描中排除的扩展名。要分隔扩展名，请使用 | 字符。例如，`lib\|obj`。
- 排除的路径：要从实时扫描或计划的扫描中排除的路径。要分隔路径，请使用 | 字符。例如，`C:\Example|C:\Example1`。
- 排除的进程：要从实时扫描或计划的扫描中排除的进程。要分隔进程，请使用 | 字符。例如，`C:\Example.exe|C:\Example1.exe`。
- **Submit samples for further analysis**（提交示例进行进一步分析）：控制是否向 Microsoft 发送可能需要进一步分析以确定是否是恶意的文件。选项：始终提示、发送安全示例、从不发送、发送所有示例。默认值为发送安全示例。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Device Guard 设备策略

March 31, 2022

Device Guard 是 Windows 10 和 Windows 11 中提供的一项安全功能。此功能通过使用 Windows 虚拟机管理程序来支持设备上的安全服务，从而实现基于虚拟化的安全性。Device Guard 策略将启用安全启动、UEFI 锁和虚拟化等安全功能。

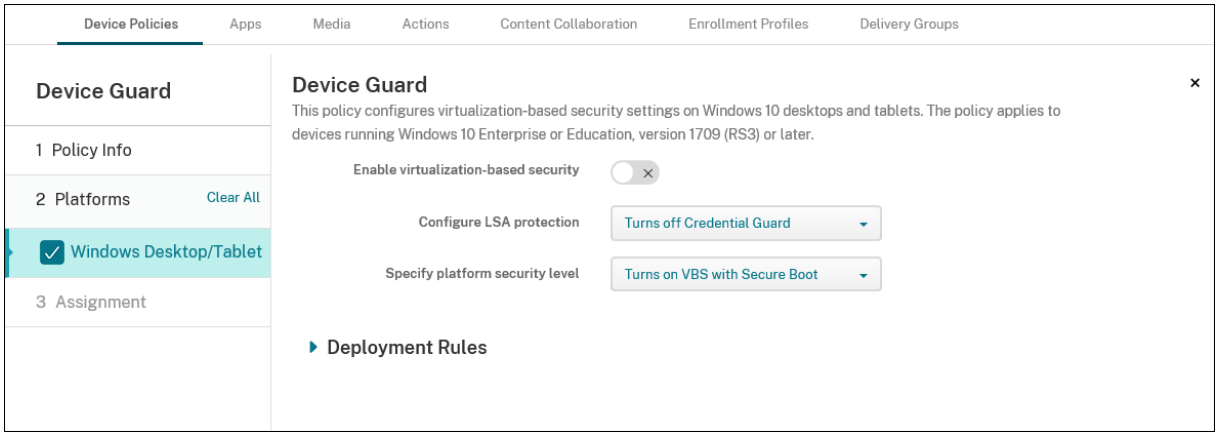
必备条件

- 使用企业版或教育版许可证的 Windows 10 和 Windows 11 Desktop 和 Tablet
- 在 Windows 中启用的 Device Guard

  有关 Device Guard 的详细信息，请参阅https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Windows Desktop 和 Tablet 设置



- 启用基于虚拟化的安全性：禁用或启用基于虚拟化的安全功能。基于虚拟化的安全性使用 Windows 虚拟机管理程序来支持安全服务。
- **Configure LSA protection**（配置 LSA 保护）：用于配置凭据防护。此设置允许用户打开启用了基于虚拟化的安全性的 Credential Guard 以在下次重新启动时保护凭据。选项包括 **Turns off Credential Guard**（关闭凭据防护）、**Turns on Credential Guard with UEFI lock**（使用 UEFI 锁定打开凭据防护）和 **Turns on Credential Guard without UEFI lock**（在没有 UEFI 锁定的情况下打开凭据防护）。默认值为 **Turns off Credential Guard**（关闭凭据防护）。
- **Specify platform security level**（指定平台安全级别）：允许您在下次重新启动时指定平台安全级别。选项为打开启用了安全启动功能的 **VBS** 和打开启用了安全启动和直接内存访问功能的 **VBS**。默认值为 **Turns on VBS with Secure Boot**（使用安全启动打开 VBS）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 查询设备以确定基于虚拟化的安全设置是否与服务器上的设置匹配。如果安全设置匹配，Endpoint Management 不会将此策略部署到设备。如果安全设置不匹配，Endpoint Management 将部署此策略。

设备运行状况证明设备策略

March 31, 2022

在 Endpoint Management 中，您可以要求 Windows 10 和 Windows 11 设备报告其运行状况。为报告其运行状况，设备会将特定数据和运行时信息发送给 Health Attestation Service (HAS) 进行分析。HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 Endpoint Management。Endpoint Management 使用行状况证明证书的内容来部署您设置的自动操作。

HAS 验证的数据包括：

- AIK 是否存在
- Bit Locker 状态
- 启动调试是否已启用
- 启动管理器修订列表版本
- 代码完整性是否已启用
- 代码完整性修订列表版本
- Apple 部署计划策略
- ELAM 驱动程序是否已加载
- 颁发时间
- 内核调试是否已启用
- PCR
- 重置计数
- 重新启动计数
- 安全模式是否已启用
- SBCP 哈希
- 安全启动是否已启用
- 测试签名是否已启用
- 已启用 VSM
- 已启用 WinPE

有关详细信息，请参阅 Microsoft 设备 HealthAttestation CSP 页面。

可以使用 Microsoft 云或本地 Windows DHA 服务器配置 DHA，如下所示：

- 要使用 Microsoft 云配置 DHA，请执行以下操作：添加设备运行状况证明策略并按本文中所述对其进行配置。
- 使用本地 Windows DHA 服务器配置 DHA：配置 DHA 服务器。然后，添加设备运行状况证明策略并按本文中所述对其进行配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要配置 DHA 服务器，请在运行 Windows Server 2016 技术预览版 5 或更高版本的计算机上安装 DHA 服务器角色。有关说明，请参阅配置本地设备运行状况证明服务器。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Windows Desktop/Tablet 设置

如果您通过使用 **Microsoft** 云配置 **DHA**

- 启用设备运行状况证明：选择是否需要设备运行状况证明。默认值为关。

如果您使用本地 **Windows DHA** 服务器配置 **DHA**

- 启用设备运行状况证明：设置为开。
- 配置本地 **Health Attestation Service**：设置为开。
- 本地 **DHA** 服务 **FQDN**：键入您设置的 DHA 服务器的完全限定域名。
- 本地 **DHA API** 版本：选择 DHA 服务器上安装的 DHA 服务版本。

设备名称设备策略

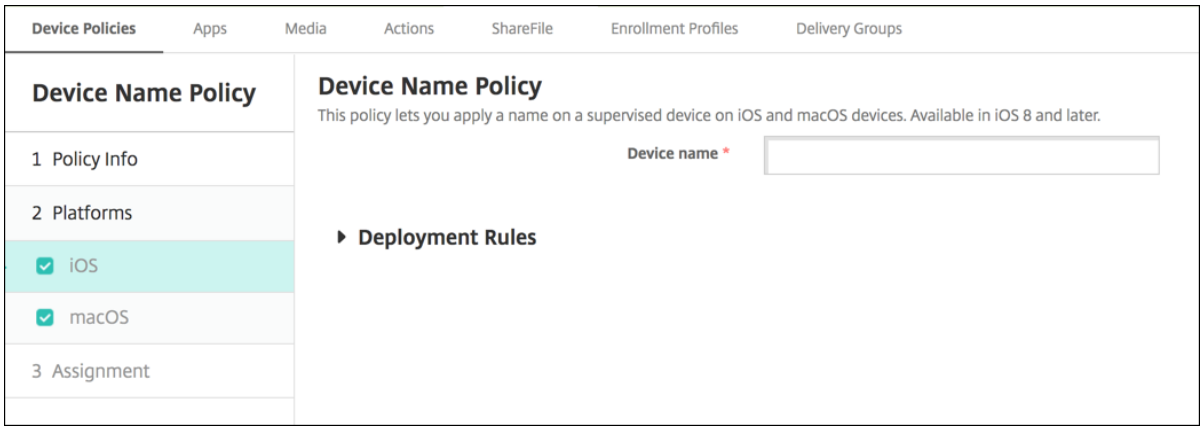
January 30, 2023

可以在受监督的 iOS 和 macOS 设备上设置名称，以便轻松识别设备。可以使用宏、文本或二者的组合定义设备的名称。例如，要将设备名称设置为设备的序列号，可以使用 ${device.serialnumber}。要将设备的名称设置为用户名和域的组合，可以使用 ${user.username}@example.com。有关宏的详细信息，请参阅 Endpoint Management 中的宏。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 和 macOS 设置



- 设备名称：键入宏、宏组合或宏和文本组合，为每个设备指定唯一名称。例如，使用 ${device.serialnumber} 将设备名称设置为每台设备的序列号，或者使用 ${device.serialnumber} ${ user.username } 在设备名称中包含用户的 Apple ID。

教育配置设备策略

March 31, 2022

教育配置设备策略定义以下对象：

- 面向教师设备的 Apple“课堂”应用程序设置。
- 用于在教师与学生设备之间执行客户端身份验证的证书。

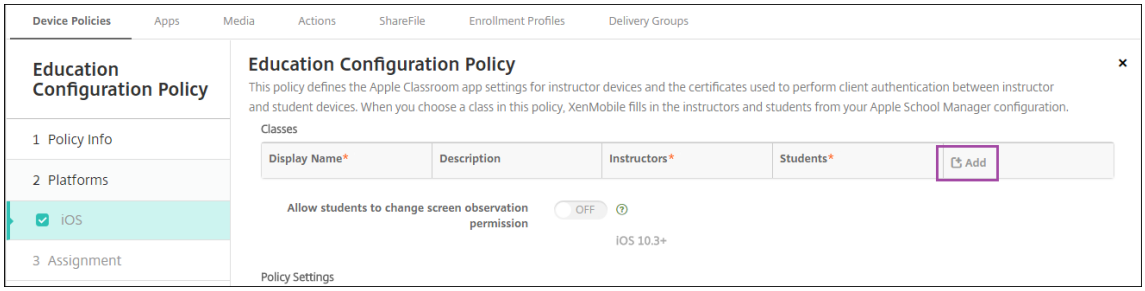
iOS (iPadOS) 设备支持的教育配置设备策略。

在此策略中选择一个班级时，Endpoint Management 控制台将填写您的 Apple 校园教务管理配置中的教师和学生。如果此策略中的 Apple“课堂”应用程序设置对所有班级都相同，请创建一个策略。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

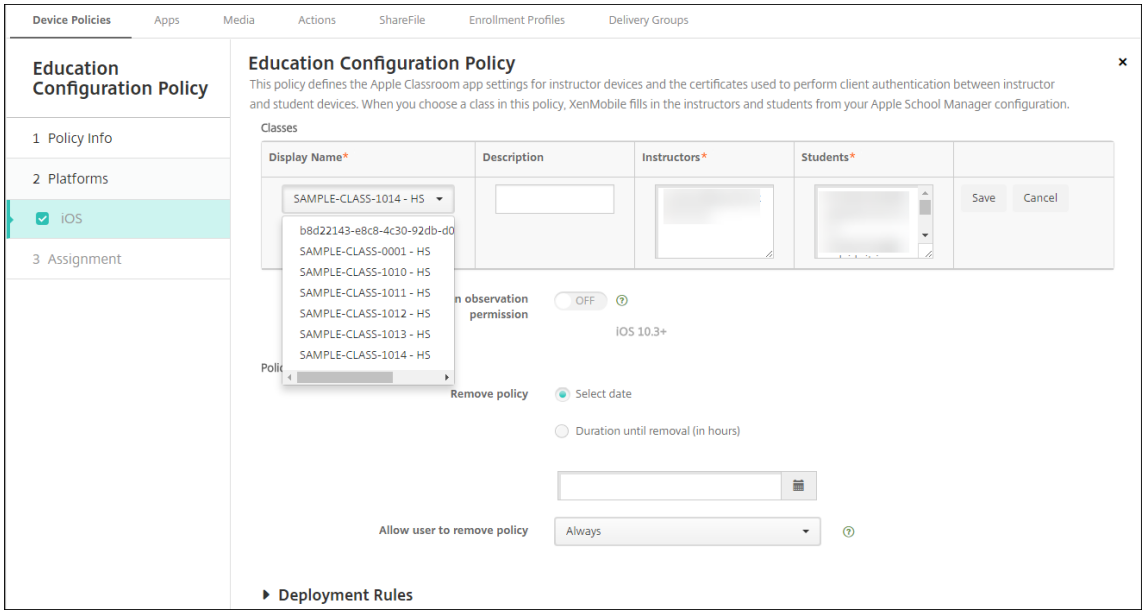
iOS 设置

- 课程：要添加课程，请单击添加。

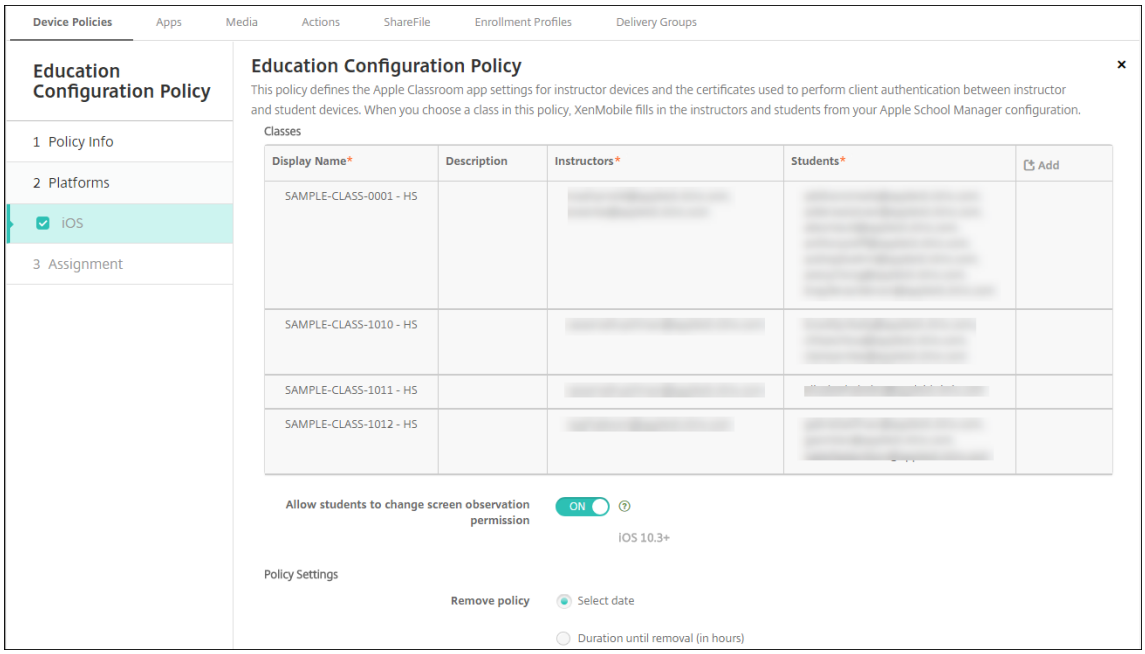


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

然后，单击显示名称列表。此时将显示从您的已连接 Apple 校园教务管理帐户中获取的班级列表。



从显示名称中选择班级时，Endpoint Management 将填写教师和学生。继续添加班级。



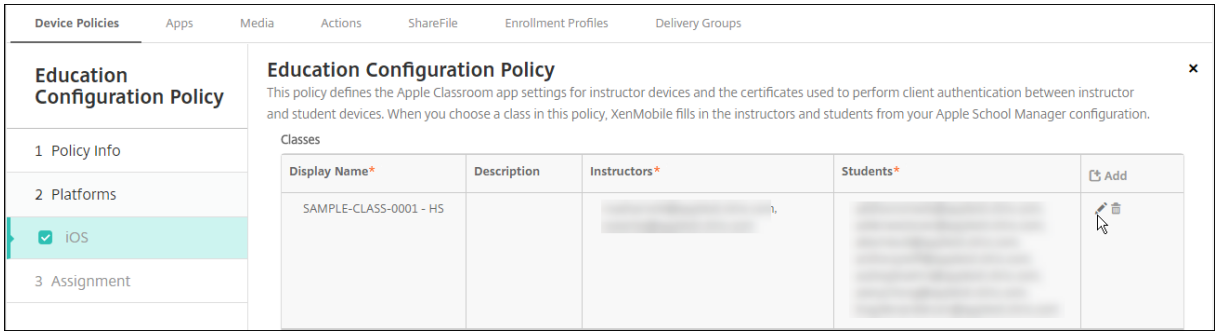
- 允许学生更改屏幕观察权限：如果设置为开，则注册参加托管课程的学生可以选择是否允许教师观察其设备屏幕。默认设置为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

编辑策略中的班级信息

可以向班级添加说明（“课堂”应用程序中的“显示名称”）。还可以添加或删除教师和学生。Endpoint Management 不保存对您的 Apple 校园教务管理帐户所做的此类更改。有关详细信息，请参阅与 Apple 教育功能相集成中的“管理教师、学生和班级数据”。

将鼠标悬停在要编辑的班级的添加列上，然后单击铅笔图标。



要从策略中删除班级，请将鼠标悬停在要删除的班级的添加列上，然后单击垃圾桶图标。

Endpoint Management 选项设备策略

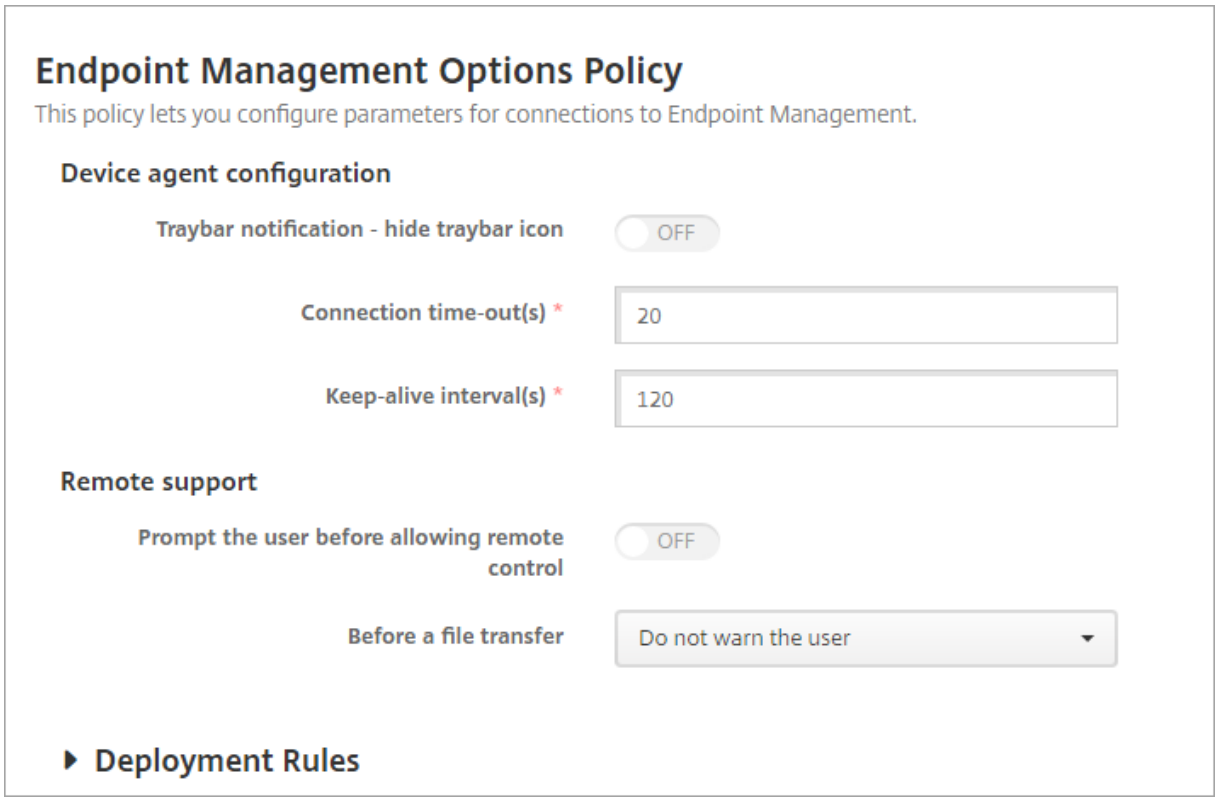
May 6, 2022

可以添加 Endpoint Management 选项策略，以配置从 Android 设备连接到 Endpoint Management 时的 Secure Hub 行为。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

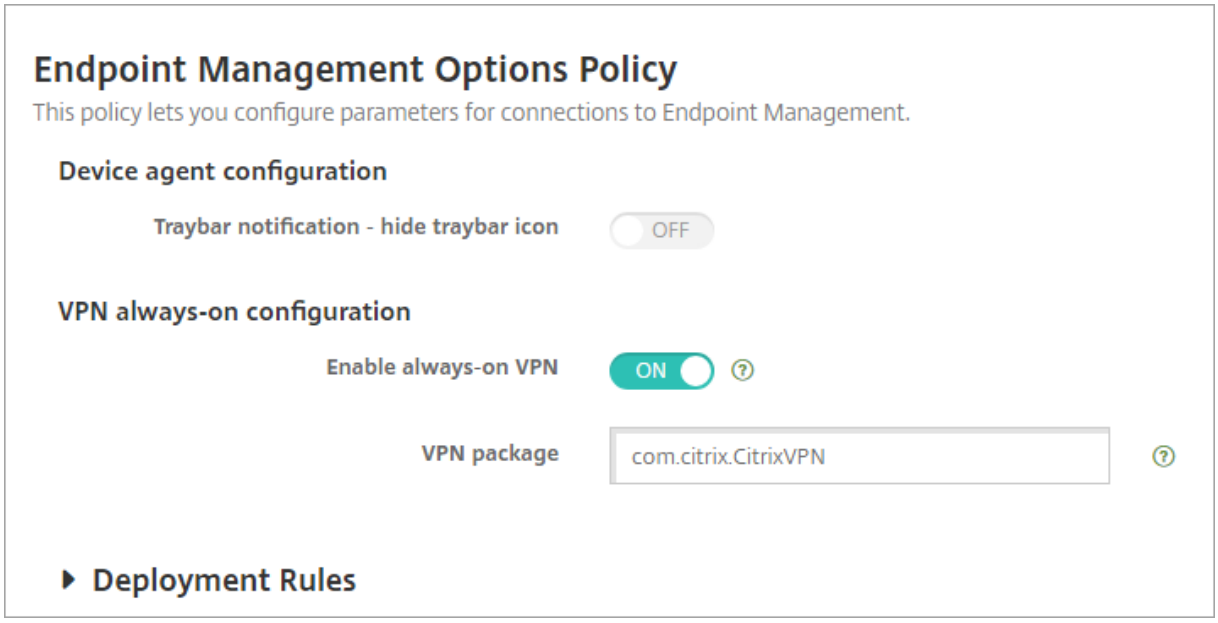
Android 设置



- 托盘栏通知 **-** 隐藏托盘栏图标：选择是隐藏还是显示托盘栏图标。默认值为关。
- 连接**:** 超时：键入连接超时前连接可以空闲的时间长度（秒）。默认值为 20 秒。
- 保持连接时间间隔：键入保持连接打开的时间长度（秒）。默认值为 120 秒。
- 在允许远程控制前提示用户：选择是否在允许远程支持控制前提示用户。默认值为关。
- 在文件传输前：在列表中，单击是否向用户警告文件传输，或是否请求用户许可。可用值：不警告用户、警告用户和请求用户许可。默认值为不警告用户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android Enterprise 设置



支持从 Android 版本 7 开始。

- 托盘栏通知 **-** 隐藏托盘栏图标：选择是隐藏还是显示托盘栏图标。默认值为关。
- 启用始终可用的 **VPN**：选择是否启用始终可用的 VPN。当此设置设为开时，VPN 服务将在设备打开电源时启动。VPN 服务在设备打开时继续运行。默认设置为关。
- **VPN** 包：键入设备使用的 VPN 应用程序的软件包名称。默认情况下，Citrix SSO 应用程序的软件包名称 **com.citrix.CitrixVPN** 将在此字段中自动填充。

Endpoint Management 卸载设备策略

March 31, 2022

可以在 Endpoint Management 中添加设备策略以从 Android 设备中卸载 Endpoint Management。部署后，此策略将从部署组中的所有设备中删除 Endpoint Management。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Android 设置

- 从设备中卸载 **Endpoint Management**：选择是否从部署此策略的每个设备中卸载 Endpoint Management。默认值为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Exchange 设备策略

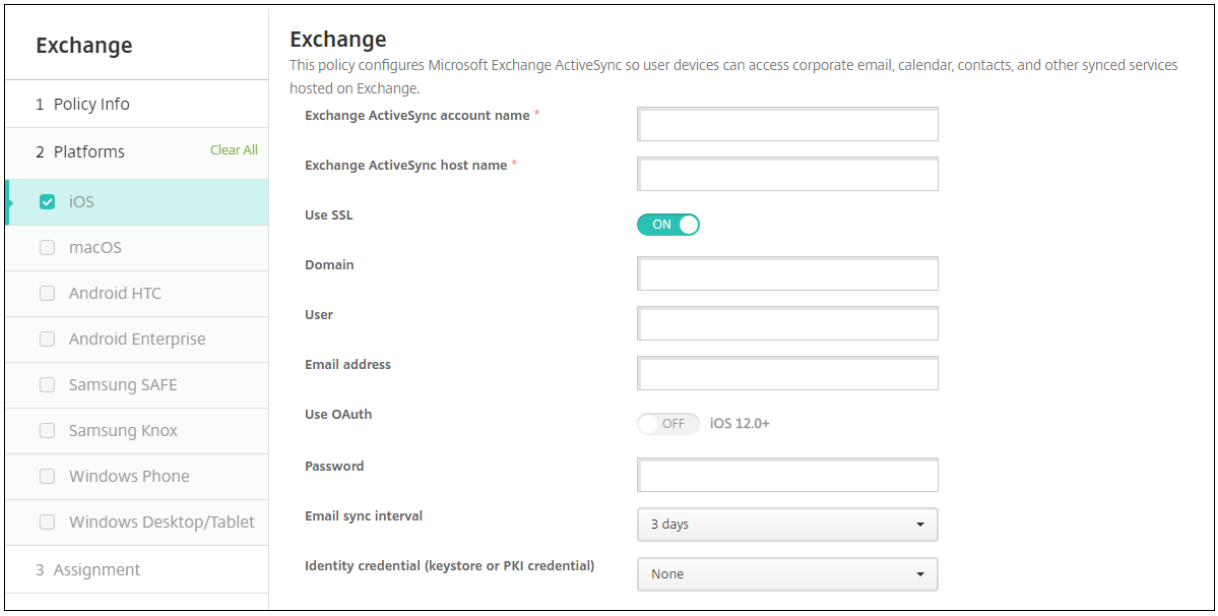
November 7, 2022

可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以允许其访问 Exchange 上托管的企业电子邮件。每个平台都需要一组不同的值，这些值将在以下各节中详细说明。

要创建此策略，需要 Exchange Server 的主机名或 IP 地址。有关 ActiveSync 设置的信息，请参阅 Microsoft 文章 ActiveSync CSP。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- **Exchange ActiveSync** 帐户名称：键入显示在用户设备上的电子邮件帐户的说明。
- **Exchange ActiveSync** 主机名：键入电子邮件服务器的地址。
- 使用 **SSL**：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为开。
- 域：输入 Exchange Server 所在的域。可以在此字段中使用系统宏 `$user.domainname` 自动查找用户的域名。
- 用户：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `$user.username` 自动查找用户名。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 `$user.mail` 自动查找用户的电子邮件帐户。
- 使用 **OAuth**：如果设置为开，连接将使用 OAuth 进行身份验证。默认值为关。此选项适用于 iOS 12.0 及更高版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 密码：输入 Exchange 用户帐户的可选密码。使用 **OAuth** 设置为于时不会显示此设置。
- 电子邮件同步时间间隔：在列表中，选择电子邮件与 Exchange Server 同步的频率。默认值为 **3** 天。
- 身份凭据 **(**密钥库或 **PKI)**：如果为 Endpoint Management 配置了身份提供程序，则在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。默认值为无。
- **Authorize moving email between accounts**（授权在帐户之间移动电子邮件）：选择是否允许用户：
  - 将电子邮件从此帐户移出到另一个帐户
  - 从其他帐户转发电子邮件
  - 答复来自其他帐户的邮件。

  默认值为关。
- 仅从电子邮件应用程序发送电子邮件：选择是否限制用户只能从 iOS 邮件应用程序发送电子邮件。默认值为关。
- **Prevent users from syncing recent addresses**（阻止用户同步最近使用的地址）：选择是否阻止用户同步最近使用的地址。默认值为关。
- 启用 **S/MIME** 签名：选择此帐户是否支持 S/MIME 签名。默认值为开。设置为开时，将显示以下两个字段。
  - 签署身份凭据：选择要使用的签名凭据。
  - **User can override S/MIME signing**（用户可以替代 S/MIME 签名）：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 签名。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - **User can override S/MIME signing certificate UUID**（用户可以替代 S/MIME 签名证书 UUID）：如果设置为开，用户可以在其设备的设置中选择要使用的签名凭据。默认值为关。此选项适用于 iOS 12.0 及更高版本。
- 启用 **S/MIME** 加密：选择此帐户是否支持 S/MIME 加密。默认值为关。设置为开时，将显示以下两个字段。
  - 加密身份凭据：选择要使用的加密凭据。
  - 启用 **“**为消息单独设置 **S/MIME”** 开关：设置为开时，向用户显示一个选项，用于为其撰写的每条消息打开或关闭 S/MIME 加密。默认值为关。
  - **User can override S/MIME encryption**（用户可以替代 S/MIME 加密）：如果设置为开，用户可以在其设备的设置中选择 S/MIME 是否默认处于打开状态。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - **User can override S/MIME encryption certificate UUID**（用户可以替代 S/MIME 加密证书 UUID）：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 加密身份和加密。默认值为关。此选项适用于 iOS 12.0 及更高版本。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。

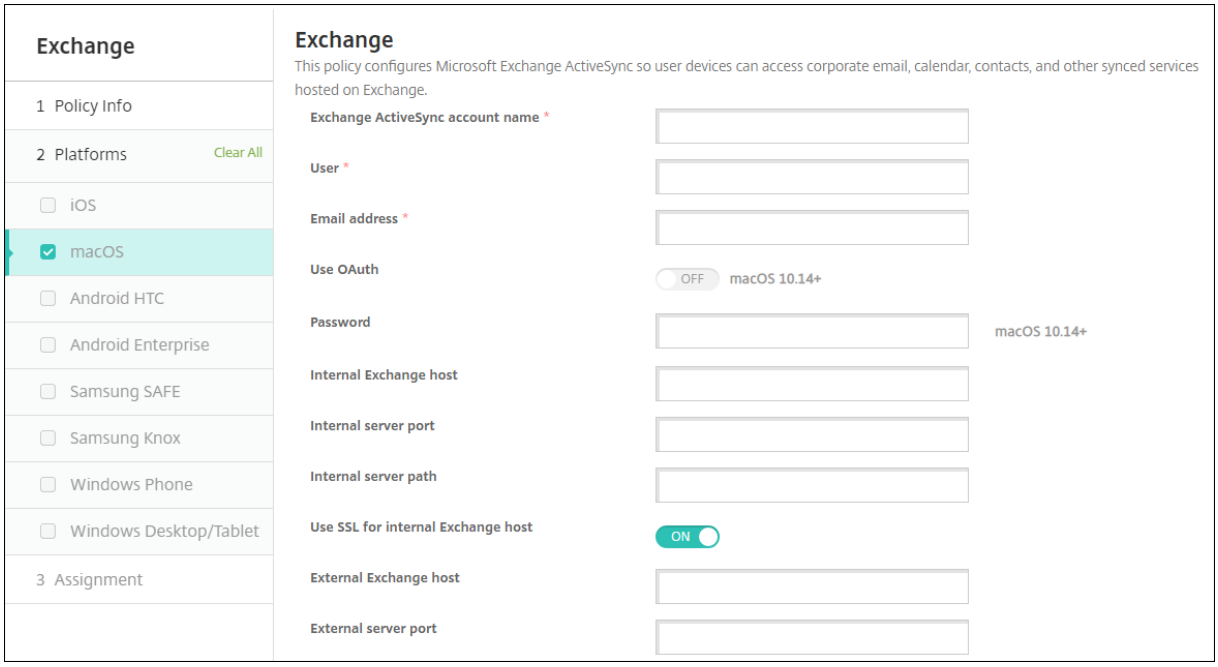
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

同步的 **Exchange** 服务

同步的 Exchange 服务设置允许您选择是否同步以下功能：

- 日历
- 通讯录
- 邮件
- 备注
- 提醒

macOS 设置



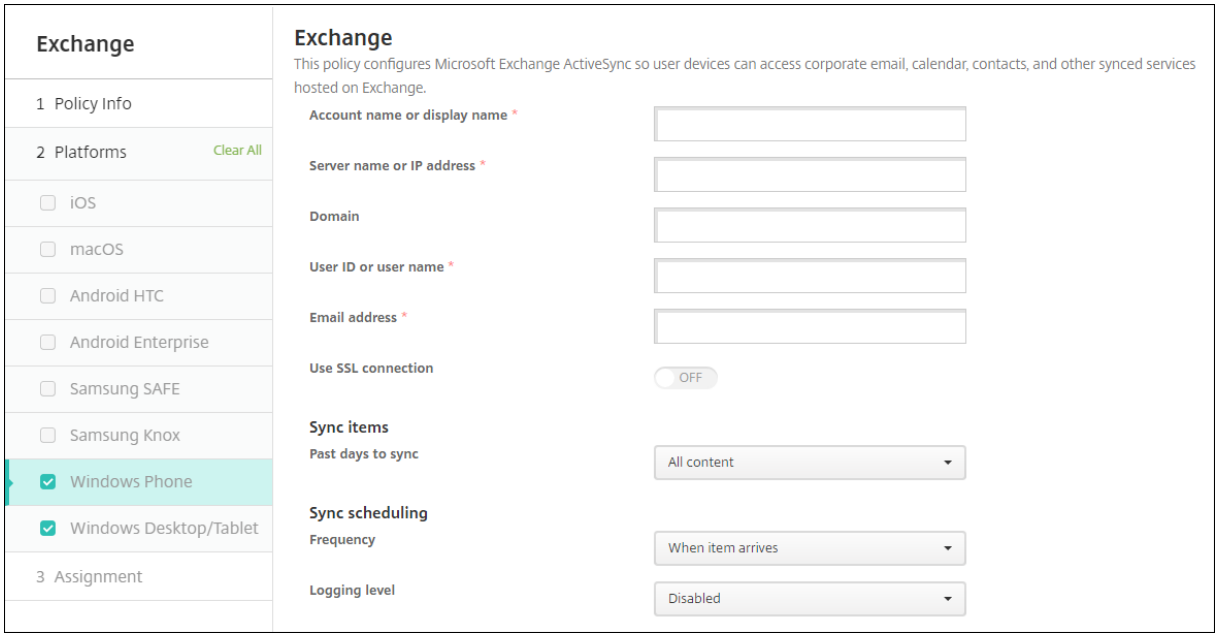
- **Exchange ActiveSync** 帐户名称：键入显示在用户设备上的电子邮件帐户的说明。
- 用户：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `$user.username` 自动查找用户名。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 `$user.mail` 自动查找用户的电子邮件帐户。
- 使用 **OAuth**：如果设置为开，连接将使用 OAuth 进行身份验证。默认值为关。此选项适用于 macOS 10.14 及更高版本。
- **OAuth** 登录 **URL**：指定在不使用自动发现服务时要加载到 Web 视图中以使用 OAuth 进行身份验证的 URL。使用 **OAuth** 设置为开时将显示此字段。
- 密码：输入 Exchange 用户帐户的可选密码。使用 **OAuth** 设置为于时不会显示此设置。
- 内部 **Exchange** 主机：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选内部 Exchange 主机名。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 内部服务器端口：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选内部 Exchange Server 端口。
- 内部服务器路径：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选内部 Exchange Server 路径。
- 对内部 **Exchange** 主机使用 **SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。默认值为开。
- 外部 **Exchange** 主机：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选外部 Exchange 主机名。
- 外部服务器端口：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选外部 Exchange Server 端口号。
- 外部服务器路径：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选外部 Exchange Server 路径。
- 对外部 **Exchange** 主机使用 **SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。默认值为开。
- 允许投递邮件：选择是否允许用户在两个 Mac 之间以无线方式共享文件，且无需连接到现有网络。默认值为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop/Tablet 设置



> 注意：
>
> 此策略不允许您设置用户密码。用户在推送策略后必须从其设备设置该参数。

- 帐户名称或显示名称：键入 Exchange ActiveSync 帐户名称。
- 服务器名称或 **IP** 地址：键入 Exchange Server 的主机名或 IP 地址。
- 域：输入 Exchange Server 所在的域。可以在此字段中使用系统宏 `$user.domainname` 自动查找用户的域名。
- 用户 **ID** 或用户名：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `$user.username` 自动查找用户名。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 `$user.mail` 自动查找用户的电子邮件帐户。
- 使用 **SSL** 连接：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为关。
- 要同步的过去天数：在列表中，单击要将设备上过去多少天内的所有内容与 Exchange Server 同步。默认值为所有内容。
- 频率：在列表中，单击同步从 Exchange Server 发送到设备的数据时要使用的计划。默认值为项目到达时。
- 日志记录级别：在列表中，单击已禁用、基本或高级以指定记录 Exchange 活动时的详细级别。默认值为已禁用。

文件设备策略

November 7, 2022

可以添加和部署文件，以便用户在其 Android 和 Android Enterprise 设备上访问。可以指定要在设备上存储文件的目录。例如，您希望用户收到公司文档或.pdf 文件。将文件部署到设备，让用户知道文件的位置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android 设备不支持本机运行脚本。用户需要第三方软件来运行脚本。

利用此策略可以添加以下文件类型：

- 文本文件（.xml、.html、.py 等）
- 其他文件，如文档、图片、电子表格或演示文稿

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Android Enterprise 设置

- 要导入的文件：要选择要导入的文件，请单击浏览并导航到文件所在的位置。
- 目标文件夹：在列表中，选择要存储上载的文件的位置，或者选择新增以指定文件位置。选择 %Flash Storage%\ 或 %XenMobile Storage%\ 宏以指示存储上载的文件的位置。宏将扩展到每台设备上的适用位置。
  - %XenMobile Storage%\ 扩展到内部存储目录中的 Android/data/com.zenprise/。
  - 对于 Android 9.0 及更低版本，%Flash Storage%\ 将文件保存到外部存储目录中。
  - 对于 Android 10.0 及更高版本，%Flash Storage%\ 将文件保存到内部存储目录的下载文件夹中。
  - 对于 Android 11.0 及更高版本，由于 Google 对目标位置的访问施加了限制，因此 %XenMobile Storage%\ 不再适用。
- 目标文件名：可选。如果必须在部署到设备之前更改文件名，请键入文件名。
- 如果文件存在：在列表中，选择是否复制现有文件。默认值为仅在存在差异时复制文件。

> 重要：
>
> “文件”设备策略不再支持在 Android Enterprise 上添加脚本。如果现有策略包含脚本，则在选择策略时会显示一条错误消息，您可以重新添加策略以解决问题。

Android 设置

- 要导入的文件：要选择要导入的文件，请单击浏览并导航到文件所在的位置。
- 文件类型：选择文件或脚本。
- 立即执行：选择脚本后，将显示立即执行选项。启用此设置时没有反应。用户必须手动运行脚本。
- 替换宏表达式：选择是否将脚本中的宏令牌名称替换为设备或用户属性。有关宏语法，请参阅宏。默认值为关。
- 目标文件夹：在列表中，选择要存储上载的文件的位置，或者选择新增以指定文件位置。选择 %Flash Storage%\ 或 %XenMobile Storage%\ 宏以指示存储上载的文件的位置。宏将扩展到每台设备上的适用位置。
  - %XenMobile Storage%\ 扩展到内部存储目录中的 Android/data/com.zenprise/。
  - 对于 Android 9.0 及更低版本，%Flash Storage%\ 将文件保存到外部存储目录中。
  - 对于 Android 10.0 及更高版本，%Flash Storage%\ 将文件保存到内部存储目录的下载文件夹中。
  - 对于 Android 11.0 及更高版本，由于 Google 对目标位置的访问施加了限制，因此 %XenMobile Storage%\ 不再适用。
- 目标文件名：可选。如果必须在部署到设备之前更改文件名，请键入文件名。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 如果文件存在：在列表中，选择是否复制现有文件。默认值为仅在存在差异时复制文件。

FileVault 设备策略

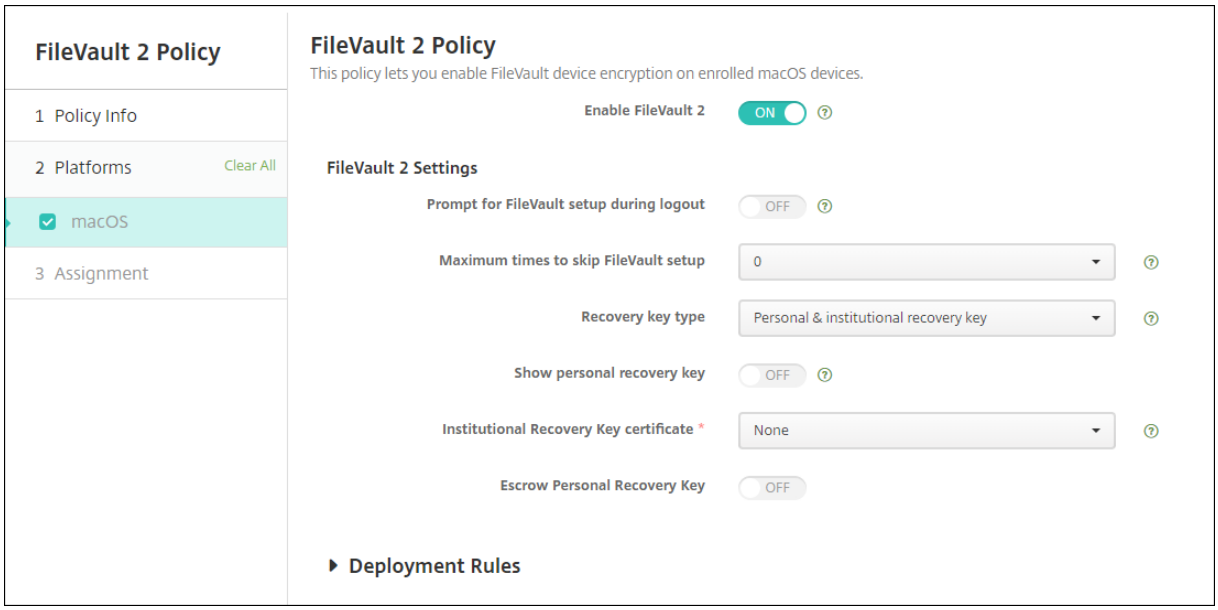
March 31, 2022

macOS FileVault 完整磁盘加密 (FileVault 2) 功能通过加密系统卷的内容来保护系统卷。用户在每次设备启动时都使用其帐户密码登录启用了 FileVault 的 macOS 设备。如果用户丢失了自己的密码，可以通过恢复密钥来解锁磁盘并重置密码。

此设备策略将启用 FileVault 用户设置屏幕并配置恢复密钥等设置。有关 FileVault 的详细信息，请参阅 Apple 支持站点。

要添加 FileVault 策略，请转至配置 **>** 设备策略。

macOS 设置



- 启用 **FileVault**：如果设置为开，则将在接下来的 N 次注销过程中提示用户启用 FileVault，如选项跳过 **FileVault** 设置的最大次数指定。如果设置为 **Off**（关），用户不会收到启用 FileVault 的提示，但他们仍然可以自行启用 FileVault。
- **Prompt for FileVault setup during logout**（注销过程中提示进行 FileVault 设置）：如果设置为开，用户在注销时会看到一条提示，要求其启用 FileVault。
- 跳过 **FileVault** 设置的最大次数：用户可以跳过 FileVault 设置的最大次数。用户达到最大次数时，必须设置 FileVault 才能登录。如果设置为 **0**，用户必须在首次尝试登录过程中启用 FileVault。默认值为 **0**。
- 恢复密钥类型：忘记了密码的用户可以键入恢复密钥以解锁磁盘并重置自己的密码。恢复密钥选项：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 个人恢复密钥：个人恢复密钥对用户而言是唯一的。FileVault 设置过程中，用户将选择创建恢复密钥还是允许其 iCloud 帐户解锁磁盘。要在 FileVault 设置完成后向用户显示恢复密钥，请启用显示个人恢复密钥。显示该密钥将使用户能够录制该密钥以供将来使用。要允许用户在丢失密钥时查找密钥，请启用 **Escrow personal recovery key**（托管个人恢复密钥）。

    您可以通过安全操作轮换个人恢复密钥。有关轮换个人恢复密钥的详细信息，请参阅安全操作。

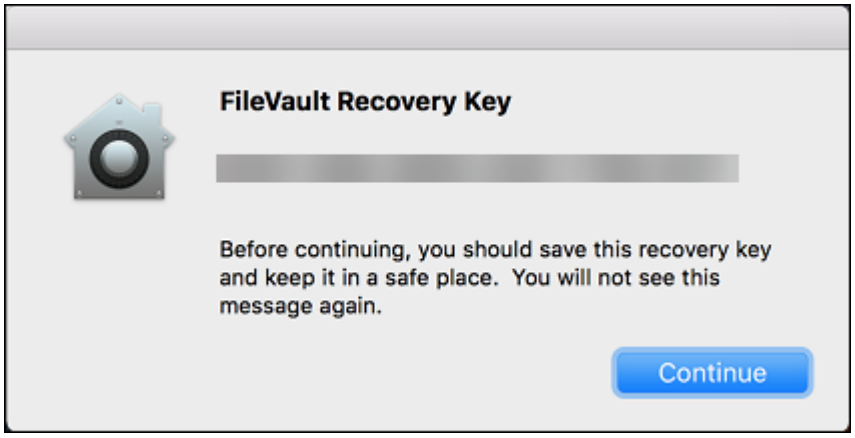
    有关恢复密钥管理的信息，请参阅 Apple 支持站点。

  - 机构恢复密钥：可以创建一个机构（或主）恢复密钥和 FileVault 证书，以后您将使用这些凭据来解锁用户设备。有关信息，请参阅 Apple 支持站点。使用 Endpoint Management 可将 FileVault 证书部署到设备。有关信息，请参阅证书和身份验证。

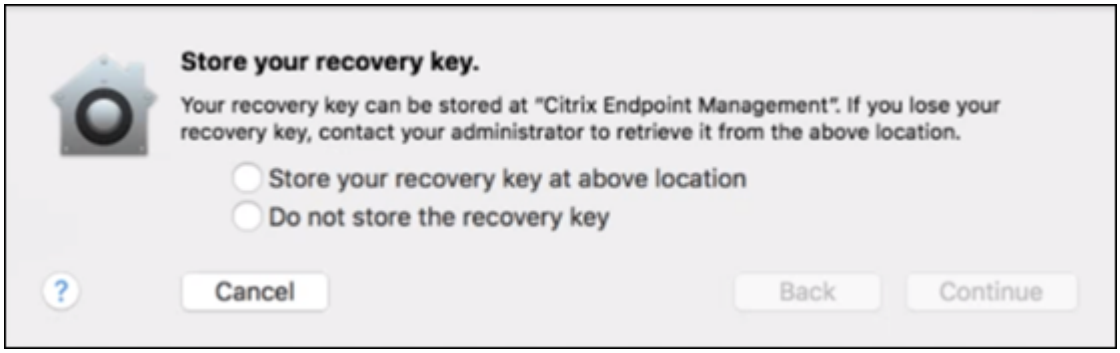
  - 个人和机构恢复密钥：一旦同时启用这两种类型的恢复密钥，则仅当用户丢失了自己的个人恢复密钥时才必须解锁用户设备。

- **Institutional recovery key certificate**（机构恢复密钥证书）：如果选择 **Institutional recovery key**（机构恢复密钥）或 **Personal & Institutional recovery key**（个人和机构恢复密钥）作为 **Recovery key type**（恢复密钥类型），请选择该密钥的恢复密钥证书。

- **Show personal recovery key**（显示个人恢复密钥）：如果设置为开，用户设备将在设置 FileVault 后向用户显示个人恢复密钥。默认值为关。



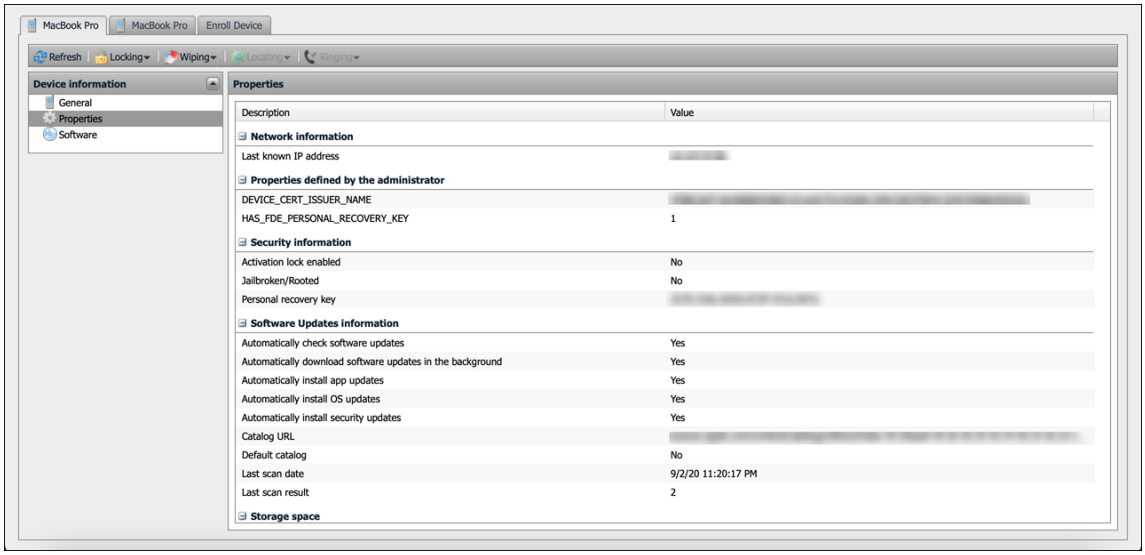
- **Escrow personal recovery key**（托管个人恢复密钥）：启用后，用户可以使用 Endpoint Management 为每台设备存储个人恢复密钥的副本。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要从 Endpoint Management 访问密钥，请转到 **Manage**（管理）**> Devices**（设备），选择 macOS 设备，然后单击 **Edit**（编辑）。然后，转到 **Device details**（设备详细信息）**> General**（常规）并找到 **Personal recovery Key**（个人恢复密钥）。

要允许用户从自助服务门户查看其恢复密钥，请启用 **Escrow personal recovery key**（托管个人恢复密钥）和 **Display personal recovery key to user**（向用户显示个人恢复密钥）。密钥将显示在自助服务门户的 **Properties**（属性）页面上的 **Security information**（安全信息）下。有关自助服务门户的详细信息，请参阅自助服务门户。



即使未启用启用 **FileVault** 设置，也可以启用 **Escrow personal recovery key**（托管个人恢复密钥）设置。如果禁用 **Enable FileVault**（启用 FileVault）设置，用户仍然可以自行启用 FileVault。在这种情况下，启用 **Escrow personal recovery key**（托管个人恢复密钥）以允许用户使用 Endpoint Management 存储其密钥的副本。

如果用户在将设备注册到 Endpoint Management 之前启用了 FileVault，Endpoint Management 不会存储其恢复密钥。设备在控制台中显示为已启用 FileVault。

防火墙设备策略

July 8, 2022

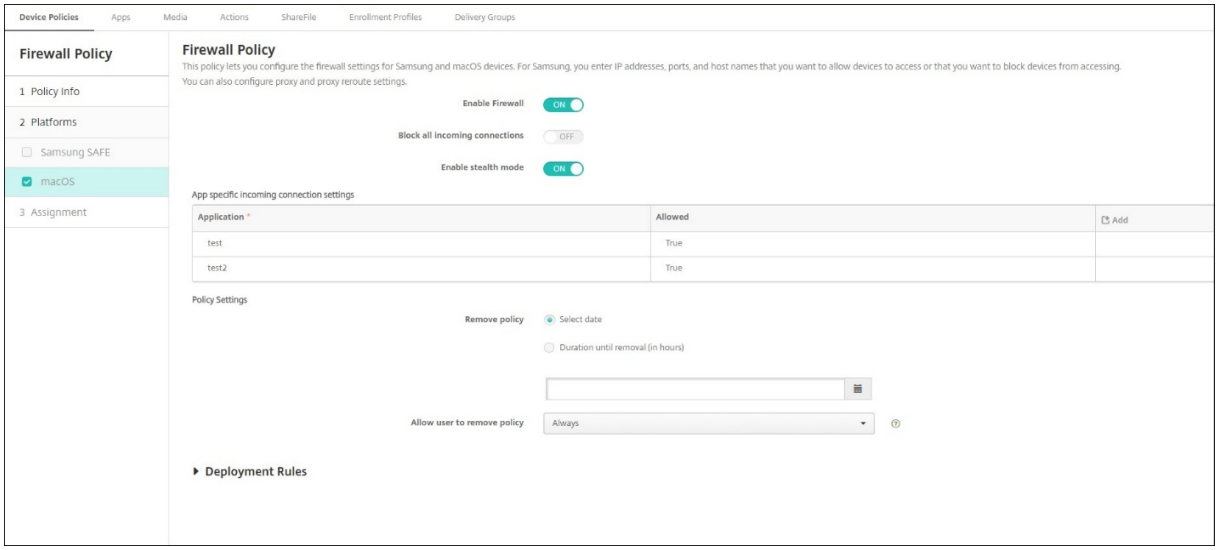
此策略允许您为 Samsung、macOS 和 Windows 设备配置防火墙设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

macOS 设置

需要 macOS 10.12 及更高版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

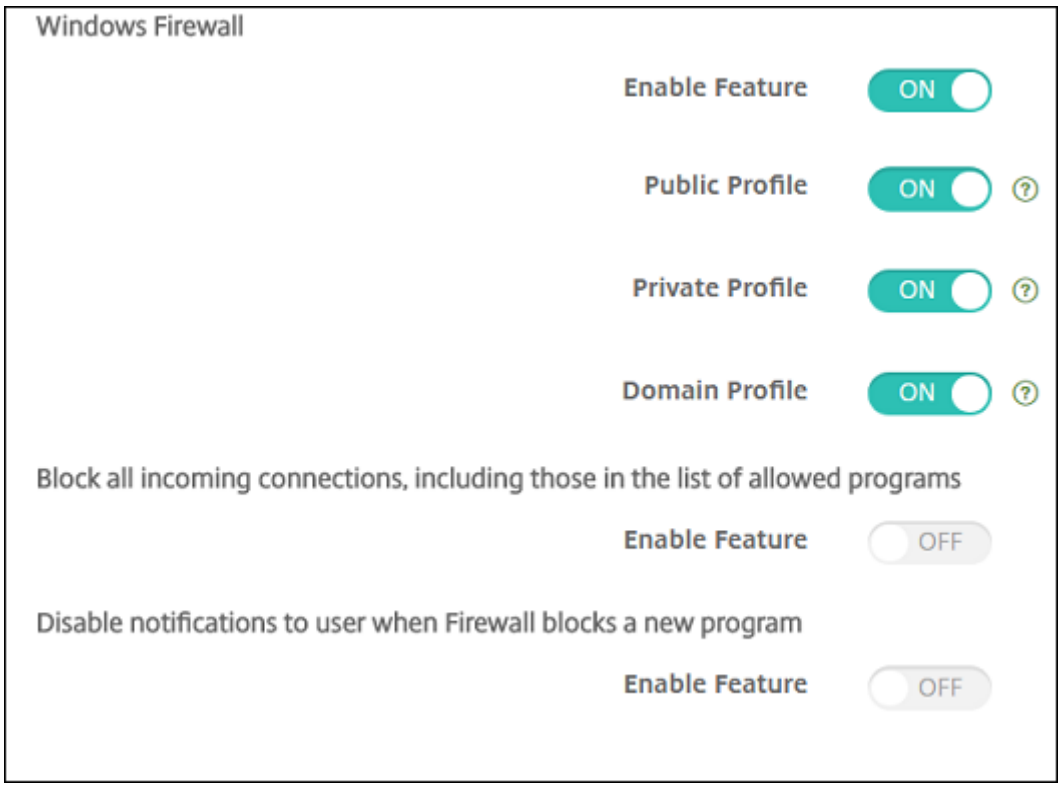


- 启用防火墙。要启用防火墙，请将此选项设置为开。
- 阻止所有传入连接。将此选项设置为开时，将阻止除基础服务所需的连接以外的所有传入连接。
- 启用隐藏模式。在隐藏模式下，设备不响应或承认测试应用程序尝试使用（例如 Ping）从网络对其进行的访问。要启用隐藏模式，请将此选项设置为开。
- 应用程序特定的传入连接设置。要允许特定应用程序接收连接，请添加这些应用程序并将允许设置为真。

Windows Desktop 和 **Tablet** 设置

需要运行 Windows 10（版本 1709 或更高版本）或 Windows 11 的 Windows Desktop 和 Tablet 设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 启用功能：控制部署了此策略的计算机上的传入和传出流量。默认值为开。
- 公用配置文件：控制在计算机连接到公共场所（例如机场或咖啡店）中的不可信网络时的 Windows 防火墙。默认值为开。
- 专用配置文件：控制在计算机连接到可信网络（例如家庭网络）时的 Windows 防火墙。默认值为开。
- 域配置文件：控制在计算机连接到域网络（例如工作区）时的 Windows 防火墙。默认值为开。
- 阻止所有传入连接，包括允许运行的程序列表中的传入连接：默认值为关。
- 禁止在防火墙阻止新程序时向用户发送通知：默认值为关。

字体设备策略

March 31, 2022

可以在 Endpoint Management 中添加一个设备策略，用于向 iOS 和 macOS 设备添加更多字体。字体必须是 TrueType (`.ttf`) 字体或 OpenType (`.oft`) 字体。不支持字体集合（`.ttc` 或 `.otc`）。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 用户可见名称：键入用户在其字体列表中看到的名称。
- 字体文件：要选择添加到用户设备的字体文件，请单击浏览，然后导航到该文件位置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。

macOS 设置

- 用户可见名称：键入用户在其字体列表中看到的名称。
- 字体文件：要选择添加到用户设备的字体文件，请单击浏览，然后导航到该文件位置。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

主屏幕布局设备策略

March 31, 2022

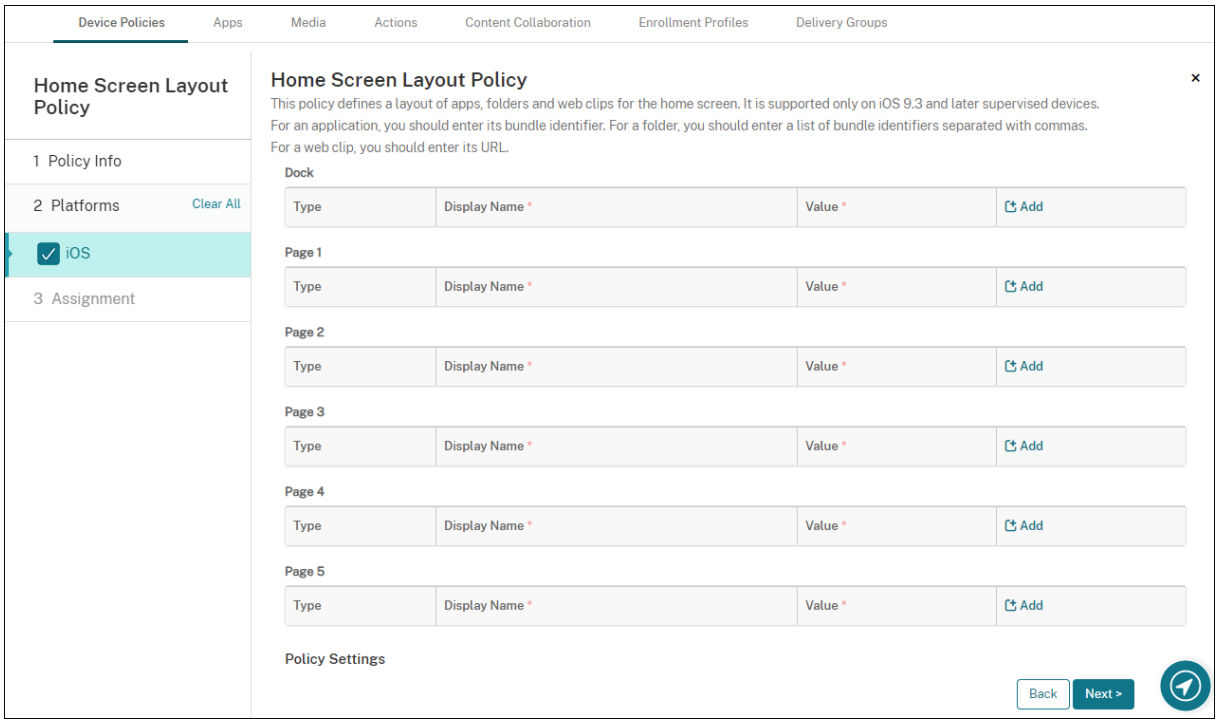
主屏幕布局设备策略允许您为受监督的 iOS 设备的 iOS 主屏幕指定应用程序和文件夹的布局。

> 重要：
>
> 向设备部署多个主屏幕布局策略会导致在设备上产生 iOS 错误。无论是通过此 Endpoint Management 策略还是通过 Apple Configurator 定义主屏幕，都存在此限制。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

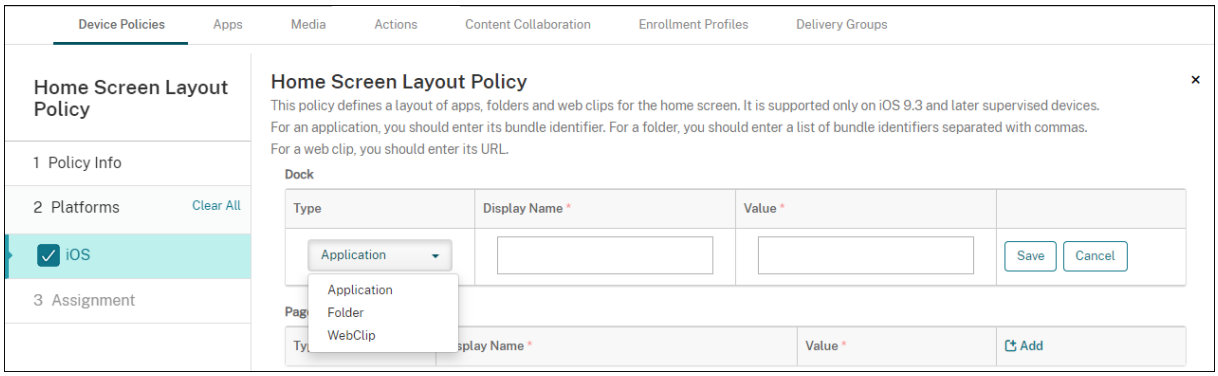
iOS 设置



- 对于要配置的每个屏幕区域（例如，基站或第 **1** 页），单击添加。
- 类型：选择应用程序、文件夹或 **Web** 剪辑。

  “限制”设备策略中的受限应用程序使用 **>** 仅允许部分应用程序设置可以阻止 Web 剪辑在主屏幕上正确显示。为了正确显示 Web 剪辑，请执行以下任一操作：

  - 将受限应用程序使用设置为允许所有应用或不允许某些应用程序。
  - 将受限应用程序使用设置为仅允许部分应用程序后，添加捆绑包 ID 为 `com.apple.webapp` 的应用程序以允许 Web 剪辑。



- 显示名称：应用程序或文件夹在主屏幕上显示的名称。
- 值：对于应用程序，请键入捆绑包标识符。对于文件夹，请键入捆绑包标识符列表（以逗号分隔）。对于 Web 剪辑，请键入捆绑包 ID `com.apple.webClip.managed` 并在 Web 剪辑策略中配置 Web 剪辑的 URL。如果同一个 URL 存在多个 Web 剪辑值，该行为在 iOS 11.3 及更高版本的设备上未定义。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅适用于 iOS 9.3 及更高版本。

“导入设备配置”设备策略

December 20, 2022

通过“导入设备配置”设备策略，您可以将自定义配置部署到 Citrix Ready Workspace Hub 设备。一般步骤如下：

1. 手动配置您的第一个 Citrix Ready Workspace Hub 设备。
2. 从设备下载配置文件。
3. 配置“导入设备配置”策略并部署该策略以将配置推送到所有其他设备。

有关详细信息，请参阅 Workspace Hub 设备管理。

Workspace Hub 设置

- **URL**：文件共享 Web 服务器上托管的配置文件的 URL。

“导入 iOS 和 macOS 配置文件”设备策略

April 11, 2023

可以将 iOS 和 macOS 设备的设备配置 XML 文件导入到 Endpoint Management 中。此文件包含您使用 Apple Configurator 2 或 Profile Creator 准备的设备安全策略和限制。配置 XML 文件可以包含宏。有关详细信息，请参阅宏。

用例

使用 Profile Creator 导入在适用于 macOS 设备的 Endpoint Management 外部创建的以下配置：

- **System Policy Control**（系统策略控制）：该策略标识经认证的 Apple 开发人员签名的应用程序，并允许用户从 Mac App Store 下载经过验证的应用程序。

  配置策略时：

  - 选择 **Enable Gatekeeper**（启用 Gatekeeper）以确保用户仅运行经过验证且受信任的软件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 选择 **Allow Identified Developers**（允许已识别的开发人员）以确保用户安装仅经认证的 Apple 开发人员签名的应用程序。

- **Privacy Preferences Policy Control**（隐私首选项策略控制）：该策略允许您授予或限制对某些文件或功能的跨应用程序访问，例如定位服务、摄像头和屏幕捕获。

  配置您计划部署的设置。有关详细信息，请参阅隐私首选项策略控制有效负载设置。

- **Kernel Extensions Policy**（内核扩展策略）：该策略允许用户安装扩展，以扩展操作系统的本机功能。内核扩展在内核级别运行。

  配置您计划部署的设置。有关详细信息，请参阅内核扩展策略有效负载设置。

- **Ethernet Settings Policy**（以太网设置策略）：该策略允许您管理以太网网络连接。

  配置您计划部署的设置。有关详细信息，请参阅以太网设置。

使用 Apple Configurator 2 或 Profile Creator 为 macOS 和 iOS 设备配置以下策略：

- **Wi-Fi** 策略：此策略允许您管理用户将其设备连接到 Wi-Fi 网络的方式。

  配置策略时：

  - 将目标 SSID 添加到优先级列表的顶部。
  - 选择用户加入网络时要使用的连接模式。如果选择系统，设备将使用系统凭据对用户进行身份验证。如果选择登录窗口，设备将使用在登录窗口中输入的相同凭据对用户进行身份验证。

  有关详细信息，请参阅 Wi-Fi 设置。

- 限制策略：此策略允许或限制在用户设备上使用某些功能。

  配置您计划部署的设置。有关详细信息，请参阅限制概述。

- **VPN** 策略：此策略提供与专用网络的设备级加密连接。

  配置您计划部署的设置。有关详细信息，请参阅 VPN 概述。

使用 **Apple Configurator 2** 创建配置文件

1. 从 Apple App Store 安装 Apple Configurator 2。
2. 启动 Apple Configurator 2，然后转到文件 **>** 新建配置文件。此时将显示一个新配置窗口。
3. 在常规设置窗格中，键入配置文件的名称和标识符，然后添加任何其他有效负载选项。
4. 在左侧窗格中，选择一个有效负载，单击配置，然后输入设置。请不要为您的配置文件签名，因为不支持已签名的配置文件。

   要在单个配置文件中添加多个有效负载，请选择一个有效负载，然后单击右上角的 **Add Payload**（添加有效负载）按钮。

5. 转到文件 **>** 保存，选择要保存 XML 文件的名称和位置，然后单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

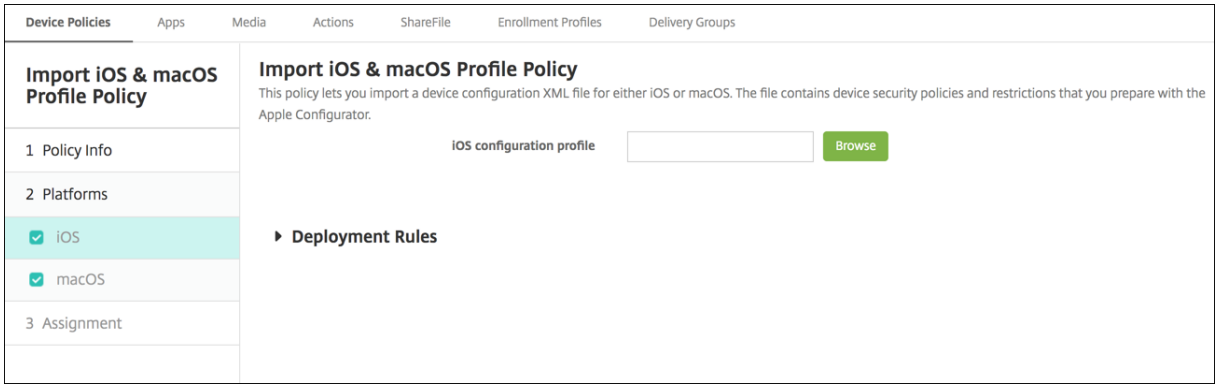
使用 **Profile Creator** 创建配置文件

1. 从 GitHub 安装 Profile Creator。
2. 启动 Profile Creator，然后转到文件 **>** 新建。此时将显示一个新配置窗口。
3. 在常规设置窗格中，键入配置文件的名称和说明，然后添加任何其他有效负载选项。
   - 建议：选择 **Prevent users from removing this profile**（阻止用户删除此配置文件）。
   - 将 **Payload Scope**（有效负载作用域）设置为 **System**（系统）或 **User**（用户）。
4. 在左侧窗格中，选择策略，配置设置，然后单击右上角的添加。

   要在单个配置文件中配置多个策略，请选择一个策略，然后单击添加按钮。
5. 转到文件 **>** 导出，选择要保存 XML 文件的名称和位置，然后单击保存。

要在 Endpoint Management 控制台中导入适用于 iOS 和 macOS 配置文件设备策略的配置文件，请转到配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 和 **macOS** 设置



- **iOS** 配置文件或 **macOS** 配置文件：要选择要导入的配置文件，请单击浏览，然后导航到此文件所在位置。

键盘锁管理设备策略

April 11, 2023

Android 键盘锁管理设备和工作挑战锁定界面。此策略允许您管理 Android Enterprise 工作配置文件键盘锁和高级设备键盘锁的功能。您可以控制：

- 工作配置文件设备上的键盘锁管理。可以在用户解锁设备键盘锁和工作质询键盘锁之前指定其可用的功能。例如，默认情况下，用户可以使用指纹解锁并在锁定屏幕上查看未编辑的通知。
- 在完全托管设备和专用设备上进行键盘锁管理。可以指定可用的功能，例如信任代理和安全摄像头，然后才能解锁键盘锁屏幕。或者，可以选择禁用所有键盘锁功能。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 具有工作配置文件的完全托管设备上的键盘锁管理。这些设备以前称为 COPE（企业拥有但由个人使用）设备。可以使用一个键盘锁管理策略将单独的设置应用到设备和工作配置文件。

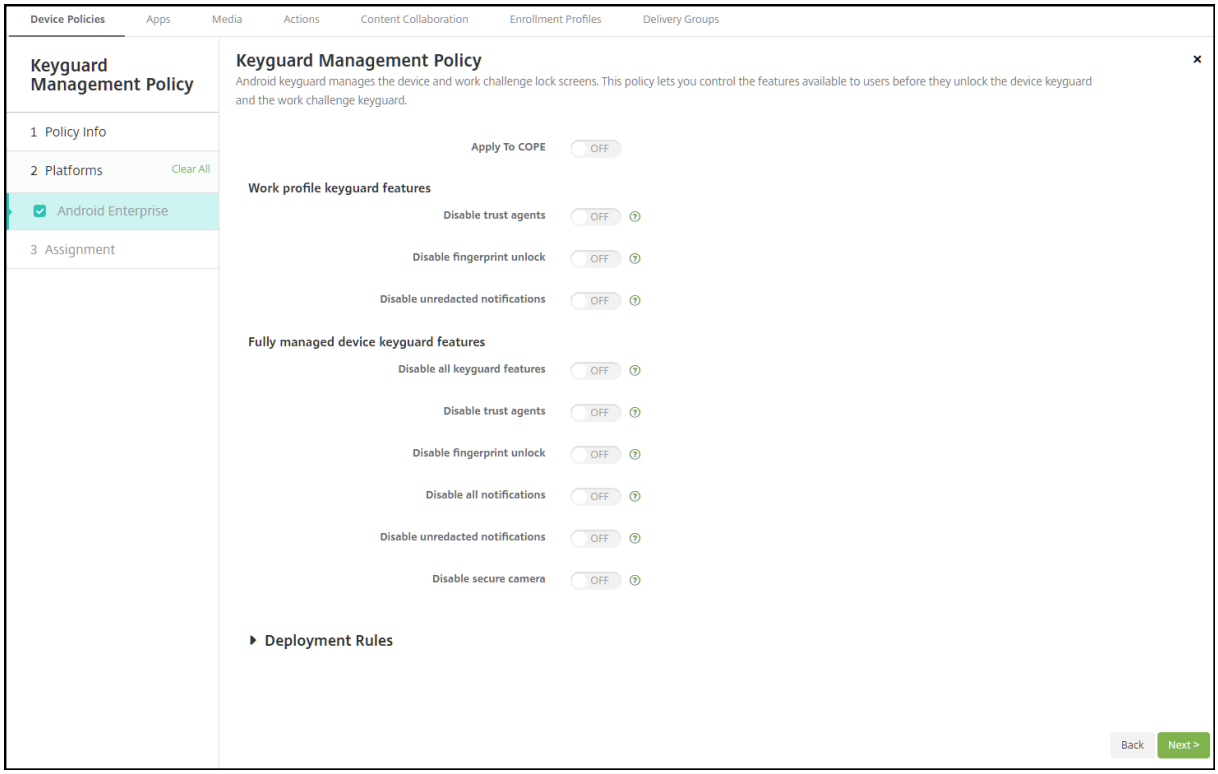
要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

观看此视频以了解更多：



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android Enterprise 设置



- 应用到 **COPE**：允许您为具有工作配置文件的完全托管设备配置键盘锁管理设备策略。

  当此设置设为开时，您可以将单独的设置应用到设备或具有工作配置文件的完全托管设备上的工作配置文件。

  当此设置设为关时，您可以将设置应用到工作配置文件设备或完全托管设备。为工作配置文件配置的设置仅适用于工作配置文件设备。为完全托管设备配置的设置仅适用于完全托管设备。

  默认设置为关。

- 工作配置文件键盘锁功能：控制在用户解锁工作配置文件键盘锁（锁屏界面）之前以下功能是否可用。

  - 禁用信任代理：如果设置为关，则在工作配置文件中设置了质询时，信任代理可以在安全的键盘锁屏幕上运行。设置为开将在工作配置文件中禁用所有信任代理。默认设置为关。
  - 禁用生物特征身份验证：如果设置为关，则在工作配置文件中设置了质询时，可以在安全的键盘锁屏幕上使用生物特征识别身份验证。设置为开将在工作配置文件中禁用生物特征识别身份验证。此设置将禁用指纹解锁、人脸身份验证和虹膜身份验证。默认设置为关。适用于 Android 9.0 及更高版本。
  - 禁用指纹解锁：如果设置为关，则在工作配置文件中设置了质询时，可以在安全的键盘锁屏幕上使用指纹解锁。设置为开将在工作配置文件中禁用指纹解锁。默认设置为关。
  - 禁用人脸身份验证：如果设置为关，则在工作配置文件中设置了质询时，可以在安全的键盘锁屏幕上使用人脸身份验证。设置为开将在工作配置文件中禁用人脸身份验证。默认设置为关。适用于 Android 9.0 及更高版本。
  - 禁用虹膜身份验证：如果设置为关，则在工作配置文件中设置了质询时，可以在安全的键盘锁屏幕上使用虹膜身份验证。设置为开将在工作配置文件中禁用虹膜身份验证。默认设置为关。适用于 Android 9.0 及

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

更高版本。

- 禁用未编辑的通知：如果设置为关，已遍及的通知和未编辑的通知将显示在安全的键盘锁屏幕上。设置为开将禁用未编辑的通知并仅显示已编辑的通知。默认设置为关。

- 完全托管设备键盘锁功能：控制在用户解锁设备键盘锁（锁屏界面）之前以下功能是否可用。这些功能适用于完全托管设备或专用设备。
  - 禁用所有键盘锁功能：如果设置为关，则可以在安全的键盘锁屏幕上使用所有当前和将来的键盘锁自定义设置。设置为开将禁用所有键盘锁自定义设置。默认设置为关。
  - 禁用信任代理：如果设置为关，信任代理可以在安全的键盘锁屏幕上运行。设置为开将禁用信任代理。默认设置为关。
  - 禁用生物特征身份验证：如果设置为关，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用生物特征识别身份验证。设置为开将在设备上禁用生物特征识别身份验证。禁用的生物特征识别身份验证功能为指纹解锁、人脸身份验证和虹膜身份验证。默认设置为关。适用于 Android 9.0 及更高版本。
  - 禁用指纹解锁：如果设置为关，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用指纹解锁。设置为开将在设备上禁用指纹解锁。默认设置为关。
  - 禁用人脸身份验证：如果设置为关，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用人脸身份验证。设置为开将在设备上禁用人脸身份验证。默认设置为关。适用于 Android 9.0 及更高版本。
  - 禁用虹膜身份验证：如果设置为关，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用虹膜身份验证。设置为开将在设备上禁用虹膜身份验证。默认设置为关。适用于 Android 9.0 及更高版本。
  - 禁用所有通知：如果设置为关，所有通知都将显示在安全的键盘锁屏幕上。设置为开将显示所有通知。默认设置为关。
  - 禁用未编辑的通知：如果设置为关，已遍及的通知和未编辑的通知将显示在安全的键盘锁屏幕上。设置为开将禁用未编辑的通知并仅显示已编辑的通知。默认设置为关。
  - 禁用安全摄像头：如果设置为关，可以在安全的键盘锁屏幕上使用安全摄像头。设置为开将禁用安全摄像头。默认设置为关。

网亭设备策略

July 24, 2023

网亭策略允许您通过限制可运行的应用程序，将设备限制为网亭策略。Citrix Endpoint Management 不控制设备的哪部分锁定在网亭模式。部署策略后，该设备将管理网亭模式设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

要将 iPad 设置为在网亭模式下运行，请使用 “应用程序锁定” 设备策略。有关将 iPad 设置为自助终端的信息，请参阅将 iPad 配置为自助终端。您还可以将 iPad 配置为只打开一个网站。有关信息，请参阅 Web 剪辑策略。

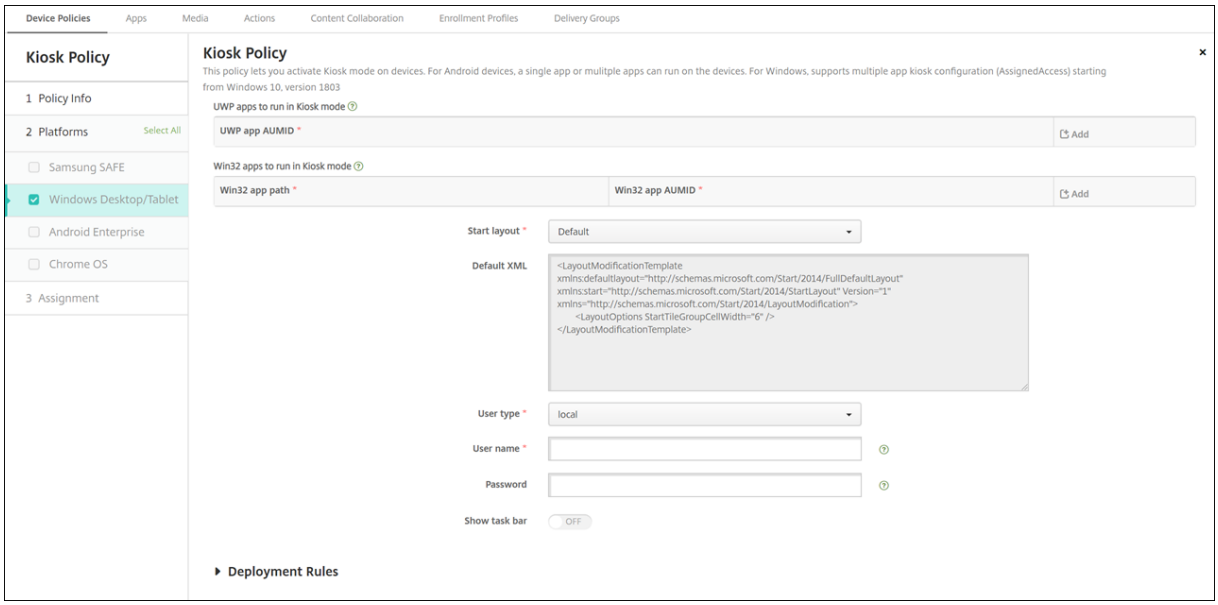
Windows Desktop 和 **Tablet** 设置

对于 Windows Desktop 和 Tablet 设备，网亭策略仅适用于本地用户以及在 Azure AD 中注册的用户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

单个应用程序或多个应用程序可以在 Windows Desktop 和 Tablet 设备上以展台模式运行。

> 注意：
>
> 信息亭设备策略仅适用于 Windows 10 设备。
> 要在 Windows 11 设备上部署单应用程序自助服务终端，可以使用自定义 XML 设备策略将我们提供给设备的 XML 脚本部署。有关更多信息，请参阅在 Windows 11 设备上部署单应用程序自助服务终端。



- **UWP** 应用程序 **AUMID**：单击 添加，选择通用 Windows 平台 (UWP) 应用程序，然后为每个 UWP 应用程序输入应用程序用户模型 ID (AUMID)。例如，输入以下 AUMID：
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Win32** 应用程序路径和 **Win32** 应用 **AUMID**：单击 添加，选择 Windows 桌面 (Win32) 应用程序，然后输入每个 Win32 应用的路径和 AUMID。例如，输入以下路径和 AUMID：
  - `%windir%\system32\mspaint.exe` 或 `C:\Windows\System32\mspaint.exe`
  - `{ 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7 } \mspaint.exe`
- **“开始”** 屏幕布局：只有应用程序的默认开始屏幕可用。
- 默认 **XML**：只有默认 XML 脚本可用。
- **Select user type**（选择用户类型）：指定接收网亭策略的用户类型。您的选项：
  - 本地： Endpoint Management 为目标设备创建用户或添加现有用户。
  - **Azure AD**： Endpoint Management 添加在 Azure AD 中注册的用户。
- 用户名：输入用户名以接收网亭策略。
  - 要在目标设备上创建本地用户名，请输入名称。确保您的本地用户名不包含域。如果输入现有名称，Endpoint Management 不会创建用户或更改当前密码。
  - 要添加 Azure AD 用户，请以 `azuread\user` 格式输入名称。`user` 部分可以是在 Azure AD 中创建用户时输入的名称，也可以是在 Azure AD 中创建用户时输入的用户名。分配的用户不能是 Azure AD 管理员。
- 密码： Azure AD 用户没有密码配置。请仅键入本地用户名对应的密码。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 显示任务栏：启用任务栏，以便为用户提供查看和管理应用程序的简便方法。默认值为关。
- 单击下一步保存更改。

对于您希望允许在网亭模式下运行的 UWP 应用程序，需要提供 AUMID。要获取为当前设备用户安装的所有 Microsoft 应用商店应用程序的 AUMID 的列表，请运行以下 PowerShell 命令。

```
$installedapps = get-AppxPackage

$aumidList = @()
foreach ($app in $installedapps)
{

    foreach ($id in (Get-AppxPackageManifest $app).package.applications
       .application.id)
    {

        $aumidList += $app.packagefamilyname + "!"+ $id
     }

 }


$aumidList
<!--NeedCopy-->
```

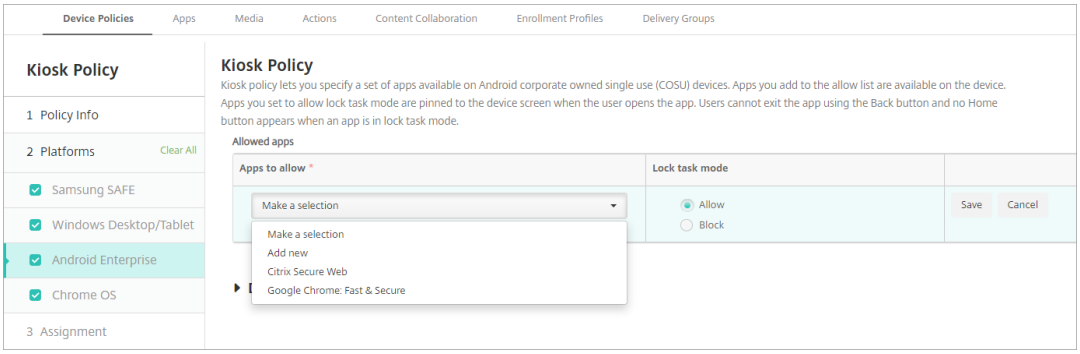
Android Enterprise 设置

对于专用 Android Enterprise 设备（又称为企业拥有，单一用途 (COSU) 设备），可以允许运行应用程序并设置锁定任务模式。

要允许运行应用程序，请单击添加。可以将多个应用程序添加到允许列表中。有关详细信息，请参阅 Android Enterprise。

- **Apps to allow**（要允许运行的应用程序）：输入要允许运行的应用程序的软件包名称，或者从列表中选择应用程序。
  - 单击新增以输入列表中允许运行的应用程序的软件包名称。
  - 从列表中选择现有应用程序。该列表显示了在 Endpoint Management 中上载的应用程序。默认情况下，Secure Hub 和 Google Play 服务都在允许列表中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 锁定任务模式：选择允许可设置要在用户启动应用程序时固定到设备屏幕的应用程序。选择阻止可设置不固定的应用程序。默认设置为允许。

当某个应用程序处于锁定任务模式时，用户打开时该应用程序将固定到设备屏幕。没有显示“主页”按钮，“返回”按钮被禁用。用户使用编程到该应用程序中的一项操作退出该应用程序，例如注销。

Launcher 配置设备策略

March 31, 2022

使用 Citrix Launcher 可以自定义由 Endpoint Management 部署的 Android Enterprise 设备和旧版 Android 设备的用户体验。

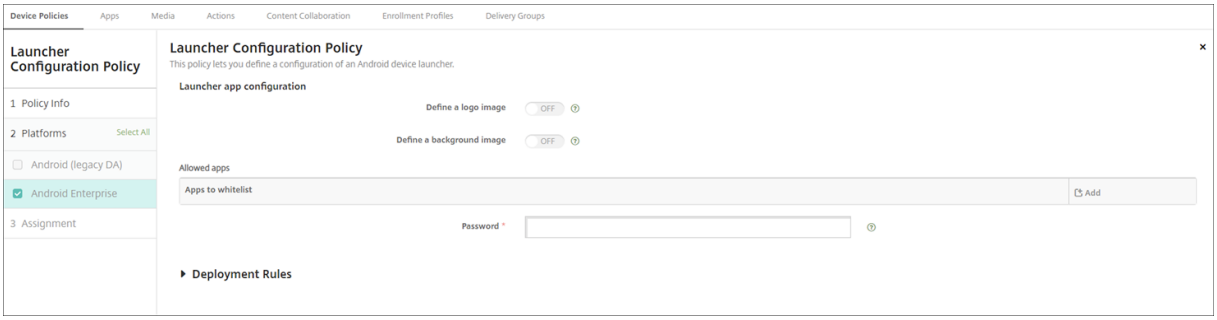
请使用 Launcher 配置策略控制以下 Citrix Launcher 功能：

- 管理 Android Enterprise 设备和旧版 Android 设备，以便用户只能访问您指定的应用程序。
- （可选）为 Citrix Launcher 图标指定自定义徽标图片以及为 Citrix Launcher 指定自定义背景图片。
- 指定用户在退出启动程序前必须键入的密码。

Citrix Launcher 并不作为设备平台在已提供的安全层之外额外提供的一个安全层。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

Android Enterprise 和 Android 设置



- 定义徽标图片：选择是否对 Citrix Launcher 图标使用自定义徽标图片。默认值为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 徽标图片：启用定义徽标图片时，单击浏览并导航到图片文件所在位置，选择此文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- 定义背景图片：选择是否对 Citrix Launcher 背景使用自定义图片。默认值为关。
- 背景图片：启用定义背景图片时，单击浏览并导航到图片文件所在位置，选择此文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- 允许的应用程序：对于要在 Citrix Launcher 中允许使用的每个应用程序，单击添加，然后执行以下操作：
  - 要添加的新应用程序：输入要添加的应用程序的完整名称。例如，com.android.calendar 表示 Android 日历应用程序。
  - 单击保存以添加应用程序，或单击取消以取消添加应用程序。
- 密码：用户退出 Citrix Launcher 时必须输入的密码。

LDAP 设备策略

March 31, 2022

可以在 Endpoint Management 中为 iOS 设备创建 LDAP 策略，用于提供与要使用的 LDAP 服务器有关的信息，包括任何必要的帐户信息。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。

配置此策略之前，您需要提供 LDAP 主机名。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 帐户说明：输入可选帐户说明。
- 帐户用户名：输入可选用户名。
- 帐户密码：输入可选密码。此字段仅适用于加密的配置文件。
- **LDAP** 主机名：输入 LDAP 服务器的主机名。此字段为必填字段。
- 使用 **SSL**：选择是否使用安全套接字层连接到 LDAP 服务器。默认值为开。
- 搜索设置：添加查询 LDAP 服务器时要使用的搜索设置。可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。单击添加，然后执行以下操作：
  - 说明：输入搜索设置的说明。此字段为必填字段。
  - 范围：选择基础、一级或子树以定义搜索 LDAP 树的深度。默认值为基础。
    - 基础搜索“搜索基础”指向的节点。
    - 一级搜索基础节点及其下一级节点。
    - 子树搜索基础节点及其所有子节点，而无论深度为何。
  - 搜索基础：输入开始搜索时所在节点的路径。例如 ou=people 或 0=example corp。此字段为必填字段。
  - 单击保存添加搜索设置，或单击取消以取消添加搜索设置。
  - 为要添加的每个搜索设置重复执行这些步骤。
- 策略设置

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    * 选择日期：单击日历可选择具体删除日期。
    * 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。

macOS 设置

- 帐户说明：输入可选帐户说明。
- 帐户用户名：输入可选用户名。
- 帐户密码：输入可选密码。此字段仅适用于加密的配置文件。
- **LDAP** 主机名：输入 LDAP 服务器的主机名。此字段为必填字段。
- 使用 **SSL**：选择是否使用安全套接字层连接到 LDAP 服务器。默认值为开。
- 搜索设置：添加查询 LDAP 服务器时要使用的搜索设置。可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。单击添加，然后执行以下操作：
  - 说明：输入搜索设置的说明。此字段为必填字段。
  - 范围：选择基础、一级或子树以定义搜索 LDAP 树的深度。默认值为基础。
    * 基础搜索 “搜索基础” 指向的节点。
    * 一级搜索基础节点及其下一级节点。
    * 子树搜索基础节点及其所有子节点，而无论深度为何。
  - 搜索基础：输入开始搜索时所在节点的路径。例如 ou=people 或 0=example corp。此字段为必填字段。
  - 单击保存添加搜索设置，或单击取消以取消添加搜索设置。
  - 为要添加的每个搜索设置重复执行这些步骤。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    * 选择日期：单击日历可选择具体删除日期。
    * 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

位置设备策略

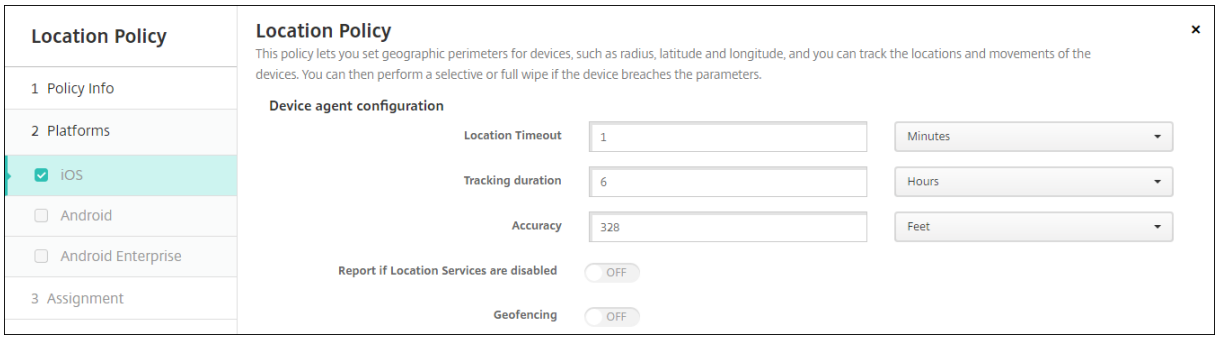
March 31, 2022

可以在 Endpoint Management 中创建定位设备策略以强制实施地理边界。用户超出定义的边界（也称为地理围栏）时，Endpoint Management 可以执行某些操作。例如，您可以配置策略以在用户超出定义的外围时向用户发出警告消息。您还可以配置策略以在用户超出外围时立即或延迟一段时间后擦除用户的公司数据。有关安全操作的信息（例如，启用跟踪和定位设备），请参阅安全操作。

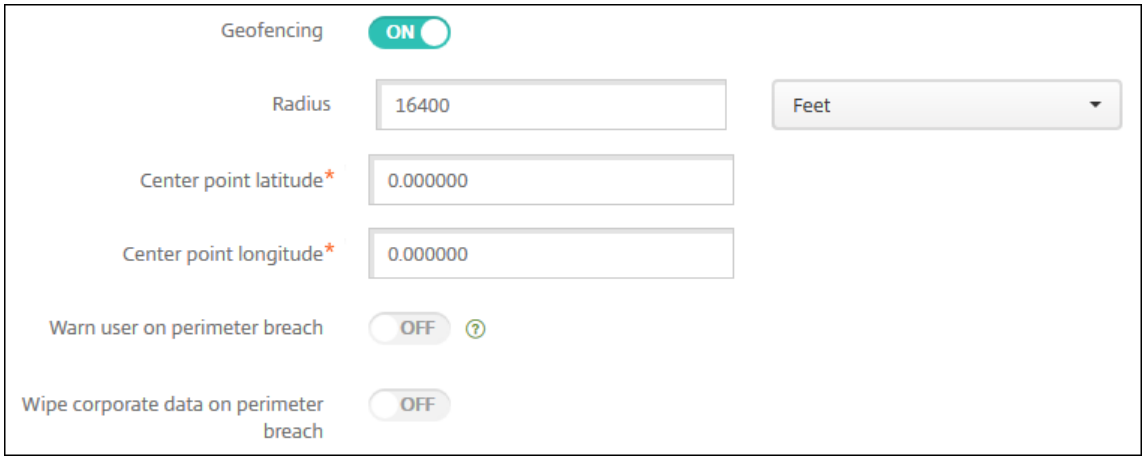
要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 设置



- 定位超时：键入数值，然后单击秒或分钟以设置 Endpoint Management 尝试修复设备位置的频率。有效值为 60-900 秒或 1-15 分钟。默认值为 **1** 分钟。
- 跟踪持续时间：键入数值，然后单击小时或分钟以设置 Endpoint Management 跟踪设备的时间长度。有效值为 1–10 小时或 10–600 分钟。默认值为 **6** 小时。
- 准确度：键入数值，然后单击米、英尺或码以设置 Endpoint Management 跟踪设备的接近程度。有效值为 10–5000 码、30–15000 英尺或 10-5000 米。默认值为 **328** 英尺（**100** 米）。
- 禁用定位服务时报告：选择当用户关闭 GPS 时设备是否向 Endpoint Management 发送报告。默认值为关。
- 地理围栏



启用地理围栏后，请配置以下设置：

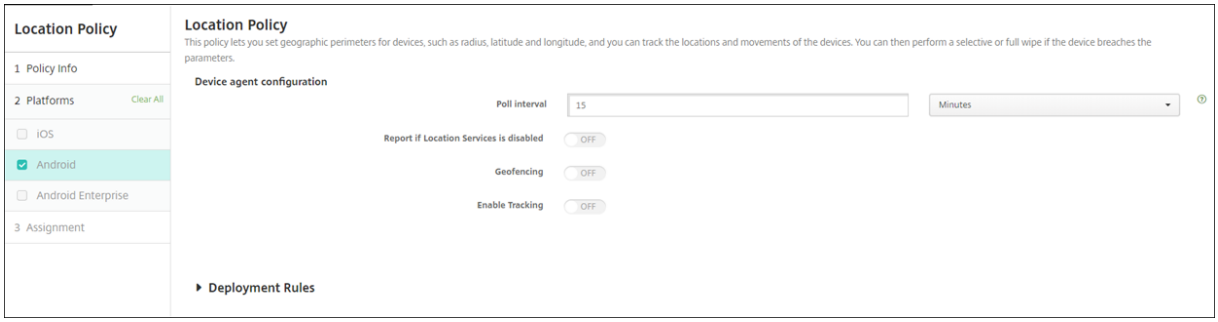
- 半径：键入数值，然后单击要用于度量半径的单位。默认值为 **16400** 英尺（**5000** 米）。半径的有效值如下：
  - 164–16400 英尺
  - 50-50000 米
  - 54-54680 码
  - 1-31 英里
- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

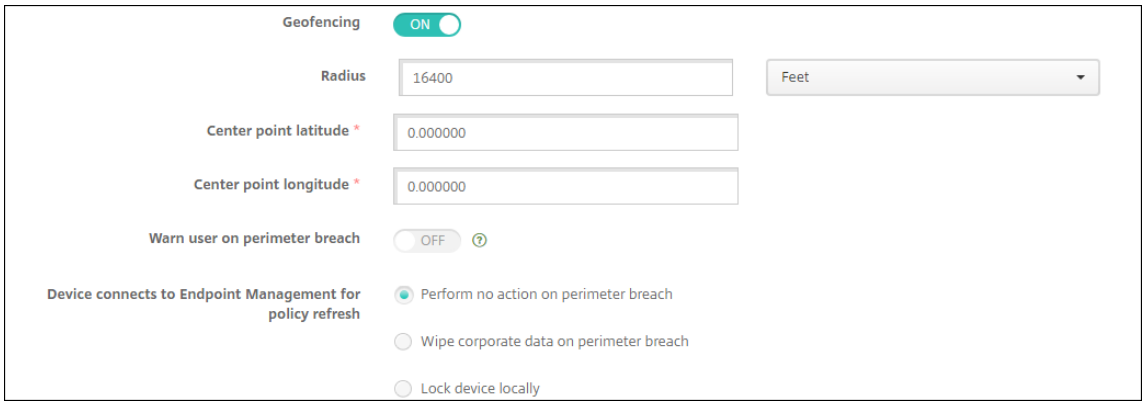
- 超出边界时警告用户：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 Endpoint Management 即可显示警告消息。
- 超出边界时擦除公司数据：选择当用户超出边界时是否擦除用户设备。默认值为关。启用此选项时，将显示本地擦除延迟字段。
  - 键入数值，然后单击秒或分钟以设置擦除用户设备中的公司数据之前延迟的时间长度。此延迟使用户有机会在 Endpoint Management 选择性擦除其设备之前返回到允许的位置。默认值为 **0** 秒。

Android（旧版 **DA**）设置

Android 位置跟踪需要 Android 9 或更高版本。



- 轮询间隔：键入数值，然后单击分钟、小时或天以设置 Endpoint Management 尝试修复设备所在位置的频率。有效值为 15-1440 分钟、1-24 小时或任意天数。默认值为 **15** 分钟。
- 禁用定位服务时报告：选择当用户关闭 GPS 时设备是否向 Endpoint Management 发送报告。默认值为关。
- 地理围栏



  启用地理围栏后，请配置以下设置：

- 半径：键入数值，然后单击要用于度量半径的单位。默认值为 **16400** 英尺（**5000** 米）。半径的有效值如下：
  - 164–164000 英尺
  - 1-50 千米
  - 50-50000 米
  - 54-54680 码

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

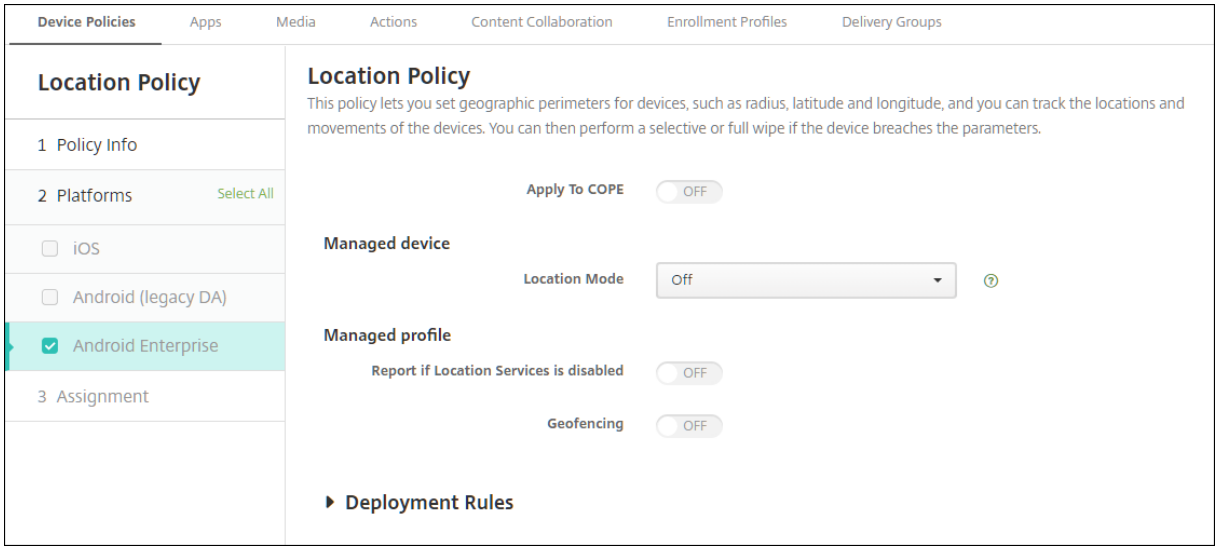
  - 1-31 英里

- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- 超出边界时警告用户：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 Endpoint Management 即可显示警告消息。
- 设备连接到 **Endpoint Management** 以刷新策略：针对用户超出边界时选择以下选项之一：
  - 超出边界时不执行任何操作：不执行任何操作。这是默认值。
  - 超出边界时擦除公司数据：在指定的时间长度后擦除公司数据。启用此选项时，将显示本地擦除延迟字段。
    - 键入数值，然后单击秒或分钟以设置擦除用户设备中的公司数据之前延迟的时间长度。此延迟使用户有机会在 Endpoint Management 选择性擦除其设备之前返回到允许的位置。默认值为 **0** 秒。
  - 本地锁定设备：在指定的时间长度后锁定用户的设备。启用此选项时，将显示锁定延迟字段。
    - 键入数值，然后单击秒或分钟以设置锁定用户设备之前延迟的时间长度。此延迟使用户有机会在 Endpoint Management 锁定其设备之前返回到允许的位置。默认值为 **0** 秒。
- 启用跟踪：选择设备是否跟踪用户位置。默认值为关。

Android Enterprise 设置

要使 Android 位置跟踪起作用，请确保满足以下要求：

- Android 9 或更高版本
- 在 Android Enterprise 的“限制设备”策略中启用了“允许位置共享”设置
- 连接计划（推荐使用 Firebase Cloud Messaging）



应用到使用工作配置文件的完全托管设备

对于具有工作配置文件的完全托管设备（以前称为 COPE 设备），只有位置模式设置可用。

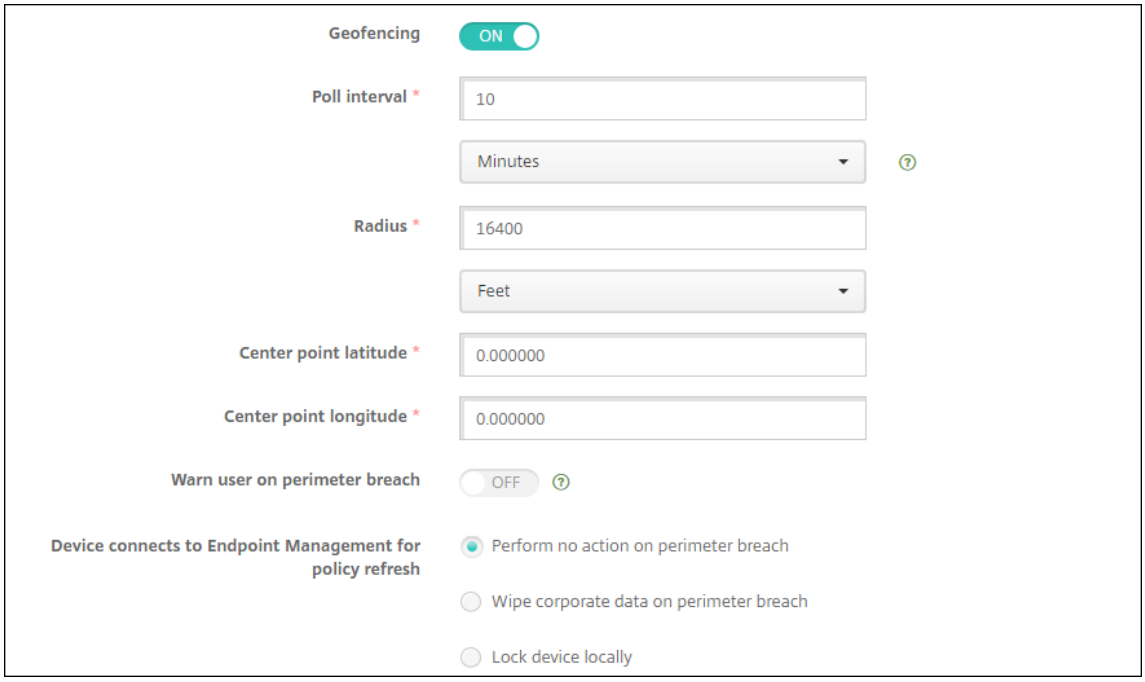
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备：允许您为具有工作配置文件的完全托管设备配置位置模式。启用此设置后，请为工作配置文件配置以下设置：
  - 禁用定位服务时报告：选择当用户关闭 GPS 时设备是否向 Endpoint Management 发送报告。默认值为关。
  - 地理围栏：请参阅本文中托管设备下的设置。

当应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备设置为“关”时，设置将应用到托管设备和工作配置文件，如以下部分中所示。默认设置为关。

托管设备

- 位置模式：指定要启用的位置检测程度。仅当位置模式设置为高精度或电池节能时，可以使用“定位”安全操作。默认值为高精度。
  - 高精度：启用所有位置检测方法，包括 GPS、网络和其他传感器。
  - 仅限传感器：仅启用 GPS 和其他传感器。
  - 电池节能：仅启用网络位置提供程序。
  - 关：禁用位置检测。
- 地理围栏：



启用地理围栏后，请配置以下设置：

- 轮询间隔：键入数值，然后单击分钟、小时或天以设置 Endpoint Management 尝试修复设备所在位置的频率。有效值为 1-1440 分钟、1-24 小时或任意天数。默认值为 **10** 分钟。将此值设置为小于 10 分钟可能会对设备的电池寿命产生不利影响。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 半径：键入数值，然后单击要用于度量半径的单位。默认值为 **16400** 英尺（**5000** 米）。半径的有效值如下：
  - 164–164000 英尺
  - 1-50 千米
  - 50-50000 米
  - 54-54680 码
  - 1-31 英里
- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。要查找值，请转至管理 **>** 设备，选择设备，单击安全，然后单击定位。定位设备后，Endpoint Management 会在安全性下的设备详细信息 **>** 常规页面中报告设备位置。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- 超出边界时警告用户：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 Endpoint Management 即可显示警告消息。
- 设备连接到 **Endpoint Management** 以刷新策略：针对用户超出边界时选择以下选项之一：
  - 超出边界时不执行任何操作：不执行任何操作。这是默认设置。
  - 超出边界时擦除公司数据：在指定的时间长度后擦除公司数据。启用此选项时，将显示本地擦除延迟字段。
    - 键入数值，然后单击秒或分钟以设置擦除用户设备中的公司数据之前延迟的时间长度。此延迟使用户有机会在 Endpoint Management 选择性擦除其设备之前返回到允许的位置。默认值为 **0** 秒。
  - 本地锁定设备：在指定的时间长度后锁定用户的设备。启用此选项时，将显示锁定延迟字段。
    - 键入数值，然后单击秒或分钟以设置锁定用户设备之前延迟的时间长度。此延迟使用户有机会在 Endpoint Management 锁定其设备之前返回到允许的位置。默认值为 **0** 秒。

工作配置文件

- 禁用定位服务时报告：选择当用户关闭 GPS 时设备是否向 Endpoint Management 发送报告。默认值为关。
- 地理围栏：请参阅本文中托管设备下的设置。

锁屏界面消息设备策略

March 31, 2022

“锁屏界面消息”策略允许您设置以下 iOS 设备丢失时要在其上显示的消息：

- 共用的 iPad 的登录窗口
- 受监督 iOS 设备的锁屏界面

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 设置

- 设备的资产标签信息：设备的资产标签。Apple 设备将截断长字符串，因此，请务必在将此策略部署到生产环境之前测试字符串。字符串长度取决于 Apple 设备型号和 Apple 设置，可以对其进行更改。
- 登录窗口和锁屏界面脚注：有助于返回设备的信息，例如地址或其他联系信息。例如，您的消息格式可能是“如果丢失，则返回到”。Apple 设备将截断长字符串，因此，请务必在将此策略部署到生产环境之前测试字符串。字符串长度取决于 Apple 设备型号和 Apple 设置，可以对其进行更改。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    * 选择日期：单击日历可选择具体删除日期。
    * 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

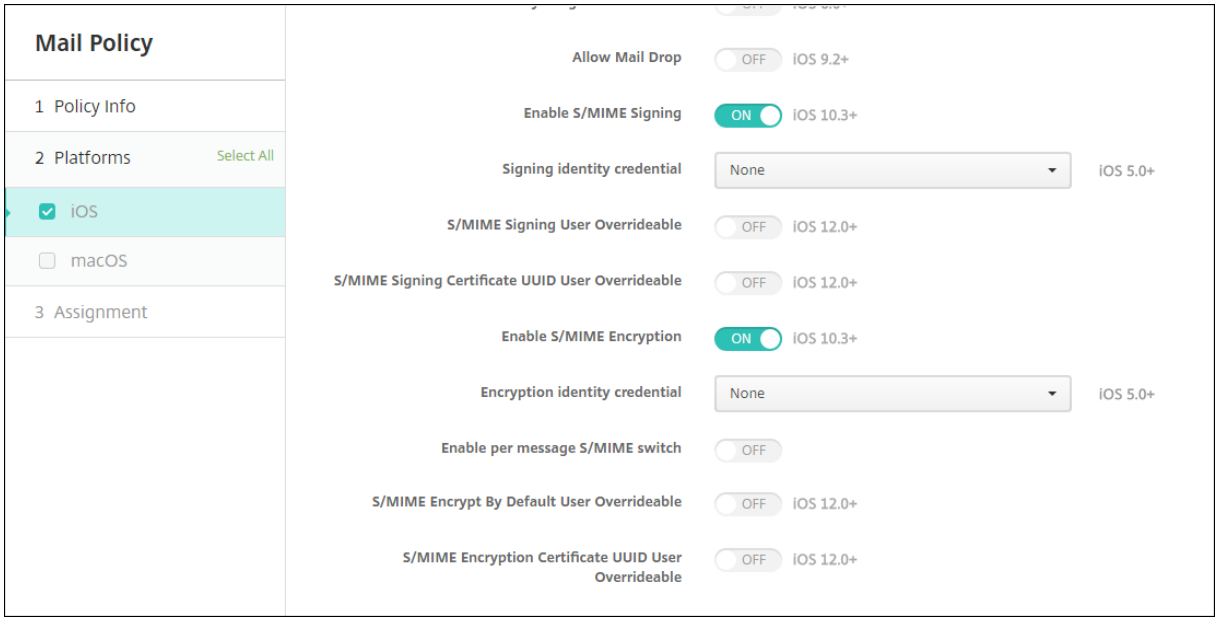
邮件设备策略

March 31, 2022

可以在 Endpoint Management 中添加邮件设备策略以在用户的 iOS 或 macOS 设备上配置电子邮件帐户。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 和 macOS 设置



- 帐户说明：键入在邮件和设置应用程序中显示的帐户说明。此字段为必填字段。
- 帐户类型：选择 **IMAP** 或 **POP** 以选择要用于用户帐户的协议。默认值为 **IMAP**。选择 **POP** 时，以下路径前缀选项将消失。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 路径前缀：键入 **INBOX** 或您的 IMAP 邮件帐户路径前缀。此字段为必填字段。
- 用户显示名称：键入要用于邮件及其他用途的完整用户名。此字段为必填字段。
- 电子邮件地址：键入帐户的完整电子邮件地址。此字段为必填字段。
- 传入电子邮件设置
  - 电子邮件服务器主机名：键入传入电子邮件服务器主机名或 IP 地址。此字段为必填字段。
  - 电子邮件服务器端口：键入传入邮件服务器端口号。默认值为 **143**。此字段为必填字段。
  - 用户名：键入电子邮件帐户的用户名。此名称通常与电子邮件地址中 @ 字符前面的部分相同。此字段为必填字段。
  - 身份验证类型：选择要使用的身份验证类型。默认值为密码。选择无时，以下密码字段将消失。
  - 密码：键入传入邮件服务器的可选密码。
  - 使用 **SSL**：选择传入邮件服务器是否使用安全套接字层身份验证。默认值为关。
- 传出电子邮件设置
  - 电子邮件服务器主机名：输入传出邮件服务器主机名或 IP 地址。此字段为必填字段。
  - 电子邮件服务器端口：键入传出邮件服务器端口号。如果未输入端口号，将使用指定协议的默认端口。
  - 用户名：键入电子邮件帐户的用户名。此名称通常与电子邮件地址中 @ 字符前面的部分相同。此字段为必填字段。
  - 身份验证类型：选择要使用的身份验证类型。默认值为密码。
  - 密码：键入传出邮件服务器的可选密码。
  - 传出密码和传入密码相同：选择传入密码和传出密码是否相同。默认值为关，表示密码不相同。
  - 使用 **SSL**：选择传出邮件服务器是否使用安全套接字层身份验证。默认值为关。
- 策略
  - 授权电子邮件在帐户之间移动：选择是否允许用户：
    - 将电子邮件从此帐户移出到另一个帐户
    - 从其他帐户转发电子邮件
    - 答复来自其他帐户的邮件。

    默认值为关。
  - 仅从邮件应用程序发送电子邮件：选择是否限制用户只能从 iOS 邮件应用程序发送电子邮件。
  - 禁用最新邮件同步：选择是否阻止用户同步最近使用的地址。默认值为关。此选项仅适用于 iOS 6.0 及更高版本。
  - 允许投递邮件：选择是否允许对运行 iOS 9.2 及更高版本的设备使用 Apple 投递邮件。默认值为关。
  - 启用 **S/MIME** 签名：选择此帐户是否支持 S/MIME 签名。默认值为开。设置为开时，将显示以下两个字段。
    - 签署身份凭据：选择要使用的签名凭据。
    - **S/MIME** 签名用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 签名。默认值为关。此选项适用于 iOS 12.0 及更高版本。
    - **S/MIME** 签名证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中选择要使用的签名凭据。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - 启用 **S/MIME** 加密：选择此帐户是否支持 S/MIME 加密。默认值为关。设置为开时，将显示以下两个字段。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 加密身份凭据：选择要使用的加密凭据。
    * 启用 **“为消息单独设置 S/MIME”** 开关：设置为开时，向用户显示一个选项，用于为其撰写的每条消息打开或关闭 S/MIME 加密。默认值为关。
    * 默认 **S/MIME** 加密用户可替代：如果设置为 **“开”**，用户可以在其设备的设置中选择 **S/MIME** 是否默认处于打开状态。默认值为关。此选项适用于 iOS 12.0 及更高版本。
    * **S/MIME** 加密证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 加密身份和加密。默认值为关。此选项适用于 iOS 12.0 及更高版本。
- 策略设置
  - 删除策略：要稍后删除策略，请将此设置配置为在选择日期或删除前的持续时间 **(**小时**)** 后删除策略。
  - 允许用户删除策略：允许用户始终删除邮件策略，仅使用需要通行码或从不删除。仅适用于 macOS。
  - 配置文件作用域：仅适用于 macOS，选择策略是适用于每个用户级别还是适用于整个系统。

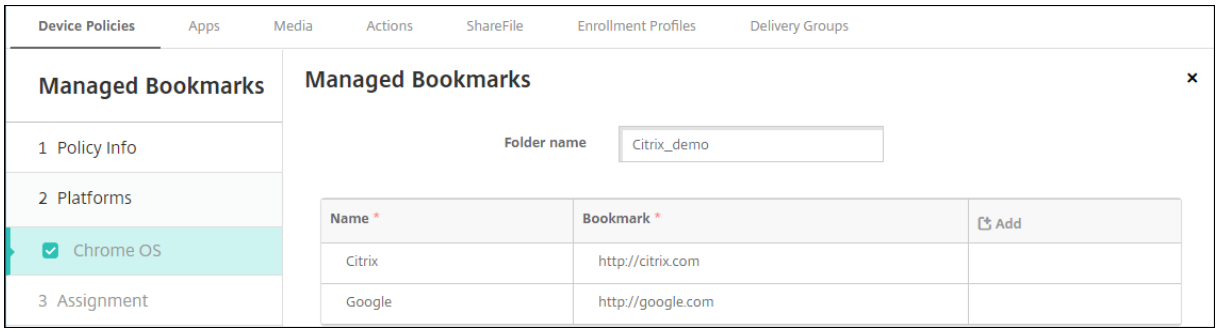
托管书签设备策略

March 31, 2022

使用托管书签设备策略，您可以将书签文件夹部署到 Chrome OS 设备。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Chrome OS 设置



- 文件夹名称：部署到 Chrome OS 设备的书签文件夹的名称。
- 名称：书签的名称。
- 书签：书签的 URL。

托管配置策略

April 11, 2023

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

“托管配置”设备策略控制各种应用程序配置选项和应用程序限制。可以为要控制的每个 Android Enterprise 应用程序创建此策略。

应用程序开发人员定义了可用于应用程序的选项和工具提示。如果工具提示提到使用“模板化值”，请改用相应的 Endpoint Management 宏。有关详细信息，请参阅远程配置概述（在 Android 开发人员站点上）和宏。

应用程序配置设置可以包含以下项目：

- 电子邮件应用程序设置
- 允许或阻止 Web 浏览器的 URL
- 通过手机网络连接或仅通过 Wi-Fi 连接控制应用程序内容同步的选项

有关为您的应用程序显示的设置的信息，请联系应用程序开发人员。

必备条件

- 在 Google 上完成 Android Enterprise 设置任务，并将 Android Enterprise 连接到托管 Google Play。有关详细信息，请参阅 Android Enterprise。
- 将 Android Enterprise 应用程序添加到 Endpoint Management。有关详细信息，请参阅将应用程序添加到 Endpoint Management。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

PerApp VPN 的要求

要为 AE 创建 PerApp VPN，则除了配置“托管配置”设备策略外，您还需要执行额外的步骤。此外，必须验证是否满足以下必备条件：

- 本地 Citrix Gateway
- 设备上安装了以下应用程序：
  - Citrix SSO
  - Citrix Secure Hub

为 AE 设备配置 PerApp VPN 的一般工作流程如下：

1. 按本文中所述配置 VPN 配置文件。
2. 将 Citrix ADC 配置为接受来自 PerApp VPN 的流量。有关详细信息，请参阅 Citrix Gateway 上的完整 VPN 设置。

限制

由于 Android 11 中引入了 包可见性限制，以下限制适用于使用 Android Enterprise 的 Android 11+ 设备上的每个 VPN：

- 如果在 VPN 会话启动后将允许/拒绝列表上的应用程序部署到设备上，则用户必须重新启动 VPN 会话。然后，该应用程序可以通过 VPN 会话路由流量。

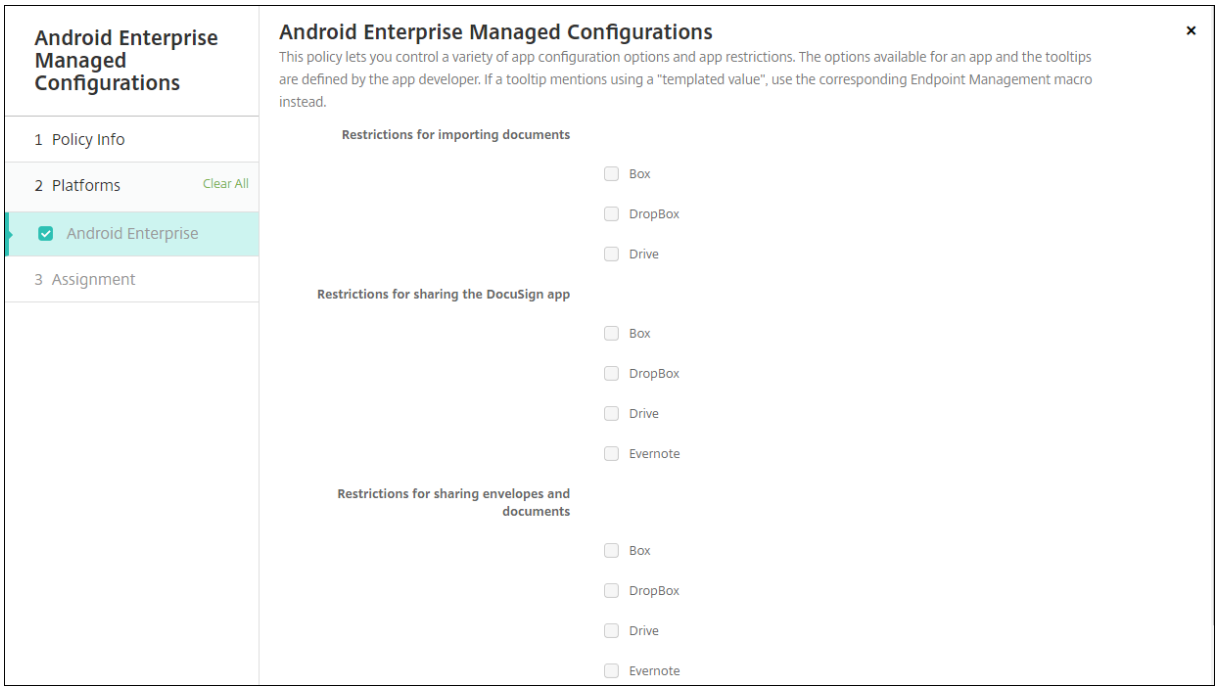
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 如果每个应用程序 VPN 与 AlwaysOn VPN 会话一起使用：在设备上安装新应用程序后，用户必须重新启动其工作配置文件或重新启动设备。然后，该应用程序可以通过 VPN 会话路由流量。

Android Enterprise 设置

选择添加“托管配置”设备策略后，系统将提示选择应用程序。如果没有要添加到 Endpoint Management 中的 Android Enterprise 应用程序，将无法继续操作。

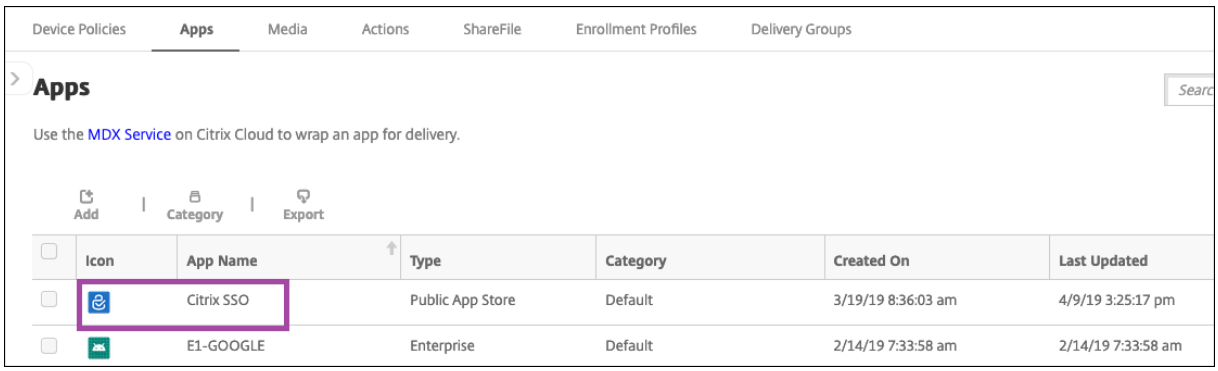
选择应用程序后，配置策略设置。这些设置与每个应用程序特定相关。



为 Android Enterprise 配置 VPN 配置文件

使用配置了“托管配置”设备策略的 Citrix SSO 应用程序，使 VPN 配置文件可供 Android Enterprise 设备使用。

首先将 Citrix SSO 作为 Google Play 应用商店应用程序添加到 Endpoint Management 控制台中。请参阅添加公共应用商店应用程序。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

观看此视频以了解更多：



为 **Citrix SSO** 创建 **Android Enterprise** 托管配置

为 Citrix SSO 配置“托管配置”设备策略以创建 VPN 配置文件。安装了 Citrix SSO 应用程序并部署了策略的设备可以访问您创建的 VPN 配置文件。

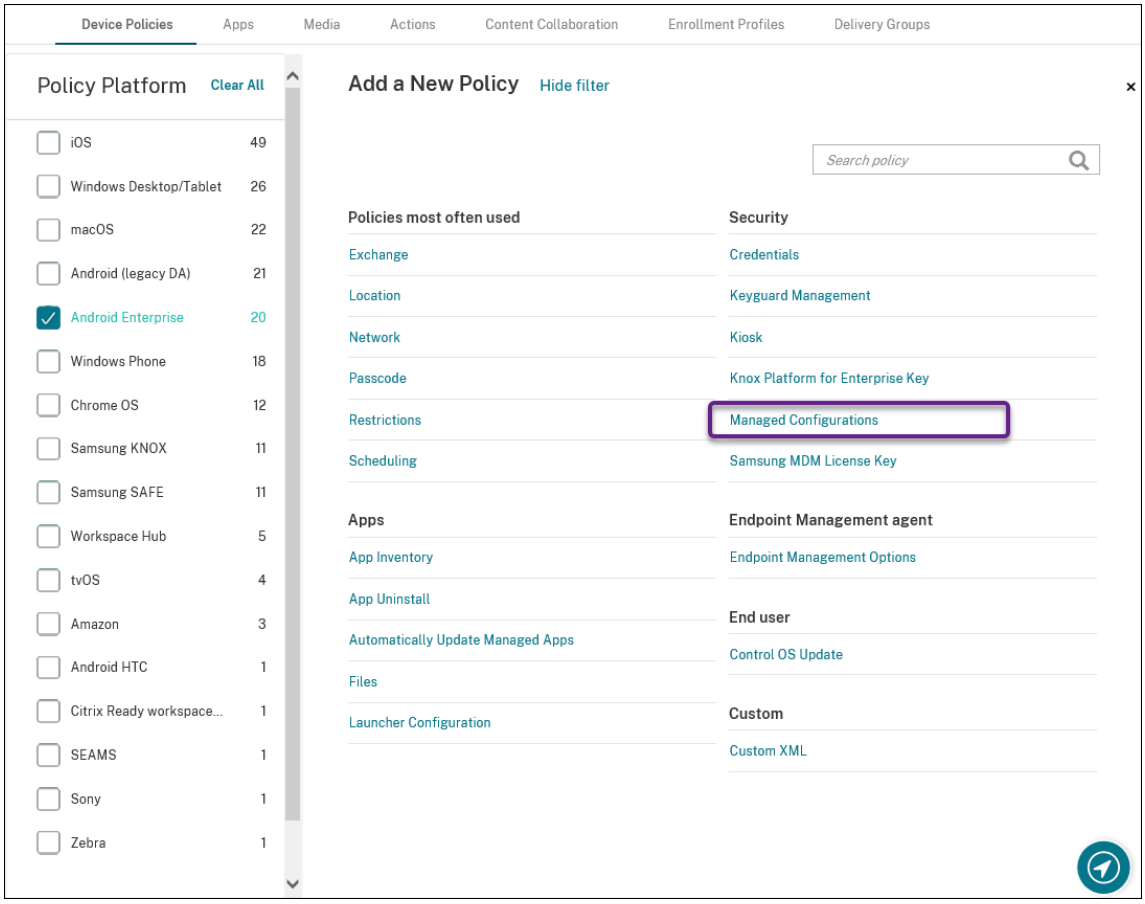
在以下情况下，Endpoint Management 将使用设备密钥库中的用户证书：

- Citrix Gateway 配置为进行基于证书的身份验证。
- 在 Endpoint Management 页面 **Settings**（设置）**> Citrix Gateway** 中启用了 **Deliver user certificate for authentication**（交付用于身份验证的用户证书）。

您需要您的 Citrix Gateway FQDN 和端口。

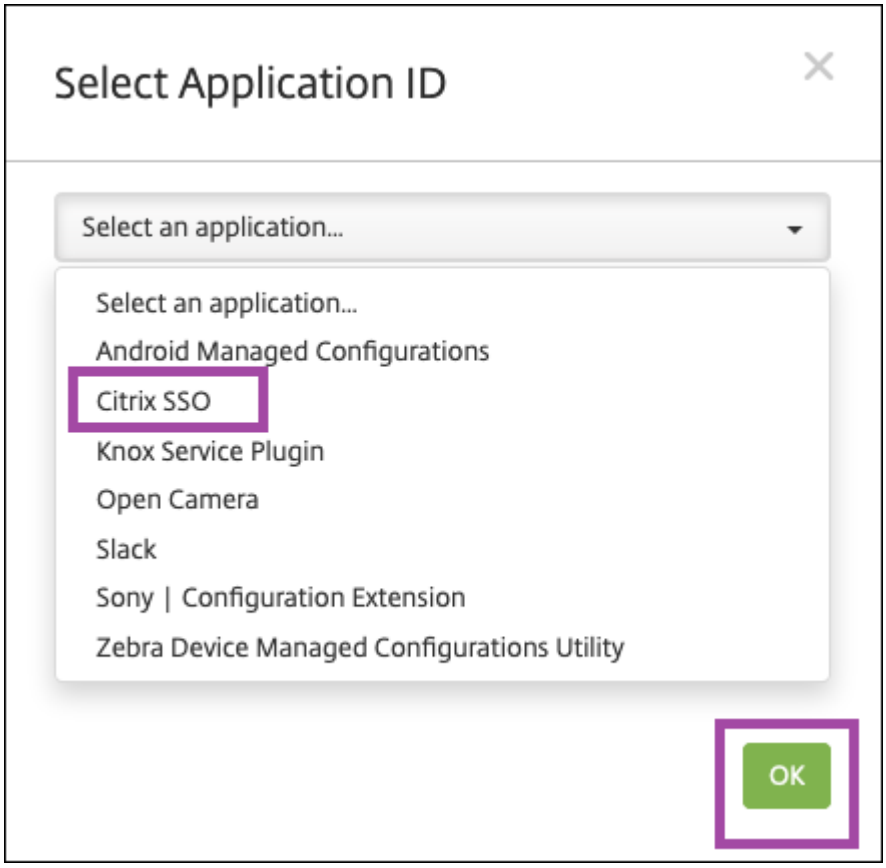
1. 在 Endpoint Management 控制台中，单击配置 **>** 设备策略。单击添加。
2. 选择 **Android Enterprise**。单击托管配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

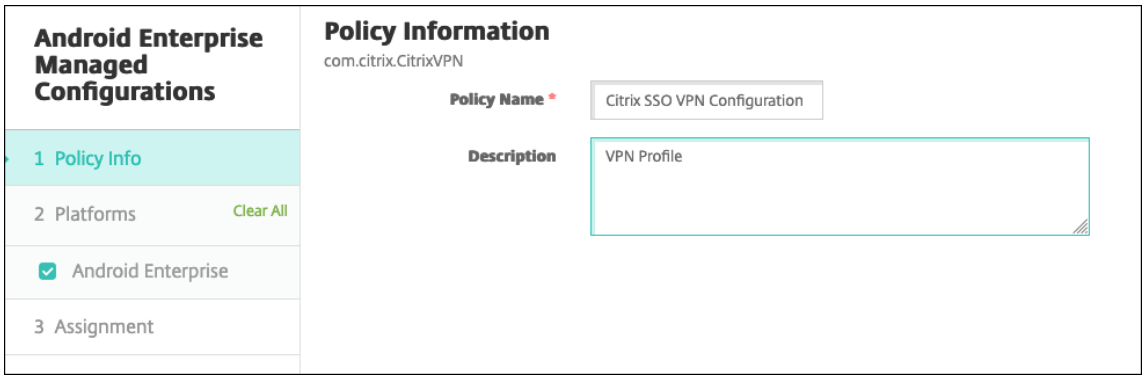


3. 显示选择应用程序 **ID** 窗口时，从列表中选择 **Citrix SSO**，然后单击确定。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 键入 Citrix SSO VPN 配置的名称和说明。单击下一步。



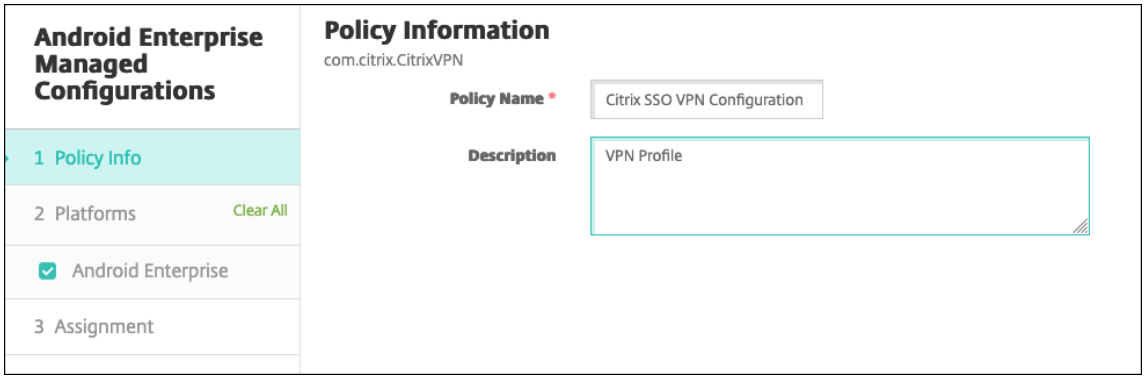
5. 配置 VPN 配置文件参数。

   - **VPN** 配置文件名称：键入 VPN 配置文件的名称。如果要创建多个 VPN 配置文件，请为每个配置文件使用唯一的名称。如果不提供名称，则会将您在服务器地址字段中放置的地址用作 VPN 配置文件名称。
   - 服务器地址 **(*)**：键入您的 Citrix Gateway FQDN。如果 Citrix Gateway 端口不是 443，请键入您的端口。使用 URL 格式。例如，`https://gateway.mycompany.com:8443`。
   - 用户名 **(**可选**)**：提供最终用户用于对 Citrix Gateway 进行身份验证的用户名。可以将 Endpoint Management 宏 {user.username} 用于此字段。（请参阅宏。）如果不提供用户名，系统会在连接到 Citrix Gateway 时提示用户提供用户名。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 密码 **(**可选**)**：提供最终用户用于对 Citrix Gateway 进行身份验证的密码。如果不提供密码，系统会在连接到 Citrix Gateway 时提示用户提供密码。
- 证书别名 **(**可选**)**：键入证书别名。证书别名使应用程序能够更轻松地访问证书。在凭据设备策略中使用相同的证书别名时，应用程序将检索证书并对 VPN 进行身份验证，而无需用户执行任何操作。
- **PerApp VPN** 类型 **(**可选**)**：如果您使用 PerApp VPN 来限制哪些应用程序使用此 VPN，则可以配置此设置。如果选择允许，**PerAppVPN** 应用程序列表中列出的应用程序包名称的网络流量将通过 VPN 路由。所有其他应用程序的网络流量都会在 VPN 外部进行路由。如果选择不允许，**PerAppVPN** 应用程序列表中列出的应用程序包名称的网络流量将在 VPN 外部路由。所有其他应用程序的网络流量都通过 VPN 路由。默认设置为允许。
- **PerApp VPN** 应用程序列表： VPN 上允许或阻止其流量的应用程序列表，具体取决于 **PerApp VPN** 类型的值。列出以逗号或分号分隔的应用程序包的名称。应用程序包名称区分大小写，并且必须以与 Google Play 应用商店中完全一致的显示方式显示在此列表中。此列表是可选的。将此列表保留为空，以便预配设备范围的 VPN。
- 默认 **VPN** 配置文件：键入 VPN 配置文件的名称，以便用户在 Citrix SSO 应用程序中轻按连接开关（而非特定配置文件）时使用。如果此字段留空，则主配置文件将用于连接。如果只配置了一个配置文件，则将其标记为默认配置文件。对于始终可用的 VPN，必须将此字段设置为用于建立始终可用的 VPN 的 VPN 配置文件名称。
- 禁用用户配置文件：如果此设置设为 “开”，用户将无法在其设备上创建自己的 VPN。如果此设置设为 “关”，用户可以在其设备上创建自己的 VPN。默认设置为关。
- 阻止不受信任的服务器：此设置在以下情况下设置为 “关”：
  - 为 Citrix Gateway 使用自签名证书时
  - 颁发 Citrix Gateway 证书的 CA 的根证书不在系统 CA 列表中时。

  如果此设置设为 “开”，Android 操作系统将验证 Citrix Gateway 证书。如果验证失败，则不允许连接。默认值为开。



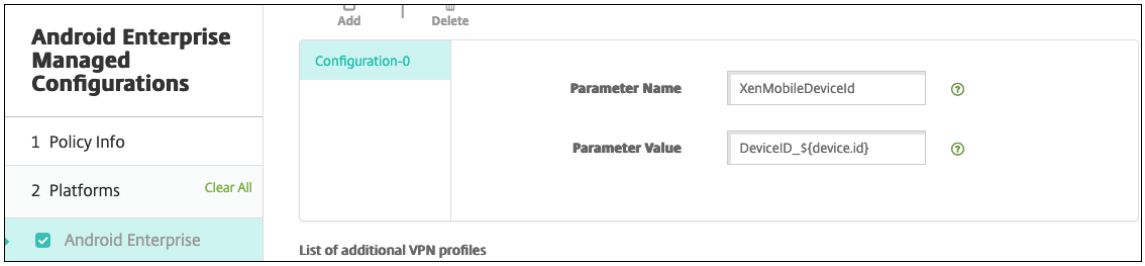
6. 也可以创建自定义参数。支持自定义参数 **XenMobileDeviceId** 和 **UserAgent**。选择当前 VPN 配置，然后单击添加。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



a) 创建自定义参数：

- 参数名称：键入 **XenMobileDeviceId**。此字段是用于根据 Endpoint Management 中的设备注册进行网络访问检查的设备 ID。如果 Endpoint Management 注册并管理设备，则允许建立 VPN 连接。否则，在 VPN 建立时将拒绝身份验证。
- 参数值 Endpoint Management 用于确定设备的注册和管理状态，XenMobileDeviceID 的值设置为 `DeviceID_${ device.id }`。

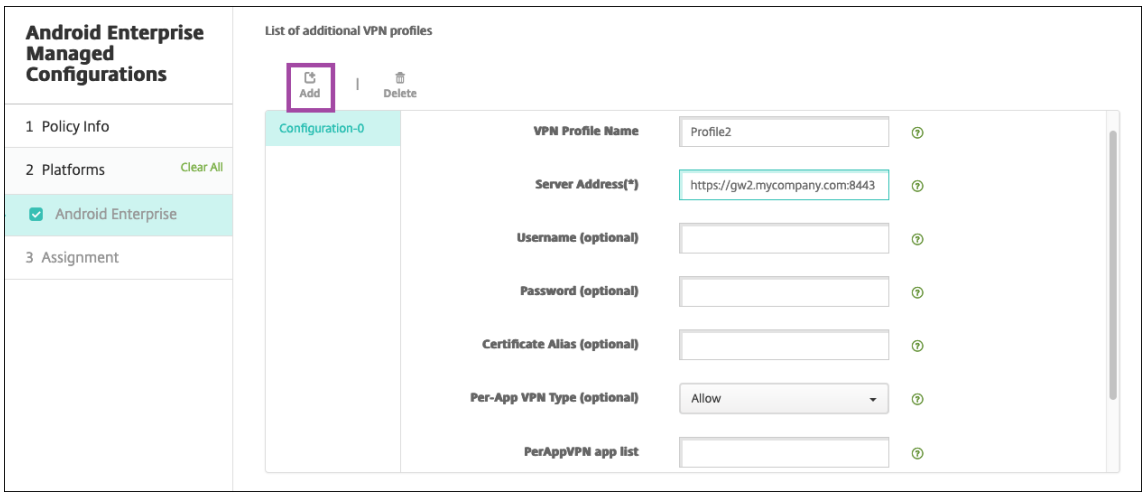


a) 要创建另一个自定义参数，请再次单击添加。创建此自定义参数。

- 参数名称：键入 **UserAgent**。此文本附加到用户代理 HTTP 标头，用于在 Citrix Gateway 上执行额外的检查。与 Citrix Gateway 通信时，Citrix SSO 应用程序将此文本的值附加到用户代理 HTTP 标头。
- 参数值：键入要附加到用户代理 HTTP 标头的文本。此文本必须符合 HTTP 用户代理规范。

7. 或者，创建更多 VPN 配置文件配置。单击配置列表下的添加。列表中将显示一个新配置。选择新配置并重复步骤 5 以及（可选）步骤 6。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



8. 创建所有所需 VPN 配置文件后，单击下一步。
9. 为 Citrix SSO 的此托管配置配置部署规则。
10. 单击保存。

Citrix SSO 的此托管配置现在显示在已配置的设备策略列表中。

要为您配置的 VPN 配置文件启用始终启用功能，请设置 Endpoint Management 选项设备策略。

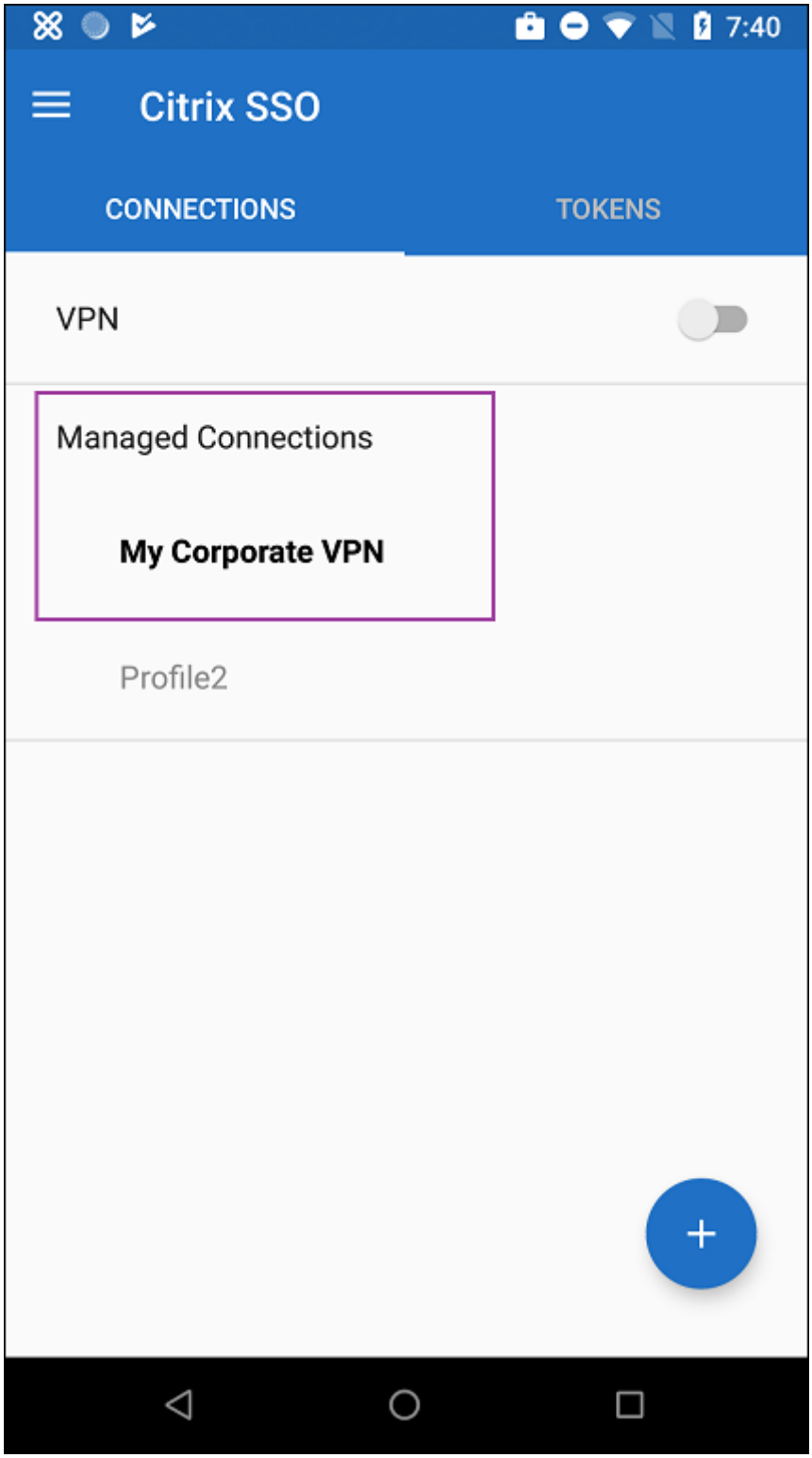
> 注意：
>
> 适用于 Android Enterprise 的始终可用的 VPN 需要 Citrix Secure Hub 19.5.5 或更高版本。

从设备访问 **VPN** 配置文件

要访问您创建的 VPN 配置文件，Android Enterprise 用户将从 Google Play 应用商店安装 Citrix SSO。

您配置的一个或多个 VPN 配置文件将显示在应用程序的托管连接区域中。用户轻按 VPN 配置文件将使用该 VPN 配置文件进行连接。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



用户进行身份验证并连接后，VPN 配置文件旁边会显示一个复选标记。键图标指示 VPN 已连接。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使用 **Zebra OEMConfig** 管理 **Zebra Android** 设备

使用 Zebra Technologies OEMConfig 管理工具管理 Zebra Android 设备。有关 Zebra OEMConfig 应用程序的信息，请参阅 Zebra Technologies Web 站点。

Endpoint Management 支持 Zebra OEMConfig 9.2 及更高版本。有关在设备上安装 Zebra OEMConfig 的系统要求的信息，请参阅 Zebra Technologies Web 站点上的 OEMConfig 设置。

我们当前支持以下 Zebra 设备：

- EC50, EC55, ET56
- TC52x, TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

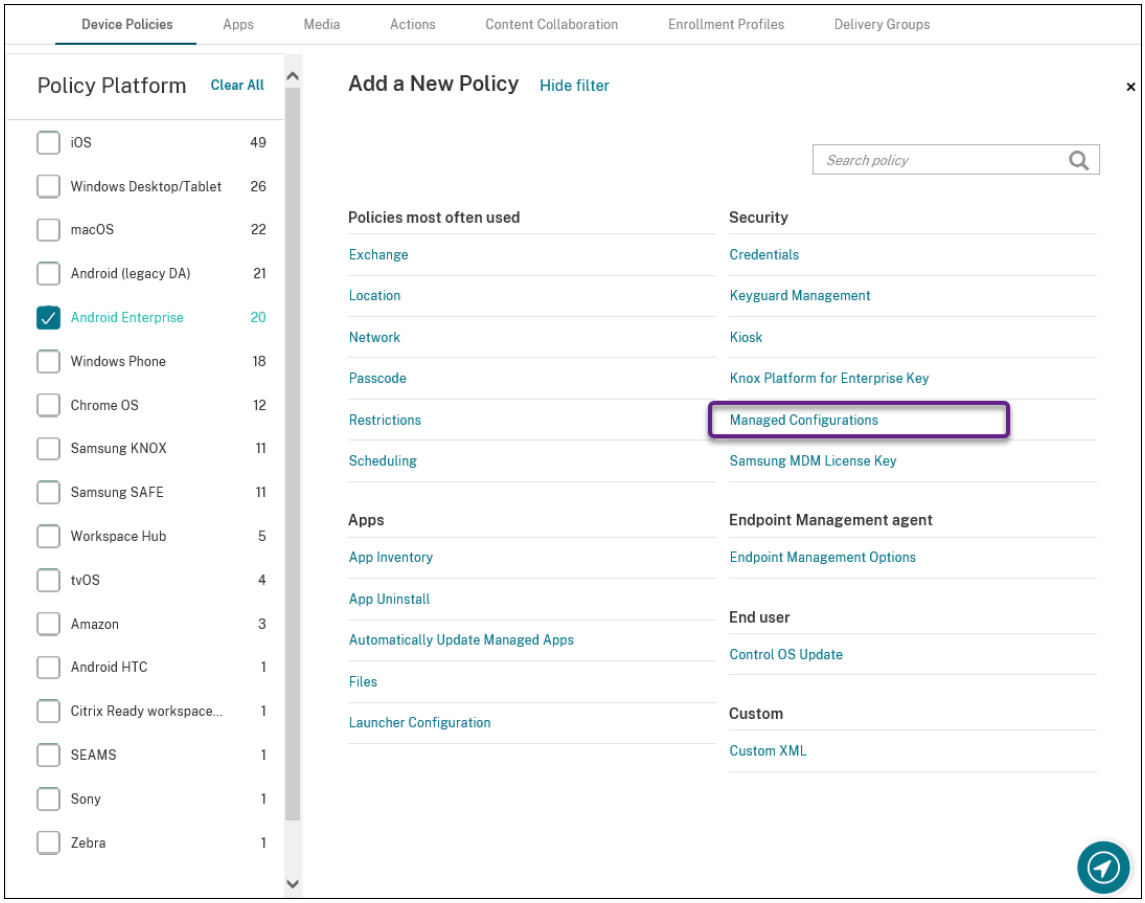
首先，在 Endpoint Management 控制台中，将 Zebra OEMConfig 应用程序添加为 Google Play 应用商店应用程序。请参阅添加公共应用商店应用程序。

为 **Zebra OEMConfig** 应用程序创建 **Android Enterprise** 托管配置

为 Zebra OEMConfig 应用程序配置“托管配置”设备策略。该策略适用于安装了 Zebra OEMConfig 应用程序并部署了该策略的 Zebra 设备。

1. 在 Endpoint Management 控制台中，单击配置 **>** 设备策略。单击添加。
2. 选择 **Android Enterprise**。单击托管配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 显示选择应用程序 **ID** 窗口时，从列表中选择 **ZebraOEMConfig powered by MX**（ZebraOEMConfig，由 MX 提供技术支持），然后单击确定。
4. 键入 Zebra OEMConfig 配置的名称和说明。单击下一步。
5. 键入 Zebra OEMConfig 配置的名称。
6. 配置可用参数。例如：
   - 要禁用设备前面的摄像头，请选择 **Camera Configuration**（摄像头配置）并将 **Use of Front Camera**（使用前置摄像头）设置为 **Off**（关）。
   - 要更改设备时间格式，请选择 **Clock Configuration**（时钟配置），然后将 **Time Format**（时间格式）设置为 **12**（12 小时制）或 **24**（24 小时制）。

有关所有可用配置的列表和说明，请参阅 Zebra Technologies Web 站点上的 Zebra 托管配置。

1. 或者，创建更多 Zebra OEMConfig 配置。单击配置列表下的添加。列表中将显示一个新配置。选择新配置并配置参数。
2. 创建需要的所有 Zebra OEMConfig 配置后，请单击 **Next**（下一步）。
3. 为 Zebra OEMConfig 的这一托管配置配置部署规则。
4. 单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

托管域设备策略

March 31, 2022

可以定义应用到电子邮件和 Safari 浏览器的托管域。托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护公司数据。

对于受 iOS 监督的设备，您可以指定：

- URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。
- 用户可以在 Safari 浏览器中保存密码的 URL。

有关将 iOS 设备设置为受监督模式的步骤，请参阅使用 Apple Configurator 2 部署设备。

用户向域不在托管电子邮件域列表上的收件人发送电子邮件时，在用户的设备上此邮件将带有标记，以警告用户正在向企业域外部的人员发送邮件。

对于文档、附件或下载内容等项目：当用户使用 Safari 从位于托管 Web 域列表上的 Web 域打开某个项目（文档、附件或下载内容）时，将由合适的企业应用程序打开此项目。如果此项目所在的 Web 域不在托管 Web 域列表上，用户无法使用合适的企业应用程序打开此项目。必须使用未托管的个人应用程序打开。

对于受监督的设备，即使您未指定 Safari 密码自动填充域：如果设备配置为暂时多用户，用户将无法保存密码。但是，如果设备未配置为暂时多用户，用户可以保存所有密码。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

指定域：

格式	说明
`example.com`	将 `example.com` 下面的所有路径视为已托管，但 `site.example.com/` 除外。
`foo.example.com`	将 `foo.example.com` 下面的所有路径视为已托管，但 `example.com/` 和 `bar.example.com/` 除外。
`\*.example.com`	将 `foo.example.com` 或 `bar.example.com` 下面的所有路径视为已托管，但 `example.com/` 除外。
`example.com/sub`	将 `example.com/sub` 及其下面的所有路径视为已托管，但 `example.com/` 除外。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

格式	说明
foo.example.com/sub	将 foo.example.com/sub 下面的所有路径视为已托管，但 example.com、example.com/sub、foo.example.com/ 和 bar.example.com/sub 除外。
*.example.com/sub	将 foo.example.com/sub 或 bar.example.com/sub 下面的所有路径视为已托管，但 example.com 和 foo.example.com/ 除外。

规则：

- 比较域时，会忽略 URL 中的前导 “www.” 和尾部斜线。
- 如果条目包含端口号，只有指定此端口号的地址才被视为托管。否则，仅将标准端口视为托管（http 为端口 80，https 为端口 443）。例如，模式 `*.example.com:8080` 匹配 `https://site.example.com:8080/page.html`，但不匹配 `https://site.example.com/page.html`，而模式 `*.example.com` 匹配 `https://site.example.com/page.html` 和 `https://site.example.com/page.html`，但不匹配 `https://site.example.com:8080/page.html`。
- 托管 Safari Web 域定义具有累计性。所有托管 Safari Web 域负载定义的模式用于匹配 URL 请求。

设置：

- 托管域
  - 取消标记电子邮件域：对于要包含在列表中的每个电子邮件域，单击添加，然后执行以下操作：
    - 托管电子邮件域：键入电子邮件域。
    - 单击保存以保存电子邮件域，或单击取消不保存电子邮件域。
  - 托管 **Safari Web** 域：对于要包含在列表中的每个 Web 域，单击添加，然后执行以下操作：
    - 托管 **Web** 域：键入 Web 域。
    - 单击保存以保存 Web 域，或单击取消不保存 Web 域。
  - **Safari** 密码自动填充域：对于要包含在列表中的每个自动填充域，单击添加，然后执行以下操作：
    - **Safari** 密码自动填充域：键入自动填充域。
    - 单击保存以保存自动填充域，或单击取消不保存自动填充域。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

最大常驻用户数设备策略

March 31, 2022

“最大常驻用户数”设备策略适用于运行 iOS (iPadOS) 的共享设备。有关共用的 iPad 的详细信息，请参阅与 Apple 教育功能相集成。

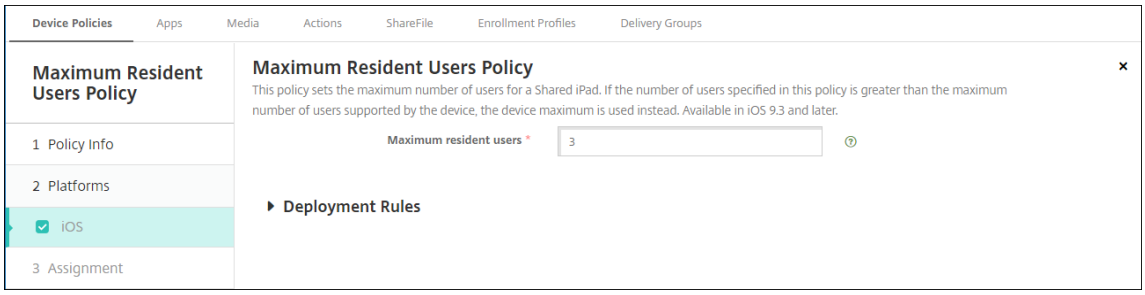
iPad 在设置助理期间处于“等待配置”阶段时，必须部署此策略。Apple 不允许在共用的 iPad 注册后部署此策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 最大常驻用户数：共用的 iPad 的最大用户数。如果在此策略中指定的用户数大于设备支持的最大用户数：Endpoint Management 将改为使用最大设备数。默认值为 **5** 个用户。

  Apple 建议您将“最大常驻用户数”值保持为尽可能低的值。低值会将每个用户的 iPad 存储量最大化。此外，低值还会将与 iCloud 的通信降至最低，并提供更快的登录体验。有关 Apple 如何在 iPad 上处理共享存储的信息，请参阅 https://developer.apple.com/education/shared-ipad/。



MDM 选项设备策略

March 31, 2022

MDM 选项设备策略管理受监督的 iOS 设备上的“查找我的 iPhone/iPad 激活锁”。有关将 iOS 设备设置为受监督模式的步骤，请参阅使用 Apple Configurator 2 部署设备。

激活锁是一项“查找我的 iPhone/iPad”功能，用于阻止重新激活丢失或被盗的受监督设备。激活锁需要用户的 Apple ID 和密码，之后用户才能关闭“查找我的 iPhone/iPad”、擦除设备或重新激活设备。对于组织拥有的设备，绕过激活锁是（例如）重置或重新分配设备的必要操作。

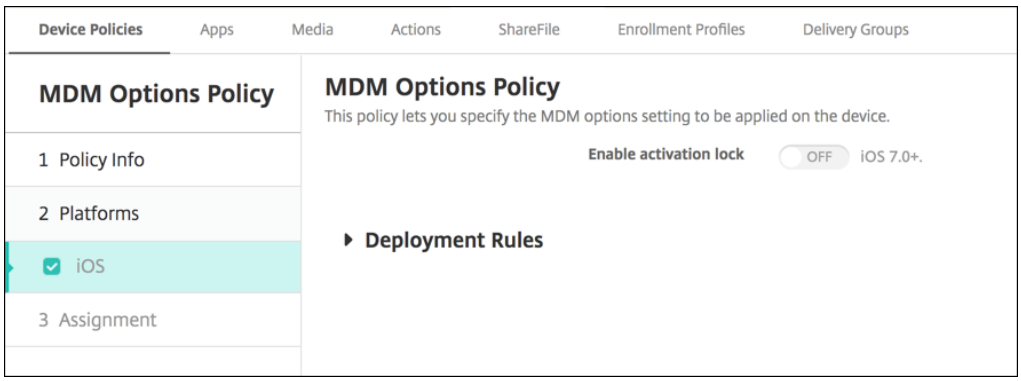
要启用激活锁，请配置并部署 Endpoint Management MDM 选项设备策略。之后可以从 Endpoint Management 控制台管理设备，而不需要用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 Endpoint Management 控制台发出“激活锁绕过”安全操作。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

例如，如果用户在执行完全擦除操作之前或之后归还了丢失的手机或设置了设备：手机提示输入 Apple App Store 帐户凭据时，可以通过从 Endpoint Management 控制台发出“激活锁绕过”安全操作来绕过该设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- 启用激活锁：选择是否要在部署此策略的设备上启用激活锁。默认值为关。

通过部署 MDM 选项设备策略启用激活锁后：当您在管理 **>** 设备页面上选择这些设备并单击安全时，将显示安全操作激活锁绕过。通过“激活锁绕过”，可以在设备激活之前从受监督的设备中删除激活锁，而不需要知晓设备用户的 Apple ID 和密码。可以在执行完全擦除操作之前或之后向设备发送“激活锁绕过”安全操作。有关详细信息，请参阅绕过 iOS 激活锁。

网络设备策略

July 24, 2023

网络设备策略允许您通过定义以下项目来管理用户如何将设备连接到 Wi-Fi 网络：

- 网络名称和类型
- 身份验证和安全策略
- 代理服务器使用
- 其他 Wi-Fi 相关详细信息

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

必备条件

在创建策略之前，请完成以下操作：

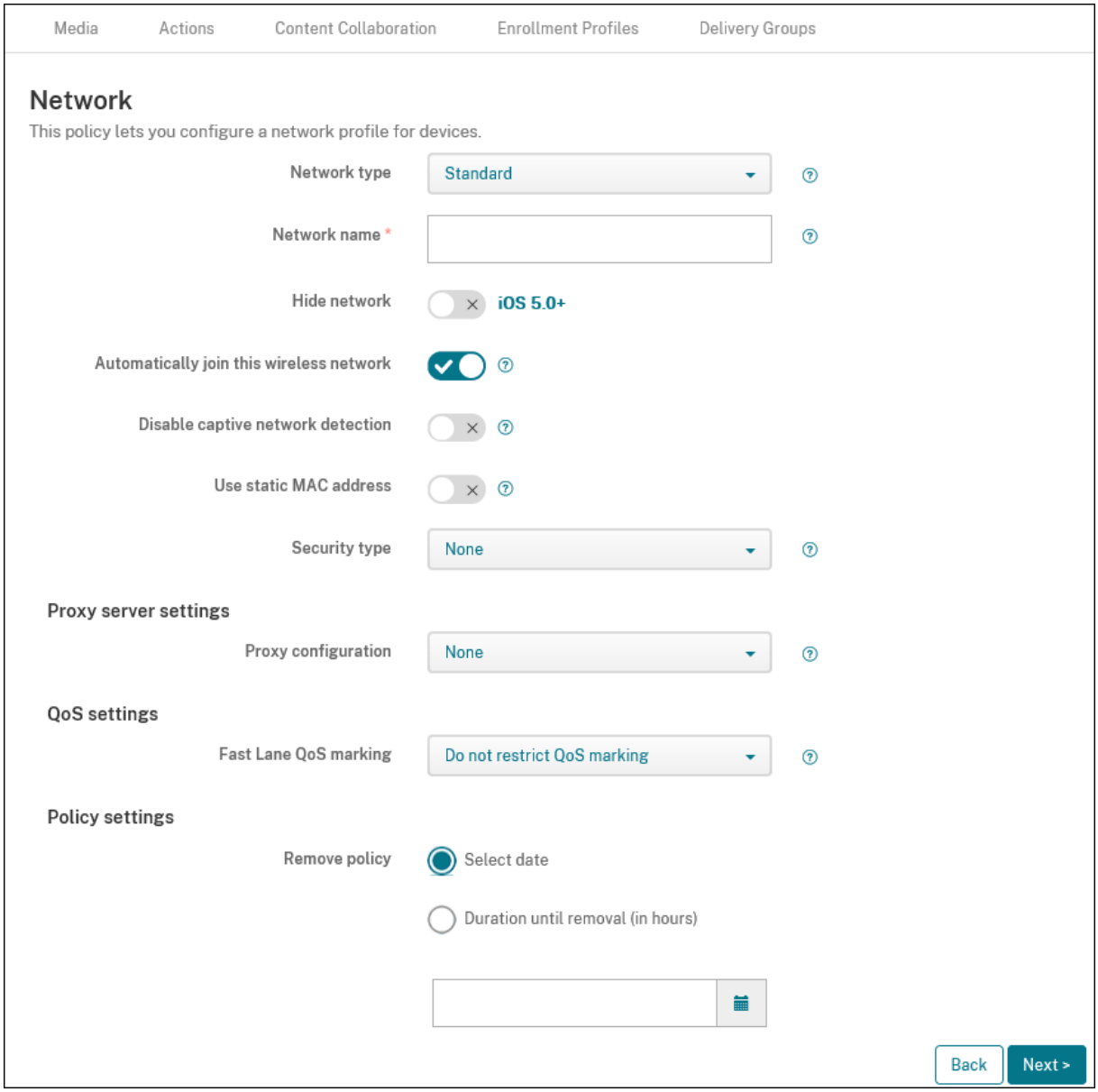
- 创建计划使用的任何交付组。
- 了解网络名称和类型。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 了解计划使用的任何身份验证或安全类型。
- 了解可能需要的任何代理服务器信息。
- 安装所有必需的 CA 证书。
- 具有所有必需共享密钥。
- 为基于证书的身份验证创建 PKI 实体。
- 配置凭据提供程序。

有关更多信息，请参阅 身份验证 及其子文章。

iOS 和 tvOS 设置



- 网络类型：在列表中，选择标准、传统热点或 **Hotspot 2.0** 以设置您计划使用的网络类型。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 网络名称：键入显示在设备的可用网络列表中的 SSID。不适用于 **Hotspot 2.0**。
- 隐藏网络：选择是否隐藏网络。
- 自动加入此无线网络：选择设备是否自动加入网络。如果设备连接到另一个网络，则它不会加入此网络。在设备自动连接之前，用户必须断开与以前的网络的连接。默认值为开。
- 禁用俘获型网络检测：专用网络助手可帮助用户访问订阅网络或 Wi-Fi 热点网络。您通常会在咖啡馆、酒店和其他公共场所找到这些网络。如果设置为开，设备仍可以连接到俘获型网络，但用户必须打开浏览器并手动登录。默认值为关。
- 使用静态 **MAC** 地址： MAC 地址是设备在网络中传输的唯一标识符。为了提高隐私性，iOS 和 iPadOS 设备每次连接到网络时都可以使用不同的 MAC 地址。如果设置为开，设备在连接到此网络时将始终使用相同的 MAC 地址。如果设置为关，设备每次连接到此网络时都将使用不同的 MAC 地址。默认值为关。
- 安全类型：在列表中，选择您计划使用的安全类型。不适用于 **Hotspot 2.0**。
  - 无 - 无需进一步配置。
  - WEP
  - WPA/WPA2/WPA3 Personal
  - 任何 (Personal)
  - WEP Enterprise
  - WPA/WPA2/WPA3 企业版：对于 Windows 10 的最新版本，请将简单证书注册协议 (SCEP) 配置为使用 WPA-2 企业版。然后，Endpoint Management 可以将证书发送到设备以向 Wi-Fi 服务器进行身份验证。要配置 SCEP，请转到设置 **>** 凭据提供程序的“分发”页面。有关更多信息，请参阅 凭证提供程序。
  - 任何 (Enterprise)

  以下各节列出了要为上述各个连接类型配置的选项。
- 代理服务器设置
  - 代理配置：在列表中，选择无、手动或自动以设置 VPN 连接通过代理服务器路由的方式，然后配置任何其他选项。默认值为无，表示无需进一步配置。
  - 如果选择手动，请配置以下设置：
    - 主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。
    - 端口：键入代理服务器端口号。
    - 用户名：键入向代理服务器进行身份验证的可选用户名。
    - 密码：键入向代理服务器进行身份验证的可选密码。
  - 如果选择自动，请配置以下设置：
    - 服务器 **URL**：键入用于定义代理配置的 PAC 文件的 URL。
    - 允许在无法访问 **PAC** 时直接连接：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。默认值为开。
- 快车道 **QoS** 标记：如果不限制支持 Cisco 快车道 QoS 的 Wi-Fi 网络的 QoS 标记，则将允许所有应用程序使用 L2 和 L3 标记。如果限制 QoS 标记，请指定能够使用 L2 和 L3 标记的应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 启用 **QoS** 标记：如果限制 QoS 标记，请使用此设置完全将其禁用或仅标记某些应用程序。如果设置为关，则完全禁用 QoS 标记。如果设置为开，请配置可以使用 QoS 标记的应用程序列表。默认值为开。
  - 允许 **Apple** 音频/视频通话：选择音频和视频通话应用程序是否可以使用 QoS 标记。如果设置为关，视频和音频通话的质量可能会受到影响。
  - 允许特定应用程序：将应用程序软件包 ID 添加到此列表中，以允许应用程序使用 QoS 标记。

- **Hotspot 2.0** 设置
  - 显示的运算符名称： Hotspot 设备广播的友好名称。用户会在其可用 Wi-Fi 网络列表中看到此名称。
  - 域名：用于 Hotspot 2.0 协商的域名。
  - 允许连接漫游伙伴网络：如果设置为开，从其家用网络漫游的设备可以连接到合作伙伴网络。
  - 漫游联盟组织标识符 **(OI)**：添加设备可以访问的组织标识符列表。漫游联盟 OI 属于使用共享身份验证方法的组织。如果您配置的热点不可用，设备将连接到此处列出的漫游联盟 OI。
  - 网络访问标识符 **(NAI)** 领域名称：配置用于识别连接到漫游网络的用户的领域名称列表。NAI 以 `user@realm` 形式传输。
  - 移动设备国家/地区代码 **(MCC)** 和移动设备网络配置 **(MNC)**：移动设备国家/地区代码由三位数字组成，用于标识网络所属的国家/地区。移动网络代码由 2 个或 3 个唯一数字组成。一起使用时，MCC/MNC 唯一标识移动网络运营商。

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。不适用于 iOS。

适用于 **iOS** 的 **“WPA”**、**“WPA Personal”**、“任何 **(Personal)”** 设置

密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。

适用于 **iOS** 的 **“WEP Enterprise”**、**“WPA Enterprise”**、**“WPA2 Enterprise”**、**“WPA3 Enterprise”**、**“**任何 **(Enterprise)”** 设置

选择这些安全类型中的任何一种时，EAP 设置将显示在 **QoS** 设置之后。

> 重要提示：
>
> 如果选择 **WPA2 Enterprise** 安全类型，则必须至少允许一个 EAP 协议。

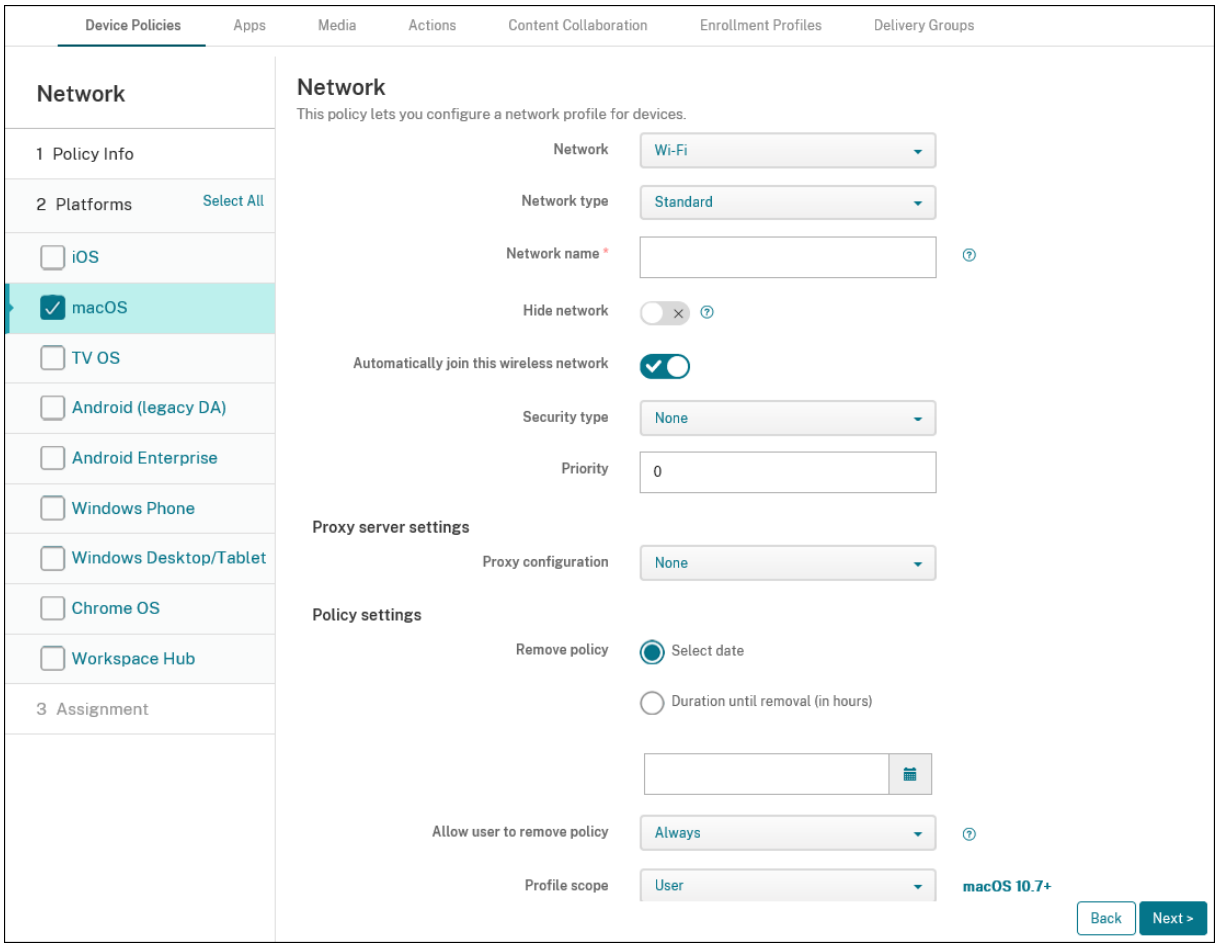
- 允许使用的 **EAP** 协议：启用要支持的 EAP 类型，然后配置相关设置。每个可用 EAP 类型的默认值为关。
- 内部身份验证 **(TTLS)**：仅在启用 *TTLS* 时需要。在列表中，选择要使用的内部身份验证方法。选项包括：**PAP**、**CHAP**、**MSCHAP** 或 **MSCHAPv2**。默认值为 **MSCHAPv2**。
- 使用 **PAC** 的 **EAP-FAST**：选择是否使用受保护的访问凭据 (PAC)。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 如果选择使用 **PAC**，请选择是否要使用预配 PAC。
    - 如果选择预配 **PAC**，请选择是否允许在最终用户客户端与 Endpoint Management 之间建立匿名 TLS 握手。
      - 匿名预配 **PAC**
- 身份验证：
  - 用户名：键入用户名。
  - 为连接单独设置密码：选择用户是否在每次登录时都需要提供密码。
  - 密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。
  - 身份凭据 **(**密钥库或 **PKI** 凭据**)**：在列表中，选择身份凭据的类型。默认值为无。
  - 外部标识：仅在启用 **PEAP**、**TTLS** 或 **EAP-FAST** 时需要。键入外部可见的用户名。您可以通过键入 “anonymous” 等通用术语以使用户名不可见来增加安全性。
  - 需要 **TLS** 证书：选择是否需要 TLS 证书。
- 信任
  - 可信证书：要添加可信证书，请单击添加，然后，针对要添加的各个证书执行以下操作：
    - 应用程序：在列表中，单击要添加的应用程序。
    - 单击保存以保存证书，或者单击取消。
  - 可信服务器证书名称：要添加可信服务器证书公用名，请单击添加，然后针对要添加的名称执行以下操作：
    - 证书：键入服务器证书的名称。可以使用通配符指定名称，如 wpa.*.example.com。
    - 单击保存以保存证书名称，或者单击取消。
- 允许信任例外：选择当证书不可信时是否在用户设备上显示证书信任对话框。默认值为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

macOS 设置



- 网络：在列表中，选择您计划使用的网络选项。默认设置为 **Wi-Fi**。
  - Wi-Fi
  - 全球以太网
  - 第一个活动的以太网
  - 第二个活动的以太网
  - 第三个活动的以太网
  - 第一个以太网
  - 第二个以太网
  - 第三个以太网
- 网络类型：在列表中，选择标准、传统热点或 **Hotspot 2.0** 以设置您计划使用的网络类型。
- 网络名称：键入显示在设备的可用网络列表中的 SSID。不适用于 **Hotspot 2.0**。
- 隐藏网络：选择是否隐藏网络。
- 自动加入此无线网络：选择是否自动加入网络。如果设备已连接到另一个网络，则不会加入此网络。在设备自动连接之前，用户必须断开与以前的网络的连接。默认值为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 安全类型：在列表中，选择您计划使用的安全类型。不适用于 **Hotspot 2.0**。
  - 无 - 无需进一步配置。
  - WEP
  - WPA/WPA2 Personal
  - 任何 (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - 任何 (Enterprise)

  以下各节列出了要为上述各个连接类型配置的选项。
- 优先级：对于多个网络，请键入一个数字以定义网络连接的优先级。设备首先连接到优先级最低的网络。负数是可接受的。默认值为 **0**。
- 代理服务器设置
  - 代理配置：在列表中，选择无、手动或自动以设置 VPN 连接通过代理服务器路由的方式，然后配置任何其他选项。默认值为无，表示无需进一步配置。
  - 如果选择手动，请配置以下设置：
    * 主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。
    * 端口：键入代理服务器端口号。
    * 用户名：键入向代理服务器进行身份验证的可选用户名。
    * 密码：键入向代理服务器进行身份验证的可选密码。
  - 如果选择自动，请配置以下设置：
    * 服务器 **URL**：键入用于定义代理配置的 PAC 文件的 URL。
    * 允许在无法访问 **PAC** 时直接连接：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。默认值为开。
- **Hotspot 2.0** 设置
  - 显示的运算符名称： Hotspot 设备广播的友好名称。用户会在其可用 Wi-Fi 网络列表中看到此名称。
  - 域名：用于 Hotspot 2.0 协商的域名。
  - 允许连接漫游伙伴网络：如果设置为开，从其家用网络漫游的设备可以连接到合作伙伴网络。
  - 漫游联盟组织标识符 **(OI)**：添加设备可以访问的组织标识符列表。漫游联盟 OI 属于使用共享身份验证方法的组织。如果您配置的热点不可用，设备将连接到此处列出的漫游联盟 OI。
  - 网络访问标识符 **(NAI)** 领域名称：配置用于识别连接到漫游网络的用户的领域名称列表。NAI 以 `user@realm` 形式传输。
  - 移动设备国家/地区代码 **(MCC)** 和移动设备网络配置 **(MNC)**：移动设备国家/地区代码由三位数字组成，用于标识网络所属的国家/地区。移动网络代码由 2 个或 3 个唯一数字组成。一起使用时，MCC/MNC 唯一标识移动网络运营商。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 选择日期：单击日历可选择具体删除日期。
    * 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

适用于 **macOS** 的 **“WPA”**、**“WPA Personal”**、**“WPA 2 Personal”**、**“**任何 **(Personal)”** 设置

- 密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。

适用于 **macOS** 的 **“WEP Enterprise”**、**“WPA Enterprise”**、**“WPA2 Enterprise”**、**“**任何 **(Enterprise)”** 设置

- 连接模式：如果设置为开，则选择用户加入网络时要使用的连接模式。默认值为关。
  - 系统：如果已标记，则设备将使用系统凭据对用户进行身份验证。默认值已清除。
  - 登录窗口：如果已标记，设备将使用在登录窗口中输入的相同凭据对用户进行身份验证。默认值已清除。

选择这些安全类型中的任何一种时，EAP 设置将显示在 **QoS** 设置之后。

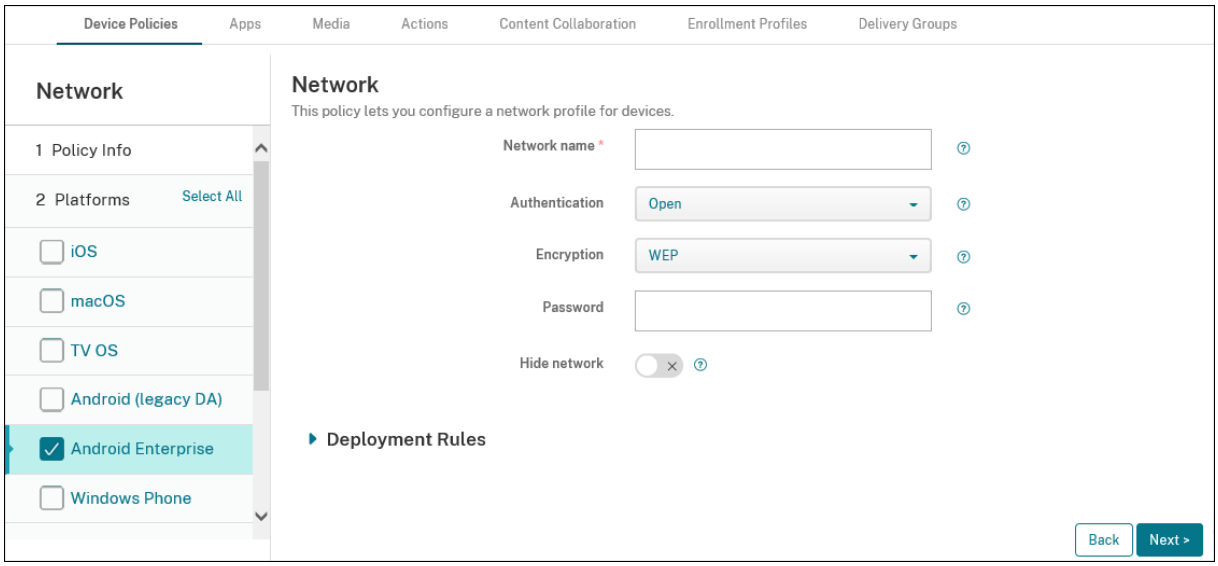
> 重要提示：
>
> 如果选择 **WPA2 Enterprise** 安全类型，则必须至少允许一个 EAP 协议。

- 允许使用的 **EAP** 协议：启用要支持的 EAP 类型，然后配置相关设置。每个可用 EAP 类型的默认值为关。
- 内部身份验证 **(TTLS)**：仅在启用 *TTLS* 时需要。在列表中，选择要使用的内部身份验证方法。选项包括：**PAP**、**CHAP**、**MSCHAP** 或 **MSCHAPv2**。默认值为 **MSCHAPv2**。
- 使用 **PAC** 的 **EAP-FAST**：选择是否使用受保护的访问凭据 (PAC)。
  - 如果选择使用 **PAC**，请选择是否使用预配 PAC。
    * 如果选择预配 **PAC**，请选择是否允许在最终用户客户端与 Endpoint Management 之间建立匿名 TLS 握手。
      · 匿名预配 **PAC**
- 身份验证：
  - 使用 **Active Directory** 身份验证：选择是否启用 Active Directory 身份验证。适用于 macOS 10.7 及更高版本。要使此选项可用，请完成以下操作：
    * 将 **PEAP** 设置为 EAP 协议。
    * 将配置文件范围设置为 系统。只有在将策略应用于整个系统时，才能使用此设置选项。
  - 用户名：键入用户名。
  - 为连接单独设置密码：选择用户是否在每次登录时都需要提供密码。
  - 密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。
  - 身份凭据 **(**密钥库或 **PKI** 凭据**)**：在列表中，选择身份凭据的类型。默认值为无。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 外部标识：仅在启用 **PEAP**、**TTLS** 或 **EAP-FAST** 时需要。键入外部可见的用户名。您可以通过键入“anonymous”等通用术语以使用户名不可见来增加安全性。
  - 需要 **TLS** 证书：选择是否需要 TLS 证书。
- 信任
  - 可信证书：要添加可信证书，请单击添加，然后，针对要添加的各个证书执行以下操作：
    - 应用程序：在列表中，单击要添加的应用程序。
    - 单击保存以保存证书，或者单击取消。
  - 可信服务器证书名称：要添加可信服务器证书公用名，请单击添加，然后针对要添加的名称执行以下操作：
    - 证书：键入要添加的服务器证书的名称。可以使用通配符指定名称，如 wpa.*.example.com。
    - 单击保存以保存证书名称，或者单击取消。
- 允许信任例外：选择当证书不可信时是否在用户设备上显示证书信任对话框。默认值为开。

Android Enterprise 设置



- 网络名称：键入在用户设备上的可用网络列表中的 SSID。
- 身份验证：在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - 共享虚拟机
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下各节列出了要为上述各个连接类型配置的选项。默认值为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

适用于 **Android Enterprise** 的 **“开放”**、**“共享”** 设置

- 加密：在列表中，选择已禁用或 **WEP**。默认值为 **WEP**。
- 密码：键入可选密码。
- 隐藏网络：选择是否隐藏网络。

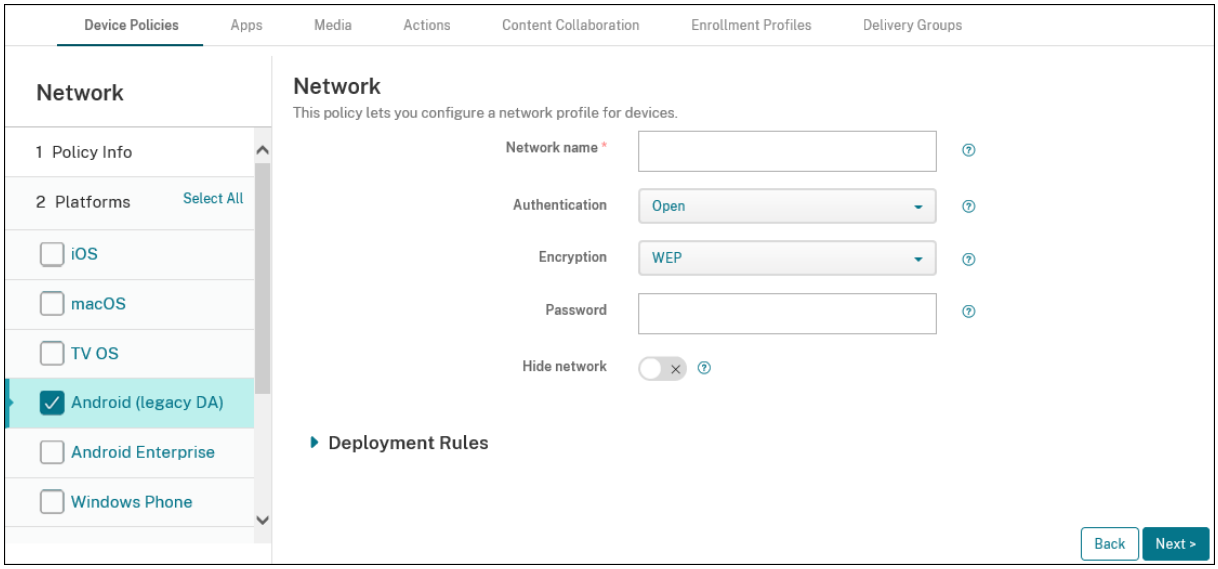
适用于 **Android** 的 **“WPA”**、**“WPA-WPA2”**、**“WPA2-PSK”** 设置

- 加密：在列表中，选择 **TKIP** 或 **AES**。默认值为 **TKIP**。
- 密码：键入可选密码。
- 隐藏网络：选择是否隐藏网络。

适用于 **Android** 的 **802.1x** 设置

- **EAP** 类型：在列表中，选择 **PEAP**、**TLS** 或 **TTLS**。默认值为 **PEAP**。
- 密码：键入可选密码。
- 身份验证阶段 **2**：在列表中，选择无、**PAP**、**MSCHAP**、**MSCHAPPv2** 或 **GTC**。默认值为 **PAP**。
- 身份：键入可选用户名和域。
- 匿名：键入外部可见的可选用户名。您可以通过键入 “anonymous” 等通用术语以使用户名不可见来增加安全性。
- **CA** 证书：在列表中，选择要使用的证书。
- 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
- 隐藏网络：选择是否隐藏网络。

Android（旧版 **DA**）设置



- 网络名称：键入在用户设备上的可用网络列表中的 SSID。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 身份验证：在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - 共享（仅限 Android Enterprise）
  - WPA（仅限 Android Enterprise）
  - WPA-PSK（仅限 Android Enterprise）
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下各节列出了要为上述各个连接类型配置的选项。

适用于 **Android** 的 **“开放”**、**“共享”** 设置

- 加密：在列表中，选择已禁用或 **WEP**。默认值为 **WEP**。
- 密码：键入可选密码。
- 隐藏网络：选择是否隐藏网络。

适用于 **Android** 的 **“WPA”**、**“WPA-WPA2”**、**“WPA2-PSK”** 设置

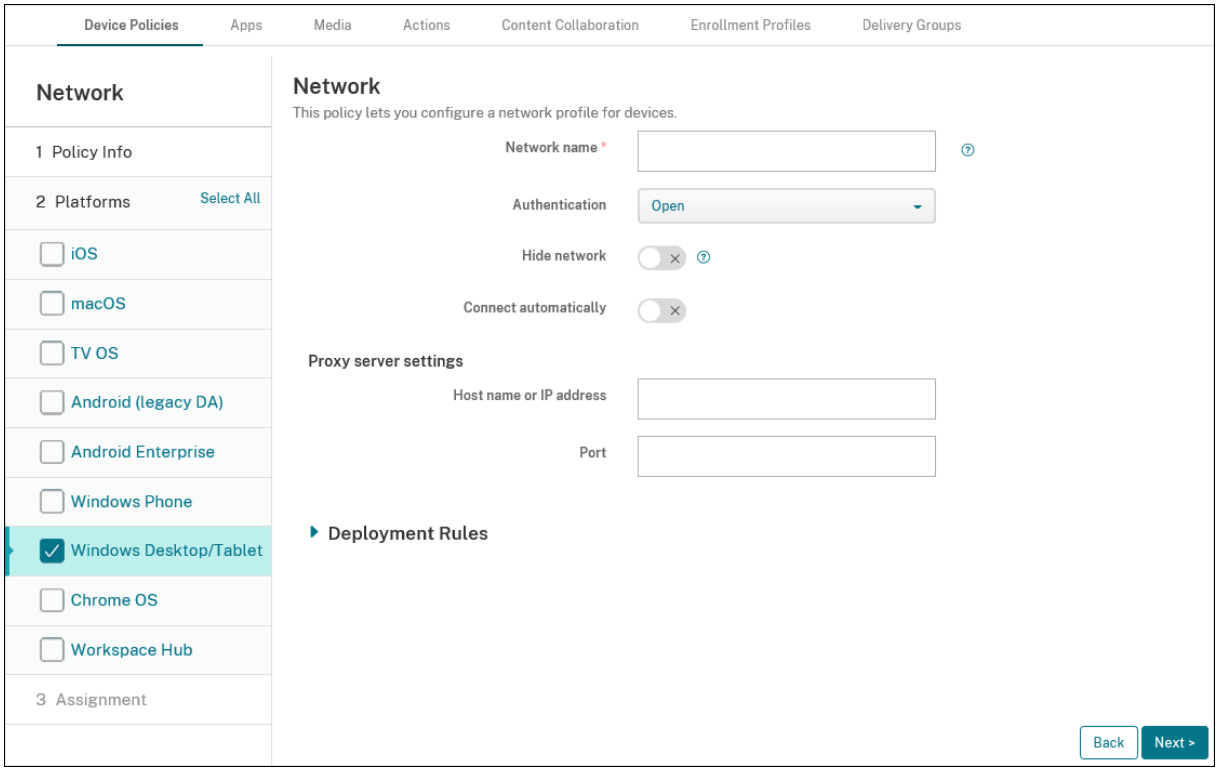
- 加密：在列表中，选择 **TKIP** 或 **AES**。默认值为 **TKIP**。
- 密码：键入可选密码。
- 隐藏网络：选择是否隐藏网络。

适用于 **Android** 的 **802.1x** 设置

- **EAP** 类型：在列表中，选择 **PEAP**、**TLS** 或 **TTLS**。默认值为 **PEAP**。
- 密码：键入可选密码。
- 身份验证阶段 **2**：在列表中，选择无、**PAP**、**MSCHAP**、**MSCHAPPv2** 或 **GTC**。默认值为 **PAP**。
- 身份：键入可选用户名和域。
- 匿名：键入外部可见的可选用户名。您可以通过键入 “anonymous” 等通用术语以使用户名不可见来增加安全性。
- **CA** 证书：在列表中，选择要使用的证书。
- 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
- 隐藏网络：选择是否隐藏网络。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop/Tablet 设置



- 网络名称：显示在可用网络列表中的 SSID。
- 身份验证：在列表中，单击用于 Wi-Fi 连接的安全类型。
  - 开放
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 企业版：对于 Windows 10 的最新版本，请将 SCEP 配置为使用 WPA-2 企业版。通过 SCEP 配置，Endpoint Management 可以将证书发送到设备以对 Wi-Fi 服务器进行身份验证。要配置 SCEP，请转到设置 **>** 凭据提供程序的分发页面。有关更多信息，请参阅 凭证提供程序。

以下各节列出了要为上述各个连接类型配置的选项。

打开 Windows 10 和 Windows 11 的设置

- 隐藏网络：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。

适用于 Windows 10 和 Windows 11 的 WPA Personal、WPA-2 Personal 设置

- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- 共享密钥：为所选方法提供加密密钥。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 隐藏网络：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。

Windows 10 和 **Windows 11** 的 **WPA-2 Enterprise** 设置

- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- **EAP** 类型：在列表中，选择 **PEAP-MSCHAPv2** 或 **TLS** 以设置 EAP 类型。默认值为 **PEAP-MSCHAPv2**。
- 隐藏网络：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。
- 启用 **SCEP**?：选择是否使用 SCEP 将证书推送到用户设备。
- **SCEP** 的凭据提供程序：在列表中，选择 SCEP 凭据提供程序。默认值为无。

网络使用设备策略

March 31, 2022

您可以设置网络使用规则，以指定 iOS 设备使用网络（例如手机网络数据网络）的方式。这些规则适用于托管应用程序和指定的 SIM。托管应用程序是指您通过 Endpoint Management 部署到用户设备的应用程序。它们不包括用户在未通过 Endpoint Management 部署的情况下直接下载到其设备的应用程序。它们也不包括设备在 Endpoint Management 中注册时已安装在设备上的应用程序。此策略适用于面向 iOS 13 设备的 SIM。您可以配置应用程序规则、SIM 规则或两者。SIM 规则适用于该设备上的所有托管应用程序。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 应用程序规则
  - 允许手机网络数据漫游：选择指定的应用程序是否可以在漫游时使用手机网络数据连接。默认值为关。
  - 允许手机网络数据：选择指定的应用程序是否可以使用手机网络数据连接。默认值为关。
  - 应用程序标识符匹配：对于要添加到此列表中的每个应用程序，单击添加，然后配置以下设置：
    - 应用程序标识符：键入应用程序标识符。
  - 单击保存将应用程序保存到列表，或单击取消不将应用程序保存到列表。
- **SIM** 规则
  - **SIM Wi-Fi** 助理策略：启用 **Switch from poor Wi-Fi**（从连接信号弱的 Wi-Fi 切换）功能可使 Wi-Fi 助理策略更加积极地从连接信号弱的 Wi-Fi 切换到蜂窝网络连接。此设置会增加蜂窝移动数据的使用量并影响电池寿命。
  - **SIM ICCID**：对于要添加到列表中的每个 SIM 卡，单击添加，然后配置以下设置：
    - **ICCID**：键入要添加的 SIM 卡的 19 或 20 位数字。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

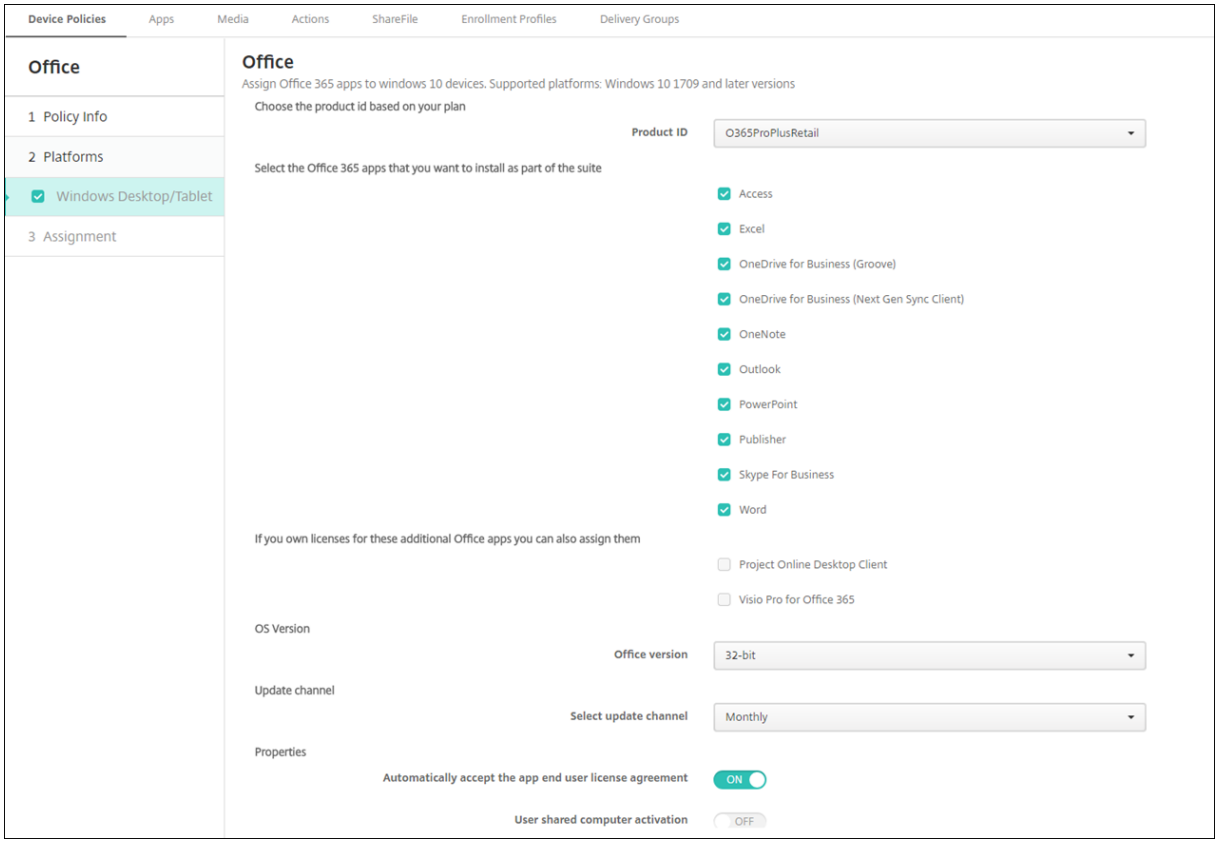
Office 设备策略

March 31, 2022

Endpoint Management 允许您使用 Office 配置服务提供程序 (CSP) 部署 Microsoft Office 365 产品。通过配置 Office 设备策略，您可以将 Microsoft Office 应用程序部署到运行 Windows 10（版本 1709 或更高版本）或 Windows 11 的任何设备。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Windows Desktop/Tablet 设置



- 产品 **ID**：根据您的 Office 365 计划选择产品 ID。选项为 **O365ProPlusRetail**、**O365BusinessRetail** 或 **O365SmallBusPremRetail**。
- **Office 365** 应用程序：选择要部署的 Office 365 应用程序。默认选择所有应用程序。
- 附加 **Office** 应用程序：如果您有 **Project Online Desktop Client** 或 **Visio Pro for Office 365** 的许可证，则可以选择这些应用程序以进行安装。
- **Office** 版本：选择安装 **32** 位还是 **64** 位版本的 Office。
- 更新渠道：选择希望更新发生的频率。选项为月度、月度 **(**定向**)**、半年度或半年度 **(**定向**)**。
- 属性：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 自动接受应用程序最终用户许可协议：选择开或关。默认值为开。
  - 用户共享计算机激活：选择计算机是否共享。选项为开或关。默认值为关。
- **Office** 语言： Office 以 Windows 已安装的语言自动安装。可以选择要安装的其他语言。

组织信息设备策略

March 31, 2022

“组织信息”设备策略指定从 Endpoint Management 推送到 iOS 设备的警报消息的组织信息。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 名称：键入运行 Endpoint Management 的组织的名称。
- 地址：键入组织的地址。
- 电话：键入组织的支持电话号码。
- 电子邮件：键入支持电子邮件地址。
- 魔术字：键入用于描述组织托管的服务的单词或短语。

“操作系统更新”设备策略

July 24, 2023

通过“操作系统更新”设备策略，可以：

- 将最新的操作系统更新部署到受监督的 iOS 设备。

  “操作系统更新”设备策略仅适用于在 Apple 部署计划中注册的受监督设备。

- 将最新的操作系统和应用程序更新部署到注册了 Apple 部署计划并且运行 macOS 10.11.5 及更高版本的 macOS 设备。

> 注意：
>
> Apple 目前仅将操作系统更新限制为主要版本。管理员无权更新次要版本。有关更多信息，请参阅 Apple 文档中的这篇文章。

- 运行 Windows 10 或 Windows 11 的受监督 Desktop 和 Tablet 设备的最新操作系统更新。

  您还可以使用操作系统更新策略来管理运行 Windows 10（版本 1607 或更高版本）或 Windows 11 的台式机和平板电脑的交付优化设置。交付优化是微软为 Windows 10 和 Windows 11 更新提供的点对点客户端更新

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

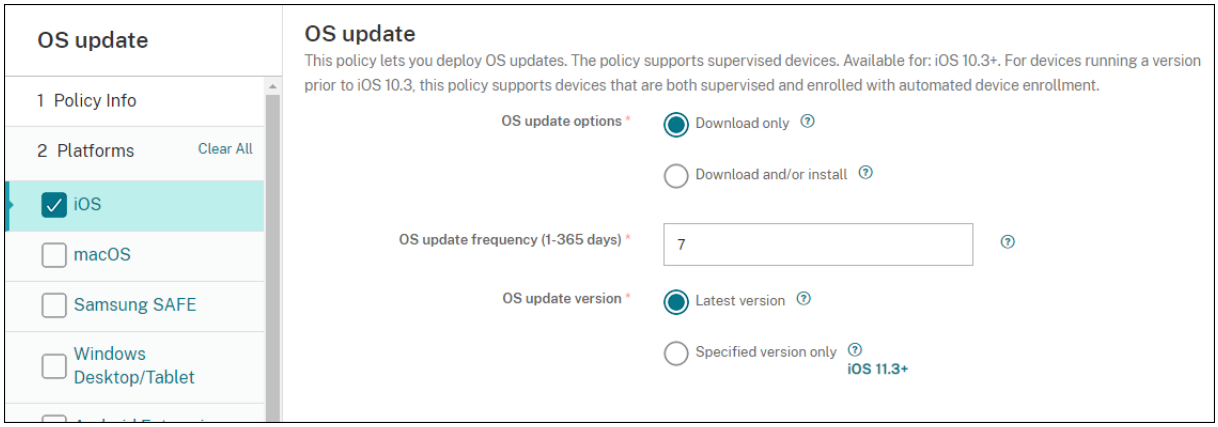
服务。传递优化的目标是减少更新过程中出现的带宽问题。带宽降低是通过在多个设备和自建共享下载任务实现的。有关详细信息，请参阅微软文章，为 Windows 10 更新配置交付优化。

- 将最新的操作系统更新部署到托管 Android Enterprise 设备（Android 7.0 及更高版本）。
- 将指定的操作系统更新文件部署到 Citrix Ready Workspace Hub 设备。

> 重要提示：
>
> 操作系统更新策略不允许您完全禁用更新。要将更新延迟 90 天，请创建限制策略。请参阅 限制设备策略。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

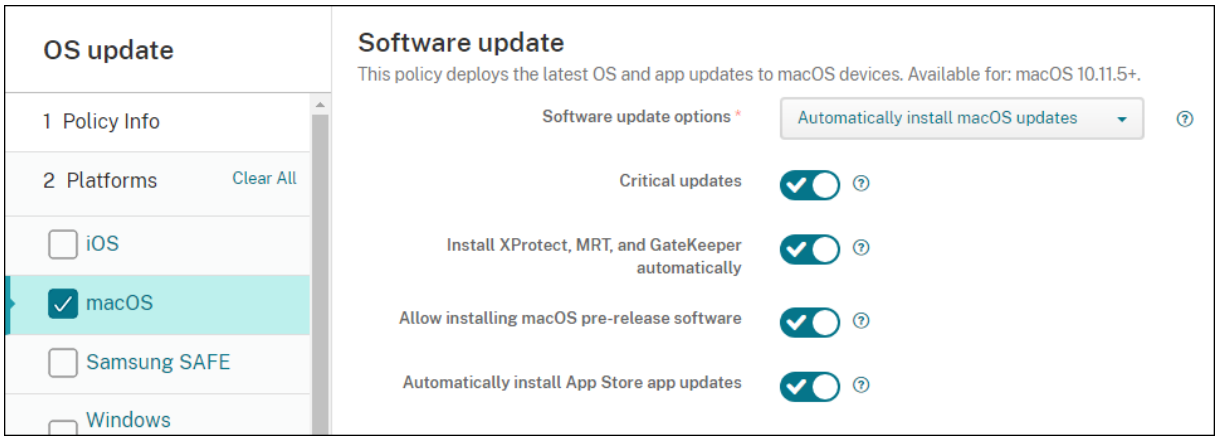


以下设置适用于受监督的 iOS 设备。

- 操作系统更新选项：这两个选项都将根据操作系统更新频率将最新的操作系统更新下载到受监督的设备。设备将提示用户安装更新。提示在用户解锁设备后可见。
- 操作系统更新频率：确定 Endpoint Management 检查和更新设备操作系统的频率。默认值为 **7** 天。
- 操作系统更新版本：指定用于更新受监督的 iOS 设备的版本。默认值为最新版本。
  - 最新版本：选择此选项可更新到最新的操作系统版本。
  - **Specific version only**（仅限特定版本）：选择此选项可更新到特定的操作系统版本，然后键入版本号。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

macOS 设置



- 软件更新选项：控制 macOS 设备检查和安装更新的方式。从以下选项中进行选择：
  - 自动安装 **macOS** 更新：自动下载并安装更新。
  - **Download new updates when available**（下载新更新 (如果可用)）：下载更新但需要手动安装。
  - 检查更新：检查更新是否存在但未自动下载或安装更新。
  - 不要检查更新：不要检查新的更新、下载更新或自动安装更新。用户仍然可以手动安装更新。
- **Critical updates**（关键更新）：允许自动安装关键 macOS 更新。
- **Install xProtect, MRT, and GateKeeper updates automatically**（自动安装 xProtect、MRT 和 GateKeeper 更新）：允许 macOS 设备自动安装安全软件的更新。
- **Allow installation of macOS pre-release software**（允许安装 macOS 预发行软件）：允许用户安装 macOS 软件的预发行版本。
- **Automatically install App Store app updates**（自动安装 App Store 应用程序更新）：允许 App Store 应用程序自动更新。

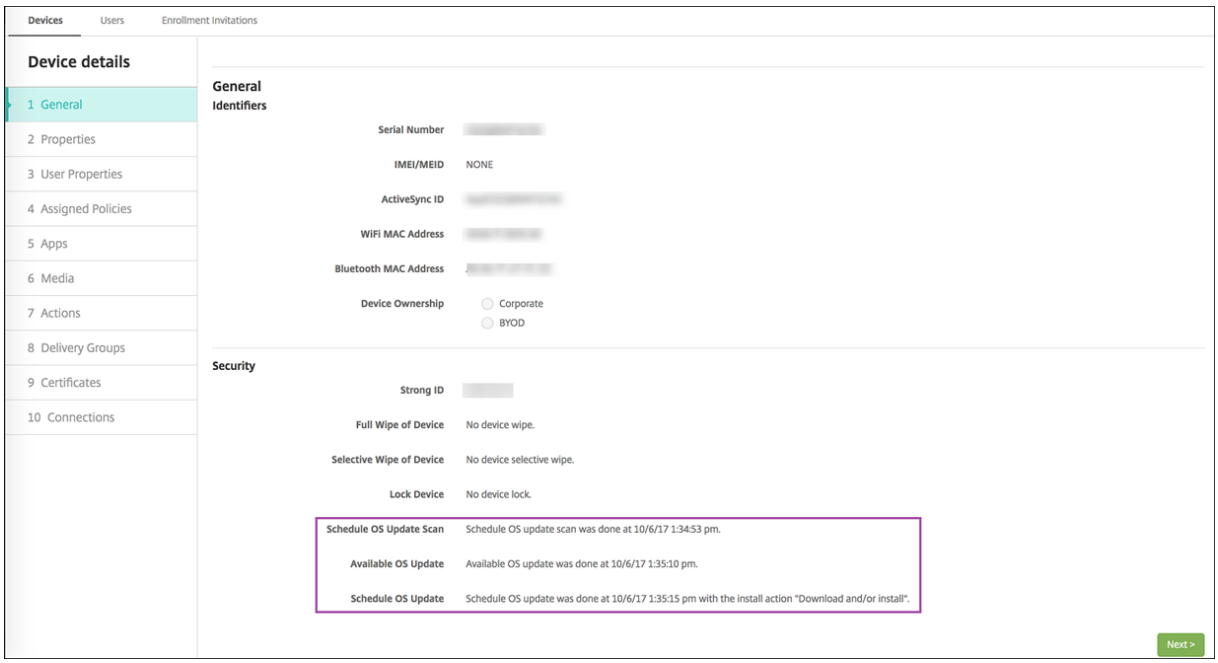
获取 iOS 和 macOS 更新操作的状态

对于 iOS 和 macOS，Endpoint Management 不向设备部署“控制操作系统更新”策略。相反，Endpoint Management 将使用该策略向设备发送以下 MDM 命令：

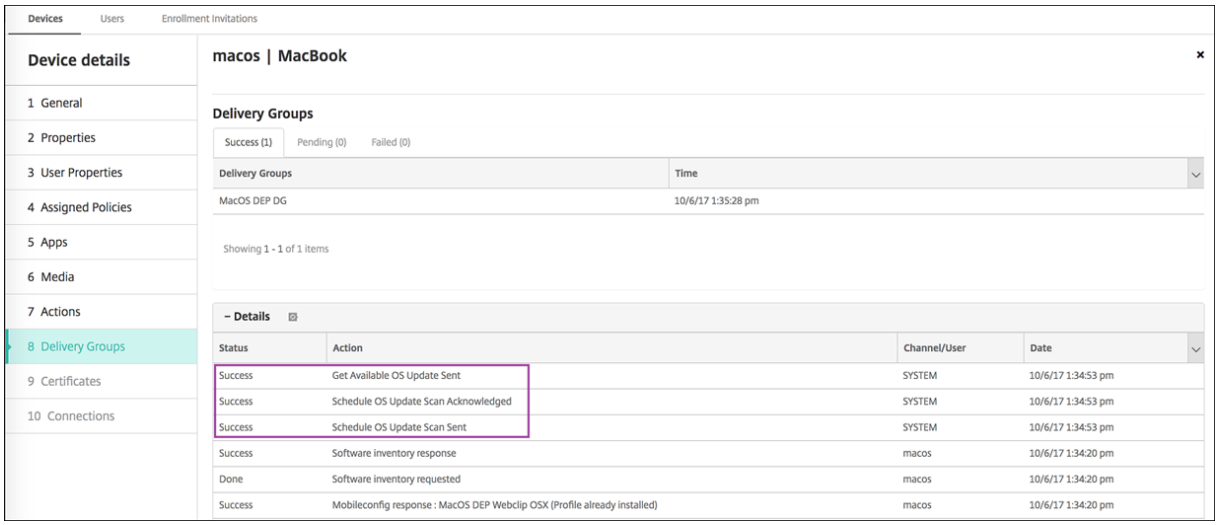
- 安排操作系统更新扫描：请求设备在后台扫描操作系统更新。（iOS 可选）
- 可用的操作系统更新：查询设备中的可用操作系统更新列表。
- 安排操作系统更新：请求设备执行 macOS 更新、应用程序更新或两者。因此，设备操作系统将确定何时下载或安装操作系统和应用程序更新。

管理 **>** 设备 **>** 设备详细信息 **(**常规**)** 页面显示安排的和可用的操作系统更新扫描以及安排的 macOS 和应用程序更新的状态。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

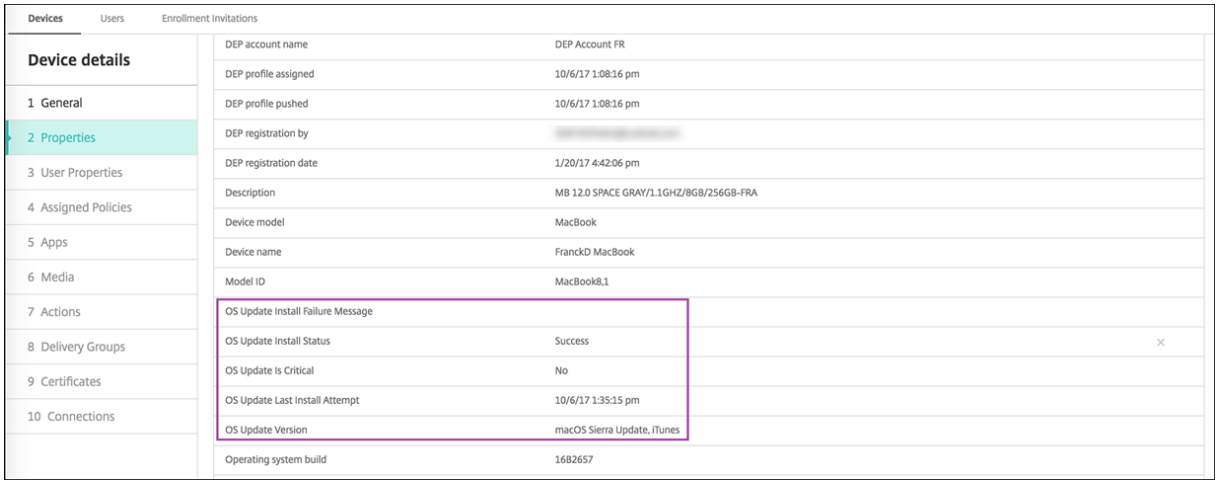


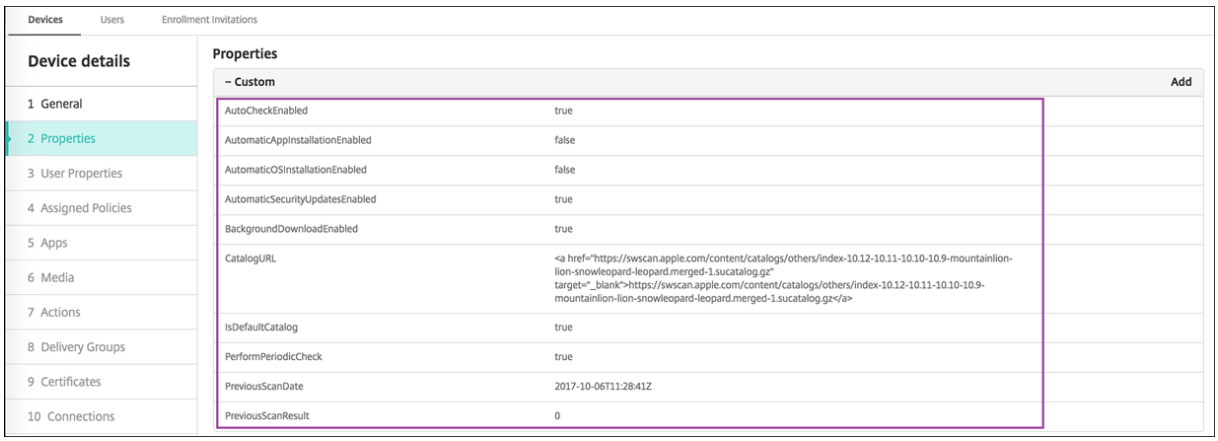
有关更新操作的状态的更多详细信息，请转至管理 **>** 设备 **>** 设备详细信息 **(**交付组**)** 页面。



有关可用的操作系统更新和最后一次安装尝试等详细信息，请转至管理 **>** 设备 **>** 设备详细信息 **(**属性**)** 页面。

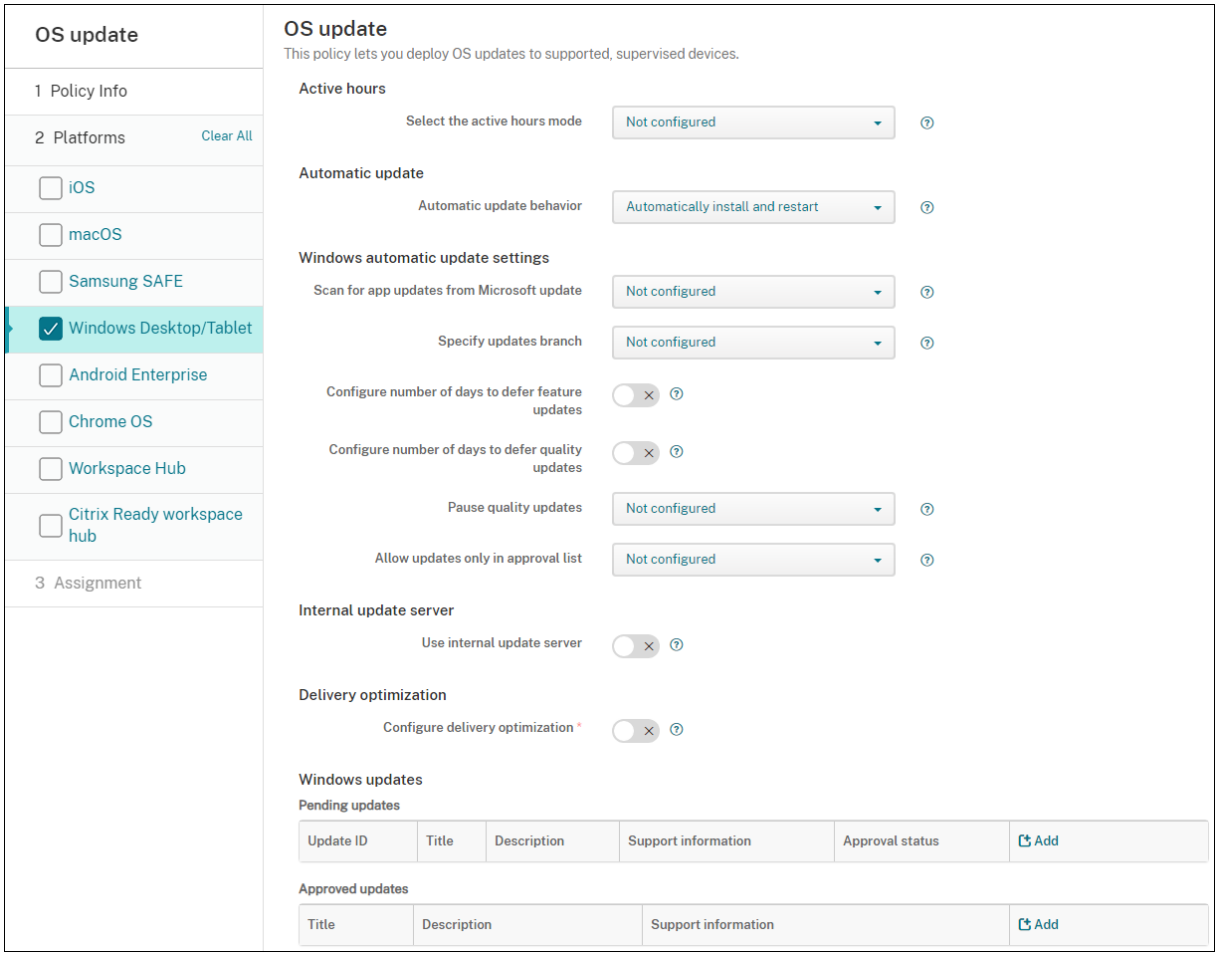
© 1999–2023 Cloud Software Group, Inc. All rights reserved.





© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop 和 Tablet 设置



- 选择使用时段模式：选择用于配置执行操作系统更新的使用时段。可以指定小时的范围或开始和结束时间。选择一种模式后，将显示更多设置：指定使用时段的最大范围或使用时段开始时间和使用时段结束时间。未配置允许 Windows 随时执行操作系统更新。默认值为未配置。
- 自动更新行为：配置用户设备上的 Windows 更新服务的下载、安装和重新启动行为。默认值为自动安装并重新启动。
  - 下载更新前通知用户： Windows 在更新可用时通知用户。Windows 不自动下载和安装更新。用户必须启动下载和安装操作。
  - 自动安装并通知以安排设备重新启动： Windows 在不按流量计费的网络中自动下载更新。设备未在使用中以及不依赖电池电源运行时，Windows 将在自动维护期间安装更新。如果自动维护在两天内无法安装更新，Windows Update 将立即安装更新。如果安装需要重新启动，Windows 将提示用户安排重新启动时间。用户最长有 7 天时间来安排重新启动。7 天后，Windows 将强制设备重新启动。允许用户控制开始时间可降低在重新启动时未正确关闭的应用程序导致的意外数据丢失的风险。
  - 自动安装并重新启动：默认设置。Windows 在不按流量计费的网络中自动下载更新。设备未在使用中以及不依赖电池电源运行时，Windows 将在自动维护期间安装更新。如果自动维护在两天内无法安装更新，Windows Update 将立即安装更新。如果安装要求重新启动，Windows 将在设备不活动时重新启动设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 在指定时间自动安装并重新启动：选择此选项时，将显示更多设置，以便您可以指定日期和时间。默认值为每天凌晨 3 点。自动安装操作在指定时间发生，设备重新启动操作在 15 分钟倒计时后发生。Windows 准备好重新启动时，已登录的用户可以中断 15 分钟倒计时以延迟重新启动。
  - 自动安装并重新启动，无需最终用户控制： Windows 在不按流量计费的网络中自动下载更新。设备未在使用中以及不依赖电池电源运行时，Windows 将在自动维护期间安装更新。如果自动维护在两天内无法安装更新，Windows Update 将立即安装更新。如果安装要求重新启动，Windows 将在设备不活动时重新启动设备。此选项还会将用户控制面板设置为只读。
  - 关闭自动更新：在设备上禁用 Windows 自动更新。
- 扫描 **Microsoft** 更新中的应用程序更新：指定 Windows 是否接受来自 Microsoft 更新服务的面向其他 Microsoft 应用程序的更新。默认值为未配置。
  - 未配置：如果不希望配置该行为，请使用此设置。Windows 不更改用户设备上的相关 UI。用户可以接受或拒绝面向其他 Microsoft 应用程序的更新。
  - 是： Windows 允许从 Windows 更新服务安装应用程序更新。用户设备上的相关设置不活动，因此，用户无法修改该设置。
  - 否： Windows 不允许从 Windows 更新服务安装应用程序更新。用户设备上的相关设置不活动，因此，用户无法修改该设置。
- 指定更新分支：指定要用于更新的 Windows 更新服务分支。默认值为未配置。
  - 未配置：如果不希望配置该行为，请使用此设置。Windows 不更改用户设备上的相关 UI。用户可以选择 Windows 更新服务分支。
  - **Current Branch**： Windows 接收来自 Current Branch 的更新。用户设备上的相关设置不活动，因此，用户无法修改该设置。
  - **Current Branch for Business**： Windows 接收来自 Current Branch for Business 的更新。用户设备上的相关设置不活动，因此，用户无法修改该设置。
- 配置推迟功能更新的天数：如果设置为开，Windows 将推迟功能更新指定的天数，并且用户无法更改此设置。如果设置为关，用户可以更改推迟功能更新的天数。默认值为关。
- 配置推迟质量更新的天数：如果设置为开，Windows 将推迟质量更新指定的天数，并且用户无法更改此设置。如果设置为关，用户可以更改推迟质量更新的天数。默认值为关。
- 暂停质量更新：指定是否暂停质量更新 35 天。默认值为未配置。
  - 未配置：如果不希望配置该行为，请使用此设置。Windows 不更改用户设备上的相关 UI。用户可以选择暂停质量更新 35 天。
  - 是： Windows 暂停来自 Windows 更新服务的质量更新的安装 35 天。用户设备上的相关设置不活动，因此，用户无法修改该设置。
  - 否：Windows 不暂停来自 Windows 更新服务的质量更新的安装。用户设备上的相关设置不活动，因此，用户无法修改该设置。
- 仅允许安装审批列表中的更新：指定是否仅安装 MDM 服务器审批的更新。Endpoint Management 不支持配置更新的审批列表。默认值为未配置。
  - 未配置：如果不希望配置该行为，请使用此设置。Windows 不更改用户设备上的相关 UI。用户可以选择允许安装的更新。
  - 是，仅安装审批的更新：仅允许安装审批的更新。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 否，安装所有适用的更新：允许在设备上安装所有适用的更新。
- 使用内部更新服务器：指定是从 Windows 更新服务获取更新还是通过 Windows Server Update Services (WSUS) 从内部更新服务器获取。如果设置为关，设备将使用 Windows 更新服务。如果设置为开，设备将连接到指定的 WSUS 服务器以获取更新。默认值为关。
  - 接受除 **Microsoft** 以外的其他实体签名的更新：指定是否接受除 Microsoft 以外的第三方实体签名的更新。此功能要求设备信任第三方供应商证书。默认值为关。
  - 允许连接到 **Microsoft** 更新服务：允许设备上的 Windows 更新定期连接到 Microsoft 更新服务，即使设备配置为从 WSUS 服务器获取更新亦如此。默认值为开。
  - **WSUS** 服务器：指定 WSUS 服务器的服务器 URL。
  - 托管更新的备用 **Intranet** 服务器：指定托管更新和接收报告信息的备用 Intranet 服务器 URL。
- 配置交付优化：是否对 Windows 10 和 Windows 11 更新使用交付优化。默认设置为关。
- 缓存大小：传递优化缓存的最大大小。值 **0** 表示缓存大小无限制。默认值为 **10** GB。
- 允许 **VPN** 对等缓存：是否允许设备在通过 VPN 连接到域网络时参与对等缓存。设置为开时，设备可以从其他域网络设备进行下载或上载到其他域网络设备，在 VPN 上或企业域网络中皆可。默认设置为关。
- 下载方法：传递优化的下载方法可以用于下载 Windows 更新、应用程序和应用程序更新。默认值为 **HTTP** 与对等在同一 **NAT** 后面混合。选项包括：
  - 仅限 **HTTP**，无对等：禁用对等缓存，但允许传递优化从 Windows Update 服务器或 Windows Server Update Services (WSUS) 服务器下载内容。
  - **HTTP** 与对等在同一 **NAT** 后面混合：在同一网络中启用对等共享。传递优化云服务使用与目标客户端相同的公用 IP 查找连接到 Internet 的其他客户端。这些客户端随后将尝试使用其专用子网 IP 连接到同一网络红的其他对等体。
  - **HTTP** 与对等跨专用组混合：根据设备 Active Directory 域服务 (AD DS) 或设备进行身份验证的域自动选择组。对等跨内部子网在属于相同组的设备之间发生，包括远程办公室内的设备。
  - **HTTP** 与 **Internet** 对等混合：为传递优化启用 Internet 对等源。
  - 简单下载模式，无对等：禁用传递优化云服务。传递优化在以下情况下自动切换到此模式：传递优化云服务不可用时、无法访问时或内容文件大小小于 10 MB 时。在此模式下，传递优化提供可靠的下载体验，无对等缓存。
  - 不使用传递优化，改为使用 **BITS**：允许客户端使用 BranchCache。有关详细信息，请参阅 Microsoft 文章分支缓存。
- 最大下载带宽：最大下载带宽，单位为 KBs/秒。默认值为 **0**，表示动态带宽调整。
- 最大下载带宽的百分比：传递优化可以跨所有并发下载活动使用的最大下载带宽。值为可用下载带宽的百分比。默认值为 **0**，表示动态调整。
- 最大上载带宽：最大上载带宽，单位为 KBs/秒。默认值为 **0**。值 **0** 表示带宽无限制。
- 每月上载数据上限：传递优化在每个日历月可以上载到 Internet 对等方的最大大小，单位为 GB。默认值为 20 GB。值 **0** 表示每月上载无限制。

Endpoint Management 如何处理对 **Windows Desktop** 和 **Tablet** 设备的批准更新

您可以指定是否仅安装审批的更新。Endpoint Management 按如下方式处理更新：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 对于安全更新，例如 Windows Defender 定义，Endpoint Management 将在下次同步过程中自动审批更新并向设备发送安装命令。
- 对于所有其他更新类型，Endpoint Management 将等待您审批后再向设备发送安装命令。

必备条件

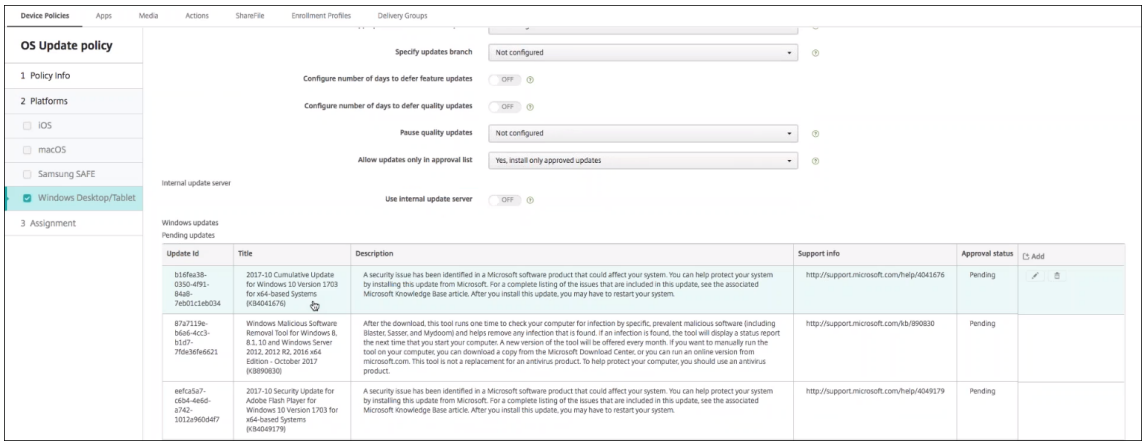
- 必须将 Microsoft 根证书发送到 Endpoint Management 服务器作为服务器证书。
- 有关导入服务器证书的信息，请参阅证 书和身份验证中的“要导入证书”。

仅安装审批的更新

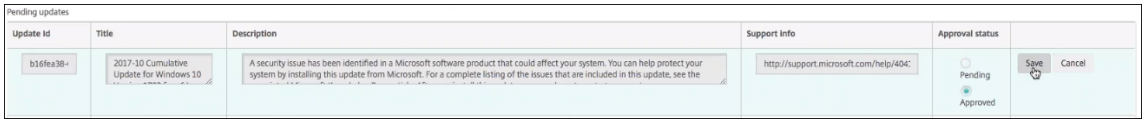
1. 转至配置 > 设备策略并打开“操作系统更新”设备策略。
2. 将仅允许安装审批列表中的更新设置更改为是，仅安装审批的更新。

审批更新

1. 在“操作系统更新”设备策略中，向下滚动到待定更新表。Endpoint Management 从设备中获取表中列出的更新。
2. 搜索审批状态为待定的更新。
3. 单击要审批的更新对应的行，然后单击该行对应的编辑图标（在添加列中）。



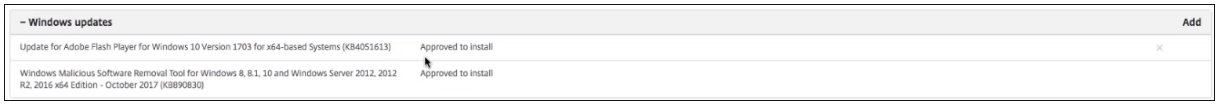
4. 要审批更新，请单击已审批，然后单击保存。



> 注意：
>
> 虽然“待定更新”表包含添加和删除命令，但这些命令不会导致 Endpoint Management 数据库发生任何更改。编辑审批状态是唯一可用于待定更新的操作。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要查看设备的 Windows 更新状态，请转至管理 **>** 设备 **>** 属性。



发布了某个更新时，更新 **ID** 将在第一列中显示，状态为（成功或失败）。可以为更新失败的设备创建报告或自动化操作。发布的日期和时间也将显示。

更新如何用于首次部署和后续部署

设备上的“操作系统更新”设备策略的对首次部署产生的影响与对设备更新后的部署产生的影响有所差别。

- 必须至少配置一个“操作系统更新”设备策略并将其分配给交付组，Endpoint Management 才能查询设备更新。

  Endpoint Management 在设备 MDM 同步期间查询设备的可安装更新。

- 第一个“操作系统更新”设备策略部署后，Windows 更新的列表为空，因为尚未报告任何设备。
- 当已分配的交付组报告中的设备更新时，Endpoint Management 会将这些更新保存在其数据库中。要审批任何报告的更新，请再次编辑该策略。

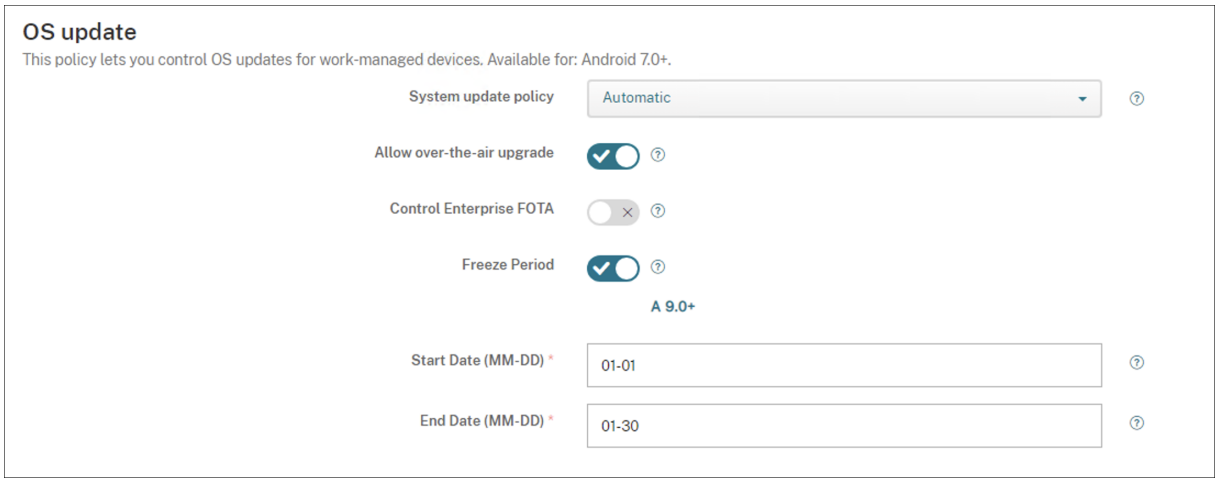
  更新批准仅适用于正在编辑的策略。在一个策略中审批的更新在另一个策略中不显示为已审批。下次设备同步时，Endpoint Management 会向设备发送一条命令以指示更新已审批。

- 对于第二个“操作系统更新”设备策略，更新列表包含 Endpoint Management 数据库中存储的更新。批准每个策略的更新。

  每次设备同步过程中，Endpoint Management 都会查询设备的已审批的更新状态，直至设备报告已安装更新。对于要求在安装后重新启动的更新，Endpoint Management 将查询更新的状态，直至设备报告更新已安装。

- Endpoint Management 不按交付组或设备限制策略配置页面中显示的更新。设备报告的所有更新都在列表中显示。

Android Enterprise 设置



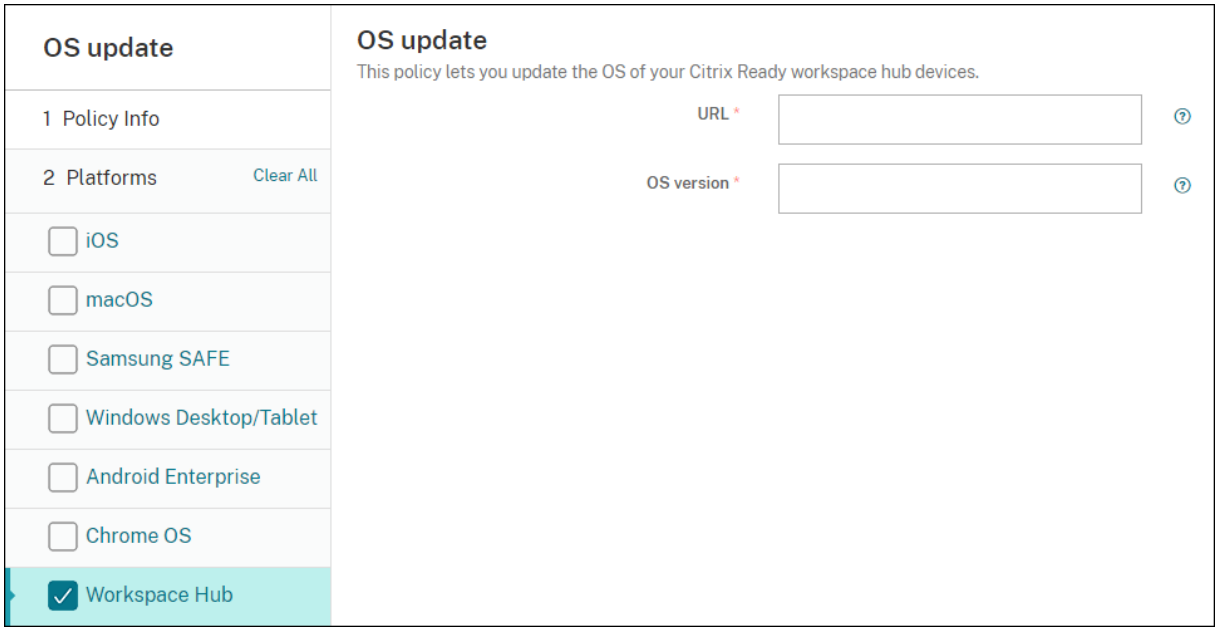
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 系统更新策略：确定系统更新的发生时间。如果启用 控制企业 **FOTA** 设置，则无论此设置的配置如何，都会自动进行更新。
  - 自动：当更新可用时安装更新。
  - 窗口：在 开始时间和结束时间中指定的日常维护时段内自动安装更新。
    - 开始时间：维护时段的开始时间，测量方式为在设备本地时间从午夜开始的分钟数 (**0** - **1440**)。默认值为 **0**。
    - 结束时间：维护时段的结束时间，测量方式为在设备本地时间从午夜开始的分钟数 (**0** - **1440**)。默认值为 **120**。
  - 推迟：允许用户将更新最长推迟 30 天。
  - 默认：将更新策略设置为系统默认值。
- 允许无线升级：如果禁用，用户设备将无法以无线方式接收软件更新。默认值为开。
- **Freeze Period**（冻结期限）：如果设置为 **On**（开），则在为 **Automatic**（自动）、**Postpone**（推迟）和 **Windowed**（窗口化）更新策略指定的日期范围内，不会在设备上安装操作系统更新。一次只能为一台设备设置一个冻结期限。冻结期限不得超过 90 天。
  - **Start Date/End Date**（开始日期/结束日期）：如果启用了 **Freeze Period**（冻结期限），则指不会安装操作系统更新的日期范围。
- **Freeze Period**（冻结期限）：如果设置为 **On**（开），则在为 **Automatic**（自动）、**Postpone**（推迟）和 **Windowed**（窗口化）更新策略指定的日期范围内，不会在设备上安装操作系统更新。一次只能为一台设备设置一个冻结期限。冻结期限不得超过 90 天。
  - **Start Date/End Date**（开始日期/结束日期）：如果启用了 **Freeze Period**（冻结期限），则指不会安装操作系统更新的日期范围。

Workspace Hub 设置

可以使用“操作系统更新”设备策略为 Citrix Ready Workspace Hub 设备指定更新文件。Workspace Hub 设备使用 Endpoint Management 服务器签入时，设备会下载更新文件并自动安装。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- **URL**：上载操作系统更新文件的 URL。首先，从操作系统供应商处下载操作系统更新文件，然后将其上载到可通过 HTTP 或 HTTPS 访问的共享中。请勿使用任何凭据保护该共享。类的更新文件仅适用于相同类的设备。

  URL 的结尾还必须是在操作系统更新文件中使用的 `VERSION-CLASS-KERNEL-ARCHITECTURE-BUILDNUM.lfi` 格式的命名。

  Citrix Ready Workspace Hub 设备使用 Endpoint Management 服务器签入时，设备会下载更新文件并自动安装。无论正在安装的设备操作系统版本较低还是较高，都会进行安装。

  该策略仅适用于与在策略中配置的更新文件具有相同类的设备。例如，如果策略具有适用于 NComputing 设备（NC 类）的更新文件，则只有签入的 NComputing 设备才会收到更新。如果 ViewSonic 设备（VS 类）签入，Endpoint Management 将不应用更新。

- 操作系统版本：格式为 `VERSION-CLASS-KERNEL-ARCHITECTURE-BUILDNUM` 或 `VERSION-CLASS-KERNEL-BUILDNUM` 的操作系统版本。

通行码设备策略

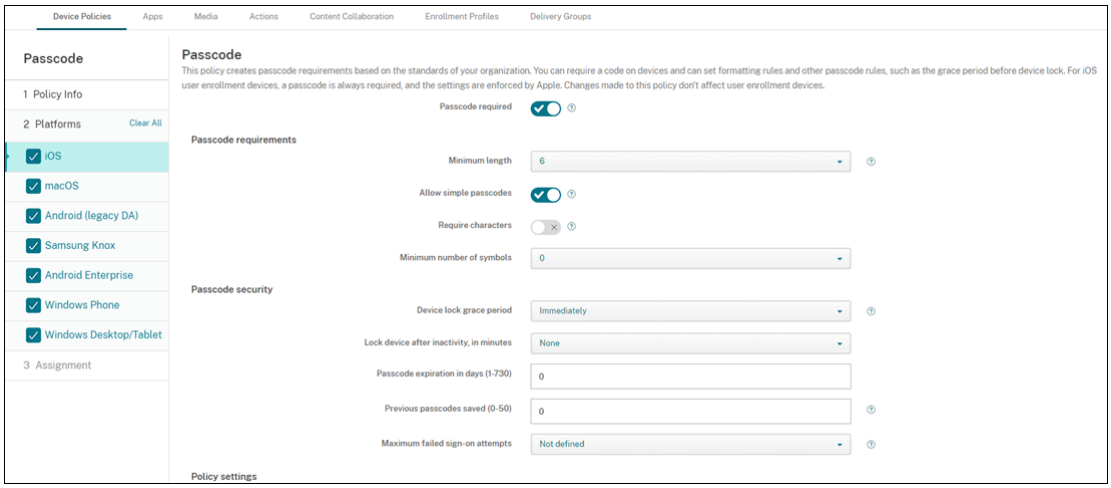
November 7, 2022

根据贵组织的标准在 Endpoint Management 中创建通行码策略。可以要求在用户设备上输入通行码，并且可以设置各种格式和通行码规则。为 iOS、macOS、Android、Android Enterprise 和 Windows Desktop/Tablet 创建策略。每种平台需要一组不同的值，本文将对此进行介绍。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 设置

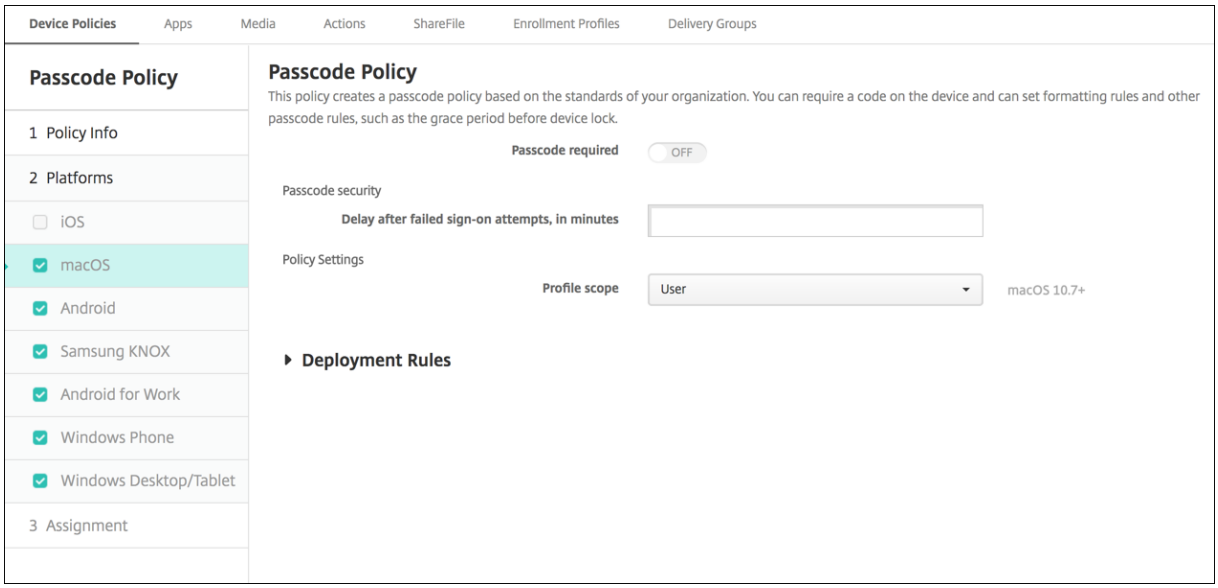


- 需要通行码：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。
- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 **6**。
  - 允许使用简单通行码：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为开。
  - 需含字符：选择是否要求通行码至少包含一个字母。默认值为关。
  - 符号数下限：在列表中，单击通行码必须包含的符号数量。默认值为 **0**。
- 通行码安全
  - 设备锁定宽限期：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。默认值为立即。
  - **Lock device after inactivity**（不活动后锁定设备）：在框中，输入设备在锁定之前可以不活动的时间长度。值可以介于 1 到 15 分钟之间。将该值设置为无将禁用此策略。默认值为无。
  - 通行码有效期限 **(1 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 失败登录尝试次数上限：在列表中，单击用户在登录之前可以失败的次数。
    - 如果您将此数字设置为大于 6，则在第六次尝试之后，设备会在两次尝试之间施加一段时间延迟。每次失败尝试的延迟都会增加。在最后一次尝试之后，所有数据和设置都将被安全删除。
    - 如果将数值设置为 6 或更低的值，则会在不实施时间延迟的情况下擦除设备。
    - 如果选择未定义，则在尝试 6 次后，设备会增加两次尝试之间的时间限制，但不会被擦除。

    默认值为未定义。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

macOS 设置



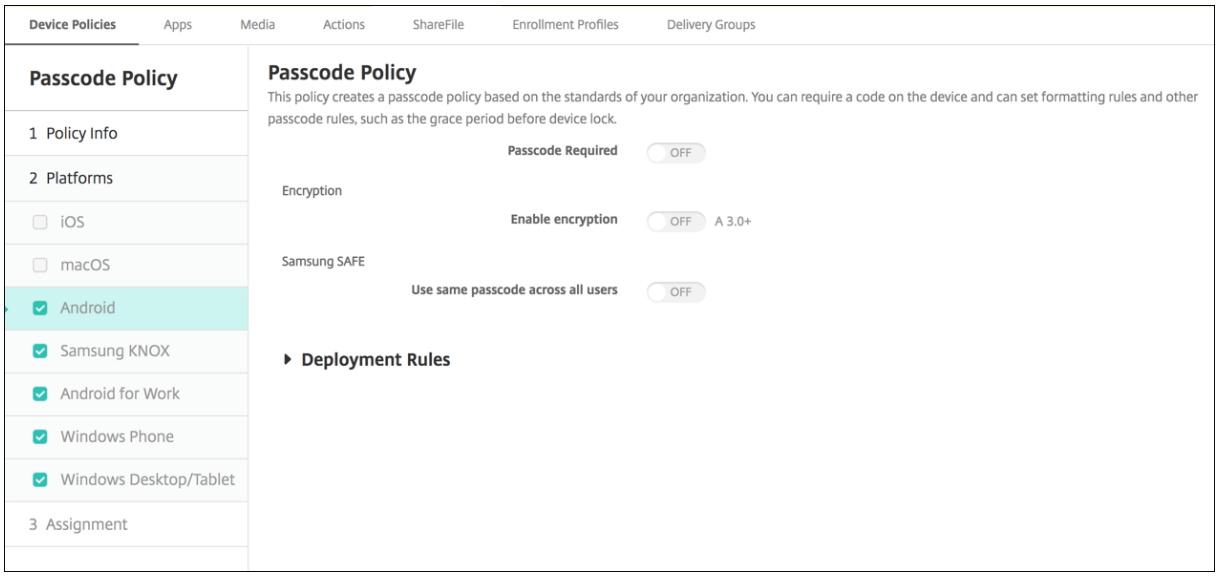
- 需要通行码：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。
- 如果需要通行码已禁用，请在尝试登录失败后的延迟时间 **(**分钟**)** 旁边，键入允许用户重新输入其通行码之前延迟的分钟数。
- 如果启用了需要通行码，请配置以下设置：
- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 **6**。
  - 允许使用简单通行码：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为开。
  - 需含字符：选择是否要求通行码至少包含一个字母。默认值为关。
  - 符号数下限：在列表中，单击通行码必须包含的符号数量。默认值为 **0**。
- 通行码安全
  - 设备锁定宽限期：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。默认值为无。
  - 不活动后锁定设备：在列表中，单击设备在锁定之前可以不活动的时间长度。该值可以介于 1 到 5 分钟之间。将该值设置为无将禁用此策略。默认值为无。
  - 通行码有效期限 **(1 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 失败登录尝试次数上限：在列表中，单击用户在登录之前可以失败的次数。
    - 如果您将此数字设置为大于 6，则在第六次尝试之后，设备会在两次尝试之间施加一段时间延迟。每次失败尝试的延迟都会增加。最后一次尝试后，设备将锁定。
    - 如果将数值设置为 6 或更低的值，设备将锁定而不实施时间延迟。
    - 如果选择未定义，则在尝试 6 次后，设备会增加两次尝试之间的时间限制，但不会锁定。

    默认值为未定义。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 尝试登录失败后的延迟时间 **(**分钟**)**：键入用户达到最大失败尝试次数后登录窗口出现之前的分钟数。
  - 强制重置通行码：如果设置为关，则用户在设备收到此策略后下次进行身份验证时无需重置其通行码。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Android（旧版 **DA**）设置



> 注意：
>
> Android 的默认值为关。

- 需要通行码：选择此选项以要求输入通行码并显示 Android 通行码设备策略的配置选项。页面将展开，允许您配置通行码要求、通行码安全和加密的设置。
- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 6。
  - 生物特征识别：选择是否启用生物特征识别。如果启用此选项，需含字符字段将隐藏。默认值为关。
  - 必填字符：在列表中，单击“无限制”、“数字和字母”、“仅限数字”或“仅字母”以配置通行码的组成方式。默认值为无限制。
  - 高级规则：选择是否应用高级通行码规则。默认值为关。
  - 启用高级规则时，请在下面每个列表中，单击通行码必须包含的每种字符类型的最小数量：
    - 符号：符号的最小数量。

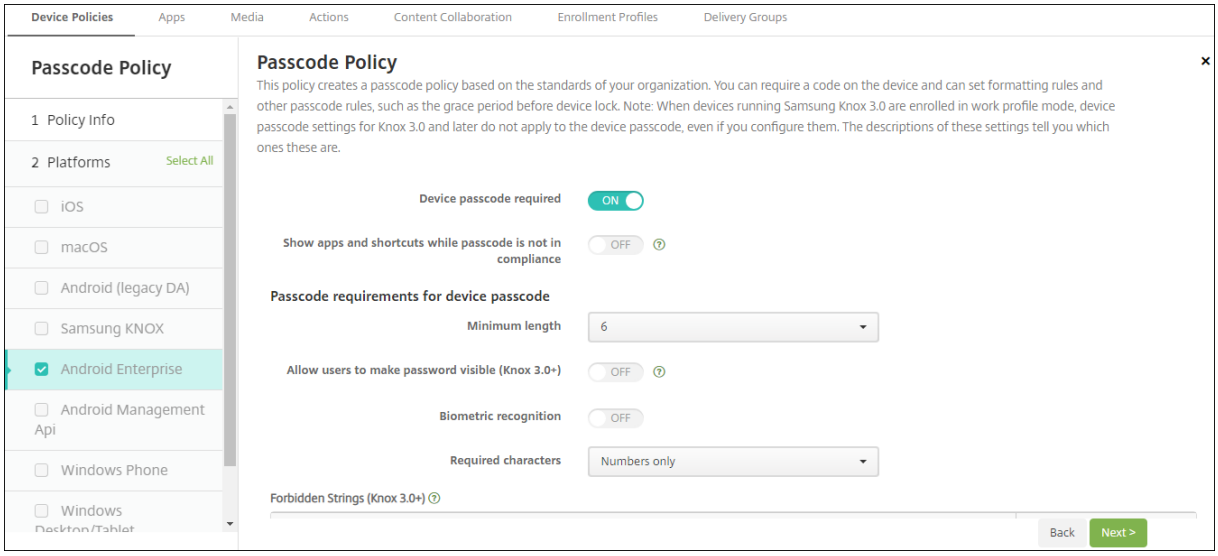
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 字母：字母的最小数量。
    * 小写字母：小写字母的最小数量。
    * 大写字母：大写字母的最小数量。
    * 数字或符号：数字或符号的最小数量。
    * 数字：数字的最小数量。

- 通行码安全
  - 不活动后锁定设备：在列表中，单击设备在锁定之前可以不活动的时间长度。默认值为无
  - 通行码有效期限 **(1 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 失败登录尝试次数上限：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被擦除。默认值为未定义。
- 加密
  - 启用加密：选择是否启用加密。无论需要通行码设置为何，此选项都可用。

    要加密其设备，用户必须首先具有充电电池并接通设备电源，直至加密完成。此过程可能需要一小时或更长时间。如果中断加密过程，用户可能会丢失其设备上的部分或全部数据。设备加密后，过程无法逆转，除非执行出厂重置，但这样会擦除设备上的所有数据。

Android Enterprise 设置



对于 Android Enterprise 设备，可以要求设备的通行码或 Android Enterprise 工作配置文件的安全质询或两者。

- 需要设备通行码：需要设备上的通行码。当此设置设为开时，请配置设备通行码的通行码要求和设备通行码的通行码安全性下的设置。默认设置为关。
- **Show apps and shortcuts while passcode is not in compliance**（在通行码不合规时显示应用程序和快捷方式）：如果此设置为开，设备上的应用程序和快捷方式也不会被隐藏，即使通行码不合规亦如此。当此设

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

置设为关时，如果通行码不合规，应用程序和快捷方式将被隐藏。如果启用此设置，Citrix 建议您创建一项自动操作，以便在通行码不合规时将设备标记为不合规。默认设置为关。

- 设备通行码的通行码要求：
  - 最小长度：指定通行码的最小长度。默认值为 6。
  - 生物特征识别：启用生物特征识别。如果此设置设为开，则隐藏需含字符字段。默认值为关。
  - 需含字符：指定通行码所需的字符类型。在列表中，选择无限制、数字和字母、仅数字或仅字母。请仅对运行 Android 7.0 的设备使用无限制。Android 7.1 及更高版本不遵守无限制设置。默认值为数字和字母。
  - 高级规则：对可能出现在通行码中的字符类型应用高级规则。当此设置设为开时，请在数量下限和数量上限下配置设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为关。
  - 数量下限：
    * 符号：指定符号的最小数量。默认值为 **0**。
    * 字母：指定字母的最小数量。默认值为 **0**。
    * 小写字母：指定小写字母的最小数量。默认值为 **0**。
    * 大写字母：指定大写字母的最小数量。默认值为 **0**。
    * 数字或符号：指定数字或符号的最小数量。默认值为 **0**。
    * 数字：指定数字的最小数量。默认值为 **0**。
    * 更改的字符：适用于运行 Samsung Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作配置文件设备的设备。指定用户必须在以前的通行码中更改的字符数量。默认值为 **0**。
  - 数量上限：适用于运行 Samsung Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作配置文件设备的设备。
    * 字符可以出现的次数：指定某个字符可以在通行码中出现的最大次数。默认值为 **0**，这意味着没有上限。
    * 字母序列长度：指定通行码中字母序列的最大长度。默认值为 **0**，这意味着没有上限。
    * 数字序列长度：指定通行码中数字序列的最大长度。默认值为 **0**，这意味着没有上限。
- 设备密码的密码复杂性（**Android 12+**）：
  - 应用密码复杂性：要求密码的复杂程度由平台定义，而不是自定义密码要求。仅适用于 Android 12+ 和使用 Secure Hub 22.9 或更高版本的设备。
  - 复杂程度：预定义的密码复杂程度。
    * 无：无需密码。
    * 低：密码可以是：
      - 一种模式
      - 至少包含四位数字的 PIN 码
    * 中：密码可以是：
      - 不包含重复序列 (4444) 或有序序列 (1234) 且至少有四位数字的 PIN 码
      - 按字母顺序，最少包含四个字符
      - 至少包含四个字符的字母数字
    * 高：密码可以是：
      - 不包含重复序列 (4444) 或有序序列 (1234) 且至少有八位数字的 PIN 码

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 按字母顺序，最少包含六个字符
- 至少包含六个字符的字母数字

> 注意：
> 对于 BYOD 设备，最小长度、必填字符、生物识别和高级规则等密码设置不适用于 Android 12+。改用密码复杂性。

- 设备通行码的通行码安全性：
  - 此次数后擦除设备 **(**失败登录尝试次数**)**：指定用户可以登录失败的次数，超过此次数后，设备将被完全擦除。默认值为未定义。
  - 不活动后锁定设备：指定设备在锁定之前可以不活动的分钟数。将该值设置为 0 将禁用此策略。
  - 通行码有效期限 **(1 - 730** 天**)**：指定有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：指定要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
- 工作配置文件安全质询：要求用户完成安全质询才能访问 Android Enterprise 工作配置文件中运行的应用程序。适用于运行 Android 7.0 及更高版本的设备。当此设置设为开时，请配置工作配置文件安全质询的通行码要求和工作配置文件安全质询的通行码安全性下的设置。默认设置为关。
- 工作配置文件安全质询的通行码要求：
  - 最小长度：指定通行码的最小长度。默认值为 6。
  - 生物特征识别：启用生物特征识别。如果此设置设为开，则隐藏需含字符字段。默认值为关。
  - 需含字符：指定通行码所需的字符类型。在列表中，选择无限制、数字和字母、仅数字或仅字母。请仅对运行 Android 7.0 的设备使用无限制。Android 7.1 及更高版本不遵守无限制设置。默认值为数字和字母。
  - 高级规则：对可能出现在通行码中的字符类型应用高级规则。当此设置设为开时，请在数量下限和数量上限下配置设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为关。
  - 数量下限：
    - 符号：指定符号的最小数量。默认值为 **0**。
    - 字母：指定字母的最小数量。默认值为 **0**。
    - 小写字母：指定小写字母的最小数量。默认值为 **0**。
    - 大写字母：指定大写字母的最小数量。默认值为 **0**。
    - 数字或符号：指定数字或符号的最小数量。默认值为 **0**。
    - 数字：指定数字的最小数量。默认值为 **0**。
    - 更改的字符：适用于运行 Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。指定用户必须在以前的通行码中更改的字符数量。默认值为 **0**。
  - 数量上限：适用于运行 Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。
    - 字符可以出现的次数：指定某个字符可以在通行码中出现的最大次数。默认值为 **0**，这意味着没有上限。
    - 字母序列长度：指定通行码中字母序列的最大长度。默认值为 **0**，这意味着没有上限。
    - 数字序列长度：指定通行码中数字序列的最大长度。默认值为 **0**，这意味着没有上限。
- 工作档案安全挑战的密码复杂性（**Android 12+**）：
  - 应用密码复杂性：要求密码的复杂程度由平台定义，而不是自定义密码要求。仅适用于 Android 12+ 和

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使用 Secure Hub 22.9 或更高版本的设备。

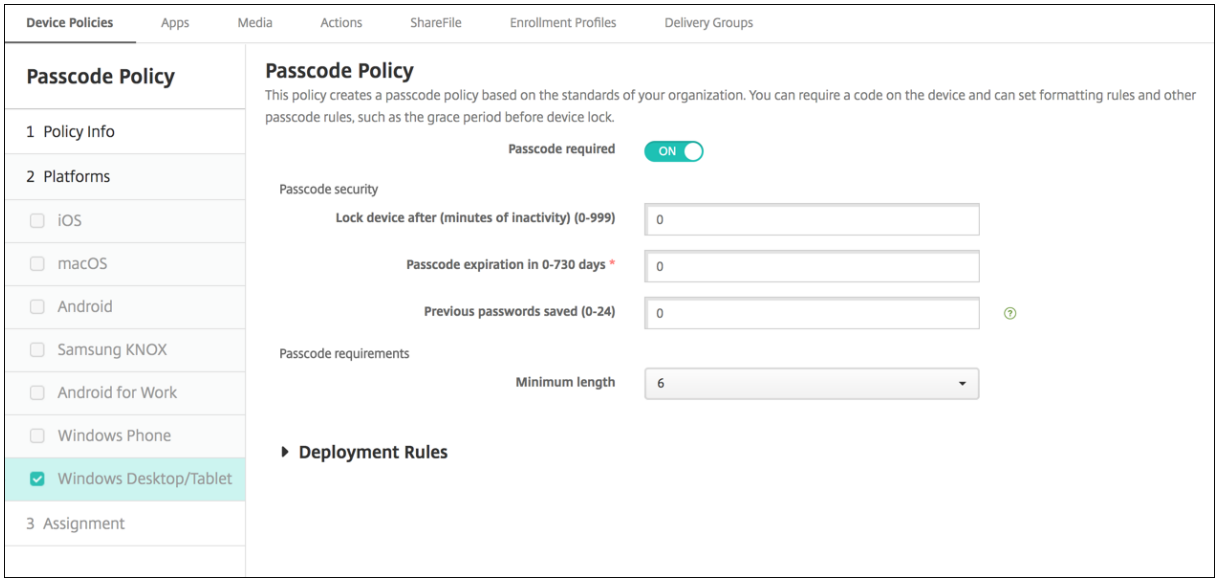
- 复杂程度：预定义的密码复杂程度。
  - 无：无需密码。
  - 低：密码可以是：
    - 一种模式
    - 至少包含四位数字的 PIN 码
  - 中：密码可以是：
    - 不包含重复序列 (4444) 或有序序列 (1234) 且至少有四位数字的 PIN 码
    - 按字母顺序，最少包含四个字符
    - 至少包含四个字符的字母数字
  - 高：密码可以是：
    - 不包含重复序列 (4444) 或有序序列 (1234) 且至少有八位数字的 PIN 码
    - 按字母顺序，最少包含六个字符
    - 至少包含六个字符的字母数字

      > 注意：
      >
      > 如果您为工作配置文件启用密码复杂性，则还必须为该设备启用该功能。

- 工作配置文件安全质询的通行码安全性
  - 此次数后擦除容器 **(**失败登录尝试次数**)**：指定用户可以登录失败的次数，超过此次数后，工作配置文件及其数据将从设备中擦除。擦除后，用户必须重新初始化工作配置文件。默认值为未定义。
  - **Lock container after inactivity**（不活动后锁定容器）：指定在锁定工作配置文件之前设备可以不活动的分钟数。该值可以介于 0 到 999 分钟之间。将该值设置为 0 将禁用此策略。
  - 通行码有效期限 **(1 - 730** 天**)**：指定有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：指定要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop/Tablet 设置



- 需要通行码：选择此选项将不要求提供 Windows Desktop/Tablet 设备的通行码。默认值为开，表示需要提供通行码。禁用此设置时，页面折叠，不再显示以下选项。
- 通行码安全
  - 不活动后锁定设备：键入设备在锁定之前可以不活动的分钟数。默认值为 **0**。
  - 通行码有效期限 **(0 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 0-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-24)**：键入要保存的使用过的通行码数量。用户无法使用在此列表中找到的任何通行码。有效值为 1-24。在此字段中输入介于 1 到 24 之间的数值。默认值为 **0**。
- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 **6**。

通行码锁定宽限期设备策略

March 31, 2022

“通行码锁宽限期” 设备策略适用于运行 iOS (iPadOS) 的共享设备。有关共用的 iPad 的详细信息，请参阅与 Apple 教育功能相集成。

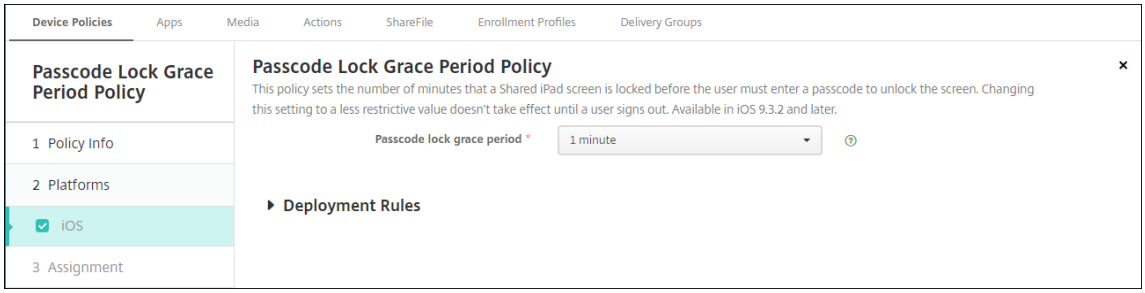
要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 通行码锁宽限期：共用的 iPad 屏幕保持锁定的分钟数，之后用户必须输入通行码才能解锁屏幕。将此设置更改为限制性较低的值在用户注销后才能生效。默认值为立即。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

默认情况下，共用的 iPad 在不活动两分钟后自动锁定自身。



个人热点设备策略

March 31, 2022

当用户不在 Wi-Fi 网络范围内，可以允许用户通过其 iOS 设备的个人热点功能，使用手机网络数据连接来连接到 Internet。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 禁用个人热点：选择是否在用户设备上禁用个人热点功能。默认值为关，表示在用户设备上关闭个人热点。此策略不禁用该功能。用户仍可以在其设备上使用个人热点，但是部署此策略后，将关闭个人热点功能，因此默认情况下不打开此功能。

电源管理设备策略

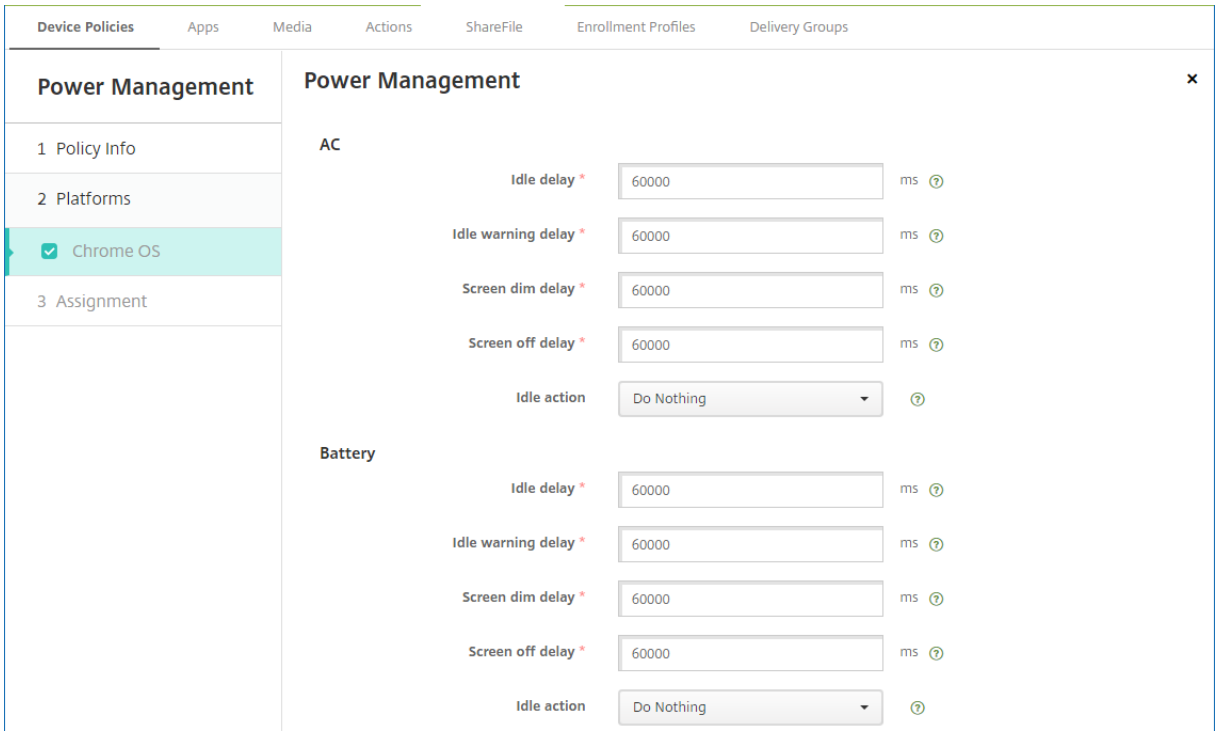
March 31, 2022

通过电源管理设备策略，您可以控制 Chrome OS 设备在使用交流电或电池电源时如何响应空闲时间。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Chrome OS 设置



以下设置针对交流电和电池显示。

- 空闲延迟：执行空闲操作之前无用户输入的时间长度。请以分钟为单位进行指定。交流电的默认值为 **60** 分钟。电池的默认值为 **10** 分钟。
- 空闲警告延迟：显示警告对话框之前无用户输入的时间长度。请以分钟为单位进行指定。交流电的默认值为 **58** 分钟。电池的默认值为 **8** 分钟（空闲延迟操作开始前 2 分钟）。
- 屏幕变暗延迟：屏幕变暗之前无用户输入的时间长度。请以分钟为单位进行指定。交流电的默认值为 **3** 分钟。电池的默认值为 **1** 分钟。
- 屏幕关闭延迟：关闭屏幕之前无用户输入的时间长度。请以分钟为单位进行指定。交流电的默认值为 **10** 分钟。电池的默认值为 **3** 分钟。
- 空闲操作：达到空闲延迟之后要执行的操作。选项包括挂起、注销、关机、不执行任何操作。默认值为挂起。

“配置文件删除”设备策略

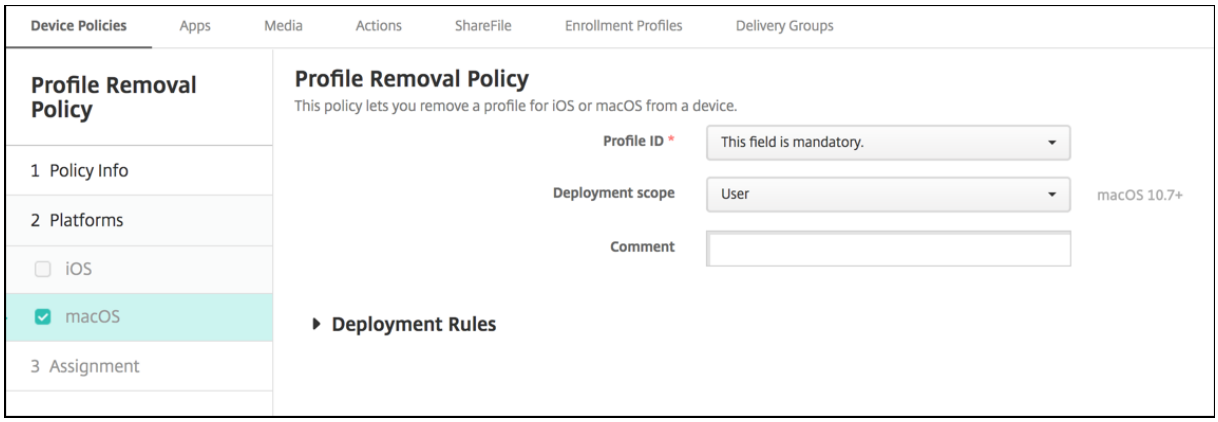
March 31, 2022

可以在 Endpoint Management 中创建应用程序配置文件删除设备策略。此策略在部署时，将从用户的 iOS 或 macOS 设备删除应用程序配置文件。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

macOS 设置



- 配置文件 **ID**：在列表中，单击应用程序配置文件 ID。此字段为必填字段。
- 部署范围：在列表中，单击用户或系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。
- 备注：键入可选备注。

预配配置文件设备策略

March 30, 2022

开发或代码签名 iOS 企业应用程序时，通常包含企业分发预配配置文件，Apple 需要此配置文件才能允许应用程序在 iOS 设备上运行。如果预配配置文件缺失或已过期，用户轻按应用程序以将其打开时，应用程序将崩溃。

预配配置文件的主要问题是，它们在 Apple 开发人员门户上生成一年之后将过期，您必须跟踪用户注册的所有 iOS 设备上的所有预配配置文件的过期日期。跟踪过期日期不仅涉及到跟踪实际的过期日期，还要跟踪每个用户正在使用的应用程序版本。两种解决方案分别为通过电子邮件将预配配置文件发送给用户或者将其置于 Web 门户中以供下载和安装。这些解决方案可行，但容易出错，因为需要用户响应电子邮件中的说明，或访问 Web 门户并下载正确的配置文件，然后再进行安装。

要使此过程对用户透明，您可以在 Endpoint Management 使用设备策略来安装和删除预配配置文件。在必要时删除缺失或过期的预配配置文件并在用户设备上安装最新的配置文件，这样一来，只需轻按应用程序，即可将其打开并使用。

创建预配配置文件策略之前，必须创建预配配置文件。有关详细信息，请参阅 Apple 在 Apple 开发人员站点上发布的关于如何创建开发预配配置文件的文章。

iOS 设置

- **iOS** 预配配置文件：单击浏览并导航到要导入的预配配置文件所在位置，选择此文件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

删除预配配置文件设备策略

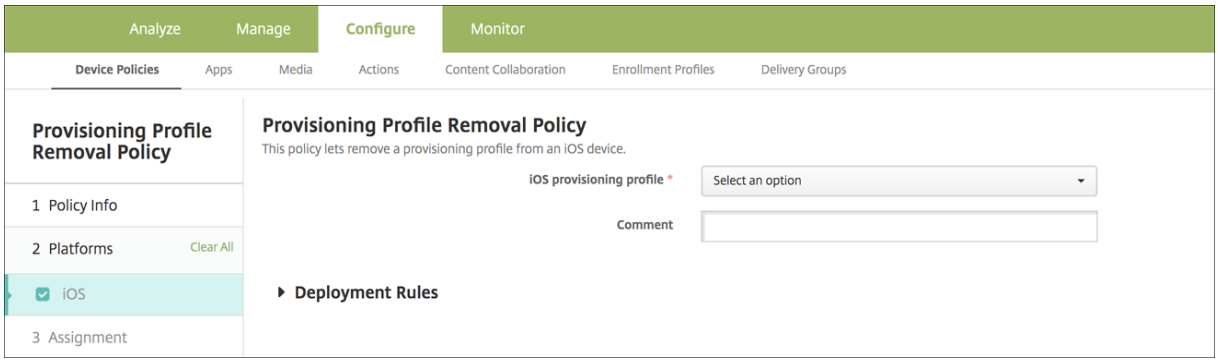
March 31, 2022

预配配置文件允许您将 iOS 应用程序分发到用户设备。Apple 要求您使用预配配置文件对应用程序进行签名，以授权该应用程序在 iOS 设备上运行。有关详细信息，请参阅预配配置文件设备策略。

要删除或替换较旧的预配配置文件，请使用“预配配置文件删除”设备策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- **iOS** 预配配置文件：在列表中，单击要删除的预配配置文件。
- 备注：（可选）添加备注。

代理设备策略

March 31, 2022

代理设备策略为支持的 iOS 设备指定全局 HTTP 代理设置。只能为每个设备部署一个全局 HTTP 代理策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

必备条件

在部署此策略之前，请务必将要为其设置全局 HTTP 代理的所有 iOS 设备设置为受监督模式。有关详细信息，请参阅使用 Apple Configurator 2 部署设备或通过 Apple 部署计划部署设备。

将代理策略发送到设备之前，设置部署规则以注册设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 设置

- 代理配置：单击手动或自动以设置在用户设备上配置代理的方式。
  - 如果单击手动，可以配置以下设置：
    - 代理服务器的主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
    - 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。
    - 用户名：键入向代理服务器进行身份验证的可选用户名。
    - 密码：键入向代理服务器进行身份验证的可选密码。
  - 如果单击自动，可以配置以下设置：
    - 代理 **PAC URL**：键入用于定义代理配置的 PAC 文件的 URL。
    - 允许在无法访问 **PAC** 时直接连接：选择是否允许用户在无法访问 PAC 文件时直接连接到目标。默认值为开。
- 允许旁路代理以访问俘获型网络：选择是否允许旁路代理以访问俘获型网络。默认值为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

公共会话设备策略

March 31, 2022

将 Chrome OS 设备配置为在不需要用户登录的公共会话中运行。相反，登录屏幕上将显示公共会话提示。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

部署公共会话设备

将公共会话策略分配给特定交付组，而非所有用户组。有关配置交付组的信息，请参阅部署资源。成功注册设备并注销后，“公共会话”和配置的显示名称将显示在登录屏幕上。

要从公共会话模式中删除设备，请执行以下操作：

1. 从交付组中删除策略。
2. 在管理 **>** 设备中，选择设备，然后单击部署。

   此操作将从设备中删除 Endpoint Management 策略。然后，您可以从控制台中删除设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Chrome OS 设置

- 公开会话
  - **Public session enabled**（已启用公共会话）：选择是启用还是禁用公共会话。需要 Google Workspace Chrome 配置。默认值为开。
  - 显示名称：键入要在设备的登录屏幕上显示的名称。
  - 会话持续时间 **(**分钟**)**：键入会话持续的分钟数。在这段时间之后，系统会将用户注销。默认值为 **60**。
- 安全性
  - 禁用隐身模式：不允许用户在隐身模式下浏览。默认值为开。
  - 显示主页按钮：允许用户在其浏览器中看到主页按钮。默认设置为关。
  - **Disable proceeding from the safe browsing warning page**（禁用从安全浏览警告页面继续操作）：不允许用户继续访问可能有害的站点。默认值为开。
  - **Safe browsing mode**（安全浏览模式）：打开安全浏览模式，在用户即将访问可能有害的站点时发出警告。默认设置为关。
  - **Disable saving browsing history**（禁用保存浏览历史记录）：不允许浏览器保存浏览历史记录或同步其他 Chrome OS 设备中的标签页。默认值为开。
  - **Disable deleting browsing and download history**（禁用删除浏览和下载历史记录）：不允许用户从其会话中删除浏览和下载历史记录。用户可以直接编辑或删除历史数据库文件。默认值为开。
  - **Disable bookmarks bar edit**（禁用书签栏编辑）：不允许用户编辑您配置的书签。默认值为开。
  - **External storage accessibility**（外部存储可访问性）：选择用户是否可以访问外部存储设备，例如 USB 驱动器。请在默认、只读或读写之间进行选择。默认值为已禁用。
  - 允许的 **Web** 站点：配置用户可以访问的 Web 站点列表。允许使用通配符表达式，例如 `http://*.citrix.com`。
  - 阻止的 **Web** 站点：配置用户无法访问的 Web 站点列表。允许使用通配符表达式。
- 内容
  - 主页设置：选择用户在主页上看到的内容。选项包括新建标签页和主页 **URL**。默认值为新建标签页。
  - **Pop-up default settings**（弹出窗口默认设置）：选择是否允许弹出窗口。默认值为允许弹出窗口。
  - **Pop-ups allowed from these sites**（允许来自这些站点的弹出窗口）：如果您阻止弹出窗口，则可以配置允许来自其中的弹出窗口的特定站点。
  - **Pop-ups not allowed from these sites**（不允许来自这些站点的弹出窗口）：如果允许弹出窗口，则可以配置阻止来自其中的弹出窗口的特定站点。
  - **Pages to load on startup**（启动时要加载的页面）：配置会话开始时要加载的 URL 列表。
- 书签
  - **Enable bookmarks bar**（启用书签栏）：如果设置为开，则会显示书签栏。默认值为开。
  - **Folder name**（文件夹名称）：键入书签文件夹的名称。
  - 书签：配置要显示的书签列表，包括名称和书签 URL。
- **Chrome** 应用程序
  - 允许安装的应用程序：选择用户是否可以安装应用程序。选项为允许、不允许或未指定。如果选择未指定，则会显示设备默认值。默认值为允许。
  - 还可以配置要允许或阻止的应用程序列表。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

* **App Name**（应用程序名称）：键入应用程序的名称。
* 应用程序 **ID**：键入应用程序的应用程序 ID。
* 允许安装的应用程序：选择此应用程序为允许、不允许还是未指定。默认值为允许。
* 已安装：如果设置为开，则应用程序将自动安装在设备上。默认设置为关。
* 已固定：如果设置为开，应用程序将固定到任务栏。默认设置为关。
* **URL**：键入应用程序 URL。
* 扩展策略：键入 JSON 参数或特定于您正在配置的应用程序的 URL。

限制设备策略

July 24, 2023

> 注意：
>
> 如果升级包含新的“限制”设备策略设置，则必须编辑并保存策略。Endpoint Management 在保存升级后的“限制”设备策略之后才部署升级的策略。

限制设备策略允许或限制用户设备上的某些特性或功能，例如相机。可以设置安全限制和媒体内容的限制。还可以设置关于用户能够安装和无法安装的应用程序类型的限制。大多数限制设置默认为开或允许。主要的例外情况是 iOS 安全 - 强制功能和所有 Windows Tablet 功能，其默认值为关或限制。

如果您为任何选项选择开，则意味着用户可以执行该操作或使用该功能。例如：

- 相机：如果设置为开，用户将可以使用其设备上的相机。如果设置为关，用户将无法在其设备上使用相机。
- 屏幕截图：如果设置为开，用户可以在其设备上拍摄屏幕截图。如果设置为关，则用户无法在其设备上拍摄屏幕截图。

如果您同时配置了限制设备策略和展台设备策略，则限制设备策略优先。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 设置

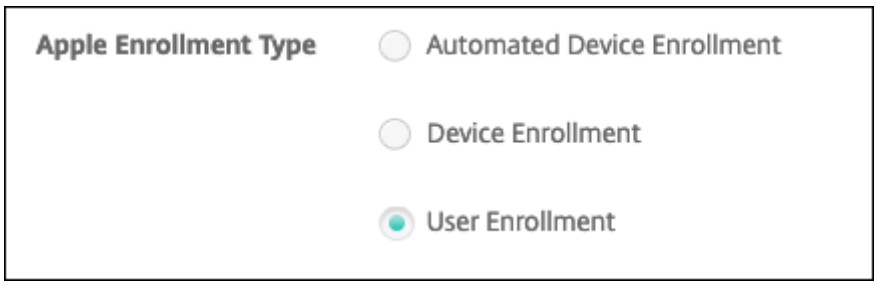


某些 iOS 限制策略设置仅适用于特定版本的 iOS，如此处和 Endpoint Management 控制台限制策略页面中所述。

当设备在用户注册模式、无监督（完全 MDM）模式或受监督模式下注册时，这些设置将适用。下表显示了适用于 iOS 13 及更高版本的每个设置的注册模式。

- **Automated Device Enrollment**（自动设备注册）：受监督的设备。这些是通过批量注册注册的设备。
- **Device Enrollment**（设备注册）：未受监督的设备。这些设备单独注册，整个设备完全进行 MDM。
- **User Enrollment**（用户注册）：仅托管特定用户的设备。有关用户注册的详细信息，请参阅 Apple 文档。

当设备在用户注册模式、未受监督（完全 MDM）模式或受监督模式下注册时，iOS 限制策略设置可能会适用。下表显示了适用于 iOS 13 及更高版本的每个限制策略设置的注册模式。



（Apple 注册类型）

如表中所示，自 iOS 13 起，以前在未受监督和监督模式下可用的某些设置仅在监督模式下可用。以下规则适用：

- 如果受监管的 iOS 13+ 设备在 Endpoint Management 中注册，这些设置将应用到该设备。
- 如果不受监督的 iOS 13+ 设备在 Endpoint Management 中注册，这些设置将不应用到该设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 如果 iOS 12（或更低版本）的设备已在 Endpoint Management 中注册，然后升级到 iOS 13，则不会发生任何变化。这些设置与升级之前一样应用到设备。

有关将 iOS 设备设置为受监督模式的信息，请参阅使用 Apple Configurator 2 部署设备。

设置	用户注册	不受监督	受监督
允许硬件控制			
相机	否	是	是
FaceTime	否	否	是
屏幕截图	是	否	是
允许“课堂”应用程序远程观察学生的屏幕	否	否	是
允许“课堂”应用程序运行 AirPlay 和查看屏幕而不提示	否	否	是
照片流	否	是	是
共享照片流	否	是	是
允许共用的 iPad 临时会话	否	否	是
语音拨号	否	是	是
Siri	是	是	是
设备锁定时允许	是	是	是
Siri 猥亵语言过滤器	否	否	是
安装应用程序	否	否	是
允许在漫游时执行全局后台获取	否	是	是
允许使用应用程序			
Apple App Store	否	否	是
应用内购买	否	是	是
所有购买均需使用 Apple App Store 密码	否	是	是
Safari	否	否	是
自动填充	否	否	是
强制显示欺诈警告	是	是	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	用户注册	不受监督	受监督
启用 JavaScript	否	是	是
阻止弹出窗口	否	是	是
接受 Cookie	否	是	是
网络 - 允许执行 **iCloud** 操作			
iCloud 文档和数据	否	否	是
iCloud 备份	否	是	是
iCloud 照片钥匙链	否	是	是
iCloud 照片库	否	是	是
安全 - 强制			
加密备份	是	是	是
有限广告跟踪	否	是	是
首次 AirPlay 配对时输入通行码	是	是	是
需要配对的 Apple Watch 才能使用腕部监测	是	是	是
使用 AirDrop 共享托管文档	是	是	是
安全 - 允许			
接受不可信 SSL 证书	否	是	是
自动更新证书信任设置	否	是	是
Require managed pasteboard（需要托管粘贴板）	是	是	是
在非托管应用程序中使用托管应用程序的文档	是	是	是
非托管应用程序读取托管联系人	否	否	是
托管应用程序写入非托管联系人	否	否	是
在托管应用程序中使用非托管应用程序的文档	是	是	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	用户注册	不受监督	受监督
诊断结果提交到 Apple	是	是	是
通过 Touch ID 解锁设备	否	是	是
锁定时接收 Wallet 通知	否	是	是
提交	否	是	是
托管应用程序的 iCloud 同步	是	是	是
企业书籍备份	是	是	是
企业书籍的笔记和重点同步	是	是	是
Spotlight 中的 Internet 结果	否	是	是
企业应用程序信任	否	是	是
仅监管设置 - 允许			
允许修改 eSIM	否	否	是
擦除所有内容和设置	否	否	是
屏幕时间	否	否	是
播客	否	否	是
安装配置文件	否	否	是
Touch ID and Face ID modification（Touch ID 和面容 ID 修改）	否	否	是
从设备安装应用程序	否	否	是
键盘快捷方式	否	否	是
已配对 Apple Watch	否	否	是
修改通行码	否	否	是
修改设备名称	否	否	是
修改壁纸	否	否	是
自动下载应用程序	否	否	是
AirDrop	否	否	是
iMessage	否	否	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	用户注册	不受监督	受监督
Siri 用户生成的内容	否	否	是
iBooks	否	否	是
删除应用程序	否	是	是
游戏中心	否	否	是
添加好友	否	否	是
多人游戏	否	否	是
修改帐户设置	否	否	是
修改应用程序手机网络数据设置	否	否	是
修改应用程序手机网络数据设置	否	否	是
Allow network drive connections（允许建立网络驱动器连接）	否	否	是
Allow USB device connections（允许使用 USB 设备连接）	否	否	是
Allow Find My Device（允许查找我的设备）	否	否	是
允许“查找我的好友”设置	否	否	是
修改“查找我的好友”设置	否	否	是
与非 Configurator 主机配对	否	否	是
预测键盘	否	否	是
键盘自动更正	否	否	是
键盘拼写检查	否	否	是
允许使用 QuickPath 键盘	否	否	是
定义查找	否	否	是
单应用程序捆绑 **ID**			
新闻	否	否	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	用户注册	不受监督	受监督
Apple 音乐服务	否	否	是
Apple 音乐	否	否	是
通知修改	否	否	是
受限应用程序使用	否	否	是
诊断提交修改	否	否	是
蓝牙修改	否	否	是
允许听写	否	否	是
修改 Wi-Fi 是打开还是关闭	否	否	是
仅加入由网络策略安装的 Wi-Fi 网络	否	否	是
允许“课堂”应用程序运行 AirPlay 和查看屏幕而不提示	否	否	是
允许“课堂”应用程序锁定到应用程序以及锁定设备而不提示	否	否	是
自动加入“课堂”应用程序课程而不提示	否	否	是
允许 AirPrint	否	否	是
允许在钥匙串中存储 AirPrint 凭据	否	否	是
允许使用 iBeacon 发现 AirPrint 打印机	否	否	是
仅允许通过 AirPrint 打印到证书受信任的目标打印机	否	否	是
添加 VPN 配置	否	否	是
修改手机网络套餐设置	否	否	是
删除系统应用程序	否	否	是
设置新的附近的设备	否	否	是
允许 USB 受限模式	否	否	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	用户注册	不受监督	受监督
强制延迟软件更新	否	否	是
强制执行的软件更新延迟	否	否	是
强制课堂申请离开课程的权限	否	否	是
在自动填充之前强制执行身份验证	否	否	是
强制自动填写日期和时间	否	否	是
密码自动填充	否	否	是
密码邻近请求	否	否	是
密码共享	否	否	是
允许修改个人热点	否	否	是
安全 **-** 在锁屏界面中显示			
控制中心	是	是	是
通知	是	是	是
“今天”视图	是	是	是
媒体内容 **-** 允许			
成人音乐、博客及 iTunes U 资料	否	否	是
iBooks 中暴露的性内容	否	是	是
评级地区	否	是	是
电影	否	是	是
电视节目	否	是	是
应用程序	否	是	是

- 允许硬件控制
  - 相机：允许用户在其设备上使用相机。
    - **FaceTime**：允许用户在其设备上使用 FaceTime。适用于受监督的 iOS 设备。
  - 屏幕截图：允许用户在其设备上截取屏幕截图。
    - 允许 **“课堂”** 应用程序远程观察学生的屏幕：如果未选中此限制，教师将无法使用“课堂”应用程序远程观察学生的屏幕。默认设置为选中，教师可以使用“课堂”应用程序观察学生的屏幕。允许 **“课堂”** 应用程序运行 **AirPlay** 和查看屏幕而不提示的设置确定学生是否接收向教师授予权限的提示。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

适用于受监督的 iOS 设备。

* 允许 **“课堂”** 应用程序运行 **AirPlay** 和查看屏幕而不提示：如果选中此限制，教师可以在学生的设备上执行 AirPlay 和查看屏幕操作，而不提示授予权限。默认设置为未选中。适用于受监督的 iOS 设备。

- 照片流：允许用户使用 MyPhotoStream 通过 iCloud 与其所有 iOS 设备共享照片。
- 共享照片流：允许用户使用 iCloud Photo Sharing 与同事、朋友和家人共享照片。
- **Allow shared iPad temporary session**（允许共享 iPad 临时会话）：阻止访问共享 iPad 上的临时会话。
- 语音拨号：在用户设备上启用拨号。
- **Siri**：允许用户使用 Siri。
  * 设备锁定时允许：允许用户在其设备锁定时使用 Siri。
  * **Siri** 猥亵语言过滤：启用 Siri 猥亵语言过滤。默认为限制此功能，也就是说不会进行猥亵语言过滤。有关 Siri 和安全性的详细信息，请参阅 Siri 和听写策略。
- 安装应用程序：允许用户安装应用程序。适用于受监督的 iOS 设备。
- 允许在漫游时执行全局后台获取：允许设备在漫游时自动向 iCloud 同步邮件帐户。设置为关时，在 iOS 手机漫游时将禁用全局后台获取活动。默认值为开。

- 允许使用应用程序
  - **Apple App Store**：允许用户访问 Apple App Store。适用于受监督的 iOS 设备。
  - 应用程序内购买：允许用户进行应用程序内购买。
    * 所有购买均需使用 **Apple App Store** 密码：需要密码才能进行应用程序内购买。默认为限制此功能，也就是说进行应用程序内购买无需密码。
  - **Safari**：允许用户访问 Safari。适用于受监督的 iOS 设备。
    * 自动填充：允许用户在 Safari 上设置用户名和密码自动填充功能。
    * 强制显示欺诈警告：如果启用此设置，则当用户访问可疑网络钓鱼 Web 站点时，Safari 会向用户发出警报。默认为限制此功能，也就是说不会发出警报。
    * 启用 **JavaScript**：允许在 Safari 上运行 JavaScript。
    * 阻止弹出窗口：查看 Web 站点时阻止弹出窗口。默认为限制此功能，也就是说不阻止弹出窗口。
  - 接受 **Cookie**：设置为接受 Cookie 的程度。在列表中，选择某个选项以允许或限制 Cookie。默认选项为总是，即允许所有 Web 站点在 Safari 中保存 Cookie。其他选项为仅限当前 **Web** 站点、从不和仅来自访问的 **Web** 站点。

- 网络 **-** 允许执行 **iCloud** 操作
  - **iCloud** 文档和数据：允许用户将文档和数据同步到 iCloud。适用于受监督的 iOS 设备。
  - **iCloud** 备份：允许用户向 iCloud 备份其设备。
  - **iCloud** 钥匙串：允许用户在 iCloud 钥匙串中存储密码、Wi-Fi 网络信息、信用卡信息以及其他信息。
  - 云照片库：允许用户访问其 iCloud 照片库。

- 安全 **-** 强制

  默认为限制以下功能，即不启用任何安全功能。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 加密备份：强制加密到 iCloud 的备份。
- 有限广告跟踪：阻止有针对性的广告跟踪。
- 首次 **AirPlay** 配对时输入通行码：需要使用屏幕上显示的一次性代码验证已启用 AirPlay 的设备才可以使用 AirPlay。
- 需要配对的 **Apple Watch** 才能使用腕部监测：需要配对的 Apple Watch 才能使用腕部监测。
- 使用 **AirDrop** 共享托管文档：将此选项设置为开会使 AirDrop 显示为非托管放置目标。

- 安全 **-** 允许
  - 接受不可信 **SSL** 证书：允许用户接受 Web 站点的不可信 SSL 证书。
  - 自动更新证书信任设置：允许自动更新可信证书。
  - **Require managed pasteboard**（需要托管粘贴板）：允许复制和粘贴功能遵循应用到在非托管应用程序中使用托管应用程序中的文档和在托管应用程序中使用非托管应用程序中的文档的相同限制。
    例如，配置以下各项：
    * **Require managed pasteboard**（需要托管粘贴板）：开
    * 在非托管应用程序中使用托管应用程序中的文档：关
    * 在托管应用程序中使用非托管应用程序中的文档：开
      将策略部署到 iOS 设备后，用户无法将数据从托管应用程序复制并粘贴到非托管应用程序，但可以将数据从非托管应用程序复制并粘贴到托管应用程序。
  - 在非托管应用程序中使用托管应用程序中的文档：允许用户将托管（企业）应用程序中的数据移动到非托管（私人）应用程序。
  - 在托管应用程序中使用非托管应用程序中的文档：允许用户将非托管（私人）应用程序中的数据移动到托管（企业）应用程序。
  - 将诊断结果提交给 **Apple**：允许将有关用户设备的匿名诊断数据发送给 Apple。
  - **Touch ID or Face ID to unlock device**（通过 Touch ID 或面容 ID 解锁设备）：允许用户使用 Touch ID 或面容 ID 解锁其设备。
  - **Wallet notifications when locked**（锁定时接收 Wallet 通知）：允许 Wallet 通知显示在锁屏界面上。
  - **Handoff**：允许用户从一台 iOS 设备向附近的另一台 iOS 设备转移活动。
  - 托管应用程序的 **iCloud** 同步：允许用户向 iCloud 同步托管应用程序。
  - 企业通讯簿备份：允许将企业通讯簿备份到 iCloud。
  - 企业书籍的笔记和重点同步：允许用户添加到企业书籍的笔记和重点同步到 iCloud。
  - 企业应用程序信任：允许信任企业应用程序。企业应用程序是指为贵组织自定义的任何应用程序。这些产品可以在内部开发，也可以从外部供应商处开发并购买。有关其他信息，请参阅 Install custom enterprise apps on iOS（在 iOS 上安装自定企业级应用）。
  - **Spotlight** 中的 **Internet** 结果：允许 Spotlight 显示来自 Internet 以及设备的搜索结果。
  - 非托管应用程序读取托管联系人：可选。仅当非托管应用程序中来自托管应用程序的文档处于禁用状态时才可用。如果启用，则非托管应用程序可以读取托管帐户的联系人数据。默认设置为关。截至 iOS 12 适用。
  - 托管应用程序写入非托管联系人：可选。如果启用，则允许托管应用程序将联系人写入非托管帐户的联系人。如果非托管应用程序中来自托管应用程序的文档处于启用状态，则此限制无效。默认设置为关。截至 iOS 12 适用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 仅监管设置 **-** 允许

  这些设置仅适用于受监管设备。有关将 iOS 设备设置为受监督模式的步骤，请参阅使用 Apple Configurator 2 部署设备。

  - 允许修改 **eSIM**：允许用户更改其设备上的 eSIM 设置。
  - 擦除所有内容和设置：允许用户擦除其设备中的所有内容和设置。
  - 屏幕时间：允许用户启用“屏幕时间”。
  - 播客：允许用户下载和同步播客。
  - 安装配置文件：允许用户安装并非由您部署的配置文件。
  - **Touch ID and Face ID modification**（Touch ID 和面容 ID 修改）：允许用户更改或删除其 Touch ID 或面容 ID。
  - 从设备安装应用程序：允许用户安装应用程序。禁用此设置将阻止最终用户安装新应用程序。App Store 处于禁用状态，其图标将从主屏幕中删除。
  - 键盘快捷方式：允许用户为其常用的字词或短语创建自定义键盘快捷方式。
  - 配对的 **Apple Watch**：允许用户将 Apple Watch 与受监督的设备配对。
  - 修改通行码：允许用户在受监督的设备上更改通行码。
  - 修改设备名称：允许用户更改其设备的名称。
  - 修改壁纸：允许用户在更改其设备上的壁纸。
  - 自动下载应用程序：允许下载应用程序。
  - **AirDrop**：允许用户与附近的 iOS 设备共享照片、视频、Web 站点、位置及其他信息。
  - **iMessage**：允许用户使用 iMessage 通过 Wi-Fi 传递文本消息。
  - **Siri** 用户生成的内容：允许 Siri 从 Web 查询用户生成的内容。用户，而非传统新闻记者；生成用户生成的内容。例如，在 Twitter 或 Facebook 上找到的内容是用户生成的。
  - **iBooks**：允许用户使用 iBooks 应用程序。
  - 删除应用程序：允许用户从其设备中删除应用程序。
  - 游戏中心：允许用户在其设备上通过游戏中心在线玩游戏。
    - 添加好友：允许用户向好友发送玩游戏通知。
    - 多人游戏：允许用户在其设备上启动多人游戏。
  - 修改帐户设置：允许用户修改其设备帐户设置。
  - 修改应用程序手机网络数据设置：允许用户修改使用手机网络数据的方式。
  - **Allow network drive connections**（允许建立网络驱动器连接）：阻止连接到“文件”应用程序中的网络驱动器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Allow USB device connections**（允许建立 USB 设备连接）：阻止连接到“文件”应用程序中的任何已连接的 USB 设备。
- **Allow Find My Device**（允许查找我的设备）：禁用“Find My app”（查找我的应用程序）中的 **Find My Device**（查找我的设备）选项。
- **Allow Find My Friends settings**（允许“查找我的好友”设置）：禁用“查找我的好友”应用程序中的查找我的好友选项。
- 修改**“**查找我的好友**”**设置：允许用户更改其“查找我的好友”设置。
- 与非配置器主机配对：允许管理员控制用户设备可以与哪些设备配对。禁用此设置将阻止配对，与运行 Apple Configurator 的监督主机配对除外。如果未配置任何监督主机证书，将禁用所有配对。
- 预测键盘：允许用户设备使用预测键盘，在用户键入时提供建议单词。如果要管理标准化测试，不允许用户访问建议的单词，在此类情况下可以禁用此选项。
- 键盘自动更正：允许用户设备使用键盘自动更正。如果要管理标准化测试，不允许用户访问自动更正，在此类情况下可以禁用此选项。
- 键盘拼写检查：在键入时允许用户设备使用拼写检查。如果要管理标准化测试，不允许用户访问拼写检查，在此类情况下可以禁用此选项。
- 定义查找：在键入时允许用户设备使用定义查找。如果要管理标准化测试，不允许用户在键入时查找定义，在此类情况下可以禁用此选项。
- 单个应用程序捆绑 **ID**：创建允许保留对设备的控制权并防止与其他应用或功能交互的应用程序列表。
  要添加应用程序，请单击添加，键入应用程序名称，然后单击保存。对要添加的每个应用程序重复该过程。
- 新闻：允许用户使用新闻应用程序。
- **Apple** 音乐服务：允许用户使用 Apple 音乐服务。如果您不允许使用 Apple 音乐服务，则音乐应用程序以经典模式运行。
- **Apple** 音乐：允许用户使用 Apple 音乐。
- 修改通知：允许用户修改通知设置。
- 受限应用程序使用：允许用户使用所有应用程序或者使用或不使用某些应用程序，具体取决于您提供的捆绑包 ID。仅适用于受监督的设备。如果选择仅允许某些应用程序，请添加捆绑包 ID 为 `com.apple.webapp` 的应用程序以允许 Web 剪辑。

  > 注意：
  >
  > 自 iOS 11 起，Apple 引入了对适用于应用程序限制的策略所做的更改。Apple 不再允许您通过限制适当的 iOS 应用程序包来删除对“设置”应用程序和“电话”应用程序的访问权限。

  配置限制设备策略以阻止某些应用程序，然后部署了该策略之后：如果以后要允许这些应用程序中的一些或全部，更改并部署限制设备策略不会更改显示。在这种情况下，iOS 不会将更改应用于 iOS 配置文件。要继续操作，请使用配置文件删除策略删除 iOS 配置文件，然后部署更新的限制设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

如果将此设置更改为仅允许某些应用程序：部署此策略之前，建议使用 Apple 部署计划注册的设备的用户从设置助理登录其 Apple 帐户。否则，用户可能必须在其设备上禁用双重身份验证，才能登录其 Apple 帐户并访问允许的应用程序。

- 修改诊断提交：允许用户在设置 **> Diagnostics & Usage**（诊断和使用）窗格中修改诊断提交和应用程序分析设置。
- 修改蓝牙：允许用户修改蓝牙设置。
- 允许听写：仅在监督下使用。如果此限制设置为关，则不允许听写输入，包括语音转换为文本。默认设置为 开。
- **Modify whether Wi-Fi is on or off**（修改 Wi-Fi 是打开还是关闭）：阻止在“设置”或“控制中心”中打开或关闭 Wi-Fi。进入飞行模式也没有任何影响。此限制并不妨碍选择要使用的 Wi-Fi 网络。
- 仅加入由网络策略安装的 **Wi-Fi** 网络：可选。仅在监督下使用。如果此限制设置为开，则仅在 Wi-Fi 网络是通过配置文件设置的情况下设备才能加入这些网络。默认设置为关。
- 允许 **“**课堂**”** 应用程序运行 **AirPlay** 和查看屏幕而不提示：如果选中此限制，教师可以在学生的设备上执行 AirPlay 和查看屏幕操作，而不提示授予权限。默认设置为未选中。适用于受监督的 iOS 设备。
- 允许 **“**课堂**”** 应用程序锁定到应用程序以及锁定设备而不提示：如果此限制设置为开，“课堂”应用程序会自动将用户设备锁定到某个应用程序并锁定设备，而不提示用户。默认设置为关。适用于运行 iOS 11（最低版本）的受监督设备。
- 自动加入 **“**课堂**”** 应用程序课程而不提示：如果此限制设置为开，“课堂”应用程序会自动将用户加入到课程中，而不提示用户。默认设置为关。适用于运行 iOS 11（最低版本）的受监督设备。
- 允许 **AirPrint**：如果此限制设置为关，用户将无法通过 AirPrint 打印。默认设置为 开。此限制设置为开时，将显示这些额外的限制。适用于运行 iOS 11（最低版本）的受监督设备。
  - 允许在钥匙串中存储 **AirPrint** 凭据：如果未选中此限制，AirPrint 用户名和密码将不存储在钥匙串中。默认设置为选中。适用于运行 iOS 11（最低版本）的受监督设备。
  - 允许使用 **iBeacon** 发现 **AirPrint** 打印机：如果未选中此限制，则禁止 iBeacon 发现 AirPrint 打印机。此设置将阻止虚假 AirPrint 蓝牙信标对网络流量进行网络钓鱼。默认设置为选中。适用于运行 iOS 11（最低版本）的受监督设备。
  - 仅允许通过 **AirPrint** 打印到证书受信任的目标打印机：如果选中此限制，用户可以使用 AirPrint 仅打印到证书受信任的目标打印机。默认设置为未选中。适用于运行 iOS 11（最低版本）的受监督设备。
- 添加 **VPN** 配置：如果此限制设置为关，用户将无法创建 VPN 配置。默认设置为 开。适用于运行 iOS 11（最低版本）的受监督设备。
- 修改手机网络套餐设置：如果此限制设置为关，用户将无法修改手机网络套餐设置。默认设置为 开。适用于运行 iOS 11（最低版本）的受监督设备。
- 删除系统应用程序：如果此限制设置为关，用户将无法从其设备中删除系统应用程序。默认设置为 开。适用于运行 iOS 11（最低版本）的受监督设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 设置新的附近的设备：如果此限制设置为“关”，用户将无法设置新的附近的设备。默认设置为开。适用于运行 iOS 11（最低版本）的受监督设备。
- 允许 **USB** 受限模式：如果设置为关，设备在锁定状态下可以始终连接到 USB 附属设施。默认值为开。仅适用于 iOS 11.3 及更高版本的受监督设备。
- 强制延迟软件更新：如果 开启，则延迟用户对软件更新的可见性。设置此限制后，用户在软件更新发布日期后的指定天数之后才能看到软件更新。默认设置为关。仅适用于 iOS 11.3 及更高版本的受监督设备。操作系统更新策略包含用于控制设备接收更新的频率的更多设置。请参阅“操作系统更新”设备策略。
- 强制执行的软件更新延迟 **(**天**)**：允许您指定在设备上延迟软件更新的天数。最长延迟时间为 **90** 天。默认值为 **30** 天。仅适用于 iOS 11.3 及更高版本的受监督设备。
- 强制课堂申请离开课程的权限：如果设置为开，通过“课堂”应用程序在非托管课程中注册的学生在尝试离开课程时将向教师申请权限。默认设置为关。仅适用于 iOS 11.3 及更高版本的受监督设备。
- **Force authentication before autofill**（在自动填充之前强制执行身份验证）：强制用户在使用自动填充功能之前进行身份验证。
- 强制自动填写日期和时间：允许您在受监督设备上自动设置日期和时间。如果 开启，设备用户将无法清除常规 **>** 日期和时间下的 自动设置。仅当设备可以确定其位置时，设备上的时区才会更新。也就是说，当设备启用了手机网络连接或启用了带定位服务的 Wi-Fi 连接时。默认设置为关。仅适用于 iOS 12 及更高版本的受监督设备。
- 密码自动填充：可选。如果禁用，用户将无法使用“自动填充密码”或“自动使用强密码”功能。默认值为开。截至 iOS 12 适用。
- 密码邻近请求：可选。如果禁用，用户的设备将不从附近的设备请求密码。默认值为开。截至 iOS 12 适用。
- 密码共享：可选。如果禁用，用户将无法使用“AirDrop 密码”功能共享其密码。默认值为开。截至 iOS 12 适用。
- **Allow personal hotspot modification**（允许修改个人热点）：阻止用户更改个人热点设置。

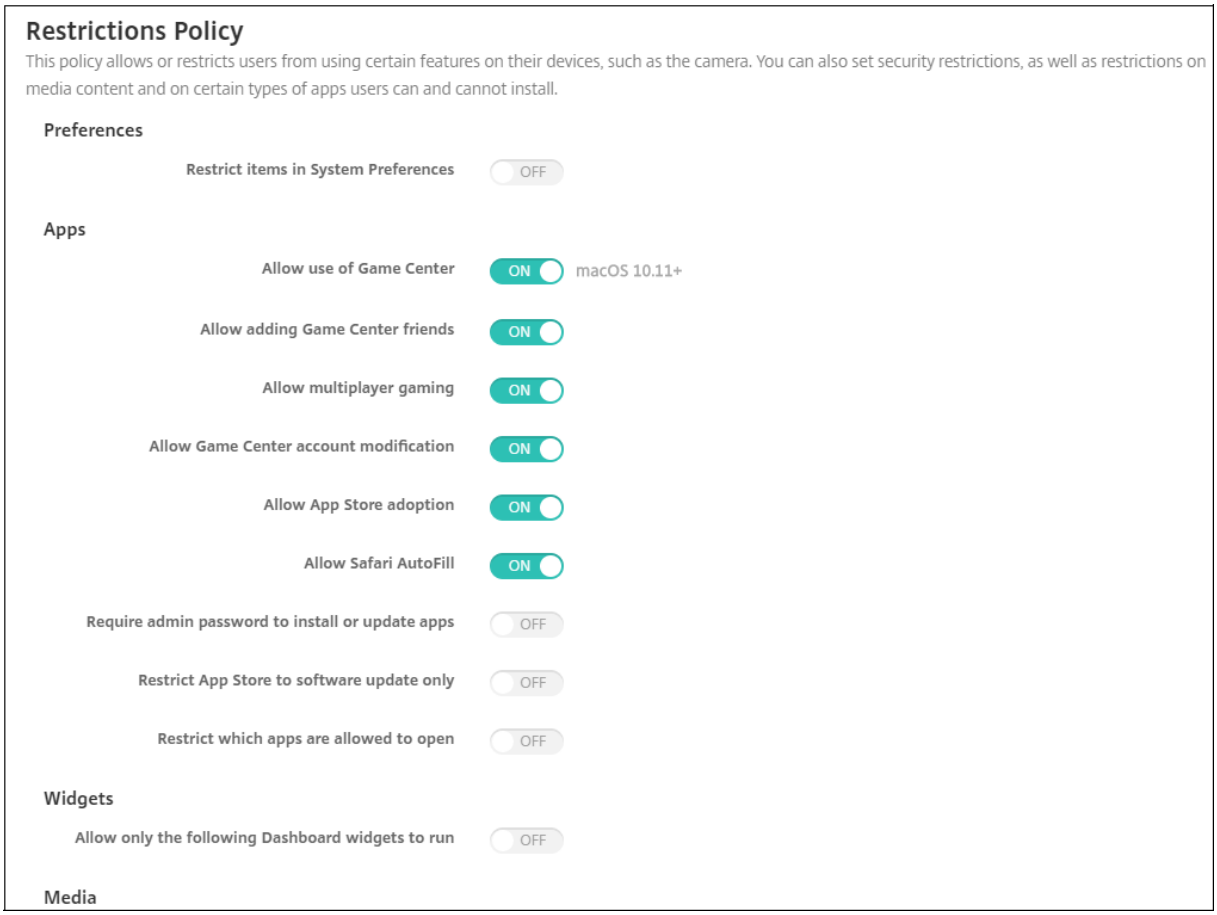
- 安全 **-** 在锁屏界面中显示
  - 控制中心：允许访问锁屏界面上的控制中心。控制中心允许用户轻松修改飞行模式、Wi-Fi、蓝牙、请勿打扰模式和锁定旋转设置。
  - 通知：允许在锁屏界面上显示通知。
  - **“**今天**”** 视图：允许在锁屏界面上显示“今天”视图，此视图汇总了天气及当天的日历项目等信息。
- 媒体内容 **-** 允许
  - 成人音乐、博客及 **iTunes U** 资料：允许用户设备上出现成人资料。
  - **iBooks** 中暴露的性内容：允许从 iBooks 下载成人资料。
  - 评分地区：设置从其获得家长控制评分的地区。在列表中，单击某个国家/地区以设置评分地区。默认值为美国。
  - 电影：设置是否允许在用户设备上播放电影。如果允许播放电影，可以选择为电影设置评分级别。在列表中，单击某个选项以允许或限制在设备上播放电影。默认值为“允许所有电影”。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 电视节目：设置是否允许在用户设备上播放电视节目。如果允许播放电视节目，可以选择为电视节目设置评分级别。在列表中，单击某个选项以允许或限制在设备上播放电视节目。默认值为“允许所有电视节目”。
- 应用程序：设置是否允许在用户设备上使用应用程序。如果允许使用应用程序，可以选择为应用程序设置评分级别。在列表中，单击某个选项以允许或限制在设备上使用应用程序。默认值为“允许所有应用程序”。

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅适用于 iOS 9.3 及更高版本。

macOS 设置



设置	不受监督	受监督
应用程序		
允许使用游戏中心	否	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	不受监督	受监督
允许添加游戏中心好友	否	是
允许多人游戏	否	是
允许修改游戏中心帐户	是	是
允许应用商店采用	是	是
允许 Safari 自动填充	否	是
需要提供管理员密码才能安装或更新应用程序	是	是
将应用商店限制为仅提供软件更新	是	是
限制允许打开的应用程序	是	是
媒体		
允许 AirDrop	否	是
功能		
锁定桌面图片	否	是
允许使用相机	否	是
允许 Apple 音乐	否	是
允许 Spotlight 推荐	是	是
允许查找	是	是
允许使用本地帐户的 iCloud 密码	是	是
允许 iCloud 文档和数据	是	是
允许 iCloud 桌面和文档	否	是
允许 iCloud 钥匙串同步	否	是
允许 iCloud 邮件	是	是
允许 iCloud 通讯录	是	是
允许 iCloud 日历	是	是
允许 iCloud 提醒事项	是	是
允许 iCloud 书签	是	是
允许 iCloud 备忘录	是	是
允许 iCloud 照片	是	是
允许自动解锁	是	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	不受监督	受监督
允许 Touch ID 解锁 Mac	是	是
强制延迟软件更新	否	是
密码自动填充	否	是
密码邻近请求	否	是
密码共享	是	是

- 首选项
  - 限制系统首选项中的项目：允许或限制用户访问系统首选项。默认值为关，表示完全允许用户访问系统首选项。如果启用，可以配置以下设置。
    - 系统首选项窗格：选择是启用还是禁用选择的设置。默认为启用所有设置，即默认情况下为开。
      - 用户和组
      - 常规
      - 辅助工具
      - App Store
      - 软件更新
      - 蓝牙
      - CD 和 DVD
      - 日期和时间
      - 桌面和屏幕保护程序
      - 显示
      - 基站
      - 节能程序
      - 扩展
      - 光纤通道
      - iCloud
      - Ink
      - Internet 帐户
      - 键盘
      - 语言和文字
      - Mission Control
      - 鼠标
      - 网络
      - 通知
      - 家长控制
      - 打印机和扫描仪
      - 配置文件

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 安全和隐私
- 共享
- 声音
- 听写和语音
- Spotlight
- 启动磁盘
- Time Machine
- 触控板
- Xsan

- 应用程序
  - 允许使用游戏中心：允许用户通过游戏中心在线玩游戏。默认值为开。
  - 允许添加游戏中心好友：允许用户向好友发送玩游戏通知。默认值为开。
  - 允许多人游戏：允许用户发起多人游戏。默认值为开。
  - 允许修改游戏中心帐户：允许用户修改其游戏中心帐户设置。默认值为开。
  - 允许应用商店采用：允许或限制应用商店采用 OS X 中预先存在的应用程序。默认设置为开。
  - 允许 **Safari** 自动填充：允许 Safari 自动使用其存储的密码、地址和其他基本信息填充 Web 站点上的字段。默认值为开。
  - 需要提供管理员密码才能安装或更新应用程序：需要提供管理员密码才能安装或更新应用程序。默认值为关，表示无需提供管理员密码。
  - 将应用商店限制为仅提供软件更新：将应用商店限制为仅提供更新，这样会在应用商店中禁用除“更新”之外的所有选项卡。默认值为关，即允许完整的应用商店访问。
  - 限制允许打开的应用程序：限制或允许用户可以使用的应用程序。默认值为“关”，表示所有应用程序均可以使用。如果启用，请配置以下设置：
    * 允许运行的应用程序：单击添加，输入允许启动的应用程序的名称和捆绑包 ID，然后单击保存。对于 Citrix 移动生产力应用程序，请在添加应用程序时使用软件包 **ID** 字段中的 ID。请对允许启动的每个应用程序重复此步骤。
    * 不允许使用的文件夹：单击添加，键入要限制用户访问的文件夹的文件路径（例如，/Applications/Utilities），然后单击保存。为不希望用户访问的所有文件夹重复此步骤。
    * 允许使用的文件夹：单击添加，键入要允许用户访问的文件夹的文件路径，然后单击保存。为希望用户可以访问的所有文件夹重复此步骤。
- 小组件
  - 只允许运行以下仪表板小组件：如果启用，则用户只能运行在此设置中配置的仪表板小组件。默认值为关，表示允许用户运行所有小组件。如果启用，可以配置以下设置：
    * 允许运行的小组件：单击添加，键入允许运行的小组件的名称和 ID，然后单击保存。为希望在控制板上运行的每个小组件重复执行此步骤。
- 媒体
  - 允许 **AirDrop**：允许用户与附近的 iOS 设备共享照片、视频、Web 站点、位置及其他信息。
- 共享
  - 自动启用新共享服务：选择是否自动启用共享服务。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 邮件：选择是否允许使用共享的邮箱。
  - **Facebook**：选择是否允许使用共享的 Facebook 帐户。
  - 视频服务 **- Flickr**、**Vimeo**、**Tudou** 和 **Youku**：选择是否允许使用共享的视频服务。
  - 添加到 **Aperture**：选择是否允许将共享功能添加到 Aperture。
  - 新浪微博：选择是否允许共享的新浪微博账户。
  - **Twitter**：选择是否允许使用共享的 Twitter 帐户。
  - 消息：选择是否允许对消息进行共享访问。
  - 添加到 **iPhoto**：选择是否允许将共享功能添加到 iPhoto。
  - 添加到阅读列表：选择是否允许将共享功能添加到阅读列表。
  - **AirDrop**：选择是否允许使用共享的 AirDrop 帐户。
- 功能
  - 锁定桌面图片：选择用户是否可以更改桌面图片。默认值为关，表示用户可以更改桌面图片。
  - 允许使用相机：选择用户是否可以在其 Mac 上使用相机。默认值为关，表示用户无法使用相机。
  - 允许 **Apple** 音乐：允许用户使用 Apple 音乐服务（macOS 10.12 及更高版本）。如果您不允许使用 Apple 音乐服务，则音乐应用程序以经典模式运行。仅适用于受监督的设备。默认值为开。
  - 允许 **Spotlight** 推荐：选择用户是否可以使用 Spotlight 推荐搜索其 Mac 并提供来自 Internet 和 App Store 的 Spotlight 推荐。默认值为关，表示阻止用户使用 Spotlight 推荐。
  - 允许查找：选择用户是否可以使用上下文菜单或 Spotlight 搜索菜单查找字词的定义。默认值为 “关”，表示阻止用户在其 Mac 上使用查找。
  - 允许使用本地帐户的 **iCloud** 密码：选择用户是否可以使用其 Apple ID 和 iCloud 密码登录其 Mac。启用此策略意味着用户对其 Mac 上的所有登录屏幕仅使用一个 ID 和密码。默认值为开，表示允许用户使用其 Apple ID 和 iCloud 密码访问其 Mac。
  - 允许使用 **iCloud** 文档和数据：选择是否允许用户在其 Mac 上访问存储在 iCloud 上的文档和数据。默认值为开，表示阻止用户在其 Mac 上使用 iCloud 文档和数据。
    * 允许 **iCloud** 桌面和文档：（macOS 10.12.4 及更高版本）默认选中。
  - 允许 **iCloud** 钥匙串同步：允许 iCloud 钥匙串同步（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 邮件：允许用户使用 iCloud 邮件（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 通讯录：允许用户使用 iCloud 通讯录（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 日历：允许用户使用 iCloud 日历（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 提醒事项：允许用户使用 iCloud 提醒事项（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 书签：允许用户与 iCloud 书签同步（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 备忘录：允许用户使用 iCloud 备忘录（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 照片：如果将此设置更改为关，未完全从 iCloud 照片库中下载的所有照片都将从本地设备存储中删除（macOS 10.12 及更高版本）。默认值为开。
  - 允许自动解锁：有关此选项及 Apple Watch 的信息，请参阅 https://www.imore.com/auto-unlock（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **Touch ID** 解锁 **Mac**：（macOS 10.12.4 及更高版本）。默认值为开。
  - 强制延迟软件更新：如果启用，则此设置 会延迟用户对软件更新的可见性。用户在软件更新发布日期后的指定天数之后才能看到软件更新。默认设置为关。仅适用于运行 macOS 10.13.4 及更高版本的受监督设

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

备。操作系统更新策略包含用于控制设备接收更新的频率的更多设置。请参阅“操作系统更新”设备策略。

- 强制执行的软件更新延迟 **(**天**)**：指定在设备上延迟软件更新的天数。最大值为 90 天。默认值为 **30**。仅适用于运行 macOS 10.13.4 及更高版本的受监督设备。
- 密码自动填充：可选。如果禁用，用户将无法使用“自动填充密码”或“自动使用强密码”功能。默认值为开。（macOS 10.14 及更高版本）
- 密码邻近请求：可选。如果禁用，用户的设备将不从附近的设备请求密码。默认值为开。（macOS 10.14 及更高版本）
- 密码共享：可选。如果禁用，用户将无法使用“AirDrop 密码”功能共享其密码。默认值为开。（macOS 10.14 及更高版本）

tvOS 设置

- 安全性和媒体设置 **-** 允许
  - 首次 **AirPlay** 配对时输入通行码：需要使用屏幕上显示的一次性代码验证已启用 AirPlay 的设备才可以使用 AirPlay。
  - **iBooks** 中暴露的性内容：允许从 iBooks 下载成人资料。
  - 成人音乐、博客及 **iTunes U** 资料：允许用户设备上出现成人资料。
  - 应用程序内购买：允许用户进行应用程序内购买。
    - 所有购买均需使用 **Apple App Store** 密码：需要密码才能进行应用程序内购买。默认为限制此功能，也就是说进行应用程序内购买无需密码。
- 仅监管设置 **-** 允许
  - 修改设备名称：允许用户更改其设备的名称。
  - 允许与 **Apple TV Remote** 应用程序配对：允许用户将其设备与 Apple TV Remote 应用程序配对。
  - **Siri** 猥亵语言过滤： Siri 猥亵语言过滤：启用 Siri 猥亵语言过滤。默认为限制此功能，也就是说不会进行猥亵语言过滤。

    有关 Siri 和安全性的详细信息，请参阅 Siri 和听写策略。
  - 启用 **AirPlay**：允许用户在此设备上通过流技术推送内容或镜像其 iOS 设备屏幕。
  - 受限应用程序使用：允许用户使用所有应用程序或者使用或不使用某些应用程序，具体取决于您提供的捆绑包 ID。仅适用于受监督的设备。

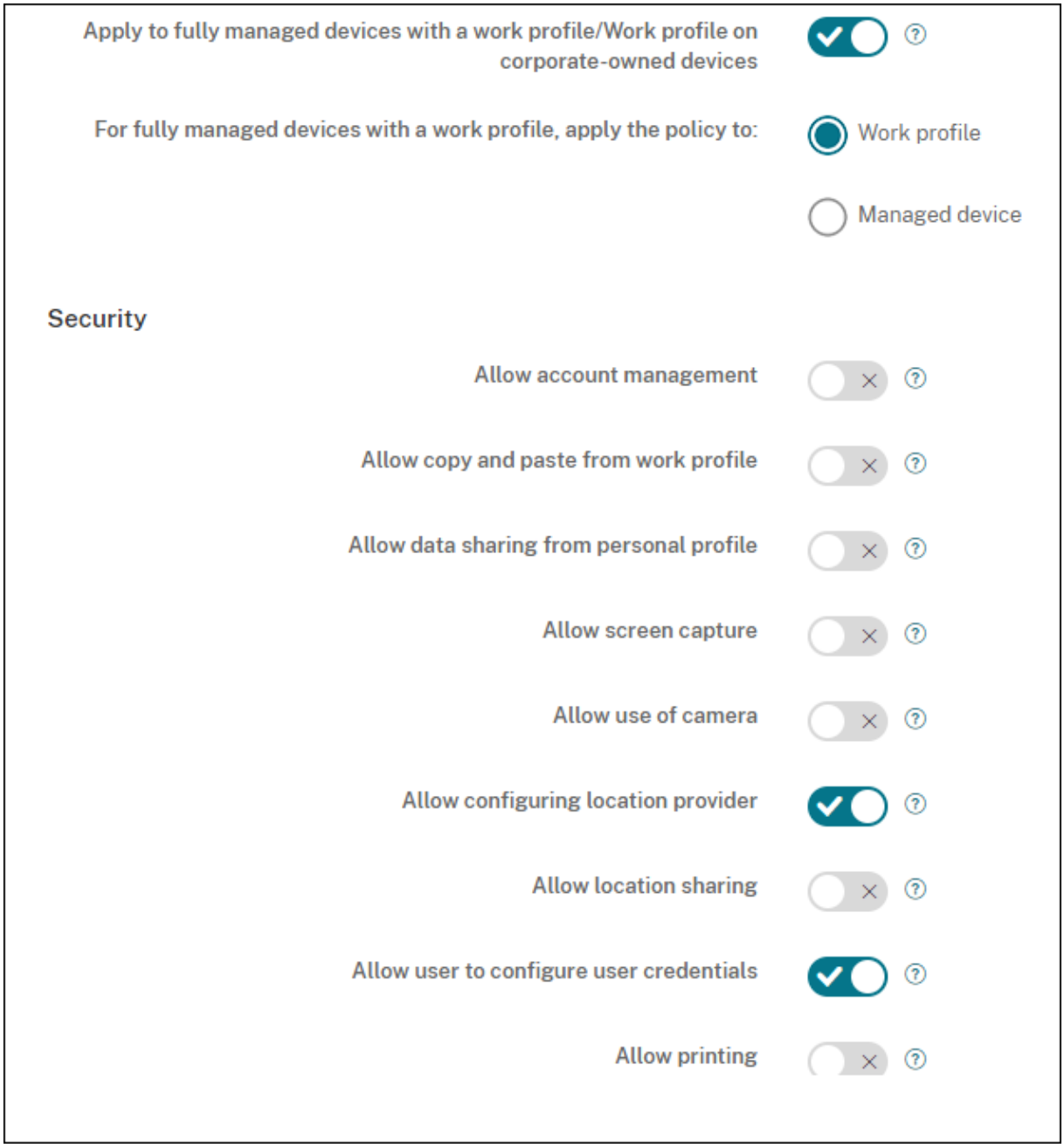
    配置限制设备策略以阻止某些应用程序，然后部署了该策略之后：如果以后要允许这些应用程序中的一些或全部，更改并部署限制设备策略不会更改显示。在这种情况下，iOS 不会将更改应用于 iOS 配置文件。如果将此设置更改为仅允许某些应用程序：部署此策略之前，建议使用 Apple 部署计划注册的设备的用户从设置助理登录其 Apple 帐户。否则，用户可能必须在其设备上禁用双重身份验证，才能登录其 Apple 帐户并访问允许的应用程序。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。不适用于 iOS。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android 设置

- 相机：允许用户在其设备上使用相机。如果设置为关，则将禁用相机。默认值为开。

Android Enterprise 设置



当新设备或恢复出厂设置的 Android 设备在工作配置文件模式下注册时，运行 Android 9.0-10.x 的设备会注册为具有工作配置文件的完全托管设备。运行 Android 11+ 的设备将注册为企业拥有的设备上的工作配置文件。限制策略可以应用到设备上的工作配置文件，也可以应用到托管设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在企业拥有的设备上的工作配置文件模式下注册的设备上，以下限制不起作用：

- 允许备份服务
- 启用系统应用
- 保持键盘锁不锁定设备
- 允许使用状态栏
- 保持设备屏幕处于打开状态
- 允许用户控制应用程序设置
- 允许用户配置用户凭据
- 允许 VPN 配置
- 允许 USB 大容量存储
- 允许恢复出厂设置
- 允许卸载应用程序
- 允许使用非 Google Play 应用程序
- 允许跨配置文件复制和粘贴
- 启用应用程序验证
- 允许帐户管理
- 允许打印
- 允许使用 NFC
- 允许添加用户

默认情况下，如果某个设备是在工作配置文件模式下在 Android Enterprise 中注册的，**USB** 调试和未知来源设置在该设备上将处于禁用状态。

观看此视频以了解更多：



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备：允许为具有工作配置文件的完全托管设备配置凭据策略设置。这些设备也称为 COPE（企业拥有但由个人使用）设备。当此设置设为开时，选择以下设置之一：
  - 工作配置文件：您配置的限制设置仅适用于设备上的工作配置文件。
  - 托管设备：您配置的限制设置仅适用于设备。

  当此设置设为关时，您配置的凭据设置将应用到设备，但明确应用于工作配置文件的设置除外。默认设置为关。

当应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备处于关闭状态时，请配置以下设置：

- 安全性
  - 允许帐户管理：允许在工作配置文件和托管设备中向帐户中添加对象。默认设置为关。
  - 允许从工作配置文件复制和粘贴：如果设置为开，用户可以将工作配置文件中的应用程序中的数据复制并粘贴到配置文件中的应用程序。默认设置为关。
  - 允许从配置文件共享数据：如果设置为开，用户可以将配置文件中的应用程序中的文件和数据复制、粘贴和共享到工作配置文件中的应用。默认设置为关。
  - 允许屏幕捕获：允许用户记录或捕获设备屏幕的屏幕拍图。默认设置为关。
  - 允许使用相机：允许用户使用设备摄像头拍照并制作视频。默认设置为关。
  - 允许 **VPN** 配置：允许用户创建 VPN 配置。适用于运行 Android 6 及更高版本的工作配置文件设备以及完全托管设备。默认值为开。
  - 允许备份服务：允许用户在其设备上备份应用程序和系统数据。默认值为开。
  - 允许 **NFC**：允许用户使用近场通信 (NFC) 将网页、照片、视频或其他内容从他们的设备发送到另一台设备。对于 MDM 4.0 及更高版本。默认值为开。
  - 允许配置位置提供程序：允许用户在其设备上打开 GPS。适用于 Android API 28 及更高版本。默认值为开。
  - 允许位置共享：对于托管配置文件，设备所有者可以覆盖此设置。默认设置为关。

    > 提示：
    >
    > 您可以在 Endpoint Management 中创建位置设备策略来强制执行地理边界。请参阅位置设备策略。

  - 允许用户配置用户凭据：指定用户是否可以在托管密钥库中配置凭据。默认值为开。
  - 允许打印：如果打 开，则该设置允许用户在用户设备可以访问的任何打印机上进行打印。默认值为关。适用于：Android 9 及更高版本。
  - 允许 **USB** 调试：默认值为 关闭。
- 应用程序
  - 启用系统应用程序：允许用户运行预安装的设备应用程序。默认设置为关。要启用特定应用程序，请在 系统应用程序列表表中单击 添加。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 系统应用列表：要在设备上启用的系统应用程序的列表。将 启用系统应用程序设置为 开，然后添加应用程序包名称。要查找系统应用程序的软件包名称，可以使用 Android Debug Bridge (adb) 调用 Android 软件包管理器 (pm) 命令。例如，`adb shell "pm list packages -f name"`，其中 “name” 为软件包名称的一部分。有关详细信息，请参阅 https://developer.android.com/studio/command-line/adb。对于 Android Enterprise 设备，可以使用 Android Enterprise 应用程序权限策略限制应用程序权限。
  - 禁用应用程序：阻止指定的应用程序列表在设备上运行。默认设置为关。要禁用已安装的应用程序，请将设置更改为 开，然后在应用程 序列表表中单击 添加。
    * 应用程序列表：要阻止的应用程序的列表。请将禁用应用程序设置为开并添加应用程序。请键入应用程序软件包名称。更改和部署某个应用程序列表将覆盖之前的应用程序列表。例如：如果禁用了 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，Endpoint Management 将启用 com.example.2。
  - 启用应用程序验证：允许操作系统扫描应用程序以检测恶意行为。默认值为开。
  - 启用谷歌应用程序：允许用户将 Google 移动服务中的应用下载到设备上。默认值为开。
  - 允许非 **Google Play** 应用：允许从 Google Play 以外的商店安装应用。默认设置为关。
  - 允许所有配置文件使用非 **Google Play** 应用：如果设置为开，则用户可以在设备上的所有配置文件上安装 Google Play 以外的其他应用商店的应用。默认设置为关。
  - 允许用户控制应用程序设置：允许用户卸载应用程序、禁用应用程序、清除缓存和数据、强制停止任何应用程序以及清除默认设置。用户从 “设置” 应用程序执行这些操作。默认值为 关。
  - 允许卸载应用：允许用户从托管 Google Play 商店中卸载应用。默认设置为关。

- **BYOD** 工作配置文件
  - 启用已连接的应用程序：如果启用，用户可以选择能够利用工作和个人数据跨工作和个人配置文件进行通信的应用程序。启用后，点按 “添加”，选择所需的应用程序，然后点按 “保存”。启用此功能需要工作配置文件。默认设置为关。
  - 允许在主屏幕上显示工作配置文件应用程序小组件：如果此设置设为开，则用户可以将工作配置文件应用程序小组件放置在设备主屏幕上。如果此设置设为关，则用户无法将工作配置文件应用程序小组件放置在设备主屏幕上。默认设置为关。
    * 带有允许的小部件的应用程序：您希望在主屏幕上允许的应用程序的列表。将允许在主屏幕上显示工作配置文件应用程序小组件设置为开并添加应用程序。单击添加并从列表中选择希望允许在主屏幕上显示其小组件的应用程序。单击保存。重复该过程将允许更多应用程序小组件。
  - 允许在设备联系人中添加工作配置文件联系人：在家长配置文件中显示托管 Android Enterprise 配置文件中的联系人，以便接收传入呼叫（Android 7.0 及更高版本）。默认设置为关。

- 仅限完全托管的设备
  - 允许添加用户：允许用户在设备上添加新用户。默认值为开。
  - 允许数据漫游：允许用户在漫游时使用蜂窝数据。默认值为 “关”，即在用户设备上禁用漫游。默认设置为关。
  - 允许短信：允许用户发送和接收短消息。默认设置为关。
  - 允许使用状态栏：如果 开启，此设置将启用受管设备和专用设备（也称为 COSU 设备）上的状态栏。此设

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

置禁用允许从全屏模式中逃脱的通知、快速设置和其他屏幕叠加。用户可以转到系统设置并查看通知。适用于 Android 6.0 及更高版本。默认设置为关。

- 允许蓝牙：允许用户使用蓝牙。默认值为开。
  - 允许蓝牙共享：如果取消选中，用户将无法在其设备上建立传出的蓝牙共享。默认值处于选中状态。
- 允许配置日期和时间：允许用户更改设备上的日期和时间。默认值为开。
- 允许恢复出厂设置：允许用户在其设备上进行出厂设置。默认值为开。
- 保持设备屏幕处于打开状态：如果此设置设为开，设备插入时设备屏幕保持打开状态。默认设置为关。
- 允许 **USB** 大容量存储：允许通过 USB 连接在用户的设备和计算机之间传输大型数据文件。默认值为开。
- 允许麦克风：允许用户在其设备上使用麦克风。默认值为开。
- 允许共享：允许用户配置便携式热点和连接数据。默认设置为关。
- 防止键盘锁定设备：如果开启，此设置将禁用托管设备和专用设备（也称为 **COSU** 设备）上的锁屏上的钥匙保护。默认设置为关。
- 允许更改 **Wi-Fi**：如果 开启，用户可以打开或关闭 Wi-Fi 并连接到 Wi-Fi 网络。默认值为开。
- 允许文件传输：允许通过 USB 传输文件。默认设置为关。

- **Samsung**
  - 启用 **TIMA** 密钥库： TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书路由到默认密钥库提供商进行存储。默认设置为关。
  - 允许共享列表：允许用户在共享通过列表中的应用程序之间共享内容。默认值为开。
  - 启用审核日志：启用事件审计日志的创建以便对设备进行取证分析。默认设置为关。

- 三星：仅限完全托管的设备
  - 启用 **ODE** 可信启动验证：使用 ODE 可信启动验证建立从引导加载程序到系统映像的信任链。默认值为开。
  - 仅允许紧急呼叫：允许用户在其设备上启用“仅紧急呼叫”模式。默认设置为关。
  - 允许固件恢复：允许用户在其设备上恢复固件。默认值为开。
  - 允许快速加密：允许仅加密已使用的内存空间。这种加密与加密所有数据的全磁盘加密形成了鲜明对比。该数据包括设置、应用程序数据、下载的文件和应用程序、媒体和其他文件。默认值为开。
  - 启用通用标准模式：将设备置于通用标准模式。通用准则配置强制执行严苛的安全流程。默认值为开。
  - 启用重启横幅：当用户的设备重新启动时，显示 DoD 批准的系统使用通知消息或横幅。默认设置为关。
  - 允许更改设置：允许用户更改完全托管设备上的设置。默认值为开。
  - 启用后台数据使用：允许应用程序在后台同步数据。对于完全托管的设备。默认值为开。
  - 允许剪贴板：允许用户将数据复制到设备上的剪贴板。
    - 允许剪贴板共享：允许用户在设备和计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。
  - 允许主页密钥：允许用户在完全托管的设备上使用 **Home** 键。默认值为开。
  - 允许模拟位置：允许用户伪造他们的 GPS 位置。适用于完全托管设备。默认设置为关。
  - **NFC**：允许用户在其完全托管设备上使用 NFC（MDM 3.0 及更高版本）。默认值为开。
  - 允许关闭电源：允许用户关闭完全托管的设备的电源（MDM 3.0 及更高版本）。默认值为开。
  - 允许直接 **Wi-Fi**：允许用户通过 Wi-Fi 连接直接连接到另一台设备。默认值为开。如果 开启，则必须启用允许 **Wi-Fi** 更改设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 允许 **SD** 卡：允许用户在设备上使用 SD 卡（如果可用）。默认值为开。
- 允许 **USB** 主机存储：当 USB 设备连接到其设备时，允许用户的设备充当 USB 主机。然后，用户的设备为 USB 设备提供电源。默认值为开。
- 允许语音拨号器：允许用户在其设备上使用语音拨号器（MDM 4.0 及更高版本）。默认值为开。
- 允许 **S** 梁：允许用户使用 NFC 和 Wi-Fi Direct（MDM 4.0 及更高版本）与其他人共享内容。默认值为开。
- 允许 **S** 语音：允许用户在其设备上使用智能个人助理和知识导航器（MDM 4.0 及更高版本）。默认值为开。
- 允许 **USB** 共享：允许用户使用 USB 连接与另一台设备共享移动数据连接。默认值为关。如果 开启 “ 允许共享” 设置也必须为 “ 开”。
- 允许蓝牙共享：允许用户使用蓝牙连接与其他设备共享移动数据连接。默认值为关。如果 开启 “ 允许共享” 设置也必须为 “ 开”。
  - 允许蓝牙共享：如果取消选中，用户将无法在其设备上建立传出的蓝牙共享。默认值处于选中状态。
- 允许 **Wi-Fi** 共享：允许用户使用 Wi-Fi 连接与其他设备共享移动数据连接。默认值为关。如果 开启 “ 允许共享” 设置也必须为 “ 开”。
- 允许传入彩信：允许用户接收彩信。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 允许传出彩信：允许用户发送彩信。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 允许传入短信：允许用户接收 SMS 消息。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 允许传出短信：允许用户发送短信。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 配置移动网络：允许用户使用其蜂窝数据连接。默认设置为关。
- 按天限制 **(MB)**：输入移动数据用户每天可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按周限制 **(MB)**：输入移动数据用户每周可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按月限制 **(MB)**：输入移动数据用户每月可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 仅允许安全的 **VPN** 连接：允许用户仅使用安全连接（MDM 4.0 及更高版本）。默认值为开。
- 允许录音：允许用户使用自己的设备录制音频（MDM 4.0 及更高版本）。默认值为开。如果 打开，则必须打开 允许麦克风设置。
- 允许录制视频：允许用户使用自己的设备录制视频（MDM 4.0 及更高版本）。默认设置为关。如果 启用，则必须打开 允许使用相机设置。
- 漫游时允许推送消息：允许用户使用蜂窝数据进行推送。默认设置为关。如果为开，则必须启用允许数据漫游设置。
- 漫游时允许自动同步：允许用户使用蜂窝数据进行同步。默认设置为关。如果为开，则必须启用允许数据漫游设置。
- 漫游时允许语音通话：允许用户使用蜂窝数据进行语音通话。默认设置为关。如果为开，则必须启用允许数据漫游设置。

- **Samsung:** 完全托管设备
  - 启用吊销检查：启用对已吊销证书的检查。默认设置为关。

当适用于具有工作配置文件**/**企业拥有的设备上的工作配置文件的完全托管设备设置为 “开” 且对于具有工作配置文件的完全托管设备，请将策略应用到设置为工作配置文件时，请配置以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 安全性
  - 允许帐户管理：允许在工作配置文件和托管设备中向帐户中添加对象。默认设置为关。
  - 允许跨配置文件复制和粘贴：如果 开启，用户可以在 Android Enterprise 配置文件中的应用程序和个人区域中的应用之间复制和粘贴。默认设置为关。
  - 允许屏幕捕获：允许用户记录或捕获设备屏幕的屏幕拍图。默认设置为关。
  - 允许使用相机：允许用户使用设备摄像头拍照并制作视频。默认设置为关。
  - 允许配置位置提供程序：允许用户在其设备上打开 GPS。适用于 Android API 28 及更高版本。默认值为开。
  - 允许位置共享：对于托管配置文件，设备所有者可以覆盖此设置。默认设置为关。

    > 提示：
    >
    > 您可以在 Endpoint Management 中创建位置设备策略来强制执行地理边界。请参阅位置设备策略。

  - 允许用户配置用户凭据：指定用户是否可以在托管密钥库中配置凭据。默认值为开。
  - 允许打印：如果打 开，则该设置允许用户在用户设备可以访问的任何打印机上进行打印。默认值为关。适用于：Android 9 及更高版本。
- 应用程序
  - 启用系统应用程序：允许用户运行预安装的设备应用程序。默认设置为关。要启用特定应用程序，请在 系统应用程序列表表中单击 添加。
    * 系统应用列表：要在设备上启用的系统应用程序的列表。将 启用系统应用程序设置为 开，然后添加应用程序包名称。要查找系统应用程序的软件包名称，可以使用 Android Debug Bridge (adb) 调用 Android 软件包管理器 (pm) 命令。例如，`adb shell "pm list packages -f name"`，其中 “name” 为软件包名称的一部分。有关详细信息，请参阅 https://developer.android.com/studio/command-line/adb。对于 Android Enterprise 设备，可以使用 Android Enterprise 应用程序权限策略限制应用程序权限。
  - 禁用应用程序：阻止指定的应用程序列表在设备上运行。默认设置为关。要禁用已安装的应用程序，请将设置更改为 开，然后在应用程 序列表表中单击 添加。
    * 应用程序列表：要阻止的应用程序的列表。请将禁用应用程序设置为开并添加应用程序。请键入应用程序软件包名称。更改和部署某个应用程序列表将覆盖之前的应用程序列表。例如：如果禁用了 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，Endpoint Management 将启用 com.example.2。
  - 启用应用程序验证：允许操作系统扫描应用程序以检测恶意行为。默认值为开。
  - 启用谷歌应用程序：允许用户将 Google 移动服务中的应用下载到设备上。默认值为开。
  - 允许非 **Google Play** 应用：允许从 Google Play 以外的商店安装应用。默认设置为关。
  - 允许用户控制应用程序设置：允许用户卸载应用程序、禁用应用程序、清除缓存和数据、强制停止任何应用程序以及清除默认设置。用户从 “设置” 应用程序执行这些操作。默认值为 关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 允许卸载应用：允许用户从托管 Google Play 商店中卸载应用。默认设置为关。

- **BYOD** 工作配置文件

  - 允许在主屏幕上显示工作配置文件应用程序小组件：如果此设置设为开，则用户可以将工作配置文件应用程序小组件放置在设备主屏幕上。如果此设置设为关，则用户无法将工作配置文件应用程序小组件放置在设备主屏幕上。默认设置为关。
    * 带有允许的小部件的应用程序：您希望在主屏幕上允许的应用程序的列表。将允许在主屏幕上显示工作配置文件应用程序小组件设置为开并添加应用程序。单击添加并从列表中选择希望允许在主屏幕上显示其小组件的应用程序。单击保存。重复该过程将允许更多应用程序小组件。
  - 允许在设备联系人中添加工作配置文件联系人：在家长配置文件中显示托管 Android Enterprise 配置文件中的联系人，以便接收传入呼叫（Android 7.0 及更高版本）。默认设置为关。

- **Samsung**

  - 启用 **TIMA** 密钥库： TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书路由到默认密钥库提供商进行存储。默认设置为关。
  - 允许共享列表：允许用户在共享通过列表中的应用程序之间共享内容。默认值为开。
  - 启用审核日志：启用事件审计日志的创建以便对设备进行取证分析。默认设置为关。

- **Samsung:** 完全托管设备

  - 启用吊销检查：启用对已吊销证书的检查。默认设置为关。

当适用于具有工作配置文件**/**企业拥有的设备上的工作配置文件的完全托管设备设置为 “开” 且对于具有工作配置文件的完全托管设备，请将策略应用到设置为托管设备时，请配置以下设置：

- 安全性

  - 允许帐户管理：允许在工作配置文件和托管设备中向帐户中添加对象。默认设置为关。
  - 允许跨配置文件复制和粘贴：如果 开启，用户可以在 Android Enterprise 配置文件中的应用程序和个人区域中的应用之间复制和粘贴。默认设置为关。
  - 允许屏幕捕获：允许用户记录或捕获设备屏幕的屏幕拍图。默认设置为关。
  - 允许使用相机：允许用户使用设备摄像头拍照并制作视频。默认设置为关。
  - 允许 **VPN** 配置：允许用户创建 VPN 配置。适用于运行 Android 6 及更高版本的工作配置文件设备以及完全托管设备。默认值为开。
  - 允许备份服务：允许用户在其设备上备份应用程序和系统数据。默认值为开。
  - 允许 **NFC**：允许用户使用近场通信 (NFC) 将网页、照片、视频或其他内容从他们的设备发送到另一台设备。对于 MDM 4.0 及更高版本。默认值为开。
  - 允许配置位置提供程序：允许用户在其设备上打开 GPS。适用于 Android API 28 及更高版本。默认值为开。
  - 允许位置共享：对于托管配置文件，设备所有者可以覆盖此设置。默认设置为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 提示：
>
> 您可以在 Endpoint Management 中创建位置设备策略来强制执行地理边界。请参阅位置设备策略。

  - 允许用户配置用户凭据：指定用户是否可以在托管密钥库中配置凭据。默认值为开。
  - 允许打印：如果打 开，则该设置允许用户在用户设备可以访问的任何打印机上进行打印。默认值为关。适用于：Android 9 及更高版本。
  - 允许 **USB** 调试：默认值为 关闭。

- 应用程序
  - 启用系统应用程序：允许用户运行预安装的设备应用程序。默认设置为关。要启用特定应用程序，请在 系统应用程序列表表中单击 添加。
    * 系统应用列表：要在设备上启用的系统应用程序的列表。将 启用系统应用程序设置为 开，然后添加应用程序包名称。要查找系统应用程序的软件包名称，可以使用 Android Debug Bridge (adb) 调用 Android 软件包管理器 (pm) 命令。例如，`adb shell "pm list packages -f name"`，其中 “name” 为软件包名称的一部分。有关详细信息，请参阅 https://developer.android.com/studio/command-line/adb。对于 Android Enterprise 设备，可以使用 Android Enterprise 应用程序权限策略限制应用程序权限。
  - 禁用应用程序：阻止指定的应用程序列表在设备上运行。默认设置为关。要禁用已安装的应用程序，请将设置更改为 开，然后在应用程 序列表表中单击 添加。
    * 应用程序列表：要阻止的应用程序的列表。请将禁用应用程序设置为开并添加应用程序。请键入应用程序软件包名称。更改和部署某个应用程序列表将覆盖之前的应用程序列表。例如：如果禁用了 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，Endpoint Management 将启用 com.example.2。
  - 启用应用程序验证：允许操作系统扫描应用程序以检测恶意行为。默认值为开。
  - 启用谷歌应用程序：允许用户将 Google 移动服务中的应用下载到设备上。默认值为开。
  - 允许非 **Google Play** 应用：允许从 Google Play 以外的商店安装应用。默认设置为关。
  - 允许用户控制应用程序设置：允许用户卸载应用程序、禁用应用程序、清除缓存和数据、强制停止任何应用程序以及清除默认设置。用户从 “设置” 应用程序执行这些操作。默认值为 关。
  - 允许卸载应用：允许用户从托管 Google Play 商店中卸载应用。默认设置为关。

- 仅限完全托管的设备
  - 允许添加用户：允许用户在设备上添加新用户。默认值为开。
  - 允许数据漫游：允许用户在漫游时使用蜂窝数据。默认值为 “关”，即在用户设备上禁用漫游。默认设置为关。
  - 允许短信：允许用户发送和接收短消息。默认设置为关。
  - 允许使用状态栏：如果 开启，此设置将启用受管设备和专用设备（也称为 COSU 设备）上的状态栏。此设置禁用允许从全屏模式中逃脱的通知、快速设置和其他屏幕叠加。用户可以转到系统设置并查看通知。适用于 Android 6.0 及更高版本。默认设置为关。
  - 允许蓝牙：允许用户使用蓝牙。默认值为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 允许蓝牙共享：如果取消选中，用户将无法在其设备上建立传出的蓝牙共享。默认值处于选中状态。
  - 允许配置日期和时间：允许用户更改设备上的日期和时间。默认值为开。
  - 允许恢复出厂设置：允许用户在其设备上进行出厂设置。默认值为开。
  - 允许恢复出厂设置保护：如果设置为开，则在使用恢复模式重置设备时，用户必须提供重置前设备上的帐户的凭据。如果在重置之前设置了设备锁定，他们还可以提供设备锁定。如果设置为 关，则重置后无需进行身份验证。默认值为开。
  - 保持设备屏幕处于打开状态：如果此设置设为开，设备插入时设备屏幕保持打开状态。默认设置为关。
  - 允许 **USB** 大容量存储：允许通过 USB 连接在用户的设备和计算机之间传输大型数据文件。默认值为开。
  - 允许麦克风：允许用户在其设备上使用麦克风。默认值为开。
  - 允许共享：允许用户配置便携式热点和连接数据。默认设置为关。启用此设置时，这些设置适用于 Samsung 设备：
  - 防止键盘锁定设备：如果开启，此设置将禁用托管设备和专用设备（也称为 **COSU** 设备）上的锁屏上的钥匙保护。默认设置为关。
  - 允许更改 **Wi-Fi**：如果 开启，用户可以打开或关闭 Wi-Fi 并连接到 Wi-Fi 网络。默认值为开。
  - 允许文件传输：允许通过 USB 传输文件。默认设置为关。

- **Samsung**

  - 启用 **TIMA** 密钥库： TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书路由到默认密钥库提供商进行存储。默认设置为关。
  - 允许共享列表：允许用户在共享通过列表中的应用程序之间共享内容。默认值为开。
  - 启用审核日志：启用事件审计日志的创建以便对设备进行取证分析。默认设置为关。

- 三星：仅限完全托管的设备

  - 启用 **ODE** 可信启动验证：使用 ODE 可信启动验证建立从引导加载程序到系统映像的信任链。默认值为开。
  - 仅允许紧急呼叫：允许用户在其设备上启用“仅紧急呼叫”模式。默认设置为关。
  - 允许固件恢复：允许用户在其设备上恢复固件。默认值为开。
  - 允许快速加密：允许仅加密已使用的内存空间。这种加密与加密所有数据的全磁盘加密形成了鲜明对比。该数据包括设置、应用程序数据、下载的文件和应用程序、媒体和其他文件。默认值为开。
  - 启用通用标准模式：将设备置于通用标准模式。通用准则配置强制执行严苛的安全流程。默认值为开。
  - 启用重启横幅：当用户的设备重新启动时，显示 DoD 批准的系统使用通知消息或横幅。默认设置为关。
  - 允许更改设置：允许用户更改完全托管设备上的设置。默认值为开。
  - 启用后台数据使用：允许应用程序在后台同步数据。对于完全托管的设备。默认值为开。
  - 允许剪贴板：允许用户将数据复制到设备上的剪贴板。默认值为开。
    * 允许剪贴板共享：允许用户在设备和计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。
  - 允许主页密钥：允许用户在完全托管的设备上使用 **Home** 键。默认值为开。
  - 允许模拟位置：允许用户伪造他们的 GPS 位置。适用于完全托管设备。默认设置为关。
  - **NFC**：允许用户在其完全托管设备上使用 NFC（MDM 3.0 及更高版本）。默认值为开。
  - 允许关闭电源：允许用户关闭完全托管的设备的电源（MDM 3.0 及更高版本）。默认值为开。
  - 允许直接 **Wi-Fi**：允许用户通过 Wi-Fi 连接直接连接到另一台设备。默认值为开。如果 开启，则必须启用

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

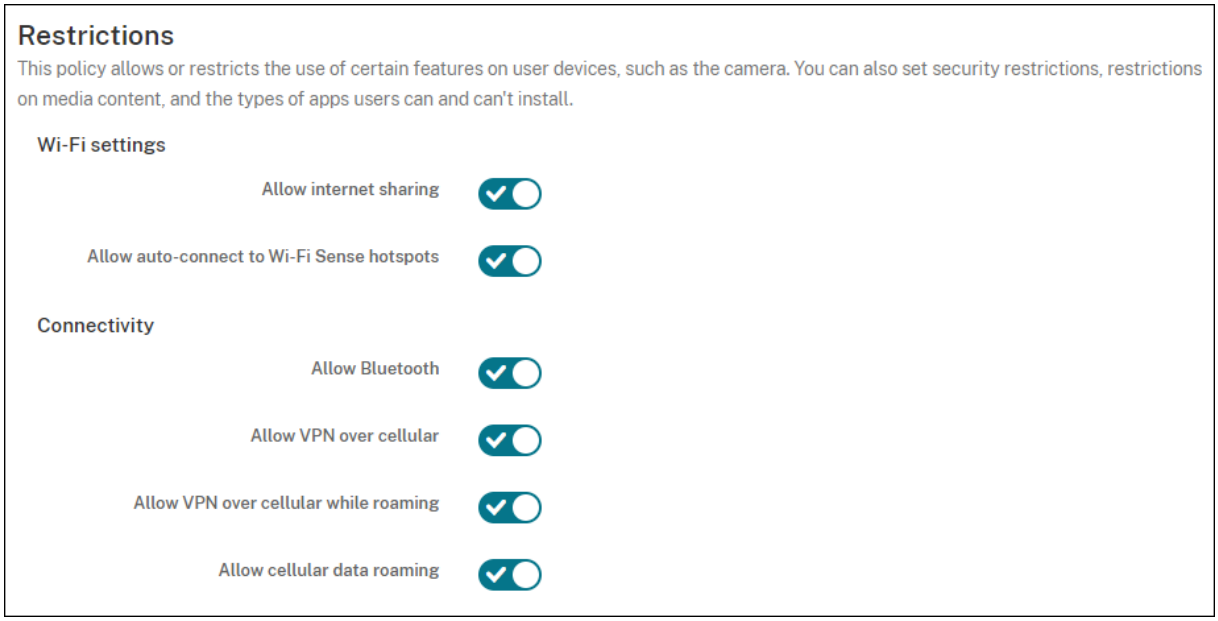
允许 **Wi-Fi** 更改设置。

- 允许 **SD** 卡：允许用户在设备上使用 SD 卡（如果可用）。默认值为开。
- 允许 **USB** 主机存储：当 USB 设备连接到其设备时，允许用户的设备充当 USB 主机。然后，用户的设备为 USB 设备提供电源。默认值为开。
- 允许语音拨号器：允许用户在其设备上使用语音拨号器（MDM 4.0 及更高版本）。默认值为开。
- 允许 **S** 梁：允许用户使用 NFC 和 Wi-Fi Direct（MDM 4.0 及更高版本）与其他人共享内容。默认值为开。
- 允许 **S** 语音：允许用户在其设备上使用智能个人助理和知识导航器（MDM 4.0 及更高版本）。默认值为开。
- 允许 **USB** 共享：允许用户使用 USB 连接与另一台设备共享移动数据连接。默认值为关。如果 开启 “ 允许共享” 设置也必须为 “ 开”。
- 允许蓝牙共享：允许用户使用蓝牙连接与其他设备共享移动数据连接。默认值为关。如果 开启 “ 允许共享” 设置也必须为 “ 开”。
- 允许 **Wi-Fi** 共享：允许用户使用 Wi-Fi 连接与其他设备共享移动数据连接。默认值为关。如果 开启 “ 允许共享” 设置也必须为 “ 开”。
- 允许传入彩信：允许用户接收彩信。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 允许传出彩信：允许用户发送彩信。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 允许传入短信：允许用户接收 SMS 消息。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 允许传出短信：允许用户发送短信。默认设置为关。如果 开启，则必须打开 允许短信设置。
- 配置移动网络：允许用户使用其蜂窝数据连接。默认设置为关。
- 按天限制 **(MB)**：输入移动数据用户每天可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按周限制 **(MB)**：输入移动数据用户每周可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按月限制 **(MB)**：输入移动数据用户每月可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 仅允许安全的 **VPN** 连接：允许用户仅使用安全连接（MDM 4.0 及更高版本）。默认值为开。
- 允许录音：允许用户使用自己的设备录制音频（MDM 4.0 及更高版本）。默认值为开。如果 打开，则必须打开 允许麦克风设置。
- 允许录制视频：允许用户使用自己的设备录制视频（MDM 4.0 及更高版本）。默认设置为关。如果 启用，则必须打开 允许使用相机设置。
- 漫游时允许推送消息：允许用户使用蜂窝数据进行推送。默认设置为关。如果为开，则必须启用允许数据漫游设置。
- 漫游时允许自动同步：允许用户使用蜂窝数据进行同步。默认设置为关。如果为开，则必须启用允许数据漫游设置。
- 漫游时允许语音通话：允许用户使用蜂窝数据进行语音通话。默认设置为关。如果为开，则必须启用允许数据漫游设置。

- **Samsung:** 完全托管设备
  - 启用吊销检查：启用对已吊销证书的检查。默认设置为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Windows Desktop/Tablet 设置



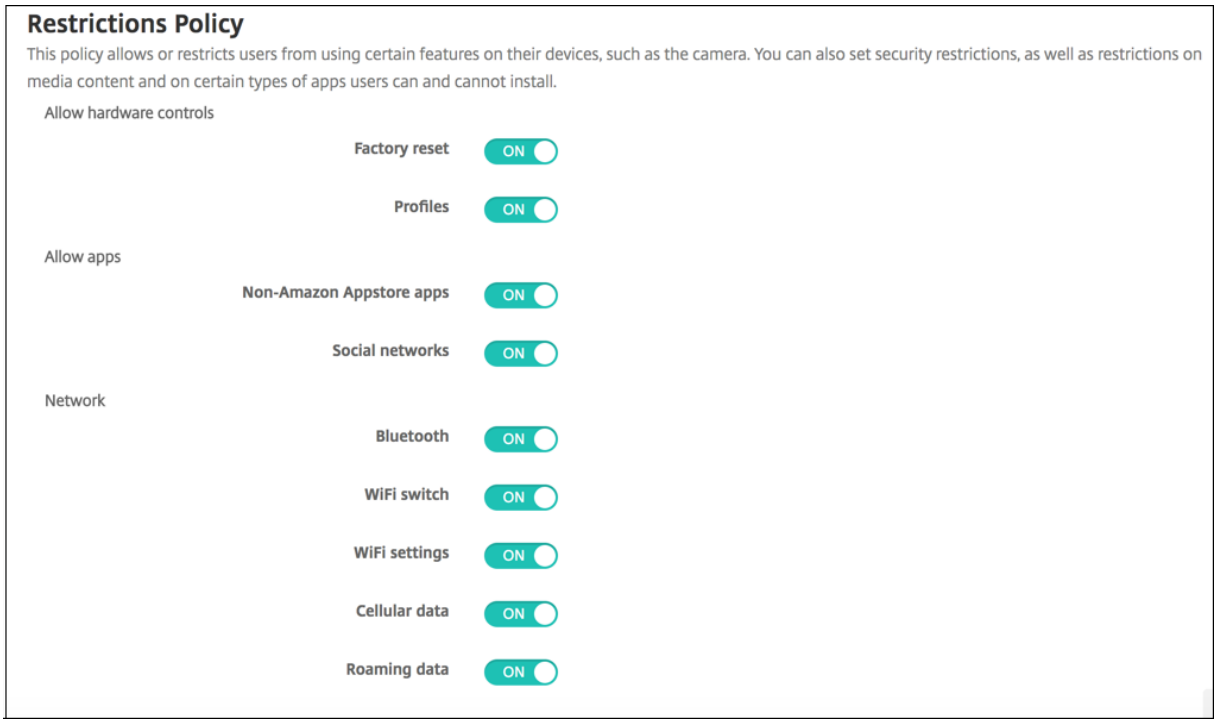
- **Wi-Fi** 设置
  - 允许 **Internet** 共享：允许设备通过将其设为 Wi-Fi 热点与其他设备共享其 Internet 连接。
- 连接
  - 允许使用蓝牙：允许设备通过蓝牙进行连接。
  - 允许通过手机网络使用 **VPN**：允许设备通过 VPN 连接到手机网络。
  - 允许在漫游时通过手机网络使用 **VPN**：允许设备在通过手机网络漫游时使用 VPN。
  - 允许使用手机网络数据漫游：允许用户在漫游时使用手机网络数据。
- 帐户
  - 允许使用 **Microsoft** 帐户连接：允许设备使用 Microsoft 帐户进行与电子邮件无关的连接身份验证和服务。
  - 允许使用非 **Microsoft** 电子邮件：允许用户添加非 Microsoft 电子邮件帐户。
- 系统
  - 允许使用存储卡：允许设备使用存储卡。
  - 遥测：在列表中，单击某个选项以允许或限制设备发送遥测信息。默认值为允许。其他选项为不允许和允许，次要数据请求除外。
  - 允许应用访问位置服务：允许应用访问定位服务。
  - 允许预览内部版本：允许用户预览 Microsoft 内部版本。
- 相机：仅限 Windows Desktop/Tablet
  - 允许使用相机：允许用户使用其设备相机。
- 蓝牙：仅限 Windows Desktop/Tablet
  - 允许使用可发现模式：允许蓝牙设备查找本地设备。
  - 本地设备名称：本地设备的名称。
- 体验：仅限 Windows Desktop/Tablet

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 允许使用 **Cortana**：允许用户访问 Cortana（智能个人助手和知识导航器）。
  - 允许发现设备：允许对设备进行网络发现。
  - 允许手动取消注册 **MDM**：允许用户手动从 Endpoint Management MDM 中取消注册其设备。
  - 允许同步设备设置：允许用户在漫游时在 Windows 10 和 Windows 11 设备之间同步设置。
- 超出锁定范围：仅限 Windows Desktop/Tablet
  - 在锁定屏幕上允许 **Toast** 通知：允许在锁定屏幕上显示 Toast 通知。仅限 Windows Desktop/Tablet
- 应用程序
  - **Allow automatic updates from app store**（允许从应用商店自动更新）：允许应用商店中的应用程序自动更新。仅限 Windows Desktop/Tablet。
- 隐私：仅限 Windows Desktop/Tablet
  - 允许输入个性化：允许运行输入个性化服务。输入个性化服务根据用户键入的内容改进了预测性输入，例如笔和触摸键盘。
- 设置：仅限 Windows Desktop/Tablet。
  - 允许自动播放：允许用户更改自动播放设置。
  - 允许使用流量感知：允许用户更改流量感知设置。
  - 允许设置日期时间：允许用户更改日期和时间设置。
  - 允许设置语言：允许用户更改语言设置。
  - 允许设置电源睡眠：允许用户更改电源和睡眠设置。
  - 允许设置区域：允许用户更改区域设置。
  - 允许设置登录选项：允许用户更改登录设置。
  - 允许设置工作区：允许用户更改工作区设置。
  - 允许使用您的帐户：允许用户更改帐户设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Amazon 设置



- 允许硬件控制
  - 恢复出厂设置：允许用户在其设备上恢复出厂设置
  - 配置文件：允许用户在其设备上更改硬件配置文件。
- 允许使用应用程序
  - 非亚马逊应用商店应用程序：允许用户在其设备上安装非亚马逊应用商店应用程序。
  - 社交网络：允许用户从其设备访问社交网络。
- 网络
  - 蓝牙：允许用户使用蓝牙。
  - **Wi-Fi** 开关：允许应用程序更改 Wi-Fi 连接状态。
  - **Wi-Fi** 设置：允许用户更改 Wi-Fi 设置。
  - 配置移动网络：允许用户使用其蜂窝数据连接。
  - 漫游数据：允许用户在漫游时使用手机网络数据。
  - 定位服务：允许用户使用 GPS。
- **USB** 操作：
  - 调试：允许用户设备通过 USB 连接到计算机以进行调试。

漫游设备策略

March 31, 2022

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可以在 Endpoint Management 中添加一个设备策略，以配置在受支持的 iOS 设备上是否允许语音和数据漫游。禁用语音漫游时，会自动禁用数据漫游。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 禁用语音漫游：选择是否禁用语音漫游。启用此选项时，会自动禁用数据漫游。默认值为关，表示允许语音漫游。
- 禁用数据漫游：选择是否禁用数据漫游。此选项仅在启用语音漫游时可用。默认值为关，表示允许数据漫游。

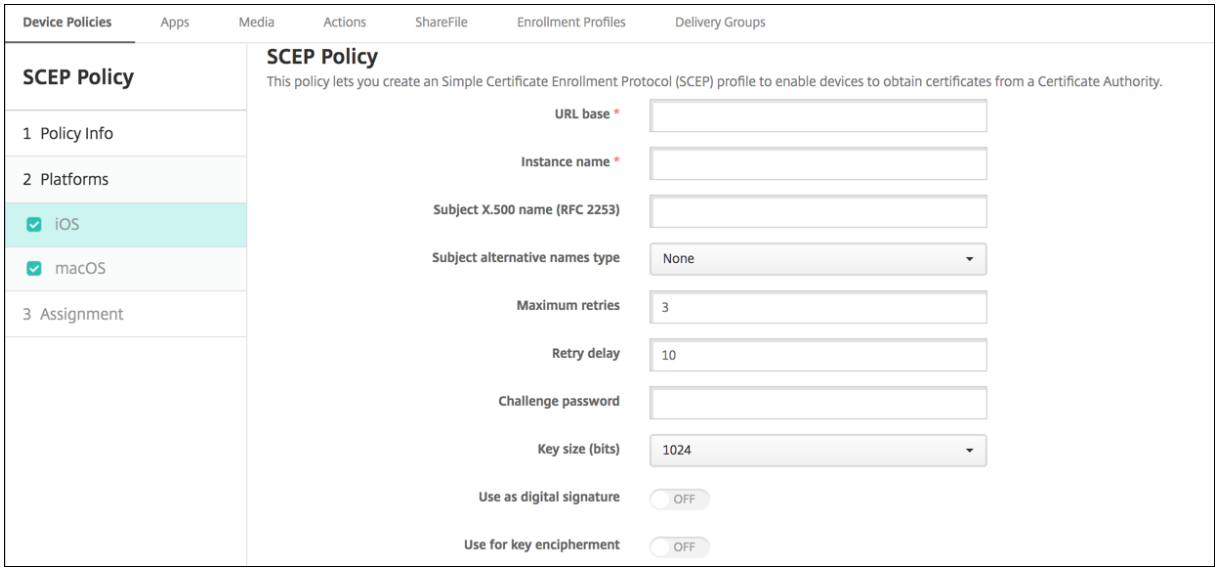
SCEP 设备策略

March 31, 2022

通过此策略，您可以将 iOS 和 macOS 设备配置为通过简单证书注册协议 (SCEP) 从外部 SCEP 服务器检索证书。要从连接到 Endpoint Management 的 PKI 向使用 SCEP 的设备交付证书，请在分布式模式下创建一个 PKI 实体和 PKI 提供程序。有关详细信息，请参阅 PKI 实体。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

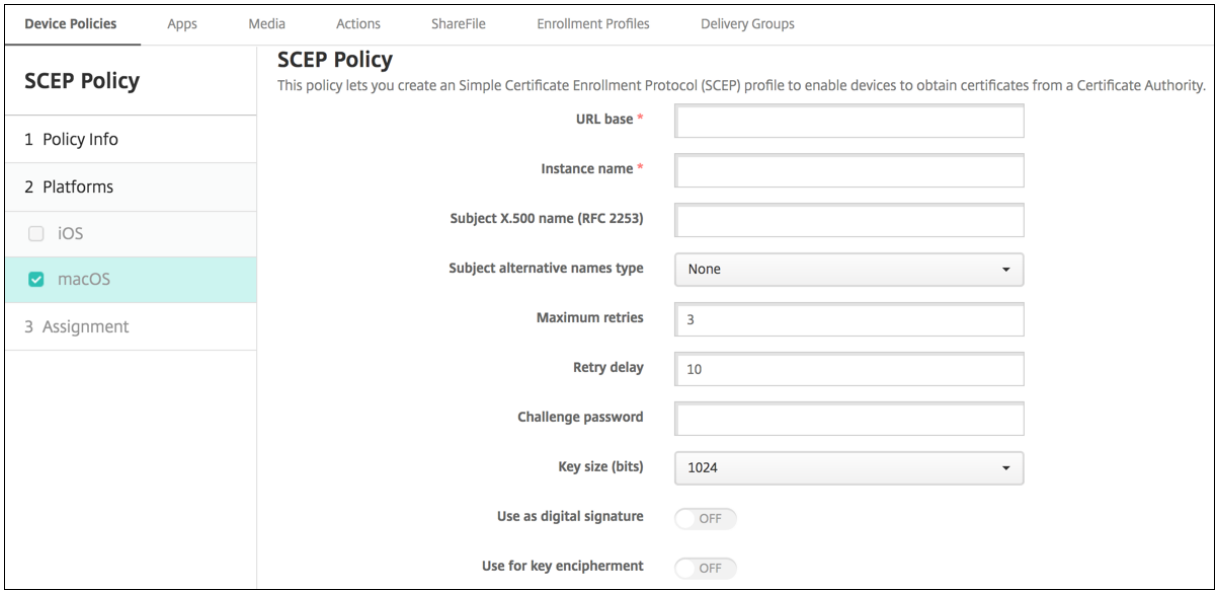


- **URL** 基：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。如果将一次性密码配置为重复使用，请使用 HTTPS 保护密码。此步骤不是必需步骤。
- 实例名称：键入 SCEP 服务器可以识别的任何字符串。例如，可以是类似 example.org 的域名。如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。此步骤不是必需步骤。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 使用者 **X.500** 名称 **(RFC 2253)**：键入作为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。例如，`/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`，转换为：`[ [ [ “C” , “US” ] ], [ [ “O” , “Apple Inc.” ] ], …, [ [ “1.2.5.3” , “bar” ] ] ]`。OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。
- 使用者备用名称类型：选择备用名称类型。可选的备用名称类型可以提供 CA 颁发证书所需的值。可以指定无、**RFC 822** 名称、**DNS** 名称或 **URI**。
- 最大重试次数：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。默认值为 **3**。
- 重试延迟：键入执行下次重试之前需要等待的秒数。第一次重试尝试没有延迟。默认值为 **10**。
- 质询密码：输入预共享密钥。
- 密钥大小 **(**位**)**：选择 **2048** 或更大值作为密钥大小，单位为位。
- 用作数字签名：指定是否要将证书用作数字签名。SCEP 服务器在使用公钥解密哈希之前验证用作数字签名的证书。
- 用于密钥加密：选择是否要将证书用于密钥加密。服务器首先检查是否允许客户端提供的证书用于密钥加密。然后，服务器使用证书中的公钥来验证是否使用私钥加密了一段数据。否则，操作将失败。
- **SHA-256** 指纹 **(X** 六进制字符串**)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹。设备在注册期间使用指纹来确认 CA 响应的真实性。可以提供 SHA-256 指纹，或选择证书来导入其签名。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **URL** 基：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。如果将一次性密码配置为重复使用，请使用 HTTPS 保护密码。此步骤不是必需步骤。
- 实例名称：键入 SCEP 服务器可以识别的任何字符串。例如，可以是类似 example.org 的域名。如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。此步骤不是必需步骤。
- 使用者 **X.500** 名称 **(RFC 2253)**：键入作为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。例如，`/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`，转换为：`[ [ [ "C", "US" ] ], [ [ "O", "Apple Inc." ] ], …, [ [ "1.2.5.3", "bar" ] ] ]`。OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。
- 使用者备用名称类型：选择备用名称类型。可选的备用名称类型可以提供 CA 颁发证书所需的值。可以指定无、**RFC 822** 名称、**DNS** 名称或 **URI**。
- 最大重试次数：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。默认值为 **3**。
- 重试延迟：键入执行下次重试之前需要等待的秒数。第一次重试尝试没有延迟。默认值为 **10**。
- 质询密码：键入预共享密钥。
- 密钥大小 **(**位**)**：选择 **2048** 或更大值作为密钥大小，单位为位。
- 用作数字签名：指定是否要将证书用作数字签名。SCEP 服务器在使用公钥解密哈希之前验证用作数字签名的证书。
- 用于密钥加密：选择是否要将证书用于密钥加密。服务器首先检查是否允许客户端提供的证书用于密钥加密。然后，服务器使用证书中的公钥来验证是否使用私钥加密了一段数据。否则，操作将失败。
- **SHA-256** 指纹 **(X** 六进制字符串**)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹。设备在注册期间使用指纹来确认 CA 响应的真实性。可以提供 SHA-256 指纹，或选择证书来导入其签名。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Siri 和听写策略

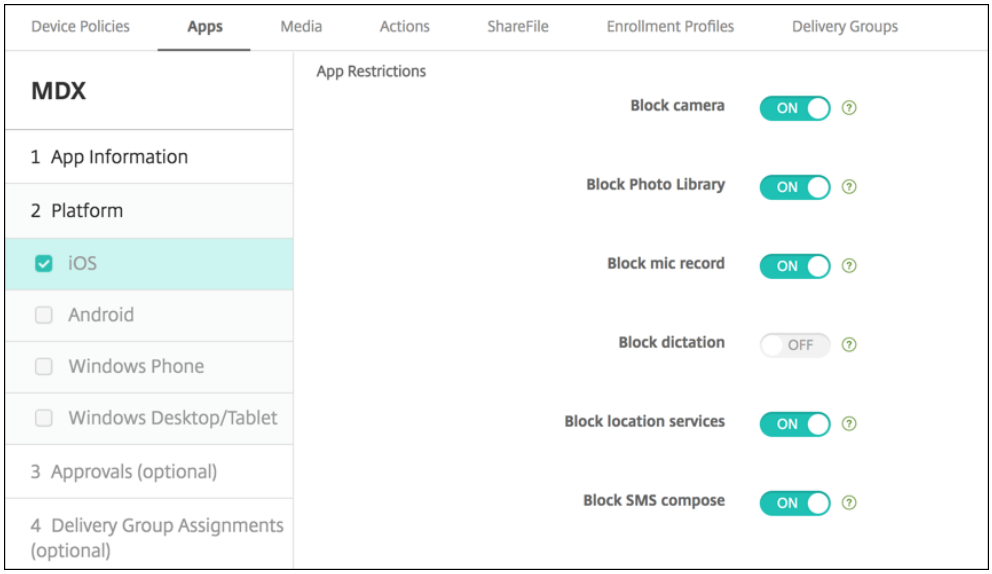
December 3, 2021

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用户向 Siri 提问时或在托管 iOS 设备上听写文本时，Apple 将收集语音数据以改进 Siri 的功能。语音数据通过 Apple 的基于云的服务传输，因此存在于安全的 Endpoint Management 容器外部。但是，由听写产生的文本仍保留在容器内部。

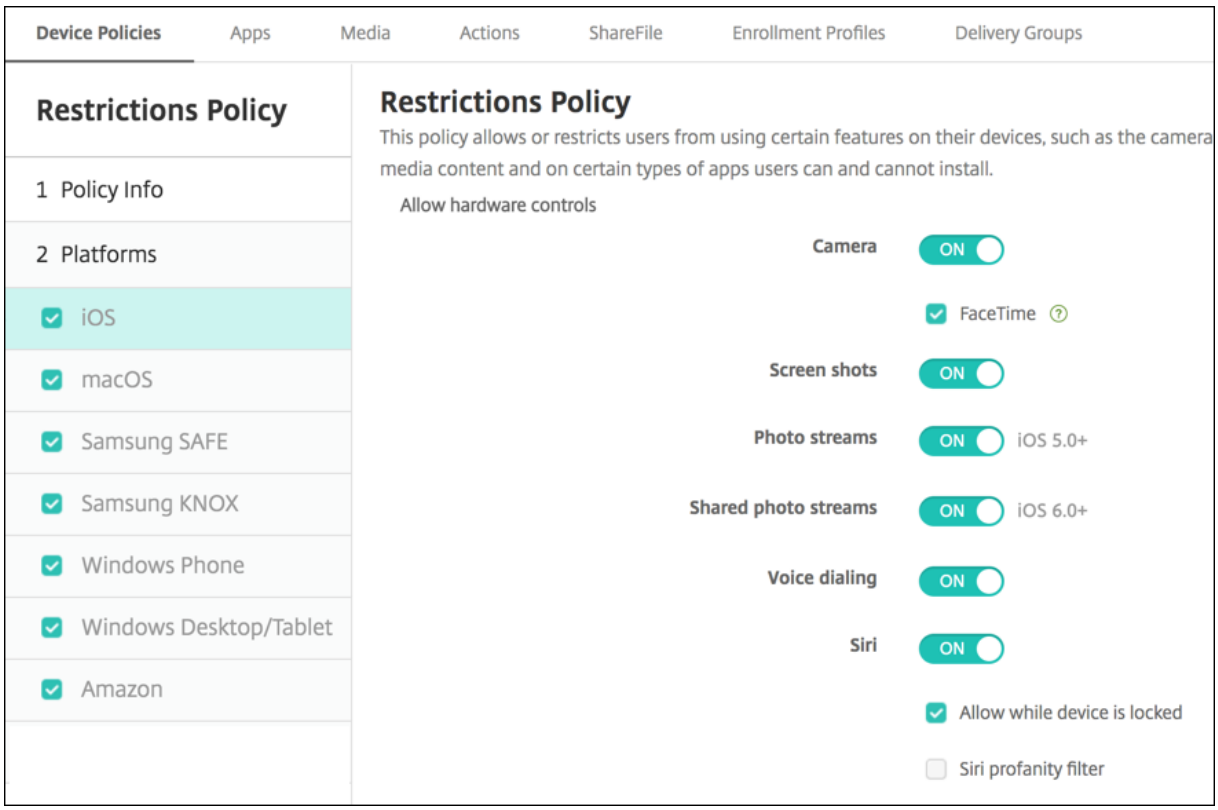
Endpoint Management 允许您根据安全性要求阻止 Siri 和听写服务。

在 MAM 部署中，默认情况下，每个应用程序的阻止听写策略均为开，表示禁用设备的麦克风。如果要允许听写，则将其设置为关。可以在 Endpoint Management 控制台中的配置 **>** 应用程序下找到该策略。选择应用程序，单击编辑，然后单击 **iOS**。



在 MDM 部署中，还可以通过配置 **>** 设备策略下的 Siri 策略禁用 Siri。默认允许使用 Siri。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



决定是否允许使用 Siri 和听写服务时，需要谨记以下几点事项：

- 根据 Apple 公开发布的信息，Apple 最长将保留 Siri 和听写语音数据两年时间。该数据将被分配一个随机编号以代表用户，并且语音文件与此随机编号相关联。
- 可以在任何 iOS 设备上转至设置 **>** 常规 **>** 键盘并轻按启用听写下方的链接来查看 Apple 隐私政策。

SSO 帐户设备策略

March 31, 2022

SSO 帐户设备策略设备策略允许您在 Endpoint Management 中创建单点登录 (SSO) 帐户。这些帐户允许用户仅一次性登录即可从各种应用程序访问 Endpoint Management 和内部公司资源。用户无需在设备上存储任何凭据。可以跨应用程序（包括 App Store 中的应用程序）使用此 SSO 帐户企业用户凭据。此策略专为 Kerberos 身份验证后端设计。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 帐户名称：输入显示在用户设备上的 Kerberos SSO 帐户名称。此字段为必填字段。
- **Kerberos** 主体名称：输入 Kerberos 主体名称。此字段为必填字段。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 身份凭据 **(**密钥库或 **PKI** 凭据**)**：在此列表中，单击可用于在无需用户交互的情况下续订 Kerberos 凭据的可选身份凭据。
- **Kerberos** 领域：输入此策略的 Kerberos 领域。这通常是您的域名，所有字母均大写（例如，EXAMPLE.COM）。此字段为必填字段。
- 允许访问的 **URL**：对于需要 SSO 的每个 URL，单击添加，然后执行以下操作：
  - 允许访问的 **URL**：输入当用户从 iOS 设备访问时需要 SSO 的 URL。
    例如，当用户尝试浏览某个站点，且该 Web 站点发起 Kerberos 质询时：如果该站点不在此 URL 列表中，iOS 设备将不会通过提供 Kerberos 在以前的 Kerberos 登录中缓存到设备上的 Kerberos 令牌来尝试 SSO。URL 的主机部分必须完全匹配。例如，`https://shopping.apple.com` 有效，但 `https://*.apple.com` 无效。
    此外，如果 Kerberos 未基于主机匹配激活，URL 将仍然回退到标准 HTTP 调用。如果 URL 仅配置为使用 Kerberos 实现 SSO，这可能意味着一切，包括标准密码质询或 HTTP 错误。
  - 单击添加以添加 URL，或单击取消以取消添加 URL。
- 应用程序标识符：对于允许使用此登录的每个应用程序，单击添加，然后执行以下操作：
  - 应用程序标识符：输入允许使用此登录的应用程序的应用程序标识符。如果不添加任何应用程序标识符，此登录将匹配所有应用程序标识符。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

应用商店设备策略

March 31, 2022

可以在 Endpoint Management 中创建策略，以指定设备是否在主屏幕上显示应用商店 Web 剪辑。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS、Android 和 Windows Desktop/Tablet 设置

对于配置的每个平台，选择是否在用户设备上显示应用商店 Web 剪辑。默认值为开。

已订阅的日历设备策略

March 31, 2022

可以在 Endpoint Management 中添加一个设备策略，用于在 iOS 设备上将已订阅的日历添加日历列表中。Apple 支持站点上的“下载”中提供了您可以订阅的公共日历列表。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

必备条件

必须已经订阅某个日历，才能在用户设备上将其添加到已订阅的日历列表中。

iOS 设置

- 说明：输入日历的说明。此字段为必填字段。
- **URL**：输入日历 URL。可以输入 iCalendar 文件 (.ics) 的 `webcal://` URL 或 `https://` 链接。此字段为必填字段。
- 用户名：输入用户的登录名称。此字段为必填字段。
- 密码：输入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到日历。默认值为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

条款和条件设备策略

August 8, 2023

如果希望用户接受贵公司用于控制企业网络连接的特定政策，可以在 Endpoint Management 中创建条款和条件设备策略。当用户向 Endpoint Management 注册其设备时，系统会向其显示条款和条件，用户必须接受这些条款和条件才能注册其设备。拒绝这些条款和条件会取消注册过程。

如果贵公司具有国际用户，并且希望用户接受采用其本地语言描述的条款和条件，则可以采用不同的语言创建不同的条款和条件策略。必须为计划部署的每个平台和语言组合提供一个文件。对于 Android 和 iOS 设备，必须提供 PDF 文件。对于 Windows 设备，必须提供文本 (.txt) 文件和随附的图像文件。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 和 **Android** 设置

- 要导入的文件：单击浏览并导航到要导入的条款和条件文件所在位置，选择此文件。
- 默认条款和条件：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。默认值为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 如果通过设备注册计划 (DEP) 注册 iOS 设备，则不显示条款和条件。

Windows Tablet 设置

- 要导入的文件：单击浏览并导航到要导入的条款和条件文件所在位置，选择此文件。
- 图片：单击浏览并导航到要导入的图片文件所在位置，选择此文件。
- 默认条款和条件：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。默认值为关。

通道设备策略

March 31, 2022

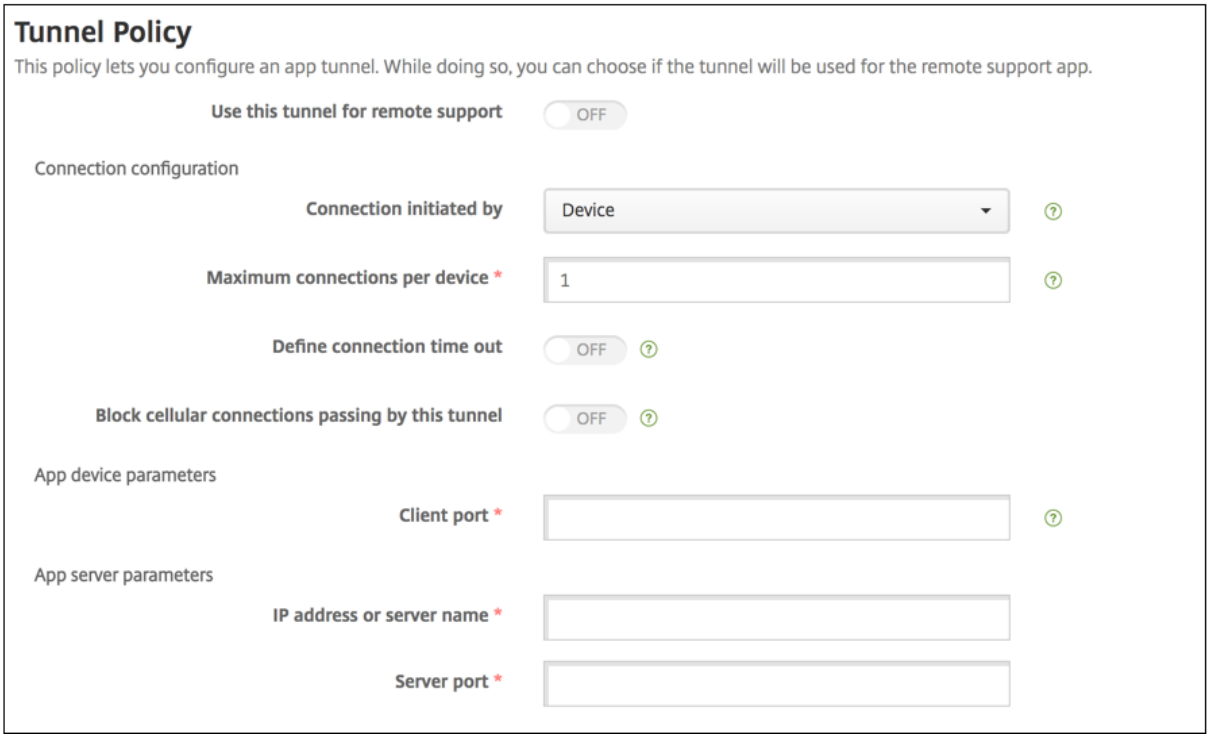
应用程序通道旨在提高移动应用程序的服务连续性及数据传输可靠性。应用程序通道定义移动设备应用程序的客户端组件与应用程序服务器组件之间的代理参数。可以为 Android 设备配置通道策略。

通过在此策略中定义的通道发送的任何应用程序流量均先通过 Endpoint Management，然后再被重定向到运行此应用程序的服务器。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android 设置



- 连接发起者：单击设备或服务器以指定发起连接的源。
- 每台设备最大连接数：键入一个数字，用于指定应用程序可以建立的并发 TCP 连接数。此字段仅适用于设备发起的连接。
- 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
  - 连接超时：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度（秒）。
- 阻止手机网络连接通过此通道：选择是否在漫游时阻止此通道。不会阻止 WiFi 和 USB 连接。
- 客户端端口：键入客户端端口号。在大多数情况下，此值与服务器端口相同。
- **IP** 地址或服务器名称：键入应用程序服务器的 IP 地址或名称。此字段仅适用于设备发起的连接。
- 服务器端口：键入服务器端口号。

VPN 设备策略

July 24, 2023

VPN 设备策略用于配置虚拟专用网络 (VPN) 设置，这些设置使用户设备能够安全地连接到企业网络。可以为以下平台配置 VPN 设备策略。每种平台需要一组不同的值，本文将对此进行详细介绍。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

PerApp VPN 的要求

可以通过 VPN 策略为以下平台配置 PerApp VPN 功能：

- iOS
- macOS
- Android（旧版 DA）

对于 Android Enterprise，请使用“托管配置”设备策略配置 VPN 配置文件。

PerApp VPN 选项可用于某些连接类型。下表显示了 PerApp VPN 选项何时可用。

平台	连接类型	备注
iOS	Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix SSO 或 Custom SSL。	
macOS	Cisco AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA 或 Custom SSL。	
Android（旧版 DA）	Citrix SSO	

要使用 Citrix SSO 应用程序为 iOS 和 Android（旧版 DA）设备创建 PerApp VPN，则除了 VPN 策略配置外，您还需要执行额外的步骤。此外，必须验证是否满足以下必备条件：

- 本地 Citrix Gateway
- 设备上安装了以下应用程序：
  - Citrix SSO
  - Citrix Secure Hub

使用 Citrix SSO 应用程序为 iOS 和 Android 设备配置 PerApp VPN 的一般工作流程如下：

1. 按本文中所述配置 VPN 设备策略。
   - 对于 iOS，请参阅为 iOS 配置 Citrix SSO 协议。通过 VPN 设备策略为 iOS 配置 Citrix SSO 协议后，还需要创建应用程序属性策略以将应用程序与 PerApp VPN 策略相关联。有关更多信息，请参阅 配置每个应用程序的 VPN。
     - 对于连接的身份验证类型字段，如果选择证书，则必须首先为 Endpoint Management 配置基于证书的身份验证。请参阅 客户端证书或证书加域身份验证。
   - 对于 Android（旧版 DA），请参阅 配置适用于 Android 的 Citrix SSO 协议。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

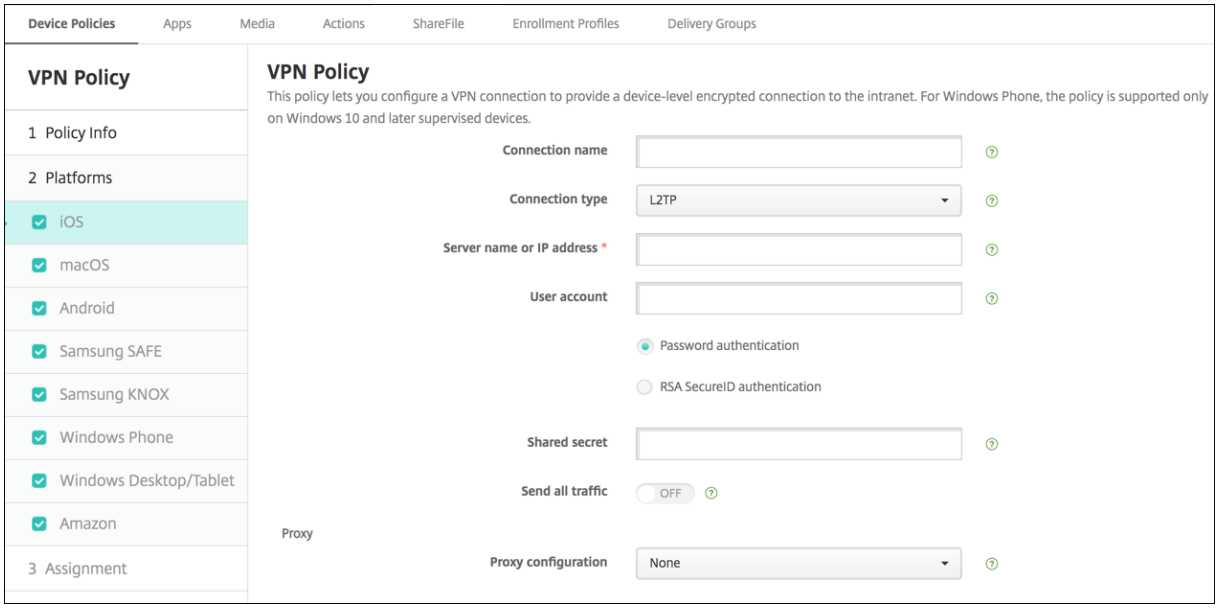
- 对于连接的身份验证类型字段，如果选择证书或密码和证书，则必须首先为 Endpoint Management 配置基于证书的身份验证。请参阅 客户端证书或证书加域身份验证。

2. 将 Citrix ADC 配置为接受来自 PerApp VPN 的流量。有关详细信息，请参阅 Citrix Gateway 上的完整 VPN 设置。

iOS 设置

适用于 iOS 的 VPN 设备策略中的 Citrix VPN 连接类型不支持 iOS 12。执行以下步骤可删除现有 VPN 设备策略并使用 Citrix SSO 连接类型创建 VPN 设备策略：

1. 删除适用于 iOS 的 VPN 设备策略。
2. 使用以下设置添加适用于 iOS 的 VPN 设备策略：
   - 连接类型： **Citrix SSO**
   - 启用 **PerApp VPN**：开
   - 提供程序类型：数据包通道
3. 添加适用于 iOS 的“应用程序属性”设备策略。对于 **PerApp VPN** 标识符，请选择 **iOS_VPN**。



- 连接名称：键入连接的名称。
- 连接类型：在列表中，选择将用于此连接的协议。默认值为 **L2TP**。
  - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
  - **PPTP**：点对点通道。
  - **IPSec**：企业 VPN 连接。
  - **Cisco Legacy AnyConnect**：此连接类型要求在用户设备上安装 Cisco Legacy AnyConnect VPN 客户端。Cisco 正在分阶段淘汰基于现已弃用的 VPN 框架的 Cisco Legacy AnyConnect 客户端。
    要使用当前的 Cisco AnyConnect 客户端，请使用连接类型自定义 **SSL**。对于必需的设置，请参阅本节中的“配置自定义 SSL 协议”。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - **Juniper SSL**： Juniper Networks SSL VPN 客户端。
  - **F5 SSL**： F5 Networks SSL VPN 客户端。
  - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。
  - **Ariba VIA**： Ariba Networks Virtual Internet Access 客户端。
  - **IKEv2**（仅限 **iOS**）：仅限适用于 iOS 的 Internet 密钥交换 2 版。
  - **AlwaysOn IKEv2**：总是使用 IKEv2 进行访问。
  - **AlwaysOn IKEv2** 双配置：总是使用 IKEv2 双配置进行访问。
  - **Citrix SSO**：适用于 iOS 12 及更高版本的 Citrix SSO 客户端。
  - 自定义 **SSL**：自定义安全套接字层。捆绑包 ID 为 **com.cisco.anyconnect** 的 Cisco AnyConnect 客户端需要使用此连接类型。指定连接名称为 **Cisco AnyConnect**。还可以部署 VPN 策略并为 iOS 设备启用网络访问控制 (NAC) 过滤器。该过滤器阻止安装了不合规应用程序的设备建立 VPN 连接。配置需要 iOS VPN 策略的特定设置，如下面的 iOS 部分中所述。有关启用 NAC 筛选器所需的其他设置的详细信息，请参阅 网络访问控制。

以下各节列出了前面每种连接类型的配置选项。

为 **iOS** 配置 **L2TP** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 选择密码身份验证或 **RSA SecurID** 身份验证。
- 共享机密：键入 IPsec 共享密钥。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **iOS** 配置 **PPTP** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 选择密码身份验证或 **RSA SecurID** 身份验证。
- 加密级别：在列表中，选择一种加密级别。默认值为无。
  - 无：不使用加密。
  - 自动：使用服务器支持的最强加密级别。
  - 最大 **(128** 位**)**：始终使用 128 位加密。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **iOS** 配置 **IPsec** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择共享机密或证书以选择此连接的身份验证类型。默认值为共享机密。
- 如果启用共享机密，请配置以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 组名称：键入可选组名称。
  - 共享机密：键入可选共享密钥。
  - 使用混合身份验证：选择是否使用混合身份验证。利用混合身份验证，服务器首先向客户端验证自己的身份，然后客户端向服务器验证自己的身份。默认值为关。
  - 提示输入密码：选择是否在用户连接到网络时提示用户输入其密码。默认值为关。
- 如果启用证书，请配置以下设置：
  - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
  - 连接时提示输入 **PIN**：选择是否在连接到网络时需要用户输入其 PIN。默认值为关。
  - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。
- 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
- **Safari** 域：单击添加可添加 Safari 域名。

为 **iOS** 配置 **Cisco** 旧版 **AnyConnect** 协议

要从 Cisco 旧版 AnyConnect 客户端转换到新的 Cisco AnyConnect 客户端，请使用自定义 SSL 协议。

- 提供程序捆绑包标识符：对于 Legacy AnyConnect 客户端，捆绑包 ID 为 com.cisco.anyconnect.gui。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 组：键入可选组名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 包括所有网络：选择是否允许所有网络使用此连接。默认值为关。
- 排除本地网络：选择不允许本地网络使用连接，还是允许本地网络使用连接。默认值为关。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

为 **iOS** 配置 **Juniper SSL** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 领域：键入可选领域名称。
- 角色：键入可选角色名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置 “按需启用 VPN” 设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **F5 SSL** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置 “按需启用 VPN” 设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **SonicWALL** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 登录组或域：键入可选登录组或域。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    * 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置 “按需启用 VPN” 设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果将此选项设置为 “开”，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **Ariba VIA** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    * 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **IKEv2** 协议

本节包括用于 IKEv2、Always On IKEv2 和 Always On IKEv2 双配置协议的设置。对于 Always On IKEv2 双配置协议，请为手机网络和 Wi-Fi 网络配置所有这些设置。

- 允许用户禁用自动连接：面向 Always On 协议。选择是否允许用户禁用与其设备上的网络的自动连接。默认值为关。
- 服务器的主机名或 **IP** 地址：键入 VPN 服务器的主机名或 IP 地址。
- 本地标识符： IKEv2 客户端的 FQDN 或 IP 地址。此字段为必填字段。
- 远程标识符： VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
- 设备身份验证：为此连接的身份验 证类型选择 共享密钥、证书或基于设备标识符的设备证书。默认值为共享机密。
  - 如果选择共享机密，请键入可选共享密钥。
  - 如果选择证书，请选择要使用的身份凭据。默认值为无。
  - 如果选择基于设备标识符的设备证书，请选择要使用的设备标识类型。默认值为 **IMEI**。要使用此选项，请使用 REST API 批量导入证书。请参阅使用 REST API 批量上传证书。仅当您选择 **Always On IKEv2**（始终启用 IKEv2）时才可用。
- 已启用扩展身份验证：选择是否启用扩展身份验证协议 (EAP)。如果设置为开，请键入用户帐户和身份验证密码。
- 失效对等体检测时间间隔：选择联系对等设备以确保对等设备仍可访问的频率。默认值为无。选项包括：
  - 无：禁用失效对等体检测。
  - 低：每 30 分钟联系一次对等体。
  - 中：每 10 分钟联系一次对等体。
  - 高： 1 分钟联系一次对等体。
- 禁用移动性和多宿主：选择是否禁用此功能。
- 使用 **IPv4/IPv6** 内部子网属性：选择是否启用此功能。
- 禁用重定向：选择是否禁用重定向。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Enable Fallback**（启用回退）：如果启用，此设置将允许通道通过蜂窝移动数据传输符合 Wi-Fi 助理的条件且需要 VPN 的流量。默认设置为关。
- 设备在睡眠状态下启用 **NAT** 保持连接：面向 Always On 协议。保持连接数据包维护 IKEv2 连接的 NAT 映射。芯片在设备处于唤醒状态时定期发送这些数据包。如果此设置设为开，即使设备处于睡眠状态时，芯片也会发送保持连接数据包。通过 Wi-Fi 传输时，默认时间间隔为 20 秒，通过手机网络传输时为 110 秒。可以使用 NAT 保持连接时间间隔参数更改时间间隔。
- **NAT** 保持连接时间间隔 **(**秒**)**：默认值为 20 秒。
- 启用完全向前保密：选择是否启用此功能。
- **DNS** 服务器 **IP** 地址：可选。DNS 服务器 IP 地址字符串的列表。这些 IP 地址可以包括 IPv4 和 IPv6 地址的混合。单击添加可键入地址。
- 域名：可选。通道的主域。
- 搜索域：可选。用于完全限定单标签主机名的域字符串的列表。
- 将补充匹配域附加到解析程序列表：可选。确定是否将补充匹配域列表添加到解析程序的搜索域列表。默认值为开。
- 补充匹配域：可选。用于确定要使用 DNS 服务器地址中包含的 DNS 解析程序设置的 DNS 查询的域字符串的列表。此键将创建一个拆分 DNS 配置，在该配置中，只有某些域中的主机才能使用通道的 DNS 解析程序进行解析。不在此列表的其中一个域中的主机将使用系统的默认解析程序进行解析。

如果此参数包含一个空字符串，该字符串将为默认域。因此，拆分通道配置可以将所有 DNS 查询先定向到 VPN DNS 服务器，然后再定向到主 DNS 服务器。如果 VPN 通道为网络的默认路由，列出的 DNS 服务器将成为默认解析程序。在这种情况下，补充匹配域列表将被忽略。

- **IKE SA** 参数和子 **SA** 参数：为每个安全关联 (SA) 参数选项配置以下设置：
  - 加密算法：在此列表中，选择要使用的 IKE 加密算法。默认值为 **3DES**。
  - 完整性算法：在列表中，选择要使用的完整性算法。默认值为 **SHA-256**。
  - **Diffie Hellman** 组：在列表中，选择 Diffie Hellman 组号。默认值为 **2**。
  - **IKE** 生存时间 **(**分钟**)**：键入 10 至 1440 之间的整数，表示 SA 生存时间（重新生成密钥时间间隔）。默认值为 **1440** 分钟。
- 服务异常：面向 Always On 协议。服务异常是指不通过 Always On VPN 运行的系统服务。请配置以下服务异常设置：
  - 语音邮件：在列表中，选择处理语音邮件异常的方式。默认值为允许通过通道传输流量。
  - **AirPrint**：在列表中，选择处理 AirPrint 异常的方式。默认值为允许通过通道传输流量。
  - 允许在 **VPN** 通道外部传输来自强制 **Web** 表格的流量：选择是否允许用户在 VPN 通道外部连接到公共热点。默认值为关。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 允许在 **VPN** 通道外部传输来自所有强制联网应用程序的流量：选择是否允许在 VPN 通道外部打开所有热点网络应用程序。默认值为关。
  - 强制联网应用程序捆绑包标识符：对于允许用户访问的每个热点网络应用程序捆绑包标识符，单击添加并键入热点网络应用程序捆绑包标识符。单击保存以保存该应用程序捆绑包标识符。

- **PerApp VPN**：为 IKEv2 连接类型配置这些设置。
  - 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：单击添加可添加 Safari 域名。
- 代理配置：选择 VPN 连接通过代理服务器进行路由的方式。默认值为无。

为 **iOS** 配置 **Citrix SSO** 协议

Citrix SSO 客户端可从 Apple Store 获取。

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    * 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果将此选项设置为“开”，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - 提供程序类型：设置为数据包通道。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。
- 自定义 **XML**：对于要添加的每个自定义 XML 参数，请单击添加并指定键/值对。可用参数如下：
  - **disableL3**：禁用系统级 VPN。仅允许使用 PerApp VPN。不需要任何值。
  - 用户代理：将目标为 VPN 插件客户端的任何 Citrix Gateway 策略与此设备策略相关联。对于插件发起的请求，此键的值会自动添加到 VPN 插件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

为 **iOS** 配置自定义 **SSL** 协议

要从 Cisco Legacy AnyConnect 客户端转换为 Cisco AnyConnect 客户端，请执行以下操作：

1. 通过自定义 SSL 协议配置 VPN 设备策略。将该策略部署到 iOS 设备。
2. 从 https://apps.apple.com/us/app/cisco-secure-client/id1135064690 上载 Cisco AnyConnect 客户端，将该应用程序添加到 Endpoint Management，然后再将其部署到 iOS 设备。
3. 从 iOS 设备中删除旧 VPN 设备策略。

设置：

- 自定义 **SSL** 标识符 **(**反向 **DNS** 格式**)**：设置为捆绑包标识符。对于 Cisco AnyConnect 客户端，请使用 **com.cisco.anyconnect**。
- 提供程序捆绑包标识符：如果在自定义 **SSL** 标识符中指定的应用程序具有多个类型相同（应用程序代理或数据包通道）的 VPN 提供程序，请指定此捆绑包标识符。对于 Cisco AnyConnect 客户端，请使用 **com.cisco.anyconnect**。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 包括所有网络：选择是否允许所有网络使用此连接。默认值为关。
- 排除本地网络：选择不允许本地网络使用连接，还是允许本地网络使用连接。默认值为关。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果将此选项设置为“开”，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
  - 提供程序类型：提供程序类型指示提供程序是 VPN 服务还是代理服务。对于 VPN 服务，请选择数据包通道。对于代理服务，请选择应用程序代理。对于 Cisco AnyConnect 客户端，请选择数据包通道。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。
- 自定义 **XML**：对于要添加的每个自定义 XML 参数，请单击添加并执行以下操作：
  - 参数名称：键入要添加的参数的名称。
  - 值：键入与参数名称关联的值。
  - 单击保存以保存参数，或者单击取消不保存参数。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置 **VPN** 设备策略以支持 **NAC**

1. 配置 NAC 过滤器所需的连接类型为自定义 **SSL**。
2. 指定连接名称为 **VPN**。
3. 对于自定义 **SSL** 标识符，请键入 **com.citrix.NetScalerGateway.ios.app**
4. 对于提供程序捆绑包标识符，请键入 **com.citrix.NetScalerGateway.ios.app.vpnplugin**

步骤 3 和 4 中的值来自 NAC 过滤所需的 Citrix SSO 安装。请勿配置身份验证密码。有关使用 NAC 功能的详细信息，请参阅 网络访问控制。

为 **iOS** 配置 **"**按需启用 **VPN"** 选项

- 按需域：对于每个域以及当用户连接时要执行的关联操作，请单击添加并执行以下操作：
- 域：键入要添加的域。
- 操作：在列表中，选择其中一项可能采取的操作：
  - 始终建立：域始终触发 VPN 连接。
  - 从不建立：域从不触发 VPN 连接。
  - 必要时建立：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。
  - 单击保存以保存域，或者单击取消不保存域。
- 按需规则
  - 操作：在列表中，选择要采取的操作。默认值为 **EvaluateConnection**。可能的操作包括：
    - 允许：允许在触发时 VPN 按需进行连接。
    - 连接：无条件启动 VPN 连接。
    - 断开连接：删除 VPN 连接并且在规则匹配时不按需重新连接。
    - **EvaluateConnection**：评估每个连接的 ActionParameters 阵列。
    - 忽略：保持任何现有 VPN 连接，并且在规则匹配时不按需重新连接。
  - **DNSDomainMatch**：对于要添加且设备的搜索域列表可以与之匹配的每个域，请单击添加并执行以下操作：
    - **DNS** 域：键入域名。可以使用通配符 "*" 前缀来匹配多个域。例如，*.example.com 匹配 mydomain.example.com、yourdomain.example.com 和 herdomain.example.com。
    - 单击保存以保存域，或者单击取消不保存域。
  - **DNSServerAddressMatch**：对于要添加且网络的任何指定 DNS 服务器可以匹配的每个 IP 地址，请单击添加并执行以下操作：
    - **DNS** 服务器地址：键入要添加的 DNS 服务器地址。可以使用通配符 "*" 后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的所有 DNS 服务器。
    - 单击保存以保存 DNS 服务器地址，或者单击取消不保存 DNS 服务器地址。
  - **InterfaceTypeMatch**：在列表中，选择使用的主要网络接口硬件的类型。默认值为未指定。可能的值包括：
    - 未指定：匹配任何网络接口硬件。此选项是默认选项。
    - 以太网：仅匹配以太网网络接口硬件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * **WiFi**：仅匹配 Wi-Fi 网络接口硬件。
    * 手机网络：仅匹配手机网络网络接口硬件。
  - **SSIDMatch**：对于要添加且匹配当前网络的每个 SSID，请单击添加并执行以下操作。
    * **SSID**：键入要添加的 SSID。如果网络不是 Wi-Fi 网络，或者如果 SSID 未出现，匹配将失败。将此列表留空可匹配任何 SSID。
    * 单击保存以保存 SSID，或单击取消不保存 SSID。
  - **URLStringProbe**：键入要提取的 URL。如果此 URL 在未经重定向的情况下成功提取，此规则匹配。
  - **ActionParameters : Domains**：对于要添加且 EvaluateConnection 检查的每个域，请单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。
  - **ActionParameters : DomainAction**：在列表中，选择指定的 **ActionParameters : Domains** 域的 **VPN** 行为。默认值为 **ConnectIfNeeded**。可能的操作包括：
    * **ConnectIfNeeded**：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。
    * **NeverConnect**：域从不触发 VPN 连接。
  - **ActionParameters: RequiredDNSServers**：对于要用于解析指定域的每个 DNS 服务器，请单击添加并执行以下操作：
    * **DNS** 服务器：仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。键入 DNS 服务器 IP 地址。此服务器可以位于设备的当前网络配置之外。如果无法访问 DNS 服务器，作为响应，将建立 VPN 连接。确保此 DNS 服务器是内部 DNS 服务器或可信的外部 DNS 服务器。
    * 单击保存以保存 DNS 服务器，或者单击取消不保存 DNS 服务器。
  - **ActionParameters : RequiredURLStringProbe**：（可选）键入使用 GET 请求探查的 HTTP 或 HTTPS（首选）URL。如果无法解析 URL 的主机名、服务器无法访问或者服务器不响应，则建立 VPN 连接。仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。
  - **OnDemandRules : XML content**：键入或复制并粘贴 XML 按需配置规则。
    * 单击检查字典验证 XML 代码。如果 XML 有效，有效 **XML** 将显示在 **XML** 内容文本框下方。如果无效，系统将显示一条错误消息来描述该错误。

- 代理
  - 代理配置：在列表中，选择 VPN 连接通过代理服务器进行路由的方式。默认值为无。
    * 如果启用手动，请配置以下设置：
      · 代理服务器的主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
      · 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。
      · 用户名：键入可选代理服务器用户名。
      · 密码：键入可选代理服务器密码。
    * 如果配置自动，请配置以下设置：
      · 代理服务器 **URL**：键入代理服务器的 URL。此字段为必填字段。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

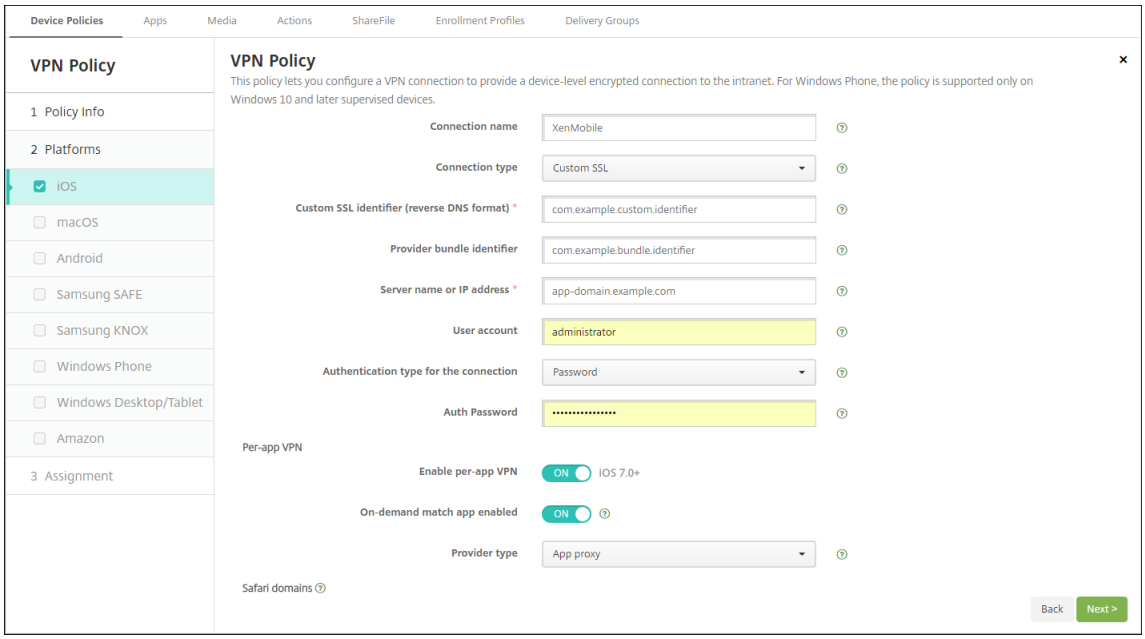
* 选择日期：单击日历可选择具体删除日期。
* 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

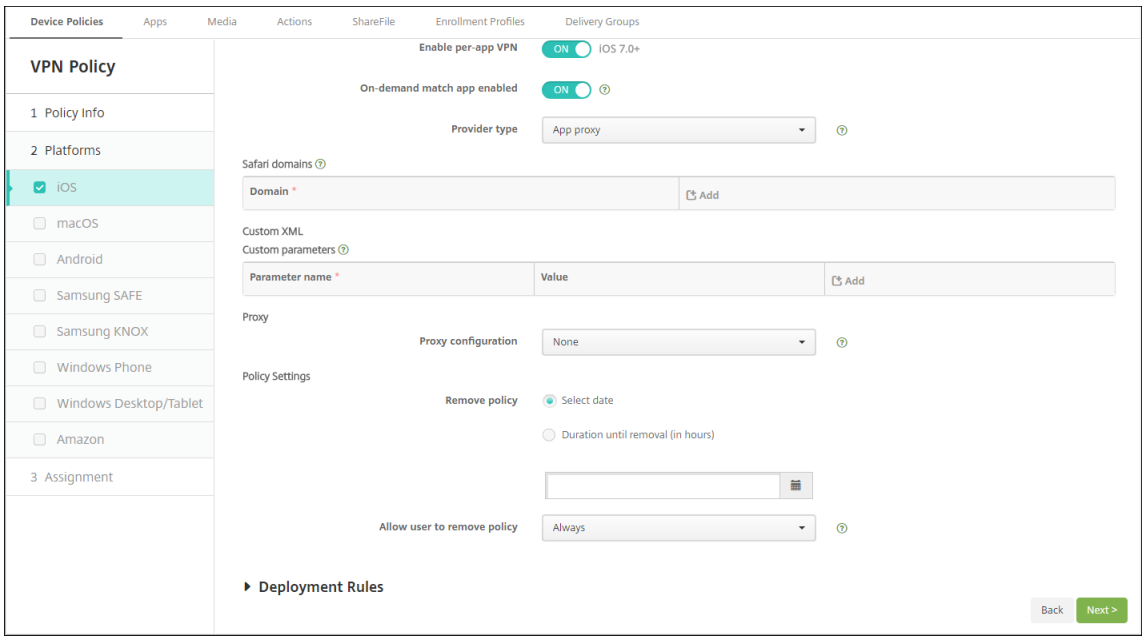
配置 **PerApp VPN**

iOS 的 PerApp VPN 选项适用于以下连接类型：Cisco 旧版 AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix VPN、Citrix SSO 和自定义 SSL。

要配置 PerApp VPN，请执行以下操作：

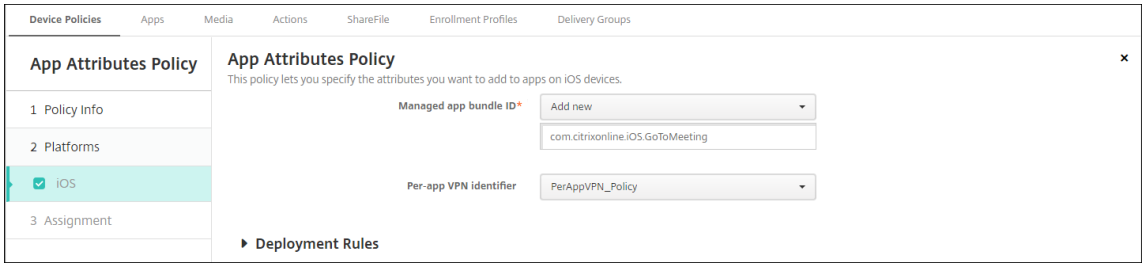
1. 在配置 **>** 设备策略中，创建 VPN 策略。例如：



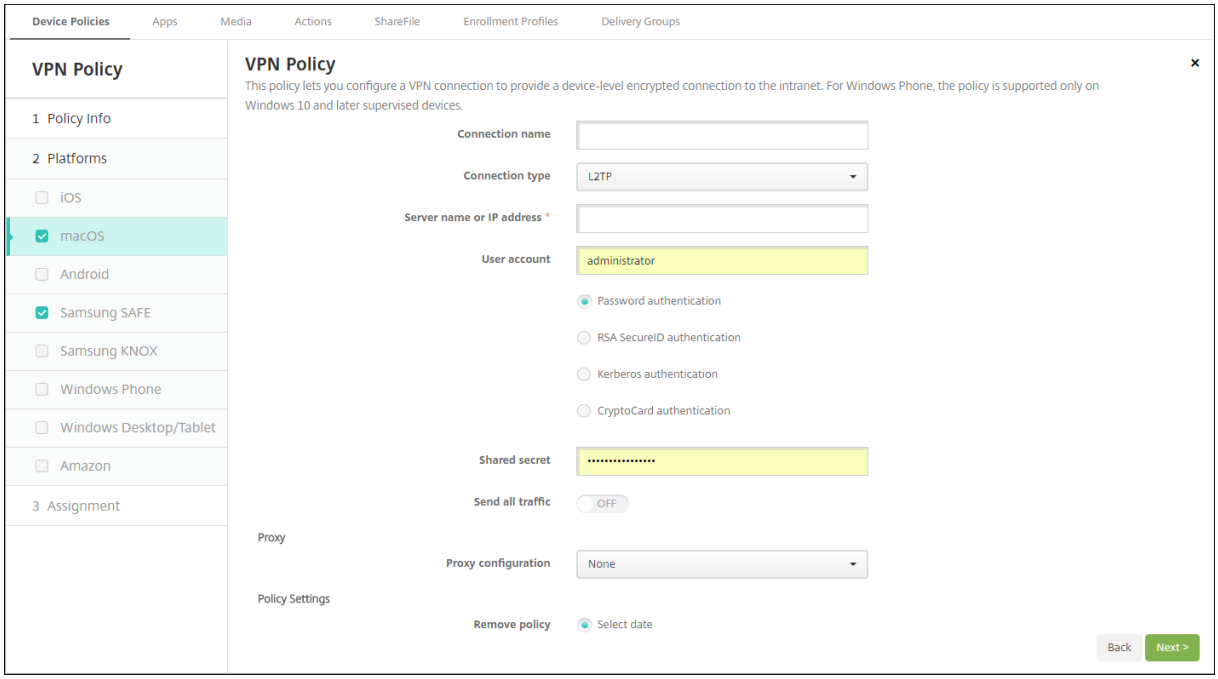


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 在配置 **>** 设备策略中，创建应用程序属性策略以将应用程序与 PerApp VPN 策略相关联。对于 **PerApp VPN** 标识符，请选择在步骤 1 中创建的 VPN 策略的名称。对于托管应用程序捆绑包 **ID**，请从应用程序列表中进行选择，或者键入应用程序捆绑包 ID。（如果部署了 iOS 的应用程序清单策略，应用程序列表将包含应用程序。）



macOS 设置



- 连接名称：键入连接的名称。
- 连接类型：在列表中，选择将用于此连接的协议。默认值为 L2TP。
  - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
  - **PPTP**：点对点通道。
  - **IPSec**：企业 VPN 连接。
  - **Cisco AnyConnect**： Cisco AnyConnect VPN 客户端。
  - **Juniper SSL**： Juniper Networks SSL VPN 客户端。
  - **F5 SSL**： F5 Networks SSL VPN 客户端。
  - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。
  - **Ariba VIA**： Ariba Networks Virtual Internet Access 客户端。
  - **Citrix VPN**： Citrix VPN 客户端。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 自定义 **SSL**：自定义安全套接字层。

以下各节列出了前面每种连接类型的配置选项。

为 **macOS** 配置 **L2TP** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 选择密码身份验证、**RSA SecurID** 身份验证、**Kerberos** 身份验证或 **CryptoCard** 身份验证。默认值为密码身份验证。
- 共享机密：键入 IPsec 共享密钥。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **macOS** 配置 **PPTP** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 选择密码身份验证、**RSA SecurID** 身份验证、**Kerberos** 身份验证或 **CryptoCard** 身份验证。默认值为密码身份验证。
- 加密级别：选择所需的加密级别。默认值为无。
  - 无：不使用加密。
  - 自动：使用服务器支持的最强加密级别。
  - 最大 **(128** 位**)**：始终使用 128 位加密。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **macOS** 配置 **IPsec** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择共享机密或证书以选择此连接的身份验证类型。默认值为共享机密。
  - 如果启用共享机密身份验证，请配置以下设置：
    - 组名称：键入可选组名称。
    - 共享机密：键入可选共享密钥。
    - 使用混合身份验证：选择是否使用混合身份验证。利用混合身份验证，服务器首先向客户端验证自己的身份，然后客户端向服务器验证自己的身份。默认值为关。
    - 提示输入密码：选择是否在用户连接到网络时提示用户输入其密码。默认值为关。
  - 如果启用证书身份验证，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在连接到网络时需要用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置按需启用 VPN 选项。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

为 **macOS** 配置 **Cisco AnyConnect** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 组：键入可选组名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置按需启用 VPN 选项。
  - 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
    - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
    - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
      - 域：键入要添加的域。
      - 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置 **Juniper SSL** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 领域：键入可选领域名称。
- 角色：键入可选角色名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置按需启用 VPN 选项。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

为 **macOS** 配置 **F5 SSL** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置按需启用 VPN 选项。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置 **SonicWALL** 移动连接协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 登录组或域：键入可选登录组或域。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置按需启用 VPN 选项。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置 **Ariba VIA** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置按需启用 VPN 选项。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置自定义 **SSL** 协议

- 自定义 **SSL** 标识符 **(**反向 **DNS** 格式**)**：以反向 DNS 格式键入 SSL 标识符。此字段为必填字段。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。此字段为必填字段。
- 用户帐户：键入可选用户帐户。
  - 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认值为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置按需启用 VPN 选项。
  - **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
    - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
    - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
      - 域：键入要添加的域。
      - 单击保存以保存域，或者单击取消不保存域。
- 自定义 **XML**：对于要添加的每个自定义 XML 参数，请单击添加并执行以下操作：
  - 参数名称：键入要添加的参数的名称。
  - 值：键入与参数名称关联的值。
  - 单击保存以保存域，或者单击取消不保存域。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置 **“**按需启用 **VPN”** 选项

- 按需域：对于要添加的每个域以及当用户与之连接时要执行的关联操作，请单击添加并执行以下操作：
  - 域：键入要添加的域。
  - 操作：在列表中，选择其中一项可能采取的操作：
    - 始终建立：域始终触发 VPN 连接。
    - 从不建立：域从不触发 VPN 连接。
    - 必要时建立：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。
  - 单击保存以保存域，或者单击取消不保存域。
- 按需规则
  - 操作：在列表中，选择要采取的操作。默认值为 **EvaluateConnection**。可能的操作包括：
    - 允许：允许在触发时 VPN 按需进行连接。
    - 连接：无条件启动 VPN 连接。
    - 断开连接：删除 VPN 连接并且在规则匹配时不按需重新连接。
    - **EvaluateConnection**：评估每个连接的 **ActionParameters** 阵列。
    - 忽略：保持任何现有 VPN 连接，并且在规则匹配时不按需重新连接。
  - **DNSDomainMatch**：对于设备的搜索域列表可以与之匹配的域，请单击添加并执行以下操作：
    - **DNS** 域：键入域名。可以使用通配符 “*” 前缀来匹配多个域。例如，*.example.com 匹配 mydomain.example.com、yourdomain.example.com 和 herdomain.example.com。
    - 单击保存以保存域，或者单击取消不保存域。
  - **DNSServerAddressMatch**：对于要添加且网络的任何指定 DNS 服务器可以匹配的每个 IP 地址，请单击添加并执行以下操作：
    - **DNS** 服务器地址：键入要添加的 DNS 服务器地址。可以使用通配符 “*” 后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的所有 DNS 服务器。
    - 单击保存以保存 DNS 服务器地址，或者单击取消不保存 DNS 服务器地址。
  - **InterfaceTypeMatch**：在列表中，单击使用的主要网络接口硬件的类型。默认值为未指定。可能的值包括：
    - 未指定：匹配任何网络接口硬件。此选项是默认选项。
    - 以太网：仅匹配以太网网络接口硬件。
    - **WiFi**：仅匹配 Wi-Fi 网络接口硬件。
    - 手机网络：仅匹配手机网络网络接口硬件。
  - **SSIDMatch**：对于要添加且匹配当前网络的每个 SSID，请单击添加并执行以下操作。
    - **SSID**：键入要添加的 SSID。如果网络不是 Wi-Fi 网络，或者如果 SSID 未出现，匹配将失败。将此列表留空可匹配任何 SSID。
    - 单击保存以保存 SSID，或单击取消不保存 SSID。
  - **URLStringProbe**：键入要提取的 URL。如果此 URL 在未经重定向的情况下成功提取，此规则匹配。
  - **ActionParameters : Domains**：对于要添加且 EvaluateConnection 检查的每个域，请单击添加并执行以下操作：
    - 域：键入要添加的域。

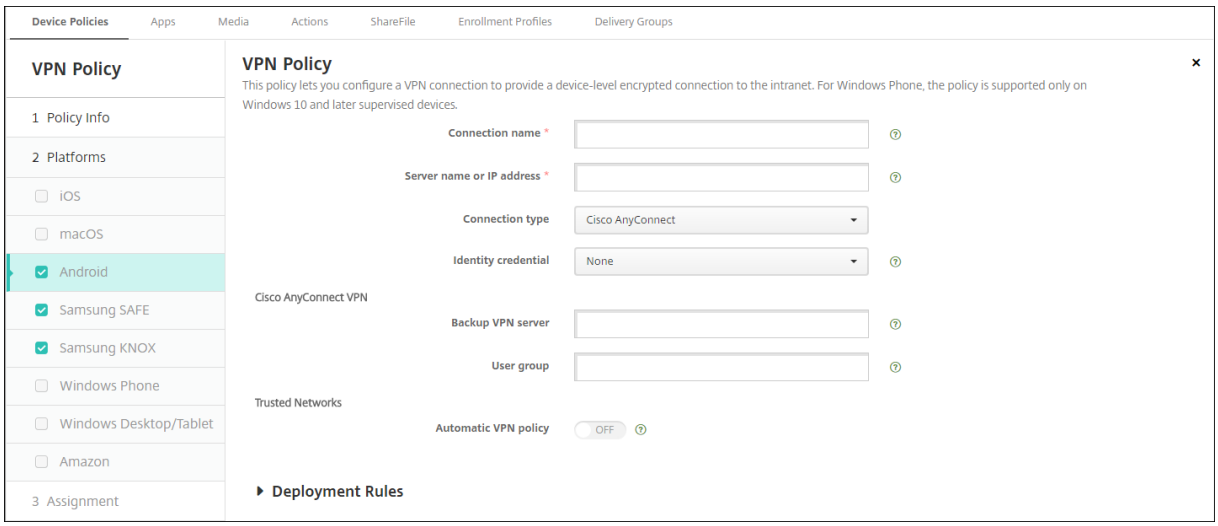
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

    * 单击保存以保存域，或者单击取消不保存域。
  - **ActionParameters : DomainAction**：在列表中，选择指定的 **ActionParameters : Domains** 域的 **VPN** 行为。默认值为 **ConnectIfNeeded**。可能的操作包括：
    * **ConnectIfNeeded**：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。
    * **NeverConnect**：域从不触发 VPN 连接。
  - **ActionParameters: RequiredDNSServers**：对于要用于解析指定域的每个 DNS 服务器，请单击添加并执行以下操作：
    * **DNS** 服务器：仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。键入要添加的 DNS 服务器 IP 地址。此服务器可以位于设备的当前网络配置之外。如果无法访问 DNS 服务器，作为响应，将建立 VPN 连接。此 DNS 服务器必须为内部 DNS 服务器或可信的外部 DNS 服务器。
    * 单击保存以保存 DNS 服务器，或者单击取消不保存 DNS 服务器。
  - **ActionParameters : RequiredURLStringProbe**：（可选）键入使用 GET 请求探查的 HTTP 或 HTTPS（首选）URL。如果无法解析 URL 的主机名、服务器无法访问或者服务器不响应，则建立 VPN 连接。仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。
  - **OnDemandRules : XML** 内容：键入或复制并粘贴 XML 按需配置规则。
    * 单击检查字典验证 XML 代码。如果 XML 有效，有效 **XML** 将显示在 **XML** 内容文本框下方。如果无效，系统将显示一条错误消息来描述该错误。

- 代理
  - 代理配置：在列表中，选择 VPN 连接通过代理服务器进行路由的方式。默认值为无。
    * 如果启用手动，请配置以下设置：
      · 代理服务器的主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
      · 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。
      · 用户名：键入可选代理服务器用户名。
      · 密码：键入可选代理服务器密码。
    * 如果配置自动，请配置以下设置：
      · 代理服务器 **URL**：键入代理服务器的 URL。此字段为必填字段。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    * 选择日期：单击日历可选择具体删除日期。
    * 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android（旧版 **DA**）设置



为 **Android** 配置 **Cisco AnyConnect VPN** 协议

- 连接名称：输入 Cisco AnyConnect VPN 连接的名称。此字段为必填字段。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的名称或 IP 地址。此字段为必填字段。
- 身份凭据：在列表中，选择身份凭据。
- 备份 **VPN** 服务器：键入备份 VPN 服务器信息。
- 用户组：键入用户组信息。
- 可信网络
  - 自动 **VPN** 策略：启用或禁用此选项，以设置 VPN 响应可信网络和不可信网络的方式。如果启用，请配置以下设置：
    - 可信网络策略：在列表中，选择所需的策略。默认值为断开连接。可能的选项包括：
      - 断开连接：客户端终止可信网络中的 VPN 连接。这是默认设置。
      - 连接：客户端在可信网络中启动 VPN 连接。
      - 不执行任何操作：客户端不执行任何操作。
      - 暂停：用户在可信网络外部建立 VPN 会话，然后进入配置为可信的网络时，VPN 会话将挂起。用户再次离开可信网络时，会话恢复。此设置无需在离开可信网络后建立新的 VPN 会话。
    - 不可信网络策略：在列表中，选择所需的策略。默认值为连接。可能的选项包括：
      - 连接：客户端在不可信网络中启动 VPN 连接。
      - 不执行任何操作：客户端在不可信网络中启动 VPN 连接。此选项将禁用始终启用 VPN。
  - 可信域：对于客户端位于可信网络时网络接口拥有的每个域后缀，请单击添加以执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。
  - 可信服务器：对于客户端位于可信网络时网络接口拥有的每个服务器地址，请单击添加并执行以下操作：
    - 服务器：键入要添加的服务器。
    - 单击保存以保存服务器，或者单击取消不保存服务器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

为 **Android** 配置 **Citrix SSO** 协议

- 连接名称：键入 VPN 连接的名称。此字段为必填字段。
- 服务器名称或 **IP** 地址：键入 Citrix Gateway 的 FQDN 或 IP 地址。
- 连接的身份验证类型：选择身份验证类型并填写针对该类型显示的以下字段中的任何字段：
  - 用户名和密码：键入身份验证类型密码或密码和证书的 VPN 凭据。可选。如果未提供 VPN 凭据，Citrix VPN 应用程序将提示输入用户名和密码。
  - 身份凭据：针对身份验证类型证书或密码和证书显示。在列表中，选择身份凭据。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。如果未启用 PerApp VPN，所有流量都将通过 Citrix VPN 通道传输。如果启用 PerApp VPN，请指定以下设置。默认值为关。
  - 允许列表或阻止列表：如果选择允许列表，则允许列表中的所有应用程序都通过此 VPN 传输。如果选择阻止列表，除阻止列表通道中的应用程序以外的所有应用程序都将通过此 VPN 传输。
  - 应用程序列表：允许列表或阻止列表中的应用程序。单击添加，然后键入以逗号分隔的应用程序软件包名称的列表。
- 自定义 **XML**：单击添加，然后键入自定义参数。Endpoint Management 支持 Citrix VPN 的以下参数：
  - **DisableUserProfiles**：可选。要启用此参数，请键入 **Yes** 作为值。如果启用了此参数，Endpoint Management 将不显示用户添加的 VPN 连接，并且用户无法添加连接。此设置属于全局限制，适用于所有 VPN 配置文件。
  - **userAgent**：字符串值。可以指定要在每个 HTTP 请求中发送的自定义用户代理字符串。指定的用户代理字符串附加到现有 Citrix VPN 用户代理。

配置 **VPN** 以支持 **NAC**

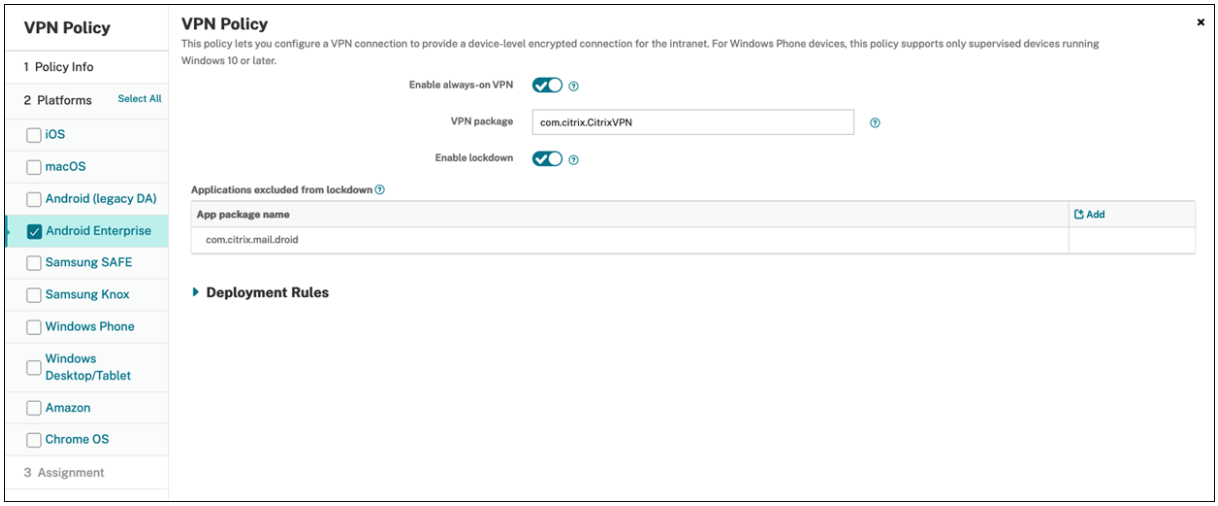
1. 使用连接类型自定义 **SSL** 配置 NAC 过滤器。
2. 指定连接名称为 **VPN**。
3. 对于自定义 **XML**，请单击添加并执行以下操作：
   - 参数名称：键入 **XenMobileDeviceId**。此字段是用于根据 Endpoint Management 中的设备注册进行 NAC 检查的设备 ID。如果 Endpoint Management 注册并管理设备，则允许建立 VPN 连接。否则，在 VPN 建立时将拒绝身份验证。
   - 值：键入 **DeviceID_${device.id}**，该值是参数 **XenMobileDeviceId** 的值。
   - 单击保存保存参数。

为 **Android Enterprise** 配置 **VPN**

要为 Android 企业设备配置 VPN，请为 Citrix SSO 应用程序创建 Android Enterprise 托管配置设备策略。请参阅为 Android Enterprise 配置 VPN 配置文件。

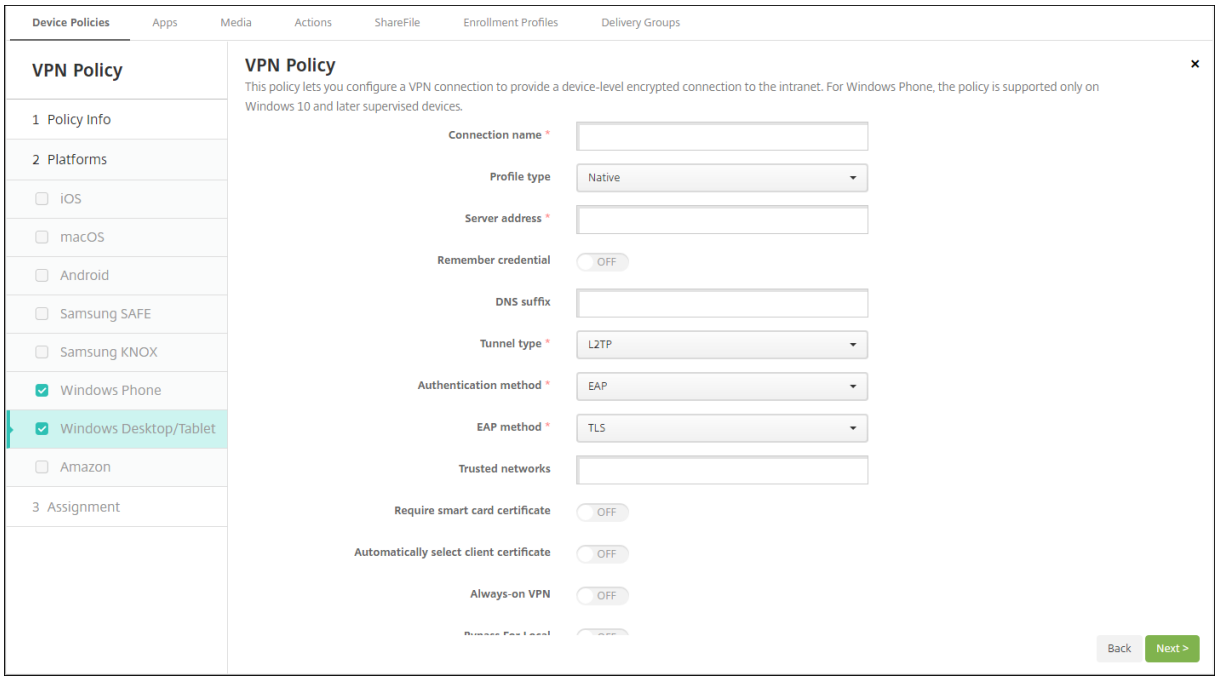
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android Enterprise 设置



- 启用永远在线的 **VPN**：选择 VPN 是否始终处于开启状态。默认值为关。启用后，VPN 连接保持可用，直到用户手动断开连接。
- **VPN** 包键入 VPN 应用程序设备使用的软件包名称。
- 启用锁定：如果禁用，如果 VPN 连接不存在，则没有应用程序可以访问网络。如果启用，您在以下设置中配置的应用程序可以访问网络，即使 VPN 连接不存在。适用于 Android 10 及更高版本的设备。
- **Applications exluded from lockdown**（从锁定中排除的应用程序）：单击 **Add**（添加）键入要绕过锁定设置的应用程序的软件包名称。

Windows Desktop/Tablet 设置

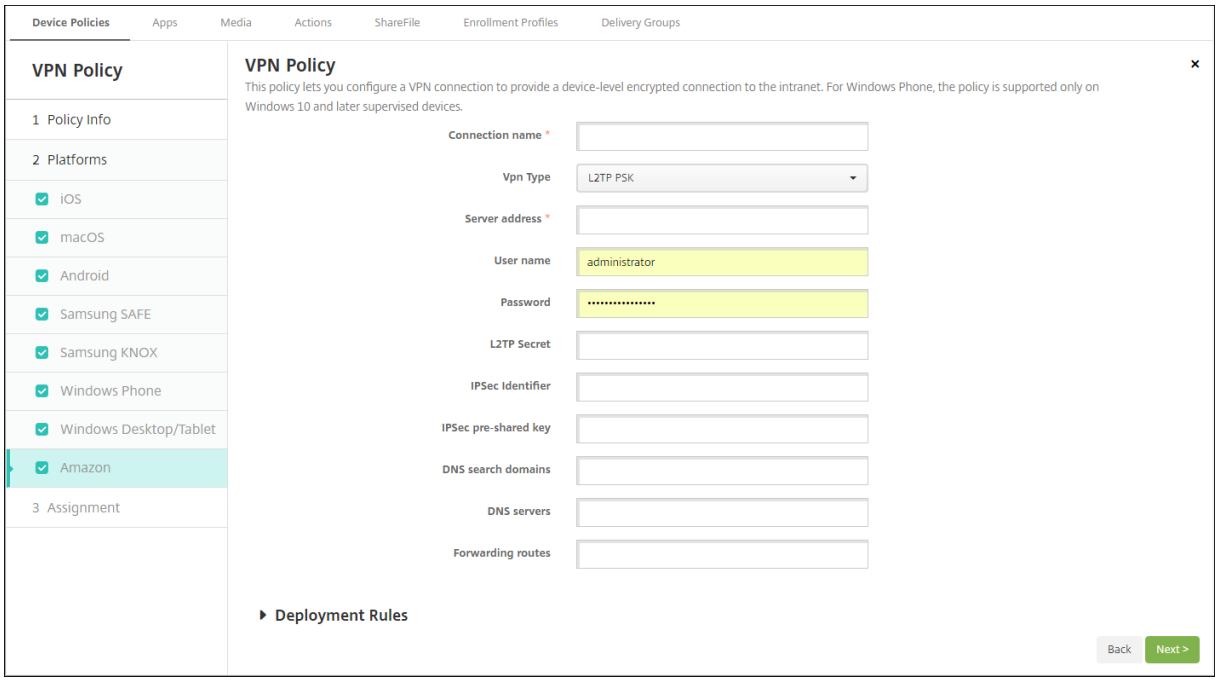


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 连接名称：输入连接的名称。此字段为必填字段。
- 配置文件类型：在列表中，选择本机或插件。默认值为本机。
- 配置本机配置文件类型：这些设置应用于内置于用户 Windows 设备上的 VPN。
  - 服务器地址：键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
  - 记住凭据：选择是否缓存凭据。默认值为关。启用后，会在合适的时候缓存凭据。
  - **DNS** 后缀：键入 DNS 后缀。
  - 通道类型：在列表中，选择要使用的 VPN 通道类型。默认值为 **L2TP**。可能的选项包括：
    - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
    - **PPTP**：点对点通道。
    - **IKEv2**： Internet 密钥交换第 2 版。
  - 身份验证方法：在列表中，选择要使用的身份验证方法。默认值为 **EAP**。可能的选项包括：
    - **EAP**：扩展身份验证协议。
    - **MSChapV2**：使用 Microsoft 的质询-握手身份验证协议相互验证身份。当您选择通道类型 **IKEv2** 时，此选项不可用。
  - **EAP** 方法：在列表中，选择要使用的 EAP 方法。默认值为 **TLS**。启用 MSChapV2 身份验证时此字段不可用。可能的选项包括：
    - **TLS**：传输层安全性
    - **PEAP**：受保护的可扩展身份验证协议
  - 可信网络：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - 需要智能卡证书：选择是否需要智能卡证书。默认值为关。
  - 自动选择客户端证书：选择是否自动选择用于身份验证的客户端证书。默认值为关。启用需要智能卡证书时此选项不可用。
  - 始终启用 **VPN**：选择是否始终启用 VPN。默认值为关。启用后，VPN 连接保持可用，直到用户手动断开连接。
  - 绕过本地地址：键入地址和端口号，以允许本地资源绕过代理服务器。
- 配置插件配置文件类型：这些设置应用于从 Windows 应用商店获取并安装在用户设备上的 VPN 插件。
  - 服务器地址：键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
  - 记住凭据：选择是否缓存凭据。默认值为关。启用后，会在合适的时候缓存凭据。
  - **DNS** 后缀：键入 DNS 后缀。
  - 客户端应用程序 **ID**：键入 VPN 插件的软件包系列名称。
  - 插件配置文件 **XML**：单击浏览并导航到要使用的自定义 VPN 插件配置文件所在位置，选择此文件。有关格式及详细信息，请联系插件提供商。
  - 可信网络：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - 始终启用 **VPN**：选择是否始终启用 VPN。默认值为关。启用后，VPN 连接保持可用，直到用户手动断开连接。
  - 绕过本地地址：键入地址和端口号，以允许本地资源绕过代理服务器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Amazon 设置



- 连接名称：输入连接的名称。
- **VPN** 类型：选择连接类型。可能的选项包括：
  - **L2TP PSK**：使用预共享密钥身份验证的第二层通道协议。这是默认设置。
  - **L2TP RSA**：使用 RSA 身份验证的第二层通道协议。
  - **IPSEC XAUTH PSK**：使用预共享密钥和扩展身份验证的 Internet 协议安全性。
  - **IPSEC HYBRID RSA**：使用混合 RSA 身份验证的 Internet 协议安全性。
  - **PPTP**：点对点通道。

以下各节列出了前面每种连接类型的配置选项。

为 **Amazon** 配置 **L2TP PSK** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **L2TP** 密钥：键入共享密钥。
- **IPSec** 标识符：键入用户连接时在其设备上看到的 VPN 连接的名称。
- **IPSec** 预共享密钥：键入密钥。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置适用于 **Amazon** 的 **L2TP RSA** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **L2TP** 密钥：键入共享密钥。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 服务器证书：在列表中，选择要使用的服务器证书。
- **CA** 证书：在列表中，选择要使用的 CA 证书。
- 身份凭据：在列表中，选择要使用的身份凭据。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

为 **Amazon** 配置 **IPSEC XAUTH PSK** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **IPSec** 标识符：键入用户连接时在其设备上看到的 VPN 连接的名称。
- **IPSec** 预共享密钥：键入共享密钥。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

为 **Amazon** 配置 **IPSEC AUTH RSA** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 服务器证书：在列表中，选择要使用的服务器证书。
- **CA** 证书：在列表中，选择要使用的 CA 证书。
- 身份凭据：在列表中，选择要使用的身份凭据。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 单击保存以保存路由，或者单击取消不保存路由。

为 **Amazon** 配置 **IPSEC HYBRID RSA** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 服务器证书：在列表中，选择要使用的服务器证书。
- **CA** 证书：在列表中，选择要使用的 CA 证书。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

配置适用于 **Amazon** 的 **PPTP** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- **PPP** 加密 **(MPPE)**：选择是否使用 Microsoft 点对点加密 (MPPE) 进行数据加密。默认值为关。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

墙纸设备策略

March 31, 2022

“墙纸” 设备策略允许您添加.png 或.jpg 文件，以设置 iOS 设备锁定屏幕、主屏幕或二者的墙纸。此策略仅适用于受监督设备。要在 iPad 和 iPhone 上使用不同的墙纸，需要创建不同的墙纸策略并将其部署到相应的用户。

下表列出了 Apple 建议的用于 iOS 设备的图片尺寸。

iPhone

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备	图片尺寸（像素）
iPhone 12 Pro Max	2778 x 1284
iPhone 12 和 iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X、XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 第二代	1334 x 750
iPhone 7 PLus、8 PLus	2208 x 1242
iPhone 7、8	1334 x 750
iPhone 8 PLus	1334 x 750
iPhone 8	1334 x 750

iPad

设备	图片尺寸（像素）
iPad Pro（第一代、第二代和第三代 12.9 英寸）	2732 x 2048
iPad Pro 10.5 英寸	2224 x 1668
iPad Pro（9.7 英寸）	1536 x 2048
iPad Air 2	2048 x 1536

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 适用于：在列表中，选择锁屏界面、主 **(**图标列表**)** 屏幕或锁屏界面和主屏幕以设置墙纸的显示位置。
- 墙纸文件：要选择墙纸文件，请单击浏览，然后导航到文件所在的位置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Web 内容过滤器设备策略

March 31, 2022

可以对要添加到允许或阻止列表的特定站点使用 Apple 自动过滤功能来过滤 iOS 设备上的 Web 内容。Web 内容过滤设备策略仅在受监督模式下的 iOS 设备上可用。有关将 iOS 设备置于受监督模式的信息，请参阅使用 Apple Configurator 2 部署设备。

> 注意：
>
> Android 设备不支持 Web 内容过滤。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 过滤器类型：在列表中，单击内置或插件，然后按照所选选项后面的步骤操作。默认值为内置。

内置过滤器类型

- **Web** 内容过滤器
  - 启用自动过滤：是否使用 Apple 自动过滤功能来分析 Web 站点是否包含不合适的内容。默认值为关。
  - 允许访问的 **URL**：启用自动过滤设置为关时将忽略此列表。启用自动过滤设置为开时，无论自动过滤器是否允许访问，始终可以访问此列表中的项目。对于要添加到允许列表中的每个 URL，单击添加，然后执行以下操作：
    * 键入允许访问的 Web 站点的 URL。必须在 Web 地址前添加 `https://` 或 `https://`。
    * 单击保存将 Web 站点保存到允许列表中，或单击取消不保存此站点。
  - 阻止的 **URL**：始终阻止此列表中的项目。对于要添加到阻止列表中的每个 URL，单击添加，然后执行以下操作：
    * 输入要阻止的 Web 站点的 URL。必须在 Web 地址前添加 `https://` 或 `https://`。
    * 单击保存将 Web 站点保存到阻止列表中，或单击取消不保存此站点。
- 书签允许列表
  - 书签允许列表：指定用户可以访问的站点。要启用对 Web 站点的访问，请添加其 URL。
    * **URL**：用户可以访问的每个 Web 站点的 URL。例如，要启用对 Secure Hub 应用商店的访问，请将 Endpoint Management 服务器 URL 添加到 **URL** 列表中。必须在 Web 地址前添加 `https://` 或 `https://`。此字段为必填字段。
    * 书签文件夹：输入可选书签文件夹名称。如果将此字段留空，书签将添加到默认书签目录。
    * 标题：输入 Web 站点的描述性标题。例如，为 URL `https://google.com` 输入 “Google”。
    * 单击保存将 Web 站点保存到允许列表中，或单击取消不保存此站点。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

插件过滤器类型

- 过滤器名称：输入过滤器的唯一名称。
- 标识符：输入提供过滤器服务的插件的捆绑包 ID。
- 服务地址：输入可选服务器地址。有效格式包括 IP 地址、主机名或 URL。
- 用户名：输入服务的可选用户名。
- 密码：输入服务的可选密码。
- 证书：在列表中，单击用于向服务验证用户身份的可选身份证书。默认值为无。
- 过滤 **WebKit** 流量：选择是否过滤 WebKit 流量。
- 过滤 **Socket** 流量：选择是否过滤套接字流量。
- 自定义数据：对于要添加到 Web 过滤器的每个自定义密钥，单击添加，然后执行以下操作：
  - 密钥：键入自定义密钥。
  - 值：键入自定义密钥的值。
  - 单击保存以保存自定义密钥，或单击取消不保存此密钥。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

Web 剪辑设备策略

April 11, 2023

您可以向 Web 站点中放置快捷方式或 Web 剪辑，以与应用程序一起出现在用户设备上。可以指定自己的图标来表示 iOS、iPadOS、macOS 和 Android 设备的 Web 剪辑。Windows 平板电脑只需要一个标签和一个 URL。对于 iOS 和 iPadOS 设备，请配置主屏幕布局设备策略以组织您创建的 Web 剪辑。如果限制对 iOS 上的应用程序的访问，请务必将限制设备策略配置为允许 Web 剪辑。有关配置这些策略的信息，请参阅主屏幕布局设备策略和“限制”设备策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 标签：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。URL 的开头必须为协议，例如 `https://server`。
- 可删除：选择用户是否可以删除 Web 剪辑。默认值为关。共用的 iPad 不支持此选项。
- 待更新的图标：通过单击浏览并导航到要用于 Web 剪辑的图标文件所在位置，选择此图标。
- 复合图标：选择此图标是否应用某些效果（圆角、阴影和光照反射）。默认值为关，表示添加效果。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 全屏：选择链接的 Web 页面是否以全屏模式打开。此设置还使 iPad 只能打开单个 Web 站点。或者，要将 iPad 设置为在网亭模式下运行，请使用“应用程序锁定”设备策略。有关详细信息，请参阅将 iPad 配置为网亭。默认值为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。
  - 配置文件作用域：选择此策略是应用到用户还是整个系统。默认值为用户。仅适用于 iOS 9.3 及更高版本。

macOS 设置

- 标签：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。URL 的开头必须为协议，例如 `https://server`。
- 待更新的图标：通过单击“浏览”并导航到要用于 Web 剪辑的图标文件所在位置，选择此图标。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。

Android 设置

- 规则：选择此策略是添加还是删除 Web 剪辑。默认值为添加。
- 标签：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。
- 定义图标：选择是否使用图标文件。默认值为关。
- 图标文件：如果定义图标设置为开，请单击浏览并导航到要使用的图标文件所在位置，选择此文件。

Windows Desktop/Tablet 设置

- 名称：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。

Windows 代理设备策略

March 31, 2022

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使用 Windows 代理设备策略在托管 Windows 桌面和平板电脑运行 PowerShell 脚本。可以指向作为企业应用程序上载到 Endpoint Management 的脚本文件以及托管脚本的其他服务器。有关添加企业应用程序的信息，请参阅添加应用程序。

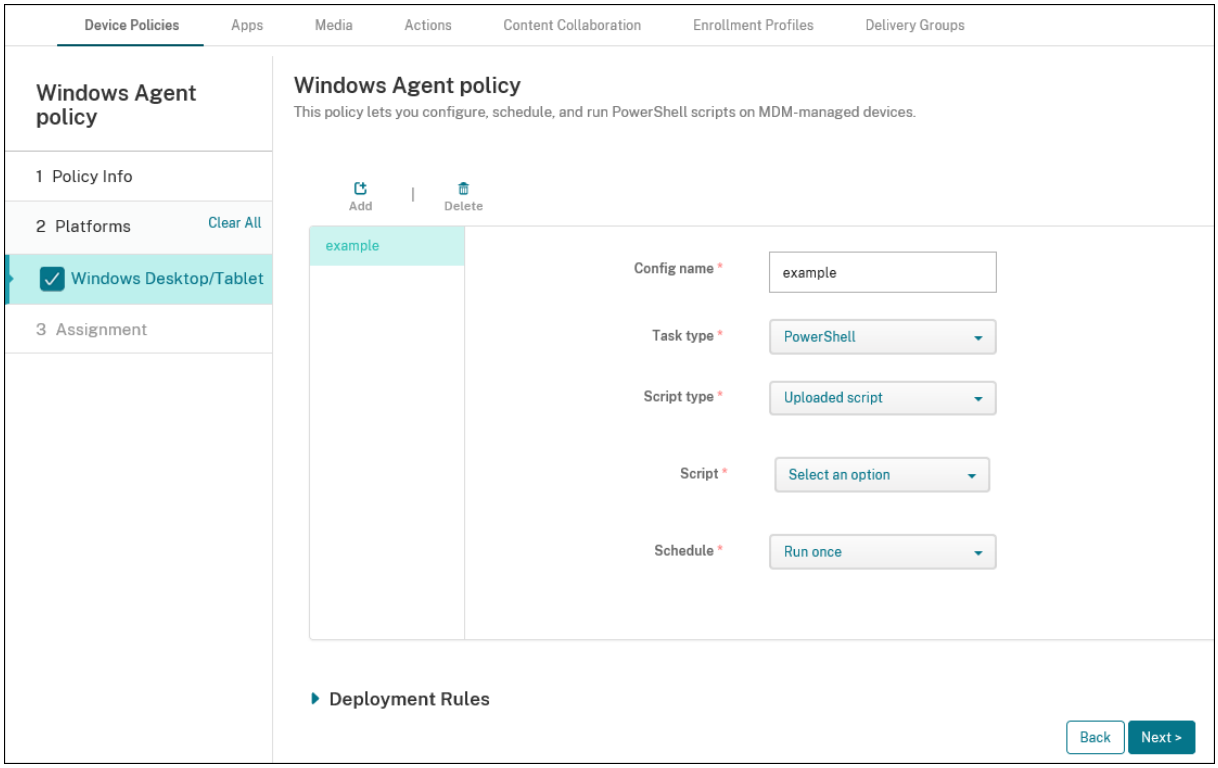
所有脚本都以特权状态执行，您不需要以管理员身份运行脚本。

部署并运行脚本后，可以根据脚本的结果配置自动操作。例如，您运行监视注册表项并返回结果的脚本。根据返回的结果，运行自动操作。该操作授予或拒绝对应用程序的访问权限、将设备标记为不合规或产生其他影响。

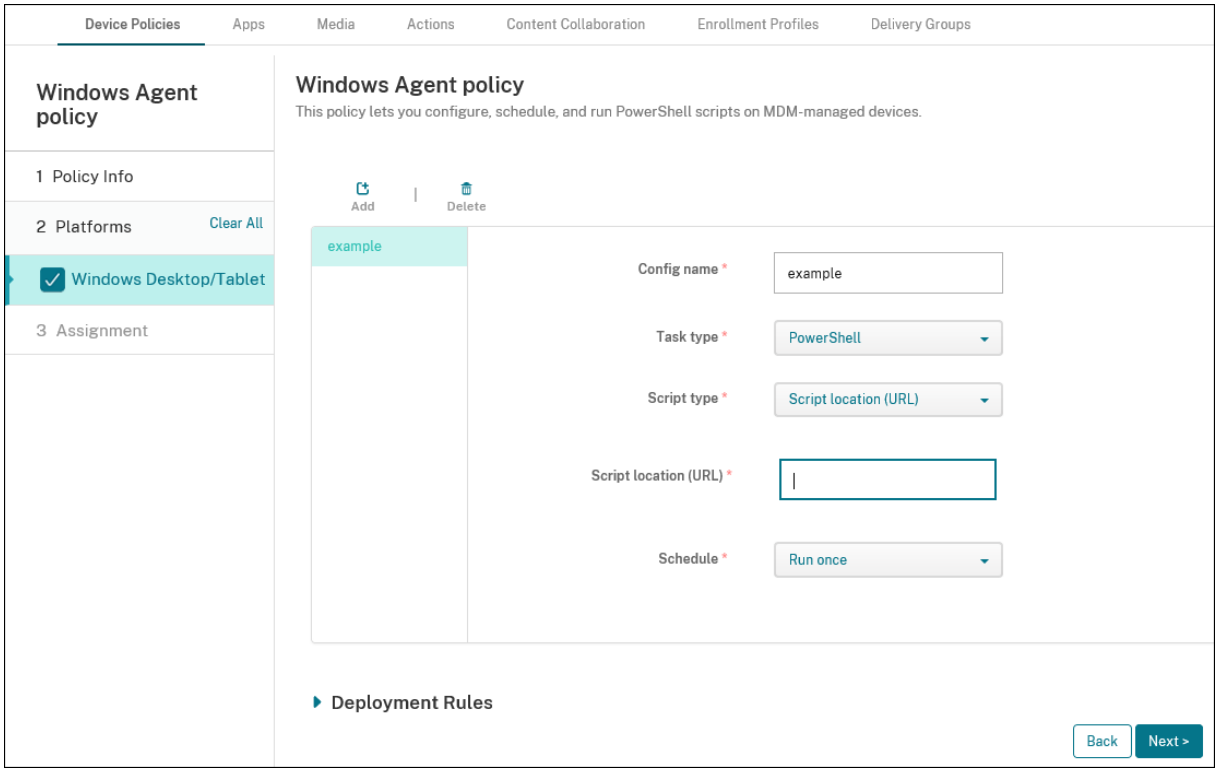
还可以使用此策略通过配置指向.msi 文件和.mst 文件的 PowerShell 脚本来部署自定义的 MSI 安装程序。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Windows Desktop 和 **Tablet** 设置



© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 配置名称：键入配置的描述性名称。
- 任务类型：选择 **PowerShell**。
- 脚本类型：为已上载到 Endpoint Management 的脚本选择上载的脚本，或者为在外部托管的脚本选择脚本位置 **(URL)**。有关如何将脚本上载到 Endpoint Management 的详细信息，请参阅将 Win32 应用程序添加为企业应用程序。
  - 选择脚本：如果选择上载的脚本，请选择要运行的脚本。
  - 脚本位置 **(URL)**：如果选择脚本位置 **(URL)**，请输入要运行的脚本的位置。此 URL 必须将脚本作为有效负载传递。Endpoint Management 不支持将脚本作为 JavaScript 下载提供的 URL。该脚本还必须公开发布。
- 计划：选择 **Run once**（运行一次）将运行所选脚本一次，选择 **Run on a recurring basis**（循环运行）将定期运行脚本。
  - **Run every (hours)**（运行时间间隔 (小时)）：键入两次运行脚本之间的小时数。

要检查脚本的状态，请导航到控制台中的管理 **>** 设备。选择要检查脚本状态的设备，然后单击编辑。在属性下，可以通过单击 **Windows** 代理标题下的下载来检查脚本的状态。

部署 **PowerShell** 脚本以触发自动操作

1. 创建 PowerShell 脚本以监视注册表项。以下 PowerShell 脚本将检查防火墙是否已启用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
$body = @{
  }

$firewallEnabled = Get-ItemPropertyValue HKLM:\SYSTEM\
   CurrentControlSet\Services\SharedAccess\Parameters\
   FirewallPolicy\StandardProfile -Name EnableFirewall
if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"
 }
  else {

$body["firewallEnabled"]="false"
 }

$body | ConvertTo-Json -Depth 10
<!--NeedCopy-->
```

此脚本将返回以下值之一

```
{

    "firewallEnabled":  "true"
 }

<!--NeedCopy-->
```

或

```
{

    "firewallEnabled":  "false"
 }

<!--NeedCopy-->
```

2. 将脚本作为企业应用程序上载到 Endpoint Management 控制台，或者在可访问的 URL 上托管脚本。
3. 配置本文中介绍的 Windows 代理设备策略。确保脚本已计划立即运行。
4. 脚本运行后，确定脚本状态。
   a) 导航到控制台中的管理 **>** 设备。
   b) 选择要检查其脚本状态的设备，然后单击编辑。
   c) 单击 **Windows** 代理标题下的下载。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 根据收到的状态配置自动操作。有关配置自动化操作的详细信息，请参阅基于 Windows 代理设备策略结果创建自动化操作。该部分显示了为示例脚本和 Windows 代理设备策略创建的特定自动操作。

Windows GPO 配置设备策略

August 8, 2023

Windows GPO 配置设备策略允许您执行以下操作：

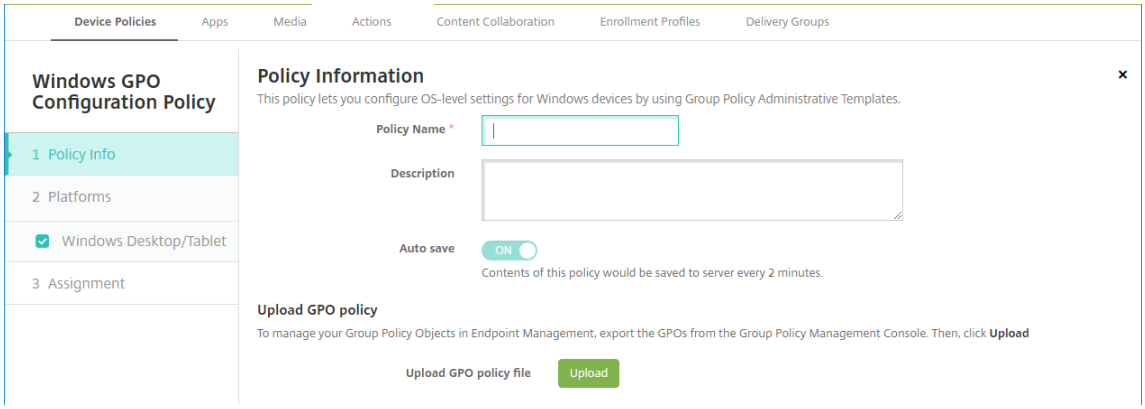
- 使用 Endpoint Management 控制台导入组策略对象 (GPO) 并将其部署到 Windows 10 和 Windows 11 设备。
- 为受 Citrix Workspace Environment Management 支持的任何 Windows 设备配置 GPO。
- 在设备和用户级别配置 GPO。

导入 GPO 以便部署到 Windows 10 和 Windows 11 设备

可以通过 Endpoint Management 控制台导入和部署 GPO，而非依赖 AD 管理员使用组策略管理控制台管理 GPO。

要在 Endpoint Management 中创建 GPO 的备份，请执行以下操作：

1. 请求您的 AD 管理员从组策略管理控制台导出 GPO，并向您提供这些文件。
2. 在 Endpoint Management 控制台中，转到配置 > 设备策略并创建 **Windows GPO** 配置策略。
3. 单击上载，找到该文件，然后单击打开以导入该文件。



有关配置 GPO 的信息，请参阅本文中的Windows Desktop 和 Tablet 设置。

配置 GPO 以便部署到 Citrix Workspace Environment Management

Windows GPO 配置设备策略允许您为 Citrix Workspace Environment Management (WEM) 支持的任何 Windows 设备配置 GPO。Endpoint Management 将策略推送到 Citrix WEM 服务。然后，WEM 服务将使用安装在设备上的 WEM 代理将 GPO 应用到设备及其应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

有关安装 Workspace Environment Management 代理的信息，请参阅安装和配置。

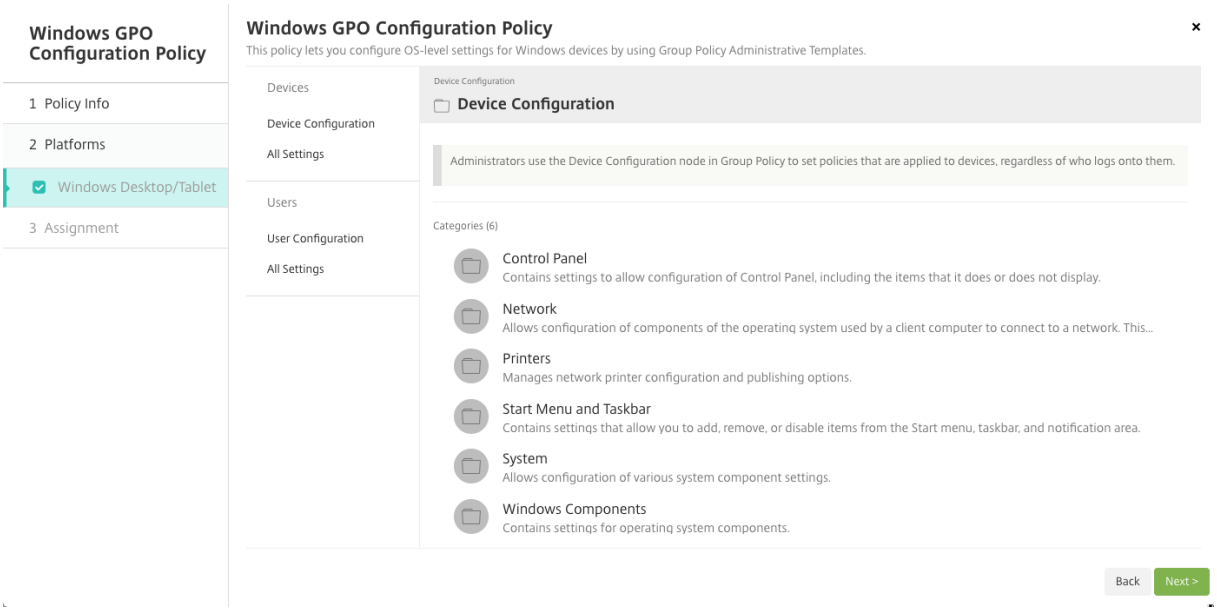
此策略使用所有 Windows 操作系统 ADMX 文件。如果要上载第三方 ADMX 文件，请使用应用程序配置设备策略。有关上载第三方 ADMX 文件的详细信息，请参阅应用程序配置设备策略。

- 可以向 WEM 支持的任何设备推送 GPO 配置，即使 Endpoint Management 本身不支持该设备亦如此。有关支持的设备列表，请参阅操作系统要求。
- 此策略要求设备安装并配置 WEM 代理。无需 MDM 或 MAM 即可注册设备。
- Endpoint Management 通过 WEM 通道推送 GPO 设置。（Microsoft 不支持通过 MDM 通道推送设备级别的设置。）接收 Windows GPO 配置设备策略的设备在名为 WEM 的 Endpoint Management 模式下运行。在已注册设备的管理 **>** 设备列表中，WEM 管理的设备的模式列中列出了 **WEM**。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Windows Desktop 和 **Tablet** 设置

此策略允许您在设备和用户级别配置 GPO。



选择并配置要部署到您的 Windows 设备的 Windows GPO。可以修改设备配置和用户配置。策略在树形结构中列出。单击所有设置将显示每个设置。有关设置的信息，请从 Microsoft 下载 GPO 参考表。

要配置设置，请先启用该设置。在配置过程中，Endpoint Management 会自动保存更改，以便这些设置保持不变。如果您尝试在保存设置之前离开页面，则弹出消息将指示存在未保存的更改。

如果某个设置有两个选项，则会显示单选按钮选项。对于两个以上的选项，将出现一个菜单。

> 注意：
>
> 如果需要检查已配置的设置，可以执行以下操作。
>
> 1. 在 Endpoint Management 控制台中，打开要编辑的 **Windows GPO** 配置策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 在设备或用户下，选择所有设置。
3. 按状态（升序）对表进行排序。所有未配置的策略都具有未配置状态。您配置的策略都在顶部列出。

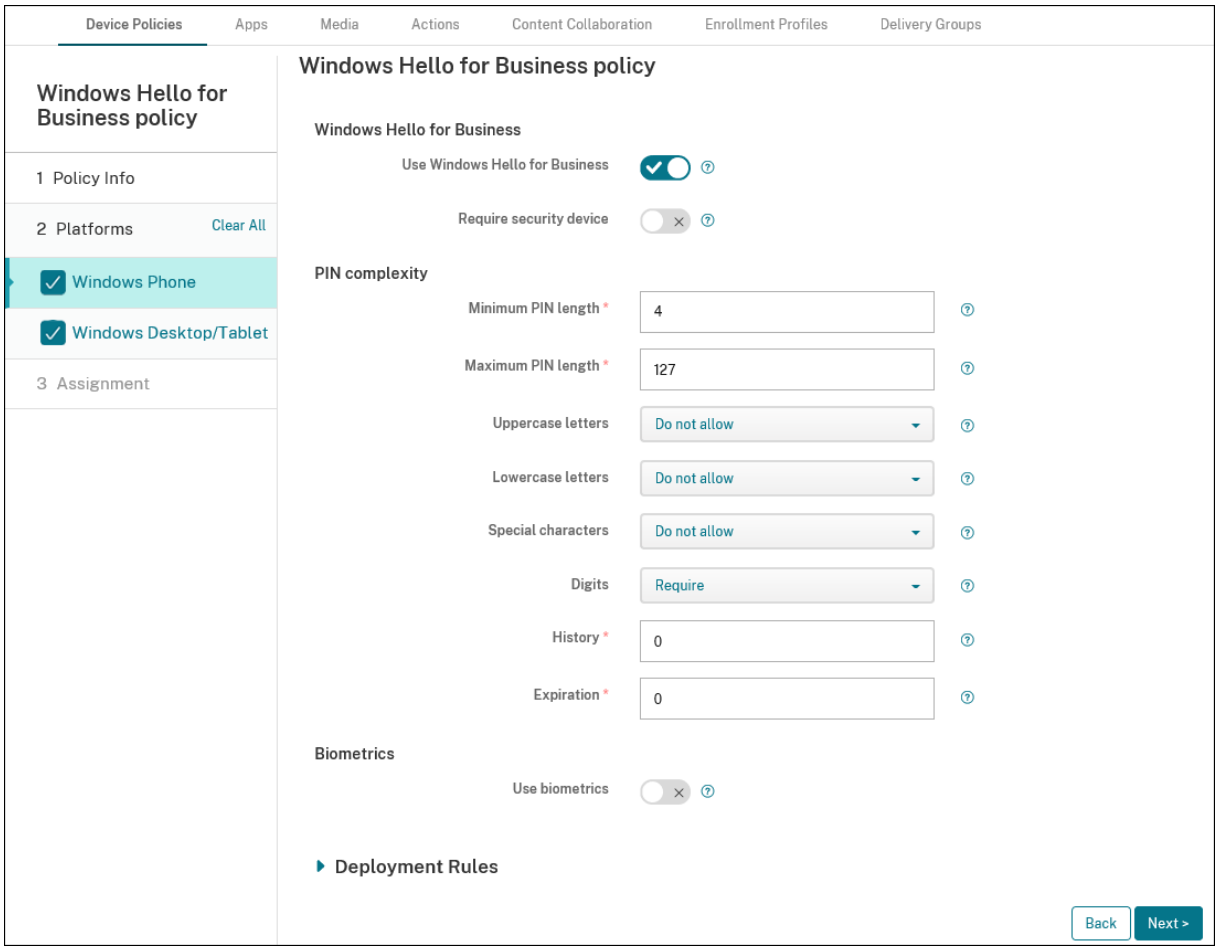
Windows Hello 企业版设备策略

March 30, 2022

Windows Hello 企业版允许其使用 Active Directory 或 Azure Active Directory 帐户登录 Windows 设备。请使用 Windows Hello 企业版设备策略启用此功能，以便用户能够在其设备上置备 Windows Hello 企业版。此策略还允许您配置通行码限制和其他安全功能。

请转至配置 **>** 设备策略以添加 Windows Hello 企业版策略。配置以下设置：

Windows Desktop/Tablet 设置



- 使用 **Windows Hello** 企业版：启用此功能将允许用户在其设备上置备 Windows Hello 企业版。
- 需要安全设备：要求用户具有受信任的平台模块 (TPM) 才能登录。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 最小/最大 **PIN** 长度：用户 PIN 的最小和最大长度。最小 **PIN** 长度默认值为 **4**。最大 **PIN** 长度默认值为 **127**。
- 大写字母、小写字母、特殊字符：选择允许、要求还是不允许使用每种类型的字符。默认值为不允许。
- 数字：允许、要求还是不允许使用数字。默认值为要求。
- 历史记录：用户不能重复使用的过去的 PIN 的数量。默认值为 **0**，表示用户可以重复使用所有 PIN。
- 过期时间：用户必须更改其 PIN 的天数。默认值为 **0**，表示 PIN 不过期。
- 使用生物特征识别：允许使用生物特征识别来代替 PIN 进行用户登录。

添加应用程序

July 24, 2023

将应用程序添加到 Endpoint Management 可提供移动应用程序管理 (MAM) 功能。Endpoint Management 可协助进行应用程序交付、软件许可、配置和应用程序生命周期管理。

启用 MDX 的应用程序是准备某些类型的应用程序以分发到用户设备的重要组成部分。有关 MDX 的简介，请参阅 Endpoint Management 组件和 MAM SDK 概述。

- Citrix 建议对启用了 MDX 的应用程序使用 MAM SDK。或者，您可以继续使用 MDX 封装应用程序，直至弃用 MDX Toolkit。请参阅弃用。
- 您无法使用 MDX Toolkit 打包 Citrix 移动生产力应用程序。从 Citrix 下载获取移动生产力应用程序 MDX 文件。

将应用程序添加到 Endpoint Management 控制台时，您可以：

- 配置应用程序设置
- （可选）将应用程序划分为多种类别，以便在 Secure Hub 对其进行组织整理
- （可选）定义工作流，以便在允许用户访问应用程序之前要求批准
- 向用户部署应用程序

本文介绍了添加应用程序的一般工作流程。有关平台详细信息，请参阅以下文章：

- 分发 Android Enterprise 应用程序
- 分发 Apple 应用程序

> 重要：
>
> Citrix Endpoint Management 支持添加和维护多达 300 个应用程序。超过此限制会导致您的系统变得不稳定。

应用程序类型和功能

下表汇总了您可以使用 Endpoint Management 部署的应用程序类型。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序类型	来源	备注	请参阅
MDX	您为用户开发的 iOS 和 Android 应用程序。Citrix 移动生产力应用程序	使用 MAM SDK 开发 iOS 或 Android 应用程序，或者使用 MDX Toolkit 封装。对于移动生产力应用程序，请从 Citrix 下载中下载公共应用商店 MDX 文件。然后将应用程序添加到 Endpoint Management。	添加 MDX 应用程序
公共应用商店	Google Play 或 Apple App Store 等公共应用商店提供的免费或付费应用程序。	上载应用程序，启用了 MDX 的应用程序，然后将应用程序添加到 Endpoint Management。	添加公共应用商店应用程序
Web 和 SaaS 应用程序	您的内部网络（Web 应用程序）或公共网络 (SaaS)。	Citrix Workspace 从在 MDM 中注册的 iOS 和 Android 设备向本机 SaaS 应用程序提供移动单点登录功能。或者，使用安全断言标记语言 (SAML) 应用程序连接器	添加 Web 或 SaaS 应用程序
Enterprise	未启用 MDX 的专用应用程序，包括 Win32 应用程序。启用了 MDX 的专用 Android Enterprise 应用程序。企业应用程序位于内容分发网络位置或 Endpoint Management 服务器中。	将应用程序添加到 Endpoint Management。	添加企业应用程序
Web 链接	不需要单点登录的 Internet Web 地址、内联网 Web 地址或 Web 应用程序。	在 Endpoint Management 中配置 Web 链接。	添加 Web 链接

在规划应用程序分发时，请考虑以下功能：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 关于无提示安装
- 关于必需应用程序和可选应用程序
- 关于应用程序类别
- 从 Citrix CDN 交付企业应用程序
- 启用 Microsoft 365 应用程序
- 应用工作流
- 应用商店和 Citrix Secure Hub 外观方案
- 通过应用商店获取 Citrix Virtual Apps and Desktops

关于无提示安装

Citrix 支持 iOS、Android Enterprise 和 Samsung 应用程序的无提示安装和升级。静默安装意味着系统不会提示用户安装您部署到设备的应用程序。应用程序将在后台自动安装。

实施无提示安装的必备条件：

- 对于 iOS，请将托管 iOS 设备置于受监督模式。有关详细信息，请参阅导入 iOS 和 macOS 配置文件设备策略。
- 对于 Android Enterprise，应用程序会安装在设备上的 Android 工作配置文件中。有关详细信息，请参阅 Android Enterprise。
- 对于 Samsung 设备，请在设备上启用 Samsung Knox。

  为此，您可以将 Samsung MDM 许可证密钥设备策略设置为生成 Samsung ELM 和 Knox 许可证访问代码。有关详细信息，请参阅 Samsung MDM 许可证密钥设备策略。

关于必需应用程序和可选应用程序

将应用程序添加到交付组时，您可以选择它们是可选的还是必需的。Citrix 建议根据需要部署应用程序。

- 所需的应用程序以无提示方式安装在用户设备上，从而最大限度地减少交互。启用此功能还将允许应用程序自动更新。
- 可选应用程序允许用户选择要安装的应用程序，但用户必须通过 Secure Hub 手动开始安装。

对于标记为必需的应用程序，用户在诸如以下情况下能够立即收到更新：

- 上载新应用程序并根据需要对其进行标记。
- 根据需要标记现有应用程序。
- 用户删除所需的应用程序。
- Secure Hub 更新可用。

必需应用程序的强制部署要求

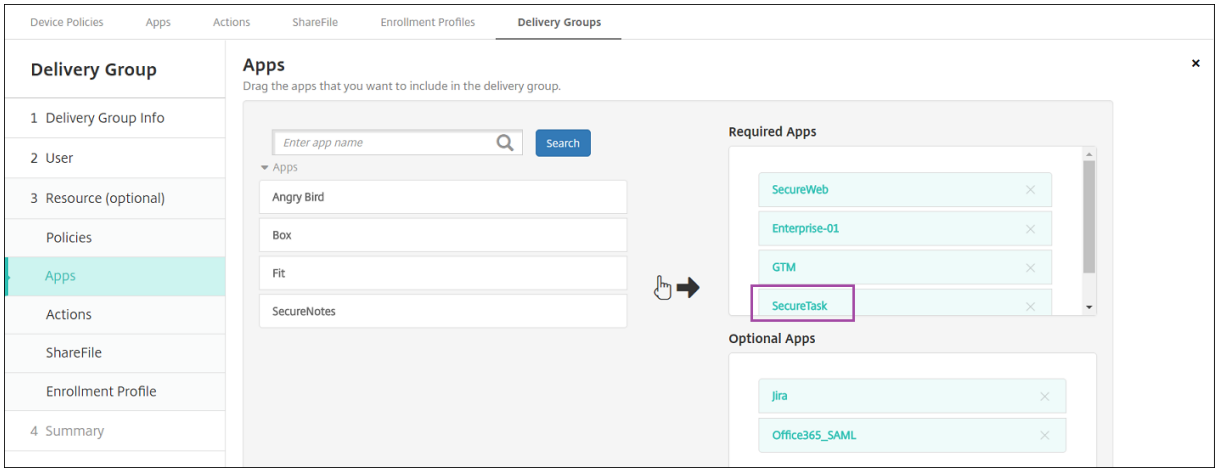
- Secure Hub 10.5.15 for iOS 和 Secure Hub 10.5.20 for Android（最低版本）
- MAM SDK 或 MDX Toolkit 10.6（最低版本）

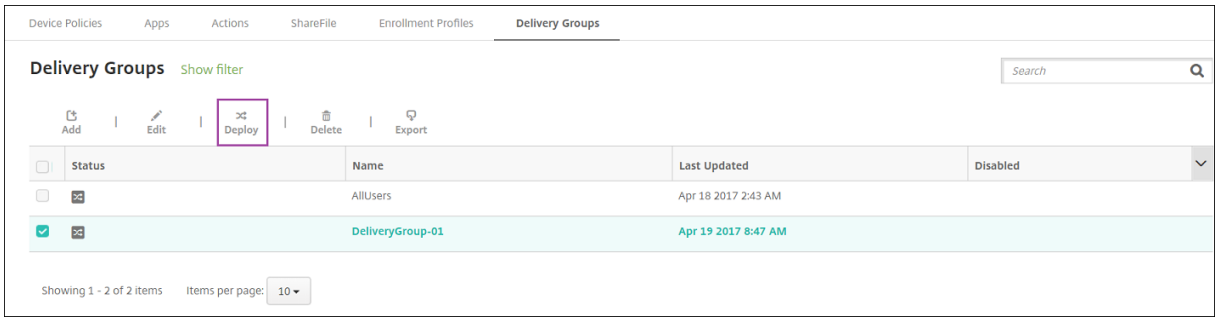
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 升级 Endpoint Management 和 Secure Hub 之后：拥有注册设备的用户必须注销然后登录 Secure Hub 才能获得所需的应用程序部署更新。

示例

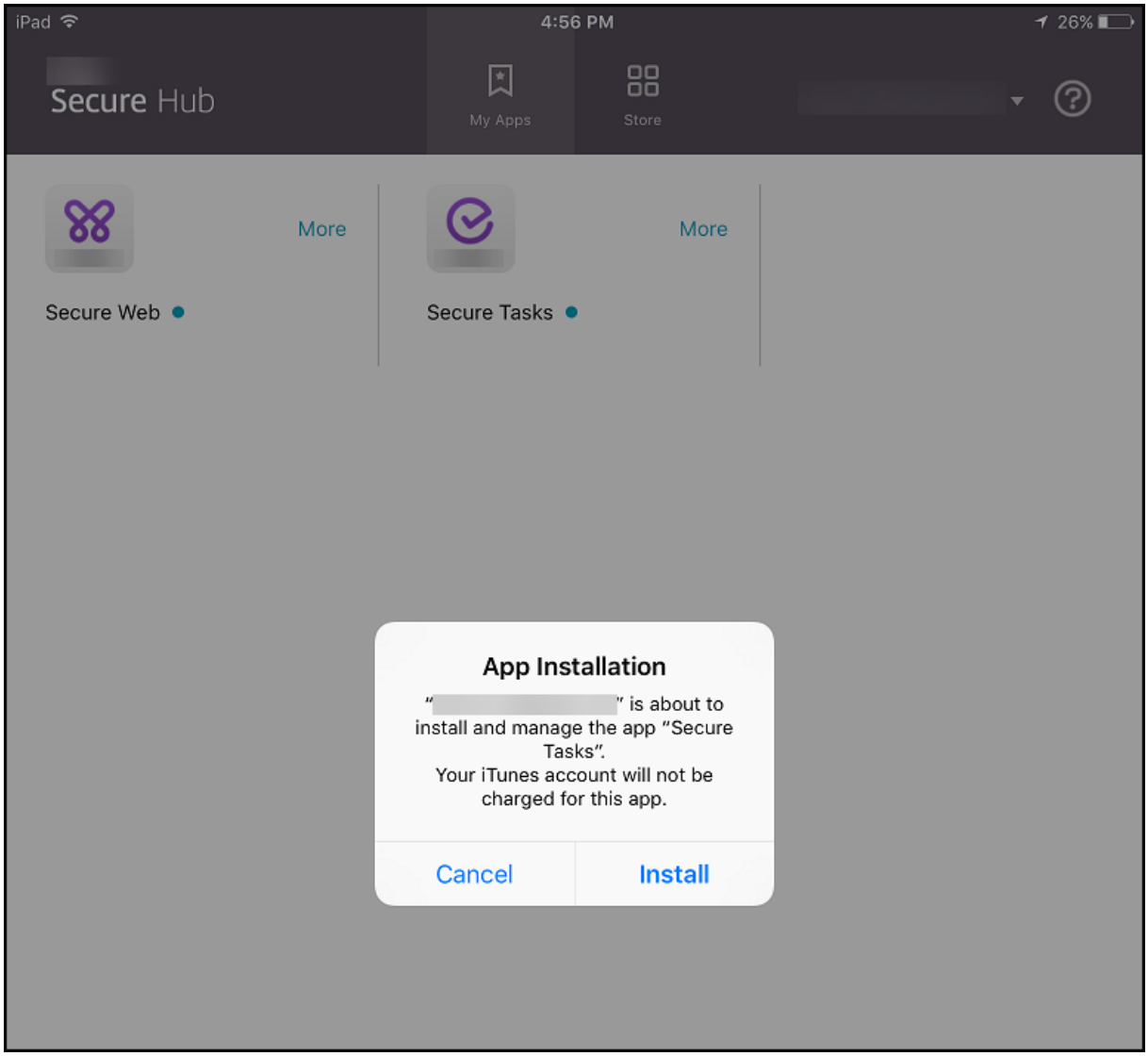
以下示例显示了向交付组添加名为 Secure Tasks 的应用程序并部署交付组的顺序。

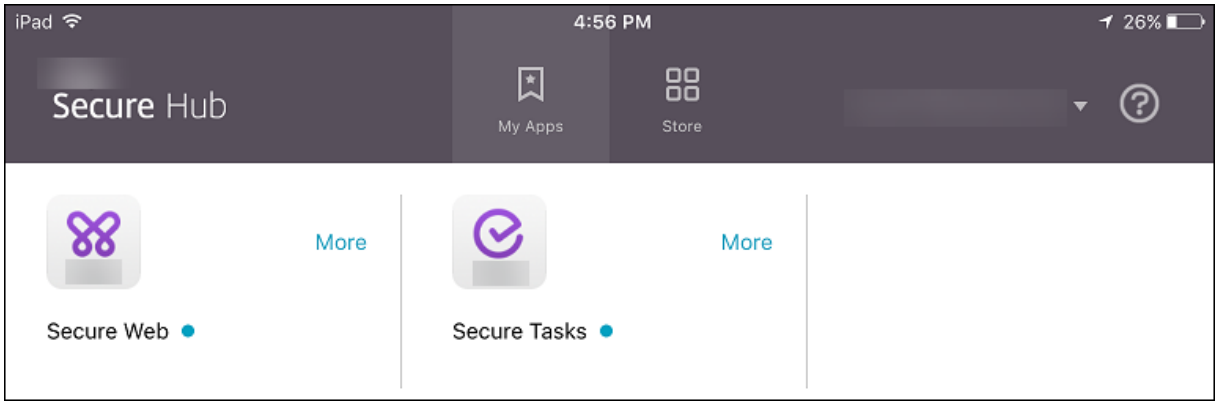




示例应用程序 Secure Tasks 部署到用户设备后，Secure Hub 将提示用户安装该应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.





> 重要：
>
> 启用了 MDX 的必需应用程序（包括企业应用程序和公共应用商店应用程序）将立即升级。即使您配置了应用程序更新宽限期 MDX 策略并且用户选择以后升级应用程序，也会执行此升级。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

面向企业和公共应用商店应用程序的 **iOS** 必需应用程序工作流

1. 首次注册期间部署移动生产力应用程序。必需应用程序安装在设备上。
2. 在 Endpoint Management 控制台上更新应用程序。
3. 使用 Endpoint Management 控制台部署必需应用程序。
4. 主屏幕上的应用程序将更新。并且，对于公共应用商店应用程序，升级将自动启动。系统不会提示用户进行更新。
5. 用户从主屏幕中打开应用程序。即使您设置了应用程序更新宽限期并且用户以后轻按即可升级应用程序，应用程序也会立即升级。

面向企业应用程序的 **Android** 必需应用程序工作流

1. 首次注册期间部署移动生产力应用程序。必需应用程序安装在设备上。
2. 使用 Endpoint Management 控制台部署必需应用程序。
3. 应用程序已升级。（Nexus 设备提示安装更新，但 Samsung 设备执行无提示安装。）
4. 用户从主屏幕中打开应用程序。即使您设置了应用程序更新宽限期并且用户以后轻按即可升级应用程序，应用程序也会立即升级。（Samsung 设备执行无提示安装。）

面向公共应用商店应用程序的 **Android** 必需应用程序工作流

1. 首次注册期间部署移动生产力应用程序。必需应用程序安装在设备上。
2. 在 Endpoint Management 控制台上更新应用程序。
3. 使用 Endpoint Management 控制台部署必需应用程序。或者，在设备上打开 Secure Hub Store。更新图标在应用商店中显示。
4. 应用程序升级自动启动。（Nexus 设备将提示用户安装更新。）
5. 在主屏幕中打开应用程序。应用程序已升级。系统不会提示用户提供宽限期。（Samsung 设备执行无提示安装。）

根据需要配置应用程序时卸载应用程序

可以允许用户根据需要卸载配置的应用程序。转到配置 **>** 交付组，然后将应用程序从必需应用程序移动到可选应用程序。

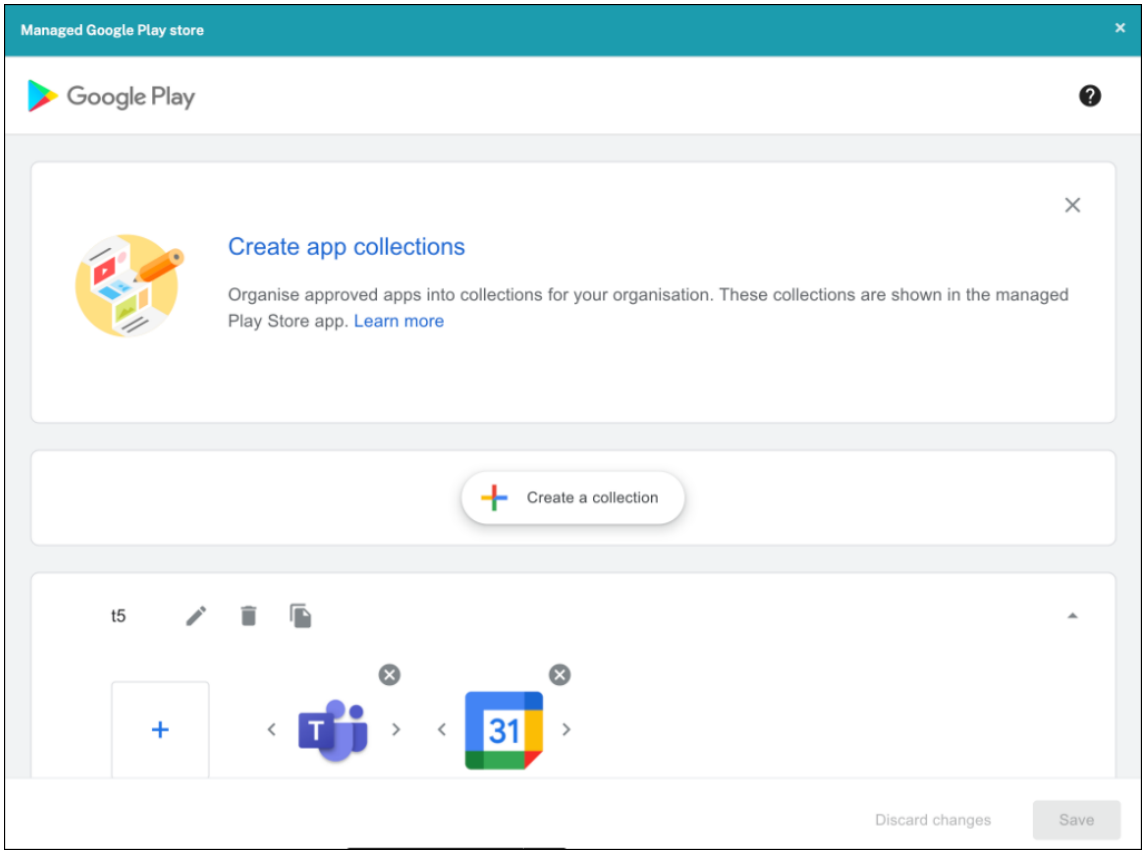
建议：请使用特殊交付组临时将应用程序更改为可选，以便特定用户可以卸载该应用程序。然后，您可以将现有的必需应用程序更改为可选，将应用程序部署到该交付组，然后从这些设备中卸载该应用程序。之后，如果您希望该交付组的未来注册需要该应用程序，则可以将该应用程序设置回必需。

整理应用程序 **(Android Enterprise)**

用户登录 Secure Hub 时，会收到您已在 Endpoint Management 中设置的应用程序、Web 链接和应用商店的列表。在 Android Enterprise 中，您可以将这些应用整理到集合中，以便用户只能访问特定的应用、商店或网页链接。例如，您创建 Finance 集合，然后向该集合中添加仅与财务相关的应用程序。或者，您可以配置向其分配销售应用程序的销售集合。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在 Endpoint Management 控制台中，单击 配置 **>** 应用程序 **>** 组织应用程序。此时将显示 **Google Play** 托管商店窗口。



2. 点击 创建集合，然后选择要添加到该集合的应用程序。
3. 添加完收藏集后，单击“保存”。

> 注意：
>
> IT 管理员需要先批准应用，然后才能将其添加到托管的 Google Play 窗口中的收藏夹中。IT 管理员可以通过访问 https://play.google.com/work 来批准应用程序。在未来的版本中，您无需批准应用程序即可将其添加到收藏夹。

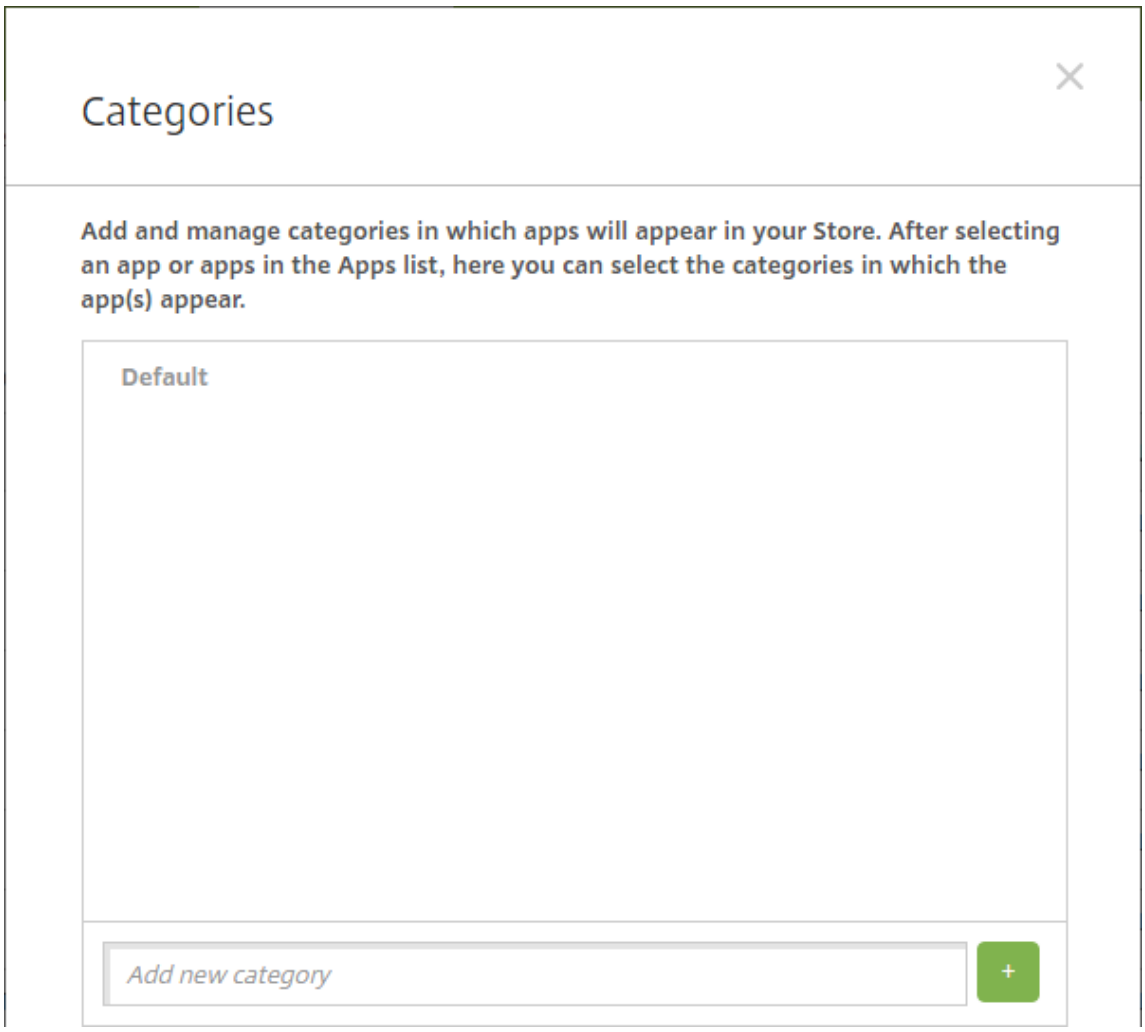
关于应用程序类别（**iOS** 和 **MDX**）

用户登录 Secure Hub 时，会收到您已在 Endpoint Management 中设置的应用程序、Web 链接和应用商店的列表。在 iOS 或 MDX 中，您可以使用应用程序类别仅允许用户访问某些应用程序、应用商店或 Web 链接。例如，您可以创建“财务”类别，然后向其中添加仅与财务相关的应用程序。您也可以配置“销售”类别，并向其分配销售应用程序。

添加或编辑应用程序、Web 链接或应用商店时，可以将应用程序添加到您所配置的一个或多个类别中。

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序 **>** 类型。此时将显示类别对话框。

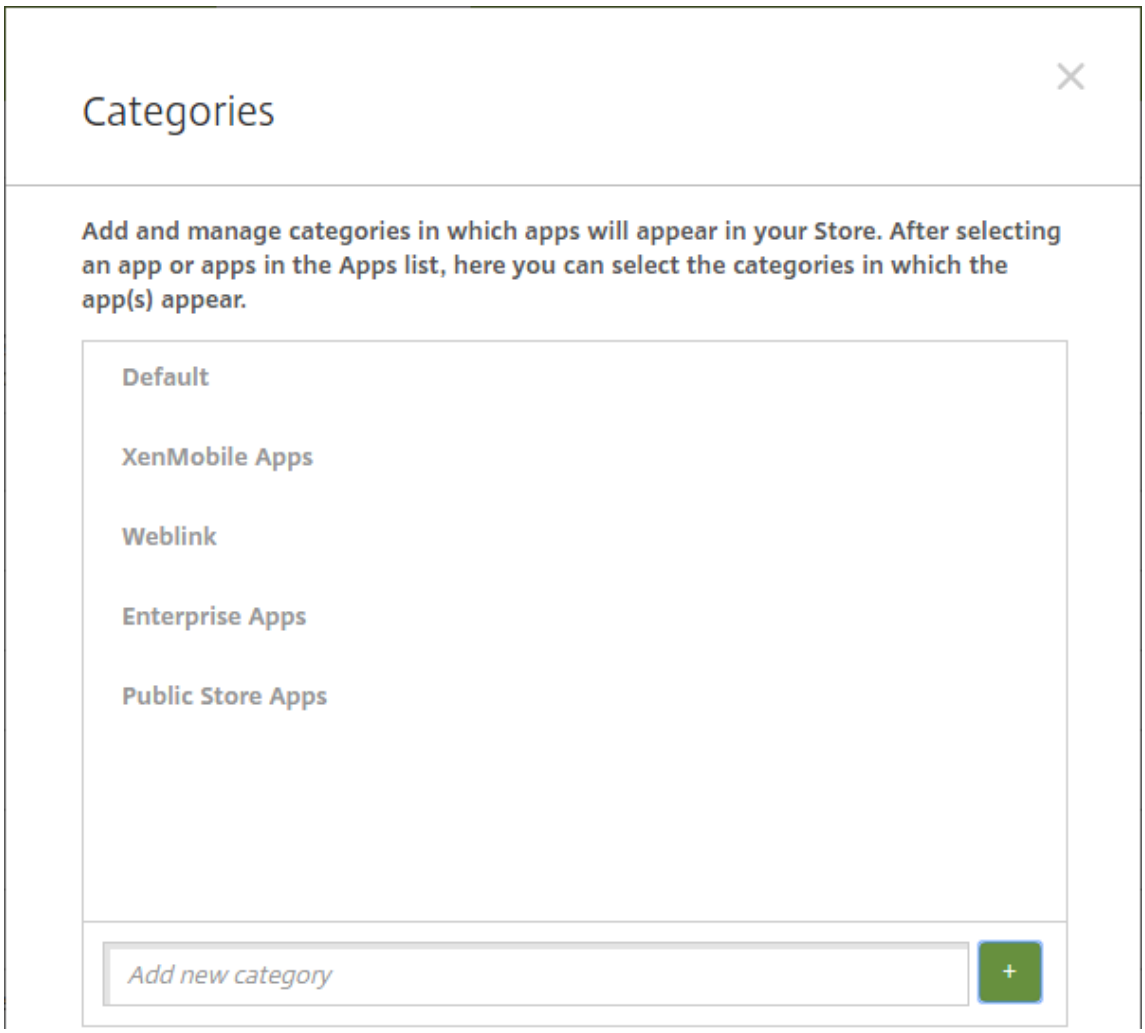
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 对于要添加的每个类别，执行以下操作：

   - 在对话框底部的添加新类别字段中键入要添加的类别的名称。例如，可以键入企业应用程序以创建企业应用程序类别。
   - 单击加号 (+) 以添加类别。此时已添加新创建的类别并显示在类别对话框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 添加完类别后，关闭类别对话框。
4. 在应用程序页面上，可以将现有应用程序放到新类别中。
   - 选择要分类的应用程序。
   - 单击编辑。此时将显示应用程序信息页面。
   - 在应用程序类别列表中，通过选中新类别的复选框应用新类别。对于您不想应用于应用程序的现有类别，可以取消选中其对应的复选框。
   - 单击交付组分配选项卡或单击后面各页面上的下一步完成剩余的应用程序设置页面。
   - 单击交付组分配页面上的保存以应用新类别。新类别将应用于应用程序并显示在应用程序表中。

添加 **MDX** 应用程序

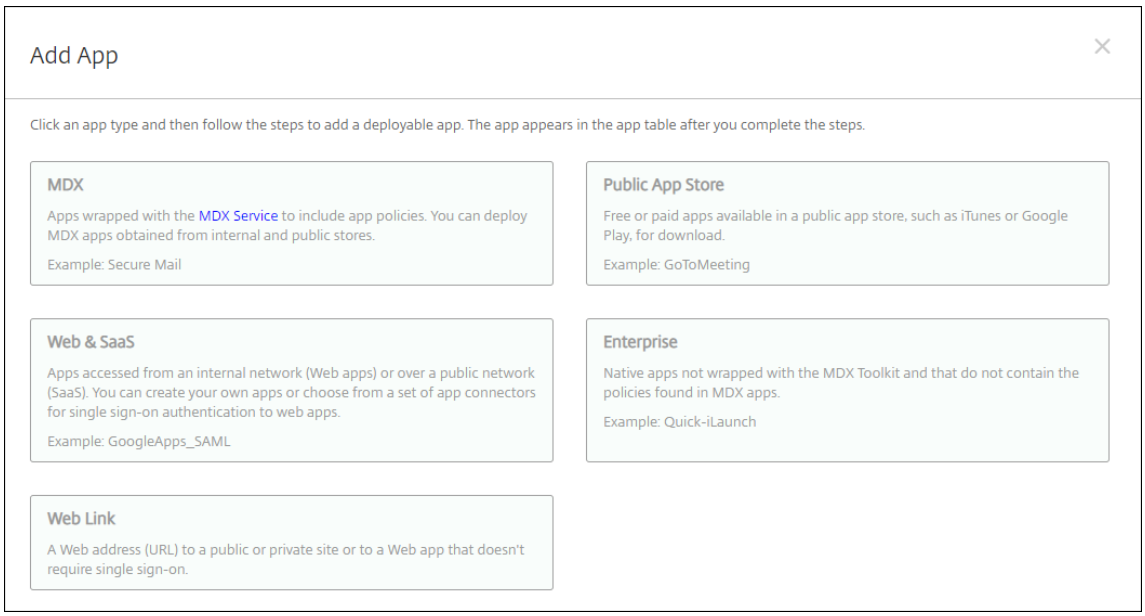
收到适用于 iOS 或 Android 应用程序的 MDX 文件时，可以将应用程序上载到 Endpoint Management。上载应用程序后，可以配置应用程序详细信息和策略设置。有关每种设备平台类型可用的应用程序策略的信息，请参阅：

- MAM SDK 概述

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- MDX 策略概览

1. 对于 Citrix 移动生产力应用程序，请下载公共应用商店 MDX 文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management** 生产力应用程序。
2. 对于其他类型的 MDX 应用程序，请获取 MDX 文件。
3. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。

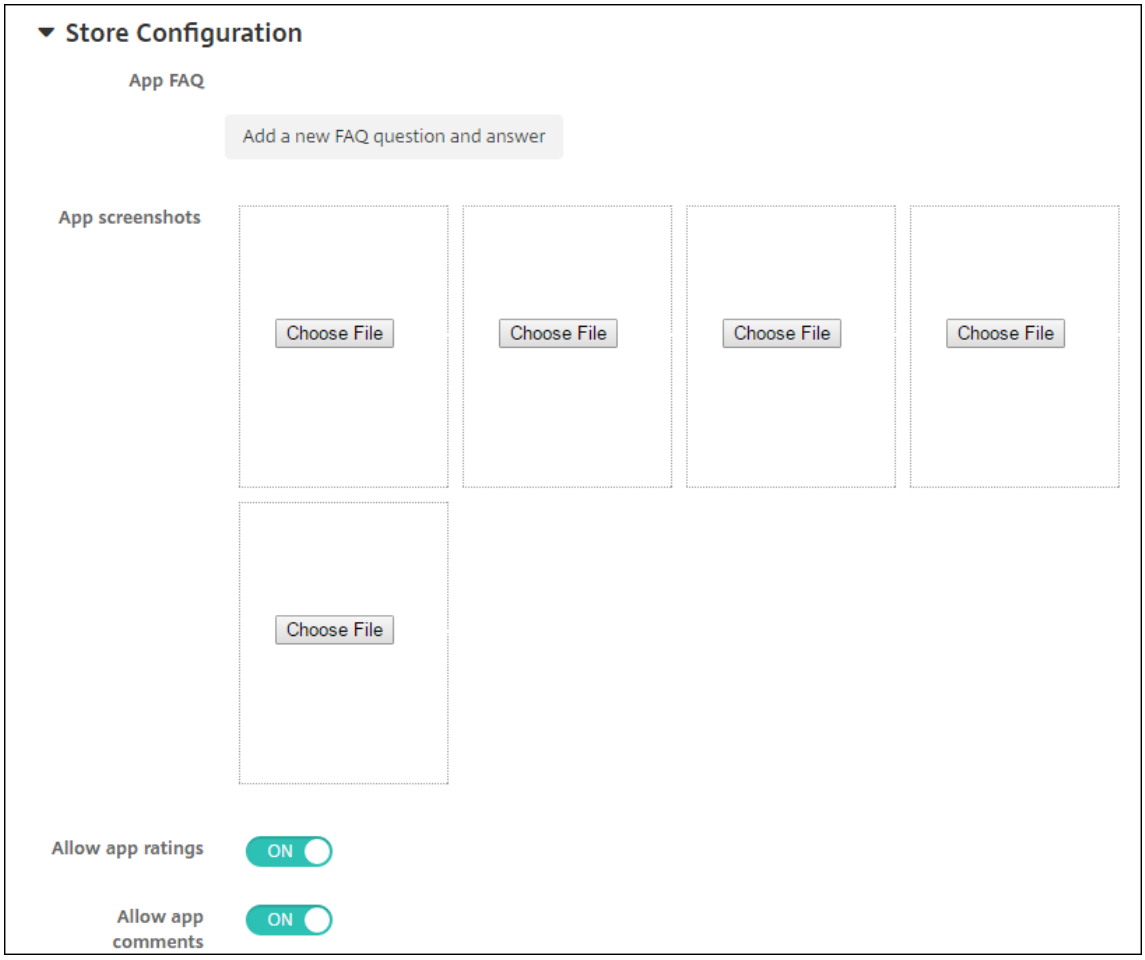


4. 单击 **MDX**。此时将显示 **MDX** 应用程序信息页面。
5. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。该名称显示在应用程序表格中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
6. 单击下一步。此时将显示应用程序平台页面。
7. 在平台下，选择要添加的平台。如果您只为一个平台进行配置，请取消选中其他平台。
8. 要选择要上载的 MDX 文件，请单击上载并导航到文件所在位置。
9. 在应用程序详细信息页面中，配置以下设置：
   - 文件名：键入与应用程序关联的文件名。
   - 应用程序说明：键入应用程序的说明。
   - 应用程序版本：（可选）键入应用程序版本号。
   - 软件包编号：键入来自托管的 Google Play 商店中的应用程序的软件包 ID。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
- 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
- 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否从 iOS 设备中删除应用程序。默认值为开。
- 阻止备份应用程序数据：选择是否阻止用户在 iOS 设备上备份应用程序数据。默认值为开。
- 产品轨迹：指定要推送到 iOS 设备的产品轨迹。如果您有一个专为测试而设计的轨迹，则可以选择并将其分配给您的用户。默认值为 生产。
- 强制管理应用程序：对于安装为非托管的应用程序，请选择是否提示用户允许在未受监督的 iOS 设备上管理此应用程序。默认值为开。
- 通过批量购买部署的应用程序：选择是否使用 Apple 批量购买部署应用程序。如果设置为开，并且您部署了应用程序的 MDX 版本并使用批量购买部署该应用程序，Secure Hub 将仅显示批量购买实例。默认设置为关。

10. 配置 **MDX** 策略。MDX 策略因平台而异，并且包含面向策略区域的选项，包括身份验证、设备安全和应用程序限制。在控制台中，每种策略都具有介绍此策略的提示。
11. 配置部署规则。有关详细信息，请参阅配置部署规则。
12. 展开应用商店配置。

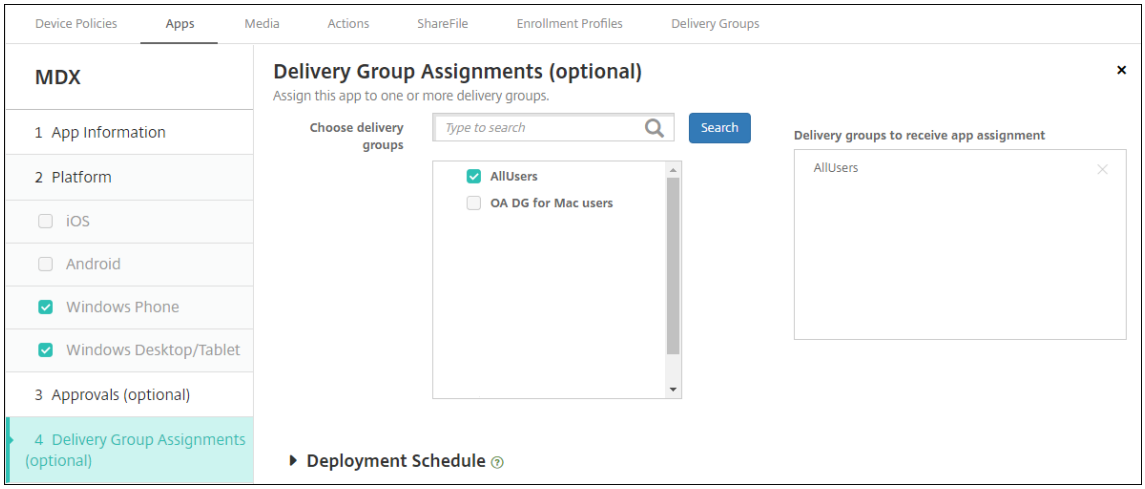


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

或者，您可以配置以下内容：

- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

13. 单击下一步。此时将显示交付组分配页面。



14. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。

15. 展开部署计划，然后配置以下设置：

- 部署：选择是否将应用程序部署到设备。默认值为开。
- 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
- 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

如果在设置 **>** 服务器属性中配置了计划后台部署密钥，为始终启用的连接部署选项适用。

始终启用选项：

- 不适用于 iOS 设备
- 不适用于开始使用版本为 10.18.19 或更高版本的 Endpoint Management 的 Android 和 Android Enterprise 客户
- 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用

配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

16. 单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

添加公共应用商店应用程序

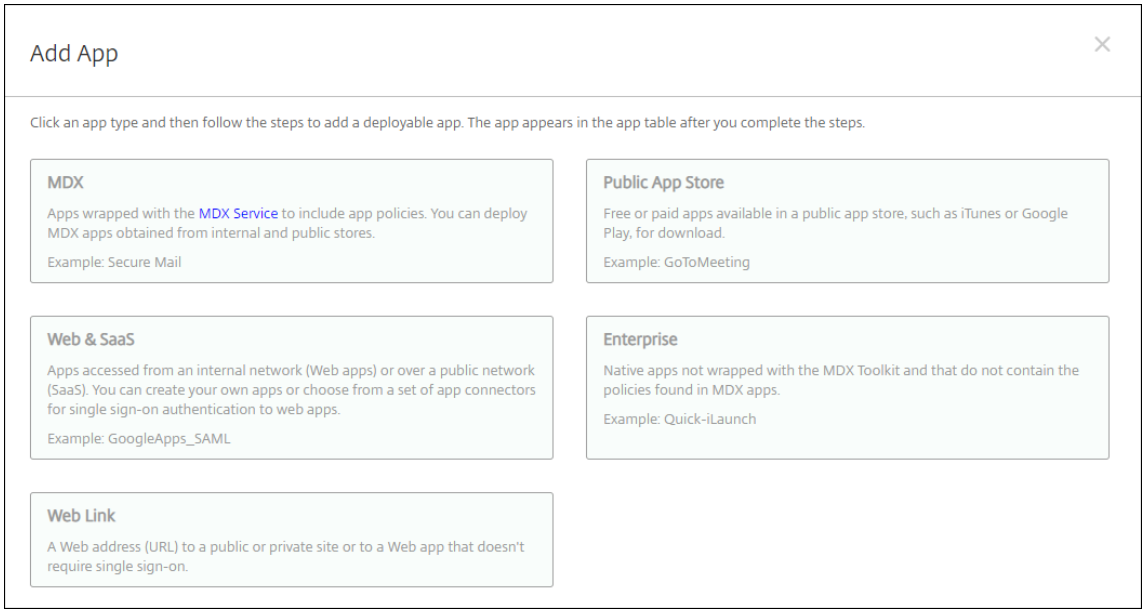
可以向 Endpoint Management 中添加公共应用商店（如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。

可通过相关设置将系统配置为从 Apple App Store 中检索应用程序名称和说明。在应用商店中检索应用程序信息时，Endpoint Management 会覆盖现有名称和说明。手动配置 Google Play 应用商店应用程序信息。

添加面向 Android Enterprise 的付费公共应用商店应用程序时，可以查看批量购买许可状态。该状态显示可用许可证总数、当前正在使用的数量以及占用这些许可证的每个用户的电子邮件地址。面向 Android Enterprise 的批量购买计划简化了批量查找、购买和分发应用程序及其他数据的过程。

配置应用程序信息并选择用于交付应用程序的平台，以：

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。



2. 单击公共应用商店。此时将显示应用程序信息页面。
3. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在应用程序表中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 单击下一步。此时将显示应用程序平台页面。
5. 在平台下，选择要添加的平台。如果您只为一个平台进行配置，请取消选中其他平台。

下一步，请为每个平台配置应用程序设置。请参阅：

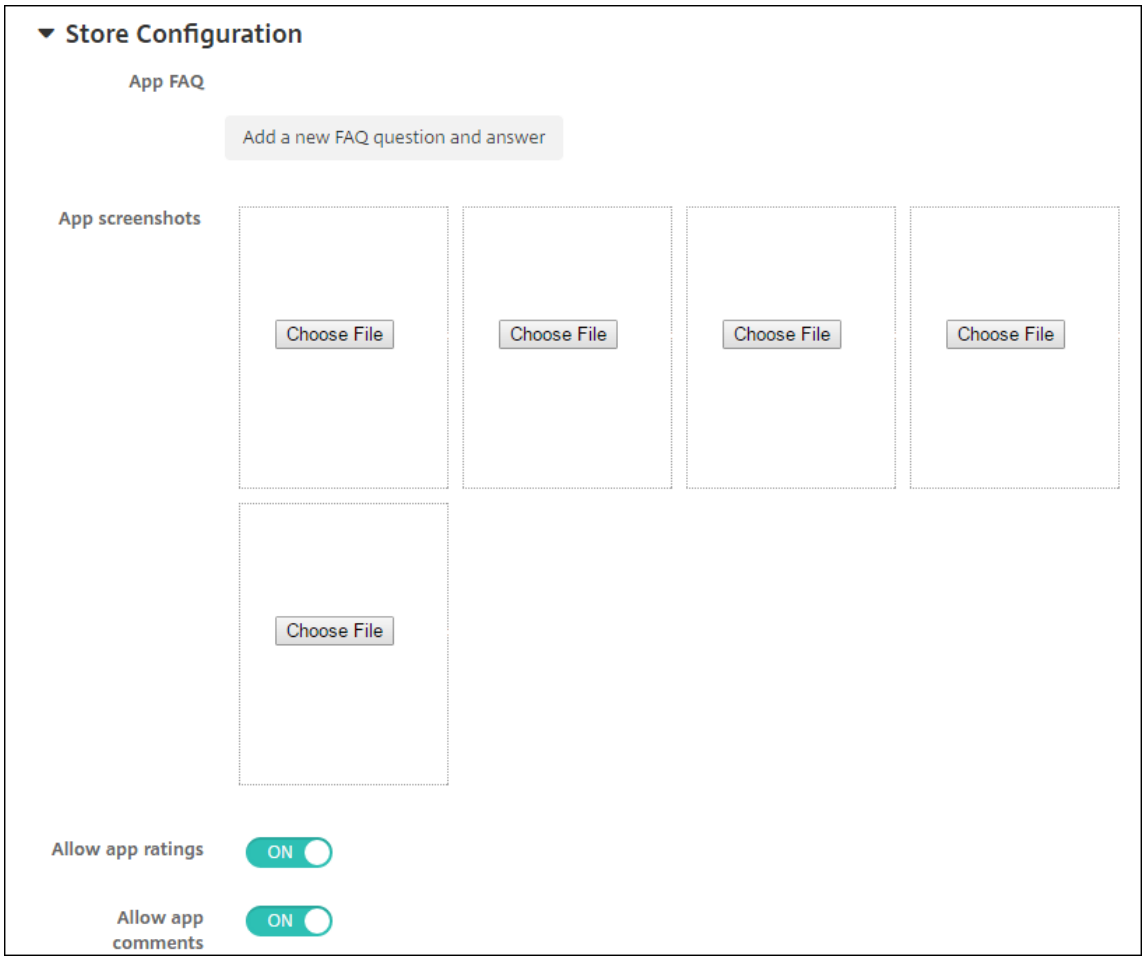
- 为 Google Play 应用程序配置应用程序设置
- 托管应用商店应用程序

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 配置 iOS 应用程序的应用程序设置

完成为平台配置设置后，请设置平台部署规则和应用商店配置。

1. 配置部署规则。有关详细信息，请参阅配置部署规则。
2. 展开应用商店配置。



或者，您可以配置以下内容：

- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

为 **Google Play** 应用程序配置应用程序设置

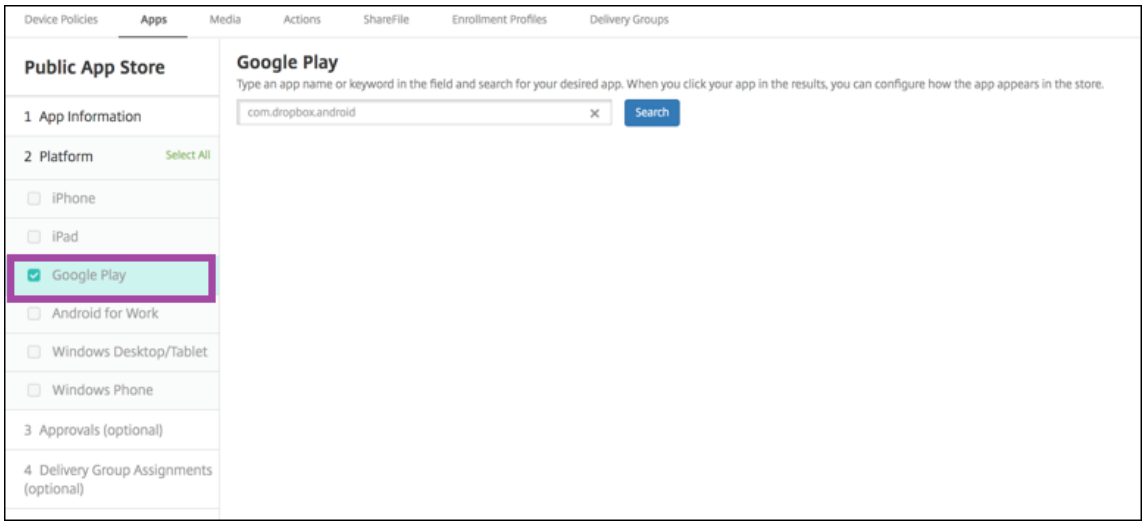
> 注意：
>
> 要使可从托管 Google Play 访问的 Google Play 应用商店中的所有应用程序，请使用访问托管 **Google Play** 应用商店中的所有应用程序服务器属性。（请参阅服务器属性。）将此属性设置为 **true** 将允许所有 Android

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

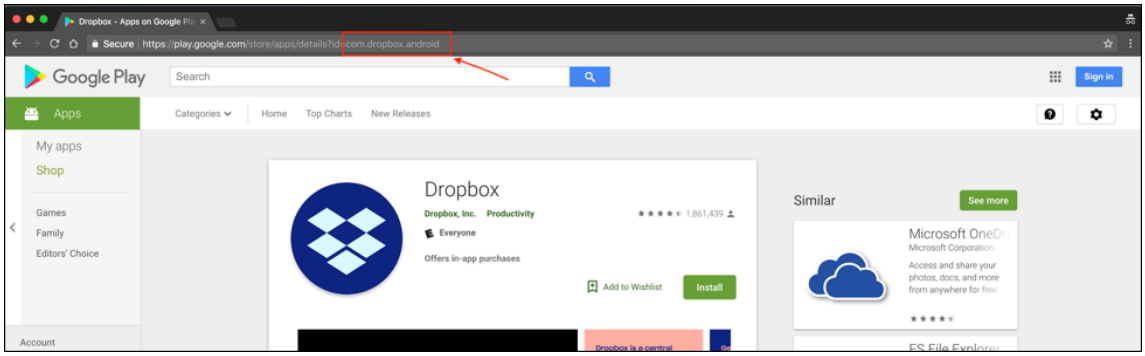
> Enterprise 用户访问公共 Google Play 应用商店应用程序。然后，您可以使用限制设备策略来控制对这些应用程序的访问。

配置 Google Play 应用商店应用程序的设置要求执行的步骤与适用于其他平台的应用程序不同。手动配置 Google Play 应用商店应用程序信息。

1. 确保在“平台”下选择“**Google Play**”。

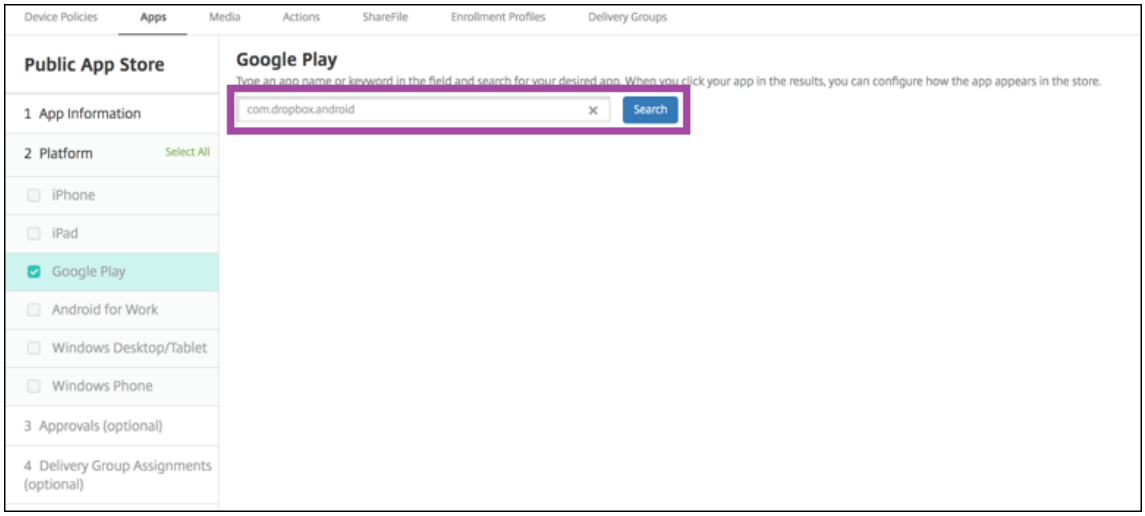


2. 转至 Google Play 应用商店。从 Google Play 应用商店复制软件包 ID。可以在应用程序的 URL 中找到 ID。

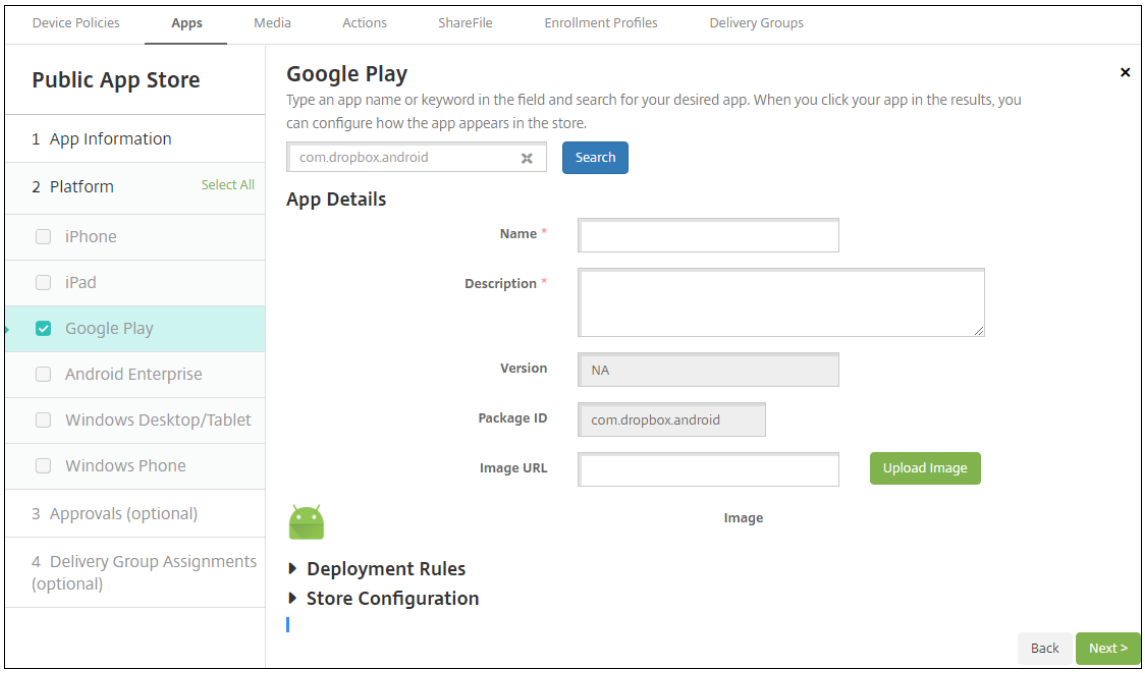


3. 在 Citrix Endpoint Management 控制台中添加公共应用商店应用程序时，将软件包 ID 粘贴到搜索栏中。单击搜索。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 如果软件包 ID 有效，将显示一个 UI，允许您输入应用程序详细信息。



5. 可以为要随应用商店中的应用程序显示的映像配置 URL。要使用 Google Play 应用商店中的映像，请执行以下操作：

   a) 转至 Google Play 应用商店。右键单击该应用程序映像并复制映像地址。

   b) 将映像地址粘贴到映像 **URL** 字段中。

   c) 单击 **Upload image**（上载映像）。该映像将显示在 **Image**（映像）旁边。

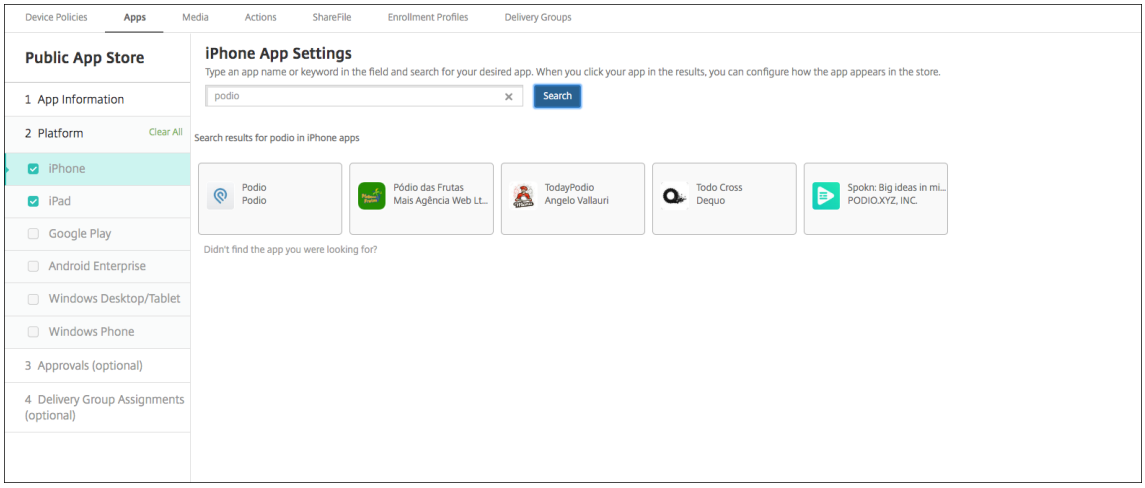
如果未配置映像，通用 Android 映像将随应用程序显示。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置 **iOS** 应用程序的应用程序设置

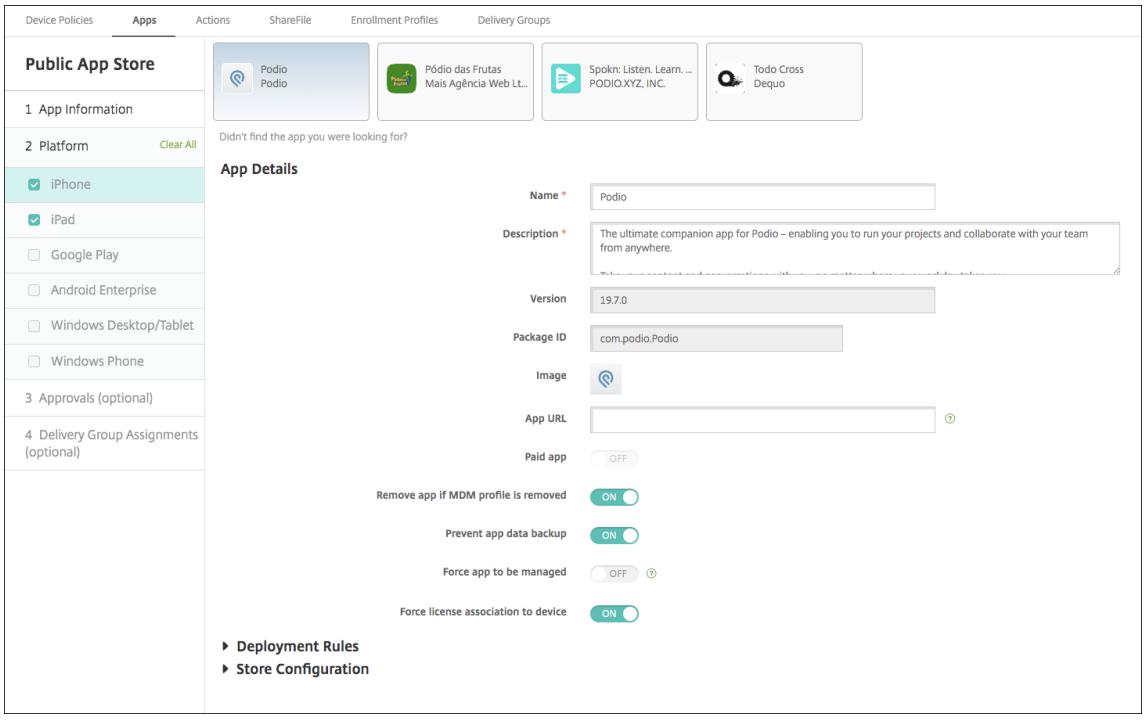
1. 在搜索框中键入应用程序名称，然后单击搜索。此时将显示符合搜索条件的应用程序。此时将显示符合搜索条件的应用程序。

   下图显示了 iPhone 上的应用程序中的 **podio** 的搜索结果。



2. 单击要添加的应用程序。

3. 应用程序详细信息字段预填充了与所选应用程序相关的信息（包括名称、说明、版本号和关联的图像）。



4. 配置以下设置：

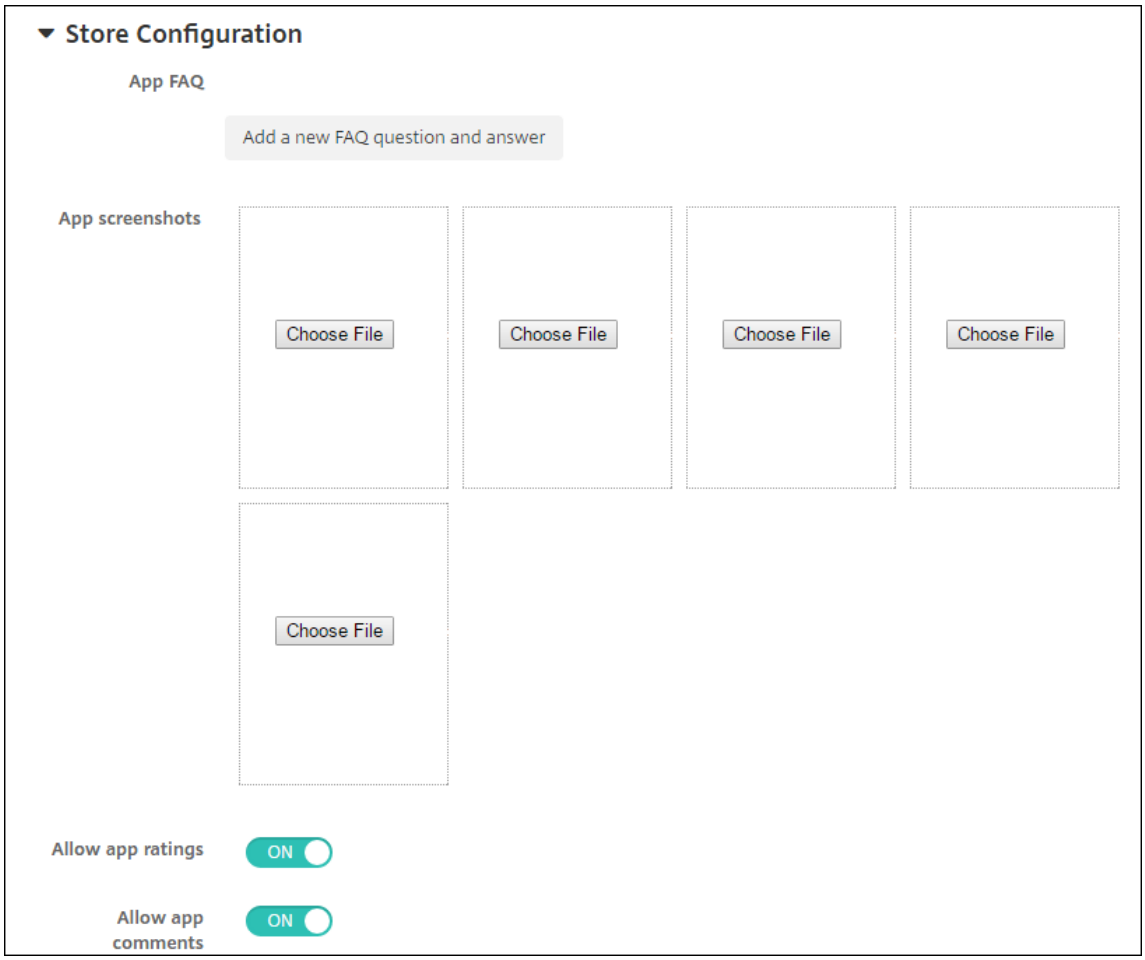
   - 如有需要，可更改应用程序的名称和说明。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 应用程序 **URL**：输入以逗号分隔的 URL 列表，以便从 Workspace 应用程序启动您的应用程序。此字段仅适用于 iPhone 和 iPad 设备。
- 付费应用程序：此字段已预配置，并且无法更改。
- 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否删除应用程序。默认值为开。
- 阻止备份应用程序数据：选择是否阻止应用程序备份数据。默认值为开。
- 产品轨迹：指定要推送到用户设备的产品轨迹。如果您有一个专为测试而设计的轨迹，则可以选择并将其分配给您的用户。默认值为 生产。
- 强制管理应用程序：对于安装为非托管的应用程序，请选择是否提示用户允许在未受监督的 iOS 设备上管理此应用程序。默认值为关。对于通过用户注册注册的 iOS 设备，Endpoint Management 不强制执行此设置，也不提示用户允许应用程序管理。
- 强制与设备建立许可证关联：选择是否将（开发时启用了设备关联的）应用程序与设备而非用户关联。如果所选应用程序不支持分配到设备，您将无法更改此设置。

5. 配置部署规则。有关详细信息，请参阅配置部署规则。

6. 展开应用商店配置。



或者，您可以配置以下内容：

- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

7. 对于 iPhone 或 iPad，展开批量购买。

   a) 要启用 Endpoint Management 以为应用程序应用批量购买，请执行以下操作：在批量购买许可证列表中，单击上载批量购买许可证。

   b) 在显示的对话框中，导入许可证。

      “许可协议”表显示应用程序正在使用的许可证数量以及可用的许可证总数。

      可以取消单个用户的批量购买许可证的关联。这样将终止许可证分配并释放许可证。

   c) 添加批量购买帐户时，启用应用程序自动更新。此设置可确保 Apple Store 中出现更新时，用户设备上的应用程序会自动更新。如果应用程序启用了强制管理应用程序设置，则会更新而不提示用户。无论应用程序是必需的还是可选的，都会进行更新。

8. 完成 批量购买设置后，单击“下一步”。此时将显示审批页面。

   要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果您不需要审批工作流程，请继续执行下一步。

9. 单击下一步。此时将显示交付组分配页面。

10. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。

11. 展开部署计划，然后配置以下设置：

    - 部署：选择是否将应用程序部署到设备。默认值为开。
    - 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
    - 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

    如果在设置 **>** 服务器属性中配置了计划后台部署密钥，为始终启用的连接部署选项适用。

    始终启用选项：

    - 不适用于 iOS 设备
    - 不适用于开始使用版本为 10.18.19 或更高版本的 Endpoint Management 的 Android 和 Android Enterprise 客户
    - 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用

    配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

12. 单击保存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

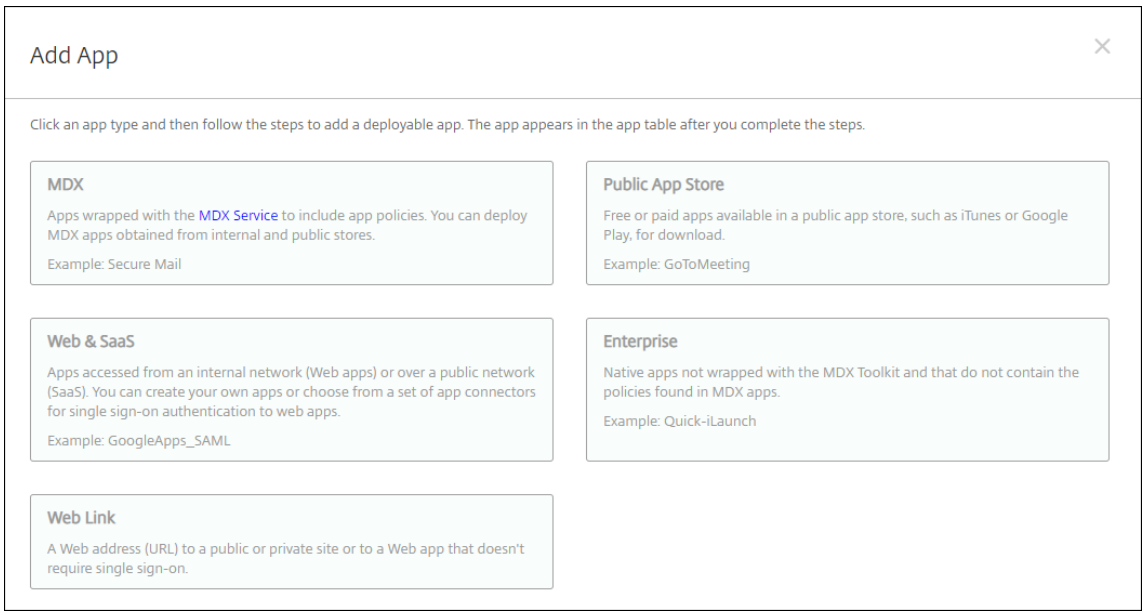
添加 **Web** 或 **SaaS** 应用程序

使用 Endpoint Management 控制台，可以向用户提供对企业应用程序、Web 应用程序和 SaaS 应用程序的单点登录 (SSO) 授权。

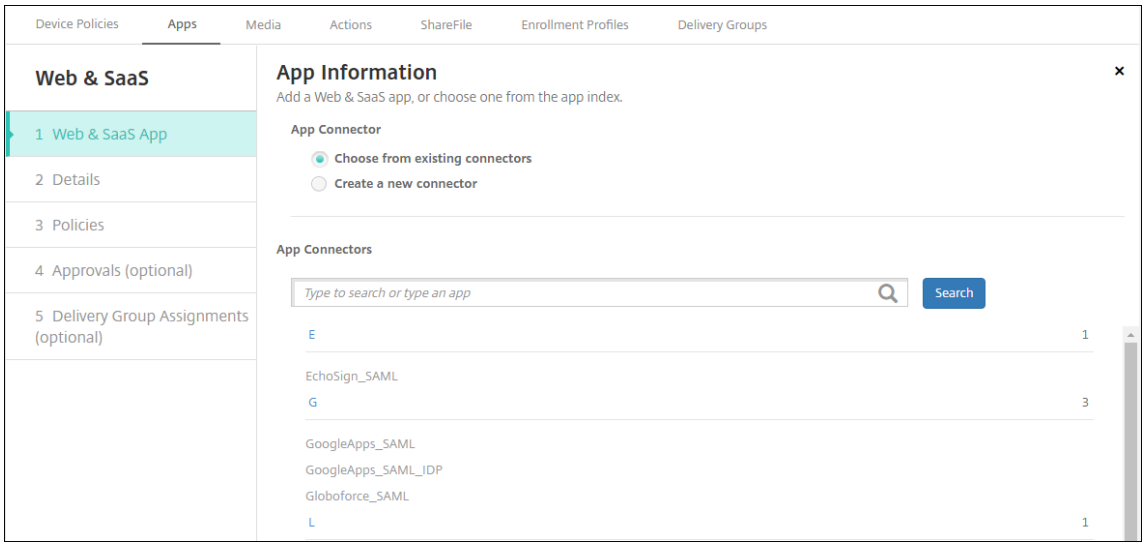
添加 Web 应用程序或 SaaS 应用程序时，您可以在 Endpoint Management 中构建自己的连接器。有关 Endpoint Management 中可用的连接器类型的列表，请参阅应用程序连接器类型。

如果应用程序仅可进行 SSO：保存设置后，应用程序将显示在 Endpoint Management 控制台的应用程序选项卡中。

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。



2. 单击 **Web** 和 **SaaS**。此时将显示应用程序信息页面。



3. 配置现有或新的应用程序连接器，如下所示。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

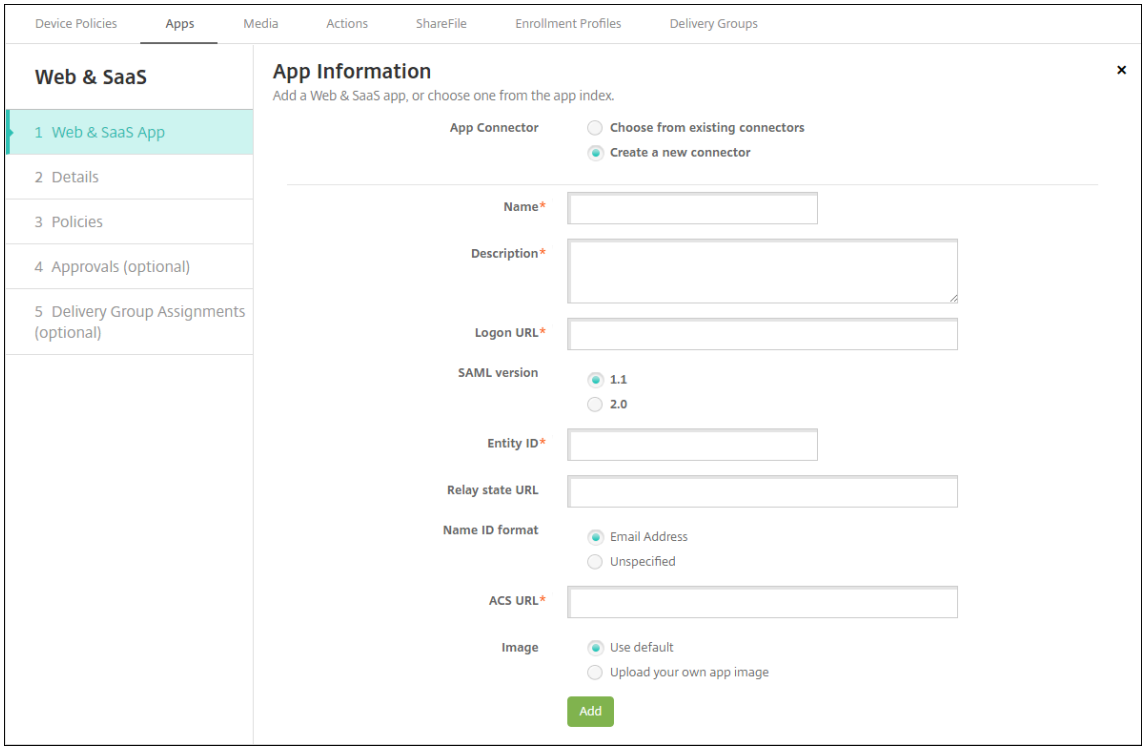
配置现有的应用程序连接器

1. 在应用程序信息页面中，从现有连接器中选择已选中，如上文所示。在“应用程序连接器”列表中单击要使用的连接器。此时将显示应用程序连接器信息。
2. 配置以下设置：
    - 应用程序名称：接受预先填充的名称或键入新名称。
    - 应用程序说明：接受预先填充的说明或键入自己的说明。
    - **URL**：接受预先填充的 URL 或键入应用程序的 Web 地址。根据您选择的连接器，此字段可以带有占位符，您必须替换占位符才能前进到下一个页面。
    - 域名：如果适用，键入应用程序的域名。此字段为必填字段。
    - 应用程序托管在内部网络中：选择应用程序是否在内部网络中的服务器上运行。如果用户从远程位置连接到内部应用程序，则必须通过 Citrix Gateway 进行连接。将此选项设置为开将向应用程序添加 VPN 关键字，并允许用户通过 Citrix Gateway 连接。默认值为关。
    - 应用程序类别：在此列表中，单击要应用于应用程序的可选类别。
    - 用户帐户配置：选择是否为应用程序创建用户帐户。如果您使用 Globoforce_SAML 连接器，则必须启用此选项才能提供无缝的 SSO 集成。
    - 如果启用用户帐户预配，请配置以下设置：
        - 服务帐户
            - 用户名：键入应用程序管理员的名称。此字段为必填字段。
            - 密码：键入应用程序管理员密码。此字段为必填字段。
        - 用户帐户
            - 用户授权结束时：在列表中，单击不再允许用户访问应用程序时采取的操作。默认值为禁用帐户。
        - 用户名规则
            - 对于要添加的每项用户名规则，请执行以下操作：
                - 用户属性：在列表中，单击要添加到规则中的用户属性。
                - 长度 **(**字符数**)**：在列表中，单击要在用户名规则中使用的用户属性字符数。默认值为全部。
                - 规则：您添加的每个用户属性自动附加到用户名规则中。
    - 密码要求
        - 长度：键入用户密码最小长度。默认值为 **8**。
    - 密码过期时间
        - 有效期 **(**天**)**：键入密码有效的天数。有效值为 **0–90**。默认值为 90。
        - 过期后自动重置密码：选择是否在密码过期时自动重置密码。默认值为关。如果不启用此字段，用户在其密码过期后将无法打开应用程序。

配置新的应用程序连接器

1. 在应用程序信息页面中，选择创建新连接器。此时将显示应用程序连接器字段。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



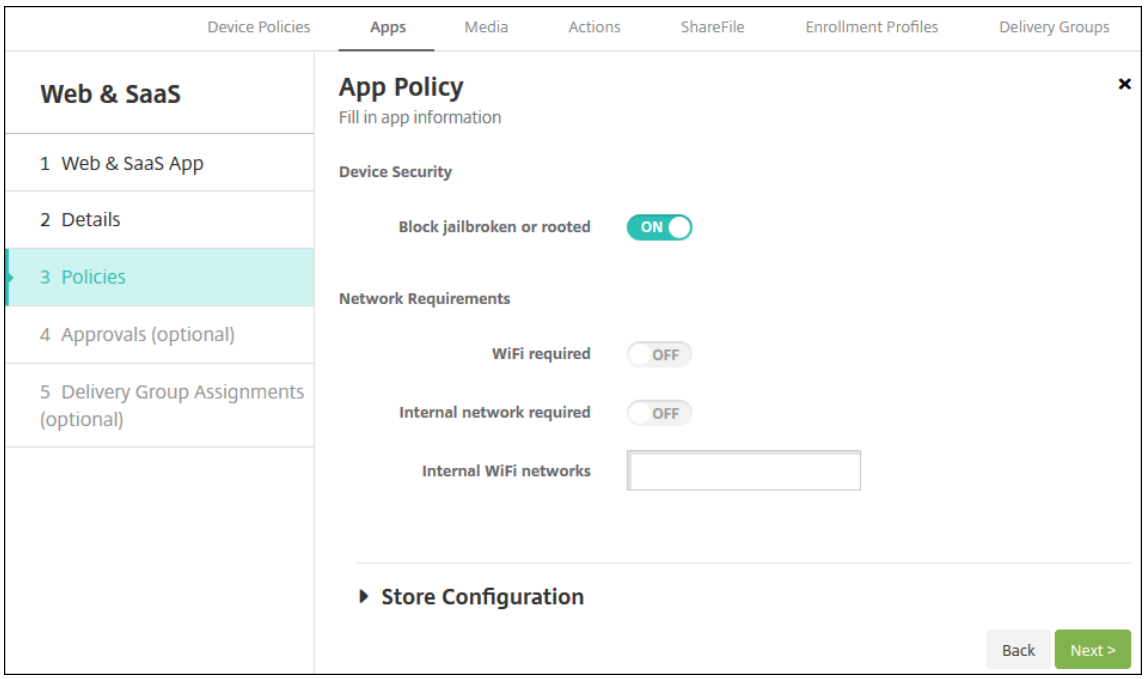
2. 配置以下设置：

   - 名称：键入连接器的名称。此字段为必填字段。
   - 说明：键入连接器的说明。此字段为必填字段。
   - 登录 **URL**：键入或复制并粘贴用户登录站点的 URL。例如，如果您要添加的应用程序有登录页面，请打开 Web 浏览器并访问该应用程序的登录页面。例如，它可能是 `https://www.example.com/logon`。此字段为必填字段。
   - **SAML** 版本：选择 **1.1** 或 **2.0**。默认值为 **1.1**。
   - 实体 **ID**：键入 SAML 应用程序的标识。
   - 中继状态 **URL**：键入 SAML 应用程序的 Web 地址。中继状态 URL 是来自应用程序的响应 URL。
   - 名称 **ID** 格式：选择电子邮件地址或未指定。默认值为电子邮件地址。
   - **ACS URL**：键入身份提供程序或服务提供商的声明使用者服务 URL。ACS URL 为用户提供 SSO 功能。
   - 图片：选择是使用默认 Citrix 图片还是上载您自己的应用程序图片。默认值为“使用默认值”。
     - 要上载自己的图片，请单击浏览并导航到文件所在位置。该文件必须是.PNG 文件。不能上载 JPEG 或 GIF 文件。如果添加自定义图形，以后将无法进行更改。

3. 完成后，单击添加。此时将显示详细信息页面。

4. 单击下一步。此时将显示应用程序策略页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

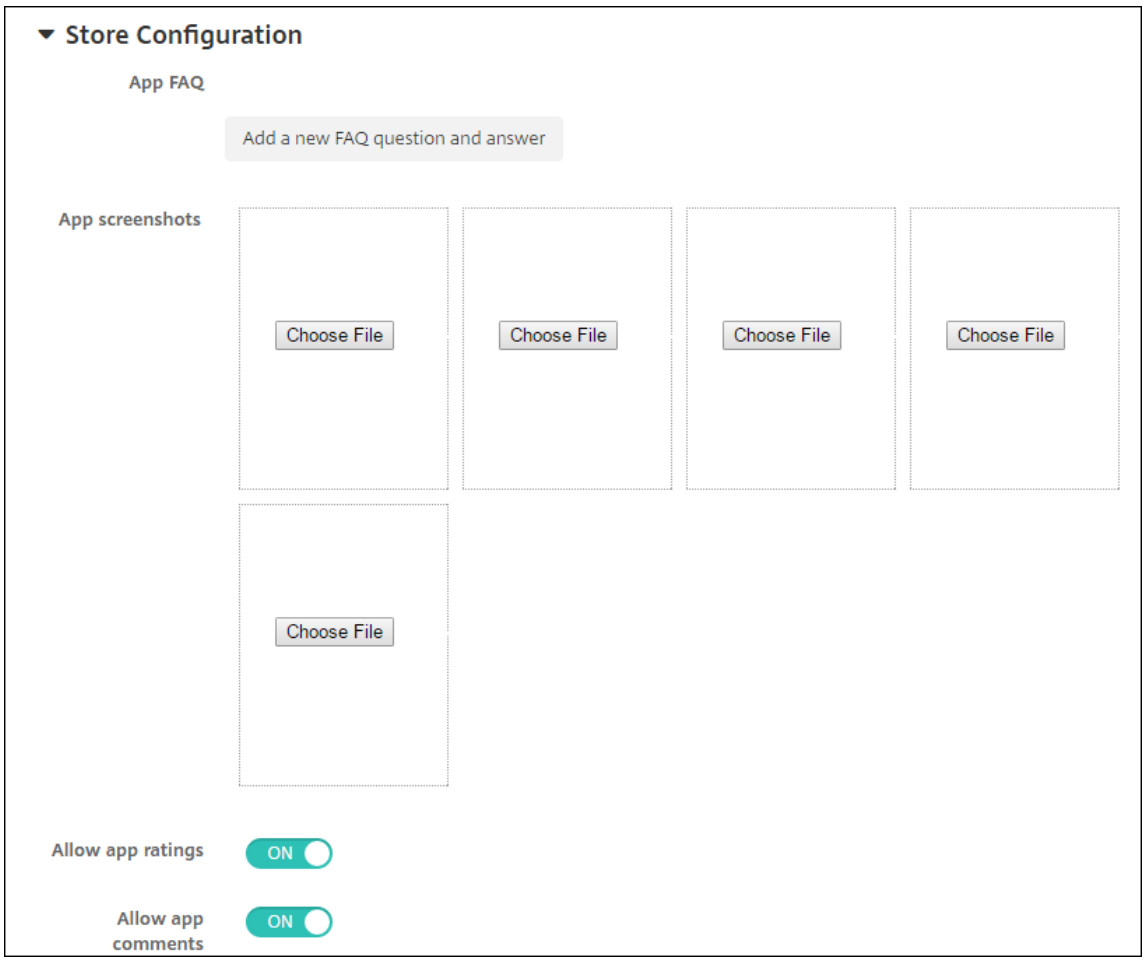


5. 配置以下设置：

   - 设备安全
   - 阻止越狱或获得 **Root** 权限：选择是否阻止已被越狱或获得 Root 权限的设备访问应用程序。默认值为开。
   - 网络要求
   - 需要连接 **WiFi**：选择运行应用程序是否需要使用 Wi-Fi 连接。默认值为关。
   - 需要连接内部网络：选择运行应用程序是否需要使用内部网络。默认值为关。
   - 内部 **WiFi** 网络：如果启用了需要连接 **Wi-Fi**，请键入要使用的内部 Wi-Fi 网络。

6. 展开应用商店配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

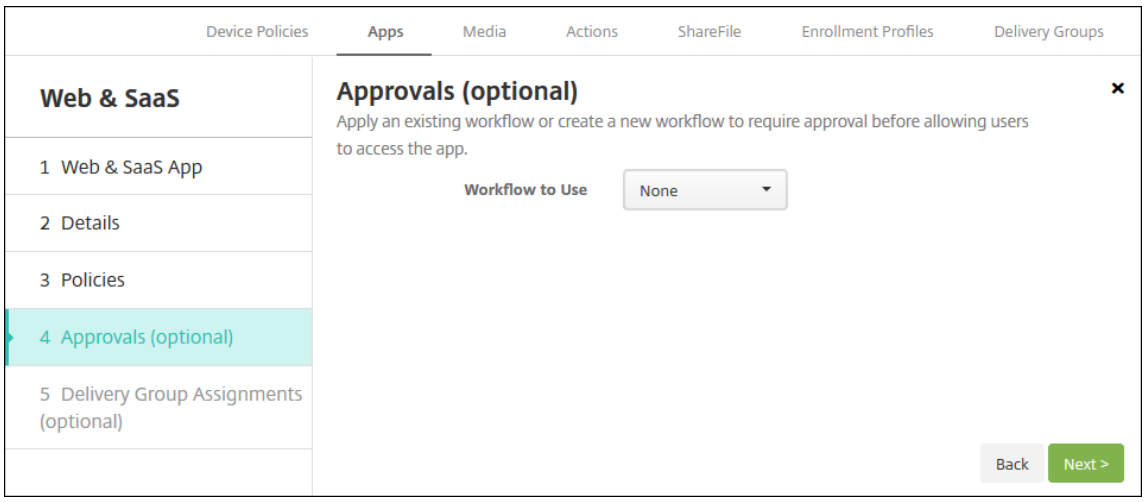


或者，您可以配置以下内容：

- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

7. 单击下一步。此时将显示审批页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果您不需要审批工作流程，请继续执行下一步。

8. 单击下一步。此时将显示交付组分配页面。
9. 在选择交付组旁边，键入以查找交付组或者选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。
10. 展开部署计划，然后配置以下设置：

    - 部署：选择是否将应用程序部署到设备。默认值为开。
    - 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
    - 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

    如果在设置 **>** 服务器属性中配置了计划后台部署密钥，为始终启用的连接部署选项适用。

    始终启用选项：

    - 不适用于 iOS 设备
    - 不适用于开始使用版本为 10.18.19 或更高版本的 Endpoint Management 的 Android 和 Android Enterprise 客户
    - 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用

    配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。
11. 单击保存。

添加企业应用程序

Endpoint Management 中的企业应用程序是您开发或从其他来源获得的私有应用程序。除了作为启用了 MDX 的应用程序交付的专用 Android Enterprise 应用程序外，企业应用程序未使用 MAM SDK 或 MDX Toolkit 准备。可以在

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

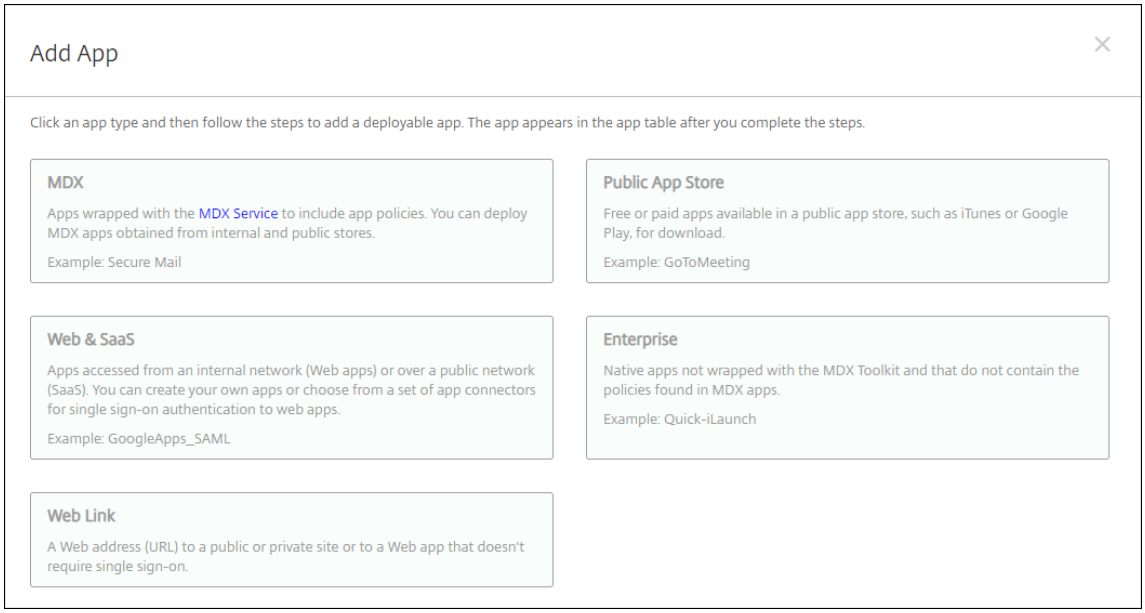
Endpoint Management 控制台中的应用程序选项卡中上载企业应用程序。企业应用程序支持以下平台（和相应的文件类型）：

- iOS（.ipa 文件）
- macOS（.pkg 文件）

  Endpoint Management 不限制您上传的 PKG 文件的大小，但会限制文件上传时间。默认情况下，您必须在 100 秒内完成上传。有关详细信息，请参阅服务器属性。
- Android（.apk 文件）
- Android Enterprise（.apk 文件）
- 另请参阅：将 Win32 应用程序添加为企业应用程序
- 另请参阅：启用了 MDX 的专用应用程序

不支持将从 Google Play 商店下载的应用程序添加为企业应用程序。将 Google Play 应用商店中的应用程序添加为公共应用商店应用程序。请参阅添加公共应用商店应用程序。

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。

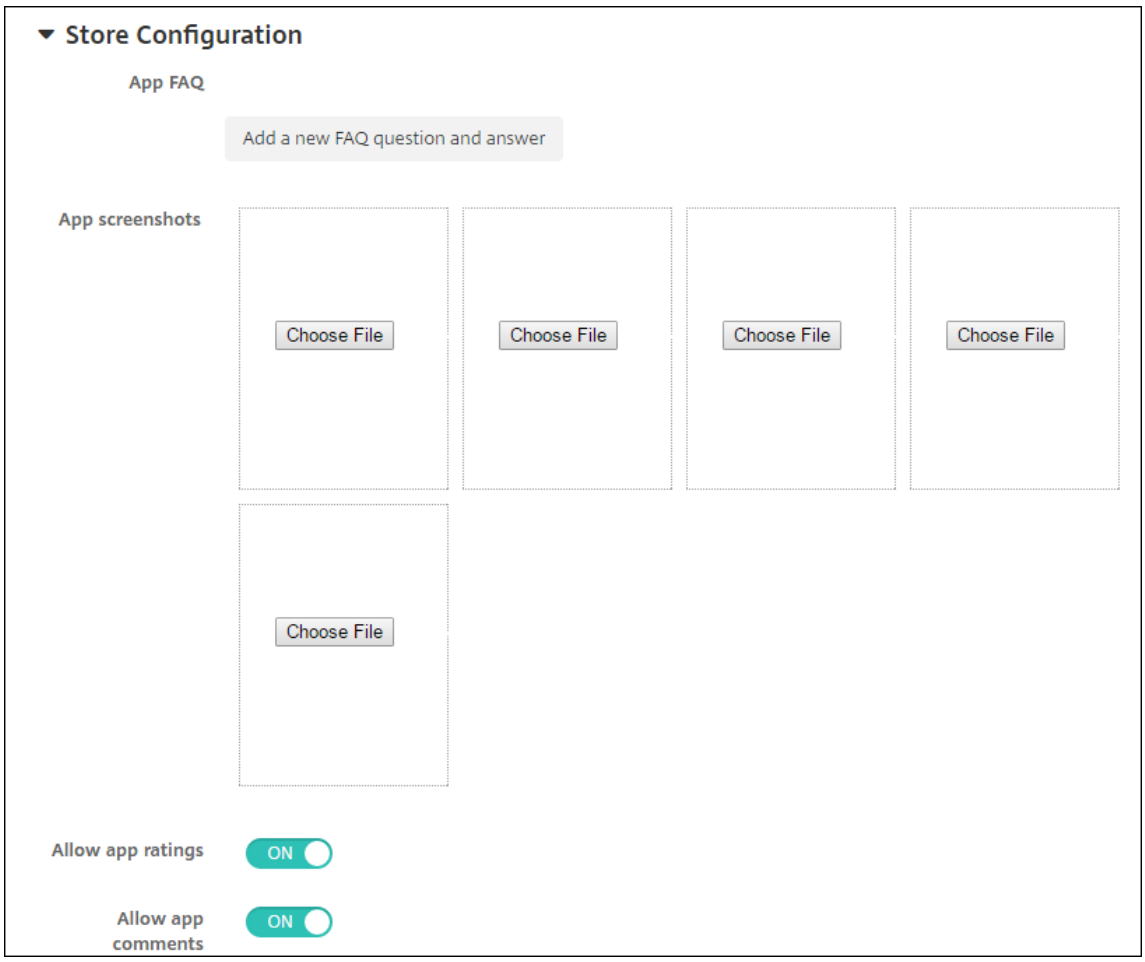


2. 单击企业。此时将显示应用程序信息页面。
3. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 单击下一步。此时将显示应用程序平台页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 在平台下，选择要添加的平台。如果您只为一个平台进行配置，请取消选中其他平台。
6. 对于所选的每个平台，单击上载并导航到要上载的文件所在位置，选择此文件。
7. 单击下一步。此时将显示平台的应用程序信息页面。
8. 为平台类型配置设置，例如：
    - 文件名：（可选）键入应用程序的新名称。
    - 应用程序说明：（可选）键入应用程序的新说明。
    - 应用程序版本：无法更改此字段。
    - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
    - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
    - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
    - 软件包 **ID**：您的应用程序的唯一标识符。
    - 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否从设备中删除应用程序。默认值为开。此设置不适用于 macOS。
    - 阻止备份应用程序数据：选择是否阻止应用程序备份数据。默认值为开。此设置不适用于 macOS。
    - 强制管理应用程序：选择是否将应用程序作为托管应用程序安装在未受监督的设备上。设备类型决定了启用后 Endpoint Management 处理此设置的方式。如果启用了此设置，应用程序将更新但不提示用户。无论应用程序是必需的还是可选的，都会进行更新。默认值为关。
        - 对于 iOS 设备，如果已安装应用程序，用户会收到允许托管该应用程序的提示。如果将某个应用程序部署到不存在该应用程序的设备，则无论此设置的状态如何，该应用程序都将安装为托管应用程序。在 iOS 9.0 及更高版本中可用。对于通过用户注册注册的 iOS 设备，Endpoint Management 不强制执行此设置，也不提示用户允许应用程序管理。
        - 对于 macOS 设备，请启用该设置，然后将应用程序部署到设备。该应用程序会自动安装为托管应用程序。用户不会收到任何提示。如果将某个应用程序部署到不存在该应用程序的设备，则无论此设置的状态如何，该应用程序都将安装为托管应用程序。适用于 macOS 11.0 及更高版本。
9. 配置部署规则。有关详细信息，请参阅配置部署规则。
10. 展开应用商店配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



或者，您可以配置以下内容：

- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

11. 单击下一步。此时将显示审批页面。

    要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果您不需要审批工作流程，请继续执行下一步。

12. 单击下一步。此时将显示交付组分配页面。

13. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。

14. 展开部署计划，然后配置以下设置：

    - 部署：选择是否将应用程序部署到设备。默认值为开。
    - 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

如果在设置 **>** 服务器属性中配置了计划后台部署密钥，为始终启用的连接部署选项适用。

始终启用选项：

- 不适用于 iOS 设备
- 不适用于开始使用版本为 10.18.19 或更高版本的 Endpoint Management 的 Android 和 Android Enterprise 客户
- 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用

配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

15. 单击保存。

将 **Win32** 应用程序添加为企业应用程序

可以将适用于 Win32 应用程序的 MSI、APPX、AppxBundle、PS1 或 EXE 文件上载到 Endpoint Management 以便为托管的 Windows 10 和 Windows 11 Desktop 和 Tablet 设备进行部署。使用 Endpoint Management 部署这些文件后，Windows 设备随后将按如下所示安装应用程序：

- 如果升级后的应用程序在安装过程中删除旧版本，设备将仅包括升级后的应用程序。
- 如果升级后的应用程序无法删除旧版本，但可以安装新版本，则设备包含该应用程序的两个版本。Endpoint Management 不再有旧版本的信息。
- 如果旧版本存在时升级后的应用程序无法安装，则新应用程序将不安装。在这种情况下，首先部署应用程序卸载设备策略以删除旧版本。然后，部署新版本。

要求

- Windows 10（版本 1607 或更高版本）或 Windows 11
- Windows 10 Professional 或 Windows 11 Professional
- Windows 10 Enterprise 或 Windows 11 Enterprise
- 通过 /quiet 选项安装的单机版 Win 32 MSI 应用程序。对于此部署用例，Microsoft 不支持具有多个应用程序、嵌套的 MSI 或交互式安装的 MSI。

查找元数据

向 Endpoint Management 中添加 Win32 应用程序时，请指定该应用程序的元数据。要查找元数据，请使用 Windows 计算机上的 Orca 应用程序并记录以下信息：

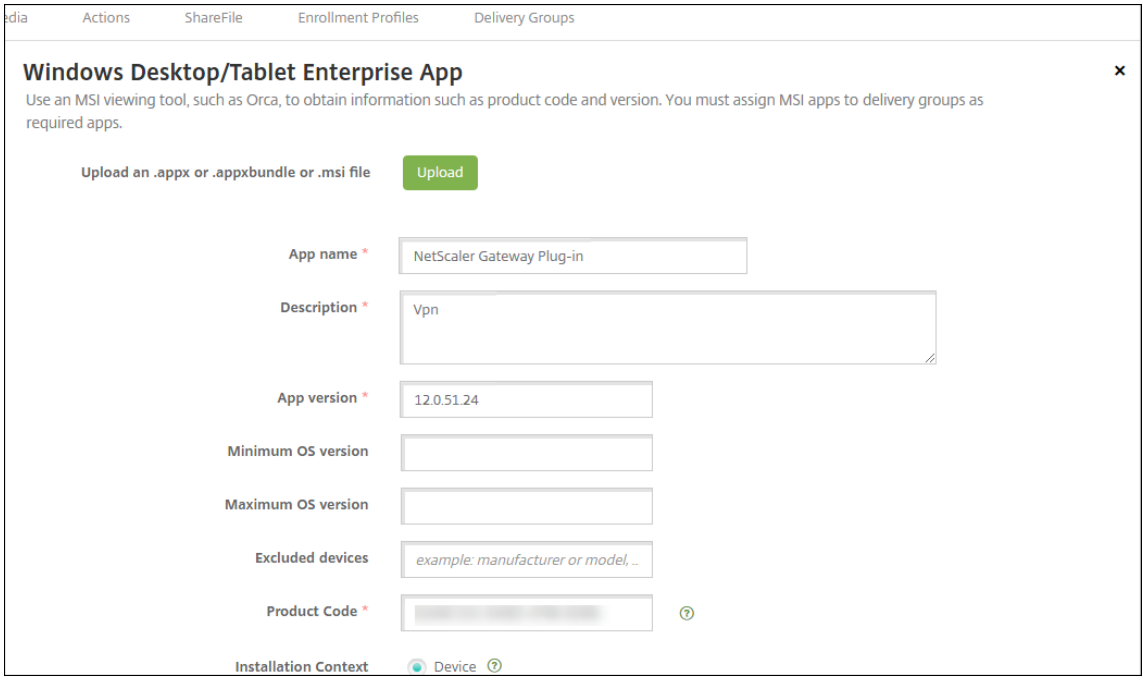
- 产品代码
- 产品名称
- 产品版本

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 软件包安装类型，即每用户或每计算机

将 **Win32** 应用程序添加到 **Endpoint Management**

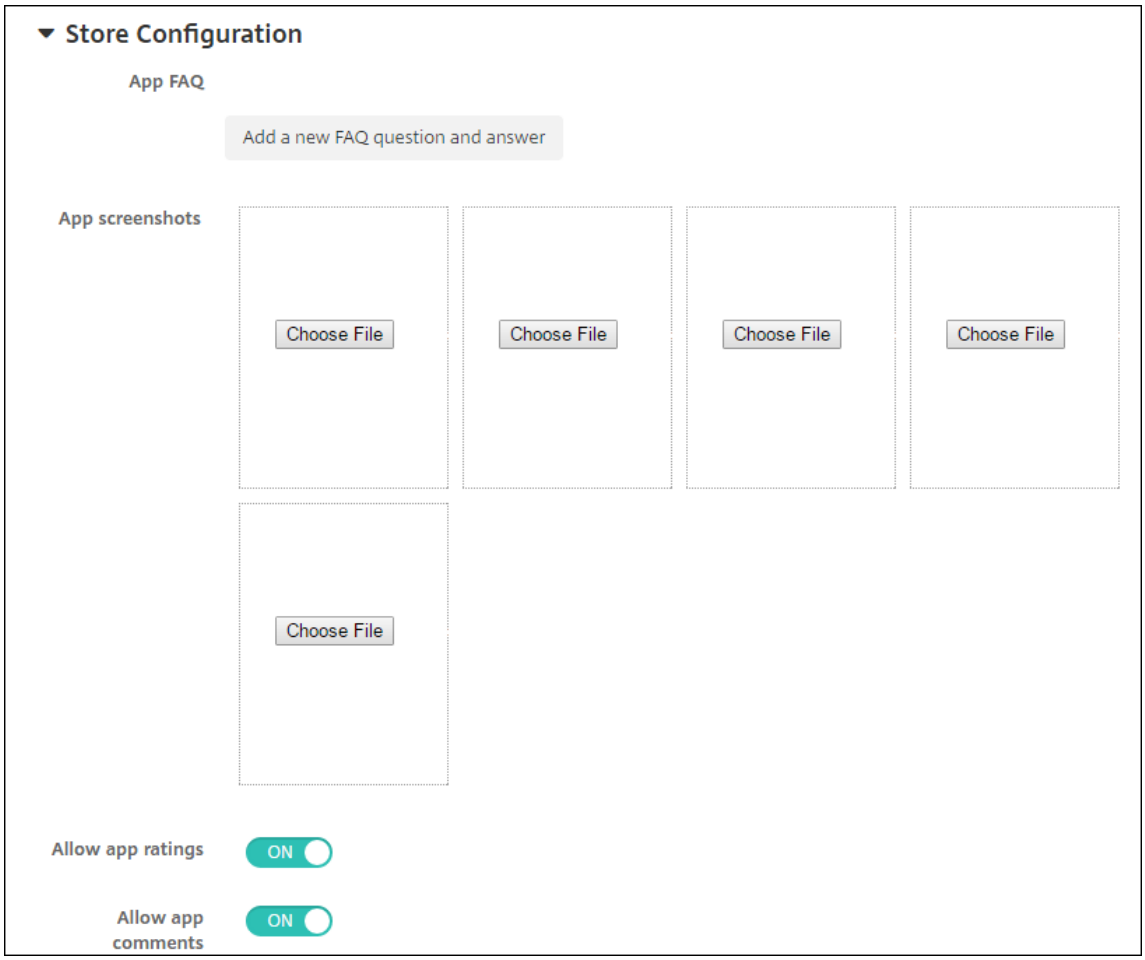
1. 转至配置 **>** 应用程序，单击企业，然后在应用程序信息页面中键入应用程序的名称。
2. 取消选中除 **Windows Desktop/Tablet** 之外的所有“平台”复选框。
3. 在 **Windows Desktop/Tablet** 企业应用程序页面上，单击上载并导航到该文件。
4. 配置以下设置：



- 应用程序名称：应用程序的名称，来自应用程序元数据。
- 说明：应用程序的说明。
- 应用程序版本：应用程序版本号，来自应用程序元数据。
- 最低操作系统版本：可选。设备可以运行以使用该应用程序的最旧操作系统版本。
- 最高操作系统版本：可选。设备必须运行才能使用该应用程序的最新操作系统。
- 排除的设备：可选。无法运行应用程序的设备的制造商或型号。
- 产品代码： UUID 格式的 MSI 应用程序产品代码，来自应用程序元数据。
- 安装上下文：根据应用程序元数据，选择应用程序是针对设备还是针对用户安装。此设置不适用于 EXE 文件。
- 命令行：调用 MSIEXEC.exe 时使用的命令行选项
- 安装命令行：添加用于无提示安装 EXE 文件的命令行参数。
- 卸载命令行：添加命令行参数以无提示方式卸载 EXE 文件。
- 重试次数：将安装标记为失败之前，可以重试安装和下载操作的次数。
- 超时：安装程序将安装解释为失败并且不再监视该过程之前，安装过程运行的分钟数。
- 重试时间间隔：两次重试操作之间的分钟数。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

5. 配置部署规则。有关详细信息，请参阅配置部署规则。
6. 展开应用商店配置。



或者，您可以配置以下内容：

- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

7. 单击下一步，直至系统显示摘要页面，然后单击保存。
8. 转至配置 > 交付组，并添加 Win32 应用程序作为必需应用程序。
9. 部署应用程序后，让您的用户知晓该应用程序可用。

升级 **Win32** 应用程序

1. 查找应用程序的元数据，如前面部分“查找元数据”中所述。
2. 转至配置 > 应用程序以上载应用程序的新版本。更新应用程序版本。如果应用程序的新版本具有不同的产品代码，请更新该设置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

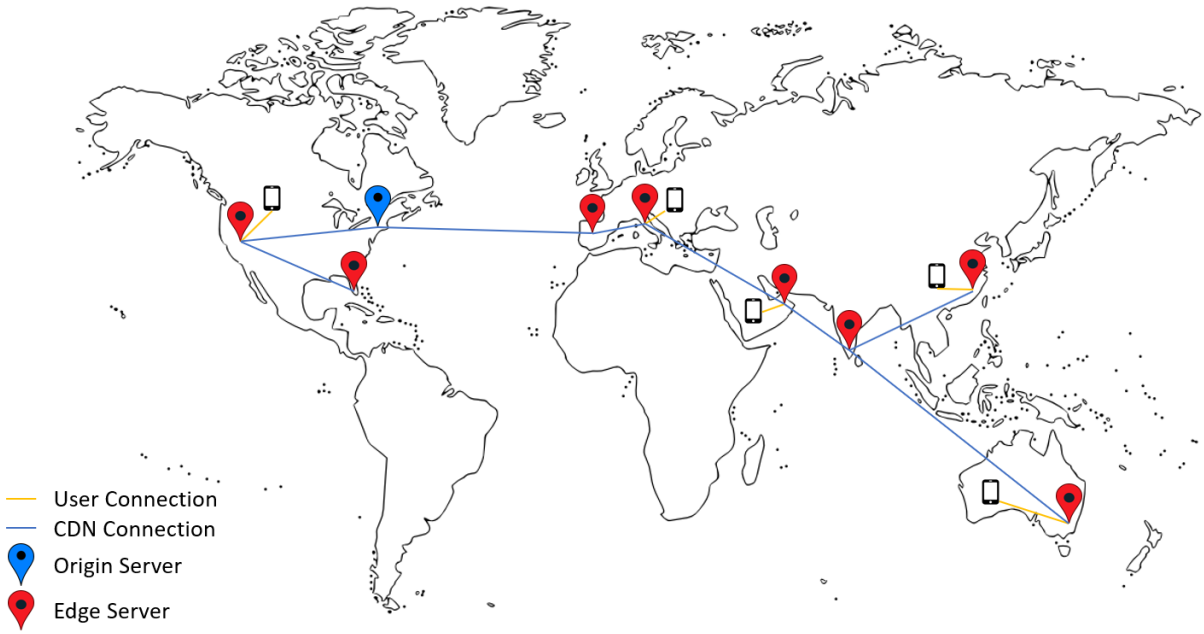
3. 提交所做的更改并部署应用程序。

从 **Citrix CDN** 交付企业和 **MDX** 应用

您可以从 Citrix 内容分发网络 (CDN) 交付企业和 MDX 应用程序。CDN 是指一组地理位置分散的服务器，它们协同工作以安全地提供应用程序内容的快速交付。本地服务器将应用程序交付给移动设备。

CDN 通过附近的 CDN 分发点将内容分发到靠近移动设备的地理位置，从而缩短了应用下载时间。CDN 将应用程序从最近的接入点 (POP) 位置交付给用户。

下图显示了 CDN 如何将应用程序分发到离移动设备用户最近的边缘服务器的示例。当移动设备请求应用程序时，边缘服务器将缓存来自原始服务器的内容。



用户可以使用 Secure Hub 连接到应用程序。添加应用程序时，Endpoint Management 会为其创建应用程序连接器。

针对企业应用程序的 Citrix CDN 支持适用于以下平台：

- iOS（MDM 或 MAM 注册）
- Android（MDM 或 MAM 注册）
- Windows Desktop 或 Tablet（MDM 注册）
- macOS（MDM 注册）

对 MDX 应用程序的 Citrix CDN 支持可用于以下平台：

- iOS（MDM 或 MAM 注册）
- Android（MDM 或 MAM 注册）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

CDN 的工作原理

作为 CDN 服务的核心，服务器连接在一起，以加快交付应用程序的速度。该目标通过将应用程序安全地放置在世界各地的不同分发点来实现。在初始连接到 Endpoint Management 服务器期间使用的移动设备的 DNS 服务器是决定分发点的因素。

例如：假设移动设备的 DNS 服务器 IP 源自佛罗里达州劳德代尔堡。CDN 使用离该位置最近的本地分发点将应用程序交付给移动设备。使用 CDN 可以缩短应用程序下载时间。

当移动设备首次请求或推送企业应用程序时，Endpoint Management 会将该应用程序复制到本地分发点，并将该应用程序保留 24 小时以供其他本地设备下载。

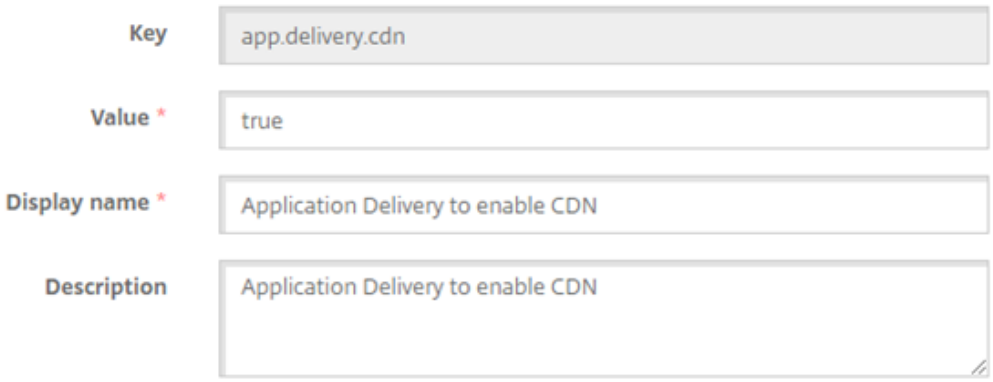
从 Citrix CDN 交付企业应用程序

在 Endpoint Management 版本 19.4.1 中，所有新的多租户客户的企业应用程序交付默认为 CDN 交付。对于本版本之前的现有客户，请按照本部分中的说明进行操作。

对于已经在 Endpoint Management 服务器上的企业应用程序，Endpoint Management 将继续从服务器交付这些应用程序，直到完成以下步骤后重新上传这些应用程序。

> 重要：
>
> 只有 Citrix Cloud 管理员才能为账户启用 CDN。仅当您以 Citrix Cloud 管理员角色登录时，服务器属性 `app.delivery.cdn` 才会在 Endpoint Management 中可见。有关 Citrix Cloud 管理员的信息，请参阅管理 Citrix Cloud 管理员。

1. 为您的帐户启用 CDN：在 Endpoint Management 控制台中：转到设置 **>** 服务器属性。
2. 搜索 `app.delivery.cdn`，然后单击编辑。
3. 将值更改为 **true**。



4. 在 Endpoint Management 控制台中，再次上载您的企业应用程序：
   a) 转到配置 **>** 应用程序，然后按类型（企业）和平台筛选应用程序列表。
   b) 选择一个应用程序，单击编辑，单击下一步，然后单击上载。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

c) 对每个企业应用程序重复上述步骤。

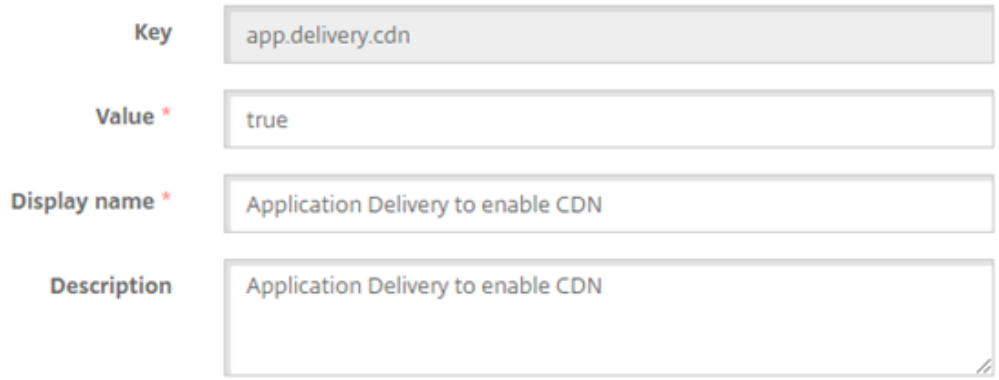
从 **Citrix CDN** 交付 **MDX** 应用程序

在 Endpoint Management 版本 20.12.0 中，对于所有新的多租户客户，MDX 应用程序交付默认为 CDN 交付。对于本版本之前的现有客户，请按照本部分中的说明进行操作。

对于已经在 Endpoint Management 服务器上的 MDX 应用程序，Endpoint Management 将继续从服务器交付这些应用程序，直到完成以下步骤后重新上传这些应用程序。

> 重要：
>
> 只有 Citrix Cloud 管理员才能为账户启用 CDN。仅当您以 Citrix Cloud 管理员角色登录时，服务器属性 `app.delivery.cdn` 才会在 Endpoint Management 中可见。有关 Citrix Cloud 管理员的信息，请参阅管理 Citrix Cloud 管理员。

1. 为您的帐户启用 CDN：在 Endpoint Management 控制台中：转到设置 **>** 服务器属性。
2. 搜索 `app.delivery.cdn`，然后单击编辑。
3. 将值更改为 **true**。



4. 在 Endpoint Management 控制台中，再次上传 MDX 应用程序：
   a) 前往 配置 **>** 应用程序，然后按 类型 (**MDX**) 和 平台筛选应用列表。
   b) 选择一个应用程序，单击编辑，单击下一步，然后单击上载。
   c) 对每个 MDX 应用程序重复上一步。

添加 **Web** 链接

Web 链接是指向 Internet 或 Intranet 站点的 Web 地址。Web 链接还可以指向不需要 SSO 的 Web 应用程序。Web 链接配置完成后，链接将以图标的形式显示在应用商店中。当用户通过 Secure Hub 登录时，将显示该链接以及可用应用程序和桌面的列表。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可以从 Endpoint Management 控制台中的应用程序选项卡配置 Web 链接。配置完 Web 链接后，该链接将以链接图标的形式显示在应用程序表中的列表中。当用户通过 Secure Hub 登录时，将显示该链接以及可用应用程序和桌面的列表。

观看此视频以了解更多：

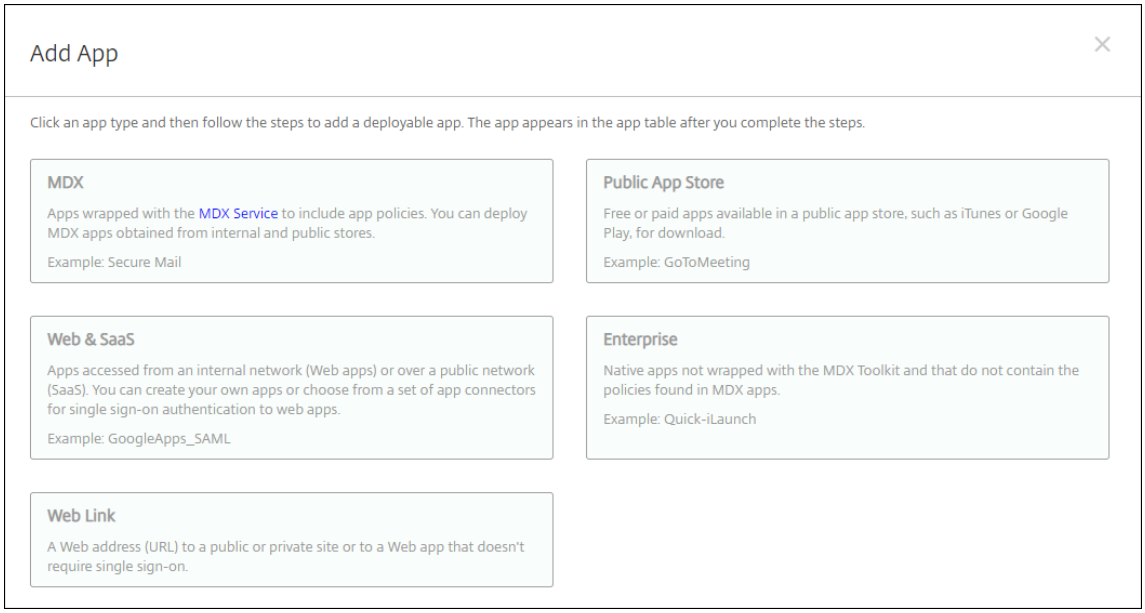


要添加链接，请提供以下信息：

- 链接的名称
- 链接的说明
- Web 地址 (URL)
- 类别
- 角色
- .png 格式的图片（可选）

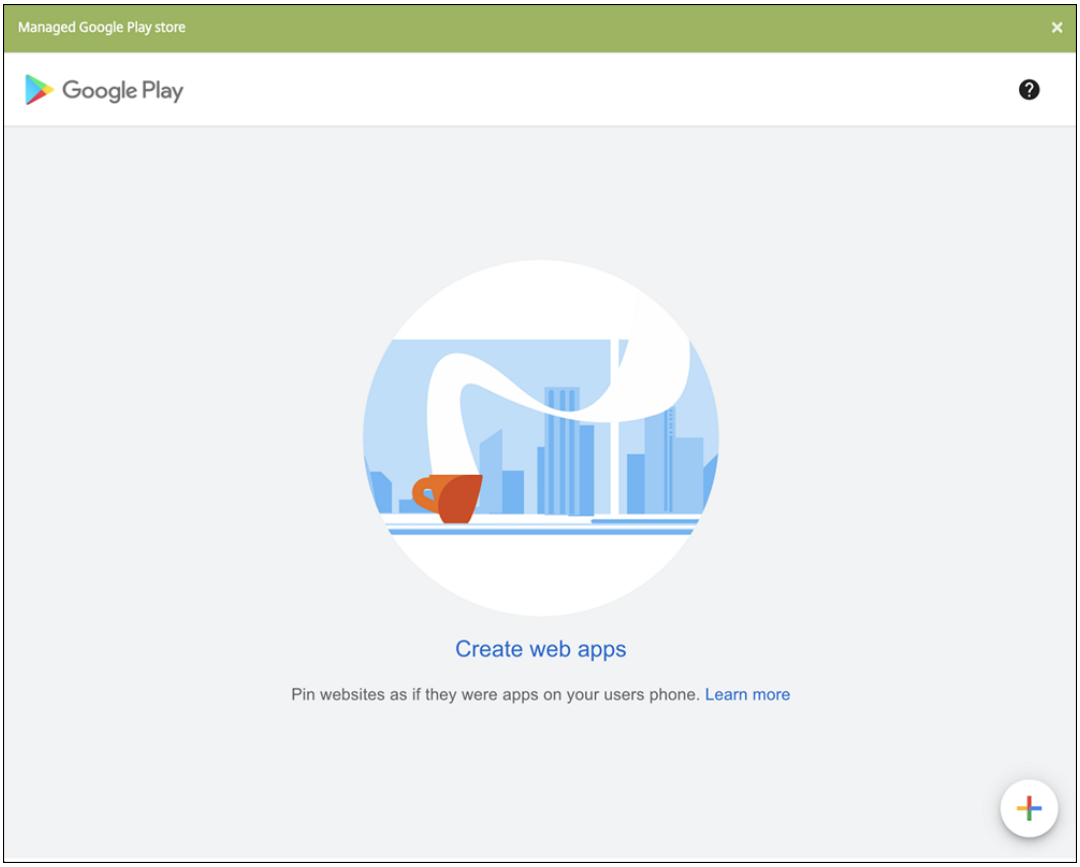
1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



2. 单击 **Web** 链接。此时将显示应用程序信息页面。
3. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 单击下一步。此时将显示应用程序平台页面。
5. 在平台下，选择其他平台以添加适用于 iOS、Android（旧版 DA）和 Windows 8 的 Web 应用程序，或者选择 **Android Enterprise**。清除您不想包含的所有平台的复选框。
   - 如果选择其他平台，请继续执行下一步以配置设置。
   - 如果选择 **Android Enterprise**，请单击上载按钮打开托管 Google Play 应用商店。您无需注册开发者帐户即可发布 Web 应用程序。单击右下角的加号图标以继续。

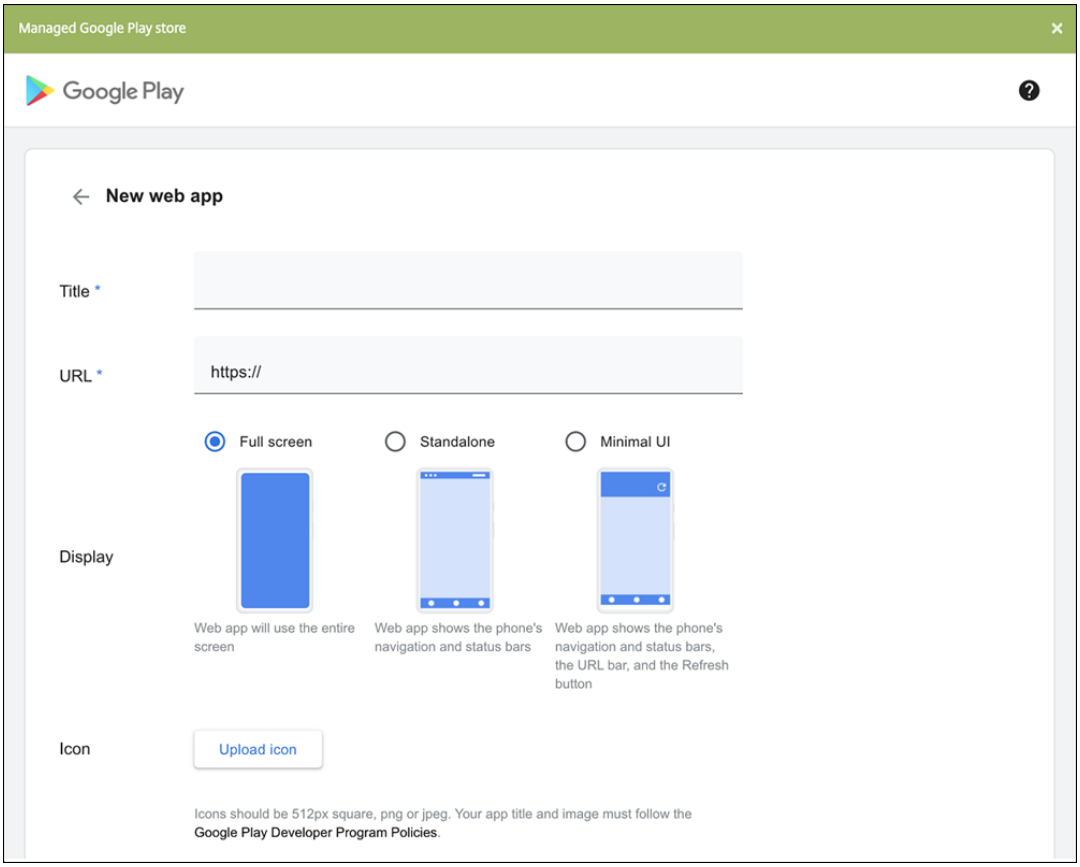
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



配置以下设置：

- 标题：键入 Web 应用程序的名称。
- **URL**：键入应用程序的 Web 地址。
- 显示：选择如何在用户设备上显示 Web 应用程序。可用选项包括全屏、独立和最小 **UI**。
- 图标：为 Web 应用程序上传您自己的图片。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



完成后，单击创建。您的 Web 应用程序最多可能需要 10 分钟才能发布。

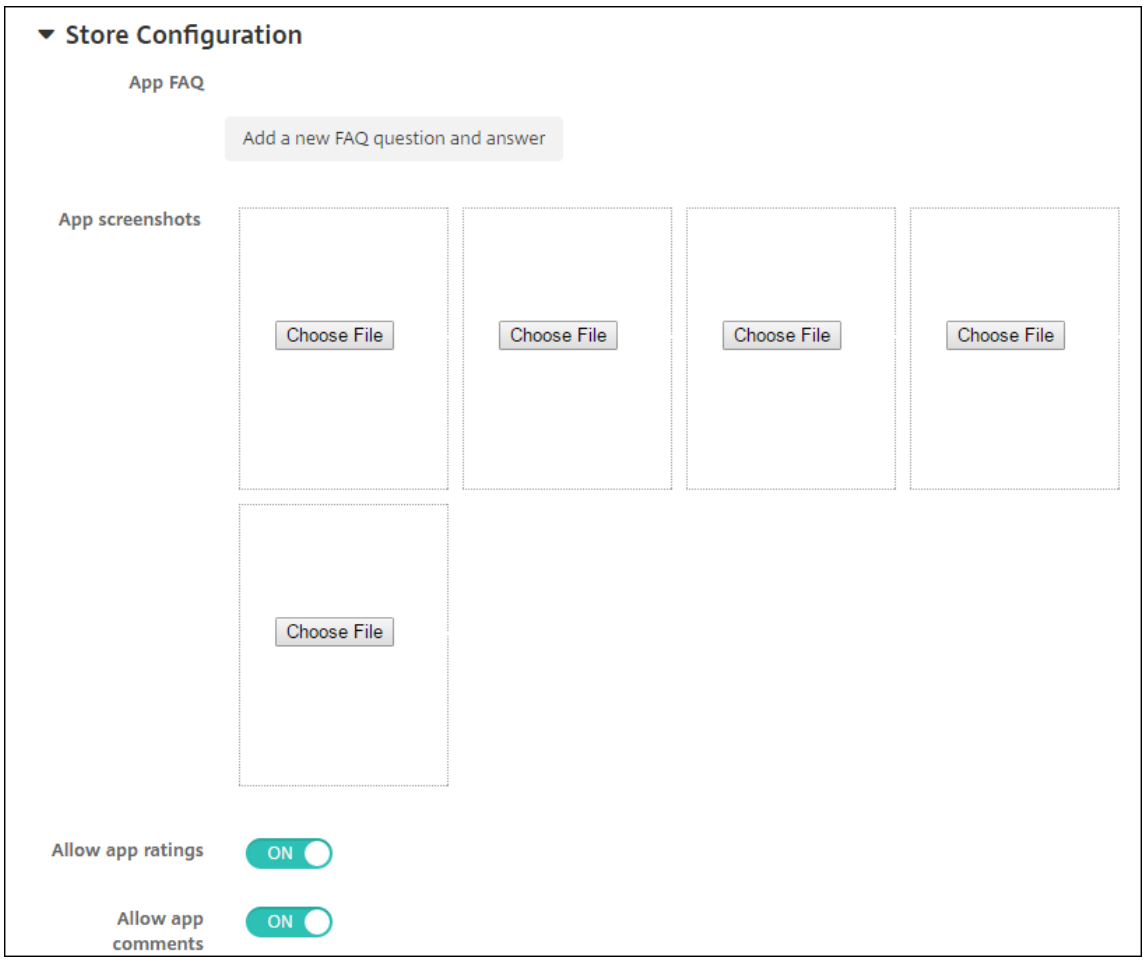
6. 对于 Android Enterprise 以外的平台，请配置以下设置：

   - 应用程序名称：接受预先填充的名称或键入新名称。
   - 应用程序说明：接受预先填充的说明或键入自己的说明。
   - **URL**：接受预先填充的 URL 或键入应用程序的 Web 地址。根据您选择的连接器，此字段可以带有占位符，您必须替换占位符才能前进到下一个页面。
   - 应用程序托管在内部网络中：选择应用程序是否在内部网络中的服务器上运行。如果用户从远程位置连接到内部应用程序，则必须通过 Citrix Gateway 进行连接。将此选项设置为开将向应用程序添加 VPN 关键字，并允许用户通过 Citrix Gateway 连接。默认值为关。
   - 应用程序类别：在此列表中，单击要应用于应用程序的可选类别。
   - 图片：选择是使用默认 Citrix 图片还是上载您自己的应用程序图片。默认值为 “使用默认值”。
     - 要上载自己的图片，请单击浏览并导航到文件所在位置。该文件必须是.PNG 文件。不能上载 JPEG 或 GIF 文件。如果添加自定义图形，以后将无法进行更改。

7. 配置部署规则。有关详细信息，请参阅配置部署规则。

8. 展开应用商店配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



或者，您可以配置以下内容：

- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

9. 单击下一步。此时将显示交付组分配页面。
10. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。
11. 展开部署计划，然后配置以下设置：

    - 部署：选择是否将应用程序部署到设备。默认值为开。
    - 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
    - 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

    如果在设置 **>** 服务器属性中配置了计划后台部署密钥，为始终启用的连接部署选项适用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

始终启用选项：

- 不适用于 iOS 设备
- 不适用于开始使用版本为 10.18.19 或更高版本的 Endpoint Management 的 Android 和 Android Enterprise 客户
- 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用

配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

12. 单击保存。

启用 **Microsoft 365** 应用程序

可以打开 MDX 容器以允许 Secure Mail、Secure Web 和 Citrix Files 向 Microsoft Office 365 应用程序传输文档和数据。有关详细信息，请参阅允许与 Office 365 应用程序安全交互。

应用工作流

要指定或创建工作流，请配置以下设置：

- 要使用的工作流：在此列表中，单击现有工作流或单击创建新工作流。默认值为无。

  如果选择创建新工作流，请配置以下设置。

  - 名称：键入工作流的唯一名称。
  - 说明：（可选）键入工作流的说明。
  - 电子邮件审批模板：在列表中，选择要指定的电子邮件审批模板。单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
  - 经理审批级别：在列表中，选择此工作流所需的经理审批级别数。默认值为 1 级。可能的选项包括：
    * 不需要
    * 1 级
    * 2 级
    * 3 级
  - 选择 **Active Directory** 域：在列表中，选择用于工作流的合适 Active Directory 域。
  - 查找所需的其他审批者：在搜索字段中键入其他所需人员的姓名，然后单击搜索。名称源于 Active Directory。
  - 姓名显示在此字段中后，选中姓名旁边的复选框。姓名和电子邮件地址显示在选定的其他所需审批者列表中。

    要从选定的其他所需审批者列表中删除人员，请执行以下操作之一：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

* 单击搜索以查找选定域中的所有人员列表。
* 在搜索框中键入完整姓名或部分姓名，然后单击搜索以限制搜索结果。
* 在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。滚动列表，并取消选中要删除的各个姓名旁边的复选框。

应用商店和 **Citrix Secure Hub** 外观方案

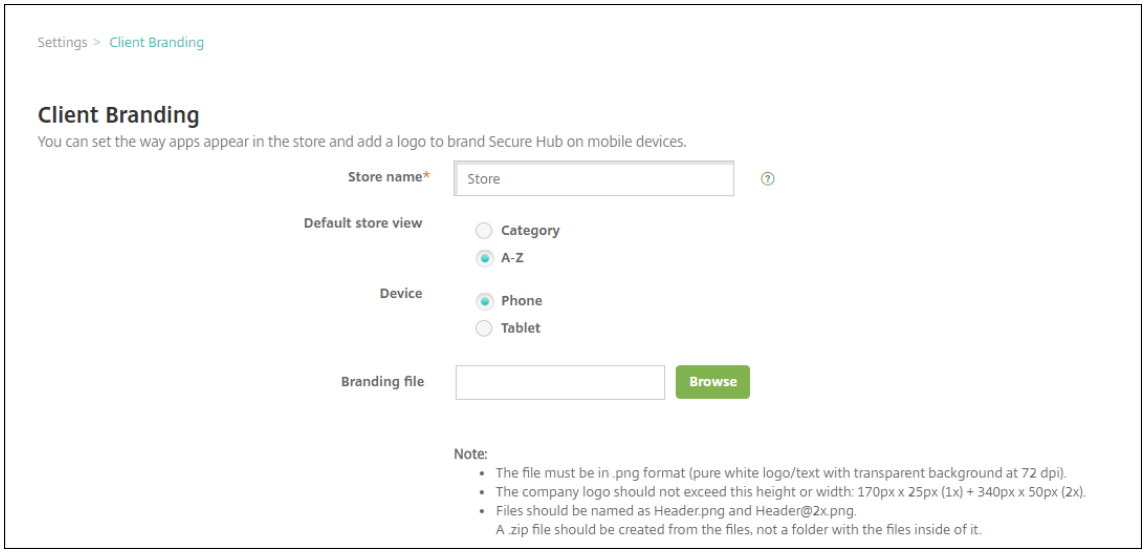
可以设置应用程序在应用商店中的显示方式，并将您的徽标添加到 Secure Hub 和应用商店中。这些标记功能适用于 iOS 和 Android 设备。

开始之前，请确保您的自定义图片已准备就绪并且可供访问。

自定义图片必须满足以下要求：

- 文件必须采用.png 格式
- 使用纯白徽标或文本以及 72 dpi 的透明背景。
- 公司徽标不能超过这个高度或宽度：170 px x 25 px (1x) 和 340 px x 50 px (2x)。
- 将文件命名为 Header.png 和 Header@2x.png。
- 从文件而不是文件所在的文件夹创建.zip 文件。

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在客户端下方，单击客户端外观方案。此时将显示客户端外观方案页面。



配置以下设置：

- 应用商店名称：应用商店名称显示在用户的帐户信息中。更改此名称也会更改用于访问应用商店服务的 URL。通常无需更改默认名称。

  > 重要：
  >
  > 商店名称只能包含字母数字字符。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 默认应用商店视图：选择类别或 **A-Z**。默认值为 **A-Z**。
- 设备选项：选择电话或平板电脑。默认值为电话。
- 外观方案文件：要选择外观方案图像或图像的.zip 文件，请单击浏览并导航到文件位置。

3. 单击保存。

要将此软件包部署到用户设备，请创建一个部署软件包，然后部署该软件包。

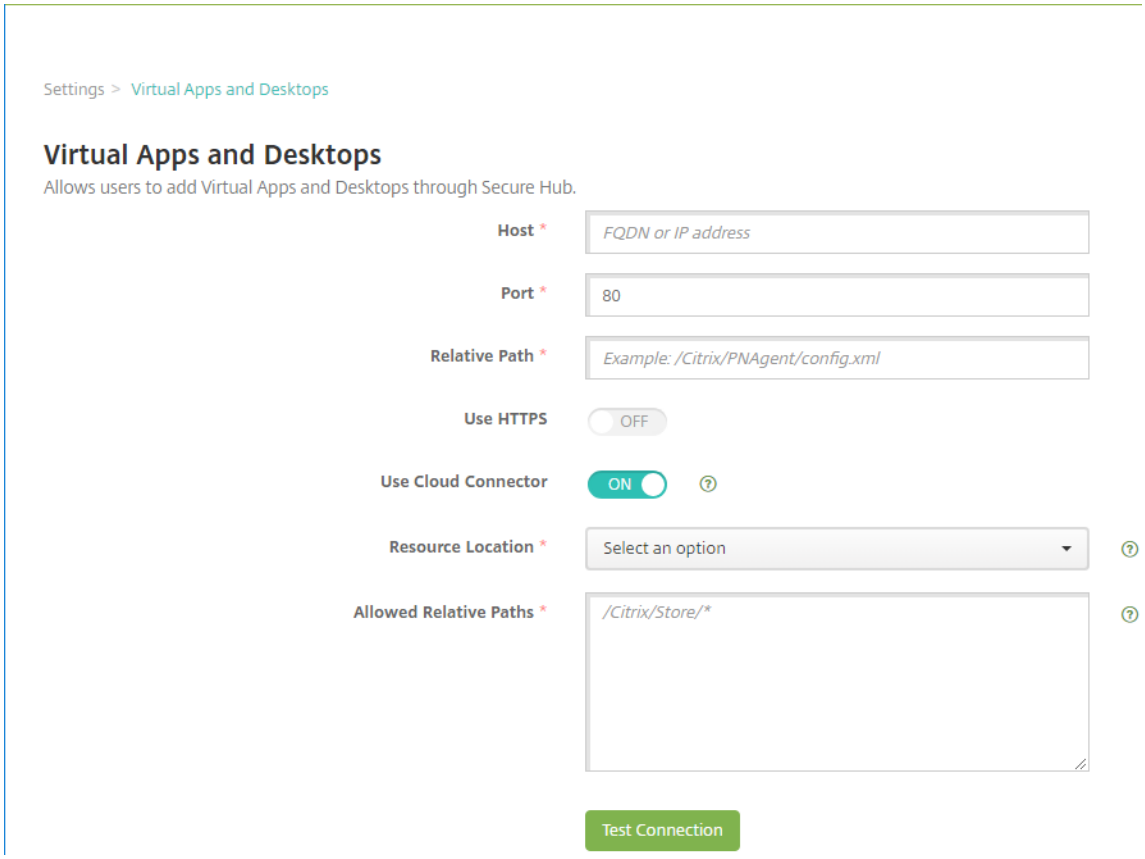
通过应用商店获取 **Citrix Virtual Apps and Desktops**

> 重要：
>
> 如果 Endpoint Management 启用了 Workspace，Citrix Workspace 将提供对 Virtual Apps and Desktops 的访问权限。本节中的设置不适用于您的站点。

Endpoint Management 可以从 Citrix Virtual Apps and Desktops 收集应用程序，并使应用程序在应用商店中向移动设备用户提供。用户可直接在应用商店中订购应用程序，并从 Citrix Workspace 启动这些应用程序。Citrix Workspace 应用程序必须安装在用户设备上才能启动应用程序。

要配置此设置，需要本地 StoreFront 的完全限定域名 (FQDN) 或 IP 地址和端口号。

1. 在 Endpoint Management Web 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击 **Virtual Apps and Desktops**。此时将显示 **Virtual Apps and Desktops** 页面。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 配置以下设置：

   - 主机：键入 StoreFront 的完全限定域名 (FQDN) 或 IP 地址。
   - 端口：键入 StoreFront 的端口号。默认值为 80。
   - 相对路径：键入路径。例如，/Citrix/PNAgent/config.xml
   - 使用 **HTTPS**：选择是否在 StoreFront 与客户端设备之间启用安全身份验证。默认值为关。
   - 使用 **Cloud Connector**：选择开可使用 Cloud Connector 连接到 StoreFront 服务器。然后，指定资源位置以及连接的允许使用的相对路径。
     - 资源位置：从在 Citrix Cloud Connector 中定义的资源位置进行选择。
     - 允许使用的相对路径：允许为指定资源位置使用的相对路径。每行请指定一个路径。可以使用星号 (*) 通配符。

     假定资源位置为 `https://storefront.company.com`，并且您希望提供对以下 URL 的访问权限：

     - `https://storefront.company.com/Citrix/PNAgent/Config.xml`
     - `https://storefront.company.com/Citrix/PNAgent/enum.aspx`
     - `https://storefront.company.com/Citrix/PNAgent/launch.aspx`

     要允许 URL 为 `https://storefront.company.com/Citrix/PNAgent/*` 的所有请求，请输入此路径：`/Citrix/PNAgent/*`

     Endpoint Management 会阻止所有其他路径。

4. 单击测试连接以验证 Endpoint Management 是否可以连接到指定的 StoreFront 服务器。
5. 单击保存。

应用程序连接器类型

September 14, 2020

下表列出了添加 Web 或 SaaS 应用程序时 Endpoint Management 中可用的连接器及连接器类型。还可以在添加 Web 或 SaaS 应用程序时向 Endpoint Management 添加新连接器。

表中指出连接器是否支持用户帐户管理。支持用户帐户管理时，您可以自动或通过工作流创建新帐户。

连接器名称	SSO SAML	支持用户帐户管理
EchoSign_SAML	Y	Y
Globoforce_SAML		注意：使用此连接器时，必须启用用户管理功能以进行预配以确保无缝 SSO 集成。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

连接器名称	SSO SAML	支持用户帐户管理
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y
Office365_SAML	Y	Y
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML*	Y	
ShareFile_SAML_SP*	Y	
WebEx_SAML_SP	Y	Y

* 如果您的站点启用了 Workspace，则不需要。

Citrix Launcher

December 3, 2021

Citrix Launcher 允许您自定义 Endpoint Management 部署的 Android Enterprise 设备和旧版 Android 设备的用户体验。借助 Citrix Launcher，您可以阻止用户访问某些设备设置，并将设备限制为一个应用程序或少数应用程序。

Citrix Launcher 的 Secure Hub 管理所支持的最低 Android 版本为 Android 6.0。

使用 启动器配置策略来控制这些 Citrix Launcher 功能：

- 管理 Android Enterprise 设备和旧版 Android 设备，以便用户只能访问您指定的应用程序。
- （可选）为 Citrix Launcher 图标指定自定义徽标图片以及为 Citrix Launcher 指定自定义背景图片。
- 指定用户必须键入的密码才能退出启动器。

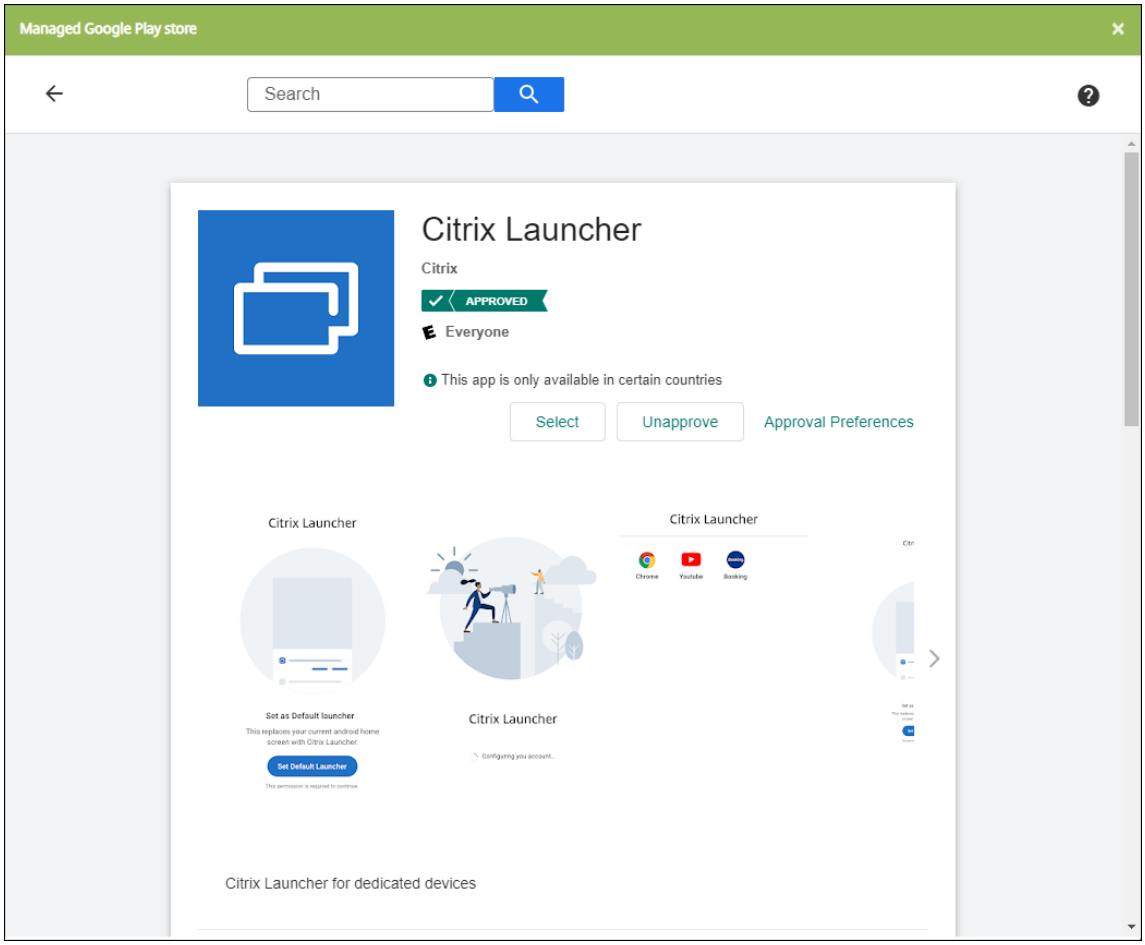
Citrix Launcher 并不打算成为设备平台已提供的额外安全层的安全保护。

为 **Android Enterprise** 设备设置 **Citrix Launcher**

1. 将 Citrix Launcher 应用程序（com.citrix.launcher.droid）作为公共商店应用程序添加到 Endpoint Management 中。在 配置 **>** 应用程序中，单击 添加，然后单击 公共应用商店。有关更多信息，请参阅 添加公

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

共应用商店应用程序。



2. 在 Kiosk 设备策略中，指定哪些应用必须在公司拥有的设备上可用于专用（也称为 Android 公司拥有的一次性使用 (COSU) 设备）。转到 配置 **>** 设备策略，单击 添加，然后选择 **Kiosk**。然后在允许列表中选择 Citrix Launcher 应用程序和任何其他应用程序。如果您之前将应用程序添加到列表中，则无需再次上传应用程序。有关详细信息，请参阅 Android Enterprise 设置。

3. 添加启动器配置设备策略。转到 配置 **>** 设备策略，单击 添加，然后选择 启动器配置。在启动器配置策略中，添加您在 Kiosk 策略中指定的任何应用程序。您无需添加在 Kiosk 策略中指定的所有应用程序。您必须仅在 Kiosk 策略中添加 Citrix Launcher 应用程序。有关详细信息，请参阅 Launcher 配置策略。

4. 创建交付组并部署资源。有关更多信息，请参阅本文中 的添加交付组和部署资源部 分。

在公司拥有的 Android Enterprise 设备上部署 Citrix Launcher 以供专用之后，Endpoint Management 将安装应用程序并替换默认的 Secure Hub 启动器。如果退出 Citrix Launcher 应用程序，Secure Hub 将再次成为默认启动器。

为旧版 **Android** 设备设置 **Citrix Launcher**

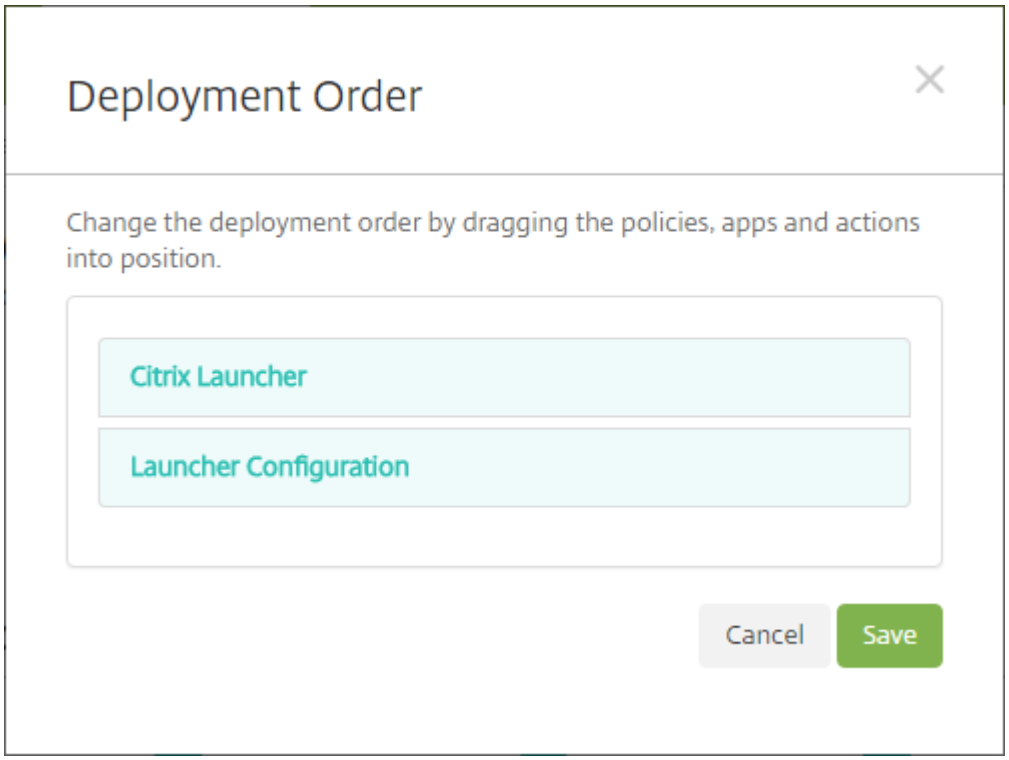
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 2020 年 8 月，Citrix 弃用了对旧版 Android 设备的 CitrixLauncher.apk 的支持。您可以在不收到新功能更新的情况下继续为 Android 设备使用旧版 Citrix Launcher 应用程序（com.citrix.launcher）。

1. 要找到 Citrix Launcher 应用程序，请转到 Citrix Endpoint Management 下载页面并搜索 **Citrix Launcher**。下载最新的文件。该文件已准备好上传到 Endpoint Management 中，不需要打包。
2. 添加启动器配置设备策略。转到 配置 **>** 设备策略，单击 添加，然后选择 启动器配置。有关详细信息，请参阅 Launcher 配置策略。
3. 将 Citrix Launcher 应用程序作为企业应用程序添加到 Endpoint Management。在配置 **>** 应用程序中，单击添加，然后单击企业。有关详细信息，请参阅添加企业应用程序。
4. 创建交付组并部署资源。有关更多信息，请参阅本文中 的添加交付组和部署资源部 分。

添加交付组并部署资源

1. 使用 “配置” **>** **“**交付组**”** 中的以下配置为 **Citrix Launcher** 创建交付组。
   - 在 策略页面上，添加 启动器配置策略。
   - 在应用程序页面上，将 **Citrix Launcher** 拖动到必需应用程序。
   - 在摘要页面上，单击部署顺序并确保 **Citrix Launcher** 应用程序位于 **Launcher** 配置策略之前。



2. 通过向交付组中的所有用户发送推送通知，将资源部署到交付组。有关向交付组添加资源的更多信息，请参阅 部署资源。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

不使用 **Citrix Launcher** 管理设备

您可以使用已经可用的功能，而不是使用 Citrix Launcher。

要预配专用设备，请执行以下操作：

1. 通过将设 备所有者模式设置为专用设备来创建注册配置文件。请参阅 预配专用 Android Enterprise 设备 和 注册配置文件。
2. 创建 Kiosk 设备策略以将应用程序添加到允许列表并设置锁定任务模式。如果您之前将应用程序添加到列表中，则无需再次上传应用程序。有关详细信息，请参阅 Android Enterprise 设置。
3. 在您创建的注册配置文件中注册每台设备。

使用 **Apple** 批量购买功能添加应用程序

July 8, 2022

Apple 商务管理 (ABM) 和 AApple 校园教务管理 (ASM) 允许您批量购买应用程序和书籍的许可证，以及将批量购买信息与 Endpoint Management 同步。然后可以使用 Endpoint Management 将这些应用程序和书籍部署到 iOS 和 macOS 设备。批量购买内容简化了组织查找、购买和分发应用程序和书籍的过程。

有关使用 ABM 或 ASM 购买内容的详细信息，请参阅《Apple 商务管理用户指南》或《Apple 校园教管理用户指南》。本文介绍如何将从 ABM 和 ASM 批量购买的许可证同步到 Endpoint Management 以及如何管理这些许可证。

> 注意：
>
> 自 2021 年 1 月 14 日起，Apple 批量购买计划 (VPP) 不再提供。批量购买功能集成在 ABM 和 ASM 中。如果您当前使用设备注册计划 (DEP) 或 VPP，则可以升级到 ABM 或 ASM。有关详细信息，请参阅 Apple 文档 Upgrade from Apple Deployment Programs（从 Apple 部署计划进行升级）。

关于 **Apple** 批量购买

使用 ABM 或 ASM 批量购买内容时，请注意以下问题：

- 可以为以下内容购买许可证：
  - 公共应用程序和书籍
  - 专用于贵组织开发的自定义应用程序
- 可以将批量购买的应用程序和书籍部署到组织拥有的设备和 BYO 设备。通过 ABM 或 ASM 注册的组织拥有的设备支持 MDM 或 MDM+MAM 注册，但不支持 MAM 注册。
- 有关分发应用程序的信息，请参阅分发 Apple 应用程序。
- 有关已知问题的列表，请参阅知识中心文章 CTX222633。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

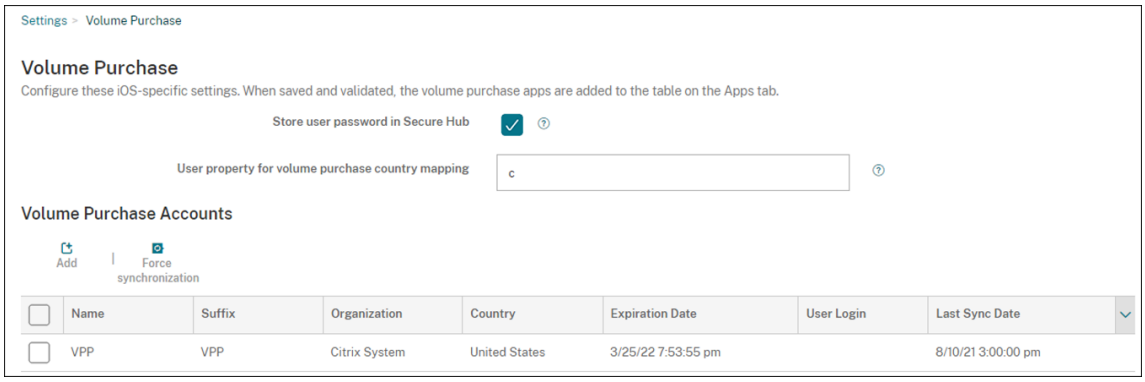
添加批量购买帐户

在 ABM 或 ASM 门户中购买内容后，请从该门户下载与 Endpoint Management 关联的内容令牌。然后，在 Endpoint Management 中，基于此内容代码创建一个批量购买帐户。此代码允许 Endpoint Management 同步来自 ABM 或 ASM 的内容许可证。

批量购买后，可以使用托管许可证购买内容并将其部署到设备。如果您当前使用兑换代码，并且希望更改为托管许可证，请参阅 Apple 支持文档。

在 Endpoint Management 中添加批量购买帐户

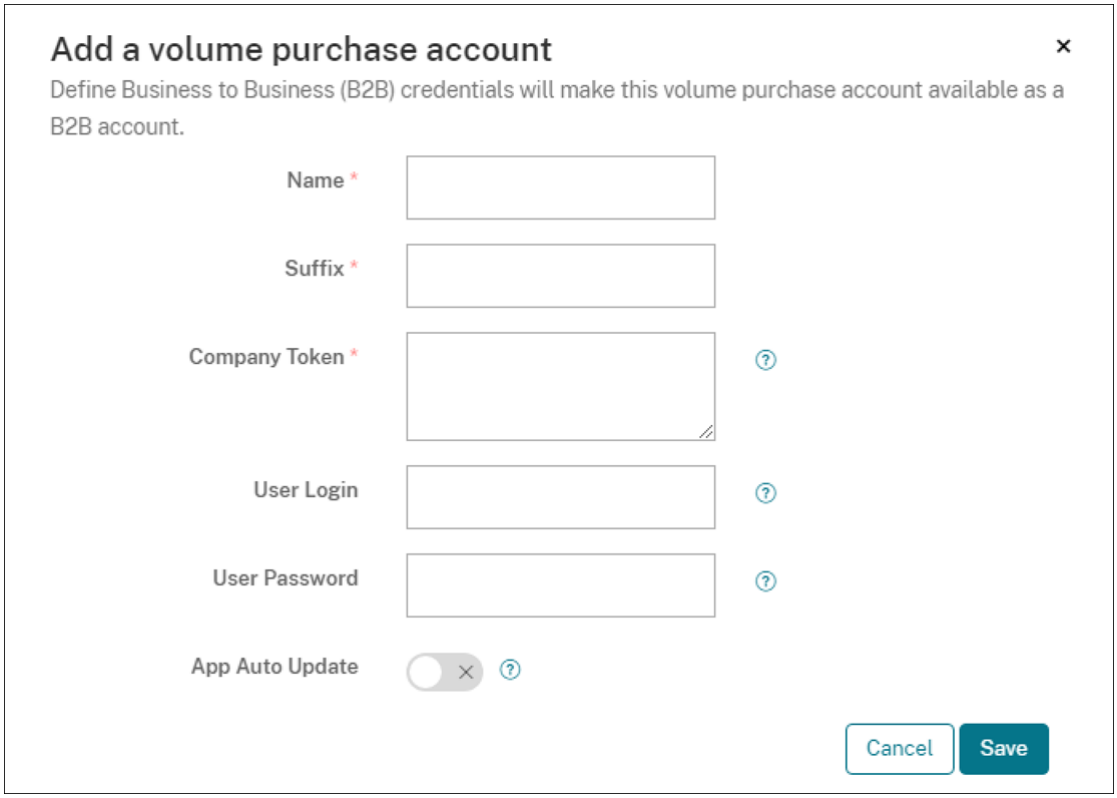
1. 在 ABM 或 ASM 门户中，根据需要购买内容，然后将内容代码文件下载到一个安全的位置。
2. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
3. 单击批量购买。此时将显示批量购买配置页面。



4. 配置以下设置：
   - 在 **Secure Hub** 中存储用户密码：选择是否将用户名和密码存储在 Secure Hub 中以用于 Endpoint Management 身份验证。默认值为开。
   - 批量购买国家/地区映射的用户属性：键入国家/地区映射代码以允许用户从国家/地区特定的应用商店下载应用程序。请联系您的内容管理员以获取此代码。

     Endpoint Management 使用国家/地区映射代码来选择批量购买的属性池。例如，如果用户属性是美国，若映射代码适用于英国，该用户将无法下载应用程序。
5. 单击添加。此时将显示添加批量购买帐户对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 配置以下帐户设置：

> 注意：
>
> 如果您使用 Apple Configurator 1，请按如下所示上载许可证文件：单击配置 > 应用程序，转至应用程序的平台页面，然后展开批量购买。

- 名称：键入帐户的描述性名称。
- 后缀：键入从 Apple 应用商店继承的应用程序名称中要出现的后缀。例如，如果输入 **VP**，**Secure Mail** 应用程序将在应用程序列表中显示为 **Secure Mail - VP**。
- 公司令牌：复制并粘贴您在步骤 1 中下载的内容令牌。
- 用户登录名：（可选）键入此批量购买帐户的管理员的用户名。如果已配置，则需要用户名和密码才能将批量购买的自定义应用程序同步到 Endpoint Management 中。
- 用户密码：（可选）键入您所键入的用户名对应的密码。
- 应用程序自动更新：如果设置为开，则在 Endpoint Management 控制台中批量购买的应用程序和可选应用程序将在新版本可用时自动更新。您仍然必须在 Endpoint Management 控制台中手动更新企业应用程序和公共应用商店应用程序。如果此设置设为关，您仍然可以在 Endpoint Management 控制台中手动更新购买批量购买的应用程序。应用程序在控制台中更新后，已安装该应用程序的设备也会收到该更新。默认值为关。

成功添加批量帐户后，将显示一条消息，通知您以下信息：

- 在配置 > 应用程序页面上，批量购买的应用程序将显示在应用程序列表中。显示的应用程序名称中附带您配置的后缀。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 在配置 > 媒体页面上，批量购买的书籍将显示在“媒体”列表中。显示的书籍名称中附带您配置的后缀。

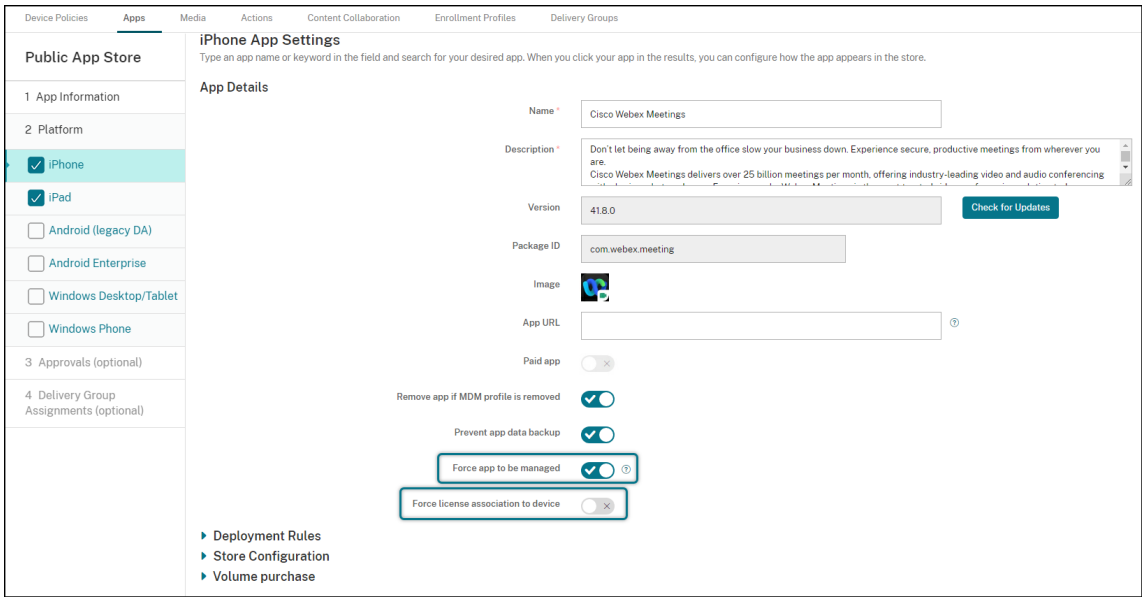
配置批量购买的应用程序

添加批量购买帐户后，应用程序信息将同步到 Endpoint Management，并且将显示在配置 > 应用程序页面上。您现在可以配置这些应用程序，优化交付组以及调整 iOS 和 macOS 设备的设备策略设置。完成该配置后，用户可以注册其设备。

配置批量购买的应用程序时，请注意以下设置：

- 在配置 > 应用程序页面上：
  - 要允许 Endpoint Management 将应用程序部署到设备而非部署给用户，请打开强制与设备建立许可证关联。此设置设为“开”时，用户无需使用其 Apple ID，也无需登录其 App Store 帐户即可下载这些应用程序。
  - 我们建议您为应用程序打开强制管理应用程序，以便该应用程序作为托管应用程序自动安装。

> 注意：
>
> 为使强制管理应用程序设置生效，必须在设置 > 服务器属性页面上将 `apple.app.force.managed` 服务器属性配置为 **True**。有关详细信息，请参阅服务器属性



- 在配置 > 交付组页面上：

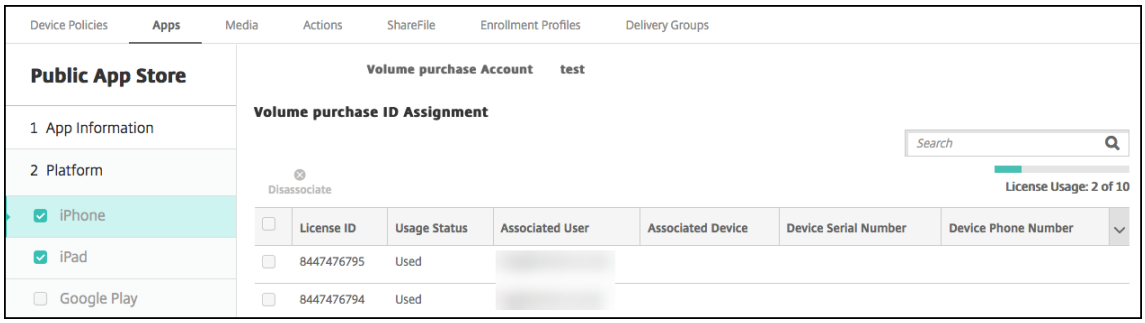
  要在用户设备上无提示安装应用程序，并且用户交互最少，请转至应用程序页面，然后将该应用程序拖动到必需应用程序列表。默认情况下，除 Secure Hub 以外的应用程序为可选应用程序，这意味着用户必须通过 Secure Hub 手动启动应用程序安装。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

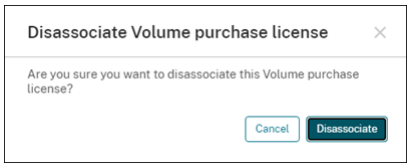
跟踪和管理应用程序许可证的使用

您可以跟踪应用程序的许可证使用情况。如果需要，可以收回已使用的许可证，使其可供其他用户或设备使用。

1. 单击配置 **>** 应用程序。
2. 选择一个应用程序，然后单击编辑。
3. 转至平台页面，然后展开批量购买。
   在批量购买 **ID** 分配表中，可以跟踪使用的许可证数量以及使用这些许可证的用户或设备。



4. 要收回许可证，请选择该许可证，然后单击取消关联。



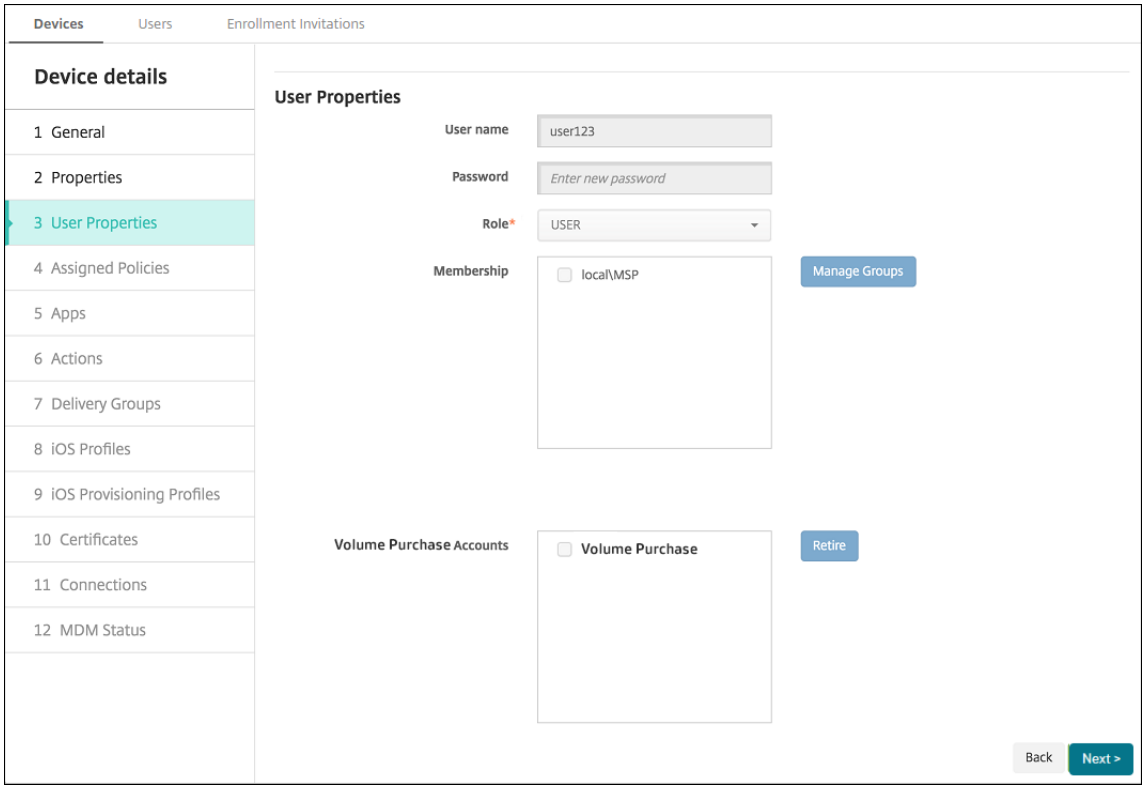
5. 单击取消关联以确认该操作。

停用批量购买帐户中的用户

如果将应用程序许可证关联到用户，则可以停用批量购买帐户中的用户以收回分配给这些用户的所有许可证。用例包括用户离开贵组织时。

1. 单击管理 **>** 设备。
2. 选择属于目标用户的设备，然后单击编辑。
3. 转至用户属性页面并根据需要选择批量购买帐户。
4. 单击停用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Endpoint Management 吊销用户的选定批量购买帐户中的应用程序许可证。

同步应用程序信息

Endpoint Management 定期将应用程序信息与 ABM 或 ASM 同步。如果需要，可以手动同步应用程序信息。同步可确保应用程序许可证和其他应用程序信息反映所有更改。此类更改包括您何时从批量购买帐户手动删除应用程序。

更改默认同步时间间隔

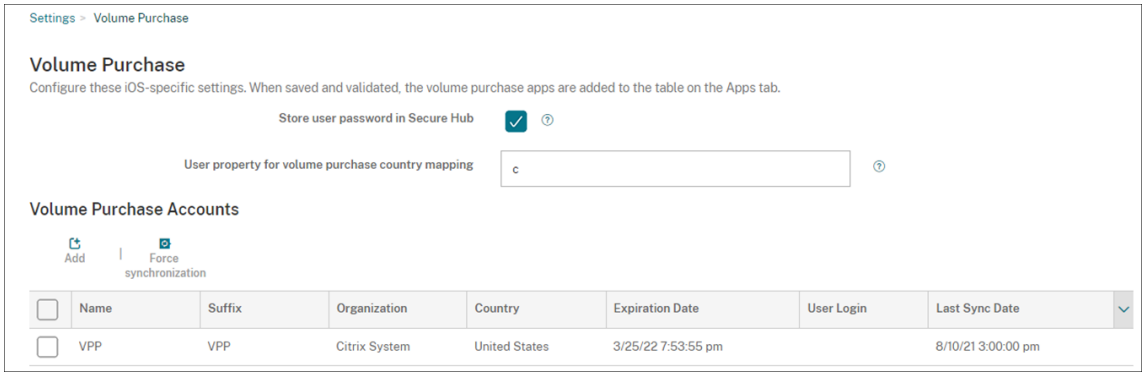
默认情况下，Endpoint Management 按每隔 1440 分钟（24 小时）的最小时间间隔为基准刷新批量购买许可证。Citrix Cloud 管理员可以通过服务器属性 `vpp.baseline` 更改默认时间间隔。有关详细信息，请参阅服务器属性。

手动同步应用程序信息

可以强制与 ABM 或 ASM 同步，以立即获取最新的应用程序信息。

1. 单击设置 **>** 批量购买
2. 选择一个批量购买帐户，然后单击强制同步。或者在不选择批量购买帐户的情况下单击强制同步以同步所有帐户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 确认同步操作。同步开始。

   同步可能需要几分钟时间才能完成，具体取决于批量购买许可证的数量。同步完成后，Endpoint Management 将刷新批量购买页面并在新的上次同步日期列中更新同步日期和时间。

检查应用程序更新

如果在添加批量购买帐户时打开了应用程序自动更新设置，Endpoint Management 将定期检查批量购买应用程序和可选应用程序的新版本并进行更新。如果需要，可以手动检查任何应用程序的新版本以及将应用程序更新应用到 Endpoint Management。

Endpoint Management 收到所需应用程序的新版本后，会向设备推送新版本以执行无提示安装，而不提示用户。

检查并应用应用程序的新版本

1. 单击配置 **>** 应用程序。此时将显示应用程序页面。
2. 选择一个应用程序，然后单击编辑。
3. 转至平台页面，然后单击版本旁边的检查更新。
4. 转至平台页面，然后单击版本旁边的检查更新。
5. 在出现的更新对话框中，如果新版本可用，请应用更新。

续订批量购买帐户的内容令牌

内容令牌每年过期一次。当令牌即将过期时，Endpoint Management 将显示许可证过期警告。请及时续订内容令牌以防止您的用户中断。

1. 在 ABM 或 ASM 门户中，下载更新的令牌。
2. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
3. 单击批量购买。此时将显示批量购买配置页面。
4. 使用更新后的令牌信息编辑批量购买帐户。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

将 Citrix Content Collaboration 与 Endpoint Management 结合使用

April 11, 2023

Citrix Content Collaboration 与 Endpoint Management 的集成取决于站点是否启用了 Workspace。

- 将 Citrix Workspace 和 Citrix Workspace 应用程序与 Citrix Content Collaboration 结合使用时，可以从 Citrix Workspace 部署 Content Collaboration。用户从 Citrix Workspace 访问 Citrix Files。有关信息，请参阅 部署 和 创建或将 Content Collaboration (ShareFile) 帐户链接到 Citrix Cloud。
- 如果 Endpoint Management 未启用 Workspace，Endpoint Management 将有两个用于与 Citrix Content Collaboration 集成的选项：Citrix Files 和存储区域连接器。

Citrix Files

可以将 Endpoint Management 配置为提供对 Content Collaboration 帐户的访问权限。该配置：

- 为移动用户提供对完整 Content Collaboration 功能集（例如，文件共享、文件同步和存储区域连接器）的访问权限。
- 可以为 Citrix Files 提供移动生产力应用程序用户的单点登录身份验证以及全面的访问控制策略。
- 通过 Endpoint Management 控制台提供 Content Collaboration 配置、服务级别监视和许可证使用情况监视。

有关为企业帐户配置 Endpoint Management 的更多信息，请参阅使用 Citrix Files 进行单点登录的 SAML。

存储区域连接器

可以将 Endpoint Management 配置为仅提供对通过 Endpoint Management 控制台创建的存储区域连接器的访问权限。该配置：

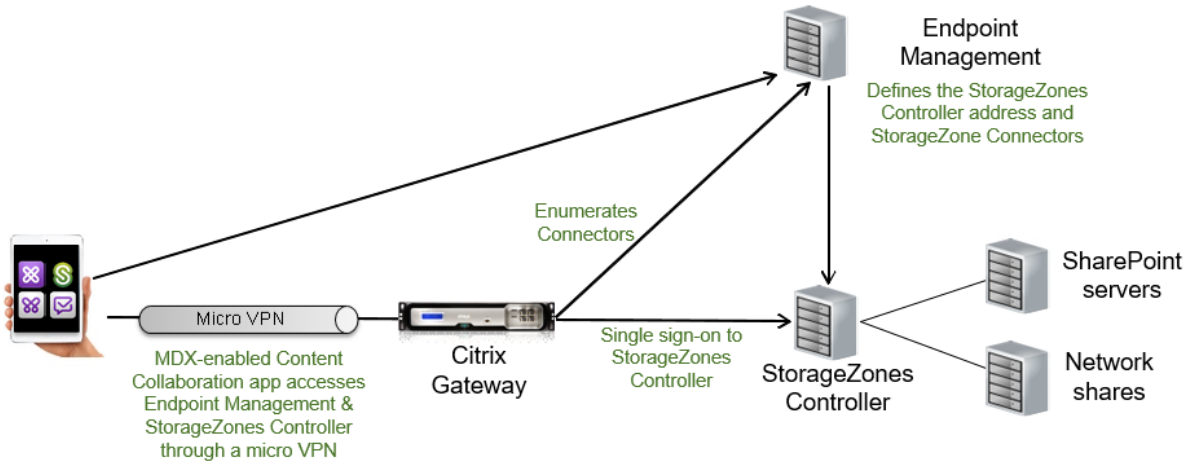
- 提供对现有本地存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问。
- 不需要您设置 Citrix Content Collaboration 子域或托管 Citrix Files 数据。
- 为用户提供通过适用于 Citrix Files for iOS 和 Citrix Files for Android 的 Citrix 移动生产力应用程序对数据进行移动访问的权限。用户可以编辑 Microsoft Office 文档。用户还可以从移动设备预览和批注 Adobe PDF 文件。
- 遵守防止在企业网络外部泄漏用户信息的安全限制。
- 可以通过 Endpoint Management 控制台对存储区域连接器进行简单设置。如果您以后决定在 Endpoint Management 中使用完整的 Citrix Files 功能，可以在 Endpoint Management 控制台中更改配置。

仅限 Endpoint Management 与存储区域连接器的集成：

- Citrix Content Collaboration 将单点登录配置用于 Citrix Gateway 以向存储区域控制器进行身份验证。
- 由于不使用 Citrix Files 控制平面，因此 Endpoint Management 不通过 SAML 进行身份验证。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

下图显示了 Endpoint Management 与存储区域连接器结合使用的高级体系结构。



要求

- 最低组件版本：
  - ShareFile for iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - 存储区域控制器 5.11.20

    本文包含有关如何配置存储区域控制器 5.0 的说明
- 请确保要运行存储区域控制器的服务器满足系统要求。有关要求，请参阅 系统要求。

Citrix Files 数据的存储区域和受限存储区域的要求不适用于 Endpoint Management 仅与存储区域连接器的集成。

Endpoint Management 不支持 Documentum 连接器。

- 运行 PowerShell 脚本：
  - 在 32 位 (x86) 版本的 PowerShell 中运行脚本。

安装任务

按显示顺序完成以下任务以安装和设置存储区域控制器。这些步骤专门用于 Endpoint Management 仅与存储区域连接器的集成。存储区域控制器文档中包含其中一些文章。

1. 为存储区域控制器配置 NetScaler

   可以将 Citrix Gateway 用作存储区域控制器的 DMZ 代理。

2. 安装 SSL 证书

   托管标准区域的存储区域控制器需要 SSL 证书。托管受限区域的存储区域控制器使用内部地址，不需要 SSL 证书。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

3. 准备您的服务器

   需要为存储区域连接器完成 IIS 和 ASP.NET 设置。

4. 安装存储区域控制器
5. 准备存储区域控制器以仅与存储区域连接器结合使用
6. 指定存储区域的代理服务器

   存储区域控制器控制台允许您为存储区域控制器指定代理服务器。还可以使用其他方法指定代理服务器。

7. 配置域控制器以信任存储区域控制器进行委派

   配置域控制器以在网络共享或 SharePoint 站点上支持 NTLM 或 Kerberos 身份验证。

8. 将辅助存储区域控制器加入存储区域

   要配置存储区域以实现高可用性，请至少将两个存储区域控制器连接到该存储区域。

安装存储区域控制器

1. 下载并安装存储区域控制器软件：

   a) 在 Citrix Files 下载页面 https://www.citrix.com/downloads/sharefile.html 上，登录并下载最新的存储区域控制器安装程序。

   b) 安装存储区域控制器会将服务器上的默认 Web 站点更改为控制器的安装路径。在默认 Web 站点上启用匿名身份验证。

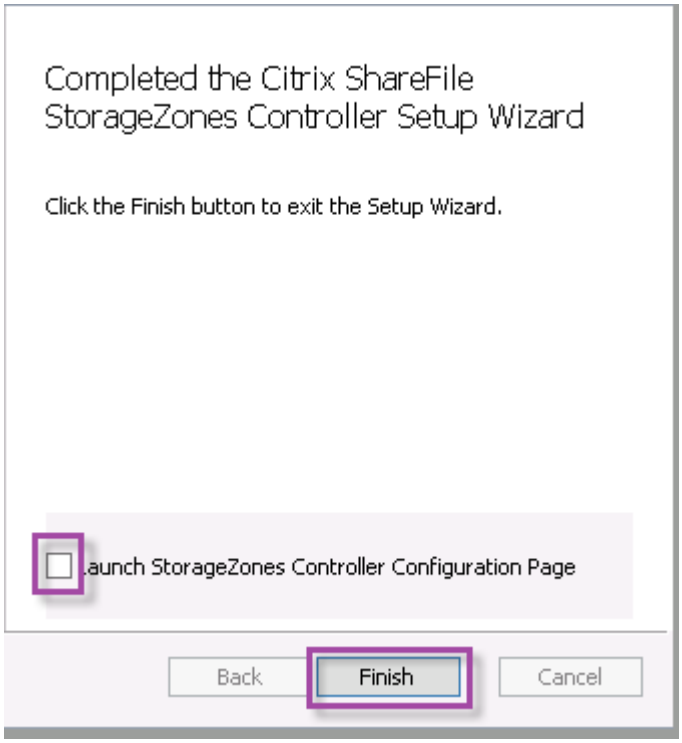
2. 在要安装存储区域控制器的服务器上，运行 StorageCenter.msi。

   存储区域控制器设置向导将会启动。

3. 回复提示：

   - 在目标文件夹页面上，如果 Internet Information Services (IIS) 安装在默认位置中，则保留默认值。如果不是，请浏览到 IIS 安装位置。
   - 安装完成后，取消选中 **Launch StorageZones Controller Configuration Page**（启动存储区域控制器配置页面）复选框，然后单击 **Finish**（完成）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 出现提示时，重新启动存储区域控制器。
5. 要测试安装是否成功，请导航到 `https://localhost/`。（如果出现证书错误，请考虑改为使用 HTTP 进行连接。）如果安装成功，则将显示 Citrix Files 徽标。

   如果没有显示 Citrix Files 徽标，请清除浏览器缓存，然后重试。

   > 重要：
   >
   > 如果您打算克隆存储区域控制器，请先捕获磁盘映像，然后再继续配置存储区域控制器。

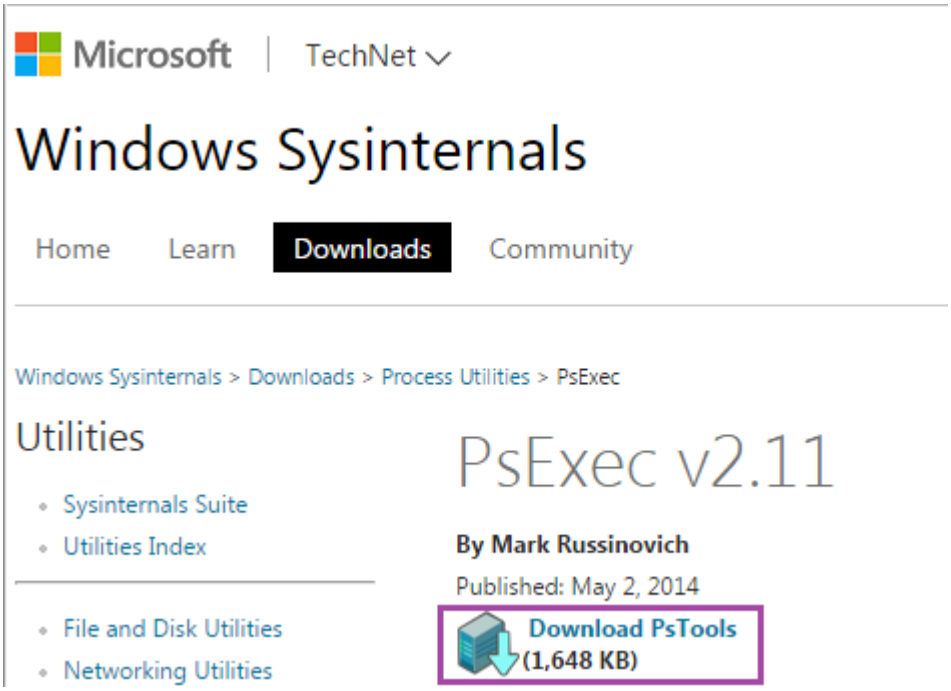
准备存储区域控制器以仅与存储区域连接器结合使用

对于仅与存储区域连接器的集成，不要使用存储区域控制器管理控制台。该接口需要 Citrix Files 管理员帐户，这对此解决方案没有必要。因此，请运行 PowerShell 脚本以在不使用 Citrix Files 控制平面的情况下准备要使用的存储区域控制器。该脚本执行以下操作：

- 将当前存储区域控制器注册为主存储区域控制器。以后可以将辅助存储区域控制器加入主控制器。
- 创建区域并为其设置密码。

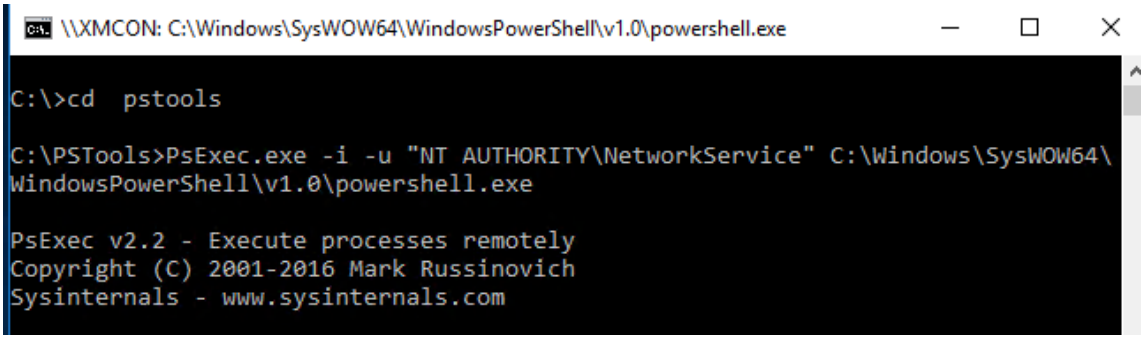
1. 从存储区域控制器服务器下载 p SexEC 工具：导航到 Microsoft Windows 系统内部，然后单击 下载 **PStools**。将工具提取到 C 驱动器的根目录。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



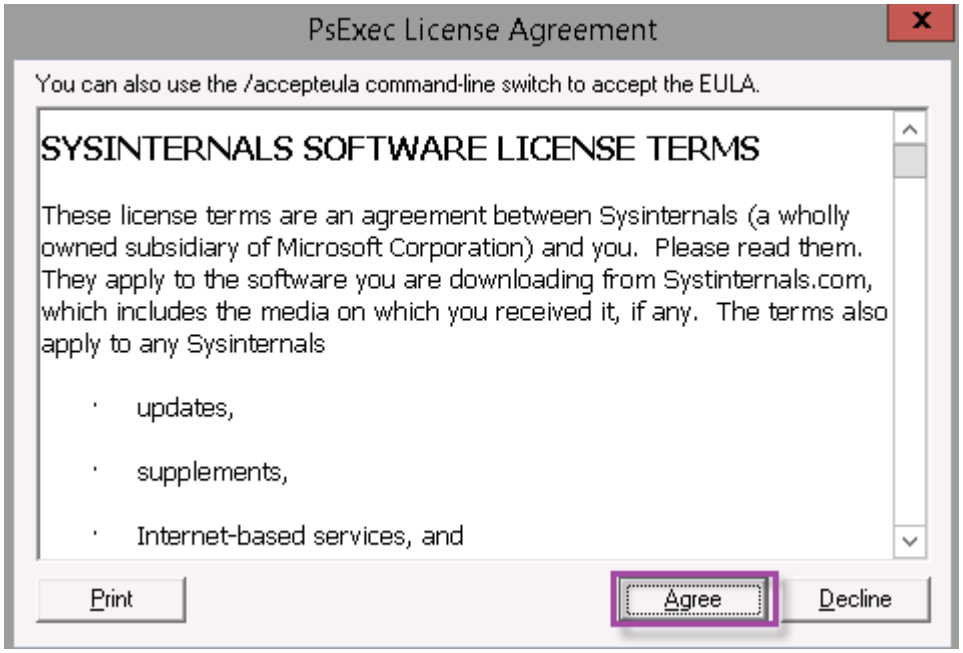
2. 运行 PsExec 工具：以管理员用户身份打开命令提示窗口，然后键入以下命令：

```
```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy--> ```
```




3. 出现提示时，单击 **Agree**（同意）以运行 Sysinternals 工具。

© 1999–2023 Cloud Software Group, Inc. All rights reserved. 
```



此时打开 PowerShell 窗口。

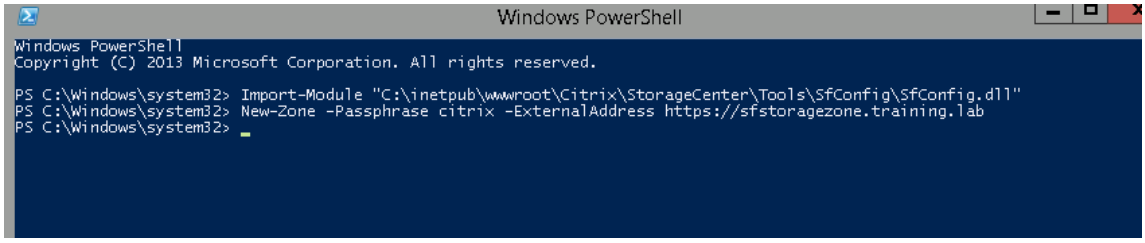
4. 在 PowerShell 窗口中，键入以下命令：

```
```
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
<!--NeedCopy--> ```
```

其中：

**Passphrase**（密码）：您要分配给站点的密码。请将其记录下来。无法从控制器恢复密码。如果丢失了密码，则无法重新安装存储区域、将更多存储区域控制器加入到存储区域，或者在服务器出现故障时恢复存储区域。

**ExternalAddress**（外部地址）：存储区域控制器服务器的外部完全限定的域名。




您的主存储区域控制器现已就绪。

在登录到 Endpoint Management 以创建存储区域连接器之前：完成以下配置（如果适用）：

指定存储区域的代理服务器

© 1999–2023 Cloud Software Group, Inc. All rights reserved. 
```

配置域控制器以信任存储区域控制器进行委派

将辅助存储区域控制器加入存储区域

要创建存储区域连接器，请参阅Endpoint Management 中的定义存储区域控制器连接。

将辅助存储区域控制器加入存储区域

要配置存储区域以实现高可用性，请至少将两个存储区域控制器连接到该存储区域。要将辅助存储区域控制器加入区域，请在另一台服务器上安装存储区域控制器。然后将该控制器加入主控制器的区域。

1. 在您要将其加入主服务器的存储区域控制器服务器上打开 PowerShell 窗口。
2. 在 PowerShell 窗口中，键入以下命令：

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

   例如：

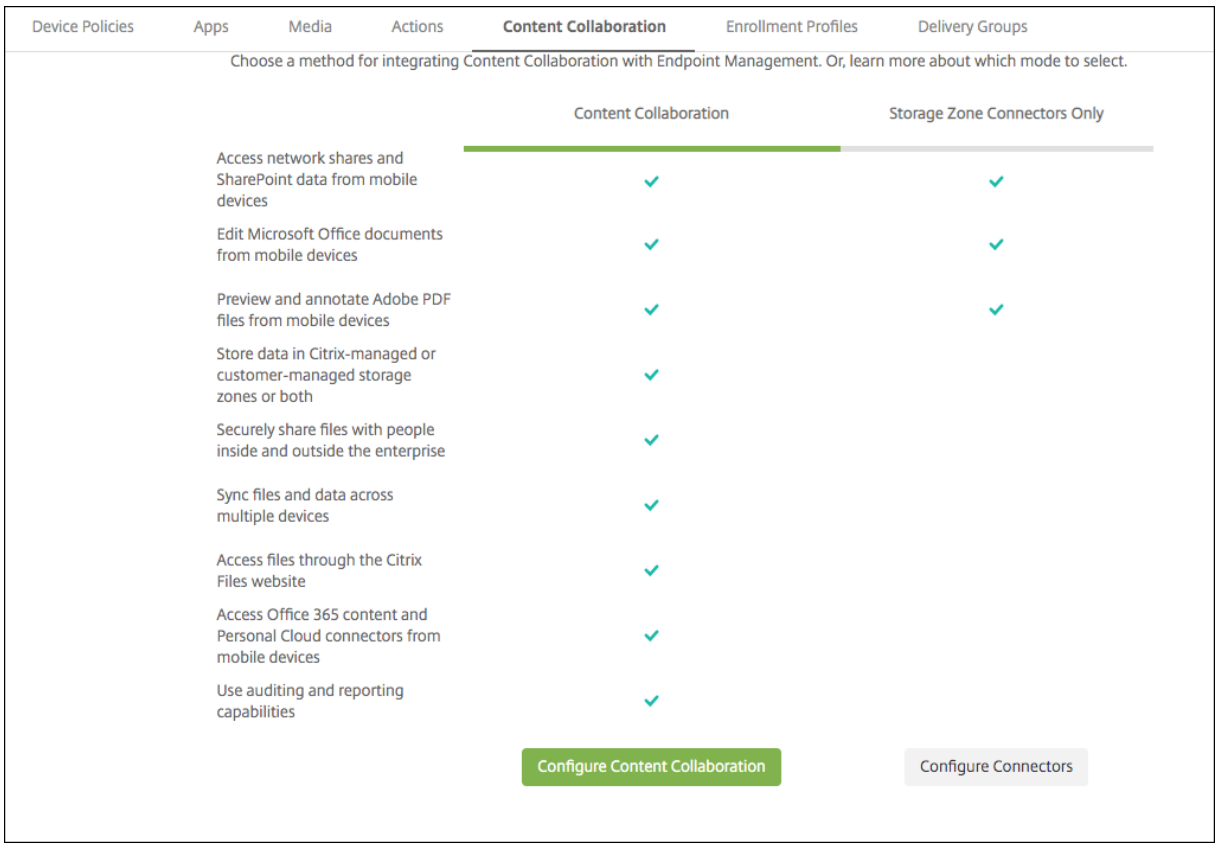
   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

在 **Endpoint Management** 中定义存储区域控制器连接

在添加存储区域连接器之前，可以为针对存储区域连接器启用的每个存储区域控制器配置连接信息。可以按本节所述定义存储区域控制器，也可以在添加连接器时定义存储区域控制器。

在您第一次访问配置 **> Content Collaboration** 页面时，页面上会总结适用于 Enterprise 帐户的 Endpoint Management 与存储区域连接器结合使用之间差异。

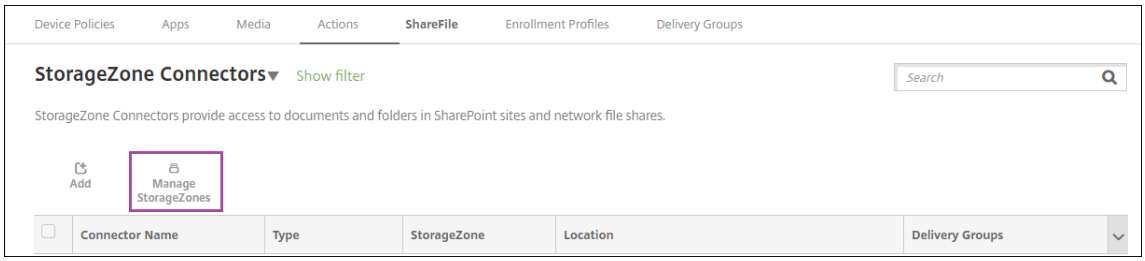
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



单击配置连接器继续执行本文中的配置步骤。

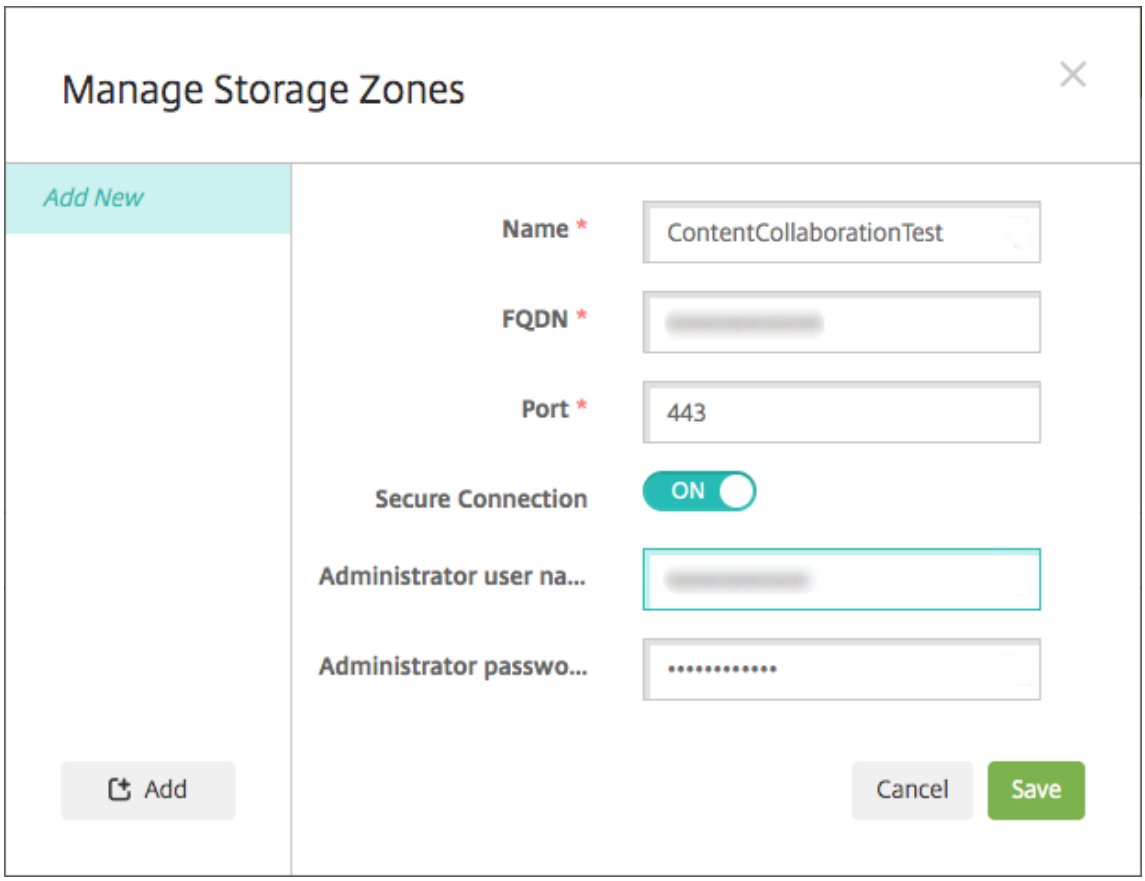


1. 在配置 **> Content Collaboration** 中，单击管理存储区域。



2. 在管理存储区域中，添加连接信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



- 名称：存储区域的描述性名称，用于在 Endpoint Management 中标识存储区域。请勿在名称中包含空格或特殊字符。
- **FQDN** 和端口：可从 Endpoint Management 服务器访问的存储区域控制器的完全限定域名和端口号。
- 安全连接：如果对与存储区域控制器的连接使用 SSL，则使用默认设置“开”。如果不对连接使用 SSL，则将此设置更改为“关”。
- 管理员用户名和管理员密码：管理员服务帐户用户名称（采用 domain\admin 形式）和密码。或者，对存储区域控制器具有读写权限的用户帐户。

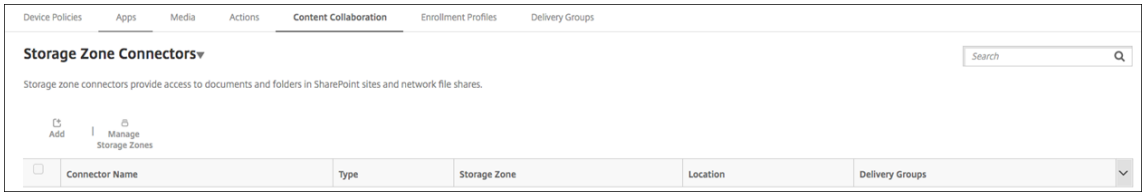
3. 单击保存。
4. 要测试连接，请验证 Endpoint Management 服务器是否可以访问端口 443 上的存储区域控制器的完全限定的域名。
5. 要定义另一个存储区域控制器连接，请在管理存储区域中单击添加按钮。

   要编辑或删除存储区域控制器连接的信息，请在管理存储区域中选择连接名称。然后单击编辑或删除。

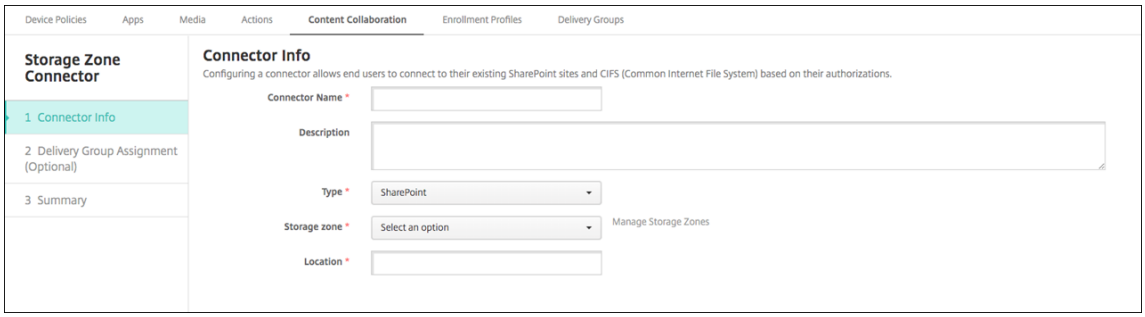
在 **Endpoint Management** 中添加存储区域连接器

1. 转到配置 **> Content Collaboration**，然后单击添加。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

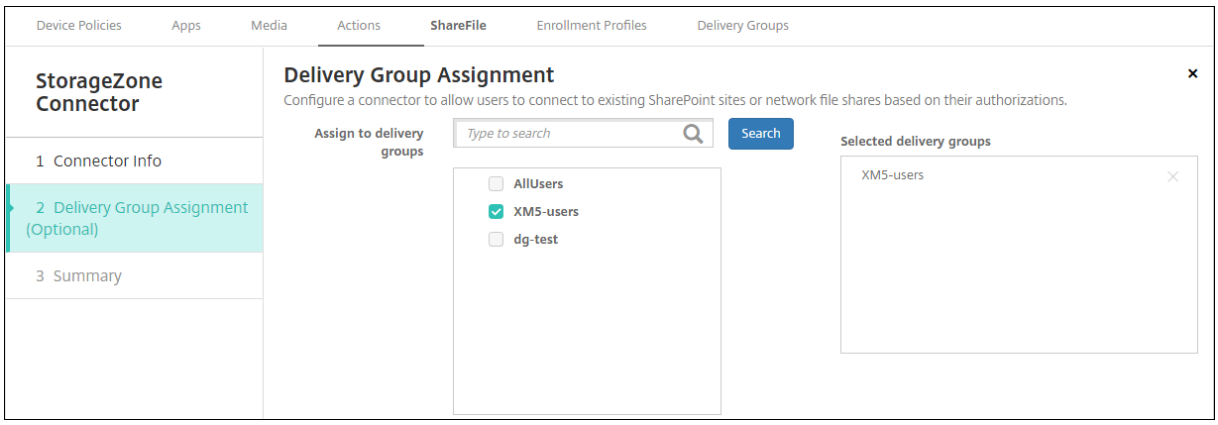


2. 在连接器信息页面上，配置以下设置：



- 连接器名称：在 Endpoint Management 中标识存储区域连接器的名称。
- 说明：有关此连接器的可选备注。
- 类型：选择 **SharePoint** 或网络。
- 存储区域：选择与连接器关联的存储区域。如果没有列出存储区域，请单击管理存储区域以定义存储区域控制器。
- 位置：对于 SharePoint，指定 SharePoint 根级别站点、站点集合或文档库的 URL（采用 `https://sharepoint.company.com` 形式）。对于网络共享，指定统一命名约定 (UNC) 路径的完全限定域名（采用 \\server\share 形式）。

3. 在交付组分配页面上，可以选择将连接器分配给交付组。或者，可以通过使用配置 **>** 交付组将连接器关联到交付组。



1. 在摘要页面上，可以查看配置的选项。要调整配置，请单击上一步。
2. 单击保存以保存连接器。
3. 测试连接器：
   a) 封装 Citrix Files 客户端时，请将网络访问策略设置为通道 **- Web SSO**。

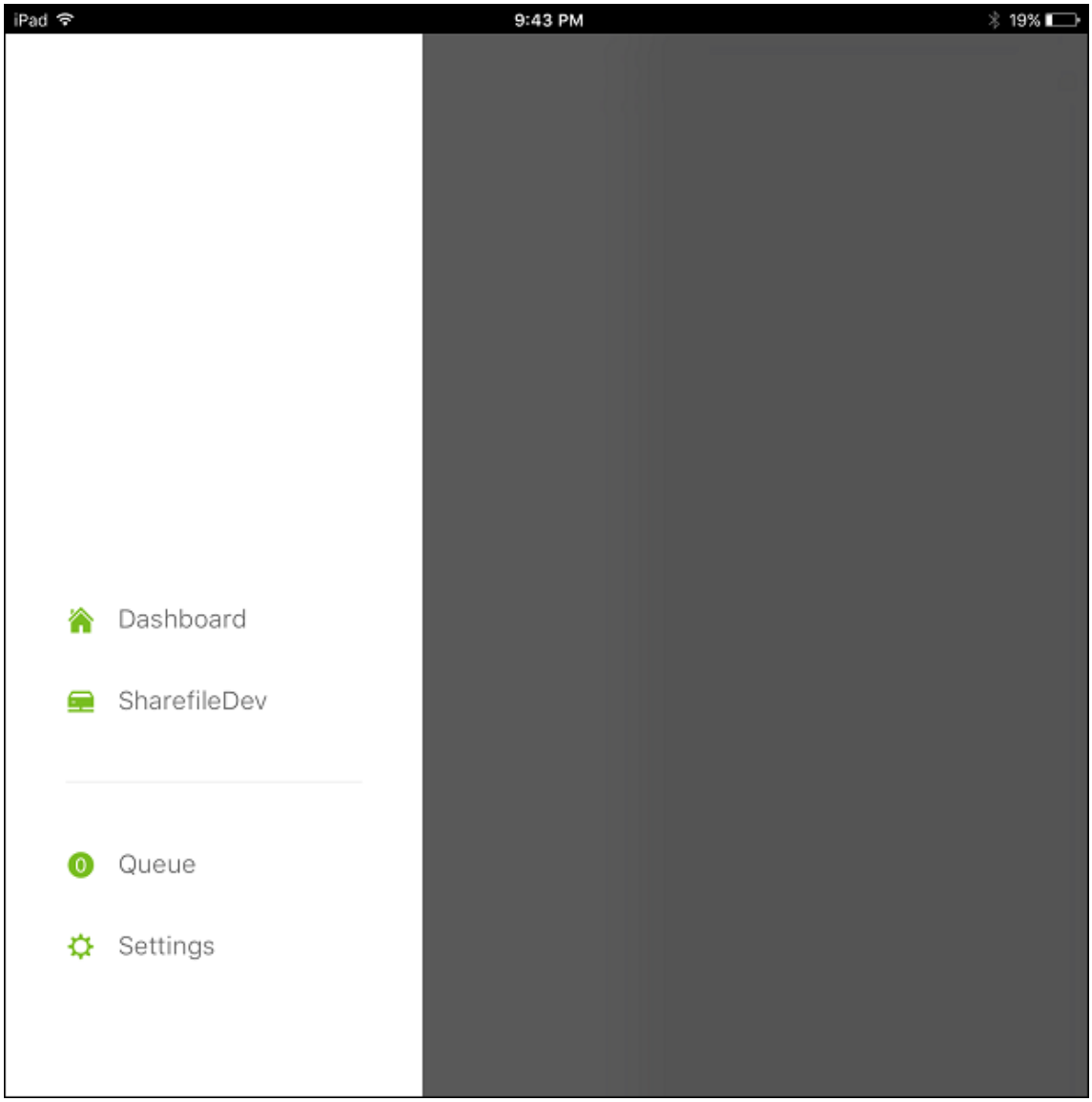
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在此通道模式下，MDX 框架会终止来自 MDX 应用程序的 SSL/HTTP 流量。MDX 随后代表用户启动与内部连接的新连接。此策略设置允许 MDX 框架检测和响应 Web 服务器发出的身份验证质询。

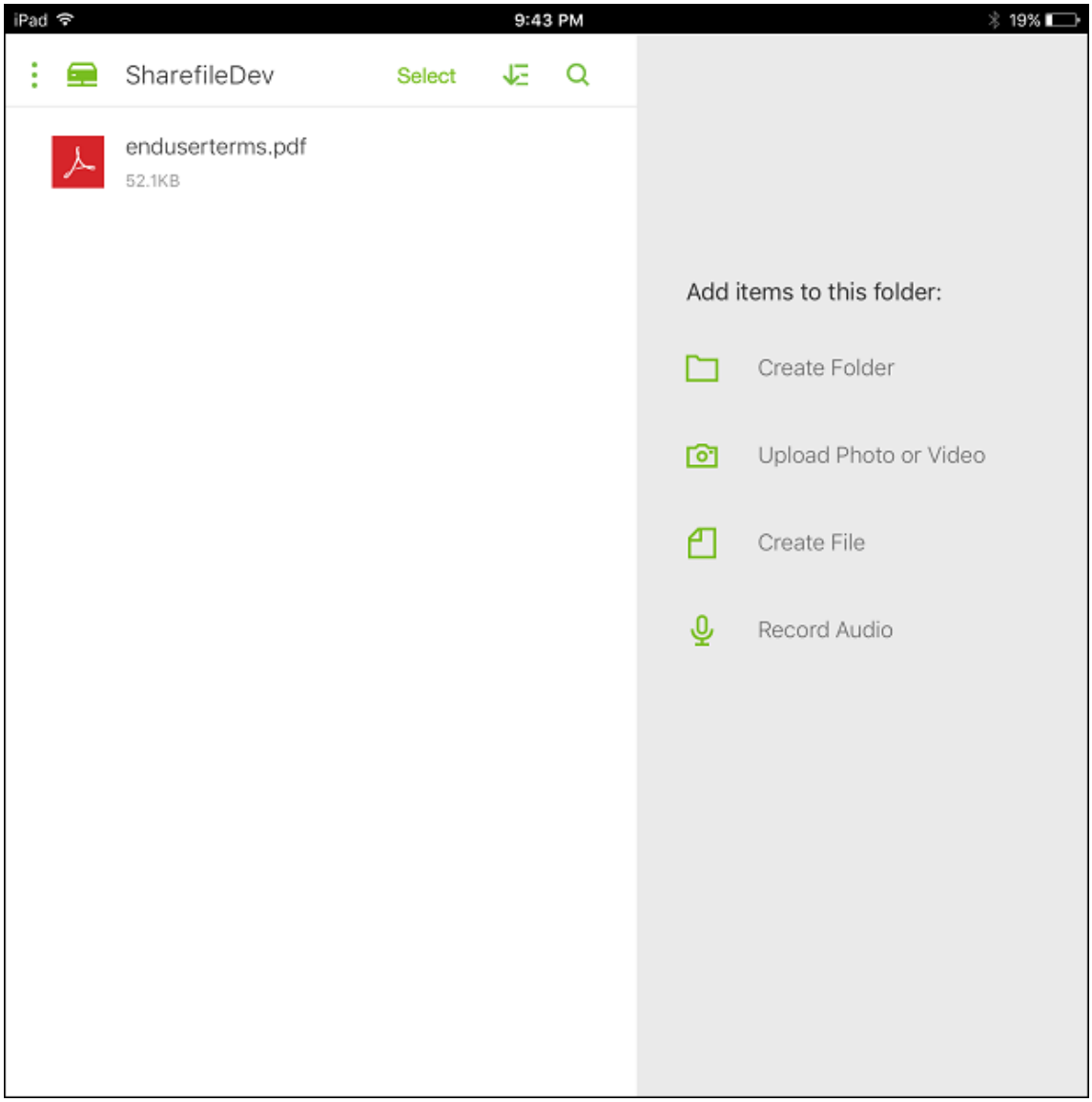
b) 将 Citrix Files 客户端添加到 Endpoint Management。有关详细信息，请参阅 将 Citrix Files 客户端添加到 Endpoint Management。

c) 在支持的设备上，验证到 Citrix Files 和连接器的单点登录。

在以下示例中，SharefileDev 是连接器的名称。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

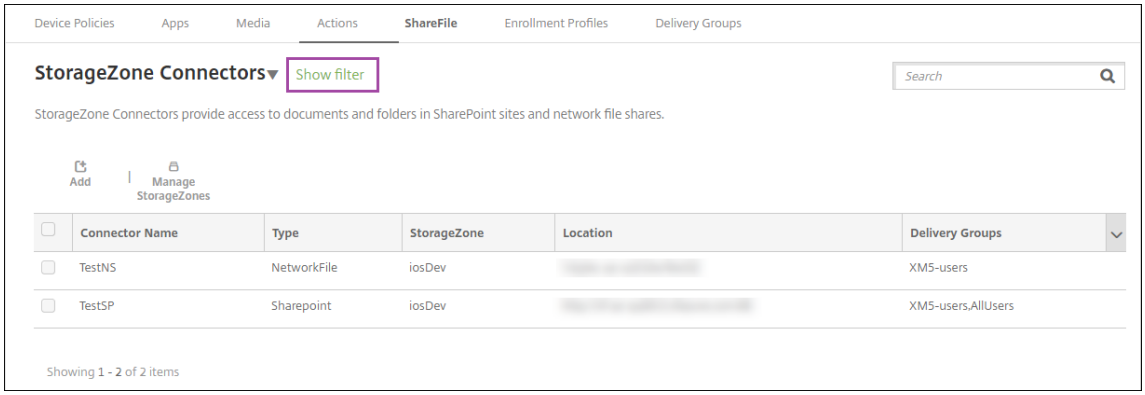


过滤存储区域连接器列表

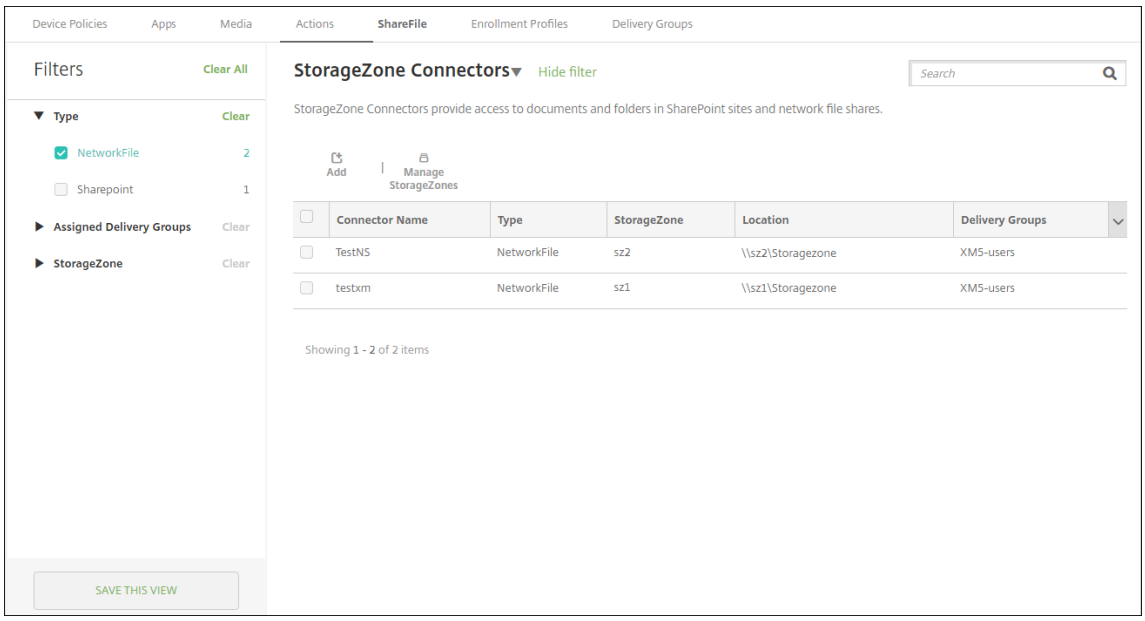
可以按连接器类型、分配的交付组和存储区域来过滤存储区域连接器列表。

1. 转到配置 **> Content Collaboration**，然后单击显示过滤器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

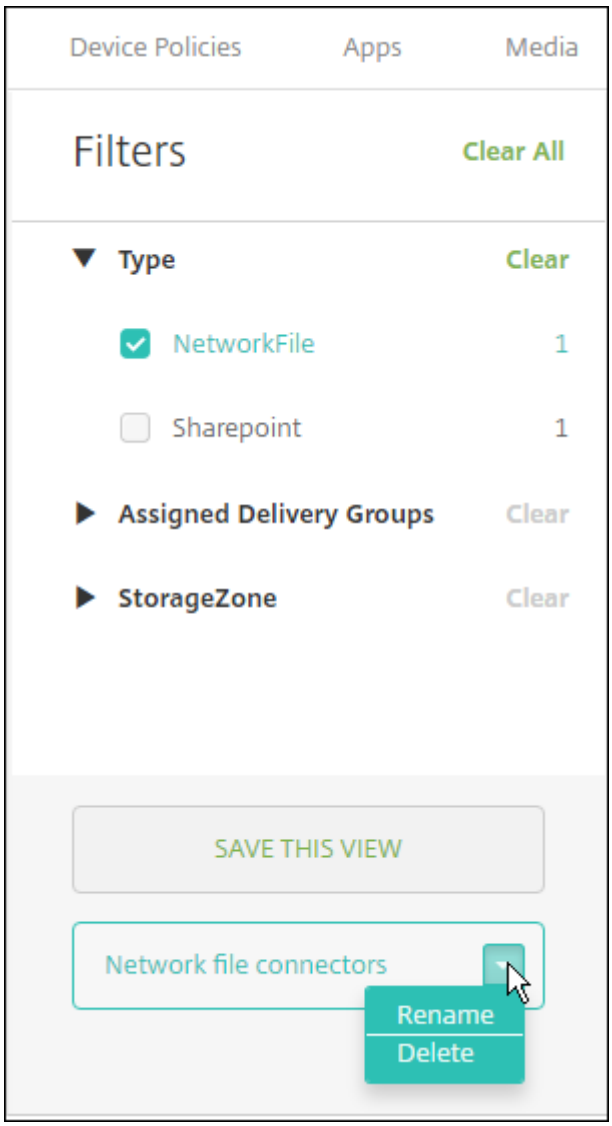


2. 展开要进行选择的过滤器标题。要保存过滤器，请单击保存此视图，键入过滤器名称，并单击保存。



3. 要重命名或删除过滤器，请单击过滤器名称旁边的箭头图标。

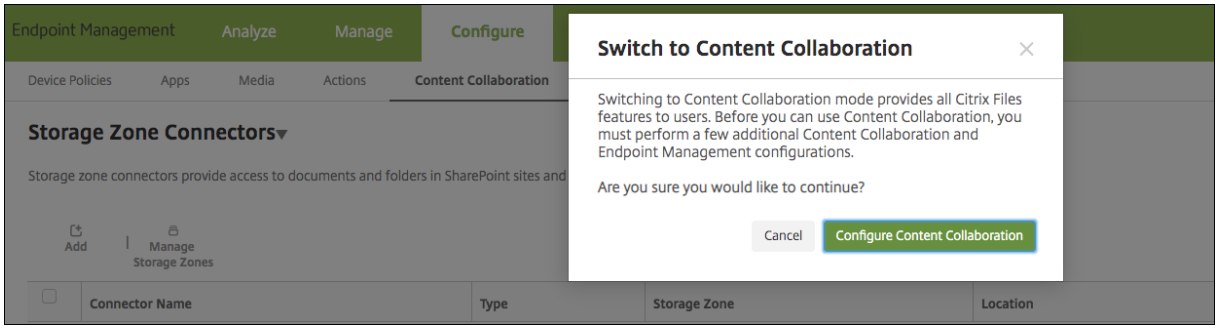
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



切换到 **Enterprise** 帐户

将存储区域连接器与 Endpoint Management 集成后，可以稍后切换到完整的 Enterprise 功能集。Endpoint Management 会保留现有的存储区域连接器集成设置。

转到配置 **> Content Collaboration**，单击存储区域连接器下拉菜单，然后单击配置 **Content Collaboration**。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

有关配置企业帐户的信息，请参阅使用 Citrix Files 进行单点登录的 SAML。

适用于 **HDX** 应用程序的 **SmartAccess**

June 9, 2022

此功能允许您根据设备属性、设备的用户属性或设备上已安装的应用程序控制对 HDX 应用程序的访问。您可以通过设置自动化操作使用此功能将设备标记为不合规，以拒绝该设备的访问。与此功能结合使用的 HDX 应用程序通过拒绝访问不合规设备的 SmartAccess 策略在 Citrix Virtual Apps and Desktops 中配置。Endpoint Management 使用签名的加密标记向 StoreFront 传达设备的状态。StoreFront 随后根据应用程序的访问控制策略允许或拒绝访问。

要使用此功能，您的部署要求：

- Citrix Virtual Apps and Desktops
- Citrix Endpoint Management
- Endpoint Management 配置有 SAML 证书，用于签名和加密标记。不带私钥的相同证书在 StoreFront 服务器上上载。

要开始使用此功能，请执行以下操作：

- 配置 Endpoint Management 服务器证书并将其上载到 StoreFront 应用商店
- 使用所需的 SmartAccess 策略配置至少一个 Citrix Virtual Apps and Desktops 交付组
- 在 Endpoint Management 中设置自动操作

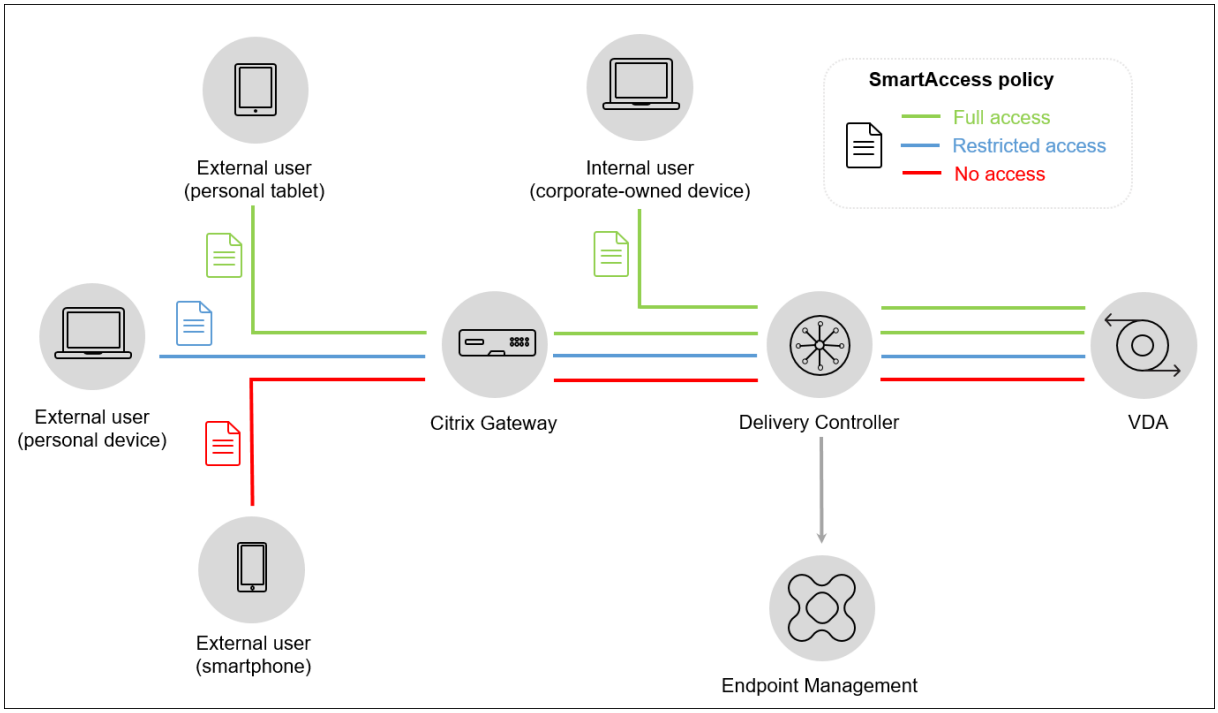
通过 **SmartAccess** 访问适用于端点的 **HDX** 应用程序

通过此功能，您可以应用基于策略的访问控制以限制设备对 HDX 应用程序的访问。可以将以下访问级别应用到 HDX 应用程序：

- 完全访问权限。设备可以访问 Secure Hub 应用商店提供的所有 HDX 应用程序。
- 受限制的访问。设备可以访问一个或多个 HDX 应用程序，但不能访问所有 HDX 应用程序。
- 没有访问权限。设备无法访问任何 HDX 应用程序。

下图说明了访问控制的工作原理。尝试在 Secure Hub 中启动 HDX 应用程序会触发到 Delivery Controller 的请求。然后，Delivery Controller 将请求转发到 Endpoint Management 服务器进行验证。验证的结果决定了设备的访问级别。例如，如果设备已越狱，则拒绝访问 HDX 应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



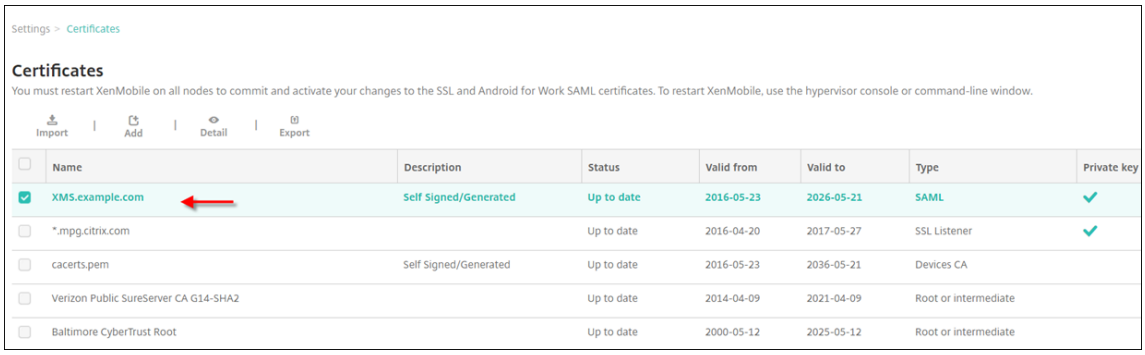
导出并配置 **Endpoint Management** 服务器证书并将其上载到 **StoreFront** 应用商店

SmartAccess 使用签名的加密标记在 Endpoint Management 与 StoreFront 服务器之间进行通信。要启用该通信，请将 Endpoint Management 服务器证书添加到 StoreFront 应用商店。

有关在通过基于域和证书的身份验证启用 Endpoint Management 时集成 StoreFront 和 Endpoint Management 的更多信息，请参阅 支持知识中心。

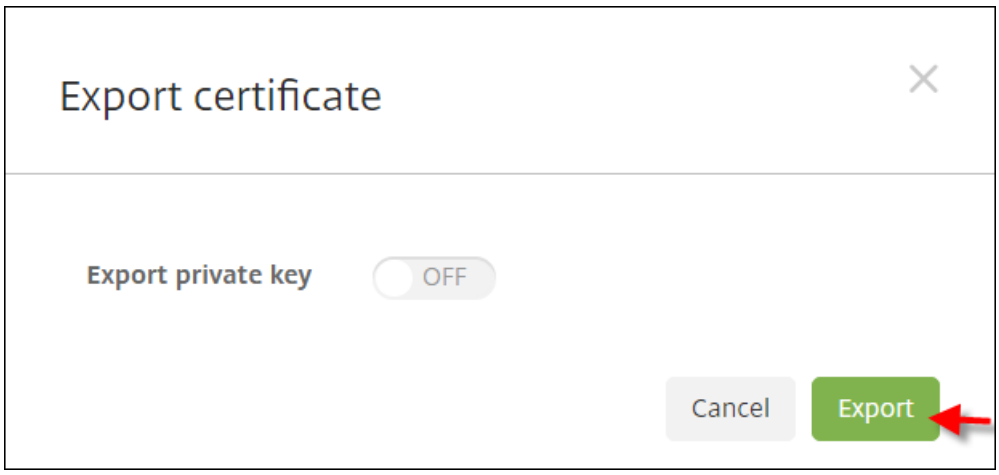
从 **Endpoint Management** 导出 **SAML** 证书

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。单击证书。
2. 找到 Endpoint Management 服务器的 SAML 证书。

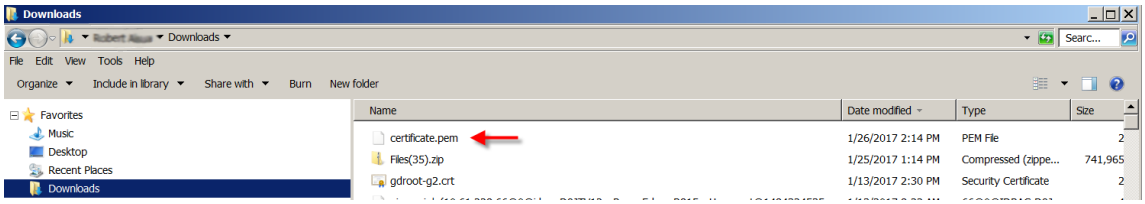


3. 确保导出私钥设置为关。单击导出将该证书导出到您的下载目录。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

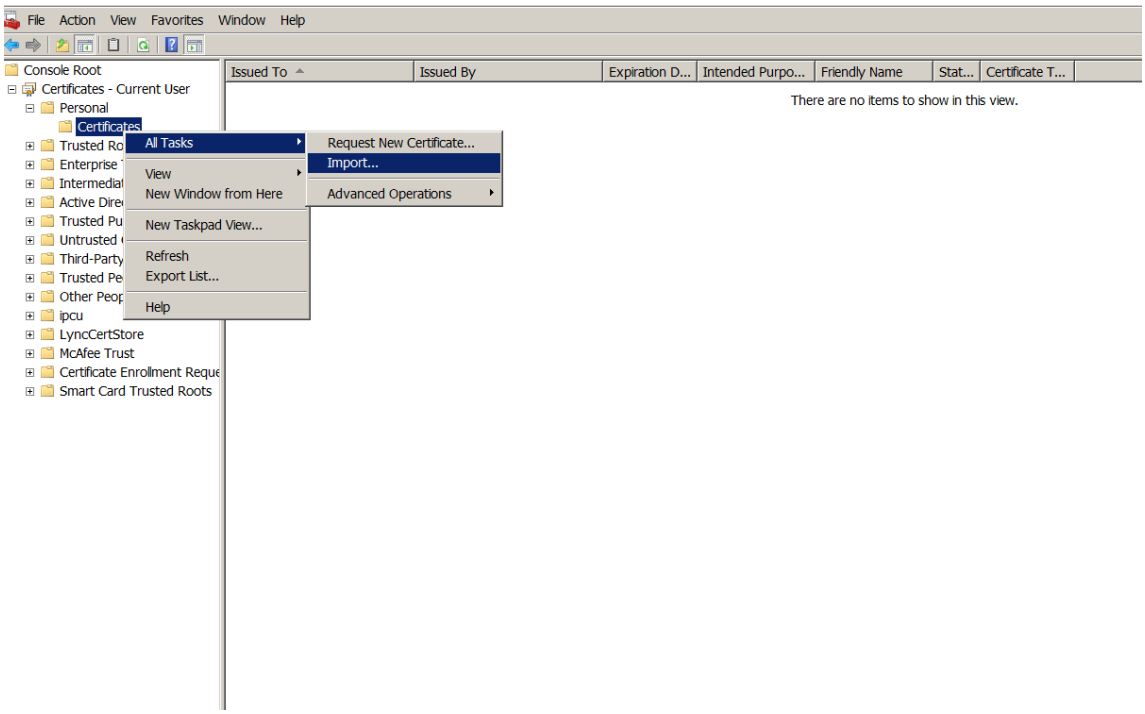


4. 在您的下载目录中找到该证书。证书为 PEM 格式。



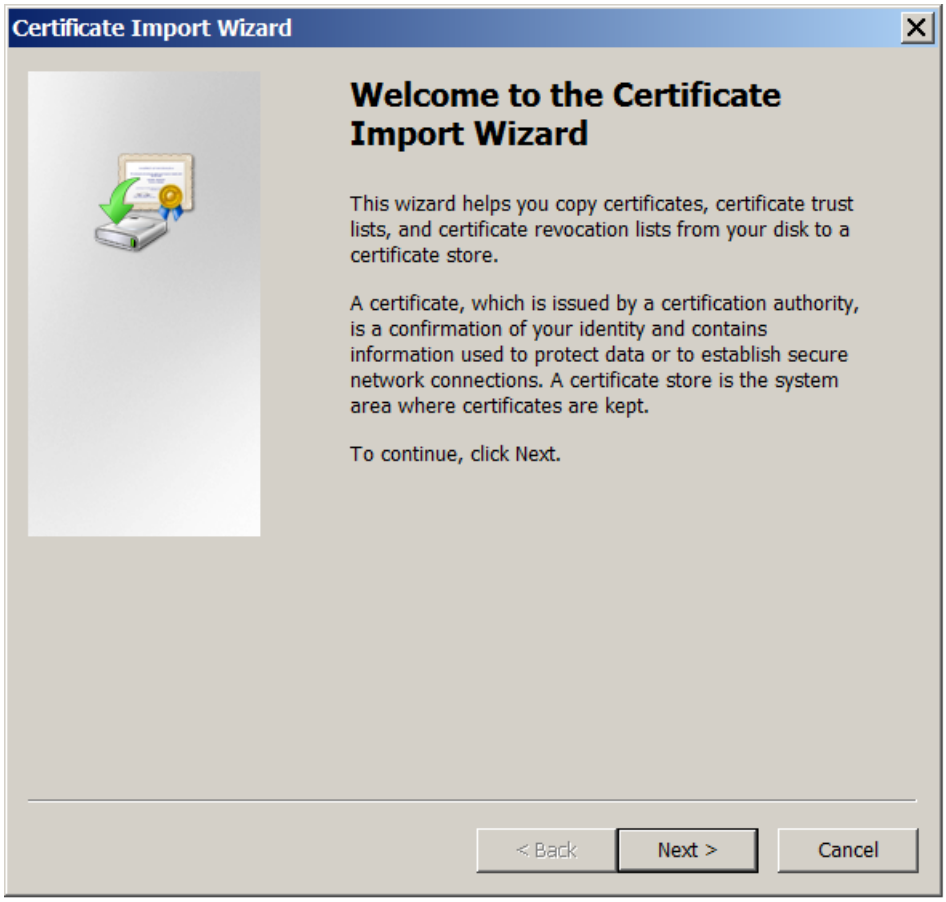
将证书从 **PEM** 转换为 **CER**

1. 打开 Microsoft 管理控制台 (MMC)，然后右键单击证书 **>** 所有任务 **>** 导入。

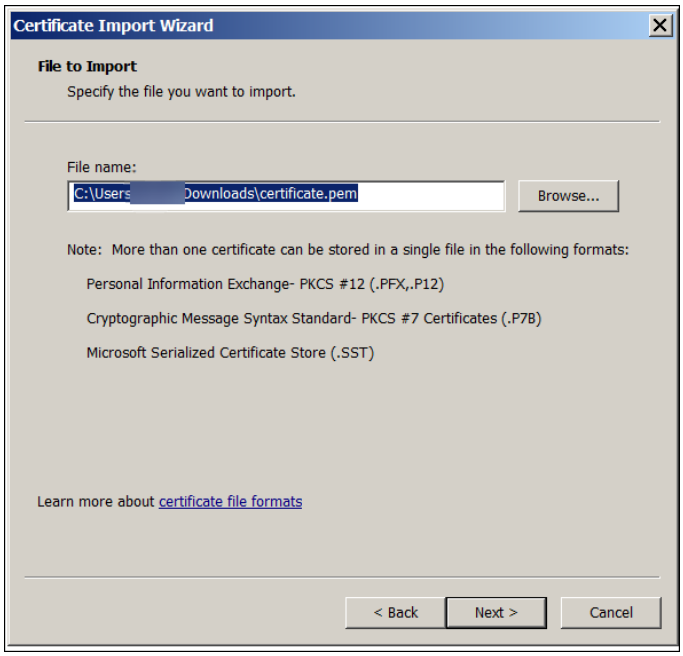


2. 证书导入向导显示时，单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

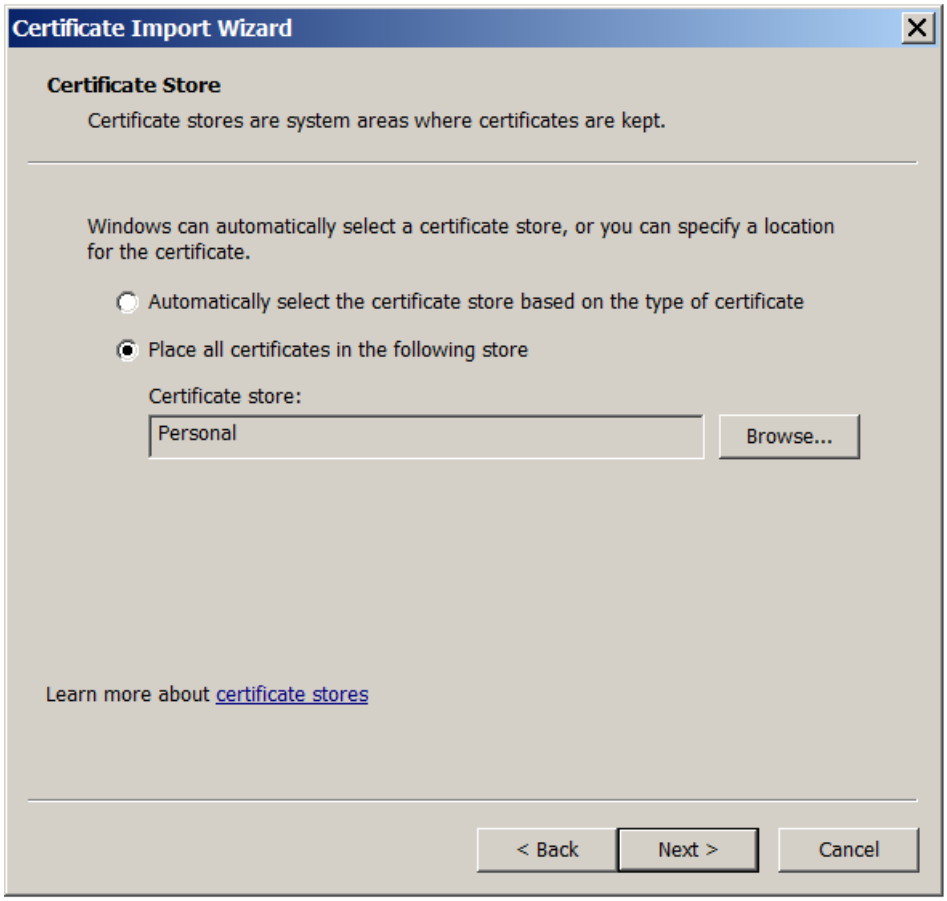


3. 浏览到下载目录中的证书。



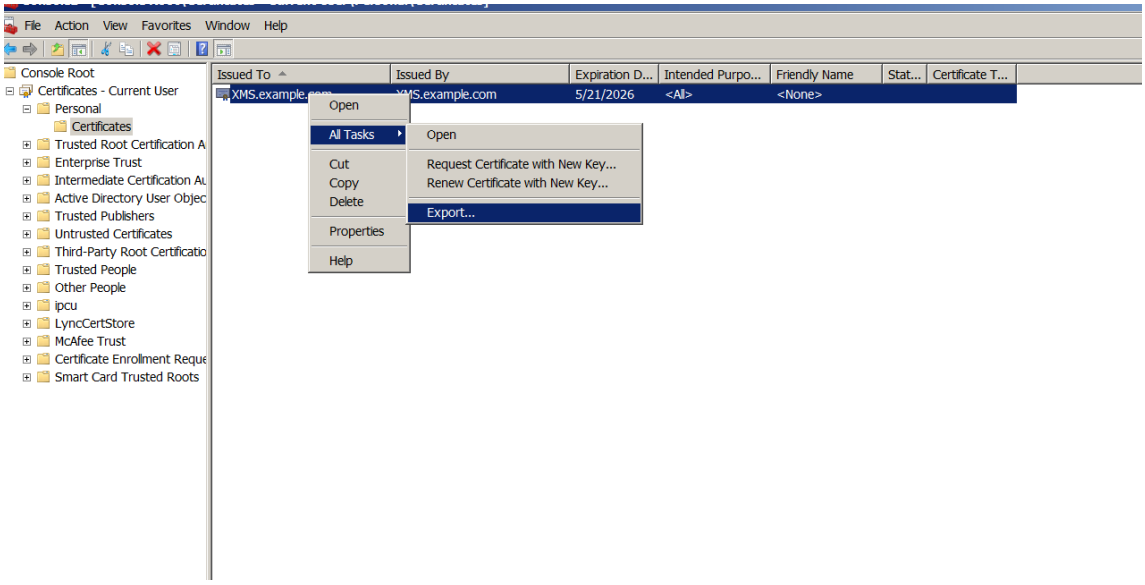
4. 选择将所有的证书都放入下列存储，然后选择个人作为证书存储。单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



5. 检查您的选择，然后单击完成。单击确定消除确认窗口。

6. 在 MMC 中，右键单击证书，然后选择所有任务 **>** 导出。



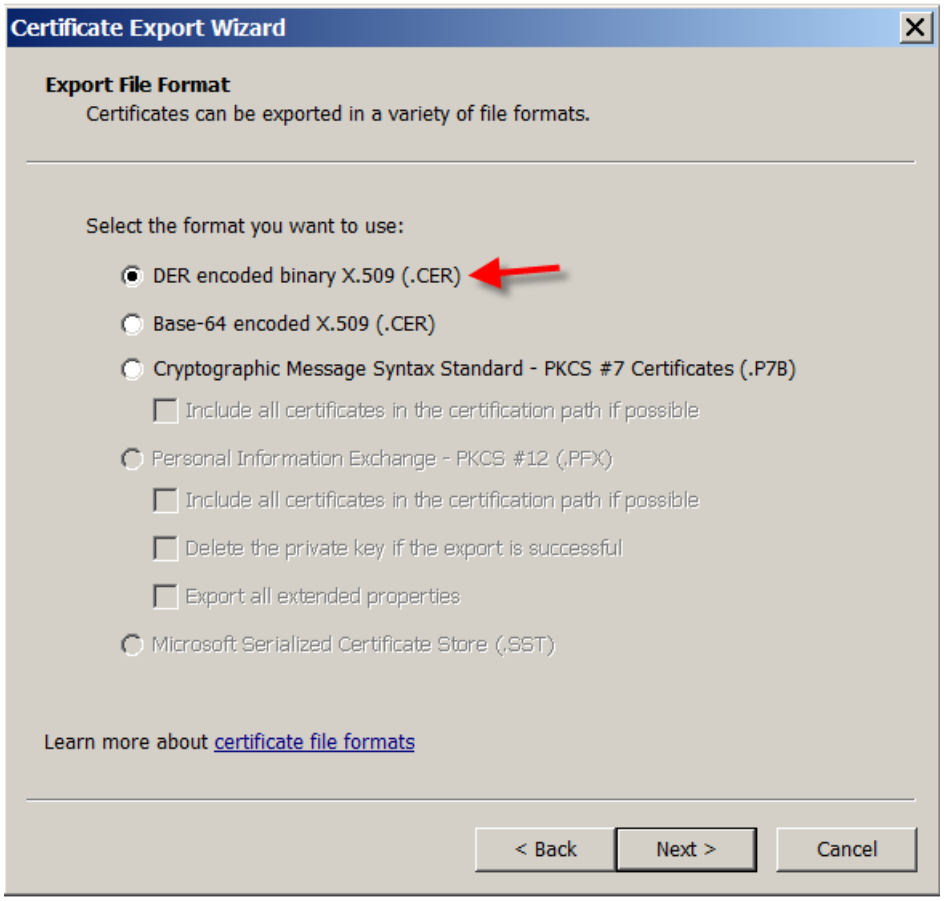
7. 证书导出向导显示时，单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



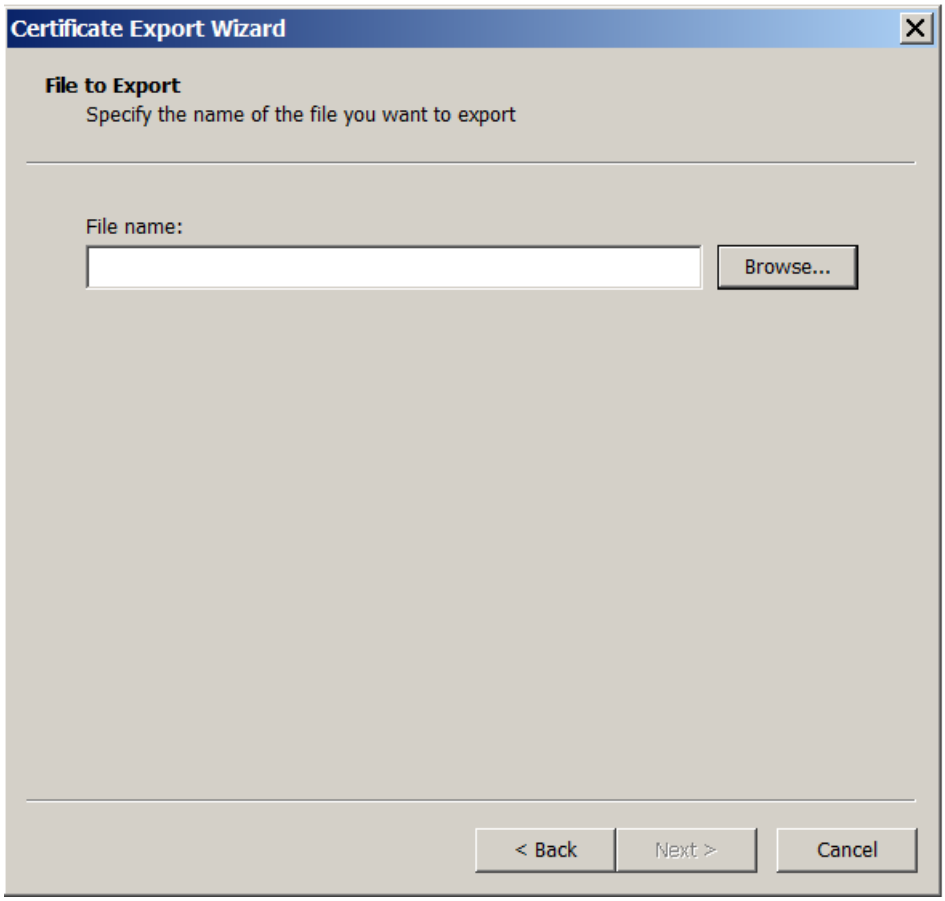
8. 选择格式 **DER** 编码二进制 **X.509 (.CER)**。单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

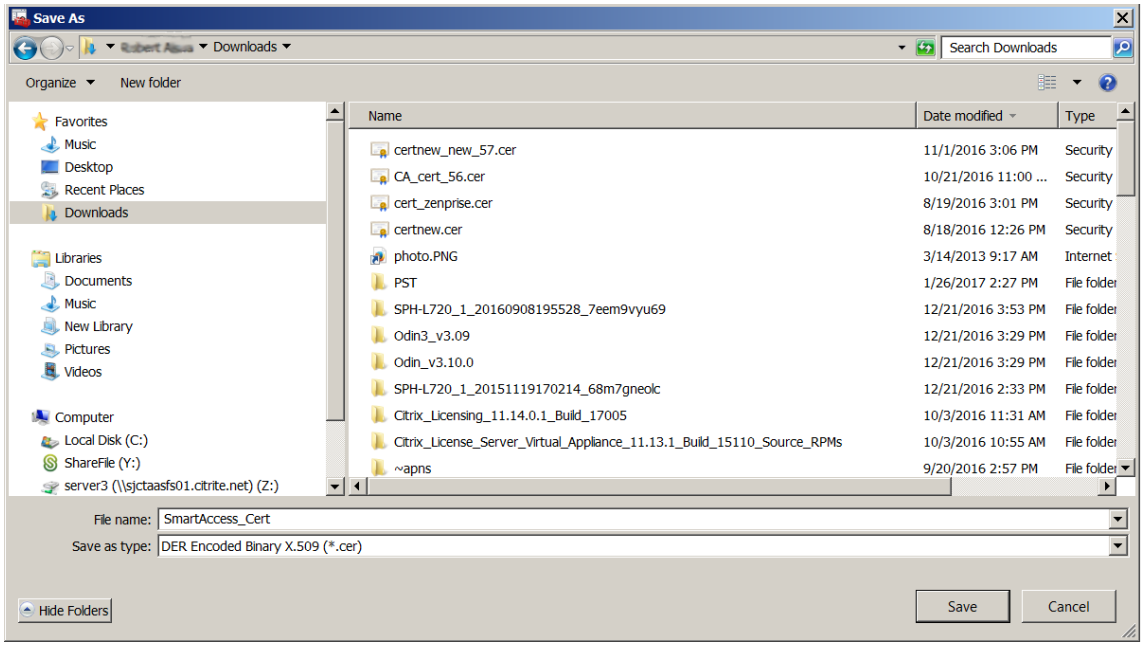


9. 浏览到该证书。键入证书名称，然后单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

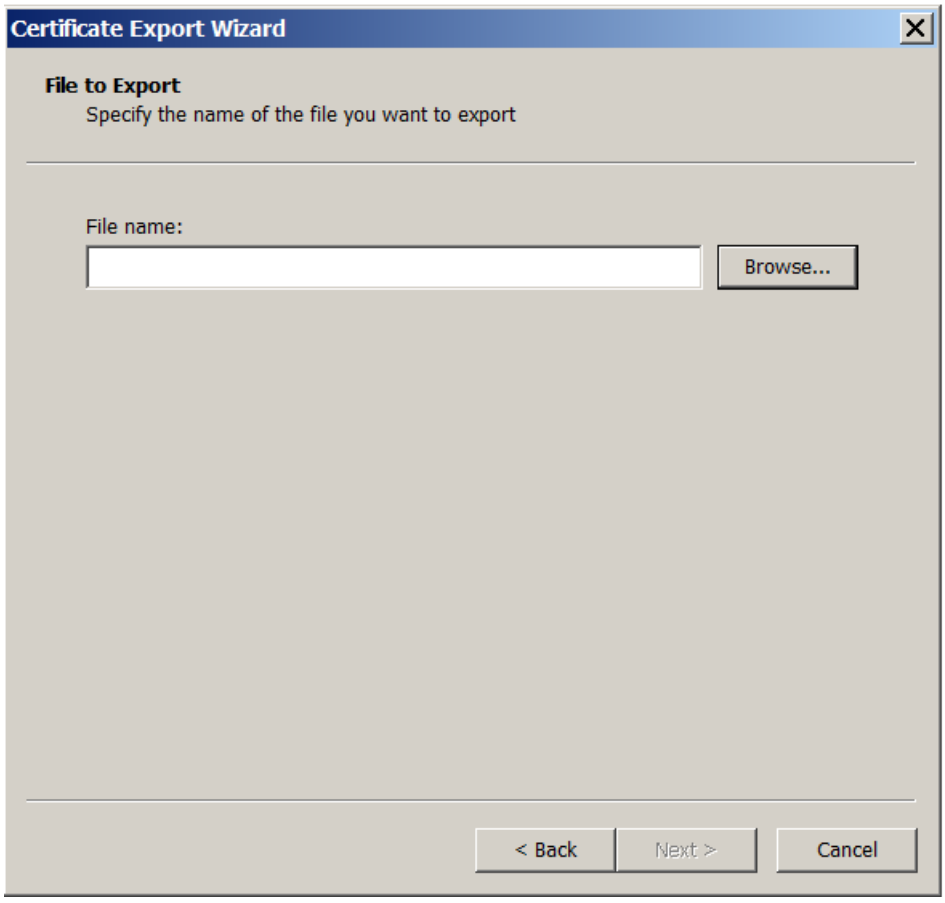


10. 保存该证书。



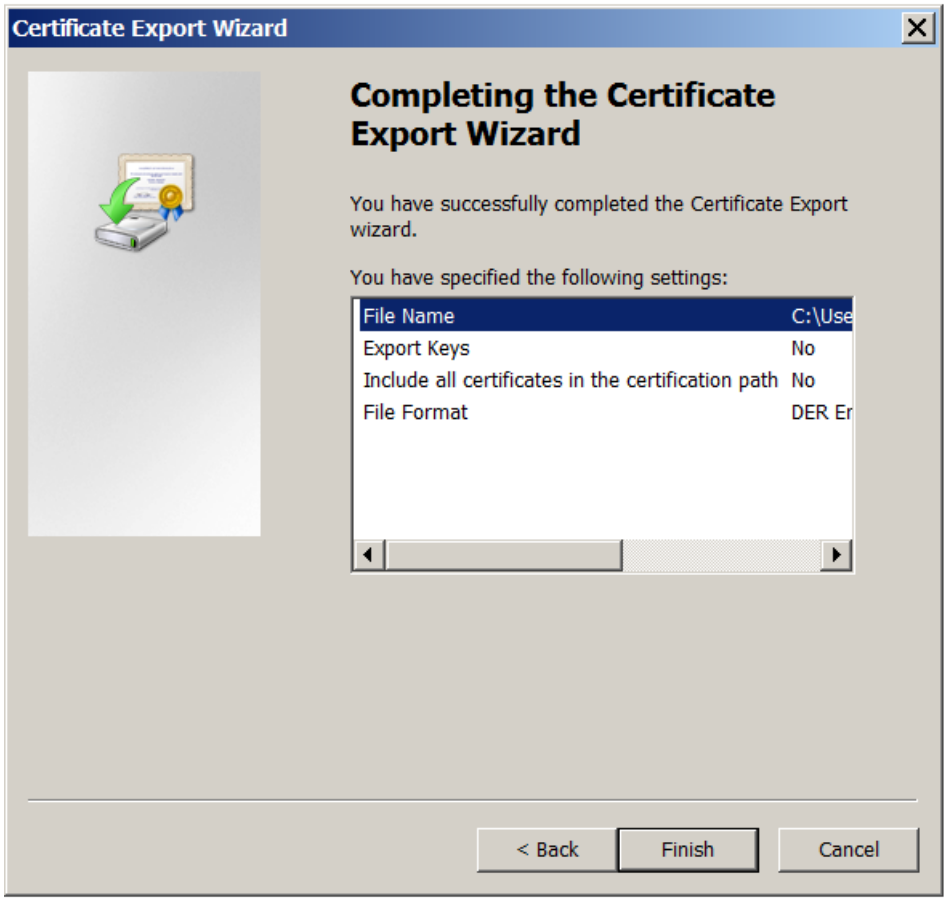
11. 浏览到该证书，然后单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

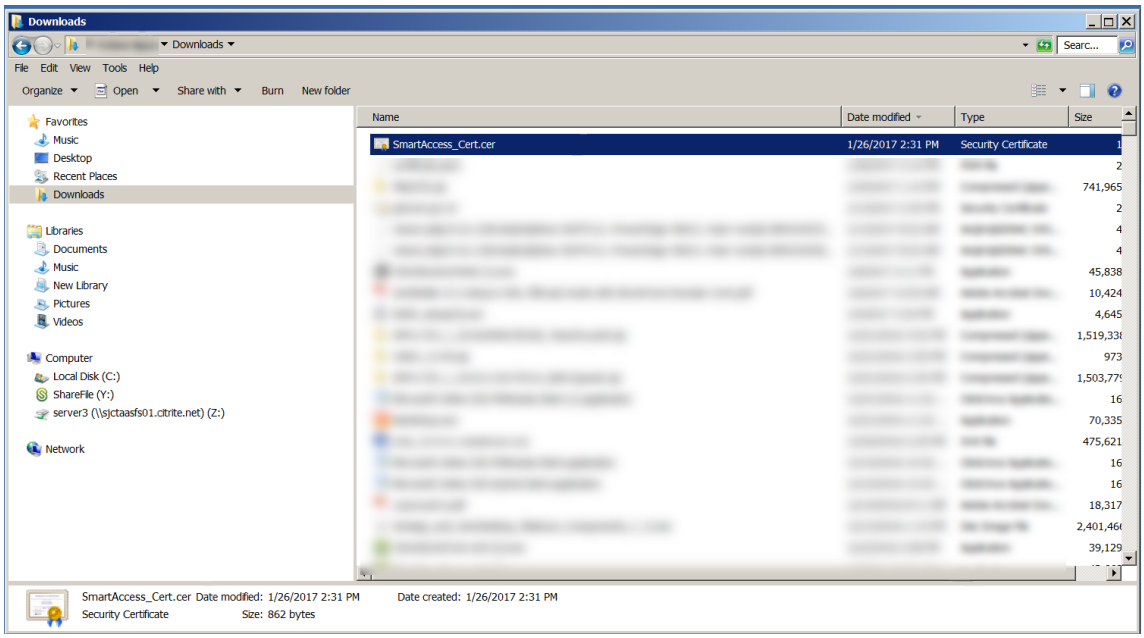


12. 检查您的选择，然后单击完成。单击确定消除确认窗口。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



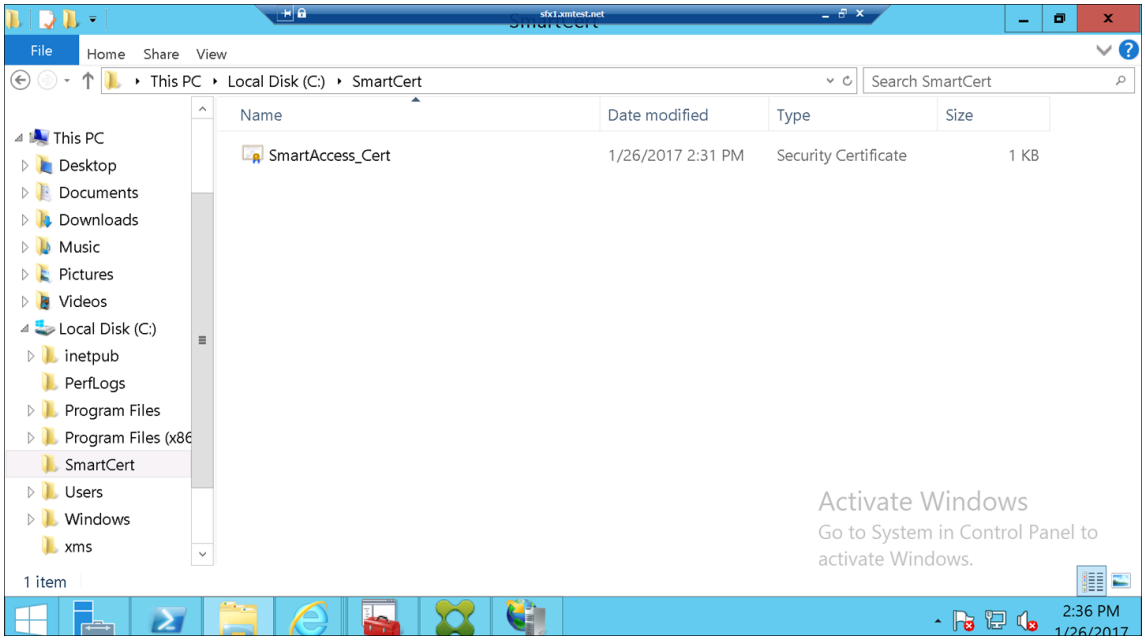
13. 在您的下载目录中找到该证书。请注意，证书为 CER 格式。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

将证书复制到 **StoreFront** 服务器

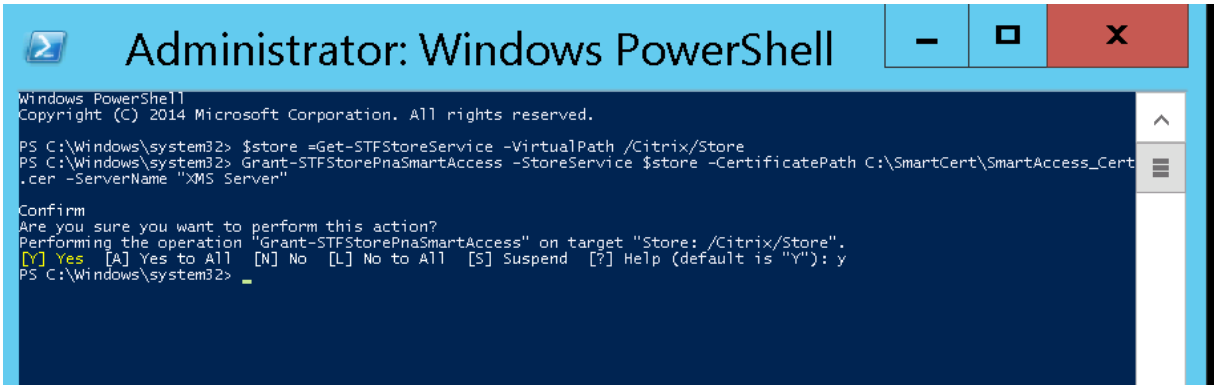
1. 在 StoreFront 服务器上，创建一个名为 **SmartCert** 的文件夹。
2. 将证书复制到 **SmartCert** 文件夹。



在 **StoreFront** 应用商店中配置证书

在 StoreFront 服务器上，运行以下 PowerShell 命令以在该应用商店上配置转换后的 Endpoint Management 服务器证书：

```
1    Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2  <!--NeedCopy-->
```



如果 StoreFront 应用商店上存在任何现有证书，请运行以下 PowerShell 命令以将其吊销：

```
1    Revoke-STFStorePnaSmartAccess -StoreService $store -All
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
<!--NeedCopy-->
```



或者，可以在 StoreFront 服务器上运行以下任意 PowerShell 命令以吊销 StoreFront 应用商店中的现有证书：

- 按名称吊销：

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "
       My XM Server"
<!--NeedCopy-->
```

- 按指纹吊销：

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess -StoreService $store -
       CertificateThumbprint "[Thumbprint]
<!--NeedCopy-->
```

- 按服务器对象吊销：

```
    $store = Get-STFStoreService -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess -StoreService $store

    Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

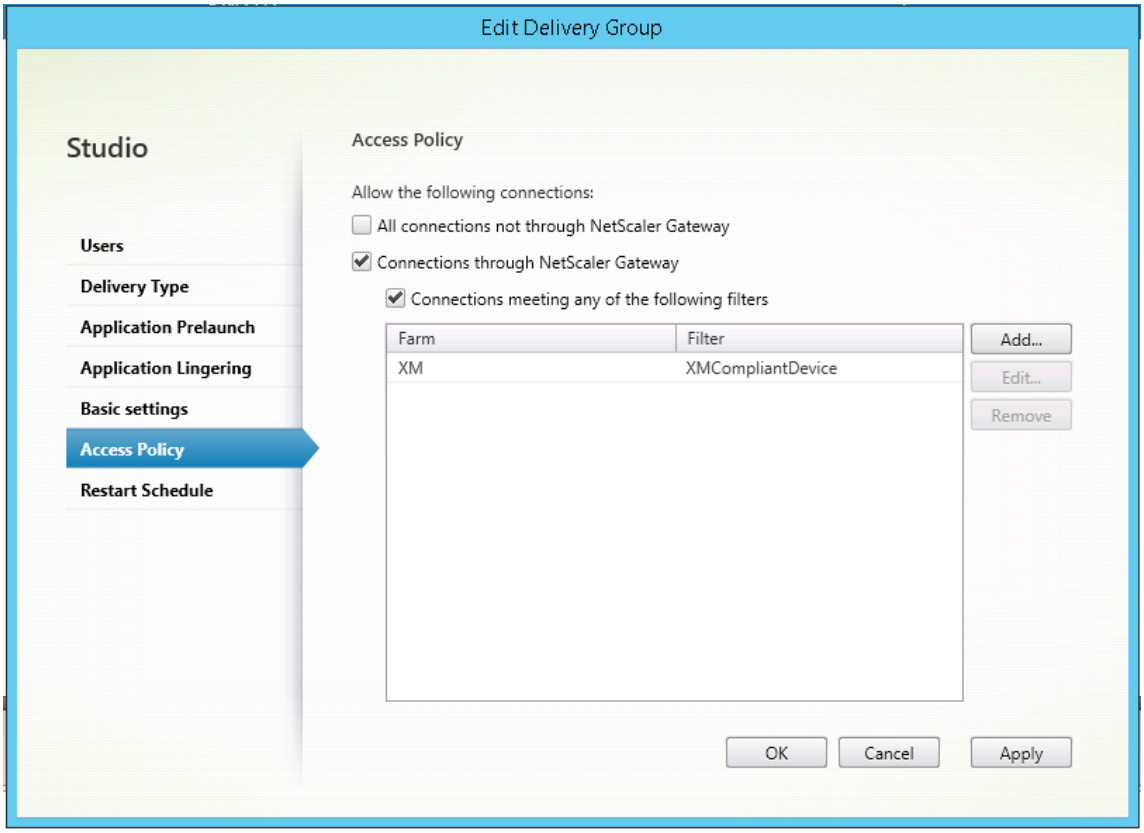
为 **Citrix Virtual Apps and Desktops** 配置 **SmartAccess** 策略

要将所需的 SmartAccess 策略添加到用于提供 HDX 应用程序的交付组中，请执行以下操作：

1. 从 Citrix Cloud 控制台打开 Citrix Studio。
2. 在 Studio 导航窗格中选择交付组。
3. 选择用于提供要控制对其访问的一个或多个应用程序的组。然后在操作窗格中选择编辑交付组。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

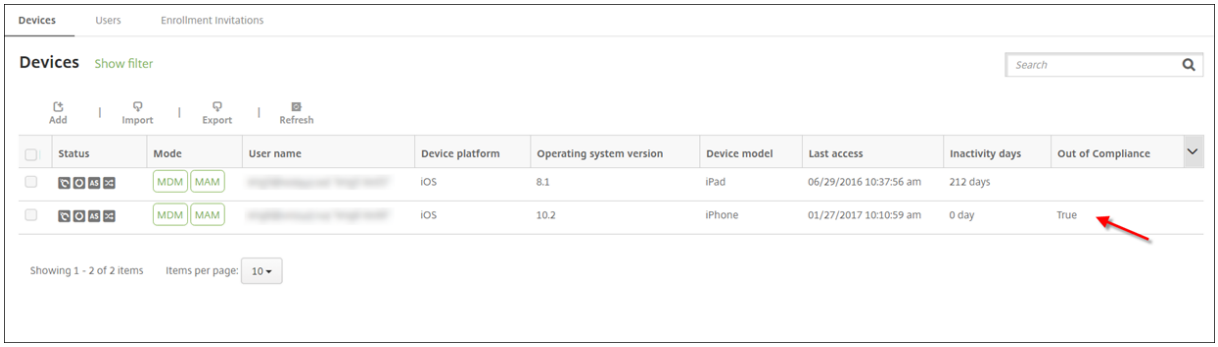
4. 在访问策略页面上，选择通过 **Citrix Gateway** 的连接和 **Connection meeting any of the following**（满足以下任一情况的连接）。
5. 单击添加。
6. 添加场为 **XM** 且过滤器为 **XMCompliantDevice** 的访问策略。



7. 单击应用以应用您所做的任何更改并使窗口保持打开，或单击确定应用更改并关闭窗口。

在 **Endpoint Management** 中设置自动操作

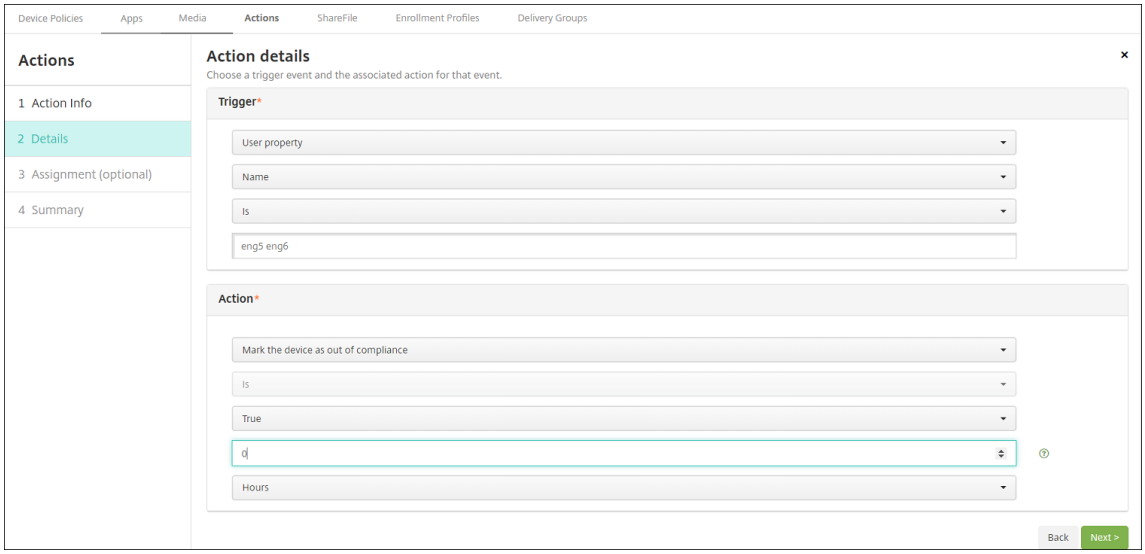
您在交付组中为 HDX 应用程序设置的 SmartAccess 策略在某个设备不合规时拒绝访问该设备。使用自动化操作将设备标记为不合规。



1. 在 Endpoint Management 控制台中，单击配置 **>** 操作。此时将显示操作页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 单击添加以添加操作。此时将显示操作信息页面。
3. 在操作信息页面上，键入操作的名称和说明。
4. 单击下一步。此时将显示操作详细信息页面。在以下示例中，创建了一个在设备的用户属性名称为 **eng5** 或 **eng6** 时立即将其标记为不合规的触发器。



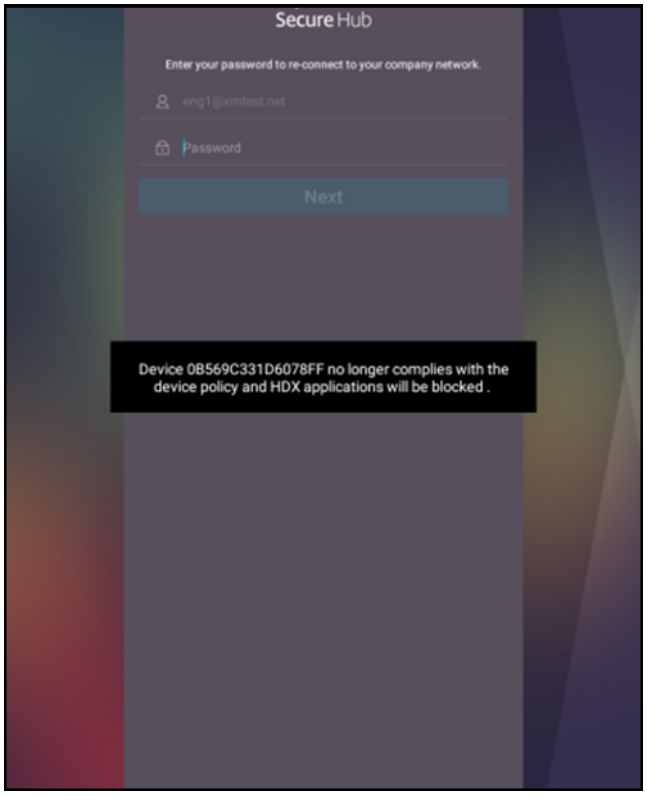
5. 在触发器列表中，选择设备属性、用户属性或已安装应用程序的名称。SmartAccess 不支持事件触发器。
6. 在操作列表中：
   - 选择 将设备标记为不合规。
   - 选择是。
   - 选择 **True**。
   - 要将操作设置为满足触发条件时立即将设备标记为不合规，请将时间范围设置为 **0**。
7. 选择要应用此操作的一个或多个 Endpoint Management 交付组。
8. 检查操作的摘要。
9. 单击下一步，然后单击保存。

当设备被标记为不合规时，HDX 应用程序不会再在 Secure Hub 应用商店中显示。用户将无法再订阅这些应用程序。不会向设备发送任何通知，并且 Secure Hub 应用商店中没有任何迹象指示以前提供过 HDX 应用程序。

如果希望用户在设备被标记为不合规时接收通知，请创建一个通知，然后创建一项用于发送该通知的自动化操作。

本示例将在设备被标记为不合规时创建并发送以下通知：Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked（设备序列号或电话号码不再符合设备策略，HDX 应用程序将被阻止）。

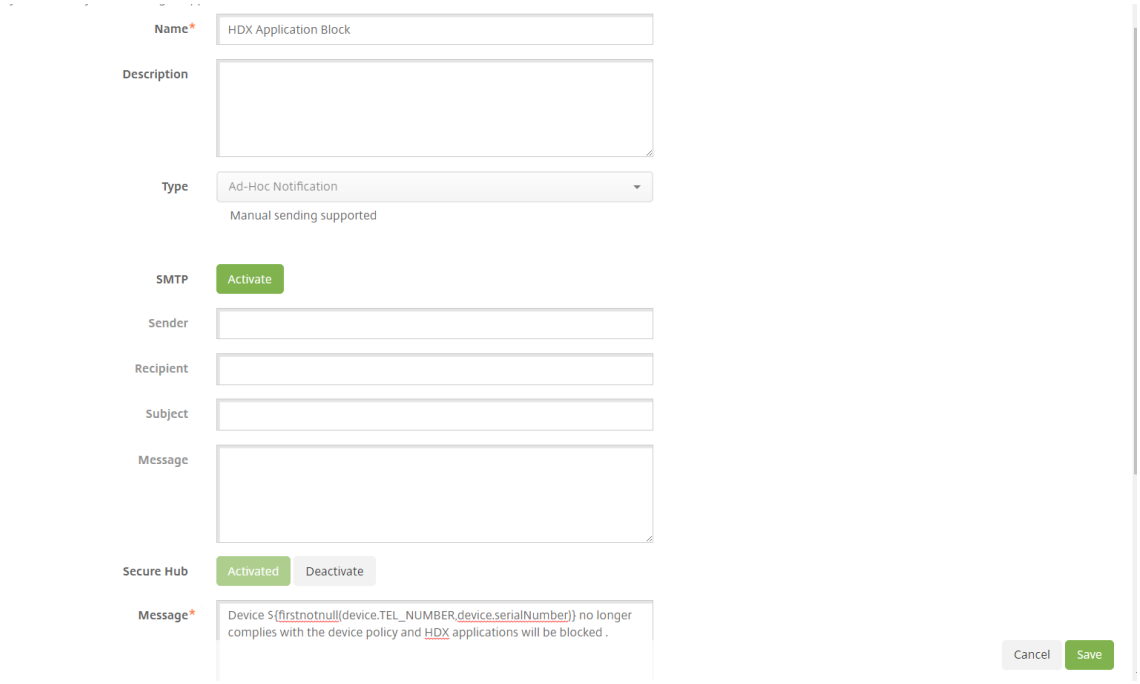
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



创建当设备被标记为不合规时用户看到的通知

1. 在 Endpoint Management 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击通知模板。此时将显示通知模板页面。
3. 单击添加在通知模板页面上进行添加。
4. 配置以下设置：
    - 名称： HDX 应用程序阻止
    - 说明：设备不合规时的代理通知
    - 类型：临时通知
    - **Secure Hub**：已激活
    - 消息：设备 `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 不再符合设备策略，HDX 应用程序将被阻止。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

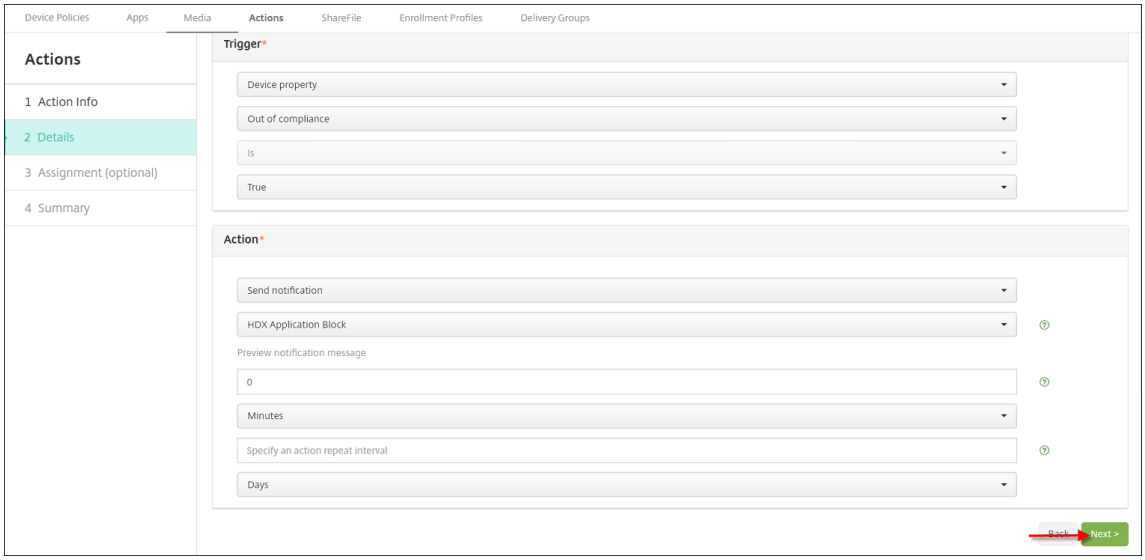


5. 单击保存。

创建当设备标记为不合规时用于发送通知的操作

1. 在 Endpoint Management 控制台中，单击配置 **>** 操作。此时将显示操作页面。
2. 单击添加以添加操作。此时将显示操作信息页面。
3. 在操作信息页面上，输入操作的名称和说明：
   - 名称：HDX 阻止了通知
   - 说明：由于设备不合规，HDX 阻止了通知
4. 单击下一步。此时将显示操作详细信息页面。
5. 在触发器列表中：
   - 选择设备属性。
   - 选择 不合规。
   - 选择是。
   - 选择 **True**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 在操作列表中，指定满足触发条件时发生的操作：
   - 选择发送通知
   - 选择 **HDX Application Block, the notification you created**（HDX 应用程序阻止，您创建的通知）
   - 选择 **0**。将此值设置为 0 会导致通知在满足触发条件时立即发送。
7. 选择要应用此操作的一个或多个 Endpoint Management 交付组。在此示例中，请选择 **AllUsers**。
8. 检查操作的摘要。
9. 单击下一步，然后单击保存。

有关设置自动化操作的详细信息，请参阅自动化操作。

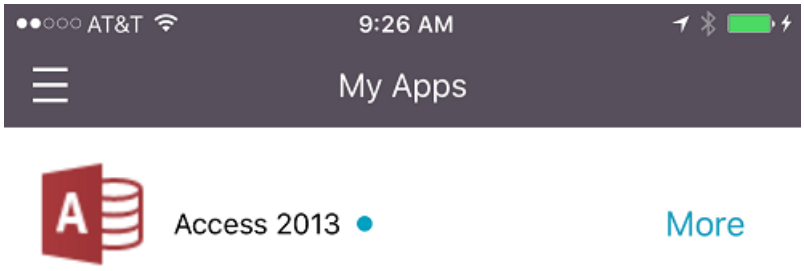
用户如何重新获取对 **HDX** 应用程序的访问权限

用户可以在设备恢复合规后再次获取对 HDX 应用程序的访问权限：

1. 在设备上，转至 Secure Hub 应用商店以刷新应用商店中的应用程序。
2. 转至该应用程序并轻按添加以添加该应用程序。

添加后，该应用程序将在“我的应用程序”中显示，旁边带有一个蓝点，因为这是新安装的应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



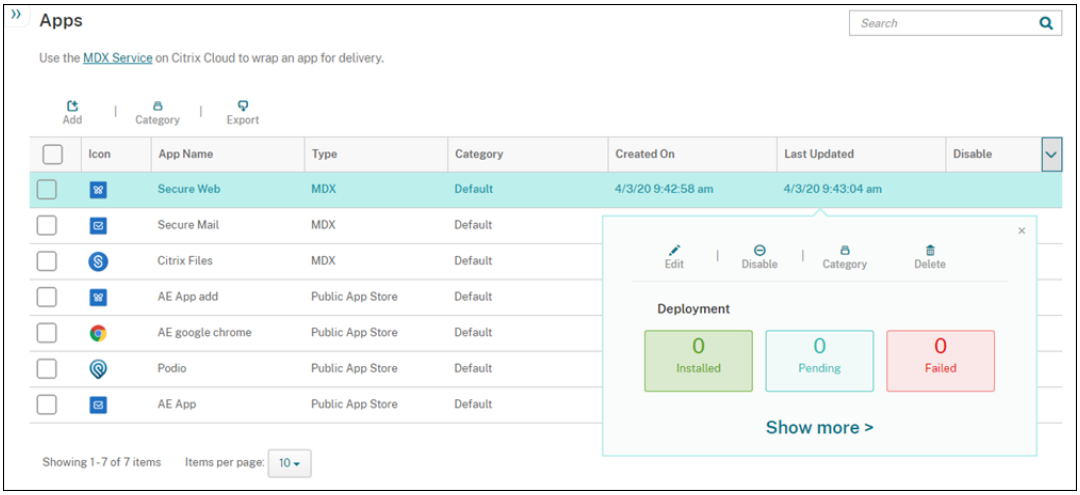
升级 **MDX** 或企业应用程序

May 6, 2022

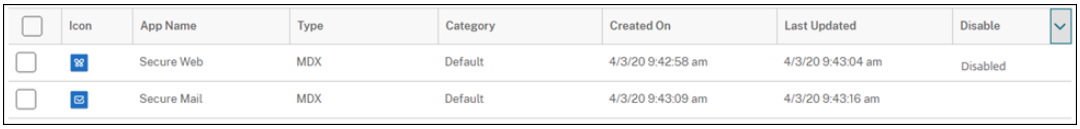
要在 Endpoint Management 中升级 MDX 或企业应用程序，请在 Endpoint Management 控制台中禁用该应用程序，然后上载该应用程序的新版本。

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序。此时将显示应用程序页面。
2. 对于托管设备（在 Endpoint Management 中注册用于移动设备管理的设备），跳至步骤 3。对于未托管设备（在 Endpoint Management 中注册仅用于企业版应用程序管理目的的设备），请执行以下操作：
   a) 在应用程序表中，选中应用程序旁边的复选框或单击包含要更新的应用程序的行。
   b) 在显示的菜单中单击禁用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



c) 在确认对话框中单击禁用。已禁用显示在应用程序的禁用列中。



> 注意：
>
> 禁用应用程序时，用户在注销后无法重新连接到应用程序。禁用应用程序是可选的，但我们建议禁用该应用程序以避免应用程序功能问题。例如，用户在上载新版本的同时请求下载应用程序可能会导致出现问题。

3. 在应用程序表中，单击应用程序旁边的复选框或单击包含要更新的应用程序的行。
4. 在显示的菜单中单击编辑。此时将显示应用程序信息页面，您最初为应用程序选择的平台处于选中状态。
5. 配置以下设置：
   - 名称：（可选）更改应用程序名称。
   - 说明：（可选）更改应用程序说明。
   - 应用程序类别：（可选）更改应用程序类别。
6. 单击下一步。此时将显示首先选择的平台页面。请为选择的每个平台执行以下操作：
   a) 单击上载并导航到要上载的替换文件所在位置，选择该文件。应用程序将上载到 Endpoint Management。

   如果您要上载适用于 Android Enterprise 的应用程序，则会出现一个托管 Google Play 窗口。请在此处上载新版本的应用程序。有关更多详细信息，请参阅分发 Android Enterprise 应用程序。

   b) 可选，更改平台的应用程序详细信息和策略设置。

   c)（可选）配置部署规则和应用商店。有关信息，请参阅 添加 MDX 应用程序。
7. 单击保存。此时将显示应用程序页面。
8. 如果在步骤 2 中禁用了该应用程序，请执行以下操作：
   a) 在应用程序表中，通过单击选择已更新的应用程序，然后在显示的菜单中单击启用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

b) 在显示的确认对话框中，单击启用。用户现在可以访问该应用程序并接收提示用户升级应用程序的通知。

添加媒体

December 3, 2021

将媒体添加到 Endpoint Management，以便将媒体部署到用户设备。可以使用 Endpoint Management 部署您通过 Apple 批量购买获取的 Apple Books。

在 Endpoint Management 中配置批量购买帐户后，您购买的书籍以及免费书籍将显示在配置 **>** 媒体中。从媒体页面中，可以通过选择交付组并指定部署规则来配置书籍在 iOS 设备中的部署。

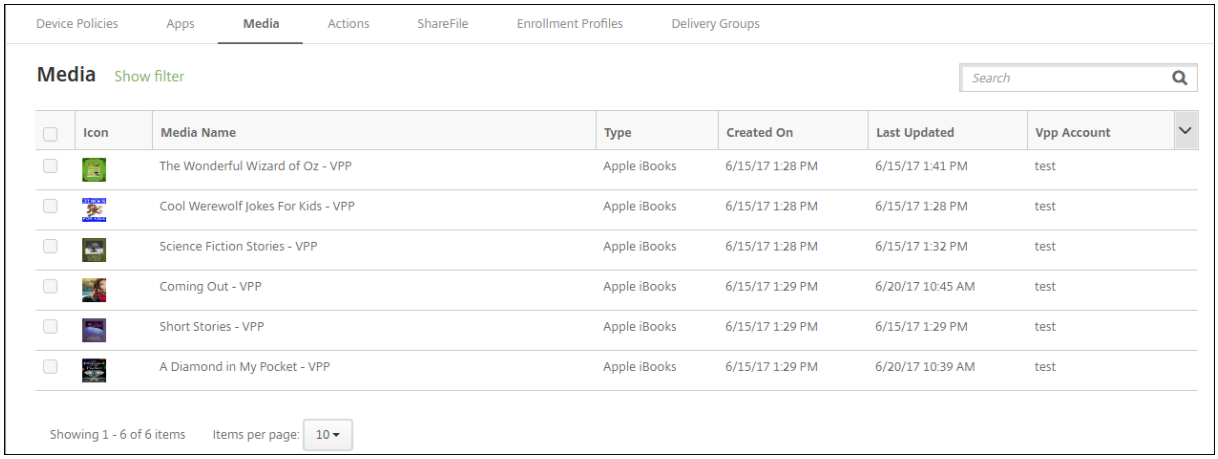
用户首次收到书籍并接受批量购买许可证时，已部署的书籍将在设备上安装。这些书籍将在 Apple 书籍应用程序中显示。不能取消书籍许可证与用户的关联，也不能从设备中删除书籍。Endpoint Management 将书籍安装为必需媒体。如果用户从其设备中删除了已安装的书籍，该书籍仍保留在 Apple 书籍应用程序中，可随时下载。

必备条件

- iOS 设备
- 如 Apple 批量购买中所述，在 Endpoint Management 中配置 Apple 批量购买。

配置书籍

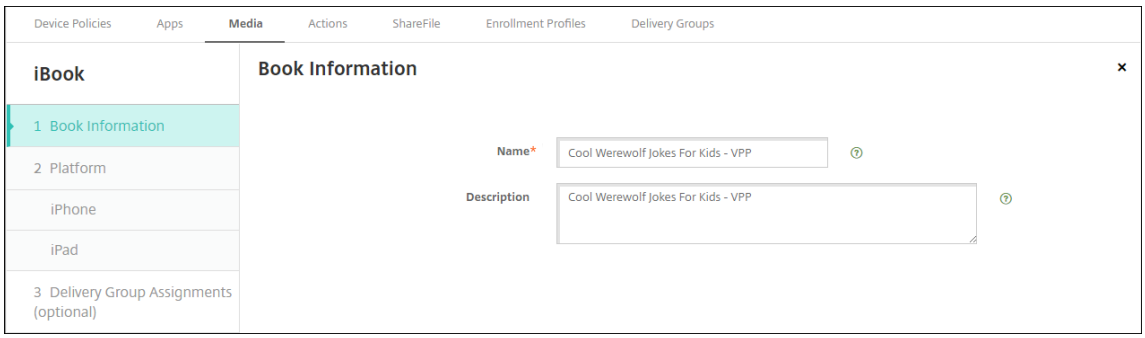
通过批量购买获取的 Apple Books 显示在配置 **>** 媒体页面上。



配置要部署的 **Apple** 书籍

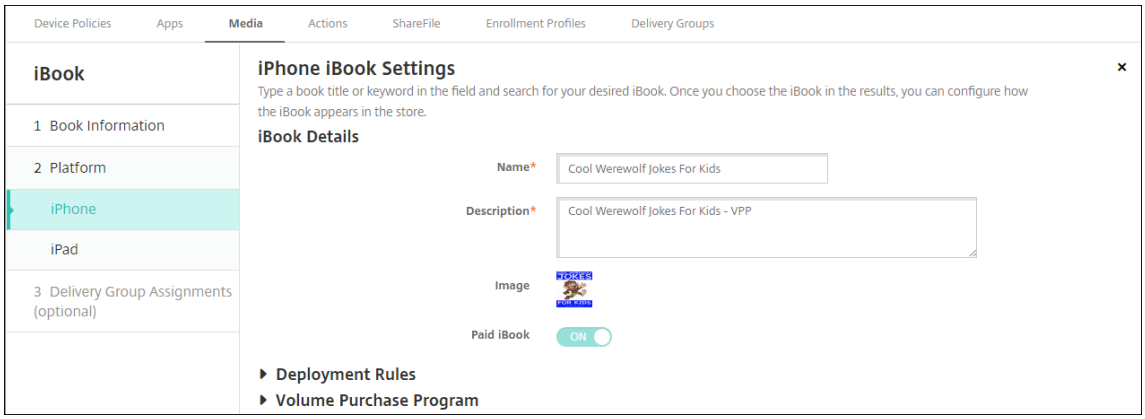
1. 在配置 **>** 媒体中，选择一本图书并单击编辑。此时将显示书籍信息页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

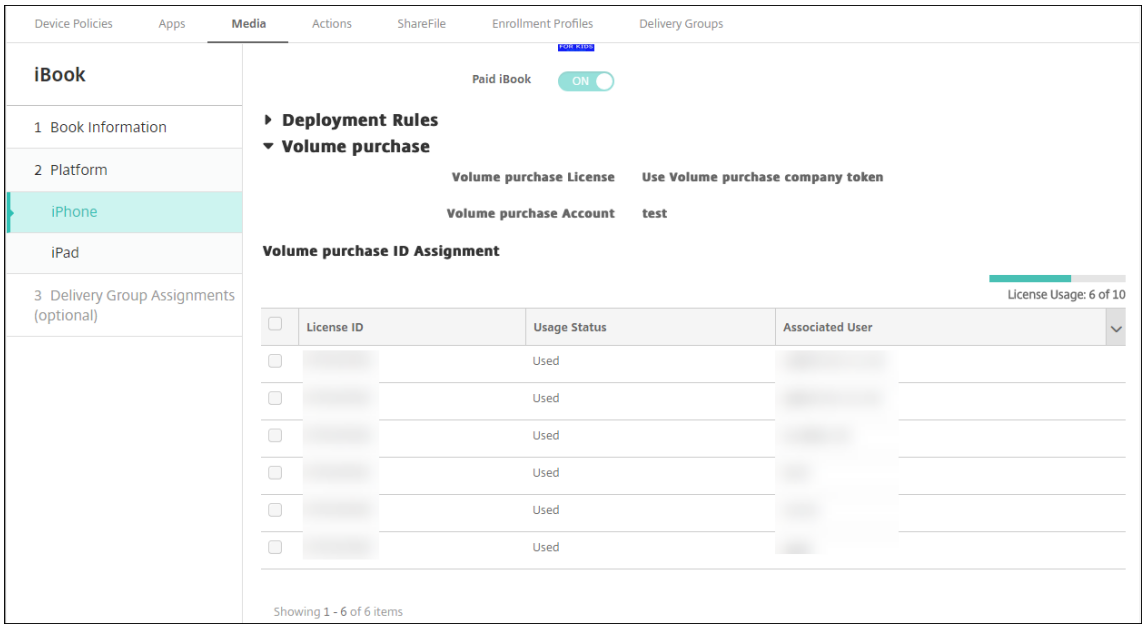


名称和描述仅显示在 Endpoint Management 控制台和日志中。

2. 在 **iPhone iBook** 设置和 **iPad iBook** 设置页面中：虽然您可以选择更改书籍名称和说明，但 Citrix 建议您不要更改这些设置。图片仅供参考，不可编辑。**Paid iBook** 指示书籍是通过 Apple 批量购买购买的。

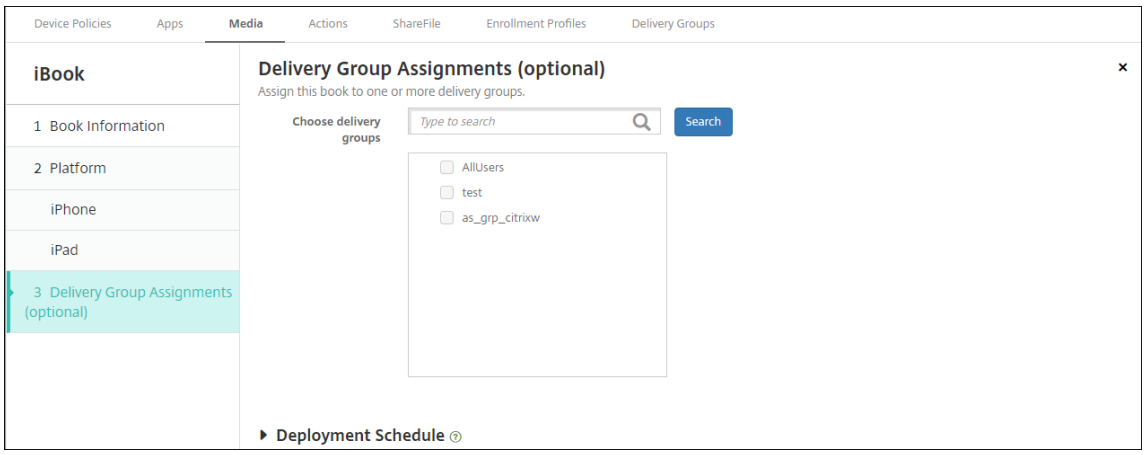


还可以指定部署规则或查看批量购买信息。

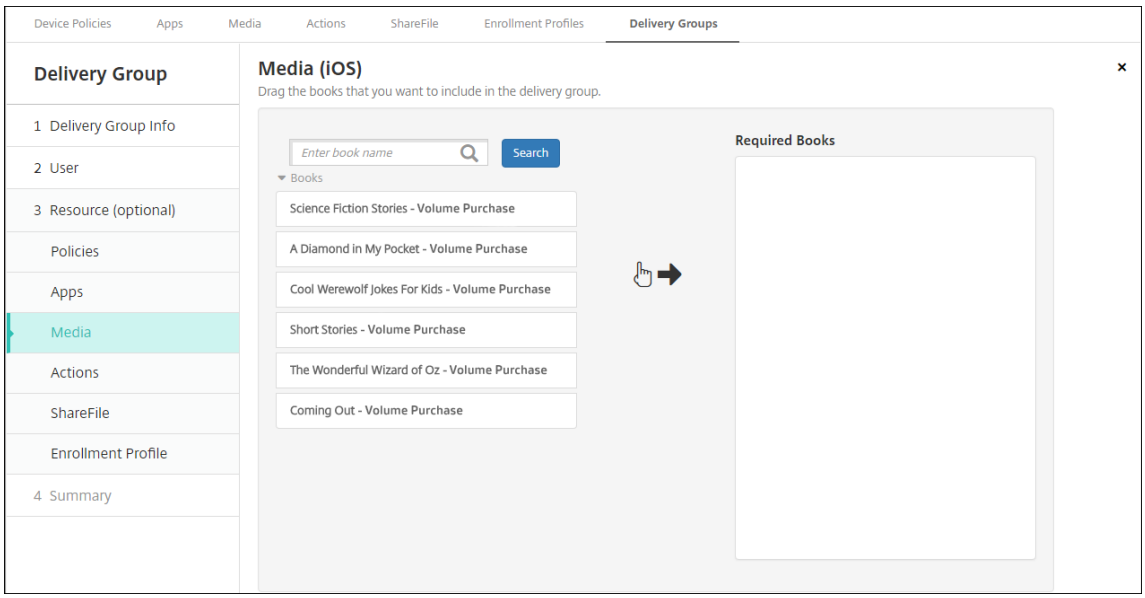


3.（可选）将书籍分配给部署组并设置部署计划。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

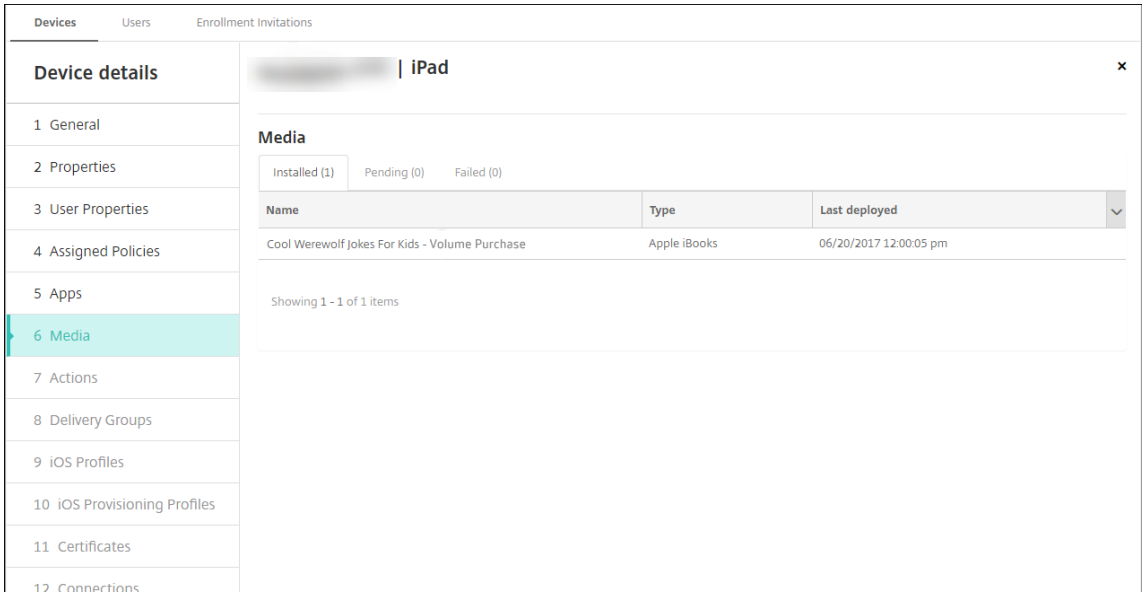


还可以从配置 **>** 交付组的媒体选项卡将书籍分配给交付组。Endpoint Management 仅支持所需的书籍部署。



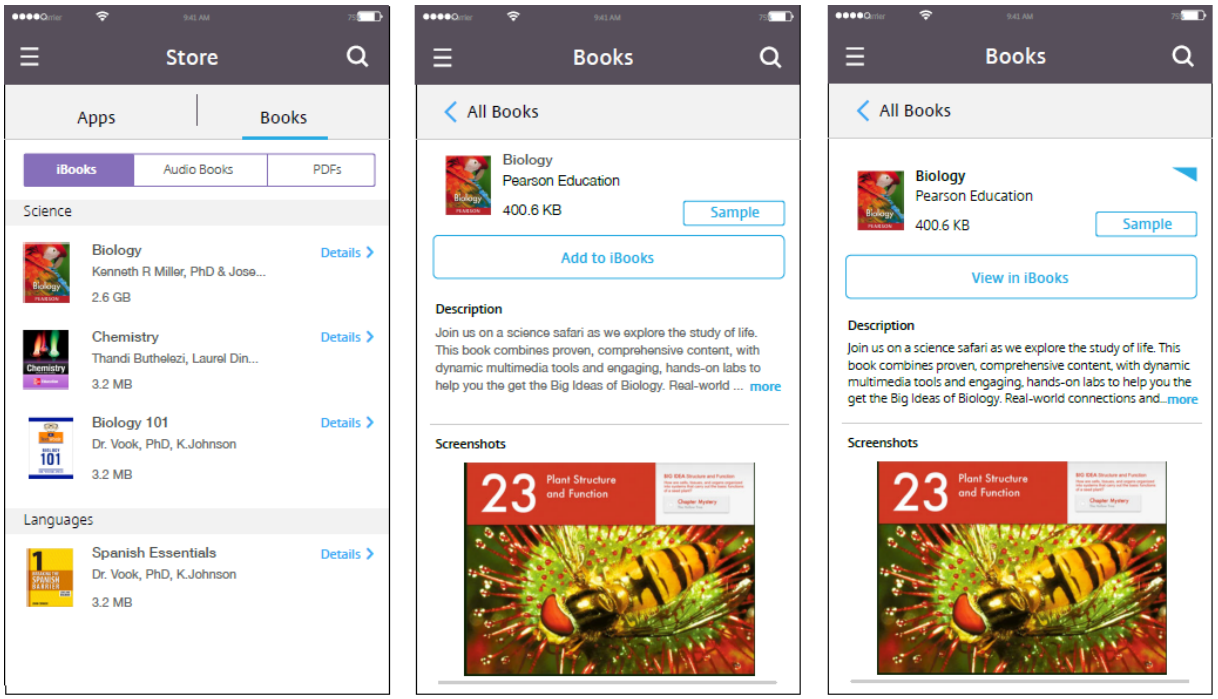
4. 使用管理 **>** 设备的媒体选项卡可查看部署状态。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



> 注意：
>
> 在配置 > 媒体页面上，如果您选择某本书籍并单击删除，Endpoint Management 将从列表中删除该书籍。但是，Endpoint Management 下次与 Apple 批量购买同步时，除非已将其从 Apple 批量购买中删除，否则该书籍会在列表中重新出现。从列表中删除某本书籍不会将其从设备中删除。

书籍显示在用户设备上，如以下示例所示。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

部署资源

February 22, 2022

在设备配置和管理过程中，通常需在 Endpoint Management 控制台中创建资源（策略、应用程序和媒体）和操作，然后使用交付组对其进行封装。交付组定义用户类别，以便您可以将指定的策略、应用程序、媒体和操作部署到其设备。使用 Endpoint Management 控制台，您可以：

- 添加、管理和部署交付组。
- 更改 Endpoint Management 将交付组中的资源和操作推送到设备的顺序。此命令称为部 署订单。

  您可以在 Endpoint Management 控制台中指定部署顺序。但是，当用户位于具有重复或冲突策略的多个交付组中时，Endpoint Management 将确定部署顺序。请参阅计算步骤。

关于交付组

交付组中包含的内容通常取决于用户的特征，例如公司、国家/地区、部门、办公地址和职务。交付组可让您更好地控制谁获得哪些资源以及何时获得资源。您可以将交付组部署到所有用户或定义的用户组。

安装和配置 Endpoint Management 将创建默认交付组 allUsers。此组包含所有本地和 Active Directory 用户。您无法删除 allUsers 组，但可以在不想向所有用户推送资源时将其禁用。有关详细信息，请参阅启用和禁用 allUsers 交付组。

将资源部署到交付组时，您将向交付组中的所有用户发送推送通知。对于 Apple 设备，请使用 Apple 推送通知服务 (APN) 发送通知。有关更多信息，请参阅 APNs 证书)。对于 Android 设备，请使用 Firebase Cloud Messaging (FCM)。有关更多信息，请参阅 Firebase Cloud Messaging。对于 Windows 设备，请使用 Windows 推送通知服务 (WNS)。

关于部署资源

在将资源推送到设备时，请考虑以下事项：

- 部署顺序： 部署顺序是 Endpoint Management 向设备推送资源（策略、应用程序和媒体）和操作的顺序。部署顺序适用于为设备管理 (MDM) 或应用程序管理 (MAM) 和 MDM 的组合配置了注册配置文件的交付组中的设备。
- 部署规则： Endpoint Management 使用您为用户和设备属性指定的部署规则来筛选策略、应用程序、媒体、操作和交付组。例如，某个部署规则可能指定当域名与特定值匹配时推送部署软件包。

  在交付组中，您可以根据用户和设备属性指定接收资源的用户和设备的子集。交付组中的用户和设备属性筛选优先于在资源上设置的部署规则。
- 部署计划： Endpoint Management 使用您为策略、应用程序、媒体和操作指定的部署计划来控制这些项目的部署。您可以指定现在、在设定的日期和时间或满足部署条件时进行部署。您可以在创建规则时指定计划。请参阅配置部署规则。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在添加交付组之前，请考虑部署顺序、规则和计划与部署目标的关系。

部署顺序

部署顺序是指 Endpoint Management 向设备推送资源的顺序。当存在资源的先决条件和资源之间的依赖关系时，部署顺序很重要。资源包括策略、应用程序、操作和交付组。

例如，如果您要推出具有基于证书的身份验证的 Wi-Fi 策略，则必须在 Wi-Fi 策略之前推出认证策略。否则，会发生错误。相反，对于某些策略（例如条款和条件、软件清单和操作），部署顺序无关紧要。

添加交付组时，您可以指定将资源部署到设备的顺序。但是，Endpoint Management 始终会识别用户位于具有重复或冲突策略的多个交付组中的每种情况。在这些情况下，Endpoint Management 会计算交付给设备的对象和它执行的操作的部署顺序。

在确定部署顺序时，Endpoint Management 将对资源应用过滤器和控制标准，例如部署规则和部署计划。下表显示了您可以将哪些标准应用于每种类型的资源。

资源	设备平台	部署规则	部署计划	用户/组
设备策略	Y	Y	Y	-
应用程序	Y	Y	Y	-
媒体	Y	Y	Y	-
操作	-	Y	Y	-
交付组	-	Y	-	Y

计算步骤

当 Endpoint Management 需要计算部署顺序时，它将执行以下步骤。

> 注意：
>
> 设备平台不会影响计算步骤。

1. 根据用户、组和部署规则的过滤器确定特定用户的所有交付组。
2. 创建选定交付组中所有资源（策略、应用程序、媒体和操作）的有序列表。该列表建立在设备平台、部署规则和部署计划的过滤器的基础之上。排序算法如下所述：
    a) 将具有管理员定义的部署顺序的交付组中的资源置于没有交付组的资源之前。有关详细信息，请参阅使用用户定义顺序进行计算
    b) 作为交付组之间的决胜局，请按交付组名称的反向字母顺序对交付组中的资源进行排序。例如，Endpoint Management 将交付组 B 中的资源置于交付组 A 的资源之前。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

c) 在排序时，如果为交付组的资源指定了管理员定义的部署顺序，请保持该顺序。否则，请按资源名称的字母顺序对该交付组中的资源进行排序。

d) 如果同一资源多次出现，请删除重复的资源。只提供这些资源中的第一个。

与管理员定义的订单关联的资源在没有管理员定义订单的资源之前部署。

使用管理员定义的订单进行计算示例

假设您有两个交付组：

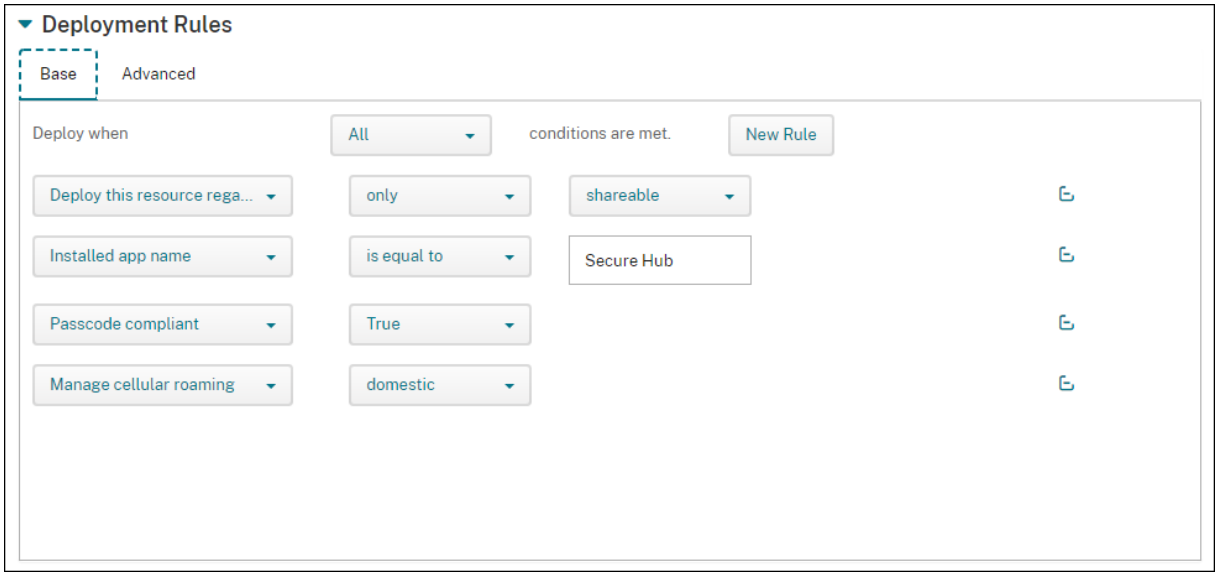
- 交付组客户经理 1：具有 未指定的资源订单。包含策略 网络和 密码。
- 交付组客户经理 2：具有 指定的资源订单。按顺序包含 连接计划、限制、密码和 网络策略。

如果计算算法仅按名称对部署组进行排序，则 Endpoint Management 将按此顺序进行部署，从交付组 Account Manager 1：网络、密码、连接计划和 限制开始。Endpoint Management 将忽略客户经理 2 交付组中的 密码和 网络（两者都是重复的）。

但是，Account Managers 2 组具有用户指定的部署顺序。因此，计算算法将客户经理 2 交付组中的资源放置在列表中的位置，高于账户经理 1 交付组中的资源。因此，Endpoint Management 按以下顺序部署策略：连接计划、限制、通行码和 网络。Endpoint Management 会忽略账户经理 1 交付组中的 网络和 密码策略，因为它们是重复的。该算法遵循 Endpoint Management 管理员指定的顺序。

配置部署规则

配置部署规则以在满足特定条件时交付资源。可以配置基本部署规则或高级部署规则。



使用基本编辑器添加部署规则时，首先选择何时部署资源。

- 全部：当用户或设备满足您配置的所有条件时交付资源。
- 任何：当用户或设备至少满足您配置的一个条件时交付资源。

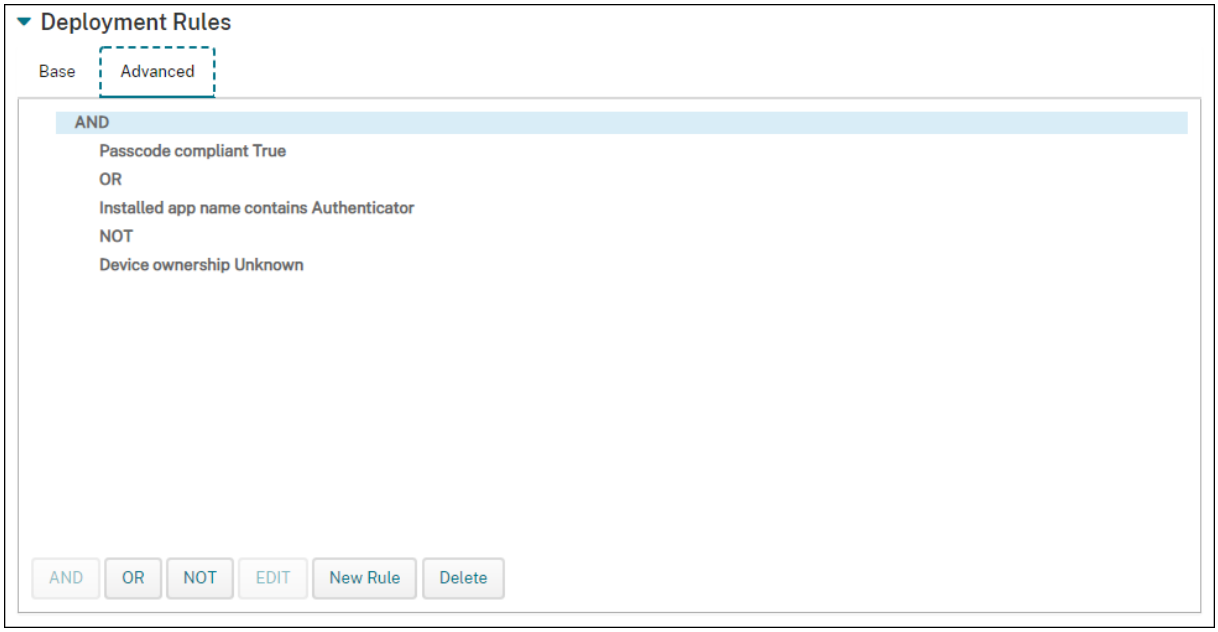
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

单击 新建规则从可用规则列表中选择要添加的规则。根据所部署的资源和为其配置资源的平台，可用规则会有所不同。每条规则中都有条件。

您可以指定部署资源：

- 仅当选定的属性存在时或选定的属性存在时除外。
- 当属性与您键入的文本完全匹配时，属性将包含您键入的文本，或者属性与您键入的文本不匹配。
- 当设备或用户符合您选择的属性或不符合您选择的属性时。
- 当设备或用户属性与您从预定义列表中选择的条件匹配时。

使用高级编辑器创建更复杂的部署规则。您可以从更多规则中进行选择，也可以在创建高级规则时组合不同的布尔逻辑运算符。



使用交付组

您可以通过以下方式使用交付组：

- 添加交付组
- 部署到交付组
- 删除交付组
- 编辑交付组
- 启用和禁用 allUsers 交付组。

添加交付组

创建交付组时，请指定用户分配是在 Endpoint Management 中还是在 Citrix Cloud 中进行管理。创建交付组后，您无法更改此规范。

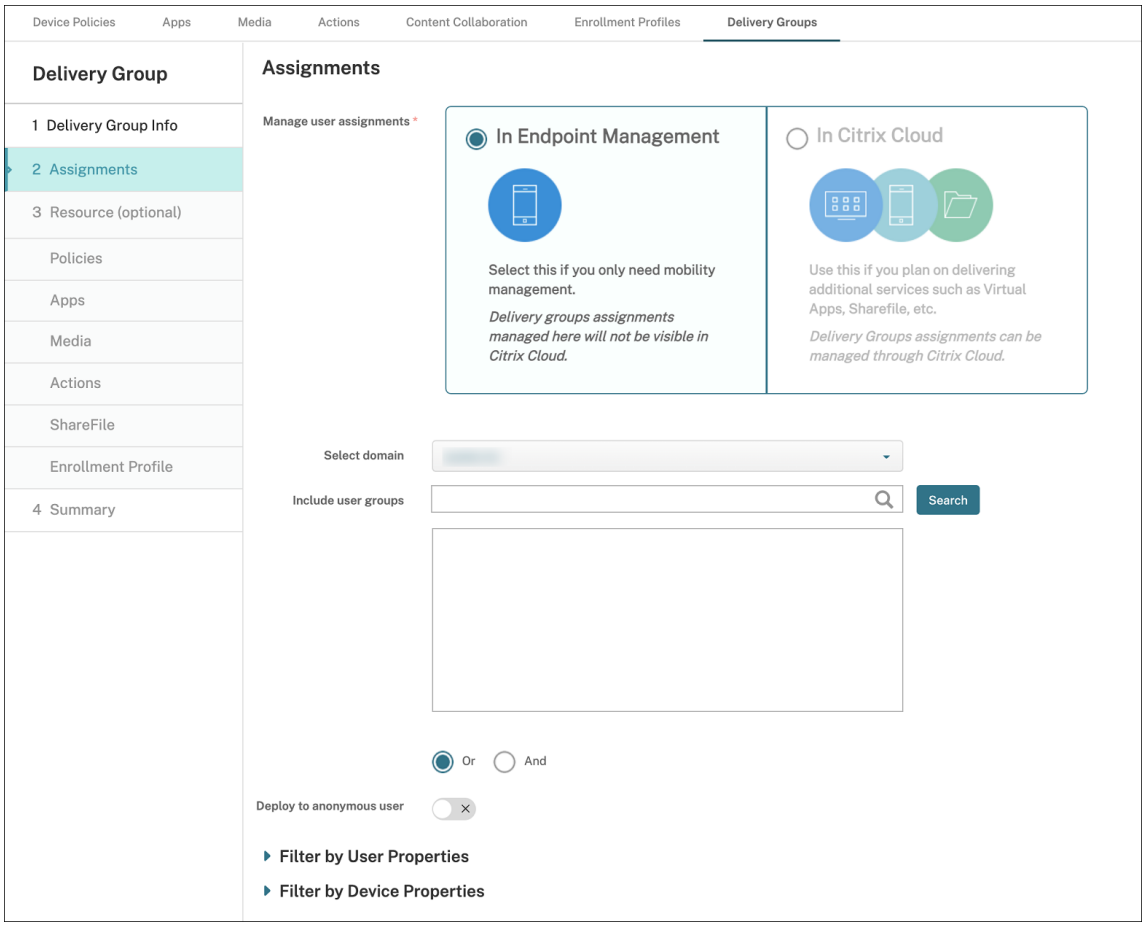
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

如果计划使用交付组交付其他 Citrix Cloud 服务，请指定以管理 Citrix Cloud 中的用户分配。其他 Citrix Cloud 服务包括 Citrix Virtual Apps and Desktops、Citrix Content Collaboration 或安全浏览器服务。您只能将 Active Directory 用户添加到 Citrix Cloud 中托管的交付组。

如果您只需要用户和应用程序交付组的移动性管理，请将 管理用户分配设置为 在 **Endpoint Management** 中。您无法在 Citrix Cloud 的 Endpoint Management 中看到具有管理用户的交付组。因此，您无法使用 Endpoint Management 中托管的交付组来交付其他服务。

> 注意：
>
> 我们建议在创建设备策略和注册配置文件之前添加交付组。有关创建它们的信息，请参阅 设备策略 和 注册配置文件。

1. 在 Endpoint Management 控制台中，单击配置 **>** 交付组。
2. 在交付组页面上，单击添加。
3. 在交付组信息页面中，键入交付组的名称和说明，然后单击下一步。
4. 在分配页面上，指定如何管理交付组分配。



- 管理用户分配：
  - 在 **Endpoint Management** 中：如果您计划为只需要移动性管理的用户和应用程序创建交付组，

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

请选择此选项。您看不到其用户分配在 Citrix Cloud 的 Endpoint Management 中管理的交付组，也无法使用它们来交付其他服务。

- 在 **Citrix Cloud** 中：如果计划使用交付组提供其他服务，请选择此选项。这些服务可能包括 Citrix Virtual Apps and Desktops 或 Citrix Content Collaboration。

5. 将用户添加到交付组。

> 重要：
>
> 创建交付组后，您无法更改 管理用户分配设置。

- 选择域：在列表中，选择要从中选择用户的域。
- 包括用户组：执行以下操作之一：
  - 在用户组列表中，单击要添加的组。选定的组将显示在选定用户组列表中。
  - 单击搜索以查看选定域中所有用户组的列表。您也可以在搜索框中键入完整或部分组名称，然后单击“ 搜索”以缩小搜索范围。

  要从选定用户组列表中删除某个用户组，请执行以下操作之一：
  - 在 选定的用户组列表中，单击要删除的每个组旁边的 **X** 。
  - 单击搜索以查看选定域中所有用户组的列表。或者，在单击“搜索”缩小 搜索范围之前，键入完整或部分组名称。清除要删除的每个组的复选框。
- 或/与：选择用户是位于任意组（或）即可，还是必须位于所有组中（与），才能向其部署资源。
- 部署到匿名用户：选择是否部署到交付组中未经身份验证的用户。未经身份验证的用户是指您无法进行身份验证但仍允许其设备连接到 Endpoint Management 的用户。

6. 展开 按用户属性筛选或按设备属性筛选以指定交付组管理资源的方式。
   - 如果选择 按设备属性筛选，请展开设备平台以配置部署规则：
     - 设备属性-**Android** （请参阅创建规则以将资源部署到 Android 设备）
     - 设备属性-**iOS**
     - 设备属性-仅限 **Windows** 台式机/平板电脑
   - 默认情况下将显示基础选项卡。在“ 基本”选项卡下，指定何时部署策略。可以选择在满足全部条件时部署策略，或在满足任意条件时部署策略。默认选项为全部。
     - 单击新建规则以定义条件。
     - 在列表中，选择条件。例如，选择设备所有权和 BYOD。
     - 对于要添加的每个条件，单击“ 新建规则”。
   - 单击高级选项卡以使用布尔选项组合规则。此时将显示您在基础选项卡上选择的条件。
     - 单击“ 与”、“ 或”或“ 不”，然后单击“ 新建规则”。
     - 在列表中，选择要添加到规则的条件，然后单击右侧的加号 (+)。
       您可以随时单击以选择条件，然后单击 编辑更改条件或单击 删除以删除条件。

7. 单击“ 下一步”转到“ 策略”页面。您可以选择在此处为交付组添加策略、应用程序、媒体或操作。有关详细信息，请参阅：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 向交付组添加策略
- 将应用程序添加到交付组
- 将媒体添加到交付组
- 向交付组添加操作

8. 如果您对交付组感到满意，请单击 摘要以查看配置摘要。
9. 单击保存。新的交付组将显示在交 付组页面上。

向交付组添加策略

1. 在 资源（可选）列表中，单击 策略。
2. 对于要添加的每个策略，执行以下操作之一：
   - 滚动可用策略的列表以查找要添加的策略。或者，在搜索框中键入完整或部分策略名称，然后单击 “ 搜索”。
   - 将要添加的策略拖到右侧的框中。

   要从框中删除策略，请单击策略名称旁边的 **X** 。
3. 单击 下一步转到 应用程序页面。

将应用程序添加到交付组

1. 对于要添加的每个应用程序，执行以下操作之一：
   - 滚动可用应用程序的列表以查找要添加的应用程序。或者，在搜索框中键入完整或部分应用名称，然后单击 “ 搜索”。
   - 将应用程序拖动到 必需的应用程序框或 可选应用程序框中。

   对于标记为必填的应用，在以下情况下，用户可以立即接收更新：
   - 您上传了一个新应用程序并将其标记为必填。
   - 您将现有应用程序标记为必填。
   - 用户删除所需的应用程序。
   - Secure Hub 更新可用。

   有关强制部署必需应用程序的信息，包括如何启用该功能，请参阅 关于必需和可选应用程序。

   要从框中删除应用程序，请单击应用程序名称旁边的 **X** 。
2. 单击 “ 下一步” 转到 “ 媒体” 页面。

将媒体添加到交付组

1. 对于要添加的每本书籍，执行以下操作：
   - 滚动浏览可用书籍的列表以查找要添加的书籍。或者，在搜索框中键入完整或部分书名，然后单击 “ 搜索”。
   - 将要添加的图书拖到 必填书籍框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

对于标记为必填的电子书，在以下情况下，用户会立即收到更新：

- 您上传了一本新书并将其标记为必填。
- 您将现有电子书标记为必填。
- 用户删除了所需的电子书。
- Secure Hub 更新可用。

要从框中删除书籍，请单击图书名称旁边的 **X** 。

2. 单击 “ 下一步” 转到 “ 操作” 页面。

向交付组添加操作

1. 对于要添加的每个操作，执行以下操作：

   - 滚动可用操作的列表以查找要添加的操作。或者，在搜索框中键入完整或部分操作名称，然后单击 “ 搜索”。
   - 将要添加的动作拖动到右侧的框中。

   要从框中删除操作，请单击操作名称旁边的 **X** 。

2. 单击 下一步转到 **Content Collaboration** （以前称为 **ShareFile**）页面。

应用 **Content Collaboration** 配置

Content Collaboration 页面（以前称为 ShareFile）会有所不同，具体取决于您是为企业帐户还是为存储区域连接器配置了 **Endpoint Management**（配置 **> Content Collaboration**）。

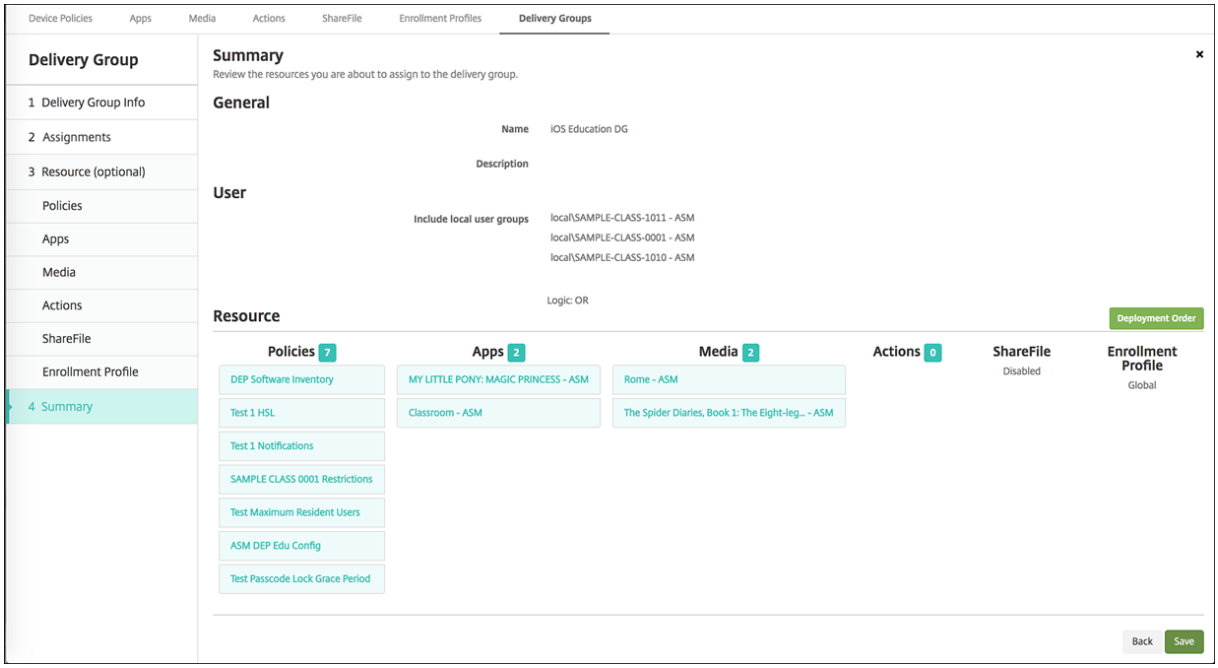
- 如果已将企业帐户配置为与 Endpoint Management 配合使用，请将 启用 **Content Collaboration** 设置为开。此设置为交付组提供对 Content Collaboration 内容和数据的单点登录访问权限。
- 如果已将存储区域连接器配置为与 Endpoint Management 结合使用，请将要包含在交付组中的存储区域连接器拖到右侧的框中。

检查已配置的选项并更改部署顺序

在摘要页面上，您可以查看为交付组配置的选项并更改资源的部署顺序。“摘要” 页面按类别显示您的资源。摘要页面不显示部署顺序。

> 注意：
>
> 单击上一步返回上一页更改配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



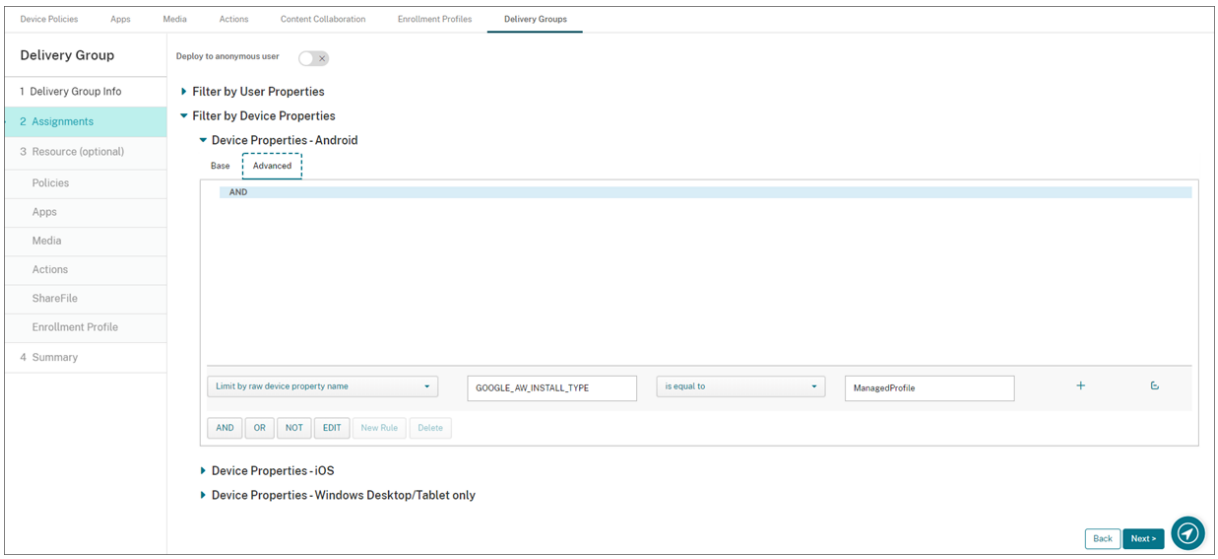
要查看或更改部署顺序：

1. 单击 部署顺序。
2. 在“部署顺序”对话框中，按照要部署的顺序将资源拖动到该位置。资源按自上而下的顺序部署。
3. 单击保存以保存部署顺序。

配置完交付组后，在摘要页面上，单击 保存。

创建将资源部署到 **Android Enterprise** 的规则

您可以使用 Android 设备属性规则管理将交付组部署到 Android Enterprise 设备。如果向同一用户注册多个设备，则可以根据设备注册模式或设备应用程序包 ID 为 Android Enterprise 创建高级筛选器。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要使用设备注册模式将交付组部署到 Android Enterprise 设备上：

1. 创建交付组。
2. 在 分配页面上，展开 按设备属性筛选。
3. 在 设备属性 **— Android** 中，打开 高级选项卡，然后单击 新规则。
4. 在列表中，选择要添加到规则的条件：
   - 对于新的 Android Enterprise 设备，请选择 “ 按原始设备属性名称限制”，然后在第一个值字段中 键入 **GOOGLE_AW_IN** STAL_TYPE。然后，您必须将条件设置为等于其中一种注册模式。
   - 对于现有 Android Enterprise 设备，请选择 按已知设备属性名称限制，然后在第一个值字段中选择 **Android Enterprise** 安装类型。然后，您必须将条件设置为等于其中一种注册模式。
5. 在第二个字段中，键入 Android Enterprise 设备的注册模式：
   - **DeviceAdministrator**：指定仅供工作使用的公司拥有的设备（也称为设备所有者模式）
   - **ManagedProfile**：指定 BYOD — 通过工作配置文件管理注册的个人设备（也称为配置文件所有者模式）
   - **CorporateOwnedSingleUse**：指定专用设备（以前称为企业拥有的一次性设备）
   - **CorporateOwnedPersonallyEnabled**：指定具有工作配置文件的完全托管设备（以前称为企业拥有、个人启用的设备）
6. 按照所述完成配置交付组添加交付组。

   有关更多信息，请参阅 设备部署方案和配置文件。

要使用设备应用程序包 ID 将交付组部署到 Android Enterprise 设备，请执行以下操作：

1. 在 设备属性 **— Android** 中，打开 高级选项卡，然后单击 新规则。
2. 在列表中，选择 已安装的应用程序名称，然后输入应用程序包 ID。

编辑交付组

不能更改现有交付组的名称。要更新其他设置，请转到 配置 **>** 交付组，选择要编辑的组，然后单击 编辑。

启用和禁用 **allUsers** 交付组

AllUsers 是唯一一个您可以启用或禁用的交付组。您无法像删除其他交付组那样删除所有用户。

在 交付组页面中，通过选中 AllUsers 旁边的复选框或单击包含 **AllUsers** 的行来选择 **AllUsers** 交付组。然后执行以下操作之一：

- 单击禁用可禁用 AllUsers 交付组。仅当启用了 allUsers 组（默认值）时，此命令才可用。禁用的交付组将显示在交付组表中的已禁用标题下方。
- 单击启用可启用 AllUsers 交付组。仅当禁用了 allUsers 组时，此命令才可用。已禁用不再显示在交付组表格中的 已禁用标题下。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

部署到交付组

部署到交付组意味着向所有使用 Apple、Android 和 Windows 平板电脑设备的用户发送推送通知。

对于使用其他平台设备的用户，如果这些设备已连接到 Endpoint Management，则他们会立即收到资源。否则，根据其计划策略，用户将在下次连接时收到资源。

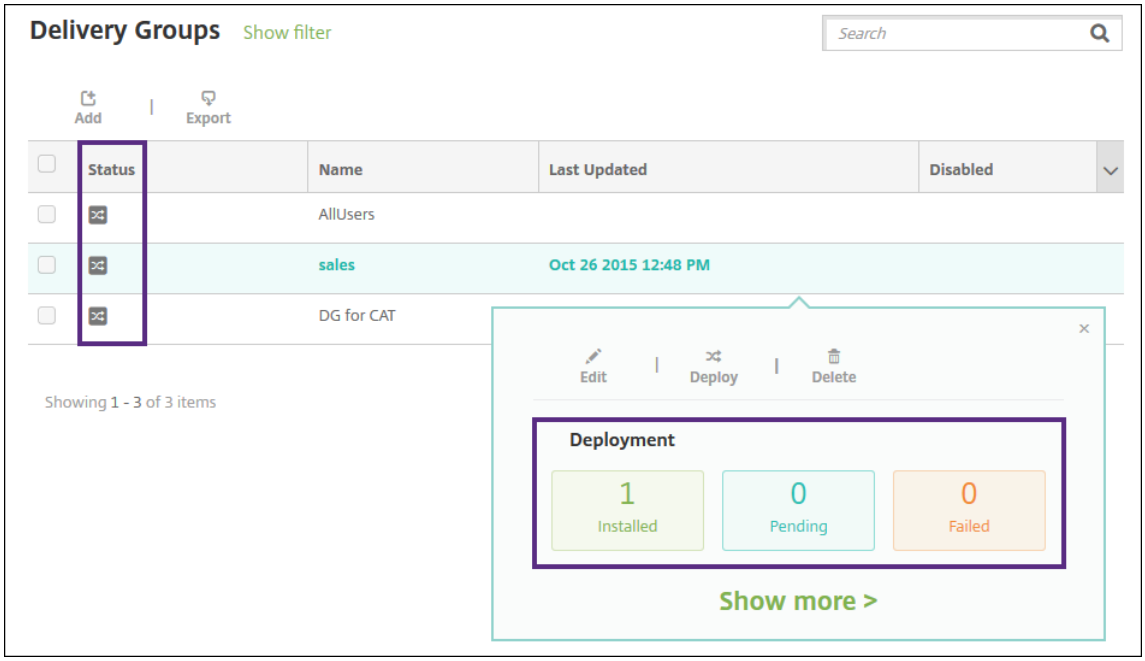
要使更新后的应用显示在 Android 设备上应用商店的“已更新的可用”列表中，请首先向用户设备部署应用清单策略。

1. 在交付组页面上，执行以下操作之一：
   - 要同时部署多个交付组，请选中要部署的组旁边的复选框。
   - 要部署单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。
2. 单击部署。

   根据您选择单个交付组的方式，部署命令将显示在交付组的上方或右侧。

   验证是否列出了要部署应用程序、策略和操作的组。然后单击“ 部署”。将根据设备平台和计划策略向选定的组部署应用程序、策略和操作。

   可以通过以下方式之一在交付组页面上检查部署状态。
   - 查看状态标题下方交付组的部署图标，此图标指示任何部署失败状态。
   - 单击包含交付组的行以显示显示 已安装、待定和 失败的部署的叠加层。



克隆交付组

如果要创建类似于现有交付组的交付组，请克隆交付组。使用克隆作为新交付组的起点。然后对克隆进行更改，例如添加注册配置文件或新的 AD 用户集。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在 Endpoint Management 控制台中，单击 配置，然后选择 交付组选项卡。
2. 从交付组列表中，选择要用作新组基础的交付组。
3. 选择 克隆。
4. 在克隆交付组对话框中，输入新组的名称以及描述（可选）。
5. 选择 克隆。

删除交付组

您无法删除 allUsers 交付组，但可以在不想向所有用户推送资源时将其禁用。请参阅启用和禁用 allUsers 交付组。

> 重要：
>
> 您不能撤消删除。

1. 在交付组页面上，执行以下操作之一：
   - 要同时删除多个交付组，请选中要删除的组旁边的复选框。
   - 要删除单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。
2. 单击删除。

   根据您选择单个交付组的方式，删除命令将显示在交付组的上方或右侧。
3. 在 “ 删除” 对话框中，单击 “ 删除”。

导出交付组表

1. 单击 交付组表格上方的 导出。Endpoint Management 提取交付组表中的信息，并将其转换为.csv 文件。
2. 按照您的浏览器的常规步骤打开或保存.csv 文件。

宏

November 7, 2022

Endpoint Management 阻止将宏作为在以下项目的文本字段中填充用户或设备属性数据的方式：

- 策略
- 通知
- 注册模板
- 设备配置 XML 文件
- 自动化操作
- 凭据提供程序证书签名请求

Endpoint Management 将宏替换为相应的用户或系统值。例如，可以为涵盖数千个用户的单个 Exchange 配置文件中的某个用户预填充邮箱值。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

宏语法

宏可以采用以下格式：

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] ] }`

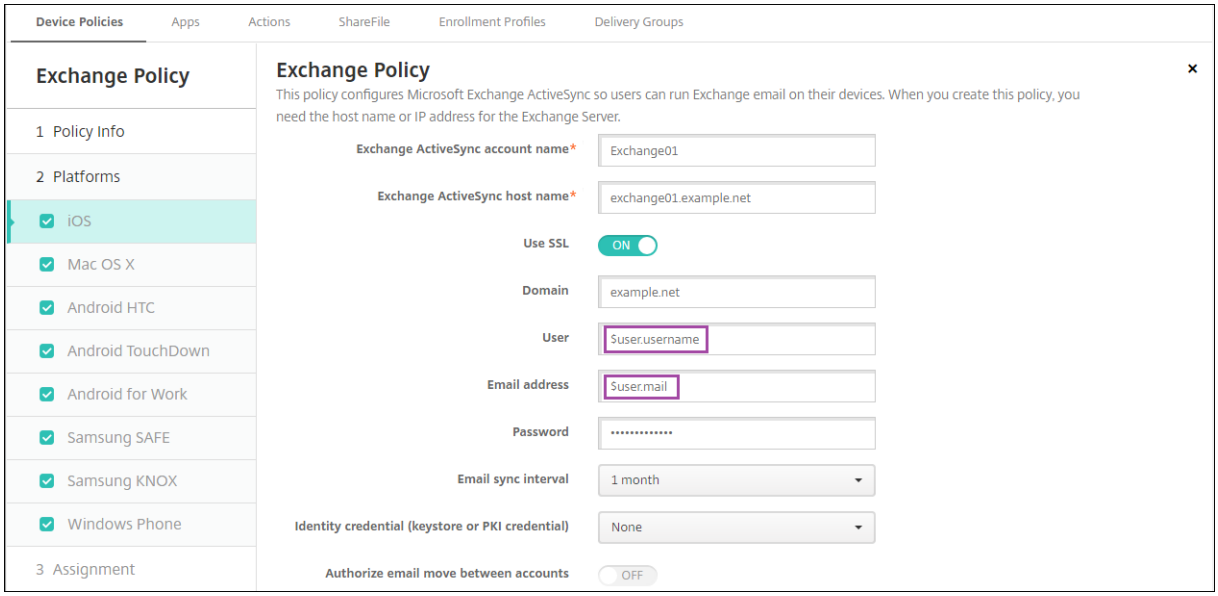
美元符号 ($) 后的所有语法以花括号 ({ }) 括起。

- 限定的属性名称是指用户属性、设备属性或自定义属性。
- 限定的属性名称包括一个前缀，后跟实际属性名称。
- 用户属性的格式为 `${ user.[PROPERTYNAME] (prefix="user.")}`。
- 设备属性的格式为 `${ device.[PROPERTYNAME] (prefix="device.")}`。
- 属性名称区分大小写。
- 函数可以是受限列表，或者指向用于定义函数的第三方引用的链接。适用于通知消息的以下宏包括函数 `firstnotnull`：

设备 `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 已被阻止...

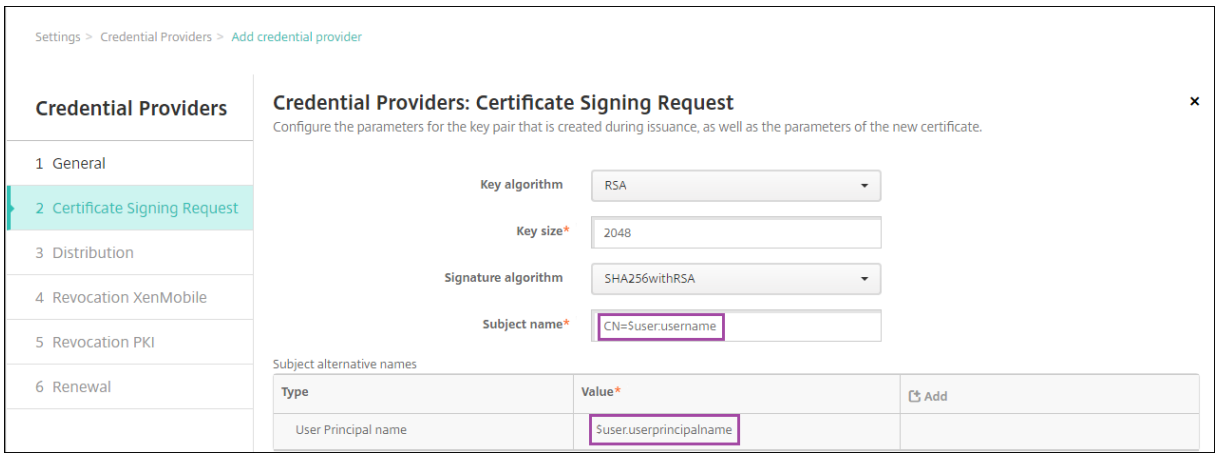
- 对于自定义宏（您定义的属性），前缀为 `${ custom }`。您可以忽略前缀。

下面是用于在策略的文本字段中填充用户名值的常用宏 `${ user.username }` 的示例。此宏在配置由多个用户使用的 Exchange ActiveSync 配置文件和其他配置文件时非常有用。以下示例显示了如何在 Exchange 策略中使用宏。适用于用户的宏为 `${ user.username }`。电子邮件地址的宏为 `${ user.mail }`。



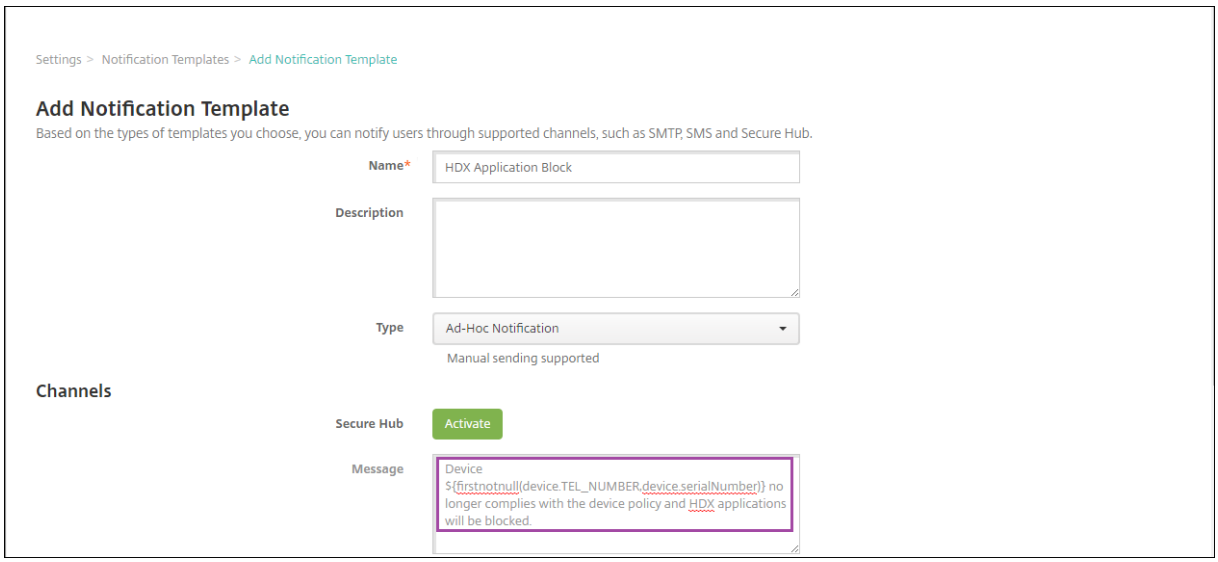
以下示例显示了如何为证书签名请求使用宏。适用于使用者名称的宏为 **CN=$user.username**。适用于使用者备用名称的值的宏为 **$user.userprincipalname**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



以下示例显示了如何在通知模板中使用宏。示例模板定义阻止 HDX 应用程序时由于不合规设备而向用户发送的消息。适用于消息的宏为：

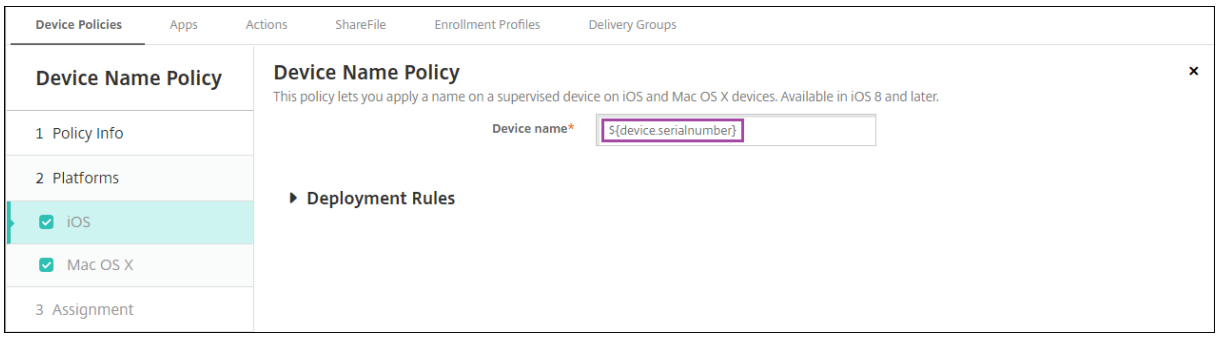
设备 `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 不再符合设备策略，HDX 应用程序将被阻止。



有关在通知中使用的宏的更多示例，请转至设置 > 通知模板，选择一个预定义的模板，然后单击编辑。

以下示例显示了“设备名称”设备策略中的宏。可以键入宏、宏的组合或宏和文本的组合，为每个设备设置唯一名称。例如，使用 `${ device.serialnumber }` 可将设备名称设置为每个设备的序列号。使用 `${ device.serialnumber } ${ user.username }` 可在设备名称中包含用户名。设备名称设备策略适用于受监督的 iOS 和 macOS 设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



适用于默认通知模板的宏

可以在默认通知模板中使用以下宏：

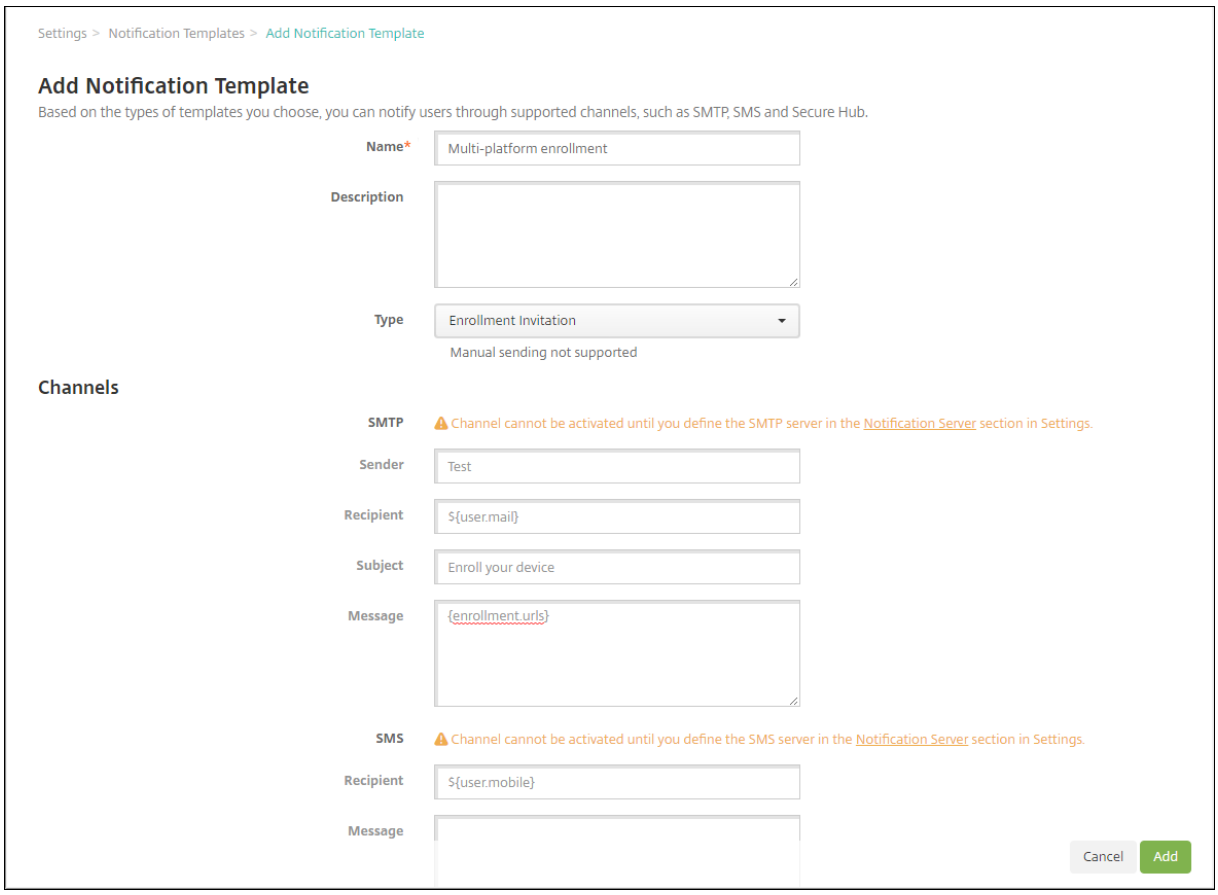
- ${ account.SUPPORT_EMAIL }
- ${ applicationName }
- ${ enrollment.andriod.agent.download.url }
- ${ enrollment.ios.agent.download.url }
- ${ enrollment.pin }
- ${ enrollment.url }
- ${ enrollment.urls }
- ${ enrollment.ios.url }
- ${ enrollment.macos.url }
- ${ enrollment.android.url }
- ${ enrollment.ios.platform }
- ${ enrollment.macos.platform }
- ${ enrollment.android.platform }
- ${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}
- ${ firstnotnull(device.TEL_NUMBER,user.mobile)}
- ${ outofcompliance.reason(smg_block)}
- ${ outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

> 注意：
>
> Endpoint Management 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

下例显示了如何创建包含适用于多个设备平台的注册 URL 的通知。适用于消息的宏为：

${enrollment.urls}

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



下面这些示例显示了如何为提示用户单击适用于其设备平台的注册 URL 的通知创建消息：

示例 1：

```
To enroll, click the link below that applies to your device platform:

${
 enrollment.ios.platform }
  - ${
 enrollment.ios.url }


${
 enrollment.macos.platform }
  - ${
 enrollment.macos.url }


${
 enrollment.android.platform }
  - ${
 enrollment.android.url }
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
19
20
21 <!--NeedCopy-->
```

示例 2：

```
1  To enroll an iOS device, click the link ${
2   enrollment.ios.url }
3   .
4
5  To enroll a macOS device, click the link ${
6   enrollment.macos.url }
7   .
8
9  To enroll an Android device, click the link ${
10  enrollment.android.url }
11  .
12
13 <!--NeedCopy-->
```

适用于特定策略的宏

对于设备名称设备策略（适用于 iOS 和 macOS），您可以使用以下宏作为 设备名称：

- ${ device.serialnumber }
- ${ user.username } @example.com
- ${ device.serialnumber }
- ${ device.serialnumber }
- ${ user.username }
- ${ enrollment.pin }
- ${ user.dnsroot }

对于手机网络设备策略（适用于 iOS），您可以将宏用于非字符串字段的值，例如代理服务器端口。例如，您现在可以使用 ${ device.xyz } 或 ${ setting.xyz } 等宏，这将扩展到整数。

对于使用“导入 iOS 和 macOS 配置文件”设备策略导入到 Endpoint Management 的设备配置 XML 文件，可以将宏用于非字符串字段的值。

对于 Samsung MDM 许可证密钥设备策略，您可以使用此宏作为 **ELM** 许可证密钥：

- ${ elm.license.key }

对于 Web 剪辑设备策略，可以对 **URL** 使用以下宏：

- ${ webeas-url }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用于获取内置设备属性的宏

显示名称	宏
设备 ID	`$device.id`
设备 GUID	`$device.uniqueid`
设备 IMEI	`$device.imei`
操作系统系列	`$device.OSFamily`
序列号	`$device.serialNumber`

适用于所有设备属性的宏

显示名称：帐户已暂停?

- **Web** 元素： `GOOGLE_AW_DIRECTORY_SUSPENDED`
- 宏： `${ device.GOOGLE_AW_DIRECTORY_SUSPENDED }`

显示名称：激活锁绕过码

- **Web** 元素： `ACTIVATION_LOCK_BYPASS_CODE`
- 宏： `${ device.ACTIVATION_LOCK_BYPASS_CODE }`

显示名称：已启用激活锁

- **Web** 元素： `ACTIVATION_LOCK_ENABLED`
- 宏： `${ device.ACTIVATION_LOCK_ENABLED }`

显示名称：处于活动状态的 Apple App Store 帐户

- **Web** 元素： `ACTIVE_ITUNES`
- 宏： `${ device.ACTIVE_ITUNES }`

显示名称：管理员已禁用

- **Web** 元素： `ADMIN_DISABLED`
- 宏： `${ device.ADMIN_DISABLED }`

显示名称： AIK 是否存在?

- **Web** 元素： `WINDOWS_HAS_AIK_PRESENT`
- 宏： `${ device.WINDOWS_HAS_AIK_PRESENT }`

显示名称： Amazon MDM API 可用

- **Web** 元素： `AMAZON_MDM`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.AMAZON_MDM }`

显示名称： Android Enterprise 设备 ID

- **Web** 元素：`GOOGLE_AW_DEVICE_ID`
- 宏：`${ device.GOOGLE_AW_DEVICE_ID }`

显示名称：启用了 Android Enterprise 的设备?

- **Web** 元素：`GOOGLE_AW_ENABLED_DEVICE`
- 宏：`${ device.GOOGLE_AW_ENABLED_DEVICE }`

显示名称： Android Enterprise 安装类型

- **Web** 元素：`GOOGLE_AW_INSTALL_TYPE`
- 宏：`${ device.GOOGLE_AW_INSTALL_TYPE }`

显示名称：反间谍软件签名状态

- **Web** 元素：`ANTI_SPYWARE_SIGNATURE_STATUS`
- 宏：`${ device.ANTI_SPYWARE_SIGNATURE_STATUS }`

显示名称：反间谍软件状态

- **Web** 元素：`ANTI_SPYWARE_STATUS`
- 宏：`${ device.ANTI_SPYWARE_STATUS }`

显示名称：防病毒软件签名状态

- **Web** 元素：`ANTI_VIRUS_SIGNATURE_STATUS`
- 宏：`${ device.ANTI_VIRUS_SIGNATURE_STATUS }`

显示名称：防病毒软件状态

- **Web** 元素：`ANTI_VIRUS_STATUS`
- 宏：`${ device.ANTI_VIRUS_STATUS }`

显示名称： ASM 部署计划激活锁绕过码

- **Web** 元素：`DEP_ACTIVATION_LOCK_BYPASS_CODE`
- 宏：`${ device.DEP_ACTIVATION_LOCK_BYPASS_CODE }`

显示名称： ASM 部署计划托管密钥

- **Web** 元素：`DEP_ESCROW_KEY`
- 宏：`${ device.DEP_ESCROW_KEY }`

显示名称：资产标签

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：ASSET_TAG
- 宏：${ device.ASSET_TAG }

显示名称：自动检查软件更新

- **Web** 元素：AutoCheckEnabled
- 宏：${ device.AutoCheckEnabled }

显示名称：自动在后台下载软件更新

- **Web** 元素：BackgroundDownloadEnabled
- 宏：${ device.BackgroundDownloadEnabled }

显示名称：自动安装应用程序更新

- **Web** 元素：AutomaticAppInstallationEnabled
- 宏：${ device.AutomaticAppInstallationEnabled }

显示名称：自动安装操作系统更新

- **Web** 元素：AutomaticOSInstallationEnabled
- 宏：${ device.AutomaticOSInstallationEnabled }

显示名称：自动安装安全更新

- **Web** 元素：AutomaticSecurityUpdatesEnabled
- 宏：${ device.AutomaticSecurityUpdatesEnabled }

显示名称：自动更新状态

- **Web** 元素：AUTOUPDATE_STATUS
- 宏：${ device.AUTOUPDATE_STATUS }

显示名称：可用 RAM

- **Web** 元素：MEMORY_AVAILABLE
- 宏：${ device.MEMORY_AVAILABLE }

显示名称：可用软件更新

- **Web** 元素：AVAILABLE_OS_UPDATE_HUMAN_READABLE
- 宏：${ device.AVAILABLE_OS_UPDATE_HUMAN_READABLE }

显示名称：可用存储空间

- **Web** 元素：FREEDISK
- 宏：${ device.FREEDISK }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称：备用电池

- **Web** 元素： `BACKUP_BATTERY_PERCENT`
- 宏： `${ device.BACKUP_BATTERY_PERCENT }`

显示名称：基带固件版本

- **Web** 元素： `MODEM_FIRMWARE_VERSION`
- 宏：‘${device.MODEM_FIRMWARE_VERSION}

显示名称：电池正在充电

- **Web** 元素： `BATTERY_CHARGING_STATUS`
- 宏： `${ device.BATTERY_CHARGING_STATUS }`

显示名称：电池正在充电

- **Web** 元素： `BATTERY_CHARGING`
- 宏： `${ device.BATTERY_CHARGING }`

显示名称：电池剩余电量

- **Web** 元素： `BATTERY_ESTIMATED_CHARGE_REMAINING`
- 宏： `${ device.BATTERY_ESTIMATED_CHARGE_REMAINING }`

显示名称：电池运行时

- **Web** 元素： `BATTERY_RUNTIME`
- 宏： `${ device.BATTERY_RUNTIME }`

显示名称：电池状态

- **Web** 元素： `BATTERY_STATUS`
- 宏： `${ device.BATTERY_STATUS }`

显示名称： BES PIN

- **Web** 元素： `BES_PIN`
- 宏： `${ device.BES_PIN }`

显示名称： BES 服务器代理 ID

- **Web** 元素： `AGENT_ID`
- 宏： `${ device.AGENT_ID }`

显示名称： BES 服务器名称

- **Web** 元素： `BES_SERVER`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.BES_SERVER }`

显示名称： BES 服务器版本

- **Web** 元素：`BES_VERSION`
- 宏：`${ device.BES_VERSION }`

显示名称： BIOS 信息

- **Web** 元素：`BIOS_INFO`
- 宏：`${ device.BIOS_INFO }`

显示名称： BitLocker 状态

- **Web** 元素：`WINDOWS_HAS_BIT_LOCKER_STATUS`
- 宏：`${ device.WINDOWS_HAS_BIT_LOCKER_STATUS }`

显示名称：蓝牙 MAC 地址

- **Web** 元素：`BLUETOOTH_MAC`
- 宏：`${ device.BLUETOOTH_MAC }`

显示名称：启动调试是否已启用?

- **Web** 元素：`WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- 宏：`${ device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED }`

显示名称：启动管理器修订列表版本

- **Web** 元素：`WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`
- 宏：`${ device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION }`

显示名称：运营商代码

- **Web** 元素：`CARRIER_CODE`
- 宏：`${ device.CARRIER_CODE }`

显示名称：运营商设置版本

- **Web** 元素：`CARRIER_SETTINGS_VERSION`
- 宏：`${ device.CARRIER_SETTINGS_VERSION }`

显示名称：目录 URL

- **Web** 元素：`CatalogURL`
- 宏：`${ device.CatalogURL }`

显示名称：手机网络高度

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：GPS_ALTITUDE_FROM_CELLULAR
- 宏：${ device.GPS_ALTITUDE_FROM_CELLULAR }

显示名称：手机网络路线

- **Web** 元素：GPS_COURSE_FROM_CELLULAR
- 宏：${ device.GPS_COURSE_FROM_CELLULAR }

显示名称：手机网络水平精度

- **Web** 元素：GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- 宏：${ device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR }

显示名称：手机网络纬度

- **Web** 元素：GPS_LATITUDE_FROM_CELLULAR
- 宏：${ device.GPS_LATITUDE_FROM_CELLULAR }

显示名称：手机网络经度

- **Web** 元素：GPS_LONGITUDE_FROM_CELLULAR
- 宏：${ device.GPS_LONGITUDE_FROM_CELLULAR }

显示名称：手机网络速度

- **Web** 元素：GPS_SPEED_FROM_CELLULAR
- 宏：${ device.GPS_SPEED_FROM_CELLULAR }

显示名称：手机网络技术

- **Web** 元素：CELLULAR_TECHNOLOGY
- 宏：${ device.CELLULAR_TECHNOLOGY }

显示名称：手机网络时间戳

- **Web** 元素：GPS_TIMESTAMP_FROM_CELLULAR
- 宏：${ device.GPS_TIMESTAMP_FROM_CELLULAR }

显示名称：手机网络垂直精度

- **Web** 元素：GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- 宏：${ device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR }

显示名称：下次登录时更改密码?

- **Web** 元素：GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- 宏：‘${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称：客户端设备 ID

- **Web** 元素：`CLIENT_DEVICE_ID`
- 宏：`${ device.CLIENT_DEVICE_ID }`

显示名称：已启用云备份

- **Web** 元素：`CLOUD_BACKUP_ENABLED`
- 宏：`${ device.CLOUD_BACKUP_ENABLED }`

显示名称：代码完整性是否已启用?

- **Web** 元素：`WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- 宏：`${ device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED }`

显示名称：代码完整性修订列表版本

- **Web** 元素：`WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- 宏：`${ device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION }`

显示名称：颜色

- **Web** 元素：`COLOR`
- 宏：`${ device.COLOR }`

显示名称： CPU 时钟速度

- **Web** 元素：`CPU_CLOCK_SPEED`
- 宏：`${ device.CPU_CLOCK_SPEED }`

显示名称： CPU 类型

- **Web** 元素：`CPU_TYPE`
- 宏：`${ device.CPU_TYPE }`

显示名称：创建时间

- **Web** 元素：`GOOGLE_AW_DIRECTORY_CREATION_TIME`
- 宏：`${ device.GOOGLE_AW_DIRECTORY_CREATION_TIME }`

显示名称：关键软件更新

- **Web** 元素：`AVAILABLE_OS_UPDATE_IS_CRITICAL`
- 宏：`${ device.AVAILABLE_OS_UPDATE_IS_CRITICAL }`

显示名称：当前运营商网络

- **Web** 元素：`CARRIER`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.CARRIER }`

显示名称：当前移动设备国家/地区代码

- **Web** 元素：`CURRENT_MCC`
- 宏：`${ device.CURRENT_MCC }`

显示名称：当前移动设备网络代码

- **Web** 元素：`CURRENT_MNC`
- 宏：`${ device.CURRENT_MNC }`

显示名称：允许数据漫游

- **Web** 元素：`DATA_ROAMING_ENABLED`
- 宏：`${ device.DATA_ROAMING_ENABLED }`

显示名称：最后一次 iCloud 备份日期

- **Web** 元素：`LAST_CLOUD_BACKUP_DATE`
- 宏：`${ device.LAST_CLOUD_BACKUP_DATE }`

显示名称：默认目录

- **Web** 元素：`IsDefaultCatalog`
- 宏：`${ device.IsDefaultCatalog }`

显示名称： Apple 部署计划帐户名称

- **Web** 元素：`BULK_ENROLLMENT_DEP_ACCOUNT_NAME`
- 宏：`${ device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME }`

显示名称： Apple 部署计划策略

- **Web** 元素：`WINDOWS_HAS_DEP_POLICY`
- 宏：`${ device.WINDOWS_HAS_DEP_POLICY }`

显示名称： Apple 部署计划配置文件已分配

- **Web** 元素：`PROFILE_ASSIGN_TIME`
- 宏：`${ device.PROFILE_ASSIGN_TIME }`

显示名称： Apple 部署计划配置文件已推送

- **Web** 元素：`PROFILE_PUSH_TIME`
- 宏：`${ device.PROFILE_PUSH_TIME }`

显示名称： Apple 部署计划配置文件已删除

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：`PROFILE_REMOVE_TIME`
- 宏：`${ device.PROFILE_REMOVE_TIME }`

显示名称： Apple 部署计划注册者

- **Web** 元素：`DEVICE_ASSIGNED_BY`
- 宏：`${ device.DEVICE_ASSIGNED_BY }`

显示名称： Apple 部署计划注册日期

- **Web** 元素：`DEVICE_ASSIGNED_DATE`
- 宏：`${ device.DEVICE_ASSIGNED_DATE }`

显示名称：说明

- **Web** 元素：`DESCRIPTION`
- 宏：`${ device.DESCRIPTION }`

显示名称：设备型号

- **Web** 元素：`SYSTEM_OEM`
- 宏：`${ device.SYSTEM_OEM }`

显示名称：设备名称

- **Web** 元素：`DEVICE_NAME`
- 宏：`${ device.DEVICE_NAME }`

显示名称：设备类型

- **Web** 元素：`DEVICE_TYPE`
- 宏：`${ device.DEVICE_TYPE }`

显示名称：已激活“请勿打扰”

- **Web** 元素：`DO_NOT_DISTURB`
- 宏：`${ device.DO_NOT_DISTURB }`

显示名称： ELAM 驱动程序是否已加载?

- **Web** 元素：`WINDOWS_HAS_ELAM_DRIVER_LOADED`
- 宏：`${ device.WINDOWS_HAS_ELAM_DRIVER_LOADED }`

显示名称：加密合规性

- **Web** 元素：`ENCRYPTION_COMPLIANCE`
- 宏：`${ device.ENCRYPTION_COMPLIANCE }`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称： ENROLLMENT_KEY_GENERATION_DATE

- **Web** 元素： ENROLLMENT_KEY_GENERATION_DATE
- 宏： ${ device.ENROLLMENT_KEY_GENERATION_DATE }

显示名称：企业 ID

- **Web** 元素： ENTERPRISEID
- 宏： ${ device.ENTERPRISEID }

显示名称：外部存储 1：可用空间

- **Web** 元素： EXTERNAL_STORAGE1_FREE_SPACE
- 宏： ${ device.EXTERNAL_STORAGE1_FREE_SPACE }

显示名称：外部存储 1：可用空间

- **Web** 元素： EXTERNAL_STORAGE1_FREE_SPACE
- 宏： ${ device.EXTERNAL_STORAGE1_FREE_SPACE }

显示名称：外部存储器 1：名称

- **Web** 元素： EXTERNAL_STORAGE1_NAME
- 宏： ${ device.EXTERNAL_STORAGE1_NAME }

显示名称：外部存储 1：总空间

- **Web** 元素： EXTERNAL_STORAGE1_TOTAL_SPACE
- 宏： ${ device.EXTERNAL_STORAGE1_TOTAL_SPACE }

显示名称：外部存储 2：可用空间

- **Web** 元素： EXTERNAL_STORAGE2_FREE_SPACE
- **Macros:** ${ device.EXTERNAL_STORAGE2_FREE_SPACE }

显示名称：外部存储器 2：名称

- **Web** 元素： EXTERNAL_STORAGE2_NAME
- 宏： ${ device.EXTERNAL_STORAGE2_NAME }

显示名称：外部存储 2：总空间

- **Web** 元素： EXTERNAL_STORAGE2_TOTAL_SPACE
- 宏： ${ device.EXTERNAL_STORAGE2_TOTAL_SPACE }

显示名称：已加密外部存储

- **Web** 元素： EXTERNAL_ENCRYPTION

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.EXTERNAL_ENCRYPTION }`

显示名称：已启用 FileVault

- **Web** 元素：`IS_FILEVAULT_ENABLED`
- 宏：`${ device.IS_FILEVAULT_ENABLED }`

显示名称：防火墙状态

- **Web** 元素：`DEVICE_FIREWALL_STATUS`
- 宏：`${ device.DEVICE_FIREWALL_STATUS }`

显示名称：防火墙状态

- **Web** 元素：`DEVICE_FIREWALL_STATUS`
- 宏：`${ device.DEVICE_FIREWALL_STATUS }`

显示名称：防火墙状态

- **Web** 元素：`FIREWALL_STATUS`
- 宏：`${ device.FIREWALL_STATUS }`

显示名称：固件版本

- **Web** 元素：`FIRMWARE_VERSION`
- 宏：`${ device.FIRMWARE_VERSION }`

显示名称：首次同步

- **Web** 元素：`ZMSP_FIRST_SYNC`
- 宏：`${ device.ZMSP_FIRST_SYNC }`

显示名称： Google Directory 别名

- **Web** 元素：`GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- 宏：`${ device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS }`

显示名称： Google Directory 系列名称

- **Web** 元素：`GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- 宏：`${ device.GOOGLE_AW_DIRECTORY_FAMILY_NAME }`

显示名称： Google Directory 名称

- **Web** 元素：`GOOGLE_AW_DIRECTORY_NAME`
- 宏：`${ device.GOOGLE_AW_DIRECTORY_NAME }`

显示名称： Google Directory 主电子邮件

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：GOOGLE_AW_DIRECTORY_PRIMARY
- 宏：${ device.GOOGLE_AW_DIRECTORY_PRIMARY }

显示名称：Google Directory 别名

- **Web** 元素：GOOGLE_AW_DIRECTORY_USER_ID
- 宏：${ device.GOOGLE_AW_DIRECTORY_USER_ID }

显示名称：GPS 高度

- **Web** 元素：GPS_ALTITUDE_FROM_GPS
- 宏：${ device.GPS_ALTITUDE_FROM_GPS }

显示名称：GPS 路线

- **Web** 元素：GPS_COURSE_FROM_GPS
- 宏：${ device.GPS_COURSE_FROM_GPS }

显示名称：GPS 水平精度

- **Web** 元素：GPS_HORIZONTAL_ACCURACY_FROM_GPS
- 宏：${ device.GPS_HORIZONTAL_ACCURACY_FROM_GPS }

显示名称：GPS 纬度

- **Web** 元素：GPS_LATITUDE_FROM_GPS
- 宏：${ device.GPS_LATITUDE_FROM_GPS }

显示名称：GPS 经度

- **Web** 元素：GPS_LONGITUDE_FROM_GPS
- 宏：${ device.GPS_LONGITUDE_FROM_GPS }

显示名称：GPS 速度

- **Web** 元素：GPS_SPEED_FROM_GPS
- 宏：${ device.GPS_SPEED_FROM_GPS }

显示名称：GPS 时间戳

- **Web** 元素：GPS_TIMESTAMP_FROM_GPS
- 宏：${ device.GPS_TIMESTAMP_FROM_GPS }

显示名称：GPS 垂直精度

- **Web** 元素：GPS_VERTICAL_ACCURACY_FROM_GPS
- 宏：${ device.GPS_VERTICAL_ACCURACY_FROM_GPS }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称：硬件设备 ID

- **Web** 元素：`HW_DEVICE_ID`
- 宏：`${ device.HW_DEVICE_ID }`

显示名称：硬件加密功能

- **Web** 元素：`HARDWARE_ENCRYPTION_CAPS`
- 宏：`${ device.HARDWARE_ENCRYPTION_CAPS }`

显示名称：HAS_CONTAINER

- **Web** 元素：`HAS_CONTAINER`
- 宏：`${ device.HAS_CONTAINER }`

显示名称：当前登录的 Apple App Store 帐户的哈希值

- **Web** 元素：`ITUNES_STORE_ACCOUNT_HASH`
- 宏：`${ device.ITUNES_STORE_ACCOUNT_HASH }`

显示名称：家用运营商网络

- **Web** 元素：`SIM_CARRIER_NETWORK`
- 宏：`${ device.SIM_CARRIER_NETWORK }`

显示名称：家庭移动设备国家/地区代码

- **Web** 元素：`SIM_MCC`
- 宏：`${ device.SIM_MCC }`

显示名称：家庭移动设备网络代码

- **Web** 元素：`SIM_MNC`
- 宏：`${ device.SIM_MNC }`

显示名称：ICCID

- **Web** 元素：`ICCID`
- 宏：`${ device.ICCID }`

显示名称：标识

- **Web** 元素：`AS_DEVICE_IDENTITY`
- 宏：`${ device.AS_DEVICE_IDENTITY }`

显示名称：IMEI/MEID 编号

- **Web** 元素：`IMEI`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.IMEI }`

显示名称：IMSI

- **Web** 元素：`SIM_ID`
- 宏：`${ device.SIM_ID }`

显示名称：已加密内部存储

- **Web** 元素：`LOCAL_ENCRYPTION`
- 宏：`${ device.LOCAL_ENCRYPTION }`

显示名称：IP 位置

- **Web** 元素：`IP_LOCATION`
- 宏：`${ device.IP_LOCATION }`

显示名称：IPV4 地址

- **Web** 元素：`IP_ADDRESSV4`
- 宏：`${ device.IP_ADDRESSV4 }`

显示名称：IPv6 地址

- **Web** 元素：`IP_ADDRESSV6`
- 宏：`${ device.IP_ADDRESSV6 }`

显示名称：颁发时间

- **Web** 元素：`WINDOWS_HAS_ISSUED_AT`
- 宏：`${ device.WINDOWS_HAS_ISSUED_AT }`

显示名称：已越狱/获得 Root 权限

- **Web** 元素：`ROOT_ACCESS`
- 宏：`${ device.ROOT_ACCESS }`

显示名称：启动调试是否已启用?

- **Web** 元素：`WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- 宏：`${ device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED }`

显示名称：展台模式

- **Web** 元素：`IS_KIOSK`
- 宏：`${ device.IS_KIOSK }`

显示名称：上次已知 IP 地址

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：LAST_IP_ADDR
- 宏：${ device.LAST_IP_ADDR }

显示名称：上次策略更新时间

- **Web** 元素：LAST_POLICY_UPDATE_TIME
- 宏：${ device.LAST_POLICY_UPDATE_TIME }

显示名称：上次扫描日期

- **Web** 元素：PreviousScanDate
- 宏：${ device.PreviousScanDate }

显示名称：上次扫描结果

- **Web** 元素：PreviousScanResult
- 宏：${ device.PreviousScanResult }

显示名称：上次安排的软件更新

- **Web** 元素：AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- 宏：${ device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME }

显示名称：上次安排的软件更新失败消息

- **Web** 元素：AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- 宏：${ device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG }

显示名称：上次安排的软件更新状态

- **Web** 元素：AVAILABLE_OS_UPDATE_INSTALL_STATUS
- 宏：${ device.AVAILABLE_OS_UPDATE_INSTALL_STATUS }

显示名称：上次同步

- **Web** 元素：ZMSP_LAST_SYNC
- 宏：${ device.ZMSP_LAST_SYNC }

显示名称：已启用定位器服务

- **Web** 元素：DEVICE_LOCATOR
- 宏：${ device.DEVICE_LOCATOR }

显示名称： MAC 地址

- **Web** 元素：MAC_ADDRESS
- 宏：${ device.MAC_ADDRESS }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称： MAC 地址网络连接

- **Web** 元素： MAC_NETWORK_CONNECTION
- 宏： ${ device.MAC_NETWORK_CONNECTION }

显示名称： MAC 地址类型

- **Web** 元素： MAC_ADDRESS_TYPE
- 宏： ${ device.MAC_ADDRESS_TYPE }

显示名称：邮箱设置

- **Web** 元素： GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- 宏： ${ device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP }

显示名称：主电池

- **Web** 元素： MAIN_BATTERY_PERCENT
- 宏： ${ device.MAIN_BATTERY_PERCENT }

显示名称：已启用 MDM 丢失模式

- **Web** 元素： IS_MDM_LOST_MODE_ENABLED
- 宏： ${ device.IS_MDM_LOST_MODE_ENABLED }

显示名称： MDX_SHARED_ENCRYPTION_KEY

- **Web** 元素： MDX_SHARED_ENCRYPTION_KEY
- 宏： ${ device.MDX_SHARED_ENCRYPTION_KEY }

显示名称： MEID

- **Web** 元素： MEID
- 宏： ${ device.MEID }

显示名称：移动电话号码

- **Web** 元素： TEL_NUMBER
- 宏： ${ device.TEL_NUMBER }

显示名称：型号 ID

- **Web** 元素： MODEL_ID
- 宏： ${ device.MODEL_ID }

显示名称：型号

- **Web** 元素： MODEL_NUMBER

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.MODEL_NUMBER }`

显示名称：网络适配器类型

- **Web** 元素：`NETWORK_ADAPTER_TYPE`
- 宏：`${ device.NETWORK_ADAPTER_TYPE }`

显示名称：操作系统内部版本号

- **Web** 元素：`SYSTEM_OS_BUILD`
- 宏：`${ device.SYSTEM_OS_BUILD }`

显示名称：操作系统版本

- **Web** 元素：`OS_EDITION`
- 宏：`${ device.OS_EDITION }`

显示名称：操作系统语言（区域设置）

- **Web** 元素：`SYSTEM_LANGUAGE`
- 宏：`${ device.SYSTEM_LANGUAGE }`

显示名称：操作系统版本

- **Web** 元素：`SYSTEM_OS_VERSION`
- 宏：`${ device.SYSTEM_OS_VERSION }`

显示名称：组织地址

- **Web** 元素：`ORGANIZATION_ADDRESS`
- 宏：`${ device.ORGANIZATION_ADDRESS }`

显示名称：组织电子邮件

- **Web** 元素：`ORGANIZATION_EMAIL`
- 宏：`${ device.ORGANIZATION_EMAIL }`

显示名称：组织魔术字

- **Web** 元素：`ORGANIZATION_MAGIC`
- 宏：`${ device.ORGANIZATION_MAGIC }`

显示名称：组织名称

- **Web** 元素：`ORGANIZATION_NAME`
- 宏：`${ device.ORGANIZATION_NAME }`

显示名称：组织电话号码

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：ORGANIZATION_PHONE
- 宏：${ device.ORGANIZATION_PHONE }

‘显示名称：不合规

- **Web** 元素：OUT_OF_COMPLIANCE
- 宏：${ device.OUT_OF_COMPLIANCE }

显示名称：所有者

- **Web** 元素：CORPORATE_OWNED
- 宏：${ device.CORPORATE_OWNED }

显示名称：通行码合规性

- **Web** 元素：PASSCODE_IS_COMPLIANT
- 宏：${ device.PASSCODE_IS_COMPLIANT }

显示名称：通行码遵从配置

- **Web** 元素：PASSCODE_IS_COMPLIANT_WITH_CFG
- 宏：${ device.PASSCODE_IS_COMPLIANT_WITH_CFG }

显示名称：存在通行码

- **Web** 元素：PASSCODE_PRESENT
- 宏：${ device.PASSCODE_PRESENT }

显示名称： PCR0

- **Web** 元素：WINDOWS_HAS_PCR0
- 宏：${ device.WINDOWS_HAS_PCR0 }

显示名称：超出边界

- **Web** 元素：GPS_PERIMETER_BREACH
- 宏：${ device.GPS_PERIMETER_BREACH }

显示名称：定期检查

- **Web** 元素：PerformPeriodicCheck
- 宏：${ device.PerformPeriodicCheck }

显示名称：已激活个人热点

- **Web** 元素：PERSONAL_HOTSPOT_ENABLED
- 宏：${ device.PERSONAL_HOTSPOT_ENABLED }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称：地理围栏的 PIN 码

- **Web** 元素：`PIN_CODE_FOR_GEO_FENCE`
- 宏：`${ device.PIN_CODE_FOR_GEO_FENCE }`

显示名称：平台

- **Web** 元素：`SYSTEM_PLATFORM`
- 宏：`${ device.SYSTEM_PLATFORM }`

显示名称：平台 API 级别

- **Web** 元素：`API_LEVEL`
- 宏：`${ device.API_LEVEL }`

显示名称：策略名称

- **Web** 元素：`POLICY_NAME`
- 宏：`${ device.POLICY_NAME }`

显示名称：主电话号码

- **Web** 元素：`IDENTITY1_PHONENUMBER`
- 宏：`${ device.IDENTITY1_PHONENUMBER }`

显示名称：主 SIM 卡运营商

- **Web** 元素：`IDENTITY1_CARRIER_NETWORK_OPERATOR`
- 宏：`${ device.IDENTITY1_CARRIER_NETWORK_OPERATOR }`

显示名称：主 SIM 卡 ICCID

- **Web** 元素：`IDENTITY1_ICCID`
- 宏：`${ device.IDENTITY1_ICCID }`

显示名称：主 SIM 卡 IMEI

- **Web** 元素：`IDENTITY1_IMEI`
- 宏：`${ device.IDENTITY1_IMEI }`

显示名称：主 SIM 卡 IMSI

- **Web** 元素：`IDENTITY1_IMSI`
- 宏：`${ device.IDENTITY1_IMSI }`

显示名称：主 SIM 卡漫游

- **Web** 元素：`IDENTITY1_ROAMING`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.IDENTITY1_ROAMING }`

显示名称：主 SIM 卡漫游

- **Web** 元素：`IDENTITY1_ROAMING_COMPLIANCE`
- 宏：`${ device.IDENTITY1_ROAMING_COMPLIANCE }`

显示名称：产品名称

- **Web** 元素：`PRODUCT_NAME`
- 宏：`${ device.PRODUCT_NAME }`

显示名称：发布者设备 ID

- **Web** 元素：`PUBLISHER_DEVICE_ID`
- 宏：`${ device.PUBLISHER_DEVICE_ID }`

显示名称：重置计数

- **Web** 元素：`WINDOWS_HAS_RESET_COUNT`
- 宏：`${ device.WINDOWS_HAS_RESET_COUNT }`

显示名称：重新启动计数

- **Web** 元素：`WINDOWS_HAS_RESTART_COUNT`
- 宏：`${ device.WINDOWS_HAS_RESTART_COUNT }`

显示名称：安全模式是否已启用?

- **Web** 元素：`WINDOWS_HAS_SAFE_MODE`
- 宏：`${ device.WINDOWS_HAS_SAFE_MODE }`

显示名称： SBCP 哈希

- **Web** 元素：`WINDOWS_HAS_SBCP_HASH`
- 宏：`${ device.WINDOWS_HAS_SBCP_HASH }`

显示名称：屏幕: 高度

- **Web** 元素：`SCREEN_HEIGHT`
- 宏：`${ device.SCREEN_HEIGHT }`

显示名称：屏幕：颜色数量

- **Web** 元素：`SCREEN_NB_COLORS`
- 宏：`${ device.SCREEN_NB_COLORS }`

显示名称：屏幕: 大小

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：SCREEN_SIZE
- 宏：${ device.SCREEN_SIZE }

显示名称：屏幕: 宽度

- **Web** 元素：SCREEN_WIDTH
- 宏：${ device.SCREEN_WIDTH }

显示名称：屏幕：X 轴分辨率

- **Web** 元素：SCREEN_XDPI
- 宏：${ device.SCREEN_XDPI }

显示名称：屏幕：Y 轴分辨率

- **Web** 元素：SCREEN_YDPI
- 宏：${ device.SCREEN_YDPI }

显示名称：辅助电话号码

- **Web** 元素：IDENTITY2_PHONENUMBER
- 宏：${ device.IDENTITY2_PHONENUMBER }

显示名称：辅助 SIM 卡运营商

- **Web** 元素：IDENTITY2_CARRIER_NETWORK_OPERATOR
- 宏：${ device.IDENTITY2_CARRIER_NETWORK_OPERATOR }

显示名称：辅助 SIM 卡 ICCID

- **Web** 元素：IDENTITY2_ICCID
- 宏：${ device.IDENTITY2_ICCID }

显示名称：备选 SIM 卡 IMEI

- **Web** 元素：IDENTITY2_IMEI
- 宏：${ device.IDENTITY2_IMEI }

显示名称：备选 SIM 卡 IMSI

- **Web** 元素：IDENTITY2_IMSI
- 宏：${ device.IDENTITY2_IMSI }

显示名称：主 SIM 卡漫游

- **Web** 元素：IDENTITY2_ROAMING
- 宏：${ device.IDENTITY2_ROAMING }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称：辅助 SIM 卡漫游合规性

- **Web** 元素：`IDENTITY2_ROAMING_COMPLIANCE`
- 宏：`${ device.IDENTITY2_ROAMING_COMPLIANCE }`

显示名称：安全启动是否已启用?

- **Web** 元素：`WINDOWS_HAS_SECURE_BOOT_ENABLED`
- 宏：`${ device.WINDOWS_HAS_SECURE_BOOT_ENABLED }`

显示名称：安全启动状态

- **Web** 元素：`SECURE_BOOT_STATE`
- 宏：`${ device.SECURE_BOOT_STATE }`

显示名称：已启用 SecureContainer

- **Web** 元素：`DLP_ACTIVE`
- 宏：`${ device.DLP_ACTIVE }`

显示名称：安全修补级别

- **Web** 元素：`SYSTEM_SECURITY_PATCH_LEVEL`
- 宏：`${ device.SYSTEM_SECURITY_PATCH_LEVEL }`

显示名称：序列号

- **Web** 元素：`SERIAL_NUMBER`
- 宏：`${ device.SERIAL_NUMBER }`

显示名称：支持 SMS 功能

- **Web** 元素：`IS_SMS_CAPABLE`
- 宏：`${ device.IS_SMS_CAPABLE }`

显示名称：受监督

- **Web** 元素：`SUPERVISED`
- 宏：`${ device.SUPERVISED }`

显示名称：暂停原因

- **Web** 元素：`GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- 宏：`${ device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON }`

显示名称：状态被篡改

- **Web** 元素：`TAMPERED_STATUS`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 宏：`${ device.TAMPERED_STATUS }`

显示名称：条款和条件

- **Web** 元素：`TERMS_AND_CONDITIONS`
- 宏：`${ device.TERMS_AND_CONDITIONS }`

显示名称：已接受条款和协议?

- **Web** 元素：`GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- 宏：`${ device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS }`

显示名称：测试签名是否已启用?

- **Web** 元素：`WINDOWS_HAS_TEST_SIGNING_ENABLED`
- 宏：`${ device.WINDOWS_HAS_TEST_SIGNING_ENABLED }`

显示名称：总 RAM

- **Web** 元素：`MEMORY`
- 宏：`${ device.MEMORY }`

显示名称：总存储空间

- **Web** 元素：`TOTAL_DISK_SPACE`
- 宏：`${ device.TOTAL_DISK_SPACE }`

显示名称： TPM 版本

- **Web** 元素：`TPM_VERSION`
- 宏：`${ device.TPM_VERSION }`

显示名称： UDID

- **Web** 元素：`UDID`
- 宏：`${ device.UDID }`

显示名称：用户帐户控制状态

- **Web** 元素：`UAC_STATUS`
- 宏：`${ device.UAC_STATUS }`

显示名称：用户代理

- **Web** 元素：`USER_AGENT`
- 宏：`${ device.USER_AGENT }`

显示名称：用户定义的 #1

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Web** 元素：`USER_DEFINED_1`
- 宏：`${ device.USER_DEFINED_1 }`

显示名称：用户定义的 #2

- **Web** 元素：`USER_DEFINED_2`
- 宏：`${ device.USER_DEFINED_2 }`

显示名称：用户定义的 #3

- **Web** 元素：`USER_DEFINED_3`
- 宏：`${ device.USER_DEFINED_3 }`

显示名称：用户语言 (区域设置)

- **Web** 元素：`USER_LANGUAGE`
- 宏：`${ device.USER_LANGUAGE }`

显示名称：供应商

- **Web** 元素：`VENDOR`
- 宏：`${ device.VENDOR }`

显示名称：支持语音功能

- **Web** 元素：`IS_VOICE_CAPABLE`
- 宏：`${ device.IS_VOICE_CAPABLE }`

显示名称：允许语音漫游

- **Web** 元素：`VOICE_ROAMING_ENABLED`
- 宏：`${ device.VOICE_ROAMING_ENABLED }`

显示名称：VSM 是否已启用?

- **Web** 元素：`WINDOWS_HAS_VSM_ENABLED`
- 宏：`${ device.WINDOWS_HAS_VSM_ENABLED }`

显示名称：Wi-Fi MAC 地址

- **Web** 元素：`WIFI_MAC`
- 宏：`${ device.WIFI_MAC }`

显示名称：WINDOWS_ENROLLMENT_KEY

- **Web** 元素：`WINDOWS_ENROLLMENT_KEY`
- 宏：`${ device.WINDOWS_ENROLLMENT_KEY }`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称： WinPE 是否已启用?

- **Web** 元素： `WINDOWS_HAS_WINPE`
- 宏： `${ device.WINDOWS_HAS_WINPE }`

显示名称： WNS 通知状态

- **Web** 元素： `PROPERTY_WNS_PUSH_STATUS`
- 宏： `${ device.PROPERTY_WNS_PUSH_STATUS }`

显示名称： WNS 通知 URL

- **Web** 元素： `PROPERTY_WNS_PUSH_URL`
- 宏： `${ device.PROPERTY_WNS_PUSH_URL }`

显示名称： WNS 通知 URL 过期日期

- **Web** 元素： `PROPERTY_WNS_PUSH_URL_EXPIRY`
- 宏： `${ device.PROPERTY_WNS_PUSH_URL_EXPIRY }`

显示名称： Endpoint Management 代理 ID

- **Web** 元素： `ENROLLMENT_AGENT_ID`
- 宏： {device.ENROLLMENT_AGENT_ID}‘

显示名称： Endpoint Management 代理修订版

- **Web** 元素： `EW_REVISION`
- 宏： `${ device.EW_REVISION }`

显示名称： Endpoint Management 代理版本

- **Web** 元素： `EW_VERSION`
- 宏： `${ device.EW_VERSION }`

显示名称： Zebra API 可用

- **Web** 元素： `ZEBRA_MDM`
- 宏： `${ device.ZEBRA_MDM }`

显示名称： Zebra MXMF 版本

- **Web** 元素： `ZEBRA_MDM_VERSION`
- 宏： `${ device.ZEBRA_MDM_VERSION }`

显示名称： Zebra Patch 版本

- **Web** 元素： `ZEBRA_PATCH_VERSION`
- 宏： `${ device.ZEBRA_PATCH_VERSION }`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用于获取内置用户属性的宏

显示名称	宏
domainname（域名；默认域）	${ user.domainname }
loginname（用户名加域名）	${ user.loginname }
username（如有，则为登录名去掉域）	${ user.username }

适用于所有用户属性的宏

显示名称	**Web** 元素	宏
Active Directory 失败登录尝试次数	badpwdcount	${ user.badpwdcount }
ActiveSync 用户电子邮件	asuseremail	${ user.asuseremail }
ASM 数据源	asmpersonsource	${ user.asmpersonsource }
ASM 部署计划帐户名称	asmdepaccount	${ user.asmdepaccount }
ASM 管理式 Apple ID	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
ASM 通行码类型	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ASM 人员 ID	asmpersonid	${ user.asmpersonid }
ASM 人员状态	asmpersonstatus	${ user.asmpersonstatus }
ASM 人员职称	asmpersontitle	${ user.asmpersontitle }
ASM 人员的唯一 ID	asmpersonuniqueid	${ user.asmpersonuniqueid }
ASM 源系统 ID	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
ASM 学生年级	asmpersongrade	${ user.asmpersongrade }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称	**Web** 元素	宏
BES 用户电子邮件	besuseremail	${ user.besuseremail }
公司	company	${ user.company }
公司名称	companyname	${ user.companyname }
国家/地区	c	${ user.c }
部门	department	${ user.department }
说明	description	${ user.description }
禁用的用户	disableduser	${ user.disableduser }
显示名称	displayname	${ user.displayname }
标识名	distinguishedname	${ user.distinguishedname }
域名	domainname	${ user.domainname }
电子邮件	mail	${ user.mail }
名字	givenname	${ user.givenname }
家庭住址	homestreetaddress	${ user.homestreetaddress }
居住城市	homecity	${ user.homecity }
居住国家/地区	homecountry	${ user.homecountry }
住宅传真	homefax	${ user.homefax }
住宅电话	homephone	${ user.homephone }
居住州/省/自治区/直辖市/地区	homestate	${ user.homestate }
住宅邮政编码	homezip	${ user.homezip }
IP 电话	ipphone	${ user.ipphone }
中间名首字母	middleinitial	${ user.middleinitial }
中间名	middlename	${ user.middlename }
移动	mobile	${ user.mobile }
名称	cn	${ user.cn }
办公室地址	physicaldeliveryofficena	${ user.physicaldeliveryofficename }

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

显示名称	**Web** 元素	宏
办公室所在城市	l	${ user.l }
办公室传真号码	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
办公室所在州/省/自治区/直辖市	st	${ user.st }
办公室所在街道地址	officestreetaddress	${ user.officestreetaddress }
办公室电话号码	telephonenumber	${ user.telephonenumber }
办公室所在地邮政编码	postalcode	${ user.postalcode }
邮箱	postofficebox	${ user.postofficebox }
寻呼机	pager	${ user.pager }
主组 ID	primarygroupid	${ user.primarygroupid }
SAM 帐户	samaccountname	${ user.samaccountname }
街道地址	streetaddress	${ user.streetaddress }
姓氏	sn	${ user.sn }
标题	title	${ user.title }
用户登录名	userprincipalname	${ user.userprincipalname }

自动化操作

July 24, 2023

可以在 Endpoint Management 中创建自动操作，以对以下内容的响应进行编程：

- 事件
- 用户或设备属性
- 用户设备上存在应用程序

创建自动化操作时，针对操作定义的触发器确定在用户设备连接到 Endpoint Management 时进行的操作。触发事件

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

后，您可以在采取更实质性的操作之前向用户发送通知以更正问题。

设置为自动出现的影响范围如下：

- 完全或选择性地擦除设备。
- 将设备设置为不合规。
- 吊销设备。
- 在采取更严重的操作之前，向用户发送通知以更正问题。

可以为仅 MAM 模式配置应用程序锁定和应用程序擦除操作。

你可以使用自动操作在 Azure AD 中将加入 Azure Active Directory (AD) 的 Windows 10 和 Windows 11 设备标记为不合规。

> 注意：
>
> 在通知用户之前，您必须在 Endpoint Management 设置中为 SMTP 配置通知服务器，以便 Endpoint Management 可以发送消息。有关信息，请参阅通知。此外，请在继续操作前设置计划使用的通知模板。有关详细信息，请参阅 创建和更新通知模板。

示例操作

下面是使用自动化操作的一些示例：

示例一

- 您要检测先前阻止的应用程序（例如，“Words with Friends”）。可以指定一个触发器，用于在检测到 “Words with Friends” 应用程序时，将用户设备设置为不合规。然后，该操作向用户通知必须删除该应用程序才能使其设备恢复合规状态。您还可以设置等待用户按指示进行操作的时间限制。过了该时间限制后，将发生定义的操作，例如，选择性擦除设备。

示例二

- 您想验证客户是否正在使用最新固件，并在用户需要更新其设备时阻止对资源的访问。您可以指定一个触发器，用于在用户设备未安装最新版本时将用户设备设置为不合规。可以使用自动操作来阻止资源并通知客户。

示例三

- 将用户设备置于不合规状态，用户随后修复该设备。可以配置策略来部署将设备重置为合规状态的软件包。

示例四

- 您希望将在特定时间段内处于不活动状态的用户设备标记为不合规。可以按如下所示为不活动设备创建自动化操作：
  1. 在 Endpoint Management 控制台中，转到 设置 **>** 网络访问控制，然后选择 非活动设备。有关 非活动设备设置的详细信息，请参阅 网络访问控制。
  2. 按照添加 和管理操作中概述的步骤添加操作。唯一的区别是，您在操作详细信息页面上按如下所示配置设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 触发器。选择设备属性、不合规性和真。
- 操作。选择发送通知，然后选择使用设置中的通知模板创建的模板。然后在执行该操作之前设置延迟时间（以天、小时或分钟为单位）。设置用户解决触发问题前重复执行操作的时间间隔。

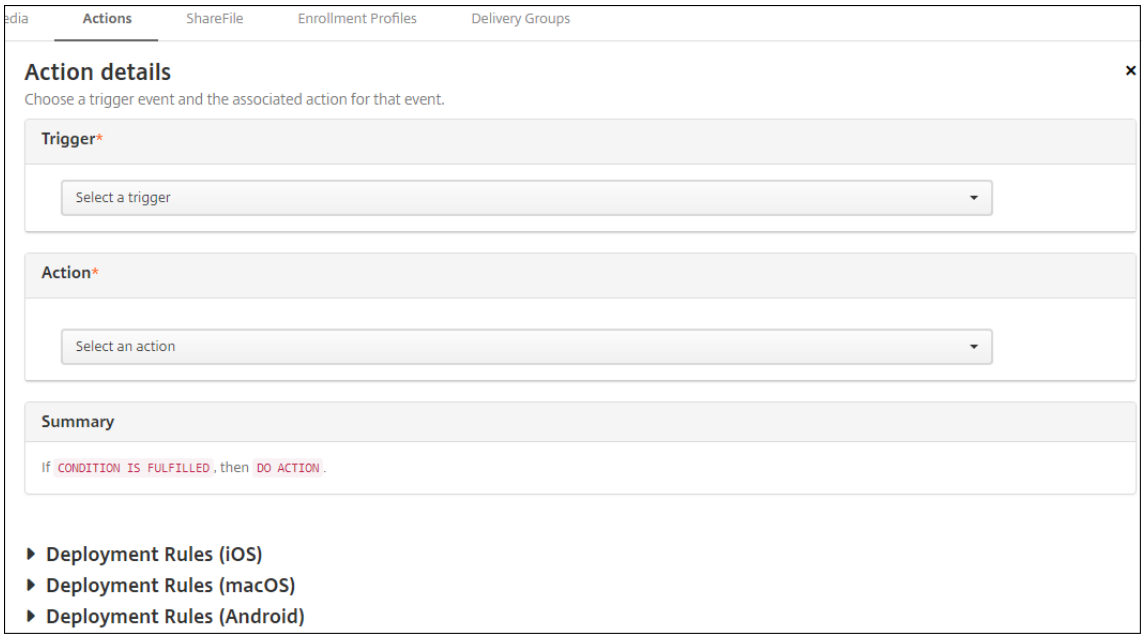
> 提示：
>
> 要批量删除非活动设备，请使用 Endpoint Management 公共 REST API。首先，您可以手动获取要删除的不活动设备的设备 ID，然后运行删除 API 以将其批量删除。

添加和管理操作

要添加、编辑和过滤自动化操作，请执行以下操作：

1. 在 Endpoint Management 控制台中，单击配置 **>** 操作。此时将显示操作页面。
2. 在操作页面上，执行以下操作之一：
   - 单击添加以添加操作。
   - 选择要编辑或删除的现有操作。单击要使用的选项。
3. 此时将显示操作信息页面。
4. 在操作信息页面上，输入或修改以下信息：
   - 名称：键入名称来标识操作。此字段为必填字段。
   - 说明：描述执行该操作的目的。
5. 单击下一步。此时将显示操作详细信息页面。

   以下示例显示如何设置事件触发器。如果选择其他触发器，出现的选项将与此处显示的选项有所差别。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. 在操作详细信息页面上，输入或修改以下信息：

   在触发器列表中，单击适用于此操作的事件触发器类型。选择以下触发器之一：

   - 事件：检查设备状态是否与您选择的不合规事件匹配，然后对其做出反应。
   - 设备属性：检查 MDM 管理的设备上的设备属性的特定值，然后对其做出反应。有关更多信息，请参阅 设备属性名称和值 PDF。
   - 用户属性：对用户属性的特定值（通常来自 Active Directory）做出反应。
   - 已安装应用程序的名称：对正在安装的应用程序做出反应。不应用于仅 MAM 模式。要求在设备上启用应用程序清单策略。默认情况下，应用程序清单策略在所有平台上均处于启用状态。有关详细信息，请参阅 应用清单设备策略
   - **Policy returned value**（策略返回的值）：检查从 PowerShell 脚本返回的值是否满足某些逻辑条件。必须启用和配置 Windows 代理策略。有关 Windows 代理策略的详细信息，请参阅 Windows 客户端设备策略。

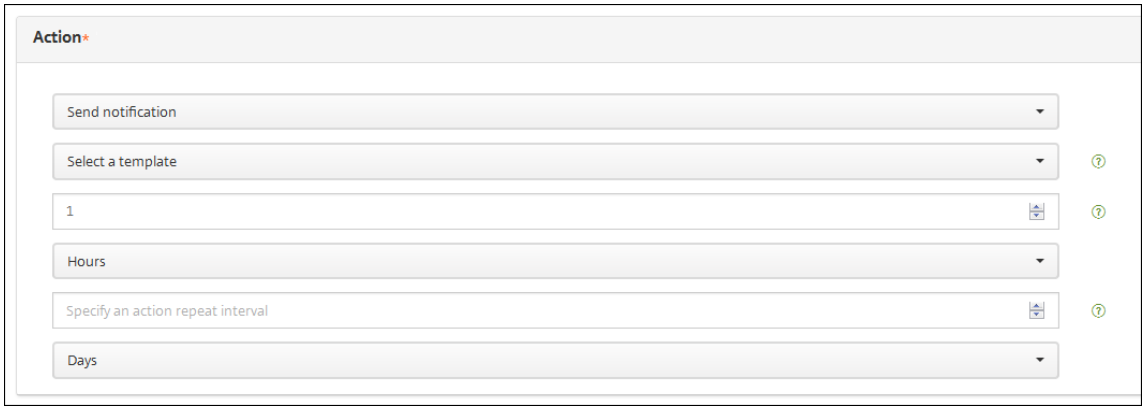
7. 在下一个列表中，单击对触发器的响应。

8. 在操作列表中，单击符合触发器条件时要执行的操作。除发送通知操作外，请选择一个时间范围，让用户可以解决导致触发的问题。如果在该时间范围内未解决此问题，将执行选定的操作。有关操作的定义，请参阅安全操作。

   如果选择发送通知，则按照以下步骤发送通知操作。

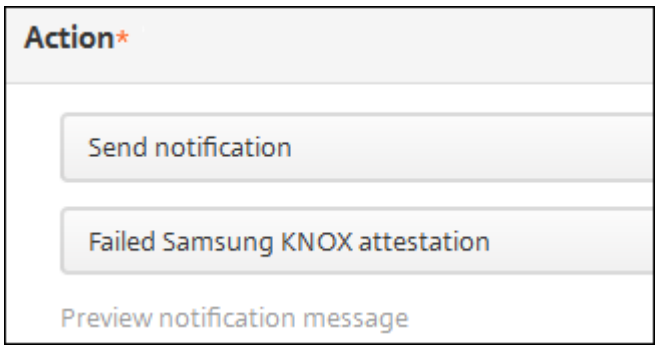
9. 在下一个列表中，选择用于通知的模板。此时将显示与所选事件有关的通知模板。如果没有与通知类型对应的模板，系统会提示您配置模板，并显示消息：此事件类型的模板不存在。请使用设置中的通知模板来创建模板。

   要通知用户，请使用 “设置”>“通知服务器” 配置 SMTP 设置，以便 Endpoint Management 可以发送邮件。请参阅 通知。此外，在继续操作之前，请使用设置 > 通知模板来设置您计划使用的任何通知模板。请参阅 创建和更新通知模板。

   选择模板后，单击预览通知消息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



10. 在以下字段中，以天、小时或分钟为单位设置执行该操作之前的延迟。设置用户解决触发问题前重复执行操作的时间间隔。



11. 在摘要中，验证您是否已按预期创建自动化操作。



12. 配置操作详细信息后，可以分别为每个平台配置部署规则。为此，针对您选择的每个平台执行步骤 13。
13. 配置部署规则。有关配置部署规则的常规信息，请参阅部署资源。

    对于此示例：

    - 设备所有权必须为 **BYOD**。
    - 设备必须兼容通行码。
    - 设备的移动设备国家/地区代码不能仅为“安道尔”。

14. 针对该操作配置了平台部署规则后，单击下一步。此时将显示操作分配页面，您可以在此将操作分配给一个或多个交付组。此步骤可选。
15. 在选择交付组旁边，键入以查找交付组或者在列表中选择组。选择的组显示在用于接收应用程序分配的交付组列表中。
16. 展开部署计划，然后配置以下设置：

    - 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。如果选择关，则无需其他选项。
    - 在部署计划旁边，单击立即或稍后。默认选项为立即。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 如果单击以后，请单击日历图标，然后选择部署的日期和时间。
- 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
- 在为始终启用的连接部署旁边，单击开或关。默认选项为关。

  如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则适用此选项。

  > 注意：
  >
  > 如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则适用此选项。
  >
  > 始终启用选项：
  >
  > - 不适用于 iOS 设备
  > - 不适用于开始使用版本 10.18.19 或更高版本的 Endpoint Management 的 Android 和 Android Enterprise 客户
  > - 不建议开始使用 10.18.19 之前的 Endpoint Management 版本的 Android 和 Android Enterprise 客户使用
  >
  > 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

17. 单击下一步。此时将显示摘要页面，您可以在此验证操作配置。
18. 单击保存以保存操作。

面向仅 **MAM** 模式的应用程序锁定和应用程序擦除操作

您可以针对 Endpoint Management 控制台中列出的全部四种类别的触发器（即事件、设备属性、用户属性和已安装应用程序的名称），擦除或锁定设备上的应用程序。

配置应用程序擦除或应用程序锁定自动操作

1. 在 Endpoint Management 控制台中，单击配置 **>** 操作。
2. 在操作页面上，单击添加。
3. 在操作信息页面上，输入操作名称和可选说明。
4. 在操作详细信息页面上，选择所需的触发器。
5. 在操作中，选择一项操作。

   针对此步骤，请记住以下条件：

   触发器类型为事件，但值不是 **Active Directory** 已禁用用户时，将不显示应用程序擦除和应用程序锁定操作。

   触发器类型为设备属性，值为已启用 **MDM** 丢失模式时，将不显示以下操作：

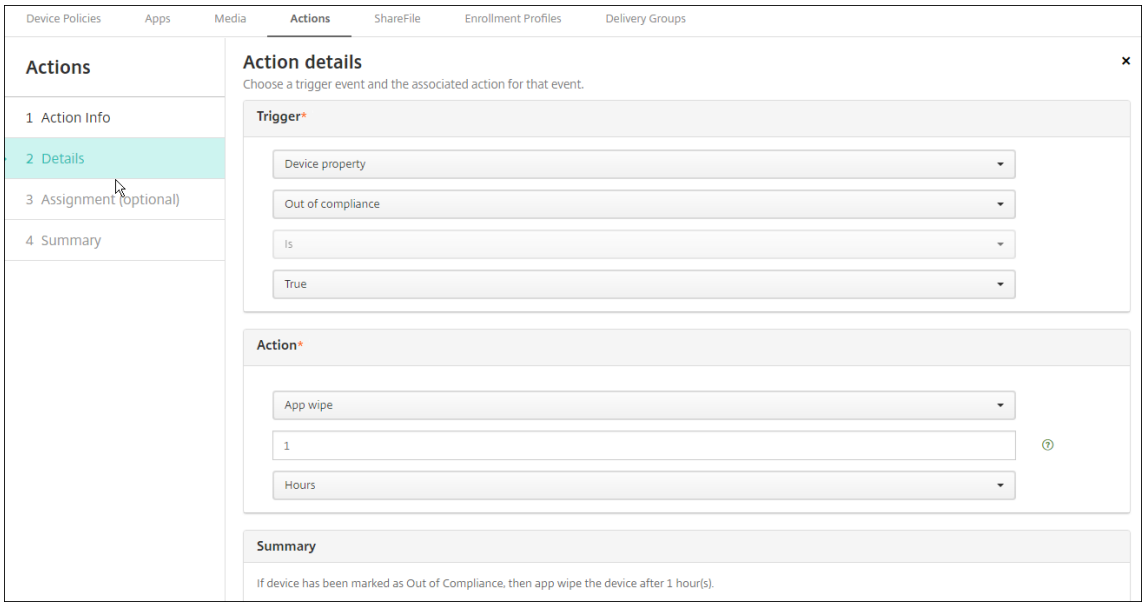
   - 选择性擦除设备
   - 完全擦除设备

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 吊销设备

每个选项都会自动设置 1 小时延迟，但也可选择以分钟、小时或天为单位的延迟期限。延迟的目的是在执行操作之前让用户有时间解决问题。有关应用程序擦除和应用程序锁定操作的详细信息，请参阅安全操作。

> 注意：
>
> 如果您将触发器设置为事件，重复时间间隔将自动设置为最小值 1 小时。设备必须刷新策略以与服务器同步，才能传入通知。通常情况下，设备将在用户通过 Secure Hub 登录或手动刷新其策略时与服务器同步。
>
> 在执行任何操作之前，还可能会再延迟 1 小时左右，以便允许 Active Directory 数据库与 Endpoint Management 同步。

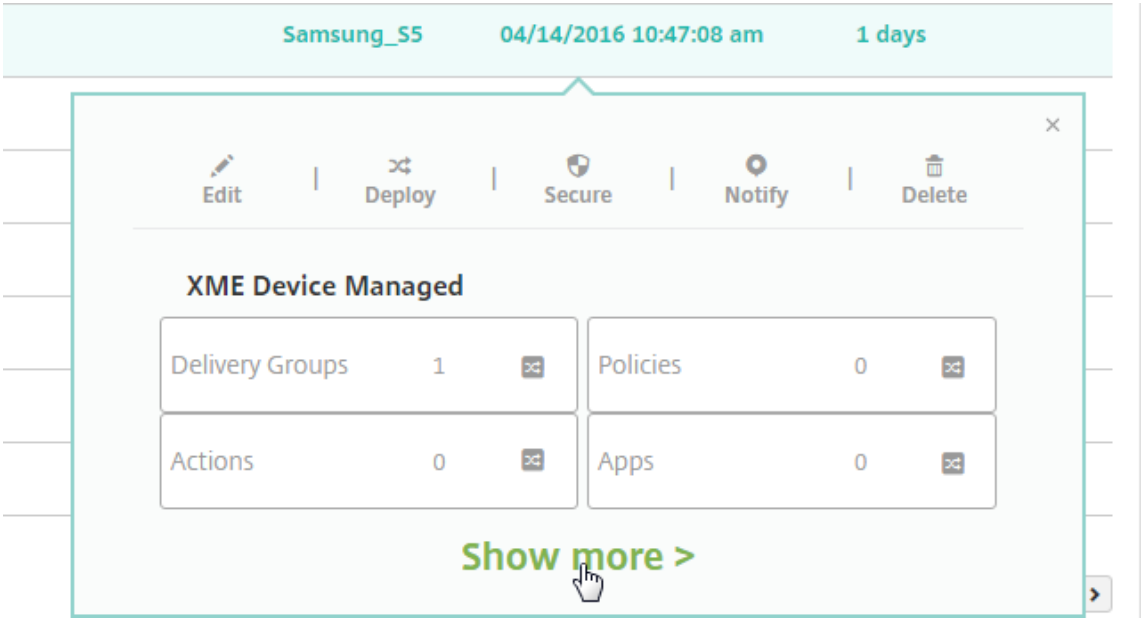


6. 配置部署规则，然后单击下一步。
7. 配置交付组分配和部署计划，然后单击下一步。
8. 单击保存。

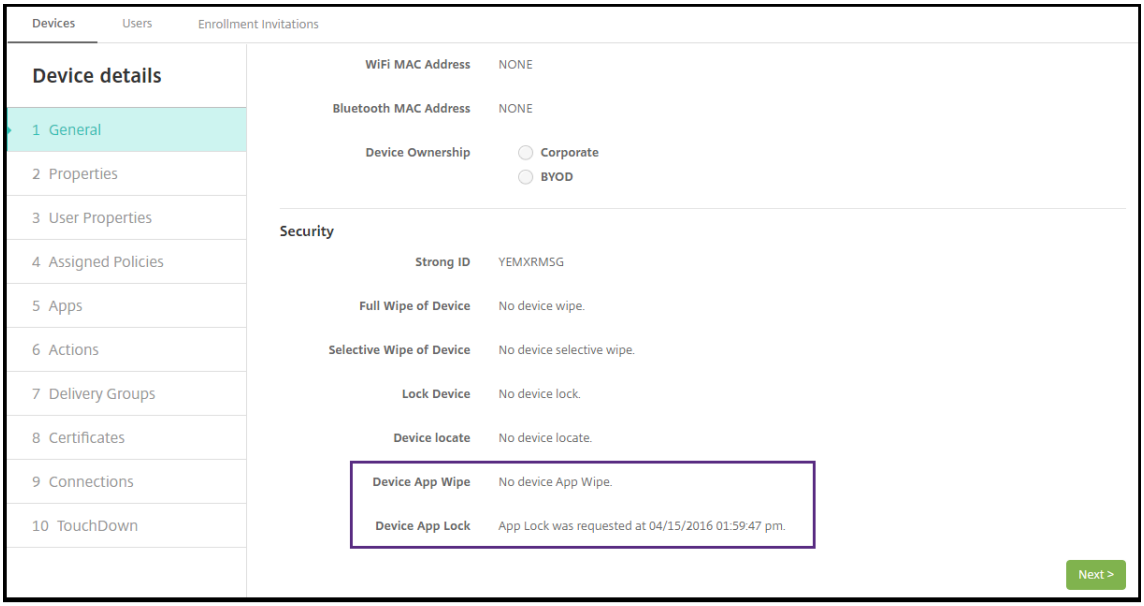
检查应用程序锁定或应用程序擦除状态

1. 转至管理 > 设备，单击某个设备，然后单击显示更多。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

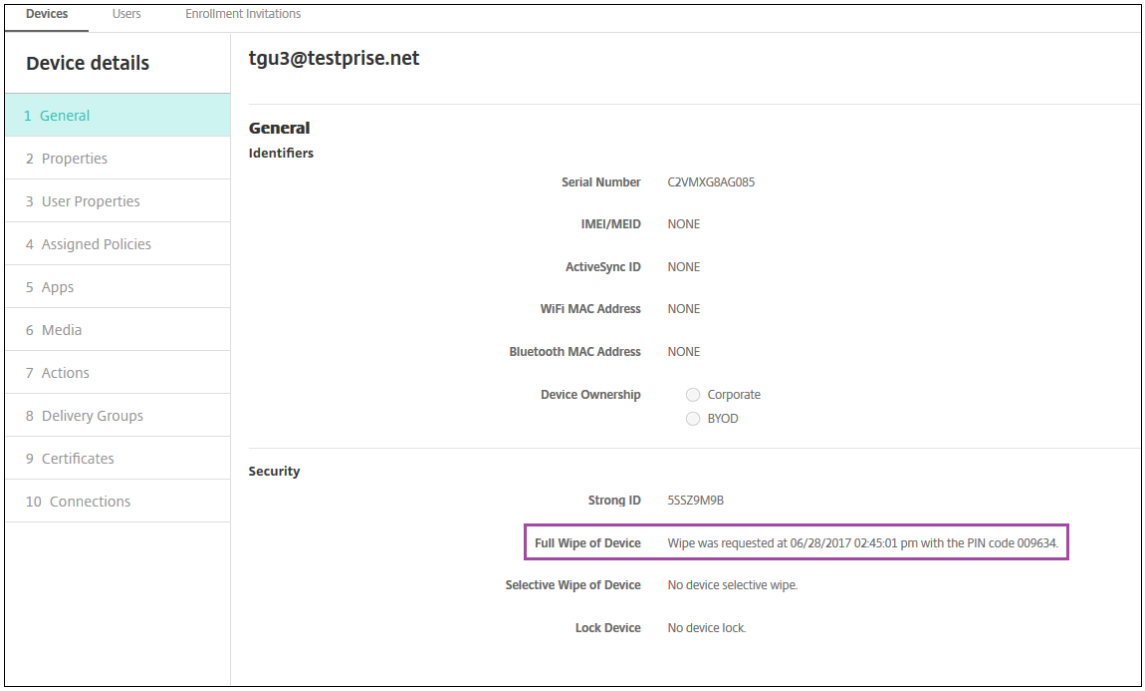


2. 滚动到设备应用程序擦除和设备应用程序锁定。



擦除设备后，系统将提示用户输入 PIN 代码。如果用户忘记了该代码，您可以在“设备详细信息”中查找。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



在 **Azure AD** 中将 **Windows 10** 和 **Windows 11** 设备标记为不合规

当加入 Azure AD 的 Windows 10 和 Windows 11 设备被 Endpoint Management 标记为不合规时，它们也可以在 Azure AD 中标记为不合规。要启用此功能，请添加对本地 MDM 应用程序的权限，以访问 Azure AD 门户中的 Microsoft Graph API。

1. 使用您的 Azure AD 管理员凭据登录 Azure AD 门户。
2. 在 Azure AD 门户中，导航到 **Azure Active Directory >** 移动性 **(MDM** 和 **MAM)**。选择本地 **MDM** 应用程序。
3. 单击本地应用程序设置 **>** 所需权限 **>** 添加 **>** 选择 **API > Microsoft Graph**。单击选择并保存。
4. 在所需权限下，选择 **Microsoft Graph**。在启用访问权限下，选择读取和写入目录数据。
5. 在所需权限下，选择 **Microsoft Graph**。然后单击授予权限。
6. 单击是授予权限。

当运行 Windows 10 或 Windows 11 的 Azure AD 注册设备不合规时，Endpoint Management 还会在 Azure AD 中将该设备标记为不合规。

基于 **Windows** 代理设备策略结果创建自动化操作

使用 Windows 代理设备策略部署用于监视托管 Windows 桌面和平板电脑上的注册表值的脚本。根据从脚本返回的值，您可以配置要运行的自动化操作。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 配置 Windows 代理设备策略并检查脚本返回的值。有关 Windows 代理设备策略的信息，请参阅 Windows 代理设备策略。

   该文章和本部分内容包括一个基于名为 `EntApp_2019_checkFirewall` 的脚本的示例。相关的 Windows 代理设备策略定义了名为 `cName_checkFirewall` 的配置。该配置运行示例脚本。

   脚本在设备上运行后，您将获得创建操作所需的信息，如 Windows Agent 设备策略中所述。

2. 在 Endpoint Management 控制台中，单击配置 **>** 操作。
3. 在操作页面上，单击添加。
4. 在操作信息页面上，输入操作名称和可选说明。
5. 在操作详细信息页面上，选择 **Policy returned value**（策略返回的值）触发器。

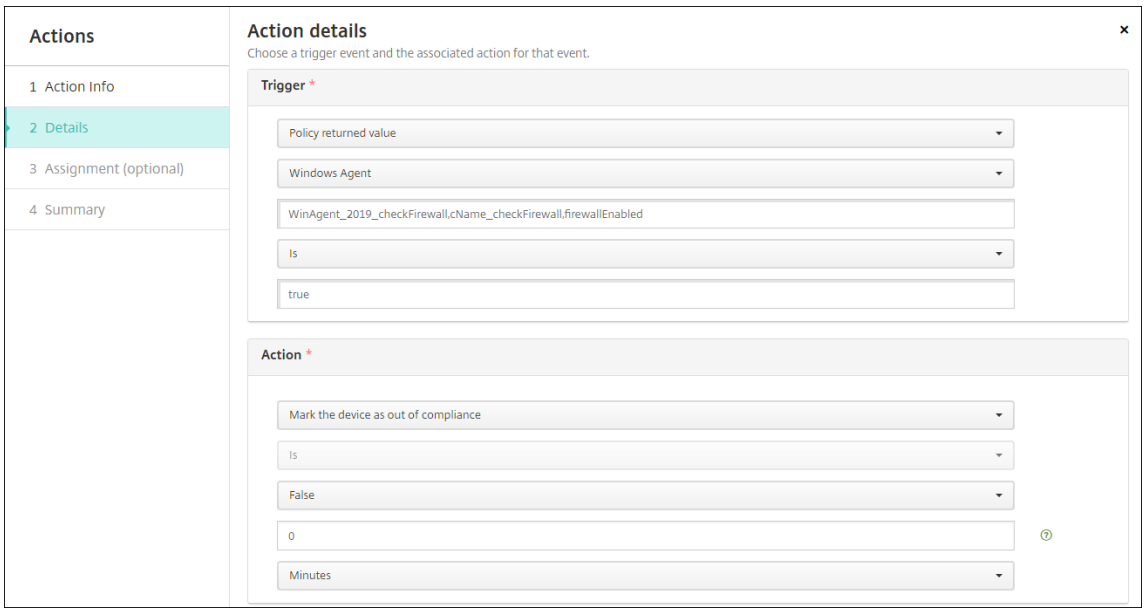


6. 在显示的字段中，定义触发器和操作：

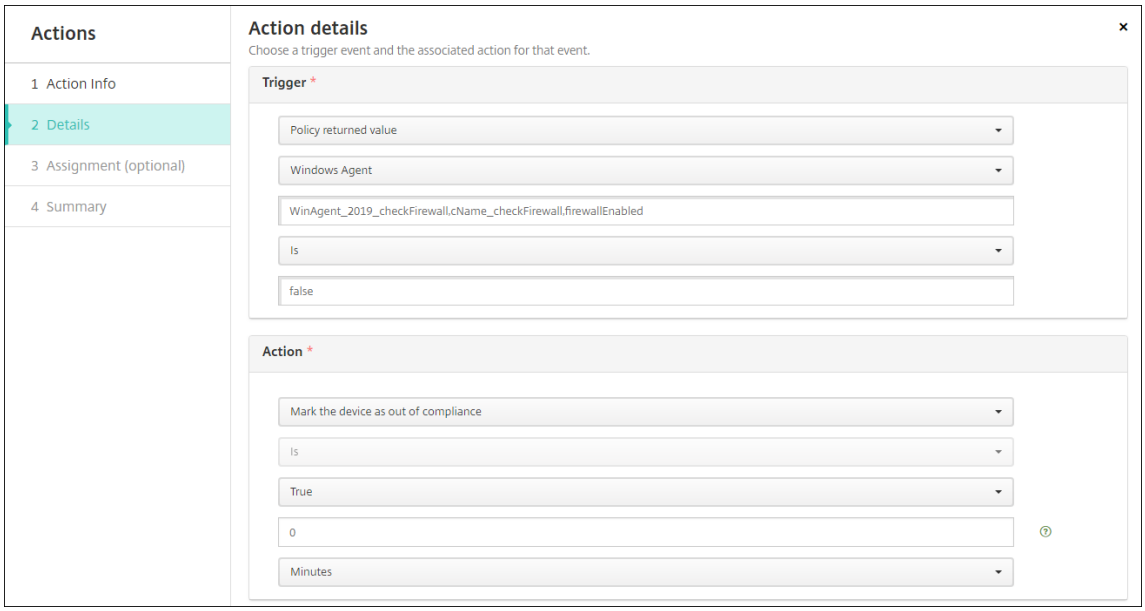
   - **Windows Agent settings**（Windows 代理设置）：键入您创建的 Windows 代理策略的策略名称、配置名称和键名称。
   - **Drop-down menu**（下拉菜单）：选择 **Is**（是）、**Is Not**（不是）、**Contains**（包含）或 **Does Not Contain**（不包含）逻辑。此逻辑应用到下一个字段，并在应用逻辑时导致操作触发。
   - 输入字符串：输入运行在策略中上载的 PowerShell 脚本所产生的字符串。有关查找该字符串的信息，请参阅 Windows Agent 设备策略。
   - 操作：选择一项操作、操作值，然后选择解析该操作的时间范围。

   在我们的示例中：如果键名称 `firewallEnabled` 返回值 **`true`**，则以下操作将设备标记为合规。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



如果键名称 `firewallEnabled` 返回值 **`false`**，则以下操作将设备标记为不合规。



7. 如果需要，请设置部署计划并选择交付组。

监视和支持

May 8, 2023

您可以使用 Endpoint Management 控制板和 Endpoint Management 支持页面来监视 Endpoint Management 服务器并对其进行故障排除。使用 Endpoint Management 支持页面可访问与支持相关的信息和工具。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在 Endpoint Management 控制台中，单击右上角的扳手图标。

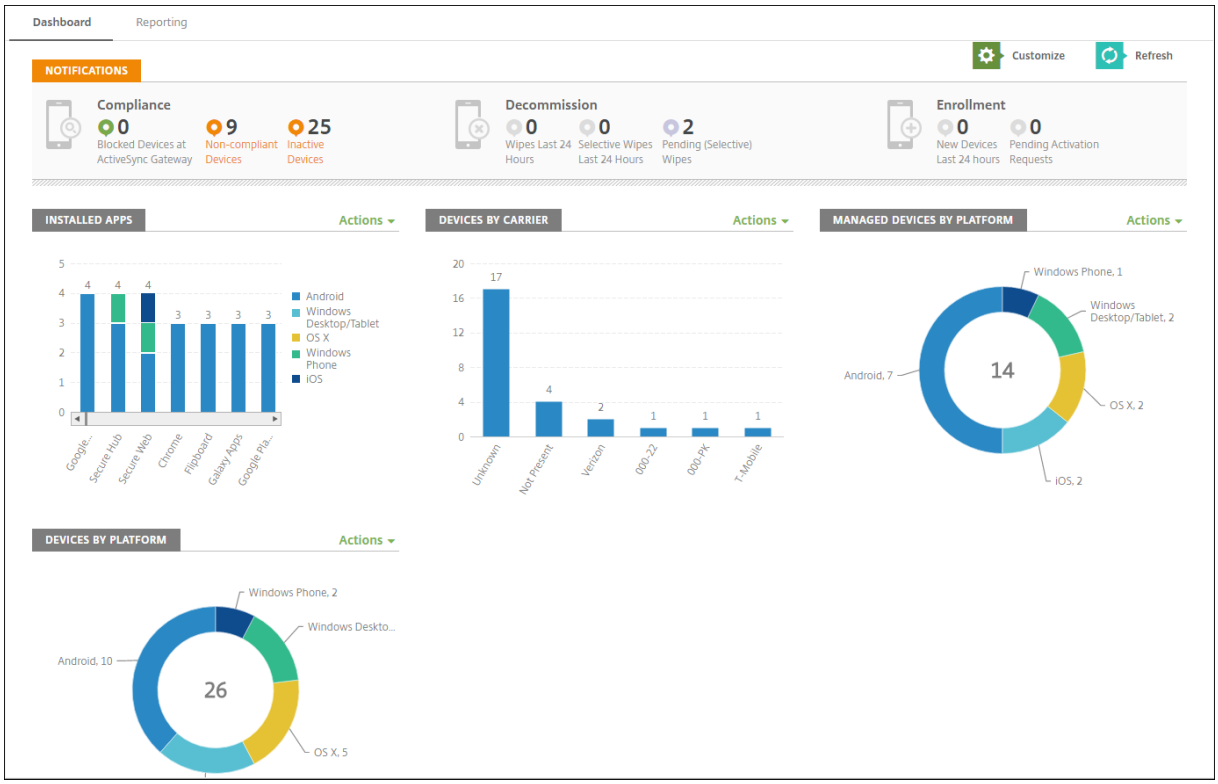


此时将显示故障排除和支持页面。

使用 Endpoint Management 故障排除和支持页面以执行以下操作：

- 访问诊断。
- 访问 Citrix 产品文档和知识中心的链接。
- 访问日志操作。
- 使用高级配置选项。
- 访问工具和实用程序。

还可以通过访问 Endpoint Management 控制台控制板一目了然地查看信息。根据这些信息，您可以使用小组件快速查看问题和成功方法。



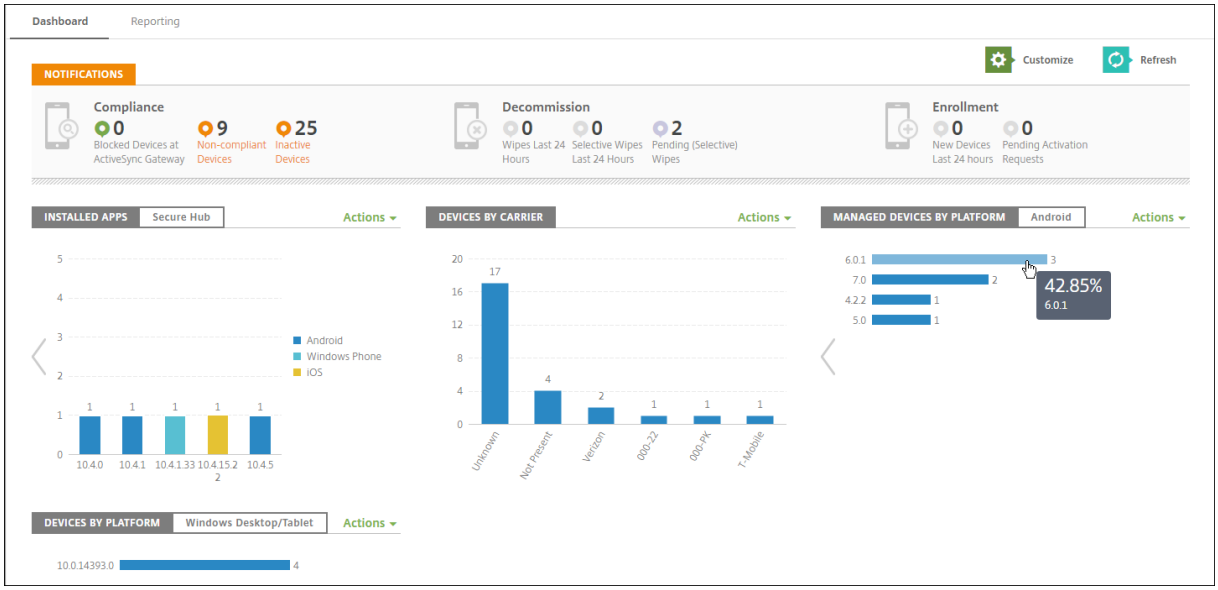
控制板通常是您登录 Endpoint Management 控制台时首先显示的页面。要从控制台中的其他地方访问控制板，请单击分析。单击控制板中的自定义可编辑页面布局以及编辑显示的小组件。

- 我的控制板：最多可以保存四个控制板。可以单独编辑这些控制板，并通过选择保存的控制板来查看每个控制板。
- 布局样式：在此行中，可以选择在控制板上显示的小组件数以及如何布局小组件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

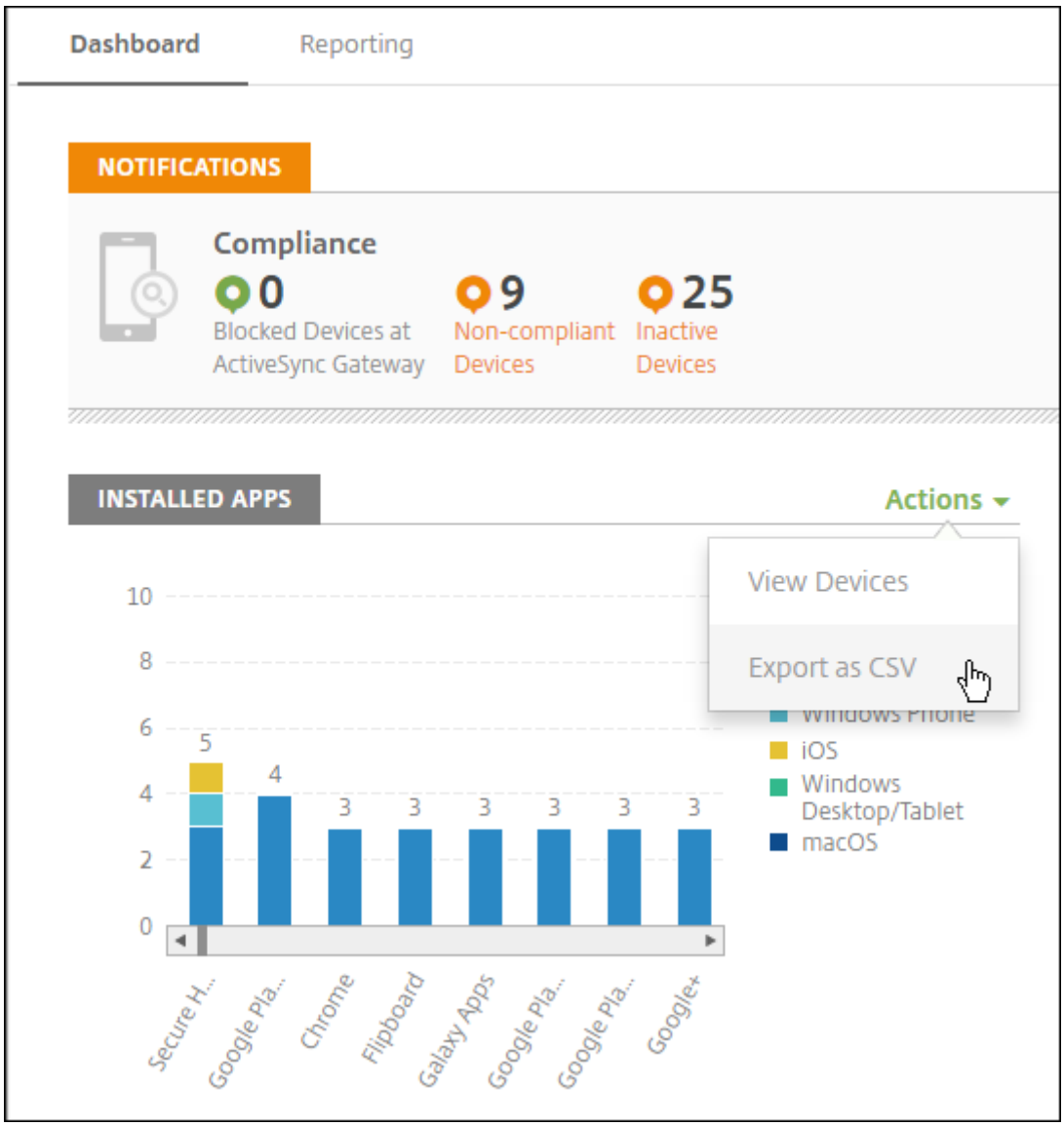
- 小组件选择：可以选择在控制板上显示的信息。
  - 通知：选中左侧数字上方的复选框可将“通知”栏添加到小组件上方。此栏显示兼容设备、不活动设备以及过去 24 小时擦除或注册的设备数。
  - 设备 **(**按平台**)**：按平台显示托管设备和非托管设备数。
  - 设备 **(**按运营商**)**：按运营商显示托管设备和非托管设备数。单击每个栏可按平台查看明细。
  - 托管设备 **(**按平台**)**：按平台显示托管设备数。
  - 非托管设备 **(**按平台**)**：按平台显示非托管设备数。此图表中显示的设备可能安装了代理，但设备的权限已被吊销或设备已被擦除。
  - 设备 **(**按 **ActiveSync Gateway** 状态**)**：显示按 ActiveSync Gateway 状态分组的设备数。信息中显示“已阻止”、“已允许”或“未知”状态。可以单击每个栏来按平台细分数据。
  - 设备 **(**按所有权**)**：显示按所有权状态分组的设备数。信息中显示“公司拥有”、“员工拥有”或“未知所有权”状态。
  - 失败的交付组部署：按软件包显示失败部署总数。仅显示部署失败的软件包。
  - 设备 **(**按阻止原因**)**：显示 ActiveSync 阻止的设备数
  - 已安装的应用程序：键入应用程序信息图的应用程序名称。
  - 批量购买应用程序许可证使用情况：显示 Apple 批量购买应用程序的许可证使用情况统计信息。

通过每个小组件，可以单击各个部分深入查看详细信息。



还可以单击操作菜单将信息导出为.csv 文件。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



面向技术支持管理员的“监视”页面

您可以在监视页面上监视 Endpoint Management 并对其进行故障排除。此界面是针对技术支持管理员定制的，用于有效地执行基于用户的故障排除。

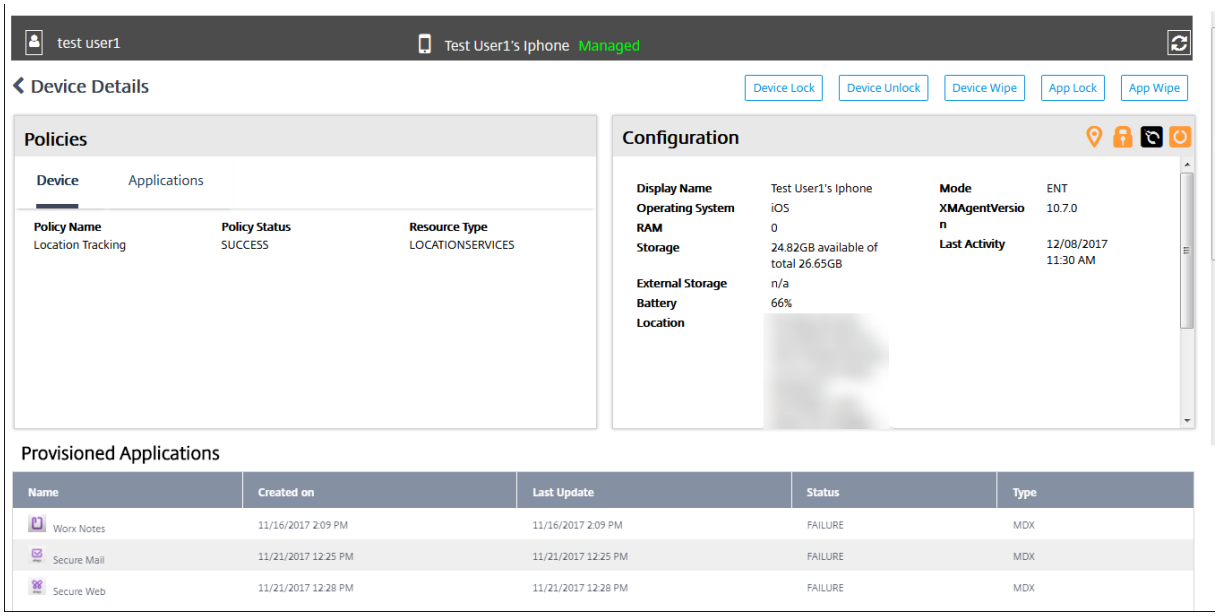
技术支持管理员必须具有以下权限才能访问监视选项卡和所有可用的工作流程：

- 授权访问
  - 管理控制台访问
  - 公共 API 访问
- 控制台功能
  - 监视
  - 设备

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 完全擦除设备
  - 查看位置
    * 查找设备
    * 跟踪设备
  - 锁定设备
  - 解锁设备
  - 应用程序锁定
  - 应用程序擦除
  - 应用程序

监视页面提供设备策略和配置的统一视图。此视图包括应用程序锁定/解锁、应用程序擦除、设备锁定/解锁和设备擦除等故障排除操作。



使用监视页面可以执行以下操作：

- 搜索要进行故障排除的 Active Directory (AD) 用户和设备。
- 分析包含以下选项的设备详细信息页面：
  - 策略：显示选定的设备和应用程序的设备和应用程序策略。有关修改策略的信息，请参阅设备策略和添加应用程序。
  - 配置：显示设备配置。此面板包括指示设备是否启用了定位服务以及是否由 MAM 或 MDM 托管的图标。此面板还显示存储加密状态。
  - 正在运行的应用程序表：显示设备上当前正在运行的应用程序的详细信息。
- 对设备进行故障排除。此页面上可用的安全操作基于设备的注册以及已登录的管理员可用的权限：
  - 设备锁定/解锁
  - 设备擦除
  - 应用程序锁定/解锁（设备注册了 MAM 时可用）
  - 应用程序擦除（设备注册了 MAM 时可用）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

有关可以执行的操作的详细信息，请参阅安全操作。

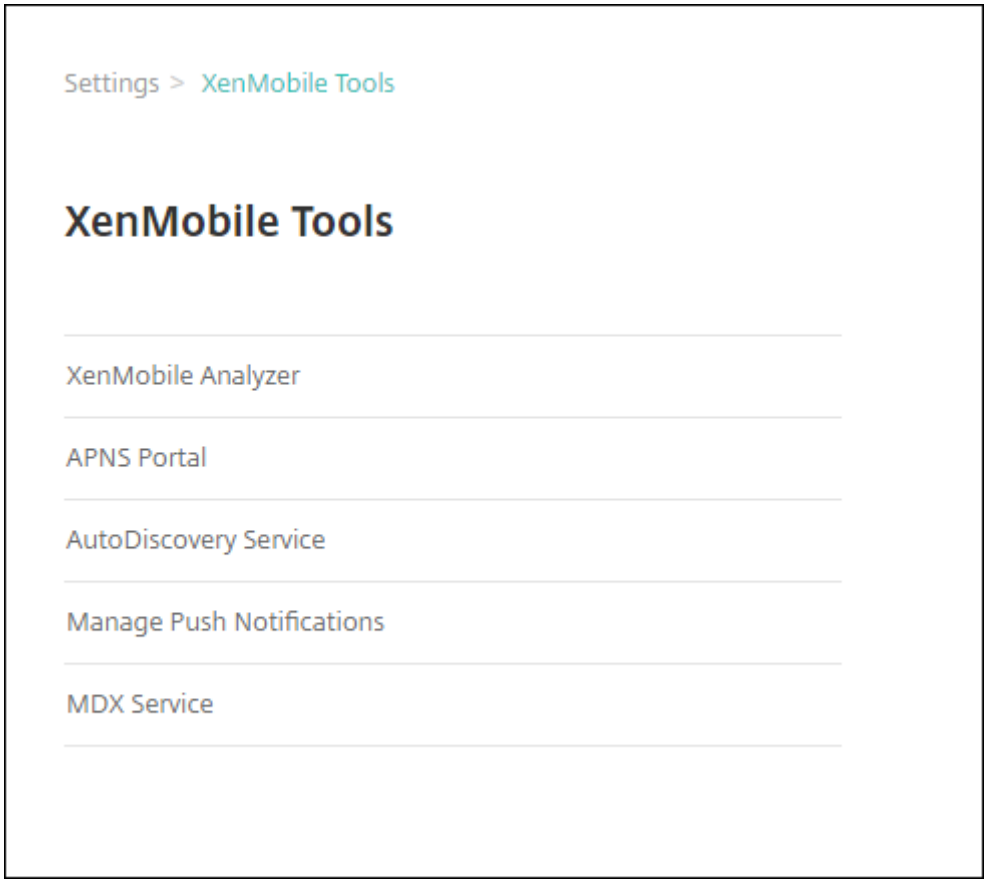
“监视”页面在上次加载后 60 分钟内可能无法按预期运行，因为此页面不处理登录令牌的刷新。解决方法为通过重新加载页面来刷新令牌：单击服务控制台上的 **Citrix Cloud** 链接，然后单击 **Endpoint Management >** 管理 **>** 监视。

从控制台访问 **Endpoint Management** 工具

您可以从 Endpoint Management 控制台访问这些 Endpoint Management 工具：

- **APNs** 门户 – 向 Citrix 提交请求以对 APNs 证书进行签名，随后将该证书提交给 Apple。
- 自动发现服务 – 为您的域中的 Endpoint Management 请求并配置自动发现。
- 管理推送通知 – 管理 iOS 和 Windows 移动应用的推送通知。

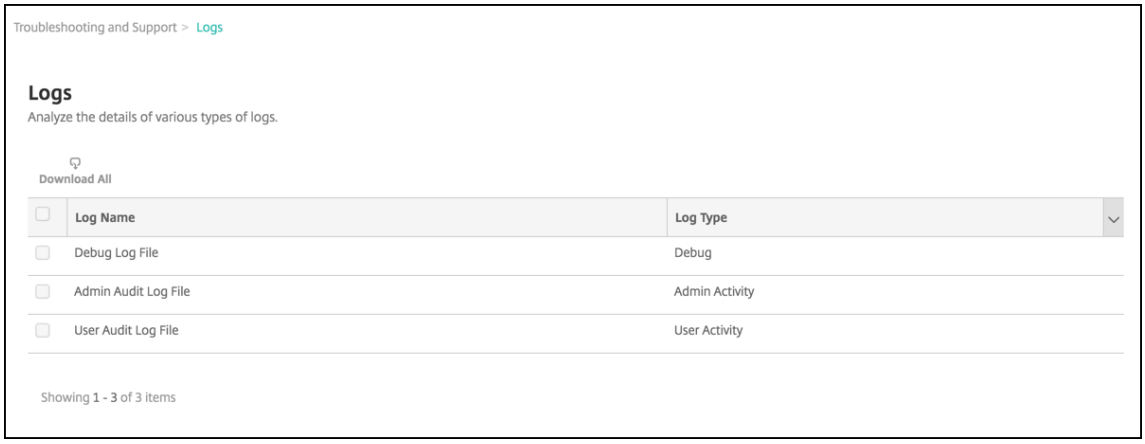
要访问这些工具，请转到设置 **> Endpoint Management** 工具。此页面对具有云管理员或客户管理员角色的用户可用。



在 **Endpoint Management** 中查看和分析日志文件

1. 在 Endpoint Management 控制台中，单击控制台右上角的扳手图标。此时将打开故障排除和支持页面。
2. 在日志操作下方，单击日志。此时将显示日志页面。单独的日志将显示在表格中。

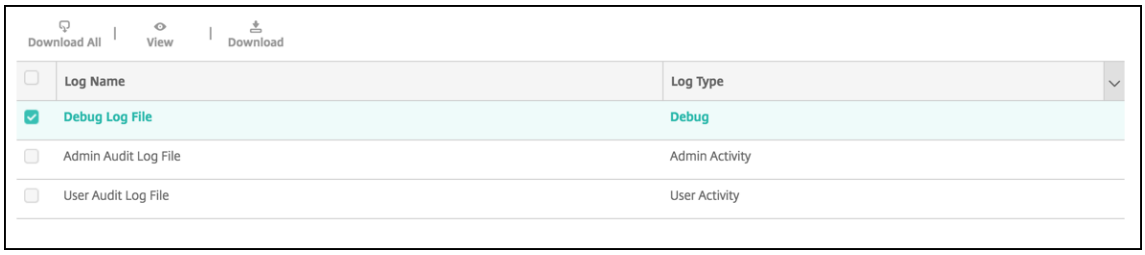
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 选择要查看的日志：

   - 调试日志文件中包含对 Citrix 技术支持有用的信息，例如错误消息和服务器相关操作。
   - 管理员审核日志文件中包含与 Endpoint Management 控制台上的活动有关的审核信息。
   - 用户审核日志文件中包含与配置的用户有关的信息。

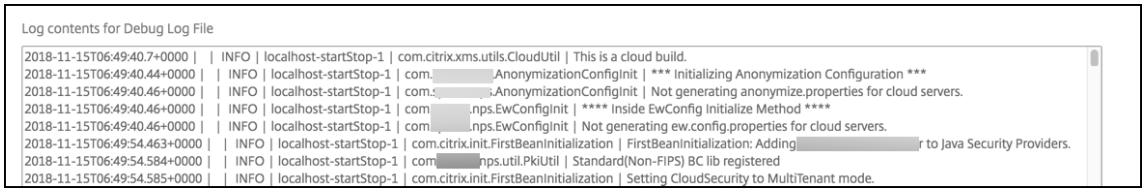
4. 使用表格顶部的操作可下载全部日志，也可以查看或下载单个日志。



> 注意：
>
> 如果选择多个日志文件，则仅全部下载可用。

5. 执行以下操作之一：

   - 全部下载：控制台下载系统中存在的所有日志（包括调试、管理员审核、用户审核、服务器日志等）。
   - 查看：在表格下方显示所选日志的内容。
   - 下载：控制台仅下载所选的单个日志文件类型。控制台还会下载与该类型相同的所有存档日志。



Endpoint Management 使用 log4j syslog 追加器发送 RFC5424 格式的 syslog 消息。syslog 消息数据是没有任何特定格式的纯文本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

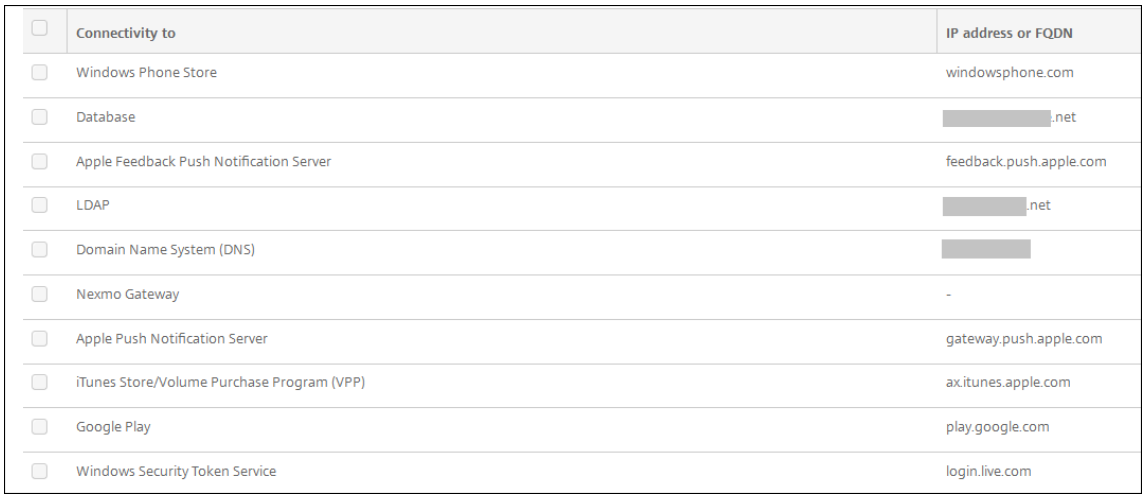
连接检查

June 9, 2022

从 Endpoint Management 的故障排除和支持页面，可以检查 Endpoint Management 与 Citrix Gateway 及其他服务器和位置的连接情况。要运行 Endpoint Management 连接检查，您需要支持或管理员角色。使用基于角色的访问控制 (RBAC) 设置此角色。有关分配角色的更多信息，请参阅使用 RBAC 配置角色。

运行 **Endpoint Management** 连接检查

1. 在 Endpoint Management 控制台中，单击控制台右上角的扳手图标。此时将显示故障排除和支持页面。
2. 在诊断下，单击 **Endpoint Management Connectivity Checks**（Endpoint Management 连接检查）。此时将显示 **Endpoint Management Connectivity Checks**（Endpoint Management 连接检查）页面。如果 Endpoint Management 环境包含加入群集的节点，将显示所有节点。



Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	.net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	.net
Domain Name System (DNS)	
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

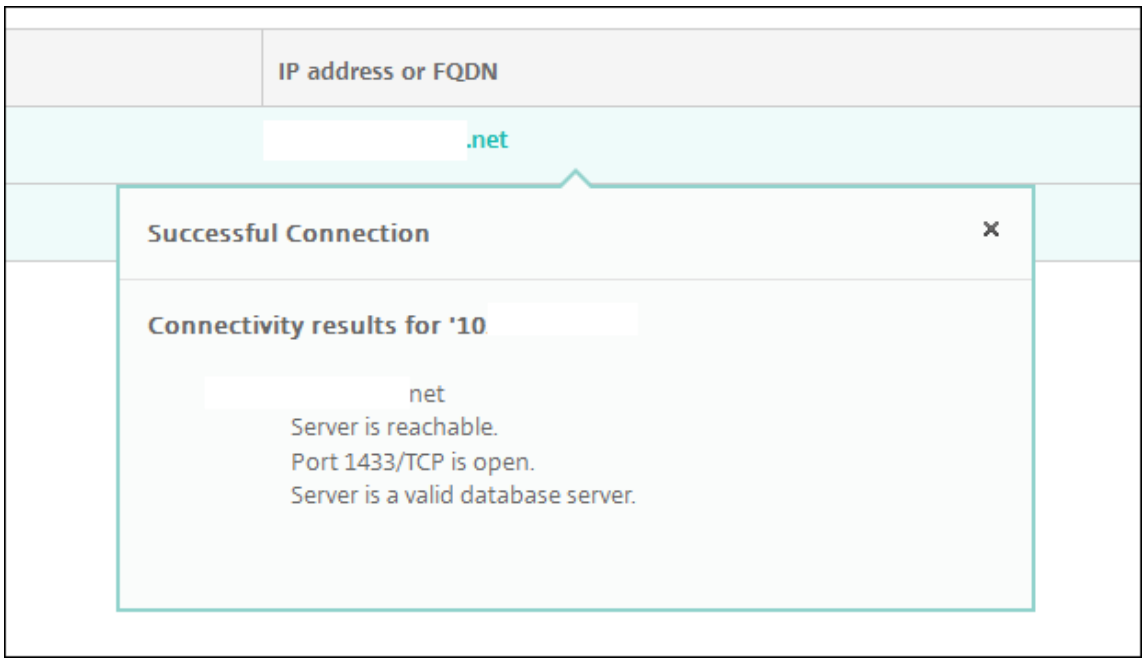
3. 选择执行连接测试时要包括的服务器，然后单击测试连接。此时将显示测试结果页面。



Connectivity to	IP address or FQDN	
Database	net	✓
Windows Phone Store	windowsphone.com	✓

4. 在测试结果表中选择一个服务器以查看该服务器的详细结果。

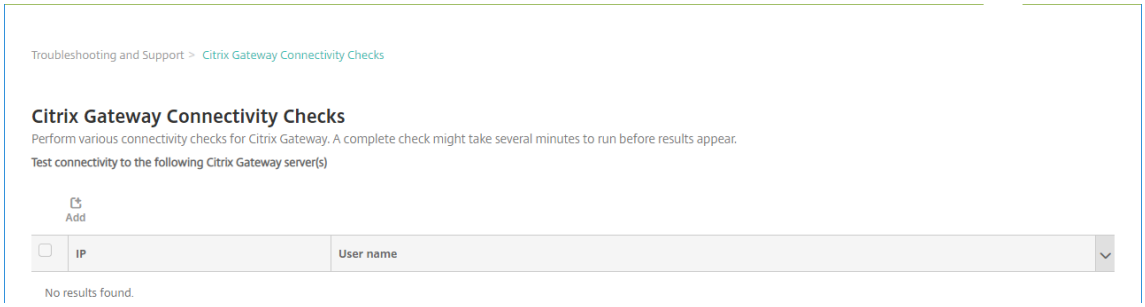
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



有关 Endpoint Management 可以执行的连通性检查及其详细信息，请参阅连通性检查详细信息。

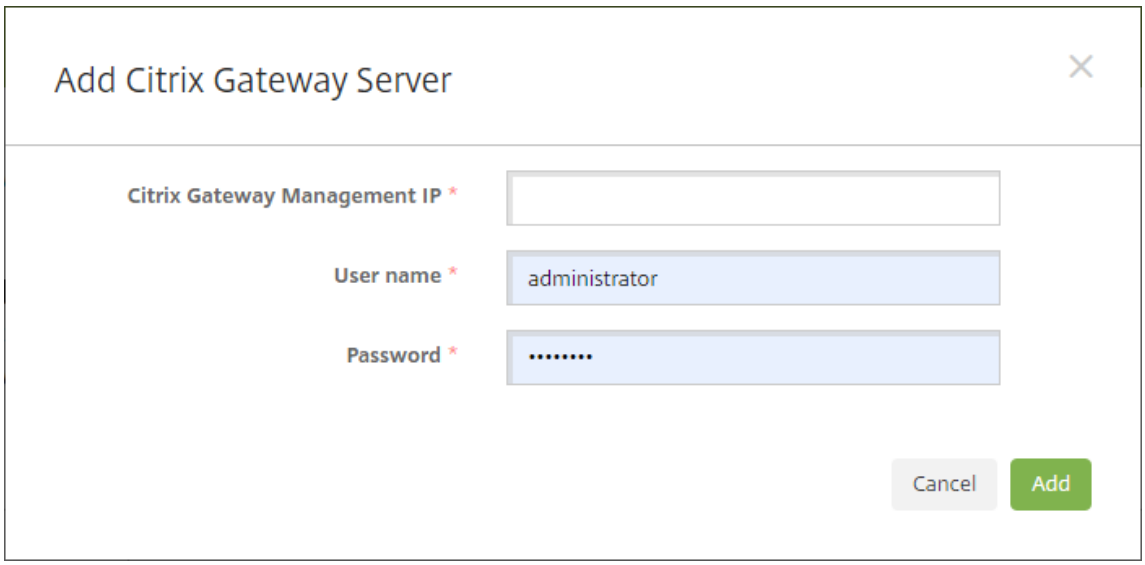
执行 **Citrix Gateway** 连接性检查

1. 在故障排除和支持页面上的诊断下，单击 **Citrix Gateway** 连接检查。此时将显示 **Citrix Gateway** 连接检查页面。如果 Endpoint Management 与 Citrix Gateway 之间没有连接，则该表为空。



2. 单击添加。此时将显示添加 **Citrix Gateway** 服务器对话框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 在 **Citrix Gateway** 管理 **IP** 中，键入运行要测试的 Citrix Gateway 的服务器的管理 IP 地址。

   如果要对以前已添加的 Citrix Gateway 服务器执行连接检查，系统会提供 IP 地址。

4. 键入关于此 Citrix Gateway 的管理员凭据。

   如果要对以前已添加的 Citrix Gateway 服务器执行连接检查，系统会提供用户名。

5. 单击添加。此 Citrix Gateway 将添加到 **Citrix Gateway** 连接检查页面上的表格中。
6. 选择 Citrix Gateway 服务器，然后单击测试连接。结果将显示在测试结果表格中。
7. 在测试结果表中选择一个服务器以查看该服务器的详细结果。

连接检查详细信息

下表列出了 Endpoint Management 可以执行的各种连接检查，并包括每个检查的详细信息。

与此对象的连接	**IP** 地址或 **FQDN**	详细信息
Apple 推送通知服务器	api.push.apple.com	检查 Apple 推送通知服务器与 Endpoint Management 节点之间的连接。需要 Apple 推送通知服务器才能向 iOS、macOS 和 tvOS 设备发送消息。
Apple 反馈推送通知服务器	feedback.push.apple.com	检查 Apple Feedback Server 与 Endpoint Management 节点之间的连接。Apple Feedback Push Notification Server 为您提供有关发送到 iOS 和 macOS 设备的失败远程通知的信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

与此对象的连接	**IP** 地址或 **FQDN**	详细信息
Citrix 许可证服务器	许可证服务器的 IP 地址	检查 Citrix 许可证服务器与 Endpoint Management 节点之间的连接。运行 Citrix 产品的服务器会联系 Citrix 许可证服务器来获取许可证。
Citrix Gateway	在 Endpoint Management 中配置的 Citrix Gateway 的 FQDN	检查 Citrix Gateway 与 Endpoint Management 节点之间的连接。Endpoint Management 客户端应用程序（例如 Secure Mail 和 Secure Web）使用 Citrix Gateway 通过 VPN 服务器进行连接以访问内部网络。
数据库	数据库服务器的 IP 地址或 FQDN	检查 Endpoint Management 数据库与 Endpoint Management 节点之间的连接。
域名系统 (DNS)	在 Endpoint Management 中配置的 IP 地址	检查 DNS 服务器与 Endpoint Management 节点之间的连接。
Secure Ticket Authority 服务	localhost	检查 Endpoint Management 节点与身份验证服务、STA (Secure Ticket Authority) 服务和群集服务的连接。
Firebase Cloud Messaging (FCM) 服务器		检查 FCM 服务器与 Endpoint Management 节点之间的连接。使用 FCM，您可以通知客户端应用程序有新电子邮件或者其他数据可同步。可以发送通知消息以提高用户参与度和留存率。FCM 是 Google Cloud Messaging (GCM) 的替代产品。
Google Play	play.google.com	检查 Google Store Server 与 Endpoint Management 节点之间的连接。Google Play 用于提供包括托管的专用企业应用程序交付应用商店在内的服务。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

与此对象的连接	**IP** 地址或 **FQDN**	详细信息
iTunes Store/批量购买	vpp.itunes.apple.com	检查 Apple Store Server 与 Endpoint Management 节点之间的连接。Apple Store 用于提供包括托管的专用企业应用程序交付应用商店在内的服务。
LDAP	在 Endpoint Management 中配置的 LDAP 的 IP 地址或 FQDN	检查 LDAP 服务器与 Endpoint Management 节点之间的连接。
Microsoft 推送通知服务器	sin.notifiy.windows.com	检查 Windows 通知服务器与 Endpoint Management 节点之间的连接。Windows 通知服务器用于向 Windows 设备发送消息。
Content Collaboration 服务	在 Endpoint Management 中配置的 Content Collaboration 服务的 IP 地址或 FQDN	检查 Content Collaboration 服务与 Endpoint Management 之间的连接。Content Collaboration 服务是一个安全的基于云的平台，供企业存储和共享大型文件。
Windows Desktop/Tablet 应用商店	windows.microsoft.com	检查 Windows Desktop/Tablet Store 与 Endpoint Management 节点之间的连接。Windows Desktop/Tablet Store 用于提供包括托管的专用企业应用程序交付应用商店在内的服务。
Windows 安全令牌服务	login.live.com	检查 Windows Security Token Server 与 Endpoint Management 节点之间的连接。Windows Security Token Service 支持面向 Windows 设备的双重身份验证（域加安全令牌）。

移动服务提供商

December 3, 2021

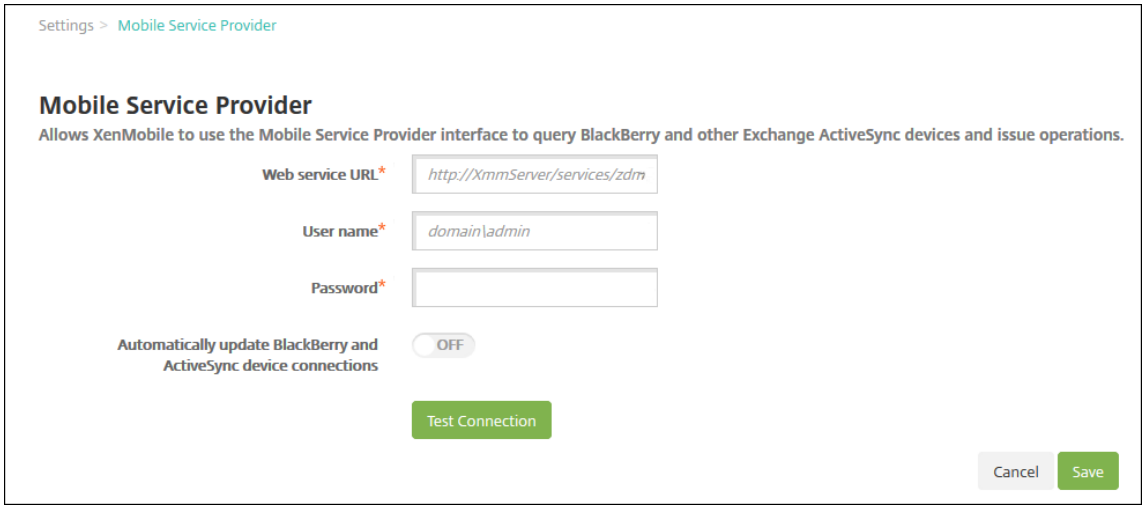
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

可以启用 Endpoint Management 以使用移动服务提供商界面来查询黑莓和 Exchange ActiveSync 设备并发出操作。

例如，假设贵组织有 1000 个用户，每个用户使用一个或多个设备。指示所有用户使用 Endpoint Management 注册其设备后，Endpoint Management 控制台会指示用户注册的设备数量。通过配置此设置，您可以确定有多少设备连接到 Exchange Server。这样，您可以执行以下操作：

- 确定是否有用户仍需要注册其设备。
- 向连接到 Exchange Server 的用户设备发出命令，例如数据擦除。

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示 设置页面。
2. 在服务器下方，单击移动服务提供商。此时将显示移动服务提供商页面。



3. 配置以下设置：
   - **Web** 服务 **URL**：键入 Web 服务的 URL，例如 `https://XmmServer/services/xdmservice`。
   - 用户名：以 `domain\\admin` 格式键入用户名。
   - 密码：键入密码。
   - 自动更新黑莓和 **ActiveSync** 设备连接：选择是否自动更新设备连接。默认值为关
   - 单击测试连接以验证连接性。
4. 单击保存。

报告

December 3, 2021

Endpoint Management 提供以下预定义报告，您可以利用这些报告分析应用程序和设备部署情况。每个报告都显示为一个表格和一个图表。您可以按列对表格进行排序和过滤。可以从更加详细的信息中选择图表中的元素。

- 总应用程序部署尝试次数：列出用户尝试在其设备上安装的已部署应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 应用程序 **(**按平台**)**：按设备平台和版本列出应用程序和应用程序版本。
- 应用程序 **(**按类型**)**：按版本、类型和类别列出应用程序。
- 设备注册：列出所有已注册的设备。
- 设备和应用程序：列出正在运行托管应用程序的设备。
- 不活动设备：在 Endpoint Management 服务器属性 `device.inactivity.days.threshold` 指定的天数内没有任何活动的设备的列表。
- 已越狱/获得 **Root** 权限的设备：列出已越狱的 iOS 设备和已获得 Root 权限的 Android 设备。
- 条款和条件：列出接受条款和条件协议以及拒绝条款和条件协议的用户。可以选择图表的各个区域以查看更多详细信息。
- 排名前 **10** 的失败部署： - 最多列出 10 个部署失败的应用程序。
- 被设备和用户阻止的应用程序：列出用户的设备上的阻止列表中的应用程序。
- 不合规设备：列出不符合合规性标准的设备。标准包括设备是否越狱、正在运行的操作系统版本以及设备是否具有通行码。该报告还显示与设备关联的用户名以及设备是否已加密。对于 iOS 设备，加密列将显示“N/A”（不适用）。

可以使用.csv 格式导出每个表格中的数据，这些数据在 Microsoft Excel 等程序中打开。可以使用 PDF 格式导出每个报告的图表。

报告选项卡包含设备详细信息，例如序列号、IMEI/MEID、应用程序和连接。有关特定设备的更全面的报告，请转到管理 **>** 设备，单击该设备，单击显示更多，然后查看设备详细信息页面。设备详细信息页面列出了设备安全属性、设备属性、分配的策略、应用程序、操作、证书等。有关设 备详细信息页面的信息，请参阅 获取有关设备的信息。

以下几个方面决定了 Endpoint Management 如何收集与部署到托管设备或安装在托管设备上的应用程序有关的信息。

- 设备类型
- 注册方法
- 是否部署了 应用程序清单设备策略

对于 Android 设备，行为因设备类型和注册方法而异。下表显示了列出适用于 **Android Enterprise** 的应用程序的位置（设备详细信息页面、报告或不可用）。除非另有说明，否则应用程序列表将包括所有应用程序。

	MDM+MAM（所有应用程序）	MDM（所有应用程序）
可选应用程序（未部署“应用程序清单”策略）	设备详细信息页面和报告	公共应用程序；设备详细信息页面和报告
可选应用程序（未部署“应用程序清单”策略）	不可用	不可用
必需的应用程序（已部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

	MDM+MAM（所有应用程序）	MDM（所有应用程序）
可选应用程序（已部署“应用程序清单”策略）	企业应用程序、MDX 应用程序、公共应用程序和 Web 链接应用程序；报告	设备详细信息页面和报告

下表显示了列出适用于 **Android**（旧版 **DA**）的应用程序的位置（设备详细信息页面、报告或不可用）。除非另有说明，否则应用程序列表将包括所有应用程序。

	MDM+MAM（所有应用程序）	MDM（公共应用程序和企业应用程序）	MAM
可选应用程序（未部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	不适用
可选应用程序（未部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	不可用
必需的应用程序（已部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	不适用
可选应用程序（已部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	不可用

对于 iOS 设备，行为因注册方法而异。下表显示了列出应用程序的位置（设备详细信息页面或报告）。除非另有说明，否则应用程序列表将包括所有应用程序。

	MDM+MAM（所有应用程序）	MDM（公共应用程序和企业应用程序）	MAM（所有应用程序）
可选应用程序（未部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	设备详细信息页面和报告；这些应用程序将显示为处于挂起状态（即使未安装）或手动安装后仍处于挂起状态。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

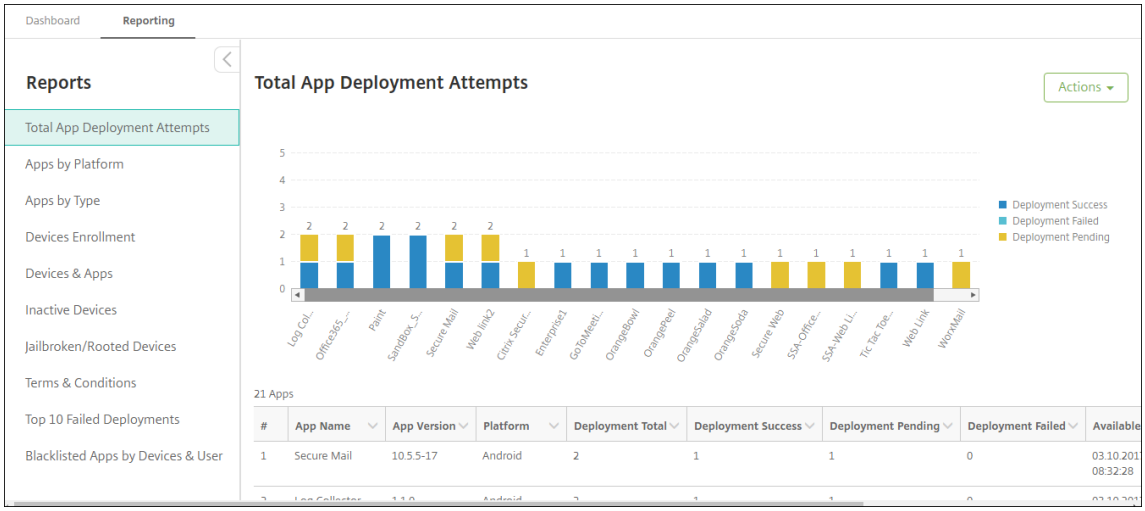
	MDM+MAM（所有应用程序）	MDM（公共应用程序和企业应用程序）	MAM（所有应用程序）
可选应用程序（未部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	Web、SaaS 和 Web 链接应用程序在设备详细信息页面上作为已安装的应用程序列出；这些旖旎公用程序不在报告中列出。手动安装企业应用程序、MDX 应用程序和公共应用程序后，这些应用程序不会在设备详细信息页面上列出。手动安装应用程序后，这些应用程序不会在报告中列出。
必需的应用程序（已部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	无法将“应用程序清单”策略部署到设备。应用程序在设备详细信息页面和报告中列出。这些应用程序显示为处于挂起状态（即使未安装）或手动安装后仍处于挂起状态。
可选应用程序（已部署“应用程序清单”策略）	设备详细信息页面和报告	设备详细信息页面和报告	无法将“应用程序清单”策略部署到设备。Web、SaaS 和 Web 链接应用程序在设备详细信息页面上作为已安装的应用程序列出；这些旖旎公用程序不在报告中列出。手动安装企业应用程序、MDX 应用程序和公共应用程序后，这些应用程序不会在设备详细信息页面上列出。手动安装应用程序后，这些应用程序不会在报告中列出。

对于 macOS 和 Windows 设备，Endpoint Management 仅在部署应用程序清单策略时收集应用程序清单。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

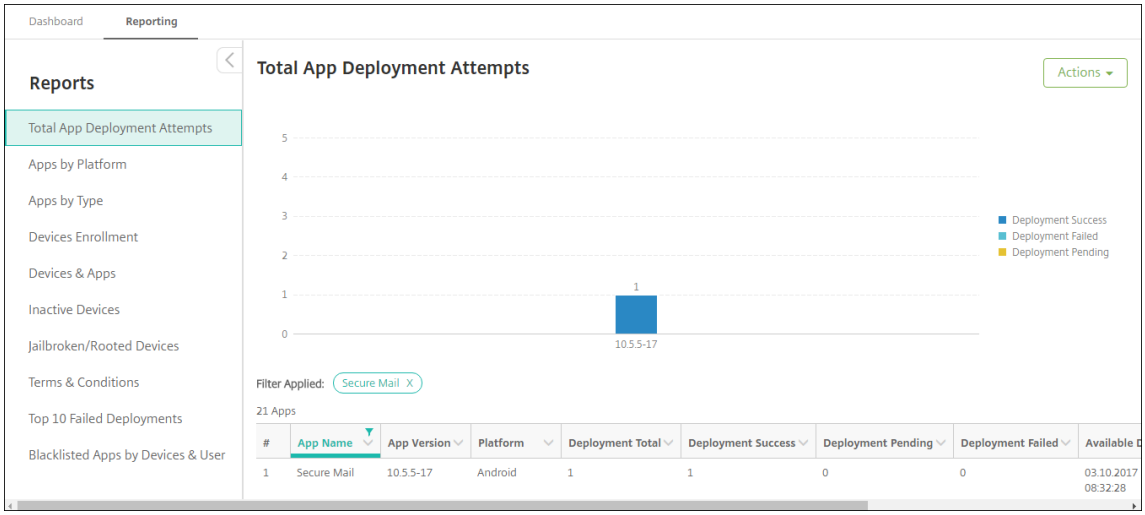
生成报告

1. 在 Endpoint Management 控制台中，单击分析 **>** 报告。此时将显示报告页面。
2. 单击要生成的报告。



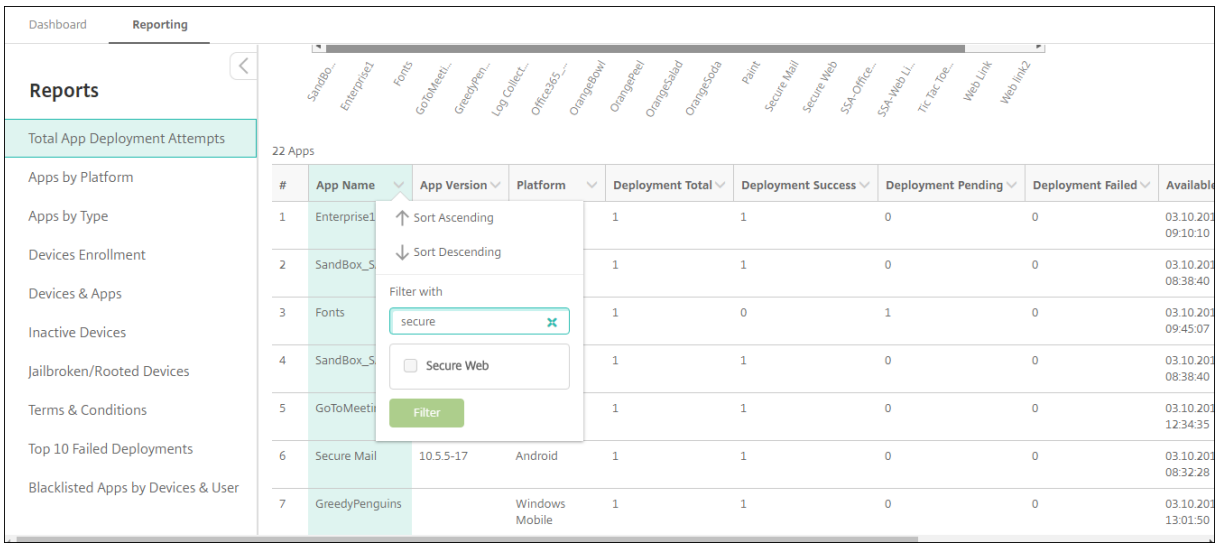
查看报告的更多详细信息

1. 单击图表的各个区域以深入查看更多详细信息。



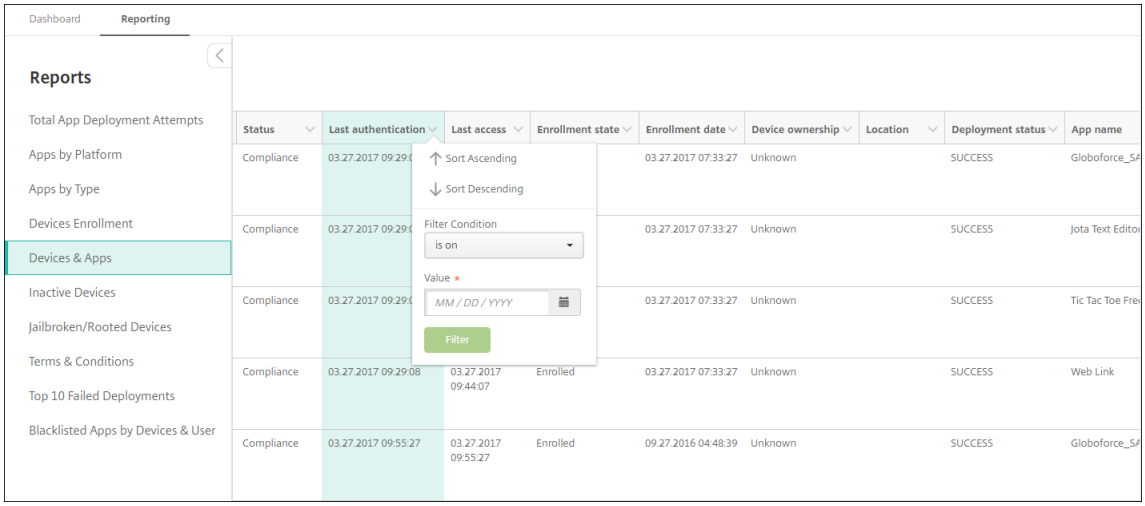
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要对表格列进行排序、过滤或搜索，请单击列标题



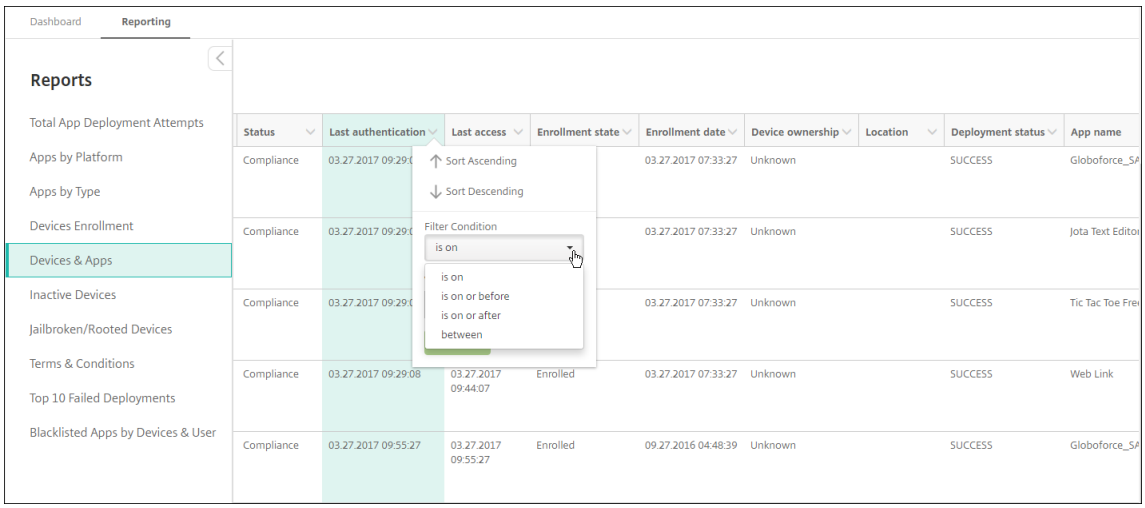
按日期过滤报告

1. 单击列标题以查看过滤设置。

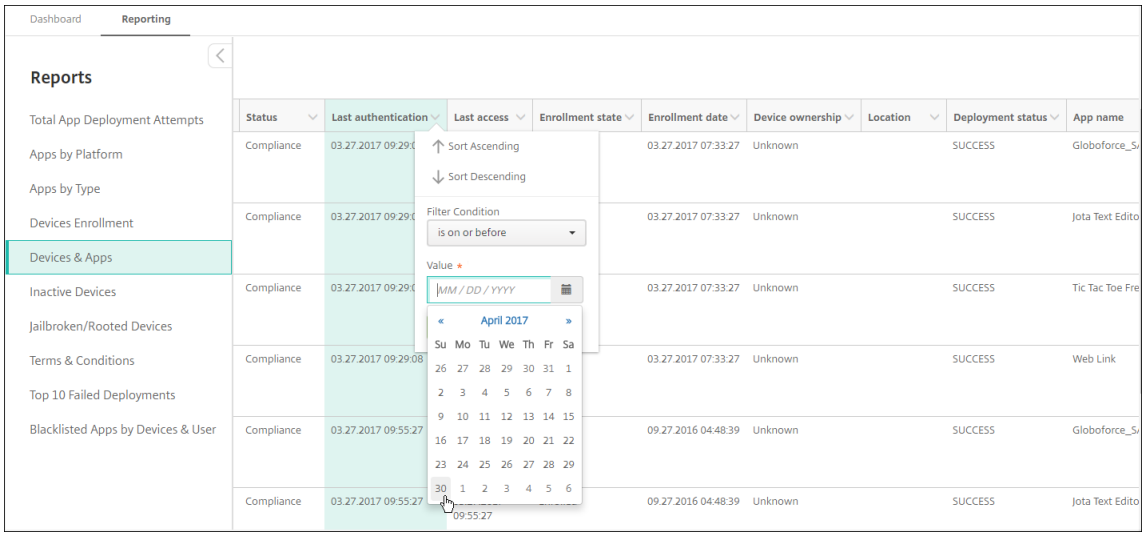


2. 在过滤条件中，选择要限制报告的日期的方式。

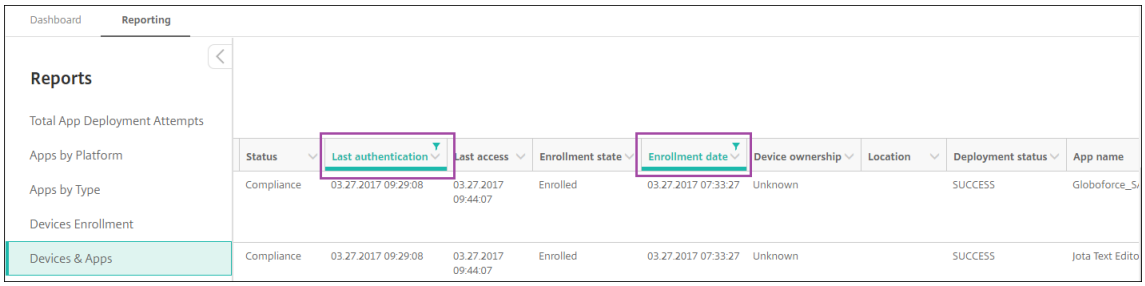
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 使用日期选择器指定日期。

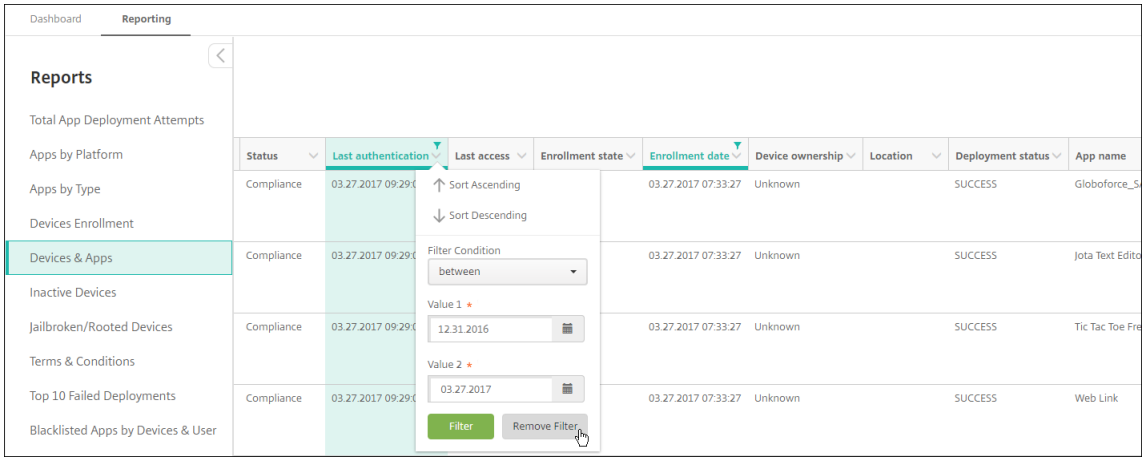


4. 带日期过滤器的列将按以下示例所示进行显示。



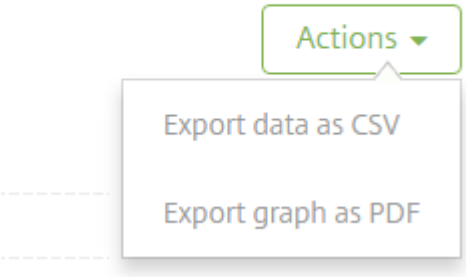
5. 要删除过滤器，请单击列标题，然后单击删除过滤器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



导出图表或表格

- 要导出 PDF 格式的图表，请依次单击操作和将图表导出为 **PDF**。
- 要导出 CSV 格式的表格数据，请依次单击操作和将数据导出为 **CSV**。



REST API

October 18, 2022

使用 Endpoint Management REST API，您可以：

- 调用 Endpoint Management 控制台中显示的服务
- 使用任意 REST 客户端调用 REST 服务

API 不要求您登录 Endpoint Management 控制台即可调用这些服务。

有关完整的当前可用 API 集，请下载适用 于 REST 服务的公共 API PDF。

对于启用了工作空间的 Endpoint Management 环境，我们有 API 来管理移动和桌面端点设备以及为 Workspace

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序配置设置。转到 https://developer.cloud.com/citrixworkspace 并导航到 **Citrix Endpoint Management > 移动应用程序集成**。

访问 **REST API** 所需的权限

访问 REST API 需要具有以下权限：

- Citrix Cloud 管理员
- 公共 API 访问权限，设置为基于角色的访问配置的一部分。有关信息，请参阅使用 RBAC 配置角色。
- 超级用户权限

要使用 Citrix Cloud 帐户访问 REST API，请生成 API 密钥：

1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
2. 选择 **API** 访问 **>** 安全客户端。
3. 键入安全客户端的名称，然后单击 创建客户端。

然后，Citrix Cloud 会创建安全的客户端 ID 和客户端密钥。下载此信息的副本并将其安全地离线保存以供参考。关闭对话框后，Citrix Cloud 不会存储唯一标识符。

调用 **REST API** 服务

您可以使用 REST 客户端或 cURL 命令调用 REST API 服务。以下示例使用适用于 Chrome 的高级 REST 客户端。

> 注意：
>
> 在下面的示例中，请更改主机名和端口号以匹配您的环境。

登录

此处显示的示例介绍了使用通过 Citrix Cloud API 检索的令牌登录。

URL:`https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

方法类型：POST

内容类型：application/json

索取样品：

```
{

 "bearerToken": "eyJ0eOiJSUzJiibGcI1AiONiJ9.
    eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"
 }

<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

您必须使用 Citrix Cloud API `https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients` 检索不记名令牌。有关信息，请参阅 开发人员文档。

响应示例：

```
{

 "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
 }

<!--NeedCopy-->
```

相关信息

- Endpoint Management REST API

ActiveSync Gateway

November 7, 2022

ActiveSync 是 Microsoft 开发的移动数据同步协议。ActiveSync 与手持设备和台式（便携式）计算机同步数据。

可以在 Endpoint Management 中配置 ActiveSync Gateway 规则。ActiveSync Gateway 保留在 Endpoint Management 中配置的所有设备的 ActiveSync ID 列表。根据您配置的规则，您可以根据这些 ActiveSync ID 允许或拒绝设备访问 ActiveSync 数据。例如，如果激活规则缺少所需的应用程序，Endpoint Management 将检查所需应用程序的应用程序访问策略。如果缺少所需的应用程序，该策略将拒绝访问 ActiveSync 数据。对于每个规则，可以选择允许或拒绝。默认设置为允许。

有关应用程序访问设备策略的详细信息，请参阅应用程序访问设备策略。

Endpoint Management 支持以下规则：

匿名设备：检查设备是否处于匿名模式。如果在设备尝试重新连接时 Endpoint Management 无法重新对用户进行身份验证，则可以执行此检查。

禁止的应用程序：检查设备是否具有应用程序访问策略中定义的禁止的应用程序。

隐式允许和拒绝：这是 ActiveSync Gateway 的默认操作。网关创建不满足其他任何过滤器规则条件的所有设备的设备列表。然后，网关将根据该列表允许或拒绝连接。如果任何规则均不匹配，则默认为隐式允许。

不活动设备：按照服务器属性中的 **Device Inactivity Days Threshold**（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。

缺少所需的应用程序：检查设备是否缺少在应用程序访问策略中定义的所需应用程序。

非推荐应用程序：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

不合规密码：检查用户密码是否合规。在 iOS 和 Android 设备上，Endpoint Management 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。例如，在 iOS 设备上，如果 Endpoint Management 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规设备”属性检查设备是否不合规。使用 Endpoint Management API 的自动操作或第三方通常会更改该属性。

吊销状态：检查设备证书是否已吊销。再次授权之前，已吊销的设备无法重新注册。

已获得 **root** 权限的 **Android** 设备和已越狱的 **iOS** 设备：检查 Android 设备或 iOS 设备是否已被越狱。

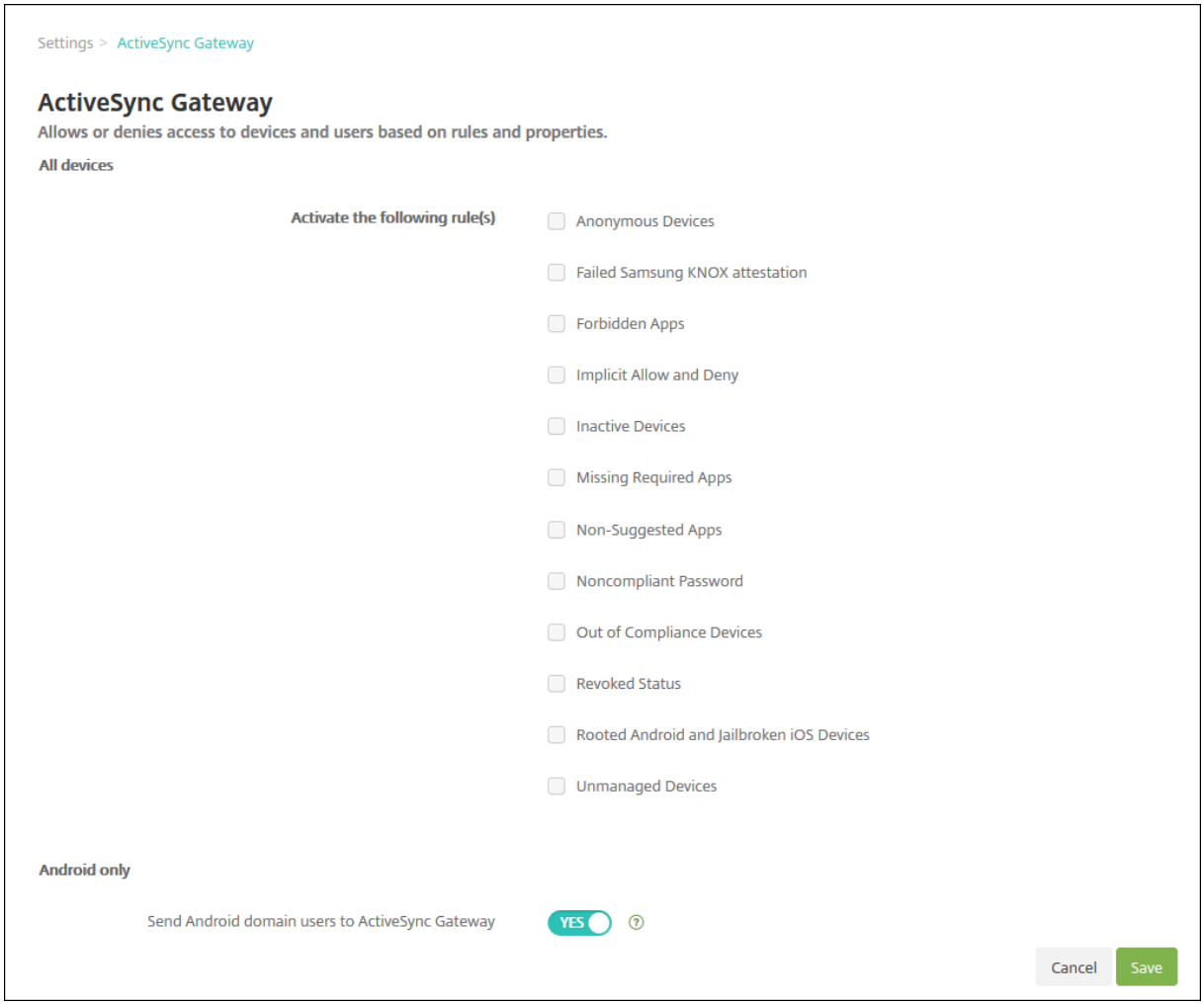
非托管设备：检查设备是否仍处于托管状态，受 Endpoint Management 控制。例如，在 MAM 下注册的设备或已取消注册的设备为非托管设备。

将 **Android** 域用户发送到 **ActiveSync Gateway**：单击是使 Endpoint Management 将 Android 设备所有者的用户名和 ActiveSync ID 发送到 ActiveSync Gateway。除非您正在运行旧配置，否则请关闭此功能。在最新的配置中，只要网关上存在与设备关联的用户名，此功能就允许任何设备访问 ActiveSync 数据。

配置 **ActiveSync Gateway** 设置

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **ActiveSync Gateway**。此时将显示 **ActiveSync Gateway** 页面。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



1. 在激活以下规则中，选择要激活的一个或多个规则。
2. 在仅限 **Android** 中的将 **Android** 域用户发送到 **ActiveSync Gateway** 中，单击是以确保 Endpoint Management 将 Android 设备信息发送到 ActiveSync Gateway。
3. 单击保存。

适用于 **Exchange ActiveSync** 的 **Endpoint Management** 连接器

July 8, 2022

XenMobile Mail Manager 现已更名为适用于 Exchange ActiveSync 的 Endpoint Management 连接器。有关 Citrix 统一产品组合的详细信息，请参阅 Citrix 产品指南。

连接器通过以下方法扩展 Endpoint Management 的功能：

- 用于 Exchange ActiveSync (EAS) 设备的动态访问控制。可以自动允许或阻止 EAS 设备访问 Exchange 访问。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 使 Endpoint Management 能够访问 Exchange 提供的 EAS 设备合作信息的功能。
- Endpoint Management 能够根据 EAS 状态擦除移动设备。
- 使 Endpoint Management 能够访问关于黑莓设备的信息以及执行擦除和重置密码等控制操作的功能。

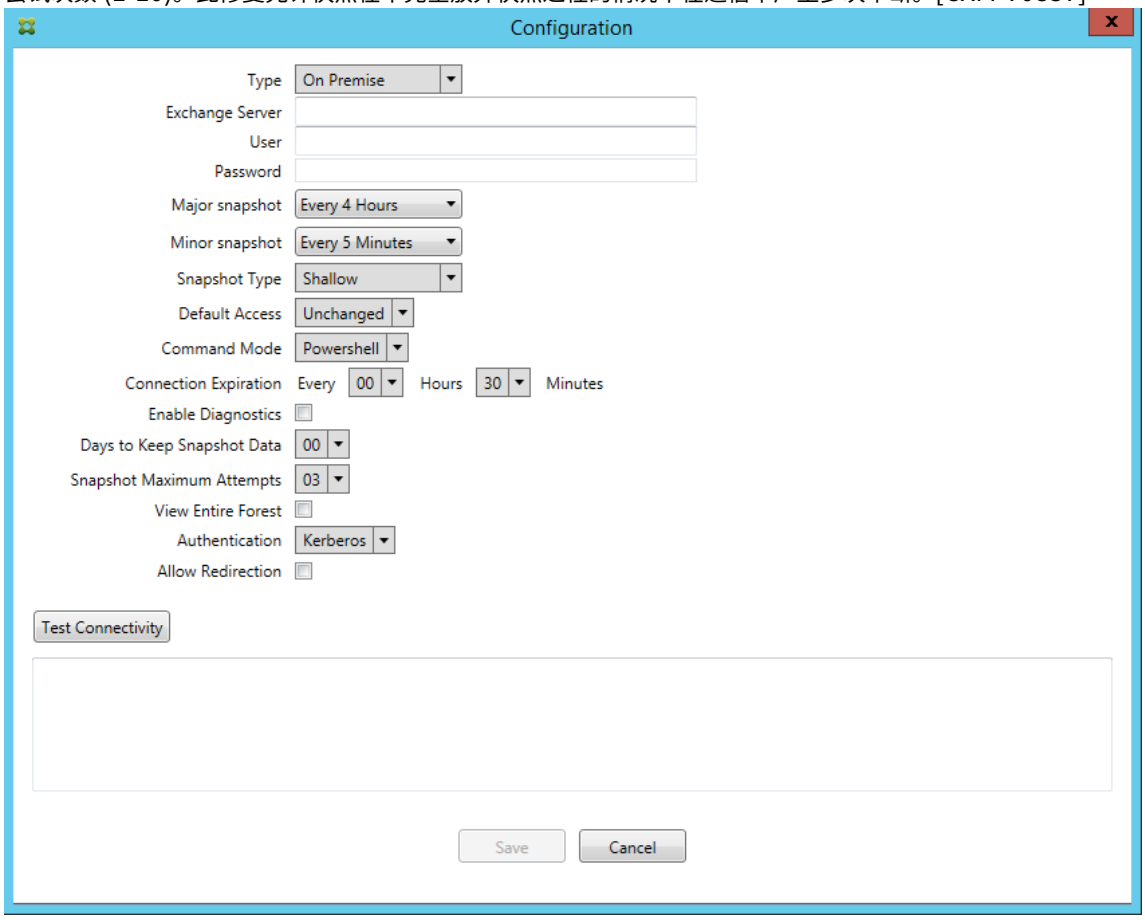
要根据 EAS 状态擦除设备，请使用 ActiveSync 触发器配置自动操作。请参阅自动化操作。

> 重要：
>
> 鉴于 Microsoft 在此处宣布的身份验证更改，自 2022 年 10 月起，适用于 Exchange ActiveSync 的 Endpoint Management 和 Citrix Gateway 连接器将不再支持 Exchange Online。适用于 Exchange 的 Endpoint Management 连接器将继续与 Microsoft Exchange Server（本地）结合使用。

版本 **10.1.10** 中的新增功能

10.1.10 版中修复了以下问题：

- 遇到频繁出现的网络问题的客户可能无法在之前提供的三次尝试中完成快照。在本版本中，管理员可以配置最大尝试次数 (1-10)。此修复允许快照在不完全放弃快照过程的情况下在通信中产生多次中断。[CXM-70837]



- 在早期版本中，快照类型未显示在 Exchange 配置列表中。现在，快照类型则显示在该位置。[CXM-70846]
- PowerShell 报告的 PSRemotingTransport 异常表示与 Exchange 的会话不再可行。默认情况下，状态将添加到配置文件中的“严重错误”列表中。这样，当检测到 PSRemotingTransport 异常时，连接被标记为错

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

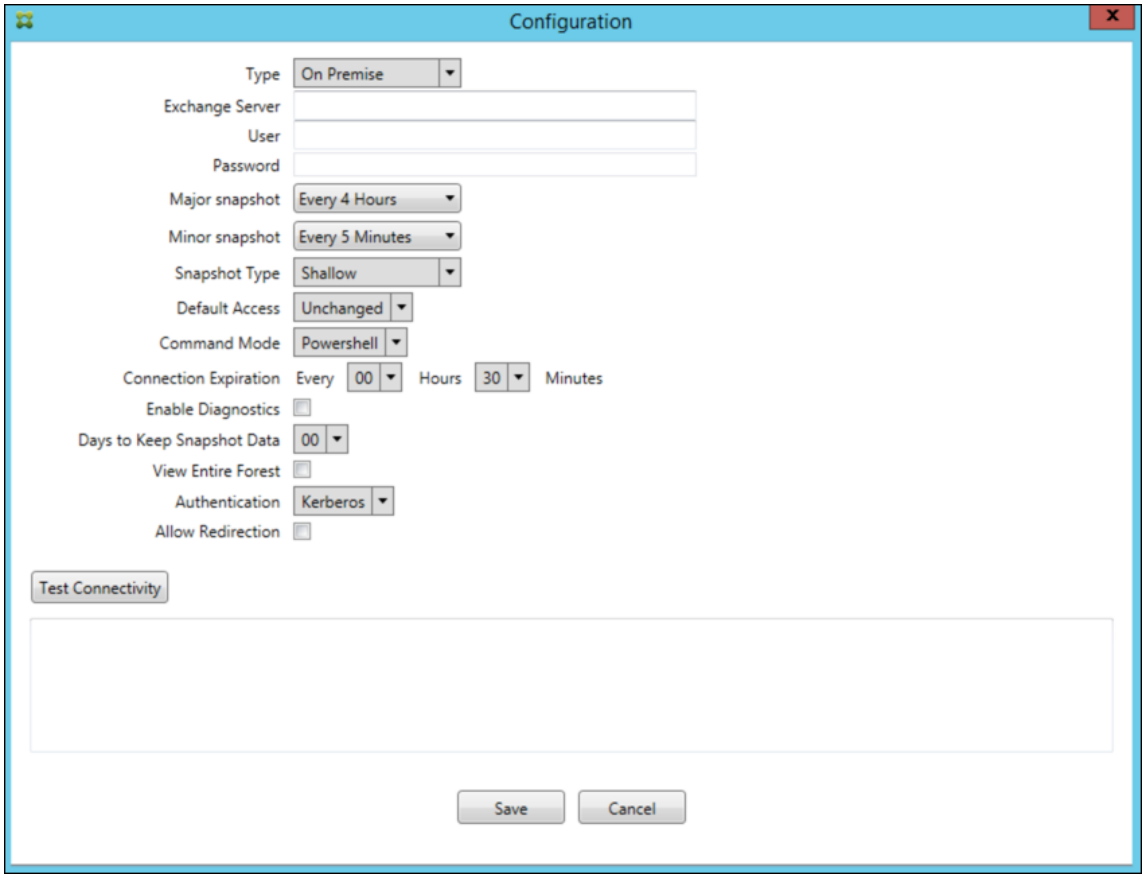
误以供稍后处理。下一个通信使用有效的连接或创建连接。[XMHELP-2184、CXM-70836]

- 保存配置更改后，在加载新配置之前，可能并非所有之前配置的内部组件都已正确处理。此问题可能会导致出现不可预测的行为。该行为取决于特定的更改以及该更改是否与之前的配置冲突。在本版本中，所有内部组件都会在加载新配置之前处理。[XMHELP-2259、CXM-71388]

版本 **10.1.9** 中的新增功能

版本 10.1.9 中修复了以下问题：

- 现在，对配置所做的更改将以更加一致的方式进行处理。当服务检测到配置中的更改时，每个内部子系统都将停止运行，这意味着任何活动的或计划的处理过程都会中断。接下来将加载新配置并重新启动子系统，这意味着将使用新设置重新建立所有计划以及其他内部基础结构。此问题更正了版本 10.1.8 中的一个已知问题。[CXM-47709、CXM-61330]
- 在升级期间，现有数据库配置不合并到新配置文件。现在，数据库配置将合并到升级后的配置文件。[CXM-49326]
- 在快照相关的诊断文件中，列标题缺失。这些标题都将还原。[CXM-62680]
- 从早期版本升级时，配置文件的默认设置部分被正在使用的配置文件中的类似部分覆盖。此问题阻止了服务在升级后加载在默认设置部分中添加或改进的功能。截至本版本，默认设置部分始终反映最新配置。[CXM-62681]
- 运行应用程序时，管理员将无法再通过按 Shift 键访问某些选项。这些选项以前是随 Citrix 权限提供的。现在，某些选项已完全可用（例如“允许重定向”），其他选项（例如，挂起检测和计数更正）已弃用。[CXM-62767]



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

早期版本中的新增功能

下面的部分列出了适用于 Exchange ActiveSync 的 Endpoint Management 连接器的早期版本中的新增功能和已修复的问题。

版本 **10.1.8** 中的新增功能

- Exchange 有可能会降低适用于 Exchange ActiveSync 服务的 Citrix Endpoint Management 连接器的速度，使其发出命令不会太频繁。此问题在与 Office 365 的连接中很常见。此限制产生的影响要求该服务先暂停指定的期限，然后再发送下一个命令。配置控制台现在显示剩余的暂停时间量。[CXM-48044]
- 修改了配置文件 (config.xml) 的 “Watchdog” 和/或 “SpecialistsDefaults” 部分时，所做的更改在升级后不反映在配置文件中。在本版本中，修改正确地合并到新配置文件中。[CXM-52523]
- 更多详细信息已添加到发送至 Google Analytics 的分析中，特别是相关的快照。[CXM-56691]
- Exchange 测试连接功能将仅尝试初始化连接一次。由于可以限制 Office 365 的连接，因此，受到限制时，测试连接可能会显示为失败。适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器现在最多尝试初始化连接三次。[CXM-58180]
- 为影响有关 Exchange 的策略，适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器必须将包括每个邮箱的所有相关设备的 **Set-CASMailbox** 命令编译到两个列表中，即允许和阻止列表。如果设备未包含在这两个列表中，Exchange 将回退到其默认访问状态。如果该默认访问状态与设备的所需状态不同，设备将变得不合规。因此，如果 Exchange 默认访问状态为阻止，但实际应为允许，用户可能会丢失对其电子邮件的访问权限。或者，应阻止其访问电子邮件的用户可能会被授予访问权限。适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器现在将确保具有有效所需状态的所有设备都包括在每个 **Set-CasMailbox** 命令中。[CXM-61251]

以下问题在版本 10.1.8 中属于已知问题：

如果管理员在配置应用程序中做出了修改配置数据的更改，而服务正在执行长时间持续进行的操作，例如快照或策略评估，服务可能会进入不确定的状态。可能会出现的症状可能为不处理策略更改，或者不启动快照。必须重新启动服务，才能将服务返回到工作状态。在启动服务之前，您可能需要使用 Windows 服务管理器终止服务。[CXM-61330]

版本 **10.1.7** 中的新增功能

- XenMobile Mail Manager 现已更名为适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
- 我们已弃用 Exchange 配置对话框中的 **Disable Pipelining**（禁用流水线操作）选项。可以在 config.xml 文件中为每个命令配置多个步骤来实现相同功能。[CXM-54593]

版本 10.1.7 中修复了以下问题：

- 在 “Snapshot History”（快照历史记录）窗口中，显示的错误消息可能几乎没有上下文。现在，错误消息的前缀为错误发生位置的上下文。[CXM-49157]
- XmmGoogleAnalytics.dll 没有与版本对应的文件版本。[CXM-52518]
- 为了改进诊断，我们最近更改了用于为邮箱设置 “允许/阻止” 状态的设备 ID 列表的字符串格式。但是，指定的设备太多会超过最大字符串大小。现在，我们使用内部数组数据结构。此结构没有大小限制，并且还会为数据设

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

置合适格式以便用于诊断。[CXM-52610]

- 检测到未与 Exchange 同步的设备策略时，其命令可能包括不属于相关邮箱的设备。适用于 Exchange ActiveSync 的 Endpoint Management 连接器现在可确保针对 Exchange 的命令仅表示属于其各自邮箱的设备。[CXM-54842]
- 在某些环境中，Microsoft 程序集不可用。现在，所需的程序集明确与应用程序一起安装。[CXM-55439]
- 如果设备或邮箱的标识名中属性名称与等号之间有空格，或等号后面与值前面有空格，适用于 Exchange ActiveSync 的 Endpoint Management 连接器可能无法正确将设备与其邮箱匹配，反之亦然。结果可能是在快照协调期间某些设备和/或邮箱被拒绝。[CXM-56088]

> 注意：
>
> 下面的“新增功能”部分在提到适用于 Exchange ActiveSync 的 Endpoint Management 连接器时使用其以前的名称 XenMobile Mail Manager。名称自版本 10.1.7 起更改。

版本 **10.1.6.20** 中的更新

10.1.6 更新包含版本 10.1.6.20 中的以下修复：

- 检测到未与 Exchange 同步的设备策略时，其命令可能包括不属于相关邮箱的设备。XenMobile Mail Manager 现在可确保针对 Exchange 的命令仅表示属于其各自邮箱的设备。[CXM-54842]

版本 **10.1.6** 中的新增功能

XenMobile Mail Manager 版本 10.1.6 包含以下已修复的问题和增强功能：

- “Snapshot History”（快照历史记录）窗口有时会进入窗口不再更新的状态。改进了窗口刷新机制以更加可靠地更新。[CXM-47983]
- 对分区快照和非分区快照使用两个不同的模式和代码路径。由于非分区快照等同于使用单个“*”分区配置的分区快照，因此不需要非分区快照模式。现在，默认快照模式为具有 36 个分区（0-9、A-Z）的分区快照。[CXM-49093]
- 在“Snapshot History”（快照历史记录）窗口中，错误消息会被状态消息覆盖。现在，XenMobile Mail Manager 提供两个单独的字段，以便用户可以同时查看状态和错误。[CXM-51942]
- 连接到 Exchange Online (Office 365) 时，快照相关查询可能会导致数据集被截断。XenMobile Mail Manager 执行多命令流水线脚本时，可能会出现此问题。上游命令无法足够快速地将数据传递给下游命令，这样下游命令就会提前完成工作。因此会出现不完整的数据。现在，XenMobile Mail Manager 可以模仿流水线本身，并等到上游命令完成后再调用下游命令。经过此更改，所有数据都将得以处理和捕获。[CXM-52280]
- 如果在针对 Exchange 的策略更新命令中发生无法解决的错误，则会在很长一段时间内重复向工作队列返回相同命令。这种情况会导致多次向 Exchange 发送该命令。在此版本的 XenMobile Mail Manager 中，仅偶尔向工作队列返回导致出现错误的命令。[CXM-52633]
- 如果针对特定邮箱的策略更新涉及允许或阻止所有设备：由于空列表被转换为空字符串而不是 **NULL**，发出的 **Set-CASMailbox** 命令会失败。现在会发送正确的数据。[CXM-53759]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 处理新设备时，Exchange 可能会在一段时间（通常为 15 分钟）内返回状态 “DeviceDiscovery”。以前，XenMobile Mail Manager 不会专门处理这种状态。现在，XenMobile Mail Manager 会处理这种状态。在 UI 的 “Monitor”（监视）选项卡中，用户可以过滤处于此状态的设备。[CXM-53840]
- 以前，XenMobile Mail Manager 不会检查是否能够向 XenMobile Mail Manager 数据库执行写入操作。因此，如果权限受到限制，则可能无法预测该行为。现在，XenMobile Mail Manager 会从数据库捕获并验证所需的权限。XenMobile Mail Manager 会在测试连接时（显示的消息）或在主配置窗口底部的数据库指示器（悬停显示消息）中指示降低的权限。[CXM-54219]
- 根据当前工作负载，在被定向时，XenMobile Mail Manager 服务可能无法迅速停止。因此，该服务看上去处于无响应状态。进行了一些改进后，正在进行的任务可以中断，因而可以比较正常地关闭。[CXM-54282]

版本 **10.1.5** 中的新增功能

XenMobile Mail Manager 版本 10.1.5 包含以下已修复的问题：

- Exchange 向 XenMobile Mail Manager 活动应用限制时，系统不会指示（在日志外部）发生了限制。在此版本中，用户可以将鼠标悬停在活动快照上，此时将显示 “限制” 状态。此外，XenMobile Mail Manager 受到限制时，在 Exchange 解除限制禁令之前，会禁止开始创建主要快照。[CXM-49617]
- 如果在创建主要快照期间 XenMobile Mail Manager 受到 Exchange 限制：可能是在下一次尝试创建快照之前，可以使用的时间不够。此问题会导致进一步限制和快照失败。现在，XenMobile Mail Manager 会在两次快照尝试之间等待 Exchange 指定的最小等待时间。[CXM-49618]
- 启用了诊断时，命令文件中显示的 **Set-CasMailbox** 命令中，每个属性名称前面都缺少连字符。仅在设置诊断文件的格式时会发生此问题，发送到 Exchange 的实际命令则不会发生此问题。由于缺少连字符，用户无法剪切命令并直接将其粘贴到 PowerShell 命令提示窗口进行测试或验证。现已添加连字符。[CXM-52520]
- 如果邮箱标识的格式为 `lastname， firstname`，在从查询返回数据时，Exchange 会在逗号前面添加一个反斜杠。XenMobile Mail Manager 使用该标识查询更多数据时，必须去掉此反斜杠。[CXM-52635]

已知限制

> 注意：
>
> 以下限制在版本 10.1.6 中已解决。

XenMobile Mail Manager 存在一个可能会导致针对 Exchange 的命令失败的已知限制。为了向 Exchange 应用策略更改，XenMobile Mail Manager 会发出 **Set_CASMailbox** 命令。此命令可以接受两个设备列表：一个要允许的列表和一个要阻止的列表。此命令应用于与邮箱关联使用的设备。

这些列表不能超过 256 个字符（按 Microsoft API 划分的每个列表）。如果其中一个列表超过该限制，命令将完全失败，导致无法为与相应邮箱关联的设备设置策略。报告的错误（显示在 XenMobile Mail Manager 日志中）类似如下所示。下面是阻止的列表示例。

“Message:’Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’ to the target. Exception setting “ActiveSyncBlockedDeviceIDs”: “The length of the property is too long. The maximum length is 256 and

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

the length of the value provided is …""（消息: 无法将参数 ActiveSyncBlockedDeviceIDs 绑定到目标。设置 ActiveSyncBlockedDeviceIDs 时发生异常:"属性的长度太长。最大长度为 256，提供的值长度为…"）

设备 ID 长度可能会有所差别，但一条很好的指导原则是，同时允许或阻止大约 10 个或更多设备可能会超过该限制。虽然很少会出现许多设备与某个特定邮箱关联，但仍有可能出现。在 XenMobile Mail Manager 改进为能够处理此情况之前，我们建议您将与一个用户和邮箱关联的设备数限制在 10 以内。[CXM-52633]

版本 **10.1.4** 中的新增功能

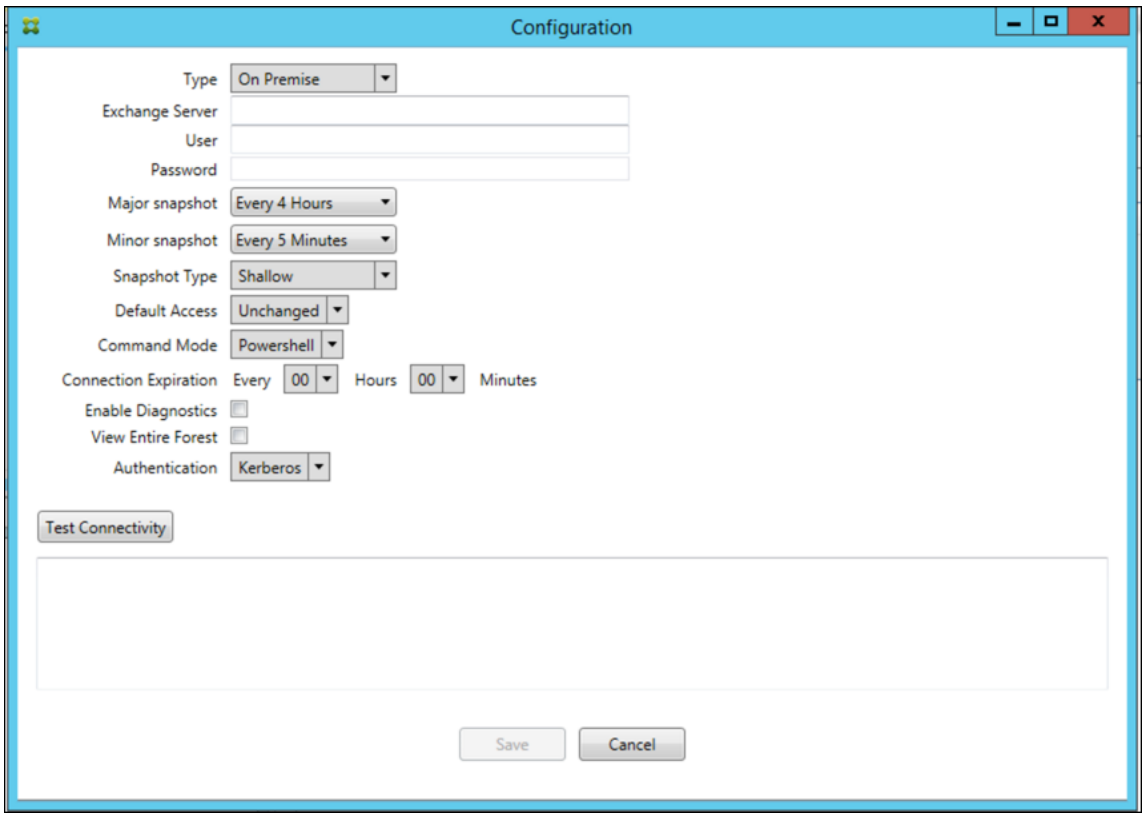
XenMobile Mail Manager 版本 10.1.4 包含以下已修复的问题：

- 由于安全性的削弱，PCI 委员会正在弃用 TLS 1.0 和 TLS 1.1。对 1.2 的支持已添加到 XenMobile Mail Manager 中。[CXM-38573、CXM-32560]
- XenMobile Mail Manager 包括一个新的诊断文件。在 Exchange 指定内容中选择了 **Enable Diagnostics**（启用诊断）时，将生成新的快照历史记录文件。在每次尝试创建快照时，都会向该文件中添加一行以记录快照结果。[CXM-49631]
- 在命令诊断文件中，**Set-CASMailbox** 命令不显示允许或阻止的设备列表。而是在该文件中的相关参数中显示内部类名称。现在，XenMobile Mail Manager 以逗号分隔的列表显示设备 ID 的列表。[CXM-50693]
- 由于指定内容错误导致尝试获取与 Exchange 的连接失败时：不正确的消息覆盖错误消息："All connections in use"（正在使用所有连接）。现在显示更具描述性的消息，例如，"All connections are inoperable"（所有连接均无法使用）、"Connection pool is empty"（连接池为空）、"All connections are throttled"（所有连接都受限制），以及 "No available connections"（没有可用的连接）。[CXM-50783]
- 有时，允许/阻止/擦除命令会在 XenMobile Mail Manager 内部缓存中排队多次。此问题导致发送到 Exchange 的命令出现延迟。XenMobile Mail Manager 现在仅排队每个命令的一个实例。[CXM-51524]

版本 **10.1.3** 中的新增功能

- **Google Analytics** 支持：我们希望了解您使用 XenMobile Mail Manager 的方式，以便我们可以专注于可以改进产品的方面。
- 用于启用诊断的设置："Configure"（配置）控制台中的 **Configure**（配置）对话框中显示 **Enable Diagnostics**（启用诊断）复选框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



版本 **10.1.3** 中已修复的问题

- 在 **Snapshot History**（快照历史记录）窗口中，显示快照当前状态的工具提示不反映实际状态。[CXM-5570]
- 偶尔，XenMobile Mail Manager 无法向命令诊断文件中写入。发生此问题时，完全不记录命令历史记录。[CXM-49217]
- 某个连接出错时，该连接可能无法标记为“出错”。因此，后续命令可能会尝试使用该连接，并导致出现另一个错误。[CXM-49495]
- 在 Exchange Server 中启用了限制时，可能会在检查运行状况例程中引发异常。因此，可能无法清除出错或已过期的连接。此外，在限制时间到期之前，XenMobile Mail Manager 可能无法创建连接。[CXM-49794].
- 超过 Exchange 的最大会话计数后，XenMobile Mail Manager 报告“Device Capture Failed”（设备捕获失败）错误，此消息并不准确。相反，该消息应指明正在使用 XenMobile Mail Manager 通常用于 Exchange 通信的两个会话。[CXM-49994]

版本 **10.1.2** 中的新增功能

- 改进了与 **Exchange** 的连接： XenMobile Mail Manager 使用 PowerShell 会话与 Exchange 进行通信。尤其是在用于 Office 365 时，PowerShell 会话在一段时间之后可能会变得不稳定，从而阻止后续命令成功运行。现在可以在 XenMobile Mail Manager 中设置连接的过期期限。当连接达到其到期时间时，XenMobile Mail Manager 将正常关闭 PowerShell 会话，并创建一个会话。这样，PowerShell 会话不太可能变得不稳定，从而大大降低快照失败的可能性。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 改进快照工作流程：主要快照是一项耗时且流程密集型操作。如果在创建快照期间发生错误，XenMobile Mail Manager 现在会多次（最多三次）尝试完成快照。后续尝试并不是从头开始。XenMobile Mail Manager 会从其中断的地方继续。此增强功能允许在创建快照期间出现短暂的错误，通常可提高快照的成功率。
- 改进了诊断：现在快照过程中可选地生成三个新的诊断文件，快照操作故障排除变得更加这些文件有助于确定 PowerShell 命令问题、缺少信息的邮箱以及无法与邮箱相关的设备。管理员可以使用这些文件确定 Exchange 中可能不正确的数据。
- 改进了内存使用率： XenMobile Mail Manager 现在可以更高效地使用内存。管理员可以计划 XenMobile Mail Manager 自动重新启动以向系统提供初始状态。
- **Microsoft .NET Framework 4.6** 必备条件：现在，Microsoft.NET Framework 的必备版本现在为版本 4.6。

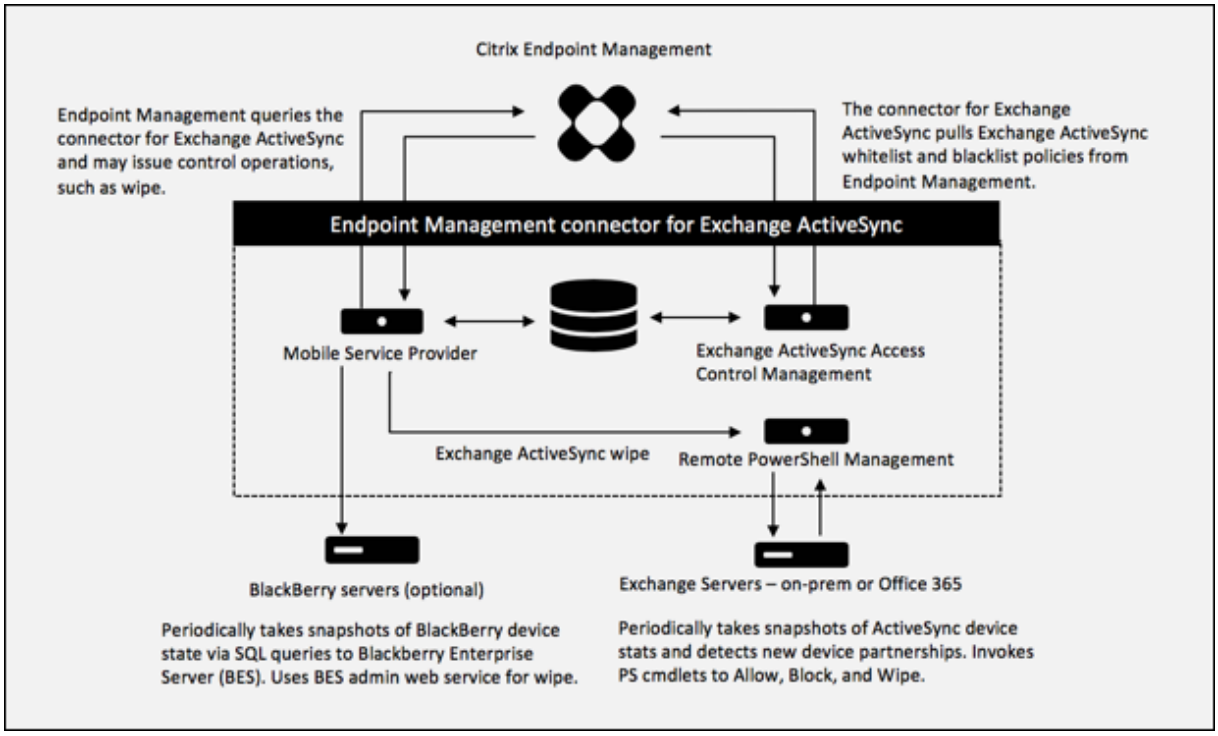
已修复的问题

- 提示输入凭据错误：Office 365 会话不稳定通常会导致此错误。改进了与 Exchange 的连接增强功能解决了该问题。（XMHELP 293、XMHELP 311、XMHELP 801）
- 邮箱和设备计数不准确：XenMobile Mail Manager 改进了邮箱到设备关联算法。改进的诊断功能有助于确定 XenMobile Mail Manager 认为不在其职责领域的邮箱和设备。(XMHELP-623)
- 无法识别允许/阻止/擦除命令：修复了有时无法识别 XenMobile Mail Manager 允许/阻止/擦除命令的缺陷。(XMHELP-489)
- 内存管理：改进了内存管理和缓解。(XMHELP-419)

体系结构

下图显示了适用于 Exchange ActiveSync 的 Endpoint Management 连接器的主要组件。有关详细的参考体系结构图，请参阅体系结构。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



两个主要组成部分是：

- **Exchange ActiveSync** 访问控制管理：与 Endpoint Management 进行通信以从 Endpoint Management 中检索 Exchange ActiveSync 策略，并将此策略与所有本地定义的策略合并以确定应被允许或拒绝访问 Exchange 的 Exchange ActiveSync 设备。本地策略允许扩展策略规则，以允许 Active Directory 组、用户、设备类型或设备用户代理（通常为移动平台版本）执行访问控制。
- 远程 **PowerShell** 管理：负责计划和调用远程 PowerShell 命令，以执行 Exchange ActiveSync 访问控制管理编译的策略。此组件定期创建 Exchange ActiveSync 数据库的快照，以检测新的或已更改的 Exchange ActiveSync 设备。

系统要求和必备条件

使用适用于 Exchange ActiveSync 的 Endpoint Management 连接器需要满足以下最低系统要求：

- Windows Server 2016、Windows Server 2012 R2 或 Windows Server 2008 R2 Service Pack 1。必须是基于英语的服务器。对 Windows Server 2008 R2 Service Pack 1 的支持将于 2020 年 1 月 14 日结束。
- Microsoft SQL Server 2016 Service Pack 2、SQL Server 2014 Service Pack 3 或 SQL Server 2012 Service Pack 4。
- Microsoft .NET Framework 4.6。
- 黑莓 Enterprise Service 版本 5（可选）。

Microsoft Exchange Server 的最低支持版本：

- Microsoft Office 365
- Exchange Server 2016

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Exchange Server 2013
- Exchange Server 2010 Service Pack 3（支持将于 2020 年 1 月 14 日结束）

必备条件

- 必须安装 Windows Management Framework。
  - PowerShell V5、V4 和 V3
- 必须通过 Set-ExecutionPolicy RemoteSigned 将 PowerShell 执行策略设置为 RemoteSigned。
- 必须在运行适用于 Exchange ActiveSync 的连接器的计算机和远程 Exchange Server 之间打开 TCP 端口 80。

设备电子邮件客户端：并非所有电子邮件客户端始终为设备返回相同的 ActiveSync ID。由于适用于 Exchange ActiveSync 的连接器要求每个设备具有唯一的 ActiveSync ID，因此，仅支持为每个设备一致地生成相同的唯一 ActiveSync ID 的电子邮件客户端。这些电子邮件客户端已通过 Citrix 测试，执行时没有错误：

- Samsung 本机电子邮件客户端
- iOS 本机电子邮件客户端

Exchange：运行 Exchange 的本地计算机的要求如下所示：

在 Exchange 配置用户界面中指定的凭据必须能够连接到 Exchange Server，并且具有执行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：

- 针对 **Exchange Server 2010 SP2**：
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- 对于 **Exchange Server 2013** 和 **Exchange Server 2016**：
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 如果将适用于 Exchange ActiveSync 的连接器配置为查看整个林，则必须授权运行 **Set-AdServerSettings -ViewEntireForest $true**
- 提供的凭据必须具有通过远程 Shell 连接到 Exchange Server 的权限。默认情况下，安装 Exchange 的用户具有此权限。
- 要建立远程连接并运行远程命令，凭据必须与远程计算机上的管理员用户相对应。可以使用 Set-PSSessionConfiguration 消除管理要求，但是对该命令的讨论不在本文档的范围内。有关详细信息，请参阅 Microsoft 文章关于会话配置。
- 此外，Exchange Server 还必须配置为支持通过 HTTP 进行的远程 PowerShell 请求。通常，只需要在 Exchange Server 上运行下列 PowerShell 命令的管理员：WinRM QuickConfig。
- Exchange 有许多限制策略。其中一个策略控制每个用户允许的并发 PowerShell 连接的数目。在 Exchange 2010 中，一个用户允许的同时连接数默认为 18。达到连接限制时，适用于 Exchange ActiveSync 的连接器无法连接到 Exchange Server。存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。如果有兴趣，可以通过 PowerShell 调查与远程管理相关的 Exchange 限制策略。

Office 365 Exchange 的要求

- 权限：在 Exchange 配置用户界面中指定的凭据必须能够连接到 Office 365，并且具有运行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- 特权：提供的凭据必须已获得授权，可以通过远程 Shell 连接到 Office 365 服务器。默认情况下，Office 365 联机管理员具有必备特权。
- 限制策略： Exchange 有许多限制策略。其中一个策略控制每个用户允许的并发 PowerShell 连接的数目。在 Office 365 中，一个用户允许的同时连接数默认为三个。达到连接限制时，适用于 Exchange ActiveSync 的连接器无法连接到 Exchange Server。存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。如果有兴趣，可以通过 PowerShell 调查与远程管理相关的 Exchange 限制策略。

安装和配置

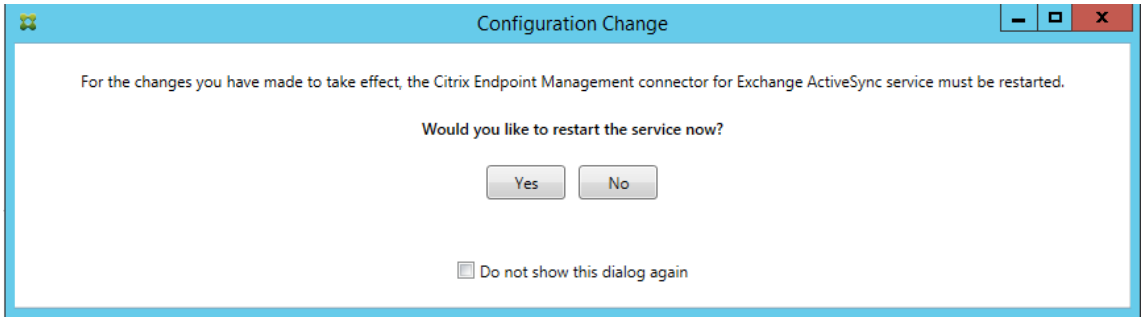
1. 单击 XmmSetup.msi 文件，然后按照安装程序中的提示安装适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
2. 在设置向导的最后一个屏幕中让 **Launch the Configure utility**（启动配置实用程序）保留选中。或者，从

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

开始菜单中，打开适用于 Exchange ActiveSync 的连接器。

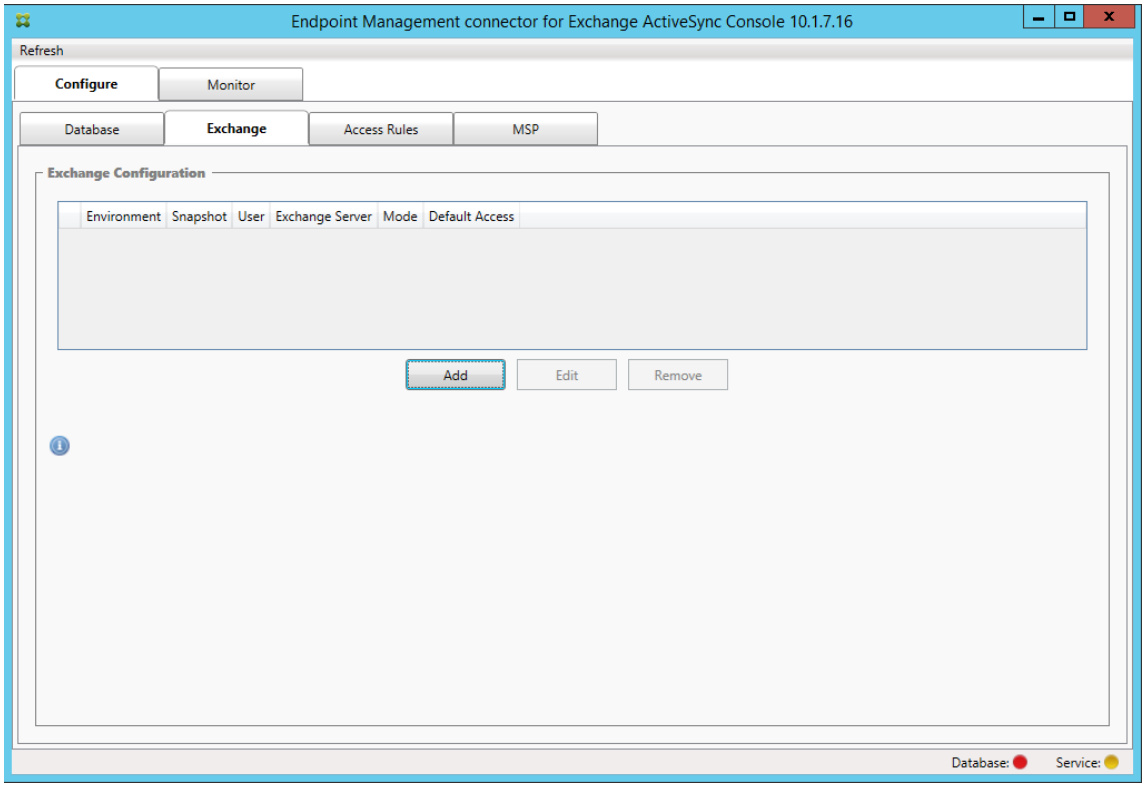
3. 配置以下数据库属性：
   - 选择 **Configure**（配置）**> Database**（数据库）选项卡。
   - 输入 SQL Server 的名称（默认值为 localhost）。
   - 将数据库保留为默认 **CitrixXmm**。
4. 选择以下用于 SQL 的身份验证模式之一：
   - **SQL**：输入有效 SQL 用户的用户名和密码。
   - **Windows Integrated**（**Windows** 集成）：如果选择此选项，XenMobile Mail Manager Service 的登录凭据必须更改为具有访问 SQL Server 权限的 Windows 帐户。为此，请打开控制面板 **>** 管理工具 **>** 服务，在 XenMobile Mail Manager Service 条目上单击鼠标右键，然后单击登录选项卡。

   如果还为黑莓数据库连接选择了 “Windows Integrated”（Windows 集成），必须同时为此处指定的 Windows 帐户提供黑莓数据库访问权限。
5. 单击 **Test Connectivity**（测试连接）检查是否可以连接到 SQL Server，然后单击 **Save**（保存）。
6. 此时将显示一条消息，提示您重新启动服务。单击是。



7. 配置一个或多个 Exchange Server：
   - 如果管理单个 Exchange 环境，则仅指定一台服务器。如果管理多个 Exchange 环境，则为每个 Exchange 环境指定一个 Exchange Server。
   - 单击 **Configure**（配置）**> Exchange** 选项卡，然后单击 **Add**（添加）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



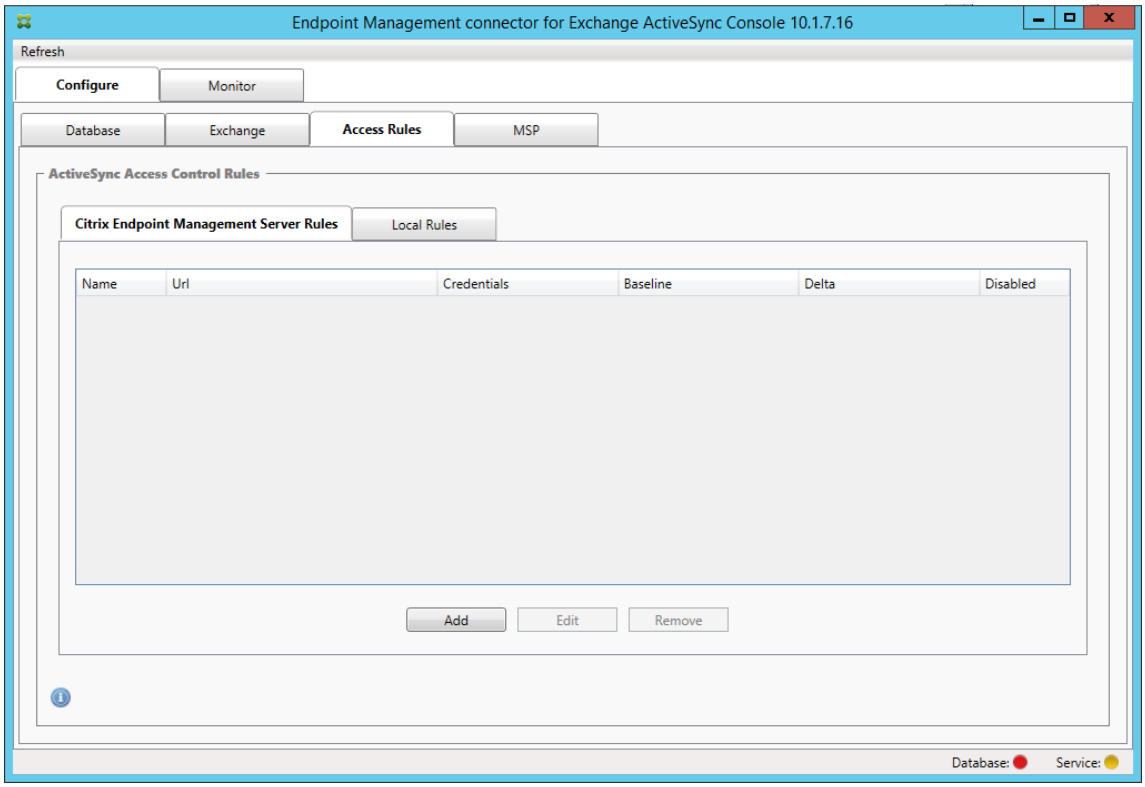
8. 选择 Exchange Server 环境的类型：**On Premise**（本地）或 **Office 365**。

   - 如果选择 **On Premise**（本地），请输入要用于远程 PowerShell 命令的 Exchange Server 名称。
   - 输入在“要求”部分中指定的 Exchange Server 上具有适当权限的 Windows 身份的用户名，然后输入该用户的密码。
   - 选择运行主要快照的计划。主要快照检测每个 Exchange ActiveSync 合作关系。
   - 选择运行次要快照的计划。次要快照检测新创建的 Exchange ActiveSync 合作关系。
   - 选择“Snapshot Type”（快照类型）：**Deep**（深层）或 **Shallow**（浅层）。浅层快照通常更快并且足以执行适用于 Exchange ActiveSync 的连接器的所有 Exchange ActiveSync 访问控制功能。
   - 选择默认访问：**Allow**（允许）、**Block**（阻止）或 **Unchanged**（保持不变）。此设置控制如何处理显式 Endpoint Management 或本地规则确定的设备以外的所有设备。如果选择 **Allow**（允许），则允许 ActiveSync 访问所有此类设备。如果选择 **Block**（阻止），则拒绝访问。如果选择 **Unchanged**（保持不变），则不进行任何更改。
   - 选择 ActiveSync 命令模式：**PowerShell** 或 **Simulation**（模拟）。
   - 在 **PowerShell** 模式下，适用于 Exchange ActiveSync 的连接器会发出 PowerShell 命令以执行所需的访问控制。在“Simulation”（模拟）模式下，适用于 Exchange ActiveSync 的连接器不发出 PowerShell 命令，但是会将预期命令和预期结果记录到数据库中。在“Simulation”（模拟）模式下，用户随后可使用 **Monitor**（监视）选项卡查看启用 PowerShell 模式时会发生的情况。
   - 在 **Connection Expiration**（连接过期）中，设置连接存在的小时数和分钟数。当连接达到指定的期限时，该连接将被标记为已过期，以便绝不会再次使用该连接。当不再使用已过期的连接时，适用于 Exchange ActiveSync 的连接器将正常关闭该连接。再次需要连接时，如果没有连接可用，则会初始化新连接。如果未指定，则将使用默认值 30 分钟。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

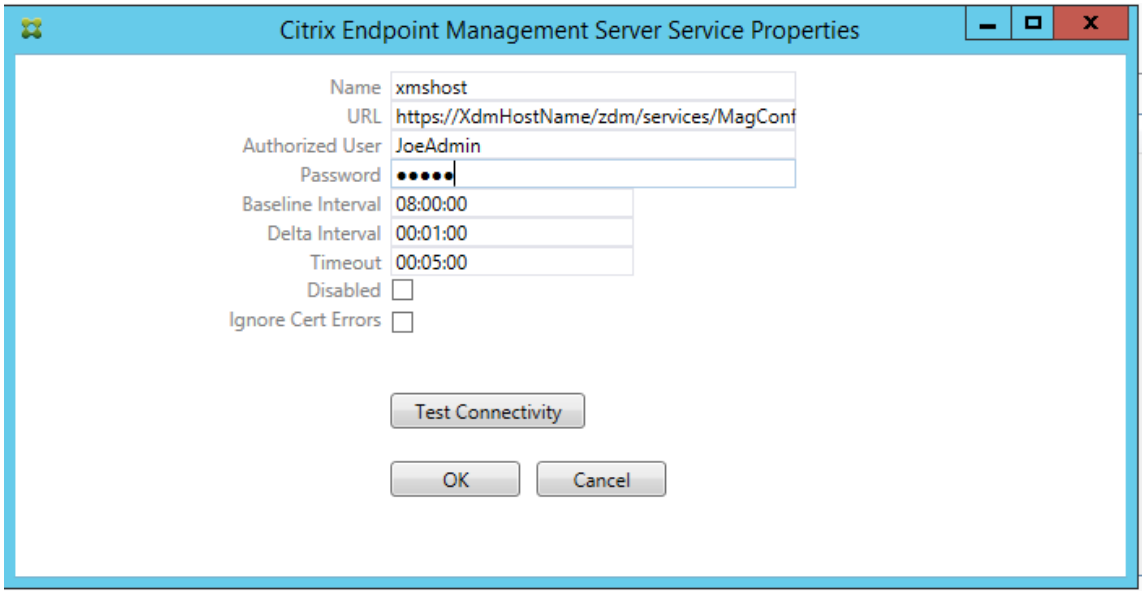
- 选择 **View Entire Forest**（查看整个林）可将适用于 Exchange ActiveSync 的连接器配置为查看 Exchange 环境中的整个 Active Directory 林。
- 选择身份验证协议：**Kerberos** 或 **Basic**（基本）。适用于 Exchange ActiveSync 的连接器支持本地部署的“Basic”（基本）身份验证。这将允许在连接器服务器不属于 Exchange Server 所在域的成员的情况下使用连接器。
- 单击 **Test Connectivity**（测试连接）检查是否可以连接到 Exchange Server，然后单击 **Save**（保存）。
- 此时将显示一条消息，提示您重新启动服务。单击是。

9. 配置访问规则：选择 **Configure**（配置）**> Access Rules**（访问规则）选项卡，单击 **Citrix Endpoint Management Rules**（Citrix Endpoint Management 规则）选项卡，然后单击 **Add**（添加）。



10. 在 **Endpoint Management server Service Properties**（Endpoint Management 服务器服务属性）页面上，修改 URL 字符串以指向 Endpoint Management 服务器。例如，如果实例名称为 `zdm`，则输入 `https://<XdmHostName>/zdm/services/MagConfigService`。在此示例中，将 `XdmHostName` 替换为 Endpoint Management 服务器的 IP 或 DNS 地址。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

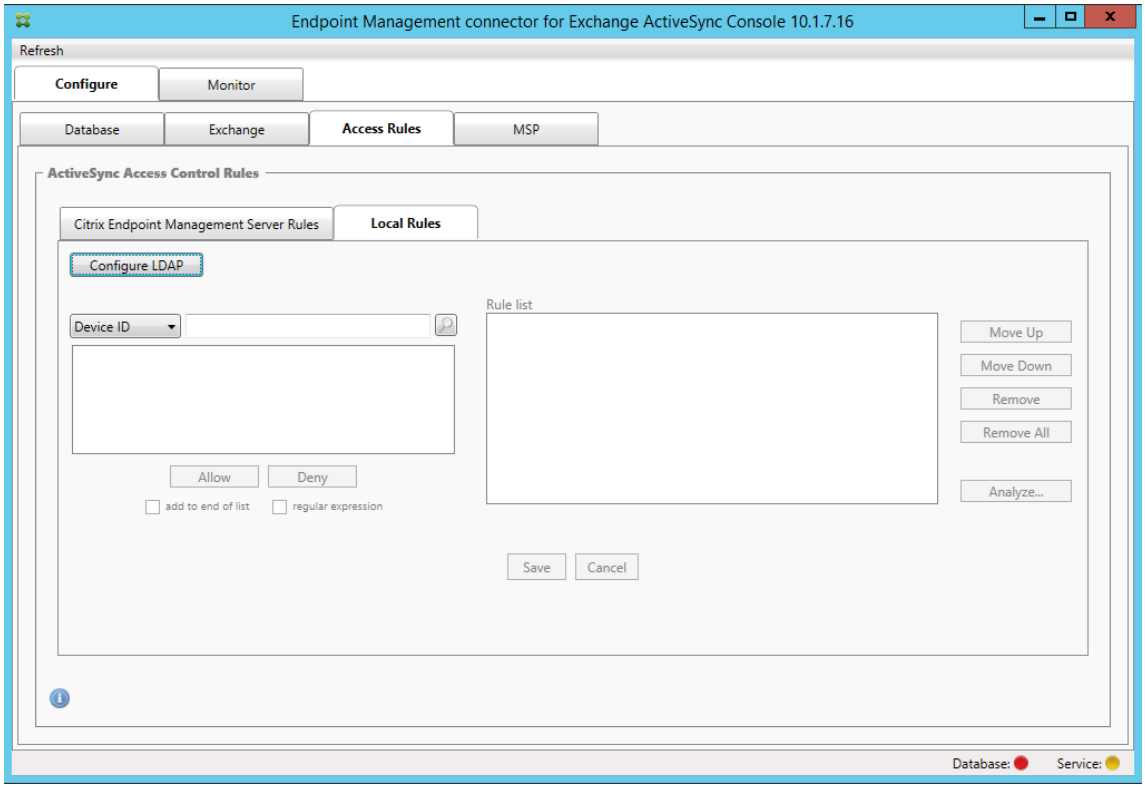


- 输入服务器的授权用户。
- 输入用户密码。
- 保留 **Baseline Interval**（基准时间间隔）、**Delta Interval**（时间间隔差）和 **Timeout**（超时）值的默认值。
- 单击 **Test Connectivity**（测试连接）检查与服务器的连接，然后单击 **OK**（确定）。

如果选中 **Disabled**（已禁用）复选框，Endpoint Management Mail Service 将不从 Endpoint Management 收集策略。

11. 单击 **Local Rules**（本地规则）选项卡。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



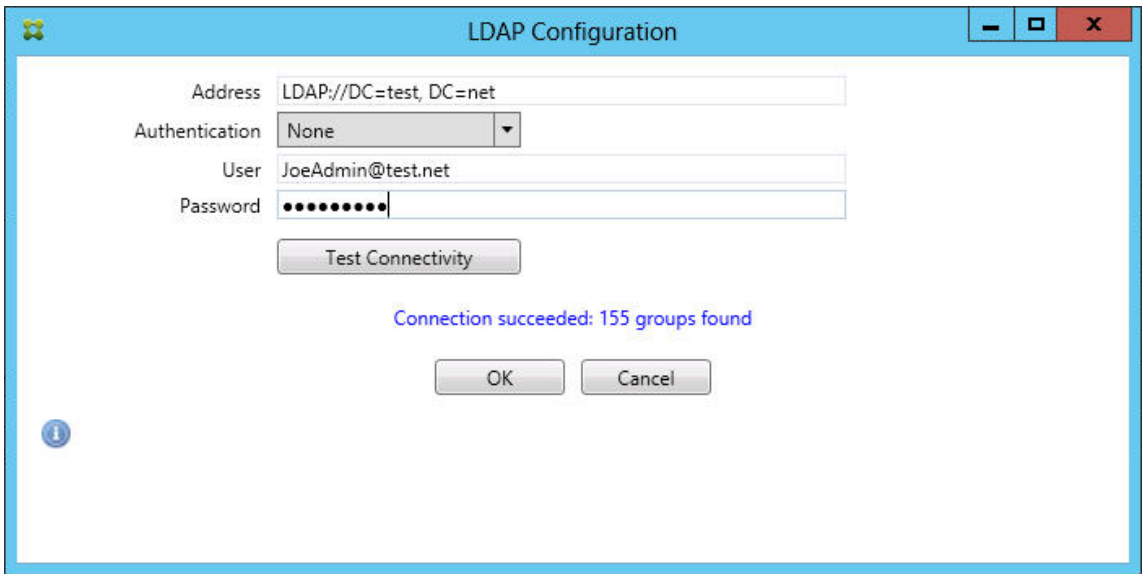
- 您可以根据 ActiveSync 的“Device ID”（设备 ID）、“Device Type”（设备类型）、“AD Group”（AD 组）、“User”（用户）或设备“UserAgent”（用户代理）添加本地规则。在列表中选择适当的类型。
- 在文本框中输入文本或文本片段。也可单击查询按钮，查看与片段匹配的实体。

对于除“Group”（组）以外的所有类型，系统依赖在快照中找到的设备。因此，如果刚刚开始且尚未完成快照，则没有实体可用。

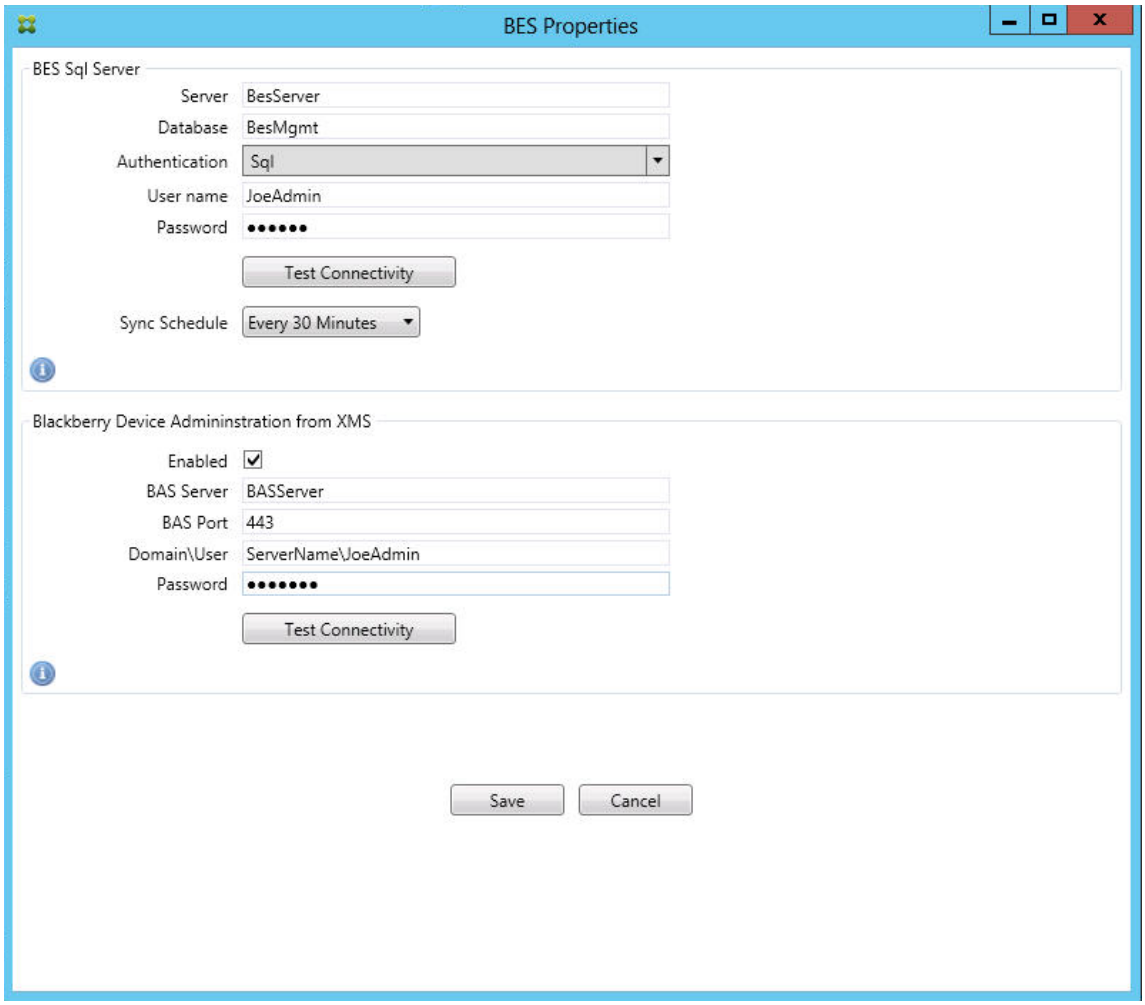
- 选择一个文本值，然后单击 **Allow**（允许）或 **Deny**（拒绝），将其添加到右侧的 **Rule List**（规则列表）窗格。可使用 **Rule List**（规则列表）窗格右侧的按钮更改规则的顺序或移除规则。该顺序很重要，因为对于指定的用户和设备，将按照显示的顺序评估规则，并且一旦与较靠前的规则（离顶部较近）匹配，则后续的规则将失效。例如，如果存在一条允许所有 iPad 设备的规则，而后续的规则阻止用户 Matt，则 Matt 的 iPad 将仍被允许，因为 iPad 规则的有效优先级高于 Matt 规则。
- 要对规则列表中的规则进行分析以找到潜在的覆盖、冲突或补充结构，请单击 **Analyze**（分析），然后单击 **Save**（保存）。

12. 如果要建立应用于 Active Directory 组的本地规则，请单击 **Configure LDAP**（配置 LDAP），然后配置 LDAP 连接属性。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



13. （可选）配置 BlackBerry Enterprise Server (BES) 的一个或多个实例：单击 **Add**（添加），然后输入 BES SQL Server 的服务器名称



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

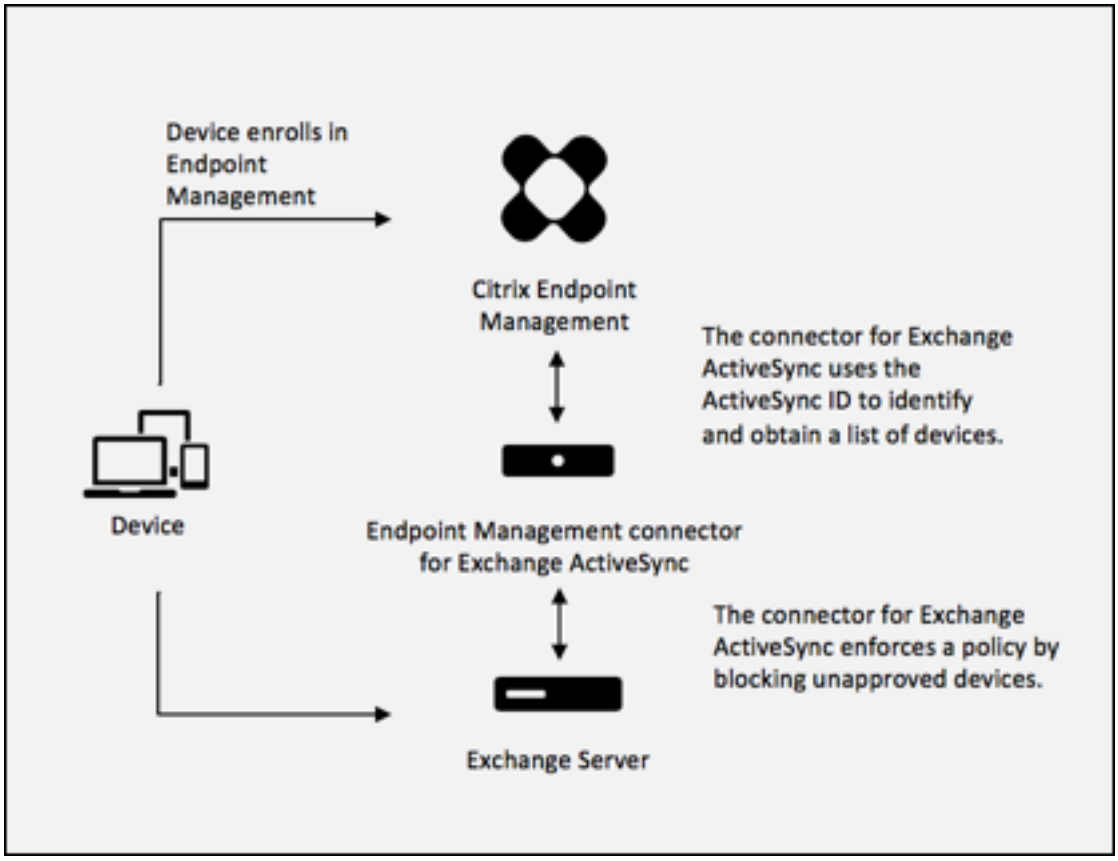
- 输入 BES 管理数据库的数据库名称。
- 选择 **Authentication**（身份验证）模式。如果选择 “Windows Integrated”（Windows 集成）身份验证，则适用于 Exchange ActiveSync 的连接器服务的用户帐户就是用于连接 BES SQL Server 的帐户。如果还为连接器数据库连接选择了 Windows 集成，则必须同时为此处指定的 Windows 帐户提供连接器数据库访问权限。
- 如果选择 **SQL authentication**（SQL 身份验证），请输入用户名和密码。
- 设置 **Sync Schedule**（同步计划）。这是用于连接到 BES SQL Server 并检查任何设备更新的计划。
- 单击 **Test Connectivity**（测试连接）检查与 SQL Server 的连接。如果选择 Windows 集成，则此测试使用当前登录的用户而非连接器服务用户，因此不能准确测试 SQL 身份验证。
- 要支持从 Endpoint Management 对黑莓设备进行远程擦除和重置密码的功能，请选中 **Enabled**（已启用）复选框。
- 输入 BES 完全限定的域名 (FQDN)。
- 输入用于管理 Web 服务的 BES 端口。
- 输入 BES 服务必需的完全限定用户和密码。
- 单击 **Test Connectivity**（测试连接）测试与 BES 的连接，然后单击 **Save**（保存）。

使用 **ActiveSync ID** 强制执行电子邮件策略

您的企业电子邮件策略可以规定不批准特定设备使用企业电子邮件。为与此策略保持一致，您希望确保员工无法通过此类设备访问企业电子邮件。适用于 Exchange ActiveSync 的 Endpoint Management 连接器和 Endpoint Management 会共同协作以强制实施此类电子邮件策略。Endpoint Management 设置企业电子邮件访问策略。当未经批准的设备向 Endpoint Management 注册时，适用于 Exchange ActiveSync 的 Endpoint Management 连接器会强制实施此策略。

设备上的电子邮件客户端使用设备 ID（也称为 ActiveSync ID，用于标识设备）向 Exchange Server（或 Office 365）广播自己。Secure Hub 获取类似的标识符，并在注册设备时将标识符发送给 Endpoint Management。通过比较两个设备 ID，适用于 Exchange ActiveSync 的连接器可以确定特定设备是否应该具有企业电子邮件访问权限。下图说明了此概念：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



如果 Endpoint Management 向适用于 Exchange ActiveSync 的连接器发送的 ActiveSync ID 不同于设备向 Exchange 发布的 ID，该连接器无法指示 Exchange 如何处理此设备。

匹配 ActiveSync ID 可以在大多数平台上可靠地执行。但是，Citrix 已发现在某些 Android 实现上，来自设备的 ActiveSync ID 不同于邮件客户端向 Exchange 广播的 ID。为缓解此问题，可以执行以下操作：

- 在 Android 平台上，Citrix 建议您使用 Citrix Secure Mail。

为确保正确执行公司电子邮件访问策略，您可以采取防御性安全立场。默认情况下，通过将静态策略设置为拒绝，配置适用于 Exchange ActiveSync 的 Endpoint Management 连接器以阻止电子邮件。这意味着，如果员工在 Android 设备上配置了另一个电子邮件客户端，而 ActiveSync ID 检测不起作用，公司电子邮件将拒绝对员工的访问。

访问控制规则

适用于 Exchange ActiveSync 的 Endpoint Management 连接器提供了一种基于规则的方法，为 Exchange ActiveSync 设备动态配置访问控制。连接器访问控制规则由两部分组成，即一个匹配的表达式和一个所需的访问状态（“允许”或“阻止”）。规则可能会针对给定的 Exchange ActiveSync 设备进行评估，以确定该规则是否适用于该设备或是否与该设备匹配。有多种匹配的表达式；例如，一条规则可能与给定“设备类型”（或特定 Exchange ActiveSync 设备 ID）的所有设备或者特定用户的所有设备等匹配。

在规则列表中添加、删除和重新排列规则期间，任何时候单击取消按钮都会将规则列表还原回首次打开时的状态。除非单击保存，否则关闭配置工具时将丢失您对此窗口所做的任何更改。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

适用于 Exchange ActiveSync 的 Endpoint Management 连接器有三种类型的规则，即本地规则、Endpoint Management 服务器规则（也称为 XDM 规则）和默认访问规则。

本地规则：本地规则的优先级最高：如果设备与本地规则匹配，规则评估将停止。既不查询 Endpoint Management 服务器规则也不查询默认访问规则。本地规则是通过 **Configure**（配置）**> Access Rules**（访问规则）**> Local Rules**（本地规则）选项卡在适用于 Exchange ActiveSync 的连接器中本地配置的。支持匹配基于给定的 Active Directory 组内用户的成员身份。支持匹配基于以下字段的正则表达式：

- ActiveSync Device ID（ActiveSync 设备 ID）
- ActiveSync Device Type（ActiveSync 设备类型）
- User Principal Name (UPN)（用户主体名称 (UPN)）
- ActiveSync User Agent（ActiveSync 用户代理）（通常为设备平台或电子邮件客户端）

只要完成了主要快照并找到设备，您应能够添加常规或正则表达式规则。如果尚未完成主要快照，则只能添加正则表达式规则。

Endpoint Management 服务器规则： Endpoint Management 服务器规则是指对提供有关托管设备的规则的外部 Endpoint Management 服务器的引用。Endpoint Management 服务器可通过自身的高级规则进行配置，这些规则可标识要基于 Endpoint Management 已知属性允许或阻止的设备（例如设备是否越狱或设备是否包含禁用的应用程序）。Endpoint Management 评估高级规则并生成一组允许或阻止的 ActiveSync 设备 ID，然后将其传递到 XenMobile Mail Manager。

默认访问规则：默认访问规则是唯一的，它可以潜在匹配每个设备，并且始终是最后一个被评估。此规则是一条笼统的规则，这意味着如果给定的设备与本地规则或 Endpoint Management 服务器规则不匹配，该设备的所需访问状态将由默认访问规则的所需访问状态决定。

- **Default Access - Allow**（默认访问 **-** 允许）：允许与本地规则或 Endpoint Management 服务器规则不匹配的任何设备。
- **Default Access - Block**（默认访问 **-** 阻止）：阻止与本地规则或 Endpoint Management 服务器规则不匹配的任何设备。
- **Default Access - Unchanged**（默认访问 **-** 未更改）：与本地规则或 Endpoint Management 服务器规则不匹配的任何设备将不会由适用于 Exchange ActiveSync 的连接器以任何方式修改其访问状态。如果设备已被 Exchange 置于隔离模式，则不会采取任何措施；例如，从隔离模式删除设备的唯一方法是使用显式本地规则或 XDM 规则覆盖隔离。

关于规则评估

对于 Exchange 向适用于 Exchange ActiveSync 的连接器报告的每个设备，将按照优先级从最高到最低的顺序对这些规则进行评估，如下所示：

- 本地规则
- Endpoint Management 服务器规则
- 默认访问规则

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

找到匹配项时，评估将停止。例如，如果本地规则与给定设备匹配，则不会根据任何 Endpoint Management 服务器规则或默认访问规则对该设备进行评估。这同样适用于给定的规则类型。例如，如果本地规则列表中有多条规则与某个给定设备匹配，则遇到第一个匹配项时，评估即停止。

当设备属性发生变化、添加或删除设备或者规则本身发生变化时，适用于 Exchange ActiveSync 的连接器会重新评估当前定义的规则集合。主要快照以可配置的时间间隔选取设备属性更改和删除操作。次要快照以可配置的时间间隔选取新设备。

Exchange ActiveSync 还具有控制访问的规则。了解这些规则在适用于 Exchange ActiveSync 的连接器的上下文中的工作方式至关重要。Exchange 可能通过以下三种级别的规则进行配置：个人免除、设备规则以及组织设置。适用于 Exchange ActiveSync 的连接器通过以编程方式发出远程 PowerShell 请求来自动化访问控制，以影响个人免除列表。这些是与给定邮箱关联的允许和阻止的 Exchange ActiveSync 设备 ID 列表。部署后，适用于 Exchange ActiveSync 的连接器有效地接替了 Exchange 中免除列表的管理功能。请参阅 Microsoft 文章使用 Exchange 和 Configuration Manager 进行设备管理。

在为相同的字段定义了多条规则的情况下，分析特别有用。您可以对规则之间的关系进行故障排除。请从规则字段的角度来执行分析；例如，规则是基于匹配的字段（例如 ActiveSync 设备 ID、ActiveSync 设备类型、用户、用户代理等）按组进行分析的。

规则术语

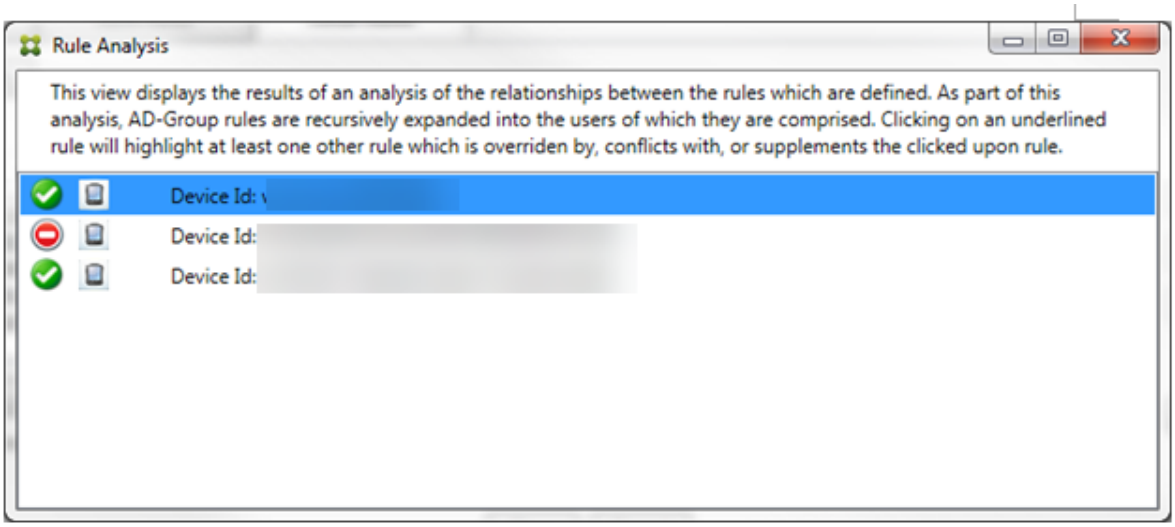
- 覆盖规则：当多条规则可以应用于同一设备时会发生覆盖。因为规则是按照列表中的优先级进行评估的，可能会应用的后面的规则实例可能永远不会被评估。
- 冲突规则：当多条规则可以应用于同一设备但访问状态（允许/阻止）不匹配时会发生冲突。如果冲突规则不是正则表达式规则，冲突将始终隐式包含覆盖
- 补充规则：当多条规则是正则表达式规则，因此可能需要确保两个（或多个）正则表达式可以合并到一条正则表达式规则中或者不是重复功能时，会发生补充。补充规则的访问状态（允许/阻止）可能还会发生冲突。
- 主要规则：主要规则是已在对话框内单击的规则。规则通过围绕它的实线框可视化地指示出来。该规则还将具有一个或两个绿色箭头，用来指示向上或向下方向。如果箭头指向上方，该箭头指示辅助规则在主要规则前面。如果箭头指向下方，该箭头指示辅助规则在主要规则后面。只有一个主要规则可以随时处于活动状态。
- 辅助规则：辅助规则以某种方式与主要规则相关（通过覆盖、冲突或补充关系）。规则通过围绕它的虚线框可视化地指示出来。对于每条主要规则，可以存在一条和多条辅助规则。单击任何带有下划线的条目时，始终从主要规则的角度突出显示一条或多条辅助规则。例如，辅助规则被主要规则覆盖，或辅助规则的访问状态与主要规则冲突，或辅助规则对主要规则进行补充。

规则类型在 **“Rule Analysis”**（规则分析）对话框中的显示方式

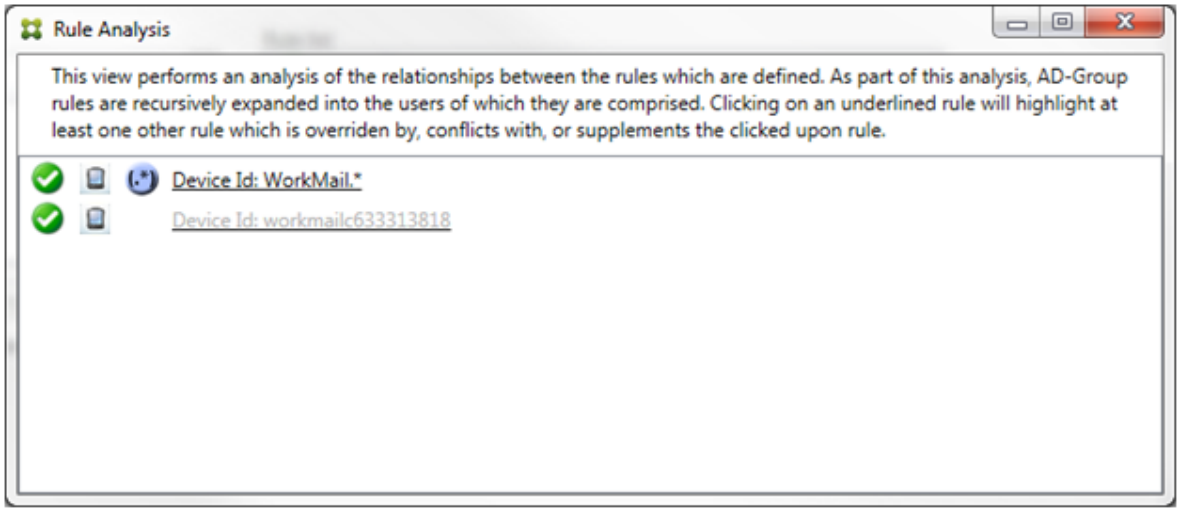
没有冲突、覆盖或补充时，“Rule Analysis”（规则分析）对话框中没有带下划线的条目。单击任何项目都没有效果；例如，出现正常选定项目的视觉效果。

“Rule Analysis”（规则分析）窗口包含一个复选框，选中该复选框时，将仅显示冲突、覆盖、冗余或补充规则。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

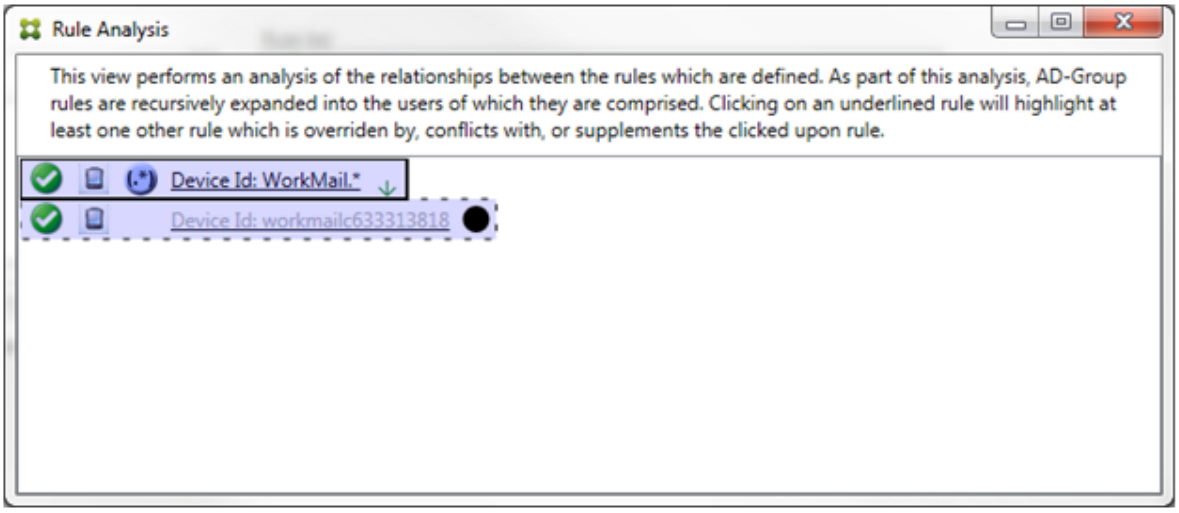


当出现覆盖时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。至少有一条辅助规则以较浅字体显示，指示该规则已被优先级较高的规则覆盖。您可以单击被覆盖的规则以了解覆盖该规则的一条或多条规则。每当被覆盖的规则由于该规则是主要规则或辅助规则而突出显示时，它旁边都会显示一个黑色圆圈，以进一步指示该规则处于不活动状态。例如，在单击该规则之前，对话框显示如下：

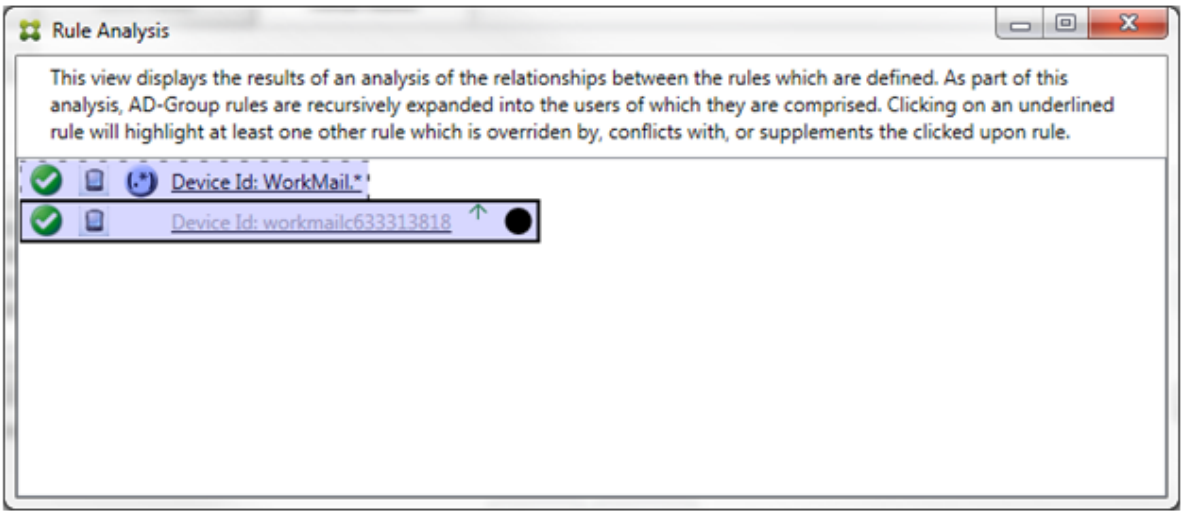


单击优先级最高的规则时，对话框显示如下：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



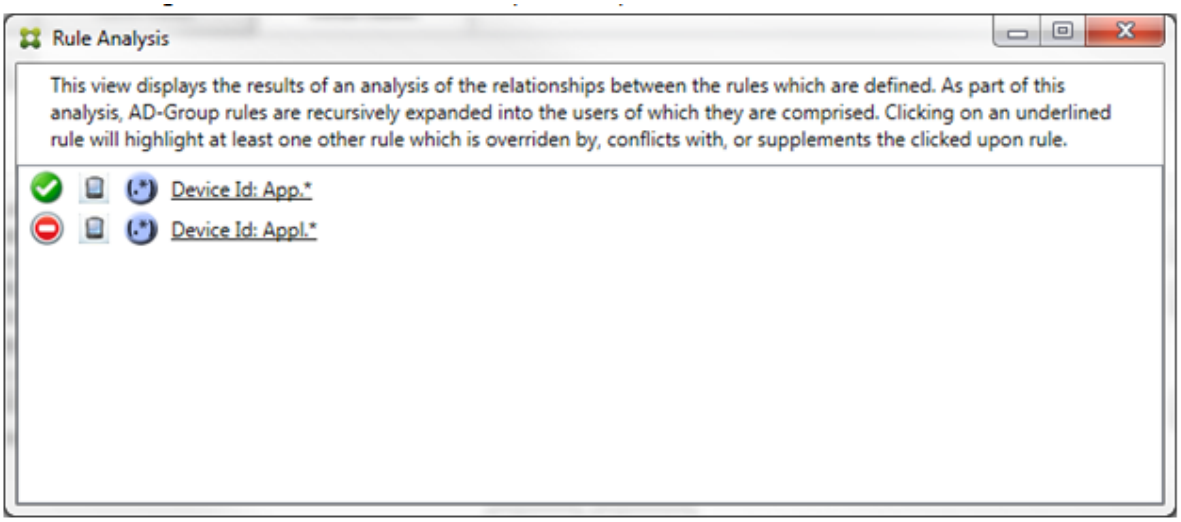
在此示例中，正则表达式规则 `WorkMail.*` 是主要规则（以实线框指示），常规规则 `workmailc633313818` 是辅助规则（以虚线框指示）。辅助规则旁边的黑点是一个视觉提示，可进一步指示由于它的前面有较高优先级的正则表达式而处于不活动状态（永远不会被评估）。单击被覆盖的规则后，对话框显示如下：



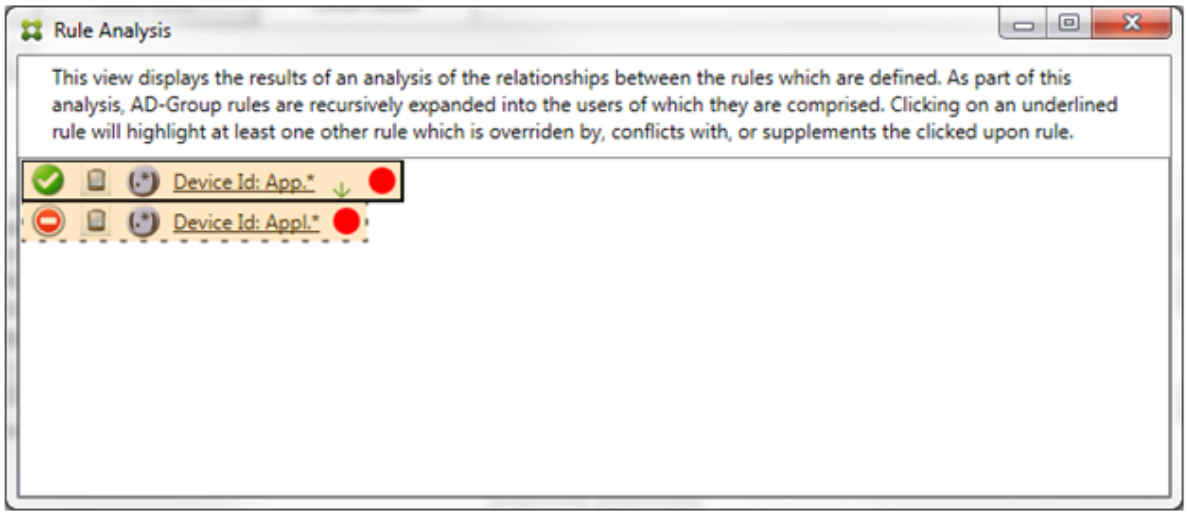
在前面的示例中，正则表达式规则 `WorkMail.*` 是辅助规则（以虚线框指示），常规规则 `workmailc633313818` 是主要规则（以实线框指示）。对于这一简单的示例，没有太大差异。对于更为复杂的示例，请参阅本主题中后面所述的复杂表达式示例。在定义了许多规则的情景中，单击被覆盖的规则将快速识别已覆盖该规则的一条或多条规则。

当出现冲突时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。发生冲突的规则用红点指示。只有相互冲突的规则才可能定义了两条或多条正则表达式规则。在所有其他冲突情景中，不仅将有冲突，而且还会发生覆盖。在简单的示例中单击任一规则之前，对话框显示如下：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



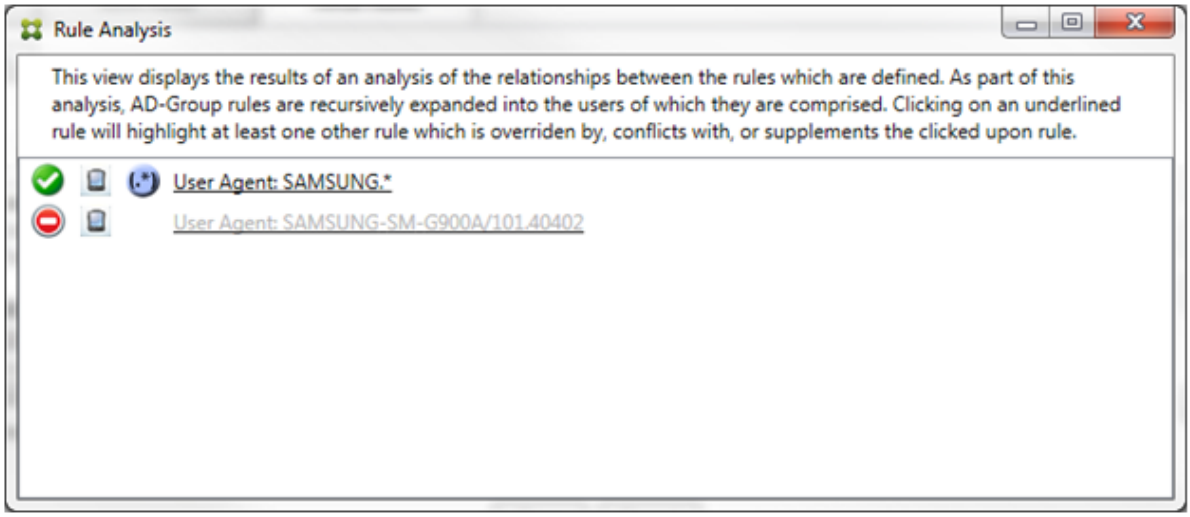
检查这两条正则表达式规则即可明显发现，第一条规则允许设备 ID 包含 `Appl` 的所有设备，第二条规则拒绝设备 ID 包含 Appl 的所有设备。此外，即使第二条规则拒绝了设备 ID 包含 `Appl` 的所有设备，也不会拒绝符合条件的设备，因为允许规则的优先级较高。单击第一条规则后，对话框显示如下：



在上述情景中，主要规则（正则表达式规则 `App.*`）和辅助规则（正则表达式规则 `Appl.*`）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

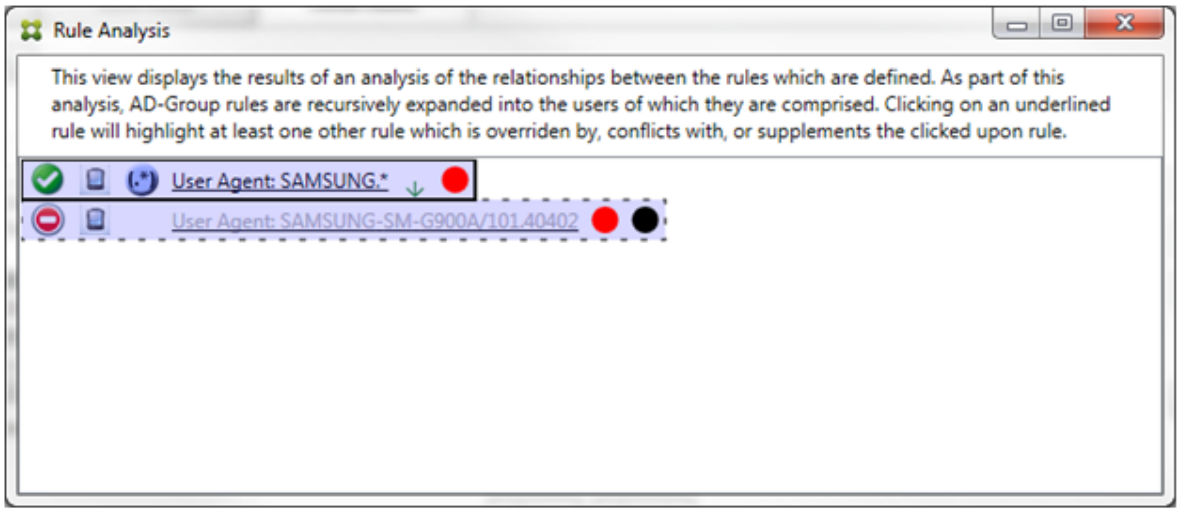
在同时存在冲突和覆盖的情景中，主要规则（正则表达式规则 `App.*`）和辅助规则（正则表达式规则 `Appl.*`）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



在前面的示例中，显而易见，第一条规则（正则表达式规则 SAMSUNG.*）不仅覆盖下一条规则（常规规则 SAMSUNG-SM-G900A/101.40402），而且这两条规则的访问状态有所不同（主要规则指定“允许”，辅助规则指定“阻止”）。第二条规则（常规规则 SAMSUNG-SM-G900A/101.40402）以较浅文本显示，指示该规则已被覆盖，并因此处于不活动状态。

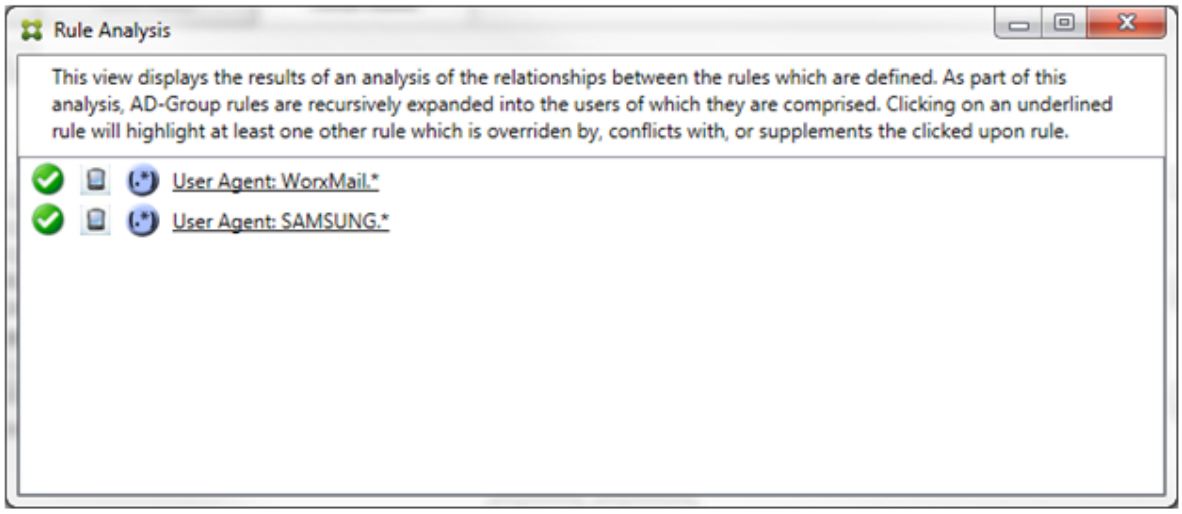
单击正则表达式规则后，对话框显示如下：



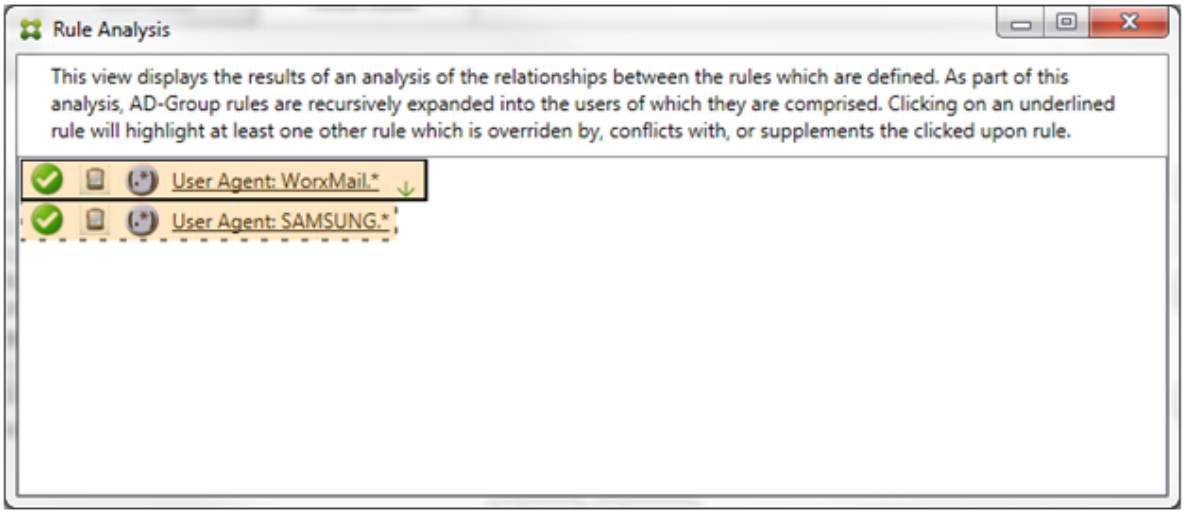
主要规则（正则表达式规则 SAMSUNG.*）后跟一个红点，指示其访问状态与一条或多条辅助规则发生冲突。辅助规则（常规规则 SAMSUNG-SM-G900A/101.40402）后跟一个红点，指示其访问状态与主要规则发生冲突。此外，该规则还后跟黑点，指示其已被覆盖，并因此处于不活动状态。

至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。仅相互补充的规则将只涉及正则表达式规则。当规则相互补充时，将以黄色叠加表示。在简单的示例中单击任一规则之前，对话框显示如下：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



目测会很容易发现这两条规则都是正则表达式规则，都已应用到适用于 Exchange ActiveSync 的 Endpoint Management 连接器中的 ActiveSync 设备 ID 字段。单击第一条规则后，对话框显示如下：

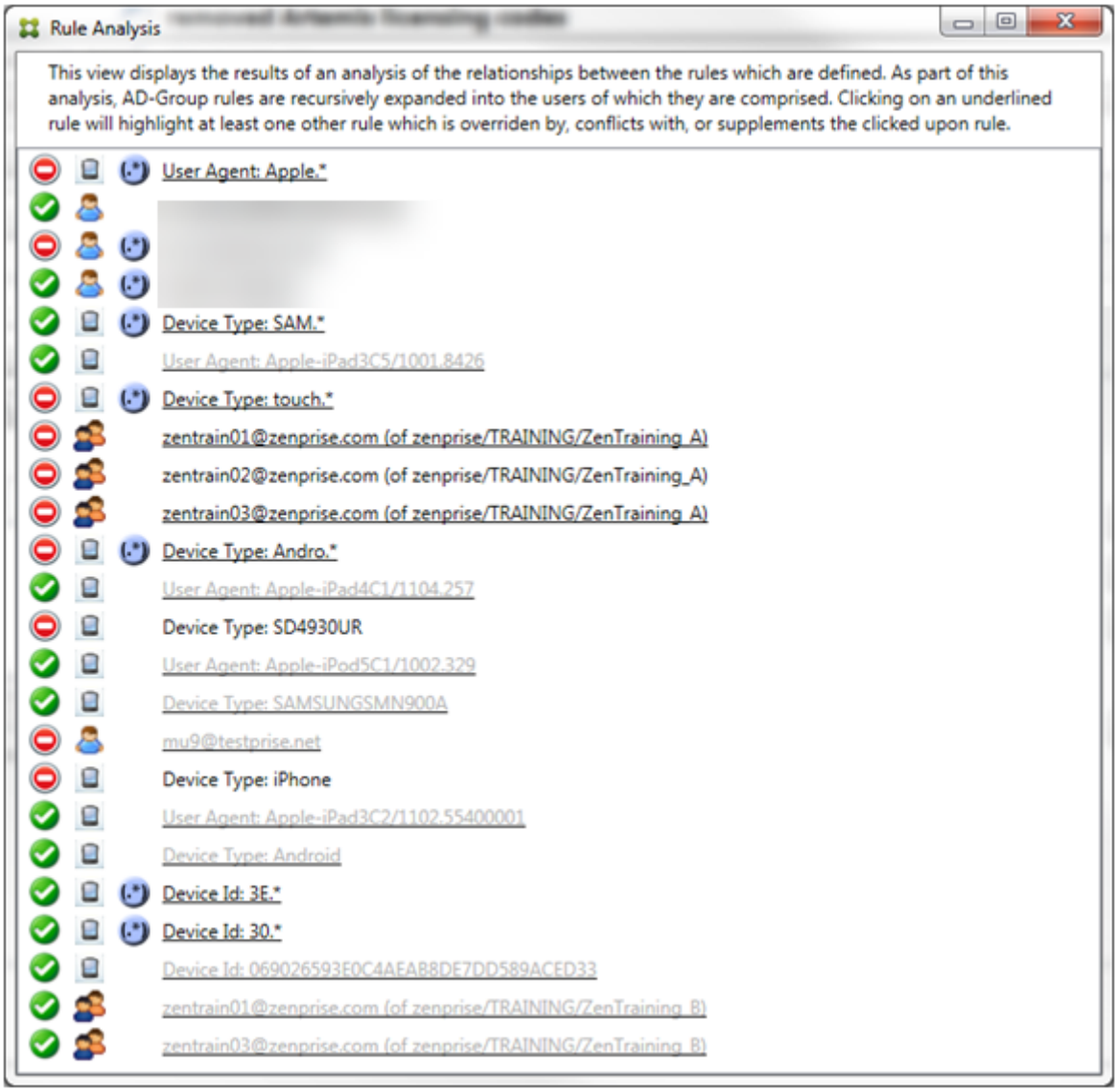


主要规则（正则表达式规则 `WorkMail.*`）以黄色叠加突出显示，指示至少存在另外一个是正则表达式的辅助规则。辅助规则（正则表达式规则 `SAMSUNG.*`）以黄色叠加突出显示，指示辅助规则与主要规则都是要应用于适用于 Exchange ActiveSync 的连接器内同一字段的正则表达式规则。在此示例中，该字段为 ActiveSync 设备 ID。这些正则表达式可能叠加，也可能不叠加。是否正确制作正则表达式由您来决定。

复杂表达式示例

许多潜在的覆盖、冲突或补充都可能会发生，使其不可能举例说明所有可能的情景。以下示例探讨了不会执行的操作，同时还阐明了规则分析视觉构建的强大功能。大多数项目在下图中加了下划线。许多项目以较浅的字体显示，指示存在问题的规则已被优先级较高的规则以某种方式覆盖。列表中还包含许多正则表达式规则，如  所示。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

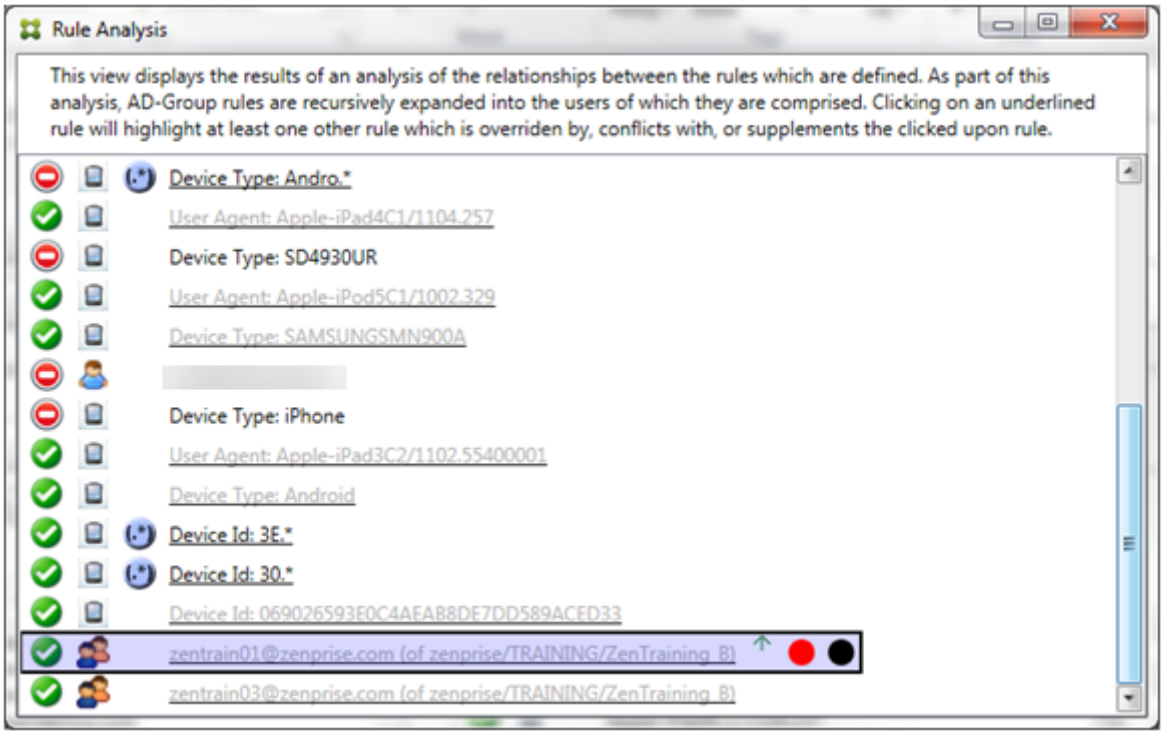


如何分析覆盖

要查看覆盖了特定规则的一条或多条规则，您可以单击该规则。

示例 **1**：此示例调查了覆盖 `zentrain01@zenprise.com` 的原因。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

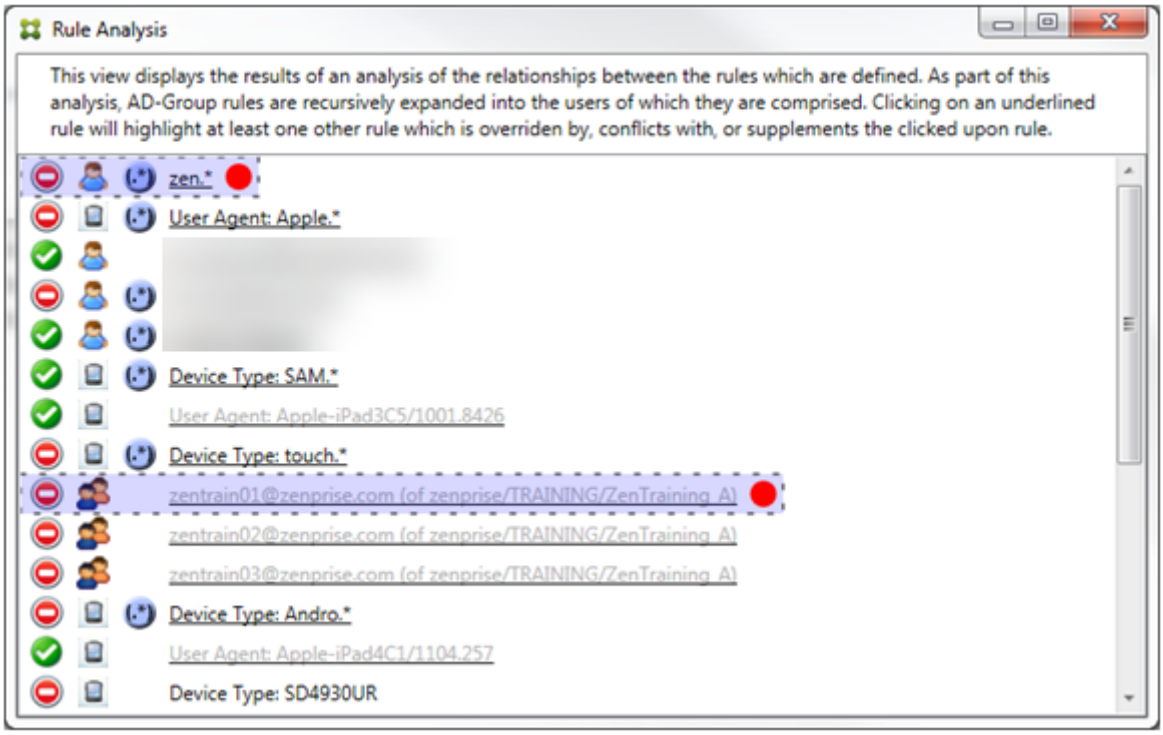


主要规则（AD-Group 规则 `zenprise/TRAINING/ZenTraining B`，`zentrain01@zenprise.com` 是其中的一个成员）具有以下特性：

- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示一条或多条辅助规则都能够在该箭头上方找到）。
- 后跟一个红色圆圈和一个黑色圆圈，分别指示一条或多条辅助规则与其访问状态存在冲突，并且主要规则已被覆盖且因此处于不活动状态。

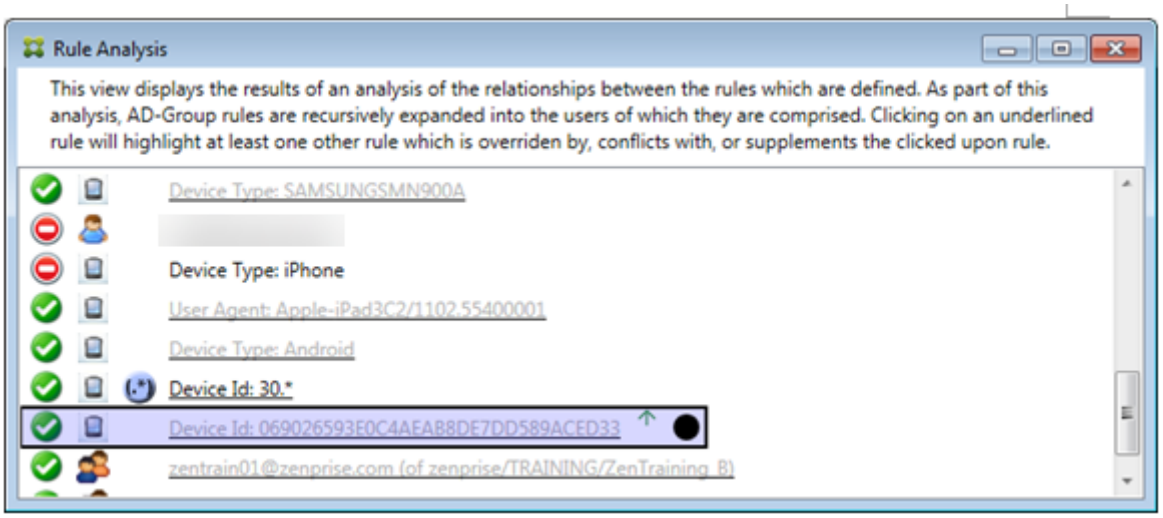
向上滚动时，您会看到以下内容：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



在此示例中，有两条辅助规则覆盖主要规则：正则表达式规则 `zen.*` 和常规规则 `zentrain01@zenprise.com`（属于 `zenprise/TRAINING/ZenTraining A`）。对于后一条辅助规则，出现了以下情况：Active Directory 组规则 `ZenTraining A` 包含用户 `zentrain01@zenprise.com`，Active Directory 组规则 `ZenTraining B` 也包含用户 `zentrain01@zenprise.com`。但是，由于辅助规则的优先级高于主要规则，因此主要规则被覆盖。主要规则的访问状态是“允许”，并且由于这两条辅助规则的访问状态都是“阻止”，因此，后跟一个红色圆圈以进一步指示访问冲突。

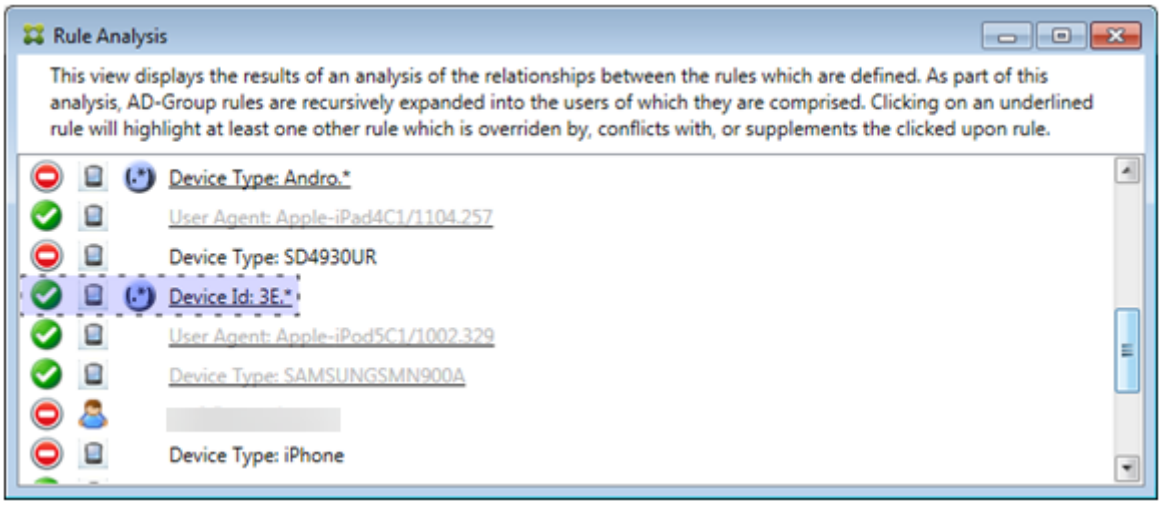
示例 **2**：此示例显示了覆盖 ActiveSync 设备 ID 为 `069026593E0C4AEAB8DE7DD589ACED33` 的设备的原因：



主要规则（常规设备 ID 规则 `069026593E0C4AEAB8DE7DD589ACED33`）具有以下特性：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示辅助规则能够在该箭头上方找到）。
- 后跟一个黑色圆圈，指示辅助规则已覆盖主要规则，并因此处于非活动状态。



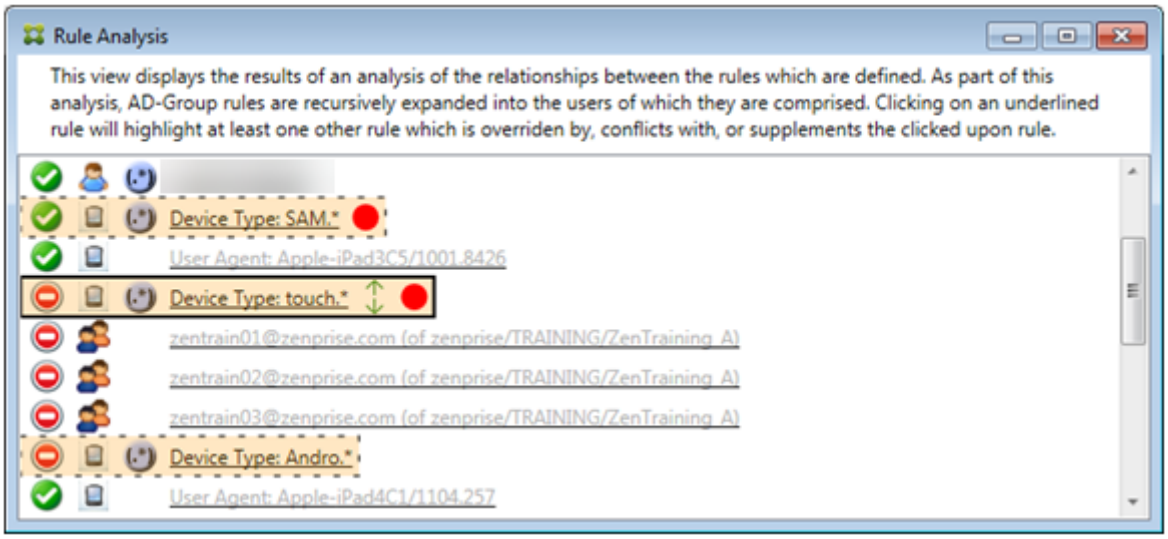
在此示例中，一条辅助规则覆盖主要规则：正则表达式 ActiveSync 设备 ID 规则 `3E.*`。由于正则表达式 `3E.*` 将会与 `069026593E0C4AEAB8DE7DD589ACED33` 匹配，因此，主要规则永远不会被评估。

如何分析补充和冲突

在此示例中，主要规则是正则表达式 ActiveSync 设备类型规则 `touch.*`。特性如下：

- 以实线框指示，并使用黄色叠加作为警告，提示正在针对特定规则字段运行多条正则表达式规则，在这种情况下为 ActiveSync 设备类型。
- 两个箭头分别指向上方和下方，指示至少存在一条具有较高优先级的辅助规则以及至少存在一条具有较低优先级的辅助规则。
- 它旁边的红色圆圈表示至少有一个辅助规则的访问权限设置为 “ 允许”，这与主规则对 **Block** 的访问权限冲突
- 存在两条辅助规则，即正则表达式 ActiveSync 设备类型规则 `SAM.*` 和正则表达式 ActiveSync 设备类型规则 `Andro.*`。
- 这两条辅助规则都加了虚线框，指示其属于辅助规则。
- 这两条辅助规则都以黄色叠加，指示其也应用于 ActiveSync 设备类型的规则字段。
- 在此类情景中，您应确保其正则表达式规则不冗余。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



如何进一步分析规则

本示例探讨了规则关系如何始终从主要规则的角度建立。前面的示例显示了单击应用于设备类型值为 `touch.*` 的规则字段的正则表达式规则的情况。单击辅助规则 `Andro.*` 将显示一组不同的突出显示的辅助规则。

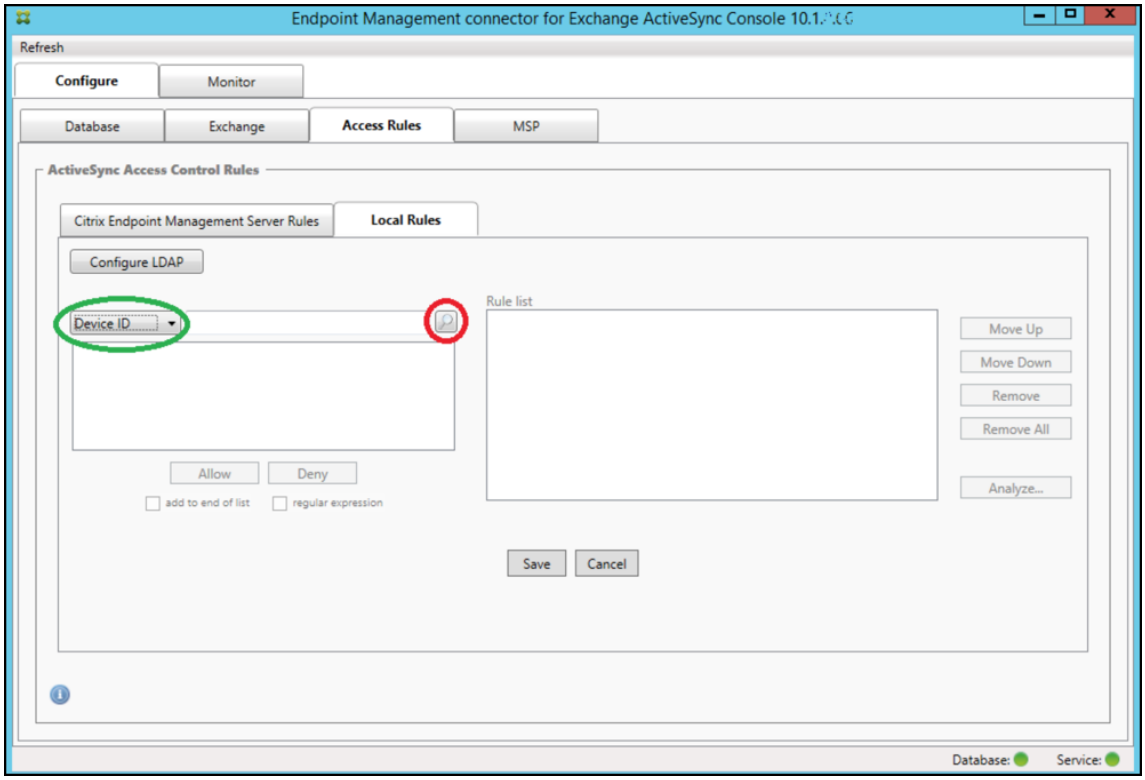


© 1999–2023 Cloud Software Group, Inc. All rights reserved.

此示例显示了规则关系中包含的覆盖规则。此规则是常规 ActiveSync 设备类型规则 `Android`，已被覆盖（通过浅色字体和旁边的黑色圆圈指示），并且其访问状态还与主要规则正则表达式 ActiveSync 设备类型规则 `Andro.*` 发生冲突。在单击该规则之前，该规则是辅助规则。在前面的示例中，常规 ActiveSync 设备类型规则 `Android` 未显示为辅助规则，因为从主要规则（正则表达式 ActiveSync 设备类型规则 `touch.*`）的角度来看，该规则与主要规则不相关。

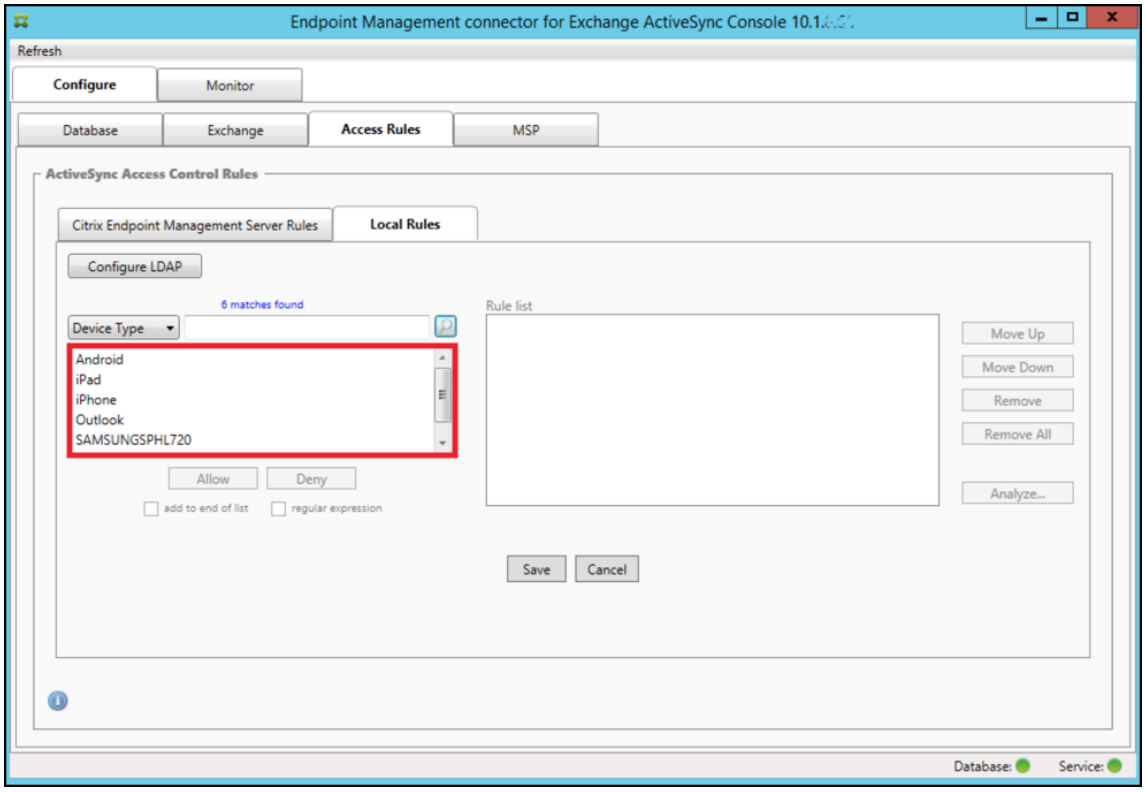
配置常规表达式本地规则

1. 单击 **Access Rules**（访问规则）选项卡。



2. 在 **Device ID**（设备 ID）列表中，选择要为其创建本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。在此示例中，已选择 **Device Type**（设备类型）字段，并且选项显示在下面的列表框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

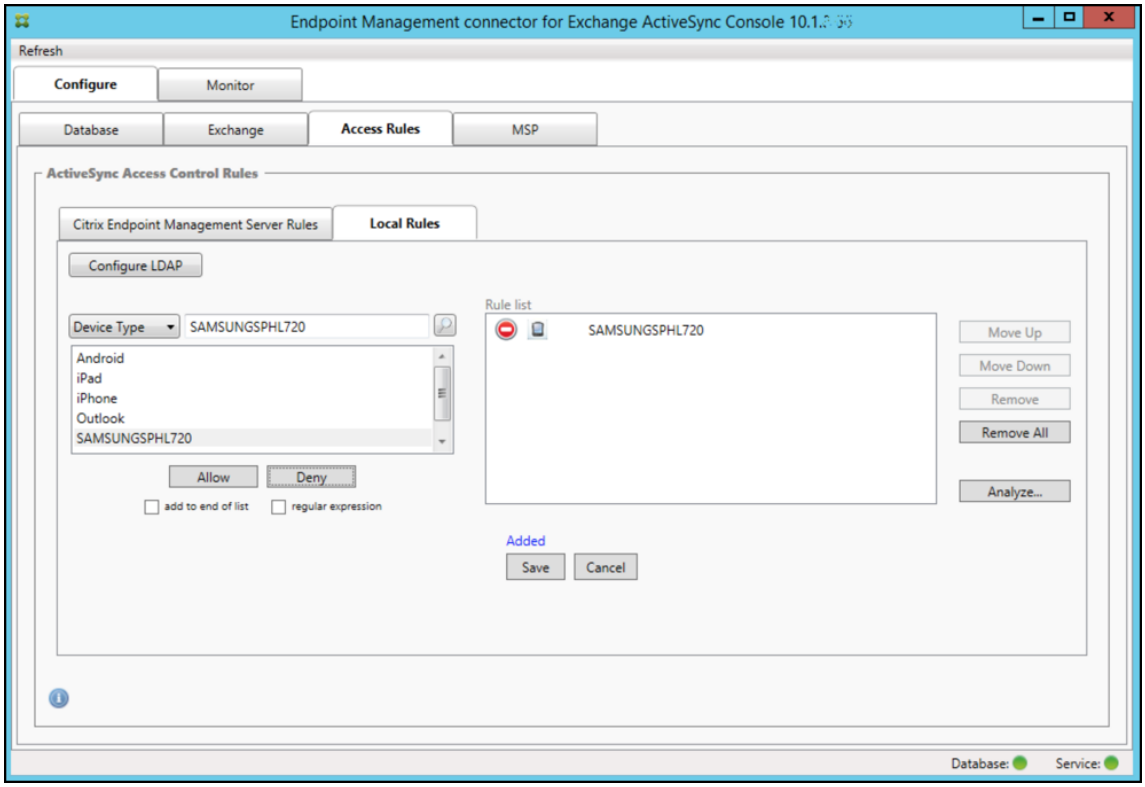


4. 在结果列表框中单击其中一个项目，然后单击以下选项之一：

   - **Allow**（允许）表示 Exchange 将配置为允许所有匹配设备的 ActiveSync 流量。
   - **Deny**（拒绝）表示 Exchange 将配置为拒绝所有匹配设备的 ActiveSync 流量。

   在此示例中，将拒绝访问设备类型为 SamsungSPhl720 的所有设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



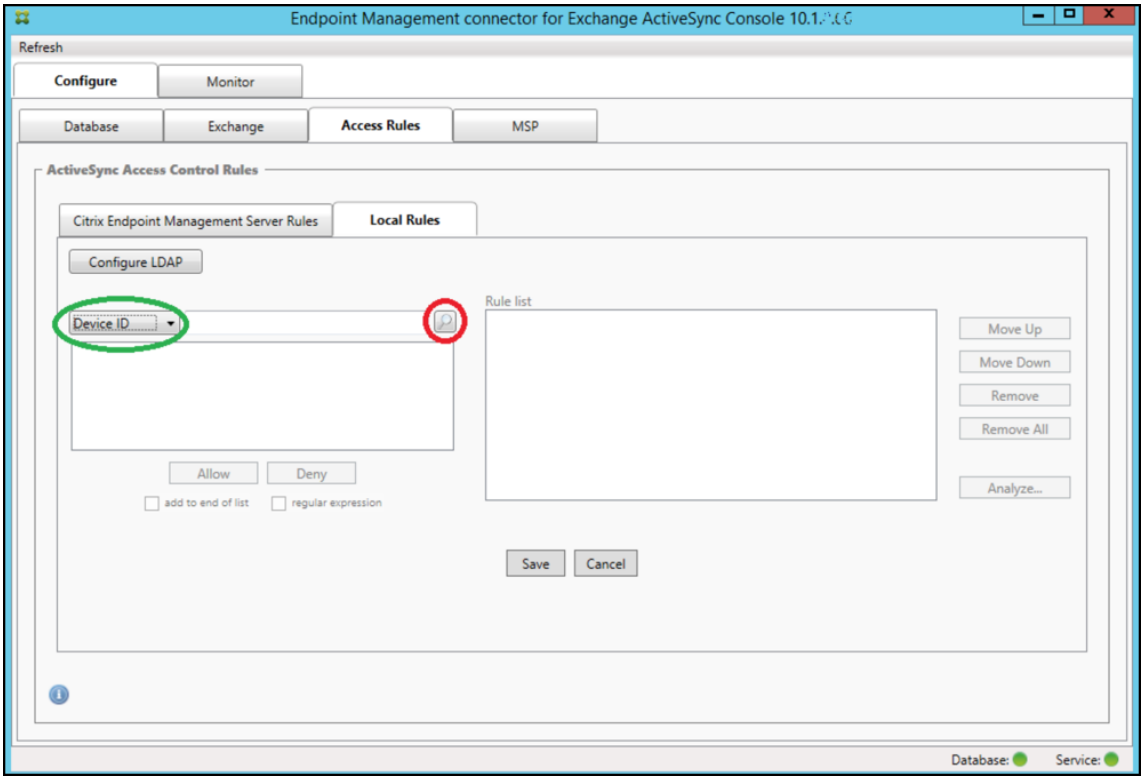
添加正则表达式

正则表达式局部规则可以通过出现在它们旁边的图标来区分-—  。要添加正则表达式规则，您可以通过给定字段的结果列表中的现有值来构建正则表达式规则（只要已完成主要快照），或只需键入您想要的正则表达式。

从现有字段值构建正则表达式

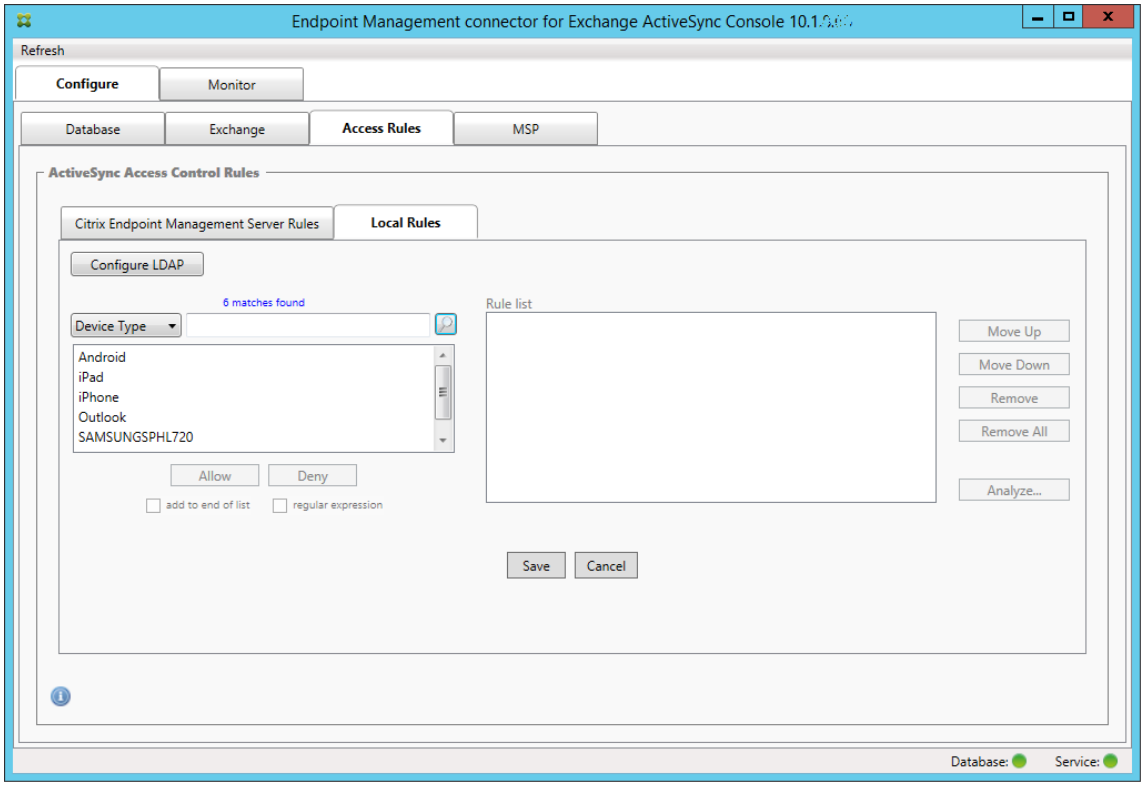
1. 单击 **Access Rules**（访问规则）选项卡。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

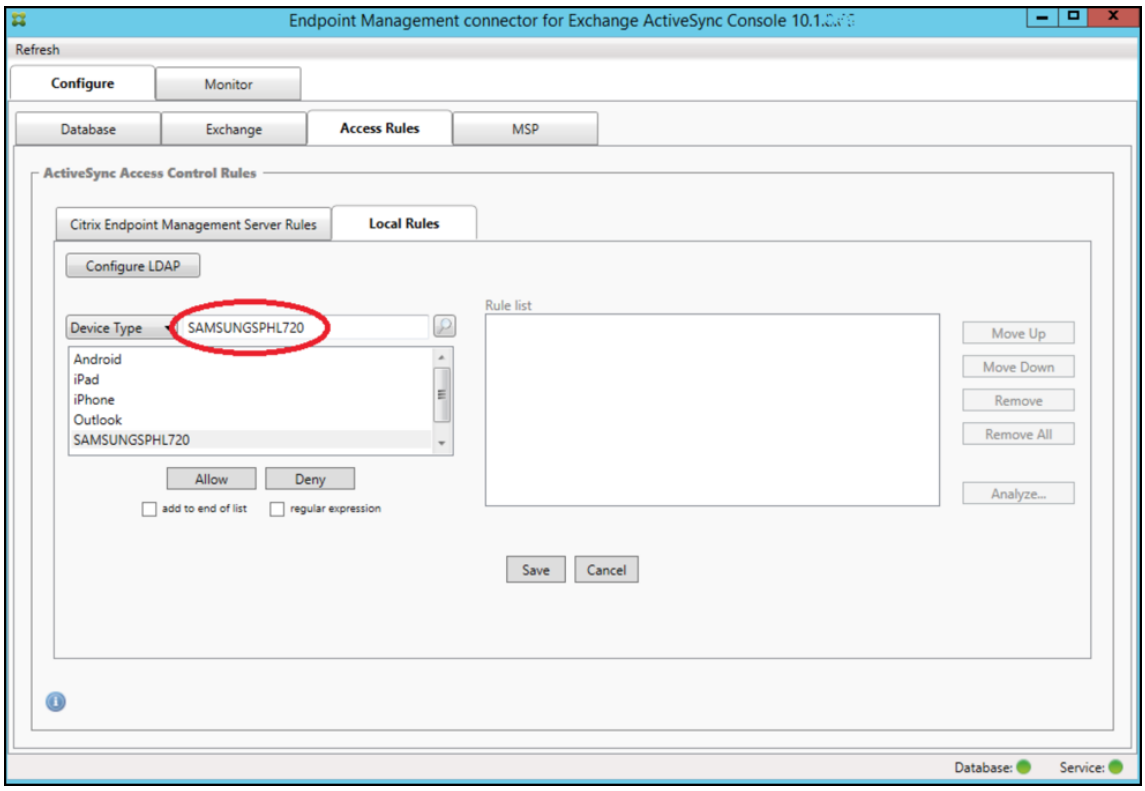


2. 在 **Device ID**（设备 ID）列表中，选择要为其创建正则表达式本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。在此示例中，已选择 **Device Type**（设备类型）字段，并且选项显示在下面的列表框中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 单击结果列表中的其中一个项目。在此示例中，已选择 **SAMSUNGSPHL720**，并显示在 **Device Type**（设备类型）旁边的文本框中。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

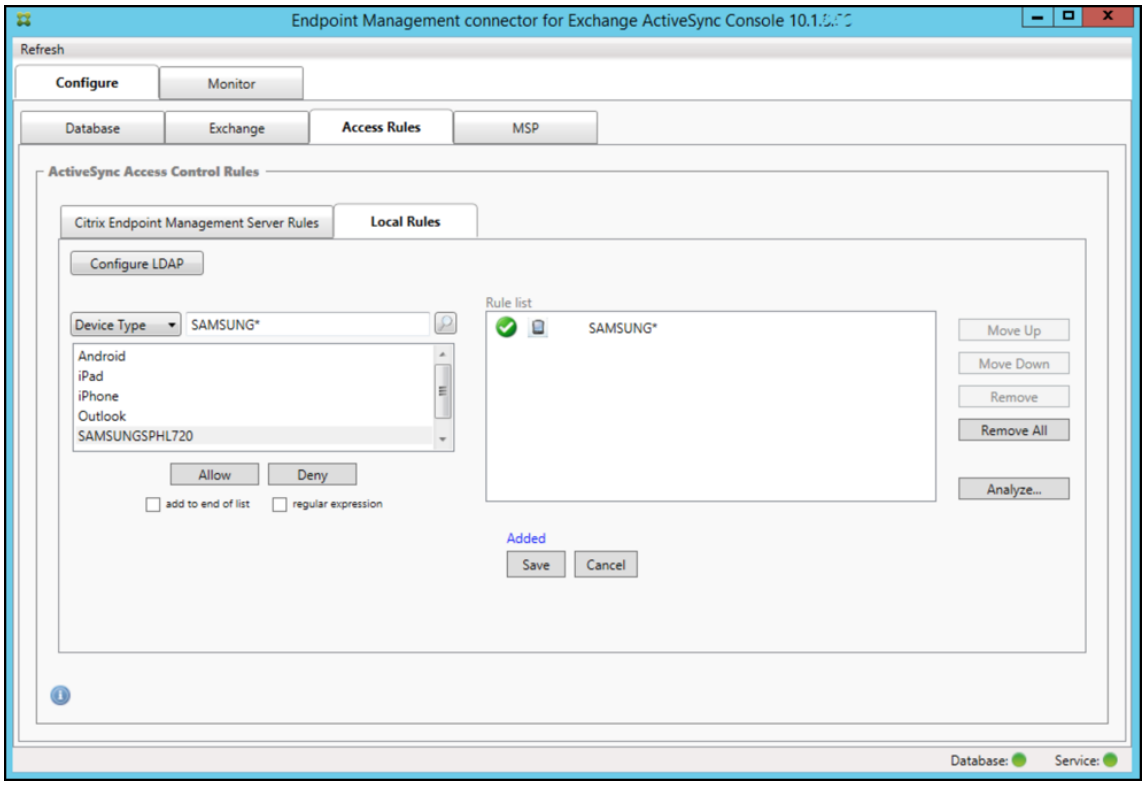
5. 要允许设备类型值中包含 “Samsung” 的所有设备类型，请按照以下步骤添加正则表达式规则：

   a. 在所选项目文本框中单击。

   b. 将文本从 **SAMSUNGSPHL720** 更改为 **SAMSUNG.***。

   c. 确保选中正则表达式复选框。

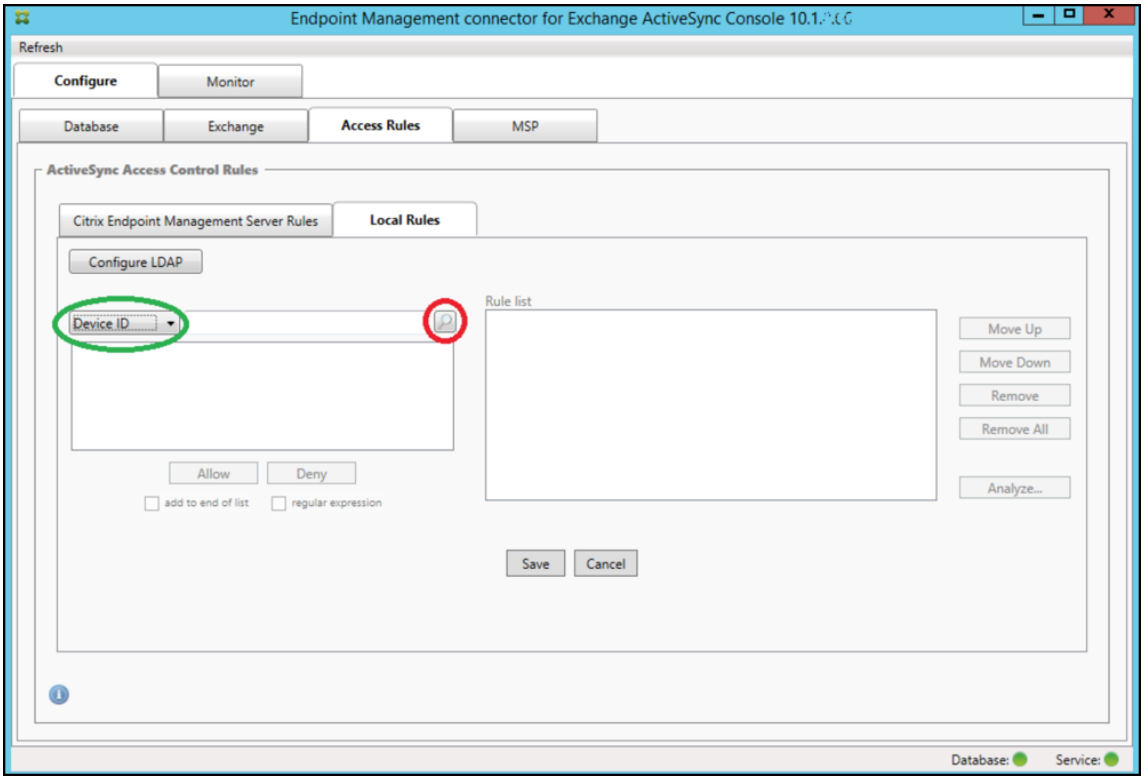
   d. 单击允许。



构建访问规则

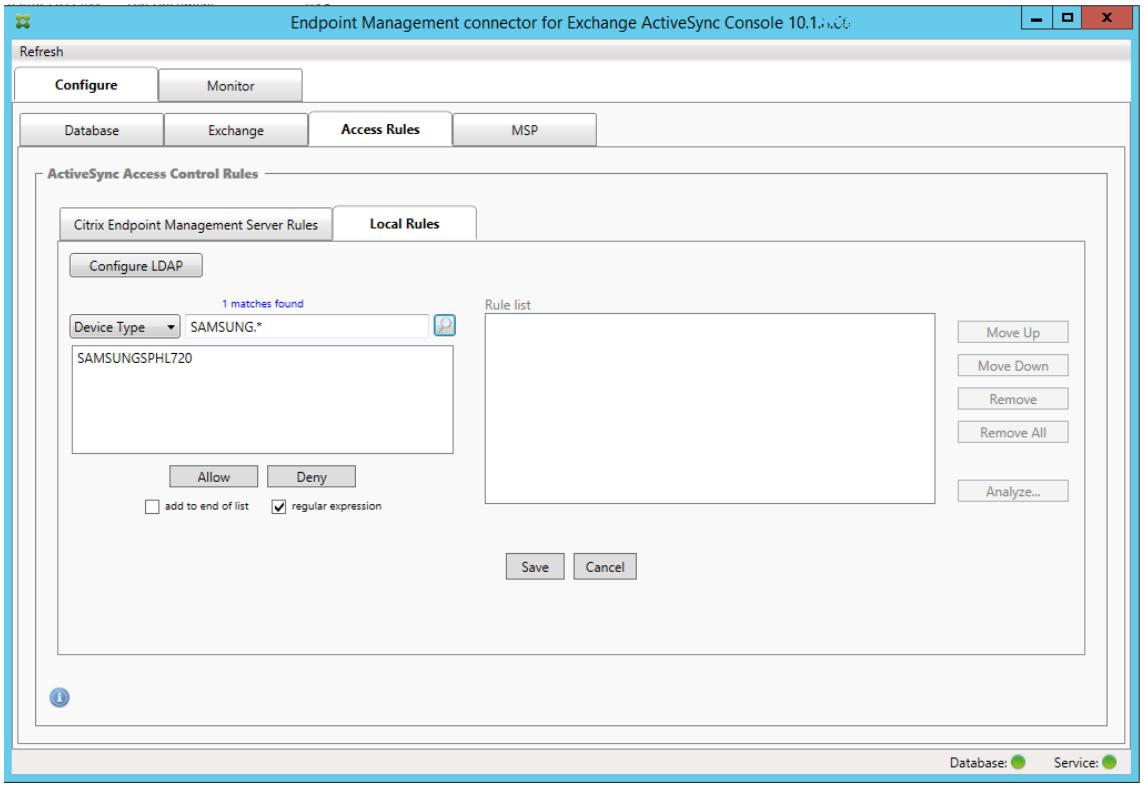
1. 单击 **Local Rules**（本地规则）选项卡。
2. 要输入正则表达式，需要使用 “Device ID”（设备 ID）列表和所选项目文本框。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 选择要匹配的字段。此示例使用 设备类型。
4. 键入正则表达式。此示例使用 `samsung.*`
5. 确保选中 “regular expression”（正则表达式）复选框，然后单击 **Allow**（允许）或 **Deny**（拒绝）。在此示例中，选择的是 **Allow**（允许）。最终结果如下所示：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

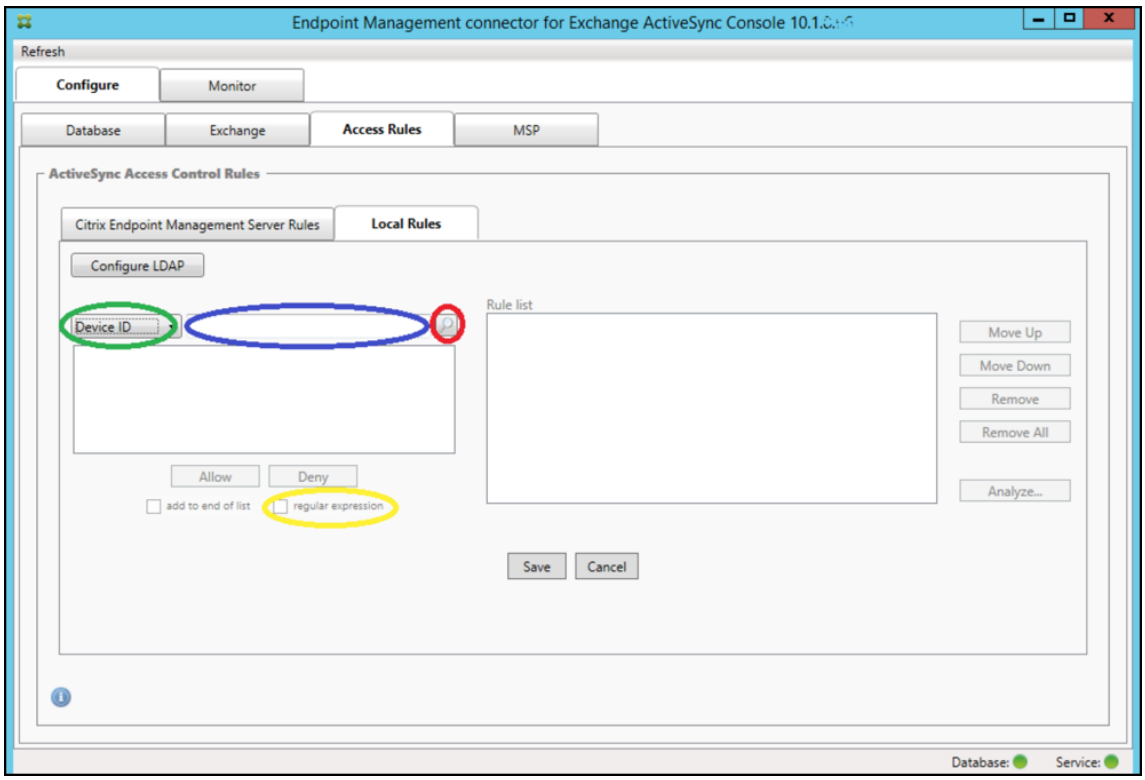


查找设备

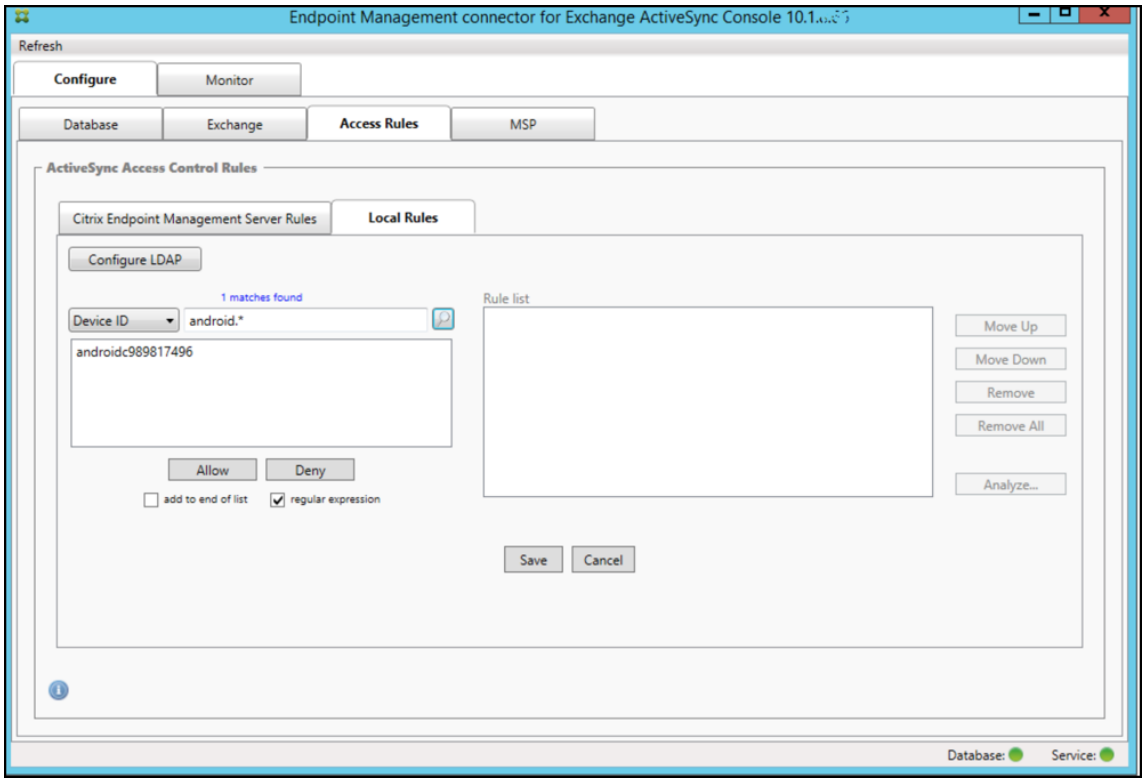
通过选中“regular expression”（正则表达式）复选框，可以针对与给定表达式匹配的特定设备运行搜索。此功能仅在成功完成主要快照时可用。即使没有计划使用正则表达式规则，您也可以使用此功能。例如，假定您要查找 ActiveSync 设备 ID 中包含文本 `workmail` 的所有设备。为此，请执行以下过程。

1. 单击 **Access Rules**（访问规则）选项卡。
2. 确保设备匹配字段选择器设置为“Device ID”（设备 ID）（默认值）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 在所选项目文本框（上图中以蓝色显示的框）内单击，然后键入 `workmail.*`。
4. 确保选中 “regular expression”（正则表达式）复选框，然后单击放大镜图标显示匹配项，如下图所示。



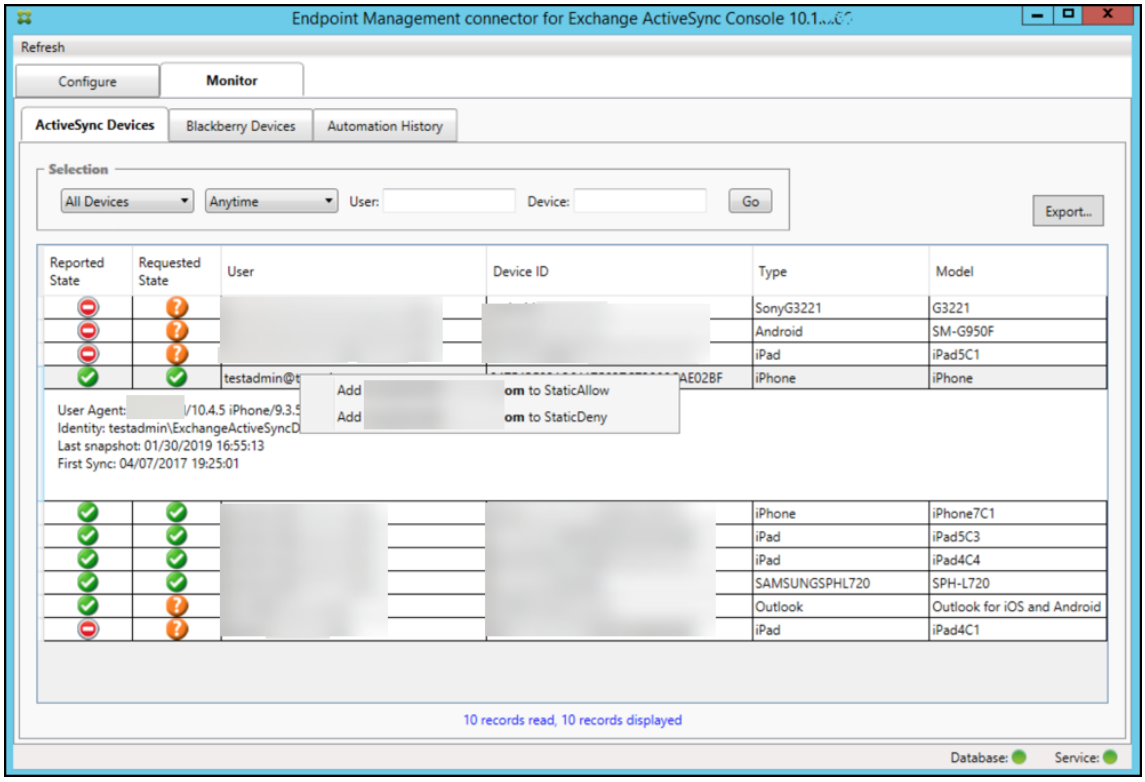
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

将单个用户、设备或设备类型添加到静态规则

可以基于 ActiveSync 设备选项卡上的用户、设备 ID 或设备类型添加静态规则。

1. 单击 **ActiveSync Devices**（ActiveSync 设备）选项卡。
2. 在列表中，右键单击用户、设备或设备类型，然后选择是允许所选内容还是拒绝所选内容。

   下图显示了选定 user1 时的“允许”/“拒绝”选项。



设备监视

通过适用于 Exchange ActiveSync 的 Endpoint Management 连接器中的监视器选项卡，可以浏览已检测到的 Exchange ActiveSync 和黑莓设备以及已发出的自动化 PowerShell 命令的历史记录。**Monitor**（监视）选项卡有以下三个选项卡：

- **ActiveSync** 设备：
  - 您可以通过单击 **Export**（导出）按钮导出显示的 ActiveSync 设备合作关系。
  - 您可以通过右键单击 **User**（用户）、**Device ID**（设备 ID）或 **Type**（类型）列并选择适当的允许或阻止规则类型来添加本地（静态）规则。
  - 要折叠展开的行，请按住 Ctrl 键并单击该展开的行。
- **Blackberry Devices**（黑莓设备）
- **Automation History**（自动化历史记录）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Configure（配置）选项卡显示所有快照的历史记录。快照历史记录显示快照发生的时间、发生了多久、检测到多少设备以及出现的任何错误。

- 在 **Exchange** 选项卡中，单击所需 Exchange Server 的信息图标。

故障排除和诊断

适用于 Exchange ActiveSync 的 Endpoint Management 连接器将错误和其他操作信息记录到其日志文件：安装文件夹\log\XmmWindowsService.log。适用于 Exchange ActiveSync 的连接器还会将重要事件记录到 Windows 事件日志中。

更改日志记录级别

适用于 Exchange ActiveSync 的 Endpoint Management 连接器包括以下日志记录级别：错误、信息、警告、调试和跟踪。

> 注意：
>
> 每个连续级别将生成更多详细信息（更多数据）。例如，错误级别提供最少的详细信息，而跟踪级别提供最多的详细信息。

要更改日志记录级别，请执行以下操作：

1. 在 `C:\Program Files\Citrix\Citrix` Endpoint Management 连接器中，打开 nlog.config 文件。
2. 在 `<rules>` 部分中，更改您更倾向于使用的日志记录级别的 *minilevel* 参数。例如：

```
1      <rules >
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. 保存该文件。

   所做的更改将立即生效。您不需要重新启动适用于 Exchange ActiveSync 的连接器。

常见错误

以下列表包括常见错误：

- 适用于 Exchange ActiveSync 的连接器服务未启动

  检查日志文件和 Windows 事件日志中的错误。包括以下典型原因：

  - 适用于 Exchange ActiveSync 的连接器服务无法访问 SQL Server。以下这些问题可能导致此情况：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

* SQL Server 服务不在运行。
* 身份验证失败。

如果已配置 “Windows Integrated”（Windows 集成）身份验证，必须允许适用于 Exchange ActiveSync 的连接器服务的用户帐户进行 SQL 登录。适用于 Exchange ActiveSync 的连接器服务的帐户默认为 “Local System”（本地系统），但是可能会更改为任何具有本地管理员权限的帐户。如果已配置 SQL 身份验证，必须在 SQL 中正确配置 SQL 登录。

故障排除工具

Support\PowerShell 文件夹中提供了一组用于故障排除的 PowerShell 实用程序。

故障排除工具将对用户的邮箱和设备执行深度分析（从而检测错误条件和潜在的故障区域）并对用户执行深度 RBAC 分析。该工具可以将所有 cmdlet 的原始输出保存到一个文本文件。

适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

November 7, 2022

XenMobile NetScaler Connector 现已更名为适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。有关 Citrix 统一产品组合的更多详细信息，请参阅 Citrix 产品指南。

适用于 Exchange ActiveSync 的连接器向 NetScaler 提供 ActiveSync 客户端的设备级别授权服务，而 Citrix Gateway 用作 Exchange ActiveSync 协议的反向代理。可以通过以下组合来控制授权：

- 您在 Endpoint Management 中定义的策略
- 由适用于 Exchange ActiveSync 的 Citrix Gateway 连接器在本地定义的规则

有关详细信息，请参阅 ActiveSync Gateway。

有关详细的参考体系结构图，请参阅体系结构。

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的当前版本为版本 8.5.3。

要下载连接器，请执行以下操作：

1. 转到 https://www.citrix.com/downloads。
2. 导航到 **Citrix Endpoint Management**（和 **Citrix XenMobile Server**）**> XenMobile Server (**本地**) >** 产品软件 **> XenMobile Server 10 >** 服务器组件。
3. 在 **Citrix Gateway** 连接器磁贴上，单击下载文件。

要安装连接器，请参阅安装适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。

> 重要：
>
> 鉴于 Microsoft 在此处宣布的身份验证更改，自 2022 年 10 月起，适用于 Exchange ActiveSync 的 Endpoint

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> Management 和 Citrix Gateway 连接器将不再支持 Exchange Online。适用于 Exchange 的 Endpoint Management 连接器将继续与 Microsoft Exchange Server（本地）结合使用。

版本 **8.5.3** 中的新增功能

- 本版本增加了对 ActiveSync 协议 16.0 和 16.1 的支持。
- 更多详细信息已添加到发送至 Google Analytics 的分析中，特别是相关的快照。[CXM-52261]

早期版本中的新增功能

> 注意：
>
> 以下“新增功能”部分在提到适用于 Exchange ActiveSync 的 Citrix Gateway 连接器时使用其以前的名称 XenMobile NetScaler Connector。名称自版本 8.5.2 起更改。

版本 **8.5.2** 中的新增功能

- XenMobile NetScaler Connector 现已更名为适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。

此版本中修复了以下问题：

- 如果在定义策略规则时使用多个条件，并且某个条件涉及用户 ID，则会出现以下问题：如果用户有多个别名，应用该规则时不会检查这些别名。[CXM-55355]

版本 **8.5.1.11** 中的新增功能

- 系统要求变更： NetScaler Connector 的当前版本需要使用 Microsoft.NET Framework 4.5。
- **Google Analytics** 支持：我们希望了解您使用 Connector 的方式，以便我们可以专注于可以改进产品的方面。
- 对 **TLS 1.1** 和 **1.2** 的支持：由于安全性的削弱，PCI 委员会正在弃用 TLS 1.0 和 TLS 1.1。对 TLS 1.2 的支持已添加到 XenMobile NetScaler Connector 中。

监视适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序提供了详细的日志记录。使用日志查看 Secure Mobile Gateway 允许或阻止的通过 Exchange Server 传输的所有流量。

使用日志选项卡可查看转发到适用于 Exchange ActiveSync 的连接器以进行授权的 ActiveSync 请求的历史记录。

此外，为确保适用于 Exchange ActiveSync 的连接器 Web 服务运行，还可将以下 URL 加载到连接器服务器上的浏览器中：`https://<host:port>/services/ActiveSync/Version`。如果 URL 以字符串形式返回产品版本，则 Web 服务为可响应。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

使用适用于 **Exchange ActiveSync** 的连接器模拟 **ActiveSync** 流量

可以使用适用于 Exchange ActiveSync 的 Citrix Gateway 连接器模拟启用了您的策略时的 ActiveSync 流量。在连接器配置实用程序中，单击 **Simulator**（模拟器）选项卡。结果将根据您配置的规则显示策略的应用方式。

为适用于 **Exchange ActiveSync** 的连接器选择过滤器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器过滤器的工作方式是针对给定策略违规情况或属性设置分析设备。如果设备满足条件，则将设备放入设备列表中。此设备列表既不是允许列表也不是阻止列表。它是满足定义条件的设备的列表。以下过滤器可用于 Endpoint Management 中的适用于 Exchange ActiveSync 的连接器。每个过滤器均有两个选项：允许或拒绝。

- 匿名设备：允许或拒绝在 Endpoint Management 中已注册但用户的身份未知的设备。例如，如果用户具有过期的 Active Directory 密码或未知凭据，已注册的用户将具有未知身份。
- 禁止的应用程序：基于策略中的阻止列表定义的设备列表以及是否存在阻止列表中的应用程序来允许或拒绝设备。
- 隐式允许**/**拒绝：创建不满足其他任何过滤器规则条件的所有设备的设备列表，并根据该列表允许或拒绝。“隐式允许/拒绝”选项可确保“设备”选项卡中的适用于 Exchange ActiveSync 的连接器状态为已启用，并显示您设备的连接器状态。“隐式允许/拒绝”选项还可以控制所有其他未选定的连接器过滤器。例如，连接器拒绝运行阻止列表中的应用程序。但是，连接器允许所有其他过滤器，因为“隐式允许/拒绝”选项设置为允许。
- 不活动设备：创建在指定时间内与 Endpoint Management 没有通信的设备的设备列表。这些设备被视为非活动状态。因此，过滤器会允许或拒绝这些设备。
- 缺少所需的应用程序：用户注册时，将收到必须安装的所需应用程序的列表。“缺少所需的应用程序”过滤器指示一个或多个应用程序不再存在；例如，用户删除了一个或多个应用程序。
- 非推荐应用程序：用户注册时，用户将收到要安装的应用程序列表。“非推荐应用程序”过滤器会在设备中检查不在该列表中的应用程序。
- 不合规密码：创建设备上没有通行码的所有设备的设备列表。
- 不合规设备：允许您拒绝或允许满足自己内部 IT 合规条件的设备。合规是由名为“不合规”的设备属性定义的任意设置，它是一个可以为真或假的布尔标志。（您可以手动创建此属性并设置值。或者，您可以根据设备是否满足特定条件，使用自动操作在设备上创建此属性。）
  - 不合规 **= True**：如果设备不满足您 IT 部门设定的合规标准和策略定义，则该设备不合规。
  - 不合规 **= False**：如果设备满足您 IT 部门设定的合规标准和策略定义，则该设备合规。
- 吊销状态：创建所有已吊销设备的设备列表，并根据吊销状态允许或拒绝。
- 已获得 **Root** 权限的 **Android** 设备**/**已越狱的 **iOS** 设备：创建包括所有标记为获得 root 权限的设备的设备列表，并根据获得 root 权限的状态允许或拒绝。
- 未托管设备：创建包括 Endpoint Management 数据库中所有设备的设备列表。在阻止模式下部署移动应用程序网关。

配置与适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的连接

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器通过安全 Web 服务与 Endpoint Management 和其他远程配置提供程序进行通信。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. 在适用于 Exchange ActiveSync 的连接器配置实用程序中，单击 **Config Providers**（配置提供程序）选项卡，然后单击 **Add**（添加）。
2. 在 **Config Providers**（配置提供程序）对话框中的 **Name**（名称）中，输入具有管理权限并用于 Endpoint Management 服务器的基本 HTTP 授权的用户名。
3. 在 **URL** 中，输入 Endpoint Management GCS 的 Web 地址，格式通常为 `https://<FQDN>/<instanceName>/services/<MagConfigService>`。*MagConfigService* 名称区分大小写。
4. 在 **Password**（密码）中，输入用于 Endpoint Management 服务器的基本 HTTP 授权的密码。
5. 在 **Managing Host**（管理主机）中，输入适用于 Exchange ActiveSync 的连接器的服务器名称。
6. 在 **Baseline Interval**（基准时间间隔）中，指定从 Endpoint Management 提取新刷新的动态规则集的时间间隔。
7. 在 **Delta interval**（时间间隔差）中，指定提取动态规则更新的时间间隔。
8. 在 **Request Timeout**（请求超时）中，指定服务器请求超时的时间间隔。
9. 在 **Config Provider**（配置提供程序）中，选择配置提供程序服务器实例是否提供策略配置。
10. 在 **Events Enabled**（事件已启用）中，如果希望在设备被阻止时适用于 Exchange ActiveSync 的连接器通知 Endpoint Management，则启用此选项。如果要在任何 Endpoint Management 自动化操作中使用连接器规则，则需要使用此选项。
11. 依次单击 **Save**（保存）和 **Test Connectivity**（测试连接），测试网关到配置提供程序的连接。如果连接失败，请检查本地防火墙设置是否允许连接，或与管理员联系。
12. 连接成功后，取消选中 **Disabled**（禁用）复选框，然后单击 **Save**（保存）。

添加配置提供程序时，适用于 Exchange ActiveSync 的连接器会自动创建一个或多个与该提供程序关联的策略。`NewPolicyTemplate` 部分的 `config\policyTemplates.xml` 中包含的模板定义将定义策略。会为在本节中定义的每个策略元素创建一个新策略。

如果满足以下条件，操作员可以添加、删除或修改策略元素：策略元素符合架构定义，并且不修改标准替换字符串（用括号括起）。接下来，为提供程序添加新组并更新策略以将新组包括在内。

从 **Endpoint Management** 中导入策略

1. 在适用于 Exchange ActiveSync 的连接器配置实用程序中，单击 **Config Providers**（配置提供程序）选项卡，然后单击 **Add**（添加）。
2. 在 **Config Providers**（配置提供程序）对话框中的 **Name**（名称）中，输入用于 Endpoint Management 的基本 HTTP 授权的用户名。用户必须具有管理权限。
3. 在 **URL** 中，输入 Endpoint Management Gateway Configuration Service (GCS) 的 Web 地址，格式通常为 `https://<xdmHost>/xdm/services/<MagConfigService>`。MagConfigService 名称区分大小写。
4. 在 **Password**（密码）中，输入用于 Endpoint Management 服务器的基本 HTTP 授权的密码。
5. 单击 **Test Connectivity**（测试连接），测试网关到配置提供程序的连接。如果连接失败，请检查本地防火墙设置是否允许连接，或与管理员核查。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

6. 连接成功后，取消选中 **Disabled**（禁用）复选框，然后单击 **Save**（保存）。
7. 在 **Managing Host**（管理主机）中，保留本地主机计算机的默认 DNS 名称。在多个 Forefront Threat Management Gateway (TMG) 服务器配置在一个阵列中时，此设置用于协调与 Endpoint Management 的通信。

   保存设置后，打开 GCS。

配置适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器策略模式

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器可以在以下 6 种模式下运行：

- **Allow All**（全部允许）：此策略模式授权对通过适用于 Exchange ActiveSync 的连接器的所有流量进行访问。不使用其他过滤规则。
- **Deny All**（全部拒绝）：此策略模式阻止通过适用于 Exchange ActiveSync 的连接器的所有流量进行访问。不使用其他过滤规则。
- **Static Rules: Block Mode**（静态规则: 阻止模式）：此策略模式运行在结尾具有隐式拒绝或阻止语句的静态规则。适用于 Exchange ActiveSync 的连接器会阻止其他过滤规则不允许使用的设备。
- **Static Rules: Permit Mode**（静态规则: 允许模式）：此策略模式运行在结尾具有隐式许可或允许语句的静态规则。允许未被阻止的设备或被其他过滤规则拒绝的设备通过适用于 Exchange ActiveSync 的连接器。
- **Static + ZDM Rules: Block Mode**（静态 + ZDM 规则: 阻止模式）。此策略模式首先运行静态规则，然后执行来自 Endpoint Management 的、在结尾具有隐式拒绝或阻止语句的动态规则。将根据已定义的过滤器和 Endpoint Management 规则允许或拒绝设备。与定义的过滤器和规则不匹配的任何设备都会被阻止。
- **Static + ZDM Rules: Permit Mode**（静态 + ZDM 规则: 许可模式）。此策略模式首先运行静态规则，然后执行来自 Endpoint Management 的、在结尾具有显式许可或允许语句的动态规则。将根据已定义的过滤器和 Endpoint Management 规则允许或拒绝设备。与定义的过滤器和规则不匹配的任何设备都会被允许。

适用于 Exchange ActiveSync 的连接器进程根据从 Endpoint Management 收到的基于 iOS 和 Windows 的移动设备的唯一 ActiveSync ID 允许或阻止动态规则。Android 设备的特性由于制造商不同而有所不同，且有些设备没有准备好公开唯一的 ActiveSync ID。为进行补偿，Endpoint Management 会发送 Android 设备的用户 ID 信息，以便做出允许或阻止决定。因此，如果用户只有一个 Android 设备，则其允许和阻止功能正常。如果用户具有多个 Android 设备，则所有设备都被允许，因为无法区别 Android 设备。可以将网关配置为通过 ActiveSyncID（如果已知）静态阻止这些设备。还可以将网关配置为根据设备类型或用户代理进行阻止。

要指定策略模式，请在 SMG Controller 配置实用程序中执行以下操作：

1. 单击 **Path Filters**（路径过滤器）选项卡，然后单击 **Add**（添加）。
2. 在 **Path Properties**（路径属性）对话框中，从 **Policy**（策略）列表中选择策略模式，然后单击 **Save**（保存）。

可以在配置实用程序的 **Policies**（策略）选项卡中查看这些规则。这些规则将在适用于 Exchange ActiveSync 的连接器上自上而下处理。“Allow”（允许）策略显示时带有绿色选中标记。“Deny”（拒绝）策略显示为红色圆圈，中间横穿一条直线。要刷新屏幕并查看最新更新的规则，请单击 **Refresh**（刷新）。也可在 config.xml 文件中修改规则的顺序。

要测试规则，请单击 **Simulator**（模拟器）选项卡。在字段中指定值。可以从日志中获取值。结果消息指定“允许”或“阻止”。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置静态规则

请输入具有 ActiveSync 连接 HTTP 请求的 ISAPI 过滤功能读取的值的静态规则。静态规则支持适用于 Exchange ActiveSync 的连接器根据下列准则允许或阻止流量：

- **User**（用户）：适用于 Exchange ActiveSync 的连接器使用在设备注册时捕获的授权用户值和名称结构。该结构的常见形式是 `domain\username`，由运行 Endpoint Management 的服务器引用，该服务器通过 LDAP 连接到 Active Directory。连接器配置实用程序中的 **Log**（日志）选项卡显示通过连接器传递的值。如果连接器必须确定值结构或者如果结构不同，则会传递这些值。
- **DeviceID (ActiveSyncID)**：也称为所连接设备的 ActiveSyncID。此值通常可在 Endpoint Management 控制台的特定设备属性页面中找到。此值也可从适用于 Exchange ActiveSync 的连接器配置实用程序的 **Log**（日志）选项卡中筛选出来。
- **DeviceType**（设备类型）：适用于 Exchange ActiveSync 的连接器可确定设备是 iPhone、iPad 还是其他设备类型，并能根据准则加以允许或阻止。与其他值一样，连接器配置实用程序可显示为 ActiveSync 连接处理的所有已连接设备的类型。
- **UserAgent**（用户代理）：包含有关所使用的 ActiveSync 客户端的信息。通常情况下，指定的值对应于移动设备平台的特定操作系统内部版本和版本。

在服务器上运行的适用于 Exchange ActiveSync 的连接器配置实用程序始终管理静态规则。

1. 在 SMG Controller 配置实用程序中，单击 **Static Rules**（静态规则）选项卡，然后单击 **Add**（添加）。
2. 在 **Static Rule Properties**（静态规则属性）对话框中，指定要用作条件的值。例如，可通过输入用户名（例如 AllowedUser）然后取消选中 **Disabled**（禁用）复选框，输入允许访问的用户。
3. 单击保存。

   静态规则现在即生效。此外，还可使用正则表达式来定义值，但必须在 config.xml 文件中启用规则处理模式。

配置动态规则

Endpoint Management 中的设备策略和属性定义动态规则，并且可以触发动态适用于 Exchange ActiveSync 的连接器过滤器。触发器建立在是否存在策略冲突或属性设置的基础之上。适用于 Exchange ActiveSync 的连接器过滤器的工作方式是针对给定策略违规情况或属性设置分析设备。如果设备满足条件，则将设备放入设备列表中。此设备列表既不是允许列表也不是阻止列表。它是满足定义条件的设备的列表。以下配置选项可用于定义是否要使用适用于 Exchange ActiveSync 的连接器允许或拒绝“设备列表”中的设备。

> 注意：
>
> 请使用 Endpoint Management 控制台配置动态规则。

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **ActiveSync Gateway**。此时将显示 ActiveSync Gateway 页面。
3. 在激活以下规则中，选择要激活的一个或多个规则。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

4. 在“仅限 Android”中的将 **Android** 域用户发送到 **ActiveSync Gateway** 中，单击是以确保 Endpoint Management 将 Android 设备信息发送到 Secure Mobile Gateway。

   启用了此选项后，如果 Endpoint Management 没有设备用户的 ActiveSync 标识符，Endpoint Management 会将 Android 设备信息发送到连接器。

通过编辑适用于 **Exchange ActiveSync** 的连接器的 **XML** 文件来配置自定义策略

可以在适用于 Exchange ActiveSync 的连接器配置实用程序的策略选项卡上查看默认配置中的基本策略。如果要创建自定义策略，可以编辑适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的 XML 配置文件 (config\config.xml)。

1. 在文件中找到 **PolicyList** 部分，然后添加新的 **Policy** 元素。
2. 如果还需要新组，例如另一个静态组或支持另一个 GCP 的组，请将新 **Group** 元素添加到 **GroupList** 部分。
3. 也可以通过重新排列 **GroupRef** 元素，更改现有策略中组的顺序。

配置适用于 **Exchange ActiveSync** 的连接器的 **XML** 文件

适用于 Exchange ActiveSync 的连接器使用 XML 配置文件表示连接器的各项操作。此外，此文件还指定组文件和过滤器在评估 HTTP 请求时采取的关联操作。默认情况下，此文件命名为 config.xml 且位于以下位置：..\Program Files\Citrix\XenMobile NetScaler Connector\config。

GroupRef 节点

GroupRef 节点定义逻辑组名称。默认值为 AllowGroup 和 DenyGroup。

> 注意：
>
> GroupRef 节点在 GroupRefList 节点中出现的顺序非常重要。

GroupRef 节点的 ID 值标识逻辑容器或用于匹配特定用户帐户或设备的成员集合。操作属性指定过滤器处理与集合中的规则匹配的成员的方式。例如，与 AllowGroup 集中的规则匹配的用户帐户或设备将为“passes”。pass 表示允许其访问 Exchange CAS。与 DenyGroup 集中的规则匹配的用户帐户或设备为“rejected”。rejected 表示不允许其访问 Exchange CAS。

特定的用户帐户/设备或组合满足两个组中的规则时，会使用优先级约定来引导请求的结果。优先级通过 GroupRef 节点在 config.xml 文件中的自上而下的顺序体现。GroupRef 节点以优先级顺序排序。“允许”组中针对给定条件的规则将始终优先于“拒绝”组中针对相同条件的规则。

组节点

此外，config.xml 还定义组节点。这些节点将逻辑容器 AllowGroup 和 DenyGroup 链接到外部 XML 文件。存储在外部文件中的条目构成过滤器规则的基础。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 在此版本中，仅支持外部 XML 文件。

默认安装会在配置中实施两个 XML 文件：allow.xml 和 deny.xml。

配置适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

可以将适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置为基于以下属性，选择性地阻止或允许 ActiveSync 请求：**Active Sync** 服务 **ID**、设备类型、用户代理（设备操作系统）、授权用户和 **ActiveSync** 命令。

默认配置支持静态和动态组的组合。通过使用 SMG Controller 配置实用程序维护静态组。静态组可由已知类别的设备组成，如使用给定用户代理的所有设备。

名为网关配置提供程序的外部源负责维护动态组。适用于 Exchange ActiveSync 的连接器会定期连接这些组。Endpoint Management 可以将允许和阻止设备与用户的组导出到适用于 Exchange ActiveSync 的连接器。

名为网关配置提供程序的外部源负责维护动态组。适用于 Exchange ActiveSync 的连接器定期收集动态组。Endpoint Management 可以将允许和阻止设备与用户的组导出到连接器。

策略是组的有序列表，其中每个组都有关联的操作（允许或阻止）和组成员列表。一个策略可以有任何数量的组。策略内组的排序很重要，因为找到匹配项时就会执行组的操作，不会评估后续的组。

成员定义匹配请求中属性的方式。可以匹配单个属性，如设备 ID，或多个属性，如设备类型和用户代理。

为适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器选择安全模型

建立安全模型对于为任何规模的组织成功部署移动设备都至关重要。默认情况下，通常使用受保护或被隔离的网络控制来允许访问用户、计算机或设备。这种做法并非始终属于理想做法。对于确保移动设备的安全性，每个管理 IT 安全的组织的做法可能会略有不同，或者采用定制的方法。

相同的逻辑适用于移动设备安全性。由于移动设备和类型、每个用户的移动设备以及操作系统平台和应用程序的数量都非常大，因此，使用宽容模型属于较差的选择。在大多数组织中，受限模式是最合乎逻辑的选择。

Citrix 允许适用于 Exchange ActiveSync 的连接器与 Endpoint Management 集成的配置方案如下所示：

宽容模型（许可模式）

宽容安全模型的运行前提是，默认情况下允许或授权任何设备进行访问。只有通过规则和过滤，某些设备才将被阻止并应用限制。宽容安全模型非常适合对移动设备的安全要求相对宽松的组织。该模型仅应用限制性控制来在适当的位置拒绝访问（策略规则失败时）。

限制性模型（阻止模式）

受限安全模型的运行前提是，默认情况下不允许或授权任何设备进行访问。通过安全检查点的任何访问都要进行过滤和检查，并且拒绝访问，除非允许访问的规则获得通过。受限安全模型适合对移动设备具有相对严格的安全标准的组织。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

该模式仅在所有允许访问的规则都通过时，才授权访问网络服务的使用和功能。

管理适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

可以使用适用于 Exchange ActiveSync 的 Citrix Gateway 连接器构建访问控制规则。这些规则允许或阻止访问来自托管设备的 ActiveSync 连接请求。访问基于设备状态、应用程序允许列表或阻止列表以及其他合规条件。

通过使用适用于 Exchange ActiveSync 的连接器配置实用程序，可以构建强制实施公司电子邮件策略的动态和静态规则。这些规则和策略允许您阻止违反合规性标准的用户。也可设置电子邮件附件加密，使通过您的 Exchange Server 到达托管设备的所有附件都被加密。只有具有托管设备的授权用户才能查看加密的附件。

卸载 **XNC**

1. 使用管理员帐户运行 XncInstaller.exe。
2. 按照屏幕说明完成卸载。

安装、升级或卸载适用于 **Exchange ActiveSync** 的连接器

1. 使用管理员帐户运行 XncInstaller.exe 以安装适用于 Exchange ActiveSync 的连接器，或者升级或删除现有连接器。
2. 按照屏幕说明完成安装、升级或卸载。

安装适用于 Exchange ActiveSync 的连接器后，必须手动重新启动 Endpoint Management 配置服务和通知服务。

安装适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

可以将适用于 Exchange ActiveSync 的连接器安装在其自己的服务器上，或与 Endpoint Management 安装在相同的服务器上。

可出于以下原因考虑将适用于 Exchange ActiveSync 的连接器安装在其自己的服务器上（与 Endpoint Management 分开）：

- Endpoint Management 服务器在云端被远程托管（物理位置）
- 如果您不希望 Endpoint Management 服务器的重新启动影响适用于 Exchange ActiveSync 的连接器（可用性）。
- 如果您希望服务器的系统资源完全专用于适用于 Exchange ActiveSync 的连接器（性能）

适用于 Exchange ActiveSync 的连接器在服务器上放置的 CPU 负载取决于托管的设备数量。一般建议是，如果连接器与 Endpoint Management 部署在同一台服务器上，则会再配置一个 CPU 核心。对于大量设备（超过 50000 个），如果没有群集环境，可能需要预配更多核心。连接器的内存占用量不足，无法保证更多内存。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的系统要求

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器通过在 Citrix Gateway 设备上配置的 SSL 桥接与 Citrix Gateway 进行通信。该桥接允许设备将所有安全流量直接桥接到 Endpoint Management。适用于 Exchange ActiveSync 的连接器要求的最低系统配置如下：

组件	要求
计算机和处理器	733 MHz Pentium III 733 MHz 或更高版本的处理器。2.0 GHz Pentium III 或更高版本的处理器（建议）
Citrix Gateway	Citrix Gateway 设备，软件版本 10
内存	1 GB
硬盘	具有 150 MB 可用硬盘空间的 NTFS 格式本地分区
操作系统	Windows Server 2016、Windows Server 2012 R2 或 Windows Server 2008 R2 Service Pack 1。必须是基于英语的服务器。对 Windows Server 2008 R2 Service Pack 1 的支持将于 2020 年 1 月 14 日结束。
其他设备	与主机操作系统兼容的网络适配器（用于与内部网络通信）
Microsoft .NET Framework	版本 8.5.1.11 需要使用 Microsoft.NET Framework 4.5。
显示	VGA 或更高分辨率的显示器

适用于 Exchange ActiveSync 的连接器的主机计算机要求的最小可用硬盘空间如下：

- 应用程序： 10 - 15 MB（建议 100 MB）
- 日志记录： 1 GB（建议 20 GB）

有关 Exchange ActiveSync 连接器的平台支持的信息，请参阅 支持的设备操作系统。

设备电子邮件客户端

并非所有电子邮件客户端都一致地为设备返回相同的 ActiveSync ID。由于适用于 Exchange ActiveSync 的连接器要求每个设备具有唯一的 ActiveSync ID，因此，仅支持为每个设备一致地生成相同的唯一 ActiveSync ID 的电子邮件客户端。Citrix 已测试这些电子邮件客户端，并且这些客户端在执行时没有错误：

- Samsung 本机电子邮件客户端
- iOS 本机电子邮件客户端

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

部署适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器使您可以使用 Citrix Gateway 来代理并平衡 Endpoint Management 服务器与 Endpoint Management 托管设备之间的通信负载。适用于 Exchange ActiveSync 的连接器定期与 Endpoint Management 通信以同步策略。可以将适用于 Exchange ActiveSync 的连接器和 Endpoint Management 共同或单独组成群集。

适用于 **Exchange ActiveSync** 的连接器组件

- 适用于 **Exchange ActiveSync** 的连接器服务：此服务提供一个 REST Web 服务界面，Citrix Gateway 可以调用该界面以确定来自设备的 ActiveSync 请求是否获得授权。
- **Endpoint Management** 配置服务：此服务与 Endpoint Management 进行通信，以将 Endpoint Management 策略更改与适用于 Exchange ActiveSync 的连接器同步。
- **Endpoint Management** 通知服务：此服务将未经授权的设备访问通知发送到 Endpoint Management。这样，Endpoint Management 可以采取恰当的措施，例如通知用户设备被阻止的原因。
- 适用于 **Exchange ActiveSync** 的连接器配置实用程序：此应用程序允许管理员配置并监视适用于 Exchange ActiveSync 的连接器。

设置适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的侦听地址

要使适用于 Exchange ActiveSync 的 Citrix Gateway 连接器接收来自 Citrix Gateway 的授权传输 ActiveSync 流量的请求，请执行以下操作。指定适用于 Exchange ActiveSync 的连接器在其上侦听 Citrix Gateway Web 服务调用的端口。

1. 从开始菜单中，选择适用于 Exchange ActiveSync 的连接器配置实用程序。
2. 单击 **Web Service**（Web 服务）选项卡，然后键入连接器 Web 服务的侦听地址。可以选择 **HTTP** 或 **HTTPS**，或者同时选择两者。如果适用于 Exchange ActiveSync 的连接器与 Endpoint Management 的位置相同（安装在同一服务器上），请选择与 Endpoint Management 不冲突的端口值。
3. 配置值后，单击 **Save**（保存），然后单击 **Start Service**（启动服务），启动 Web 服务。

在适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器中配置设备访问控制策略

要配置将应用于托管设备的访问控制策略，请执行以下操作：

1. 在适用于 Exchange ActiveSync 的连接器配置实用程序中，单击 **Path Filters**（路径过滤器）选项卡。
2. 选择第一行 **Microsoft-Server-ActiveSync is for ActiveSync**（Microsoft-Server-ActiveSync 适用于 ActiveSync），然后单击 **Edit**（编辑）。
3. 在 **Policy**（策略）列表中，选择所需策略。对于包含 Endpoint Management 策略的策略，请选择 **Static + ZDM: Permit Mode**（静态 **+ ZDM:** 允许模式）或 **Static + ZDM: Block Mode**（静态 **+ ZDM:** 阻止模式）。这些策略将本地（或静态）规则与 Endpoint Management 的规则组合在一起。Permit Mode（许可模式）表示允许未被规则明确识别的所有设备访问 ActiveSync。Block Mode（阻止模式）表示阻止此类设备。
4. 设置策略后，单击 **Save**（保存）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

配置与 **Endpoint Management** 的通信

指定要与适用于 Exchange ActiveSync 的 Citrix Gateway 连接器和 Citrix Gateway 结合使用的 Endpoint Management 服务器的名称和属性。

> 注意：
>
> 此任务假定您已安装并配置 Endpoint Management。Exchange ActiveSync 配置实用程序使用“适用于 Endpoint Management 的配置提供程序”这一术语。

1. 在适用于 Exchange ActiveSync 的连接器配置实用程序中，单击 **Config Providers**（配置提供程序）选项卡，然后单击 **Add**（添加）。
2. 输入您在此部署中使用的 Endpoint Management 服务器的名称和 URL。如果您在多租户部署中部署了多个 Endpoint Management 服务器，则对每个服务器实例而言，此名称必须唯一。
3. 在 **URL** 中，输入 Endpoint Management 全局配置提供程序 (GCP) 的 Web 地址，格式通常为 `https://<FQDN>/<instanceName>/services/<MagConfigService>`。*MagConfigService* 名称区分大小写。
4. 在 **Password**（密码）中，输入用于 Endpoint Management Web 服务器的基本 HTTP 授权的密码。
5. 在 **Managing Host**（管理主机）中，输入安装了适用于 Exchange ActiveSync 的连接器的服务器名称。
6. 在 **Baseline Interval**（基准时间间隔）中，指定从 Endpoint Management 提取新刷新的动态规则集的时间间隔。
7. 在 **Request Timeout**（请求超时）中，指定服务器请求超时的时间间隔。
8. 在 **Config Provider**（配置提供程序）中，选择配置提供程序服务器实例是否提供策略配置。
9. 在 **Events Enabled**（事件已启用）中，如果希望在设备被阻止时 Secure Mobile Gateway 通知 Endpoint Management，则启用此选项。如果在任何 Endpoint Management 自动操作中都使用了 Secure Mobile Gateway 规则，则此选项是必需的。
10. 配置服务器后，单击 **Test Connectivity**（测试连接），测试与 Endpoint Management 的连接。
11. 建立连接后，单击 **Save**（保存）。

为适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器部署冗余和可扩展性

要扩展适用于 Exchange ActiveSync 的 Citrix Gateway 连接器和 Endpoint Management 部署，可在多个 Windows Server 上安装适用于 Exchange ActiveSync 的连接器实例。所有连接器实例都指向同一个 Endpoint Management 实例。然后，您可以使用 Citrix Gateway 来平衡服务器的负载。

适用于 Exchange ActiveSync 的连接器配置有两种模式：

- 在非共享模式下，每个适用于 Exchange ActiveSync 的连接器实例都与一个 Endpoint Management 服务器进行通信，并且保存所产生策略的自己的私有副本。例如，对于 Endpoint Management 服务器的群集，您可以在每个 Endpoint Management 服务器上运行一个连接器实例。然后，连接器从本地 Endpoint Management 实例获取策略。
- 在共享模式下，一个适用于 Exchange ActiveSync 的连接器节点被指定为主节点。连接器与 Endpoint Management 进行通信。其他节点通过 Windows 网络共享或 Windows（或第三方）复制功能共享产生的配

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

置。

整个适用于 Exchange ActiveSync 的连接器配置在一个文件夹中（由多个 XML 文件组成）。连接器进程将检测对此文件夹中的任何文件所做的更改，并自动重新加载配置。共享模式中的主节点没有故障转移功能。但是，系统可以容忍主服务器关闭几分钟（例如，重新启动）。上次已知良好的配置在连接器进程中缓存。

高级概念

December 3, 2021

“Endpoint Management 高级概念”文章深入介绍了 Endpoint Management 的产品信息。目地是通过专业技巧帮助缩短部署时间。这些文章可能会引用编写了相关内容的技术专家的观点。

有关终端节点管理环境的决策点、建议、常见问题和使用案例，请参阅本节中的 Endpoint Management 部署 。

有关 Endpoint Management 的社区支持论坛，请参阅 Citrix Discussions。

Endpoint Management 部署

December 3, 2021

规划 Endpoint Management 部署时，需要考虑多种因素。应选择什么设备？应如何管理设备？如何确保您的网络在提供出色的用户体验的同时保持安全？需要配备哪些硬件以及如何对其进行故障排除？本部分中的文章旨在帮助回答这些问题。包括的内容为各种用例以及与涵盖您的部署顾虑的主题有关的建议。

请谨记，指导原则或建议可能不适用于所有环境或用例。请务必先设置一个测试环境，然后再在 Endpoint Management 部署中使用。

本部分中的文章涵盖以下领域：

- 评估：规划您的部署时的常见用例以及需要考虑的问题。
- 设计和配置：设计和配置您的环境的建议
- 运行和监视：确保正在运行的环境平稳运行。

评估

与任何部署相同，您的首要任务应为评估自己的需求。您对 Endpoint Management 的主要需求是什么？需要管理环境中的每个设备，只管理应用程序，还是两者都需要管理？您的 Endpoint Management 环境需要什么级别的安全性？让我们先了解一下规划您的部署时的常见用例以及需要考虑的问题。

- 管理模式
- 设备要求

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 安全性和用户体验
- 应用程序
- 用户社区
- 电子邮件策略
- Endpoint Management 集成

设计和配置

完成部署需求的评估后，可以决定如何设计和配置您的环境。计划的项目包括：

- 选择您的服务器硬件
- 设置应用程序和设备策略
- 获取注册的用户

本节介绍了其中每种场景的用例和建议等。

- 与 Citrix Gateway 和 Citrix ADC 集成
- MDX 应用程序的 SSO 和代理注意事项
- 身份验证
- 服务器属性
- 设备和应用程序策略
- 用户注册选项

运行和监视

Endpoint Management 环境启动并运行后，您将希望对其进行监视以确保平稳运行。监视部分探讨了您可以从何处查找 Endpoint Management 及其组件生成的各种日志和消息以及如何阅读这些日志。本部分内容还介绍了您可以执行的各种常见故障排除步骤以缩短客户支持反馈时间。

- 应用程序预配和取消预配
- 基于控制板的操作
- 基于角色的访问控制和 Endpoint Management 支持
- 监视和支持
- Citrix 支持过程

管理模式

December 3, 2021

管理模式是包括移动设备管理 (MDM) 和移动应用程序管理 (MAM) 的术语。您可以配置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 注册配置文件将 Android 和 iOS 设备注册到 MDM、MAM 或两者 (MDM+MAM)。如果您选择 MDM+MAM，则可以让用户选择退出 MDM。
- 用于将 Windows 10 和 Windows 11 设备注册到 MDM 的注册配置文件。

可以在注册配置文件中指定注册选项，您会将这些选项附加到交付组。有关注册选项的信息，请参阅 注册配置文件。以下各部分内容重点介绍了管理设备和应用程序的注意事项。

移动设备管理 (MDM)

在 MDM 模式下，可以配置和支持移动设备以及确保移动设备的安全。MDM 允许您在系统级别保护设备和设备上的数据。可以配置策略、操作和安全功能。例如，如果设备丢失、被盗或不合规，可以选择性擦除设备。

即使您不选择在设备上管理应用程序，也可以交付移动应用程序，例如公共应用商店和企业应用程序。

下面是 MDM 的常见用例：

- MDM 是需要设备级别的管理策略或某些限制的公司拥有的设备的考虑因素。这些限制包括完全擦除、选择性擦除或地理位置。
- 当客户需要管理实际设备，但不需要 MDX 策略时。
- 用户仅需要电子邮件传送给其移动设备上的本机电子邮件客户端，并且 Exchange ActiveSync 或客户端访问服务器已可从外部访问时。在此用例中，可以使用 MDM 配置电子邮件传送。
- 部署本机企业应用程序（非 MDX）、公共应用商店应用程序或从公共应用商店交付的 MDX 应用程序时。请注意，MDM 解决方案本身不能防止设备上的应用程序之间的机密数据的数据泄漏。数据泄漏可能会在 Office 365 应用程序中执行复制和剪贴操作或“另存为”操作时发生。

移动应用程序管理 (MAM)

MAM 保护应用程序并且允许您控制应用程序数据共享。MAM 还允许您独立于个人数据来管理公司数据和资源。为 MAM 配置了 Endpoint Management 的情况下，可以使用启用了 MDX 的移动应用程序提供每应用程序容器化和控制。

通过使用 MDX 策略，Endpoint Management 提供通过网络访问（例如 Micro VPN）进行的应用程序级别控制、应用程序和设备交互和应用程序访问。

MAM 通常适用于自带 (BYO) 设备，因为即使设备未托管，公司数据仍受保护。MDX 有许多不需要 MDM 控制的仅 MAM 策略。

MAM 还支持 Citrix 移动生产力应用程序。此功能包括：

- 将电子邮件安全传递到 Citrix Secure Mail
- 安全的 Citrix 移动生产力应用程序之间的数据共享
- Citrix Files 中的安全数据存储。

有关详细信息，请参阅移动生产力应用程序。

MAM 通常适用于以下示例：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 您提供在应用程序级别管理的移动应用程序，例如 MDX 应用程序。
- 您不需要在系统级别管理设备。

MDM+MAM

通过 Endpoint Management，您可以指定用户是否可以选择退出设备管理。这种灵活性对包括混合用例的环境非常有用。这些环境可能需要通过 MDM 策略管理设备才能访问您的 MAM 资源。

MDM+MAM 适用于以下示例：

- 您具有同时需要 MDM 和 MAM 的单个用例。需要 MDM 才能访问您的 MAM 资源。
- 有些用例需要 MDM，而有些用例不需要。
- 有些用例需要 MAM，而有些用例不需要。

设备管理和 **MDM** 注册

Endpoint Management Enterprise 环境可以包括混合用例，其中某些用例要求通过 MDM 策略进行设备管理以访问 MAM 资源。

为用户部署 Citrix 移动生产力应用程序之前，请完全评估您的用例并决定是否要求 MDM 注册。如果以后决定更改 MDM 注册的要求，用户可能需要重新注册其设备。有关详细信息，请参阅注册配置文件。

有关注册和 Citrix Gateway 的信息，请参阅 与 Citrix Gateway 和 Citrix ADC 集成。

下面概述了要求 MDM 注册的优势和劣势（以及缓解操作）。

MDM 注册为可选时

优势

- 用户不需要将其设备置于 MDM 管理模式即可访问 MAM 资源。此选项可以增加用户采用率。
- 能够安全访问 MAM 资源以保护企业数据。
- 应用程序通行码等 MDX 策略可以控制对每个 MDX 应用程序的应用程序访问。
- 配置 Citrix Gateway、Endpoint Management 和每应用程序超时以及 Citrix PIN 将提供一层额外的保护。
- 虽然 MDM 操作不适用于设备，但某些 MDX 策略可用于拒绝 MAM 访问。拒绝将取决于系统设置，例如越狱或获得 root 权限的设备。
- 用户可以选择是否在首次使用过程中通过 MDM 注册其设备。

劣势

- MAM 资源适用于未在 MDM 中注册的设备。
- MDM 策略和操作仅适用于 MDM 注册的设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

缓解方案

- 使用户同意在其选择不遵从合规性的情况下追究其责任的公司条款和条件。使管理员监视未托管的设备。
- 使用应用程序计时器管理应用程序访问和安全性。降低的超时值提高了安全性，但会影响用户体验。

要求 **MDM** 注册时

优势

- 能够将 MAM 资源的访问仅限制到 MDM 托管的设备。
- 根据需要，MDM 策略和操作可能适用于环境中的所有设备。
- 用户无法选择退出注册其设备。

劣势

- 要求所有用户通过 MDM 注册。
- 可能会降低反对公司管理其个人设备的用户的采用率。

缓解方案

- 针对 Endpoint Management 在其设备上实际管理的对象以及信息管理员可以访问的资源向用户提供教育培训。

设备要求

December 3, 2021

考虑采用任何部署的重点是您计划推出的设备集合。在 iOS、Android 和 Windows 平台上，选项非常多。有关 Endpoint Management 支持的设备列表，请参阅 支持的设备平台。

在自带设备 (BYOD) 环境中，可以混合使用支持的平台。但是，通知用户可以注册的设备时，请考虑“支持的设备平台”一文中的限制信息。即使仅允许在您的环境中使用一个或两个设备，Endpoint Management 在 iOS、Android 和 Windows 设备上运行时也略有差别。在每个平台上提供不同的功能集。

此外，并非所有应用程序设计都同时针对平板电脑和手机的外形规则。做出广泛传播的更改之前，请测试应用程序以确保其适合您要推出的设备屏幕。

可以同时考虑注册因素。Apple 和 Google 提供企业注册计划。通过 Apple 部署计划 和 Google Android Enterprise，你可以购买预先配置好供员工使用的设备。

有关注册的详细信息，请参阅 用户注册选项。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

安全性和用户体验

July 8, 2022

对于任何组织而言，安全性都至关重要，但在提高安全性和改善用户体验方面，您必须在两者之间实现权衡。例如，您的环境可能非常安全，但用户使用起来很困难。或者，您的环境可能具有良好的用户体验，但访问控制却不那么严格。本虚拟手册中的其他部分详细介绍了安全功能。本文的目的是全面概述 Endpoint Management 中的常见安全问题和可用的安全选项。

下面是针对每种用例需要谨记的一些主要注意事项：

- 您要保护某些应用程序的安全还是整个设备的安全？或者还是同时保护这两者的安全？
- 您希望您的用户如何进行身份验证？要使用 LDAP 还是基于证书的身份验证？或者还是组合使用这两者？
- 您希望用户的会话在超时之前持续多久？请谨记，后台服务、Citrix ADC 以及能够在脱机时访问应用程序的超时值不同。
- 是否希望用户设置设备级别通行码和应用程序级别通行码？您希望允许用户尝试登录多少次？请谨记 MAM 可能会针对每个应用程序实施的其他身份验证要求，以及用户对这些要求可能存在的看法。
- 您还希望对用户实施其他哪些限制？是否要授予用户访问 Siri 等云服务的权限？他们可以在每个应用程序中使用您为其提供的哪些功能，以及不能使用哪些功能？您想要部署公司网络 (Wi-Fi) 策略以防止在办公室内使用蜂窝数据计划吗？

应用程序与设备

首先要考虑的事情之一是您是否想要保护以下对象的安全：

- 仅特定应用程序（移动应用程序管理或 MAM）
- 整个设备（移动设备管理或 MDM）。
- MDM+MAM

通常情况下，如果您不需要设备级别控制，则只需要管理移动应用程序，尤其是当贵组织支持自带设备 (BYOD) 时。

使用 Endpoint Management 未托管的设备的用户可以通过应用商店安装应用程序。您可以通过应用程序策略控制对应用程序的访问，而不是通过设备级别控制，如选择性擦除或完全擦除。根据您设置的值，这些策略要求设备定期检查 Endpoint Management，以确认仍然允许运行应用程序。

MDM 允许您保护整个设备的安全，包括对设备上的所有软件执行清单操作的能力。MDM 允许您在设备越狱、获得 root 权限或安装了不安全的软件时阻止注册。但是，采用此级别的控制会使用户极不愿意允许对其私人设备拥有太多控制权限，因此会降低注册率。

身份验证

身份验证对用户体验有很大的影响。如果贵组织已在运行 Active Directory，则使用 Active Directory 是您的用户访问系统的最简单方法。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

身份验证用户体验的另一个重要方面是超时。高安全性环境可能会让用户在每次访问系统时登录。对于所有组织或用例来说，这种选择可能并不理想。

用户熵

要提高安全性，可以启用一项名为用户熵的功能。Citrix Secure Hub 与其他一些应用程序通常共享通用数据（例如，密码、PIN 和证书）以确保一切正常运行。此信息存储在 Secure Hub 中的一个通用保管库中。如果您通过 **Encrypt Secrets**（加密机密）选项启用用户熵，Endpoint Management 将创建一个名为 UserEntropy 的保管库。Endpoint Management 将信息从通用保管库移动到这一新保管库中。为使 Secure Hub 或其他应用程序访问这些数据，用户必须输入密码或 PIN。

启用用户熵将会在多个位置添加另一层身份验证。因此，无论何时应用程序需要访问 UserEntropy 保管库中的共享数据（包括密码、PIN 和证书），用户都必须进行身份验证。

您可以通过阅读关于 MDX Toolkit 来了解有关用户熵的更多信息。要启用用户熵，您可以在客户端属性中找到相关设置。

策略

MDX 和 MDM 策略都为组织提供了很大的灵活性，但也可以限制用户。在某些情况下，您可能希望具有该限制，但策略也会导致系统无法使用。例如，您可能希望阻止对可能会向外部位置发送敏感数据的云应用程序（例如 Siri 或 iCloud）进行访问。您可以设置一个策略来阻止访问这些服务，但请谨记，此类策略会导致发生意外结果。例如，iOS 键盘麦克风依赖于云访问。

应用程序

企业移动性管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 让组织能够保护和控制移动设备，而 MAM 有助于应用程序交付和管理。随着 BYOD 的采用越来越多，您通常可以实施 MAM 解决方案（例如 Endpoint Management）以协助执行以下操作：

- 应用程序交付
- 软件授权
- configuration
- 应用程序生命周期管理

借助 Endpoint Management，您可以通过配置特定的 MAM 策略和 VPN 设置来为这些应用程序增加更多的安全性，以防止数据泄露和其他安全威胁。Endpoint Management 为组织提供了在同一环境中同时包含 MDM 和 MAM 功能的灵活性。

除了能够将应用程序交付到移动设备外，Endpoint Management 还通过 MDX 技术提供应用程序容器化。MDX 通过平台提供的独立于设备级别加密的加密来保护应用程序的安全。可以擦除或锁定应用程序。应用程序受基于策略的精细控制。独立软件供应商 (ISV) 可以使用移动应用程序 SDK 应用这些控制。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在企业环境中，用户使用各种各样的移动应用程序来协助完成自己的工作职责。这些应用程序可能包括公共应用商店中的应用程序、内部开发的应用程序或本机应用程序。Endpoint Management 按如下所示对这些应用程序进行分类：

公共应用商店：这些应用程序包括公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。组织外的供应商通常在公共应用商店中提供其应用程序。这种方式让其客户可以直接从 Internet 下载应用程序。根据用户的需求，您可以在组织中使用很多公共应用程序。例如，GoToMeeting、Salesforce 和 EpicCare 应用程序属于此类应用程序。

Citrix 不支持直接从公共应用商店下载应用程序二进制文件，然后使用 MDX Toolkit 将其打包以进行企业分发。要通过 MDX 启用第三方应用程序，请与您的应用程序供应商联系以获取应用程序二进制文件。可以使用 MDX Toolkit 封装二进制文件，也可以将 MAM SDK 与二进制文件集成。

内部应用程序：许多组织都有内部开发人员，他们创建提供特定功能并在组织内独立开发和分发的应用程序。在某些情况下，一些组织可能还有 ISV 提供的应用程序。您可以将此类应用程序作为本机应用程序进行部署，也可以通过使用 MAM 解决方案（例如 Endpoint Management）容器化这些应用程序。例如，某医疗机构会创建一个内部应用程序，以允许医师在移动设备上查看患者信息。然后，组织可以启用 MAM SDK 或通过 MDM 封装应用程序，以保护患者信息的安全并启用对后端患者数据库服务器的 VPN 访问。

Web 和 **SaaS** 应用程序：这些应用程序包括通过内部网络访问的应用程序（Web 应用程序）或通过公用网络访问的应用程序 (SaaS)。Endpoint Management 还允许您使用一组应用程序连接器创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器便于对现有 Web 应用程序进行单点登录 (SSO)。有关详细信息，请参阅应用程序连接器类型。例如，您可以使用基于安全声明标记语言 (SAML) 的 Google Apps SAML for SSO 登录 Google Apps。

移动生产力应用程序：移动生产力应用程序是 Citrix 开发且在 Endpoint Management 许可证中附带的应用程序。有关详细信息，请参阅关于移动生产力应用程序。Citrix 还提供其他 业务就绪型应用程序。ISV 通过使用移动应用程序 SDK 开发业务就绪型应用程序。

HDX 应用程序： HDX 应用程序是您通过 StoreFront 发布且由 Windows 托管的应用程序。如果您有 Citrix Virtual Apps and Desktops 环境，则可以将这些应用程序与 Endpoint Management 集成以向注册用户提供这些应用程序。

根据您计划通过 Endpoint Management 部署和管理的移动应用程序的类型，基础配置和体系结构会有所不同。假设具有不同权限级别的多组用户可能会使用某一个应用程序。在这种情况下，您可以创建独立的交付组以部署该应用程序的两个版本。请确保用户组成员身份相互排斥，以避免用户设备上出现策略不匹配的情况。

您还可能希望使用 Apple 批量购买管理 iOS 应用程序许可。此选项要求您注册 Apple 批量购买计划。此外，必须使用 Endpoint Management 控制台配置批量购买设置。该配置允许您使用批量购买许可证分发应用程序。鉴于各种此类用例，在实施 Endpoint Management 环境之前请务必评估和规划您的 MAM 策略。规划您的 MAM 策略时，您可以先明确以下各项：

应用程序类型：列出您计划支持的不同类型的应用程序。然后，对应用程序进行分类，例如公共应用程序、本机应用程序、Citrix 移动生产力应用程序、Web 应用程序、内部应用程序和 ISV 应用程序。此外，还按不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。此分类可帮助您对齐每种类型的应用程序所需的 Endpoint Management 设置。例如：某些应用可能不符合打包条件。或者，一些应用程序可能需要使用移动应用程序 SDK 来启用用于与其他应用程序进行交互的特殊 API。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

网络要求：通过适当的设置为应用程序配置特定的网络访问要求。例如，某些应用程序可能需要通过 VPN 访问您的内部网络。某些应用程序可能需要 Internet 访问权限才能通过 DMZ 对访问进行路由。为了允许此类应用程序连接到所需网络，您必须相应地配置各种设置。定义每应用程序网络的要求，以帮助您预先完成体系及结构决策。这项工作简化了总体执行进程。

安全要求：定义适用于单个应用程序或所有应用程序的安全要求。某些设置（例如 MDX 策略）适用于单个应用程序。会话和身份验证设置适用于所有应用程序。某些应用程序可能具有特定的加密、容器化、封装、身份验证、地理围栏、通行码或数据共享要求。请提前概述这些要求，以简化部署。

部署要求：您可能希望使用基于策略的部署以仅允许合规用户下载已发布的应用程序。例如，您可能希望某些应用程序要求：

- 基于设备平台的加密已启用
- 设备已托管
- 设备满足最低操作系统版本
- 某些应用程序仅适用于企业用户

请提前列出此类要求，以便您可以配置适当的部署规则或操作。

许可要求：记录应用程序相关的许可要求。此类笔记将帮助您有效地管理许可证使用情况，以及决定是否需要在 Endpoint Management 中配置特定功能以便于进行许可。例如，如果部署免费或付费 iOS 应用程序，Apple 会通过让用户登录其 Apple Store 帐户来强制对该应用程序执行许可要求。您可以注册 Apple 批量购买，以通过 Endpoint Management 分发和管理这些应用程序。批量购买允许用户无需登录其 Apple Store 帐户即可下载应用程序。此外，诸如 Samsung Knox 之类的工具有特殊的许可要求，您需要在部署这些功能之前完成这些要求。

允许列表和阻止列表要求：您可能希望阻止用户安装或使用某些应用程序。创建使设备不合规的应用程序允许列表。然后，设置在设备不合规时触发的策略。另一方面，某个应用程序可能可以使用，但可能会出于某个原因而被列入阻止列表。在这种情况，可以将该应用程序添加到允许列表中，并指出该应用程序是可以使用的但不是必需的。此外，请谨记，预先安装在新设备上的应用程序可能包括一些不属于操作系统的常用应用程序。这些应用程序可能会与您的阻止列表策略相冲突。

应用程序用例

某医疗机构计划部署 Endpoint Management 以用作其移动应用程序的 MAM 解决方案。移动应用程序将交付给公司和自带设备用户。IT 决定交付和管理以下应用程序：

- 移动生产力应用程序：由 Citrix 提供的 iOS 和 Android 应用程序。
- **Citrix Files**：用于访问共享数据以及共享、同步和编辑文件的应用程序。

公共应用商店

- **Secure Hub**：所有移动设备用来与 Endpoint Management 通信的客户端。IT 通过 Secure Hub 客户端向移动设备推送安全设置、配置和移动应用程序。Android 和 iOS 设备通过 Secure Hub 在 Endpoint Management 中注册。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Citrix Workspace** 应用程序：允许用户打开 Citrix Virtual Apps 托管的移动设备应用程序的移动应用程序。
- **GoToMeeting**：在线会议、桌面共享和视频会议客户端，让用户可以通过 Internet 实时与其他计算机用户、客户、客户端或同事联系。
- **Salesforce1**： Salesforce1 允许用户从移动设备访问 Salesforce，并将所有 Chatter、CRM、自定义应用程序和业务流程集中在一起，以使 Salesforce 任何用户拥有统一的体验。
- **RSA SecurID**：用于双重身份验证的基于软件的令牌。
- **EpicCare** 应用程序：这些应用程序让医疗工作人员可以安全便携地访问患者图表、患者列表、计划和消息。
  - **Haiku**：适用于 iPhone 和 Android 手机的移动应用程序。
  - **Canto**：适用于 iPad 的移动应用程序
  - **Rover**：适用于 iPhone 和 iPad 的移动应用程序。

HDX： Citrix Virtual Apps 将 HDX 应用程序交付到 Citrix Workspace。

- **Epic Hyperspace**：用于电子病历管理的 Epic 客户端应用程序。

ISV

- **Vocera**： HIPAA 合规 VoIP 和消息传送移动应用程序，通过 iPhone 和 Android 智能手机随时随地扩展 Vocera 语音技术的优势。

内部应用程序

- **HCMail**：该应用程序用于撰写加密邮件、在内部邮件服务器上搜索通讯簿以及使用电子邮件客户端将加密邮件发送给联系人。

内部 **Web** 应用程序

- **PatientRounding**：该 Web 应用程序用于按不同的部门记录患者健康信息。
- **Outlook Web Access**：允许通过 Web 浏览器访问电子邮件。
- **SharePoint**：用于组织范围的文件和数据共享。

下表列出了 MAM 配置所需的基本信息。

应用程序名称	应用程序类型	MDX 打包	iOS	Android
Secure Mail	移动生产力应用程序	版本 10.4.1 及更高版本不使用	是	是
Secure Web	移动生产力应用程序	版本 10.4.1 及更高版本不使用	是	是
Citrix Files	移动生产力应用程序	版本 10.4.1 及更高版本不使用	是	是
Secure Hub	公共应用程序	不适用	是	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序名称	应用程序类型	MDX 打包	iOS	Android
Citrix Workspace 应用程序	公共应用程序	不适用	是	是
GoToMeeting	公共应用程序	不适用	是	是
SalesForce1	公共应用程序	不适用	是	是
RSA SecurID	公共应用程序	不适用	是	是
Epic Haiku	公共应用程序	不适用	是	是
Epic Canto	公共应用程序	不适用	是	否
Epic Rover	公共应用程序	不适用	是	否
Epic Hyperspace	HDX 应用程序	不适用	是	是
Vocera	ISV 应用程序	是	是	是
HCMail	内部应用程序	是	是	是
PatientRounding	Web 应用程序	不适用	是	是
Outlook Web Access	Web 应用程序	不适用	是	是
SharePoint	Web 应用程序	不适用	是	是

以下各表列出了您在 Endpoint Management 中配置 MAM 策略时可以查询的特定要求。

应用程序名称	需要 VPN	（与容器外部的应用程序）交互	交互（来自容器之外的应用程序）	基于设备平台的加密
Secure Mail	Y	选择性允许	允许	不需要
Secure Web-	Y	允许	允许	不需要
Citrix Files	Y	允许	允许	不需要
Secure Hub	Y	不适用	不适用	不适用
Citrix Workspace 应用程序	Y	不适用	不适用	不适用
GoToMeeting	N	不适用	不适用	不适用
SalesForce1	N	不适用	不适用	不适用
RSA SecurID	N	不适用	不适用	不适用
Epic Haiku	Y	不适用	不适用	不适用
Epic Canto	Y	不适用	不适用	不适用

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序名称	需要 VPN	（与容器外部的应用程序）交互	交互（来自容器之外的应用程序）	基于设备平台的加密
Epic Rover	Y	不适用	不适用	不适用
Epic Hyperspace	Y	不适用	不适用	不适用
Vocera	Y	已阻止	已阻止	不需要
HCMail	Y	已阻止	已阻止	必需
PatientRounding	Y	不适用	不适用	必需
Outlook Web Access	Y	不适用	不适用	不需要
SharePoint	Y	不适用	不适用	不需要

应用程序名称	代理过滤	许可	地理围栏	移动应用程序 SDK	最低操作系统版本
Secure Mail	必需	不适用	选择性必需	不适用	强制执行
Secure Web-	必需	不适用	不需要	不适用	强制执行
Secure Notes	必需	不适用	不需要	不适用	强制执行
Citrix Files	必需	不适用	不需要	不适用	强制执行
Secure Hub	不需要	批量购买	不需要	不适用	不强制执行
Citrix Workspace 应用程序	不需要	批量购买	不需要	不适用	不强制执行
GoToMeeting	不需要	批量购买	不需要	不适用	不强制执行
SalesForce1	不需要	批量购买	不需要	不适用	不强制执行
RSA SecurID	不需要	批量购买	不需要	不适用	不强制执行
Epic Haiku	不需要	批量购买	不需要	不适用	不强制执行
Epic Canto	不需要	批量购买	不需要	不适用	不强制执行
Epic Rover	不需要	批量购买	不需要	不适用	不强制执行
Epic Hyperspace	不需要	不适用	不需要	不适用	不强制执行
Vocera	必需	不适用	必需	必需	强制执行
HCMail	必需	不适用	必需	必需	强制执行

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序名称	代理过滤	许可	地理围栏	移动应用程序 SDK	最低操作系统版本
PatientRound-ing	必需	不适用	不需要	不适用	不强制执行
Outlook Web Access	必需	不适用	不需要	不适用	不强制执行
SharePoint	必需	不适用	不需要	不适用	不强制执行

用户社区

每个组织都由多个以不同的功能角色运作的用户社区组成。这些用户社区使用您通过用户设备提供的各种资源执行不同的任务和办公功能。用户可能会使用您提供的移动设备在家中或远程办公室工作。或者，用户可能会拥有私人移动设备，这允许其访问遵从某些安全合规规则的工具。

随着越来越多的用户社区开始使用移动设备来完成自己的工作职责，企业移动性管理 (EMM) 将对防止数据泄漏至关重要。EMM 对于实施组织的安全限制也是至关重要的。为了实现高效率以及更加复杂的移动设备管理，您可以对用户社区进行分类。这样可以简化将用户映射到资源的过程，并将适当的安全策略与用户保持一致。

以下示例说明了如何对医疗机构的用户社区进行分类以实现 EMM。

用户社区用例

本示例医疗机构提供技术资源以及向多个用户提供访问权限，包括网络和附属机构员工和志愿者。此机构已选择仅向非执行用户推出 EMM 解决方案。

此机构的用户角色和功能可以划分为几个子组，包括：临床、非临床和合同工。选定的用户将收到企业移动设备，而其他用户可以从其私人设备访问有限的公司资源。要强制执行正确的安全限制级别以及防止数据泄漏，此机构决定企业 IT 负责管理注册的每个设备。这些设备可能是公司拥有的设备，也可能是自带设备 (BYOD)。此外，用户只能注册一个设备。

下面的部分概述了每个子组的角色和功能：

临床

- 护士
- 医师（医生、外科医生等）
- 专家（营养学家、麻醉师、放射科医师、心脏病专家、肿瘤学家等）
- 外部医师（从远程办公室工作的非雇员医师和办公室工作人员）
- 家庭医疗服务（执行患者家访的医师服务的办公室和移动工作人员）
- 研究专家（在六家研究机构执行临床研究以寻找医学问题答案的知识型工作者和高级用户）
- 教育和培训（护士、医师以及教育和培训专家）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

非临床

- 共享服务（执行各种后勤功能的办公室工作人员，包括：HR、工资单、应付账款和供应链服务）
- 医师服务（执行各种医疗保健管理、管理服务以及针对提供商的业务流程解决方案的办公室工作人员，包括：管理服务、分析和业务智能、业务系统、客户服务、财务、托管式医疗管理、患者访问解决方案、收支周期解决方案等）
- 支持服务（执行各种非临床功能的办公室工作人员，包括：收益管理、临床整合、沟通、薪酬与绩效管理、设施和物业服务、HR 技术系统、信息服务、内部审计和流程改进等。）
- 慈善活动（执行支持慈善活动的各项功能的办公室和移动工作人员）

合同工

- 制造商和供应商合作伙伴（通过站点到站点 VPN 现场连接和远程连接，提供各种非临床支持功能）

根据上述信息，此机构创建了以下实体。有关 Endpoint Management 中交付组的更多信息，请参阅 部署资源。

Active Directory 组织单位 **(OU)** 和组

对于 OU **=** Endpoint Management 资源：

- OU = 临床；组 =
  - XM-护士
  - XM-医师
  - XM-专家
  - XM-外部医师
  - XM-家庭医疗服务
  - XM-研究专家
  - XM-教育和培训
- OU = 非临床；组 =
  - XM-共享服务
  - XM-医师服务
  - XM-支持服务
  - XM-慈善活动

Endpoint Management 本地用户和组

针对组 = 合同工，用户 =

- Vendor1
- Vendor2
- 供应商 3
- … 供应商 10

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 交付组

- 临床-护士
- 临床-医师
- 临床-专家
- 临床-外部医师
- 临床-家庭医疗服务
- 临床-研究专家
- 临床-教育和培训
- 非临床-共享服务
- 非临床-医师服务
- 非临床-支持服务
- 非临床-慈善活动

交付组和用户组映射

Active Directory 组	Endpoint Management 交付组
XM-护士	临床-护士
XM-医师	临床-医师
XM-专家	临床-专家
XM-外部医师	临床-外部医师
XM-家庭医疗服务	临床-家庭医疗服务
XM-研究专家	临床-研究专家
XM-教育和培训	临床-教育和培训
XM-共享服务	非临床-共享服务
XM-医师服务	非临床-医师服务
XM-支持服务	非临床-支持服务
XM-慈善活动	非临床-慈善活动

交付组和资源映射

以下各表列出了分配给此用例中每个交付组的资源。第一个表显示了移动应用程序分配。第二个表显示了公共应用程序、HDX 应用程序和设备管理资源。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 交付组	Citrix 移动应用程序	公共移动应用程序	HDX 移动应用程序
临床-护士	X		
临床-医师			
临床-专家			
临床-外部医师	X		
临床-家庭医疗服务	X		
临床-研究专家	X		
临床-教育和培训		X	X
非临床-共享服务		X	X
非临床-医师服务		X	X
非临床-支持服务	X	X	X
非临床-慈善活动	X	X	X
合同工	X	X	X

Endpoint Management 交付组	公共应用程序：RSA SecurID	公共应用程序：EpicCare Haiku	HDX 应用程序：Epic Hyperspace	通行码策略	设备限制	自动操作	网络策略
临床-护士							X
临床-医师					X		
临床-专家							
临床-外部医师							
临床-家庭医疗服务							
临床-研究专家							
临床-教育和培训		X	X				
非临床-共享服务		X	X				

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 交付组	公共应用程序：RSA SecurID	公共应用程序：EpicCare Haiku	HDX 应用程序：Epic Hyperspace	通行码策略	设备限制	自动操作	网络策略
非临床-医师服务		X	X				
非临床-支持服务		X	X				

备注和注意事项

- Endpoint Management 在初始配置过程中创建名为“所有用户”的默认交付组。如果不禁用此交付组，所有 Active Directory 用户都将具有在 Endpoint Management 中注册的权限。
- Endpoint Management 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果某个用户所属的组未在 Endpoint Management 中映射，该用户将无法注册。同样，如果用户是多个组的成员，Endpoint Management 仅会将该用户分类为映射到 Endpoint Management 的组的一部分。

安全要求

与 Endpoint Management 环境相关的安全注意事项的范围可能会很快变得难以承受。有许多连锁件和设置。您可能不知道从何处着手或如何选择才能确保提供可接受的保护级别。为了简化这些选择，Citrix 提供了有关高安全性、较高安全性和最高安全性的建议，如下表中所述。

安全问题并不是您的设备注册模式的唯一考虑因素：MAM、MDM+MAM（MDM 可选）或 MDM+MAM（MDM 必选）。此外，务必要查看用例的要求，并确定是否可以在选择管理模式之前缓解安全问题。

高：使用这些设置可提供最佳的用户体验，同时保持大多数组织可接受的基本安全级别。

较高：这些设置在安全性和可用性之间建立更加稳健的权衡。

最高：遵循这些建议，安全级别非常高，但可用性和用户采用率会降低。

管理模式安全注意事项

下表列出了实现每种安全级别的管理模式。

高安全性	更高的安全性	最高安全性
MAM、MDM+MAM	MDM+MAM	MDM+MAM

备注：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 根据用例，仅 MAM 部署可以满足安全要求，并提供良好的用户体验。
- 对通过应用程序容器化即可满足所有业务和安全要求的用例（例如 BYOD），Citrix 建议采用仅 MAM 模式。
- 对于高安全性环境（和公司发放的设备），Citrix 建议采用 MDM+MAM 以充分利用可用的所有安全功能。

Citrix ADC 和 **Citrix Gateway** 安全注意事项

下表列出了针对每种安全级别的 Citrix ADC 和 Citrix Gateway 建议。

高安全性	更高的安全性	最高安全性
推荐使用 Citrix ADC。MAM 和 MDM+MAM 需要使用 Citrix Gateway	如果 Endpoint Management 位于 DMZ 中，则使用 SSL 桥接的 NetScaler for XenMobile 向导配置。	SSL 卸载与端到端加密

备注：

- 通过 NAT 或现有的第三方代理/负载平衡器将 Endpoint Management 服务器公开给 Internet 可能是 MDM 的一个选项。但是，在这种情况下，SSL 流量将在 Endpoint Management 服务器上终止，这会带来潜在的安全风险。
- 对于高安全性环境，采用默认 Endpoint Management 配置的 Citrix Gateway 通常可以满足或超过安全要求。
- 对于具有最高安全性需求的 MDM 注册，SSL 终止于 Citrix Gateway 允许您检查外围流量的功能，同时维持端到端 SSL 加密。
- 用于定义 SSL/TLS 密码的选项。
- 有关详细信息，请参阅与 Citrix Gateway 和 Citrix ADC 集成。

注册安全注意事项

下表列出了针对每种安全级别的 Citrix ADC 和 Citrix Gateway 建议。

高安全性	更高的安全性	最高安全性
仅限 Active Directory 组成员身份。禁用“所有用户”交付组。	仅限邀请的注册安全模式。仅限 Active Directory 组成员身份。禁用“所有用户”交付组	注册安全模式关联到设备 ID。仅限 Active Directory 组成员身份。禁用“所有用户”交付组

> 备注：
>
> - Citrix 通常建议只允许预定义的 Active Directory 组中的用户进行注册。此限制需要禁用内置的“所有用

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> 户”交付组。
> - 您可以使用注册邀请来限制收到邀请的用户才可以注册。注册邀请不适用于 Windows 设备。
> - 您可以使用一次性 PIN (OTP) 注册邀请作为双重身份验证解决方案以及控制用户可以注册的设备数。(OTP 邀请不适用于 Windows 设备。)

设备通行码安全注意事项

下表列出了针对每种安全级别的设备通行码建议。

高安全性	更高的安全性	最高安全性
推荐。设备级别加密要求高安全性。可以通过 MDM 强制要求。可以通过使用 MDX 策略（不合规的设备行为）来设置仅限 MAM 的要求。	使用 MDM、MAM 或 MDM+MAM 策略强制执行。	通过使用 MDM 和 MDX 策略强制要求。MDM 复杂通行码策略。

> 备注：
> - Citrix 建议使用设备通行码。
> - 可以通过 MDM 策略强制要求输入设备通行码。
> - 您可以使用 MDX 策略将设备通行码作为使用托管应用程序的要求；例如，对于 BYOD 使用案例。
> - Citrix 建议组合使用 MDM 和 MDX 策略选项来提高 MDM+MAM 注册的安全性。
> - 对于具有最高安全性要求的环境，可以配置复杂通行码策略，并通过 MDM 强制实施这些策略。您可以配置自动操作，以便在设备不符合通行码策略时通知管理员或执行选择性设备擦除/完全设备擦除。

应用程序

November 7, 2022

企业移动性管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 让组织能够保护和控制移动设备，而 MAM 有助于应用程序交付和管理。在越来越多地采用 BYOD 的情况下，您通常可以实施 MAM 解决方案，例如 Endpoint Management。Endpoint Management 可协助进行应用程序交付、软件许可、配置和应用程序生命周期管理。可以要求或允许用户同时选择进行 MDM 管理。

通过 Endpoint Management，您可以通过配置 MAM 策略和 VPN 设置以防止数据泄漏和其他安全威胁来保护这些应用程序的安全。Endpoint Management 为组织提供了将设备注册为“仅 MAM”或“MDM+MAM”的灵活性。

除了能够将应用程序交付到移动设备外，Endpoint Management 还通过 MDX 技术提供应用程序容器化。这些应用程序受基于策略的精细控制。独立软件供应商 (ISV) 可以使用移动应用程序 SDK 应用这些控制。

在企业环境中，用户使用各种各样的移动应用程序来协助完成自己的工作职责。这些应用程序可能包括公共应用商店中的应用程序、内部开发的应用程序或本机应用程序。Endpoint Management 按如下所示对这些应用程序进行分类：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 公共应用商店：这些应用程序包括公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。组织外的供应商通常在公共应用商店中提供其应用程序。这种方式让其客户可以直接从 Internet 下载应用程序。根据用户的需求，您可以在组织中使用很多公共应用程序。例如，GoToMeeting、Salesforce 和 EpicCare 应用程序属于此类应用程序。
  - 如果使用 **MAM SDK**：请从应用程序供应商处获取应用程序二进制文件。然后，将 MAM SDK 集成到应用程序中。
  - 如果您使用 **MDX Toolkit**：Citrix 不支持直接从公共应用商店下载应用程序二进制文件，然后使用 MDX Toolkit 将其打包以进行企业分发。要打包第三方应用程序，请与您的应用程序供应商合作以获取应用程序二进制文件。然后，您可以使用 MDX Toolkit 打包二进制文件。
- 内部应用程序：许多组织都有内部开发人员，他们创建提供特定功能并在组织内独立开发和分发的应用程序。在某些情况下，一些组织可能还有 ISV 提供的应用程序。您可以将此类应用程序作为本机应用程序进行部署，也可以通过使用 MAM 解决方案（例如 Endpoint Management）容器化这些应用程序。

  例如，某医疗机构可能会创建一个内部应用程序，以允许医师在移动设备上查看患者信息。然后，组织可以使用以下方法之一来保护患者信息的安全并启用对患者数据库的 VPN 访问：
  - MAM SDK
  - MDX Toolkit
- **Web** 和 **SaaS** 应用程序：这些应用程序包括通过内部网络访问的应用程序（Web 应用程序）或通过公用网络访问的应用程序 (SaaS)。Endpoint Management 还允许您使用一组应用程序连接器创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器便于对现有 Web 应用程序进行单点登录 (SSO)。有关详细信息，请参阅应用程序连接器类型。例如，您可以使用基于安全声明标记语言 (SAML) 的 Google Apps SAML for SSO 登录 Google Apps。
- 移动生产力应用程序：移动生产力应用程序是 Citrix 开发且在 Endpoint Management 许可证中附带的应用程序。有关详细信息，请参阅关于移动生产力应用程序。Citrix 还提供 ISV 使用移动应用程序 SDK 开发的其他业务就绪型应用程序。
- **HDX** 应用程序： HDX 应用程序是您通过 StoreFront 发布且由 Windows 托管的应用程序。如果使用 Citrix Virtual Apps and Desktops 以及 Citrix Workspace，HDX 应用程序可供已注册的用户使用。

根据您计划通过 Endpoint Management 部署和管理的移动应用程序的类型，基础配置可能会有所不同。例如，具有不同权限级别的多组用户可能会使用某一个应用程序。在这种情况下，您可能必须创建独立的交付组以部署同一应用程序的两个独立版本。此外，您还必须确保用户组成员身份相互排斥，以避免在用户设备上发生策略不匹配。

还可以使用 Apple 批量购买管理 iOS 应用程序许可。此选项要求您注册批量购买计划并在 Endpoint Management 控制台中配置批量购买设置。该配置允许您使用批量购买许可证分发应用程序。鉴于各种用例，在实施 Endpoint Management 环境之前请务必评估和规划您的 MAM 策略。规划您的 MAM 策略时，您可以先明确以下各项：

- 应用程序类型 - 列出您计划支持的不同应用程序类型，并对其进行分类，例如，公共、本机、Web、内部或 ISV 应用程序。此外，还按不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。此分类将有助于调整每种类型的应用程序所需的各种 Endpoint Management 设置。例如，一些应用程序可能需要使用移动应用程序 SDK 来启用特殊 API 才能与其他应用程序交互。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 网络要求：配置具有特定网络访问要求的应用程序的设置。例如，某些应用程序可能需要通过 VPN 访问您的内部网络。某些应用程序可能需要 Internet 访问权限才能通过 DMZ 对访问进行路由。为了允许此类应用程序连接到所需网络，必须相应地配置各种设置。明确每个应用程序网络要求有助于在早期做出您的体系结构决策，这将简化整体实施流程。
- 安全要求：可以定义应用到单个应用程序或所有应用程序的安全要求。
  - MDX 策略等设置适用于单个应用程序
  - 会话和身份验证设置适用于所有应用程序
  - 某些应用程序可能具有特定的容器化、MDX、身份验证、地理围栏、通行码或数据共享要求。

  请提前概述这些要求，以简化部署。有关 Endpoint Management 中的安全性的详细信息，请参阅安全性和用户体验。
- 部署要求：您可能希望使用基于策略的部署以仅允许合规用户下载已发布的应用程序。例如，某些应用程序会要求设备处于托管状态，或者设备满足最低操作系统版本要求。您可能还希望某些应用程序仅提供给企业用户。请提前列出此类要求，以便您可以配置适当的部署规则或操作。
- 许可要求：保留应用程序相关的许可要求的记录。您的笔记可以帮助您有效地管理许可证使用情况，以及决定是否在 Endpoint Management 中配置特定功能以便于进行许可。例如，如果部署免费或付费 iOS 应用程序，Apple 会强制执行应用程序的许可要求。因此，用户必须登录其 Apple App Store 帐户。

  但是，您可以注册加入 Apple 批量购买计划，以通过 Endpoint Management 分发和管理这些应用程序。批量购买允许用户无需登录其 Apple App Store 帐户即可下载应用程序。

  有些平台需要在部署这些功能之前完成特殊的许可要求。
- 允许列表和阻止列表要求：您可以确定不希望用户安装或使用的应用程序。创建阻止列表将定义不合规事件。然后，您可以设置策略，以便在事件发生时触发。另一方面，某个应用程序可能可以使用，但会出于某个原因而被列入阻止列表。在这种情况，可以将该应用程序添加到允许列表中，并指出该应用程序是可以使用的但不是必需的。此外，请谨记，预先安装在新设备上的应用程序可能包括一些不属于操作系统的常用应用程序。此类应用程序可能会与您的阻止列表策略发生冲突。

用例

某医疗机构计划部署 Endpoint Management 以用作其移动应用程序的 MAM 解决方案。移动应用程序将交付给公司和自带设备用户。IT 决定交付和管理以下应用程序：

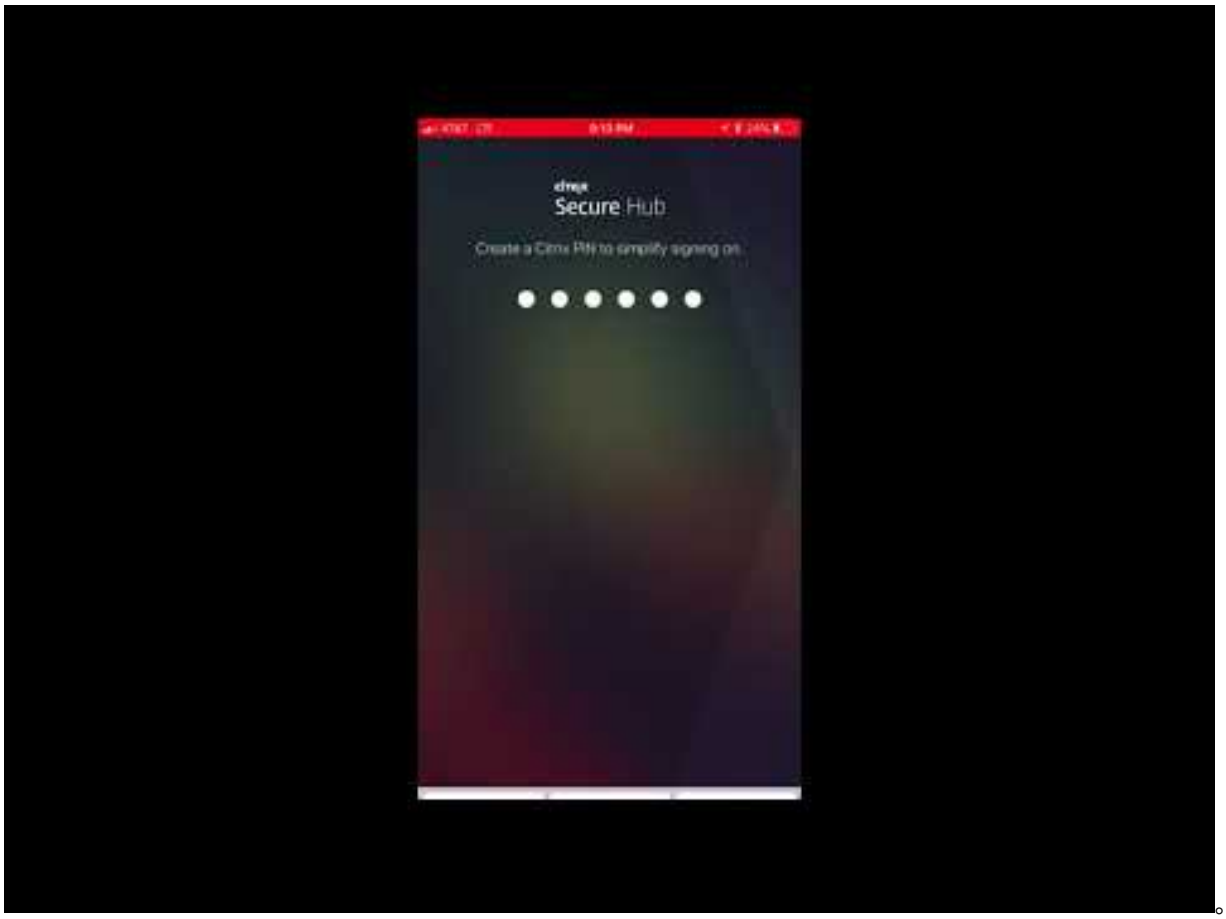
移动生产力应用程序：由 Citrix 提供的 iOS 和 Android 应用程序。有关详细信息，请参阅移动生产力应用程序。

Citrix Secure Hub：对于在 Endpoint Management 10.18.14 之前登录的客户：可以通过 Secure Hub 将安全设置、配置和移动应用程序推送到移动设备。Android 和 iOS 设备通过 Secure Hub 在 Endpoint Management 中注册。

对于截至 Endpoint Management 10.18.14 的新客户：Secure Hub 支持使用 Workspace 应用商店。打开 Secure Hub 时，用户不再看到 Secure Hub 应用商店。现在，用户单击 “添加应用程序” 按钮后将转到 Workspace 应用商店。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

下面的视频演示了 iOS 设备如何使用 Citrix Workspace 应用程序注册 Citrix Endpoint Management。



Citrix Workspace 应用程序： Citrix Workspace 应用程序集成了现有的 Citrix Receiver 技术、Secure Hub 以及其他 Citrix Workspace 客户端技术。Workspace 应用程序为最终用户提供统一的上下文体验。

GoToMeeting：在线会议、桌面共享和视频会议客户端，让用户可以通过 Internet 实时与其他计算机用户、客户、客户端或同事联系。

Salesforce1： Salesforce1 允许用户从移动设备访问 Salesforce，并将所有 Chatter、CRM、自定义应用程序和业务流程集中在一起，以使 Salesforce 任何用户拥有统一的体验。

RSA SecurID：用于双重身份验证的基于软件的令牌。

EpicCare 应用程序：这些应用程序让医疗工作人员可以安全便携地访问患者图表、患者列表、计划和消息。

Haiku：适用于 iPhone 和 Android 手机的移动应用程序。

Canto：适用于 iPad 的移动应用程序

Rover：适用于 iPhone 和 iPad 的移动应用程序。

HDX：这些应用程序通过 Citrix Workspace 在 Citrix Virtual Apps 中交付。

- **Epic Hyperspace**：用于电子病历管理的 Epic 客户端应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

ISV:

- **Vocera**： HIPAA 合规 VoIP 和消息传送移动应用程序，通过 iPhone 和 Android 智能手机随时随地扩展 Vocera 语音技术的优势。

内部应用程序：

- **HCMail**：该应用程序用于撰写加密邮件、在内部邮件服务器上搜索通讯簿以及使用电子邮件客户端将加密邮件发送给联系人。

内部 **Web** 应用程序：

- **PatientRounding**：该 Web 应用程序用于按不同的部门记录患者健康信息。
- **Outlook Web Access**：允许通过 Web 浏览器访问电子邮件。
- **SharePoint**：用于组织范围的文件和数据共享。

下表列出了 MAM 配置所需的基本信息。

应用程序名称	应用程序类型	启用了 **MDX**	**iOS**	**Android**
Secure Mail	移动生产力应用程序	否	是	是
Secure Web	移动生产力应用程序	否	是	是
Citrix Files	移动生产力应用程序	否	是	是
Secure Hub	公共应用程序	不适用	是	是
Citrix Workspace 应用程序	公共应用程序	不适用	是	是
GoToMeeting	公共应用程序	不适用	是	是
SalesForce1	公共应用程序	不适用	是	是
RSA SecurID	公共应用程序	不适用	是	是
Epic Haiku	公共应用程序	不适用	是	是
Epic Canto	公共应用程序	不适用	是	否
Epic Rover	公共应用程序	不适用	是	否
Epic Hyperspace	HDX 应用程序	不适用	是	是
Vocera	ISV 应用程序	是	是	是
HCMail	内部应用程序	是	是	是
PatientRounding	Web 应用程序	不适用	是	是

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序名称	应用程序类型	启用了 **MDX**	**iOS**	**Android**
Outlook Web Access	Web 应用程序	不适用	是	是
SharePoint	Web 应用程序	不适用	是	是

下表列出了您在 Endpoint Management 中配置 MAM 策略时可以查询的特定要求。

应用程序名称	需要 **VPN**	（与容器外部的应用程序）交互	（从容器外部的应用程序）交互	代理过滤	许可	地理围栏	移动应用程序 **SDK**	最低操作系统版本
Secure Mail	Y	选择性允许	允许	必需	不适用	选择性必需	不适用	强制执行
Secure Web	Y	允许	允许	必需	不适用	不需要	不适用	强制执行
Citrix Files	Y	允许	允许	必需	不适用	不需要	不适用	强制执行
Secure Hub	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Citrix Workspac 应用程序	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
GoToMeetiNg	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
SalesForc	N	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
RSA SecurID	N	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Epic Haiku	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Epic Canto	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Epic Rover	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序名称	需要 **VPN**	（与容器外部的应用程序）交互	（从容器外部的应用程序）交互	代理过滤	许可	地理围栏	移动应用程序 **SDK**	最低操作系统版本
Epic Hyper-space	Y	不适用	不适用	不需要	不适用	不需要	不适用	不强制执行
Vocera	Y	已阻止	已阻止	必需	不适用	必需	必需	强制执行
HCMail	Y	已阻止	已阻止	必需	不适用	必需	必需	强制执行
PatientRc ing	Y	不适用	不适用	必需	不适用	不需要	不适用	不强制执行
Outlook Web Access	Y	不适用	不适用	必需	不适用	不需要	不适用	不强制执行
SharePoi	Y	不适用	不适用	必需	不适用	不需要	不适用	不强制执行

用户社区

December 3, 2021

每个组织都由多个以不同的功能角色运作的用户社区组成。这些用户社区使用您通过用户移动设备提供的各种资源执行不同的任务和办公功能。用户可能会使用您提供的移动设备在家中或远程办公室工作。或者，用户可能会使用私人移动设备，这允许其访问遵从某些安全合规规则的工具。

如果存在多个使用移动设备的用户社区，企业移动性管理 (EMM) 将对防止数据泄漏以及强制遵守组织层面的安全限制至关重要。为了实现高效率以及更加复杂的移动设备管理，您可以对用户社区进行分类。这样可以简化将用户映射到资源的过程，并确保正确的安全策略应用到正确的用户。

将用户社区分类可以包括使用以下组件：

- Active Directory 组织单位 (OU) 和组

  添加到特定 Active Directory 安全组的用户可以接收策略以及应用程序等资源。将用户从 Active Directory 安全组中删除将删除对以前允许访问的 Endpoint Management 资源的访问权限。

- Endpoint Management 本地用户和组

  对于在 Active Directory 中没有帐户的用户，可以将用户创建为本地 Endpoint Management 用户。可以通过与 Active Directory 用户相同的方式将本地用户添加到交付组中并为其预配资源。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Endpoint Management 交付组

  如果多组具有不同权限级别的用户要占用一个应用程序，您可能希望创建独立的交付组。使用单独的交付组，您可以部署同一应用程序的两个不同版本。Citrix 建议在创建设备策略之前创建交付组。

- 交付组和用户组映射

  交付组到 Active Directory 组的映射可以是一对一映射，也可以是一对多映射。将基础策略和应用程序分配给一个一对多交付组映射。将功能特定的策略和应用程序分配给多个一对一交付组映射。

- 应用程序的交付组和资源映射

  将特定的应用程序分配给每个交付组。

- MDM 资源的交付组和资源映射

  将应用程序和特定的设备管理资源分配给每个交付组。例如，为一个交付组配置以下各项的任意组合：应用程序类型（公共应用程序、HDX 应用程序等）、每种应用程序类型的特定应用程序以及设备策略和自动化操作等资源。

以下示例说明了如何对医疗机构的用户社区进行分类以实现 EMM。

用例

本示例医疗机构提供技术资源以及向多个用户提供访问权限，包括网络和附属机构员工和志愿者。此机构已选择仅向非执行用户推出 EMM 解决方案。

您可以将此机构的用户角色和功能划分为几个子组，包括：临床、非临床和合同工。选定的一组用户将收到企业移动设备，而其他用户可以从其私人设备 (BYOD) 访问有限的公司资源。要强制执行恰当的安全限制级别以及防止数据泄漏，此机构决定企业 IT 负责管理注册的每个设备。此外，用户只能注册一个设备。

以下各节概述了每个子组的角色和功能：

临床

- 护士
- 医师（医生、外科医生等）
- 专家（营养学家、麻醉师、放射科医师、心脏病专家、肿瘤学家等）
- 外部医师（从远程办公室工作的非雇员医师和办公室工作人员）
- 家庭医疗服务（执行患者家访的医师服务的办公室和移动工作人员）
- 研究专家（在六家研究机构执行临床研究以寻找医学问题答案的知识型工作者和高级用户）
- 教育和培训（护士、医师以及教育和培训专家）

非临床

- 共享服务（执行各种后勤功能的办公室工作人员，包括：HR、工资单、应付账款、供应链服务等）

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 医师服务（执行各种医疗保健管理、管理服务以及针对提供商的业务流程解决方案的办公室工作人员，包括：管理服务、分析和业务智能、业务系统、客户服务、财务、托管式医疗管理、患者访问解决方案、收支周期解决方案等）
- 支持服务（执行各种非临床功能的办公室工作人员，包括：收益管理、临床整合、沟通、薪酬与绩效管理、设施和物业服务、HR 技术系统、信息服务、内部审计和流程改进等）
- 慈善活动（执行支持慈善活动的各项功能的办公室和移动工作人员）

合同工

- 制造商和供应商合作伙伴（通过站点到站点 VPN 现场连接和远程连接，提供各种非临床支持功能）

根据上述信息，此机构创建了以下实体。有关 Endpoint Management 中交付组的更多信息，请参阅 Endpoint Management 产品文档中的 部署资源 。

Active Directory 组织单位 **(OU)** 和组

对于 **OU =** Endpoint Management 资源

- OU = 临床；组 =
  - XM-护士
  - XM-医师
  - XM-专家
  - XM-外部医师
  - XM-家庭医疗服务
  - XM-研究专家
  - XM-教育和培训
- OU = 非临床；组 =
  - XM-共享服务
  - XM-医师服务
  - XM-支持服务
  - XM-慈善活动

Endpoint Management 本地用户和组

针对组 = 合同工，用户 =

- 供应商 1
- 供应商 2
- 供应商 3
- … 供应商 10

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 交付组

- 临床-护士
- 临床-医师
- 临床-专家
- 临床-外部医师
- 临床-家庭医疗服务
- 临床-研究专家
- 临床-教育和培训
- 非临床-共享服务
- 非临床-医师服务
- 非临床-支持服务
- 非临床-慈善活动

交付组和用户组映射

Active Directory 组	Endpoint Management 交付组
XM-护士	临床-护士
XM-医师	临床-医师
XM-专家	临床-专家
XM-外部医师	临床-外部医师
XM-家庭医疗服务	临床-家庭医疗服务
XM-研究专家	临床-研究专家
XM-教育和培训	临床-教育和培训
XM-共享服务	非临床-共享服务
XM-医师服务	非临床-医师服务
XM-支持服务	非临床-支持服务
XM-慈善活动	非临床-慈善活动

应用程序的交付组和资源映射

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

	Secure Mail	Secure Web	Citrix Files	Workspace 应用程序	Salesforce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
临床-护士	X	X	X					
临床-医师								
临床-专家								
临床-外部医师	X		X					
临床-家庭医疗服务	X		X					
临床-研究专家	X		X					
临床-教育和培训							X	X
非临床-共享服务							X	X
非临床-医师服务							X	X
非临床-支持服务	X		X				X	X
非临床-慈善活动	X		X				X	X
合同工	X		X	X	X		X	X

MDM 资源的交付组和资源映射

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

	MDM：通行码策略	MDM：设备限制	MDM：自动化操作	MDM：网络策略
临床-护士				X
临床-医师		X		
临床-专家				
临床-外部医师				
临床-家庭医疗服务				
临床-研究专家				
临床-教育和培训				
非临床-共享服务				
非临床-医师服务				
非临床-支持服务				
非临床-慈善活动				
合同工				X

备注和注意事项

- Endpoint Management 在初始配置过程中创建名为“所有用户”的默认交付组。如果不禁用此交付组，所有 Active Directory 用户都将具有在 Endpoint Management 中注册的权限。
- Endpoint Management 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果某个用户所属的组未在 Endpoint Management 中映射，该用户将无法注册。同样，如果某个用户属于多个组的成员，Endpoint Management 将仅对在映射到 Endpoint Management 的组中的用户进行分类。

电子邮件策略

November 7, 2022

从移动设备安全访问电子邮件是任何组织的移动性管理计划的其中一个主要的驱动因素。确定正确的电子邮件策略是任何 Endpoint Management 设计的一个关键组成部分。Endpoint Management 根据安全性、用户体验和集成要求提供多种选项以适应不同的用例。本文介绍了选择正确的解决方案（从选择客户端到邮件通信流）的典型设计决策过程和注意事项。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

选择电子邮件客户端

对整体电子邮件策略设计而言，客户端选择通常排在第一位。可以从多个客户端中进行选择：Citrix Secure Mail、特定移动平台操作系统中随附的本机邮件或者通过公共应用商店提供的其他第三方客户端。可以支持使用单个（标准）客户端的用户社区，也可能需要使用客户端的组合，具体取决于您的需求。

下表概述了可用的不同客户端选项的一些设计注意事项：

主题	**Secure Mail**	本机（例如 **iOS Mail**）	第三方邮件
配置	通过 MDX 策略配置的 Exchange 帐户配置文件。	通过 MDM 策略配置的 Exchange 帐户配置文件。Android 支持仅限于：Android Enterprise。所有其他客户端都被视为第三方客户端。	通常需要用户手动配置。
安全性	Secure by Design，提供最高安全性。使用数据加密级别增加的 MDX 策略。Secure Mail 是通过 MDX 策略完全托管的应用程序。增加了通过 Citrix PIN 进行的身份验证层。	取决于供应商/应用程序功能集。提供较高的安全性。使用设备加密设置。依靠设备级别的身份验证来访问应用程序。	取决于供应商/应用程序功能集。提供高安全性。
集成	默认情况下，允许与托管 (MDX) 应用程序进行交互。通过 Citrix Secure Web 打开 Web URL。将文件保存到 Citrix Files 以及从 Citrix Files 附加文件。直接加入和拨入 GoToMeeting。	默认情况下，只能与其他未托管（非 MDX）应用程序交互。	默认情况下，只能与其他未托管（非 MDX）应用程序交互。
部署/许可	可以通过 MDM 直接从公共应用商店推送 Secure Mail。随附在 Endpoint Management Advanced 和 Enterprise 许可中。	平台操作系统中随附的客户端应用程序。无额外的许可要求。	可以通过 MDM 作为企业应用程序推送或者直接从公共应用商店推送。基于应用程序供应商的关联许可模式/成本。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

支持	客户端和 EMM 解决方案 (Citrix) 的单供应商支持。Secure Hub/应用程序调试日志记录功能中嵌入了支持联系人信息。可支持一个客户端。	供应商定义的支持 (Apple/Google)。可能需要支持多个客户端，具体取决于设备平台。	供应商定义的支持。可支持一个客户端，前提是第三方客户端在所有托管设备平台上都受支持。

邮件通信流和过滤注意事项

本节探讨与 Endpoint Management 环境中的邮件 (ActiveSync) 通信流有关的三种主要方案和设计注意事项。

方案 **1**：公开的 **Exchange**

支持外部客户端的环境通常具有面向 Internet 公开的 Exchange ActiveSync 服务。移动 ActiveSync 客户端通过这一面向外部的路径借助反向代理（例如 Citrix Gateway）或边缘服务器进行连接。此方案需要使用本机或第三方邮件客户端，使得这些客户端成为此方案的普遍选择。还可以在此方案中使用 Secure Mail 客户端，尽管这并不是常见的做法。这样，您将从使用 MDX 策略和管理应用程序提供的安全功能中获益。

方案 **2**：借助 **Citrix Gateway**（**Micro VPN** 和 **STA**）通过通道传输

由于其 Micro VPN 功能，此方案是使用 Secure Mail 客户端时的默认方案。在这种情况下，Secure Mail 客户端将通过 Citrix Gateway 与 ActiveSync 建立安全连接。实际上，可以考虑使用 Secure Mail 作为从内部网络直接连接到 ActiveSync 的客户端。Citrix 客户通常会作为所选的移动 ActiveSync 客户端对 Secure Mail 进行规范。该决策属于避免在公开的 Exchange Server 上面向 Internet 公开 ActiveSync 服务的措施的一部分，如第一种方案中所述。

只有启用了 MAM SDK 或 MDX 封装的应用程序才能使用 Micro VPN 功能。如果您使用 MDX 封装，此方案不适用于本机客户端。即使可以通过 MDX Toolkit 打包第三方客户端，这种做法也不常见。使用设备级别的 VPN 客户端以允许本机或第三方客户端通过通道进行访问已证实非常麻烦，不是可行的解决方案。

方案 **3**：云托管的 **Exchange** 服务

云托管的 Exchange 服务（例如 Microsoft Office 365）变得更受欢迎。在 Endpoint Management 环境中，此方案可能将与第一种方案同等对待，因为 ActiveSync 服务也对 Internet 公开。在这种情况下，云服务提供商要求会规定客户端选项。这些选项通常包括支持大多数 ActiveSync 客户端，例如 Secure Mail 以及其他本机或第三方客户端。

对此方案而言，Endpoint Management 可以在三个方面增加价值：

- 使用 MDX 策略的客户端以及通过 Secure Mail 进行的应用程序管理
- 在受支持的本机电子邮件客户端上使用 MDM 策略配置客户端

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 使用适用于 Exchange ActiveSync 的 Endpoint Management 连接器时的 ActiveSync 过滤选项

邮件流过滤注意事项

与面向 Internet 公开的大多数服务一样，必须确保路径安全并提供过滤功能以进行授权访问。Endpoint Management 解决方案包括两个设计为专用于为本机和第三方客户端提供 ActiveSync 过滤功能的组件：适用于 Exchange ActiveSync 的 Citrix Gateway 连机器和适用于 Exchange ActiveSync 的 Endpoint Management 连接器。

适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器使用 Citrix Gateway 作为 ActiveSync 流量的代理，在外围提供 ActiveSync 过滤功能。因此，过滤组件位于邮件通信流的路径中，在邮件进入或离开环境时截获邮件。适用于 Exchange ActiveSync 的连接器将用作 Citrix Gateway 与 Endpoint Management 之间的中介。当某个设备通过 Citrix Gateway 上的 ActiveSync 虚拟服务器与 Exchange 通信时，Citrix Gateway 将对适用于 Exchange ActiveSync 的连接器服务执行 HTTP 标注。该服务随后将通过 Endpoint Management 检查设备状态。根据该设备的状态，适用于 Exchange ActiveSync 的连接器会答复 Citrix Gateway，指示允许或拒绝连接。您可能还会配置静态规则以根据用户、代理和设备类型或 ID 过滤访问。

此设置允许在增加了安全层的情况下面向 Internet 公开 Exchange ActiveSync 服务，以阻止未经授权的访问。设计注意事项包括以下各项：

- **Windows Server**： Exchange ActiveSync 组件的连接器需要 Windows Server。
- 筛选规则集： Exchange ActiveSync 的连接器旨在根据设备状态和信息而不是用户信息进行筛选。尽管您可以将静态规则配置为按用户 ID 进行过滤，但不存在根据（例如）Active Directory 组成员身份进行过滤的选项。如果对 Active Directory 组过滤存在要求，可以改为使用适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
- **Citrix Gateway** 可扩展性：考虑到通过 Citrix Gateway 代理 ActiveSync 流量的要求：恰当的 Citrix Gateway 实例规模对支持增加的所有 ActiveSync SSL 连接的工作负载至关重要。
- **Citrix Gateway** 集成缓存： Citrix Gateway 上的适用于 Exchange ActiveSync 的连接器配置使用集成缓存功能来缓存来自该连接器的响应。该配置的结果是，Citrix Gateway 不需要为给定会话中的每个 ActiveSync 事务向连接器发出请求。该配置对实现足够的性能和规模而言也非常重要。集成缓存可与 Citrix Gateway Platinum Edition 一起使用。
- 自定义过滤策略：您可能需要创建自定义 Citrix Gateway 策略以限制标准本地移动客户端外部的某些 ActiveSync 客户端。此配置要求用户了解 ActiveSync HTTP 请求和 Citrix Gateway 响应程序策略创建。
- **Secure Mail** 客户端： Secure Mail 具有微型 VPN 功能，无需在外围进行过滤。通过 Citrix Gateway 进行连接时，Secure Mail 客户端通常会被视为内部（可信）ActiveSync 客户端。如果同时支持本机和第三方客户端（通过适用于 Exchange ActiveSync 的连接器）且需要 Secure Mail 客户端，Citrix 建议不要通过用于连接器的 Citrix Gateway 虚拟服务器传输 Secure Mail 流量。可以通过 DNS 实现此通信流，并保持连接器策略不影响 Secure Mail 客户端。

有关 Endpoint Management 部署中用于 Exchange ActiveSync 的 Citrix Gateway 连接器的图表，请参阅 架构。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

适用于 **Exchange ActiveSync** 的 **Endpoint Management** 连接器

适用于 Exchange ActiveSync 的 Endpoint Management 连接器是一个 Endpoint Management 组件，在 Exchange 服务级别提供 ActiveSync 过滤功能。因此，过滤仅在邮件抵达 Exchange 服务时发生，而不是在其进入 Endpoint Management 环境时发生。Mail Manager 使用 PowerShell 查询 Exchange ActiveSync 中的设备合作关系信息，并通过设备隔离操作来控制访问。这些操作可根据适用于 Exchange ActiveSync 的 Endpoint Management 连接器的规则条件隔离和取消隔离设备。

与适用于 Exchange ActiveSync 的 Citrix Gateway 连接器类似，适用于 Exchange ActiveSync 的连接器可通过 Endpoint Management 检查设备状态以基于设备合规性过滤访问权限。您可能还会配置静态规则以根据设备类型或 ID、代理版本和 Active Directory 组成员身份来过滤访问。

此解决方案不需要使用 Citrix Gateway。您无需更改现有 ActiveSync 流量的传输方式，即可部署适用于 Exchange ActiveSync 的连接器。设计注意事项包括：

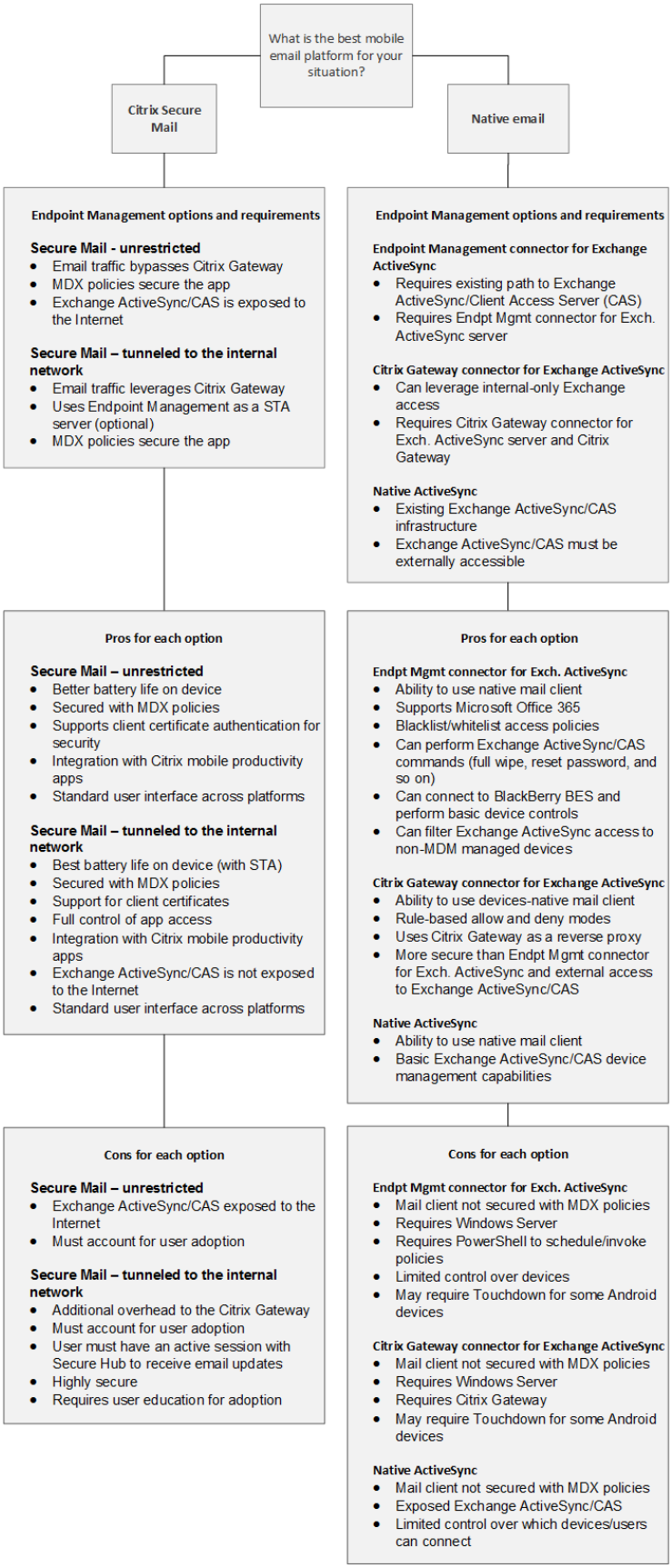
- **Windows Server**：适用于 Exchange ActiveSync 的连接器需要您部署 Windows Server。
- 过滤规则集：与适用于 Exchange ActiveSync 的 Citrix Gateway 连接器一样，适用于 Exchange ActiveSync 的连接器包含用于评估设备状态的过滤规则。此外，适用于 Exchange ActiveSync 的连接器还支持静态规则以根据 Active Directory 组成员身份进行过滤。
- **Exchange** 集成：适用于 Exchange ActiveSync 的连接器要求直接访问托管 ActiveSync 角色的 Exchange 客户端访问服务器 (CAS) 以及控制设备隔离操作。此要求可能会提出挑战，具体取决于环境体系结构和安全态势。提前评估此技术要求至关重要。
- 其他 **ActiveSync** 客户端：由于适用于 Exchange ActiveSync 的连接器在 ActiveSync 服务级别进行过滤，因此，请考虑 Endpoint Management 环境外部的其他 ActiveSync 客户端。可以配置适用于 Exchange ActiveSync 的连接器静态规则以避免对其他 ActiveSync 客户端产生非预期的影响。
- 扩展的 **Exchange** 功能：通过与 Exchange ActiveSync 直接集成，适用于 Exchange ActiveSync 的连接器将为 Endpoint Management 提供在移动设备上执行 Exchange ActiveSync 擦除的功能。适用于 Exchange ActiveSync 的连接器还允许 Endpoint Management 访问与黑莓设备有关的信息以及执行其他控制操作。

有关 Endpoint Management 部署中 Exchange ActiveSync 的 Endpoint Management 连接器的图表，请参阅体系结构。

电子邮件平台决策树

下图将帮助您区分在 Endpoint Management 部署中使用本机电子邮件或 Secure Mail 解决方案之间的利弊。每种选择都会考虑到关联的 Endpoint Management 选项以及对启用服务器、网络和数据库访问权限的要求。利弊包括与安全性、策略和用户界面注意事项有关的详细信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 集成

April 11, 2023

本文介绍了规划 Endpoint Management 与现有网络和解决方案的集成方式时要注意的事项。例如，如果您已在使用适用于 Citrix Virtual Apps and Desktops 的 Citrix Gateway：

- 要使用现有的 Citrix Gateway 实例还是使用新的专用实例?
- 是否要将使用 StoreFront 发布的 HDX 应用程序与 Endpoint Management 集成?
- 是否计划将 Citrix Files 与 Endpoint Management 结合使用?
- 是否有要集成到 Endpoint Management 的网络访问控制解决方案?

Citrix Gateway

Citrix Gateway 是 Endpoint Management 所必需的。Citrix Gateway 提供用于访问所有公司资源的 Micro VPN 路径，并提供加强的多重身份验证支持。

您可以使用现有的 Citrix Gateway 实例，也可以为 Endpoint Management 设置新实例。以下各节阐述了使用现有的 Citrix ADC 实例或新的专用 Citrix Gateway 实例的优势和劣势。

与为 **Endpoint Management** 创建的 **Citrix Gateway VIP** 共享 **Citrix Gateway MPX**

优势：

- 所有 Citrix 远程连接使用一个公用 Citrix Gateway 实例：Citrix Virtual Apps、完整 VPN 和无客户端 VPN。
- 对证书身份验证以及服务（例如 DNS、LDAP 和 NTP）访问等使用现有的 Citrix Gateway 配置。
- 使用单个 Citrix Gateway 平台许可证。

劣势：

- 在同一 Citrix Gateway 上处理两个截然不同的用例时，很难规划扩展。
- 有时某个 Citrix Virtual Apps 用例需要某个特定的 Citrix Gateway 版本。同一版本可能存在 Endpoint Management 的已知问题。或者，Endpoint Management 可能存在 Citrix Gateway 版本的已知问题。
- 如果存在 Citrix Gateway，则不能再次运行 NetScaler for XenMobile 向导为 Endpoint Management 创建 Citrix Gateway 配置。
- 除了将 Platinum 许可证用于 Citrix Gateway 11.1 或更高版本时外：安装在 Citrix Gateway 上及 VPN 连接所需的用户访问许可证汇集在池中。由于这些许可证可用于所有 Citrix Gateway 虚拟服务器，因此，Endpoint Management 以外的服务可能会占用这些许可证。

专用 **Citrix Gateway VPX/MPX** 实例

优势：

Citrix 建议使用专用的 Citrix Gateway 实例。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 更易于规划扩展，并可将 Endpoint Management 流量与资源可能已受限的 Citrix Gateway 实例分开。
- 避免在 Endpoint Management 和 Citrix Virtual Apps 需要不同的 Citrix Gateway 软件版本时出现问题。通常建议在 Endpoint Management 中使用最新的兼容 Citrix Gateway 版本和内部版本。
- 允许通过内置的 NetScaler for XenMobile 向导对 Citrix Gateway 进行 Endpoint Management 配置。
- 对服务进行虚拟和物理隔离。

劣势：

- 需要在 Citrix Gateway 上设置额外服务以支持 Endpoint Management 配置。
- 需要使用另一个 Citrix Gateway 平台许可证。为 Citrix Gateway 许可使用每个 Citrix Gateway 实例。

有关为 Endpoint Management 模式集成 Citrix Gateway 和 Citrix ADC 时应考虑的事项的信息，请参阅 与 Citrix Gateway 和 Citrix ADC 集成。

StoreFront

如果您有 Citrix Virtual Apps and Desktops 环境，则可以使用 StoreFront 将 HDX 应用程序与 Endpoint Management 集成。当您将 HDX 应用程序与 Endpoint Management 集成时：

- 这些应用程序可供注册到 Endpoint Management 的用户使用。
- 这些应用程序与其他移动应用程序一起显示在应用商店中。
- Endpoint Management 在 StoreFront 上使用 Citrix Receiver。
- 在设备上安装 Citrix Workspace 应用程序后，HDX 应用程序将开始使用该应用程序。

StoreFront 存在每个 StoreFront 实例一个服务站点的限制。假设您有多个应用商店，并想要将其与其他生产使用情况分开。在这种情况下，Citrix 通常建议考虑将一个新的 StoreFront 实例和服务站点用于 Endpoint Management。

注意事项包括：

- StoreFront 是否有任何不同的身份验证要求？StoreFront 服务站点要求使用 Active Directory 凭据进行登录。仅使用基于证书的身份验证的客户不能使用同一 Citrix Gateway 通过 Endpoint Management 枚举应用程序。
- 使用同一应用商店还是创建一个应用商店？
- 使用同一还是不同的 StoreFront 服务器？

以下各部分内容阐述了对 Citrix Workspace 和 Citrix 移动生产力应用程序使用单独的 StoreFront 和组合的 StoreFront 的优势和劣势。

将现有的 **StoreFront** 实例与 **Endpoint Management** 集成

优势：

- 同一应用商店：假定您使用同一 Citrix Gateway VIP 访问 HDX，不需要为 Endpoint Management 对 StoreFront 进行额外配置。假设您选择使用同一应用商店，并想要将 Citrix Workspace 访问定向至新的 Citrix Gateway VIP。在这种情况下，可将合适的 Citrix Gateway 配置添加到 StoreFront。
- 同一 StoreFront 服务器：使用现有的 StoreFront 安装和配置。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

劣势：

- 同一应用商店：如果为了支持 Citrix Virtual Apps and Desktops 工作负载而对 StoreFront 进行任何重新配置，也可能会对 Endpoint Management 产生不利影响。
- 同一 StoreFront 服务器：在大型环境中，要考虑 Endpoint Management 使用 Citrix Receiver 进行应用程序枚举和启动产生的额外负载。

将新的专用 **StoreFront** 实例用于与 **Endpoint Management** 集成

优势：

- 新应用商店：为 Endpoint Management 对 StoreFront 应用商店进行任何配置更改不会影响现有的 Virtual Apps and Desktops 工作负载。
- 新的 StoreFront 服务器：服务器配置更改不会影响 Virtual Apps and Desktops 工作流。此外，Citrix Receiver 用于应用程序枚举和启动的 Endpoint Management 外部的加载不会影响可扩展性。

劣势：

- 新应用商店：StoreFront 应用商店配置。
- 新的 StoreFront 服务器：需要新的 StoreFront 安装和配置。

有关更多信息，请 通过应用商店查看 Citrix Virtual Apps and Desktops。

Citrix Content Collaboration 和 Citrix Files

您可以利用 Citrix Content Collaboration 轻松、安全地交换文档、通过电子邮件发送大型文档、安全地处理向第三方的文档传输。用户可以通过 Citrix Files 应用程序从任何设备访问和同步自己的所有数据。借助 Citrix Files，用户可以与组织内部和外部的人安全地共享数据。

Citrix Content Collaboration 与 Endpoint Management 的集成取决于站点是否启用了 Workspace。

如果 **Endpoint Management** 启用了 **Workspace**

将 Citrix Workspace 和 Citrix Workspace 应用程序与 Citrix Content Collaboration 结合使用时，您可以：

- 从 Citrix Workspace 中的“文件”选项卡访问所有文件。
- 查看所有收藏夹、个人文件夹和共享文件夹以及访问云连接器。
- 提交文件以供反馈和批准，查看您的文件盒，管理您的回收站以及编辑文件。
- 有关工作区中不支持的 Citrix Collaboration 功能的信息，请参阅 部署 和 创建 Content Collaboration (ShareFile) 帐户或将其链接到 Citrix Cloud。

如果 **Endpoint Management** 未启用 **Workspace**

如果 Endpoint Management 未启用 Workspace，则需要将 Content Collaboration 与 Endpoint Management 集成。Endpoint Management 为 Citrix Files 提供：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 移动生产力应用程序用户的单点登录身份验证。
- 基于 Active Directory 的用户帐户预配。
- 全面的访问控制策略。

移动设备用户将从完整的 Enterprise 帐户功能集受益。

或者，可以将 Endpoint Management 配置为只与存储区域连接器集成。通过存储区域连接器，Citrix Files 提供对以下对象的访问：

- 文档和文件夹
- 网络文件共享
- 在 SharePoint 站点中：站点集合和文档库。

连接的文件共享可以包括 Citrix Virtual Apps and Desktops 环境中使用的相同网络主驱动器。可使用 Endpoint Management 控制台配置与 Enterprise 帐户或存储区域连接器的集成。有关更多信息，请参阅 用于 Endpoint Management 的 Citrix Files。

以下各节阐述了为 Citrix Files 制定设计决策时提出的问题。

与 **Citrix Files** 集成或仅与存储区域连接器集成

要提问的问题：

- 是否希望在 Citrix 托管的存储区域中存储数据?
- 是否要向用户提供文件共享和同步功能?
- 是否要让用户能够访问 Citrix Files Web 站点上的文件？或者，是否要从移动设备访问 Office 365 内容和个人云连接器?

设计决策：

- 如果对所有这些问题都回答“是”，则与 Enterprise 帐户集成。
- 仅与存储区域连接器的集成为 iOS 用户提供对现有本地部署存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问权限。在此配置中，您不会设置 Citrix Files 子域、将用户预配到 Citrix Files 或托管 Citrix Files 数据。将存储区域连接器与 Endpoint Management 结合使用时遵守防止在企业网络外部泄漏用户信息的安全限制。

存储区域控制器服务器位置

要提问的问题：

- 是否需要本地存储或功能（例如存储区域连接器)?
- 如果使用 Citrix Files 的本地功能，存储区域控制器将位于网络中的什么位置?

设计决策：

- 确定将存储区域控制器服务器置于 Citrix Files 云中、本地单租户存储系统中还是支持的第三方云存储中。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 存储区域控制器需要某些 Internet 访问权限以与 Citrix Files 控制平面进行通信。可以采用多种方式进行连接，包括直接访问或 NAT/PAT 配置。

存储区域连接器

要提问的问题：

- CIFS 共享路径是什么？
- SharePoint URL 是什么？

设计决策：

- 确定访问这些位置是否需要本地存储区域控制器。
- 由于存储区域连接器与内部资源（例如，文件存储库、CIFS 共享和 SharePoint）进行通信：Citrix 建议存储区域控制器位于 DMZ 防火墙后面的内部网络中，且 Citrix Gateway 位于前端。

SAML 与 **Endpoint Management** 集成

要提问的问题：

- Citrix Files 是否需要 Active Directory 身份验证？
- 首次使用适用于 Endpoint Management 的 Citrix Files 应用程序是否需要 SSO？
- 当前环境中是否存在标准 IdP？
- 使用 SAML 需要多少个域？
- Active Directory 用户是否有多个电子邮件别名？
- 是否有正在进行或计划不久将进行的任何 Active Directory 域迁移？

设计决策：

您可以选择使用 SAML 作为 Citrix Files 的身份验证机制。身份验证方式包括：

- 使用 Endpoint Management 服务器作为 SAML 的身份提供程序 (IdP)

  此选项可以提供卓越的用户体验、自动创建 Citrix Files 帐户以及启用移动应用程序 SSO 功能。

  在此过程可增强 Endpoint Management 服务器：不需要同步 Active Directory。

  使用 Citrix Files 用户管理工具进行用户预配。

- 使用受支持的第三方供应商作为 SAML 的 IdP

  如果您已有受支持的 IdP，且不需要移动应用程序 SSO 功能，此方式可能最适合您。此方式还需要使用 Citrix Files 用户管理工具进行帐户预配。

  使用第三方 IdP 解决方案（例如 ADFS）还可以在 Windows 客户端上提供 SSO 功能。请务必在选择 Citrix Files SAML IdP 之前评估用例。

- 或者，要满足这两种用例，请参阅适用 于双重身份提供商的 Citrix Content Collaboration 单点登录配置指南。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

移动应用程序

要提问的问题：

- 您计划使用哪种 Citrix Files 移动应用程序（公共、MDM、MDX）？

设计决策：

- 从 Apple App Store 和 Google Play 应用商店分发 Citrix 移动生产力应用程序。采用这种公共应用商店分发，您可以从 Citrix 下载页面获取打包的应用程序。
- 如果您的安全要求较低，并且不需要容器化，公共 Citrix Files 应用程序可能不适用。
- 有关更多信息，请参阅 Endpoint Management 的 [应用程序](/zh-cn/citrix-endpoint-management/advanced-concepts/deployment/apps.html) 和 Citrix Files。

安全性、策略和访问控制

要提问的问题：

- 对桌面、Web 和移动用户有哪些限制要求？
- 对用户要进行哪些标准访问控制设置？
- 计划使用什么文件保留策略？

设计决策：

- Citrix Files 允许您管理员工权限。有关信息，请参阅 员工权限。
- 某些 Citrix Files 设备安全设置和 MDX 策略控制相同的功能。在这些情况下，Endpoint Management 策略优先于 Citrix Files 设备安全设置。示例：如果您在 Citrix Files 中禁用外部应用程序，但在 Endpoint Management 中启用这些应用程序，则在 Citrix Files 中外部应用程序处于禁用状态。您可以配置应用程序，以实现 Endpoint Management 不要求使用 PIN/通行码，但 Citrix Files 应用程序要求使用 PIN/通行码。

标准存储区域与受限存储区域

要提问的问题：

- 是否需要受限存储区域？

设计决策：

- 标准存储区域专用于存储非敏感数据，员工可以在此区域中与非员工共享数据。此方式支持涉及在域外部共享数据的工作流。
- 受限存储区域保护敏感数据：只有通过身份验证的域用户可以访问此区域中存储的数据。

访问控制

企业可以管理网络内部和外部的移动设备。企业移动性管理解决方案（例如 Endpoint Management）非常适合为移动设备提供安全和控制功能，而与位置无关。但是，将其与网络访问控制 (NAC) 解决方案结合使用时，可以为您网络内

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

部的设备增加 QoS 和更加细化的控制。该组合让您可以通过您的 NAC 解决方案延长 Endpoint Management 设备安全评估。之后您的 NAC 解决方案可以使用 Endpoint Management 安全评估帮助制定和处理身份验证决策。

可以使用以下任意解决方案来强制实施 NAC 策略：

- Citrix Gateway
- ForeScout

Citrix 不保证其他 NAC 解决方案的集成。

NAC 解决方案与 Endpoint Management 的集成具有以下优势：

- 提高了企业网络上所有端点的安全性和合规性，并增强了对其控制能力。
- NAC 解决方案可以：
  - 在设备尝试连接到网络的同时检测到设备。
  - 查询 Endpoint Management 的设备属性。
  - 请使用该设备信息来确定允许、阻止、限制还是重定向这些设备。这些决策取决于您选择强制执行的安全策略。
- NAC 解决方案为 IT 管理员提供非托管设备和不合规设备信息。

有关 Endpoint Management 支持的 NAC 合规性筛选器的说明和配置概述，请参阅 网络访问控制。

与 **Citrix Gateway** 和 **Citrix ADC** 集成

December 3, 2021

与 Endpoint Management 集成后，Citrix Gateway 为 MAM 设备提供了远程设备访问内部网络时使用的身份验证机制。通过该集成，Citrix 移动生产力应用程序可以通过 Micro VPN 连接到 Intranet 中的公司服务器。Endpoint Management 在设备上的应用程序与 Citrix Gateway 之间创建一个 Micro VPN。Citrix Gateway 提供用于访问所有公司资源的 Micro VPN 路径，并提供加强的多重身份验证支持。

当用户选择退出 MDM 注册时，设备将使用 Citrix Gateway FQDN 进行注册。

Citrix Cloud 运营团队负责管理 Citrix ADC 负载平衡。

设计决策

以下各节概述了规划 Citrix Gateway 与 Endpoint Management 的集成时要考虑的多个设计决策。

证书

决策详细信息：

- Endpoint Management 环境中的注册和访问是否需要更高的安全性？
- 是否无法使用 LDAP？

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设计指导：

Endpoint Management 的默认配置是用户名和密码身份验证。要为 Endpoint Management 环境中的注册和访问再增加一个安全层，请考虑使用基于证书的身份验证。您可以组合使用证书与 LDAP 以实现双重身份验证，从而提高安全性，而无需 RSA 服务器。

如果禁用了 LDAP 并且不希望使用智能卡或类似方法，配置证书可代替智能卡来访问 Endpoint Management。用户随后使用 Endpoint Management 生成的唯一 PIN 进行注册。用户获取访问权限后，Endpoint Management 将创建和部署以后用来在 Endpoint Management 环境中执行身份验证的证书。

Endpoint Management 支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，Endpoint Management 将使用 Citrix Gateway 管理吊销。配置基于客户端证书的身份验证时，请考虑是否需要配置 Citrix Gateway 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh**（启用 CRL 自动刷新）。此步骤可确保使用在仅 MAM 模式下注册的设备的用户无法使用设备上的现有证书进行身份验证。Endpoint Management 将重新颁发新证书，因为吊销用户证书后，Endpoint Management 不会限制用户生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

专用或共享的 **Citrix Gateway VIP**

决策详细信息：

- 您目前是否为 Citrix Virtual Apps and Desktops 使用 Citrix Gateway?
- Endpoint Management 是否使用与 Citrix Virtual Apps and Desktops 相同的 Citrix Gateway?
- 两种通信流的身份验证要求是什么?

设计指导：

如果您的 Citrix 环境包含 Endpoint Management 以及 Virtual Apps and Desktops，两者可以使用相同的 Citrix Gateway 虚拟服务器。由于可能存在版本控制冲突和环境隔离，建议每个 Endpoint Management 环境使用专用 Citrix Gateway。

如果您使用 LDAP 身份验证，Citrix Workspace 和 Secure Hub 可以向同一 Citrix Gateway 进行身份验证，不会有任何问题。如果您使用基于证书的身份验证，Endpoint Management 将推送 MDX 容器中的证书，Secure Hub 将使用该证书向 Citrix Gateway 进行身份验证。Workspace 应用程序与 Secure Hub 是分开的，无法与 Secure Hub 使用同一证书向同一 Citrix Gateway 进行身份验证。

您可以考虑以下解决方法，这样，您可以对两个 Citrix Gateway VIP 使用同一 FQDN。您可以创建两个具有相同 IP 地址的 Citrix Gateway VIP。用于 Secure Hub 的 VIP 使用标准 443 端口，用于 Citrix Virtual Apps and Desktops（部署 Citrix Workspace 应用程序）的 VIP 使用端口 444。然后，一个 FQDN 解析为相同的 IP 地址。对于此解决方法，您可能需要将 StoreFront 配置为返回端口 444 而不是默认端口 443 的 ICA 文件。此解决方法不需要用户输入端口号。

Citrix Gateway 超时

决策详细信息：

- 您要如何配置 Endpoint Management 流量的 Citrix Gateway 超时?

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设计指南：

Citrix Gateway 包括“会话超时”和“强制超时”设置。有关详细信息，请参阅建议的配置。请谨记，后台服务、Citrix Gateway 以及脱机时访问应用程序的超时值不同。

注册 **FQDN**

> 重要：
>
> 要更改注册，FQDN 需要一个新的 SQL Server 数据库和 Endpoint Management 服务器重新构建。

Secure Web 流量

决策详细信息：

- Secure Web 是否仅限制于内部 Web 浏览？
- 是否启用 Secure Web 进行内部 Web 浏览和外部 Web 浏览？

设计指导：

如果您计划仅使用 Secure Web 进行内部 Web 浏览，Citrix Gateway 配置将非常简单。但是，如果默认情况下 Secure Web 无法访问所有内部站点，您可能需要配置防火墙和代理服务器。

如果您计划将 Secure Web 用于外部浏览和内部浏览，则必须启用 SNIP 以便具有出站 Internet 访问权限。IT 通常将注册的设备（使用 MDX 容器）视为企业网络的扩展。因此，IT 通常希望 Secure Web 连接恢复到 Citrix Gateway，通过代理服务器，然后转到 Internet。默认情况下，Secure Web 访问通过通道连接到内部网络。Secure Web 对所有网络访问使用返回到内部网络的 PerApp VPN 通道，并且 Citrix Gateway 使用拆分通道设置。

有关 Secure Web 连接的讨论，请参阅配置用户连接。

Secure Mail 的推送通知

决策详细信息：

- 是否使用推送通知？

适用于 iOS 的设计指导：

如果 Citrix Gateway 配置包括 Secure Ticket Authority (STA)，并且拆分通道已关闭，Citrix Gateway 必须允许从 Secure Mail 到 Citrix 侦听器服务 URL 的流量。这些 URL 在 Secure Mail for iOS 的推送通知中指定。

适用于 Android 的设计指导：

请使用 Firebase Cloud Messaging (FCM) 控制 Android 设备需要连接到 Endpoint Management 的方式和时间。配置了 FCM 后，任何安全操作或部署命令都将触发向 Secure Hub 推送通知，以提示用户重新连接到 Endpoint Management 服务器。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

HDX STA

决策详细信息：

- 如果集成 HDX 应用程序访问，要使用什么 STA?

设计指导：

HDX STA 必须匹配 StoreFront 中的 STA，并且必须对 Virtual Apps and Desktops 站点有效。

Citrix Files 和 Citrix Content Collaboration

决策详细信息：

- 您是否会在环境中使用存储区域控制器?
- 将使用什么 Citrix Files VIP URL?

设计指导：

如果您将在环境中包含存储区域控制器，请确保正确配置以下对象：

- Citrix Files 内容交换机 VIP（Citrix Files 控制平面用于与存储区域控制器服务器通信）
- Citrix Files 负载平衡 VIP
- 所有必需的策略和配置文件

有关信息，请参阅存储区域控制器的文档。

SAML IdP

决策详细信息：

- 如果 Citrix Files 需要 SAML，您是否要将 Endpoint Management 用作 SAML IdP?

设计指导：

推荐的最佳做法是，将 Citrix Files 与 Endpoint Management 集成，这样做比配置基于 SAML 的联合身份验证更简单。Endpoint Management 为 Citrix Files 提供：

- Citrix 移动生产力应用程序用户的单点登录 (SSO) 身份验证
- 基于 Active Directory 的用户帐户预配
- 全面的访问控制策略。

通过 Endpoint Management 控制台，可以执行 Citrix Files 配置以及监视服务级别和许可证使用情况。

有两种类型的 Citrix Files 客户端：适用于 Endpoint Management 的 Citrix Files（又称为打包的 Citrix Files）和 Citrix Files 移动客户端（又称为未打包的 Citrix Files）。要了解差别，请参阅 Citrix Files for Endpoint Management 客户端与 Citrix Files 移动客户端之间的差别。

可以将 Endpoint Management 和 Citrix Files 配置为使用 SAML 提供对以下内容的 SSO 访问：

- 使用 MDX Toolkit 启用或封装 MAM SDK 的 Citrix Files 应用程序

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 未封装的 Citrix Files 客户端，例如 Web 站点、Outlook 插件或同步客户端

如果要将 Endpoint Management 用作 Citrix Files 的 SAML IdP，请确保已实施合适的配置。有关详细信息，请参阅 SAML SSO 与 Citrix Files。

ShareConnect 直接连接

决策详细信息：

- 用户是否从运行使用直接连接的 ShareConnect 的计算机或移动设备访问主机计算机？

设计指导：

借助 ShareConnect，用户可以通过 iPad、Android 平板电脑和 Android 手机安全地连接到其计算机，以访问文件和应用程序。对于直接连接，Endpoint Management 使用 Citrix Gateway 提供对本地网络外部的资源的安全访问。有关配置详细信息，请参阅 ShareConnect。

每个管理模式的注册 **FQDN**

管理模式	注册 FQDN
采用强制 MDM 注册的 MDM+MAM	Endpoint Management 服务器 FQDN
采用可选 MDM 注册的 MDM+MAM	Endpoint Management 服务器 FQDN 或 Citrix Gateway FQDN
仅 MAM	Endpoint Management 服务器 FQDN
仅 MAM（旧版）	Citrix Gateway FQDN

部署摘要

如果您有多个 Endpoint Management 实例（例如，用于测试、开发和生产环境），则必须手动为其他环境配置 Citrix Gateway。您有工作环境时，请先记下设置，然后再尝试手动为 Endpoint Management 配置 Citrix Gateway。

一个主要决定是对与 Endpoint Management 服务器的通信使用 HTTPS 还是 HTTP。HTTPS 提供安全的后端通信，因为 Citrix Gateway 与 Endpoint Management 之间的流量已加密。重新加密会影响 Endpoint Management 服务器性能。HTTP 提供了更好的 Endpoint Management 服务器性能。Citrix Gateway 与 Endpoint Management 之间的流量未加密。以下各表显示了 Citrix Gateway 和 Endpoint Management 的 HTTP 和 HTTPS 端口要求。

HTTPS

Citrix 通常建议对 Citrix Gateway MDM 虚拟服务器配置使用 SSL 桥接。如果对 MDM 虚拟服务器使用 Citrix Gateway SSL 卸载，Endpoint Management 仅支持后端服务使用端口 80。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

管理模式	Citrix Gateway 负载平衡方法	SSL 重新加密	Endpoint Management 服务器端口
MAM	SSL 卸载	已启用	8443
MDM+MAM	MDM：SSL 桥接	不适用	443、8443
MDM+MAM	MAM：SSL 卸载	已启用	8443

HTTP

管理模式	Citrix Gateway 负载平衡方法	SSL 重新加密	Endpoint Management 服务器端口
MAM	SSL 卸载	已启用	8443
MDM+MAM	MDM：SSL 卸载	不支持	80
MDM+MAM	MAM：SSL 卸载	已启用	8443

有关 Endpoint Management 部署中的 Citrix Gateway 图表，请参阅体系结构。

MDX 应用程序的 SSO 和代理注意事项

April 11, 2023

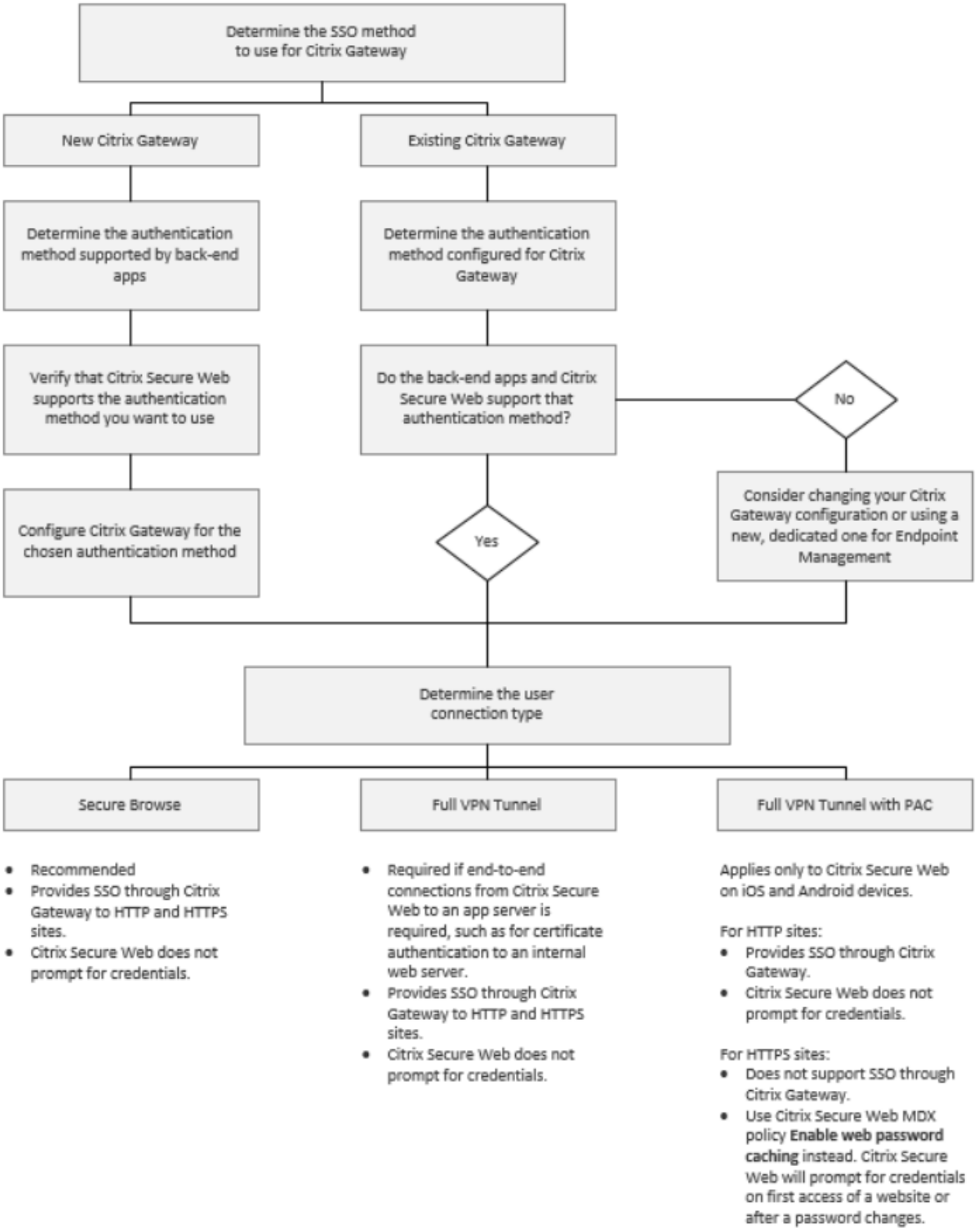
通过 Endpoint Management 与 Citrix Gateway 的集成，您可以向用户提供通过单点登录 (SSO) 访问所有后端 HTTP/HTTPS 资源的功能。根据您的 SSO 身份验证要求，将 MDX 应用程序的用户连接配置为使用 Secure Browse (通道 - Web SSO)，这是一种无客户端 VPN。

> 重要：
>
> Citrix 弃用了对 iOS 和 Android 设备的完整 VPN 通道部署使用完整 VPN 通道和代理自动配置 (PAC) 文件的支持。有关详细信息，请参阅弃用。

如果 Citrix Gateway 不是在您的环境中提供 SSO 的最佳方法，则可以为 MDX 应用程序设置基于策略的本地密码缓存。本文探讨了各种 SSO 和代理选项，重点探讨 Secure Web。这些概念适用于其他 MDX 应用程序。

下面的流程图概括了 SSO 和用户连接的决策流程。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Citrix Gateway 身份验证方法

本节提供了有关 Citrix Gateway 支持的身份验证方法的常规信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

SAML 身份验证

将 Citrix Gateway 配置为使用安全声明标记语言 (SAML) 时，用户可以连接到支持使用 SAML 协议进行单点登录的 Web 应用程序。Citrix Gateway 支持对 SAML Web 应用程序进行身份提供程序 (IdP) 单点登录。

所需的配置：

- 在 Citrix Gateway 流量配置文件中配置 SAML SSO。
- 为请求的服务配置 SAML IdP。

NTLM 身份验证

如果在会话配置文件中启用了通过 SSO 登录 Web 应用程序的功能，Citrix Gateway 将自动执行 NTLM 身份验证。

所需的配置：

- 在 Citrix Gateway 会话或流量配置文件中启用 SSO。

Kerberos 模拟

Endpoint Management 仅支持对 Secure Web 使用 Kerberos。将 Citrix Gateway 配置为进行 Kerberos SSO 时，Citrix Gateway 将在用户密码对 Citrix Gateway 可用时使用模拟。模拟是指 Citrix Gateway 使用用户凭据获得获取对 Secure Web 等服务的访问权限所需的令牌。

所需的配置：

- 配置 Citrix Gateway `Worx` 会话策略以允许其识别来自您的连接的 Kerberos 领域。
- 在 Citrix Gateway 上配置 Kerberos 约束委派 (KCD) 帐户。将该帐户配置为无密码，并将其绑定到您的 Endpoint Management 网关上的流量策略。
- 有关这些配置及其他配置的详细信息，请参阅 Citrix 博客：WorxWeb and Kerberos Impersonation SSO（WorxWeb 和 Kerberos 模拟 SSO）。

Kerberos 约束委派

Endpoint Management 仅支持对 Secure Web 使用 Kerberos。将 Citrix Gateway 配置为进行 Kerberos SSO 时，Citrix Gateway 将在用户密码对 Citrix Gateway 不可用时使用约束委派。

启用了约束委派时，Citrix Gateway 将使用指定的管理员帐户代表用户和服务获取令牌。

所需的配置：

- 在 Active Directory 中配置具有所需权限的 KCD 帐户，并在 Citrix Gateway 上配置 KDC 帐户。
- 在 Citrix Gateway 流量配置文件中启用 SSO。
- 将后端 Web 站点配置为进行 Kerberos 身份验证。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

表单填充身份验证

将 Citrix Gateway 配置为进行基于表单的单点登录时，用户登录一次即可访问您的网络中所有受保护的应用程序。此身份验证方法适用于使用“通道 - Web SSO”模式的应用程序。

所需的配置：

- 在 Citrix Gateway 流量配置文件中配置基于表单的 SSO。

摘要式 **HTTP** 身份验证

如果在会话配置文件中启用通过 SSO 登录 Web 应用程序的功能，Citrix Gateway 将自动执行摘要式 HTTP 身份验证。此身份验证方法适用于使用“通道 - Web SSO”模式的应用程序。

所需的配置：

- 在 Citrix Gateway 会话或流量配置文件中启用 SSO。

基本 **HTTP** 身份验证

如果在会话配置文件中启用通过 SSO 登录 Web 应用程序的功能，Citrix Gateway 将自动执行基本 HTTP 身份验证。此身份验证方法适用于使用“通道 - Web SSO”模式的应用程序。

所需的配置：

- 在 Citrix Gateway 会话或流量配置文件中启用 SSO。

安全通道 **- Web SSO**

本部分介绍了 Secure Web 的通道 **- Web SSO** 用户连接类型。

通过通道连接到内部网络的连接可以使用无客户端 VPN 的变体（称为“通道 - Web SSO”）。“通道 - Web SSO”是为 Secure Web 首选 **VPN** 模式策略指定的默认配置。Citrix 建议您对需要单点登录的连接使用通道 - Web SSO。

在“通道 - Web SSO”模式下，Citrix Gateway 将 HTTPS 会话分为两个部分：

- 从客户端到 Citrix Gateway
- 从 Citrix Gateway 到后端资源服务器。

这样，Citrix Gateway 将在客户端与服务器之间的所有事务中完全可见，使其能够提供 SSO。

在“通道 - Web SSO”模式下使用时，还可以为 Secure Web 配置代理服务器。有关详细信息，请参阅博客 Endpoint Management WorxWeb 在 Secure Browse 模式下通过代理服务器的流量。

> 注意：
>
> Citrix 宣布弃用了带有 PAC 的完整 VPN 通道。请参阅弃用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 支持 Citrix Gateway 提供的代理身份验证。PAC 文件中包含的规则用于定义 Web 浏览器如何选择代理以访问指定 URL。PAC 文件规则可以指定对外部和内部站点的处理方式。Secure Web 解析 PAC 文件规则并将代理服务器信息发送到 Citrix Gateway。Citrix Gateway 无法识别 PAC 文件或代理服务器。

对于 HTTPS Web 站点的身份验证：Secure Web MDX 策略启用 **Web** 密码缓存允许 Secure Web 进行身份验证并通过 MDX 提供对代理服务器的 SSO。

Citrix Gateway 拆分通道

规划 SSO 和代理配置时，还必须决定是否要使用 Citrix Gateway 拆分通道。如有需要，Citrix 建议您仅使用 Citrix Gateway 拆分通道。本节从高层角度提供了拆分通道的工作原理：Citrix Gateway 根据其路由表确定流量路径。当 Citrix Gateway 拆分通道为“开”时，Secure Hub 将内部（受保护的）网络流量与 Internet 流量区分开。Secure Hub 根据 DNS 后缀和 Intranet 应用程序做出决定。然后，Secure Hub 仅通过 VPN 通道传输内部网络流量。Citrix Gateway 拆分通道设置为“关”时，所有流量都将通过 VPN 通道传输。

如果出于安全考虑，您更希望监视所有流量，请禁用 Citrix Gateway 拆分通道。这样，所有流量都通过 VPN 通道传输。

Citrix Gateway 还具有 Micro VPN 反向拆分通道模式。此配置支持不通过通道连接到 Citrix Gateway 的 IP 地址的排除列表。这些地址通过使用设备 Internet 连接发送。有关反向拆分通道的详细信息，请参阅 Citrix Gateway 文档。

Endpoint Management 包括 反向拆分隧道排除列表。要防止通过 Citrix Gateway 使用通道连接某些 Web 站点：添加将通过 LAN 连接的完全限定域名 (FQDN) 或 DNS 后缀的列表（以逗号分隔）。Citrix Gateway 配置为使用反向拆分通道时，此列表仅适用于“通道 - Web SSO”模式。

身份验证

October 18, 2022

在 Endpoint Management 部署中，确定如何配置身份验证时，要考虑多个注意事项。本部分内容介绍影响身份验证的各种因素：

- 身份验证涉及的主要 MDX 策略、Endpoint Management 客户端属性和 Citrix Gateway 设置。
- 这些策略、客户端属性和设置的交互方式。
- 每种选择的权衡因素。

本文还提供了三个提高安全等级的建议配置示例。

一般而言，随着安全性的提高，最佳用户体验会降低，因为用户必须更加频繁地进行身份验证。如何平衡这些考虑因素取决于组织的需求和优先级。请查看推荐的三种配置，了解各种身份验证选项之间的相互作用。

身份验证模式

联机身份验证：允许用户访问 Endpoint Management 网络。需要 Internet 连接。

脱机身份验证：在设备上进行。用户解锁安全保管库并脱机访问一些项目，例如，下载的邮件、缓存的 Web 站点和笔记。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

身份验证方法

单因素

LDAP：在 Endpoint Management 中，可以配置到一个或多个与轻型目录访问协议 (LDAP) 兼容的目录的连接。此方法是提供以单点登录 (SSO) 方式访问公司环境的常用方法。可以选择对 Citrix PIN 使用 Active Directory 密码缓存功能，以改进使用 LDAP 的用户体验。同时，您可以在注册、密码过期和帐户锁定时提供复杂密码的安全性。

有关更多详细信息，请参阅域或域加安全令牌身份验证。

客户端证书： Endpoint Management 可以与行业标准证书颁发机构集成以将证书用作联机身份验证的唯一方法。Endpoint Management 在用户注册后提供此证书，这需要一次性密码、邀请 URL 或 LDAP 凭据。将客户端证书用作主要身份验证方法时，在仅客户端证书环境中需要使用 Citrix PIN 来确保设备上证书的安全。

Endpoint Management 仅支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，Endpoint Management 将使用 Citrix Gateway 管理吊销。配置基于客户端证书的身份验证时，请考虑是否需要配置 Citrix Gateway 证书吊销列表 (CRL) 设置 Enable CRL Auto Refresh（启用 CRL 自动刷新）。此步骤可确保仅在 MAM 中注册的设备无法使用设备上的现有证书进行身份验证。Endpoint Management 将重新颁发新证书，因为吊销用户证书后，Endpoint Management 不会限制用户生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

有关显示基于证书的身份验证或使用企业证书颁发机构 (CA) 颁发设备证书所需的部署的图表，请参阅身份验证。

双重身份验证

LDAP + 客户端证书：此配置是 Endpoint Management 安全性和用户体验的最佳组合。使用 LDAP 和客户端证书身份验证：

- 具有通过 Citrix Gateway 进行的双重身份验证提供的最佳 SSO 可能性和安全性。
- 通过用户知晓的内容（其 Active Directory 密码）和用户拥有的内容（设备上的客户端证书）提供安全性。

Secure Mail 可以通过客户端证书身份验证自动配置并提供无缝的首次用户体验。该功能需要正确配置的 Exchange 客户端访问服务器环境。

要实现最佳可用性，可以将 LDAP 和客户端证书身份验证与 Citrix PIN 和 Active Directory 密码缓存组合在一起。

LDAP + 令牌：此配置允许在使用 RADIUS 协议时采用 LDAP 凭据经典配置以及一次性密码。要实现最佳可用性，可以将此选项与 Citrix PIN 和 Active Directory 密码缓存组合在一起。

身份验证的重要策略、设置和客户端属性

以下三个建议配置中涉及以下策略、设置和客户端属性：

MDX 策略

应用程序通行码：如果设置为开，应用程序在处于不活动状态一段时间后启动或恢复时需要输入 Citrix PIN 或通行码才能解锁。默认值为开。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要为所有应用程序配置不活动计时器，请在 Endpoint Management 控制台中的设置选项卡上的客户端属性中设置 INACTIVITY_TIMER 值（分钟）。默认值为 15 分钟。要禁用不活动计时器以便 PIN 或通行码提示仅在应用程序启动时出现，请将值设置为 0。

要求 **Micro VPN** 会话：如果设置为开，用户必须连接到企业网络并且具有活动会话，才能访问设备上的应用程序。如果设置为 关，则无需活动会话即可访问设备上的应用程序。默认设置为关。

最长脱机时长（小时）：定义应用程序无需重新确认应用程序授权和刷新 Endpoint Management 中的策略即可运行的最长时段。满足以下条件后，iOS 应用程序会从 Endpoint Management 检索 MDX 应用程序的新策略，不会对用户造成任何干扰：

- 您设置“最长脱机期限”和
- Secure Hub for iOS 具有有效的 Citrix Gateway 令牌。

如果 Secure Hub 没有有效的 Citrix Gateway 令牌，则用户必须先通过 Secure Hub 进行身份验证，应用程序策略才能更新。由于 Citrix Gateway 会话处于非活动状态或强制会话超时策略，Citrix Gateway 令牌可能会失效。当用户再次登录 Secure Hub 时，他们可以继续运行应用程序。

将在期限过期前 30 分钟、15 分钟和 5 分钟提醒用户登录。超过时间后，将锁定应用程序，直到用户登录。默认值为 **72** 小时（**3** 天）。最长期限为 1 小时。

> 注意：
>
> 请谨记，在用户经常出差并使用国际漫游的情况下，默认值 72 小时（3 天）可能太短。

后台服务票证到期：后台网络服务票证保持有效的时间段。当 Secure Mail 通过 Citrix Gateway 连接到运行 ActiveSync 的 Exchange Server 时，Endpoint Management 会发出一个令牌。Secure Mail 使用该令牌连接到内部 Exchange Server。此属性设置确定 Secure Mail 可以使用该令牌（无需使用新令牌）进行身份验证并连接到 Exchange Server 的持续时间。超过时间限制后，用户必须重新登录以生成新令牌。默认值为 **168** 小时（**7** 天）。当此超时到期时，邮件通知将停止。

要求 **Micro VPN** 会话宽限期 **(**分钟**)**：确定验证联机会话之前，用户可以脱机使用应用程序的分钟数。默认值为 **0**（无宽限期）。

有关身份验证策略的信息，请参阅：

- 如果使用 MAM SDK：MAM SDK 概述
- 如果使用 MDX Toolkit：适用于 iOS 的 Endpoint Management MDX 策略和适用于 Android 的 Endpoint Management MDX 策略

Endpoint Management 客户端属性

> 注意：
>
> 客户端属性是应用于连接到 Endpoint Management 的所有设备的全局设置。

Citrix PIN：要实现简单点登录体验，您可以选择启用 Citrix PIN。使用 PIN 时，用户不需要重复输入其他凭据，例如 Active Directory 用户名和密码。您可以仅将 Citrix PIN 配置为独立脱机身份验证，也可以将 PIN 与 Active

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Directory 密码缓存组合在一起以简化身份验证，从而实现最佳可用性。可在 Endpoint Management 控制台中的设置 **>** 客户端 **>** 客户端属性中配置 Citrix PIN。

下面概述了一些重要属性。有关详细信息，请参阅客户端属性。

ENABLE_PASSCODE_AUTH

显示名称：启用 Citrix PIN 身份验证

此键允许您打开 Citrix PIN 功能。启用 Citrix PIN 或通行码后，系统将提示用户定义要使用的 PIN（而非其 Active Directory 密码）。如果启用了 **ENABLE_PASSWORD_CACHING**，或者如果 Endpoint Management 使用证书身份验证，请启用此设置。

可能的值： **true** 或 **false**

默认值： **false**

ENABLE_PASSWORD_CACHING

显示名称：启用用户密码缓存

此键允许您在移动设备本地缓存用户的 Active Directory 密码。当您将此键设置为 true 时，系统将提示用户设置 Citrix PIN 或通行码。当您将此键设置为 **true** 时，必须将 ENABLE_PASSCODE_AUTH 键设置为 true。

可能的值： **true** 或 **false**

默认值： **false**

PASSCODE_STRENGTH

显示名称： PIN 强度要求

此键定义 Citrix PIN 或通行码的强度。当您更改此设置时，系统会在下次提示用户进行身份验证时提示他们设置新的 Citrix PIN 或密码。

可能的值：低、中或强

默认值：中

INACTIVITY_TIMER

显示名称：不活动计时器

此键定义用户可以保持其设备处于不活动状态且之后访问应用程序不会提示输入 Citrix PIN 或通行码的时间（分钟）。要为 MDX 应用程序启用此设置，必须将应用程序通行码设置设为开。如果“应用程序密码”设置设置为“关”，则用户将被重定向到 Secure Hub 进行全面身份验证。更改此设置时，该值将在系统下次提示用户进行身份验证时生效。默认值为 15 分钟。

ENABLE_TOUCH_ID_AUTH

显示名称：启用 Touch ID 身份验证

允许在脱机身份验证时使用指纹读取器（仅限 iOS）。联机身份验证仍需要使用主要身份验证方法。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

ENCRYPT_SECRETS_USING_PASSCODE

显示名称：使用通行码加密机密

此键允许将敏感数据存储在移动设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串。此配置键允许对密钥进行强加密，但还会添加用户熵（用户生成的只有自己知道的随机 PIN 代码）。

可能的值： **true** 或 **false**

默认值： **false**

Citrix Gateway 设置

会话超时：如果启用此设置，则 Citrix Gateway 在指定的时间间隔内未检测到任何网络活动时，Citrix Gateway 将断开会话。对于通过 Citrix Gateway 插件、Citrix Workspace、Secure Hub 或通过 Web 浏览器连接的用户，强制执行此设置。默认值为 **1440** 分钟。如果将此值设置为零，则该设置处于禁用状态。

强制超时：如果启用此设置，则超过超时时间间隔后，无论用户正在执行什么操作，Citrix Gateway 都将断开会话。超时间隔过后，用户无法采取任何措施来防止断开连接。对于通过 Citrix Gateway 插件、Citrix Workspace、Secure Hub 或通过 Web 浏览器连接的用户，强制执行此设置。如果 Secure Mail 使用 STA（一种特殊 Citrix Gateway 模式），此设置将不应用到 Secure Mail 会话。默认值为无值，这意味着会话将针对任何活动延长。

有关 Citrix Gateway 的超时设置的详细信息，请参阅 Citrix Gateway 文档。

有关提示用户在其设备上输入凭据以在 Endpoint Management 中执行身份验证的情景的详细信息，请参阅身份验证提示情景。

默认配置设置

这些设置是由以下对象提供的默认设置：

- 适用于 XenMobile 的 NetScaler 向导
- MAM SDK 或 MDX Toolkit
- Endpoint Management 控制台

设置	设置的查找位置	默认设置
会话超时	Citrix Gateway	1440 分钟
强制超时	Citrix Gateway	无值（关）
最长脱机期限	MDX 策略	72 小时
后台服务票据过期日期	MDX 策略	168 小时（7 天）
要求 Micro VPN 会话	MDX 策略	关
要求 Micro VPN 会话宽限期	MDX 策略	0

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设置	设置的查找位置	默认设置
应用程序通行码	MDX 策略	开
使用通行码加密机密	Endpoint Management 客户端属性	false
启用 Citrix PIN 身份验证	Endpoint Management 客户端属性	false
PIN 强度要求	Endpoint Management 客户端属性	中
PIN 类型	Endpoint Management 客户端属性	数字
启用用户密码缓存	Endpoint Management 客户端属性	false
不活动计时器	Endpoint Management 客户端属性	15
启用 Touch ID 身份验证	Endpoint Management 客户端属性	false

建议的配置

本节提供的三个 Endpoint Management 配置示例是从最低安全性和最佳用户体验到最高安全性和干扰较多的用户体验。这些示例可为您在考虑如何在自己的配置中权衡这些因素时提供有用的参考要点。修改这些设置可能需要更改其他设置。例如，最长脱机时间不得超过会话超时时间。

最高安全性

这种配置提供了最高级别的安全性，但在可用性方面存在明显的权衡。

设置	设置的查找位置	建议设置	行为影响
会话超时	Citrix Gateway	1440	仅当要求进行联机身份验证时，用户输入其 Secure Hub 凭据 - 每 24 小时一次。
强制超时	Citrix Gateway	无值	如果存在任何活动，则将延长会话。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

最长脱机期限	MDX 策略	23	要求每天刷新策略。
后台服务票据过期日期	MDX 策略	72 小时	STA 超时，允许在没有 Citrix Gateway 会话令牌的情况下进行长时间会话。对于 Secure Mail，使 STA 超时时间长于会话超时时间可避免邮件通知停止。在这种情况下，如果用户在会话过期之前未打开应用程序，Secure Mail 不会提示用户。
要求 Micro VPN 会话	MDX 策略	关	提供有效的网络连接和 Citrix Gateway 会话以使用应用程序。
要求 Micro VPN 会话宽限期	MDX 策略	0	无宽限期（如果启用了“要求 Micro VPN 会话”）。
应用程序通行码	MDX 策略	开	需要应用程序的通行码。
使用通行码加密机密	Endpoint Management 客户端属性	true	从用户熵派生的密钥保护保管库。
启用 Citrix PIN 身份验证	Endpoint Management 客户端属性	true	启用 Citrix PIN 以实现简化的身份验证体验。
PIN 强度要求	Endpoint Management 客户端属性	强	高密码复杂性要求。
PIN 类型	Endpoint Management 客户端属性	字母数字	PIN 是一个字母数字序列。
启用密码缓存	Endpoint Management 客户端属性	false	Active Directory 密码未缓存，Citrix PIN 用于离线身份验证。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

不活动计时器	Endpoint Management 客户端属性	15	如果在此时间段内用户未使用 MDX 应用程序或 Secure Hub，则提示进行脱机身份验证。
启用 Touch ID 身份验证	Endpoint Management 客户端属性	false	在 iOS 中对脱机身份验证用例禁用 Touch ID。

更高的安全性

比较均衡的方法，此配置要求用户更加频繁地（最多每 3 天一次，而不是 7 天）进行身份验证，安全性较高。身份验证数量的增加会更频繁地锁定容器，从而在不使用设备时提供数据安全性。

设置	设置的查找位置	建议设置	行为影响
会话超时	Citrix Gateway	4320	仅当要求进行联机身份验证时，用户输入其 Secure Hub 凭据 - 每 3 天一次。
强制超时	Citrix Gateway	无值	如果存在任何活动，则将延长会话。
最长脱机期限	MDX 策略	71	要求每 3 天刷新一次策略。在会话超时之前，允许刷新时间存在小时级差异。
后台服务票据过期日期	MDX 策略	168 小时	STA 超时，允许在没有 Citrix Gateway 会话令牌的情况下进行长时间会话。对于 Secure Mail，使 STA 超时时间长于会话超时时间可避免邮件通知在不提示用户的情况下停止。
要求 Micro VPN 会话	MDX 策略	关	提供有效的网络连接和 Citrix Gateway 会话以使用应用程序。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要求 Micro VPN 会话宽限期	MDX 策略	0	无宽限期（如果启用了“要求 Micro VPN 会话”）。
应用程序通行码	MDX 策略	开	需要应用程序的通行码。
使用通行码加密机密	Endpoint Management 客户端属性	false	不需要使用用户熵来加密保管库。
启用 Citrix PIN 身份验证	Endpoint Management 客户端属性	true	启用 Citrix PIN 以实现简化的身份验证体验。
PIN 强度要求	Endpoint Management 客户端属性	中	强制执行中等密码复杂性规则。
PIN 类型	Endpoint Management 客户端属性	数字	PIN 是一个数字序列。
启用密码缓存	Endpoint Management 客户端属性	true	用户 PIN 缓存和保护 Active Directory 密码。
不活动计时器	Endpoint Management 客户端属性	30	如果在此时间段内用户未使用 MDX 应用程序或 Secure Hub，则提示进行脱机身份验证。
启用 Touch ID 身份验证	Endpoint Management 客户端属性	true	在 iOS 中对脱机身份验证用例启用 Touch ID。

高安全性

此配置提供基本级别的安全性，对用户来说最方便。

设置	设置的查找位置	建议设置	行为影响

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

会话超时	Citrix Gateway	10080	仅当要求进行联机身份验证时，用户输入其 Secure Hub 凭据 - 每 7 天一次
强制超时	Citrix Gateway	无值	如果存在任何活动，则将延长会话。
最长脱机期限	MDX 策略	167	要求每周（每 7 天）刷新一次策略。在会话超时之前，允许刷新时间存在小时级差异。
后台服务票据过期日期	MDX 策略	240	STA 超时，允许在没有 Citrix Gateway 会话令牌的情况下进行长时间会话。对于 Secure Mail，使 STA 超时时间长于会话超时时间可避免邮件通知停止。在这种情况下，如果用户在会话过期之前未打开应用程序，Secure Mail 不会提示用户。
要求 Micro VPN 会话	MDX 策略	关	提供有效的网络连接和 Citrix Gateway 会话以使用应用程序。
要求 Micro VPN 会话宽限期	MDX 策略	0	无宽限期（如果启用了“要求 Micro VPN 会话”）。
应用程序通行码	MDX 策略	开	需要应用程序的通行码。
使用通行码加密机密	Endpoint Management 客户端属性	false	不需要使用用户熵来加密保管库。
启用 Citrix PIN 身份验证	Endpoint Management 客户端属性	true	启用 Citrix PIN 以实现简化的身份验证体验。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

PIN 强度要求	Endpoint Management 客户端属性	低	无密码复杂性要求
PIN 类型	Endpoint Management 客户端属性	数字	PIN 是一个数字序列。
启用密码缓存	Endpoint Management 客户端属性	true	用户 PIN 缓存和保护 Active Directory 密码。
不活动计时器	Endpoint Management 客户端属性	90	如果在此时间段内用户未使用 MDX 应用程序或 Secure Hub，则提示进行脱机身份验证。
启用 Touch ID 身份验证	Endpoint Management 客户端属性	true	在 iOS 中对脱机身份验证用例启用 Touch ID。

使用递升式身份验证

某些应用程序可能需要增强的身份验证。例如，令牌或主动会话超时等辅助身份验证因素。您可以通过 MDX 策略控制此身份验证方法。此方法还需要一个单独的虚拟服务器来控制身份验证方法（在相同或不同的 Citrix Gateway 设备上）。

设置	设置的查找位置	建议设置	行为影响
备用 Citrix Gateway	MDX 策略	需要辅助 Citrix Gateway 设备的 FQDN 和端口。	允许通过辅助 Citrix Gateway 设备身份验证和会话策略控制增强的身份验证。

如果用户打开使用备用 Citrix Gateway 的应用程序，则所有其他应用程序都使用该 Citrix Gateway 实例与内部网络进行通信。与具有增强安全性的 Citrix Gateway 实例的会话超时后，会话将仅切换回安全性较低的 Citrix Gateway 实例。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

要求使用 **Micro VPN** 会话

对于某些应用程序，例如 Secure Web，您可以确保用户仅在具有经过身份验证的会话时才运行应用程序。此策略强制执行该方式，并允许有一个宽限期以便用户可以完成其工作。

设置	设置的查找位置	建议设置	行为影响
要求 Micro VPN 会话	MDX 策略	开	确保设备处于联机状态并且具有有效的身份验证令牌。
要求 Micro VPN 会话宽限期	MDX 策略	15	允许在用户无法继续使用应用程序之前有 15 分钟的宽限期

服务器属性

June 9, 2022

服务器属性是适用于跨整个 Endpoint Management 实例的操作、用户和设备的全局属性。Citrix 建议评估您的环境中设置的本文中介绍的服务器属性。更改其他服务器属性之前，请务必咨询 Citrix。

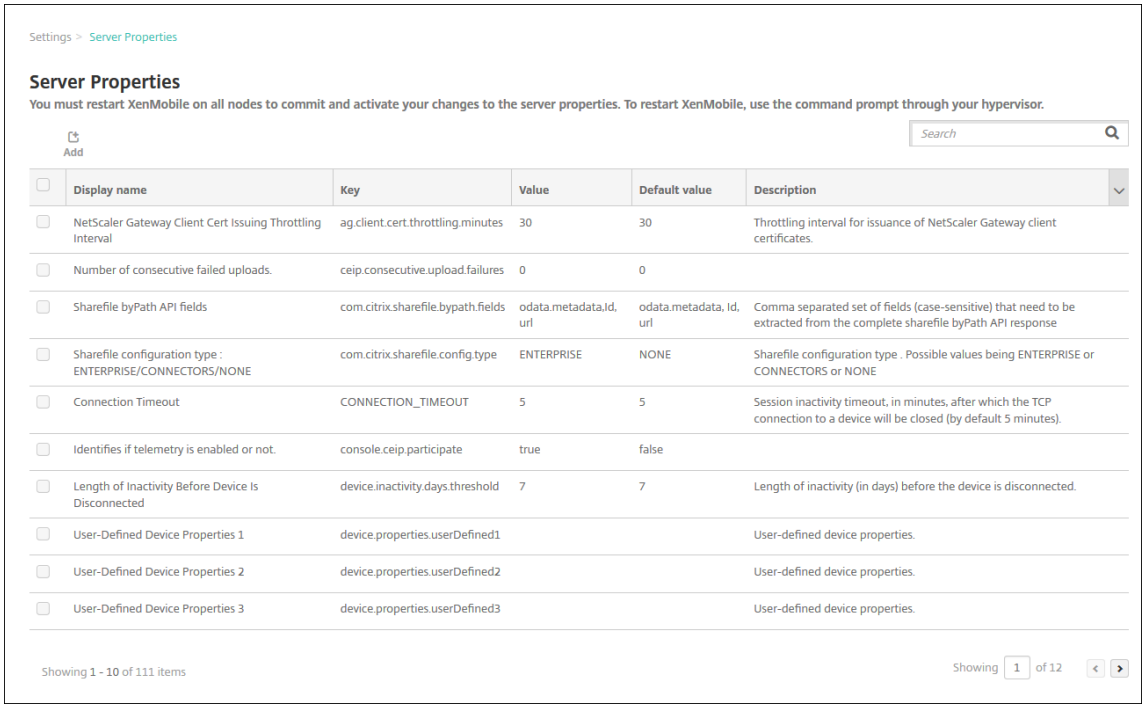
要更新服务器属性，请转至设置 **>** 服务器属性。

添加、编辑或删除服务器属性

在 Endpoint Management 中，可以将属性应用到服务器。

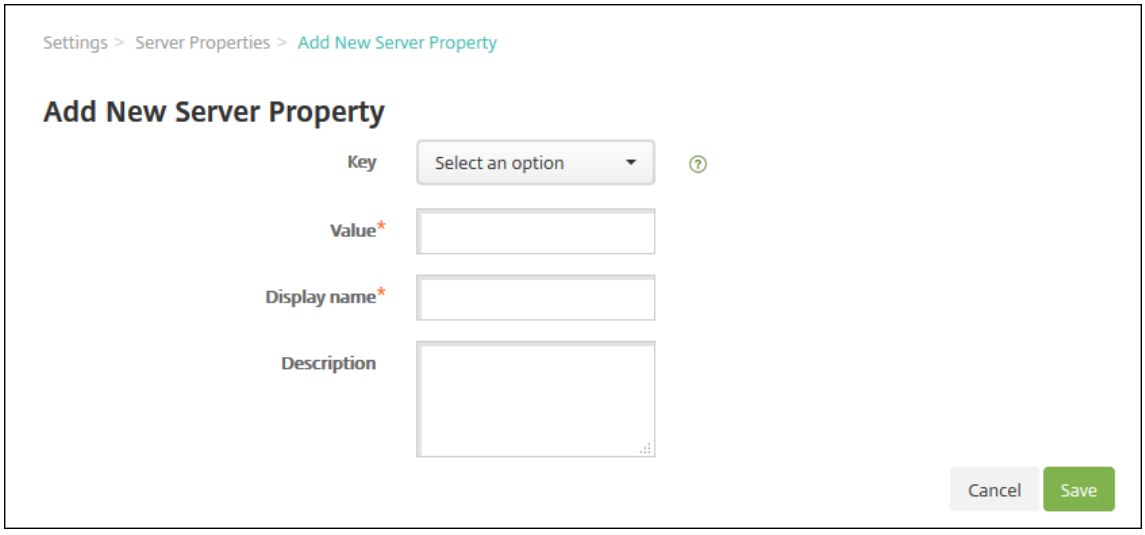
1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击服务器属性。此时将显示服务器属性页面。可以从此页面添加、编辑和删除服务器属性。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



添加服务器属性

1. 单击添加。此时将显示添加新服务器属性页面。



2. 配置以下设置：

   - 密钥：在列表中，选择合适的密钥。键区分大小写。如果要编辑属性值或申请特殊密钥，请联系 Citrix 支持。
   - 值：根据选择的键输入一个值。
   - 显示名称：输入新属性值显示在服务器属性表中的名称。
   - 说明：（可选）键入新服务器属性的说明。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

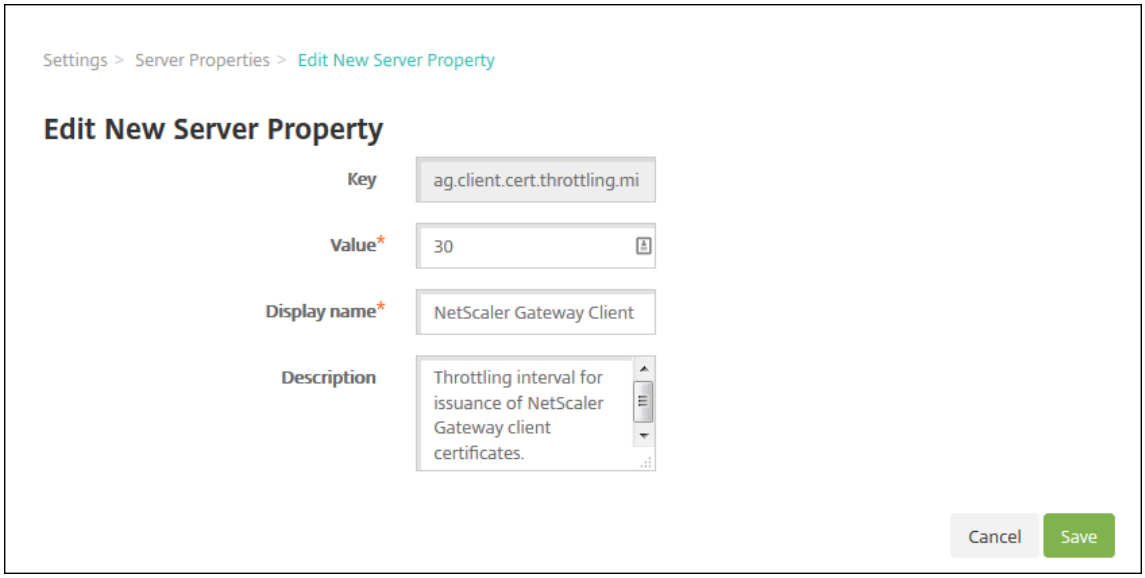
3. 单击保存。

编辑服务器属性

1. 在服务器属性表中，选择要编辑的服务器属性。

   选中服务器属性旁边的复选框时，选项菜单将显示在服务器属性列表上方。单击列表中的其他任意位置可在列表右侧打开选项菜单。

2. 单击编辑。此时将显示编辑新服务器属性页面。



3. 适当更改以下信息：

   - 键：无法更改此字段。
   - 值：属性值。
   - 显示名称：属性名称。
   - 说明：属性说明。

4. 单击保存以保存您所做更改，或单击取消保留属性不变。

删除服务器属性

1. 在“ 服务器属性”表中，选择要删除的服务器属性。
2. 单击删除。此时将显示确认对话框。再次单击删除。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

服务器属性定义

访问托管 **Google Play** 应用商店中的所有应用程序

- 如果设置为 **true**，Endpoint Management 将使公共 Google Play 应用商店中的所有应用程序可从托管 Google Play 应用商店访问。您可以使用 限制设备策略 来控制对这些应用程序的访问。默认值为 **false**。

始终添加设备

- 如果设置为 **true**，Endpoint Management 会将设备添加到 Endpoint Management 控制台，即使注册失败亦如此。因此，您可以查看尝试注册了哪些设备。默认值为 **false**。

AG 客户端证书颁发限制时间间隔

- 两次生成证书之间的宽限期。此时间间隔阻止 Endpoint Management 在短时间内为某个设备生成多个证书。Citrix 建议不要更改此值。默认值为 **30** 分钟。

允许删除在指定时间段内被标记为非活动状态的设备

- 如果为 **true**，则在指定时间（以天为单位）内处于不活动状态的设备将从 Endpoint Management 中删除并删除。活动期限由设备自动从 **CEM** 服务器中删除之前可以处于非活动状态的时间长度属性进行设置。默认值为 **true**。要更改此属性的值，请咨询您的 Citrix 代表。

Audit Logger（审核记录器）

- 如果设置为 **False**，则不记录用户界面 (UI) 事件。默认值为 **False**。

阻止注册已获得 **Root** 权限的 **Android** 设备和已越狱的 **iOS** 设备

此属性设置为真时，Endpoint Management 将阻止注册已获得 Root 权限的 Android 设备和已越狱的 iOS 设备。对于所有安全级别，建议的设置为 **true**。默认值为 **true**。

cdn.s3.retry.interval 和 **cdn.s3.max.retry**

`cdn.s3.retry.interval` 和 `cdn.s3.max.retry` 服务器属性协同工作，以设置每次 macOS PKG 文件上传的最长时间限制。默认情况下，Endpoint Management 将文件上传时间限制为 100 秒。如果文件上传超过该限制，上传将失败。要更改默认值，请按如下方式配置 `cdn.s3.retry.interval` 和 `cdn.s3.max.retry` 键：

- `cdn.s3.retry.interval`. 允许您定义 Endpoint Management 验证文件上传是否成功完成的时间间隔（以毫秒为单位）。默认值为 `10000`。
- `cdn.s3.max.retry`. 允许您定义验证重试的最大次数，之后上传失败。默认值为 `10`。

两个密钥一起工作以限制文件上传时间。默认情况下，时间限制为 100 秒（10000*10 毫秒）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

证书续订 **(**秒**)**

- Endpoint Management 在证书过期之前开始续订证书的秒数。例如，当证书在 12 月 30 日到期且此属性设置为 30 天时。如果设备在 12 月 1 日至 12 月 30 日之间连接，Endpoint Management 将尝试续订证书。默认值为 **2592000** 秒（30 天）。

连接超时

- 会话不活动超时（分钟），在这段时间之后 Endpoint Management 关闭与设备的 TCP 连接。会话保持打开状态。适用于 Android 设备。默认值为 **5** 分钟。

默认部署渠道

- 确定 Endpoint Management 将资源部署到设备的方式：在用户级别 (**DEFAULT_TO_USER**) 或设备级别。默认值为 **DEFAULT_TO_DEVICE**。

弃用移动服务提供商

- 不支持用于查询 Blackberry 和其他 Exchange ActiveSync 设备的移动服务提供商界面。启用后，移动服务提供商界面在控制台中隐藏。默认值为 **true**。

设备标记

- 如果将 `enable.device.tagging` 设置为 **true**，Endpoint Management 会自动按设备类型为设备添加标签。可以使用设备标记部署策略和应用程序，或者配置交付组。Endpoint Management 为设备应用以下标记：
  - BYOD 标记
    - iOS 用户注册
    - Android Enterprise 工作配置文件
  - 公司标记
    - Android Enterprise 完全托管企业设备
    - 批量注册
      - Apple 商务管理设备
      - Apple 校园教务管理设备
      - Windows AutoPilot 设备
      - Android Enterprise 批量注册

禁用主机名验证

- 默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。当主机名验证失败时，服务器日志会包含以下错误：“无法连接到批量购买服务器：主机名 ‘192.0.2.0’ 与对等方提供的证书主题不匹配”。如果主机

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

名验证中断了您的部署，请将此属性更改为 **true**。默认值为 **false**。

禁用 **SSL** 服务器验证

- 如果为 **True**，则在满足所有以下条件时禁用 SSL 服务器证书验证：
  - 您在 Endpoint Management 上启用了基于证书的身份验证
  - Microsoft CA 服务器是证书颁发者
  - 其根 Endpoint Management 不信任的内部 CA 已为您的证书签名。

  默认值为 **True**。

启用崩溃报告

- 如果设置为 **true**，Citrix 将收集崩溃报告和诊断信息以帮助对 Secure Hub for iOS 和 Secure Hub for Android 相关问题进行故障排除。如果设置为 **false**，则不收集任何数据。默认值为 **true**。

启用/禁用休眠统计信息日志记录以进行诊断

- 如果设置为 **True**，则启用休眠统计日志记录，以协助对应用程序性能问题进行故障排除。Hibernate 是用于 Endpoint Management 连接到 Microsoft SQL Server 的组件。默认情况下，此日志记录功能已禁用，因为它会影响应用程序的性能。只应在短时间内启用日志记录功能，以避免生成巨大的日志文件。Endpoint Management 将此日志写入 /opt/sas/logs/hibernate_stats.log。默认值为 **False**。

启用 **macOS OTAE**

- 如果设置为 **false**，则阻止在 macOS 设备上使用注册链接，这意味着 macOS 用户只能使用注册邀请进行注册。默认值为 **true**。

启用通知触发器

- 启用或禁用 Secure Hub 客户端通知. 值 **true** 表示启用通知。默认值为 **true**。

完全拉取 **ActiveSync** 允许和拒绝的用户

- Endpoint Management 拉取 ActiveSync 允许和拒绝的用户的完整列表（基准）的时间间隔（秒）。默认值为 **28800** 秒。

确定是否已启用遥测

- 确定是否已启用遥测。遥测又称为客户体验改善计划 (CEIP)。您可以在安装或升级 Endpoint Management 时选择加入 CEIP。如果 Endpoint Management 有 15 次连续失败的上载，则会禁用遥测。默认值为 **false**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

不活动超时 **(**分钟**)**

- Endpoint Management 注销非活动用户的分钟数。用户必须使用 Endpoint Management 公共 API 才能访问 Endpoint Management 控制台或任何第三方应用程序。超时值为 **0** 表示非活动用户保持登录状态。对于访问该 API 的第三方应用程序，通常有必要保持登录状态。默认值为 **5**。
- 如果 **Web** 服务超时类型服务器属性为 **INACTIVITY_TIMEOUT**：此属性定义分钟数，超过此时间后，Endpoint Management 注销执行了以下操作的不活动管理员：
  - 使用适用于 REST 的公共 API 服务访问 Endpoint Management 控制台
  - 使用适用于 REST 的公共 API 服务来访问任何第三方应用程序。超时为 **0** 意味着不活动用户保持登录状态。

include.device.properties.during.search

- 在设备搜索中包括所有设备属性。默认值为关，该设置将搜索范围限制到以下设备属性，以便快速搜索：
  - 序列号
  - IMEI
  - Wi-Fi MAC 地址
  - 蓝牙 MAC 地址
  - Active Sync ID
  - 用户名

  当此属性设置为开时，设备搜索可能需要更长时间。

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- 指定脱机 iOS 或 macOS 设备被视为无法访问之前的天数。当 iOS 或 macOS 设备达到指定的限制时，它们将停止使用 Endpoint Management 进行检查。两个属性的默认值都为 **45** 天。

如有需要，**iOS** 设备管理注册将安装根 **CA**

- 对于所有 Endpoint Management 环境，服务器属性 **ios.mdm.enrollment.installRootCaIfRequired** 设置为 **False**。Endpoint Management 使用公开信任的证书链，因此无需将根 CA 推送到设备。（此属性仅用于本地环境。）

iOS 设备管理注册最后一个步骤延迟

- 在设备注册过程中，此属性的值指定在设备上安装 MDM 配置文件与启动代理之间需等待的时间量。Citrix 建议仅针对网络延迟或速度问题编辑此属性。在这种情况下，请勿将该值设置为超过 5000 毫秒（5 秒）。默认值为 **1000** 毫秒（1 秒）。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

iOS 设备管理身份交付模式

- 指定 Endpoint Management 使用 **SCEP**（出于安全原因而推荐使用）还是 **PKCS12** 向设备分发 MDM 证书。在 PKCS12 模式下，密钥对在服务器上生成，并且不执行任何协商。默认值为 **SCEP**。

iOS 设备管理身份密钥大小

- 定义 MDM 身份、iOS 配置文件服务和 Endpoint Management iOS 代理身份的私钥的大小。默认为 **2048**。

iOS 设备管理身份续订天数

- 指定 Endpoint Management 在证书过期之前开始续订证书的天数。例如：如果证书将于 10 天后过期，并且此属性设置为 **10** 天：当设备在过期之前 9 天连接时，Endpoint Management 会颁发新证书。默认值为 **30** 天。

iOS MDM APNS 私钥密码

- 此属性包含 APNs 密码，Endpoint Management 向 Apple 服务器推送通知需要该密码。

设备断开连接之前不活动的时长

- 指定设备在 Endpoint Management 将其断开连接之前可以保持不活动状态的时长，包括最后一次身份验证。默认值为 **7** 天。

设备在自动从 **CEM** 中删除之前可以处于非活动状态的时间长度

- 设备在自动从 Endpoint Management 中删除之前可以处于非活动状态的时间长度（以天为单位）。最短时间为 **14** 天，默认值为 **30** 天。要使此属性生效，必须将允许删除在指定时间段内标记为不活动的设备服务器属性设置为 **true**。

local.user.account.lockout.time

- 指定用户在超过锁定限制后必须等待的分钟数。支持的值为 0-999。默认值为 **30** 分钟。

local.user.account.lockout.limit

- 指定每个用户连续无效登录尝试的最大次数。支持的值为 0-999。默认值为 **6** 次尝试。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

mac.dep.admin.passwd.rotate

使用此服务器属性，您可以为通过 Apple 部署计划注册的 macOS 设备配置管理员密码轮换间隔。Endpoint Management 会检查是否每天轮换管理员账户的密码。默认情况下，Endpoint Management 每 10,080 分钟（7 天）轮换一次密码。按如下方式配置 `mac.dep.admin.passwd.rotate` 密钥：

- 值：管理员定义
  的 Endpoint Management 轮换密码的时间间隔（以分钟为单位）。键入等于或大于 360（6 小时）的值。Endpoint Management 忽略小于 360 的值，而是每 360 分钟（6 小时）轮换一次密码。
- 显示名称：管理员定义
- 说明：由管理员定义

MAM Only Device Max（仅 MAM 设备最大值）

- 此自定义键限制每个用户可以注册的仅 MAM 设备数。按如下所示配置键。值为 **0** 表示设备注册数不受限制。
- 键 = **number.of.mam.devices.per.user**
- 值 = **5**
- 显示名称 = 仅 **MAM** 设备最大值
- 说明 = 限制每个用户可以注册的 **MAM** 设备数。

MaxNumberOfWorker

- 导入许多批量购买许可证时使用的线程数量。默认值为 **3**。如果需要进一步优化，可以增加线程的数量。但是，线程数量越大会导致 CPU 使用率高。

Citrix Gateway (NetScaler) 单点登录

- 如果设置为 **False**，则在从 Citrix Gateway 到 Endpoint Management 的单点登录期间禁用 Endpoint Management 回调功能。如果 Citrix Gateway 配置包括回调 URL，则 Endpoint Management 使用回调功能验证 Citrix Gateway 会话 ID。默认值为 **False**。

连续失败的上载次数

- 显示客户体验改善计划 (CEIP) 上载过程中连续失败的次数。Endpoint Management 会在上载失败时增加该值。上载失败 15 次后，Endpoint Management 将禁用 CEIP（又称为遥测）。有关详细信息，请参阅服务器属性确定是否已启用遥测。Endpoint Management 在上载成功时将该值重置为 **0**。

每个设备的用户数

- 能够在 MDM 中注册相同设备的用户的最大数量。值 **0** 表示能够注册相同设备的用户数量不受限制。默认值为 **0**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

optional.user.identity.attributes

- 此服务器属性允许您自定义可选 Active Directory 用户属性。

  创建自定义密钥，然后在值字段中编辑用户属性，以定义 Endpoint Management 创建用户帐户时可以访问的属性。有关详细信息，请参阅 自定义用户属性。

  - 键：自定义键
  - 键：**optional.user.identity.attributes**
  - 值：**commonName**、**firstName**、**lastName**、**displayName**、**streetAddress**、**city**、**state**、**country**、**workPhone**、**homePhone**、**mobilePhone**、**company**、**department**、**description**、**employeeID**、**faxNumber**、**initials**、**ipPhone**、**manager**、**homePostalAddress**、**otherMobile**、**pager**、**physicalDeliveryOfficeName**、**postalCode**、**postOfficeBox**、**title**、**organization**、**preferredLanguage**
  - 显示名称：**optional.user.identity.attributes**
  - 说明：可选 **Active Directory** 用户属性

macOS 和 **iOS/iPadOS** 注册配置文件的组织名称

- 键入的 `apple.mdm.enrollment.profile.organization.name` 的值与提供注册配置文件的组织的名称相对应。当用户将其设备注册到 Endpoint Management 时，将显示名称。显示的默认名称为 **Citrix Workspace**。

提取允许和被拒绝的用户的增量更改

- Endpoint Management 在运行 PowerShell 命令以获取 ActiveSync 设备的增量时等待来自域的响应的秒数。默认值为 **60** 秒。

从 **Microsoft** 证书服务器读取超时

- Endpoint Management 在执行读取时等待来自证书服务器的响应的秒数。如果证书服务器速度缓慢，并且具有大量流量，您可以将此值增加到 60 秒或更长时间。在 120 秒后不响应的证书服务器需要维护。默认值为 **15000** 毫秒（15 秒）。

REST Web 服务

- 启用 REST Web 服务。默认值为 **true**。

以指定大小的块检索设备信息

- 此值在内部用于设备导出期间的多线程处理。如果该值较高，则单个线程解析较多的设备。如果该值较低，则有较多的线程提取设备。降低该值可能会提高导出和设备列表提取的性能，但可能会减少可用内存。默认值为 **1000**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

shp.console.enable

- 如果设置为 **False**，则阻止访问自助服务门户。导航到端口 4443 上的门户的用户会收到 “拒绝被访问” 消息。如果设置为 **true**，则提供通过端口 443 访问自助服务门户的权限。

  默认值为 **False**。

enable.new.shp

- 如果设置为 **False**，则阻止用户从自助服务门户启用其设备。如果设置为 **True**，用户可以从自助服务门户启用其设备。

  BitLocker 恢复密钥功能要求您将此属性设置为 **False**，并将 `shp.console.enable` 属性设置为 **True**。

  默认值为 **False**。

会话日志清理时间 **(**天**)**

- Endpoint Management 保留会话日志的天数。默认值为 **7**。

Content Collaboration 配置类型

- 指定 Citrix Files 存储类型。**ENTERPRISE** 表示启用 Citrix Files Enterprise 模式。**CONNECTORS** 表示仅提供对通过 Endpoint Management 控制台创建的存储区域连接器的访问权限。默认值为 **NONE**，此时显示配置 **> Citrix Files** 屏幕的初始视图，在该屏幕中可以选择 “ShareFile Enterprise” 与 “Citrix Files 连接器”。默认值为 **NONE**。

静态超时（分钟）

- 如果 **Web** 服务超时类型服务器属性为 **STATIC_TIMEOUT**：此属性定义分钟数，超过此时间后，Endpoint Management 注销执行了以下操作的管理员：
  - 使用适用于 REST 的公共 API 服务访问 Endpoint Management 控制台。
  - 使用适用于 REST 的公共 API 服务访问任何第三方应用程序。

  默认值为 **60**。

触发代理消息抑制

- 启用或禁用 Secure Hub 客户端消息传递。值 **false** 表示启用消息传递。默认值为 **true**。

触发代理声音抑制

- 启用或禁用 Secure Hub 客户端声音。值 **false** 表示启用声音。默认值为 **true**。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Android 设备的未经身份验证的应用程序下载

- 如果设置为 **True**，则可以将自托管应用程序下载到运行 Android Enterprise 的 Android 设备。如果启用了在 Google Play 应用商店中静态提供下载 URL 的 Android Enterprise 选项，Endpoint Management 将需要此属性。在这种情况下，下载 URL 不能包括带有身份验证令牌的一次性票据（由 **XAM** 一次性票据服务器属性定义）。默认值为 **False**。

Windows 设备的未经身份验证的应用程序下载

- 仅适用于不验证一次性票证的较旧 Secure Hub 版本。如果设置为 **False**，则可以将未经身份验证的应用程序从 Endpoint Management 下载到 Windows 设备。默认值为 **False**。

使用 **ActiveSync ID** 对 **ActiveSync** 擦除设备执行操作

- 如果为 **true**，适用于 Exchange ActiveSync 的 Endpoint Management 连接器将使用 ActiveSync 标识符作为 **asWipeDevice** 方法的参数。默认值为 **false**。

仅限来自 **Exchange** 的用户

- 如果设置为 **true**，则禁用针对 ActiveSync Exchange 用户的用户身份验证。默认值为 **false**。

批量购买基准间隔

- Endpoint Management 从 Apple 重新导入批量购买许可证的最小时间间隔。刷新许可证信息可确保 Endpoint Management 反映所有更改，例如，手动从批量购买中删除导入的应用程序时。默认情况下，Endpoint Management 按每 **1440** 分钟的最小时间间隔为基准刷新批量购买许可证。
  - 如果您安装了许多批量购买许可证（例如，超过 50000）：Citrix 建议增加基准时间间隔以降低导入许可证的频率和开销。
  - 如果您预计 Apple 会频繁更改批量购买许可证：Citrix 建议降低该值以使更改及时更新到 Endpoint Management 中。
  - 两个基准之间的最小时间间隔为 60 分钟。此外，Endpoint Management 每隔 60 分钟执行一次增量导入，以捕获自上次导入后所做的更改。因此，如果批量购买基准时间间隔为 60 分钟，则基准之间的时间间隔可能会最长延迟 119 分钟。

Web 服务超时类型

- 指定如何使从公共 API 中获取的身份验证令牌过期。
  - 如果设置为 **STATIC_TIMEOUT**： Endpoint Management 会将令牌视为已过期，具体取决于服务器属性静态超时 **(**分钟**)** 的值。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 如果设置为 **INACTIVITY_TIMEOUT**：Endpoint Management 会将令牌视为已过期，具体取决于服务器属性不活动超时 **(**分钟**)** 的值。默认值为 **STATIC_TIMEOUT**。

Windows Tablet MDM 证书延长的有效期 **(5** 年**)**

- MDM 为 Windows Tablet 颁发的设备证书的有效期。在设备管理过程中，设备使用设备证书向 MDM 服务器进行身份验证。如果设置为 **true**，有效期为五年。如果设置为 **false**，有效期为两年。默认值为 **true**。

Windows WNS 通道 **-** 续订之前的天数

- ChannelURI 的续订频率。默认值为 **10** 天。

Windows WNS 检测信号时间间隔

- Endpoint Management 在以每五分钟三次的速率连接到某个设备之后再次连接到该设备之前等待的时间。默认值为 **6** 小时。

XAM 一次性票据

- 一次性身份验证令牌 (OTT) 对下载应用程序有效的毫秒数。此属性与 **Android** 设备的未经身份验证的应用程序下载属性和 **Windows** 设备的未经身份验证的应用程序下载属性一起使用。这些属性指定是否允许进行未经身份验证的应用程序下载。默认值为 **3600000**。

Endpoint Management MDM 自助服务门户控制台的最长不活动时间间隔 **(**分钟**)**

- 此属性名称反映了较旧的 Endpoint Management 版本。此属性控制 Endpoint Management 控制台的最大不活动时间间隔。该时间间隔是 Endpoint Management 从 Endpoint Management 控制台注销不活动用户之前的分钟数。超时为 **0** 表示非活动用户保持登录状态。默认值为 **30**。

设备和应用程序策略

July 24, 2023

通过 Endpoint Management 设备和应用程序策略，可以在多种因素之间实现最佳平衡，例如：

- 企业安全性
- 公司数据和资产保护
- 用户隐私
- 高效、积极的用户体验

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

这些因素之间的最佳平衡点可能有所差别。例如，监管比较严格的组织（例如金融组织）要求采取比其他行业（例如教育和零售行业）更严格的安全控制措施，而后者主要考虑的是如何提高用户工作效率。

您可以根据用户的身份、设备、位置和连接类型集中控制和配置策略来限制对公司内容的恶意使用。如果设备丢失或被盗，您可以远程禁用、锁定或擦除业务应用程序和数据。综合上述因素，我们可以开发一种解决方案，不仅可以提高员工满意度和工作效率，同时还能确保安全性和管理控制。

本文主要介绍与安全性有关的多个设备和应用程序策略。

解决安全风险的策略

Endpoint Management 设备和应用程序策略解决可能会带来安全风险的多种情况，例如在以下情况下：

- 用户尝试从不可信设备和不可预测的位置访问应用程序和数据。
- 用户在设备之间传递数据
- 未经授权的用户尝试访问数据
- 已离开公司的用户使用自己的设备 (BYOD)。
- 用户错放设备
- 用户必须始终安全地访问网络
- 用户使自己的设备处于托管状态且您必须将工作数据与个人数据区分开
- 设备处于空闲状态并需要再次验证用户凭据。
- 用户将敏感内容复制并粘贴到不受保护的电子邮件系统。
- 用户在保存了个人帐户和公司帐户的设备上收到包含敏感数据的电子邮件附件或 Web 链接。

保护公司数据时，这些情况与两个主要考虑因素相关，即数据所处的状态：

- 静态
- 传输中

Endpoint Management 如何保护静态数据

存储在移动设备上的数据称为静态数据。Endpoint Management 使用 iOS 和 Android 平台提供的设备加密。Endpoint Management 通过 Citrix MAM SDK 提供的合规性检查等功能补充基于平台的加密。

通过 Endpoint Management 中的移动应用程序管理 (MAM) 功能可以对 Citrix 移动生产力应用程序、启用了 MDX 的应用程序及其关联数据进行完整的管理、安全保护和控制。

移动应用程序 SDK 通过使用 Citrix MDX 应用程序容器技术启用 Endpoint Management 部署的应用程序。容器技术将企业应用程序和数据与个人应用程序和用户设备上的数据分离开来。数据分离允许您通过基于策略的综合控制来保护任何自定义开发的、第三方或 BYO 移动应用程序的安全。

Endpoint Management 还包括应用级加密。Endpoint Management 单独加密存储在任何启用了 MDX 的应用程序中的数据，而无需设备通行码，也无需管理设备即可实施策略。

- 在 iOS 设备上，Endpoint Management 使用功能强大的经 FIPS 验证的加密服务和库，例如钥匙串。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- OpenSSL 为各种设备平台提供经 FIPS 验证的模块。OpenSSL 进一步保护动态数据以及管理和注册设备所需的证书。
- Endpoint Management 使用 MAM SDK 共享文件库 API 在具有相同钥匙串访问组的应用程序之间共享托管内容。例如，您可以通过注册的应用程序共享用户证书，以便应用程序可以从安全保管库中获取证书。
- Endpoint Management 使用平台提供的设备加密。
- Endpoint Management MAM 控制在应用程序级别执行合规性检查，以验证设备加密是否在每次应用程序启动时启用。

Endpoint Management 如何保护传输中的数据

在用户的移动设备与您的内部网络之间移动的数据称为传输中的数据。MDX 应用程序容器技术实现了通过 Citrix Gateway 对内部网络进行应用程序特定的 VPN 访问。

假设存在员工希望通过移动设备访问驻留在安全企业网络中的以下资源的情况：

- 公司电子邮件服务器
- 公司 Intranet 上托管的启用了 SSL 的 Web 应用程序
- 存储在文件服务器或 Microsoft SharePoint 上的文档

MDX 支持从移动设备通过应用程序特定的 Micro VPN 访问所有这些企业资源。每个设备都有自己的专用 Micro VPN 通道。

Micro VPN 功能不需要设备范围的 VPN（可能会危及不可信移动设备上的安全）。因此，内部网络不会面临可能影响整个公司系统的恶意软件或攻击。公司移动应用程序和个人移动应用程序能够在一个设备上共存。

要提供更高级别的安全性，可以使用 “备用 Citrix Gateway” 策略配置启用了 MDX 的应用程序。该策略用于身份验证和与应用程序的 Micro VPN 会话。您可以将备用 Citrix Gateway 与 “要求 Micro VPN 会话” 策略结合使用，以强制应用程序向特定网关重新进行身份验证。此类网关通常具有不同的（具有更高保障）身份验证要求和流量管理策略。

除了安全功能外，Micro VPN 功能还提供数据优化技术，包括压缩算法。压缩算法可确保：

- 仅传输最少的数据
- 传输在最快的时间内完成。速度改进了用户体验，这是移动设备采用的关键成功因素。

请定期重新评估设备策略，例如在以下情况下：

- 由于发布了设备操作系统更新，新版本的 Endpoint Management 包括新的或更新的策略时。
- 添加设备类型时：

  尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。因此，您可能会发现 iOS、Android 和 Windows 设备之间的差异，甚至不同制造商提供的 Android 设备设备之间的差异。
- 使 Endpoint Management 操作与企业或行业变化（例如，新公司安全策略或合规性规章）保持同步。
- 新版本的 MAM SDK 包括新的或更新的策略时
- 添加或更新应用程序时
- 由于新应用程序或新要求而需要为用户集成新工作流

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

应用程序策略和用例场景

虽然您可以选择通过 Secure Hub 提供的应用程序，您可能还希望定义这些应用程序与 Endpoint Management 的交互方式。使用应用程序策略：

- 如果您希望用户在特定时间段过后进行身份验证。
- 如果您希望为用户提供对其信息的脱机访问权限。

以下个部分内容包括一些策略和示例用法。

- 有关您可以使用 MAM SDK 集成到 iOS 和 Android 应用程序中的第三方策略的列表，请参阅 MAM SDK 概述。
- 有关每个平台的所有 MDX 策略的列表，请参阅 MDX 策略概览。

身份验证策略

- 设备通行码

  为什么要使用此策略：启用“设备通行码”策略可强制执行仅当设备上已启用设备通行码时用户才能访问 MDX 应用程序。此功能可确保在设备级别使用 iOS 加密。

  用户示例：启用此策略意味着，用户必须先在其 iOS 设备上设置一个通行码，然后才能访问 MDX 应用程序。

- 应用程序通行码

  为什么要使用此策略：启用“应用程序通行码”策略可让 Secure Hub 提示用户先向托管应用程序进行身份验证，然后才能打开应用程序并访问数据。用户可使用其 Active Directory 密码、Citrix PIN 或 iOS Touch ID 进行身份验证，具体取决于您在 Endpoint Management 控制台中的设置 **>** 客户端属性下配置的设置。可以在“客户端属性”中设置不活动计时器，以便 Secure Hub 不提示用户重新向托管应用程序进行身份验证，直到计时器过期。

  应用程序通行码与设备通行码不同。将设备通行码策略推送到设备后，Secure Hub 会提示用户配置通行码或 PIN。用户必须在打开设备或非活动计时器过期时解锁其设备。有关详细信息，请参阅 Citrix Endpoint Management 中的身份验证。

  用户示例：在设备上打开 Citrix Secure Web 应用程序时，如果不活动期限已过期，用户必须输入其 Citrix PIN，才能浏览 Web 站点。

- 要求 **Micro VPN** 会话

  为什么使用此策略：如果应用程序需要访问 Web 应用程序（Web 服务）才能运行，请启用此策略。然后，Endpoint Management 会提示用户连接到企业网络或在使用应用程序之前具有活动会话。

  用户示例：用户尝试打开启用了“要求 Micro VPN 会话”策略的 MDX 应用程序时：只能在连接到网络后才能使用该应用程序。连接必须使用手机网络或 Wi-Fi 服务。

- 最长脱机期限

  为什么使用此策略：将此策略用作额外的安全选项。该策略可确保在指定时间内脱机运行应用程序的用户必须重新确认应用程序授权并刷新策略。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用户示例：如果您为某个 MDX 应用程序配置“最长脱机期限”，用户可以打开并脱机使用该应用程序，直到脱机计时器期限过期。此时，如果系统提示，用户必须通过手机网络或 Wi-Fi 服务重新连接网络并重新进行身份验证。

其他访问策略

- 应用程序更新宽限期 **(**小时**)**

  为什么要使用此策略：应用程序更新宽限期是指为用户预留的一段时间，到此时间后，用户必须更新应用商店中发布的较新版本的应用程序。在过期时，用户必须更新该应用程序才能访问该应用程序中的数据。设置此值时，请谨记您的移动办公人员的需求，尤其是在国际出差时可能很长一段时间脱机的用户。

  用户示例：加载应用商店中的新版本的 Secure Mail，然后将应用程序更新宽限期设置为 6 小时。然后，Secure Hub 用户在路由到应用商店之前有 6 个小时的时间升级 Secure Mail。

- 活动轮询期限 **(**分钟**)**

  为什么要使用此策略：活动轮询期限是指 Endpoint Management 检查应用程序以确定何时执行安全操作（例如，应用程序锁定和应用程序擦除）的时间间隔。

  用户示例：如果将“活动轮询期限”策略设置为 60 分钟，然后发送应用程序锁定命令，则将在上次轮询后的 60 分钟内发生锁定。

不合规设备行为策略

当设备低于最低合规性要求时，“不合规设备行为”策略将允许您选择要执行的操作。有关信息，请参阅不合规设备行为。

应用程序交互策略

为什么要使用这些策略：可使用应用程序交互策略来控制文档和数据从 MDX 应用程序传输到设备上其他应用程序的流。例如，您可以阻止用户：

- 将数据移动到容器外部的个人应用程序
- 将容器外部的数据粘贴到容器化应用程序中

用户示例：您将应用程序交互策略设置为“限制”，这意味着用户可以将文本从 Secure Mail 复制到 Secure Web。用户无法将该数据复制到容器外部的个人 Safari 或 Chrome 浏览器。此外，用户还可以从 Secure Mail 打开附加的文档到 Citrix Files 或 QuickEdit。用户无法在容器外部的个人文件查看应用程序中打开附加的文档。

应用程序限制策略

为什么要使用这些策略：可使用应用程序限制策略来控制用户可以从打开的 MDX 应用程序访问的功能。这些限制有助于确保该应用程序运行时不会发生任何恶意活动。在 iOS 和 Android 之间应用程序限制策略略有不同。例如，在 iOS 中，您可以在 MDX 应用程序运行时阻止对 iCloud 的访问。在 Android 中，您可以在 MDX 应用程序运行时停止 NFC 的使用。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用户示例：假设您在 iOS 上启用应用程序限制策略以阻止在 MDX 应用程序中使用听写功能。因此，在 MDX 应用程序运行时，用户无法在 iOS 键盘上使用听写功能。因此，用户听写的数据不会传递到不安全的第三方云听写服务。用户在容器外部打开其个人应用程序时，用户仍可使用听写选项进行自己的个人通信。

应用程序网络访问策略

为什么要使用这些策略：可使用应用程序网络访问策略来提供从设备上容器中的 MDX 应用程序访问企业网络内部数据的权限。隧道-Web SSO 选项仅允许对 HTTP 和 HTTPS 流量进行隧道传输。该选项为 HTTP 和 HTTPS 流量以及 PKINIT 身份验证提供单点登录 (SSO)。

用户示例：用户打开启用了通道的 MDX 应用程序时，浏览器将打开 Intranet 站点，而无需用户启动 VPN。该应用程序会自动使用 Micro VPN 技术访问内部站点。

应用程序地理定位和地理围栏策略

为什么要使用这些策略：控制应用程序地理定位和地理围栏功能的策略包括中心点经度、中心点纬度和半径。这些策略包含在 MDX 应用程序中访问特定地理区域的数据的权限。这些策略按纬度和经度坐标半径定义地理区域。如果用户尝试在定义的半径外使用应用程序，则应用程序保持锁定状态，用户无法访问应用程序数据。

用户示例：用户在其办公地点时可以访问合并和收购数据。当用户离开办公地点时，不可访问此敏感数据。

Secure Mail 应用程序策略

- 后台网络服务

  为什么要使用此策略： Secure Mail 中的后台网络服务使用 Secure Ticket Authority (STA)，实际上这是用于通过 Citrix Gateway 进行连接的 SOCKS5 代理。STA 支持长时间连接，与 Micro VPN 相比，可延长电池寿命。因此，STA 非常适用于持续连接的邮件。Citrix 建议您为 Secure Mail 配置这些设置。NetScaler for XenMobile 向导会自动为 Secure Mail 设置 STA。

  用户示例：未启用 STA 且 Android 用户打开 Secure Mail 时，系统提示用户打开 VPN（在设备上保持打开状态）。启用了 STA 且 Android 用户打开 Secure Mail 时，Secure Mail 将无缝连接，而无需任何 VPN。

- 默认同步时间间隔

  为什么要使用此策略：此设置指定用户首次访问 Secure Mail 时同步到 Secure Mail 的电子邮件默认天数。两周的电子邮件同步所需的时间超过三天的电子邮件。要同步的更多数据会延长用户的设置过程。

  用户示例：假设用户首次设置 Secure Mail 时默认同步时间间隔设置为三天。用户可以在其收件箱中看到他们从现在到过去三天收到的任何电子邮件。如果用户想查看三天以前的电子邮件，可以执行搜索。Secure Mail 随即将显示服务器上存储的较早电子邮件。安装 Secure Mail 后，每个用户都可以更改此设置以更好地满足自己的需求。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

设备策略和用例行为

设备策略（有时称为 MDM 策略）确定 Endpoint Management 管理设备的方式。尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。下面列出了其中一些设备策略，并介绍了相应的使用方法。有关所有设备策略的列表，请参阅设备策略下的文章。

- 应用程序清单策略

  为什么要使用此策略：要查看用户安装的应用程序，请将“应用程序清单”策略部署到设备。如果您未部署该策略，则只能查看用户从应用商店安装的应用程序，但看不到个人安装的应用程序。使用“应用程序清单”策略阻止某些应用程序在公司设备上运行。

  用户示例：使用 MDM 托管的设备的用户不能禁用此功能。用户的个人安装的应用程序对 Endpoint Management 管理员可见。

- 应用程序锁定策略

  为什么要使用此策略：对于 Android，应用程序锁定策略允许您将应用程序放置在允许列表或阻止列表中。例如，对于允许运行的应用程序，可以配置展台设备。通常情况下，只将应用程序锁定策略部署到公司拥有的设备，因为它会限制用户可以安装的应用程序。您可以设置覆盖密码以允许用户访问被阻止的应用程序。

  用户示例：假设您部署的应用程序锁定策略阻止“愤怒的小鸟”应用程序。用户可以从 Google Play 安装“愤怒的小鸟”应用程序，但当其打开该应用程序时，将显示一条消息，告知其管理员已阻止该应用程序。

- 连接计划策略

  为什么要使用此策略：“连接计划”策略使 Windows Mobile 设备能够重新连接回 Endpoint Management 以进行 MDM 管理、应用程序推送和策略部署。对于 Android 和 Android Enterprise 设备，请改用 Google Firebase Cloud Messaging (FCM)。FCM 控制与 Endpoint Management 的连接。计划选项如下所示：

  - 从不：手动进行连接。用户必须从其设备上的 Endpoint Management 启动连接。Citrix 建议不要对生产部署使用此选项，因为这会阻止您将安全策略部署到设备。因此，用户不会收到新应用程序或策略。默认情况下，从不选项处于启用状态。
  - 每隔：按照指定间隔进行连接。发送锁定或擦除等安全策略时，Endpoint Management 将在下次设备连接时在设备上处理该策略。
  - 定义计划： Endpoint Management 尝试在网络连接断开后将用户的设备重新连接到 Endpoint Management 服务器。Endpoint Management 通过在您定义的时间范围内定期传输控制数据包来监视连接。

  用户示例：您希望将通行码策略部署到注册的设备。计划策略可确保设备以固定间隔重新连接到服务器以收集新策略。

- 凭据策略

  为什么要使用此策略：通常与网络策略一起使用，凭据策略允许您将证书进行身份验证部署到需要证书身份验证的内部资源中

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用户示例：您部署在设备上配置无线网络的网络策略。Wi-Fi 网络要求使用证书进行身份验证。凭据策略将部署证书，该证书随后存储在操作系统密钥库中。之后，用户在连接到内部资源时可以选择该证书。

- **Exchange** 策略

  为什么要使用此策略：使用 Endpoint Management 时，您有两种方式传递 Microsoft Exchange ActiveSync 电子邮件。

  - **Secure Mail** 应用程序：使用从公共应用商店或应用商店分发的 Secure Mail 应用程序传递电子邮件。
  - 本机电子邮件应用程序：为设备上的本机电子邮件客户端启用 ActiveSync 电子邮件。可以使用宏提取其 Active Directory 属性中的用户数据进行填充，例如，提取 `${ user.username }` 中的数据填充用户名，提取 `${ user.domain }` 中的数据填充用户域。

  用户示例：当您推送 Exchange 策略时，将向设备发送 Exchange Server 详细信息。Secure Hub 随后提示用户进行身份验证并且其电子邮件开始同步。

- 定位策略

  为什么要使用此策略：如果已在设备上为 Secure Hub 启用了 GPS，您可以通过定位策略在地图上对设备进行地理定位。部署此策略并随后从 Endpoint Management 发送定位命令后，设备将返回位置坐标。

  用户示例：部署了定位策略且在设备上启用了 GPS 后，如果用户错放了设备，他们可以登录 Endpoint Management 自助服务门户，然后选择定位选项，可在地图上查看其设备位置。用户选择是否允许 Secure Hub 使用定位服务。当用户自己注册设备时，您无法强制使用定位服务。使用此策略的另一个注意事项是对电池寿命的影响。

- 通行码策略

  为什么要使用此策略：通行码策略允许您在托管设备上强制执行 PIN 代码或密码。此通行码策略允许您在设备上设置通行码的复杂性和超时。

  用户示例：将通行码策略部署到托管设备时，Secure Hub 会提示用户配置通行码或 PIN。通行码或 PIN 允许用户在启动期间或非活动计时器过期时访问其设备。

- 配置文件删除策略

  为什么要使用此策略：假设您将某个策略部署到一组用户，以后必须从其中一部分用户删除该策略。可以通过创建“配置文件删除”策略来删除所选用户的策略。然后，使用部署规则将“配置文件删除”策略仅部署到指定的用户。

  用户示例：将配置文件删除策略部署到用户设备时，用户可能不会发现所做的更改。例如，如果“配置文件删除”策略删除了禁用设备相机的限制，用户不知道该更改。当所做的更改影响用户体验时，请考虑让用户了解。

- 限制策略

  为什么要使用此策略：限制策略允许您使用许多选项来锁定和控制托管设备上的特性和功能。可以为受支持的设备启用数百个限制选项。例如，您可以：禁用设备上的相机或麦克风、强制执行漫游规则以及强制访问第三方服务（例如应用商店）。

  用户示例：如果您将限制部署到 iOS 设备，用户可能无法访问 iCloud 或 Apple App Store。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 条款和条件策略

  为什么要使用此策略：可能有必要向用户告知托管其设备涉及的法律法规。此外，您可能希望确保用户知道向设备推送公司数据时的安全风险。您可以通过“条款和条件”文档在用户注册之前发布规则和声明。

  用户示例：用户将在注册过程中看到条款和条件信息。如果他们拒绝接受所列条件，则注册过程将结束，他们将无法访问公司数据。您可以生成报告以提供给 HR/法律/合规团队，报告中显示接受或拒绝这些条款的用户。

- **VPN** 策略

  为什么要使用此策略：使用 VPN 策略，可通过使用较旧 VPN 网关技术访问后端系统。该策略支持多个 VPN 提供商，包括 Cisco AnyConnect、Juniper 和 Citrix VPN。此外，也可以将此策略链接到 CA 并按需启用 VPN（如果 VPN 网关支持此选项）。

  用户示例：启用 VPN 策略后，当用户访问内部域时，用户的设备将打开 VPN 连接。

- **Web** 剪辑策略

  为什么要使用此策略：如果您想要向设备推送可直接打开 Web 站点的图标，可使用 Web 剪辑策略。Web 剪辑包含指向 Web 站点的链接，并可以包括自定义图标。在设备上，Web 剪辑类似应用程序图标。

  用户示例：用户可以单击 Web 剪辑图标打开 Internet 站点以获取所需服务的访问权限。使用 Web 链接比在浏览器中键入链接地址更方便。

- 网络策略

  为什么要使用此策略：网络策略允许您将 Wi-Fi 网络详细信息（例如 SSID、身份验证数据和配置数据）部署到受管设备。

  用户示例：在部署网络策略后，设备将自动连接到 Wi-Fi 网络并对用户进行身份验证，以便用户可访问此网络。

- **Endpoint Management** 应用商店策略

  为什么要使用此策略：该应用商店是一个统一的应用商店，管理员可以在此发布其用户所需的所有公司应用程序和数据资源。管理员可以添加：

  - Web 应用程序、SaaS 应用程序和启用了 MAM SDK 的应用程序或 MDX 封装的应用程序
  - Citrix 移动生产力应用程序
  - 本机移动应用程序，例如.ipa 或.apk 文件
  - Apple App Store 或 Google Play 应用程序
  - Web 链接
  - 使用 Citrix StoreFront 发布的 Citrix Virtual Apps

  用户示例：用户将其设备注册到 Endpoint Management 后，他们将通过 Citrix Secure Hub 应用程序访问应用商店，如果使用 Citrix Workspace，则通过 Workspace 访问应用商店。然后，用户可以查看所有可用的企业应用程序和服务。用户可以在应用商店中单击某个应用程序以进行安装、访问数据、对应用程序进行评分和评论以及下载应用程序更新。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

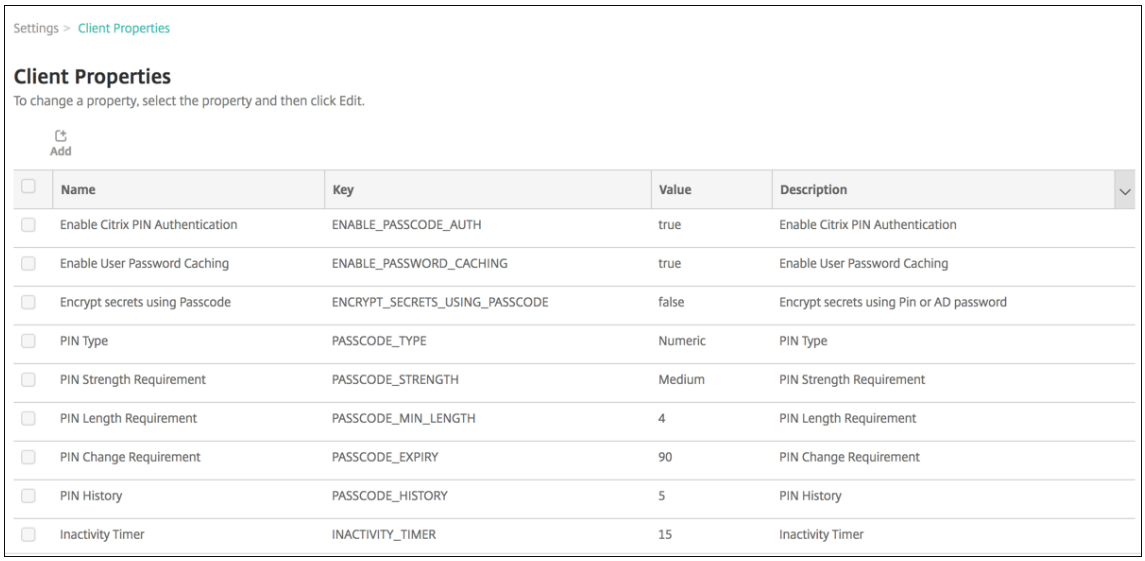
客户端属性

March 16, 2022

客户端属性包含用户设备上直接提供给 Secure Hub 的信息。可以使用这些属性配置高级设置，如 Citrix PIN。从 Citrix 支持获取客户端属性。

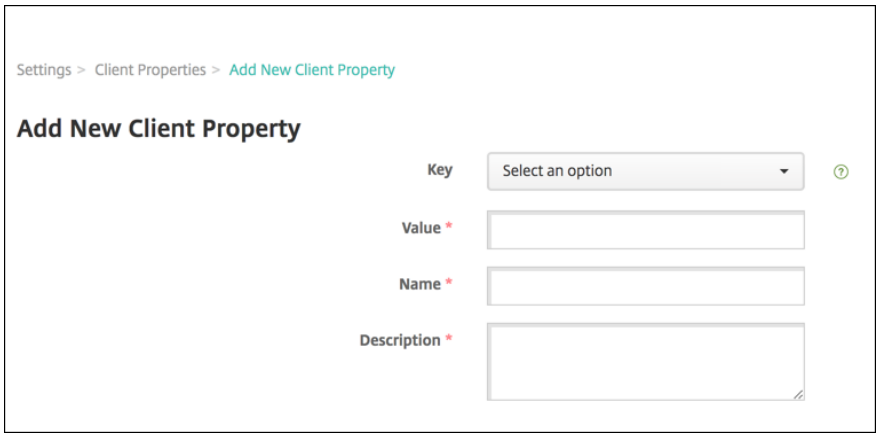
每次发布 Secure Hub 以及有时发布客户端应用程序时，均会更改客户端属性。有关通常要配置的客户端属性的详细信息，请参阅本文末尾的客户端属性参考。

1. 在 Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在客户端下方，单击客户端属性。此时将显示客户端属性页面。可以从此页面添加、编辑和删除客户端属性。



添加客户端属性

1. 单击添加。此时将显示添加新客户端属性页面。



2. 配置以下设置：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 键：在列表中，单击要添加的属性键。重要：更新这些设置之前，请联系 Citrix 技术支持。您可以申请一个特殊键。
- 值：选定属性的值。
- 名称：属性的名称。
- 说明：属性的说明。

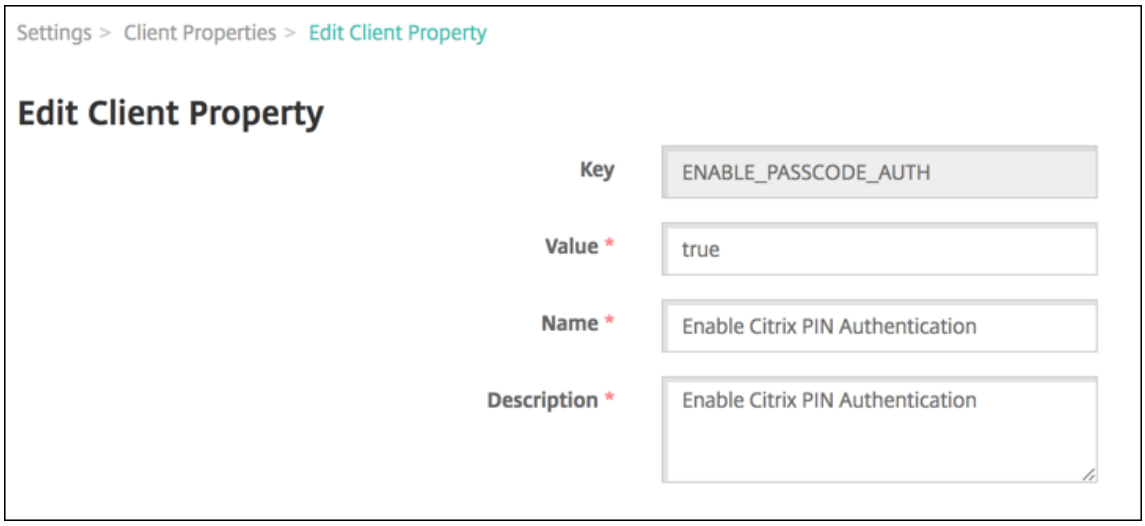
3. 单击保存。

编辑客户端属性

1. 在客户端属性表格中，选择要编辑的客户端属性。

   选中客户端属性旁边的复选框，以打开客户端属性列表上方的选项菜单。单击列表中的其他任意位置可在列表右侧打开选项菜单。

2. 单击编辑。此时将显示编辑客户端属性页面。



3. 适当更改以下信息：

   - 键：无法更改此字段。
   - 值：属性值。
   - 名称：属性名称。
   - 说明：属性说明。

4. 单击保存以保存您所做更改，或单击取消保留属性不变。

删除客户端属性

1. 在客户端属性表格中，选择要删除的客户端属性。

   可以通过选中每个属性旁边的复选框，选择多个要删除的属性。

2. 单击删除。此时将显示确认对话框。再次单击删除。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

客户端属性参考

Endpoint Management 的预定义客户端属性及其默认设置如下所示。

- **ALLOW_CLIENTSIDE_PROXY**
  - 显示名称：ALLOW_CLIENTSIDE_PROXY
  - 如果您的用户需要使用他们在 iOS 手机上配置的代理，请将此自定义策略设置为默认值为 **true**。

    某些用户可能已在其设备上的设置 **> Wi-Fi >** 配置代理中配置了代理。如果 Secure Hub 无法为这些用户打开，请让他们执行以下操作之一：

    * 从设备中删除代理配置，然后重新启动 Secure Hub。
    * 将设备连接到另一个 Wi-Fi 网络。Secure Hub 重新进行身份验证后，它将获取 **ALLOW_CLIENTSIDE_PROXY** 属性并打开。
  - 如果 **ALLOW_CLIENTSIDE_PROXY** 设置为 **false**，并且用户在其设备上配置了代理，Endpoint Management 将检测代理。但是，Secure Hub 不使用代理并显示错误消息。如果设备连接到启用了代理的接入点或路由器，Endpoint Management 将不检测代理。为了获得最高的安全性，我们建议您使用证书固定。有关为 Secure Hub 启用证书固定的信息，请参阅证书固定。
  - 要配置此自定义客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **ALLOW_CLIENTSIDE_PROXY**，并设置值。
- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 显示名称：MDX 容器自毁期限
  - 自毁功能阻止在经过指定天数的非活动状态后访问 Secure Hub 和托管应用程序。超过该时间限制后，应用程序将不再可用。擦除数据包括清除已安装的各应用程序的应用程序数据，包括应用程序缓存和用户数据。

    不活动时间是指在经过特定时间长度后，服务器不接收身份验证请求以验证用户。假设此属性为 30 天。如果用户不使用应用程序的时间超过 30 天，此策略将生效。

    此全局安全策略适用于 iOS 和 Android 平台，是对现有应用程序锁定和擦除策略的增强。
  - 要配置此全局策略，请转至设置 **>** 客户端属性，然后添加自定义键 **CONTAINER_SELF_DESTRUCT_PERIOD**。
  - 值：天数
- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - 显示名称：向 IT 技术支持人员发送设备日志
  - 此属性启用或禁用向 IT 技术支持人员发送日志的功能。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **DISABLE_LOGGING**
  - 显示名称：禁用日志记录

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 使用此属性可阻止用户从其设备收集和上载日志。此属性禁用 Secure Hub 以及已安装的所有 MDX 应用程序的日志记录功能。用户无法从“支持”页面发送任何应用程序的日志。即使显示了邮件撰写对话框，也不附加日志。此时将显示一条消息，指示日志记录功能已禁用。此设置还阻止您在 Endpoint Management 控制台中更新 Secure Hub 和 MDX 应用程序的日志设置。

    此属性设置为 **true** 时，Secure Hub 会将阻止应用程序日志设置为 **true**。因此，应用新策略时，MDX 应用程序将停止日志记录。

  - 可能的值：**true** 或 **false**

  - 默认值：**false**（不禁用日志记录）

- **ENABLE_CRASH_REPORTING**

  - 显示名称：启用崩溃报告
  - 如果设置为 **true**，Citrix 将收集崩溃报告和诊断信息以帮助对 Secure Hub for iOS 和 Secure Hub for Android 相关问题进行故障排除。如果设置为 **false**，则不收集任何数据。
  - 可能的值：**true** 或 **false**
  - 默认值：**true**

- **ENABLE_CREDENTIAL_STORE**

  - 显示名称：启用凭据存储区
  - 启用凭据存储区意味着 Android 或 iOS 用户在访问 Citrix 移动生产力应用程序时输入一次其密码。可以使用凭据存储区，而无论您是否启用了 Citrix PIN。如果不启用 Citrix PIN，用户输入其 Active Directory 密码。Endpoint Management 只对 Secure Hub 和公共应用商店应用程序支持将 Active Directory 密码用于凭据存储区。如果您将 Active Directory 密码用于凭据存储区，Endpoint Management 将不支持 PKI 身份验证。
  - 要在 Secure Mail 中自动注册，需要将此属性设置为 **true**。
  - 要配置此自定义客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **ENABLE_CREDENTIAL_STORE**，并将值设置为 **true**。

- **ENABLE_PASSCODE_AUTH**

  - 显示名称：启用 Citrix PIN 身份验证

  - 此属性允许您打开 Citrix PIN 功能。启用 Citrix PIN 或通行码后，系统将提示用户定义要使用的 PIN（而非其 Active Directory 密码）。如果启用了 ENABLE_PASSWORD_CACHING，或者如果 Endpoint Management 使用证书身份验证，此设置将自动启用。

    执行脱机身份验证时，Citrix PIN 将在本地验证，并且允许用户访问请求的应用程序或内容。执行联机身份验证时，Citrix PIN 或通行码将解锁 Active Directory 密码或证书，随后将发送该密码或证书以通过 Endpoint Management 执行身份验证。

    如果 ENABLE_PASSCODE_AUTH 设置为 true，ENABLE_PASSWORD_CACHING 设置为 false，联机身份验证将始终提示输入密码，因为 Secure Hub 不保存该密码。

  - 可能的值：**true** 或 **false**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 默认值：**false**

- **ENABLE_PASSWORD_CACHING**
  - 显示名称：启用用户密码缓存
  - 此属性允许在移动设备上本地缓存 Active Directory 密码。将此属性设置为 **true** 时，还必须将 **ENABLE_PASSCODE_AUTH** 属性设置为 **true**。如果启用了用户密码缓存，Endpoint Management 将提示用户设置 Citrix PIN 或通行码。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **ENABLE_TOUCH_ID_AUTH**
  - 显示名称：启用 Touch ID 身份验证
  - 对于支持 Touch ID 身份验证的设备，此属性将在设备上启用或禁用 Touch ID 身份验证。要求：

    用户设备必须启用 Citrix PIN 或 LDAP。如果 LDAP 身份验证处于关闭状态（例如，因为使用了仅基于证书的身份验证），则用户必须设置 Citrix PIN。在这种情况下，Endpoint Management 要求使用 Citrix PIN，即使客户端属性 **ENABLE_PASSCODE_AUTH** 为 **false** 也是如此。

    将 **ENABLE_PASSCODE_AUTH** 设置为 **false**，以便用户启动应用程序时，他们必须响应提示以使用 Touch ID。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **ENABLE_WORXHOME_CEIP**
  - 显示名称：启用 Secure Hub CEIP
  - 此属性将打开客户体验改善计划。该功能会定期向 Citrix 发送匿名配置和使用数据。该数据将帮助 Citrix 提高 Endpoint Management 的品质、可靠性和性能。
  - 值：**true** 或 **false**
  - 默认值：**false**
- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 显示名称：使用通行码加密机密
  - 此属性将敏感数据存储在设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串。此属性允许使用强加密的密钥，但还会添加用户熵。用户熵是用户生成的只有自己知道的随机 PIN 代码。

    Citrix 建议您启用此属性以帮助提高用户设备的安全性。因此，用户将遇到多个要求输入 Citrix PIN 的身份验证提示。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **INACTIVITY_TIMER**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 显示名称：不活动计时器
  - 此属性定义用户可以保持其设备处于不活动状态且之后访问应用程序不会提示输入 Citrix PIN 或通行码的时间长度。要为 MDX 应用程序启用此设置，请将“应用程序通行码”设置设为“开”。如果“应用程序通行码”设置设为关，用户将被重定向到 Secure Hub 以执行完全身份验证。更改此设置时，该值将在系统下次提示用户进行身份验证时生效。

    在 iOS 上，不活动计时器还将管理 MDX 应用程序和非 MDX 应用程序对 Secure Hub 的访问。
  - 可能的值：任意正整数
  - 默认值：**15**（分钟）

- **ON_FAILURE_USE_EMAIL**
  - 显示名称：失败时使用电子邮件向 IT 技术支持人员发送设备日志
  - 此属性启用或禁用使用电子邮件向 IT 发送设备日志的功能。
  - 可能的值：**true** 或 **false**
  - 默认值：**true**

- **PASSCODE_EXPIRY**
  - 显示名称：PIN 更改要求
  - 此属性定义 Citrix PIN 或通行码的有效时间长度，超过此时间后，系统将强制用户更改其 Citrix PIN 或通行码。更改此设置时，仅在当前 Citrix PIN 或通行码过期时才设置新值。
  - 可能的值：**1** 到 **99**（建议）。为了永远不重置 PIN，请将该值设置为一个大的数值（例如 100000000000）。如果最初设置的过期期限介于 1 到 99 天之间，然后在该时间段内更改为更大的数值，PIN 在初始期限结束时仍会过期，但之后永不过期。
  - 默认值：**90**（天）

- **PASSCODE_HISTORY**
  - 显示名称：PIN 历史记录
  - 此属性定义之前使用的 Citrix PIN 或通行码的数量，用户在更改其 Citrix PIN 或通行码时不能重用。如果更改此设置，用户下次重置其 Citrix PIN 或通行码时将设置新值。
  - 可能的值：**1** 到 **99**
  - 默认值：**5**

- **PASSCODE_MAX_ATTEMPTS**
  - 显示名称：PIN 尝试次数
  - 此属性定义用户可以尝试输入错误 Citrix PIN 或通行码的次数，之后系统将提示用户进行完全身份验证。用户成功执行完全身份验证后，系统将提示其创建 Citrix PIN 或通行码。
  - 可能的值：任意正整数
  - 默认值：**15**

- **PASSCODE_MIN_LENGTH**
  - 显示名称：PIN 长度要求

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 此属性定义 Citrix PIN 的最小长度。
- 可能的值：**4** 到 **10**
- 默认值：**6**

- **PASSCODE_STRENGTH**
  - 显示名称：PIN 强度要求
  - 此属性定义 Citrix PIN 或通行码的强度。更改此设置时，系统将在下次提示用户进行身份验证时提示其创建 Citrix PIN 或通行码。
  - 可能的值：低、中、高或强
  - 默认值：中
  - 每种强度设置的密码规则如下所示，具体取决于 PASSCODE_TYPE 设置：

数字通行码的规则：

通行码强度	数字通行码类型的规则	允许	不允许
低	所有数字，允许使用任意顺序	444444、123456、654321	
中（默认设置）	所有数字不能相同，也不能连续。	444333、124567、136790、555556、788888	444444、123456、654321
高	相邻的数字不能相同。	123512、134134、132312、131313、987456	080080、112233、135579、987745、919199
强	请勿使用同一编号超过两次。请勿连续使用三个或更多连续数字。请勿按相反的顺序使用三个或更多连续的数字。	102983、085085、824673、132312	132132、131313、902030

字母数字通行码的规则：

通行码强度	字母数字通行码类型的规则	允许	不允许
低	必须至少包含一个数字和一个字母	aa11b1、Abcd1#、Ab123~、aaaa11、aa11aa	AAAaaa、aaaaaa、abcdef

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

通行码强度	字母数字通行码类型的规则	允许	不允许
中（默认设置）	除“低”通行码强度的规则外，字母和所有数字都不能相同。字母和数字都不能连续。	aa11b1、aaa11b、aaa1b2、abc145、xyz135、sdf123、ab12c3、a1b2c3、Abcd1#、Ab123~	aaaa11、aa11aa 或 aaa111；abcd12、bcd123、123abc、xy1234、xyz345 或 cba123
高	至少包括一个大写字母和一个小写字母。	Abcd12、jkrtA2、23Bc#、AbCd	abcd12、DFGH2
强	至少包括一个数字、一个特殊符号、一个大写字母以及一个小写字母。	Abcd1#、Ab123~、xY12#3、Car12#、AAbc1#	abcd12、Abcd12、dfgh12、jkrtA2

- **PASSCODE_TYPE**
  - 显示名称：PIN 类型
  - 此属性定义用户能够定义数字型 Citrix PIN 还是字母数字型通行码。选择数字时，用户只能定义数字 (Citrix PIN)。选择字母数字时，用户可以使用字母和数字的组合（通行码）。

    如果更改此设置，用户必须在系统下次提示进行身份验证时设置新 Citrix PIN 或通行码。
  - 可能的值：数字或字母数字
  - 默认值：数字
- **REFRESHINTERVAL**
  - 显示名称：REFRESHINTERVAL
  - 默认情况下，Endpoint Management 每隔 3 天会对 AutoDiscovery Server (ADS) 执行 ping 命令查找固定证书。要更改刷新时间间隔，请转至设置 **>** 客户端属性，添加自定义键 **REFRESHINTERVAL**，并将值设置为小时数。
  - 默认值：**72** 小时（3 天）
- **SEND_LDAP_ATTRIBUTES**
  - 对于 Android、iOS 或 macOS 设备的仅 MAM 部署：可以配置 Endpoint Management，以便使用电子邮件凭据在 Secure Hub 中注册的用户能够自动在 Secure Mail 中注册。因此，用户不需要提供额外的信息或执行额外的步骤即可在 Secure Mail 中注册。
  - 要配置此全局客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **SEND_LDAP_ATTRIBUTES**，并按如下所示设置值。
  - 值：`userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 与 MDM 策略类似，属性值会指定为宏。
  - 以下示例介绍了帐户服务如何响应此属性：

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName=
    eng1,displayName=user\,test1,email=user@site.com\,user@site.com"
    name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - 对于此属性，Endpoint Management 会将逗号字符视为字符串终止符。因此，如果属性值包括一个逗号，请在其前面添加一个反斜杠。反斜杠将阻止客户端将嵌入的逗号解释为属性值的结尾。反斜杠字符表示为 `"\\"`。

- **HIDE_THREE_FINGER_TAP_MENU**
  - 此属性未设置或设置为 **false** 时，用户可以通过在其设备上执行三指轻按操作来访问隐藏的功能菜单。隐藏的功能菜单允许用户重置应用程序数据。将此属性设置为 **true** 将禁止用户访问隐藏的功能菜单。
  - 要配置此全局客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **HIDE_THREE_FINGER_TAP_MENU**，然后设置值。
- **TUNNEL_EXCLUDE_DOMAINS**
  - 显示名称：通道排除域
  - 默认情况下，MDX 将从 Micro VPN 通道中排除移动应用程序 SDK 和应用程序用于各种功能的某些服务端点。例如，这些端点包括不需要通过企业网络路由的服务，例如 Google Analytics、Citrix Cloud Services 和 Active Directory 服务。可使用此客户端属性覆盖排除的默认域列表。
  - 要配置此全局客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **TUNNEL_EXCLUDE_DOMAINS**，并设置值。
  - 值：要将默认列表替换为要从通道中排除的域，请键入以逗号分隔的域后缀列表。要在通道中包括所有域，请键入 **none**。默认值：

    ```
    app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test
    .citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.
    launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net
    ,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf
    -staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,
    stream.launchdarkly.com
    ```

用户注册选项

June 9, 2022

可以通过多种方式让用户在 Endpoint Management 中注册其设备。在考虑具体情况之前，请决定要在 MDM+MAM、MDM 还是 MAM 中注册哪些设备。有关这些管理模式的详细信息，请参阅 管理模式。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

在最高级别，有四个注册选项：

- 注册邀请：向用户发送注册邀请或邀请 URL。注册邀请和 URL 不适用于 Windows 设备。
- 自助门户：设置用户可以访问的门户以下载 Secure Hub、请求注册和查看设备信息。
- 手动注册：发出电子邮件、手册或某些其他通信信息，让用户知晓系统已启动并且可以进行注册。用户随后将手动下载 Secure Hub 并注册其设备。
- 企业：另一个用于设备注册的选项是通过 Apple 部署计划和 Google Android Enterprise。您可以通过其中的每个计划来购买预配置并且可随时供用户使用的设备。有关详细信息，请参阅 Apple 支持中的 Apple 部署计划文章和 Android Enterprise Web 站点上的 Google Android Enterprise 文档。

注册邀请

可以通过电子邮件向使用 iOS、macOS、Android Enterprise 或旧版 Android 设备的用户发送注册邀请。注册邀请不适用于 Windows 设备。

你还可以通过 SMTP 向使用 iOS、macOS、Android Enterprise、Android 或 Windows 设备的用户发送安装链接。有关详细信息，请参阅注册设备。

如果选择使用注册邀请方法，您可以：

- 选择邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。
- 使用这些模式的任意组合。
- 从 Endpoint Management 设置页面启用或禁用这些模式。

有关每种注册安全模式的信息，请参阅配置注册安全模式。

邀请可实现多种目的。最常见的邀请用法是通知用户系统可用，并且可以进行注册。邀请 URL 是唯一的。用户使用邀请 URL 后，该 URL 将不再可用。可以使用此属性将用户或设备注册限制到您的系统。

配置注册配置文件时，可以根据 Active Directory 组控制特定用户能够注册的设备数。例如，您可能会允许您的财务部门每个用户只使用一台设备。

请注意某些注册选项的附加成本和陷阱。要使用 SMTP 发送邀请，需要额外的基础结构。有关此选项的详细信息，请参阅通知。

此外，要通过电子邮件发送邀请，请确保用户拥有在 Secure Hub 外部访问电子邮件的方法。您可以使用一次性密码 (OTP) 注册安全模式作为 MDM 注册的 Active Directory 密码的替代方法。

自助服务门户

可以使用管理员用于访问 Endpoint Management 控制台的相同 URL 访问自助门户。最终用户将看到自助服务门户，而非管理控制台。用户可以在自助服务门户中下载 Secure Hub、申请注册和查看设备信息。

要设置门户，请在 设置 **>** 服务器属性中更新以下服务器属性：

- `shp.console.enable`：设置为 **True** 以提供对自助服务门户的访问权限。
- `enable.new.shp`：设置为 **True** 以允许用户从自助服务门户启用其设备。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

手动注册

进行手动注册时，用户将通过自动发现或者通过输入服务器信息连接到 Endpoint Management。使用自动发现时，用户将仅通过其电子邮件地址或用户主体名称格式的 Active Directory 凭据进行登录。不使用自动发现时，用户必须输入其服务器地址和 Active Directory 凭据。有关设置自动发现的详细信息，请参阅设 置 Endpoint Management 自动发现服务。

可以通过多种方式简化手动注册过程。可以创建一个指南，将其分发给用户，并请用户自行注册。可以请您的 IT 部门在某个时间段内手动注册几组用户。可以使用用户必须输入其凭据或服务器信息的任何类似的方法。

用户加入

设置您的环境后，需要确定如何使用户加入到您的环境中。本文开头的部分探讨了用户注册安全模式的具体信息。本节将探讨您与用户取得联系的方法。

开放式注册与选择性邀请

登录用户时，可以通过两种基本方法允许注册：

- 开放式注册。默认情况下，任何具有 LDAP 凭据和 Endpoint Management 环境信息的用户都可以注册。
- 有限注册。可以通过仅允许具有邀请的用户进行注册来限制用户数量。还可以通过 Active Directory 组限制开放式注册。

使用此邀请方法时，还可以限制用户能够注册的设备数。在大多数情况下，可接受开放式注册，但有几点事项需要注意：

- 对于 MAM 注册，您可以通过 Active Directory 组成员身份轻松限制开放式注册。
- 对于 MDM 注册，您可以根据 Active Directory 组成员身份限制可以注册的设备数。如果仅允许在您的环境中注册企业设备，该限制通常不是问题。但是，您可能希望考虑在要限制环境中的设备数量的 BYOD 工作区中使用此方法。

通常很少执行选择性邀请，因为与开放式注册相比，此注册方法需要执行更多操作。为使用户在您的环境中注册其设备，必须向每个用户发送一个唯一的邀请。有关如何发送注册邀请的信息，请参阅 注册邀请。

为要在环境中注册的每个用户或组发送邀请。该过程可能需要很长时间，具体取决于贵组织的规模。可以使用 Active Directory 组批量创建邀请，但必须分批执行此方法。

首次与用户联系

决定要使用开放式注册还是选择性邀请并设置了这些环境后，请告知用户其注册选项。

如果您使用选择性邀请方法，则电子邮件是该过程的一部分。对于开放式注册，还可以通过 Endpoint Management 控制台发送电子邮件。有关详细信息，请参阅 注册邀请。

在任一情况下，都请谨记，如果要发送电子邮件，则需要 SMTP 服务器。制定决策时，这些服务器可能有需要考虑的附加成本。考虑一下您期望新用户如何访问信息。如果希望所有用户都通过 Endpoint Management 访问其电子邮件，向其发送邀请电子邮件将是一个问题。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

还可以通过 Endpoint Management 以外的其他方式为开放式注册环境发送通信。对于该选项，请务必包含所有相关信息。让用户知道他们可以从哪里获取 Secure Hub 应用程序以及注册时使用的方法。如果您关闭了发现，还要为用户提供 Endpoint Management 服务器地址。要了解有关发现的更多信息，请参阅 设置 Endpoint Management 自动发现服务。

应用程序预配和取消预配

September 13, 2022

应用程序预配与移动应用程序生命周期管理紧密相关：在 Endpoint Management 环境中准备、配置、交付和管理移动应用程序。在某些情况下，预配流程可能还包括开发或修改应用程序代码。Endpoint Management 具有可用于应用程序预配的各种工具和流程。

在阅读这篇有关应用程序预配的文章之前，我们建议您先阅读应用程序和用户社区。当您最终确定了您的组织计划向用户交付的应用程序类型时，可以制定在应用程序的整个生命周期对其进行管理的流程。

在定义应用程序预配流程时，请考虑以下几点：

- 应用程序分析：贵组织可能先开始分析有限数量的应用程序。但是，随着用户采用率的提高和环境的扩大，您管理的应用程序数量会迅速增加。预先定义特定的应用程序配置文件，以使应用程序预配易于管理。应用程序配置可帮助您从非技术角度将应用程序分类到相应逻辑组。例如，您可以根据以下因素创建应用程序配置文件：
  - 版本：要跟踪的应用程序版本
  - 实例：为具有不同访问级别的多组不同用户部署的多个实例
  - 平台：iOS、Android 或 Windows
  - 目标受众：标准用户、部门、高管
  - 所有权：拥有该应用程序的部门
  - 类型：MDX、公共、Web 和 SaaS 或者 Web 链接
  - 升级周期：应用程序的升级频率
  - 许可：许可要求和所有权
  - MAM SDK 或 MDX 策略：将 MDX 功能应用到您的移动应用程序
  - 网络访问：访问类型，例如通过单点登录（通道 - Web SSO）传输 HTTP 和 HTTPS 流量。

示例：

因数	Secure Mail	邮件	内部	Epic Rover
版本	10.1	10.1	X.x	X.x
实例	VIP	医师	临床	临床
平台	iOS	iOS	iOS	iOS
目标用户	VIP 用户	医师	临床用户	临床用户
所有权	IT	IT	IT	IT

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

因数	Secure Mail	邮件	内部	Epic Rover
类型	MDX	MDX	本机	公用
升级周期	按季度	按季度	每年	不适用
许可	不适用	不适用	不适用	批量购买
MDX 策略	是	是	是	否
网络访问	VPN	VPN	VPN	公用

- 应用程序版本控制：维护和跟踪应用程序版本是预配流程的关键部分。版本控制对用户通常是透明的。仅当有新版本的应用程序可下载时，他们才会收到通知。从您的角度而言，以非生产容量检查和测试每个应用程序版本也是至关重要的，以避免影响生产站点。

  此外，评估是否需要某个特定升级也很重要。应用程序升级通常有两种类型：次要升级（例如特定缺陷的修复），或者引入重大变化的主要版本。在这两种情况下，请仔细查看应用程序的发行说明以评估是否需要升级。

- 应用程序开发：将 MAM SDK 集成到您开发的移动应用程序中时，您将 MDX 功能应用到这些应用程序。请参阅 MAM SDK 概述。

  MAM SDK 取代了计划于 2023 年 7 月弃用的 MDX Toolkit。有关应用程序封装的信息，请参阅 MDX Toolkit。打包应用程序的应用程序预配流程与标准的未打包应用程序的预配流程有所差别。

- 应用程序安全性：在预配流程中，要定义各个应用程序或应用程序配置文件的安全要求。可以在部署应用程序之前将安全要求映射到特定 MDM 或 MAM 策略。该规划简化并加快了应用程序部署过程。例如：

  - 您可能会以不同的方式部署某些应用程序。
  - 您可能希望对 Endpoint Management 环境的体系结构进行更改。这些更改取决于应用程序所需的安全合规性类型。例如，特定应用程序可能需要端到端 SSL 加密或地理围栏。

- 应用程序交付： Endpoint Management 允许您以 MDM 应用程序或 MAM 应用程序方式交付应用程序。MDM 应用程序将显示在应用商店中。此应用商店允许您方便地向用户交付公共应用程序或本机应用程序。除了强制执行设备级别限制外，不需要其他应用程序控件。但是，使用 MAM 交付应用程序可以完全控制应用程序交付以及控制应用程序本身。通常情况下，通过 MAM 交付应用程序更合适。

- 应用程序维护：

  - 执行初始审核：跟踪您的生产环境中存在的应用程序版本以及上一个升级周期。记下需要升级才能实现的特定功能或缺陷修复。
  - 建立基准：维护每个应用程序的最新稳定版本列表。如果升级后出现意外问题，请准备好回退到早期的应用程序版本。制定回滚计划。在部署到生产环境之前，在测试环境中测试应用程序升级。如果可能，请先将升级部署到生产用户的子集，然后再部署到整个用户群。
  - 订阅 Citrix 软件更新通知和任何第三方软件供应商通知：始终拥有最新版本的应用程序至关重要。早期访问版本 (EAR) 内部版本可以提前进行测试。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

  - 制定通知用户的策略：定义应用程序升级可用时通知用户的策略。请在部署之前对用户进行培训，使用户做好准备。请考虑在更新应用程序之前发送多个通知。根据应用程序的情况，最佳的通知方法可能是电子邮件通知或 Web 站点。

应用程序生命周期管理涉及应用程序从其初始部署到停用的完整生命周期。应用程序的生命周期有以下阶段：

1. 规范要求：首先提出业务用例和用户要求。
2. 开发：验证应用程序是否满足业务需求。
3. 测试：确定测试用户、问题和缺陷。
4. 部署：将应用程序部署到生产用户。
5. 维护：更新应用程序版本。在生产环境中更新应用程序之前，先在测试环境中部署应用程序。

基于控制板的操作

December 3, 2021

可以通过访问 Endpoint Management 控制台控制板一目了然地查看信息。根据这些信息，您可以使用小组件快速查看问题和成功方法。

控制板通常是您首次登录 Endpoint Management 控制台时显示的屏幕。要从控制台中的其他地方访问控制板，请单击分析。单击控制板中的自定义可编辑页面布局以及编辑显示的小组件。

- 我的控制板：最多可以保存四个控制板。可以单独编辑这些控制板，并通过选择保存的控制板来查看每个控制板。
- 布局样式：在此行中，可以选择在控制板上显示的小组件数以及如何布局小组件。
- 小组件选择：可以选择在控制板上显示的信息。
  - 通知：选中左侧数字上方的复选框可将“通知”栏添加到小组件上方。此栏显示兼容设备、不活动设备以及过去 24 小时擦除或注册的设备数。
  - 设备 **(**按平台**)**：按平台显示托管设备和非托管设备数。
  - 设备 **(**按运营商**)**：按运营商显示托管设备和非托管设备数。单击每个栏可按平台查看明细。
  - 托管设备 **(**按平台**)**：按平台显示托管设备数。
  - 非托管设备 **(**按平台**)**：按平台显示非托管设备数。此图表中显示的设备可能安装了代理，但设备的权限已被吊销或设备已被擦除。
  - 设备 **(**按 **ActiveSync Gateway** 状态**)**：显示按 ActiveSync Gateway 状态分组的设备数。信息中显示“已阻止”、“已允许”或“未知”状态。可以单击每个栏来按平台细分数据。
  - 设备 **(**按所有权**)**：显示按所有权状态分组的设备数。信息中显示“公司拥有”、“员工拥有”或“未知所有权”状态。
  - 失败的交付组部署：按软件包显示失败部署总数。仅显示部署失败的软件包。
  - 设备 **(**按阻止原因**)**：显示 ActiveSync 阻止的设备数
  - 已安装的应用程序：通过使用此小组件，可以键入应用程序名称，将有一个图形显示有关该应用程序的信息。
  - 批量购买应用程序许可证使用情况：显示 Apple 批量购买应用程序的许可证使用情况统计信息。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用例

可以通过多种方式使用控制板小组件监视您的环境，其中的部分示例如下。

- 您已部署 Citrix 移动生产力应用程序并且要接收与移动生产力应用程序无法在设备上安装有关的支持票证。使用不合规设备和已安装的应用程序小组件查看未安装 Citrix 移动生产力应用程序的设备。
- 您希望监视不活动的设备，以便能够从环境中删除这些设备并回收许可证。使用不活动设备小组件跟踪此统计信息。
- 您要接收与未正确同步的数据有关的支持票证。您可能希望使用设备 **(**按 **ActiveSync Gateway** 状态**)** 和设备 **(**按阻止原因**)** 小组件来确定问题是否与 ActiveSync 有关。

报告

您的环境完成设置并且用户注册后，可以运行报告以了解您的部署。Endpoint Management 随附多个内置报告，以帮助您更好地了解环境中运行的设备。有关详细信息，请参阅报告。

基于角色的访问控制和 **Endpoint Management** 支持

December 3, 2021

Endpoint Management 使用基于角色的访问控制 (RBAC) 来限制用户和组对 Endpoint Management 系统功能的访问，例如 Endpoint Management 控制台、自助服务门户和公共 API。本文介绍了 Endpoint Management 中内置的角色，并且介绍了决定使用 RBAC 的 Endpoint Management 的支持模式的注意事项。

内置角色

可以更改授予以下内置角色的访问权限，并且可以添加角色。有关与每个角色关联的全套访问权限和功能权限及其默认设置，请下载 基于角色的访问控制默认值。有关每个功能的定义，请参阅使用 RBAC 配置角色。

管理角色

授予的默认访问权限：

- 除对自助服务门户的访问权限以外的完整系统访问权限。
- 默认情况下，管理员可以执行某些支持任务，例如检查连接和创建支持包。

注意事项：

- 您的部分或所有管理员是否需要访问自助服务门户？如果是，则可以编辑管理员角色或添加管理员角色。
- 要进一步限制部分管理员或管理员组的访问权限，请根据管理员模板添加角色并编辑权限。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

用户

授予的默认访问权限：

- 对自助服务门户的访问权限，该权限允许已通过身份验证的用户生成注册链接。这些连接允许用户注册其设备或向自身发送注册邀请。
- 对 Endpoint Management 控制台的受限访问权限：设备功能（例如擦除、锁定/解锁设备；锁定/解锁容器；查看位置和设置地理限制；设备响铃；重置容器密码）；添加、删除和发送注册邀请。

注意事项：

- “用户”角色允许您使用户能够自助操作。
- 要支持共享设备，请为共享设备注册创建一个用户角色。

Endpoint Management 支持模式的注意事项

可以采用的支持模式变化非常大，并且可能涉及负责处理 1 级和 2 级支持的第三方（员工负责处理 3 级和 4 级支持）。无论您如何分发支持负载，都请谨记本部分内容中特定于您的 Endpoint Management 部署和用户基础的注意事项。

用户使用公司拥有的设备还是 **BYO** 设备？
影响支持的主要问题是在您的 Endpoint Management 环境中哪些用户拥有用户设备。如果您的用户使用公司拥有的设备，您可能会提供较低级别的支持，作为锁定设备的一种方法。在这种情况下，您可能会提供帮助用户解决设备问题以及教授设备使用方法的技术支持人员。请考虑您可能会通过何种方式使用技术支持人员的 RBAC 设备预配和支持角色，具体取决于需要支持的设备类型。

如果您的用户使用 BYO 设备，贵组织可能会期望用户寻找自己的设备支持来源。在这种情况下，贵组织提供的支持更多的是专注于解决 Endpoint Management 特定问题的管理角色。

您的桌面的支持模式是什么？
请考虑您的桌面的支持模式是否适用于其他公司拥有的设备。您可以使用相同的支持组织吗？他们需要哪些额外的培训？

您是否希望向用户授予对 **Endpoint Management** 自助服务门户的访问权限？
尽管某些组织偏向于不向用户授予对 Endpoint Management 的访问权限，但是，向用户提供某些自助支持功能可以减轻您的支持组织的负担。如果 RBAC 的默认用户角色包括您不希望授予的权限，请考虑创建一个仅具有您希望包括的权限的新角色。可以根据需要创建多种角色以满足您的要求。

Citrix 支持过程

December 3, 2021

可以请 Citrix Technical Support Services 团队帮助解决与 Citrix 产品有关的问题。该团队提供解决方法和解决方案，并且与开发团队紧密合作以提供解决方案。

Citrix Consulting Services 或 Citrix Education Services 提供与产品培训有关的帮助以及与产品使用情况、配置、安装或环境设计和体系结构有关的建议。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix Consulting 协助完成与 Citrix 产品有关的项目，包括概念证明、经济影响评估、基础结构运行状况检查、设计要求分析、体系结构设计验证、集成和操作过程开发。

Citrix Education 提供针对 Citrix 虚拟化、云和网络连接技术的一流 IT 培训和认证。

Citrix 建议您在创建支持案例之前充分利用 Citrix 自助服务资源和建议。例如，您可以从多个位置访问 Citrix 技术专家撰写的文章和公告、查看针对 Citrix 解决方案和技术的产品文档或者阅读来自 Citrix 主管、产品团队和技术专家的坦率谈话。请分别参阅知识中心、产品文档和博客页面。

要获得更多交互式帮助，可以参与讨论论坛，您可以在论坛中提问问题以及获取其他客户提供的现实答案、在用户小组和兴趣小组内部共享想法、意见、技术信息和最佳做法，或者与负责监视 Citrix 支持社交网络站点的 Citrix 支持工程师互动。分别请参阅 支持论坛 和 Citrix 社区 页面。

您还有权访问培训和认证课程以提高自己的技能。请参阅 Citrix Education。

Citrix Insight Services 提供适用于您的 Citrix 环境的简单在线故障排除平台和运行状况检查器。适用于 Citrix Endpoint Management、Citrix Virtual Apps and Desktops、Citrix Hypervisor 和 Citrix Gateway。请参阅分析工具。

要获取技术支持，可以通过电话或网络创建支持案例。对于严重性较低和中等严重性的问题，可以使用网络，对于严重性较高的问题，可以使用电话。要联系支持以解决 Endpoint Management 问题，请参阅 Citrix 支持服务。

如果寻求在交付 Citrix 解决方案方面具有丰富经验的训练有素的单一联系人，Citrix Services 提供技术关系经理。有关 Citrix 服务方案和效益的详细信息，请参阅 Citrix Worldwide Services（Citrix 全球服务）。

在 **Endpoint Management** 中发送组注册邀请

December 3, 2021

Author:
John Bartel III

您可以在 Endpoint Management 中向群组和嵌套群组发送注册邀请。注册邀请不适用于 Windows 设备。

设置组邀请时，可以指定一个或多个设备平台。还可以标记设备，以便能够（例如）将公司拥有的设备与员工拥有的设备区分开来。之后，请为用户设备设置身份验证类型。

> 注意：
>
> 如果您打算使用自定义通知模板，必须在配置注册安全模式之前设置模板。有关通知模板的详细信息，请参阅创建和更新通知模板。

有关用户帐户、角色和注册安全模式以及邀请的基础配置的详细信息，请参阅用户帐户、角色和注册。

常规步骤

1. 在 Endpoint Management 控制台中，导航到管理 **>** 注册邀请。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. 单击屏幕左上角的添加，然后单击添加邀请。
3. 单击收件人菜单中的组。

   在此步骤中，可以选择一个或多个平台。如果贵公司混合使用不同的操作系统平台，请选择所有平台。仅当确定所有用户都未使用特定的平台时，才能取消选中该平台。

4. 邀请过程中，可以选择标记设备。选择公司或员工。

   通过标记设备，可以轻松分离公司拥有的设备和员工拥有的设备。

5. 在域列表中，选择组所在的域。
6. 在组列表中，选择要向其发送邀请的 Active Directory 组。
7. 注 册模式允许您为用户设置喜欢的注册安全性类型。

   - 用户名 + 密码
   - 高安全性
   - 邀请 URL
   - 邀请 URL + PIN
   - 邀请 URL + 密码
   - 双重
   - 用户名 + PIN

   > 注意：
   >
   > 我们弃用了“ 高安全性”注册安全模式。要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。对于使用用户名 **+** 密码、双重或用户名 **+ PIN** 注册的设备，用户必须下载 Secure Hub 并手动输入其凭据。

8. 对于代理下载、注册 **URL**、注册 **PIN** 和注册确认模板，请选择您以前创建的自定义通知模板。或者，请选择列出的默认模板。

   对于这些通知模板，请使用您在 Endpoint Management 中配置的 SMTP 服务器设置。请先设置 SMTP 信息，然后再继续操作。

   > 注意：
   >
   > 此时间后过期和最大尝试次数选项根据您选择的注册模式选项而变化。不能更改这些选项。

9. 请为发送邀请选择“开”，然后单击保存并发送以完成该过程。

嵌套组支持

可以使用嵌套组发送邀请。通常情况下，嵌套组在具有相似权限的组相互绑定的大型环境中使用。

导航到设置 **> LDAP**，然后启用支持嵌套组选项。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

故障排除和已知限制

问题：即使已将用户从 Active Directory 组中删除，也可以向这些用户发出邀请。

解决方案：最长可能需要 6 个小时才能将更改传播到所有服务器，具体取决于您的 Active Directory 环境的规模。如果最近删除了某个用户或嵌套组，Endpoint Management 可能仍然会将这些用户视为组的一部分。

因此，最好等待 6 个小时以后再向您的用户发出其他组邀请。

为 **EWS** 配置基于证书的身份验证以接收 **Secure Mail** 推送通知

December 3, 2021

必须执行以下操作，才能使 Secure Mail 推送通知工作：

- 为基于证书的身份验证配置 Exchange Server。在启用了基于证书的身份验证的 Endpoint Management 中注册 Secure Hub 时，此要求尤为必要。
- 在进行基于证书的身份验证的 Exchange Mail Server 上配置 Active Sync 和 Exchange Web 服务 (EWS) 虚拟目录。

除非完成这些配置，否则对 Secure Mail 推送通知的订阅将失败，并且 Secure Mail 中不会发生任何徽章更新。

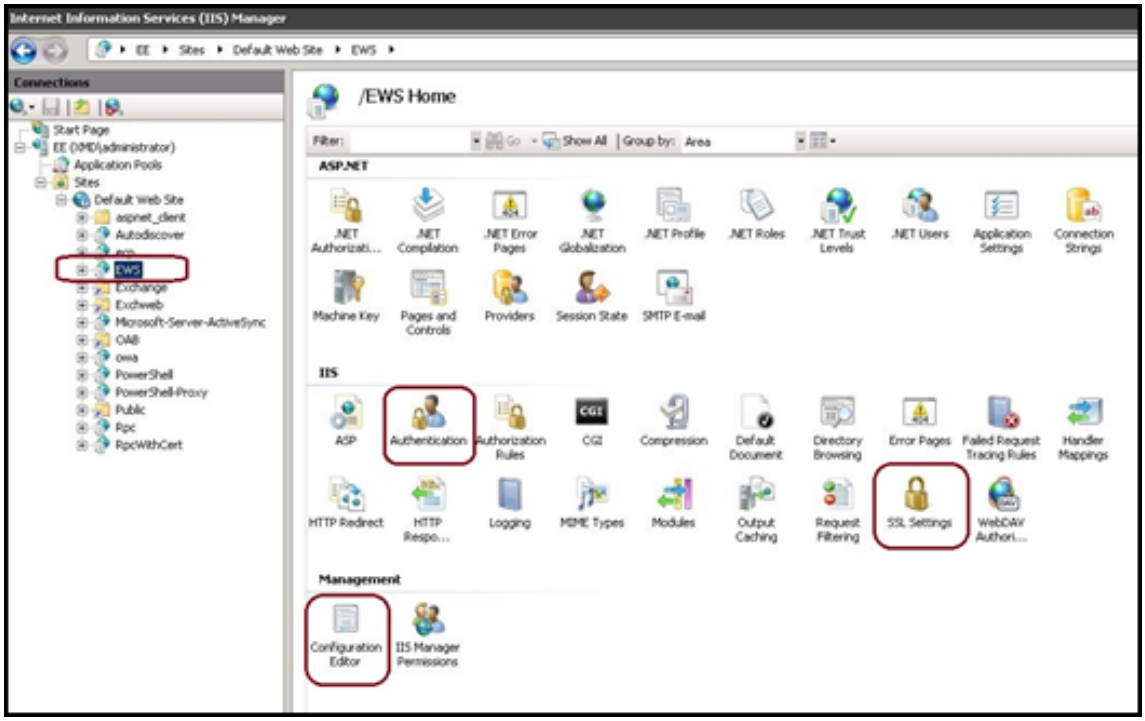
本文介绍了配置基于证书的身份验证的步骤。这些配置专门针对 Exchange Server 上的 EWS 虚拟目录。

要开始配置，请执行以下操作：

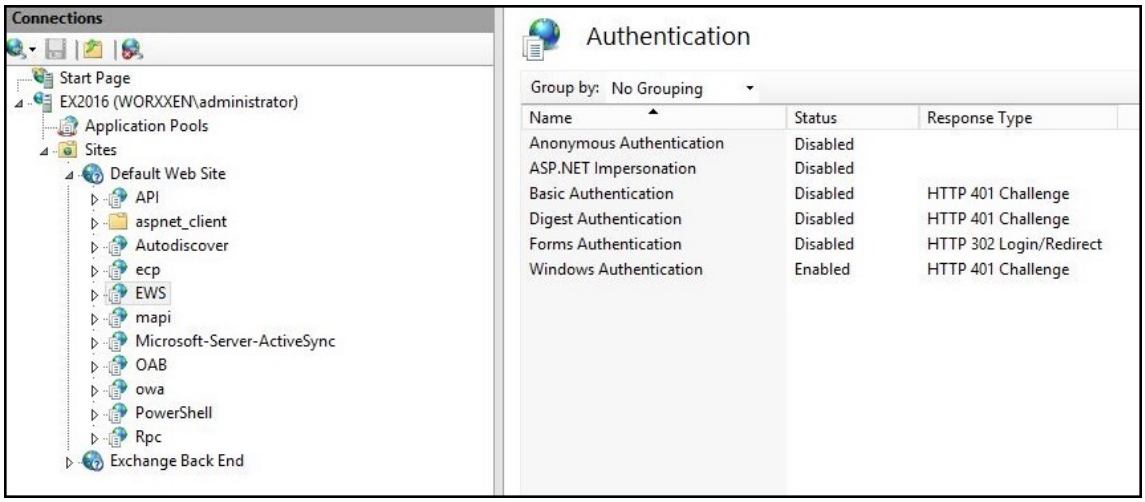
1. 登录安装了 EWS 虚拟目录的一个或多个服务器。
2. 打开 IIS 管理器控制台。
3. 在 **Default Web Site**（默认 Web 站点）下，单击 EWS 虚拟目录。

   “身份验证”、“SSL” 和 “配置编辑器” 管理单元位于 IIS 管理器控制台的右侧。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 确保 EWS 的身份验证设置按下图中所示进行配置。

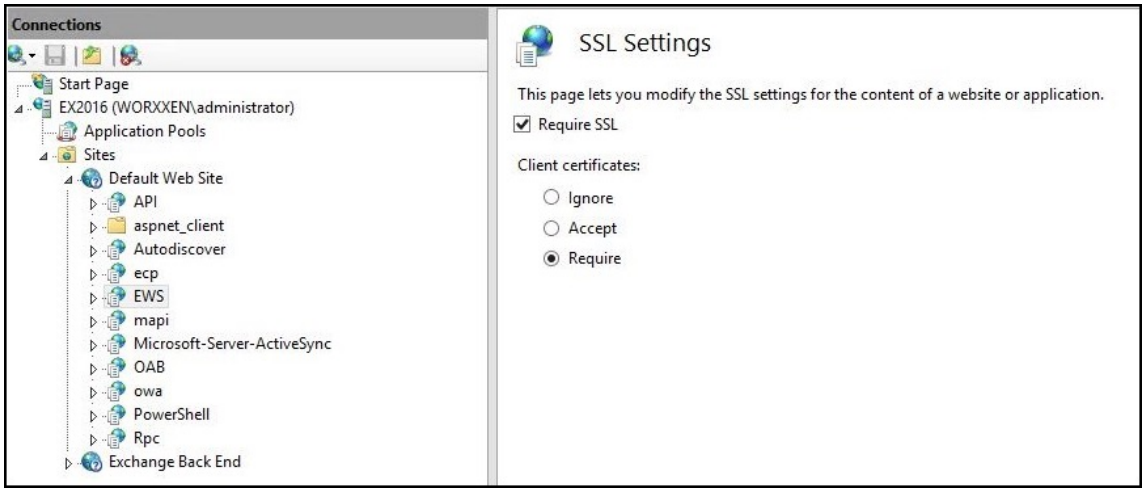


5. 为 EWS 虚拟目录配置 **SSL** 设置。

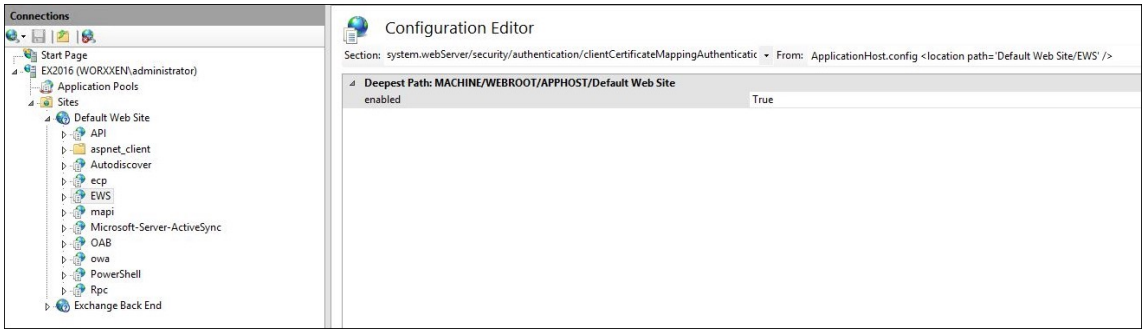
   a) 选中 **Require SSL**（要求 SSL）复选框。

   b) 在 客户端证书下，单击 需要。或者，如果其他 EWS 邮件客户端使用用户名和密码对 Exchange Server 进行身份验证，请单击接受。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 单击 **Configuration Editor**（配置编辑器）并在 **Section**（部分）下拉列表中，导航到以下部分：
   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**
7. 将 **enabled** 值设置为 **True**。

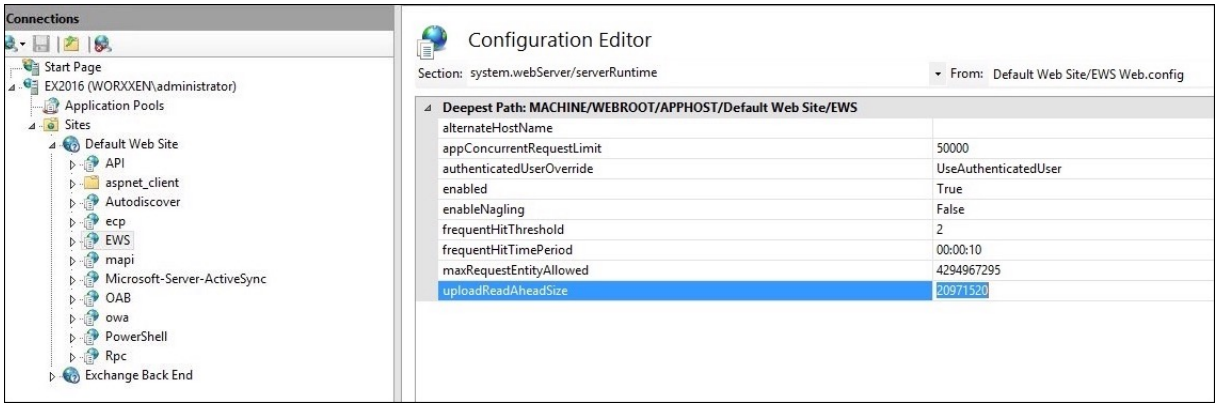


8. 单击 **Configuration Editor**（配置编辑器）并在 **Section**（部分）下拉列表中，导航到以下部分：
   - **system.webServer/serverRuntime**
9. 将 **uploadReadAheadSize** 值设置为 **10485760** (10 MB) 或 **20971520** (20 MB)，或者设置为贵组织需要的值。

   > 重要：
   >
   > 如果未正确设置此值，订阅 EWS 推送通知时基于证书的身份验证会失败，并显示错误代码 413。
   >
   > 不要将此值设置为 **0**。

有关详细信息，请参阅微软文章微 软 IIS 服务器运行时。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



有关对 Secure Mail 存在的 iOS 推送通知问题进行故障排除的详细信息，请参阅此 Citrix 支持知识中心文章。

相关信息

Secure Mail for iOS 的推送通知

配置本地设备运行状况证明服务器

December 3, 2021

你可以通过本地 Windows 服务器为 Windows 10 和 Windows 11 移动设备启用设备运行状况证明 (DHA)。要在本地启用 DHA，请先配置一个 DHA 服务器。

配置 DHA 服务器后，请创建 Endpoint Management 策略以启用本地 DHA 服务。有关信息，请参阅 设备运行状况证明设备策略。

DHA 服务器的必备项

- 运行使用“桌面体验”安装选项安装的 Windows Server Technical Preview 5 或更高版本的服务器。
- 一个或多个 Windows 10 和 Windows 11 客户端设备。这些设备必须安装运行最新 Windows 版本的 TPM 1.2 或 2.0。
- 以下证书：
  - **DHA SSL** 证书：链接到具有可导出的私钥的企业可信根证书的 x.509 SSL 证书。此证书保护传输过程中的 DHA 数据通信，包括：
    - 服务器到服务器（DHA 服务和 MDM 服务器）通信
    - 服务器到客户端（DHA 服务和 Windows 10 或 Windows 11 设备）通信
  - **DHA** 签名证书：链接到具有可导出的私钥的企业可信根证书的 x.509 证书。DHA 服务使用此证书进行数字签名。
  - **DHA** 加密证书：链接到具有可导出的私钥的企业可信根证书的 x.509 证书。DHA 服务还使用此证书进行加密。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 请选择下面的其中一种证书验证模式：
  - **EKCert**：EKCert 验证模式已针对组织中未连接到 Internet 的设备进行优化。连接到在 EKCert 验证模式下运行的 DHA 服务的设备不能直接访问 Internet。
  - **AIKCert**：AIKCert 验证模式已针对能够直接访问 Internet 的运行环境优化。连接到在 AIKCert 验证模式下运行的 DHA 服务的设备必须能够直接访问 Internet，并且能够从 Microsoft 获取 AIK 证书。

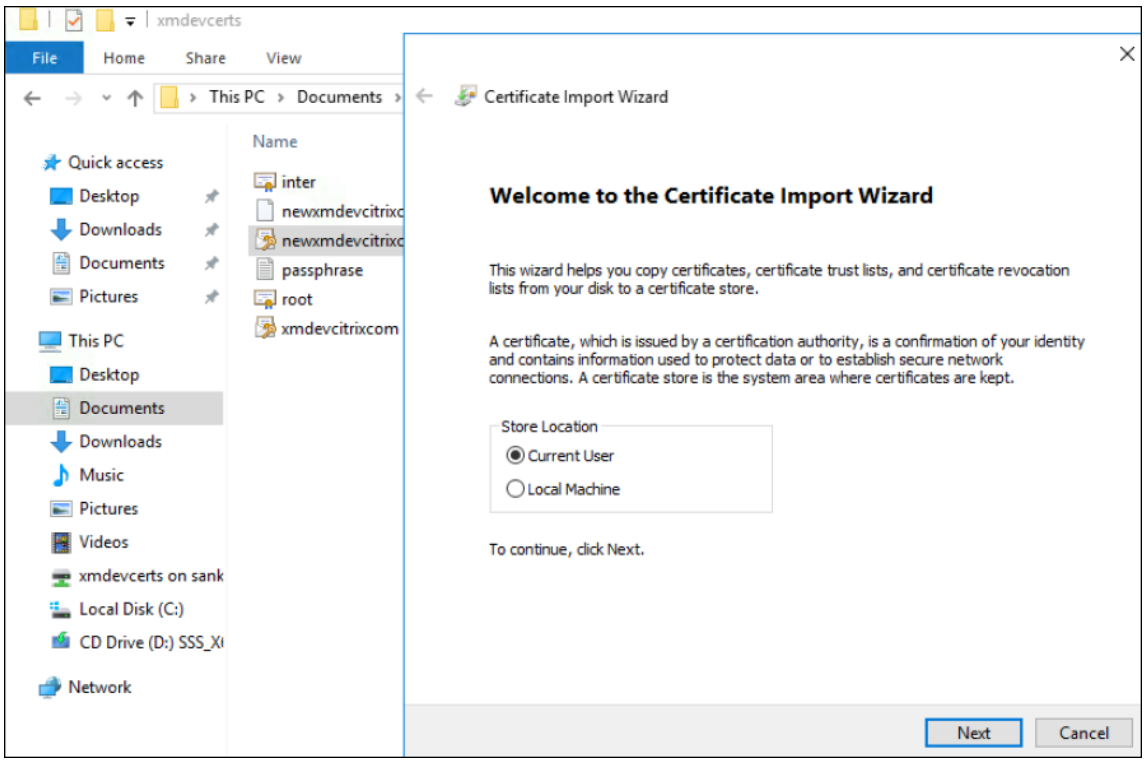
向 **Windows Server** 中添加 **DHA** 服务器角色

1. 在 Windows Server 中，如果尚未打开服务器管理器，请单击开始，然后单击服务器管理器。
2. 单击添加角色和功能。
3. 在开始之前页面上，单击下一步。
4. 在选择安装类型页面上，单击基于角色或基于功能的安装，然后单击下一步。
5. 在选择目标服务器页面上，单击从服务器池中选择服务器，选择服务器，然后单击下一步。
6. 在选择服务器角色页面上，选中“设备运行状况证明”复选框。
7. 可选：单击添加功能以添加所需的其他角色服务和功能。
8. 单击下一步。
9. 在选择功能页面上，单击下一步。
10. 在 **Web** 服务器角色 **(IIS)** 页面上，单击下一步。
11. 在选择角色服务页面上，单击下一步。
12. 在设备运行状况证明服务页面上，单击下一步。
13. 在确认安装选项页面上，单击安装。
14. 安装完成后，单击关闭。

向服务器的证书存储中添加 **SSL** 证书

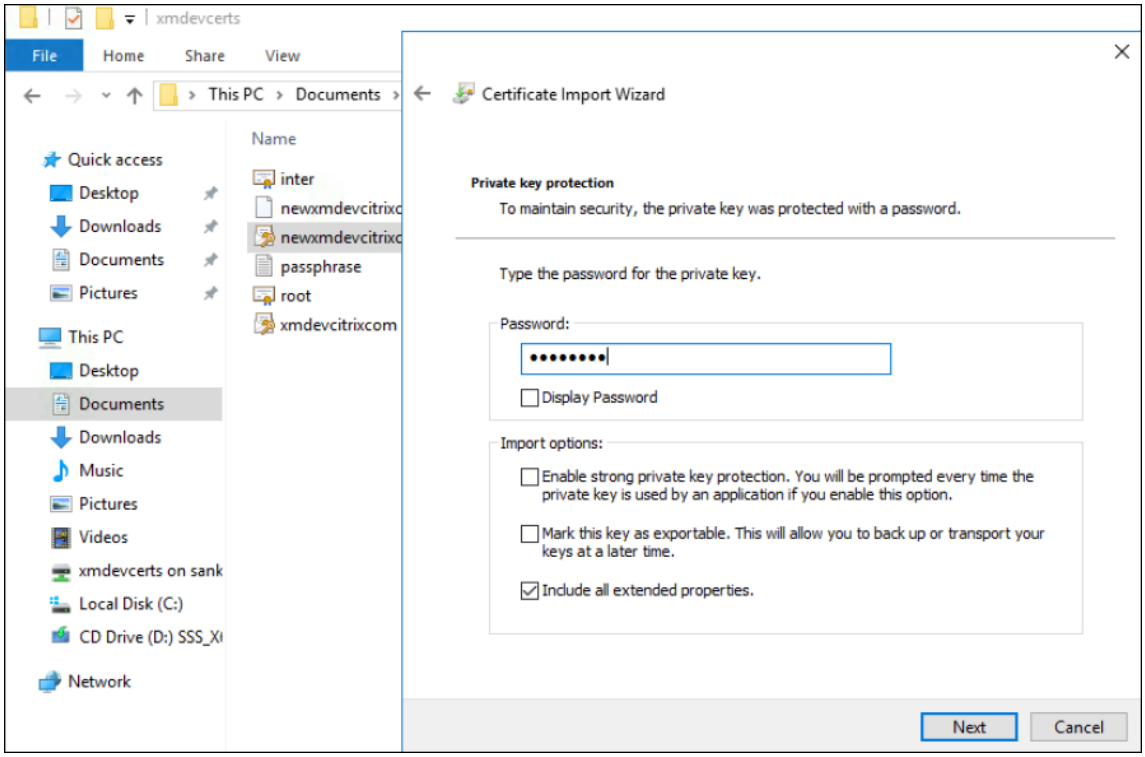
1. 转至 SSL 证书文件并选择该文件。
2. 对于应用商店位置，请选择当前用户，然后单击下一步。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



3. 键入私钥对应的密码。

4. 确保选中导入选项包括所有扩展属性。单击下一步。



5. 显示此窗口时，单击是。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



6. 确认证书是否已安装：

   a) 打开命令提示窗口。

   b) 键入 `mmc` 并按 Enter 键。您必须是管理员角色，才能查看本地计算机存储中的证书。

   c) 在“文件”菜单中，单击添加/删除管理单元。

   d) 单击添加。

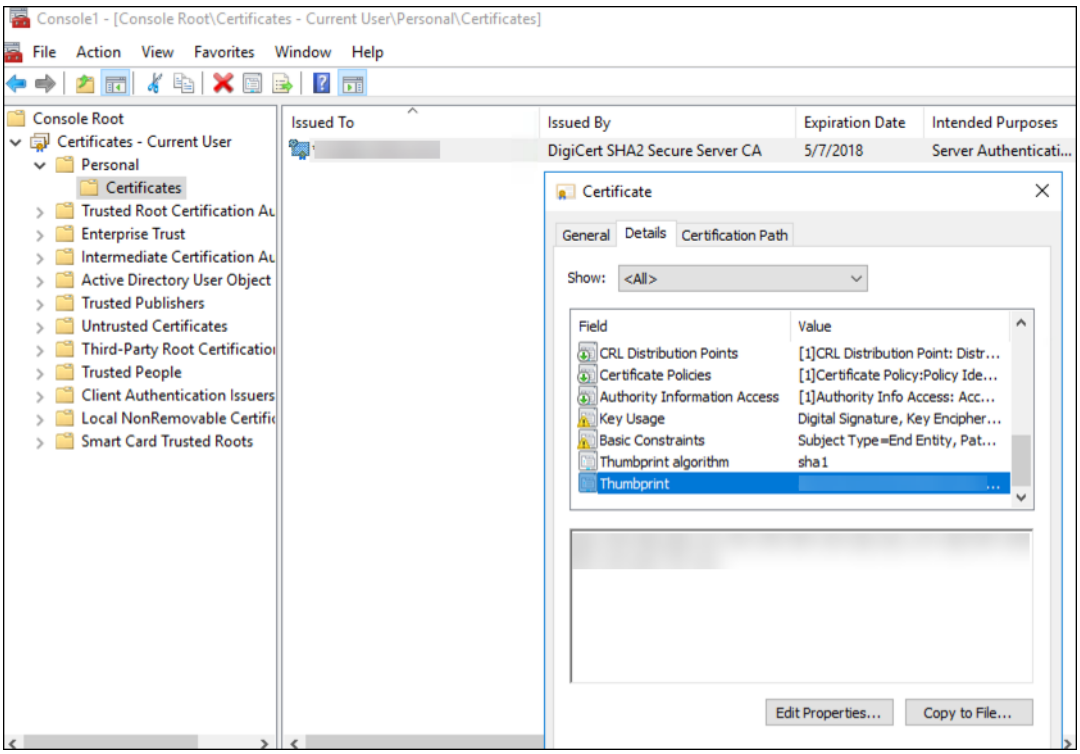
   e) 在“添加独立管理单元”对话框中，选择证书。

   f) 单击添加。

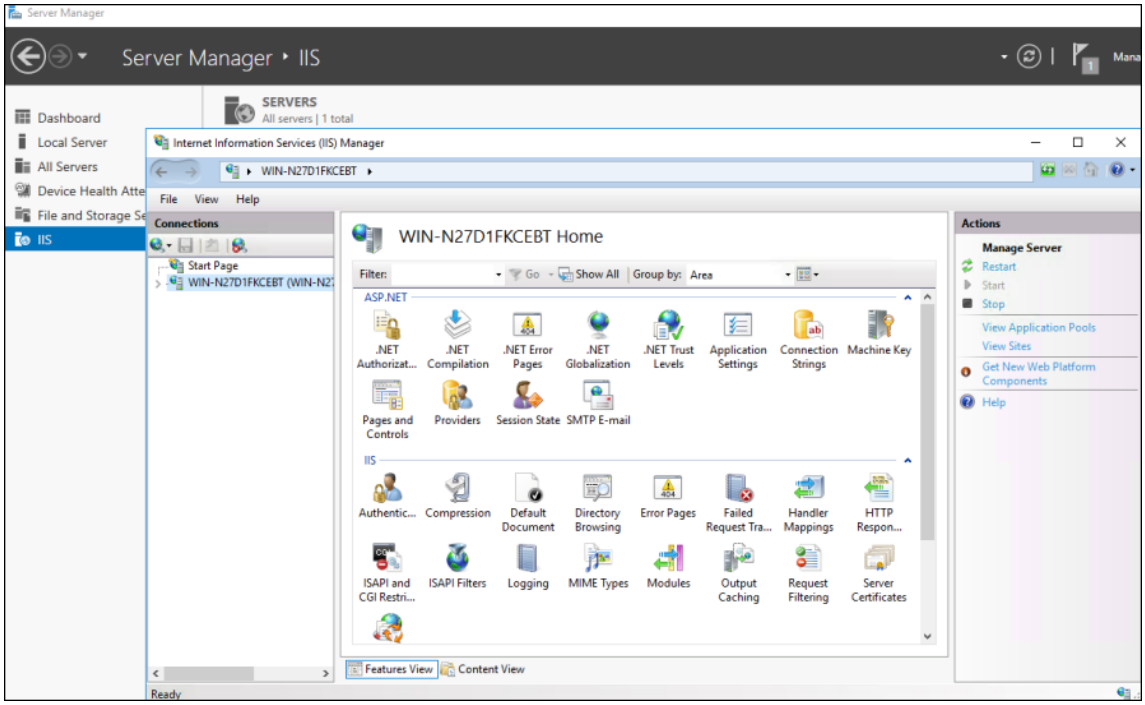
   g) 在“证书管理单元”对话框中，选择“ 我的用户帐户”。（如果您以服务帐户所有者的身份登录，请选择服务帐户。）

   h) 在“选择计算机”对话框中，单击完成。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

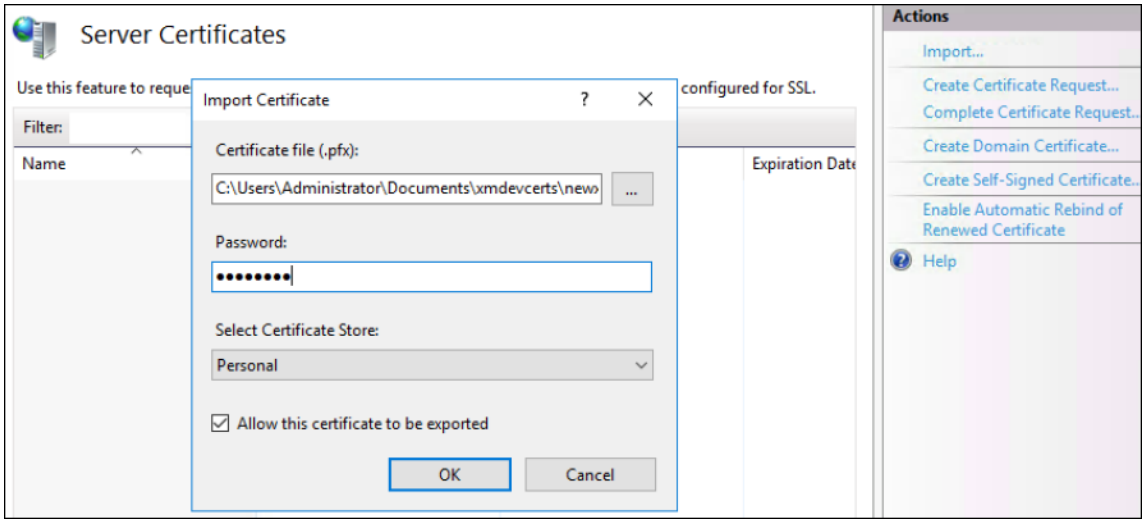


7. 转至服务器管理器 **> IIS**，然后从图标列表中选择服务器证书。



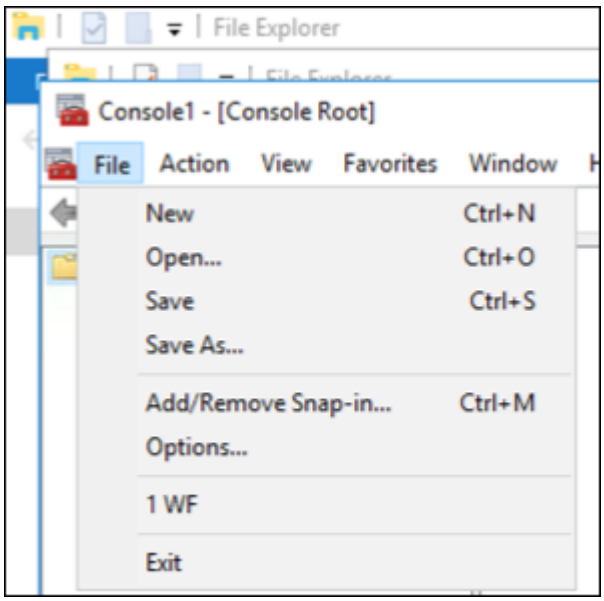
8. 在“操作”菜单中，选择导入**...** 以导入 SSL 证书。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



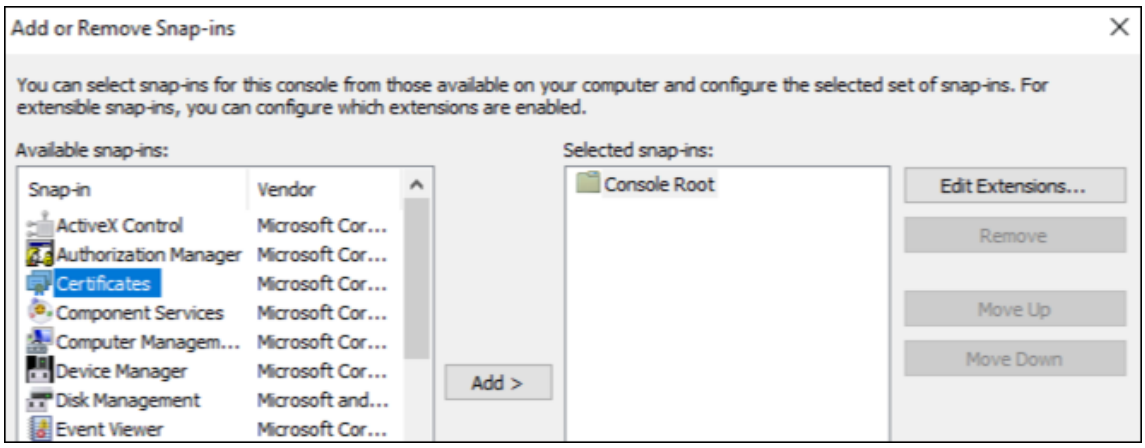
获取并保存证书的指纹

1. 在“文件资源管理器”搜索栏中，键入 mmc。
2. 在“控制台根节点”窗口中，单击文件 **>** 添加/删除管理单元。

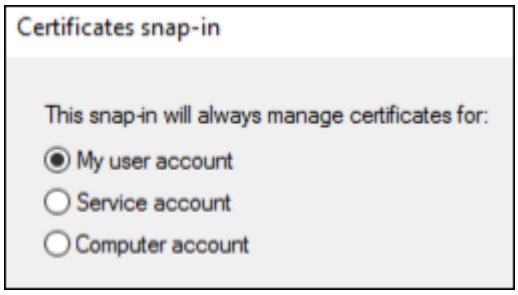


3. 从可用管理单元中选择证书并将其添加到选定的管理单元中。

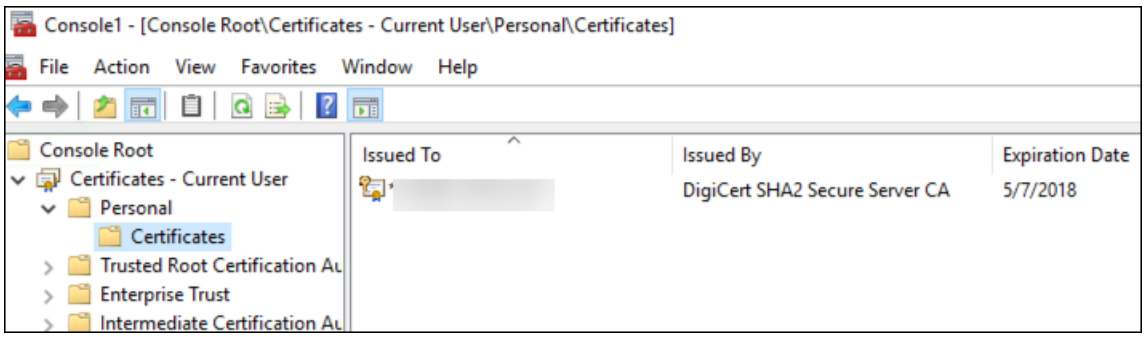
© 1999–2023 Cloud Software Group, Inc. All rights reserved.



4. 选择我的用户帐户。

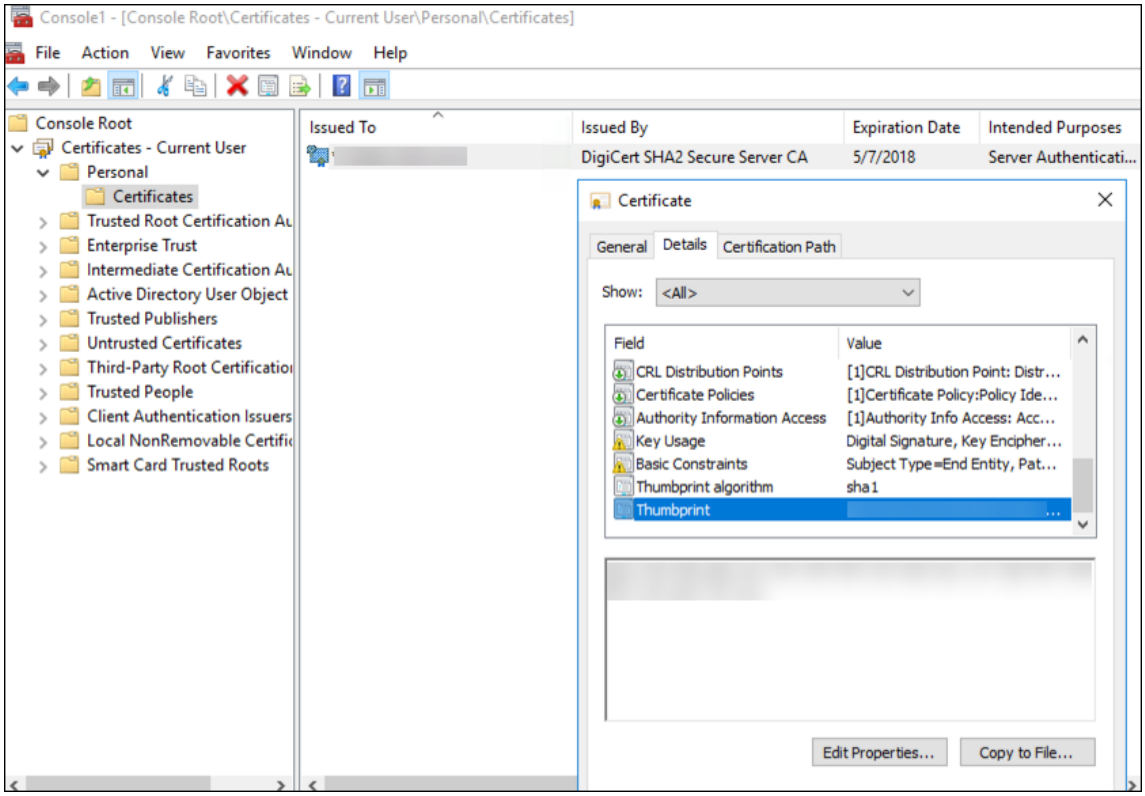


5. 选择证书，然后单击确定。



6. 双击证书并选择详细信息选项卡。向下滚动以查看证书指纹。

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



7. 将指纹复制到文件中。在 PowerShell 命令中使用指纹时，请删除空格。

安装签名证书和加密证书

在 Windows Server 上运行以下 PowerShell 命令以安装签名证书和加密证书。

替换占位符 ReplaceWithThumbprint 并在两边加双引号，如下所示。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
    $keyname icacls $keypath /grant IIS_IUSRS`:R

<!--NeedCopy-->
```

提取 **TPM** 根证书并安装可信证书包

在 Windows Server 上运行以下命令：

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

配置 **DHA** 服务

在 Windows Server 上运行以下命令以配置 DHA 服务。

替换占位符 ReplaceWithThumbprint。

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

在 Windows Server 上运行以下命令以为 DHA 服务设置证书链策略：

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

响应以下提示，如下所示：

```
  Confirm

    Are you sure you want to perform this action?

    Performing the operation "Install-DeviceHealthAttestation" on
       target "[Machine Name]".

```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
       Help (default is "Y"): A

    Adding SSL binding to website 'Default Web Site'.

    Add SSL binding?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

    Add application pool?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding web application 'DeviceHealthAttestation' to website '
       Default Web Site'.

    Add web application?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding firewall rule 'Device Health Attestation Service' to allow
       inbound connections on port(s) '443'.

    Add firewall rule?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Setting initial configuration for Device Health Attestation Service
       .

    Set initial configuration?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Registering User Access Logging.

    Register User Access Logging?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
<!--NeedCopy-->
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

检查配置

要检查 DHASActiveSigningCertificate 是否处于活动状态，请在服务器上运行以下命令：

```
Get-DHASActiveSigningCertificate
```

如果证书处于活动状态，则将显示证书类型（签名证书）和指纹。

要检查 DHASActiveSigningCertificate 是否处于活动状态，请在服务器上运行这些命令

替换占位符 ReplaceWithThumbprint 并在两边加双引号，如下所示。

```
1 Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
      -Force
2
3 Get-DHASActiveEncryptionCertificate
4 <!--NeedCopy-->
```

如果证书处于活动状态，则将显示指纹。

要执行最终检查，请转至以下 URL：

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

如果 DHA 服务正在运行，则将显示 “Method not allowed”（方法不允许）。



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

© 2023 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).