Citrix 端点管理

Citrix Endpoint Management 是一种用于管理端点的解决方案，提供移动设备管理 (MDM) 和移动应用程序管理 (MAM) 功能。借助 Citrix 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。通过对身份、设备、应用程序、数据和网络实施严格的安全保护，您的业务信息将受到保护。

Citrix® 和客户职责

Citrix 云运营处理各种基础架构和监控任务。因此，您可以专注于用户体验以及设备、应用程序和策略的管理。

Citrix 职责：

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

客户职责：

- NetScaler 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/活动目录
- DNS
- ShareFile：初始 ShareFile 配置、本地存储区域控制器安装、Citrix Files 更新
- Citrix Endpoint Management 配置：设备、策略、应用程序、交付组、操作和客户端证书

与微软端点管理器集成

Citrix Endpoint Management 与 Microsoft Endpoint Manager (MEM) 集成。该集成将 Citrix Endpoint Management 微 VPN 的价值添加到支持 Microsoft Intune 的应用程序（例如 Microsoft Edge 浏览器）中。通过此集成，您可以：

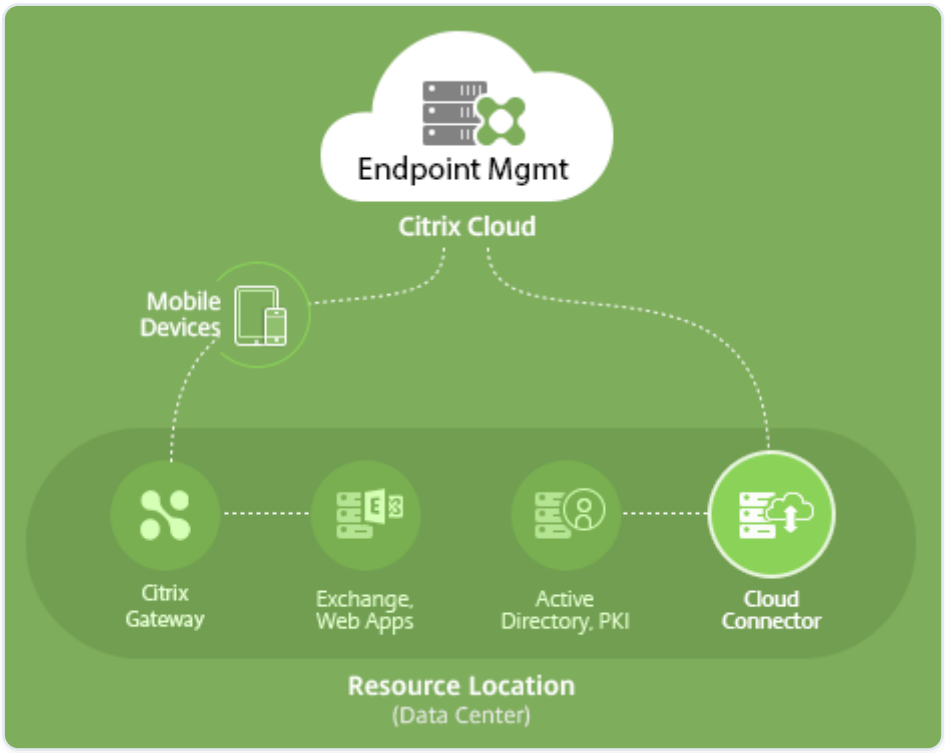
- 使用 Azure AD 条件访问保护 Office 365 应用程序。有关详细信息，请参阅与 Azure AD 条件访问集成。
- 使用 Intune 和 Citrix 封装您自己的业务线应用程序，以在 Intune 移动应用程序管理 (MAM) 容器内提供微 VPN 功能。
- 在一个容器中管理和交付 Office 365 应用程序、业务线应用程序和 Citrix Secure Mail。这种管理方法提供了极致的安全性和生产力。例如，您可以：
    - 阻止单个设备或操作系统
    - 根据设备、用户或用户组自定义 ActiveSync 策略
    - 在设备级别进行隔离
    - 监控单个连接或设备
    - 避免凭据和数据缓存带来的安全风险

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

Cloud Connector 和资源位置

您通过 Cloud Connector 连接到 Citrix Endpoint Management。Cloud Connector 充当 Citrix Cloud 与您的资源位置之间的通信通道。Cloud Connector 实现了云管理，无需复杂的网络或基础结构配置，例如 VPN 或 IPsec 隧道。

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



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

思杰端点管理入门

提示：

XenMobile® 迁移服务

如果您正在使用本地 XenMobile Server，我们的 XenMobile 迁移服务可以帮助您开始使用 Citrix Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 无需重新注册设备。

有关详细信息，请联系您当地的 Citrix 销售人员、系统工程师或 Citrix 合作伙伴。

要了解有关我们迁移服务的更多信息，请参阅 迁移到 Citrix Endpoint Management 服务的 3 个理由。

要了解迁移的原因、方法以及迁移到 Citrix Endpoint Management 的优势，请访问 CEM 迁移服务课程目录，或参阅 Citrix Endpoint Management (CEM) 迁移服务 指南。

> 当您评估或购买 Citrix Endpoint Management 时，Citrix Endpoint Management 运营团队会提供持续的入门帮助。运营团队还会与您沟通，以确保核心 Citrix Endpoint Management 服务正常运行并正确配置。此图显示了入门步骤。



要注册 Citrix 帐户并申请 Citrix Endpoint Management 试用版，请联系您的 Citrix 销售代表。准备好继续时，请访问 https://onboarding.cloud.com。

有关 Citrix Endpoint Management 入门和配置的快速概述，请观看此视频。

<iframe src="https://www.youtube.com/embed/ycFLYxn7aII" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
在开始之前想了解更多信息？请尝试以下资源：

Citrix Endpoint Management 文档： 提供完整的 Citrix Endpoint Management 文档，从入门到初始配置再到高级配置。一篇“新增功能”文章介绍了新功能和修复。当该文章有新版本可用时，Citrix 会通知您。

Citrix Endpoint Management 入门手册：整合了所有关于 Citrix Endpoint Management 的可用信息，以便您可以顺利地启用和部署 Citrix Endpoint Management。您可以使用该文档记录内部流程的更改，并记录您的高级和功能设计。

Citrix Endpoint Management 部署手册：规划 Citrix Endpoint Management 部署涉及许多注意事项。该手册包含针对您的 Citrix Endpoint Management 环境的建议、常见问题和用例。

SalesIQ：为我们的 Citrix 合作伙伴提供更多资源。

后续步骤

有关 Citrix Endpoint Management 入门流程的信息，请参阅入门和资源设置。

完成入门后，请参阅准备注册设备和交付资源。

弃用公告

有关即将淘汰的 Citrix Endpoint Management 功能的提前通知，请参阅弃用。

思杰端点管理支持

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

Citrix Endpoint Management 版本的滚动更新大约每两周进行一次。对于您（客户）而言，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。我们分批增量交付更新，以确保产品质量并最大限度地提高可用性。

Citrix Endpoint Management 客户直接从 Citrix Endpoint Management 云运营团队接收更新和通信。这些更新让您及时了解新功能、已知问题、已修复问题等。

Citrix 云运营团队使用最新的 Citrix Endpoint Management 滚动修补程序维护 Citrix Endpoint Management 环境。要在滚动修补程序之前获取所需的特定修补程序或修复，请联系 Citrix 技术支持。

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

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

您可能请求的更改示例包括：

- Citrix Files 与云中的 NetScaler Gateway 集成
- 更改 NetScaler Gateway 身份验证类型
- 验证与客户数据中心资源的连接
- 更改微型 VPN 的拆分隧道配置
- 由于某些服务器配置更改而重启 Citrix Endpoint Management 组件

服务级别协议

Citrix Endpoint Management 采用行业最佳实践，以实现云规模和高度服务可用性。

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

新增功能

Citrix 致力于在推出新功能和产品更新后，立即将其提供给 Citrix Endpoint Management 客户。新版本提供更多价值，因此没有理由延迟更新。

- Citrix Endpoint Management 的滚动更新大约每三个月发布一次。
- 这些更新不会导致您的实例或设备用户出现任何停机。
- 并非每个版本都包含新功能，有些更新包括修复和性能增强。

对您（客户）而言，此过程是透明的。我们首先仅将更新应用于 Citrix® 内部站点，然后逐步应用于客户环境。以波次增量交付更新有助于确保产品质量并最大限度地提高可用性。

您还会直接从 Citrix Endpoint Management 云运营团队收到 Citrix Endpoint Management 更新和通信。这些更新让您及时了解新功能、已知问题、已修复问题等。

有关更多详细信息，包括云规模和服务可用性，请参阅 Citrix Endpoint Management 服务级别协议。要监控服务中断和计划维护，请参阅 服务运行状况控制板。

思杰端点管理 26.8.0

- **支持软件更新设置设备策略中的“安装安全更新”：** iOS 设备的软件更新设置设备策略中新增了一个设置“**安装安全更新**”。此设置指定用户是否可以控制可用安全更新的自动安装。此功能适用于 iOS 18 及更高版本。默认值为“**允许**”。有关详细信息，请参阅软件更新设置设备策略。
- **支持应用程序设置设备策略：** 在“**配置(声明式)**”下添加了一个新的设备策略“**应用程序设置**”。此策略允许您使用 Apple 的声明式设备管理配置应用程序允许和拒绝列表。此策略仅支持受监督的 iOS 27 及更高版本设备。有关详细信息，请参阅应用程序设置设备策略。
- **支持外部智能设置设备策略：** 在“**配置(声明式)**”下添加了一个新的设备策略“**外部智能设置**”。此策略允许您在受监督的 iOS 26.4 及更高版本设备上管理外部 AI 集成。有关详细信息，请参阅外部智能设置设备策略。
- **支持智能设置设备策略：** 在“**配置(声明式)**”下添加了一个新的设备策略“**智能设置**”。此策略允许您在受监督的 iOS 26.4 及更高版本设备上管理 Apple Intelligence 功能。有关详细信息，请参阅智能设置设备策略。
- **支持 iOS 27：** Citrix Endpoint Management 和 Citrix Mobile 生产力应用程序现在与 iOS 27 兼容。

- **Secure Hub APNs 证书续订：** 适用于 Citrix Endpoint Management 26.5 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 November 9, 2026 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 September 18, 2027。
- **Android 旧版设备管理员模式弃用：** 从 CEM 26.8.0 开始，Citrix Endpoint Management 中弃用 Android 旧版 DA 模式。MDX 应用程序的 **Android（旧版 DA）**平台已重命名为 **Android (Citrix MAM Only)**，供仅在 Citrix MAM 模式下注册的 Android 设备使用。

CEM 26.8.0 中修复的问题

- 当分配的许可证超过 2,100 个时，用户无法通过 Secure Hub 安装可选的批量采购计划 (VPP) 应用程序，并且安装会重定向到 App Store。

Citrix 端点管理 26.5.0

- **支持 Android Enterprise 设备上的凭据管理器应用程序：** Android Enterprise 设备的限制策略中新增了一个设置“**凭据管理器应用程序**”。此设置控制应用程序是否可以充当凭据提供程序，默认设置为“**关闭**”。此功能适用于 Android 14 及更高版本，并且需要 Secure Hub 26.5.0 或更高版本。有关详细信息，请参阅限制策略。
- **支持 Android 17：** Citrix Endpoint Management 和 Citrix Mobile 生产力应用程序现在支持运行 Android 17 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。

CEM 26.5.0 中修复的问题

- 在 CEM 控制台中手动编辑设备的“**不合规**”状态不会触发合规性状态同步到 Azure AD。
- 通过 `/api/v1/application/store/{id}/platform/iphone` REST API 进行的 iOS 应用程序更新失败并显示错误 1493。
- 公共 REST API 调用（例如设备查询）在从 Citrix Cloud Secure Client 迁移到服务主体身份验证后，失败并显示错误 1001。

Citrix 端点管理 26.2.0

- **增强应用程序清单以支持 iOS 26.x 应用程序大小检索：** Citrix Endpoint Management 支持检索运行 iOS 26.x 的设备的应用程序大小信息。您可以在“**设备详细信息 > 应用程序**”下找到该信息。
- **增强的设备证书故障排除：** Citrix Endpoint Management 现在包含一个服务器端更新，以支持在 **Citrix Secure Hub** 中引入的设备证书故障排除增强功能。启用后，此功能允许最终用户直接从 **Secure Hub** 应用程序查看设备证书运行状况状态并自动修复证书问题。

要为现有用户启用此功能，客户管理员必须添加客户端属性 `aeDeviceCertRenewSupport`。有关详细信息，请参阅客户端属性。

有关客户端此功能的更多信息，请参阅设备证书故障排除增强功能。

- **支持检索 iOS 设备上与运营商网络相关的设备信息：** Citrix Endpoint Management 现在支持检索 iOS 设备上每个 SIM 卡的额外运营商网络相关设备信息。您可以在“**设备详细信息 > 属性 > 插槽 x SIM 卡信息**”下查看这些详细信息。新支持的字段包括：
  - Slot x — 运营商设置版本
  - Slot x — 当前运营商网络
  - Slot x — 当前移动国家代码（以前列在“网络信息”下）
  - Slot x — 当前移动网络代码（以前列在“网络信息”下）
  - Slot x — 是否首选数据
  - Slot x — 是否漫游
  - Slot x — 是否首选语音
  - Slot x — 标签 ID
- **支持 Microsoft Exchange Online 的 OAuth 身份验证：** Microsoft 宣布 Exchange Online 将于 March 2026 永久取消对使用客户端提交 (SMTP AUTH) 的基本身份验证的支持，并于 April 30, 2026 达到 100% 的拒绝率。 有关详细信息，请参阅 Exchange Online 将淘汰客户端提交的基本身份验证 (SMTP AUTH)。

  Citrix Endpoint Management 支持 SMTP 服务器的 OAuth 身份验证。通过选择 **Microsoft Exchange Online OAuth 2.0** 并提供所需的 **租户 ID**、**客户端 ID** 和 **客户端密钥** 来启用此功能。如果您使用 Microsoft Exchange Online，Citrix 建议切换到 OAuth 身份验证。有关配置详细信息，请参阅 通知。

CEM 26.2.0 中修复的问题

- 在 Citrix Endpoint Management 控制台中管理设备、应用程序和交付组等操作明显变慢，有时甚至失败。

思杰端点管理 25.11.0

- **Secure Hub APNs 证书续订：** Citrix Endpoint Management 25.9 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 January 4, 2026 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 November 9, 2026。

CEM 25.11.0 中修复的问题

- 当 iOS 设备对未安装的应用程序具有应用锁定策略时，设备会锁定并显示错误“引导式访问应用不可用。请联系您的管理员”，并且触摸屏会变得无响应，即使强制重启后也是如此。
- 当管理员上传应用程序文件以更新任何移动平台的现有企业应用时，更新会失败。创建新的企业应用不受影响，只有编辑现有应用会受到影响。

思杰端点管理 25.9.0

- **支持 Android 16：** Citrix Endpoint Management 和 Citrix Mobile 生产力应用程序现在支持运行 Android 16 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。
- **支持 iOS 26：** Citrix Endpoint Management 和 Citrix Mobile 生产力应用程序现在兼容 iOS 26。
- **支持旧版 MDX 策略升级通知：** 当使用旧版策略的现有 Secure Mail 和 Secure Web MDX 应用程序更新到 25.9.0 版本时，Citrix Endpoint Management 现在会显示升级警报。
- **支持基于证书身份验证的新强证书映射：** 引入了一种新的映射方法，以在颁发符合强映射要求的证书时提供更大的灵活性。Citrix Endpoint Management (CEM) 现在将 `URL=tag:microsoft.com`、`2022-09-14:sid:<user's SID>` 附加到证书的主题备用名称 (SAN)。
  - 要为现有用户启用此功能，客户管理员必须添加客户端属性 `MICROSOFT_CERTIFICATE_STRONG_MAPPING`。有关详细信息，请参阅 客户端属性。
  - 强证书映射仅在 **Windows Server 2019 及更高版本**上受支持。有关详细信息，请参阅 Microsoft 强映射。
- **支持 Apple 部署计划页面中的新 iOS 设置助理选项：** Apple 为 Apple Business Management 注册添加了一些新的 iOS 设置助理选项屏幕。以下新选项已添加到“**设置 > Apple 部署计划 > iOS 设置助理选项**”页面中。您可以配置 Citrix Endpoint Management (CEM) 以跳过这些屏幕。有关详细信息，请参阅 iOS 设置助理选项。
  - 操作按钮
  - 锁定模式
  - 智能
  - 相机按钮
- **支持 iOS 18.x 版本的新 iOS 限制：** 在 iOS 的限制策略中，已添加以下新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 iOS 18 及更高版本。默认值为“**开**”。有关详细信息，请参阅 限制策略。

  - 允许外部智能集成
  - 允许登录到外部智能集成
  - 允许邮件智能回复
  - 允许备忘录转录
  - 允许 Safari 摘要
  - 允许视觉智能摘要
  - 允许备忘录转录摘要
  - 允许 Apple 智能报告
  - 允许修改默认通话应用
  - 允许修改默认消息应用
  - 允许外部智能工作区 ID
  - 默认浏览器修改
  - 允许 FaceTime 远程控制
- **支持 iOS 17.x 版本的新 iOS 限制：** 在 iOS 限制策略中，已为 iOS 17.2 及更高版本添加了以下新设置。默认设置为 **开**。有关详细信息，请参阅 限制策略。
  - 允许实时语音邮件
- **管理配置策略文本框：** 当客户将 **Knox Service Plugin** 与 **托管配置策略** 结合使用时，**分离应用策略** 上所有文本框的最大字符长度增加到 8,192 个字符。
- **增强的 Android Enterprise 设备双 SIM 卡和 eSIM 支持：** Citrix Endpoint Management (CEM) 现在为 Android Enterprise 设备提供全面的双 SIM 卡支持，以确保与 iOS 的功能对等。此增强功能使管理员能够在设备属性中查看所有已安装的 SIM 卡和 eSIM，包括两个物理 SIM 卡、一个 SIM 卡加一个 eSIM 或两个 eSIM 的配置。此更新解决了双 SIM 卡 Android Enterprise 设备日益普及的问题，并为客户提供了对其移动设备连接选项的完整可见性，与之前为 iOS 设备提供的 eSIM 功能相匹配。此功能仅支持：
  - Secure Hub 25.7.0 或更高版本，以及
  - Android 13 或更高版本

CEM 25.9.0 中已修复的问题

- 即使未上传任何旧版 MDX 应用程序，旧版 MDX 警报仍会继续显示在 CEM 控制台上。
- 即使注册配置文件配置为 **仅 MDM**，设备注册计划 (DEP) 设备仍会继续执行 **MDM+MAM** 注册。
- 启用“**显示新视图**”功能后，即使对设备列表应用了筛选器，设备计数也会显示不正确。

- Android Enterprise 设备无法接收管理员通过 Citrix Endpoint Management™ (CEM) 发送的**注册应用**通知。
- iOS 用户无法启动 Secure Mail/Secure Web 应用程序，并且在从 Secure Mail/Secure Web 重定向到 Secure Hub 时遇到“无法打开”错误。

Citrix 端点管理 25.7.0

- **增强的用户身份验证工作流：** 使用本地 Active Directory (AD) 注册设备并随后使用 Microsoft Azure Active Directory (AAD) 与 Citrix 身份提供程序集成的用户无需重新注册。您可以将本地 Active Directory 中的帐户同步到 Microsoft Azure Active Directory。有关详细信息，请参阅用户身份验证工作流。

Citrix 端点管理 25.5.0

- **与 Apple Business Management 同步以管理设备分配：** Citrix Endpoint Management (CEM) 现在通过与 Apple Business Management (ABM) 同步来确保准确的设备分配。此更新验证只有正确分配的设备才会出现在 CEM 中，从而防止出现已从 CEM 中删除并分配给其他供应商管理解决方案的设备记录。例如，如果设备被移动到其他解决方案，它们在同步后将不再出现在 CEM 中。此功能由客户管理的租户服务器属性 `remove.unassigned.abm.devices` 控制。默认情况下，此属性设置为 **False**。有关详细信息，请参阅服务器属性。

> **注意：**
>
> 即使管理员尝试移动已注册的 Apple Business Management (ABM) 设备，它们也不会从 CEM 中删除。

- **支持声明式设备管理 (DDM)：** 引入了一项新功能“声明式设备管理支持”，以实现与 iOS 15 及更高版本中 Apple 声明式设备管理 (DDM) 的兼容性。此功能通过使用声明式数据模型，减少对序列化命令和设备轮询的依赖，从而提高性能和可扩展性。有关更多信息，请参阅利用声明式管理数据模型扩展设备。如果需要，请联系您的管理员启用此功能。

  启用 DDM 功能后，支持以下声明式设备策略：

  - Google 帐户
  - 密码
  - 软件更新强制执行
  - 软件更新设置

- 状态订阅
- 用户身份

CEM 25.5.0 中修复的问题

- 如果基于角色的访问控制 (RBAC) 管理员没有 **服务器属性** 权限，则在设备页面上切换 **显示新视图** 时会意外注销。
- 启用“显示新视图”功能后，基于角色的访问控制 (RBAC) 管理员会意外看到搜索输入框。
- 当 **部署计划** 中的 **部署条件** 设置为“仅当上次部署失败时”时，某些策略在重新注册期间未部署到 AE 设备。

Citrix 端点管理 25.3.0

- **支持设备页面上的持久筛选器：** 在新的设备页面中，所有**可筛选**选项现在都支持筛选器。这些筛选器会为登录用户跨会话保存，从而消除了管理员每次访问设备页面时重新应用相同筛选器的需要。如果取消选择相应的列，筛选器将自动删除。
- **支持在系统擦除设备时保留 eSIM：** 限制策略中添加了一项新设置 **擦除时保留 eSIM**。此设置可确保当系统因多次密码尝试失败而擦除设备，或者在 **设置 > 通用 > 还原** 中选择 **抹掉所有内容和设置** 选项时，eSIM 得到保留。此功能适用于 iOS 17.2 及更高版本，默认设置为 **关闭**。有关更多信息，请参阅限制策略。

CEM 25.3.0 中已修复的问题

- 当 MDM 证书续订失败时，旧证书会被 Citrix Endpoint Management (CEM) 标记为已吊销，阻止 Secure Hub (SH) 重新连接到服务器。结果是，即使旧证书尚未过期，SH 也无法使用它与服务器通信。
- 批量采购计划 (VPP) 应用程序图标在应用程序升级到新版本时不会更新。

Citrix 端点管理 25.1.0

- **Secure Hub APNs 证书续订：** Citrix Endpoint Management 24.10 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 February 9, 2025 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 January 4, 2026。
- **支持阻止或限制 iOS 版 Apple Intelligence：** 在 iOS 的限制策略中，已添加新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 iOS 18 及更高版本，默认设置为 **开**。有关详细信息，请参阅限制策略。新设置包括：
  - 生成式表情符号

  - 图像游乐场
  - 图像魔杖
  - iPhone 镜像
  - 个性化手写结果
  - 书写工具
  - 通话录音
  - 要隐藏的应用
  - 要锁定的应用
  - 邮件摘要
  - RCS 消息

- **支持阻止或限制 macOS 上的 Apple Intelligence：** 在 macOS 的限制策略中，已添加新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 macOS 15 及更高版本，默认设置为“**开**”。有关详细信息，请参阅限制策略。新设置包括：

  - 图像游乐场
  - iPhone 镜像
  - 写作工具
  - 允许修改媒体共享

CEM 25.1.0 中修复的问题

- 正在为 AE 设备生成大量负载证书。
- 当“**部署计划**”中的“**部署条件**”设置为“仅当上次部署失败时”时，某些策略在重新注册期间不会部署到 AE 设备。
- 当您尝试将 GEO 特定批量采购计划 (VPP) 应用程序同步到 Citrix Endpoint Management (CEM) 服务器时，同步失败，且未显示任何错误消息。即使在手动批量采购同步期间，VPP 应用程序也不会显示在 Citrix Endpoint Management 应用程序列表中。

Citrix 端点管理 24.10.0

- **使用 Azure Active Directory 基于组的管理进行身份验证：** Citrix Endpoint Management 支持通过 Azure Active Directory (AAD) 进行基于组的身份验证，允许管理员使用 AAD 组成员身份在组级别管理访问。此更新通过集中式组控制提供了更大的灵活性和增强的安全性。尽管此新功能简化了访问管理，但传统的 Citrix Identity 登录机制仍然可用，以确保向后兼容性。有关详细信息，请参阅使用 Azure Active Directory 基于组的管理进行身份验证。

- **支持阻止网络分发的第三方应用程序：** 在限制策略中，已添加新设置“**网络分发应用程序**”以阻止 iOS 设备上的网络分发第三方应用程序。此设置适用于 iOS 17.5 及更高版本。有关详细信息，请参阅限制策略。如有需要，请联系您的管理员启用此功能。
- **统一平台体验：** Citrix Endpoint Management 通过在 Citrix 产品中提供统一导航来启用统一平台体验。此功能更改了整体用户界面中导航栏的位置，并添加了一个新的左侧导航栏。
- **Citrix Endpoint Management 增强功能，支持 Windows 2022 CA 服务器：** Citrix Endpoint Management 支持以下 CA 服务器：
  - Windows 服务器 2016
  - Windows 服务器 2019
  - Windows 服务器 2022
- **“监视”选项卡已弃用：** Citrix Endpoint Management 中的“监视”选项卡将于 2024 年 10 月起弃用。有关详细信息，请参阅弃用和删除。
- **更新公共 Rest API 文档以包含设备丢失模式 API：** 已在公共 Rest API 文档中添加丢失模式 API。
- **修改 API 调用以使用 POST 正文而非 URL：** 已更新 API 调用，以便在公共 Rest API 文档中将数据包含在请求正文中，而不是 URL 中。
- **支持 Android 15：** Citrix Endpoint Management 和 Citrix Mobile 生产力应用程序现在支持 Android Enterprise 设备更新到 Android 15。有关安全和隐私优势的更多信息，请参阅Android 开发者文档。
- **支持 iOS 18：** Citrix Endpoint Management 和 Citrix Mobile 生产力应用程序现在与 iOS 18 兼容，但目前不支持所有新的 iOS 18 功能。
- **支持 macOS 15：** Citrix Endpoint Management 和 Citrix Mobile 生产力应用程序现在与 macOS 15 兼容，但目前不支持所有新的 macOS 15 功能。

CEM 24.10.0 中修复的问题

- 某些应用程序的 VPP 测试连接和 VPP 同步失败。

思杰端点管理 24.8.0

- **支持托管配置反馈（技术预览版）：** 托管配置反馈功能允许管理员从配置了托管配置策略的 Android 设备获取应用程序状态的反馈。有关详细信息，请参阅支持托管配置反馈（技术预览版）。

- **Android 设备合规性强制执行（技术预览版）：** 对于以设备所有者模式注册的 Android 设备，客户管理员可以管理设备合规性。有关详细信息，请参阅Android 设备合规性强制执行（技术预览版）。

CEM 24.8.0 中修复的问题

- 安全操作“删除所有用户”在共享 iPad 上失败。
- Citrix Endpoint Management 上的一些 iOS 公共应用程序无法在 Apple Store 中找到。
- 在 Citrix Endpoint Management 24.4.0 中，当使用 CEM 作为 SAML SSO 身份提供商 (IDP) 时，续订 SAML 证书后 SAML SSO 失败。
- 在基于证书的身份验证场景中，Secure Hub 由于证书续订失败而出现功能问题。系统管理员可能会注意到 PKI 证书的生成从未停止，尤其是在 Android 平台上。
- Secure Hub 商店中，针对启用了 MAM SDK 的新版本应用程序，更新选项不可用。

思杰端点管理 24.6.0

- **支持阻止 iOS 17.4 及更高版本上的第三方应用程序：** 在限制策略中，新增了一个设置 **替代应用商店**，以防止从网络安装替代应用商店应用程序，并防止任何已安装的替代应用商店应用程序安装其他应用程序。有关详细信息，请参阅 限制设备策略。
- **支持 Firebase Cloud Messaging 使用新的 HTTP v1 API：** Google 将于 June 21, 2024 弃用 FCM 的旧版 HTTP API。为了使 FCM 能够与新 API 良好配合，Firebase Cloud Messaging 页面中新增了一个字段 **服务帐户密钥文件**，供您上传服务帐户密钥 JSON 文件。有关详细信息，请参阅 Firebase Cloud Messaging。

CEM 24.6.0 中修复的问题

- 管理员更新 AD 组后，分配给交付组的移动应用程序最终用户将无法访问，并且用户可能会变为匿名状态。
- 当客户在 **客户端支持** 设置中直接选择 **将设备日志发送到 IT 帮助台** 时，Secure Hub 日志无法发送到 IT 帮助台。

思杰端点管理 24.4.0

- **新增 Knox Platform for Enterprise Key 设备策略：** 新增了设备策略 **Knox Platform for Enterprise Key**。此策略允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息，并使用 KPE 许可证来增强 Samsung 设备的安全性。有关详细信息，请参阅 Knox Platform for Enterprise Key 设备策略。

- **在自动注册中强制执行最低操作系统版本以完成设置：** 借助 iOS 17，MDM 现在可以在使用自动设备注册时，对注册设备强制执行最低操作系统版本。有关详细信息，请参阅 中的步骤 3(/zh-cn/citrix-endpoint-management/device-management/apple/apple-deployment-program.html#step-3-add-your-account-to-citrix-endpoint-management)。
- **支持 iOS 17 恢复服务：** 借助恢复服务功能，MDM 服务器可以向用户设备发送包含 Wi-Fi 详细信息和默认 MDM 注册配置文件的擦除命令。然后，设备会自动擦除所有用户数据，连接到指定的 Wi-Fi 网络，并使用提供的注册配置文件重新注册到 MDM 服务器。
- **支持 Samsung 增强型认证 v3：** Samsung 增强型认证 v3 改进了 Samsung Knox 设备上的 CEM 安全功能。有关详细信息，请参阅 Samsung Knox 增强型认证。
- **现代化设备注册中的排序和筛选功能：** CEM 中的列表视图目前难以导航且用户友好性较差。通过将筛选和排序选项移动到列标题，客户可以轻松组合这些功能，从而更简单直观地找到所需数据。
- **支持立即为 iOS 设备安装操作系统更新：** 在操作系统更新设备策略中，iOS 操作系统更新选项中新增了一个名为“**立即安装**”的单选按钮。此功能允许您立即为 iOS 设备安装之前下载的操作系统更新。有关详细信息，请参阅 适用于 iOS 的操作系统更新设备策略。
- **增强自动“始终开启 VPN”连接重启功能：** Citrix Secure Access 应用程序中新增了一个托管配置设置“**始终开启 VPN（可选）**”，必须将其设置为“true”才能使此增强功能可靠地用于“始终开启 VPN”配置文件。有关详细信息，请参阅 配置适用于 Android 的 Citrix SSO 协议 和 为 Citrix SSO 创建 Android Enterprise 托管配置。

CEM 24.4.0 中修复的问题

- 企业应用程序在 iOS 设备上升级后可能会报告不正确的版本号。
- 已注册的 iOS 设备在 Secure Hub 上会提示输入 UPN。

Citrix 端点管理 24.1.0

此版本解决了若干问题，有助于提高整体性能和稳定性。未添加任何新功能。

Citrix 端点管理 23.12.0

在 Android 的 802.1x 设置中添加了一个新的必填字段“域”： 在“**Android Enterprise 平台网络策略**”设置页面中，为 **802.1x EAP** 身份验证类型添加了一个新字段“**域**”。有关详细信息，请参阅 适用于 Android 的 802.1x 设置。

当前已知问题

Citrix Endpoint Management 25.9.0 中的已知问题

当管理员上传应用程序文件以更新 iOS、macOS 或 Android（旧版设备管理员）的现有企业应用程序时，更新会失败。创建新的企业应用程序不受影响，只有编辑现有应用程序会受到影响。

Citrix 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**下选择所有三种日志类型（**调试**、**管理员审计**、**用户审计**）进行下载不起作用。仅下载调试日志。作为一种解决方法，您可以单独下载每个日志，或者在隐身模式下打开浏览器，通过勾选所有三个复选框来下载所有日志。

在 Android Enterprise 中创建 Web 链接时，尝试保存带有图标的应用程序时会发生错误。此错误是 Google 服务问题。作为一种解决方法，请在不上传图标的情况下保存应用程序。

即使在弃用后，Samsung Knox/SAFE 策略在已注册设备上仍然处于活动状态，并且无法禁用或配置。解决方法是取消注册设备并重新注册。

Citrix Endpoint Management 22.4.0 中的已知问题

在“**监视**”选项卡上搜索已注册的 Active Directory 用户时，不会显示该用户的任何已注册设备。您仍然可以查看分配给用户的策略和应用程序，并使用“**管理 > 设备**”中的所有安全操作。iOS 和 Android 已注册设备均受影响。

由于 Google 服务中的问题，私有应用程序无法使用 Android Enterprise 发布。问题解决后，我们将更新文档。

Citrix Endpoint Management 21.12.0 中的已知问题

迁移到基于 Citrix Cloud 的 RBAC 后，即使管理员用户在迁移前具有自定义权限，他们在 Citrix Cloud 中具有完全访问权限，在 CEM 中也获得完全访问权限。解决方法是，您可以在 Citrix Cloud 身份和访问管理页面上使用所需的访问权限更新管理员权限。

2018 年之前加入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。这些权限包括更改本地用户的密码。要解决此问题，您可以致电支持人员以阻止对控制台的直接本地管理员访问，仅允许 Citrix Cloud 管理员访问。

Citrix Endpoint Management 21.11.0 中的已知问题

在仅注册 MAM 的 iOS 设备上，企业应用程序无法安装。

当 CEM 服务器升级到 21.11.0 时，Android Enterprise 的“**自动更新托管应用程序**”策略无法应用于设备。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。

Citrix 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。我们已向 Microsoft 报告此问题，并正在与他们合作解决。我们将提供任何进展的更新。

Citrix Endpoint Management 21.9.1 中的已知问题

在以公司拥有的设备模式注册工作资料的 Android 设备上：用户可能会看到错误，提示他们无法在其个人资料上安装或搜索应用程序。如果他们看到这些错误，请更新 Google Play 商店应用程序并重试。

Citrix Endpoint Management 21.5.0 中的已知问题

用户无法向 Azure Active Directory (AAD) 进行身份验证，如果他们：

1. 使用 AAD 凭据将其设备注册到 Citrix Endpoint Management。
2. 启动 Office 365 应用程序并完成 AAD 注册。
3. 从 Microsoft Authenticator 应用程序中删除其帐户。
4. 启动 Office 365 应用程序并注销。

解决方法是，从 Citrix Endpoint Management 中取消注册设备，然后重新注册。

Citrix 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该设备上注册的用户是不同的 Azure Active Directory 用户，则 iOS 设备上的重新注册会失败。解决方法是，在重新注册之前，从设备上的 Microsoft Authenticator 应用程序中注销原始用户。

Citrix Endpoint Management 21.2.0 中的已知问题

将 Citrix Secure Web 添加为 Android Enterprise 的 MDX 应用程序时，托管 Google Play 无法使用应用程序标识符找到该应用程序。如果搜索“Citrix Secure Web”而不是应用程序标识符，托管 Google Play 可以找到该应用程序。此问题是 Google 的一个错误。

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。

Citrix 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 Citrix Endpoint Management 未启用 Workspace：单点登录到 Citrix Files 或 ShareFile 域 URL 会导致错误。用户无法登录。此错误仅在使用“**公司员工登录**”选项的浏览器中发生。

要解决此问题：如果您尚未在 NetScaler Gateway 上从 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
- 受影响的 SSO 配置(/zh-cn/citrix-adc/current-release/aaa-tm/single-sign-on-types/enable-sso-for-auth-pol.html#impacted-sso-configurations)

完成此变通办法后，用户可以使用浏览器中的“**公司员工登录**”选项通过 SSO 身份验证登录 Citrix Files 或 ShareFile 域 URL。

Citrix Endpoint Management 20.2.1 中的已知问题

在 Citrix Endpoint Management 控制台中配置带有 ShareFile URL 的 ShareFile 后，单击“**测试连接**”按钮会导致错误。要解决此问题，请禁用 ShareFile 的多重身份验证。在此 重置用户电话号码以进行两步验证 中了解有关此问题和变通办法的更多信息。

Citrix Endpoint Management 20.1.0 中的已知问题

在 Citrix Cloud 中向库添加用户时，Citrix Endpoint Management 报告成功，但用户未添加。

Citrix Endpoint Management 19.11.0 中的已知问题

无法从控制台删除 MDX 和公共应用程序。作为变通办法，选择要删除的应用程序，然后单击“**编辑**”。取消选择 **Android Enterprise**，然后从平台列表中选择任何其他平台。保存应用程序。然后即可删除该应用程序。

Citrix Endpoint Management 19.5.0 中的已知问题

注册 Citrix Ready® 工作区中心设备时，请在允许列表中定义以太网 (eth0) MAC 地址，以避免注册失败。

Citrix Endpoint Management 19.4.1 中的已知问题

在 Windows GPO 设备策略中通过 Tab 键切换选项时，会跳过单选按钮和复选框。

Citrix Endpoint Management 19.2.1 中的已知问题

如果您通过 Google 管理控制台删除 Android Enterprise 企业版来取消注册它：尝试重新注册该企业版可能会失败。请始终使用 Citrix Endpoint Management 控制台取消注册 Android Enterprise 企业版，如 取消注册 Android Enterprise 企业版 中所述。Google Workspace 客户请按照 取消注册 Android Enterprise 企业版 中的说明进行操作。

Citrix Endpoint Management 19.2.0 中的已知问题

在 Citrix Endpoint Management 10.18.3 中创建公共商店应用程序时：在 iPad 应用程序设置页面上，如果您在未搜索应用程序的情况下单击“**返回**”，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。此问题在为 iOS 或 Android 创建公共商店应用程序时都会发生。

Citrix 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：`A configuration error occurred. Please try again`。当您关闭错误消息时，您的 Android Enterprise 配置已保存，但“**启用 Android Enterprise**”处于“**关闭**”状态。要解决此问题，请将应用程序类别数量减少到 30 个或更少。

Citrix Endpoint Management 10.18.5 中的已知问题

当 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才能安装该应用程序。此第三方问题是 Google 错误 ID #76022819。

Citrix Endpoint Management 10.18.3 中的已知问题

删除已注册设备的 Citrix Cloud 管理员后：Citrix Endpoint Management 不会更新 Citrix Endpoint Management 控制台中的用户角色，直到管理员从 Citrix Secure Hub 应用程序或自助服务门户再次登录。

Citrix Endpoint Management 10.7.4 中的已知问题

如果您使用 Citrix 身份提供程序和 Azure Active Directory 为 Citrix Endpoint Management 配置单点登录 (SSO)：当 Citrix Endpoint Management 管理员或用户被重定向到“**Azure Active Directory 登录**”屏幕时，该屏幕会显示消息“Citrix Secure Hub 的登录页面。”正确的消息应为“Citrix Endpoint Management 控制台的登录页面。”

新增功能历史记录

我们将有关旧版 Citrix Endpoint Management 的部分从 新增功能 移至本文。

思杰端点管理 23.9.0

> **注意：**
>
> 由于产品版本回滚，Citrix Endpoint Management 23.9.0 的文档更新已回滚。

思杰端点管理 23.7.0

- **Play Integrity API：** Play Integrity API 将取代 Google 即将弃用的 SafetyNet Attestation API，具体请参阅 弃用时间表。有关启用此 API 的更多信息和步骤，请参阅 启用 Play Integrity API。
- **支持 iOS 设备上的 eSIM 和双 SIM 卡功能：** Citrix Endpoint Management 现在支持 iOS 设备上的 eSIM 和双 SIM 卡功能。eSIM 支持允许您从 iOS 设备检索电话号码、IMEI、ICCID 等信息，并在 Citrix Endpoint Management UI 上显示。有关设备属性的更多信息，请参阅 设备属性名称和值。

思杰端点管理 23.6.0

支持 macOS 14 设备： Citrix Endpoint Management 现在支持使用 macOS 14 的 Apple 设备。有关详细信息，请参阅 操作系统支持列表。

此版本解决了若干问题，有助于提高整体性能和稳定性。

思杰端点管理 23.4.0

此版本解决了若干问题，有助于提高整体性能和稳定性。未添加任何新功能。

思杰端点管理 23.2.0

此版本解决了若干问题，有助于提高整体性能和稳定性。未添加任何新功能。

思杰端点管理 23.1.0

此版本解决了若干问题，有助于提高整体性能和稳定性。未添加任何新功能。

Citrix 端点管理 22.12.0

此版本解决了若干问题，有助于提高整体性能和稳定性。未添加任何新功能。

Citrix 端点管理 22.10.0

以下功能现已向商业客户推出。面向美国政府客户的版本将在三个月内开始发布。有关商业版和美国政府版产品之间的功能差异，请参阅 Citrix Endpoint Management service for US Government。

Windows 信息保护策略已删除。 有关详细信息，请参阅 Deprecation。

支持 Windows 11 22H2。 Citrix Endpoint Management 现在允许 IT 管理员使用现有 MDM 功能将 Windows 11 22H2 设备注册到 CEM。有关注册 Windows 设备的更多信息，请参阅 Windows Desktop and Tablet。

现已支持 macOS 13。 Citrix Endpoint Management 现在支持使用 macOS 版本 13 的 Apple 设备。

此版本还解决了各种问题，有助于提高整体性能和稳定性。

Citrix 端点管理 22.9.0

支持 Android 13 和 iOS 16。 Citrix Endpoint Management 现在支持 Android 13 和 iOS 16。

处理器类型和处理器架构。 CEM 控制台上的 Windows 设备现在还会显示每个设备的处理器类型和处理器架构。

此版本还解决了各种问题，有助于提高整体性能和稳定性。

Citrix 端点管理 22.7.0

此版本解决了各种问题，有助于提高整体性能和稳定性。未添加任何新功能。

修复

有时，在**故障排除和支持 > 日志**下选择所有三种日志类型（**调试**、**管理员审核**、**用户审核**）进行下载不起作用。仅下载调试日志。作为一种变通方法，您可以单独下载每个日志，或者在隐身模式下打开浏览器，通过选中所有三个复选框来下载所有日志。

在 Android Enterprise 中创建 Web 链接时，尝试保存带有图标的应用程序时发生错误。这是 Google 服务问题。作为一种变通方法，保存应用程序时不要上传图标。

即使在弃用后，Samsung Knox/SAFE 策略在已注册设备上仍然处于活动状态，并且无法禁用或配置。作为一种变通方法，取消注册并重新注册设备。

思杰端点管理 22.6.0

添加了新的限制策略，以允许设备上所有配置文件使用非 Google Play 应用程序。 有关更多详细信息，请参阅 限制设备策略。

弃用了对移动服务提供商 (MSP) 接口的支持。 添加了一个新的服务器属性，可从控制台中删除 MSP 接口。有关详细信息，请参阅 服务器属性。

弃用了对 Nexmo SMS 网关的支持。 通过添加名为 deprecate.carrier.sms.gateway 的服务器属性（默认设置为 True），弃用了对 Nexmo SMS 的支持。Nexmo SMS 也已在自助服务门户中弃用。有关详细信息，请参阅 通知。

现在，所选应用程序可以在 Android Enterprise 的工作和个人配置文件之间进行通信。 Android Enterprise 的限制策略中提供了一个名为“启用连接的应用程序”的新切换开关，允许所选应用程序同时使用工作和个人数据。有关详细信息，请参阅 限制策略。

Google 正在弃用 Citrix Endpoint Management 中用于应用程序类别和许可证的多个 API：

- 现在，您可以选择要添加的应用程序，而不是批准它们。请参阅 托管应用商店应用程序。
- 现在，您可以将应用程序组织到集合中，而不是 Android Enterprise 的类别中。请参阅 组织应用程序 (Android Enterprise)。
- 您不再需要批准 MDX 应用程序。请参阅 添加 MDX 应用程序。
- 您不能再将应用程序许可证与用户解除关联。请参阅 添加应用程序。

思杰端点管理 22.5.0

已删除对 Windows 10 设备“允许自动连接到 WiFi Sense 热点”限制策略的支持。 有关详细信息，请参阅 Windows 桌面/平板电脑设置。

本次发布还解决了许多有助于提高整体性能和稳定性的问题。

思杰 端点管理 22.4.0

在操作系统更新设备策略中添加了一个新选项，用于设置冻结期，在此期间无法安装操作系统更新。 有关详细信息，请参阅 操作系统更新设备策略。

本次发布还解决了许多有助于提高整体性能和稳定性的问题。

思杰 端点管理 22.3.0

现在可以自动删除在设定时间内处于非活动状态的设备。(预览版) 添加了一个新的预览版服务器属性，名为 **允许删除在指定时间内标记为非活动状态的设备**，该属性将运行一个后台作业来删除在指定时间（天）内处于非活动状态的设备。有关详细信息，请参阅 服务器属性。

本次发布还解决了许多有助于提高整体性能和稳定性的问题。

思杰 端点管理 22.2.0

在应用程序清单设备策略中添加了一条注释，指出在使用 Windows 11 设备时，必须等待 24 小时才能显示清单结果。 有关详细信息，请参阅 应用程序清单设备策略。

为 Android Enterprise 的“系统更新策略”添加了“默认”选项，允许管理员将系统更新策略恢复为其默认值。 有关详细信息，请参阅 操作系统更新设备策略。

添加了新的限制策略，以允许设备上所有配置文件使用非 Google Play 应用程序。 有关详细信息，请参阅 限制设备策略。

已删除对以下功能的支持：

- **RBAC 角色 - 共享和 COSU 设备注册器**
- **安卓 - 索尼 和 宏达电**
- **高安全性注册模式**
- **派生凭据**
- **SEAMS**
- **Windows Phone 设备** 有关详细信息，请参阅弃用。

添加了新的限制策略，以限制从个人配置文件复制、粘贴和导入文件到工作配置文件。 有关详细信息，请参阅限制设备策略。

Citrix 端点管理 22.1.0

此版本解决了许多有助于提高整体性能和稳定性的问题。未添加任何新功能。

Citrix 端点管理 21.12.0

支持使用 Citrix Identity Provider 注册已启用 Apple 部署计划的 iOS 设备。 通过 Apple 部署计划部署 iOS 设备时，您现在可以启用 Apple Business Manager 用户使用 Citrix Identity Provider 作为身份提供程序来注册其设备。此功能支持通过 Citrix Cloud 使用 Azure Active Directory 和 Okta 进行身份验证。有关详细信息，请参阅通过 Apple 部署计划部署设备。

默认情况下允许用户在 iOS 上配置和使用代理。 拥有 iOS 设备的用户现在可以默认使用其设备上配置的代理。要阻止使用客户端代理，请将此功能的客户端属性更改为 **false**。有关此设置的详细信息，请参阅客户端属性。

为 iOS 设备添加了蓝牙设备策略。 您现在可以配置蓝牙设备策略，以在受监管的 iOS 设备上启用或禁用蓝牙。有关此设置的详细信息，请参阅蓝牙设备策略。

Citrix Endpoint Management 21.12.0 中修复的问题

当 CEM 服务器升级到 21.11.0 时，Android Enterprise 的**自动更新托管应用**策略无法在设备上应用。策略失败会影响设备上的应用更新。作为一种解决方法，管理员可以编辑并保存策略以刷新默认值。

Citrix 端点管理 21.11.0

为自动更新 Android Enterprise 托管应用配置优先级。 您现在可以指定 Android Enterprise 托管应用是以低优先级还是高优先级自动更新。您还可以推迟自动更新。有关详细信息，请参阅自动更新托管应用设备策略。

应用通知设备策略支持分组类型和预览类型设置。 通过这两个设置，您可以控制应用通知在受监管的 iOS 设备上的分组和预览方式。有关详细信息，请参阅应用通知设备策略。

应用程序属性设备策略支持更多 iOS 应用程序属性。 您现在可以为安装在 iOS 设备上的应用程序指定以下属性：

- **可移除应用程序：** 指定当应用程序是托管应用程序时，用户是否可以移除它。适用于 iOS 14 及更高版本。

关联域功能的属性：

- **关联域：** 指定要添加到应用程序的关联域。适用于 iOS 13 及更高版本。
- **启用关联域直接下载：** 指定是否直接在域上启用声明的站点关联验证。适用于 iOS 14 及更高版本。

有关详细信息，请参阅 应用程序属性设备策略。

Citrix Endpoint Management 21.11.0 中的已修复问题

有时，当您单击“**导出配置脚本**”从“**设置 > NetScaler Gateway**”页面时，您会收到一个损坏的 CSV 文件。作为一种解决方法，请在添加或编辑 NetScaler Gateway 配置时下载配置脚本。

思杰端点管理 21.10.1

延长不活动后锁定设备的时间。 设备锁定前最长不活动时间已增加到 15 分钟。有关详细信息，请参阅 密码设备策略。

添加了从 iOS 应用程序粘贴内容的限制设置。 限制设备策略现在支持 iOS 的“**要求托管粘贴板**”功能。通过此限制设置，您可以阻止或允许将内容从托管应用程序粘贴到非托管应用程序，反之亦然。

此设置适用于 iOS 15 及更高版本。有关详细信息，请参阅 iOS 限制设备策略。

Citrix Endpoint Management 21.10.1 中的已修复问题

使用 WPA2 和 WPA3 网络安全类型的网络策略无法部署到 iOS 和 macOS 设备。

思杰端点管理 21.10.0

在 Citrix Cloud 中为云管理员分配自定义角色。 在 October 4, 2021 之后加入的 Citrix Endpoint Management 新客户现在可以在 Citrix Cloud 中为云管理员分配自定义角色。以前，您必须在 Citrix Endpoint Management 中分配自定义角色。此功能允许您执行与管理员相关的自定义，而无需在 Citrix Cloud 和 Citrix Endpoint Management 之间切换。此外，**COSU devices enroller** 和 **Shared devices enroller** 模板已从 Citrix Endpoint Management 中删除。**COSU devices enroller** 现在通过注册配置文件处理，**Shared devices enroller** 在平台级别通过自助服务终端模式或 Citrix Launcher 处理。

支持 Windows 11 设备。 您现在可以使用 Citrix Endpoint Management 管理 Windows 11 设备。有关详细信息，请参阅操作系统支持列表。

iOS 用户注册模式现已作为公共预览版提供。 您现在可以在 iOS 和 iPadOS 设备上利用 Apple 用户注册功能。用户注册集成了托管 Apple ID，以在设备上创建用户身份。有关用户注册的更多信息，请参阅托管 Apple ID。

更新了跟踪 iOS 设备位置的最大值。 您现在可以将位置策略配置为跟踪 iOS 设备的位置长达 10 小时。请参阅位置设备策略。

Citrix Endpoint Management 21.10.0 中已修复的问题

在 Citrix Cloud 控制台中更新管理员角色时，更改不会反映在 Citrix Endpoint Management 控制台中。此问题严格来说是一个用户界面问题，不影响任何功能。只有在 21.10.0 或更高版本中加入的客户会受到影响。

为 Android 设备创建注册配置文件以在企业拥有的设备模式下注册工作配置文件时，必须启用 **BYOD 工作配置文件**设置。如果未启用此设置，设备将无法注册。

Citrix 端点管理 21.9.1

将 Azure AD 或 Okta 配置为身份提供程序，以在没有 Cloud Connector 的情况下注册和管理用户设备（预览版）。 如果您通过 Citrix Cloud 配置身份提供程序，则无需 Cloud Connector 即可在 Citrix Endpoint Management 和 Citrix Cloud 之间建立通信。Citrix Endpoint Management 仍需要 Cloud Connector 来实现以下功能：

- LDAP
- PKI 服务器

- 内部 DNS 查询
- Citrix 虚拟应用™

有关此功能的更多信息，请参阅身份提供程序身份验证。

支持 iOS 15 和 macOS 12 设备。 您现在可以使用 Citrix Endpoint Management 管理 iOS 15 和 macOS 12 设备。有关详细信息，请参阅操作系统支持列表。

适用于 Android Enterprise 的始终开启 VPN。 您现在可以为 Android Enterprise 设备启用始终开启 VPN。您还可以选择启用锁定功能。除非您将应用程序从锁定中排除，否则它们需要 VPN 连接才能访问网络。有关详细信息，请参阅VPN 设备策略。

完全托管的 Android 11+ 设备在企业自有设备模式下注册工作配置文件。 新模式进一步分离了设备上的个人配置文件和工作配置文件。此更改为组织提供了对托管配置文件的更大控制权，并为用户提供了对其个人配置文件的更多隐私。有关详细信息，请参阅 Android Enterprise。

能够为客户端应用程序设置全局同意。 您现在可以设置全局同意，这样用户就不需要在每台设备上提供同意。有关详细信息，请参阅 为 Azure AD 合规性管理配置 Citrix Endpoint Management。

现在可检测到 Azure AD 权限更改。 当 Azure AD 权限发生更改时，Citrix Endpoint Management 现在会自动发出警告，以便您可以使用 **Azure AD 合规性管理**设置批准更改。按照同意链接并单击**批准**以接受更改。以前，您必须手动启动此批准。有关详细信息，请参阅 为 Azure AD 合规性管理配置 Citrix Endpoint Management。

Citrix Endpoint Management 21.9.1 中已修复的问题

如果您向交付组添加部署规则，则资源级别（策略、应用程序、操作）的任何新部署规则或现有部署规则将不再适用。

Citrix Endpoint Management 的“导出数据”功能无法导出完整的数据集。请使用以下变通方法检索有关托管设备的数据：

- 通过导航到 **分析 > 报告 > 设备注册** 从控制台导出数据。
- 使用报告 API 导出数据。有关报告 API 的信息，请参阅 开发人员文档。

如果通过 Citrix Cloud 访问 Citrix Endpoint Management，为 macOS 添加企业应用程序会导致授权错误。作为一种变通方法，请联系支持人员并请求直接访问您的 Citrix Endpoint Management 控制台。然后，您可以为 macOS 设备添加企业应用程序。

Citrix 端点管理 21.9.0

Chrome OS 凭据策略设置（预览版）。 凭据策略设置现已可用于 Chrome OS。Chromebook 设备可以使用凭据策略来利用 Chrome 操作系统内置的证书管理功能。管理员可以上传证书颁发机构的

私有证书，用于签署和颁发客户端证书。此证书允许 Citrix Endpoint Management 创建证书并将其推送到 Chromebook 设备。有关详细信息，请参阅 凭据设备策略。

Citrix Endpoint Management 21.9.0 中已修复的问题

注册 iOS 15 或 macOS 12 设备后，MDM 配置配置文件显示为“未验证”。

Citrix 端点管理 21.8.0

支持 Android 12。 Citrix Endpoint Management 现在支持 Android Enterprise 设备更新到 Android 12。有关安全和隐私优势的摘要，请参阅 Android 文档。

支持在为 Android Enterprise 注册生成 QR 码时编辑 JSON 输出。 在为 Android Enterprise 注册生成 QR 码时，您现在可以通过直接编辑 JSON 输出将注册信息添加到 QR 码。有关详细信息，请参阅 Android Enterprise。

自动更新托管的可选应用程序。 托管的可选应用程序现在会自动接收更新。此功能包括可选企业应用程序、可选批量采购应用程序和可选公共应用程序。有关批量采购应用程序的信息，请参阅 添加 Apple 批量采购帐户。

当用户将其 macOS 设备连接到 Wi-Fi 网络时，使用 Active Directory 对用户进行身份验证。 Citrix Endpoint Management 现在支持 macOS 设备每次连接到配置的 Wi-Fi 网络时使用 Active Directory 进行身份验证。此功能仅适用于以下安全类型：

- **WEP 企业版**
- **WPA 企业版**
- **WPA2 企业版**
- **任何 (企业版)**

有关详细信息，请参阅 网络设备策略。

克隆交付组以用作新交付组的基础。 此功能允许您复制包含多个策略、应用程序和操作的复杂交付组。然后，您可以编辑副本，例如添加注册配置文件或一组新的 Active Directory 用户。有关详细信息，请参阅 克隆交付组。

Azure AD 设备合规性正式发布。 Citrix Endpoint Management 现在通过 Azure AD 条件访问策略支持 Azure AD 设备合规性。有关此功能的详细信息，请参阅 与 Azure AD 条件访问集成。

Citrix Endpoint Management 21.8.0 中已修复的问题

用户名或密码中包含某些特殊字符的用户无法注册。

Citrix 端点管理 21.7.1

此版本包含有助于提高整体性能和稳定性的增强功能。

Citrix Endpoint Management 21.7.1 中已修复的问题

当为 Citrix Endpoint Management 配置身份提供程序时，如果您不配置可选字段，最终用户将无法进行身份验证。

Citrix 端点管理 21.7.0

如果您通过 Citrix Cloud 使用 Azure Active Directory 或 Okta 进行身份验证，您现在可以为 iOS 和 Android 设备创建不同的注册配置文件。当您通过 Citrix Cloud 将 Azure Active Directory 或 Okta 配置为身份验证方法时，Citrix Endpoint Management 支持多种具有不同注册类型的注册配置文件。有关详细信息，请参阅 注册配置文件。

按设备类型和注册模式自动标记设备。如果您启用服务器属性 `enable.device.tagging`，Citrix Endpoint Management 会标记任何新注册的设备。您可以使用设备标签来部署策略和应用程序或配置交付组。Citrix Endpoint Management 会为以下设备应用标签：

- BYOD 标签
  - iOS 用户注册
  - Android Enterprise 工作配置文件
- 公司标签
  - Android Enterprise 完全托管的公司设备
  - 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

有关详细信息，请参阅 服务器属性

对于启用了工作区体验的 Citrix Endpoint Management 客户： Citrix Endpoint Management 支持通过 Citrix Workspace 应用程序注册 MDM 的用户使用 Azure Active Directory、Okta 和本地 NetScaler Gateway 进行身份验证。有关详细信息，请参阅通过 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 和通过 Citrix Cloud 使用本地 NetScaler Gateway 进行身份验证。

思杰端点管理 21.6.0

将 Wi-Fi 设备策略重命名为网络设备策略。我们将 Wi-Fi 设备策略重命名为“网络设备策略”，以支持 macOS 的以太网。 对于 macOS，除了 Wi-Fi 选项之外，您现在还具有以下以太网选项：

- 全局以太网
- 第一个活动以太网
- 第二个活动以太网
- 第三个活动以太网
- 第一个以太网
- 第二个以太网
- 第三个以太网

有关详细信息，请参阅网络设备策略。

Apple Business Manager (ABM) 和共享 iPad 的“删除所有用户”支持。 用户现在可以使用 ABM 帐户登录共享 iPad。“删除所有用户”安全操作也适用于共享 iPad。有关详细信息，请参阅共享 iPad 。

使用 Citrix Endpoint Management REST API 批量将证书上传到 iOS 设备。 如果逐个上传证书不切实际，请使用 Citrix Endpoint Management Server REST API 批量将证书上传到 iOS 设备。

1. 配置连接类型为**始终开启 IKEv2** 的 iOS VPN 设备策略。
2. 选择**基于设备身份的设备证书**作为设备身份验证方法。
3. 选择要使用的**设备身份类型**。
4. 使用 REST API 批量导入设备证书。

有关配置 VPN 设备策略的信息，请参阅VPN 设备策略。有关批量导入证书的信息，请参阅使用 REST API 批量将证书上载到 iOS 设备。

iOS 应用程序的全隧道模式已弃用。 从此版本开始，MDX 不再支持 Citrix iOS 移动生产力应用程序中的全隧道模式。以下选项已从“网络访问应用程序策略”中删除：

- 使用以前的设置
- 隧道 - 完全 VPN
- 隧道 - 完全 VPN 和 Web SSO

如果您正在使用**隧道 - 完全 VPN** 或**隧道 - 完全 VPN 和 Web SSO** 策略，则必须切换到**隧道 - Web SSO** 策略。如果您继续使用已弃用的策略，您的电子邮件将无法同步。有关详细信息，请参阅MDX 应用程序的 SSO 和代理注意事项。

更具信息量的证书选择。 配置 Microsoft PKI、通用 PKI、凭据策略或凭据提供程序时，证书菜单会提供更多有用的信息来区分证书。此信息包括：

- 证书名称
- 证书的生效日期
- 证书的失效日期
- 证书序列号

Citrix 端点管理 21.5.1

此版本包含有助于提高整体性能和稳定性的增强功能。

思杰端点管理 21.5.0

Citrix Secure Hub APNs 证书续订。 Citrix Endpoint Management 的 Citrix Secure Hub Apple 推送通知服务 (APNs) 证书将于 June 17, 2021 到期。此更新将续订 Citrix Secure Hub APNs 证书，该证书将于 May 7, 2022 到期。

FIPS 140-2 合规性。 Citrix Endpoint Management 服务器端组件现已符合 FIPS 140-2 标准。有关详细信息，请参阅 FIPS 14-2 合规性。

Citrix Endpoint Management 21.5.0 中的修复问题

我们提供了一个新的“Get Devices by Filters”API，它解决了以前“Get Devices by Filters”API 中的问题，并一次返回最多 100 台设备的分页结果。请参阅 Public API for REST Services PDF 中的“3.16.3 Get Devices by Filters”部分。

当您使用包 ID 搜索要添加到 Citrix Endpoint Management 控制台的 Google Play 应用程序时，强制性 **名称** 字段显示为空。您仍然可以手动输入应用程序名称。

思杰端点管理 21.4.0

Citrix 已获得 Google Android Enterprise 高级管理解决方案集的验证。请参阅 Citrix Endpoint Management 获得新的 Android Enterprise 验证。

与 Azure AD 条件访问集成（预览版）。 您现在可以配置 Citrix Endpoint Management，以将 Azure AD 条件访问支持应用于 Office 365 应用程序。此功能现已推出预览版，可让您在部署 Office 365 应用程序时向设备用户部署零信任方法。您可以使用设备状态、风险评分、位置和设备保护来

定义对托管 Android Enterprise 和 iOS 设备上的 Office 365 应用程序的访问权限。有关信息，请参阅 与 Azure AD 条件访问集成。

使用 Android 设备属性规则管理向 Android Enterprise 设备部署交付组。 如果您将多个 Android Enterprise 设备注册到同一用户，您现在可以根据设备注册配置文件或应用程序包 ID 部署交付组资源。在交付组中，使用 Android 平台的设备属性为新的或现有的 Android Enterprise 设备创建高级规则。有关详细信息，请参阅 添加交付组。

支持轮换通过 Apple Deployment Program 注册的 macOS 设备的管理员密码。 将 Apple Business Manager 帐户添加到 Citrix Endpoint Management 时，您可以指定设置以在 macOS 设备上创建管理员帐户。Citrix Endpoint Management 在“设置助理”工作流期间自动在设备上创建管理员帐户。然后，用户使用指定的信息登录其 macOS 设备。Citrix Endpoint Management 现在支持轮换该管理员帐户的密码，以增强安全性。有关详细信息，请参阅 通过 Apple Deployment Program 部署设备。

通过 Citrix Cloud 配置新的 AutoDiscovery 服务。 AutoDiscovery 服务现已托管在 Citrix Cloud 中。Citrix 迁移了所有现有的 AutoDiscovery 服务配置，且服务未中断。要访问新的 AutoDiscovery 服务或更改配置，请转到 `https://adsui.cloud.com`（商业版）或 `https://adsui.cem.cloud.us/`（政府版）。有关详细信息，请参阅 为 Citrix Endpoint Management 设置 AutoDiscovery 服务。

在新的 AutoDiscovery 服务配置中，使用 **MAM 端口** 设置而不是 **NetScaler Gateway FQDN** 将 MAM 流量定向到您的数据中心。如果您输入完全限定域名以及 NetScaler Gateway 的端口，客户端设备将使用 **MAM 端口** 设置中的配置。

当您转到 `https://adsui.cloud.com`（商业版）或 `https://adsui.cem.cloud.us/`（政府版）访问新的 AutoDiscovery 服务用户界面时，广告拦截器可能会阻止网站打开。要访问 AutoDiscovery 服务，请禁用整个网站的广告拦截器。

向 Android Enterprise 限制添加了设置。 我们向所有注册模式添加了两个设置，以更紧密地与 Google 设置保持一致并简化配置。

- **允许蓝牙共享：** 如果未选中，用户无法在其设备上建立传出蓝牙共享。
- **允许应用卸载：** 允许用户从托管的 Google Play 商店中卸载应用。

此外，我们将**允许无线升级**设置从限制策略移至操作系统更新策略。

有关这些更改的更多信息，请参阅限制设备策略和操作系统更新设备策略。

支持通过内容分发网络 (CDN) 交付 MDX 应用程序。 MDX 应用程序现已支持 CDN。为了加快应用程序下载速度，CDN 会将这些 MDX 应用程序发送到位于 Citrix Endpoint Management 服务器附近

的用户设备。使用 CDN 可以缩短应用程序下载时间。要开始使用，请参阅通过 Citrix CDN 交付 MDX 应用程序。

Citrix Endpoint Management 21.4.0 中已修复的问题

企业应用程序无法安装在运行 macOS 11.0 或更高版本的设备上，但 Citrix Endpoint Management 控制台显示它们已成功安装。

Citrix 端点管理 21.3.0

将 Android Enterprise 应用程序添加到 Intune 托管环境的简化流程。 您现在可以同时将 Android Enterprise 应用程序添加到 Citrix Endpoint Management 控制台和 Intune 控制台。有关此工作流的更多信息，请参阅将 Android Enterprise 应用程序添加到 Citrix Cloud Library。

为 Android Enterprise 注册生成二维码。 Citrix Endpoint Management 现在可以为 Android Enterprise 注册生成二维码。通过使用 Citrix Endpoint Management 控制台生成注册二维码，您可以避免可能存在恶意行为的外部站点。有关生成二维码的更多信息，请参阅创建二维码。

macOS 设备引导令牌支持。 Citrix Endpoint Management 现在支持为 macOS 设备托管引导令牌。引导令牌在设置助理工作流期间生成。通过 Citrix Endpoint Management 托管引导令牌的一个好处是，可以为 FileVault 启用远程帐户，并能够解锁 FileVault 卷。有关更多信息，请参阅引导令牌。

Citrix 端点管理 21.2.0

更新的 Citrix Launcher 应用程序允许您限制用户在 Android Enterprise 设备上访问一个或一小组应用程序。 您还可以选择为 **Citrix Launcher** 图标上传自定义徽标图像，并指定用户必须输入才能退出应用程序的密码。有关更多信息，请参阅Citrix Launcher。

iOS 和 macOS 的新设置助理选项。 您现在可以指定在用户设置 iOS 或 macOS 设备时跳过更多设置屏幕。

- iOS
  - **恢复完成：** 防止用户在设置过程中看到恢复是否完成。适用于 iOS 14.0 及更高版本。
  - **更新完成：** 阻止用户在设置过程中查看软件更新是否完成。适用于 iOS 14.0 及更高版本。
- macOS
  - **辅助功能：** 阻止用户自动听到旁白。仅当设备连接到以太网时可用。适用于 macOS 11 及更高版本。
  - **生物识别：** 阻止用户设置触控 ID 和面容 ID。适用于 macOS 10.12.4 及更高版本。

- **原彩显示：** 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。如果此设置被清除，用户必须设置触控 ID 和 Apple ID。请确保 **Apple ID** 和 **生物识别** 设置已清除。
- **屏幕使用时间：** 阻止用户启用屏幕使用时间。适用于 macOS 10.15 及更高版本。

有关配置设置选项的更多信息，请参阅通过 Apple 部署计划部署设备。

macOS PKG 文件上传现在受上传时间而非文件大小限制。 您现在可以上传更大的 PKG 文件，例如适用于 macOS 设备的 Microsoft Office。Citrix Endpoint Management 已取消之前 0.5 GB 的文件大小限制，转而限制文件上传时间。默认情况下，您必须在 100 秒内完成上传。有关更多信息，请参阅添加企业应用。

Citrix Endpoint Management 不再支持用于基于证书的身份验证的弱加密算法。 在 Citrix Endpoint Management 控制台中为凭据提供程序创建证书签名请求时，请选择更强的密码。有关已删除的签名算法列表，请参阅弃用。

Citrix Endpoint Management 21.2.0 中已修复的问题

创建用户时，会为同一用户创建两个 PKI 证书。用户可能无法通过 Citrix Secure Web 访问内部网站或通过 Citrix Secure Mail 接收电子邮件。

添加 RBAC 角色时，Citrix Endpoint Management 在执行以下操作后变得无响应：

- 将权限应用于特定用户组，然后清除 Active Directory 域复选框。
- 重复选择授权访问项或控制台功能项。

Citrix 端点管理 21.1.1

> **注意：**

> 由于中断，您的交付组历史记录可能已被删除。交付组历史记录收集已恢复。

> **全新外观。** Citrix 已使用新颜色、字体、切换开关和其他格式更改更新了 Citrix Endpoint Management 控制台。某些新的 UI 元素可能无法正确加载，直到您清除浏览器缓存并刷新。

macOS 现已提供应用程序卸载策略。 您现在可以使用应用程序卸载策略从 macOS 设备中删除托管应用程序。有关详细信息，请参阅应用程序卸载设备策略。

交付组增强功能。 您现在可以使用设备属性规则以及现有用户属性规则来管理交付组的部署。如果您为同一用户注册多个设备，您现在可以根据唯一的设备属性（例如设备所有权、型号、操作系统版本、合规性等）在交付组中创建高级筛选器。有关详细信息，请参阅添加交付组。

现在可用于创建报告的 API。 报告 API 是使用 JSON 作为查询语言的只读 API。这些 API 允许您执行以下操作：

- 创建关于应用程序版本控制、设备操作系统修补、Android DA（旧版）到 Android Enterprise 迁移进度等方面的强大合规性报告。
- 以安全的方式对您的云数据库发出自定义查询。
- 导出有关您的云服务的数据，例如应用程序、设备、用户、注册和软件列表。
- 以 JSON 或 CSV 格式保存信息。

这些 API 相当于在云中访问本地数据库并运行自定义 SQL 查询。要了解有关报告 API 的更多信息，请参阅 Citrix Developer portal 上的文档。

Citrix 端点管理 21.1.0

使用 Citrix Cloud API 密钥对 REST API 进行身份验证。 您现在可以生成唯一的客户端 ID 和客户端密钥，以使用您的 Citrix Cloud 帐户访问 REST API。有关详细信息，请参阅 REST API。

Android Enterprise 限制的重组。 Android Enterprise 的限制设置已重新组织以提高清晰度。有时，设置名称会进行细微更改。有关重组的更多信息，请参阅 Android Enterprise 设置。

Citrix 端点管理 20.12.0

此版本包含有助于提高整体性能和稳定性的增强功能。

在注册 Android Enterprise 设备时使用 Azure Active Directory (AAD) 或 Okta 进行身份验证（预览版）。 在注册 Android Enterprise 设备时使用 AAD 或 Okta 作为身份验证方法的功能现已作为预览版提供。此功能除了支持增强型注册配置文件外，还支持 BYOD 和完全托管模式。有关使用 Okta 进行单点登录的更多信息，请参阅通过 Citrix Cloud 使用 Okta 进行身份验证。有关使用 AAD 进行单点登录的更多信息，请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。

将企业和批量购买应用作为受管应用安装到 macOS 设备。“**强制应用受管**”设置现已适用于 macOS。如果要管理已安装但尚未受管的应用，请为该应用启用此设置，然后将该应用部署到设备。该应用将自动作为受管应用安装。用户不会收到任何提示。如果将应用部署到设备上不存在该应用的位置，则无论该设置的状态如何，该应用都将作为受管应用安装。有关详细信息，请参阅添加企业应用和配置批量购买应用。

Citrix Endpoint Management 20.12.0 中已修复的问题

默认通知模板使用名称 XenMobile 而不是 Citrix Endpoint Management。

Android Enterprise 用户可能无法收到注册后添加的应用。

Windows 设备的 BitLocker 加密恢复密钥在自助服务门户 (SHP) 中不可用。当您在 BitLocker 设备策略中启用“**操作系统驱动器恢复**”设置并使用 BitLocker 加密已注册的 Windows 设备时，恢复密钥不会显示在 SHP 中。作为一种解决方法，请打开 CEMHELP 工单并请求与产品管理部门进行 SRE 讨论。

Citrix 端点管理 20.11.0

移除对 Android TouchDown 的支持。 DigiCert 已于 July 2, 2018 停止支持 Android TouchDown。所有 Android TouchDown 选项已从 Citrix Endpoint Management 控制台中移除。

Citrix 端点管理 20.10.1

限制访问 REST API 的方法。 通过联系 Citrix 支持，您可以确保只有 Citrix Cloud 帐户才能访问 REST API。启用此功能后，本地管理员帐户无法访问 API。请参阅REST API。

Citrix Endpoint Management 20.10.1 中已修复的问题

用户未收到注册邀请电子邮件。

如果将 Citrix Endpoint Management 配置为自由裁量证书颁发机构，则 VPN、网络和其他凭据设备策略将无法部署。

Citrix 端点管理 20.10.0

允许静态或动态 MAC 地址。 作为网络策略的一部分，iOS 和 iPadOS 设备现在每次连接到配置的 Wi-Fi 网络时都可以使用不同的 MAC 地址。您也可以选择让 MAC 地址保持静态。但是，使用动态 MAC 地址会使设备难以持续识别，从而增强隐私。请参阅网络策略。

使用 Azure Active Directory (AAD) 或 Okta 作为身份平台。 将 AAD 或 Okta 用作身份平台的功能现已作为公共预览版提供。通过 Citrix Secure Hub 注册的用户可以使用其 AAD 或 Okta 凭据。要使用这些方法之一进行单点登录，请为基于证书的身份验证配置 NetScaler Gateway。有关使用 Okta 进行单点登录的详细信息，请参阅通过 Citrix Cloud 使用 Okta 进行身份验证。有关使用 AAD 进行单点登录的详细信息，请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。

使用 UPN 或电子邮件进行 Okta 身份验证。 将 Okta 设置为身份平台时，您可以允许用户使用其 UPN 或电子邮件地址登录。请参阅使用 Okta 进行单点登录。

Citrix Endpoint Management 20.10.0 中修复的问题

用户未收到注册邀请电子邮件。

思杰端点管理 20.9.1

将分配的策略重新部署到 iOS 和 Android 设备。 如果用户删除了策略，您现在可以将策略重新部署到 iOS 和 Android 设备。转至**管理 > 设备 > 分配的策略**，选择策略，然后单击**重置状态**以将部署状态更改为待定。有关详细信息，请参阅iOS 支持的注册方法和Android 设备支持的注册方法。

FileVault 设备策略现在允许密钥存储和轮换。 使用 FileVault 设备策略，您现在可以将个人恢复密钥存储在 Citrix Endpoint Management 中。最终用户可以使用自助服务门户请求其恢复密钥，管理员可以使用安全操作轮换个人恢复密钥。有关新功能的详细信息，请参阅FileVault 设备策略。

对 macOS 更新选项进行更精细的控制。 OS 更新设备策略现在允许您控制 macOS 设备检查、下载和安装更新的方式。您还可以配置允许的软件更新类型。有关新设置的详细信息，请参阅OS 更新设备策略。

Citrix Endpoint Management 20.9.1 中修复的问题

某些 iOS 设备上的 MDM 证书未续订。在这种情况下，**管理 > 设备 > 设备详细信息 > 证书**页面会显示一个即将过期的 Apple MDM 证书。Citrix Endpoint Management 服务器日志包含消息 **The new MDM payload does not match the old payload**。我们建议您重新注册受影响的设备以解决此问题。Citrix 技术支持可以识别要重新注册的设备，并在需要时实施临时缓解措施。

思杰端点管理 20.9.0

此版本包含有助于提高整体性能和稳定性的增强功能。

Citrix Endpoint Management 20.9.0 中修复的问题

当 Azure AD 用户登录到配置为信息亭的某些已加入 Azure AD 的 Windows 10 设备时，信息亭模式未激活。

在注册运行 macOS 10.14+ 的设备后，设备属性并非总能填充到 Citrix Endpoint Management 控制台中。重新启动设备以查看属性。

部署的资源有时在 macOS 10.14+ 设备上直到设备重新启动后才生效。

Citrix 端点管理 20.8.0

更轻松地在托管配置中使用证书别名。 在**凭据**设备策略中，将新的**证书别名**设置与 **Android Enterprise 托管配置**设备策略结合使用。这样做允许应用程序在 VPN 上进行身份验证，而无需用户操作。您无需在应用程序日志中查找凭据别名，而是创建凭据别名。通过在 **Android Enterprise 托**

管配置设备策略的**证书别名**字段中键入别名来创建别名。然后，在**凭据**设备策略的**证书别名**设置中键入相同的证书别名。请参阅托管配置策略和凭据设备策略。

密码设备策略允许您在不合规的 Android Enterprise 设备上显示应用程序和快捷方式。 适用于 Android Enterprise 的密码设备策略新增了一个设置：**当密码不合规时显示应用程序和快捷方式**。启用此设置可在设备密码不再合规时使应用程序和快捷方式保持可见。Citrix 建议您创建自动化操作，以便在密码不合规时将设备标记为不合规。请参阅密码设备策略。

控制 Android Enterprise 设备上的"使用一个锁"设置。 "**密码**"设备策略中的新设置"**启用统一密码**"可让您控制设备是否需要为设备和工作配置文件设置单独的密码。在此设置之前，用户通过设备上的"**使用一个锁**"设置来控制此行为。当"**启用统一密码**"设置为"**开**"时，用户可以为设备和工作配置文件使用相同的密码。如果"**启用统一密码**"设置为"**关**"，则用户不能为设备和工作配置文件使用相同的密码。默认设置为"**关**"。"**启用统一锁**"设置适用于运行 Android 9.0 或更高版本的 Android Enterprise 设备。请参阅密码设备策略。

Citrix Endpoint Management 20.8.0 中已修复的问题

如果您在 19.12.0 或更高版本中载入了 Citrix Endpoint Management，要删除 Android Enterprise 订阅，请从控制台取消注册 Android Enterprise。然后从 Google Play 中删除配置。如果您首先在 Google Play 商店中单击"**删除企业**"，则 Android Enterprise 订阅在 Citrix Endpoint Management 控制台中仍保持活动状态。

Citrix 端点管理 20.7.1

将注册屏幕中的配置文件名称更改为 Citrix Workspace。 当用户将其设备注册到 Citrix Endpoint Management 时，显示的配置文件名称现在是 Citrix Workspace。您可以自定义此名称并显示您的组织名称。要自定义名称，请更改新服务器属性 `apple.mdm.enrollment.profile.organization.name` 的值。请参阅服务器属性。

Citrix Endpoint Management 20.7.1 中已修复的问题

在某些云站点上，Citrix Endpoint Management 控制台的"**监视**"页面无法加载。

当您编辑 `optional.user.identity.attributes` 服务器属性中的值并保存更改时，将显示错误消息。

Citrix 端点管理 20.7.0

Citrix Endpoint Management 支持使用本地 NetScaler Gateway 进行身份验证（预览功能）。 您现在可以将本地 NetScaler Gateway 配置为通过 Citrix Secure Hub 注册的用户的身份提供程序。有关详细信息，请参阅通过 Citrix Cloud 使用本地 NetScaler Gateway 进行身份验证（预览）。

自定义可选的 Active Directory 用户属性列表。 新的服务器属性 `optional.user.identity.attributes` 使您能够删除和恢复 Citrix Endpoint Management 用于识别 Active Directory 中用户帐户的可选属性。有关详细信息，请参阅自定义 Active Directory 用户属性。

Citrix Endpoint Management 20.7.0 中的修复问题

Apple iTunes 批量购买应用无法与 Citrix Endpoint Management 同步。

使用 Citrix Cloud Connector 在 Citrix Endpoint Management 上安装多个 LDAP Active Directory (AD) 时，只有第一个安装的 AD 会填充到 Citrix Endpoint Management 设置中。作为一种解决方法，您可以检查 Citrix Cloud。如果这些域被标记为未使用，请手动将其标记为**已使用**。将域标记为已使用后，它将在 Citrix Endpoint Management 中可用。

如果您在 19.12.0（2019 年 12 月）或更高版本中加入了 Citrix Endpoint Management：添加多个 LDAP 身份验证域时，无法更改默认域。

思杰端点管理 20.6.0

如果您在 19.8.0 版本（August 1, 2019）之后加入了 Citrix Endpoint Management，请登录 Citrix Cloud 并单击 Citrix Endpoint Management 服务磁贴以访问控制台。所有在 19.8.0 之前加入的客户将很快过渡到 Citrix Cloud 登录。为了增强安全性，Citrix 建议您配置单点登录。如需帮助，请联系 Citrix 技术支持。

Citrix Endpoint Management 的 Citrix Secure Hub Apple 推送通知服务 (APNs) 证书将于 July 12, 2020 到期。因此，代理通知将失败，并且应用程序推送可能会在 iOS 设备上延迟。此更新将续订 Citrix Secure Hub APNs 证书，该证书将于 June 18, 2021 到期。

禁用在 Android Enterprise 工作配置文件或完全托管设备上打印的功能。 在“限制”设备策略中，“**不允许打印**”设置允许您指定用户是否可以打印到可从 Android Enterprise 设备访问的任何打印机。有关详细信息，请参阅Android Enterprise 设置。

配置 macOS 的连接模式和网络优先级。 在网络设备策略中，为 macOS 设备启用“**连接模式**”设置，以选择用户如何加入网络。设备可以使用系统凭据或在登录窗口输入的凭据来验证用户。如果您有多个网络，请在“**优先级**”字段中键入一个数字以设置网络连接的优先级。设备将选择数字最小的网络。有关详细信息，请参阅网络设备策略中的 macOS 设置。

启用在 iOS 设备上配置的代理。 如果您希望允许 iOS 用户使用他们在“**设置 > 网络**”中配置的代理服务器，Citrix Endpoint Management 现在要求您启用新的客户端属性 `ALLOW_CLIENTSIDE_PROXY`。有关详细信息，请参阅客户端属性参考中的 `ALLOW_CLIENTSIDE_PROXY`。

自动更新托管 Google Play 应用的托管应用策略。 此新策略允许您限制用户在 Android Enterprise 设备上为托管 Google Play 应用配置自动应用更新的功能。您可以允许用户配置策略。或者，您可以指定自动更新始终应用、从不应用或仅在设备连接到 Wi-Fi 时应用。

Citrix Endpoint Management 20.6.0 中的修复问题

在 Citrix Endpoint Management 控制台中，您无法看到 MDX 封装的 iOS 和 Android 应用的程序包 ID。

当 Citrix Endpoint Management 发送 Active Directory 组成员的查询时，身份服务会递归运行查询。这些查询会消耗更多资源。因此，拥有大量 Active Directory 用户的站点可能会遇到日常操作中断。

在 Citrix Endpoint Management 控制台中，某些应用程序的状态显示为“待定”，即使它们已安装。此限制是由于 macOS 造成的，并且特定于具有不同 pkg 和应用程序标识符的 PKG 文件。

Citrix 端点管理 20.5.0

使用 Citrix Endpoint Management 与 Microsoft Endpoint Manager 集成时，简化了 Intune 托管应用程序的配置。 配置 Intune 托管应用程序时，您不再在 Citrix Endpoint Management 控制台中设置**强制应用程序受管**选项。您现在在 EMS 控制台中设置该选项。

支持使用 Citrix Endpoint Management 与 Microsoft Endpoint Manager 集成，限制通过 Microsoft Edge 发布的 Intune 托管应用程序的 Web 内容传输。 Citrix Endpoint Management 与 Microsoft Endpoint Manager 集成支持 EMS 控制台中 Microsoft Edge 的新托管浏览器策略**限制与其他应用程序的 Web 内容传输**。

解锁本地用户帐户。 如果用户达到最大连续无效登录尝试次数，本地用户帐户将锁定 30 分钟。系统将拒绝所有进一步的身份验证尝试，直到锁定期限到期。要在 Citrix Endpoint Management 控制台中解锁帐户，请转到**管理 > 用户**，选择用户帐户，然后单击**解锁本地用户**。有关详细信息，请参阅解锁本地用户帐户。要更改失败登录尝试次数和锁定时间，请更新 **local.user.account.lockout.time** 和 **local.user.account.lockout.limit** 服务器属性。有关详细信息，请参阅服务器属性。

Citrix 内容分发网络 (CDN) 现在为 macOS (MDM 注册) 交付企业应用程序。 为了加快应用程序下载的交付速度，CDN 将 macOS 应用程序发送到全球 Citrix Endpoint Management 服务器附近的用户设备。有关详细信息，请参阅从 Citrix CDN 交付企业应用程序。

Citrix Endpoint Management 20.5.0 中已修复的问题

具有导出注册邀请的 RBAC 权限的管理员可以导出所有注册邀请，无论是否存在限制。

尝试部署 PowerShell 脚本以在 Windows 设备上触发自动化操作可能会失败，并出现 500 内部服务器错误。如果将**操作信息**页面上的**描述**字段留空并选择**策略返回值**作为触发器，则会出现此问题。要解决此问题，在使用**策略返回值**作为触发器时，请勿将**描述**字段留空。

编辑现有 iOS 限制策略时，会发生错误。

Citrix 端点管理 20.4.1

支持最新的基于 HTTP/2 的 APNs 提供程序 API。 Apple 对 Apple 推送通知服务旧版二进制协议的支持将于 March 31, 2021 结束。Apple 建议您改用基于 HTTP/2 的 APNs 提供程序 API。Citrix Endpoint Management 现在支持基于 HTTP/2 的 API。有关详细信息，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 APNs 连接的帮助，请参阅连接性检查。

本地用户帐户的密码要求。 在 Citrix Endpoint Management 控制台中添加或编辑本地用户帐户时，请确保遵循最新的密码要求。有关详细信息，请参阅添加本地用户帐户。

使用应用程序捆绑包 ID 号将应用程序添加到应用程序通知设备策略。 单击**添加新项**并在出现的字段中键入应用程序捆绑包 ID。有关详细信息，请参阅应用程序通知设备策略。

iOS 13 的设备策略更新。 iOS 13 的设备策略现在具有以下功能：

- **网络使用策略：** 我们为应用网络使用策略添加了更多功能，并将其重命名为网络使用策略。您现在还可以根据 iOS 13 设备上的 SIM ICCID 配置网络使用规则。请参阅网络使用设备策略
- **限制策略：** 您现在可以限制共享设备的临时会话、eSIM 修改、查找我的 iPhone 等。有关详细信息，请参阅限制设备策略中的 iOS 设置部分。

Citrix Endpoint Management 20.4.1 中已修复的问题

使用基于 Azure Active Directory 的身份验证和设备注册时，Android 设备用户无法注册。错误提示用户身份验证没有设备访问权限。

思杰端点管理 20.4.0

在 Citrix Endpoint Management 控制台中发布 Android Enterprise Web 应用程序。您不再需要前往托管 Google Play 或 Google 开发者门户来为 Citrix Endpoint Management 发布 Android Enterprise Web 应用程序。当您在**配置 > 应用程序 > Web 链接**中单击**上载**时，将打开一个托管 Google Play 商店 UI，供您上载和保存文件。应用程序审批和发布大约需要 10 分钟。有关详细信息，请参阅添加 Web 链接。

iOS 13 的设备策略更新。 iOS 13 的设备策略现在具有以下功能：

- **应用程序锁定策略：** 您可以启用语音控制并允许用户访问语音控制调整。请参阅应用程序锁定设备策略。
- **Exchange 策略：** 您可以启用或禁用日历、联系人、邮件、备忘录和提醒的同步。请参阅 Exchange 设备策略。
- **配置文件删除策略：** 已删除允许在 iOS 设备上删除策略的设置，因为 iOS 不再支持该功能。请参阅配置文件删除设备策略。
- **VPN 策略：** 对于以下连接协议，您现在可以包含所有网络流量或从 VPN 中排除本地网络：
  - 适用于 iOS 的 Cisco 旧版 AnyConnect 协议
  - 适用于 iOS 的自定义 SSL 协议

  对于以下连接协议，当 Wi-Fi 助理从 Wi-Fi 切换时，您现在可以允许流量通过蜂窝 VPN 隧道：
  - 适用于 iOS 的 IKEv2 协议
- **网络策略：** 您现在可以使用 WPA3 Personal 和 WPA3 Enterprise 作为**安全类型**选项。请参阅网络设备策略。

Citrix Endpoint Management 20.4.0 中已修复的问题

当使用浏览器缩放时，**分析**控制板上的数据可视化图表无法正确缩放。

当使用仅限 MAM 的注册时，用户仍然可以访问用于 MDM 的 Apple 无线注册门户。

当设备处于待机状态时，选择性擦除操作失败。

思杰端点管理 20.3.0

增强型注册配置文件已为所有客户启用

此版本为所有客户启用了在 Citrix Endpoint Management 20.2.1 中向部分客户发布的增强型注册配置文件功能。有关此功能的信息，请参阅 在单个环境中配置多种设备和应用程序管理模式。

Android 设备默认注册到 Android Enterprise

从本版本开始，Android Enterprise 是 Android 设备的默认注册选项。如果您的 Citrix Endpoint Management 部署启用了 Android Enterprise，所有新注册或重新注册的 Android 设备都将默认注册为 Android Enterprise 设备。

此更改支持 Google 对 Android 所做的更改。Google 已弃用设备管理器的设备管理模式，并鼓励客户使用 Android Enterprise 管理所有 Android 设备。（请参阅 Google Android Enterprise 开发者指南中的 设备管理员弃用。）

从 Citrix Endpoint Management 19.11.0 开始，Citrix 传达了将所有 Android 设备迁移到 Android Enterprise 所需的操作。有关 Citrix Endpoint Management 支持过渡到 Android Enterprise 的更多信息，请参阅博客 Android Enterprise 作为 Citrix Endpoint Management 服务的默认设置。

如果您的 Citrix Endpoint Management 部署包含必须继续以设备管理员模式管理的设备，请为这些旧设备创建注册配置文件。

要为旧设备创建注册配置文件：

1. 在 Citrix Endpoint Management 控制台中，转至 **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. 单击 **下一步** 或在 **平台** 下选择 **Android**。“注册配置”页面随即显示。
4. 将 **管理** 设置为 **旧版设备管理（不推荐）**。单击 **下一步**。
5. 选择 **分配（选项）**。“交付组分配”屏幕随即显示。
6. 选择包含注册专用设备的管理员的交付组或多个交付组。然后单击 **保存**。

要继续在设备管理员模式下管理旧版设备，请使用此配置文件注册或重新注册它们。您可以通过让用户下载 Citrix Secure Hub 并提供注册服务器 URL 来注册设备管理员设备，这与工作配置文件设备类似。

Citrix Endpoint Management 20.3.0 中已修复的问题

尝试按 **上次访问** 或 **非活动天数** 排序设备会导致 500 内部服务器错误。

对于使用 Amazon Web Services 和新的 Citrix 增强型注册配置文件的客户：iOS 设备无法注册。作为一种解决方法，请创建一个包含所有交付组的默认注册配置文件。请参阅 创建注册配置文件。

当您将密码设备策略部署到 macOS 设备时，该策略应用于系统级别而不是用户级别。因此，用户不会在数小时甚至数天内收到更改密码的提示。

思杰终端管理 20.2.1

在单个环境中配置多种设备和应用程序管理模式

> **关于此功能：**

> 增强型注册配置文件支持将分两个版本推出。Citrix® 会发送有关即将发布的版本的通知。

> 在为您启用增强型注册配置文件功能之前，注册配置文件仅限制用户可以注册的设备数量。

> 您现在可以配置单个 Citrix Endpoint Management 站点以支持多种注册配置。注册配置文件的作用已扩展，以包含设备和应用程序管理的注册设置。

注册配置文件在单个 Citrix Endpoint Management 控制台中支持多种用例和设备迁移路径。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 注册的能力）
- 将 Android 设备管理员注册迁移到 Android Enterprise 注册（完全托管、工作资料、专用设备）

注册配置文件取代了现已弃用的服务器属性 `xms.server.mode`。此更改不会影响您现有的交付组和已注册设备。

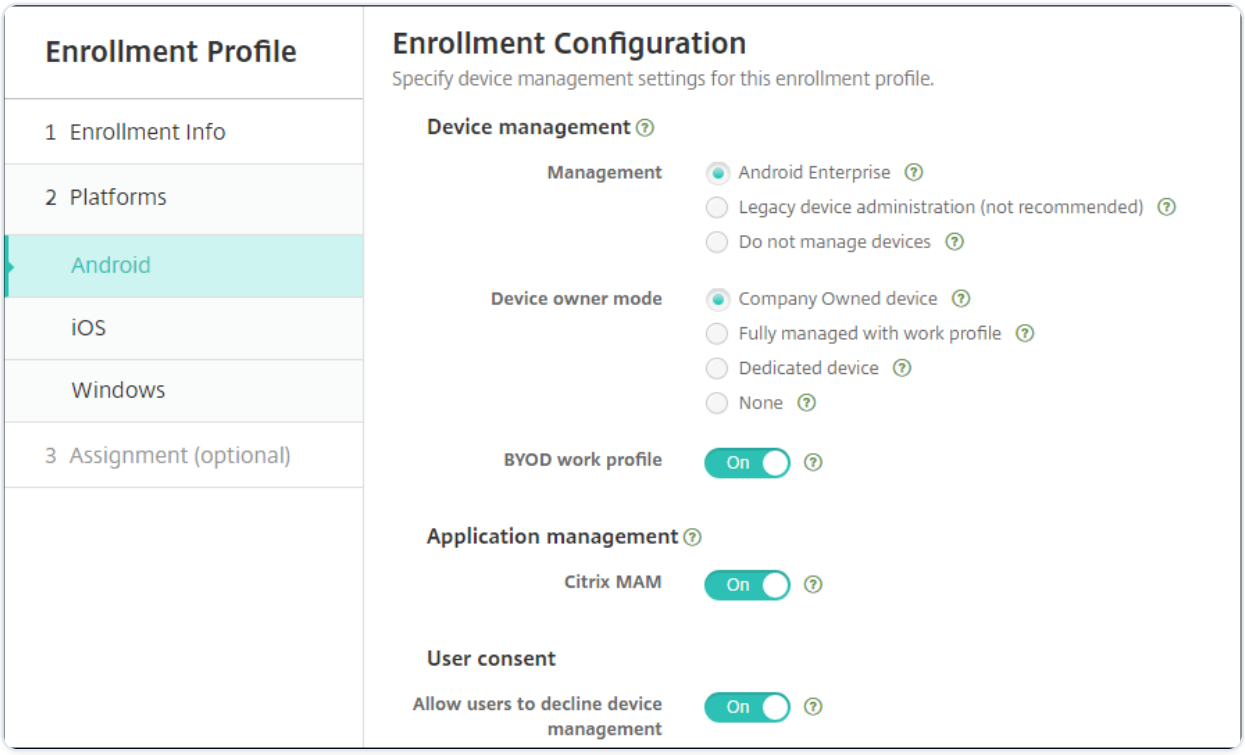
下表显示了从现有服务器属性模式到新注册配置文件功能的自动迁移路径：

现有服务器属性	新管理模式
ENT 模式 (iOS)	通过 Citrix MAM 进行 Apple 设备注册
ENT 模式 (Android)	传统设备管理员结合 Citrix MAM
ENT 模式 (安卓企业版)	完全托管设备上的工作配置文件，结合 Citrix MAM
MAM 模式 (iOS 和 Android)	思杰 MAM
MDM 模式 (iOS)	Apple 设备注册
MDM 模式 (Android)	传统设备管理员
MDM 模式 (安卓企业版)	完全托管设备上的工作配置文件

创建交付组时，可以将注册配置文件附加到该组。如果不附加注册配置文件，Citrix Endpoint Management 将附加全局注册配置文件。

注册配置文件提供以下设备管理功能：

- **从 Android 设备管理员 (DA) 模式迁移到 Android Enterprise 更轻松。** 对于 Android Enterprise 设备，设置包括设备所有者模式，例如：完全托管、完全托管设备上的工作配置文件或专用。有关详细信息，请参阅 Android Enterprise。



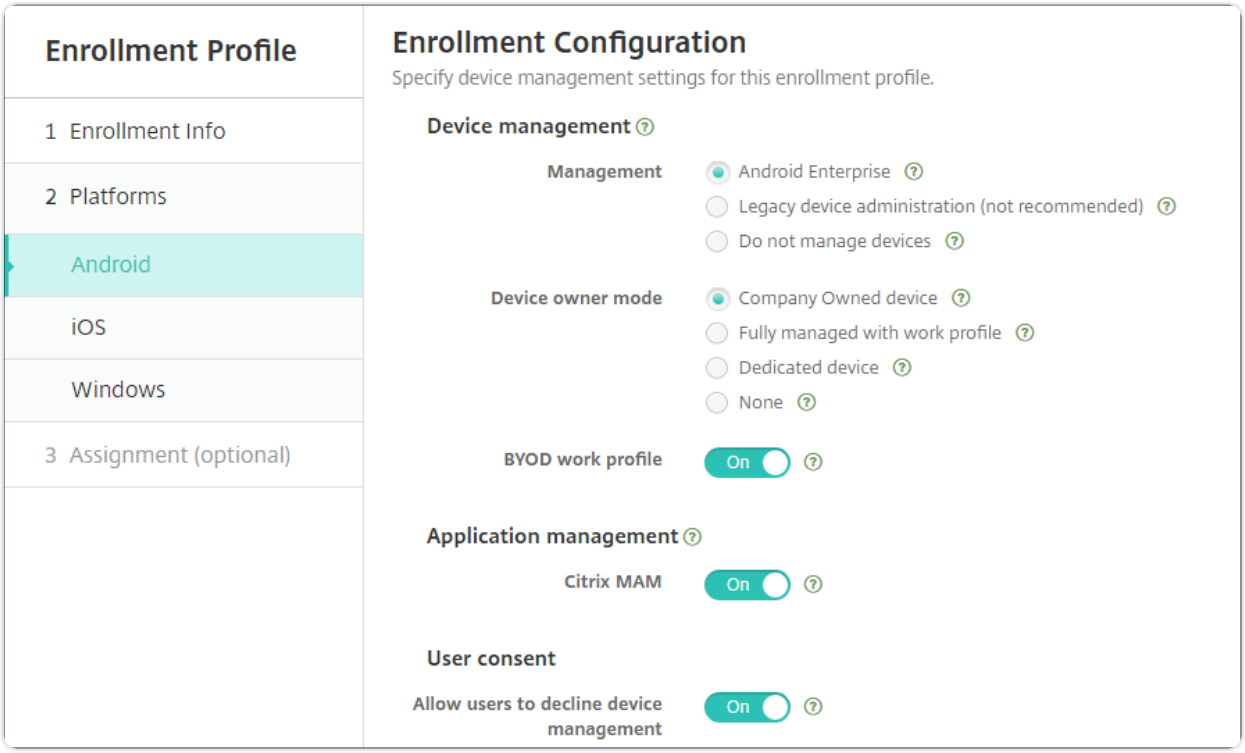
对于本次升级，您当前的 Citrix Endpoint Management 服务器模式和 **设置 > Android Enterprise** 配置将映射到新的注册配置文件设置，如下所示。

当前配置	管理设置	设备所有者模式设置	CITRIX MAM 设置
移动设备管理；托管 Google Play (Android Enterprise)	安卓企业版	完全托管设备上的工作配置文件	关
MDM；Google Workspace（旧版设备管理员）	旧版 DA	不适用	关
MAM	不管理设备	不适用	开
MDM+MAM；托管式 Google Play (安卓企业版)	安卓企业版*	完全托管设备上的工作资料	开
MDM+MAM；谷歌工作区 (旧版 DA)	旧版 DA*	不适用	开

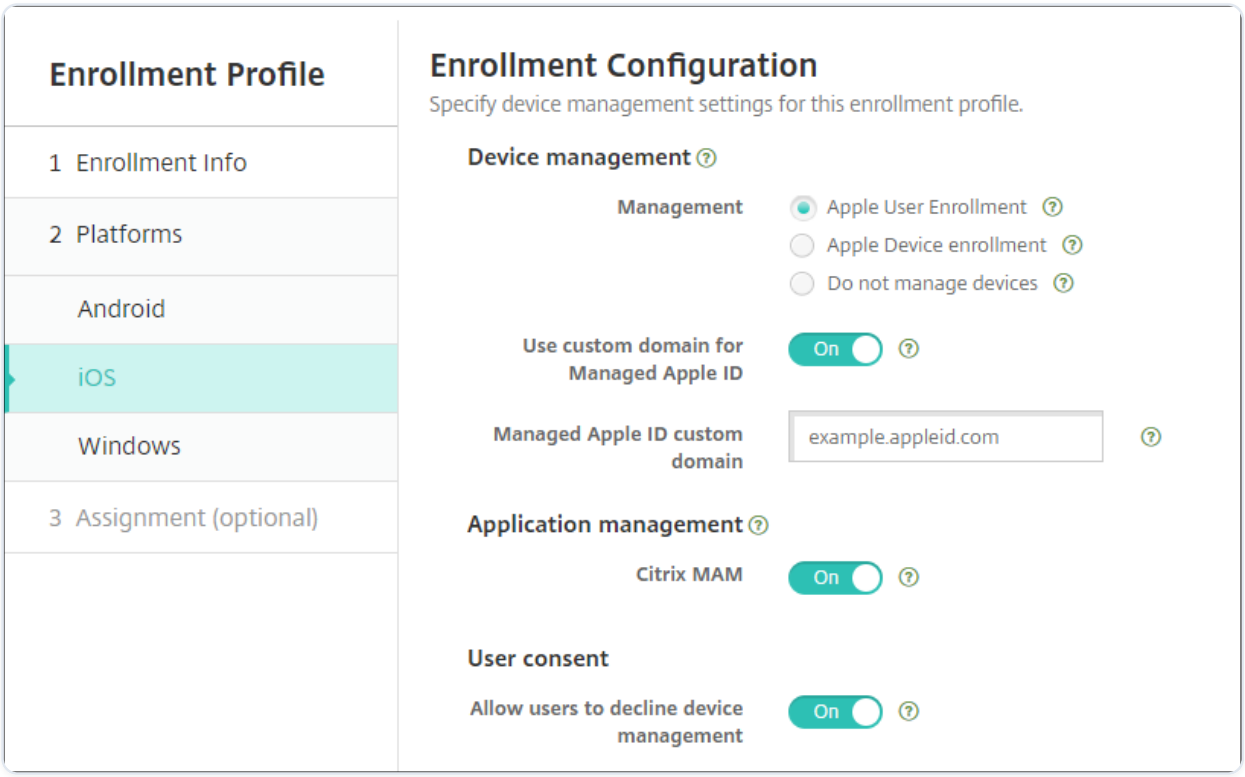
* 如果需要注册，则**允许用户拒绝设备管理**为**关**。

升级后，您当前的注册配置文件将反映这些映射。请考虑是否要创建其他注册配置文件，以在您从旧版 DA 迁移时处理任何新的用例。

如果您加入 Citrix Endpoint Management 19.12.0 或更高版本，则全局注册配置文件具有这些预定义设置。



- **更轻松的 iOS 管理。**对于 iOS 设备，设置包括选择将设备注册为托管或非托管。



对于此次升级，您之前的配置将按如下方式映射到新的注册配置文件设置。

服务器模式	管理设置	CITRIX MAM 设置
MDM	设备注册	关
MAM	不管理设备	开
MDM+MAM	设备注册	开

如果需要注册，则**允许用户拒绝设备管理**为**关**。

如果您加入 Citrix Endpoint Management 19.12.0 或更高版本，全局注册配置文件将具有这些预定义设置。

iOS 的注册配置文件页面(/en-us/citrix-endpoint-management/media/enrollment-profile-ios.png)

- **允许 Windows 10 设备自动注册到 Citrix Workspace 应用程序。**

  Windows 的注册配置文件页面(/en-us/citrix-endpoint-management/media/enrollment-profile-windows.png)

  对于此升级，您之前的 MDM 配置将映射到新的注册配置文件设置 **完全托管**。

  如果您加入 Citrix Endpoint Management 19.12.0 或更高版本，全局注册配置文件将具有这些预定义设置。

Windows 的注册配置文件页面(/en-us/citrix-endpoint-management/media/enrollment-profile-windows.png)

增强型注册配置文件存在以下限制：

- 当 Citrix Endpoint Management 与 Citrix Workspace 集成时，增强型注册配置文件功能不适用于 iOS 和 Android 设备。
- 增强型注册配置文件功能不适用于一次性 PIN 或双因素身份验证注册邀请。

有关详细信息，请参阅注册配置文件。

Citrix Endpoint Management 20.2.1 中的其他更新

- **简化专用 Android Enterprise (COSU) 设备的注册。** Citrix Endpoint Management 现在允许您通过创建注册配置文件来注册专用 Android Enterprise 设备（也称为 COSU 设备）。您不再需要为注册专用设备创建基于角色的访问控制 (RBAC) 角色。请参阅预配专用 Android Enterprise 设备。
- **使用 Keyguard 管理策略禁用 Android 设备上的生物识别身份验证。** Keyguard 管理设备策略现在允许您禁用运行 Android 9.0 及更高版本的设备的指纹解锁、面部身份验证、虹膜身份验证或所有生物识别身份验证。
- **在资源中心获取指导。** 使用资源中心访问产品内数据。要从仪表板获取指导，请单击右下角的图标。



Citrix Endpoint Management 20.2.1 中的已修复问题

以前，您需要编辑设备的权限才能使用 Citrix Endpoint Management API 向设备发送通知。现在，您需要发送通知权限才能发送通知。

当您注册启用了 WEM 的 Windows 桌面/平板电脑设备，然后在 MDM 中注册同一设备时，Citrix Endpoint Management 控制台会显示该设备的两个单独条目。

思杰端点管理 20.1.0

- **支持 Android Enterprise COPE 设备。** Citrix Endpoint Management 支持具有工作资料的 Android Enterprise 完全托管设备。Google 以前将这些设备称为 COPE（公司拥有个人启用）设备。

  Android Enterprise 完全托管设备具有设备配置文件和工作配置文件。您可以将单独的策略设置应用于设备和工作配置文件。在此版本中：

  - 您可以使用以下设备策略将单独的设置应用于设备和工作配置文件：凭据、键盘锁管理、密码 和 限制。
  - 您可以将位置设备策略的位置模式设置应用于 COPE 设备本身，但不能应用于 COPE 设备的工作配置文件。位置设备策略中的其他设置不适用于 COPE 设备。请参阅 位置设备策略。
  - 您可以单独将锁定安全操作应用于设备或工作配置文件。

- **通过 Citrix Workspace 应用程序自动注册 Windows 10 设备。** Citrix Endpoint Management 现在可以使用 Citrix Workspace 应用程序自动注册 Windows 10 桌面和平板电脑。

Citrix Endpoint Management 20.1.0 中的已修复问题

设置 > Apple 部署计划页面不包括适用于新 iOS 13 设置助理屏幕的跳过选项。在注册过程中，用户必须点击“开始使用”和“外观”屏幕。

默认情况下，**管理 > 设备**的**筛选器**选项卡处于打开状态。

对于在同一组虚拟机上的多租户客户，ShareFile 单点登录 (SSO) 失败。

思杰端点管理 19.12.0

现在，您可以根据设备属性为 Windows 设备配置交付组。(预览版) 配置交付组时，现在可以根据设备属性配置组。此功能仅适用于 Windows 台式机和平板电脑。要请求访问此预览功能，请联系您的 Citrix 销售或支持代表。有关此功能的更多信息，请参阅添加交付组 (预览版)。

将组策略对象 (GPO) 导入 Citrix Endpoint Management 并将其直接部署到 Windows 10 设备。 您可以通过 Citrix Endpoint Management 控制台导入和部署 GPO，而无需依赖 AD 管理员从组策略管理控制台部署 GPO。请参阅Windows GPO 配置设备策略。

为 Windows 台式机和平板电脑安装 EXE 应用程序。 您现在可以将 EXE 应用程序作为企业应用程序上传到 Windows 台式机和平板电脑。有关详细信息，请参阅将 Win32 应用程序添加为企业应用程序。

用户无法再从 iOS 设备中删除策略。 某些设备策略不再允许用户从 iOS 设备中删除策略。以下策略已从 iOS 中删除了“**允许用户删除策略**”设置：APN 策略、邮件策略、密码策略、预配配置文件策略、代理策略 和 VPN 策略。

Citrix Endpoint Management 19.12.0 中已修复的问题

如果您使用 Citrix Endpoint Management 公共 REST API 更新应用程序版本号，然后使用控制台更新：应用程序版本不会更新。

有时 Citrix Endpoint Management 无法在 Windows 设备上安装 EXE 应用程序，因为文件哈希不正确。

思杰端点管理 19.11.0

Apple 大宗采购计划迁移到 Apple 商务管理 (ABM) 和 Apple 教育管理 (ASM)

使用 Apple 大宗采购计划 (VPP) 的公司和机构需要在 December 1, 2019 之前迁移到 Apple 商务管理或 Apple 教育管理中的“应用和图书”。

在 Citrix Endpoint Management 中迁移 VPP 帐户之前，请参阅此Apple 支持文章。

如果您的组织或学校仅使用大宗采购计划 (VPP)，则可以注册 ABM/ASM，然后邀请现有 VPP 购买者加入您的新 ABM/ASM 帐户。对于 ASM，请导航到 `<https://school.apple.com>`。对于 ABM，请导航到 `<https://business.apple.com>`。

要更新您在 Citrix Endpoint Management 上的大宗采购（以前称为 VPP）帐户，请执行以下操作：

1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。将显示“**设置**”页面。
2. 点击 **批量采购**。**批量采购** 配置页面随即出现。
3. 确保您的 ABM 或 ASM 帐户具有与您之前的 VPP 帐户相同的应用程序配置。
4. 在 ABM 或 ASM 门户中，下载更新的令牌。
5. 在 Citrix Endpoint Management 控制台中，执行以下操作：
    a. 使用该位置的更新令牌信息编辑现有批量采购帐户。
    b. 编辑您的 ABM 或 ASM 凭据。不要更改后缀。
    c. 点击两次“**保存**”。

有关详细信息，请参阅：

- Apple 批量采购
- 通过 Apple 部署计划部署设备
- 批量注册 Apple 设备

注册配置文件控制 Android 设备的注册选项

如果您的 Citrix Endpoint Management 部署启用了 Android Enterprise，则注册配置文件现在控制 Android 设备的注册方式。注册配置文件确定 Android 设备是以默认的 Android Enterprise 模式（完全托管或工作配置文件）还是以旧版（设备管理员）模式注册。

默认情况下，全局注册配置文件将新的和恢复出厂设置的 Android Enterprise 设备注册为完全托管设备，并将 BYOD Android Enterprise 设备注册为工作配置文件设备。有关详细信息，请参阅 Android Enterprise。

将旧版 Android 设备准备为 Android Enterprise 默认注册

Google 正在弃用设备管理的设备管理员模式，并鼓励客户以设备所有者模式或配置文件所有者模式管理所有 Android 设备。（请参阅 Google Android Enterprise 开发者指南中的 设备管理员弃用。）为支持此更改，Citrix 将 Android Enterprise 作为 Android 设备的默认注册选项。

此更改意味着，如果您的 Citrix 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。

为了让您为这一更改做好准备，Citrix Endpoint Management 现在允许您创建注册配置文件，以控制 Android 设备的注册方式。

您的组织可能尚未准备好以设备所有者模式或配置文件所有者模式开始管理旧版 Android 设备。在这种情况下，您可以继续以设备管理员模式管理它们。为旧版设备创建注册配置文件，并重新注册所有已注册的旧版设备。

要为旧版设备创建注册配置文件，请执行以下操作：

1. 在 Citrix Endpoint Management 控制台中，转至**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. 单击**下一步**或在**平台**下选择 **Android**。“注册配置”页面随即显示。
4. 将**管理**设置为**旧版设备管理（不推荐）**。单击**下一步**。
5. 选择**分配（选项）**。“交付组分配”屏幕随即显示。
6. 选择包含注册专用设备的管理员的交付组。然后单击**保存**。

要继续以设备管理员模式管理旧版设备，请使用此配置文件注册或重新注册它们。您可以通过让用户下载 Citrix Secure Hub 并提供注册服务器 URL 来注册设备管理员设备，这与工作配置文件设备类似。

有关 Citrix Endpoint Management 对过渡到 Android Enterprise 的支持的详细信息，请参阅博客：Android Enterprise 作为 Citrix Endpoint Management 服务的默认设置。

Citrix Endpoint Management 19.11.0 中已修复的问题

在 Citrix Endpoint Management 控制台中搜索 Google Play 商店应用程序时，应用程序名称为空。您可以手动输入名称以保存应用程序。

上传适用于 Android Enterprise 的 MDX 应用程序后，托管的 Google Play 商店 UI 可能无法在 Citrix Endpoint Management 控制台中打开。在问题修复之前，请转到托管的 Google Play 商店手动批准并保存应用程序。

对于 iOS，如果您执行以下操作，位置跟踪将不起作用：配置并部署位置策略，从设备安全操作启用跟踪，然后删除已部署的位置策略并创建新策略。

当用户从 LDAP 导入其用户名时，用户名中包含撇号的用户无法注册其设备。

Citrix 端点管理 19.10.0

扩展了对 Zebra OEMConfig 的支持。 Citrix Endpoint Management 现在支持使用 Zebra Technologies 管理工具 Zebra OEMConfig 管理 Zebra 设备。（有关信息，请参阅 Zebra Technologies 网站。）要使用 Zebra OEMConfig 应用程序管理设备，请发布该应用程序并配置 托管配置设备策略。

Windows 应用程序的内容分发网络 (CDN) 可用性。 您现在可以使用内容分发网络部署 Windows 应用程序。请参阅 从 Citrix CDN 交付企业应用程序。

支持名称中包含特殊字符的用户的组邀请。 当您选择一个组来接收注册邀请时，Citrix Endpoint Management 现在会从 Active Directory 获取用户列表。该列表包括名称中包含特殊字符的用户。请参阅 注册邀请。

Citrix Endpoint Management 19.10.0 中已修复的问题

注册新设备或重新注册旧设备后，**管理 > 设备** 上会间歇性显示错误消息。

当您在 **管理 > 设备 > 已注册设备** 中选择 Chrome 或 Workspace 集线器设备，然后单击 **编辑** 时，将显示以下消息：`A configuration error occurred. Please try again.` 当您将鼠标悬停在设备列表中的这些设备上并单击 **显示更多** 时，也会出现该消息。无论哪种情况，单击 **确定** 继续。

Citrix 端点管理 19.9.1

- **支持 iOS 和 Android 的加密管理。** 注意：此功能已于 2021 年 3 月起弃用。Citrix Endpoint Management 转而使用 iOS 和 Android 平台提供的设备加密。Citrix 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。
- **支持 iPadOS。** Citrix Endpoint Management 支持 iPadOS 13.x。适用于 iOS 的设备策略适用于运行 iPadOS 的设备。
    - **简化了 Android Enterprise 的应用程序管理。** 您不再需要前往托管 Google Play 或 Google Developer 门户来批准或发布适用于 Citrix Endpoint Management 的应用程序。因此，应用程序的批准和发布大约需要 10 分钟，而不是数小时。

  - **在 Citrix Endpoint Management 控制台中批准适用于公共应用商店的 Android Enterprise 应用程序。** 您现在无需离开 Citrix Endpoint Management 控制台即可批准托管 Google Play 商店应用程序。在搜索字段中输入应用程序名称后，托管 Google Play 商店 UI 将打开，其中包含批准和保存应用程序的说明。然后，您的应用程序将填充到结果中，允许您配置其详细信息。请参阅 添加公共应用商店应用程序。
  - **在 Citrix Endpoint Management 控制台中批准适用于 Android Enterprise 的 MDX 应用程序。** 您现在无需离开 Citrix Endpoint Management 控制台即可批准适用于 Android Enterprise 的托管 Google Play 商店应用程序。上传 MDX 文件后，托管 Google Play 商店 UI 将打开，其中包含批准和保存应用程序的说明。请参阅 添加 MDX 应用程序。
  - **在 Citrix Endpoint Management 控制台中发布 Android Enterprise 企业应用。** 添加 Android Enterprise 私有应用时，您不再需要注册 Google Play 开发者帐户。Citrix Endpoint Management 控制台会打开一个托管的 Google Play 商店 UI，供您上传和发布 APK 文件。请参阅添加企业应用。

- **适用于工作配置文件模式或完全托管模式下的 Android Enterprise 设备的更多证书管理功能。** 除了在托管密钥库中安装证书颁发机构外，您现在还可以管理以下功能：

  - **配置特定托管应用使用的证书。** Android Enterprise 的“凭据”设备策略现在包含“**使用证书的应用**”设置。您可以指定应用使用此策略中选择的凭据提供程序颁发的用户证书。应用在运行时会静默获得证书访问权限。要将证书用于所有应用，请将应用列表留空。请参阅凭据设备策略。
  - **从托管密钥库中静默删除证书或卸载所有非系统证书颁发机构证书。** 请参阅凭据设备策略。
  - **阻止用户修改存储在托管密钥库中的凭据。** Android Enterprise 的“限制”设备策略现在包含“**允许用户配置用户凭据**”设置。默认情况下，该设置设置为“**开**”。请参阅限制设备策略。

- **位置设备策略现已适用于 Android Enterprise。** 您可以为处于托管模式或托管配置文件模式下运行的 Android Enterprise 设备定义位置设置。Android 位置跟踪需要 Android 8.5 及更高版本。请参阅位置设备策略。
- **轻松访问 BitLocker 恢复密钥。** 如果用户丢失了 BitLocker 恢复密钥，解锁设备可能会很困难。Citrix Endpoint Management 现在在设备详细信息下显示 Windows 桌面和平板电脑的 BitLocker 恢复密钥。请参阅BitLocker 恢复密钥。

Citrix Endpoint Management 19.9.1 中已修复的问题

添加包含特殊字符的自定义属性后，管理员无法访问 XenMobile® 控制台上的“设备”页面。

在 macOS 上，从 Citrix Endpoint Management 推送的企业应用仍处于挂起状态。此第三方问题是 Apple 错误 #50311461，已在 macOS 10.14.4 中修复。

RBAC 角色 `Tier 2 techs` 无法为用户数超过 2000 的用户组创建注册邀请。只有完全管理用户才能创建邀请。

在 iOS 设备上，设备升级到 iOS 13.1.x 后，管理员可能会失去向受密码保护的设备发送“解锁设备”命令的能力。要解决此问题，请参阅 `https://support.citrix.com/article/CTX262076`。

Citrix 端点管理 19.9.0

- **管理 Android Enterprise 工作配置文件和完全托管设备的锁屏功能。** Android 锁屏管理设备和工作挑战锁屏。使用“锁屏管理”设备策略控制：
  - 工作配置文件设备上的锁屏管理。您可以指定用户在解锁设备锁屏和工作挑战锁屏之前可用的功能。例如，默认情况下，用户可以使用指纹解锁并在锁屏上查看未编辑的通知。
  - 完全托管和专用设备上的锁屏管理。您可以在用户解锁锁屏界面之前，指定可用功能，例如信任代理和安全摄像头。或者，您可以选择禁用所有锁屏功能。

  请参阅锁屏管理设备策略。
- **Samsung Knox 容器密码重置。** **容器密码重置**安全操作不再适用于 Android Enterprise Samsung Knox 设备。使用**容器锁定**安全操作重置 Samsung Knox 容器的密码。**容器密码重置**安全操作仍适用于设备管理员模式下的 Samsung 设备。
- **为您的 Android Enterprise 应用程序配置产品轨道。** 为 Android Enterprise 添加公共商店应用程序或 MDX 应用程序时，配置要推送到用户设备的产品轨道。例如，如果您有一个专为测试设计的轨道，则可以将其选择并分配给特定的交付组。要了解有关发布版本的更多信息，请参阅 Google Play 帮助中心。有关配置产品轨道的信息，请参阅添加 MDX 应用程序 或添加公共应用商店应用程序。
- **Windows GPO 配置策略自动启用。** 如果您在 Citrix Cloud 中预配 Citrix Workspace Environment Management 站点，Windows GPO 配置策略将自动启用。有关详细信息，请参阅 Windows GPO 配置设备策略。
- **移动设备管理 (MDM) 和 Workspace Environment Management (WEM) 托管设备在控制台中合并。** 如果设备同时受 MDM 和 WEM 管理，则现在在 Citrix Endpoint Management 控制台中显示为一个设备。控制台中的设备标签为 **MDM, WEM**。以前，设备会显示为两个不同的设备。您现在还可以删除受 MDM 和 WEM 管理的设备。

Citrix Endpoint Management 19.9.0 中已修复的问题

部署应用程序访问设备策略后，不合规设备不会触发配置的操作。

无法配置用于 Chrome OS 设备的 Google Workspace 管理员凭据。

Citrix Endpoint Management 和 Apple School Manager 之间的连接失败。

MAM 设备会擦除应用程序和应用程序数据，因为无法获取用户域详细信息。因此，设备会将用户视为已删除。

注册新设备或重新注册旧设备后，**管理**选项卡上会间歇性显示错误消息。

Citrix 端点管理 19.8.0

- **对于现有客户：限制对 Citrix Endpoint Management 控制台和自助服务门户的端口访问：**

  对于在 Citrix Endpoint Management 19.8.0 (August 1, 2019) 之前加入的客户：

  - 您可以要求管理员登录 Citrix Cloud 控制台，以通过 SSO 访问 Citrix Endpoint Management 控制台。Citrix 强烈建议所有控制台访问都通过 Citrix Cloud 进行。

    将新服务器属性 `enable.cloud.console.sso` 设置为 **True**，这意味着您无法直接访问 Citrix Endpoint Management 控制台。尝试直接通过端口 4443 访问 Citrix Endpoint Management 控制台将导致 500 错误。
  - 自助服务门户仅可通过端口 443 访问。现在，尝试通过端口 4443 访问将导致“访问被拒绝”消息。

- **对于从 Citrix Endpoint Management 19.8.0 (August 1, 2019) 开始加入的客户：**

  - 新客户登录 Citrix Cloud 控制台，以通过 SSO 访问 Citrix Endpoint Management 控制台。
  - 访问自助服务门户需要更改服务器属性。默认情况下，新客户无法访问自助服务门户。

    要授予用户访问自助服务门户的权限，请将 `shp.console.enable` 更新为 **True**。

Citrix Endpoint Management 19.8.0 中已修复的问题

导入 CA 证书时，控制台不会在 **PKI 实体**下显示更新或新的证书。

为 iOS 配置 VPN 设备策略以使用 Citrix SSO 协议时：启用“**连接时提示输入 PIN**”设置并保存策略后，该设置会恢复为“**关闭**”。

对于从早期版本迁移的客户，如果设备的注册配置文件已被删除，则在控制台中打开“**管理**”选项卡会显示错误。

思杰端点管理 19.7.1

- **访问托管 Google Play 商店中的所有 Google Play 应用程序。“访问托管 Google Play 商店中的所有应用程序”**服务器属性使公共 Google Play 商店中的所有应用程序都可以从托管 Google Play 商店访问。将此属性设置为 **true** 允许所有 Android Enterprise 用户使用公共 Google Play 商店应用程序。管理员随后可以使用限制设备策略 来控制对这些应用程序的访问。

- **在 Android Enterprise 设备上启用系统应用程序。**要允许用户在 Android Enterprise 工作配置文件模式或完全托管模式下运行预安装的系统应用程序，请配置限制设备策略。该配置授予用户访问默认设备应用程序（例如相机、图库等）的权限。要限制对特定应用程序的访问，请使用应用程序权限策略 设置应用程序权限。

Citrix Endpoint Management 19.7.1 中已修复的问题

通过 SMTP/SMS 发送注册链接时，发送的链接不起作用。

尝试使用 Citrix Endpoint Management 控制台更新公共 iOS 应用程序时，会显示配置错误。

某些第三方批量购买应用程序无法自动更新。此问题是由于主机名被阻止引起的。有关详细信息，请参阅 `<https://support.apple.com/zh-cn/HT201999>`。

将适用于 iOS 的 Microsoft Word 或 PowerPoint 添加到云应用程序库时，将应用程序分配给用户组失败。您必须删除并重新添加遇到此问题的任何 Intune 应用程序。

Citrix 端点管理 19.6.1

- **位置设备策略现在支持 Android 设备跟踪。** 您现在可以启用设备跟踪，以您定义的频率轮询特定设备。您可以使用此策略跟踪送货人员以获得更准确的送货估算，跟踪丢失或被盗的设备，或强制执行地理边界。有关详细信息，请参阅位置设备策略。

Citrix Endpoint Management 19.6.1 中的已修复问题

对于自动上传的应用程序，其应用程序图标不会显示在 Citrix Endpoint Management 控制台中。

服务器属性 `bulk.enrollment.fetchRosterInfoDelay` 中的时间段结束后，并且 Apple School Manager 设备与服务器同步后：Apple School Manager 用户帐户将从服务器中删除，设备将进入匿名状态。

显示名称中包含特殊德语字符（例如变音符号）的用户无法注册。

当您尝试使用 Apple Store 中的新应用程序 URL 配置公共应用程序时，会显示以下错误消息：“找不到您输入的应用程序。请检查 URL 并重试。”

Citrix 端点管理 19.6.0

- **Apple 批量购买应用程序的自动更新。** 添加批量购买帐户（**设置 > iOS 设置**）后，您现在可以为所有 iOS 应用程序启用自动更新。请参阅Apple 批量购买 中的**应用程序自动更新**设置。

Citrix Endpoint Management 19.6.0 中的已修复问题

如果注册表值的长度超过 2048 个字符，则在将注册表项添加到 Windows Embedded Compact 策略时会显示以下错误：`Console error: could not execute statement; SQL [n/a]; nested exception is org.hibernate.exception.DataException: could not execute statement`。

在 iOS 设备上安装配置文件期间，配置文件信息中显示“未验证”。

当 Azure AD 用户登录到配置为信息亭的某些 Windows 10 Azure AD 加入设备时，信息亭模式不会激活。如果您以 `azuread\user` 格式输入 Azure AD 用户名，则不会出现此问题。有关详细信息，请参阅 信息亭设备策略。

对于自动上传的应用程序，其应用程序图标不会显示在 Citrix Endpoint Management 控制台中。

添加批量购买帐户（**设置 > iOS 设置**）时，如果令牌超过 350 个字符，则会显示以下消息：`The entered company token is not valid, please enter a new one.`

Citrix 端点管理 19.5.0

- **iOS MDM 注册工作流更改。** 为了通过减少误导性配置文件安装来提高平台安全性，Apple 发布了一个新的工作流，用于手动将设备注册到 MDM。此新工作流会影响所有 MDM 解决方案，包括 Citrix Endpoint Management。

  对于注册到 Apple Business Manager 或 Apple School Manager 中分配的服务器的 MDM 注册，没有变化。工作流更改仅适用于 MDM 中的手动注册。

  Citrix 还简化了注册过程。以前，iOS 设备用户在注册期间会收到两个提示：一个用于根 CA，一个用于 MDM 设备证书。Citrix 安装了根 CA，以便灵活使用未签名和已签名证书。由于所有 Citrix Cloud 部署都使用受信任的证书，因此不再需要根 CA。

  iOS 设备用户在注册期间只会收到 MDM 设备证书提示。该提示标记为“XenMobile Profile Service”。

  为支持此更改，Citrix 将服务器属性 `ios.mdm.enrollment.installRootCaIfRequired` 的值更改为 `false`。在 MDM 注册期间会打开一个 Safari 窗口，以简化用户的配置文件安装。有关详细信息，请参阅 注册 iOS 设备 和以下 YouTube 视频：



- **Citrix Endpoint Management 新客户的更改：**
  - **Workspace 体验部署。** 您可以创建一个名为 Workspace 的单独交付组，以开始将 Workspace 体验部署到新设备。通过使用 Workspace 交付组，您可以将 Workspace 体验交付给一小部分用户，而不会干扰所有用户。
  - **Citrix Endpoint Management 19.5.0 及更高版本新客户的预配置策略和应用程序。** 如果您从 Citrix Endpoint Management 19.5.0 或更高版本开始使用，我们将预配置一些设备策略和移动生产力应用程序。此配置使您能够立即向设备用户部署基本功能。请参阅 默认设备策略和移动生产力应用程序。
- **适用于 Android Enterprise 的 Knox Platform for Enterprise 设备策略（已弃用）。** 您现在可以为运行 Knox 3.0 或更高版本的 Android Enterprise 设备输入 KPE Premium 和 Standard 许可证密钥。
- **Chrome OS 的公共会话设备策略。** 您现在可以配置 Chrome OS 设备以支持访客会话。有关配置此策略的信息，请参阅公共会话设备策略。
- **RBAC 权限更改。** RBAC 权限“添加/删除本地用户”现在分为两个权限：“添加本地用户”和“删除本地用户”。

Citrix Endpoint Management 19.5.0 中已修复的问题

企业应用程序不会在运行 iOS 11.4 或更高版本的受监管设备上静默升级。

编辑设备策略时，将显示以下错误消息：`A configuration error occurred. Please try again`。

思杰端点管理 19.4.1

- **通过 Workspace Environment Management (WEM) 与 Citrix Endpoint Management 集成，您可以管理所有受支持的已加入域的 Windows 设备。** 此集成提供以下优势和功能：
  - 仅使用 WEM 无法进行 MDM 部署。仅使用 Citrix Endpoint Management，您只能管理 Windows 10 设备。通过集成这两种产品，您可以：
    - WEM 可以访问 MDM 功能
    - 通过 Citrix Endpoint Management 管理更广泛的 Windows 操作系统
  - 这种管理形式是配置 Windows GPO。目前，管理员将 ADMX 文件导入 Citrix Endpoint Management 并将其推送到 Windows 10 桌面和平板电脑以配置特定应用程序。使用 Windows GPO 配置设备策略，您可以配置 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接收 GPO 配置，即使 Citrix Endpoint Management 不原生支持该设备。
  - 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以名为 WEM 的新 Citrix Endpoint Management 模式运行。在已注册设备的“**管理 > 设备**”列表中，WEM 管理设备的“**模式**”列显示“**WEM**”。

  有关详细信息，请参阅Windows GPO 配置设备策略。
- **对于 Citrix Endpoint Management 19.4.1 的新多租户客户，企业应用程序的 CDN 交付现在是默认设置。** 如果您是亚太地区的新客户，请联系您的 Citrix 支持代表以启用 CDN 交付。在所有区域，希望使用 CDN 交付企业应用程序的现有客户必须在启用该功能后重新上传现有应用程序。请参阅 从 Citrix CDN 交付企业应用程序。
- **支持 Android Enterprise 的 Web 和 SaaS 应用程序以及 Web 链接。** Citrix Endpoint Management 现在支持向 Android Enterprise 设备交付 Web 或 SaaS 应用程序的链接以及 Web 链接。Web 和 SaaS 应用程序以及 Web 链接的添加方式与为其他平台添加的方式相同。请参阅 添加 Web 或 SaaS 应用程序 和 添加 Web 链接。
- **Chrome OS 设备的更多限制：**
  - **在禁用设备上显示说明。** 您现在可以添加自定义消息以在禁用的 Chrome OS 设备上显示。
  - **允许用户安装特定的扩展程序、应用程序和主题。** 输入允许从这些源下载的 URL 列表。

  有关详细信息，请参阅 Chrome OS 设置。

Citrix Endpoint Management 19.4.1 中已修复的问题

在 Android Enterprise 设备上，以下应用程序类型可能不会显示在 Citrix Secure Hub 中：在 Google Play 平台中配置的公共应用商店应用程序以及在 Android 平台中配置的企业应用程序。

Android Enterprise 应用程序在设备取消注册并重新注册之前不会显示。如果您在交付组中更新应用程序，它们也会显示。

自动化操作可能无法部署到 Android Enterprise 设备。

您的 Android Enterprise 企业的名称和所有者可能无法在 Google Play 商店管理员控制台中正确显示。

思杰端点管理 19.3.1

Citrix Endpoint Management 19.3.1 中已修复的问题

如果您在 19.3.1 版本之前为 Windows 10 桌面和平板设备部署了应用商店设备策略：当用户单击“开始”菜单中的 Windows 应用商店链接时，会显示一条消息：“500 Internal Server Error”或“HTTP Status 404 - Either you've reached an old URL or this device isn't registered”。要解决此问题，您必须重新创建并部署您的应用商店设备策略。

如果 Active Directory 用户组被分配到 RBAC 角色权限，则无法删除包含该用户组的 LDAP 配置。作为一种解决方法，如果您从 RBAC 中取消分配相应的 Active Directory 组，则可以删除该域。

思杰端点管理 19.3.0

- **支持 Android Enterprise 策略统一中的 Samsung Knox。** 对于运行 Samsung Knox 3.0 或更高版本以及 Android 8.0 或更高版本的 Android Enterprise 设备：Knox 和 Android Enterprise 组合成一个统一的设备和配置文件管理解决方案。在以下设备策略的 Android Enterprise 页面上配置 Knox 设置：
  - **操作系统更新设备策略。** 控制 Samsung Enterprise FOTA 更新。请参阅 操作系统更新设备策略。
  - **密码设备策略。** 请参阅 密码设备策略。
  - **限制设备策略。** 请参阅 限制设备策略。
  - **Samsung MDM 许可证密钥设备策略（已弃用）。** 配置 Knox 许可证密钥。
- **适用于 Android Enterprise 的应用程序清单设备策略。** 您现在可以收集托管设备上 Android Enterprise 应用程序的清单。有关详细信息，请参阅 应用程序清单设备策略。

- **适用于 Android Enterprise 的文件设备策略。** 您现在可以将脚本文件添加到 Citrix Endpoint Management，以便在 Android Enterprise 设备上执行功能。请参阅 文件设备策略。
- **锁定并重置 Android Enterprise 的密码。** Citrix Endpoint Management 现在支持对在工作配置文件模式下运行 Android 8.0 及更高版本的 Android Enterprise 设备执行“锁定并重置密码”安全操作。请参阅 安全操作。
- **Windows 10 桌面和平板电脑设备上的自助服务终端支持 Azure Active Directory。** 您现在可以在自助服务终端模式下添加已加入域的 Azure AD 设备。请参阅 自助服务终端设备策略。
- **对于启用了工作区体验的 Citrix Endpoint Management 客户：Citrix Endpoint Management 支持通过 iOS 和 Android 上的 Citrix Workspace 应用程序进行联合身份验证。** 此功能不支持 Azure Active Directory。有关信息，请参阅 选择或更改身份验证方法。
- **公共 REST API 更改。** Citrix Endpoint Management REST 服务公共 API 现在包含一个用于编辑 MDX 应用程序容器内平台详细信息的 API。请参阅 PDF 中的“3.15.2.4 更新 MDX 应用程序容器内的平台详细信息”部分，REST 服务公共 API。

Citrix Endpoint Management 19.3.0 中的已修复问题

使用“**通过密码锁定**”安全操作远程锁定完全托管的 Android Enterprise 设备可能会失败，且不会通知您失败。为确保设备已锁定，请设置两次“**通过密码锁定**”。设备将使用您设置的第二个密码锁定。

如果企业从 Managed Google Play 中删除并在 Citrix Endpoint Management 服务器上更新，Android Enterprise 设备有时无法注册。

对于 Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成：对 Intune 应用商店应用名称或描述所做的更改不会保存。

编辑 iOS Intune 应用后，该应用将无法从 Microsoft Company Portal 应用安装。

如果被分配为 Citrix Cloud 自定义管理员权限而非完全管理员权限，则无法单击“**管理**”按钮来导航资源。

TLS 版本弃用

为提高 Citrix Endpoint Management 服务的安全性，Citrix 现已阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的任何通信。由于其安全性减弱，PCI 理事会正在弃用 TLS 1.0。

此更改如何影响您

如果您通过本地 NetScaler Gateway (NetScaler Gateway) 使用移动应用程序管理，则必须更新负载均衡器服务以启用 TLS 1.2。

以下连接器的旧版本仅支持 TLS 1.0：

- 适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器
- 适用于 Exchange ActiveSync 的 NetScaler Gateway 连接器

按如下方式升级您的连接器：

- 如果您使用的是适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器版本 10.1.3 或更低版本，请升级到版本 10.1.4 或更高版本。
- 如果您使用的是适用于 Exchange ActiveSync 的 NetScaler Gateway 连接器版本 8.5.0 或更低版本，请升级到版本 8.5.1.11 或更高版本。

操作方法

如果您使用本地 NetScaler Gateway (NetScaler Gateway)，请在负载均衡器服务上启用 TLS 1.2。有关信息，请参阅 `<https://support.citrix.com/article/CTX247095>`。

要下载 Exchange ActiveSync 的任一连接器：

```
1.  Go to `<https://www.citrix.com/downloads>`.

1.  Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server)
> XenMobile Server (on-premises) > Product Software > XenMobile Server 10
> Server Components**.

1.  Locate the connector tile and then click **Download File**.
```

思杰端点管理 19.2.1

- **在 Chrome 设备上的自助服务终端中运行多个应用程序。** 您现在可以将多个应用程序添加到 Chrome OS 的自助服务终端策略。您可以选择在用户启动设备时自动启动应用程序。请参阅 自助服务终端设备策略。

Citrix Endpoint Management 19.2.1 中的已修复问题

在 Android Enterprise 取消注册后重新注册时，已批准的应用程序可能不会显示在以工作配置文件模式注册的设备上。

当用户首次在 Intune MDM+MAM 上运行 Citrix Secure Mail 时，设置会引导用户完成选择 Intune MAM/XenMobile 的工作流程。

思杰端点管理 19.2.0

- **通过内容分发网络 (CDN) 交付企业应用程序。** 当用户不在 Citrix Endpoint Management 服务器附近时，企业应用程序交付可能需要一段时间。为了加快应用程序下载速度，您可以改为通过全球内容分发网络 (CDN) 位置交付企业应用程序。企业应用程序的 CDN 支持适用于 iOS 应用程序（MDM 或 MAM 注册）和 Android 应用程序（MDM 或 MAM 注册）。企业应用程序的 CDN 支持不适用于 Windows 应用程序。要开始使用，请参阅 通过 Citrix CDN 交付企业应用程序。
- **Citrix Workspace 的 DEP 设备注册更改。** 如果 Citrix Endpoint Management 与 Citrix Workspace 集成，则 Citrix Workspace 应用程序将作为必需应用程序包含在 DEP 部署包中。此功能要求您将 iOS 的 DEP 帐户设置配置为关闭所需凭据。Citrix Secure Hub 会提示用户在注册 Citrix Endpoint Management 之前将设备注册到 Citrix Workspace。
- **服务器属性 ios.mdm.enrollment.installRootCalfRequired 现已设置为 false。** Citrix Endpoint Management 使用公开信任的证书链，因此无需将根 CA 推送到设备。因此，iOS 设备用户在注册期间不再收到安装根 CA 的提示。
- **网络和凭据策略现在支持 Apple TV OS。** 此外，您现在可以配置 AirPlay 安全设备策略来控制哪些设备可以连接到 Apple TV 设备。有关详细信息，请参阅 网络、凭据 和 Airplay 安全设备策略文章。
- **位置设备策略现已适用于 Android Enterprise。** 您可以为处于托管模式或运行在托管配置文件模式下的 Android Enterprise 设备定义位置设置。请参阅 位置设备策略。
- **增强了对 Alexa for Business 的支持。** Citrix Endpoint Management 现在支持 Alexa for Business 会议、向您的组织添加 Alexa 技能、编辑技能组。请参阅 Alexa for Business。
- **Windows 代理策略的自动化操作。** 使用 Windows 代理策略，您可以根据注册表值自动执行在 Windows 桌面和平板电脑上运行的操作。有关详细信息，请参阅 Windows 代理设备策略 和 自动化操作 文章。
- **对于 Android Enterprise，密码中所需字符的“无限制”选项现已弃用。** 运行 Android 7 或更高版本的 Android Enterprise 设备不再支持创建没有字符限制的密码。如果您之前将**所需字符**设置为**无限制**，则此更新会将该值更改为**仅数字**。此更改不影响当前用户登录体验。有关详细信息，请参阅 Android Enterprise 设置。

Citrix Endpoint Management 19.2.0 中的已修复问题

当应用从 Intune 库中删除后，用户尝试从 Citrix Cloud 库中删除该应用时，无法删除。

在 Endpoint Manager 控制台中上传 Google Play 应用时未添加应用图标图像：如果之后为该应用上传图像，则该图像不会显示在应用列表中。

思杰端点管理 19.1.2

- **文件设备策略现已可用于 Android Enterprise。** 您可以将脚本文件添加到 Citrix Endpoint Management，以在 Android Enterprise 设备上执行功能。请参阅文件设备策略。
- **为 Chrome OS 设备配置时区设置。** 您现在可以为 Chrome 设备选择时区并指定如何检测时区。有关详细信息，请参阅限制设备策略。
- **RBAC 管理员的组权限现在限制了“用户”和“注册邀请”页面上显示的用户信息。** 以前，Citrix Endpoint Management 控制台在**管理 > 用户**和**管理 > 注册邀请**页面上包含所有本地用户和域用户的信息。

  要指定 RBAC 管理员有权查看和管理哪些用户组，请编辑管理员角色并指定用户组。有关详细信息，请参阅使用 RBAC 配置角色。
- **从 Citrix Workspace 应用程序启动第三方应用程序。** 对于已启用 Citrix Workspace 的客户：在向用户部署新应用程序之前，您可以添加一个逗号分隔的 URL 列表，以从 Citrix Workspace 应用程序启动这些应用程序。有关详细信息，请参阅添加应用程序。

Citrix Endpoint Management 19.1.2 中的已修复问题

您无法在 Citrix Endpoint Management 控制台中上传版本高于 11.5.09 的 Google Play 服务 APK。

在**配置 > 应用程序 > 公共应用商店**中编辑 Windows 桌面和平板电脑应用程序时，会显示此消息：“应用程序搜索失败”。搜索这些应用程序时，会显示此消息：“连接到 Windows 桌面商店 URL 时出错：未能检索公共应用程序详细信息”。

第三方通知

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

Citrix Endpoint Management 第三方通知(/zh-cn/citrix-endpoint-management/downloads/third-party-notices-endpoint-management.pdf)

弃用

本文中的公告是关于 Citrix Endpoint Management 正在逐步淘汰的功能的提前通知，以便您能够及时做出业务决策。Citrix 会监控客户使用情况和反馈，以确定何时撤回这些功能。公告可能会在后续版本中发生变化，并且可能不会包含所有已弃用的功能。有关产品生命周期支持的详细信息，请参阅产品生命周期支持策略文章。

> **重要提示：**

> 感谢您使用 Citrix Endpoint Management Analyzer Tool，我们对此表示感谢。由于我们发布节奏频繁且稳定，此工具不再需要。Citrix 已决定自 March 31, 2023 起停止此服务。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。有关详细信息，请参阅 连接检查。

弃用和移除

以下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，直到在未来版本中将其删除。

在 Citrix Endpoint Management 中，*已删除*的项目要么已被删除，要么不再受支持。

有关已达到生命周期终止 (EOL) 的移动生产力应用程序的信息，请参阅 (/zh-cn/mobile-productivity-apps/eol-deprecated-apps.html)。

项目	描述	宣布弃用	已删除	替代方案
通过 Citrix Cloud™ (CC) 库管理 Microsoft Intune 应用程序。	弃用通过 CC 库管理 Microsoft Intune 应用程序的支持。如果您已在使用 Intune 应用程序，则不会受到影响。	2025 年 3 月	2025 年 4 月	无替代方案。
适用于 Android Enterprise 的两项仅限 Samsung 完全托管设备的限制。	已从限制策略中弃用以下设置：启用 ODE 可信启动验证和启用吊销检查。	2025 年 2 月	2025 年 3 月	无替代方案
仅限 Samsung Knox 容器的限制，适用于 Android Enterprise。	已从限制策略中弃用以下设置：将应用程序移动到容器、强制执行多重身份验证、强制执行容器身份验证和启用安全键盘	2025 年 2 月	目标：2025 年 6 月	无替代方案

项目	描述	宣布弃用	已删除	替代方案
与 ShareFile 集成	如果 ShareFile（现为 Progress）停止支持，则与 ShareFile 的集成将被弃用。	2025 年 1 月		无替代方案
监视选项卡	已弃用 Citrix Endpoint Management 中的监视选项卡。	2024 年 9 月	2024 年 10 月	无替代方案
Citrix Endpoint Management 政府版产品	已弃用对 Citrix Endpoint Management 政府版的支持。	2022 年 1 月	2022 年 7 月	Citrix Endpoint Management 标准版产品
SafetyNet 证明 API	已弃用对 Android SafetyNet 证明的支持，具体请参阅 Google 的公告此处。	2023 年 7 月	2023 年 11 月	Play 完整性 API
Chrome 操作系统	已弃用对 Chrome OS 的支持。	2022 年 7 月	2023 年 5 月	无替代方案
tvOS	已弃用对 tvOS 的支持。	2022 年 7 月	2023 年 5 月	无替代方案
Windows 信息保护 (WIP)	已弃用对 Windows 信息保护的支持，具体请参阅 Microsoft 的公告此处。	2022 年 8 月	2022 年 10 月	无替代方案
Citrix 端点管理分析器	已弃用对 Citrix Endpoint Management	2022 年 7 月	目标: March 31, 2023	无替代方案

项目	描述	宣布弃用	已删除	替代方案
	Analyzer 工具的支持。			
Workspace hub 设备管理	弃用对 Citrix Ready® workspace hub 设备的支持。	2022 年 1 月	2022 年 6 月	无替代方案
Microsoft 商业版应用商店	弃用对 Microsoft Store for Business 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	无替代方案
三星 SAFE	弃用对 Samsung SAFE 的支持。	2022 年 1 月	2022 年 6 月	使用 安卓企业版。
Zebra 的自定义 XML	弃用对 Zebra 设备上自定义 XML 的支持。	2022 年 1 月	2022 年 6 月	使用 Android Enterprise 托管配置。
PKI 身份：通用、Symantec PKI、DigiCert 和 Entrust	弃用对通用、DigiCert Managed 和 Entrust 适配器 PKI 实体的支持。	2021 年 6 月	2022 年 1 月	无替代方案
适用于 Workspace 的 Android	弃用对 Android for Workspace 的支持	2022 年 1 月	2022 年 4 月	无替代方案
运营商短信网关	弃用对 Nexmo 短信网关通知的支持	2022 年 1 月	2022 年 4 月	使用 SMTP 服务器通知

项目	描述	宣布弃用	已删除	替代方案
移动服务提供商 (MSP)	弃用对 MSP 接口的支持，该接口用于查询 Blackberry 和其他 Exchange ActiveSync 设备并发出操作	2022 年 1 月	2022 年 4 月	无替代方案
MDX 工具包	弃用对 MDX Toolkit 的支持，转而支持移动应用管理 (MAM) SDK。在过渡期内，您可以同时使用 MDX 封装的应用程序和 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 - 共享设备注册器和 COSU 设备注册器	弃用对共享设备注册器和 COSU 设备注册器的预定义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 School Manager 或 Apple Business Manager 配置 iOS 设备。通过注册配置文件配置 Android COSU（专用）设备。
允许自动连接到 Wi-Fi 感知热点限制，适用于 Windows 设备。	取消对 Windows 10 设备上“允许自动连接到 Wi-Fi 感知热点”限制的支持。Windows 10 不再支持此功能。有关信息，请参阅	2021 年 10 月	2022 年 2 月	无替代方案

项目	描述	宣布弃用	已删除	替代方案
	Microsoft 文档。			
MDX：备用网关服务器	弃用适用于 iOS 和 Android 设备的分步身份验证。	2020 年 3 月	2021 年 9 月	无替代方案
MDX：微型 VPN（完整隧道模式）	弃用适用于 iOS 和 Android 设备的完整虚拟专用网络 (VPN) 隧道。	2020 年 3 月	2021 年 9 月	使用 MAM SDK Web SSO 模式或创建按应用程序 VPN 策略并使用 Citrix SSO 连接类型。
MDX：PAC 文件支持	弃用对代理自动配置 (PAC) 文件的支持，以及适用于 iOS 和 Android 设备的完整 VPN 隧道部署。	2020 年 3 月	2021 年 9 月	使用 NetScaler Gateway 通过代理服务器连接以访问内部网络。
MDX 共享设备支持	弃用适用于 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 School Manager 或 GroundControl。
Android - 索尼	已弃用对 Android 索尼设备和索尼特定策略的支持。	2021 年 1 月	2022 年 2 月	使用安卓企业版
安卓 - HTC	已弃用对 Android HTC 设	2021 年 1 月	2022 年 2 月	使用 安卓企业版

项目	描述	宣布弃用	已删除	替代方案
	备和 HTC 特定策略的支持。			
Android - 亚马逊	已弃用对 Android 亚马逊设备和亚马逊特定策略的支持。	2021 年 1 月	2022 年 2 月	使用 安卓企业版
Knox 移动注册（旧版 DA）	已弃用在所有 Android 版本上旧版设备管理员模式中的 Knox 移动注册 (KME) 支持。	May 4, 2021	2021 年 9 月	使用 KME 注册到 Android Enterprise 模式。Android 8、9、10、11 支持 Android Enterprise。
高安全性注册模式	已弃用对使用 **高安全性** 注册安全模式生成注册邀请的支持。	2021 年 7 月	2022 年 2 月	有关支持的注册安全模式列表，请参阅注册邀请。
派生凭据	已弃用对派生凭据和 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列表，请参阅 iOS。
APNs 出站端口	Apple 对 APNs 旧版二进制协议的支持将于 March 31, 2021 结束。Apple 建议您改用基于 HTTP/2 的 APNs 提供程序 API。作为此更改的一部分，我们将弃用对端口 2195 和 2196 的支持，这些端口用于向	2020 年 10 月	2021 年 3 月	请改用端口 443。请参阅网络和防火墙要求。

项目	描述	宣布弃用	已删除	替代方案
	`*.push.apple.com` 发送 APNs 通知。			
MDX 服务	已弃用对 MDX 服务的支持，转而支持移动应用程序管理 (MAM) SDK。在过渡期间，您可以使用通过 MDX Toolkit 封装的 MDX 应用程序和使用 MAM SDK 开发的应用程序。	2020 年 3 月	2021 年 9 月	要继续封装企业应用程序，请使用 MDX Toolkit。
自助服务门户中的注册邀请设置	已弃用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	请联系您的管理员，在 Citrix Endpoint Management 控制台中生成注册邀请。
注册邀请设置	弃用对使用设备 IMEI、序列号和 UDID 创建注册邀请的支持。	2021 年 4 月	2021 年 7 月	在 Citrix Endpoint Management 控制台中创建注册邀请时，请在 **管理 > 注册邀请** 下配置可用设置。
基于证书的身份验证签名算法（非 FIPS 和弱密码）	弃用对以下签名算法的支持：SHA1withRSA、SHA224withRSA、SHA1withECDSA、	2020 年 5 月	2021 年 6 月	在 Citrix Endpoint Management 控制台中为凭据提供程序创建 CSR 时（**设置 > 凭据提供程序 > 证书签名请**

项目	描述	宣布弃用	已删除	替代方案
	SHA224withECDSA、SHA1withDSA、RIPEMD160withRSA、RIPEMD128withRSA、RIPEMD256withRSA。			求），请选择更强的密码。
适用于 Android 7.x 和 iOS 12.x 的 Citrix 移动应用程序和 Workspace 应用程序	弃用对 Android 7.x 和 iOS 12.x 版本的 Citrix Secure Hub、Citrix Secure Mail、Citrix Secure Web 和 Citrix Workspace 应用程序的支持。	2021 年 4 月	2021 年 6 月	至少使用每个主要操作系统平台的当前版本和上一版本。旧设备仍可注册。但是，Citrix 不会测试或支持旧设备。
适用于 Android 的 RSA 软令牌支持	弃用对将 RSA 软令牌直接导入到适用于 Android 的 Citrix Secure Hub 的支持。	2021 年 1 月	2021 年 2 月	您可以将 RSA 软令牌导入到 Google Play 中提供的 RSA Secure ID 应用程序中。然后，您可以使用该令牌进行 NetScaler Gateway 身份验证。
Internet Explorer 11	弃用对将 Internet Explorer 与 Citrix Endpoint Management 控制台结合使用的支持。	2021 年 1 月	2021 年 1 月	使用以下 Web 浏览器的最新版本：Google Chrome、Mozilla Firefox、Microsoft

项目	描述	宣布弃用	已删除	替代方案
				Edge、Apple Safari
Citrix Endpoint Management Analyzer 中的网关配置检查	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 检查来检查您的 Citrix ADC 配置，以确保 Citrix Endpoint Management 部署就绪。
针对 Android Enterprise 设备上的旧版设备管理员模式发布的应用程序	我们不再向注册到 Android Enterprise 的设备交付为旧版 DA 平台发布的应用程序。	2020 年 10 月	2020 年 11 月	对于 Android Enterprise 设备，请为 Android Enterprise 平台发布应用程序。要继续向处于 DA 模式的设备发布旧版 DA 应用程序，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。自升级到以 Android API 级别 29 为目标的 Citrix Secure Hub 以来，Citrix 不再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。

项目	描述	宣布弃用	已删除	替代方案
安卓 TouchDown	DigiCert 停止支持 Android TouchDown。Citrix 已从 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	已弃用对 Android 10 设备上旧版设备管理员模式的新注册或重新注册的支持。已注册的设备将继续工作。	2020 年 2 月	2020 年 9 月	将新的 Android 10+ 设备注册到 Android Enterprise。
MDX 加密	已弃用 MDX 加密以及 Citrix Endpoint Management 控制台中的 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。请确保您已测试并计划在 2020 年 7 月之前完成 MDX 加密的迁移。
视窗移动/CE	已弃用对 Windows Mobile/CE 设备的支持。	2018 年 4 月	2020 年 9 月	使用 Windows 10 桌面版和笔记本电脑。
Samsung SEAMS 容器	已弃用对 Samsung SEAMS 容器的支持。	2020 年 6 月	2020 年 8 月	请使用 Android Enterprise。
远程支持	远程支持客户端已弃用。	2019 年 1 月	2020 年 8 月	无替代方案

项目	描述	宣布弃用	已删除	替代方案
适用于 Android 6.x 和 iOS 11.x 的 Citrix 移动应用程序和 Workspace 应用程序	已弃用对 Android 6.x 和 iOS 11.x 版本的 Citrix Secure Hub、Citrix Secure Mail、Citrix Secure Web 和 Citrix Workspace 应用程序的支持。	2020 年 4 月	2020 年 6 月	至少使用每个主要操作系统平台的当前版本和上一版本。旧设备仍可注册。但是，Citrix 不测试或支持旧设备。
适用于 iOS 的 Citrix Secure Hub 网络扩展	已弃用允许您为 iOS 设备自定义网络功能的网络扩展框架。Citrix Secure Hub 版本 20.3.0。	2018 年 10 月	2020 年 3 月	无替代方案
使用本地账户进行 API 登录	管理员不再能够使用本地账户登录 REST API。	2020 年 10 月		管理员可以使用 Citrix Cloud 账户登录。请参阅 REST API。
自签名安全套接字层 (SSL) 证书	弃用对所有设备平台自签名 SSL 证书的支持。	2020 年 5 月		将您现有的自签名证书替换为来自知名证书颁发机构 (CA) 的受信任 SSL 证书。
完整 VPN 隧道 - Android	弃用对 Android 完整 VPN 隧道的支持。	2020 年 3 月	2021 年 9 月	MAM SDK Web SSO 模式。
允许 VPN 模式切换 - Android	弃用对 Android 允许 VPN 模式切换的支持。	2020 年 3 月	2021 年 9 月	无替代方案

项目	描述	宣布弃用	已删除	替代方案
入站文档交换 - Android	弃用对 Android 入站文档交换的支持。	2020 年 3 月	2021 年 9 月	无替代方案

系统要求

在等待 Citrix 预配 Citrix Endpoint Management 期间，请务必通过安装 Cloud Connector 为您的 Citrix Endpoint Management 部署做好准备。尽管 Citrix 托管并交付您的 Citrix Endpoint Management 解决方案，但仍需要进行一些通信和端口设置。此设置将 Citrix Endpoint Management 基础结构连接到企业服务，例如 Active Directory。

云连接器要求

Citrix 使用 Cloud Connector 将 Citrix Endpoint Management 体系结构集成到您现有的基础结构中。Cloud Connector 通过端口 443 安全地将以下资源位置集成到 Citrix Endpoint Management：LDAP、PKI 服务器、内部 DNS 查询和 Citrix Workspace 枚举。

- 至少两台已加入 Active Directory 域的专用 Windows Server 计算机。这些计算机可以是虚拟的，也可以是物理的。安装连接器的计算机必须与 UTC 时间同步，才能正常安装和运行。有关最新要求的完整列表，请参阅您的 Citrix 客户团队提供的部署材料。

  入门向导将指导您在这些计算机上安装 Cloud Connector。
- 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 Citrix Endpoint Management 结合使用。

林功能级别	域功能级别	支持的域控制器
Windows 服务器 2016	Windows 服务器 2016	Windows Server 2016、Windows Server 2019
Windows 服务器 2016	Windows 服务器 2019	Windows 服务器 2019
Windows 服务器 2019	Windows 服务器 2019	Windows 服务器 2019

注意：

> Windows Server 2012 R2、2012 和 2008 R2 已达到生命周期终止，不再受支持。有关详细信息，请参阅 Microsoft 产品生命周期文档。

NetScaler Gateway 要求

Citrix Endpoint Management 需要在您的资源位置安装 NetScaler Gateway，以用于以下场景：

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

要求如下：

- 域 (LDAP) 身份验证
- NetScaler 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。

- 公共 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。

- 用于 NetScaler Gateway 虚拟服务器的未使用的公共 IP 地址
- 用于 NetScaler Gateway 虚拟服务器的可公开解析的完全限定域名 (FQDN)
- 云托管的 Citrix Endpoint Management 中间和根证书（在脚本捆绑包中提供）
- 用于代理负载均衡器 IP 的未使用的内部私有 IP 地址
- 有关端口要求，请参阅本文稍后介绍的NetScaler Gateway 端口要求。
- Citrix Endpoint Management 与 Microsoft Endpoint Manager 集成
- 在 Microsoft Azure 上部署 Citrix ADC VPX 实例(/zh-cn/citrix-adc/current-release/deploying-vpx/deploy-vpx-on-azure.html)

有关 NetScaler Gateway 要求的信息，请参阅您的 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 Citrix Endpoint Management Premium Service 产品中提供。存储区域控制器通过为您的 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：

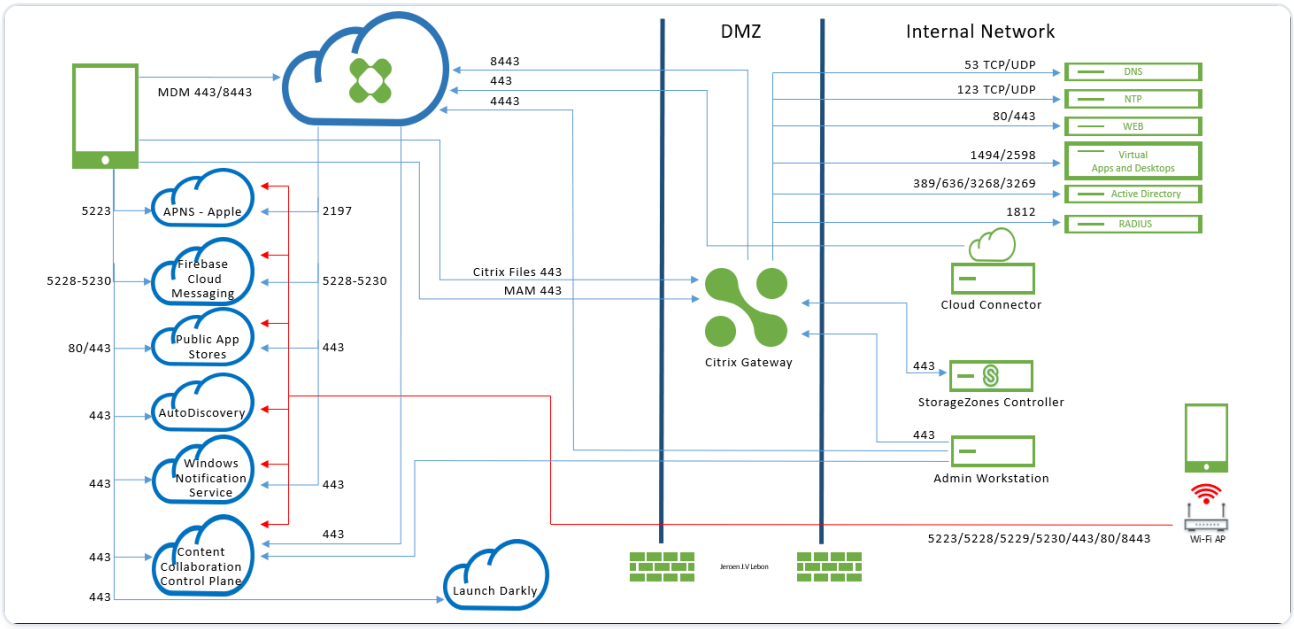
- 专用物理或虚拟机
- Windows Server 2012 R2（数据中心版、标准版或基础版）、Windows Server 2016、Windows Server 2019 或 Windows Server 2022
- 2 个 vCPU
- 4 GB RAM
- 50 GB 硬盘空间
- Web 服务器 (IIS) 的服务器角色：
  - 应用程序开发：ASP. NET 4.5.2
  - 安全性：基本身份验证
  - 安全性：Windows 身份验证

Citrix Files 平台要求：

- Citrix Files 安装程序需要 Windows Server 上的管理权限
- Citrix Files 管理员用户名

端口要求

为了使设备和应用程序能够与 Citrix Endpoint Management 通信，您需要在防火墙中打开特定端口。下图显示了 Citrix Endpoint Management 的流量流。



以下各节列出了您必须打开的端口。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。

NetScaler Gateway 端口要求

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

- Citrix 端点管理
- StoreFront
- 其他内部网络资源，例如 Intranet 网站

有关 NetScaler Gateway 的详细信息，请参阅 NetScaler 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	描述	源	目标
53（TCP 和 UDP）	用于 DNS 连接。	NetScaler 网关 SNIP	DNS 服务器
80/443	NetScaler Gateway 通过第二个防火墙将微 VPN 连接传递到内部网络资源。	NetScaler 网关 SNIP	内网网站
123 (TCP 和 UDP)	用于网络时间协议 (NTP) 服务。	NetScaler 网关 SNIP	NTP 服务器

TCP 端口	描述	源	目标
389	用于不安全的 LDAP 连接。	NetScaler Gateway NSIP（如果使用负载平衡器，则为 SNIP）	LDAP 身份验证服务器或 Microsoft Active Directory
443	用于从思杰工作区到思杰虚拟应用和桌面的思杰店面连接。	互联网	NetScaler 网关
443	用于连接 Citrix Endpoint Management 以交付 Web、移动和 SaaS 应用程序。	互联网	NetScaler 网关
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://*.blob.core.windows.net/`, `https://*.servicebus.windows.net`
443	如果启用，通过浏览器访问 Citrix Endpoint Management 自助服务门户时使用。	访问点（浏览器）	思杰端点管理（`https://<sitename>/zdm/shp`）
636	用于安全的 LDAP 连接。	NetScaler Gateway NSIP（如果使用负载平衡器，则为 SNIP）	LDAP 身份验证服务器或 Active Directory
1494	用于内部网络中基于 Windows 的应用程序的 ICA 连接。Citrix	NetScaler 网关 SNIP	Citrix 虚拟应用和桌面

TCP 端口	描述	源	目标
	建议保持此端口打开。		
1812	用于 RADIUS 连接。	思杰 NetScaler Gateway NSIP	RADIUS 身份验证服务器
2598	用于通过会话可靠性连接到内部网络中的 Windows 应用程序。Citrix 建议保持此端口打开。	思杰 NetScaler Gateway SNIP	Citrix 虚拟应用和桌面
3269	用于 Microsoft 全局编录安全 LDAP 连接。	NetScaler Gateway NSIP（如果使用负载均衡器，则为 SNIP）	LDAP 身份验证服务器或 Active Directory
4443	供管理员通过浏览器访问 Citrix Endpoint Management 控制台。	访问点（浏览器）	思杰端点管理
8443	用于注册、应用商店和移动应用管理 (MAM)。	NetScaler 网关 SNIP	Citrix 端点管理
8443	用于 Citrix Secure Mail 身份验证令牌的安全票证颁发机构 (STA) 端口	NetScaler 网关 SNIP	Citrix 端点管理

网络和防火墙要求

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

从内部网络到 Citrix Cloud 的开放端口：

TCP 端口	源 IP	描述	目标	目标 IP	
443		云连接器	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com` (commercial), `https://*.sharefile.com`, `https://cwsproduction.blob.core.windows.net/downloads`, `https://*.servicebus.windows.net`		
443		管理控制台	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com` (commercial), `https://*.citrix.com`, `https://cwsproduction.blob.core.window`		

TCP 端口	源 IP	描述	目标	目标 IP	
			`s.net/downloads`		
443		Citrix Endpoint Management 自助服务门户通过浏览器访问（如果门户已启用）	Citrix 端点管理		
4443		Citrix Endpoint Management 控制台通过浏览器访问	Citrix 端点管理		

从 Internet 到 DMZ 的开放端口：

TCP 端口	描述	源 IP	目标	目标 IP
443	Citrix Endpoint Management 客户端设备		NetScaler 网关 IP	
443	Citrix Endpoint Management 客户端设备		NetScaler 网关 VIP	
443	Citrix 文件 公共 IP	CTX208318	NetScaler 网关 VIP	

从 DMZ 到内部网络开放的端口：

TCP 端口	描述	源 IP	目标	目标 IP
389 或 636	NetScaler 网关 NSIP		活动目录 IP	

TCP 端口	描述	源 IP	目标	目标 IP
53 (UDP)	NetScaler 网关 NSIP		DNS 服务器 IP	
443	NetScaler 网关 SNIP		Exchange (EAS) 服务器 IP	
443	NetScaler 网关 SNIP		内部 Web 应用程序/服务	
443	NetScaler 网关 SNIP		存储区域控制器 IP	

从内部网络到 DMZ 开放的端口：

TCP 端口	描述	源 IP	目标	目标 IP
443	管理客户端		NetScaler 网关 NSIP	

从内部网络到 Internet 开放的端口：

TCP 端口	描述	源 IP	目标	目标 IP
443	Exchange (EAS) 服务器 IP		Citrix 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`

从公司 Wi-Fi 到 Internet 开放的端口：

TCP 端口	描述	源 IP	目标	目标 IP
8443 / 443	Citrix Endpoint Management 客户端设备		思杰端点管理	
5223	Citrix Endpoint Management 客户端设备		Apple APNS 服务器	`17.0.0.0/8`
5228	Citrix Endpoint Management 客户端设备		Firebase 云消息传递	`android.apis.google.com`, `fcm.googleapis.com`
5229	Citrix Endpoint Management 客户端设备		Firebase 云消息传递	`android.apis.google.com`, `fcm.googleapis.com`
5230	Citrix Endpoint Management 客户端设备		Firebase 云消息传递	`android.apis.google.com`, `fcm.googleapis.com`
443	Citrix Endpoint Management 客户端设备		Firebase 云消息传递	`fcm.googleapis.com`
443	Citrix Endpoint Management 客户端设备		Windows 推送通知服务	`*.notify.windows.com`
443 / 80	Citrix Endpoint Management 客户端设备		Apple iTunes 应用商店	`ax.apps.apple.com`, `*.mzstatic.com`, `vpp.itunes.apple.com`

TCP 端口	描述	源 IP	目标	目标 IP
443 / 80	Citrix Endpoint Management 客户端设备		谷歌应用商店	`play.google.com`, `android.clients.google.com`, `android.l.google.com`, `android.com`, `google-analytics.com`
443 / 80	Citrix Endpoint Management 客户端设备		Microsoft 应用商店	`login.live.com`, `*.notify.windows.com`
443	Citrix Endpoint Management 客户端设备		适用于 iOS 和 Android 的 Citrix Endpoint Management AutoDiscovery 服务	`discovery.cem.cloud.us`
443	Citrix Endpoint Management 客户端设备		适用于 Windows 的 Citrix Endpoint Management AutoDiscovery 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	Citrix Endpoint Management 客户端设备		Google 移动管理、Google API、Google Play 商店 API	`*.googleapis.com`

TCP 端口	描述	源 IP	目标	目标 IP
443	Citrix Endpoint Management 客户端设备		早于 v470 版本的 CloudDPC 的连接性检查。从 N MR1 开始的 Android 连接性检查要求 `https://www.google.com/generate_204` 可访问，或者给定的 Wi-Fi 网络指向可访问的 PAC 文件)	`connectivitycheck.android.com`, `www.google.com`

AutoDiscovery 服务连接的端口要求

此端口配置可确保从适用于 Android 的 Citrix Secure Hub 连接的 Android 设备可以从内部网络访问 Citrix Endpoint Management AutoDiscovery 服务 (ADS)。在下载通过 ADS 提供的任何安全更新时，访问 ADS 的能力非常重要。

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

> 如果要启用证书锁定，请完成以下先决条件：

- **收集 Citrix Endpoint Management 服务器和 NetScaler Gateway 证书：** 证书必须是 PEM 格式的公共证书，而不是私钥。
- **联系 Citrix 支持并提交启用证书锁定的请求：** 在此过程中，系统会要求您提供证书。

证书锁定要求设备在注册之前连接到 ADS。此要求可确保 Citrix Secure Hub 获得最新的安全信息。要使 Citrix Secure Hub 注册设备，设备必须能够访问 ADS。因此，在内部网络中开放 ADS 访问对于启用设备注册至关重要。

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

FQDN	端口	IP 和端口使用情况
`discovery.cem.cloud.us`	443	Citrix Secure Hub - 通过 CloudFront 进行 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。

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 网络要求。

应用程序要求

Citrix Endpoint Management 支持添加和维护最多 300 个应用程序。超过此限制会导致系统变得不稳定。

Citrix 端点管理兼容性

要使用新功能、修复和策略更新，Citrix® 建议您安装以下各项的最新版本：

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

  MDX Toolkit 计划于 2023 年 7 月达到 EOL。要继续管理您的企业应用程序，您必须集成 MAM SDK。
- 移动生产力应用程序

本文总结了您可以集成的受支持 Citrix Endpoint Management 组件的版本。

最新版本的 Citrix Secure Hub、MDX Toolkit 和移动生产力应用程序与最新版本以及之前两个版本的 Citrix 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需要最新版本的 Citrix Secure Hub。应用程序的之前两个版本与最新的 Citrix Secure Hub 兼容。

有关移动生产力应用程序两周分阶段发布节奏的更多信息，请参阅 发布时间表。有关支持详细信息，请参阅 移动生产力应用程序支持。

MAM SDK

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

MDX 工具包

MDX Toolkit 计划于 2023 年 7 月达到 EOL。要继续管理您的企业应用程序，您必须集成 MAM SDK。

Citrix 支持 MDX Toolkit 的最新三个版本 (n.n.n)。请参阅 MDX Toolkit 中的新增功能。

浏览器支持

Citrix Endpoint Management 控制台需要以下受支持的 Web 浏览器之一：

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

支持的设备操作系统

本文介绍了 Citrix Endpoint Management 支持的企业移动管理设备。由于平台限制和安全功能，Citrix Endpoint Management 并非在所有平台上都支持所有功能。

有关移动生产力应用程序的最新版本，请参阅 移动生产力应用程序支持。

> **注意：**
>
> - Citrix 支持每个主要操作系统平台的当前版本和以前版本。某些 Citrix Endpoint Management 功能在较旧的平台版本上不起作用。有关弃用公告，请参阅 弃用。
> - Citrix Endpoint Management™ 支持 Windows x86 和 ARM 类型设备的设备管理。

操作系统支持列表

Citrix Endpoint Management 支持以下操作系统：

- **安卓：** 10.x, 11.x, 12.x, 13.x, 14.x, 15.x, 16.x, 17.x

Citrix® 建议在使用 Android Enterprise 之前升级到 Android 10+。有关详细信息，请参阅 Android 注意事项。

- **苹果iOS：** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  Citrix Endpoint Management 和 Citrix 移动应用程序目前不支持适用于 iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x 和 iOS 27.x 的所有新功能。

- **iPadOS** 版本：13.x、14.x、15.x、16.x、17.x、18.x、26.x、27.x

  Citrix Endpoint Management 和 Citrix 移动应用程序目前不支持所有新的 iPadOS 14.x、iPadOS 15.x、iPadOS 16.x、iPadOS 17.x、iPadOS 18.x、iPadOS 26.x 和 iPadOS 27.x 功能。

- **macOS** 版本：11.x、12.x、13.x、14.x、15x

  Citrix Endpoint Management 和 Citrix 移动生产力应用程序目前不支持适用于 macOS 11、macOS 12、macOS 13、macOS 14 和 macOS 15 的所有新功能。

- **Windows 10 和 Windows 11 台式机和平板电脑：**（仅限 MDM）

  - Windows 10 专业版和 Windows 11 专业版
  - Windows 10 企业版和 Windows 11 企业版
  - Windows 10 教育版和 Windows 11 教育版
  - Windows IoT 企业版

  请参阅 Microsoft 文档，以了解针对特定操作系统的支持级别。

Android 注意事项

升级到 Android 10 或更高版本之前：有关 Google 设备管理 API 弃用如何影响运行 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 弃用了设备管理 API，这会影响运行 Android 10+ 的设备。Android 10+ 设备在旧版设备管理模式下注册失败。Citrix 不支持在设备管理模式下注册 Android 设备。
- Citrix 建议将 Android Enterprise 用于 Android 设备。有关详细信息，请参阅从设备管理迁移到 Android Enterprise。
- Google API 更改不影响在仅 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在 subjectAltName (SAN) 扩展中具有匹配主机名的安全证书。

- 要验证主机名，服务器必须提供具有匹配 SAN 的证书。Citrix 仅信任具有与主机名匹配的 SAN 的证书。

语言支持

Citrix 移动生产力应用程序和 Citrix Endpoint Management 控制台已针对英语以外的语言进行了调整。即使应用程序未本地化为用户的首选语言，此支持也包括非英语字符和键盘输入。有关所有 Citrix 产品的全球化支持的更多信息，请参阅 `<https://support.citrix.com/article/CTX119253>`。

本文列出了最新版 Citrix Endpoint Management 中支持的语言。

Citrix 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 表示该应用程序支持该特定语言。

iOS 和 安卓

语言	安全中心	安全邮件	安全网络	安全笔记	安全任务	QUICKED IT
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

语言	安全中心	安全邮件	安全网络	安全笔记	安全任务	QUICKED IT
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	-	-	-
波兰语	X	X	X	-	-	-

从右到左语言支持

下表总结了每个应用程序对中东语言文本的支持。X 表示该功能适用于该平台。Windows 设备不支持从右到左的语言。

应用程序	IOS	安卓
Citrix 安全集线器	X	X
Citrix 安全邮件	X	X
Citrix 安全网络	X	X
QuickEdit	X	X

FIPS 140-2 合规性

美国国家标准与技术研究院 (NIST) 发布了联邦信息处理标准 (FIPS)。FIPS 规定了安全系统中使用的加密模块的安全要求。FIPS 140-2 是此标准的第二个版本。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 上所有静态数据和传输中数据的加密操作均使用 FIPS 验证的加密模块。在 Android 上，所有静态数据加密操作使用 Citrix® 提供的 FIPS 验证的加密模块或设备制造商提供的平台加密模块。有关设备制造商模块的更多信息，请联系您的 Citrix 代表。

适用于受支持的 Windows 设备上的移动设备管理 (MDM) 的所有静态数据和传输中数据的加密操作均使用 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的加密操作均使用 FIPS 验证的加密模块。MDM 流的所有静态数据和传输中数据均端到端使用 FIPS 兼容的加密模块。该安全性包括前面所述的移动设备加密操作，以及移动设备与 NetScaler Gateway 之间的加密操作。

MDX Vault 使用 FIPS 验证的加密模块加密 iOS 和 Android 设备上的 MDX 封装的应用程序和相关的静态数据。

关于 Citrix Endpoint Management 的信息

Citrix Endpoint Management 是一种统一端点管理 (UEM) 解决方案，可将所有应用程序和端点整合到一个统一视图中，以提高安全性和生产力。有关 UEM 的概述，请参阅 Citrix Tech Zone 技术简报 Citrix Endpoint Management。

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

Citrix Endpoint Management 的 MDM 功能使您能够：

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

Citrix Endpoint Management 的 MAM 功能使您能够：

- 保护自带移动设备上的应用程序和数据。
- 交付企业移动应用程序。
- 锁定应用程序并擦除其数据。

结合 MDM 和 MAM 功能，您可以：

- 通过使用 MDM 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 Citrix Endpoint Management 支持 MDM、MAM 或 MDM+MAM 的功能。

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
Android Enterprise 功能概述：			

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
设备注册支持	是	是	是
域身份验证支持	是	否	是
支持域加安全令牌身份验证	否	否	是
支持客户端证书身份验证	否	是	是
支持客户端证书加域身份验证	否	否	是
支持客户端证书加安全令牌	否	否	是
支持 Azure AD 身份提供程序	是	否	是
支持 Okta 身份提供程序	是	否	是
对本机 SaaS 应用程序进行单点登录	是	否	是
Citrix 内容分发网络对企业应用的支持	是	是	是
Citrix 内容分发网络对 MDX 应用的支持	是	是	是
通过预配专用 Android Enterprise (COSU) 设备支持共享设备	是	否	是
Android（旧版）：			
设备注册支持	是	是	是
支持域或域加安全令牌身份验证	否	否	是

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
支持客户端证书身份验证	否	是	是
支持客户端证书加域身份验证	否	否	是
支持客户端证书加安全令牌	否	否	是
支持 Azure AD 和 Citrix 身份提供程序	是	否	是
支持 Okta 身份提供程序	是	否	是
对本机 SaaS 应用程序进行单点登录	是	否	是
Citrix 内容分发网络对企业应用的支持	是	是	是
Citrix 内容分发网络对 MDX 应用的支持	是	是	是
Chrome 浏览器：			
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

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
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
本机 SaaS 应用程序的单点登录	是	否	是
Citrix 内容分发网络对企业应用程序的支持	是	是	是
Citrix 内容分发网络对 MDX 应用程序的支持	是	是	是
苹果教育集成	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
视窗：			
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

功能（按平台）	MDM (1)	MAM (2)	MDM+MAM
支持域或域加安全令牌身份验证	是	否	否
支持客户端证书身份验证	是	否	否
支持客户端证书加域身份验证	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
Citrix 内容分发网络对企业应用程序的支持	是	否	否
工作区环境管理™ 集成 (3)	是	否	否

注意：

(1) 部署顺序仅适用于配置了 MDM 注册配置文件的交付组中的设备。

(2) MAM 注册需要 NetScaler Gateway。

(3) Workspace Environment Management (WEM) 集成提供了对各种 Windows 操作系统上的 MDM 功能的访问。

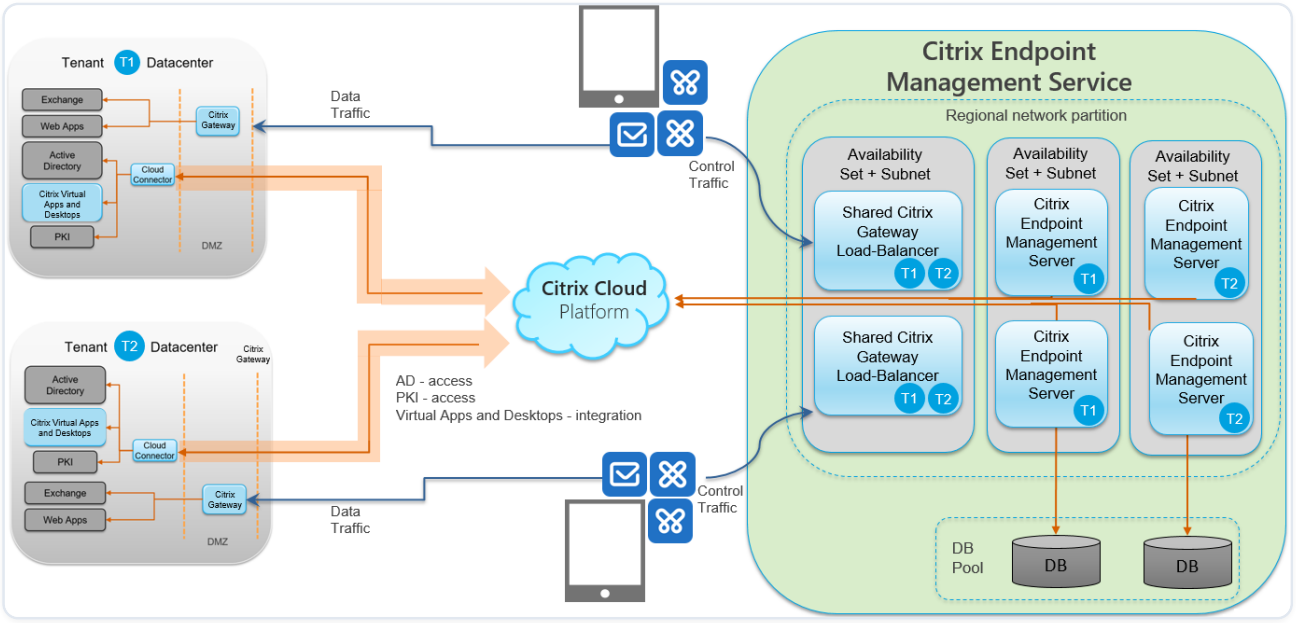
有关详细信息，请参阅管理模式。

体系结构

您的组织的设备和应用程序管理要求决定了 Citrix Endpoint Management 体系结构中的 Citrix Endpoint Management 组件。Citrix Endpoint Management 的组件是模块化的，并且相互构建。例如，您的部署包括 NetScaler Gateway：

- NetScaler Gateway 为用户提供对移动应用程序的远程访问，并跟踪用户设备类型。
- Citrix Endpoint Management 是您管理这些应用程序和设备的地方。

下图显示了 Citrix Endpoint Management 云部署及其与数据中心集成的总体体系结构概述。



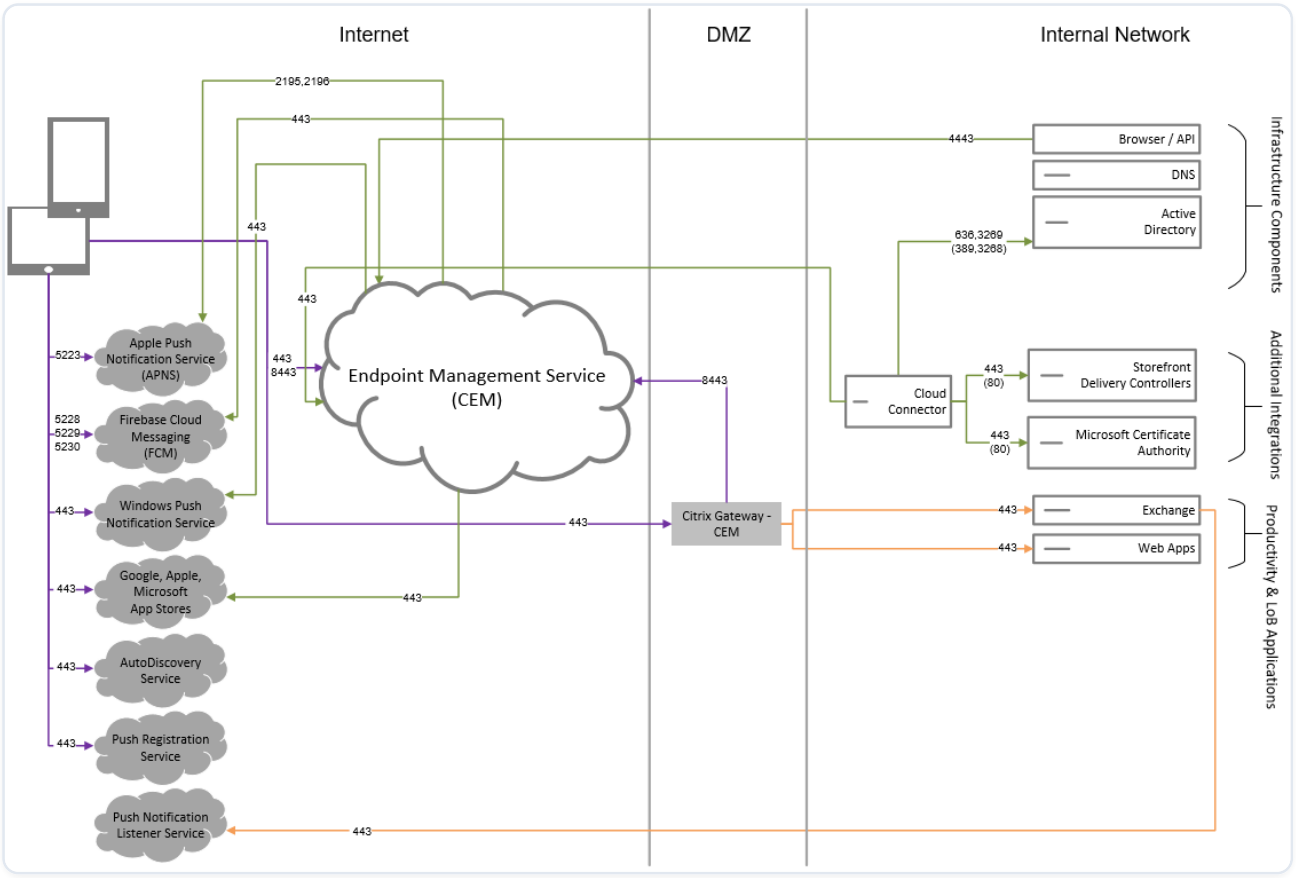
以下小节包含以下内容的参考体系结构图：

- Citrix 端点管理
- 可选组件，例如外部证书颁发机构、适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器，以及 Citrix Endpoint Management MDM+MAM 和 Intune MAM 流量流。

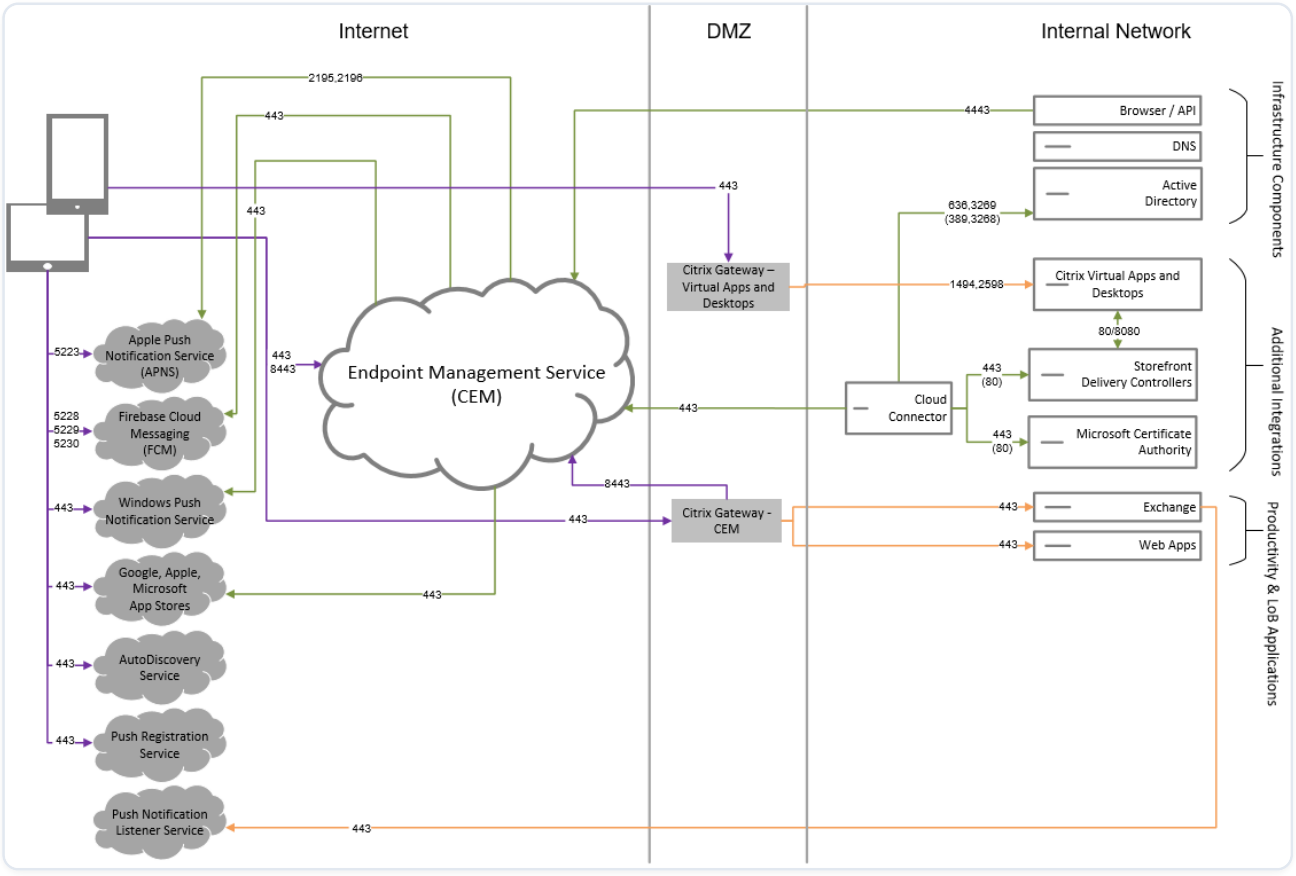
有关 Citrix ADC 和 NetScaler Gateway 要求的详细信息，请参阅 `<https://docs.citrix.com/>` 处的 Citrix 产品文档。

核心参考体系结构

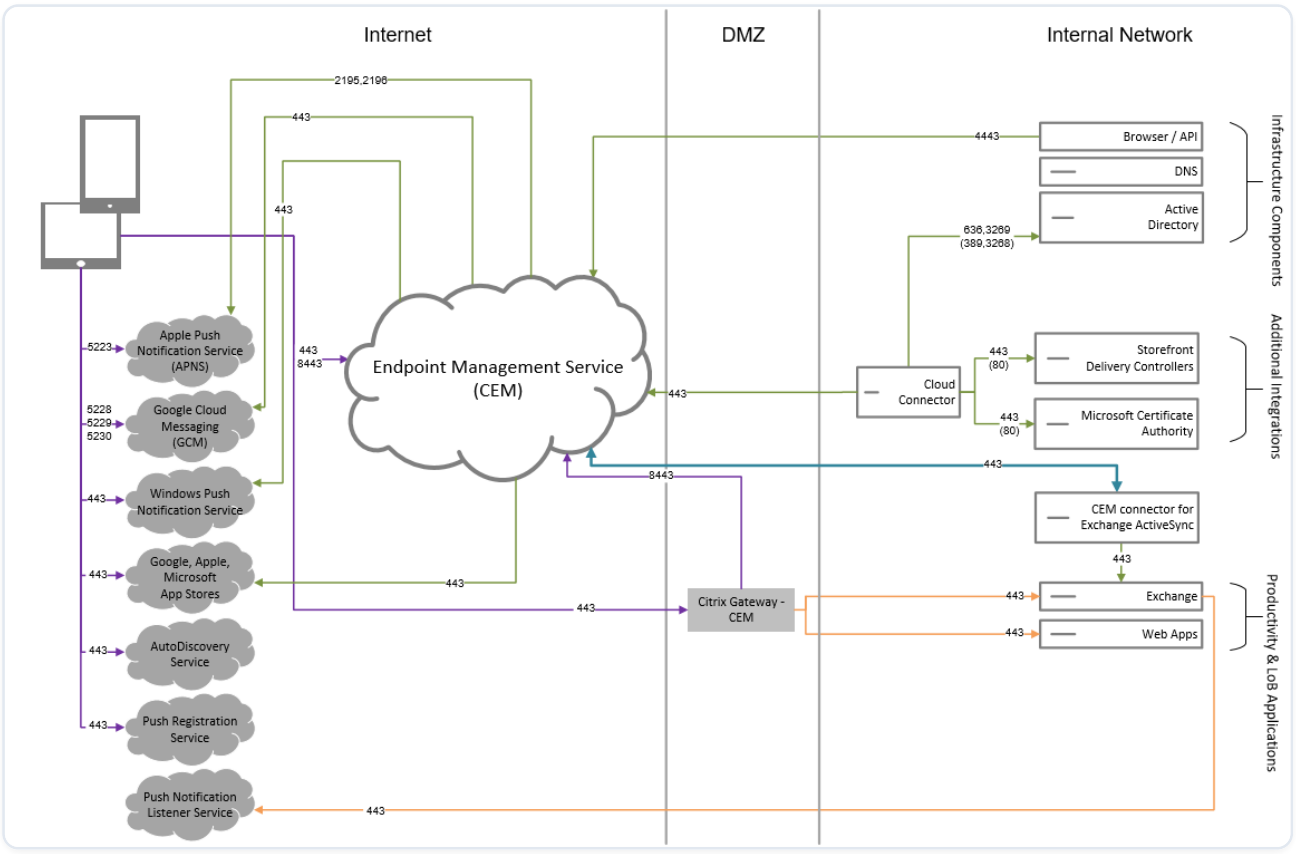
有关端口要求的详细信息，请参阅系统要求。



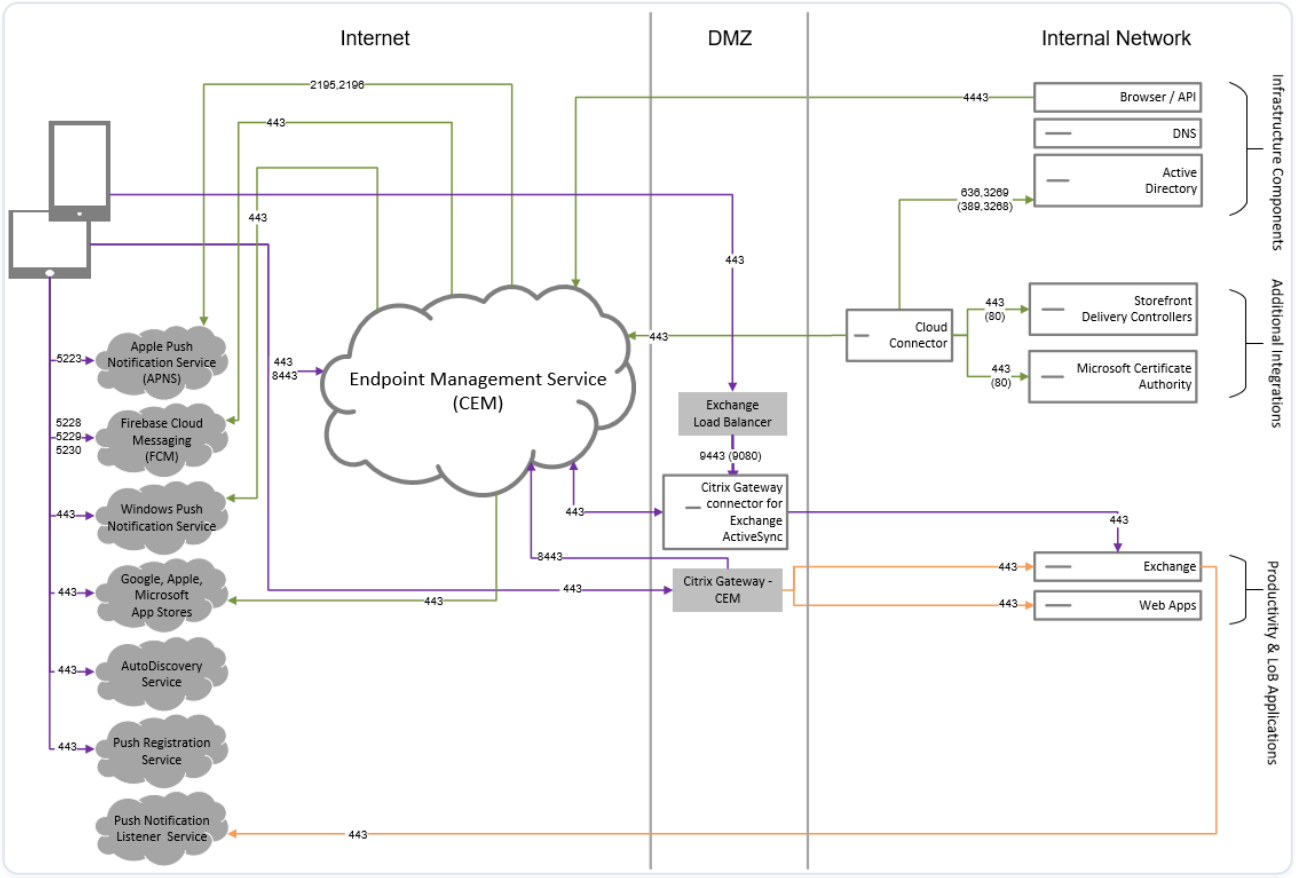
Citrix Virtual Apps and Desktops™ 的参考架构



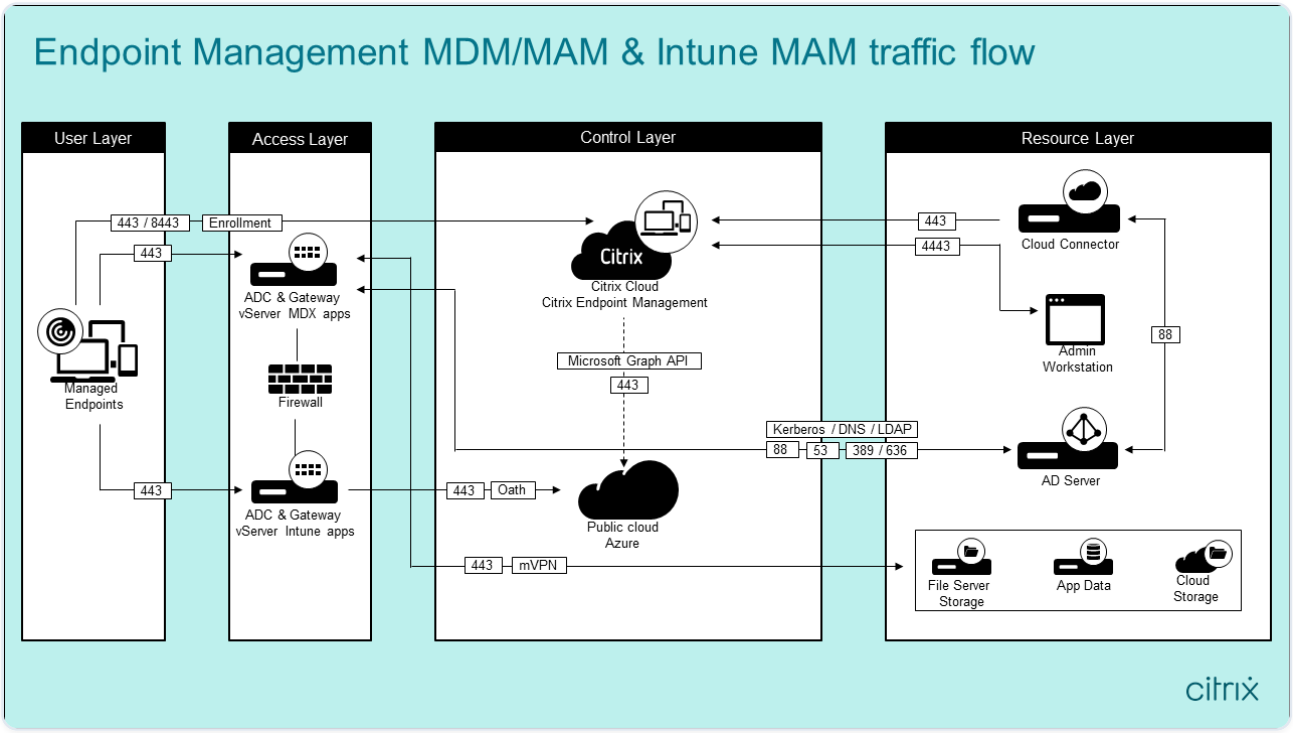
Citrix Endpoint Management 与 Exchange ActiveSync 连接器的参考架构



NetScaler Gateway 与 Exchange ActiveSync 连接器的参考架构



Citrix Endpoint Management MDM+MAM 和 Intune MAM 的参考架构



资源位置

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

- 靠近订阅者
- 靠近数据
- 扩展要求
- 安全属性

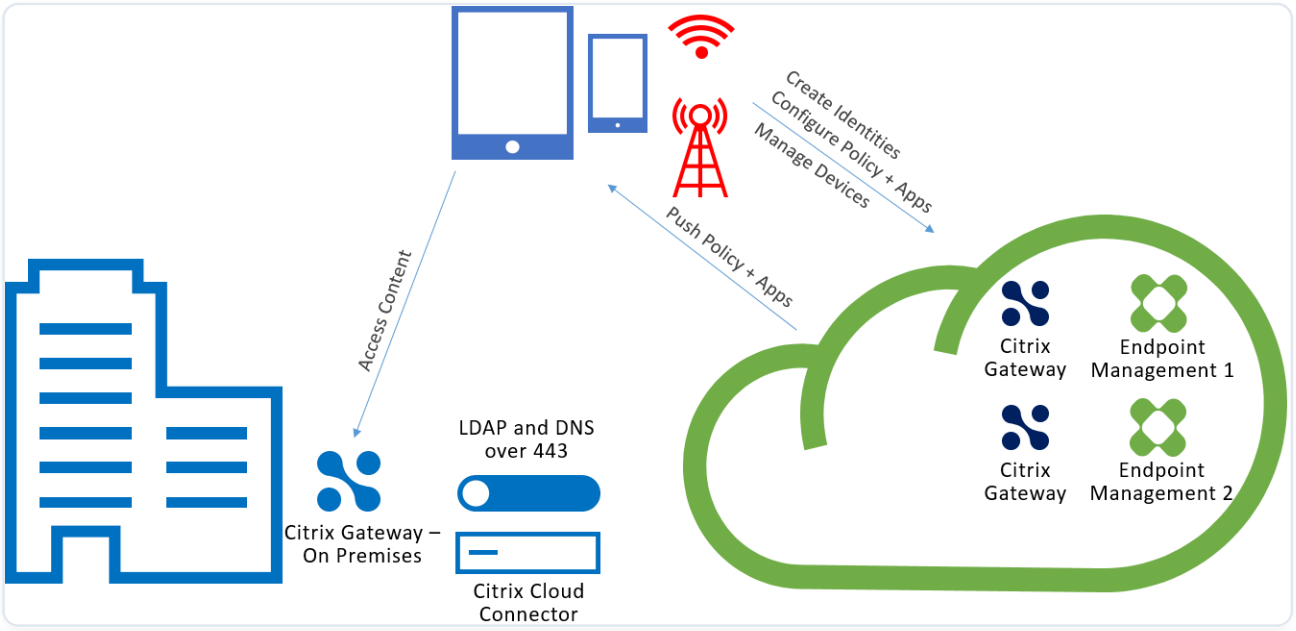
您可以构建任意数量的资源位置。例如，您可以：

- 在数据中心为总部构建一个资源位置，基于需要靠近数据的订阅者和应用程序。
- 在公有云中为全球用户添加一个单独的资源位置。或者，在分支机构中构建单独的资源位置，以提供最适合分支机构员工使用的应用程序。
- 在提供受限应用程序的单独网络上添加另一个资源位置。此设置可提供对其他资源和订阅者的受限可见性，而无需调整其他资源位置。

云连接器

Cloud Connector 负责验证和加密 Citrix Cloud 与您的资源位置之间的所有通信。访问以下服务需要 Cloud Connector：LDAP、IdP、PKI 服务器、内部 DNS 查询、Citrix Virtual Apps、NetScaler Gateway、Citrix Workspace 和 Microsoft Endpoint Manager。

下图显示了 Cloud Connector 的流量流。



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

Cloud Connector 仅在设备注册期间承受负载。有关详细信息，请参阅 Cloud Connector 的规模和大小注意事项。

包含移动应用程序管理 (MAM) 的解决方案需要由本地 NetScaler Gateway 提供的微型 VPN。在此场景中：

- 以下组件位于您的数据中心：
  - 云连接器
  - NetScaler 网关
  - 您的 Exchange、Web 应用程序、Active Directory 和 PKI 服务器
- 移动设备与 Citrix Endpoint Management 和您的本地 NetScaler Gateway 通信。

Citrix 端点管理 组件

Citrix Endpoint Management 控制台。 您可以使用 Citrix Endpoint Management 管理员控制台配置 Citrix Endpoint Management。有关使用 Citrix Endpoint Management 控制台的详细信息，请参

阅 (/zh-cn/citrix-endpoint-management/endpoint-management.html) 下的文章。当 Citrix Endpoint Management 的新增功能文章更新以发布新版本时，Citrix 会通知您。

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

- 远程支持客户端不适用于 Citrix Endpoint Management。
- Citrix 不支持 Citrix Endpoint Management 与本地 syslog 服务器的 syslog 集成。相反，您可以从 Citrix Endpoint Management 控制台的**故障排除和支持**页面下载日志。执行此操作时，您必须单击**全部下载**。

MAM SDK。 MDX Toolkit 计划于 2023 年 7 月达到 EOL。要继续管理您的企业应用程序，您必须集成 MAM SDK。

- 移动应用程序管理 (MAM) SDK 提供了 iOS 和 Android 平台未涵盖的 MDX 功能。您可以启用 MDX 并保护 iOS 或 Android 应用程序。您可以将这些应用程序发布到内部商店或公共应用程序商店。请参阅 (/zh-cn/mdx-toolkit/mam-sdk-overview.html)。

移动生产力应用程序。 Citrix 开发的移动生产力应用程序在 Citrix Endpoint Management 环境中提供了一套生产力与通信工具。您的公司策略可保护这些应用程序。有关详细信息，请参阅 (/zh-cn/mobile-productivity-apps.html)。

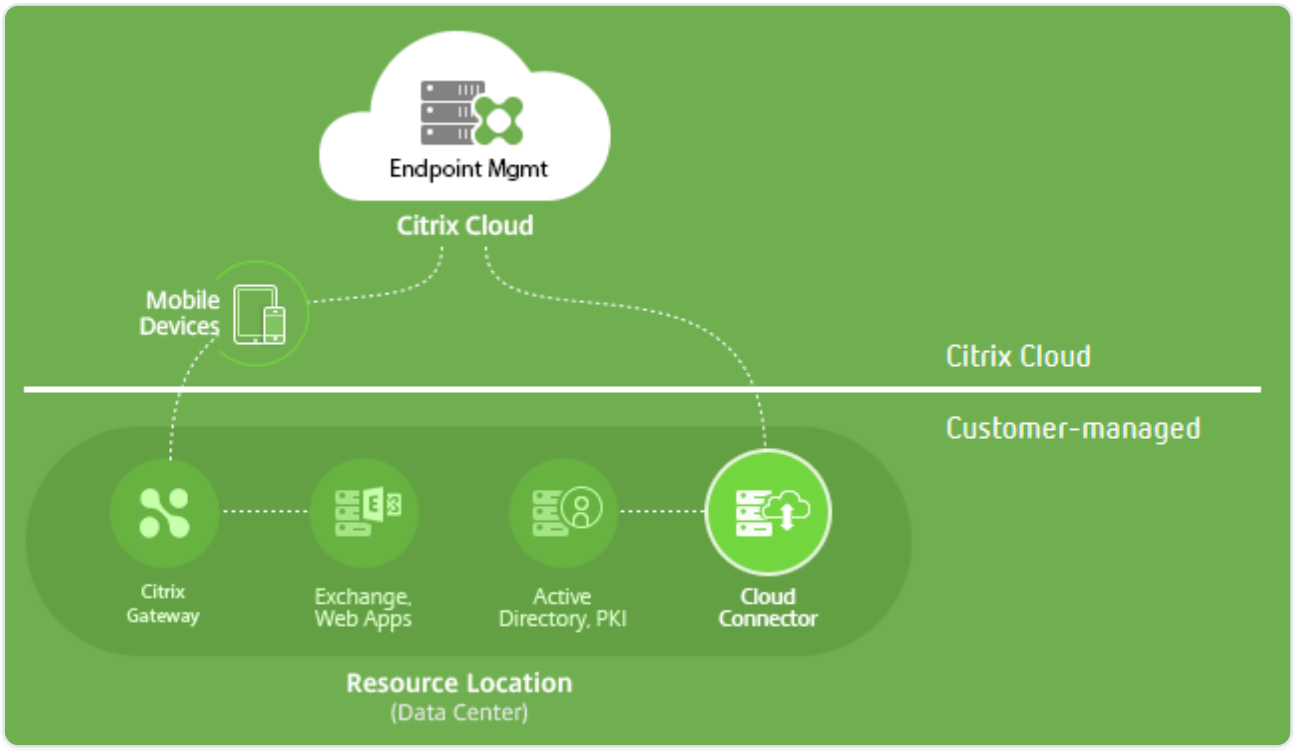
Citrix Endpoint Management for Exchange ActiveSync 连接器。 Citrix Endpoint Management for Exchange ActiveSync 连接器为使用本机移动电子邮件应用程序的用户提供安全的电子邮件访问。Exchange ActiveSync 连接器在 Exchange 服务级别提供 ActiveSync 筛选。因此，筛选仅在邮件到达 Exchange 服务时发生，而不是在邮件进入 Citrix Endpoint Management 环境时发生。该连接器不需要使用 NetScaler Gateway。您可以在不更改现有 ActiveSync 流量路由的情况下部署连接器。有关详细信息，请参阅 (/zh-cn/citrix-endpoint-management/restrict-email-access/connector-exchange-activesync.html)。

NetScaler Gateway for Exchange ActiveSync 连接器。 NetScaler Gateway for Exchange ActiveSync 连接器为使用本机移动电子邮件应用程序的用户提供安全的电子邮件访问。Exchange ActiveSync 连接器在边界处提供 ActiveSync 筛选。筛选使用 NetScaler Gateway 作为 ActiveSync 流量的代理。因此，筛选组件位于邮件流量流的路径中，在邮件进入或离开环境时进行拦截。Exchange ActiveSync 连接器充当 NetScaler Gateway 和 Citrix Endpoint Management 之间的中介。有关详细信息，请参阅 (/zh-cn/citrix-endpoint-management/restrict-email-access/gateway-connector-exchange-activesync.html)。

Citrix Endpoint Management 技术安全概述

Citrix Cloud 管理 Citrix Endpoint Management 环境的控制平面。控制平面包括 Citrix 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 与客户数据中心集成。使用 Cloud Connector 的 Citrix Endpoint Management 客户通常在其数据中心管理 NetScaler Gateway。

下图说明了该服务及其安全边界。



本节中的信息：

- 介绍 Citrix Cloud 的安全功能。
- 定义 Citrix 与客户之间在保护 Citrix Cloud 部署方面的职责划分。
- 不是 Citrix Cloud 或其任何组件或服务的配置或管理指南。

有关 Citrix Endpoint Management 用于提供全面端到端安全性的技术信息，请参阅 移动企业安全与生产力。

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。这些对象位于您的目录、DNS 和类似服务中。控制平面通过 Citrix Cloud Connector 经由安全的 HTTPS 连接访问这些服务。

公司数据（例如电子邮件、内网和 Web 应用程序流量）通过 NetScaler Gateway 在设备和应用程序服务器之间直接流动。NetScaler Gateway 部署在客户数据中心。

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。服务本身由多租户和单租户组件混合组成。但是，根据服务架构，客户元数据始终为每个租户单独存储，并使用唯一凭据进行保护。

凭据处理

该服务处理以下类型的凭据：

- **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使用客户目录中的目录验证这些凭据。
- **管理员凭据：** 管理员通过 Citrix Cloud 进行身份验证，Citrix Cloud 使用 Citrix Online 的登录系统。此过程会生成一个一次性签名的 JSON Web Token (JWT)，该令牌授予管理员对服务的访问权限。
- **Active Directory 凭据：**控制平面需要绑定凭据才能从 Active Directory 读取用户元数据。这些凭据使用 AES-256 加密并保存在每个租户的数据库中。

部署注意事项

Citrix 建议您查阅已发布的最佳实践文档，以了解如何在您的环境中部署 NetScaler Gateway。

更多资源

建议客户查阅与其 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。另请考虑在您的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：Citrix Cloud 平台安全部署指南
- Citrix ADC 安全部署指南

与移动威胁防御软件集成

移动威胁防御 (MTD) 软件可检测、分析并帮助防止针对企业移动设备的复杂网络攻击。MTD 与统一 Citrix Endpoint Management (UEM) 的结合可提高组织的安全性和可见性。

MTD 软件提供 Citrix Endpoint Management 用于以下目的的威胁数据：

- 防范恶意软件、网络钓鱼、网络攻击和中间人攻击
- 确定设备合规性状态

- 确定风险级别
- 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：

- 检查点
- 瞭望
- 万德拉
- 津佩里姆

如需了解更多信息或请求演示，请联系我们的 MTD 合作伙伴或您的 Citrix 销售代表。

Citrix 端点管理与 Microsoft 端点管理器集成

Citrix Endpoint Management 与 Microsoft Endpoint Manager (MEM) 集成，为支持 Microsoft Intune 的应用程序（例如 Microsoft Edge 浏览器）增加了 Citrix Endpoint Management 微 VPN 的价值。

要激活集成，请联系 Citrix Cloud 运营团队。

此版本支持以下用例：

- Intune MAM 与 Citrix 端点管理 MDM+MAM。

  本文重点介绍 Intune MAM + Citrix Endpoint Management MDM+MAM 用例。将 Citrix 添加为 MDM 提供程序后，配置 Intune 托管应用程序以交付到设备。

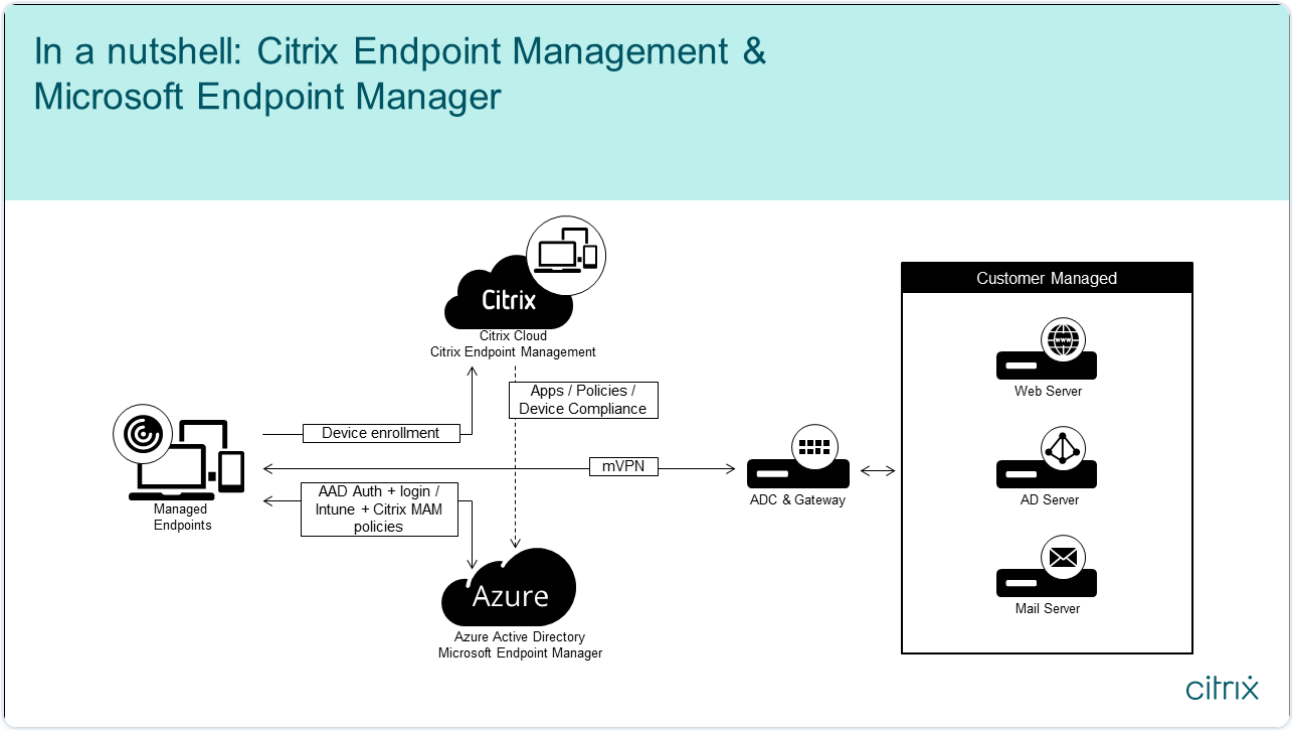
  > **重要提示：**
  >
  > - 对于此用例，Citrix Secure Mail 不支持与 Intune 集成。
  > - Citrix Secure Mail 与 Intune 的集成已弃用，并将在未来版本中移除。有关更多详细信息，请参阅 Secure Mail 中的新增功能。

- Intune MAM 和 Citrix Endpoint Management MDM。
- Intune MAM。
- Intune MAM 和 Intune MDM。适用于 iOS 的 Citrix Secure Mail 支持此用例的单点登录。

有关设置 Citrix Endpoint Management 与 MEM 集成的易于遵循的图形指南，请参阅 入门指南。

有关与 Azure AD 条件访问集成的详细信息，请参阅 与 Azure AD 条件访问集成。

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



系统要求

MDX 启用

- MAM SDK

  或

- MDX 工具包

微软

- Azure Active Directory (AD) 访问（具有租户管理员权限）
- 启用 Intune 的租户

防火墙规则

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

先决条件

- **Microsoft Edge 浏览器：** 移动应用 SDK 已集成到适用于 iOS 和 Android 的 Microsoft Edge 浏览器应用中。有关 Microsoft Edge 的更多信息，请参阅 Microsoft Edge 文档。

- **Citrix Cloud 帐户：** 要注册 Citrix 帐户并申请 Citrix Endpoint Management 试用版，请联系您的 Citrix 销售代表。准备好继续时，请访问 https://onboarding.cloud.com。有关申请 Citrix Cloud 帐户的更多信息，请参阅 注册 Citrix Cloud。

  > **注意：**
  >
  > 您提供的电子邮件必须是未与 Azure AD 关联的地址。您可以使用任何免费电子邮件服务。

- **适用于 iOS 的 APNs 证书：** 请确保为 iOS 配置 APNs 证书。要了解有关设置这些证书的更多信息，请参阅此 Citrix 博客文章：创建和导入 APNs 证书。
- **Azure AD 同步：** 设置 Azure AD 与本地 Active Directory 之间的同步。请勿在域控制器计算机上安装 AD 同步工具。有关设置此同步的更多信息，请参阅 Microsoft 关于 Azure Active Directory 的文档。

配置 NetScaler Gateway

如果您正在设置新的 Citrix Endpoint Management 部署，请安装以下 NetScaler 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 NetScaler Gateway 与 Citrix Endpoint Management 和 MEM 集成使用，请执行以下操作：

- 使用管理界面和子网 IP 配置 NetScaler Gateway。
- 所有客户端到服务器的通信都使用 TLS 1.2。有关为 NetScaler Gateway 配置 TLS 1.2 的信息，请参阅 CTX247095。

如果您正在将 Citrix Endpoint Management 与 MEM 集成，并使用 Citrix Endpoint Management MDM+MAM 部署，请配置两个 Citrix Gateway。MDX 应用程序流量通过一个 NetScaler Gateway 路由。Intune 应用程序流量通过另一个 NetScaler Gateway 路由。配置：

- 两个公共 IP。
- 可选地，一个网络地址转换的 IP。
- 两个 DNS 名称。示例：`https://mam.company.com`。
- 两个公共 SSL 证书。配置与保留的公共 DNS 名称匹配的证书或使用通配符证书。
- 一个具有内部不可路由的 RFC 1918 IP 地址的 MAM 负载均衡器。

- 一个 LDAP Active Directory 服务帐户。

同意委托权限提示

对于需要用户进行身份验证的托管应用程序，这些应用程序会请求 Microsoft Graph 公开的应用程序权限。通过同意这些权限提示，应用程序可以访问所需的资源和 API。某些应用程序需要 Microsoft Azure AD 全局管理员的同意。对于这些委托权限，全局管理员必须授予 Citrix Cloud 请求令牌的权限。然后，这些令牌将启用以下权限。有关详细信息，请参阅 Microsoft Graph 权限参考。

- **登录并读取用户配置文件：** 此权限允许用户登录并连接到 Azure AD。Citrix® 无法查看用户凭据。
- **读取所有用户的基本配置文件：** 此应用读取组织中用户的配置文件属性。这些属性包括组织中用户的显示名称、名字和姓氏、电子邮件地址和照片。
- **读取所有组：** 此权限允许为应用和策略分配指定 Azure AD 组。
- **以登录用户身份访问目录：** 此权限验证 Intune 订阅并启用 NetScaler Gateway 和 VPN 配置。
- **读取和写入 Microsoft Intune 应用：** 此应用可以读取和写入以下内容：
  - Microsoft 管理的属性
  - 组分配和应用状态
  - 应用配置
  - 应用保护策略

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

- 批准为微型 VPN 选择的 Active Directory。全局管理员还必须生成一个客户端密钥，NetScaler Gateway 使用该密钥与 Azure AD 和 Intune 进行通信。
- 不担任 Citrix 管理员角色。相反，Citrix 管理员将 Azure AD 帐户分配给具有相应 Intune 应用程序管理员权限的用户。然后，Intune 管理员担任 Citrix Cloud 管理员角色，从 Citrix Cloud 内部管理 Intune。

> **注意：**
>
> Citrix 仅在设置期间使用 Intune 全局管理员密码，并将身份验证重定向到 Microsoft。Citrix 无法访问该密码。

配置 Citrix Endpoint Management 与 MEM 的集成

1. 登录 Citrix Cloud 站点并申请 Citrix Endpoint Management 试用版。
2. 销售工程师会与您安排一次入职会议。告知他们您需要 Citrix Endpoint Management 与 MEM 集成。请求获批后，单击“**管理**”。

   Citrix Cloud 站点(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems1.png)
3. 在此处，您可以单击站点右上角的齿轮图标，也可以单击“**配置站点**”。

   Citrix Cloud 站点(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-configure-site.png)
4. 按照第一步中的链接转到“**身份和访问管理**”页面。

   身份和访问管理链接(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems2.png)
5. 单击“**连接**”以连接您的 Azure AD 安装。

   身份和访问管理页面(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems3.png)
6. 输入 Azure AD 管理员用于登录的唯一登录 URL，然后单击“**确认**”。

   登录 URL 屏幕和连接按钮(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems4.png)
7. 添加 Azure AD 全局管理员帐户，然后接受权限请求。

   使用其他帐户按钮(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems5.png)

   接受按钮](/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems6.png)
8. 确认您的 Azure AD 实例已成功连接。要指示连接成功，**未连接**文本会更改为**已启用**。

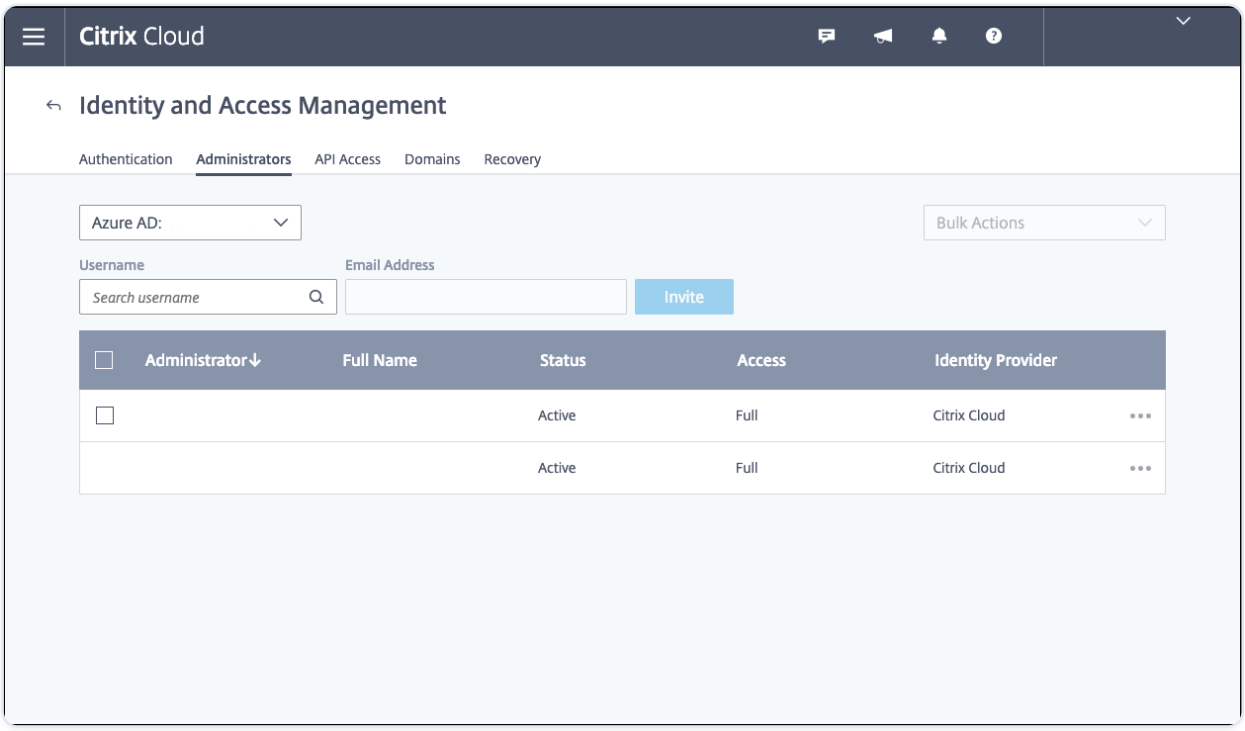
   断开连接按钮(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems7.png)
9. 点击“**管理员**”选项卡，然后将您的 Azure AD Intune 管理员添加为 Citrix Cloud 管理员。从下拉菜单中选择 Azure AD 或 Citrix Identity，然后搜索您要添加的用户名。点击“**邀请**”，然后授予用户“**完全访问权限**”或“**自定义访问权限**”，再点击“**发送邀请**”。

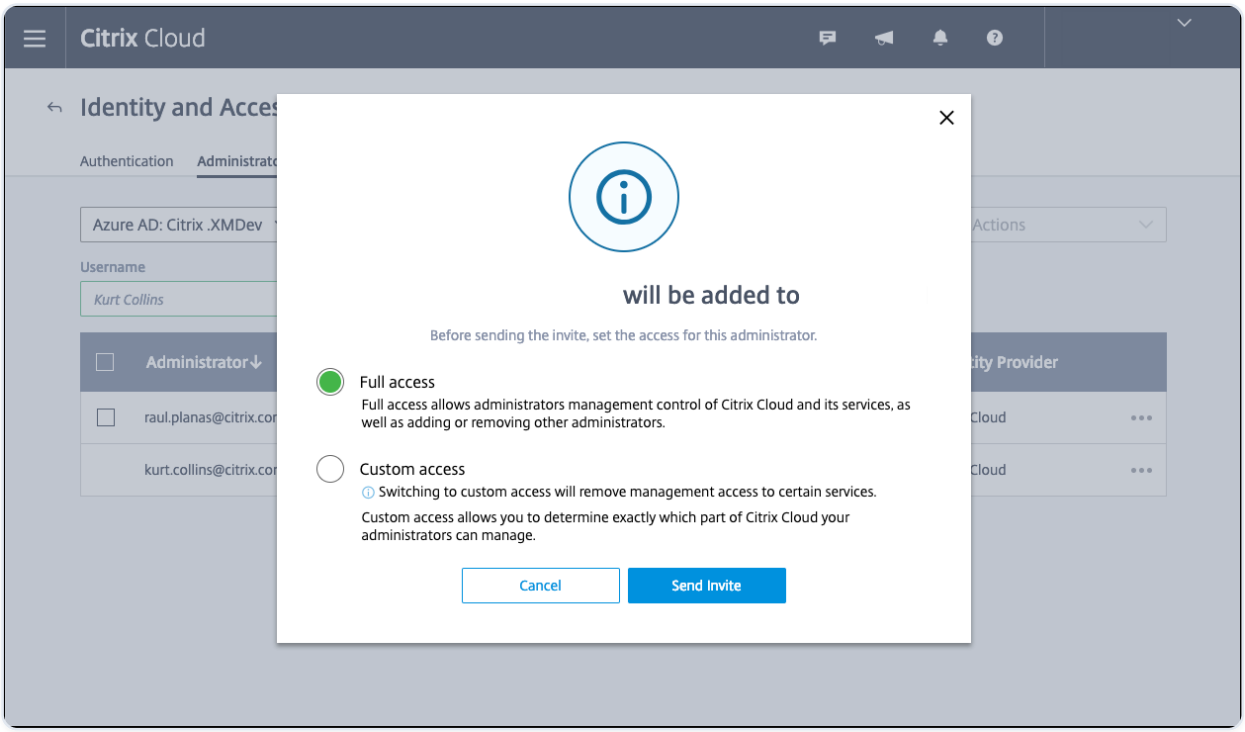
> **注意：**

> Citrix Endpoint Management 对“**自定义访问权限**”要求以下规则：库和 Citrix Endpoint Management。

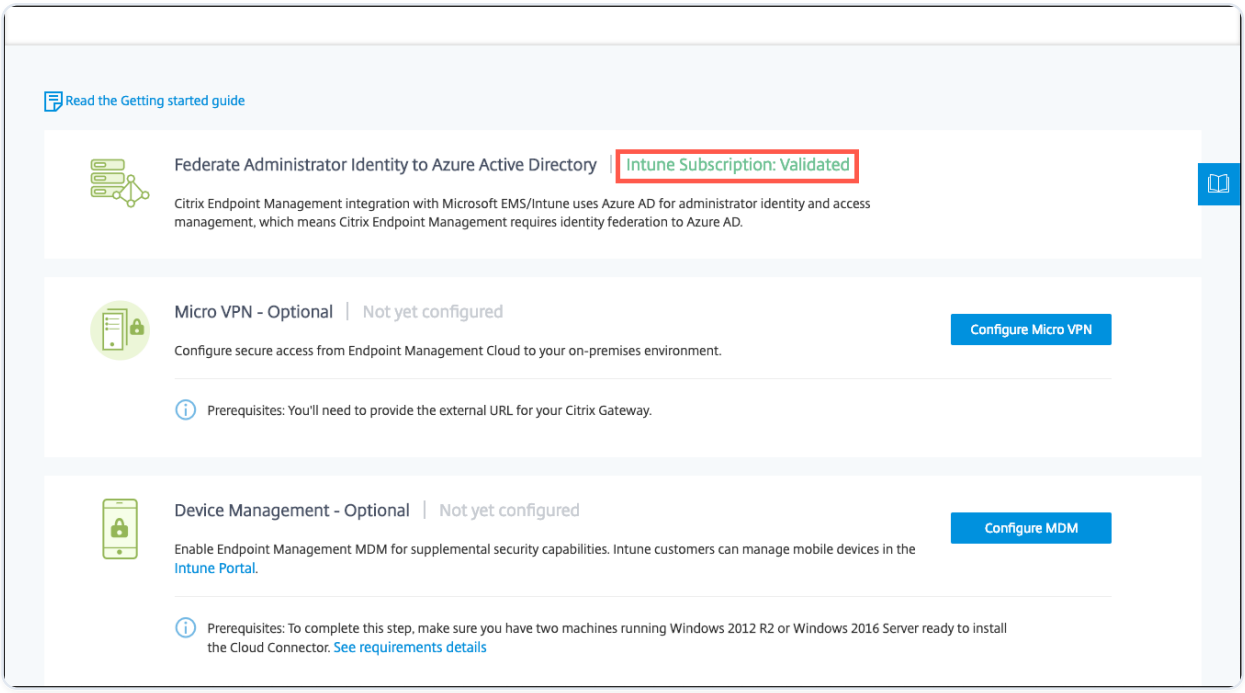
> 因此，Azure AD Intune 管理员会收到一封电子邮件邀请，要求其创建密码并登录 Citrix Cloud。在管理员登录之前，请确保您已从所有其他帐户注销。

Azure AD Intune 管理员必须遵循此过程中的其余步骤。





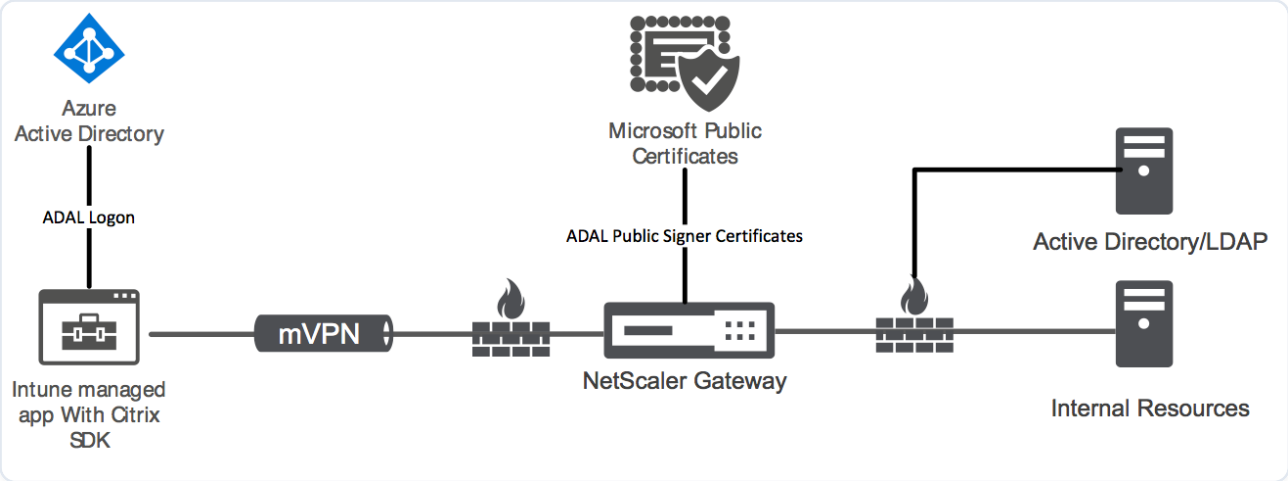
10. 使用新帐户登录后，在“**Citrix Endpoint Management**”下，点击“**管理**”。如果您配置正确，页面会显示 Azure AD 管理员已登录且您的 Intune 订阅有效。



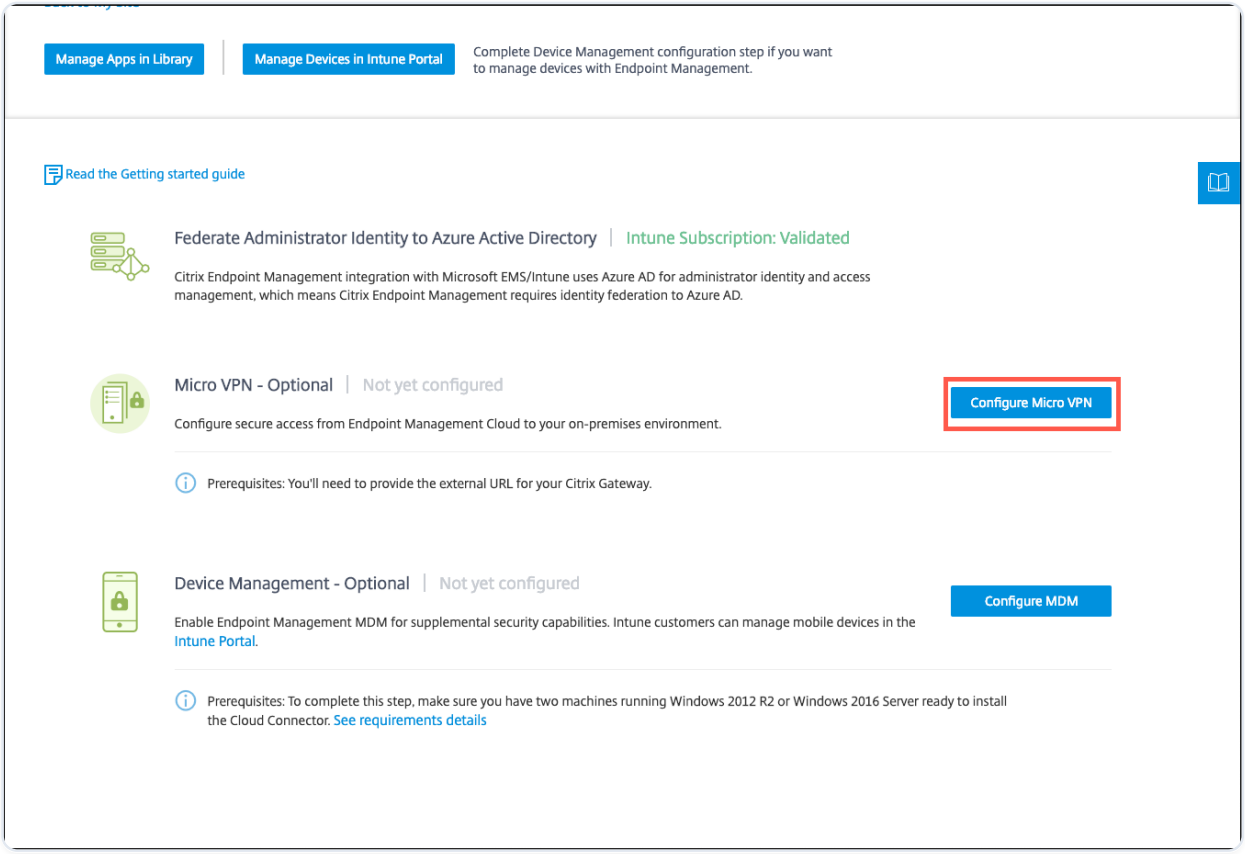
配置 NetScaler Gateway 以用于微 VPN

要将微 VPN 与 Intune 结合使用，您必须配置 NetScaler Gateway 以向 Azure AD 进行身份验证。现有的 NetScaler Gateway 虚拟服务器不适用于此用例。

首先，配置 Azure AD 以与本地 Active Directory 同步。此步骤对于确保 Intune 和 NetScaler Gateway 之间的身份验证正常进行是必要的。

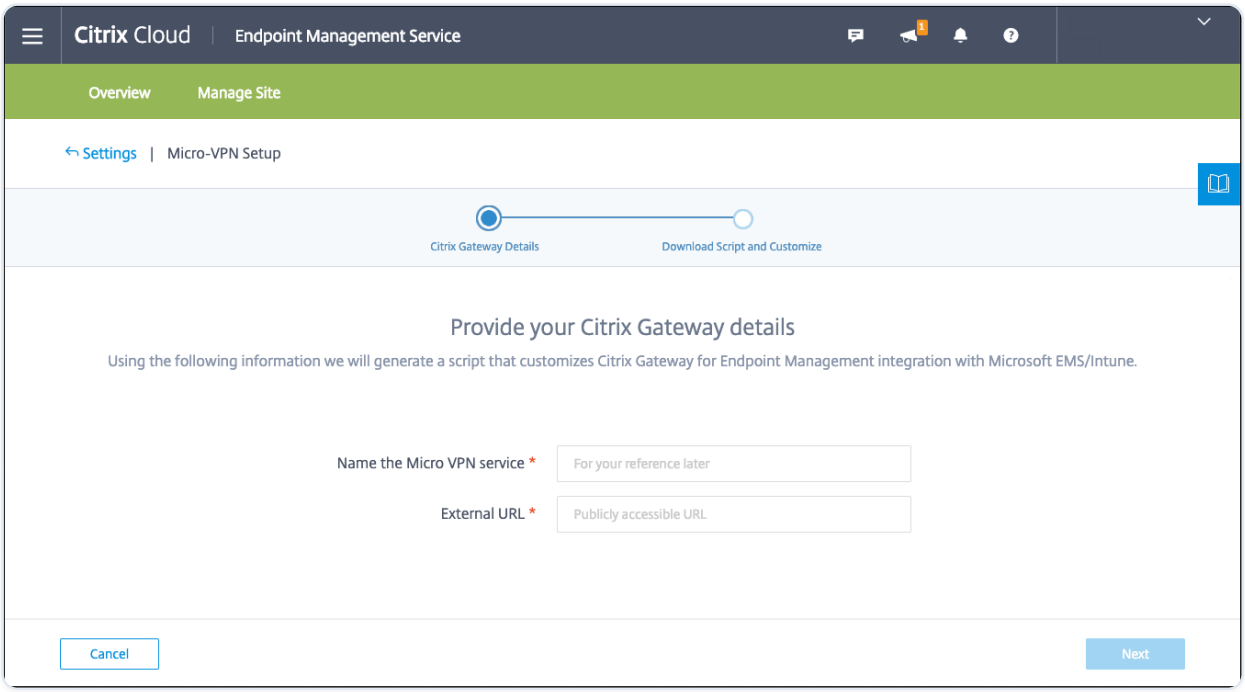


1. 在 Citrix Cloud 控制台中，在“**Citrix Endpoint Management**”下，点击“**管理**”。
2. 在“**微 VPN**”旁边，点击“**配置微 VPN**”。

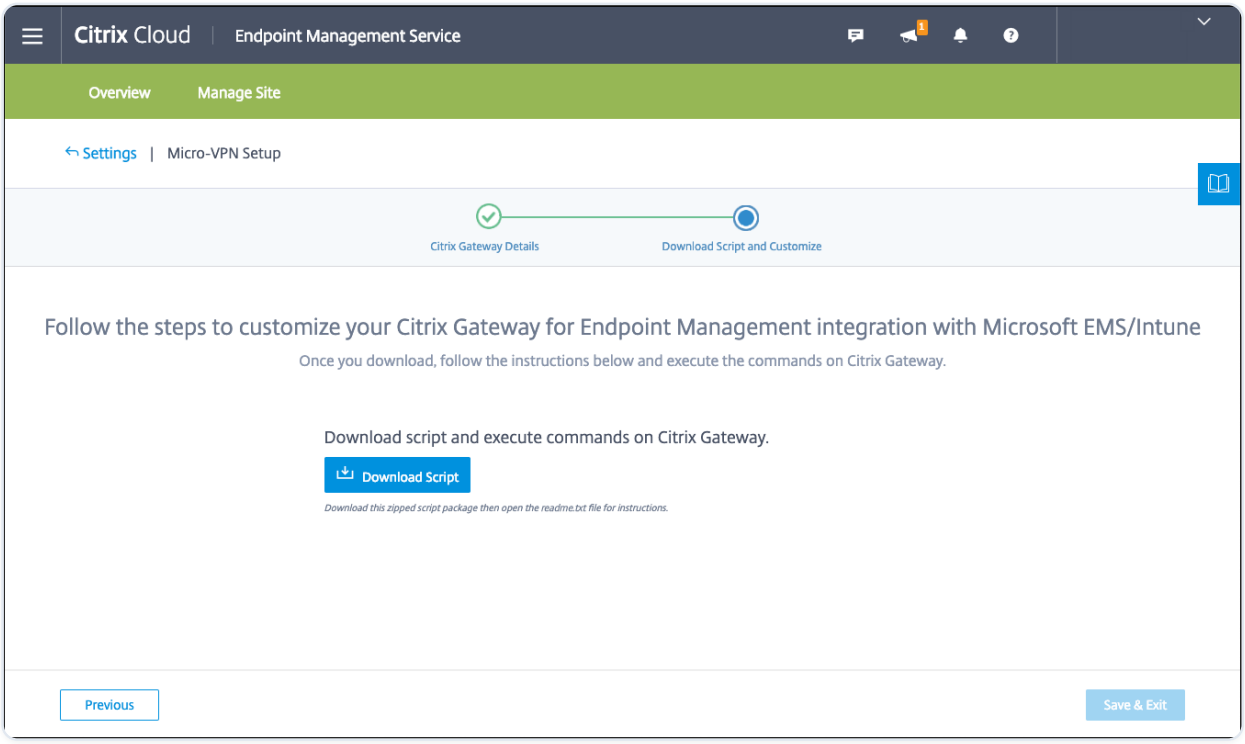


3. 输入微 VPN 服务的名称和 NetScaler Gateway 的外部 URL，然后单击“**下一步**”。

   此脚本将 NetScaler Gateway 配置为支持 Azure AD 和 Intune 应用程序。



4. 单击“**下载脚本**”。.zip 文件包含一个自述文件，其中包含实现脚本的说明。即使您可以从此处保存并退出，也只有在 NetScaler Gateway 安装上运行脚本后，微 VPN 才会设置完成。



注意：

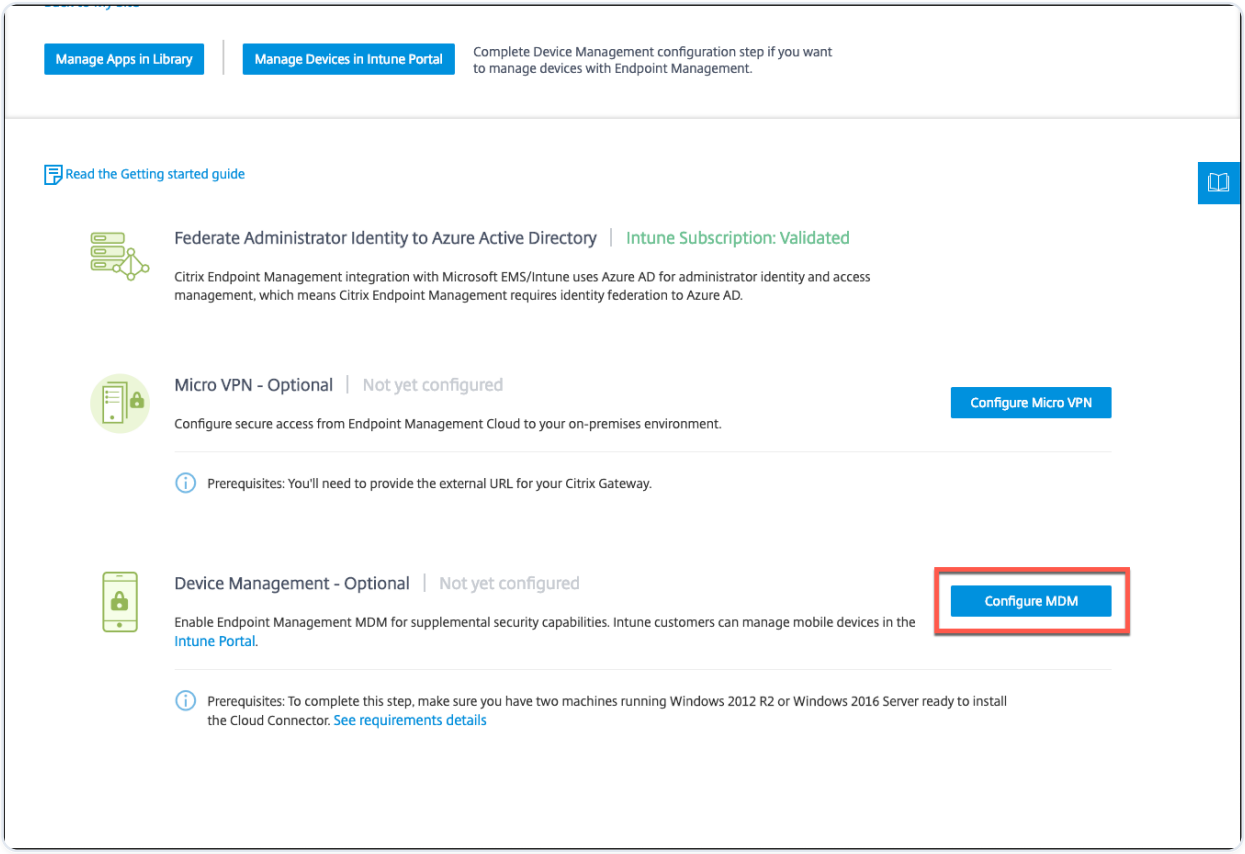
完成 NetScaler Gateway 配置过程后，如果 OAuth 状态不是 COMPLETE，请参阅“故障排除”部分。

配置设备管理

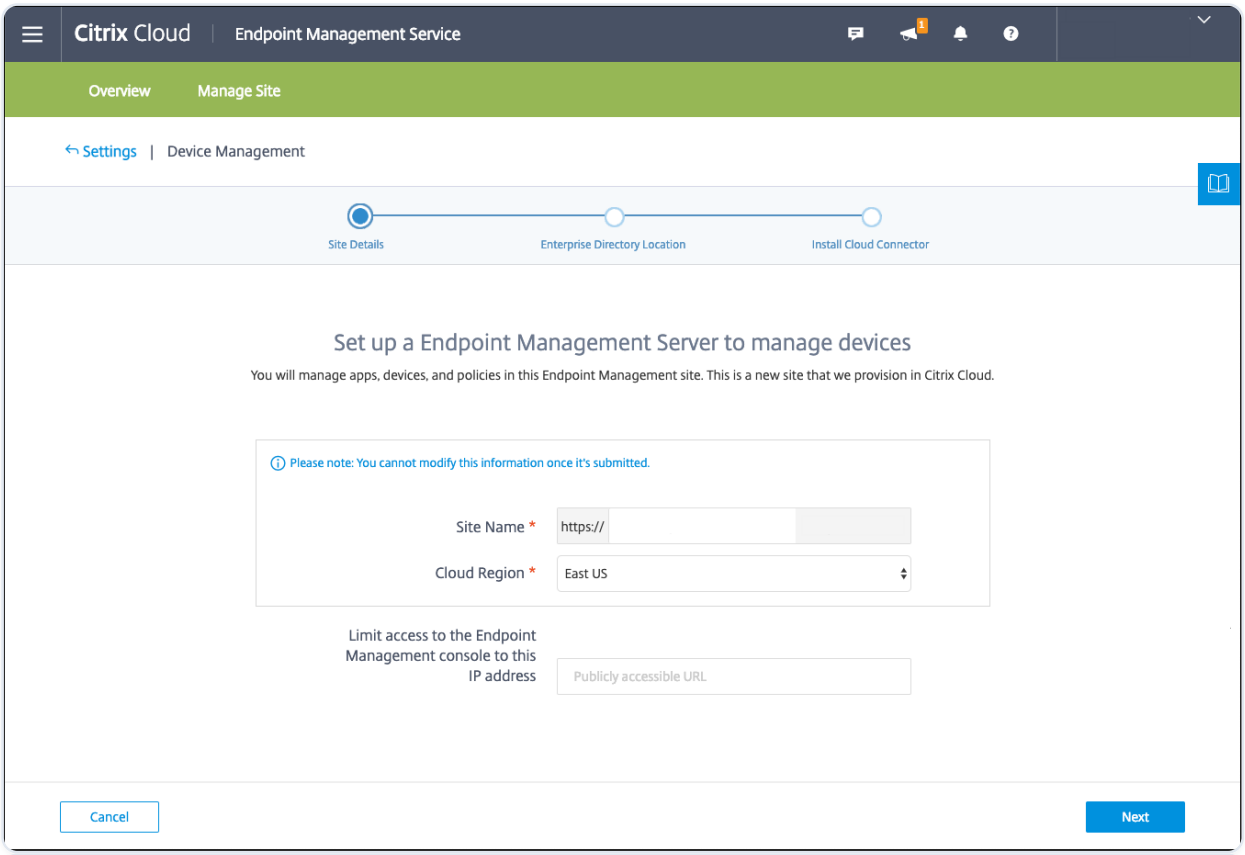
如果除了应用程序之外还需要管理设备，请选择一种设备管理方法。您可以使用 Citrix Endpoint Management MDM+MAM 或 Intune MDM。

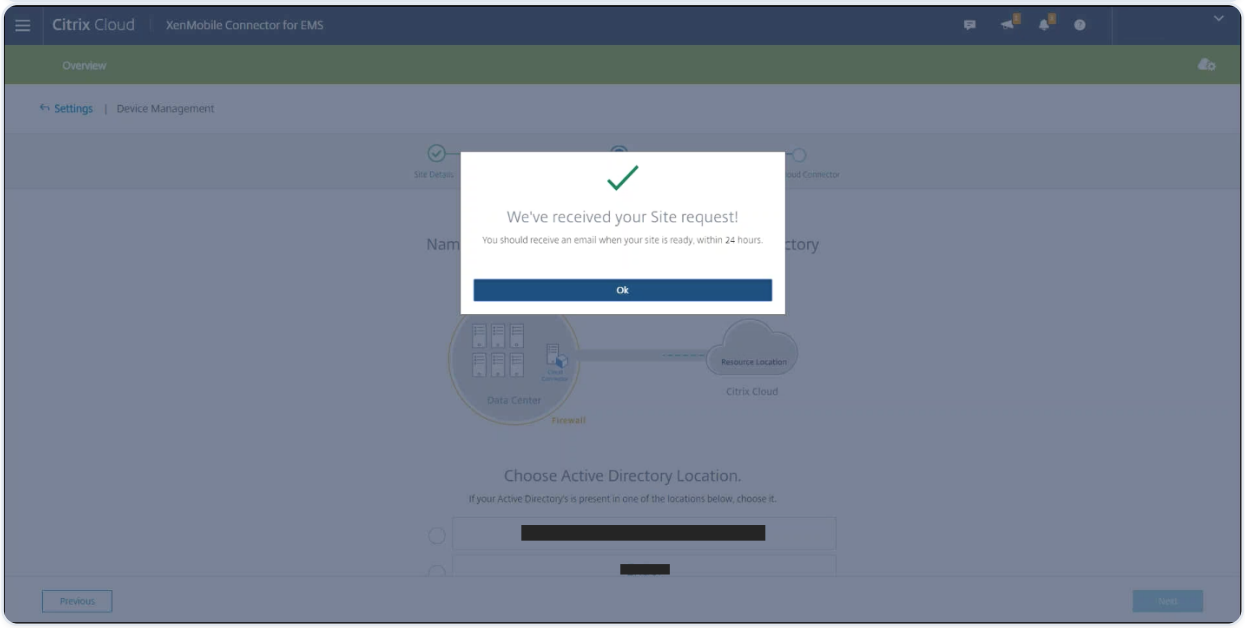
> **注意：**
>
> 控制台默认为 Intune MDM。要使用 Intune 作为 MDM 提供程序，请参阅 Microsoft Intune 文档。

1. 在 Citrix Cloud 控制台中，在“Citrix Endpoint Management 与 MEM 集成”下，单击“**管理**”。在“**设备管理 - 可选**”旁边，单击“**配置 MDM**”。

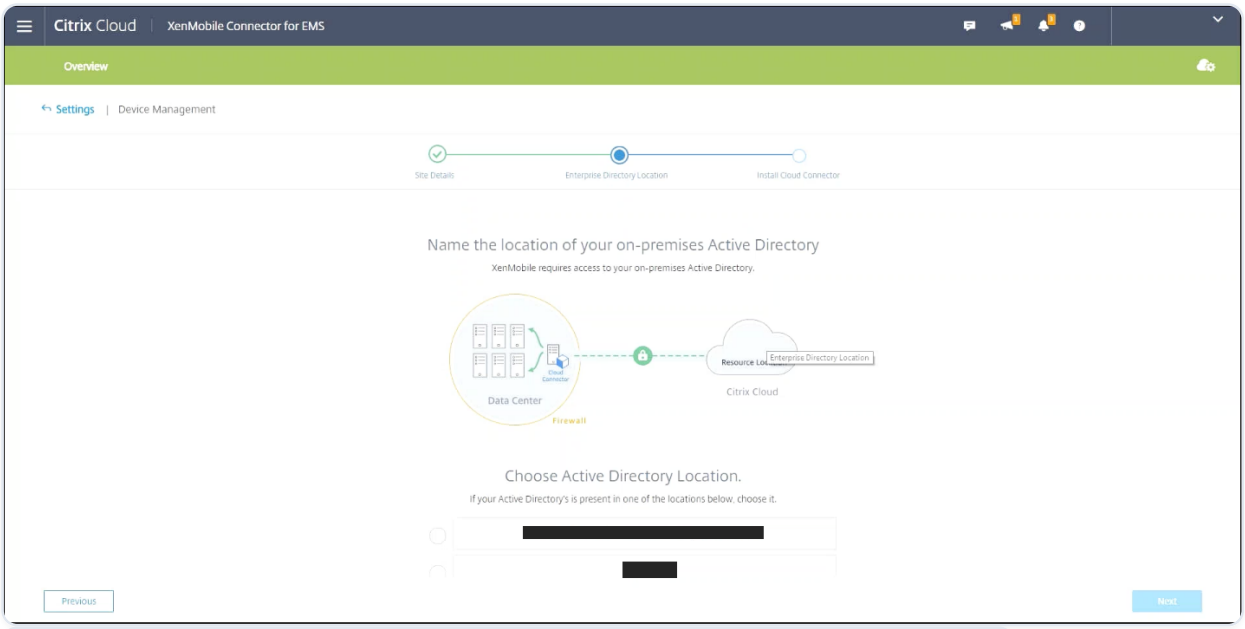


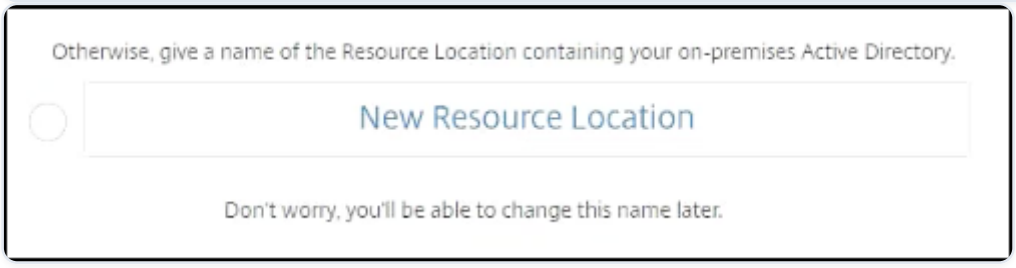
2. 输入唯一的站点名称，选择离您最近的云区域，然后单击“**请求站点**”。站点准备就绪后，您将收到一封电子邮件。



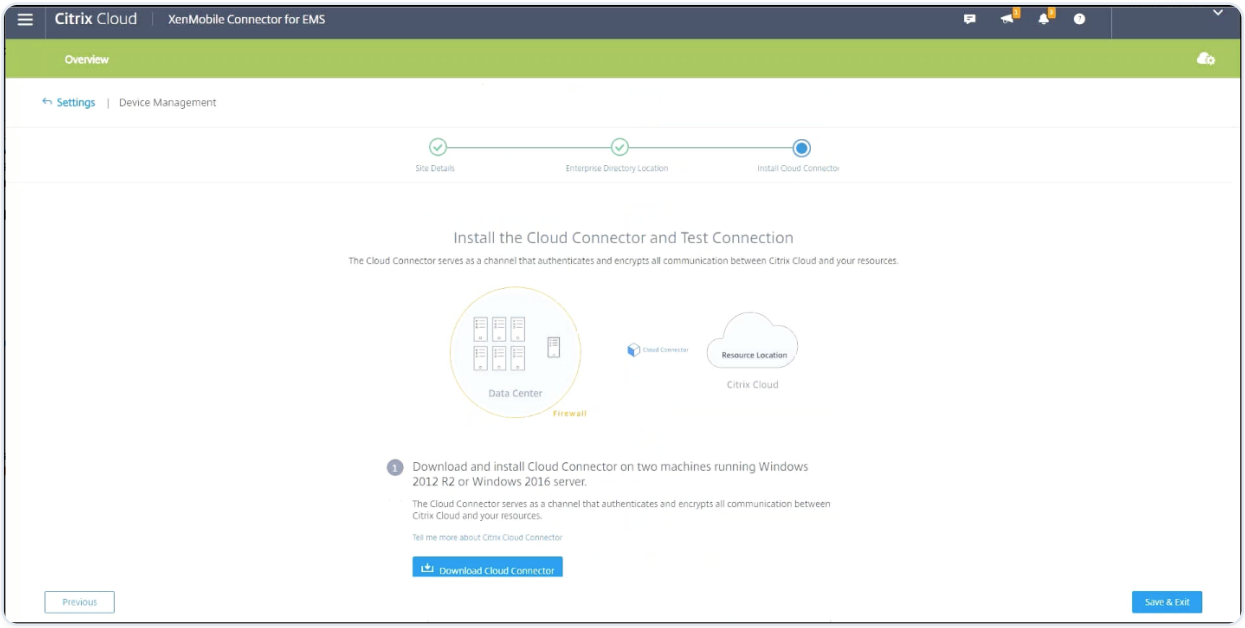


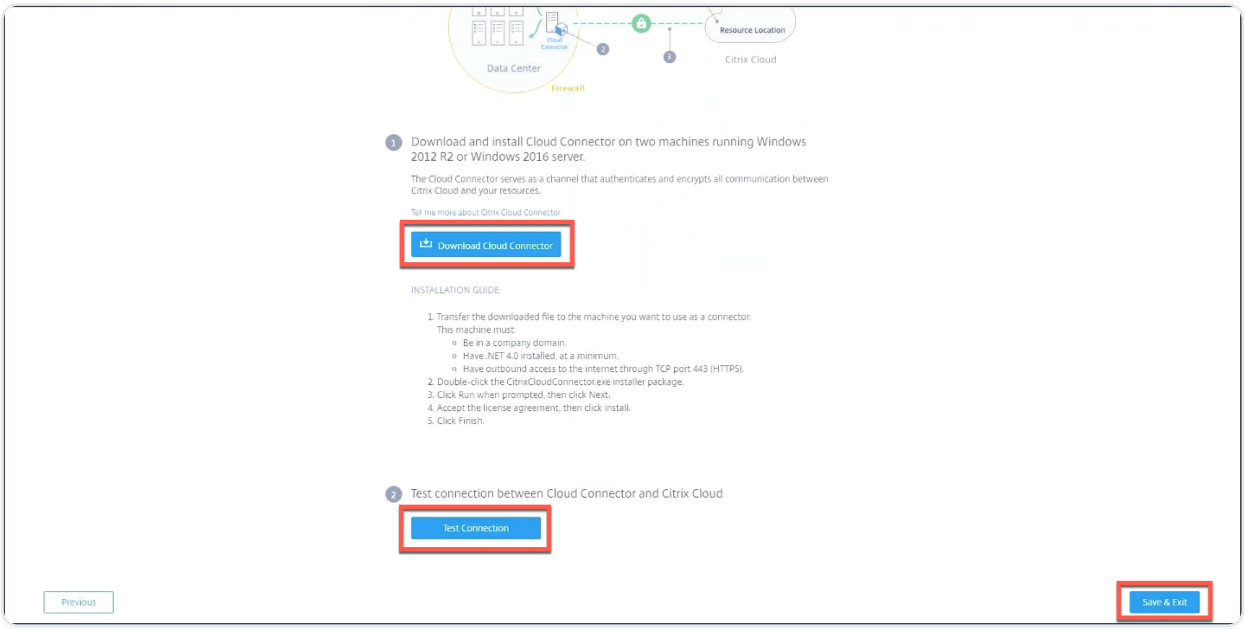
3. 单击“**确定**”关闭提示。选择要与您的站点关联的 Active Directory 位置或创建资源位置，然后单击“**下一步**”。



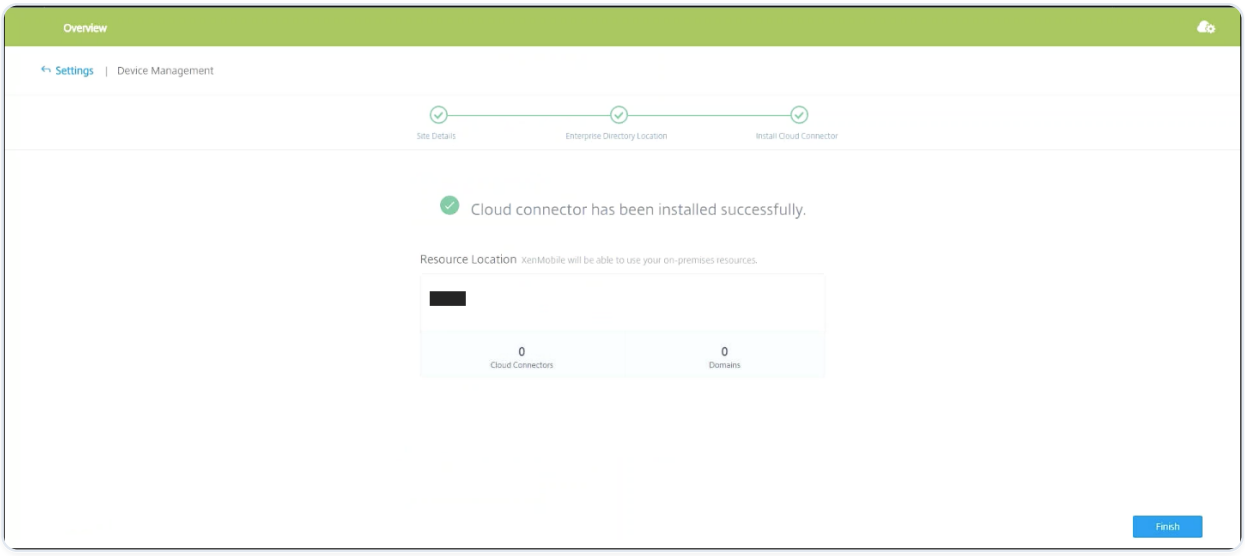


4. 单击**下载云连接器**，然后按照屏幕上的说明安装云连接器。安装后，单击**测试连接**以验证 Citrix Cloud 与云连接器之间的连接。

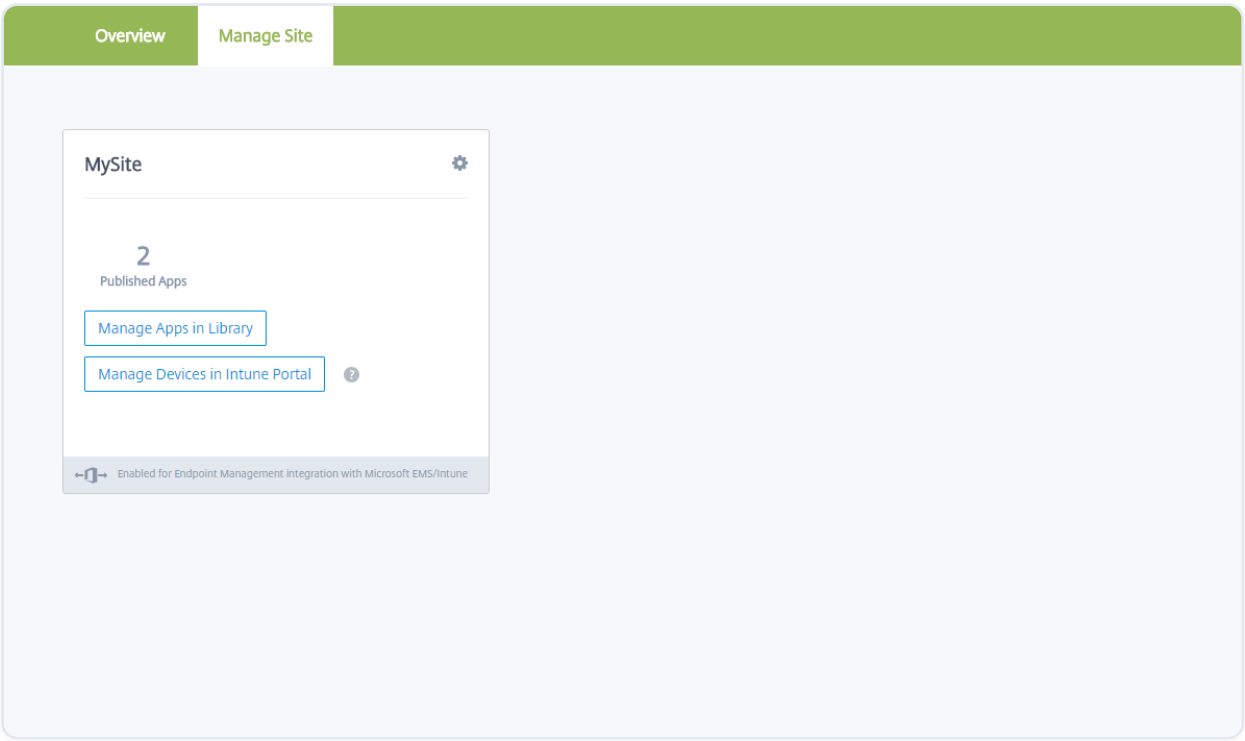




5. 单击**保存并退出**以完成。您的资源位置随即显示。单击**完成**将返回到设置屏幕。



6. 您现在可以从站点磁贴访问 Citrix Endpoint Management 控制台。在此处，您可以执行 MDM 管理任务并分配设备策略。有关设备策略的更多信息，请参阅设备策略。



配置 Intune 托管应用程序以交付到设备

> **注意：**
>
> 自 April 1, 2025 起，通过库管理 Microsoft Intune 应用程序将不再可用。如果您需要相关服务的帮助，请联系 Citrix 支持以启用此功能。

要配置 Intune 托管应用程序以进行交付：

- 将应用程序添加到 Citrix Cloud 库
- 创建 Citrix 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 应用添加到 Citrix Cloud 库

对于要添加的每个应用：

1. 在 Citrix Cloud 控制台中，单击菜单图标，然后单击“**库**”。

   Citrix Cloud 库页面(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-integration-with-ems20.png)

2. 单击右上角的加号图标，然后单击“**添加移动应用**”。

添加移动应用选项(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems36.png)

3. 如果您已在 Citrix Endpoint Management 控制台中配置 Android Enterprise，请在“**选择应用程序**”下选择“**Microsoft Intune 应用**”。选择一个应用模板进行自定义，或单击“**上传我的应用**”。

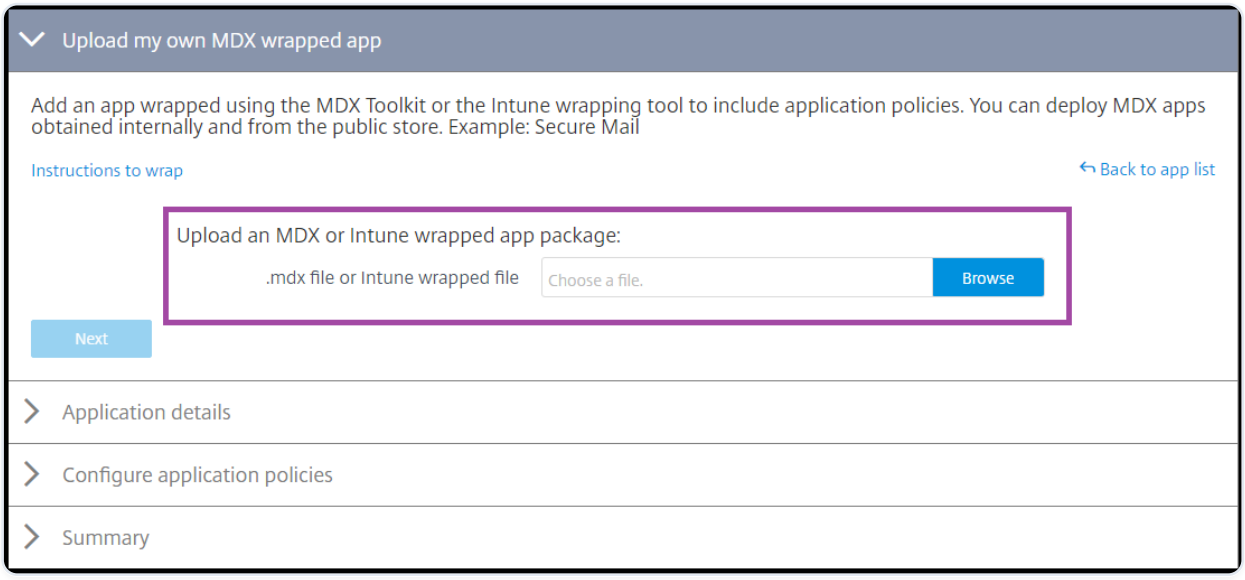
   要配置的策略(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-integration-with-ems25.png)

   Citrix 提供现有应用模板，每个模板都带有一组预配置的默认策略。对于客户上传的应用，适用以下策略：

   - **MDX 文件：** 包括启用了 MAM SDK 的应用或 MDX 封装的应用，例如：
     - Intune 应用保护策略和包中的默认 MDX 策略
     - 公共商店应用，例如与捆绑包 ID 或包 ID 匹配的 Intune 应用保护策略和默认 MDX 策略
   - **IPA 文件：** Intune 应用保护策略。
   - **APK 文件：** Intune 应用保护策略。

   > **注意：**
   >
   > 如果应用未通过 Intune 封装，则 Intune 应用保护策略不适用。

4. 单击 **上传我自己的应用** 并上传您的 .mdx 或 Intune 封装文件。



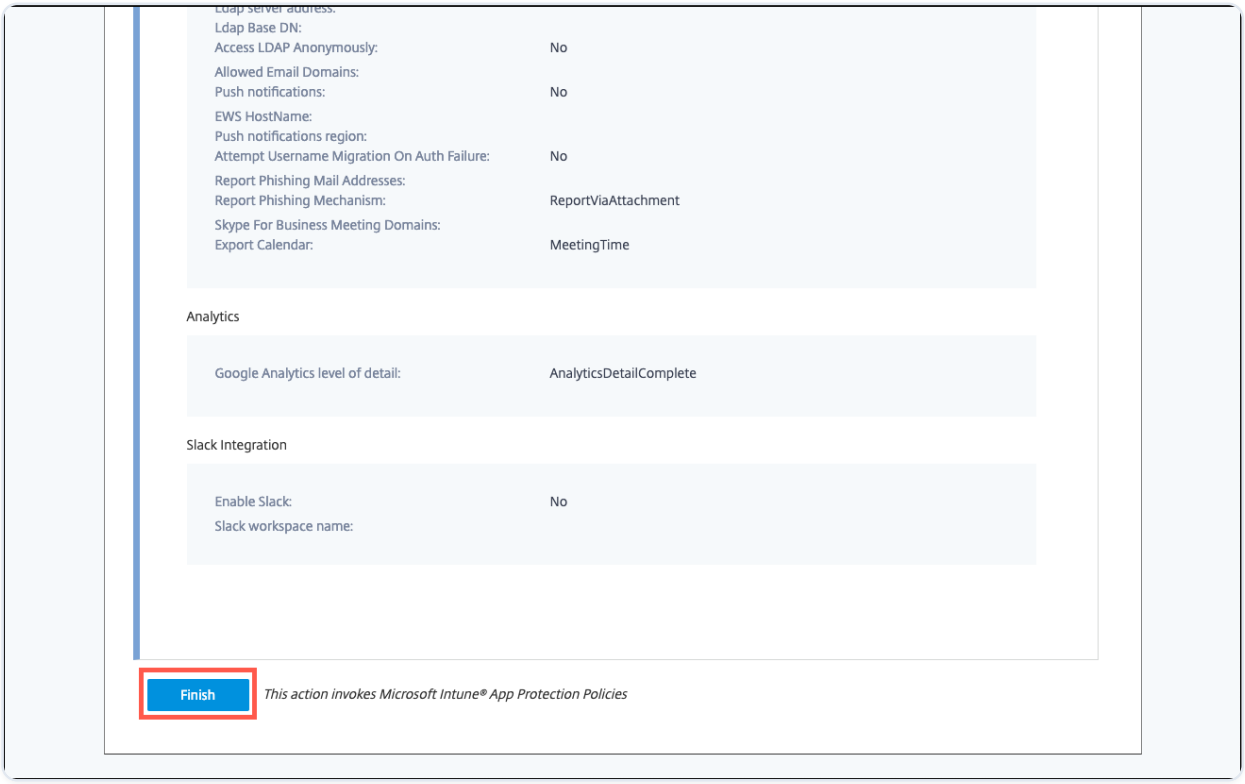
5. 输入应用的名称和描述，选择应用是可选还是必需，然后单击 **下一步**。

6. 配置应用程序设置。以下配置使 Citrix Endpoint Management 和 Intune 容器能够相互传输数据。

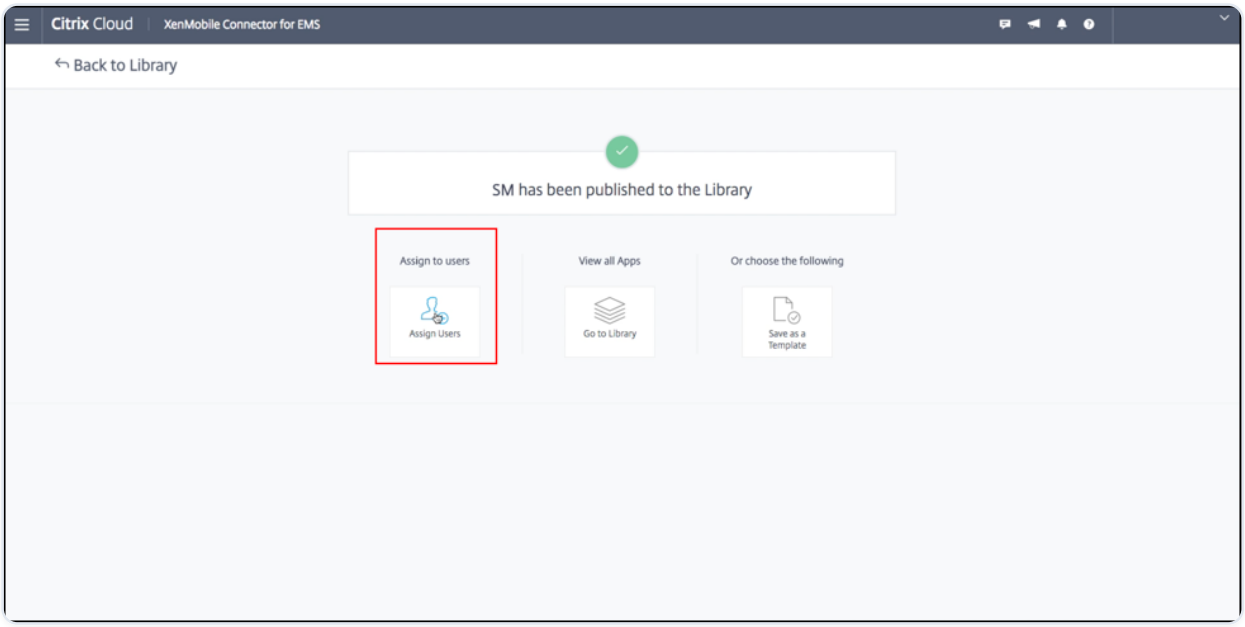
   - **允许应用从其他应用接收数据：** 选择 **策略托管应用**。
   - **允许应用将数据传输到其他应用：** 选择 **所有应用**。
   - **限制与其他应用的剪切、复制、粘贴：** 选择 **策略托管应用**。

7. 配置保存数据的存储库。对于 **选择可保存公司数据的存储服务**，选择 **LocalStorage**。
8. 可选：为应用设置数据重定位、访问和 PIN 策略。单击 **下一步**。
9. 查看应用的摘要，然后单击 **完成**。

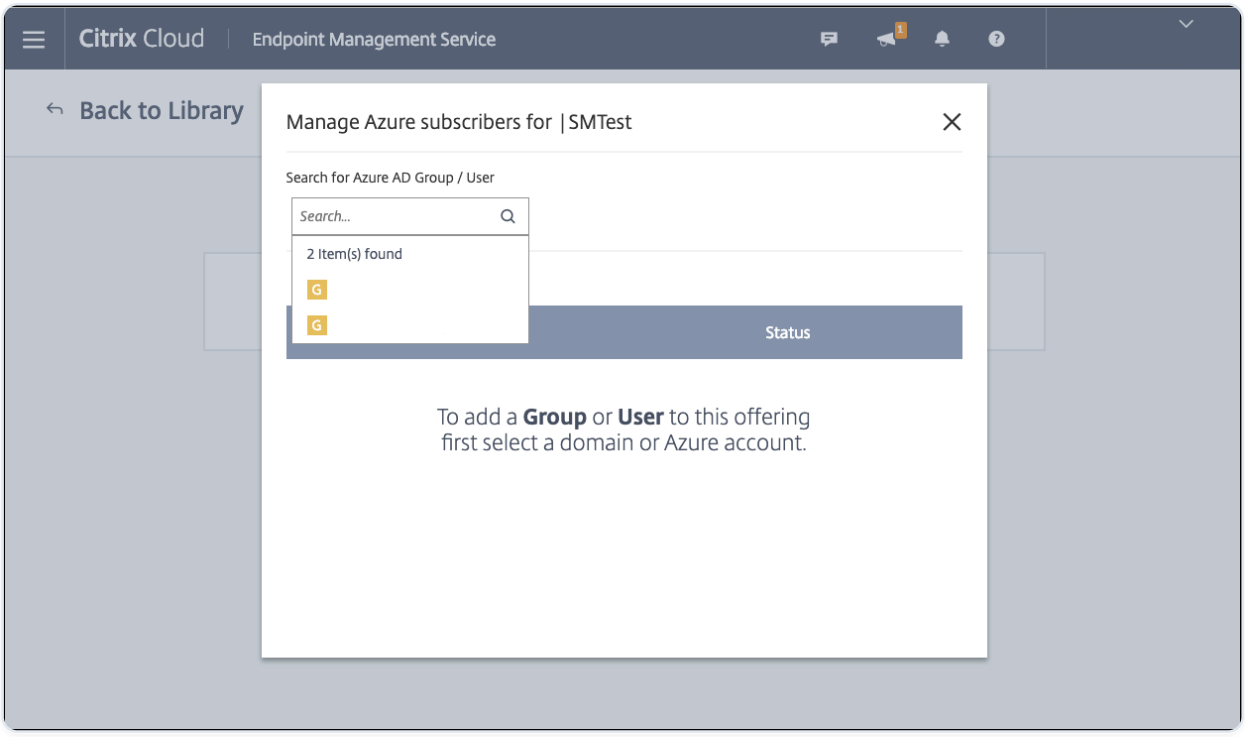
   应用配置过程可能需要几分钟。过程完成后，将显示一条消息，指示应用已发布到库中。



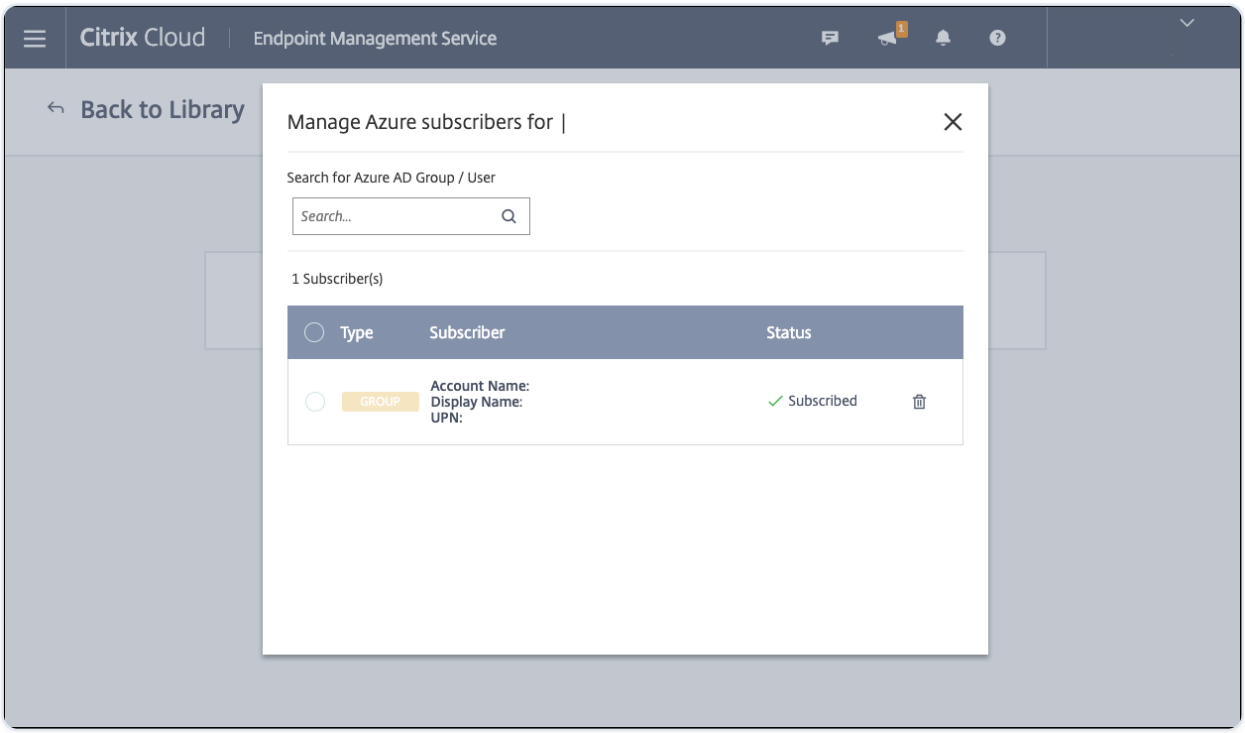
10. 要将用户组分配给应用，请单击 **分配用户**。



11. 在搜索框中，搜索用户组并单击以添加它们。您不能添加单个用户。



12. 添加完所有所需组后，单击 X 关闭窗口。



添加用户组时可能会出现错误。当用户组未同步到本地 Active Directory 时，会发生此错误。

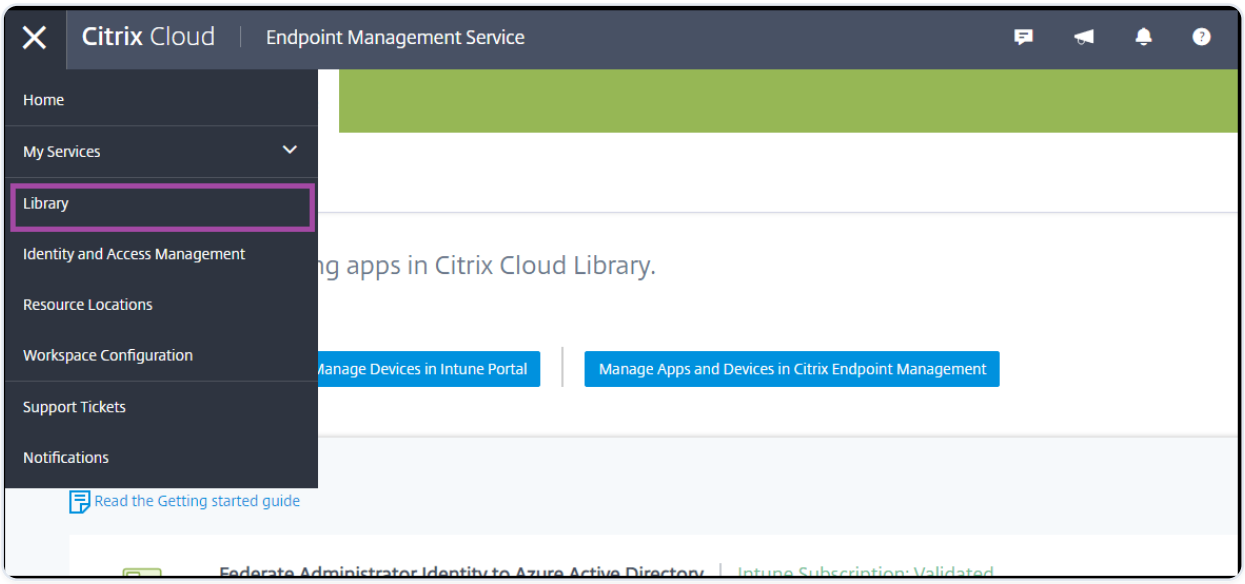
将 Android Enterprise 应用程序添加到 Citrix Cloud Library

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：

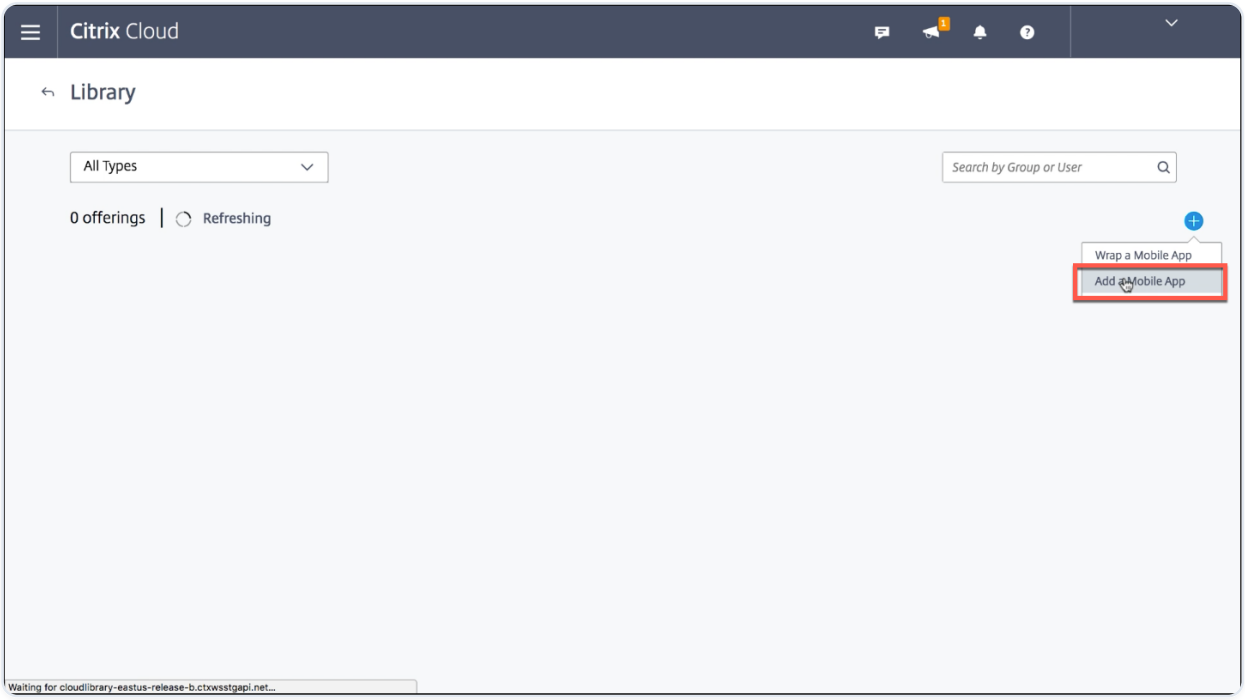
- 将 Citrix Cloud 与您的 Azure Active Directory (AAD) 帐户联合。请参阅将 Azure Active Directory 连接到 Citrix Cloud。
- 在 Citrix Endpoint Management 中配置 LDAP 和 云连接器。
- 在 Citrix Endpoint Management 中设置 Android Enterprise。确保 Android Enterprise 设备在 MDM+MAM 中注册。要设置 Android Enterprise，请参阅Android Enterprise。

按照此过程操作会将 Android Enterprise 应用程序同时添加到 Citrix 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**库**。



2. 单击右上角的加号图标，然后单击**添加移动应用程序**。



3. 在**选择应用程序**下，选择**Android Enterprise 应用程序**。

   选择应用程序(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app1.png)

4. 在“托管 Google Play 商店”窗口中搜索并批准应用程序。Google 窗口关闭后，单击“**下一步**”。

   Google Play 商店(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app2.png)

   已选择应用程序(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app3.png)

5. 添加应用程序详细信息，然后单击“**下一步**”。

   应用程序详细信息(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app4.png)

6. 如果您搜索并选择了 Citrix 移动生产力应用程序，则可以配置微 VPN 策略。配置这些策略后，单击“**下一步**”。

   微 VPN 策略(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app5.png)

7. 配置 Intune 应用程序保护策略。单击“**下一步**”。

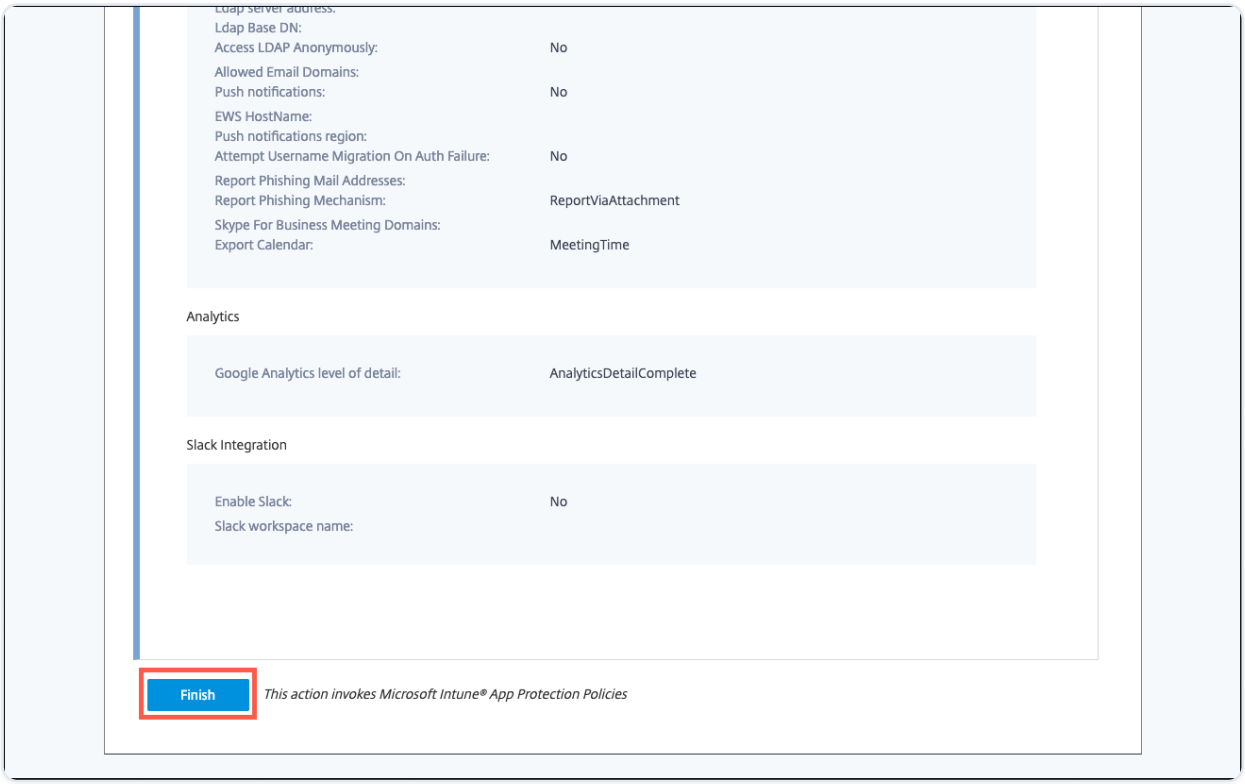
   Intune 策略(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app6.png)

8. 配置应用程序设置。以下配置允许 Citrix Endpoint Management 和 Intune 容器相互传输数据。

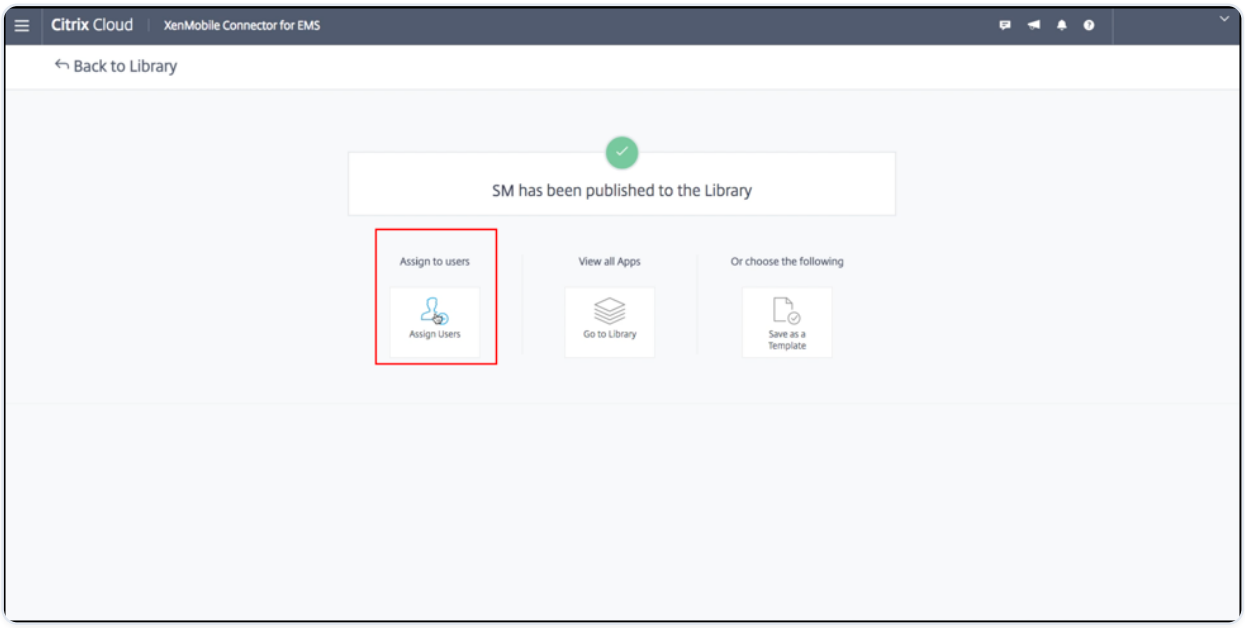
   - **允许应用程序从其他应用程序接收数据：**选择“**策略托管的应用程序**”。
   - **允许应用程序将数据传输到其他应用程序：**选择“**所有应用程序**”。
   - **限制与其他应用程序的剪切、复制、粘贴：**选择“**策略托管的应用程序**”。

9. 配置已保存数据的存储库。对于“**选择可将公司数据保存到哪些存储服务**”，选择“**LocalStorage**”。
10. 可选：为应用设置数据重定位、访问和 PIN 策略。单击**下一步**。
11. 查看应用的摘要，然后单击**完成**。

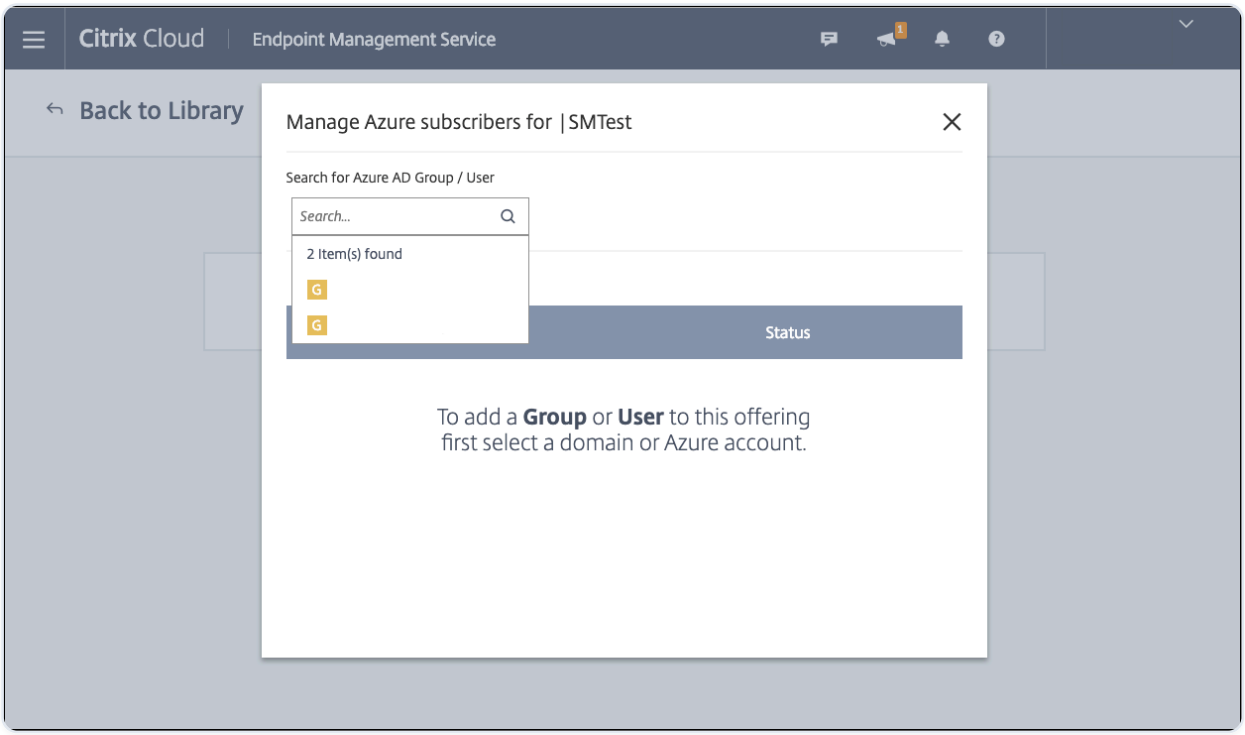
    应用配置过程可能需要几分钟。过程完成后，将显示一条消息，指示应用已发布到库中。该应用在 Citrix Endpoint Management 和 Intune 控制台中可用。在 Citrix Endpoint Management 控制台中，该应用是新交付组的一部分，并被标识为公共应用商店应用。



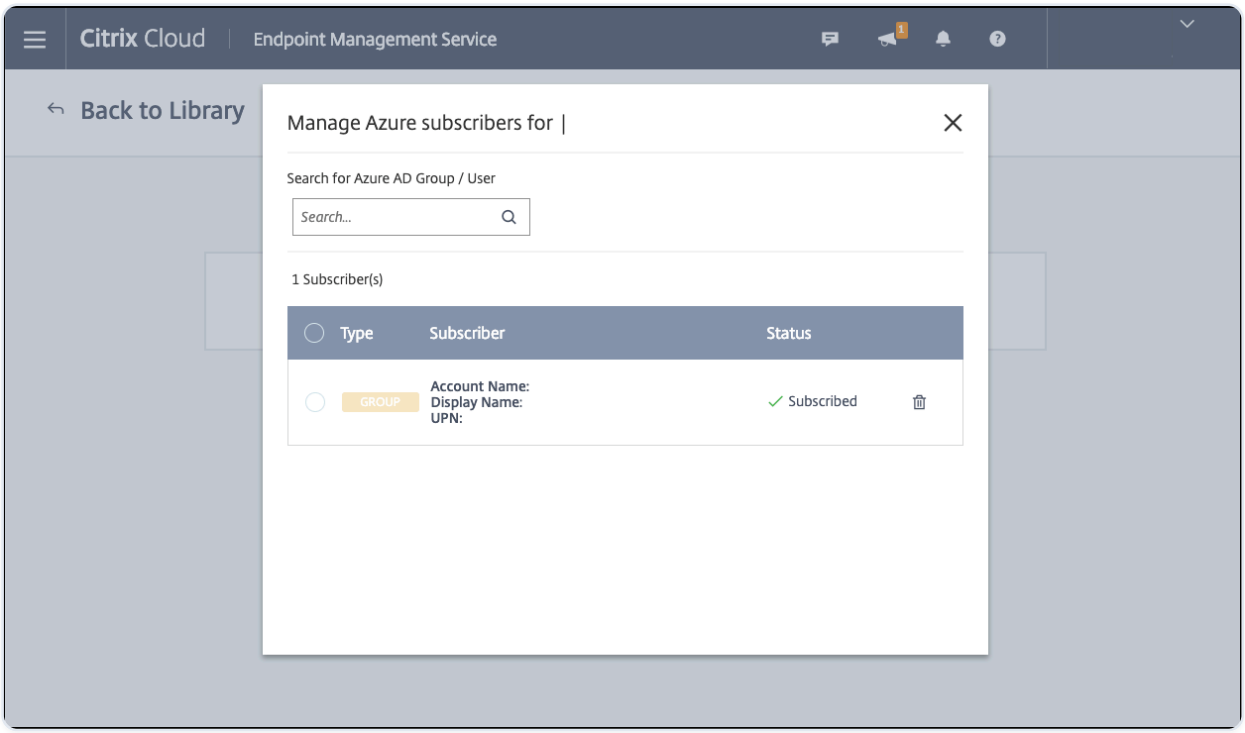
12. 要将用户组分配给应用，请单击**分配用户**。



13. 在搜索框中，搜索用户组并单击以添加它们。您无法添加单个用户。



14. 添加完所有所需组后，单击 X 关闭窗口。



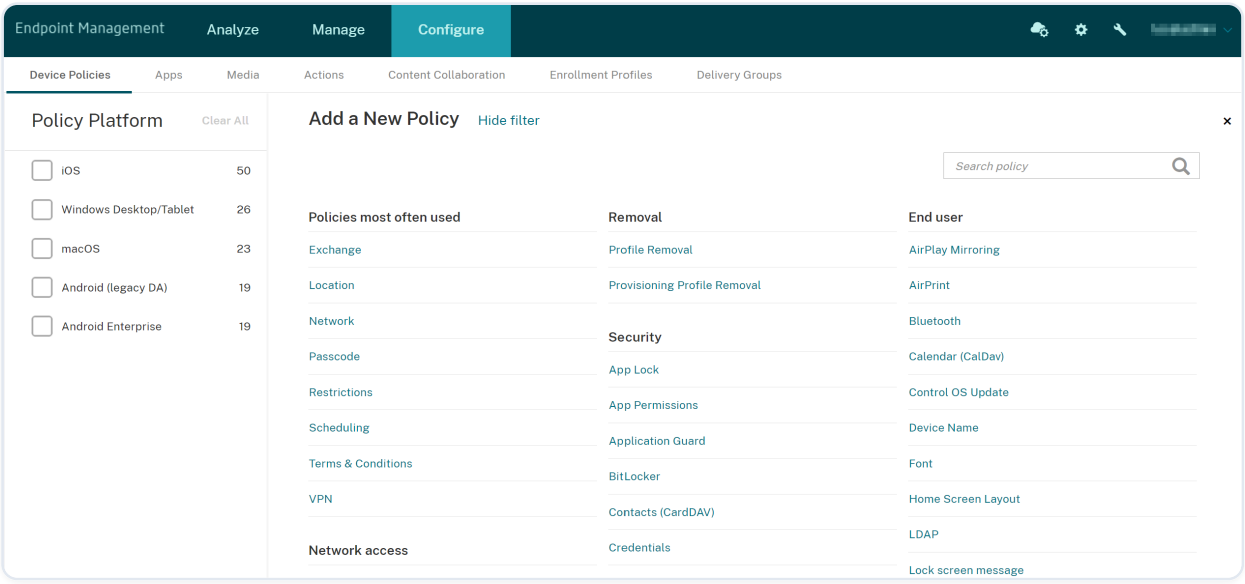
添加用户组时可能会看到错误。当用户组尚未同步到本地 Active Directory 时，会发生此错误。

控制托管应用之间传输的数据类型

使用 Citrix Endpoint Management 设备策略控制 Citrix Endpoint Management 或 Intune 容器内托管应用之间可以传输的数据类型。您可以配置限制策略以仅允许标记为“公司”的数据。配置应用配置策略以标记数据。

要配置限制设备策略：

1. 在 Citrix 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**”。出现“**添加新策略**”页面。



3. 从策略列表中单击“**限制**”。
4. 在“**策略信息**”页面上，键入策略的名称和（可选）描述。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 - 允许**”下，将“**非托管应用程序中的托管应用程序文档**”设置为“**关闭**”。将此设置设为“**关闭**”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“**关闭**”。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 Citrix Endpoint Management 控制台中，单击“**配置 > 设备策略**”。
2. 单击“**添加**”。出现“**添加新策略**”页面。
3. 从策略列表中单击“**应用程序配置**”。
4. 在“**策略信息**”页面上，键入策略的名称和（可选）描述。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，将以下文本添加到“**字典内容**”：

```
<dict>

    <key>IntuneMAMUPN</key>

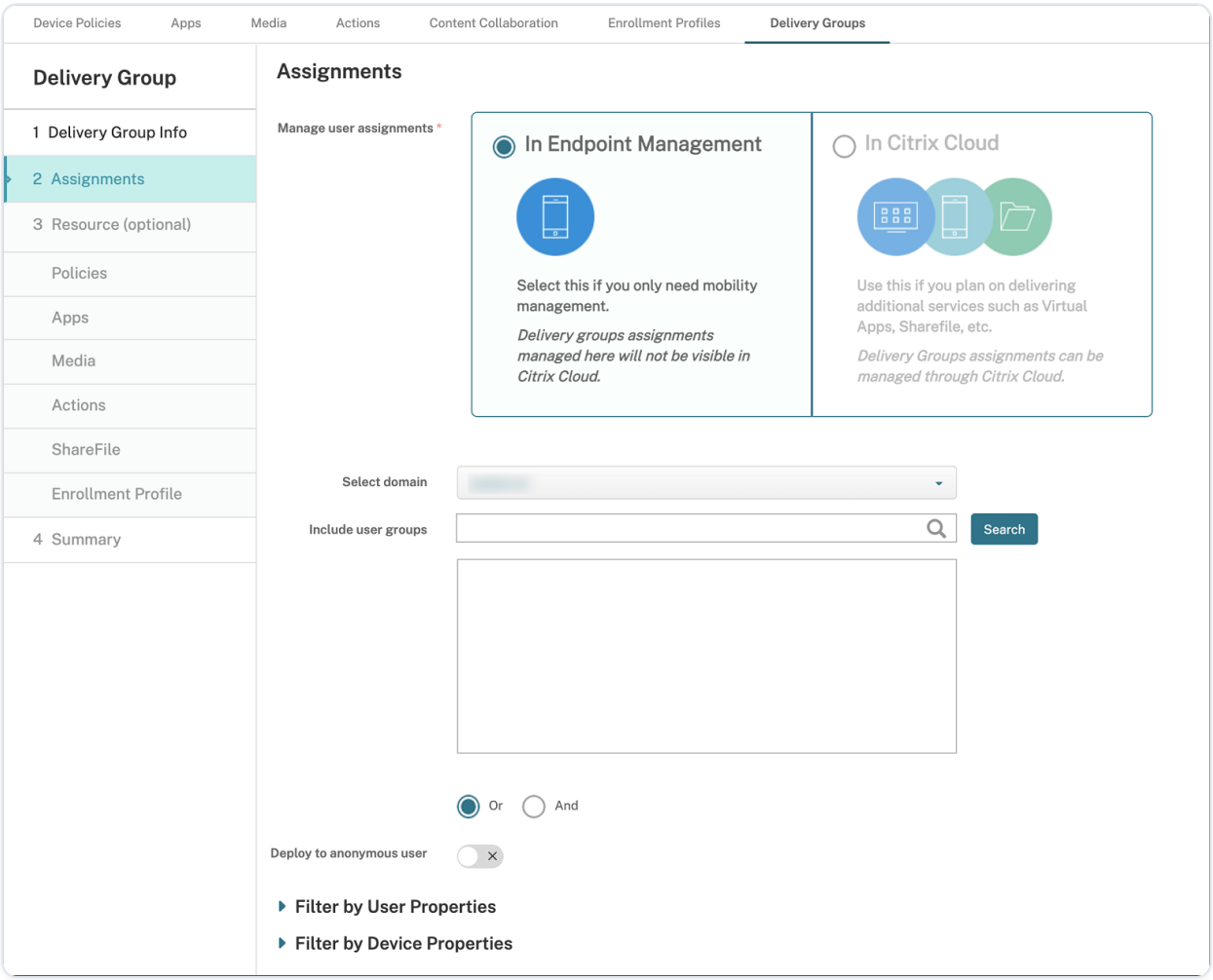
    <string>${user.userprincipalname}</string>

</dict>
```

8. 点击 **检查字典**。
9. 单击“**下一步**”。
10. 点击 **保存**。

配置应用程序和设备策略的交付组

1. 在 Citrix Endpoint Management 控制台中，点击 **配置 > 交付组**。
2. 在 **交付组** 页面上，点击 **添加**。**交付组信息** 页面随即出现。
3. 在 **交付组信息** 页面上，键入交付组的名称和（可选）描述。点击 **下一步**。
4. 在 **分配** 页面上，指定要如何部署交付组：选择 **在 Citrix Endpoint Management 中** 或 **在 Citrix Cloud 中**。



5. 如果您选择 **在 Citrix Endpoint Management 中**：

   - **选择域**： 从列表中，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，点击要添加的组。所选组将显示在 **选定用户组** 列表中。
     - 点击 **搜索** 以查看所选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，然后点击 **搜索** 以限制用户组列表。

     要从 **选定用户组** 列表中删除用户组，请执行以下操作之一：

     - 在 **选定用户组** 列表中，点击要删除的每个组旁边的 **X**。
     - 单击“**搜索**”以查看所选域中所有用户组的列表。滚动列表并清除要删除的每个组的复选框。
     - 在搜索框中键入完整或部分组名，然后单击“**搜索**”以限制用户组列表。滚动列表并清除要删除的每个组的复选框。

6. 单击“**下一步**”。

7. 在“**策略**”页面中，将您创建的“限制”策略和“应用程序配置”策略从左侧拖动到右侧。单击“**下一步**”。
8. 在“**应用程序**”页面中，将要交付的应用程序从页面左侧拖动到“**所需应用程序**”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**”。未受监督设备上的用户会收到提示，要求允许管理应用程序。如果用户接受提示，则该应用程序将在设备上进行管理。如果用户拒绝提示，则该应用程序在设备上不可用。

配置 思杰安全邮件

> **注意：**
>
> Citrix Secure Mail 与 Intune 的集成已弃用，并将在未来版本中删除。有关详细信息，请参阅 Secure Mail 中的新增功能。

> Citrix Secure Mail 现在支持各种配置。您可以将 Citrix Secure Mail 封装在连接到本地 Exchange Server 的 Intune MAM 容器中。您可以将 Citrix 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，因此请改用 LDAP。

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

> Citrix Secure Mail 还会自动填充用户名。要启用此功能，您必须首先配置以下自定义策略。

1. 在 Citrix Endpoint Management 控制台中，转到“**设置 > 服务器属性**”，然后单击“**添加**”。
2. 在列表中，单击“**自定义密钥**”，然后在“**密钥**”字段中，键入 `xms.store.idpuser_attrs`。
3. 将值设置为“**true**”，然后在“**显示名称**”中，键入 `xms.store.idpuser_attrs`。单击“**保存**”。
4. 点击 **客户端属性**，然后点击 **添加**。

5. 选择 **自定义密钥**，然后在 **密钥** 字段中键入 **SEND_LDAP_ATTRIBUTES**。
6. 在 **值** 字段中键入 `userPrincipalName=${user.userprincipalname},email=${user.mail},displayname=${user.displayname},sAMAccountName=${user.samaccountname},aadupn=${user.id_token.upn},aadtid=${user.id_token.tid}`。输入描述，然后点击 **保存**。

   以下步骤仅适用于 iOS 设备。

7. 转到 **配置 > 设备策略**，点击添加，然后选择 **应用程序配置** 策略。
8. 输入策略名称，然后点击 **下一步**。

   在“标识符”列表中，点击 **添加新项**。在出现的文本框中，输入您的 Citrix 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。

```
&lt;dict>


&lt;key>XenMobileUserAttributes&lt;/key>


&lt;dict>


&lt;key>userPrincipalName&lt;/key>


&lt;string>${user.userprincipalname}&lt;/string>


&lt;key>email&lt;/key>


&lt;string>${user.mail}&lt;/string>
```

```
&lt;key>displayname&lt;/key>

&lt;string>${user.displayname}&lt;/string>

&lt;key>sAMAccountName&lt;/key>

&lt;string>${user.samaccountname}&lt;/string>

&lt;key>aadupn&lt;/key>

&lt;string>${user.id_token.upn}&lt;/string>

&lt;key>aadtid&lt;/key>

&lt;string>${user.id_token.tid}&lt;/string>

&lt;/dict>

&lt;key>IntuneMAMUPN&lt;/key>

&lt;string>${user.id_token.upn}&lt;/string>
```

```
&lt;/dict>
```

10. 清除 **Windows 桌面/平板电脑** 复选框，然后点击 **下一步**。
11. 选择要部署策略的用户组，然后点击 **保存**。

故障排除

常见问题

问题： 打开应用程序时，出现以下错误消息：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： 每个应用程序只允许一个策略。

问题： 您的应用程序无法连接到内部资源。

解决方案： 确保防火墙端口已正确打开，您使用的是正确的租户 ID 等。

NetScaler Gateway 问题

下表列出了 NetScaler Gateway 配置的常见问题及其解决方案。为了进行故障排除，请启用更多日志并通过以下方式进行检查：

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

问题	解决方案
在 Azure 上为 Gateway App 配置所需的权限不可用。	检查是否有可用的正确 Intune 许可证。尝试使用 manage.windowsazure.com 门户查看是否可以添加权限。如果问题仍然存在，请联系 Microsoft 支持。
NetScaler Gateway 无法访问 `login.microsoftonline.com` 和 `graph.windows.net`。	从 NS Shell 中，检查您是否可以访问以下 Microsoft 网站：`curl -v -k https://login.microsoftonline.com`。然后，检查 NetScaler Gateway 上是否配置了 DNS 以及防

问题	解决方案
	火墙设置是否正确（以防 DNS 请求被防火墙阻止）。
配置 OAuthAction 后，ns.log 中出现错误。	检查是否启用了 Intune 许可，以及 Azure Gateway 应用程序是否设置了正确的权限。
Sh OAuthAction 命令未将 OAuth 状态显示为“已完成”。	检查 Azure Gateway App 上的 DNS 设置和已配置的权限。
Android 或 iOS 设备未显示双重身份验证提示。	检查双因素设备 ID logonSchema 是否绑定到身份验证虚拟服务器。

OAuth 错误条件和状态

状态	错误条件
完成	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	Graph 终结点已关闭或无法访问
CERTFETCH	无法与“令牌终结点: `https://login.microsoftonline.com`”通信，因为存在 DNS 错误。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。

- 当您使用 Citrix 和 Intune 部署应用程序以支持微型 VPN 时：当用户提供其用户名和密码以访问摘要站点时，即使其凭据有效，也会出现错误。
- 将 **Split tunnel** 从 **On** 更改为 **Off** 并等待当前网关会话过期后：外部流量将直接通过，而无需经过 NetScaler Gateway，直到用户在完整 VPN 模式下启动内部站点。

- 将“开放策略”从**仅托管应用**更改为**所有应用**后，用户无法在非托管应用中打开文档，直到他们关闭并重新启动 Citrix Secure Mail。
- 在全 VPN 模式下，当分流隧道为**开**，并且分流 DNS 从本地更改为远程时，内部站点无法加载。

已知问题

当 mVPN 策略**启用 http/https 重定向（带 SSO）**被禁用时，Citrix Secure Mail 无法运行。

第三方已知问题

在适用于 Android 的 Citrix Secure Mail 上，当用户点击**创建新事件**时，新事件创建页面不显示。

当您使用 Citrix 和 Intune 部署适用于 iOS 的 Citrix Secure Mail 以支持微 VPN 时：当用户将应用移至后台时，模糊 Citrix Secure Mail 屏幕的应用策略未强制执行。

入门和资源设置

如果您是 Citrix、Citrix Cloud 或 Citrix Endpoint Management 的新用户，本文将指导您完成入门。了解工作流程以及开始所需详细信息。

- **从何处开始？**
  - 如果您尚未购买 Citrix Endpoint Management 订阅，请参阅面向新 Citrix 客户。
  - 如果您已拥有 Citrix Endpoint Management 订阅，请跳至“管理”按钮可用时。
  - 如果您的 Citrix Endpoint Management 站点已预配，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操作。Citrix Endpoint Management 控制台会通过“预配后设置”等消息告知您是否缺少先决条件。
- **入门后我该做什么？** 完成本文所述的入门和资源配置后，请在 Citrix Endpoint Management 控制台中继续配置。有关后续步骤的信息，请参阅准备注册设备和交付资源。

面向新 Citrix® 客户

对于新接触 Citrix Endpoint Management 的 Citrix Cloud 客户：

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

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 Citrix Endpoint Management，请申请服务演示。

1. 使用您的 Citrix Cloud 管理员凭据登录您的 Citrix Cloud 帐户。Citrix Cloud 主页随即显示。

   所有 Citrix Cloud 管理员帐户均按如下方式创建：

   - Citrix Cloud 管理员默认是 Citrix Endpoint Management 管理员。
   - 具有客户访问权限创建的 Citrix Cloud 管理员必须选择 Citrix Endpoint Management 才能管理 Citrix Endpoint Management。
2. 在 Citrix Cloud 主页上，找到 Citrix Endpoint Management 服务磁贴，然后单击 **Request Demo**。

3. 填写并提交演示请求表单。Citrix Endpoint Management 服务磁贴上的按钮将变为 **Demo Requested**。

如果您在请求处理之前单击 Citrix Endpoint Management 服务磁贴，则会出现一个屏幕，建议您联系您的代表或合作伙伴。Citrix 销售代表可以提供有关该服务的更多信息和详细信息。

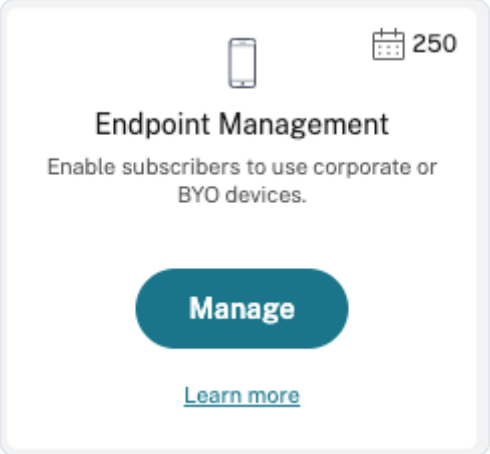
在等待试用期间，请务必通过查看系统要求来为您的 Citrix Endpoint Management 部署做好准备。尽管 Citrix 托管并交付您的 Citrix Endpoint Management 解决方案，但您必须处理一些通信和端口要求。

继续下一节。

当“管理”按钮可用时

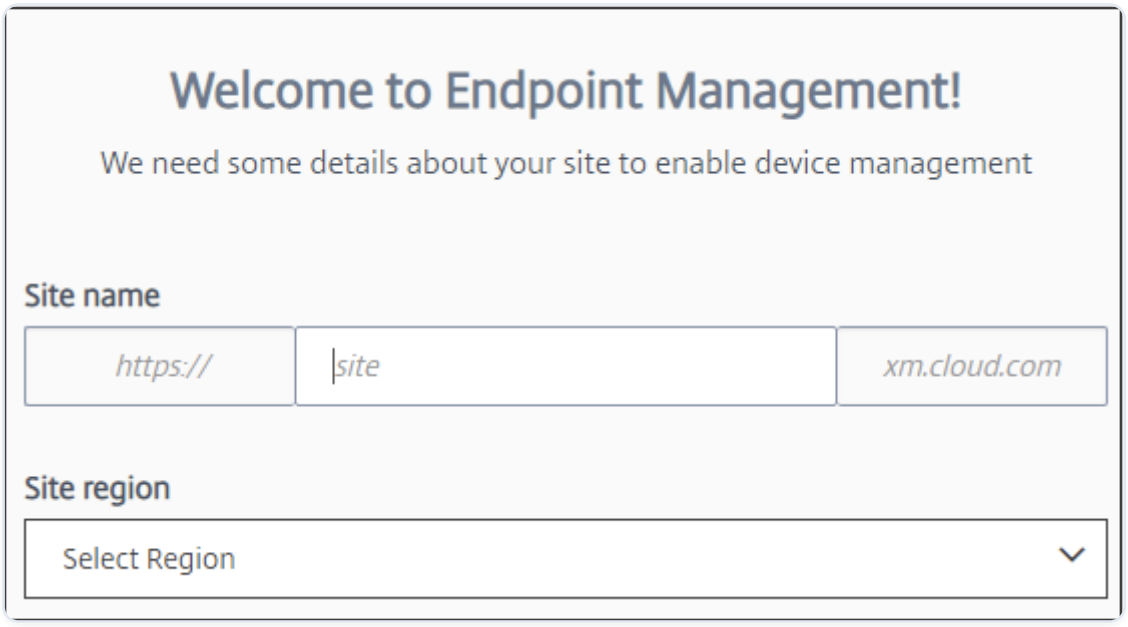
此视频将指导您完成入门：

<iframe src="https://www.youtube.com/embed/ycFLYxn7all" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
当您的 Citrix Endpoint Management 服务可用时，Citrix Endpoint Management 服务磁贴上的按钮将变为 **Manage**。



要开始设置：

1. 使用您的 Citrix Cloud 管理员凭据登录到您的 Citrix Cloud 帐户。
2. 单击 Citrix Endpoint Management 磁贴中的 **Manage** 以访问 Citrix 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**。

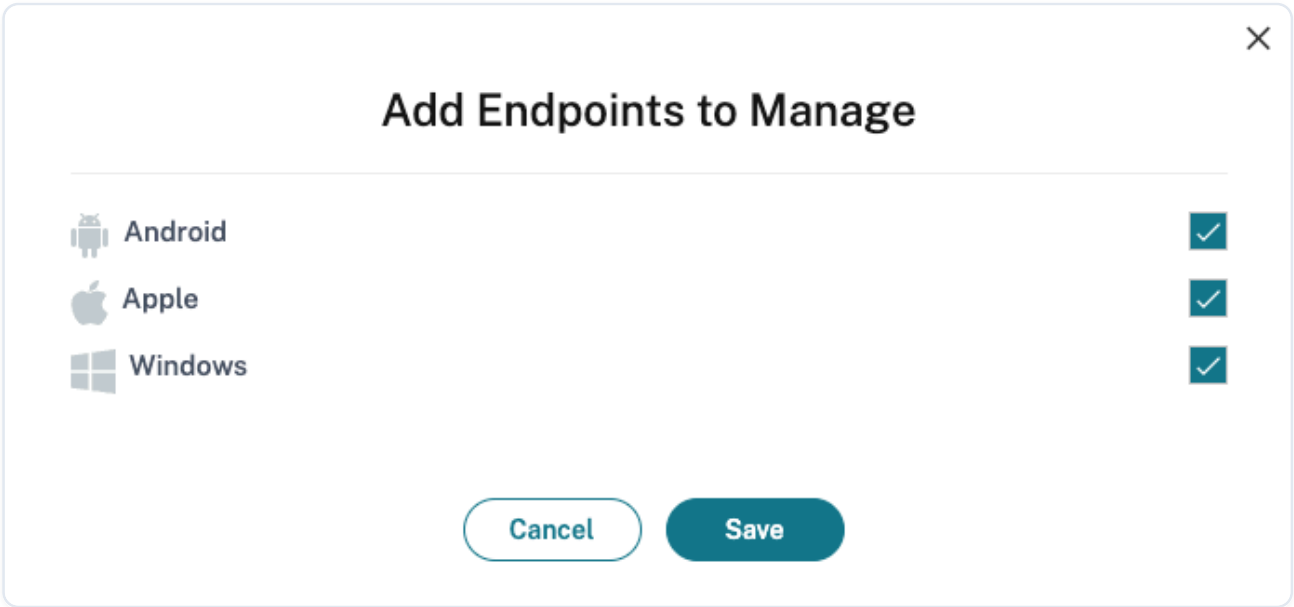


注意：

要请求允许的 IP 地址，请联系 Citrix 支持代表。

Citrix Endpoint Management 控制台随后打开，并显示一条消息，指出我们正在预配您的套件，并且在预配期间，某些 Citrix Endpoint Management 功能已被锁定。

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**”。您可以随时添加或清除端点，以在控制台中显示或隐藏它们。显示和隐藏端点不会影响您的配置。



预配完成后，我们会向您发送一封电子邮件。

资源中心



单击“**资源中心**”图标，无需离开控制台即可观看操作方法视频。

预配期间

在我们预配 Citrix Endpoint Management 的同时，您可以开始进行配置。

配置资源位置

在为 Citrix Endpoint Management 配置轻型目录访问协议 (LDAP) 连接之前，您需要资源位置。资源位置拥有向订阅者交付云服务所需的资源。每个域需要一个资源位置。有关帮助，请参阅 Citrix Cloud 文章 资源位置。

在等待试用期间，请务必通过查看 系统要求 来为您的 Citrix Endpoint Management 部署做好准备。尽管 Citrix 托管并交付您的 Citrix Endpoint Management 解决方案，但仍需要一些通信和端口要求。该设置将 Citrix Endpoint Management 基础结构连接到企业服务，例如 Active Directory。您必须提供的信息包含在 入门手册 的“Citrix Endpoint Management 试用销售工程师参与”部分中。

在您获得试用访问权限后，**Citrix Endpoint Management** 按钮将变为“**管理**”。单击“**管理**”以打开 Citrix Endpoint Management 控制台。

配置身份验证

站点预配完成后，您可以继续进行配置。我们建议您设置云托管身份提供程序 (IdP) 或轻量级目录访问协议 (LDAP) 以导入组、用户帐户和相关属性。

配置 IdP

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

要在 Citrix Cloud 中配置 IdP 并将其设置为 Citrix Endpoint Management：

- 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 NetScaler Gateway 进行身份验证

配置 LDAP

您可以在 Citrix Endpoint Management 中配置与一个或多个符合 LDAP 的目录的连接，以进行基于域的身份验证。Citrix Endpoint Management 支持 LDAP 中嵌套的组。嵌套组每天在当地时间凌晨 12 点同步。

作为配置 LDAP 的一部分，您必须安装至少一个 Cloud Connector。

如需快速概览，请观看此视频。

<iframe src="https://www.youtube.com/embed/LJ6IDZyfO8s" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
要设置 LDAP：

1. 在“**设置**”页面上，滚动到“**LDAP**”磁贴，然后单击“**设置**”。
2. 按照屏幕上的指导下载并安装 Cloud Connector。Cloud Connector 是实现 Citrix Cloud 与您的资源之间通信所必需的。如需帮助，请参阅 Citrix Cloud Connector。

如果您有 LDAP 配置，并且将 Azure AD 或 Okta 添加为身份提供程序，Citrix Endpoint Management 会将您的 Active Directory 组的 IdP 特定信息同步到 Citrix Endpoint Management 数据库中。此配置不会影响您现有的交付组和用户注册。但是，之后您无法在 Citrix 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。

如果在注册后更改了**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 NetScaler Gateway

与 Citrix Endpoint Management 集成后，NetScaler Gateway 可为您的内部网络和资源提供远程设备访问权限。

Citrix Endpoint Management 在以下情况下需要 NetScaler Gateway：

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

如需快速概览，请观看此视频。

<iframe src="https://www.youtube.com/embed/r79jdnVznE0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
下表总结了本地 NetScaler Gateway 解决方案支持的功能。

支持的功能	本地 NETSCALER GATEWAY
思杰安全邮件 (STA)*	是
隧道式 - Web SSO（Web 单点登录）	是
完整 VPN（不适用于 iOS 版 Citrix 移动生产力应用程序）	是
每应用 VPN	是
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
拆分隧道	是
拆分 DNS	是

* Citrix Cloud 安全票证颁发机构 (STA) 服务配置

** 本地配置

*** 全局服务器负载平衡配置

本地 NetScaler Gateway 用例

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

- 您需要按应用程序 VPN 功能。
- 您需要完全隧道、拆分隧道、反向拆分隧道或拆分 DNS。对于使用客户端证书或端到端 SSL 连接到内部网络中资源的连接，我们建议使用完整 VPN 隧道。

- 您使用 Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成功能。

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

1. 在“**设置**”页面上，滚动到“**NetScaler Gateway**”磁贴，然后单击“**开始设置**”。
2. 选择“**NetScaler Gateway（本地）**”作为类型。
3. 按照屏幕上的指导进行操作。有关信息，请参阅配置本地 NetScaler Gateway 以与 Citrix Endpoint Management 结合使用。

配置通知服务器

要发送通知，您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的连接和通信可能性。要在 Citrix 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

Citrix Endpoint Management 需要 Apple 推送通知服务 (APNs) 证书才能注册和管理 Apple 设备。如果您计划将推送通知用于适用于 Apple 的 Citrix Secure Mail，Citrix Endpoint Management 也需要 APNs 证书。有关 Citrix Endpoint Management 和 APNs 的信息，请参阅适用于 iOS 的 Citrix Secure Mail 推送通知。

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 网站。

如需快速概览，请观看此视频。

<iframe src="https://www.youtube.com/embed/pVj37DNBxMM" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
要使用 Citrix 证书签名请求配置 APNs：

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 安卓企业版

在您创建交付组并通过云库将用户分配给交付组后，Citrix Endpoint Management 将完全配置。从此时起，Citrix Endpoint Management 管理将在 Citrix Cloud 中进行。组合界面简化了 Citrix Cloud 和 Citrix Endpoint Management 之间的切换。

您可以使用谷歌应用商店或谷歌工作区为思杰端点管理设置安卓企业版。

1. **如果您的组织不使用 Google Workspace：** 您可以使用托管 Google Play 将 Citrix 注册为您的 EMM 提供商。如果您使用托管 Google Play，则可以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 的访问权限，允许用户安装和使用您提供的企业应用。如果您的组织使用第三方身份服务，您可以将托管 Google Play 帐户与您现有的身份帐户关联。

   由于此类企业不与域绑定，因此您可以为一个组织创建多个企业。例如，组织内的每个部门或区域都可以注册为不同的企业。此设置使您能够使用不同的企业来管理不同的设备和应用程序集。

2. **如果您的组织已使用 Google Workspace 为用户提供 Google 应用访问权限：** 您可以使用 Google Workspace 将 Citrix 注册为您的 EMM。如果您的组织使用 Google Workspace，则它具有现有的企业 ID 和现有用户的 Google 帐户。要将 Citrix Endpoint Management 与 Google Workspace 结合使用，您需要与 LDAP 目录同步，并使用 Google Directory API 从 Google 检索 Google 帐户信息。

   此类企业与现有域绑定。因此，每个域只能创建一个企业。要在 Citrix 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。该帐户通过您的 Google Workspace 计划为用户提供对托管 Google Play 和其他 Google 服务的访问权限。

如需快速概览，请观看此视频。

<iframe src="https://www.youtube.com/embed/O_SpR-Eds9k" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
要开始使用：

1. 在**设置**页面上，展开**Android**磁贴。
2. 在**Android Enterprise**磁贴上，单击**设置**。
3. 根据您向用户提供 Google 应用程序访问权限的方式，选择 **Google Play** 或 **G Suite**。 如果您之前使用 Google Play 配置了 Android Enterprise 平台，则 UI 会将您带到 Google Play 商店重新注册。单击**重新注册**，返回 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 云消息传递

Citrix 建议您使用 Firebase Cloud Messaging (FCM) 来控制 Android 设备连接到 Citrix Endpoint Management 的方式和时间。Citrix Endpoint Management 会向已启用 FCM 的 Android 设备发送连接通知。任何安全操作或部署命令都会触发推送通知，提示用户重新连接到 Citrix Endpoint Management 服务器。请参阅 Firebase Cloud Messaging。

与微软端点管理器集成

Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成将 Citrix Endpoint Management 微型 VPN 的价值添加到 Microsoft Intune 感知应用程序（例如 Microsoft Edge 浏览器）中。

Citrix Endpoint Management 与 MEM 的集成还允许企业使用 Intune 和 Citrix 封装自己的业务线应用程序。应用程序封装在 Intune 移动应用程序管理 (MAM) 容器中提供微型 VPN 功能。Citrix Endpoint Management 微型 VPN 使您的应用程序能够访问本地资源。您可以在一个容器中管理和交付 Office 365 应用程序、业务线应用程序和 Citrix Secure Mail。单个容器提供极致的安全性和生产力。

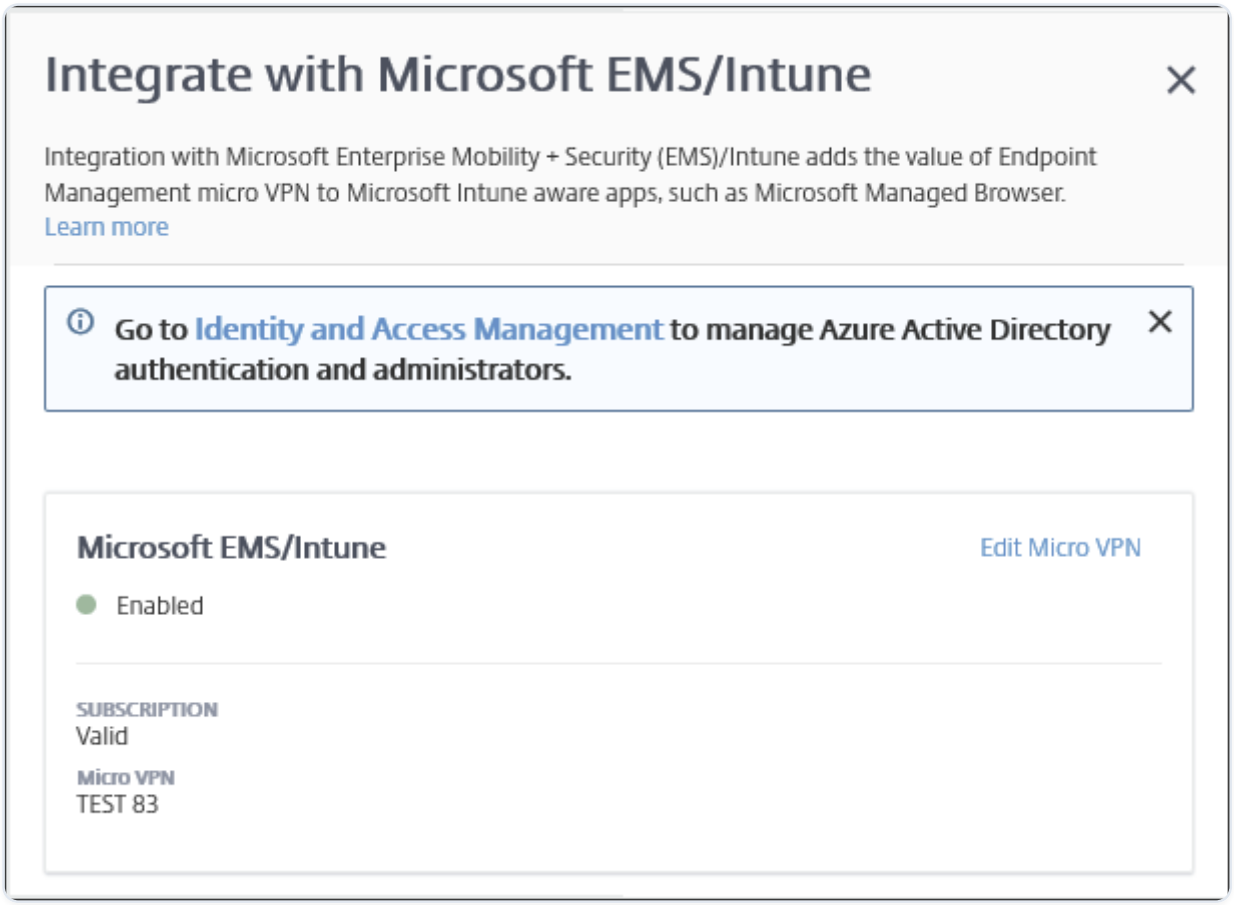
- Citrix Cloud 管理员默认是 Citrix Endpoint Management 管理员。
- 使用客户访问权限创建的 Citrix Cloud 管理员必须选择 Citrix Endpoint Management 才能管理 Citrix Endpoint Management。

在 Citrix Endpoint Management 控制台中，您只能更改用户的角色和成员资格。要随时更改角色，请从 Citrix Cloud 控制板访问 Citrix Endpoint Management 控制台。转到**管理**选项卡，然后单击**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 集成。

在 Citrix Cloud 中完成配置后，按如下方式返回 Citrix Endpoint Management 控制台：转到 Citrix Cloud **主页**，然后单击 **Citrix 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 Citrix 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 会指示您是否已成功启用连接。

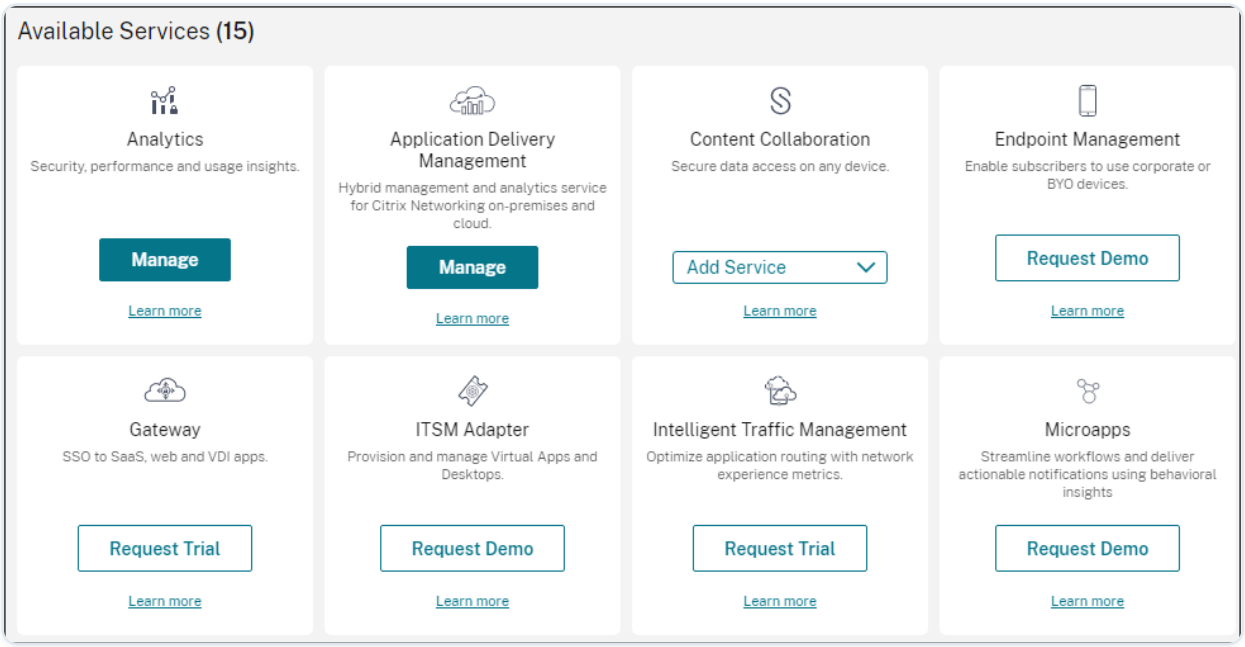


在 Citrix Cloud 控制台中，您还可以更改用户名或密码，以及删除或编辑本地用户。请参阅身份和访问管理。

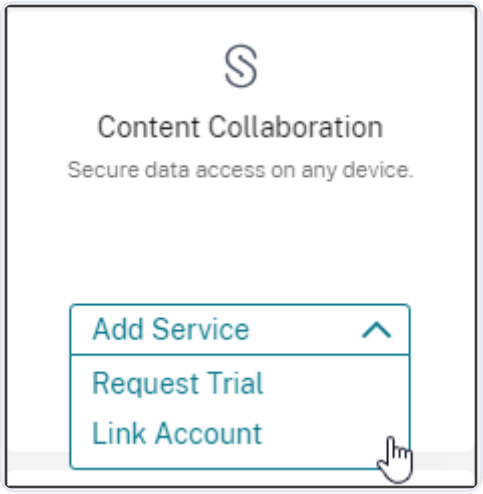
将现有 ShareFile 帐户链接到 Citrix Cloud

如果您在注册 Citrix Cloud 之前拥有 ShareFile 帐户，则必须将该帐户链接到 Citrix Cloud。要链接您的帐户，您的电子邮件地址必须是 ShareFile 帐户的管理员。准备好继续时，请转到 `<https://onboarding.cloud.com>`。

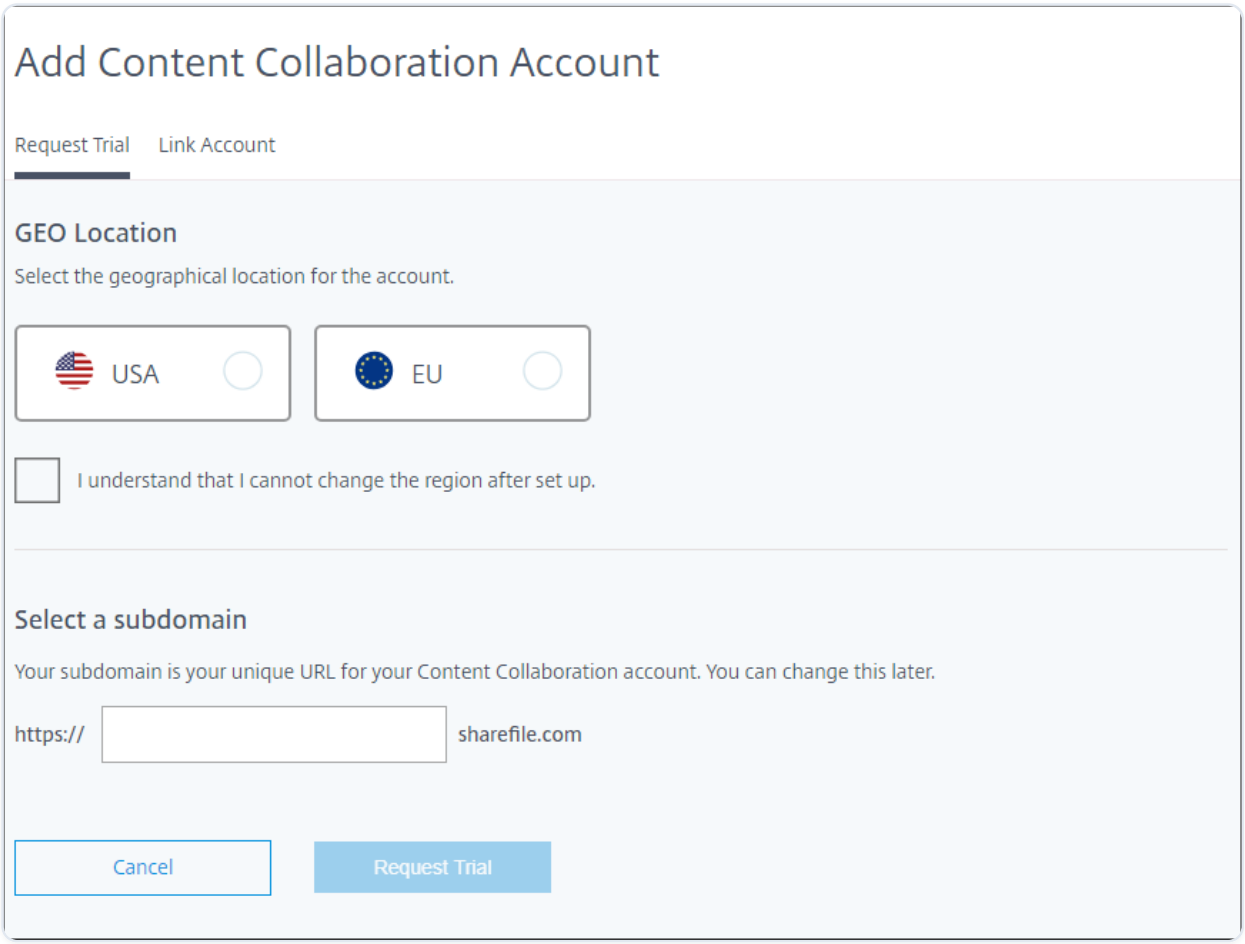
1. 登录后，将显示一个类似于以下内容的屏幕。



2. 在 **ShareFile** 磁贴中，选择**链接帐户**。



3. 在我们确认您的 ShareFile 帐户后，将显示以下页面：



4. 点击**链接帐户**选项卡以完成此过程。您可以立即从 Citrix Cloud 管理您的 ShareFile 帐户。

Cloud Connectors 的规模和大小注意事项

在评估 Citrix Endpoint Management 服务的规模和可扩展性时，请根据您的具体要求研究并测试 Cloud Connectors 的配置。Cloud Connector 仅在设备注册期间承受负载。机器配置不足可能会对系统性能产生负面影响。

Citrix® 要求每个资源位置部署两个 Cloud Connector。请将 Cloud Connector 安装在专用服务器上，该服务器不与其他任何组件或产品共享职责。在我们的测试中，Cloud Connectors 以高可用性 (HA) 集的形式部署（**它们不进行负载均衡**）。

测试配置

- 两台专用 Windows Server 2019，2 个 vCPU，4 GB 内存
- Android 和 iOS 设备注册到 MDM+MAM，在 8 小时内平均分配
- Citrix Endpoint Management 配置为每小时为每 1,000 台设备注册 125 台设备
  - 1,000 台设备（每小时注册 125 台设备）
  - 5,000 台设备（每小时注册 625 台设备）

- 10,000 台设备（每小时注册 1250 台设备）
- 20,000 台设备（每小时注册 2500 台设备）

测试结果

云连接器	1,000 台设备	5,000 台设备	10,000 台设备	20,000 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%
内存最大值	76%	76%	76%	79%

准备注册设备和交付资源

重要提示：

在继续之前，请务必完成 (/zh-cn/citrix-endpoint-management/onboarding-and-resource-setup.html) 中描述的所有任务。

及时告知用户即将发生的更改。请参阅 Citrix 用户采用工具包欢迎页。

Citrix Endpoint Management 支持各种注册选项。本文介绍了启用所有受支持设备注册所需的基本设置。下图总结了基本设置。

准备设备注册环境的工作流图 (/en-us/citrix-endpoint-management/media/workflow-prepare-for-device-enrollment.png)

有关受支持设备的列表，请参阅 (/zh-cn/citrix-endpoint-management/system-requirements/supported-device-platforms.html)。

为 iOS 设备设置 Apple 推送通知服务 (APNs) 证书

重要提示：

Apple 对 APNs 旧版二进制协议的支持将于 March 31, 2021 结束。Apple 建议您改用基于 HTTP/2 的 APNs 提供商 API。从 20.1.0 版本开始，Citrix Endpoint Management 支持基于 HTTP/2 的 API。有关详细信息，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 APNs 连接的帮助，请参阅 连接检查。

Citrix Endpoint Management 需要 Apple 提供的 Apple 推送通知服务 (APNs) 证书才能注册和管理 iOS 设备。Citrix Endpoint Management 还需要 APNs 证书才能用于 Citrix Secure Mail for iOS 推送通知。

- 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 网站。
- 要获取 APNs 证书并将其导入 Citrix Endpoint Management，请参阅 (/zh-cn/citrix-endpoint-management/authentication/apns.html)。

  创建证书页面 (/en-us/citrix-endpoint-management/media/create-apns-certificate.png)
- 有关 Citrix Endpoint Management 和 APNs 的更多信息，请参阅 (/zh-cn/citrix-secure-mail/push-notifications.html)。

为安卓设备设置 Firebase Cloud Messaging (FCM)

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

- FCM 设置要求您配置您的 Google 帐户。要创建 Google Play 凭据，请参阅管理您的开发者帐户信息。您还可以使用 Google Play 添加、购买和批准应用程序，以便部署到设备上的 Android Enterprise 工作区。您可以使用 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。
- 要设置 FCM，请参阅 Firebase Cloud Messaging。

设置 Citrix Endpoint Management 自动发现服务

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

借助自动发现服务，用户可以：

- 使用其企业网络凭据注册其设备。
- 无需输入有关 Citrix 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`。

我们建议您在高度安全的环境中使用自动发现服务。自动发现服务支持公钥证书锁定，可防止中间人攻击。证书锁定可确保当 Citrix 客户端与 Citrix Endpoint Management 通信时，使用由您的企业签名的证书。要为您的 Citrix Endpoint Management 站点配置证书锁定，请联系 Citrix 支持。有关证书锁定的信息，请参阅证书锁定。

要访问自动发现服务，请导航到 `<https://adsui.cloud.com>`（商业版）。

先决条件

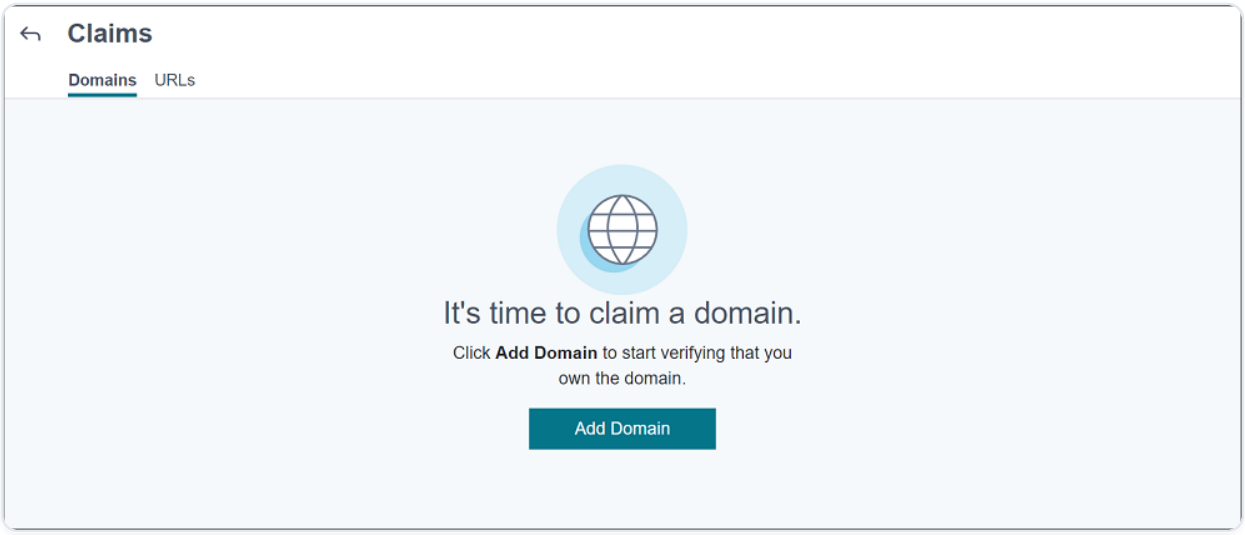
- Citrix Cloud 中的新自动发现服务需要最新版本的 Citrix Secure Hub：
  - 对于 iOS，Citrix Secure Hub 版本 21.6.0 或更高版本
  - 对于 Android，Citrix Secure Hub 版本 21.8.5 或更高版本

  运行早期版本 Citrix Secure Hub 的设备可能会遇到服务中断。
- 要访问新的自动发现服务，您必须拥有具有完全访问权限的 Citrix Cloud 管理员帐户。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。

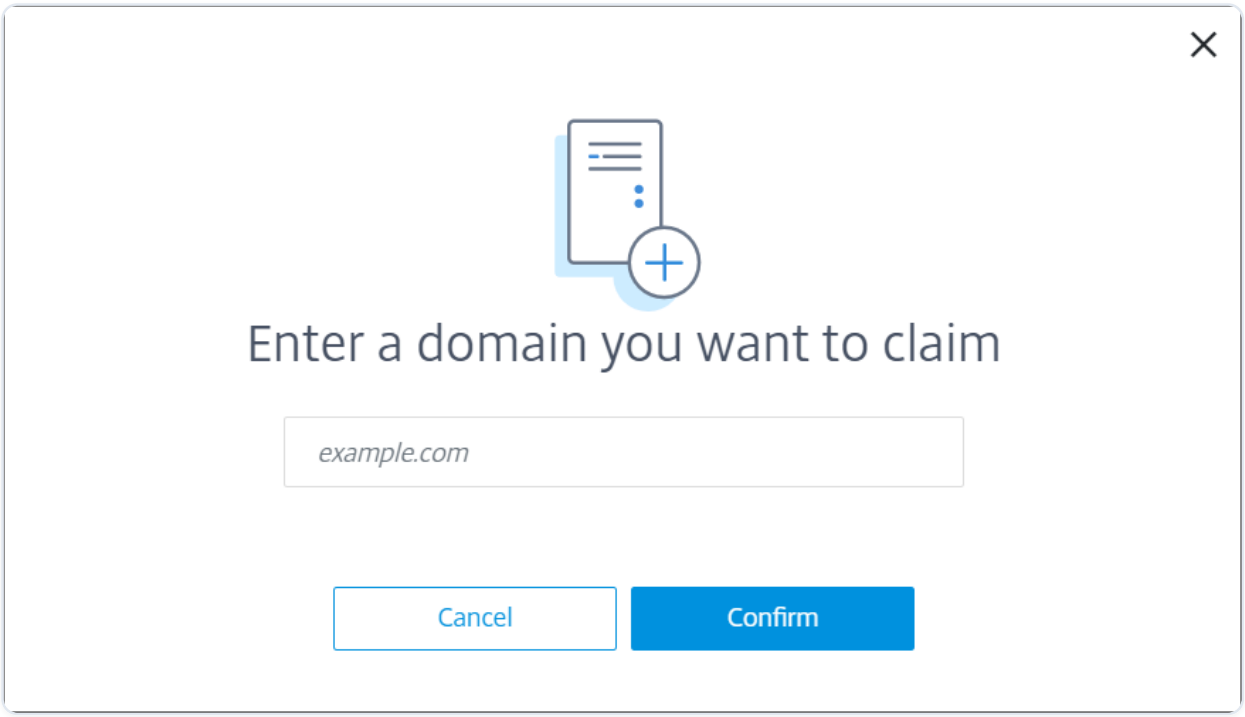
  Citrix 已将所有现有 AutoDiscovery 记录迁移到 Citrix Cloud，服务未中断。迁移的记录不会自动显示在新控制台中。您必须在新 AutoDiscovery 服务中重新声明域以证明所有权。有关详细信息，请参阅 CTX312339。
- 在开始将 AutoDiscovery 服务用于您的 Citrix Endpoint Management 部署之前，请验证并声明您的域。您最多可以声明 10 个域。该声明会将已验证的域与 AutoDiscovery 服务关联起来。要声明 10 个以上的域，请提交 SRE 票证或联系 Citrix 技术支持。
- 使用 MAM 端口设置而不是 NetScaler Gateway FQDN 将 MAM 流量定向到您的数据中心。如果您输入完全限定域名以及 NetScaler Gateway 的端口，客户端设备将使用 **MAM 端口**设置中的配置。
- 如果广告拦截器阻止站点打开，请确保为整个网站禁用广告拦截器。

声明域

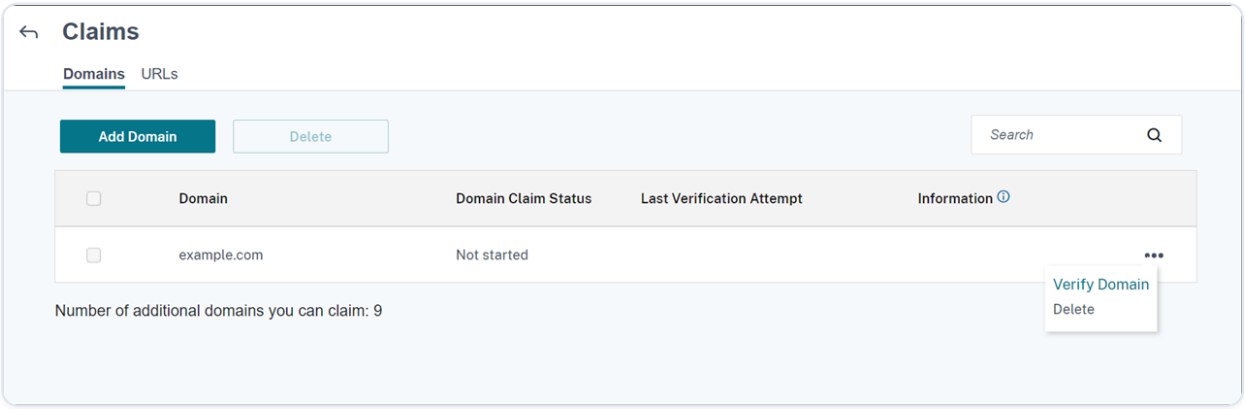
1. 在“**声明 > 域**”选项卡上，单击“**添加域**”。



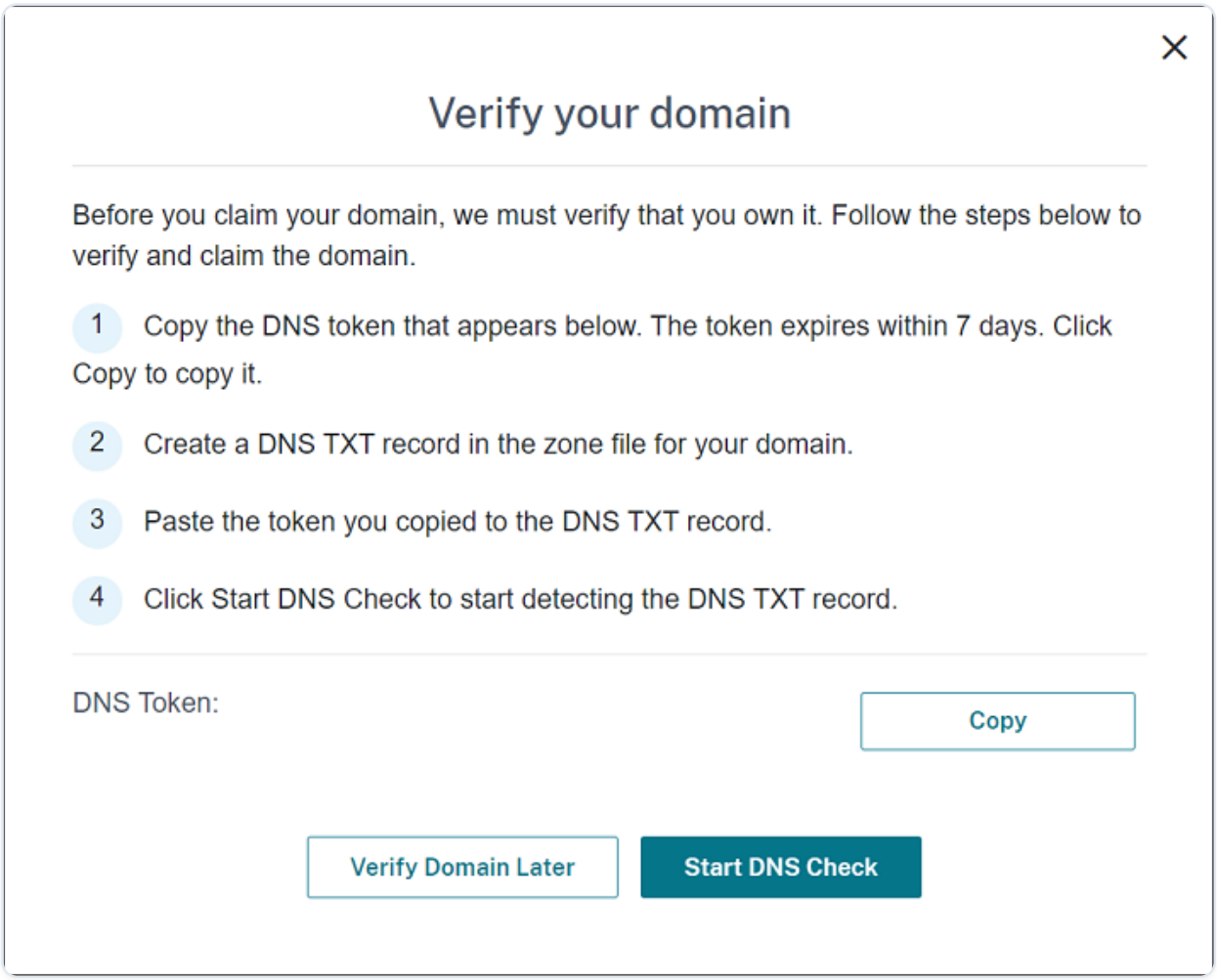
2. 在出现的对话框中，输入您的 Citrix Endpoint Management 环境的域名，然后单击“**确认**”。您的域将显示在“**声明 > 域**”中。



3. 在您添加的域上，单击省略号菜单并选择“**验证域**”以开始验证过程。此时将显示“**验证您的域**”页面。



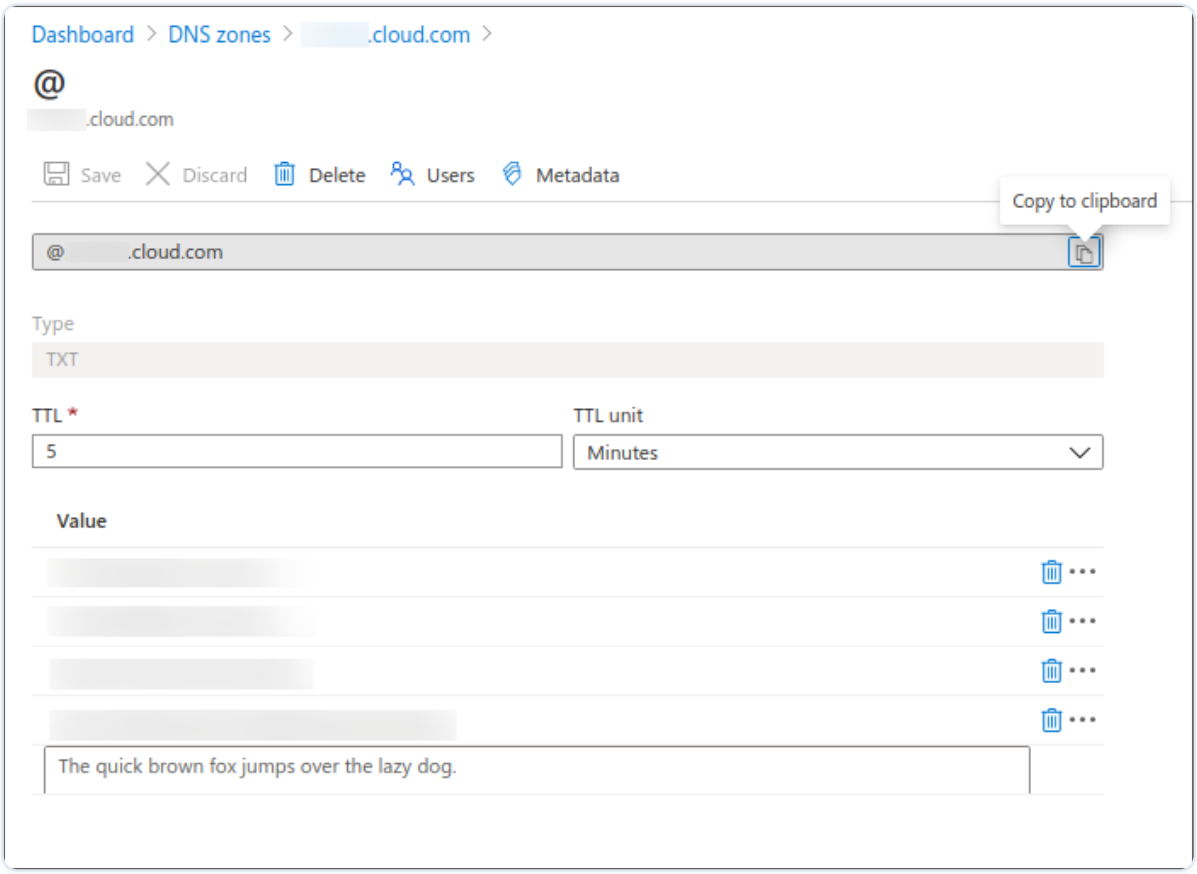
4. 在“**验证您的域**”页面上，按照说明验证您是否拥有该域。



a. 单击“**复制**”将 DNS 令牌复制到剪贴板。

b. 在您的域的区域文件中创建 DNS TXT 记录。为此，请转到您的域托管服务提供商门户并添加您复制的 DNS 令牌。

   以下屏幕截图显示了一个域托管服务提供商门户。您的门户可能有所不同。



c. 在 Citrix Cloud 中，在**验证您的域**页面上，单击**开始 DNS 检查**以开始检测您的 DNS TXT 记录。如果您想稍后验证域，请单击**稍后验证域**。

验证过程通常需要大约一个小时。但是，返回响应可能需要长达两天的时间。在状态检查期间，您可以注销并再次登录。

配置完成后，您的域状态将从**待处理**变为**已验证**。

5. 声明您的域后，提供有关 AutoDiscovery 服务的信息。单击您添加的域上的省略号菜单，然后单击**添加 Citrix Endpoint Management 信息**。此时将显示**AutoDiscovery 服务信息**页面。
6. 输入以下信息，然后单击**保存**。

- **Citrix Endpoint Management Server FQDN：** 输入 Citrix 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 流量控制。
- **NetScaler Gateway FQDN：** 输入 NetScaler 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 MDM 部署，请将此字段留空。

> **注意：**

> Citrix 建议您使用**MAM 端口**设置而不是**NetScaler Gateway FQDN**来控制 MAM 流量。如果您输入完全限定域名以及 NetScaler Gateway 的端口，客户端设备将使用**MAM 端口**设置中的配置。

- **实例名称：** 输入您之前配置的 Citrix Endpoint Management 服务器的实例名称。如果您不确定实例名称，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 AutoDiscovery

如果您计划注册 Windows 设备，请执行以下操作：

1. 联系 Citrix 支持并创建支持请求以启用 Windows 自动发现。
2. 获取 `enterpriseenrollment.mycompany.com` 的公共签名非通配符 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上一步中创建的支持请求。

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

   - 具有指定其服务的主域的 CN 的 SubjectDN（例如，enterpriseenrollment.mycompany1.com）。
   - 剩余域的相应 SAN（例如，enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.com 等）。
3. 在您的 DNS 中创建规范名称 (CNAME) 记录，并将您的 SSL 证书地址 (enterpriseenrollment.mycompany.com) 映射到 autodisc.xm.cloud.com。

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

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

至此，您可以注册所有受支持的设备。转到下一节，准备向设备交付资源。

与 Azure AD 条件访问集成

您可以将 Citrix Endpoint Management 配置为对 Office 365 应用程序应用 Azure AD 条件访问支持。此功能允许您在部署 Office 365 应用程序时向设备用户部署零信任方法。您可以使用设备状态、风险评分、位置和设备保护来应用自动化操作，并定义对托管的 Android Enterprise 和 iOS 设备上的 Office 365 应用程序的访问。

要强制执行 Azure AD 设备合规性，您必须为单个 Office 365 应用程序配置条件访问策略。您可以限制用户在非托管和不合规设备上访问特定的 Office 365 应用程序，并且只允许在托管和合规设备上访问单个应用程序。

先决条件

- 对于此集成，您必须拥有有效的 Azure AD 高级订阅，包括 Intune 和 Microsoft Office 365 许可证。
- Citrix Secure Hub 21.4.0 及更高版本
- 在 Citrix Cloud 中将 Azure AD 配置为身份提供程序 (IdP)，然后将 Citrix 身份设置为 Citrix 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 Citrix 多租户 AAD 应用程序，以允许移动应用程序使用 AAD 客户端应用程序进行身份验证。仅当 Azure 全局管理员将“**用户可以注册应用程序**”的值设置为“**否**”时才需要。在 Azure 门户中的“**Azure Active Directory > 用户 > 用户设置**”下配置此设置。要提供同意，请参阅 为 Azure AD 合规性管理配置 Citrix Endpoint Management。
- 在开始 Azure AD 设备注册过程之前，请在设备上安装 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所需的公共应用商店应用程序。
- 在 Azure AD 控制台中禁用“**安全默认值**”设置。启动 Azure AD 配置时，您将使用更精细的 Azure AD 条件访问策略替换安全默认值。有关安全默认值的更多信息，请参阅 Microsoft 文档。

通过 Azure AD 条件访问策略配置设备合规性

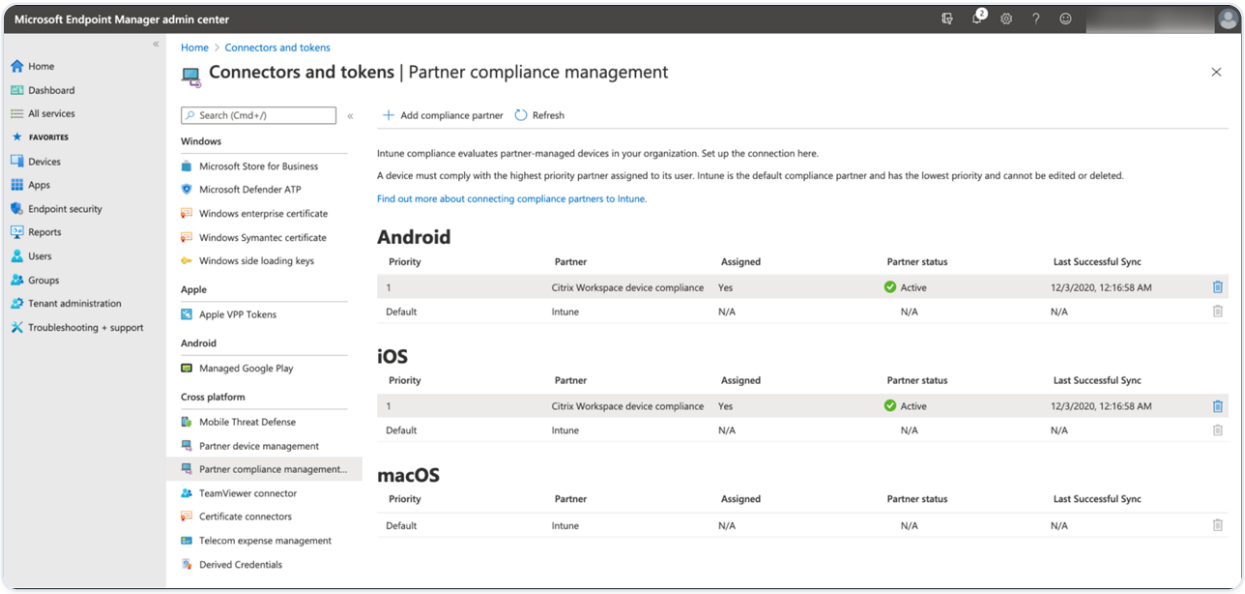
通过 Azure AD 条件访问策略配置设备合规性的常规步骤如下：

1. **Citrix 端点管理配置：**
    - 在 Microsoft Endpoint Manager 管理中心，将 **Citrix Workspace 设备合规性**添加为每个设备平台的合规性合作伙伴，并分配用户组。
    - 在 Citrix Endpoint Management 中，从 Microsoft Endpoint Manager 管理中心同步信息。

2. **Azure AD 配置：** 在 Azure AD 门户中，为单个 Office 365 应用程序设置条件访问策略。
3. **Citrix Endpoint Management 配置：** 为 Office 365 应用程序配置条件访问策略后，在 Citrix Endpoint Management 中将 Microsoft Authenticator 应用程序和 Office 365 应用程序添加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，并将其设置为所需应用程序。

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

1. 登录 Microsoft Endpoint Manager 管理中心，然后导航到“**租户管理 > 连接器和令牌 > 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合作伙伴。然后分配用户组。



2. 在 Citrix Endpoint Management 中，转到 **设置 > Azure AD 合规性管理**。
3. （可选）设置全局同意，以便用户无需在每台设备上提供同意。在 **客户端应用同意** 旁边，单击 **提供同意**。输入您的全局管理员 Azure AD 凭据，然后按照提示为客户端应用提供全局同意。
4. 单击 **连接** 以从 Microsoft Endpoint Manager 管理中心同步信息。

   从 Microsoft Endpoint Manager 管理中心同步信息(/en-us/citrix-endpoint-management/media/device-compliance-connect.png)

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

   权限请求(/en-us/citrix-endpoint-management/media/device-compliance-permissions-request.png)

在 Azure AD 中配置条件访问策略

在 Azure AD 门户中，为 Office 365 应用配置条件访问策略以强制执行设备合规性。转到 **设备 > 条件访问 > 策略 > 新策略**。有关详细信息，请参阅 Microsoft 文档。

要为 Intune 管理的应用配置设备合规性：

- 配置 Intune 管理的应用以交付到设备
- 要求批准的客户端应用
- 要求应用保护策略和批准的客户端应用以访问云应用

在 Citrix Endpoint Management 中配置应用

为 Office 365 应用配置条件访问策略后，将 Microsoft Authenticator 应用和 Office 365 应用作为公共应用商店应用添加到 Citrix Endpoint Management 中。将这些公共应用分配给交付组，并将其设置为所需应用。有关信息，请参阅 添加公共应用商店应用。

用户身份验证工作流

1. 已使用本地 Active Directory (AD) 注册设备并随后使用 Microsoft Azure Active Directory (AAD) 与 Citrix 身份提供程序集成的用户无需重新注册。您可以将帐户从本地 Active Directory 同步到 Microsoft Azure Active Directory。有关详细信息，请参阅 准备您的 Active Directory 和 Azure AD。
2. Citrix Endpoint Management 将 Microsoft Authenticator 和配置的 Office 365 应用作为所需应用推送到设备。如果将 Web 浏览器应用配置为 Android 平台所需的公共应用商店应用，Citrix Endpoint Management 也会将其推送到用户设备。
3. Citrix Secure Hub 自动安装并显示通过 Citrix Endpoint Management 管理的所有应用。
4. 当用户尝试登录任何可用的 Office 365 应用时，设备会提示用户点击**Azure AD 注册**链接以开始注册过程。
5. 用户点击注册链接后，Microsoft Authenticator 应用会打开。用户输入 Azure AD 凭据并同意设备注册条款。然后 Microsoft Authenticator 应用关闭，Citrix Secure Hub 重新打开。
6. Citrix Secure Hub 显示一条消息，指示 Azure AD 设备注册已完成。用户现在可以使用 Microsoft 应用访问其云资源。

   注册完成后，Azure AD 会在控制台中将设备标记为已管理且合规。

默认设备策略和移动生产力应用

如果您从 Citrix Endpoint Management 19.5.0 或更高版本开始加入，我们会预配置一些设备策略和移动生产力应用。该配置使您能够：

- 立即将基本功能部署到设备
- 从安全工作区的推荐基线配置开始

对于 安卓、安卓企业版、iOS、macOS 和 Windows 桌面/平板电脑平台，您的站点具有以下预配置的设备策略：

- **密码设备策略：** 密码设备策略为**开**，所有默认密码设置均已启用。
- **应用清单设备策略：** 应用清单设备策略为**开**。
- **限制设备策略：** 限制设备策略为**开**，所有默认限制设置均已启用。

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，创建您的交付组并禁用 AllUsers 交付组。您可以在交付组中重用预配置的设备策略和应用程序。

所有 Citrix 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。有关一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，您的站点具有以下预配置的移动生产力应用程序：

- **Citrix 安全邮件**
- **Citrix 安全 Web**
- **Citrix 文件**

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。

继续配置 Citrix 端点管理

完成设备注册的基本设置后，您配置 Citrix Endpoint Management 的方式会根据您的用例而有很大差异。例如：

- 您的安全要求是什么？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？
- 用户拥有自己的设备还是使用公司拥有的设备？

- 您希望将哪些设备策略推送到设备？
- 您为用户提供哪些类型的应用程序？

本节通过引导您查阅本文档集中的文章，帮助您了解众多配置选项。

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

- 安全和身份验证。Citrix 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 Citrix Endpoint Management 实例提供通配符证书。
  - 有关身份验证组件和按安全级别推荐的配置的讨论，请参阅“高级概念”文章：身份验证。另请参阅安全和用户体验。
  - 有关 Citrix Endpoint Management 操作期间使用的身份验证组件概述，请参阅证书和身份验证。
  - 您可以从以下身份验证类型中进行选择。配置身份验证包括在 Citrix Endpoint Management 和 NetScaler Gateway 控制台中执行的任务。
    - 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
  - 要向用户交付证书，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用户在 Citrix Endpoint Management 中注册其设备所需的凭据类型和注册步骤。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
  - 可用于注册大量设备的程序：
    - 通过 Apple 部署计划部署设备
    - 批量注册 Apple 设备
    - 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。

    - 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 Citrix Endpoint Management 设备策略均记录在 设备策略 下。有关一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。客户端属性包含直接提供给用户设备上的 Citrix Secure Hub 的信息。请参阅 客户端属性 和 Citrix Endpoint Management 客户端属性。
    - 交付组。有关与交付组相关的示例用例，请参阅 用户社区 和 添加交付组。

- 准备部署应用程序
    - 有关 Citrix Endpoint Management 支持的应用程序的信息，请参阅 添加应用程序。
    - 您可以使用 Apple Volume Purchase 管理 iOS 应用程序许可。有关详细信息，请参阅 Apple Volume Purchase。
    - 您可以使用 Citrix Endpoint Management 部署通过 Apple 批量采购获得的 iBooks。请参阅 添加媒体。
    - Citrix 提供移动生产力应用程序，包括 Citrix Secure Mail 和 Citrix Secure Web。请参阅 关于移动生产力应用程序。
    - 作为 Citrix Secure Mail 的替代方案，您可以将本机邮件交付到设备。请参阅：
        - 电子邮件策略
        - 适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器
        - 适用于 Exchange ActiveSync 的 NetScaler Gateway 连接器
    - 要允许用户安全地将文档和数据传输到 Microsoft Office 365 应用程序，请参阅 允许与 Office 365 应用程序安全交互 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 是一种应用程序封装技术，可为使用 Citrix Endpoint Management 进行安全部署的企业应用程序做准备。MAM SDK 取代了 MDX Toolkit。MDX Toolkit 计划于 2023 年 7 月达到 EOL。

      有关 MAM SDK 的信息，请参阅 MAM SDK 概述。

  - 有关应用程序的更多信息，请参阅 添加应用程序 下的其他文章。

- Citrix Endpoint Management 中的基于角色的访问控制 (RBAC) 功能允许您将预定义角色或权限集分配给用户和组。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。
- 您可以在 Citrix Endpoint Management 中创建自动化操作，以指定针对事件、特定设置或用户设备上应用程序的存在而采取的操作。有关信息，请参阅 自动化操作。

证书和身份验证

在 Citrix Endpoint Management 操作期间，有多个组件在身份验证中发挥作用：

- **Citrix Endpoint Management：** Citrix Endpoint Management 服务器是您定义注册安全性和注册体验的位置。用户入门选项包括：
    - 注册是向所有人开放还是仅限邀请。
    - 是否需要双因素身份验证或三因素身份验证。Citrix Endpoint Management 客户端属性允许您启用 Citrix PIN 身份验证并配置 PIN 复杂性和过期时间。
- **NetScaler Gateway：** NetScaler Gateway 为微 VPN SSL 会话提供终止。NetScaler Gateway 还提供网络传输中安全性，并允许您定义用户每次访问应用程序时使用的身份验证体验。
- **Citrix Secure Hub：** Citrix Secure Hub 和 Citrix Endpoint Management 在注册操作中协同工作。Citrix Secure Hub 是设备上与 NetScaler Gateway 通信的实体：当会话过期时，Citrix Secure Hub 从 NetScaler Gateway 获取身份验证票证，并将票证传递给 MDX 应用程序。Citrix 建议使用证书锁定，这可以防止中间人攻击。有关详细信息，请参阅 Citrix Secure Hub 文章中的此部分：证书锁定。

  Citrix Secure Hub 还促进了 MDX 安全容器：Citrix Secure Hub 推送策略，在应用程序超时时与 NetScaler Gateway 创建会话，并定义 MDX 超时和身份验证体验。Citrix Secure Hub 还负责越狱检测、地理位置检查以及您应用的任何策略。
- **MDX 策略：** MDX 策略在设备上创建数据保管库。MDX 策略将微 VPN 连接导回 NetScaler Gateway，强制执行离线模式限制，并强制执行客户端策略（例如超时）。

Citrix Endpoint Management 使用以下身份验证方法对用户进行资源身份验证：

- 移动设备管理 (MDM)
    - 云托管身份提供程序 (IdPs)
    - 轻量级目录访问协议 (LDAP)
        - 邀请 URL + PIN
        - 双因素身份验证
- 移动应用程序管理 (MAM)

  - LDAP
  - 证书
  - 安全令牌 MAM 身份验证需要 NetScaler Gateway。

有关其他配置详细信息，请参阅以下文章：

- 上传、更新和续订证书
- NetScaler 网关和 Citrix 端点管理
- 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
- 使用 Citrix Files 进行 SAML 单点登录
- 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 NetScaler Gateway 进行身份验证
- 要向 Wi-Fi 服务器进行身份验证，请向设备发送证书：网络设备策略
- 要推送不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）：凭据设备策略

证书

Citrix Endpoint Management 在安装过程中生成自签名安全套接字层 (SSL) 证书，以保护与服务器的通信流。请使用来自知名证书颁发机构的受信任 SSL 证书替换此 SSL 证书。

Citrix Endpoint Management 还使用其自己的公钥基础结构 (PKI) 服务，或从 CA 获取客户端证书。所有 Citrix 产品都支持通配符和主题备用名称 (SAN) 证书。对于大多数部署，您只需要两个通配符或 SAN 证书。

客户端证书身份验证为移动应用程序提供了额外的安全层，并允许用户无缝访问 HDX 应用程序。配置客户端证书身份验证后，用户输入其 Citrix PIN 即可对启用 Citrix 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 用于保护客户端证书或在设备本地保存 Active Directory 凭据。

要使用 Citrix Endpoint Management 注册和管理 iOS 设备，请设置并创建 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 Citrix Endpoint Management 组件的证书格式和类型：

思杰端点管理组件	证书格式	所需证书类型
NetScaler 网关	PEM (BASE64)、PFX (PKCS #12)	SSL、根 (NetScaler Gateway 会自动将 PFX 转换为 PEM。
思杰端点管理	.p12（在基于 Windows 的计算机上为 .pfx）	SSL、SAML、APN（Citrix Endpoint Management 还在安装过程中生成完整的 PKI。）**重要提示：** Citrix Endpoint Management 不支持 .pem 扩展名的证书。要使用 .pem 证书，请将 .pem 文件拆分为证书和密钥，然后将每个文件导入 Citrix Endpoint Management。
StoreFront	PFX (PKCS #12)	SSL，根

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

对于 NetScaler Gateway 和 Citrix Endpoint Management，建议从公共 CA（例如 Verisign、DigiCert 或 Thawte）获取服务器证书。您可以从 NetScaler Gateway 或 Citrix Endpoint Management 配置实用程序创建证书签名请求 (CSR)。创建 CSR 后，将其提交给 CA 进行签名。当 CA 返回签名证书时，您可以将证书安装在 NetScaler Gateway 或 Citrix Endpoint Management 上。

> **重要提示：**

> iOS、iPadOS 和 macOS 中受信任证书的要求

> Apple 对 TLS 服务器证书有新的要求。请验证所有证书是否符合 Apple 的要求。请参阅 Apple 的出版物，`<https://support.apple.com/zh-cn/HT210176>`。

> Apple 正在缩短 TLS 服务器证书的最大允许有效期。此更改仅影响 2020 年 9 月之后颁发的服务器证书。请参阅 Apple 的出版物，`<https://support.apple.com/zh-cn/HT211025>`。

LDAP 身份验证

Citrix Endpoint Management 支持针对一个或多个符合轻型目录访问协议 (LDAP) 的目录进行基于域的身份验证。LDAP 是一种软件协议，提供对组、用户帐户和相关属性信息的访问。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

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

IdP 的支持用例：

- 通过 Citrix 云 的 Azure 活动目录
  - Workspace 集成是可选的
  - 配置为基于证书身份验证的 NetScaler Gateway
  - Android Enterprise（预览版。支持 BYOD、完全托管设备和增强型注册配置文件）
  - 适用于 MDM+MAM 和 MDM 注册的 iOS
  - 适用于 Apple Business Manager 注册的 iOS 和 macOS
  - 旧版 Android (DA)

  自动注册功能（例如 Apple School Manager）目前不受支持。
- 通过 Citrix Cloud 的 Okta
  - Workspace 集成是可选的
  - 配置为基于证书身份验证的 NetScaler Gateway
  - Android Enterprise（预览版。支持 BYOD、完全托管设备和增强型注册配置文件）
  - 适用于 MDM+MAM 和 MDM 注册的 iOS
  - 适用于 Apple Business Manager 注册的 iOS 和 macOS
  - 旧版 Android (DA)

  自动注册功能（例如 Apple School Manager）目前不受支持。
- 通过 Citrix Cloud 的本地 NetScaler Gateway

- NetScaler Gateway 配置为基于证书的身份验证
- Android Enterprise (预览版。支持 BYOD、完全托管设备和增强型注册配置文件)
- iOS 用于 MDM+MAM 和 MDM 注册
- 旧版 Android (DA) 自动注册功能（例如 Apple Deployment Program）目前不受支持。

上传、更新和续订证书

建议您列出 Citrix Endpoint Management 部署所需的证书。使用此列表跟踪证书的到期日期和密码。本文将帮助您管理证书的整个生命周期。

您的环境可能包含以下证书：

- Citrix 端点管理服务器
  - MDM FQDN 的 SSL 证书（如果您从 XenMobile Server 迁移到 Citrix Endpoint Management，则需要此证书。否则，Citrix 会管理此证书。）
  - SAML 证书（适用于 Citrix Files）
  - 上述证书以及任何其他内部资源（StoreFront/Proxy 等）的根证书和中间 CA 证书
  - 适用于 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）
- MDX 工具包
  - Apple 开发者证书
  - Apple 预配配置文件（按应用程序）
  - Apple APNs 证书（用于 Citrix 安全邮件）
  - Android 密钥库文件

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

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捆绑包中。
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该证书。

上传证书

您上传的每个证书都在“证书”表中有一个条目，其中包括其内容的摘要。当您配置需要证书的 PKI 集成组件时，请选择一个服务器证书以满足条件。例如，您可能希望配置 Citrix Endpoint Management 以与您的 Microsoft 证书颁发机构 (CA) 集成。与 Microsoft CA 的连接必须使用客户端证书进行身份验证。

Citrix Endpoint Management 可能没有给定证书的私钥。同样，Citrix Endpoint Management 可能不需要上传证书的私钥。

本节提供了上传证书的一般步骤。有关创建、上传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。

您有两种上传证书的选项：

- 将证书单独上传到控制台。
- 使用 REST API 批量上传证书。此选项仅适用于 iOS 设备。

将证书上传到控制台时，您可以：

- 导入密钥库。然后，您需要识别密钥库存储库中要安装的条目，除非您上传的是 PKCS #12 格式。
- 导入证书。

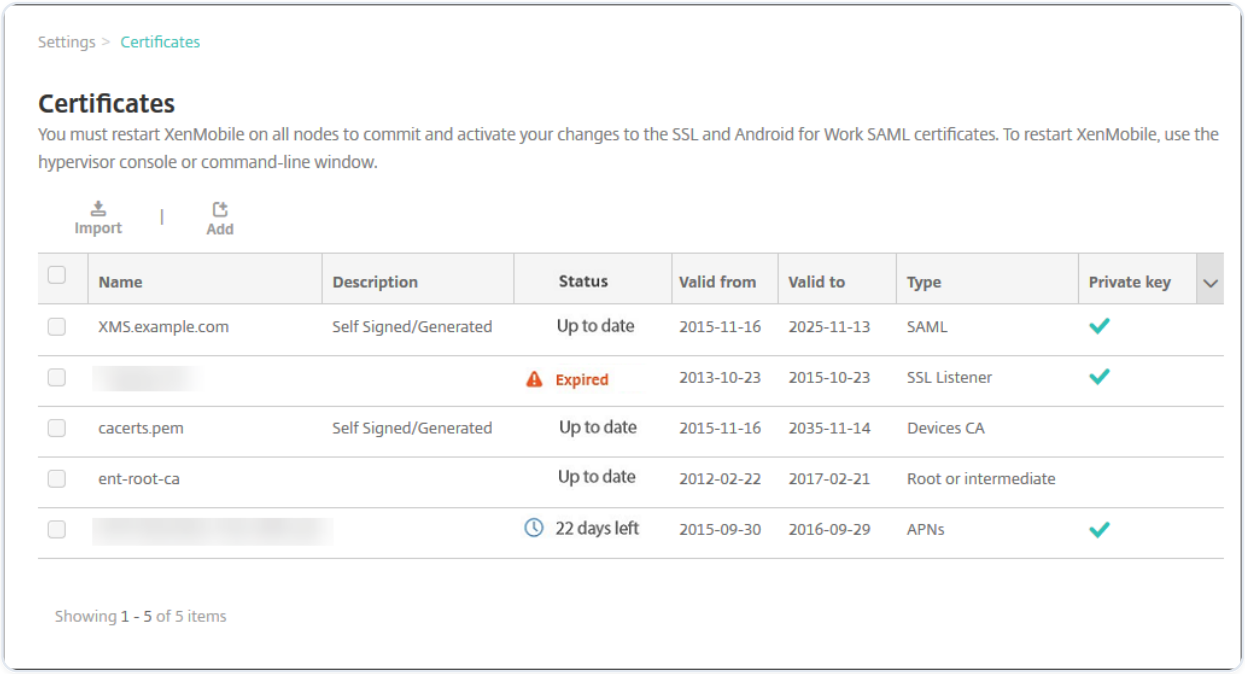
您可以上传 CA 用于签署请求的 CA 证书（不带私钥）。您还可以上传 SSL 客户端证书（带私钥）以进行客户端身份验证。

配置 Microsoft CA 实体时，您需要指定 CA 证书。您可以从所有作为 CA 证书的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 Citrix Endpoint Management 拥有私钥的所有服务器证书列表中进行选择。

导入密钥库

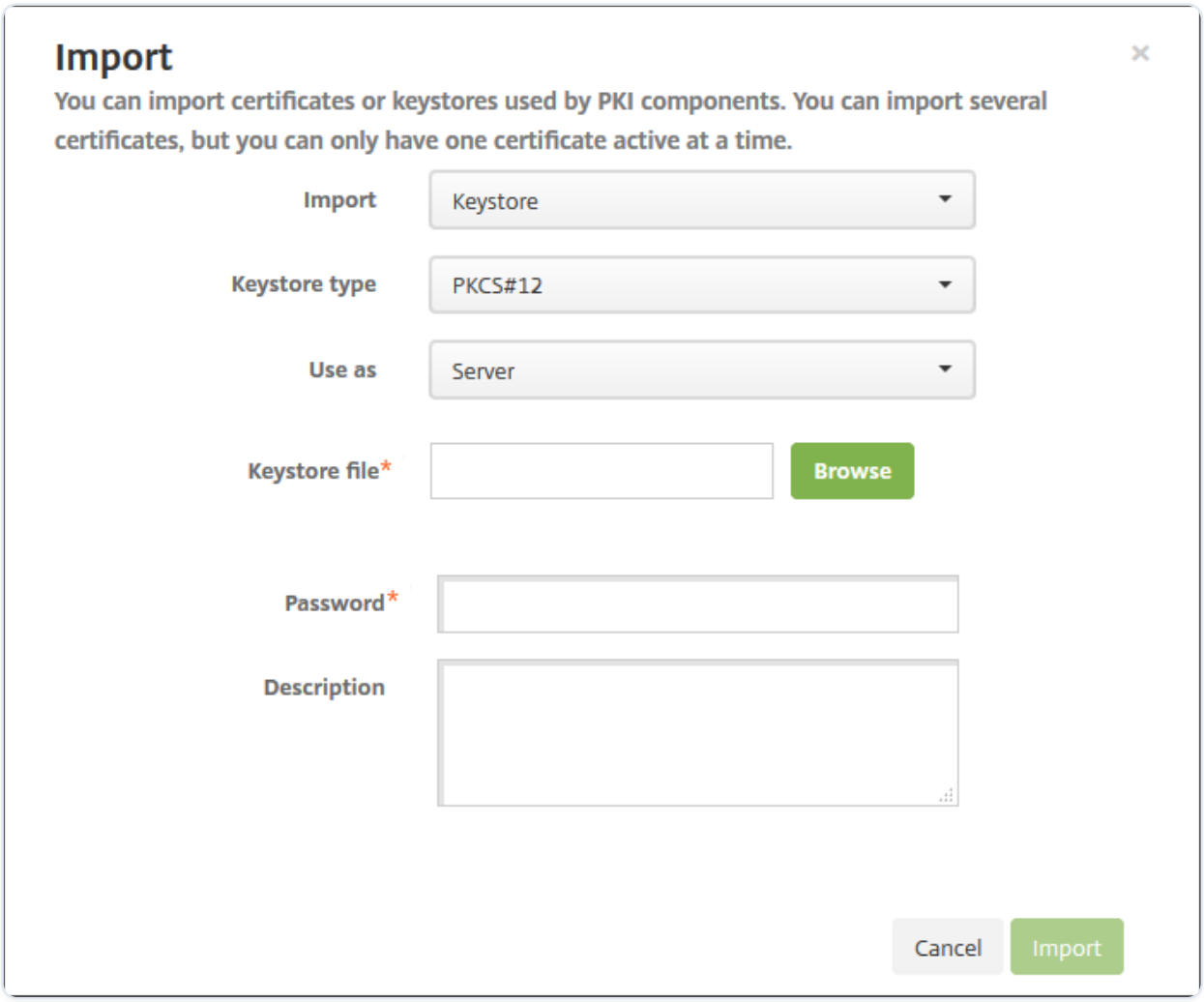
密钥库是安全证书的存储库。根据设计，密钥库可以有许多条目。从密钥库加载时，您必须指定标识要加载的条目的条目别名。如果您未指定别名，则会加载存储中的第一个条目。由于 PKCS #12 文件通常只有一个条目，因此当您选择 PKCS #12 作为密钥库类型时，别名字段不会出现。

1. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标。使用搜索栏查找并打开“**证书**”设置。



2. 单击“**导入**”。“**导入**”对话框随即出现。
3. 配置以下设置：

   - **导入**：选择“**密钥库**”。



- **密钥库类型：** 在下拉列表中单击 **PKCS #12**。
- **用途：** 在列表中，单击您计划如何使用证书。可用选项包括：
  - **服务器：** 服务器证书是 Citrix Endpoint Management 在功能上使用的证书。您可以将服务器证书上传到 Citrix Endpoint Management Web 控制台。这些证书包括 CA 证书、RA 证书以及用于客户端与基础结构的其他组件进行身份验证的证书。此外，您还可以使用服务器证书作为要部署到设备的证书的存储。此用途尤其适用于用于在设备上建立信任的 CA。
  - **SAML：** 安全断言标记语言 (SAML) 认证允许您为服务器、网站和应用程序提供 SSO 访问权限。
  - **APNs：** 来自 Apple 的 APNs 证书通过 Apple 推送网络启用移动设备管理。
  - **SSL 侦听器：** 安全套接字层 (SSL) 侦听器会通知 Citrix Endpoint Management 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 .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。

- **描述：** （可选）键入密钥库的描述，以帮助您将其与其他密钥库区分开来。

4. 单击 **导入**。密钥库将添加到“证书”表中。

导入证书

导入证书时，Citrix Endpoint Management 会尝试从输入构建证书链。Citrix Endpoint Management 会导入链中的所有证书，为每个证书创建一个服务器证书条目。此操作仅在文件或密钥库条目中的证书确实形成链时才有效。链中每个后续证书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描述。该描述仅附加到链中的第一个证书。您可以稍后更新其余证书的描述。

1. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标。使用搜索栏查找并打开“**证书**”设置。
2. 在“**证书**”页面上，单击“**导入**”。“**导入**”对话框随即出现。配置以下内容：

   - **导入：** 单击**证书**。
   - **用途：** 选择您计划如何使用证书。可用选项包括：
     - **服务器：** 服务器证书是 Citrix Endpoint Management 功能性使用的证书。您将服务器证书上传到 Citrix Endpoint Management Web 控制台。这些证书包括 CA 证书、RA 证书以及用于与基础架构的其他组件进行客户端身份验证的证书。此外，您还可以使用服务器证书作为要部署到设备的证书的存储。此选项尤其适用于用于在设备上建立信任的 CA。
     - **SAML：** 安全断言标记语言 (SAML) 认证允许您为服务器、网站和应用程序提供单点登录 (SSO) 访问。
     - **SSL 侦听器：** 安全套接字层 (SSL) 侦听器通知 Citrix Endpoint Management 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。私钥与证书一起用于加密和解密。选择文件，然后单击**打开**。
   - **描述：** （可选）键入证书的描述，以帮助您将其与其他证书区分开来。

3. 单击**导入**。证书将添加到“证书”表中。

使用 REST API 批量上传证书

有时，一次上传一个证书是不合理的。在这些情况下，请使用 REST API 批量上传证书。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. 将每个证书文件重命名为 `device_identity_value.p12` 格式。`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识别方法。如果一个设备的序列号为 `A12BC3D4EFGH`，则将您希望安装在该设备上的证书文件命名为 `A12BC3D4EFGH.p12`。

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

```
A12BC3D4EFGH.p12=password1!

A12BC3D4EFIJ.p12=password2@

A12BC3D4EFKL.p12=password3#
```

3. 将所有证书和您创建的文本文件打包到一个 .zip 文件中。
4. 启动您的 REST API 客户端，登录 Citrix Endpoint Management，并获取身份验证令牌。
5. 导入您的证书，并确保在消息正文中包含以下内容：

```
{

    "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

}
```

REST API 客户端(/en-us/citrix-endpoint-management/media/bulk-import-certificates.png)

6. 创建一个 VPN 策略，凭据类型为 **Always on IKEv2**，设备身份验证方法为 **Device Certificate Based on Device Identity**。选择您在证书文件名中使用的 **Device identity type**。请参阅 VPN 设备策略。
7. 注册 iOS 设备并等待 VPN 策略部署。通过检查设备上的 MDM 配置来确认证书安装。您还可以在 Citrix Endpoint Management 控制台中查看设备详细信息。

   iOS MDM 管理(/en-us/citrix-endpoint-management/media/bulk-certificate-ios.png)

   设备详细信息(/en-us/citrix-endpoint-management/media/bulk-certificate-device-details.png)

您还可以通过创建一个文本文件来批量删除证书，该文件中列出了要删除的每个证书的 `device_identity_value`。在 REST API 中，调用删除 API 并使用以下请求，将 `device_identity_value` 替换为相应的标识符：

```
{
    "identityType"="device_identity_value"
}
```

REST API 客户端(/en-us/citrix-endpoint-management/media/bulk-delete-certificates.png)

更新证书

Citrix Endpoint Management 系统中每个公钥一次只允许存在一个证书。如果您尝试为与已导入证书相同的密钥对导入证书，您可以：

- 替换现有条目。
- 删除条目。

上传新证书以替换旧证书后，您无法删除旧证书。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。新证书在列表中的位置低于旧证书。

更新您的证书

1. 通过遵循客户端证书或证书加域身份验证中的步骤创建替换证书。

> **重要提示：**
>
> 请勿使用现有私钥创建证书的选项。当您创建证书以更新即将过期的证书时，私钥也必须是新的。

2. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标。使用搜索栏查找并打开“**证书**”设置。
3. 在“**导入**”对话框中，导入新证书。

当您更新服务器证书时，使用先前证书的组件会自动切换到使用新证书。同样，如果您已在设备上部署了服务器证书，则该证书会在下次部署时自动更新。

要更新 APNs 证书，请执行创建证书的步骤，然后转到 Apple 推送证书门户。有关详细信息，请参阅续订 APNs 证书。

如果您的 NetScaler Gateway 已设置为 SSL 卸载，请确保使用新的 cacert.pem 更新您的负载均衡器。

> **注意：**
>
> 如果您已从本地 XenMobile 迁移到 Citrix Endpoint Management，并且正在更新证书，请在完成上述步骤后联系 Citrix 支持。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 NetScaler 并重新启动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)

您可以请求 Citrix Cloud Operations 刷新或重新生成 Citrix Endpoint Management 部署中的内部 PKI 证书颁发机构 (CA)。请为这些请求开具技术支持案例。

```
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，则该证书将变为无效。您将无法再在您的环境中运行安全事务，也无法访问 Citrix Endpoint Management 资源。证书颁发机构 (CA) 会提示您在到期日期之前续订 SSL 证书。执行前面描述的步骤来更新证书，然后开始在已注册设备上续订证书。

对于受支持的 iOS、macOS 和 Android 设备，您可以通过安全操作“证书续订”来启动证书续订。您可以从 Citrix Endpoint Management 控制台或公共 REST API 续订设备证书。对于已注册的 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)。

设备下次连接回 Citrix Endpoint Management 时，Citrix Endpoint Management 服务器会根据新的 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** 并选择要续订设备证书的设备。
2. 单击 **安全**，然后单击 **证书续订**。

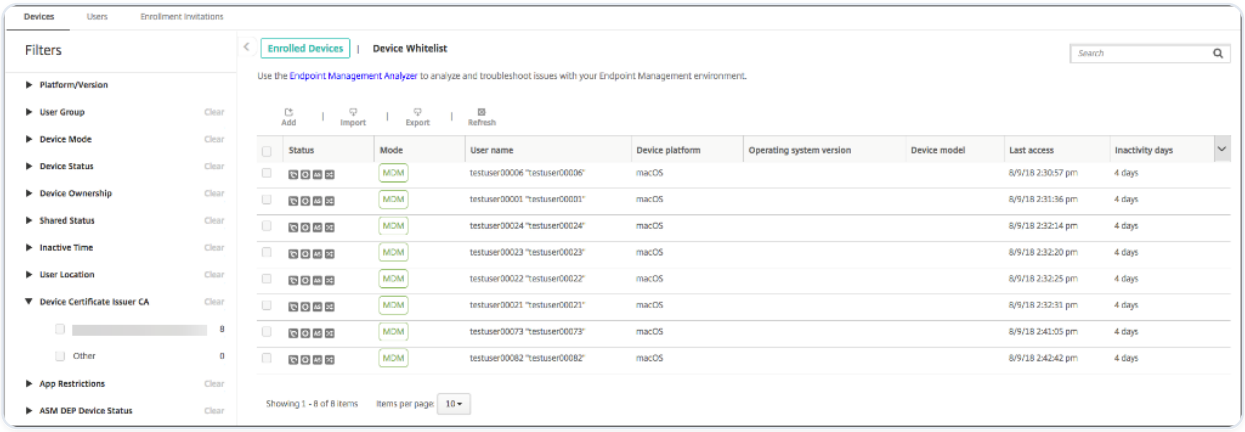


已注册的设备将继续正常工作，不受中断影响。当设备重新连接到服务器时，Citrix Endpoint Management 会颁发设备证书。

要查询属于特定设备证书颁发者 CA 组的设备：

1. 在 **管理 > 设备** 中，展开 **筛选器** 窗格。
2. 在 **筛选器** 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

Citrix Endpoint Management 在内部将以下证书颁发机构 (CA) 用于 PKI：根 CA、设备 CA 和服务器 CA。这些 CA 是一个逻辑组，并具有一个组名称。在 Citrix Endpoint Management 预配期间，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。已注册的设备将继续正常工作，不受中断影响。当设备重新连接到服务器时，Citrix Endpoint Management 会颁发设备证书。有关详细信息，请下载 Public API for REST Services PDF。

- 返回仍在使用旧 CA 的设备列表（请参阅 Public API for REST Services PDF 中的 3.16.2 节）
- 续订设备证书（请参阅 3.16.58 节）
- 获取所有 CA 组（请参阅 3.23.1 节）

适用于 Citrix Secure Mail 的 APNs 证书

Apple 推送通知服务 (APNs) 证书每年都会过期。请务必在证书过期之前创建 APNs SSL 证书并在 Citrix 门户中更新。如果证书过期，用户将面临 Citrix Secure Mail 推送通知不一致的问题。此外，您将无法再为您的应用程序发送推送通知。

适用于 iOS 设备管理的 APNs 证书

要使用 Citrix Endpoint Management 注册和管理 iOS 设备，请设置并创建 Apple 的 APNs 证书。如果证书过期，用户将无法注册 Citrix Endpoint Management，并且您无法管理其 iOS 设备。有关详细信息，请参阅APNs 证书。

您可以通过登录 Apple 推送证书门户查看 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。

您还会在过期日期前 30 天和 10 天收到 Apple 发送的电子邮件通知。该通知包含以下信息：

```
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
```

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：

- 使用预配配置文件对应用程序进行签名。
- 使用相应的分发证书对应用程序进行签名。

要验证您是否拥有有效的 iOS 分发证书，请执行以下操作：

1. 在 Apple 企业开发者门户中，为您计划使用 MDX 包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 示例为：`com.CompanyName.ProductName`。
2. 在 Apple 企业开发者门户中，转到 **Provisioning Profiles > Distribution**（预配配置文件 > 分发）并创建内部预配配置文件。对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，请参阅包装 iOS 移动应用程序。

要确认所有 Citrix Endpoint Management 服务器证书均有效，请执行以下操作：

1. 在 Citrix Endpoint Management 控制台中，单击“**设置 > 证书**”。
2. 检查所有证书（包括 APNs、SSL 侦听器、根证书和中间证书）是否有效。

Android 密钥库

密钥库是包含用于签署 Android 应用程序的证书的文件。当密钥有效期到期时，用户将无法无缝升级到应用程序的新版本。

NetScaler 网关

有关如何处理 NetScaler Gateway 证书过期的详细信息，请参阅 Citrix 支持知识中心中的如何处理 NetScaler 上的证书过期。

过期的 NetScaler Gateway 证书会阻止用户注册和访问应用商店。过期的证书还会阻止用户在使用 Citrix Secure Mail 时连接到 Exchange Server。此外，用户无法枚举和打开 HDX 应用程序（具体取决于哪个证书已过期）。

过期监视器和命令中心可以帮助您跟踪 NetScaler Gateway 证书。该中心会在证书过期时通知您。这些工具可帮助监控以下 NetScaler Gateway 证书：

- 适用于 MDM FQDN 的 SSL 证书
- 适用于 Gateway FQDN 的 SSL 证书
- 适用于 ShareFile SZC FQDN 的 SSL 证书
- 适用于 Exchange 负载平衡（卸载配置）的 SSL 证书
- 适用于 StoreFront 负载平衡的 SSL 证书
- 上述证书的根 CA 证书和中间 CA 证书

NetScaler 网关和 Citrix 端点管理

与 Citrix Endpoint Management 集成后，NetScaler Gateway 可为您的内部网络和资源提供远程设备访问。Citrix Endpoint Management 会在设备上的应用程序与 NetScaler Gateway 之间创建微型 VPN。

您可以使用 Citrix Gateway 服务（预览版）或本地 NetScaler Gateway（也称为 NetScaler Gateway）。有关这两种 NetScaler Gateway 解决方案的概述，请参阅配置 NetScaler Gateway 与 Citrix Endpoint Management 配合使用。

配置远程设备访问内部网络的身份验证

1. 在 Citrix 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，单击“**NetScaler Gateway**”。此时将显示“**NetScaler Gateway**”页面。在以下示例中，存在一个 NetScaler Gateway 实例。



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**”。
   - **交付用户证书以进行身份验证：** 选择是否希望 Citrix Endpoint Management 与 Citrix Secure Hub 共享身份验证证书。共享证书可使 NetScaler Gateway 处理客户端证书身份验证。默认值为“**关**”。
   - **凭据提供程序：** 单击下拉列表中的凭据提供程序。有关详细信息，请参阅凭据提供程序。
4. 点击 **保存**。

添加 Citrix Gateway 服务实例（预览版）

保存身份验证设置后，将 NetScaler Gateway 实例添加到 Citrix Endpoint Management。

1. 在 Citrix 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 NetScaler Gateway 磁贴，然后单击“**开始设置**”。此时将显示“**NetScaler Gateway**”页面。
3. 选择 **Citrix Gateway 服务（云）** 并指定 Gateway 服务的资源位置。

   NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/settings-add-gateway-service.png)

   - **Gateway 服务的资源位置：** 如果您使用 Citrix Secure Mail，则需要此项。指定 STA 服务的资源位置。资源位置必须包含已配置的 NetScaler Gateway。如果您以后想删除为 Gateway 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。新的 NetScaler Gateway 已添加。“**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**”。如果所选资源位置中没有可用的 Gateway Connector，请单击“**添加 Gateway Connector**”。按照屏幕上的指导安装 Gateway Connector。您也可以稍后添加 Gateway Connector。
4. 单击“**保存并导出脚本**”。

   - **保存并导出脚本**。单击此按钮可保存您的设置并导出配置包。您可以将包中的脚本上传到 NetScaler Gateway，以使用 Citrix Endpoint Management 设置对其进行配置。有关信息，请参阅这些步骤之后的“配置本地 NetScaler Gateway 以与 Citrix Endpoint Management 结合使用”。

   您已添加新的 NetScaler Gateway。“**NetScaler Gateway**”磁贴将显示在“**设置**”页面上。要编辑实例，请单击“**查看更多**”。

配置本地 NetScaler Gateway 以与 Citrix Endpoint Management 结合使用

要配置本地 NetScaler Gateway 以与 Citrix Endpoint Management 结合使用，请按照以下部分中详述的以下常规步骤操作。

1. 验证您的环境是否满足先决条件。
2. 从 Citrix Endpoint Management 控制台导出脚本包。
3. 从包中提取文件。如果您仅在 NetScaler Gateway 上使用经典策略，并且运行的是 Citrix ADC 13.0 或更早版本，请使用文件名中包含“Classic”的脚本。如果您使用任何高级策略，或者运行的是 Citrix ADC 13.1 或更高版本，请使用文件名中包含“Advanced”的脚本。
4. 在 NetScaler Gateway 上运行相应的脚本。有关最新的详细说明，请参阅脚本随附的 readme 文件。
5. 测试配置。

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

- MDM 和 MAM 所需的 NetScaler Gateway 虚拟服务器
- NetScaler Gateway 虚拟服务器的会话策略
- Citrix Endpoint Management 服务器详细信息
- 用于证书验证的代理负载平衡器
- NetScaler Gateway 虚拟服务器的身份验证策略和操作。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
- NetScaler Gateway 上的静态本地 DNS 记录
- 其他绑定：服务策略、CA 证书

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 NetScaler Gateway 配置脚本的先决条件

思杰端点管理要求：

- 在导出脚本包之前，请在 Citrix Endpoint Management 中完成 LDAP 和 NetScaler Gateway 配置。如果更改设置，请再次导出脚本包。

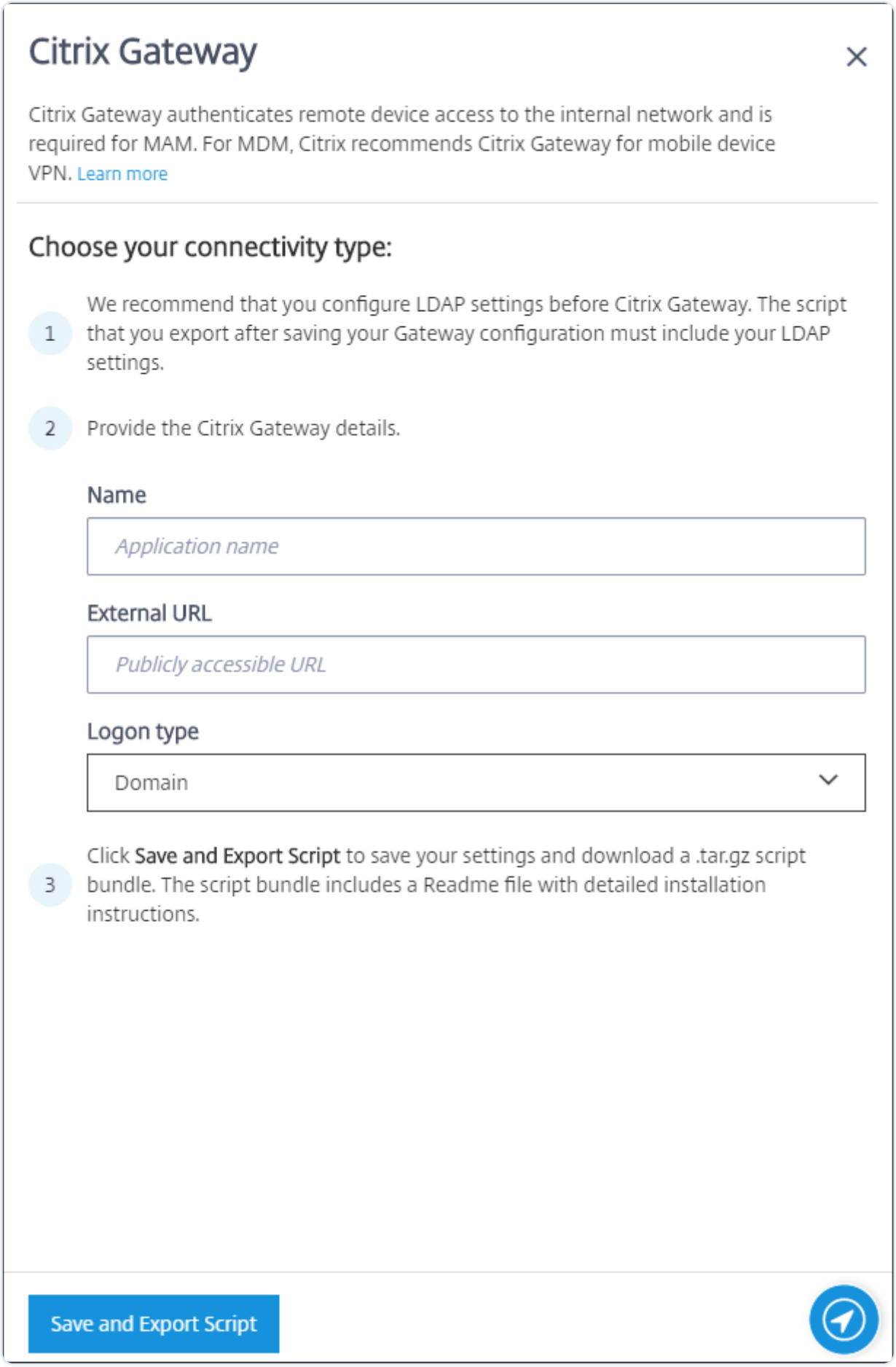
NetScaler Gateway 要求：

- 当在 NetScaler Gateway 上使用基于证书的身份验证时，您必须在 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。
- NetScaler Gateway（最低版本 11.0，内部版本 70.12）。
- NetScaler Gateway IP 地址已配置并已连接到 LDAP 服务器，除非 LDAP 已进行负载平衡。
- NetScaler Gateway 子网 (SNIP) IP 地址已配置，已连接到必要的后端服务器，并通过端口 8443/TCP 具有公共网络访问权限。
- DNS 可以解析公共域。
- NetScaler Gateway 需使用平台/通用或试用许可证。有关详细信息，请参阅 `<https://support.citrix.com/article/CTX126049>`。

从 Citrix Endpoint Management 导出脚本包

保存身份验证设置后，您将 NetScaler Gateway 实例添加到 Citrix Endpoint Management。

1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。**设置**页面随即打开。
2. 在**设置**页面上，滚动到 NetScaler Gateway 磁贴，然后单击**开始设置**。**NetScaler Gateway**页面随即显示。
3. 选择 **NetScaler Gateway (本地)** 并配置以下设置：



- **名称：** 键入 NetScaler Gateway 实例的名称。

- **外部 URL：** 键入 NetScaler Gateway 的公共可访问 URL。例如，`https://receiver.com`。
- **登录类型：** 选择登录类型。类型包括：**域**、**仅安全令牌**、**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，请参阅配置多个域的身份验证。

NetScaler Gateway 上的基于证书的身份验证需要额外配置。例如，您必须将根 CA 证书上传到 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**保存并导出脚本**。

   - **保存并导出脚本**。单击此按钮可保存您的设置并导出配置包。您可以将包中的脚本上传到 NetScaler Gateway，以使用 Citrix Endpoint Management 设置对其进行配置。有关信息，请在完成这些步骤后参阅“配置本地 NetScaler Gateway 以与 Citrix Endpoint Management 结合使用”。

   您已添加新的 NetScaler Gateway。**NetScaler 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
- 公共根 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）上传并安装到 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。

   NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/install-certificates-on-netscaler-gateway.png)

   以下示例显示了如何安装根证书。

   NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/install-certificates-detail-on-netscaler-gateway.png)

NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/nsgconfigbundle-folder.png)

NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/install-certificates-detail-filled-on-netscaler-gateway.png)

NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/certificates-list-netscaler-gateway.png)

确保同时安装根证书和中间证书。

2. 编辑脚本 (ConfigureCitrixGatewayScript_Classic.txt 或 ConfigureCitrixGatewayScript_Advanced.txt)，将所有占位符替换为您的环境中的详细信息。

   NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/script-placeholders-netscaler-gateway.png)

3. 在 NetScaler bash shell 中运行您编辑的脚本，如脚本包中包含的自述文件所述。例如：

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

   NetScaler Gateway 配置屏幕(/en-us/citrix-endpoint-management/media/run-script-for-netscaler-gateway.png)

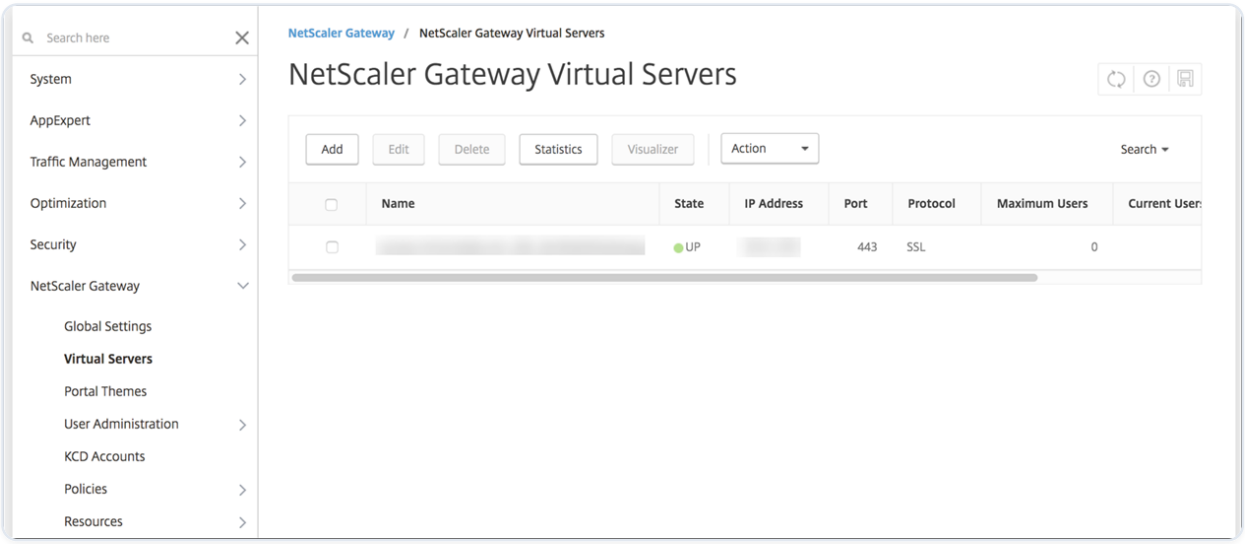
   脚本完成后，将显示以下行。

   NetScaler Gateway 成功屏幕(/en-us/citrix-endpoint-management/media/script-success-netscaler-gateway.png)

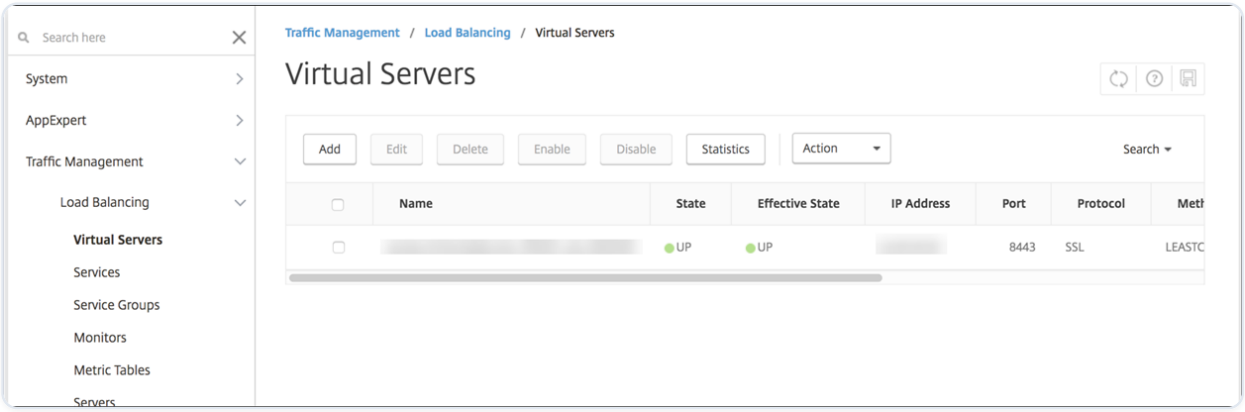
测试配置

要验证配置：

1. 验证 NetScaler Gateway 虚拟服务器的状态显示为 **UP**。



2. 验证代理负载平衡虚拟服务器的状态显示为 **UP**。



3. 打开 Web 浏览器，连接到 NetScaler Gateway URL，然后尝试进行身份验证。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，并确保它同时获得 MDM 和 MAM 注册。

为多个域配置身份验证

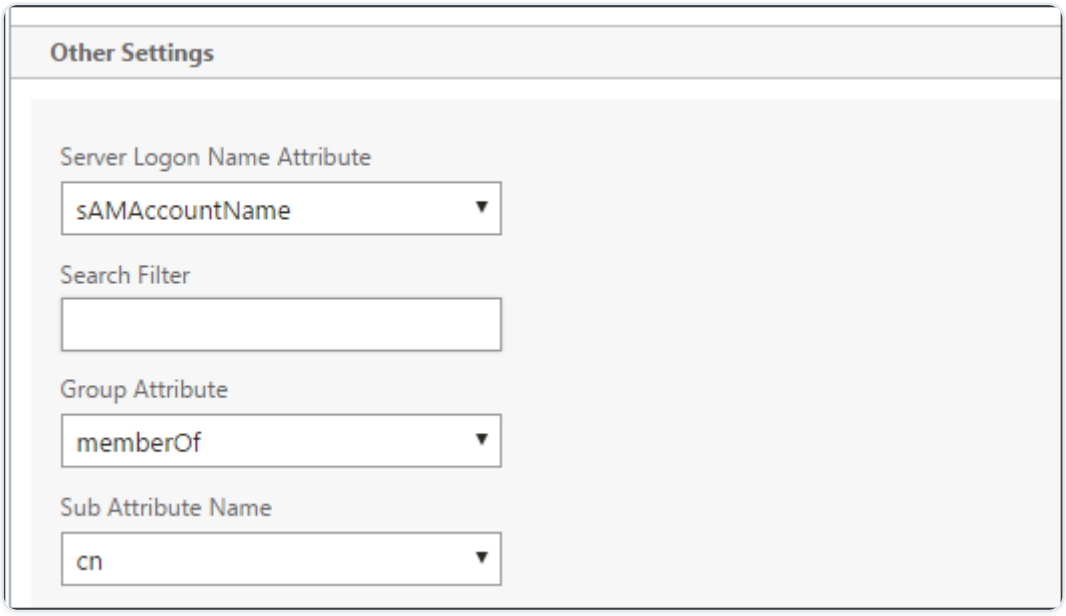
如果您有多个 Citrix Endpoint Management 实例（例如用于测试、开发和生产环境），则需要手动为其他环境配置 NetScaler Gateway。（NetScaler for XenMobile 向导只能使用一次。）

NetScaler Gateway 配置

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

1. 在 NetScaler Gateway 配置实用程序中，在“**Configuration**”（配置）选项卡上，展开“**NetScaler Gateway > Policies > Authentication**”（NetScaler Gateway > 策略 > 身份验证）。
2. 在导航窗格中，单击“**LDAP**”。

3. 单击以编辑 LDAP 配置文件。将“**Server Logon Name Attribute**”（服务器登录名属性）更改为 **userPrincipalName** 或您要用于搜索的属性。记下您指定的属性。在 Citrix Endpoint Management 控制台中配置 LDAP 设置时，您将提供此属性。

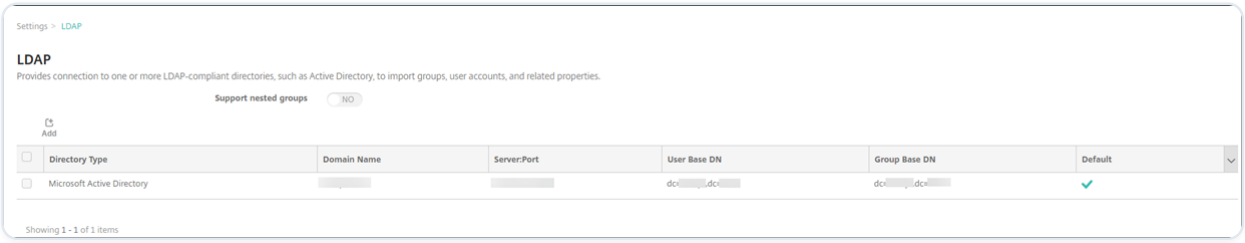


4. 为每个 LDAP 策略重复这些步骤。每个域都需要一个单独的 LDAP 策略。
5. 在绑定到 NetScaler Gateway 虚拟服务器的会话策略中，导航到 **编辑会话配置文件 > 已发布的应用程序**。确保 **单点登录域** 为空。

思杰端点管理配置

要在多域环境中配置 Citrix Endpoint Management LDAP：

1. 在 Citrix Endpoint Management 控制台中，转到 **设置 > LDAP** 并添加或编辑目录。



2. 提供信息。

   - 在 **域别名** 中，指定用于用户身份验证的每个域。使用逗号分隔域，并且域之间不要使用空格。例如：domain1.com,domain2.com,domain3.com
   - 确保 **用户搜索依据** 字段与 NetScaler Gateway LDAP 策略中指定的 **服务器登录名属性** 匹配。

   Citrix 端点管理 LDAP 设置屏幕(/en-us/citrix-endpoint-management/media/ldap-settings-multiple-domains2.png)

丢弃到特定 URL 的入站连接请求

如果您的环境中 NetScaler Gateway 配置为 SSL 卸载，您可能希望网关丢弃针对特定 URL 的入站连接请求。如果您需要额外的安全性，请联系 Citrix Cloud Operations 并请求他们允许您的 IP 访问您的本地数据中心。

域或域加安全令牌身份验证

Citrix Endpoint Management 支持针对一个或多个符合轻量级目录访问协议 (LDAP) 的目录进行基于域的身份验证。您可以在 Citrix Endpoint Management 中配置与一个或多个目录的连接。Citrix Endpoint Management 使用 LDAP 配置来导入组、用户帐户和相关属性。

> **重要提示：**
>
> 在用户将设备注册到 Citrix Endpoint Management 后，Citrix Endpoint Management 不支持将身份验证模式从一种类型更改为另一种类型。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 是一种开源、与供应商无关的应用程序协议，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有关整个网络中可用的用户、系统、网络、服务和应用程序的信息。

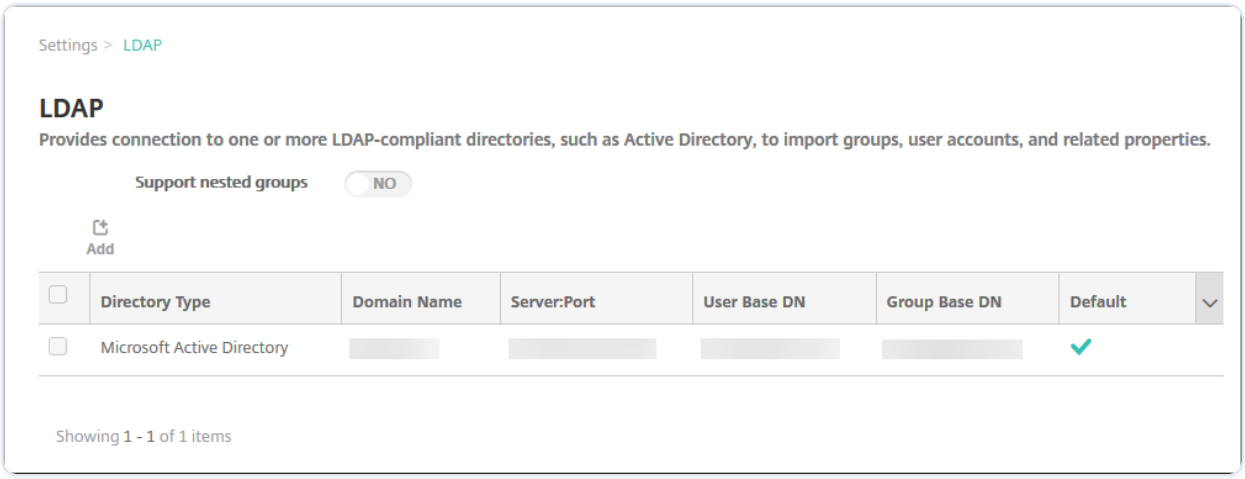
LDAP 的常见用途是为用户提供单点登录 (SSO)，其中单个密码（每个用户）在许多服务之间共享。单点登录使用户能够一次登录公司网站，以进行对公司内网的身份验证访问。

客户端通过连接到 LDAP 服务器（称为目录系统代理 (DSA)）来启动 LDAP 会话。然后，客户端向服务器发送操作请求，服务器使用相应的身份验证进行响应。

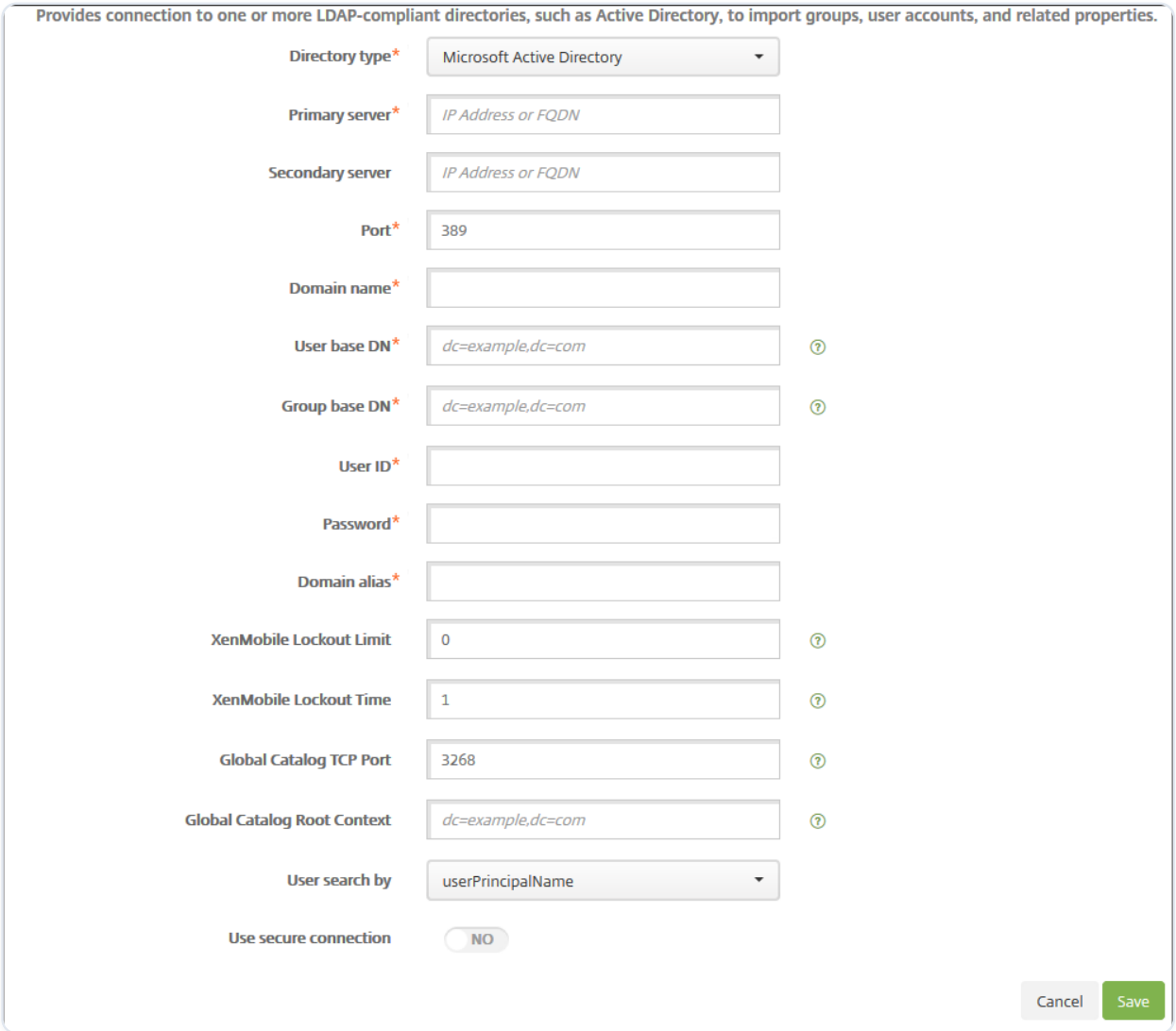
在 Citrix Endpoint Management 中添加或编辑 LDAP 连接

通常，在加入 Citrix 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已加入，请使用本部分中的信息添加 LDAP 连接。

1. 在 Citrix Endpoint Management 控制台中，转到 **设置 > LDAP**。
2. 在 **服务器** 下，单击 **LDAP**。**LDAP** 页面随即显示。



3. 在 **LDAP** 页面上，单击 **添加** 或 **编辑**。**添加 LDAP** 或 **编辑 LDAP** 页面随即显示。



4. 配置以下设置：

- **目录类型：** 在下拉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 地址或完全限定域名 (FQDN)。

- **辅助服务器：**（可选）如果已配置辅助服务器，请输入辅助服务器的 IP 地址或 FQDN。如果无法访问主服务器，此服务器将用作故障转移服务器。
- **端口：** 键入 LDAP 服务器使用的端口号。默认情况下，未加密 LDAP 连接的端口号设置为 **389**。安全 LDAP 连接使用端口号 **636**，Microsoft 未加密 LDAP 连接使用 **3268**，Microsoft 安全 LDAP 连接使用 **3269**。
- **域名：** 键入域名。
- **用户基本 DN：** 通过唯一标识符键入 Active Directory 中用户的位置。语法示例包括：`ou=users`、`dc=example` 或 `dc=com`。
- **组基本 DN：** 键入 Active Directory 中组的位置。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。
- **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。
- **Citrix Endpoint Management 锁定限制：** 键入一个介于 **0** 到 **999** 之间的数字，表示失败登录尝试的次数。值为 **0** 表示 Citrix Endpoint Management 永远不会根据失败的登录尝试锁定用户。默认值为 **0**。

  请考虑将此锁定限制设置为低于 LDAP 锁定策略的值。这样做有助于防止在 Citrix Endpoint Management 无法向 LDAP 服务器进行身份验证时用户被锁定。例如，如果 LDAP 锁定策略为 5 次尝试，请将此锁定限制配置为 **4** 或更低。
- **Citrix Endpoint Management 锁定时间：** 键入一个介于 **0** 到 **99999** 之间的数字，表示用户超出锁定限制后必须等待的分钟数。值为 **0** 表示用户在锁定后无需强制等待。默认值为 **1**。
- **全局编录 TCP 端口：** 键入全局编录服务器的 TCP 端口号。默认情况下，TCP 端口号设置为 **3268**；对于 SSL 连接，请使用端口号 **3269**。
- **全局编录根上下文：**（可选）键入用于在 Active Directory 中启用全局编录搜索的全局根上下文值。此搜索是对标准 LDAP 搜索的补充，可在任何域中进行，无需指定实际域名。
- **用户搜索方式：** 选择 Citrix Endpoint Management 在此目录中搜索用户时使用的用户名或用户 ID 格式。用户在注册时以这种格式输入其用户名或用户 ID。如果在注册后更改“**用户搜索方式**”设置，用户必须重新注册。

  如果选择“**userPrincipalName**”，用户将以以下格式输入用户主体名称 (UPN)：

  - `*username*@*domain*`

  如果选择“**sAMAccountName**”，用户将以以下格式之一输入安全帐户管理器 (SAM) 名称：

- `*username*@*domain*`
- `*domain\username*`

- **使用安全连接：** 选择是否使用安全连接。默认值为“**否**”。

5. 点击 **保存**。

删除符合 LDAP 的目录

1. 在“**LDAP**”表中，选择要删除的目录。

   您可以选择多个要删除的属性，方法是选中每个属性旁边的复选框。

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

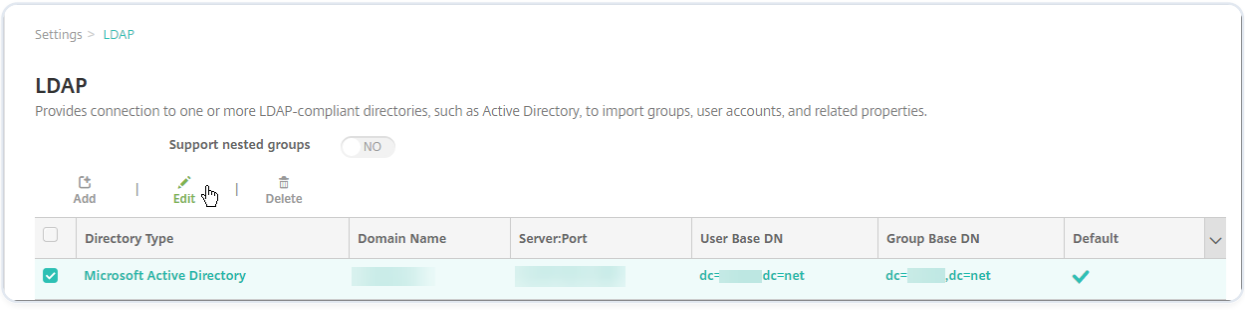
您可以将 Citrix Endpoint Management 配置为要求用户使用其 LDAP 凭据加一次性密码通过 RADIUS 协议进行身份验证。

为了获得最佳可用性，您可以将此配置与 Citrix PIN 和 Active Directory 密码缓存结合使用。通过该配置，用户无需重复输入其 LDAP 用户名和密码。用户输入用户名和密码以进行注册、密码过期和帐户锁定。

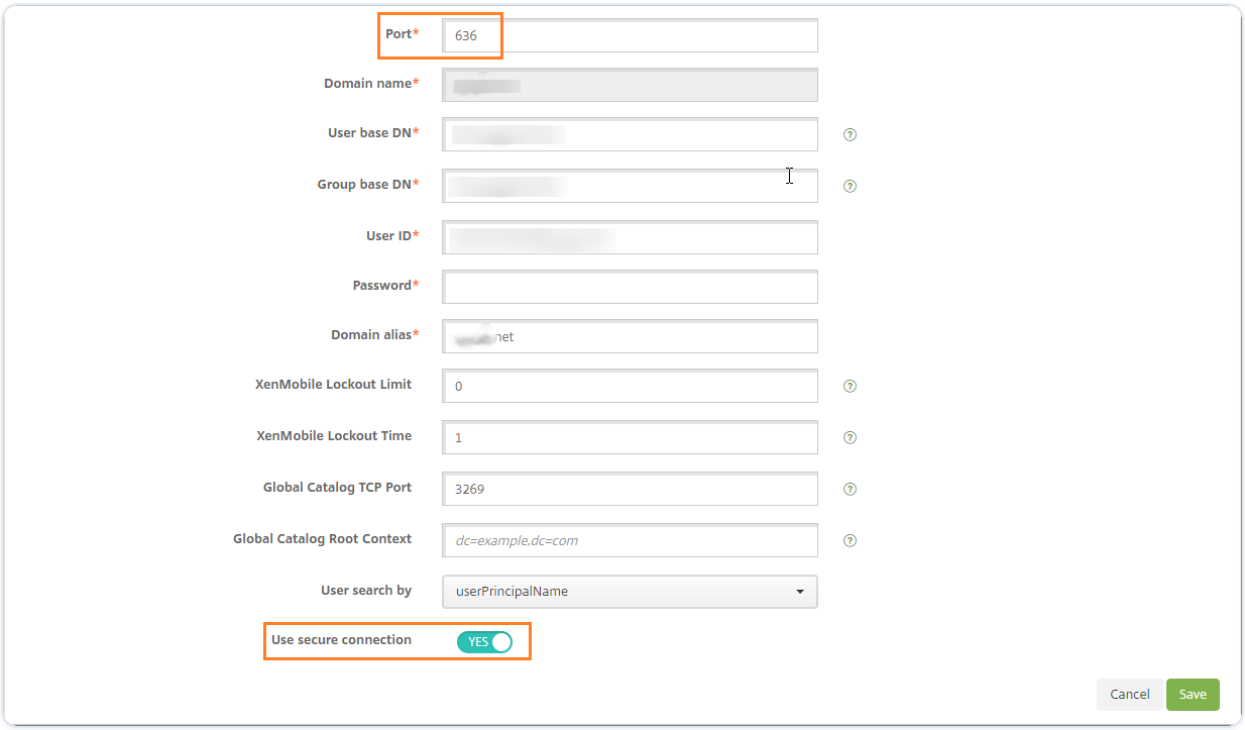
配置 LDAP 设置

使用 LDAP 进行身份验证要求您在 Citrix Endpoint Management 上安装来自证书颁发机构的 SSL 证书。有关详细信息，请参阅上载证书。

1. 在“**设置**”中，单击“**LDAP**”。
2. 选择“**Microsoft Active Directory**”，然后单击“**编辑**”。



3. 验证端口是否为 **636**（用于安全 LDAP 连接）或 **3269**（用于 Microsoft 安全 LDAP 连接）。
4. 将“**使用安全连接**”更改为“**是**”。



配置 NetScaler Gateway 设置

以下步骤假定您已将 NetScaler Gateway 实例添加到 Citrix Endpoint Management。要添加 NetScaler Gateway 实例，请参阅NetScaler Gateway 和 Citrix Endpoint Management。

1. 在“**设置**”中，单击“**NetScaler Gateway**”。
2. 选择 NetScaler Gateway，然后单击“**编辑**”。
3. 从“**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**”并选中以下复选框：“**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。

为域和安全令牌身份验证配置 NetScaler Gateway

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

客户端证书或证书加域身份验证

Citrix Endpoint Management 的默认配置是用户名和密码身份验证。为了在注册和访问 Citrix Endpoint Management 环境时增加一层安全性，请考虑使用基于证书的身份验证。在 Citrix Endpoint Management 环境中，此配置是安全性与用户体验的最佳组合。证书加域身份验证具有最佳的 SSO 可能性，并结合了 NetScaler Gateway 提供的双因素身份验证安全性。

为了获得最佳可用性，您可以将证书加域身份验证与 Citrix PIN 和 Active Directory 密码缓存结合使用。这样，用户无需重复输入其 LDAP 用户名和密码。用户在注册、密码过期和帐户锁定期间输入用户名和密码。

重要提示：

Citrix Endpoint Management 不支持用户在 Citrix Endpoint Management 中注册设备后，将身份验证模式从域身份验证更改为其他身份验证模式。

如果您不允许 LDAP 并使用智能卡或类似方法，配置证书可让您将智能卡表示给 Citrix Endpoint Management。然后，用户使用 Citrix Endpoint Management 为他们生成的唯一 PIN 进行注册。用户获得访问权限后，Citrix Endpoint Management 会创建并部署用于向 Citrix Endpoint Management 环境进行身份验证的证书。

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

在高度安全的环境中，在公共或不安全的网络中在组织外部使用 LDAP 凭据被认为是组织的主要安全威胁。对于高度安全的环境，使用客户端证书和安全令牌的双因素身份验证是一种选择。有关详细信息，请参阅配置 Citrix Endpoint Management 以进行证书和安全令牌身份验证。

客户端证书身份验证适用于在 MAM 和 MDM+MAM 中注册的设备。要对这些设备使用客户端证书身份验证，您必须配置 Microsoft 服务器、Citrix Endpoint Management，然后是 NetScaler Gateway。请按照本文中描述的这些一般步骤操作。

在 Microsoft 服务器上：

1. 将证书管理单元添加到 Microsoft 管理控制台。
2. 将模板添加到证书颁发机构 (CA)。
3. 从 CA 服务器创建 PFX 证书。

在 Citrix Endpoint Management 中：

1. 将证书上传到 Citrix 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. 配置 NetScaler Gateway 以交付用户证书进行身份验证。

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

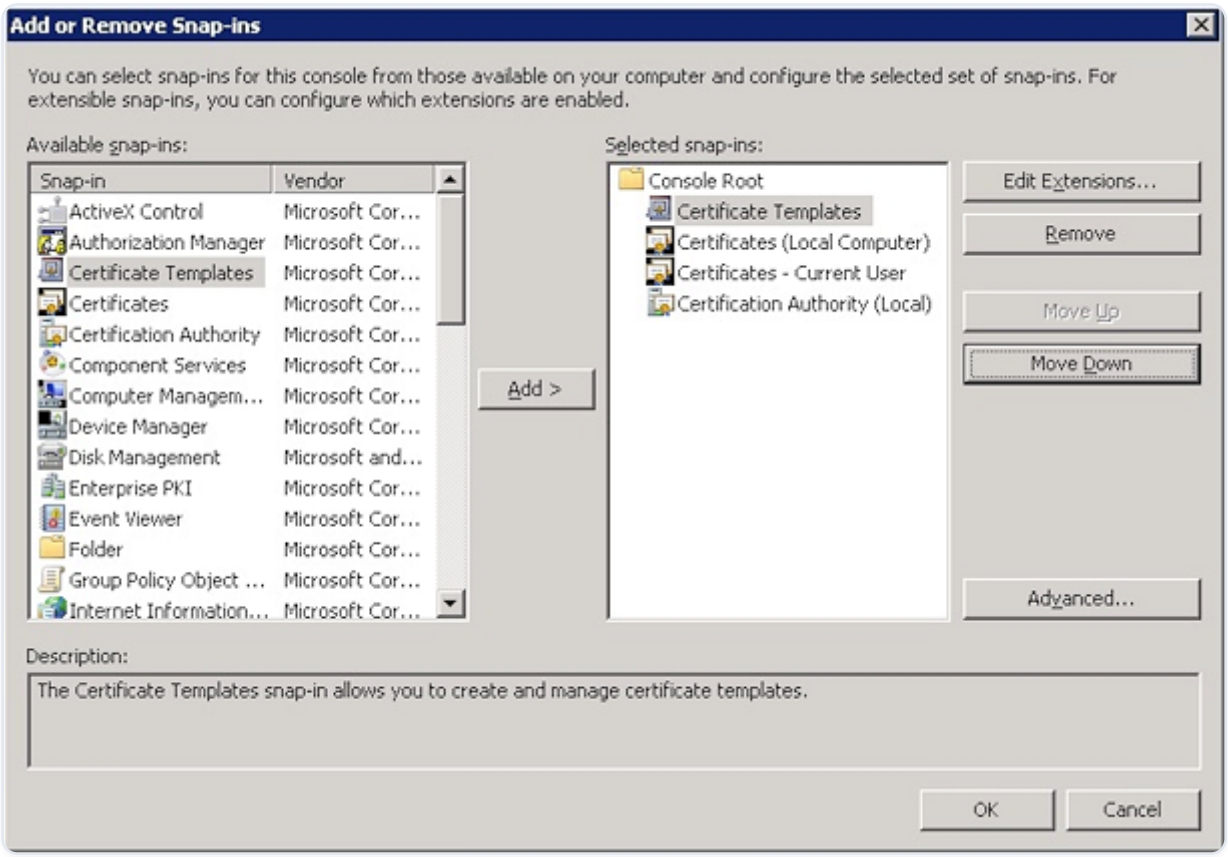
- 客户端身份验证
- SSL 配置文件基础结构
- 配置和绑定客户端证书身份验证策略。

先决条件

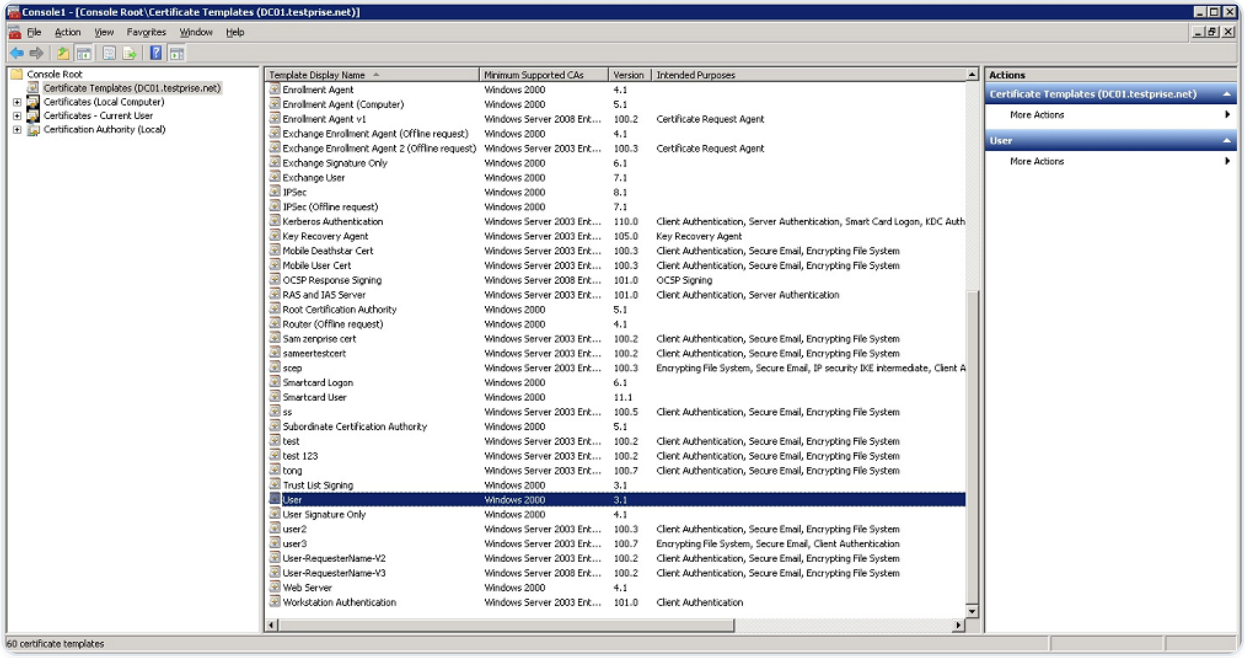
- 创建 Microsoft 证书服务实体模板时，请通过排除特殊字符来避免已注册设备可能出现的身份验证问题。例如，请勿在模板名称中使用以下字符：`: ! $ () # % + * ~ ? | {} []`
- 要为 Exchange ActiveSync 配置基于证书的身份验证，请参阅 Microsoft Exchange Server 文档。将 Exchange ActiveSync 的证书颁发机构 (CA) 服务器站点配置为要求客户端证书。
- 如果您使用私有服务器证书来保护 ActiveSync 到 Exchange Server 的流量，请确保移动设备具有所有根/中间证书。否则，在 Citrix Secure Mail 中设置邮箱期间，基于证书的身份验证将失败。在 Exchange IIS 控制台中，您必须：
  - 添加一个用于 Citrix Endpoint Management 与 Exchange 结合使用的网站，并绑定 Web 服务器证书。
  - 使用端口 9443。
  - 对于该网站，您必须添加两个应用程序，一个用于“Microsoft-Server-ActiveSync”，另一个用于“EWS”。对于这两个应用程序，在 **SSL 设置**下，选择**要求 SSL**。

将证书管理单元添加到 Microsoft 管理控制台

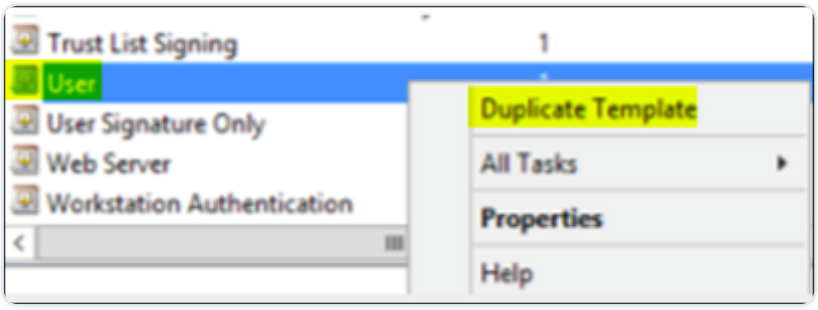
1. 打开控制台，然后单击**添加/删除管理单元**。
2. 添加以下管理单元：
   - 证书模板
   - 证书（本地计算机）
   - 证书 - 当前用户
   - 证书颁发机构（本地）



3. 展开 **证书模板**。



4. 选择 **用户** 模板并 **复制模板**。

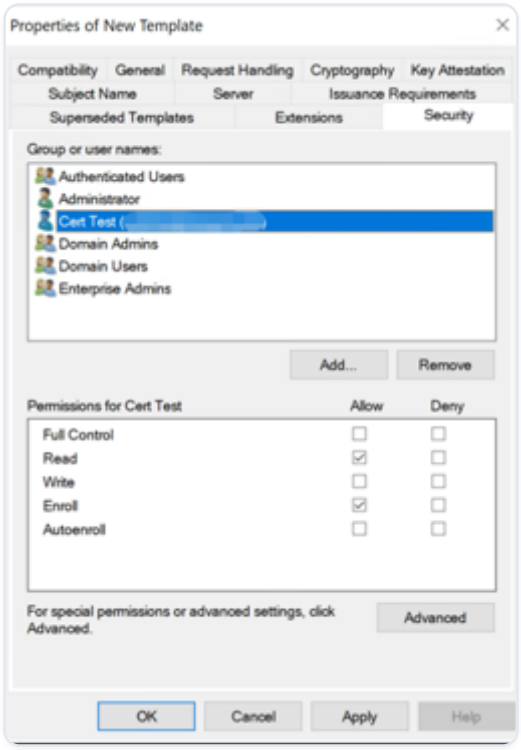


5. 提供模板显示名称。

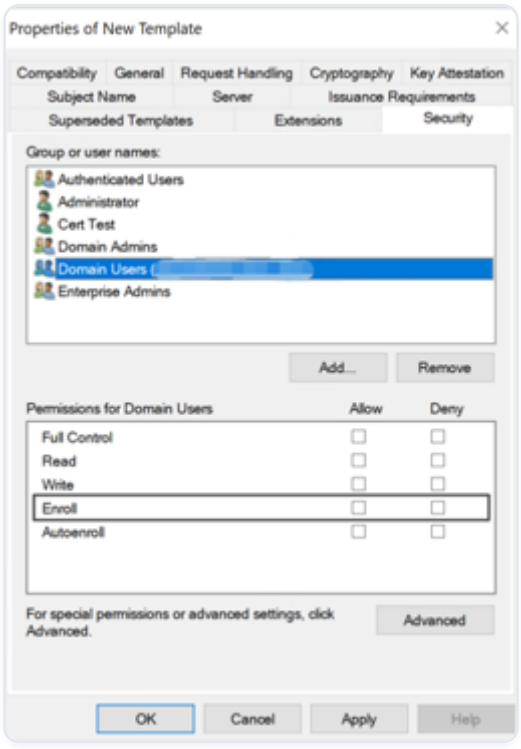
> **重要提示：**
>
> 不建议选择 **在 Active Directory 中发布证书** 选项。如果选择此选项，它会为 Active Directory 中的所有用户创建客户端证书，这可能会使您的 Active Directory 数据库变得混乱。

6. 对于模板类型，选择 **Windows 2003 Server**。在 Windows 2012 R2 服务器中，在 **兼容性** 下，选择 **证书颁发机构**，并将收件人设置为 **Windows 2003**。
7. 在 **安全性** 下，配置以下内容：
   a. 单击 **添加**，然后选择 Citrix Endpoint Management 用于生成证书的 AD 用户帐户。

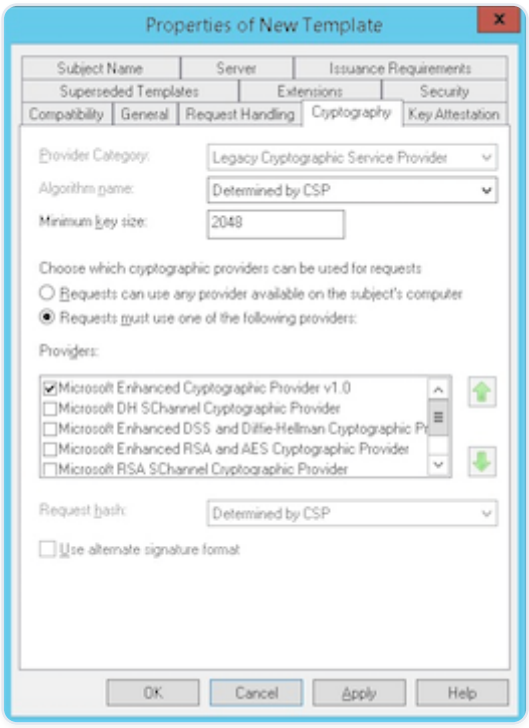
> **重要提示：**
>
> 此处仅添加服务帐户用户。仅向此 AD 用户帐户添加 **注册** 权限。
>
> 本文稍后将介绍如何使用服务帐户创建用户 .pfx 证书。有关信息，请参阅 从 CA 服务器创建 PFX 证书。



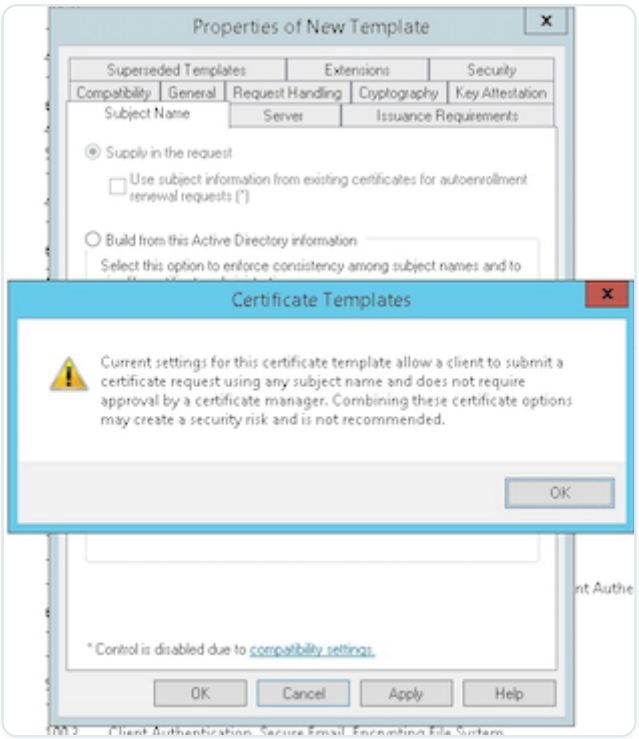
b. 从 **域用户** 撤销 **注册** 权限。



8. 在 **加密** 下，请确保提供密钥大小。您稍后将在 Citrix Endpoint Management 配置期间输入密钥大小。

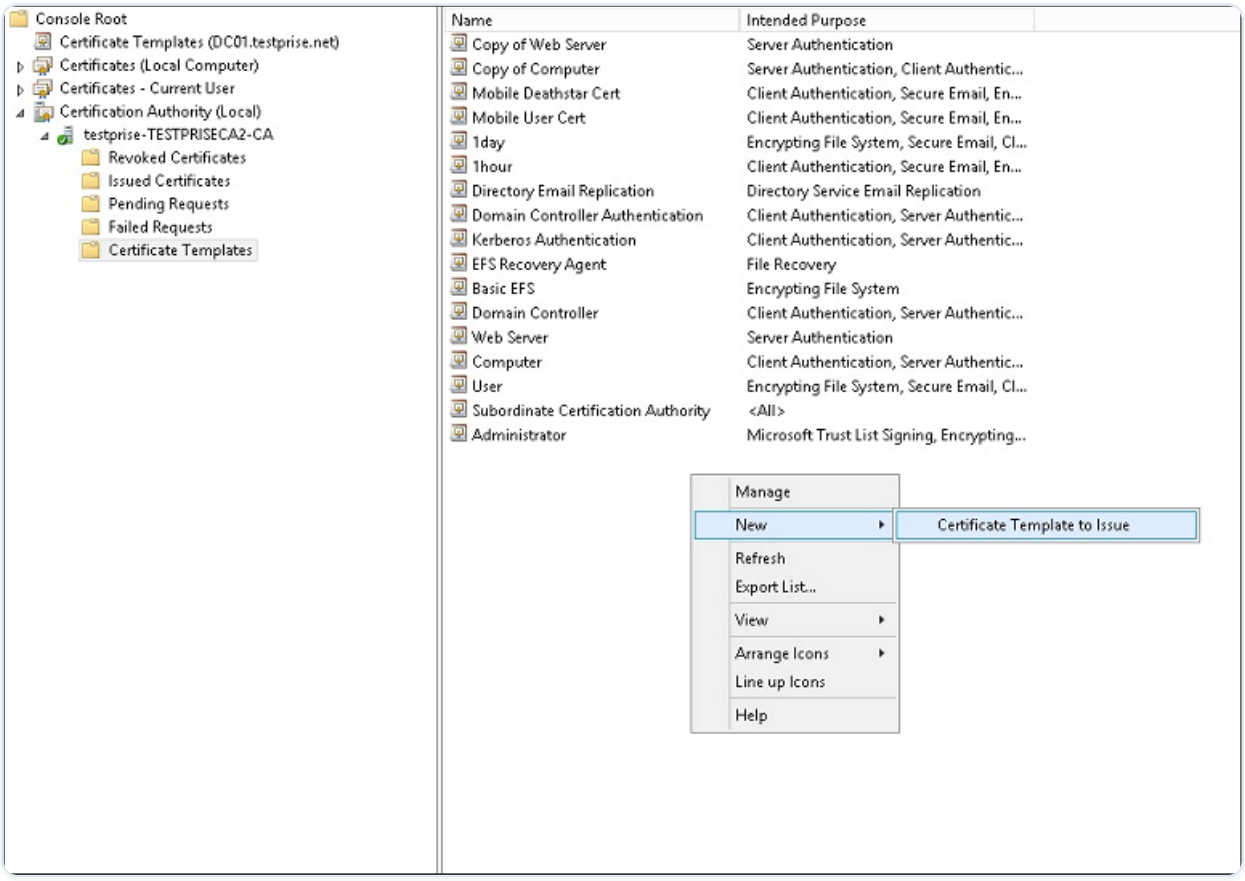


9. 在 **使用者名称** 下，选择 **在请求中提供**。应用更改，然后保存。

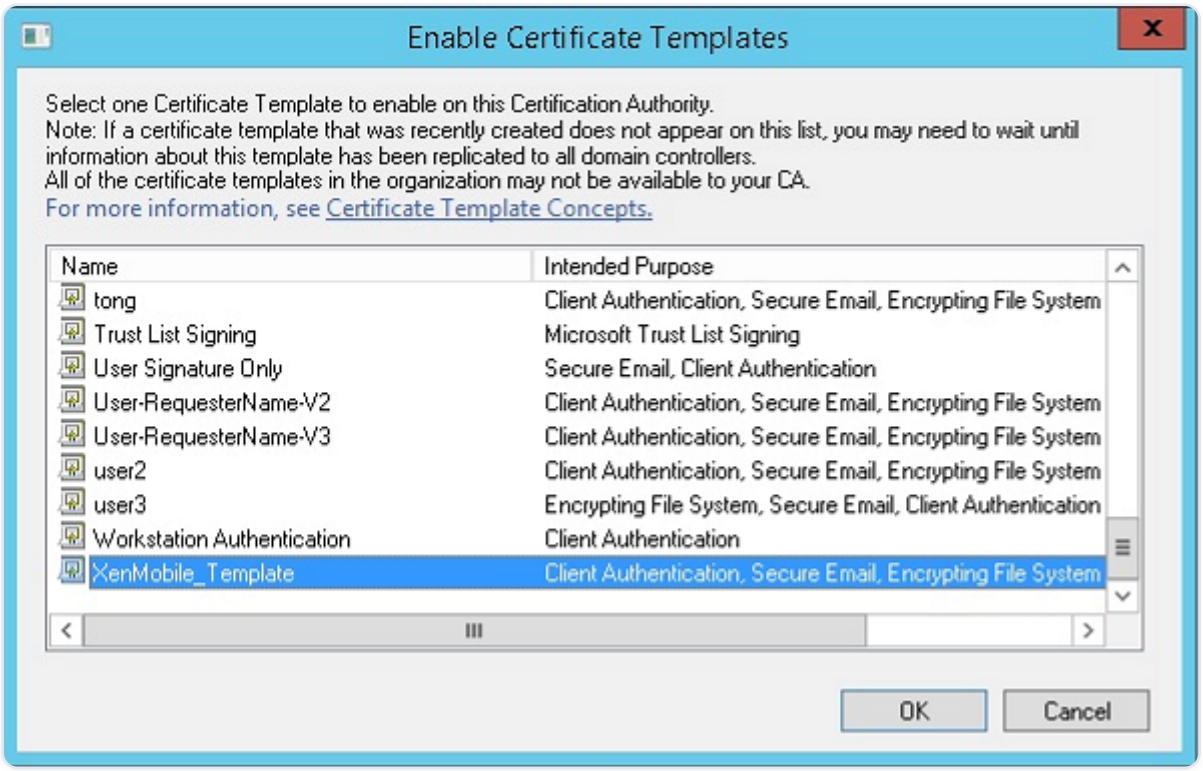


将模板添加到证书颁发机构

1. 转到 **证书颁发机构** 并选择 **证书模板**。
2. 右键单击右侧窗格，然后选择 **新建 > 要颁发的证书模板**。

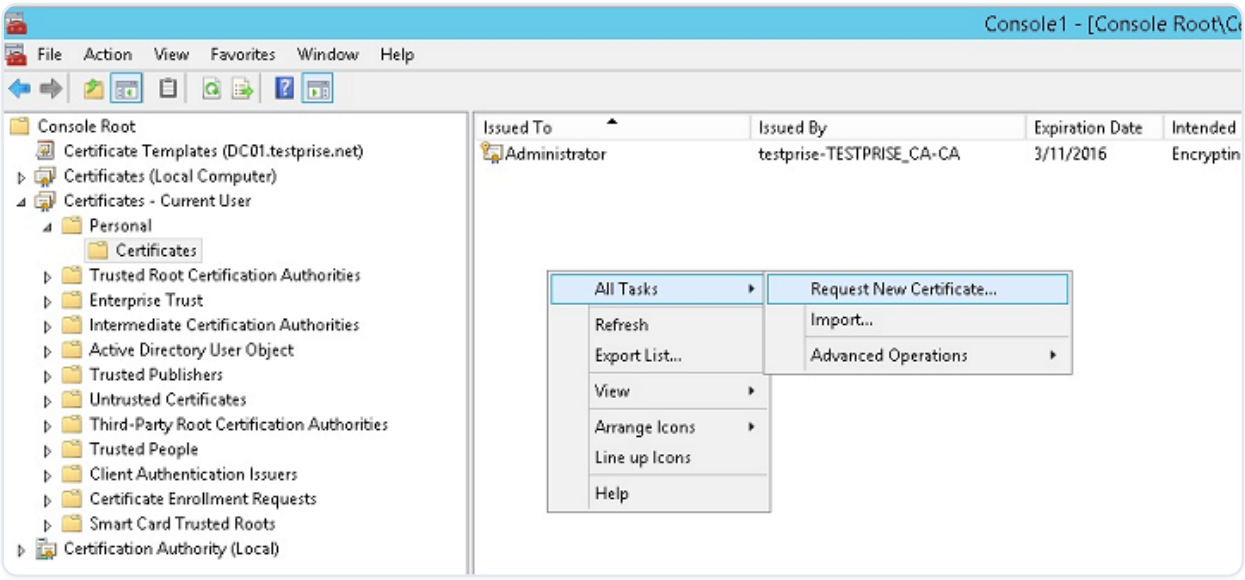


3. 选择您在上一步中创建的模板，然后单击 **确定** 将其添加到 **证书颁发机构**。

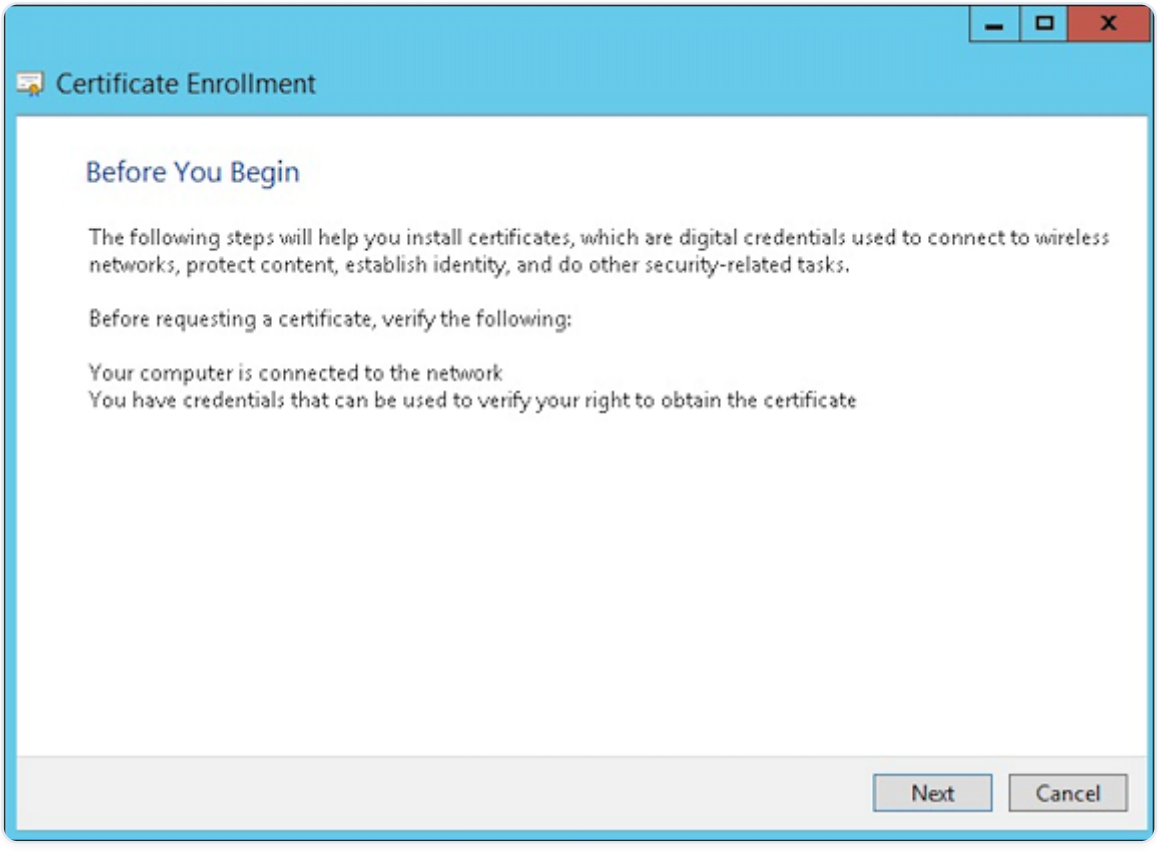


从 CA 服务器创建 PFX 证书

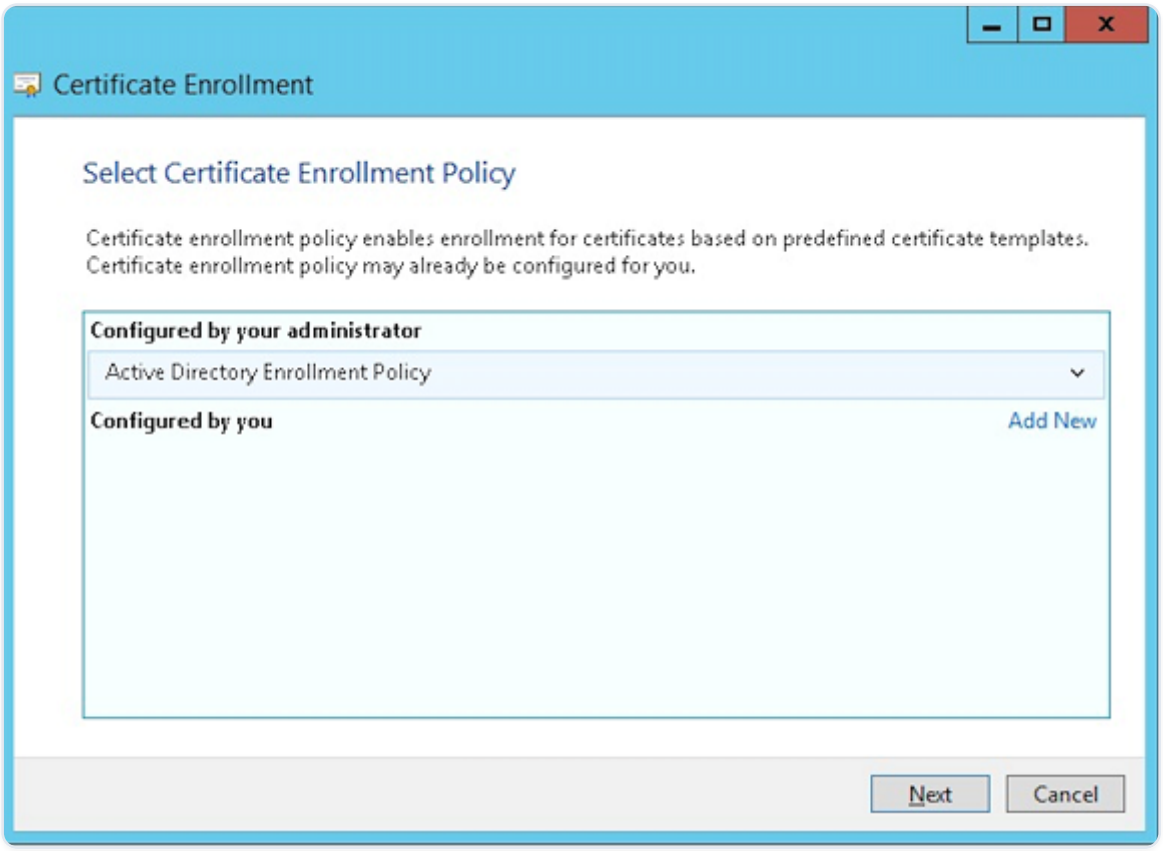
1. 使用您登录的服务帐户创建用户 .pfx 证书。.pfx 文件将上传到 Citrix Endpoint Management，然后 Citrix Endpoint Management 会为注册其设备的用户请求用户证书。
2. 在“**当前用户**”下，展开“**证书**”。
3. 右键单击右侧窗格，然后单击“**请求新证书**”。



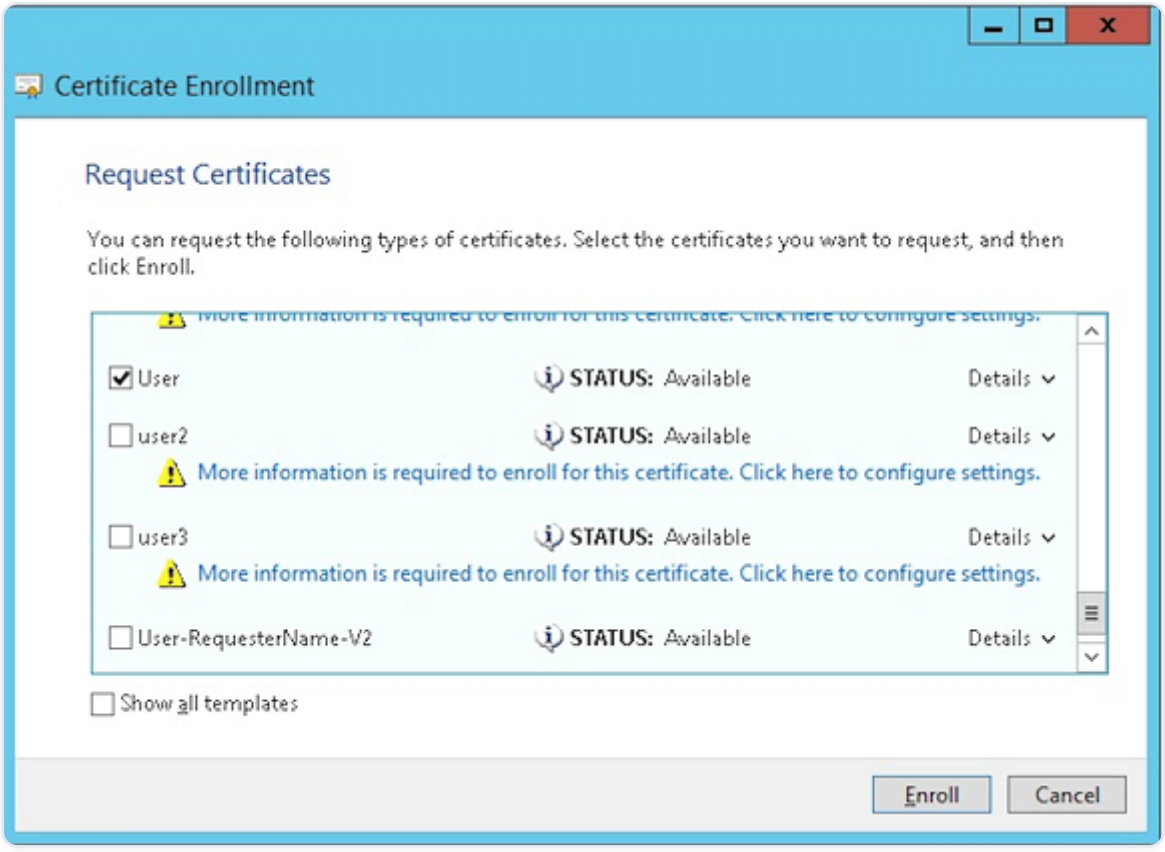
4. 此时将显示“**证书注册**”屏幕。单击“**下一步**”。



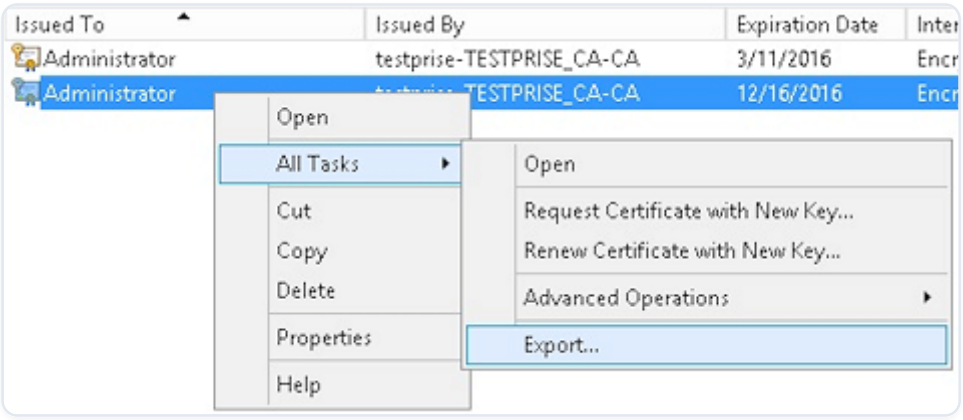
5. 选择“**Active Directory 注册策略**”，然后单击“**下一步**”。



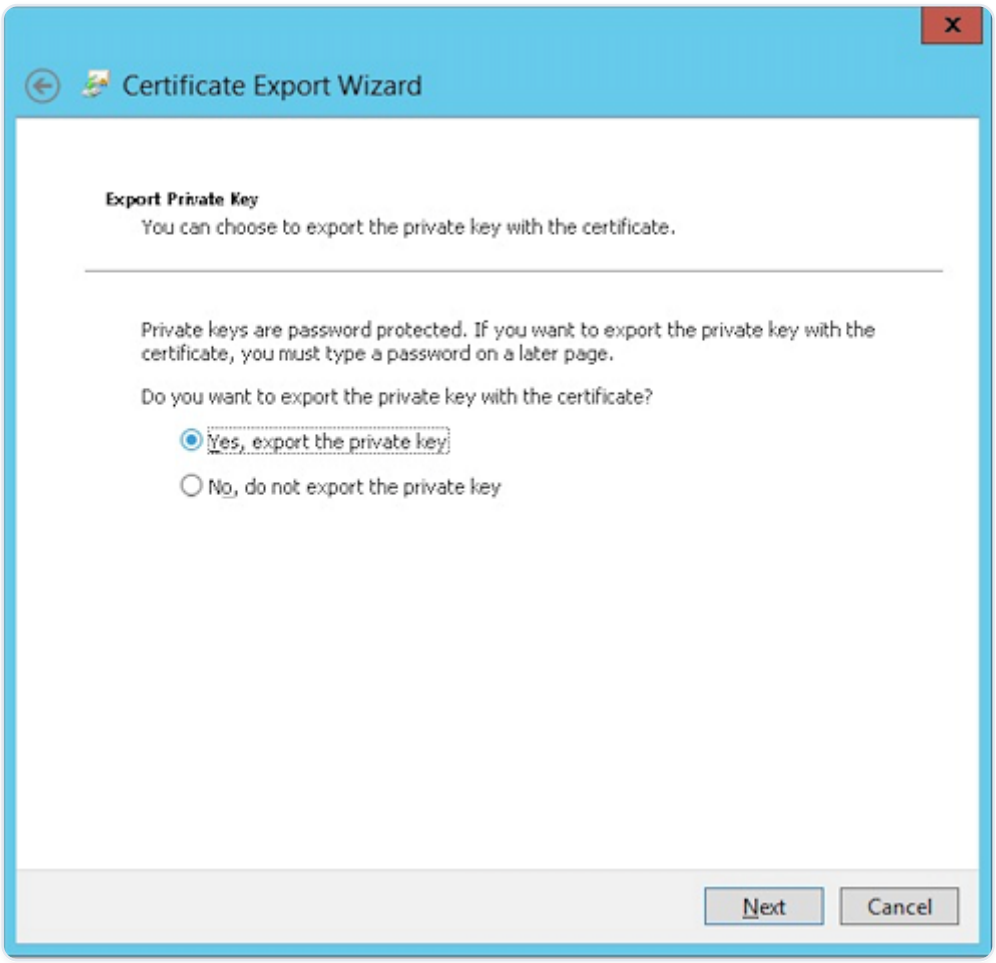
6. 选择“**用户**”模板，然后单击“**注册**”。



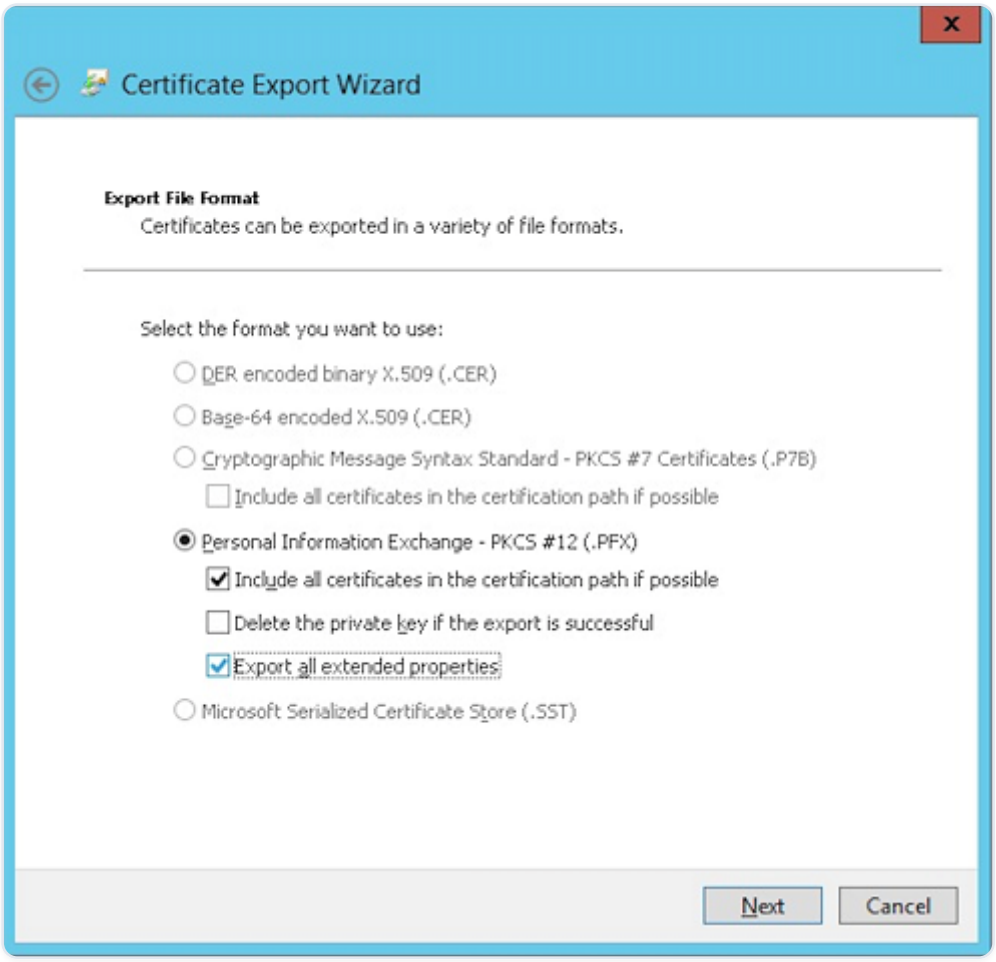
7. 导出您在上一步中创建的 .pfx 文件。



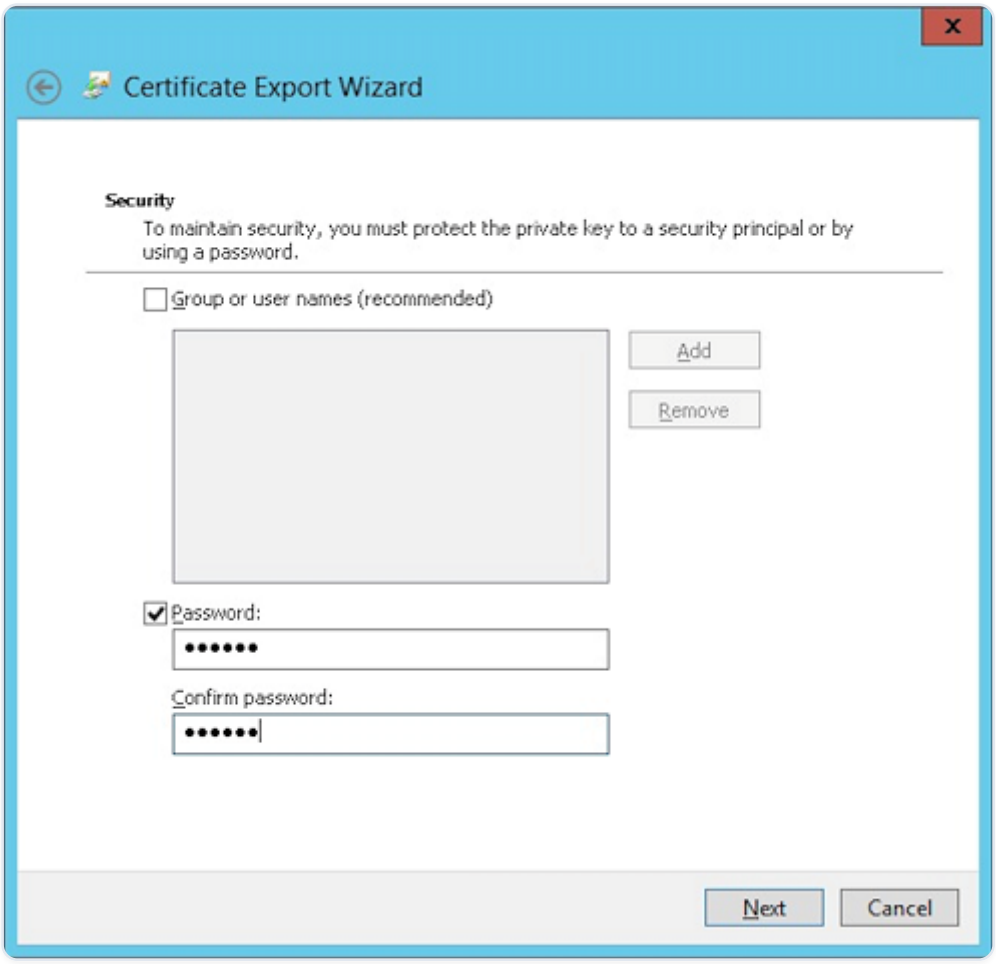
8. 单击“**是，导出私钥**”。



9. 选择“**如果可能，包括证书路径中的所有证书**”，并选中“**导出所有扩展属性**”复选框。



10. 设置一个密码，用于将此证书上传到 Citrix Endpoint Management 时使用。

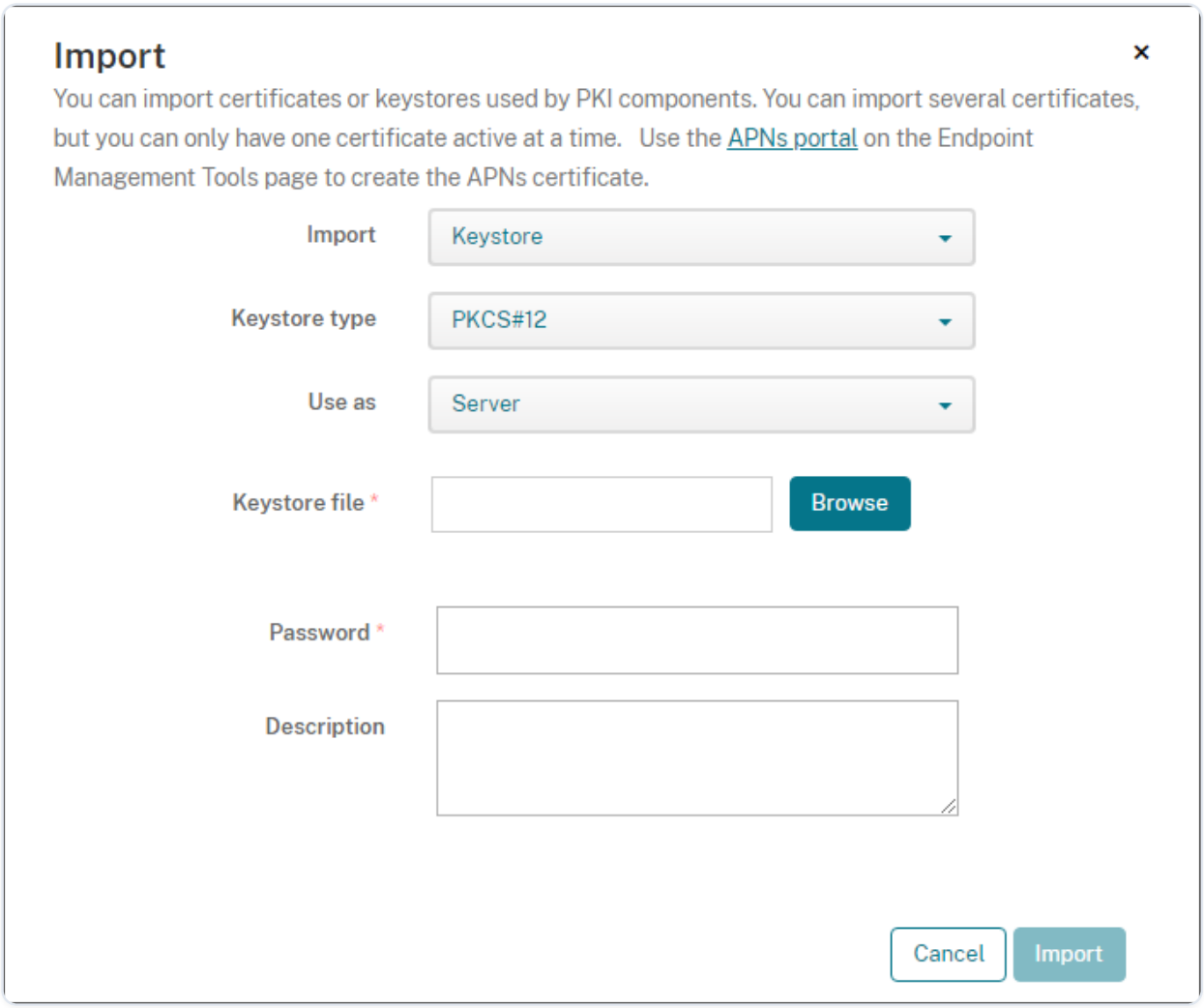


11. 将证书保存到硬盘。

将证书上传到 Citrix Endpoint Management

1. 在 Citrix 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. 单击“**证书**”，然后单击“**导入**”。
3. 输入以下参数：

    - **导入：**密钥库
    - **密钥库类型：**PKCS #12
    - **用途：**服务器
    - **密钥库文件：**单击“浏览”以选择您创建的 .pfx 证书。
    - **密码：**输入您为此证书创建的密码。



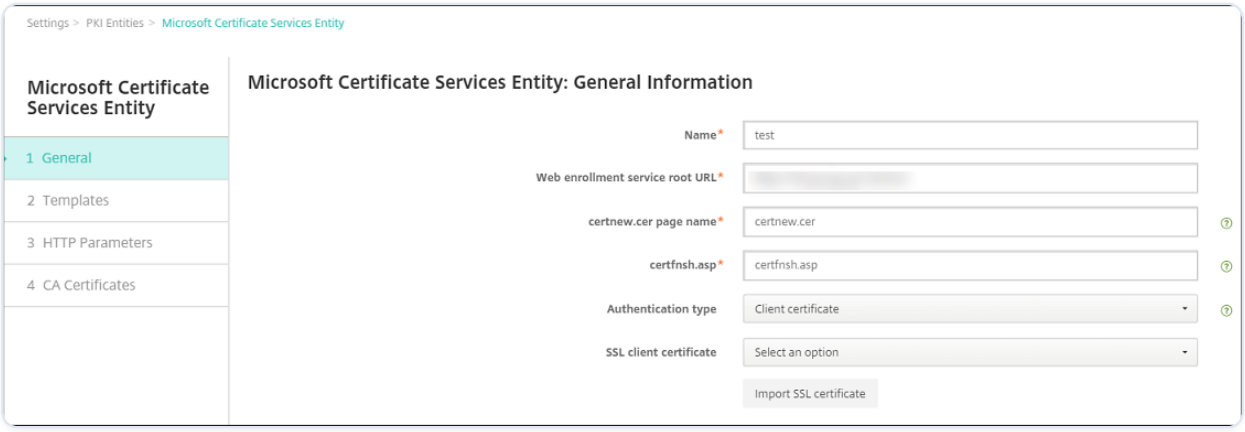
4. 单击 **Import**。
5. 验证证书是否正确安装。正确安装的证书将显示为用户证书。

为基于证书的身份验证创建 PKI 实体

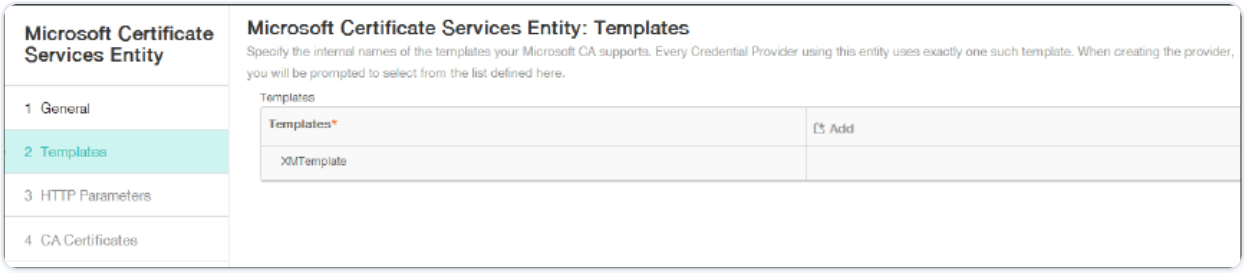
1. 在 **设置** 中，转至 **更多 > 证书管理 > PKI 实体**。
2. 单击 **添加**，然后单击 **Microsoft 证书服务实体**。此时将显示 **Microsoft 证书服务实体: 常规信息** 屏幕。
3. 输入以下参数：

   - **名称：** 键入任何名称。
   - **Web 注册服务根 URL：** `https://RootCA-URL/certsrv/`（请务必在 URL 路径中添加最后一个斜杠 /。）
   - **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

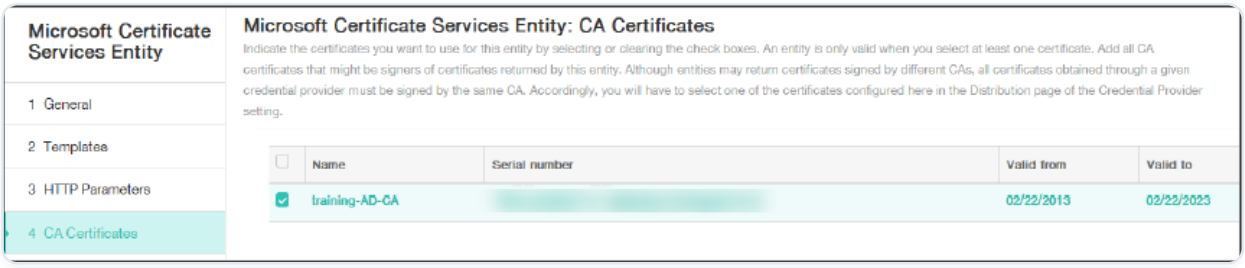
- **SSL 客户端证书：** 选择用于颁发 Citrix Endpoint Management 客户端证书的用户证书。如果不存在证书，请按照上一节中的过程上载证书。



4. 在 **模板** 下，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 是从 Citrix Endpoint Management 客户端证书导入的链的一部分。



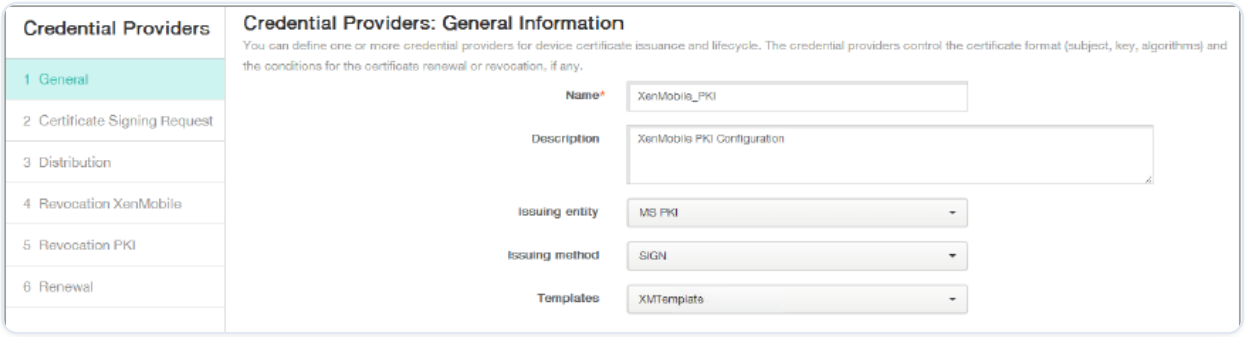
7. 点击 **保存**。

配置凭据提供程序

1. 在**设置**中，转到**更多 > 证书管理 > 凭据提供程序**。
2. 单击 **添加**。
3. 在**常规**下，输入以下参数：

- **名称：**键入任何名称。
- **描述：**键入任何描述。

- **颁发实体：**选择之前创建的 PKI 实体。
- **颁发方法：**SIGN
- **模板：**选择在 PKI 实体下添加的模板。

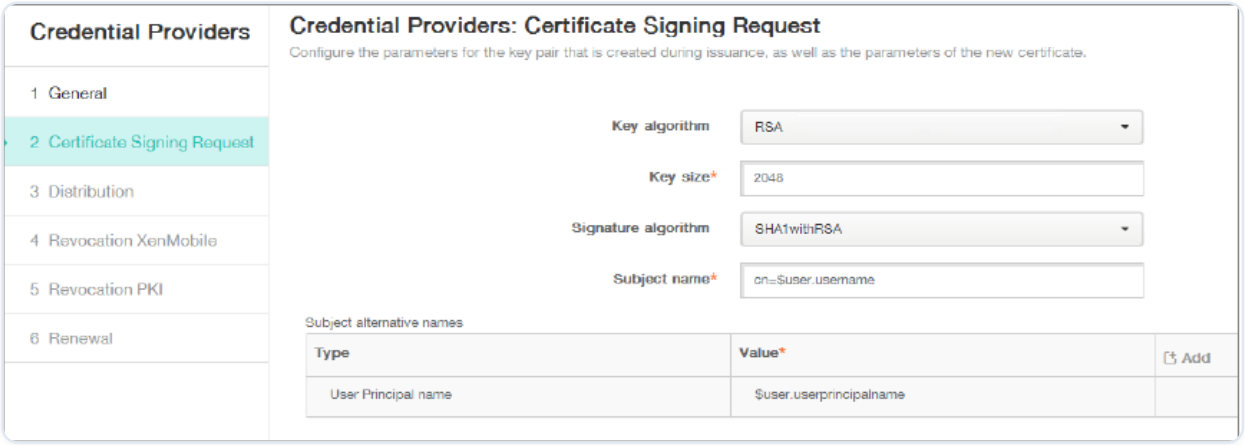


4. 单击**证书签名请求**，然后输入以下参数：

- **密钥算法：**RSA
- **密钥大小：**2048
- **签名算法：**SHA256withRSA
- **主题名称：**`cn=$user.username`

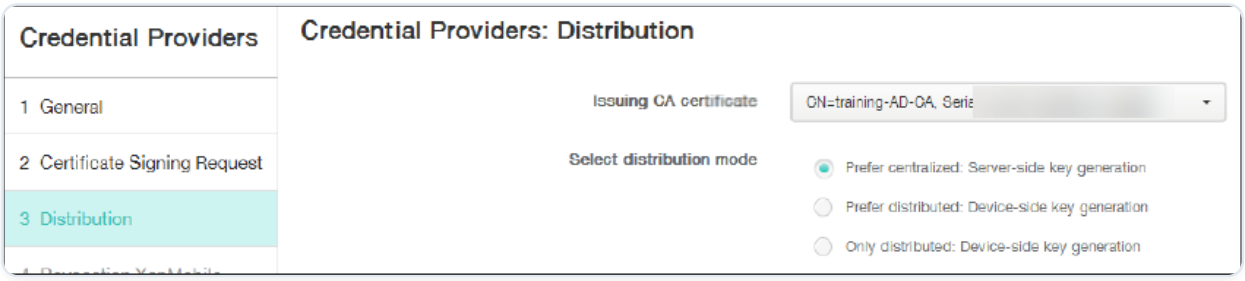
对于 **主题备用名称**，单击 **添加**，然后输入以下参数：

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

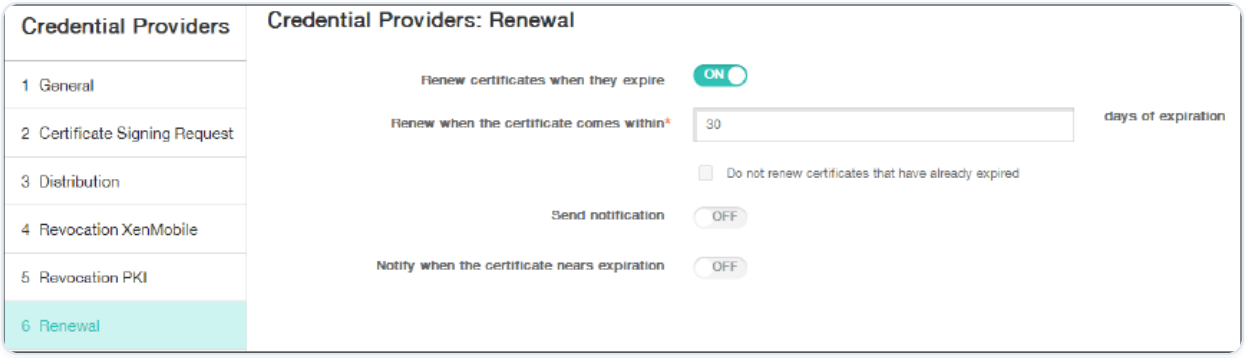


5. 单击 **分发**，然后输入以下参数：

- **颁发 CA 证书：** 选择签署 Citrix 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**。



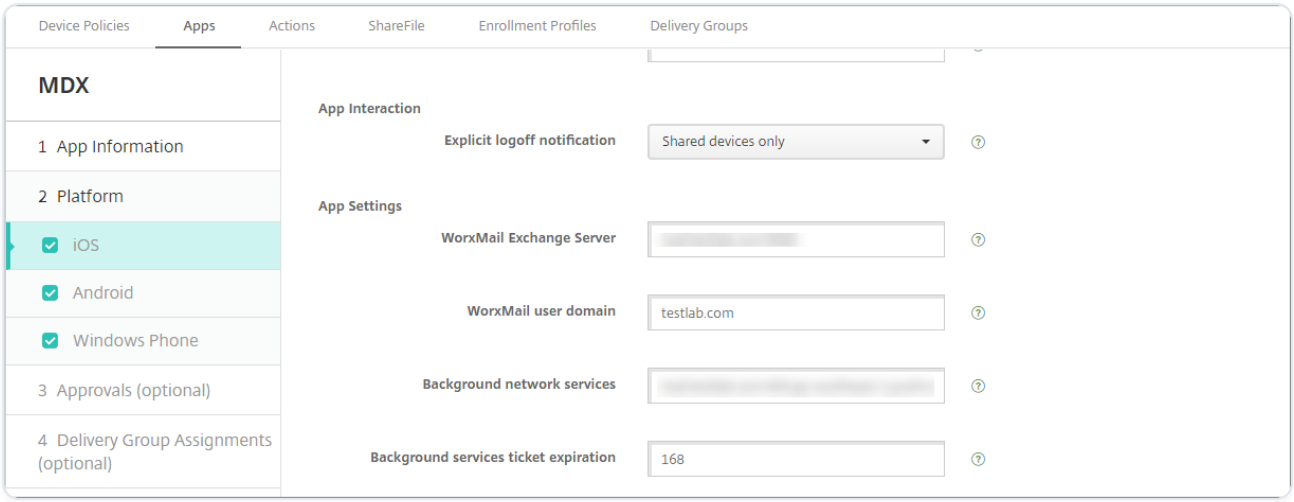
6. 对于接下来的两个部分（**吊销 Citrix Endpoint Management** 和 **吊销 PKI**），根据需要设置参数。在此示例中，这两个选项都已跳过。
7. 单击 **续订**。
8. 启用 **在证书过期时续订**。
9. 将所有其他设置保留为默认值，或根据需要进行更改。



10. 点击 **保存**。

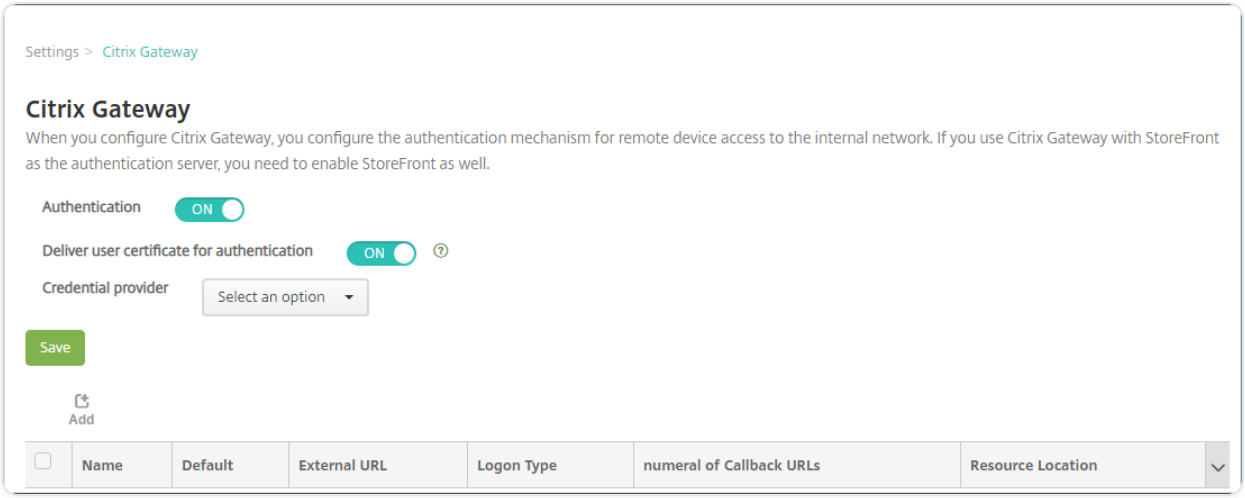
配置 Citrix Secure Mail 以使用基于证书的身份验证

将 Citrix Secure Mail 添加到 Citrix Endpoint Management 时，请务必在 **应用程序设置** 下配置 Exchange 设置。

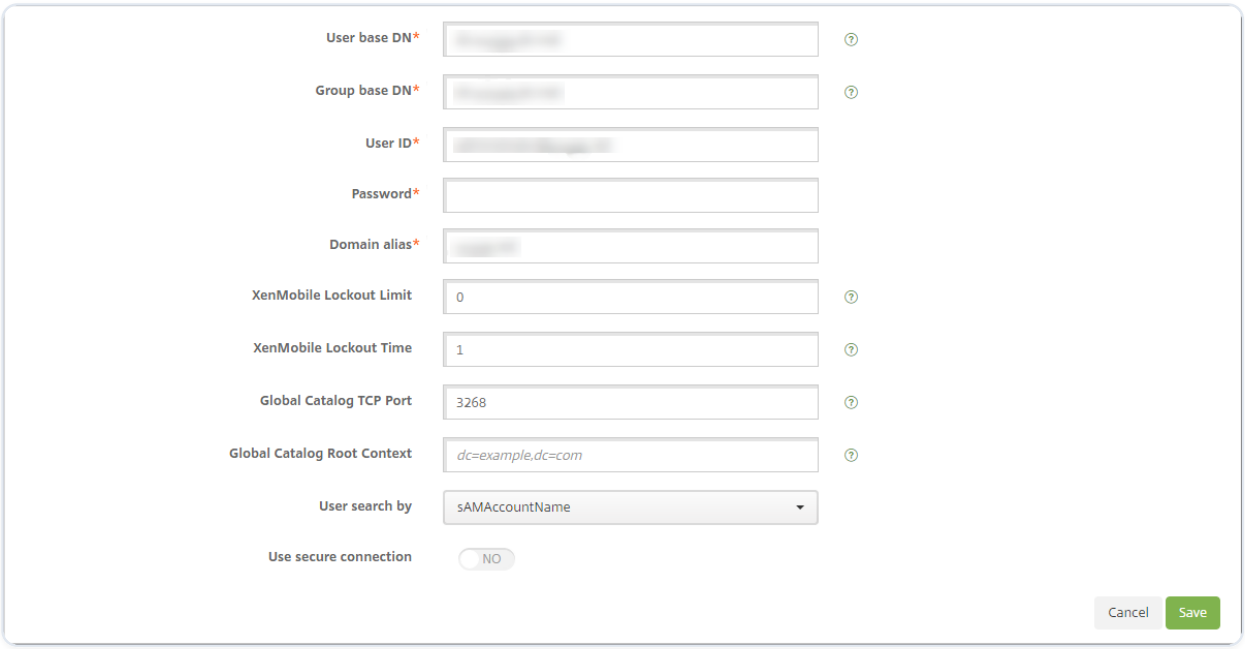


在 Citrix Endpoint Management 中配置 NetScaler Gateway 证书交付

1. 在 Citrix 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，单击“**NetScaler Gateway**”。
3. 如果尚未添加 NetScaler 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
   - **设为默认值：** 开
4. 对于“**身份验证**”和“**交付用户证书以进行身份验证**”，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. 若要使用用户证书中的 sAMAccount 属性作为用户主体名称 (UPN) 的替代项，请在 Citrix Endpoint Management 中按如下方式配置 LDAP 连接器：转到“**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** 并选择以下复选框：**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。

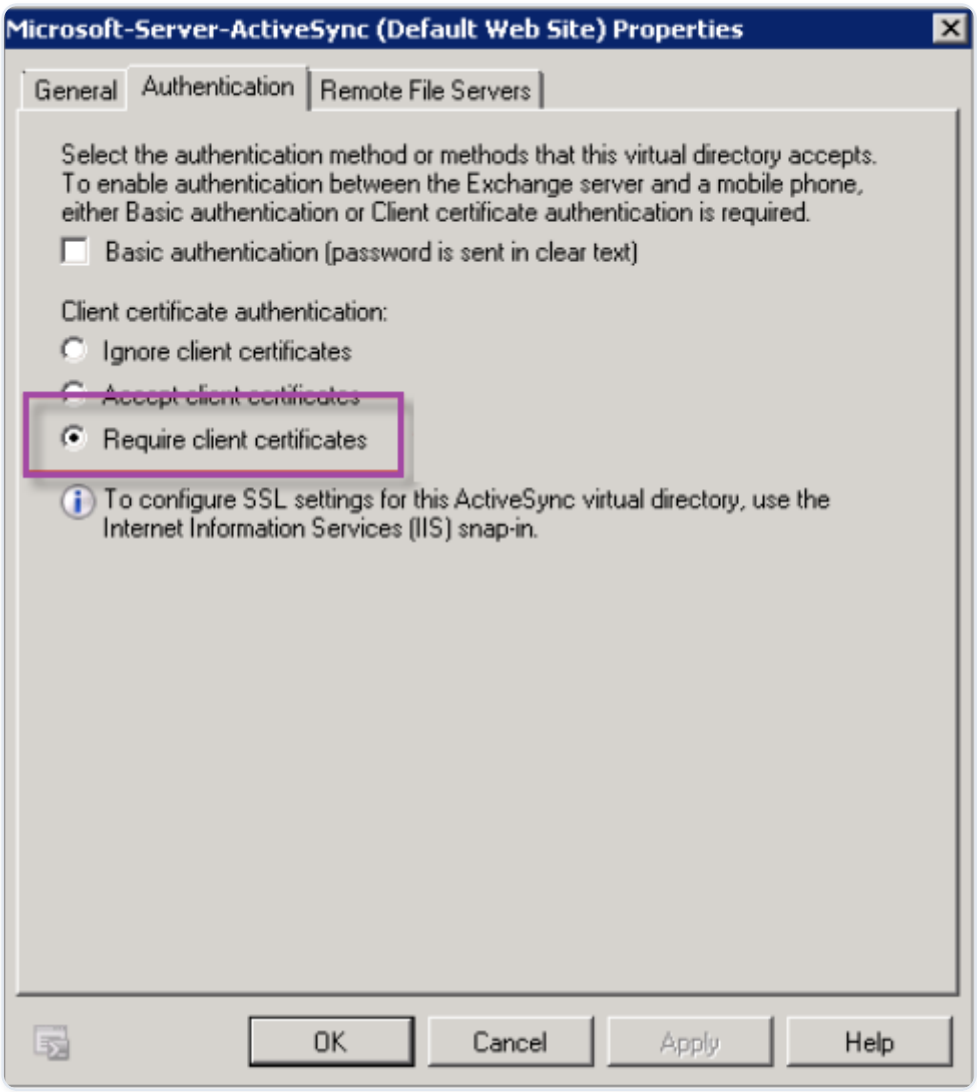
客户端证书配置故障排除

在成功配置上述配置以及 NetScaler Gateway 配置后，用户工作流程如下：

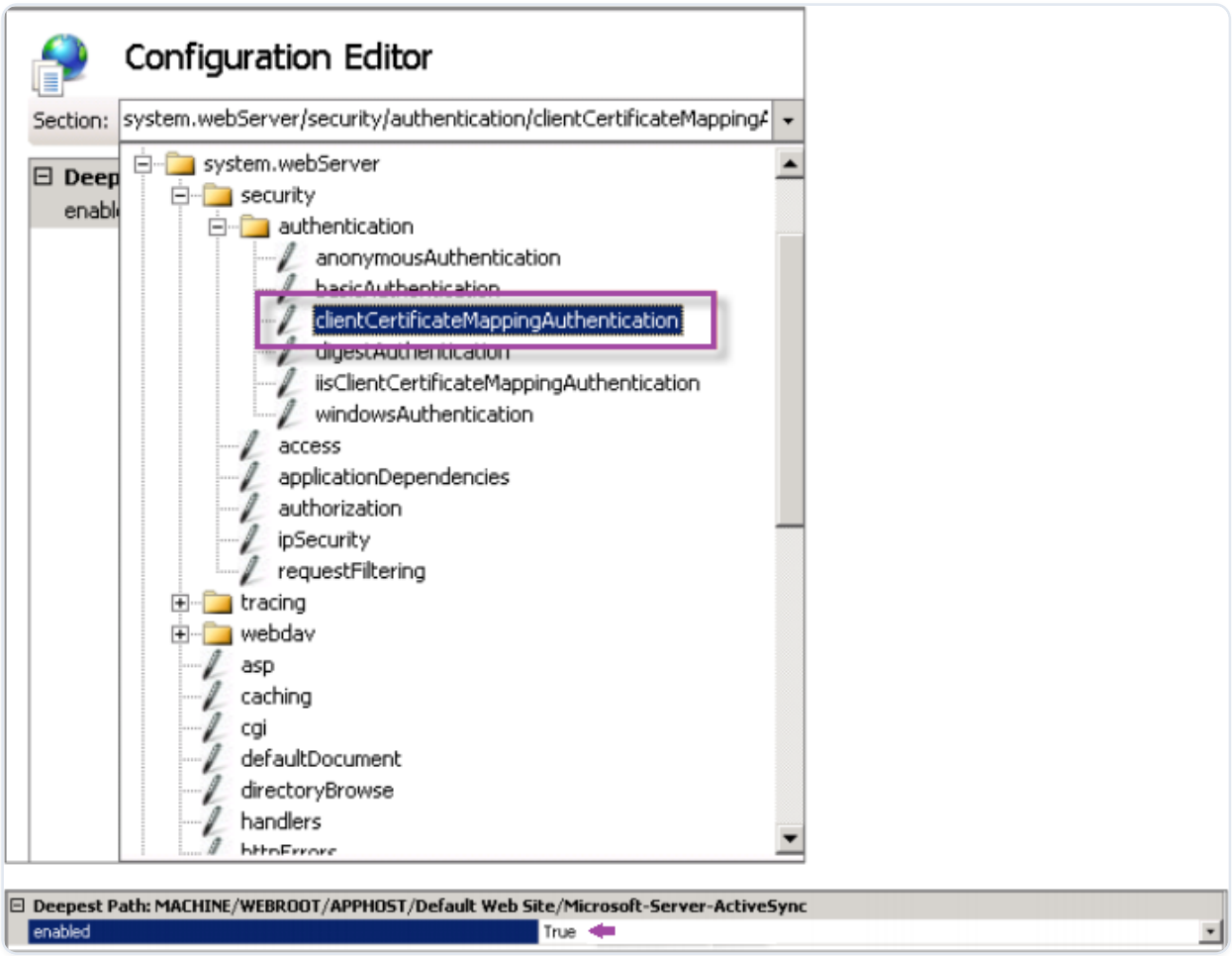
1. 用户注册其移动设备。
2. Citrix Endpoint Management 提示用户创建 Citrix PIN。
3. 然后，用户将被重定向到应用商店。
4. 当用户启动 Citrix Secure Mail 时，Citrix Endpoint Management 不会提示他们输入邮箱配置的用户凭据。相反，Citrix Secure Mail 会从 Citrix Secure Hub 请求客户端证书，并将其提交给 Microsoft Exchange Server 进行身份验证。如果用户启动 Citrix Secure Mail 时 Citrix Endpoint Management 提示输入凭据，请检查您的配置。

如果用户可以下载并安装 Citrix Secure Mail，但在邮箱配置期间 Citrix Secure Mail 未能完成配置：

1. 如果 Microsoft Exchange Server ActiveSync 使用私有 SSL 服务器证书来保护流量，请验证移动设备上是否安装了根/中间证书。
2. 验证为 ActiveSync 选择的身份验证类型是否设置为 **需要客户端证书**。



3. 在 Microsoft Exchange Server 上，检查 **Microsoft-Server-ActiveSync** 站点以验证是否启用了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是禁用的。该选项位于 **配置编辑器 > 安全 > 身份验证** 下。



选择 **True** 后，请务必单击 **Apply** 以使更改生效。

4. 检查 Citrix Endpoint Management 控制台中的 NetScaler Gateway 设置：确保“**Deliver user certificate for authentication**”为“**On**”，并且“**Credential provider**”已选择正确的配置文件。

确定客户端证书是否已交付到移动设备

1. 在 Citrix 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，然后搜索此条目：

   NetScaler Gateway 凭据：请求的凭据，CertId=

验证是否已启用客户端证书协商

1. 运行此 `netsh` 命令以显示绑定到 IIS 网站的 SSL 证书配置：

   ```
   netsh http show sslcert
   ```

2. 如果“**Negotiate Client Certificate**”的值为“**Disabled**”，请运行以下命令以启用它：

   ```
   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=23498dfsdfhaf98rhkjqf9823rkjhdasf98asfk appid={123asd456jd-a12b-3c45-
d678-123456lkjhgf} certstorename=ExampleCertStoreName
verifyclientcertrevocation=Enable
VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable
clientcertnegotiation=Enable
```

如果无法通过 Citrix Endpoint Management 将根/中间证书交付到 Windows Phone 8.1 设备：

- 通过电子邮件将根/中间证书 (.cer) 文件发送到 Windows Phone 8.1 设备并直接安装它们。

如果 Citrix Secure Mail 未能成功安装在 Windows Phone 8.1 上，请验证以下内容：

- 应用程序注册令牌 (.AETX 文件) 通过 Citrix Endpoint Management 使用企业中心设备策略进行交付。
- 应用程序注册令牌是使用与用于包装 Citrix Secure Mail 和签署 Citrix Secure Hub 应用程序的证书提供商相同的企业证书创建的。
- 相同的发布者 ID 用于签名和封装 Citrix Secure Hub、Citrix Secure Mail 和应用程序注册令牌。

PKI 实体

Citrix Endpoint Management 公钥基础设施 (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。这些组件可以是 Citrix Endpoint Management 内部的，也可以是外部的。内部组件称为酌情组件。外部组件是企业基础架构的一部分。

Citrix Endpoint Management 支持以下类型的 PKI 实体：

- Microsoft 证书服务
- 酌情证书颁发机构 (CA)

Citrix Endpoint Management 支持以下 CA 服务器：

- Windows 服务器 2016
- Windows 服务器 2019

- Windows 服务器 2022

> **注意：**

> Windows Server 2012 R2、2012 和 2008 R2 已达到生命周期终止，因此不再受支持。有关详细信息，请参阅 Microsoft 产品生命周期文档。

常见 PKI 概念

无论其类型如何，每个 PKI 实体都具有以下功能的子集：

- **签名：** 基于证书签名请求 (CSR) 颁发新证书。
- **获取：** 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 Citrix Endpoint Management 指明哪个 CA 证书是该实体颁发（或恢复）的证书的签名者。该 PKI 实体可以返回由任意数量的不同 CA 签名的（已获取或新签名的）证书。

将这些机构的每个证书作为 PKI 实体配置的一部分提供。为此，请将证书上传到 Citrix Endpoint Management，然后在 PKI 实体中引用它们。对于酌情 CA，证书隐式为签名 CA 证书。对于外部实体，必须手动指定证书。

> **重要提示：**

> 创建 Microsoft 证书服务实体模板时，请避免已注册设备可能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

Citrix Endpoint Management 通过其 Web 注册界面与 Microsoft 证书服务进行交互。Citrix Endpoint Management 仅支持通过该界面颁发新证书。如果 Microsoft CA 生成 NetScaler Gateway 用户证书，则 NetScaler Gateway 支持这些证书的续订和吊销。

要在 Citrix 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，请使用 SSL 客户端身份验证来保护 Citrix Endpoint Management 与证书服务 Web 界面之间的连接。

添加 Microsoft 证书服务实体

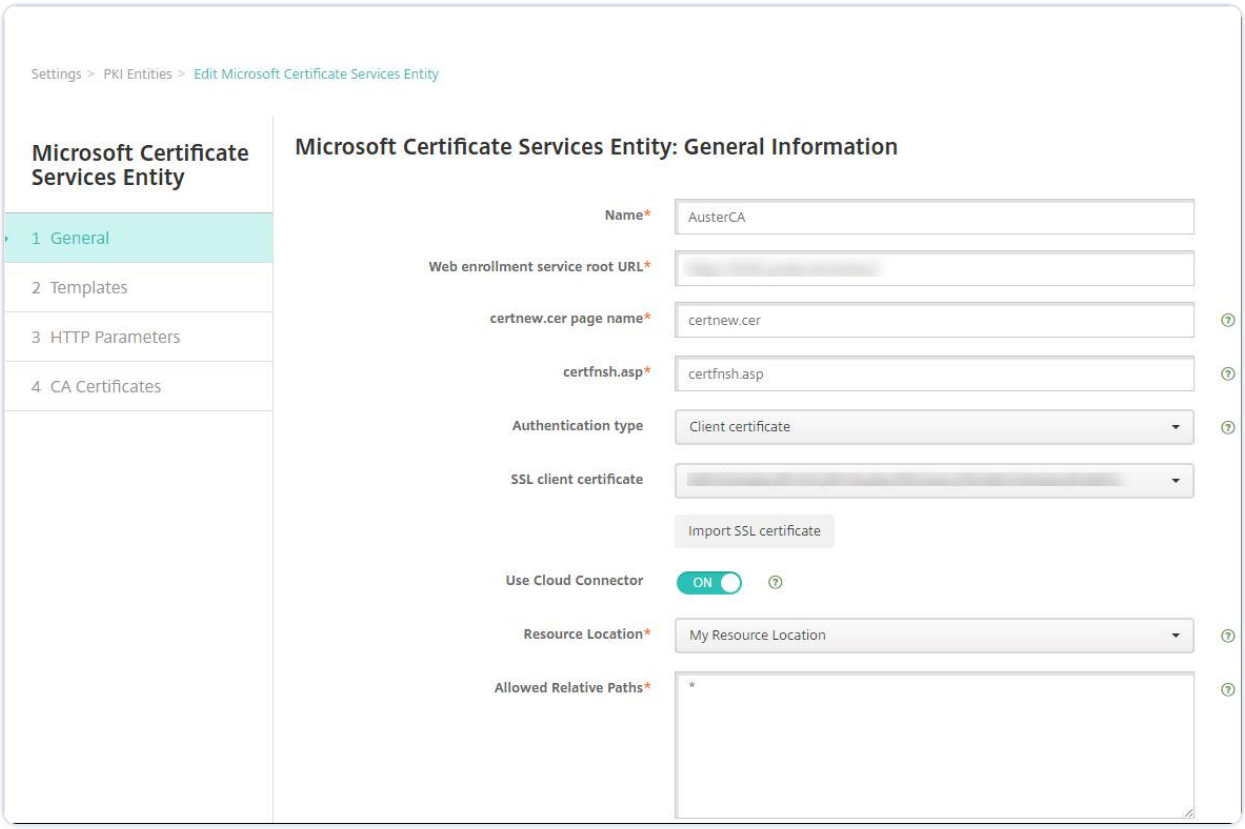
1. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标，然后单击 **PKI 实体**。
2. 在 **PKI 实体** 页面上，单击 **添加**。

   将显示 PKI 实体类型菜单。
3. 单击 **Microsoft 证书服务实体**。

   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：

   - **名称：** 键入新实体的名称，以后将使用该名称引用该实体。实体名称必须是唯一的。
   - **Web 注册服务根 URL：** 键入 Microsoft CA Web 注册服务的基 URL。例如：`https://192.0.0.1/certsrv/`。该 URL 可以使用纯 HTTP 或基于 SSL 的 HTTP。
   - **certnew.cer 页面名称：** certnew.cer 页面的名称。除非您因某种原因已将其重命名，否则请使用默认名称。
   - **certfnsh.asp：** certfnsh.asp 页面的名称。除非您因某种原因已将其重命名，否则请使用默认名称。
   - **身份验证类型：** 选择要使用的身份验证方法。
     - **无**
     - **HTTP 基本：** 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**”以使用 Cloud Connector 连接到 PKI 服务器。然后，为连接指定“**资源位置**”和“**允许的相对路径**”。
     - **资源位置：** 从 Citrix Cloud Connector 中定义的资源位置中选择。
     - **允许的相对路径：** 指定资源位置允许的相对路径。每行指定一个路径。可以使用星号 (*) 通配符。

       假设资源位置为 `https://www.ServiceRoot/certsrv`。要提供对该路径中所有 URL 的访问权限，请在“**允许的相对路径**”中输入 `/*`。



5. 单击“**测试连接**”以确保服务器可访问。如果不可访问，将显示一条消息，指出连接失败。检查您的配置设置。
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，您可以指定 Microsoft CA 支持的模板的内部名称。创建凭据提供程序时，您可以从此处定义的列表中选择一个模板。使用此实体的每个凭据提供程序都只使用一个此类模板。

   有关 Microsoft 证书服务模板要求，请参阅您的 Microsoft 服务器版本的 Microsoft 文档。Citrix Endpoint Management 对其分发的证书没有要求，但 证书 中注明的证书格式除外。
7. 在“**Microsoft 证书服务实体: 模板**”页面上，单击“**添加**”，键入模板名称，然后单击“**保存**”。对要添加的每个模板重复此步骤。
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 Citrix Endpoint Management 要添加到 Microsoft Web 注册界面的 HTTP 请求中的自定义参数。自定义参数仅对在 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**”。

   出现 **Microsoft 证书服务实体：CA 证书** 页面。在此页面上，您必须告知 Citrix Endpoint Management 系统通过此实体获取的证书的签名者。当您的 CA 证书续订时，请在 Citrix

Endpoint Management 中更新它。Citrix Endpoint Management 会透明地将更改应用于该实体。

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. 点击 **保存**。

该实体显示在 PKI 实体表中。

NetScaler Gateway 证书吊销列表 (CRL)

Citrix Endpoint Management 仅支持第三方证书颁发机构的证书吊销列表 (CRL)。如果您配置了 Microsoft CA，Citrix Endpoint Management 将使用 NetScaler Gateway 来管理吊销。

配置基于客户端证书的身份验证时，请考虑是否配置 NetScaler Gateway 证书吊销列表 (CRL) 设置 **启用 CRL 自动刷新**。此步骤可确保处于仅 MAM 模式的设备用户无法使用设备上的现有证书进行身份验证。

Citrix Endpoint Management 会重新颁发新证书，因为它不限制用户在证书被吊销后生成用户证书。当 CRL 检查过期的 PKI 实体时，此设置会提高 PKI 实体的安全性。

自由裁量 CA

当您向 Citrix Endpoint Management 提供 CA 证书和关联的私钥时，将创建一个自由裁量 CA。Citrix Endpoint Management 根据您指定的参数在内部处理证书颁发、吊销和状态信息。

配置自由裁量 CA 时，您可以为该 CA 激活联机证书状态协议 (OCSP) 支持。如果启用 OCSP 支持，CA 会将扩展 `id-pe-authorityInfoAccess` 添加到 CA 颁发的证书中。该扩展指向以下位置的 Citrix Endpoint Management 内部 OCSP 响应程序：

`https://<server>/<instance>/ocsp`

配置 OCSP 服务时，请为相关自由裁量实体指定 OCSP 签名证书。您可以将 CA 证书本身用作签名者。为避免不必要地暴露您的 CA 私钥（建议）：创建由 CA 证书签名的委托 OCSP 签名证书，并包含此扩展：`id-kp-OCSPSigning extendedKeyUsage`。

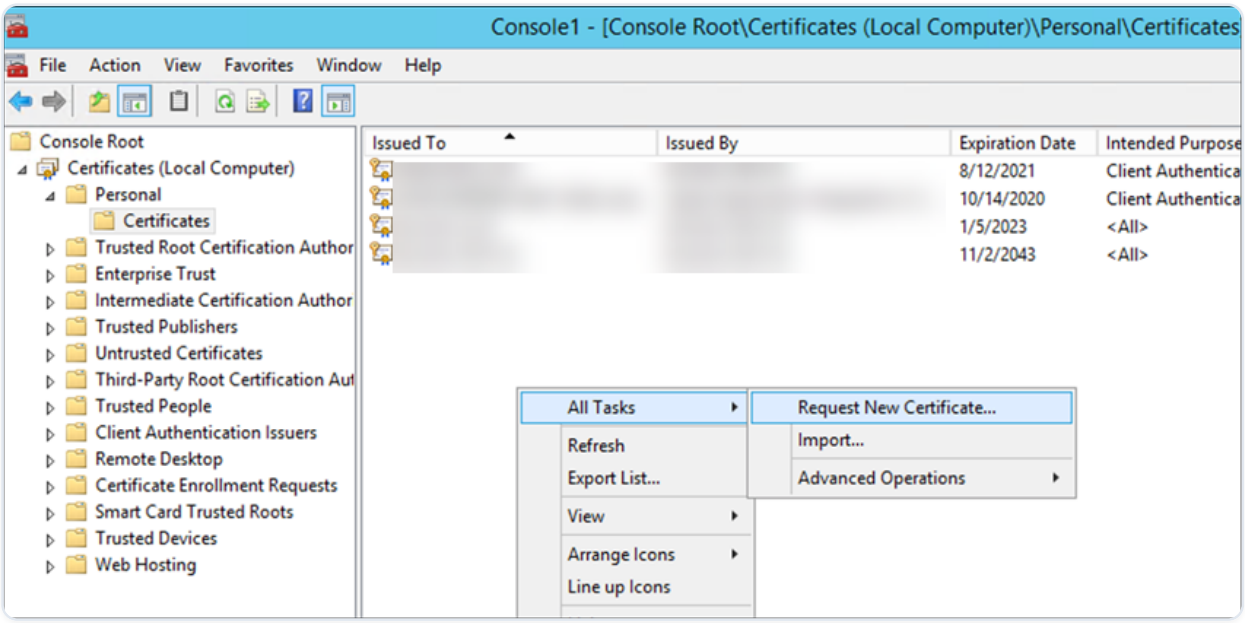
Citrix Endpoint Management OCSP 响应程序服务支持基本的 OCSP 响应以及请求中的以下哈希算法：

- SHA-256
- SHA-384
- SHA-512

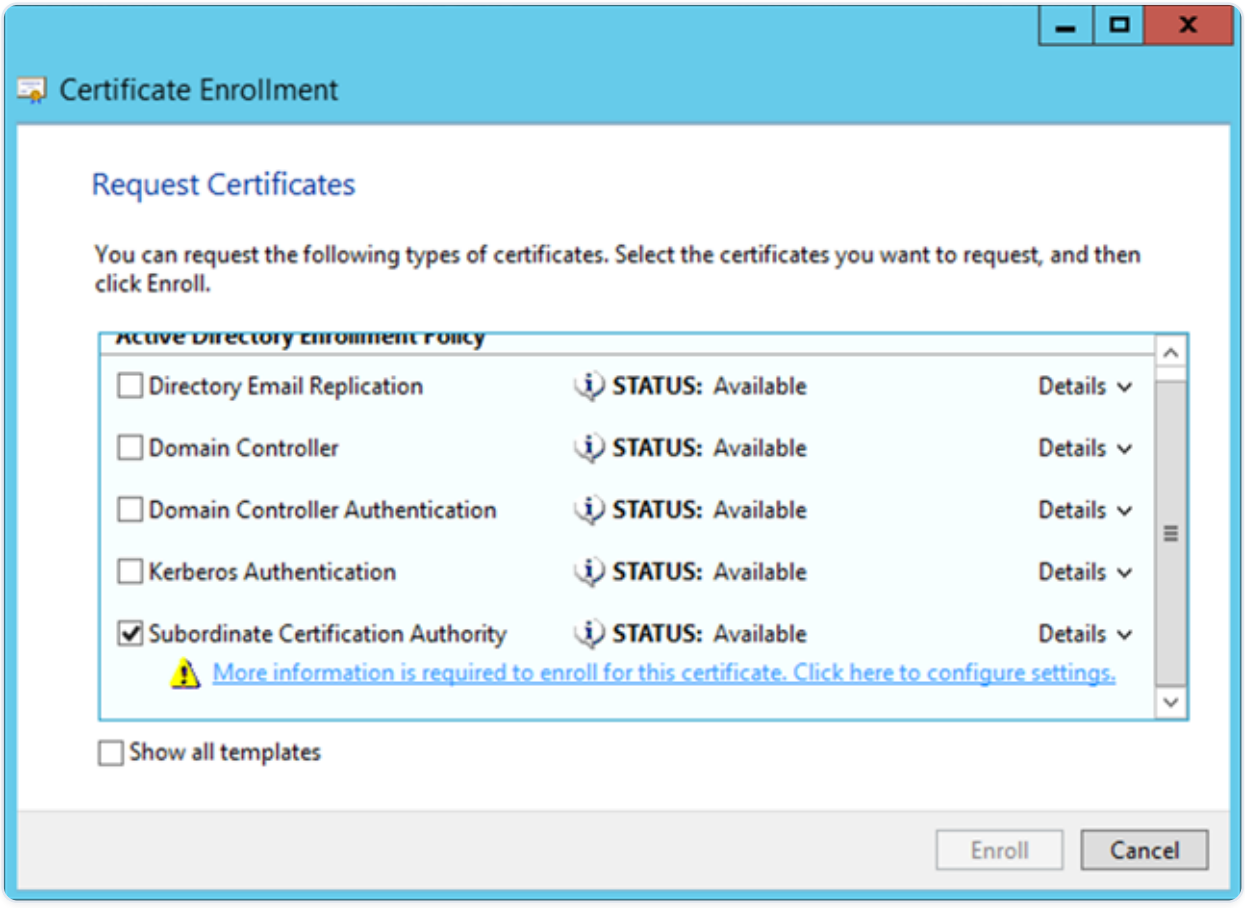
响应使用 SHA-256 和签名证书密钥算法（DSA、RSA 或 ECDSA）进行签名。

为您的 CA 生成并导入证书

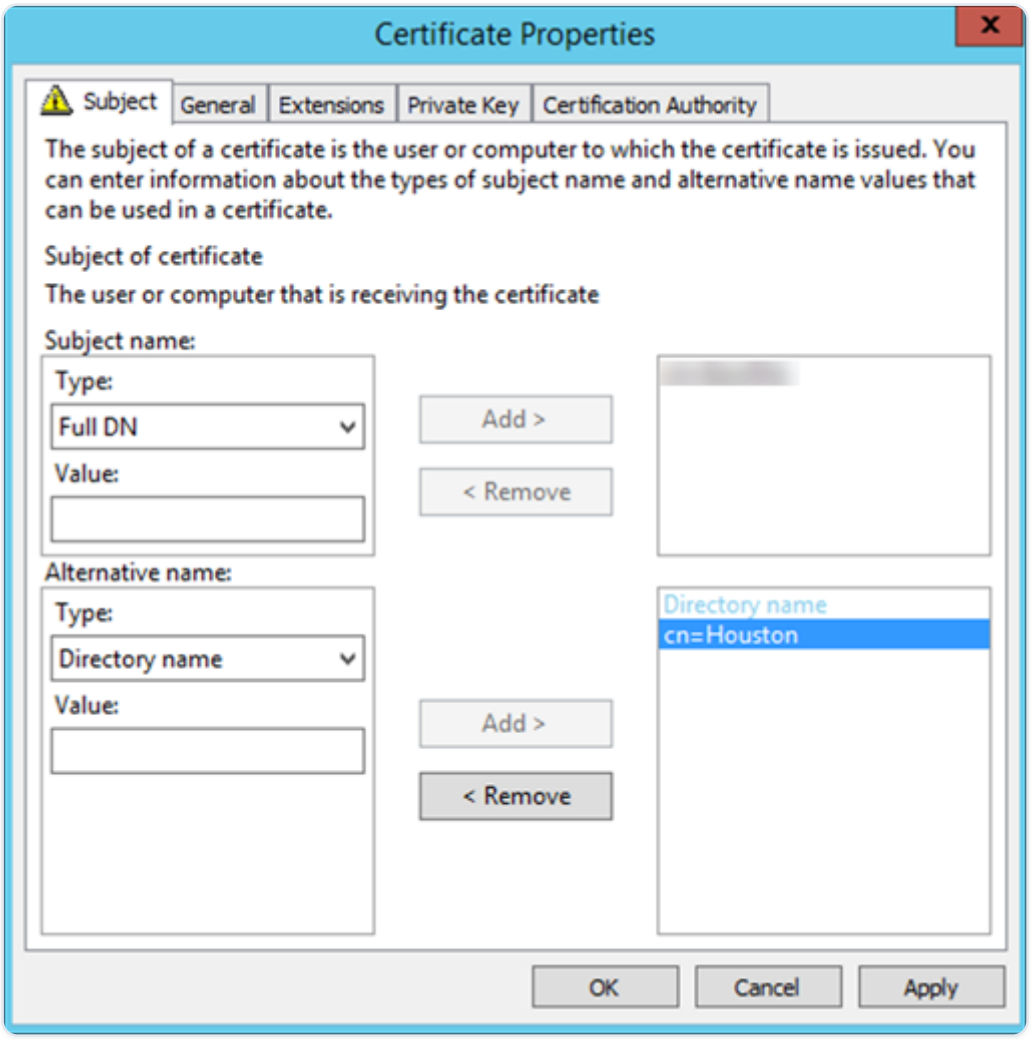
1. 在您的服务器上，使用本地系统帐户打开 Microsoft 管理控制台 (MMC)，然后打开证书管理单元。在右侧窗格中，右键单击，然后单击**所有任务 > 请求新证书**。



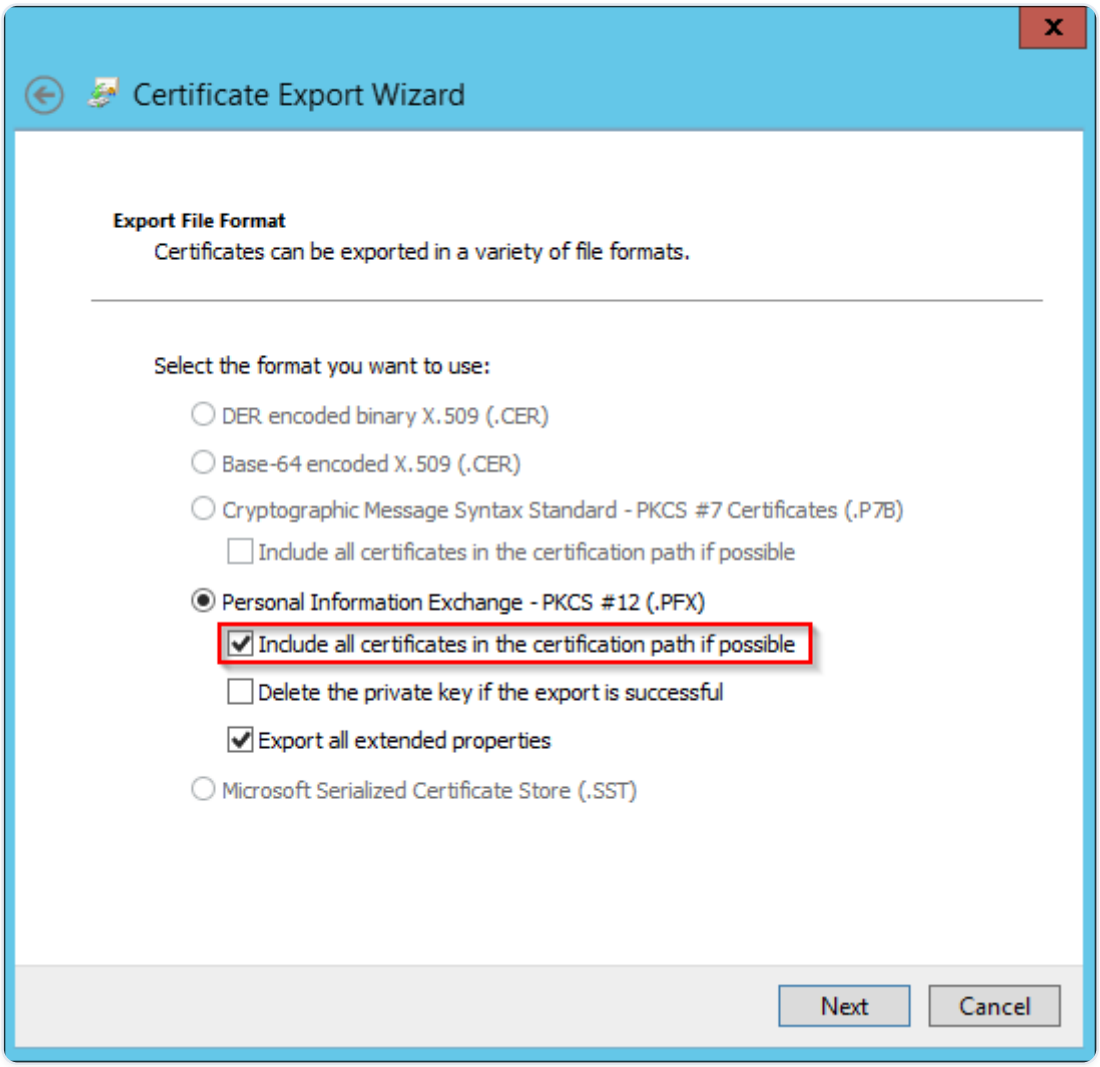
2. 在打开的向导中，单击两次**下一步**。在**请求证书**列表中，选择**从属证书颁发机构**，然后单击**更多信息**链接。



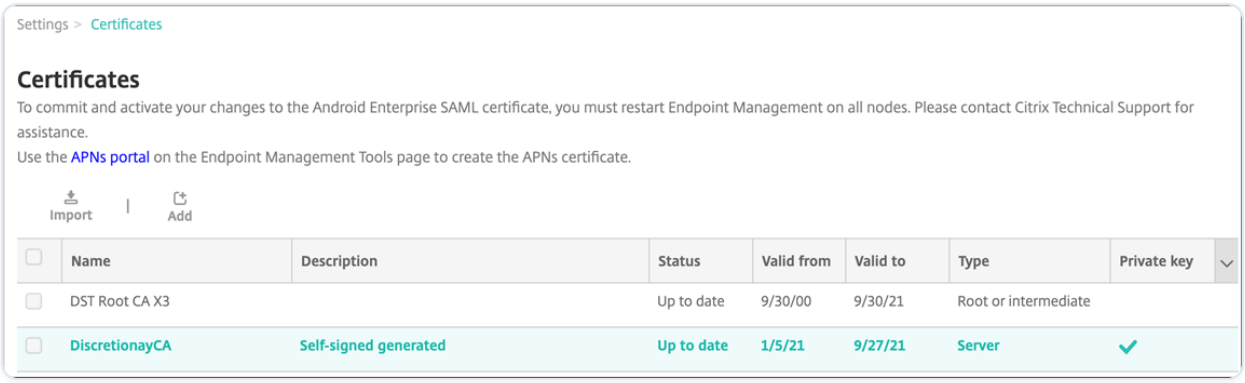
3. 在窗口中，键入**主题名称**和**备用名称**。单击**确定**。



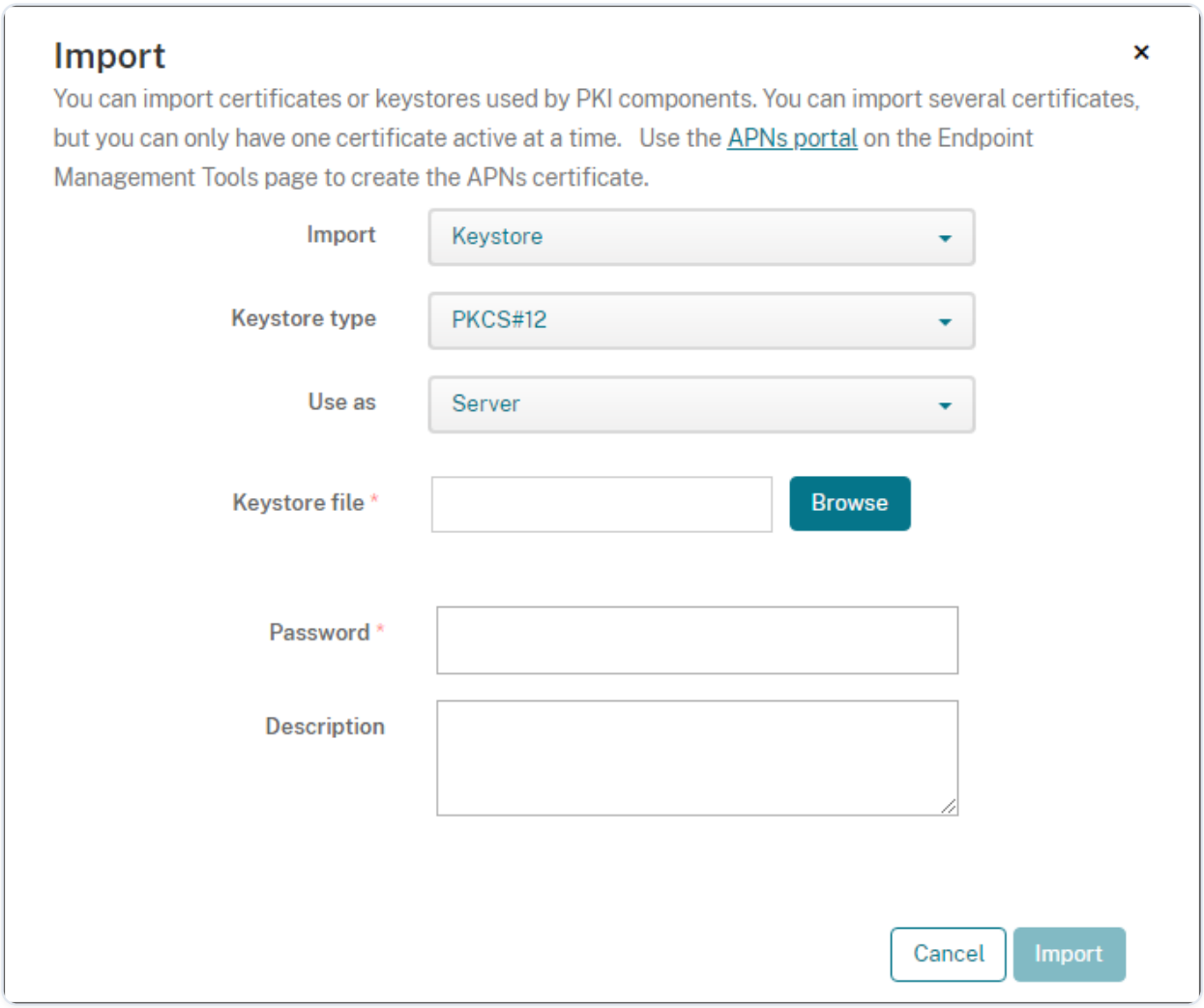
4. 单击**注册**，然后单击**完成**。
5. 在 MMC 中，右键单击您创建的证书。单击**所有任务 > 导出**。将证书导出为包含私钥的 .pfx 文件。选择**如果可能，包括证书路径中的所有证书**选项。



6. 在 Citrix Endpoint Management 控制台中，导航到**设置 > 证书**。



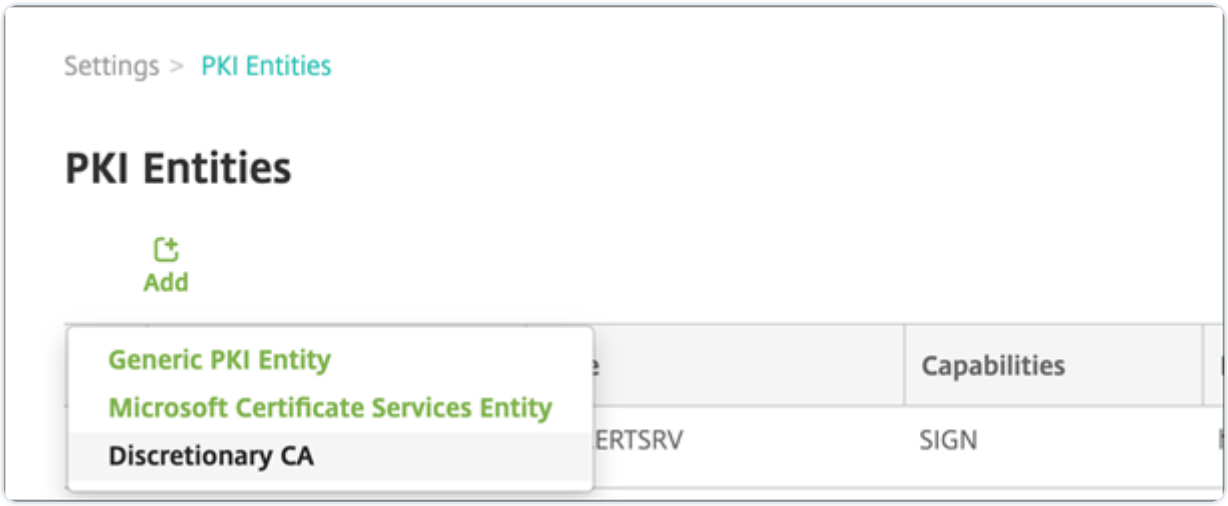
7. 单击**导入**。在打开的窗口中，浏览查找您之前导出的证书和私钥文件。



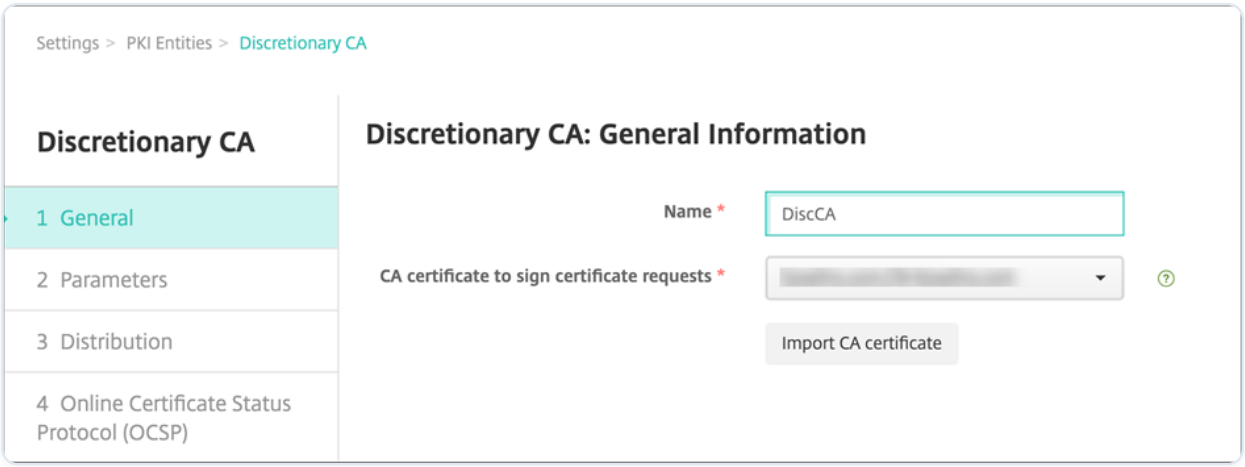
8. 单击“**导入**”。证书将添加到表中。

添加自由裁量 CA

1. 在 Citrix 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**”。



3. 单击“**自由裁量 CA**”。

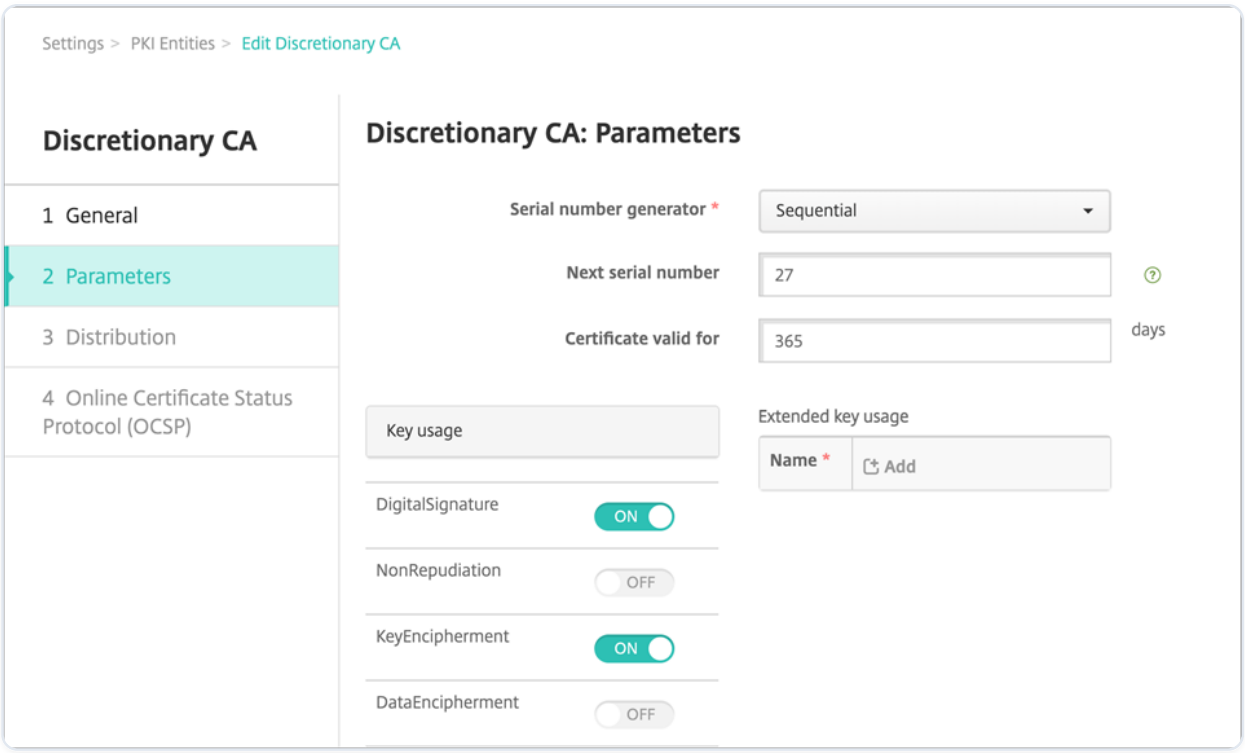


4. 在“**自由裁量 CA: 常规信息**”页面上，配置以下内容：

   - **名称：** 键入自由裁量 CA 的描述性名称。
   - **用于签署证书请求的 CA 证书：** 单击自由裁量 CA 用于签署证书请求的证书。

     此证书列表是根据您在 Citrix Endpoint Management 的“**配置 > 设置 > 证书**”中上传的包含私钥的 CA 证书生成的。

5. 单击“**下一步**”。



6. 在“**自由裁量 CA: 参数**”页面上，配置以下内容：

   - **序列号生成器：** 自由裁量 CA 会为其颁发的证书生成序列号。在此列表中，单击“**顺序**”或“**非顺序**”以确定如何生成这些数字。

- **下一个序列号：** 键入一个值以确定颁发的下一个数字。
- **证书有效期：** 输入证书的有效天数。
- **密钥用法**：通过将相应的密钥设置为“**开**”，识别由自由裁量 CA 颁发的证书的用途。设置后，CA 仅限于为这些用途颁发证书。
- **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**”。

   PKI 分发页面(/en-us/citrix-endpoint-management/media/pki-entities-discretionary-ca-distribution.png)

8. 在“**自由裁量 CA: 分发**”页面上，选择一个分发模式：

   - **集中式：服务器端密钥生成**。Citrix® 建议使用集中式选项。私钥在服务器上生成并存储，然后分发给用户设备。
   - **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，并且需要一个具有 **keyUsage keyEncryption** 扩展的 RA 加密证书和一个具有 **keyUsage digitalSignature** 扩展的 RA 签名证书。同一个证书可用于加密和签名。

9. 单击“**下一步**”。

   PKI OCSP 页面(/en-us/citrix-endpoint-management/media/pki-entities-discretionary-ca-ocsp.png)

10. 在“**自由裁量 CA: 在线证书状态协议 (OCSP)**”页面上，配置以下内容：

    - 如果要将 `AuthorityInfoAccess` (RFC2459) 扩展添加到此 CA 签名的证书中，请将“**为此 CA 启用 OCSP 支持**”设置为“**开**”。此扩展指向 `https://<server>/<instance>/ocsp` 处的 CA OCSP 响应程序。
    - 如果您启用了 OCSP 支持，请选择一个 OSCP 签名 CA 证书。此证书列表是根据您上传到 Citrix Endpoint Management 的 CA 证书生成的。

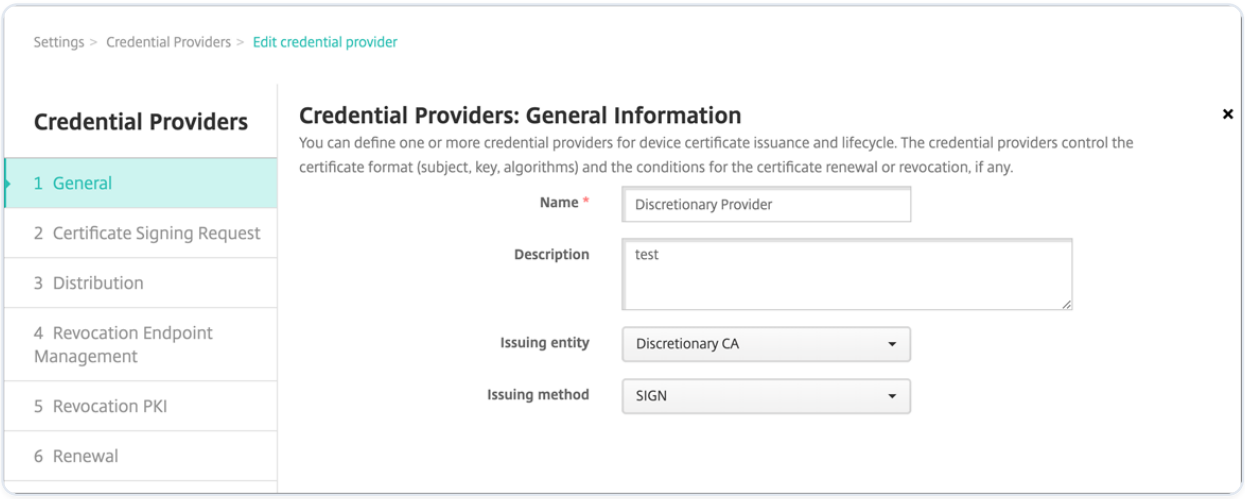
    启用此功能可让 Citrix ADC 有机会检查证书状态。Citrix 建议您启用此功能。

11. 点击 **保存**。

    自由裁量 CA 将显示在 PKI 实体表中。

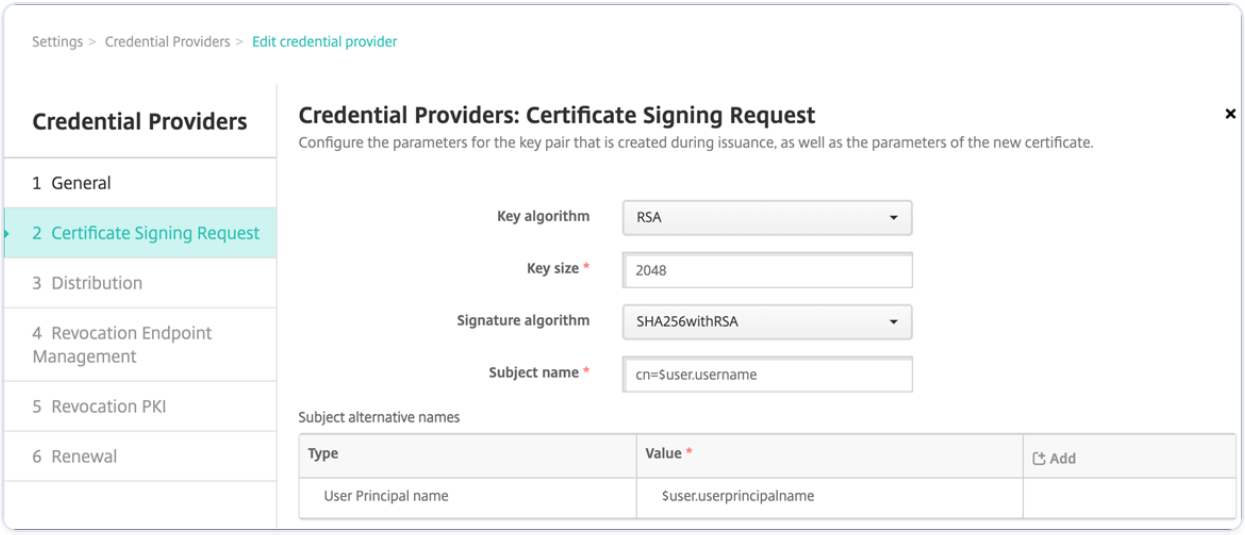
配置凭据提供程序

1. 在 Citrix 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：** 为新的提供程序配置键入一个唯一的名称。此名称稍后用于在 Citrix Endpoint Management 控制台的其他部分中识别此配置。
- **描述：** 描述凭据提供程序。尽管此字段是可选的，但描述可以提供有关此凭据提供程序的有用详细信息。
- **颁发实体：** 选择 **自由裁量 CA**。
- **颁发方法：** 单击“**签名**”或“**获取**”作为系统从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，配置以下内容：



- **密钥算法：** 为新的密钥对选择密钥算法。可用值为 **RSA**、**DSA** 和 **ECDSA**。
- **密钥大小：** 键入密钥对的大小（以位为单位）。此字段为必填项。Citrix 建议使用 **2048** 位。
- **签名算法：** 单击新证书的值。值取决于密钥算法。Citrix 建议使用 **SHA256withRSA**。
- **主题名称：** 必填。键入新证书主题的专有名称 (DN)。使用 `CN=${user.username}` 作为用户名，或使用 `CN=${user.samaccountname}` 作为 sAMAccountName。

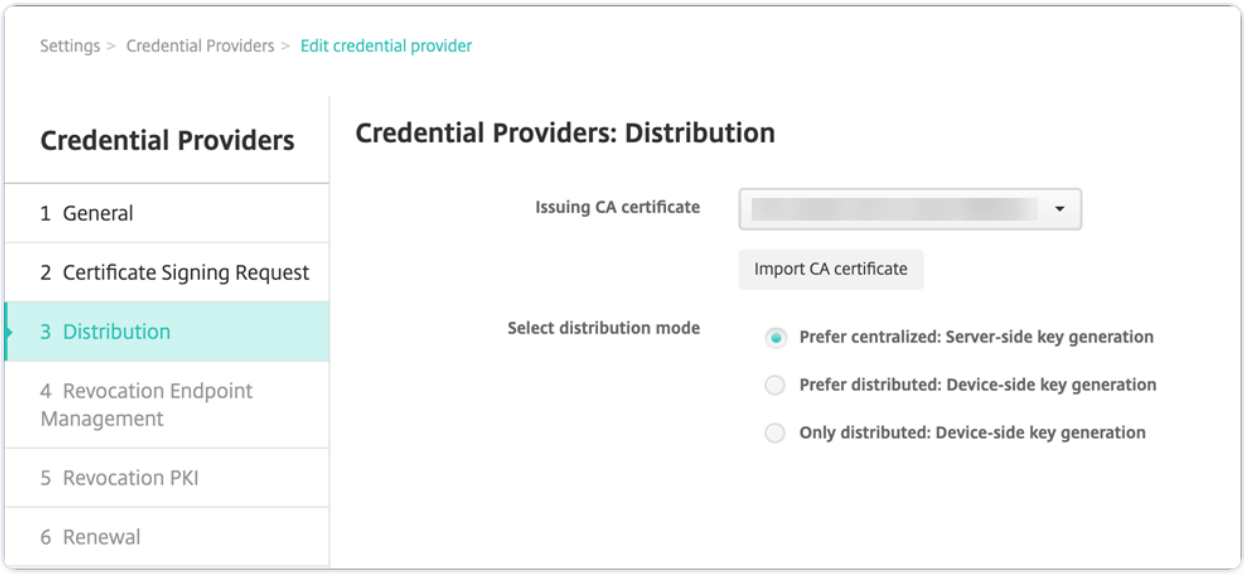
- 要向“**主题备用名称**”表中添加条目，请单击“**添加**”。选择备用名称的类型，然后在第二列中键入一个值。

  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 Citrix Endpoint Management 宏。

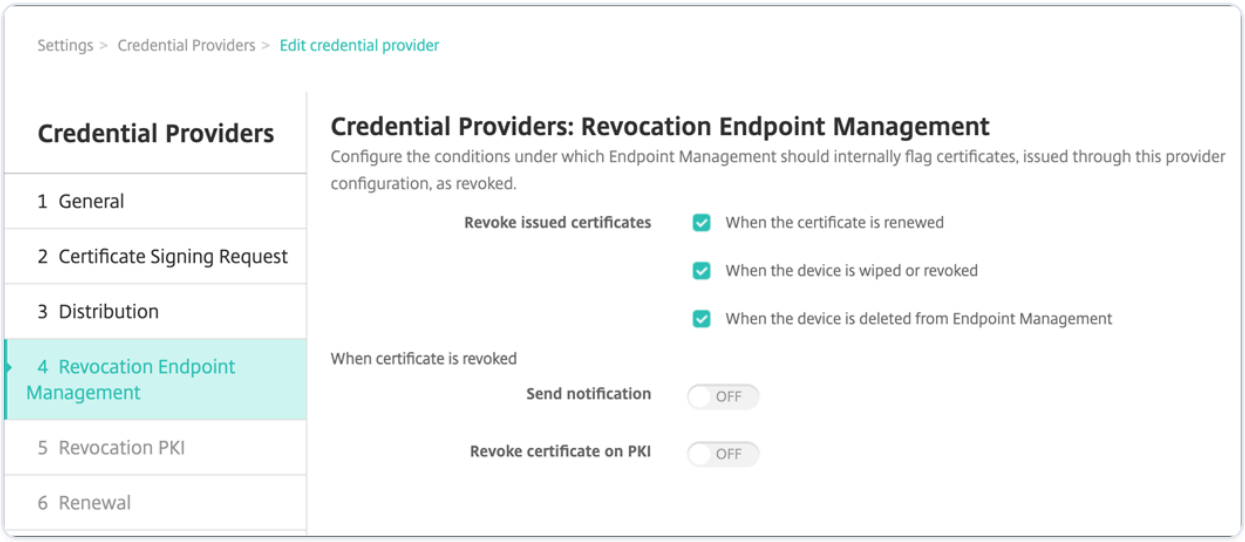
4. 单击**下一步**。在**凭据提供程序: 分发**页面上，配置以下内容：



- **颁发 CA 证书：** 选择您之前添加的自由裁量 CA 证书。
- **选择分发模式：** 选择以下生成和分发密钥的方式之一：
  - **首选集中式：服务器端密钥生成：** Citrix 建议使用此集中式选项。它支持 Citrix Endpoint Management 支持的所有平台，并且在使用 NetScaler Gateway 身份验证时是必需的。私钥在服务器上生成并存储，然后分发到用户设备。
  - **首选分布式：设备端密钥生成：** 私钥在用户设备上生成和存储。此分布式模式使用 SCEP，并且需要一个具有 keyUsage keyEncryption 的 RA 加密证书以及一个具有 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可用于加密和签名。
  - **仅分布式：设备端密钥生成：** 此选项的工作方式与**首选分布式：设备端密钥生成**相同，不同之处在于，如果设备端密钥生成失败或不可用，则没有其他选项。

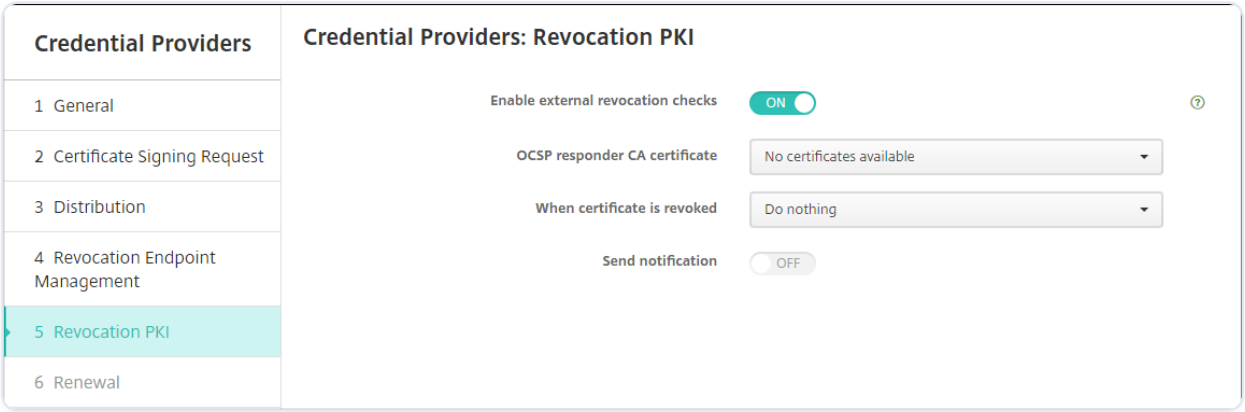
如果您选择了**首选分布式：设备端密钥生成**或**仅分布式：设备端密钥生成**，请单击 RA 签名证书和 RA 加密证书。同一个证书可用于两者。这些证书将显示新字段。

5. 单击**下一步**。在**凭据提供程序: 吊销 Citrix Endpoint Management** 页面上，配置 Citrix Endpoint Management 在何种条件下将通过此提供程序配置颁发的证书内部标记为已吊销。配置以下内容：



- 在**吊销已颁发证书**中，选择指示何时吊销证书的选项之一。
- 要指示 Citrix Endpoint Management 在证书被吊销时发送通知：将**发送通知**的值设置为**开**，然后选择一个通知模板。
- **在 PKI 上吊销证书**在使用 Citrix Endpoint Management 作为您的自由裁量 PKI 时不起作用。

6. 点击“**下一步**”。在“**凭据提供程序: 吊销 PKI**”页面上，确定证书被吊销时要对 PKI 执行的操作。您还可以选择创建通知消息。配置以下内容：



- **启用外部吊销检查：** 将此设置设为“**开**”。将显示更多与吊销 PKI 相关的字段。
- 在“**OCSP 响应程序 CA 证书**”列表中，选择证书主题的专有名称 (DN)。

  您可以将 Citrix Endpoint Management 宏用于 DN 字段值。例如：`CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`
- 在“**证书被吊销时**”列表中，单击以下操作之一，以在证书被吊销时对 PKI 实体执行操作：

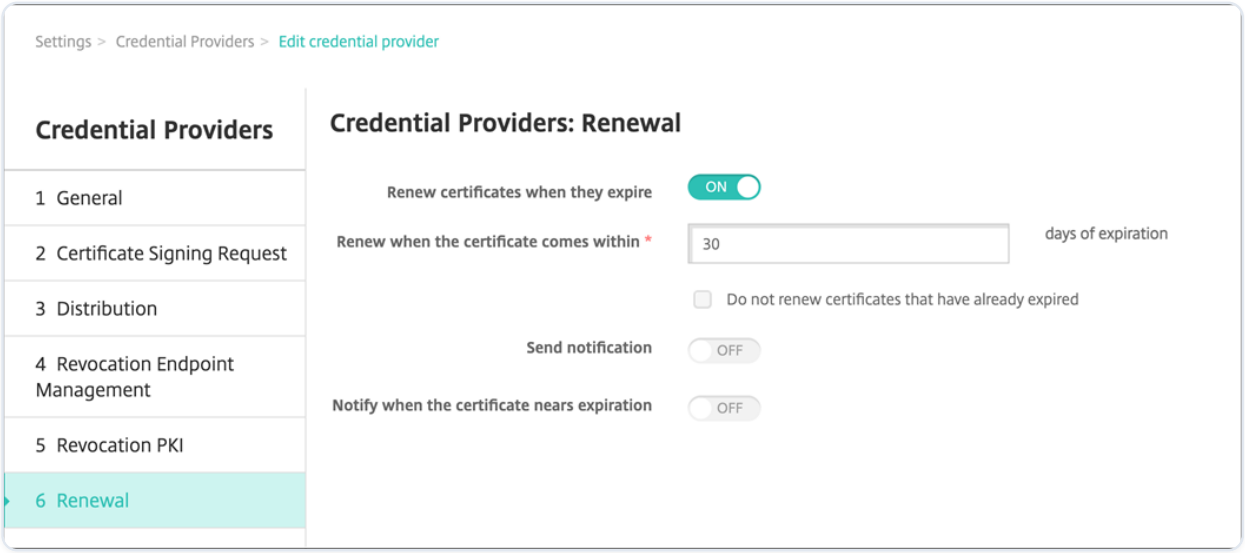
  - 不执行任何操作。
  - 续订证书。
  - 吊销并擦除设备。

- 要指示 Citrix Endpoint Management 在证书被吊销时发送通知：将“**发送通知**”的值设置为“**开**”。

  您可以在两个通知选项之间进行选择：

  - 如果选择“**选择通知模板**”，您可以选择一个预先编写的通知消息，然后对其进行自定义。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**”，您可以编写自己的通知消息。除了提供收件人的电子邮件地址和消息之外，您还可以设置通知的发送频率。

7. 点击“**下一步**”。在“**凭据提供程序: 续订**”页面上，配置以下内容：



将 **在证书过期时续订证书** 设置为 **开**。将显示更多字段。

- 在 **在证书到期前续订** 字段中，键入证书到期前多少天续订证书。
- （可选）选择 **不续订已过期的证书**。在这种情况下，“已过期”表示 `NotAfter` 日期已过，而不是证书已被吊销。Citrix Endpoint Management 不会在证书内部吊销后续订证书。

要指示 Citrix Endpoint Management 在证书续订时发送通知，请将 **发送通知** 设置为 **开**。要指示 Citrix Endpoint Management 在证书即将到期时发送通知，请将 **在证书即将到期时通知** 设置为 **开**。 对于上述任一选择，您都可以从两个通知选项中进行选择：

- **选择通知模板：** 选择一个预先编写的通知消息，然后您可以对其进行自定义。这些模板位于“通知模板”列表中。

- **输入通知详细信息：** 编写您自己的通知消息。提供收件人的电子邮件地址、消息以及发送通知的频率。

8. 点击 **保存**。

凭据提供程序

凭据提供程序是您在 Citrix Endpoint Management 系统的各个部分中使用的实际证书配置。凭据提供程序定义了证书的来源、参数和生命周期。无论证书是设备配置的一部分还是独立存在（即按原样推送到设备），这些操作都会发生。

设备注册限制了证书的生命周期。也就是说，Citrix Endpoint Management 在注册之前不会颁发证书，尽管 Citrix Endpoint Management 可能会在注册过程中颁发一些证书。此外，在一次注册上下文中从内部 PKI 颁发的证书，在注册被撤销时也会被撤销。管理关系终止后，不会保留任何有效证书。

您可以在许多地方使用一个凭据提供程序配置，这意味着一个配置可以同时管理任意数量的证书。统一性体现在部署资源和部署上。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 的颁发设置决定了部署到 D 的证书。同样，当 C 更新时，D 的续订设置适用。并且，当 C 被删除或 D 被撤销时，D 的撤销设置也适用。

根据这些规则，Citrix Endpoint Management 中的凭据提供程序配置决定了以下内容：

- 证书的来源。
- 获取证书的方法：签署新证书或获取（恢复）现有证书和密钥对。
- 颁发或恢复的参数：例如，证书签名请求 (CSR) 参数，如密钥大小、密钥算法和证书扩展。
- 证书交付到设备的方式。
- 撤销条件：尽管当管理关系断开时，Citrix Endpoint Management 中的所有证书都会被撤销，但配置可能会指定更早的撤销。例如，配置可以指定在关联的设备配置被删除时撤销证书。此外，在某些条件下，Citrix Endpoint Management 中关联证书的撤销可能会发送到后端公钥基础设施 (PKI)。也就是说，Citrix Endpoint Management 中的证书撤销可能会导致 PKI 上的证书撤销。
- 续订设置：通过给定凭据提供程序获得的证书在接近过期时可以自动续订。或者，与此情况分开，当过期临近时可以发出通知。

配置选项的可用性主要取决于您为凭据提供程序选择的 PKI 实体类型和颁发方法。

证书颁发方法

您可以通过签名获取证书，这被称为颁发方法。

使用此方法，颁发涉及创建新的私钥、创建 CSR，并将 CSR 提交给证书颁发机构 (CA) 进行签名。Citrix Endpoint Management 支持 MS 证书服务实体和自由裁量 CA 实体的签名方法。

凭据提供程序使用签发方法。

证书交付

Citrix Endpoint Management 中提供两种证书交付模式：集中式和分布式。分布式模式使用简单证书注册协议 (SCEP)，并且仅在客户端支持该协议（仅限 iOS）的情况下可用。在某些情况下，分布式模式是强制性的。

为了使凭据提供程序支持分布式（SCEP 辅助）交付，需要一个特殊的配置步骤：设置注册机构 (RA) 证书。RA 证书是必需的，因为如果您使用 SCEP 协议，Citrix Endpoint Management 会充当实际证书颁发机构的委托（注册商）。Citrix Endpoint Management 必须向客户端证明它有权充当此类角色。该权限是通过将前面提到的证书上传到 Citrix Endpoint Management 来建立的。

需要两种不同的证书角色（尽管单个证书可以满足这两个要求）：RA 签名和 RA 加密。这些角色的限制如下：

- RA 签名证书必须具有 X.509 密钥用法数字签名。
- RA 加密证书必须具有 X.509 密钥用法密钥加密。

要配置凭据提供程序 RA 证书，您需要将证书上传到 Citrix Endpoint Management，然后在凭据提供程序中链接到它们。

仅当凭据提供程序配置了证书角色证书时，才认为该提供程序支持分布式交付。您可以将每个凭据提供程序配置为优先使用集中式模式、优先使用分布式模式或要求使用分布式模式。实际结果取决于上下文：如果上下文不支持分布式模式，但凭据提供程序要求此模式，则部署失败。同样，如果上下文要求分布式模式，但凭据提供程序不支持分布式模式，则部署失败。在所有其他情况下，将遵循首选设置。

下表显示了 Citrix Endpoint Management 中的 SCEP 分布情况：

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 配置配置文件	是	否
SHTP 注册	否	否

上下文	支持 SCEP	需要 SCEP
SHTP 配置	否	否
Windows 平板电脑注册	否	否
Windows 平板电脑配置	否，网络设备策略除外，该策略支持 Windows 10 和 Windows 11 版本	否

证书吊销

吊销分为三种类型。

- **内部吊销：** 内部吊销会影响 Citrix Endpoint Management 维护的证书状态。Citrix Endpoint Management 在评估所提供的证书或提供证书的 OCSP 状态信息时会考虑此状态。凭据提供程序配置决定了此状态在各种条件下的受影响方式。例如，凭据提供程序可能会指定在证书从设备中删除时将其标记为已吊销。
- **外部传播吊销：** 也称为 Citrix Endpoint Management 吊销，此类吊销适用于从外部 PKI 获取的证书。当 Citrix Endpoint Management 在凭据提供程序配置定义的条件下内部吊销证书时，该证书会在 PKI 上被吊销。
- **外部诱导吊销：** 也称为 PKI 吊销，此类吊销也仅适用于从外部 PKI 获取的证书。每当 Citrix Endpoint Management 评估给定证书状态时，Citrix Endpoint Management 都会向 PKI 查询该状态。如果证书被吊销，Citrix Endpoint Management 会内部吊销该证书。此机制使用 OCSP 协议。

这三种类型并非相互排斥，而是共同适用。外部吊销或独立发现可能导致内部吊销。内部吊销可能会影响外部吊销。

证书续订

证书续订是现有证书的吊销与另一证书的颁发相结合的过程。

Citrix Endpoint Management 首先尝试获取新证书，然后再吊销旧证书，以避免在颁发失败时服务中断。对于分布式（支持 SCEP）交付，吊销也仅在证书成功安装到设备上之后发生。否则，吊销会在新证书发送到设备之前发生。该吊销与证书安装的成功或失败无关。

吊销配置要求您指定一个持续时间（以天为单位）。当设备连接时，服务器会验证证书 `NotAfter` 日期是否晚于当前日期减去指定持续时间。如果证书符合该条件，Citrix Endpoint Management 会尝试续订证书。

创建凭据提供程序

配置凭据提供程序主要取决于您为凭据提供程序选择的颁发实体和颁发方法。您可以区分使用内部实体或外部实体的凭据提供程序：

- 自由裁量实体是 Citrix Endpoint Management 内部的实体，属于内部实体。自由裁量实体的颁发方法始终是签名。签名意味着在每次颁发操作中，Citrix Endpoint Management 都会使用为该实体选择的 CA 证书对新的密钥对进行签名。密钥对是在设备上还是在服务器上生成，取决于您选择的分发方法。
- 外部实体是您企业基础架构的一部分，包括 Microsoft CA。

1. 在 Citrix 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：** 为新的提供程序配置键入一个唯一的名称。此名称稍后用于在 Citrix Endpoint Management 控制台的其他部分中标识该配置。
   - **描述：** 描述凭据提供程序。尽管此字段是可选的，但描述可以提供有关此凭据提供程序的有用详细信息。
   - **颁发实体：** 单击证书颁发实体。
   - **颁发方法：** 单击**签名**或**获取**，作为系统从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，请选择您在凭据提供程序的 PKI 实体下添加的模板。

     当在**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**”。

   出现**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，配置以下内容：

   - **密钥算法**：选择新密钥对的密钥算法。可用值包括 **RSA**、**DSA** 和 **ECDSA**。
   - **密钥大小**：键入密钥对的大小（以位为单位）。此字段为必填项。

     允许的值取决于密钥类型。例如，DSA 密钥的最大大小为 2048 位。为避免假阴性（这取决于底层硬件和软件），Citrix Endpoint Management 不强制执行密钥大小。在生产环境中激活凭据提供程序配置之前，请务必在测试环境中对其进行测试。

- **签名算法**：单击新证书的值。值取决于密钥算法。
- **主题名称**：必需。键入新证书主题的专有名称 (DN)。例如： `CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation`

  例如，对于客户端证书身份验证，请使用以下设置：

  - **密钥算法**：RSA
  - **密钥大小**：2048
  - **签名算法**：SHA256withRSA
  - **主题名称**： `cn=$user.username`
- 要向**主题备用名称**表中添加条目，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：

  - **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 Citrix Endpoint Management 宏。

6. 单击“**下一步**”。

   出现 **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。因为凭据提供程序使用自由裁量的 CA 实体，所以凭据提供程序的 CA 证书始终是实体本身上配置的 CA 证书。此处显示 CA 证书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的方式之一：
     - **首选集中式：服务器端密钥生成：** Citrix 建议使用此集中式选项。它支持 Citrix Endpoint Management 支持的所有平台，并且在使用 NetScaler Gateway 身份验证时是必需的。私钥在服务器上生成并存储，然后分发到用户设备。
     - **首选分布式：设备端密钥生成：** 私钥在用户设备上生成并存储。此分布式模式使用 SCEP，并且需要一个具有 keyUsage keyEncryption 的 RA 加密证书和一个具有 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可用于加密和签名。

- **仅分布式：设备端密钥生成：** 此选项的工作方式与“首选分布式：设备端密钥生成”相同，不同之处在于，由于它是“仅”而不是“首选”，因此如果设备端密钥生成失败或不可用，则没有其他选项可用。

如果您选择了 **首选分布式：设备端密钥生成** 或 **仅分布式：设备端密钥生成**，请单击 RA 签名证书和 RA 加密证书。同一个证书可用于两者。这些证书将出现新字段。

8. 单击“**下一步**”。

出现 **凭据提供程序：吊销 Citrix Endpoint Management** 页面。在此页面上，您可以配置 Citrix Endpoint Management 在何种条件下将通过此提供程序配置颁发的证书内部标记为已吊销。

9. 在 **凭据提供程序：吊销 Citrix Endpoint Management** 页面上，执行以下操作：

- 在 **吊销已颁发证书** 中，选择指示何时吊销证书的选项之一。
- 要指示 Citrix Endpoint Management 在证书被吊销时发送通知：将 **发送通知** 的值设置为 **开**，并选择一个通知模板。
- 要在证书从 Citrix Endpoint Management 吊销时在 PKI 上吊销证书：将 **在 PKI 上吊销证书** 设置为 **开**，并且在 **实体列表** 中，单击一个模板。实体列表显示所有具有吊销功能的可用实体。当证书从 Citrix Endpoint Management 吊销时，吊销调用将发送到从实体列表中选择的 PKI。

10. 单击“**下一步**”。

将显示**凭据提供程序: 吊销 PKI** 页面。在此页面上，您可以确定在证书被吊销时对 PKI 采取哪些操作。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**的设置更改为**开**。将显示更多与吊销 PKI 相关的字段。
- 在**OCSP 响应程序 CA 证书**列表中，单击证书主题的专有名称 (DN)。

  您可以将 Citrix Endpoint Management 宏用于 DN 字段值。例如：`CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`
- 在**证书被吊销时**列表中，单击以下操作之一，以在证书被吊销时对 PKI 实体执行操作：
  - 不执行任何操作。
  - 续订证书。
  - 吊销并擦除设备。
- 要指示 Citrix Endpoint Management 在证书被吊销时发送通知：将**发送通知**的值设置为**开**。

您可以选择以下两种通知选项：

- 如果选择**选择通知模板**，您可以选择一个预先编写的通知消息，然后对其进行自定义。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**，您可以编写自己的通知消息。除了提供收件人的电子邮件地址和消息外，您还可以设置发送通知的频率。

12. 单击“**下一步**”。

    将显示**凭据提供程序: 续订**页面。在此页面上，您可以配置 Citrix Endpoint Management 以执行以下操作：

    - 续订证书。您可以选择在续订时发送通知，并选择从操作中排除已过期的证书。
    - 为即将过期的证书发出通知（续订前通知）。

13. 在**凭据提供程序: 续订**页面上，如果要续订过期证书，请执行以下操作：

    将“**证书过期时续订**”设置为“**开**”。将显示更多字段。

    - 在“**证书在以下天数内到期时续订**”字段中，键入证书到期前多少天续订。
    - （可选）选择“**不续订已过期的证书**”。在这种情况下，“已过期”表示 `NotAfter` 日期已过，而不是已吊销。Citrix Endpoint Management 不会在证书内部吊销后续订它们。

    要指示 Citrix Endpoint Management 在证书续订时发送通知：将“**发送通知**”设置为“**开**”。要指示 Citrix Endpoint Management 在证书即将到期时发送通知：将“**证书即将到期时通知**”设置为“**开**”。 对于这两种选择，您可以选择以下两种通知选项之一：

    - **选择通知模板：** 选择一个预先编写的通知消息，您可以对其进行自定义。这些模板位于通知模板列表中。
    - **输入通知详细信息：** 编写您自己的通知消息。提供收件人的电子邮件地址、消息以及发送通知的频率。

    在“**证书在以下天数内到期时通知**”字段中，键入在证书到期前多少天发送通知。

14. 点击 **保存**。

    凭据提供程序将显示在“凭据提供程序”表中。

APNs 证书

要在 Citrix Endpoint Management 中注册和管理 Apple 设备，您需要从 Apple 设置 Apple 推送通知服务 (APNs) 证书。此证书通过 Apple 推送网络启用移动设备管理。

工作流摘要:

步骤 1： 通过以下任一方法创建证书签名请求 (CSR)：

- 通过 macOS 上的“钥匙串访问”创建 CSR（Citrix® 推荐）
- 通过 Microsoft IIS 创建 CSR
- 通过 OpenSSL 创建 CSR

步骤 2： 在 Citrix Endpoint Management 工具中签署 CSR

步骤 3： 将已签名的 CSR 提交给 Apple 以获取 APNs 证书

步骤 4： 使用用于步骤 1 的同一台计算机，完成 CSR 并导出 PKCS #12 文件：

- 通过 macOS 上的“钥匙串访问”创建 PKCS #12 文件
- 通过 Microsoft IIS 创建 PKCS #12 文件
- 通过 OpenSSL 创建 PKCS #12 文件

步骤 5： 将 APNs 证书导入 Citrix Endpoint Management

步骤 6： 续订 APNs 证书

创建证书签名请求

建议您使用 macOS 上的“钥匙串访问”创建 CSR。您也可以使用 Microsoft IIS 或 OpenSSL 创建 CSR。

重要提示：

- 对于用于创建证书的 Apple ID：
  - Apple ID 必须是公司 ID，而不是个人 ID。
  - 记录您用于创建证书的 Apple ID。
  - 要续订证书，请使用相同的组织名称和 Apple ID。使用不同的 Apple ID 续订证书需要重新注册设备。
- 如果您意外或有意撤销证书，您将失去管理设备的能力。
- 如果您使用 iOS Developer Enterprise Program 创建了移动设备管理器推送证书：请务必在 Apple 推送证书门户中处理迁移证书的任何操作。

使用 macOS 上的“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，启动“钥匙串访问”应用。
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. 证书助理会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。
   - **通用名称：**管理证书的个人或角色帐户的通用名称。
   - **CA 电子邮件地址：**证书颁发机构的电子邮件地址。
4. 选择**保存到磁盘**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，将文件保存到您的计算机，然后单击**保存**。
6. 指定密钥对信息：选择 2048 位的**密钥大小**和 **RSA 算法**，然后单击**继续**。CSR 文件已准备好，可作为 APNs 证书过程的一部分进行上传。
7. 当证书助理完成 CSR 过程时，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**创建证书请求**。
4. 键入相应的专有名称 (DN) 信息。例如，您可以键入 Citrix 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**，为位长度选择 **2048**，然后单击**下一步**。
6. 输入文件名并指定保存 CSR 的位置，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。您可以从 OpenSSL 网站下载并安装 OpenSSL。

1. 在安装 OpenSSL 的计算机上，从命令提示符或 shell 运行以下命令。

`openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.csr -newkey rsa:2048`

2. 出现以下证书命名信息消息。按要求输入信息。

```
You are about to be asked to enter information that will be
incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a
DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:RWC

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

Organizational Unit Name (eg, section) [:Marketing

Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com
```

3. 在下一条消息中，输入 CSR 私钥的密码。

```
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:
```

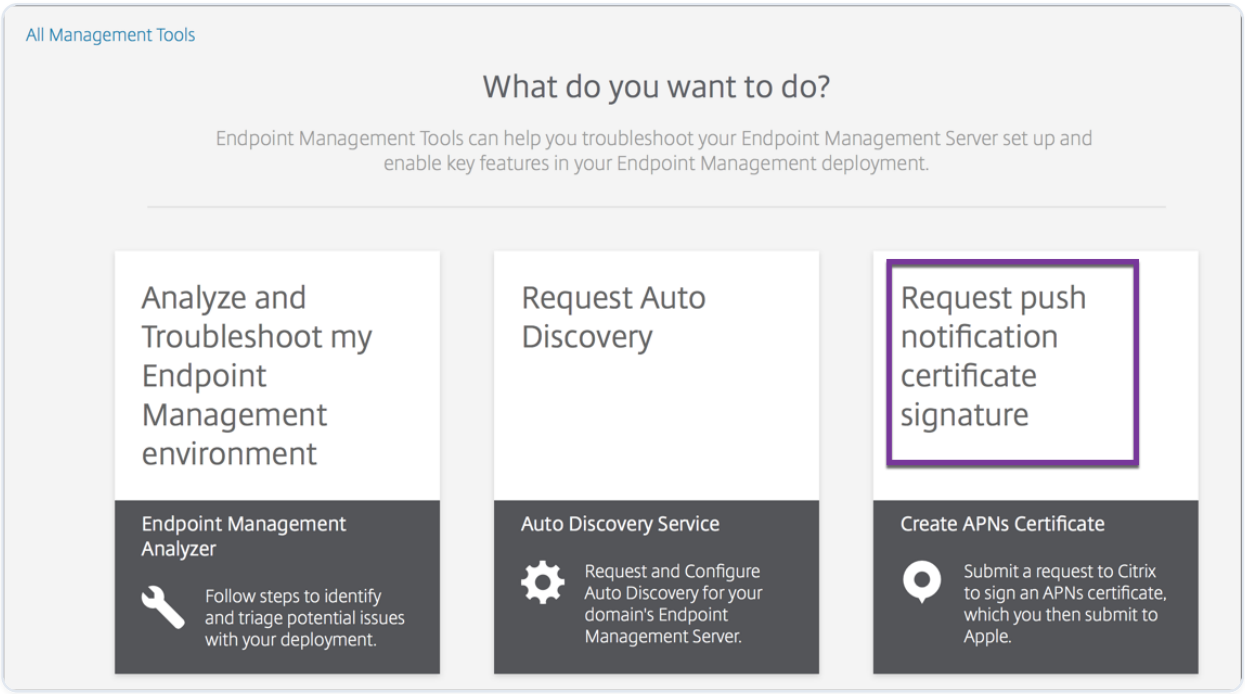
```
An optional company name []:
```

4. 要继续，请按照下一节中的说明签署 CSR。

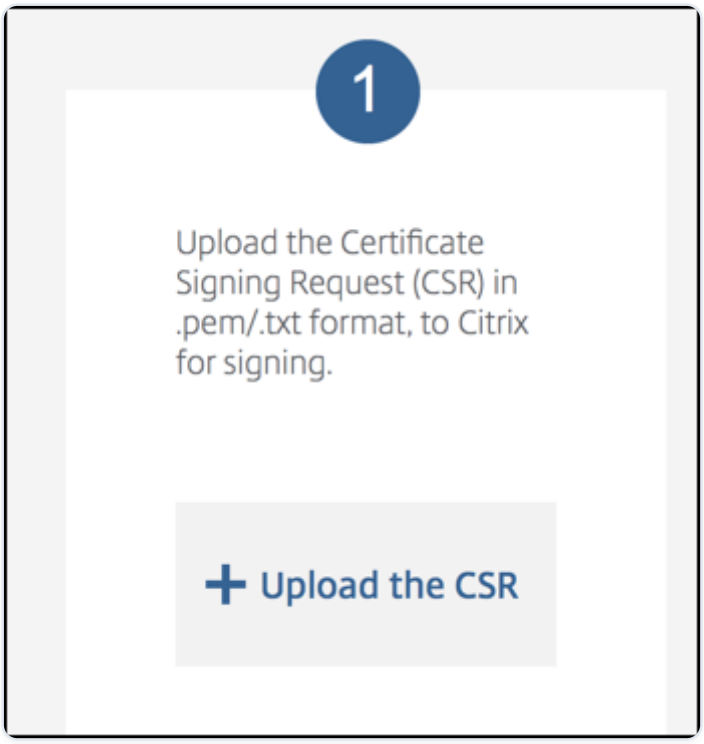
签署 CSR

要将证书与 Citrix Endpoint Management 结合使用，您必须将其提交给 Citrix 进行签名。Citrix 将使用其移动设备管理签名证书签署 CSR，并以 `.plist` 格式返回已签名的文件。

1. 在浏览器中，转到 Citrix Endpoint Management Tools 网站，然后单击 **Request push notification certificate signature**。



2. 在**创建新证书页面**上，单击**上传 CSR**。



3. 浏览并选择证书。

> **重要提示：**
>
> 证书必须采用 .pem/txt 格式。如果需要，可以通过右键单击并重命名文件，将证书的文件名扩展名更改为 .pem 或 .txt。

4. 在 **Citrix Endpoint Management APNs CSR Signing** 页面上，单击 **Sign**。CSR 已签名并自动保存到您配置的下载文件夹。
5. 要继续，请按照下一节中的说明提交已签名的 CSR。

将已签名的 CSR 提交给 Apple 以获取 APNs 证书

从 Citrix 收到已签名的证书签名请求 (CSR) 后，将 CSR 提交给 Apple 以获取导入 Citrix Endpoint Management 所需的 APNs 证书。

> **注意：**
>
> 一些用户报告了登录 Apple 推送门户时出现问题。作为替代方案，您可以登录到 Apple Developer Portal。然后，您可以按照以下步骤操作：

1. 在浏览器中，转到 Apple Push Certificates Portal。

2. 单击“**创建证书**”。
3. 首次使用 Apple 创建证书时：选中“**我已阅读并同意这些条款和条件**”复选框，然后单击“**接受**”。
4. 单击“**选择文件**”，浏览到计算机上已签名的 CSR，然后单击“**上传**”。确认消息指示上传成功。
5. 单击“**下载**”以检索 .pem 证书。
6. 要继续，请按照下一节中的说明完成 CSR 并导出 PKCS #12 文件。

完成 CSR 并导出 PKCS #12 文件

从 Apple 收到 APNs 证书后，返回到“钥匙串访问”、“Microsoft IIS”或“OpenSSL”以将证书导出为 PCKS #12 文件。

PKCS #12 文件包含 APNS 证书文件和您的私钥。PFX 文件通常具有 .pfx 或 .p12 扩展名。您可以互换使用 .pfx 和 .p12 文件。

> **重要提示：**
>
> Citrix 建议您从本地系统保存或导出个人密钥和公钥。您需要这些密钥才能访问 APNs 证书以供重复使用。如果没有相同的密钥，您的证书将无效，并且您必须重复整个 CSR 和 APNs 过程。

使用 macOS 上的“钥匙串访问”创建 PKCS #12 文件

> **重要提示：**
>
> 对于此任务，请使用您用于生成 CSR 的同一 macOS 设备。

1. 在设备上，找到从 Apple 收到的生产身份 (.pem) 证书。
2. 启动“钥匙串访问”应用程序，然后导航到“**登录 > 我的证书**”选项卡。将产品身份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. 要开始将证书导出为 PCKS #12 (.pfx) 证书，请选择证书和私钥，右键单击，然后选择“**导出 2 项**”。
5. 为证书文件指定一个用于 Citrix Endpoint Management 的唯一名称。名称中不要包含空格字符。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 建议您使用唯一且强度高的密码。此外，请务必妥善保管证书和密码，以备将来使用和参考。
7. “钥匙串访问”应用会提示您输入登录密码或选定的钥匙串。输入密码，然后单击“**确定**”。现在，保存的证书已可用于 Citrix Endpoint Management 服务器。
8. 要继续，请参阅将 APNs 证书导入 Citrix Endpoint Management。

使用 Microsoft IIS 创建 PKCS #12 文件

> **重要提示：**
>
> 对于此任务，请使用您用于生成 CSR 的同一 IIS 服务器。

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“**完成证书请求**”。
4. 浏览到 Apple 提供的 Certificate.pem 文件。然后，键入一个友好名称或证书名称，然后单击“**确定**”。名称中不要包含空格字符。
5. 选择您在步骤 4 中标识的证书，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到 Citrix Endpoint Management 中。
7. 将 .pfx 证书复制到您计划安装 Citrix Endpoint Management 的服务器上。
8. 要继续，请参阅将 APNs 证书导入 Citrix Endpoint Management。

使用 OpenSSL 创建 PKCS #12 文件

如果您使用 OpenSSL 创建 CSR，也可以使用 OpenSSL 创建 .pfx APNs 证书。

1. 在命令提示符或 shell 中，运行以下命令。`Customer.privatekey.pem` 是您的 CSR 中的私钥。`APNs_Certificate.pem` 是您刚从 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。请记住此密码，因为在将证书上传到 Citrix Endpoint Management 时会再次使用此密码。

3. 记下 .pfx 证书文件的位置。然后，将文件复制到 Citrix Endpoint Management 服务器，以便您可以使用控制台上传该文件。
4. 要继续，请按照下一节中的说明将 APNs 证书导入 Citrix Endpoint Management。

将 APNs 证书导入 Citrix Endpoint Management

收到新的 APNs 证书后：将 APNs 证书导入 Citrix Endpoint Management，以首次添加证书或替换现有证书。

1. 在 Citrix 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。
5. 输入密码，然后单击“**导入**”。

有关 Citrix Endpoint Management 中证书的详细信息，请参阅证书和身份验证。

续订 APNs 证书

> **重要提示：**

> 如果您在续订过程中使用不同的 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，然后转到 Apple 推送证书门户。使用该门户上传新证书。登录后，将显示您现有的证书或从您以前的 Apple 开发者帐户导入的证书。

在证书门户中，续订证书时唯一的区别是单击“**续订**”。您必须拥有证书门户的开发者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。

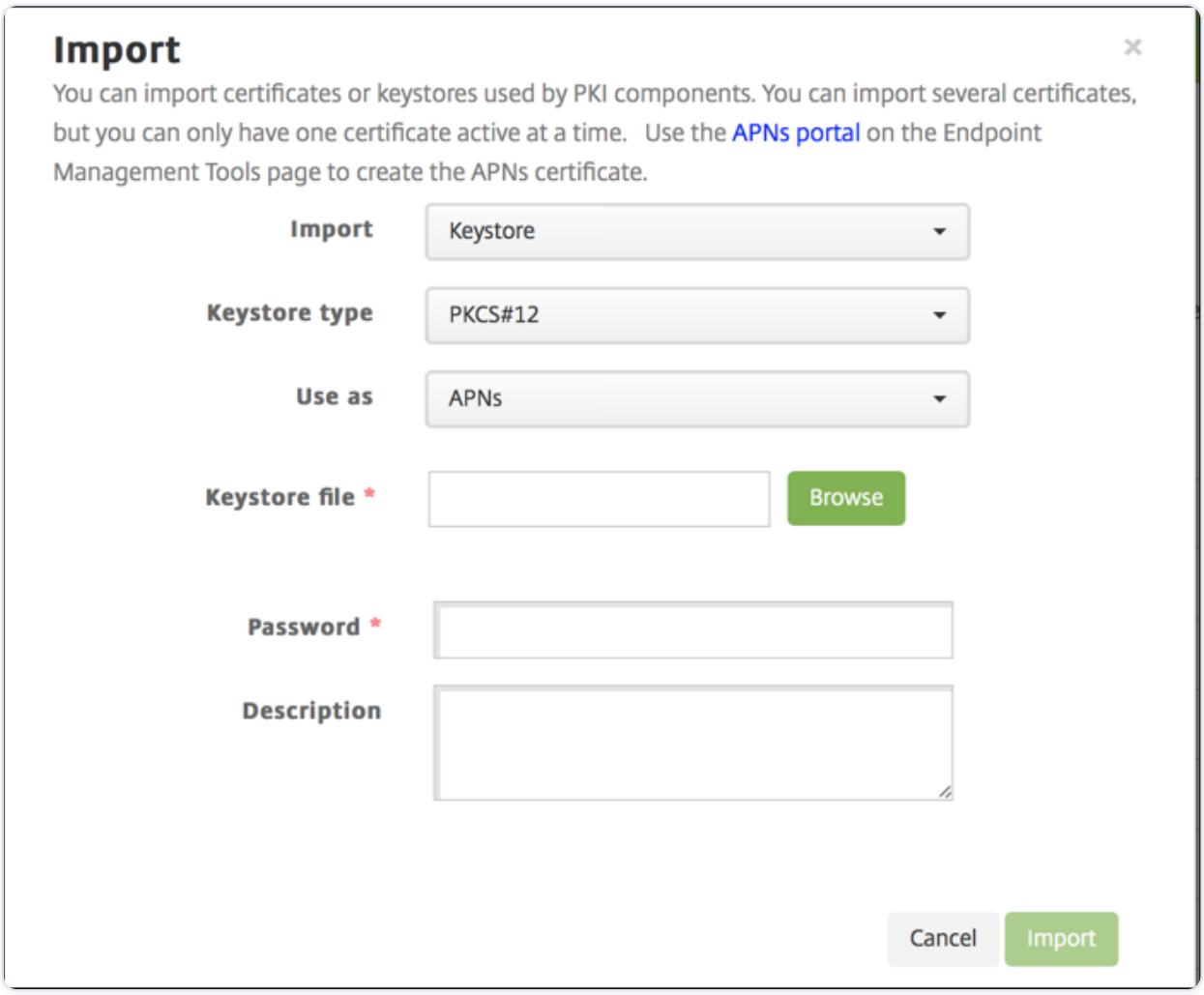
要确定 APNs 证书何时到期，请在 Citrix Endpoint Management 控制台中，转到“**设置 > 证书**”。如果证书到期，请勿吊销它。

1. 使用 Microsoft IIS、钥匙串访问 (macOS) 或 OpenSSL 生成 CSR。有关生成 CSR 的详细信息，请参阅创建证书签名请求。
2. 在浏览器中，转到 Citrix Endpoint Management 工具。然后，单击“**请求推送通知证书签名**”。
3. 单击“**+ 上传 CSR**”。
4. 在对话框中，导航到 CSR，单击“**打开**”，然后单击“**签名**”。

5. 收到 `.plist` 文件后，请保存它。
6. 在步骤 3 标题中，单击“**Apple 推送证书门户**”并登录。
7. 选择要续订的证书，然后单击“**续订**”。
8. 上传 `.plist` 文件。您会收到一个 .pem 文件作为输出。保存该 .pem 文件。
9. 使用该 .pem 文件，完成 CSR（根据您在步骤 1 中创建 CSR 的方法）。
10. 将证书导出为 .pfx 文件。

在 Citrix Endpoint Management 控制台中，导入 .pfx 文件并按如下方式完成配置：

1. 转到 **设置 > 证书 > 导入**。
2. 从**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. 从**用作**中，选择 **APNs**。



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. 键入可选的**描述**。
8. 单击 **Import**。

Citrix Endpoint Management 会将您重定向回**证书**页面。**名称**、**状态**、**有效期从**和**有效期至**字段会更新。

用于 Citrix Files 单点登录的 SAML

> **免责声明：**

> 如果 ShareFile（现为 Progress）停止支持，此功能将被弃用。

> 您可以配置 Citrix Endpoint Management 和 ShareFile 以使用安全断言标记语言 (SAML) 为 Citrix Files 移动应用程序提供单点登录 (SSO) 访问。此功能包括：

- 已启用 MAM SDK 或使用 MDX Toolkit 封装的 Citrix Files 应用程序
- 未封装的 Citrix Files 客户端，例如网站、Outlook 插件或同步客户端
- **对于封装的 Citrix Files 应用程序：**登录 Citrix Files 的用户将被重定向到 Citrix Secure Hub 进行用户身份验证并获取 SAML 令牌。成功验证后，Citrix Files 移动应用程序会将 SAML 令牌发送到 ShareFile。首次登录后，用户可以通过 SSO 访问 Citrix Files 移动应用程序。他们还可以将 ShareFile 中的文档附加到 Citrix Secure Mail 邮件中，而无需每次都登录。
- **对于未封装的 Citrix Files 客户端：**使用 Web 浏览器或其他 Citrix Files 客户端登录 Citrix Files 的用户将被重定向到 Citrix Endpoint Management。Citrix Endpoint Management 会对用户进行身份验证，然后用户获取一个 SAML 令牌并将其发送到 ShareFile。首次登录后，用户可以通过 SSO 访问 Citrix Files 客户端，而无需每次都登录。

要将 Citrix Endpoint Management 用作 ShareFile 的 SAML 身份提供程序 (IdP)，您必须按照本文所述配置 Citrix Endpoint Management 以用于企业帐户。或者，您可以将 Citrix Endpoint Management 配置为仅与存储区域连接器配合使用。有关详细信息，请参阅 ShareFile 与 Citrix Endpoint Management 的使用。

有关详细的参考体系结构图，请参阅 体系结构。

先决条件

在配置 Citrix Endpoint Management 和 Citrix Files 应用程序的 SSO 之前，请完成以下先决条件：

- 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 Citrix Endpoint Management 兼容性。

- 兼容版本的 Citrix Files 移动应用程序和 Citrix Secure Hub。
- ShareFile 管理员帐户。
- Citrix Endpoint Management 与 ShareFile 之间的连接已验证。

配置 ShareFile 访问

在为 ShareFile 设置 SAML 之前，请按如下方式提供 ShareFile 访问信息：

1. 在 Citrix Endpoint Management Web 控制台中，单击“**配置 > ShareFile**”。此时将显示“**ShareFile**”配置页面。

   ShareFile 配置设置(/en-us/citrix-endpoint-management/media/configure-content-collaboration-saml-for-non-mdx-apps.png)

2. 配置以下设置：

   - **域：** 键入您的 ShareFile 子域名。例如：`example.sharefile.com`。
   - **分配给交付组：** 选择或搜索要能够与 ShareFile 配合使用 SSO 的交付组。
   - **ShareFile 管理员帐户登录**
   - **用户名：** 键入 ShareFile 管理员用户名。此用户必须具有管理员权限。
   - **密码：** 键入 ShareFile 管理员密码。
   - **用户帐户预配：** 将此设置保持禁用状态。使用 ShareFile 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**”以验证 ShareFile 管理员帐户的用户名和密码是否已通过指定 ShareFile 帐户的身份验证。
4. 点击 **保存**。

   - Citrix Endpoint Management 与 ShareFile 同步并更新 ShareFile 设置“**ShareFile 颁发者/实体 ID**”和“**登录 URL**”。
   - “**配置 > ShareFile**”页面显示“**应用程序内部名称**”。您需要此名称才能完成 (#modify-the-citrix-filescom-sso-settings) 中稍后描述的步骤。

为封装的 Citrix Files MDX 应用程序设置 SAML

对于使用 MAM SDK 准备的 Citrix Files 应用程序，您无需使用 NetScaler Gateway 进行单点登录配置。要为非封装的 Citrix Files 客户端（例如网站、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 NetScaler Gateway。

要为封装的 Citrix Files MDX 应用程序配置 SAML：

1. 下载适用于 Citrix Endpoint Management 客户端的 ShareFile。请参阅 ShareFile 工具/应用程序下载。
2. 使用 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 Citrix Endpoint Management 控制台中，上传已准备好的 Citrix Files 移动应用程序。有关上传 MDX 应用程序的信息，请参阅 将 MDX 应用程序添加到 Citrix Endpoint Management。
4. 验证 SAML 设置：使用您之前配置的管理员用户名和密码登录 ShareFile。
5. 验证 ShareFile 和 Citrix Endpoint Management 是否配置为相同的时区。确保 Citrix Endpoint Management 显示配置时区的正确时间。否则，SSO 可能会失败。

验证 Citrix Files 移动应用程序

1. 在用户设备上，安装并配置 Citrix 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 将在不提示输入用户名或密码的情况下启动。

使用 Citrix Secure Mail 进行验证

1. 在用户设备上，如果尚未完成，请安装并配置 Citrix Secure Hub。
2. 从应用商店下载、安装并设置 Citrix Secure Mail。
3. 打开新的电子邮件表单，然后点击“**从 ShareFile 附加**”。无需输入用户名或密码即可显示可附加到电子邮件的文件。

为其他 Citrix Files 客户端配置 NetScaler Gateway

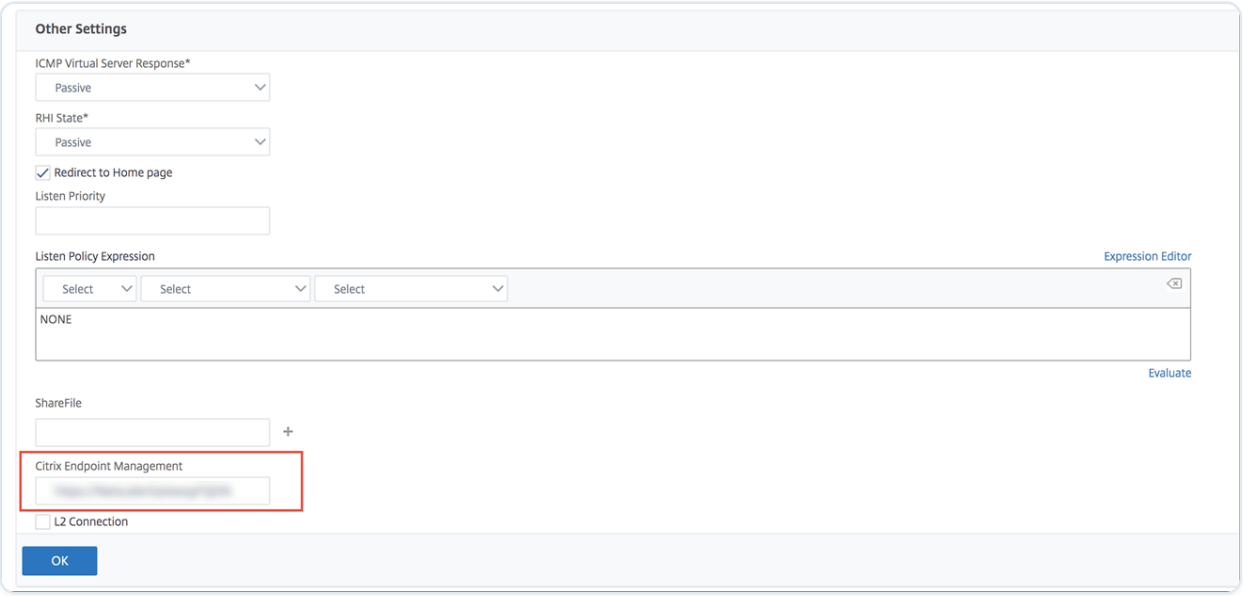
要为非封装的 Citrix Files 客户端（例如网站、Outlook 插件或同步客户端）配置访问权限，请按如下方式配置 NetScaler Gateway 以支持使用 Citrix Endpoint Management 作为 SAML 身份提供程序。

- 禁用主页重定向。
- 创建 Citrix Files 会话策略和配置文件。
- 在 NetScaler Gateway 虚拟服务器上配置策略。

禁用主页重定向

禁用通过 /cginfra 路径发出的请求的默认行为。此操作使用户能够看到原始请求的内部 URL，而不是配置的主页。

1. 编辑用于 Citrix Endpoint Management 登录的 NetScaler Gateway 虚拟服务器的设置。在 NetScaler Gateway 中，转到“**其他设置**”，然后清除标记为“**重定向到主页**”的复选框。



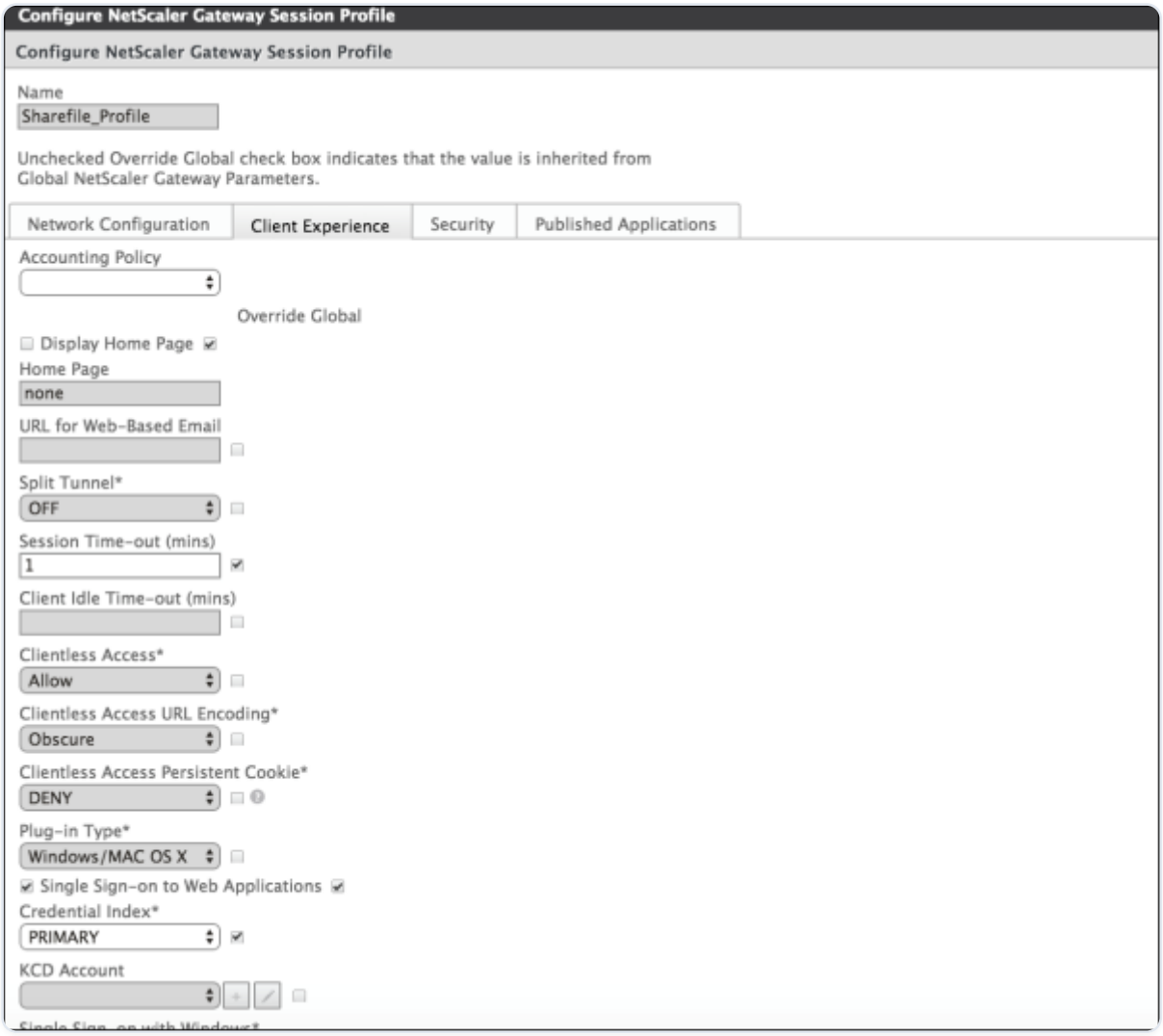
2. 在“**ShareFile**”（现在称为 ShareFile）下，键入您的 Citrix Endpoint Management 内部服务器名称和端口号。
3. 在 **Citrix Endpoint Management** 下，输入其 URL。

   此配置授权通过 /cginfra 路径对您输入的 URL 发出请求。

创建 Citrix Files 会话策略和请求配置文件

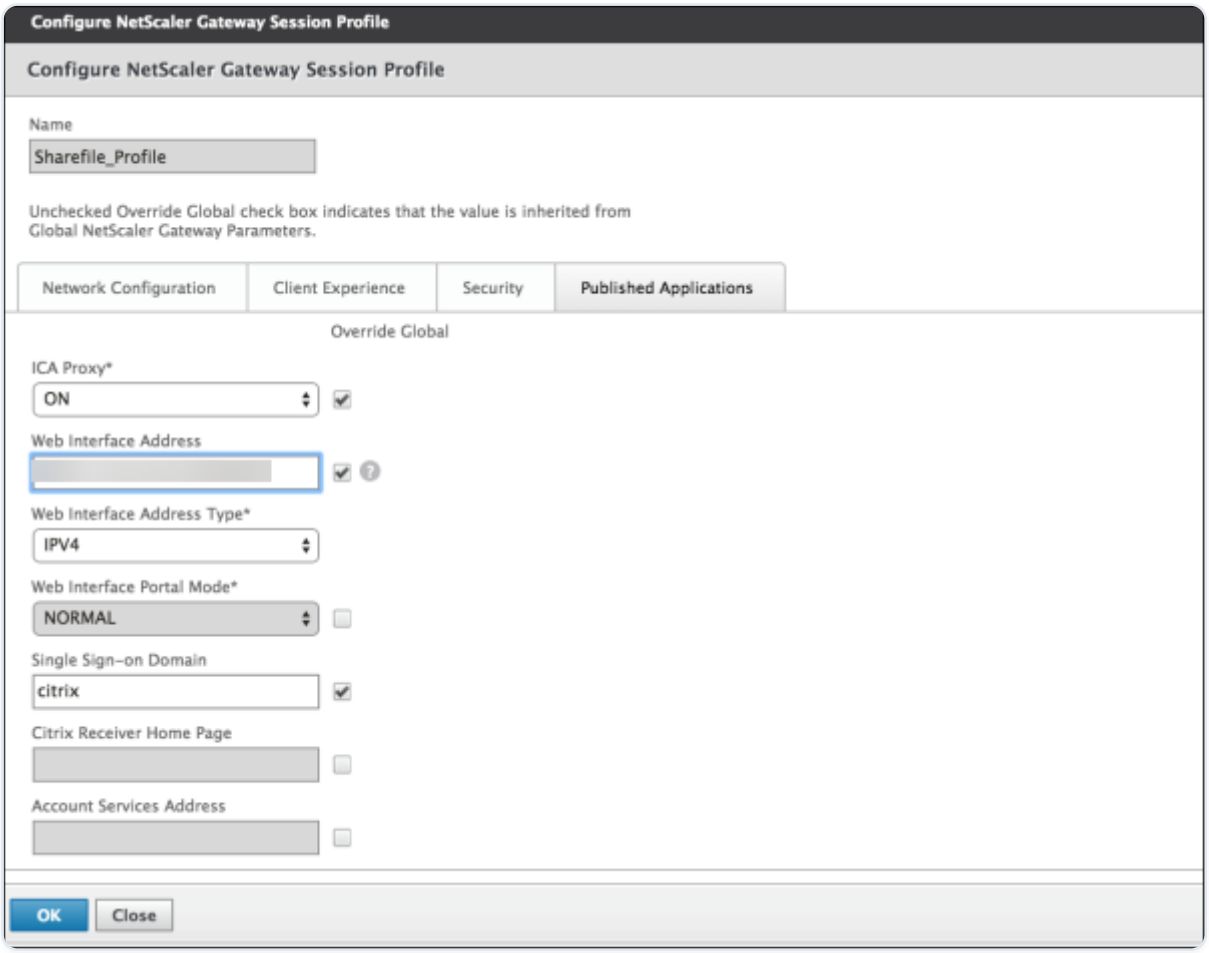
配置以下设置以创建 Citrix Files 会话策略和请求配置文件：

1. 在 NetScaler Gateway 配置实用程序中，在左侧导航窗格中，单击 **NetScaler Gateway > 策略 > 会话**。
2. 创建会话策略。在**策略**选项卡上，单击**添加**。
3. 在**名称**字段中，键入 **ShareFile_Policy**。
4. 通过单击 **+** 按钮创建操作。此时将显示**创建 NetScaler® Gateway 会话配置文件**页面。



配置以下设置：

- **名称：** 键入 **ShareFile_Profile**。
- 单击**客户端体验**选项卡，然后配置以下设置：
  - **主页：** 键入 **none**。
  - **会话超时（分钟）：** 键入 **1**。
  - **Web 应用程序的单点登录：** 选择此设置。
  - **凭据索引：** 单击**主要**。
- 单击**已发布的应用程序**选项卡。

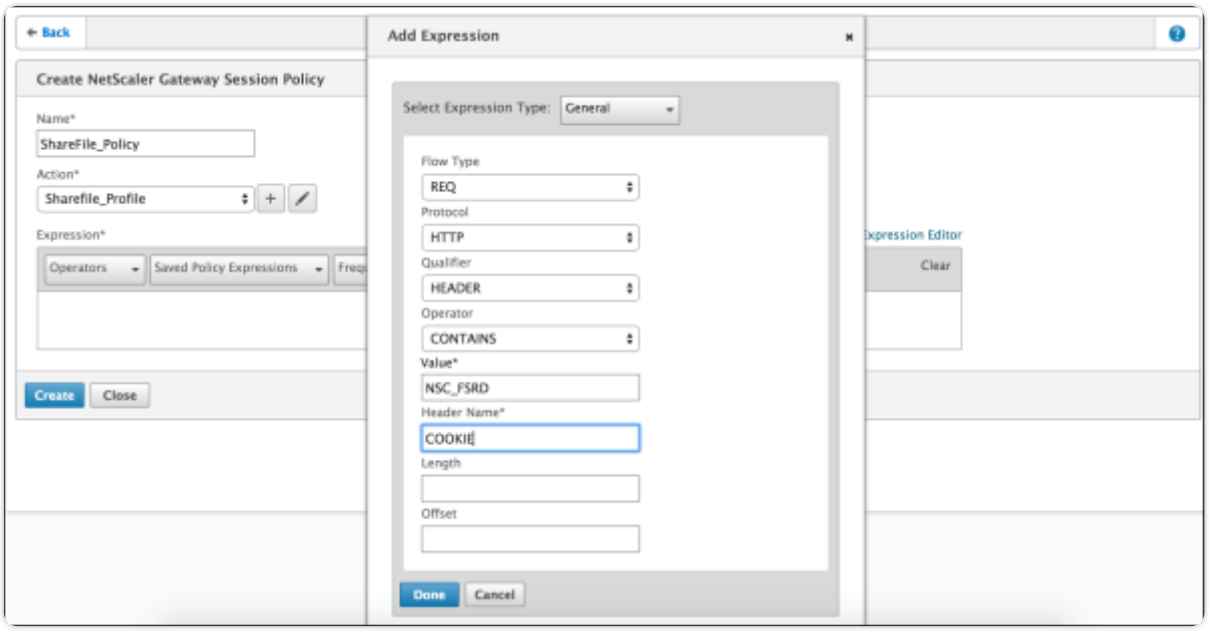


配置以下设置：

- **ICA® 代理：** 单击 **开**。
- **Web 界面地址：** 键入您的 Citrix Endpoint Management 服务器 URL。
- **单点登录域：** 键入您的 Active Directory 域名。

  配置 NetScaler Gateway 会话配置文件时，**单点登录域**的域后缀必须与 LDAP 中定义的 Citrix Endpoint Management 域别名匹配。

5. 单击 **创建** 以定义会话配置文件。
6. 单击 **表达式编辑器**。



配置以下设置：

- **值：** 键入 **NSC_FSRD**。
- **标头名称：** 键入 **COOKIE**。

7. 单击 **创建**，然后单击 **关闭**。



在 NetScaler Gateway 虚拟服务器上配置策略

在 NetScaler Gateway 虚拟服务器上配置以下设置。

1. 在 NetScaler Gateway 配置实用程序中，在左侧导航窗格中，单击 **NetScaler Gateway > 虚拟服务器**。
2. 在**详细信息**窗格中，单击您的 NetScaler Gateway 虚拟服务器。
3. 单击**编辑**。
4. 单击**已配置的策略 > 会话策略**，然后单击**添加绑定**。
5. 选择 **ShareFile_Policy**。

6. 编辑所选策略的自动生成**优先级**数字，使其相对于列出的任何其他策略具有最高优先级（最小的数字）。例如：

   VPN 虚拟服务器会话策略绑定屏幕(/en-us/citrix-endpoint-management/media/configure-sharefile-ns-config-policies-on-nsg-vs.png)

7. 单击**完成**，然后保存正在运行的 NetScaler Gateway 配置。

修改 Citrix Files.com SSO 设置

对 MDX 和非 MDX Citrix Files 应用程序进行以下更改。

> **重要提示：**

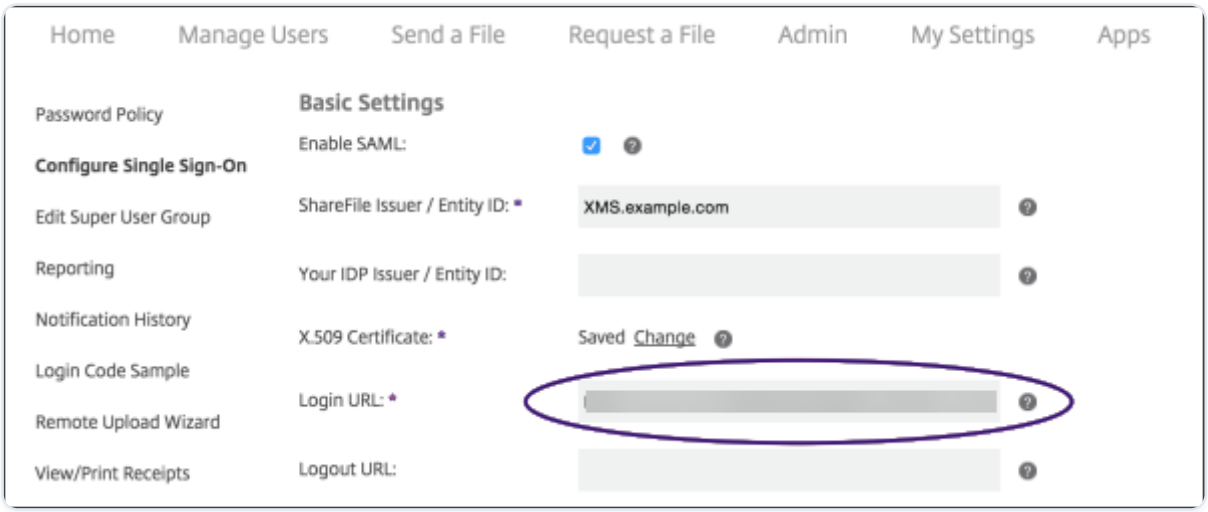
> 新数字将附加到内部应用程序名称：

> - 每次编辑或重新创建 Citrix Files 应用程序时
> - 每次更改 Citrix Endpoint Management 中的 ShareFile 设置时

> 因此，您还必须更新 Citrix Files 网站中的登录 URL，以显示更新后的应用程序名称。

1. 以 ShareFile 管理员身份登录您的 ShareFile 帐户 (`https://<subdomain>.sharefile.com`)。
2. 在 ShareFile Web 界面中，单击**管理员**，然后选择**配置单点登录**。
3. 按如下方式编辑**登录 URL**：

   以下是编辑前的**登录 URL** 示例：`https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`。



- 在 Citrix Endpoint Management 服务器 FQDN 前面插入 NetScaler Gateway 虚拟服务器外部 FQDN 和 **/cginfra/https/**，然后在 Citrix Endpoint Management FQDN 后面添加 **8443**。

  以下是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

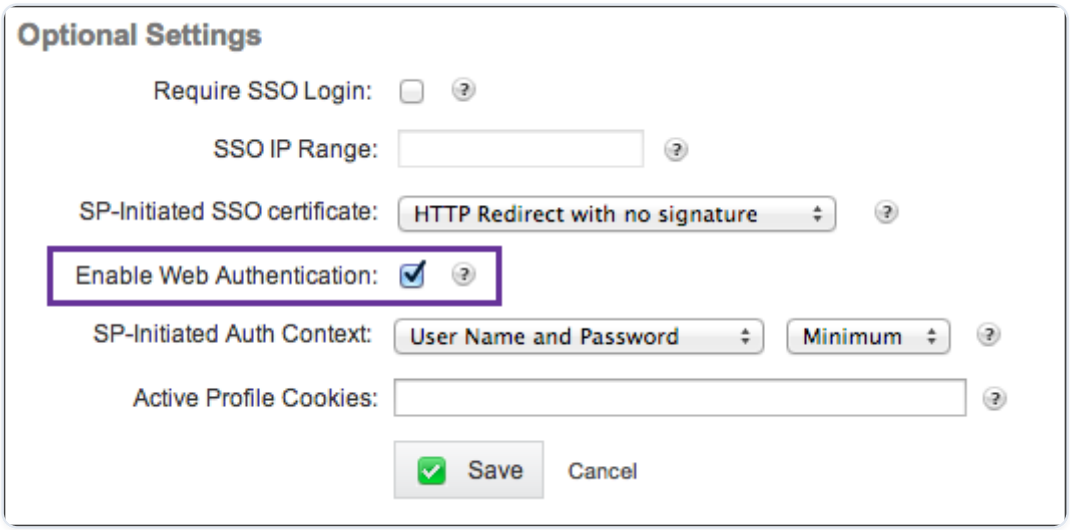
- 将参数 `&app=ShareFile_SAML_SP` 更改为内部 Citrix Files 应用程序名称。内部名称默认为 `ShareFile_SAML`。但是，每次更改配置时，内部名称后面都会附加一个数字（`ShareFile_SAML_2`、`ShareFile_SAML_3` 等）。您可以在**配置 > ShareFile** 页面上查找**应用程序内部名称**。

  以下是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- 将 `&nssso=true` 添加到 URL 的末尾。

  以下是最终 URL 的示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`。

4. 在**可选设置**下，选中**启用 Web 身份验证**复选框。



验证配置

执行以下操作以验证配置。

1. 将浏览器指向 `https://<subdomain>sharefile.com/saml/login`。

   您将被重定向到 NetScaler Gateway 登录表单。如果您未被重定向，请验证前面的配置设置。

2. 输入您已配置的 NetScaler Gateway 和 Citrix Endpoint Management 环境的用户名和密码。

   您在 `<subdomain>.sharefile.com` 的 Citrix Files 文件夹将显示。如果您没有看到您的 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

Citrix 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 Secure Hub 注册 MDM 的用户。

要将 Citrix Secure Hub 与 MDM+MAM 结合使用，请将 Citrix Endpoint Management 配置为使用 NetScaler Gateway 进行 MAM 注册。有关详细信息，请参阅 NetScaler Gateway 和 Citrix Endpoint Management。

Citrix Endpoint Management 使用 Citrix Cloud 服务（Citrix 身份）与 Azure Active Directory 联合。Citrix 建议您使用 Citrix 身份提供程序，而不是直接连接到 Azure Active Directory。

Citrix Endpoint Management 支持 Azure AD 对以下平台进行身份验证：

- 未注册 Apple Business Manager 或 Apple School Manager 的 iOS 和 macOS 设备
- 已注册 Apple Business Manager 的 iOS 和 macOS 设备
- Android Enterprise 设备（预览版），适用于 BYOD 和完全托管模式

通过 Citrix Cloud 使用 Azure AD 进行身份验证存在以下限制：

- 不适用于 Citrix Endpoint Management 本地帐户。
- 不支持通过 Azure AD 进行注册邀请的身份验证。如果您向用户发送包含注册 URL 的注册邀请，用户将通过 LDAP 而不是 Azure AD 进行身份验证。

先决条件

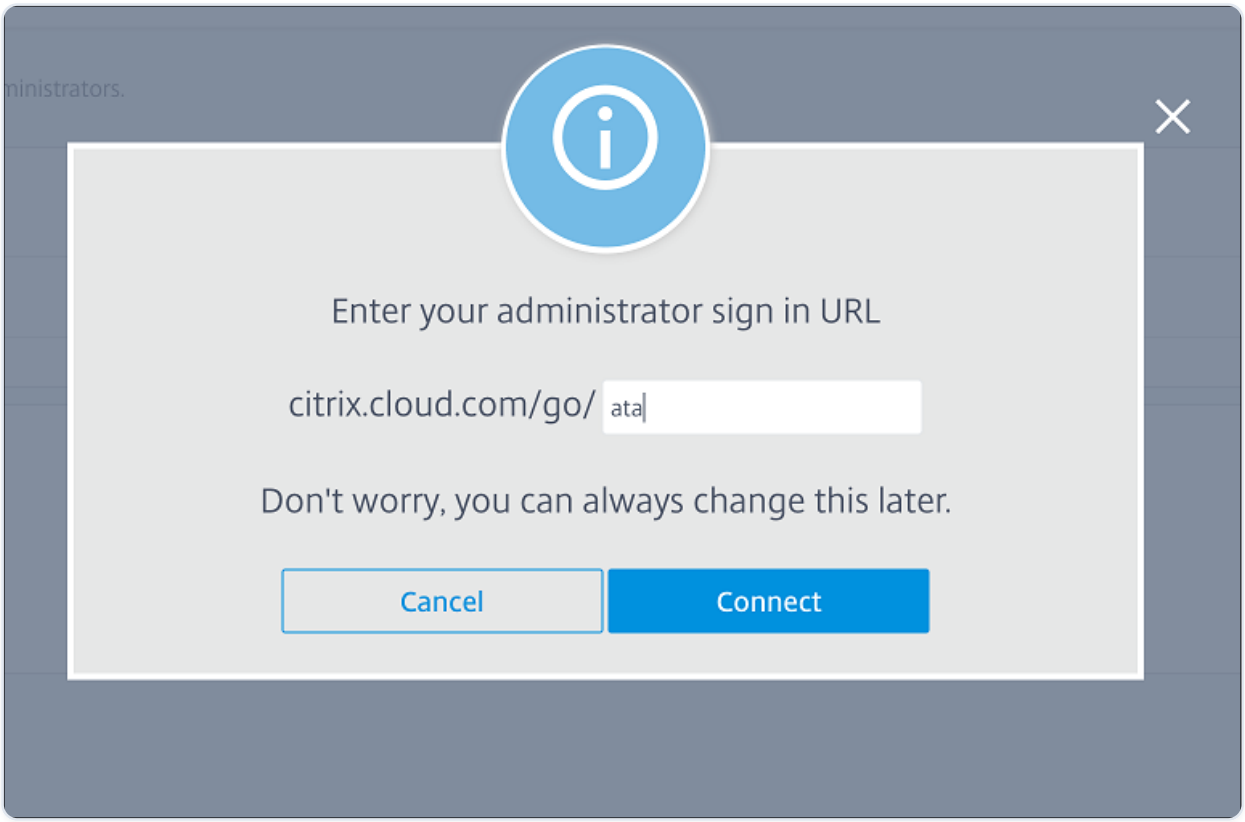
> **注意：**
>
> 不支持独立的 Azure Active Directory，与 Citrix Endpoint Management 集成需要本地 Active Directory。

- 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 中的用户名和电子邮件地址匹配。
- Citrix Cloud 帐户，并安装了 Citrix Cloud Connector 以进行目录服务同步。
- NetScaler Gateway。Citrix 建议您启用基于证书的身份验证或 Azure AD，以获得完整的单点登录体验。如果您在 NetScaler Gateway 上使用 LDAP 身份验证进行 MAM 注册，则最终用户在注册期间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。
- 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，他们将无法使用身份提供程序进行身份验证来注册。有关详细信息，请参阅注册安全性。

将 Citrix Cloud 配置为使用 Azure Active Directory 作为身份提供程序

要设置此服务以与 Citrix Secure Hub 配合使用，请在 Citrix Cloud 中配置 Azure Active Directory。

1. 转至 https://citrix.cloud.com 并登录您的 Citrix Cloud 帐户。
2. 从 Citrix Cloud 菜单中，转至**身份和访问管理**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。**身份和访问管理 > 身份验证**页面显示用于登录您的 Citrix Cloud 和 Azure AD 帐户的帐户。
5. 要为通过 Citrix Secure Hub 注册的用户启用 Azure AD 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 Secure Hub 注册用户设备。

将 Citrix 身份配置为 Citrix Endpoint Management 的 IdP 类型

此配置仅适用于通过 Citrix Secure Hub 注册的用户。在 Citrix Cloud 中配置 Azure Active Directory 后，请按如下方式配置 Citrix Endpoint Management。

1. 在 Citrix 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：** 输入一个唯一的名称以标识您正在创建的 IdP 连接。
   - **IDP 类型：** 选择 **Citrix Identity Platform**。
   - **身份验证域：** 选择 **Azure Active Directory**。此域对应于 Citrix Cloud **工作区配置 > 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** 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**。请确保在本地 Active Directory 和 Azure Active Directory 中使用相同的标识符配置所有用户。Citrix Endpoint

Management 使用此标识符将身份提供程序上的用户与本地 Active Directory 用户进行映射。

- **用户标识符字符串：** 此字段将自动填充。

4. 单击 **下一步**，查看 **摘要** 页面，然后单击 **保存**。

   Citrix Secure Hub 用户、Citrix Endpoint Management 控制台用户和自助服务门户用户现在可以使用其 Azure Active Directory 凭据登录。已加入域的 Citrix Secure Hub 用户可以使用 Citrix Secure Hub 登录其 Azure AD 凭据。Citrix Secure Hub 对 MAM 设备使用客户端证书身份验证。

Citrix Secure Hub 身份验证流程

Citrix Endpoint Management 使用以下流程通过 Azure AD 作为 IdP 对通过 Citrix Secure Hub 注册的设备上的用户进行身份验证：

1. 用户启动 Citrix Secure Hub。
2. Citrix Secure Hub 将身份验证请求传递给 Citrix identity，后者将请求传递给 Azure Active Directory。
3. 用户键入其 Azure Active Directory 用户名和密码。
4. Azure Active Directory 验证用户并将代码发送给 Citrix identity。
5. Citrix identity 将代码发送给 Citrix Secure Hub，后者将代码发送给 Citrix Endpoint Management 服务器。
6. Citrix Endpoint Management 通过使用代码和密钥获取 ID 令牌，然后验证 ID 令牌中的用户信息。Citrix Endpoint Management 返回一个会话 ID。

使用 Azure Active Directory 基于组的管理进行身份验证

Citrix Endpoint Management 现在支持通过 Azure Active Directory (AAD) 访问其服务的基于组的身份验证。此更新确保管理员可以使用 AAD 组成员身份在组级别管理访问，从而提供灵活性和增强的安全性。传统的 Citrix Identity 登录机制仍可作为替代方案使用。

主要增强功能

- **Azure AD 组集成**：管理员现在可以通过利用 Azure AD 组来管理用户对 CEM 服务的访问。这简化了权限管理并允许基于组的访问控制。
- **使用 Azure AD 组进行 Citrix Endpoint Management 登录身份验证**：用户可以通过 Azure AD 组进行身份验证，从而与现有组织身份基础架构实现无缝集成。

- **传统 Citrix Identity 支持**：Citrix Identity 登录仍然可用，确保用户可以按照自己的节奏进行过渡。

功能标志

- **Citrix Cloud™ 功能标志**：`fullAccessGroups` – 此功能默认启用，以允许组的完全访问。
- **Citrix Endpoint Management 功能标志**：`cc.group.based.admin` – 在 Citrix Endpoint Management 中启用基于组的管理功能。

先决条件

- Azure AD 在 Citrix Cloud 门户中配置。
- 需要设置 Citrix Cloud 的管理员登录 URL，以便通过 Azure AD 组访问 Citrix Endpoint Management。

配置步骤

1. 登录 Azure 门户并访问 Azure Active Directory。
2. 导航到“用户”并选择“创建新用户”。
3. 导航到“组”，单击“新建组”，然后将新创建的用户添加为该组的成员。
4. 使用管理员凭据登录到 Citrix Cloud。
5. 导航到“身份和访问管理”，为新的 Azure AD 组分配完全权限或自定义权限。
6. Azure AD 组中的用户现在可以使用管理员登录 URL 登录到 Citrix Endpoint Management™。

通过 NetScaler Gateway 使用 Azure Active Directory 进行 MAM 注册的身份验证

Citrix Endpoint Management 支持通过 NetScaler Gateway 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 Secure Hub 注册 MAM 的用户。

先决条件

要将 Citrix Endpoint Management 配置为通过 NetScaler Gateway 使用 Azure AD 作为 MAM 注册设备的身份提供程序 (IdP)，请确保满足以下先决条件：

- 将 Citrix Endpoint Management 配置为通过 Citrix Cloud 使用 Azure AD 作为 MDM 注册设备的 IdP。有关为 MDM 配置 Azure AD 的详细信息，请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。

- 将 Azure AD 连接到 Citrix Cloud。有关详细信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。
- 根据平台分别启用以下相关功能标志：
  - iOS：
    - iOS-V3表单-MAM
    - iOS-SAML认证-MAM
  - 安卓：
    - Android-V3表单-MAM
    - Android-SAML认证-MAM

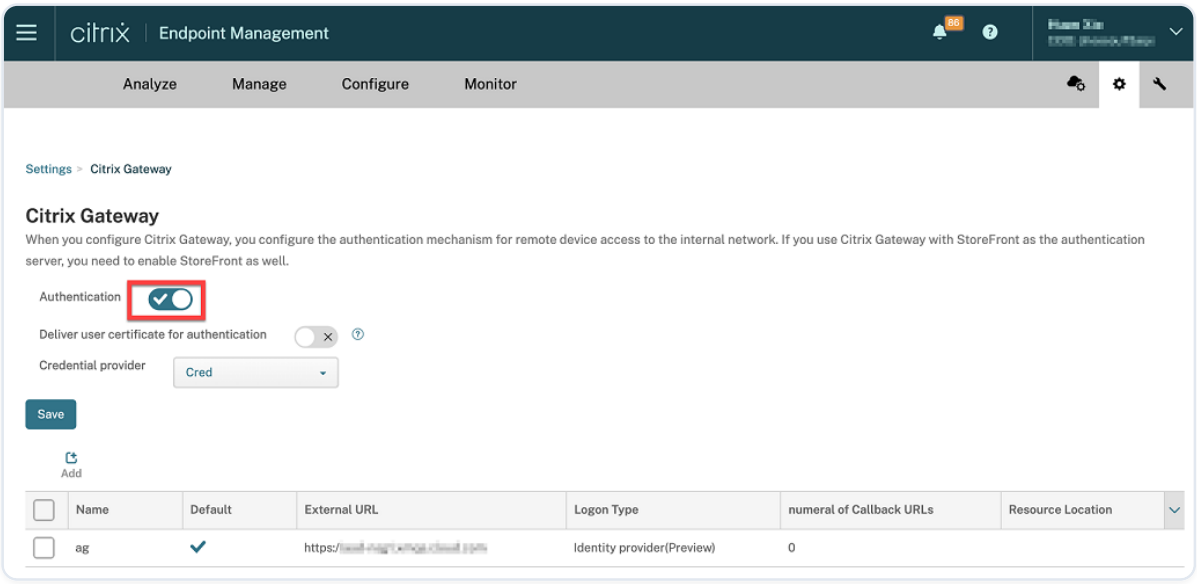
> **注意：**
>
> 要启用此功能，请联系您的支持团队。

- 对于安卓，启用 **Android Enterprise**。

> **注意：**
>
> 此功能未在旧版 Android 设备管理员 (DA) 模式下进行测试或验证。不支持此模式。

将 Azure AD 配置为 MAM 的 IdP

1. 在 Citrix Endpoint Management 中按如下方式配置 NetScaler Gateway：
   a. 登录到 Citrix Endpoint Management 控制台，然后单击“**设置**”⚙ 图标。
   b. 在“**服务器**”下单击“**NetScaler Gateway**”。
   c. 启用“**身份验证**”切换按钮。



d. 确保网关的“**登录类型**”为*身份提供程序*。

e. 点击 **保存**。

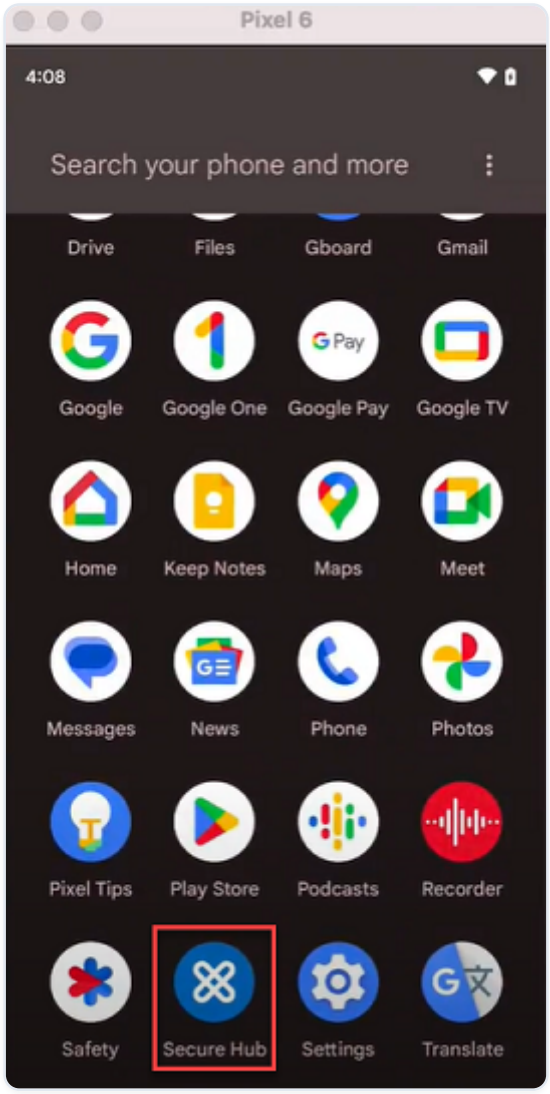
2. 使用 将 Azure AD 配置为 SAML IdP 将 Azure AD 配置为 SAML IdP。
3. 使用高级策略，通过 将 NetScaler ADC 配置为 SAML 服务提供程序 (SP) 将 NetScaler ADC 配置为 SAML SP。
4. 使用 通过 GUI 设置身份验证虚拟服务器 创建 AAA 虚拟服务器。
5. 使用 配置身份验证虚拟服务器 配置 AAA 虚拟服务器。
6. 使用 身份验证配置文件 创建和配置身份验证配置文件。
7. 将身份验证配置文件绑定到网关虚拟服务器并保存所有配置。

现在，Azure AD 已添加为注册了 MAM 的设备的身份提供程序，您可以使用 Azure AD 对其进行身份验证。

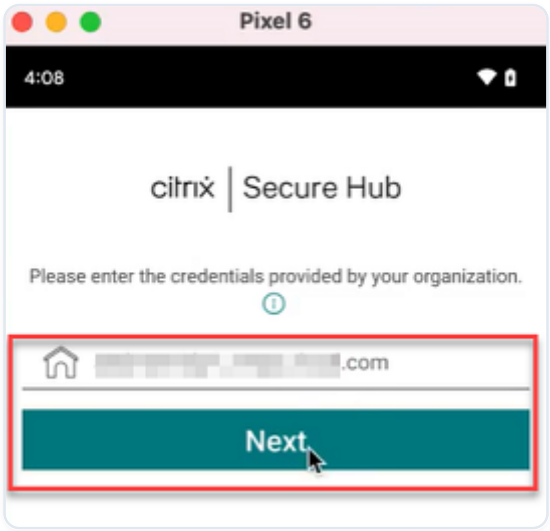
预期行为

以下示例使用 Android 设备：

1. 在您的移动设备上，打开 Citrix Secure Hub 应用程序。

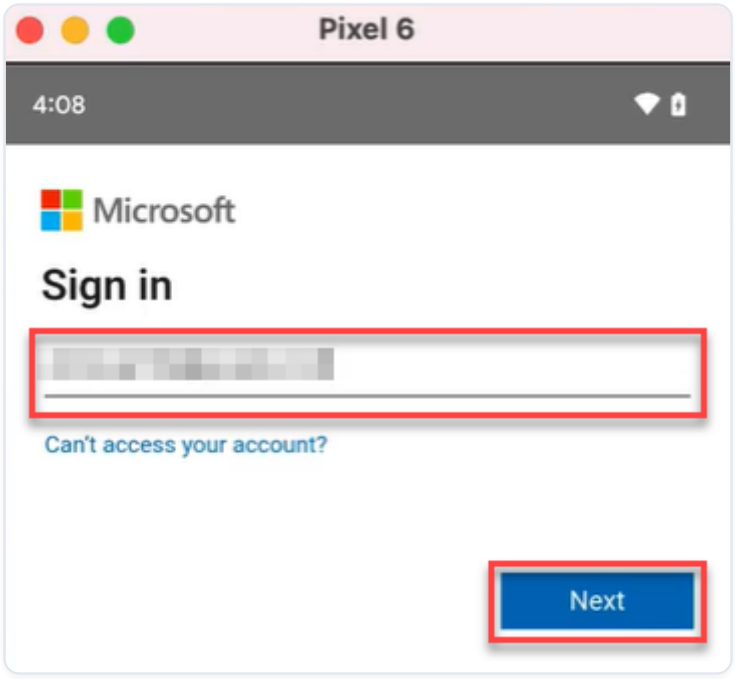


2. 提供所需的权限。
3. 在登录页面上，输入您的组织提供的凭据，然后点击 **Next**。

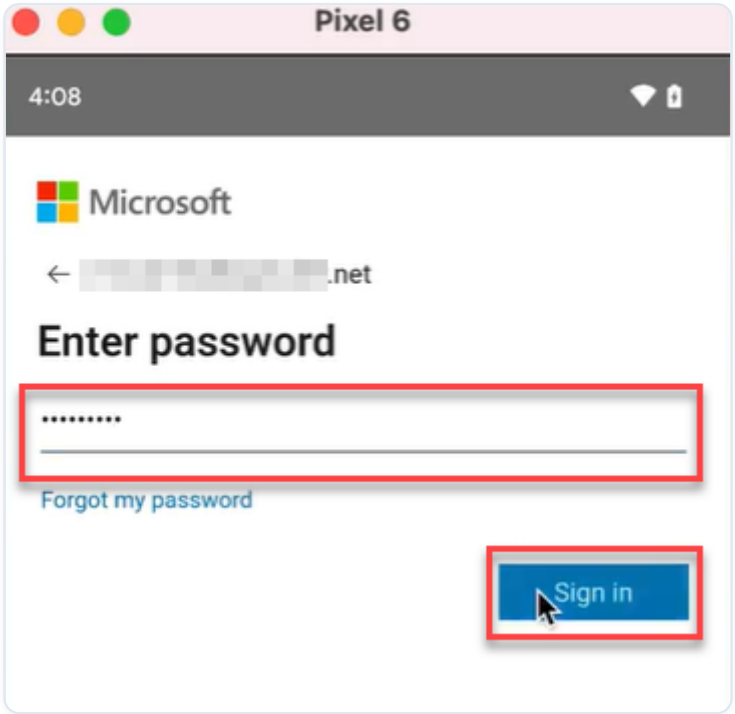


您将被重定向到 Microsoft 登录页面。

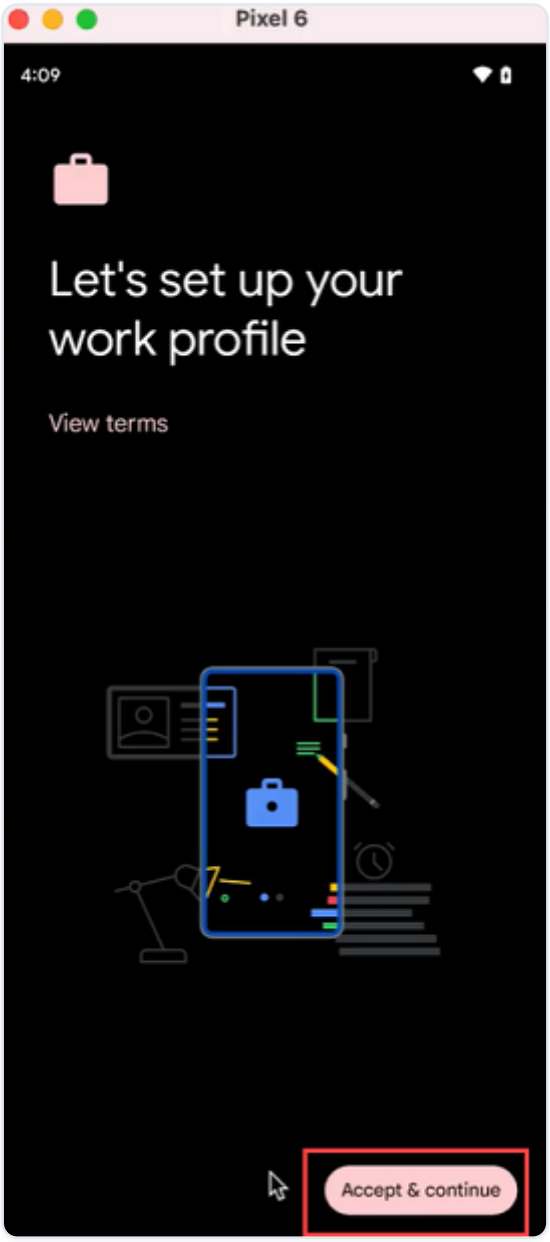
4. 在 Microsoft 登录页面上，输入您的电子邮件 ID，然后点击 **Next**。



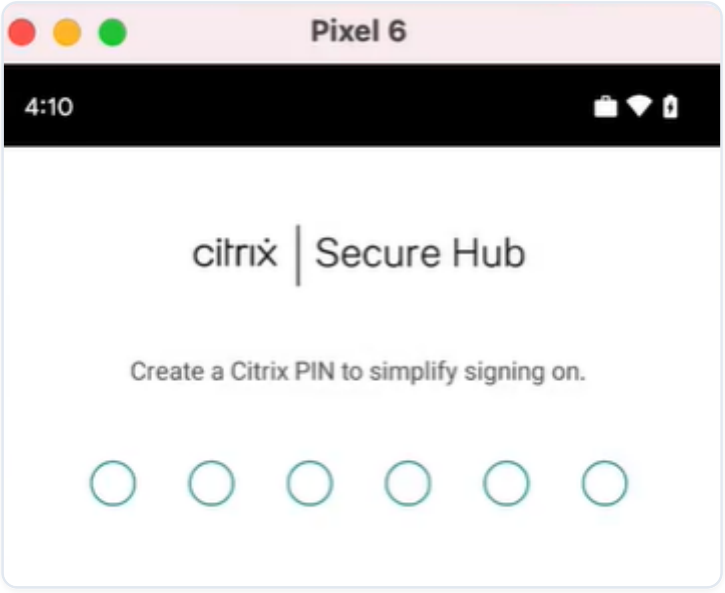
5. 输入密码，然后点击 **Sign in**。



6. 在“**设置您的工作配置文件**”页面上，点击“**接受并继续**”。



7. 为 Citrix Secure Hub 应用程序创建 PIN 并确认。



您已成功重定向到 Citrix Secure Hub 主页。

通过 Citrix Cloud 使用 Okta 进行身份验证

Citrix 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 Secure Hub 注册 MDM 的用户。

注册 MAM 的设备无法通过 Citrix Cloud 使用 Okta 凭据进行身份验证。要将 Citrix Secure Hub 与 MDM+MAM 结合使用，请将 Citrix Endpoint Management 配置为使用 NetScaler Gateway 进行 MAM 注册。有关详细信息，请参阅 NetScaler Gateway 和 Citrix Endpoint Management。

Citrix 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，而不是直接连接到 Okta。

Citrix Endpoint Management 支持以下平台通过 Okta 进行身份验证：

- 未注册 Apple Business Manager 或 Apple School Manager 的 iOS 和 macOS 设备
- 已注册 Apple Business Manager 的 iOS 和 macOS 设备
- Android Enterprise 设备（预览版），适用于 BYOD 和完全托管模式

通过 Citrix Cloud 使用 Okta 进行身份验证存在以下限制：

- 不适用于 Citrix Endpoint Management 本地帐户。
- 不支持通过 Okta 进行注册邀请的身份验证。如果您向用户发送包含注册 URL 的注册邀请，则用户将通过 LDAP 而非 Okta 进行身份验证。

先决条件

- Okta 用户凭据
- Active Directory 中的用户组必须与 Okta 中的用户组匹配。
- Active Directory 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匹配。
- 已安装 Citrix Cloud Connector 的 Citrix Cloud 帐户，用于目录服务同步。
- NetScaler Gateway。Citrix 建议您启用基于证书的身份验证以获得完整的单点登录体验。如果您在 NetScaler 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。
- 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**。如果用户拒绝设备管理，他们将无法使用身份提供程序进行身份验证来注册。有关详细信息，请参阅注册安全性。

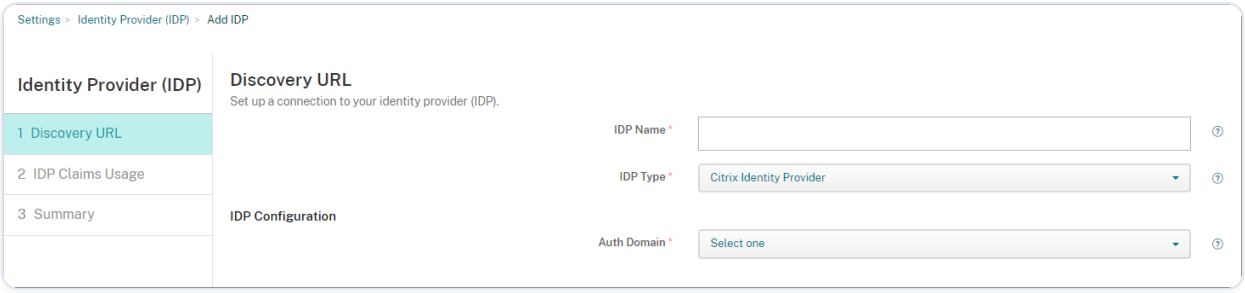
将 Citrix Cloud 配置为使用 Okta 作为身份提供程序

要在 Citrix Cloud 中配置 Okta，请参阅将 Okta 作为身份提供程序连接到 Citrix Cloud。

将 Citrix 身份配置为 Citrix Endpoint Management 的 IdP 类型

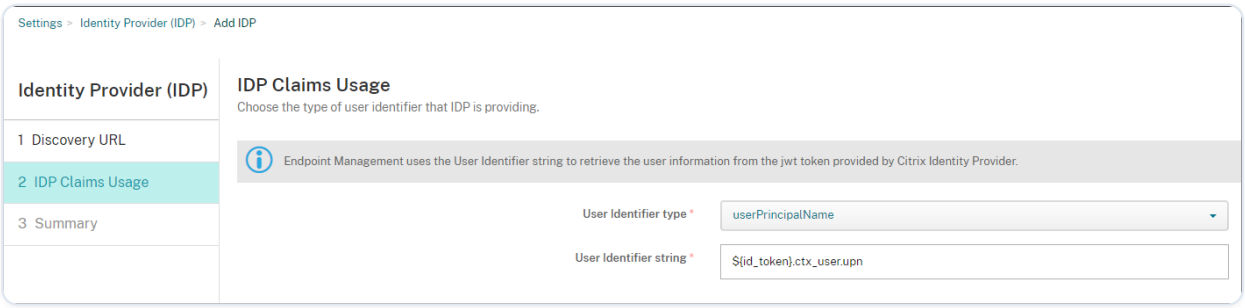
此配置仅适用于通过 Citrix Secure Hub 注册的用户。在 Citrix Cloud 中配置 Azure Active Directory 后，按如下方式配置 Citrix Endpoint Management：

1. 在 Citrix Endpoint Management 控制台中，转到**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：** 键入一个唯一名称以标识您正在创建的 IdP 连接。
- **IDP 类型：** 选择 **Citrix Identity Provider**。
- **身份验证域：** 选择 Citrix Cloud 域。如果您不确定选择哪个域，您的域会显示在 Citrix Cloud 的**身份和访问管理 > 身份验证**页面上。

3. 单击**下一步**。在 **IDP 声明使用**页面上，配置以下内容：



- **用户标识符类型：** 此字段设置为 **userPrincipalName**。请确保在本地 Active Directory 和 Okta 中为所有用户配置相同的标识符。Citrix Endpoint Management 使用此标识符将身份提供程序上的用户与本地 Active Directory 用户进行映射。
- **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 Citrix Secure Hub 用户可以使用 Citrix Secure Hub 及其 Okta 凭据登录。Citrix Secure Hub 对 MAM 设备使用客户端证书身份验证。

Citrix Secure Hub 身份验证流程

Citrix Endpoint Management 使用以下流程通过 Citrix Secure Hub 注册的设备上使用 Okta 作为 IdP 对用户进行身份验证：

1. 用户启动 Citrix Secure Hub。
2. Citrix Secure Hub 将身份验证请求传递给 Citrix identity，后者将请求传递给 Okta。
3. 用户输入其用户名和密码。
4. Okta 验证用户并将代码发送给 Citrix identity。
5. Citrix identity 将代码发送给 Citrix Secure Hub，后者将代码发送给 Citrix Endpoint Management 服务器。
6. Citrix Endpoint Management 使用代码和密钥获取 ID 令牌，然后验证 ID 令牌中的用户信息。Citrix Endpoint Management 返回会话 ID。

通过 NetScaler Gateway 使用 Okta 进行 MAM 注册的身份验证

Citrix Endpoint Management 支持通过 NetScaler Gateway 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 Secure Hub 注册 MAM 的用户。

先决条件

要将 Citrix Endpoint Management 配置为通过 NetScaler Gateway 使用 Okta 作为 MAM 注册设备的身份提供程序 (IdP)，请确保满足以下先决条件：

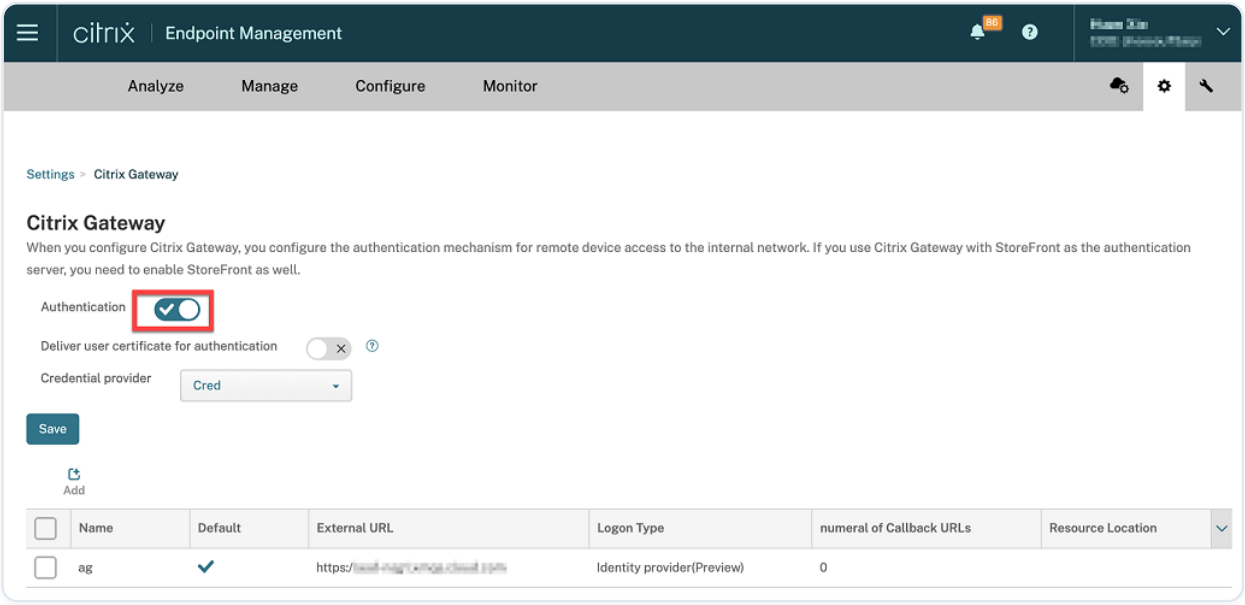
- 将 Citrix Endpoint Management 配置为通过 Citrix Cloud 使用 Okta 作为 MDM 注册设备的 IdP。有关配置 Okta 以用于 MDM 的更多信息，请参阅通过 Citrix Cloud 使用 Okta 进行身份验证。
- 根据平台分别启用以下相关功能标志：
  - iOS：
    - iOS-V3表单-MAM
    - iOS-SAML认证-MAM
  - 安卓：
    - 安卓-V3Form-MAM
    - 安卓-SAMLAuth-MAM

> **注意：**
>
> 要启用此功能，请联系您的支持团队。

- 下载并安装最新版本的 Citrix Secure Hub。
- 确保 Okta 服务可供您的组织使用，并且已在 Okta 中创建或导入相关用户和组。

在 Citrix 端点管理 中配置 NetScaler 网关

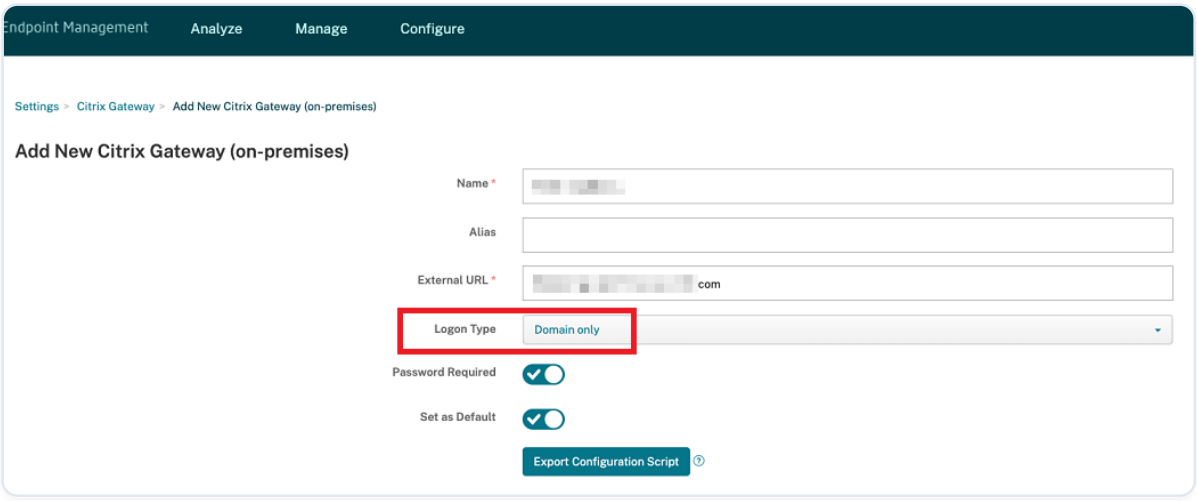
1. 登录 Citrix Endpoint Management 控制台，然后单击**设置** 图标。
2. 在**服务器**下，单击**NetScaler Gateway**。
3. 启用**身份验证**切换按钮。



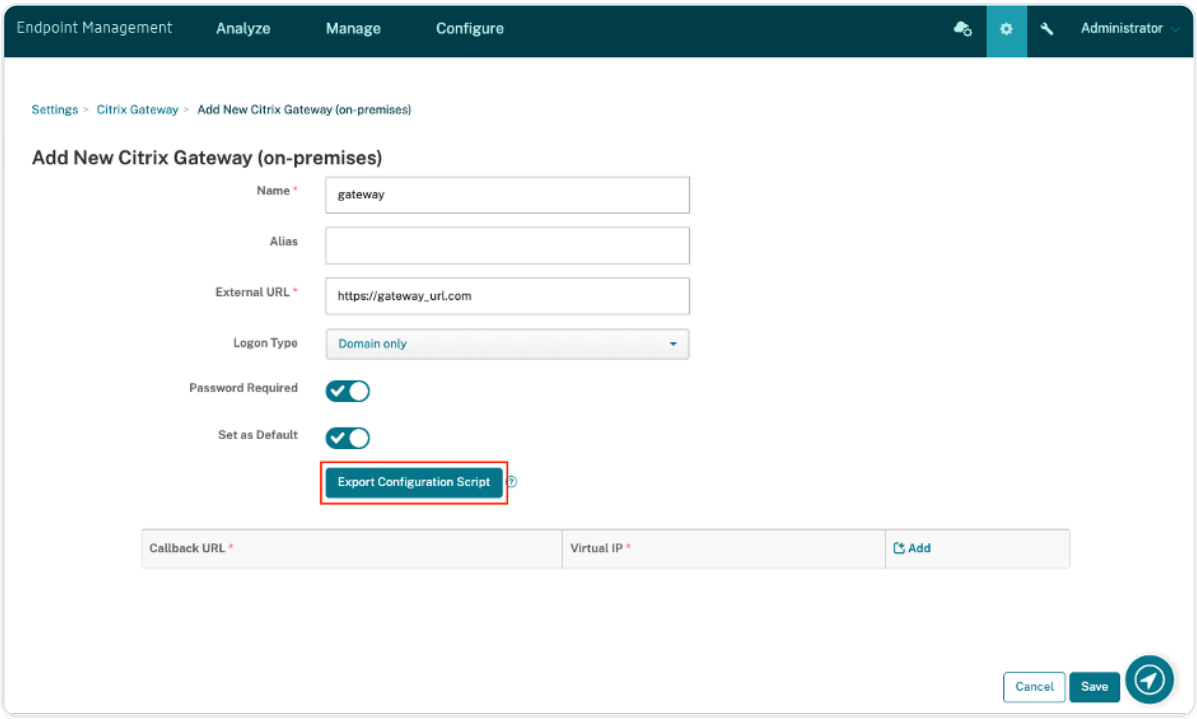
4. 确保网关的**登录类型**为*身份提供程序*。
5. 点击 **保存**。

准备本地 NetScaler Gateway

1. 如果尚未为 Citrix Endpoint Management 配置本地 NetScaler Gateway，请执行以下步骤：
   a. 在 Citrix Endpoint Management 控制台中，单击**设置** 图标。
   b. 在**服务器**下，单击**NetScaler Gateway**。
   c. 单击**编辑**。
   d. 单击**登录类型**下拉菜单，然后选择*仅限域*。



e. 单击**导出配置脚本**。



导出配置脚本已下载。

f. 单击**登录类型**下拉菜单，然后选择*身份提供程序*。

将登录类型更新为身份提供程序(/en-us/citrix-endpoint-management/media/logon-type-identity-provider.png)

g. 点击 **保存**。

h. 打开下载的 zip 文件并从中提取文件。

i. 运行提取的 .txt 文件中的脚本，以准备本地 NetScaler Gateway。

提取 zip 文件信息(/en-us/citrix-endpoint-management/media/export-configuration-script-zip-file.png)

2. 登录 Citrix ADC 管理控制台，然后导航到 **NetScaler Gateway** > **Virtual Servers**。
3. 单击与您的 Citrix Endpoint Management 设置相关的网关。
4. 解除绑定本地 NetScaler Gateway 上的任何现有身份验证策略。

配置 Okta

1. 以管理员身份登录 Okta。
2. 单击 **应用程序** > **应用程序** > **浏览应用目录**。

   在 Okta 中浏览应用程序目录(/en-us/citrix-endpoint-management/media/browse-app-catalog.png)

3. 在 **Browse App Integration Catalog** 下的搜索栏中键入 **NetScaler Gateway**，然后选择 **NetScaler Gateway (SAML, SWA)**。

   在“浏览应用程序集成目录”中搜索 NetScaler Gateway(/en-us/citrix-endpoint-management/media/browse-app-citrix-gateway.png)

4. 单击 **添加集成**。

   NetScaler Gateway 添加集成(/en-us/citrix-endpoint-management/media/citrix-gateway-add-integration.png)

5. 在 **Application label** 字段中输入相关名称。
6. 在 **Login URL** 字段中输入网关虚拟服务器 URL，然后单击 **Next**。

   NetScaler Gateway 常规设置(/en-us/citrix-endpoint-management/media/add-citrix-gateway-general-settings.png)

   > **注意：**
   >
   > 在 **Login URL** 字段中输入的 URL 必须与 Citrix Endpoint Management 设置的 NetScaler Gateway URL 相同。

7. 在 **所需登录选项** > **登录方法** 下，选择 **SAML 2.0**。

   NetScaler 网关 - SAML 2.0(/en-us/citrix-endpoint-management/media/citrix-gateway-add-saml.png)

8. 单击 **View Setup Instructions**，并按照页面中提供的说明在 Citrix® 本地网关管理控制台中创建 SAML 策略。

NetScaler Gateway SAML - 查看设置说明(/en-us/citrix-endpoint-management/media/saml-view-setup-instructions.png)

> **注意：**
>
> - 在配置 NetScaler Gateway 11.1 或更高版本时安装 CA 证书后，创建 SAML 操作。要创建 SAML 操作，请导航到 **Security** > **AAA - Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Actions** > **SAML Actions**。单击 **Add** 并填写上一页中提供的信息。请勿遵循页面中提供的导航路径，即 **Netscaler Gateway** > **Policies** > **Authentication** > **SAML** > **Servers**。
> - 此外，请勿遵循提供的创建 SAML 策略的步骤，因为这些步骤使用的是经典策略。我们现在使用的是高级策略。请执行以下步骤 9 以使用高级策略创建 SAML 策略。

9. 为 SAML 操作创建相应的 SAML 策略，并按如下方式将策略绑定到身份验证虚拟服务器：

   a. 导航到 **安全** > **AAA-应用流量** > **策略** > **身份验证** > **高级策略**，然后单击 **添加**。

   b. 在“创建身份验证策略”页面上，提供以下详细信息：

      - **Name** - 为 SAML 策略指定一个名称。
      - **Action Type** - 选择 *SAML* 作为身份验证操作类型。
      - **操作** - 选择要绑定 SAML 策略的 SAML 服务器配置文件。
      - **表达式** - 显示 SAML 策略用于确定用户是否必须使用 SAML 服务器进行身份验证的规则或表达式的名称。在文本框中，将值 **rule** = `true` 设置为使 SAML 策略生效并运行相应的 SAML 操作。

   c. 将 SAML 策略绑定到 VPN 虚拟服务器，并通过身份验证配置文件将 VPN 虚拟服务器链接到身份验证虚拟服务器。有关绑定过程的更多信息，请参阅 绑定身份验证策略。

10. 使用 使用 GUI 设置身份验证虚拟服务器 创建 AAA 虚拟服务器。
11. 使用 配置身份验证虚拟服务器 配置 AAA 虚拟服务器。
12. 使用 身份验证配置文件 创建并配置身份验证配置文件。
13. 将身份验证配置文件绑定到网关虚拟服务器并保存所有配置。
14. 在 Citrix 本地网关管理控制台中创建 SAML 策略后，单击“完成”。

现在，您可以看到两个用于 Citrix Endpoint Management 集成的应用程序，即用于 Citrix Cloud 的 Web 应用程序和用于 Citrix Endpoint Management MAM 身份验证的 SAML 应用程序。

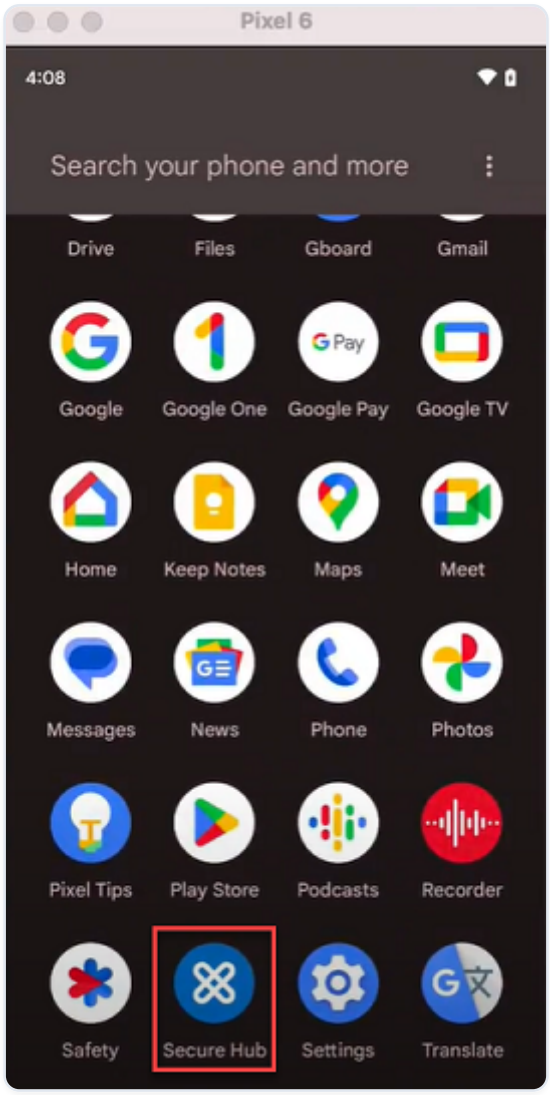
15. 将相关用户和组分配给您创建的 SAML 应用程序。

现在，Okta 已添加为已注册 MAM 的设备的身份提供程序，您可以使用 Okta 对其进行身份验证。

预期行为

以下示例使用 Android 设备：

1. 在您的移动设备上，打开 Citrix Secure Hub 应用程序。



2. 提供所需的权限。
3. 在登录页面上，输入您的组织提供的凭据，然后点击“**下一步**”。

   Citrix Secure Hub 登录页面(/en-us/citrix-endpoint-management/media/mam-authentication-microsoft-sign-in-username.png)

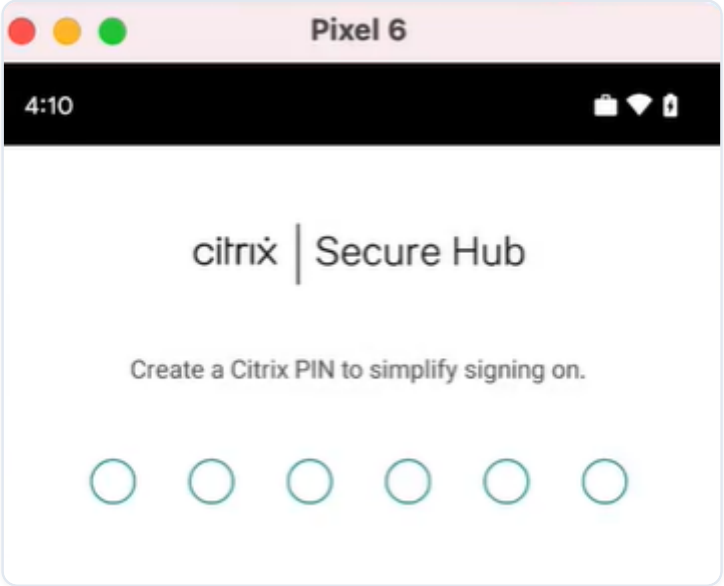
   您将被重定向到 Okta 登录页面。
4. 在 Okta 登录页面上，输入您的凭据，然后点击“**登录**”。

Okta 登录页面(/en-us/citrix-endpoint-management/media/mam-idp-okta-sign-in.png)

5. 在“**让我们设置您的工作配置文件**”页面上，点击“**接受并继续**”。

   让我们设置您的工作配置文件页面(/en-us/citrix-endpoint-management/media/lets-setup-your-workprofile.png)

6. 为 Citrix Secure Hub 应用程序创建 PIN 并确认。



您已成功重定向到 Citrix Secure Hub 主页。

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

Citrix Endpoint Management 支持通过 Citrix Cloud 使用本地 NetScaler Gateway 进行身份验证。此身份验证方法仅适用于通过 Citrix Secure Hub 注册 MDM 的用户。

注册 MAM 的设备无法通过 Citrix Cloud 使用本地 NetScaler Gateway 凭据进行身份验证。要将 Citrix Secure Hub 与 MDM+MAM 结合使用，请将 Citrix Endpoint Management 配置为使用 NetScaler Gateway 进行 MAM 注册。有关详细信息，请参阅NetScaler Gateway 和 Citrix Endpoint Management。

Citrix Endpoint Management 支持通过 Citrix Cloud 使用本地 NetScaler Gateway 对以下平台进行身份验证：

- iOS 设备
- Android Enterprise 设备，适用于 BYOD 和完全托管模式

> **注意：**

> Citrix Endpoint Management 不支持通过 Citrix Cloud 使用本地 NetScaler Gateway 对注册邀请进行身份验证。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 NetScaler Gateway 作为身份提供程序进行身份验证。

> 建议您启用基于证书的身份验证以获得完整的单点登录体验。如果您在 NetScaler Gateway 上使用 LDAP 身份验证进行 MAM 注册，则最终用户在注册期间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。

先决条件

- NetScaler Gateway。Citrix 建议您启用基于证书的身份验证以获得完整的单点登录体验。如果您在 NetScaler Gateway 上使用 LDAP 身份验证进行 MAM 注册，则最终用户在注册期间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。
- 已安装 Citrix Cloud Connector 以进行目录服务同步的 Citrix Cloud 帐户。
- Citrix Secure Hub 20.5.0 及更高版本。

将 Citrix Cloud 配置为使用 NetScaler Gateway 作为身份提供程序

要在 Citrix Cloud 中设置 NetScaler Gateway 身份验证，请参阅将本地 NetScaler Gateway 连接为 Citrix Cloud 的身份提供程序。

将 Citrix 身份提供程序配置为 Citrix Endpoint Management 的 IdP 类型

此配置仅适用于通过 Citrix Secure Hub 注册的用户。在 Citrix Cloud 中配置 NetScaler Gateway 后，按如下方式配置 Citrix Endpoint Management。

1. 在 Citrix Endpoint Management 控制台中，转到**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：** 键入一个唯一名称，以标识您正在创建的 IdP 连接。
   - **IDP 类型：** 选择 **Citrix 身份提供程序**。
   - **身份验证域：** 选择 **NetScaler Gateway**。此域对应于 Citrix Cloud **工作区配置 > 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**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：** 此字段会自动填充。
4. 单击**下一步**，查看**摘要**页面，然后单击**保存**。

现在，您可以使用本地 NetScaler Gateway 作为身份提供程序，通过 Citrix Secure Hub 注册用户设备。

Citrix Secure Hub 身份验证流程

Citrix Endpoint Management 使用以下流程，通过本地 NetScaler Gateway 作为 IdP 对通过 Citrix Secure Hub 注册的设备上的用户进行身份验证：

1. 用户启动 Citrix Secure Hub。
2. Citrix Secure Hub 将身份验证请求传递给 Citrix 身份，后者再将请求传递给本地 NetScaler Gateway。
3. 用户键入其用户名和密码。
4. 本地 NetScaler Gateway 验证用户并将代码发送到 Citrix 身份。
5. Citrix 身份将代码发送到 Citrix Secure Hub，Citrix Secure Hub 再将代码发送到 Citrix Endpoint Management 服务器。
6. Citrix Endpoint Management 使用代码和密钥获取 ID 令牌，然后验证 ID 令牌中的用户信息。Citrix Endpoint Management 返回一个会话 ID。

nFactor 身份验证

nFactor 身份验证允许您在使用 Citrix Secure Hub 时，使用 NetScaler 当前支持的所有身份验证模式。它通过要求用户提供更多身份证明才能获得访问权限，从而增强了应用程序的安全性。有关 nFactor 身份验证的更多信息，请参阅 nFactor 身份验证。

此外，有关不同的身份验证和授权方法以及如何配置它们的更多信息，请参阅 身份验证和授权。

Citrix Endpoint Management 支持以下 nFactor 身份验证类型：

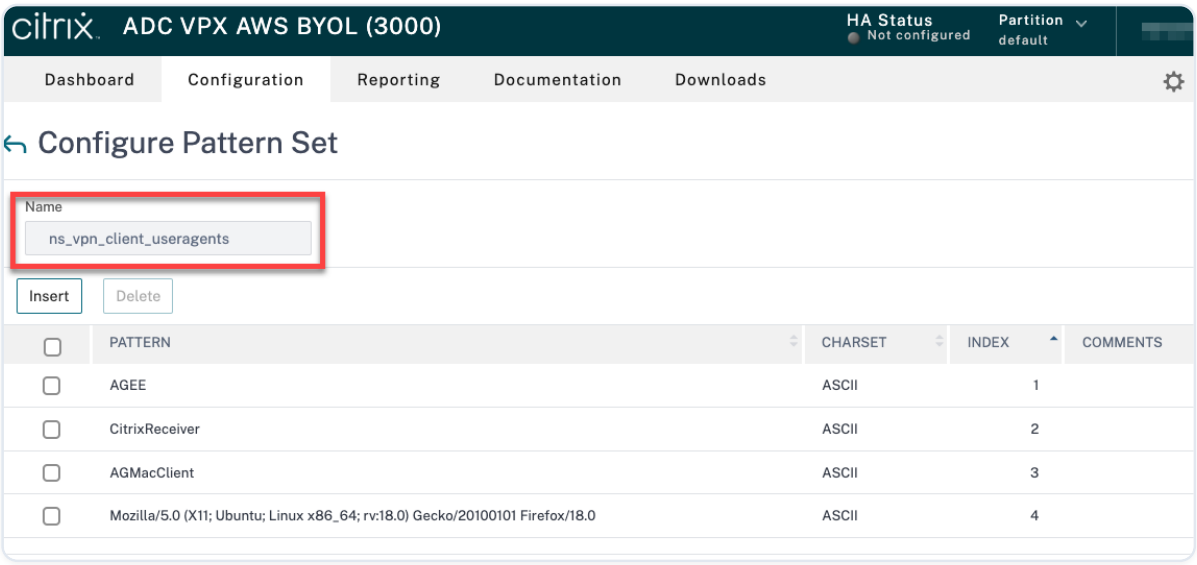
- 本地
- 轻型目录访问协议 (LDAP)
- RADIUS
- SAML
- 客户端证书身份验证

先决条件

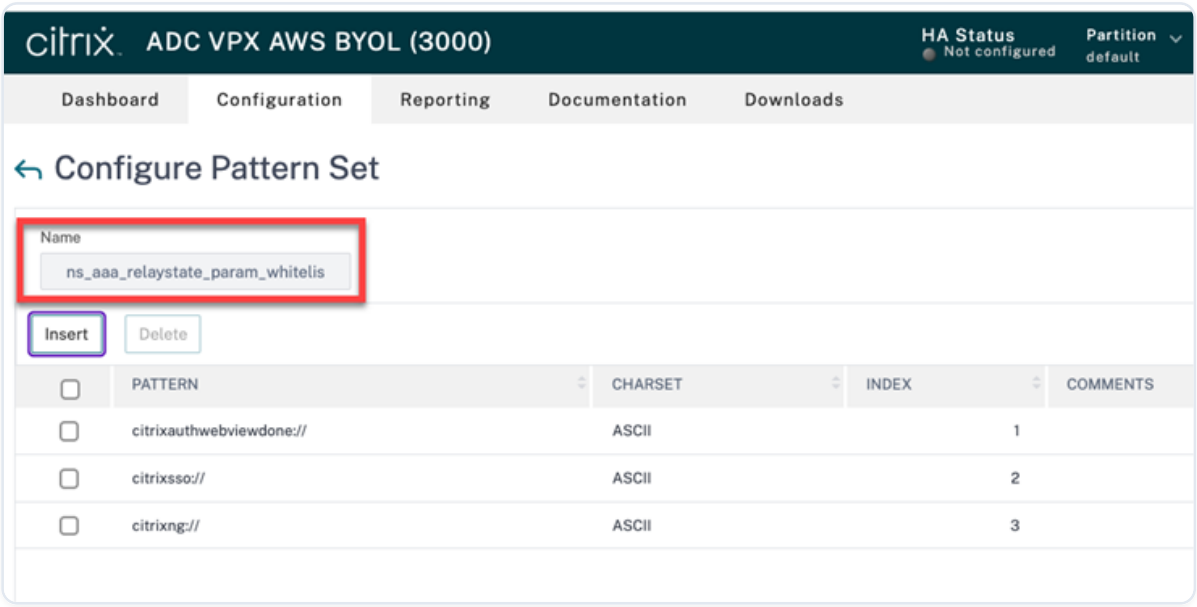
要将 Citrix Endpoint Management 配置为使用 nFactor 身份验证，请确保满足以下先决条件：

- 确保您使用的是 NetScaler 13.0 或更高版本。

- 确保您已在 NetScaler® 中为您的 Android 和 iOS 设备配置了以下模式集设置：
  - Ns_vpn_client_useragents



  - Ns_aaa_relaystate_param_whitelist



- 确保您已从 Apple 或 Google Play 安装了最新版本的 Citrix Secure Hub。
- 确保您在 NetScaler Gateway 中使用高级身份验证策略。
- 确保将客户端属性 **ENABLE_MAM_NFACTOR_SSO** 设置为 **True**，无论是在本地还是在云中。有关 **ENABLE_MAM_NFACTOR_SSO** 属性的更多信息，请参阅客户端属性参考。

> **注意：**

> 如果客户端属性 **Enable nFactor SSO** 设置为 **False**，请确保经典身份验证策略已绑定到 NetScaler Gateway。

配置 nFactor 身份验证

根据您的 NetScaler Gateway 设置方式，为 Citrix Endpoint Management 配置 nFactor 身份验证，具体如下：

- Citrix Endpoint Management 已使用经典身份验证策略与 NetScaler Gateway 设置完毕。有关更多信息，请参阅在现有 NetScaler Gateway 中将经典策略更新为高级身份验证策略。
- Citrix Endpoint Management 使用高级身份验证策略与 NetScaler Gateway 设置完毕。有关更多信息，请参阅使用高级策略配置 NetScaler Gateway 设置。

在现有 NetScaler Gateway 中将经典策略更新为高级身份验证策略

如果您的 Citrix Endpoint Management 已在 NetScaler Gateway 中使用经典身份验证策略进行设置，则必须使用以下方法之一将经典身份验证策略更新为高级身份验证策略：

- 创建高级身份验证策略，并将网关配置更改为使用高级身份验证策略。有关更多信息，请参阅身份验证策略。
- 将经典身份验证策略更新为高级身份验证策略。有关更多信息，请参阅使用 NSPEPI 工具转换策略表达式。

使用高级策略配置 NetScaler Gateway 设置

要在 NetScaler Gateway 中使用高级身份验证策略为 Citrix Endpoint Management 配置 nFactor 身份验证，请参阅配置 nFactor 身份验证。

> **注意：**
>
> - 您可以从支持的身份验证类型中选择相关的身份验证类型。
> - 如果您使用的是 SAML 身份验证类型，则可以使用以下方法之一通过 MAM IdP 配置 SAML：
>   - 要使用 Azure Active Directory 进行配置，请参阅通过 NetScaler Gateway 使用 Azure Active Directory 进行 MAM 注册的身份验证。

- 要使用 Okta 进行配置，请参阅通过 NetScaler Gateway 使用 Okta 进行 MAM 注册的身份验证。

用户帐户、角色和注册

您可以在 Citrix Endpoint Management 控制台的“**管理**”选项卡和“**设置**”页面中执行用户配置任务。除非另有说明，否则本文中提供了以下任务的步骤。

- 注册安全模式和邀请
  - 在“**设置 > 注册**”中，最多可配置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以及用户注册其设备所需的步骤数。
- 用户帐户和组的角色
  - 在“**设置 > 基于角色的访问控制**”中，将预定义角色或权限集分配给用户和组。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。
  - 在“**设置 > 通知模板**”中，创建或更新通知模板，以用于自动化操作、注册以及发送给用户的标准通知消息。您可以配置通知模板，通过两个不同的通道发送消息：Citrix Secure Hub 或 SMTP。有关详细信息，请参阅：创建和更新通知模板。
- 用户帐户和组：
  - 在“**管理 > 用户**”中，您可以手动添加本地用户帐户，或使用 .csv 预配文件导入帐户并管理本地组。但是，大多数 Citrix Endpoint Management 部署都连接到 LDAP 以获取用户和组信息。在以下用例中，您可能更喜欢在本地创建用户帐户：
    - 在零售等环境中，设备是共享的，而不是专用于单个用户。
    - 如果您使用不受支持的目录，例如 Novell eDirectory。
  - 在“**设置 > 工作流**”中，使用工作流管理用户帐户的创建和删除。

关于用户帐户

Citrix Endpoint Management 用户帐户可以是本地用户、Active Directory 用户或云用户。

- **云用户：** 云用户是一种特殊的用户帐户，当管理员添加到您的 Citrix Cloud 客户帐户时，Citrix Cloud 会创建该帐户。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。

  要将管理员添加到 Citrix Cloud 帐户，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，以指定 Citrix Endpoint Management 中设备注册的安全级别和通知模板。

Citrix 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其设备必须执行的步骤。您可以在 Citrix Endpoint Management 控制台中通过**管理 > 注册邀请**页面配置注册安全模式。有关信息，请参阅 注册邀请。

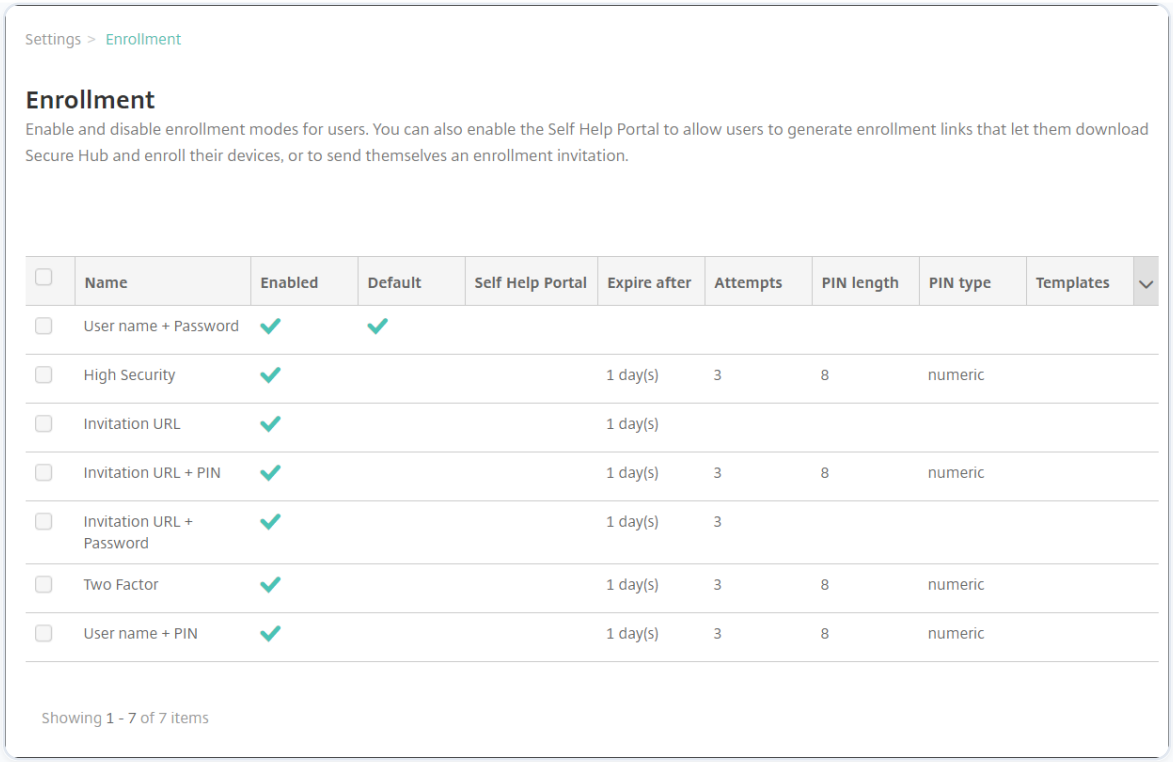
> **注意：**
>
> 如果您计划使用自定义通知模板，则必须在配置注册安全模式之前设置这些模板。有关通知模板的详细信息，请参阅 创建或更新通知模板。

1. 在 Citrix 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。该页面包含所有可用注册安全模式的表格。默认情况下，所有注册安全模式都处于启用状态。
3. 选择列表中的任何注册安全模式以对其进行编辑。然后，将该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以查看列表右侧的选项菜单。

   > **提示：**

> 编辑注册安全模式时，可以指定一个过期期限，在此期限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。该值将显示在用户和组注册邀请配置页面中。



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
- 双因素
- 用户名 + PIN

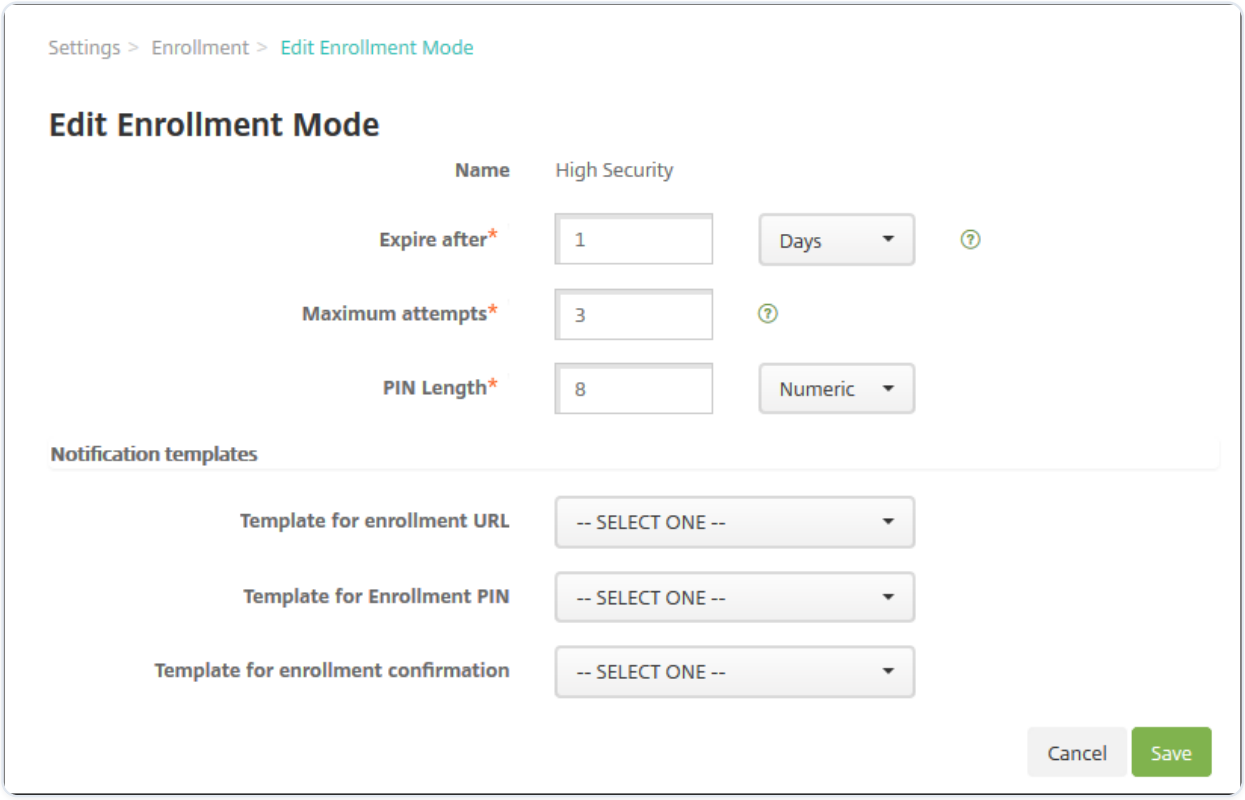
有关特定于平台的注册安全模式的信息，请参阅按平台划分的注册安全模式。

您可以将注册邀请作为一种有效方式，限制特定用户或组的注册能力。要发送注册邀请，您只能使用**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**、**双因素身份验证**或**用户名 + PIN**注册的设备，用户必须在 Citrix Secure Hub 中手动输入其凭据。

您可以将一次性 PIN (有时也称为 OTP) 注册邀请用作双因素身份验证解决方案。一次性 PIN 注册邀请可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，选择一个注册安全模式，然后单击**编辑**。**编辑注册模式**页面随即显示。根据您选择的模式，您可能会看到不同的选项。



2. 根据需要更改以下信息：

- **过期时间：** 输入一个过期截止日期，在此日期之后用户无法注册其设备。此值显示在用户和组注册邀请配置页面中。

  键入 **0** 以防止邀请过期。

- **天数：** 在下拉列表中单击“**天数**”或“**小时**”，以与您在“**过期时间**”中输入的过期截止日期相对应。
- **最大尝试次数：** 键入用户在被锁定在注册过程之外之前可以尝试注册的次数。此值显示在用户和组注册邀请配置页面中。

  键入 **0** 以允许无限次尝试。

- **PIN 长度：** 键入一个数字以设置生成的 PIN 的长度。
- **数字：** 在下拉列表中单击“**数字**”或“**字母数字**”以选择 PIN 类型。
- **通知模板：**
  - **注册 URL 模板：** 在下拉列表中单击一个模板，以用于注册 URL。例如，“注册邀请”模板会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：** 在下拉列表中单击一个模板，以用于注册 PIN。
- **注册确认模板：** 在下拉列表中单击一个模板，以用于通知用户他们已成功注册。

3. 点击 **保存**。

将注册安全模式设置为默认值

默认注册安全模式用于所有设备注册请求，除非您选择其他注册安全模式。如果未将任何注册安全模式设置为默认值，则必须为每个设备注册创建一个注册请求。

1. 如果您要用作默认值的注册安全模式未启用，请选择它并单击“**启用**”。您可以设置为默认值的注册安全模式只有“**用户名 + 密码**”、“**双重身份验证**”或“**用户名 + PIN**”。
2. 选择注册安全模式，然后单击“**默认**”。所选模式现在是默认值。如果之前设置了其他注册安全模式为默认值，则该模式将不再是默认值。

禁用注册安全模式

禁用注册安全模式会使其无法使用，无论是用于组注册邀请还是在自助服务门户上。您可以通过禁用一个注册安全模式并启用另一个来更改允许用户注册其设备的方式。

1. 选择注册安全模式。

   您无法禁用默认注册安全模式。如果您要禁用默认注册安全模式，则必须首先删除其默认状态。

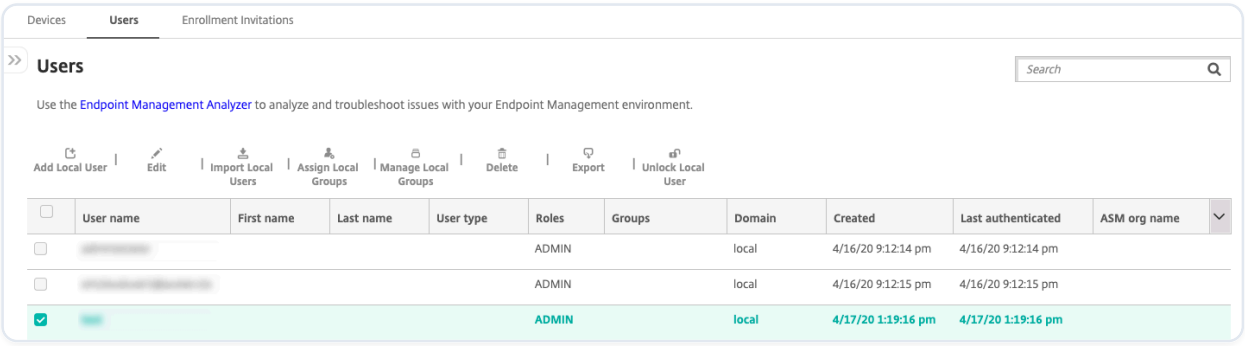
2. 单击“**禁用**”。注册安全模式不再启用。

添加、编辑、解锁或删除本地用户帐户

您可以手动将本地用户帐户添加到 Citrix Endpoint Management，或者可以使用预配文件导入帐户。有关从预配文件导入用户帐户的步骤，请参阅导入用户帐户。

所有 Citrix Cloud 管理员都将创建为 Citrix Endpoint Management 管理员。如果您创建具有自定义访问权限的 Citrix Cloud 管理员，请确保该访问权限包括 Citrix Endpoint Management。有关添加 Citrix Cloud 管理员的信息，请参阅添加管理员。

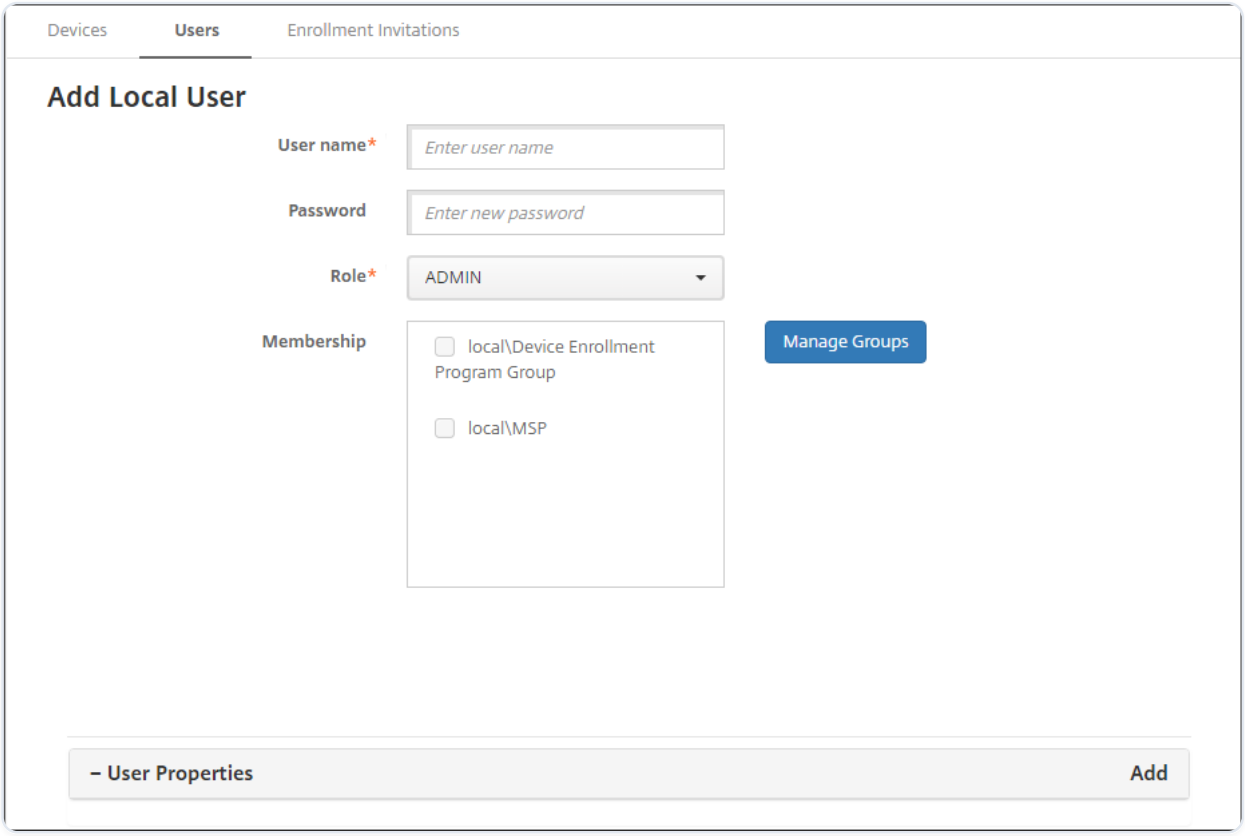
1. 在 Citrix Endpoint Management 控制台中，单击“**管理 > 用户**”。此时将显示“**用户**”页面。



2. 单击“**显示筛选器**”以筛选列表。

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，这是一个必填字段。名称中可以包含以下内容：空格、大写字母和小写字母。
   - **密码：** 键入可选的用户密码。密码必须至少包含 14 个字符，并满足以下所有条件：
     - 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

  - 不要包含字典词或受限词，例如您的 Citrix® 用户名或电子邮件地址
  - 不要包含三个以上连续重复的字符或键盘模式，例如 1111、1234 或 asdf

- **角色：** 在下拉列表中单击用户角色。有关角色的详细信息，请参阅 使用 RBAC 配置角色。可能的选项包括：
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **成员资格：** 在下拉列表中单击要添加用户的组。
- **用户属性：** 添加可选的用户属性。对于要添加的每个用户属性，单击“**添加**”并执行以下操作：
  - **用户属性：** 在下拉列表中单击一个属性，然后在该属性旁边的字段中键入用户属性值。
  - 点击“**完成**”保存用户属性，或点击“**取消**”。

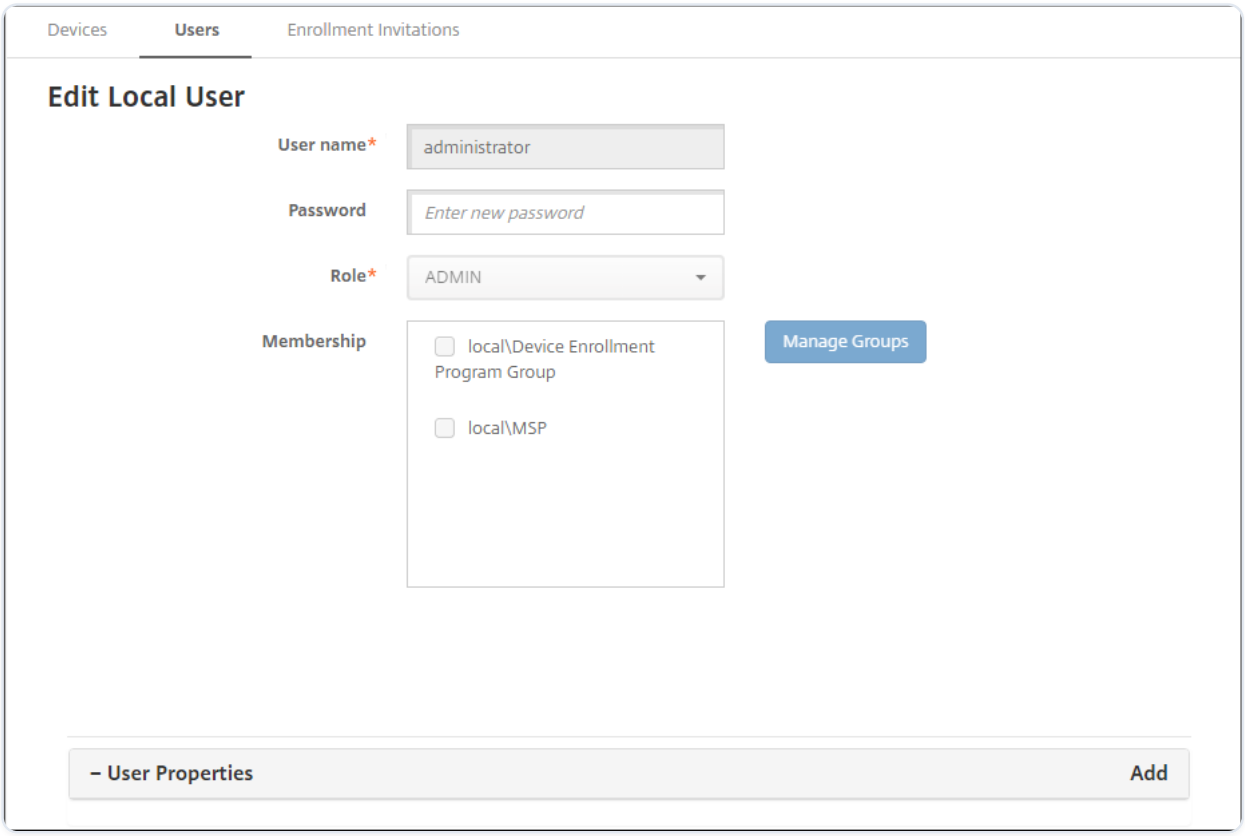
  要删除现有用户属性，请将鼠标悬停在包含该属性的行上，然后单击右侧的“**X**”。该属性将立即删除。

  要编辑现有用户属性，请单击该属性并进行更改。单击“**完成**”保存更改后的列表，或单击“**取消**”以保持列表不变。

3. 单击“**保存**”。创建用户后，本地用户帐户的“**用户类型**”字段将保持为空。

编辑本地用户帐户

1. 在“**用户**”页面上的用户列表中，单击以选择一个用户，然后单击“**编辑**”。此时将显示“**编辑本地用户**”页面。



2. 根据需要更改以下信息：

   - **用户名：** 您无法更改用户名。
   - **密码：** 更改或添加用户密码。
   - **角色：** 在下拉列表中单击用户角色。
   - **成员资格：** 在下拉列表中单击要添加或编辑用户帐户的组。要从组中删除用户帐户，请清除组名称旁边的复选框。
   - **用户属性：** 执行以下操作之一：
     - 对于要更改的每个用户属性，请单击该属性并进行更改。单击“**完成**”保存更改后的列表，或单击“**取消**”以保持列表不变。
     - 对于要添加的每个用户属性，请单击“**添加**”并执行以下操作：
       - **用户属性：** 在下拉列表中单击一个属性，然后在属性旁边的字段中键入用户属性。
       - 单击 **完成** 以保存用户属性，或单击 **取消**。
     - 对于要删除的每个现有用户属性，将鼠标悬停在包含该属性的行上，然后单击右侧的 **X**。该属性将立即删除。

3. 单击 **保存** 以保存更改，或单击 **取消** 以保持用户不变。

解锁本地用户帐户

本地用户帐户根据以下服务器属性锁定：

- `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 Citrix Endpoint Management 控制台解锁该帐户。

1. 在 **用户** 页面上，在用户帐户列表中，单击以选择一个用户帐户。
2. 单击 **解锁用户**。将出现一个确认对话框。
3. 单击 **解锁** 以解锁用户帐户，或单击 **取消** 以保持用户不变。

您无法从 Citrix Endpoint Management 控制台打开 Active Directory 用户。锁定的 Active Directory 用户必须联系其 Active Directory 帮助台以重置密码。

删除本地用户帐户

1. 在 **用户** 页面上，在用户帐户列表中，单击以选择一个用户帐户。

   您可以通过选中每个用户帐户旁边的复选框来选择多个用户帐户进行删除。
2. 点击“**删除**”。此时将显示确认对话框。
3. 点击“**删除**”以删除用户帐户，或点击“**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，然后点击“**删除**”。

如果您删除的用户已注册设备，并且您希望重新注册这些设备，请在重新注册之前删除这些设备。要删除设备，请转至“**管理 > 设备**”，选择设备，然后点击“**删除**”。

导入用户帐户

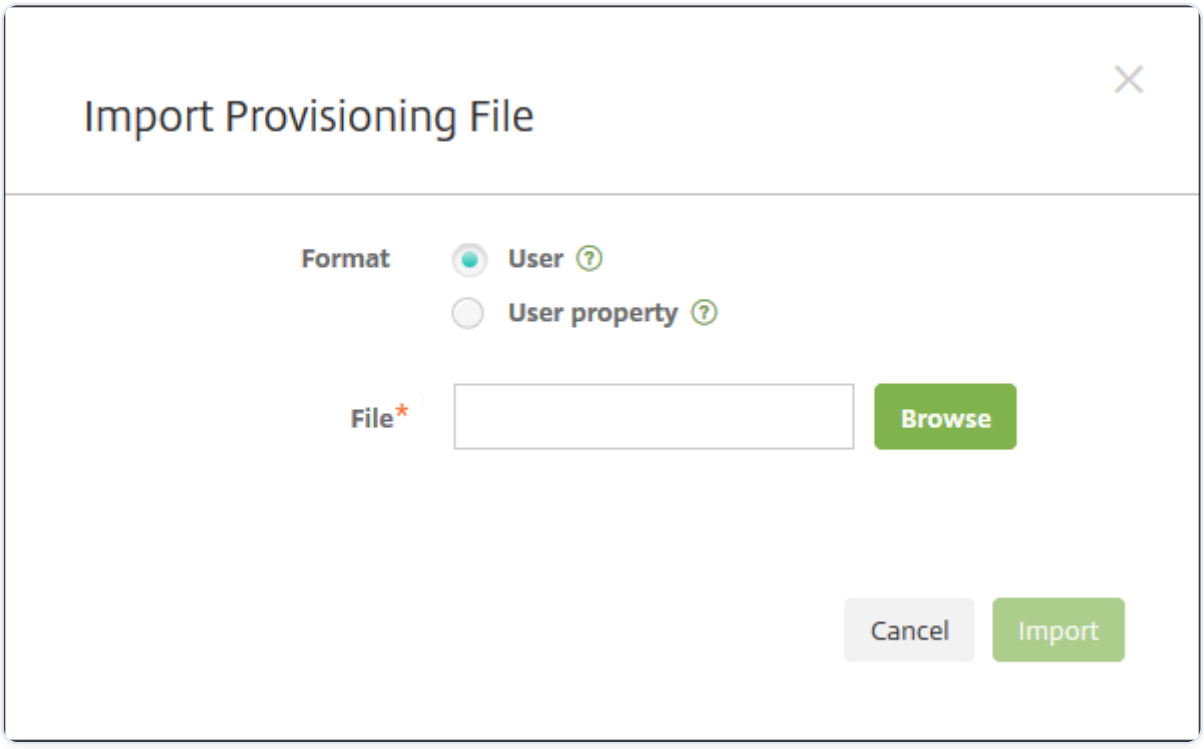
您可以从名为预配文件的 .csv 文件导入本地用户帐户和属性，该文件可以手动创建。有关设置预配文件格式的详细信息，请参阅预配文件格式。

> **注意：**

- 对于本地用户，请在导入文件中使用域名和用户名。例如，指定 `username@domain`。如果您创建或导入的本地用户用于 Citrix Endpoint Management 中的托管域，则该用户无法使用相应的 LDAP 凭据进行注册。
- 如果要将用户帐户导入 Citrix Endpoint Management 内部用户目录，请禁用默认域以加快导入过程。请记住，禁用域会影响注册。内部用户导入完成后，请重新启用默认域。
- 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 是托管域，请勿创建具有此 UPN 格式的本地用户：user@example.com。

准备好预配文件后，请按照以下步骤将文件导入 Citrix Endpoint Management。

1. 在 Citrix Endpoint Management 控制台中，点击“**管理 > 用户**”。此时将显示“**用户**”页面。
2. 点击“**导入本地用户**”。此时将显示“**导入预配文件**”对话框。



3. 为您要导入的预配文件格式选择“**用户**”或“**属性**”。
4. 通过单击“**浏览**”并导航到文件位置来选择要使用的预配文件。
5. 单击 **Import**。

预配文件格式

您可以创建预配文件并使用它将用户帐户和属性导入到 Citrix Endpoint Management。预配文件可使用以下格式之一：

- **用户预配文件字段：** `user;password;role;group1;group2`
- **用户属性预配文件字段：**
  `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> **注意：**
>
> - 使用分号 (;) 分隔预配文件中的字段。如果字段的一部分包含分号，请使用反斜杠字符 (\) 对其进行转义。例如，在预配文件中将属性 **propertyV; test;1;2** 键入为 **propertyV\;test\;1\;2**。
> - **角色**的有效值为预定义角色 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。
> - 在属性预配文件中，属性特性请使用小写。数据库区分大小写。

用户预配内容的示例

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

作为另一个示例，`AUser0;1.password;USER;ActiveDirectory.test.net` 表示：

- **用户：** AUser0
- **密码：** 1.password
- **角色：** USER
- **组：** ActiveDirectory.test.net

用户属性预配内容的示例

条目 `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` 表示：

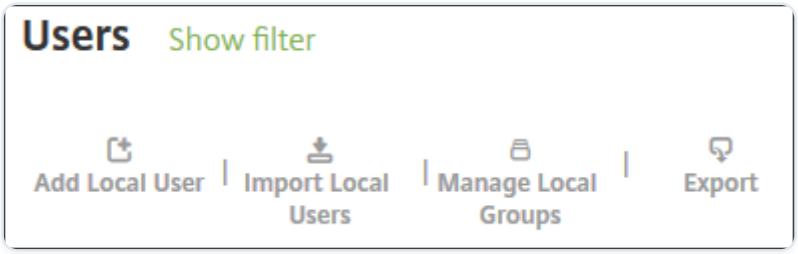
- **用户：** user01
- **属性 1**
  - **名称：** propertyN
  - **值：** propertyV;test;1;2
- **属性 2：**
  - **名称：** prop 2
  - **值：** prop2 值

添加或删除组

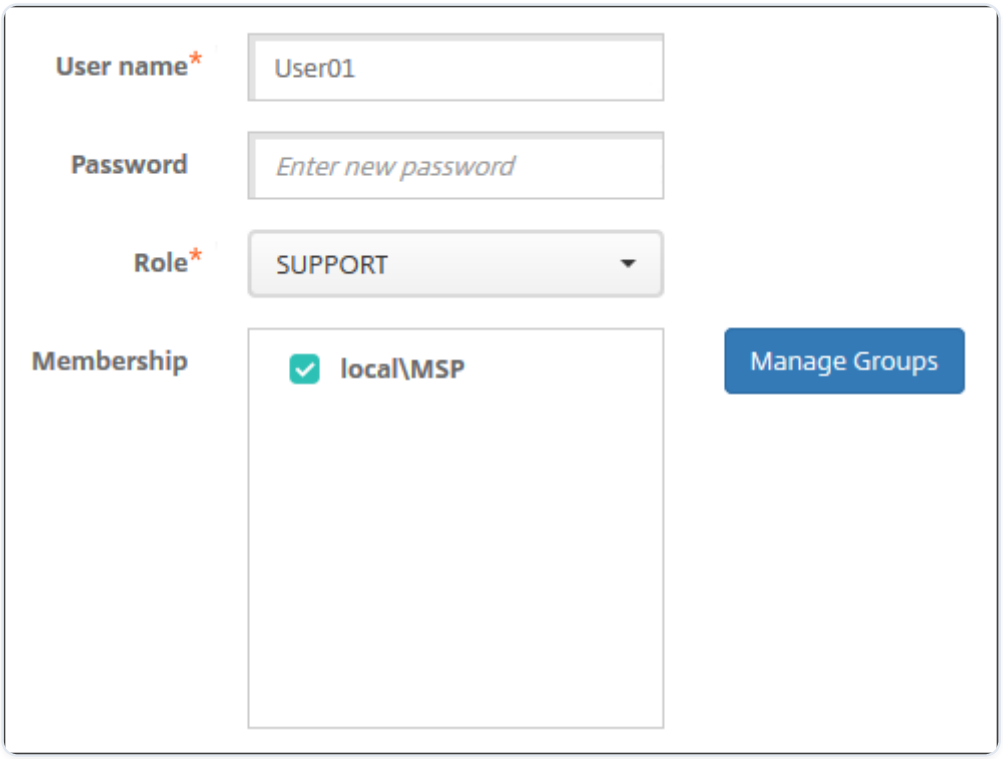
您可以在 Citrix Endpoint Management 控制台的以下页面（**用户**、**添加本地用户**或**编辑本地用户**）上的**管理组**对话框中管理组。没有组编辑命令。

添加本地组

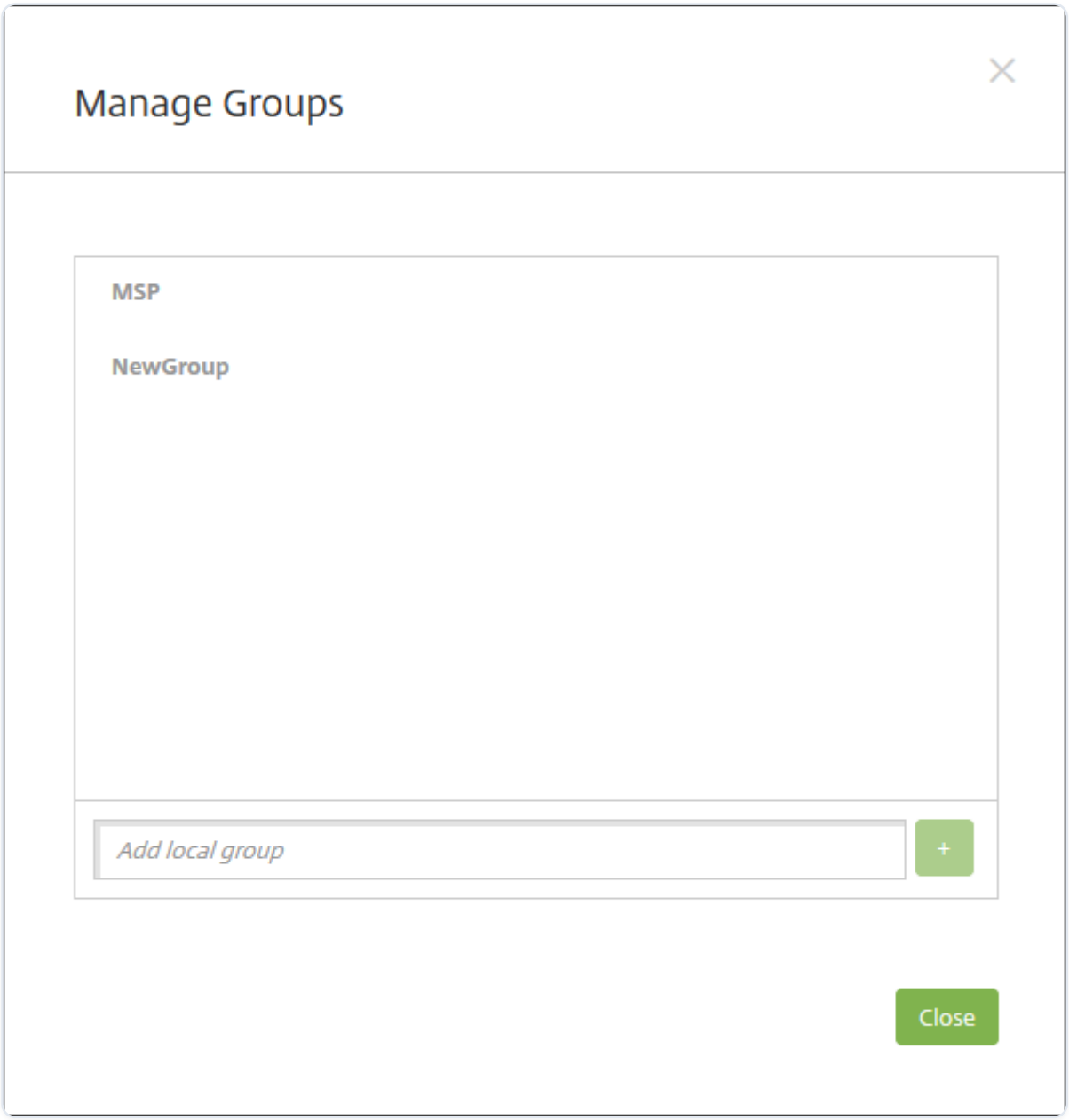
1. 执行以下操作之一：
   - 在**用户**页面上，单击**管理本地组**。



   - 在**添加本地用户**页面或**编辑本地用户**页面上，单击**管理组**。


User name*
User01
Password
Enter new password
Role*
SUPPORT
Membership
local\MSP
Manage Groups

管理组对话框随即显示。



2. 在组列表下方，键入新的组名称，然后单击加号 (+)。用户组将添加到列表中。
3. 单击**关闭**。

删除组

删除组对用户帐户没有影响。相反，删除组只会移除用户与该组的关联。用户还会失去对与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，任何其他组关联保持不变。如果用户未与任何其他本地组关联，则他们将与顶级关联。

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**”。

此时将显示“**管理组**”对话框。

用户组管理(/en-us/citrix-endpoint-management/media/local-users-and-groups-manage-group-remove.png)

2. 在“**管理组**”对话框中，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**”以确认操作并删除组。

> **重要提示：**
>
> 无法撤消此操作。

5. 在“**管理组**”对话框中，单击“**关闭**”。

创建和管理工作流

您可以使用工作流来管理用户帐户的创建和删除。在创建工作流之前，请确定组织中拥有批准用户帐户请求权限的人员。然后，使用工作流模板创建和批准用户帐户请求。

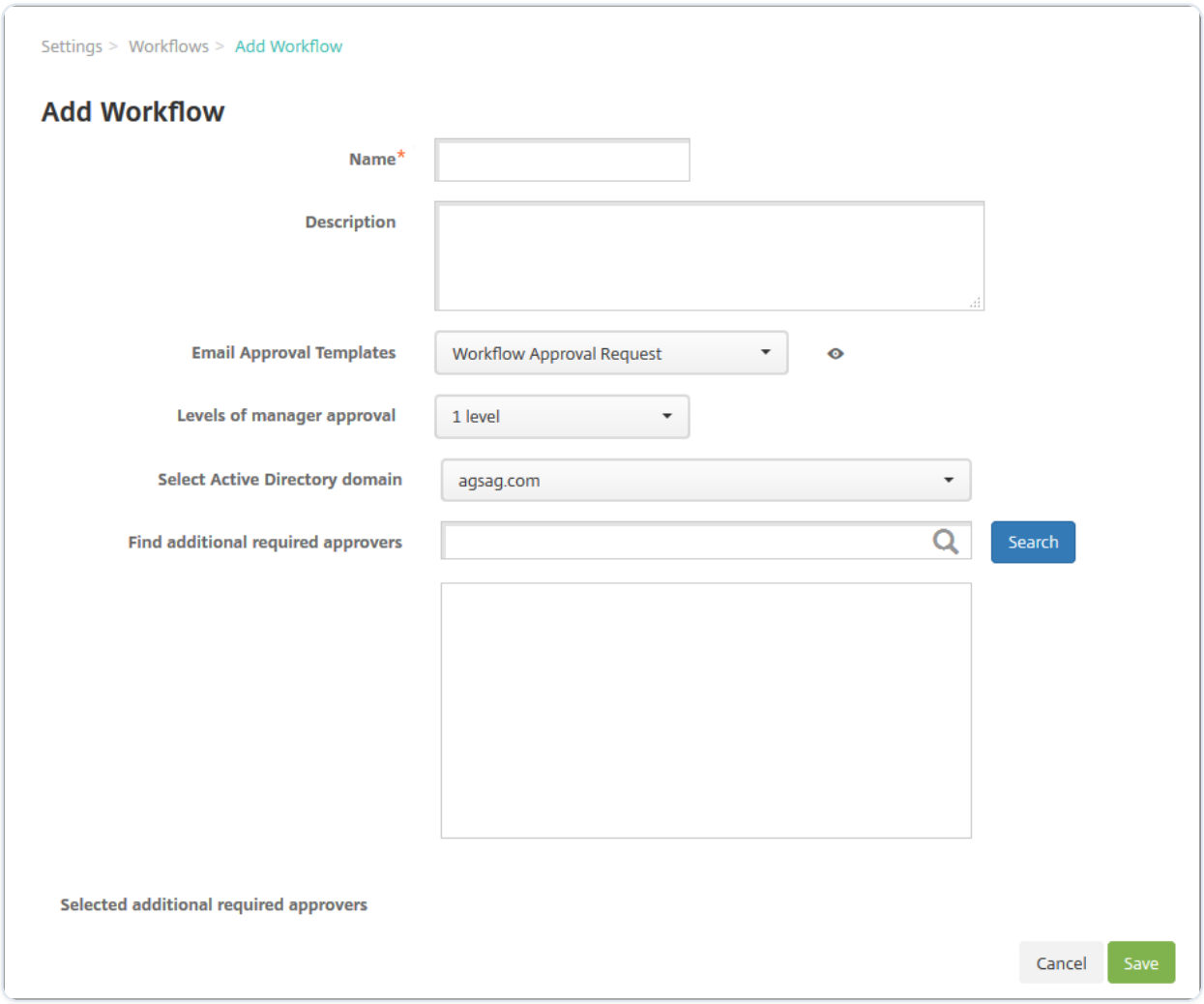
首次设置 Citrix Endpoint Management 时，您需要配置工作流电子邮件设置，这些设置必须在您使用工作流之前进行设置。您可以随时更改工作流电子邮件设置。这些设置包括电子邮件服务器、端口、电子邮件地址以及创建用户帐户的请求是否需要批准。

您可以在 Citrix Endpoint Management 中的两个位置配置工作流：

- 在 Citrix Endpoint Management 控制台的 **设置 > 工作流** 页面中。在 **工作流** 页面上，您可以配置多个工作流以用于应用程序配置。在“工作流”页面上配置工作流时，您可以在配置应用程序时选择该工作流。
- 在应用程序中配置应用程序连接器时，提供工作流名称，然后配置批准用户帐户请求的个人。请参阅添加应用程序。

您可以为用户帐户的经理审批分配最多三个级别。如果您需要其他人批准用户帐户，您可以使用其姓名或电子邮件地址搜索并选择他们。当 Citrix Endpoint Management 找到该人员时，您可以将其添加到工作流中。工作流中的所有个人都会收到电子邮件以批准或拒绝新的用户帐户。

1. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标。将显示 **设置** 页面。
2. 单击 **工作流**。将显示 **工作流** 页面。
3. 单击 **添加**。将显示 **添加工作流** 页面。



4. 配置以下设置：

- **名称：** 为工作流键入一个唯一的名称。
- **描述：** （可选）为工作流键入一个描述。
- **电子邮件审批模板：** 在列表中，选择要分配的电子邮件审批模板。您可以在 Citrix Endpoint Management 控制台的 **设置** 下的 **通知模板** 部分创建电子邮件模板。当您单击此字段右侧的眼睛图标时，您会看到正在配置的模板的预览。
- **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 个级别
- **选择 Active Directory 域：** 在列表中，选择要用于工作流的相应 Active Directory 域。

- **查找其他必需的审批者：** 在搜索字段中键入名称，然后单击“**搜索**”。名称源自 Active Directory。
- 当名称出现在字段中时，选中名称旁边的复选框。名称和电子邮件地址将显示在“**选定的其他必需审批者**”列表中。
    - 要从列表中删除名称，请执行以下操作之一：
        - 单击“**搜索**”以查看所选域中的所有人员列表。
        - 在搜索框中键入完整或部分名称，然后单击“**搜索**”以限制搜索结果。
        - “**选定的其他必需审批者**”列表中的人员在搜索结果列表中其姓名旁边有复选标记。滚动列表并清除要删除的每个姓名旁边的复选框。

5. 单击“**保存**”。创建的工作流将显示在“**工作流**”页面上。

创建工作流后，您可以查看工作流详细信息、查看与工作流关联的应用程序或删除工作流。创建工作流后，无法编辑工作流。如果需要具有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，在现有工作流列表中，选择一个特定的工作流。为此，请单击表中的行或选中工作流旁边的复选框。
2. 要删除工作流，请单击“**删除**”。将出现一个确认对话框。再次单击“**删除**”。

> **重要提示：**
>
> 无法撤消此操作。

注册配置文件

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，错误消息会告知用户他们已超出设备注册限制。

    - 是否允许用户拒绝设备管理。

您可以使用注册配置文件在单个 Citrix Endpoint Management 控制台中组合多个用例和设备迁移路径。一些用例包括：

- 移动设备管理（仅限 MDM）
- MDM+移动应用程序管理 (MAM)
- 仅限 MAM
- 公司拥有的注册
- BYOD 注册（选择退出 MDM 注册的能力）
- 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 Citrix Workspace 应用程序自动注册 Windows 10 和 Windows 11 设备（预览版）

如果您的当前站点仅支持 MDM 并且您想添加 MAM，则必须配置 NetScaler Gateway。有关详细信息，请参阅NetScaler Gateway 要求。

创建交付组时，可以使用名为 Global 的默认注册配置文件，也可以指定其他注册配置文件。

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：** 您可以指定管理和设备所有者模式。例如：公司拥有的设备、完全托管的工作配置文件和 BYOD 工作配置文件。

  新设备默认注册到 Android Enterprise。您可以选择使用旧版 Android 设备管理员 (DA) 模式管理设备。新设备也默认注册到应用程序管理。

  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**模式作为公共预览版提供。要启用此功能，请联系您的支持团队。

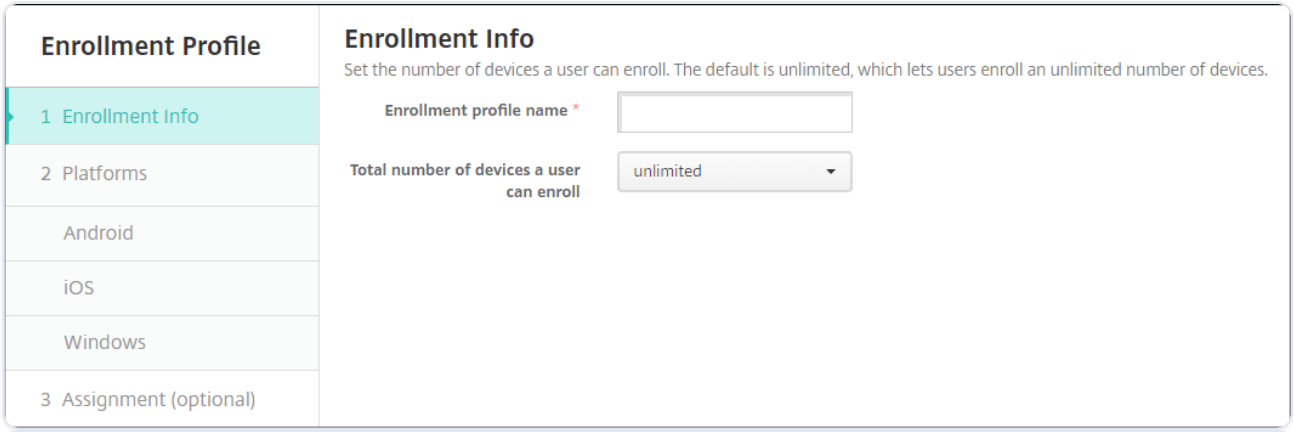
  如果选择 Apple 用户注册，您可以选择为托管 Apple ID 使用自定义域并配置该域。

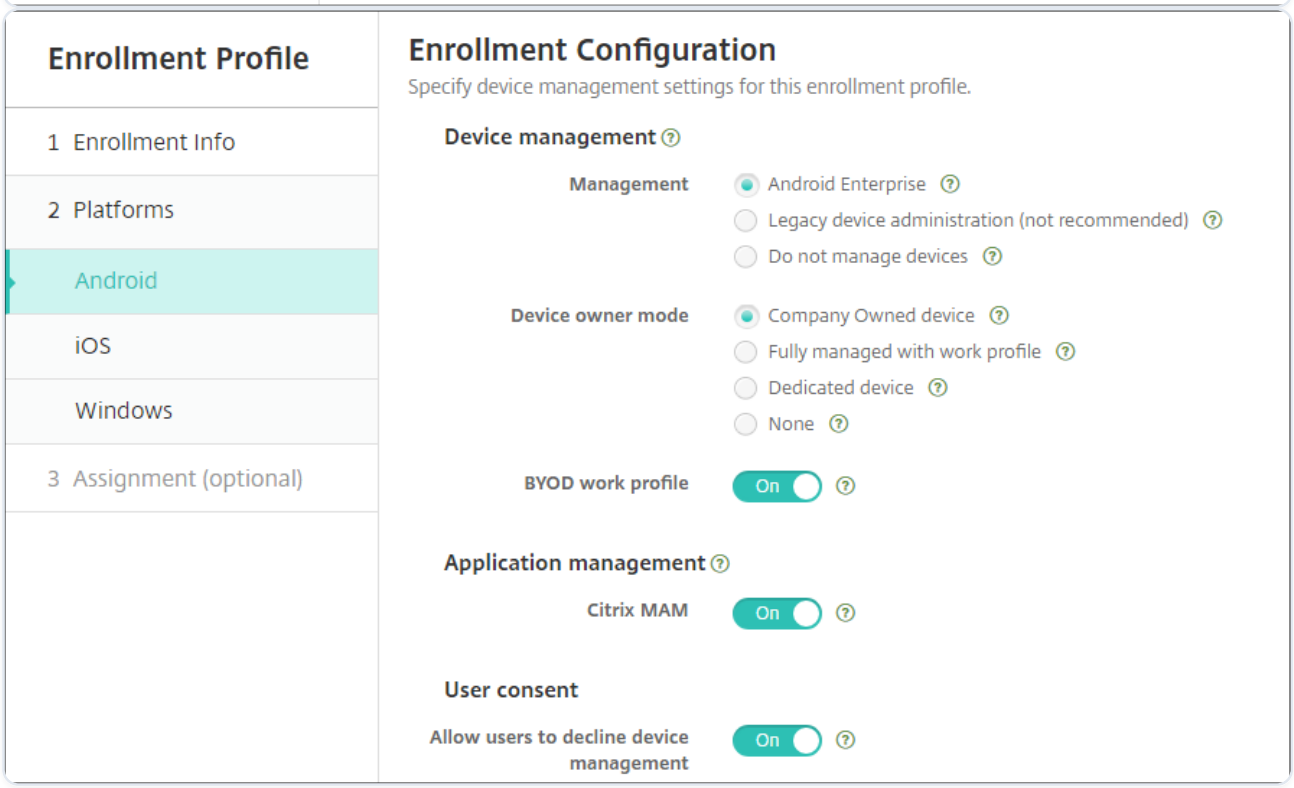
  新设备默认注册到 Apple 设备管理。新设备也默认注册到应用程序管理。
- **对于 Windows 10 和 Windows 11 设备：** 您可以指定是否使用 Citrix® 设备管理 for Windows。新设备默认注册到设备管理。

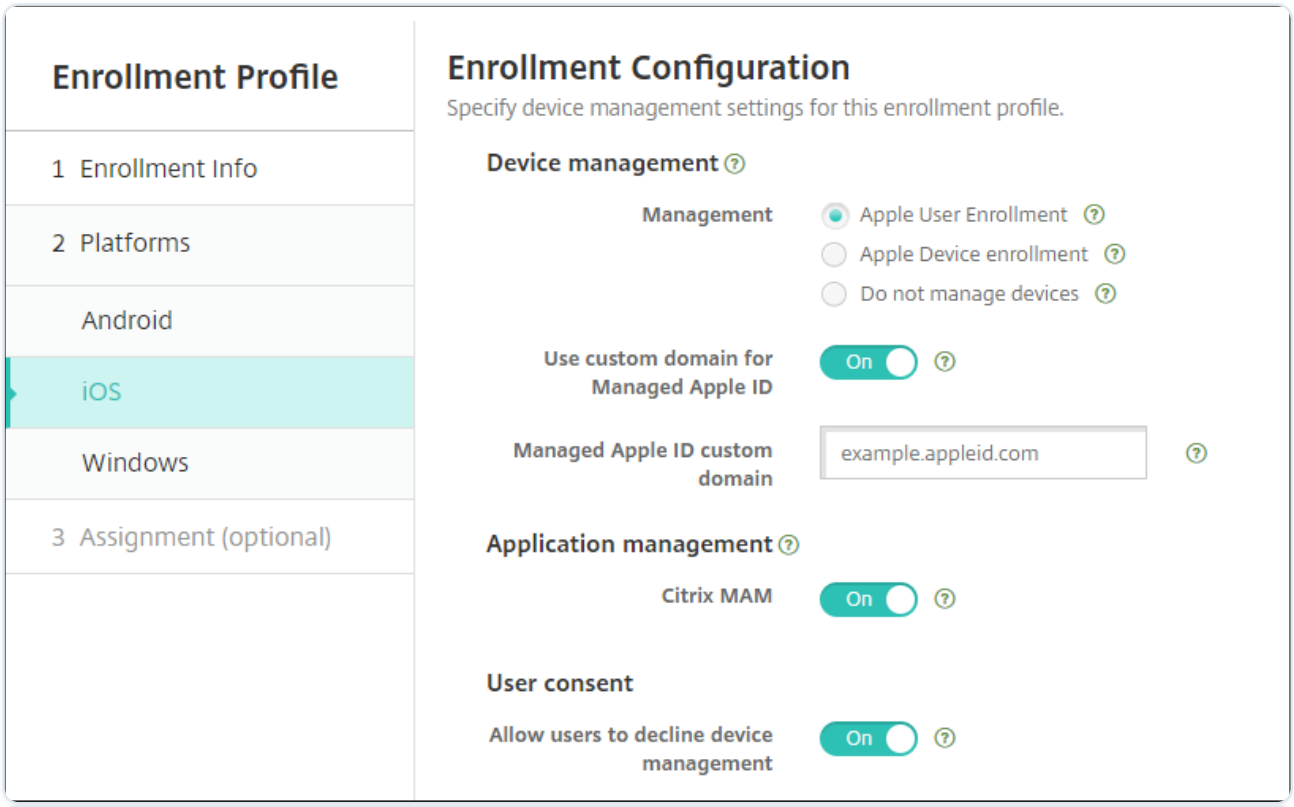
全局注册配置文件

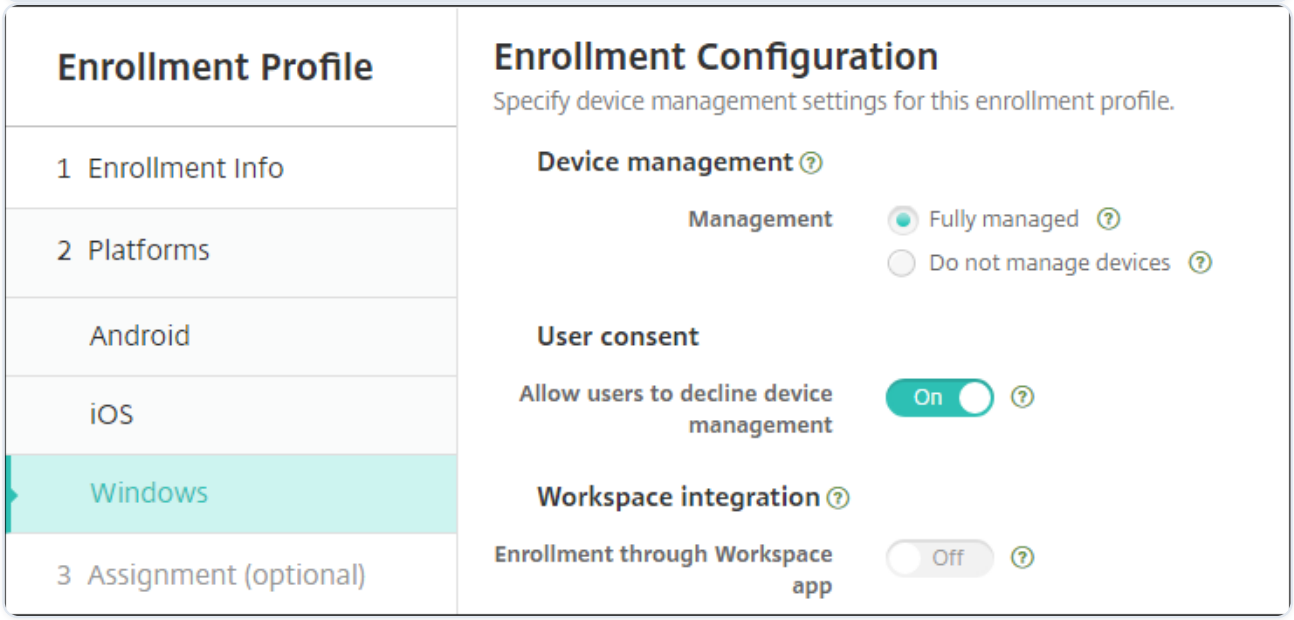
默认注册配置文件名为 Global。Global 配置文件在您有机会创建注册配置文件之前，对于测试很有用。

如果您加入 Citrix Endpoint Management 20.2.1 或更高版本，Global 注册配置文件将具有预定义设置。以下屏幕截图显示了 Global 注册配置文件的默认设置。仅 MAM 部署会显示这些选项的子集。









注册配置文件、交付组和注册

注册配置文件和交付组的交互方式如下：

- 您可以将注册配置文件附加到一个或多个交付组。
- If a user belongs to multiple delivery groups that have different enrollment profiles, the name of the delivery group determines the enrollment profile used. Citrix Endpoint Management selects the delivery group that appears last in an alphabetized list of delivery groups. For example, suppose that you have the following:

  - 两个注册配置文件，分别命名为“EP1”和“EP2”。
  - 两个交付组，分别命名为“DG1”和“DG2”。
  - “DG1”与“EP1”关联。
  - “DG2”与“EP2”关联。

  If the enrolling user is in both the "DG1" and "DG2" delivery groups, Citrix Endpoint Management uses the "EP2" enrollment profile to determine the enrollment type for the user.

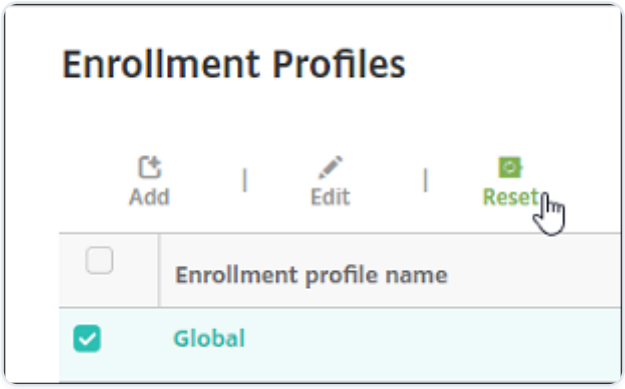
- 部署顺序仅适用于已配置 MDM（设备管理）注册配置文件的交付组中的设备。
- 设备注册后，对注册配置文件的一些更改需要重新注册：
  - 更改配置以将设备从 MDM+MAM 降级到 MAM 或 MDM 注册。当您更新注册配置文件或将设备移动到不同的交付组时，可能会发生降级。
  - 将 MAM 添加到已配置为 MDM 的注册配置文件中。
  - 将 MDM 添加到已配置为 MAM 的注册配置文件中。
- 切换到不同的注册配置文件不会影响现有已注册设备。但是，用户必须取消注册然后重新注册这些设备才能使更改生效。

创建注册配置文件

1. 在 Citrix 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，用户可以注册无限数量的设备。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 管理的 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，交付组的名称决定了所使用的注册配置文件。Citrix Endpoint Management 会选择按字母顺序排列的交付组列表中最后出现的交付组。要创建交付组，请转到 **Configure > Delivery Groups**。

您的注册配置文件列表显示在“**Configure > Enrollment Profiles**”页面上。要编辑全局配置文件或将其重置为原始默认值，请选择全局配置文件所在的行，然后单击“**重置**”。您无法删除全局配置文件。



通知

您可以在 Citrix Endpoint Management 中使用通知来实现以下目的：

- 与选定的用户组就多项系统相关功能进行通信。您还可以将这些通知定向到特定用户。例如，所有使用 iOS 设备的用户、设备不合规的用户、拥有员工自有设备的用户等。
- 注册用户及其设备
- 在满足特定条件时自动通知用户（使用自动化操作）。例如：
  - 当用户设备因合规性问题即将被公司域阻止时
  - 当设备已被越狱或 Root 时

有关自动化操作的详细信息，请参阅自动化操作。

要使用 Citrix Endpoint Management 发送通知，您必须配置网关和通知服务器。您可以在 Citrix Endpoint Management 中设置通知服务器以配置 SMTP 服务器。这些服务器会向用户发送电子邮件通知。您可以使用通知通过 SMTP 发送消息。

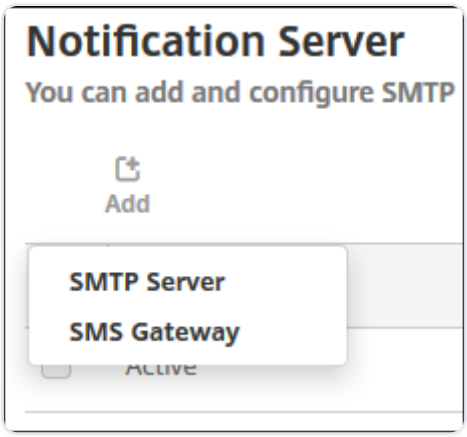
- SMTP 是一种面向连接的、基于文本的协议，其中邮件发送方与邮件接收方进行通信。邮件发送方发出命令字符串并提供必要数据，通常通过 TCP 连接。SMTP 会话由 SMTP 客户端（发送消息的人）发出的命令和 SMTP 服务器的相应响应组成。

先决条件

- 配置 SMTP 通知服务器以向用户发送消息。如果服务器托管在内部服务器上，请联系您的系统管理员获取配置信息。如果服务器是托管电子邮件服务，请在服务提供商的网站上查找相应的配置信息。
- 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。
- 在您的网络 DMZ 中，从 Citrix Endpoint Management 打开端口 25，使其指向内部网络上的 SMTP 服务器。这使得 Citrix Endpoint Management 能够成功发送通知。

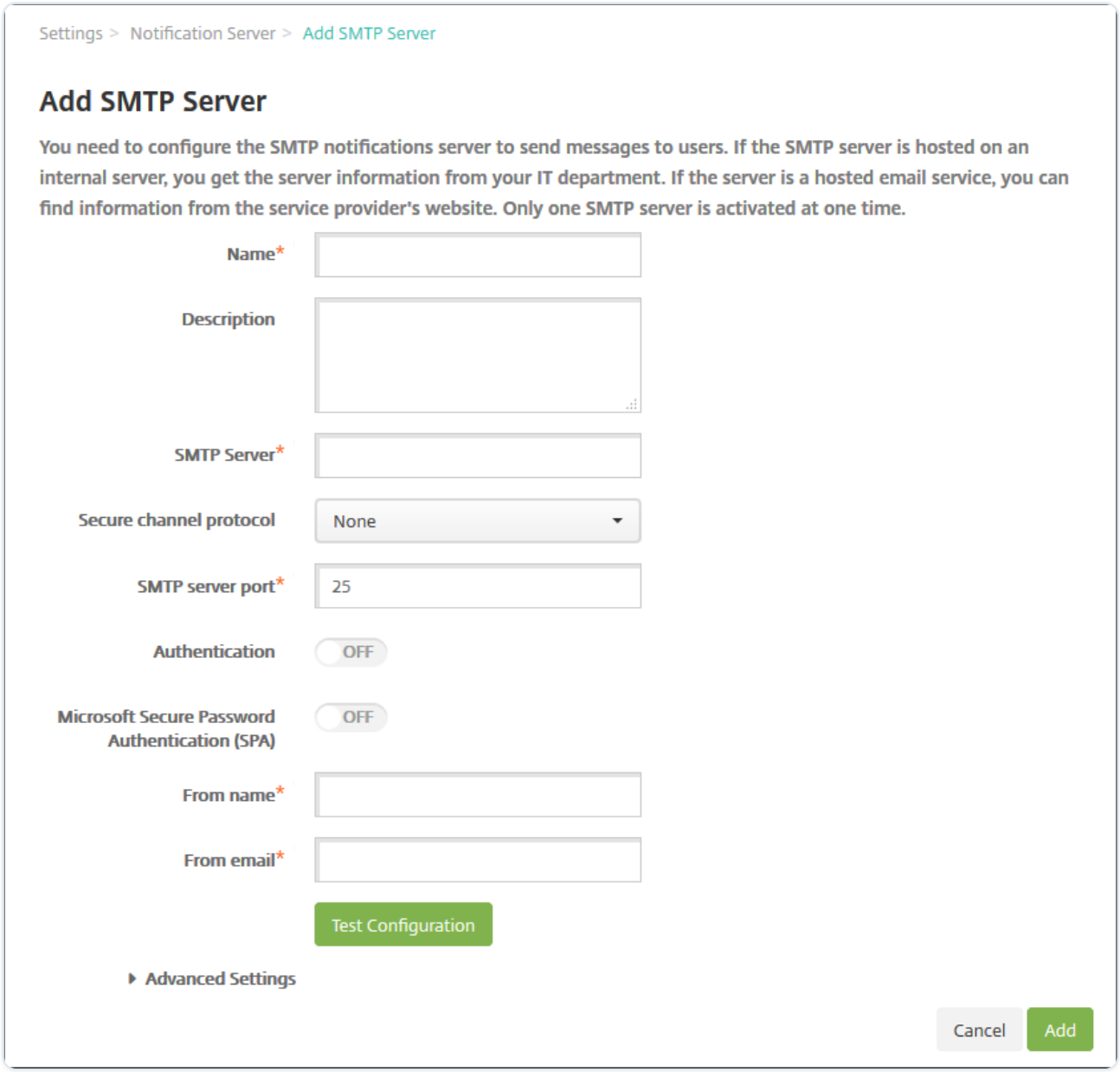
配置 SMTP 服务器

1. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标。将显示“**设置**”页面。
2. 在**通知**下，单击**通知服务器**。**通知服务器**页面显示。
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。

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。
   - **描述:** （可选）输入服务器的描述。
   - **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:** 在下拉列表中单击**SSL**、**TLS**或**无**，以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，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:** 键入用于身份验证的用户名。
- **密码：** 输入身份验证用户的密码。

> **重要提示：**
>
> 要将 OAuth 与 Microsoft Exchange Online 结合使用，您必须首先 在 Microsoft Entra ID 中注册您的应用程序。注册后，启用 **身份验证** 和 **Microsoft Exchange Online OAuth 2.0**。

- 如果您启用 **身份验证** 和 **Microsoft Exchange Online OAuth 2.0**，请配置以下设置：
  - **用户名：** 输入用于身份验证的用户名。
  - **租户 ID：** 输入您的 Microsoft Entra ID 目录的租户 ID。
  - **客户端 ID：** 输入您注册的应用程序的客户端（应用程序）ID。您可以在 Azure 门户 > 您的注册应用程序 > **应用程序（客户端）ID** 中找到它。
  - **客户端密钥：** 输入您注册的应用程序的客户端密钥。您可以在 Azure 门户 > 您的注册应用程序 > **证书和密钥** 中找到它。
- **Microsoft 安全密码身份验证 (SPA)：** 如果 SMTP 服务器正在使用 SPA，请单击 **开**。默认值为 **关**。
- **发件人名称：** 输入在客户端从该服务器收到通知电子邮件时，**发件人** 框中显示的名称。例如，公司 IT。
- **发件人电子邮件：** 输入当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**，然后配置这些设置：
   - **SMTP 重试次数：** 输入重试从 SMTP 服务器发送的失败消息的次数。默认值为 5。
   - **SMTP 超时：** 输入发送 SMTP 请求时等待的持续时间（以秒为单位）。如果消息发送因超时而持续失败，请增加此值。降低此值时请谨慎，以免增加超时和未送达消息的数量。默认值为 30 秒。
   - **SMTP 收件人最大数量：** 输入 SMTP 服务器发送的每封电子邮件的最大收件人数量。默认值为 100。
4. 单击 **添加**。

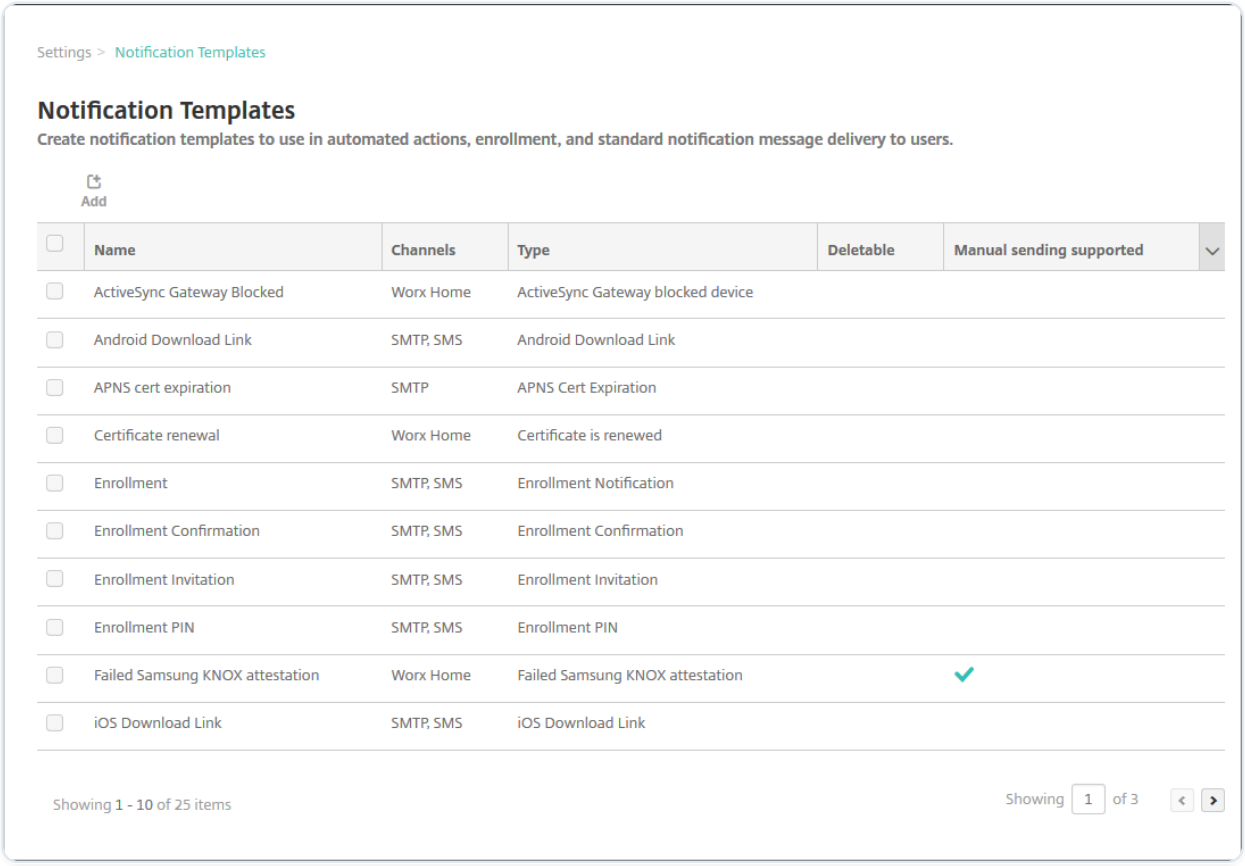
创建和更新通知模板

您可以在 Citrix Endpoint Management 中创建或更新通知模板，以用于自动化操作、注册以及发送给用户的标准通知消息。您可以配置通知模板，通过两种不同的通道发送消息：Citrix Secure Hub 或 SMTP。

Citrix Endpoint Management 包含许多预定义的通知模板。这些模板反映了 Citrix Endpoint Management 针对系统中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，则必须先设置这些通道才能激活它们。如果尚未设置通道，Citrix Endpoint Management 会在您添加通知模板时提示您设置通道。

1. 在 Citrix 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。



添加通知模板

1. 单击“**添加**”。如果未设置 SMTP 服务器，则会显示一条有关使用 SMTP 通知的消息。您可以选择立即设置 SMTP 服务器，也可以稍后设置。

   如果您选择立即设置 SMTP 服务器设置，则会重定向到“**设置**”页面上的“**通知服务器**”页面。设置完要使用的通道后，您可以返回“**通知模板**”页面以继续添加或修改通知模板。

   > **重要提示：**
   >
   > 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无法激活这些通道。因此，这些通道无法用于发送用户通知。

2. 配置以下设置：

   - **名称：**键入模板的描述性名称。
   - **描述：**键入模板的描述。
   - **类型：**在下拉列表中单击通知类型。仅显示所选类型支持的通道。只允许一个 APNS 证书过期模板，这是一个预定义模板。您无法添加此类型的模板。

   > **注意：**
   >
   > 对于某些模板类型，“支持手动发送”短语会显示在类型下方。这些模板类型在**控制板**上的**通知**列表和**设备**页面上可用。您可以从这些位置手动向用户发送通知。如果任何模板在任何通道的“主题”或“消息”字段中使用以下宏，则不支持手动发送：

   - ${outofcompliance.reason(whitelist_blacklist_apps_name)}
   - ${outofcompliance.reason(smg_block)}

     > **注意：**
     >
     > Citrix Endpoint Management 控制台包含“黑名单”和“白名单”术语。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

3. 在**通道**下，配置要用于此通知的每个通道的信息。您可以选择任何或所有通道。您选择的通道取决于您希望如何发送通知：

- 如果您选择 **Citrix Secure Hub**，则只有 iOS 和 Android 设备会收到通知，通知会显示在设备通知托盘中。
- 如果您选择 **SMTP**，则使用其电子邮件地址注册的用户会收到消息。

思杰安全中心：

- **激活：** 单击以启用通知通道。
- **消息：** 键入要发送给用户的消息。如果您正在使用 Citrix Secure Hub，则此字段为必需字段。有关在消息中使用宏的信息，请参阅宏。
- **声音文件：** 在列表中，单击用户在收到通知时听到的通知声音。

SMTP：

- **激活：** 单击以启用通知通道。

  只有在设置 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、电子邮件地址或两者。
- **收件人：** 此字段有一个预构建的宏，适用于除即席通知之外的所有通知，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。您可以通过在此字段中添加更多收件人（例如公司管理员）的地址来添加他们。使用分号 (;) 分隔宏和其他地址。要发送即席通知，您可以输入特定的收件人，或者您可以从“**管理 > 设备**”页面选择设备并从那里发送通知。有关详细信息，请参阅设备。
- **主题：** 为通知键入描述性主题。此字段为必填项。
- **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**”。当所有通道都正确配置后，它们将按此顺序显示在“**通知模板**”页面上：SMTP 和 Citrix Secure Hub。任何未正确配置的通道将显示在已正确配置的通道之后。

编辑通知模板

1. 选择一个通知模板。将显示该模板的编辑页面。您可以编辑模板（**类型**字段除外），并激活或停用通道。
2. 点击 **保存**。

删除通知模板

您只能删除您添加的通知模板。您无法删除预定义的通知模板。

1. 选择一个现有通知模板。
2. 单击“**删除**”。将显示一个确认对话框。

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

Citrix Endpoint Management 中的基于角色的访问控制 (RBAC) 功能允许您将角色分配给用户和组。角色是控制用户对系统功能访问级别的权限集。

Citrix Endpoint Management 附带以下默认用户角色。您可以将默认角色用作模板，自定义这些模板以创建自己的用户角色。

- **管理员：** 授予完整的系统访问权限。
- **用户：** 允许用户注册设备并访问自助服务门户。

您可以使用 Citrix 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 **身份和访问管理 > 管理员** 将角色分配给 Citrix Cloud 中的管理员。请参阅 。

使用 RBAC 功能

您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** 将角色分配给本地用户。您只能为本地用户分配一个角色。要更改角色，您可以手动编辑用户帐户。或者，您可以为本地用户创建一个组，并将角色分配给该组。
- **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 Citrix Endpoint Management 控制台中创建 RBAC 角色，并通过 Citrix Cloud 中的 **身份和访问管理 > 管理员** 将角色分配给这些用户。
- **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，则所有权限将合并以定义该用户的权限。例如，假设 ADGroupA 用户可以定位经理设备，而 ADGroupB 用户可以擦除员工设备。属于这两个组的用户可以定位和擦除经理和员工的设备。如果用户属于具有冲突权限的组，则允许的权限优先。

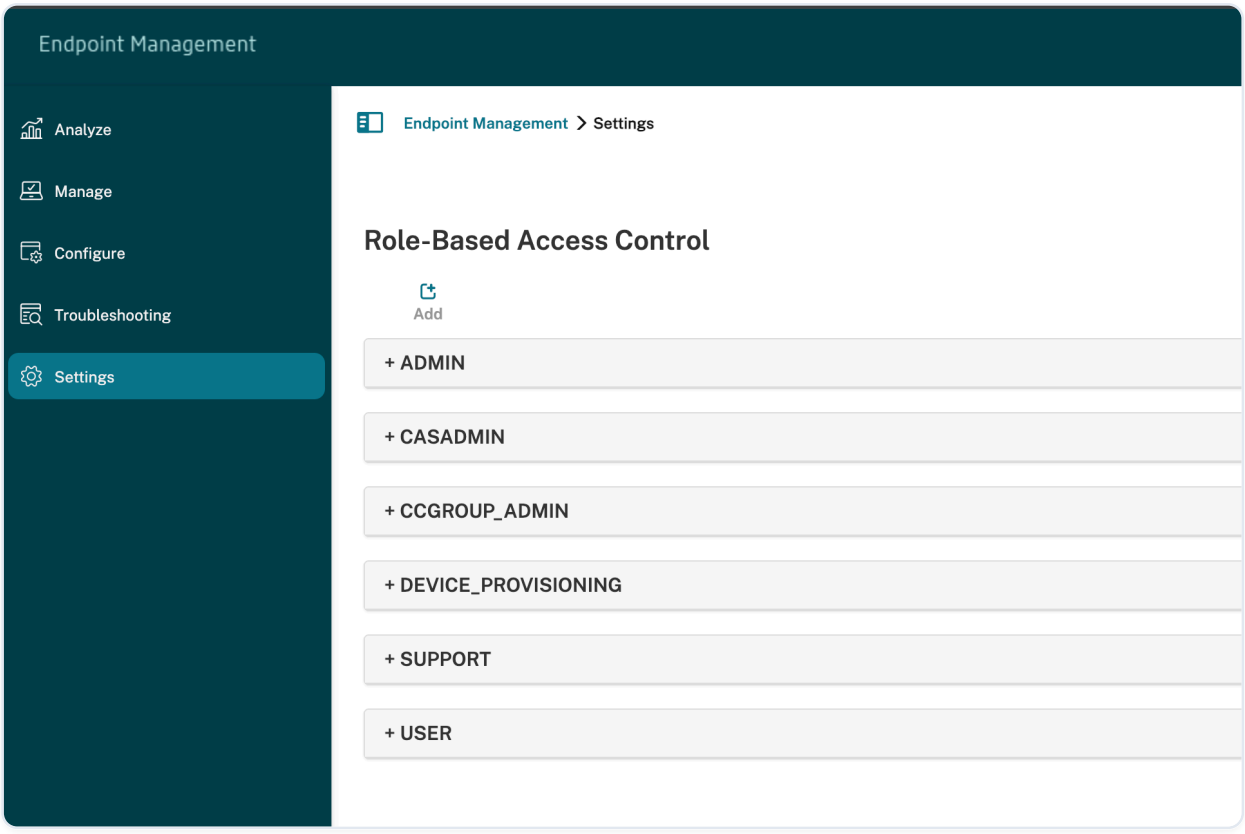
有关详细信息，请参阅 关于用户帐户。

创建或编辑角色

1. 在 Citrix 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。



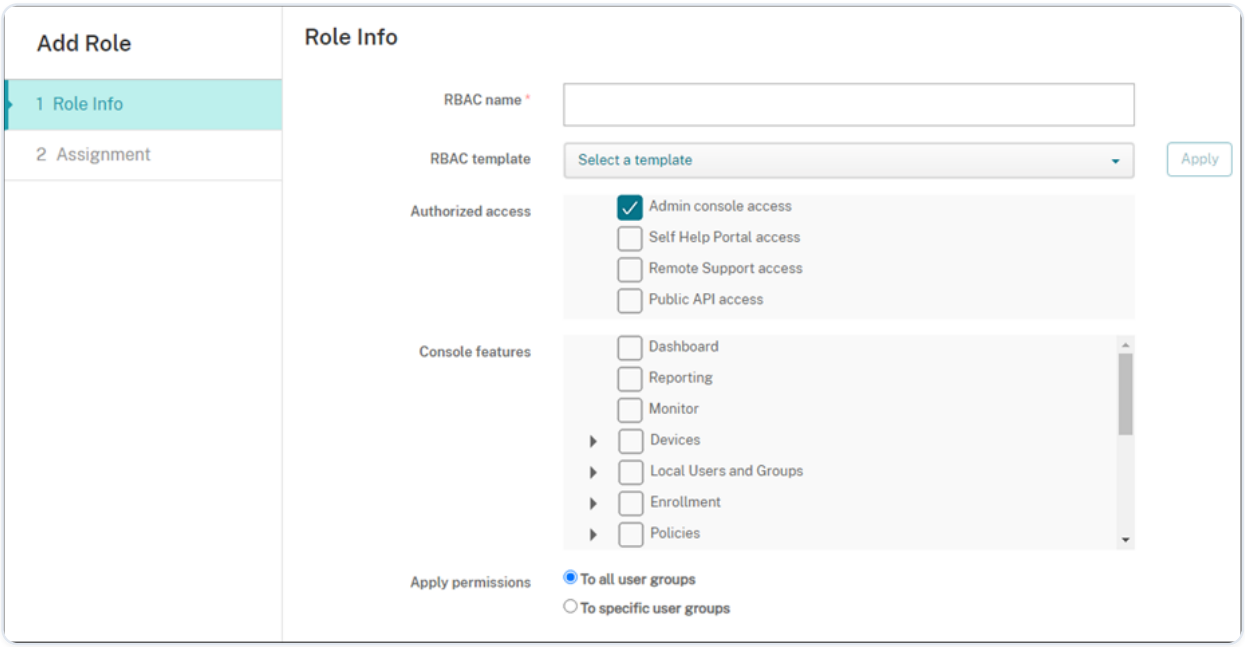
3. 要添加角色，请单击“**添加**”。或者，要编辑角色，请单击现有角色右侧的笔形图标。

> **注意：**
>
> 您可以通过单击已定义角色右侧的垃圾桶图标来删除该角色。您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：** 为新用户角色输入一个描述性名称。您无法更改现有角色的名称。
   - **RBAC 模板：** （可选）选择一个模板作为新角色的起点。（编辑角色时，您无法选择或更改模板。）RBAC 模板是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。Citrix Endpoint Management 会使用所选模板的预定义访问和功能权限填充这些字段。



5. 要自定义角色，请在“**授权访问**”和“**控制台功能**”中选择或清除复选框。

   单击控制台功能旁边的三角形可显示并选择该功能特有的权限。单击顶级复选框不会选择单个权限。展开顶级权限后，选择各个选项。

6. **应用权限：** 单击“**到特定用户组**”以将权限应用于您选择的组。

   例如，如果 RBAC 管理员拥有 ActiveDirectory 用户组的权限：

   - 该管理员只能访问属于 ActiveDirectory 组的用户的相关信息。
   - 该管理员无法查看任何其他本地或 AD 用户。该管理员可以查看属于这些组的任何子组的成员用户。
   - 该管理员可以向以下对象发送邀请：
     - 权限组及其子组
     - 属于权限组及其子组的用户

   思杰端点管理 RBAC 配置(/en-us/citrix-endpoint-management/media/rbac-apply-permissions.png)

7. 单击“**下一步**”并输入以下信息，以将角色分配给用户组。

   思杰端点管理 RBAC 配置(/en-us/citrix-endpoint-management/media/rbac-assignment-page.png)

   - **选择域：**从列表中选择一个域。
   - **搜索用户组：**单击“**搜索**”以查看所有可用组的列表。键入完整或部分组名称以缩小搜索范围。

- **包括用户组：**在出现的列表中，选择要为其分配角色的用户组。

8. 点击 **保存**。

将角色添加到 Citrix Cloud 管理员

无需通过 Citrix Endpoint Management 控制台将 RBAC 角色分配给 Citrix Cloud 管理员，而是从 Citrix Cloud 控制台分配角色。

1. 在 Citrix Cloud 控制台中，导航到“**身份和访问管理 > 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 **邀请**。

   单击现有管理员行末尾的 **...** 以编辑这些权限。
3. 单击 **自定义访问**。为管理员分配权限时，您可以选择在 Citrix Endpoint Management 控制台中创建的 RBAC 角色。

   Citrix Cloud 中的 RBAC 角色(/en-us/citrix-endpoint-management/media/rbac-roles-citrix-cloud.png)
4. 单击 **发送邀请** 以向新管理员发送邀请，或单击 **保存** 以完成管理员编辑。

预定义角色

每个预定义的 RBAC 角色都具有某些关联的访问和功能权限。下表描述了管理员角色和用户角色的每个权限。您不能删除或编辑预定义角色。

- 有关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值
- 有关 Citrix Endpoint Management 用户帐户的信息，请参阅 关于用户帐户。

> **重要提示：**
>
> 在“设置”权限下，RBAC 权限授予管理员用户完全访问权限，包括分配其自身权限的能力。仅将此访问权限授予您打算授予其操作 Citrix Endpoint Management 系统中所有内容的权限的用户。

管理员角色

预定义的管理员角色在 Citrix Endpoint Management 中提供特定访问权限。默认情况下，**授权访问**（自助服务门户除外）、**控制台功能** 和 **应用权限** 处于启用状态。

您可以使用 **管理 > 用户** 更改分配有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用户和本地用户拥有完全访问权限。

管理员的授权访问

管理员控制台访问权限	管理员可以访问 Citrix Endpoint Management 控制台上的所有功能。
自助服务门户访问	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，以编程方式执行 Citrix Endpoint Management 控制台上可用的操作。这些操作包括管理证书、应用程序、设备、交付组和本地用户。

适用于管理员的控制台功能

管理员对 Citrix Endpoint Management 控制台拥有不受限制的访问权限。

仪表板	**仪表板**是管理员登录 Citrix Endpoint Management 控制台后看到的第一个页面。**仪表板**显示有关通知和设备的基本信息。
报告	**分析 > 报告**页面提供预定义报告，可用于分析您的应用程序和设备部署。
设备	**管理 > 设备**页面是您管理用户设备的地方。您可以在此页面上添加单个设备，或导入设备预配文件以一次性添加多个设备。
本地用户和组	“**管理 > 用户**”页面是您添加、编辑或删除本地用户和本地用户组的位置。
注册	“**管理 > 注册邀请**”页面是您管理如何邀请用户将其设备注册到 Citrix Endpoint Management 的位置。

策略	“**配置 > 设备策略**”页面是您管理设备策略（例如 VPN 和网络）的位置。
应用程序	“**配置 > 应用程序**”页面是您管理用户可以在其设备上安装的各种应用程序的位置。
媒体	“**配置 > 媒体**”页面是您管理用户可以在其设备上安装的各种媒体的位置。
操作	“**配置 > 操作**”页面是您管理对触发事件的响应的位置。
交付组	“**配置 > 交付组**”页面是您管理交付组及其关联资源的位置。
注册配置文件	“**配置 > 注册配置文件**”页面是您指定用户如何注册其设备的位置。
适用于企业的 Alexa	“**设置**”页面是您管理适用于企业的 Alexa 配置文件的位置。
设置	“**设置**”页面是您管理系统设置（例如客户端和服务器属性、证书和凭据提供程序）的位置。**重要提示：**这些设置包括 RBAC 权限。RBAC 权限授予管理员完全访问权限，包括分配其自身权限的能力。仅向您打算授予操作 Citrix Endpoint Management 系统中所有内容的权限的用户授予此访问权限。
支持	“**故障排除和支持**”页面是您执行故障排除活动（例如运行诊断和生成日志）的地方。

管理员的设备限制

管理员通过设置设备限制、设置并向设备发送通知、管理设备上的应用程序等方式，在整个控制台中访问设备功能。

完全擦除设备	擦除设备上的所有数据和应用程序，包括设备上的存储卡（如果有）。
清除限制	移除一个或多个设备限制。

选择性擦除设备	擦除设备上的所有企业数据和应用程序，保留个人数据和应用程序。
查看位置	查看设备位置并设置地理限制。包括：定位设备、跟踪设备。
锁定设备	远程锁定设备，以便用户无法使用该设备。
解锁设备	远程解锁设备，以便用户可以使用该设备。
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	在启用激活锁时，在受监管的 iOS 设备上存储旁路代码。要擦除设备，请使用此代码自动清除激活锁。
获取常驻用户	列出当前设备上具有活动帐户的用户。此操作会强制设备与 Citrix 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。用户可以再次登录。
响铃设备	远程以最大音量响铃 Windows 设备 5 分钟。
重新启动设备	从 Citrix Endpoint Management 控制台重新启动 Windows 设备。
部署到设备	将应用程序、通知、限制和其他资源发送到设备。
编辑设备	更改设备上的设置。
设备通知	向设备发送通知。
添加/删除设备	从 Citrix Endpoint Management 添加或删除设备。

设备导入	将一组设备从文件导入到 Citrix Endpoint Management。
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 Citrix Endpoint Management。
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 Citrix Endpoint Management。在 iOS 上，用户可以登录，但无法访问应用程序。
应用程序擦除	在 Android 上，此限制会删除用户的 Citrix Endpoint Management 帐户。在 iOS 上，此限制会删除用户访问 Citrix Endpoint Management 功能所需的加密密钥。
查看软件清单	查看设备上安装了哪些软件。
请求 AirPlay 镜像	请求开始 AirPlay 流式传输。
停止 AirPlay 镜像	停止 AirPlay 流式传输。
启用丢失模式	在 **管理 > 设备** 页面上，您可以将受监管设备置于丢失模式，以在锁定屏幕上阻止受监管设备。然后，当设备丢失或被盗时，您可以定位该设备。
禁用丢失模式	在 **管理 > 设备** 页面上，您可以为已设置为丢失模式的设备禁用丢失模式。
更新设备操作系统	您可以将操作系统更新设备策略部署到设备。
关闭设备	从 Citrix Endpoint Management 控制台关闭 iOS 设备。
重新启动设备	从 Citrix 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 Citrix Endpoint Management 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
获取本地用户锁定 ID
删除本地用户锁定

注册

管理员可以添加和删除注册邀请、向用户发送通知，并将注册表导出为 .csv 文件。

添加/删除注册	向单个用户或用户组添加或删除注册邀请。
通知用户	向单个用户或用户组发送注册邀请。
导出注册邀请表	从“注册”页面收集注册信息并将其导出为 .csv 文件。

策略

添加/删除策略	添加或删除设备或应用程序策略。
编辑策略	更改设备或应用程序策略。
上传策略	上传设备或应用程序策略。
克隆策略	复制设备或应用程序策略。
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 Citrix Endpoint Management 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）。
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	向 Citrix Endpoint Management 添加或删除 MDX 应用程序、内部网络应用程序 (Web 应用程序) 或公共网络应用程序 (SaaS)。
编辑 MDX、Web 和 SaaS 应用程序	更改 Citrix Endpoint Management 中的 MDX 应用程序、内部网络应用程序 (Web 应用程序) 或公共网络应用程序 (SaaS)。
添加/删除类别	添加或删除应用程序可在应用商店中显示的类别。
将公共/企业应用程序分配到交付组	将公共应用商店应用程序或 MDX 应用程序分配到交付组以进行部署。
将 MDX/WebLink/SaaS 应用程序分配到交付组	将 MDX 应用程序、不需要单点登录的应用程序 (WebLink) 或来自公共网络 (SaaS) 的应用程序分配到交付组。
导出应用程序表	从“应用程序”页面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或批量采购许可证的媒体。

添加/删除应用商店或企业图书
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。触发器可以是事件、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。触发器可以是事件、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。
导出操作	从“操作”页面收集操作信息并将其导出到 .csv 文件。

交付组

管理员从**配置 > 交付组**页面管理交付组。

添加/删除交付组	创建或删除交付组，该操作会添加指定用户以及可选策略、应用程序和操作。
编辑交付组	更改现有交付组，这会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”页面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

适用于企业的 ALEXA

管理适用于企业的 Alexa 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

管理员设置

管理员在**设置**页面上配置各种设置。

RBAC	RBAC 分配。**重要提示：**此权限授予管理员完全访问权限，包括分配其自身权限的能力。仅将此访问权限授予您打算授予其操作 Citrix Endpoint Management 系统中所有内容的权限的用户。
LDAP	管理一个或多个符合 LDAP 的目录（例如 Active Directory），以导入组、用户帐户和相关属性。
注册	为用户和自助服务门户启用注册安全模式。
版本管理	查看当前安装的版本。包括：版本管理更新
证书	编辑 APNS 证书
通知模板	创建通知模板，用于自动化操作、注册以及向用户发送标准通知消息。
工作流	管理用户帐户的创建、批准和删除，以用于应用程序配置。

凭据提供程序	添加一个或多个有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 证书服务或自由裁量 CA）。
测试 PKI 连接	使用“**设置 > PKI 实体**”页面上的“**测试连接**”按钮，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，例如密码类型、强度和过期时间。
客户端支持	设置用户联系支持服务的方式（电子邮件、电话或支持工单电子邮件）。
客户端品牌	为应用商店创建自定义商店名称和默认商店视图。添加显示在应用商店或 Citrix Secure Hub 中的自定义徽标。
运营商短信网关	设置运营商短信网关，以配置 Citrix Endpoint Management 通过运营商短信网关发送的通知。
通知服务器	设置 SMTP 网关服务器以向用户发送电子邮件。
ActiveSync 网关	通过规则和属性管理用户对用户和设备的访问。
谷歌浏览器	配置 Citrix Endpoint Management 以与您的 Google Workspace 帐户通信。
Apple 部署计划	将 Apple 部署计划帐户添加到 Citrix Endpoint Management。
Apple Configurator 设备注册	在 Citrix 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 网关	在 Citrix Endpoint Management 中配置 NetScaler Gateway（现已更名为 NetScaler Gateway）设置。
网络访问控制	设置确定设备不合规的条件，使其无法访问网络。
服务器属性	添加或修改服务器属性。需要重新启动所有节点上的 Citrix Endpoint Management。
虚拟应用和桌面	允许用户通过 Citrix Workspace 应用程序添加 Citrix Virtual Apps and Desktops。
Citrix 文件	将 Citrix Endpoint Management 与企业帐户配合使用时：配置设置以连接到 ShareFile 和管理员服务帐户以进行用户帐户管理。需要现有的 Citrix Files 域和管理员凭据。将 Citrix Endpoint Management 与存储区域连接器配合使用时：配置 Citrix Endpoint Management 以指向存储区域连接器中定义的网络共享和 SharePoint 位置。
安卓企业版	配置 Android Enterprise 服务器设置。
身份提供程序 (IdP)	配置身份提供程序。
思杰端点管理工具	访问 Citrix 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 连接性检查	通过 IP 地址对 NetScaler Gateway 执行各种连接性检查。需要用户名和密码。
Citrix Endpoint Management 连接性检查	对选定的 Citrix Endpoint Management 功能（例如数据库、DNS 和 Google Plan）执行连接性检查。

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	查看和下载日志文件。
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。配置单个策略，将其部署到大量用户，并让每个目标用户显示用户特定的值。
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 (APNs) 证书请求，或上传适用于 iOS 的 Citrix Secure Mail APNs 证书。
Citrix 洞察服务	将日志上传到 Citrix Insight Services (CIS)，以获取各种问题的帮助。
用于 Exchange ActiveSync 状态的设备 NetScaler Gateway 连接器	查询 Citrix Endpoint Management，以获取发送到 Exchange ActiveSync 连接器的设备状态。查询基于设备 ActiveSync ID。

限制组访问

管理员用户可以将权限应用于所有用户组。

用于设备预配的控制台功能

设备预配用户对 Citrix Endpoint Management 控制台具有以下受限访问权限。默认情况下，以下每个功能都已启用。

设备限制

编辑设备	更改设备上的设置。
添加/删除设备	从 Citrix Endpoint Management 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，但无权配置这些功能。

用户角色

具有用户角色的用户对 Citrix Endpoint Management 具有以下受限访问权限。

供用户使用的授权访问

自助服务门户	仅向用户提供对 Citrix Endpoint Management 中的自助服务门户的访问权限。

供用户使用的控制台功能

用户对 Citrix Endpoint Management 控制台具有以下受限访问权限。

供用户使用的设备受限访问

完全擦除设备	擦除设备上的所有数据和应用程序，包括设备上的存储卡（如果有）。
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	查看设备位置并设置地理限制。包括：定位设备、查看设备位置、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	在启用激活锁时，在受监管的 iOS 设备上存储绕过代码。要擦除设备，请使用此代码自动清除激活锁。

获取常驻用户	列出当前设备上具有活动帐户的用户。此操作会强制设备与 Citrix 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。用户可以再次登录。
响铃设备	远程使 Windows 设备以最大音量响铃 5 分钟。
重启设备	重启 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 Citrix Endpoint Management。在 iOS 上，用户可以登录，但无法访问应用程序。
应用程序擦除	在 Android 上，此限制会删除用户的 Citrix Endpoint Management 帐户。在 iOS 上，此限制会删除用户访问 Citrix Endpoint Management 功能所需的加密密钥。
查看软件清单	查看设备上安装了哪些软件。

用户的注册限制

添加/删除注册	添加或删除针对一个用户或一组用户的注册邀请。
通知用户	向一个用户或一组用户发送注册邀请。

限制所有角色的组访问

对于默认角色，此权限默认已设置，并可应用于所有用户组。您无法编辑此角色。

许可证

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 Citrix Endpoint Management 的许可证和活动使用情况

设备管理

Citrix Endpoint Management 可以在单个管理控制台中预配、管理、保护和清点各种设备类型。

- 使用一组通用的设备策略来管理受支持的设备。要快速查看按平台提供的设备策略，请执行以下操作：

  a. 转到 Citrix Endpoint Management 控制台，然后导航到 **Configure > Device Polices**（配置 > 设备策略）。

  b. 单击 **Add**（添加），然后选择要查看的平台。

  有关详细信息，请参阅筛选已添加的设备策略列表。

- 通过对身份、公司拥有的设备和 BYO 设备、应用程序、数据和网络实施严格的安全措施来保护业务信息。指定用于对设备进行身份验证的用户身份。配置如何在设备上将企业数据和个人数据分开。
- 无论设备或操作系统如何，均可向最终用户交付任何应用程序。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。
- 使用预配和配置控件来设置设备。这些控件包括设备注册、策略应用和访问权限。
- 使用安全和合规性控件创建具有可操作触发器的自定义安全基线。例如，锁定、擦除或通知违反定义的合规性标准的设备。
- 使用操作系统更新控件来阻止或强制执行操作系统更新。此功能对于防止针对操作系统漏洞的数据丢失至关重要。

要访问有关每个受支持平台的文章，请在内容列表中展开“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了如何执行常规设备管理任务。

设备管理工作流程

本节中的工作流程图提供了设备管理任务的建议顺序。

1. **添加设备和应用程序的推荐先决条件：** 提前执行以下设置可让您不间断地配置设备和应用程序。

   添加设备和应用程序之前的推荐步骤(/en-us/citrix-endpoint-management/media/workflow-prereqs-for-adding-devices-apps.png)

请参阅：

部署资源

使用 RBAC 配置角色

创建和更新通知模板

创建和管理工作流程

2. **添加设备：**

   添加设备工作流程(/en-us/citrix-endpoint-management/media/workflow-add-devices.png)

   请参阅：

   准备注册设备和交付资源

   设备策略

   部署到交付组

   自动化操作

3. **准备注册邀请：** 您可以向使用 iOS、iPadOS、macOS、Android Enterprise 和旧版 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。

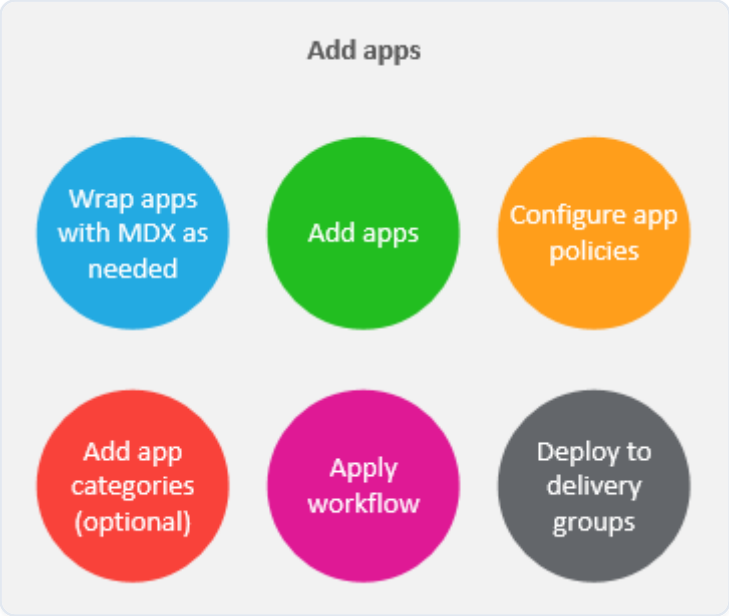
   准备注册邀请工作流程(/en-us/citrix-endpoint-management/media/workflow-enrollment-invitations.png)

   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

添加应用程序

关于应用程序类别

应用工作流程

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 Citrix Endpoint Management 控制板之外，我们还建议您查看每个版本的新增功能内容。新增功能提供了有关任何所需操作的信息，例如配置新的设备策略。



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

为了远程安全地管理用户设备，您需要在 Citrix Endpoint Management 中注册用户设备。Citrix Endpoint Management 客户端软件安装在用户设备上，并且用户身份经过身份验证。然后，安装 Citrix 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，请参阅本节中的设备文章。

在 Citrix Endpoint Management 控制台中：

- 您可以向使用 iOS、iPadOS、macOS、Android Enterprise 和旧版 Android 设备的用户发送注册邀请。注册邀请不适用于 Windows 设备。
- 您可以向使用 iOS、iPadOS、Android Enterprise 或旧版 Android 设备的用户发送邀请 URL。邀请 URL 不适用于 Windows 设备。

注册邀请的发送方式如下：

- 如果 Active Directory 用户在 Active Directory 中有电子邮件地址，他们会收到邀请。本地用户会在用户属性中指定的电子邮件地址收到邀请。

用户注册后，其设备将在 **管理 > 设备** 中显示为已管理。邀请 URL 的状态显示为 **已兑换**。

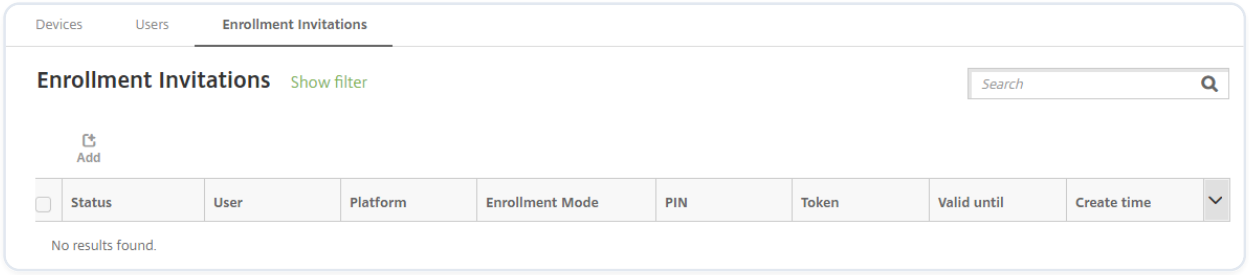
先决条件

- 已配置 LDAP
- 如果使用本地组和本地用户：
  - 一个或多个本地组。
  - 本地用户分配到本地组。
  - 交付组与本地组关联。
- 如果使用 Active Directory：

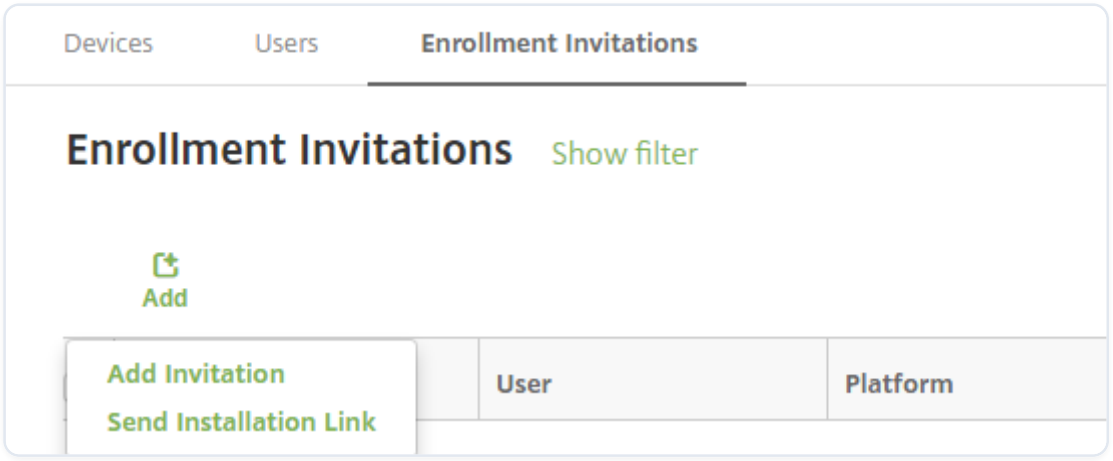
- 交付组与 Active Directory 组关联。

创建注册邀请

1. 在 Citrix Endpoint Management 控制台中，单击“**管理 > 注册邀请**”。将显示“**注册邀请**”页面。



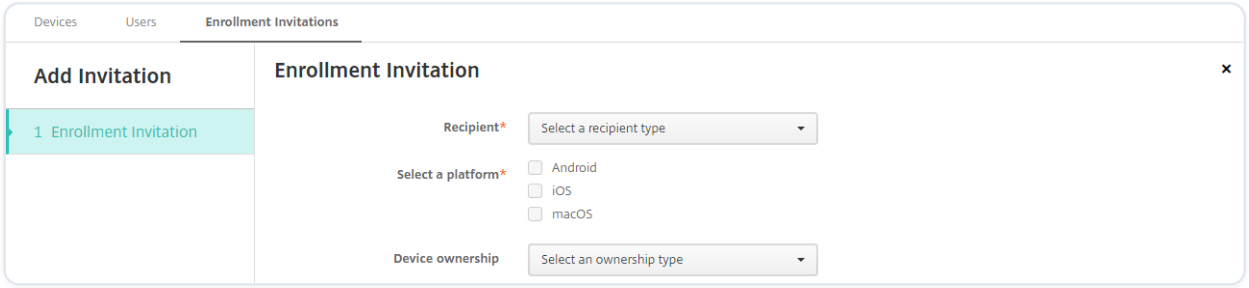
2. 单击“**添加**”。将显示注册选项菜单。



- 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**”。

这些步骤之后将介绍发送注册邀请和安装链接。

3. 单击“**添加邀请**”。将显示“**注册邀请**”屏幕。



4. 配置以下设置：

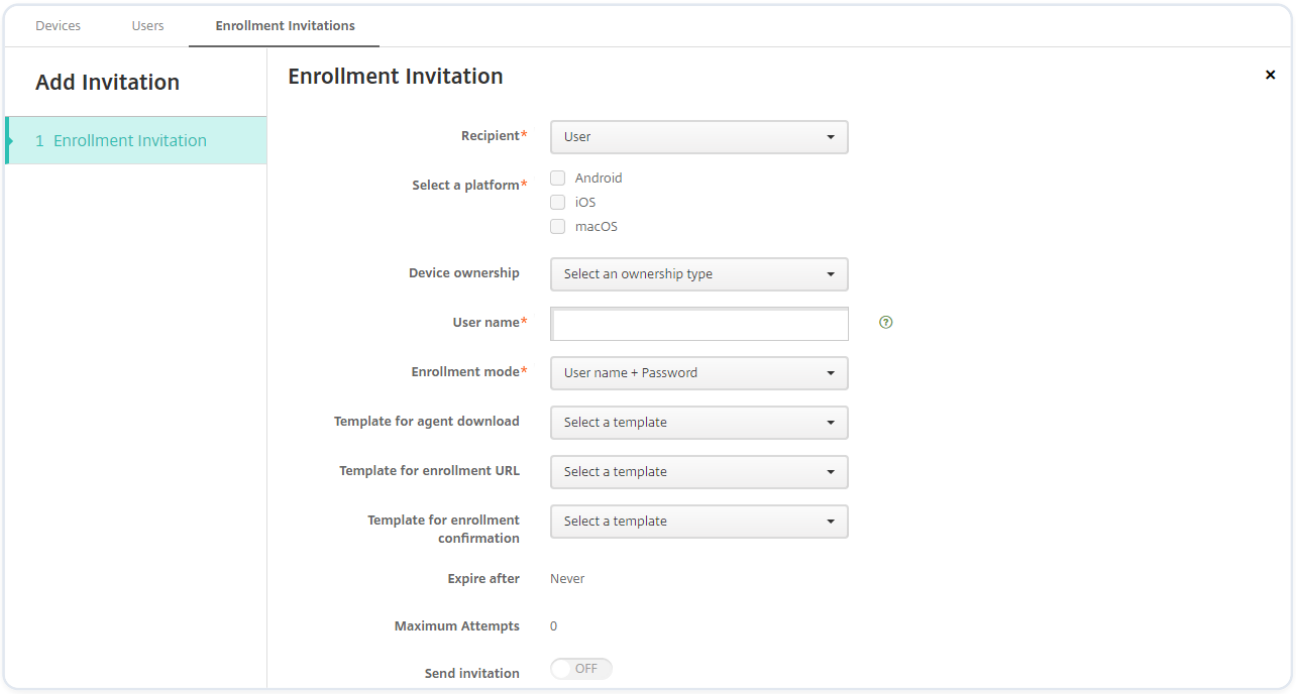
- **收件人：选择组**或**用户**。
- **选择平台：如果收件人是组**，则所有平台均已选择。您可以更改平台选择。如果**收件人是用户**，则未选择任何平台。选择一个平台。

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。**

用户或组的设置将显示，如下面各节所述。

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。该用户必须作为本地用户或 Active Directory 用户存在于 Citrix Endpoint Management 中。如果用户是本地用户，请设置该用户的电子邮件属性，以便您可以向该用户发送通知。如果用户在 Active Directory 中，则前提是已配置 LDAP。
   - **电话号码：**如果您选择多个平台或仅选择 macOS，则此设置不会显示。（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，则此设置不会显示。选择一个运营商以与用户的电话号码关联。
   - **注册模式：选择用户的注册安全模式。默认值为用户名 + 密码。**以下某些选项并非适用于所有平台：
     - **用户名 + 密码**
     - **邀请 URL**
     - **邀请 URL + PIN**
     - **邀请 URL + 密码**
     - **双因素**

- **用户名 + PIN**

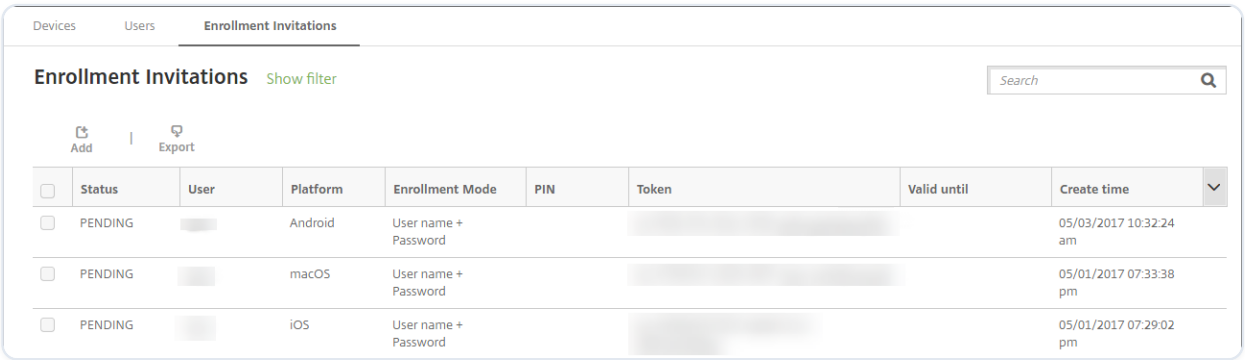
我们已弃用对**高安全性**注册模式的支持。要发送注册邀请，您只能使用**邀请 URL**、**邀请 URL + PIN** 或**邀请 URL + 密码**注册安全模式。对于使用**用户名 + 密码**、**双因素**或**用户名 + PIN** 注册的设备，用户必须下载 Citrix Secure Hub 并手动输入其凭据。

有关详细信息，请参阅按平台划分的注册安全模式。注册 PIN 也称为一次性 PIN。此类 PIN 仅在用户注册时有效。

> **注意：**
>
> 当您选择任何包含 PIN 的注册安全模式时，将显示**注册 PIN 模板**字段。单击**注册 PIN**。

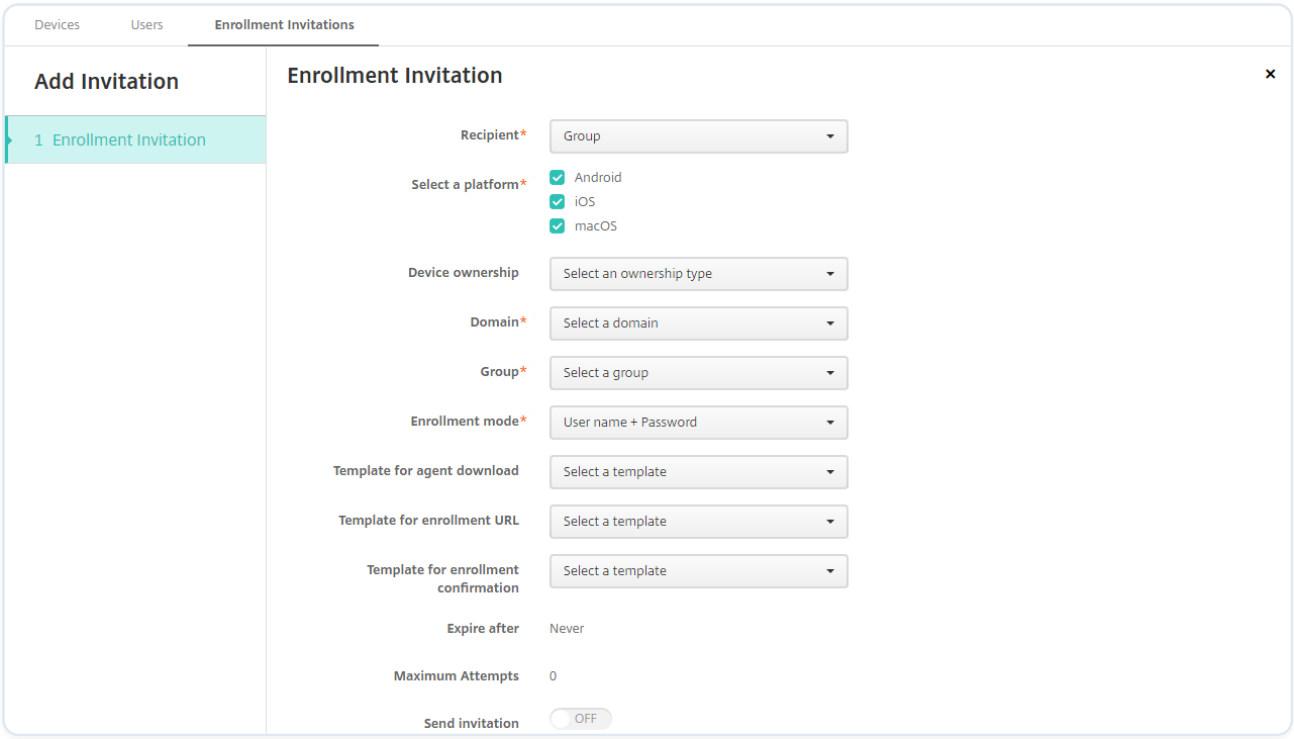
- **代理下载模板：** 选择名为**下载链接**的下载链接模板。该模板适用于所有受支持的平台。
- **注册 URL 模板：** 选择**注册邀请**。
- **注册确认模板：** 选择**注册确认**。
- **在此之后过期：** 此字段在您配置注册安全模式时设置，并指示注册何时过期。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- **最大尝试次数：** 此字段在您配置注册安全模式时设置，并指示注册过程发生的最大次数。
- **发送邀请：** 选择**开**可立即发送邀请。选择**关**可将邀请添加到**注册邀请**页面上的表格中，但不发送。

2. 如果您启用了**发送邀请**，请单击**保存并发送**。否则，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

下图显示了为组配置注册邀请的设置。



1. 配置以下设置：

   - **域：** 选择接收邀请的组的域。
   - **组：** 选择接收邀请的组。Citrix Endpoint Management 从 Active Directory 获取用户列表。该列表包括名称中包含特殊字符的用户。
   - **注册模式：** 选择您希望组中的用户如何注册。默认值为**用户名 + 密码**。以下某些选项并非适用于所有平台：
     - **用户名 + 密码**
     - **邀请 URL**
     - **邀请 URL + PIN**
     - **邀请 URL + 密码**
     - **双因素**
     - **用户名 + PIN**

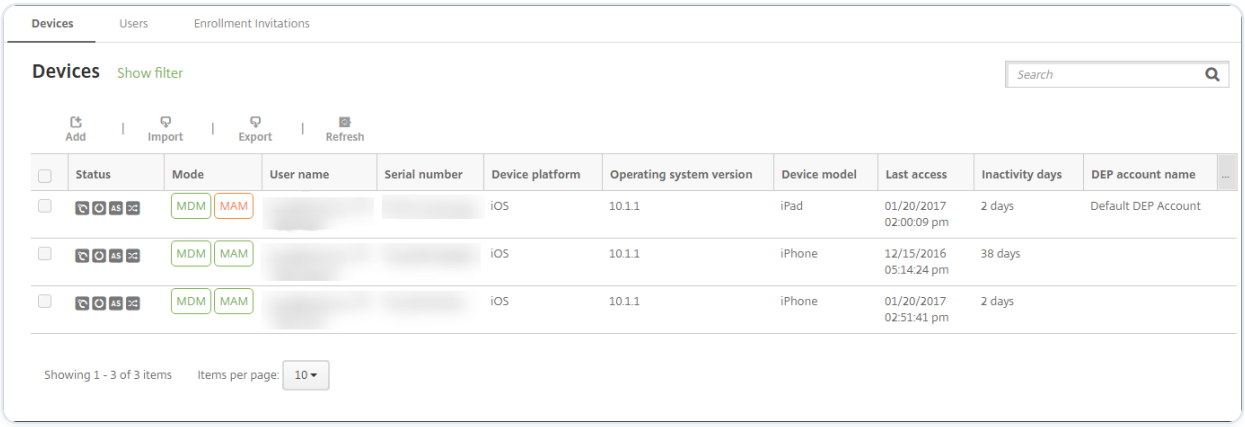
   我们已弃用对**高安全性**注册模式的支持。要发送注册邀请，您只能使用**邀请 URL**、**邀请 URL + PIN** 或**邀请 URL + 密码**注册安全模式。对于使用**用户名 + 密码**、**双因素**或**用户名 + PIN** 注册的设备，用户必须下载 Citrix Secure Hub 并手动输入其凭据。

   仅显示对每个选定平台有效的注册安全模式。有关详细信息，请参阅按平台划分的注册安全模式。

> **注意：**
>
> 当您选择任何包含 PIN 的注册安全模式时，将显示**注册 PIN 模板**字段。单击**注册 PIN**。

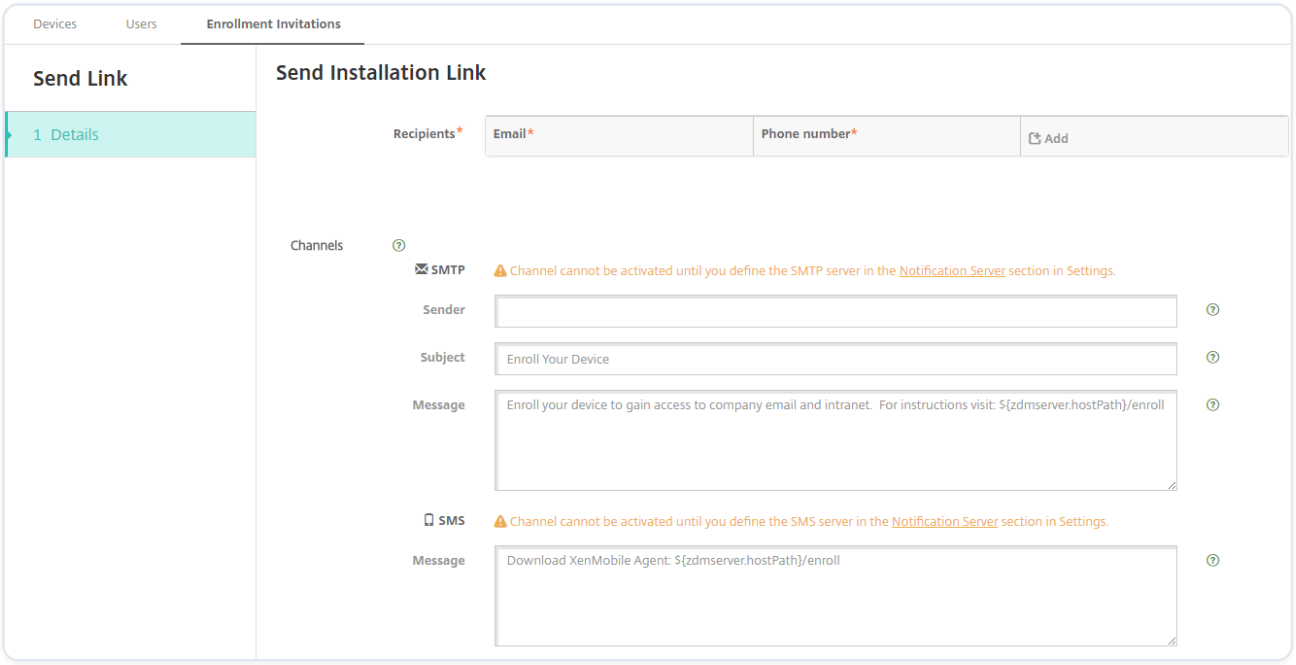
- **代理下载模板**：选择名为“**下载链接**”的下载链接模板。该模板适用于所有受支持的平台。
- **注册 URL 模板**：选择“**注册邀请**”。
- **注册确认模板**：选择“**注册确认**”。
- **过期时间**：此字段在配置注册安全模式时设置，指示注册何时过期。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- **最大尝试次数**：此字段在配置注册安全模式时设置，指示注册过程发生的最大次数。
- **发送邀请**：选择“**开**”可立即发送邀请。选择“**关**”可将邀请添加到“**注册邀请**”页面上的表格中，但不发送。

2. 如果您启用了“**发送邀请**”，请单击“**保存并发送**”。否则，单击“**保存**”。邀请将显示在“**注册邀请**”页面上的表格中。



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。此字段为必填项。
  - **电话号码**：键入收件人的电话号码。此字段为必填项。

> **注意：**
>
> 要删除收件人，请将鼠标悬停在包含该条目的行上，然后单击右侧的垃圾桶图标。此时将显示一个确认对话框。单击**删除**以删除该条目，或单击**取消**以保留该条目。
>
> 要编辑收件人，请将鼠标悬停在包含该条目的行上。然后，单击右侧的笔形图标。更新该条目，然后单击**保存**以保存更改的条目，或单击**取消**以保持该条目不变。

- **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之前，这些通道无法激活。有关详细信息，请参阅通知。
- **SMTP：** 配置这些可选设置。如果您未在这些字段中输入任何内容，则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：** 键入可选的发件人。
  - **主题：** 键入邮件的可选主题。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，“注册您的设备以访问组织应用程序和电子邮件。”

2. 单击**发送**。

> **注意：**
>
> 如果您的环境使用 sAMAccountName：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。

按平台划分的注册安全模式

下表显示了可用于注册用户设备的安全模式。在表中，**是**表示哪些设备平台支持具有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	NETSCALER 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）	安卓企业版	IOS（用户注册模式）	IOS	MACOS	视窗
通过 Citrix Cloud 将 Azure AD 和 Okta 作为身份提供程序	客户端证书	MDM+MAM 或 MDM	是	是	是	是	是	否	否

MDM 注册安全模式	NETSCALER 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）	安卓企业版	IOS（用户注册模式）	IOS	MACOS	视窗
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 模式不支持 NetScaler Gateway 上的客户端证书）	是	是	是	是	是	是	是
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

MDM 注册安全模式	NETSCALER 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）	安卓企业版	IOS（用户注册模式）	IOS	MACOS	视窗
邀请 URL + 密码	LDAP、LDAP + 客户端证书以及仅客户端证书	MDM +MAM 或 MDM	是	是	是	否	是	否	否
双因素身份验证（用户名 + 密码 + PIN）	LDAP、LDAP + 客户端证书以及仅客户端证书	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

以下描述了注册安全模式在 iOS、Android 和 Android Enterprise 设备上的行为：

- **用户名 + 密码**（默认）

- 向用户发送一条包含注册 URL 的通知。当用户点击该 URL 时，Citrix Secure Hub 将打开。用户随后输入用户名和密码，以在 Citrix Endpoint Management 中注册设备。

- **邀请 URL**
  - 向用户发送一条包含注册 URL 的通知。当用户点击该 URL 时，Citrix Secure Hub 将打开。Citrix Endpoint Management 服务器名称和“**是，注册**”按钮将显示。用户点击“**是，注册**”以在 Citrix Endpoint Management 中注册设备。
- **邀请 URL + PIN**
  - 向用户发送以下电子邮件：
    - 一封包含注册 URL 的电子邮件，用户可以通过该 URL 经由 Citrix Secure Hub 将设备注册到 Citrix Endpoint Management。
    - 一封包含一次性 PIN 的电子邮件，用户在注册设备时必须输入该 PIN 以及用户的 Active Directory（或本地）密码。
  - 在此模式下，用户只能通过通知中的注册 URL 进行注册。如果用户丢失了通知邀请，则无法注册。但是，您可以发送另一个邀请。
- **邀请 URL + 密码**
  - 向用户发送一个包含注册 URL 的通知。当用户单击该 URL 时，Citrix Secure Hub 将打开。Citrix Endpoint Management 服务器名称将显示，以及一个允许用户输入密码的字段。
- **双因素**
  - 向用户发送一个包含注册 URL 和一次性 PIN 的通知。当用户单击该 URL 时，Citrix Secure Hub 将打开。Citrix Endpoint Management 服务器名称将显示，以及两个允许用户输入密码和 PIN 的字段。
- **用户名 + PIN**
  - 向用户发送以下电子邮件：
    - 一封包含注册 URL 的电子邮件，用户可以通过该 URL 下载并安装 Citrix Secure Hub。Citrix Secure Hub 打开后，系统会提示用户输入用户名和密码以将设备注册到 Citrix Endpoint Management。
    - 一封包含一次性 PIN 的电子邮件，用户在注册设备时必须输入该 PIN 以及用户的 Active Directory（或本地）密码。
  - 如果用户丢失了通知邀请，则无法注册。但是，您可以发送另一个邀请。

以下描述了注册安全模式在 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。当用户单击该 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在 Citrix Endpoint Management 中注册设备。
- **双因素**
  - 向用户发送包含注册 URL 和一次性 PIN 的单个通知。当用户单击该 URL 时，Safari 浏览器将打开。此时将显示一个登录页面，其中包含两个字段，供用户键入密码和 PIN。
- **用户名 + PIN**
  - 向用户发送以下电子邮件：
    - 一封包含注册 URL 的电子邮件。当用户单击该 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在 Citrix Endpoint Management 中注册设备。
    - 一封包含一次性 PIN 的电子邮件，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。
  - 如果用户丢失了通知邀请，则无法注册。但是，您可以发送另一个邀请。

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。

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、解锁和擦除。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：** 在设备激活之前，从受监管的 iOS 设备中移除激活锁。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，用户无法登录 Citrix Endpoint Management。在 iOS 上，用户可以登录，但无法访问任何应用程序。
- **应用程序擦除：** 从 Citrix Secure Hub 中移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：** 为已注册到 Apple School Manager 的 iOS 设备创建激活锁绕过代码。

- **证书续订：** 对于受支持的 iOS、macOS 和 Android 设备，“证书续订”安全操作会启动证书续订。设备下次重新连接到 Citrix Endpoint Management 时，Citrix Endpoint Management 服务器会根据新的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 Citrix 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，并向设备发送要显示的消息、电话号码和脚注。第二次发送此命令会将设备带出丢失模式。
- **启用跟踪：** 在 Android 或 iOS 设备上，此命令允许 Citrix 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**”选项卡中。使用“**启用跟踪**”持续跟踪设备。Citrix Secure Hub 在设备运行时定期报告位置。
- **完全擦除：** 立即擦除设备上的所有数据和应用程序，包括任何存储卡中的数据。已擦除的设备会保留在“**管理 > 设备**”页面上的设备列表中，以供审计。您可以从设备列表中删除已擦除的设备。
  - 对于 Android 设备，此请求还可以包括擦除存储卡的选项。
  - 对于具有工作配置文件（COPE 设备）的 Android Enterprise 完全托管设备，您可以在选择性擦除删除工作配置文件后执行完全擦除。
  - 对于 iOS 和 macOS 设备，擦除会立即发生，即使设备已锁定。

    对于 iOS 11 设备和 iPadOS 12 设备（最低版本）：当您确认完全擦除时，您可以选择保留设备上的蜂窝数据套餐。

    对于 iOS 11.3 设备（最低版本）：当您确认完全擦除时，您可以阻止 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 Citrix Endpoint Management 管理且已擦除的设备上进行近距离设置。

    对于 iOS 17 设备（最低版本）：当您确认完全擦除时，设备会自动擦除所有用户数据，连接到指定的 Wi-Fi 网络，并使用提供的注册配置文件重新注册到 MDM 服务器。
  - 如果设备用户在存储卡内容被删除之前关闭设备，用户可能仍然可以访问设备数据。
  - 您可以取消擦除请求，直到请求发送到设备。
- **定位：** 定位设备并报告设备位置，包括地图，位于“**管理 > 设备**”页面上的“**设备详细信息 > 常规**”下。“定位”是一次性操作。使用“**定位**”在您执行操作时显示当前设备位置。要在一段时间内持续跟踪设备，请使用“**启用跟踪**”。
  - 将此操作应用于 Android（Android Enterprise 除外）设备或 Android Enterprise（公司所有或 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位置权限。如果用户在注册期间未授予权限，Citrix Endpoint Management 会在发送**定位**命令时再次请求位置权限。
  - 将此功能应用于 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，仅当设备处于 MDM 丢失模式时，该命令才会成功。
- **锁定：** 远程锁定设备。如果设备被盗且必须锁定，则锁定功能很有用。Citrix Endpoint Management 会生成一个 PIN 码并将其设置到设备中。要访问设备，用户需要输入 PIN 码。使用**取消锁定**可从 Citrix Endpoint Management 控制台移除锁定。
- **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：
    - 以工作配置文件模式注册到 Android Enterprise 的设备，以及
    - 运行早于 Android 7.0 版本的 Android 设备
  - 对于以工作配置文件模式注册到 Android Enterprise 且运行 Android 7.0 或更高版本的设备：
    - 密码锁定工作配置文件。设备未锁定。
    - 如果未发送密码，或者发送的密码不符合要求且工作配置文件没有密码：设备已锁定。
    - 如果未发送密码，或者发送的密码不符合要求，但工作配置文件有密码：工作配置文件已锁定，但设备未锁定。

> **注意：**
>
> 密码重置功能仅支持 BYOD 三星设备，并且控制台管理员应具有 `DEVICE_ACTION_CONTAINER_PASSWORD_RESET` 权限。

- **通知（响铃）：** 在设备上播放声音。

> **注意：**
>
> 此功能仅支持 iOS 设备。

- **重新启动：** 重新启动 Windows 10 和 Windows 11 设备。对于 Windows 平板电脑和 PC，将显示一条有关待处理重新启动的消息。重新启动将在五分钟内发生。
- **请求/停止 AirPlay 镜像：** 在受监管的 iOS 设备上启动和停止 AirPlay 镜像。
- **重新启动/关机：** 立即重新启动或关闭受监管的设备。

> **注意：**
>
> 此功能仅支持 iOS 设备。

- **吊销：** 禁止设备连接到 Citrix Endpoint Management。
- **吊销/授权：** 执行与选择性擦除相同的操作。吊销后，您可以重新授权设备以重新注册。
- **响铃：** 如果设备处于丢失模式，响铃会在受监管的 iOS 设备上播放声音。声音会一直播放，直到您将设备从丢失模式中移除或用户禁用声音。
- **轮换个人恢复密钥：** 如果您已启用 FileVault 设备策略，此操作将生成一个新的个人恢复密钥，并用此新密钥替换旧密钥。您可以在请求仍处于待处理状态时取消此请求。为此，请单击**取消轮换个人恢复密钥**。
- **选择性擦除：** 从设备中擦除所有企业数据和应用程序，保留个人数据和应用程序。选择性擦除后，使用**授权**操作重新授权设备，以便用户可以重新注册。擦除的设备会保留在**管理 > 设备**页面上的设备列表中，以供审计。您可以从设备列表中移除已擦除的设备。
  - 选择性擦除 Android 设备不会断开设备与设备管理器和企业网络的连接。要阻止设备访问设备管理器，您还必须吊销设备证书。
  - 选择性擦除 Android 设备也会吊销该设备。您只能在重新授权或从控制台删除设备后才能重新注册它。
  - 对于具有工作配置文件（COPE 设备）的 Android Enterprise 完全托管设备，您可以在选择性擦除移除工作配置文件后执行完全擦除。或者，您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，此命令会移除通过 MDM 安装的任何配置文件。
  - Windows 设备上的选择性擦除还会删除当前登录用户的配置文件文件夹内容。选择性擦除不会删除您通过配置交付给用户的任何 Web 剪辑。要删除 Web 剪辑，用户需要手动取消注册其设备。您无法重新注册已选择性擦除的设备。
- **解锁：** 清除设备锁定时发送到设备的密码。此命令不会打开设备。

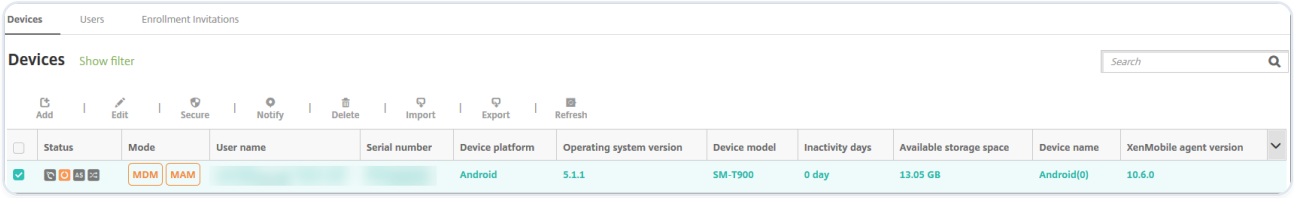
在 **管理 > 设备** 中，**设备详细信息** 页面还列出了设备安全属性。这些属性包括强 ID、锁定设备、激活锁绕过以及平台类型的其他信息。**完全擦除设备** 字段包含用户 PIN 码。设备擦除后，用户必须输入该代码。如果用户忘记了代码，您可以在此处查找。

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 Citrix Endpoint Management 控制台中删除设备

> **重要提示：**
>
> 从 Citrix Endpoint Management 控制台中删除设备时，托管应用程序和数据会保留在设备上。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”。

> 要从 Citrix Endpoint Management 控制台中删除设备，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. 仅适用于 Android 设备，将设备与公司网络断开连接：设备擦除后，在 **安全操作** 中，单击 **撤销**。

   要在擦除发生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**。

删除设备

此过程将从设备中删除托管应用程序和数据，并从 Citrix Endpoint Management 控制台的设备列表中删除该设备。您可以使用 Citrix Endpoint Management 公共 REST API 批量删除设备。

1. 转到“**管理 > 设备**”，选择一个托管设备，然后单击“**保护**”。
2. 单击“**选择性擦除**”。出现提示时，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，MDM 和 MAM 的琥珀色表示擦除命令成功。

成功的擦除命令(/en-us/citrix-endpoint-management/media/manage-devices-check-wipe-status.png)

4. 在“**管理 > 设备**”上，选择设备，然后单击“**删除**”。出现提示时，再次单击“**删除**”。

锁定、解锁、擦除或取消擦除应用程序

1. 转到“**管理 > 设备**”，选择一个托管设备，然后单击“**保护**”。
2. 在“**安全操作**”中，单击应用程序操作。

   您还可以使用“**安全操作**”框检查其帐户已禁用或从 Active Directory 中删除的用户的设备状态。“应用程序解锁”或“应用程序取消擦除”操作的存在表示应用程序已锁定或已擦除。

应用程序擦除和取消擦除

1. 转到“**管理 > 设备**”。选择一个设备。
2. 应用程序擦除
   - 单击“**保护 > 应用程序擦除**”。将显示一个对话框，其中包含以下消息：“**确定要擦除此设备上的应用程序吗？**”单击“**应用程序擦除**”。
3. 应用程序取消擦除
   - 单击“**保护 > 应用程序取消擦除**”。将显示一个对话框，其中包含以下消息：“**确定要取消擦除此设备上的应用程序吗？**”单击“**设备应用程序取消擦除**”。
4. 以同一用户身份，在同一模式下重新注册设备。
5. 从“**我的应用**”页面启动 MDX 应用程序。
6. 启动 思杰安全中心。

获取设备信息

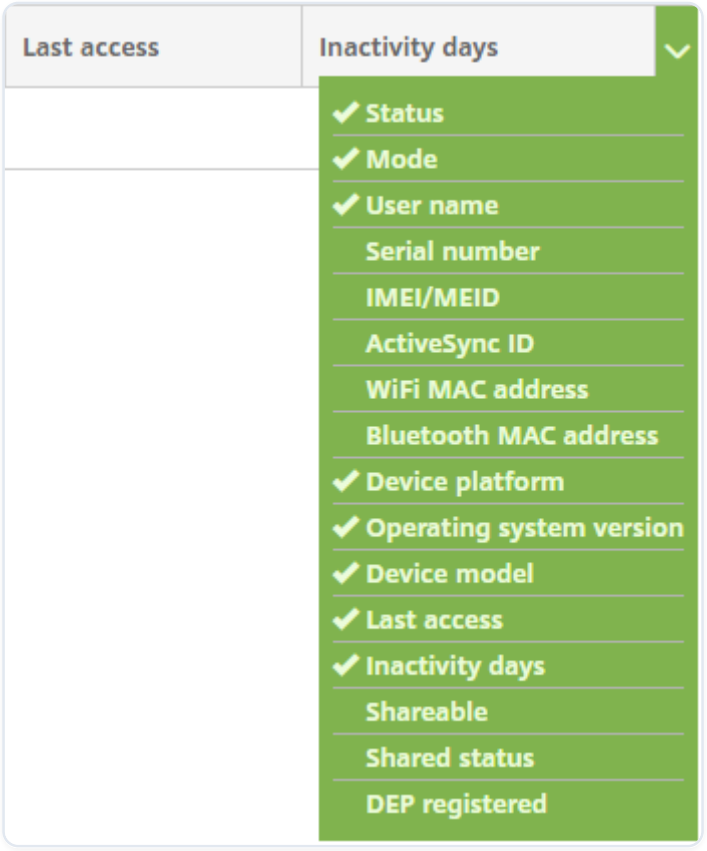
Citrix Endpoint Management 数据库存储移动设备列表。要使用您的设备填充 Citrix Endpoint Management 控制台，您可以手动添加设备，也可以从文件中导入设备列表。有关设备预配文件格式的更多信息，请参阅本文后面的设备预配文件格式。

Citrix Endpoint Management 控制台中的“**管理 > 设备**”页面列出了每个设备以及以下信息：

- **状态**：图标指示设备是否已越狱、是否受管理、ActiveSync Gateway 是否可用以及部署状态。
- **模式**：指示设备模式，例如 MDM 或 MDM+MAM。

- 有关设备的其他信息，例如“**用户名**”、“**设备平台**”、“**上次访问**”和“**非活动天数**”。这些标题是默认显示的。

要自定义“**设备**”表，请单击最后一个标题上的向下箭头。然后，选择要在表中显示的其他标题，或清除任何标题以将其删除。

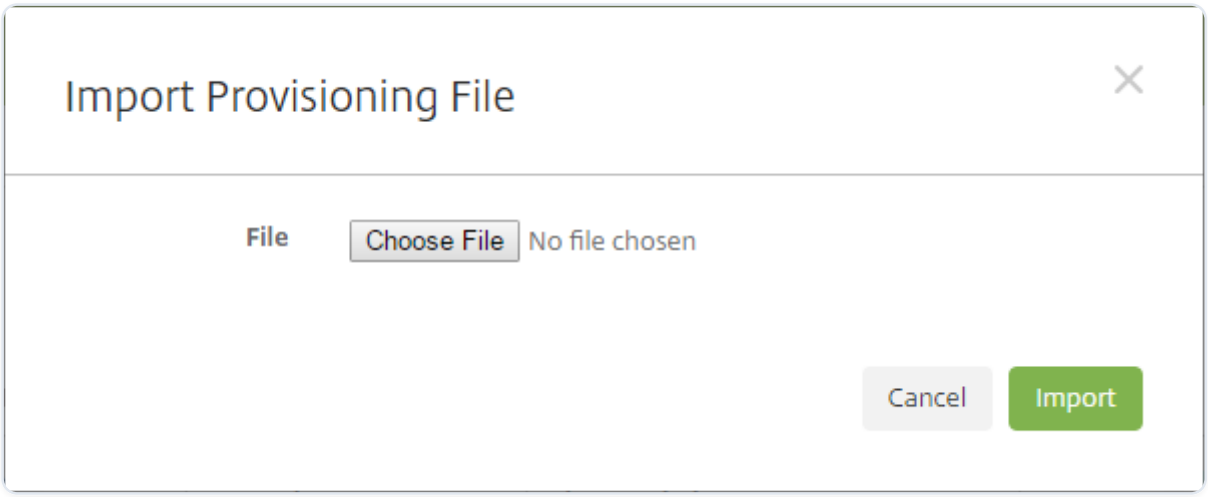


您可以手动添加设备、从设备预配文件导入设备、编辑设备详细信息、自定义 Active Directory 用户属性、执行安全操作以及向设备发送通知。您还可以将所有设备表数据导出到 .csv 文件以创建自定义报告。服务器会导出所有设备属性。如果应用筛选器，Citrix Endpoint Management 会在创建 .csv 文件时使用这些筛选器。

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提供的文件，也可以创建自己的设备预配文件。有关详细信息，请参阅本文后面的设备预配文件格式。

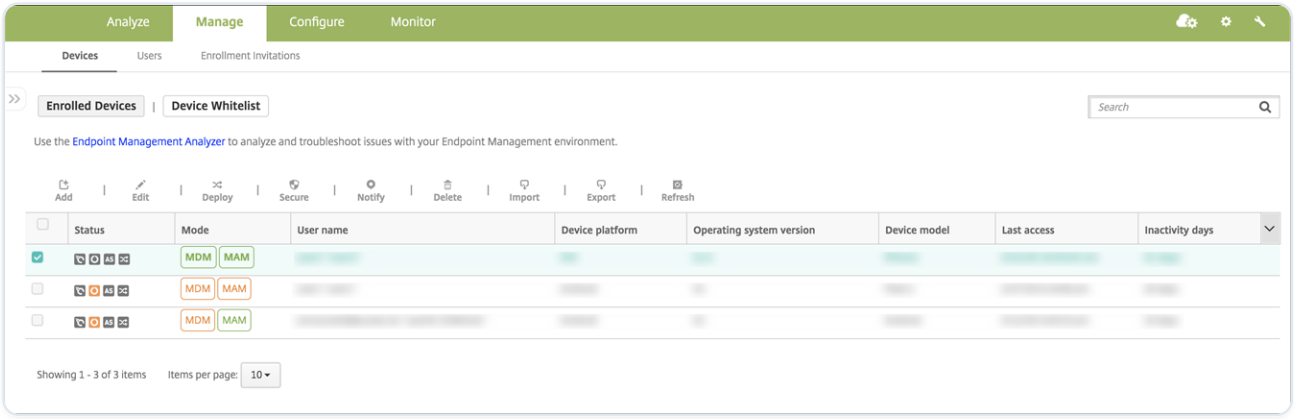
1. 转到“**管理 > 设备**”，然后单击“**导入**”。此时将显示“**导入预配文件**”对话框。



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**”表列出了导入的文件。
4. 要编辑设备信息，请选择该信息，然后单击“**编辑**”。有关“**设备详细信息**”页面的信息，请参阅获取设备信息。

部署到设备

您可以强制一个或多个设备连接到 Citrix Endpoint Management。所选设备会立即接收资源，而无需等待下一次计划签入。

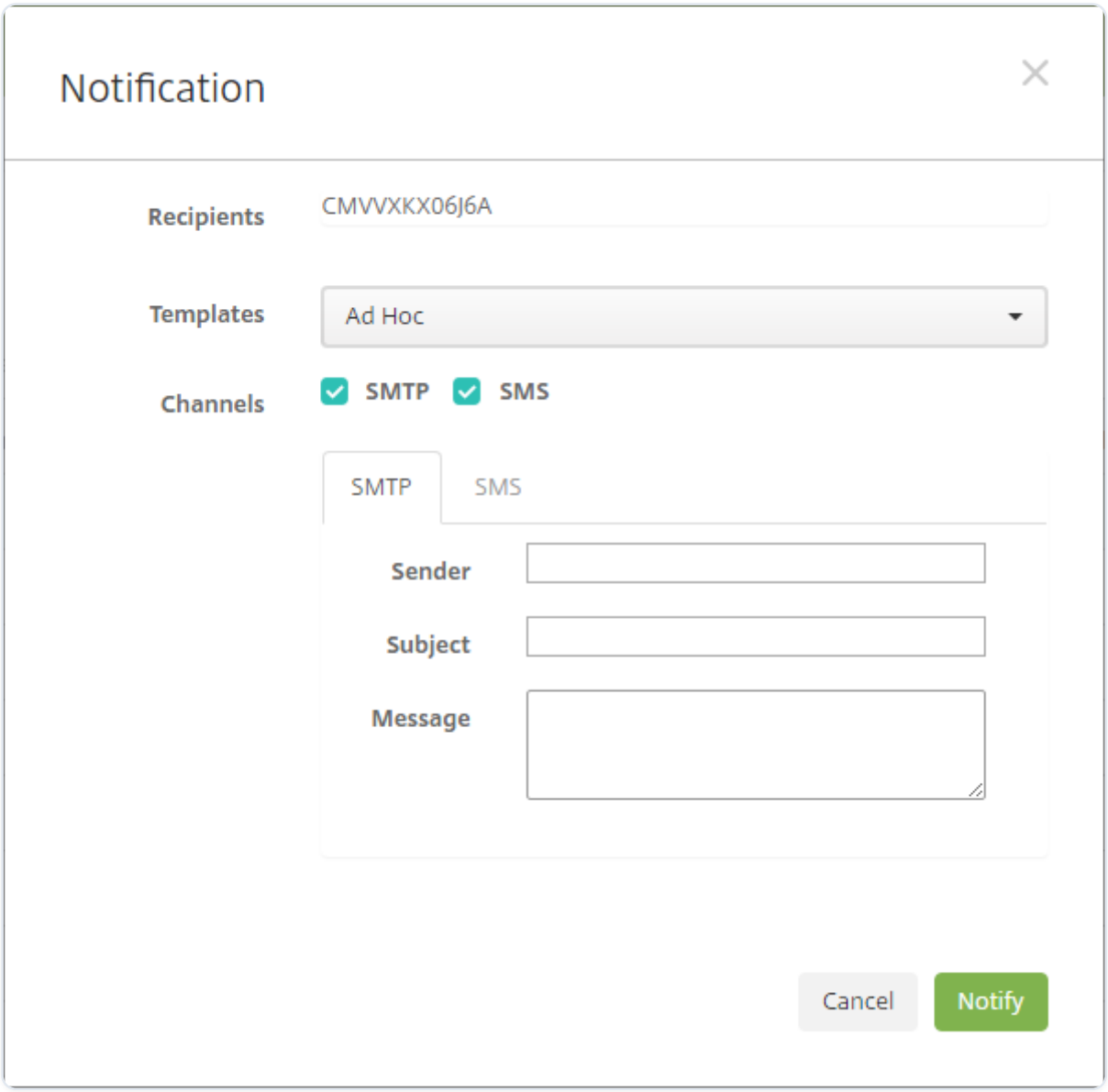


1. 转至“**管理 > 设备**”，选择一个 MDM 或 MDM+MAM 托管设备，然后单击“**部署**”。
2. 在对话框中，单击“**部署**”以确认您的操作。

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**”。“**通知**”对话框随即显示。“**收件人**”字段列出了所有将接收通知的设备。



3. 配置以下设置：

   - **模板**：在下拉列表中单击要发送的通知类型。对于除 **Ad Hoc** 之外的每个模板，**主题**和**消息**字段显示为所选模板配置的文本。
   - **通道**：选择发送消息的方式。默认值为 **SMTP**。单击选项卡可查看每个通道的消息格式。
   - **发件人**：输入可选的发件人。
   - **主题**：为 **Ad Hoc** 消息输入主题。
   - **消息**：为 **Ad Hoc** 消息输入消息。

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筛选**设备**表。

2. 单击**设备**表上方的**导出**按钮。Citrix Endpoint Management 将提取筛选后的**设备**表中的信息并将其转换为 .csv 文件。
3. 出现提示时，打开或保存 .csv 文件。

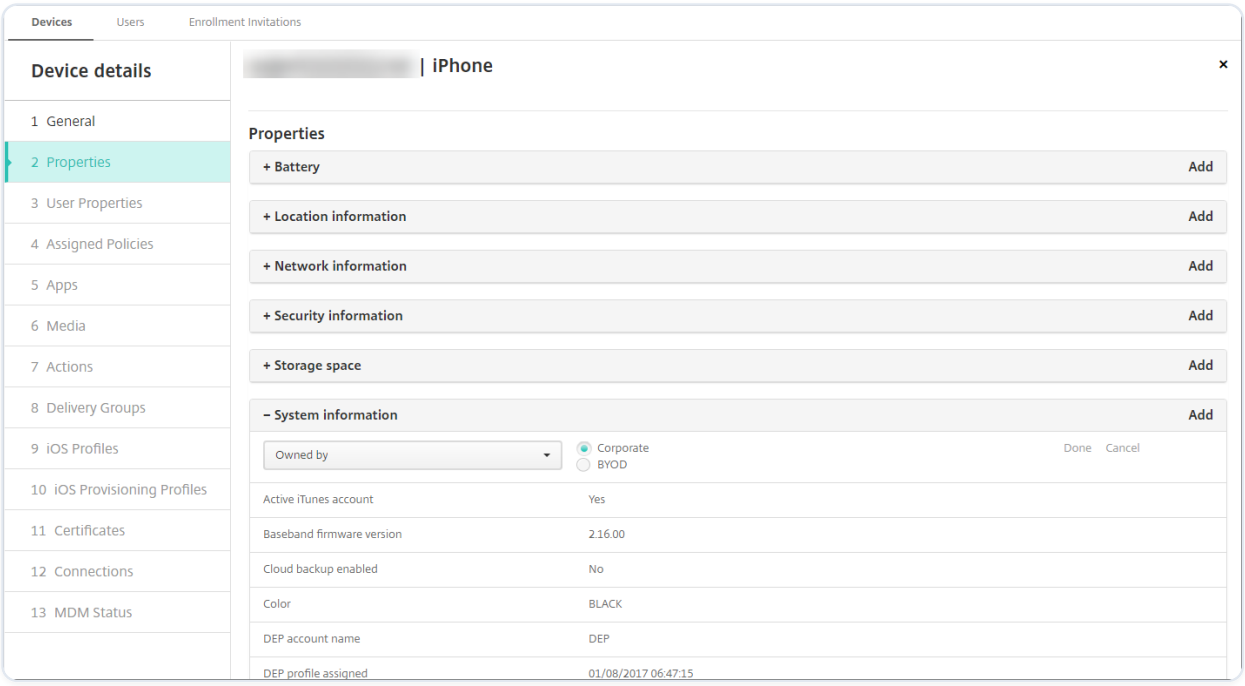
手动标记用户设备

您可以通过以下方式在 Citrix Endpoint Management 中手动标记设备：

- 在基于邀请的注册过程中。
- 在自助服务门户注册过程中。
- 通过将设备所有权添加为设备属性

您可以选择将设备标记为公司所有或员工个人所有。使用自助服务门户自行注册设备时，您可以将设备标记为公司所有或员工个人所有。您还可以手动标记设备，如下所示。

1. 在 Citrix Endpoint Management 控制台的“**设备**”选项卡中，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**”（员工个人所有）。



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 Citrix Endpoint Management 可以访问哪些属性来创建用户帐户。

要查看属性列表，请在“**设置 > 服务器属性**”中将 `optional.user.identity.attributes` 服务器属性添加为自定义密钥。在“**值**”字段中，您可以删除并稍后恢复 Citrix 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。

编辑默认值列表并保存更改后，您可以在“**管理 > 设备 > 用户属性**”中查看更新的 Active Directory 用户属性。Citrix Endpoint Management 会在用户登录设备后或在下一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，Citrix Endpoint Management 将忽略您的更改。

删除可选的 Active Directory 用户属性可能会影响以下功能：

- **用户帐户预配：** 如果您删除名字和姓氏值，Citrix Endpoint Management 无法为 ShareFile 和 Salesforce 预配用户帐户。
- **注册邀请：** 如果您删除用户的电子邮件或手机详细信息，用户将无法收到注册邀请。
- **设备通知操作：** 如果您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。
- **Citrix Secure Mail 单点登录：** 如果您删除显示名称值，用户将无法使用单点登录登录到 Citrix Secure Mail。
- **用户属性和部署规则：** 如果您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：** 如果您删除用于在**配置 > 操作**中设置自动化操作的任何可选属性，可能会影响现有配置。
- **自定义报告：** 如果您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 标识符
- 用户名

您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**。要在设备搜索中包含所有设备属性，请转至**设置 > 服务器属性**并将设置更改为 **true**。

设备预配文件格式

许多移动运营商或设备制造商提供授权移动设备列表。您可以使用这些列表，避免手动输入长串移动设备。Citrix Endpoint Management 支持一种导入文件格式，该格式适用于以下受支持的设备类型：Android、iOS 和 Windows。

您手动创建的预配文件必须采用以下格式：

`SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propert`
`propertyNameN;propertyValueN`

请记住以下几点：

- 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。如果字段的一部分包含分号，请使用反斜杠字符 (\\) 对其进行转义。

  例如，对于此属性：

  `propertyV;test;1;2`

  按如下方式转义：

  `propertyV\;test\;1\;2`
- iOS 设备需要序列号，因为序列号是 iOS 设备标识符。
- 对于其他设备平台，您必须包含序列号或 IMEI。
- **OperatingSystemFamily** 的有效值为 **WINDOWS**、**ANDROID** 或 **iOS**。

设备预配文件示例：

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;prop
ertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;prope
rtyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;
```

```
;55244201625379903;ANDROID;test.testé;value;`
```

文件中的每一行描述一个设备。该示例中的第一个条目表示以下内容：

- SerialNumber: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- ProertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

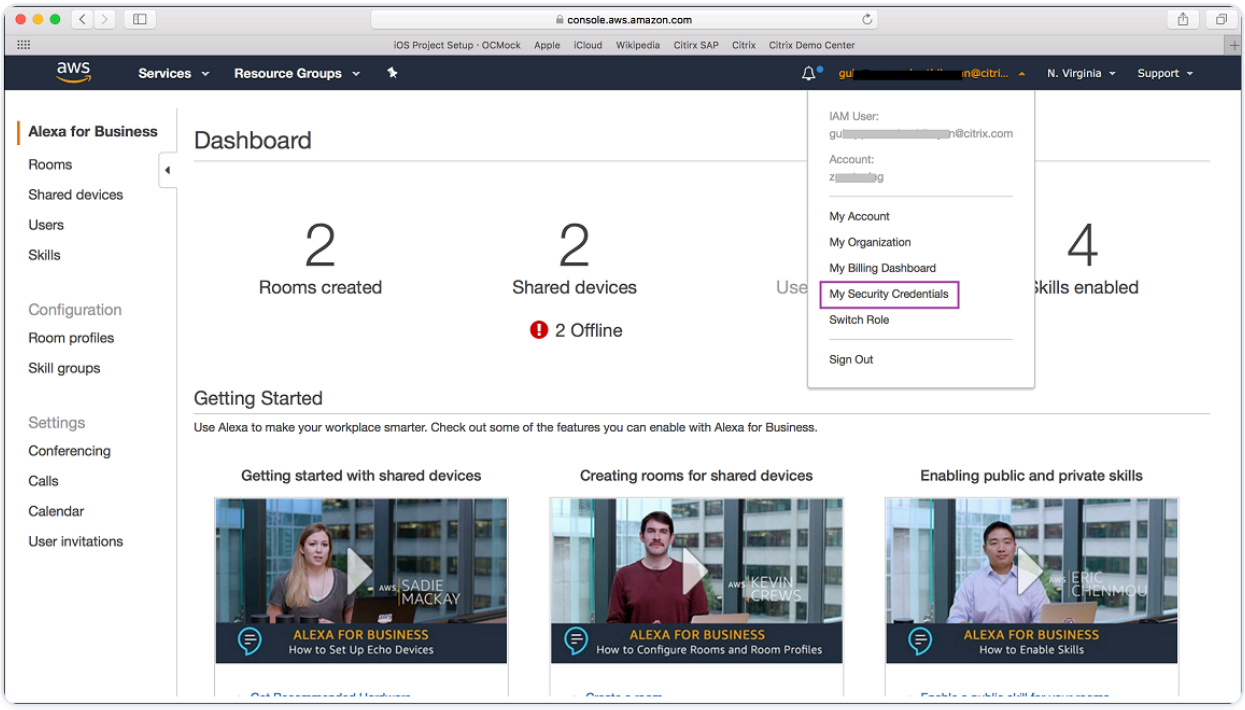
适用于企业的 Alexa

Amazon Web Services (AWS) 的适用于企业的 Alexa 服务允许您管理大量支持 Alexa 的设备，用于商业用途，例如会议室协助。Citrix Endpoint Management 允许您在 Citrix Endpoint Management 控制台中配置和管理这些设备。Citrix Endpoint Management 不会直接向 Alexa 设备部署策略。相反，Citrix Endpoint Management 会更新 AWS 服务，然后 AWS 将配置交付给 Alexa 设备。

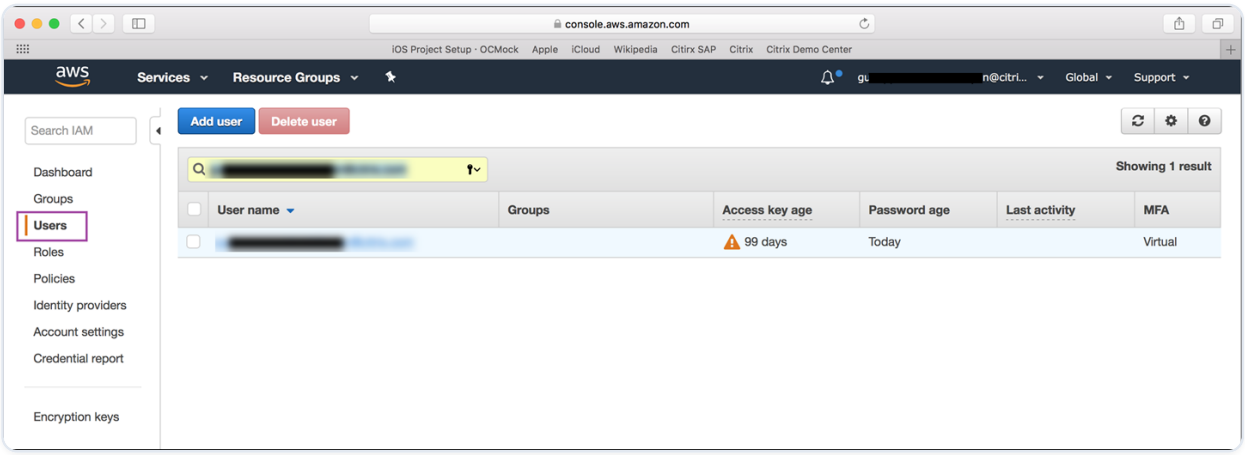
有关使用适用于企业的 Alexa 的信息，请参阅 适用于企业的 Alexa 管理指南。

向 Citrix Endpoint Management 验证您的 AWS 账户

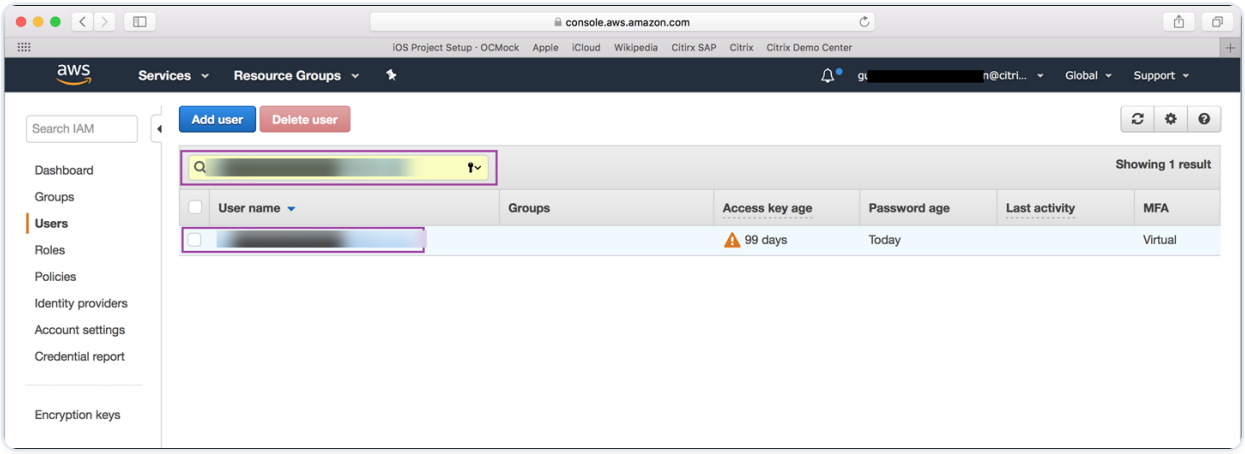
1. 要获取您的 AWS 账户凭据，请登录到 AWS 控制台，然后从用户菜单中选择 **My Security Credentials**。



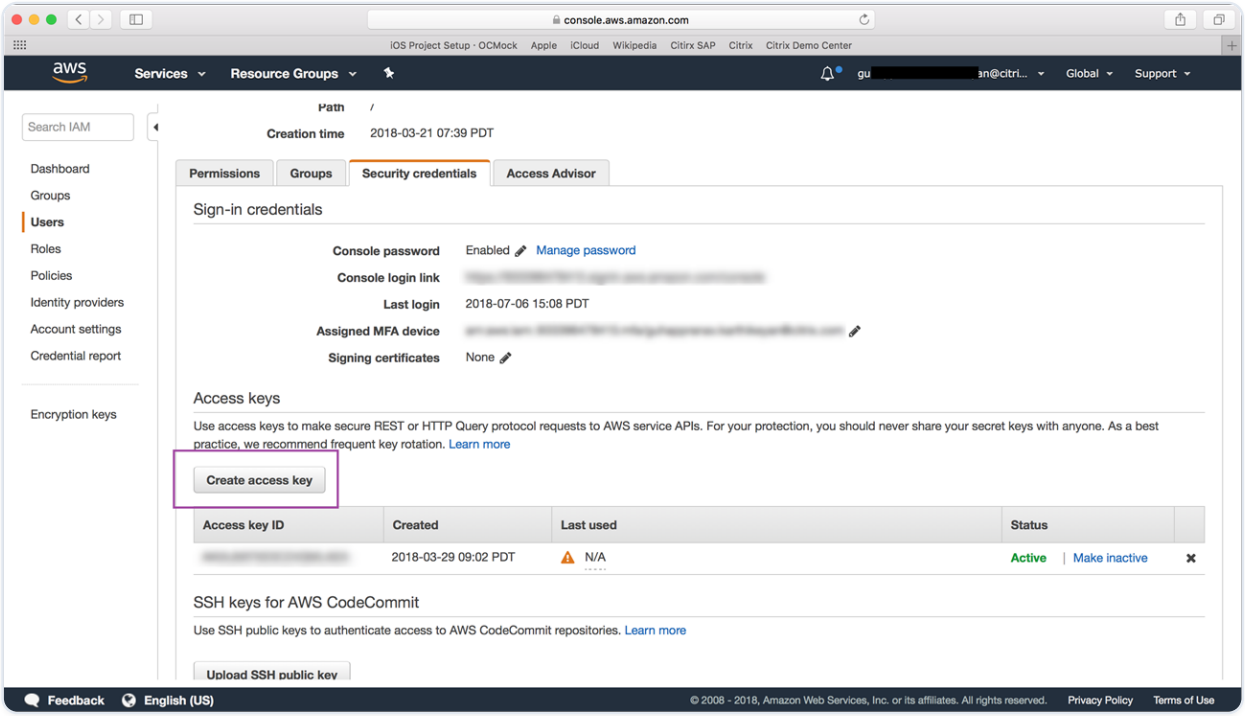
2. 在左侧面板中选择 **Users**。



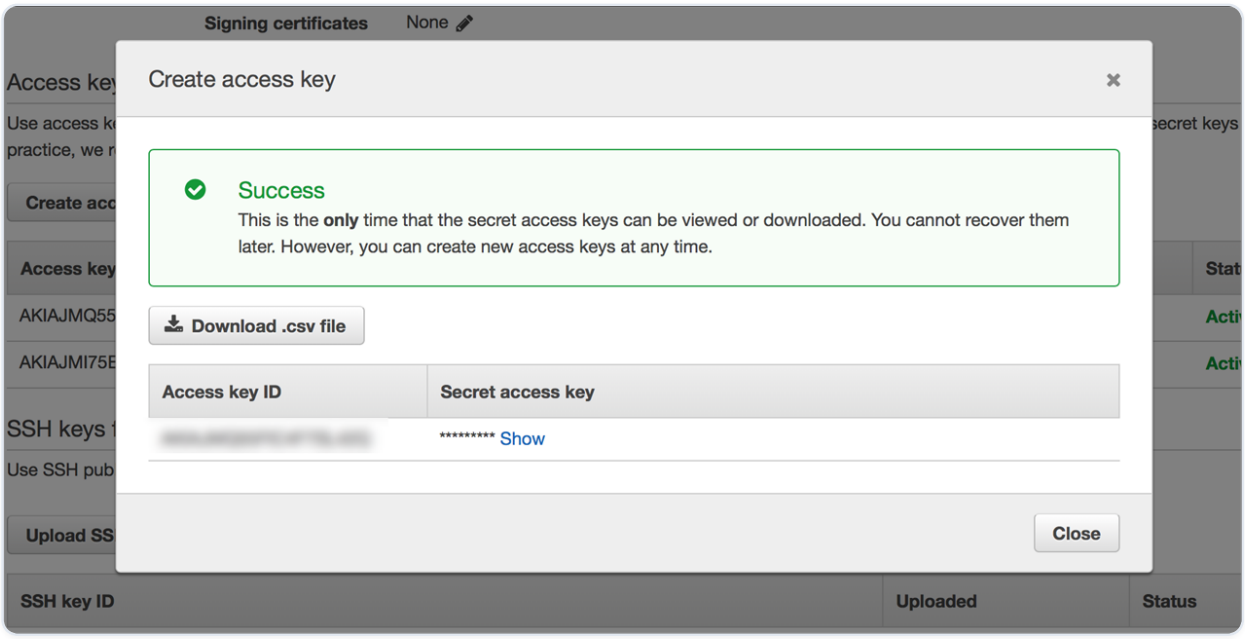
3. 搜索您的用户名，然后选择它。



4. 在 **Security Credentials** 选项卡中，单击 **Create access key** 以生成您的访问密钥 ID 和秘密访问密钥。

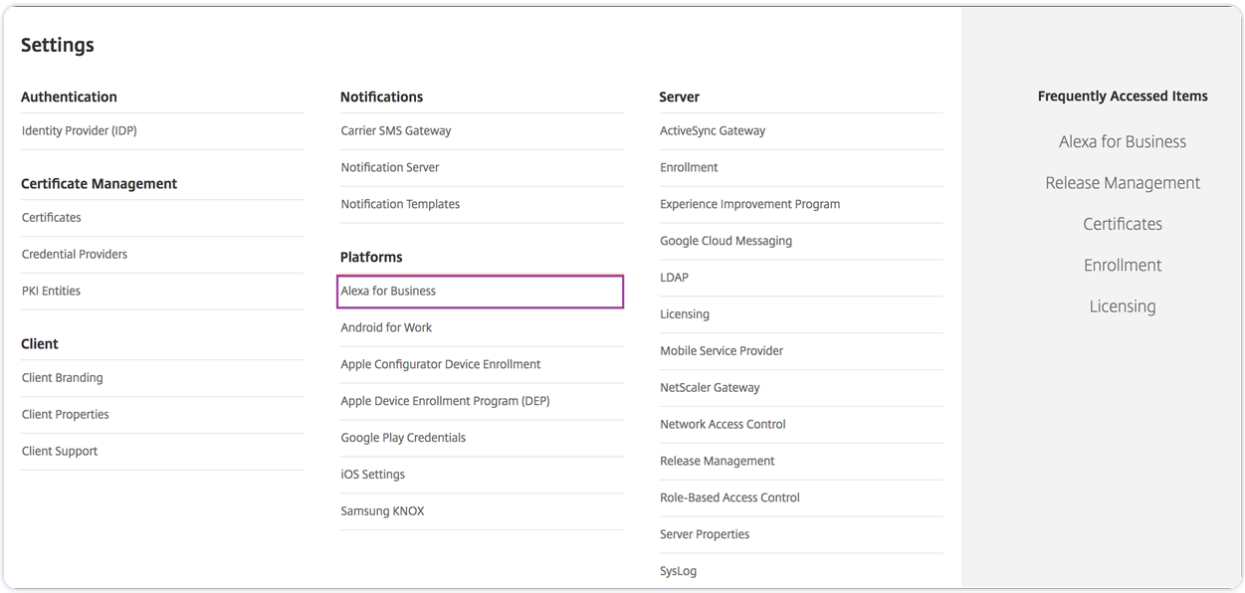


5. 下载访问密钥 ID 和秘密访问密钥。保存或记下它们。

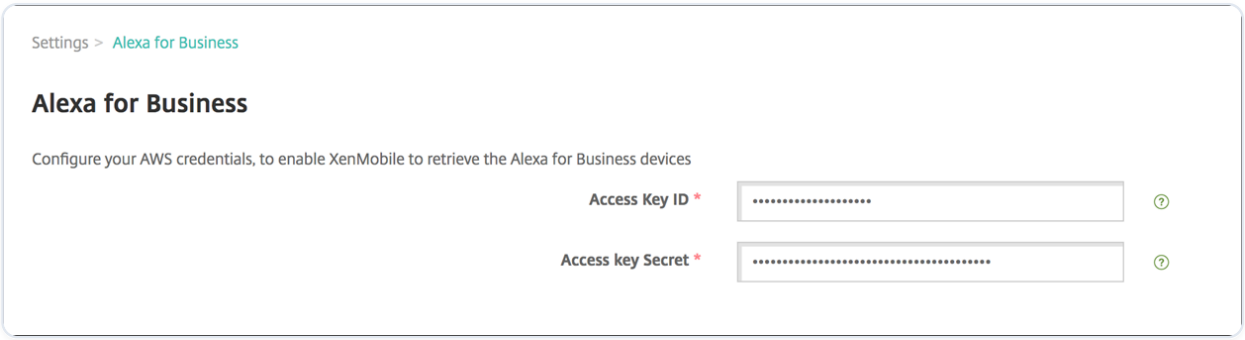


6. 在 Citrix Endpoint Management 控制台中，单击齿轮图标以转到**设置**。

7. 在**平台**下，选择 **Alexa for Business**。



8. 输入您的访问密钥 ID 和秘密访问密钥。单击**保存**。



在 Citrix Endpoint Management 上配置适用于企业的 Alexa

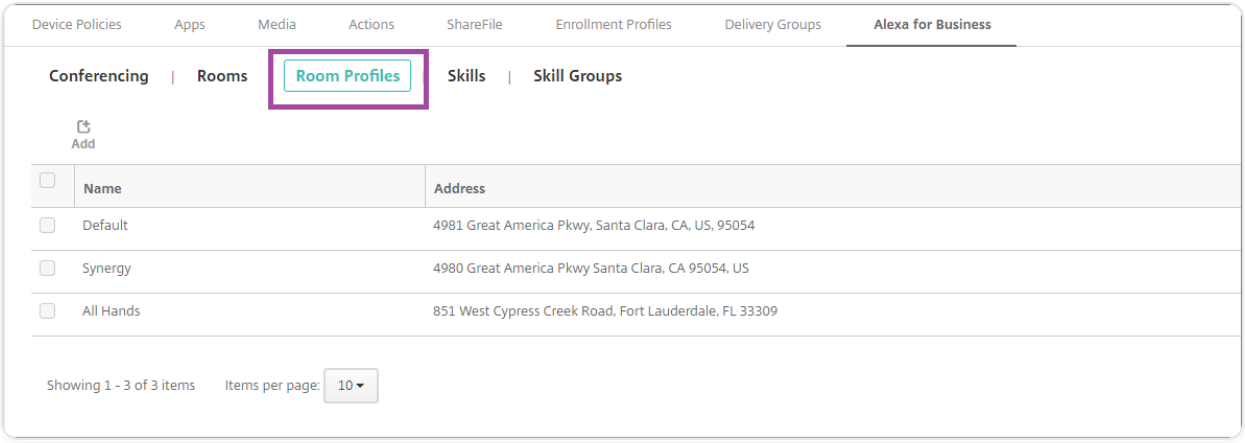
Citrix Endpoint Management 允许您配置：

- 应用于具有 Alexa 设备的房间的设置配置文件
- 代表拥有设备的物理房间
- 您分配给房间或设备的技能组
- 可以添加到技能组的 Alexa 技能商店中的 Alexa 技能
- 会议功能，可让您选择会议提供商并控制人们如何在您的房间中安排和加入会议

配置房间配置文件

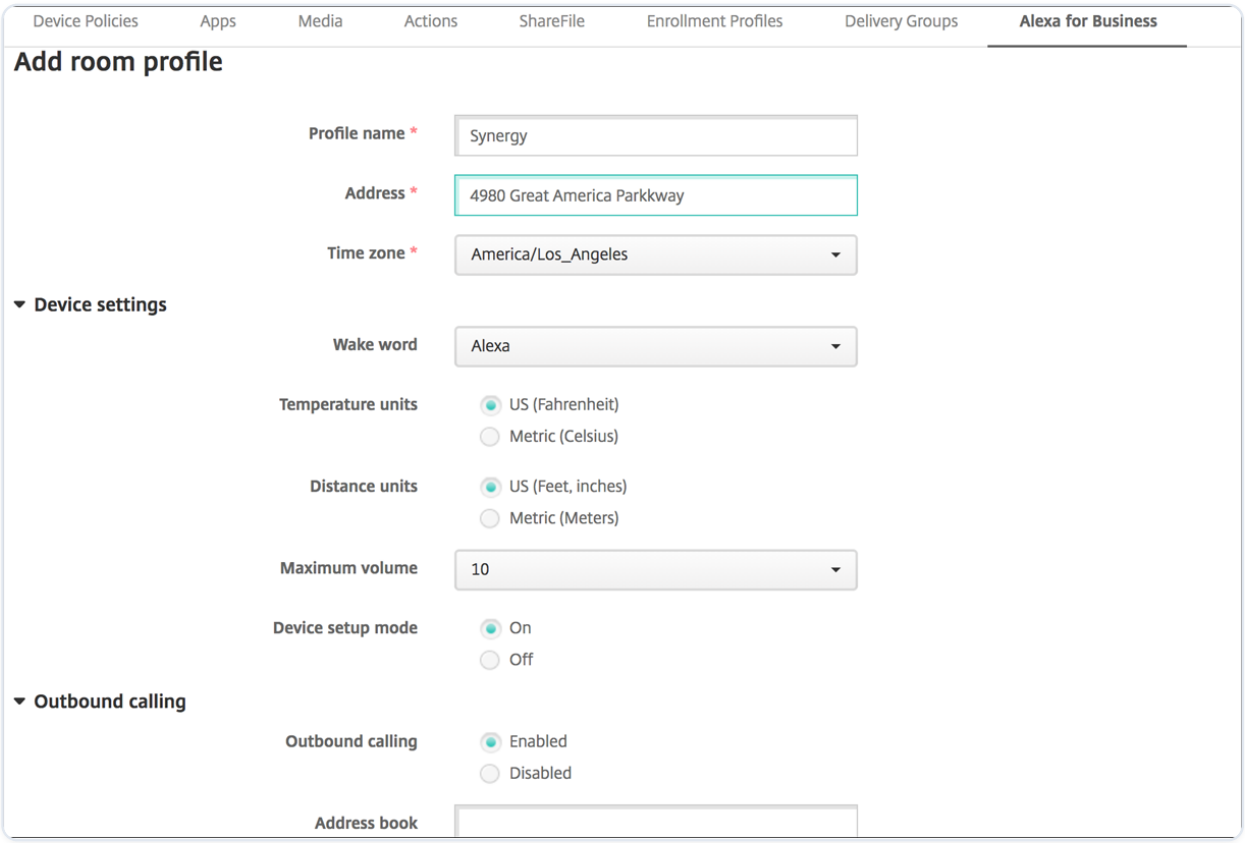
房间配置文件是一组通用配置，可应用于拥有 Alexa 设备的房间集合。您可以添加、编辑和删除房间配置文件。

1. 在 Citrix Endpoint Management 控制台中，选择 **配置 > Alexa for Business > 房间配置文件**。可用房间配置文件的列表随即显示。



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. 输入房间配置文件设置：



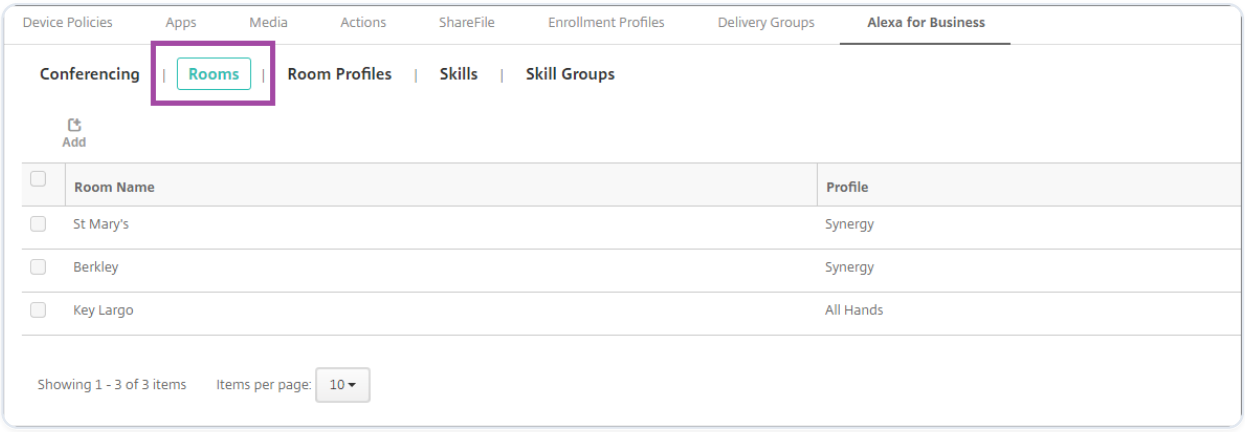
- **配置文件名称：**键入配置文件的名称。
- **地址：**键入拥有 Alexa 设备的房间所在建筑物的物理（街道）地址。
- **时区：**选择该地点的时区。
- **唤醒词：**选择 Alexa 设备响应的唤醒词。
- **温度单位：**选择 Alexa 设备报告温度时使用的单位。
- **距离单位：**选择 Alexa 设备报告距离时使用的单位。
- **最大音量：** 选择 Alexa 的最大音量设置。
- **设备设置模式：** 选择 Alexa 设备是否可以通过强制进入设备设置模式来重新配置。
- **呼出电话：** 启用或禁用 Alexa 设备的呼出电话功能。
- **通讯录：** 设置 Alexa 设备的通讯录配置。

4. 点击 **保存**。

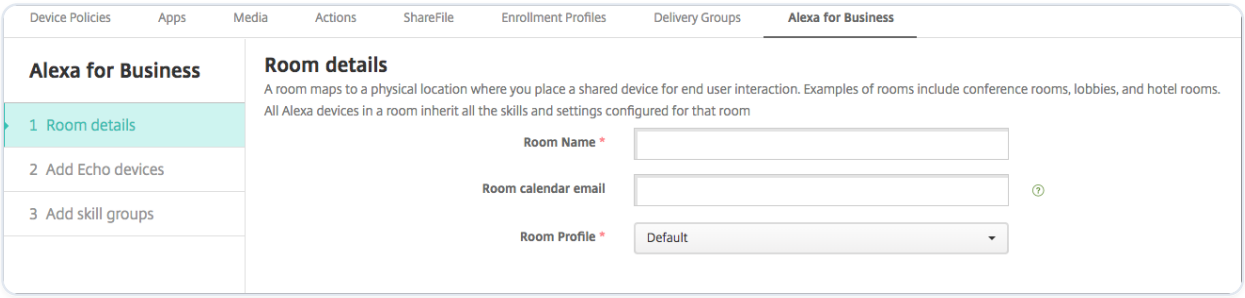
配置房间

您在 Citrix Endpoint Management 控制台中配置的房间代表建筑物中的物理会议室、会议室和其他房间。配置房间时，您可以为该房间关联一个 Alexa 设备，并向该设备添加一个技能组。您可以添加、编辑和删除房间。

1. 在 Citrix Endpoint Management 控制台中，选择 **配置 > Alexa for Business > 房间**。将显示可用房间列表。

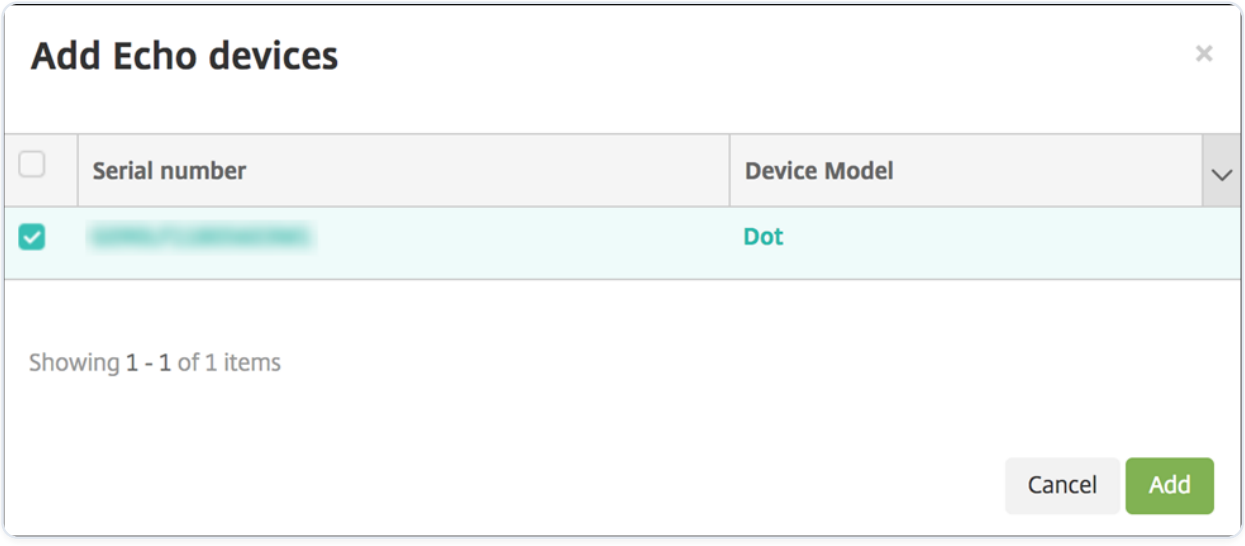


2. 要添加房间，请单击**添加**。要编辑房间，请选择要编辑的房间，然后单击**编辑**。
3. 输入以下房间设置：

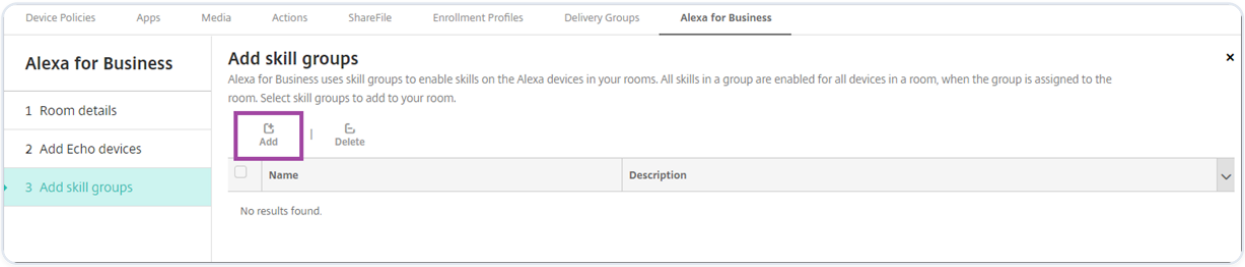


   - **房间名称：** 键入会议室、会议室或其他房间的名称。
   - **房间日历电子邮件：** 键入房间的日历电子邮件地址。
   - **房间配置文件：** 选择房间配置文件配置的名称。

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**。所选设备将显示在**添加 Echo 设备**页面中。



7. 单击“**下一步**”。
8. 要将技能组添加到房间中的 Alexa 设备，请单击**添加**。



9. 选择要添加到房间中 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。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-room2.png)
10. 点击 **保存**。

配置技能组

技能组是可应用于房间的技能集合。您可以创建一个技能组，然后将其分配给一个房间。技能允许您使用 Alexa 设备执行诸如开始和结束在线会议或查看议程项目列表等操作。您可以添加、编辑和删除技能组。

1. 在 Citrix Endpoint Management 控制台中，选择**配置 > Alexa for Business > 技能组**。可用技能组列表随即显示。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-11.png)
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： (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-group3.png)
    - **名称：**键入技能组的名称。
    - **描述：**键入技能组的简要描述。
4. 单击“**下一步**”。
5. 要向技能组添加技能，请单击**添加**。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-group3.png)
6. 选择要包含在技能组中的技能，然后单击**添加**。选定的技能将显示在**添加技能**页面中。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill-to-group2.png)
7. 要将技能组添加到您指定的房间中的 Alexa 设备，请单击**添加**。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-room-to-group1.png)
8. 选择房间。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-room-to-group2.png)

9. 点击 **保存**。

使技能可用于技能组

您可以配置可在 Alexa for Business 组织中的技能组中包含的 Alexa 技能列表。这些技能来自公共 Alexa 技能商店或发布到您组织的私有技能。

将技能添加到您的组织

1. 在 Citrix Endpoint Management 控制台中，选择 **配置 > Alexa for Business > 技能**。已启用技能的列表随即显示。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill1.png)
2. 要添加技能，请单击 **添加**。
3. 要查看更多 Alexa 技能，请选择一个类别，然后单击 **显示更多**。单击 **显示更多** 会将最多 10 个技能添加到可供您的组织添加的技能列表中。再次单击 **显示更多** 可添加更多技能。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill5.png)
4. 选择要添加到您的组织的技能。
5. 点击 **保存**。

从您的组织中删除技能

1. 在 Citrix Endpoint Management 控制台中，选择 **配置 > Alexa for Business > 技能**。已启用技能的列表随即显示。
2. 选择要从您的组织中删除的技能。
3. 单击 **禁用**。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill4.png)

配置会议

会议功能允许您配置会议提供商，例如 Google Hangout 或 Amazon Chime，这些提供商控制人们如何在配备 Alexa 设备的会议室中加入会议。您可以添加、编辑和删除会议提供商。您还可以设置默认会议提供商。

1. 在 Citrix Endpoint Management 控制台中，选择 **配置 > Alexa for Business > 会议**。可用会议室配置文件的列表随即显示。 (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-confer1.png)
2. 要添加会议提供商，请单击 **添加**。要编辑会议提供商，请选择要编辑的会议室配置文件，然后单击 **编辑**。
3. 输入会议室配置文件设置： (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-confer2.png)

- **会议提供商：** 从列表中选择一个会议提供商。
- **名称：** 键入要为会议提供商指定的名称。
- **会议 PIN：** 指定加入会议是否需要 PIN。
- **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：** 指定在发送会议 ID 之前的秒数。
  - **会议 PIN 延迟：** 指定在发送 PIN 之前的秒数。
- **SIP/H323 拨入设置** SIP/H323 拨入设置用于使用现有视频会议设备加入会议。
  - **协议：** 选择一个协议。
  - **IP 地址：** 键入 IP 地址。

4. 点击 **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 Citrix Endpoint Management 控制台中，选择 **配置 > Alexa for Business > 会议**。将显示可用会议室配置文件的列表。
2. 选择要设置为默认值的会议提供程序。
3. 单击 **设置默认值**。

Android

从设备管理迁移到 Android Enterprise

本文讨论了从旧版 Android 设备管理迁移到 Android Enterprise 的注意事项和建议。Google 正在弃用 Android 设备管理 API。该 API 支持 Android 设备上的企业应用。Android Enterprise 是 Google 和 Citrix 推荐的现代管理解决方案。

Citrix Endpoint Management 正在将 Android Enterprise 更改为 Android 设备的默认注册方法。Google 弃用 API 后，Android Q 设备在设备管理模式下的注册将失败。

Android Enterprise 支持完全托管和工作资料设备模式。Google 出版物 Android Enterprise Migration Bluebook 详细解释了旧版设备管理和 Android Enterprise 之间的不同之处。我们建议您阅读 Google 提供的迁移信息。

我们还建议您参考 Citrix Tech Zone 文章，从 Android 设备管理员迁移到 Citrix Endpoint Management 的 Android Enterprise。

设备管理弃用的影响

Google 已弃用设备管理员 API，并将从 November 2, 2020 起不再支持它们。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：

- **禁用摄像头：** 控制对设备摄像头的访问。
- **键盘锁功能：** 控制与设备锁定相关的功能，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+，则必须将该设备注册到 Android Enterprise。
  - 您必须将 Android 11 设备注册到 Android Enterprise。
  - 从 September 2020 起，对于 Android 10 设备：Citrix 不支持在设备管理模式下进行新注册或设备重新注册。已注册的设备将继续工作，直到 November 2, 2020，如前一节所述。
- 对于运行 Android 9 及更低版本的设备，我们支持旧版设备管理模式。但是，我们建议尽快将这些设备迁移到 Android Enterprise。
- 对于以 Citrix 仅 MAM 模式注册的新设备或现有设备，无需采取任何操作。已弃用的 Google API 对仅 MAM 模式下的设备没有影响。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，但位于设备上的容器中。

分析

迁移的分析阶段包括：

- 了解您的旧版 Android 设置
- 记录您的旧版设置，以便将旧版功能映射到 Android Enterprise 功能

建议的分析

1. 评估 Citrix Endpoint Management 上的 Android Enterprise：完全托管、带工作配置文件的完全托管、专用设备、工作配置文件 (BYOD)。
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：

1. 创建一个电子表格，并列出 Citrix Endpoint Management 控制台中的当前策略组。
2. 根据现有策略组创建单独的用例。
3. 对于每个用例，记录以下内容：
    - 名称
    - 业务负责人
    - 用户身份模型
    - 设备要求
        - 安全
        - 管理
        - 可用性
    - 设备清单
        - 品牌和型号
        - 操作系统版本
    - 应用程序
4. 对于每个应用程序，列出：
    - 应用程序名称
    - 包名称
    - 托管方法
    - 应用程序是公共的还是私有的
    - 应用程序是否强制（true/false）

要求映射

根据已完成的分析，确定您的 Android Enterprise 功能要求。

推荐的需求映射

1. 确定管理模式和注册方法：
    - 工作资料 (BYOD)：需要重新注册。无需恢复出厂设置。

- 完全托管：需要恢复出厂设置。通过使用 QR 码、近场通信 (NFC) 碰撞、设备策略控制器 (DPC) 标识符、零接触来注册设备。

2. 创建应用程序迁移策略。
3. 将用例要求映射到 Android Enterprise 功能。记录每个设备要求的功能，该功能与要求及其对应的 Android 版本最匹配。
4. 根据功能要求确定最低 Android 操作系统（7.0、8.0、9.0）。
5. 选择身份模型：
   - 推荐：托管式 Google Play 帐号
   - 仅当您是 Google Cloud Identity 客户时才使用 Google Workspace 帐号
6. 创建设备策略：
   - 不采取任何措施：如果设备满足最低操作系统级别
   - 升级：如果设备支持并可以更新到受支持的操作系统
   - 替换：如果设备无法更新到受支持的操作系统级别

推荐的应用程序迁移策略

完成要求映射后，将应用从 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。

- 公共商店应用

  a. 选择要迁移的应用，然后编辑应用以清除 Google Play 设置，并选择 **Android Enterprise** 作为平台。

  b. 选择交付组。如果应用是强制性的，请将应用移动到交付组中的**所需应用**列表。

  保存应用后，它会显示在 Google Play 商店中。如果您有工作配置文件，应用会显示在工作配置文件中的 Google Play 商店中。

- 私有（企业）应用

  私有应用由内部或第三方开发人员开发。我们建议您使用 Google Play 发布私有应用。

  a. 选择要迁移的应用，然后编辑应用以选择 **Android Enterprise** 作为平台。

  b. 上传 APK 文件，然后配置应用设置。

  c. 将应用发布到所需的交付组。

- MDX 应用

a. 选择要迁移的应用，然后编辑应用以选择 **Android Enterprise** 作为平台。

b. 上传 MDX 文件。完成应用审批流程。

c. 选择 MDX 策略。

对于企业 MDX 应用，我们建议将其更改为 MDX SDK 模式封装应用：

- 选项 1：将 APK 托管在 Google Play 中，使用私下分配给您组织的开发者帐户。在 Citrix Endpoint Management 中发布 MDX 文件。
- 选项 2：将应用程序从 Citrix Endpoint Management 作为企业应用程序发布。在 Citrix 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：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工作配置文件模式或完全托管模式下的设备。请参阅 配置 Android Enterprise 设备和应用程序策略。
- 如果您对旧版 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。
- 为确保将策略定向到目标设备（Android Enterprise 与旧版 DA），请向策略添加部署规则。例如，对于旧版 DA 平台，请使用此部署规则：

```
Limit by known device property name Android Enterprise

Enabled Device? Isn’t equal to true
```

该部署规则会检查设备是否未启用 Android Enterprise，并将策略和应用程序一起交付给已启用旧版 DA 的设备。

概念验证

将应用程序迁移到 Android Enterprise 后，您可以设置迁移测试以验证功能是否按预期工作。

推荐的概念验证设置

1. 设置部署基础结构：

   - 为您的 Android Enterprise 测试创建交付组。
   - 在 Citrix 端点管理中配置 Android 企业版。

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. 测试并确认功能。
6. 为每个用例完成设备设置演练。
7. 记录用户设置步骤。

部署

您现在可以部署 Android Enterprise 设置并为用户迁移做好准备。

推荐的部署策略

推荐的 Citrix 部署策略是测试所有生产系统以支持 Android Enterprise，然后稍后完成设备迁移。

- 在此场景中，用户继续使用具有当前配置的旧设备。您为 Android Enterprise 管理设置新设备。
- 仅在需要升级或更换时才迁移现有设备。
- 在现有设备达到其常规生命周期结束时将其迁移到 Android Enterprise 管理。或者，在设备因丢失或损坏而需要更换时迁移这些设备。

安卓企业版

Android Enterprise 是 Google 提供的一套工具和服务，作为 Android 设备的企业管理解决方案。借助 Android Enterprise，您可以：

- 使用 Citrix Endpoint Management 管理公司拥有的和自带设备 (BYOD) 的 Android 设备。
- 您可以管理整个设备或设备上的独立配置文件。独立配置文件将业务帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。
- 您还可以管理专用于单一用途的设备，例如库存管理。有关 Google 提供的 Android Enterprise 功能概述，请参阅 Android Enterprise Management。

资源：

- 有关 Android Enterprise 相关术语和定义的列表，请参阅 Google Android Enterprise 开发者指南文章 Android Enterprise terminology。Google 会频繁更新这些术语。
- 有关 Citrix Endpoint Management 支持的 Android 操作系统列表，请参阅 Supported device operating systems。
- 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。

- 有关部署 Android Enterprise 的信息，请参阅 Deploy resources)。

安卓企业版入门

重要提示：

不再支持设备管理模式。如果您的用户设备处于设备管理模式，请参阅 Migrate from device administration to 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。

   请参阅 (#using-managed-google-play-with-citrix-endpoint-management) 和 (#requirements)。

2. 将您的 Google Play 帐户绑定到 Citrix Endpoint Management。

请参阅 (#connecting-citrix-endpoint-management-to-google-play)。

3. 规划如何管理设备。

   请参阅 (#device-deployment-scenarios-and-profiles)。

4. 规划用户设备的注册安全性。

   请参阅 (#enrollment-security)。

5. 准备交付启用 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的 SDK，请使用基于命令行的 MDX Toolkit 来封装应用程序。

   请参阅 (/zh-cn/mdx-toolkit/mam-sdk-overview.html)。

至此，您已准备好配置您的 Android Enterprise 设备以及应用程序和设备策略、注册配置文件和应用程序。有关指导，请参阅以下部分。

配置设备

1. 创建交付组。

   控制谁在何时获得哪些资源。请参阅 (/zh-cn/citrix-endpoint-management/deploy-resources.html)。

   我们停止向注册到 Android Enterprise 的设备交付为旧版 DA 平台发布的应用程序。对于 Android Enterprise 设备，请为 Android Enterprise 平台发布应用程序。要继续向 DA 模式下的设备发布旧版 DA 应用程序，请为这些应用程序创建单独的交付组。请参阅 (/zh-cn/citrix-endpoint-management/whats-new/removed-features.html)。

2. 添加应用程序。您可以直接从 Citrix Endpoint Management 控制台批准 Google Play 中的应用程序。

   请参阅 Google 支持文章，管理组织中的应用程序。

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。

   - 当您将 Android Enterprise 公共应用商店应用程序部署到 Android 设备用户时，该用户将自动注册到 Android Enterprise。
   - 零接触注册允许您配置设备，使其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。

平衡企业安全性与用户隐私和用户体验。请参阅配置 Android Enterprise 设备和应用程序策略。

5. 分发应用程序。

   您可以使用托管 Google Play 添加、购买和批准应用程序，以便部署到设备上的 Android Enterprise 工作区。用户只能从您为其提供的托管 Google Play 安装应用程序。

   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并提供合规性。

   请参阅 安全操作。

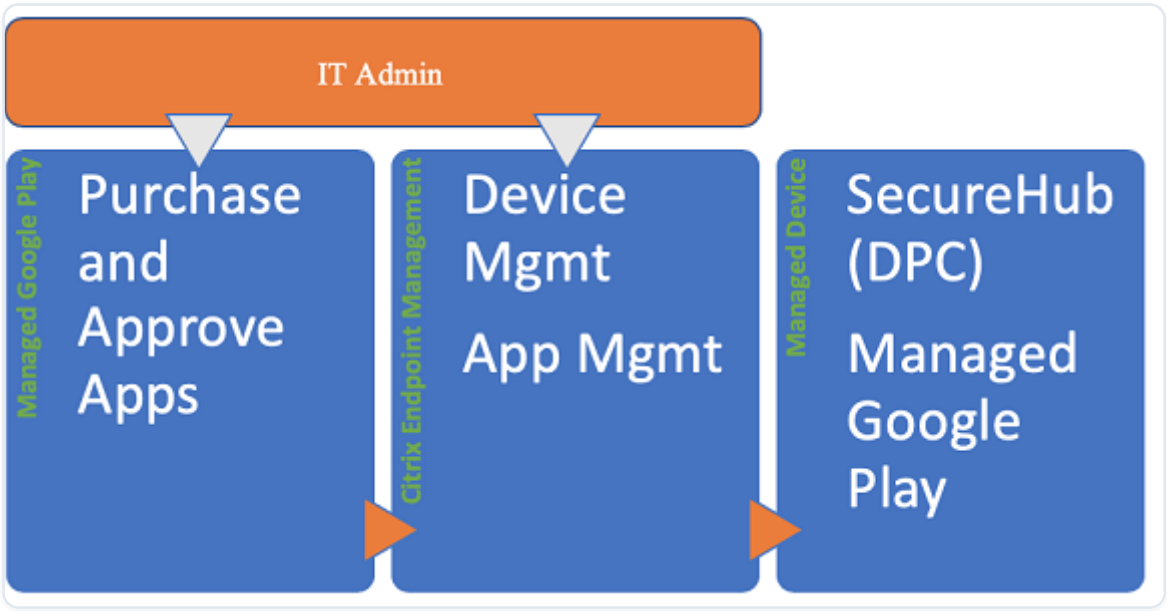
将托管 Google Play 与 Citrix Endpoint Management 结合使用

当您将 Citrix Endpoint Management 与托管 Google Play 集成以使用 Android Enterprise 时，您将创建一个企业。Google 将企业定义为组织与您的企业移动管理 (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。

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 Citrix Endpoint Management 与 Android Enterprise 集成时，完整的解决方案包含以下组件：

- **Citrix Endpoint Management：** Citrix EMM。Citrix Endpoint Management 是用于安全数字工作区的统一 Citrix Endpoint Management。Citrix 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。Citrix Secure Hub 是 Citrix Endpoint Management 的启动板。Citrix Secure Hub 在设备上强制执行策略。
- **托管 Google Play：** 一个与 Citrix 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。

此图说明了管理员如何与这些组件交互以及这些组件之间如何交互：



注意：

您可以使用托管 Google Play 或 Google Workspace（以前称为 G Suite）将 Citrix 注册为您的 EMM 提供商。本文讨论了将 Android Enterprise 与托管 Google Play 结合使用。如果您的组织使用 Google Workspace 提供对应用程序的访问，则可以将其与 Android Enterprise 结合使用。请参阅 适用于 Google Workspace 客户的旧版 Android Enterprise。

当您使用托管 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 的访问权限，允许用户安装和使用您提供的应用程序。如果您的组织使用第三方身份服务，则可以将托管 Google Play 帐户与现有身份帐户关联。

由于此类企业不与域绑定，因此您可以为一个组织创建多个企业。例如，组织内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不同的设备和应用程序集。

对于 Citrix Endpoint Management 管理员而言，托管 Google Play 将 Google Play 的用户体验和应用程序商店功能与一套专为企业设计的管理功能相结合。您可以使用托管 Google Play 添加、购买和批准应用程序，以便部署到设备上的 Android Enterprise 工作区。您可以使用 Google Play 部署公共应用程序、私人应用程序和第三方应用程序。

对于托管设备的用户而言，托管 Google Play 是企业应用程序商店。用户可以浏览应用程序、查看应用程序详细信息并安装它们。与公共版 Google Play 不同，用户只能从您为其提供的托管 Google Play 中安装应用程序。

设备部署方案和配置文件

设备部署场景指的是您部署的设备归谁所有以及如何管理它们。设备配置文件指的是 DPC 如何在设备上管理和实施策略。

工作配置文件将业务帐户、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是分开的。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。

重要提示：

当 Android Enterprise 设备更新到 Android 11 时，Google 会将作为“完全托管且带有工作配置文件”管理的设备迁移到新的安全增强型工作配置文件体验。新的注册模式称为“公司拥有设备上的工作配置文件”。有关详细信息，请参阅 Android Enterprise 完全托管且带有工作配置文件的未来变化。 对于 Android 12 设备，请参阅 工作配置文件的安全和隐私增强功能。

设备管理	用例	工作配置文件	个人配置文件	备注
公司拥有的设备（完全托管）	仅用于工作用途的公司拥有的设备	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。
完全托管且带有工作配置文件 / 公司拥有设备上的工作配置文件	适用于工作和个人用途的公司拥有的设备	是	是。这些设备上运行着两个 DPC 副本：一个以设备所有者模式管理设备，另一个以配置文件所有者模式管理工作配置文件。您可以对设备和工作配置文件应用单独的策略。	请参阅 预配带有工作配置文件或公司拥有设备上的工作配置文件的 Android Enterprise 完全托管设备。

设备管理	用例	工作配置文件	个人配置文件	备注
专用设备*	公司拥有的设备，配置用于单一用例，例如数字标牌或票据打印	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（也称为配置文件所有者模式）	是	是。DPC 仅管理工作配置文件，而不管理整个设备。	这些设备无需是新设备或恢复出厂设置。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。当用户登录专用设备上的应用程序时，其工作状态与应用程序相关，而非设备本身。

** Citrix Endpoint Management 不支持 BYOD 工作配置文件模式下的 Zebra 设备。Citrix Endpoint Management 支持将 Zebra 设备作为使用 Android Enterprise 的完全托管设备。

注册安全性

注册配置文件决定 Android 设备是注册到 MAM、MDM 还是 MDM+MAM，并为用户提供了选择退出 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。

Citrix Endpoint Management 支持以下适用于注册到 MDM 或 MDM+MAM 的 Android 设备的身份验证方法。有关详细信息，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(/zh-cn/citrix-endpoint-management/authentication/authentication-with-azure-active-directory-through-citrix-cloud.html) (预览版)

  - 通过 Citrix Cloud 使用 Okta 进行身份验证(/zh-cn/citrix-endpoint-management/authentication/authentication-with-okta-through-citrix-cloud.html) (预览版)

一种不常用的身份验证方法是客户端证书加安全令牌。有关详细信息，请参阅 `<https://support.citrix.com/article/CTX215200>`。

要求

开始使用 Android Enterprise 之前，您需要：

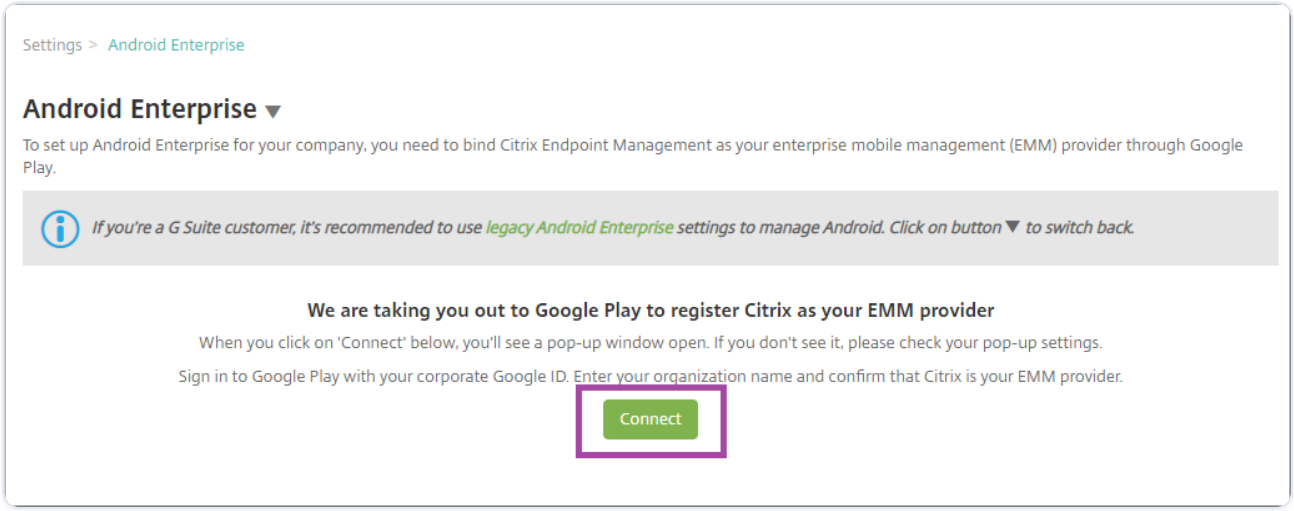
- 帐户和凭据：
  - 要使用托管 Google Play 设置 Android Enterprise，需要一个企业 Google 帐户
  - 要下载最新的 MDX 文件，需要一个 Citrix® 客户帐户
- 已为 Citrix Endpoint Management 配置的 Firebase Cloud Messaging (FCM) 和连接计划设备策略。请参阅 (/zh-cn/citrix-endpoint-management/device-management/android/firebase-cloud-messaging.html) 和 (/zh-cn/citrix-endpoint-management/policies/connection-scheduling-policy.html)。

将 Citrix Endpoint Management 连接到 Google Play 商店

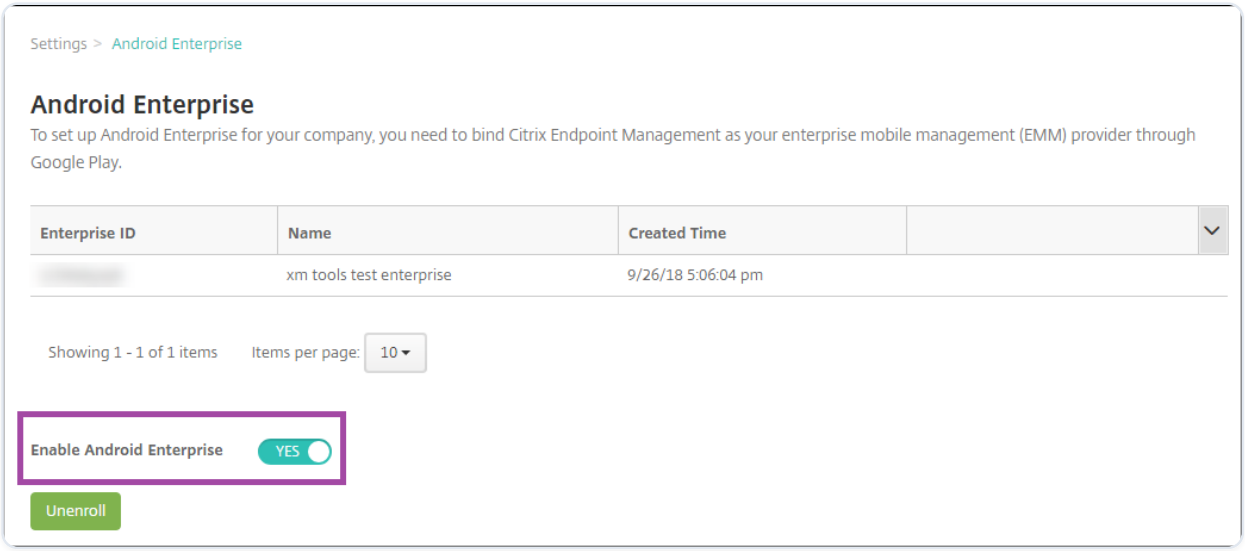
要为您的组织设置 Android Enterprise，请通过托管 Google Play 将 Citrix 注册为您的 EMM 提供商。此设置会将托管 Google Play 连接到 Citrix Endpoint Management，并在 Citrix Endpoint Management 中为 Android Enterprise 创建一个企业。

您需要一个企业 Google 帐户才能登录 Google Play。

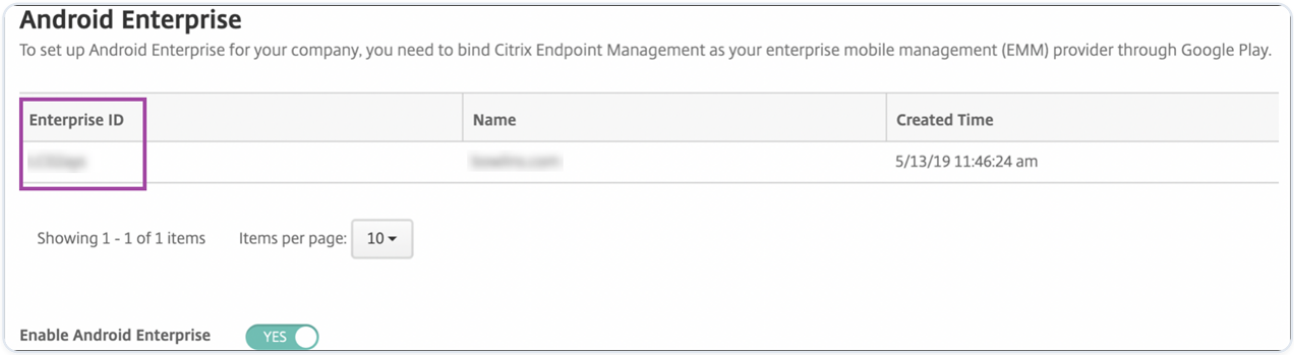
1. 在 Citrix Endpoint Management 控制台中，转到 **设置 > Android Enterprise**。
2. 单击 **Connect**。Google Play 将打开。



1. 使用您的企业 Google 帐户凭据登录 Google Play。输入您的组织名称并确认 Citrix 是您的 EMM 提供商。
2. 已为 Android Enterprise 添加企业 ID。要启用 Android Enterprise，请将 **Enable Android Enterprise** 滑动到 **Yes**。



您的企业 ID 将显示在 Citrix Endpoint Management 控制台中。



您的环境已连接到 Google，并已准备好管理设备。您现在可以为用户提供应用程序。

Citrix 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、企业应用程序以及 Web 链接。有关向用户提供这些类型应用程序的更多信息，请参阅分发 Android Enterprise 应用程序。

以下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执行以下步骤。

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. 配置用户用于访问其设备上工作配置文件的安全质询规则。请参阅配置安全质询策略。

您发布的应用程序可供已注册到您的 Android Enterprise 企业的设备使用。

> **注意：**
>
> 当您向 Android 用户部署 Android Enterprise 公共应用商店应用程序时，该用户将自动注册到 Android Enterprise。

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 Android Enterprise 的 MDX 应用程序，请执行以下操作：

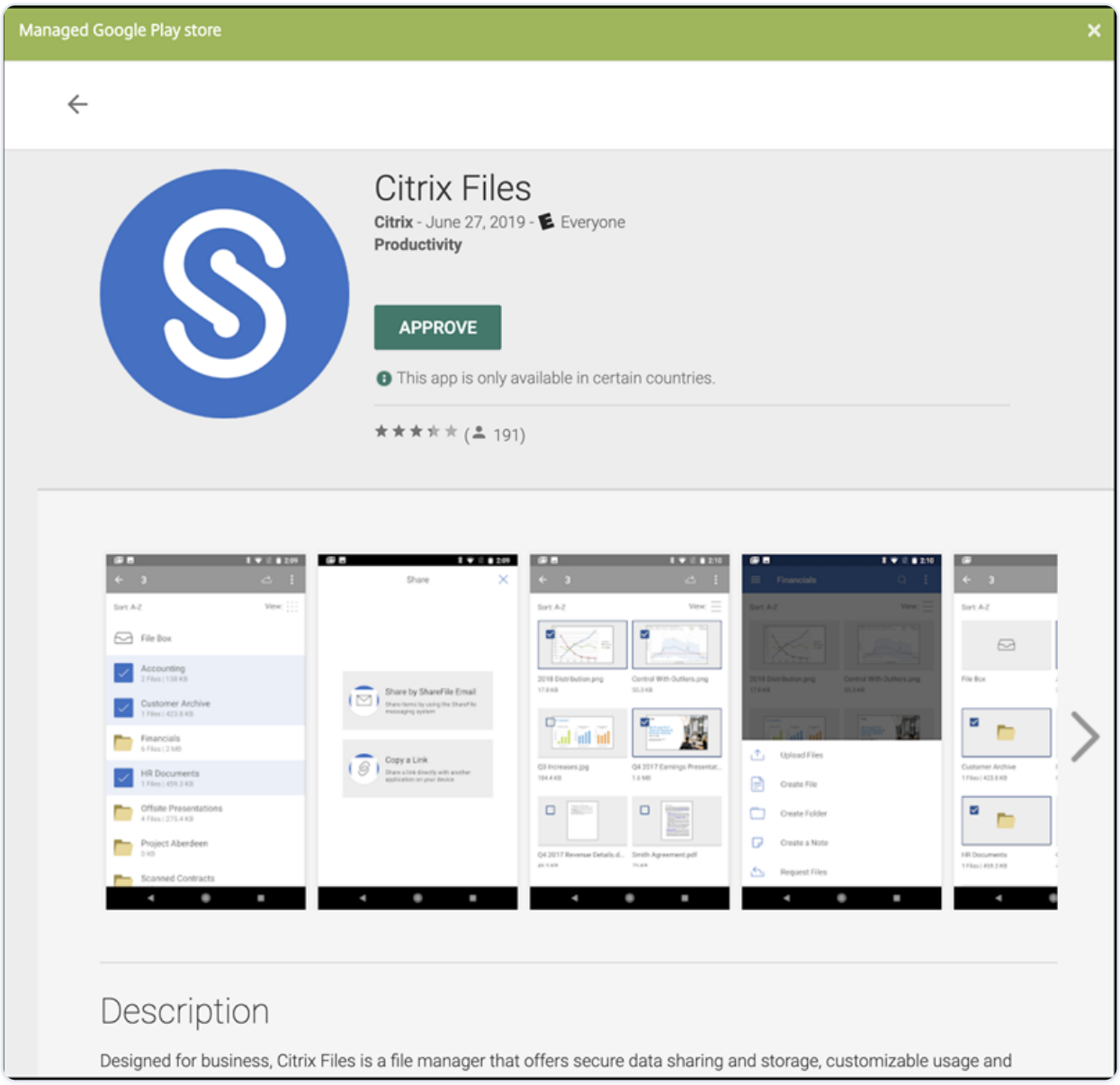
1. 在 Citrix Endpoint Management 控制台中，单击 **配置 > 应用程序**。将显示 **应用程序** 页面。

   应用程序配置屏幕(/en-us/citrix-endpoint-management/media/configure-apps-example-list.png)
2. 单击 **添加**。将显示 **添加应用程序** 对话框。

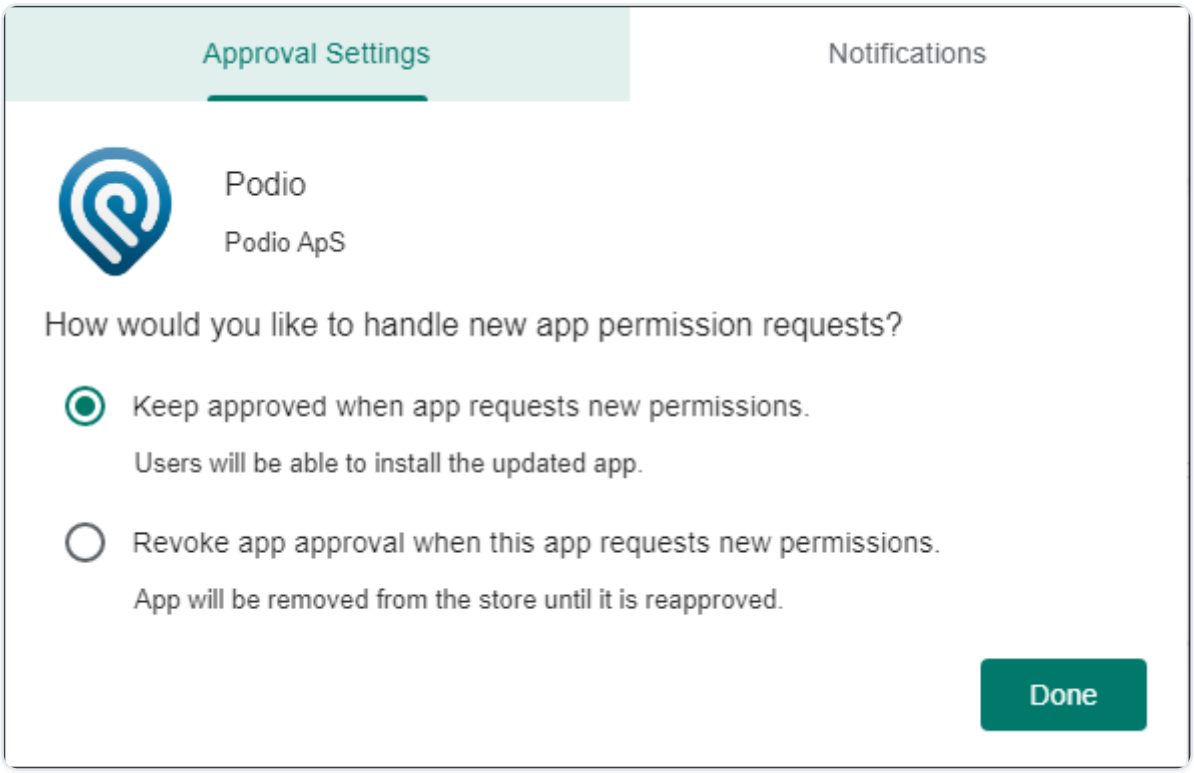
   应用程序配置屏幕(/en-us/citrix-endpoint-management/media/configure-apps-add.png)
3. 单击 **MDX**。将显示 **应用程序信息** 页面。
4. 在页面的左侧，选择 **Android Enterprise** 作为平台。
5. 在 **应用程序信息** 页面上，键入以下信息：

   - **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，单击要添加应用程序的类别。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**。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 .mdx 文件的文件位置。选择文件，然后单击 **打开**。
8. 如果附加的应用程序需要托管 Google Play 商店的批准，UI 会通知您。要在不离开 Citrix Endpoint Management 控制台的情况下批准应用程序，请单击 **是**。

   添加 MDX 应用程序(/en-us/citrix-endpoint-management/media/mdx-app-not-approved.png)
9. 当托管 Google Play 商店页面打开时，单击 **批准**。



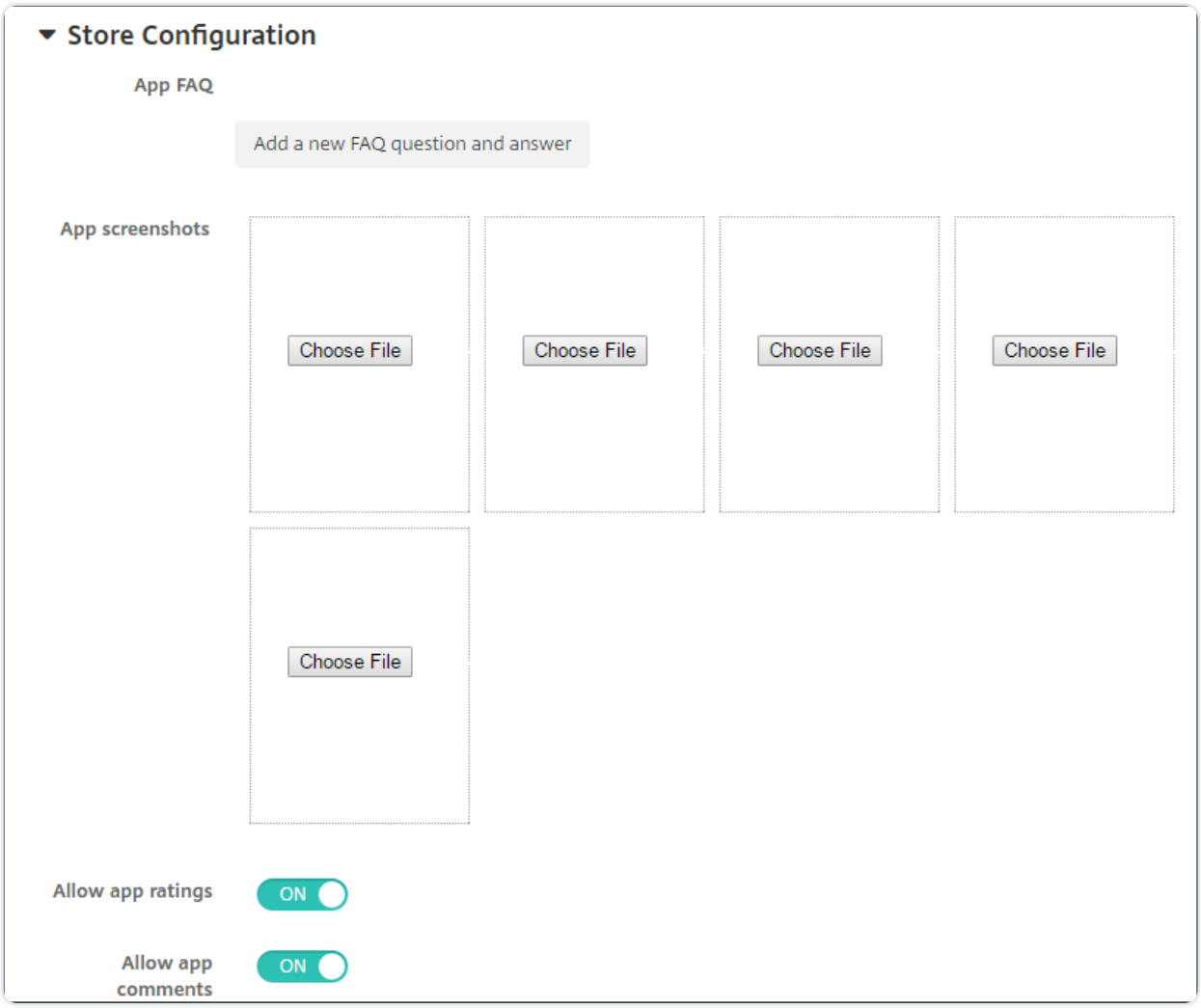
10. 再次单击**批准**。
11. 选择**当应用程序请求新权限时保持批准**。单击**保存**。



12. 应用程序获得批准并保存后，页面上将显示更多设置。配置这些设置：

    - **文件名：**键入与应用程序关联的文件名。
    - **应用程序描述：**键入应用程序的描述。
    - **产品跟踪：**指定要推送到用户设备的产品跟踪。如果您有专为测试设计的跟踪，则可以选择并将其分配给用户。默认值为“生产”。
    - **应用程序版本：**（可选）键入应用程序版本号。
    - **程序包 ID：**Google Play 商店中应用程序的 URL。
    - **最低操作系统版本：**（可选）键入设备可运行的、用于使用此应用程序的最旧操作系统版本。
    - **最高操作系统版本：**（可选）键入设备必须运行的、用于使用此应用程序的最新操作系统版本。
    - **排除的设备：**（可选）键入无法运行此应用程序的设备的制造商或型号。

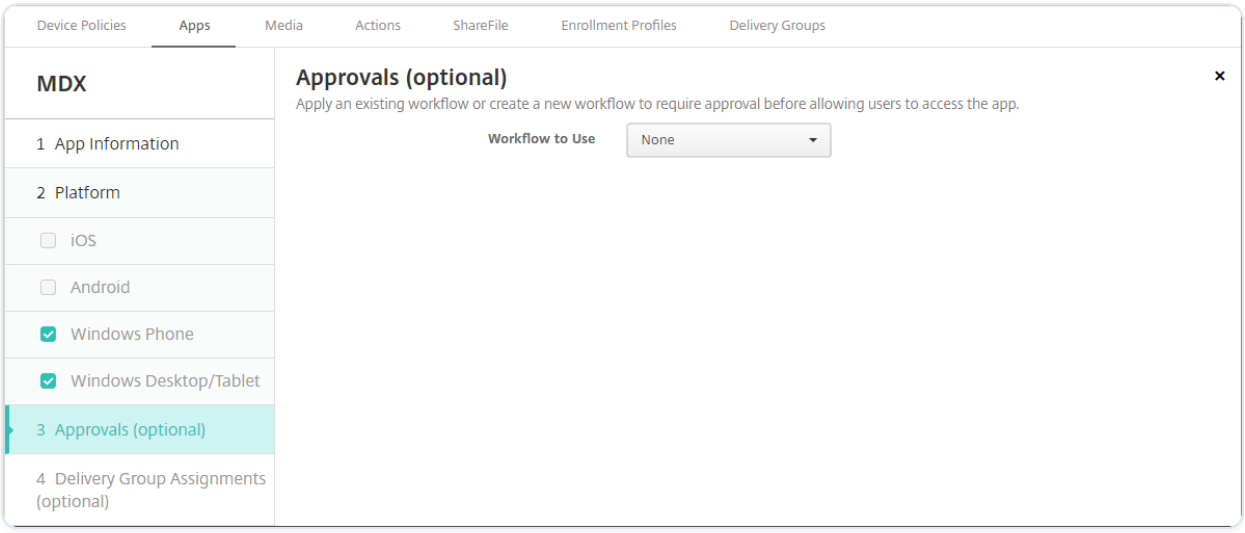
13. 配置 **MDX 策略**。有关 MDX 应用程序的应用程序策略的详细信息，请参阅MDX 策略概述和 MAM SDK 概述。
14. 配置部署规则。有关信息，请参阅部署资源。
15. 展开**应用商店配置**。此设置不适用于 Android Enterprise 应用程序，这些应用程序仅显示在托管 Google Play 中。



您可以选择为应用程序添加常见问题解答或在应用商店中显示的屏幕截图。您还可以设置用户是否可以对应用程序进行评分或评论。

- 配置以下设置：
  - **应用程序常见问题解答：** 为应用程序添加常见问题和答案。
  - **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。您上传的图形必须是 PNG 格式。您不能上传 GIF 或 JPEG 图像。
  - **允许应用程序评分：** 选择是否允许用户对应用程序进行评分。默认值为**开**。 **允许应用程序评论：** 选择是否允许用户评论所选应用程序。默认值为**开**。

16. 单击**下一步**。此时将显示**批准**页面。



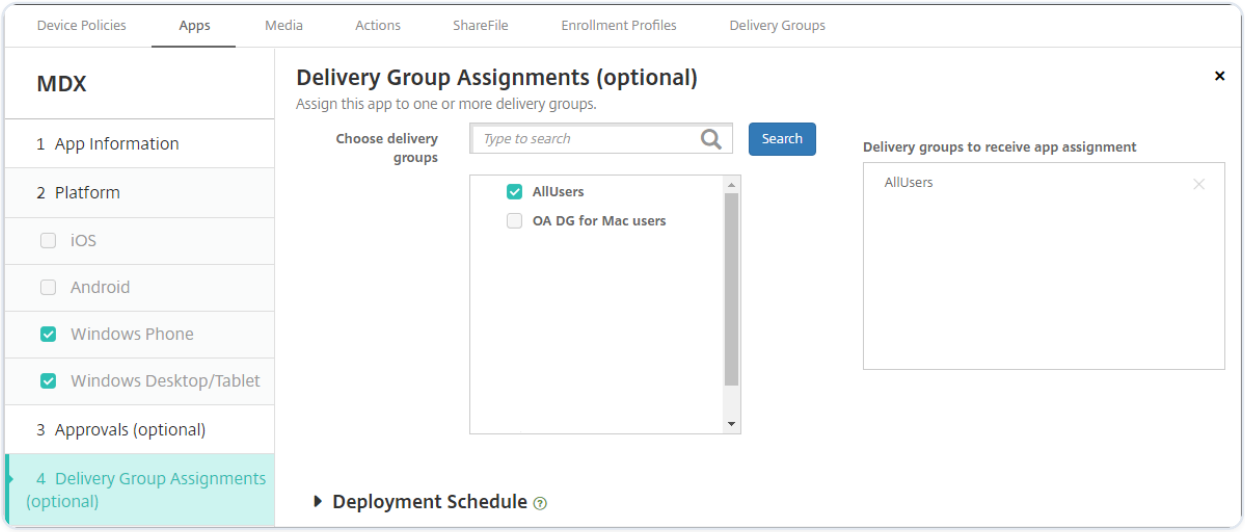
在创建用户帐户时需要批准时，您可以使用工作流。如果您不想设置批准工作流，可以跳到步骤 15。

配置以下设置以分配或创建工作流：

- **要使用的工作流：** 单击下拉列表中的现有工作流，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。
- **描述：** （可选）键入工作流的描述。
- **电子邮件审批模板：** 在列表中，选择要分配的电子邮件审批模板。当您单击此字段右侧的眼睛图标时，将出现一个对话框，您可以在其中预览模板。
- **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，选择要用于工作流的相应 Active Directory 域。
- **查找其他必需的审批者：** 在搜索字段中键入其他必需人员的姓名，然后单击“**搜索**”。姓名源自 Active Directory。
- 当姓名出现在字段中时，选中姓名旁边的复选框。姓名和电子邮件地址将显示在“**选定的其他必需审批者**”列表中。
  - 要从“**选定的其他必需审批者**”列表中删除人员，请执行以下操作之一：

- 单击“**搜索**”以查看所选域中所有人员的列表。
- 在搜索框中键入完整或部分姓名，然后单击“**搜索**”以限制搜索结果。
- “**选定的其他必需审批者**”列表中的人员在搜索结果列表中其姓名旁边带有复选标记。滚动列表并清除要删除的每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。



18. 在“**选择交付组**”旁边，键入以查找交付组，或从列表中选择一个或多个组。您选择的组将显示在“**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**”以安排部署，或单击“**关**”以阻止部署。默认选项设置为“**开**”。
- 在“部署计划”旁边，单击“**立即**”或“**稍后**”。默认选项设置为“**立即**”。
- 如果单击“**稍后**”，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“**仅当以前的部署失败时**”。默认选项设置为“**每次连接时**”。
- 在“**为始终在线连接部署**”旁边，确保选中“**关**”。默认选项设置为“**关**”。对于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的客户，Android Enterprise 不提供始终在线连接。对于在版本 10.18.19 之前开始使用 Citrix Endpoint Management 的客户，我们不建议使用这些连接。

  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。

  您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但“**为始终在线连接部署**”除外。

20. 点击 **保存**。

对每个移动生产力应用程序重复这些步骤。

配置安全质询策略

Citrix Endpoint Management 密码设备策略配置安全质询规则。当用户访问其设备或设备上的 Android Enterprise 工作配置文件时，会出现质询。安全质询可以是密码或生物识别。有关密码策略的详细信息，请参阅密码设备策略。

- 如果您的 Android Enterprise 部署包含 BYOD 设备，请为工作配置文件配置密码策略。
- 如果您的部署包含公司拥有的完全托管设备，请为设备本身配置密码策略。
- 如果您的部署包含这两种类型的设备，请配置这两种类型的密码策略。

要配置密码策略：

1. 在 Citrix Endpoint Management 控制台中，转至 **配置 > 设备策略**。
2. 单击 **添加**。
3. 单击 **Show filter** 以显示 **Policy Platform** 窗格。在 **Policy Platform** 窗格中，选择 **Android Enterprise**。
4. 在右侧窗格中单击 **Passcode**。

密码安全选项(/en-us/citrix-endpoint-management/media/password-security-policy.png)

1. 输入 **Policy Name**。单击 **Next**。

   密码安全名称(/en-us/citrix-endpoint-management/media/password-security-name.png)
2. 配置密码策略设置。
   - 将 **Device passcode required** 设置为 **On** 以查看设备本身的安全质询可用设置。
   - 将 **Work profile security challenge** 设置为 **On** 以查看工作配置文件安全质询的可用设置。
3. 单击“**下一步**”。
4. 将策略分配给一个或多个交付组。
5. 点击 **保存**。

创建注册配置文件

如果为您的 Citrix Endpoint Management 部署启用了 Android Enterprise，注册配置文件将控制 Android 设备的注册方式。当您创建注册配置文件以注册 Android Enterprise 设备时，您可以将注册配置文件配置为注册新的和恢复出厂设置的设备，如下所示：

- 完全托管设备

- 专用设备
- 具有工作资料的完全托管设备/公司自有设备上的工作资料

您还可以配置每个 Android Enterprise 注册配置文件，以将 BYOD Android 设备注册为工作资料设备。

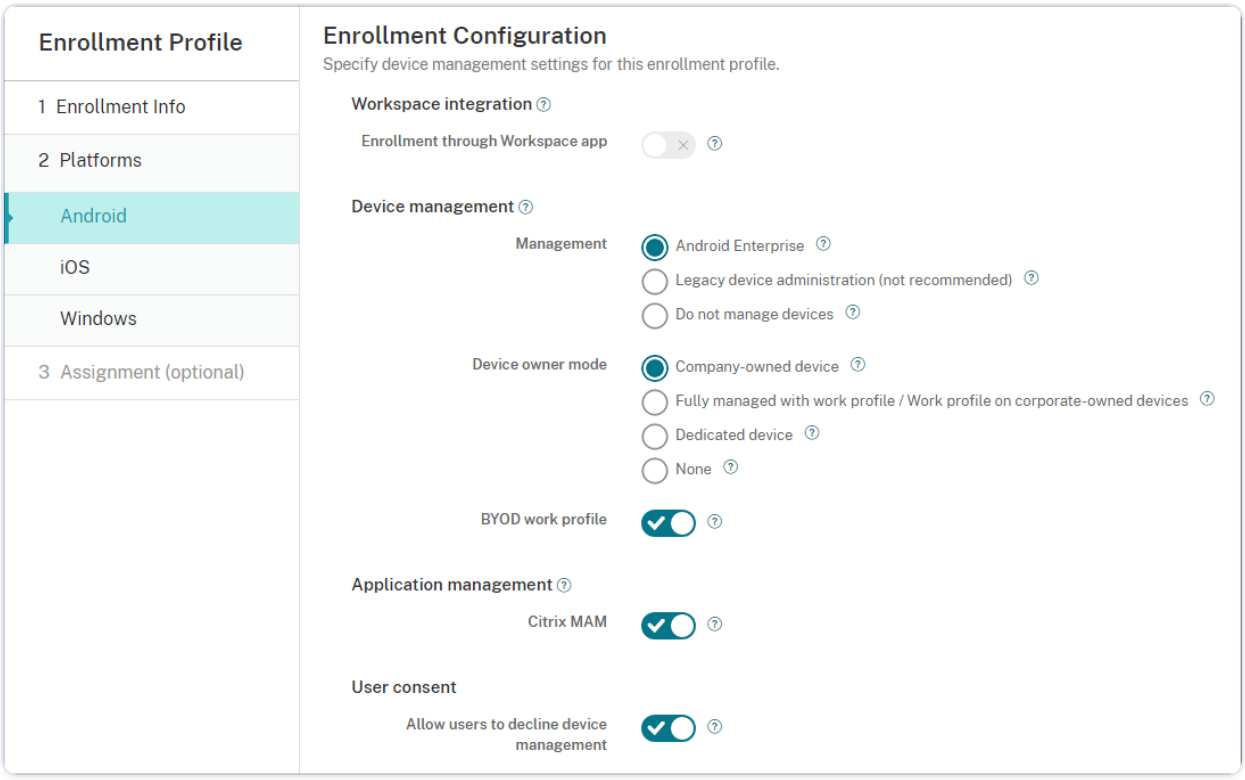
如果您的 Citrix Endpoint Management 部署启用了 Android Enterprise，所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。默认情况下，全局注册配置文件会将新的和恢复出厂设置的 Android 设备注册为完全托管设备，并将 BYOD Android 设备注册为公司自有设备上的工作资料。

创建注册配置文件时，您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，交付组的名称将决定所使用的注册配置文件。Citrix Endpoint Management 会选择按字母顺序排列的交付组列表中最后一个出现的交付组。有关详细信息，请参阅注册配置文件。

添加用于完全托管设备的注册配置文件

全局注册配置文件默认注册完全托管设备，但您可以创建更多注册配置文件来注册完全托管设备。

1. 在 Citrix Endpoint Management 控制台中，转至 **配置 > 注册配置文件**。
2. 要添加注册配置文件，请单击 **Add**。在“注册信息”页面上，键入注册配置文件的名称。
3. 设置具有此配置文件的成员可以注册的设备数量。
4. 在 **Platforms** 下选择 **Android** 或单击 **Next**。“注册配置”页面随即显示。
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**。



7. **BYOD work profile** 允许您配置注册配置文件以将 BYOD 设备注册为工作资料设备。新设备和恢复出厂设置的设备将注册为完全托管设备。将 **BYOD work profile** 设置为 **On** 以允许将 BYOD 设备注册为工作资料设备。将 **BYOD work profile** 设置为 **Off** 以将注册限制为完全托管设备。默认值为 **On**。
8. 选择是否在 Citrix MAM 中注册设备。
9. 如果您将**BYOD 工作配置文件**设置为**开**，请配置用户同意。要允许 BYOD 工作配置文件设备的用户在注册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**允许用户拒绝设备管理**将被禁用。
10. 选择**分配（选项）**。此时将显示“交付组分配”屏幕。
11. 选择包含注册完全托管设备的管理员的交付组。然后单击**保存**。

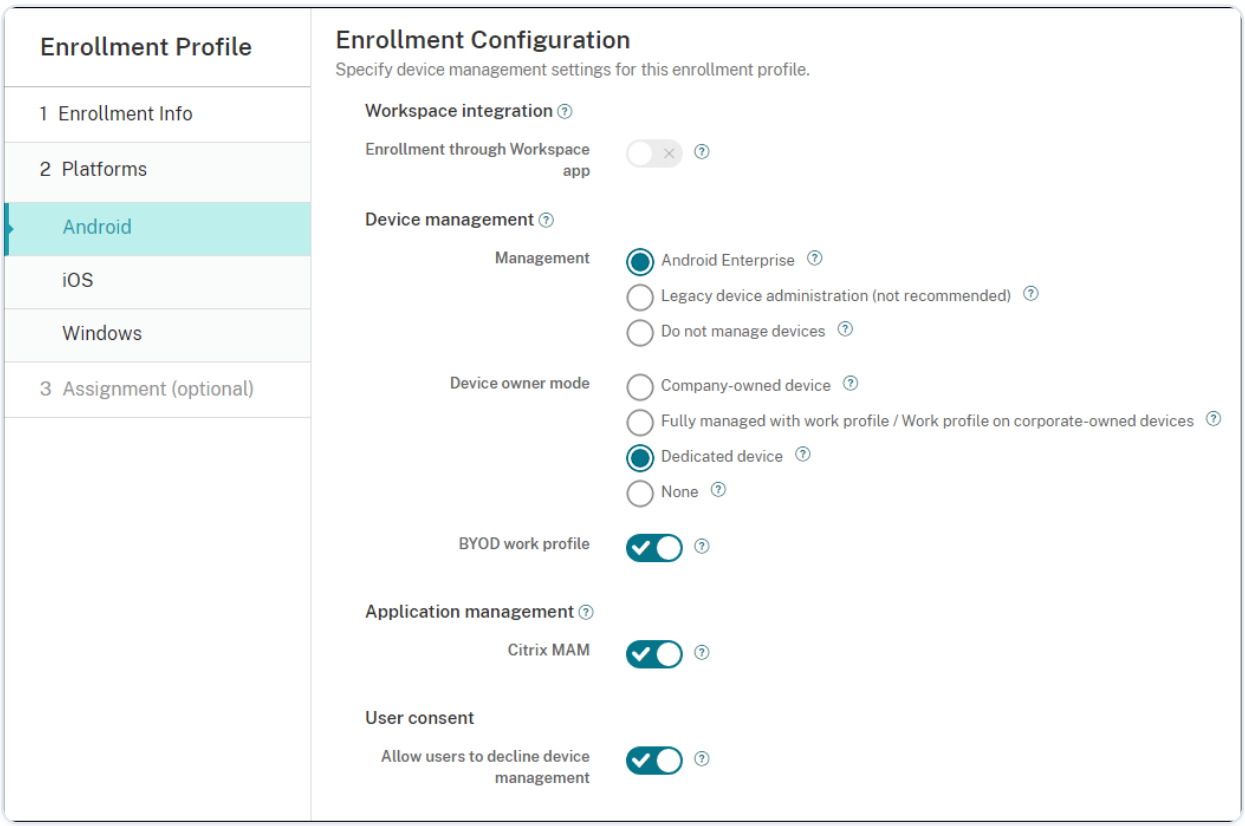
    此时将显示“注册配置文件”页面，其中包含您添加的配置文件。

添加专用设备注册配置文件

当您的 Citrix Endpoint Management 部署包含专用设备时，单个 Citrix Endpoint Management 管理员或一小组管理员会注册许多专用设备。为确保这些管理员可以注册所有必需的设备，请为他们创建注册配置文件，并允许每个用户注册无限数量的设备。

1. 在 Citrix Endpoint Management 控制台中，转至**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。将此配置文件成员可以注册的设备数量设置为**无限制**。
3. 在**平台**下选择**Android**，或单击**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**。



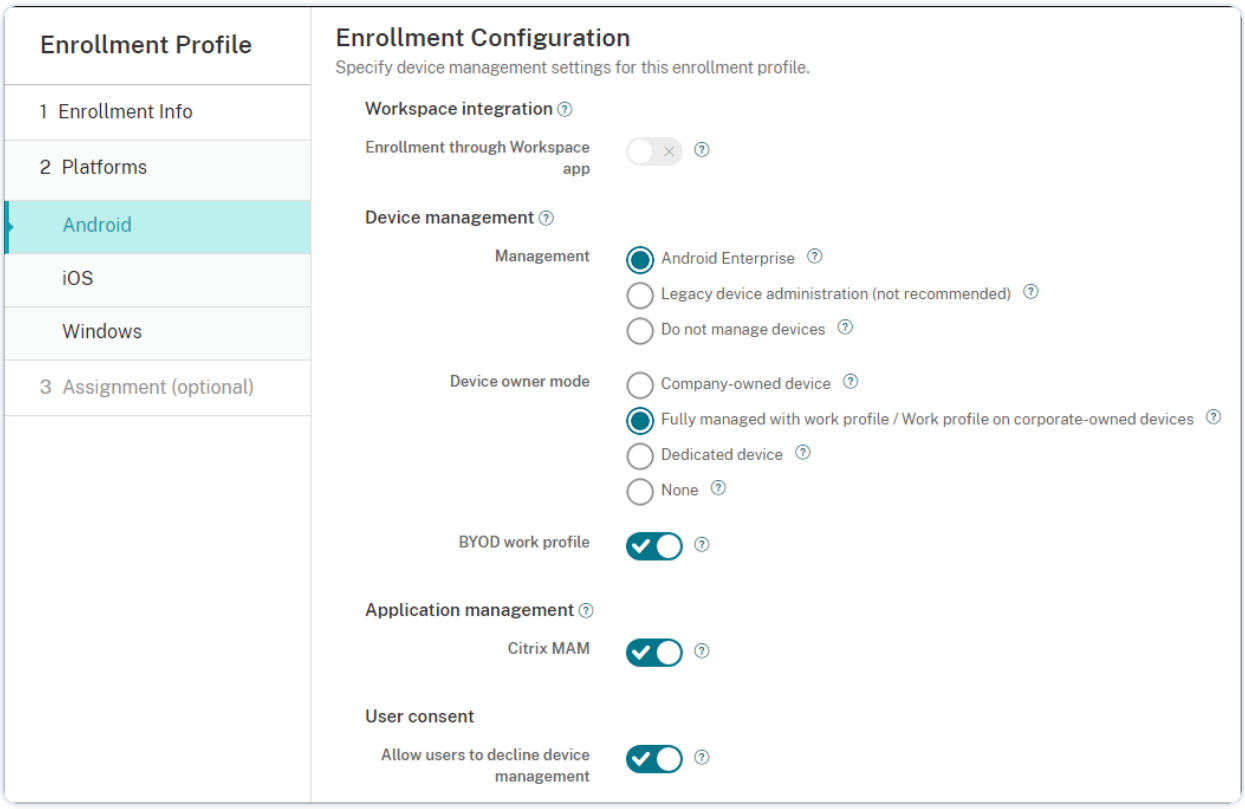
6. **BYOD 工作配置文件**允许您配置注册配置文件，以将 BYOD 设备注册为工作配置文件设备。新设备和恢复出厂设置的设备将注册为专用设备。将**BYOD 工作配置文件**设置为**开**以允许将 BYOD 设备注册为工作配置文件设备。将**BYOD 工作配置文件**设置为**关**以限制仅注册公司拥有的设备。默认值为**开**。
7. 选择是否在 Citrix MAM 中注册设备。
8. 如果将 **BYOD 工作配置文件** 设置为 **开**，请配置用户同意。要允许 BYOD 工作配置文件设备的用户在注册设备时拒绝设备管理，请将 **允许用户拒绝设备管理** 设置为 **开**。

   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 **允许用户拒绝设备管理** 将被禁用。
9. 选择 **分配（选项）**。此时将显示“交付组分配”屏幕。
10. 选择包含注册专用设备的管理员的交付组。然后单击 **保存**。

    此时将显示“注册配置文件”页面以及您添加的配置文件。

为具有工作配置文件/公司拥有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 Citrix Endpoint Management 控制台中，转至 **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. 设置具有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 **具有工作配置文件的完全托管 / 公司拥有设备上的工作配置文件**。



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。新设备和恢复出厂设置的设备将注册为具有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** 以将注册限制为专用设备。默认值为 **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。要允许 BYOD 工作配置文件设备的用户在注册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**允许用户拒绝设备管理**处于禁用状态。
9. 选择**分配（选项）**。此时将显示“交付组分配”屏幕。
10. 选择具有使用工作配置文件注册完全托管设备的管理员的交付组或交付组。然后单击**保存**。

此时将显示“注册配置文件”页面以及您添加的配置文件。

为旧版设备添加注册配置文件

Google 已弃用设备管理的设备管理员模式。Google 鼓励客户以设备所有者模式或配置文件所有者模式管理所有 Android 设备。（请参阅 Google Android Enterprise 开发人员指南中的设备管理员弃用。）

为支持此更改：

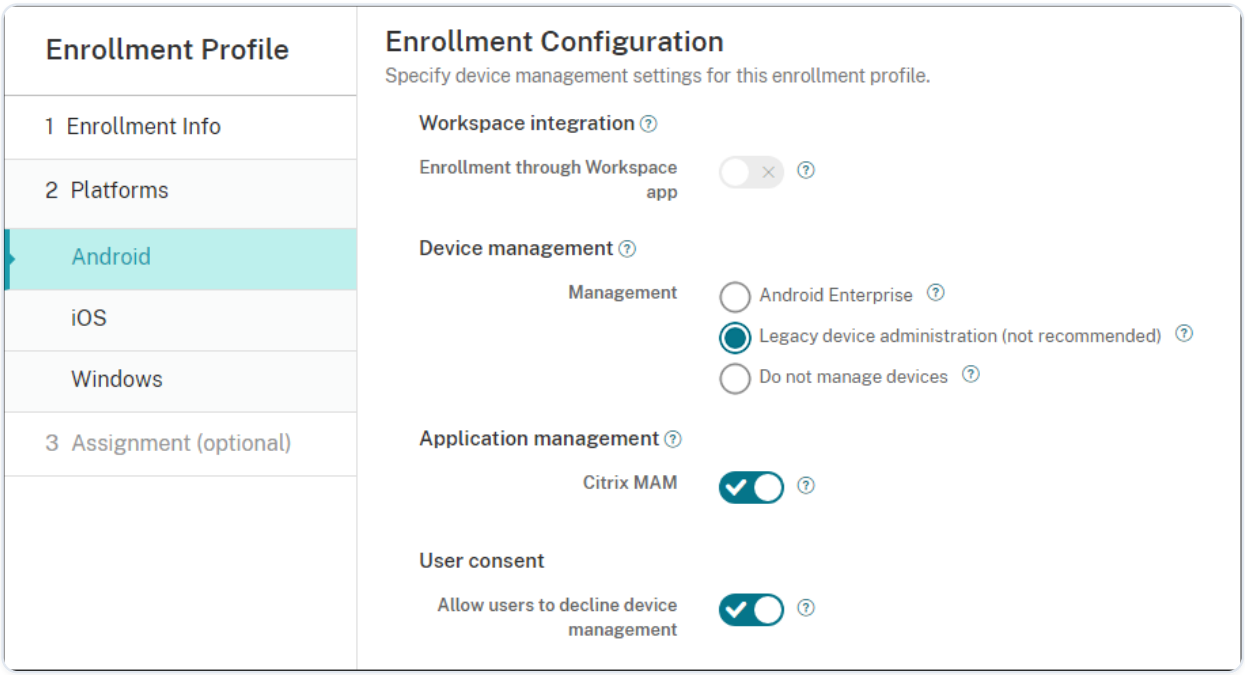
- Citrix 将 Android Enterprise 设为 Android 设备的默认注册选项。
- 如果您的 Citrix Endpoint Management 部署启用了 Android Enterprise，则所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。

您的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，您可以继续以设备管理员模式管理它们。对于已在设备管理员模式下注册的设备，Citrix Endpoint Management 将继续以设备管理员模式管理它们。

为旧版设备创建注册配置文件，以允许新的 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，请执行以下操作：

1. 在 Citrix Endpoint Management 控制台中，转至**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. 设置具有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** 或点击 **下一步**。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）**。点击 **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）**。将显示“交付组分配”屏幕。
9. 选择包含注册专用设备的管理员的交付组或多个交付组。然后点击 **保存**。

将显示“注册配置文件”页面，其中包含您添加的配置文件。

要继续在设备管理员模式下管理旧版设备，请使用此配置文件注册或重新注册它们。您可以通过让用户下载 Citrix Secure Hub 并提供注册服务器 URL 来注册设备管理员设备，这与工作配置文件设备类似。

预配 Android Enterprise 工作配置文件设备

Android Enterprise 工作配置文件设备以配置文件所有者模式注册。这些设备无需是新设备或恢复出厂设置的设备。BYOD 设备注册为工作配置文件设备。注册体验类似于 Citrix Endpoint Management 中的 Android 注册。用户从 Google Play 下载 Citrix Secure Hub 并注册其设备。

默认情况下，当您将设备作为工作配置文件设备注册到 Android Enterprise 时，设备上的 **USB 调试和未知来源** 设置将被禁用。

将设备作为工作配置文件设备注册到 Android Enterprise 时，请始终前往 Google Play。从那里，启用 Citrix Secure Hub 以显示在用户的个人配置文件中。

预配 Android Enterprise 完全托管设备

您可以在前面部分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，并以设备所有者模式注册。只有新设备或恢复出厂设置的设备才能以设备所有者模式注册。

您可以使用以下任一注册方法在设备所有者模式下注册设备：

- **DPC 标识符令牌：** 使用此注册方法时，用户在设置设备时输入字符 `afw#xenmobile`。`afw#xenmobile` 是 Citrix DPC 标识符令牌。此令牌将设备标识为由 Citrix Endpoint Management 管理，并从 Google Play 商店下载 Citrix 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 碰撞注册方法使用近场通信在两台设备之间传输数据。在新设备或恢复出厂设置的设备上，蓝牙、Wi-Fi 和其他通信模式均已禁用。NFC 是设备在此状态下可以使用的唯一通信协议。请参阅使用 NFC 碰撞注册设备。
- **QR 码：** QR 码注册可用于注册不支持 NFC 的分布式设备群，例如平板电脑。QR 码注册方法通过从设置向导扫描 QR 码来设置和配置设备配置文件模式。请参阅使用 QR 码注册设备。
- **零接触：** 零接触注册允许您配置设备在首次开机时自动注册。零接触注册支持运行 Android 9.0 或更高版本的部分 Android 设备。请参阅零接触注册。
- **Google 帐户：** 用户输入其 Google 帐户凭据以开始预配过程。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

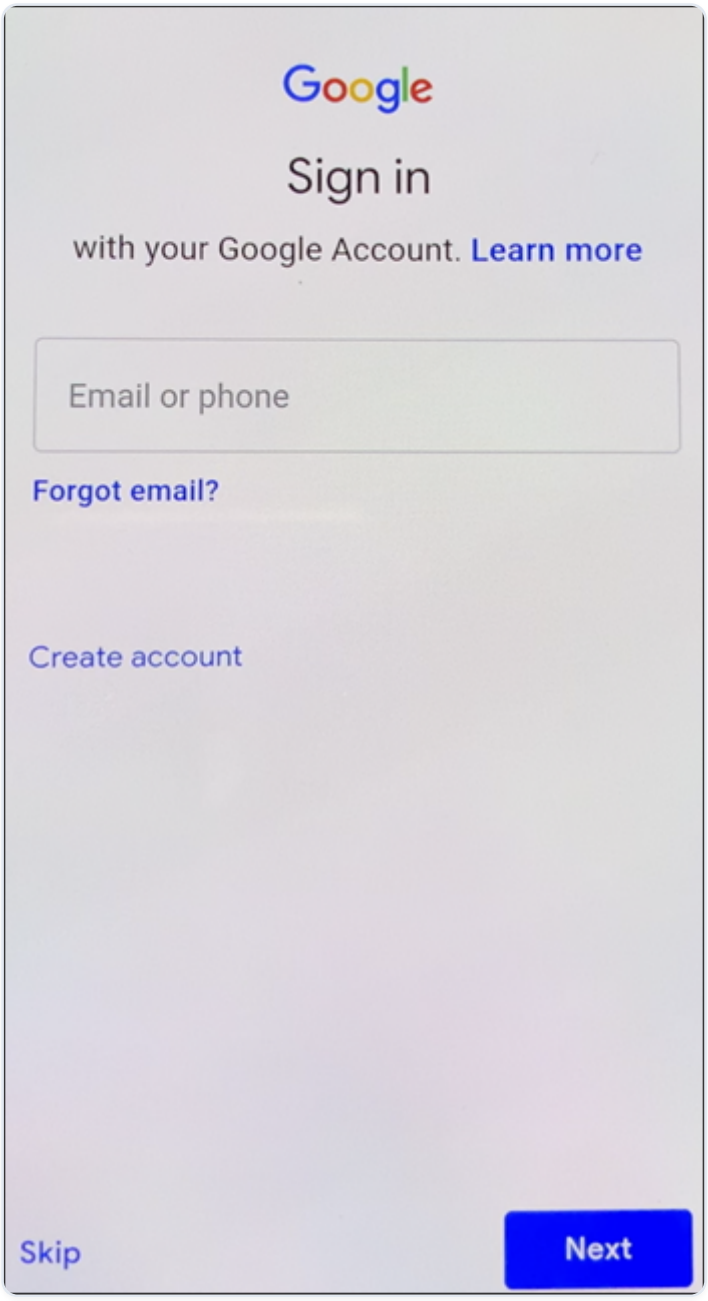
用户在首次设置时，在新设备或恢复出厂设置的设备开机后，当系统提示输入 Google 帐户时，输入 `afw#xenmobile`。此操作将下载并安装 Citrix Secure Hub。然后，用户按照 Citrix Secure Hub 设置提示完成注册。

系统要求

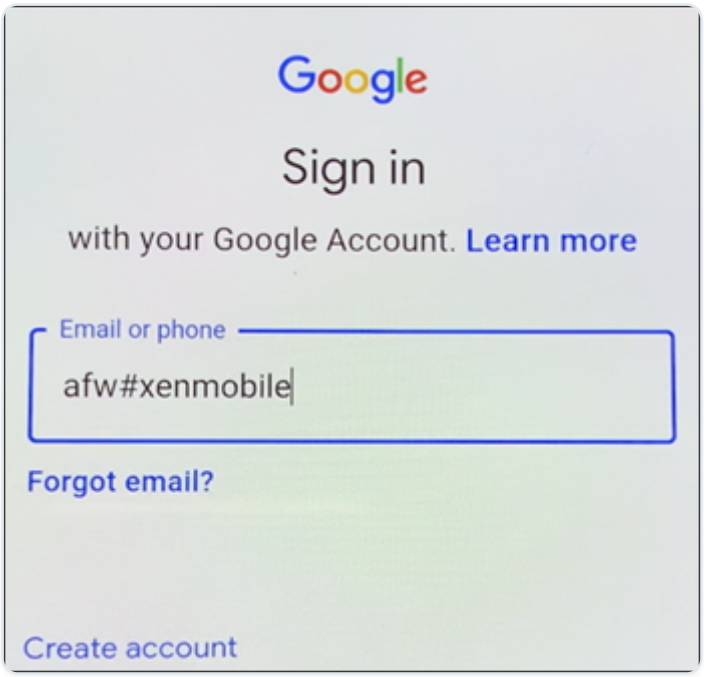
- 支持所有运行 Android 操作系统的 Android 设备。

注册设备

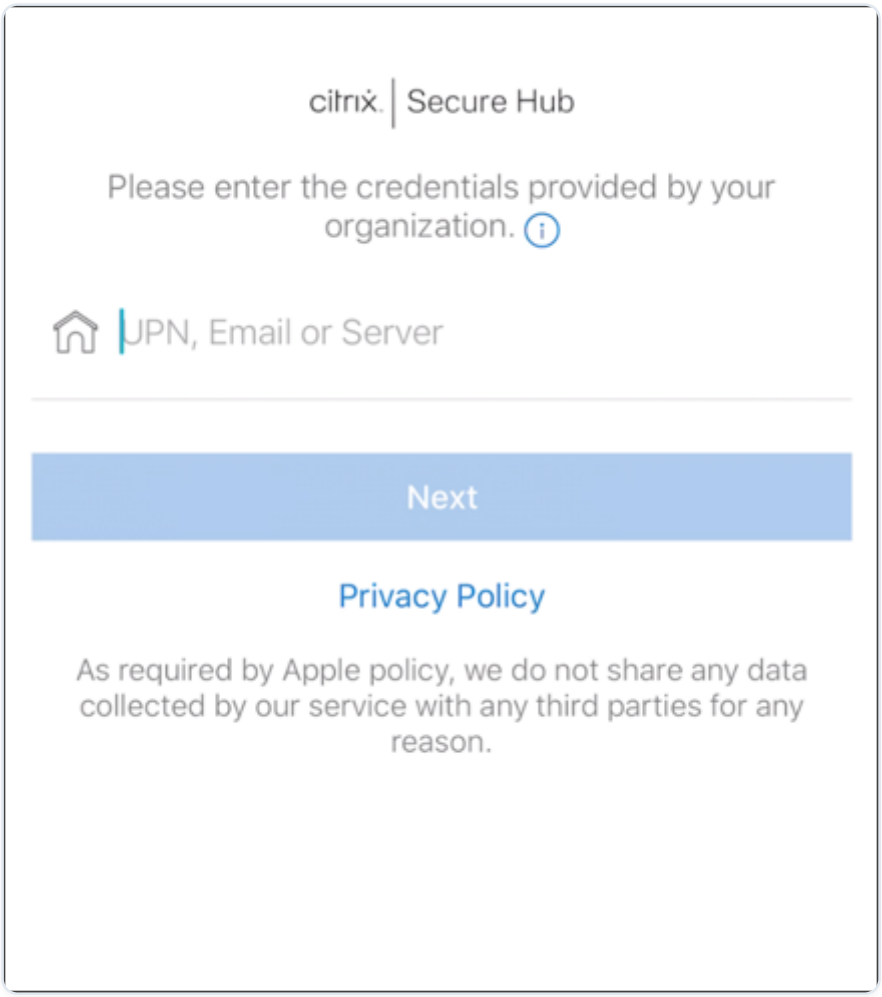
1. 打开新设备或恢复出厂设置的设备。
2. 初始设备设置加载并提示输入 Google 帐户。如果设备加载了设备主屏幕，请检查通知栏中是否有“**完成设置**”通知。



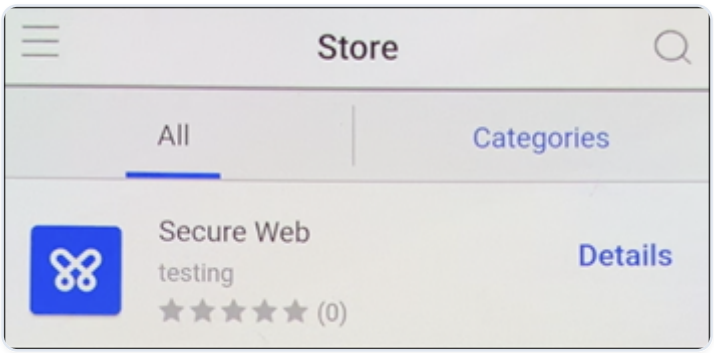
3. 在“**电子邮件或电话**”字段中输入 `afw#xenmobile`。



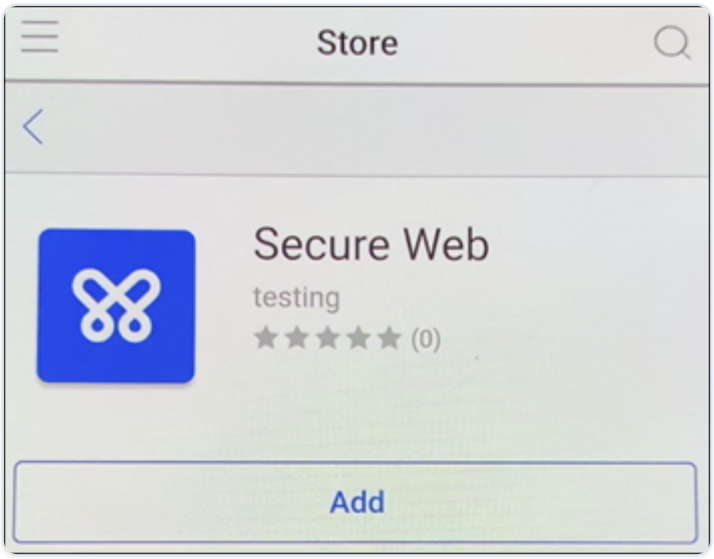
4. 在提示安装 Citrix Secure Hub 的 Android Enterprise 屏幕上点击“**安装**”。
5. 在 Citrix Secure Hub 安装程序屏幕上点击“**安装**”。
6. 针对所有应用权限请求点击“**允许**”。
7. 点击“**接受并继续**”以安装 Citrix Secure Hub 并允许其管理设备。
8. Citrix Secure Hub 现已安装并显示在默认注册屏幕上。在此示例中，未设置自动发现。如果已设置，用户可以输入其用户名/电子邮件，系统将为其找到服务器。否则，请输入环境的注册 URL，然后点击“**下一步**”。



9. Citrix Endpoint Management 的默认配置允许用户选择是使用 MAM 还是 MDM+MAM。如果出现此提示，请点击“**是，注册**”以选择 MDM+MAM。
10. 输入用户电子邮件地址和密码，然后点击“**下一步**”。
11. 系统会提示用户配置设备密码。点击“**设置**”并输入密码。
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，点击“**密码**”，点击“**PIN**”，然后输入 PIN。
13. 设备现在位于 Citrix Secure Hub 的“**我的应用**”登录屏幕上。点击“**从应用商店添加应用**”。
14. 要添加 Citrix Secure Web，请点击“**Citrix Secure Web**”。



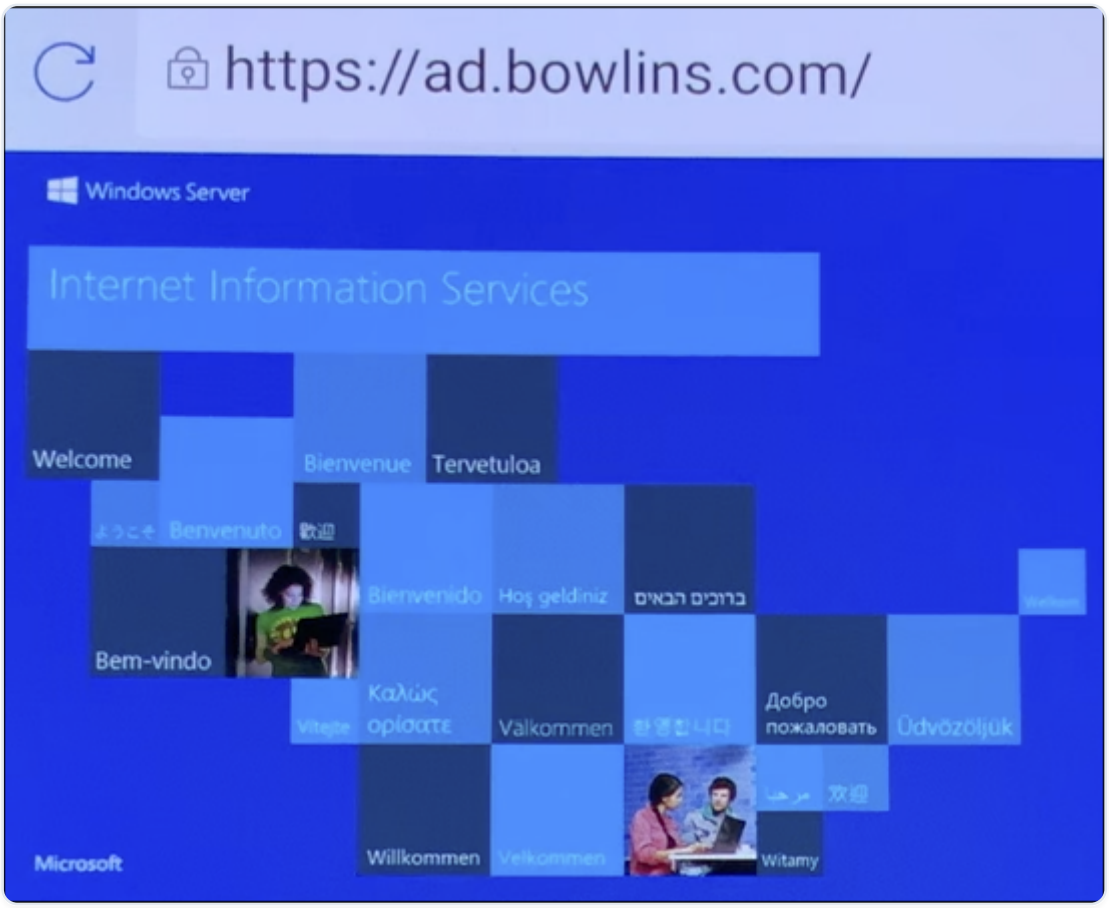
15. 点击“**添加**”。



16. Citrix Secure Hub 将用户引导至 Google Play 商店以安装 Citrix Secure Web。点击 **安装**。

    安全应用程序安装(/en-us/citrix-endpoint-management/media/secure-app-install.png)

17. 安装 Citrix Secure Web 后，点击 **打开**。在地址栏中输入内部站点的 URL，并验证页面是否加载。



18. 在设备上转到 **设置 > 帐户**。观察到 **托管帐户** 无法修改。用于屏幕共享或远程调试的开发者选项也被阻止。

    帐户修改(/en-us/citrix-endpoint-management/media/account-modification-not-allowed.png)

使用 NFC 碰撞注册设备

要使用 NFC 碰撞将设备注册为完全托管设备，需要两台设备：一台已恢复出厂设置，另一台运行 Citrix Endpoint Management 预配工具。

系统要求和先决条件

- 支持的 Android 设备。
- 具有 NFC 功能的全新或已恢复出厂设置的设备，已预配为 Android Enterprise 的完全托管设备。请参阅 预配 Android Enterprise 完全托管设备 部分。
- 另一台具有 NFC 功能的设备，运行已配置的预配工具。预配工具可在 Citrix Secure Hub 或 Citrix 下载页面 上获取。

每台设备只能有一个 Android Enterprise 配置文件。在这种情况下，配置文件用于托管的 Citrix Secure Hub。尝试添加第二个 DPC 应用程序会移除已安装的 Citrix Secure Hub。

通过 NFC 碰撞传输的数据

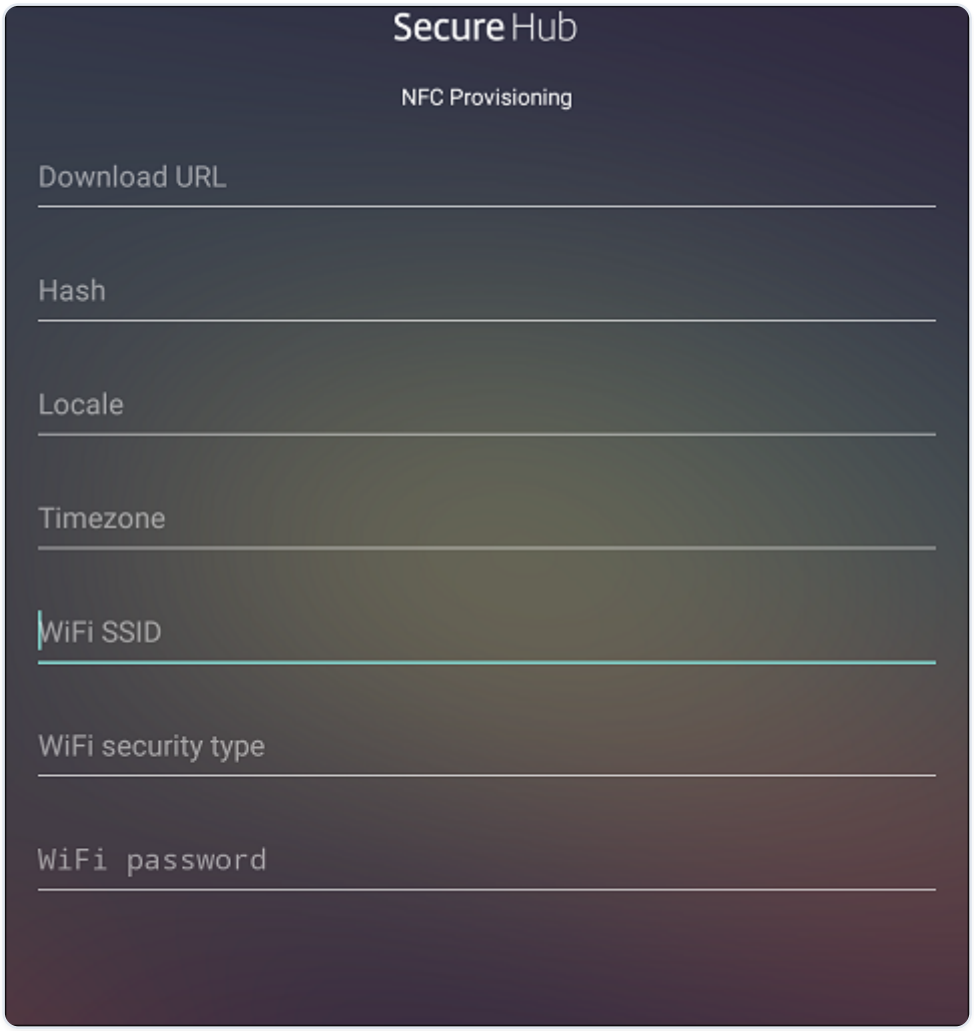
预配已恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以启动 Android Enterprise：

- DPC 应用的包名，该应用充当设备所有者（在本例中为 Citrix Secure Hub）。
- 设备可以从中下载 DPC 应用的内网/互联网位置。
- DPC 应用的 SHA-256 哈希值，用于验证下载是否成功。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备可以连接并下载 DPC 应用。注意：Android 现在不支持此步骤的 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

当两台设备接触时，预配工具中的数据将发送到恢复出厂设置的设备。然后，该数据用于下载具有管理员设置的 Citrix Secure Hub。如果您不输入时区和位置值，Android 会自动在新设备上配置这些值。

配置 CITRIX ENDPOINT MANAGEMENT 预配工具

在执行 NFC 碰触之前，您必须配置预配工具。此配置随后会在 NFC 碰触期间传输到恢复出厂设置的设备。



您可以将数据键入到必填字段中，或者使用文本文件填充这些字段。下一过程中的步骤介绍了如何使用每个字段的说明来配置文本文件。该应用在您键入信息后不会保存信息，因此您可能需要创建一个文本文件以保留信息供将来使用。

使用文本文件配置预配工具

将文件命名为 nfcprovisioning.txt，并将其放置在设备 SD 卡上的 `/sdcard/` 文件夹中。然后，应用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>`

此行是 EMM 提供商应用的内网/互联网位置。在恢复出厂设置的设备通过 NFC 碰触连接到 Wi-Fi 后，设备必须能够访问此位置才能进行下载。URL 是一个常规 URL，无需特殊格式。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

此行是 EMM 提供商应用程序的校验和。此校验和用于验证下载是否成功。获取校验和的步骤将在本文后面讨论。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

此行是运行预配工具的设备所连接的 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，则此字段必须为空。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

如果 Wi-Fi 未受保护，则此字段必须为空。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

输入语言和国家/地区代码。语言代码是 ISO 639-1 定义的两位小写 ISO 语言代码（例如 en）。国家/地区代码是 ISO 3166-1 定义的两位大写 ISO 国家/地区代码（例如 US）。例如，输入 en_US 表示在美国使用的英语。如果您不输入任何代码，则国家/地区和语言将自动填充。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

设备运行所在的时区。输入 区域/位置的数据库名称。例如，输入 **America/Los_Angeles** 表示太平洋时间。如果您不输入名称，时区将自动填充。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

此数据不是必需的，因为该值已作为 Citrix Secure Hub 硬编码到应用程序中。此处提及仅为完整性考虑。

如果 Wi-Fi 使用 WPA2 保护，则完成的 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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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 Wi-Fi 未受保护，则完成的 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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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

Citrix Secure Hub 的校验和是一个常量值：`qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。要下载 Citrix Secure Hub 的 APK 文件，请使用以下 Google Play 商店链接：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

获取应用程序校验和

先决条件：

- Android SDK 构建工具中的 **apksigner** 工具
- OpenSSL 命令行

要获取任何应用程序的校验和，请按照以下步骤操作：

1. 从 Google Play 商店下载应用的 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 -- '+/=' '-_'
   ```

   该命令返回一个有效的校验和。
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":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-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"

   }

}
```

使用的库

配置工具在其源代码中使用了以下库：

- v7 `appcompat` 库、Design Support 库和 v7 palette support 库，由 Google 在 Apache 2.0 许可下提供

  有关信息，请参阅 Support Library Features Guide。

- Butter Knife，由 Jake Wharton 在 Apache 2.0 许可下提供

使用 QR 码注册设备

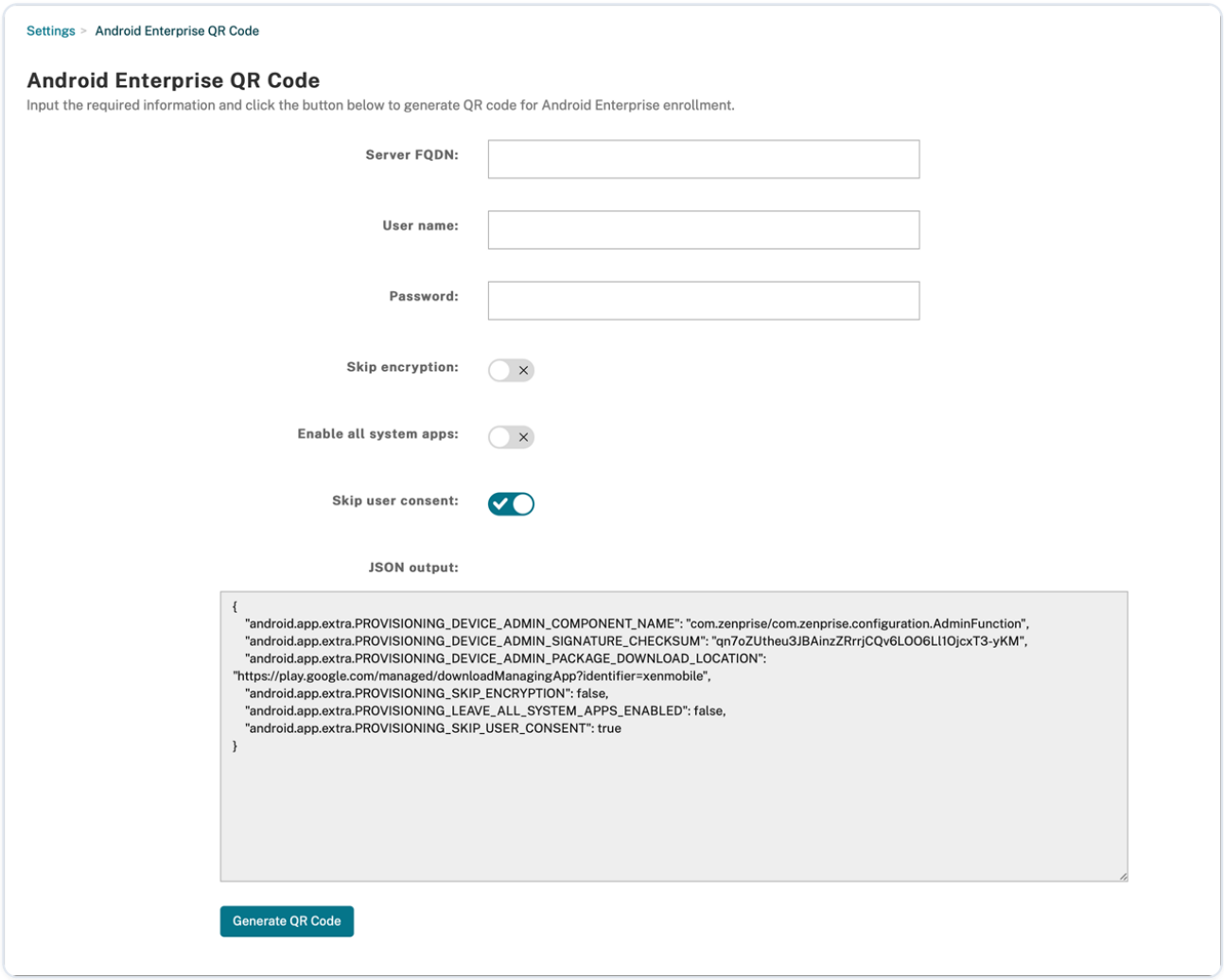
用户可以使用您为其生成的 QR 码注册完全托管的设备。

系统要求

运行 Android 7.0 或更高版本的 Android 设备。

创建 QR 码

您可以根据需要通过指定注册信息来生成 QR 码。生成 QR 码后，请将其本地保存。Citrix Endpoint Management 不会存储它。



1. 导航到 **设置 > Android Enterprise 二维码**。
2. 如有需要，请指定以下注册信息：

   - **服务器 FQDN：** 键入 Citrix Endpoint Management 服务器的 FQDN（例如，`example.cem.cloud.com`）。此字段是可选的。如果将其留空，用户在注册时必须填写此信息。
   - **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，建议将此字段留空。使用用户名和密码配置二维码对于注册自助服务终端设备很有用。如果将此字段留空，用户在注册时必须填写此信息。
   - **密码：** 键入与您输入的用户名关联的密码。如果将此字段留空，用户在注册时必须填写此信息。
   - **跳过加密：** 如果为 **开**，则设备在注册期间不会加密。默认值为 **关**。
   - **启用所有系统应用：** 如果为 **开**，则允许访问设备上的所有系统应用。默认值为 **关**。
   - **跳过用户同意：** 如果为 **关**，用户可以选择退出设备管理。默认值为 **关**。

   JSON 输出 框显示与您指定的信息对应的 JSON 内容。

3. 要添加更多注册信息，请编辑 **JSON 输出** 框中的 JSON 内容。
4. 单击 **生成二维码**。二维码将显示在 JSON 输出的右侧。
5. 右键单击二维码图像并保存。
6. 将图像发送给用户以进行设备注册。

恢复出厂设置的设备扫描此二维码以注册为完全托管设备。

注册设备

在新设备或恢复出厂设置的设备开机后：

1. 在欢迎屏幕上轻触屏幕六次，以启动二维码注册流程。
2. 出现提示时，连接到 Wi-Fi。二维码中 Citrix Secure Hub 的下载位置可通过此 Wi-Fi 网络访问。

   设备成功连接到 Wi-Fi 后，它会从 Google 下载一个二维码阅读器并启动摄像头。
3. 将摄像头对准二维码以扫描代码。

   Android 从二维码中的下载位置下载 Citrix Secure Hub，验证签名证书签名，安装 Citrix Secure Hub，并将其设置为设备所有者。

有关详细信息，请参阅此适用于 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

零接触注册允许您设置设备，使其在首次开机时自动配置为完全托管设备。

您的设备经销商会在 Android 零接触门户上为您创建一个帐户，这是一个在线工具，可让您将配置应用于设备。使用 Android 零接触门户，创建一项或多项零接触注册配置，并将这些配置应用于分配给您帐户的设备。当您的用户启动这些设备时，设备将自动注册到 Citrix Endpoint Management。分配给设备的配置定义了其自动注册过程。

系统要求

- 零接触注册支持始于 Android 9.0。

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 零接触合作伙伴列表，请参阅Android 网站。
- 由您的经销商创建的 Android Enterprise 零接触门户帐户。
- 您的经销商提供的 Android Enterprise 零接触门户帐户登录信息。

创建零接触配置

创建零接触配置时，请包含自定义 JSON 以指定配置详细信息。

使用此 JSON 配置设备以在您指定的 Citrix Endpoint Management 服务器上注册。在此示例中，将“URL”替换为您的服务器 URL。

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

  {

        "serverURL":"URL"

   }

}
```

您可以使用包含更多参数的可选 JSON 来进一步自定义配置。此示例指定了 Citrix 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。

```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

     {

        "serverURL":"URL",

        "xm_username":"username",

        "xm_password":"password"

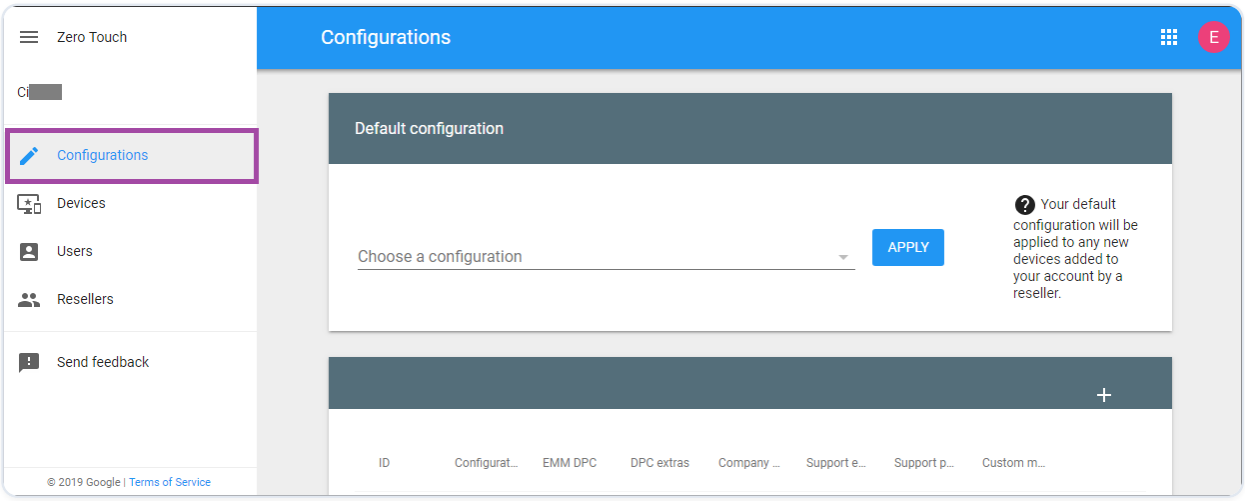
     }

       }
```

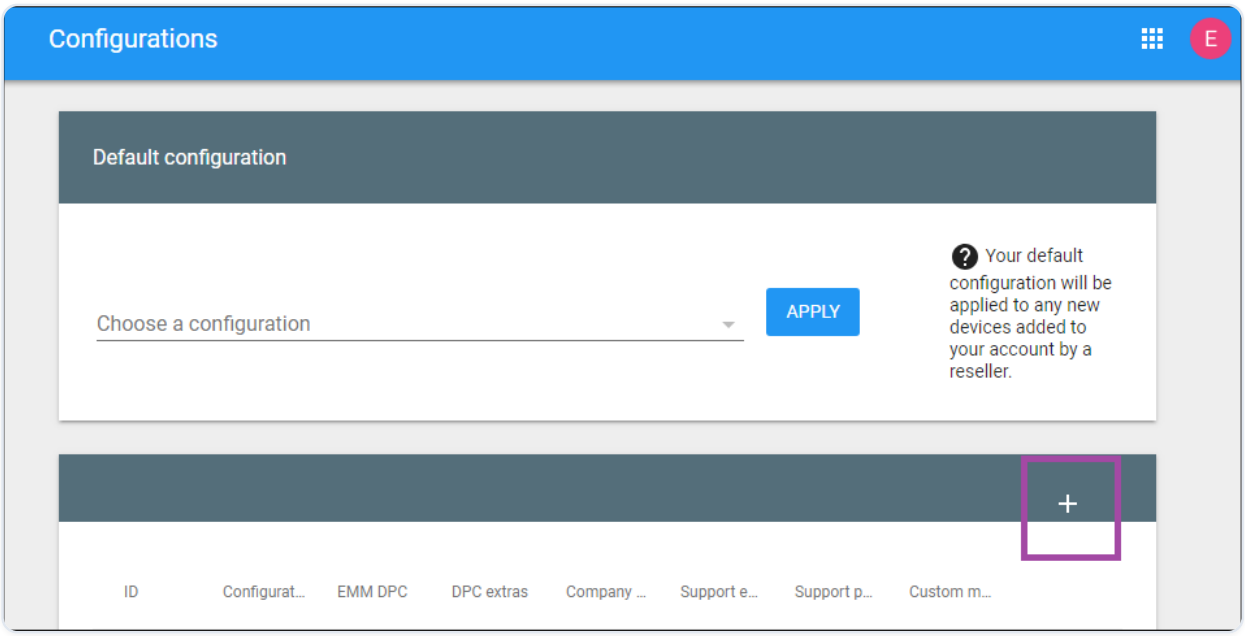
重要提示：

> 要在企业自有设备模式下将设备注册到工作配置文件中，请将 `{"desiredProvisioningMode": "managedProfile"}` 添加到 `PROVISIONING_ADMIN_EXTRAS_BUNDLE` 下的自定义 JSON 中。

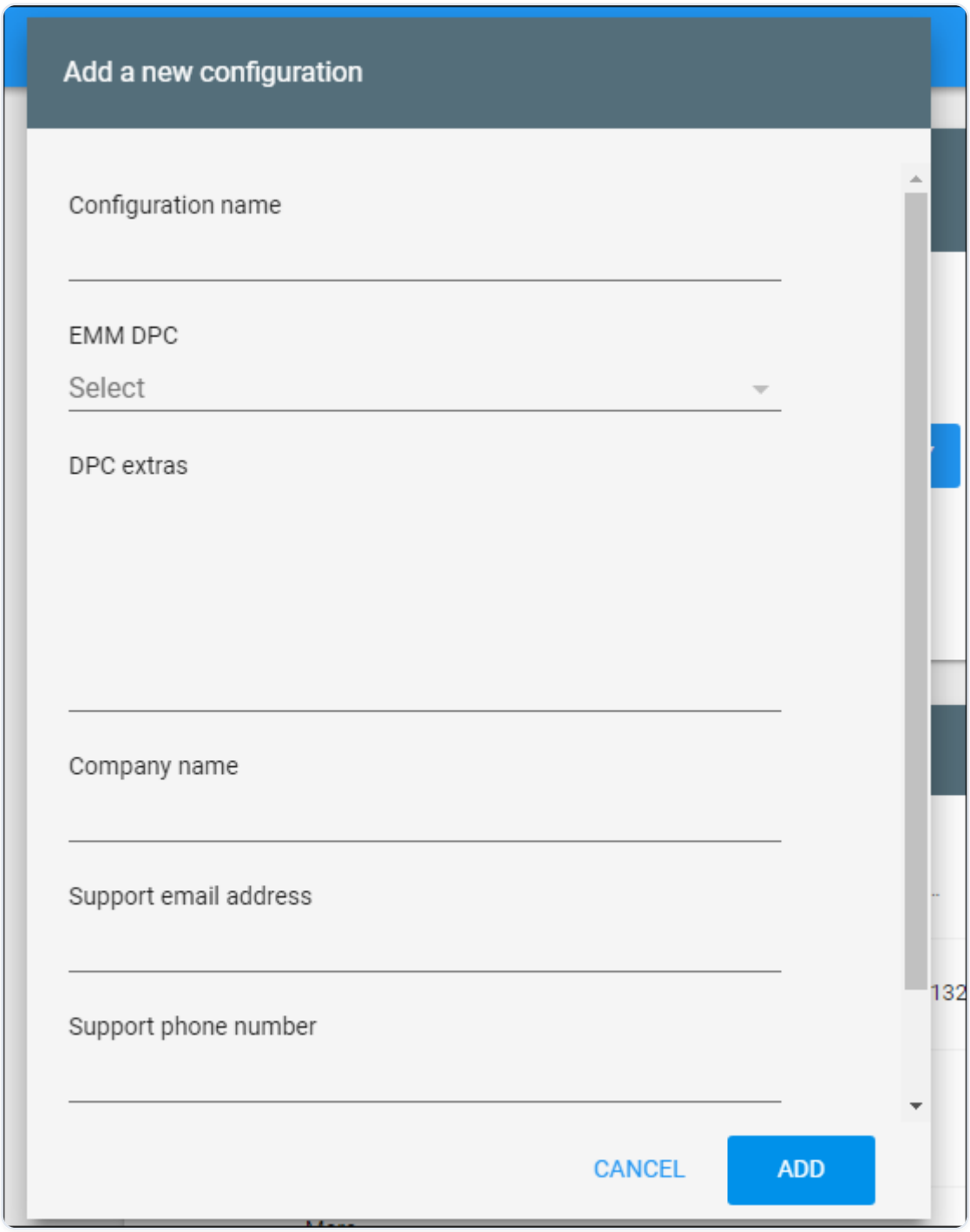
1. 访问 Android 零接触门户 https://partner.android.com/zerotouch。使用零接触设备经销商提供的帐户信息登录。
2. 单击 **Configuration**。



3. 单击配置表上方的 **+**。



4. 在出现的配置窗口中输入您的配置信息。



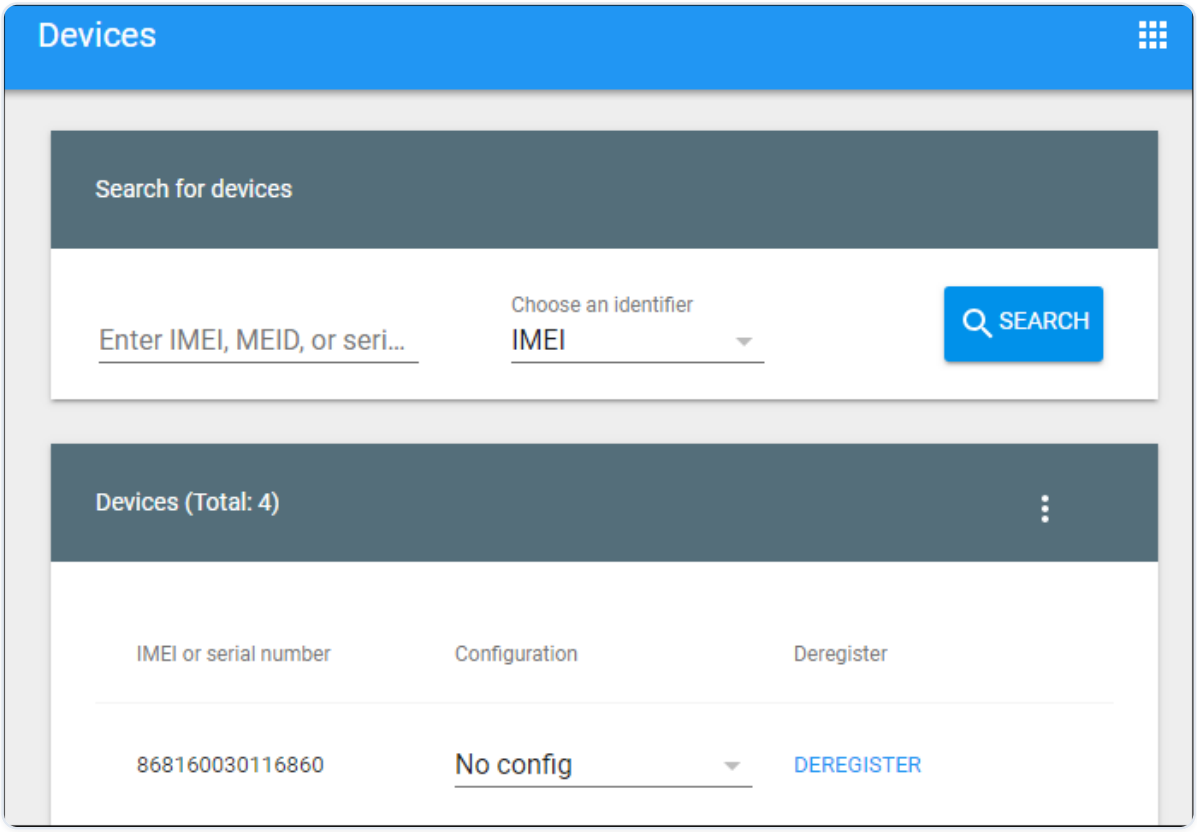
- **配置名称：** 键入您为此配置选择的名称。
- **EMM 设备策略控制器：** 选择 **Citrix Secure Hub**。
- **DPC 额外项：** 将您的自定义 JSON 文本粘贴到此字段中。
- **公司名称：** 键入您希望在设备预配期间显示在 Android Enterprise 零接触设备上的名称。
- **支持电子邮件地址：** 键入用户可以联系以获取帮助的电子邮件地址。此地址在设备预配之前显示在您的 Android Enterprise 零接触设备上。

- **支持电话号码：** 键入用户可以联系以获取帮助的电话号码。此电话号码在设备预配之前显示在您的 Android Enterprise 零接触设备上。
- **自定义消息：** （可选）添加一两句话，以帮助用户联系您，或向他们提供有关其设备状况的更多详细信息。此自定义消息在设备预配之前显示在您的 Android Enterprise 零接触设备上。

5. 单击 **添加**。
6. 要创建更多配置，请重复步骤 2 到 4。
7. 要将配置应用于设备：

   a. 在 Android 零接触门户中，单击**设备**。

   b. 在设备列表中找到该设备，然后选择要分配给它的配置。



   c. 单击**更新**。

您可以使用 CSV 文件将配置应用于许多设备。

有关如何将配置应用于许多设备的信息，请参阅面向 IT 管理员的零接触注册。此 Android Enterprise 主题包含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 设备是完全托管的设备，专门用于实现单一用例。您将这些设备限制为单个应用程序或一小组应用程序，这些应用程序是完成此用例所需任务的必需应用程序。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 完全托管设备中所述。预配专用设备在注册前需要更多设置。

要预配专用设备：

- 为 Citrix Endpoint Management 管理员添加注册配置文件，允许他们将专用设备注册到您的 Citrix Endpoint Management 部署中。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。
- （可选）将允许的应用程序设置为允许锁定任务模式。当应用程序处于锁定任务模式时，用户打开应用程序时，应用程序会固定到设备屏幕。不显示主页按钮，并且禁用返回按钮。用户通过应用程序中编程的操作（例如注销）退出应用程序。
- 将每个设备注册到您添加的注册配置文件中。

系统要求

- 专用设备的注册支持从 Android 6.0 开始。

允许应用并设置锁定任务模式

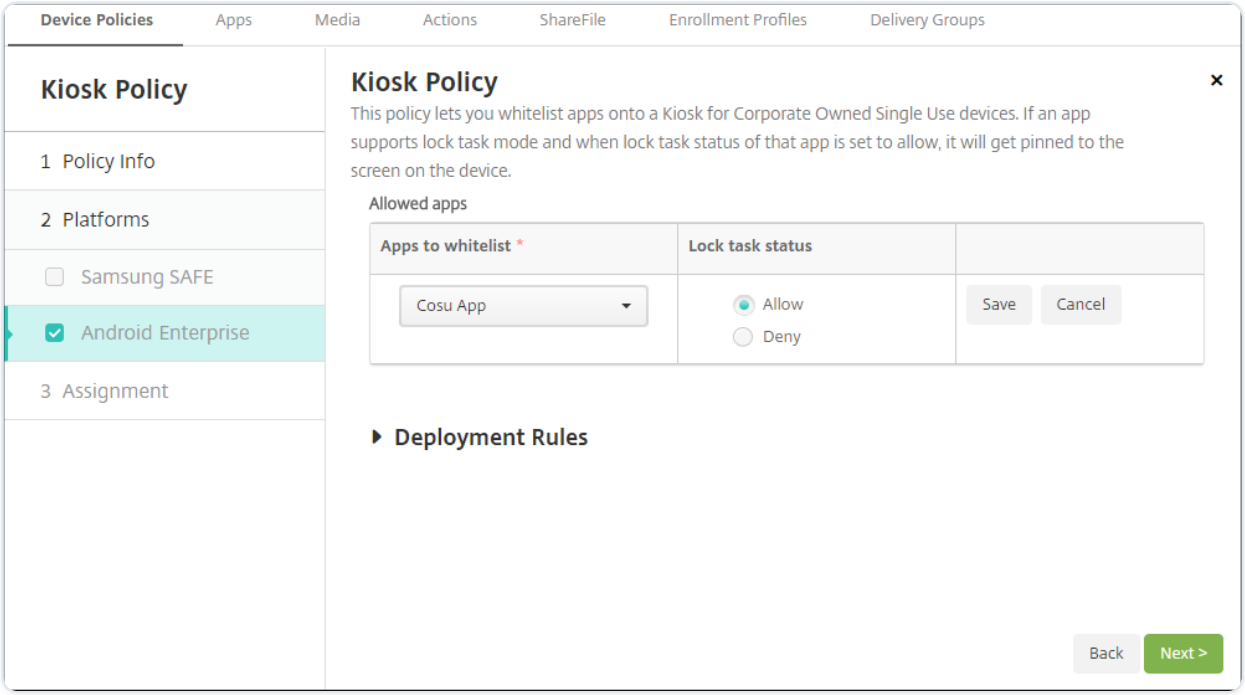
信息亭设备策略允许您允许应用并设置锁定任务模式。默认情况下，Citrix Secure Hub 和 Google Play 服务在允许列表中。

要添加信息亭策略：

1. 在 Citrix 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”下，单击“**信息亭**”。此时将显示“**信息亭策略**”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**”和可选的“**描述**”。
6. 单击“**下一步**”，然后单击“**添加**”。
7. 要允许某个应用并允许或拒绝该应用的锁定任务模式：

   从列表中选择要允许的应用。

选择“**允许**”以将应用设置为在用户启动应用时固定到设备屏幕。选择“**拒绝**”以将应用设置为不固定。默认值为“**允许**”。



8. 点击 **保存**。
9. 要允许另一个应用并允许或拒绝该应用的锁定任务模式，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在公司拥有的设备上具有工作配置文件的 Android Enterprise 全面管理设备

运行 Android 9.0-10.x 的设备注册为“具有工作配置文件的全面管理设备”。从 Android 11+ 开始，设备注册为“公司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。您的组织管理整个设备。您可以将一组策略应用于设备，并将另一组策略应用于工作配置文件。

在 Citrix Endpoint Management 控制台中，具有工作配置文件的全面管理设备显示以下术语：

- 设备所有权为“公司”所有。
- 设备 Android Enterprise 安装类型为“公司所有者个人启用”。

系统要求

- 对注册具有工作配置文件的全面管理设备的支持始于 Android 9.0。

注册设备

新设备和恢复出厂设置的设备注册为具有工作配置文件的全面管理设备。这些设备使用为其他全面管理设备所用的任何注册方法，如预配 Android Enterprise 全面管理设备中所述。运行 Android 11 的设备可以使用该部分中描述的二维码或零接触注册方法，在公司拥有的设备模式下注册工作配置文件。

重要提示：

使用二维码方法在公司拥有的设备模式下注册工作配置文件中的设备时，请在 `serverURL` 字段上方将以下内容添加到 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"
    }
```

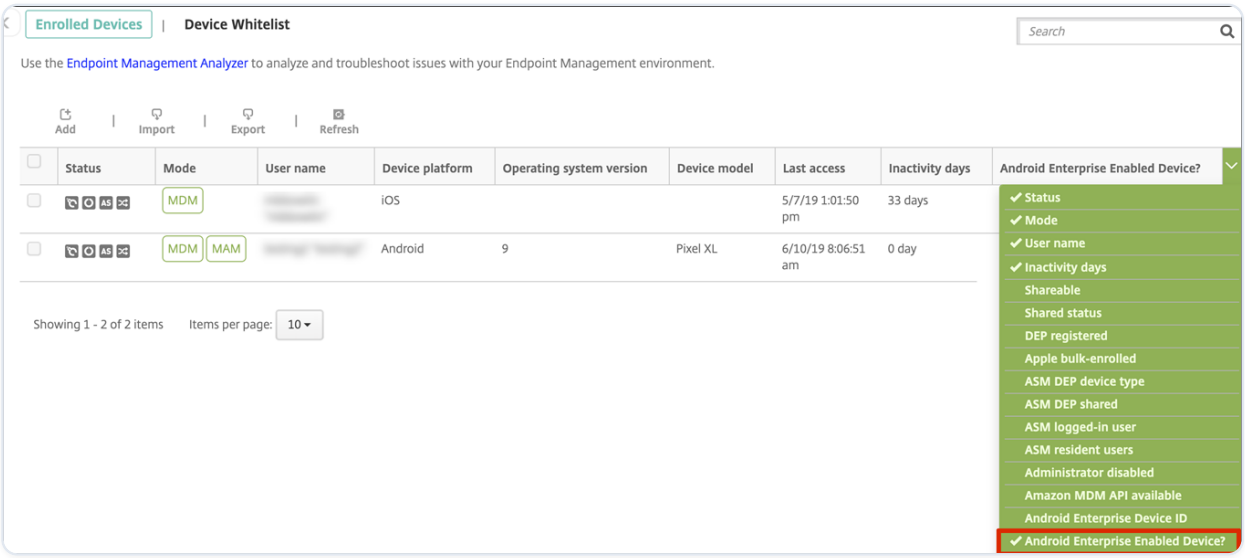
未恢复出厂设置或非新设备将注册为工作配置文件设备，如预配 Android Enterprise 工作配置文件设备中所述。

在 Citrix Endpoint Management 控制台中查看 Android Enterprise 设备

要查看 Android Enterprise 全面管理设备、专用设备以及具有工作配置文件的全面管理设备：

1. 在 Citrix Endpoint Management 控制台中，转到 **管理 > 设备**。

2. 通过单击表格右边缘的菜单，添加 **Android Enterprise 已启用设备？** 列。



3. 要查看可用的安全操作，请选择一个完全托管的设备，然后单击 **安全**。当设备完全托管时，**完全擦除** 操作可用，但 **选择性擦除** 不可用。这种差异是因为设备只允许来自托管 Google Play 商店的应用程序。用户无法从公共商店安装应用程序。您的组织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概述，请参阅 适用于 Android Enterprise 的支持的设备策略和 MDX 策略。

关于策略须知：

- **设备限制：** 数十种设备限制允许您控制以下功能：
  - 设备摄像头的使用

    - 在工作和个人配置文件之间使用复制和粘贴

- **每应用 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

此表列出了适用于 Android Enterprise 设备的所有设备策略。

> **重要提示：**
>
> 对于注册到 Android Enterprise 并使用 MDX 应用程序的设备：您可以通过 MDX 和 Android Enterprise 控制某些设置。对 MDX 使用限制最少的策略设置，并通过 Android Enterprise 控制策略。

应用权限	应用清单	应用卸载
自动更新托管应用	连接计划	凭据
自定义 XML	Citrix 端点管理选项	文件
锁屏管理	信息亭	启动器配置
位置	托管配置	网络
OS 更新	密码	限制

带工作资料的完全托管设备（COPE 设备）的设备策略

对于带工作资料的完全托管设备，您可以使用某些设备策略将单独的设置应用于整个设备和工作资料。您可以使用其他设备策略仅将设置应用于整个设备，或仅应用于带工作资料的完全托管设备的工作资料。对于在企业拥有设备模式下注册工作资料的设备，策略仅应用于工作资料，而不应用于整个设备。

策略	适用于
应用程序权限	工作资料
应用程序清单	工作资料

策略	适用于
应用程序卸载	工作资料
自动更新托管应用程序	工作资料
连接计划	工作资料
凭据(/zh-cn/citrix-endpoint-management/policies/credentials-policy.html#android-enterprise-settings)	工作配置文件
自定义 XML(/zh-cn/citrix-endpoint-management/policies/custom-xml-policy.html)	不适用
Citrix 端点管理选项	工作配置文件
文件(/zh-cn/citrix-endpoint-management/policies/files-policy.html)	工作配置文件
键盘锁管理(/zh-cn/citrix-endpoint-management/policies/keyguard-management-policy.html)	设备和工作配置文件
自助服务终端(/zh-cn/citrix-endpoint-management/policies/kiosk-policy.html#android-enterprise-settings)	不适用
启动器配置(/zh-cn/citrix-endpoint-management/policies/launcher-configuration-policy.html)	设备和工作配置文件
位置(/zh-cn/citrix-endpoint-management/policies/location-policy.html#android-enterprise-settings)	设备（仅限位置模式）
托管配置(/zh-cn/citrix-endpoint-management/policies/managed-configurations-policy.html)	工作配置文件
网络	设备
操作系统更新	不适用
密码	设备和工作配置文件

策略	适用于
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
定位	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

安全操作注意事项

- 定位安全操作会失败，除非位置设备策略将设备的定位模式设置为**高精度**或**省电**。请参阅位置设备策略。
- 在运行低于 Android 9.0 版本的企业配置文件设备上：
  - 不支持锁定和重置密码操作。
- 在运行 Android 9.0 或更高版本的企业配置文件设备上：
  - 发送的密码会锁定企业配置文件。设备本身不会被锁定。
  - 如果工作配置文件上未设置密码：

    - 如果未发送密码，或者发送的密码不符合密码要求：设备将被锁定。
  - 如果工作配置文件上设置了密码：
    - 如果未发送密码，或者发送的密码不符合密码要求：工作配置文件将被锁定，但设备本身不会被锁定。

取消注册 Android Enterprise 企业

如果您不再希望使用您的 Android Enterprise 企业，可以取消注册该企业。

> **警告：**
>
> 取消注册企业后，通过该企业注册的设备上的 Android Enterprise 应用程序将重置为默认状态。Google 不再管理这些设备。如果您注册新的 Android Enterprise 企业，则必须从托管的 Google Play 批准新组织的应用程序。然后，您可以从 Citrix Endpoint Management 控制台更新这些应用程序。

> Android Enterprise 企业取消注册后：

- 通过企业注册的设备和用户，其 Android Enterprise 应用程序将重置为默认状态。以前应用的托管配置策略不再影响操作。
- Citrix Endpoint Management 管理通过企业注册的设备。从 Google 的角度来看，这些设备是未受管理的。您无法添加新的 Android Enterprise 应用程序。您无法应用托管配置策略。您可以对这些设备应用其他策略，例如计划、密码和限制。
- 如果您尝试在 Android Enterprise 中注册设备，它们将注册为 Android 设备，而不是 Android Enterprise 设备。

使用 Citrix Endpoint Management 服务器控制台和 Citrix Endpoint Management 工具取消注册 Android Enterprise 企业。

执行此任务时，Citrix Endpoint Management 会打开一个“工具”弹出窗口。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）要求您禁用弹出窗口阻止功能，并将 Citrix 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：

1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。“设置”页面随即显示。
2. 在“设置”页面上，单击“**Android Enterprise**”。

3. 单击“**取消注册**”。

   取消注册选项(/en-us/citrix-endpoint-management/media/android-enterprise-setup-unenroll.png)

分发 Android Enterprise 应用程序

Citrix 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 Android Enterprise 应用程序。

- **托管应用商店应用程序：** 这些应用程序包括托管 Google Play 商店中提供的免费应用程序。例如，GoToMeeting。
- **MDX：** 使用 MAM SDK 准备或使用 MDX Toolkit 封装的应用程序。这些应用程序包含 MDX 策略。您可以从内部源和公共商店获取 MDX 应用程序。将 Citrix 移动生产力应用程序部署为 MDX 应用程序。
- **企业：** 您开发或从其他来源获取的私有应用程序。您通过托管 Google Play 商店向用户提供这些应用程序。托管 Google Play 商店是 Google 企业应用程序商店。
- **启用 MDX 的私有应用程序：** 使用 MAM SDK 准备或使用 MDX Toolkit 封装的企业应用程序。

您可以通过两种不同的方式添加企业应用程序和启用 MDX 的私有应用程序。

- 将应用程序作为企业应用程序添加到 Citrix Endpoint Management 控制台，如本文中的企业应用程序和启用 MDX 的私有应用程序部分所述。
- 使用您的 Google 开发者帐户将应用程序直接发布到托管 Google Play 商店。然后将应用程序作为托管应用商店应用程序添加到 Citrix 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 Citrix 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您的应用程序。Citrix 建议使用其中一种方法添加您的应用程序。

如果您需要从托管 Google Play 商店中移除自行管理的应用程序，请向 Google 提交工单。开发者可以禁用但不能删除托管 Google Play 商店中的应用程序。

以下部分提供了有关 Android Enterprise 应用程序配置的更深入信息。有关分发应用程序的信息，请参阅添加应用程序。该文章包括：

- 添加 Web 和 SaaS 应用程序或 Web 链接的通用工作流程
- 企业和公共商店应用程序所需的应用程序工作流程
- 如何从 Citrix 企业应用程序内容分发网络 (CDN) 交付企业应用程序

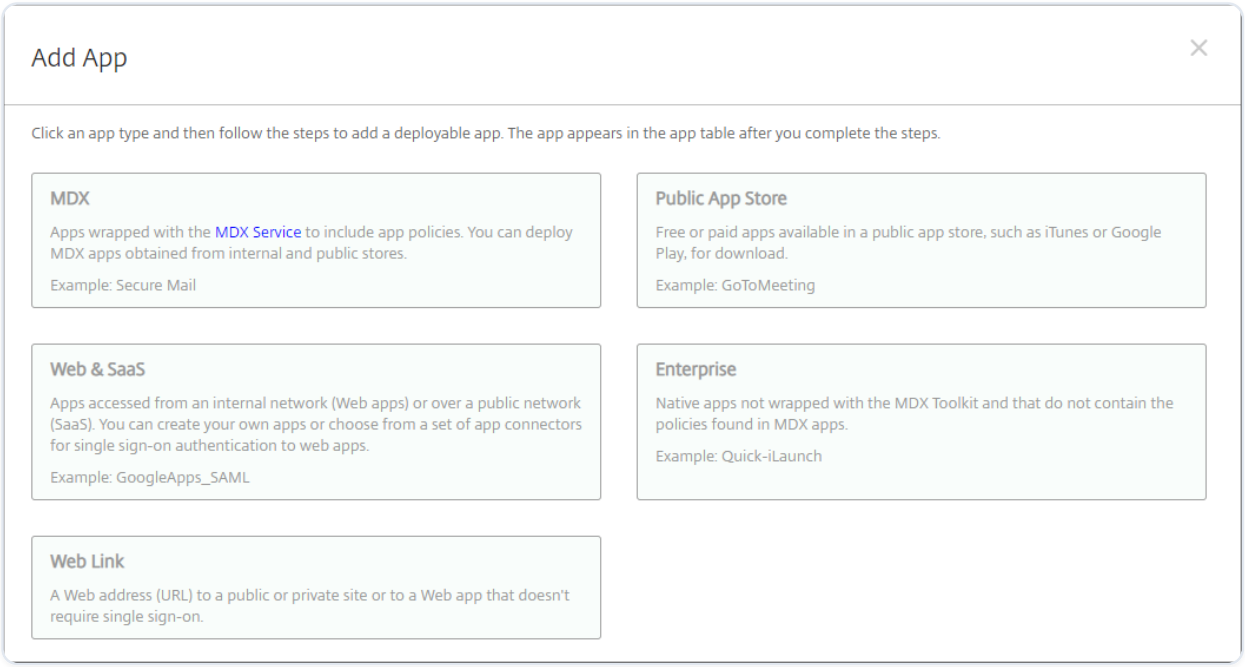
托管应用商店应用

您可以将托管 Google Play 商店中提供的免费应用添加到 Citrix Endpoint Management。

> **注意：**
>
> 要使 Google Play 商店中的所有应用都可以通过托管 Google Play 访问，请使用**访问托管 Google Play 商店中的所有应用**服务器属性。请参阅服务器属性。将此属性设置为 **true** 允许所有 Android Enterprise 用户访问公共 Google Play 商店应用。然后，您可以使用限制设备策略来控制对这些应用的访问。

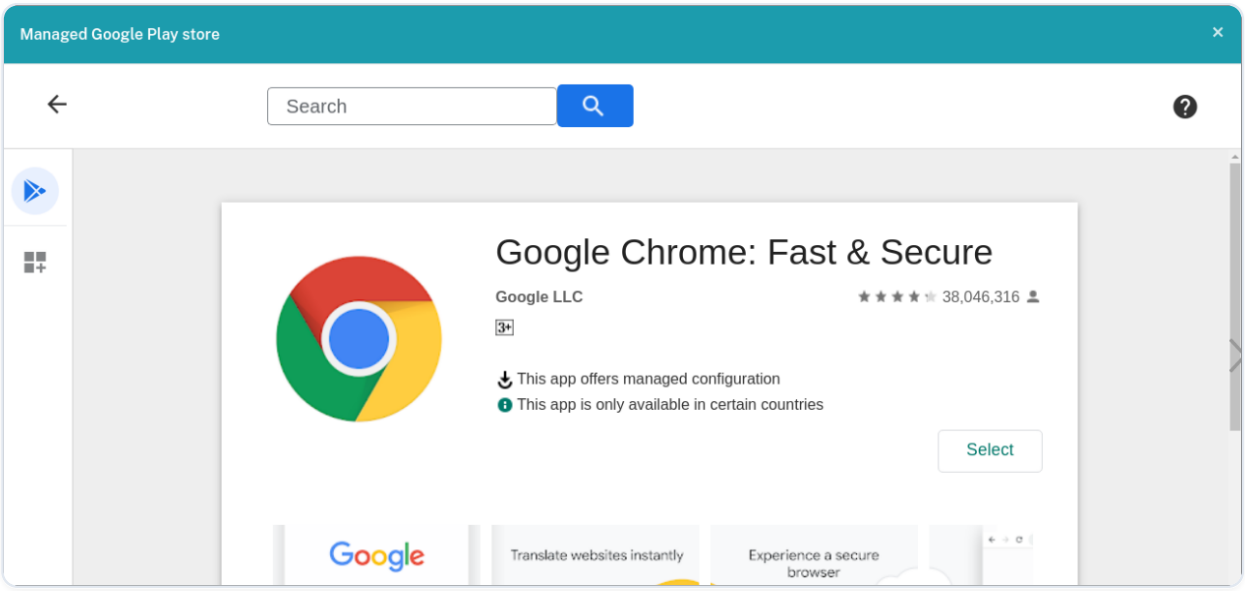
步骤 1：添加和配置应用

1. 在 Citrix Endpoint Management 控制台中，导航到**配置 > 应用**。单击**添加**。
2. 单击**公共应用商店**。



3. 在**应用信息**窗格中，键入以下信息：
   - **名称：键入应用的描述性名称。该名称显示在应用**表中的**应用名称**下。
   - **描述：**键入应用的可选描述。
4. 选择 **Android Enterprise** 作为平台。
5. 在搜索框中键入应用名称或软件包 ID，然后单击**搜索**。您可以在 Google Play 商店中找到软件包 ID。该 ID 位于应用的 URL 中。例如，`com.Slack` 是 `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US` 中的软件包 ID。

6. 将显示与搜索条件匹配的应用。单击所需应用，然后单击**选择**。



7. 再次单击**选择**。
8. 点击应用程序图标，然后配置应用程序的**名称**和**描述**。

   Android Enterprise 应用程序配置(/en-us/citrix-endpoint-management/media/android-enterprise-public-app-configure.png)

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**所需应用程序**框中。 标记为必需的应用程序(/en-us/citrix-endpoint-management/media/required-app-delivery-group.png)
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 Citrix 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。有关适用于每种设备平台类型的应用程序策略的信息，请参阅：

- MAM SDK 概述
- MDX 策略一览

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，请下载公共商店 MDX 文件：转到`<https://www.citrix.com/downloads>`。导航到**Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**。

   对于其他类型的 MDX 应用程序，请获取 MDX 文件。

2. 在 Citrix Endpoint Management 控制台中，单击**配置 > 应用程序**。单击**添加**。将显示**添加应用程序**对话框。

   应用程序配置屏幕(/en-us/citrix-endpoint-management/media/configure-apps-add.png)

3. 单击 **MDX**。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。

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。

   - 如果附加的应用程序需要托管 Google Play 商店的批准，UI 会通知您。要在不离开 Citrix Endpoint Management 控制台的情况下批准应用程序，请单击**是**。

     添加 MDX 应用程序(/en-us/citrix-endpoint-management/media/mdx-app-not-approved.png)

     托管 Google Play 商店打开后，按照说明批准并保存应用程序。

     批准 MDX 应用程序(/en-us/citrix-endpoint-management/media/mdx-approve-app.png)

     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。
   - **程序包 ID：** 键入从托管 Google Play 商店获取的应用程序的程序包 ID。
   - **最低操作系统版本：**（可选）键入设备可运行以使用应用程序的最旧操作系统版本。
   - **最高操作系统版本：**（可选）键入设备必须运行以使用应用程序的最新操作系统。
   - **排除的设备：**（可选）键入无法运行应用程序的设备的制造商或型号。

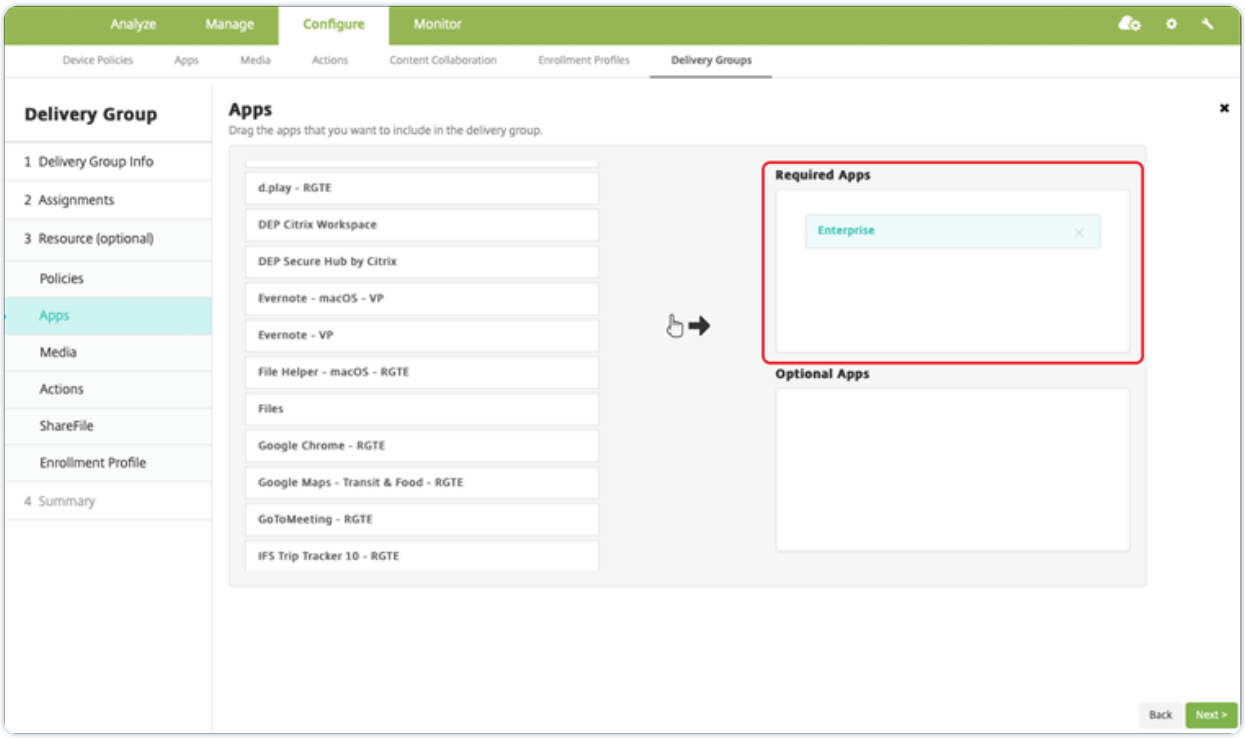
7. 配置 **MDX 策略**。MDX 策略因平台而异，包括身份验证、设备安全和应用程序限制等策略区域的选项。在控制台中，每个策略都有一个描述该策略的工具提示。有关适用于每种设备平台类型的应用程序策略的信息，请参阅：

   - MAM SDK 概述
   - MDX 策略一览

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**部分中，将所需的应用程序拖动到**所需应用程序**框中。



3. 在**摘要**页面上，单击**保存**。
4. 在**交付组**页面上，选择交付组并单击**部署**。

企业应用

企业应用是指未使用 MAM SDK 或 MDX Toolkit 准备的私有应用。您可以自行开发这些应用，也可以直接从其他来源获取。要添加企业应用，您需要与该应用关联的 APK 文件。请务必遵循 Google 的私有应用最佳实践。

观看此视频了解更多信息：

步骤 1：添加和配置应用

通过以下两种方式之一添加应用：

- 将应用直接发布到托管 Google Play 商店，并将其作为托管 Play 商店应用添加到 Citrix Endpoint Management 控制台。请按照 Google 文档中有关如何发布私有应用的说明进行操作，然后按照托管应用商店应用部分中的步骤进行操作。
- 将应用作为企业应用添加到 Citrix Endpoint Management 控制台。执行以下步骤：

1. 在 Citrix Endpoint Management 控制台中，单击**配置 > 应用**。单击**添加**。将显示**添加应用**对话框。

   (/en-us/citrix-endpoint-management/media/configure-apps-add.png)

2. 单击**企业**。在**应用信息**窗格中，键入以下信息：

   - **名称：**键入应用的描述性名称。此名称将列在“应用”表中的“应用名称”下。
   - **描述：**键入应用的可选描述。

3. 选择 **Android Enterprise** 作为平台。
4. “**上传**”按钮将打开托管式 Google Play 商店。您无需注册开发者帐户即可发布私有应用。单击右下角的“**加号**”图标以继续。

   上传私有应用(/en-us/citrix-endpoint-management/media/upload-enterprise-app.png)

   a. 输入应用的名称并上传 .apk 文件。完成后，单击“**创建**”。您的私有应用可能需要长达 10 分钟才能发布。

      添加 apk 文件(/en-us/citrix-endpoint-management/media/add-apk-file.png)

   b. 输入电子邮件地址以获取有关应用的更新。

      添加电子邮件地址(/en-us/citrix-endpoint-management/media/add-email-address.png)

   c. 应用发布后，单击私有应用的图标。如果要添加应用说明、更改应用图标以及执行其他操作，请单击“**进行高级编辑**”。否则，单击“**选择**”以打开应用信息页面。

      发布企业应用(/en-us/citrix-endpoint-management/media/publish-enterprise-app.png)

5. 单击“**下一步**”。将显示该平台的应用信息页面。
6. 配置平台类型的设置，例如：

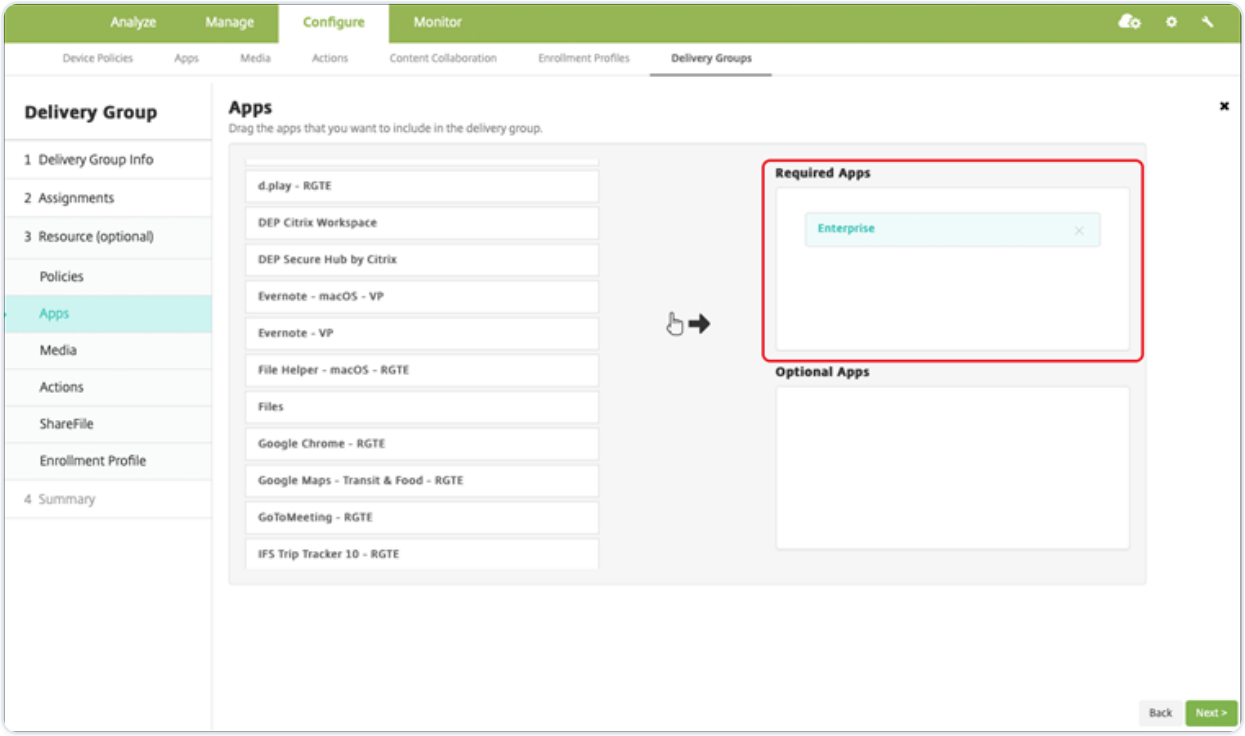
   - **文件名：**（可选）为应用键入新名称。

- **应用说明：**（可选）为应用键入新说明。
- **应用版本：**您无法更改此字段。
- **程序包 ID：**您的应用的唯一标识符。
- **最低操作系统版本：**（可选）键入设备可运行以使用该应用的最旧操作系统版本。
- **最高操作系统版本：**（可选）键入设备必须运行的最新操作系统才能使用该应用程序。
- **排除的设备：**（可选）键入无法运行该应用程序的设备制造商或型号。

7. 配置部署规则和商店配置。
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**Configure > Delivery Groups**（配置 > 交付组），然后选择您配置的交付组。单击**Edit**（编辑）。
2. 在**Apps**（应用程序）部分中，将所需的应用程序拖动到**Required Apps**（所需应用程序）框中。



3. 在**Summary**（摘要）页面上，单击**Save**（保存）。
4. 在**Delivery Groups**（交付组）页面上，选择交付组，然后单击**Deploy**（部署）。

启用 MDX 的私有应用程序

要将 Android Enterprise 应用程序添加为启用 MDX 的企业应用程序，请执行以下操作：

1. 创建私有 Android Enterprise 应用程序并启用该应用程序的 MDX 功能。
2. 将应用程序添加到 Citrix Endpoint Management 控制台。
   - 在托管的 Google Play 商店中托管和发布应用程序。
   - 将应用作为企业应用添加到 Citrix Endpoint Management 控制台。
3. 将 MDX 文件添加到 Citrix Endpoint Management。

如果您决定通过 Google Play 商店托管和发布应用，请不要选择 Google 证书签名。使用用于启用 MDX 应用的同一证书对应用进行签名。有关发布应用的详细信息，请参阅 Google 文档中的发布应用和为应用签名。MAM SDK 不会打包应用，因此除了用于开发应用的证书之外，它不需要其他证书。

有关通过 Google Play 管理中心发布专用应用的详细信息，请参阅 Google 文档中有关如何从 Play 管理中心发布专用应用的内容。

要通过 Citrix Endpoint Management 发布应用，请参阅以下各节。

准备 Android Enterprise 应用

创建 Android Enterprise 应用时，请务必遵循 Google 的专用应用最佳实践。

创建 Android Enterprise 应用后，将 MAM SDK 与应用集成，或使用 MDX Toolkit 打包应用。然后，将生成的文件添加到 XenMobile。

您可以通过上传更新的 .apk 文件来更新应用。以下步骤介绍了使用 MDX Toolkit 进行应用打包。

1. 创建您的 Android Enterprise 应用并生成签名的 .apk 文件。
2. 以下示例文件包含所有已知策略，其中某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>

        <DisableSms>false</DisableSms>

        <DisableScreenCapture>false</DisableScreenCapture>

        <DisableSensor>false</DisableSensor>

        <DisableNFC>false</DisableNFC>

        <BlockLogs>false</BlockLogs>

        <DisablePrinting>false</DisablePrinting>

        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
MvpnNetworkAccess>

        <MvpnSessionRequired>False</MvpnSessionRequired>

        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>

        <DisableLocalhostConnections>false</
DisableLocalhostConnections>

        <CertificateLabel/>

        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>

        <DefaultLoggerLevel>15</DefaultLoggerLevel>

        <MaxLogFiles>2</MaxLogFiles>
```

```
        <MaxLogFileSize>2</MaxLogFileSize>

        <RedirectSystemLogs>false</RedirectSystemLogs>

        <EncryptLogs>false</EncryptLogs>

        <GeofenceLongitude>0</GeofenceLongitude>

        <GeofenceLatitude>0</GeofenceLatitude>

        <GeofenceRadius>0</GeofenceRadius>

        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>

        <Authentication>OfflineAccessOnly</Authentication>

        <ReauthenticationPeriod>480</ReauthenticationPeriod>

        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>

    </Policies>

</MobileAppPolicies>
```

3. 使用 MDX Toolkit 打包应用。有关使用 MDX Toolkit 的信息，请参阅打包 Android 移动应用。

   将 **apptype** 参数设置为 **Premium**。在接下来描述的命令中使用上一步中的 XML 文件。

   如果您知道应用的商店 URL，请将 **storeURL** 参数设置为该商店 URL。发布应用后，用户将从商店 URL 下载应用。

   以下是用于打包名为 SampleAEapp 的应用的 MDX Toolkit 命令示例：

```
```

 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en
-Duser.variant

 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap

 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
```
```

```
 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx

 -MinPlatform 5.0

 -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>

```

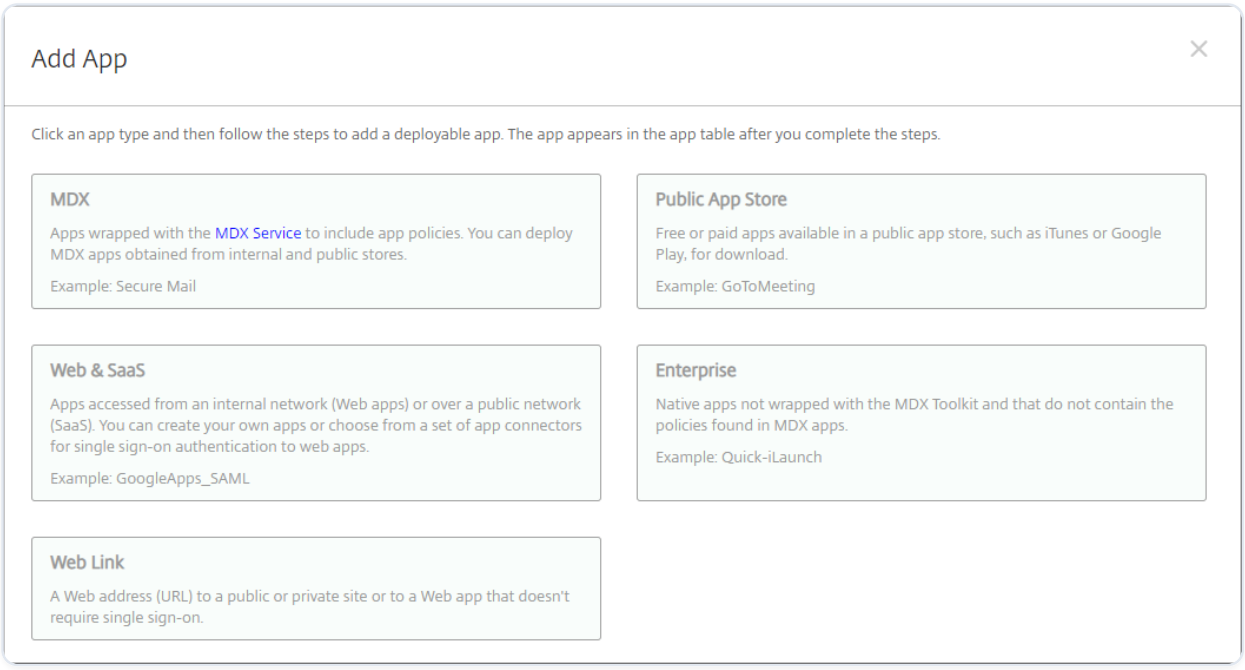
包装应用程序会生成一个已包装的 .apk 文件和一个 .mdx 文件。

添加已包装的 .apk 文件

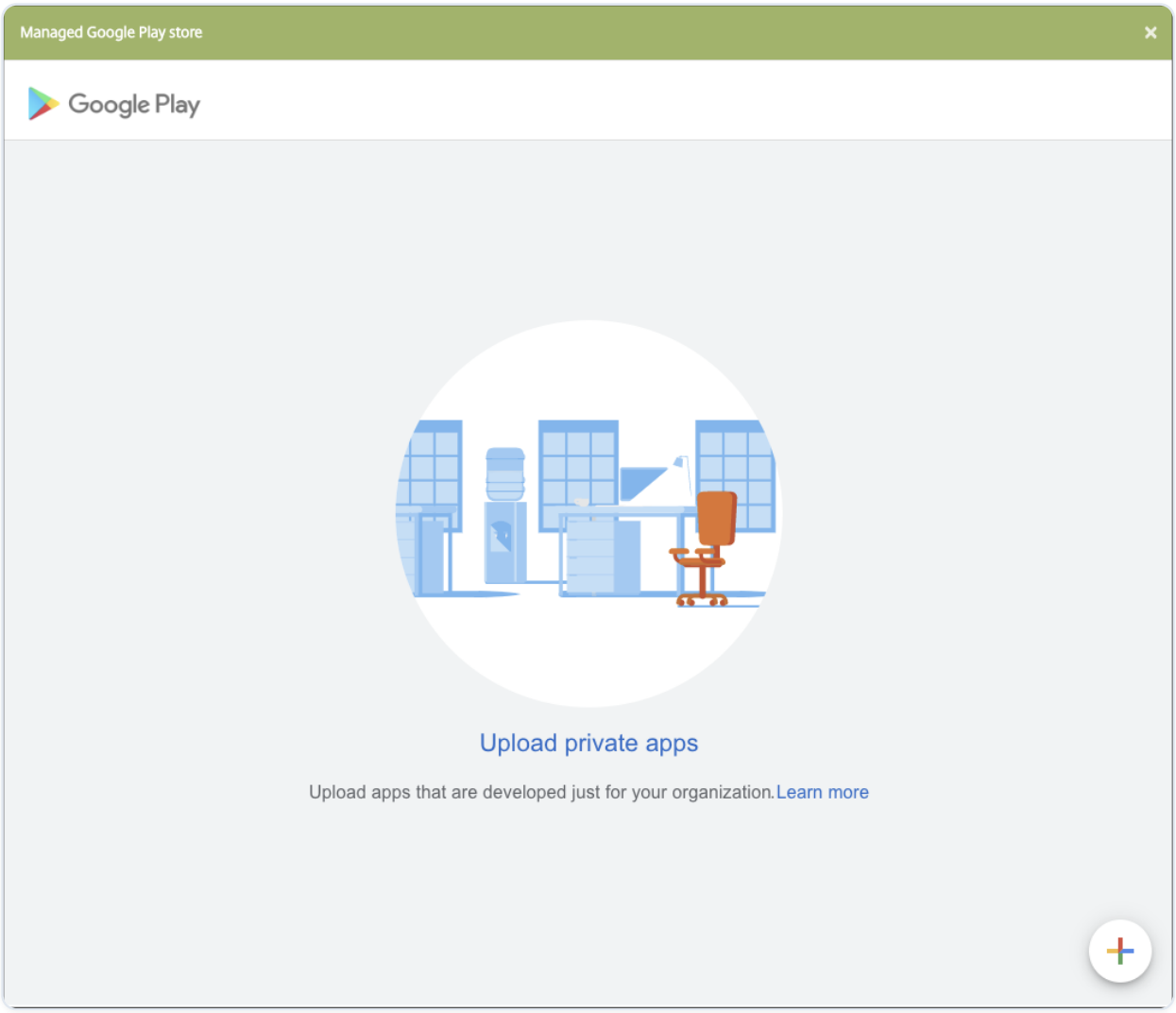
通过以下两种方式之一添加应用程序：

- 将应用程序直接发布到托管 Google Play 商店，并将其作为托管 Play 商店应用程序添加到 Citrix Endpoint Management 控制台。按照 Google 文档中的说明发布专用应用程序，然后按照托管应用商店应用程序部分中的步骤操作。
- 将应用程序作为企业应用程序添加到 Citrix Endpoint Management 控制台。执行以下步骤：

1. 在 Citrix 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。此名称将列在“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。
4. 选择 **Android Enterprise** 作为平台。
5. **上载**按钮将打开托管 Google Play 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**。您的专用应用程序可能需要长达 10 分钟才能发布。

   添加一个 apk 文件(/en-us/citrix-endpoint-management/media/add-apk-file.png)

b. 输入电子邮件地址以获取有关您的应用程序的更新。

   添加电子邮件地址(/en-us/citrix-endpoint-management/media/add-email-address.png)

c. 应用程序发布后，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。

   发布企业应用程序(/en-us/citrix-endpoint-management/media/publish-enterprise-app.png)

6. 单击**下一步**。将显示该平台的应用程序信息页面。
7. 配置平台类型的设置，例如：

   - **文件名：** （可选）为应用程序键入新名称。
   - **应用程序描述：** （可选）为应用程序键入新描述。
   - **应用程序版本：** 您无法更改此字段。

- **程序包 ID：** 应用程序的唯一标识符。
- **最低操作系统版本：** （可选）键入设备可运行的、用于使用此应用程序的最旧操作系统版本。
- **最高操作系统版本：** （可选）键入设备必须运行的、用于使用此应用程序的最新操作系统版本。
- **排除的设备：** （可选）键入无法运行此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**”页面上，单击“**下一步**”。“**审批**”页面出现。

   要使用工作流在允许用户访问应用程序之前要求审批，请参阅应用工作流。如果不需要审批工作流，可以跳到步骤 13。
10. 单击“**下一步**”。
11. “**交付组分配**”页面出现。此页面上无需执行任何操作。添加 .mdx 文件时，将为此应用程序配置交付组和部署计划。单击“**保存**”。

可选：添加或更改商店 URL

如果在打包应用程序时不知道商店 URL，请立即添加商店 URL。

1. 在托管的 Google Play 商店中查看应用程序。选择应用程序时，商店 URL 会显示在浏览器地址栏中。从 URL 形式复制应用程序的包名称。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。请务必将 `work` 更改为 `store`。
2. 使用 MDX Toolkit 将商店 URL 添加到 .mdx 文件：

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \

setinfo \

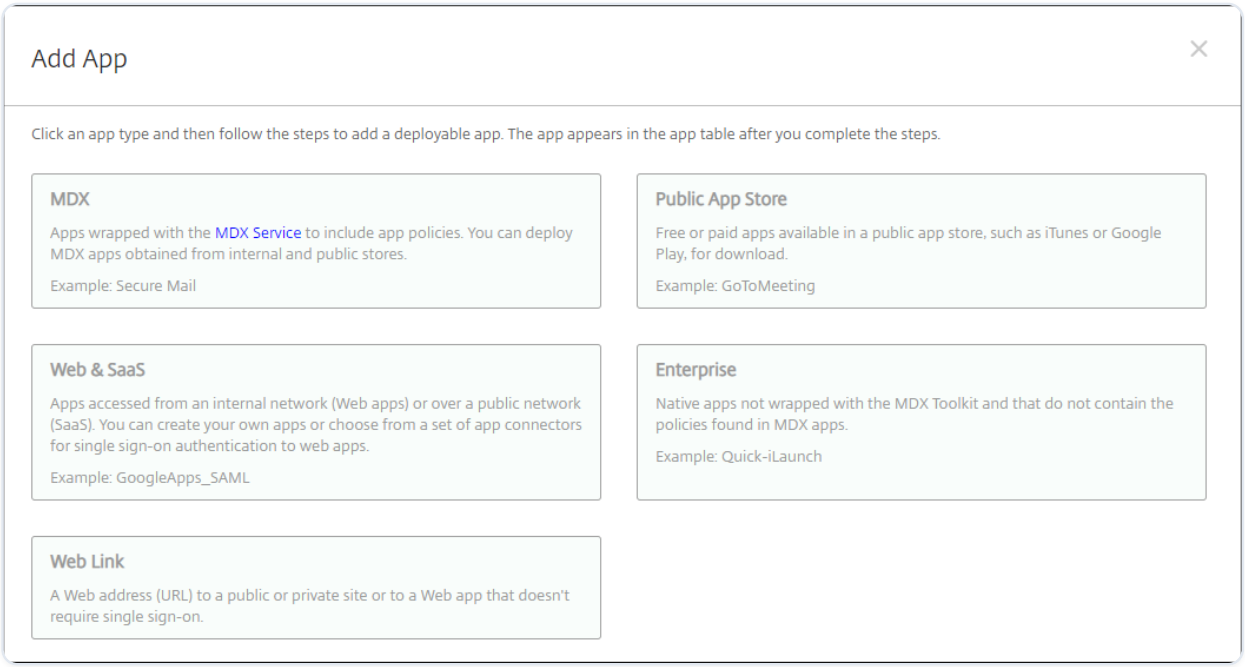
-in ~/Desktop/SampleApps/Sample.mdx \

-out ~/Desktop/SampleApps/wrapped/Sample.mdx \

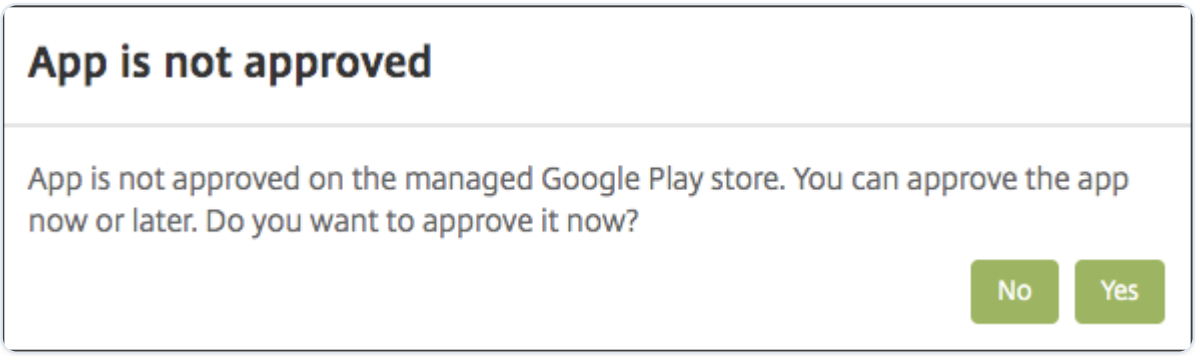
-storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"
```

添加 .mdx 文件

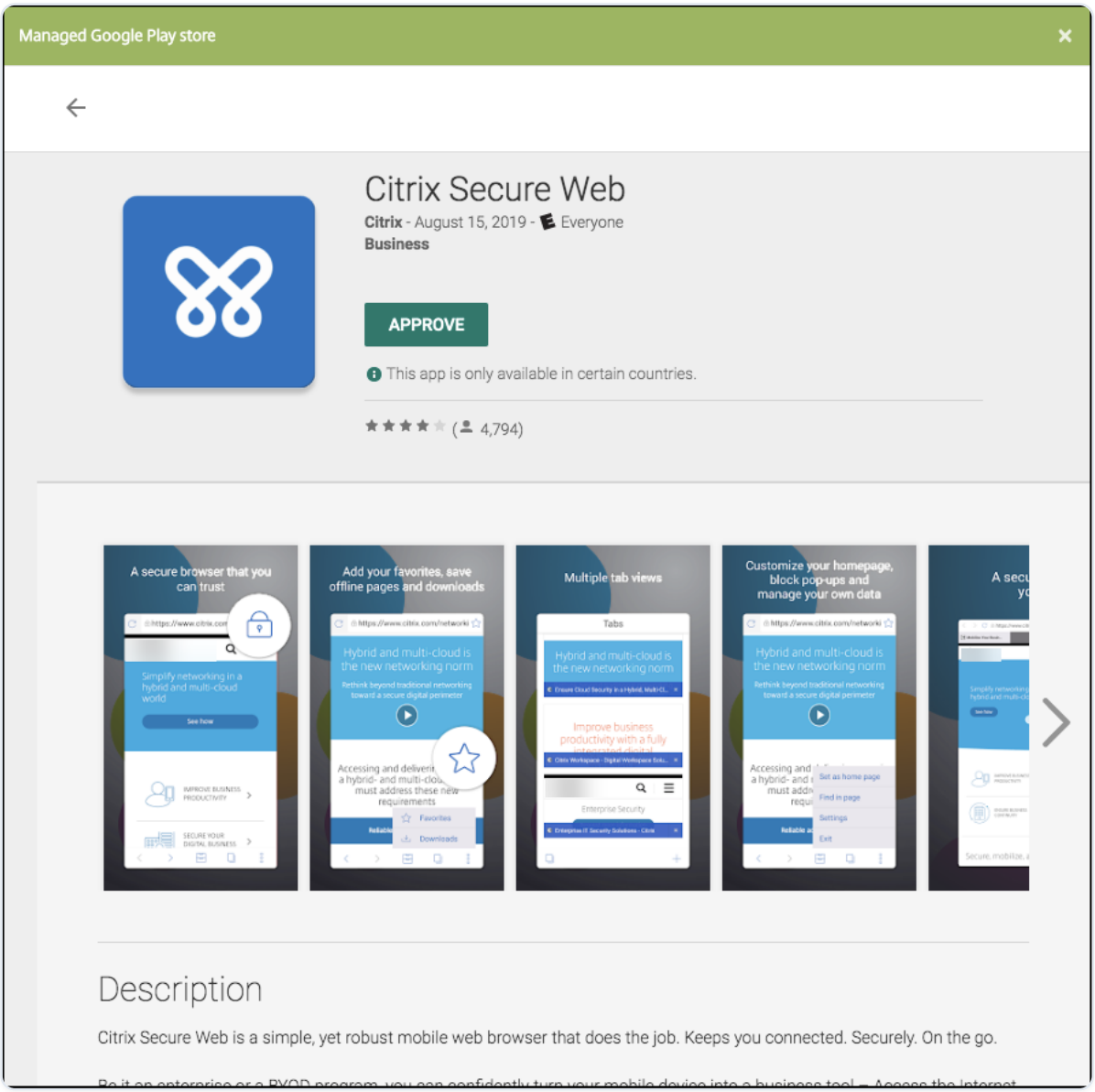
1. 在 Citrix Endpoint Management 控制台中，单击“**配置 > 应用程序**”。单击“**添加**”。“**添加应用程序**”对话框出现。



2. 单击“**MDX**”。“**MDX 应用程序信息**”页面出现。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**”表中的“**应用程序名称**”下。
   - **描述：** 键入应用程序的可选描述。
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 打包的应用程序。
   - UI 会通知您附加的应用程序是否需要托管 Google Play 商店的批准。要在不离开 Citrix Endpoint Management 控制台的情况下批准应用程序，请单击“**是**”。



托管 Google Play 商店打开后，按照说明批准并保存应用程序。



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。
- **程序包 ID：** 键入从托管 Google Play 商店获取的应用程序的程序包 ID。
- **最低操作系统版本：** （可选）键入设备可运行以使用应用程序的最旧操作系统版本。
- **最高操作系统版本：** （可选）键入设备必须运行才能使用应用程序的最新操作系统。
- **排除的设备：** （可选）键入无法运行应用程序的设备制造商或型号。

6. 配置 **MDX 策略**。MDX 策略因平台而异，包括身份验证、设备安全和应用程序限制等策略区域的选项。在控制台中，每个策略都有一个描述该策略的工具提示。有关适用于每种设备平台类型的应用程序策略的信息，请参阅：

   - MAM SDK 概述
   - MDX 第三方应用策略一览

7. 配置部署规则和应用商店配置。

   当您在**设置 > 服务器属性**中配置了计划后台部署密钥时，**部署以实现始终在线连接**适用。

   始终在线选项：

   - 不适用于 iOS 设备
   - 不适用于在开始使用 Citrix Endpoint Management 时版本为 10.18.19 或更高版本的 Android 和 Android Enterprise 客户
   - 不建议用于在开始使用 Citrix Endpoint Management 时版本低于 10.18.19 的 Android 和 Android Enterprise 客户

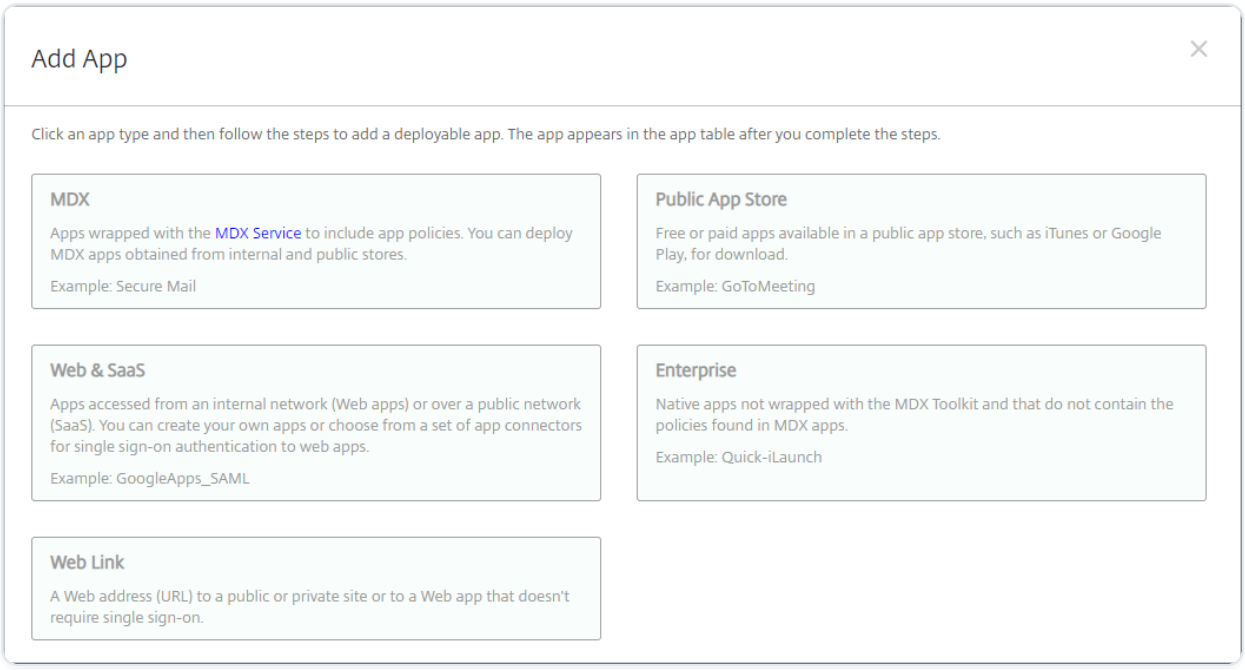
   您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但**部署以实现始终在线连接**除外。

8. 将任何交付组分配给此应用，然后单击**保存**。有关信息，请参阅部署资源。

更新应用

要更新 Android Enterprise 应用，请打包并上传更新的 .apk 文件：

1. 使用 MAM SDK 或 MDX Toolkit 打包更新应用的 .apk 文件。
2. 在 Citrix Endpoint Management 控制台中，单击**配置 > 应用**。**应用**页面随即打开。



3. 单击**添加**。**添加应用**对话框随即出现。
4. 点击“**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。此名称将列在“应用程序”表中的“应用程序名称”下。
   - “**描述：**”键入应用程序的可选描述。
5. 选择“**Android Enterprise**”作为平台。
6. 点击“**下一步**”。此时将显示“**企业应用程序**”页面。
7. 点击“**上传**”。
8. 在托管的 Google Play 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，点击 .apk 文件名旁边的“**编辑**”。

   编辑应用程序(/en-us/citrix-endpoint-management/media/publish-enterprise-app.png)
10. 导航到新的 .apk 文件并上传它。
11. 在托管的 Google Play 商店页面中，点击“**保存**”。

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

Google Workspace 客户必须使用旧版 Android Enterprise 设置来配置旧版 Android Enterprise。Google 最近将 G Suite 更名为 Google Workspace。

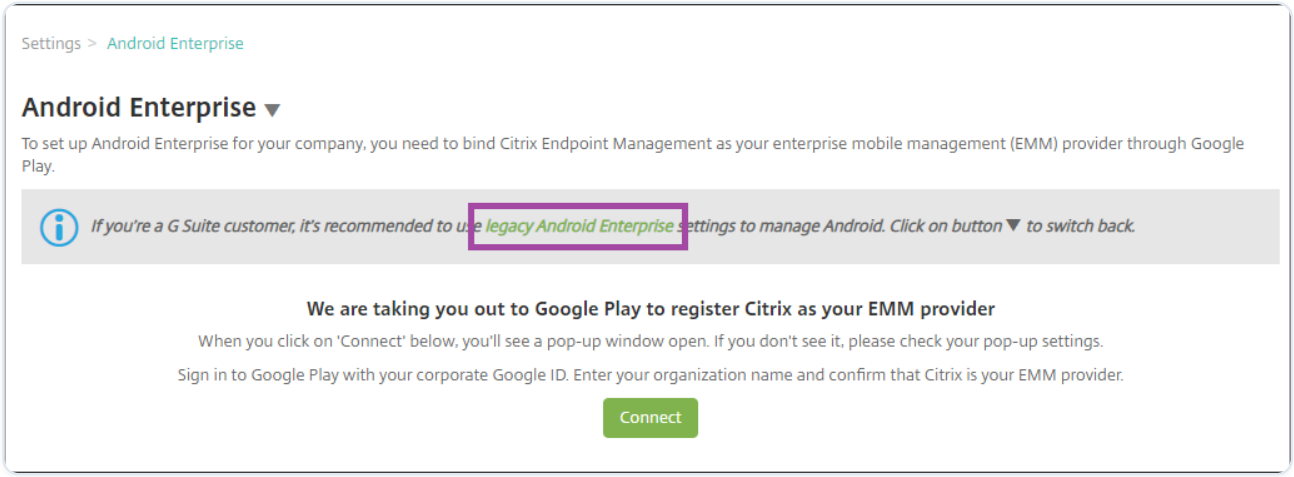
如果您的组织已使用 Google Workspace 为用户提供 Google 应用访问权限，则可以使用 Google Workspace 将 Citrix 注册为您的 EMM。如果您的组织使用 Google Workspace，则它具有现有的企业 ID 和现有用户 Google 帐户。要将 Citrix Endpoint Management 与 Google Workspace 结合使

用，您需要与 LDAP 目录同步，并使用 Google Directory API 从 Google 检索 Google 帐户信息。由于此类企业与现有域绑定，因此每个域只能创建一个企业。要在 Citrix 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。该帐户除了提供您的 Google Workspace 计划提供的任何其他 Google 服务外，还授予他们对托管 Google Play 的访问权限。

旧版 Android Enterprise 的要求：

- 可公开访问的域
- Google 管理员帐户
- 支持托管配置文件的 Android 设备
- 已安装 Google Play 的 Google 帐户
- 设备上设置的工作配置文件

要开始配置旧版 Android Enterprise，请在 Citrix Endpoint Management 设置的“**Android Enterprise**”页面中单击“**旧版 Android Enterprise**”。



创建 Android Enterprise 帐户

在设置 Android Enterprise 帐户之前，您必须向 Google 验证您的域名。

如果您已向 Google 验证您的域名，则可以跳到此步骤：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>`。

   下一页显示您输入管理员和公司信息的位置。

   帐户设置页面(/en-us/citrix-endpoint-management/media/afw-account-setup-redirect.png)
2. 输入您的管理员用户信息。

   管理员用户信息(/en-us/citrix-endpoint-management/media/afw-enter-admin-user-info.png)

3. 除了管理员帐户信息之外，还要输入您的公司信息。

   公司信息屏幕(/en-us/citrix-endpoint-management/media/afw-enter-company-info.png)

   流程的第一步已完成，您将看到以下页面。

   验证页面(/en-us/citrix-endpoint-management/media/afw-dns-verification-1.png)

验证域所有权

允许 Google 通过以下任一方式验证您的域：

- 将 TXT 或 CNAME 记录添加到您的域主机的网站。
- 将 HTML 文件上传到您的域的 Web 服务器。
- 将 `<meta>` 标记添加到您的主页。Google 建议使用第一种方法。本文不介绍验证域所有权的步骤，但您可以在此处找到所需信息：https://support.google.com/a/answer/6248925。

1. 单击 **Start** 开始验证您的域。

   出现“**验证域所有权**”页面。按照页面上的说明验证您的域。

2. 点击**验证**。

   验证按钮(/en-us/citrix-endpoint-management/media/afw-verify-domain-ownership.png)

   验证确认(/en-us/citrix-endpoint-management/media/afw-domain-verified.png)

3. Google 验证您的域所有权。

   域所有权验证(/en-us/citrix-endpoint-management/media/afw-google-verification.png)

4. 成功验证后，将显示以下页面。点击**继续**。

   成功确认页面(/en-us/citrix-endpoint-management/media/afw-dns-verification-9.png)

5. Google 创建一个 EMM 绑定令牌，您需要将此令牌提供给 Citrix® 并在配置 Android Enterprise 设置时使用。复制并保存此令牌；您在后续设置过程中需要它。

   绑定令牌(/en-us/citrix-endpoint-management/media/afw-obtain-token.png)

6. 点击**完成**以完成 Android Enterprise 的设置。此时将显示一个页面，指示您已成功验证域。

创建 Android Enterprise 服务帐户后，您可以登录 Google 管理控制台以管理您的移动性管理设置。

设置 Android Enterprise 服务帐户并下载 Android Enterprise 证书

要允许 Citrix Endpoint Management 联系 Google Play 和目录服务，您必须使用面向开发人员的 Google Project 门户创建服务帐户。此服务帐户用于 Citrix Endpoint Management 与 Google Android 服务之间的服务器到服务器通信。有关所用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，点击**创建项目**。

   创建项目选项(/en-us/citrix-endpoint-management/media/google-config-api-1.png)
3. 在 **项目名称** 中，键入项目的名称。

   项目名称选项(/en-us/citrix-endpoint-management/media/google-config-api-2.png)
4. 在控制面板上，单击 **使用 Google API**。

   使用 Google API 选项(/en-us/citrix-endpoint-management/media/google-config-api-6.png)
5. 单击 **库**，在 **搜索** 中键入 **EMM**，然后单击搜索结果。

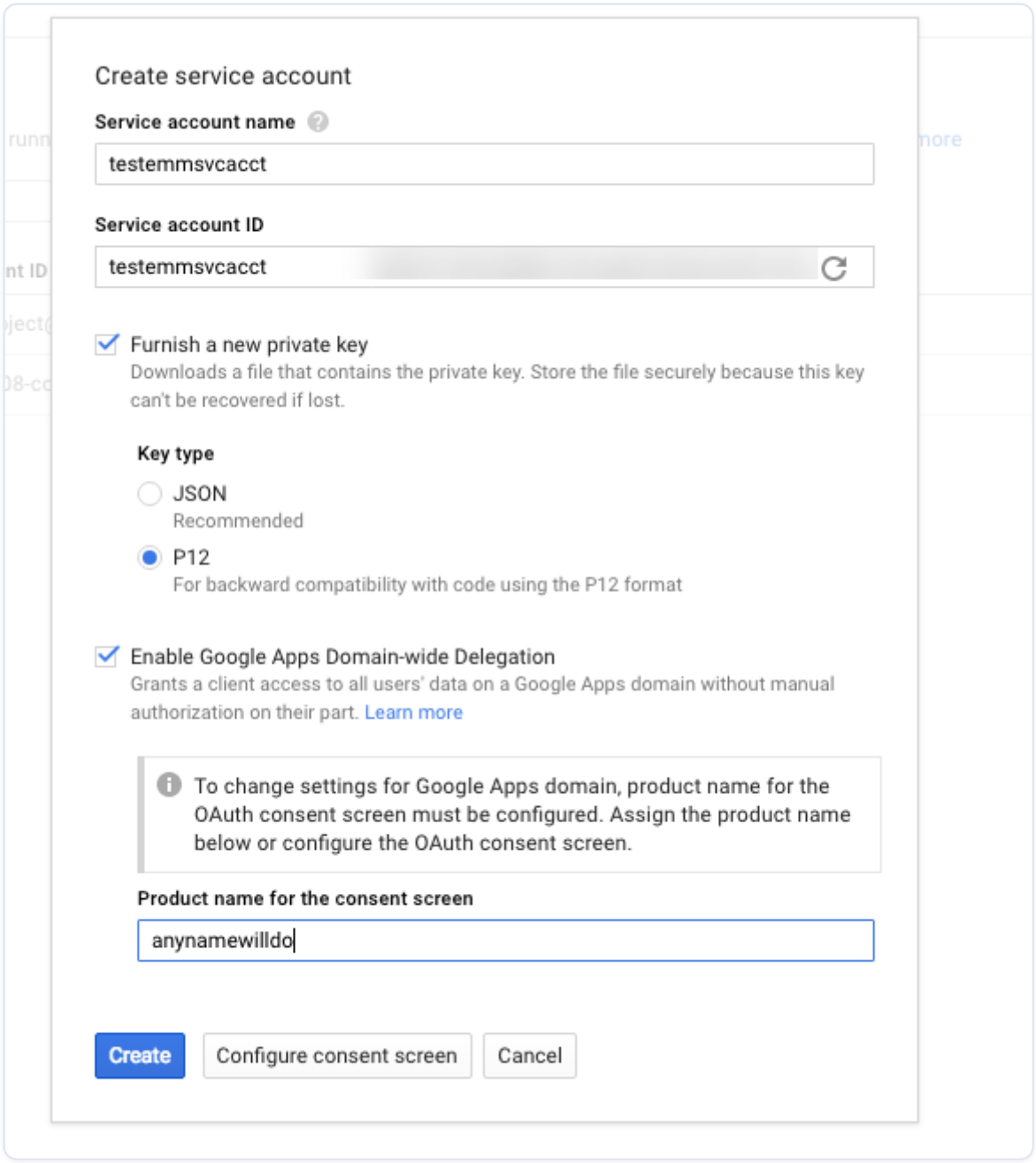
   EMM 搜索选项(/en-us/citrix-endpoint-management/media/afw-emm-search.png)
6. 在 **概览** 页面上，单击 **启用**。

   启用选项(/en-us/citrix-endpoint-management/media/afw-emm-enable.png)
7. 在 **Google Play EMM API** 旁边，单击 **转到凭据**。

   转到凭据选项(/en-us/citrix-endpoint-management/media/google-config-api-13.png)
8. 在 **将凭据添加到我们的项目** 列表中，在步骤 1 中，单击 **服务帐户**。

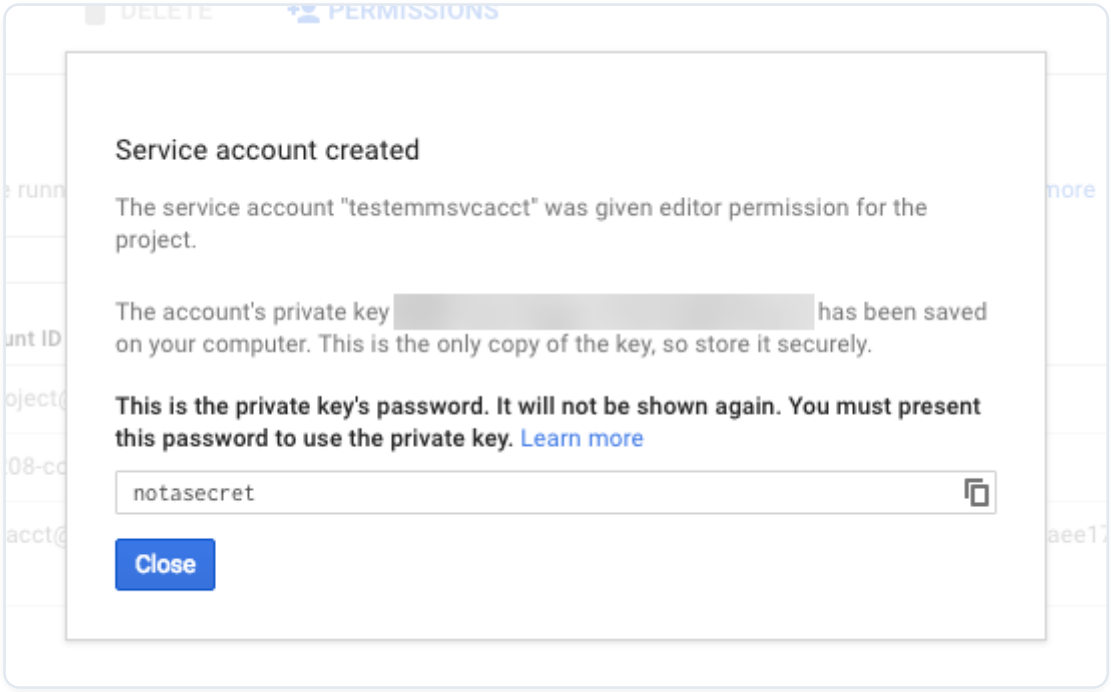
   服务帐户选项(/en-us/citrix-endpoint-management/media/google-config-api-1b.png)
9. 在 **服务帐户** 页面上，单击 **创建服务帐户**。

   创建服务帐户选项(/en-us/citrix-endpoint-management/media/google-config-api-1e.png)
10. 在**创建服务帐号**中，命名该帐号，然后选中**提供新的私钥**复选框。单击 **P12**，选中**启用 Google Apps 域范围授权**复选框，然后单击**创建**。

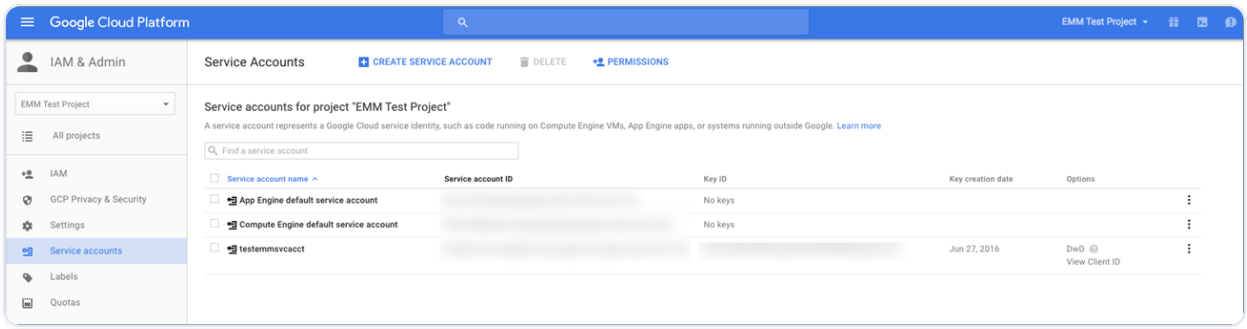


证书 (P12 文件) 已下载到您的计算机。请务必将证书保存在安全位置。

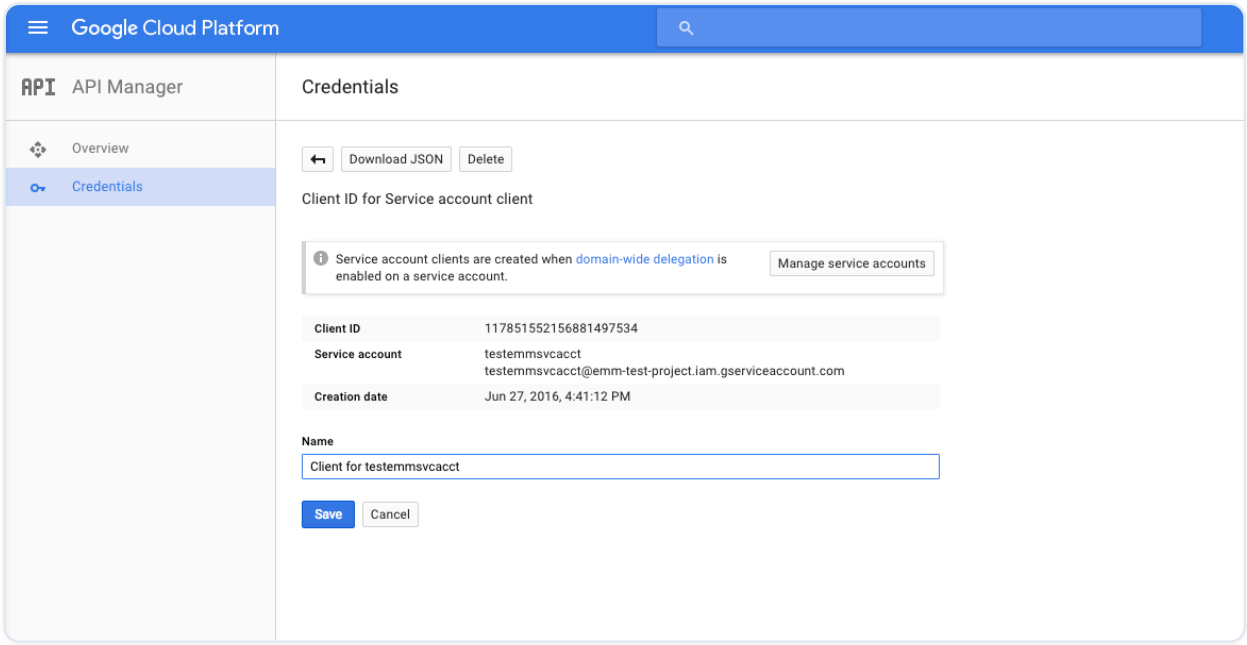
11. 在**服务帐号已创建**确认页面上，单击**关闭**。



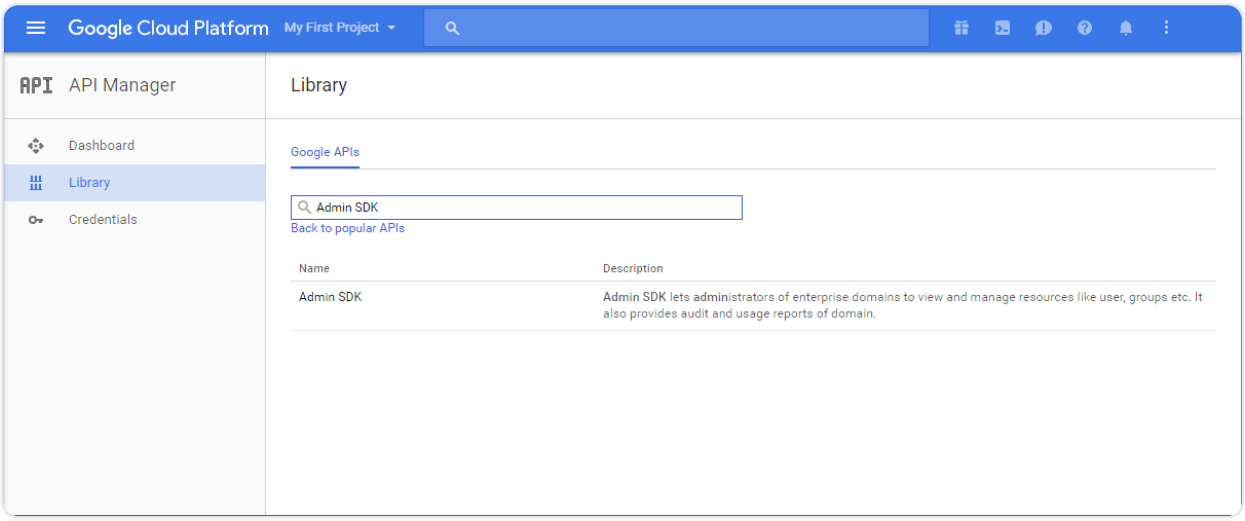
12. 在**权限**中，单击**服务帐号**，然后在您的服务帐号的**选项**下，单击**查看客户端 ID**。



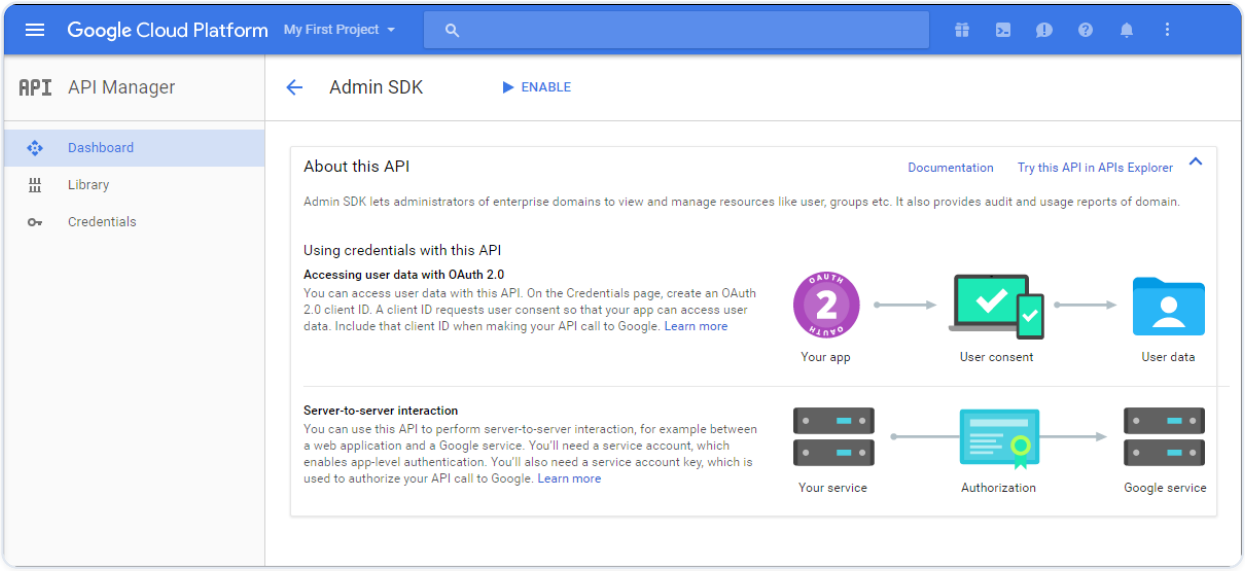
13. Google 管理控制台上显示帐号授权所需的详细信息。将**客户端 ID** 和**服务帐号 ID** 复制到以后可以检索信息的位置。您需要此信息以及域名，以便发送给 Citrix 支持人员以添加到允许列表。



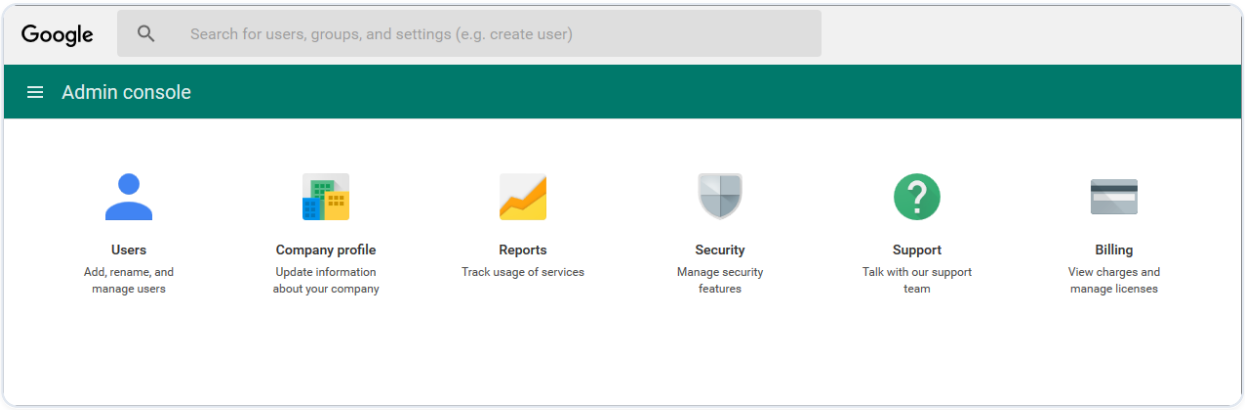
14. 在**库**页面上，搜索 **Admin SDK**，然后单击搜索结果。



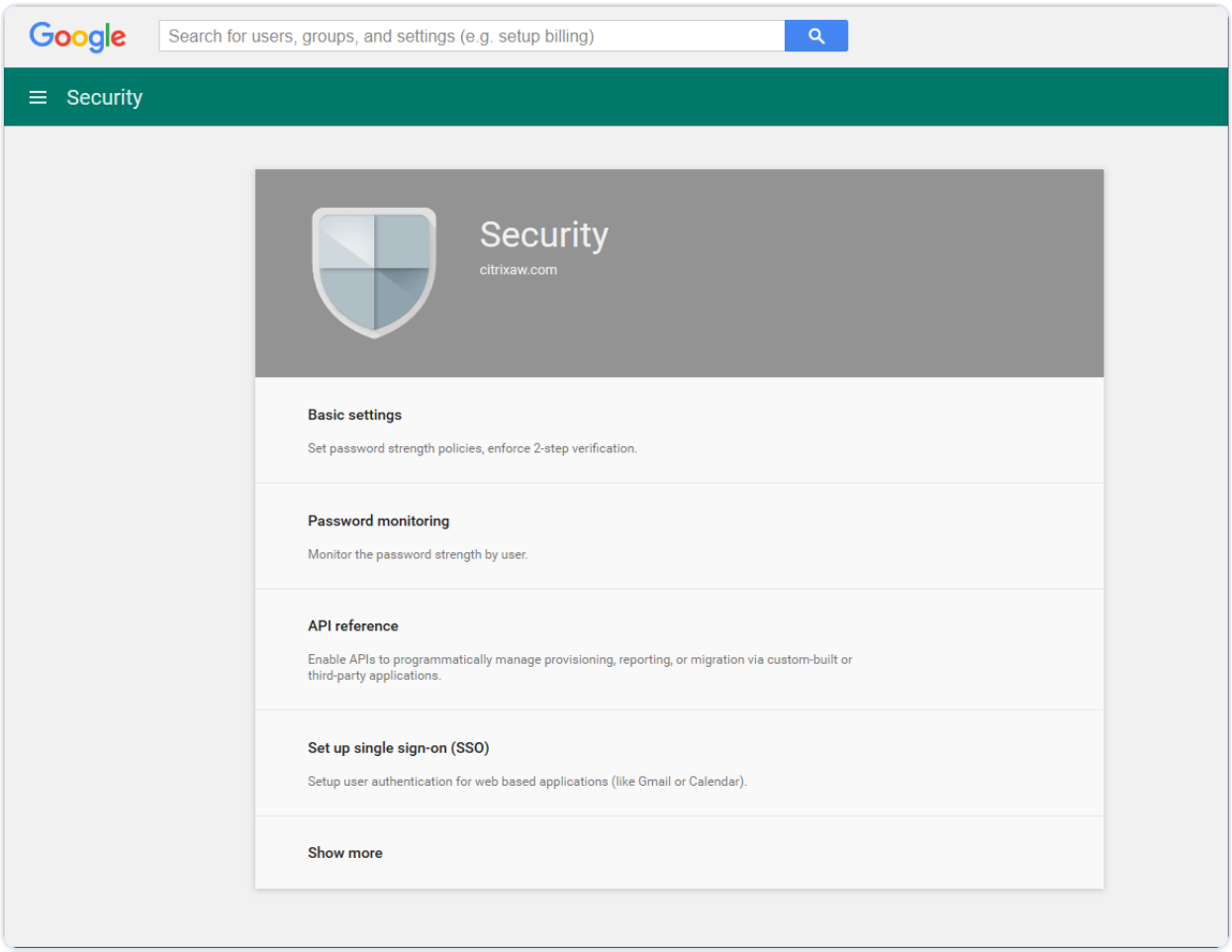
15. 在**概览**页面上，单击**启用**。

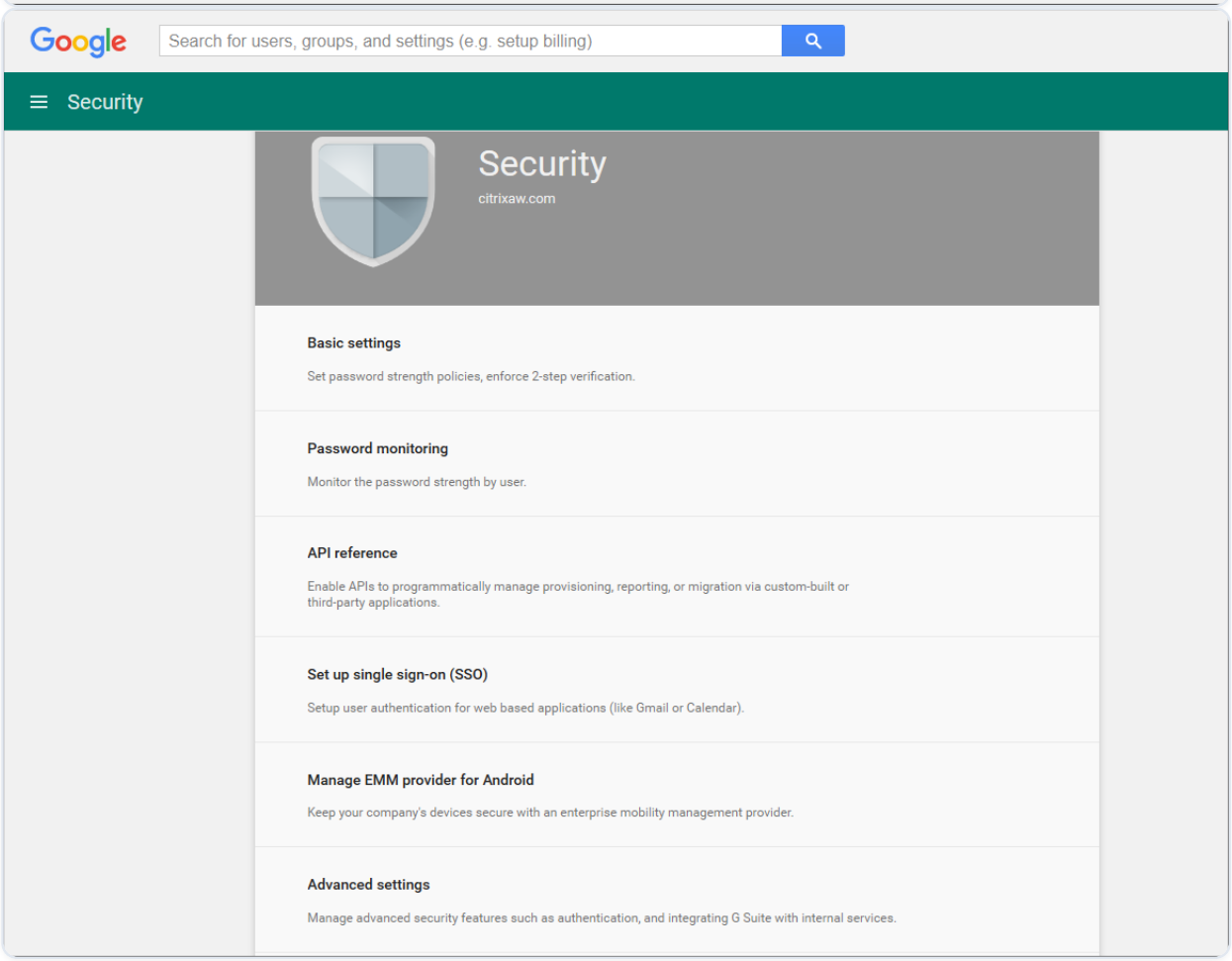


16. 打开您的域的 Google 管理控制台，然后单击**安全**。

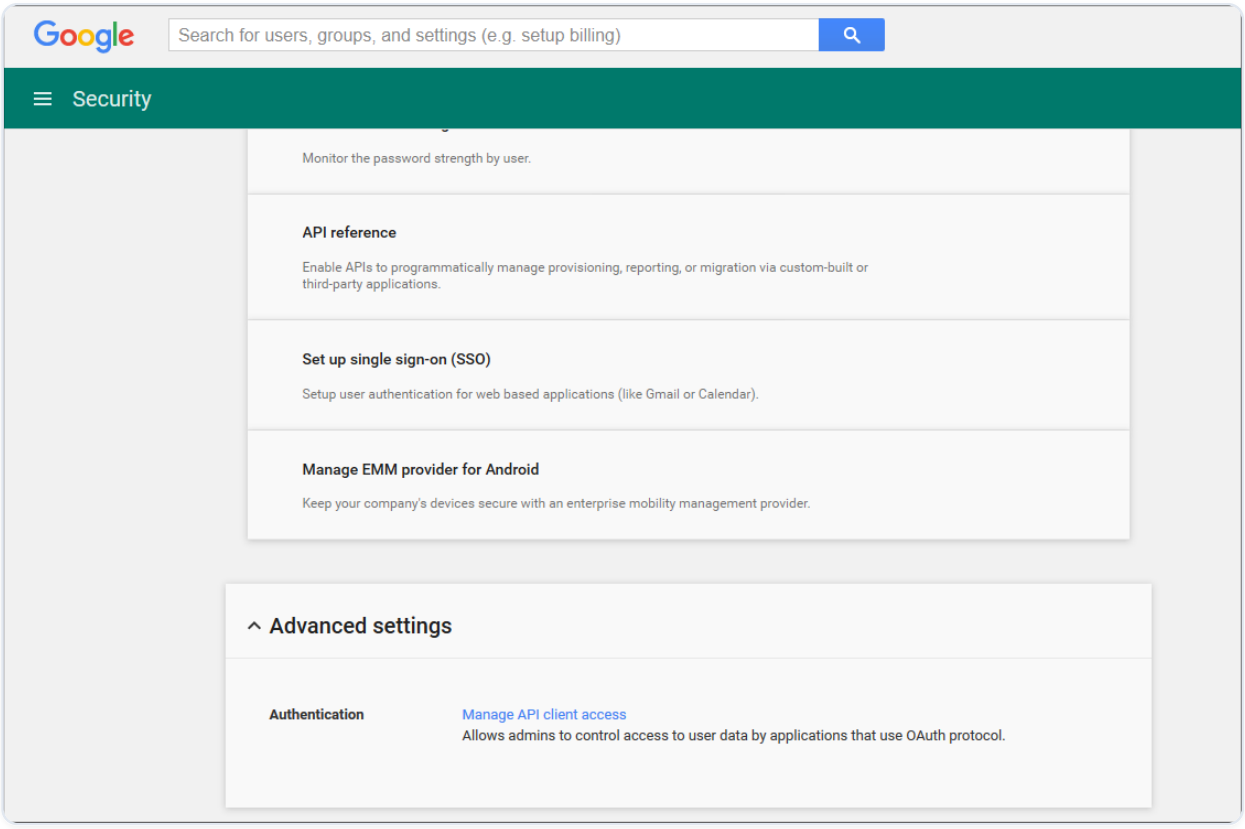


17. 在“**设置**”页面上，单击“**显示更多**”，然后单击“**高级设置**”。

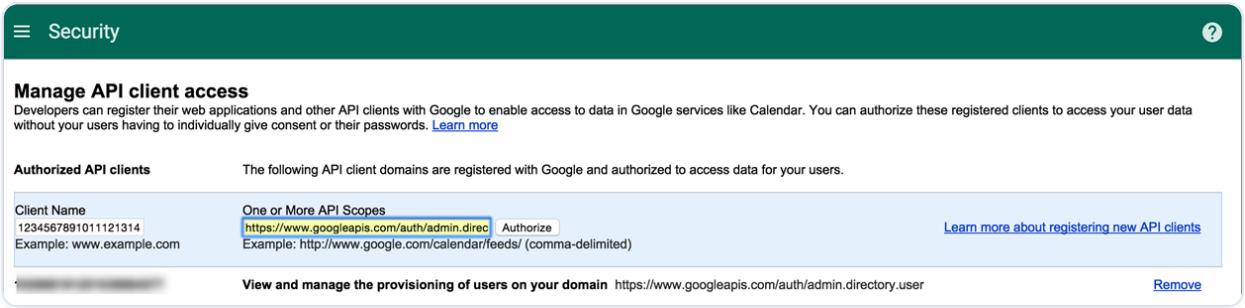

Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Show more


Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Manage EMM provider for Android
Keep your company's devices secure with an enterprise mobility management provider.
Advanced settings
Manage advanced security features such as authentication, and integrating G Suite with internal services.

18. 单击“**管理 API 客户端访问**”。



19. 在“**客户端名称**”中，键入您之前保存的客户端 ID；在“**一个或多个 API 范围**”中，键入 `https://www.googleapis.com/auth/admin.directory.user`，然后单击“**授权**”。



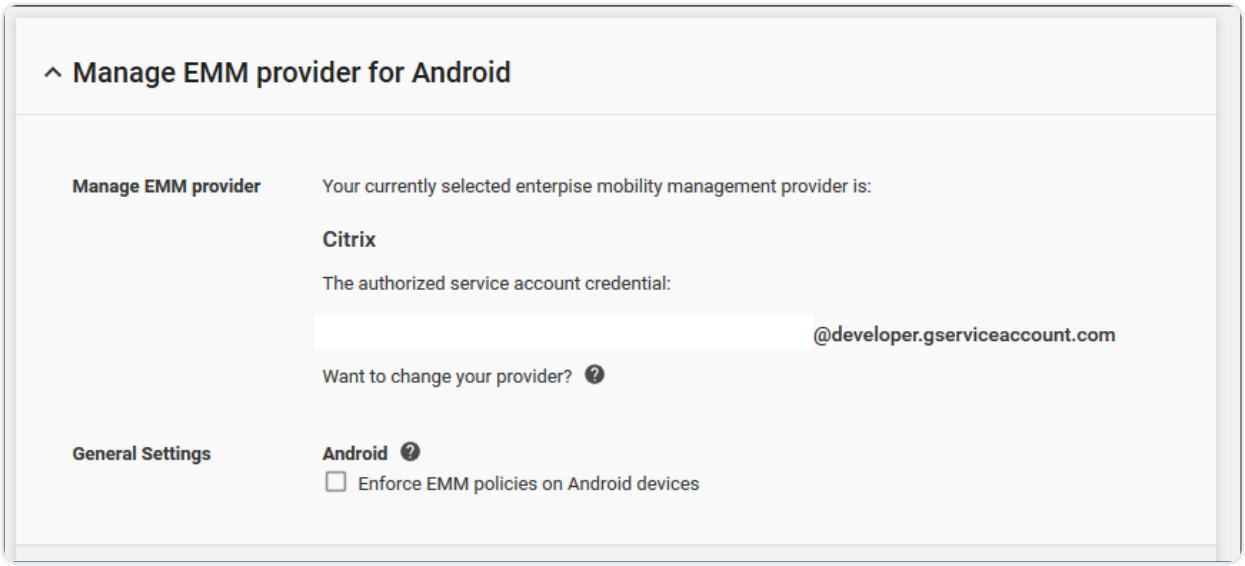
绑定到 EMM

在使用 Citrix Endpoint Management 管理 Android 设备之前，您必须联系 Citrix 技术支持并提供您的域名、服务帐户和绑定令牌。Citrix 会将该令牌绑定到 Citrix Endpoint Management，作为您的企业移动性管理 (EMM) 提供商。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“**安全性**”。
2. 单击“**管理 Android 的 EMM 提供商**”。

   您会看到您的 Google Android Enterprise 帐户已绑定到 Citrix 作为您的 EMM 提供商。

确认令牌绑定后，您可以开始使用 Citrix Endpoint Management 控制台管理 Android 设备。导入您在步骤 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)，并定义至少一个 Android Enterprise 设备策略。



导入 P12 证书

请按照以下步骤导入您的 Android Enterprise P12 证书：

1. 在 Citrix 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**”。“**证书**”页面随即显示。

   证书页面(/en-us/citrix-endpoint-management/media/android-enterprise-certs-import.png)

2. 单击“**导入**”。“**导入**”对话框随即显示。

   导入对话框(/en-us/citrix-endpoint-management/media/afw-import-certificate-detail.png)

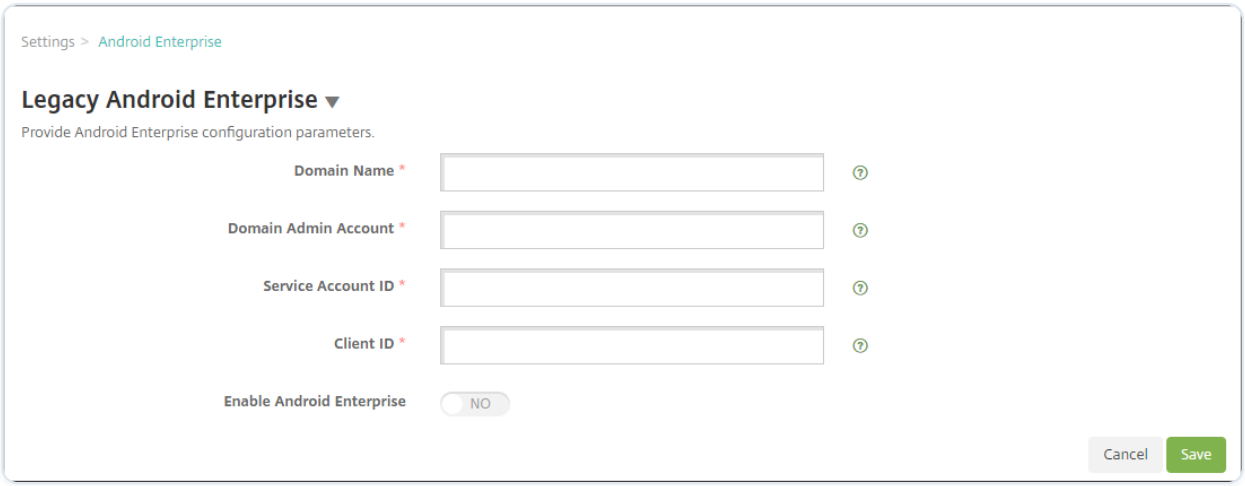
   配置以下设置：

   - **导入：** 在下拉列表中单击“**密钥库**”。
   - **密钥库类型：** 在下拉列表中单击“**PKCS#12**”。
   - **用作：** 在下拉列表中单击“**服务器**”。
   - **密钥库文件：** 单击“**浏览**”并导航到 P12 证书。
   - **密码：** 键入证书密码。此密码是您在设置 Android Enterprise 帐户时创建的私钥密码。
   - **描述：** （可选）键入证书的描述。

3. 单击 **Import**。

设置 Android Enterprise 服务器设置

1. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标。“**设置**”页面随即显示。
2. 在“**平台**”下，单击“**Android Enterprise**”。“**Android Enterprise**”页面随即显示。



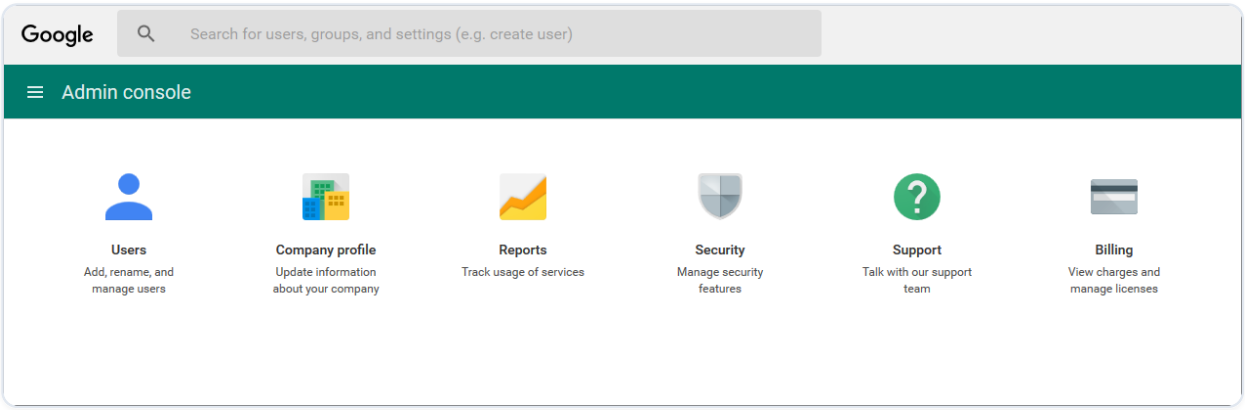
配置以下设置，然后单击“**保存**”。

- **域名：**键入您的 Android Enterprise 域名；例如，domain.com。
- **域管理员帐户：**键入您的域管理员用户名；例如，用于 Google Developer Portal 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@xxxxxxxxx.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。

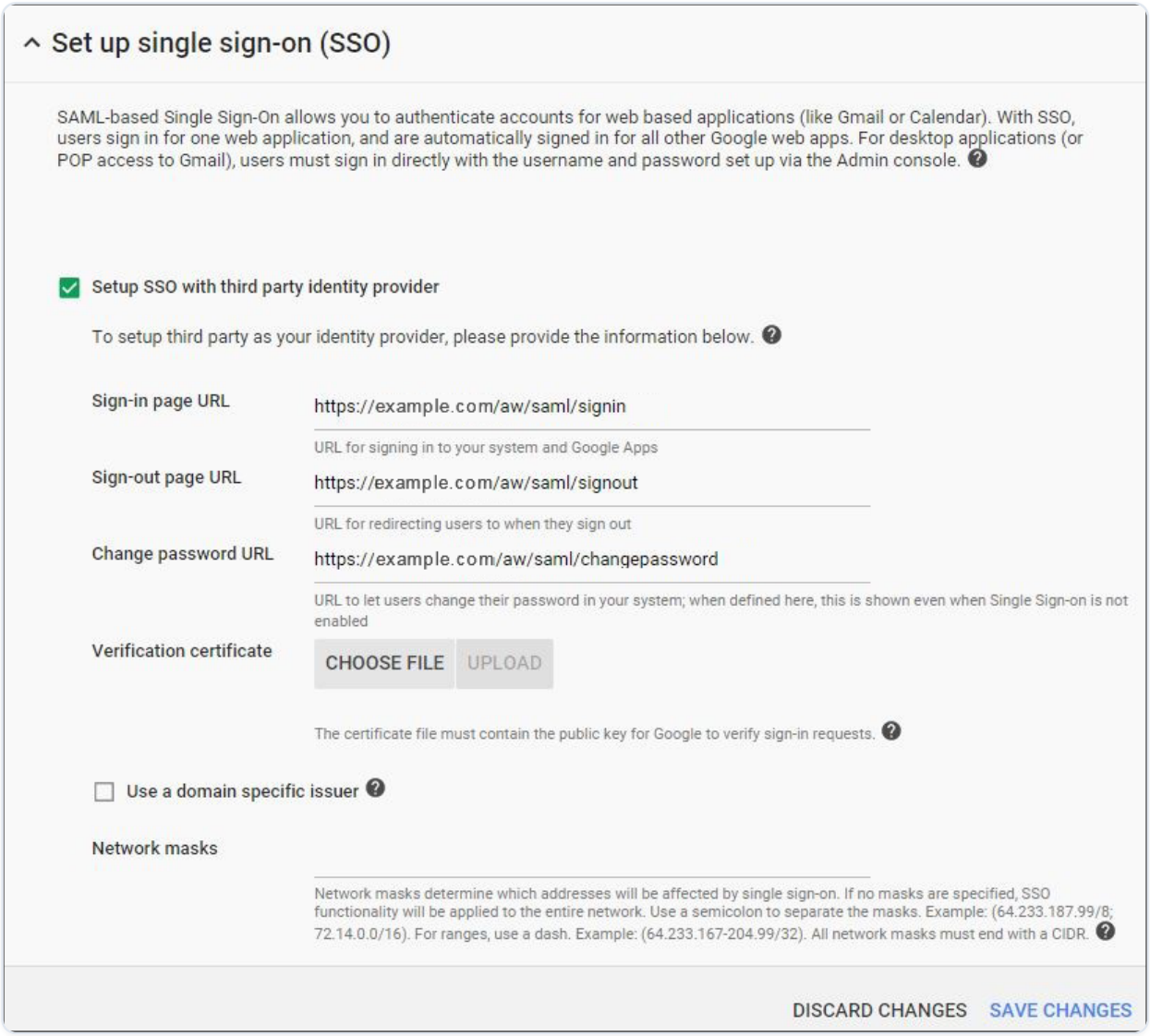
启用基于 SAML 的单点登录

1. 在 Citrix 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。

   证书页面(/en-us/citrix-endpoint-management/media/android-enterprise-certs-export.png)
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。
5. 使用您的 Android Enterprise 管理员凭据登录 Google 管理门户。有关访问门户的信息，请参阅 Google 管理门户。
6. 单击“**安全性**”。



7. 在**安全**下，单击**设置单点登录 (SSO)**，然后配置以下设置。



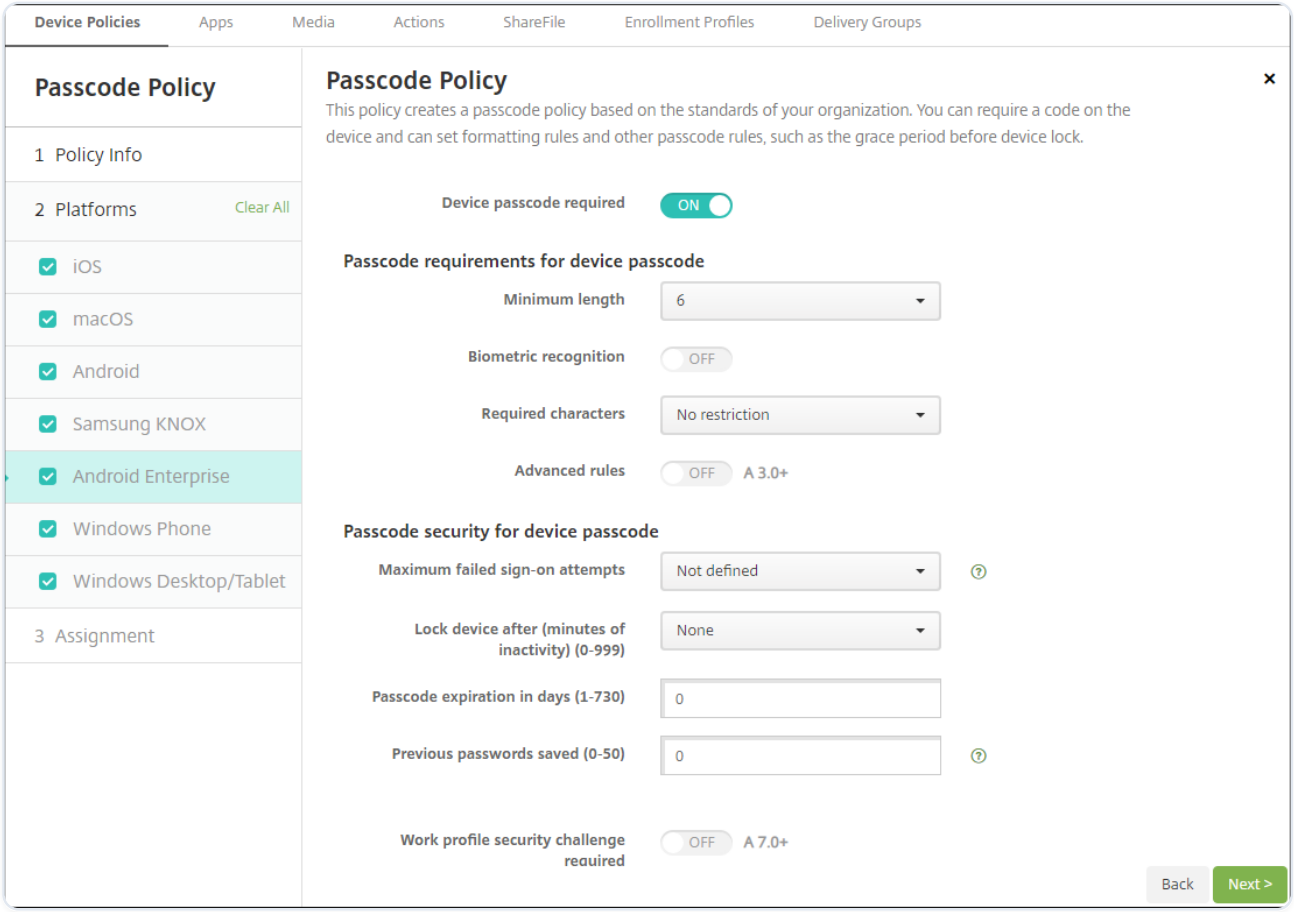
- **登录页面 URL**：键入用户登录到您的系统和 Google Apps 的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/signin`。
- **注销页面 URL**：键入用户注销时重定向到的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/signout`。

- **更改密码 URL：** 键入允许用户在您的系统中更改其密码的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/changepassword`。如果定义了此字段，即使 SSO 不可用，用户也会看到此提示。
- **验证证书：** 单击**选择文件**，然后导航到从 Citrix Endpoint Management 导出的 SAML 证书。

8. 单击**保存更改**。

设置 Android Enterprise 设备策略

设置密码策略，以便用户在首次注册时必须在其设备上设置密码。



设置任何设备策略的基本步骤如下。

1. 在 Citrix Endpoint Management 控制台中，单击**配置**，然后单击**设备策略**。
2. 单击 **添加**。
3. 在**添加新策略**对话框中，选择要添加的策略。在此示例中，单击**密码**。
4. 完成**策略信息**页面。
5. 点击 **Android Enterprise**，然后配置策略设置。
6. 将策略分配给交付组。

配置 Android Enterprise 帐户设置

在开始管理设备上的 Android 应用程序和策略之前，您必须在 Citrix Endpoint Management 中设置 Android Enterprise 域和帐户信息。首先，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 Citrix 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：** 键入您的域名。
   - **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. 点击 **保存**。

为 Citrix Endpoint Management 设置 Google Workspace 合作伙伴访问权限

Citrix Endpoint Management 的某些 Chrome 功能使用 Google 合作伙伴 API 在 Citrix Endpoint Management 和您的 Google Workspace 域之间进行通信。例如，Citrix Endpoint Management 需要用于设备策略的 API，这些策略管理 Chrome 功能，例如无痕模式和访客模式。

要启用合作伙伴 API，您需要在 Citrix Endpoint Management 控制台中设置您的 Google Workspace 域，然后配置您的 Google Workspace 帐户。

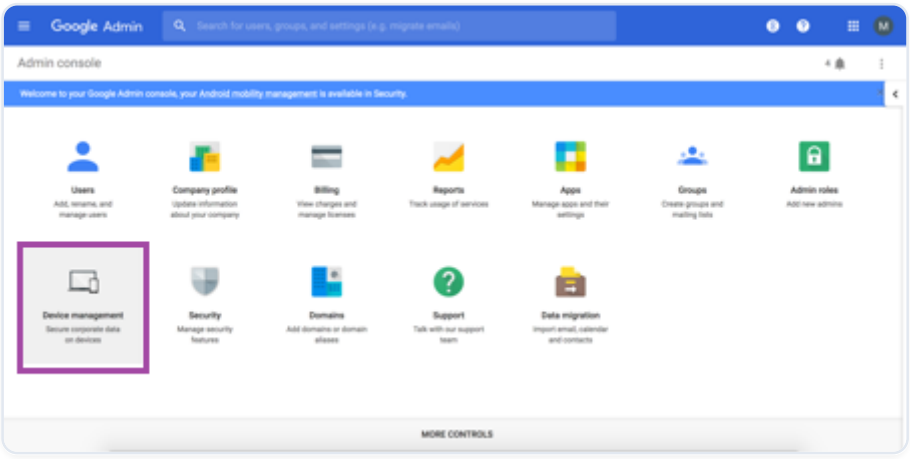
在 Citrix Endpoint Management 中设置您的 Google Workspace 域

要使 Citrix Endpoint Management 能够与您的 Google Workspace 域中的 API 通信，请转到 **设置 > Google Chrome 配置** 并配置相关设置。

- **Google Workspace 域：** 托管 Citrix Endpoint Management 所需 API 的 Google Workspace 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。使用此值配置您的 Google Workspace 域的合作伙伴访问权限。
- **Google Workspace 企业 ID：** 您的帐户的企业 ID，从您的 Google 企业帐户中填写。

为您的 Google Workspace 域中的设备和用户启用合作伙伴访问权限

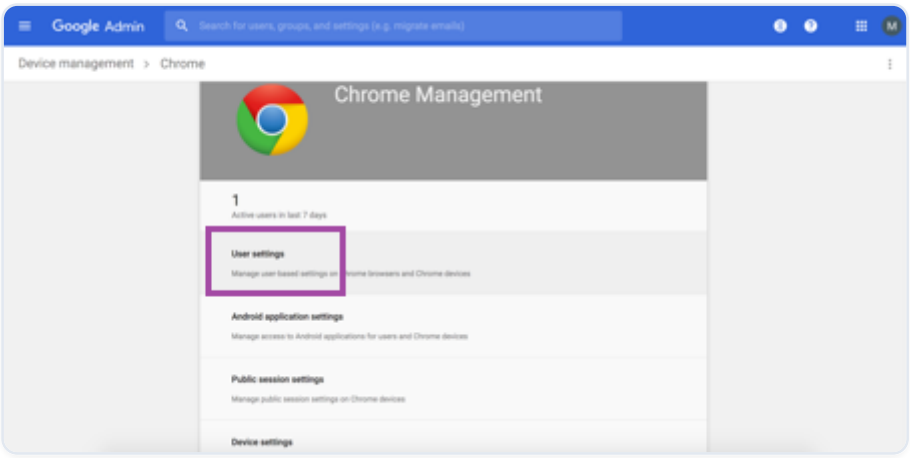
1. 登录 Google 管理控制台：`<https://admin.google.com>`
2. 单击 **设备管理**。



3. 单击 **Chrome 管理**。



4. 单击 **用户设置**。



5. 搜索 **Chrome 管理 - 合作伙伴访问**。

   Google 管理员控制台(/en-us/citrix-endpoint-management/media/google-admin-partner-access4.png)

6. 选择 **启用 Chrome 管理 - 合作伙伴访问** 复选框。
7. 同意您理解并希望启用合作伙伴访问。单击**保存**。
8. 在 Chrome 管理页面中，单击**设备设置**。

   Google 管理员控制台(/en-us/citrix-endpoint-management/media/google-admin-partner-access5.png)

9. 搜索 **Chrome 管理 - 合作伙伴访问**。

   Google 管理员控制台(/en-us/citrix-endpoint-management/media/google-admin-partner-access6.png)

10. 选择 **启用 Chrome 管理 - 合作伙伴访问** 复选框。
11. 同意您理解并希望启用合作伙伴访问。单击**保存**。
12. 转到**安全性**页面，然后单击**高级设置**。

    Google 管理员控制台(/en-us/citrix-endpoint-management/media/google-admin-partner-access7.png)

13. 单击**管理 API 客户端访问**。
14. 在 Citrix Endpoint Management 控制台中，转到**设置 > Google Chrome 配置**并复制 G Suite 客户端 ID 的值。然后，返回到**管理 API 客户端访问**页面并将复制的值粘贴到**客户端名称**字段中。
15. 在**一个或多个 API 范围**中，添加 URL: `https://www.googleapis.com/auth/chromedevicemanagementapi`



16. 单击 **Authorize**。

    出现消息“您的设置已保存”。

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，则接受的格式取决于 Citrix Endpoint Management 服务器配置为按用户主体名称 (UPN) 或 SAM 帐户名搜索用户的方式。

如果 Citrix Endpoint Management 服务器配置为按 UPN 搜索用户，则用户必须按以下格式输入 UPN：

- *用户名@域名*

如果 Citrix Endpoint Management 服务器配置为按 SAM 搜索用户，则用户必须按以下格式之一输入 SAM：

- *用户名@域名*
- *domain\username*

要确定您的 Citrix Endpoint Management 服务器配置为哪种类型的用户名，请执行以下操作：

1. 在 Citrix 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. 在页面底部，查看“**用户搜索依据**”字段：
    - 如果设置为 **userPrincipalName**，则 Citrix Endpoint Management 服务器已设置为 UPN。
    - 如果设置为 **sAMAccountName**，则 Citrix Endpoint Management 服务器将设置为 SAM。

取消注册 Android Enterprise 企业

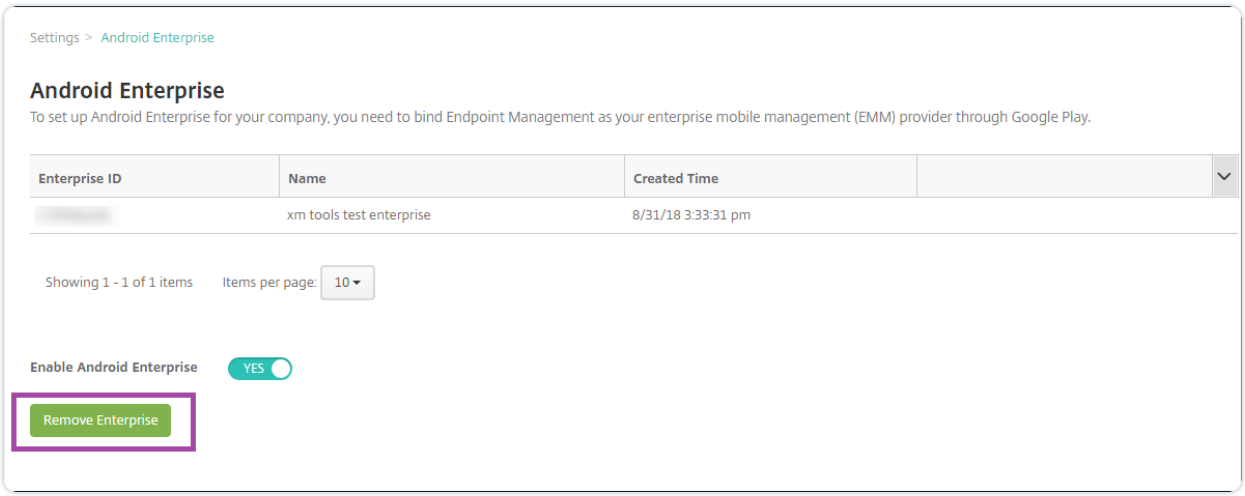
您可以使用 Citrix Endpoint Management 服务器控制台和 Citrix Endpoint Management Tools 取消注册 Android Enterprise 企业。

执行此任务时，Citrix Endpoint Management 服务器会为 Citrix Endpoint Management Tools 打开一个弹出窗口。开始之前，请确保 Citrix 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）要求您禁用弹出窗口阻止功能，并将 Citrix Endpoint Management 站点的地址添加到弹出窗口允许列表中。

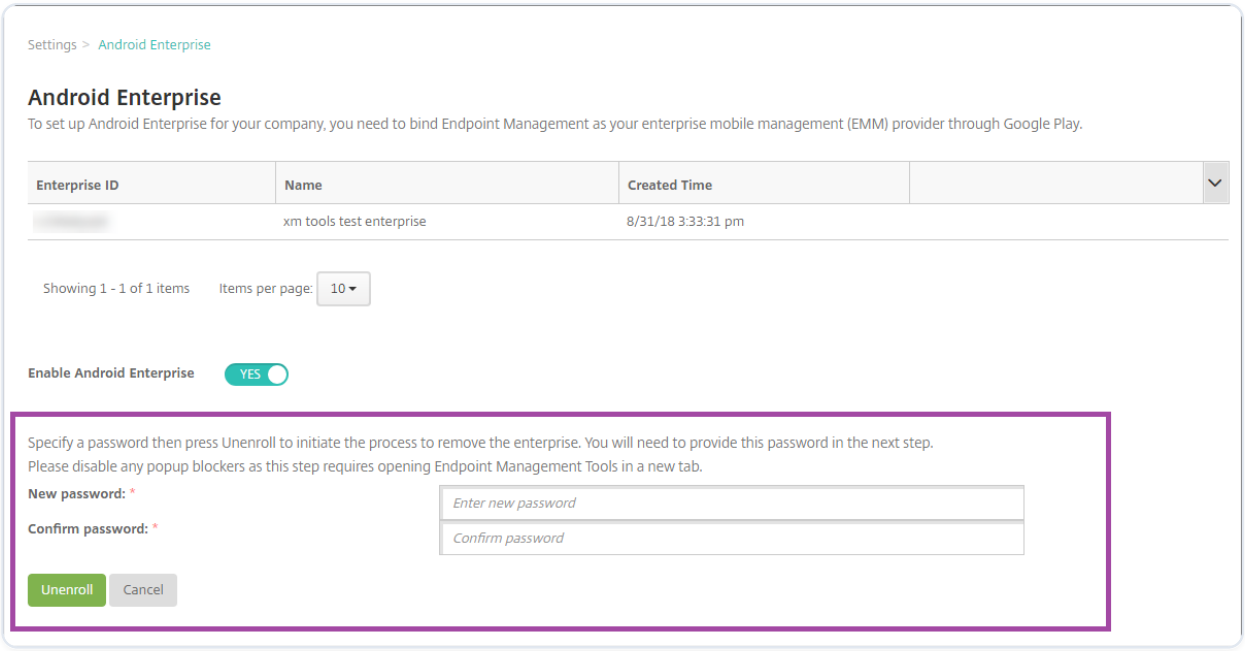
> **警告：**
>
> 企业取消注册后，通过该企业注册的设备上的 Android Enterprise 应用程序将重置为默认状态。这些设备不再由 Google 管理。在 Android Enterprise 企业中重新注册它们可能无法在没有进一步配置的情况下恢复以前的功能。
>
> Android Enterprise 企业取消注册后：
>
> - 通过该企业注册的设备和用户，其 Android Enterprise 应用程序将重置为默认状态。以前应用的应用程序权限和托管配置策略不再生效。
> - 通过该企业注册的设备由 Citrix Endpoint Management 管理，但从 Google 的角度来看是未受管理的。无法添加新的 Android Enterprise 应用程序。无法应用应用程序权限或托管配置策略。其他策略（例如计划、密码和限制）仍可应用于这些设备。
> - 如果您尝试在 Android Enterprise 中注册设备，它们将注册为 Android 设备，而不是 Android Enterprise 设备。

要取消注册 Android Enterprise 企业：

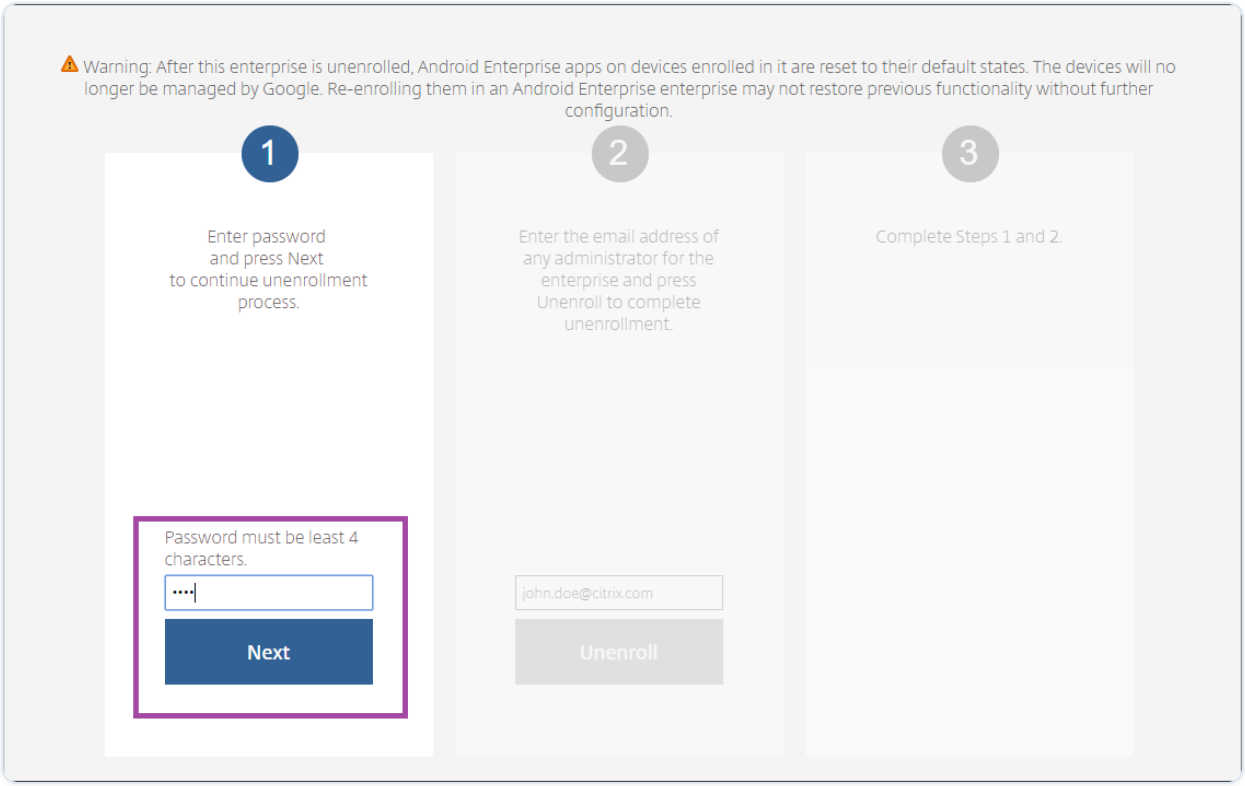
1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。“设置”页面随即显示。
2. 在“设置”页面上，单击 **Android Enterprise**。
3. 单击 **删除企业**。



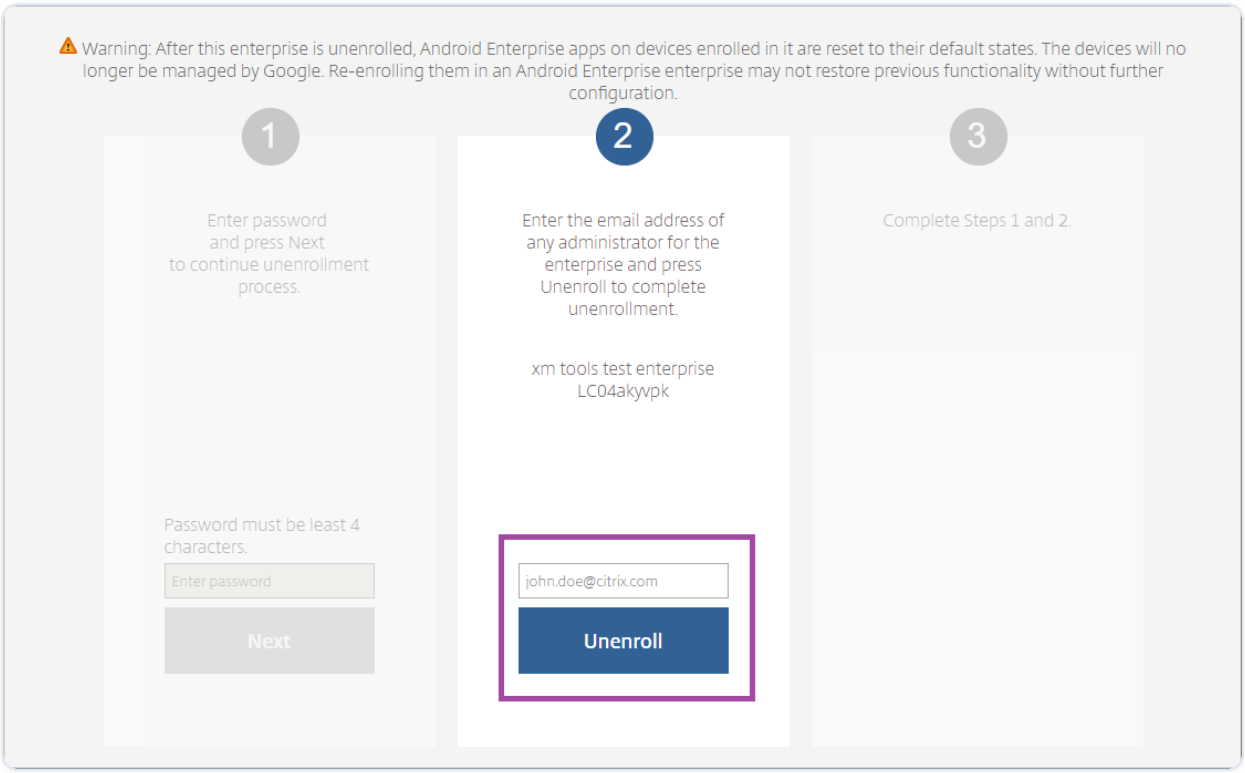
4. 指定密码。下一步完成取消注册时需要此密码。然后单击 **Unenroll**。



5. Citrix Endpoint Management Tools 页面打开后，输入您在上一步中创建的密码。



6. 单击 **注销**。



在 Android Enterprise 中预配完全托管设备

只有公司拥有的设备才能成为 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。

Citrix Endpoint Management 支持以下用于完全托管设备的注册方法：

- **afw#xenmobile:** 使用此注册方法，用户在设置设备时输入字符 `afw#xenmobile`。此令牌将设备标识为由 Citrix Endpoint Management 管理，并下载 Citrix Secure Hub。
- **QR code:** QR 码预配是一种简单的方法，可用于预配不支持 NFC 的分布式设备群（例如平板电脑）。QR 码注册方法可用于已恢复出厂设置的设备群。QR 码注册方法通过从设置向导扫描 QR 码来设置和配置完全托管设备。
- **Near field communication (NFC) bump:** NFC 碰撞注册方法可用于已恢复出厂设置的设备群。NFC 碰撞通过近场通信在两台设备之间传输数据。在恢复出厂设置的设备上，蓝牙、Wi-Fi 和其他通信模式均已禁用。NFC 是设备在此状态下可以使用的唯一通信协议。

`afw#xenmobile`

此注册方法用于在新设备或恢复出厂设置的设备开机后进行初始设置。当系统提示用户输入 Google 帐户时，用户输入 `afw#xenmobile`。此操作将下载并安装 Citrix Secure Hub。然后，用户按照 Citrix Secure Hub 设置提示完成注册。

此注册方法推荐给大多数客户，因为最新版本的 Citrix Secure Hub 是从 Google Play 商店下载的。与其他注册方法不同，您无需提供 Citrix Secure Hub 以便从 Citrix Endpoint Management 服务器下载。

先决条件：

- 支持所有运行 Android 操作系统的 Android 设备。

QR 码

要使用二维码在设备模式下注册设备，您需要通过创建 JSON 并将其转换为二维码来生成二维码。设备摄像头扫描二维码以注册设备。

先决条件：

- 支持所有运行 Android 7.0 及更高版本的 Android 设备。

从 JSON 创建二维码

使用以下字段创建 JSON。

以下字段是必需的：

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

值: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

以下字段是可选的：

- **android.app.extra.PROVISIONING_LOCALE：** 输入语言和国家/地区代码。

  语言代码是 ISO 639-1 定义的两位小写 ISO 语言代码（例如 en）。国家/地区代码是 ISO 3166-1 定义的两位大写 ISO 国家/地区代码（例如 US）。例如，输入 en_US 表示在美国使用的英语。

- **android.app.extra.PROVISIONING_TIME_ZONE：** 设备运行所在的时区。

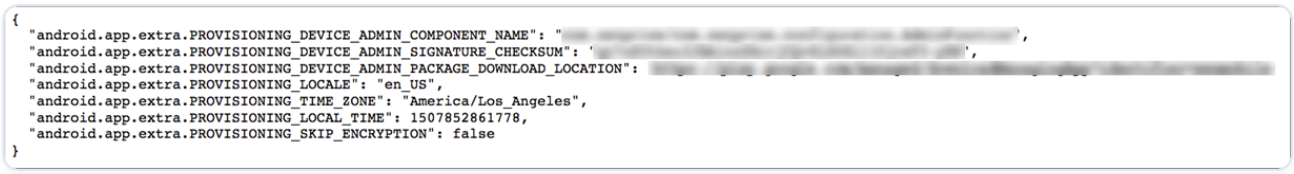
  键入 区域/位置的数据库名称。例如，键入 **America/Los_Angeles** 表示太平洋时间。如果您不键入名称，时区将自动填充。

- **android.app.extra.PROVISIONING_LOCAL_TIME:** 自纪元以来的毫秒数。

  Unix 纪元（或 Unix 时间、POSIX 时间或 Unix 时间戳）是自 January 1, 1970（UTC/GMT 午夜）以来经过的秒数。该时间不包括闰秒（在 ISO 8601 中：1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 设置为 **true** 可在配置文件创建期间跳过加密。设置为 **false** 可在配置文件创建期间强制加密。

典型的 JSON 如下所示：



```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": [redacted]
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

使用任何 JSON 验证工具（例如 https://jsonlint.com）验证创建的 JSON。使用任何在线 QR 码生成器将该 JSON 字符串转换为 QR 码。

此 QR 码由恢复出厂设置的设备扫描，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，设备必须处于恢复出厂设置状态。

1. 在欢迎屏幕上轻按六次以启动 QR 码注册流程。
2. 出现提示时，连接到 Wi-Fi。QR 码中（在 JSON 中编码）Citrix Secure Hub 的下载位置可通过此 Wi-Fi 网络访问。

   设备成功连接到 Wi-Fi 后，它会从 Google 下载一个 QR 码阅读器并启动相机。
3. 将相机对准 QR 码以扫描该码。

   Android 从 QR 码中的下载位置下载 Citrix Secure Hub，验证签名证书签名，安装 Citrix 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 适用于 Android EMM 开发人员的 Google API 文档。

NFC 碰触

使用 NFC 碰触将设备注册为完全托管设备需要两台设备：一台已恢复出厂设置的设备，以及一台运行 Citrix Endpoint Management 预配工具的设备。

先决条件：

- 支持的 Android 设备
- 已启用 Android Enterprise 的 Citrix 端点管理

- 一台新设备或已恢复出厂设置的设备，已为 Android Enterprise 预配为完全托管设备。您可以在本文后面找到完成此先决条件的步骤。
- 另一台具有 NFC 功能的设备，运行已配置的预配工具。预配工具可在 Citrix Secure Hub 中或 Citrix 下载页面 上获取。

每台设备只能有一个由企业移动性管理 (EMM) 应用程序管理的 Android Enterprise 配置文件。在 Citrix Endpoint Management 中，Citrix Secure Hub 是 EMM 应用程序。每台设备只允许一个配置文件。尝试添加第二个 EMM 应用程序会删除第一个 EMM 应用程序。

通过 NFC 碰触传输的数据

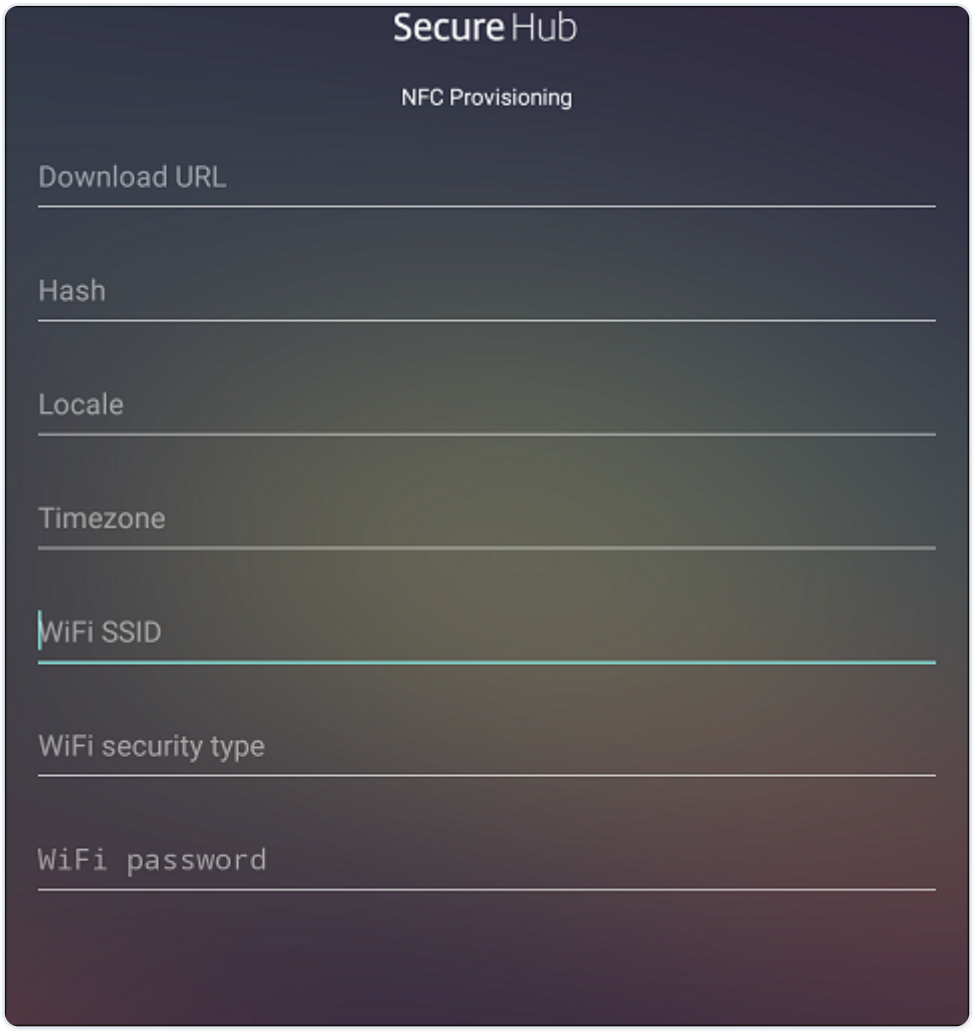
预配已恢复出厂设置的设备需要您通过 NFC 碰触发送以下数据以初始化 Android Enterprise：

- 作为设备所有者的 EMM 提供程序应用程序的包名称（在本例中为 Citrix Secure Hub）。
- 设备可从中下载 EMM 提供程序应用程序的内网/互联网位置。
- EMM 提供程序应用程序的 SHA-256 哈希值，以验证下载是否成功。
- Wi-Fi 连接详细信息，以便已恢复出厂设置的设备可以连接并下载 EMM 提供程序应用程序。注意：Android 现在不支持此步骤的 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

当两台设备碰撞时，预配工具中的数据将发送到恢复出厂设置的设备。然后，该数据用于下载具有管理员设置的 Citrix Secure Hub。如果您不输入时区和位置值，Android 会自动在新设备上配置这些值。

配置 CITRIX ENDPOINT MANAGEMENT 预配工具

在进行 NFC 碰撞之前，您必须配置预配工具。此配置随后会在 NFC 碰撞期间传输到恢复出厂设置的设备。



您可以将数据键入必填字段，也可以通过文本文件填充这些字段。以下过程中的步骤介绍了如何配置文本文件以及每个字段的说明。应用程序在您键入信息后不会保存信息，因此您可能需要创建一个文本文件来保留信息以备将来使用。

要使用文本文件配置预配工具

将文件命名为 nfcprovisioning.txt，并将文件放置在设备 SD 卡上的 **/sdcard/** 文件夹中。然后，应用程序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>`

此行是 EMM 提供商应用程序的内网/互联网位置。恢复出厂设置的设备在 NFC 碰撞后连接到 Wi-Fi 后，必须能够访问此位置以下载。URL 是常规 URL，无需特殊格式。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

此行是 EMM 提供商应用程序的校验和。此校验和用于验证下载是否成功。获取校验和的步骤将在本文稍后讨论。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

此行是运行预配工具的设备上已连接的 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，则此字段必须为空。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

如果 Wi-Fi 未受保护，则此字段必须为空。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

输入语言和国家/地区代码。语言代码是 ISO 639-1 定义的两位小写 ISO 语言代码（例如 en）。国家/地区代码是 ISO 3166-1 定义的两位大写 ISO 国家/地区代码（例如 US）。例如，输入 en_US 表示在美国使用的英语。如果您不输入任何代码，国家/地区和语言将自动填充。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

设备运行所在的时区。键入区域/位置的数据库名称。例如，输入 **America/Los_Angeles** 表示太平洋时间。如果您不键入名称，时区将自动填充。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

此数据不是必需的，因为该值已作为 Citrix Secure Hub 硬编码到应用程序中。此处提及仅为完整性考虑。

如果存在使用 WPA2 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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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

Citrix Secure Hub 的校验和是一个常量值：`qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。要下载 Citrix Secure Hub 的 APK 文件，请使用以下 Google Play 商店链接：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

获取应用程序校验和

先决条件：

- 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，请按照以下步骤操作：

1. 从 Google Play 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 -- '+/=' '-_'
   ```

   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":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-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"

   }

}
```

使用的库

预配工具在其源代码中使用了以下库：

- v7 `appcompat` 库、设计支持库和 v7 调色板支持库

  有关信息，请在 Android 开发者文档 中查找“支持库功能指南”。
- Jake Wharton 的 Butter Knife，根据 Apache 2.0 许可证发布

在 Android Enterprise 中配置工作配置文件设备

在 Android Enterprise 的工作配置文件设备上，您可以安全地将设备上的公司区域和个人区域分开。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 Citrix Endpoint Management 中的 Android 注册类似。用户从 Google Play 下载 Citrix Secure Hub 并注册其设备。

默认情况下，当设备作为工作配置文件设备注册到 Android Enterprise 时，设备上的 USB 调试和未知来源设置处于禁用状态。

提示：

将设备作为工作配置文件设备注册到 Android Enterprise 时，请务必前往 Google Play。在那里，启用 Citrix Secure Hub 以显示在用户的个人配置文件中。

Android 操作系统

> **注意：**
>
> 本文不适用于通过 Android Enterprise 管理的设备。有关这些设备的信息，请参阅本节中的其他文章。

> Citrix Endpoint Management 还支持未通过 Android 或 Samsung 企业计划管理的 Android OS 设备。要控制 Android 设备连接到 Citrix 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。

注册配置文件决定 Android 设备是注册到 MAM、MDM 还是 MDM+MAM，用户可以选择退出 MDM。Citrix Endpoint Management 支持 MDM+MAM 中 Android 设备的以下身份验证类型。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

另一种不常用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 设备管理的通用工作流程如下：

1. 完成入门过程。请参阅 入门和资源设置 和 准备注册设备和交付资源。
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

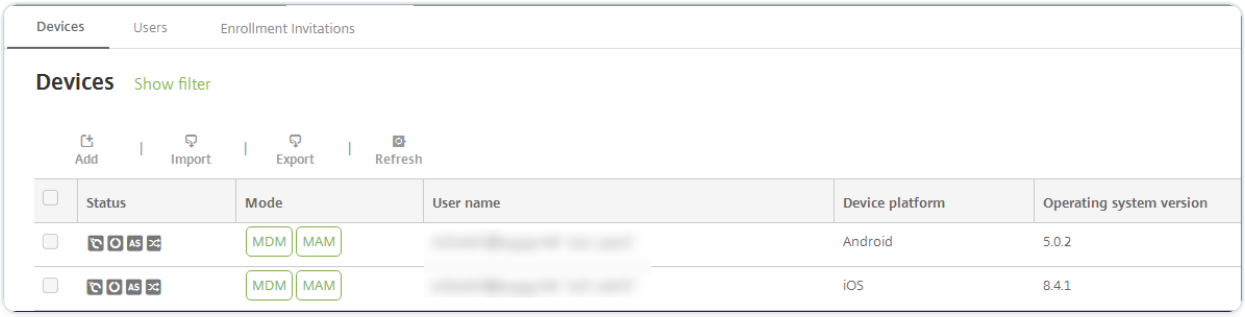
下表列出了 Citrix Endpoint Management 支持的 Android 设备注册方法：

方法	受支持
批量注册	否
手动注册	是
注册邀请	是

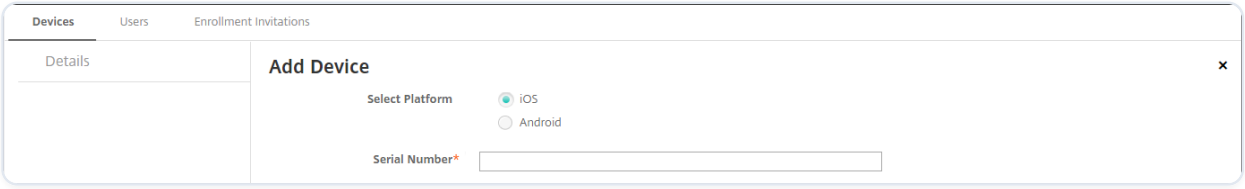
手动添加 Android 设备

如果要手动添加 Android 或 iOS 设备（例如用于测试目的），请按照以下步骤操作。

1. 在 Citrix 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。



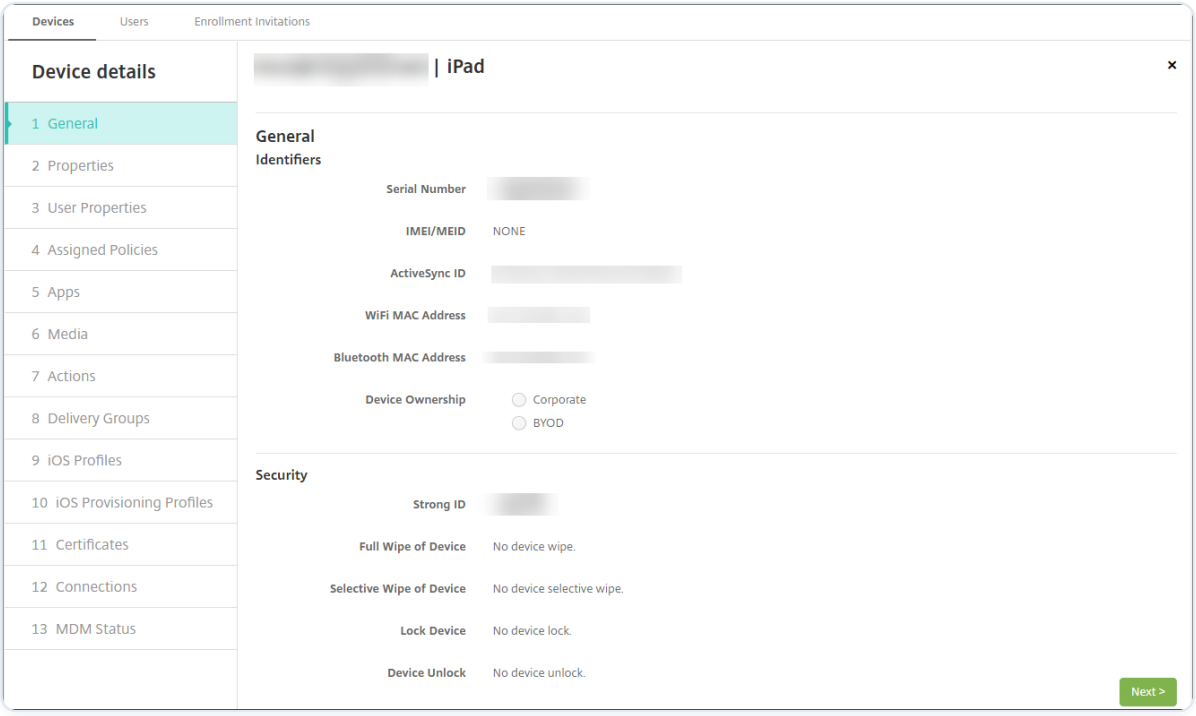
3. 配置以下设置：

   - **选择平台**：点击 **Android**。
   - **序列号**：键入设备序列号。
   - **IMEI/MEID**：可选，键入设备 IMEI/MEID 信息。

4. 点击 **添加**。**设备** 表将显示，其中设备已添加到列表底部。要查看并确认设备详细信息：选择您添加的设备，然后在出现的菜单中点击 **编辑**。

> **注意：**
>
> 当您选中设备旁边的复选框时，选项菜单会出现在设备列表上方。当您点击列表中的其他任何位置时，选项菜单会出现在列表的右侧。

- 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。
  - 交付组与本地组关联。
- 如果使用 Active Directory：
  - 交付组与 Active Directory 组关联。



5. **常规** 页面列出了设备**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、激活锁绕过以及平台类型的其他信息。“**完全擦除设备**”字段包含用户 PIN 码。设备擦除后，用户必须输入该代码。如果用户忘记了代码，您可以在此处查找。

6. **属性**页面列出了 Citrix Endpoint Management 将要预配的设备属性。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个属性。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，它最初会显示在您添加它的类别下。单击**下一步**并返回到**属性**页面后，该属性将显示在相应的列表中。

要删除属性，请将鼠标悬停在列表项上，然后单击右侧的 **X**。Citrix 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 RBAC 角色、组成员身份、托管 Google Play 帐户以及用户的属性。您可以从此页面停用托管 Google Play 帐户。
   - **分配的策略：**显示已部署、待处理和失败的策略数量。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待处理，并重新部署用户已删除的策略。
   - **应用程序：**显示上次盘点中已安装、待处理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 盘点键（例如 **HasUpdateAvailable**）的说明，请参阅 移动设备管理 (MDM) 协议。
   - **媒体：**显示上次盘点中已部署、待处理和失败的媒体部署数量。
   - **操作：**显示已部署、待处理和失败的操作数量。提供操作名称和上次部署时间。
   - **交付组：**显示成功、待处理和失败的交付组数量。对于每次部署，提供交付组名称和部署时间。选择一个交付组以查看更详细的信息，包括状态、操作以及渠道或用户。
   - **iOS 配置文件：**显示上次 iOS 配置文件盘点，包括名称、类型、组织和描述。
   - **iOS 预配配置文件：**显示企业分发预配配置文件信息，例如 UUID、过期日期和托管状态。
   - **证书：**显示有效、已过期或已吊销证书的信息，例如类型、提供商、颁发者、序列号以及过期前的剩余天数。
   - **连接：**显示首次连接状态和上次连接状态。为每个连接提供用户名、倒数第二次（上次）身份验证时间和上次身份验证时间。
   - **MDM 状态：**显示 MDM 状态、上次推送时间和上次设备回复时间等信息。

配置 Android 设备策略

使用这些策略配置 Citrix Endpoint Management 如何与运行 Android 的设备交互。此表列出了适用于 Android 设备的所有设备策略。

APN	应用访问	应用清单
应用锁定	应用卸载	凭据
Citrix 端点管理选项	Citrix 端点管理卸载	文件
启动器配置	位置	网络

密码	限制	计划
商店	条款和条件	隧道
VPN	Web 剪辑	

注册 Android 设备

1. 在您的 Android 设备上前往 Google Play 商店，下载 Citrix Secure Hub 应用程序，然后点击该应用程序。
2. 当系统提示安装应用程序时，点击**下一步**，然后点击**安装**。
3. Citrix Secure Hub 安装完成后，点击**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：
   - 允许 Citrix Secure Hub 拨打和管理电话？（必需）
   - 允许 Citrix Secure Hub 访问您设备上的照片、媒体和文件？（必需）
   - 允许 Citrix Secure Hub 访问此设备的位置？（可选）
5. 输入您的企业凭据，例如 Citrix 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：
   - 要注册 MDM+MAM，请点击 **是，注册**。
   - 要注册 MAM，请点击 **否**。
7. 在 **激活设备管理员** 屏幕中，点击 **激活**。
8. 输入您的企业密码，然后点击 **登录**。
9. 根据 Citrix Endpoint Management 的配置方式，系统可能会要求您创建 Citrix PIN。您可以使用该 PIN 登录 Citrix Secure Hub 和其他支持 Citrix Endpoint Management 的应用程序，例如 Citrix Secure Mail 和 Citrix Files。您需要输入两次 Citrix PIN。在 **创建 Citrix PIN** 屏幕中，输入一个 PIN。
10. 重新输入 PIN。Citrix Secure Hub 将打开。然后，您可以访问应用商店以查看可在 Android 设备上安装的应用。
11. 如果您已将 Citrix Endpoint Management 配置为在注册后自动将应用程序推送到设备，则系统会提示用户安装这些应用程序。此外，您在 Citrix Endpoint Management 中配置的策略也会部署到设备。点击 **安装** 以安装应用程序。

注销并重新注册 Android 设备

用户可以从 Citrix Secure Hub 中注销。当用户使用以下过程注销时，设备仍会显示在 Citrix Endpoint Management 控制台的设备清单中。但是，您无法对设备执行操作。例如，您无法跟踪设备或监控设备合规性。

1. 点击以打开 Citrix Secure Hub 应用程序。
2. 根据您使用的是手机还是平板电脑，执行以下操作：

   在手机上：

   - 从屏幕左侧滑动以打开设置窗格。
   - 轻按**首选项**，轻按**帐户**，然后轻按**删除帐户**。

   在平板电脑上：

   - 轻按右上角电子邮件地址旁边的箭头。
   - 轻按**首选项**，轻按**帐户**，然后轻按**删除帐户**。

3. 在**删除帐户?窗口中，轻按是，删除**。 Citrix Secure Hub 将取消注册您的设备。按照屏幕上的说明重新注册您的设备。

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	定位	锁定
锁定并重置密码	通知	撤销
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期间授予位置权限。用户可以选择不授予位置权限。如果用户在注册期间未授予该权限，Citrix Endpoint Management 会在发送“定位”命令时再次请求位置权限。

Firebase 云消息传递

> **注意：**
>
> Firebase Cloud Messaging (FCM) 以前称为 Google Cloud Messaging (GCM)。某些 Citrix Endpoint Management 控制台标签和消息使用 GCM 术语。

> Citrix 建议您使用 Firebase Cloud Messaging (FCM) 来控制 Android 设备连接到 Citrix Endpoint Management 的方式和时间。Citrix Endpoint Management 在配置为 FCM 时，会向已启用 FCM 的 Android 设备发送连接通知。任何安全操作或部署命令都会触发推送通知，以提示用户重新连接到 Citrix Endpoint Management 服务器。

完成本文中的配置步骤并且设备签入后，设备会在 Citrix Endpoint Management 中向 FCM 服务注册。该连接通过使用 FCM 实现了从 Citrix Endpoint Management 服务到设备的近实时通信。FCM 注册适用于新设备注册和以前注册的设备。

当 Citrix Endpoint Management 需要启动与设备的连接时，它会连接到 FCM 服务。然后，FCM 服务会通知设备进行连接。这种连接类型类似于 Apple 用于其推送通知服务的方式。

先决条件

- 最新 Citrix Secure Hub 客户端
- Google 开发者帐户凭据
- 在启用 FCM 的 Android 设备上安装 Google Play 服务

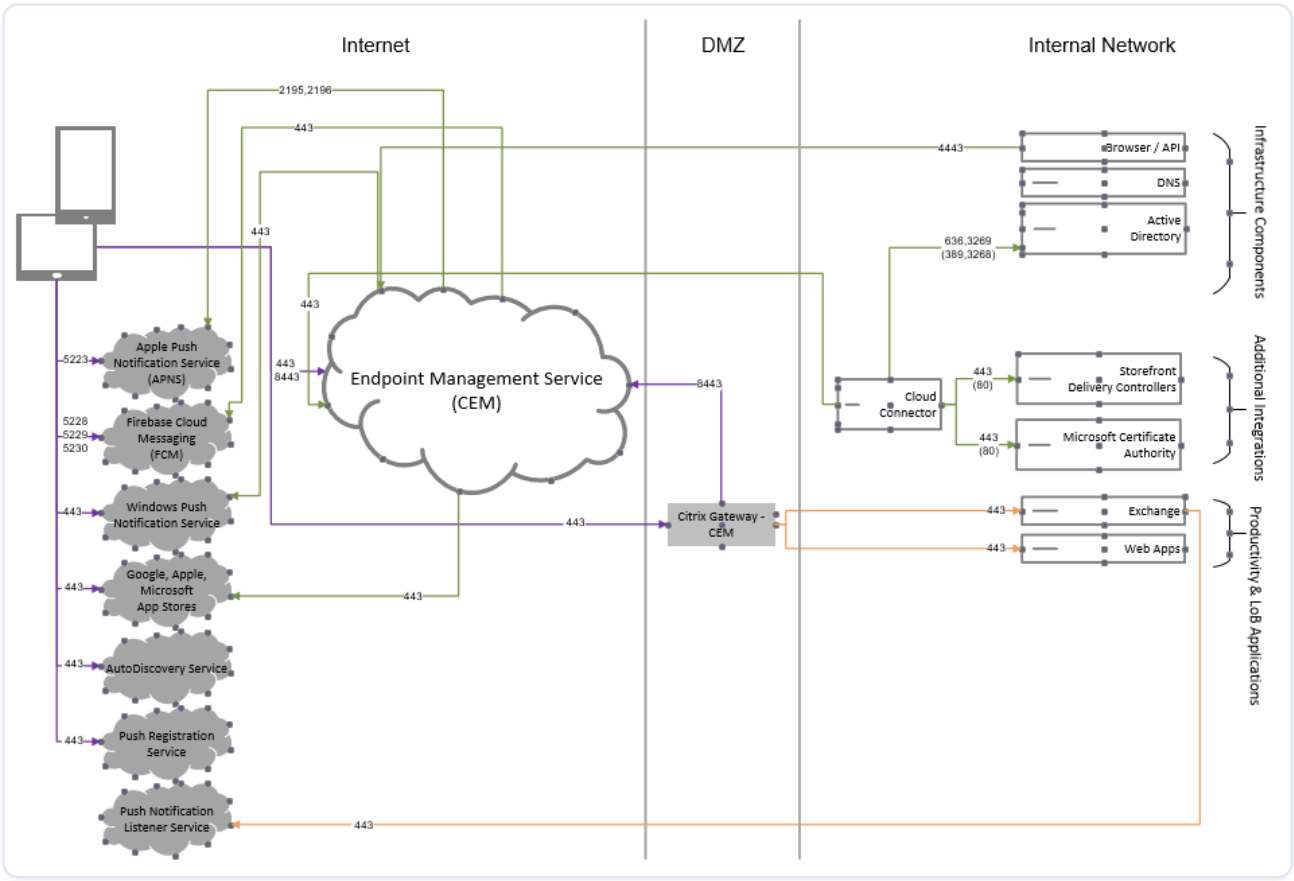
防火墙端口

- 在 Citrix Endpoint Management 上打开端口 443 以连接到 `fcm.googleapis.com` 和 `Google.com`。
- 为设备 Wi-Fi 打开端口 5228、5229 和 5230 上的出站 Internet 通信。
- 为了允许出站连接，FCM 建议将端口 5228 到 5230 添加到允许列表，且不设 IP 限制。但是，如果需要 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。这些块列在 Google ASN of 15169 中。每月更新该列表。

有关详细信息，请参阅 端口要求。

架构

此图显示了 FCM 在外部和内部网络中的通信流。

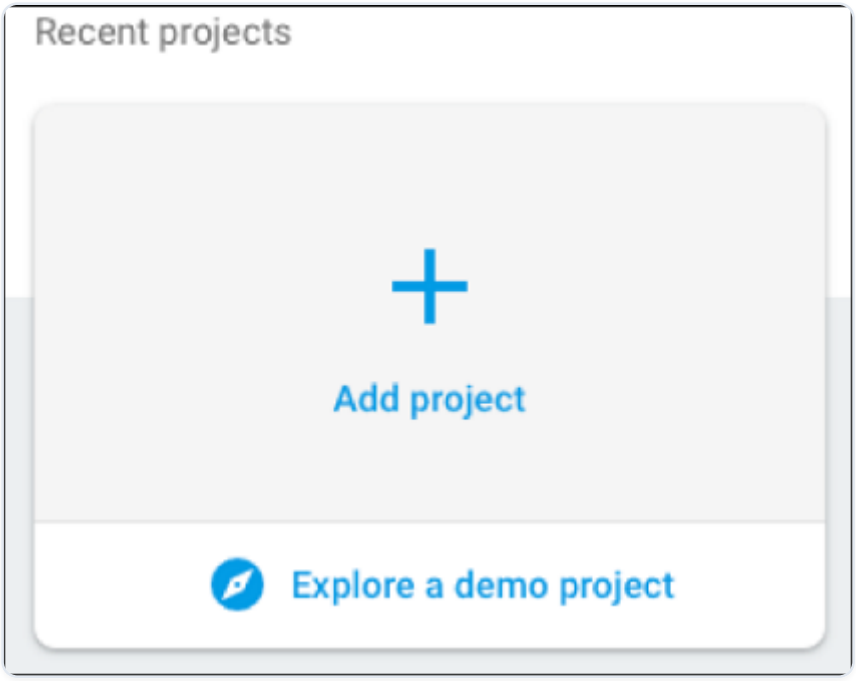


为 FCM 配置您的 Google 帐户

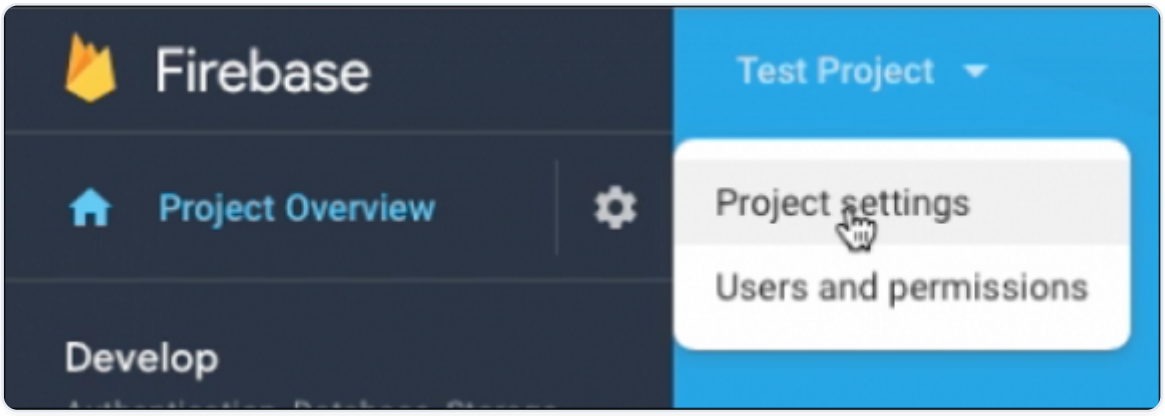
1. 使用您的 Google 开发者帐户凭据登录以下 URL：

   `<https://console.firebase.google.com/>`

2. 单击“**添加项目**”。



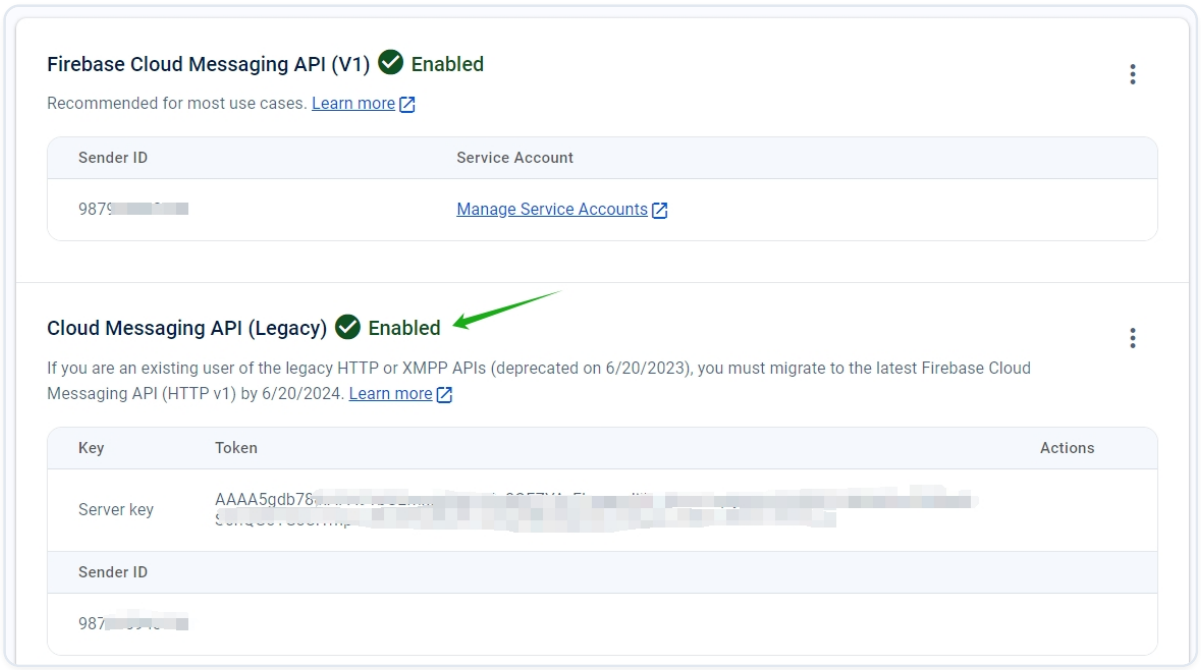
3. 创建项目后，单击“**项目设置**”。



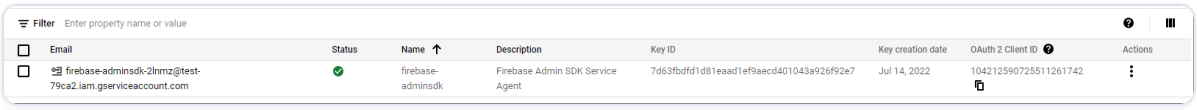
> **注意：**
>
> Google 将弃用用于 HTTP 的 FCM 旧版 API，该 API 目前在我们的 FCM 实现中使用。迁移截止日期为 June 21, 2024。我们需要将 FCM 从旧版 FCM API 迁移到 HTTP v1 API。有关详细信息，请参阅从旧版 FCM API 迁移到 HTTP v1。

4. 单击“**云消息传递**”选项卡。验证 Firebase Cloud Messaging API 已启用，然后单击“**管理服务帐户**”。

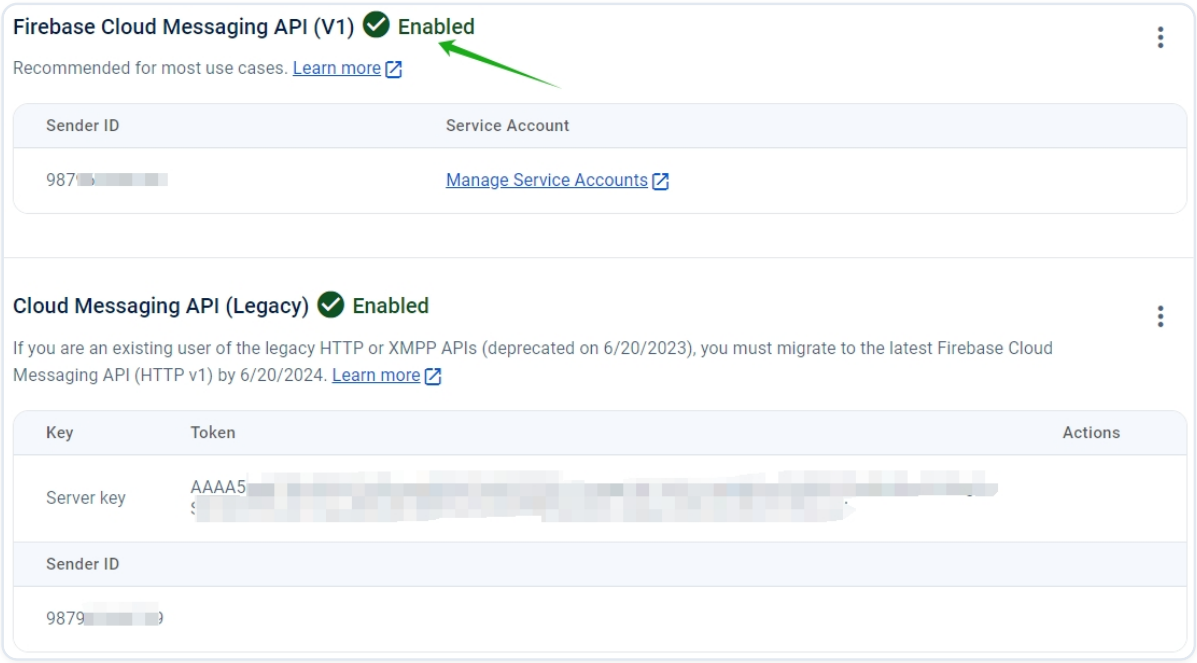
   a. 迁移之前，您可以使用旧版 API，请确保已启用 Cloud Messaging API（旧版）。从“**密钥**”和“**发件人 ID**”字段复制值。



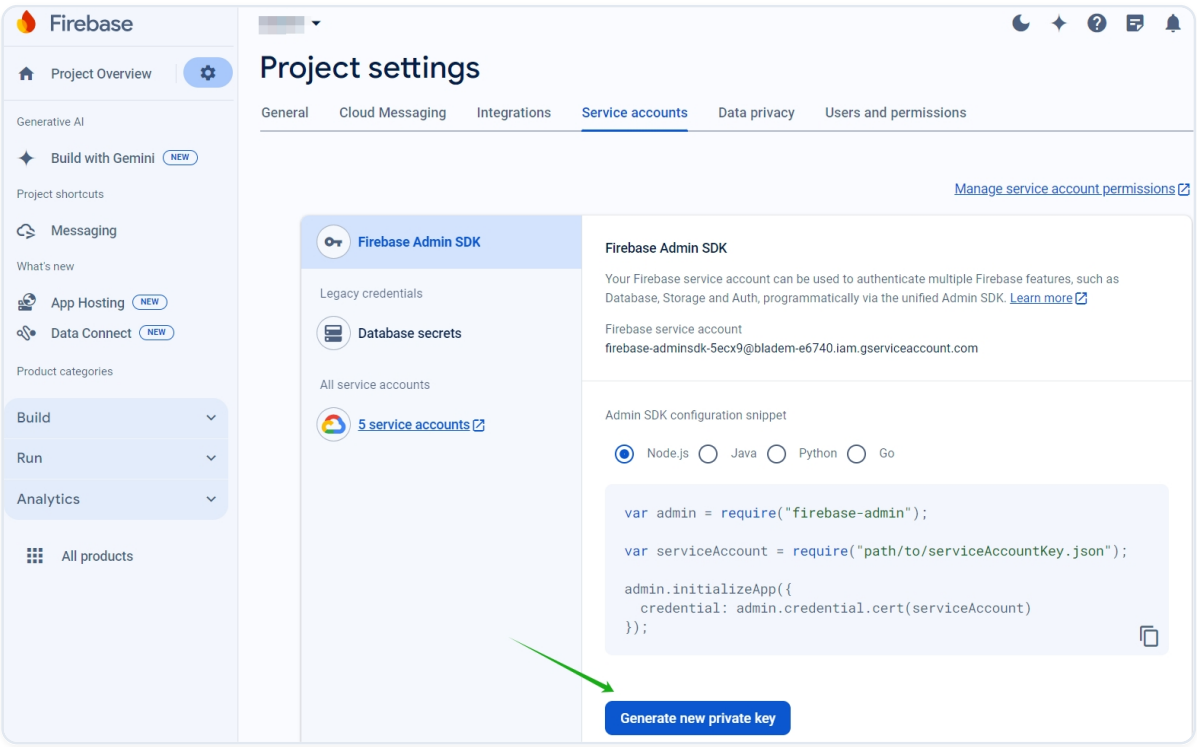
   如果未列出密钥，请单击“**操作**”下的省略号以添加密钥。



b. 迁移后，Google 将弃用旧版 API。您必须启用 Firebase Cloud Messaging API (V1)。有关详细信息，请参阅从旧版 FCM API 迁移到 HTTP v1。



从“**项目设置**”下的“**服务帐户**”下载服务帐户 JSON 文件。请参阅手动提供凭据部分，为您的服务帐户生成私钥文件。单击“**生成新私钥**”以下载服务帐户密钥 JSON 文件。



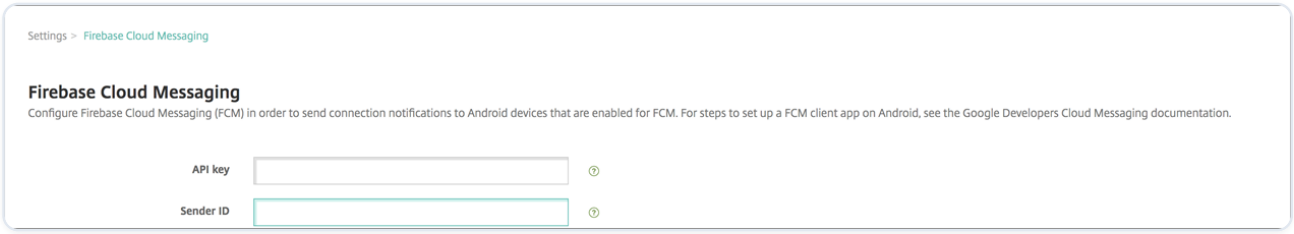
有关在 Android 上设置 FCM 客户端应用程序的步骤，请参阅此 Google Developers Cloud Messaging 文章：`<https://firebase.google.com/docs/cloud-messaging/android/client>`。

配置 Citrix Endpoint Management 以使用 FCM

在 Citrix Endpoint Management 控制台中，转到 **设置 > Firebase Cloud Messaging**。

对于 Cloud Messaging API（旧版）

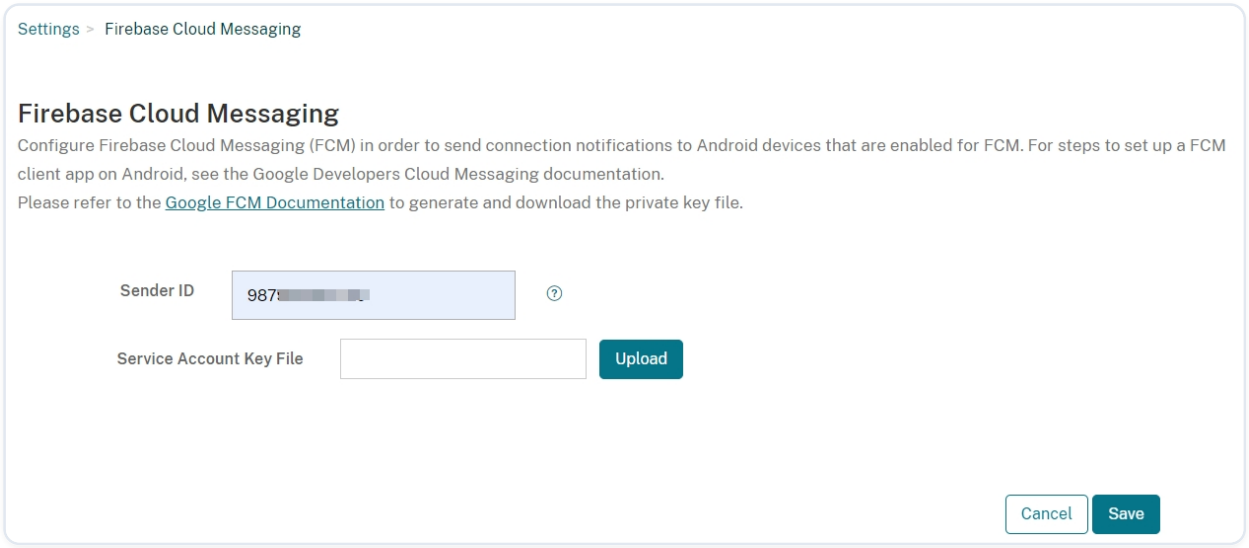
1. 在 **API 密钥**字段中输入 Firebase Cloud Messaging 配置最后一步中的 Firebase Cloud Messaging **密钥**。
2. 输入上一步骤中的 **发件人 ID** 值。



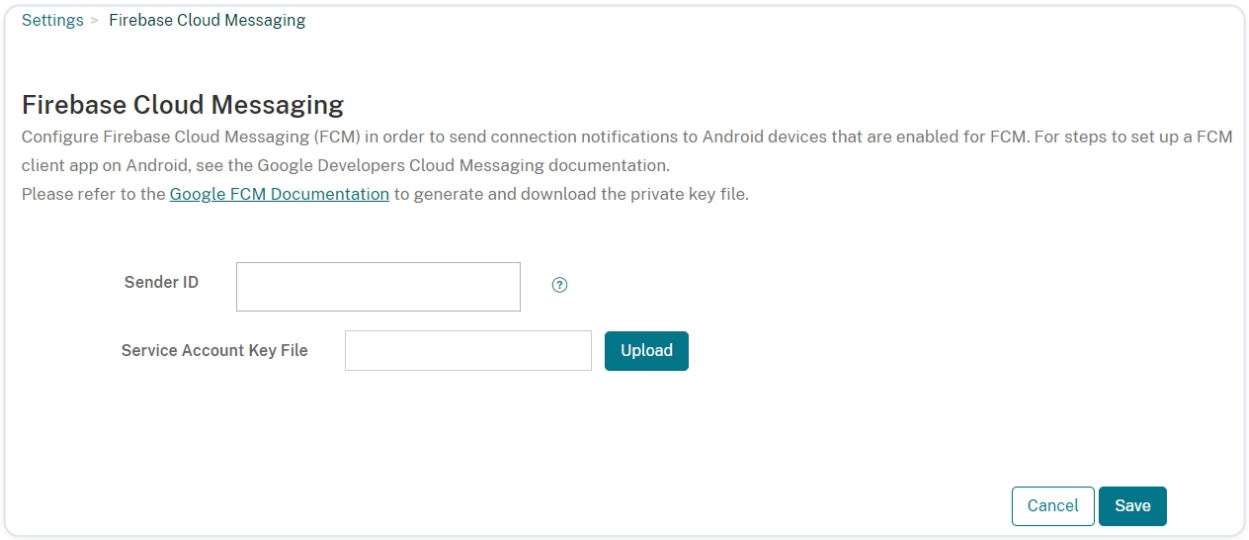
适用于 Firebase 云消息传递 API (V1)

> **注意：**
>
> - 要为 Citrix Endpoint Management 24.6.0 及更高版本启用 FCM API V1，请参阅知识中心文章 CTX677031。
> - 如果您是新的 FCM 用户，请跳过步骤 1，从步骤 2 开始。

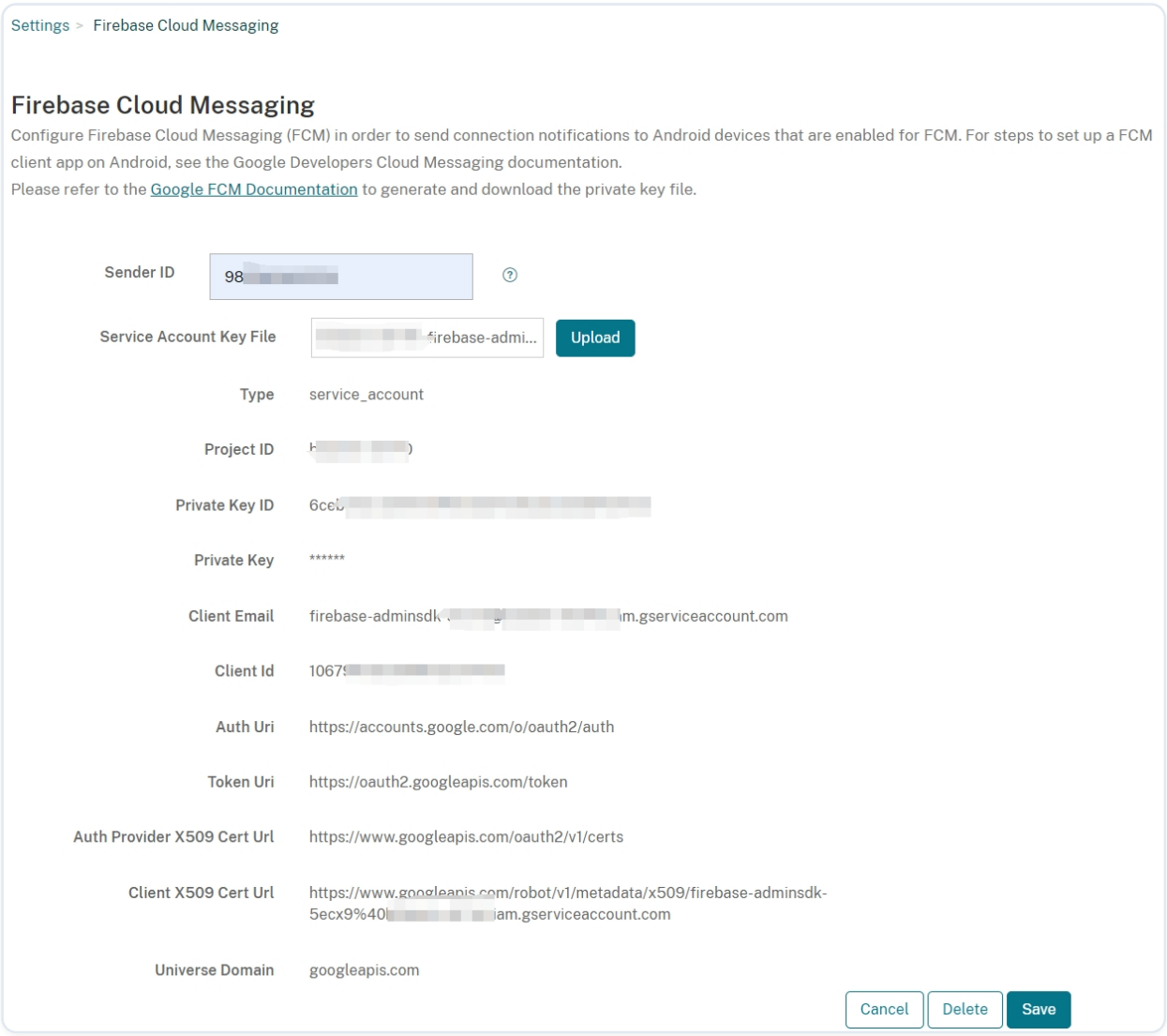
1. 如果您已在使用 FCM，您会注意到发件人 ID 会自动填充您当前的 FCM 项目，并且会有一个新选项用于上传 **服务帐户密钥文件**。



2. 如果您是新的 FCM 用户，请输入 **发件人 ID** 并从上一步骤上传 **服务帐户密钥文件**。



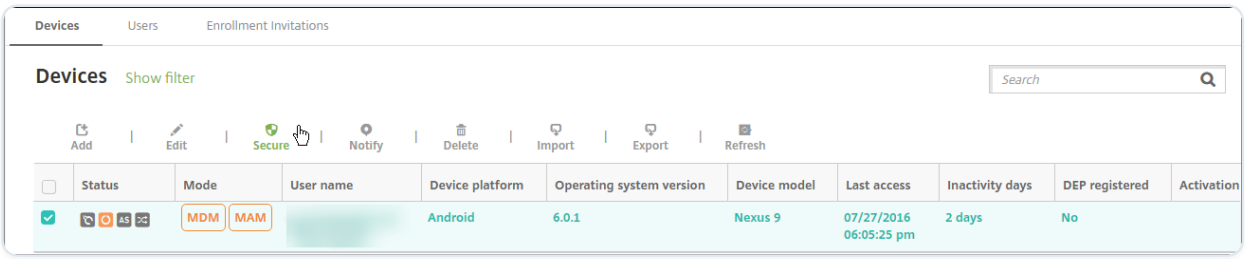
3. 上传的文件将被解析，并且相应的字段将自动生成。



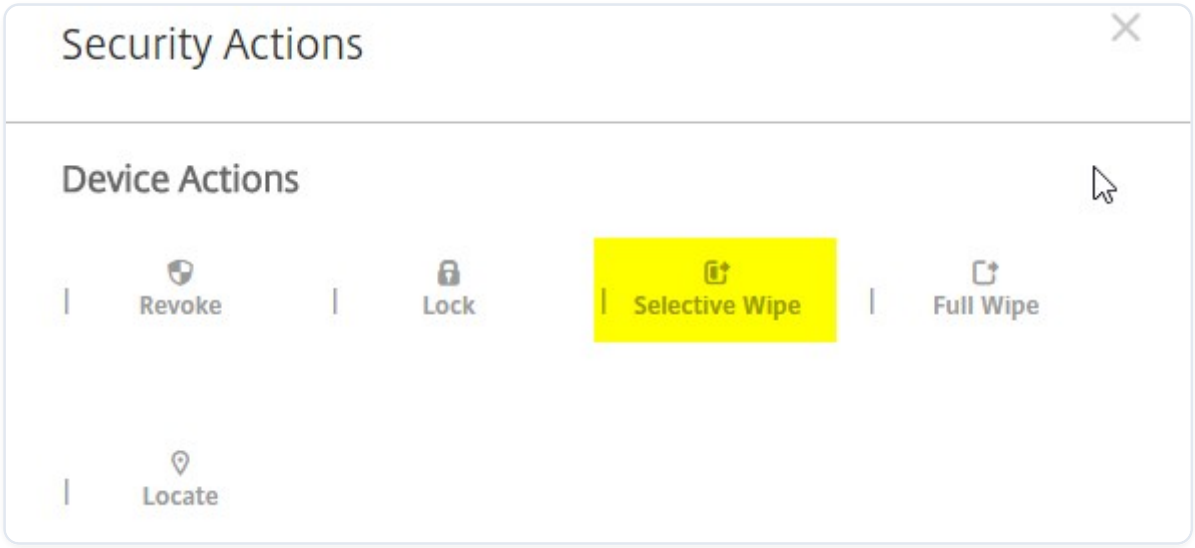
4. 验证信息并点击 **保存**。

测试您的配置

1. 注册一台 Android 设备。
2. 让设备闲置一段时间，使其与 Citrix Endpoint Management 断开连接。
3. 在 Citrix Endpoint Management 控制台中，点击 **管理**，选择 Android 设备，然后点击 **安全**。



4. 在 **设备操作** 下，点击 **选择性擦除**。



如果配置成功，设备上会发生选择性擦除。

支持托管配置反馈（技术预览版）

注意：

技术预览版中的功能可在非生产或有限生产环境中使用，并为客户提供分享反馈的机会。Citrix® 不接受技术预览版功能的任何支持案例，但欢迎提供改进这些功能的反馈。您可以通过单击“**向我们发送您的反馈**”来提供对此功能的反馈。Citrix 可能会根据反馈的严重性、关键性和重要性采取行动。

托管配置反馈功能允许管理员获取来自配置了托管配置策略的 Android 设备的应用程序状态反馈。此反馈可用于监控这些策略的有效性和状态。

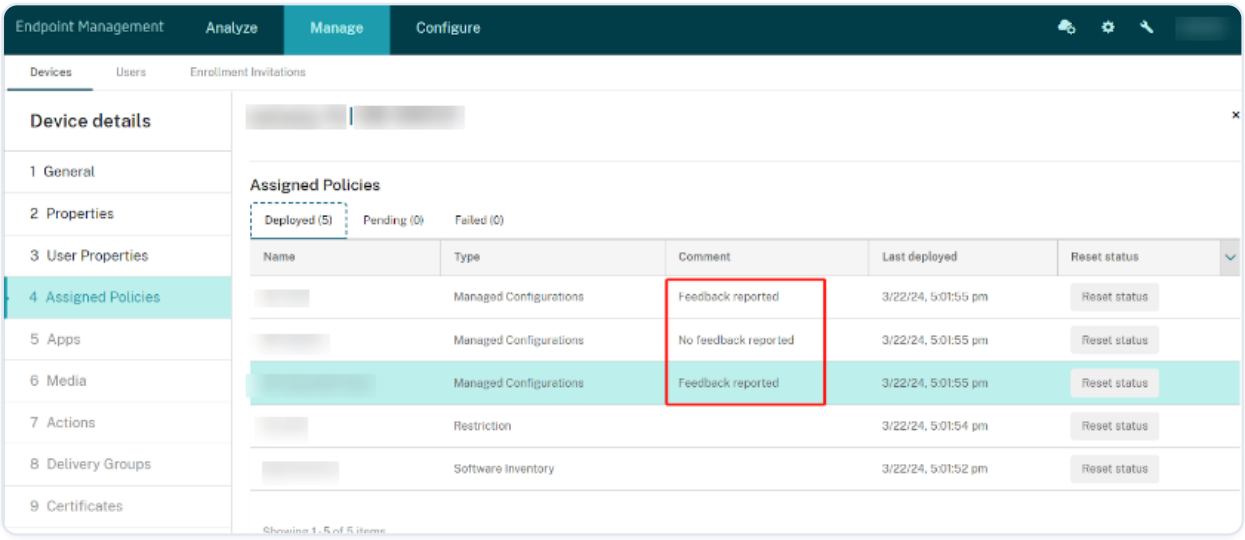
先决条件

1. `App Support`：应用程序必须支持托管配置策略。
2. `Keyed App States`：应用程序还必须支持带键的应用程序状态。有关应用程序反馈如何运作的详细信息，请参阅将应用程序反馈发送到 EMM。

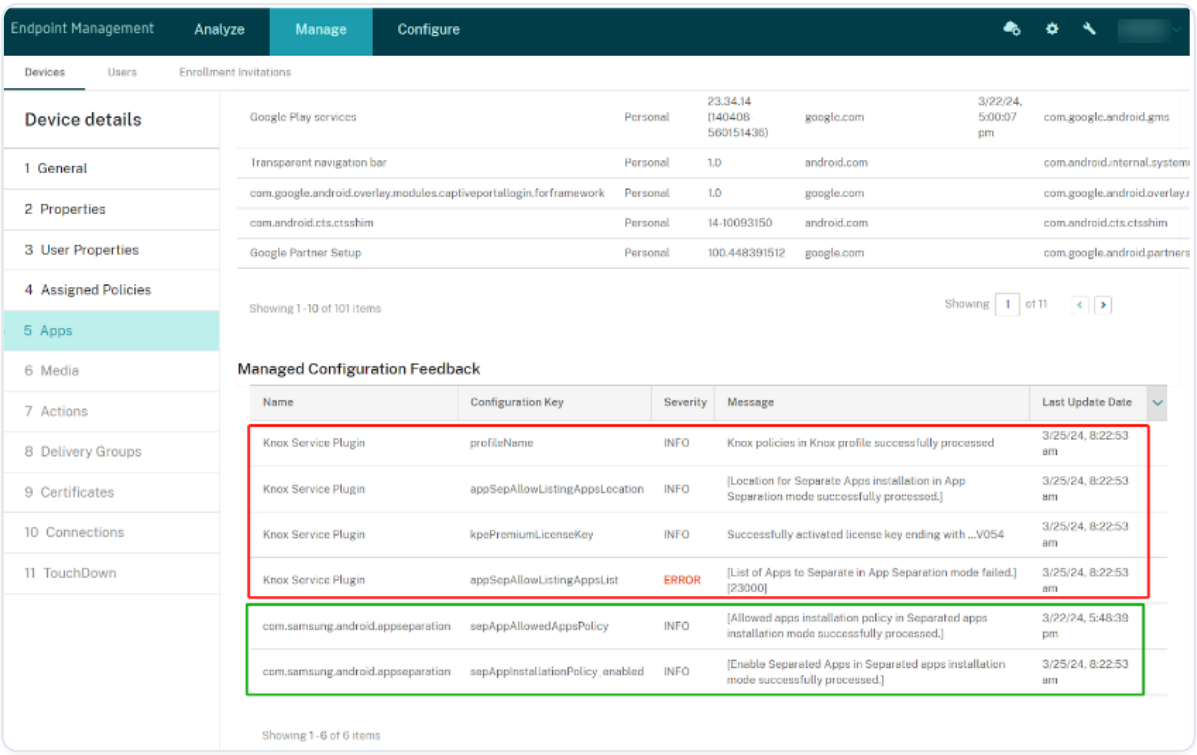
管理和利用配置反馈的步骤

1. 启用功能标志 `afw.app_managed_configurations.feedback` 适用于指定的 (Citrix Endpoint Management) CEM 服务器。
2. 验证托管配置策略。
   - 确认 Android 设备已注册并且托管配置策略已成功应用。

- 导航到“**设备详细信息**”并单击“**已分配策略**”。将显示与托管配置策略相关的注释。
  - **已报告反馈**：表示此策略相关的应用程序有可用反馈。
  - **未报告反馈**：表示此策略相关的应用程序没有报告任何反馈。



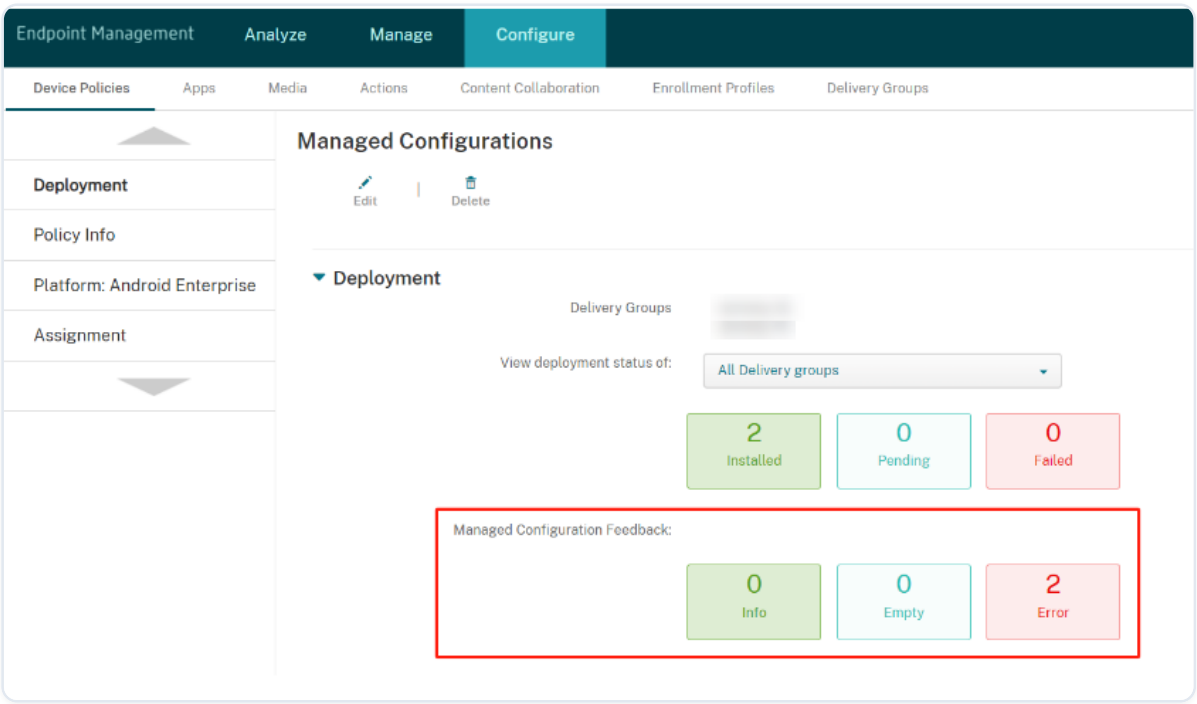
- 导航到“**设备详细信息**”并点击“**应用程序**”。详细反馈显示在“**托管配置反馈**”表下，其中包含所有应用程序数据。



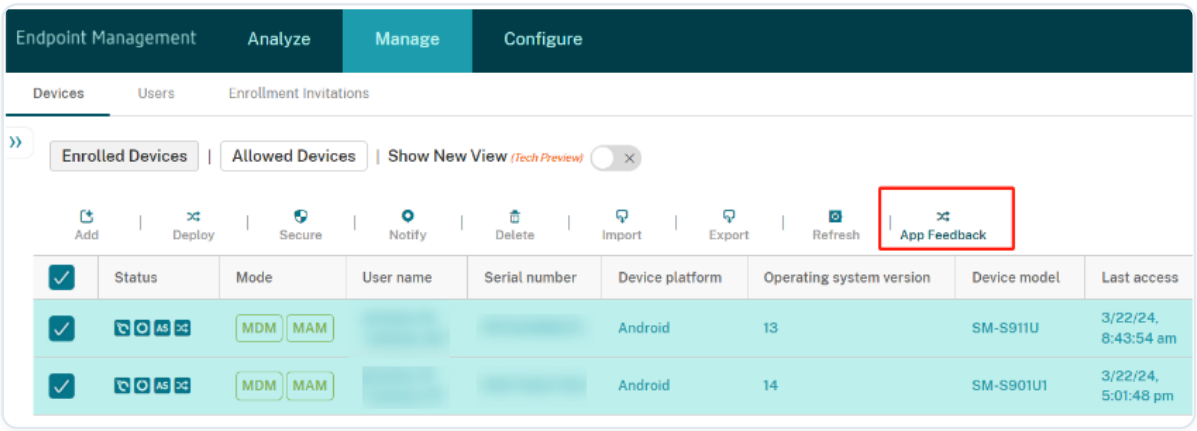
注意：

在上面的屏幕截图中，红色框突出显示了 Know Service 插件，而绿色框则指示了分离的应用程序。

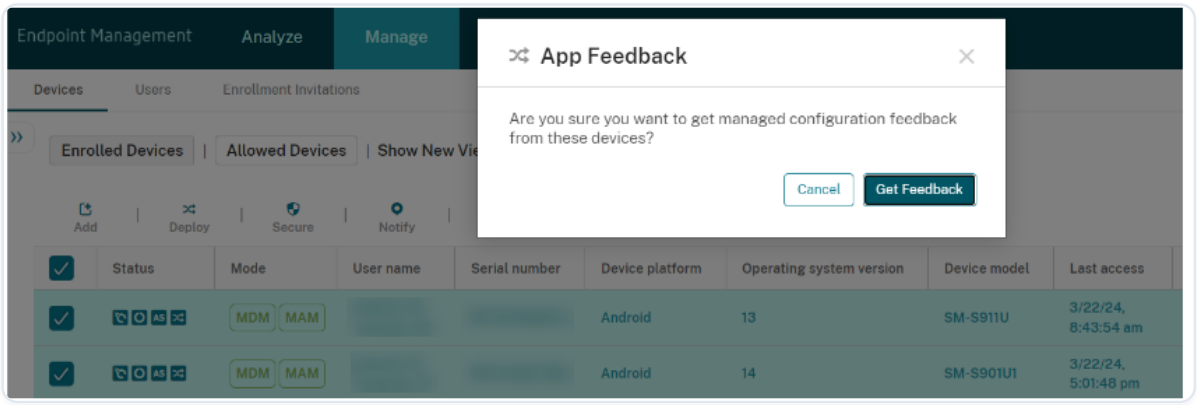
- 对于单个托管配置策略，您可以查看所有已分配设备的反馈详细信息：
  - **信息**：所有报告的反馈数据不包含错误的设备。
  - **错误**：所有报告的反馈数据包含错误的设备。
  - **空**：所有未报告反馈数据的设备。



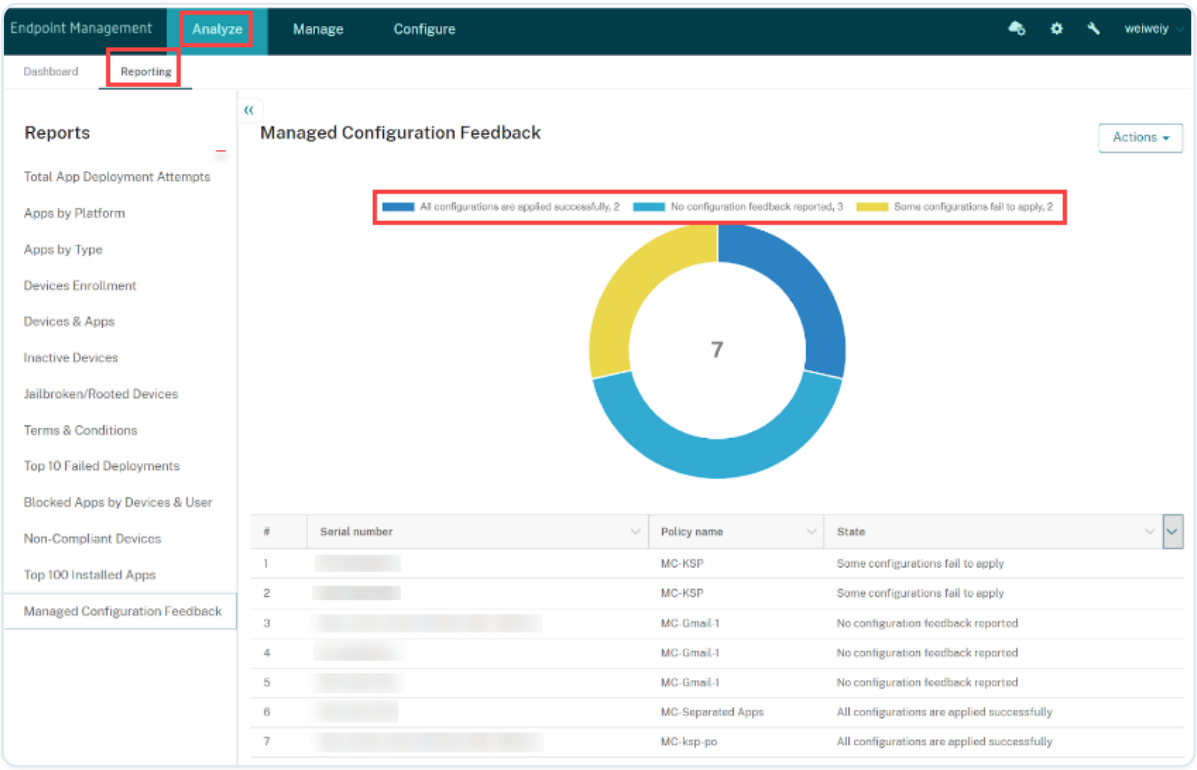
- 要手动获取反馈，请点击“**管理**”并选中复选框以查找相应的设备。例如，您可以选中相应的复选框并点击“**应用程序反馈**”。



- 点击“**获取反馈**”以从选定的设备获取托管配置反馈。



- 从托管配置反馈报告中，选择“**分析**”并点击“**报告**”以获取总体反馈。您可以查看所有设备的报告、管理配置策略以及相关的配置失败。



3. 引入了两个服务器属性以调整反馈计划。使用云管理工具修改这些属性，并控制反馈数据何时保存到数据库。

   a. 用于更新 Android Enterprise 托管配置反馈数据库的批处理大小：

   - 键：`android.managed.configuration.feedback.db.update.batch.size`
   - 您可以定义要存储到数据库的报告的批处理大小，只有存储在数据库中的数据才能在 UI 中显示。默认值为 100，最大值为 1000。

   b. Android Enterprise 托管配置反馈数据库更新时间间隔：

   - 键：`android.managed.configuration.feedback.db.update.time.interval`

- 您可以指定报告在数据库中存储的时长，即使大小未达到批处理限制。默认值为六小时。

故障排除

默认情况下，反馈报告会在每次设备签入期间检索（当 Secure Hub 连接到服务器时）。但是，您可以使用“应用程序反馈”按钮手动获取特定设备的报告。

安卓安全网

您可以使用 Android SafetyNet 功能评估已安装 Citrix 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 会在已通过 Android 兼容性测试的设备型号列表中查找相同的配置文件。API 还会使用此信息来确定未知来源是否修改了 Citrix Secure Hub。

启用 Android SafetyNet 功能后，Citrix Secure Hub 会将 SafetyNet Attestation API 请求发送到 Google Play 服务，结果会报告回 Citrix Endpoint Management。然后，Citrix Endpoint Management 会使用证明结果更新设备信息。您可以设置自动化操作，这些操作使用证明结果来触发设备上的操作。

有关 SafetyNet Attestation API 工作原理的更多信息，请参阅Android 开发者文档。

估算您需要多少 SafetyNet Attestation API 请求

SafetyNet Attestation API 请求在以下情况下发送：

- 设备注册到 Citrix Endpoint Management 时
- 发生 Citrix Secure Hub 联机身份验证时

  当服务器会话过期或用户从服务器注销然后重新登录时，会发生联机身份验证。Citrix Secure Hub 提示用户提供凭据以向服务器进行身份验证。
- 设备重新启动时
- 在您配置的重复时间间隔内，介于 24 到 1,000 小时之间。

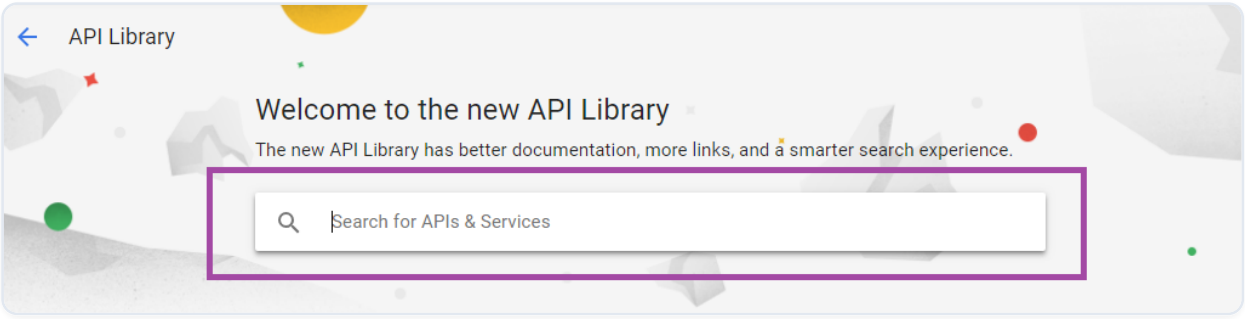
如果您的 Citrix Endpoint Management 部署每天发出超过 10,000 个请求，请填写此配额申请表。

获取 SafetyNet API 密钥

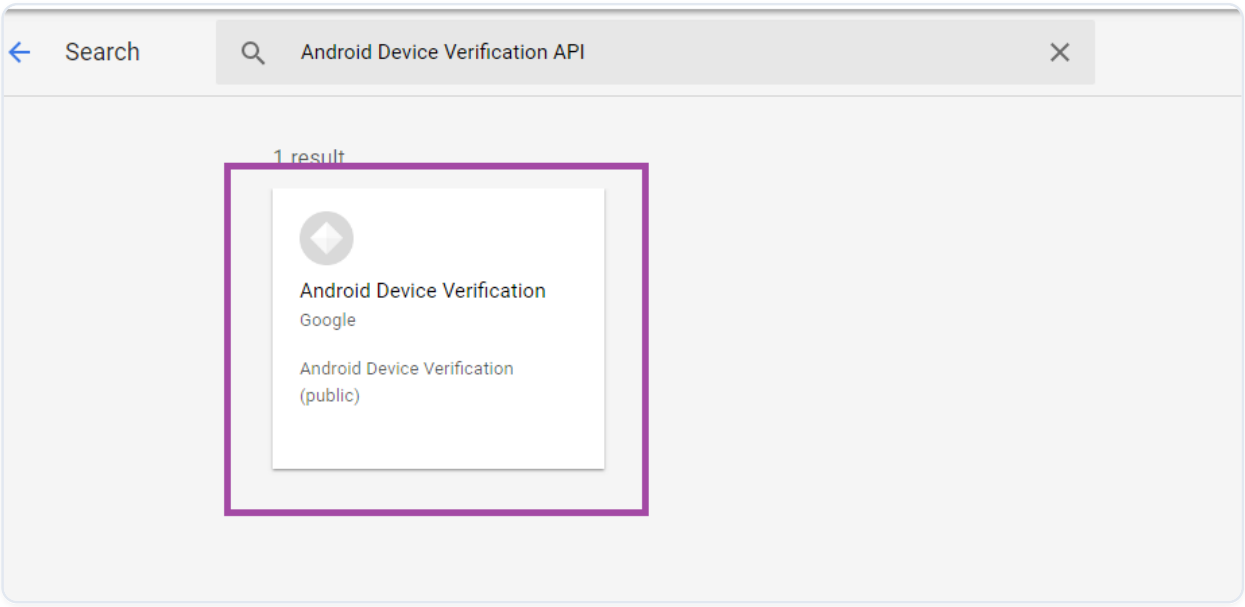
要在 Citrix Endpoint Management 中启用 Android SafetyNet，您需要 **SafetyNet API** 密钥。

1. 使用您的 Google 管理员帐户凭据登录 Google API 控制台。

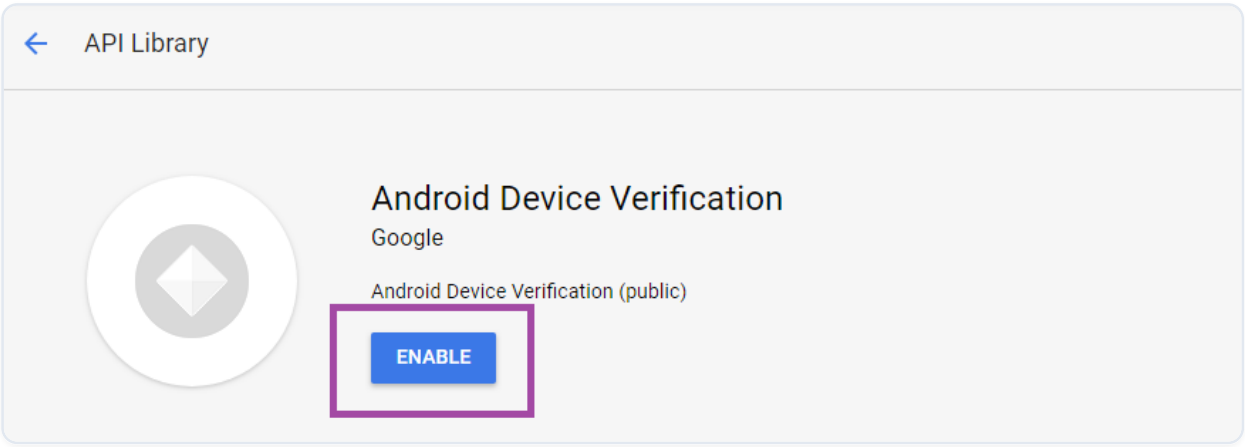
2. 转到“库”页面。
3. 搜索名为“Android Device Verification API”的接口。



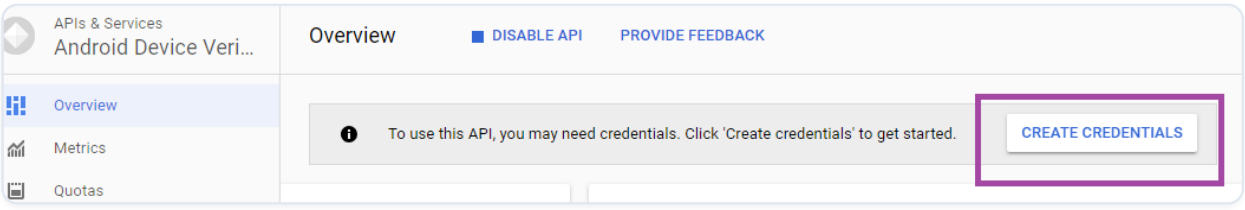
4. 单击名为 **Android Device Verification API** 的接口。



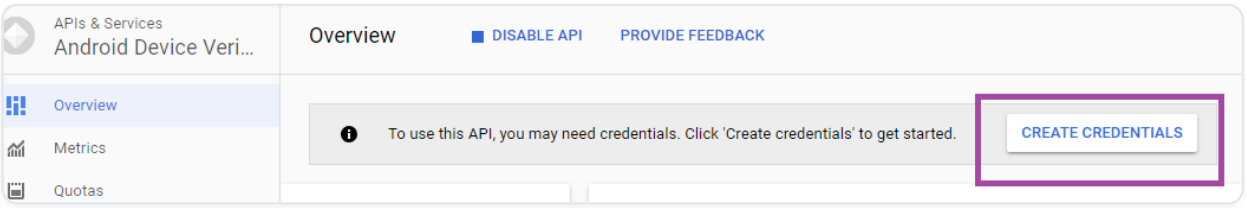
5. 如果 API 尚未启用，请单击**启用**。



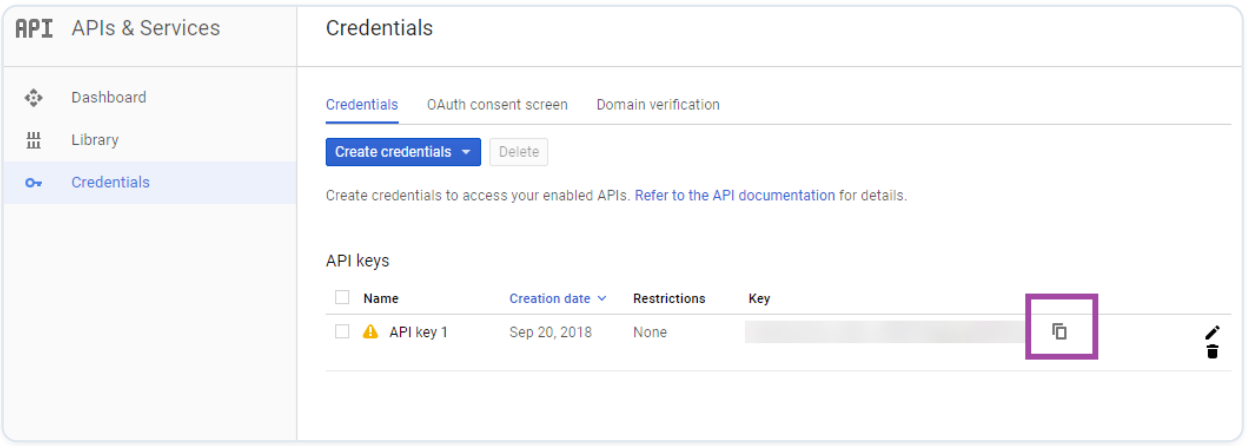
6. 单击**管理**。
7. 单击**创建凭据**以生成 API 密钥。



8. 选择 **Android 设备验证**，单击 **我需要哪些凭据**。然后单击 **完成**。



9. 在**凭据**页面上，单击密钥旁边的复制图标以复制密钥。

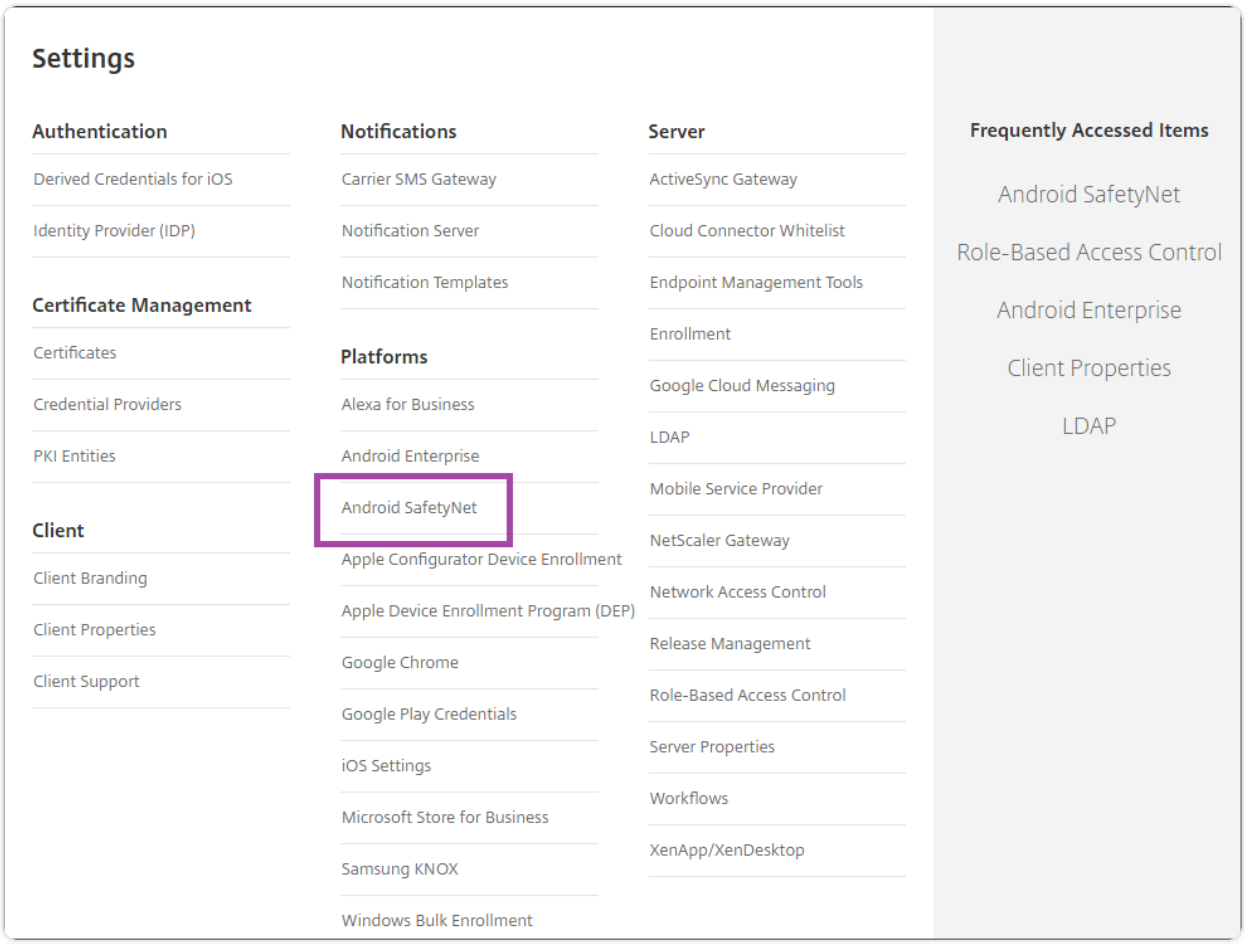


10. 保存密钥，以便在启用 Android SafetyNet 时将其粘贴到 Citrix Endpoint Management 控制台中。

启用 Android SafetyNet

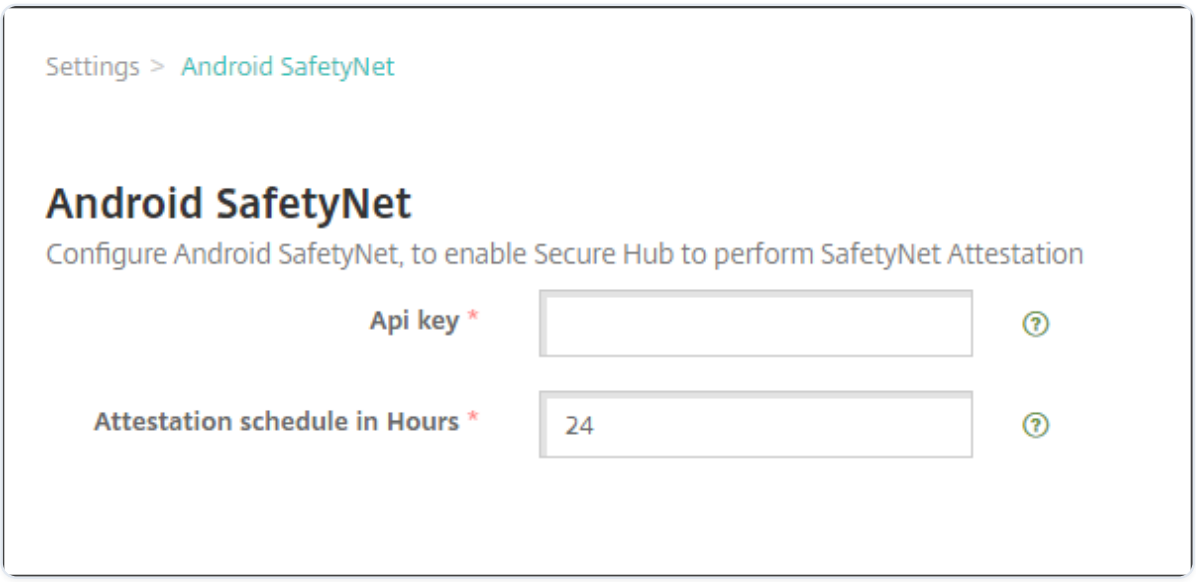
1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示**设置**页面。

2. 在**设置**页面上，单击 **Android 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。
- **证明计划（小时）**。键入 SafetyNet 证明 API 评估 Android 设备的间隔时间（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。

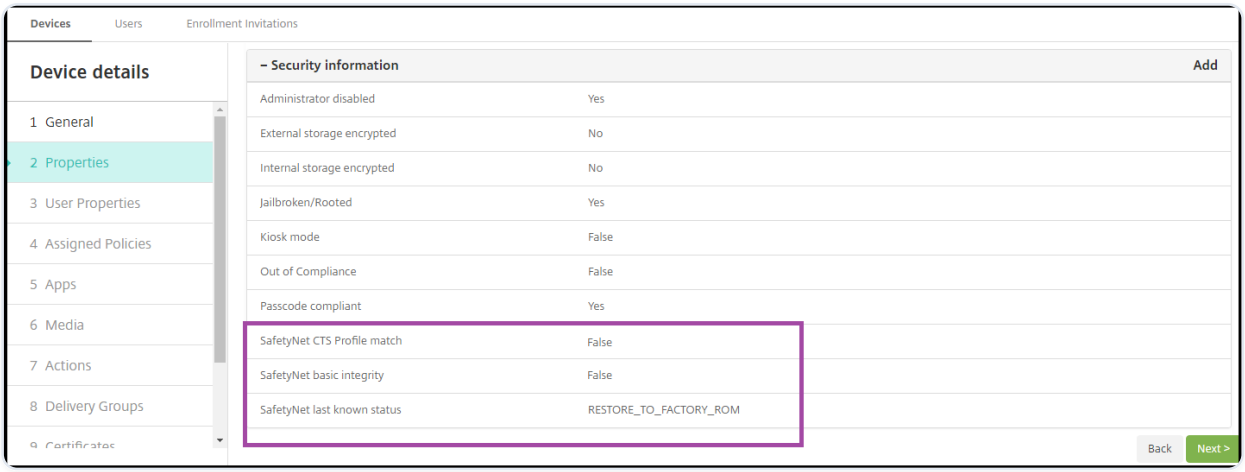


4. 点击 **保存**。

查看 Android SafetyNet 结果

要查看设备的 SafetyNet 证明 API 评估结果，请执行以下操作：

1. 在 Citrix Endpoint Management 控制台中，单击**管理 > 设备**。
2. 选择 Android 设备以查看 SafetyNet 证明 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. 结果显示在**安全**部分。



SafetyNet 证明 API 为每个设备返回以下状态：

- **SafetyNet CTS 配置文件匹配：**如果此值为 **True**，则设备具有与已通过 Android 兼容性测试套件 (CTS) 的配置文件匹配的配置文件。如果此值设置为 **False**，则设备没有与已通过 Android CTS 的配置文件匹配的配置文件。
- **SafetyNet 基本完整性：**如果此值为 **True**，则 SafetyNet 证明 API 未发现任何证据表明未知来源修改了设备上的 Citrix Secure Hub。如果此值设置为 **False**，则未知来源已修改设备上的 Citrix Secure Hub。
- **SafetyNet 上次已知状态：**此值显示设备的上次已知 SafetyNet 状态：
  - **成功：**SafetyNet 证明 API 未发现任何证据表明未知来源修改了设备上的 Citrix Secure Hub。
  - **LOCK_BOOTLOADER:** 用户必须锁定设备的引导加载程序。未知来源已修改设备上的 Citrix Secure Hub。
  - **RESTORE_TO_FACTORY_ROM：**用户必须将设备恢复到干净的出厂 ROM。未知来源已修改设备上的 Citrix Secure Hub。

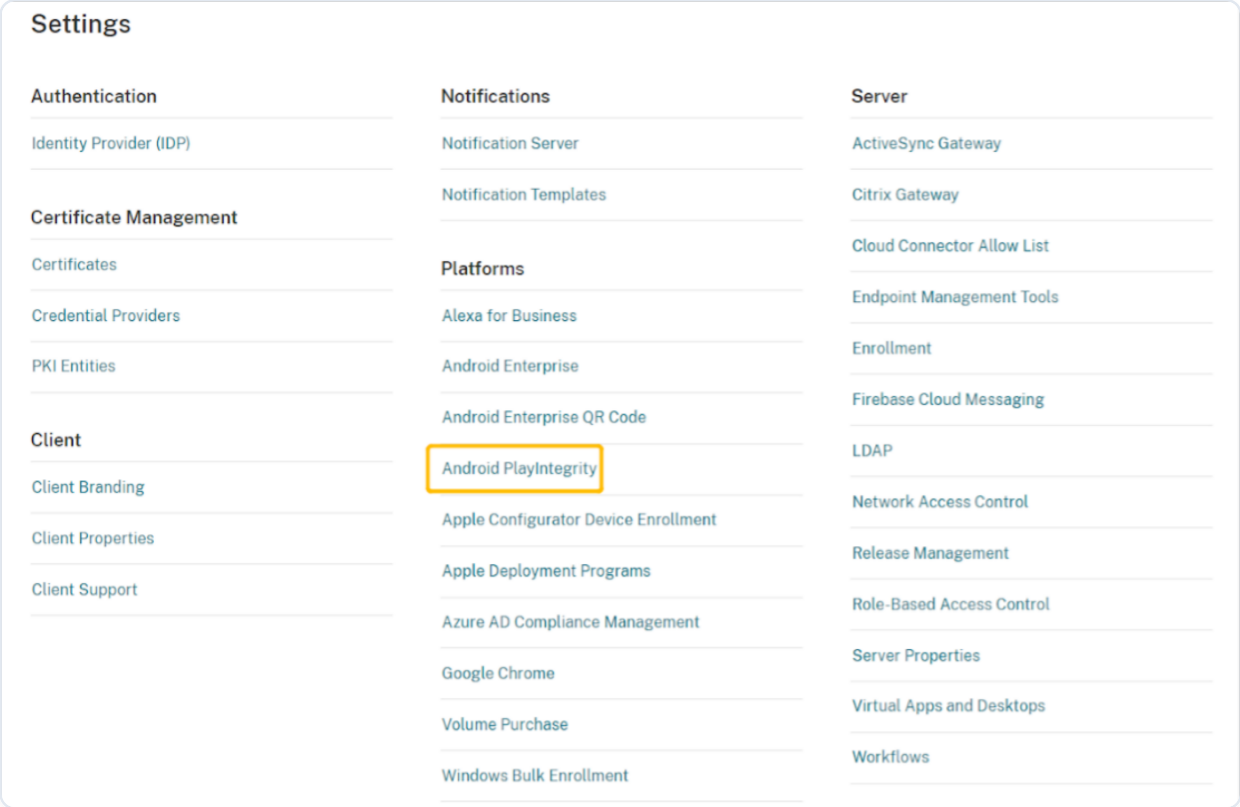
Play 完整性 API

Play Integrity API 有助于保护您的应用和游戏免受潜在的风险和欺诈性交互（例如作弊和未经授权的访问）的影响，从而使您能够采取适当措施来防止攻击并减少滥用。有关详细信息，请参阅 Play Integrity API。

启用 Play 完整性 API

请按照以下步骤切换到 Play Integrity API。

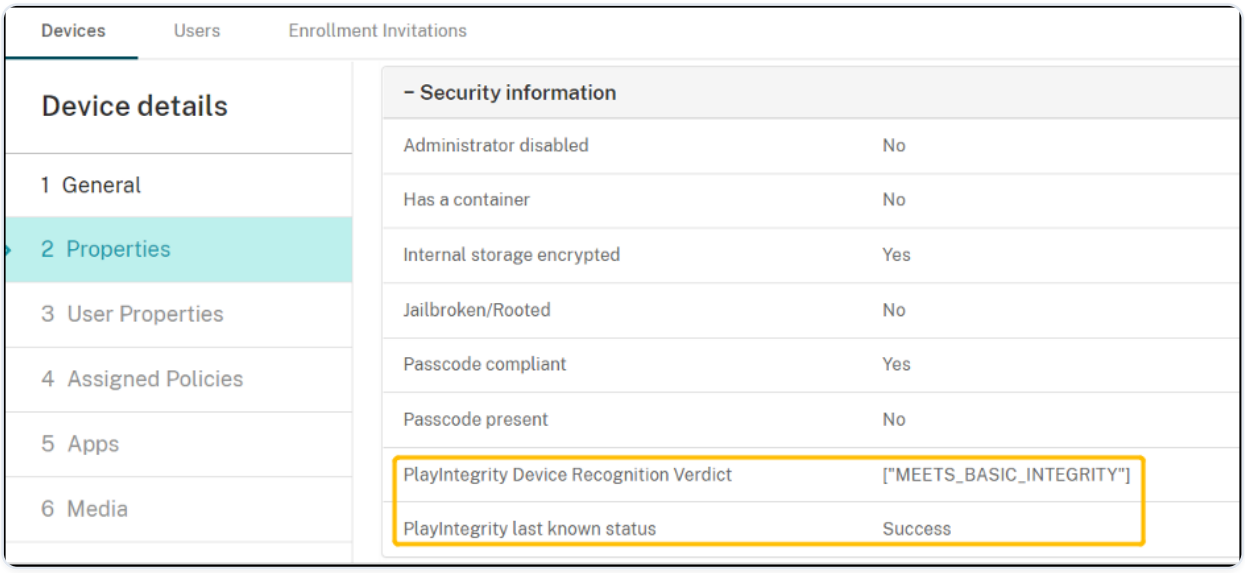
1. 为指定的 Citrix Endpoint Management 服务器启用 *afw.safetynet.attestation.api.* 弃用功能标志。
2. 在 Citrix Endpoint Management 控制台中，从“**设置**”页面中选择“**Android PlayIntegrity**”。



3. 在“证明计划”的小时字段中输入一个值。这是 PlayIntegrity 证明 API 评估您设备的时间间隔。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 Citrix 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 触发证明。

查看和分析 Play Integrity API 证明结果

1. 在 Citrix Endpoint Management 控制台中，转至“**管理 > 设备**”。
2. 选择要查看 Play Integrity API 证明结果的设备。单击“**显示更多**”。
3. 在“**设备**”选项卡中，选择“**属性**”。结果将显示在“**安全信息**”部分中。



4. Play Integrity API 证明返回以下状态：

   - 如果 **PlayIntegrity Device Recognition Verdict** 字段为 **“MEETS_BASIC_INTEGRITY”**，则表示设备上运行的 Citrix Secure Hub 至少通过了基本的系统完整性检查。
   - 如果 **PlayIntegrity Device Recognition Verdict** 字段不为 **“MEETS_BASIC_INTEGRITY”**，则表示设备上的 Citrix Secure Hub 可能在未经识别的 Android 版本上运行，可能具有已解锁的引导加载程序，或者可能未经制造商认证。
   - 如果 **PlayIntegrity last known status** 为 **Success**，则表示 PlayIntegrity API 证明已成功运行。
   - 如果 **PlayIntegrity last known status** 为 **Failure**，则表示 PlayIntegrity API 证明未能运行。

> **注意：**
>
> 在 SafetyNet Attestation 最终关闭（2023 年 11 月底）之前，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 设备被标记为不合规，即使设备是合规的。

   在 DO 注册期间，Play Integrity API 首次证明返回空值，这使得设备看起来不合规。此限制是 Google 的一个已知问题。DPC Support Lib 20230418 已发布以修复此问题。

   该修复程序从 23.9.0 版本开始可用。在此之前，请使用以下步骤作为解决方法：

   - 清除功能标志，并继续使用 SafetyNet API 以继续使用 SafetyNet Attestation API。

- 注销并重新登录以在注册后触发证明。您也可以等待下一次定期证明，默认为 24 小时。

此问题仅在注册期间发生。注册后，Play Integrity API 运行良好。

2. 新注册的 WPCOD 设备被标记为不合规，即使设备是合规的。Google 正在审查此问题。

三星

Samsung 提供多种与 Citrix Endpoint Management 兼容的解决方案。

要控制 Android 设备连接到 Citrix 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。

注册配置文件决定 Android 设备是注册到 MAM、MDM 还是 MDM+MAM，用户可以选择退出 MDM。Citrix Endpoint Management 支持以下用于注册到 MDM+MAM 的 Android 设备的身份验证类型。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

另一种很少使用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 设备管理的通用工作流程如下：

1. 完成入门过程。请参阅入门和资源设置和准备注册设备和交付资源。
2. 选择并配置注册方法。请参阅支持的注册方法。
3. 部署 Samsung 许可证密钥。
4. 配置 Samsung 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 Citrix Endpoint Management 支持的 Android 设备注册方法：

方法	受支持
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。

部署 Samsung 许可证密钥

Samsung 具有 Knox Platform Enterprise 密钥。有关详细信息，请参阅Knox Platform for Enterprise 密钥设备策略

配置 Samsung 设备策略

设备策略：

应用程序限制	应用程序卸载	密码
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。

应用锁定	应用擦除	证书续订
完全擦除	定位	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期间授予位置权限。用户可以选择不授予位置权限。如果用户在注册期间未授予该权限，Citrix Endpoint Management 会在发送“定位”命令时再次请求位置权限。

网络访问控制

您可以使用您的网络访问控制 (NAC) 解决方案来扩展 Citrix Endpoint Management 针对 Android 和 Apple 设备的设备安全评估。您的 NAC 解决方案使用 Citrix Endpoint Management 安全评估来促进和处理身份验证决策。配置 NAC 设备后，您在 Citrix Endpoint Management 中配置的设备策略和 NAC 筛选器将得到强制执行。

将 Citrix Endpoint Management 与 NAC 解决方案结合使用，可以为网络内部的设备添加 QoS 和更精细的控制。有关将 NAC 与 Citrix Endpoint Management 集成的优势摘要，请参阅访问控制。

Citrix 支持以下解决方案与 Citrix Endpoint Management 集成：

- NetScaler 网关
- ForeScout

Citrix® 不保证与其他 NAC 解决方案的集成。

在您的网络中使用 NAC 设备时：

- Citrix Endpoint Management 支持 NAC 作为 iOS、Android Enterprise 和 Android 设备的端点安全功能。
- 您可以在 Citrix Endpoint Management 中启用筛选器，根据规则或属性将设备设置为符合或不符合 NAC 规范。例如：
    - 如果 Citrix Endpoint Management 中的托管设备不符合指定条件，Citrix Endpoint Management 会将该设备标记为不合规。NAC 设备会阻止网络上的不合规设备。
    - 如果 Citrix Endpoint Management 中的托管设备安装了不合规的应用程序，NAC 筛选器可以阻止 VPN 连接。因此，不合规的用户设备无法通过 VPN 访问应用程序或网站。
    - 如果您将 NetScaler Gateway 用于 NAC，可以启用拆分隧道以防止 NetScaler Gateway 插件向 NetScaler Gateway 发送不必要的网络流量。有关拆分隧道的更多信息，请参阅配置拆分隧道。

支持的 NAC 合规性筛选器

Citrix Endpoint Management 支持以下 NAC 合规性筛选器：

匿名设备： 检查设备是否处于匿名模式。如果设备尝试重新连接时 Citrix Endpoint Management 无法重新验证用户身份，则此检查可用。

禁用应用： 检查设备是否具有应用访问策略中定义的禁用应用。有关该策略的详细信息，请参阅 应用访问设备策略。

非活动设备： 检查设备是否处于非活动状态，此状态由**服务器属性**中的**设备非活动天数阈值**设置定义。有关详细信息，请参阅 服务器属性。

缺少所需应用： 检查设备是否缺少应用访问策略中定义的任何所需应用。

非建议应用： 检查设备是否具有应用访问策略中定义的非建议应用。

不合规密码： 检查用户密码是否合规。在 iOS 和 Android 设备上，Citrix Endpoint Management 可以确定设备上当前密码是否符合发送到设备的密码策略。例如，在 iOS 上，如果 Citrix Endpoint Management 向设备发送密码策略，用户有 60 分钟的时间来设置密码。在用户设置密码之前，密码可能不合规。

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，自动化操作或使用 Citrix Endpoint Management API 的第三方会更改该属性。

已吊销状态： 检查设备证书是否已吊销。已吊销的设备在再次获得授权之前无法重新注册。

已 Root 的 Android 设备和已越狱的 iOS 设备： 检查 Android 或 iOS 设备是否已越狱。

未管理设备： 检查 Citrix Endpoint Management 是否正在管理设备。例如，已注册 MAM 的设备或未注册的设备不受管理。

> **注意：**
>
> 隐式合规/不合规筛选器仅在 Citrix Endpoint Management 正在管理的设备上设置默认值。例如，任何安装了被阻止应用或未注册的设备都将被标记为“不合规”。NAC 设备会阻止这些设备访问您的网络。

配置概述

建议您按所列顺序配置 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 Citrix Endpoint Management 中启用 NAC 筛选器。
3. 配置 NAC 解决方案：

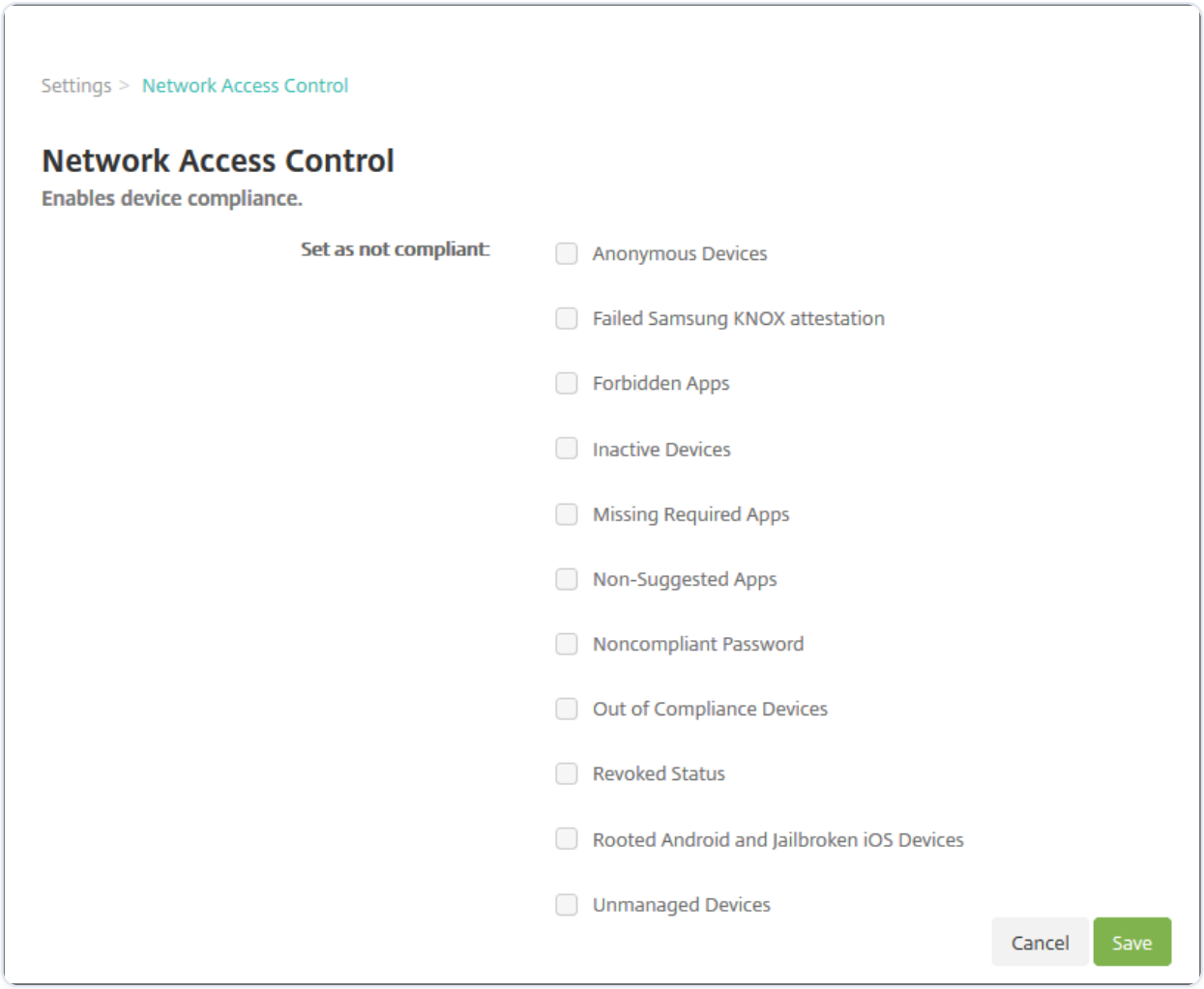
- NetScaler Gateway，详细信息请参阅 更新 NetScaler Gateway 策略以支持 NAC。

  要求您在设备上安装 Citrix SSO。请参阅 NetScaler Gateway 客户端。

- ForeScout：请参阅 ForeScout 文档。

在 Citrix Endpoint Management 中启用 NAC 筛选器

1. 在 Citrix Endpoint Management 控制台中，转到 **设置 > 网络访问控制**。



2. 选中要启用的 **设置为不合规** 筛选器对应的复选框。
3. 点击 **保存**。

更新 NetScaler Gateway 策略以支持 NAC

您必须在 VPN 虚拟服务器上配置高级（非经典）身份验证和 VPN 会话策略。

这些步骤将更新具有以下任一特征的 NetScaler Gateway：

- 与 Citrix Endpoint Management 进行了集成。

- 或者，已设置为 VPN，不属于 Citrix Endpoint Management 环境，并且可以访问 Citrix Endpoint Management。

在控制台窗口中，在您的虚拟 VPN 服务器上执行以下操作。命令和示例中的 FQDN 和 IP 地址均为虚构。

1. 如果您的 VPN 虚拟服务器上正在使用经典策略，请移除并解除绑定所有经典策略。要检查，请键入：

   `show vpn vserver <VPN_VServer>`

   移除任何包含单词 **Classic** 的结果。例如：`VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   要移除策略，请键入：

   `unbind vpn vserver <VPN_VServer> -policy <policy_name>`
2. 通过键入以下内容创建相应的“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. 通过键入以下内容将策略绑定到您的 VPN 虚拟服务器。

   `bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100`
4. 通过键入以下内容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。
5. 通过键入以下内容将 SSL 证书绑定到虚拟服务器。

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   例如：`bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`
6. 将身份验证配置文件从 VPN 虚拟服务器关联到身份验证虚拟服务器。首先，通过键入以下内容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. 通过键入以下内容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. 通过键入以下内容检查从 NetScaler 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，此查询通过获取环境中注册的第一个设备 (`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"`

   成功的结果类似于以下示例。

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. 当前一步成功后，创建到 Citrix Endpoint Management 的 Web 身份验证操作。首先，创建一个策略表达式以从 iOS VPN 插件中提取设备 ID。键入以下内容。

   `add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\', \'&\').VALUE(\"deviceidvalue\")"`

10. 通过键入以下内容将请求发送到 Citrix Endpoint Management。在此示例中，Citrix Endpoint Management IP 为 `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\")"
```

Citrix 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. 通过键入以下内容，创建用于关联操作的身份验证策略。

    ```
    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. 通过键入以下内容，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. 通过键入以下内容，添加用于关联 LDAP 策略的策略标签。

    ```
    add authentication policylabel <policy_label_name>
    ```

    例如：`add authentication policylabel ldap_pol_label`

14. 通过键入以下内容，将 LDAP 策略与策略标签关联。

    ```
    bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
    ```

15. 连接合规设备以执行 NAC 测试，确认 LDAP 身份验证成功。键入以下内容。

    ```
    bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END
    ```

16. 添加要与身份验证虚拟服务器关联的 UI。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. 通过键入以下内容，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 Citrix Secure Hub 连接。键入以下内容。

```
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
```

Apple

iOS

要在 Citrix Endpoint Management 中管理 iOS 设备，您需要设置 Apple 的 Apple Push Notification service (APNs) 证书。有关信息，请参阅 APNs 证书。

注册配置文件决定 iOS 设备是否注册到 MDM+MAM，用户可以选择退出移动设备管理 (MDM)。Citrix Endpoint Management 支持 MDM+MAM 中 iOS 设备的以下身份验证类型。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

> **iOS 13 中受信任证书的要求：**

> Apple 对 TLS 服务器证书有新的要求。请验证所有证书是否符合 Apple 的新要求。请参阅 Apple 的出版物 `<https://support.apple.com/zh-cn/HT210176>`。有关管理证书的帮助，请参阅 上载证书。

> 启动 iOS 设备管理的一般工作流程如下：

1. 完成入门过程。请参阅 入门和资源设置 和 准备注册设备和交付资源。
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

Citrix 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，您可以将软件升级推迟最多 90 天。在 iOS 的限制设备策略中，使用以下设置：

- **强制延迟软件更新**
- **强制软件更新延迟**

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。

必须保持开放的 Apple 主机名

某些 Apple 主机名必须保持开放，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各项的安装、更新和正常运行：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/zh-cn/HT201999>`。

支持的注册方法

您可以在注册配置文件中指定如何管理 iOS 设备。您可以选择以下注册设置：

- **Apple 用户注册：** 对于 BYOD 设备，可在个人数据隐私和企业数据安全之间取得平衡。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 设备注册：** 适用于受监督的 iOS 设备，设备上具有独立的个人和企业配置文件。
- **不管理设备：** 如果您只想管理应用程序，请将这些设备从 MDM 中排除。

有关创建注册配置文件的详细信息，请参阅 注册配置文件。

Citrix Endpoint Management 支持以下 iOS 设备注册方法：

方法	受支持
苹果商务管理	是
苹果学校管理	是
苹果配置器	是
手动注册	是
注册邀请	是

Apple 部署计划包括面向商业组织的 Apple Business Manager (ABM) 和面向教育组织的 Apple School Manager (ASM)。有关详细信息，请参阅通过 Apple 部署计划部署设备。

Apple School Manager 是一种教育版 Apple 部署计划。请参阅与 Apple 教育功能集成。

使用 Apple 部署计划批量注册 iOS、iPadOS 和 macOS 设备。您可以直接从 Apple、参与的 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。

受管 Apple ID

用户注册与受管 Apple ID 紧密集成。您可以使用 ABM/ASM 手动创建受管 Apple ID，也可以使用 Azure Active Directory (AAD) 动态创建。

对于非联合身份验证，请使用 ABM/ASM 创建受管 Apple ID 以添加帐户。有关在 ABM/ASM 中添加帐户的信息，请参阅 `https://support.apple.com/guide/apple-business-manager/welcome/web` 处的 Apple 文档和 `https://support.apple.com/guide/apple-school-manager/welcome/web` 处的 ASM 文档。为避免用户注册时出现额外步骤，我们建议执行以下操作：

- 创建受管 Apple ID 时，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 **Staff**。
- 让用户在注册前手动更改密码。告知用户我们建议他们使用与公司账户相同的密码。

要动态创建托管式 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 的更多信息，请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。此外，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 Business Manager 用户指南和Apple School Manager 用户指南。

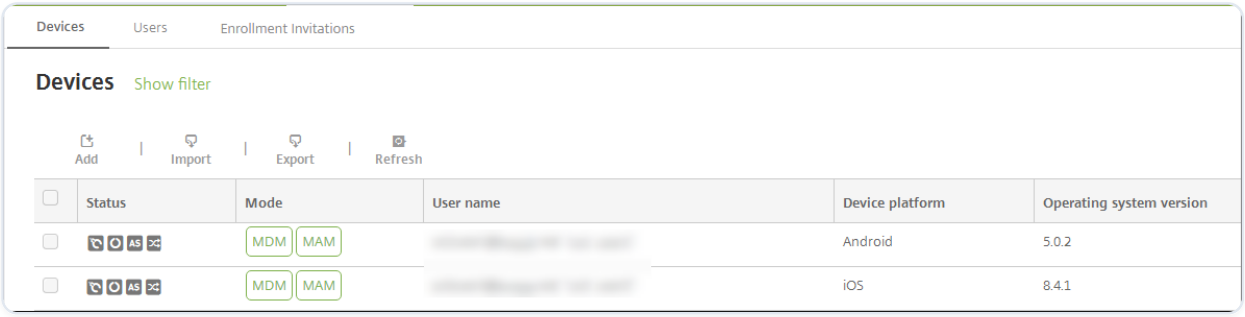
手动创建托管式 Apple ID 时，可以配置自定义域以替代默认域。您配置的自定义域将替换现有域。例如，您的公司电子邮件地址遵循 `first.last@company.com` 格式，但您希望使用

`mycompany.website.com` 作为托管式 Apple ID 的域。在 ABM/ASM 上创建托管式 Apple ID 时，电子邮件地址将变为 `first.last@mycompany.website.com`。

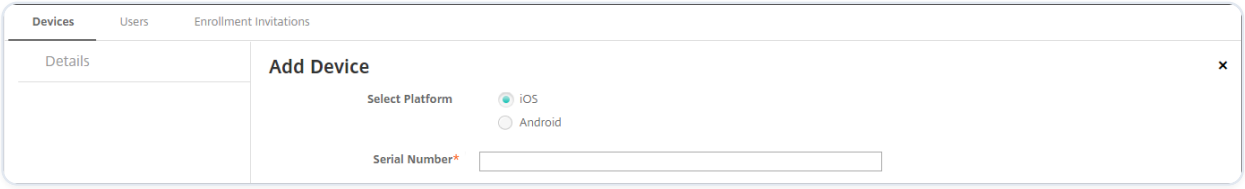
手动添加 iOS 设备

如果要手动添加 iOS 设备（例如用于测试目的），请按照以下步骤操作。

1. 在 Citrix Endpoint Management 控制台中，单击“**管理 > 设备**”。“**设备**”页面随即显示。



2. 单击“**添加**”。“**添加设备**”页面随即显示。



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**”表随即显示，设备已添加到列表底部。要查看和确认设备详细信息：选择您添加的设备，然后在出现的菜单中单击“**编辑**”。

> **注意：**
>
> 当您选中设备旁边的复选框时，选项菜单会显示在设备列表上方。如果您单击列表中的其他任何位置，选项菜单会显示在列表的右侧。

   - 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。

    - 交付组与本地组关联。

- 如果使用 Active Directory：

    - 交付组与 Active Directory 组关联。

  设备详细信息列表(/en-us/citrix-endpoint-management/media/manage-devices-details-general.png)

5. **常规**页面列出了设备**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、激活锁绕过以及平台类型的其他信息。**完全擦除设备**字段包含用户 PIN 码。设备擦除后，用户必须输入该代码。如果用户忘记了代码，您可以在此处查找。

6. **属性**页面列出了 Citrix 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个属性。有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

   添加属性后，它最初会显示在您添加它的类别下。单击**下一步**，然后返回**属性**页面后，该属性将显示在相应的列表中。

   要删除属性，请将鼠标悬停在列表上，然后单击右侧的**X**。Citrix Endpoint Management 会立即删除该项目。

7. 其余**设备详细信息**部分包含设备的摘要。

   - **用户属性**：显示 RBAC 角色、组成员身份、批量购买帐户以及用户的属性。您可以从此页面停用批量购买帐户。
   - **分配的策略**：显示已部署、待处理和失败的策略数量。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待处理并重新部署用户已删除的策略。
   - **应用程序：** 显示上次盘点中已安装、待处理和失败的应用程序部署数量。提供应用程序名称、标识符、类型及其他信息。有关 iOS 和 macOS 盘点键（例如 **HasUpdateAvailable**）的说明，请参阅移动设备管理 (MDM) 协议。
   - **媒体：** 显示上次盘点中已部署、待处理和失败的媒体部署数量。
   - **操作：** 显示已部署、待处理和失败的操作数量。提供操作名称和上次部署时间。
   - **交付组：** 显示成功、待处理和失败的交付组数量。对于每次部署，提供交付组名称和部署时间。选择一个交付组可查看更详细的信息，包括状态、操作以及渠道或用户。
   - **iOS 配置文件：** 显示上次 iOS 配置文件盘点，包括名称、类型、组织和描述。
   - **iOS 预配配置文件：** 显示企业分发预配配置文件信息，例如 UUID、过期日期和托管状态。

- **证书：** 显示有效、已过期或已吊销证书的信息，例如类型、提供商、颁发者、序列号以及过期前的剩余天数。
- **连接：** 显示首次连接状态和上次连接状态。为每个连接提供用户名、倒数第二次（上次）身份验证时间和上次身份验证时间。
- **MDM 状态：** 显示 MDM 状态、上次推送时间和上次设备回复时间等信息。

配置 iOS 设备策略

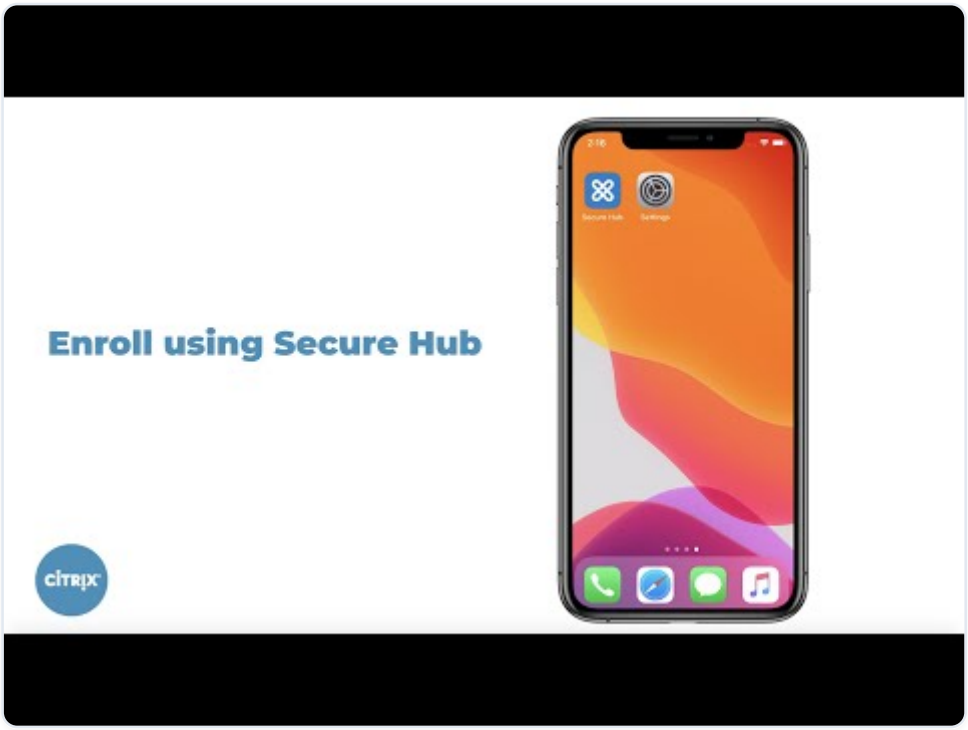
使用这些策略配置 Citrix Endpoint Management 如何与运行 iOS 或 iPadOS 的设备交互。此表列出了适用于 iOS 和 iPadOS 设备的所有设备策略。

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)	
蜂窝网络	联系人 (CardDAV)	凭据	
设备名称	教育配置	企业邮件	
字体	主屏幕布局	导入 iOS 和 macOS 配置文件	
LDAP	位置	锁屏消息	
邮件	托管域	最大驻留用户数	
MDM 选项	网络	网络使用情况	
组织信息	操作系统更新	密码	
密码锁定宽限期	个人热点	配置文件删除	
预配配置文件	预配配置文件删除	代理	
限制	漫游	SCEP	
SSO 帐户	商店	订阅日历	

条款和条件	VPN	壁纸	
Web 内容筛选器	Web 剪辑		

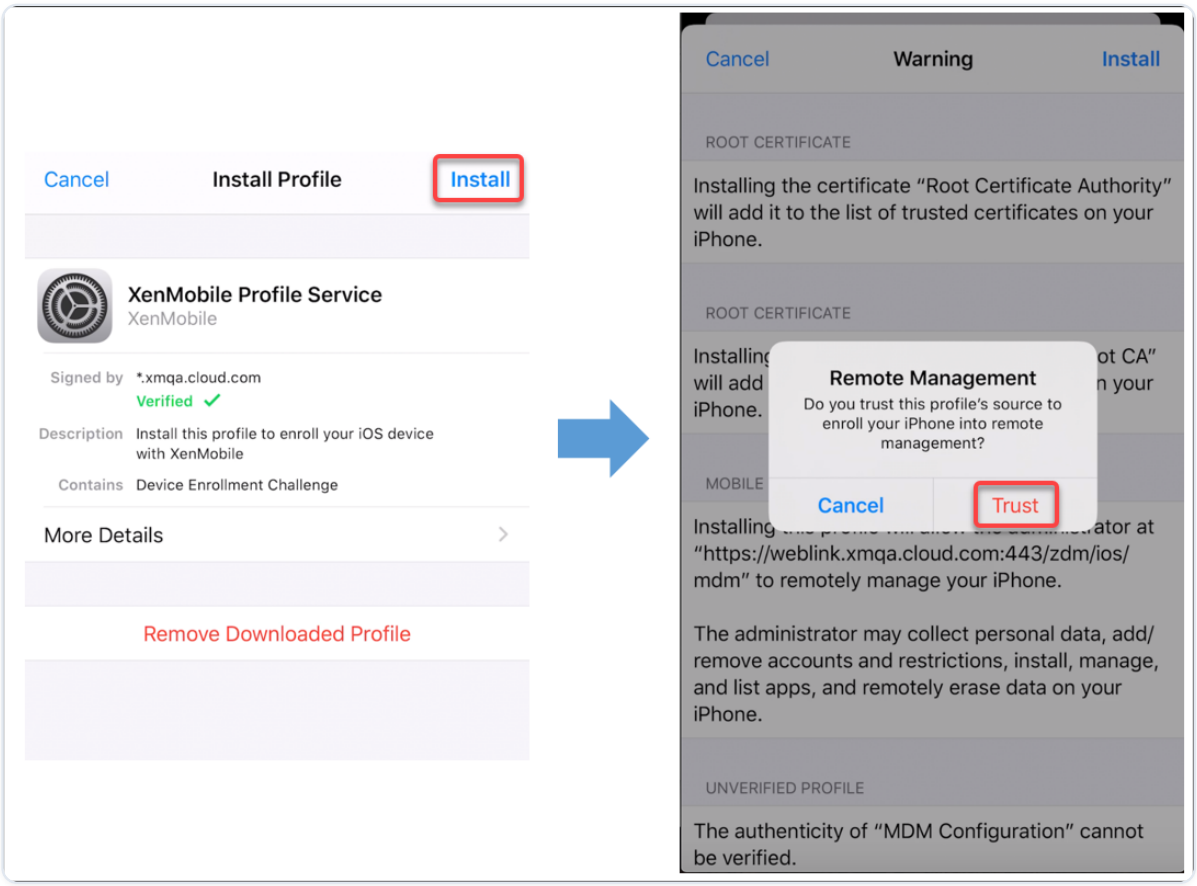
注册 iOS 设备

本节介绍用户如何将 iOS 设备（12.2 或更高版本）注册到 Citrix Endpoint Management。有关 iOS 注册的更多信息，请观看以下视频：



1. 在 iOS 设备上前往 Apple Store，下载 Citrix Secure Hub 应用程序，然后点击该应用程序。
2. 当系统提示安装应用程序时，点击**下一步**，然后点击**安装**。
3. Citrix Secure Hub 安装完成后，点击**打开**。
4. 输入您的公司凭据，例如 Citrix Endpoint Management 服务器名称、用户主体名称 (UPN) 或电子邮件地址。然后，点击**下一步**。
5. 点击**是，注册**以注册您的 iOS 设备。
6. 将显示 Citrix Endpoint Management 收集的数据列表。点击**下一步**。将显示有关组织如何使用该数据的说明。点击**下一步**。
7. 输入凭据后，在出现提示时点击**允许**以下载配置文件。下载配置文件后，点击**关闭**。
8. 在您的设备设置中，安装 XenMobile® 配置文件。
    - 转到**设置 > 通用 > 配置文件 > XenMobile Profile Service**，然后点击**安装**以添加配置文件。

- 在通知窗口中，点击**信任**以将您的设备注册到远程管理。



9. 注册成功后，打开 Citrix Secure Hub。如果您要注册 MDM+MAM：凭据验证后，在出现提示时创建并确认您的 Citrix PIN。
10. 工作流程完成后，设备将注册。然后，您可以访问应用商店以查看可在 iOS 设备上安装的应用。

安全操作

iOS 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
- 应用锁定
- 应用擦除
- 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

- 定位
- 锁定
- 响铃
- 请求/停止 AirPlay 镜像
- 重新启动/关机
- 撤销/授权
- 选择性擦除
- 解锁

iOS 的用户注册支持以下安全操作：

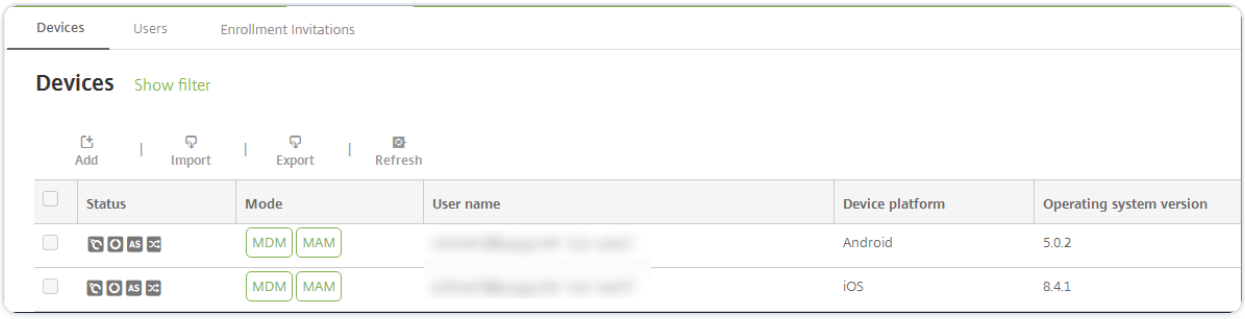
- 撤销
- 锁定
- 选择性擦除
- 证书续订

锁定 iOS 设备

您可以锁定丢失的 iOS 设备，并在设备锁定屏幕上显示附带的消息和电话号码。

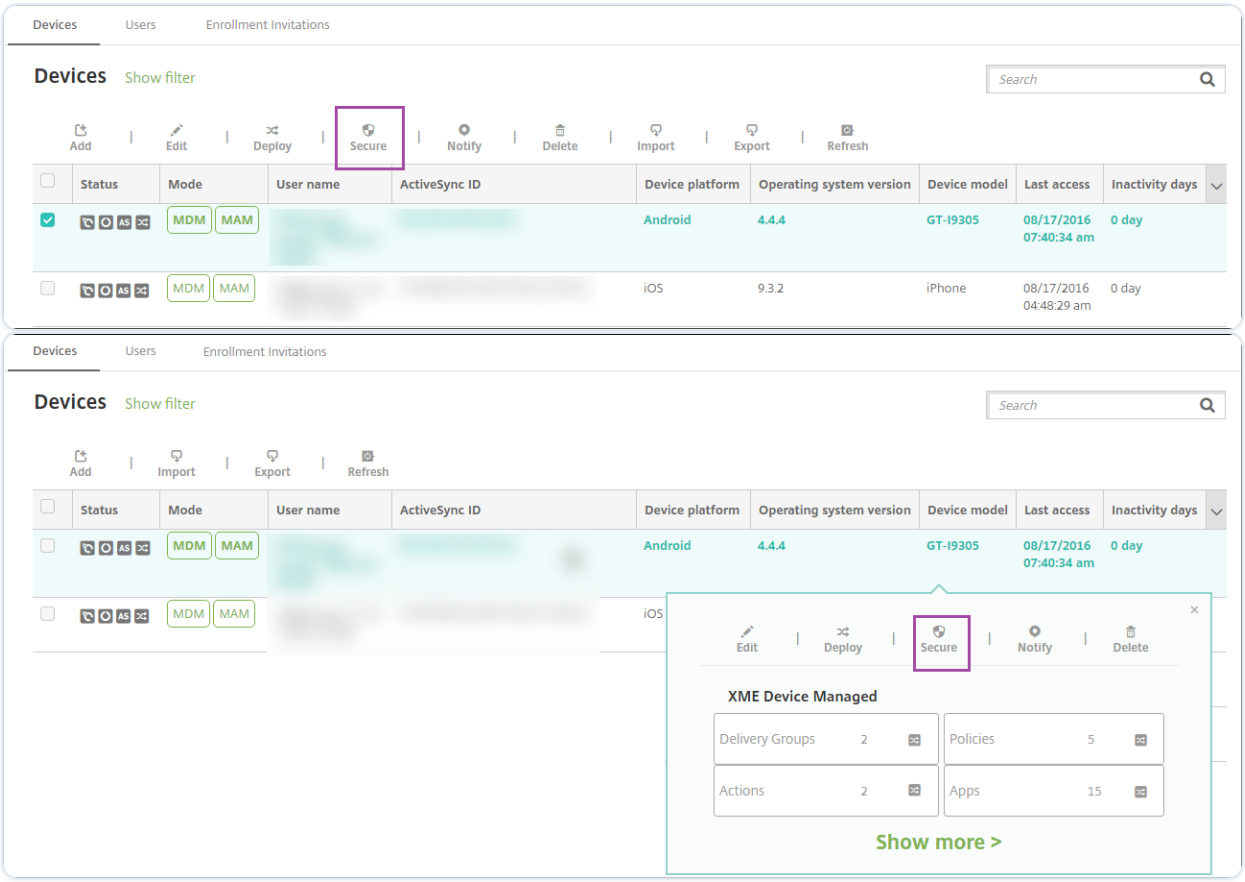
要在锁定的设备上显示消息和电话号码，请在 Citrix Endpoint Management 控制台中将 密码 策略设置为 **true**。用户也可以手动在设备上启用密码。

1. 单击 **管理 > 设备**。将显示“**设备**”页面。

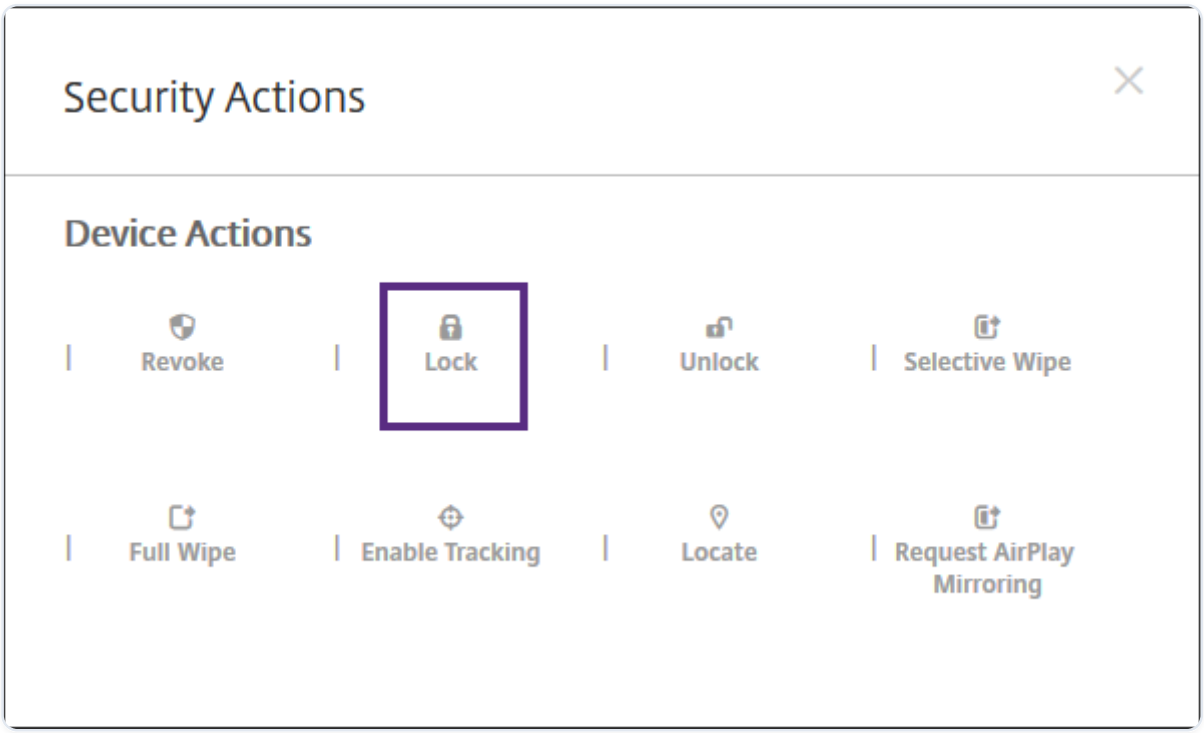


2. 选择要锁定的 iOS 设备。

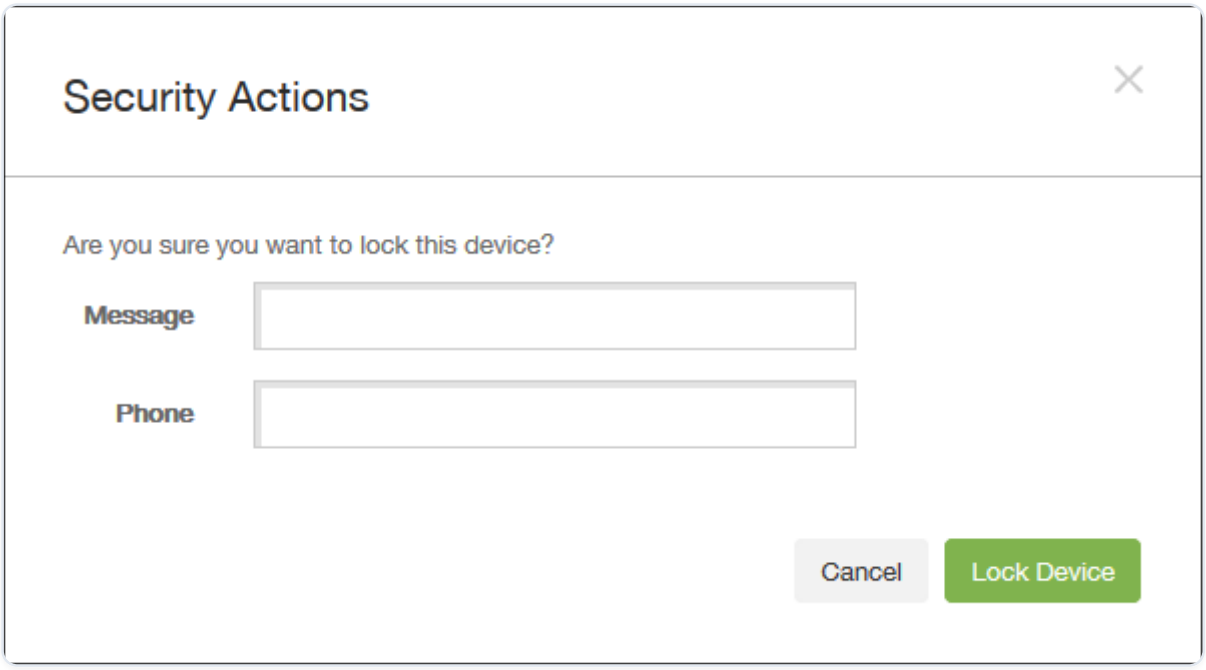
   选中设备旁边的复选框以在设备列表上方显示选项菜单。单击列表中的其他任意位置以在列表右侧显示选项菜单。



3. 在选项菜单中，单击“**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。



5. （可选）键入要在设备锁定屏幕上显示的消息和电话号码。

   iOS 会将“Lost iPad”字样附加到您在“**消息**”字段中键入的内容。

   如果您将“**消息**”字段留空并提供电话号码，Apple 会在设备锁定屏幕上显示消息“Call owner”。

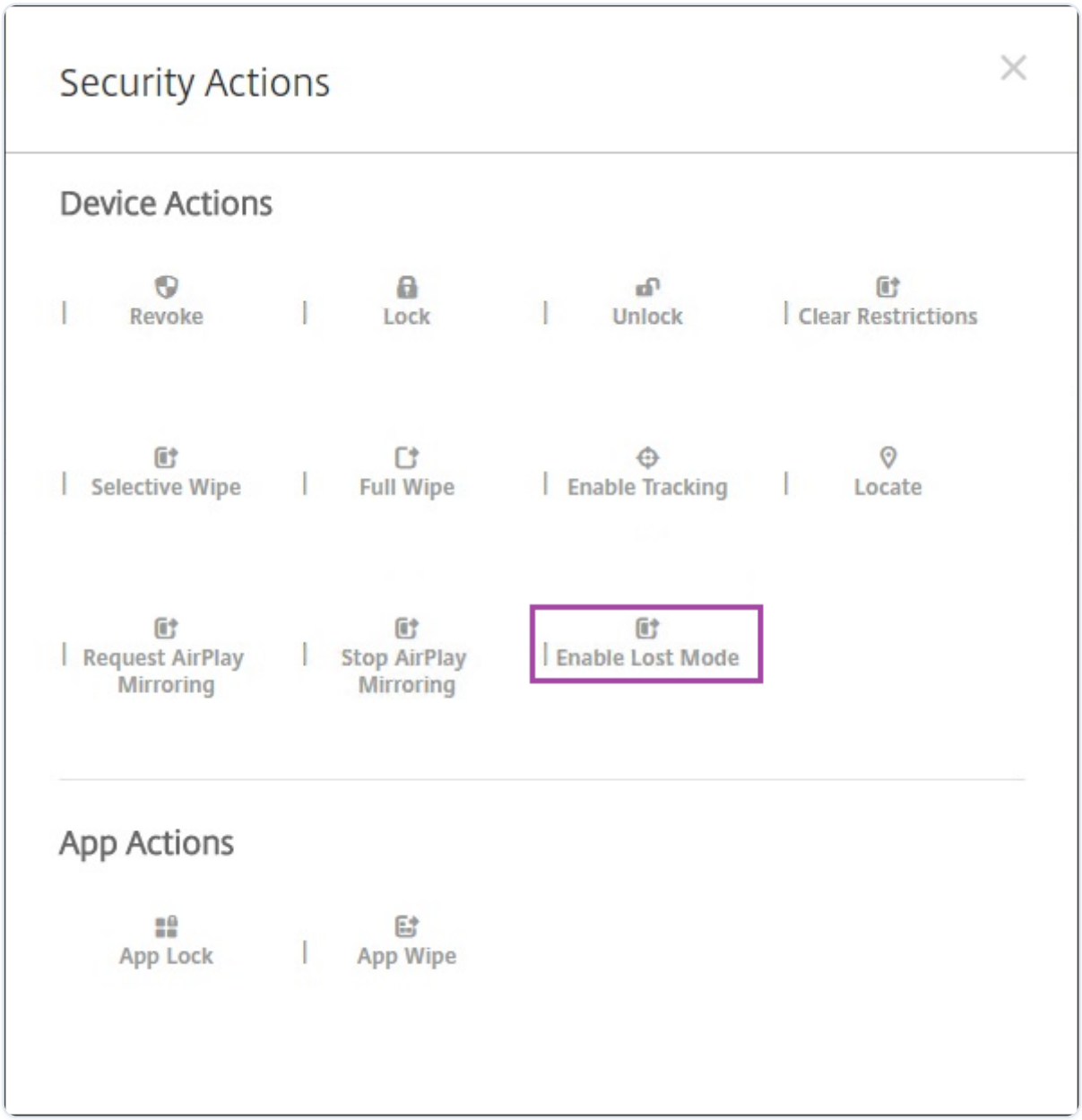
6. 单击“**锁定设备**”。

将 iOS 设备置于丢失模式

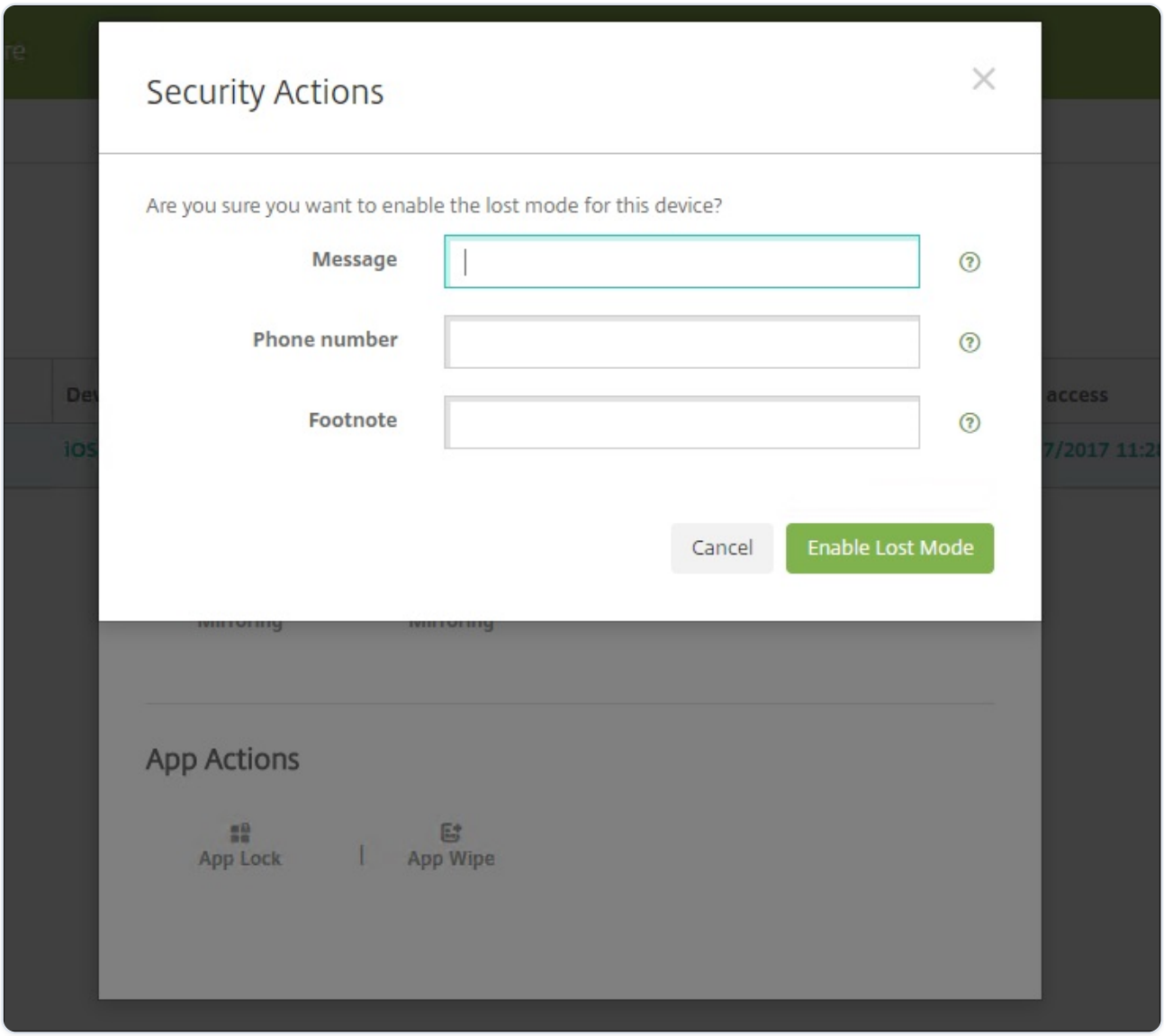
Citrix Endpoint Management 丢失模式设备属性可将 iOS 设备置于丢失模式。与 Apple 托管的丢失模式不同，Citrix Endpoint Management 丢失模式不需要用户执行以下任一操作即可启用设备定位：配置“**查找我的 iPhone/iPad**”设置或为 Citrix Secure Hub 启用定位服务。

在 Citrix Endpoint Management 丢失模式下，只有 Citrix Endpoint Management 才能解锁设备。（相比之下，如果您使用 Citrix Endpoint Management 设备锁定功能，用户可以使用您提供的 PIN 码直接解锁设备。

要启用或禁用丢失模式：转到 **管理 > 设备**，选择一个受监管的 iOS 设备，然后单击 **安全**。然后，单击 **启用丢失模式** 或 **禁用丢失模式**。

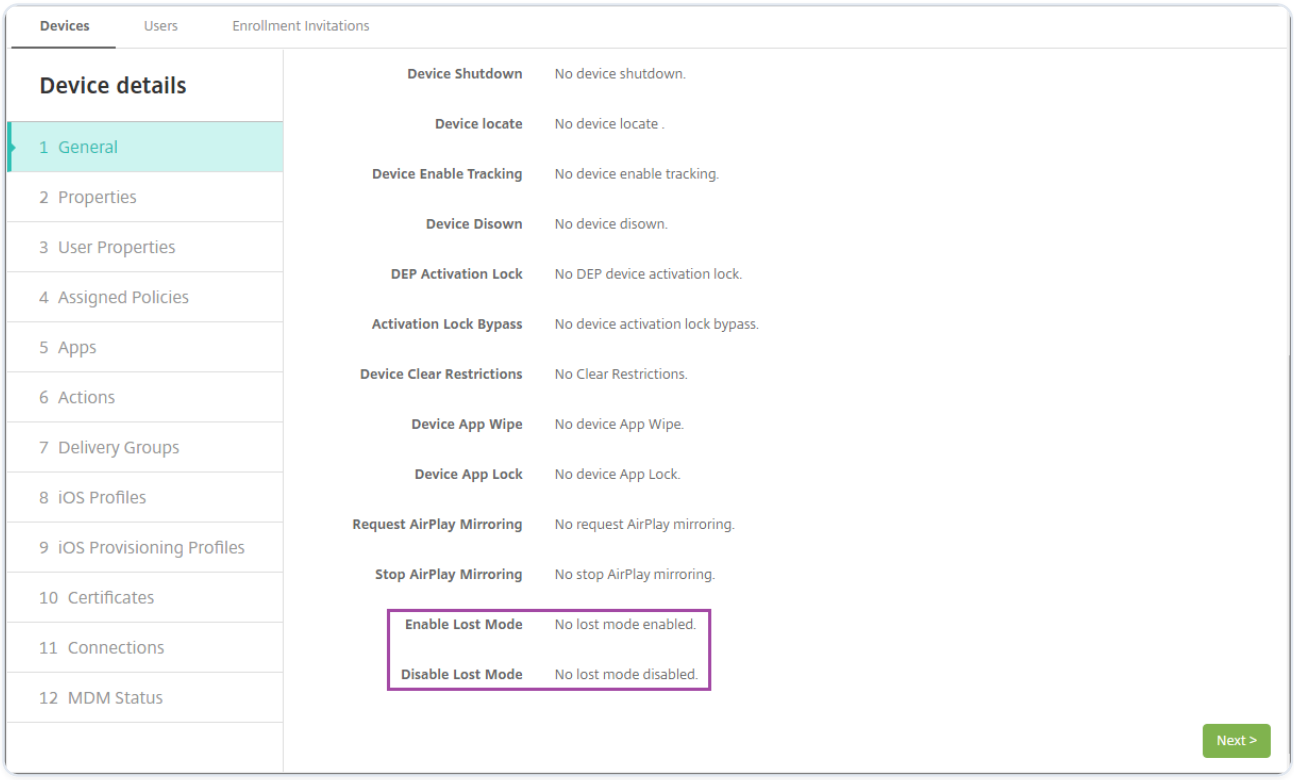


如果单击 **启用丢失模式**，请键入在设备处于丢失模式时要显示的信息。

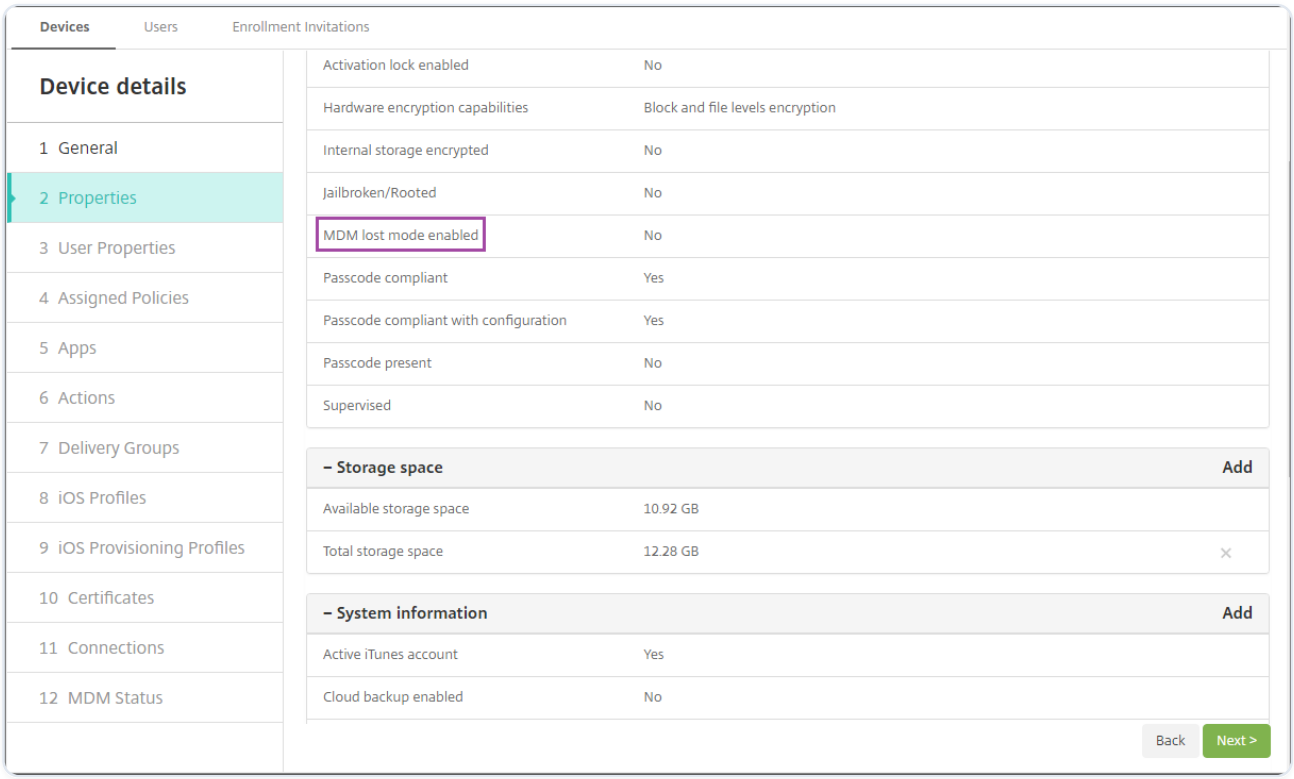


使用以下任一方法检查丢失模式状态：

- 在 **安全操作** 窗口中，验证按钮是否设置为 **禁用丢失模式**。
- 从 **管理 > 设备**，在 **安全** 下的 **常规** 选项卡中，查看上次的启用丢失模式或禁用丢失模式操作。



- 从 **管理 > 设备**，在 **属性** 选项卡中，验证 **MDM 丢失模式已启用** 设置的值是否正确。



如果在 iOS 设备上启用 Citrix Endpoint Management 丢失模式，Citrix Endpoint Management 控制台也会发生如下更改：

- 在 **配置 > 操作** 中，**操作** 列表不包括以下自动化操作：**吊销设备**、**选择性擦除设备** 和 **完全擦除设备**。

- 在 **管理 > 设备** 中，**安全操作** 列表不再包含 **吊销** 和 **选择性擦除** 设备操作。您仍然可以根据需要使用安全操作执行 **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** 中键入的内容。

如果将 **消息** 留空并提供电话号码，Apple 会在设备锁定屏幕上显示“呼叫所有者”消息。

绕过 iOS 激活锁

激活锁是“查找我的 iPhone/iPad”的一项功能，可防止丢失或被盗的受监管设备被重新激活。激活锁要求用户提供 Apple ID 和密码，然后才能执行以下操作：关闭“查找我的 iPhone/iPad”、抹掉设备或重新激活设备。对于贵组织拥有的设备，绕过激活锁是必要的，例如，用于重置或重新分配设备。

要启用激活锁，请配置并部署 Citrix Endpoint Management MDM 选项设备策略。然后，您可以从 Citrix Endpoint Management 控制台管理设备，而无需用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 Citrix Endpoint Management 控制台发出“激活锁绕过”安全操作。

例如，如果用户归还了丢失的手机，或者在完全擦除之前或之后设置设备：当手机提示输入 Apple App Store 帐户凭据时，通过发出“激活锁绕过”安全操作来跳过该步骤。

激活锁绕过的设备要求

- 通过 Apple Configurator 或 Apple 部署计划进行监管
- 配置了 iCloud 帐户
- 启用了“查找我的 iPhone/iPad”
- 已在 Citrix Endpoint Management 中注册
- 已将启用激活锁的 MDM 选项设备策略部署到设备

要在对设备执行完全擦除之前绕过激活锁：

1. 转到“**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。设备设置期间不会出现激活锁屏幕。

要在对设备执行完全擦除之后绕过激活锁：

1. 重置或擦除设备。设备设置期间会出现激活锁屏幕。
2. 前往 **管理 > 设备**，选择设备，点击 **安全**，然后点击 **激活锁绕过**。
3. 轻触设备上的“返回”按钮。主屏幕随即出现。

请注意以下事项：

- 建议您的用户不要关闭“查找我的 iPhone/iPad”。不要从设备执行完全擦除。在上述任何一种情况下，系统都会提示用户输入 iCloud 帐户密码。帐户验证后，用户在擦除所有内容和设置后将不会看到“激活 iPhone/iPad”屏幕。
- 对于已生成激活锁绕过代码且已启用激活锁的设备：如果在完全擦除后无法绕过“激活 iPhone/iPad”页面，则无需从 Citrix Endpoint Management 中删除设备。您或用户可以直接联系 Apple 支持以解除设备锁定。
- 在硬件清单盘点期间，Citrix Endpoint Management 会查询设备以获取激活锁绕过代码。如果绕过代码可用，设备会将其发送到 Citrix Endpoint Management。然后，要从设备中删除绕过代码，请从 Citrix Endpoint Management 控制台发送“激活锁绕过”安全操作。此时，Citrix Endpoint Management 和 Apple 都拥有解除设备锁定所需的绕过代码。
- “激活锁绕过”安全操作依赖于 Apple 服务的可用性。如果该操作不起作用，您可以使用以下方法之一解除设备锁定：
  - 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代码。要查找绕过代码，请前往 **管理 > 设备**，选择设备，点击 **编辑**，然后点击 **属性**。**激活锁绕过代码** 位于 **安全信息** 下。

macOS

为了在 Citrix Endpoint Management 中管理 macOS 设备，您需要设置 Apple 的 Apple Push Notification service (APNs) 证书。有关详细信息，请参阅 APNs 证书。

Citrix Endpoint Management 将 macOS 设备注册到 MDM 中。Citrix Endpoint Management 支持 MDM 中 macOS 设备的以下注册身份验证类型。

- 域
- 域加一次性密码
- 邀请 URL 加一次性密码

> **macOS 15 中受信任证书的要求：**

> Apple 对 TLS 服务器证书有新的要求。请验证所有证书是否符合 Apple 的新要求。请参阅 Apple 的出版物 `<https://support.apple.com/zh-cn/HT210176>`。有关管理证书的帮助，请参阅 上载证书。

> 启动 macOS 设备管理的一般工作流程如下：

1. 完成入门过程。请参阅 入门和资源设置 和 准备注册设备和交付资源。
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。

必须保持开放的 Apple 主机名

某些 Apple 主机名必须保持开放，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各项的安装、更新和正常运行：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/zh-cn/HT201999>`。

支持的注册方法

下表列出了 Citrix Endpoint Management 支持的 macOS 设备注册方法：

方法	受支持
苹果部署计划	是
苹果学校管理	是
苹果配置器	否
手动注册	是
注册邀请	是

Apple 为商业和教育帐户提供了设备注册计划。对于商业帐户，您可以注册 Apple Deployment Program，以便在 Citrix Endpoint Management 中使用 Apple Deployment Program 进行设备注册和管理。该计划适用于 iOS、macOS 和 Apple TV 设备。请参阅 通过 Apple Deployment Program 部署设备。

对于教育帐户，您可以创建 Apple School Manager 帐户。Apple School Manager 统一了 Deployment Program 和批量采购。Apple School Manager 是一种教育版 Apple Deployment Program。请参阅 与 Apple 教育功能集成。

您可以使用 Apple Deployment Program 批量注册 iOS、macOS 和 Apple TV 设备。您可以直接从 Apple、参与的 Apple 授权经销商或运营商处购买这些设备。

配置 macOS 设备策略

使用这些策略来配置 Citrix Endpoint Management 如何与运行 macOS 的设备交互。此表列出了适用于 macOS 设备的所有设备策略。

隔空播放镜像	应用清单	应用卸载
日历 (CalDAV)	通讯录 (CardDAV)	凭据
设备名称	Exchange 邮件	FileVault
防火墙	字体	导入 iOS 和 macOS 配置文件

操作系统更新	密码	配置文件移除
限制	SCEP	VPN
Web 剪辑		

注册 macOS 设备

Citrix Endpoint Management 提供了两种注册运行 macOS 的设备的方法。这两种方法都允许 macOS 用户通过无线方式直接从其设备注册。

- **向用户发送注册邀请：**此注册方法允许您为 macOS 设备设置以下任何注册安全模式：
  - 用户名 + 密码
  - 用户名 + PIN
  - 双因素身份验证

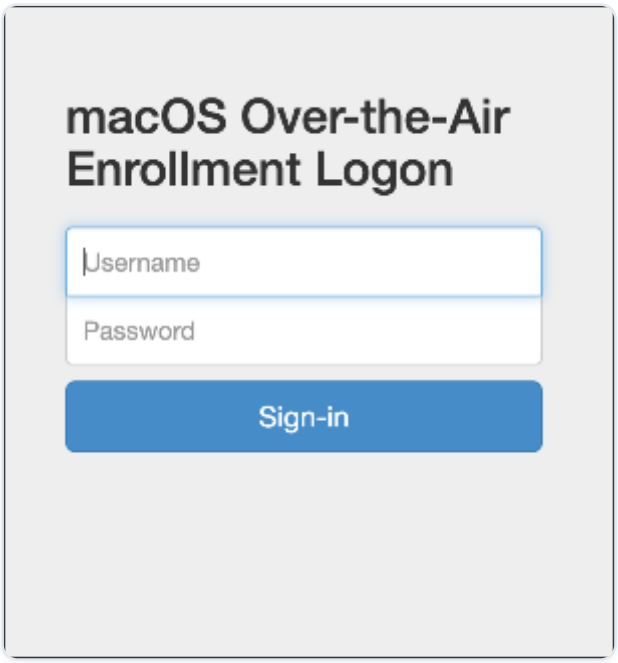
  当用户按照注册邀请中的说明操作时，将显示一个已填写用户名的登录屏幕。
- **向用户发送注册链接：**此 macOS 设备注册方法会向用户发送一个注册链接，用户可以在 Safari 或 Chrome 浏览器中打开该链接。然后，用户通过提供其用户名和密码进行注册。

  要阻止将注册链接用于 macOS 设备，请将服务器属性 **Enable macOS OTAE** 设置为 **false**。因此，macOS 用户只能通过注册邀请进行注册。

向 macOS 用户发送注册邀请

1. 为 macOS 用户注册添加邀请。请参阅注册邀请。

2. 用户收到邀请并单击链接后，Safari 浏览器中将显示以下屏幕。Citrix Endpoint Management 会填写用户名。如果您为注册安全模式选择了“**双因素**”，则会显示另一个字段。



3. 用户根据需要安装证书。用户是否看到安装证书的提示取决于您是否为 macOS 配置了以下内容：公共信任的 SSL 证书和公共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。

   Mac 设备策略已安装。您现在可以像管理移动设备一样，开始使用 Citrix 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 Citrix Endpoint Management 的服务器的完全限定域名 (FQDN)。
   - 端口 **8443** 是默认的安全端口。如果您配置了不同的端口，请使用该端口而不是 8443。
   - **instanceName**（通常显示为 `zdm`）是服务器安装期间指定的名称。

   有关发送安装链接的更多信息，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 配置了公共信任的 SSL 证书和数字签名证书，用户会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。

Mac 设备策略已安装。您现在可以像管理移动设备一样，使用 Citrix 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。

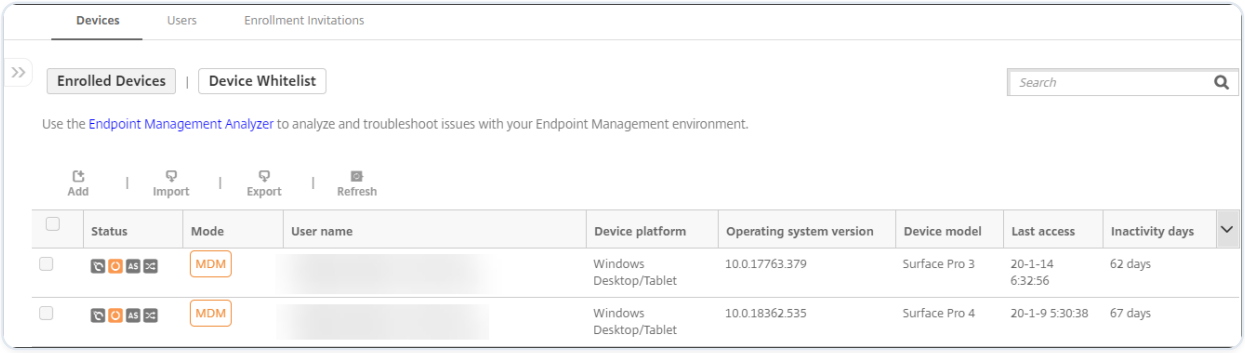
吊销	锁定	选择性擦除
完全擦除	证书续订	轮换个人恢复密钥

锁定 macOS 设备

您可以远程锁定丢失的 macOS 设备。Citrix Endpoint Management 会锁定设备。然后，它会生成一个 PIN 码并将其设置到设备中。要访问设备，用户需要输入 PIN 码。使用 **取消锁定** 可从 Citrix Endpoint Management 控制台中移除锁定。

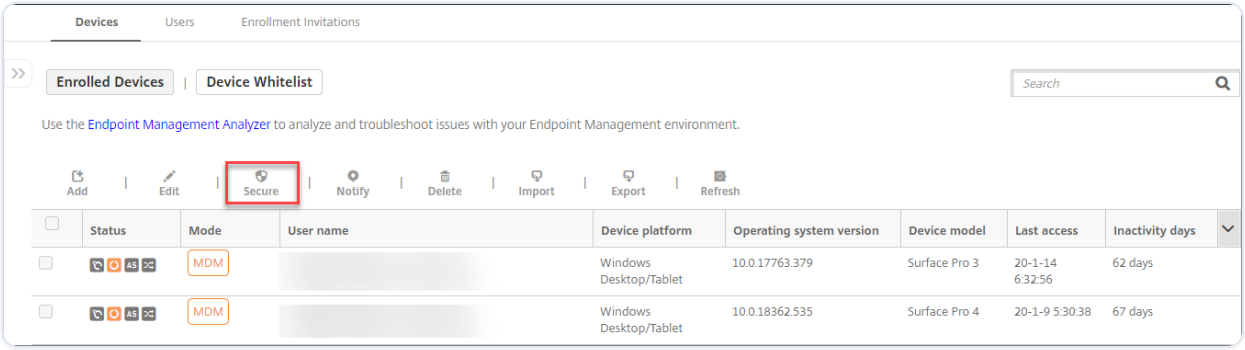
您可以使用密码设备策略配置与 PIN 码关联的更多设置。有关详细信息，请参阅macOS 设置。

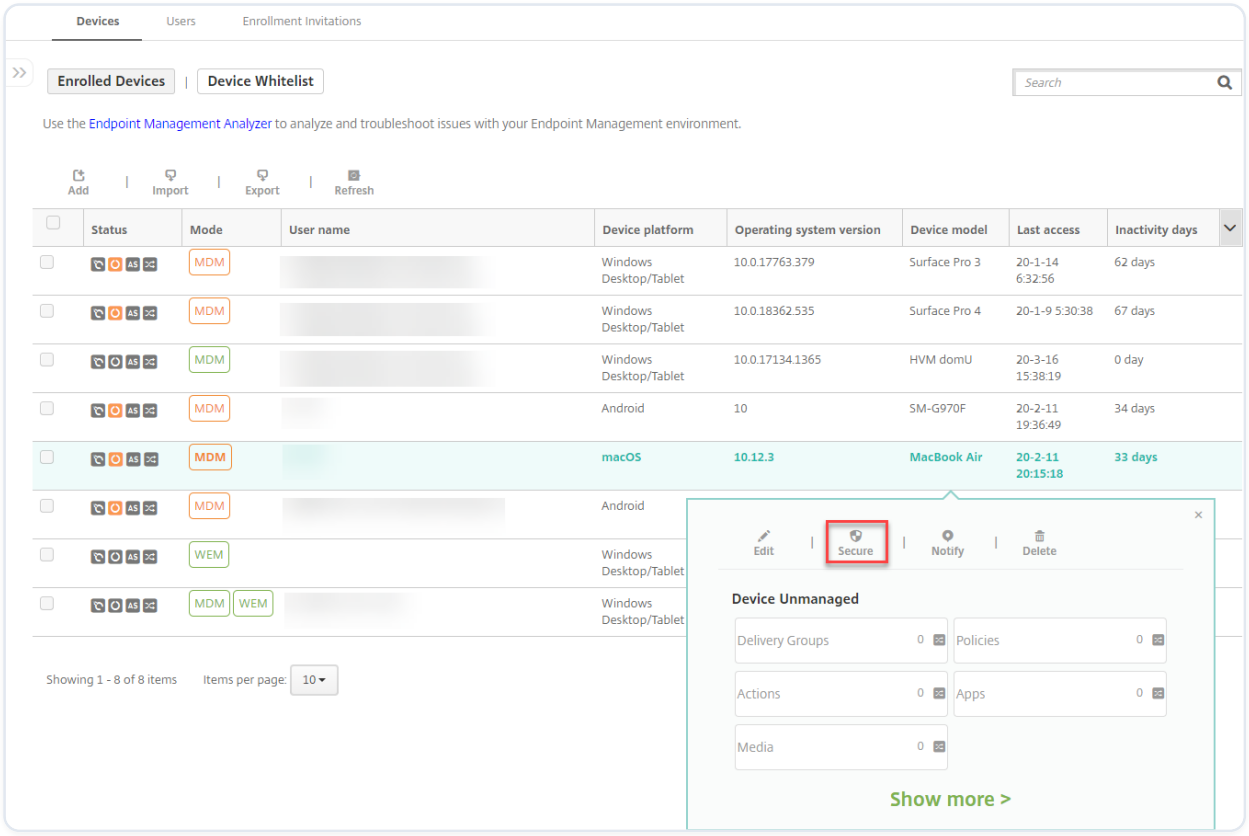
1. 单击 **管理 > 设备**。此时将显示 **设备** 页面。



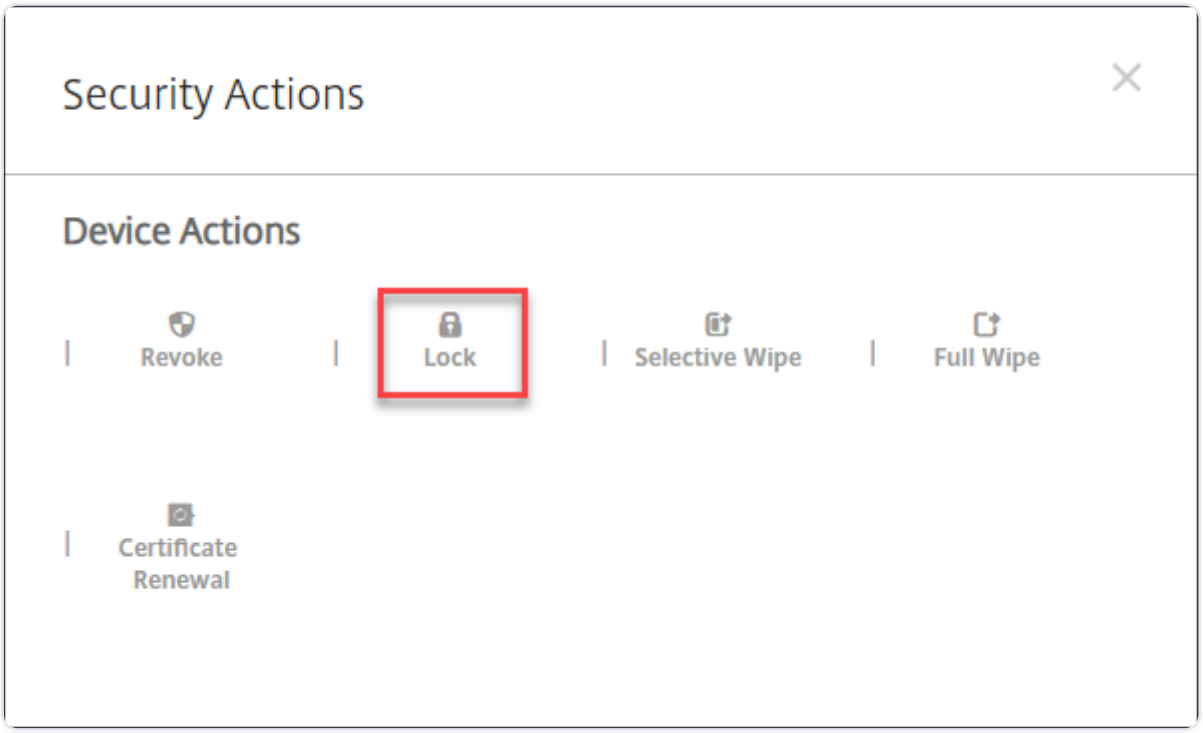
2. 选择要锁定的 macOS 设备。

   选中设备旁边的复选框，以在设备列表上方显示选项菜单。您也可以单击列表项中的其他任意位置，以在列表右侧显示选项菜单。

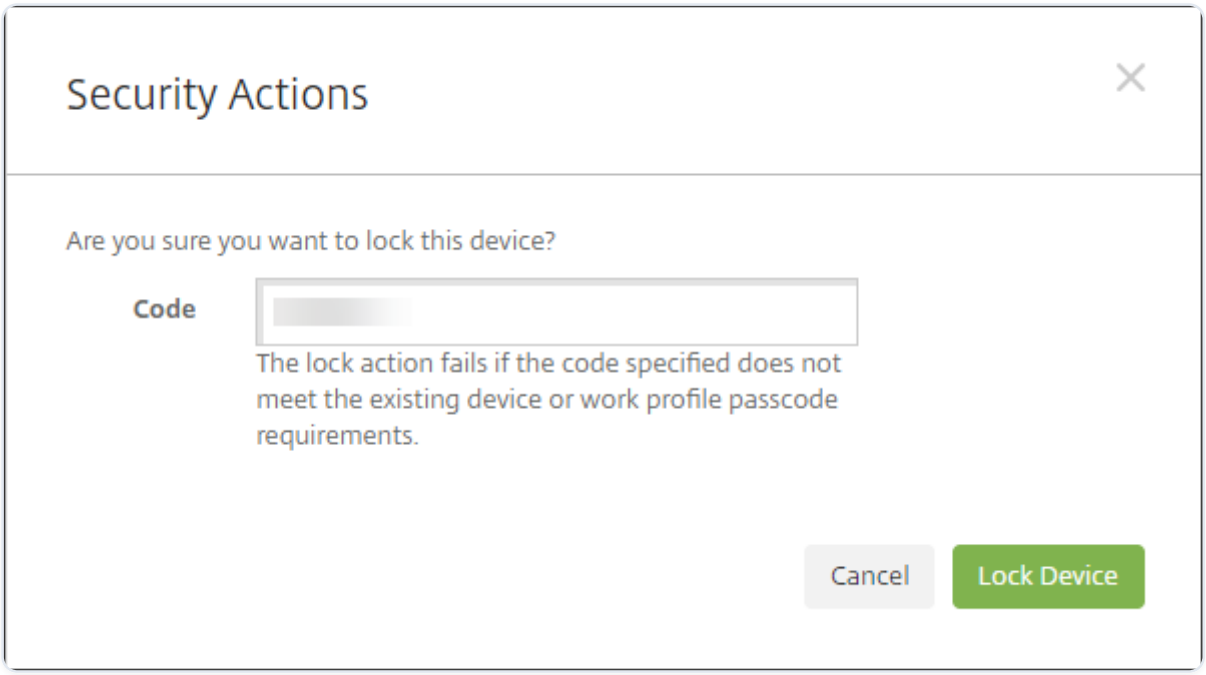




3. 在选项菜单中，单击“**安全**”。将显示“**安全操作**”对话框。



4. 单击“**锁定**”。将显示“**安全操作**”确认对话框。



5. 单击“**锁定设备**”。

> **重要提示：**
>
> 您还可以指定密码，而不是使用 Citrix 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，则锁定操作将失败。

引导令牌

引导令牌有助于在您登录 macOS 设备时向帐户授予 SecureToken macOS 属性。SecureToken 从一个受信任的帐户传递到另一个帐户。启用 SecureToken 的帐户可以在设备上执行加密操作。如果没有引导令牌，您需要在该设备上创建帐户，然后才能添加单个用户帐户，这需要遵循复杂的工作流。

Citrix Endpoint Management 支持为通过 Apple 部署计划注册的 macOS 设备托管引导令牌。您可以使用 Apple 部署计划注册直接从 Apple、参与的 Apple 授权经销商或运营商购买的 macOS 设备。有关注册 Apple 部署计划的信息，请参阅通过 Apple 部署计划部署设备。

引导令牌在设置助理工作流期间生成。具体来说，它们是在创建本地用户帐户期间生成的。设置助理在用户首次启动设备时运行。令牌保存在 Citrix Endpoint Management 数据库中，您和最终用户不可见。从 Citrix Endpoint Management 站点删除设备会删除令牌。执行出厂重置不会删除它们。

先决条件：

- 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

将引导令牌托管到 Citrix Endpoint Management 的一个好处是，可以为 FileVault 启用远程帐户，并能够解锁 FileVault 宗卷。有关 FileVault 的信息，请参阅 FileVault 设备策略。

通过 Apple 部署计划部署设备

Apple 部署计划 (ADP) 允许您在用户收到 Apple 设备之前，无需接触或准备设备即可自动将其注册到 Citrix Endpoint Management。用户拆开包装并激活设备后，设备会自动注册到 Citrix Endpoint Management，并且所有管理设置、应用程序和书籍都可供用户使用。

ADP 包括适用于商业组织的 Apple Business Manager (ABM) 和适用于教育组织的 Apple School Manager (ASM)。ABM 和 ASM 适用于 iOS、iPadOS 和 macOS 设备。有关设备资格的更多信息，请参阅Apple Business Manager 用户指南和Apple School Manager 用户指南。

> **注意：**
>
> ABM 和 ASM 结合了 Apple 之前的设备注册计划和批量采购计划。
>
> 本文将引导您完成使用 ABM 或 ASM 的一般部署工作流程：

1. 注册 ABM 或 ASM
2. 将您的 ABM 或 ASM 帐户连接到 Citrix Endpoint Management
3. 订购设备
4. 将设备分配给 Citrix Endpoint Management
5. 批量购买内容并将其与 Citrix Endpoint Management 同步
6. 为设备策略和应用程序配置部署规则
7. 添加已分配用户和资源的交付组

完成此部署过程后，设备即可拆箱并激活，以进行自动化设备注册。

先决条件

打开 Citrix Endpoint Management 和 Apple 之间连接所需的端口。有关详细信息，请参阅端口要求。

注册 ABM 或 ASM

要开始在 Apple 部署设备，请注册 ABM 或 ASM。

ABM 和 ASM 适用于组织而非个人。您必须提供许多组织详细信息和资料才能创建帐户。请求和接收帐户批准可能需要时间。

注册 ABM

要注册 ABM，请访问 business.apple.com。单击 **Enroll now** 申请新帐户。

最佳做法是使用您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

要创建您的 ASM 帐户，请访问 Apple School Manager 并按照说明注册。首次登录 ASM 时，将打开“设置助理”。

- 有关 ASM 先决条件、“设置助理”和管理任务的信息，请参阅 Apple School Manager 用户指南。
- 设置 ASM 用户帐户时，请使用与 Active Directory 域名不同的域名。例如，为 ASM 域名添加类似 `appleid` 的前缀。
- 将 ASM 连接到您的名册数据时，ASM 会为教师和学生创建托管式 Apple ID。您的名册数据包括教师、学生和班级。有关将名册数据添加到 ASM 的信息，请参阅此列表中前面链接的《Apple School Manager 用户指南》。
- 您可以自定义您机构的托管式 Apple ID 格式，如本列表中前面链接的《Apple School Manager 用户指南》中所述。

  > **重要提示：**
  >
  > 将 ASM 信息导入 Citrix Endpoint Management 后，请勿更改托管式 Apple ID。

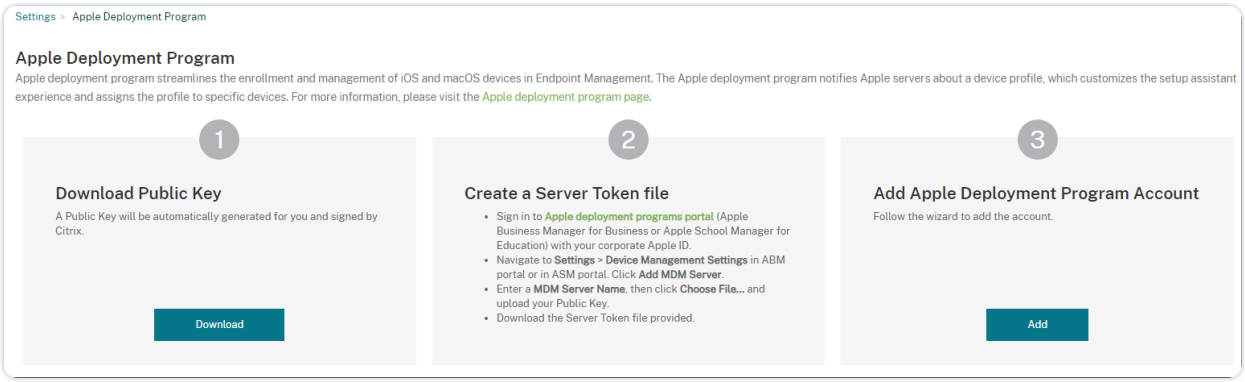
- 如果您通过经销商或运营商购买了设备，请将这些设备链接到 ASM。有关信息，请参阅此列表中前面链接的《Apple School Manager 用户指南》。

将您的 ABM 或 ASM 帐户连接到 Citrix Endpoint Management

创建 ABM 或 ASM 帐户后，将其连接到您的 Citrix Endpoint Management 服务器部署。

步骤 1: 从 Citrix Endpoint Management 服务器下载公钥

1. 在 Citrix Endpoint Management 控制台中，转到**设置 > Apple 部署计划**。



2. 在**下载公钥**下，单击**下载**。

步骤 2: 从您的 Apple 帐户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器帐户登录 Apple Business Manager 或 Apple School Manager。
2. 在侧边栏底部，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 Citrix Endpoint Management 服务器的名称。您键入的服务器名称仅供参考。它不是服务器 URL 或名称。
4. 在**上传公钥**下，单击**选择文件**。上传您从 Citrix Endpoint Management 下载的公钥，然后保存更改。
5. 单击**下载令牌**将服务器令牌文件下载到您的计算机。

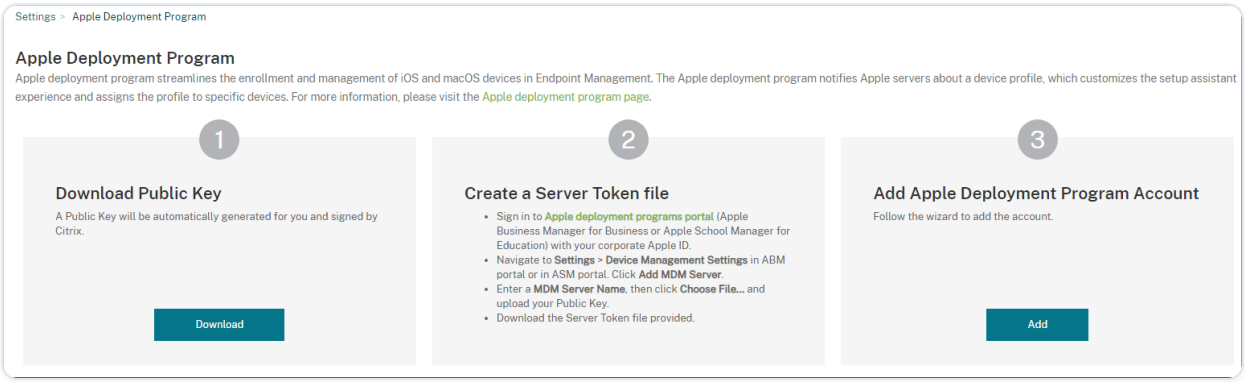
   在将 ABM 或 ASM 帐户添加到 Citrix Endpoint Management 时，您需要上传服务器令牌文件。导入令牌文件后，您的令牌信息将显示在 Citrix Endpoint Management 控制台中。
6. 在**默认设备分配**下，单击**更改**。选择您希望如何分配设备，然后提供所需信息。有关详细信息，请参阅 ABM 用户指南 或 Apple School Manager 用户指南。

步骤 3: 将您的帐户添加到 Citrix Endpoint Management

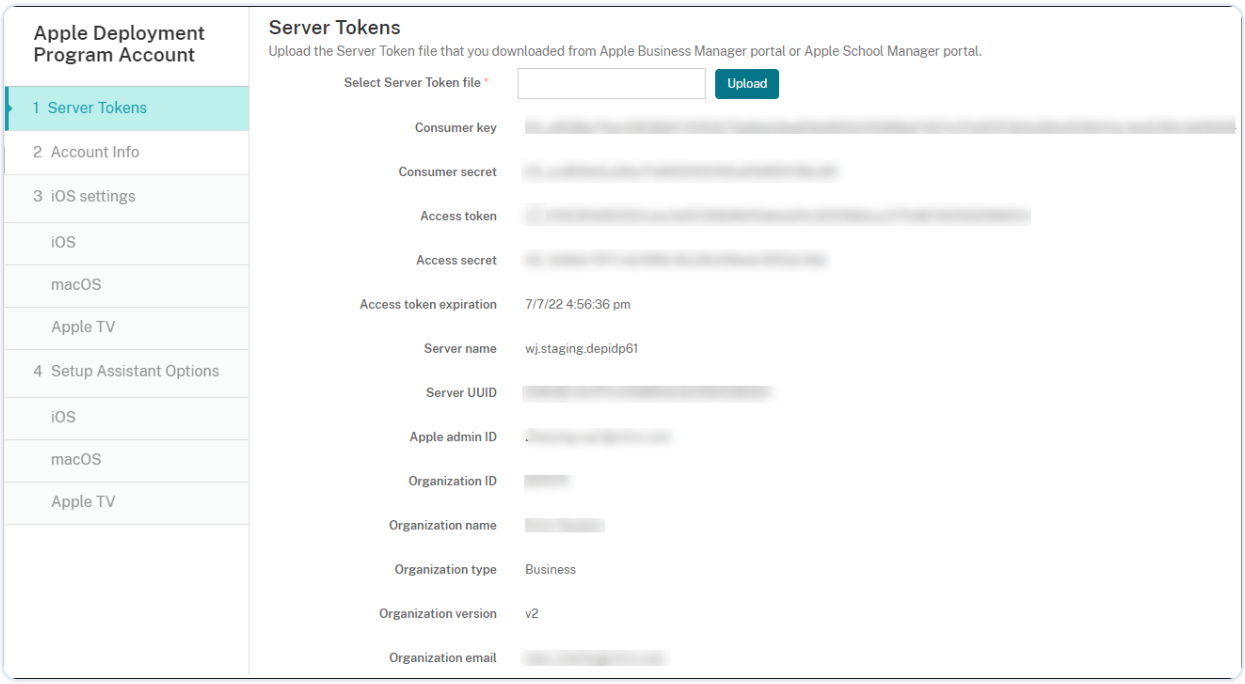
您可以将多个 ABM 或 ASM 帐户添加到 Citrix Endpoint Management。此功能使您能够按国家/地区、部门等使用不同的注册设置和设置助理选项。然后，您可以将 ABM 或 ASM 帐户与不同的设备策略关联。

例如，您可以将来自不同国家/地区的所有 ABM 或 ASM 帐户集中到同一个 Citrix Endpoint Management 服务器上，以导入和监督所有 ABM 或 ASM 设备。您首先根据部门、组织层次结构或其他结构自定义注册设置和设置助理选项。然后，您配置策略以在整个组织中提供适当的功能，并让用户获得适当的帮助。

1. 在 Citrix Endpoint Management 控制台中，转到 **设置 > Apple Deployment Program**，然后在 **添加 Apple Deployment Program 帐户** 下，单击 **添加**。

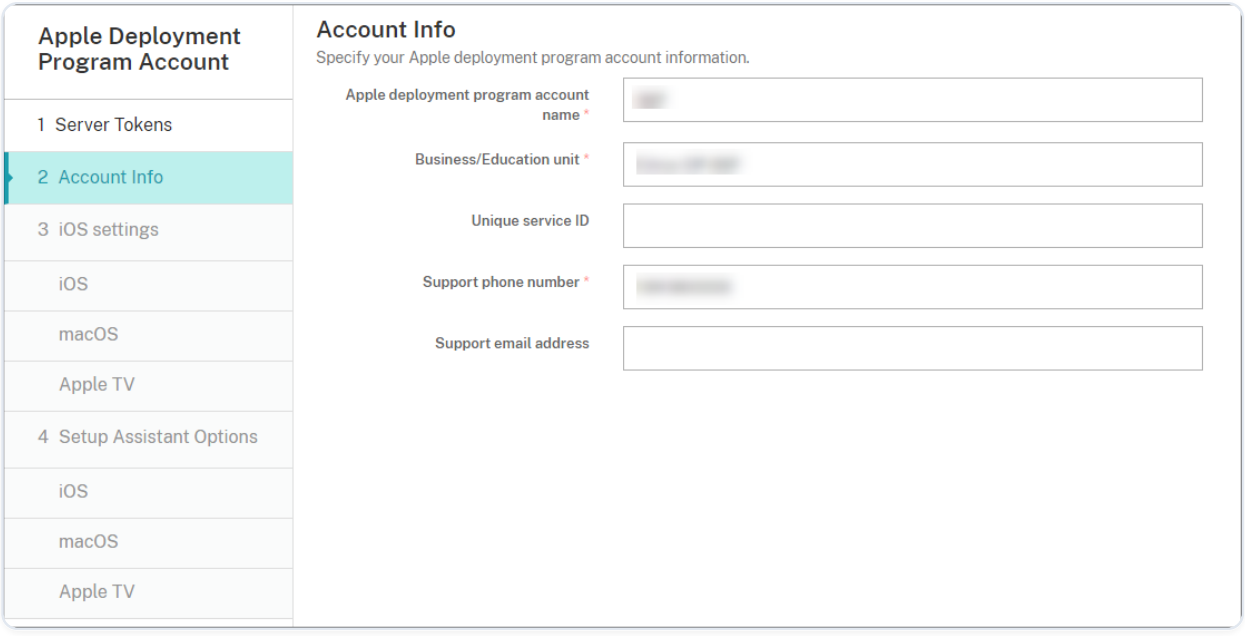


2. 在 **服务器令牌** 页面中，指定您的服务器令牌文件，然后单击 **上载**。



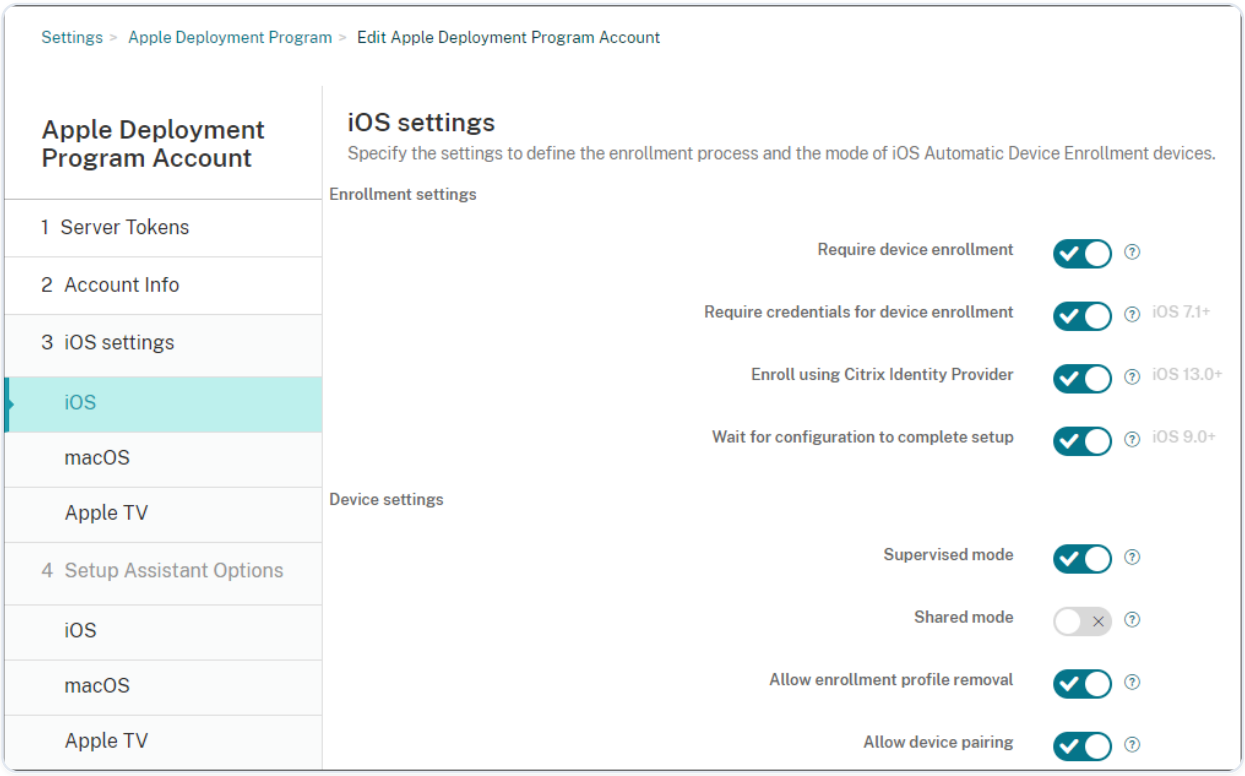
您的服务器令牌信息随即显示。

3. 在 **帐户信息** 页面中，指定以下设置：



- **Apple Deployment Program 帐户名称：** 此 ADP 帐户的唯一描述性名称，用于标识您组织 ADP 帐户的方式，例如按国家/地区或组织层次结构。
- **业务/教育单位：** 设备分配到的业务单位或部门。此字段为必填项。
- **唯一服务 ID：** 可选的唯一 ID，可帮助您进一步识别帐户。
- **支持电话号码：** 用户在设置过程中寻求帮助时拨打的支持电话号码。此字段为必填项。
- **支持电子邮件地址：** 可供最终用户使用的可选支持电子邮件地址。
- **教育后缀：** 适用于 ASM 帐户。键入通过此帐户注册的设备分配到的后缀。

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**。
- **要求设备注册凭据：** 是否要求用户在 ABM 和 ASM 设置期间输入其凭据。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 且未选择此选项，Citrix Endpoint Management 将创建 ABM 或 ASM 组件。此创建包括用户、Citrix Secure Hub、软件清单和部署组等组件。如果您选择此选项，Citrix Endpoint Management 不会创建这些组件。因此，如果您以后清除此选项，未输入凭据的用户将无法注册 ABM 或 ASM，因为这些组件不存在。在这种情况下，要添加 ABM 或 ASM 组件，请禁用然后重新启用 ABM 或 ASM 帐户。

- **使用 Citrix Identity Provider 注册：** 是否使用 Citrix Identity Provider 注册。此设置仅适用于 ABM 帐户。如果设置为 **开**，则启用 ADP 的 iOS 设备只能通过 Citrix 身份提供程序注册。默认值为 **关**。

  要启用此设置，您必须首先将 Citrix Identity Provider 配置为您的身份提供程序。转至 **设置 > 身份提供程序 (IDP)**，单击 **添加**，然后选择 **Citrix Identity Provider**。

  如果此设置设置为 **开**，请注意以下事项：

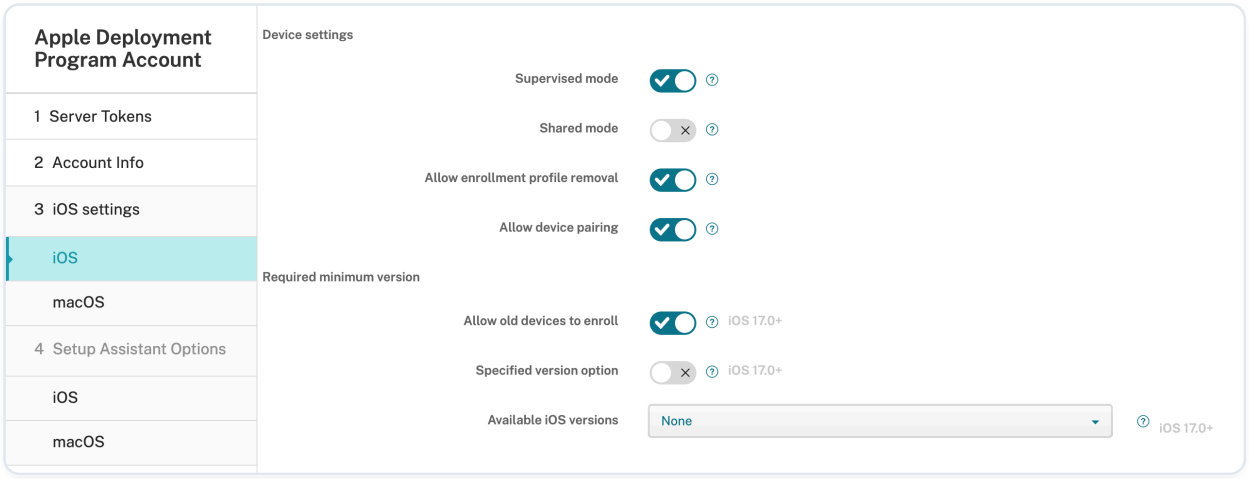
  - 您无法在 **设置 > 身份提供程序 (IDP)** 页面上删除相应的 Citrix Identity Provider 配置。
  - 编辑相应的 Citrix Identity Provider 配置时，您无法切换到其他身份提供程序。

- **等待配置完成设置：** 是否要求用户的设备处于“设置助理”模式，直到所有 MDM 资源部署到设备。此设置适用于受监督模式下的设备。默认值为 **关**。
- Apple 文档指出，当设备处于“设置助理”模式时，以下命令可能无法工作：
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - 请求镜像
  - 设备锁定

设备设置：

- **受监督模式：** 如果您使用 Apple Configurator 管理已注册设备，或者启用了“**等待配置完成设置**”时，请将其设置为“**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。
- **允许移除注册配置文件：** 是否允许设备使用可远程移除的配置文件。默认值为“**关**”。
- **允许设备配对：** 是否可以通过 Apple Music 和 Apple Configurator 管理已注册设备。默认值为“**关**”。

所需最低版本



- **允许旧设备注册：** 如果启用，即使设备无法升级到当前所需的最低版本，也可以注册。默认值为“开”。此选项仅适用于 iOS 17.0 及更高版本。
- **指定版本选项：** 是否允许管理员手动输入指定版本。默认值为“**关**”。此选项仅适用于 iOS 17.0 及更高版本。
- **可用 iOS 版本：** 您可以从列表中选择可用的 iOS 版本。如果设备的 iOS 版本低于当前版本，它将启动设备上的更新过程。如果版本将来过期，则使用可用版本列表中的最低版本。默认值为“无”，设置为“无”时将不生效。此选项仅适用于 iOS 17.0 及更高版本。
- **指定版本：** 如果设备的 iOS 版本低于当前版本，它将启动设备上的更新过程。如果版本将来过期，则使用可用版本列表中的最低版本。请输入正确的版本号，否则可能会出现未知错误。

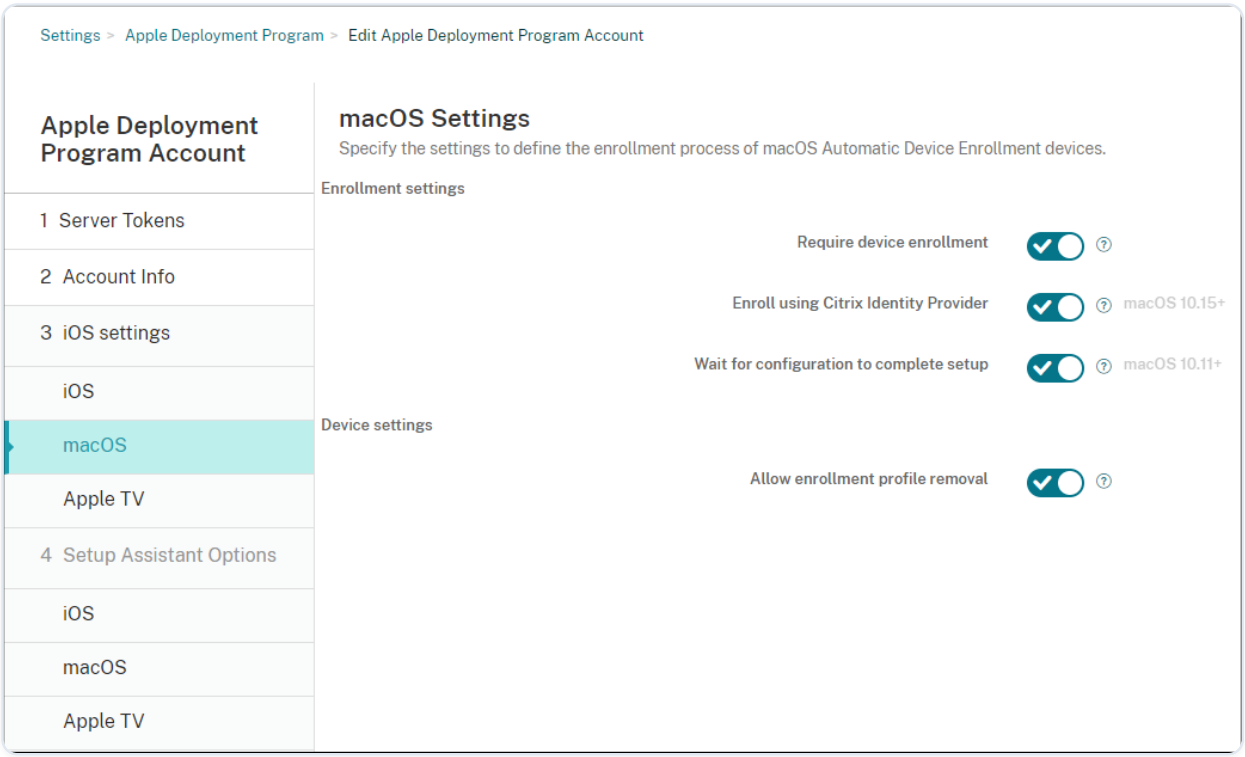
监督身份

如果您使用 GroundControl 工具，可以添加证书以执行以下操作：

- 覆盖配对限制以避免出现“信任此主机”提示。
- 通过 USB 升级受管设备操作，以在无需用户交互的情况下执行配置文件安装等活动。这样做允许 GroundControl 启用单应用模式和设备锁定以进行签出。
- 将备份恢复到 ABM 或 ASM 设备。

有关 GroundControl 的更多信息，请参阅 GroundControl 网站。

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 Identity Provider 注册：** 是否使用 Citrix Identity Provider 注册。此设置仅适用于 ABM 帐户。如果设置为“**开**”，则启用 ADP 的 macOS 设备只能通过 Citrix 身份提供程序注册。默认值为“**关**”。

  要启用此设置，您必须首先将 Citrix Identity Provider 配置为您的身份提供程序。转到“**设置 > 身份提供程序 (IDP)**”，单击“**添加**”，然后选择“**Citrix Identity Provider**”。

  如果此设置设置为“**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 Identity Provider 配置。
  - 编辑相应的 Citrix Identity Provider 配置时，您无法切换到其他身份提供程序。
- **等待配置完成设置：** 如果设置为“**开**”，则 macOS 设备不会在设置助手中继续，直到 MDM 资源密码部署到设备。该部署发生在本地帐户创建之前。此设置适用于 macOS 10.11 及更高版本的设备。默认值为“**关**”。

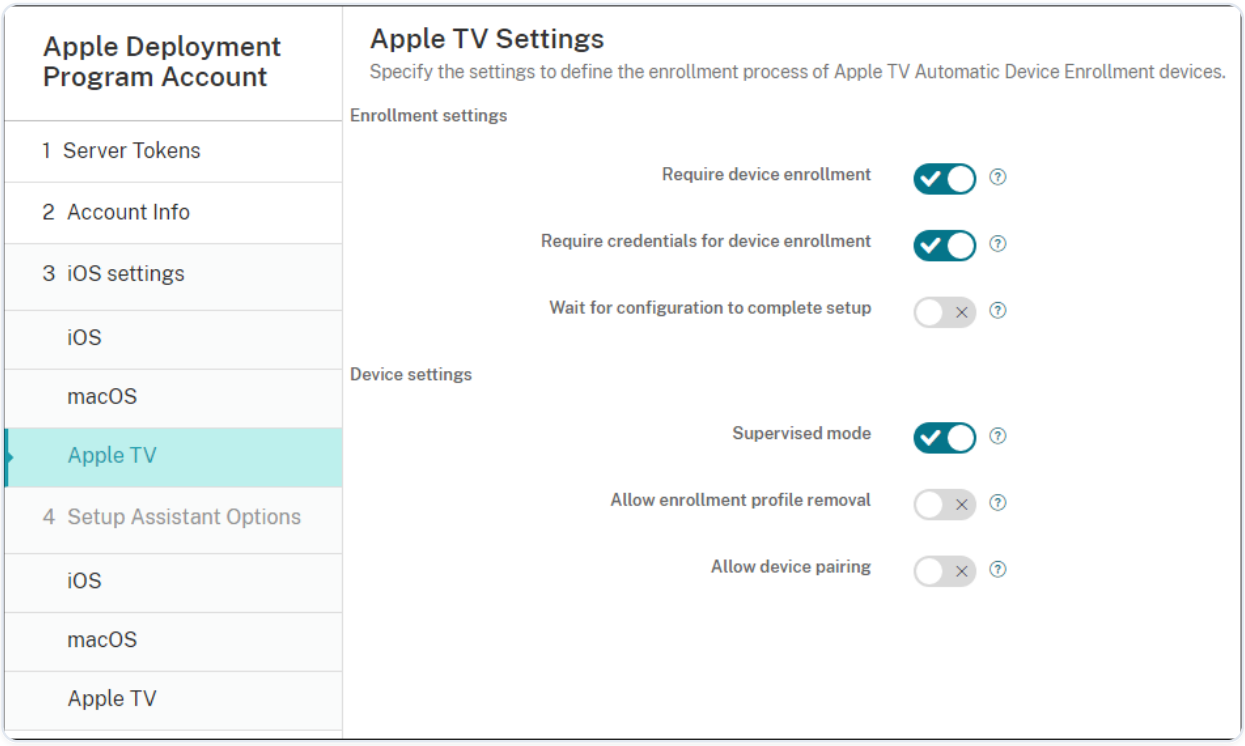
设备设置：

- **允许删除注册配置文件：** 是否允许设备使用可远程删除的配置文件。默认值为“**关**”。

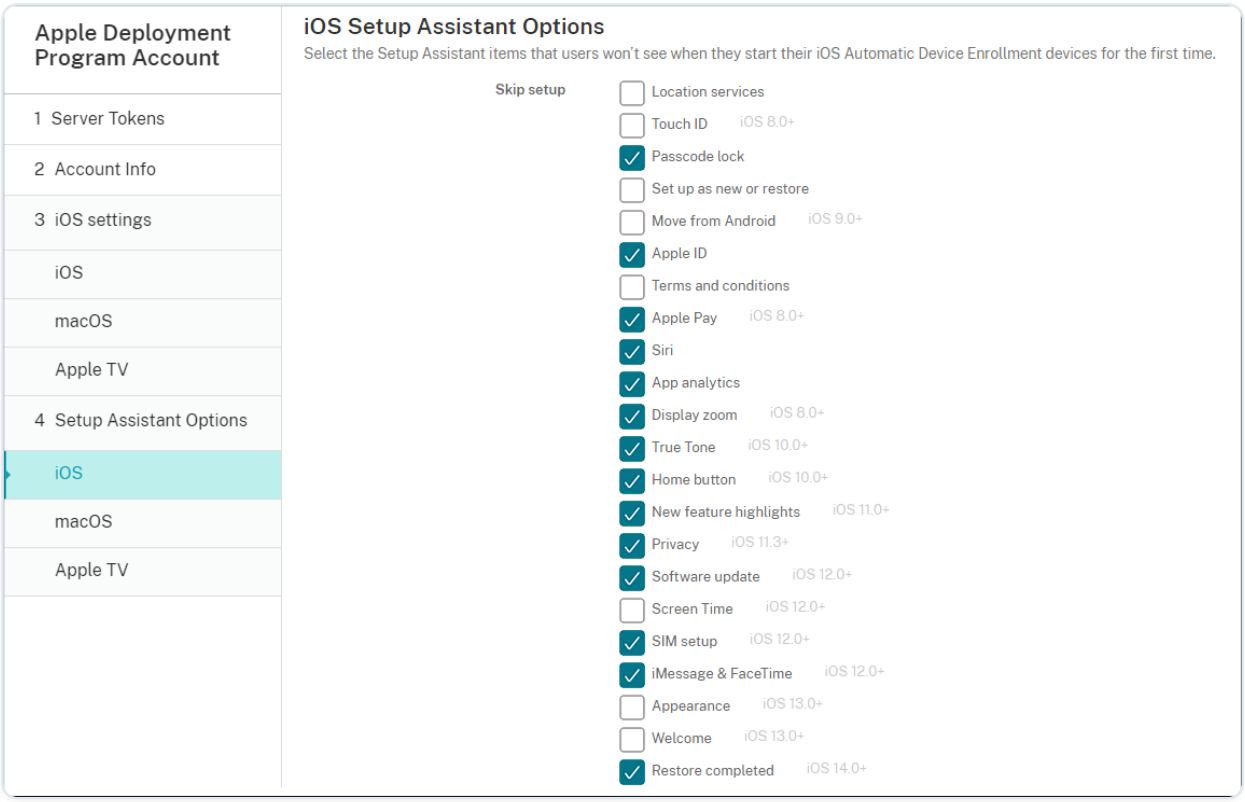
6. 在 **Apple TV 设置**中，指定以下设置：

   - **要求设备注册：** 阻止用户跳过注册。

- **要求设备注册凭据：** 在注册期间要求提供凭据。当此设置关闭时，Apple TV 将注册为默认的“设备注册计划用户”。
- **等待配置完成设置：** 设备在 **设置助理** 屏幕中等待，直到所有资源部署完毕。
- **监管模式：** 在配置限制时为管理员提供更多功能。
- **允许移除注册配置文件：** 允许用户移除注册配置文件。
- **允许设备配对：** 允许通过设备注册计划注册的设备通过 Apple 工具进行管理，例如 Apple App Store 和 Apple Configurator。



7. 在 **iOS 设置助理选项**中，选择用户首次启动设备时 iOS 设置助理跳过的步骤。当屏幕被跳过时，相关功能将使用默认设置。除非您完全限制对这些功能的访问，否则用户可以在设置完成后配置跳过的功能。有关限制对功能访问的更多信息，请参阅限制设备策略。所有项目的默认值均已清除。以下说明解释了选择某个设置时会发生什么。

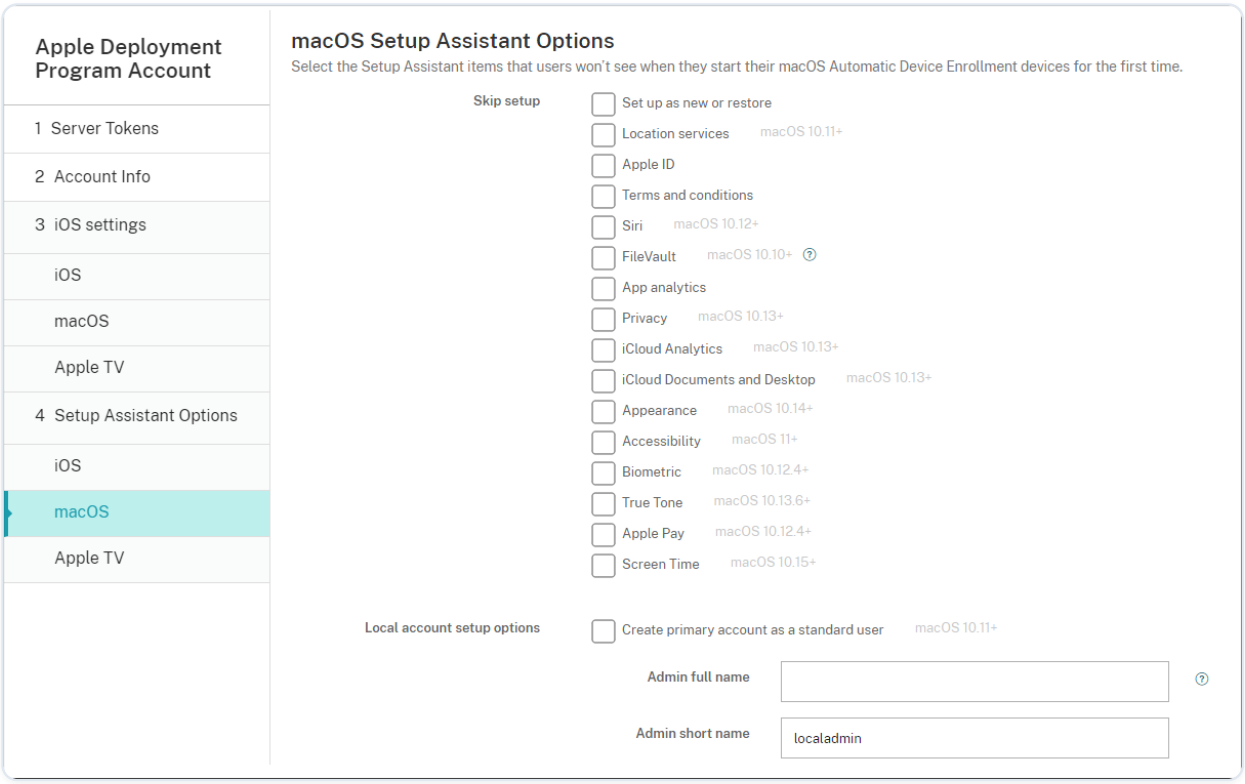


- **定位服务：** 阻止用户在设备上设置定位服务。
- **触控 ID：** 阻止用户在 iOS 设备上设置触控 ID 或面容 ID。在 iOS 15 中已弃用。
- **密码锁：** 阻止用户为设备设置密码。如果不存在密码，用户将无法使用触控 ID 或 Apple Pay。
- **设置为新设备或恢复：** 阻止用户将设备设置为新设备或从 iCloud 或 Apple App Store 备份恢复。
- **从 Android 迁移：** 阻止用户将数据从 Android 设备传输到 iOS 设备。此选项仅在选择**设置为新设备或恢复**时可用（即，跳过该步骤）。
- **Apple ID：**阻止用户为设备设置托管式 Apple ID 帐户。
- **条款和条件：**阻止用户阅读并接受设备使用条款和条件。
- **Apple Pay：**阻止用户设置 Apple Pay。如果此设置已清除，则用户必须设置触控 ID 和 Apple ID。请确保这些设置已清除。
- **Siri：**阻止用户配置 Siri。
- **应用分析：**阻止用户设置是否与 Apple 共享崩溃数据和使用统计信息。
- **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）。在 iOS 17 中已弃用。
- **原彩显示：**阻止用户设置四通道传感器以动态调整显示屏的白平衡。
- **主屏幕按钮：**阻止用户设置主屏幕按钮的反馈样式。在 iOS 15 中已弃用。

- **新功能亮点：**阻止用户查看显示 Apple 软件新功能信息的屏幕。
- **隐私：**阻止用户查看数据和隐私面板。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。
- **屏幕使用时间：**阻止用户启用屏幕使用时间。适用于 iOS 12.0 及更高版本。
- **SIM 卡设置：**阻止用户设置蜂窝网络套餐。适用于 iOS 12.0 及更高版本。
- **iMessage 与 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“**开始使用**”屏幕。适用于 iOS 13.0 及更高版本。
- **恢复完成**：阻止用户在设置过程中看到恢复是否完成。适用于 iOS 14.0 及更高版本。
- **更新完成**：阻止用户在设置过程中看到软件更新是否完成。适用于 iOS 14.0 及更高版本。
- **App Store**：阻止用户设置 App Store。适用于 iOS 11.1 及更高版本。
- **操作按钮**：阻止用户看到“操作按钮”配置窗格。适用于 iOS 17.0 及更高版本。
- **锁定模式**：如果已设置 Apple 帐户，则阻止用户看到“锁定模式”窗格。适用于 iOS 17.1 及更高版本。
- **智能**：阻止用户看到“智能”窗格。适用于 iOS 18.0 及更高版本。
- **相机按钮**：阻止用户看到“相机按钮”窗格。适用于 iOS 18.0 及更高版本。

该帐户显示在**设置 > Apple 部署计划**。

8. 在“**macOS 设置助理选项**”中，选择用户首次启动设备时 macOS 设置助理跳过的步骤。跳过某个屏幕时，相关功能将使用默认设置。除非您完全限制对这些功能的访问，否则用户可以在设置完成后配置跳过的功能。有关限制对功能访问的更多信息，请参阅限制设备策略。所有项目的默认设置均已清除。以下说明解释了选择某个设置时会发生什么。



- **设置为新设备或恢复**：阻止用户将设备设置为新设备，或从时间机器备份恢复，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式 Apple ID 帐户。
- **条款和条件**：阻止用户阅读和接受设备使用条款和条件。
- **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。Citrix Endpoint Management 仅在系统具有单个本地用户帐户且该帐户已登录 iCloud 时才应用 FileVault 设置。

  您可以使用 macOS FileVault 磁盘加密功能通过加密其内容来保护系统卷 (https://support.apple.com/zh-cn/HT204837)。如果您在未启用 FileVault 的新型便携式 Mac 上运行设置助理，系统可能会提示您启用此功能。此提示会出现在新系统以及升级到 OS X 10.10 或 10.11 的系统上，但前提是系统具有单个本地管理员帐户且该帐户已登录 iCloud。
- **应用分析**： 阻止用户设置是否与 Apple 共享崩溃数据和使用统计信息。
- **隐私**： 阻止用户查看“数据与隐私”窗格。适用于 macOS 10.13 及更高版本。
- **iCloud 分析**： 阻止用户选择是否将诊断 iCloud 数据发送给 Apple。适用于 macOS 10.13 及更高版本。
- **iCloud 文稿和桌面**： 阻止用户设置 iCloud 桌面和文稿。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：** 阻止用户自动听到 Voice Over。仅当设备连接到以太网时可用。适用于 macOS 11 及更高版本。
- **生物识别：** 阻止用户设置触控 ID 和面容 ID。适用于 macOS 10.12.4 及更高版本。
- **原彩显示：** 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。如果此设置被清除，用户必须设置触控 ID 和 Apple ID。确保已清除**Apple ID**和**生物识别**设置。
- **屏幕使用时间：** 阻止用户启用屏幕使用时间。适用于 macOS 10.15 及更高版本。
- **App Store：** 阻止用户设置 App Store。适用于 macOS 11.1 及更高版本。
- **使用 Apple Watch 解锁：** 阻止用户使用 Apple Watch 解锁其 Mac。适用于 macOS 12 及更高版本。
- **本地账户设置选项：** 指定在设备上创建账户的设置。Citrix Endpoint Management 首先使用您在此处指定的信息创建本地管理员账户。当用户激活其设备时，将创建一个用户账户作为主账户。**将主账户创建为标准用户**选项决定主账户是否具有管理员权限。

> **重要提示：**
>
> 您只能在将 **macOS 设置**页面上的**等待配置完成设置**设置为**开**之后，才能选择**将主账户创建为标准用户**。

- **将主账户创建为标准用户：** 选中此选项后，Citrix Endpoint Management 将创建具有标准权限的用户，而不是授予用户设备上的管理员权限。如果您希望授予用户设备上的管理员权限，请跳过此选项。默认情况下，此选项未选中。
- **管理员全名：** 键入系统为管理员账户显示的名称。
- **管理员短名称：** 键入设备为主文件夹和 shell 中显示的名称。
- **管理员密码：** 为管理员账户键入一个安全密码。
- **在“用户与群组”中显示管理员账户：** 如果取消选中，管理员账户将不会显示在 macOS 设置的**用户与群组**中。如果您将主账户创建为标准用户，请启用此设置以隐藏 Citrix Endpoint Management 首先创建的管理员账户。

为了增强安全性，Citrix Endpoint Management 会检查是否每天轮换管理员账户的密码。默认情况下，Citrix Endpoint Management 每 7 天轮换一次密码。要更改默认设置，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。

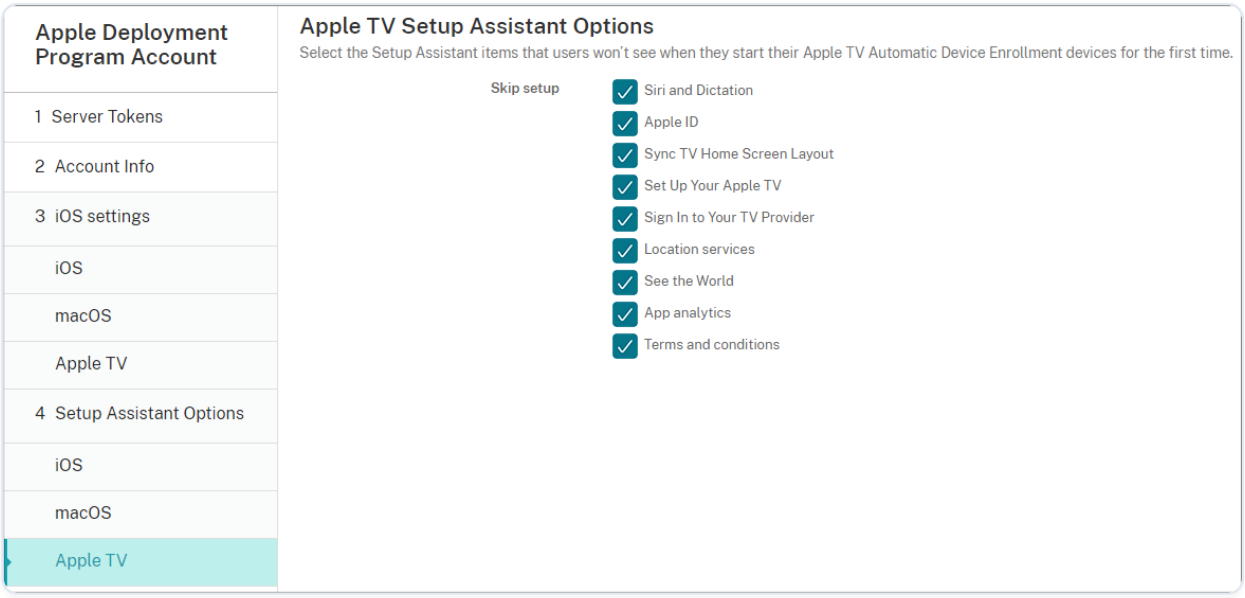
为了提高密码强度和安全性，Citrix Endpoint Management 生成的密码如下：

- 12 个字符长
- 3 个大写字母
- 3 个小写字母
- 3 个数字
- 3 个特殊字符：`! \@ # \$ % \^ * ? + = -`

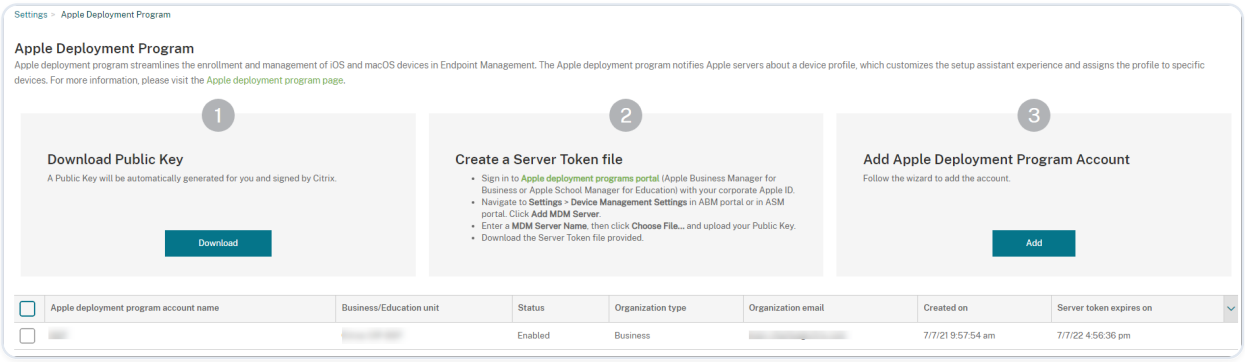
要查看设备的上一个密码、当前密码和密码更改状态，请转至**管理 > 设备**。单击该设备，单击**显示更多**，然后查看**设备详细信息 > 常规**页面。**安全**部分显示以下内容：

- **上一个管理员密码：** 允许您查看上一个密码。Citrix Endpoint Management 仅显示最后一个密码。单击“**显示密码**”以查看密码。
- **当前管理员密码：** 允许您查看当前密码。
- **更改管理员密码：** 允许您查看密码更改状态。根据实际状态，可能会显示以下信息：
  - 已在 \<特定时间值\> 请求更改密码。
  - 密码已在 \<特定时间值\> 更改。
  - 尝试更改密码失败，时间为 \<特定时间值\>。
  - 密码尚未更改。

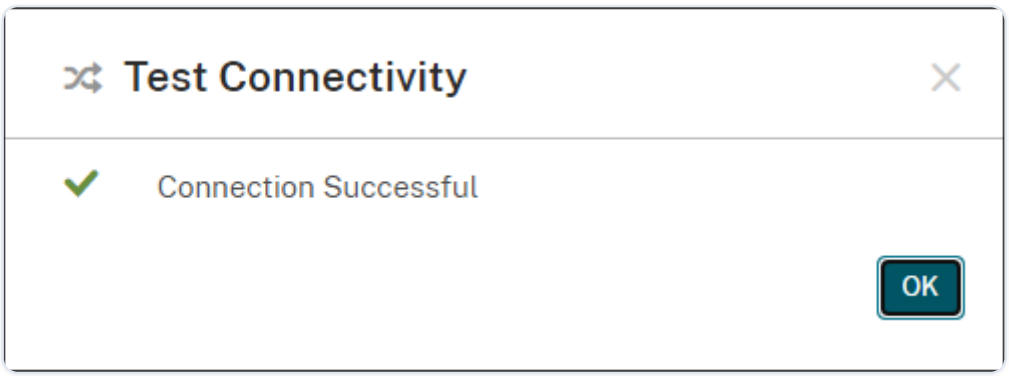
9. 在“**Apple TV 设置助理选项**”中，选择用户首次启动设备时跳过的 Apple TV 设置助理步骤。所有项目的默认设置均为未选中。保存更改。



10. 该帐户显示在“**设置 > Apple 部署计划**”中。要测试 Citrix Endpoint Management 与 Apple 之间的连接，请选择该帐户，然后单击“**测试连接**”。



将显示状态消息。



订购设备

您可以直接通过以下渠道订购设备：

- Apple。向卖家提供您的 Apple 客户编号。
- 参与的 Apple 授权经销商或运营商。向卖家提供您的组织 ID 并获取其经销商 ID。

有关管理设备供应商的更多信息，请参阅Apple Business Manager 用户指南或Apple School Manager 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 Citrix Endpoint Management

在 ABM 或 ASM 门户中，搜索订单号并使用它将此订单中的设备分配给您的 Citrix Endpoint Management。您还可以使用 Apple Configurator 2 将 iPhone、iPad、iPod touch 和 Apple TV 设备添加到 ABM 或 ASM，无论设备是在何处购买的。

有关详细信息，请参阅Apple Business Manager 用户指南或Apple School Manager 用户指南。

批量购买内容并将其同步到 Citrix 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图书的许可证。要使您的 Citrix Endpoint Management 能够与 ABM 或 ASM 通信以获取分发许可证信息，请完成以下步骤：

1. 在 ABM 或 ASM 门户中，从“**应用程序和图书**”购买公共应用程序和图书，并从“**自定义应用程序**”购买为您的 Citrix Endpoint Management 开发的自定义应用程序。
2. 在 ABM 或 ASM 门户中，下载分配给您的 Citrix Endpoint Management 的内容令牌。

   有关步骤 1 和 2 的更多信息，请参阅Apple Business Manager 用户指南或Apple School Manager 用户指南。
3. 在 Citrix Endpoint Management 控制台中，根据您下载的内容令牌创建批量购买帐户。

   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图书将显示在**管理** > **应用程序**中，您分配给 Citrix 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

在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. 指定策略或应用程序部署到特定的 ABM 帐户，或部署到除所选帐户之外的所有 ABM 帐户。

ABM 帐户列表仅包含状态为“已启用”或“已禁用”的帐户。如果 ABM 帐户已禁用，则 ABM 设备不属于此帐户。因此，Citrix Endpoint Management 不会将应用程序或策略部署到该设备。

在以下示例中，设备策略仅部署到 ABM 帐户名称为“ABM Account NR.”的设备。

Apple 设备计划设置屏幕(/en-us/citrix-endpoint-management/media/apple-dep-deployment-rule-policy-example.png)

批量注册 Apple 设备

您可以通过两种方式在 Citrix Endpoint Management 中批量注册 iOS、iPadOS 和 macOS 设备：

- 使用 Apple 部署计划 (ADP) 注册您直接从 Apple 或从参与的 Apple 授权经销商或运营商处购买的 Apple 设备。

  有关部署启用 ADP 的设备的详细信息，请参阅通过 Apple 部署计划部署设备。本文介绍了用户如何注册启用 ADP 的设备以及如何重新注册设备。
- 使用 Apple Configurator 2 注册 iOS 设备，无论您是否直接从 Apple 购买。

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 Business Manager (ABM) 和面向教育的 Apple School Manager (ASM)。通过 ADP 进行批量注册具有以下特点：

- 您无需接触或准备设备。
- 在 Citrix Endpoint Management 中完成部署设置后，您可以将设备提供给用户，用户可以立即开始使用这些设备。
- 您可以通过消除部分设置助理步骤来简化用户的设置过程。
- 有关设置 ABM 和 ASM 的详细信息，请参阅 Apple Business Manager 和 Apple School Manager 提供的文档。

通过 Apple Configurator 2 进行批量注册具有以下特点：

- 您将 iOS 设备连接到运行 macOS 10.7.2 或更高版本以及 Apple Configurator 2 应用程序的 Mac。您通过 Apple Configurator 2 准备 iOS 设备并配置策略。
- 设备在设置过程中会自动注册到 Citrix Endpoint Management。设置完成后，Citrix Endpoint Management 会将策略、应用程序和其他资源推送到设备。然后，您可以开始管理这些设备。
- 有关使用 Apple Configurator 2 的更多信息，请参阅 Apple Configurator 帮助。

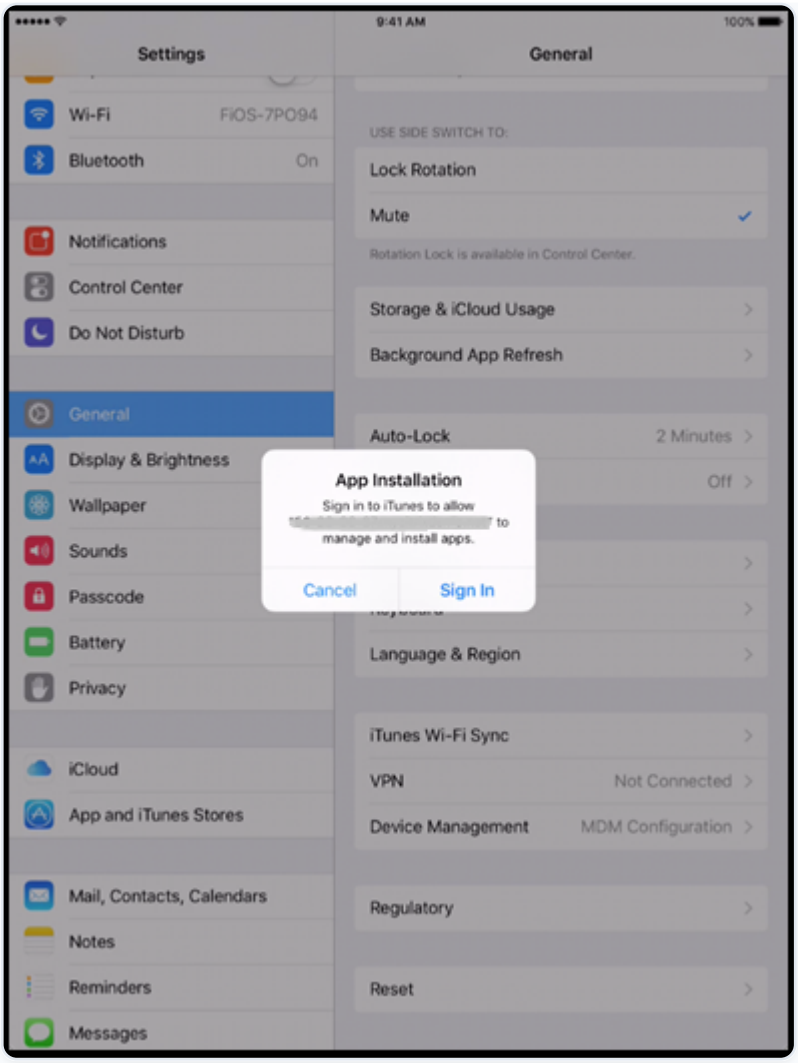
用户如何注册启用 ADP 的设备

用户按以下步骤在 Citrix Endpoint Management 中注册其设备：

1. 用户启动其设备。
2. Citrix 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. 设备自动启动 Citrix Endpoint Management 设备注册过程。
5. 用户继续在其设备上配置其他初始设置。
6. 在主屏幕中，系统可能会提示用户登录 Apple App Store，以便他们可以下载 Citrix Secure Hub。

> **注意：**

> 如果您将 Citrix 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 Citrix Secure Hub 应用程序，则此步骤是可选的。在这种情况下，您无需创建 Apple App Store 帐户或使用现有帐户。



7. 用户打开 Citrix 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。

   Citrix Endpoint Management 将所有剩余的所需应用程序部署到设备。

重新注册启用 ADP 的设备

启用 ADP 的设备从出厂重置状态注册。要重新注册启用 ADP 的设备，您必须首先完成完全擦除以取消注册设备。详细步骤如下：

1. 在 **管理 > 设备** 页面上，选择设备。
2. 单击 **安全性**。
3. 单击 **完全擦除** 以取消注册设备并将其恢复到出厂设置状态。

4. 启动设备。

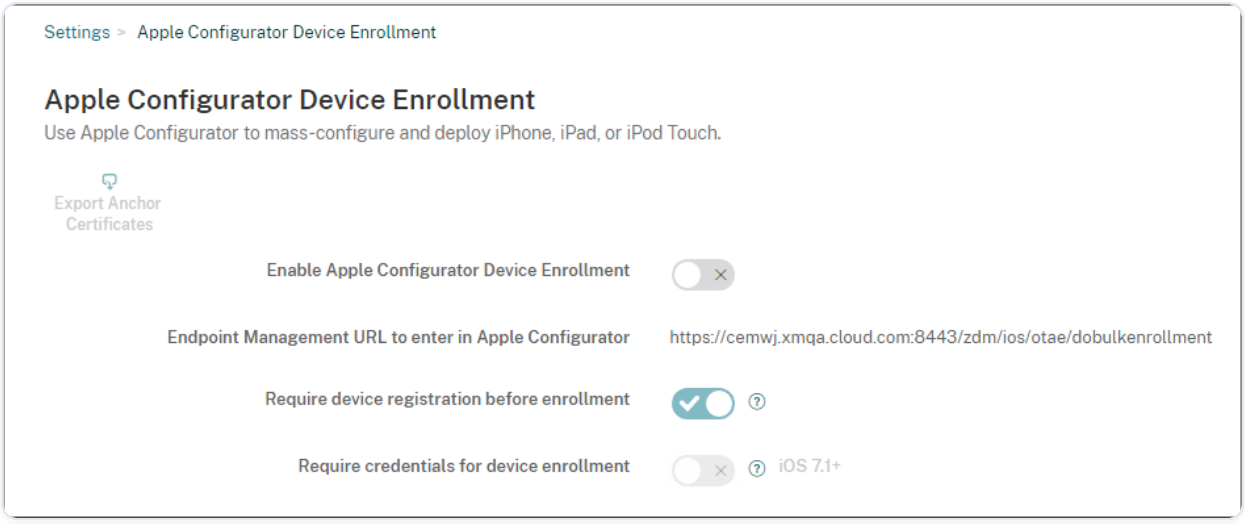
> **重要提示：**
>
> 请勿使用 **选择性擦除** 来取消注册已启用 ADP 的设备，因为 ADP 注册要求设备处于出厂重置状态。

使用 Apple Configurator 2 部署设备

您可以使用 Apple Configurator 2 部署大量设备，并配置其设置、应用程序和数据，然后将这些设备注册到 Citrix Endpoint Management 中。

步骤 1：在 Citrix Endpoint Management 中配置设置

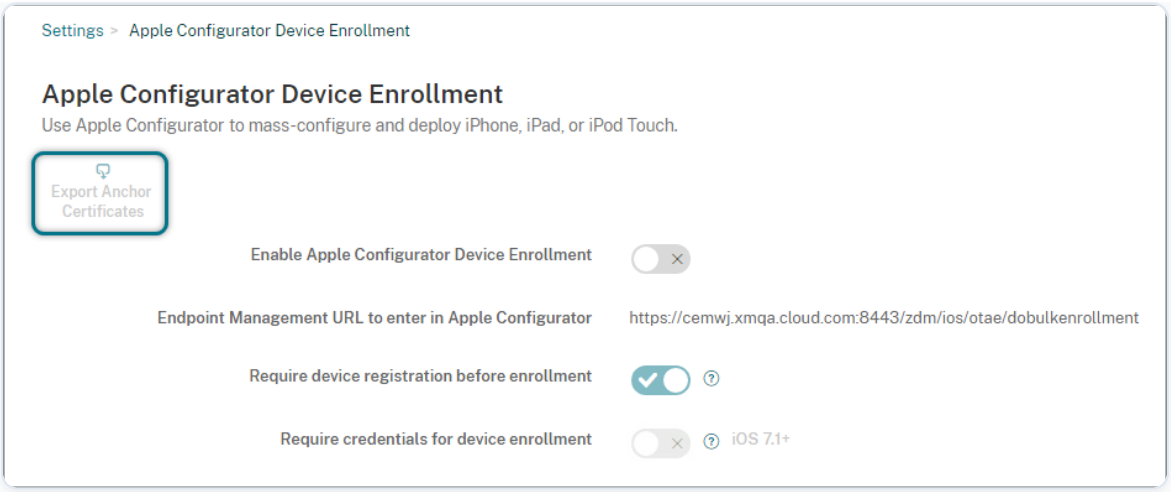
1. 在 Citrix Endpoint Management 控制台中，转至 **设置 > Apple Configurator 设备注册**。



2. 将 **启用 Apple Configurator 设备注册** 设置为 **是**。
3. 复制 **要在 Apple Configurator 中输入的注册 URL** 设置，并在 Apple Configurator 2 中配置设置时粘贴此 URL。此设置提供与 Apple 通信的 Citrix Endpoint Management 服务器的 URL。注册 URL 是 Citrix Endpoint Management 服务器的完全限定域名 (FQDN)，例如 `mdm.server.url.com`，或 IP 地址。
4. 为防止未知设备注册，请将 **注册前需要设备注册** 设置为 **是**。注意：如果此设置设为 **是**，则必须在注册前手动或通过 CSV 文件将配置的设备添加到 Citrix Endpoint Management 中的 **管理 > 设备**。
5. 要要求 iOS 设备用户在注册时输入其凭据，请将 **设备注册需要凭据** 设置为 **是**。默认值为 **否**。

> **注意：**

> 如果 Citrix Endpoint Management 服务器正在使用受信任的 SSL 证书，请跳过此步骤。单击 **导出锚点证书** 并将 certchain.pem 文件保存到 macOS 钥匙串（登录或系统）中。



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 连接线将 Apple 设备连接到 Mac。您可以同时配置多达 30 台连接的设备。如果没有 Dock 连接器，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。配置器会显示您可以准备进行监督的任何设备。
4. 要准备设备进行监督：
   - 如果您打算通过定期重新应用配置来保持对设备的控制，请选择**监督设备**。单击**下一步**。

     > **重要提示：**
     >
     > 将设备置于监督模式会在设备上安装所选版本的 iOS，并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**最新**以获取要安装的最新版本 iOS。
5. 在**注册 MDM 服务器**中，选择一个 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，为服务器提供一个名称，并从 Citrix Endpoint Management 控制台粘贴 MDM 服务器 URL。
7. 在**分配给组织**中，选择一个组织来监督设备。

有关使用 Apple Configurator 2 准备设备的更多信息，请参阅 Apple Configurator 帮助页面，准备设备。

8. 准备好每台设备后，将其打开以启动 iOS 设置助理，该助理会为设备首次使用做好准备。

使用 Apple Configurator 2 将设备添加到 ABM 或 ASM

无论设备购自何处，您都可以使用 Apple Configurator 2 将 iPhone、iPad 和 Apple TV 设备添加到您的 ABM 或 ASM 帐户。 添加设备后，它们将出现在“**设备**”部分。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 Business Manager 用户指南 或 Apple School Manager 用户指南。

续订 ADP 令牌

当您的 ADP 令牌过期时，Citrix Endpoint Management 会显示许可证过期警告。从 ASM 或 ABM 替换令牌。

步骤 1：从 Citrix Endpoint Management 服务器下载公钥

1. 在 Citrix Endpoint Management 控制台中，转到“**设置 > Apple 部署计划**”以下载新的公钥。

步骤 2：从您的 Apple 帐户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 Citrix 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 Citrix Endpoint Management 中上传服务器令牌文件

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**”，然后上传您的服务器令牌文件。
3. 单击“**下一步**”并保存更改。

与 Apple 教育功能集成

在使用 Apple 教育的环境中，您可以将 Citrix Endpoint Management 用作移动设备管理 (MDM) 解决方案。Citrix Endpoint Management 支持包括 Apple 校园教务管理 (ASM) 和适用于 iPad 的课堂 App。Citrix Endpoint Management 教育配置设备策略可配置教师和学生设备以供 Apple 教育使用。

您向教师和学生提供预配置和受监督的 iPad。该配置包括在 Citrix Endpoint Management 中注册 ASM、配置了新密码的托管 Apple ID 帐户以及所需的批量采购应用和 iBooks。

有关 Apple 教育功能的更多信息，请参阅 Apple 教育 站点以及同一站点上的 Apple 教育部署指南。

Apple 校园教务管理

请按照以下常规步骤将 Citrix Endpoint Management 与 ASM 集成。

1. 在 ASM 中为您的机构创建帐户，以在 ASM 中注册您的机构。
2. 为 Apple 校园教务管理配置教育批量采购帐户。
3. 为 Apple 校园教务管理用户添加密码。
4. 规划资源并将资源和交付组添加到 Citrix Endpoint Management。
5. 测试教师和学生设备注册。
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，您可以锁定并定位设备。

有关注册 ASM 并将您的帐户连接到 Citrix Endpoint Management 的信息，请参阅 通过 Apple 部署计划部署设备。

先决条件

- NetScaler 网关
- 为 MDM+MAM 配置的注册配置文件。
- Apple iPad 第三代（最低版本）或 iPad Mini，搭载 iOS 9.3（最低版本）

> **注意：**

> Citrix Endpoint Management 不会根据 LDAP 或 Active Directory 验证 ASM 用户帐户。但是，您可以将 Citrix Endpoint Management 连接到 LDAP 或 Active Directory，以管理与 ASM 教师或学生无关的用户和设备。例如，您可以使用 Active Directory 为其他 ASM 成员（如 IT 管理员和经理）提供 Citrix Secure Mail 和 Citrix Secure Web。

> 由于 ASM 教师和学生是本地用户，因此无需在其设备上部署 Citrix Secure Hub。

> 包含 NetScaler 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，Citrix Endpoint Management 仅将所需的批量购买应用程序和 iBooks 部署到教师和学生设备。

适用于 iPad 的课堂应用

适用于 iPad 的课堂应用使教师能够连接和管理学生设备。您可以查看设备屏幕、在 iPad 上打开应用、共享和打开网页链接，以及在 Apple TV 上展示学生屏幕。

课堂应用在 App Store 中免费提供。您将该应用上传到 Citrix Endpoint Management 控制台。然后，您使用教育配置设备策略来配置课堂应用，并将其部署到教师设备。

有关如何部署课堂应用的更多信息，请参阅分发 Apple 应用。

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 School Manager 用户添加密码

添加 ASM 帐户后，Citrix Endpoint Management 会从 ASM 导入班级和用户。Citrix Endpoint Management 将班级视为本地组，并在控制台中使用“组”一词。如果班级在 ASM 中具有组名，Citrix Endpoint Management 会将该组名分配给该班级。否则，Citrix Endpoint Management 会使用源系统 ID 作为组名。Citrix Endpoint Management 不会使用课程名称作为班级名称，因为 ASM 中的课程名称不是唯一的。

Citrix Endpoint Management 使用托管 Apple ID 创建用户类型为 **ASM** 的本地用户。这些用户是本地用户，因为 ASM 独立于所有外部数据源创建凭据。因此，Citrix Endpoint Management 不使用目录服务器来验证这些新用户。

ASM 不会将临时用户密码发送到 Citrix Endpoint Management。您可以从 CSV 文件导入它们，或手动添加。要导入临时用户密码：

1. 获取 ASM 在创建托管 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提供的用于注册到 Citrix Endpoint Management 的新密码。对此目的而言，密码类型没有限制。

   CSV 文件中条目的格式如下：
   `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`!

   其中：

   用户：`user@appleid.citrix.com`

   名字：`Firstname`

   中间名：`Middle`

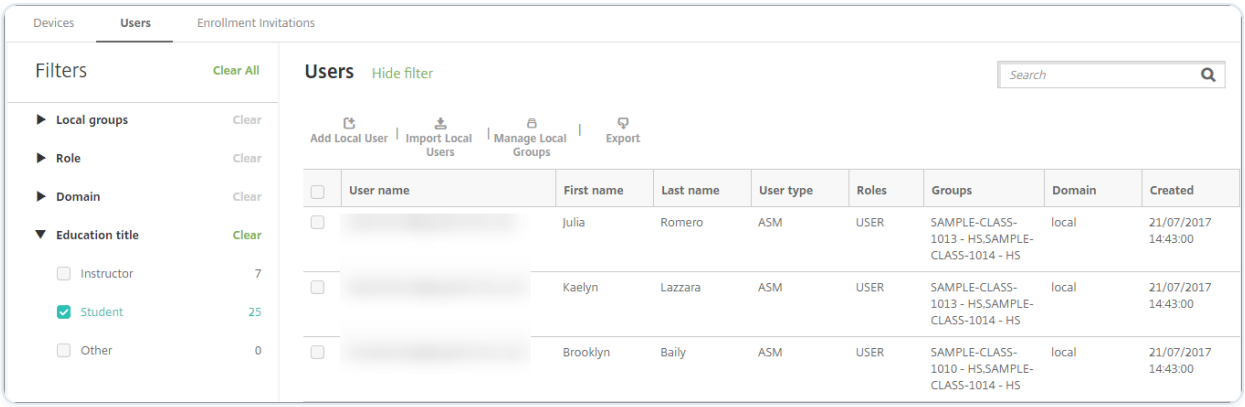
   姓氏：`Lastname`

密码：`Password123!`！

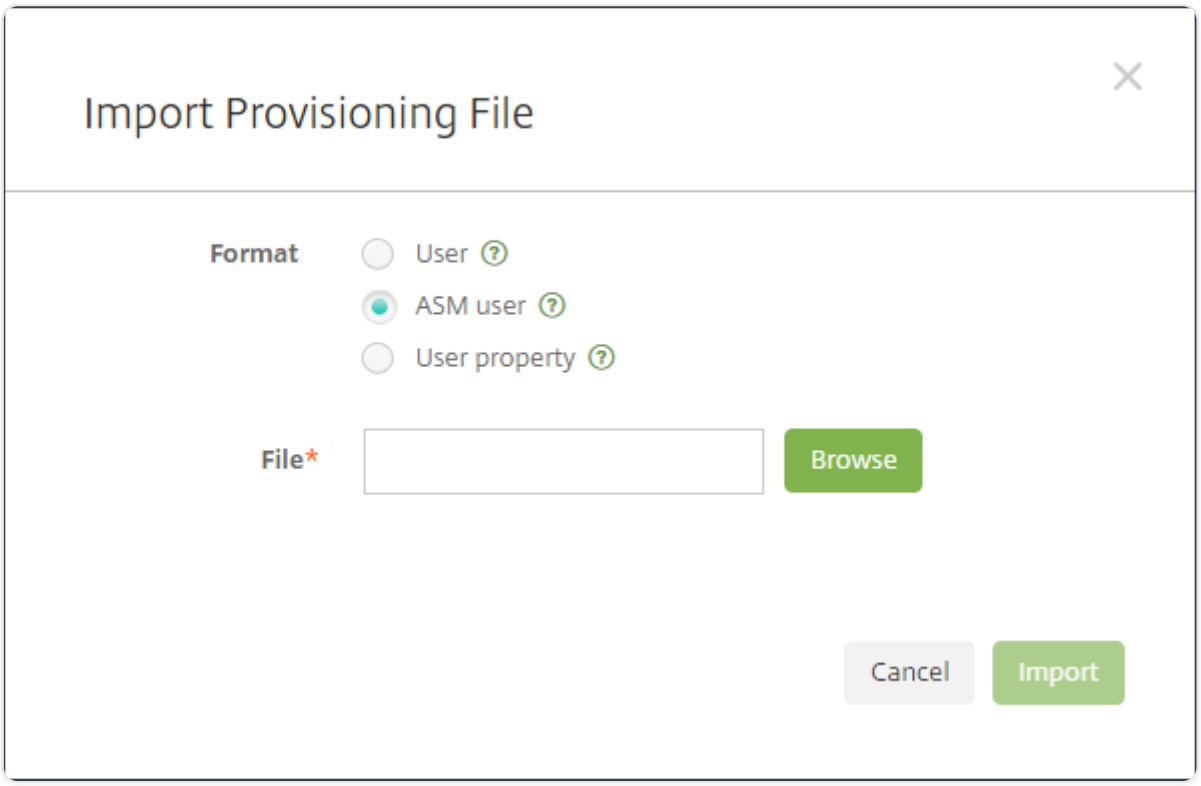
3. 在 Citrix Endpoint Management 控制台中，单击 **管理 > 用户**。此时将显示 **用户** 页面。

   以下 **管理 > 用户** 屏幕示例显示了从 ASM 导入的用户列表。在 **用户** 列表中：

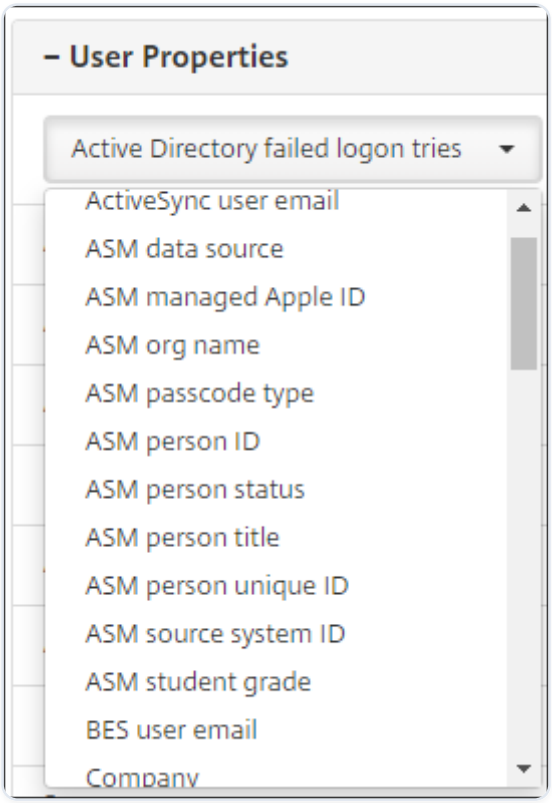
   - **用户名** 显示托管 Apple ID。
   - 用户类型为 **ASM**，表示帐户源自 ASM。
   - **组** 显示类别。



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”，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**”。



6. 要查看本地用户的属性，请选择该用户，然后单击“**编辑**”。



除了名称属性之外，还有以下 ASM 属性可用：

- **ASM 数据源：** 类的源数据，例如 **CSV** 或 **SFTP**。
- **ASM 托管式 Apple ID：** 托管式 Apple ID 可能包含您的机构名称和 `appleid`。例如，该 ID 可能类似于 johnappleseed@appleid.myschool.edu。Citrix Endpoint Management 需要托管式 Apple ID 进行身份验证。
- **ASM 组织名称：** 您在 Citrix Endpoint Management 中为帐户指定的名称。
- **ASM 密码类型：** 此人的密码策略：**复杂**（非学生密码，包含八个或更多数字和字母）、**四位**（数字）或**六位**（数字）。
- **ASM 个人唯一 ID：** 用户的标识符。
- **ASM 个人状态：** 指定托管式 Apple ID 是**活动**还是**非活动**。用户为其托管式 Apple ID 帐户提供新密码后，此状态将变为活动。
- **ASM 个人职称：** 教师、学生或其他。
- **ASM 个人唯一 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：** 学生年级信息（教师不使用）。

规划并将资源和交付组添加到 Citrix Endpoint Management

交付组指定要部署到用户类别的资源。例如，您可以为教师和学生创建一个交付组。或者，您可以创建多个交付组，以便自定义发送给不同教师或学生的应用程序、媒体和策略。您可以为每个班级创建一个或多个交付组。您还可以为管理员（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，则需要教育配置设备策略。请务必查看其他设备策略，以确定如何配置和限制教师和学生的 iPad。

- 批量购买应用程序：

  Citrix 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。Citrix Endpoint Management 不支持将此类批量购买应用程序部署为可选应用程序。

  如果您使用 Apple 课堂应用，请仅将其部署到教师设备。

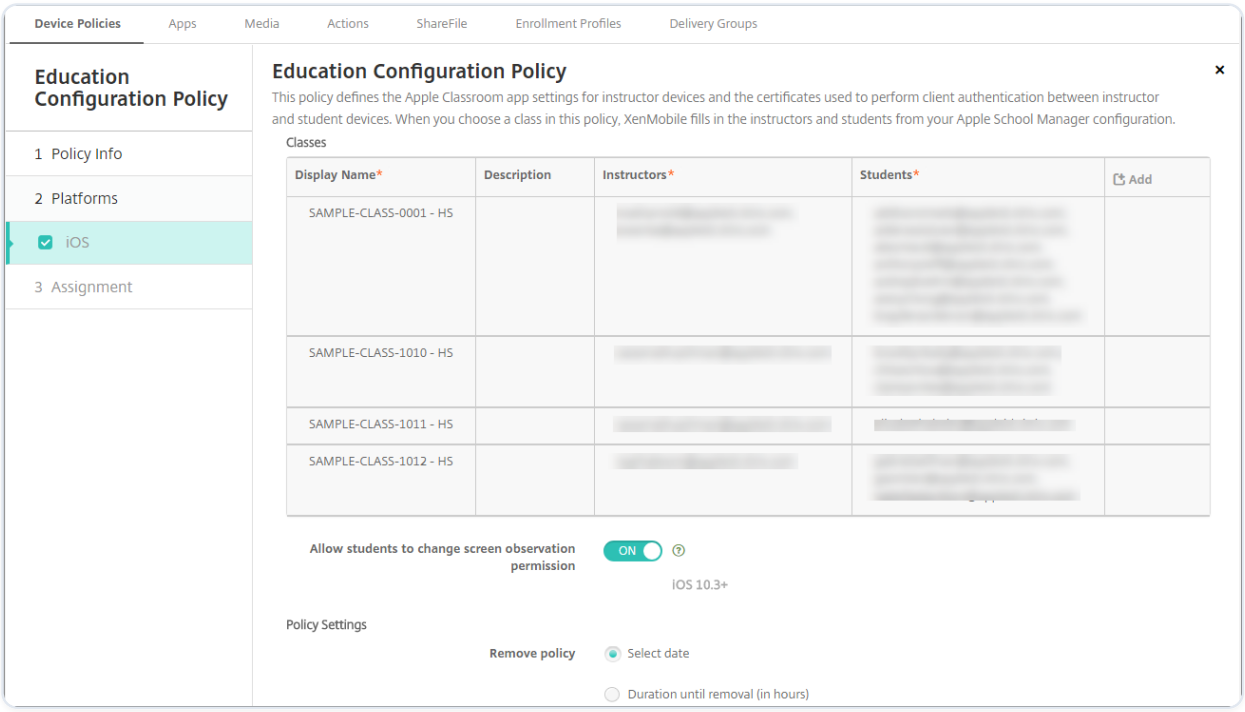
  部署您希望提供给教师或学生的任何其他应用程序。此解决方案不使用 Citrix Secure Hub 应用程序，因此无需将其部署给教师或学生。

- 批量购买 iBooks：

  Citrix Endpoint Management 连接到您的 ASM 帐户后，您购买的 iBooks 将显示在 Citrix Endpoint Management 控制台的“**配置 > 媒体**”中。该页面上列出的 iBooks 可用于添加到交付组。Citrix Endpoint Management 仅支持将 iBooks 添加为必需媒体。

规划好教师和学生的资源和交付组后，您可以在 Citrix Endpoint Management 控制台中创建这些项目。

1. 创建您希望部署到教师或学生设备的任何设备策略。有关教育配置设备策略的信息，请参阅教育配置设备策略。

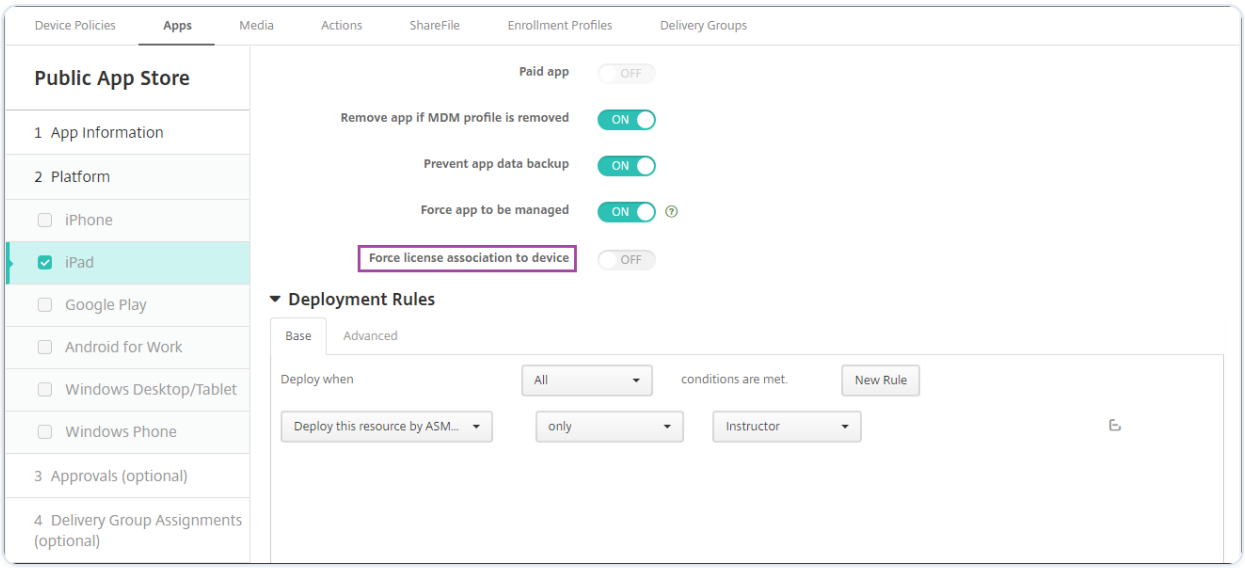


有关设备策略的信息，请参阅设备策略和各个策略文章。

2. 配置应用程序（**配置 > 应用程序**）和 iBooks（**配置 > 媒体**）：

   - 默认情况下，Citrix Endpoint Management 在用户级别分配应用程序和 iBooks。首次部署期间，教师和学生会收到注册到 ASM 的提示。接受邀请后，用户将在下次部署（六小时内）收到其 ASM 应用程序和 iBooks。Citrix 建议您强制将应用程序和 iBooks 部署到新的 ASM 用户。为此，请选择交付组，然后单击**部署**。

     您可以选择在设备级别分配应用程序（但不能分配 iBooks）。为此，请将设置**强制许可证关联到设备**更改为**开**。当您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。

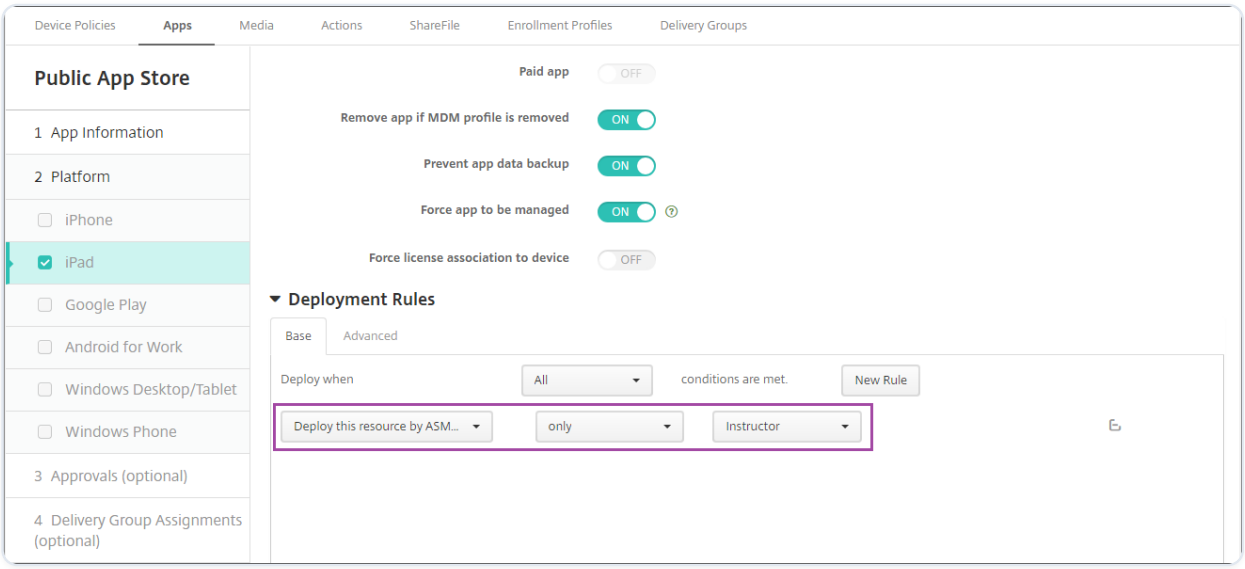


   - 要仅向教师部署应用程序，请选择仅包含教师的交付组或使用以下部署规则：

```
Deploy this resource by ASM device type

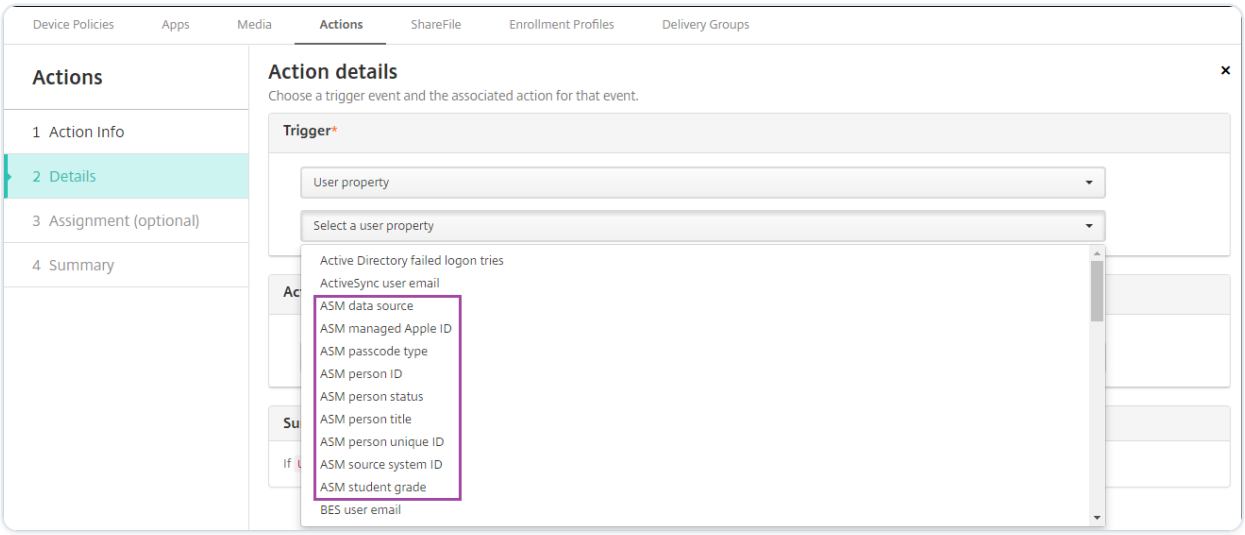
only

Instructor
```



- 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，您可以创建一个操作，以便在新应用程序安装时向学生设备发送通知。或者，您可以创建一个由用户属性触发的操作，如以下示例所示。



要创建操作，请转到**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 导入的班级。此外，为教师和学生创建部署规则。

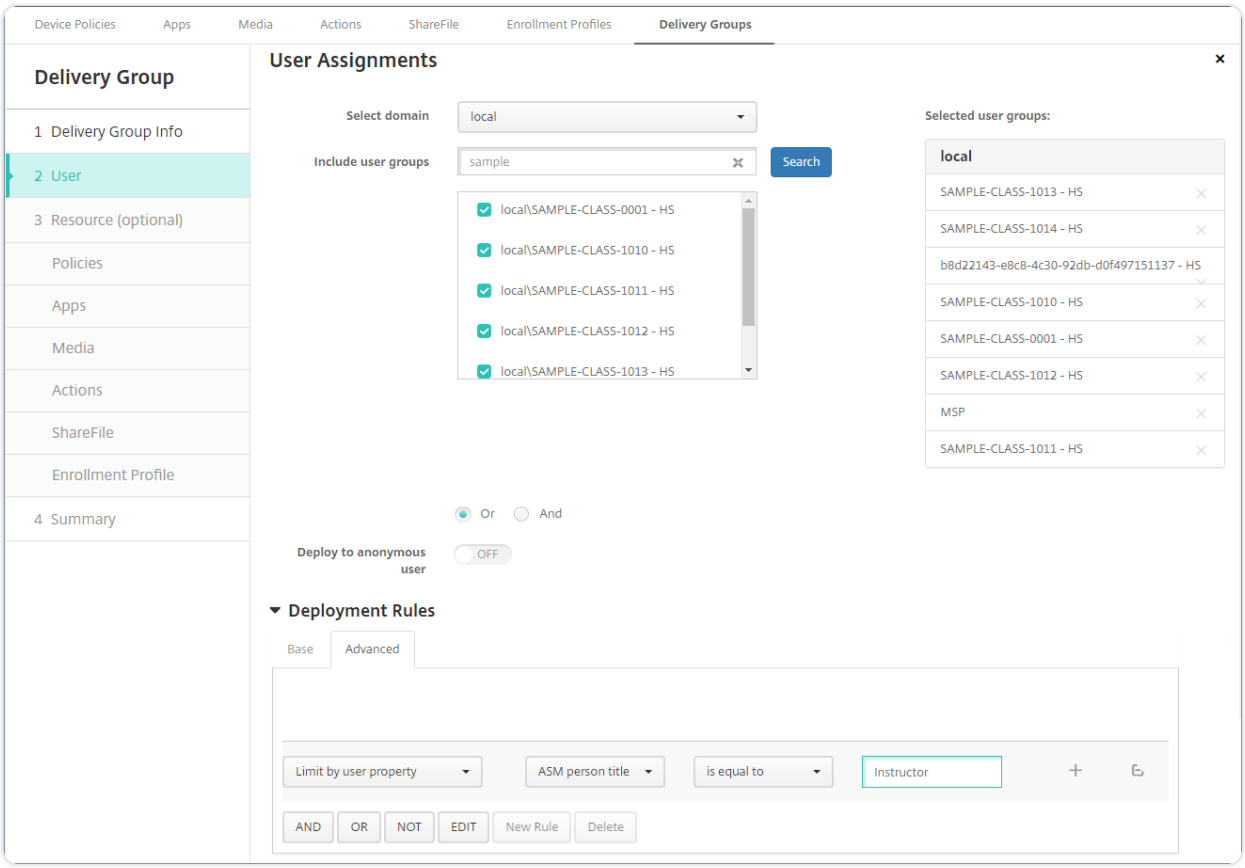
   例如，以下用户分配适用于教师。部署规则为：

```
Limit by user property

ASM person title

is equal to

Instructor
```



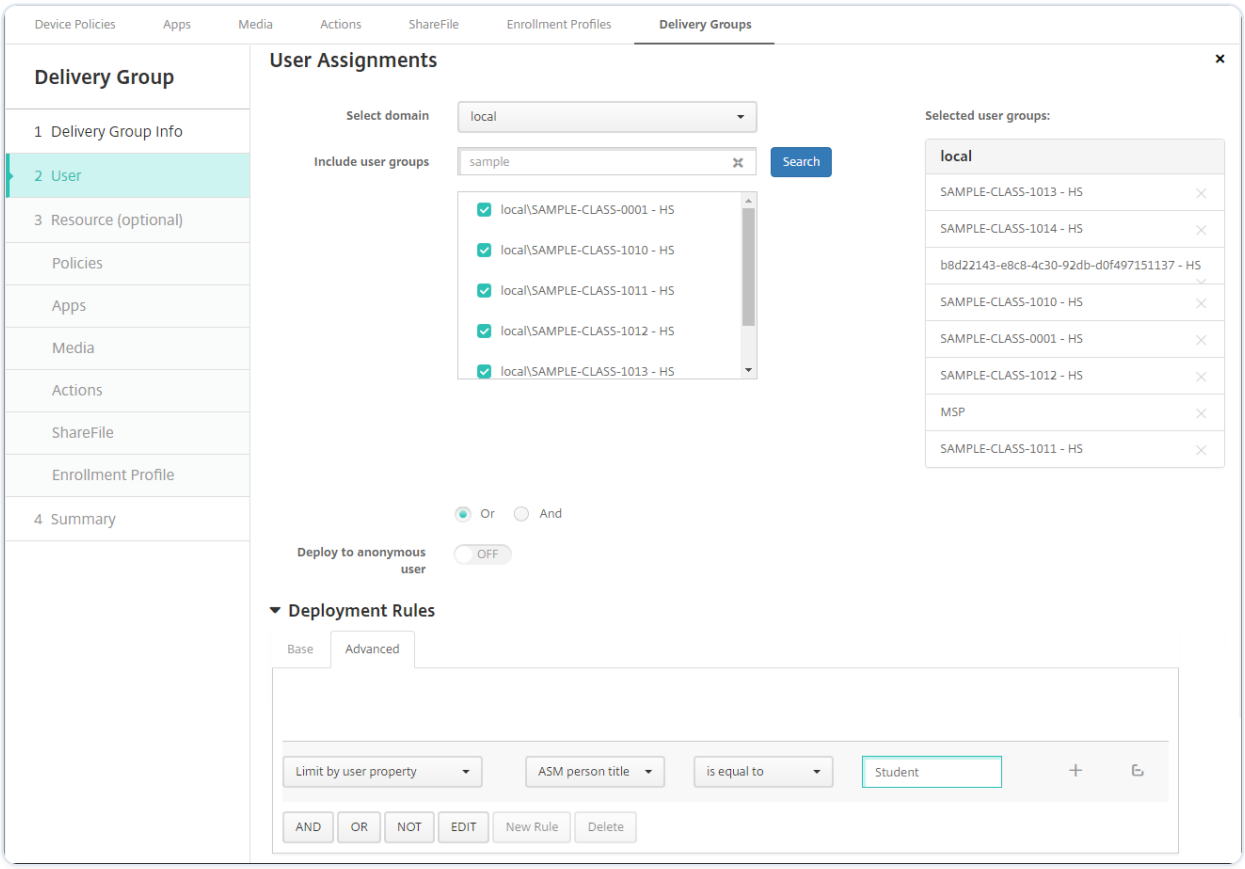
以下用户分配适用于学生。部署规则为：

```
Limit by user property

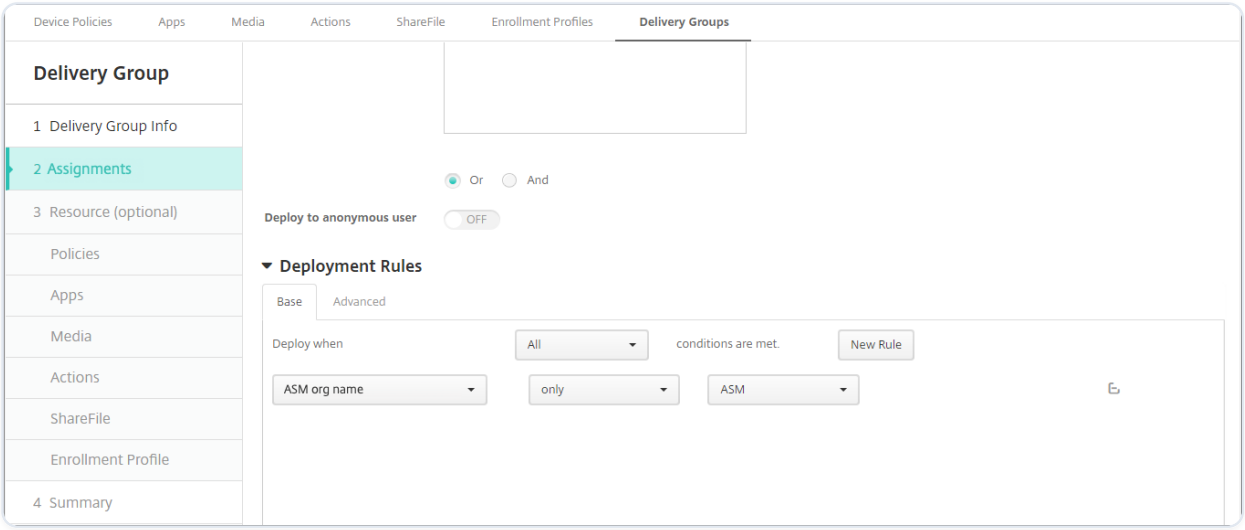
ASM person title

is equal to

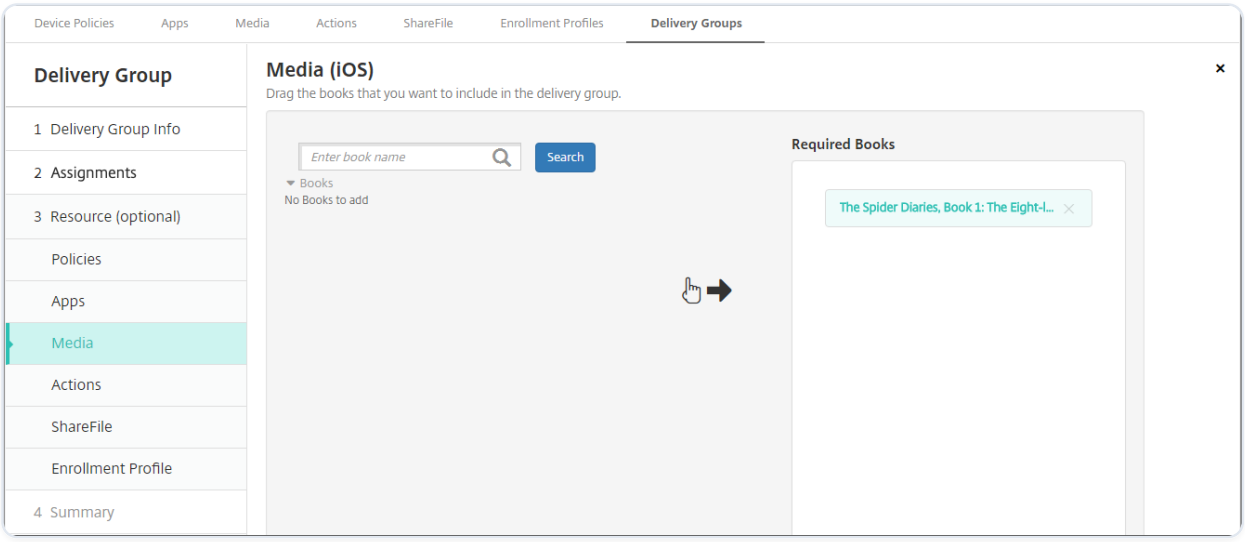
Student
```



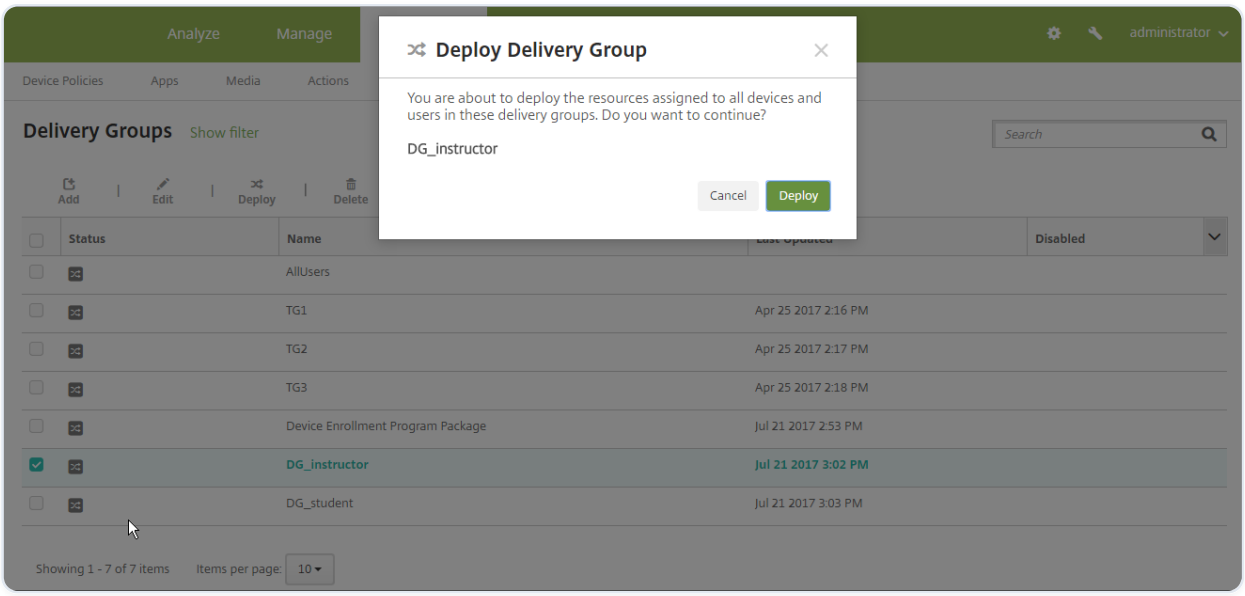
您还可以使用基于 ASM 组织名称的部署规则来筛选交付组。



5. 将资源分配给交付组。以下示例显示了交付组中的 iBook。



以下示例显示了选择交付组并单击**部署**时出现的确认对话框。



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

您可以通过以下任一方法注册设备：

- 学校管理员可以使用您在 Citrix Endpoint Management 控制台中设置的用户密码来注册教师和学生设备。因此，您可以为用户提供已设置好应用程序和媒体的设备。
- 当用户收到设备时，他们会使用您提供给他们的用户密码进行注册。注册完成后，Citrix Endpoint Management 会将设备策略、应用程序和媒体发送到设备。

要测试注册，请使用链接到 ASM 的 Apple Deployment Program 设备。

1. 如果设备未链接到 ASM，请通过硬重置擦除设备内容和设置。
2. 为教师注册一个 ASM 设备。然后，为学生注册一个 ASM 设备。

3. 在**管理 > 设备**页面中，检查两个 ASM 设备是否都仅注册到 MDM。

   您可以根据 ASM 设备状态筛选**设备**页面：**ASM 已注册**、**ASM 已共享**、**教师**和**学生**。

   设备配置屏幕(/en-us/citrix-endpoint-management/media/manage-devices-asm-filtered.png)

4. 要验证 MDM 资源是否已为每个设备正确部署：选择设备，单击**编辑**，然后检查各个页面。

   设备配置屏幕(/en-us/citrix-endpoint-management/media/manage-devices-asm-details.png)

分发设备

Apple 建议您举办活动，以便将设备分发给教师和学生。

如果您不分发预注册设备，还需向这些用户提供以下信息：

- 用于注册的 Citrix Endpoint Management 密码
- 用于托管式 Apple ID 的 ASM 临时密码。

首次用户体验如下。

1. 用户在硬重置后首次启动设备时，Citrix Endpoint Management 会在注册屏幕中提示他们注册设备。
2. 用户提供其托管式 Apple ID 和用于向 Citrix Endpoint Management 进行身份验证的 Citrix Endpoint Management 密码。
3. 在 Apple ID 设置步骤中，设备会提示用户提供其托管式 Apple ID 和 ASM 临时密码。这些项目用于向 Apple 服务验证用户身份。
4. 设备会提示用户为其托管式 Apple ID 创建密码，该密码用于保护其在 iCloud 中的数据。
5. 在设置助理结束时，Citrix Endpoint Management 开始将策略、应用程序和媒体安装到设备。对于在用户级别分配的应用程序和 iBooks，助理会提示教师和学生注册批量采购。接受邀请后，用户将在下次部署（六小时内）时收到其批量采购应用程序和 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：

- 在将 ASM 信息导入 Citrix Endpoint Management 后，请勿更改托管式 Apple ID。Citrix Endpoint Management 也使用 ASM 用户标识符来识别用户。
- 如果在创建了一个或多个教育配置设备策略后，您在 ASM 中添加或更改了班级数据：请编辑这些策略，然后重新部署它们。

- If the instructor for a class changes after you deploy the Education Configuration device policy: Review the policy to make sure it updates in the Citrix Endpoint Management console and then redeploy the policy.
- If you update user properties in the ASM portal, Citrix Endpoint Management also updates those properties in the console. However, Citrix Endpoint Management doesn't receive the ASM person title property (Instructor, Student, or Other) in the same way it receives other properties. Thus, if you change the ASM person title in the ASM, complete the following steps to reflect that change in Citrix Endpoint Management.

要管理数据：

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，请从班级学生列表中删除该用户。然后，将该用户添加到相同或另一个班级的教师列表中。

   如果您将教师帐户更改为学生帐户，请从班级中删除该用户。然后，将该用户添加到相同或另一个班级的学生列表中。您的更新将在下次同步（默认为每五分钟一次）或获取（默认为每 24 小时一次）期间显示在 Citrix Endpoint Management 控制台中。
3. 编辑 Education Configuration 设备策略以应用更改并重新部署它。

   - 如果您从 ASM 门户中删除用户，Citrix Endpoint Management 也会在获取后从 Citrix Endpoint Management 控制台中删除该用户。

     您可以通过更改此服务器属性值来缩短两个基线之间的时间间隔：**bulk.enrollment.fetchRosterInfoDelay**（默认为 **1440** 分钟）。
   - 部署资源后：如果学生加入班级，请仅包含该学生创建一个交付组，并将资源部署给该学生。
   - If a student or instructor loses their temporary password, have them contact the ASM administrator. The administrator can provide the temporary password or generate a new one.

管理丢失或被盗的设备

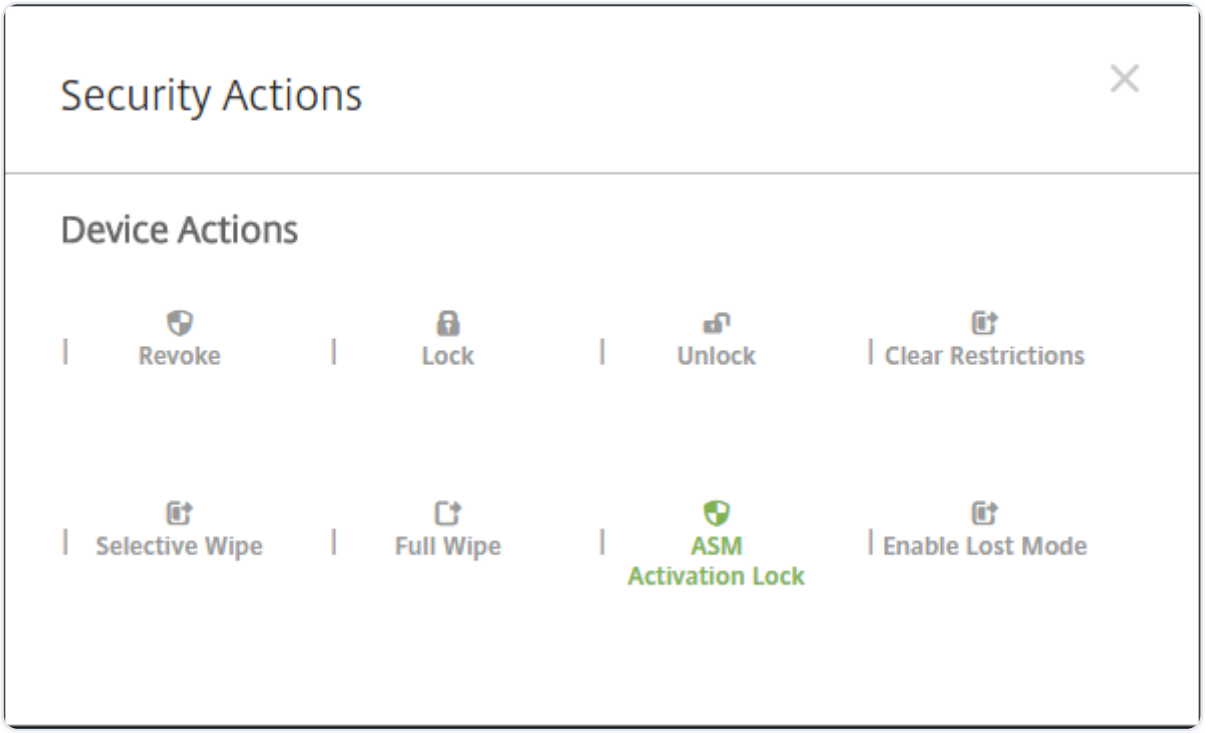
Apple 查找我的 iPhone/iPad 服务包含激活锁功能。激活锁可防止未经授权的用户使用或转售已注册 Apple 部署计划的丢失或被盗设备。

Citrix Endpoint Management 包含一个**ASM 激活锁**安全操作，可让您向已注册 ASM Apple 部署计划的设备发送锁定代码。

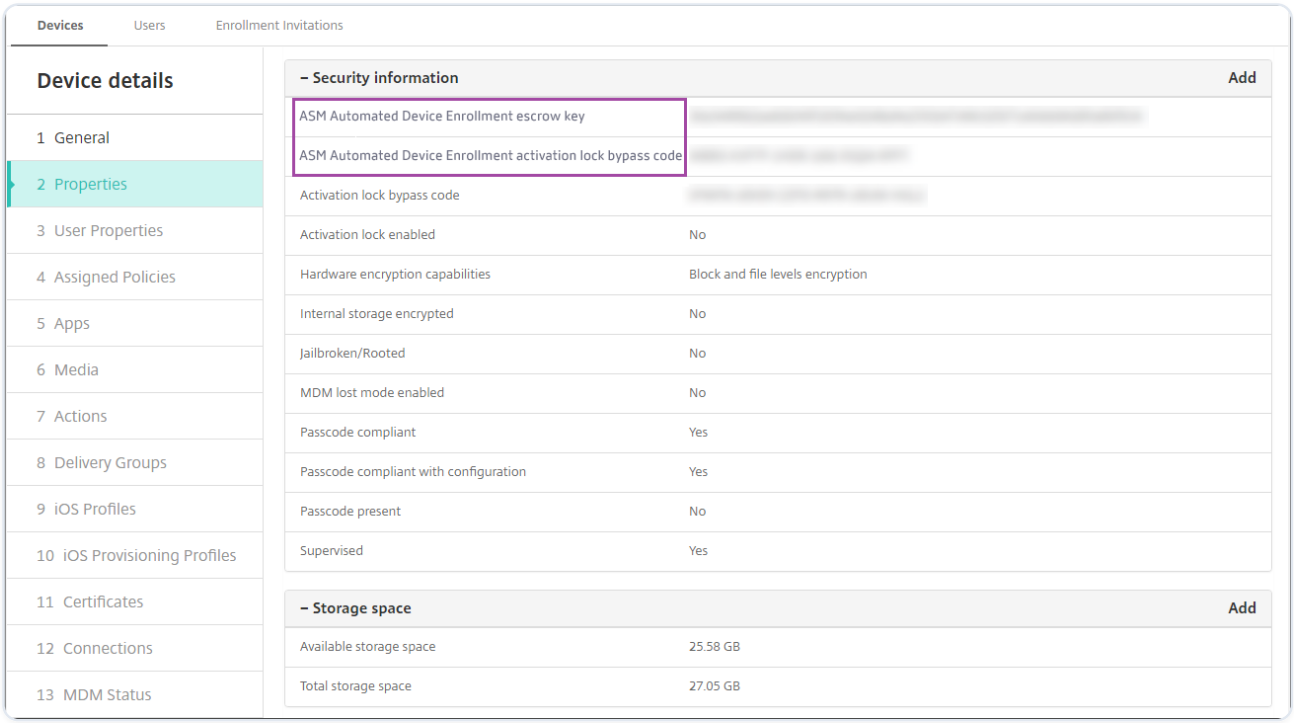
当您使用**ASM 激活锁**安全操作时，Citrix Endpoint Management 可以定位设备，而无需用户启用“查找我的 iPhone/iPad”服务。当 ASM 设备被硬重置或完全擦除时，用户需提供其托管式 Apple ID 和密码才能解锁设备。

要从控制台释放锁定，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。用户还可以将登录名留空，然后键入**ASM 激活锁绕过代码**作为密码。该信息可在**设备详细信息**的**属性**选项卡中找到。

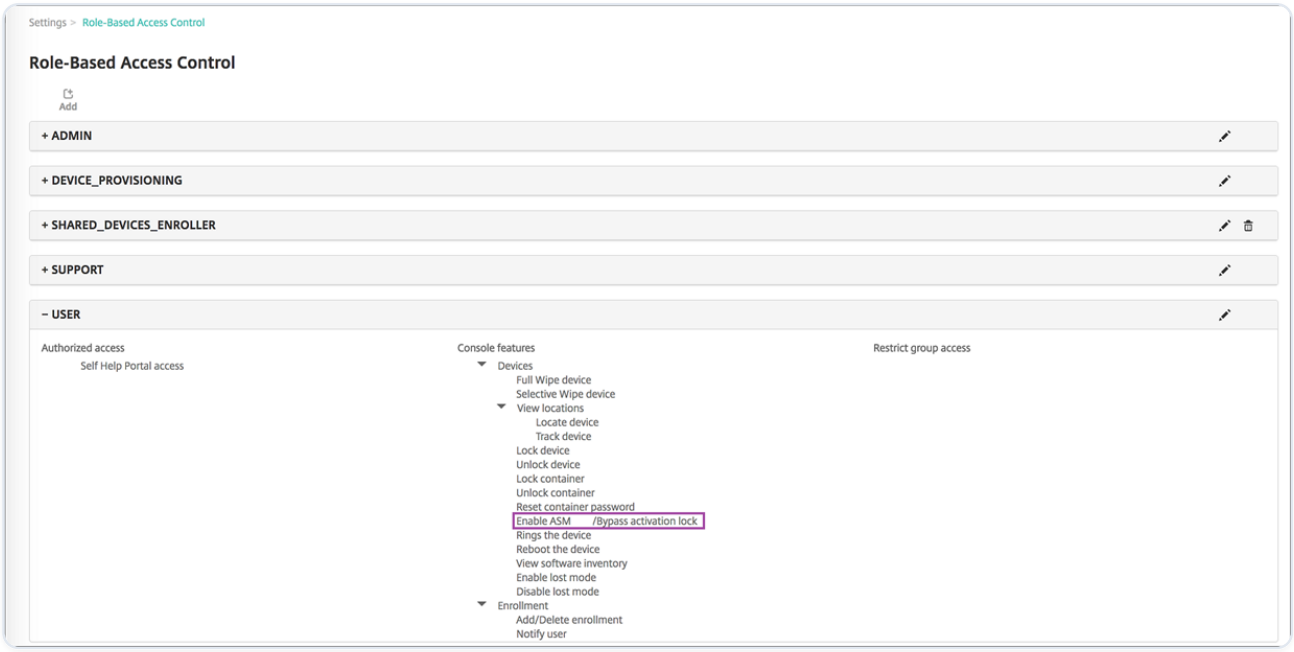
要设置激活锁，请转至**管理 > 设备**，选择设备，单击**安全性**，然后单击**ASM 激活锁**。



属性**ASM 托管密钥**和**ASM 激活锁绕过代码**显示在**设备详细信息**中。



ASM 激活锁的 RBAC 权限为**设备 > 启用 ASM 绕过激活锁**。



共享 iPad

共享 iPad 功能允许多个用户使用一台 iPad。即使设备是共享的，用户体验也可以个性化。您可以将共享 iPad 用于教育或商业用途。Apple School Manager (ASM) 除了支持 Apple Business Manager (ABM) 支持的角色外，还支持教师和学生角色。

共享 iPad 的先决条件

- Apple 校园教务管理 或 Apple 商务管理
- Citrix 端点管理

- 任何 iPad Pro、第五代 iPad、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
- 受监督的设备

配置共享 iPad

多个学生或员工可以出于不同目的共享一台 iPad。

您或设备所有者注册共享 iPad，然后将设备策略、应用程序和媒体部署到设备。之后，用户提供其受管理的 Apple ID 凭据以登录共享 iPad。如果您之前已向学生部署了教育配置策略，他们将不再以“其他用户”身份登录以共享设备。

Citrix Endpoint Management 为共享 iPad 使用两个通信通道：用于设备所有者（教师或主管）的系统通道和用于当前常驻用户（学生或员工）的用户通道。Citrix Endpoint Management 使用这些通道发送 Apple 支持的资源的相应 MDM 命令。

通过系统通道部署的资源包括：

- 设备策略，例如 教育配置、锁屏消息、最大常驻用户 和 密码锁定宽限期
- 基于设备的批量采购应用 Apple 不支持在共享 iPad 上使用企业应用或基于用户的批量采购应用。安装在共享 iPad 上的应用是设备全局的，而非按用户分配。
- 基于用户的批量采购 iBooks Apple 支持在共享 iPad 上分配基于用户的批量采购 iBooks。

通过用户通道部署的资源包括：

- 设备策略：应用程序通知、主屏幕布局、限制和 Webclip。

  Citrix 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，您可以在策略设置“**配置文件范围**”中指定部署通道。

设备策略配置屏幕(/en-us/citrix-endpoint-management/media/device-policy-shared-ipad-profile-scope.png)

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**”。

一般工作流程

通常，您会向设备所有者提供预配置和受监督的共享 iPad。这些人随后会将设备分发给学生或员工。如果您不分发预注册的共享 iPad：请务必向设备所有者提供其 Citrix Endpoint Management 服务器密码，以便他们可以注册其设备。

配置和注册共享 iPad 的一般工作流程如下。

1. 使用 Citrix Endpoint Management 服务器控制台添加 ASM 或 ABM 帐户（**设置 > Apple 部署计划**），并启用“**共享模式**”。有关详细信息，请参阅下一节“管理共享 iPad 的帐户”。
2. 如本节所述，将所需的设备策略、应用程序和媒体添加到 Citrix Endpoint Management。将这些资源分配给交付组。
3. 让设备所有者对共享 iPad 执行硬重置。此时将显示用于注册的远程管理屏幕。
4. 设备所有者注册共享 iPad。 Citrix Endpoint Management 会将配置的资源部署到每个已注册的共享 iPad。自动重新启动后，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. 设备用户输入其托管 Apple ID 和临时 ASM 密码。 共享 iPad 向 ASM 进行身份验证，并提示用户创建 ASM 密码。下次登录共享 iPad 时，设备用户将提供新的 ASM 密码。
6. 共享 iPad 的其他设备用户可以通过重复上一步来登录。

管理共享 iPad 的帐户

如果您已将 Citrix Endpoint Management 与 Apple Education 或 Apple Business 结合使用：您在 Citrix Endpoint Management 中已配置了一个现有的 ASM/ABM 帐户，用于非共享设备，例如设备所有者使用的设备。您可以将相同的 ASM/ABM 帐户和相同的 Citrix Endpoint Management 服务器用于共享设备和非共享设备。

将共享 iPad 组织到设备组中

ASM/ABM 允许您通过创建多个 MDM 服务器将设备组织成组。当您将共享 iPad 分配给 MDM 服务器时，为每组共享 iPad 创建一个设备组：

- 共享 iPad 组 1 > 设备组 1 MDM 服务器
- 共享 iPad 组 2 > 设备组 2 MDM 服务器
- 共享 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 Citrix Endpoint Management 服务器控制台创建多个 ASM/ABM 帐户时，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

共享 iPad 的特定要求如下：

- 每个设备组一个 ASM/ABM 帐户，并启用以下设置：
    - **要求设备注册**

  - **监管模式**
  - **共享模式**

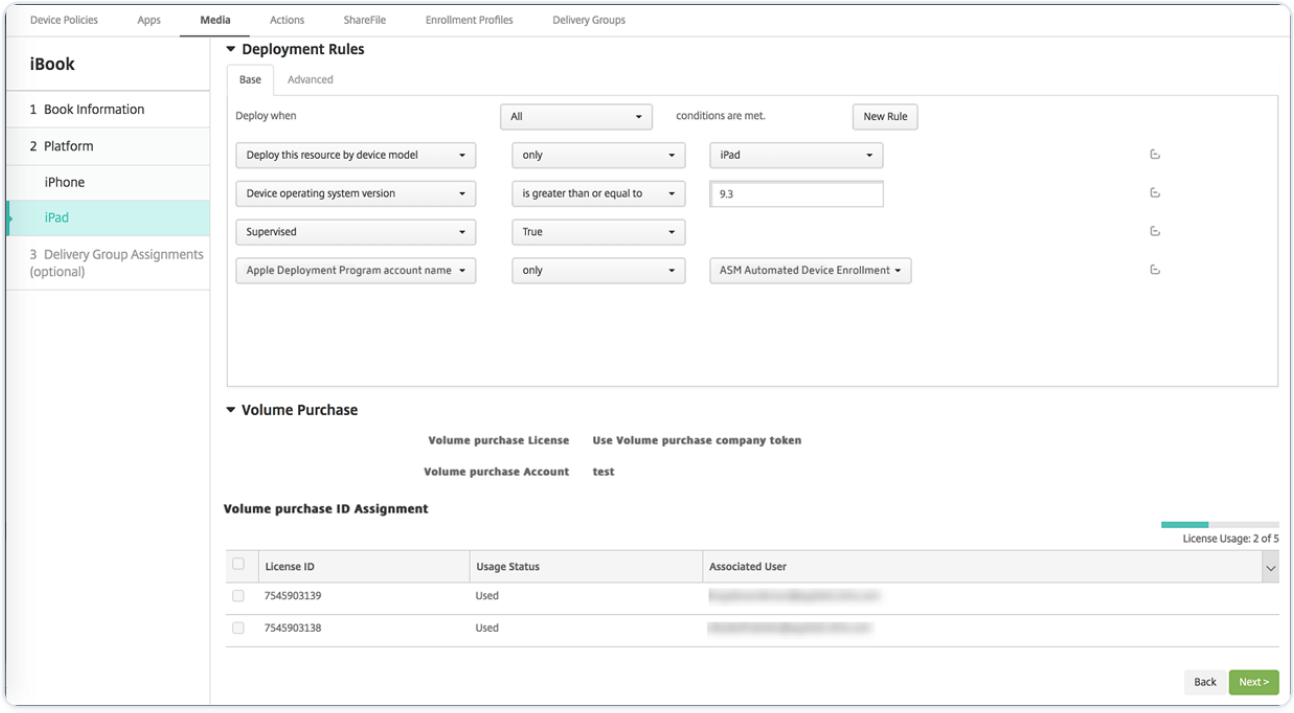
- 对于给定的教育机构，请确保所有 ASM 帐户都使用相同的 **教育后缀**。

共享 iPad 的应用程序

共享 iPad 支持分配基于设备的批量采购应用程序。在共享 iPad 上部署应用程序之前，Citrix Endpoint Management 会向 Apple 批量采购服务器发送请求，以将批量采购许可证分配给设备。要检查批量采购分配，请转到 **配置 > 应用程序 > iPad** 并展开 **批量采购**。

共享 iPad 的媒体

共享 iPad 支持分配基于用户的批量采购 iBooks。在共享 iPad 上部署 iBooks 之前，Citrix Endpoint Management 会向 Apple 批量采购服务器发送请求，以将批量采购许可证分配给用户。要检查批量采购分配，请转到 **配置 > 媒体 > iPad** 并展开 **批量采购**。



共享 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。要筛选每个设备组的策略、应用程序和媒体：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，设置此部署规则：

```
Apple Deployment Program account name
```

```
Only

Device Group 1 account
```

- 对于设备组 2 帐户，设置此部署规则：

```
Apple Deployment Program account name

Only

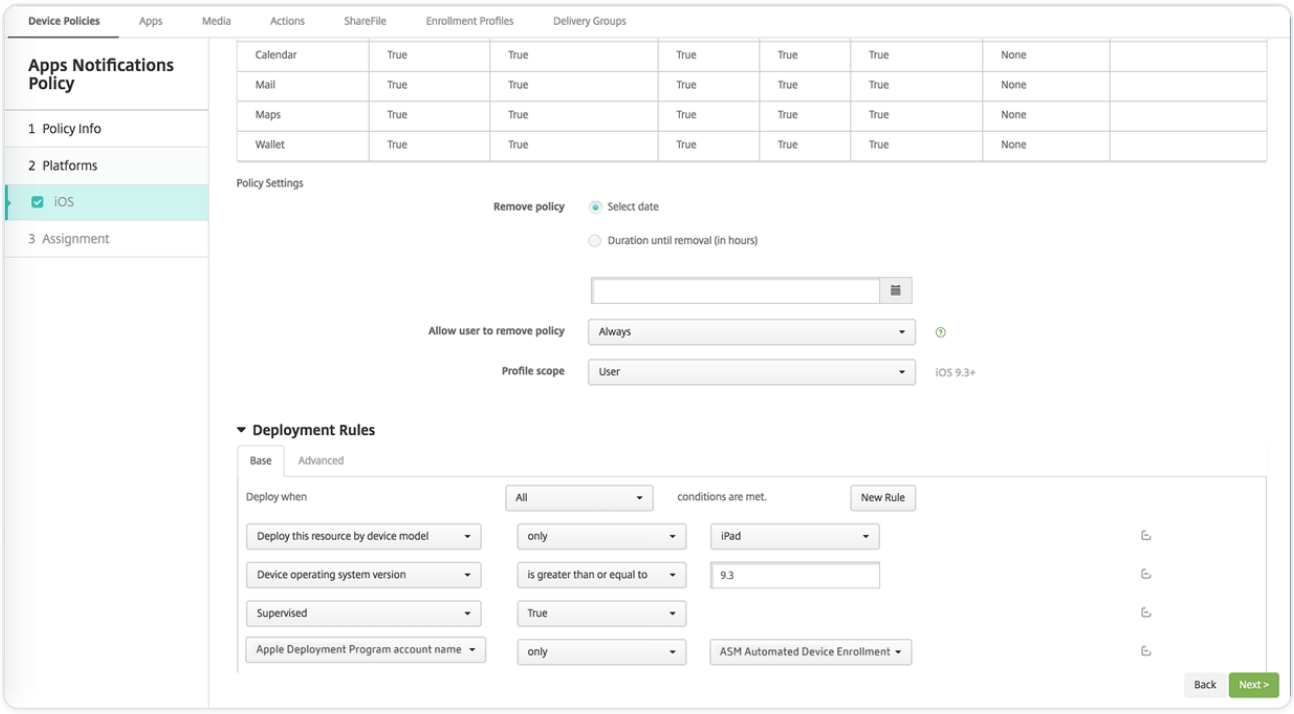
Device Group 2 account
```

- 对于设备组 N 帐户，设置此部署规则：

```
Apple Deployment Program account name

Only

Device Group N account
```



要仅将 Apple Classroom 应用程序部署到设备所有者（使用非共享 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
```

或者：

```
Deploy this resource regarding ASM/ABM shared mode

except

shareable
```

应用程序配置屏幕(/en-us/citrix-endpoint-management/media/configure-apps-deployment-rule-shareable.png)

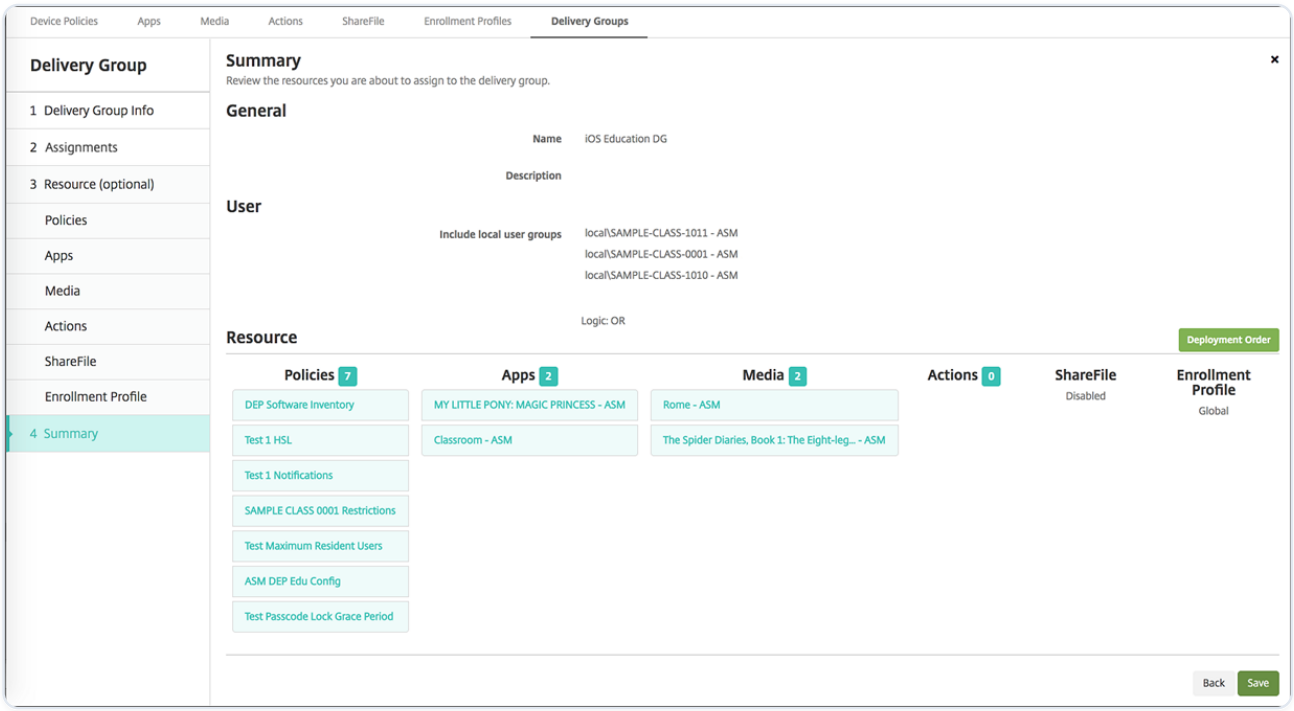
共享 iPad 的交付组

对于设备组：

- 配置一个交付组。对于教师，分配教育配置策略定义的所有课程。

交付组配置屏幕(/en-us/citrix-endpoint-management/media/configure-delivery-group-user-assignment.png)

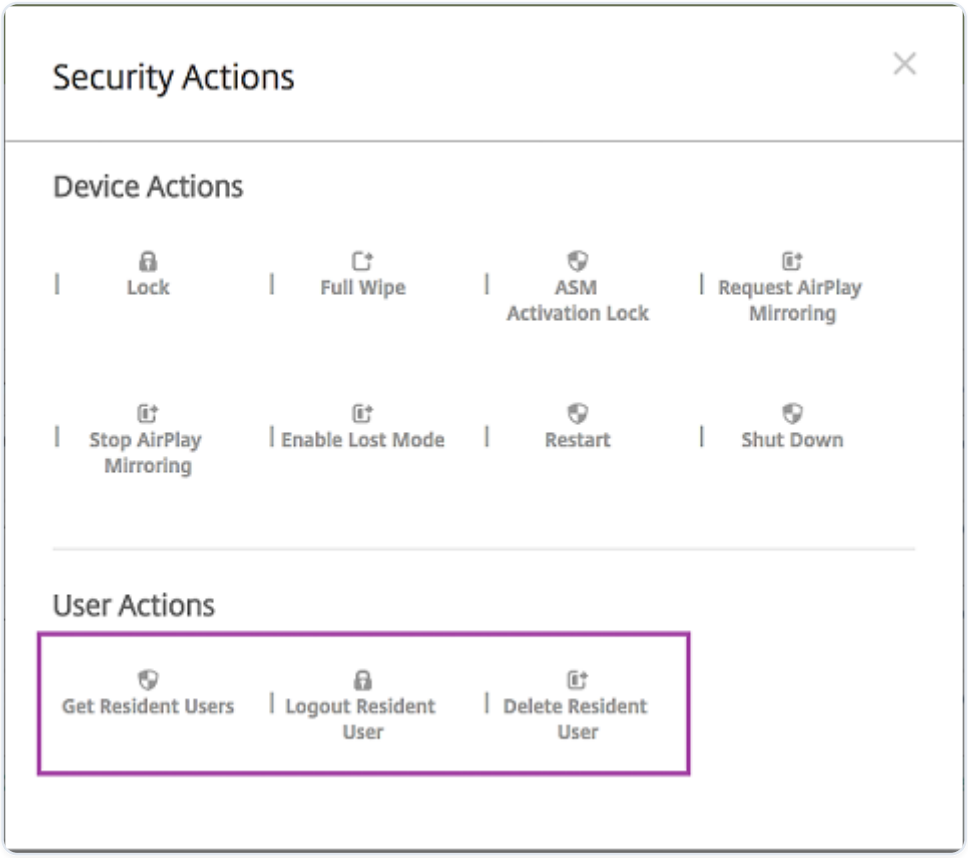
- 该交付组必须包含以下 MDM 资源：
  - 设备策略：
    - 教育配置（适用于 ASM）
    - 锁屏消息
    - 应用程序通知
    - 主屏幕布局
    - 限制
    - 最大驻留用户数
    - 密码锁定宽限期
  - 所需批量购买应用程序
  - 所需批量购买 iBooks



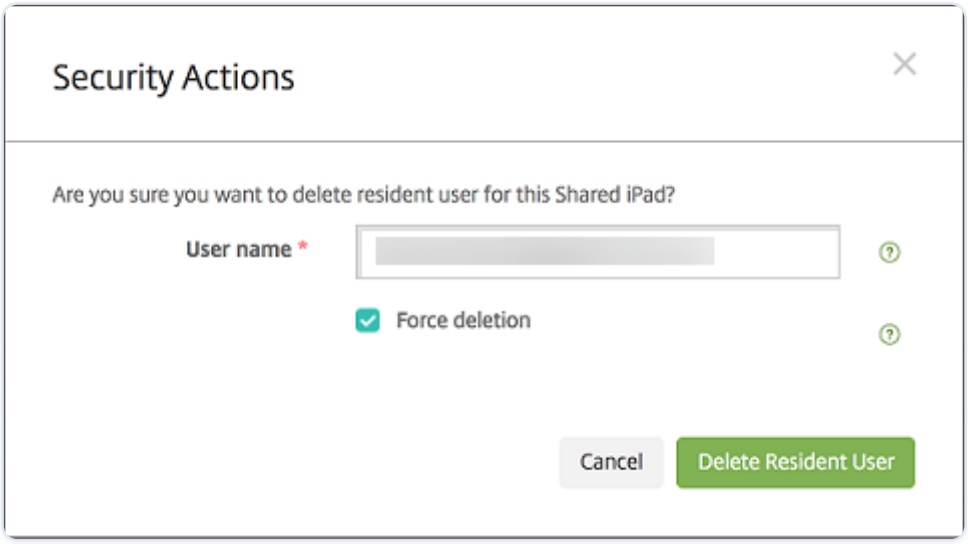
共享 iPad 的安全操作

除了现有安全操作之外，您还可以对共享 iPad 使用以下安全操作：

- **获取常驻用户：** 列出当前设备上具有活动帐户的用户。此操作强制设备与 Citrix 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。用户可以再次登录。
- **删除所有用户：** 删除设备上的所有用户。



单击**删除常驻用户**后，您可以指定用户名。

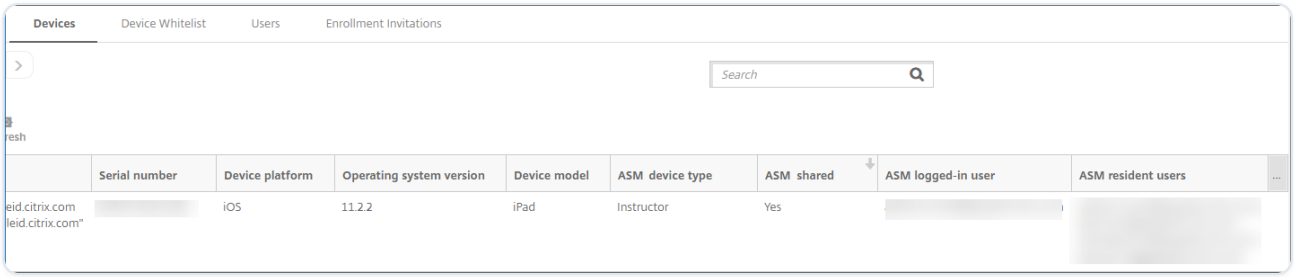


安全操作的结果显示在**管理 > 设备 > 常规**和**管理 > 设备 > 交付组**页面上。

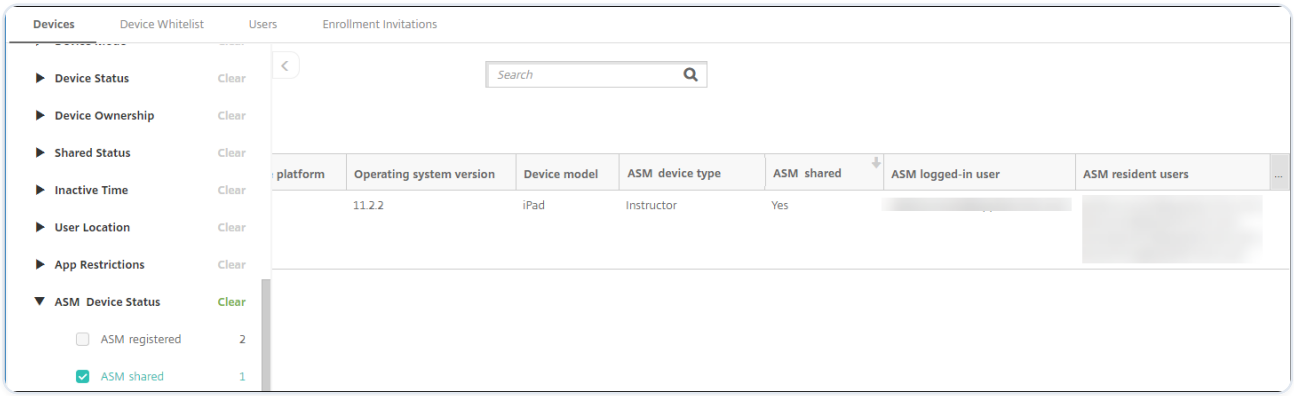
获取有关共享 iPad 的信息

在**管理 > 设备**页面上查找共享 iPad 的特定信息：

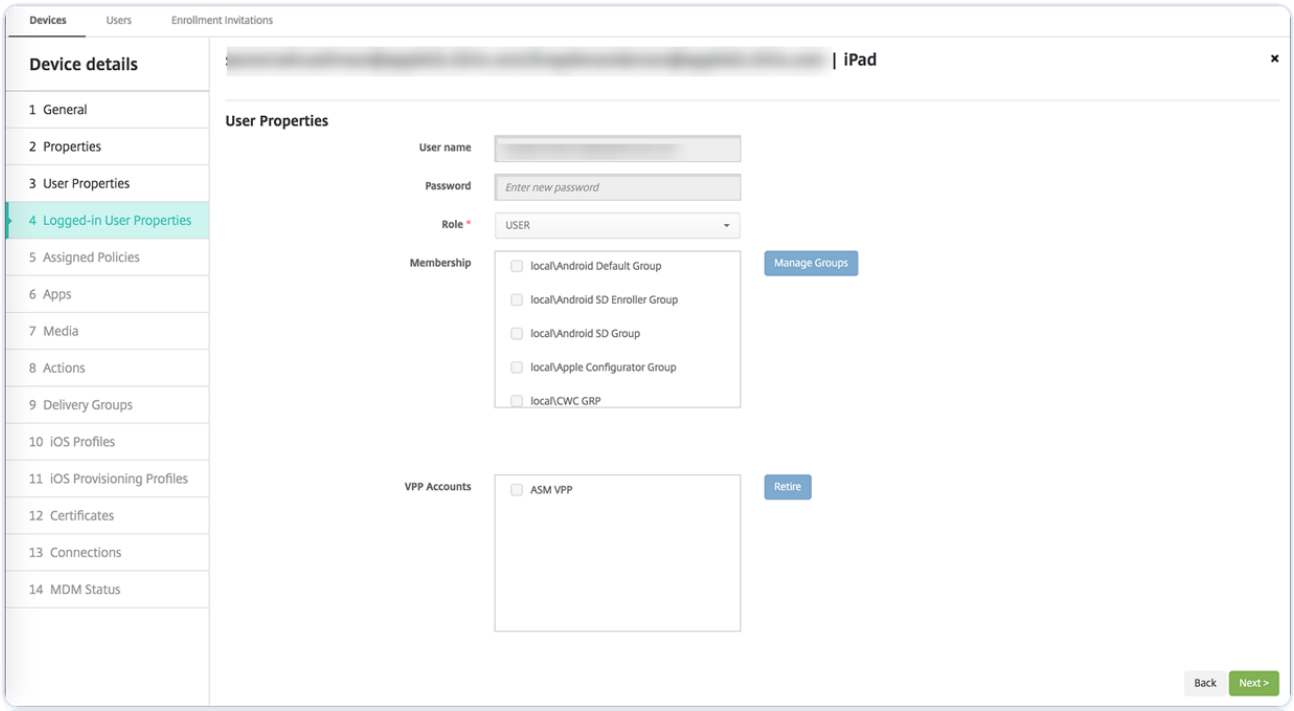
- 查找：
  - 设备是否共享 (**ASM/ABM 共享**)
  - 谁登录了共享设备 (**ASM/ABM 登录用户**)
  - 分配给共享设备的所有用户 (**ASM/ABM 常驻用户**)

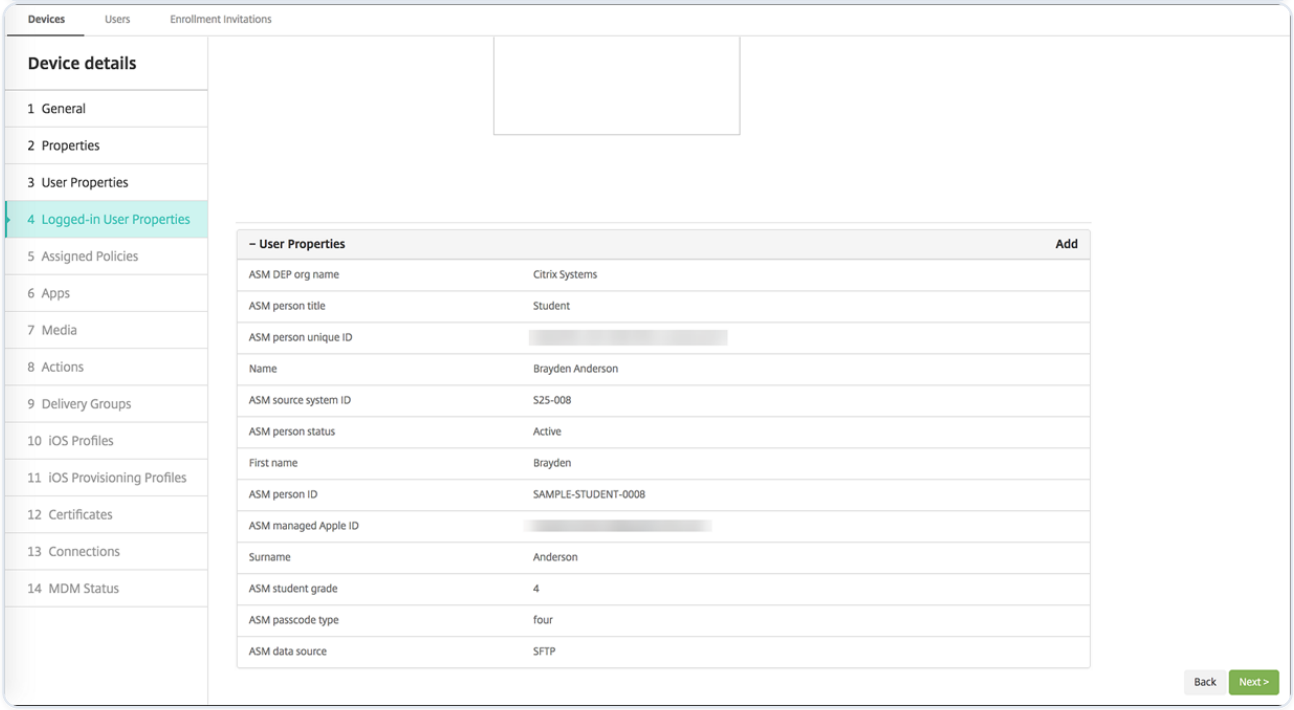


- 按设备的**ASM/ABM 设备状态**筛选设备列表：

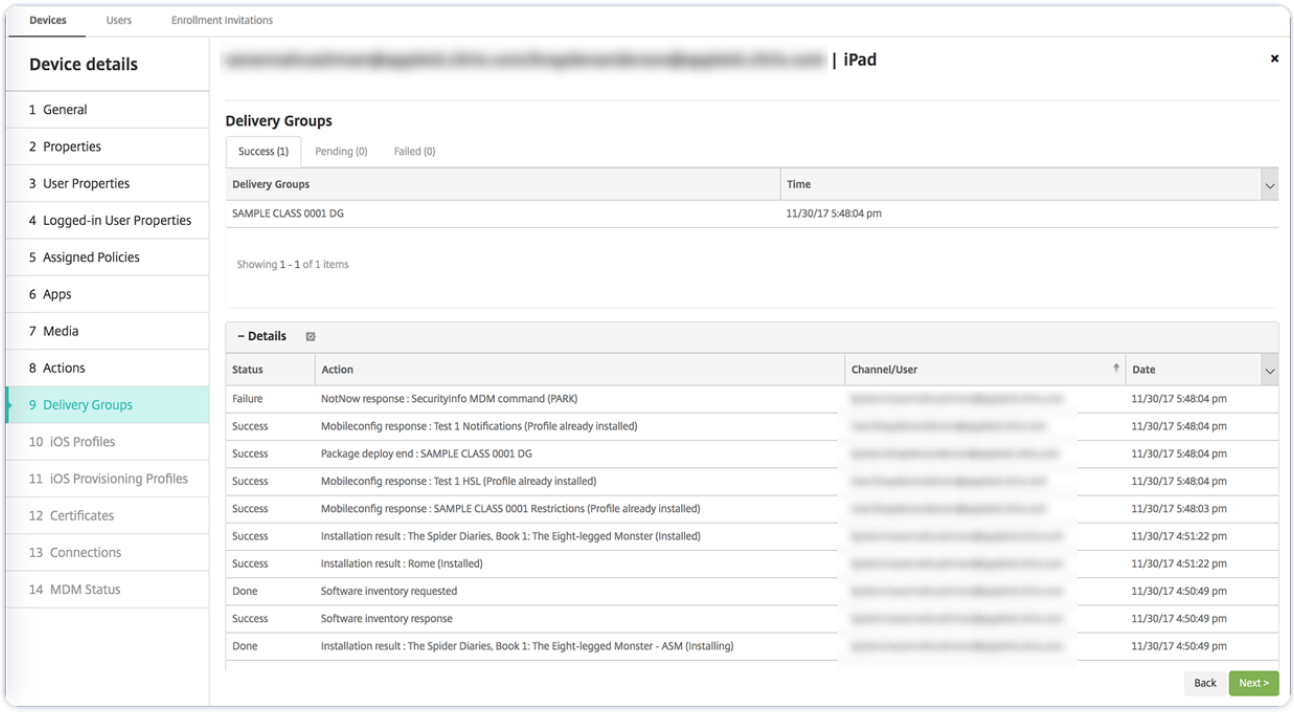


- 在**管理 > 设备 > 登录用户属性**页面上，查看登录到共享 iPad 的用户的详细信息。

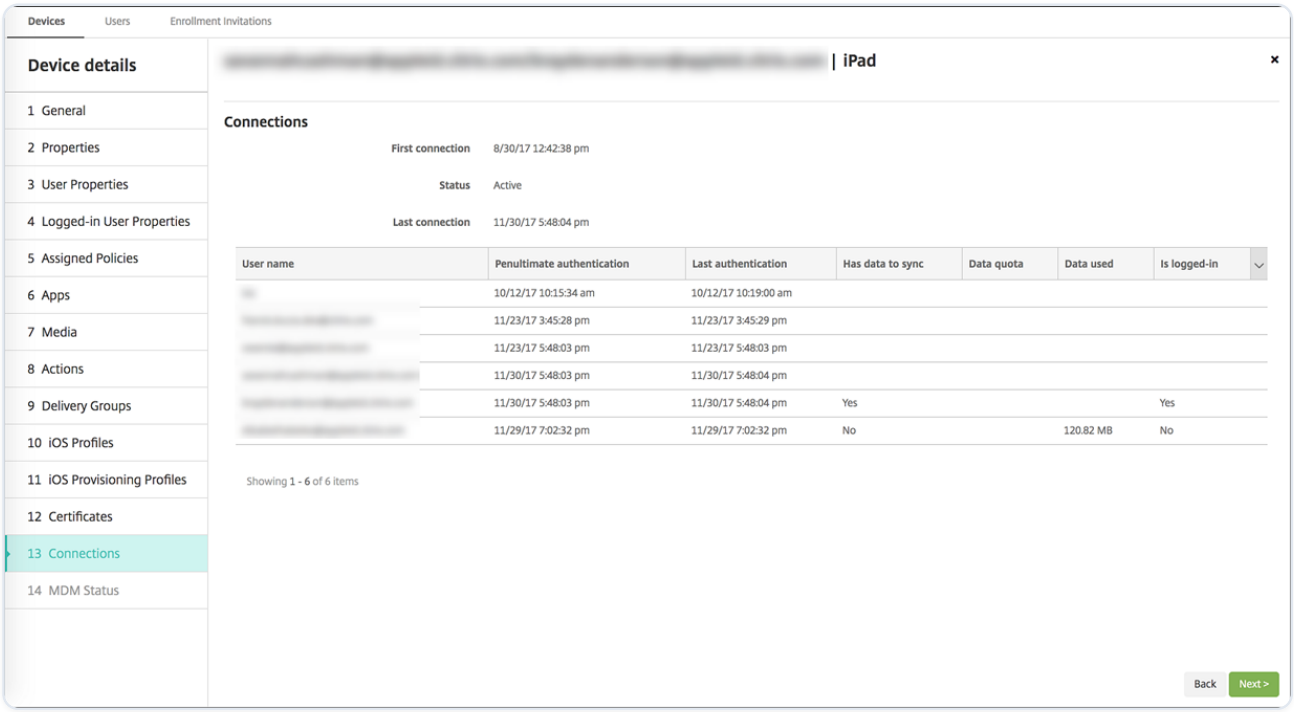




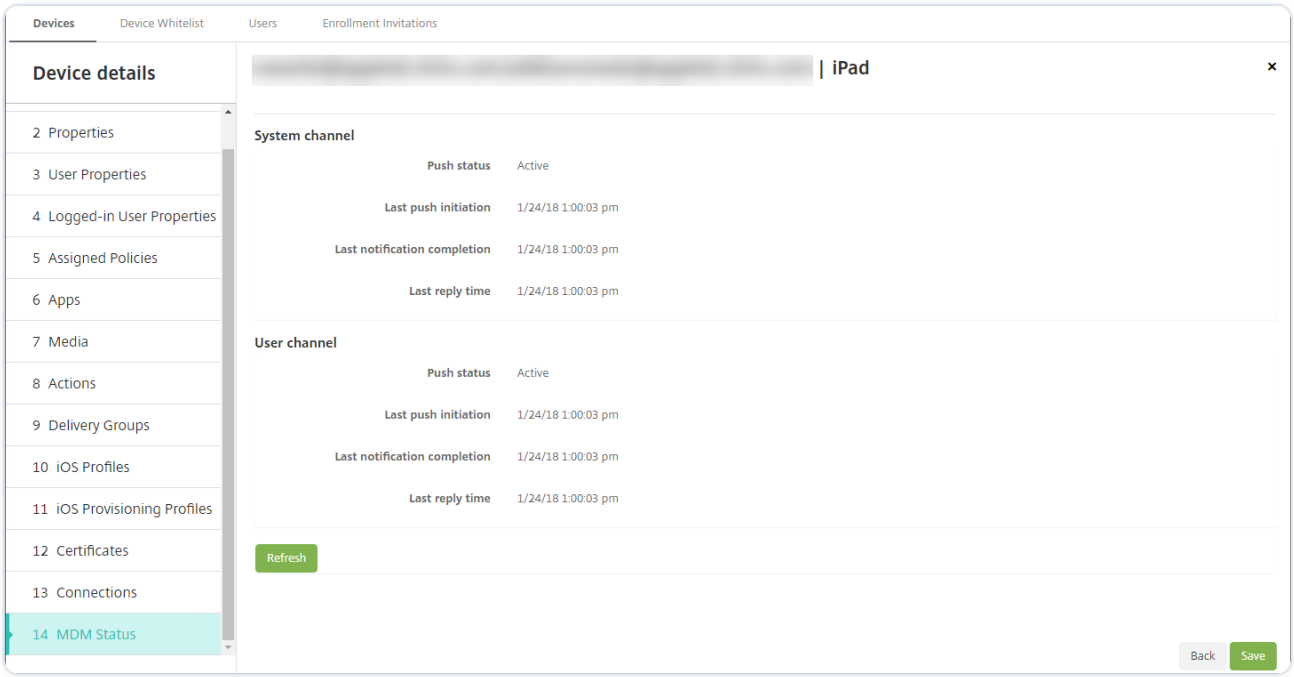
- 在**管理 > 设备 > 交付组**页面上，查看用于向交付组中的设备所有者和用户部署资源的通道。**通道/用户**列显示类型（**系统**或**用户**）和收件人。



- 获取有关常驻用户的信息：
  - **有要同步的数据：**用户是否有要同步到云的数据。
  - **数据配额：** 为用户设置的以字节为单位的数据配额。如果用户配额暂时关闭或未对用户强制执行，则可能不会显示配额。
  - **已用数据：** 用户使用的以字节为单位的数据量。如果系统收集信息时发生错误，则可能不会显示该值。
  - **是否已登录：** 用户是否已登录到设备。



- 查看两个通道的推送状态。



分发 Apple 应用

Citrix Endpoint Management 管理部署到设备的应用。您可以组织和部署以下类型的 iOS/iPadOS 和 macOS 应用。

- **公共应用商店（仅限 iOS/iPadOS）**：这些应用包括在公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用。例如，GoToMeeting。
- **企业（iOS/iPadOS/macOS）**：未启用 MDX 且不具有与 MDX 应用关联的策略的本机应用。
- **MDX（仅限 iOS/iPadOS）**：使用 MAM SDK 准备或使用 MDX Toolkit 封装的应用。这些应用包含 MDX 策略。您可以从内部源和公共商店获取 MDX 应用。
- **批量采购（iOS/iPadOS/macOS）**：通过 Apple 批量采购计划管理许可证的应用。
- **iOS 自定义应用（仅限 iOS/iPadOS）**：内部开发或由第三方开发的专有企业对企业应用。

有关不同类型应用的更多信息，请参阅 添加应用。

某些部署需要 Apple Business Management (ABM) 或 Apple School Management (ASM) 帐户。有关更多信息，请参阅以下部分。

对于每种应用类型和分发方法，Citrix 都推荐一套配置实践。有关分发其他平台应用的信息，请参阅添加应用。以下部分提供了有关 iOS 应用配置的更深入信息。

应用分发的一般步骤

场景	步骤 1：关联帐户	步骤 2：添加和配置应用	步骤 3：配置交付组并部署应用
公共应用商店应用，包括 Citrix 移动应用	不适用	**在 Citrix Endpoint Management 中：配置 > 应用程序**，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 Citrix Endpoint Management 中：**使用交付组配置和部署应用程序。
通过 Apple Volume Purchase 交付的公共应用商店应用程序，包括 Citrix 移动应用程序	注册 Apple 部署计划。**在 Citrix Endpoint Management 中：**转到**设置 > 批量购买**以添加您的批量购买帐户。	**在 ABM 或 ASM 中：**从“应用和图书”购买并添加应用程序。**在 Citrix Endpoint Management 中：**转到**配置 > 应用程序**，配置应用程序并将其分配给交付组。	**在 Citrix 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 Citrix 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 Citrix 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 Citrix Endpoint Management 中：**转到**配置 > 应用程序**。单击**添加**，然后单击**MDX**。确保为平台选择 **iPad/iPhone**。上载 MDX 文件。配置应用程序并将其分配给交付组。	**在 Citrix Endpoint Management 中：**使用交付组配置和部署应用程序。

场景	步骤 1：关联帐户	步骤 2：添加和配置应用	步骤 3：配置交付组并部署应用
使用 Apple Volume Purchase 分发的 MDX 应用程序	注册 Apple 部署计划。**在 Citrix Endpoint Management 中：**转到**设置 > 批量购买**以添加您的批量购买帐户。	**在 ABM 中：**从“应用和图书”购买并添加 MDX 应用程序。将应用程序链接到您的 ABM 帐户。**在 Citrix Endpoint Management 中：**转到**配置 > 应用程序**，配置应用程序并将其分配给交付组。	**在 Citrix Endpoint Management 中：**使用交付组配置和部署应用程序。
自定义应用程序	注册 Apple 部署计划。**在 Citrix Endpoint Management 中：**转到**设置 > 批量购买**以添加您的批量购买帐户。	**在 ABM 中：**将您的应用程序作为私人应用程序添加到 App Store。将应用程序链接到您的 ABM 帐户。**在 Citrix Endpoint Management 中：**转到**配置 > 应用程序**，配置应用程序，并将其分配给交付组。	**在 Citrix Endpoint Management 中：**使用交付组配置和部署应用程序。
启用 MDX 的自定义应用程序	注册 Apple 部署计划。**在 Citrix Endpoint Management 中：**转到**设置 > 批量购买**以添加您的批量购买帐户。	**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。将应用程序链接到您的 ABM 帐户。**在 Citrix Endpoint Management 中：**转到**配置 > 应用程序**并上传 MDX 文件。配置应用程序并将其分配给交付组。	**在 Citrix Endpoint Management 中：**使用交付组配置和部署应用程序。

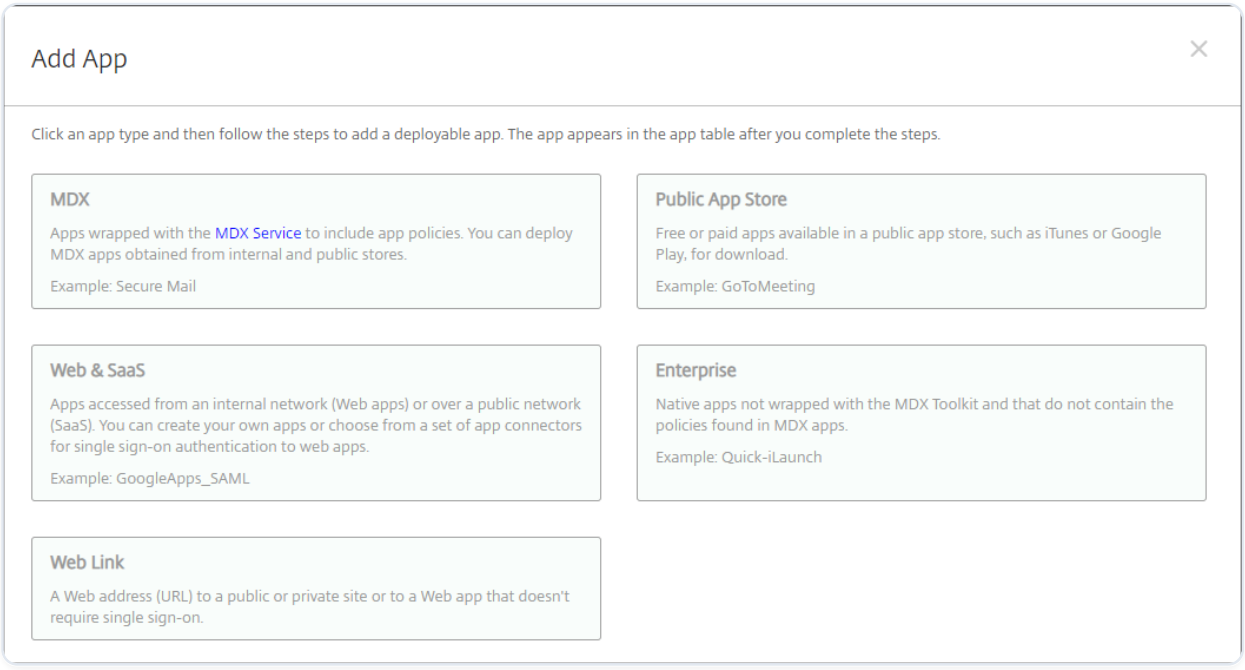
公共应用商店应用程序

您可以将 App Store 上提供的免费和付费应用程序添加到 Citrix Endpoint Management。

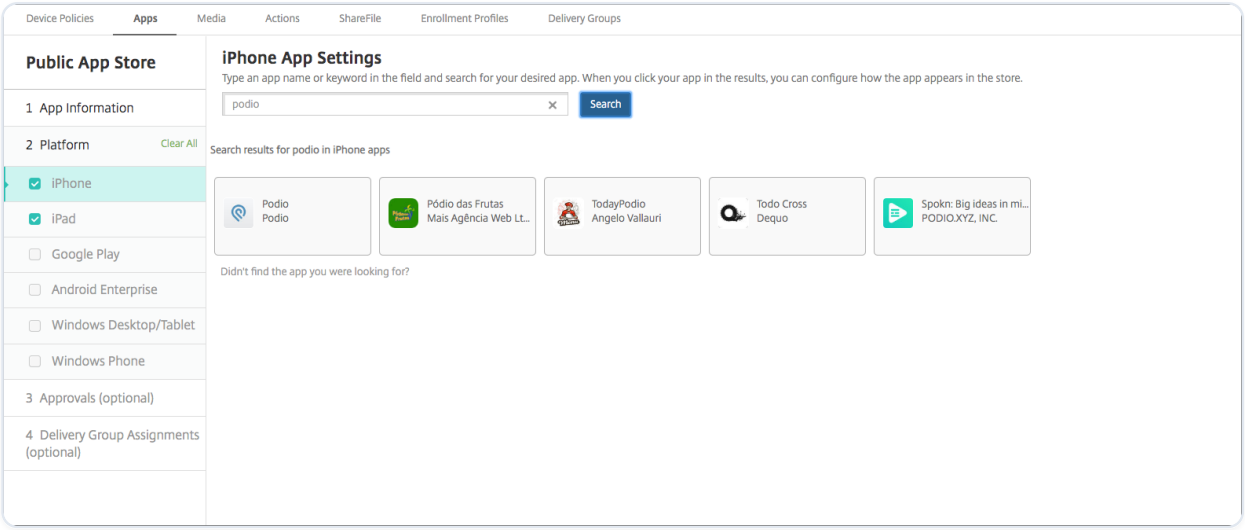
功能可用性	
需要设备监管	否
适用于用户注册模式	否
适用于	iOS/iPadOS

步骤 1：添加和配置应用程序

1. 在 Citrix 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**”。

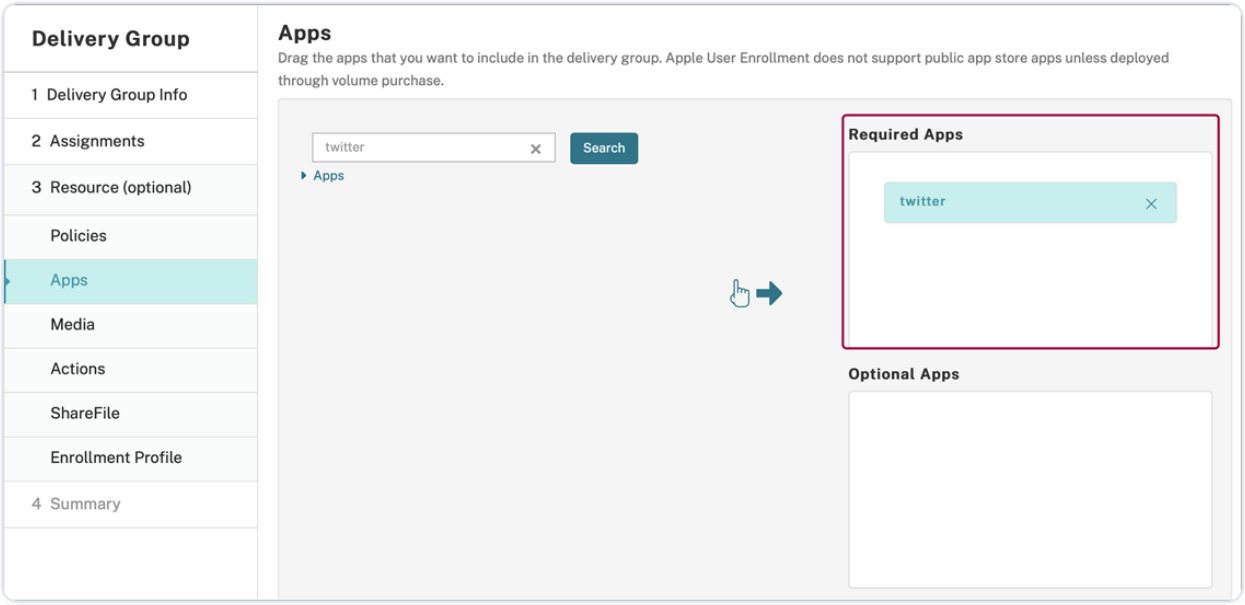


5. 符合搜索条件的应用程序将显示。单击所需的应用程序。

6. 将交付组分配给应用程序，然后单击“**保存**”。

步骤 2：配置应用程序部署

1. 在 Citrix 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“**强制应用程序受管**”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**”部分中，将所需的应用程序拖动到“**所需应用程序**”框中。



7. 返回到 **配置 > 交付组**。
8. 选择交付组，然后单击 **部署**。

9. 用户会收到安装应用程序的请求，接受后，应用程序会在后台安装。



通过 Apple 批量采购交付的公共应用商店应用程序

您可以通过 Apple 批量采购计划管理 iOS/iPadOS 应用程序许可证。请按照以下步骤将批量采购应用程序添加到 Citrix Endpoint Management。

功能可用性	
需要设备监督	否
适用于用户注册模式	是
适用于	iOS/iPadOS/macOS

步骤 1: 链接帐户

1. 设置并注册 Apple Business Manager (ABM) 或 Apple School Manager (ASM)。有关这些程序的详细信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 Citrix Endpoint Management 链接。有关链接批量采购帐户的详细信息，请参阅 Apple 批量采购。
3. 添加批量采购帐户时，请启用 **应用程序自动更新**。此设置可确保当 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 **强制应用程序受管** 设置，则无需提示用户即可更新。无论应用程序是必需的还是可选的，都会进行更新。

要使用 **强制应用程序受管** 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。

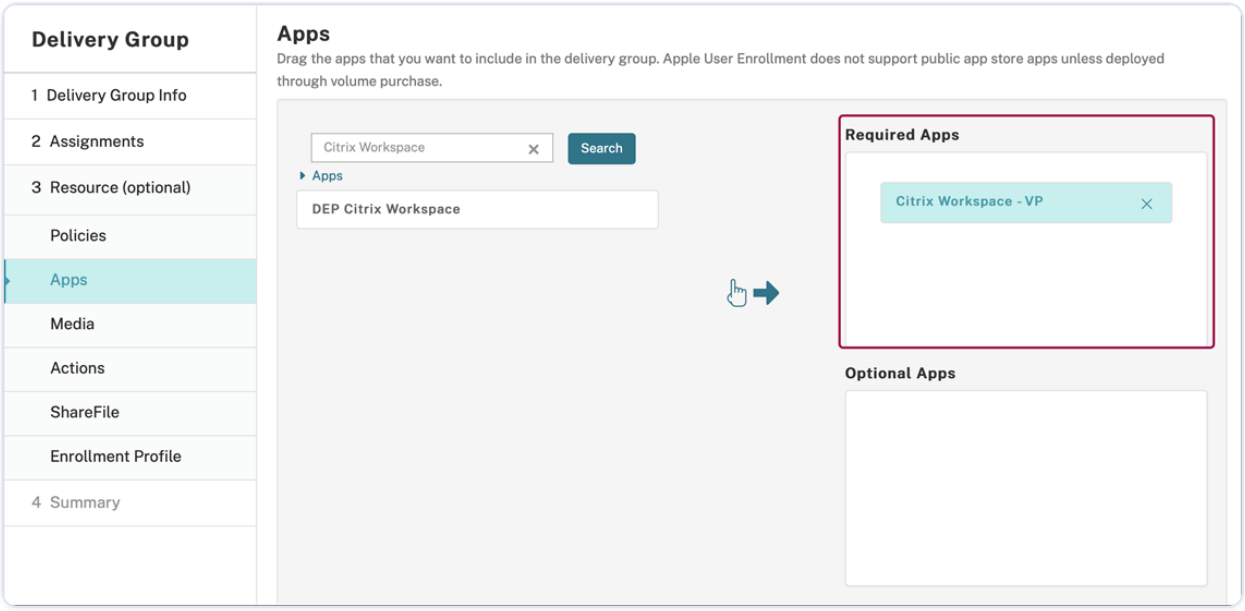
步骤 2：从 Apple 获取应用和许可证

在您的 ABM/ASM 帐户上购买应用。您可以在 Apple Books（仅适用于 iOS/iPadOS）和 Apple App Store 中进行购买。请记住，即使是免费应用，您也必须购买。在 ABM/ASM 上购买许可证后，Citrix Endpoint Management 会自动显示该应用。

有关如何使应用可供您的企业使用的信息，请参阅Apple 文档。

步骤 3：配置应用部署

1. 在 Citrix Endpoint Management 控制台中，导航到 **Configure > Apps**。
2. 选择要配置的批量购买应用，然后单击 **Edit**。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. Citrix 建议启用**强制应用受管**功能（仅限 iOS/iPadOS）。
5. 分配任何交付组，然后单击 **Save**。
6. 导航到 **Configure > Delivery Groups**，然后单击 **Add**。
7. 在 **Apps** 部分中，将所需应用拖动到 **Required Apps** 框中。



8. 导航回 **配置 > 交付组**。
9. 选择交付组，然后单击 **Deploy**。

10. 用户会收到安装应用的请求，接受后应用会在后台安装。



企业应用

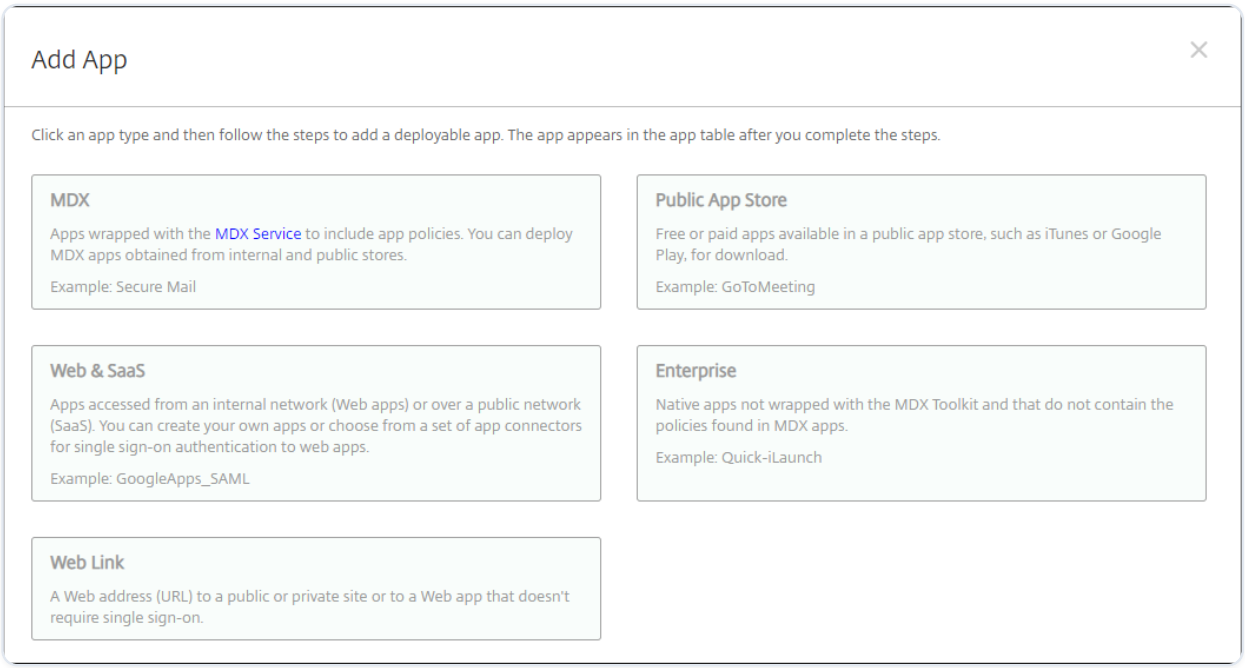
您还可以添加未关联任何 MDX 策略的本机应用程序。请按照以下步骤添加 App Store 中不存在的应用程序。

功能可用性	
需要设备监管	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 Citrix Endpoint Management 控制台中，导航到**配置 > 应用程序**。单击**添加**。

2. 单击**企业**。



3. 在**应用程序信息**页面上，配置以下内容：

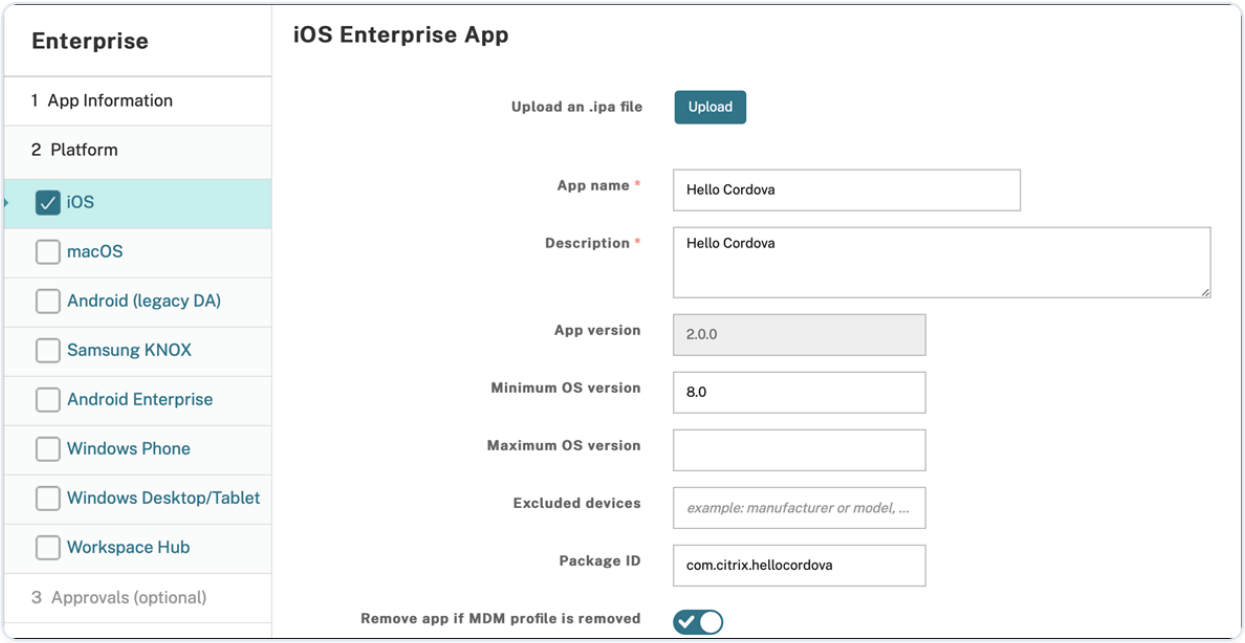
   - **名称：**键入应用程序的描述性名称。该名称将显示在“应用程序”表中的“应用程序名称”下。
   - **说明：**键入应用程序的可选说明。
   - **应用程序类别：**（可选）在列表中，单击要添加应用程序的类别。

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. 上传 IPA 文件 (iOS/iPadOS) 或上传 PKG 文件 (macOS)
7. 单击“**下一步**”。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）为应用程序键入新名称。
   - **应用程序描述：**（可选）为应用程序键入新描述。
   - **应用程序版本：**您无法更改此字段。
   - **最低操作系统版本：**（可选）键入设备可运行的、用于使用此应用程序的最旧操作系统版本。
   - **最高操作系统版本：**（可选）键入设备必须运行的、用于使用此应用程序的最新操作系统。
   - **排除的设备：**（可选）键入无法运行此应用程序的设备的制造商或型号。

- **如果 MDM 配置文件被删除，则删除应用程序：** 选择当 MDM 配置文件被删除时是否从设备中删除应用程序。默认值为“开”。（仅限 iOS/iPadOS）
- **阻止应用程序数据备份：** 选择是否阻止应用程序备份数据。默认值为“开”。（仅限 iOS/iPadOS）
- **强制应用程序受管理：** 如果您安装了非托管应用程序，如果您希望非受监管设备上的用户看到允许管理应用程序的提示，请选择“**开**”。如果他们接受提示，则应用程序将受管理。如果应用程序启用了“**强制应用程序受管理**”设置，则它会在不提示用户的情况下进行更新。无论应用程序是必需的还是可选的，都会进行更新。（仅限 iOS/iPadOS）

要使用“**强制应用程序受管理**”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。

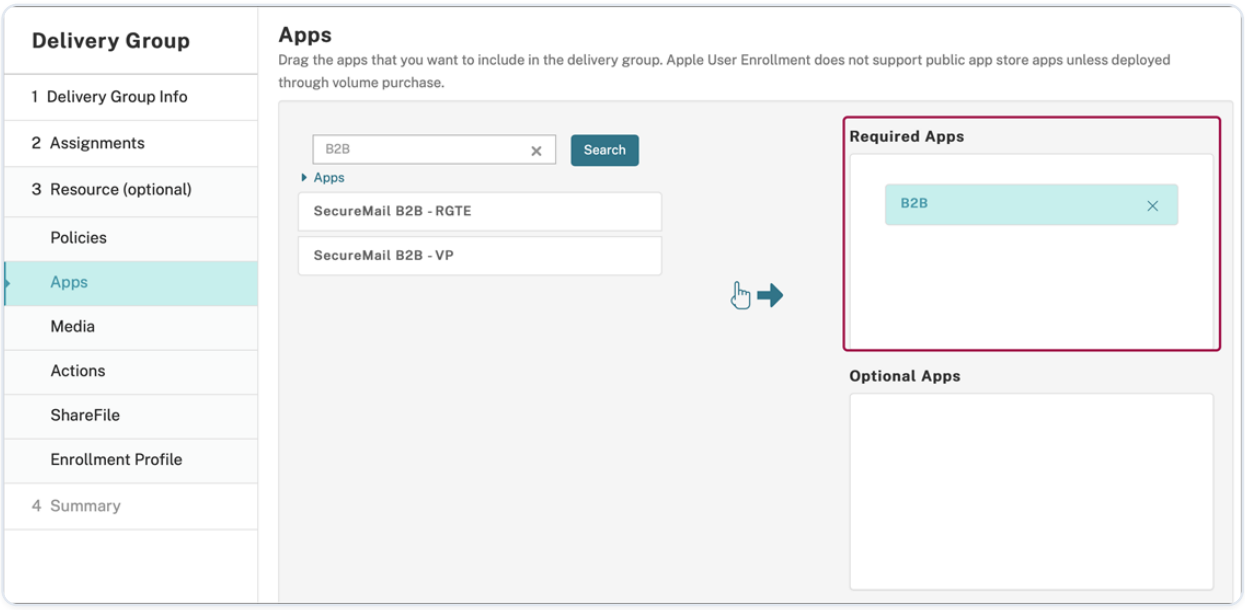


9. 将交付组分配给应用程序，然后单击“**保存**”。

步骤 2: 配置应用部署

1. 在 Citrix 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. 将所需应用程序拖动到 **所需应用程序** 框中。



3. 导航到 **配置 > 交付组**。
4. 选择交付组，然后单击 **部署**。
5. 用户会收到安装应用程序的请求，接受后，应用程序会在后台安装。



MDX 应用程序

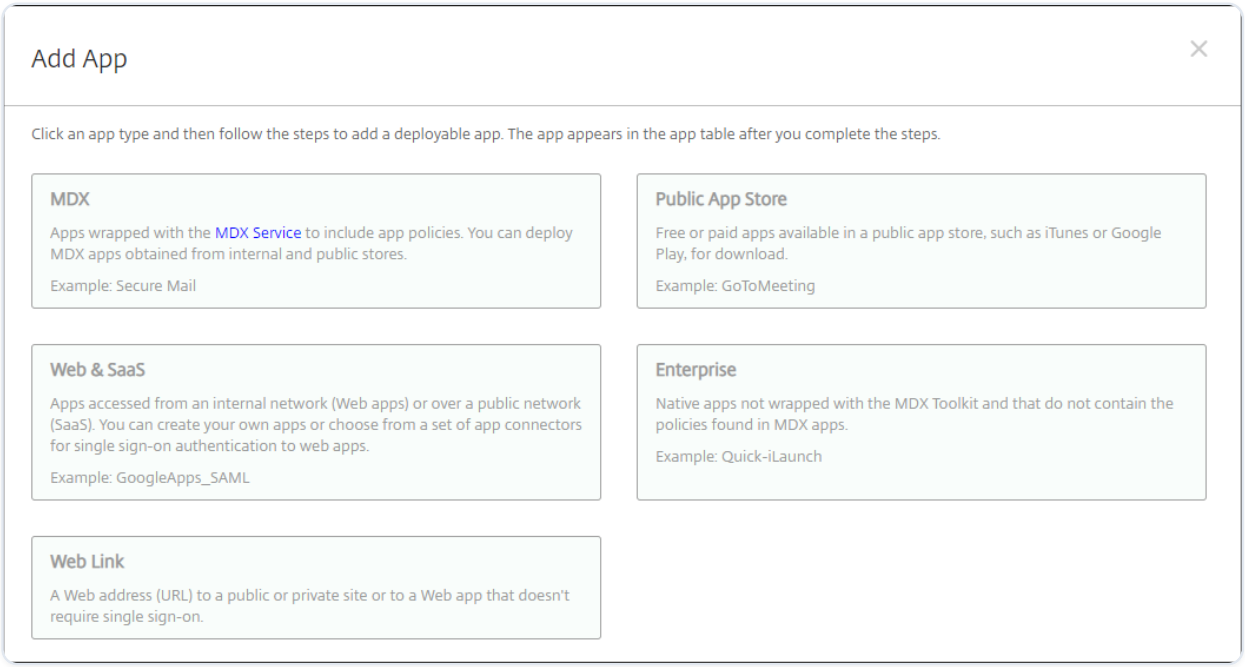
要使用 MDX 策略和安全功能，请添加已启用 MAM SDK 或已 MDX 封装的应用程序。您可以使用批量采购或不使用批量采购来部署 MDX 应用程序。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
可用平台	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 下的步骤操作，然后按照本节中的步骤操作。

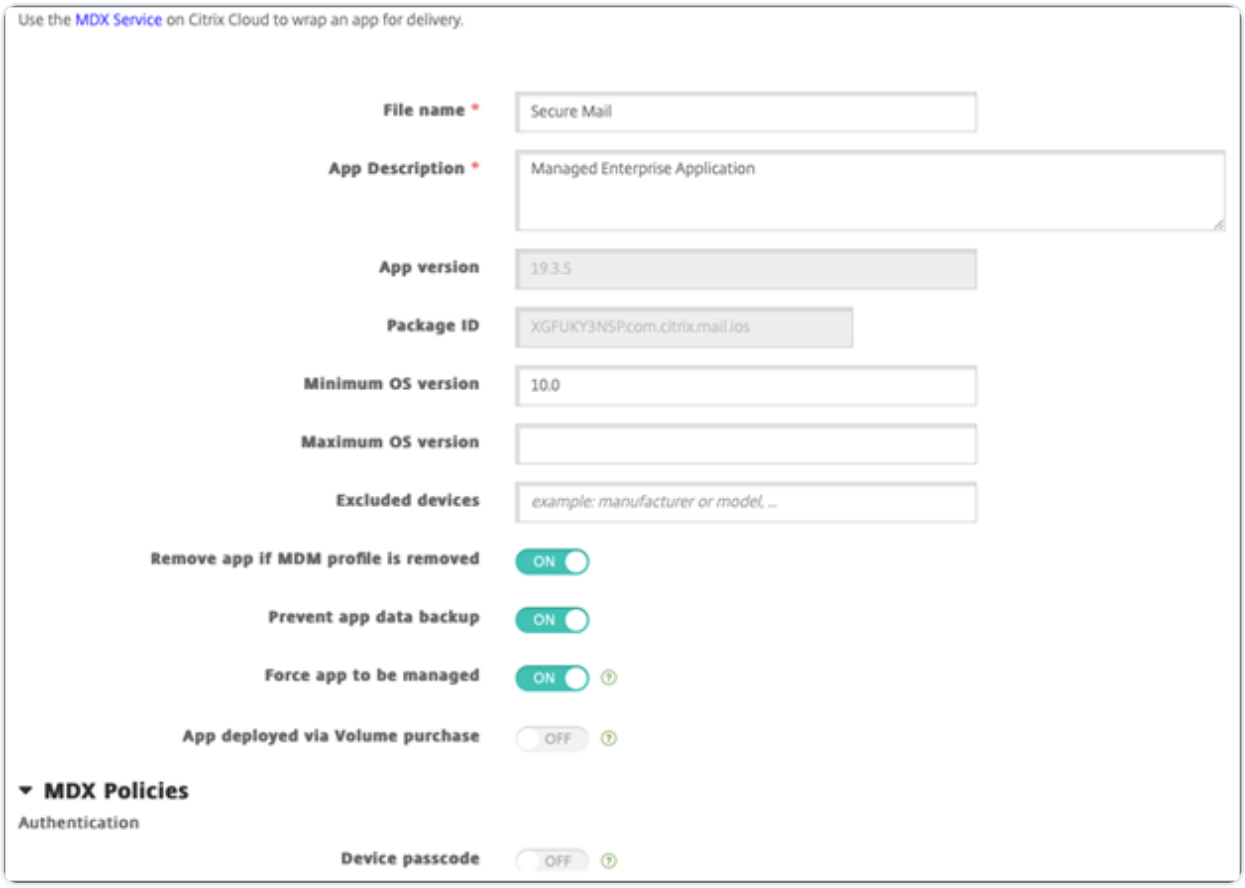
步骤 1: 添加和配置应用程序

1. 在 Citrix Endpoint Management 控制台中，导航到 **配置 > 应用程序**。单击 **添加**。
2. 单击 **MDX**。

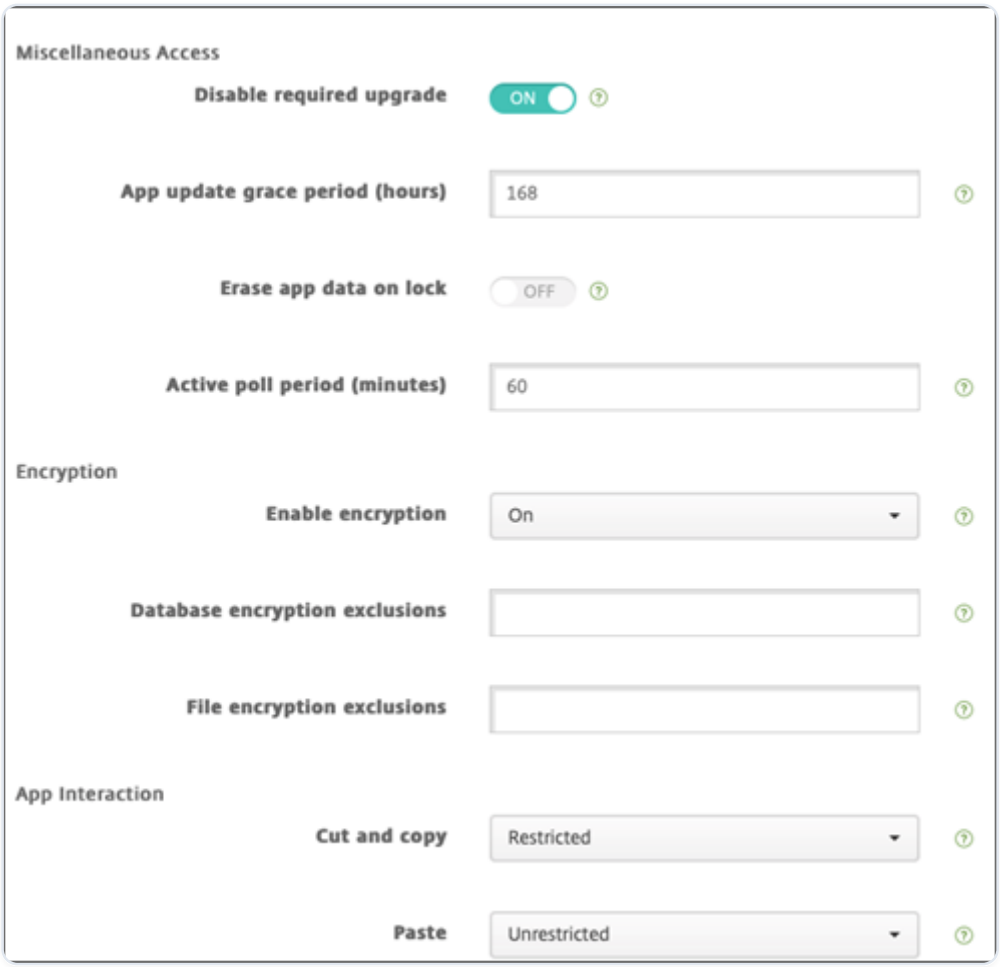


3. 为平台选择 **iPhone** 或 **iPad**。
4. 上传 MDX 文件。

5. 配置应用程序详细信息。将 **通过批量采购部署的应用程序** 设置为 **关闭**。Citrix 还建议启用 **强制管理应用程序** 功能。



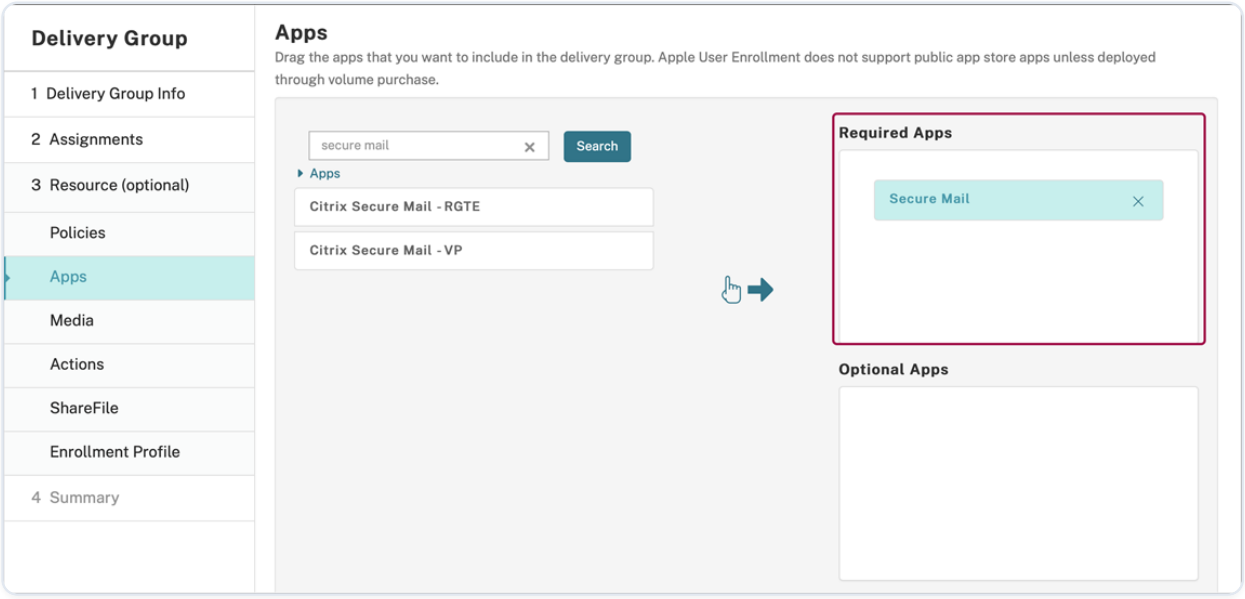
6. 配置 MDX 策略。将 **禁用强制升级** 设置为 **开**。



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 Citrix 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到 **所需应用程序** 框中。



3. 导航到 **配置 > 交付组**。
4. 选择交付组，然后单击 **部署**。
5. 用户会收到安装应用程序的请求，接受后应用程序会在后台安装。



使用 Apple 批量采购分发的 MDX 应用程序

要使用 MDX 策略和安全功能，请添加已启用 MAM SDK 或已 MDX 封装的应用程序。要使用批量采购部署应用程序，这些应用程序必须存在于应用商店中。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
适用于	iOS/iPadOS

步骤 1：链接帐户

1. 设置并注册 Apple Business Manager (ABM) 或 Apple School Manager (ASM)。有关这些程序的更多信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 Citrix Endpoint Management 链接。有关链接批量采购帐户的更多信息，请参阅 Apple 批量采购。

3. 添加批量采购帐户时，请启用**应用程序自动更新**。此设置可确保当 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**强制应用程序受管理**设置，则无需提示用户即可更新。无论应用程序是必需的还是可选的，都会进行更新。

   要使用**强制应用程序受管理**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。

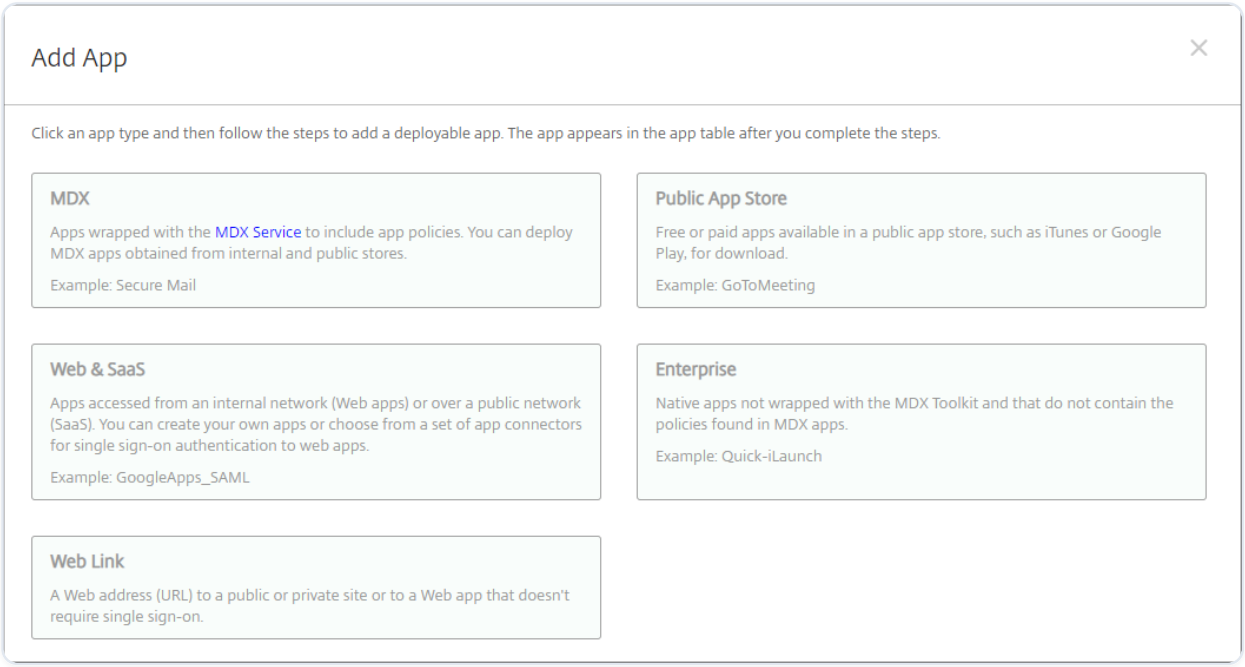
步骤 2：从 Apple 获取应用程序和许可证

在您的 ABM/ASM 帐户上购买应用程序。您可以在 Apple Books（仅适用于 iOS/iPadOS）和 Apple App Store 中进行购买。请记住，即使是免费应用程序，您也必须购买。在 ABM/ASM 上购买许可证后，Citrix Endpoint Management 会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。

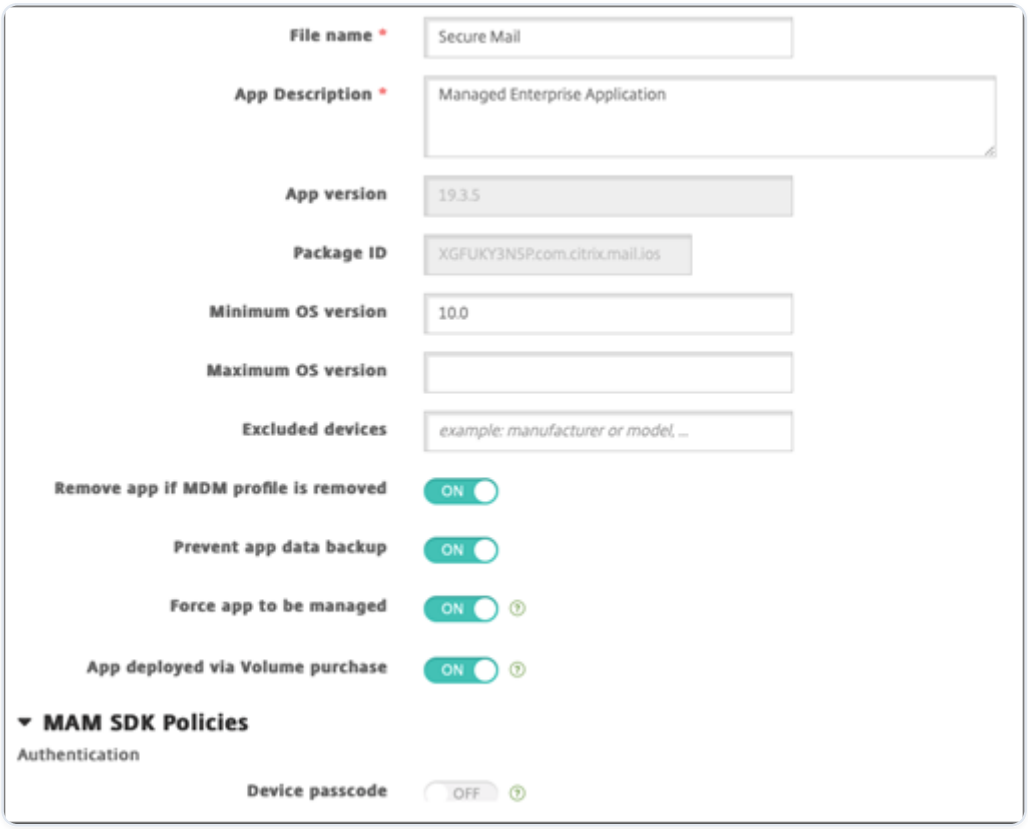
步骤 3：添加和配置应用程序

1. 在 Citrix Endpoint Management 控制台中，导航到**配置 > 应用程序**。单击**添加**。
2. 单击 **MDX**。

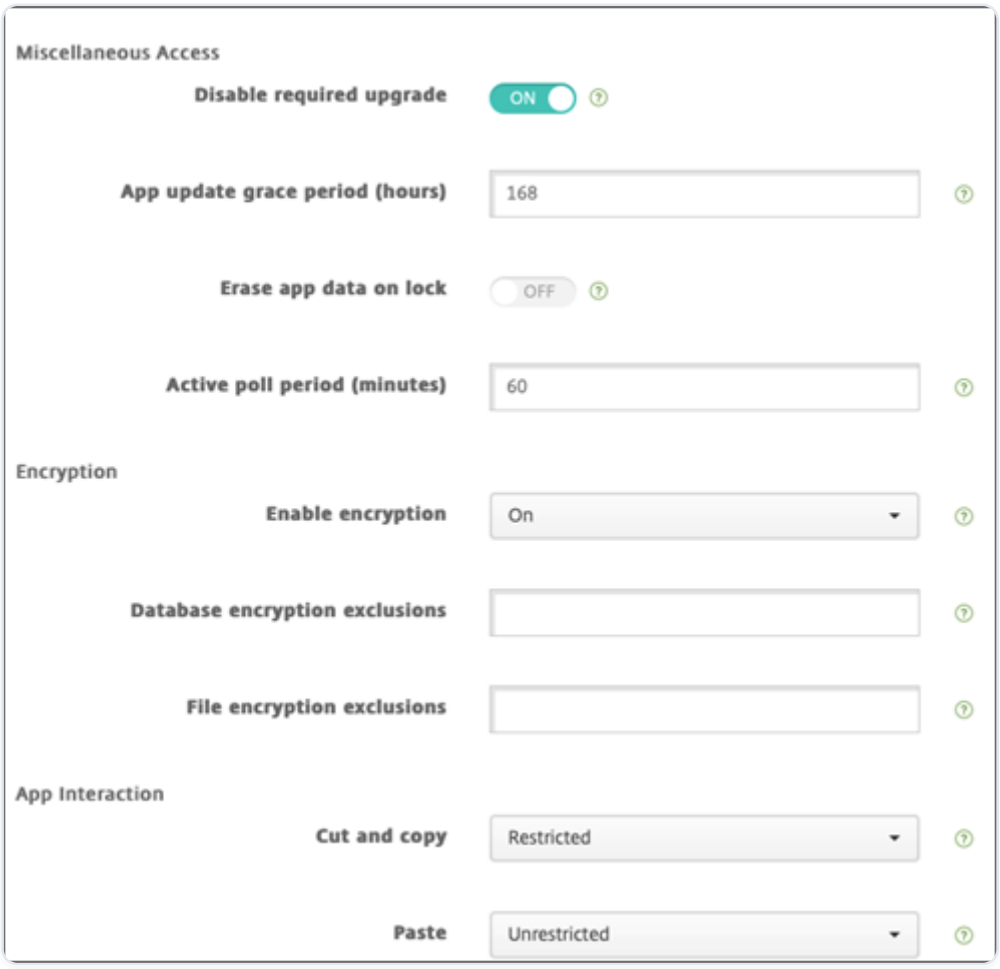


3. 选择 **iPhone** 或 **iPad** 作为平台。
4. 上载 MDX 文件。

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“**禁用强制升级**”设置为“**开**”。



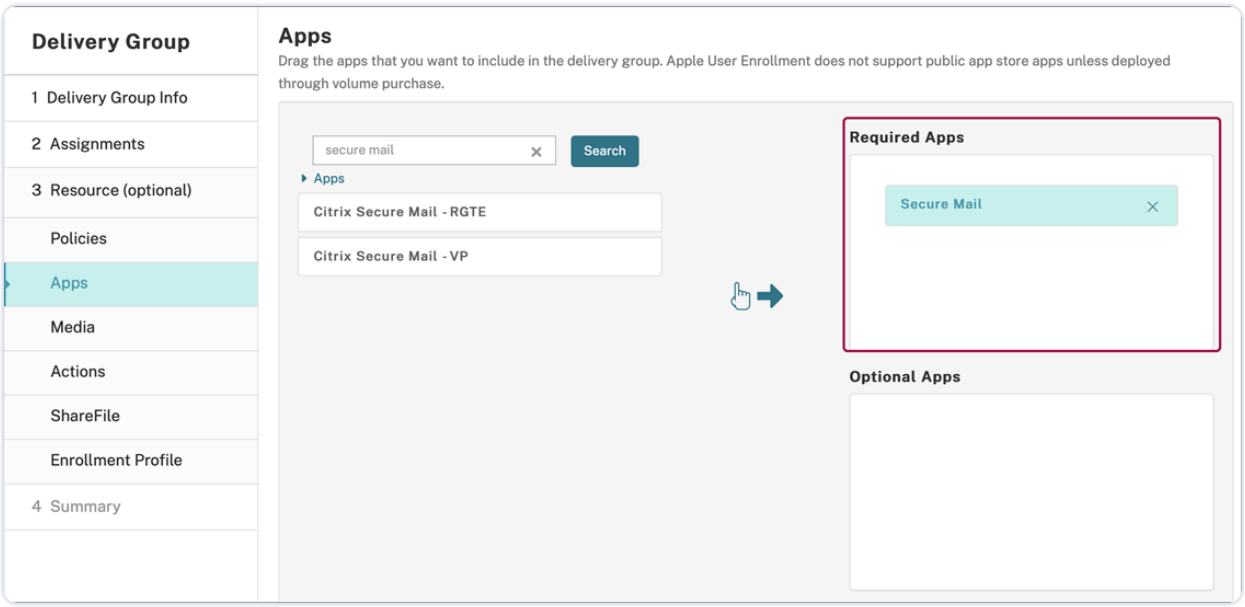
7. 为应用程序针对每个平台分配交付组，然后单击“**保存**”。

此配置会导致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 Citrix 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**”部分中，将所需的 MDX 应用程序拖动到“**所需应用程序**”框中。



3. 导航到“**配置 > 交付组**”。
4. 选择交付组，然后单击“**部署**”。
5. 用户会收到安装应用程序的请求，接受后，应用程序会在后台安装。



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。您可以使用 Citrix Endpoint Management 和 Apple 批量购买来私密且安全地分发专有应用程序。您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。

功能可用性	
需要设备监督	否
适用于用户注册模式	是
适用于	iOS/iPadOS

自定义应用的要求

- Apple 商务管理 或 Apple 校园教务管理 帐户
- Apple Volume Purchase 帐户（需要 iOS 7 或更高版本的设备）
- 使用以下 Apple 注册模式之一，在 Citrix 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

要使用批量采购部署自定义应用，请将您的批量采购帐户链接到 Citrix Endpoint Management。

1. 设置并注册 Apple Business Manager (ABM)。有关这些程序的更多信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 Citrix Endpoint Management 关联。有关关联批量购买帐户的更多信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，请启用 **App Auto Update**。此设置可确保当 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 **Force app to be managed** 设置，则无需提示用户即可更新。无论应用程序是必需的还是可选的，都会进行更新。

   要使用 **Force app to be managed** 和 **App Auto Update** 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

在您的 ABM 帐户上添加应用程序。您可以上传和分发自己的自定义应用程序，或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更多信息，请参阅 Apple 文档。

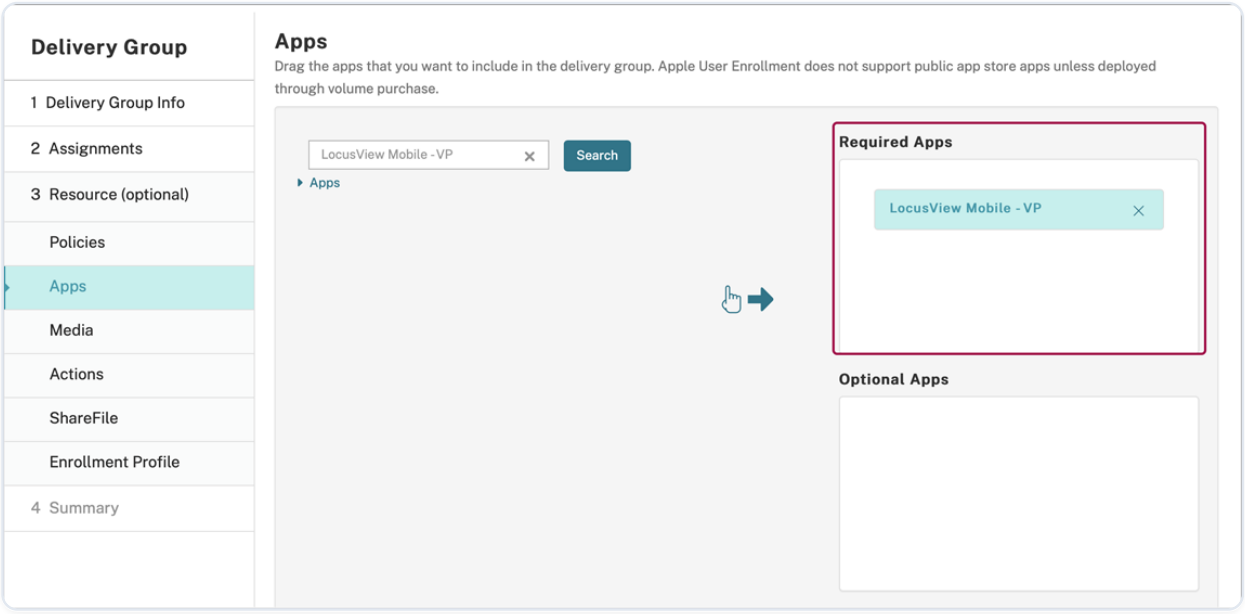
步骤 3：在 Citrix Endpoint Management 中添加和配置应用程序

1. 在 Citrix Endpoint Management 控制台中，导航到 **Configure > Apps**。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 **Edit**。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. 选择要分发应用程序的交付组。单击 **Save**。

步骤 4：配置应用程序部署

1. 在 Citrix Endpoint Management 控制台中，导航到 **Configure > Delivery Groups**，然后单击 **Add**。
2. 在 **Apps** 部分中，将所需的应用程序拖动到 **Required Apps** 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 **Deploy**。

5. 用户收到部署应用程序的请求。用户接受后，应用程序会在后台安装。



启用 MDX 的自定义应用程序

要使用 MDX 策略和安全功能，请添加已启用 MAM SDK 或已 MDX 封装的自定义应用程序。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
适用于	iOS/iPadOS

步骤 1：链接帐户

要使用批量采购部署自定义应用程序，请将您的批量采购帐户链接到 Citrix Endpoint Management。

1. 设置并注册 Apple Business Manager (ABM)。有关这些程序的更多信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 Citrix Endpoint Management 链接。有关链接批量采购帐户的更多信息，请参阅 Apple 批量采购。

3. 添加批量采购帐户时，请启用**应用程序自动更新**。此设置可确保当 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**强制应用程序受管理**设置，它会在不提示用户的情况下进行更新。无论应用程序是必需的还是可选的，都会进行更新。

   要使用**强制应用程序受管理**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

在您的 ABM 帐户上添加应用程序。您可以上传和分发自己的自定义应用程序，也可以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更多信息，请参阅 Apple 文档。

步骤 3：在 Citrix Endpoint Management 中添加和配置应用程序

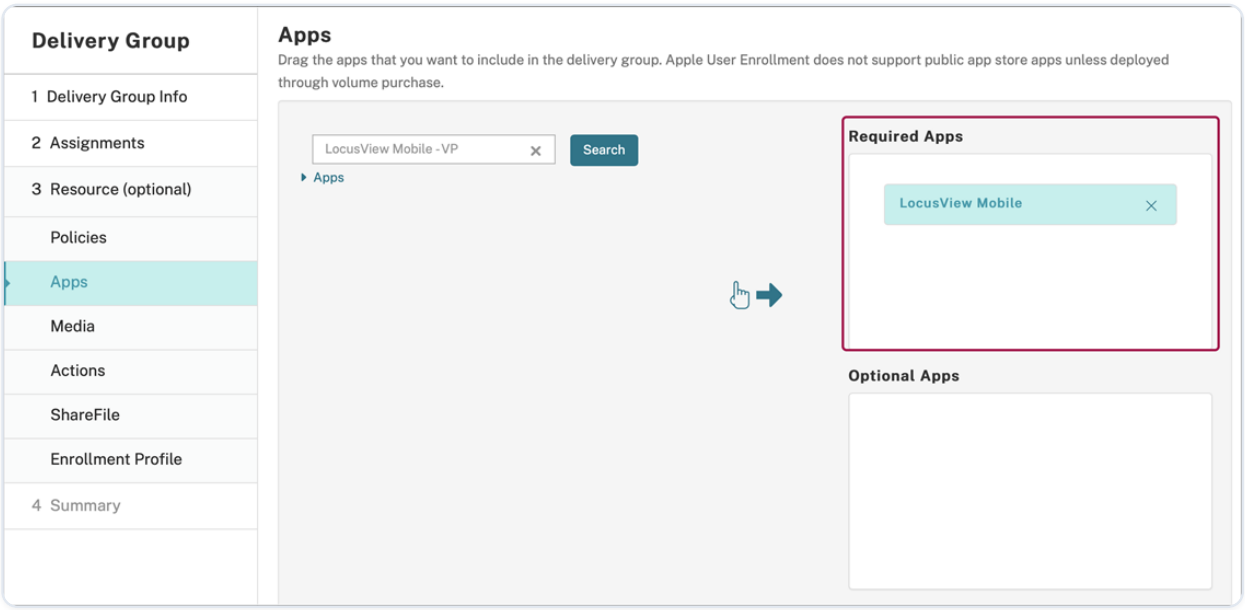
1. 在 Citrix Endpoint Management 控制台中，导航到“**配置 > 应用程序**”。单击“**添加**”。
2. 单击“**MDX**”。 (/en-us/citrix-endpoint-management/media/configure-apps-add.png)
3. 选择“**iPhone**”或“**iPad**”平台。
4. 上传要添加的应用程序的 MDX 文件。
5. 配置应用程序详细信息。将“**通过批量购买部署应用程序**”设置为“**开**”。Citrix 还建议启用“**强制管理应用程序**”功能。 (/en-us/citrix-endpoint-management/media/mdx-app-volume-purchase-on.png)
6. 配置 MDX 策略。将“**禁用强制升级**”设置为“**开**”。 (/en-us/citrix-endpoint-management/media/mdx-app-disable-required-upgrade.png)
7. 将交付组分配给应用程序，然后单击“**保存**”。

此配置会导致此应用程序在应用程序列表中显示两个条目。配置应用程序时，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 Citrix Endpoint Management 控制台中，导航到“**配置 > 应用程序**”。批量购买的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**”部分中，将所需的 MDX 应用拖动到“**所需应用**”框中。



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的请求。用户接受后，应用会在后台安装。

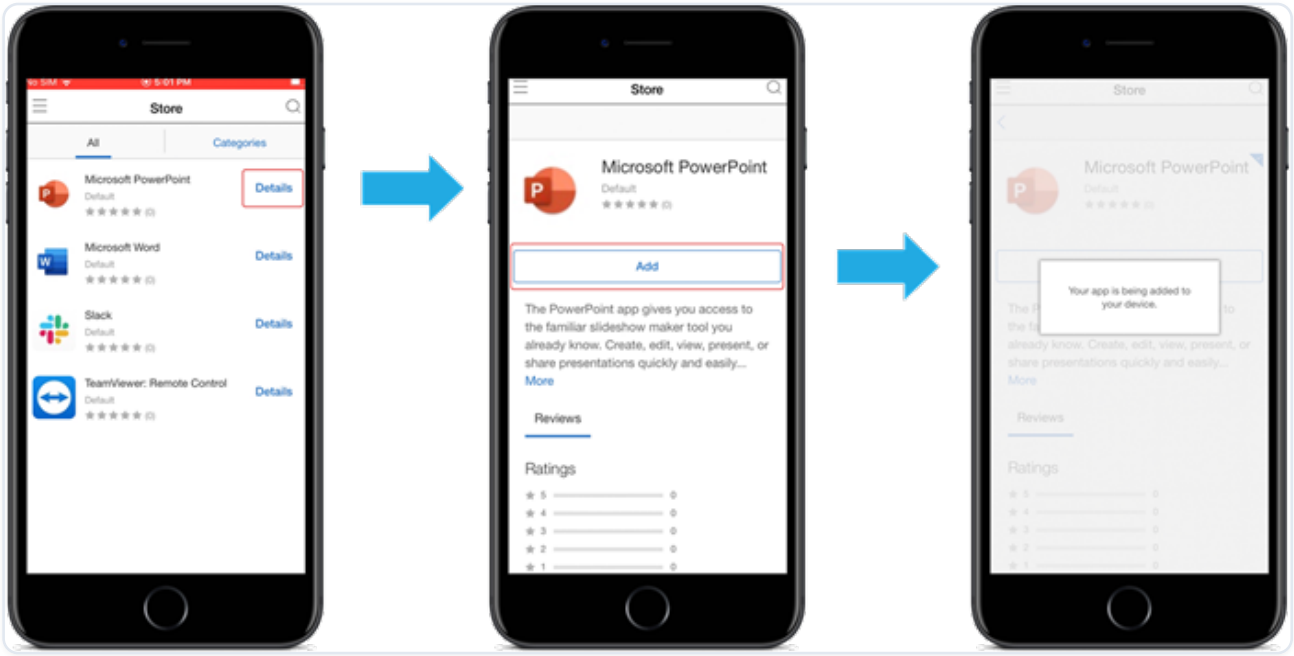


可选应用（仅限 iOS/iPadOS）

Citrix 建议将应用部署为“**必需**”。必需应用会在用户设备上静默安装，从而最大程度地减少交互。启用此功能后，应用还可以自动更新。

可选应用允许用户选择要安装的应用，但用户必须通过 Citrix Secure Hub 手动启动安装。

要安装可选应用，用户必须启动 Citrix Secure Hub，转到“**商店**”，选择所需应用的“**详细信息**”，然后单击“**添加**”。



网络访问控制

您可以使用您的网络访问控制 (NAC) 解决方案来扩展 Citrix Endpoint Management 针对 Android 和 Apple 设备的设备安全评估。您的 NAC 解决方案使用 Citrix Endpoint Management 安全评估来促进和处理身份验证决策。配置 NAC 设备后，您在 Citrix Endpoint Management 中配置的设备策略和 NAC 筛选器将得到强制执行。

将 Citrix Endpoint Management 与 NAC 解决方案结合使用，可以为网络内部的设备添加 QoS 和更精细的控制。有关将 NAC 与 Citrix Endpoint Management 集成的优势摘要，请参阅访问控制。

Citrix 支持以下解决方案与 Citrix Endpoint Management 集成：

- NetScaler 网关
- ForeScout

Citrix® 不保证与其他 NAC 解决方案的集成。

在您的网络中使用 NAC 设备时：

- Citrix Endpoint Management 支持 NAC 作为 iOS、Android Enterprise 和 Android 设备的端点安全功能。
- 您可以在 Citrix Endpoint Management 中启用筛选器，根据规则或属性将设备设置为符合或不符合 NAC 规范。例如：

- 如果 Citrix Endpoint Management 中的托管设备不符合指定条件，Citrix Endpoint Management 会将该设备标记为不合规。NAC 设备会阻止网络上的不合规设备。
- 如果 Citrix Endpoint Management 中的托管设备安装了不合规的应用程序，NAC 筛选器可以阻止 VPN 连接。因此，不合规的用户设备无法通过 VPN 访问应用程序或网站。
- 如果您将 NetScaler Gateway 用于 NAC，可以启用拆分隧道以防止 NetScaler Gateway 插件向 NetScaler Gateway 发送不必要的网络流量。有关拆分隧道的更多信息，请参阅配置拆分隧道。

支持的 NAC 合规性筛选器

Citrix Endpoint Management 支持以下 NAC 合规性筛选器：

匿名设备： 检查设备是否处于匿名模式。如果设备尝试重新连接时 Citrix Endpoint Management 无法重新验证用户身份，则此检查可用。

禁用应用： 检查设备是否具有应用访问策略中定义的禁用应用。有关该策略的详细信息，请参阅 应用访问设备策略。

非活动设备： 检查设备是否处于非活动状态，此状态由**服务器属性**中的**设备非活动天数阈值**设置定义。有关详细信息，请参阅 服务器属性。

缺少所需应用： 检查设备是否缺少应用访问策略中定义的任何所需应用。

非建议应用： 检查设备是否具有应用访问策略中定义的非建议应用。

不合规密码： 检查用户密码是否合规。在 iOS 和 Android 设备上，Citrix Endpoint Management 可以确定设备上当前密码是否符合发送到设备的密码策略。例如，在 iOS 上，如果 Citrix Endpoint Management 向设备发送密码策略，用户有 60 分钟的时间来设置密码。在用户设置密码之前，密码可能不合规。

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，自动化操作或使用 Citrix Endpoint Management API 的第三方会更改该属性。

已吊销状态： 检查设备证书是否已吊销。已吊销的设备在再次获得授权之前无法重新注册。

已 Root 的 Android 设备和已越狱的 iOS 设备： 检查 Android 或 iOS 设备是否已越狱。

未管理设备： 检查 Citrix Endpoint Management 是否正在管理设备。例如，已注册 MAM 的设备或未注册的设备不受管理。

> **注意：**

> 隐式合规/不合规筛选器仅在 Citrix Endpoint Management 正在管理的设备上设置默认值。例如，任何安装了被阻止应用或未注册的设备都将被标记为“不合规”。NAC 设备会阻止这些设备访问您的网络。

配置概述

建议您按所列顺序配置 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。

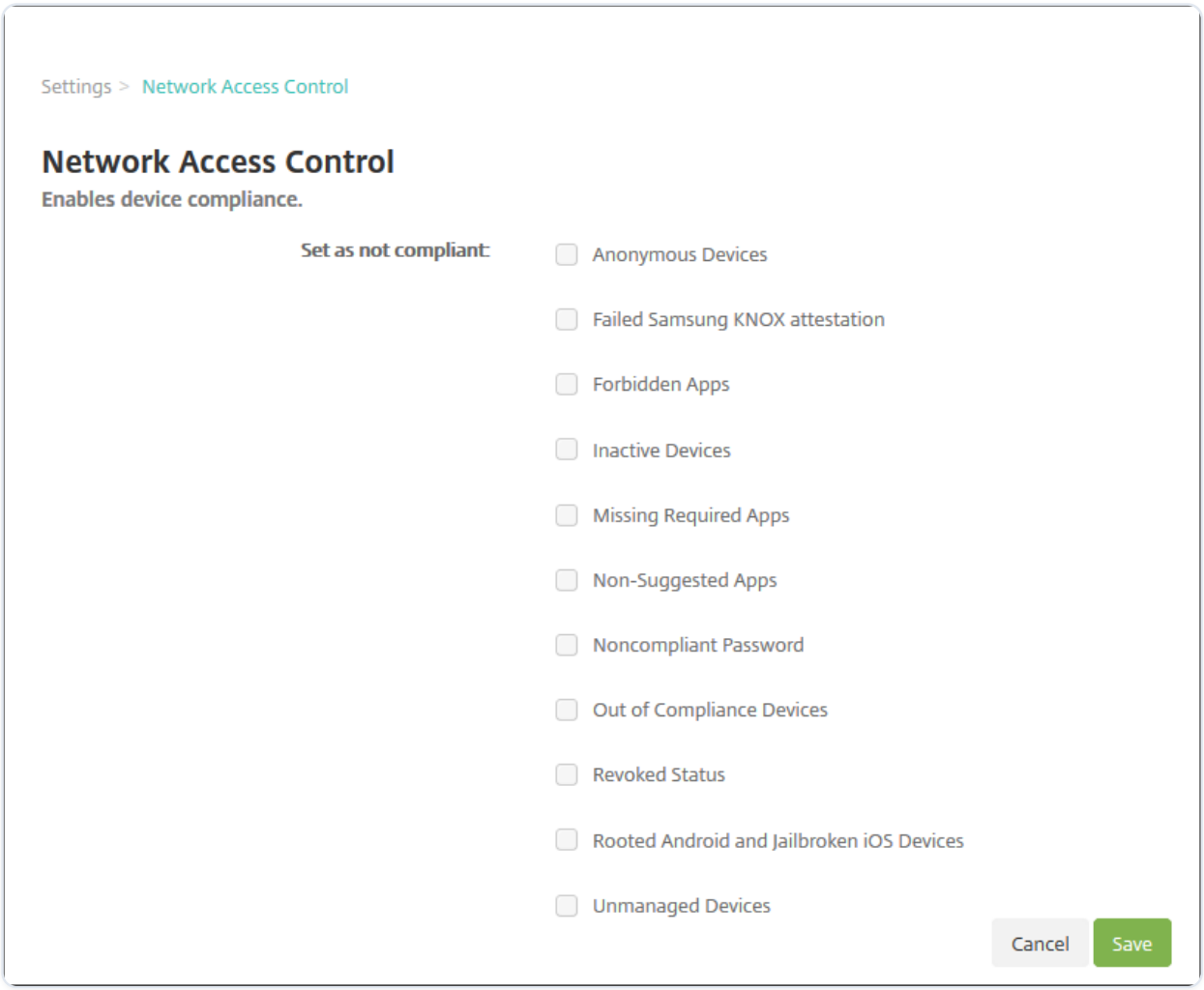
   对于 Android 设备： 请参阅 配置适用于 Android 的 Citrix SSO 协议。
2. 在 Citrix Endpoint Management 中启用 NAC 筛选器。
3. 配置 NAC 解决方案：

   - NetScaler Gateway，详细信息请参阅 更新 NetScaler Gateway 策略以支持 NAC。

     要求您在设备上安装 Citrix SSO。请参阅 NetScaler Gateway 客户端。
   - ForeScout：请参阅 ForeScout 文档。

在 Citrix Endpoint Management 中启用 NAC 筛选器

1. 在 Citrix Endpoint Management 控制台中，转到 **设置 > 网络访问控制**。



2. 选中要启用的 **设置为不合规** 筛选器对应的复选框。
3. 点击 **保存**。

更新 NetScaler Gateway 策略以支持 NAC

您必须在 VPN 虚拟服务器上配置高级（非经典）身份验证和 VPN 会话策略。

这些步骤将更新具有以下任一特征的 NetScaler Gateway：

- 与 Citrix Endpoint Management 进行了集成。
- 或者，已设置为 VPN，不属于 Citrix Endpoint Management 环境，并且可以访问 Citrix Endpoint Management。

在控制台窗口中，在您的虚拟 VPN 服务器上执行以下操作。命令和示例中的 FQDN 和 IP 地址均为虚构。

1. 如果您的 VPN 虚拟服务器上正在使用经典策略，请移除并解除绑定所有经典策略。要检查，请键入：

   ```
   show vpn vserver <VPN_VServer>
   ```

移除任何包含单词 **Classic** 的结果。例如：`VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

要移除策略，请键入：

`unbind vpn vserver <VPN_VServer> -policy <policy_name>`

2. 通过键入以下内容创建相应的“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. 通过键入以下内容将策略绑定到您的 VPN 虚拟服务器。

   `bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100`

4. 通过键入以下内容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。

5. 通过键入以下内容将 SSL 证书绑定到虚拟服务器。

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   例如：`bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. 将身份验证配置文件从 VPN 虚拟服务器关联到身份验证虚拟服务器。首先，通过键入以下内容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. 通过键入以下内容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. 通过键入以下内容检查从 NetScaler 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，此查询通过获取环境中注册的第一个设备 (`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"
   ```

   成功的结果类似于以下示例。

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. 当前一步成功后，创建到 Citrix Endpoint Management 的 Web 身份验证操作。首先，创建一个策略表达式以从 iOS VPN 插件中提取设备 ID。键入以下内容。

   ```
   add policy expression xm_deviceid_expression
   "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',
   \'&\').VALUE(\"deviceidvalue\")"
   ```

10. 通过键入以下内容将请求发送到 Citrix Endpoint Management。在此示例中，Citrix Endpoint Management IP 为 `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\")"
    ```

    Citrix 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. 通过键入以下内容，创建用于关联操作的身份验证策略。

```
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. 通过键入以下内容，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. 通过键入以下内容，添加用于关联 LDAP 策略的策略标签。

```
add authentication policylabel <policy_label_name>
```

例如：`add authentication policylabel ldap_pol_label`

14. 通过键入以下内容，将 LDAP 策略与策略标签关联。

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
```

15. 连接合规设备以执行 NAC 测试，确认 LDAP 身份验证成功。键入以下内容。

```
bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END
```

16. 添加要与身份验证虚拟服务器关联的 UI。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. 通过键入以下内容，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 Citrix Secure Hub 连接。键入以下内容。

```
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
```

Windows

Windows 桌面和平板电脑

Citrix Endpoint Management 将 Windows 10 和 Windows 11 设备注册到 MDM。Citrix Endpoint Management 支持以下用于注册到 MDM 的 Windows 10 和 Windows 11 设备的身份验证类型：

- 基于域的身份验证
  - 活动目录
  - Azure 活动目录
- 身份提供程序：
  - Azure 活动目录
  - Citrix® 身份提供程序

有关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 设备管理的通用工作流程如下：

1. 完成入门过程。请参阅入门和资源设置和准备注册设备和交付资源。

   如果您计划使用 AutoDiscovery 服务注册 Windows 设备，则必须配置 Citrix AutoDiscovery 服务。请联系 Citrix 技术支持寻求帮助。有关详细信息，请参阅请求 Windows 设备的 AutoDiscovery。
2. 选择并配置注册方法。请参阅支持的注册方法。
3. 配置 Windows 桌面和平板电脑设备策略。
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。

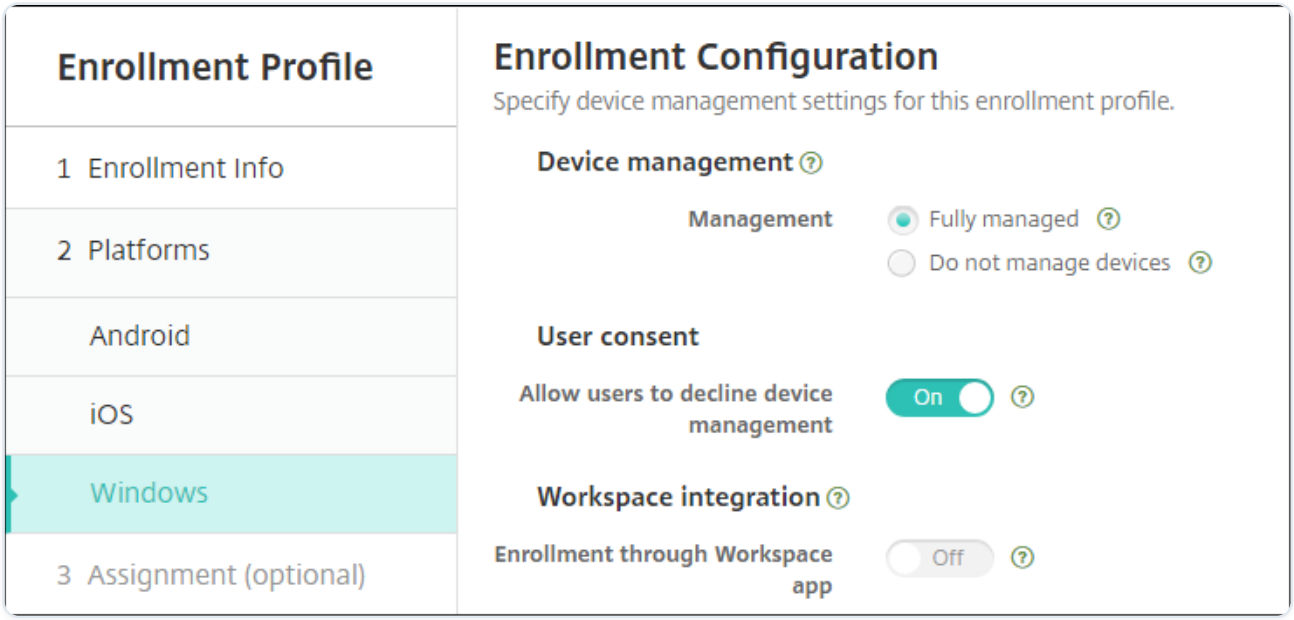
支持的注册方法

您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（无 MDM 注册）

要配置 Windows 10 和 Windows 11 设备的注册设置，请转至 **配置 > 注册配置文件 > Windows**。有关注册配置文件的更多信息，请参阅注册配置文件。



下表列出了 Citrix Endpoint Management 支持的 Windows 10 和 Windows 11 设备注册方法：

方法	受支持
Azure 活动目录注册	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 Citrix 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，请使用其他方法来简化用户的注册过程。
- 您无法向 Windows 设备发送注册邀请。Windows 用户直接通过其设备进行注册。

配置 Windows 桌面和平板电脑设备策略

使用这些策略配置 Citrix Endpoint Management 如何与运行 Windows 10 或 Windows 11 的桌面和平板设备交互。此表列出了适用于 Windows 桌面和平板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	防御者
设备防护	设备运行状况证明	交换
防火墙	信息亭	网络
办公	操作系统更新	密码
限制	商店	条款和条件
VPN	Web 剪辑	Windows 代理
Windows GPO 配置	Windows Hello 企业版	

通过 Azure Active Directory 注册 Windows 10 和 Windows 11 设备

> **重要提示：**

> 在用户注册之前，您必须在 Azure 中配置 Azure Active Directory (AD) 设置，然后配置 Citrix Endpoint Management。有关详细信息，请参阅将 Citrix 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。

您可以使用以下任一方法将 Windows 10 和 Windows 11 设备加入 Microsoft Azure AD：

- 对于公司拥有的设备：

  - 首次启动设备时，在将设备加入 Azure AD 时注册 MDM。在此场景中，用户按照本文所述完成注册：`<https://docs.microsoft.com/zh-cn/azure/active-directory/devices/azuread-joined-devices-frx>`。

    对于使用此方法注册的 Windows 设备，您可以使用 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。

  - 配置设备后，从 Windows 的“**设置**”页面将设备加入 Azure AD 时注册 MDM。在此场景中，用户按照配置设备后加入 Azure AD 时注册 MDM中所述完成注册。

- 对于个人设备（BYOD 或移动设备）：

  - 在将 Microsoft 工作帐户添加到 Windows 时注册到 Azure AD 时注册 MDM。在此场景中，用户按照注册到 Azure AD 时注册 MDM中所述完成注册。

配置设备后加入 Azure AD 时注册 MDM

1. 在设备上，从“开始”菜单导航到“**设置 > 帐户 > 访问工作或学校**”，然后单击“**连接**”。
2. 在“**设置工作或学校帐户**”对话框中，在“**备用操作**”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**”，则设备既不会加入 Azure AD，也不会注册到 Citrix Endpoint Management。

5. 单击“**加入**”以继续注册过程。
6. 单击“**完成**”以完成注册过程。

在注册到 Azure AD 时注册到 MDM

1. 在设备上，从“开始”菜单导航到“**设置 > 帐户 > 访问工作或学校**”，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。设备将注册到 Azure AD 并注册到 Citrix Endpoint Management。

   - 如果用户单击“**拒绝**”，设备将注册到 Azure AD，但不会注册到 Citrix Endpoint Management。帐户上没有“**信息**”按钮。

4. 单击“**加入**”以继续注册过程。
5. 单击“**完成**”以完成注册过程。

使用 AutoDiscovery 服务注册 Windows 设备

要为 Windows 设备配置 AutoDiscovery 服务，请请求 Citrix 技术支持以获取帮助。有关详细信息，请参阅请求 Windows 设备的 AutoDiscovery。

> **注意：**
>
> 对于要注册的 Windows 设备，SSL 侦听器证书必须是公共证书。自签名 SSL 证书的注册将失败。
>
> 用户执行以下步骤来完成注册：

1. 在设备上，从“开始”菜单导航到“**设置 > 帐户 > 访问工作或学校**”，然后单击“**仅注册到设备管理**”。
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**”。

   要以本地用户身份注册，请输入一个不存在但具有正确域名（例如，`foo@mydomain.com`）的电子邮件地址。此步骤允许用户绕过一个已知的 Microsoft 限制，即 Windows 上的内置设备管理执行注册。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。然后设备会找到 Citrix Endpoint Management 服务器并开始注册过程。
3. 输入凭据，然后单击“**继续**”。
4. 在**使用条款**对话框中，同意管理设备，然后单击**接受**。

如果域策略禁用 MDM 注册，则通过 AutoDiscovery 服务注册已加入域的 Windows 设备会失败。用户可以改用以下任一方法：

- 将设备从域中删除、注册，然后重新加入。
- 输入 Citrix Endpoint Management 服务器的 FQDN 以继续。

Windows 批量注册

通过 Windows 批量注册，您可以为 MDM 服务器设置许多设备进行管理，而无需重新映像设备。您可以使用预配包对 Windows 10 和 Windows 11 桌面和笔记本电脑设备进行批量注册。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。

定位	锁定	重新启动
吊销	选择性擦除	擦除

将 思杰端点管理 连接到 Azure 活动目录

Windows 10 和 Windows 11 设备可以注册到 Azure。在 Azure AD 中创建的用户可以访问这些设备。Citrix Endpoint Management 作为 MDM 服务部署在 Microsoft Azure 中。将 Citrix Endpoint Management 连接到 Azure AD 后，用户在将设备注册到 Azure AD 时，可以自动将其设备注册到 Citrix Endpoint Management。

要将 Citrix 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. 为应用程序提供一个名称，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 Citrix Endpoint Management 注册 FQDN 包含 cloud.com，请联系 Citrix 支持并向他们提供 Azure 中的 TXT 记录。Citrix 支持将验证子域，以便您可以继续配置。如果您的 FQDN 位于您自己的域下，则可以在 Azure 中正常验证它。
4. 选择您创建的应用程序，配置以下内容，然后单击**保存**。
   - **MDM 用户范围**。选择**所有**。
   - **MDM 使用条款 URL**。输入格式为 `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou`。
   - **MDM 发现 URL**。输入格式为 `https:// <Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe`。
5. 单击**本地 MDM 应用程序设置**。
   - 在**属性**窗格中，将 **APP ID URI** 设置为 `https:// < Citrix Endpoint Management Enrollment FQDN>:8443` 格式。此 App ID URI 是一个唯一 ID，不能在任何其他应用程序中再次使用。
   - 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**以查看密钥值。密钥值仅显示一次。保存密钥以备后用。您在步骤 7 中需要此密钥。
6. 在 Citrix Endpoint Management 控制台中，转到**设置 > 身份提供程序 (IDP)**，然后单击**添加**。

7. 在**发现 URL** 页面上，配置以下内容，然后单击**下一步**。
    - **IDP 名称**。输入一个唯一名称以标识您正在创建的 IdP 连接。
    - **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**时会看到它。
8. 在 **Windows MDM 信息**页面上，配置以下内容，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 的**属性**窗格中看到的应用程序 ID。
    - **密钥**。您在前面的步骤 4 中创建并保存的密钥值。
9. 在 **IDP 声明使用**页面上，配置以下内容，然后单击下一步。
    - **用户标识符类型**。选择 **userPrincipalName**。
    - **用户标识符字符串**。输入 `${id_token}.upn`。
10. 点击 **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. 创建一个条款和条件设备策略以及一个包含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) 无法进行 MDM 部署。仅使用 Citrix 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 Citrix Endpoint Management 管理更广泛的 Windows 操作系统。这种管理形式是配置 Windows GPO。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 桌面和平板电脑以配置特定应用程序。使用 Windows GPO 配置设备策略，您可以配置 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将 GPO 配置推送到其上，即使 Citrix Endpoint Management 不原生支持该设备。

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 Citrix 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**”列显示“**WEM**”。

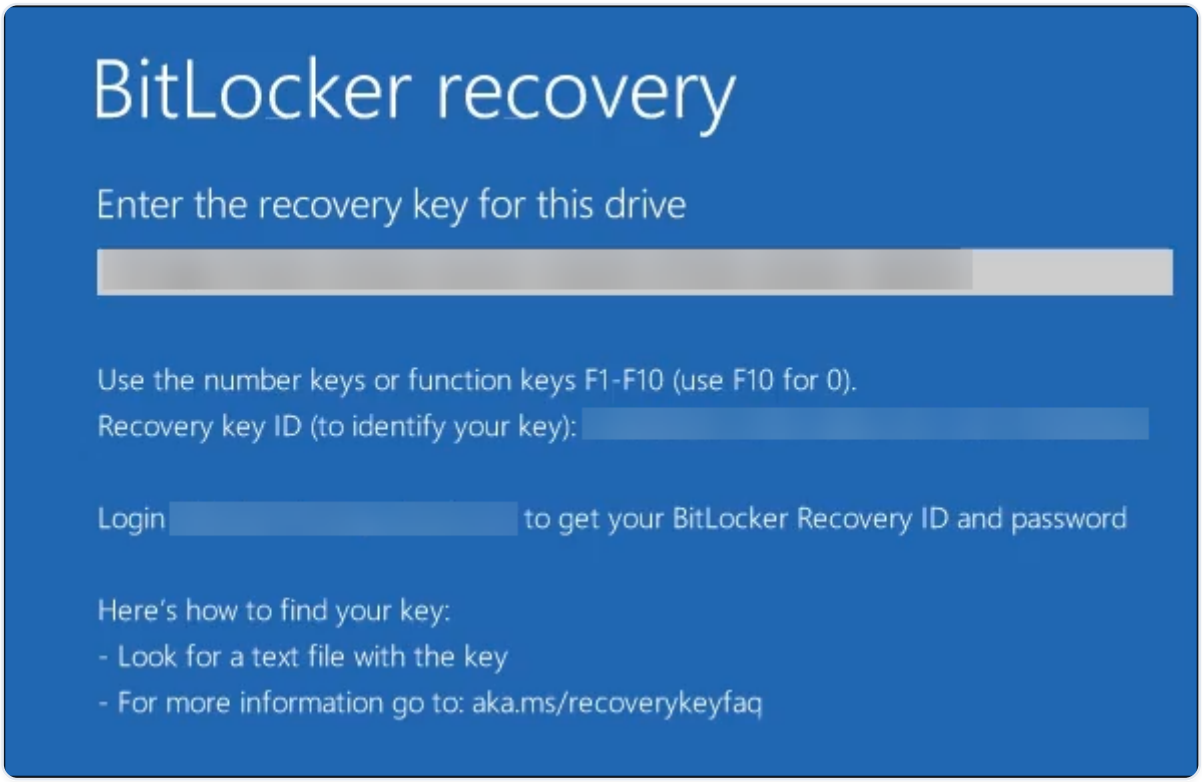
有关详细信息，请参阅 Windows GPO 配置设备策略。

BitLocker 恢复密钥

使用 BitLocker 加密磁盘是一项有用的安全功能。但是，如果用户丢失了 BitLocker 恢复密钥，解锁设备可能会很困难。Citrix 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上找到其 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 Citrix 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` 保持禁用状态。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 策略或创建一个新策略，然后启用“**将 BitLocker 恢复备份到 Citrix Endpoint Management**”设置。

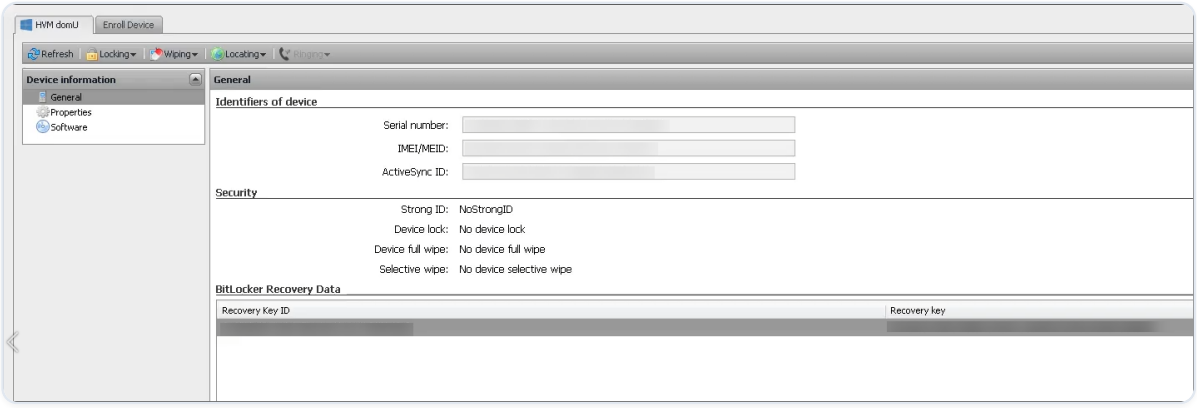
解锁设备时，最终用户会看到一条消息，要求他们输入密钥。该消息还会显示恢复密钥 ID。



要查找其 BitLocker 恢复密钥，用户请导航到自助服务门户。

1. 在“**常规**”详细信息下，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提供的密钥 ID 匹配。

- **恢复密钥：** 用户必须输入此密钥才能解锁其磁盘。在解锁提示符处输入此密钥。



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

Citrix Endpoint Management 支持批量注册 Windows 10 和 Windows 11 桌面设备及平板电脑。通过批量注册，您可以为 Citrix Endpoint Management 设置许多设备进行管理，而无需重新映像设备。您可以使用预配包进行批量注册。

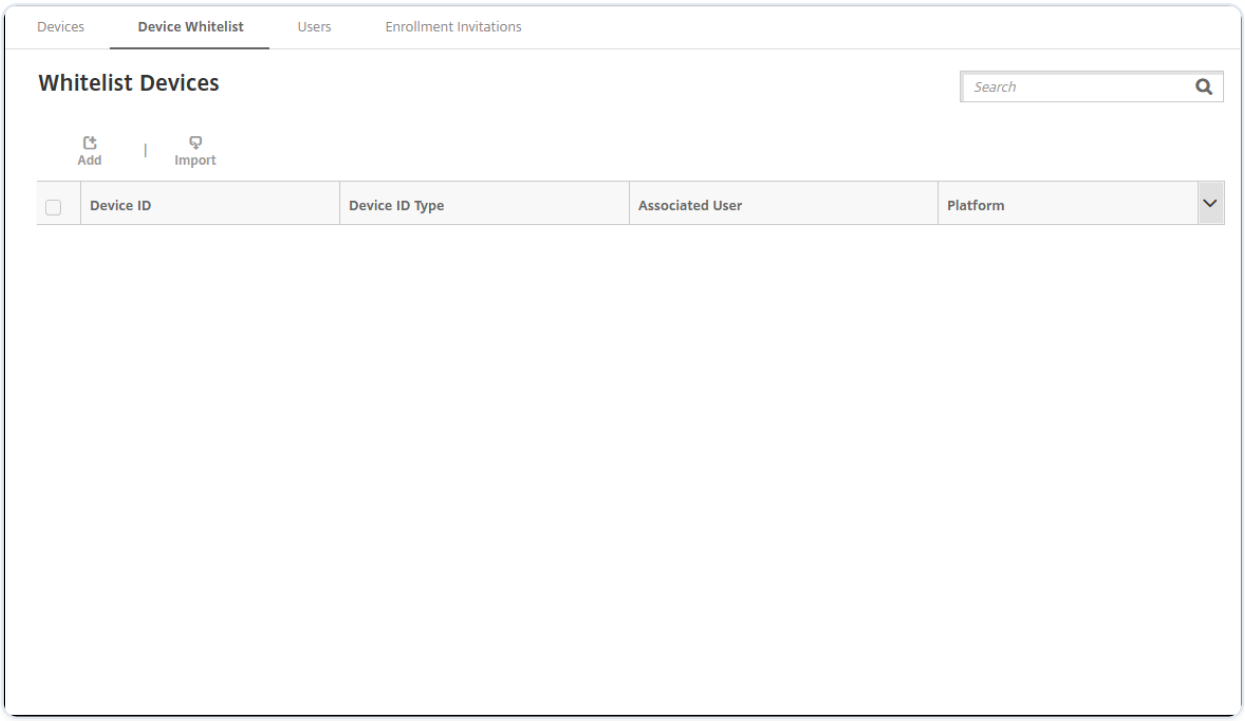
批量注册 Windows 10 和 Windows 11 设备的一般工作流程如下：

1. 分配设备。您可以按设备或批量分配设备。
2. 配置批量注册。
3. 创建预配包并将其应用于每台设备。

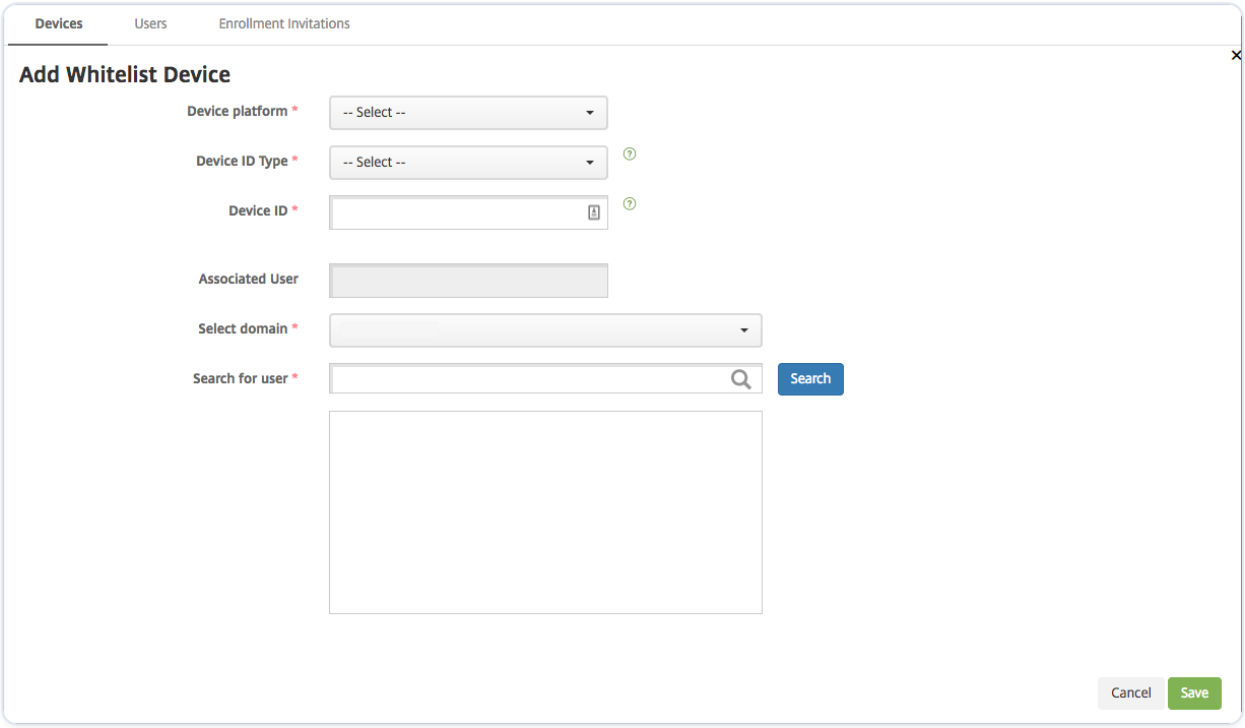
在运行批量注册之前，请确保将所有设备分配给正确的用户。通过按设备或批量添加设备来完成此分配。

按设备分配设备

1. 在 Citrix Endpoint Management 控制台中，导航到 **管理** > **设备** > **设备允许列表**。



2. 要添加每台设备，请单击 **添加**。



3. 键入以下信息：

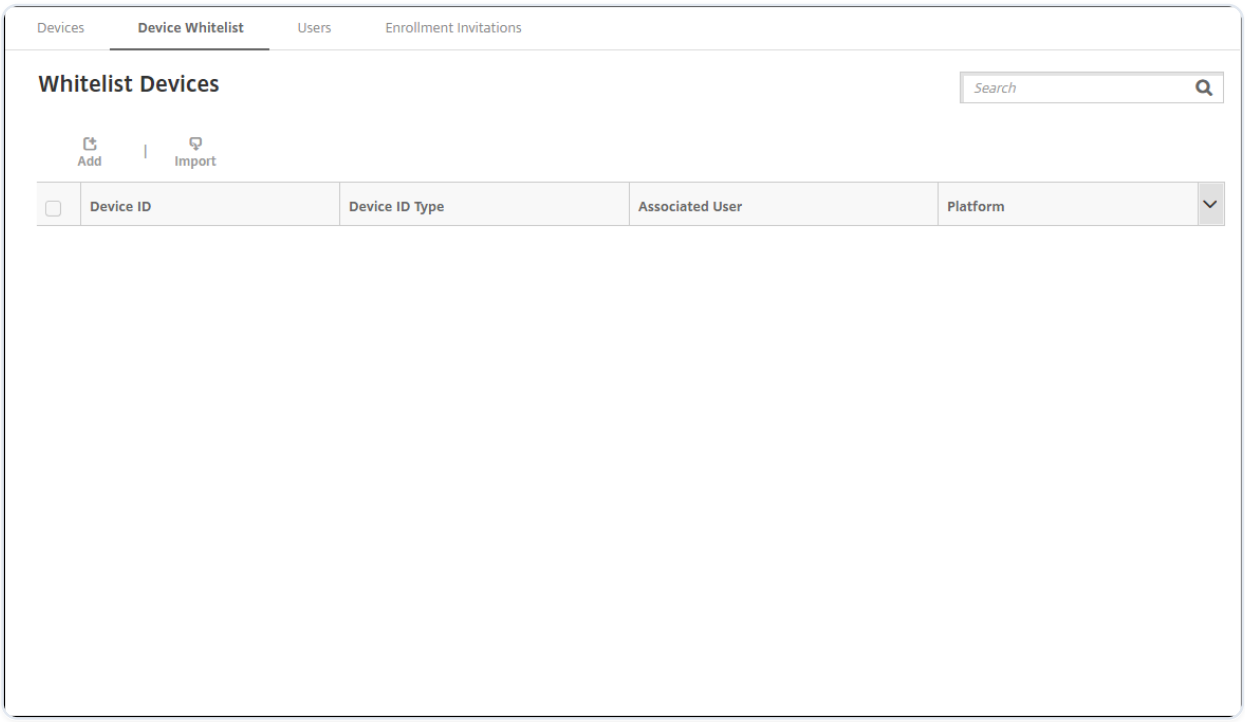
- **设备平台：** 选择 **Windows**。
- **设备 ID 类型：** 选择一个用于标识设备的 ID。Citrix Endpoint Management 支持 Windows 设备的 **硬件 ID** 和 **设备名称**。
- **设备 ID：** 输入与您之前为设备选择的类型对应的 ID。
- **关联用户：** 显示此设备的关联用户。此字段将自动填充您选择的用户。

- **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。

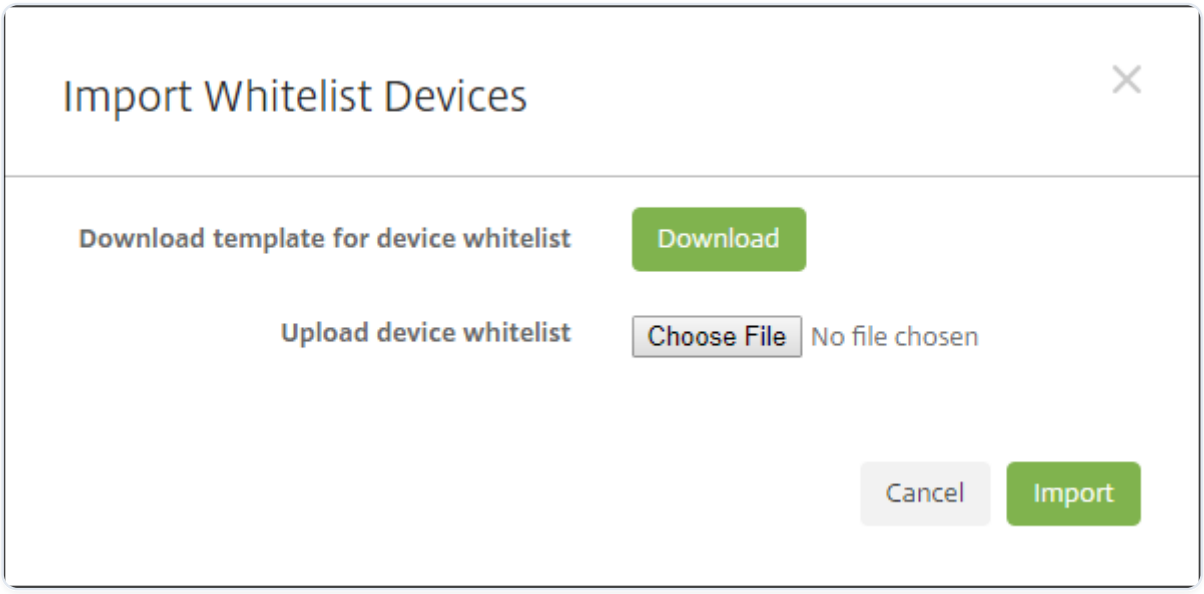
4. 点击 **保存**。

批量添加设备

1. 在 Citrix Endpoint Management 控制台中，导航到“**管理 > 设备 > 设备允许列表**”。



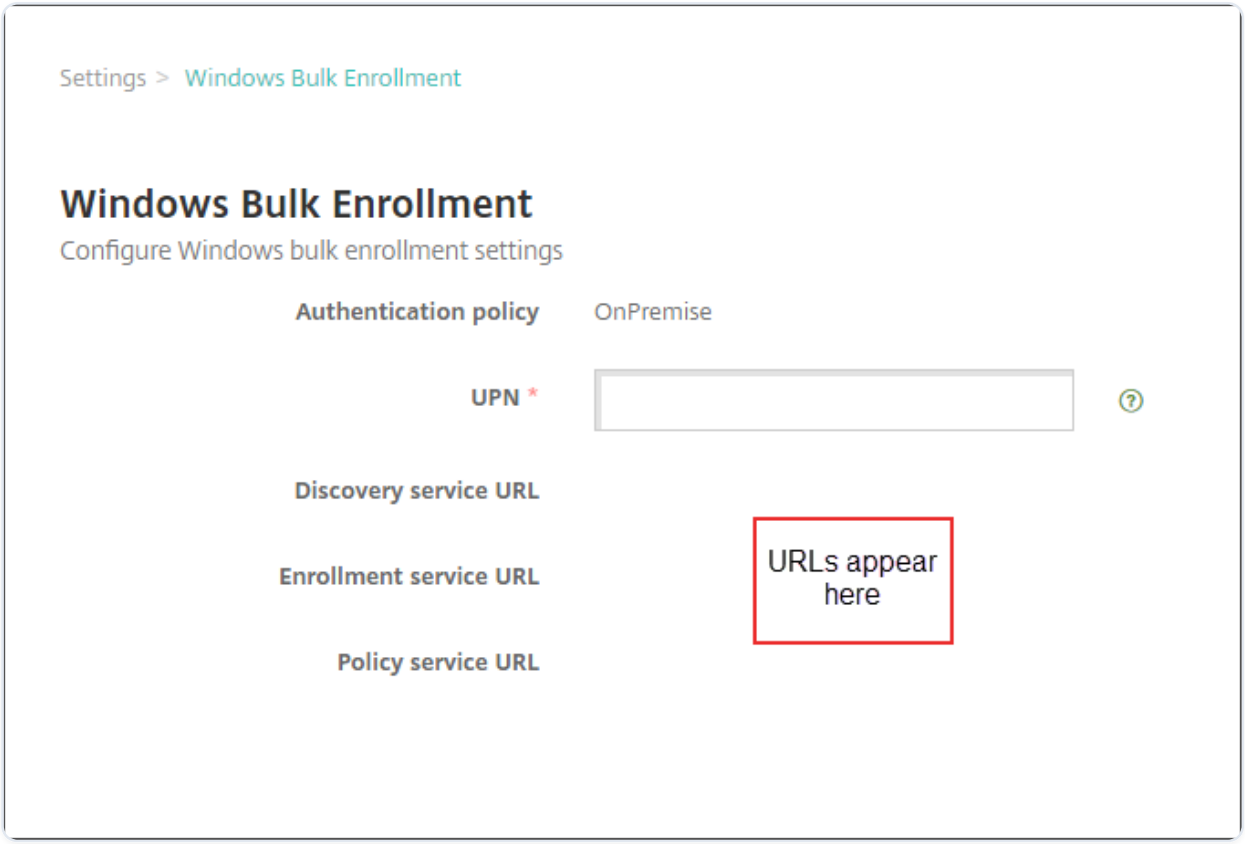
2. 单击 **Import**。



3. 单击“**下载**”以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**”上传该电子表格。

配置批量注册

1. 在 Citrix Endpoint Management 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 Citrix Endpoint Management 中具有注册权限的有效用户。您可以提供与您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，您需要这些 URL。

3. 点击 **保存**。

创建并应用预配包

要批量预配设备，请从 Microsoft Store 下载 Windows 配置设计器。Windows 配置设计器创建用于映像设备的预配包。作为这些包的一部分，您可以包含 Citrix Endpoint Management 批量注册配置设置，以便预配的设备自动注册到 Citrix Endpoint Management。

有关使用预配包的信息，请参阅 `<https://docs.microsoft.com/zh-cn/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool>`。请按照该文档中“*为本地身份验证创建并应用预配包*”部分所述的步骤操作。您需要按照这些步骤包含以下 Citrix Endpoint Management 批量注册配置设置，并将包应用于每个设备。

- **发现服务 URL**。

- **注册服务 URL**。
- **策略服务 URL**。
- **密钥**。UPN 的密码。您之前已在 UPN 字段中键入用户名。

开箱即用批量注册设备

Citrix Endpoint Management 支持开箱即用批量注册 Windows 设备。请按照以下步骤设置并执行批量注册：

1. 使用 Citrix Endpoint Management 控制台添加设备（按设备或批量）并配置批量注册。有关详细信息，请参阅批量添加设备 和配置批量注册。
2. 创建预配包，如创建并应用预配包 中所述。

   > **注意：**
   >
   > 创建预配包时，必须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 **Runtime settings > Accounts > ComputerAccount > ComputerName** 并指定设备名称。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. 将该预配包放入 USB 闪存盘。
4. 用户首次打开设备时，将 USB 闪存盘插入目标设备。

   Windows 设备会自动在 USB 闪存盘上找到预配包 (.ppkg)。有关详细说明，请参阅 Microsoft 文档中有关如何在初始设置期间应用预配包 的内容。

设备自动注册到 Citrix Endpoint Management。

对于运行 Windows 10（版本 2004 或更高版本）或 Windows 11 的设备，您可以通过仅创建一个预配包来简化注册过程。然后可以将该包应用于所有设备。因此，您不再需要为每台设备创建一个预配包。

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，将以下字符串作为设备名称的一部分包含在内：`%SERIAL%`。例如：`Surface-%SERIAL%`。该字符串将扩展为每台设备的 BIOS 序列号。

设备策略

您可以通过创建策略来配置 Citrix Endpoint Management 如何与您的设备交互。尽管许多策略对所有设备都通用，但每台设备都有一组特定于其操作系统的策略。因此，您可能会发现不同平台之间，甚至不同 Android 设备制造商之间存在差异。

要查看每个平台可用的策略：

1. 在 Citrix Endpoint Management 控制台中，转到 **配置 > 设备策略**。
2. 单击 **添加**。
3. 每个设备平台都会显示在“**策略平台**”窗格的列表中。如果该窗格未打开，请单击“**显示筛选器**”。
4. 要查看某个平台可用的所有策略列表，请选择该平台。要查看适用于多个平台的策略列表，请选择每个平台。只有当策略适用于所选的每个平台时，它才会显示在列表中。

筛选后的设备策略配置屏幕(/en-us/citrix-endpoint-management/media/policies-list-filtered.png)

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 Citrix Endpoint Management 设备策略时，请记住以下规则。如果一个或多个已注册设备上的策略发生冲突，则与 GPO 对齐的策略优先。

> 要查看 Android Enterprise 容器支持哪些策略，请参阅 Android Enterprise。

先决条件

- 创建您计划使用的任何交付组。
- 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. 命名并描述策略。

   > **重要提示：**
   >
   > 请勿在策略名称中使用正斜杠 (/)。否则，以后编辑策略时可能会发生错误。

2. 为一个或多个平台配置策略。
3. 创建部署规则（可选）。
4. 将策略分配给交付组。
5. 配置部署计划（可选）。

要创建和管理设备策略，请转至 **配置 > 设备策略**。

设备策略配置屏幕(/en-us/citrix-endpoint-management/media/configure-device-policies-unfiltered.png)

要添加策略：

1. 在 **设备策略** 页面上，单击 **添加**。此时将显示 **添加新策略** 页面。

   设备策略配置屏幕(/en-us/citrix-endpoint-management/media/configure-device-policies-add.png)

2. 单击一个或多个平台以查看所选平台的设备策略列表。单击策略名称以继续添加策略。

   设备策略配置屏幕(/en-us/citrix-endpoint-management/media/configure-device-policies-add-filtered.png)

   您也可以在搜索框中键入策略名称。键入时，将显示潜在匹配项。如果您的策略在列表中，请单击它。只有您选择的策略会保留在结果中。单击它以打开该策略的 **策略信息** 页面。

3. 选择要包含在策略中的平台。所选平台的配置页面将显示在步骤 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策略。此页面对所有策略都类似。
5. 完成平台页面。平台页面会显示您在步骤 3 中选择的每个平台。这些页面因策略而异。策略在不同平台之间可能有所不同。并非所有策略都适用于所有平台。

某些页面包含项目表。要删除现有项目，请将鼠标悬停在包含该列表的行上，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该列表的行上，然后单击右侧的笔形图标。

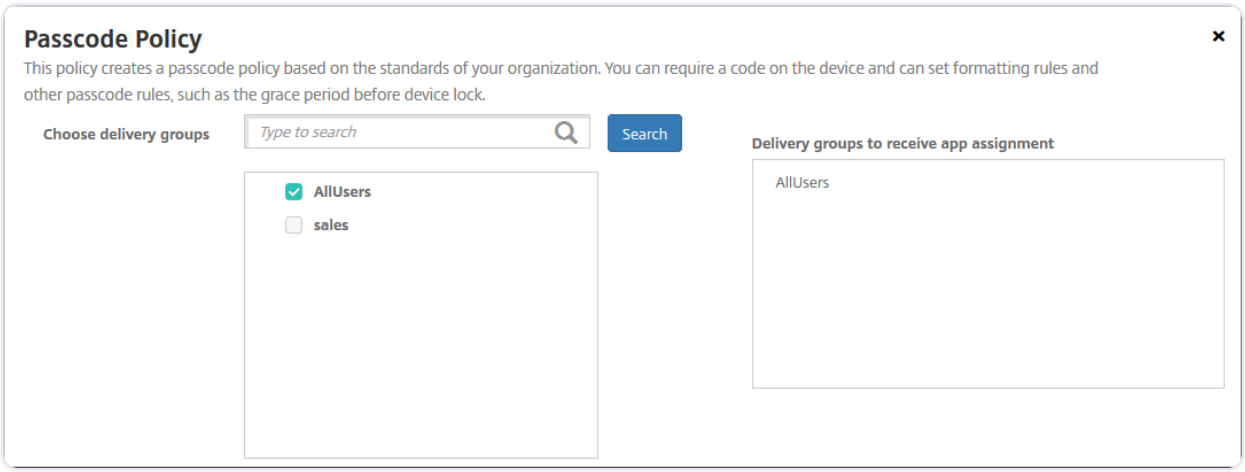
配置部署规则、分配和计划

有关配置部署规则的更多信息，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。默认显示**基本**选项卡。
   - 在列表中，单击选项以指定部署条件。您可以选择在满足所有条件时或满足任何条件时部署策略。默认选项设置为**所有**。
   - 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**。
   - 如果要添加更多条件，请再次单击**新建规则**。您可以添加任意数量的条件。
2. 单击**高级**选项卡以使用布尔选项组合规则。您在**基本**选项卡上选择的条件将显示。
3. 您可以使用更高级的布尔逻辑来组合、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 (+) 将条件添加到规则。

     随时可以单击以选择条件，然后单击“**编辑**”或“**删除**”。
   - 单击“**新建规则**”以添加另一个条件。
4. 单击“**下一步**”以转到下一个平台页面，或者在所有平台页面都完成后，转到“**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，该组将显示在“**接收应用程序分配的交付组**”框中。

   只有在选择交付组后，“**接收应用程序分配的交付组**”才会显示。



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。默认选项设置为“**开**”。
   - 在“**部署计划**”旁边，单击“**立即**”或“**稍后**”。默认选项设置为“**立即**”。
   - 如果单击“**稍后**”，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“**仅当上次部署失败时**”。默认选项设置为“**每次连接时**”。
   - 在“**为始终连接部署**”旁边，单击“**开**”或“**关**”。默认选项设置为“**关**”。

   > **注意：**
   >
   > 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。
   >
   > 始终连接选项：
   >
   > - 不适用于 iOS 设备
   > - 不适用于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户
   > - 不建议从版本 10.18.19 之前开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户使用 您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但**部署用于始终在线连接**除外。

   设备策略配置屏幕(/en-us/citrix-endpoint-management/media/deployment-schedule.png)

7. 点击 **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。

- 安卓

  要从 Android 设备中删除设备策略，请使用 Citrix Endpoint Management 卸载设备策略。有关信息，请参阅Citrix 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，所有策略都是 MDM 配置文件的一部分。因此，您可以为要删除的策略创建配置文件删除设备策略。其余策略和配置文件将保留在设备上。有关详细信息，请参阅配置文件删除设备策略。

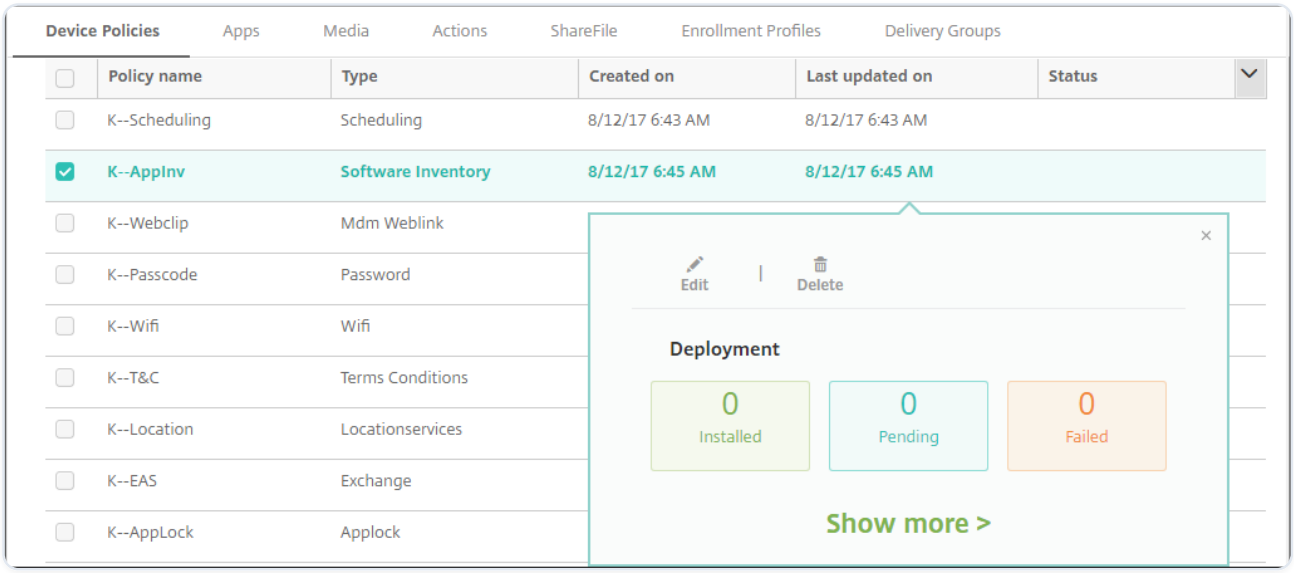
- Windows 10 系统和 Windows 11 系统

  您无法直接从 Windows 桌面或平板电脑设备中删除设备策略。但是，您可以使用以下任一方法：

  - 取消注册设备，然后将一组新策略推送到设备。用户随后重新注册以继续。
  - 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公司应用程序和数据。然后，从仅包含该设备的交付组中删除设备策略，并将该交付组推送到设备。用户随后重新注册以继续。

编辑设备策略

要编辑策略，请选择策略旁边的复选框。选项菜单将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。



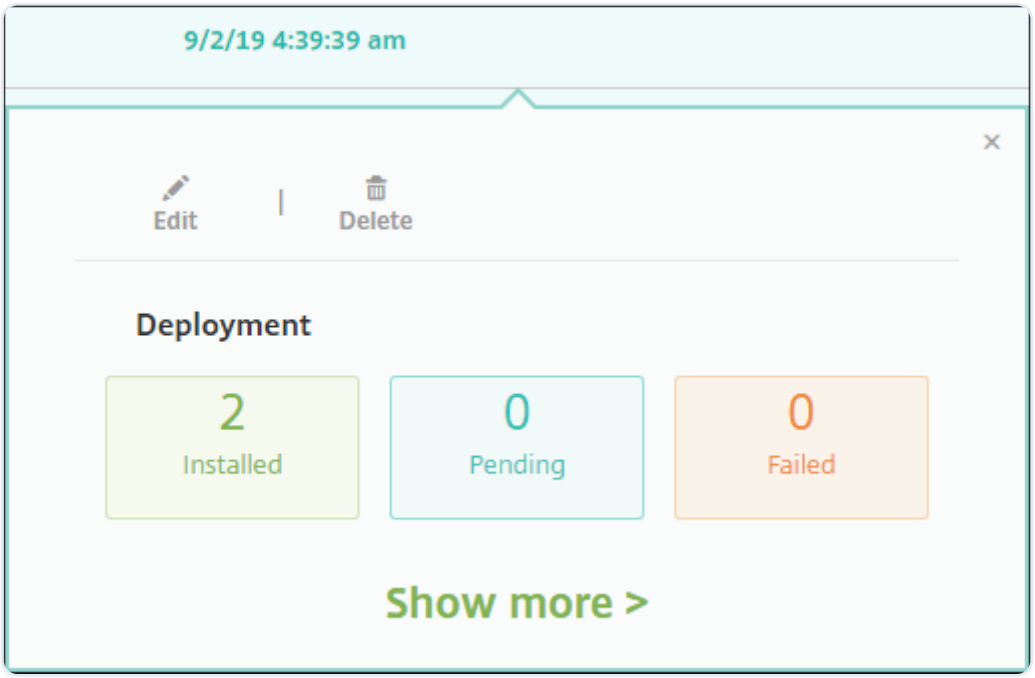
要查看策略详细信息，请单击“**显示更多**”。

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

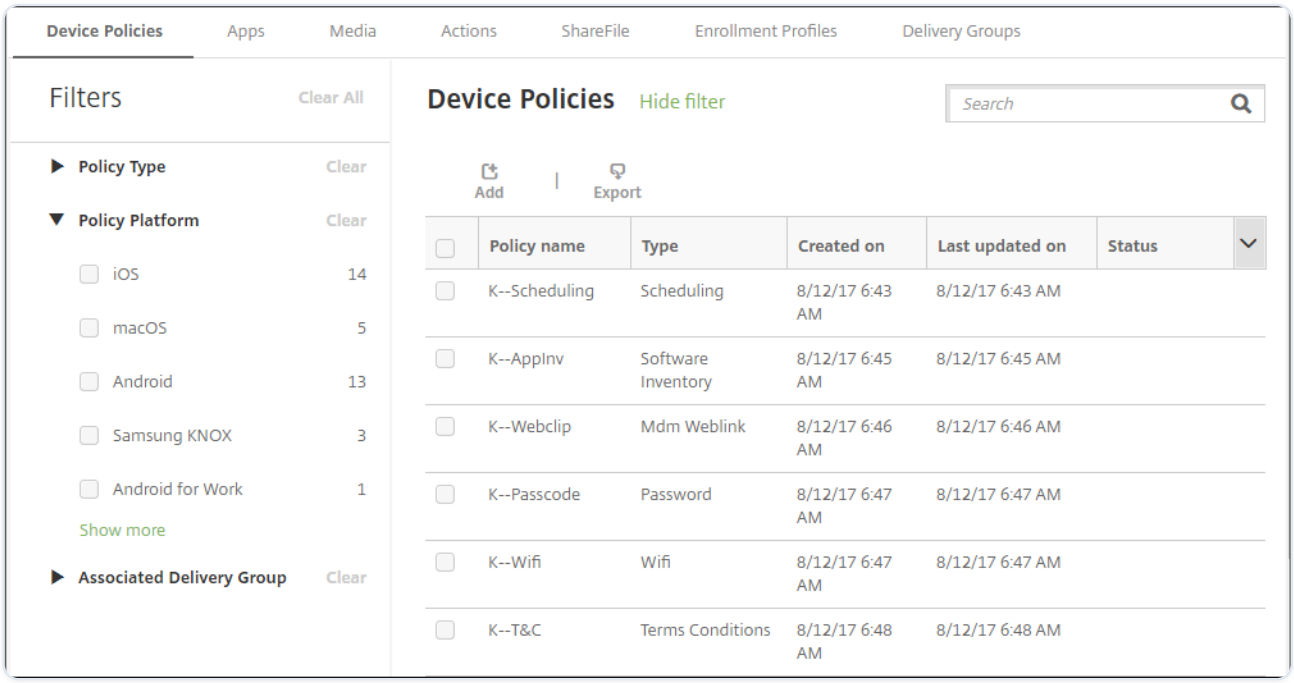
在“**配置 > 设备策略**”页面上单击策略行以检查其部署状态。



当策略部署处于待定状态时，用户可以通过点击“**首选项 > 设备信息 > 刷新策略**”从 Citrix Secure Hub 刷新策略。

筛选已添加的设备策略列表

您可以按策略类型、平台和关联的交付组筛选已添加的策略列表。在“**配置 > 设备策略**”页面上，单击“**显示筛选器**”。在列表中，选择要查看的项目的复选框。



单击“**保存此视图**”以保存筛选器。筛选器的名称将显示在“**保存此视图**”按钮下方的按钮中。

设备策略摘要

设备策略名称	设备策略描述
AirPlay 镜像	将特定的 AirPlay 设备（例如 Apple TV 或另一台 Mac 电脑）添加到 iOS 设备。您还可以将设备添加到受监管设备的允许列表中。该选项将用户限制为只能使用允许列表中的 AirPlay 设备。
AirPrint	将 AirPrint 打印机添加到 iOS 设备上的 AirPrint 打印机列表。此策略使得在打印机和设备位于不同子网的环境中提供支持变得更加容易。
APN	确定用于将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 的设置。大多数新手机中已定义此设置。如果您的组织不使用消费者 APN 从移动设备连接到互联网，请使用此策略。

设备策略名称	设备策略描述
应用程序访问	定义设备上必需、可选或禁止的应用程序列表。然后，您可以创建自动化操作，以响应设备对该应用程序列表的合规性。
应用程序属性	为 iOS 设备指定属性，例如托管应用程序捆绑包 ID 或每应用 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，您可以将 XML 配置文件（称为属性列表或 `plist`）部署到 iOS 设备。或者，您可以将键/值对部署到 Windows 10 桌面或平板设备。
应用程序清单	收集托管设备上的应用程序清单。Citrix Endpoint Management 然后将该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。通过这种方式，您可以检测应用程序访问允许列表或阻止列表中的应用程序，然后采取正确的措施。
应用程序锁定	定义用户可以在 iOS 或某些 Android 设备上运行或无法运行的应用程序列表。可以将 iPad 变成信息亭。
应用程序权限	配置工作配置文件中对 Android Enterprise 应用程序的请求如何处理 Google 所谓的“危险”权限。
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	仅适用于 Microsoft Edge 浏览器，此策略指定 Windows Defender 应用程序防护设置。这些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 用户如何接收来自指定应用程序的通知。
自动更新托管应用程序	控制已安装的托管应用程序如何在 Android Enterprise 设备上更新。

设备策略名称	设备策略描述
BitLocker	配置 Windows 10 和 Windows 11 设备上 BitLocker 界面中可用的设置。
蓝牙	启用或禁用 iOS 设备上的蓝牙。
浏览器	定义用户设备是否可以使用浏览器，或者设备可以使用哪些浏览器功能。
日历 (CalDAV)	将日历 (CalDAV) 帐户添加到 iOS 或 macOS 设备。CalDAV 帐户使用户能够将日程安排数据与任何支持 CalDAV 的服务器同步。
蜂窝网络	配置蜂窝网络设置。
连接计划	Android 设备连接回 Citrix Endpoint Management 以进行 MDM 管理、应用程序推送和策略部署所需。如果您不将此策略发送到设备且不启用 Google FCM，则设备无法连接回服务器。
联系人 (CardDAV)	将 iOS 联系人 (CardDAV) 帐户添加到 iOS 或 macOS 设备。CardDAV 帐户使用户能够将联系人数据与任何支持 CardDAV 的服务器同步。
凭据	在 Citrix Endpoint Management 中启用与 PKI 配置的集成身份验证。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。
防御者	配置 Windows 10 和 Windows 11 桌面版及平板电脑版的 Windows Defender 设置。
设备防护	启用安全功能，例如安全启动、UEFI 锁定和虚拟化。
设备健康证明	要求 Windows 10 和 Windows 11 设备报告其健康状况。为此，它们会将特定数据和运行时信息发送到健康证明服务 (HAS) 进行分析。HAS 会创建并返回一个健康证明证书，设备随后会将其发送到 Citrix Endpoint Management。

设备策略名称	设备策略描述
	当 Citrix Endpoint Management 收到健康证明证书时，它会根据该证书的内容部署您配置的自动操作。
设备名称	设置 iOS 和 macOS 设备上的名称，以便您可以识别这些设备。您可以使用宏、文本或两者的组合来定义设备名称。
教育配置	配置教师和学生设备以与 Apple Education 配合使用。如果教师使用 Classroom 应用，则需要教育配置设备策略。支持 iOS (iPadOS) 设备。
思杰端点管理选项	配置从 Android 设备连接到 Citrix Endpoint Management 时 Citrix Secure Hub 的行为。
Citrix 端点管理 卸载	从 Android 设备卸载 Citrix Endpoint Management。部署后，此策略会从部署组中的所有设备中移除 Citrix Endpoint Management。
Exchange 策略	为设备上的本机电子邮件客户端启用 ActiveSync 电子邮件。
文件	将脚本文件添加到 Citrix Endpoint Management，这些文件为用户执行特定功能。或者，您可以添加文档文件，供 Android 设备用户在其设备上访问。添加文件时，您还可以指定希望文件存储在设备上的目录。
FileVault	此策略允许您在已注册的 macOS 设备上启用 FileVault 设备加密。您还可以控制用户在登录期间跳过 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。您提供要在设备上允许或阻止的 IP 地址、端口和主机名。您还可以配置代理和代理重新路由设置。
字体	将字体添加到 iOS 和 macOS 设备。字体必须是 TrueType (.TTF) 或 OpenType (.OFT) 字体。Citrix Endpoint Management 不支持字体集合 (.TTC, .OTC)。

设备策略名称	设备策略描述
主屏幕布局	指定受监管 iOS 设备上 iOS 主屏幕的应用程序和文件夹布局。
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 Citrix Endpoint Management。该文件包含您使用 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挑战键盘锁之前可用的功能。您还可以控制完全托管和专用设备的设备键盘锁功能。例如，您可以禁用锁屏功能，如指纹解锁、信任代理和通知。
诺克斯企业平台密钥	允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息。
启动器配置	指定 Android 设备上 Citrix Launcher 的设置，例如允许的应用程序和启动器图标的自定义徽标图像。
LDAP	提供用于 iOS 设备的 LDAP 服务器信息，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，前提是设备已为 Citrix Secure Hub 启用 GPS。将此策略部署到设备后，您可以从 Citrix Endpoint Management 发送定位命令。然后，设备会响应其位置坐标。Citrix Endpoint Management 还支持地理围栏和跟踪策略。
锁屏消息	设置在以下设备丢失时显示的消息：共享 iPad 的登录窗口和受监督 iOS 设备的锁屏。
邮件	在 iOS 或 macOS 设备上配置电子邮件帐户。
托管配置	控制 Android Enterprise 设备的各种应用程序配置选项和应用程序限制。

设备策略名称	设备策略描述
托管域	定义适用于电子邮件和 Safari 浏览器的托管域。托管域通过控制哪些应用程序可以打开使用 Safari 从域下载的文档来帮助您保护公司数据。对于受监督的 iOS 设备，您可以指定 URL 或子域来控制用户如何从浏览器打开文档、附件和下载。
最大常驻用户数	指定共享 iPad 的最大用户数。支持 iOS 和 iPadOS 设备。
MDM 选项	管理受监管 iOS 设备上的“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，以指定托管应用如何在 iOS 设备上使用网络（例如蜂窝数据网络）。这些规则仅适用于托管应用。托管应用是通过 Citrix Endpoint Management 部署到用户设备的应用。
办公	将 Microsoft Office 应用部署到运行 Windows 10（版本 1709 或更高版本）或 Windows 11 的任何设备。
组织信息	指定 Citrix Endpoint Management 部署到 iOS 设备的警报消息的组织信息。
操作系统更新	将最新的操作系统更新部署到受支持和受监管的设备。
密码	在托管设备上强制执行 PIN 码或密码。您可以设置设备上密码的复杂性和超时。
密码锁定宽限期	指定共享 iPad 屏幕在用户必须输入密码才能解锁屏幕之前保持锁定的分钟数。支持 iOS 和 iPadOS 设备。

设备策略名称	设备策略描述
个人热点	允许用户在不在 Wi-Fi 网络范围内时连接到互联网。用户通过其 iOS 设备上的蜂窝数据连接，使用个人热点功能进行连接。
配置文件移除	从 macOS 设备中移除应用程序配置文件。
预置配置文件	指定要发送到设备的企业分发预置配置文件。当您开发和代码签名 iOS 企业应用程序时，通常会包含一个预置配置文件。Apple 要求该配置文件才能使应用程序在 iOS 设备上运行。如果预置配置文件丢失或已过期，则当用户点击打开应用程序时，应用程序会崩溃。
预置配置文件移除	移除 iOS 预置配置文件。
代理	指定运行 iOS 的设备的全局 HTTP 代理设置。每台设备只能部署一个全局 HTTP 代理策略。
限制	提供数百种选项来锁定和控制托管设备上的功能。限制选项的示例包括：禁用摄像头或麦克风、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	配置是否允许 iOS 设备上的语音和数据漫游。如果禁用语音漫游，则数据漫游会自动禁用。
Samsung MDM 许可证密钥	指定必须部署到设备的内置 Samsung 企业许可证管理 (ELM) 密钥。Citrix Endpoint Management 还支持 Samsung 企业空中固件 (E-FOTA) 服务。
SCEP	配置 iOS 和 macOS 设备以从外部 SCEP 服务器检索证书。您还可以使用 SCEP 从连接到 Citrix 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。
单点登录 (SSO) 帐户	创建 SSO 帐户，以便用户只需登录一次即可访问 Citrix Endpoint Management 和您的内部公司资源。用户无需在设备上存储任何凭据。Citrix Endpoint Management 将企业用户凭据用于跨应用程序（包括 App Store 中的应用程

设备策略名称	设备策略描述
	序）的 SSO 帐户。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，此策略会阻止用户在其设备上使用存储卡。
商店	指定应用程序商店 Web 剪辑是否显示在用户设备的主屏幕上。
订阅的日历	将订阅的日历添加到 iOS 设备上的日历列表。请确保在将其添加到用户设备上的订阅日历列表之前订阅日历。
条款和条件	要求用户接受贵公司管理公司网络连接的特定策略。当用户使用 Citrix Endpoint Management 注册其设备时，他们必须接受条款和条件才能注册其设备。拒绝条款和条件将取消注册过程。
隧道	定义任何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。
VPN	提供对使用传统 VPN 网关技术的后端系统的访问。此策略提供可部署到设备的 VPN 网关连接详细信息。Citrix Endpoint Management 支持多种 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 并启用按需 VPN。
壁纸	添加 .png 或 .jpg 文件以在 iOS 设备的锁定屏幕、主屏幕或两者上设置壁纸。要在 iPad 和 iPhone 上使用不同的壁纸，请创建不同的壁纸策略并将其部署给相应的用户。
Web 剪辑	将网站快捷方式或 Web 剪辑放置在用户设备上，使其与应用程序一起显示。您可以为 iOS、macOS 和 Android 设备的 Web 剪辑指定自己的图标。Windows 平板电脑仅需要标签和 URL。

设备策略名称	设备策略描述
Web 内容筛选器	筛选 iOS 设备上的 Web 内容。Citrix Endpoint Management 使用 Apple 自动筛选功能以及您添加到允许列表和阻止列表的站点。仅适用于受监管的 iOS 设备。
Windows 代理	启用此策略可在 Windows 台式机和平板电脑上运行上传的 PowerShell 脚本。
Windows GPO 配置	为 Citrix Workspace Environment Management 支持的任何 Windows 设备配置组策略对象 (GPO)。
适用于企业的 Windows Hello	启用此 Windows 功能，以便用户可以在其设备上预配适用于企业的 Windows Hello。此策略还允许您配置密码限制和其他安全功能。

按平台划分的设备策略

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
AirPlay 镜像设备策略	X	X				
AirPrint 设备策略	X					
APN 设备策略	X			X		
应用访问设备策略	X			X		
应用属性设备策略	X					
应用配置设备策略	X				X	

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
应用清单设备策略	X	X	X	X	X	
应用锁定设备策略	X			X	X	
应用权限设备策略			X			
应用卸载设备策略	X	X	X	X		
应用卸载限制设备策略						X
应用程序防护设备策略					X	
应用通知设备策略	X					
自动更新托管应用			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				

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
蜂窝设备策略	X					
连接计划设备策略			X	X		
联系人 (CardDAV) 设备策略	X	X				
将应用复制到 Samsung 容器设备策略						X
凭据设备策略	X	X	X	X	X	
自定义 XML 设备策略			X		X	
Defender 设备策略					X	
设备防护设备策略					X	
设备健康证明设备策略					X	
设备名称设备策略	X	X				
教育配置设备策略	X					

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
Citrix Endpoint Management 选项设备策略			X	X		
Citrix Endpoint Management 卸载设备策略				X		
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	X	X				

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
配置文件设备策略						
锁屏管理设备策略			X			
自助服务终端设备策略			X		X	
启动器配置设备策略			X	X		
LDAP 设备策略	X	X				
位置设备策略	X		X	X		
锁屏消息设备策略	X					
邮件设备策略	X	X				
托管配置设备策略			X			
托管域设备策略	X					
最大驻留用户设备策略	X					
MDM 选项设备策略	X					

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
网络设备策略	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	
密码设备策略	X	X	X	X	X	
密码锁定宽限期设备策略	X					
个人热点设备策略	X					
配置文件删除设备策略	X	X				
预置配置文件设备策略	X					
预置配置文件删除设备策略	X					

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
代理设备策略	X					
限制设备策略	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	
订阅日历设备策略	X					
条款和条件设备策略	X			X	X	
隧道设备策略				X		

策略	IOS	MACOS	ANDROID 企业版	ANDROID (旧版设备管理员)	WINDOWS 桌面电脑和平板电脑	其他
VPN设备策略	X	X		X	X	
壁纸设备策略	X					
Web剪辑设备策略	X	X		X	X	
Web内容筛选器设备策略	X					
Windows代理设备策略					X	
Windows GPO配置设备策略					X	
适用于企业的Windows Hello设备策略					X	

AirPlay 镜像设备策略

Apple AirPlay 功能允许用户通过 Apple TV 将内容从 iOS 设备无线传输到电视屏幕，或者将设备显示屏上的内容精确镜像到电视屏幕或另一台 Mac 电脑。

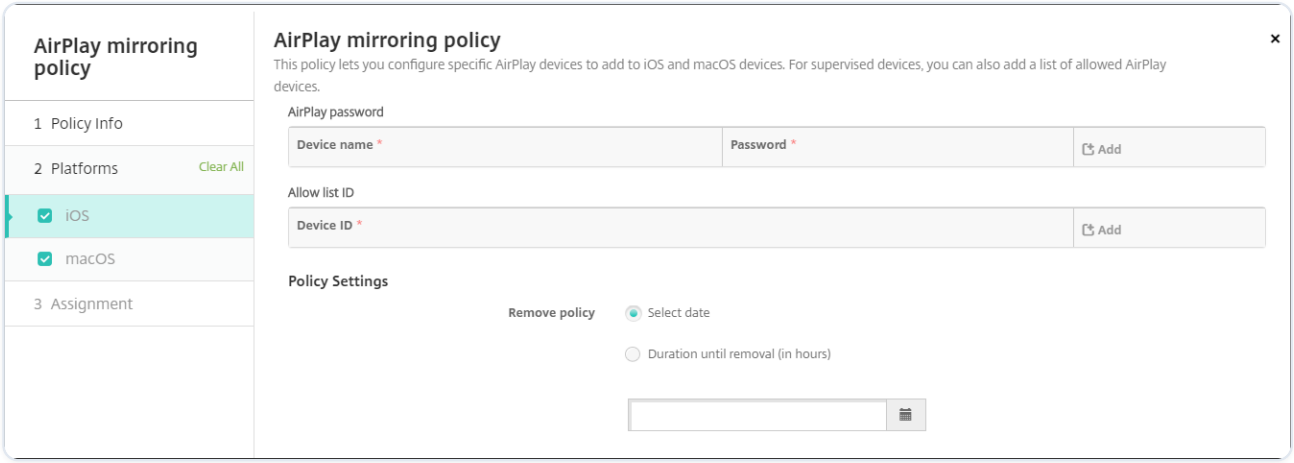
您可以在 Citrix Endpoint Management 中添加设备策略，以将特定的 AirPlay 设备（例如 Apple TV 或另一台 Mac 电脑）添加到 iOS 设备。您还可以选择将设备添加到受监管设备的允许列表，这将用户限制为只能使用这些 AirPlay 设备。有关将设备置于受监管模式的信息，请参阅使用 Apple Configurator 2 部署设备。

> **注意：**

> 在继续操作之前，请务必准备好要添加的所有设备的设备 ID 和所有密码。

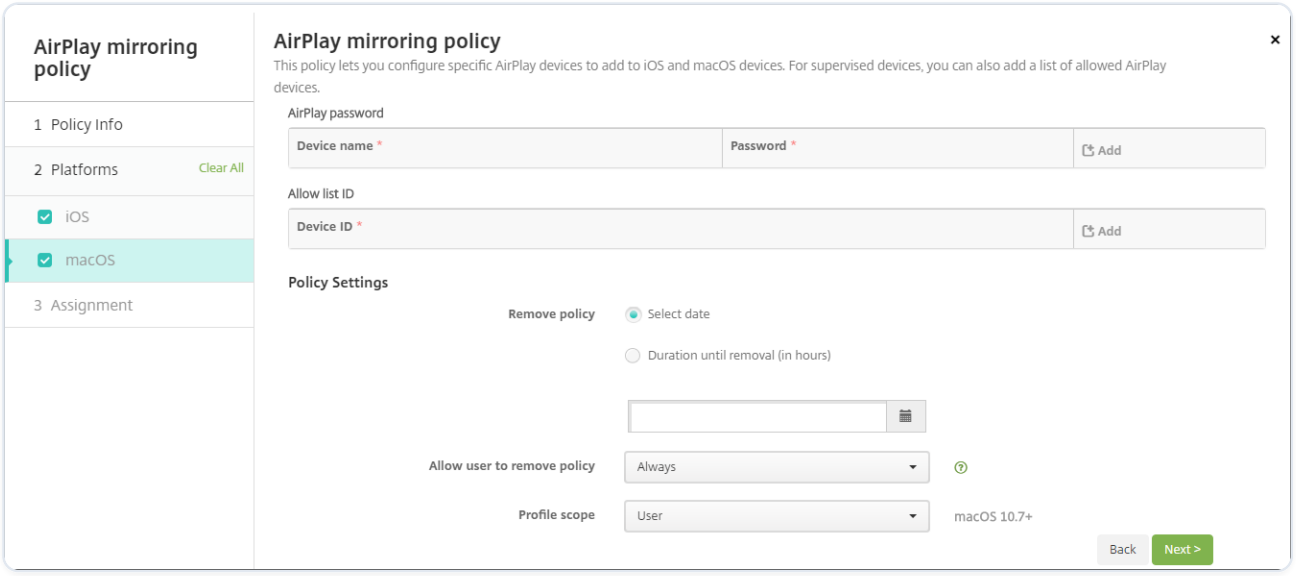
> 要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置



- **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：** 输入设备的选填密码。
  - 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：** 对于非受监管设备，此列表将被忽略。此列表中的设备 ID 是用户设备唯一可用的 AirPlay 设备。对于要添加到列表中的每个 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**
  - **移除策略：** 选择策略移除的计划方法。可用选项为 **选择日期** 和 **移除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 输入一个数字（以小时为单位），直到策略移除发生。

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：** 对于非受管设备，此列表将被忽略。此列表中的设备 ID 是用户设备可用的唯一 AirPlay 设备。对于要添加到列表中的每个 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**
  - **移除策略：** 选择策略移除的计划方法。可用选项为 **选择日期** 和 **移除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 输入一个数字（以小时为单位），直到策略被移除。
  - **允许用户移除策略：** 您可以选择用户何时可以从其设备中移除策略。从菜单中选择**始终**、**需要密码**或**从不**。如果选择**需要密码**，请在**移除密码**字段中输入密码。
  - **配置文件范围：** 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 macOS 10.7 及更高版本。

AirPrint 设备策略

AirPrint 设备策略将 AirPrint 打印机添加到 iOS 设备上的 AirPrint 打印机列表。此策略使得支持打印机和设备位于不同子网的环境变得更加容易。

> **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：** 对于要添加的每个 AirPrint 目标，请单击**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。此值对应于 `_ipps.tcp` Bonjour 记录的参数。例如，`printers/Canon_MG5300_series` 或 `printers/Xerox_Phaser_7600`。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 输入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 或更高版本。

应用权限设备策略

对于工作配置文件中的 Android Enterprise 应用程序：您可以配置这些应用程序的请求如何处理 Google 所谓的“危险”权限。您可以控制是否提示用户授予或拒绝来自应用程序的权限请求。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：

- 授予应用程序访问涉及用户私人信息的数据或资源的权限。
- 或者，可能会影响用户的存储数据或其他应用程序的操作。例如，读取用户联系人的能力就是一种危险权限。

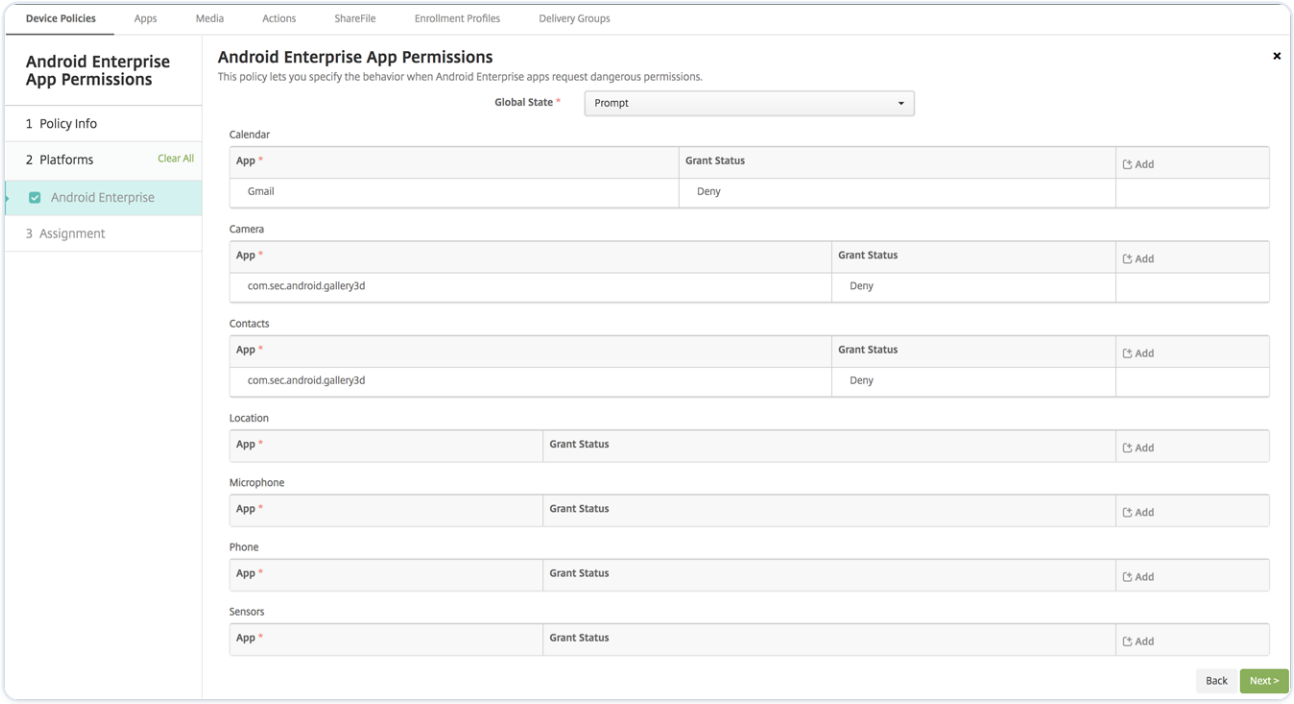
您可以配置一个全局状态来控制所有危险权限请求的行为。此配置的范围是工作配置文件中的 Android Enterprise 应用程序。您还可以为每个应用程序控制单个权限组（由 Google 定义）的危险权限请求行为。这些单独的设置会覆盖全局状态。

有关 Google 如何定义权限组的信息，请参阅 Android 开发者指南。

默认情况下，系统会提示用户授予或拒绝危险权限请求。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

安卓企业版设置



- **全局状态：** 控制所有危险权限请求的行为。在列表中，单击 **提示**、**授予** 或 **拒绝**。
  - **提示：** 系统会提示用户授予或拒绝危险权限请求。
  - **授予：** 所有危险权限请求都将获得授予。系统不会提示用户。
  - **拒绝：** 所有危险权限请求都将被拒绝。系统不会提示用户。

  默认是 **提示**。
- 为每个应用、每个权限组设置单独的行为。要配置权限组的行为：单击 **添加**。然后在 **应用** 下，从列表中选择一个应用。如果您配置 Android Enterprise 系统应用，请单击 **添加新应用** 并输入您在限制设备策略中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**。此授予状态将覆盖全局状态。
  - **提示：** 系统会提示用户授予或拒绝此应用在此权限组中的危险权限请求。
  - **授予：** 此应用在此权限组中的危险权限请求已授予。不会提示用户。

> **注意：**
>
> 对于以 **配置文件所有者** 模式注册的设备，如果设备运行的是 Android 12 或更高版本，则 **授予** 权限不适用于摄像头、位置、麦克风和传感器。

- **拒绝：** 此应用在此权限组中的危险权限请求被拒绝。不会提示用户。

默认是 **提示**。

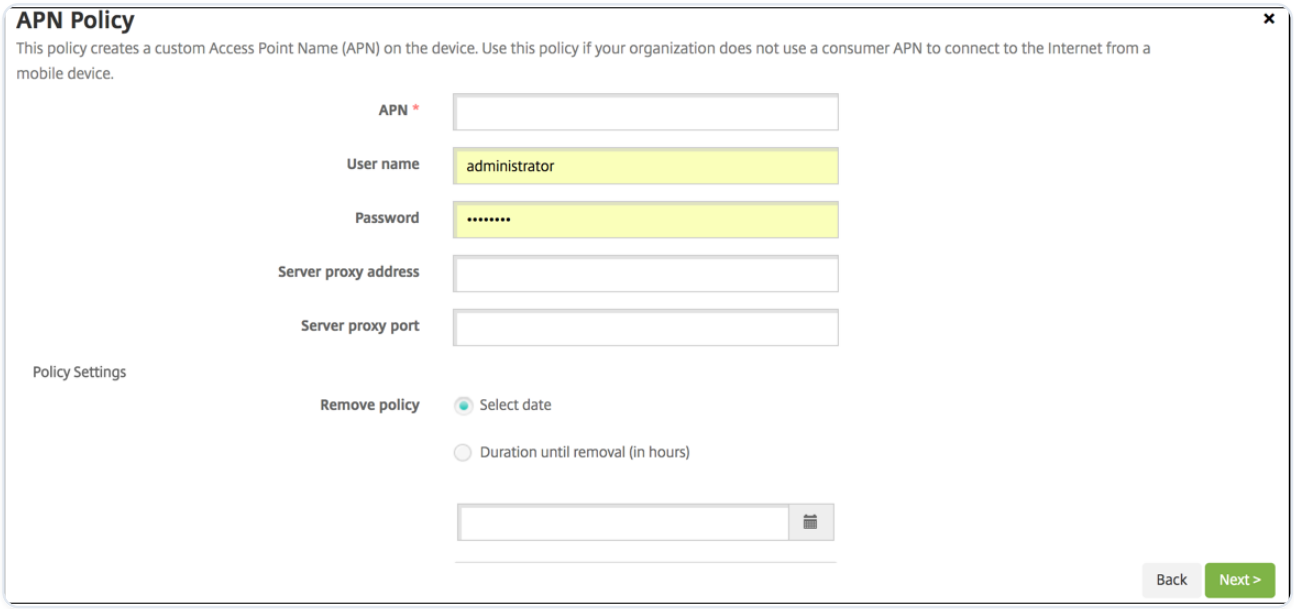
- 单击应用和授予状态旁边的 **保存**。
- 要为权限组添加更多应用，请再次单击 **添加** 并重复这些步骤。
- 完成权限组的 **授予状态** 设置后，单击 **下一步**。

APN 设备策略

您可以为 iOS 和 Android 设备添加自定义接入点名称 (APN) 设备策略。如果您的组织不使用消费者 APN 从移动设备连接到 Internet，则可以使用此策略。APN 策略确定用于将您的设备连接到特定电话运营商的通用分组无线服务 (GPRS) 的设置。此设置已在大多数新型手机中定义。

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。

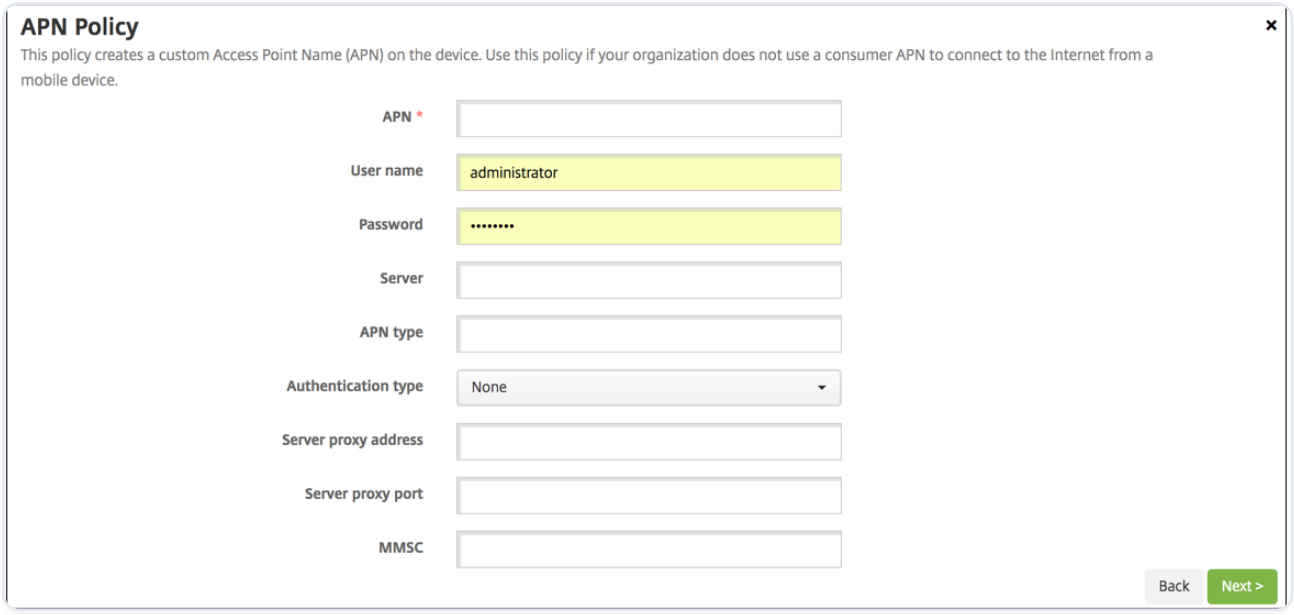
iOS 设置



- **APN：** 键入接入点的名称。该名称必须与接受的 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。如果缺少用户名，设备将在配置文件安装期间提示输入该字符串。

- **密码：** 此 APN 用户的密码。出于混淆目的，密码已编码。如果有效负载中缺少密码，设备将在配置文件安装期间提示输入密码。
- **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，在 **删除策略** 旁边，单击 **选择日期** 或 **删除前持续时间（小时）**。
  - 对于选项 **选择日期**，单击日历以选择具体的删除日期。
  - 对于选项 **需要密码**，键入密码。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括 **选择日期** 和 **删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择要删除的特定日期。
    - **直到删除的持续时间（小时）：** 键入一个数字（以小时为单位），直到策略被删除。仅适用于 iOS 6.0 或更高版本。

Android 设置



- **APN：** 键入接入点的名称。该名称必须与接受的 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。如果缺少用户名，设备会在配置文件安装期间提示输入该字符串。
- **密码：** 此 APN 用户的密码。为混淆目的，密码已编码。如果有效负载中缺少密码，设备会在配置文件安装期间提示输入密码。

- **服务器：** 此设置早于智能手机，通常为空。它引用了无线应用协议 (WAP) 网关服务器，用于无法访问或呈现标准网站的手机。
- **APN 类型：** 此设置必须与运营商对接入点的预期用途匹配。它是一个逗号分隔的 APN 服务指定符字符串，并且必须与无线运营商发布的定义匹配。示例包括：
  - `*`：所有流量都通过此接入点。
  - `mms`：多媒体流量通过此接入点。
  - `default`：所有流量（包括多媒体）都通过此接入点。
  - `supl`：安全用户平面定位与辅助 GPS 相关联。
  - `dun`：拨号网络已过时且很少使用。
  - `hipri.`：高优先级网络。
  - `fota`: 固件空中下载用于接收固件更新。
- **身份验证类型：** 在下拉列表中单击要使用的身份验证类型。默认为“无”。
- **服务器代理地址：** 运营商 APN HTTP 代理的 IP 地址或 URL。
- **服务器代理端口：** APN 代理的端口号。如果输入了服务器代理地址，则需要此端口。
- **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：** 用于 MMS 流量的多媒体消息服务服务器的地址。MMS 成功取代 SMS，用于发送包含图片或视频等多媒体内容的较大消息。这些服务器需要特定的协议（例如 MM1、... MM11）。
- **MMS 端口：** 用于 MMS 代理的端口。

应用访问设备策略

应用访问设备策略允许您定义一个应用程序列表，这些应用程序必须安装、可以安装或不得安装。如果设备上的应用程序与此策略冲突，Citrix Endpoint Management 会将设备标记为不合规。然后，您可以创建自动化操作来响应该设备合规性。

> **重要提示：**
>
> 应用访问设备策略不会阻止用户安装禁用应用或卸载所需应用。

> 您一次只能配置一种访问策略。每个策略都有一个所需应用、建议应用或禁用应用的列表，但不能在同一个应用访问策略中混合使用。如果您为每种类型的列表创建策略，请仔细命名每个策略，以便您知道哪个策略适用于哪个应用列表。

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。

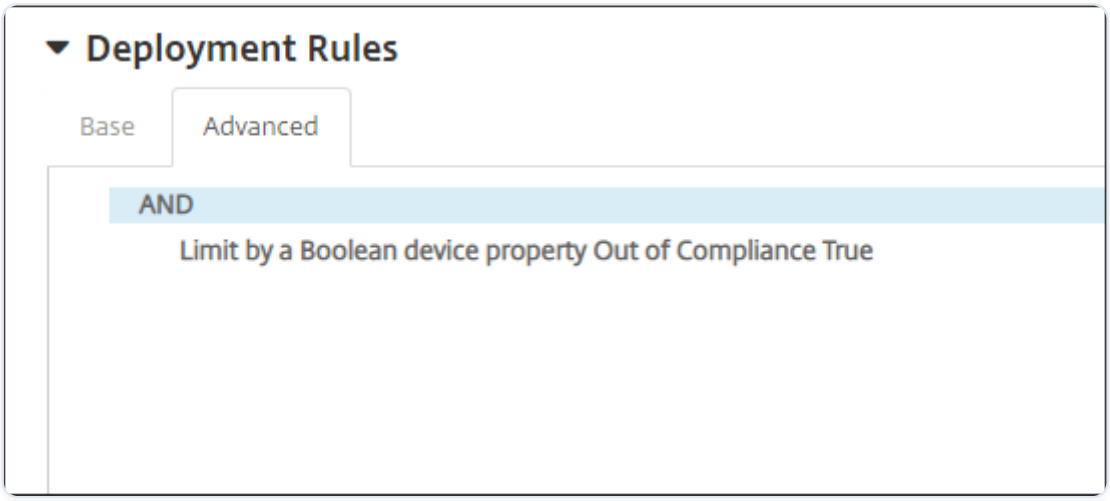
iOS 和 Android（旧版设备管理员）设置

- **访问策略：** 选择要为此策略配置的列表类型。
  - **必需：** 应用程序必须存在于设备上。如果应用程序不存在，则设备将被标记为不合规。**必需**是默认选项。
  - **禁用：** 应用程序不得存在于设备上。如果应用程序确实存在，则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：
  a. 单击**添加**，然后配置以下内容：
    - **应用程序名称：** 输入应用程序名称。
    - **应用程序标识符：** 输入可选的应用程序标识符。
  b. 点击 **保存**。
  c. 对要添加的每个应用程序重复这些步骤。

根据应用访问合规性配置自动化操作

1. 添加应用访问策略以要求或禁止应用。
2. 根据相关应用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，则将设备标记为不合规。
     - 一旦安装了该必需应用，则将设备标记为合规。
   - 禁止
     - 如果设备上存在禁止的应用，则将设备标记为不合规。
     - 一旦不再安装该禁止的应用，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. 创建一个限制策略，其中包含您希望在不合规设备上实施的设置。

a. 作为限制策略的一部分，添加一个高级部署规则，其中包含选项 **按布尔设备属性限制、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后删除限制策略。
5. 添加一个高级部署规则，其中包含选项 **按布尔设备属性限制、不合规** 和 **False**。请参阅 配置文件删除设备策略。

应用属性设备策略

应用属性设备策略允许您为 iOS 设备上的应用指定属性。通过配置此类策略，您可以实现以下目的：

- 为应用分配每应用 VPN。
- 阻止用户卸载关键任务应用。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。

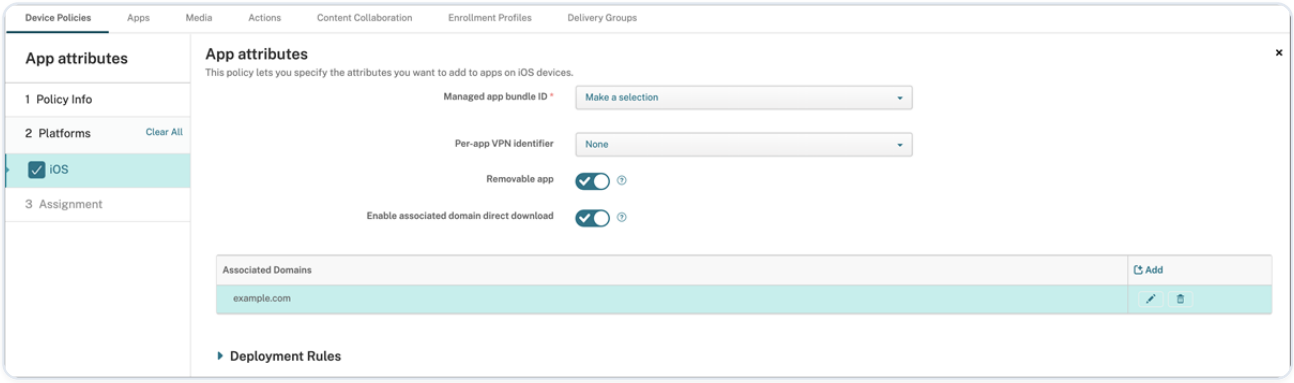
要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

关于关联域

关联域允许您在域和应用之间建立安全关联，以便您可以共享凭据或从您的网站在应用中提供功能。例如，启用此功能后，您可以在组织中的应用和网站之间共享数据和登录凭证。

有关如何启用此功能的详细信息，请参阅 Apple 网站上的支持关联域。

iOS 设置



- **托管应用捆绑包 ID：**通过以下方式指定应用：
  - 选择应用捆绑包 ID。仅在您启用**应用清单**设备策略后，这些选项才可用，该策略会收集托管设备上的应用清单。
  - 选择**添加新项**，然后键入应用捆绑包 ID。 要查找应用捆绑包 ID，请参阅查找 App Store 中应用的捆绑包 ID。
- **每应用 VPN 标识符：** (可选) 为此应用选择一个每应用 VPN。选项包括您在**设备策略 > VPN 策略**页面上配置的每应用 VPN 连接。 有关详细信息，请参阅配置每应用 VPN。
- **可移除应用：** (可选) 指定此应用在作为托管应用时是否可由用户移除。要防止用户卸载此应用，请将此选项设置为**关闭**。默认值为**开启**。
- **启用关联域直接下载：** (可选) 默认值为**开启**，表示此应用直接在域上而不是在 Apple 服务器上执行声明的站点关联验证。仅对无法访问 Internet 的域将此选项设置为**开启**。
- **关联域：** (可选) 要为此应用添加关联域，请单击**添加**，然后键入其完全限定域名 (FQDN)。

在 App Store 中查找应用的捆绑包 ID

1. 在 App Store 中找到该应用并复制 URL 末尾的数字。例如，363501921 是 Citrix Workspace 应用程序的应用 ID。
2. 转到 `https://itunes.apple.com/lookup?id=` 并在该 URL 后粘贴数字。TXT 文件将自动下载到您的计算机。
3. 在 TXT 文件中，搜索 `bundleId` 并获取应用的捆绑包 ID。示例：Citrix Workspace 应用程序的捆绑包 ID 为 `com.citrix.ReceiveriPad`。

应用配置设备策略

您可以通过部署以下内容来远程配置支持托管配置的应用程序：

- XML 配置文件 (`.plist`，也称为属性列表) 到 iOS 设备

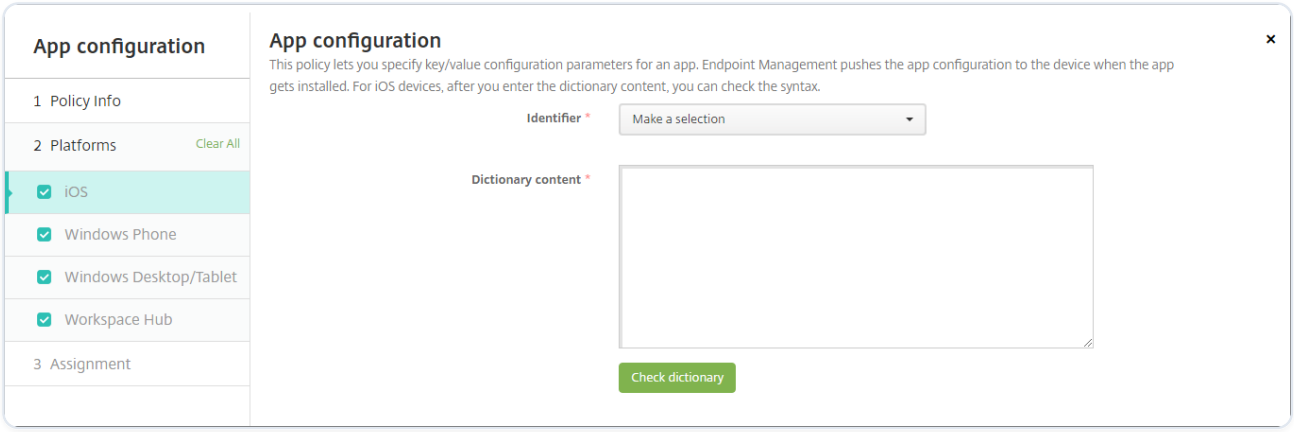
- 运行 Windows 10 或 Windows 11 的手机、桌面或平板电脑设备的键/值对

此配置指定了应用程序中的各种设置和行为。Citrix Endpoint Management 会在用户安装应用程序时将配置推送到设备。您可以配置的实际设置和行为取决于应用程序，并且超出了本文的范围。

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。

> **注意：**
>
> 各自的应用程序所有者定义应用程序配置变量。 例如，Chrome 管理并维护 Chrome 的应用程序配置变量。有关详细信息，请参阅Chrome 应用程序配置变量。

iOS 设置



- **标识符：** 在下拉列表中单击要配置的应用程序，或单击 **添加新项** 将应用程序添加到列表中。
  - 如果单击 **添加新项**，请在出现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**。Citrix Endpoint Management 会验证 XML。如果没有错误，您将在内容框下方看到 **有效 XML**。如果内容框下方出现任何语法错误，您必须先更正它们才能继续。

Windows 桌面和平板电脑设置

您可以配置通用 Windows 平台 (UWP) 应用程序或 Win 32 应用程序。要导入 Microsoft 管理模板 (ADMX) 策略设置，请配置 Win 32 应用程序。

> **注意：**

> App Configuration 设备策略支持用于 Office 等第三方应用程序的第三方 ADMX 文件。不支持作为操作系统组策略在 `%SystemRoot%\PolicyDefinitions` 下提供的适用于 Windows 的 Microsoft ADMX 模板。

- 如果选择 **UWP 应用**：在**进行选择**列表中，单击要配置的应用，或单击**添加新项**将应用添加到列表中。

  设备策略配置屏幕(/en-us/citrix-endpoint-management/media/app-configuration-policy-uwp.png)

  - 如果单击**添加新项**，请在出现的字段中键入包系列名称。
  - 对于要添加的每个配置参数，请单击**添加**，然后执行以下操作：
    - **参数名称**：输入 Windows 设备的应用程序设置的密钥名称。有关 Windows 应用设置的信息，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**：单击**浏览**并导航到要用于配置策略的 ADMX 文件。

  设备策略配置屏幕(/en-us/citrix-endpoint-management/media/app-configuration-policy-win32.png)

  - 单击**添加**。ADMX 文件中的配置选项将显示在页面的右侧。

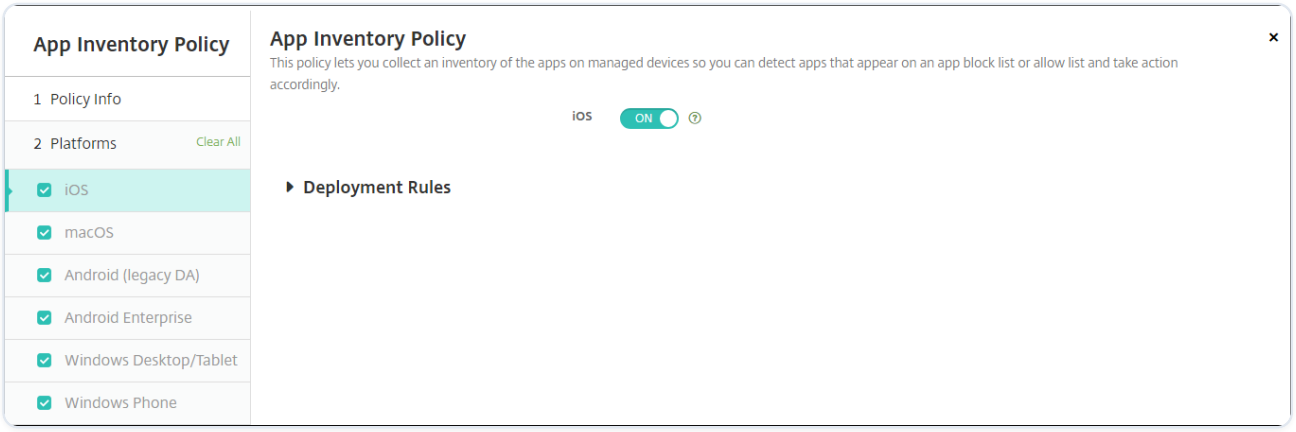
    设备策略配置屏幕(/en-us/citrix-endpoint-management/media/app-configuration-policy-win32-configuration-settings.png)
  - 选择策略路径。如果多次选择同一路径，则将强制执行与最新版本关联的配置。
  - 将**启用**设置为**开**。
  - 以键值对的形式输入任何所需的列表元素值。使用文本字符串 **&#xF000** 分隔每个键值对以及对中的值和键。
  - 包含小数的元素值可能需要特定范围内的值。

应用程序清单设备策略

应用程序清单策略允许您收集托管设备上的应用程序清单。Citrix Endpoint Management 随后可以将该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。通过这种方式，您可以检测出现在应用程序允许列表或阻止列表中的应用程序并采取正确操作。使用应用程序访问策略定义允许列表或阻止列表。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅设备策略。

iOS、macOS、Android（旧版设备管理员）、Android Enterprise 和 Windows 桌面/平板电脑



- 对于您选择的每个平台，请保留默认设置或将设置更改为 **Off**。默认值为 **On**。

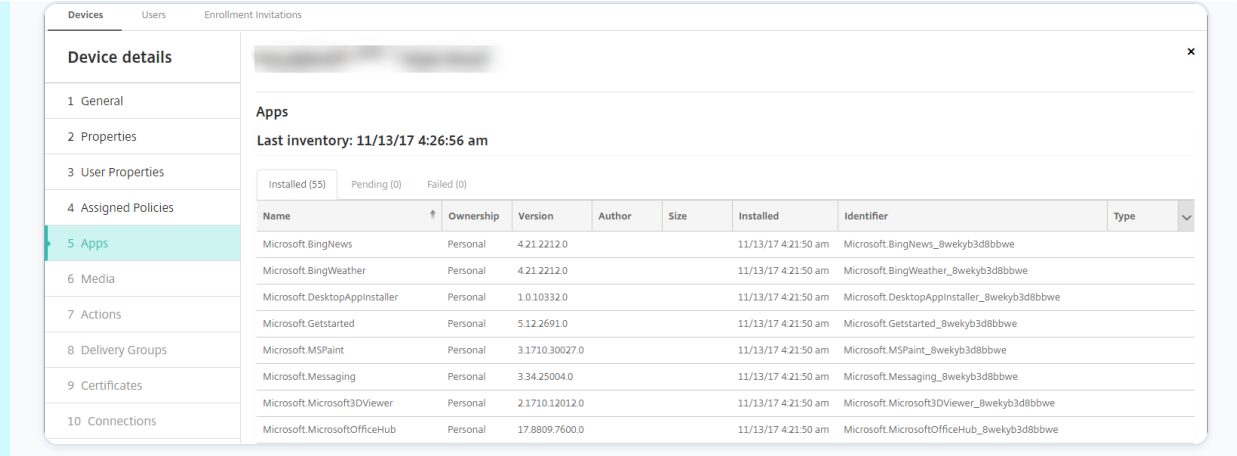
清点并删除 `Win32` 应用程序

您可以确定用户设备上的 `Win32` 应用程序是否遵循您的应用程序访问设备策略。要查看托管的 Windows 10 和 Windows 11 Desktop and Tablet 设备上的 `Win32` 应用程序清单：

1. 转至 **Configure > Device Policies**，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 **Manage > Devices**，选择要查看的 Windows 10 和 Windows 11 设备，单击 **Edit**，然后单击 **Apps** 选项卡。

   清单结果随即显示。

   > **注意：**
   >
   > 如果您正在配置 Windows 11 设备，则必须等待长达 24 小时才能获得正确的清单结果，这是 Microsoft 的设计使然。



3. 将应用程序清单与您的应用程序访问设备策略进行比较。如果设备上安装了阻止列表中的应用程序，您可以从设备中删除它们。

由不正确的“产品代码”引起的应用程序安装和卸载问题

如果 `Win32` 应用配置了不正确的产品代码，应用最初会安装，但 Microsoft 不会将应用状态返回给 Citrix Endpoint Management。结果是：

- 应用卸载设备策略不会卸载该应用。
- Citrix Endpoint Management 会继续部署该应用，因为它没有收到应用已安装的确认。每次部署时，设备都会生成错误代码，因为该应用已安装。在 **管理 > 设备 > 交付组详细信息** 中显示的错误是：`Msi Application received: Reporting:AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

要更正产品代码：

1. 手动从设备中删除该应用。
2. 在 Citrix Endpoint Management 控制台中，转到 **配置 > 应用** 并更正 `Win32` 应用的产品代码。
3. 部署 `Win32` 应用。

应用程序防护设备策略

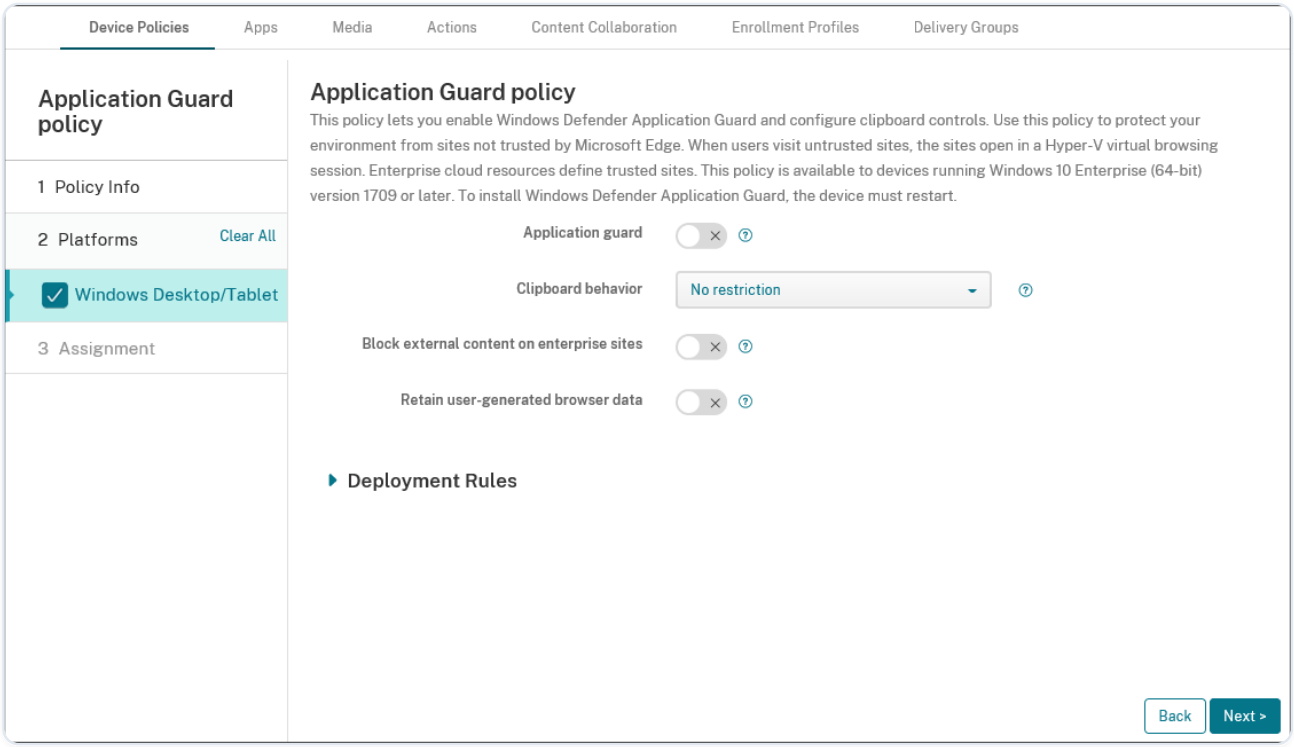
应用程序防护策略指定 Windows Defender 应用程序防护设置。这些设置包括是否启用应用程序防护以及剪贴板行为的控制。

Windows Defender 应用程序防护可保护您的环境免受未被组织定义为受信任的站点的侵害。当用户访问未列在隔离网络边界中的站点时：这些站点会在 Hyper-V 中的虚拟浏览会话中打开。企业云资源定义受信任的站点。

要求

- 运行 Windows 10 企业版（64 位）或 Windows 11 企业版（64 位）的设备。安装 Windows Defender 应用程序防护需要重启设备。
- Microsoft Edge 浏览器

Windows 桌面和平板电脑设置



- **应用程序防护：** 启用应用程序防护。默认值为“**关**”。
  - **企业云资源：** 企业云域的逗号分隔列表。
- **剪贴板行为：** 控制内容可以复制和粘贴的方向。选项如下：
  - **未配置**
  - **仅允许从浏览器复制和粘贴到电脑：** 允许用户仅从其浏览器复制和粘贴内容到其电脑。
  - **仅允许从电脑复制和粘贴到浏览器：** 允许用户仅从其电脑复制和粘贴内容到其浏览器。
  - **允许在电脑和浏览器之间复制和粘贴：** 允许用户在其电脑和浏览器之间自由复制和粘贴内容。
  - **阻止 PC 和浏览器之间的复制和粘贴：** 不允许用户在 PC 和浏览器之间复制和粘贴内容。
- **剪贴板内容：** 控制用户可以复制和粘贴的内容。选项如下：
  - **无限制**
  - **允许复制文本：** 允许用户仅复制文本。

  - **允许复制图像：** 允许用户仅复制图像。
  - **允许复制文本和图像：** 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**”，则 Windows Defender 应用程序防护会阻止未经批准的站点上的内容加载到企业站点上。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。默认设置为“**关**”。

应用锁定设备策略

应用锁定设备策略定义了一个应用列表，这些应用要么是：

- 允许在设备上运行。
- 禁止在设备上运行。

该策略的具体工作方式因每个受支持的平台而异。例如，您无法在 iOS 设备上阻止多个应用。

同样，对于 iOS 设备，每个策略只能选择一个 iOS 应用。用户只能使用其设备运行单个应用。除了在强制执行应用锁定设备策略时您明确允许的选项外，他们无法在设备上执行任何其他活动。

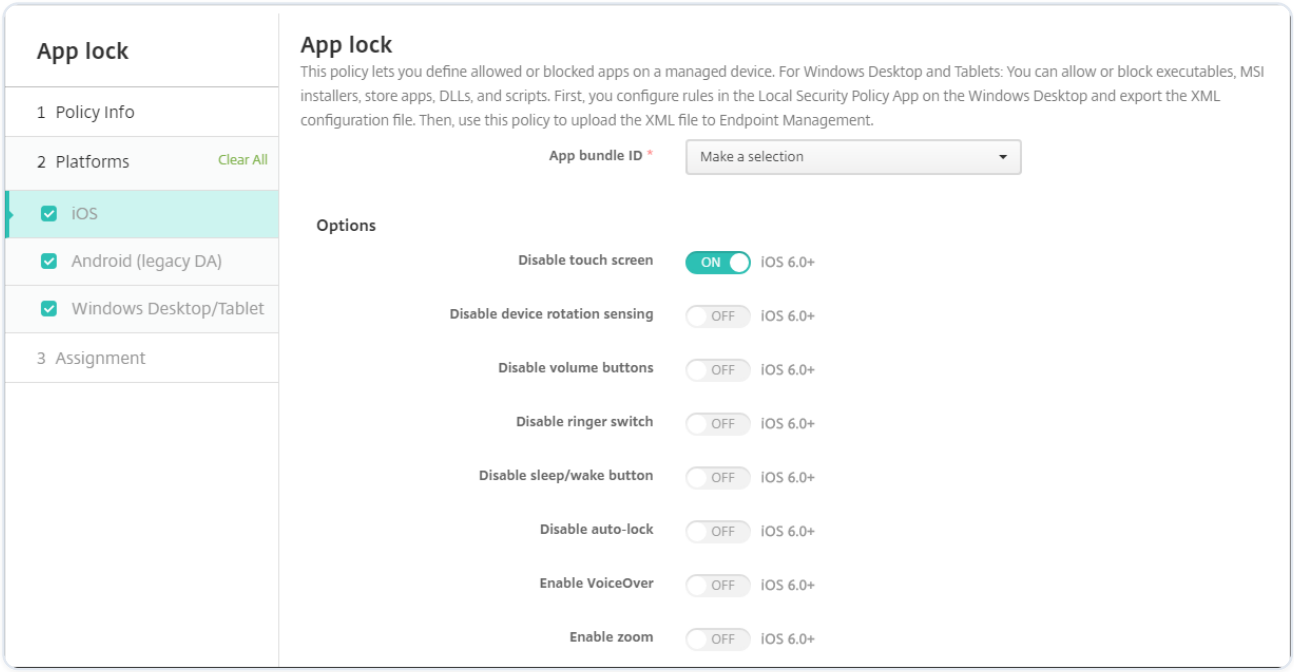
此外，iOS 设备必须处于受监管状态才能推送应用锁定策略。

尽管设备策略适用于大多数 Android L 和 M 设备，但应用锁定在 Android N 或更高版本的设备上不起作用。它不起作用是因为 Google 弃用了所需的 API。

对于托管的 Windows 桌面和平板电脑，您可以创建应用锁定设备策略，该策略定义允许列表和阻止列表上的应用。您可以允许或阻止可执行文件、MSI 安装程序、商店应用、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



- **应用捆绑包 ID：** 单击下拉列表中此策略适用的应用，或单击“**添加新项**”将应用添加到列表中。如果选择“**添加新项**”，请在出现的字段中键入应用名称。
- **选项：** 对于每个选项，默认值为“**关**”，但“**禁用触摸屏**”除外，其默认值为“**开**”。
  - 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

    当**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
  - 禁用旁白
  - 启用缩放
  - 启用反转颜色
  - 启用辅助触控
  - 启用朗读所选内容
  - 启用单声道音频
  - 启用语音控制
- **用户启用选项：** 对于每个选项，默认设置为**关**。

- 允许旁白调整
- 允许缩放调整
- 允许反转颜色调整
- 允许辅助触控调整
- 允许语音控制调整

- **策略设置**
  - **删除策略：** 选择策略删除的计划方法。可用选项为**选择日期**和**距离删除的持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **距离删除的持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 或更高版本。

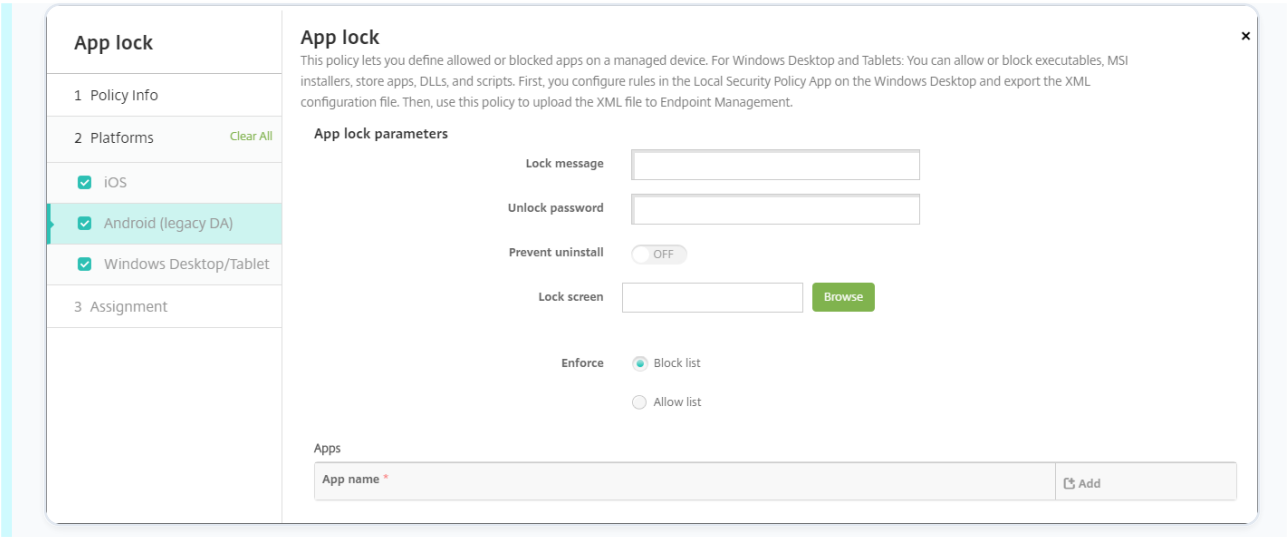
将 iPad 配置为自助服务终端

您可以使用“应用锁定”设备策略将受监督的 iPad 作为自助服务终端运行。Apple 将此功能称为“单应用模式”。有关此功能的更多信息，请参阅 Apple 文档。请确保在部署此策略之前部署要运行的应用。

1. 导航到**配置 > 设备策略**，然后单击**添加**。
2. 选择**应用锁定**策略。
3. 键入**策略名称**和可选的**描述**。
4. 仅选择 **iOS** 平台。
5. 对于**应用捆绑包 ID**，选择要在 iPad 上运行的应用。
6. 按照之前的说明配置所需的任何选项，然后保存策略。
7. 将策略添加到与您的 iPad 相同的交付组，然后部署策略。

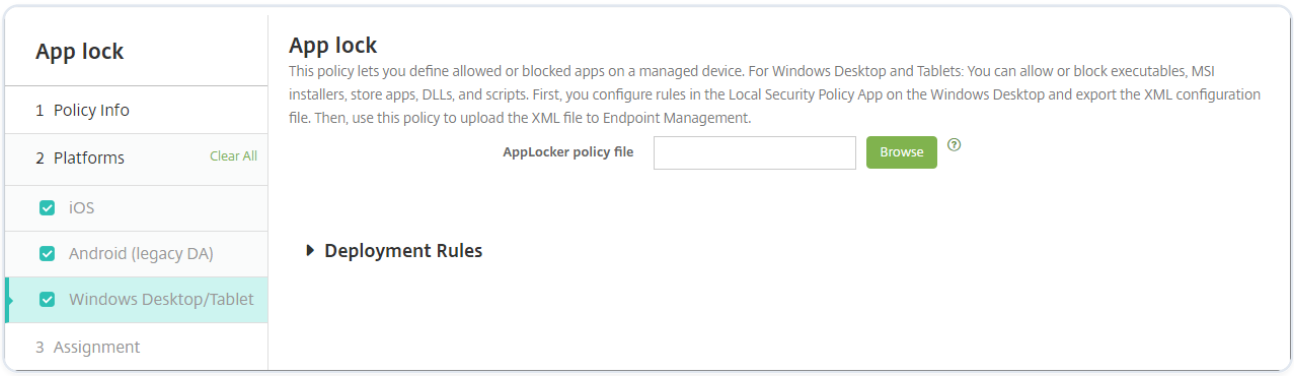
Android（旧版设备管理员）设置

> **注意：**
>
> 您无法使用“应用程序锁定”设备策略阻止 Android 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：** 通过单击“**浏览**”并导航到文件位置来选择显示在设备锁定屏幕上的图像。
  - **强制执行：** 单击“**阻止列表**”以创建不允许在设备上运行的应用程序列表。单击“**允许列表**”以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：** 在下拉列表中单击要添加到允许列表或阻止列表的应用程序名称。或者，单击“**添加新项**”将应用程序添加到可用应用程序列表。
  - 如果选择“**添加新项**”，请在出现的字段中键入应用程序名称。
  - 单击“**保存**”或“**取消**”。
  - 对要添加到允许列表或阻止列表的每个应用程序重复这些步骤。

Windows 桌面和平板电脑设置



应用程序锁定先决条件

- 在 Windows 中，在 Windows 10 或 Windows 11 桌面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出现问题。
- 然后，使用应用程序锁定设备策略将 XML 文件上传到 Citrix Endpoint Management。有关创建规则的更多信息，请参阅此 Microsoft 文章：`<https://docs.microsoft.com/zh-cn/windows/security/threat-protection/applocker/applocker-overview>`

从 Windows 配置和导出策略 XML 文件

> **重要提示：**
>
> 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 计算机上，启动“**本地安全策略**”编辑器。单击“**开始**”，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“**配置规则强制**”。
4. 选择“**已配置**”，然后选择“**强制规则**”。启用规则时，“**强制规则**”是默认设置。
5. 右键单击“**AppLocker**”，单击“**导出策略**”，然后保存 XML 文件。

> **注意：**
>
> 您可以创建“**可执行规则**”、“**Windows 安装程序规则**”、“**脚本规则**”和“**打包的应用程序规则**”。为此，请右键单击该文件夹，然后单击“**创建新规则**”。

将策略 XML 文件导入 Citrix Endpoint Management

创建一个应用锁定策略。在“**应用锁定策略文件**”设置旁边，单击“**浏览**”并导航到 XML 文件。

停止应用应用锁定策略

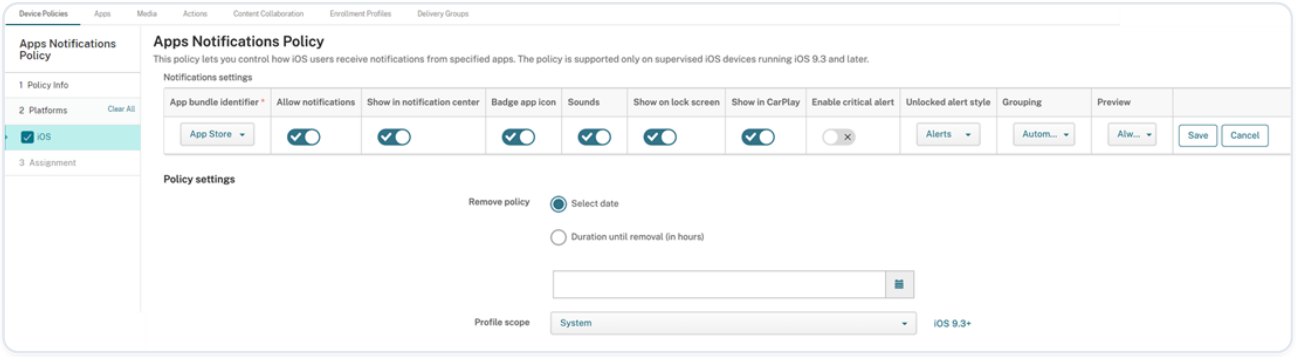
在 Citrix Endpoint Management 中部署应用锁定策略后：要停止应用该应用锁定策略，请创建一个空的 XML 文件。然后，创建另一个应用锁定策略，上传该文件，并部署该策略。已启用应用锁定的设备不受影响。首次接收策略的设备将不会应用应用锁定策略。

应用通知设备策略

应用通知策略允许您控制 iOS 用户如何接收来自指定应用的通知。此策略仅在运行 iOS 9.3 或更高版本的受监管 iOS 设备上受支持。

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



- **应用捆绑包标识符：**指定要管理通知设置的应用：
  - 选择应用捆绑包 ID。仅在启用**应用清单**设备策略后，选项才可用，该策略用于收集受管设备上的应用清单。
  - 选择**添加新项**，然后键入应用捆绑包 ID。 要查找应用捆绑包 ID，请参阅查找 App Store 中应用的捆绑包 ID。
- **允许通知：选择开**以允许通知。
- **在通知中心显示：选择开**以在用户设备的通知中心显示通知。
- **标记应用图标：选择开**以显示带有通知的标记应用图标。
- **声音：选择开**以在通知中包含声音。
- **在锁定屏幕上显示：选择开**以在用户设备的锁定屏幕上显示通知。
- **在 CarPlay 中显示：选择开**以在 Apple CarPlay 中显示通知。适用于 iOS 12 及更高版本。默认值为**开**。
- **启用紧急警报：选择开**以允许应用将通知标记为紧急通知，该通知将忽略“勿扰”和铃声设置。适用于 iOS 12 及更高版本。默认值为**关**。
- **解锁警报样式**：选择**无**、**横幅**或**警报**以配置解锁警报的显示方式。
- **预览**：选择设备如何显示应用的通知预览。适用于 iOS 14 及更高版本。
  - **始终**：在设备锁定或解锁时显示通知预览。
  - **解锁时**：仅在设备解锁时显示通知预览。

  - **从不**：清除设备上的通知预览。

- **分组**：选择设备如何对来自应用的通知进行分组。适用于 iOS 12 及更高版本的设备。
  - **自动**：将通知分组到应用指定的组中。
  - **按应用**：将来自应用的通知分组到一个组中。
  - **关闭**：清除应用的通知分组。设备按顺序显示所有通知。
- **策略设置**
  - **删除策略**：选择一种计划策略删除的方法。选项包括：
    - **选择日期**：单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）**：键入一个数字（以小时为单位），直到策略删除发生。适用于 iOS 6.0 或更高版本。
  - **配置文件范围**：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。

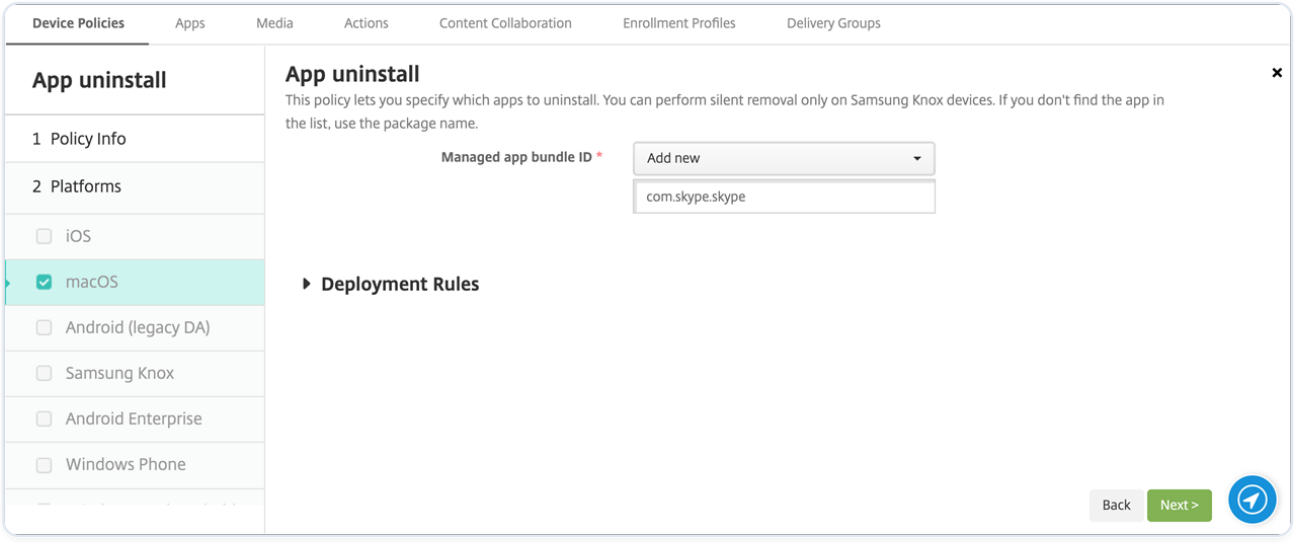
应用程序卸载设备策略

应用程序卸载策略允许您从用户设备中删除应用程序。如果您不再希望支持某个应用程序，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。

当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，然后该应用程序将被删除。

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



- **托管应用程序捆绑包 ID：** 在列表中，选择一个现有托管应用程序或**添加新应用程序**。如果此平台未配置任何应用程序，则列表为空，您必须添加新的托管应用程序。当您选择**添加新应用程序**时，将出现一个字段，您可以在其中键入托管应用程序名称。适用于 iOS 5.0 及更高版本以及 macOS 11.0 及更高版本。

安卓（旧版设备管理员）、安卓企业版以及 Windows 桌面/平板电脑设置

- **要卸载的应用程序：** 对于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：** 在下拉列表中单击现有应用程序，或单击**添加新应用程序**以输入新的应用程序名称。如果此平台未配置任何应用程序，则列表为空，您必须添加新应用程序。
  - 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，还要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。

在相应的公共应用商店应用程序安装后自动卸载企业应用程序

您可以将 Citrix Endpoint Management 配置为在安装公共应用商店版本后删除 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出现两个相似的应用程序图标。

应用程序卸载设备策略的部署条件会触发 Citrix Endpoint Management 在安装新版本时从用户设备中删除旧应用程序。此功能仅适用于以企业模式 (XME) 连接到 Citrix Endpoint Management 服务器的托管 iOS 设备。

要配置具有“已安装应用程序名称”条件的部署规则：

- 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，如示例所示，选择**已安装应用程序名称**和**等于**。键入公共应用商店应用程序的应用程序捆绑包 ID。

在此示例中，当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，Citrix Endpoint Management 将删除企业版本 (com.citrix.mail)。

应用卸载限制设备策略

您可以指定用户可以在 Amazon 设备上卸载或无法卸载的应用程序。

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。

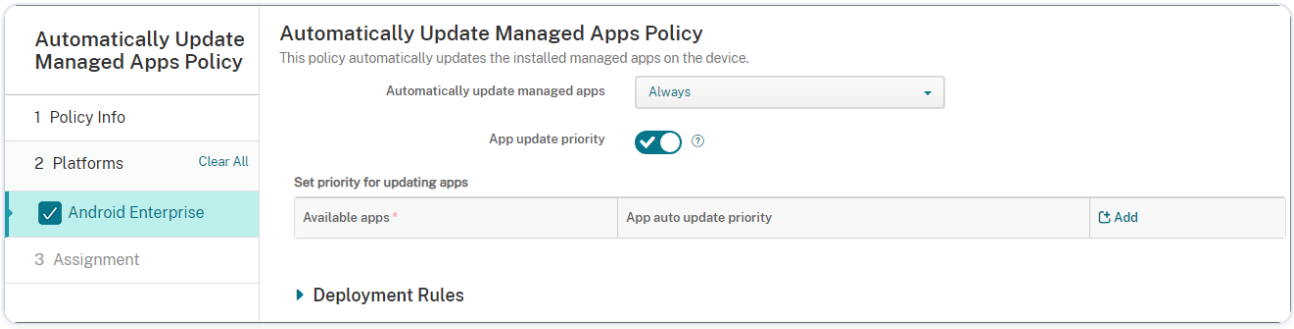
Amazon 设置

- **应用卸载限制设置：** 对于要添加的每个应用规则，单击**添加**，然后执行以下操作：
  - **应用名称：** 在下拉列表中单击一个应用，或单击**新建**以添加一个应用。
  - **规则：** 选择用户是否可以卸载该应用。默认设置为允许卸载。
  - 单击**保存**或**取消**。

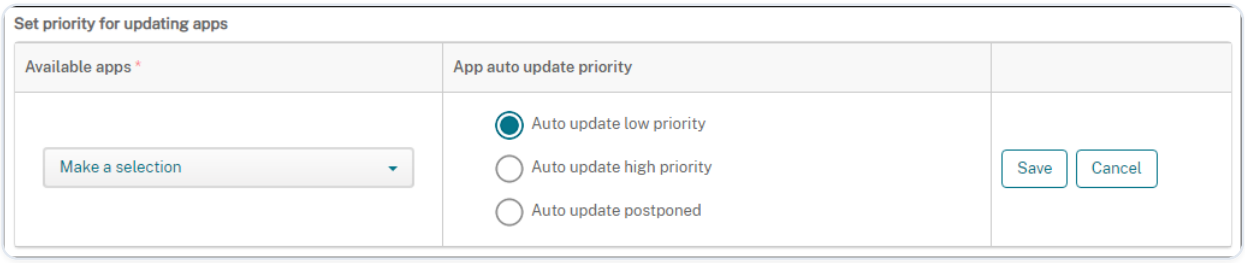
自动更新托管应用设备策略

此策略控制已安装的托管应用在 Android Enterprise 设备上的更新方式。您可以限制用户在其设备上允许应用自动更新的能力。如果您允许用户控制其设备上应用的自动更新，他们将在托管的 Google Play 商店中设置自动应用更新策略。

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**
  - **始终：** 启用应用自动更新。**始终**是默认设置。
  - **允许用户配置策略：** 允许用户在托管的 Google Play 商店中为设备配置自动应用更新策略。
  - **从不：** 禁用应用自动更新。
  - **仅当设备连接到 Wi-Fi 时：** 仅当设备连接到 Wi-Fi 时才允许应用自动更新。
- **应用更新优先级：** 如果为**开**，您可以为每个托管应用配置更新优先级级别。
- **设置应用更新优先级：** 单击**添加**以配置应用的更新优先级。



  - **可用应用：** 从菜单中选择一个应用以配置更新优先级。

- **应用自动更新优先级：** 从以下选项中选择一个更新优先级：
  - **自动更新低优先级：** 当设备正在充电、未被主动使用且连接到非计量网络时，应用会更新。
  - **自动更新（高优先级）：** 应用程序会尽快更新，不受任何限制。
  - **自动更新（推迟）：** 在新版本可用后，应用程序最长 90 天内不会自动更新。90 天后，应用程序将以低优先级自动更新。应用程序更新后，在接下来的 90 天内不会再次自动更新。用户可以随时手动更新应用程序。
- 完成后，单击“**保存**”。您可以通过单击铅笔图标来编辑配置。通过单击垃圾桶图标删除配置。

BitLocker 设备策略

Windows 10 和 Windows 11 包含一个名为 BitLocker 的磁盘加密功能，它为丢失或被盗的 Windows 设备提供额外的文件和系统保护，防止未经授权的访问。为了获得更多保护，您可以将 BitLocker 与受信任平台模块 (TPM) 芯片（版本 1.2 或更高版本）结合使用。TPM 芯片处理加密操作，并生成、存储和限制加密密钥的使用。

从 Windows 10 版本 1703 开始，MDM 策略可以控制 BitLocker。您可以使用 Citrix Endpoint Management 中的 BitLocker 设备策略来配置 Windows 10 和 Windows 11 设备上 BitLocker 向导中可用的设置。例如，在启用了 BitLocker 的设备上，BitLocker 会向用户提供以下几个选项：

- 他们希望如何在启动时解锁驱动器
- 如何备份其恢复密钥
- 如何解锁固定驱动器。

BitLocker 设备策略设置还配置是否要：

- 在没有 TPM 芯片的设备上启用 BitLocker。
- 在 BitLocker 界面中显示恢复选项。
- 在未启用 BitLocker 时，拒绝写入固定或可移动驱动器。
- 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可以访问。此密钥可在自助服务门户上找到。

> 注意

> 设备上 BitLocker 加密启动后，您无法通过部署更新的 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 企业版或 Windows 11 企业版。
- 在部署 BitLocker 设备策略之前，请为 BitLocker 的使用准备好您的环境。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。

Windows 桌面和平板电脑设置

BitLocker policy

This policy lets you enable BitLocker on an enrolled machine and specify the encryption mechanism to use.

BitLocker settings

Require device to be encrypted — ON

Encryption settings

Configure encryption methods — ON

Operating system drive — XTS AES 128-bit

Fixed drive — XTS AES 128-bit

Removable drive — XTS AES 128-bit

OS drive settings

Require additional authentication at startup — ON

Block BitLocker on devices without TPM chip — ON

TPM startup — Allow TPM

TPM startup PIN — Allow startup PIN with TPM

TPM startup key — Allow TPM key at startup

TPM startup key and PIN — Allow startup key and PIN with TPM

PIN length

Minimum PIN length — 6

BitLocker password recovery settings

BitLocker Recovery backup to Endpoint Management — ON

The Self-Help Portal displays the recovery key on the Devices page. Enable the server property shp.console.enable to provide access to the portal. **Learn more**

OS drive recovery settings

Enable OS drive recovery — ON

Allow certificate based data recovery agent — ON

48-bit recovery password — Allow 48-bit password

256-bit recovery key — Allow 256-bit recovery key

Hide OS drive recovery options — ON

Save recovery info to Active Directory Domain Services — ON

Recovery info stored in Active Directory Domain Services — Backup recovery password

Enable BitLocker after storing recovery info in Active Directory Domain Services — ON

- **Bitlocker 设置**
  - **要求设备加密：** 确定是否提示用户在 Windows 桌面或平板电脑上启用 BitLocker 加密。如果设置为“**开**”，则设备在注册完成后会显示一条消息，指示企业要求设备加密。如果设置为“**关**”，则不会提示用户，并且 BitLocker 将使用策略设置。默认为“**关**”。
- **加密设置**
  - **配置加密方法：** 确定用于特定驱动器类型的加密方法。如果设置为“**关**”，BitLocker 向导会提示设备用户选择用于驱动器类型的加密方法。所有驱动器的默认加密方法为 XTS-AES 128 位。可移动驱动器的默认加密方法为 AES-CBC 128 位。如果设置为“**开**”，BitLocker 将使用策略中指定的加密方法。如果设置为“**开**”，则会出现以下额外设置：**操作系统驱动器**、**固定驱动器**和**可移动驱动器**。为每种驱动器类型选择默认加密方法。默认为“**关**”。
- **操作系统驱动器设置**
  - **启动时需要额外身份验证：** 指定设备启动时所需的额外身份验证。还指定是否允许在没有 TPM 芯片的设备上使用 BitLocker。如果设置为“**关**”，则没有 TPM 的设备无法使用 BitLocker 加密。有关 TPM 的信息，请参阅 Microsoft 文章 受信任的平台模块技术概述。如果设置为“**开**”，则会出现以下额外设置。默认为“**关**”。
  - **阻止在没有 TPM 芯片的设备上使用 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，用户必须在启动前将其连接到设备。解锁密码最少为八个字符。默认为“**关**”。
  - **TPM 启动：** 在具有 TPM 的设备上，有四种解锁模式：仅限 TPM、TPM + PIN、TPM + 密钥和 TPM + PIN + 密钥。TPM 启动适用于仅限 TPM 模式，其中加密密钥存储在 TPM 芯片中。此模式不需要用户提供额外的解锁数据。用户设备在重新启动期间会自动解锁，使用 TPM 芯片中的加密密钥。默认为“**允许 TPM**”。
  - **TPM 启动 PIN：** 此设置为 TPM + PIN 解锁模式。PIN 最多可包含 20 位数字。使用“**最小 PIN 长度**”设置指定最小 PIN 长度。用户在 BitLocker 设置期间配置 PIN，并在设备启动期间提供 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，用户必须在启动前将其连接到设备。
  - **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。默认为 **6**。

- **BitLocker 密码恢复设置**
  - **BitLocker 恢复备份到 Citrix Endpoint Management：** 如果启用此选项，需要解锁设备的用户可以在自助服务门户上找到其 BitLocker 恢复密钥。Citrix Endpoint Management 管理员无法查看用户的 BitLocker 恢复密钥。有关查看 BitLocker 恢复密钥的更多信息，请参阅 BitLocker 恢复密钥。
- **操作系统驱动器恢复设置：** 为 BitLocker 加密的操作系统驱动器配置用户的恢复选项。
  - **启用操作系统驱动器恢复：** 如果解锁步骤失败，BitLocker 会提示用户输入配置的恢复密钥。此设置配置了在用户没有解锁密码或 USB 启动密钥时可用的操作系统驱动器恢复选项。默认为**关闭**。
  - **允许基于证书的数据恢复代理：** 指定是否允许基于证书的数据恢复代理。从“公钥策略”添加数据恢复代理，该策略位于“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更多信息，请参阅 Microsoft 文章BitLocker 组策略设置。默认为**关闭**。
  - **48 位恢复密码：** 指定是允许还是要求用户使用恢复密码。BitLocker 生成密码并将其存储在文件或 Microsoft 云帐户中。默认为**允许 48 位密码**。
  - **256 位恢复密钥：** 指定是允许还是要求用户使用恢复密钥。恢复密钥是一个 BEK 文件，存储在 USB 驱动器上。默认为**允许 256 位恢复密钥**。
  - **隐藏操作系统驱动器恢复选项：** 指定是否在 BitLocker 界面中显示或隐藏恢复选项。如果为**开**，则 BitLocker 界面中不显示任何恢复选项。在这种情况下，请将设备注册到 Active Directory，将恢复选项保存到 Active Directory，并将**将恢复信息保存到 AD DS**设置为**开**。默认为**关闭**。
  - **将恢复信息保存到 Active Directory 域服务：** 指定是否将恢复选项保存到 Active Directory 域服务。默认为**关闭**。
  - **存储在 Active Directory 域服务中的恢复信息：** 指定是将 BitLocker 恢复密码还是恢复密码和密钥包存储在 Active Directory 域服务中。存储密钥包支持从物理损坏的驱动器恢复数据。默认为**备份恢复密码**。
  - **在 Active Directory 域服务中存储恢复信息后启用 BitLocker：** 指定是否阻止用户启用 BitLocker，除非设备已连接到域并且 BitLocker 恢复信息备份到 Active Directory 成功。如果为**开**，则设备必须在启动 BitLocker 之前加入域。默认为**关闭**。
  - **预启动恢复消息和 URL：** 指定 BitLocker 是否在恢复屏幕上显示自定义消息和 URL。如果为**开**，则会出现以下额外设置：**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 Citrix Endpoint Management 恢复消息和 URL**。如果为**关**，则显示默认恢复消息和 URL。默认为**关闭**。

- **固定驱动器恢复设置：** 为 BitLocker 加密的固定驱动器配置用户的恢复选项。BitLocker 不会向用户显示有关固定驱动器加密的消息。要在启动期间解锁驱动器，用户需要提供密码或智能卡。启动解锁设置（不在此策略中）会在用户在固定驱动器上启用 BitLocker 加密时出现在 BitLocker 界面中。有关相关设置的信息，请参阅此列表前面部分的**配置操作系统驱动器恢复**。默认为**关闭**。
- **固定驱动器设置**
  - **阻止对未使用 BitLocker 的固定驱动器进行写入访问：** 如果设置为“**开**”，则用户只能在固定驱动器使用 BitLocker 加密时才能对其进行写入。默认设置为“**关**”。
- **可移动驱动器设置**
- **阻止对未使用 BitLocker 的可移动驱动器进行写入访问：** 如果设置为“**开**”，则用户只能在可移动驱动器使用 BitLocker 加密时才能对其进行写入。请根据您的组织是否允许对其他组织的可移动驱动器进行写入访问来配置此设置。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内的其他设备，例如网络驱动器。
- **其他驱动器设置**
- **提示进行其他磁盘加密：** 允许您禁用设备上其他磁盘加密的警告提示。默认设置为“**关**”。

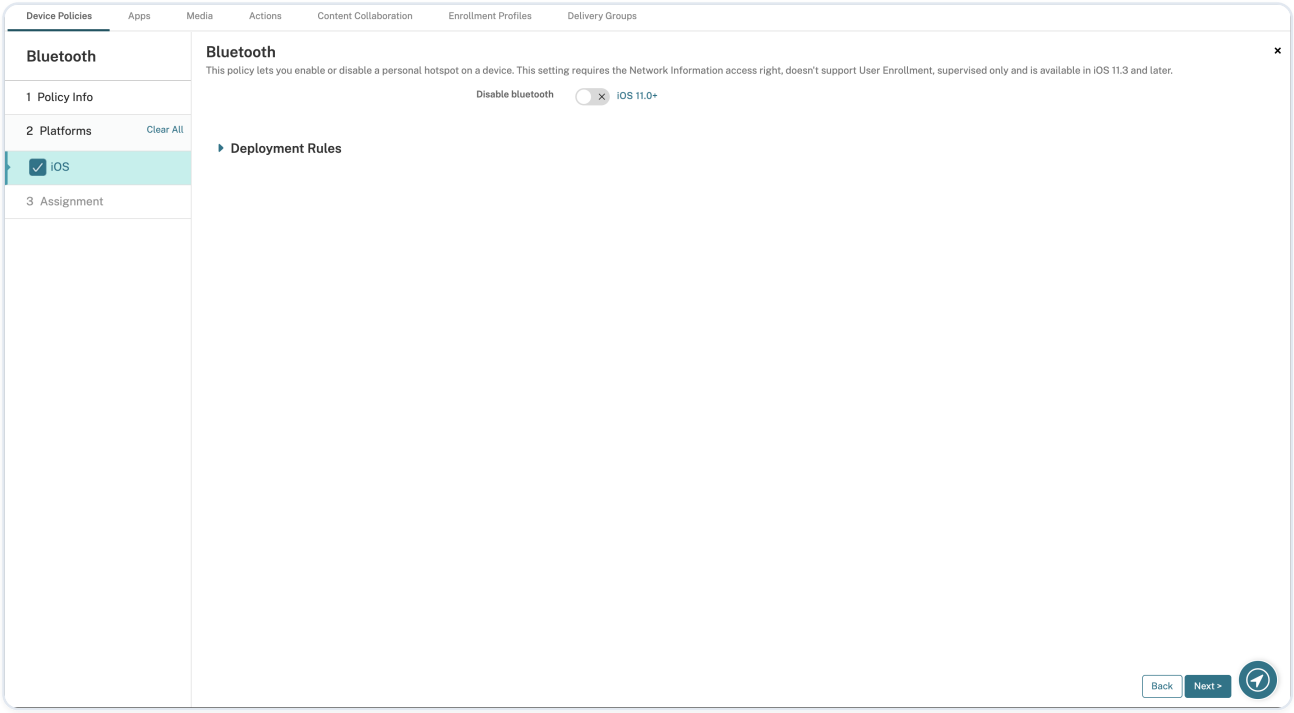
蓝牙设备策略

您可以在受监管的 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，并且适用于 iOS 11.3 及更高版本。

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



- **禁用蓝牙：** 允许您在受监管的设备上禁用或启用蓝牙。

日历 (CalDAV) 设备策略

您可以在 Citrix Endpoint Management 中添加设备策略，以将日历 (CalDAV) 帐户添加到用户的 iOS 或 macOS 设备，从而使他们能够与任何支持 CalDAV 的服务器同步日程数据。

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

- **帐户描述：** 键入帐户描述。此字段为必填项。
- **主机名：** 键入 CalDAV 服务器的地址。此字段为必填项。
- **端口：** 键入用于连接到 CalDAV 服务器的端口。此字段为必填项。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。此字段为必填项。
- **密码：** 键入可选的用户密码。
- **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：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**

- **选择日期：** 单击日历以选择要删除的具体日期。
- **删除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 或更高版本。

macOS 设置

- **帐户描述：** 键入帐户描述。此字段为必填项。
- **主机名：** 键入 CalDAV 服务器的地址。此字段为必填项。
- **端口：** 键入用于连接 CalDAV 服务器的端口。此字段为必填项。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。此字段为必填项。
- **密码：** 键入可选的用户密码。
- **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：** 选择策略删除的计划方法。可用选项为“**选择日期**”和“**删除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择要删除的特定日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 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 macOS 10.7 及更高版本。

蜂窝设备策略

此策略允许您在 iOS 设备上配置蜂窝网络设置。

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

您可以在非字符串字段中使用宏，例如“**代理服务器端口**”。

例如，您可以使用 `${device.xyz}` 或 `${setting.xyz}` 等宏，它们会扩展为整数。您还可以在设备配置 XML 文件中使用这些宏，通过使用“**导入 iOS 和 macOS 配置文件**”设备策略将其导入到 Citrix Endpoint Management 中。

- **附加 APN**
  - **名称：** 此配置的名称。
  - **身份验证类型：** 在下拉列表中单击“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：** 在下拉列表中单击 **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：** 选择一种方法来安排策略删除。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 输入一个数字（以小时为单位），表示策略删除发生前的持续时间。

连接调度设备策略

> **重要提示：**
>
> Citrix 建议您使用 Firebase Cloud Messaging (FCM) 来控制 Android 和 Android Enterprise 设备与 Citrix Endpoint Management 的连接。有关使用 FCM 的信息，请参阅 Firebase Cloud Messaging。
>
> 如果您选择不使用 FCM，则可以创建连接调度策略来控制用户设备连接到 Citrix Endpoint Management 的方式和时间。如果您选择使用 FCM，则还必须创建连接调度策略。

您可以指定用户手动连接其设备，或者设备在定义的时间范围内连接。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅 设备策略。

安卓和安卓企业设置

- **要求设备连接：** 单击要为此计划设置的选项。
  - **从不：** 手动连接。用户必须从其设备上的 Citrix Endpoint Management 启动连接。Citrix 不建议将此选项用于生产部署，因为它会阻止您向设备部署安全策略，这意味着用户永远不会收到任何新应用程序或策略。默认情况下启用“**从不**”选项。
  - **每次：** 按指定的时间间隔连接。当此选项生效并且您发送锁定或擦除等安全策略时，Citrix Endpoint Management 会在设备下次连接时处理设备上的操作。选择此选项时，将显示“**每 N 分钟连接一次**”字段，您必须在其中输入设备必须重新连接的分钟数。默认值和最小值均为 **120**。
  - **定义计划：** 用户设备上的 Citrix Endpoint Management 在网络连接丢失后尝试重新连接到 Citrix Endpoint Management 服务器。Citrix Endpoint Management 通过在您定义的时间范围内以固定间隔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，请参阅下一节“定义连接时间范围”。
    - **要求在每个这些范围内连接：** 用户的设备必须在任何已定义的时间范围内至少连接一次。
    - **使用本地设备时间而非 UTC：** 将定义的时间范围同步到本地设备时间，而不是协调世界时 (UTC)。

定义连接时间范围

启用以下选项时，将显示一个时间线，您可以在其中定义所需的时间范围。您可以启用其中一个或两个选项，以要求在特定时间段内永久连接，或要求在某些时间范围内连接。时间线中的每个方块代表 1 小时。要指定每个工作日早上 8:00 到 9:00 之间的连接，请单击时间线上每个工作日早上 8 点到 9 点之间的方块。

例如，下图中的两个时间线要求：

- 每个工作日上午 8:00 到上午 10:00 之间的永久连接
- 星期六凌晨 1:00 到星期日凌晨 2:00 之间的永久连接
- 每个工作日在上午 5:00 到上午 8:00 之间或在上午 10:00 到凌晨 12:00 之间至少有一个连接

设备策略配置屏幕(/en-us/citrix-endpoint-management/media/device-policy-scheduling-define-schedule.png)

联系人 (CardDAV) 设备策略

您可以在 Citrix Endpoint Management 中添加设备策略，以将 iOS 联系人 (CardDAV) 帐户添加到用户的 iOS 或 macOS 设备，从而使其能够与任何支持 CardDAV 的服务器同步联系人数据。

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

- **帐户描述：** 键入帐户描述。此字段为必填项。
- **主机名：** 键入 CardDAV 服务器的地址。此字段为必填项。
- **端口：** 键入用于连接到 CardDAV 服务器的端口。此字段为必填项。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。此字段为必填项。
- **密码：** 键入可选的用户密码。
- **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：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略删除发生前的持续时间。

macOS 设置

- **帐户描述：** 键入帐户描述。此字段为必填项。
- **主机名：** 键入 CardDAV 服务器的地址。此字段为必填项。
- **端口：** 键入连接到 CardDAV 服务器的端口。此字段为必填项。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。此字段为必填项。
- **密码：** 键入可选的用户密码。
- **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：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
  - **选择日期：** 单击日历以选择要删除的具体日期。
  - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
- **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
- **配置文件范围：** 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 及更高版本上可用。

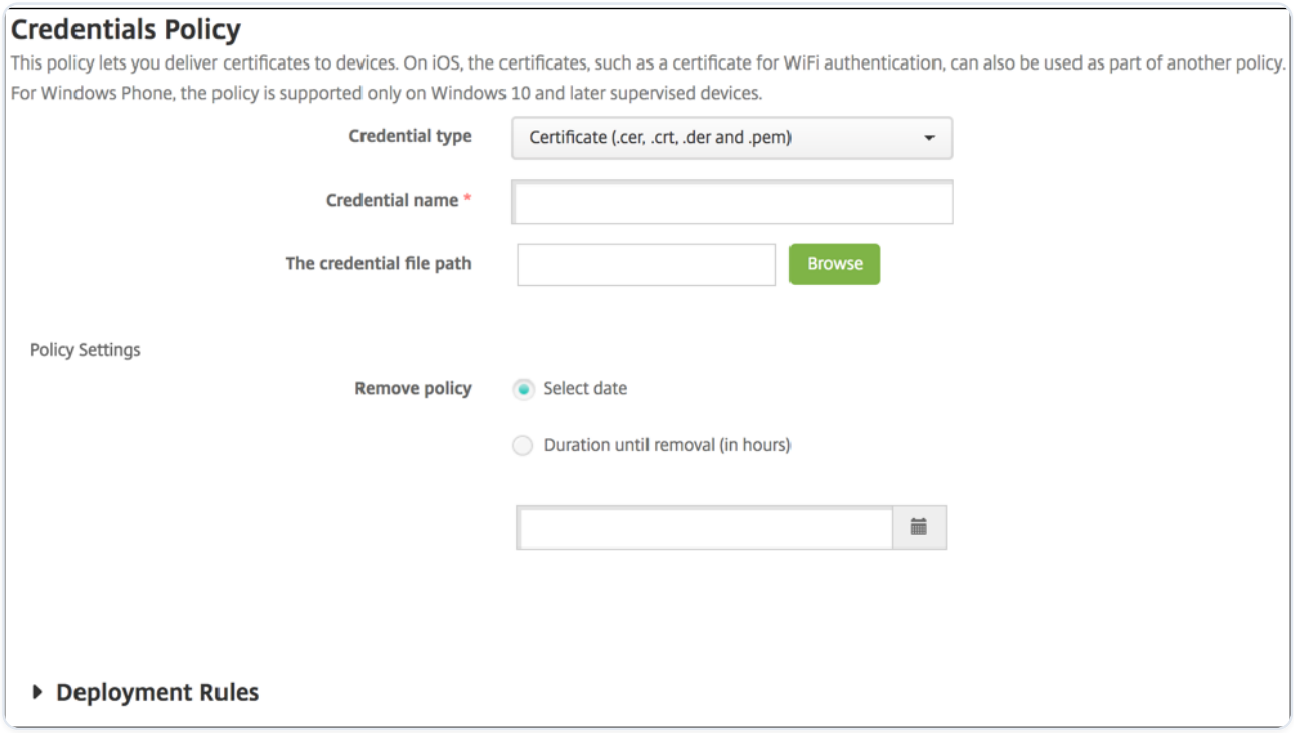
凭据设备策略

凭据设备策略指向在 Citrix 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。有关凭据的更多信息，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，本文对此进行了介绍。

> **注意：**
>
> 在创建此策略之前，您需要计划用于每个平台的凭据信息，以及任何证书和密码。
>
> 要添加或配置此策略，请转到“**配置 > 设备策略**”。有关详细信息，请参阅设备策略。

iOS 设置

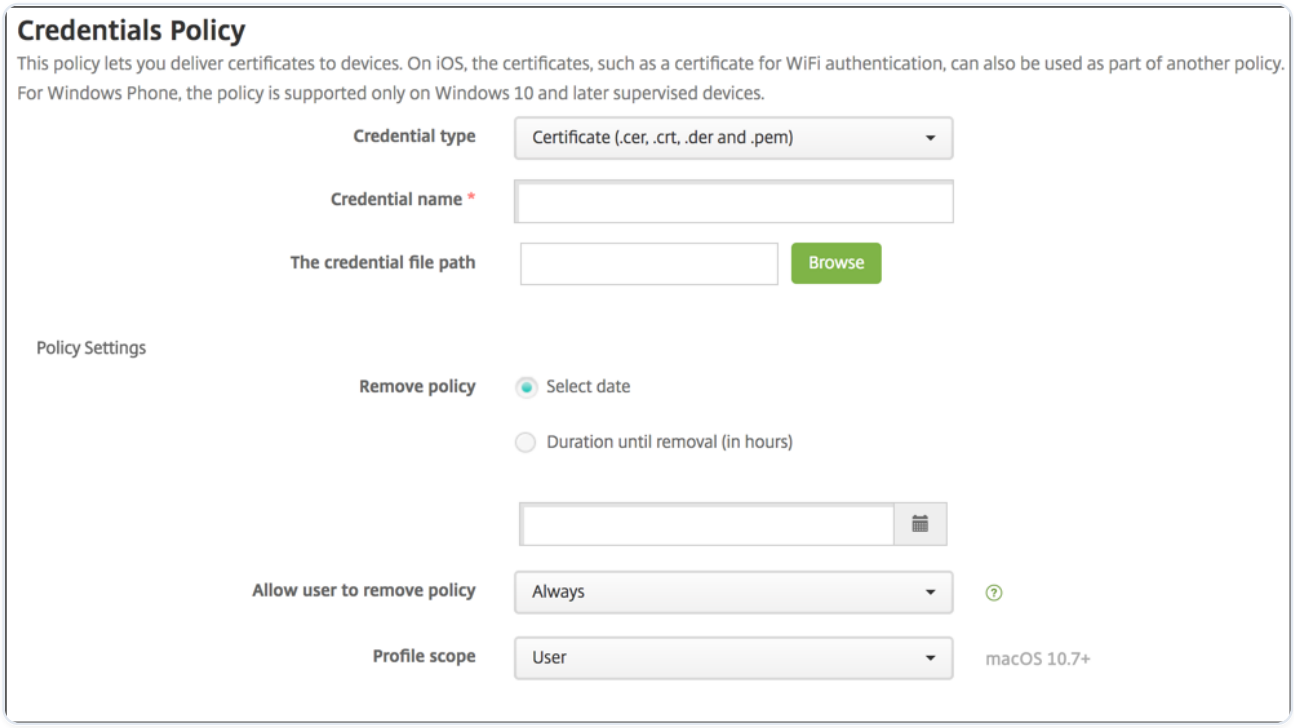


配置以下设置：

- **凭据类型：** 在下拉列表中单击要与此策略一起使用的凭据类型，然后为所选凭据输入以下信息：
  - **证书**
    - **凭据名称：** 为凭据输入一个唯一的名称。
    - **凭据文件路径：** 通过单击“浏览”并导航到文件位置来选择凭据文件。
  - **密钥库**
    - **凭据名称：** 为凭据输入一个唯一的名称。
    - **凭据文件路径：** 通过单击“浏览”并导航到文件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：** 单击下拉列表中要使用的证书。
  - **凭据提供程序**
    - **凭据提供程序：** 单击下拉列表中凭据提供程序的名称。
- **策略设置**

- **删除策略：** 选择一种计划策略删除的方法。可用选项为“**选择日期**”和“**删除前持续时间（小时）**”
  - **选择日期：** 单击日历以选择要删除的具体日期。
  - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
- **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。iOS 不可用。

macOS 设置



配置以下设置：

- **凭据类型：** 单击下拉列表中要与此策略一起使用的凭据类型，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**”并导航到文件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**”并导航到文件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：**单击下拉列表中要使用的证书。

  - **凭据提供程序**

    - **凭据提供程序：**单击下拉列表中的凭据提供程序名称。

- **策略设置**

  - **删除策略：**选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”

    - **选择日期：**单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），表示策略删除发生前的持续时间。

  - **允许用户删除策略：**您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 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 及更高版本上可用。

Android 设置



配置以下设置：

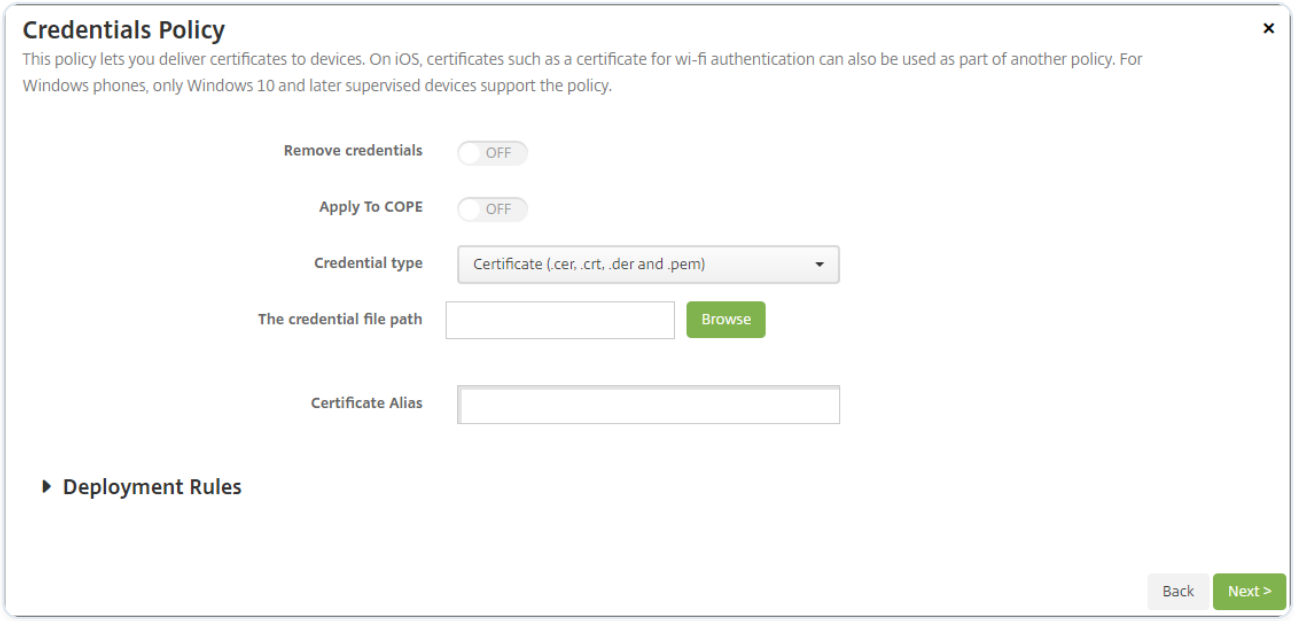
- **凭据类型：** 在下拉列表中单击要与此策略一起使用的凭据类型，然后为所选凭据输入以下信息：

  - **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”选择凭据文件，然后导航到文件位置。

- **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**选择凭据文件，然后导航到文件位置。
  - **密码：** 键入凭据的密钥库密码。
- **服务器证书**
  - **服务器证书：** 在下拉列表中单击要使用的证书。
- **凭据提供程序**
  - **凭据提供程序：** 单击下拉列表中的凭据提供程序名称。

Android 企业设置



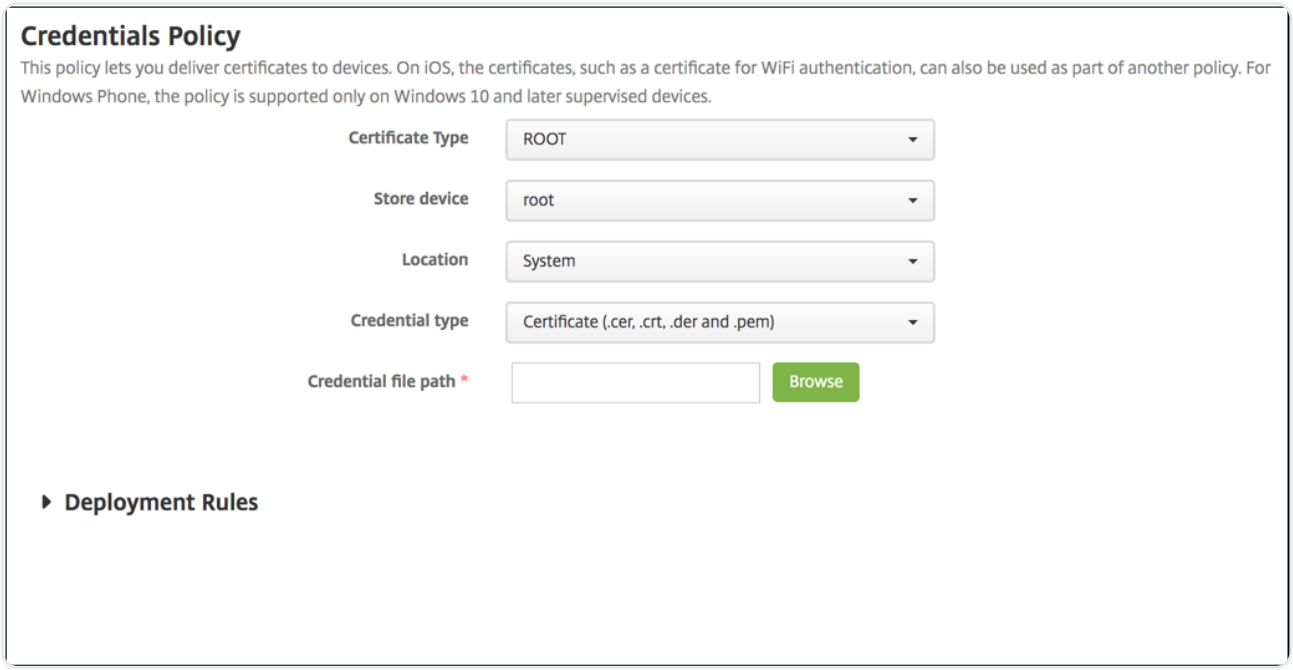
配置这些设置以确定凭据设置的应用方式：

- **移除凭据：** 设置为“**开**”以配置以下设置。默认值为“**关**”。
  - **移除用户凭据：** 从托管密钥库中移除证书。默认值为“**关**”。
  - **移除受信任的根证书：** 卸载所有非系统 CA 证书。默认值为“**关**”。
- **应用于具有工作资料的完全托管设备/公司拥有的设备上的工作资料：** 允许您为具有工作资料的完全托管设备配置凭据策略设置。当此设置设置为“**开**”时，请选择以下设置之一。此策略仅适用于设备上的工作资料。

配置凭据设置：

- **凭据类型：** 单击下拉列表中要与此策略一起使用的凭据类型，然后为所选凭据输入以下信息：
  - **证书**
    - **凭据名称：** 为凭据键入一个唯一的名称。
    - **凭据文件路径：** 通过单击“**浏览**”并导航到文件位置来选择凭据文件。
  - **密钥库**
    - **凭据名称：** 为凭据键入一个唯一的名称。
    - **凭据文件路径：** 通过单击“**浏览**”然后导航到文件位置来选择凭据文件。
    - **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更容易访问证书。在 Android Enterprise 托管配置设备策略中配置证书别名。然后，在凭据设备策略的“**证书别名**”字段中键入该别名。应用程序将检索证书并验证 VPN，而无需用户执行任何操作。
  - **服务器证书**
    - **服务器证书：** 在下拉列表中单击要使用的证书。
  - **凭据提供程序**
    - **凭据提供程序：** 在下拉列表中单击凭据提供程序的名称。
    - **使用证书的应用程序：** 要指定可从此提供程序静默访问凭据的应用程序：单击“**添加**”，选择一个应用程序，然后单击“**保存**”。
    - **证书别名：** 证书别名使应用程序更容易访问证书。在 Android Enterprise 托管配置设备策略中配置证书别名。然后，在凭据设备策略的“**证书别名**”字段中键入该别名。应用程序将检索证书并验证 VPN，而无需用户执行任何操作。

视窗桌面/平板电脑设置



- **证书类型：** 在下拉列表中单击“**ROOT**”或“**CLIENT**”。
- 如果单击“**ROOT**”，请配置以下设置：
  - **存储设备：** 在下拉列表中单击“**root**”、“**My**”或“**CA**”，以指定凭据证书存储的位置。“**My**”将证书存储在用户的证书存储中。
  - **位置：** 对于 Windows 10 和 Windows 11 平板电脑，“**System**”是唯一的位置。
  - **凭据类型**：对于 Windows 10 和 Windows 11 平板电脑，**证书**是唯一支持的凭据类型。
  - **凭据文件路径**：通过单击“**浏览**”并导航到文件位置来选择证书文件。
- 如果单击“**客户端**”，请配置以下设置：
- **位置**：对于 Windows 10 和 Windows 11 平板电脑，**系统**是唯一支持的位置。
- **凭据类型**：对于 Windows 10 和 Windows 11 平板电脑，**密钥库**是唯一支持的凭据类型。
- **凭据名称**：键入凭据的名称。此字段为必填项。
- **凭据文件路径**：通过单击“**浏览**”并导航到文件位置来选择证书文件。
- **密码**：键入与凭据关联的密码。此字段为必填项。

自定义 XML 设备策略

您可以在 Citrix Endpoint Management 中创建自定义 XML 策略，以在受支持的 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上的新软件或错误修复，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：您可以通过使用 Windows 中的开放移动联盟设备管理 (OMA DM) API 来创建自定义 XML 配置。使用 OMA DM API 创建自定义 XML 超出了本主题的范围。有关使用 OMA DM API 的更多信息，请参阅 Microsoft 开发人员网络站点上的 OMA DM 协议支持。

对于 Android Enterprise 设备：您可以通过使用 MX 管理系统 (MXMS) 来创建自定义 XML 配置。使用 MXMS API 创建自定义 XML 超出了本文的范围。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

视窗桌面/平板电脑设置

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，Citrix Endpoint Management 会检查 XML 内容语法。任何语法错误都会显示在内容框下方。在继续之前修复所有错误。

如果没有语法错误，将显示 **自定义 XML 策略** 分配页面。

使用 Windows AutoPilot 设置和配置设备

Windows AutoPilot 是一系列技术，用于设置和预配置新设备，使其为高效使用做好准备。您可以使用 Windows AutoPilot 重置、重新利用和恢复设备。AutoPilot 有助于消除当前操作系统部署的一些复杂性。使用 AutoPilot 可将任务简化为一组简单的设置和操作，从而使您的设备能够快速高效地投入使用。

要简要了解如何在 Citrix Endpoint Management 中使用 Windows AutoPilot，请观看此视频。

<iframe src="https://www.youtube.com/embed/DFCeF68NXM0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

先决条件

- 在 Azure Active Directory 门户中配置的公司品牌。
- 公司拥有 Azure Active Directory Premium P1 或 P2 订阅。
- 将 Azure Active Directory 配置为 Citrix Endpoint Management 的 IdP 类型。在 Citrix Endpoint Management 控制台中，转到 **设置 > 身份提供程序 (IDP)**。
- 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。
- 设备可以访问互联网。

有关配置先决条件的更多信息，请参阅 Microsoft Windows AutoPilot 文档：`<https://docs.microsoft.com>`。

在 Citrix Endpoint Management 中为 AutoPilot 设备配置 Windows 自动重新部署

1. 按照步骤在自定义 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>
```

2. 在 Windows 锁定屏幕上，键入组合键 **CTRL + Windows 键 + R**。
3. 使用 Azure Active Directory 帐户登录。
4. 设备验证用户是否有权重新部署设备。然后设备会重新部署。
5. 设备使用 AutoPilot 配置更新后，用户即可登录到新配置的设备。

在 Windows 11 设备上部署单应用信息亭

> **注意：**
>
> Windows 11 设备仅支持单应用信息亭模式。

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)：您要在设备上创建的用户名。这两个实例请保持相同的设置。
- `your password_here`：用户的密码。
- `your_UWP_app_id_here`：您要在设备上部署的 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>
                <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>
```

声明式设备管理策略

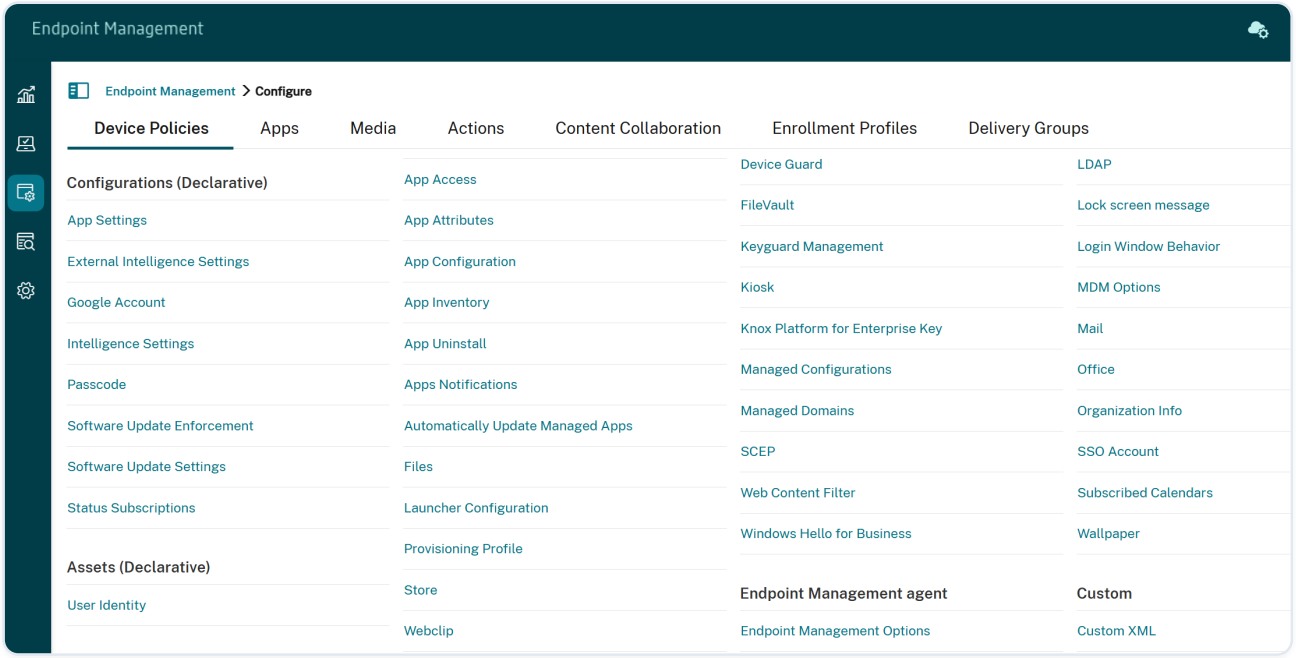
苹果在 iOS 15 中宣布了声明式设备管理 (DDM)，它采用声明式数据模型范例。这种范例允许服务器避免通常与通过 MDM 序列化命令和轮询设备相关的常见性能和可伸缩性问题。有关详细信息，请参阅利用声明式管理数据模型扩展设备。

Citrix Endpoint Management™ 现在支持 DDM，以采用 Apple 提供的最新功能。

启用 DDM 功能后，支持以下声明式设备策略：

- 应用程序设置
- 外部智能设置
- Google 帐户
- 智能设置
- 密码设备策略

- 软件更新强制执行
- 软件更新设置
- 状态订阅
- 用户身份



应用设置设备策略

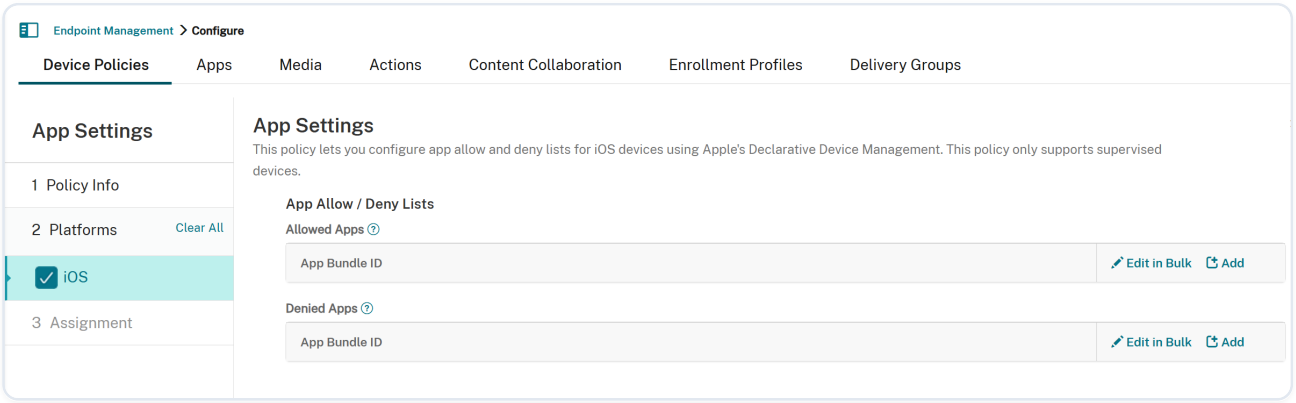
应用设置设备策略允许您使用 Apple 的声明式设备管理来配置应用允许和拒绝列表。它取代了已弃用的 `allowListedAppBundleIDs` 和 `blockedAppBundleIDs` 限制密钥。此策略仅支持受监督的设备。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- CEM 版本等于或高于 **26.8.0**。
- 适用于 **iOS 27** 或更高版本以及 **iPadOS 27** 或更高版本，仅支持受监督的设备。

iOS 设置



- **应用允许/拒绝列表**
  - **允许的应用：** 如果存在，设备将仅显示或启动列表中包含捆绑 ID 的应用。包含值 `com.apple.webapp` 以允许所有网页剪辑。这适用于 App Store 应用、市场应用以及本地安装的应用（使用 Configurator、Xcode 等）。
    - **应用捆绑 ID：** 要添加应用捆绑 ID，请单击 **添加**，键入应用捆绑 ID，然后单击 **保存**。对要添加的每个应用捆绑 ID 重复此过程。您还可以单击 **批量编辑**，输入或粘贴应用捆绑 ID（每行一个或用逗号分隔），然后单击 **保存**。
  - **拒绝的应用：** 如果存在，设备将阻止显示或启动列表中包含捆绑 ID 的应用。包含值 `com.apple.webapp` 以限制所有网页剪辑。这适用于 App Store 应用、市场应用以及本地安装的应用（使用 Configurator、Xcode 等）。

> **注意：**
>
> 拒绝系统应用可能会禁用其他功能。例如，拒绝 App Store 应用可能会阻止用户接受基于用户的批量采购计划 (VPP) 的条款和条件。我们建议您配置应用允许列表或应用拒绝列表，但不要同时配置两者。

外部智能设置设备策略

外部智能设置设备策略允许您使用 Apple 的声明式设备管理来管理外部 AI 集成（例如 ChatGPT）。此策略取代了已弃用的外部智能限制密钥。此策略仅支持受监督的设备。

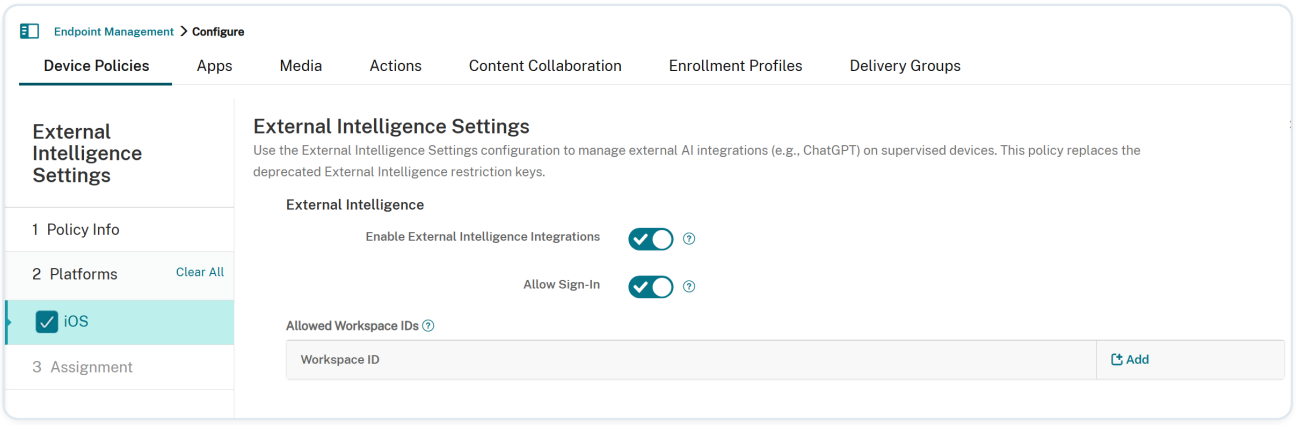
要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- CEM 版本等于或高于 **26.8.0**。

- 适用于 **iOS 26.4** 或更高版本以及 **iPadOS 26.4** 或更高版本，仅支持受监督的设备。

iOS 设置



- **外部智能**
  - **启用外部智能集成：** 如果为**关闭**，则禁用外部智能集成。默认值为**开启**。
  - **允许登录：** 如果为**关闭**，则禁用外部智能集成的登录。默认值为**开启**。
  - **允许的工作区 ID：** 字符串数组，但目前限制为单个元素。如果存在，Apple Intelligence 仅允许使用给定的外部集成工作区 ID，并且需要登录才能发出请求。用户需要登录支持登录的集成。多个值使用交集操作组合。
    - **工作区 ID：** 要添加外部智能工作区 ID，请单击**添加**，键入工作区 ID，然后单击**保存**。对要添加的每个工作区 ID 重复此过程。

Google 帐户设备策略

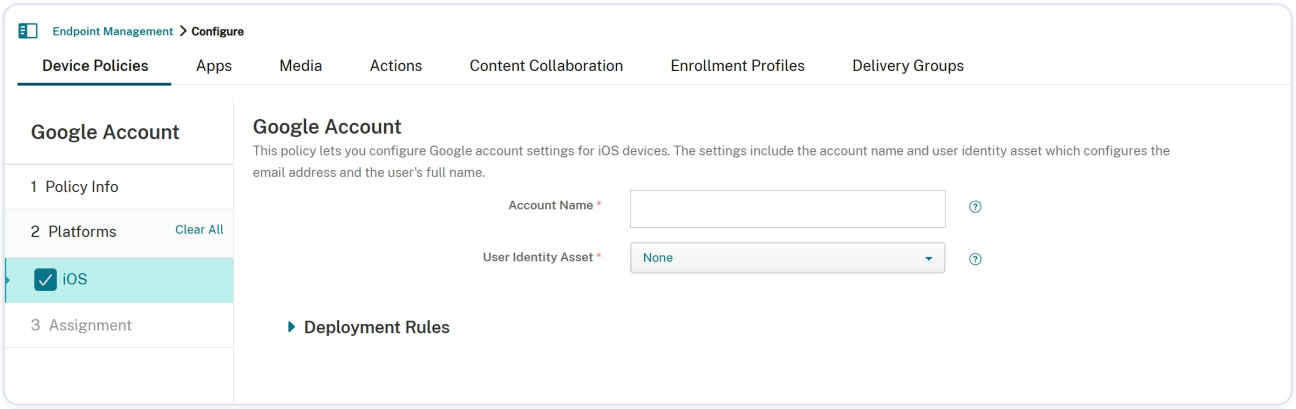
Google 帐户设备策略允许您为 iOS 设备配置 Google 帐户设置。这些设置包括帐户名称和用户身份资产，用于配置电子邮件地址和用户的全名。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- CEM 版本等于或高于 **25.5.0**。
- 用户身份策略已配置。请参阅 用户身份设备策略。

iOS 设置



- **帐户名称：** 键入 Google 帐户的名称。
- **用户身份资产：** 在列表中，选择由用户身份策略创建的用户身份资产，其中包含用户的电子邮件地址和全名。默认值为 **无**。

智能设置设备策略

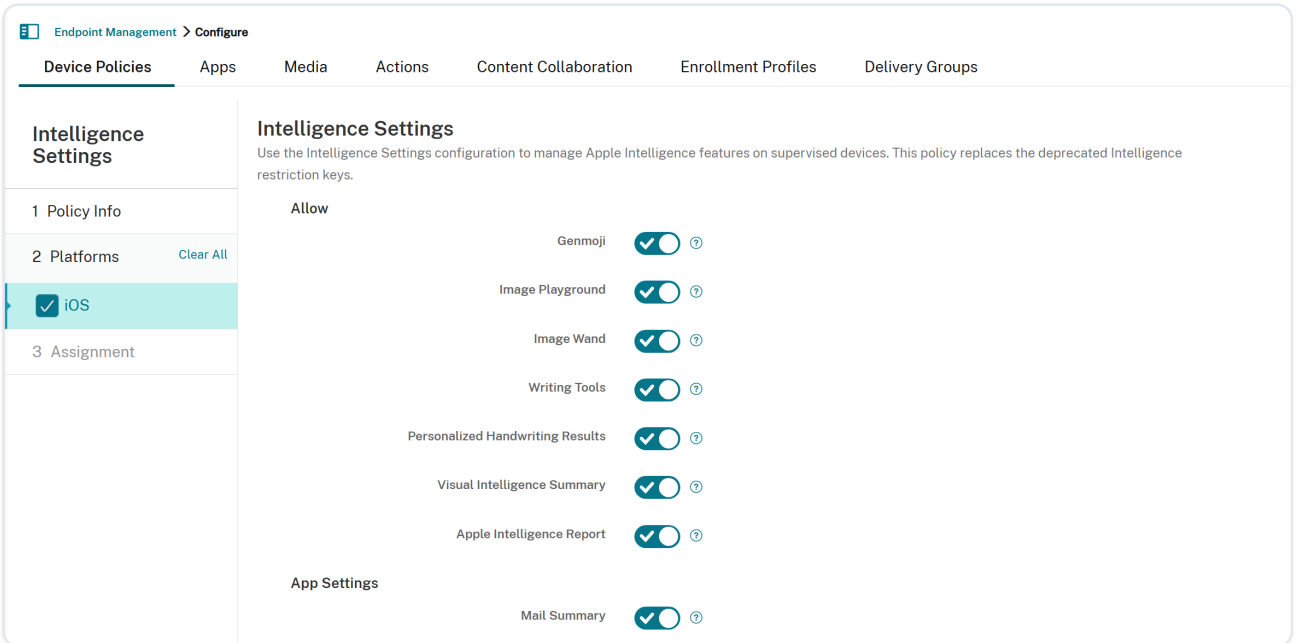
智能设置设备策略允许您使用 Apple 的声明式设备管理来管理 Apple Intelligence 功能。此策略取代了已弃用的智能限制密钥。此策略仅支持受监督的设备。

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。

先决条件

- CEM 版本等于或高于 **26.8.0**。
- 适用于 **iOS 26.4** 或更高版本以及 **iPadOS 26.4** 或更高版本，仅支持受监督的设备。

iOS 设置



- **允许**
  - **Genmoji：** 如果设置为“**关闭**”，则禁用 Genmoji。默认设置为“**开启**”。
  - **图像游乐场：** 如果设置为“**关闭**”，则禁用图像游乐场。默认设置为“**开启**”。
  - **图像魔杖：** 如果设置为“**关闭**”，则禁用图像魔杖。默认设置为“**开启**”。
  - **写作工具：** 如果设置为“**关闭**”，则禁用 Apple Intelligence 写作工具。默认设置为“**开启**”。
  - **个性化手写结果：** 如果设置为“**关闭**”，则禁用个性化手写结果，阻止系统生成用户手写文本。默认设置为“**开启**”。
  - **视觉智能摘要：** 如果设置为“**关闭**”，则禁用视觉智能摘要。默认设置为“**开启**”。
  - **Apple Intelligence 报告：** 如果设置为“**关闭**”，则禁用 Apple Intelligence 报告。默认设置为“**开启**”。
- **应用设置**
  - **邮件摘要**：如果**关闭**，则禁用邮件摘要。默认值为**开启**。
  - **邮件智能回复**：如果**关闭**，则禁用邮件智能回复。默认值为**开启**。
  - **备忘录转录**：如果**关闭**，则禁用备忘录转录。默认值为**开启**。
  - **备忘录转录摘要**：如果**关闭**，则禁用备忘录转录摘要。默认值为**开启**。
  - **Safari 摘要**：如果**关闭**，则禁用 Safari 摘要。默认值为**开启**。
- **强制**
  - **强制仅限设备听写**：如果**开启**，则强制执行仅限设备听写。默认值为**关闭**。
  - **强制仅限设备翻译**：如果**开启**，则强制执行仅限设备翻译。默认值为**关闭**。

密码设备策略

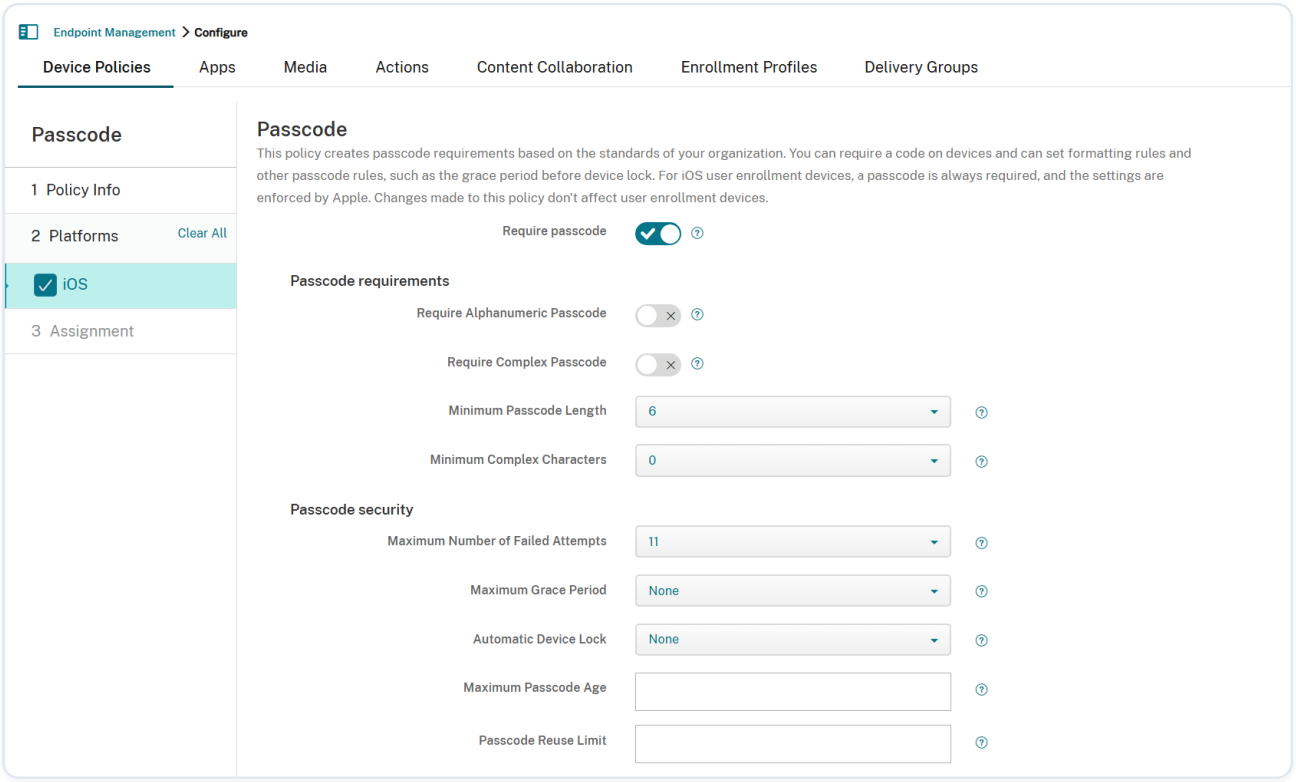
密码设备策略根据您组织的标准创建密码要求。您可以要求设备使用密码，并可以设置格式规则和其他密码规则，例如设备锁定前的宽限期。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- CEM 版本等于或高于 **25.5.0**。

iOS 设置



- **要求密码：** 选择此选项以要求密码并显示 iOS 密码设备策略的配置选项。如果为 **开**，则要求用户设置密码，对密码的长度或质量没有任何要求，并且页面会展开，让您可以配置密码要求和密码安全设置。默认值为 **开**。
- **密码要求**
  - **要求字母数字密码：** 选择是否要求密码至少包含一个字母字符和一个数字。默认值为 **关**。
  - **要求复杂密码：** 选择是否要求复杂密码。复杂密码是指不包含重复字符或递增或递减字符（例如 123 或 CBA），并且必须至少包含一个非数字和非字母字符的密码。默认值为 **关**。
  - **最小密码长度：** 选择密码可以包含的最小字符数。默认值为 **6**。
  - **最小复杂字符数：** 选择密码中复杂字符的最小数量。复杂字符是指除数字或字母以外的字符，例如 &、%、$ 和 #。默认值为 **0**。
- **密码安全**
  - **最大失败尝试次数：** 选择系统允许用户在 iOS 擦除设备之前失败的密码尝试次数。如果您不更改此设置，在六次失败尝试后，设备会强制延迟一段时间，然后用户才能再次输入密码。每次失败尝试都会增加延迟时间。在最后一次失败尝试后，系统会安全擦除 iOS 设备上的所有数据和设置。密码延迟时间从第六次尝试后开始，因此如果此值为六或更低，系统将没有延迟时间，并在用户超出限制后立即触发擦除或锁定。默认值为 **11**。
  - **最长宽限期：** 选择用户无需密码即可解锁设备的最长期间。选择 **立即** 表示没有宽限期，设备会立即要求密码。默认值为 **无**，这意味着用户可以选择任何期间。

- **自动设备锁定：** 选择设备在系统自动锁定之前可以处于空闲状态的最长时间。当设备达到此限制时，设备将锁定，用户必须输入密码才能解锁。默认值为**无**，这意味着用户可以选择任何时间段。
- **密码最长使用期限：** 选择密码可以保持不变的最长天数。在此天数之后，系统会强制用户在解锁设备之前更改密码。有效值为 0–730。值为**0**表示强制立即更改密码。默认值为空，这意味着没有密码使用期限限制。
- **密码重用限制：** 选择系统在验证新密码时检查的历史密码条目数。如果新密码与指定密码历史记录范围内的先前使用过的密码匹配，设备将拒绝该新密码。有效值为 1–50。默认值为**空**，这意味着系统不执行历史检查。

> **注意：**
>
> 如果将相同的设置作为 MDM 配置文件和声明性配置发送到设备，则适用与通过多个配置文件传递设置相同的规则。例如，如果通过配置文件（通过密码策略）和配置（通过声明性密码策略）配置密码策略，则策略将合并并强制执行最严格的设置。

软件更新强制执行设备策略

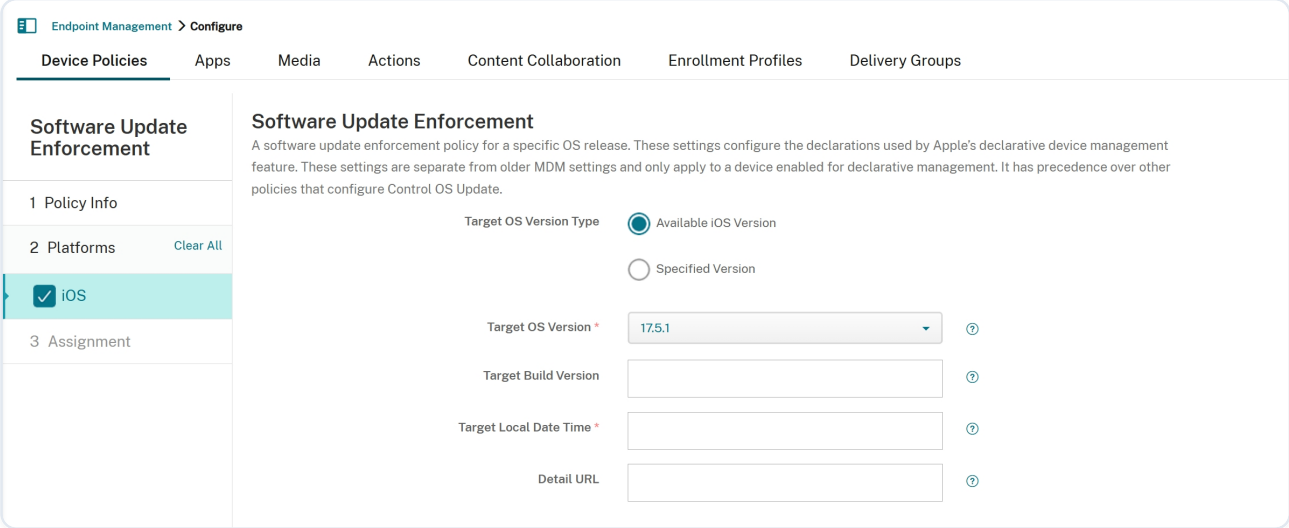
针对特定操作系统版本的软件更新强制执行设备策略使 IT 管理员能够管理 iOS 设备更新，从而控制应用哪些更新并设置完成所有更新的截止日期。这些设置配置了 Apple 声明式设备管理功能所使用的声明。这些设置与旧的 MDM 设置是分开的，并且仅适用于已启用声明式管理的设备。对于相同的设置，它优先于控制操作系统更新策略。

要添加或配置此策略，请转到**配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- CEM 版本等于或大于 **25.5.0**。
- 适用于 **iOS 17.0** 或更高版本以及 **iPadOS 17.0** 或更高版本。

iOS 设置



- **目标操作系统版本类型：** 指定如何配置目标操作系统版本。默认值为**可用 iOS 版本**。
  - **可用 iOS 版本：** 如果**开启**，请在**目标操作系统版本**中列出可用的目标操作系统版本。
  - **指定版本：** 如果**开启**，请手动输入采用建议格式的操作系统版本。
- **目标操作系统版本：（必填）** 选择或键入要在适当时间将设备更新到的目标操作系统版本。这是操作系统版本号，例如 17.7。它还可以包含补充版本标识符，例如 17.7.2。
- **目标内部版本号：** 键入要在适当时间将设备更新到的目标内部版本号，例如 20A242。系统在种子测试期间使用内部版本号进行测试。内部版本号可以包含补充版本标识符，例如 20A242a。如果内部版本号与 TargetOSVersion 键中指定的目标操作系统版本不一致，则目标操作系统版本优先。
- **目标本地日期时间：（必填）** 键入指定何时强制安装软件更新的本地日期时间值。使用 yyyy-mm-ddThh:mm:ss 格式，该格式源自 RFC3339，但不包含时区偏移。如果用户在此时间之前未触发软件更新，设备将强制安装它。
- **详细信息 URL：** 键入显示组织提供的有关强制更新的详细信息的网页 URL。

> **注意：**
>
> 软件更新强制执行策略和控制操作系统更新策略都可以管理设备上的操作系统更新。但是，软件更新强制执行策略优先于控制操作系统更新策略。如果两个策略都使用相同的设置进行部署，则控制操作系统更新策略中的配置将被覆盖且不会生效。有关详细信息，请参阅过渡到声明式设备管理。

> 此外，软件更新强制策略与控制操作系统更新策略之间存在一些差异。

策略类型	软件更新强制	控制操作系统更新
设备类型	受监管或非受监管设备	受监管设备
强制更新截止日期	✓	✗
输入帮助 URL	✓	✗
指定内部版本号	✓	✗
自动部署最新更新	✗	✓
最低支持版本	iOS 17.0	iOS 10.3 (受监管)

软件更新设置设备策略

软件更新设置设备策略可用于推迟操作系统更新并控制用户如何在“系统设置”中手动与软件更新交互。此策略仅支持受监管设备。

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。

先决条件

- CEM 版本等于或高于 **25.5.0**。
- 适用于 **iOS 18.0** 或更高版本以及 **iPadOS 18.0** 或更高版本，仅支持受监管设备。

iOS 设置

](/en-us/citrix-endpoint-management/media/software-update-setting-ios-settings1.png)

- **自动操作**
  - **下载：** 指定用户是否可以控制可用更新的自动下载。默认值为**允许**。
    - **允许** - 用户可以启用或禁用自动下载。
    - **始终开启** - 自动下载始终启用。
    - **始终关闭** - 自动下载始终禁用。
  - **安装操作系统更新：** 指定用户是否可以控制可用更新的自动安装。默认值为**允许**。
    - **允许** - 用户可以启用或禁用自动安装。
    - **始终开启** - 自动安装始终启用。
    - **AlwaysOff** - 自动安装始终禁用。

  - **Install Security Updates:** 指定用户是否可以控制可用安全更新的自动安装。默认值为 **Allowed**。
    - **Allowed** - 用户可以启用或禁用自动安装。
    - **AlwaysOn** - 自动安装始终启用。
    - **AlwaysOff** - 自动安装始终禁用。

- **延迟**
  - **Combined Period in Days:** 指定在设备上延迟主要或次要操作系统软件更新的天数。设置后，软件更新只会在软件更新发布后经过指定延迟时间才会出现。适用于 iOS 18 及更高版本。有效值为 0–90。默认值为 **0**，表示不预期延迟。

- **推荐节奏**
  - **Recommended Cadence:** 指定设备如何向用户显示软件更新。当有多个更新可用时，设备行为如下。默认值为 **All**。
    - **All** - 显示所有软件更新版本。
    - **Oldest** - 仅显示最旧（编号最低）的软件更新版本。
    - **Newest** - 仅显示最新（编号最高）的软件更新版本。

- **通知**
  - **Notifications:** 如果为 **On**，设备将显示所有软件更新强制执行通知。如果为 **Off**，设备将仅显示在强制执行截止日期前一小时触发的通知以及重新启动倒计时通知。默认值为 **On**。

- **快速安全响应**
  - **启用：** 如果设置为“**关**”，则不会向用户提供快速安全响应以进行安装。系统仍可以使用 `com.apple.configuration.softwareupdate.enforcement.specific` 配置安装快速安全响应。如果设置为“**开**”，则系统会向用户提供快速安全响应。默认设置为“**开**”。
  - **启用回滚：** 如果设置为“**关**”，则系统不会向用户提供快速安全响应回滚。如果设置为“**开**”，则系统会向用户提供快速安全响应回滚。默认设置为“**开**”。

状态订阅设备策略

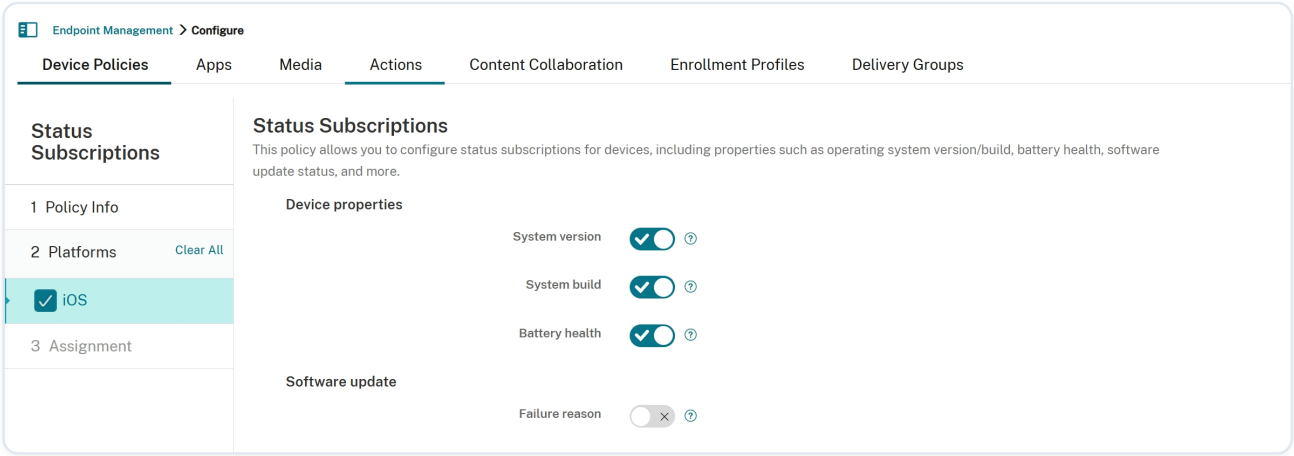
状态订阅设备策略允许您为设备配置状态订阅，包括操作系统版本/内部版本、电池健康状况、软件更新状态等属性。

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。

先决条件

- CEM 版本等于或高于 **25.5.0**。

iOS 设置



- **设备属性**
  - **系统版本：如果设置为开**，设备将报告操作系统的版本（例如，18.0），该版本将显示在“设备属性”的“系统信息”部分中。这很有用，因为当版本升级时，设备会自动报告。默认设置为**开**。适用于 iOS 15 及更高版本。
  - **系统内部版本：如果设置为开**，设备将报告操作系统的内部版本（例如，18F132），该版本将显示在“设备属性”的“系统信息”部分中。这很有用，因为当版本升级时，设备会自动报告。默认设置为**开**。适用于 iOS 15 及更高版本。
  - **电池健康状况：如果设置为开**，“设备属性”中将添加一个新设置**电池健康状况**。此设置允许管理员通过导航到**管理 > 设备 > 属性 > 电池 > 电池健康状况**来查看已注册 iOS 设备的电池健康状况。默认设置为**开**。适用于 iOS 17 及更高版本。
- **软件更新**
  - **失败原因：如果设置为开**，设备将报告操作系统更新失败的原因，该原因将显示在“设备属性”的“软件更新”信息部分中。默认设置为**关**。适用于 iOS 17 及更高版本。

用户身份设备策略

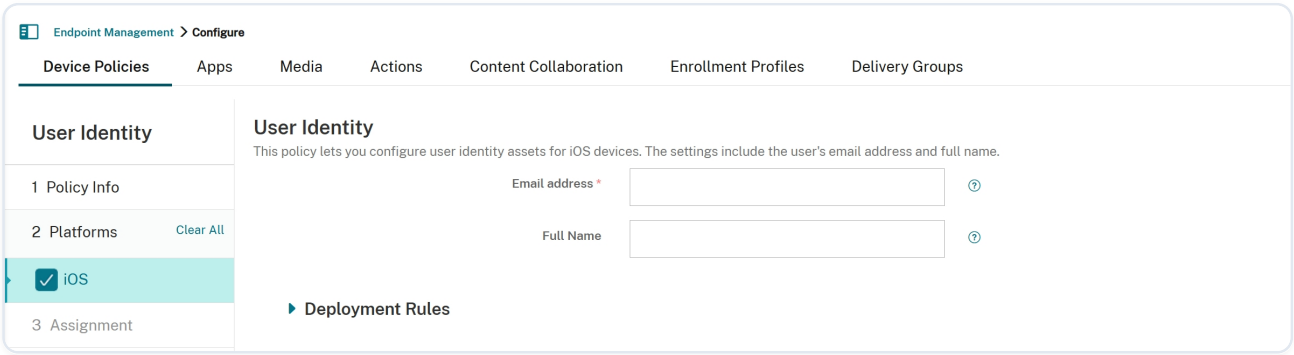
用户身份设备策略允许您为 iOS 设备配置用户身份资产。设置包括用户的电子邮件地址和全名。

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。

先决条件

- CEM 版本等于或高于 **25.5.0**。

iOS 设置



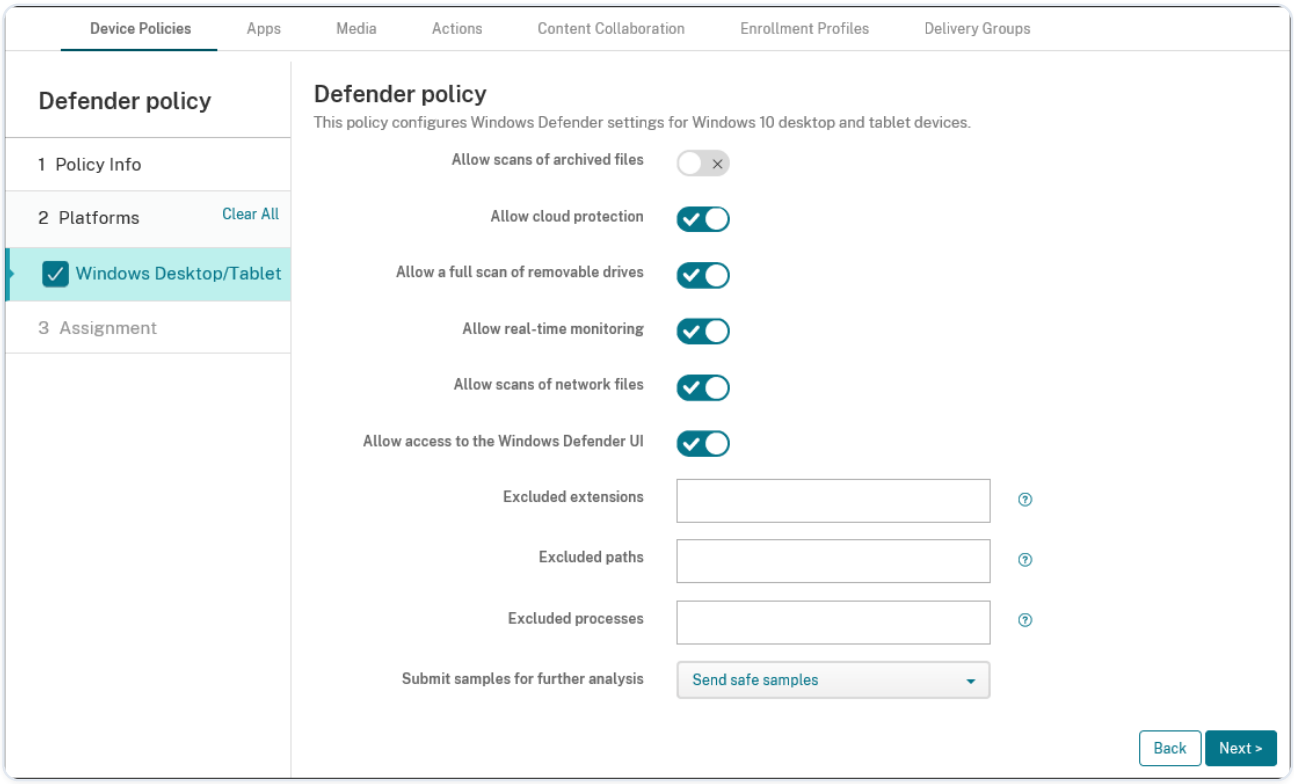
- **电子邮件地址：** 输入用户的电子邮件地址。此字段为必填项。
- **全名：** 输入用户的全名。

Defender 设备策略

Windows Defender 是 Windows 10 和 Windows 11 中包含的恶意软件防护功能。您可以使用 Citrix Endpoint Management 设备策略 Defender 来配置适用于 Windows 10 和 Windows 11 桌面及平板设备的 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。

Windows 桌面和平板电脑设置



- **允许扫描存档文件：** 允许或阻止 Defender 扫描存档文件。默认为**关闭**。

- **允许云保护：** 允许或阻止 Defender 向 Microsoft 发送有关恶意软件活动的信息。默认为**开启**。
- **允许对可移动驱动器进行完全扫描：** 允许或阻止 Defender 扫描可移动驱动器，例如 USB 闪存盘。默认为**开启**。
- **允许实时监控：** 默认为**开启**。
- **允许扫描网络文件：** 允许或阻止 Defender 扫描网络文件。默认为**开启**。
- **允许访问 Windows Defender UI：** 指定用户是否可以访问 Windows Defender 用户界面。此设置在用户设备下次启动时生效。如果此设置设为**关闭**，用户将不会收到任何 Windows Defender 通知。默认为**开启**。
- **排除的扩展名：** 要从实时或计划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：** 要从实时或计划扫描中排除的路径。要分隔路径，请使用 `|` 字符。例如，`C:\Example|C:\Example1`。
- **排除的进程：** 要从实时或计划扫描中排除的进程。要分隔进程，请使用 `|` 字符。例如，`C:\Example.exe|C:\Example1.exe`。
- **提交样本以供进一步分析：** 控制是否将可能需要进一步分析以确定其是否恶意的文件发送给 Microsoft。选项包括：**始终提示**、**发送安全样本**、**从不发送**、**发送所有样本**。默认为**发送安全样本**。

设备防护设备策略

设备防护是 Windows 10 和 Windows 11 中提供的一项安全功能。此功能通过使用 **Windows Hypervisor** 在设备上支持安全服务，从而启用基于虚拟化的安全性。设备防护策略可启用安全启动、UEFI 锁定和虚拟化等安全功能。

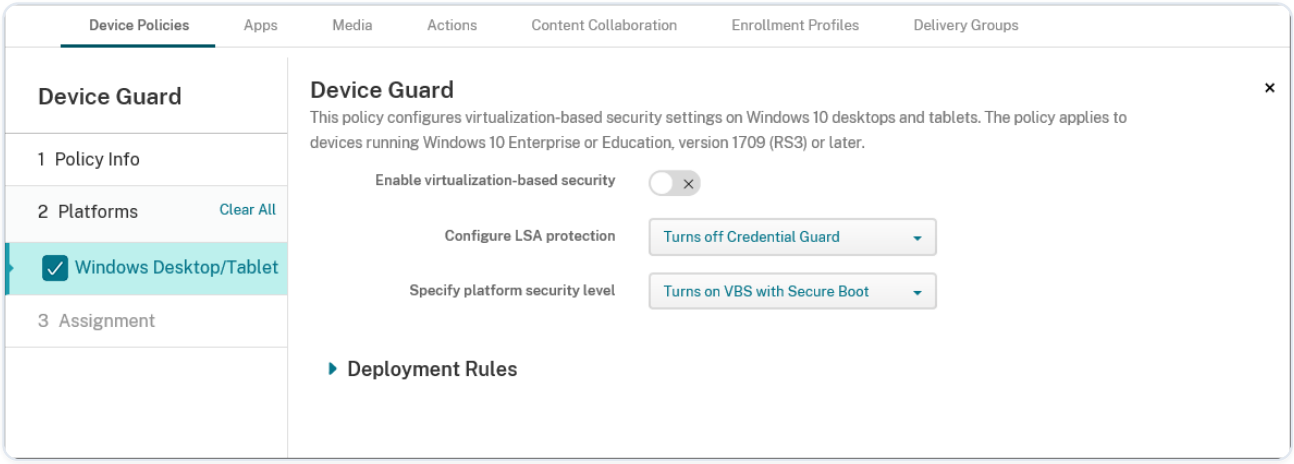
先决条件

- 具有企业版或教育版许可证的 Windows 10 和 Windows 11 桌面和平板电脑
- 在 Windows 中启用了设备防护

  有关设备防护的更多信息，请参阅 `<https://docs.microsoft.com/zh-cn/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 桌面和平板电脑设置



- **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 Hypervisor 来支持安全服务。
- **配置 LSA 保护：** 允许您配置 Credential Guard。此设置允许用户在下次重新启动时启用基于虚拟化的 Credential Guard，以帮助保护凭据。选项包括**关闭 Credential Guard**、**通过 UEFI 锁定启用 Credential Guard** 和 **不通过 UEFI 锁定启用 Credential Guard**。默认值为**关闭 Credential Guard**。
- **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。选项包括**通过安全启动启用 VBS** 和 **通过安全启动和直接内存访问启用 VBS**。默认值为**通过安全启动启用 VBS**。

Citrix 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，Citrix Endpoint Management 不会将此策略部署到设备。如果安全设置不匹配，Citrix Endpoint Management 将部署该策略。

设备健康证明设备策略

在 Citrix Endpoint Management 中，您可以要求 Windows 10 和 Windows 11 设备报告其健康状况。为了报告其健康状况，设备会将特定数据和运行时信息发送到健康证明服务 (HAS) 进行分析。HAS 会创建并返回一个健康证明证书，然后设备会将其发送到 Citrix Endpoint Management。Citrix Endpoint Management 使用健康证明证书的内容来部署您已设置的自动操作。

HAS 验证的数据包括：

- AIK 存在
- BitLocker 状态
- 启动调试已启用
- 启动管理器修订列表版本
- 代码完整性已启用

- 代码完整性修订列表版本
- Apple 部署计划策略
- ELAM 驱动程序已加载
- 颁发时间
- 内核调试已启用
- PCR
- 重置计数
- 重启计数
- 安全模式已启用
- SBCP 哈希
- 安全启动已启用
- 测试签名已启用
- VSM 已启用
- WinPE 已启用

有关详细信息，请参阅 Microsoft 设备运行状况证明 CSP 页面。

您可以通过 Microsoft Cloud 或本地 Windows DHA 服务器配置 DHA，如下所示：

- 要使用 Microsoft Cloud 配置 DHA：添加设备运行状况证明策略并按照本文所述进行配置。
- 要使用本地 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照本文所述进行配置。

  要配置 DHA 服务器，请在运行 Windows Server 2016 Technical Preview 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，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

视窗桌面/平板电脑设置

如果您使用 Microsoft Cloud 配置 DHA

- **启用设备健康状况证明**：选择是否需要设备健康状况证明。默认值为“**关**”。

如果您使用本地 Windows DHA 服务器配置 DHA

- **启用设备健康状况证明**：设置为“**开**”。

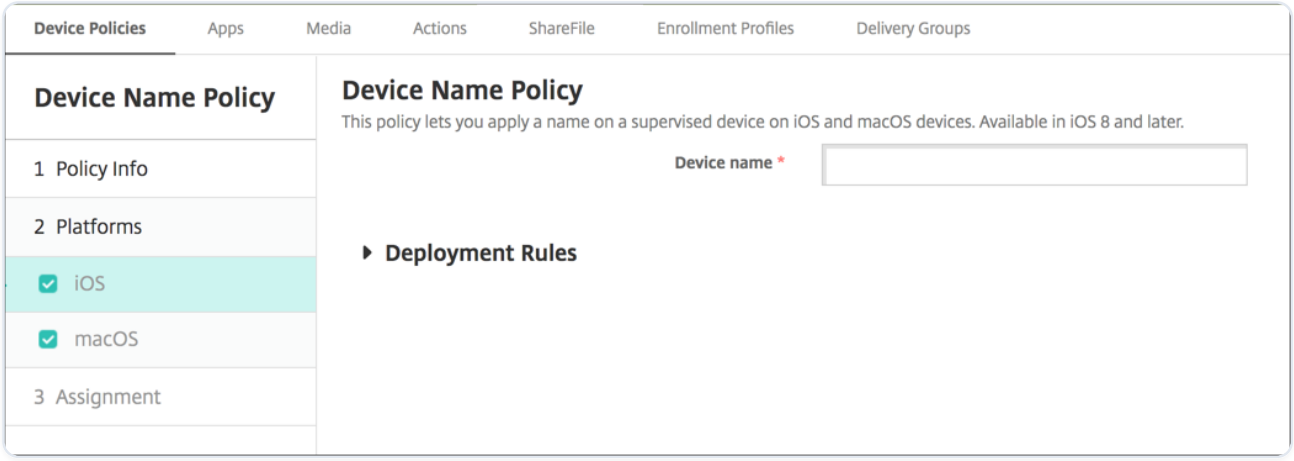
- **配置本地健康状况证明服务**：设置为“**开**”。
- **本地 DHA 服务 FQDN**：键入您设置的 DHA 服务器的完全限定域名。
- **本地 DHA API 版本**：选择安装在 DHA 服务器上的 DHA 服务版本。

设备名称策略

您可以在受监管的 iOS 和 macOS 设备上设置名称，以便轻松识别这些设备。您可以使用宏、文本或两者的组合来定义设备名称。例如，要将设备名称设置为设备的序列号，可以使用 ${device.serialnumber}。要将设备名称设置为用户名称和域的组合，可以使用 ${user.username}@example.com。有关宏的更多信息，请参阅 Citrix 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。

iOS 和 macOS 设置



- **设备名称：** 键入宏、宏组合或宏与文本的组合，以唯一命名每个设备。例如，使用 ${device.serialnumber} 将设备名称设置为每个设备的序列号，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

教育配置设备策略定义了：

- 教师设备的 Apple Classroom 应用设置。
- 用于在教师设备和学生设备之间进行客户端身份验证的证书。

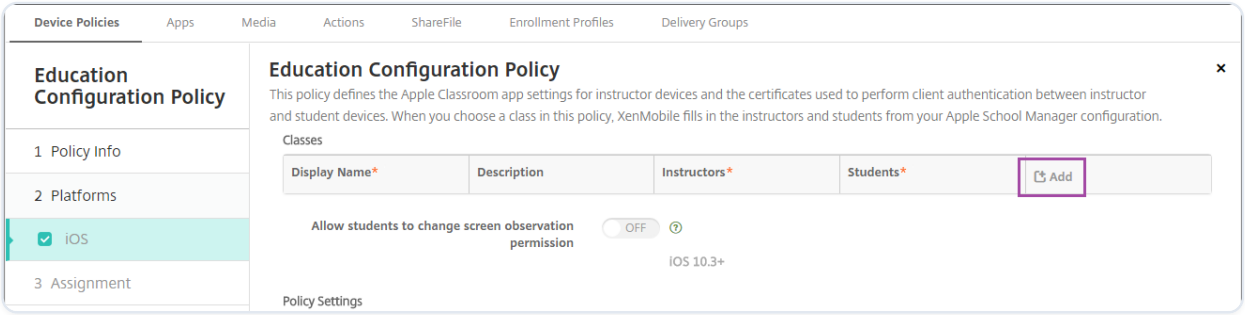
教育配置设备策略支持 iOS (iPadOS) 设备。

当您在此策略中选择一个班级时，Citrix Endpoint Management 控制台会根据您的 Apple School Manager 配置填充教师和学生信息。如果此策略中的 Apple Classroom 应用设置对所有班级都相同，则创建一个策略即可。

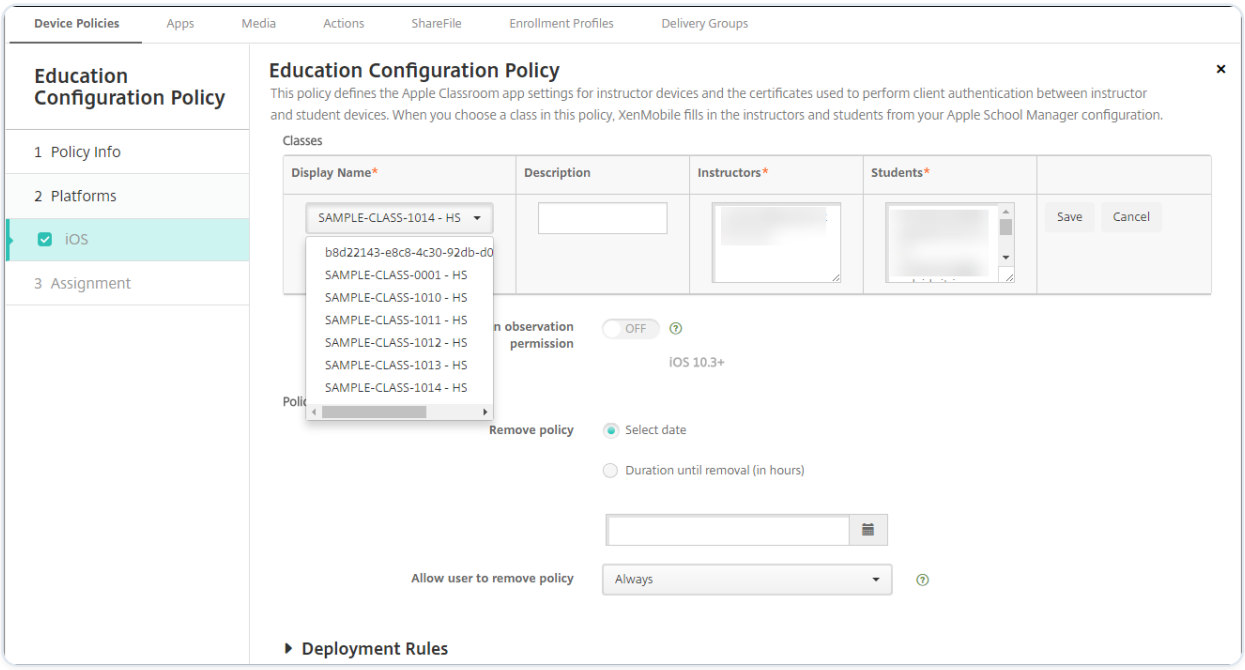
要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

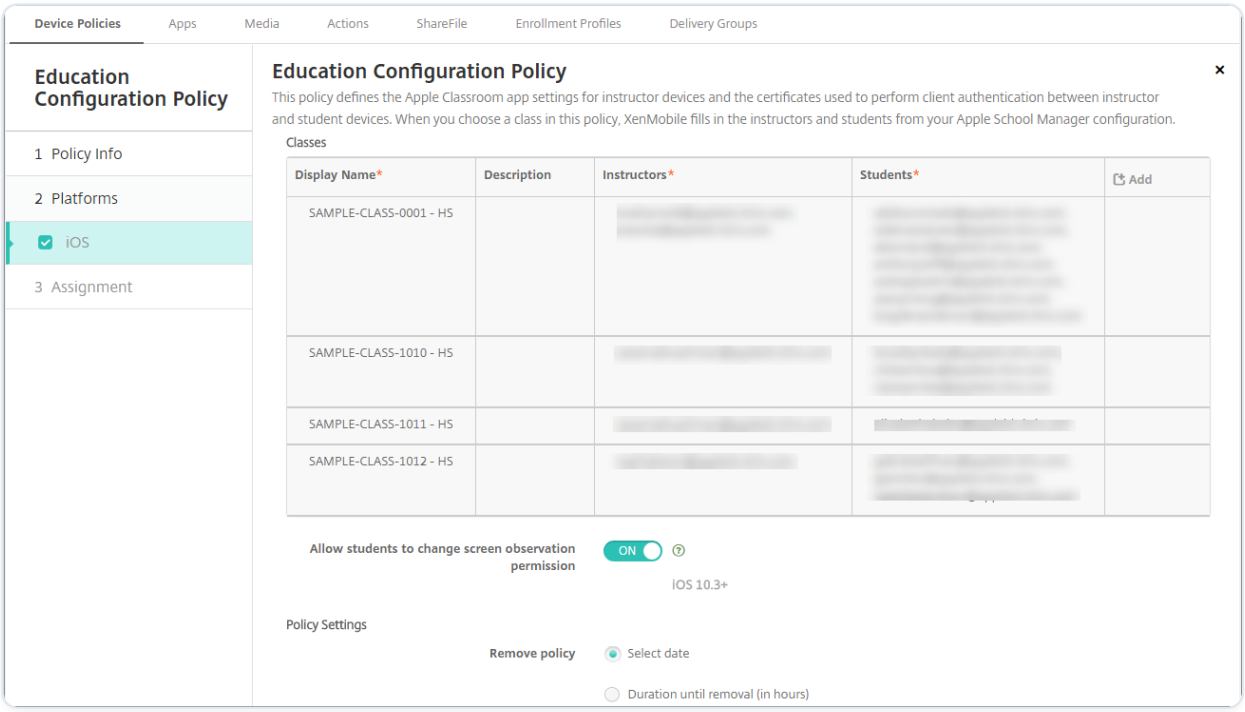
- **班级：要添加班级，请单击添加。**



然后，单击**显示名称**列表。将显示从您连接的 Apple School Manager 帐户获取的班级列表。



当您从**显示名称**中选择一个班级时，Citrix Endpoint Management 会填充教师和学生信息。继续添加班级。

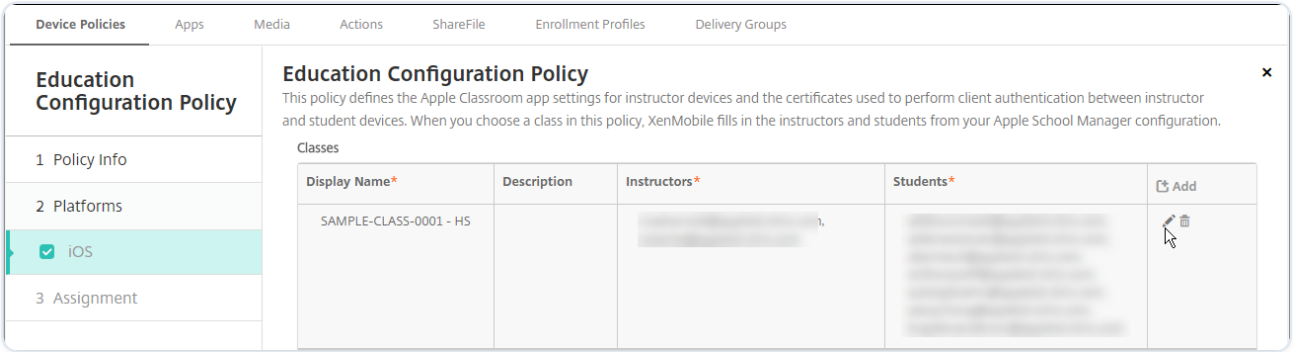


- **允许学生更改屏幕观察权限：如果设置为开**，则已注册到受管班级的学生可以选择是否允许其教师观察其设备屏幕。默认设置为**关**。
- **策略设置**
  - **删除策略**：选择一种安排策略删除的方法。可用选项为“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期**：单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）**：键入一个数字（以小时为单位），直到策略删除发生。

在策略中编辑班级信息

您可以为班级添加说明（即 Classroom 应用中的“显示名称”）。您还可以添加或删除教师和学生。Citrix Endpoint Management 不会将此类更改保存到您的 Apple School Manager 帐户。有关详细信息，请参阅与 Apple Education 功能集成中的“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。



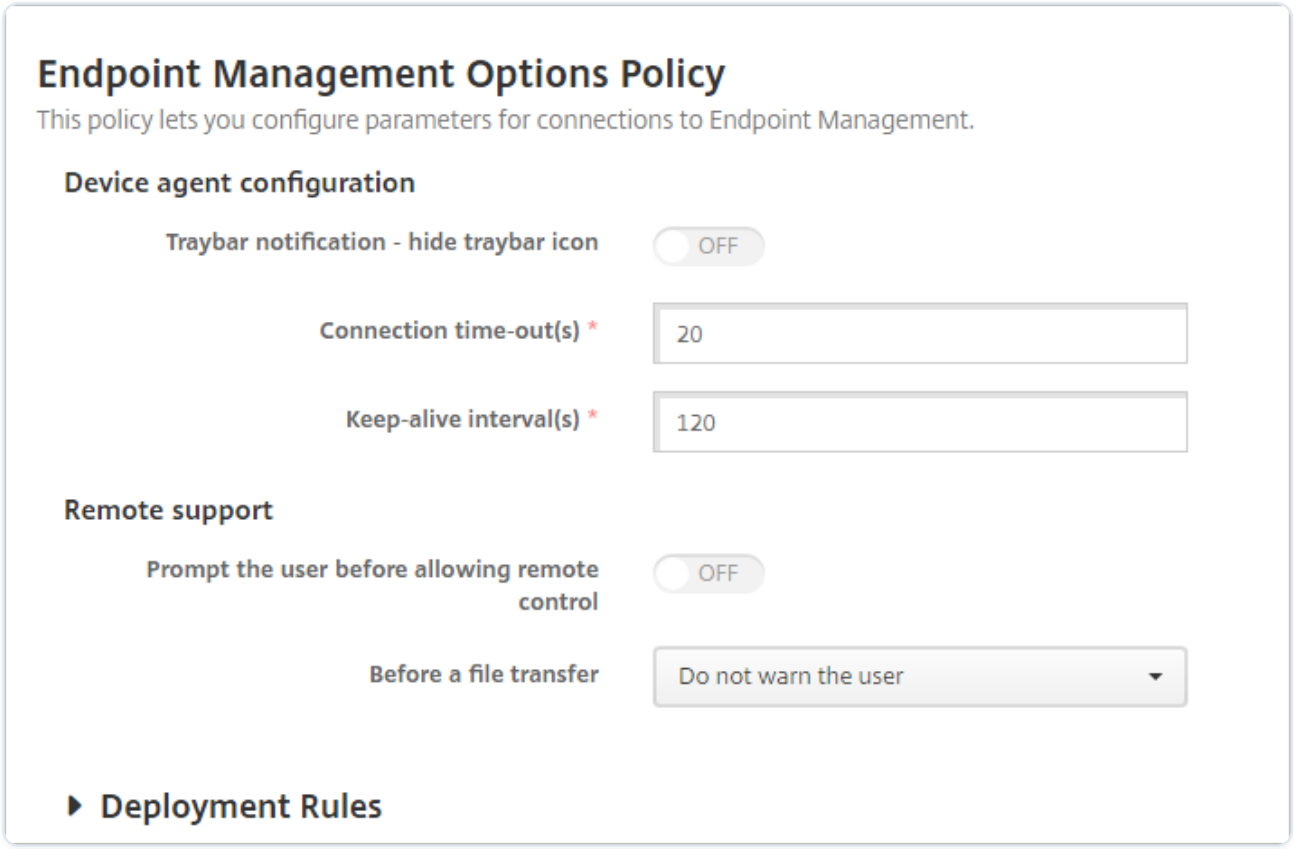
要从策略中删除班级，请将鼠标悬停在要删除的班级的“**添加**”列上，然后单击垃圾桶图标。

Endpoint Management 选项设备策略

您可以添加 Endpoint Management 选项策略，以配置从 Android 设备连接到 Citrix Endpoint Management 时的 Citrix Secure Hub 行为。

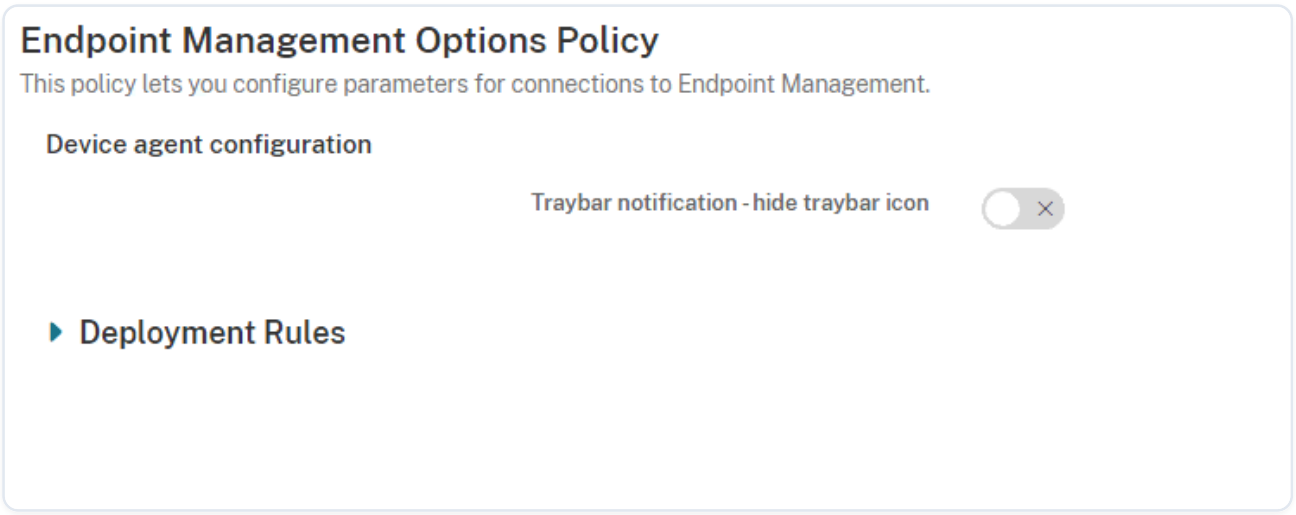
要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅设备策略。

Android 设置



- **托盘栏通知 - 隐藏托盘栏图标：** 选择托盘栏图标是隐藏还是可见。默认值为“**关**”。
- **连接：超时：** 键入连接在超时前可以保持空闲状态的秒数。默认值为 20 秒。
- **保持活动间隔：** 键入保持连接打开的秒数。默认值为 120 秒。
- **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**”。
- **文件传输前：** 在下拉列表中单击是警告用户文件传输，还是请求用户许可。可用值包括：**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**。

Android 企业版设置



从 Android 7 版开始支持。

托盘栏通知 - 隐藏托盘栏图标： 选择托盘栏图标是隐藏还是可见。默认值为“**关**”。

> **注意：**
>
> 如果您想为运行 Android Enterprise 的设备启用 VPN 服务，则可以在 **VPN 设备策略**中启用**启用始终开启的 VPN** 选项。如果您已在早期版本中在 **Endpoint Management 选项设备策略**中启用了**启用始终开启的 VPN** 选项，请确保在 **VPN 设备策略**中再次启用该选项。

Citrix Endpoint Management 卸载设备策略

您可以在 Citrix Endpoint Management 中添加设备策略，以从 Android 设备卸载 Citrix Endpoint Management。部署后，此策略会从部署组中的所有设备卸载 Citrix 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

- **从设备卸载 Citrix Endpoint Management：** 选择是否从部署此策略的每台设备卸载 Citrix Endpoint Management。默认设置为“**关**”。

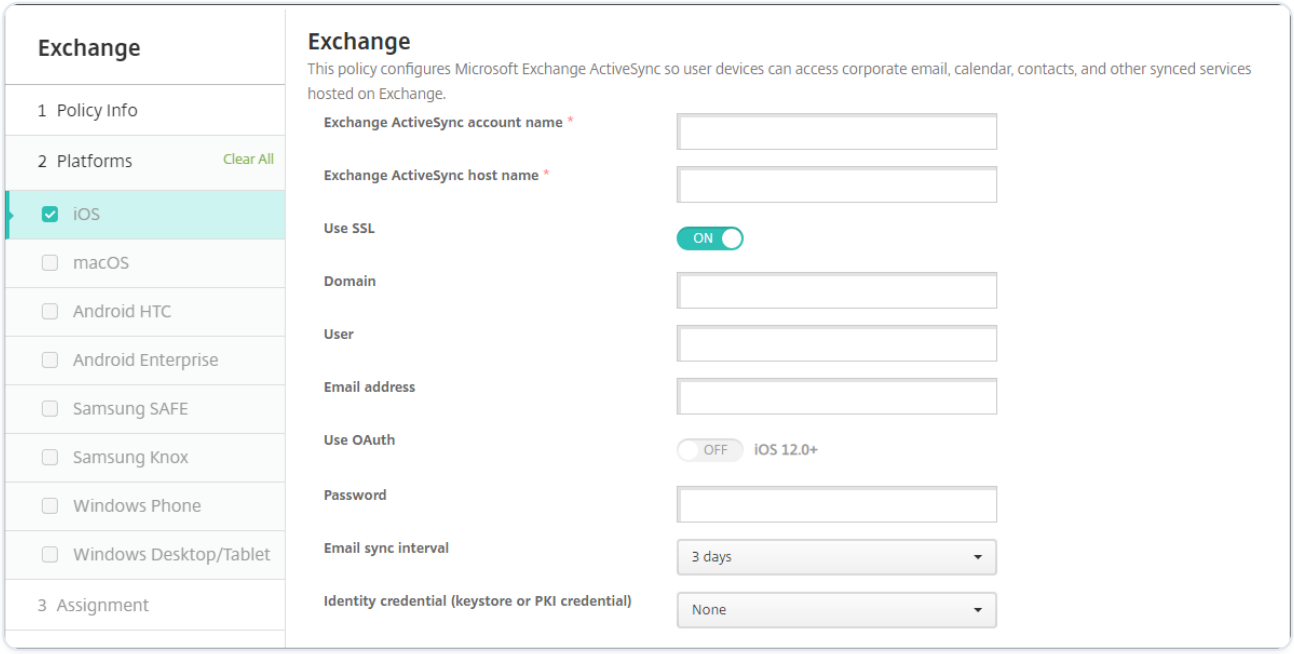
Exchange 设备策略

您可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以允许他们访问托管在 Exchange 上的公司电子邮件。每个平台都需要一组不同的值，这些值将在以下部分中详细介绍。

要创建此策略，您需要 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：** 键入在用户设备上显示的电子邮件帐户的描述。
- **Exchange ActiveSync 主机名：** 键入电子邮件服务器的地址。
- **使用 SSL：** 选择是否保护用户设备与 Exchange Server 之间的连接。默认值为 **开**。
- **域：** 输入 Exchange Server 所在的域。您可以在此字段中使用系统宏 `$user.domainname` 自动查找用户域名。
- **用户：** 指定 Exchange 用户帐户的用户名。您可以在此字段中使用系统宏 `$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。您可以在此字段中使用系统宏 `$user.mail` 自动查找用户电子邮件帐户。
- **使用 OAuth：** 如果设置为 **开**，则连接使用 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。
- **密码：** 输入 Exchange 用户帐户的可选密码。当 **使用 OAuth** 为 **开** 时，此设置不会显示。
- **电子邮件同步间隔：** 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）：** 如果您已为 Citrix Endpoint Management 配置身份提供程序，请在下拉列表中单击可选的身份凭据。仅当 Exchange 需要客户端证书身份验证时，才需要此字段。默认值为“**无**”。
- **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到另一个帐户
  - 从其他帐户转发电子邮件
  - 从其他帐户回复。

  默认值为“**关**”。
- **仅从电子邮件应用发送电子邮件：** 选择是否限制用户只能使用 iOS 邮件应用发送电子邮件。默认值为“**关**”。
- **阻止用户同步最近的地址：** 选择是否阻止用户同步最近的地址。默认值为“**关**”。
- **允许 Mail Drop：** 选择是否允许帐户使用 Mail Drop。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**”。当设置为“**开**”时，将显示以下字段。
  - **签名身份凭据：** 选择要使用的签名凭据。
  - **用户可以覆盖 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。
  - **用户可以覆盖 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**”。当设置为“**开**”时，将显示以下字段。
  - **加密身份凭据：** 选择要使用的加密凭据。
  - **启用每条消息的 S/MIME 开关：** 设置为 **开** 时，向用户显示一个选项，用于在他们撰写的每条消息中打开或关闭 S/MIME 加密。默认值为 **关**。
  - **用户可以覆盖 S/MIME 加密：** 如果设置为 **开**，用户可以在其设备设置中选择 S/MIME 是否默认开启。默认值为 **关**。此选项适用于 iOS 12.0 及更高版本。
  - **用户可以覆盖 S/MIME 加密证书 UUID：** 如果设置为 **开**，用户可以在其设备设置中打开或关闭 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**

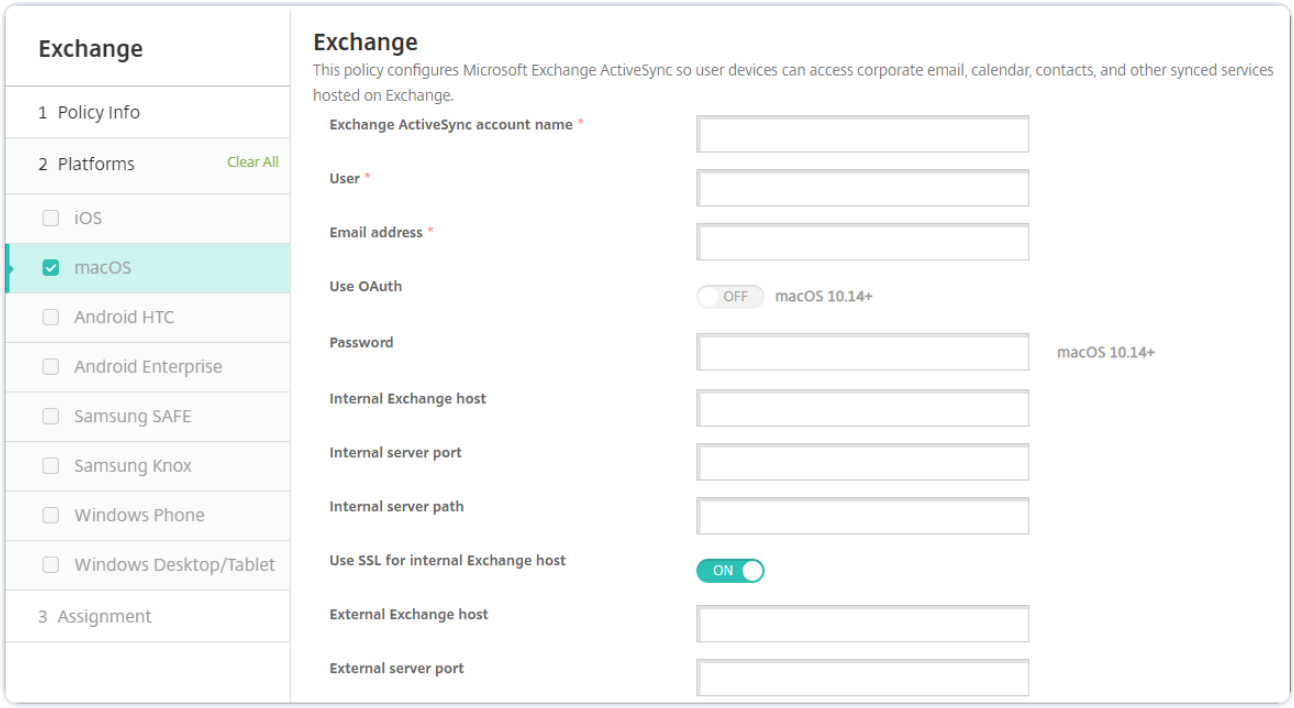
- **删除策略：** 选择一种计划策略删除的方法。可用选项为 **选择日期** 和 **删除前持续时间（小时）**
  - **选择日期：** 单击日历以选择具体的删除日期。
  - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。

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
- 联系人
- 邮件
- 备忘录
- 提醒

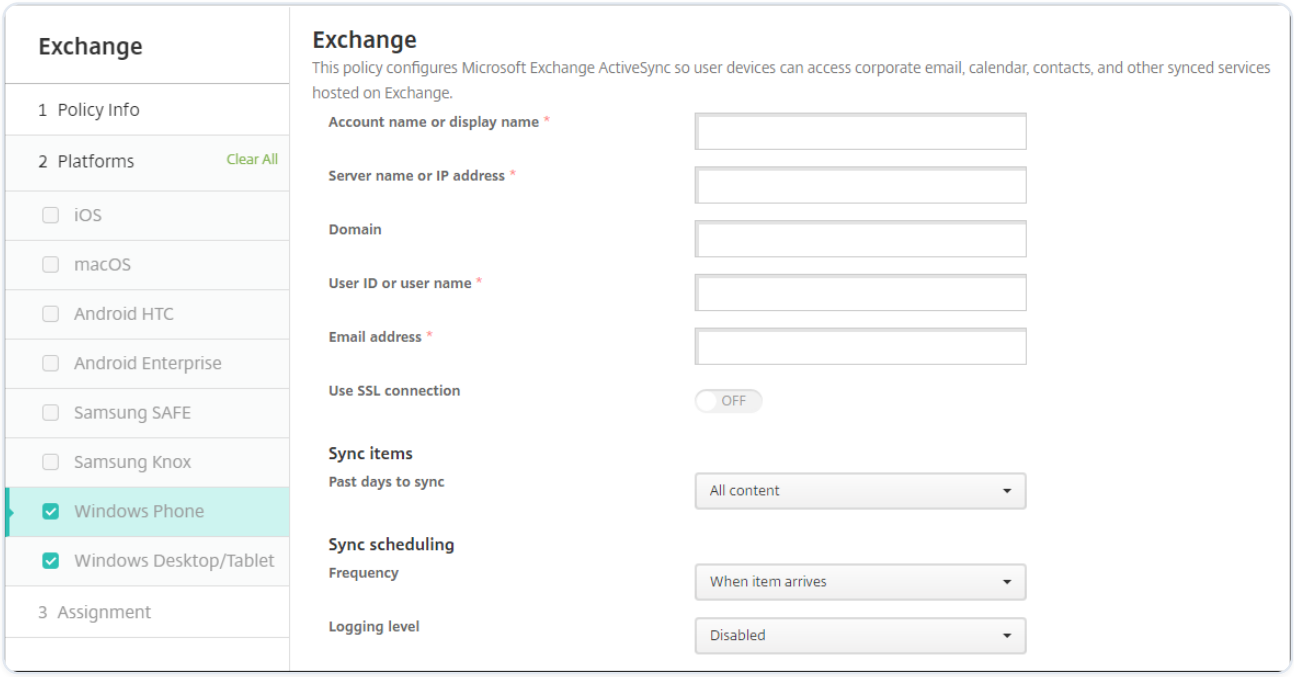
macOS 设置



- **Exchange ActiveSync 帐户名称：** 键入在用户设备上显示的电子邮件帐户的描述。
- **用户：** 指定 Exchange 用户帐户的用户名。您可以在此字段中使用系统宏 `$user.username` 自动查找用户名。
- **电子邮件地址：** 指定完整的电子邮件地址。您可以在此字段中使用系统宏 `$user.mail` 自动查找用户电子邮件帐户。

- **使用 OAuth：** 如果设置为 **On**，则连接使用 OAuth 进行身份验证。默认值为 **Off**。此选项适用于 macOS 10.14 及更高版本。
- **OAuth 登录 URL：** 指定在不使用 AutoDiscovery 服务时加载到 webview 中以使用 OAuth 进行身份验证的 URL。当 **使用 OAuth** 设置为 **On** 时，此字段显示。
- **密码：** 输入 Exchange 用户帐户的可选密码。当 **使用 OAuth** 为 **On** 时，此设置不显示。
- **内部 Exchange 主机：** 如果希望内部和外部 Exchange 主机名不同，请键入可选的内部 Exchange 主机名。
- **内部服务器端口：** 如果希望内部和外部 Exchange 服务器端口不同，请键入可选的内部 Exchange 服务器端口号。
- **内部服务器路径：** 如果希望内部和外部 Exchange 服务器路径不同，请键入可选的内部 Exchange 服务器路径。
- **对内部 Exchange 主机使用 SSL：** 选择是否保护用户设备与内部 Exchange 主机之间的连接。默认值为 **On**。
- **外部 Exchange 主机：** 如果希望内部和外部 Exchange 主机名不同，请键入可选的外部 Exchange 主机名。
- **外部服务器端口：** 如果希望内部和外部 Exchange 服务器端口不同，请键入可选的外部 Exchange 服务器端口号。
- **外部服务器路径：** 如果希望内部和外部 Exchange 服务器路径不同，请键入可选的外部 Exchange 服务器路径。
- **对外部 Exchange 主机使用 SSL：** 选择是否保护用户设备与内部 Exchange 主机之间的连接。默认值为 **On**。
- **允许隔空投送：** 选择是否允许用户在两台 Mac 之间无线共享文件，而无需连接到现有网络。默认值为“**关闭**”。
- **策略设置**
  - **删除策略：** 选择策略删除的计划方法。可用选项为“**选择日期**”和“**删除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 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 macOS 10.7 及更高版本。

Windows 桌面和平板电脑设置



> **注意：**
>
> 此策略不允许您设置用户密码。用户必须在您推送策略后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 主机名或 IP 地址。
- **域：** 输入 Exchange Server 所在的域。您可以在此字段中使用系统宏 `$user.domainname` 自动查找用户域名。
- **用户 ID 或用户名：** 指定 Exchange 用户帐户的用户名。您可以在此字段中使用系统宏 `$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。您可以在此字段中使用系统宏 `$user.mail` 自动查找用户电子邮件帐户。
- **使用 SSL 连接：** 选择是否保护用户设备与 Exchange Server 之间的连接。默认值为“**关**”。
- **同步过去的天数：** 在列表中，单击要将设备上的所有内容与 Exchange Server 同步的过去天数。默认值为“**所有内容**”。
- **频率：** 在下拉列表中单击要用于同步从 Exchange Server 发送到设备的数据的计划。默认值为“**项目到达时**”。
- **日志记录级别：** 在下拉列表中单击“**禁用**”、“**基本**”或“**高级**”，以指定记录 Exchange 活动时的详细程度。默认值为“**禁用**”。

文件设备策略

您可以添加和部署文件，供用户在其 Android 和 Android Enterprise 设备上访问。您可以指定要在设备上存储文件的目录。例如，您希望用户接收公司文档或 .pdf 文件。将文件部署到设备并告知用户文件所在位置。

Android 设备不支持原生运行脚本。用户需要第三方软件才能运行脚本。

您可以使用此策略添加以下文件类型：

- 基于文本的文件（.xml、.html、.py 等）
- 其他文件，例如文档、图片、电子表格或演示文稿

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅设备策略。

安卓企业版设置

- **要导入的文件：** 要选择要导入的文件，请单击 **Browse** 并导航到文件位置。
- **目标文件夹：** 在列表中，选择要存储上传文件的位置，或选择 **Add new** 以指定文件位置。选择 `%Flash Storage%\` 或 `%XenMobile Storage%\` 宏以指示上传文件的存储位置。该宏将扩展到每个设备上的适用位置。
  - `%XenMobile Storage%\` 扩展到内部存储目录中的 `Android/data/com.zenprise/`。
  - 对于 Android 9.0 及更早版本，`%Flash Storage%\` 将文件保存到外部存储目录。
  - 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 **Downloads** 文件夹。
  - 对于 Android 11.0 及更高版本，由于 Google 对目标位置访问施加的限制，`%XenMobile Storage%\` 不再适用。
- **目标文件名：** 可选。如果必须在将文件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**仅当文件不同时复制**。

> **重要提示：**
>
> 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，则在选择该策略时会显示错误消息，您可以重新添加该策略以解决此问题。

Android 设置

- **要导入的文件：** 要选择要导入的文件，请单击**浏览**并导航到文件位置。
- **文件类型：** 选择**文件**或**脚本**。
- **立即执行：** 当您选择**脚本**时，将显示**立即执行**选项。启用此设置时不会发生任何事情。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，选择要存储上传文件的位置，或选择**添加新项**以指定文件位置。选择 `%Flash Storage%\` 或 `%XenMobile Storage%\` 宏以指示上传文件的存储位置。宏将扩展到每个设备上的适用位置。
  - `%XenMobile Storage%\` 扩展到内部存储目录中的 `Android/data/com.zenprise/`。
  - 对于 Android 9.0 及更早版本，`%Flash Storage%\` 将文件保存到外部存储目录。
  - 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。
  - 对于 Android 11.0 及更高版本，由于 Google 对目标位置访问施加的限制，`%XenMobile Storage%\` 不再适用。
- **目标文件名：** 可选。如果必须在将文件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**仅当文件不同时复制**。

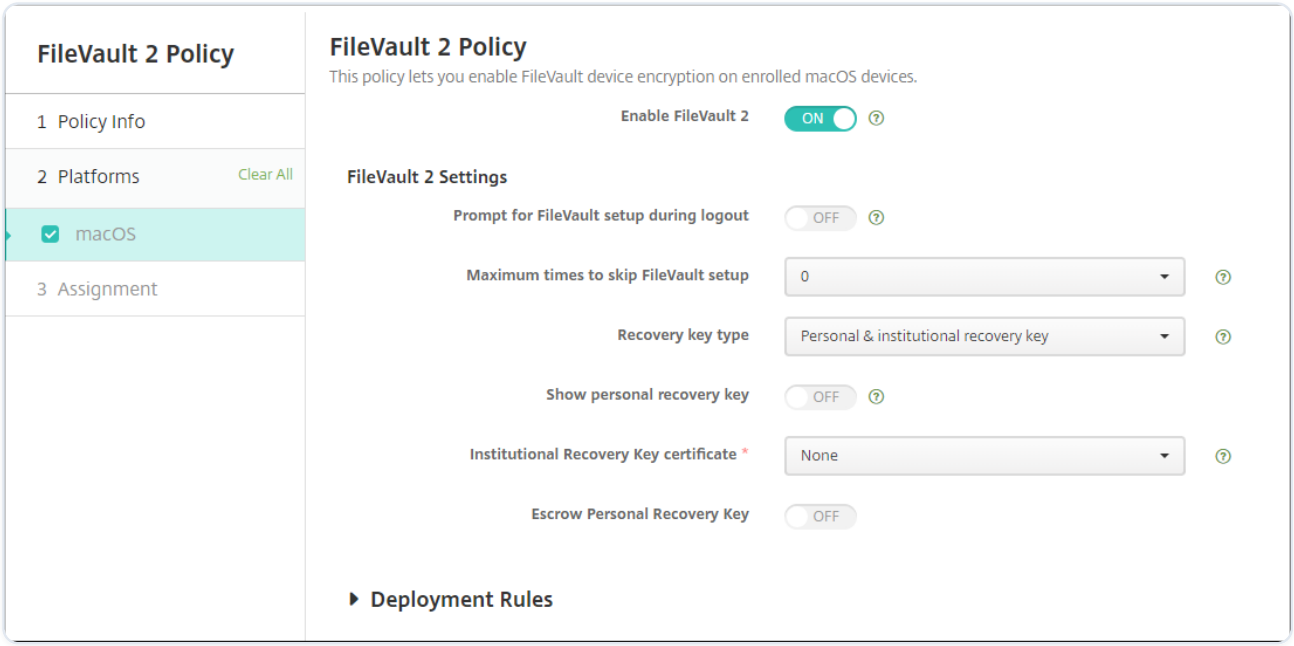
FileVault 设备策略

macOS FileVault 全盘加密 (FileVault 2) 功能通过加密其内容来保护系统卷。每次设备启动时，用户都使用其帐户密码登录到启用了 FileVault 的 macOS 设备。如果用户忘记密码，恢复密钥可帮助他们解锁磁盘并重置密码。

此设备策略启用 FileVault 用户设置屏幕并配置恢复密钥等设置。有关 FileVault 的更多信息，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：** 如果此设置为“**开**”，则会提示用户在选项“**跳过 FileVault 设置的最大次数**”指定的下 N 次注销期间启用 FileVault。如果为“**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。
- **注销时提示进行 FileVault 设置：** 如果为“**开**”，用户在注销时会看到提示，要求他们启用 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。当用户达到最大次数时，用户必须设置 FileVault 才能登录。如果为“**0**”，用户必须在首次登录尝试时启用 FileVault。默认值为“**0**”。
- **恢复密钥类型：** 忘记密码的用户可以输入恢复密钥来解锁磁盘并重置密码。恢复密钥选项：
  - **个人恢复密钥：** 个人恢复密钥对用户而言是唯一的。在 FileVault 设置期间，用户选择是创建恢复密钥还是允许其 iCloud 帐户解锁其磁盘。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**”。显示密钥使用户能够记录密钥以备将来使用。要允许用户在丢失密钥时查找密钥，请启用“**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更多信息，请参阅安全操作。

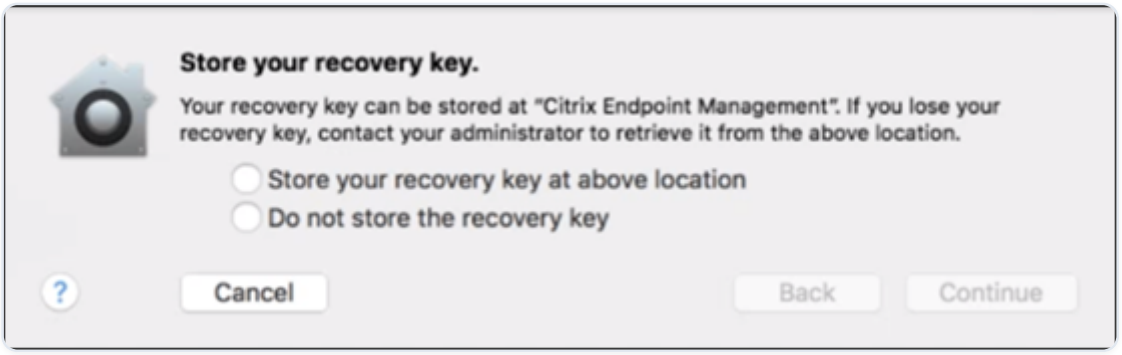
    有关恢复密钥管理的信息，请参阅 Apple 支持站点。
  - **机构恢复密钥：** 您可以创建机构（或主）恢复密钥和 FileVault 证书，然后使用它们来解锁用户设备。有关信息，请参阅 Apple 支持站点。使用 Citrix Endpoint Management 将 FileVault 证书部署到设备。有关信息，请参阅证书和身份验证。

  - **个人和机构恢复密钥：** 通过启用这两种类型的恢复密钥，您只需在用户丢失其个人恢复密钥时才需要解锁用户设备。

- **机构恢复密钥证书：** 如果您选择“**机构恢复密钥**”或“**个人和机构恢复密钥**”作为“**恢复密钥类型**”，请选择该密钥的恢复密钥证书。
- **显示个人恢复密钥：** 如果为“**开**”，用户设备在设置 FileVault 后向用户显示个人恢复密钥。默认为“**关**”。

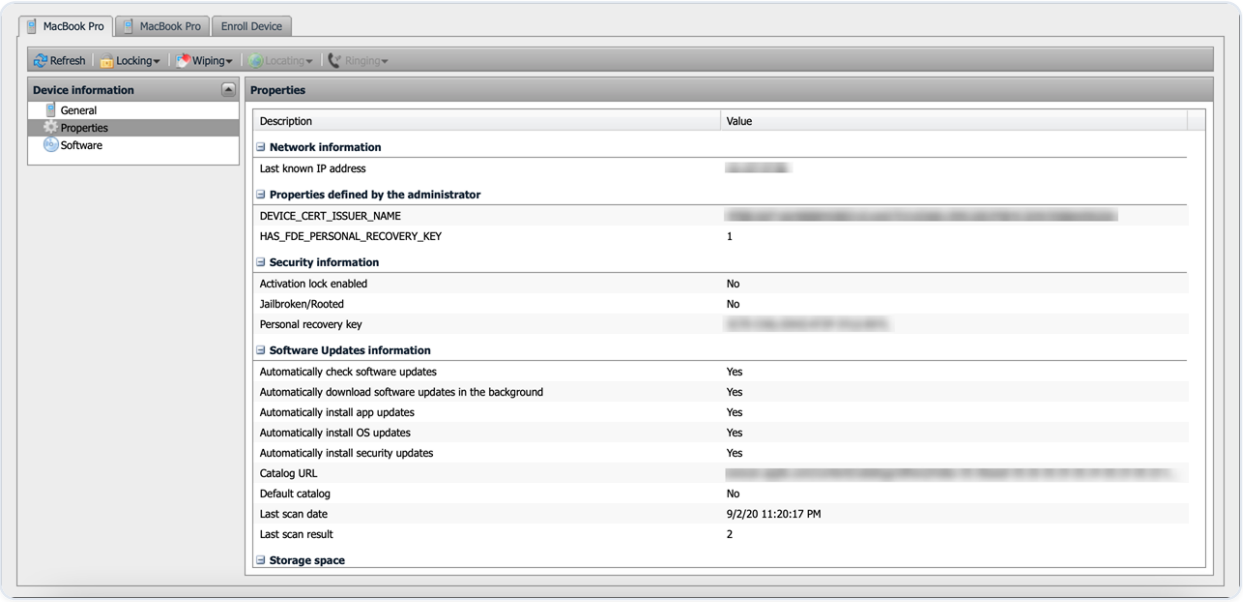


- **托管个人恢复密钥：** 启用后，用户可以将每个设备的个人恢复密钥副本存储在 Citrix Endpoint Management 中。



要从 Citrix Endpoint Management 访问密钥，请转至“**管理 > 设备**”，选择 macOS 设备，然后单击“**编辑**”。然后，转至“**设备详细信息 > 常规**”并找到“**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“**托管个人恢复密钥**”和“**向用户显示个人恢复密钥**”。密钥将显示在自助服务门户的“**属性**”页面上的“**安全信息**”下。有关自助服务门户的更多信息，请参阅自助服务门户。



您可以启用“**托管个人恢复密钥**”设置，即使您未启用“**启用 FileVault**”设置。如果您禁用“**启用 FileVault**”设置，用户仍然可以自行启用 FileVault。在这种情况下，请启用“**托管个人恢复密钥**”以允许用户将其密钥副本存储在 Citrix Endpoint Management 中。

如果用户在将设备注册到 Citrix Endpoint Management 之前启用了 FileVault，Citrix Endpoint Management 不会存储其恢复密钥。该设备在控制台中显示为已启用 FileVault。

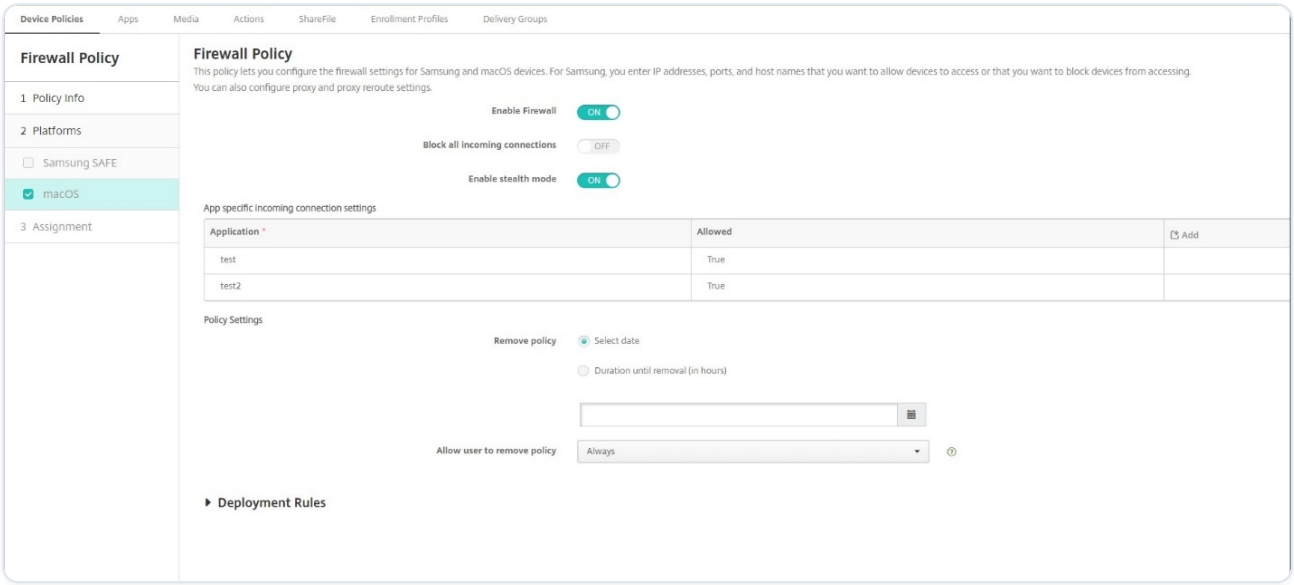
防火墙设备策略

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

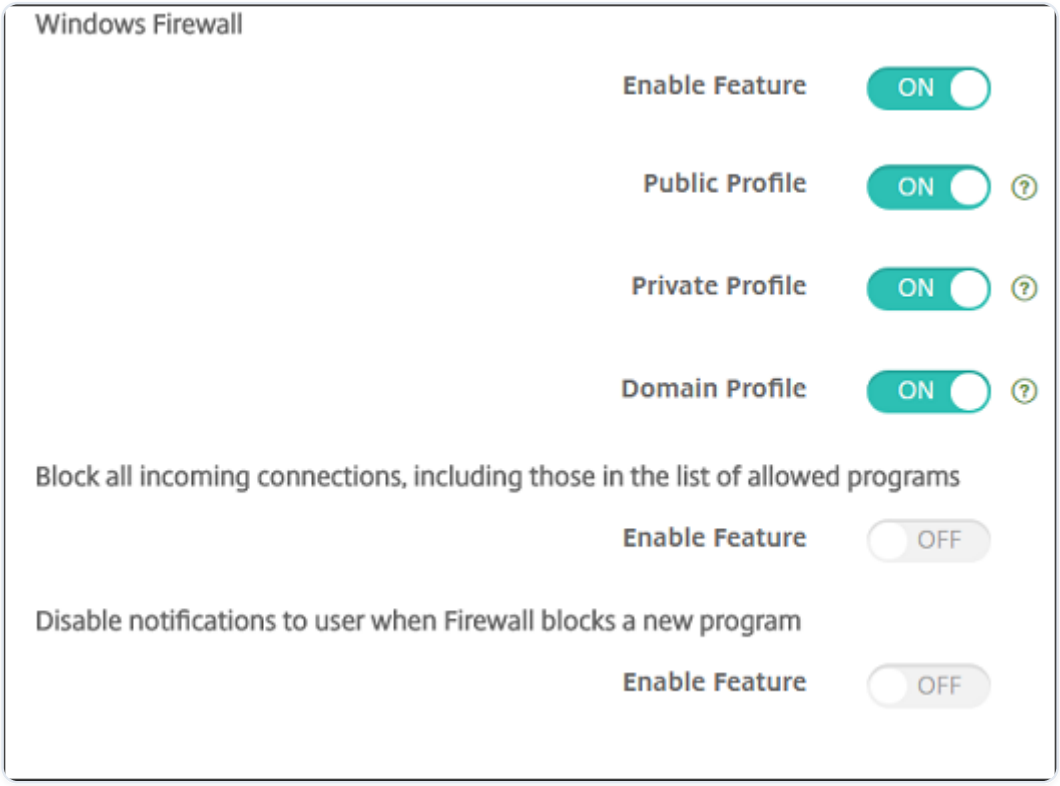
需要 macOS 10.12 或更高版本。



- **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**。当此选项设置为**开**时，它会阻止所有传入连接，但基本服务所需的连接除外。
- **启用隐身模式**。在隐身模式下，设备不会响应或确认测试应用程序（例如使用 ICMP 的 Ping）从网络对其进行的访问尝试。要启用隐身模式，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，请添加应用程序并将**允许**设置为 **True**。

Windows 桌面和平板电脑设置

需要运行 Windows 10（版本 1709 或更高版本）或 Windows 11 的 Windows 桌面和平板电脑设备。



- **启用功能：** 控制部署此策略的计算机上的传入和传出流量。默认值为**开**。
- **公共配置文件：** 控制计算机连接到公共场所（例如机场或咖啡店）的不可信网络时的 Windows 防火墙。默认值为**开**。
- **专用配置文件：** 当计算机连接到受信任的网络（例如家庭网络）时，控制 Windows 防火墙。默认值为 **开**。
- **域配置文件：** 当计算机连接到域网络（例如工作场所）时，控制 Windows 防火墙。默认值为 **开**。
- **阻止所有传入连接，包括允许程序列表中的连接：** 默认值为 **关**。

- **当防火墙阻止新程序时禁用向用户发送通知：** 默认值为 **关**。

字体设备策略

您可以在 Citrix Endpoint Management 中添加设备策略，以向 iOS 和 macOS 设备添加更多字体。字体必须是 TrueType (`.ttf`) 或 OpenType (`.oft`) 字体。不支持字体集 (`.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：要选择要添加到用户设备的字体文件，请单击浏览**，然后导航到文件位置。
- **策略设置**
  - **删除策略：选择一种计划策略删除的方法。可用选项包括选择日期**和**删除前持续时间（小时）**。
    - **选择日期：**单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），直到策略删除发生。

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：要选择要添加到用户设备的字体文件，请单击浏览**，然后导航到文件位置。
- **策略设置**
  - **删除策略：选择一种计划策略删除的方法。可用选项包括选择日期**和**删除前持续时间（小时）**。
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略被移除。
  - **允许用户移除策略：** 您可以选择用户何时可以从其设备中移除策略。从菜单中选择“**始终**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**移除密码**”字段中键入密码。
  - **配置文件范围：** 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 macOS 10.7 及更高版本。

主屏幕布局设备策略

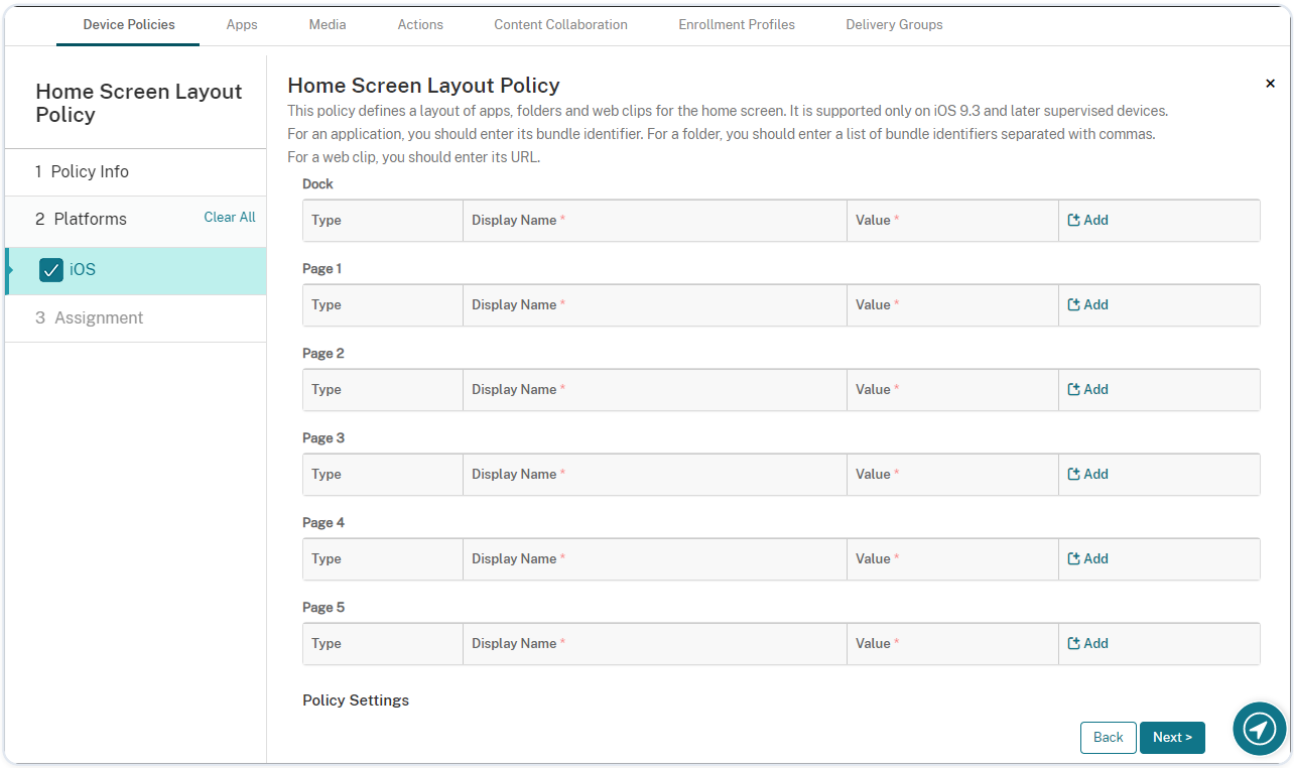
主屏幕布局设备策略允许您指定受监管 iOS 设备的 iOS 主屏幕上的应用程序和文件夹的布局。

重要提示：

将多个主屏幕布局策略部署到设备会导致设备上出现 iOS 错误。无论您是通过此 Citrix Endpoint Management 策略还是通过 Apple Configurator 定义主屏幕，此限制都适用。

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。

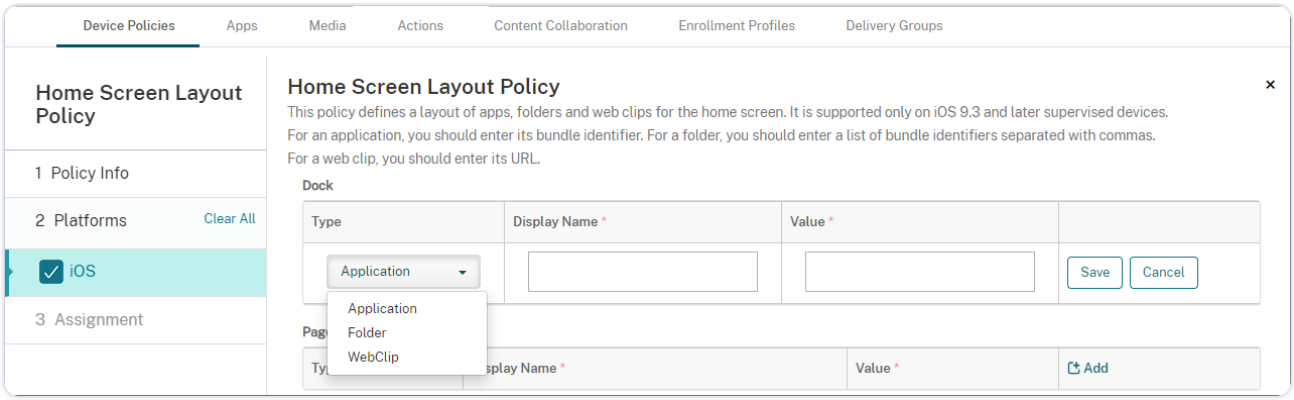
iOS 设置



- 对于要配置的每个屏幕区域（例如**Dock**或**Page 1**），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 > 仅允许某些应用程序**设置可能会阻止 Web 剪辑在主屏幕上正常显示。要使 Web 剪辑正常显示，请执行以下任一操作：

  - 将**受限应用程序使用**设置为**允许所有应用程序**或**不允许某些应用程序**。
  - 在**受限应用程序使用**设置为**仅允许某些应用程序**的情况下，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：**在主屏幕上显示的应用程序或文件夹的名称。
- **值：**对于应用程序，键入捆绑包标识符。对于文件夹，键入以逗号分隔的捆绑包标识符列表。对于 Web 剪辑，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。如果存在多个具有相同 URL 的 Web 剪辑值，则在 iOS 11.3 及更高版本设备上的行为是未定义的。
- **策略设置**
  - **移除策略：** 选择一种策略移除的计划方法。可用选项为“**选择日期**”和“**移除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 输入一个数字（以小时为单位），直到策略移除发生。
  - **配置文件范围：** 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 iOS 和 macOS 配置文件设备策略

您可以将 iOS 和 macOS 设备的设备配置 XML 文件导入到 Citrix Endpoint Management 中。该文件包含您使用 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

导入使用 Profile Creator 在 Citrix Endpoint Management 外部为 macOS 设备创建的以下配置：

- **系统策略控制：**此策略可识别由经认证的 Apple 开发者签名的应用程序，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**启用 Gatekeeper**以确保用户仅运行经过验证和受信任的软件。

  - 选择**允许已识别的开发者**以确保用户仅安装由经认证的 Apple 开发者签名的应用程序。

- **隐私偏好策略控制：**此策略允许您授予或限制跨应用程序访问某些文件或功能，例如位置服务、摄像头和屏幕捕获。

  配置您计划部署的设置。有关详细信息，请参阅隐私偏好策略控制负载设置。

- **内核扩展策略：**此策略允许用户安装可扩展操作系统本机功能的应用程序扩展。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负载设置。

- **以太网设置策略：**此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如何将其设备连接到 Wi-Fi 网络。

  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：** 该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：** 该策略提供设备级别的加密连接到专用网络。

  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 创建配置配置文件

1. 从 Apple 应用商店 安装 Apple Configurator 2。
2. 启动 Apple Configurator 2，然后转到**文件 > 新建配置文件**。将出现一个新的配置窗口。
3. 在**通用**设置窗格中，为您的配置文件键入名称和标识符，然后添加任何其他负载选项。
4. 在左侧窗格中，选择一个负载，单击**配置**，然后输入设置。不要签署您的配置文件，因为不支持已签署的配置文件。

   要在单个配置文件中添加多个负载，请选择一个负载并单击右上角的**添加负载**按钮。

5. 转到**文件 > 保存**，选择保存 XML 文件的名称和位置，然后单击**保存**。

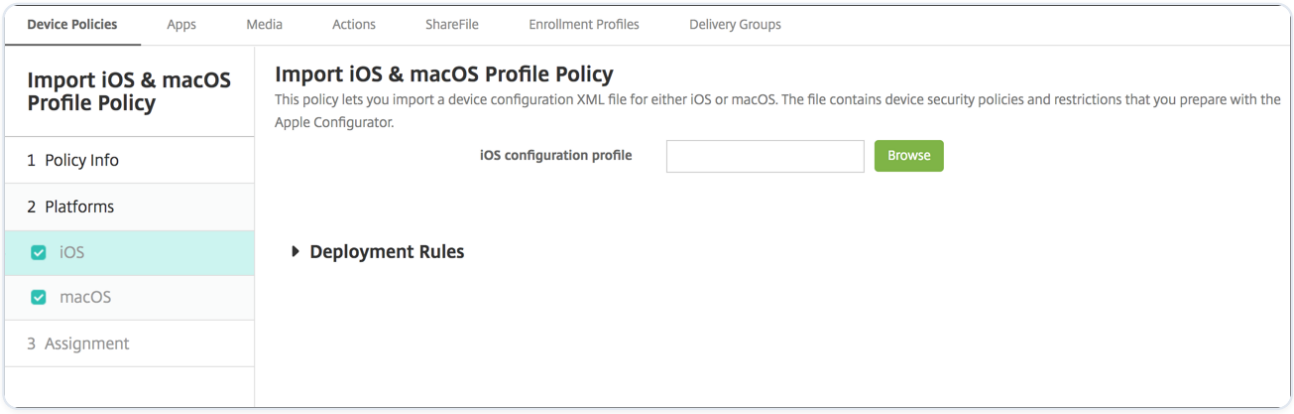
使用 Profile Creator 创建配置配置文件

1. 从 GitHub 安装 Profile Creator。
2. 启动 Profile Creator，然后转到**文件 > 新建**。将显示一个新的配置窗口。
3. 在**常规**设置窗格中，键入配置文件的名称和描述，然后添加任何其他负载选项。
   - 建议：选择**阻止用户删除此配置文件**。
   - 将**负载范围**设置为**系统**或**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**，选择保存 XML 文件的名称和位置，然后单击**保存**。

要在 Citrix Endpoint Management 控制台中导入 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 配置配置文件**或**macOS 配置配置文件**：要选择要导入的配置文件，请单击**浏览**，然后导航到文件位置。

适用于 Android 设备的合规性强制执行 (技术预览版)

> **注意：**
>
> 技术预览版中的功能可在非生产或有限生产环境中使用，并为客户提供分享反馈的机会。Citrix® 不接受技术预览版功能的任何支持案例，但欢迎提供改进这些功能的反馈。您可以通过

> 单击“**向我们发送反馈**”来提供对此功能的反馈。Citrix 可能会根据反馈的严重性、关键性和重要性采取行动。

> 对于以 *设备所有者* 模式注册的 Android 设备，客户管理员可以管理设备合规性。他们可以定义自定义规则来评估合规性，包括：

- 确保设备密码强度符合指定标准。
- 验证所有必需应用程序的安装。
- 确认已删除任何禁用应用程序。

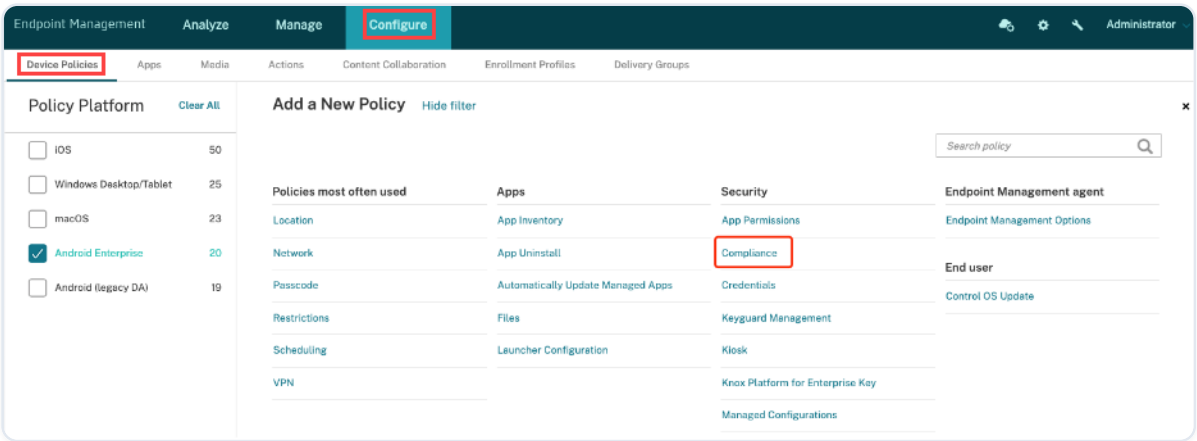
如果发现设备不合规，客户可以提示用户纠正问题。此外，还可以采取更严格的措施，例如冻结设备上的应用程序以限制用户访问，直到达到合规性。 要启用此功能，需要满足两个先决条件，因为服务器和客户端都需要进行更改：

- 将 CEM 服务器升级到 24.8.0 版本。
- 将 Secure Hub 升级到 24.8.0 版本。

Android 设备合规性管理过程

1. 激活功能标志 `afw.policy.compliance` 专门用于 CEM 服务器。
2. 添加并部署合规性策略。

   a. 在“**配置**”选项卡中，选择“**设备策略**”，然后单击“**合规性**”。



   b. 使用以下设置配置策略：

      - 启用**合规性检查**：此设置控制设备是否进行合规性检查。要撤销已部署的合规性策略，请禁用此选项并重新部署策略。仅从交付组中删除策略将无效。

   启用合规性检查(/en-us/citrix-endpoint-management/media/enable-compliance-check.png)

- 不合规操作：在**仅警告**和**冻结应用程序（仅限公司拥有的设备）之间选择。选择仅警告**将通过 Secure Hub 通知用户不合规项目，并要求他们解决这些问题。选择**冻结应用程序（仅限公司拥有的设备）**将锁定设备上的所有应用程序，但管理员可以自定义一个“未冻结应用程序”列表，以豁免特定应用程序，例如 Secure Hub（用于显示和解决不合规项目）、Google Play 商店（用于安装必要的应用程序）、设置（用于恢复出厂设置）和短信（用于紧急通信）。**冻结应用程序（仅限公司拥有的设备）**仅适用于公司拥有的设备。

冻结应用程序(/en-us/citrix-endpoint-management/media/freeze-apps.png)

- 验证密码合规性：检查设备密码是否符合指定标准。通常与密码策略一起使用。
- 验证所需应用程序：显示强制性应用程序列表。确保这些应用程序已安装在设备上。

> **注意：**
>
> - **所需应用程序**下列出的应用程序也必须包含在交付组的所需应用程序部分中，以确保其功能。否则，它们将无效。
> - 由于所需应用程序可能在托管的 Google Play 中不可用，最终用户将保持锁定模式。

> 验证所需应用程序(/en-us/citrix-endpoint-management/media/verify-required-apps.png)

- 验证禁用应用程序：显示禁用应用程序列表。确保未安装这些应用程序。

> **注意：**
>
> 管理员应避免将系统预装应用程序添加到**禁用应用程序**列表中，因为最终用户无权删除它们。

3. 部署策略。

   a. 在 Secure Hub 中，单击“刷新策略”或等待 6 小时定期同步以将策略部署到设备。

   b. 部署后，会立即触发合规性检查。处于“冻结应用”模式的不合规设备会限制设备及其应用，直到满足合规性要求。

设备策略(/en-us/citrix-endpoint-management/media/device-policy.png)

如果管理员将不合规操作配置为“冻结应用”，则 Secure Hub 和设备本身都将限制应用使用。具体而言：

- 通知栏中将显示一条持久性通知，提醒用户应用已被冻结。

思杰安全中心(/en-us/citrix-endpoint-management/media/citrix-secure-hub.png)

- 应用（默认允许的应用或“**未冻结应用**”列表中的应用除外）将被冻结，单击时无响应。
- 此状态将持续到设备达到合规性为止。即使在重新启动或进行系统升级后，设备也会立即返回此冻结状态（Secure Hub 升级期间除外，这需要用户手动启动）。

4. 不合规解决方案：

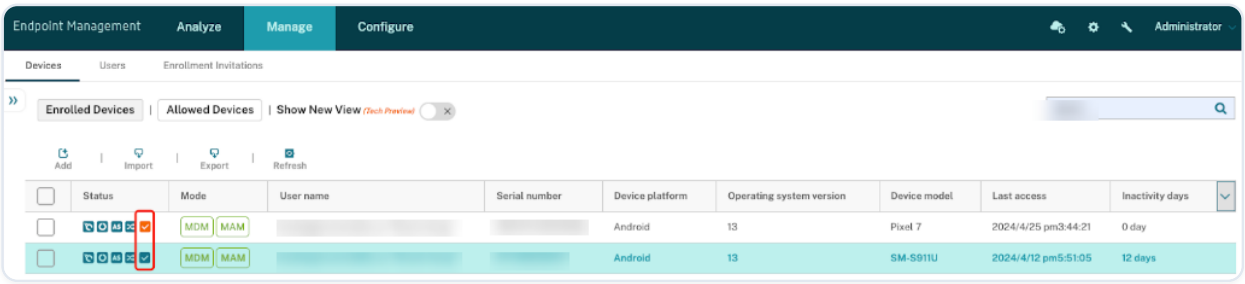
- 当设备不合规时，Secure Hub 将无法通过常规方法（单击“**设备信息**”页面中的“**刷新策略**”按钮）刷新策略。
- 相反，通过下拉显示不合规项目的页面来提供替代解决方案，刷新结果通过浮动通知传达。

刷新请求成功(/en-us/citrix-endpoint-management/media/refresh-request-succeeded.png)

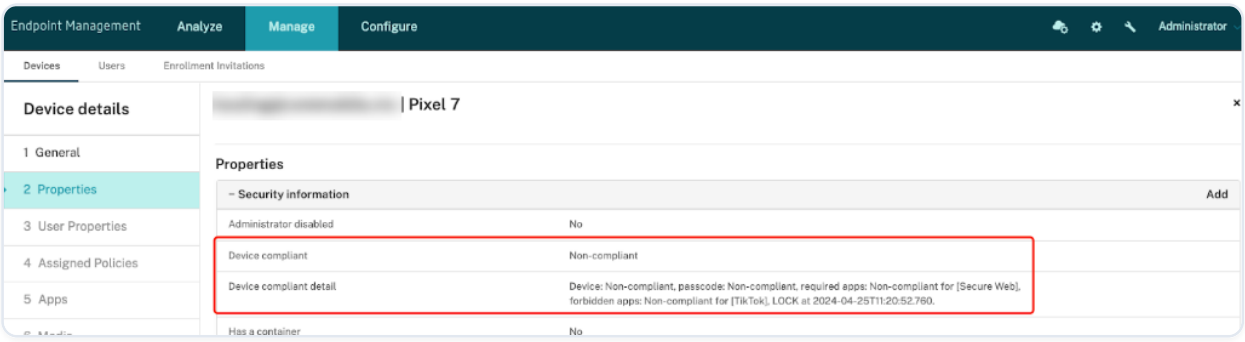
- 用户的具体操作：
  - 设置更复杂的密码以符合标准。
  - 从 Google Play 商店安装所需应用。
  - 卸载禁用应用。

5. 监控合规性

- 查看合规性状态：在 **管理** -> **设备** -> **状态** 中有一个新的合规性状态图标。绿色表示合规，橙色表示不合规。

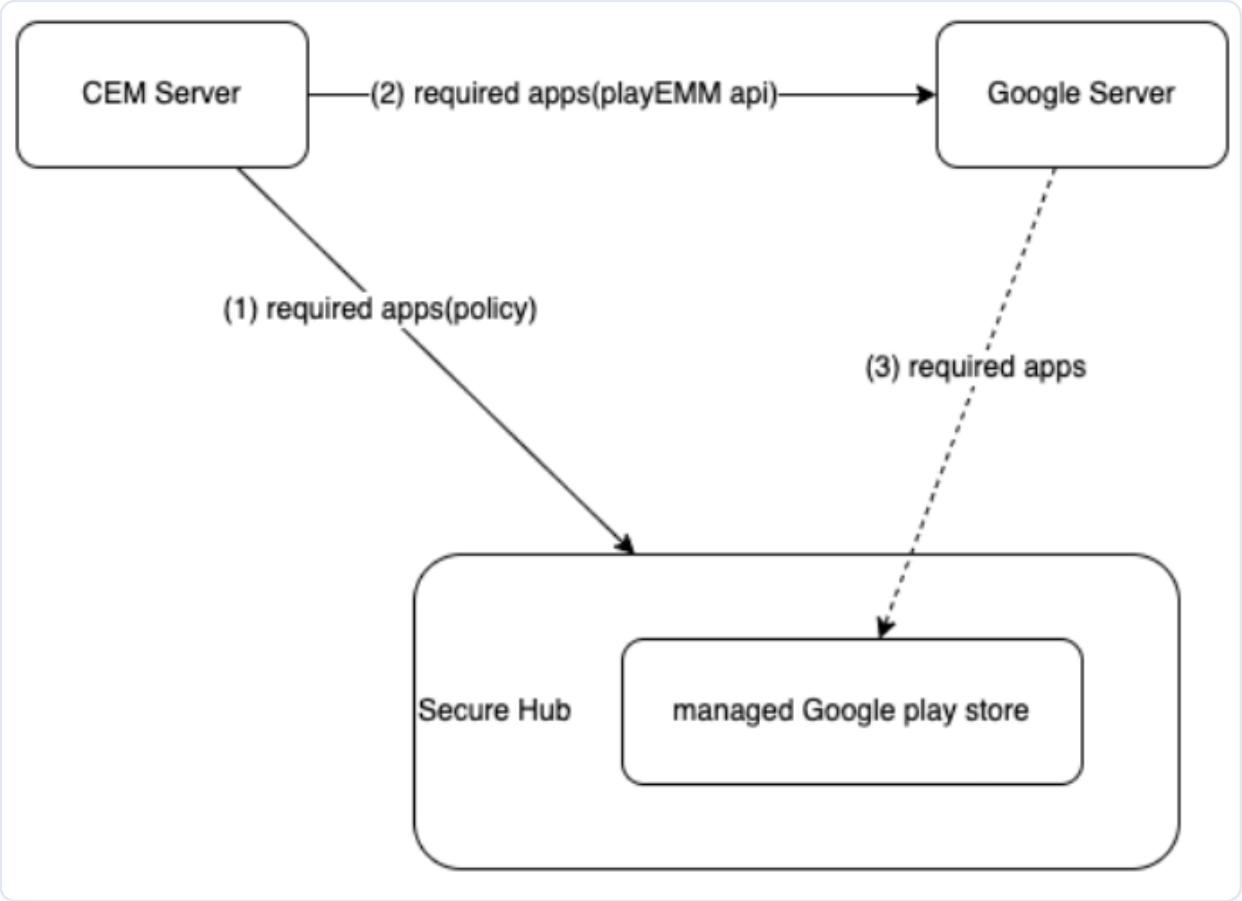


- 详细合规性状态可在 **管理** -> **设备** -> **设备详细信息** -> **属性** -> **安全信息** 中查看。



故障排除

1. 在 Google Play 商店中找不到配置的必需应用，导致设备不合规且无法解决此问题。这是一个设计缺陷。



CEM 服务器通过链接 1 和 2 将必需应用推送到 Secure Hub 和 Google 服务器，但链接 3 超出了我们的控制范围。当 Secure Hub 使用链接 1 检查必需应用时，我们无法保证托管的 Google Play 商店中提供这些应用。这种差异意味着，尽管合规性策略要求 Secure Hub 安装这些应用，但它们可能无法立即在商店中找到。通常，Google 服务器会在 24 小时内使用链接 3 将必需应用推送到设备。

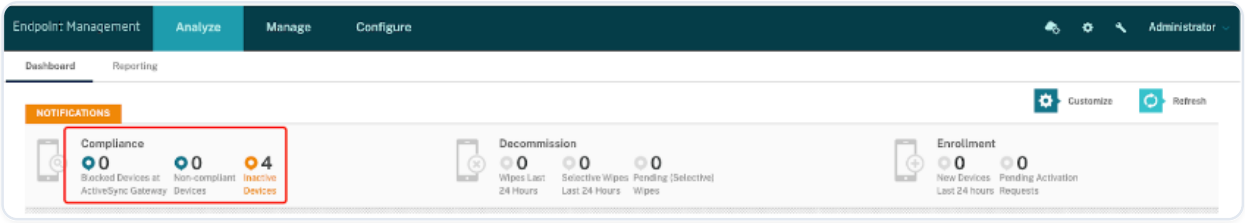
2. 在升级 Secure Hub 之前，设备不合规，并且应用被冻结。但是，升级 Secure Hub 后，所有应用都被解冻了。发生这种情况是因为在升级过程中，Secure Hub 的操作被终止，从而无法维持应用冻结状态。 此问题已知，目前尚无解决方案。我们正在积极与 Google 合作解决此问题，并

期望在未来版本中有所改进。完成升级后，用户可以手动启动 Secure Hub 以启动该过程并将应用恢复到冻结状态。

3. 如何解冻应用？最常见的方法是用户解决所有不合规问题，从而使设备合规并自动解冻所有应用。如果无法快速实现合规，可以采取以下步骤：

   - 将相关应用添加到“未冻结应用”列表并执行下拉刷新。
   - 将“不合规操作”更改为“警告”并执行下拉刷新。
   - 禁用与不合规项目对应的检查开关或主开关，然后执行下拉刷新。
   - 如果以上方法均无效，请为特定的 CEM 服务器启用功能标志 `afw.locktaskmode.disable` 并执行下拉刷新。此操作会强制解冻所有应用程序，但 Secure Hub 仍将保持阻止状态，类似于将不合规操作设置为 **警告** 时的情况。
   - 为特定的 CEM 服务器禁用功能标志 `afw.policy.compliance` 并执行下拉刷新。
   - 在 Secure Hub 无法连接到 CEM 服务器的最坏情况下，请从“设置”执行恢复出厂设置。

4. 在“分析”->“仪表板”下显示的合规性状态是 Citrix Endpoint Management™ 中与此策略中引用的合规性不同的一种合规性。此功能尚未开发，将在未来版本中增强。



5. 此功能不适用于通过 COSU/WPCOD/BYOD 模式注册的设备。目前，它仅支持以设备所有者 (DO) 模式注册的设备。

屏幕锁定管理设备策略

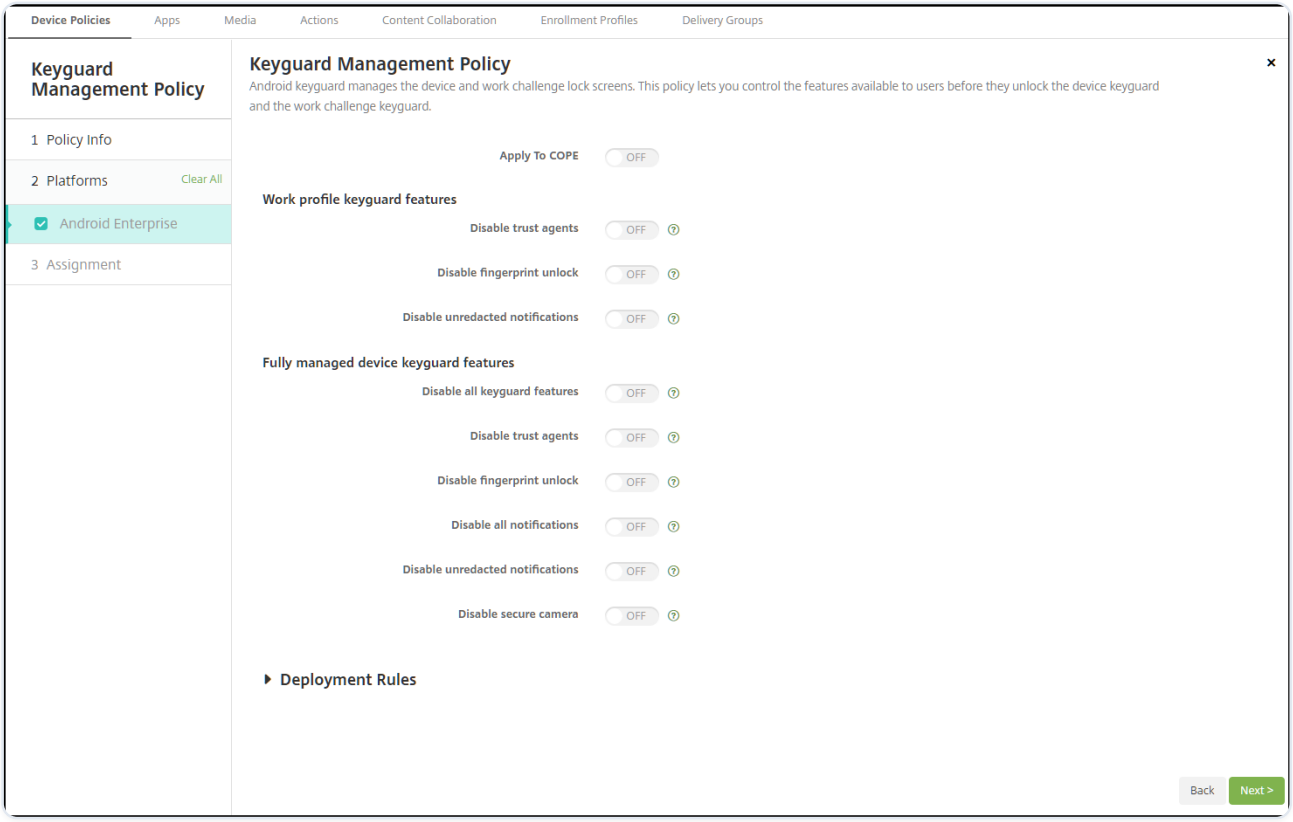
Android 屏幕锁定管理设备和工作挑战锁屏。此策略允许您管理 Android Enterprise 工作配置文件屏幕锁定和高级设备屏幕锁定的功能。您可以控制：

- 工作配置文件设备上的屏幕锁定管理。您可以指定用户在解锁设备屏幕锁定和工作挑战屏幕锁定之前可用的功能。例如，默认情况下，用户可以使用指纹解锁并在锁屏上查看未编辑的通知。
- 完全托管设备和专用设备上的屏幕锁定管理。您可以指定在解锁屏幕锁定屏幕之前可用的功能，例如信任代理和安全摄像头。或者，您可以选择禁用所有屏幕锁定功能。
- 具有工作配置文件的完全托管设备上的屏幕锁定管理。这些设备以前称为 COPE（公司拥有个人启用）设备。您可以使用一个屏幕锁定管理策略来对设备和工作配置文件应用单独的设置。

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。

观看此视频了解更多信息：

安卓企业版设置



- **应用于 COPE：** 允许您为具有工作配置文件的完全托管设备配置屏幕锁定管理设备策略设置。

  当此设置为**开**时，您可以对具有工作配置文件的完全托管设备上的设备和工作配置文件应用单独的设置。

  当此设置为**关**时，您可以将设置应用于工作配置文件设备或完全托管设备。您为工作配置文件配置的设置仅适用于工作配置文件设备。您为完全托管设备配置的设置仅适用于完全托管设备。

  默认值为**关**。

- **工作配置文件屏幕锁定功能：** 控制用户在解锁工作配置文件屏幕锁定（锁屏）之前是否可以使用以下功能。

  - **禁用信任代理**：如果设置为“**关**”，则当工作资料上设置了质询时，信任代理可以在安全的锁屏界面上运行。设置为“**开**”以禁用工作资料上的所有信任代理。默认值为“**关**”。
  - **禁用生物识别身份验证**：如果设置为“**关**”，则当工作资料上设置了质询时，生物识别身份验证可在安全的锁屏界面上使用。设置为“**开**”以禁用工作资料上的生物识别身份验证。此设置

会禁用指纹解锁、面部身份验证和虹膜身份验证。默认值为“**关**”。适用于 Android 9.0 及更高版本。

- **禁用指纹解锁**：如果设置为“**关**”，则当工作资料上设置了质询时，指纹解锁可在安全的锁屏界面上使用。设置为“**开**”以禁用工作资料上的指纹解锁。默认值为“**关**”。
- **禁用面部身份验证**：如果设置为“**关**”，则当工作资料上设置了质询时，面部身份验证可在安全的锁屏界面上使用。设置为“**开**”以禁用工作资料上的面部身份验证。默认值为“**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**”，则当工作资料上设置了质询时，虹膜身份验证可在安全的锁屏界面上使用。设置为“**开**”以禁用工作资料上的虹膜身份验证。默认值为“**关**”。适用于 Android 9.0 及更高版本。
- **禁用未编辑的通知**：如果设置为“**关**”，则编辑和未编辑的通知都会显示在安全的锁屏界面上。设置为“**开**”以禁用未编辑的通知，并且仅显示编辑的通知。默认值为“**关**”。

- **完全托管设备锁屏功能**：控制用户解锁设备锁屏（锁定屏幕）之前是否可以使用以下功能。这些功能适用于完全托管设备或专用设备。
  - **禁用所有锁屏功能**：如果设置为“**关**”，则所有当前和未来的锁屏自定义项都可在安全的锁屏界面上使用。设置为“**开**”以禁用所有锁屏自定义项。默认值为“**关**”。
  - **禁用信任代理**：如果设置为“**关**”，则信任代理可以在安全的锁屏界面上运行。设置为“**开**”以禁用信任代理。默认值为“**关**”。
  - **禁用生物识别身份验证**：如果设置为“**关**”，则当设备上设置了质询时，生物识别身份验证可在安全的锁屏界面上使用。设置为“**开**”以禁用设备上的生物识别身份验证。禁用的生物识别身份验证功能包括指纹解锁、面部身份验证和虹膜身份验证。默认值为“**关**”。适用于 Android 9.0 及更高版本。
  - **禁用指纹解锁**：如果设置为“**关**”，则当设备上设置了质询时，指纹解锁可在安全的锁屏界面上使用。设置为“**开**”以禁用设备上的指纹解锁。默认值为“**关**”。
  - **禁用面部身份验证**：如果设置为“**关**”，则当设备上设置了质询时，面部身份验证可在安全的锁屏界面上使用。设置为“**开**”以禁用设备上的面部身份验证。默认值为“**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**”，则当设备上设置了质询时，虹膜身份验证可在安全的锁屏界面上使用。设置为“**开**”以禁用设备上的虹膜身份验证。默认值为“**关**”。适用于 Android 9.0 及更高版本。
  - **禁用所有通知**：如果设置为“**关**”，则所有通知都会显示在安全的锁屏界面上。设置为“**开**”以显示所有通知。默认值为“**关**”。

- **禁用未编辑的通知**：如果设置为“**关**”，则编辑和未编辑的通知都会显示在安全的锁屏界面上。设置为“**开**”以禁用未编辑的通知，并且仅显示编辑的通知。默认值为“**关**”。
- **禁用安全摄像头**：如果设置为**关**，安全摄像头可在安全锁屏界面上使用。设置为**开**可禁用安全摄像头。默认设置为**关**。

自助服务终端设备策略

The Kiosk policy lets you restrict devices to Kiosk mode by limiting the apps that can run. Citrix Endpoint Management does not control which part of the device locks in Kiosk mode. The device manages the kiosk mode settings after you deploy the policy.

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。

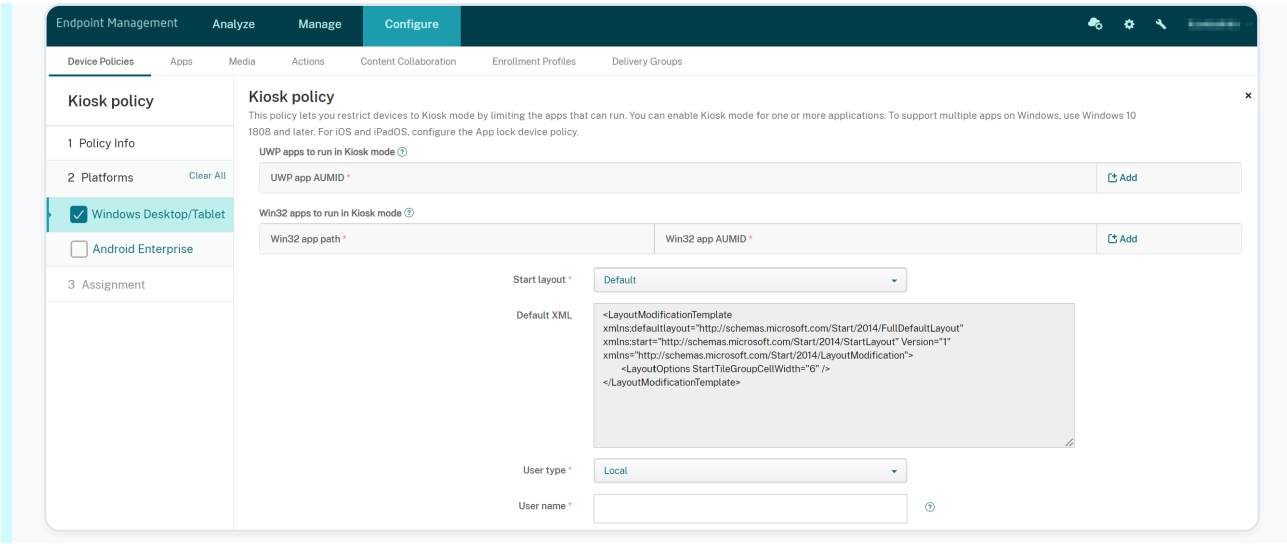
要将 iPad 设置为在自助服务终端模式下运行，请使用应用程序锁定设备策略。有关将 iPad 设置为自助服务终端的信息，请参阅将 iPad 配置为自助服务终端。您还可以将 iPad 配置为仅打开单个网站。有关信息，请参阅Webclip 策略。

Windows 桌面和平板电脑设置

对于 Windows 桌面和平板电脑设备，自助服务终端策略仅适用于本地用户和已注册到 Azure AD 的用户。

单个应用程序或多个应用程序可以在 Windows 桌面和平板电脑设备上以自助服务终端模式运行。

> **注意：**
>
> 自助服务终端设备策略仅适用于 Windows 10 设备。 要在 Windows 11 设备上部署单应用程序自助服务终端，您可以使用自定义 XML 设备策略将我们提供的 XML 脚本部署到设备。有关详细信息，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，然后输入每个 UWP 应用程序的应用程序用户模型 ID (AUMID)。例如，输入以下 AUMID：
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Win32 应用程序路径**和**Win32 应用程序 AUMID**：单击**添加**，选择 Windows 桌面 (`Win32`) 应用程序，然后输入每个 `Win32` 应用程序的路径和 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`
- **开始布局：** 仅提供应用程序的默认开始屏幕。
- **默认 XML：** 仅提供默认 XML 脚本。
- **选择用户类型：** 指定接收自助服务终端策略的用户类型。您的选项：
  - **Local:** Citrix Endpoint Management creates a user for the target device or adds an existing user.
  - **Azure AD：** Citrix Endpoint Management 添加在 Azure AD 中注册的用户。
- **用户名：** 输入接收自助服务终端策略的用户名。
  - 要在目标设备上创建本地用户名，请输入名称。请确保您的本地用户名不包含域。如果输入现有名称，Citrix 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` 部分可以是创建 Azure AD 用户时输入的**名称**，也可以是创建 Azure AD 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。仅为本地用户名键入密码。

- **显示任务栏：** 启用任务栏，为用户提供查看和管理应用程序的简便方法。默认设置为**关闭**。
- 单击**下一步**并保存更改。

对于要在自助服务终端模式下允许的 UWP 应用程序，您需要提供 AUMID。要获取当前设备用户安装的所有 Microsoft Store 应用程序的 AUMID 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
```

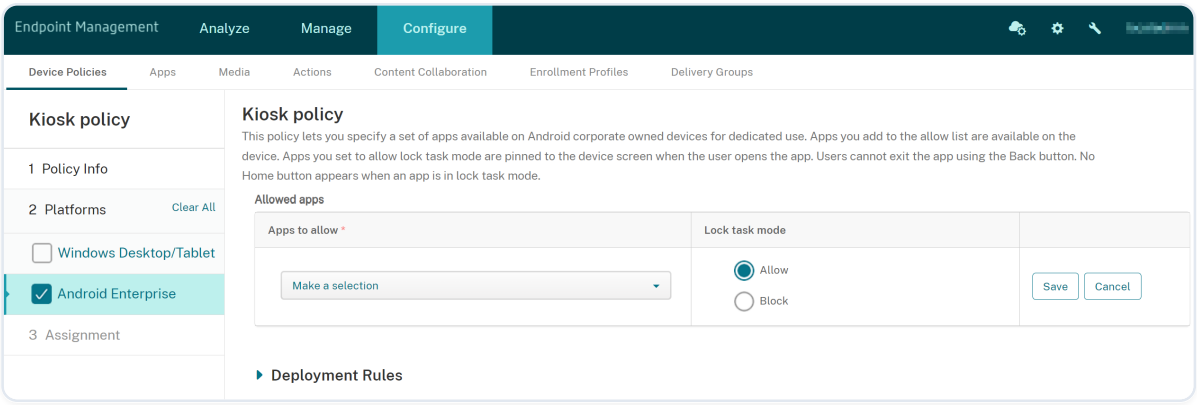
安卓企业设置

您可以允许应用程序并为专用 Android Enterprise 设备（也称为企业拥有的单用途 (COSU) 设备）设置锁定任务模式。

要允许某个应用程序，请单击**添加**。您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。

- **允许的应用程序：** 输入要允许的应用程序的程序包名称，或从列表中选择应用程序。
    - 单击**添加新项**以在列表中输入允许的应用程序的程序包名称。

- 从列表中选择现有应用程序。该列表显示在 Citrix Endpoint Management 中上传的应用程序。默认情况下，Citrix Secure Hub 和 Google Play 服务在允许列表中。



- **锁定任务模式：** 选择**允许**以在用户启动应用程序时将应用程序固定到设备屏幕。选择**阻止**以不固定应用程序。默认设置为**允许**。

当应用程序处于锁定任务模式时，用户打开应用程序时，应用程序会固定在设备屏幕上。不显示主页按钮，并且“**返回**”按钮被禁用。用户通过应用程序中编程的操作（例如注销）退出应用程序。

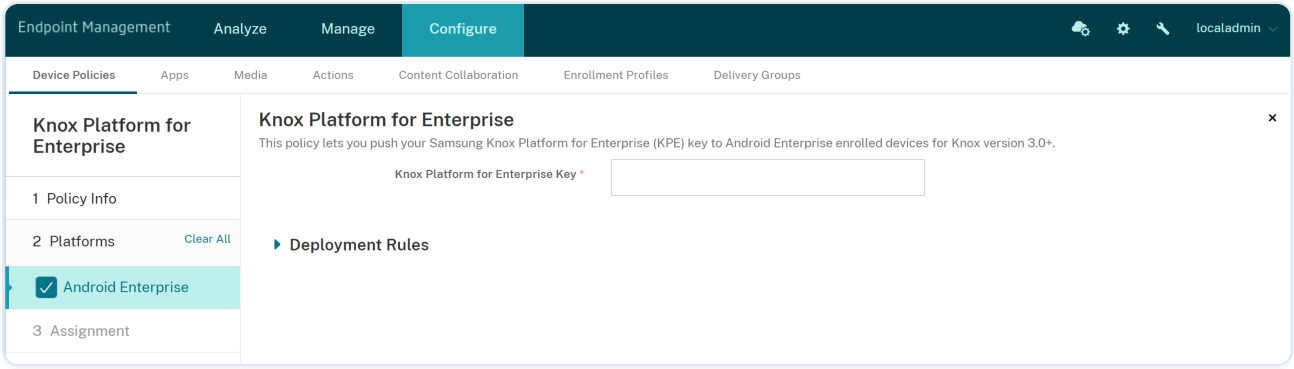
Knox Platform for Enterprise 密钥设备策略

此策略允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息。

要添加或配置此策略，请导航到**配置** > **设备策略**。有关详细信息，请参阅设备策略。

Android Enterprise 相关设置

此策略提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息。对于 Android 12 或更早版本，您必须申请 KPE 高级许可证才能使用 Knox 高级功能。对于 Android 13 或更高版本，默认提供 KPE 高级许可证。



Knox Platform for Enterprise 密钥： 输入要推送到 Android Enterprise 设备的 Samsung Knox Platform for Enterprise (KPE) 密钥。请在Samsung Knox Platform for Enterprise (KPE) 密钥处申请 KPE 许可证密钥。

启动器配置设备策略

Citrix Launcher 允许您为 Citrix Endpoint Management 部署的 Android Enterprise 设备和旧版 Android 设备自定义用户体验。

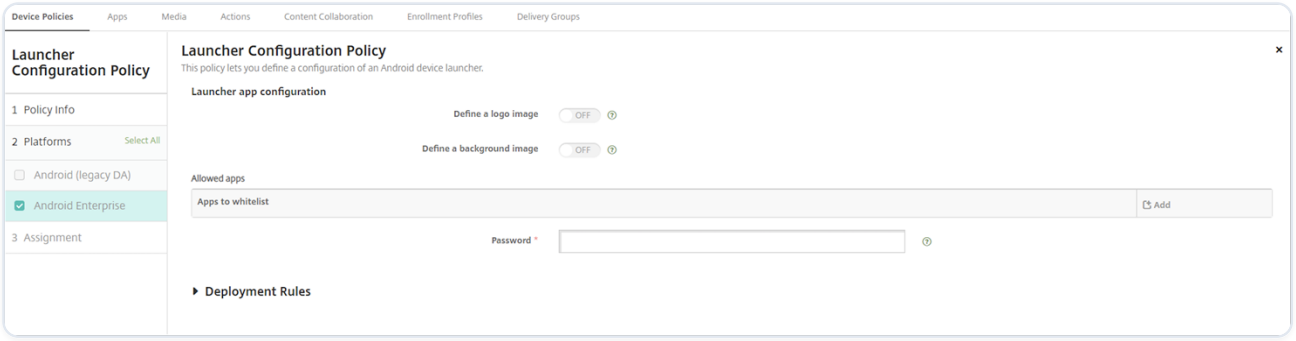
使用启动器配置策略来控制以下 Citrix Launcher 功能：

- 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像，并为 Citrix Launcher 指定自定义背景图像。
- 指定用户必须键入才能退出启动器的密码。

Citrix Launcher 并非旨在提供超越设备平台已有功能的额外安全层。

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。

安卓企业版和安卓设置



- **定义徽标图像：** 选择是否为 Citrix Launcher 图标使用自定义徽标图像。默认值为 **关**。
- **徽标图像：** 启用**定义徽标图像**后，通过单击**浏览**并导航到文件位置来选择图像文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- **定义背景图像：** 选择是否为 Citrix Launcher 背景使用自定义图像。默认值为 **关**。
- **背景图像：** 启用**定义背景图像**后，通过单击**浏览**并导航到文件位置来选择图像文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- **允许的应用程序：** 对于您要在 Citrix Launcher 中允许的每个应用程序，请单击**添加**，然后执行以下操作：
  - **要添加的新应用：** 输入要添加的应用的完整名称。例如，Android 日历应用为 com.android.calendar。
  - 单击**保存**以添加应用，或单击**取消**以取消添加应用。
- **密码：** 用户必须输入此密码才能退出 Citrix Launcher。

LDAP 设备策略

您可以在 Citrix Endpoint Management 中为 iOS 设备创建 LDAP 策略，以提供要使用的 LDAP 服务器信息，包括任何必要的帐户信息。该策略还提供了一组在查询 LDAP 服务器时要使用的 LDAP 搜索策略。

在配置此策略之前，您需要 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

- **帐户描述：** 输入可选的帐户描述。
- **帐户用户名：** 输入可选的用户名。
- **帐户密码：** 输入可选密码。仅将此字段与加密配置文件一起使用。
- **LDAP 主机名：** 输入 LDAP 服务器主机名。此字段为必填项。
- **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：** 添加在查询 LDAP 服务器时要使用的搜索设置。您可以输入任意数量的搜索设置，但必须至少添加一个搜索设置才能使帐户有用。单击**添加**，然后执行以下操作：
    - **描述：** 输入搜索设置的描述。此字段为必填项。
    - **范围：** 选择**基本**、**一级**或**子树**以定义在 LDAP 树中搜索的深度。默认值为**基本**。
        - **基本**搜索“搜索基本”指向的节点。
        - **一级**搜索基本节点及其下一级。
        - **子树**搜索基本节点及其所有子节点，无论深度如何。
    - **搜索基准：** 输入开始搜索的节点路径。例如，ou=people 或 0=example corp。此字段为必填项。
    - 单击“**保存**”以添加搜索设置，或单击“**取消**”以取消添加搜索设置。
    - 对要添加的每个搜索设置重复这些步骤。
- **策略设置**
    - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**距离删除的时间（小时）**”
        - **选择日期：** 单击日历以选择具体的删除日期。

    - **距离删除的时间（小时）：** 键入一个数字（以小时为单位），表示策略删除发生前的时间。

macOS 设置

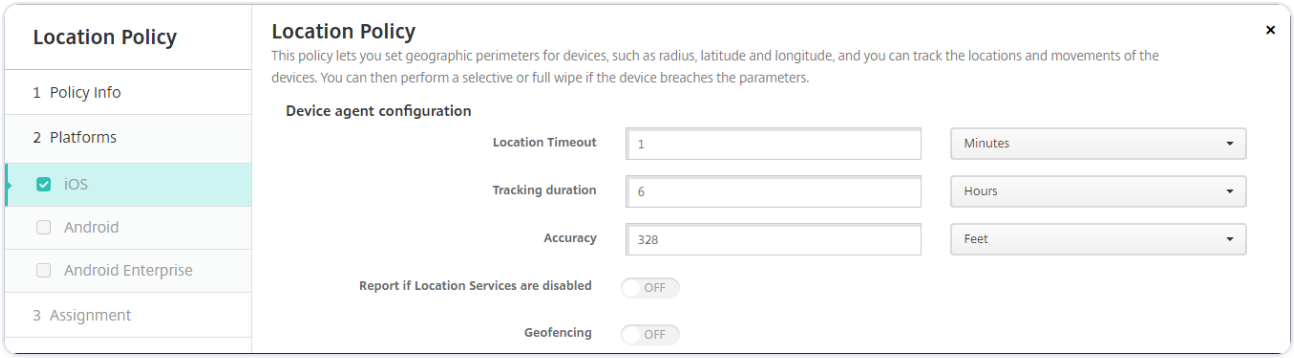
- **帐户描述：** 输入可选的帐户描述。
- **帐户用户名：** 输入可选的用户名。
- **帐户密码：** 输入可选密码。仅将此字段用于加密配置文件。
- **LDAP 主机名：** 输入 LDAP 服务器主机名。此字段为必填项。
- **使用 SSL：** 选择是否使用安全套接字层连接到 LDAP 服务器。默认值为“**开**”。
- **搜索设置：** 添加在查询 LDAP 服务器时使用的搜索设置。您可以输入任意数量的搜索设置，但必须至少添加一个搜索设置才能使帐户可用。单击“**添加**”，然后执行以下操作：
    - **描述：** 输入搜索设置的描述。此字段为必填项。
    - **范围：** 选择“**基本**”、“**一级**”或“**子树**”以定义在 LDAP 树中搜索的深度。默认值为“**基本**”。
        - **基本**”搜索“搜索基本”指向的节点。
        - **一级**”搜索基本节点及其下一级。
        - **子树**”搜索基本节点及其所有子节点，无论深度如何。
    - **搜索基本：** 输入要开始搜索的节点的路径。例如，ou=people 或 0=example corp。此字段为必填项。
    - 单击“**保存**”以添加搜索设置，或单击“**取消**”以取消添加搜索设置。
    - 对要添加的每个搜索设置重复这些步骤。
- **策略设置**
    - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**距离删除的持续时间（小时）**”
        - **选择日期：** 单击日历以选择具体的删除日期。
        - **距离删除的持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
    - **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
    - **配置文件范围：** 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 及更高版本上可用。

位置设备策略

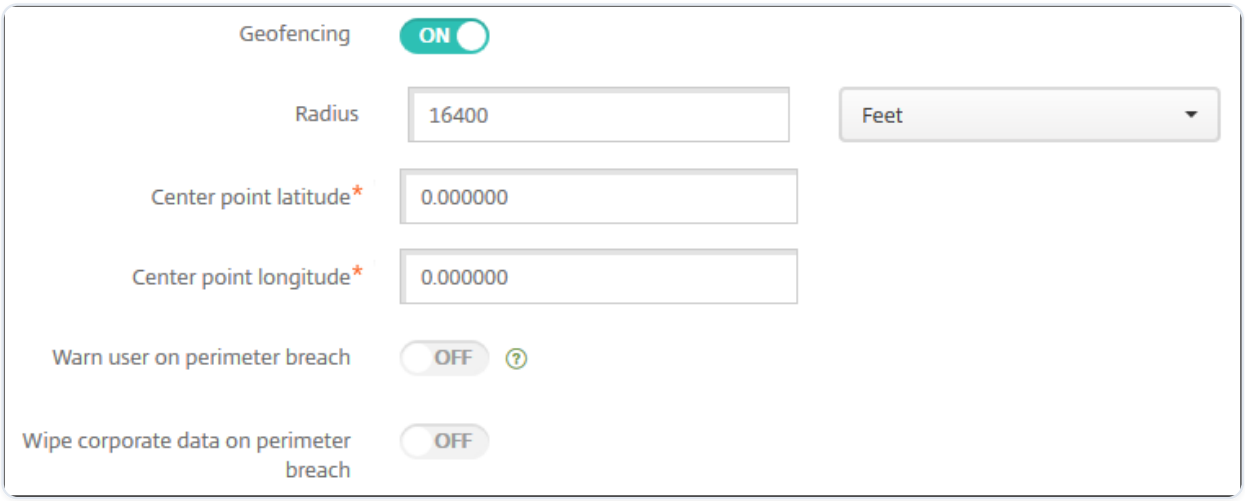
您可以在 Citrix Endpoint Management 中创建位置设备策略，以强制执行地理边界。当用户越过定义的边界（也称为*地理围栏*）时，Citrix Endpoint Management 可以执行某些操作。例如，您可以将策略配置为在用户越过定义的边界时向其发出警告消息。您还可以将策略配置为在用户越过边界时立即或延迟擦除其企业数据。有关安全操作（例如启用跟踪和定位设备）的信息，请参阅安全操作。

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。

iOS 设置



- **定位超时：** 键入一个数字，然后单击**秒**或**分钟**以设置 Citrix 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：** 键入一个数字，然后单击**小时**或**分钟**以设置 Citrix Endpoint Management 跟踪设备的时长。有效值为 1–10 小时或 10–600 分钟。默认值为**6 小时**。
- **准确性：** 键入一个数字，然后单击**米**、**英尺**或**码**以设置 Citrix Endpoint Management 跟踪设备时与设备的接近程度。有效值为 10–5000 码、30–15000 英尺或 10–5000 米。默认值为**328 英尺（100 米）**。
- **如果定位服务已禁用，则报告：** 选择当用户关闭 GPS 时设备是否向 Citrix Endpoint Management 发送报告。默认值为**关**。
- **地理围栏**

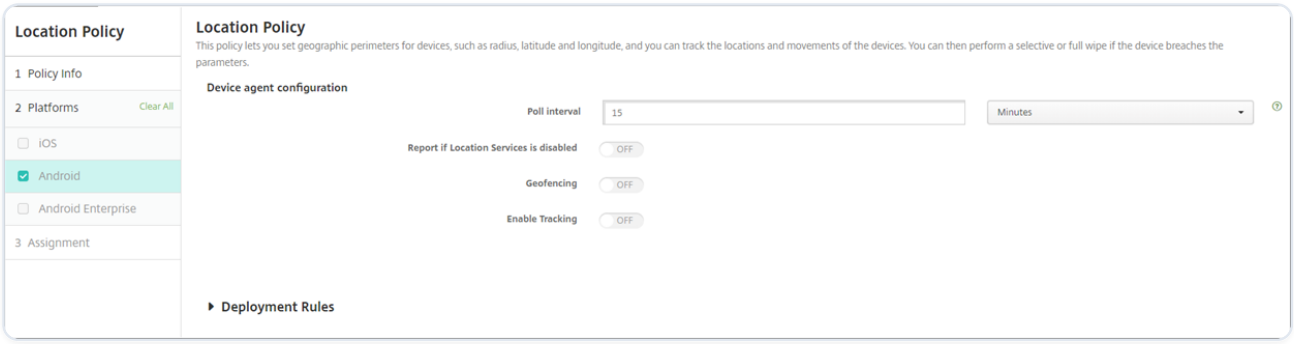


启用地理围栏时，请配置以下设置：

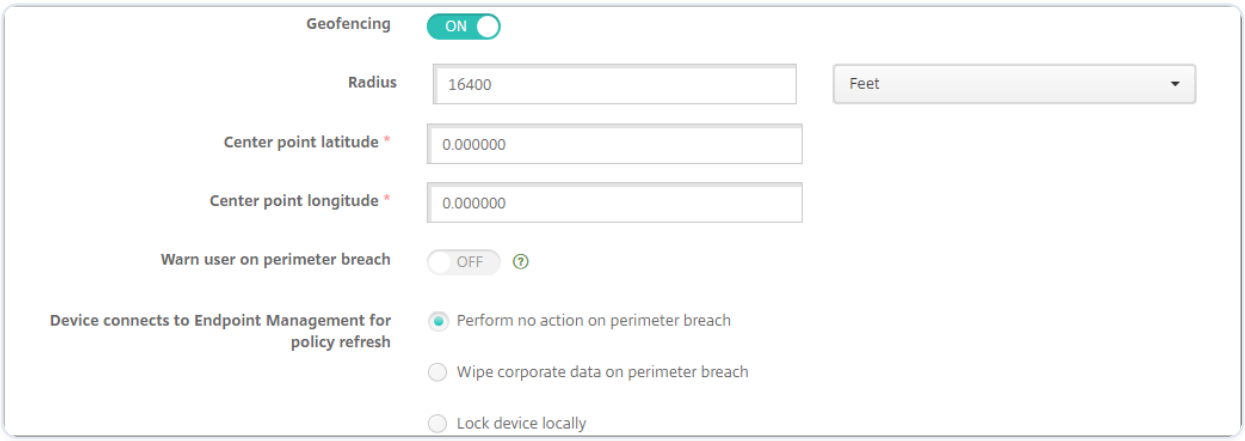
- **半径：** 键入一个数字，然后单击用于测量半径的单位。默认值为**16400 英尺（5000 米）**。半径的有效值为：
  - 164–16400 英尺
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- **中心点纬度：** 输入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- **中心点经度：** 输入经度（例如 122.402952）以定义地理围栏中心点的经度。
- **在越过边界时警告用户：** 选择当用户越过定义的边界时是否发出警告消息。默认值为“**关**”。显示警告消息不需要连接到 Citrix Endpoint Management。
- **在越过边界时擦除公司数据：** 选择当用户越过边界时是否擦除其设备。默认值为“**关**”。启用此选项后，“**本地擦除延迟**”字段将显示。
  - 键入一个数字，然后单击“**秒**”或“**分钟**”以设置在从用户设备擦除公司数据之前延迟的时间长度。此延迟使用户有机会在 Citrix 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：** 键入一个数字，然后单击“**分钟**”、“**小时**”或“**天**”以设置 Citrix Endpoint Management 尝试修复设备位置的频率。有效值为 15–1440 分钟、1–24 小时或任意天数。默认值为“**15 分钟**”。
- **在位置服务禁用时报告：** 选择当用户关闭 GPS 时设备是否向 Citrix 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：

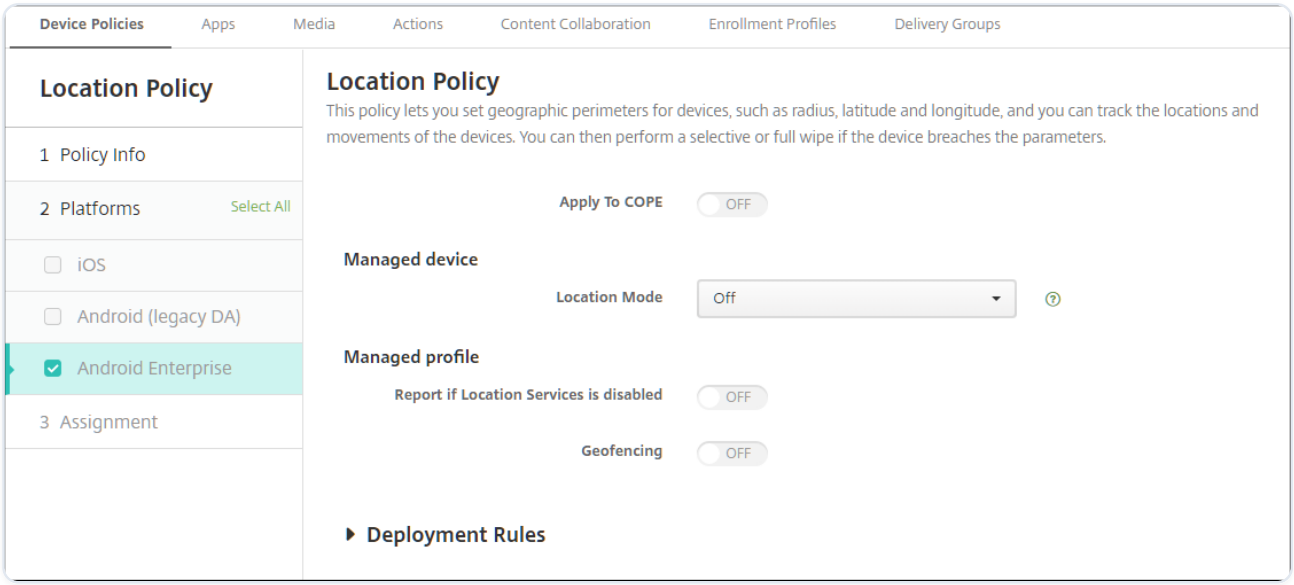
- **半径：**键入一个数字，然后单击用于测量半径的单位。默认值为 **16400 英尺（5000 米）**。半径的有效值包括：
  - 164–164000 英尺
  - 1–50 公里
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- **中心点纬度：**键入一个纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- **中心点经度：**键入一个经度（例如 122.402952）以定义地理围栏中心点的经度。
- **在突破边界时警告用户：选择当用户突破定义的边界时是否发出警告消息。默认值为关。**显示警告消息不需要连接到 Citrix Endpoint Management。

- **设备连接到 Citrix Endpoint Management 以刷新策略：**当用户突破边界时，选择以下选项之一：
  - **在突破边界时执行任何操作：**不执行任何操作。这是默认设置。
  - **在突破边界时擦除公司数据：**在指定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。
    - 键入一个数字，然后单击“**秒**”或“**分钟**”以设置在从用户设备擦除公司数据之前延迟的时间长度。此延迟使用户有机会返回到允许的位置，然后 Citrix Endpoint Management 才会选择性地擦除其设备。默认值为 **0 秒**。
  - **本地锁定设备：**在指定时间长度后锁定用户设备。启用此选项时，将显示“**锁定延迟**”字段。
    - 键入一个数字，然后单击“**秒**”或“**分钟**”以设置在锁定用户设备之前延迟的时间长度。此延迟使用户有机会返回到允许的位置，然后 Citrix Endpoint Management 才会锁定其设备。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“**关闭**”。

安卓企业版设置

要使 Android 位置跟踪正常工作，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“允许位置共享”设置
- 连接计划（建议使用 Firebase Cloud Messaging）



应用于具有工作资料的完全托管设备

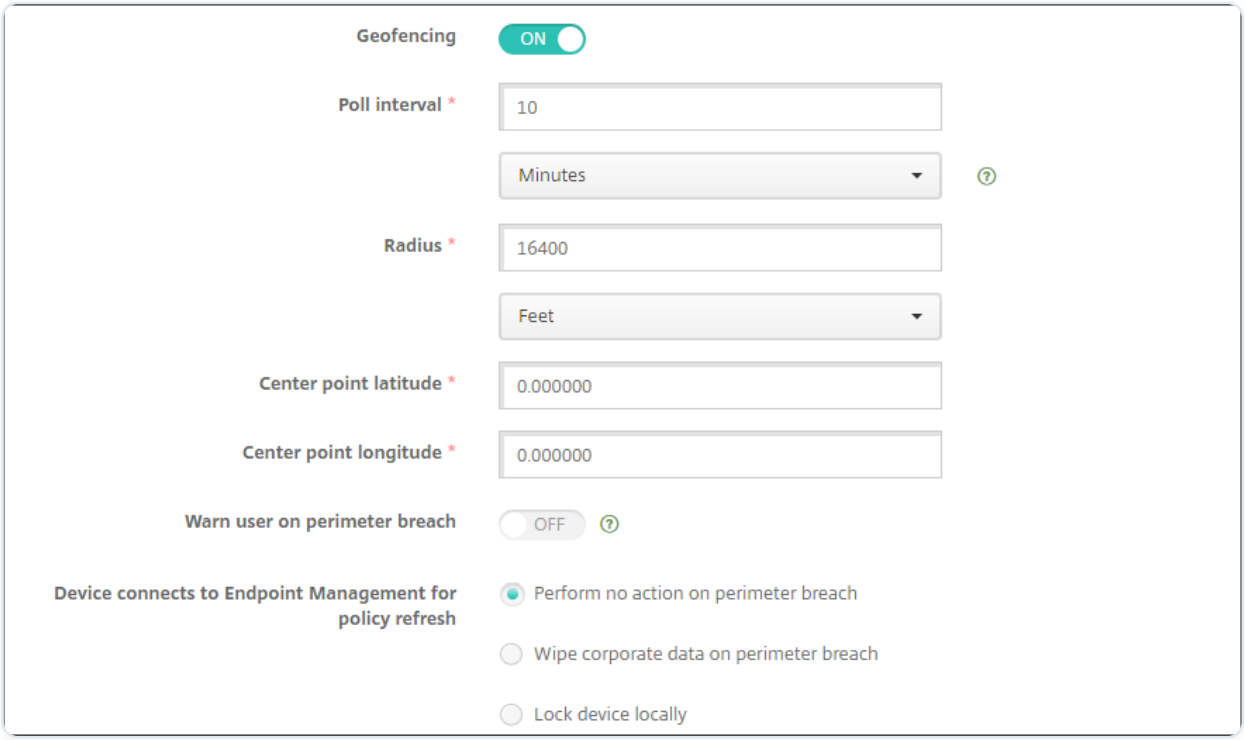
对于具有工作资料的完全托管设备（以前称为 COPE 设备），仅位置模式设置可用。

- **应用于具有工作资料的完全托管设备/公司拥有的设备上的工作资料：** 允许您为具有工作资料的完全托管设备配置位置模式。启用此设置后，请配置工作资料的设置：
  - **如果位置服务已禁用则报告：** 选择当用户关闭 GPS 时设备是否向 Citrix Endpoint Management 发送报告。默认值为“**关闭**”。
  - **地理围栏：** 请参阅本文中托管设备下的设置。

当“**应用于具有工作资料的完全托管设备/公司拥有的设备上的工作资料**”关闭时，设置将应用于托管设备和工作资料，如以下各节所示。默认值为“**关闭**”。

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“**省电**”时，才能使用“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。
  - **省电：** 仅启用网络位置提供程序。
  - **关闭：** 禁用位置检测。
- **地理围栏：**



启用**地理围栏**时，请配置以下设置：

- **轮询间隔：** 键入一个数字，然后单击**分钟**、**小时**或**天**以设置 Citrix Endpoint Management 尝试确定设备位置的频率。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续航时间产生不利影响。
- **半径：** 键入一个数字，然后单击用于测量半径的单位。默认值为**16400 英尺（5000 米）**。半径的有效值为：
  - 164–164000 英尺
  - 1–50 公里
  - 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。要查找该值，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，Citrix Endpoint Management 会在**设备详细信息 > 常规**页面中的**安全**下报告设备位置。
- **中心点经度：** 输入经度，例如 122.402952，以定义地理围栏中心点的经度。
- **在突破边界时警告用户：** 选择当用户突破定义的边界时是否发出警告消息。默认值为“**关**”。显示警告消息不需要连接到 Citrix Endpoint Management。
- **设备连接到 Citrix Endpoint Management 以刷新策略：** 当用户突破边界时，选择以下选项之一：
  - **在突破边界时执行无操作：** 不执行任何操作。此设置为默认值。
  - **在突破边界时擦除公司数据：** 在指定时间长度后擦除公司数据。启用此选项时，“**本地擦除延迟**”字段将显示。
    - 键入一个数字，然后单击“**秒**”或“**分钟**”以设置在从用户设备擦除公司数据之前延迟的时间长度。此延迟使用户有机会返回到允许的位置，然后 Citrix Endpoint Management 才会选择性地擦除其设备。默认值为“**0 秒**”。
  - **本地锁定设备：** 在指定时间长度后锁定用户设备。启用此选项时，“**锁定延迟字段**”将显示。
    - 键入一个数字，然后单击“**秒**”或“**分钟**”以设置在锁定用户设备之前延迟的时间长度。此延迟使用户有机会返回到允许的位置，然后 Citrix Endpoint Management 才会锁定其设备。默认值为“**0 秒**”。

工作配置文件

- **如果位置服务已禁用则报告：** 选择当用户关闭 GPS 时设备是否向 Citrix 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。

锁屏消息设备策略

锁屏消息策略允许您设置消息，使其在以下 iOS 设备丢失时显示：

- 共享 iPad 的登录窗口
- 受监管的 iOS 设备的锁屏

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

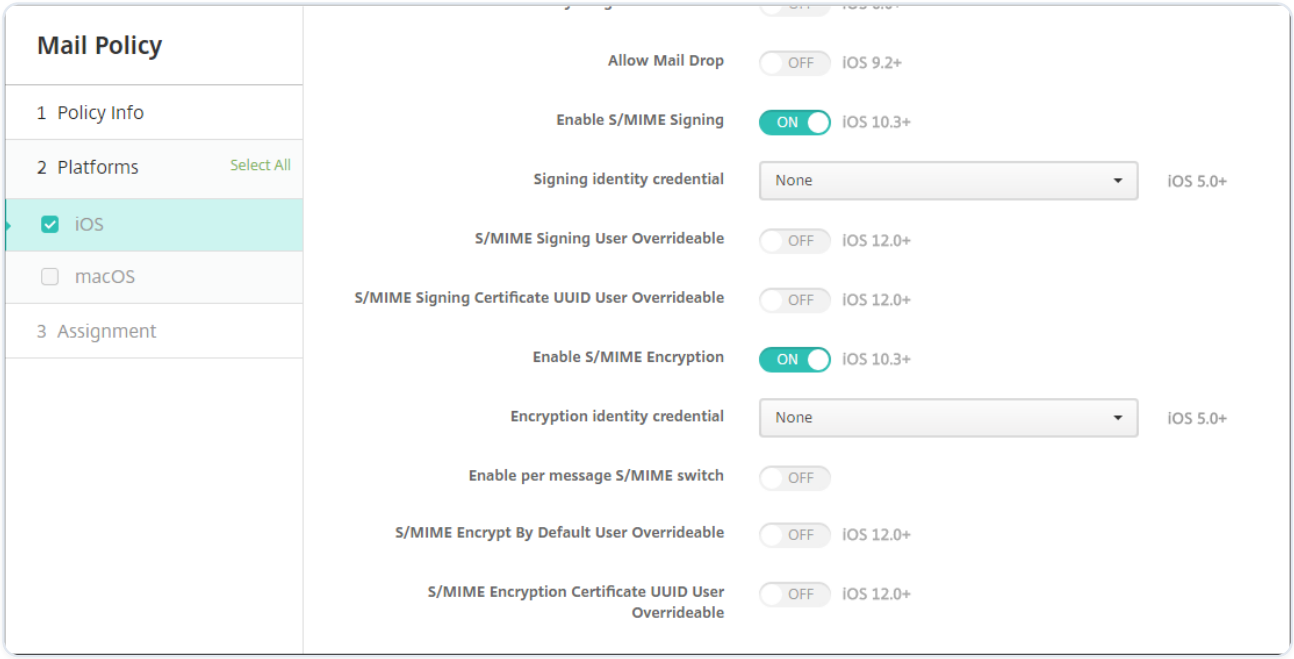
- **设备的资产标签信息：**设备的资产标签。Apple 设备会截断长字符串，因此请务必在将策略部署到生产环境之前测试字符串。字符串长度取决于 Apple 设备型号和 Apple 设置，这些设置可能会更改。
- **登录窗口和锁屏脚注：**有助于找回设备的信息，例如地址或其他联系信息。例如，您的消息可能采用“如果丢失，请归还至”的形式。Apple 设备会截断长字符串，因此请务必在将策略部署到生产环境之前测试字符串。字符串长度取决于 Apple 设备型号和 Apple 设置，这些设置可能会更改。
- **策略设置**
  - **删除策略：选择策略删除的计划方法。可用选项包括选择日期和距离删除的持续时间（小时）**
    - **选择日期：**单击日历以选择具体的删除日期。
    - **距离删除的持续时间（小时）：**键入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。

邮件设备策略

您可以在 Citrix Endpoint Management 中添加邮件设备策略，以在 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



- **帐户描述：** 键入在“邮件”和“设置”应用程序中显示的帐户描述。此字段为必填项。
- **帐户类型：** 选择 **IMAP** 或 **POP** 以选择用于用户帐户的协议。默认值为 **IMAP**。当您选择 **POP** 时，以下 **路径** 前缀选项将消失。
- **路径前缀：** 键入 **INBOX** 或您的 IMAP 邮件帐户路径前缀。此字段为必填项。
- **用户显示名称：** 键入用于邮件和其他用途的完整用户名称。此字段为必填项。
- **电子邮件地址：** 键入帐户的完整电子邮件地址。此字段为必填项。
- **传入电子邮件设置**
  - **电子邮件服务器主机名：** 键入传入邮件服务器主机名或 IP 地址。此字段为必填项。
  - **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**。此字段为必填项。
  - **用户名：** 键入电子邮件帐户的用户名。此名称通常与 @ 字符之前的电子邮件地址相同。此字段为必填项。
  - **身份验证类型：** 选择要使用的身份验证类型。默认值为 **密码**。当选择 **无** 时，以下 **密码** 字段将消失。
  - **密码：** 输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。此字段为必填项。

- **电子邮件服务器端口：** 输入传出邮件服务器端口号。如果未输入端口号，则使用给定协议的默认端口。
- **用户名：** 输入电子邮件帐户的用户名。此名称通常与电子邮件地址中 @ 字符之前的部分相同。此字段为必填项。
- **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：** 输入传出邮件服务器的可选密码。
- **传出密码与传入密码相同：** 选择传入和传出密码是否相同。默认值为“**关**”，表示密码不同。
- **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**
  - **授权在帐户之间移动电子邮件：** 选择是否允许用户执行以下操作：
    - 将电子邮件从此帐户移到另一个帐户
    - 从其他帐户转发电子邮件
    - 从其他帐户回复。

    默认设置为 **关**。
  - **仅通过邮件应用发送电子邮件：** 选择是否限制用户只能通过 iOS 邮件应用发送电子邮件。
  - **禁用邮件最近联系人同步：** 选择是否阻止用户同步最近的地址。默认设置为 **关**。此选项仅适用于 iOS 6.0 及更高版本。
  - **允许 Mail Drop：** 选择是否允许运行 iOS 9.2 及更高版本的设备使用 Apple Mail Drop。默认设置为 **关**。
  - **启用 S/MIME 签名：** 选择此帐户是否支持 S/MIME 签名。默认设置为 **开**。设置为 **开** 时，将显示以下字段。
    - **签名身份凭据：** 选择要使用的签名凭据。
    - **S/MIME 签名用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中打开和关闭 S/MIME 签名。默认设置为 **关**。此选项适用于 iOS 12.0 及更高版本。
    - **S/MIME 签名证书 UUID 用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中选择要使用的签名凭据。默认设置为 **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。默认设置为 **关**。设置为 **开** 时，将显示以下字段。
    - **加密身份凭据：** 选择要使用的加密凭据。

  - **启用每条消息 S/MIME 开关：** 设置为 **开** 时，会向用户显示一个选项，用于打开或关闭他们撰写的每条消息的 S/MIME 加密。默认设置为 **关**。
  - **S/MIME 默认加密用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中选择 S/MIME 是否默认开启。默认设置为 **关**。此选项适用于 iOS 12.0 及更高版本。
  - **S/MIME 加密证书 UUID 用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中打开和关闭 S/MIME 加密身份和加密。默认设置为 **关**。此选项适用于 iOS 12.0 及更高版本。

- **策略设置**
  - **删除策略：** 若要稍后删除策略，请将此设置配置为在“**选择日期**”或“**直到删除的持续时间（以小时为单位）**”时删除策略。
  - **允许用户移除策略：** 允许用户**始终**移除邮件策略，或者**需要密码**才能移除，或者**从不**移除。仅适用于 macOS。
  - **配置文件范围：** 仅适用于 macOS，选择策略是应用于每个**用户**级别还是整个**系统**。

托管配置策略

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。您为要控制的每个 Android Enterprise 应用程序创建此策略。

应用程序开发人员定义了应用程序可用的选项和工具提示。如果工具提示提及使用“模板化值”，请改用相应的 Citrix Endpoint Management 宏。有关详细信息，请参阅 远程配置概述（在 Android 开发者网站上）和 宏。

应用程序配置设置可以包括以下各项：

- 电子邮件应用程序设置
- 允许或阻止 Web 浏览器的 URL
- 通过蜂窝连接或仅通过 Wi-Fi 连接控制应用程序内容同步的选项

有关应用程序中显示的设置的信息，请联系应用程序开发人员。

> **注意：**

> 适用于 Android 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档以反映此名称更改。

先决条件

- 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 Citrix Endpoint Management。有关详细信息，请参阅 将应用程序添加到 Citrix Endpoint Management。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

每应用 VPN 的要求

要为 AE 创建每应用 VPN，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，您必须验证是否满足以下先决条件：

- 本地 NetScaler Gateway
- 设备上安装了以下应用程序：
  - Citrix 单点登录
  - Citrix 安全中心

为 AE 设备配置按应用 VPN 的一般工作流程如下：

1. 按照本文所述配置 VPN 配置文件。
2. 配置 Citrix ADC 以接受来自按应用 VPN 的流量。有关详细信息，请参阅 (/zh-cn/citrix-gateway/current-release/vpn-user-config/configure-full-vpn-setup.html)。

限制

由于 Android 11 中引入的软件包可见性限制，Android 11+ 设备上的 Android Enterprise 环境中按应用 VPN 存在以下限制：

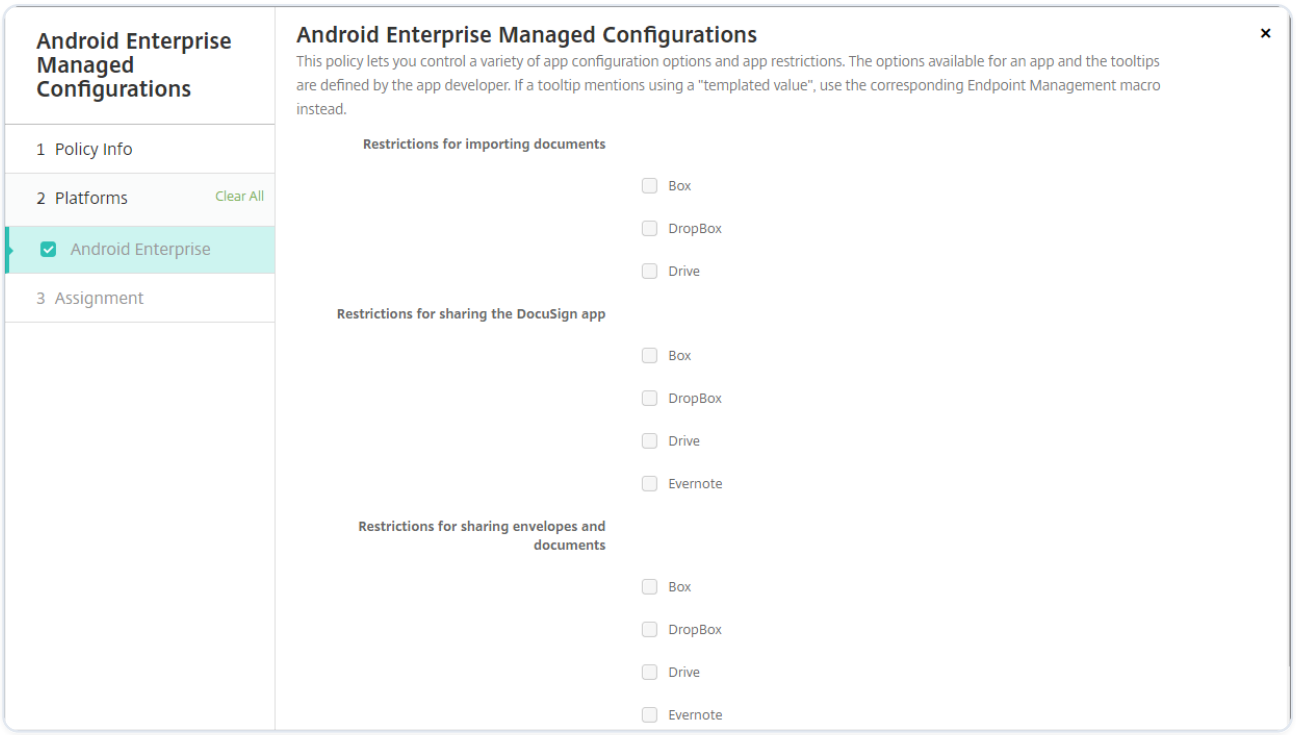
- 如果在 VPN 会话启动后，将属于允许/拒绝列表中的应用程序部署到设备，则最终用户必须重新启动 VPN 会话，以便该应用程序通过 VPN 会话路由其流量。
- 如果通过始终开启的 VPN 会话使用按应用 VPN，则在设备上安装新应用程序后，最终用户必须重新启动工作资料或重启设备，以便应用程序的流量通过 VPN 会话路由。

> **注意：**
>
> 如果您使用的是 Citrix SSO for Android 23.8.1 或更高版本，则这些限制不适用。有关详细信息，请参阅 Always On VPN 的自动重启。

安卓企业版设置

选择添加托管配置设备策略后，将出现一个选择应用程序的提示。如果 Citrix Endpoint Management 中没有添加 Android Enterprise 应用程序，则无法继续。

选择应用程序后，配置策略设置。这些设置特定于每个应用程序。



为 Android Enterprise 配置 VPN 配置文件

使用托管配置设备策略，通过 Citrix SSO 应用使 VPN 配置文件可用于 Android Enterprise 设备。

首先，将 Citrix SSO 作为 Google Play 商店应用添加到 Citrix Endpoint Management 控制台。请参阅 添加公共应用商店应用。

控制台中的 SSO 应用(/en-us/citrix-endpoint-management/media/citrixsso-app-added.png)

观看此视频了解更多信息：

(https://www.youtube.com/watch?v=wcsTKsfjFmc)[(/en-us/citrix-endpoint-management/media/shared-video-placeholder.png)]

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。已安装 Citrix SSO 应用并部署了策略的设备可以访问您创建的 VPN 配置文件。

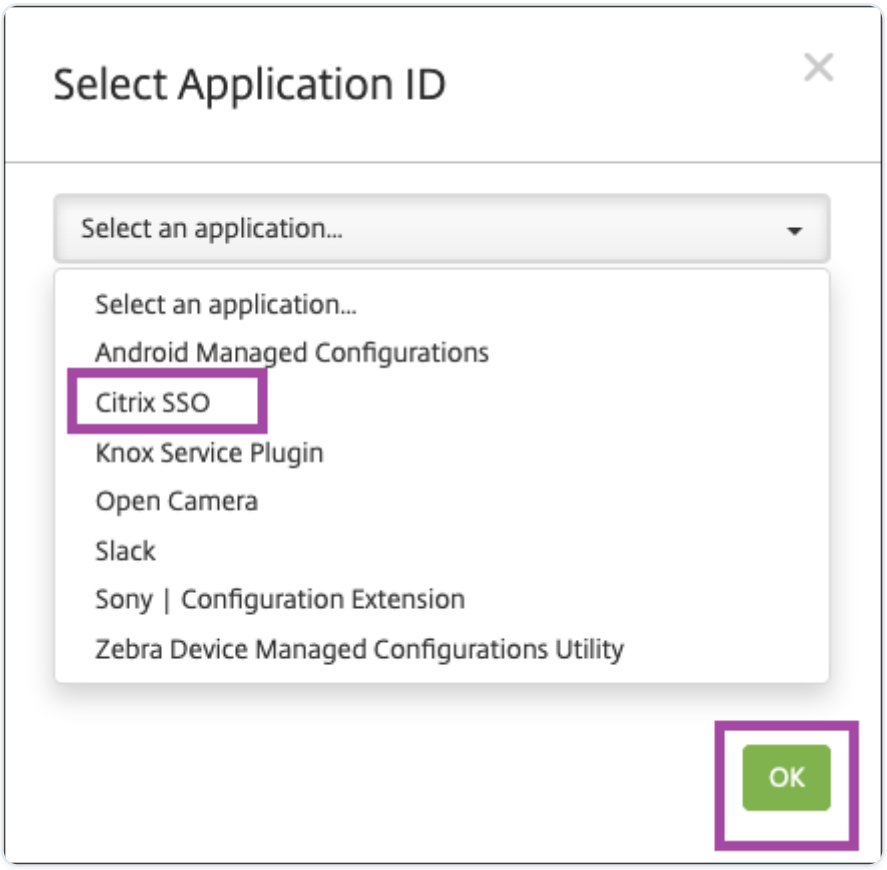
如果满足以下条件，Citrix Endpoint Management 将使用设备密钥库中的用户证书：

- NetScaler Gateway 配置为基于证书的身份验证。
- 在 Citrix Endpoint Management 页面 **设置 > NetScaler Gateway** 中启用了**交付用户证书以进行身份验证**。

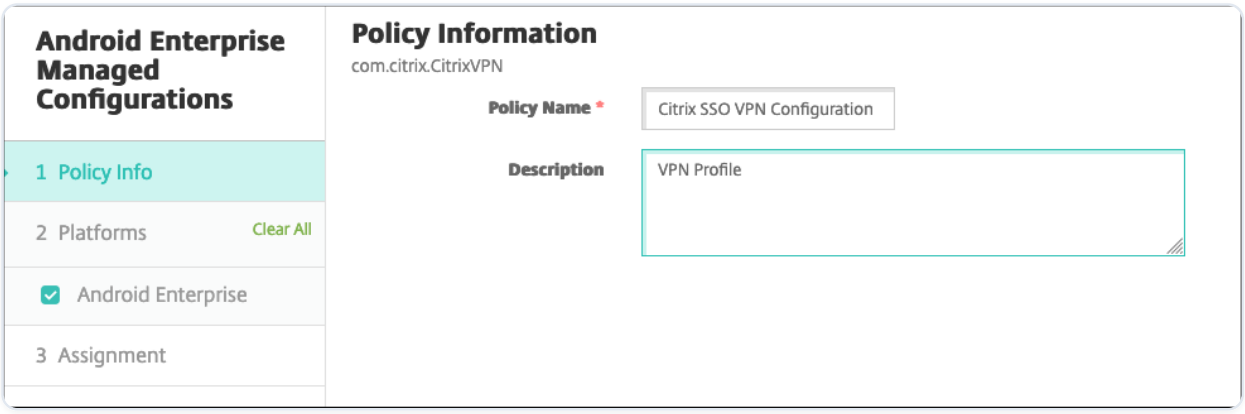
您需要 NetScaler Gateway FQDN 和端口。

1. 在 Citrix 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**。

   选择 Android Enterprise 策略(/en-us/citrix-endpoint-management/media/select-ae-managed-configuration-policy.png)
3. 当**选择应用程序 ID** 窗口出现时，从列表中选择 **Citrix SSO**，然后单击**确定**。



4. 为您的 Citrix SSO VPN 配置键入名称和描述。单击 **下一步**。



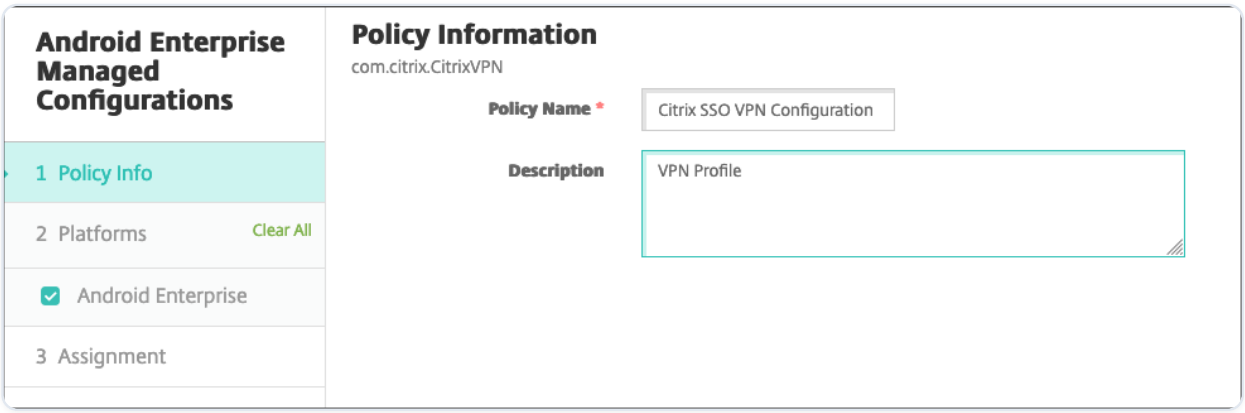
5. 配置 VPN 配置文件参数。

- **VPN 配置文件名称：** 为 VPN 配置文件键入一个名称。如果您要创建多个 VPN 配置文件，请为每个配置文件使用唯一的名称。如果您不提供名称，则您在 **服务器地址** 字段中输入的地址将用作 VPN 配置文件名称。
- **服务器地址(*):** 键入您的 NetScaler Gateway FQDN。如果您的 NetScaler Gateway 端口不是 443，请同时键入您的端口。使用 URL 格式。例如，`https://gateway.mycompany.com:8443`。
- **用户名（可选）：** 提供最终用户用于向 NetScaler Gateway 进行身份验证的用户名。您可以将 Citrix Endpoint Management 宏 {user.username} 用于此字段。（请参阅 宏。）如果您不提供用户名，则当用户连接到 NetScaler Gateway 时，系统会提示他们提供用户名。
- **密码（可选）：** 提供最终用户用于向 NetScaler Gateway 进行身份验证的密码。如果您不提供密码，则当用户连接到 NetScaler Gateway 时，系统会提示他们提供密码。
- **证书别名（可选）：** 键入证书别名。证书别名使应用程序更容易访问证书。当相同的证书别名与凭据设备策略一起使用时，应用程序会检索证书并对 VPN 进行身份验证，而无需用户执行任何操作。
- **网关证书固定（可选）：** 描述用于 NetScaler Gateway 的证书固定的 JSON 对象。示例值：`{"hash-alg" : "sha256", "pinset" : ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="]}`。有关详细信息，请参阅 使用 Android Citrix SSO 进行 NetScaler Gateway 证书固定。
- **每应用 VPN 类型（可选）：** 如果您正在使用每应用 VPN 来限制哪些应用使用此 VPN，则可以配置此设置。如果您选择 **允许**，则 **每应用 VPN 应用列表** 中列出的应用包的网络流量将通过 VPN 路由。所有其他应用的流量将路由到 VPN 外部。如果您选择 **不允许**，则 **每应用 VPN 应用列表** 中列出的应用包的网络流量将路由到 VPN 外部。所有其他应用的流量将通过 VPN 路由。默认值为 **允许**。
- **每应用 VPN 应用列表：** 一个应用列表，其流量在 VPN 上是允许还是阻止，具体取决于 **每应用 VPN 类型** 的值。列出用逗号或分号分隔的应用包名称。应用包名称区分大小写，并且

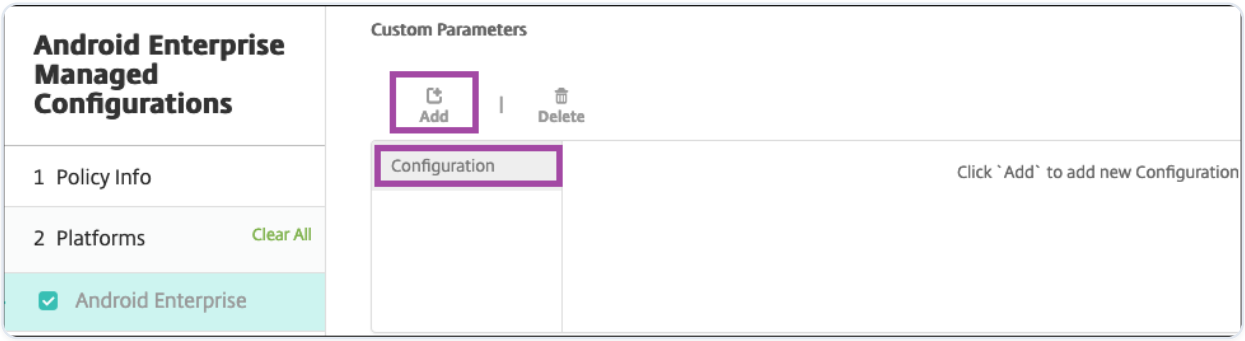
必须与它们在 Google Play 商店中显示的名称完全一致。此列表是可选的。如果为空，则表示配置设备范围的 VPN。

- **默认 VPN 配置文件：** 键入当用户在 Citrix SSO 应用中点击连接开关而不是特定配置文件时要使用的 VPN 配置文件名称。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。对于始终开启的 VPN，此字段必须设置为用于建立始终开启的 VPN 的 VPN 配置文件名称。
- **始终开启的 VPN（可选）：** 此属性指示 VPN 配置文件是否配置为始终开启的 VPN 配置文件。当设置为 **true** 时，表示该 VPN 配置文件是始终开启的 VPN 配置文件。默认值为 **false**。此属性只能分配给主 VPN 配置文件。启用此属性对于确保始终开启的 VPN 的可靠运行至关重要。
- **禁用用户配置文件：** 如果此设置为“开”，则用户无法在其设备上创建自己的 VPN。如果此设置为“关”，则用户可以在其设备上创建自己的 VPN。默认值为“关”。
- **阻止不受信任的服务器：** 在以下任一情况下，此设置处于“关闭”状态：
  - 当您为 NetScaler Gateway 使用自签名证书时
  - 当颁发 NetScaler Gateway 证书的 CA 的根证书不在系统 CA 列表中时。

  如果此设置处于“开启”状态，Android 操作系统将验证 NetScaler Gateway 证书。如果验证失败，则不允许连接。默认值为“开启”。



6. （可选）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**”。

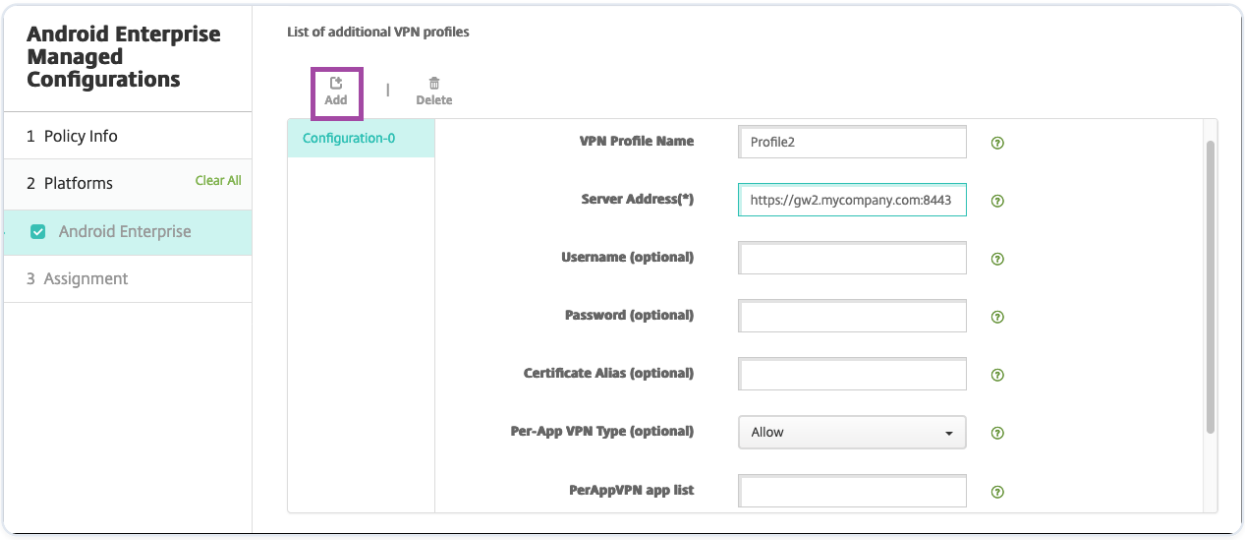


参数名称	描述	值
XenMobileDeviceId	此字段是用于根据设备在 Citrix Endpoint Management 中的注册情况进行网络访问检查的设备 ID。如果 Citrix Endpoint Management 注册并管理设备，则允许 VPN 连接。否则，在建立 VPN 时将拒绝身份验证。	为了让 Citrix Endpoint Management 确定设备的注册和管理状态，XenMobileDeviceID 的值设置为 `DeviceID_${device.id}`。
UserAgent	此文本附加到 User-Agent HTTP 标头，用于对 NetScaler Gateway 进行额外检查。Citrix SSO 应用程序在与 NetScaler Gateway 通信时，会将此文本的值附加到 User-Agent HTTP 标头。	键入要附加到 User-Agent HTTP 标头的文本。此文本必须符合 HTTP User-Agent 规范。
EnableDebugLogging	在 Citrix SSO 应用程序上启用调试日志记录，以帮助排查 Always On VPN 情况下的 VPN 连接问题。您可以在任何一个托管 VPN 配置中启用它。调试日志记录在处理托管配置时生效。	**True**：启用调试日志记录。默认值：**False**
DisableLogoutFromStoreOnExplicitDisconnect	控制当最终用户从应用程序 UI 显式断开 VPN 会话时是否从商店注销。仅适用于 Citrix Secure Private Access 部署。	**True**：禁用从 Secure Private Access 商店注销，并保持 Secure Private Access 会话完整，仅断开 Citrix Secure Access 应用程序会话。默认值：**False**。



要创建另一个自定义参数，请再次单击**添加**。

7. （可选）创建更多 VPN 配置文件配置。单击配置列表下的**添加**。新配置将显示在列表中。选择新配置并重复步骤 5，以及（可选）步骤 6。



8. 创建完所有所需的 VPN 配置文件后，单击**下一步**。
9. 为 Citrix SSO 配置此托管配置的部署规则。
10. 点击 **保存**。

此 Citrix SSO 托管配置现在显示在您已配置的设备策略列表中。

要为您配置的 VPN 配置文件启用始终开启，请设置 (/zh-cn/citrix-endpoint-management/policies/options-policy.html#android-enterprise-settings)。

> **注意：**
>
> Android Enterprise 的始终开启 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 用户需从托管的 Google Play 商店安装 Citrix SSO。

您配置的 VPN 配置文件会显示在应用程序的**托管连接**区域。用户点击 VPN 配置文件即可使用该 VPN 配置文件进行连接。

设备上 SSO 应用程序的托管连接区域(/en-us/citrix-endpoint-management/media/citrixsso-user-device-1.png)

用户通过身份验证并连接后，VPN 配置文件旁边会出现一个复选标记。密钥图标表示 VPN 已连接。

使用 Zebra OEMConfig 管理斑马 Android 设备

使用 Zebra Technologies OEMConfig 管理工具管理斑马 Android 设备。有关 Zebra OEMConfig 应用程序的信息，请参阅 Zebra Technologies 网站。

Citrix Endpoint Management 支持 Zebra OEMConfig 9.2 及更高版本。有关在设备上安装 Zebra OEMConfig 的系统要求信息，请参阅 Zebra Technologies 网站上的 OEMConfig 设置。

我们目前支持以下斑马设备：

- EC50、EC55、ET56
- TC52x, TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

开始：在 Citrix Endpoint Management 控制台中，将 Zebra OEMConfig 应用程序添加为 Google Play 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。该策略适用于已安装 Zebra OEMConfig 应用程序并已部署策略的斑马设备。

1. 在 Citrix 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**。

   选择 Android Enterprise 策略(/en-us/citrix-endpoint-management/media/select-ae-managed-configuration-policy.png)
3. 当出现“**选择应用程序 ID**”窗口时，从列表中选择 **ZebraOEMConfig powered by MX**，然后单击 **确定**。
4. 为您的 Zebra OEMConfig 配置键入名称和描述。单击 **下一步**。
5. 为 Zebra OEMConfig 配置键入名称。
6. 配置可用参数。例如：
   - 要禁用设备正面的摄像头，请选择 **摄像头配置** 并将 **前置摄像头使用** 设置为 **关闭**。
   - 要更改设备时间格式，请选择 **时钟配置** 并将 **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 网站上的 Zebra 托管配置。

1. （可选）创建更多 Zebra OEMConfig 配置。在配置列表下单击 **添加**。新配置将显示在列表中。选择新配置并配置参数。
2. 创建完所有所需的 Zebra OEMConfig 配置后，单击 **下一步**。
3. 为 Zebra OEMConfig 的此托管配置配置部署规则。
4. 点击 **保存**。

使用预定义书签管理 Chrome 浏览器

以下是使用预定义书签管理 Chrome 浏览器的示例：

```
[



{ "toplevel_name": "My managed bookmarks folder" }

,



{ "name": "Google", "url": "[google.com|http://google.com/]" }

,



{ "name": "Youtube", "url": "[youtube.com|http://youtube.com/]" }

,

{

"nested_links": [



{ "name": "Chromium", "url": "[chromium.org|http://chromium.org/]" }

,
```

```
{ "name": "Chromium Developers", "url": "[dev.chromium.org|http://
dev.chromium.org/]" }

],

"name": "Chrome links"

}

]
```

支持托管配置反馈 (技术预览版)

有关支持托管配置反馈功能的更多信息，请参阅支持托管配置反馈。

托管域设备策略

您可以定义适用于电子邮件和 Safari 浏览器的托管域。托管域通过控制哪些应用程序可以打开从使用 Safari 的域下载的文档来帮助您保护公司数据。

对于 iOS 监管设备，您可以指定：

- URL 或子域，用于控制用户如何从浏览器打开文档、附件和下载内容。
- 用户可以在 Safari 中保存密码的 URL。

有关将 iOS 设备设置为监管模式的步骤，请参阅 使用 Apple Configurator 2 部署设备。

当用户向其域不在托管电子邮件域列表中的收件人发送电子邮件时，邮件会在用户的设备上标记，以警告他们正在向公司域之外的人发送邮件。

对于文档、附件或下载等项目：当用户使用 Safari 从托管 Web 域列表中的 Web 域打开项目时，相应的公司应用程序会打开该项目。如果项目不是来自托管 Web 域列表中的 Web 域，则用户无法使用公司应用程序打开该项目。他们必须使用个人、非托管应用程序。

对于监管设备，即使您未指定 Safari 密码自动填充域：如果设备配置为临时多用户，则用户无法保存密码。但是，如果设备未配置为临时多用户，则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

要指定域：

格式	说明
`example.com`	将 `example.com` 下的任何路径视为托管，但 `site.example.com/` 除外。
`foo.example.com`	将 `foo.example.com` 下的任何路径视为托管，但 `example.com/` 或 `bar.example.com/` 除外。
`*.example.com`	将 `foo.example.com` 或 `bar.example.com` 下的任何路径视为托管，但 `example.com/` 除外。
`example.com/sub`	将 `example.com/sub` 及其下的任何路径视为托管，但 `example.com/` 除外。
`foo.example.com/sub`	将 `foo.example.com/sub` 下的任何路径视为托管，但 `example.com`、`example.com/sub`、`foo.example.com/` 或 `bar.example.com/sub` 除外。
`*.example.com/sub`	将 `foo.example.com/sub` 或 `bar.example.com/sub` 下的任何路径视为托管，但 `example.com` 或 `foo.example.com/` 除外。

规则：

- 比较域时，URL 中开头的“www.”和末尾的斜杠将被忽略。
- 如果条目包含端口号，则只有指定该端口号的地址才被视为托管。否则，只有标准端口被视为托管（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`。
- 托管的 Safari Web 域定义是累积的。所有托管的 Safari Web 域负载中定义的模式都用于匹配 URL 请求。

设置：

- **托管域**

- **未标记的电子邮件域：** 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**”以不保存电子邮件域。
- **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**”以不保存 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**”以不保存自动填充域。

- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项为“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

最大常驻用户设备策略

最大常驻用户设备策略适用于运行 iOS (iPadOS) 的共享设备。有关共享 iPad 的更多信息，请参阅与 Apple 教育功能集成。

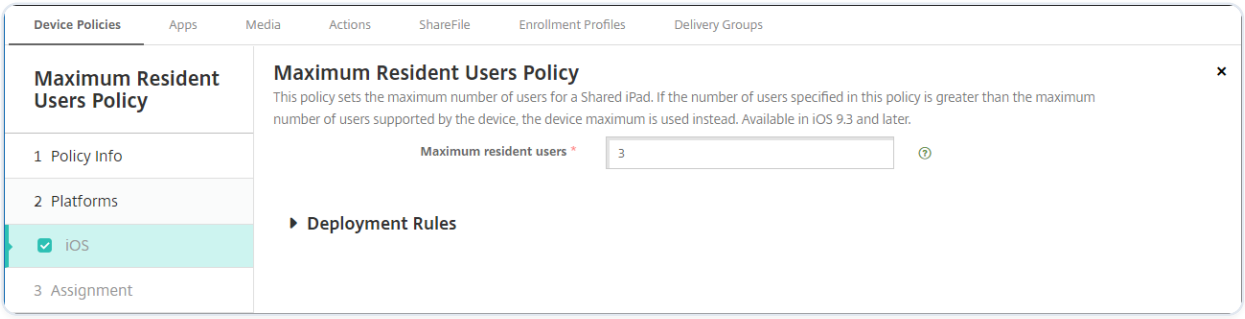
此策略必须在 iPad 在“设置助理”期间处于“等待配置”阶段时部署。Apple 不允许在共享 iPad 注册后部署此策略。

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：** 共享 iPad 的最大用户数。如果此策略中指定的用户数大于设备支持的最大用户数：Citrix Endpoint Management 将改用设备的最大值。默认值为 **5** 个用户。

Apple 建议您将最大常驻用户数的值保持在尽可能低的水平。较低的值可以最大程度地增加每个用户的 iPad 存储空间。此外，较低的值可以最大程度地减少与 iCloud 的通信，并提供更快的登录体验。有关 Apple 如何处理 iPad 上的共享存储的信息，请参阅 `<https://developer.apple.com/education/shared-ipad/>`。



MDM 选项设备策略

MDM 选项设备策略管理受监管 iOS 设备上的“查找我的 iPhone/iPad 激活锁”。有关将 iOS 设备设置为受监管模式的步骤，请参阅 使用 Apple Configurator 2 部署设备。

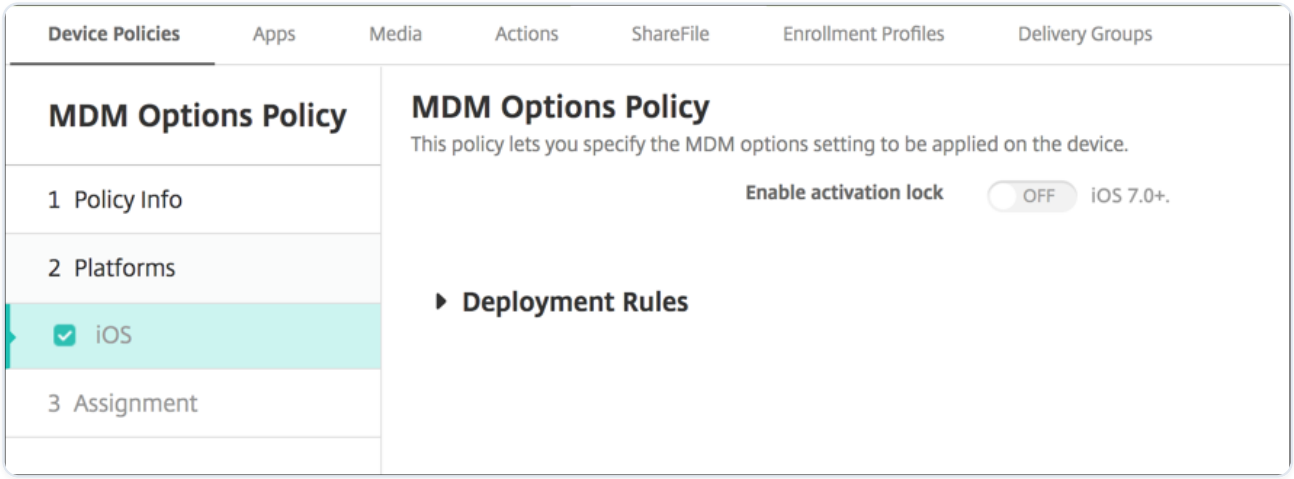
激活锁是“查找我的 iPhone/iPad”的一项功能，可防止丢失或被盗的受监管设备重新激活。激活锁需要用户 Apple ID 和密码，才能关闭“查找我的 iPhone/iPad”、抹掉设备或重新激活设备。对于贵组织拥有的设备，绕过激活锁是必要的，例如，用于重置或重新分配设备。

要启用激活锁，您需要配置并部署 Citrix Endpoint Management MDM 选项设备策略。然后，您可以从 Citrix Endpoint Management 控制台管理设备，而无需用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 Citrix Endpoint Management 控制台发出“激活锁绕过”安全操作。

例如，如果用户归还了丢失的手机，或者在完全擦除之前或之后设置设备：当手机提示输入 Apple App Store 帐户凭据时，您可以通过从 Citrix Endpoint Management 控制台发出“激活锁绕过”安全操作来绕过该步骤。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅 设备策略。

iOS 设置



- **启用激活锁：**选择是否在您部署此策略的设备上启用激活锁。默认值为 **Off**。

在您通过部署 MDM 选项设备策略启用激活锁后：当您在 **Manage > Devices** 页面上选择这些设备并单击 **Security** 时，安全操作 **激活锁绕过** 将显示。激活锁绕过允许您在设备激活之前从受监管设备中移除激活锁，而无需知道设备用户的 Apple ID 和密码。您可以在完全擦除之前或之后向设备发送激活锁绕过。有关详细信息，请参阅 绕过 iOS 激活锁。

网络设备策略

网络设备策略允许您通过定义以下各项来管理用户如何将其设备连接到 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。

先决条件

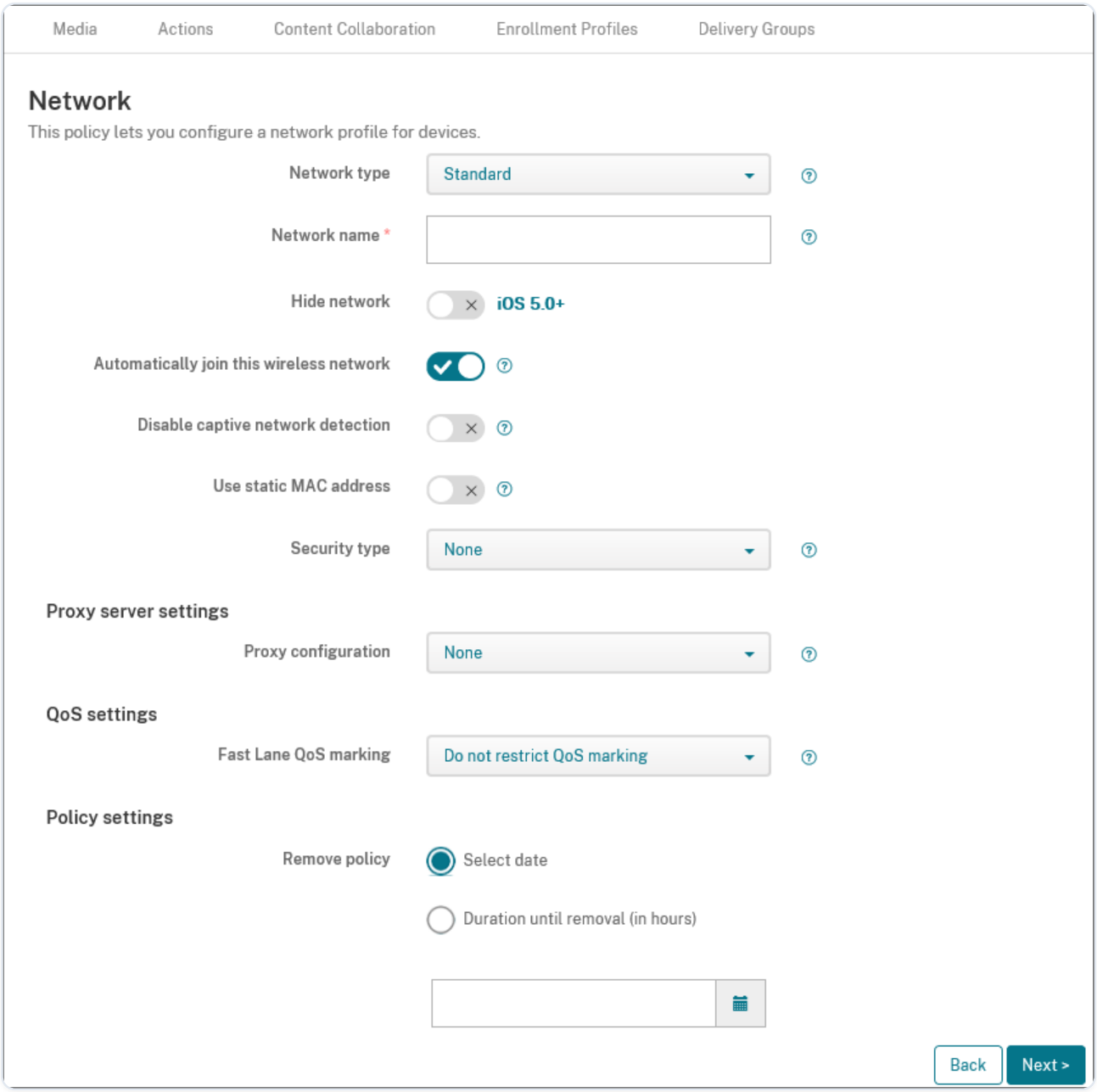
在创建策略之前，请完成以下操作：

- 创建您计划使用的任何交付组。
- 了解网络名称和类型。
- 了解您计划使用的任何身份验证或安全类型。
- 了解您可能需要的任何代理服务器信息。
- 安装所有必需的 CA 证书。

- 拥有所有必需的共享密钥。
- 创建用于基于证书的身份验证的 PKI 实体。
- 配置凭据提供程序。

有关详细信息，请参阅身份验证及其子文章。

iOS 设置



- **网络类型：** 在列表中，选择**标准**、**旧版热点**或**Hotspot 2.0**以设置您计划使用的网络类型。
- **网络名称：** 键入设备可用网络列表中显示的 SSID。不适用于**Hotspot 2.0**。
- **隐藏网络：** 选择网络是否隐藏。

- **自动加入此无线网络：** 选择设备是否自动加入网络。如果设备已连接到其他网络，则不会加入此网络。用户必须先断开与上一个网络的连接，设备才能自动连接。默认值为**开**。
- **禁用强制网络检测：** 强制网络助手可帮助用户访问订阅或 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**，设备仍可连接到强制网络，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会使用不同的 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 个人
  - 任意 (Personal)
  - WEP 企业版
  - WPA/WPA2/WPA3 企业版：对于最新版本的 Windows 10，配置简单证书注册协议 (SCEP) 以使用 WPA-2 企业版。Citrix Endpoint Management 随后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，请转至**设置 > 凭据提供程序**的“分发”页面。有关详细信息，请参阅凭据提供程序。
  - 任何 (企业版)

以下各节列出了您可以为上述每种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 连接如何通过代理服务器路由，然后配置任何其他选项。默认值为**无**，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：** 键入可选用户名以向代理服务器进行身份验证。
    - **密码：** 键入可选密码以向代理服务器进行身份验证。
  - 如果选择**自动**，请配置以下设置：

  - **服务器 URL：** 键入定义代理配置的 PAC 文件的 URL。
  - **如果 PAC 不可达，则允许直接连接：** 选择当 PAC 文件不可达时是否允许用户直接连接到目标。默认值为**开**。

- **Fast Lane QoS 标记：** 如果您不限制支持 Cisco Fast Lane QoS 的 Wi-Fi 网络的 QoS 标记，则所有应用程序都允许使用 L2 和 L3 标记。如果您限制 QoS 标记，请指定可以使用 L2 和 L3 标记的应用程序。

  - **启用 QoS 标记：** 如果您限制 QoS 标记，请使用此设置将其完全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：** 将应用程序包 ID 添加到此列表，以允许该应用程序使用 QoS 标记。

- **Hotspot 2.0 设置**

  - **显示的运营商名称：** Hotspot 设备广播的友好名称。用户在其可用 Wi-Fi 网络列表中会看到此名称。
  - **域名：** 用于 Hotspot 2.0 协商的域名。
  - **允许连接到漫游合作伙伴网络：** 如果设置为“**开**”，则脱离其家庭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 属于具有共享身份验证方法的组织。如果您配置的 Hotspot 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：** 配置用于向漫游网络识别用户的领域名称列表。NAI 以 `user@realm` 形式传输。
  - **移动国家/地区代码 (MCC) 和移动网络配置 (MNC)：** 移动国家/地区代码由三位数字组成，用于标识网络的国家/地区。移动网络代码由 2 或 3 位唯一数字组成。当它们一起使用时，MCC/MNC 唯一标识移动网络运营商或载波。

- **策略设置**

  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。

- **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。iOS 不可用。

WPA、WPA 个人、任意 (个人) iOS 设置

密码： 键入可选密码。如果将此字段留空，用户登录时可能会被要求输入密码。

WEP 企业、WPA 企业、WPA2 企业、WPA3 企业、任意 (企业) iOS 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。

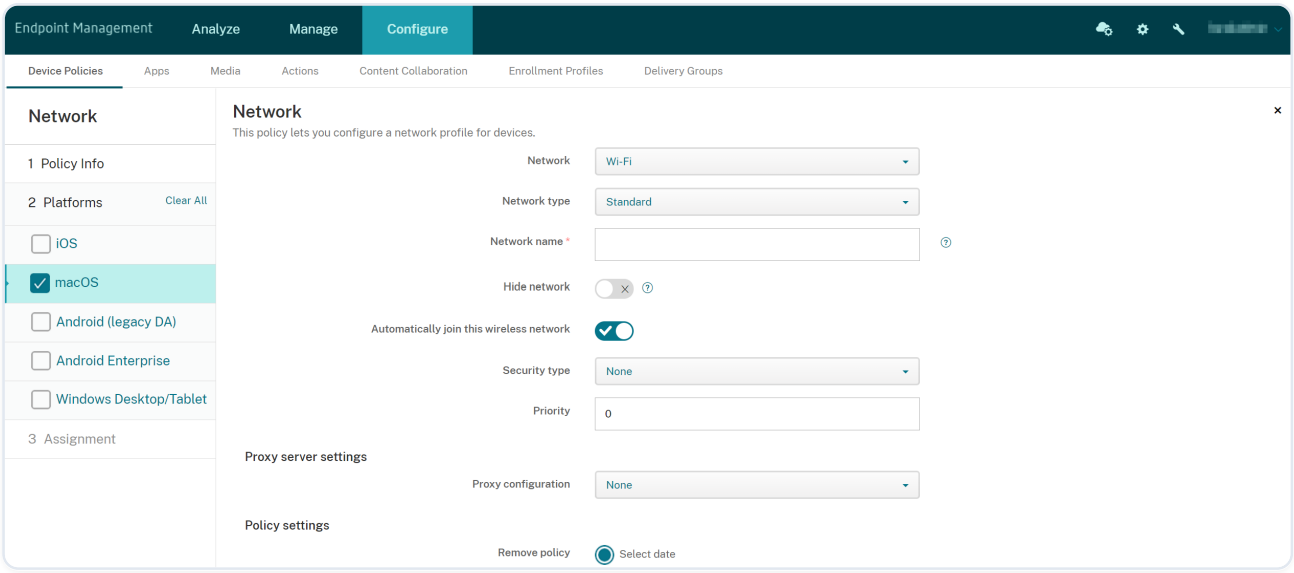
> **重要提示：**
>
> 如果选择 **WPA2 Enterprise** 安全类型，则必须至少允许一个 EAP 协议。

- **允许的 EAP 协议：** 启用要支持的 EAP 类型，然后配置相关设置。默认情况下，每个可用 EAP 类型都处于**关闭**状态。
- **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**。
- **EAP-FAST with PAC：** 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**，请选择是否允许最终用户客户端与 Citrix Endpoint Management 之间进行匿名 TLS 握手。
      - **匿名预配 PAC**
- **身份验证：**
  - **用户名：** 键入用户名。
  - **每次连接密码：** 选择是否要求用户每次登录时都输入密码。
  - **密码：** 键入可选密码。如果将此字段留空，用户登录时可能会被要求输入密码。
  - **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**。
  - **外部身份：** *仅当您启用* **PEAP**、**TTLS**，*或* **EAP-FAST** 时才需要。键入外部可见的用户名。您可以通过键入“匿名”等通用术语来提高安全性，这样用户名就不会可见。
  - **需要 TLS 证书：** 选择是否需要 TLS 证书。
- **信任**

- **受信任的证书：** 要添加受信任的证书，请单击“**添加**”，然后对要添加的每个证书执行以下操作：
  - **应用程序：** 在列表中，选择要添加的应用程序。
  - 单击“**保存**”以保存证书，或单击“**取消**”。
- **受信任的服务器证书名称：** 要添加受信任的服务器证书通用名称，请单击“**添加**”，然后对要添加的每个名称执行以下操作：
  - **证书：** 键入服务器证书的名称。您可以使用通配符指定名称，例如 wpa.*.example.com。
  - 单击“**保存**”以保存证书名称，或单击“**取消**”。

- **允许信任例外：** 选择当证书不受信任时，证书信任对话框是否显示在用户设备上。默认值为 **开**

macOS 设置



- **网络：** 在列表中，选择您计划使用的网络选项。默认值为 **Wi-Fi**。
  - 无线局域网
  - 全局以太网
  - 第一个活动以太网
  - 第二个活动以太网
  - 第三个活动以太网
  - 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**、**旧版热点**或**热点 2.0**以设置您计划使用的网络类型。
- **网络名称：** 键入设备可用网络列表中显示的 SSID。不适用于**热点 2.0**。
- **隐藏网络：** 选择网络是否隐藏。
- **自动加入此无线网络：** 选择是否自动加入网络。如果设备已连接到其他网络，则不会加入此网络。用户必须先断开与上一个网络的连接，设备才能自动连接。默认设置为**开**。
- **安全类型：** 在列表中，选择您计划使用的安全类型。不适用于**热点 2.0**。

  - 无 - 无需进一步配置。
  - WEP
  - WPA/WPA2 个人
  - 任意（个人）
  - WEP 企业版
  - WPA/WPA2 企业版
  - 任意（企业版）

  以下各节列出了为上述每种连接类型配置的选项。
- **优先级：** 对于多个网络，键入一个数字以定义网络连接的优先级。设备将首先连接到优先级数字最低的网络。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 连接如何通过代理服务器路由，然后配置任何其他选项。默认值为**无**，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：** 键入可选的用户名以向代理服务器进行身份验证。
    - **密码：** 键入可选密码以向代理服务器进行身份验证。

  - 如果选择**自动**，请配置以下设置：

    - **服务器 URL：** 键入定义代理配置的 PAC 文件的 URL。
    - **如果 PAC 不可达，则允许直接连接：** 选择当 PAC 文件不可达时是否允许用户直接连接到目标。默认值为**开**。

- **热点 2.0 设置**
  - **显示的运营商名称：** 热点设备广播的友好名称。用户在其可用 Wi-Fi 网络列表中看到此名称。
  - **域名：** 用于热点 2.0 协商的域名。
  - **允许连接到漫游伙伴网络：** 如果为“**开**”，则脱离其家庭网络漫游的设备可以连接到伙伴网络。
  - **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 属于具有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：** 配置用于向漫游网络识别用户的领域名称列表。NAI 以 `user@realm` 形式传输。
  - **移动国家/地区代码 (MCC) 和移动网络配置 (MNC)：** 移动国家/地区代码由三位数字组成，用于标识网络的国家/地区。移动网络代码由 2 或 3 位唯一数字组成。当它们一起使用时，MCC/MNC 唯一标识移动网络运营商或运营商。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**距离删除的持续时间（小时）**”
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **距离删除的持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 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 macOS 10.7 及更高版本。

macOS 的 WPA、WPA 个人版、WPA 2 个人版、任意（个人版）设置

- **密码：** 键入可选密码。如果将此字段留空，用户登录时可能会提示他们输入密码。

WEP 企业版、WPA 企业版、WPA2 企业版、任意 (企业版) 的 macOS 设置

- **连接模式：** 如果为**开**，请选择用户加入网络时要使用的连接模式。默认值为**关**。
  - **系统：** 如果选中，设备将使用系统凭据对用户进行身份验证。默认情况下未选中。
  - **登录窗口：** 如果选中，设备将使用在登录窗口输入的相同凭据对用户进行身份验证。默认情况下未选中。

当您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。

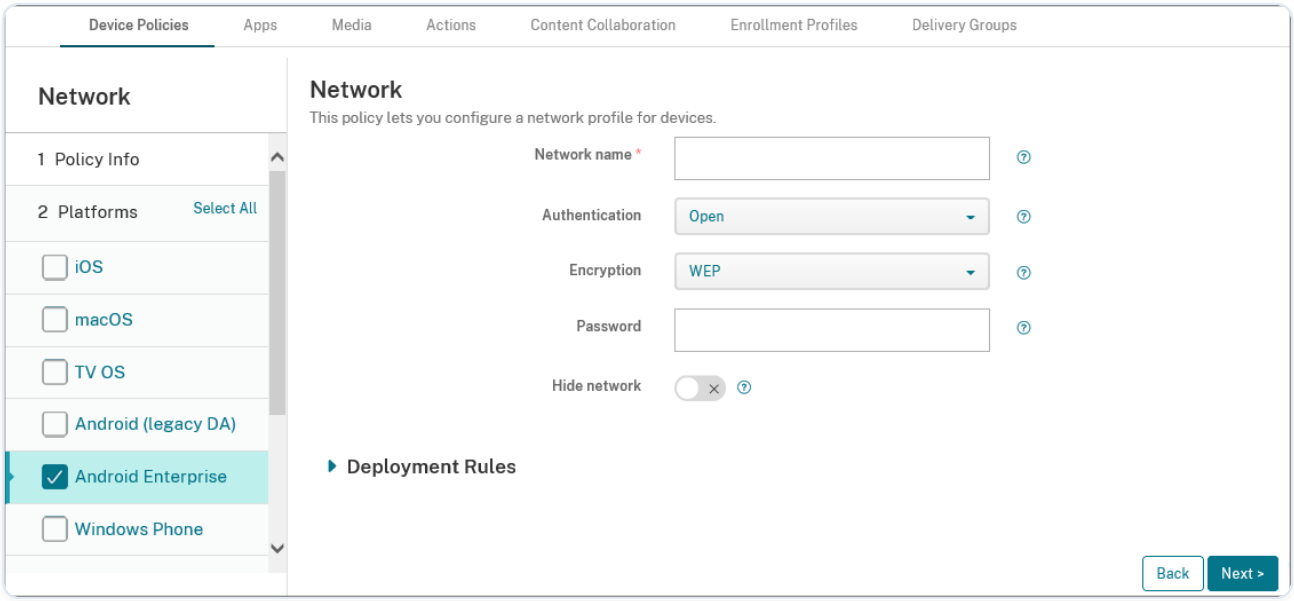
> **重要提示：**
>
> 如果您选择 **WPA2 企业版**安全类型，则必须至少允许一个 EAP 协议。

- **允许的 EAP 协议：** 启用您要支持的 EAP 类型，然后配置相关设置。对于每个可用的 EAP 类型，默认值为**关**。
- **内部身份验证 (TTLS)：** *仅当您启用 TTLS 时才需要*。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**。
- **带 PAC 的 EAP-FAST：** 选择是否使用受保护的访问凭据 (PAC)。
  - 如果您选择**使用 PAC**，请选择是否使用预配 PAC。
    - 如果您选择**预配 PAC**，请选择是否允许最终用户客户端与 Citrix Endpoint Management 之间进行匿名 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**。仅当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。
  - **每次连接密码：** 选择是否要求用户每次登录时输入密码。
  - **密码：** 键入可选密码。如果将此字段留空，用户登录时可能会被要求输入密码。
  - **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**。
  - **外部身份：** *仅当您启用* **PEAP**、**TTLS** *或* **EAP-FAST** 时才需要。键入外部可见的用户名。您可以通过键入“匿名”之类的通用术语来提高安全性，从而使用户名不可见。
  - **需要 TLS 证书：** 选择是否需要 TLS 证书。
- **信任**

- **受信任的证书：** 要添加受信任的证书，请单击 **添加**，然后对要添加的每个证书执行以下操作：
  - **应用程序：** 在列表中，选择要添加的应用程序。
  - 单击 **保存** 以保存证书，或单击 **取消**。
- **受信任的服务器证书名称：** 要添加受信任的服务器证书通用名称，请单击 **添加**，然后对要添加的每个名称执行以下操作：
  - **证书：** 键入要添加的服务器证书的名称。您可以使用通配符指定名称，例如 wpa.*.example.com。
  - 单击 **保存** 以保存证书名称，或单击 **取消**。

- **允许信任例外：** 选择当证书不受信任时，是否在用户设备上显示证书信任对话框。默认值为 **开**。

安卓企业版设置



- **网络名称：** 输入用户设备上可用网络列表中的 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
  - WPA
  - WPA-PSK
  - WPA2

- WPA2-PSK
- 802.1x EAP

以下各节列出了为上述每种连接类型配置的选项。默认值为**开放**。

开放式，Android Enterprise 的共享设置

- **加密：** 在列表中，选择**已禁用**或 **WEP**。默认值为 **WEP**。
- **密码：** 输入可选密码。
- **隐藏网络：** 选择网络是否隐藏。

适用于 Android Enterprise 的 WPA、WPA-PSK、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：** 选择网络是否隐藏。

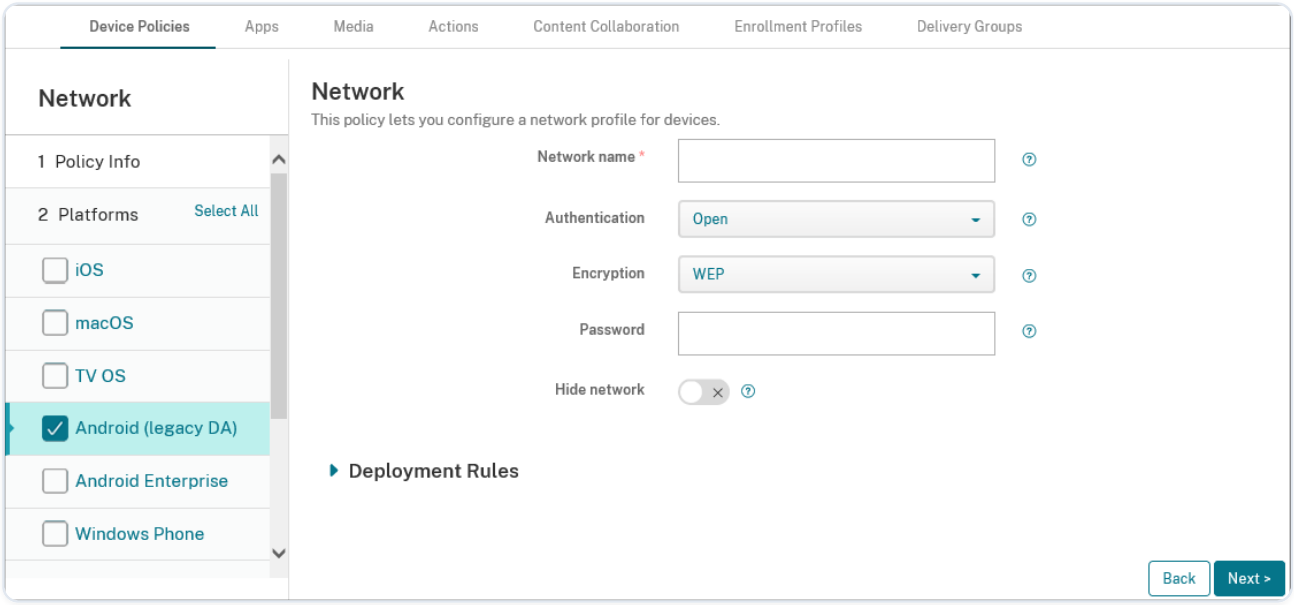
适用于 Android Enterprise 的 802.1x 设置

- **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：** 键入可选的用户名和域。
- **匿名：** 键入可选的、外部可见的用户名。您可以通过键入“anonymous”之类的通用术语来提高安全性，这样用户名就不会显示。
- **CA 证书：** 在列表中，选择要使用的证书。
- **域：** 键入所需的域名。有关详细信息，请参阅 域。

> **注意：**
>
> 在运行 Android 13 或更高版本的设备上配置 Wi-Fi 策略时，必须强制更新 **CA 证书**和 **域**字段。如果未更新，则配置将失败。

- **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：** 选择网络是否隐藏。

Android（旧版设备管理员）设置



- **网络名称：** 键入用户设备上可用网络列表中的 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（仅限 Android Enterprise）
  - WPA（仅限 安卓企业版）
  - WPA-PSK（仅限 安卓企业版）
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下各节列出了为上述每种连接类型配置的选项。

Android 的开放、共享设置

- **加密：** 在列表中，选择**禁用**或 **WEP**。默认值为 **WEP**。
- **密码：** 键入可选密码。
- **隐藏网络**：选择网络是否隐藏。

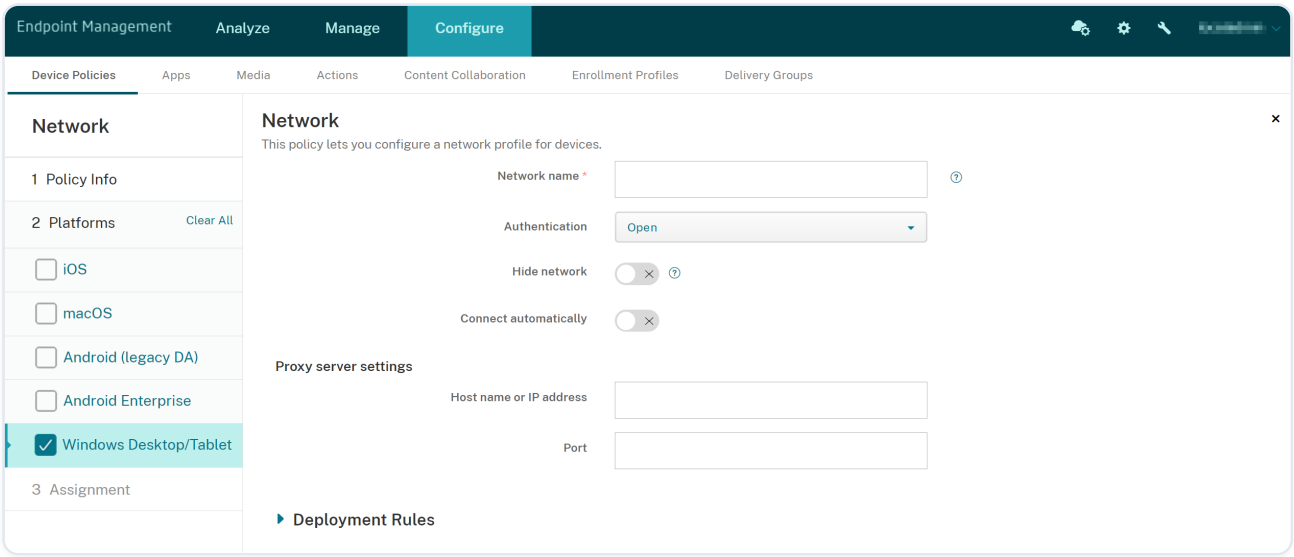
适用于 Android 的 WPA、WPA-PSK、WPA2、WPA2-PSK 设置

- **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**：选择网络是否隐藏。

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**：键入可选的用户名和域。
- **匿名**：键入可选的、外部可见的用户名。您可以通过键入“anonymous”之类的通用术语来提高安全性，这样用户名就不会显示。
- **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**：选择网络是否隐藏。

Windows 桌面/平板电脑设置



- **网络名称：** 在可用网络列表中看到的 SSID。
- **身份验证：** 单击下拉列表中要用于 Wi-Fi 连接的安全类型。
  - 开放
  - WPA 个人
  - WPA-2 个人
  - WPA 企业
  - WPA-2 企业：对于最新版本的 Windows 10，请配置 SCEP 以使用 WPA-2 企业版。SCEP 配置使 Citrix Endpoint Management 能够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。有关详细信息，请参阅凭据提供程序。

以下各节列出了为上述每种连接类型配置的选项。

适用于 Windows 10 和 Windows 11 的开放设置

- **隐藏网络：** 选择网络是否隐藏。
- **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 个人、WPA-2 个人设置

- **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：** 提供所选方法的加密密钥。
- **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。

WPA-2 企业版设置适用于 Windows 10 和 Windows 11

- **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 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

您可以设置网络使用规则，以指定 iOS 设备如何使用网络，例如蜂窝数据网络。这些规则适用于托管应用程序和指定的 SIM 卡。托管应用程序是指您通过 Citrix Endpoint Management 部署到用户设备的应用程序。它们不包括用户直接下载到其设备但未通过 Citrix Endpoint Management 部署的应用程序。它们也不包括设备在注册 Citrix Endpoint Management 时已安装在设备上的应用程序。此策略适用于 iOS 13 设备的 SIM 卡。您可以配置应用程序规则、SIM 卡规则或两者。SIM 卡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

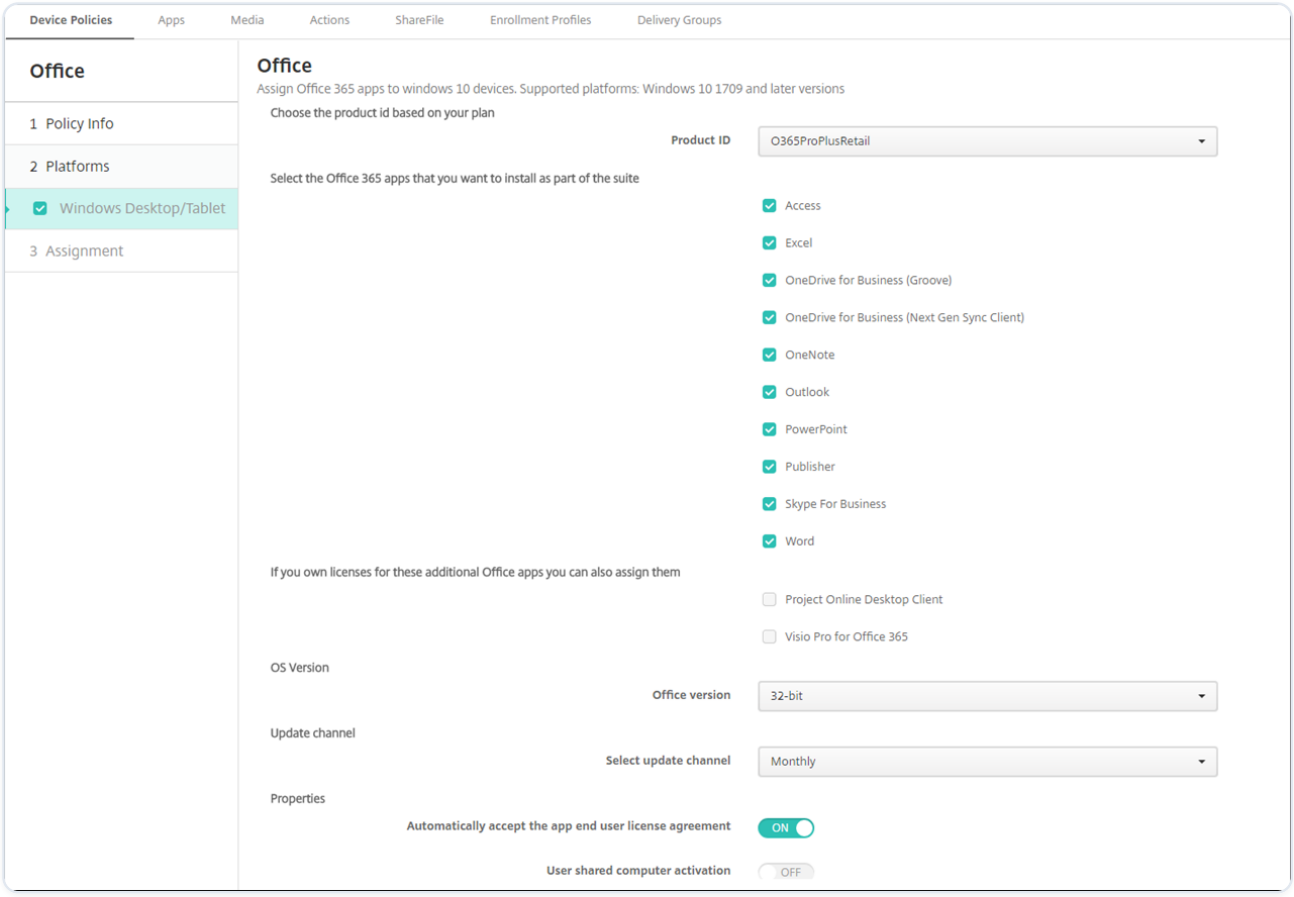
- **应用程序规则**
  - **允许漫游蜂窝数据：** 选择指定的应用程序在漫游时是否可以使用蜂窝数据连接。默认值为 **关**。
  - **允许蜂窝数据：** 选择指定的应用程序是否可以使用蜂窝数据连接。默认值为 **关**。
  - **应用程序标识符匹配：** 对于要添加到列表中的每个应用程序，单击 **添加**，然后配置以下内容：
    - **应用程序标识符：** 键入应用程序标识符。
  - 单击 **保存** 将应用程序保存到列表，或单击 **取消** 不将应用程序保存到列表。
- **SIM 卡规则**
  - **SIM 卡 Wi-Fi 辅助策略：** 启用 **从信号不佳的 Wi-Fi 切换** 会使 Wi-Fi 辅助策略更积极地从信号不佳的 Wi-Fi 切换到蜂窝连接。此设置可能会增加蜂窝数据使用量并影响电池续航时间。
  - **SIM 卡 ICCID：** 对于要添加到列表中的每个 SIM 卡，单击 **添加**，然后配置以下内容：
    - **ICCID：** 键入要添加的 SIM 卡的 19 位或 20 位数字。

Office 设备策略

Citrix Endpoint Management 允许您使用 Office 配置服务提供商 (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 桌面/平板电脑设置



- **产品 ID：** 根据您的 Office 365 计划选择产品 ID。选项包括 **O365ProPlusRetail**、**O365BusinessRetail** 或 **O365SmallBusPremRetail**。
- **Office 365 应用程序：** 选择要部署的 Office 365 应用程序。默认情况下，所有应用程序均已选中。
- **其他 Office 应用程序：** 如果您拥有 **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进行安装。
- **Office 版本：** 选择安装 Office 的 **32 位**或 **64 位**版本。
- **更新通道：** 选择更新发生的频率。选项包括**每月**、**每月（定向）**、**半年**或**半年（定向）**。
- **属性：**
  - **自动接受应用程序最终用户许可协议：** 选择**开**或**关**。默认为**开**。
  - **用户共享计算机激活：** 选择计算机是否共享。选项包括**开**或**关**。默认为**关**。
- **Office 语言：** Office 会自动安装 Windows 已安装的任何语言。您可以选择要安装的其他语言。

组织信息设备策略

组织信息设备策略指定了从 Citrix 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 Citrix Endpoint Management 的组织的名称。
- **地址：** 键入组织的地址。
- **电话：** 键入组织的支援电话号码。
- **电子邮件：** 键入支援电子邮件地址。
- **魔术：** 键入描述组织所管理服务的词语或短语。

操作系统更新设备策略

操作系统更新设备策略允许您部署：

- 受监管 iOS 设备的最新操作系统更新。

  操作系统更新设备策略仅适用于已注册 Apple 部署计划的受监管设备。

- 运行 macOS 10.11.5 及更高版本的已注册 Apple 部署计划的 macOS 设备的最新操作系统和应用程序更新。

> **注意：**
>
> Apple 目前仅将操作系统更新限制为主要版本。管理员不允许更新次要版本。有关详细信息，请参阅 Apple 文档中的这篇文章。

- 运行 Windows 10 或 Windows 11 的受监管桌面和平板电脑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 的桌面和平板电脑的传递优化设置。传递优化是 Microsoft 为 Windows 10 和 Windows 11 更新提供的点对点客户端更新服务。传递优化的目标是减少更新过程中的带宽问题。通过在多个设备之间共享下载任务来实现带宽减少。有关详细信息，请参阅 Microsoft 文章配置 Windows 10 更新的传递优化。

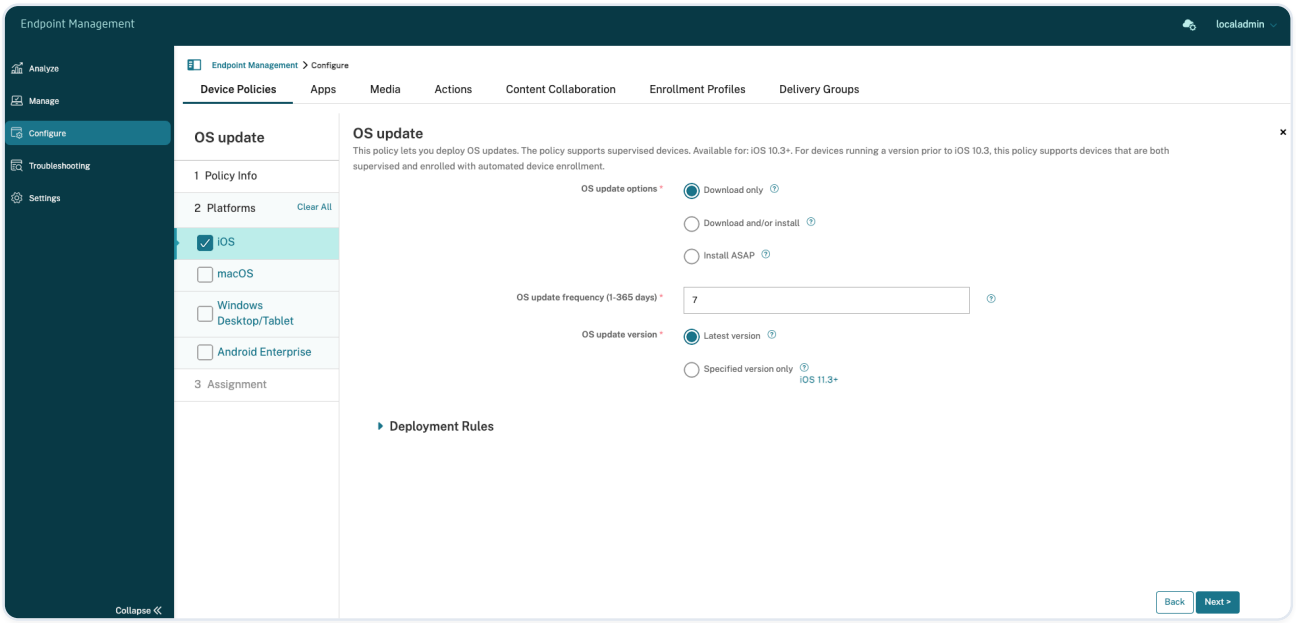
- 受管 Android Enterprise 设备（Android 7.0 及更高版本）的最新操作系统更新。

> **重要提示：**

> 操作系统更新策略不允许您完全禁用更新。要将更新延迟最多 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，请转到 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

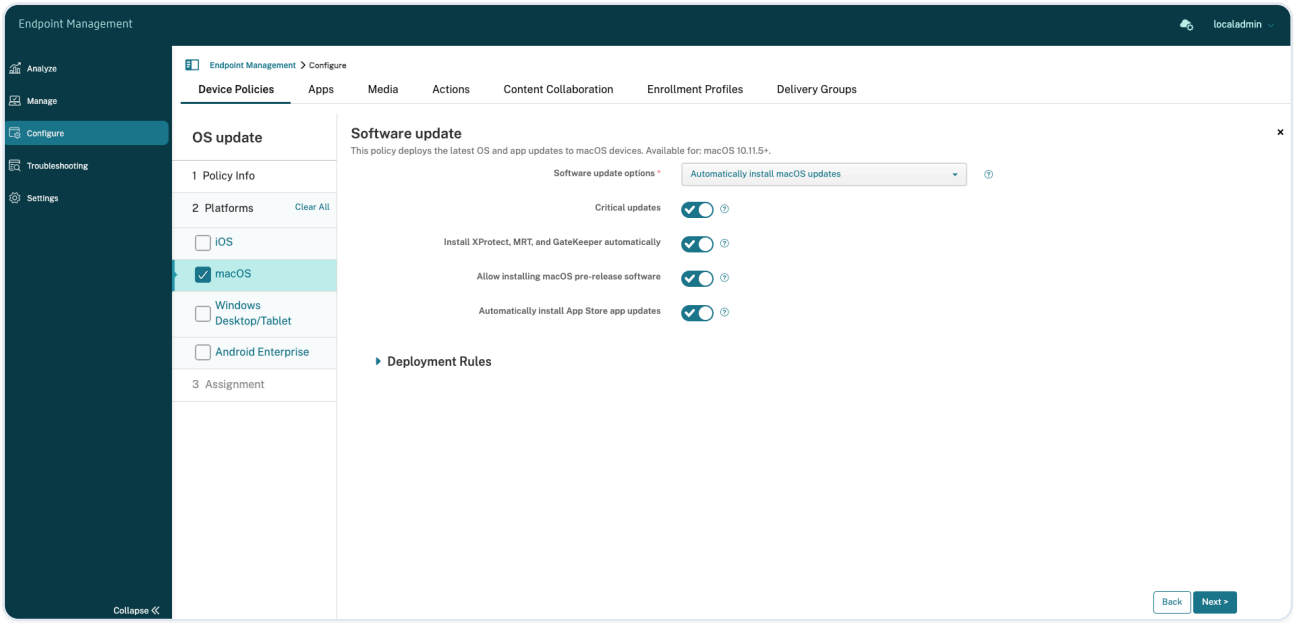
iOS 设置



以下设置适用于受监管的 iOS 设备。

- **操作系统更新选项：** 这两个选项都会根据**操作系统更新频率**将最新的操作系统更新下载到受监管的设备。设备会提示用户安装更新。提示在用户解锁设备后可见。
- **操作系统更新频率：** 确定 Citrix 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：** 指定用于更新受监管 iOS 设备的版本。默认值为**最新版本**。
  - **最新版本：** 选择更新到最新操作系统版本。
  - **仅限特定版本：** 选择更新到特定操作系统版本，然后键入版本号。

macOS 设置



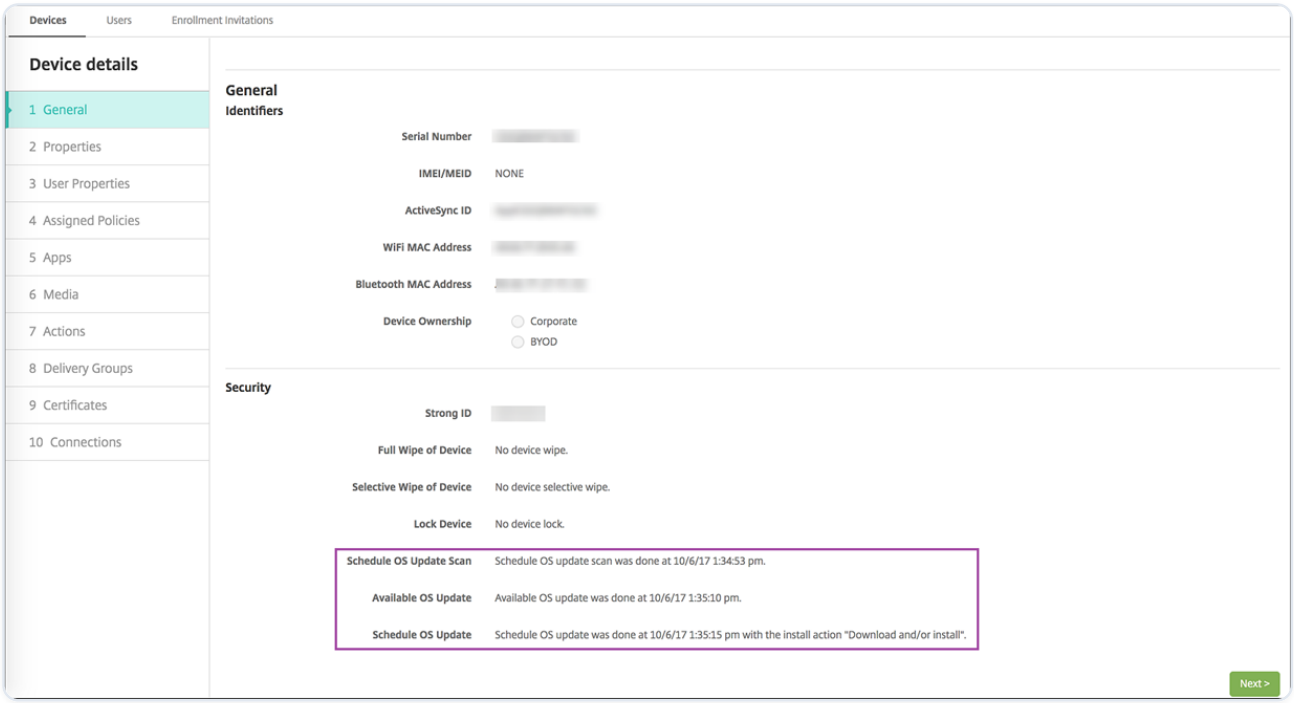
- **软件更新选项：** 控制 macOS 设备检查和安装更新的方式。从以下选项中选择：
  - **自动安装 macOS 更新：** 更新将自动下载和安装。
  - **有可用更新时下载新更新：** 更新已下载，但需要手动安装。
  - **检查更新：** 检查是否存在更新，但不会自动下载或安装更新。
  - **不检查更新：** 不检查新更新、不下载更新或不自动安装更新。用户仍可手动安装更新。
- **关键更新：** 允许自动安装关键 macOS 更新。
- **自动安装 xProtect、MRT 和 GateKeeper 更新：** 允许 macOS 设备自动安装安全软件更新。
- **允许安装 macOS 预发布软件：** 允许用户安装 macOS 软件的预发布版本。
- **自动安装 App Store 应用更新：** 允许 App Store 应用自动更新。

获取 iOS 和 macOS 更新操作的状态

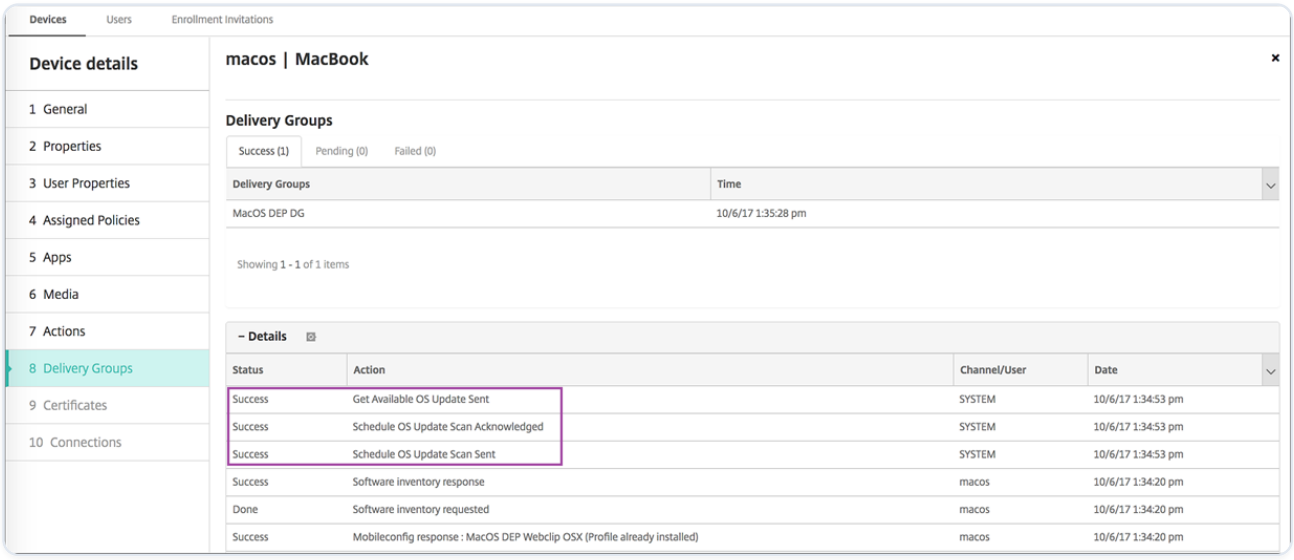
对于 iOS 和 macOS，Citrix Endpoint Management 不会将“控制操作系统更新”策略部署到设备。相反，Citrix Endpoint Management 使用该策略向设备发送以下 MDM 命令：

- 安排操作系统更新扫描：请求设备执行操作系统更新的后台扫描。（iOS 可选）
- 可用操作系统更新：查询设备以获取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，设备操作系统决定何时下载或安装操作系统和应用程序更新。

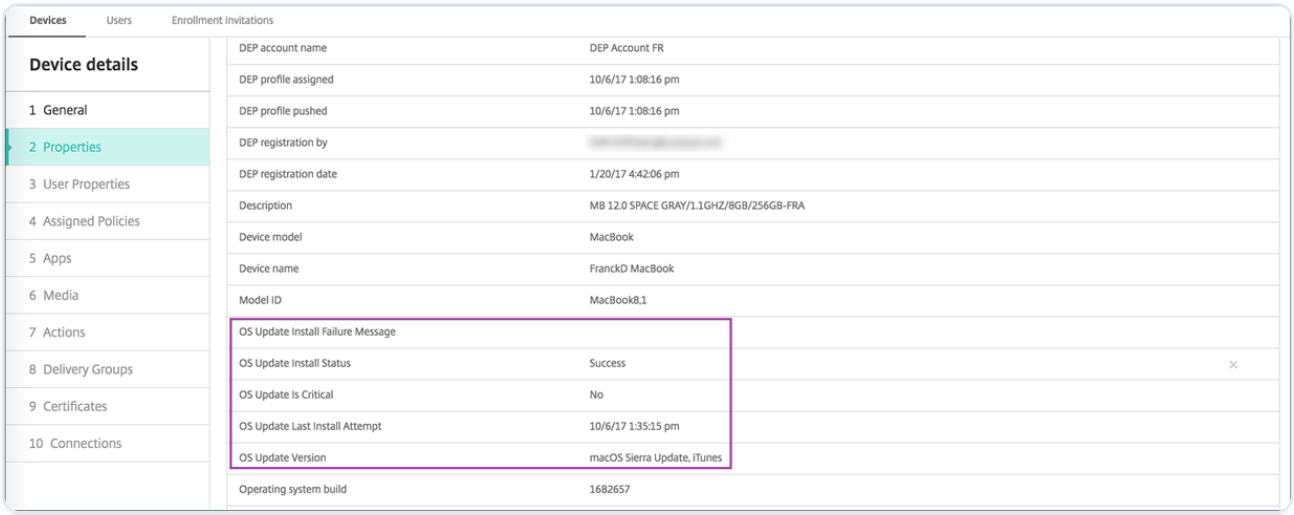
“**管理 > 设备 > 设备详细信息（常规）**”页面显示计划和可用操作系统更新扫描以及计划的 macOS 和应用程序更新的状态。

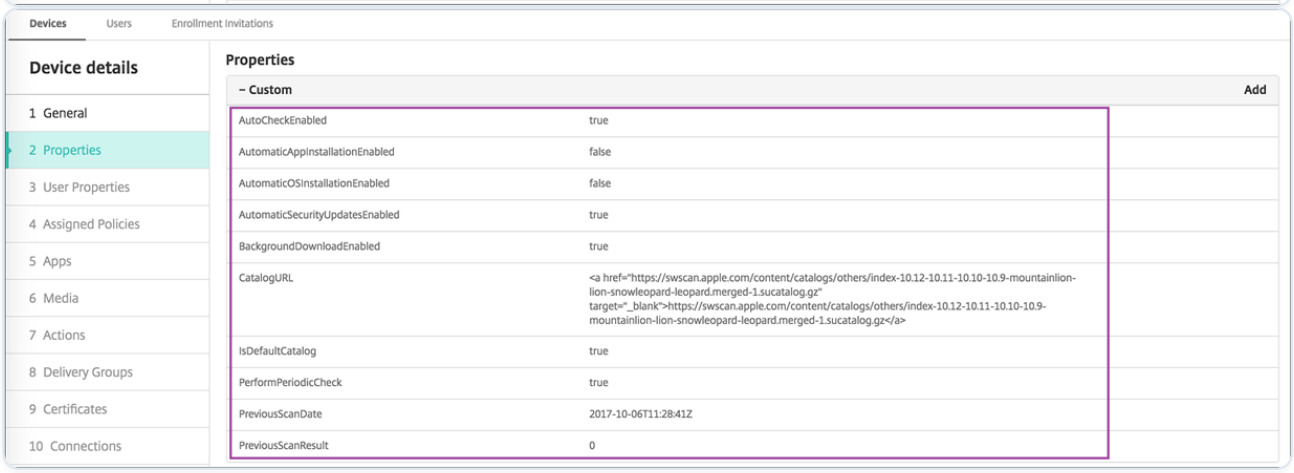


有关更新操作状态的更多详细信息，请转到“**管理 > 设备 > 设备详细信息（交付组）**”页面。

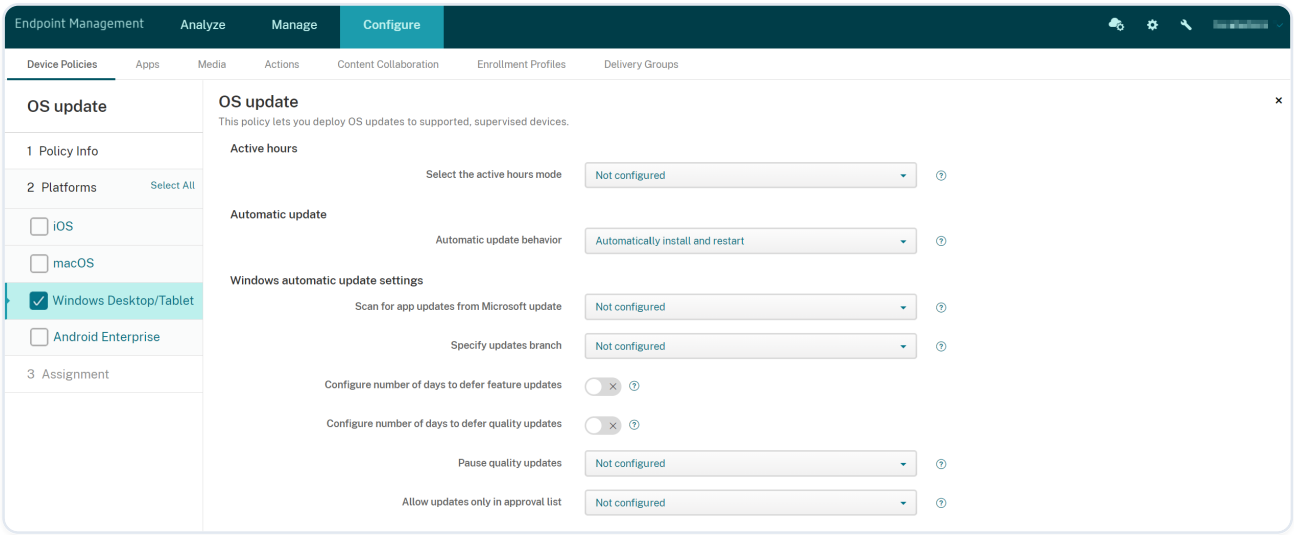


有关可用操作系统更新和上次安装尝试等详细信息，请转到“**管理 > 设备 > 设备详细信息（属性）**”页面。





Windows 桌面和平板电脑设置



- **选择活动时间模式：** 选择一种模式来配置执行操作系统更新的活动时间。您可以指定一个小时范围或一个开始和结束时间。选择模式后，将出现更多设置：**指定活动时间的最大范围**或**活动时间开始**和**活动时间结束**。**未配置**允许 Windows 随时执行操作系统更新。默认为**未配置**。
- **自动更新行为：** 配置用户设备上 Windows 更新服务的下载、安装和重启行为。默认为“**自动安装和重启**”。

- **下载更新前通知用户：** Windows 在有可用更新时通知用户。Windows 不会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启：** Windows 会在非按流量计费的网络上自动下载更新。Windows 会在设备未使用且未通过电池供电时，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 会立即安装更新。如果安装需要重启，Windows 会提示用户安排重启时间。用户有最多七天的时间来安排重启。七天后，Windows 会强制设备重启。允许用户控制启动时间可降低因应用程序在重启时未正确关闭而导致意外数据丢失的风险。
- **自动安装和重启：** 默认设置。Windows 会在非按流量计费的网络上自动下载更新。Windows 会在设备未使用且未通过电池供电时，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 会立即安装更新。如果安装需要重启，Windows 会在设备处于非活动状态时自动重启设备。
- **在指定时间自动安装和重启：** 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。默认设置为每天凌晨 3 点。自动安装在指定时间进行，设备在 15 分钟倒计时后重启。当 Windows 准备重启时，已登录的用户可以中断 15 分钟倒计时以延迟重启。
- **自动安装和重启，无需最终用户控制：** Windows 会在非按流量计费的网络上自动下载更新。Windows 会在设备未使用且未通过电池供电时，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 会立即安装更新。如果安装需要重启，Windows 会在设备处于非活动状态时自动重启设备。此选项还会将用户控制面板设置为只读。
- **关闭自动更新：** 禁用设备上的 Windows 自动更新。

- **从 Microsoft 更新扫描应用更新：** 指定 Windows 是否接受来自 Microsoft 更新服务的其他 Microsoft 应用的更新。默认为“**未配置**”。
  - **未配置：** 如果您不想配置此行为，请使用此设置。Windows 不会更改用户设备上的相关 UI。用户可以接受或拒绝其他 Microsoft 应用的更新。
  - **是：** Windows 允许从 Windows 更新服务安装应用更新。用户设备上的相关设置处于非活动状态，因此用户无法修改该设置。
  - **否：** Windows 不允许从 Windows 更新服务安装应用更新。用户设备上的相关设置处于非活动状态，因此用户无法修改该设置。
- **指定更新分支：** 指定用于更新的 Windows 更新服务分支。默认为“**未配置**”。
  - **未配置：** 如果您不想配置此行为，请使用此设置。Windows 不会更改用户设备上的相关 UI。用户可以选择 Windows 更新服务分支。

  - **当前分支：** Windows 从当前分支接收更新。用户设备上的相关设置处于非活动状态，因此用户无法修改该设置。
  - **业务当前分支：** Windows 从业务当前分支接收更新。用户设备上的相关设置处于非活动状态，因此用户无法修改该设置。

- **配置推迟功能更新的天数：** 如果为“**开**”，Windows 会将功能更新推迟指定天数，用户无法更改此设置。如果为“**关**”，用户可以更改推迟功能更新的天数。默认为“**关**”。
- **配置推迟质量更新的天数：** 如果为“**开**”，Windows 会将质量更新推迟指定天数，用户无法更改此设置。如果为“**关**”，用户可以更改推迟质量更新的天数。默认为“**关**”。
- **暂停质量更新：** 指定是否暂停质量更新 35 天。默认为“**未配置**”。
  - **未配置：** 如果您不想配置此行为，请使用此设置。Windows 不会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 会暂停从 Windows 更新服务安装质量更新 35 天。用户设备上的相关设置处于非活动状态，因此用户无法修改该设置。
  - **否：** Windows 不会暂停从 Windows 更新服务安装质量更新。用户设备上的相关设置处于非活动状态，因此用户无法修改该设置。
- **仅允许批准列表中的更新：** 指定是否仅安装 MDM 服务器批准的更新。Citrix Endpoint Management 不支持配置批准的更新列表。默认为“**未配置**”。
  - **未配置：** 如果您不想配置此行为，请使用此设置。Windows 不会更改用户设备上的相关 UI。用户可以选择允许哪些更新。
  - **是，仅安装批准的更新：** 仅允许安装批准的更新。
  - **否，安装所有适用的更新：** 允许在设备上安装任何适用的更新。
- **使用内部更新服务器：** 指定是通过 Windows 更新服务还是通过 Windows Server Update Services (WSUS) 从内部更新服务器获取更新。如果为“**关**”，设备将使用 Windows 更新服务。如果为“**开**”，设备将连接到指定的 WSUS 服务器以获取更新。默认为“**关**”。
  - **接受非 Microsoft 实体签名的更新：** 指定是否接受由 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。默认为“**开**”。
  - **WSUS 服务器：** 指定 WSUS 服务器的服务器 URL。
  - **备用内部网服务器以托管更新：** 指定备用内部网服务器 URL 以托管更新并接收报告信息。
- **配置传递优化：** 是否对 Windows 10 和 Windows 11 更新使用传递优化。默认值为 **关闭**。

- **缓存大小：** 传递优化缓存的最大大小。值为 **0** 表示缓存无限制。默认值为 **10** GB。
- **允许 VPN 对等缓存：** 设备通过 VPN 连接到域网络时，是否允许其参与对等缓存。当设置为 **开** 时，设备可以从其他域网络设备（无论是在 VPN 上还是在公司域网络上）下载或上传。默认值为 **关闭**。
- **下载方法：** 传递优化可用于下载 Windows 更新、应用程序和应用程序更新的下载方法。默认值为 **HTTP 与同一 NAT 后面的对等互连混合**。选项包括：
  - **仅 HTTP，无对等互连：** 禁用点对点缓存，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 与同一 NAT 后面的对等互连混合：** 在同一网络上启用对等共享。传递优化云服务会查找使用与目标客户端相同的公共 IP 连接到 Internet 的其他客户端。然后，这些客户端会尝试使用其专用子网 IP 连接到同一网络上的其他对等设备。
  - **HTTP 与跨专用组的对等互连混合：** 根据设备 Active Directory 域服务 (AD DS) 站点或设备进行身份验证的域自动选择组。对等互连发生在内部子网之间，在属于同一组的设备之间，包括远程办公室中的设备。
  - **HTTP 与 Internet 对等互连混合：** 为传递优化启用 Internet 对等源。
  - **无对等互连的简单下载模式：** 禁用传递优化云服务的使用。在以下情况下，传递优化会自动切换到此模式：当传递优化云服务不可用、无法访问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，且不进行点对点缓存。
  - **不使用传递优化，而是使用 BITS：** 使客户端能够使用 BranchCache。有关详细信息，请参阅 Microsoft 文章 BranchCache。
- **最大下载带宽：** 最大下载带宽，单位为 KB/秒。默认值为 **0**，表示动态带宽调整。
- **最大下载带宽百分比：** 传递优化在所有并发下载活动中可以使用的最大下载带宽。该值是可用下载带宽的百分比。默认值为 **0**，表示动态调整。
- **最大上传带宽：** 最大上传带宽，单位为 KB/秒。默认值为 **0**。值为 **0** 表示带宽无限制。
- **每月上传数据上限：** 传递优化在每个日历月可以上传到 Internet 对等设备的 GB 最大大小。默认值为 20 GB。值为 **0** 表示每月上传无限制。

Citrix Endpoint Management 如何处理 Windows 桌面和平板电脑设备的批准更新

您可以指定是否仅安装已批准的更新。Citrix Endpoint Management 按如下方式处理更新：

- 对于安全更新（例如 Windows Defender 定义），Citrix Endpoint Management 会自动批准更新并在下次同步期间向设备发送安装命令。
- 对于所有其他更新类型，Citrix Endpoint Management 会等待您的批准，然后才向设备发送安装命令。

先决条件

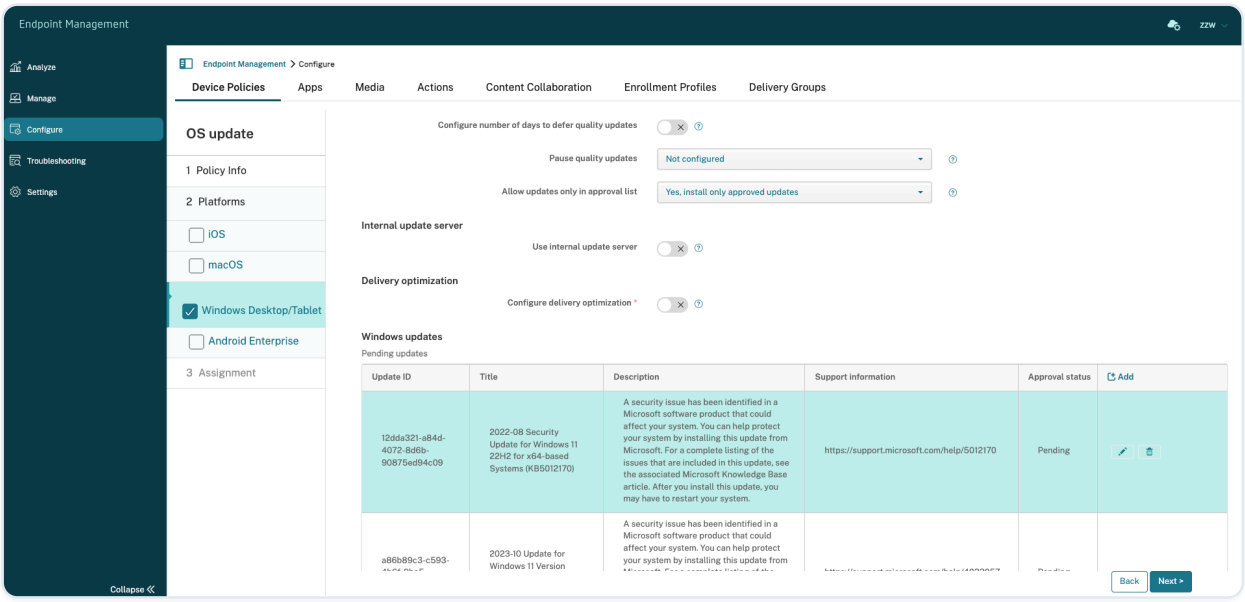
- 您必须将 Microsoft 根证书作为服务器证书上传到 Citrix Endpoint Management 服务器。
- 有关导入服务器证书的信息，请参阅 证书和身份验证 中的“导入证书”。

仅安装已批准的更新

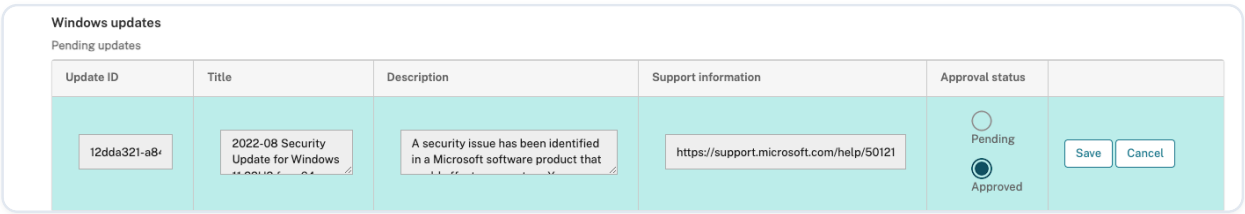
1. 转至 **Configure > Device Policies**（配置 > 设备策略），然后打开 OS Update 设备策略。
2. 将 **Allow updates only in approval list**（仅允许批准列表中的更新）设置更改为 **Yes, install only approved updates**（是，仅安装已批准的更新）。

批准更新

1. 在 OS Update 设备策略中，向下滚动到 **Pending updates**（待处理更新）表。Citrix Endpoint Management 从设备获取表中列出的更新。
2. 搜索 **Approval status**（批准状态）为 **Pending**（待处理）的更新。
3. 单击要批准的更新所在行，然后单击该行（在 **Add**（添加）列中）的编辑图标。



4. 要批准更新，请单击 **Approved**（已批准），然后单击 **Save**（保存）。



注意：

> 尽管“待处理更新”表包含添加和删除命令，但这些命令不会对 Citrix Endpoint Management 数据库造成任何更改。编辑批准状态是待处理更新唯一可用的操作。

> 要查看设备的 Windows 更新状态，请转至 **管理 > 设备 > 属性**。



更新发布后，**更新 ID** 将显示在第一列中，并带有状态（成功或失败）。您可以为更新失败的设备创建报告或自动化操作。发布日期和时间也会显示。

首次部署和后续部署的更新工作方式

操作系统更新设备策略对设备的影响在首次部署和设备获取更新后的部署之间有所不同。

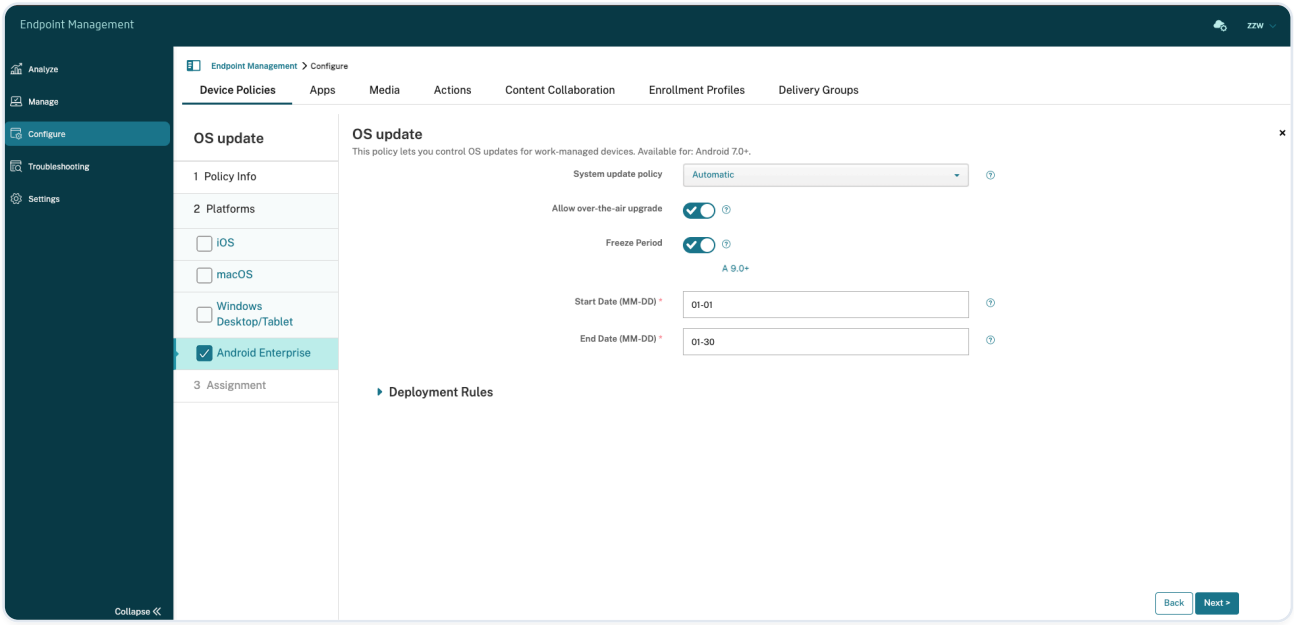
- 要使 Citrix Endpoint Management 查询设备的更新，您必须配置至少一个操作系统更新设备策略并将其分配给交付组。

  Citrix Endpoint Management 在设备 MDM 同步期间查询设备以获取可安装的更新。
- 首次部署操作系统更新设备策略后，Windows 更新列表为空，因为尚未有设备报告。
- 当分配的交付组中的设备报告更新时，Citrix Endpoint Management 会将其保存到数据库中。要批准任何报告的更新，请再次编辑策略。

  更新批准仅适用于您正在编辑的策略。在一个策略中批准的更新不会在另一个策略中显示为已批准。设备下次同步时，Citrix Endpoint Management 会向设备发送命令，指示更新已获批准。
- 对于第二个操作系统更新设备策略，更新列表包含存储在 Citrix Endpoint Management 数据库中的更新。请为每个策略批准更新。

  在每次设备同步期间，Citrix Endpoint Management 都会查询设备的已批准更新状态，直到设备报告更新已安装。对于安装后需要重新启动的更新，Citrix Endpoint Management 会查询更新状态，直到设备报告更新已安装。
- Citrix Endpoint Management 不会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会显示在列表中。

安卓企业设置



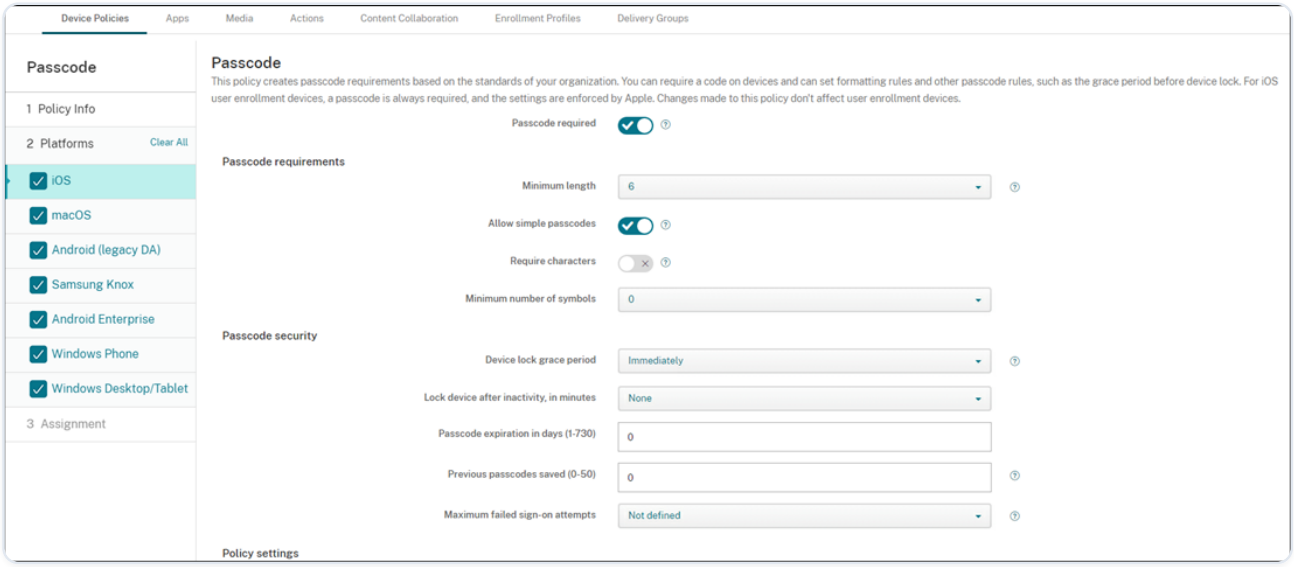
- **系统更新策略：** 确定系统更新何时发生。
  - **自动：** 在更新可用时安装更新。
  - **窗口化：** 在**开始时间**和**结束时间**中指定的每日维护窗口内自动安装更新。
    - **开始时间：** 维护窗口的开始时间，以设备本地时间从午夜开始的分钟数（**0 - 1440**）衡量。默认值为**0**。
    - **结束时间：** 维护窗口的结束时间，以设备本地时间从午夜开始的分钟数（**0 - 1440**）衡量。默认值为**120**。
  - **推迟：** 允许用户将更新推迟最多 30 天。
  - **默认：** 将更新策略设置为系统默认值。
- **允许无线升级：** 如果禁用，用户设备将无法无线接收软件更新。默认值为**开**。
- **冻结期：** 如果设置为**开**，则在为**自动**、**推迟**和**窗口化**更新策略指定的日期范围内，设备上不会安装操作系统更新。一次只能为一个设备设置一个冻结期。冻结期的长度不能超过 90 天。
  - **开始日期/结束日期：** 如果启用了**冻结期**，则在此日期范围内不安装操作系统更新。
- **冻结期：** 如果设置为**开**，则在为**自动**、**推迟**和**窗口化**更新策略指定的日期范围内，设备上不会安装操作系统更新。一次只能为一个设备设置一个冻结期。冻结期的长度不能超过 90 天。
  - **开始日期/结束日期：** 如果启用了**冻结期**，则在此日期范围内不安装操作系统更新。

密码设备策略

根据组织的标准在 Citrix Endpoint Management 中创建密码策略。您可以要求用户设备使用密码，并可以设置各种格式和密码规则。为 iOS、macOS、Android、Android Enterprise 和 Windows 桌面/平板电脑创建策略。每个平台都需要一组不同的值，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。

iOS 设置



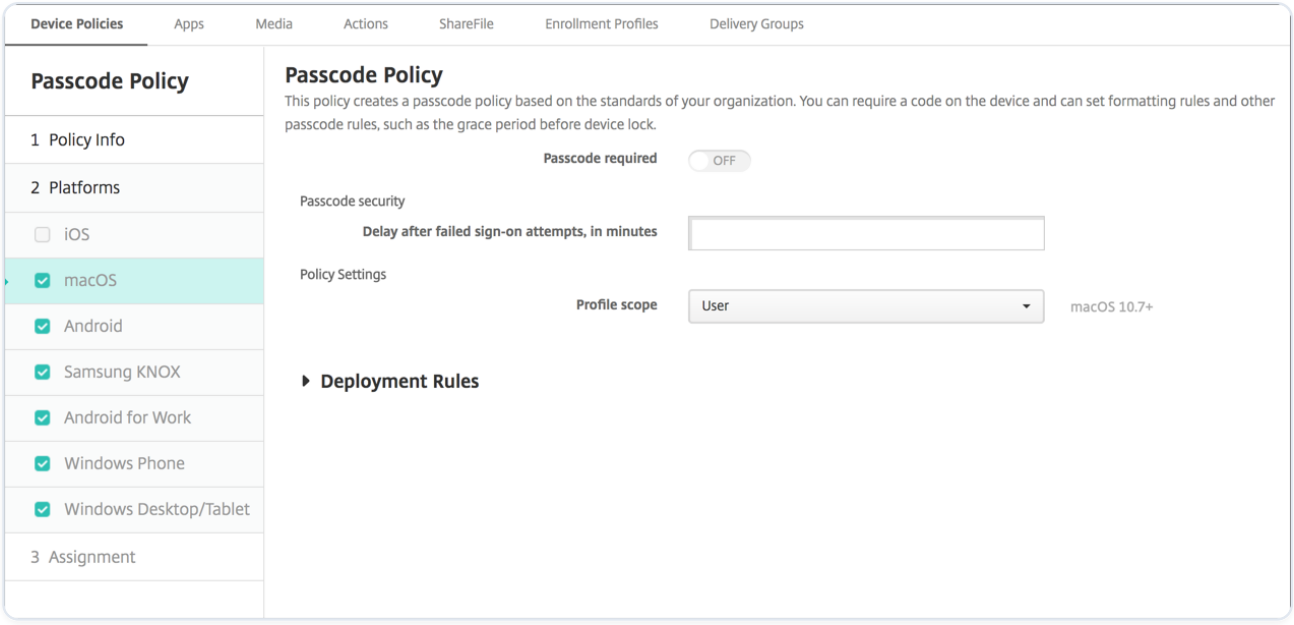
- **需要密码：** 选择此选项可要求使用密码并显示 iOS 密码设备策略的配置选项。页面将展开，允许您配置密码要求、密码安全和策略设置。
- **密码要求**
  - **最小长度：** 在下拉列表中单击最小密码长度。默认值为 **6**。
  - **允许简单密码：** 选择是否允许简单密码。简单密码是重复或顺序的字符集。默认值为 **开**。
  - **所需字符：** 选择是否要求密码至少包含一个字母。默认值为 **关**。
  - **最少符号数：** 在列表中，单击密码必须包含的符号数。默认值为 **0**。
- **密码安全**
  - **设备锁定宽限期：** 在列表中，单击用户必须输入密码才能解锁锁定的设备之前的时间长度。默认值为 **立即**。
  - **不活动后锁定设备：** 在框中，输入设备在锁定前可以处于非活动状态的时间长度。该值可以在 1 到 15 分钟之间。将值设置为 **无** 可禁用策略。默认值为 **无**。
  - **密码过期天数 (1-730)：** 键入密码过期后的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。

- **之前保存的密码 (0-50)：** 键入要保存的已用密码数。用户无法使用此列表中找到的任何密码。有效值为 0–50。默认值为 **0**，这意味着用户可以重复使用密码。
- **最大登录失败尝试次数：** 在列表中，单击用户可以失败登录的次数。
  - 如果将此数字设置为大于 6，则在第六次尝试后，设备会在尝试之间施加时间延迟。每次失败尝试都会增加时间延迟。在最后一次尝试后，所有数据和设置都将被安全擦除。
  - 如果将数字设置为 6 或更低，设备将在不实施时间延迟的情况下被擦除。
  - 如果选择**未定义**，则在 6 次尝试后，设备会在尝试之间施加递增的时间限制，但不会被擦除。

  默认值为**未定义**。

- **策略设置**
  - **删除策略：** 选择一种方法来安排策略删除。可用选项为**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

macOS 设置



- **需要密码：** 选择此选项以要求密码并显示 iOS 密码设备策略的配置选项。页面将展开，允许您配置密码要求、密码安全和策略设置。
- 如果**需要密码**被禁用，在**登录失败尝试后的延迟（分钟）**旁边，键入延迟的分钟数，然后才允许用户重新输入其密码。

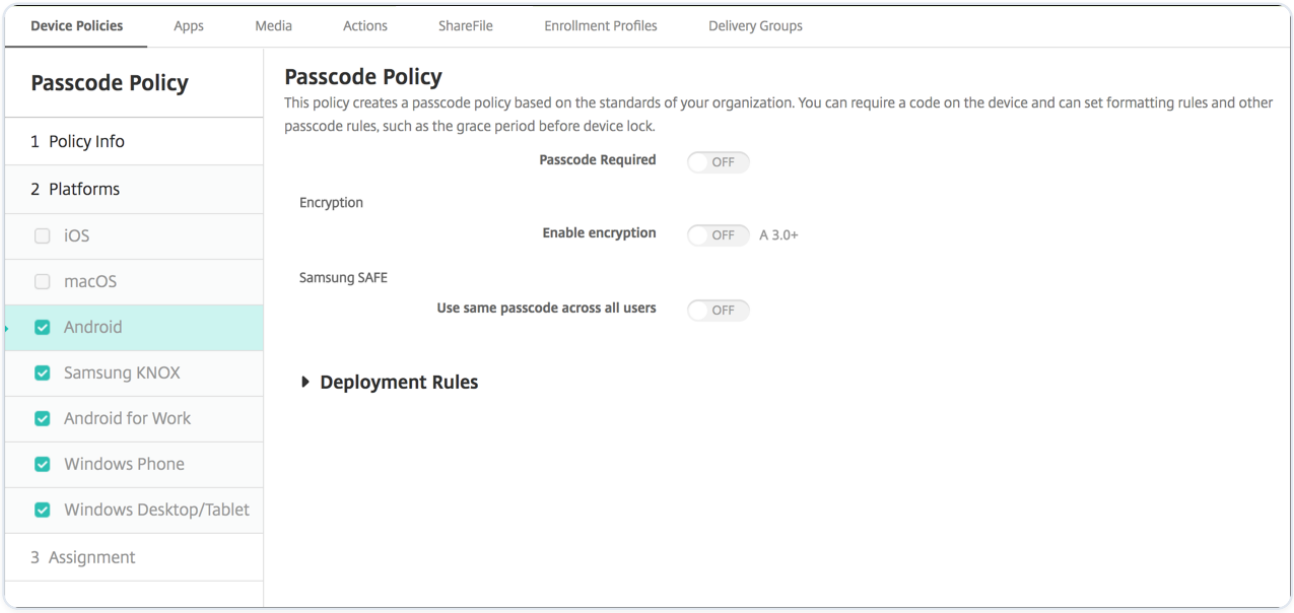
- 如果启用**需要密码**，请配置以下设置：
- **密码要求**
  - **最小长度：** 在下拉列表中单击最小密码长度。默认值为 **6**。
  - **允许简单密码：** 选择是否允许简单密码。简单密码是重复或连续的字符集。默认值为 **开**。
  - **所需字符：** 选择是否要求密码至少包含一个字母。默认值为 **关**。
  - **最少符号数：** 在列表中，单击密码必须包含的符号数。默认值为 **0**。
- **密码安全性**
  - **设备锁定宽限期：** 在列表中，单击用户必须输入密码才能解锁锁定的设备之前的时间长度。默认值为 **无**。
  - **不活动后锁定设备：** 在列表中，单击设备在锁定前可以不活动的时间长度。该值可以在 1 到 5 分钟之间。将该值设置为 **无** 以禁用此策略。默认值为 **无**。
  - **密码有效期（天，1-730）：** 键入密码过期后的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
  - **已保存的旧密码数 (0-50)：** 键入要保存的已用密码数。用户无法使用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。
  - **最大登录失败尝试次数：** 在列表中，单击用户可以登录失败的次数。
    - 如果您将此数字设置为大于 6，则在第六次尝试后，设备会在尝试之间施加时间延迟。时间延迟会随着每次失败的尝试而增加。在最后一次尝试后，设备将锁定。
    - 如果您将此数字设置为 6 或更低，设备将直接锁定，而不会施加时间延迟。
    - 如果您选择 **未定义**，则在 6 次尝试后，设备会在尝试之间施加递增的时间限制，但不会锁定。

    默认值为 **未定义**。
  - **延迟失败登录尝试后的时间（分钟）：** 输入用户达到最大失败尝试次数后，登录窗口出现前的分钟数。
  - **强制重置密码：** 如果为**关闭**，则用户在其设备收到此策略后，下次进行身份验证时无需重置密码。默认值为**开启**。
- **策略设置**
  - **移除策略：** 选择一种计划策略移除的方法。可用选项为**选择日期**和**移除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的移除日期。

- **移除前持续时间（小时）：** 输入一个数字（以小时为单位），表示策略移除前的持续时间。

- **允许用户移除策略：** 您可以选择用户何时可以从其设备中移除策略。从菜单中选择**始终**、**需要密码**或**从不**。如果选择**需要密码**，请在**移除密码**字段中输入密码。
- **配置文件范围：** 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 macOS 10.7 及更高版本。

Android（旧版设备管理员）设置



> **注意：**

> Android 的默认设置为**关闭**。

- **需要密码：** 选择此选项以要求输入密码，并显示 Android 密码设备策略的配置选项。页面将展开，允许您配置密码要求、密码安全和加密的设置。
- **密码要求**
  - **最小长度：** 在下拉列表中单击最小密码长度。默认值为 6。
  - **生物识别：** 选择是否启用生物识别。如果启用此选项，“所需字符”字段将隐藏。默认值为**关闭**。
  - **所需字符：** 在列表中，单击**无限制**、**数字和字母**、**仅数字**或**仅字母**以配置密码的组成方式。默认值为**无限制**。
  - **高级规则：** 选择是否应用高级密码规则。默认值为**关闭**。

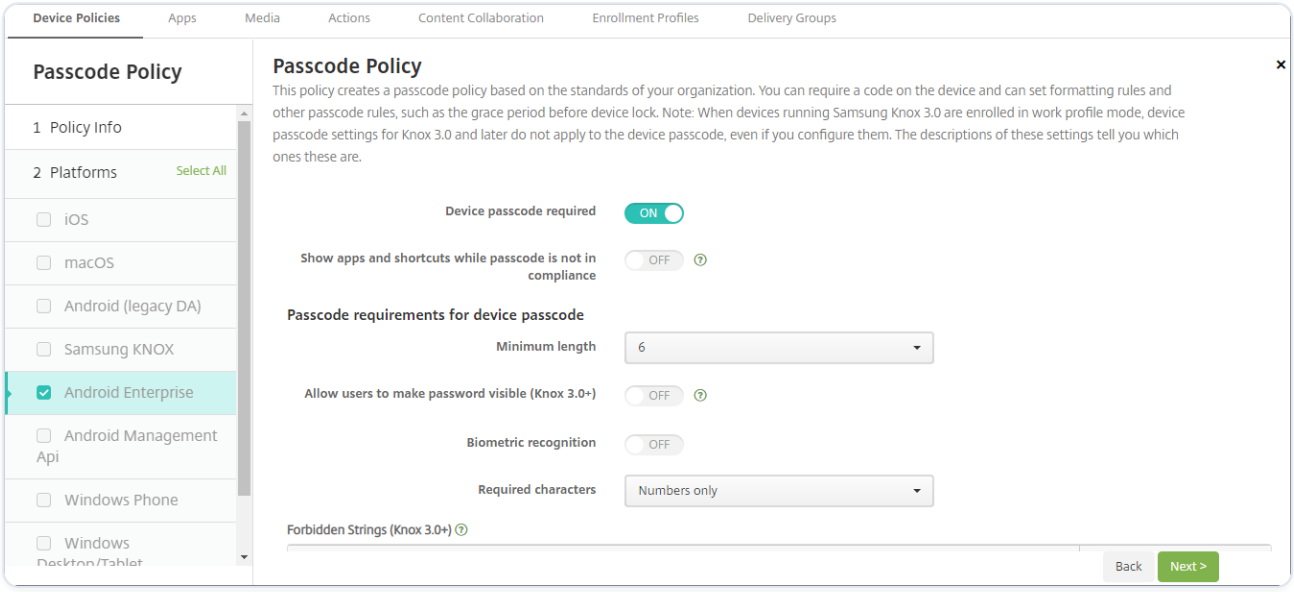
- 启用**高级规则**后，从以下每个列表中，单击密码必须包含的每种字符类型的最小数量：
  - **符号：** 符号的最小数量。
  - **字母：** 字母的最小数量。
  - **小写字母：** 小写字母的最小数量。
  - **大写字母：** 大写字母的最小数量。
  - **数字或符号：** 数字或符号的最小数量。
  - **数字：** 数字的最小数量。

- **密码安全性**
  - **不活动后锁定设备：** 在列表中，单击设备在锁定前可以不活动的时间长度。默认值为**无**
  - **密码过期天数 (1-730)：** 键入密码过期后的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
  - **已保存的以前密码 (0-50)：** 键入要保存的已用密码数量。用户无法使用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。
  - **最大登录失败尝试次数：** 在列表中，单击用户在设备被擦除前可以登录失败的次数。默认值为**未定义**。

- **加密**
  - **启用加密**：选择是否启用加密。无论“**需要密码**”设置如何，此选项都可用。

    要加密设备，用户必须从电池充满电开始，并保持设备插电状态，直到加密完成。此过程可能需要一小时或更长时间。如果中断加密过程，他们可能会丢失设备上的部分或全部数据。设备加密后，除非执行出厂重置（这将擦除设备上的所有数据），否则无法撤消此过程。

安卓企业版设置



对于 Android Enterprise 设备，您可以要求设备提供密码，或要求 Android Enterprise 工作配置文件提供安全质询，或两者兼而有之。

- **需要设备密码**：要求设备提供密码。当此设置为“**开**”时，请配置“**设备密码要求**”和“**设备密码安全**”下的设置。默认值为“**关**”。
- **在密码不合规时显示应用程序和快捷方式**：当此设置为“**开**”时，即使密码不合规，设备上的应用程序和快捷方式也不会隐藏。当此设置为“**关**”时，如果密码不合规，则会隐藏应用程序和快捷方式。如果启用此设置，Citrix® 建议您创建自动化操作，以便在密码不合规时将设备标记为不合规。默认值为“**关**”。
- **设备密码要求**：
  - **最小长度**：指定最小密码长度。默认值为 6。
  - **生物识别**：启用生物识别。如果此设置为“**开**”，则会隐藏“**所需字符**”字段。默认值为“**关**”。
  - **所需字符**：指定密码所需的字符类型。在列表中，选择“**无限制**”、“**数字和字母**”、“**仅数字**”或“**仅字母**”。仅对运行 Android 7.0 的设备使用“**无限制**”。Android 7.1 及更高版本不遵循“**无限制**”设置。默认值为“**数字和字母**”。
  - **高级规则**：对密码中可以出现的字符类型应用高级规则。当此设置为“**开**”时，请配置“**最少数量**”和“**最多数量**”下的设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为“**关**”。
  - **最少数量**：
    - **符号**：指定最少符号数。默认值为 **0**。
    - **字母**：指定最少字母数。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 及更高版本且已配置有效 Knox 许可证密钥的设备。仅适用于完全托管的设备。此设置不适用于注册为工作配置文件设备的设备。指定用户必须从其上一个密码中更改的字符数。默认值为 **0**。
  - **最大数量：** 适用于运行 Samsung Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。仅适用于完全托管的设备。此设置不适用于注册为工作配置文件设备的设备。
    - **字符可出现的次数：** 指定一个字符在密码中可出现的最大次数。默认值为 **0**，表示没有最大限制。
    - **字母序列长度：** 指定密码中字母序列的最大长度。默认值为 **0**，表示没有最大限制。
    - **数字序列长度：** 指定密码中数字序列的最大长度。默认值为 **0**，表示没有最大限制。
- **设备密码的复杂性 (Android 12+)：**
  - **应用密码复杂性：** 要求密码具有平台定义的复杂性级别，而不是自定义密码要求。仅适用于 Android 12+ 设备以及使用 Citrix Secure Hub 22.9 或更高版本的设备。
  - **复杂性级别：** 预定义的密码复杂性级别。
    - **无：** 无需密码。
    - **低：** 密码可以是：
      - 图案
      - 至少包含四位数字的 PIN
    - **中等：** 密码可以是：
      - 不包含重复序列 (4444) 或有序序列 (1234) 且至少包含四位数字的 PIN
      - 至少包含四个字符的字母密码
      - 至少包含四个字符的字母数字密码
    - **高：** 密码可以是：
      - 不包含重复序列 (4444) 或有序序列 (1234) 且至少包含八位数字的 PIN
      - 至少包含六个字符的字母密码
      - 至少包含六个字符的字母数字密码

> **注意：**
>
> 对于 BYOD 设备，密码设置（例如“最小长度”、“所需字符”、“生物识别”和“高级规则”）不适用于 Android 12+。请改用密码复杂性。

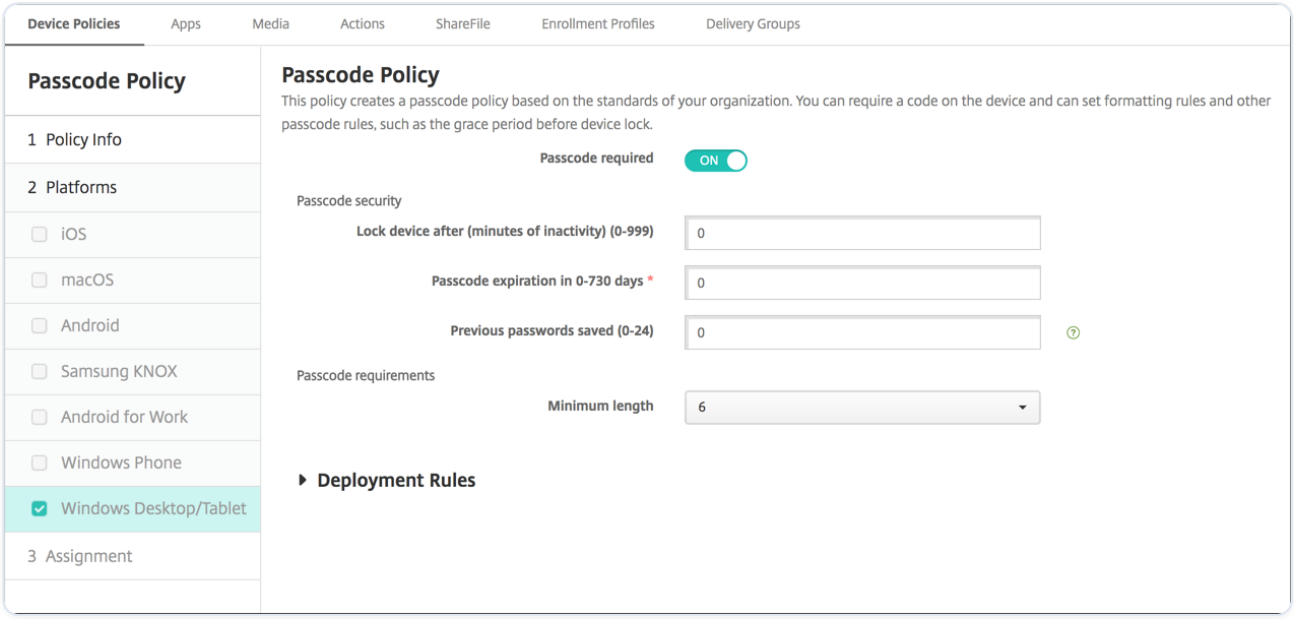
- **设备密码的密码安全性：**
  - **在（登录尝试失败）后擦除设备：** 指定用户可以登录失败的次数，超过该次数后设备将被完全擦除。默认值为**未定义**。
  - **不活动后锁定设备：** 指定设备在锁定前可以不活动的分钟数。将值设置为 0 可禁用此策略。
  - **密码过期天数 (1-730)：** 指定密码过期前的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
  - **已保存的以前密码 (0-50)：** 指定要保存的已用密码数量。用户无法使用此列表中找到的任何密码。有效值为 0–50。默认值为 **0**，表示用户可以重复使用密码。
- **工作配置文件安全质询：** 要求用户完成安全质询，才能访问在 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。当此设置为“**开**”时，请配置“**工作配置文件安全质询的密码要求**”和“**工作配置文件安全质询的密码安全性**”下的设置。默认值为“**关**”。
- **工作配置文件安全质询的密码要求：**
  - **最小长度：** 指定最小密码长度。默认值为 6。
  - **生物识别：** 启用生物识别。如果此设置为“**开**”，则“**所需字符**”字段将隐藏。默认值为“**关**”。
  - **所需字符：** 指定密码所需的字符类型。在列表中，选择“**无限制**”、“**数字和字母**”、“**仅数字**”或“**仅字母**”。仅对运行 Android 7.0 的设备使用“**无限制**”。Android 7.1 及更高版本不遵循“**无限制**”设置。默认值为“**数字和字母**”。
  - **高级规则：** 应用有关密码中可出现的字符类型的高级规则。当此设置为“**开**”时，请配置“**最少数量**”和“**最多数量**”下的设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为“**关**”。
  - **最少数量：**
    - **符号：** 指定最少符号数。默认值为“**0**”。
    - **字母：** 指定最少字母数。默认值为“**0**”。
    - **小写字母：** 指定最少小写字母数。默认值为“**0**”。
    - **大写字母：** 指定最少大写字母数。默认值为“**0**”。

    - **数字或符号：** 指定最少数字或符号数。默认值为“**0**”。
    - **数字：** 指定最少数字数。默认值为“**0**”。
    - **更改的字符：** 适用于运行 Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。指定用户必须从其上一个密码中更改的字符数。默认值为“**0**”。
  - **最多数量：** 适用于运行 Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。
    - **字符出现次数：** 指定密码中字符可出现的最大次数。默认值为 **0**，表示没有最大限制。
    - **字母序列长度：** 指定密码中字母序列的最大长度。默认值为 **0**，表示没有最大限制。
    - **数字序列长度：** 指定密码中数字序列的最大长度。默认值为 **0**，表示没有最大限制。
- **工作配置文件安全质询的密码复杂性 (Android 12+)：**
  - **应用密码复杂性：** 要求密码具有平台定义的复杂性级别，而不是自定义密码要求。仅适用于 Android 12+ 设备以及使用 Citrix Secure Hub 22.9 或更高版本的设备。
  - **复杂性级别：** 预定义的密码复杂性级别。
    - **无：** 无需密码。
    - **低：** 密码可以是：
      - 图案
      - 至少包含四个数字的 PIN
    - **中：** 密码可以是：
      - 不含重复序列 (4444) 或有序序列 (1234) 且至少包含四个数字的 PIN
      - 至少包含四个字符的字母
      - 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) 且至少包含八位数字的 PIN。
      - 字母型，至少包含六个字符。
      - 字母数字型，至少包含六个字符。

> **注意：**
>
> 如果为工作配置文件启用密码复杂性，则还必须为设备启用密码复杂性。

- **工作配置文件安全质询的密码安全性**
  - **在以下次数后擦除容器（登录尝试失败）：** 指定用户可以登录失败的次数，超过该次数后，工作配置文件及其数据将从设备中擦除。擦除发生后，用户必须重新初始化工作配置文件。默认值为**未定义**。
  - **不活动后锁定容器：** 指定设备在工作配置文件被锁定之前可以不活动的分钟数。该值可在 0 到 999 分钟之间。将该值设置为 0 可禁用此策略。
  - **密码有效期（天，1-730）：** 指定密码过期前的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
  - **已保存的先前密码（0-50）：** 指定要保存的已用密码数量。用户无法使用此列表中的任何密码。有效值为 0–50。默认值为 **0**，表示用户可以重复使用密码。

视窗桌面/平板电脑设置



- **需要密码：** 选择此选项可不要求 Windows 桌面/平板电脑设备使用密码。默认设置为**开**，即需要密码。禁用此设置后，页面将折叠，以下选项将消失。
- **密码安全性**
  - **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**。
  - **密码有效期（天，0-730）：** 键入密码过期前的天数。有效值为 0–730。默认值为 **0**，表示密码永不过期。
  - **已保存的旧密码 (0-24)：** 键入要保存的已用密码数。用户无法使用此列表中存在的任何密码。有效值为 1–24。在此字段中输入一个介于 1 到 24 之间的数字。默认值为 **0**。
- **密码要求**

- **最小长度：** 在下拉列表中单击最小密码长度。默认值为 **6**。

密码锁定宽限期设备策略

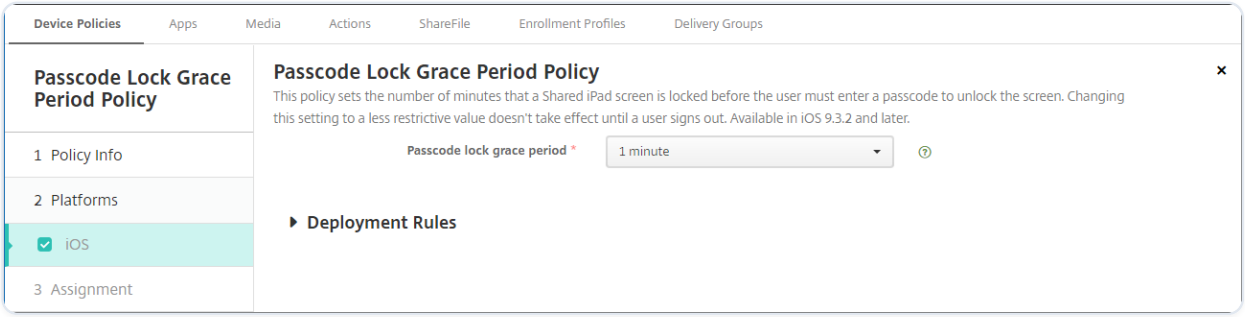
密码锁定宽限期设备策略适用于运行 iOS (iPadOS) 的共享设备。有关共享 iPad 的更多信息，请参阅(/zh-cn/citrix-endpoint-management/device-management/apple/integrate-with-apple-education.html)。

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(/zh-cn/citrix-endpoint-management/policies.html)。

iOS 设置

- **密码锁定宽限期：** 共享 iPad 屏幕在用户必须输入密码才能解锁屏幕之前保持锁定的分钟数。将此设置更改为限制较少的值，直到用户注销后才会生效。默认值为**立即**。

  默认情况下，共享 iPad 在两分钟不活动后会自动锁定。



个人热点设备策略

您可以允许用户在没有 Wi-Fi 网络覆盖的情况下，通过其 iOS 设备的个人热点功能使用蜂窝数据连接来连接互联网。

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

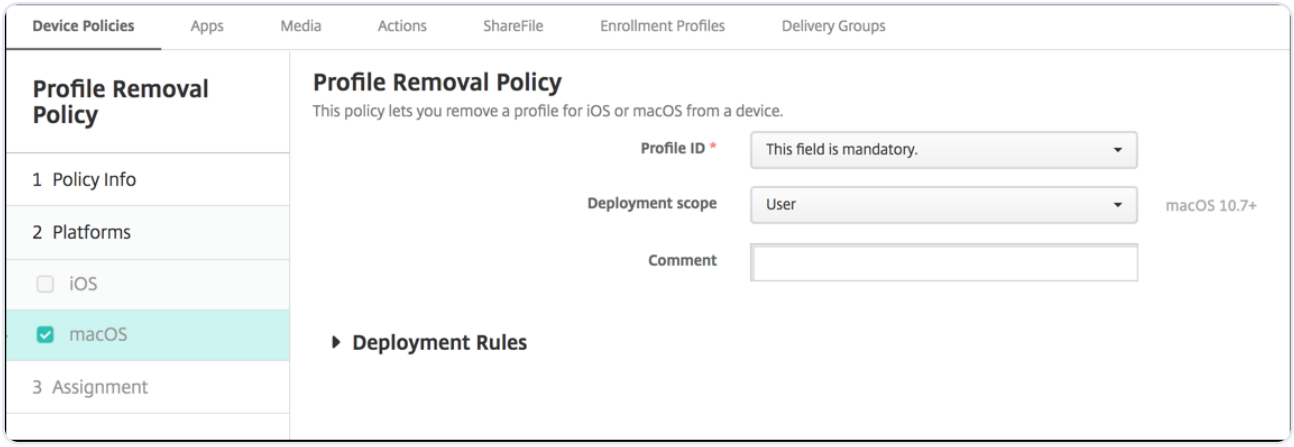
- **禁用个人热点：** 选择是否在用户设备上禁用个人热点功能。默认设置为**关**，这会关闭用户设备上的个人热点。此策略不会禁用该功能。用户仍可以在其设备上使用个人热点，但部署此策略后，个人热点将关闭，因此默认情况下不会保持开启状态。

配置文件移除设备策略

您可以在 Citrix Endpoint Management 中创建应用程序配置文件移除设备策略。部署后，该策略会从用户的 iOS 或 macOS 设备中移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。

macOS 设置



- **配置文件 ID：** 在下拉列表中单击应用程序配置文件 ID。此字段为必填项。
- **部署范围：** 在下拉列表中单击**用户**或**系统**。默认值为**用户**。此选项仅适用于 macOS 10.7 及更高版本。
- **注释：** 键入可选注释。

配置文件设备策略

当您开发并对 iOS 企业应用进行代码签名时，您通常会包含一个企业分发配置文件，这是 Apple 要求应用在 iOS 设备上运行所必需的。如果配置文件丢失或已过期，用户点击打开应用时，应用会崩溃。

配置文件的主要问题是，它们在 Apple Developer Portal 上生成后一年就会过期，您必须跟踪用户注册的所有 iOS 设备上所有配置文件的过期日期。跟踪过期日期不仅包括跟踪实际的过期日期，还包括哪些用户正在使用哪个版本的应用。两种解决方案是将配置文件通过电子邮件发送给用户，或者将其放在门户网站上供下载和安装。这些解决方案可行，但容易出错，因为它们要求用户根据电子邮件中的说明进行操作，或者访问门户网站下载正确的配置文件并进行安装。

为了让用户对这一过程透明，在 Citrix Endpoint Management 中，您可以使用设备策略安装和删除配置文件。丢失或过期的配置文件会根据需要被删除，最新的配置文件会安装到用户的设备上，这样，点击应用即可直接打开使用。

在创建配置文件策略之前，您必须创建一个配置文件。有关详细信息，请参阅 Apple 关于如何在 Apple Developer 网站 上创建开发配置文件的文章。

iOS 设置

- **iOS 配置文件：** 通过单击“**浏览**”并导航到文件位置来选择要导入的配置文件。

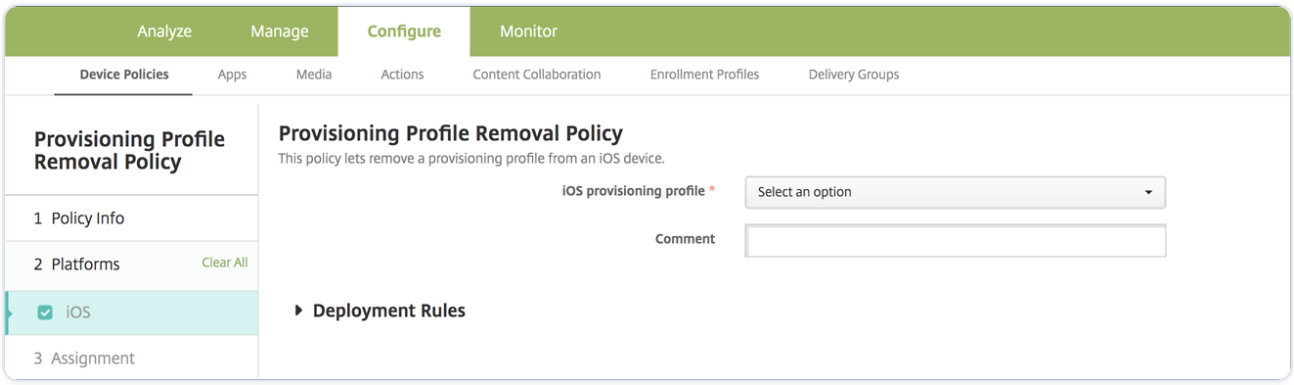
配置文件移除设备策略

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。有关更多信息，请参阅 配置文件设备策略。

要移除或替换旧的配置文件，请使用配置文件移除设备策略。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关更多信息，请参阅 设备策略。

iOS 设置



- **iOS 配置文件：** 单击下拉列表中要移除的配置文件。
- **注释：** （可选）添加注释。

代理设备策略

代理设备策略为受支持的 iOS 设备指定全局 HTTP 代理设置。每个设备只能部署一个全局 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。

先决条件

在部署此策略之前，请务必将所有要设置全局 HTTP 代理的 iOS 设备设置为监督模式。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。

在将代理策略发送到设备之前，设置部署规则以注册设备。

iOS 设置

- **代理配置：** 单击**手动**或**自动**以指定如何在用户设备上配置代理。
  - 如果单击**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。此字段为必填项。
    - **代理服务器端口：** 键入代理服务器端口号。此字段为必填项。
    - **用户名：** 键入可选用户名以向代理服务器进行身份验证。
    - **密码：** 键入可选密码以向代理服务器进行身份验证。
  - 如果单击**自动**，请配置以下设置：
    - **代理 PAC URL：** 键入定义代理配置的 PAC 文件的 URL。
    - **如果 PAC 不可达则允许直接连接：** 选择当 PAC 文件不可达时，是否允许用户直接连接到目标。默认设置为 **开**。
- **允许绕过代理访问强制门户网络：** 选择是否允许绕过代理访问强制门户网络。默认设置为 **关**。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括 **选择日期** 和 **删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略删除前的持续时间。仅适用于 iOS 6.0 及更高版本。

限制设备策略

> **注意：**
>
> 当升级包含新的限制设备策略设置时，您必须编辑并保存该策略。在您保存升级后的限制设备策略之前，Citrix Endpoint Management 不会部署它。

限制设备策略允许或限制用户设备上的某些功能或特性，例如摄像头。您可以设置安全限制和媒体内容限制。您还可以设置用户可以和不能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*”。主要例外是 iOS 安全 - 强制功能和所有 Windows 平板电脑功能，它们默认为“**关**”或“*限制*”。

您选择“**开**”的任何选项都表示用户可以执行该操作或使用该功能。例如：

- **摄像头：** 如果设置为“**开**”，用户可以使用其设备上的摄像头。如果设置为“**关**”，用户无法使用其设备上的摄像头。
- **屏幕截图：** 如果设置为“**开**”，用户可以在其设备上截屏。如果设置为“**关**”，用户无法在其设备上截屏。

如果您同时配置了限制设备策略和自助服务终端设备策略，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。

iOS 设置



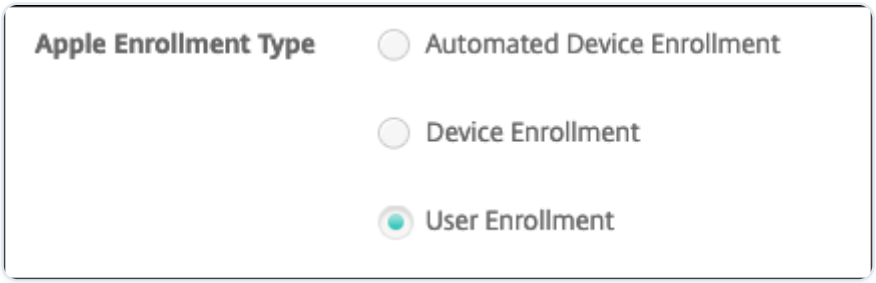
某些 iOS 限制策略设置仅适用于特定版本的 iOS，此处和 Citrix Endpoint Management 控制台限制策略页面中均有说明。

当设备注册到用户注册模式、非监督（完全 MDM）模式或监督模式时，这些设置适用。下表显示了 iOS 13 及更高版本中每个设置可用的注册模式。

- **自动设备注册：** 受监督设备。这些是通过批量注册注册的设备。
- **设备注册：** 非监督设备。这些设备是单独注册的，并且整个设备都完全受 MDM 管理。

- **用户注册：** 仅管理特定用户的设备。有关用户注册的详细信息，请参阅 Apple 文档。

当设备注册到用户注册模式、非监督（完全 MDM）模式或监督模式时，iOS 限制策略设置可能适用。下表显示了适用于 iOS 13 及更高版本中每个限制策略设置的注册模式。



如表中所示，以前在非监督模式和监督模式下可用的一些设置从 iOS 13 开始仅在监督模式下可用。以下规则适用：

- 如果监督的 iOS 13+ 设备注册到 Citrix Endpoint Management，这些设置将应用于设备。
- 如果非监督的 iOS 13+ 设备注册到 Citrix Endpoint Management，这些设置不应用于设备。
- 如果 iOS 12（或更低版本）设备已注册到 Citrix Endpoint Management，然后升级到 iOS 13，则没有变化。这些设置将像升级前一样应用于设备。

有关将 iOS 设备设置为监督模式的信息，请参阅使用 Apple Configurator 2 部署设备。

设置	用户注册	非监督	监督
允许硬件控制			
相机	否	是	是
FaceTime	否	否	是
允许 FaceTime 远程控制	否	否	是
屏幕截图	是	否	是
允许课堂应用远程观察学生屏幕	否	否	是
允许课堂应用执行 AirPlay 和屏幕共享，无需提示	否	否	是
照片流	否	是	是

设置	用户注册	非监督	监督
共享照片流	否	是	是
允许共享 iPad 临时会话	否	否	是
语音拨号	否	是	是
Siri 语音助手	是	是	是
设备锁定时允许	是	是	是
Siri 脏话过滤器	否	否	是
安装应用	否	否	是
备用应用市场	否	否	是
Web 分发应用	否	否	是
漫游时允许全局后台获取	否	是	是
允许应用			
iTunes 商店	否	否	是
应用内购买	否	是	是
购买时需要 iTunes Store 密码	否	是	是
Safari 浏览器	否	否	是
自动填充	否	否	是
强制显示欺诈警告	是	是	是
启用 JavaScript	否	是	是
阻止弹窗	否	是	是
接受 Cookie	否	是	是

设置	用户注册	非监督	监督
网络 - 允许 iCloud 操作			
iCloud 文档和数据	否	否	是
iCloud 备份	否	是	是
iCloud 照片钥匙串	否	是	是
iCloud 照片图库	否	是	是
安全性 - 强制			
加密备份	是	是	是
限制广告跟踪	否	是	是
首次 AirPlay 配对时需要密码	是	是	是
配对的 Apple Watch 使用腕部检测	是	是	是
使用 AirDrop 共享受管文档	是	是	是
安全性 - 允许			
接受不受信任的 SSL 证书	否	是	是
证书信任设置的自动更新	否	是	是
要求受管剪贴板	是	是	是
非受管应用中的受管应用文档	是	是	是
非受管应用读取受管联系人	否	否	是

设置	用户注册	非监督	监督
受管应用写入非受管联系人	否	否	是
受管应用中的非受管应用文档	是	是	是
向 Apple 提交诊断信息	是	是	是
使用触控 ID 解锁设备	否	是	是
自动解锁	否	是	是
锁定时的钱包通知	否	是	是
接力	否	是	是
受管应用的 iCloud 同步	是	是	是
企业图书备份	是	是	是
企业图书的笔记和高亮同步	是	是	是
Spotlight 中的互联网结果	否	是	是
企业应用信任	否	是	是
允许 Apple 个性化广告	否	是	是
仅限受监督设备设置 - 允许			
允许修改 eSIM	否	否	是
抹掉时保留 eSIM	否	否	是
抹掉所有内容和设置	否	否	是

设置	用户注册	非监督	监督
屏幕使用时间	否	否	是
播客	否	否	是
安装配置描述文件	否	否	是
触控 ID 和面容 ID 修改	否	否	是
从设备安装应用	否	否	是
键盘快捷键	否	否	是
配对的 Apple Watch	否	否	是
密码修改	否	否	是
设备名称修改	否	否	是
壁纸修改	否	否	是
自动下载应用	否	否	是
隔空投送	否	否	是
iMessage	否	否	是
Siri 用户生成内容	否	否	是
iBooks	否	否	是
移除应用	否	是	是
游戏中心	否	否	是
添加朋友	否	否	是
多人游戏	否	否	是
修改帐户设置	否	否	是

设置	用户注册	非监督	监督
修改应用蜂窝数据设置	否	否	是
修改应用蜂窝数据设置	否	否	是
允许网络驱动器连接	否	否	是
允许 USB 设备连接	否	否	是
允许查找我的设备	否	否	是
允许查找我的朋友设置	否	否	是
修改查找我的朋友设置	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 QuickPath 键盘	否	否	是
定义查找	否	否	是
单个应用捆绑包 ID	否	否	是
新闻	否	否	是
Apple Music 服务	否	否	是
Apple Music 广播	否	否	是
通知修改	否	否	是
受限应用使用	否	否	是

设置	用户注册	非监督	监督
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 开关状态	否	否	是
仅加入由网络策略安装的 Wi-Fi 网络	否	否	是
允许课堂应用在不提示的情况下执行 AirPlay 和查看屏幕	否	否	是
允许课堂应用在不提示的情况下锁定到某个应用并锁定设备	否	否	是
在不提示的情况下自动加入课堂应用课程	否	否	是
允许 AirPrint	否	否	是
允许将 AirPrint 凭据存储在钥匙串中	否	否	是
允许使用 iBeacon 发现 AirPrint 打印机	否	否	是
仅允许 AirPrint 连接到具有受信任证书的目标	否	否	是
添加 VPN 配置	否	否	是
修改蜂窝网络套餐设置	否	否	是
移除系统应用	否	否	是
设置新的附近设备	否	否	是

设置	用户注册	非监督	监督
允许 USB 受限模式	否	否	是
强制延迟软件更新	否	否	是
强制软件更新延迟	否	否	是
强制课堂请求离开课堂的权限	否	否	是
强制在自动填充前进行身份验证	否	否	是
强制自动日期和时间	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
允许未配对设备启动到恢复模式	否	否	是
安装快速安全响应	否	否	是
移除快速安全响应	否	否	是
允许邮件隐私保护	否	否	是
NFC	否	否	是
允许App Clips	否	否	是
生成式表情符号	否	否	是
图像游乐场	否	否	是
图像魔杖	否	否	是
iPhone 镜像	否	否	是

设置	用户注册	非监督	监督
个性化手写结果	否	否	是
书写工具	否	否	是
通话录音	否	否	是
要隐藏的应用程序	否	否	是
要锁定的应用程序	否	否	是
邮件摘要	否	否	是
RCS 消息	否	否	是
允许外部智能集成	否	否	是
允许登录外部智能集成	否	否	是
允许邮件智能回复	否	否	是
允许备忘录转录	否	否	是
允许 Safari 摘要	否	否	是
允许视觉智能摘要	否	否	是
允许备忘录转录摘要	否	否	是
允许 Apple 智能报告	否	否	是
允许修改默认通话应用	否	否	是
允许修改默认消息应用	否	否	是
允许外部智能工作区 ID	否	否	是
默认浏览器修改	否	否	是

设置	用户注册	非监督	监督
允许实时语音邮件	否	否	是
安全性 - 在锁定屏幕中显示			
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			
露骨音乐、播客和 iTunes U 材料	否	否	是
iBooks 中的露骨性内容	否	是	是
评级区域	否	是	是
电影	否	是	是
电视节目	否	是	是
应用	否	是	是

- **允许硬件控制**
  - **摄像头：** 允许用户在其设备上使用摄像头。
    - **FaceTime：** 允许用户在其设备上使用 FaceTime。适用于受监管的 iOS 设备。
    - **允许 FaceTime 远程控制：** 允许远程 FaceTime 会话请求控制设备。适用于受监管的 iOS 设备。适用于 iOS 18.4 及更高版本。
  - **屏幕截图：** 允许用户在其设备上截屏。
    - **允许课堂应用远程观察学生屏幕：** 如果未选择此限制，教师将无法使用课堂应用远程观察学生屏幕。默认设置为选中，教师可以使用课堂应用观察学生屏幕。**允许课堂应用在不提示的情况下执行 AirPlay 和查看屏幕**的设置决定了学生是否会收到提示以授予教师权限。适用于受监管的 iOS 设备。

- **允许课堂应用在不提示的情况下执行 AirPlay 和查看屏幕：** 如果选择此限制，教师可以在学生设备上执行 AirPlay 和查看屏幕，而无需提示权限。默认设置为未选中。适用于受监管的 iOS 设备。

- **照片流：** 允许用户使用“我的照片流”通过 iCloud 将照片共享到其所有 iOS 设备。
- **共享照片流：** 允许用户使用 iCloud 照片共享与同事、朋友和家人共享照片。
- **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：** 在用户设备上启用语音拨号。
- **Siri：** 允许用户使用 Siri。
  - **设备锁定时允许：** 允许用户在设备锁定时使用 Siri。
  - **Siri 脏话过滤器：** 启用 Siri 脏话过滤器。默认是限制此功能，这意味着不进行脏话过滤。

    有关 Siri 和安全性的更多信息，请参阅 Siri 和听写策略。
- **安装应用：** 允许用户安装应用。适用于受监管的 iOS 设备。
- **替代应用市场：** 阻止从网络安装替代市场应用，并阻止任何已安装的替代市场应用安装其他应用。此功能适用于 iOS 17.4 及更高版本。默认设置为**开启**。适用于受监管的 iOS 设备。
- **Web 分发应用：** 允许客户管理员阻止 iOS 设备上通过 Web 分发的第三方应用。这适用于 iOS 17.5 及更高版本。有关详细信息，请参阅限制。
- **漫游时允许全局后台获取：** 允许设备在漫游时自动将邮件帐户同步到 iCloud。当设置为“**关闭**”时，会在 iOS 手机漫游时禁用全局后台获取活动。默认为“**开启**”。

- **允许应用**
  - **iTunes Store：** 允许用户访问 iTunes Store。适用于受监管的 iOS 设备。
  - **应用内购买：** 允许用户进行应用内购买。
    - **购买时需要 iTunes Store 密码：** 要求应用内购买时输入密码。默认是限制此功能，这意味着应用内购买不需要密码。
  - **Safari：** 允许用户访问 Safari。适用于受监管的 iOS 设备。
    - **自动填充：** 允许用户在 Safari 上设置用户名和密码的自动填充。
    - **强制欺诈警告：** 如果启用此设置，并且用户访问可疑的钓鱼网站，Safari 会向用户发出警报。默认是限制此功能，这意味着不发出任何警告。
    - **启用 JavaScript：** 允许 JavaScript 在 Safari 上运行。

    - **阻止弹出窗口：** 在浏览网站时阻止弹出窗口。默认是限制此功能，这意味着不阻止弹出窗口。

  - **接受 Cookie：** 设置接受 Cookie 的程度。在列表中，选择一个选项以允许或限制 Cookie。默认选项是“**始终**”，它允许所有网站在 Safari 中保存 Cookie。其他选项包括“**仅当前网站**”、“**从不**”和“**仅来自访问过的网站**”。

- **网络 - 允许 iCloud 操作**
  - **iCloud 文档和数据：** 允许用户将文档和数据同步到 iCloud。适用于受监管的 iOS 设备。
  - **iCloud 备份：** 允许用户将其设备备份到 iCloud。
  - **iCloud 钥匙串：** 允许用户在 iCloud 钥匙串中存储密码、Wi-Fi 网络、信用卡及其他信息。
  - **云照片图库：** 允许用户访问其 iCloud 照片图库。
- **安全性 - 强制**

  默认情况下，以下功能受到限制，这意味着未启用任何安全功能。
  - **加密备份：** 强制将备份到 iCloud 的数据进行加密。
  - **限制广告跟踪：** 阻止定向广告跟踪。
  - **首次 AirPlay 配对时需要密码：** 要求 AirPlay 设备在使用 AirPlay 之前，通过一次性屏幕代码进行验证。
  - **配对的 Apple Watch 使用腕部检测：** 要求配对的 Apple Watch 使用**腕部检测**。
  - **使用 AirDrop 共享托管文档：** 将此选项设置为**开**会使 AirDrop 显示为非托管投放目标。
- **安全性 - 允许**
  - **接受不受信任的 SSL 证书：** 允许用户接受网站的不受信任的 SSL 证书。
  - **自动更新证书信任设置：** 允许自动更新受信任的证书。
  - **要求托管剪贴板：** 允许复制和粘贴功能遵循您应用于**非托管应用中的托管应用文档**和**托管应用中的非托管应用文档**的相同限制。 例如，您可以配置以下内容：
    - **要求托管剪贴板：** 开
    - **非托管应用中的托管应用文档：** 关
    - **非托管应用中的文档在托管应用中：** 开启 将策略部署到 iOS 设备后，用户无法将数据从托管应用复制并粘贴到非托管应用，但可以将数据从非托管应用复制并粘贴到托管应用。

- **托管应用中的文档在非托管应用中：** 允许用户将数据从托管（公司）应用移动到非托管（个人）应用。
- **非托管应用中的文档在托管应用中：** 允许用户将数据从非托管（个人）应用移动到托管（公司）应用。
- **将诊断数据提交给 Apple：** 允许将有关用户设备的匿名诊断数据发送给 Apple。
- **使用触控 ID 或面容 ID 解锁设备：** 允许用户使用触控 ID 或面容 ID 解锁其设备。
- **自动解锁：** 如果设置为“**关闭**”，用户无法使用 Apple Watch 解锁配对的 iPhone。默认设置为“**开启**”。适用于 iOS 14.5 及更高版本。
- **锁定时的钱包通知：** 允许钱包通知显示在锁定屏幕上。
- **接力：** 允许用户将活动从一台 iOS 设备传输到另一台附近的 iOS 设备。
- **托管应用的 iCloud 同步：** 允许用户将托管应用同步到 iCloud。
- **企业图书备份：** 允许将企业图书备份到 iCloud。
- **企业图书的笔记和高亮同步：** 允许用户添加到企业图书的笔记和高亮同步到 iCloud。
- **企业应用信任：** 允许信任企业应用程序。企业应用是为您的组织定制的任何应用。这些应用可以在内部制作，也可以由外部供应商开发和购买。有关其他信息，请参阅在 iOS 上安装自定义企业应用。
- **Spotlight 中的互联网结果：** 允许 Spotlight 除了显示设备上的搜索结果外，还显示来自互联网的搜索结果。
- **非托管应用读取托管联系人：** 可选。仅当“**托管应用中的文档在非托管应用中**”被禁用时可用。如果启用此策略，非托管应用可以读取托管帐户联系人中的数据。默认设置为“**关闭**”。适用于 iOS 12 及更高版本。
- **托管应用写入非托管联系人：** 可选。如果启用，允许托管应用将联系人写入非托管帐户的联系人。如果“**托管应用中的文档在非托管应用中**”已启用，则此限制无效。默认设置为“**关闭**”。适用于 iOS 12 及更高版本。
- **允许 Apple 个性化广告：** 如果为 **关**，Apple 广告平台将无法使用用户数据来投放个性化广告。默认值为 **开**。适用于 iOS 14.0 及更高版本。

- **仅限受监督设备设置 - 允许**

  这些设置仅适用于受监督设备。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。
  - **擦除时保留 eSIM：** 如果为 **开**，当系统因密码尝试失败次数过多或在 **设置 > 通用 > 重置** 中选择“抹掉所有内容和设置”选项而擦除设备时，系统将保留 eSIM。默认值为 **关**。

> **注意：**
>
> 如果“**查找**”启动擦除设备，系统将不会保留 eSIM。

- **抹掉所有内容和设置：** 允许用户抹掉其设备上的所有内容和设置。
- **屏幕使用时间：** 允许用户启用屏幕使用时间。
- **播客：** 允许用户下载和同步播客。
- **安装配置描述文件：** 允许用户安装非您部署的配置描述文件。
- **修改触控 ID 和面容 ID：** 允许用户更改或删除其触控 ID 或面容 ID。
- **从设备安装应用：** 允许用户安装应用。禁用此设置可阻止最终用户安装新应用。App Store 将被禁用，其图标将从主屏幕中移除。
- **键盘快捷键：** 允许用户为其经常使用的词语或短语创建自定义键盘快捷键。
- **配对的 Apple Watch：** 允许用户将 Apple Watch 与受监督设备配对。
- **修改密码：** 允许用户更改受监督设备上的密码。
- **设备名称修改：** 允许用户更改其设备的名称。
- **壁纸修改：** 允许用户更改其设备上的壁纸。
- **自动下载应用程序：** 允许应用程序下载。
- **隔空投送 (AirDrop)：** 允许用户与附近的 iOS 设备共享照片、视频、网站、位置等。
- **iMessage：** 允许用户通过 Wi-Fi 使用 iMessage 发送短信。
- **Siri 用户生成内容：** 允许 Siri 查询来自网络的用户生成内容。消费者而非传统记者会生成用户生成内容。例如，在 Twitter 或 Facebook 上找到的内容就是用户生成内容。
- **iBooks：** 允许用户使用 iBooks 应用程序。
- **移除应用程序：** 允许用户从其设备中移除应用程序。
- **Game Center：** 允许用户通过其设备上的 Game Center 玩在线游戏。
  - **添加好友：** 允许用户向好友发送玩游戏的通知。
  - **多人游戏：** 允许用户在其设备上开始多人游戏。
- **修改帐户设置：** 允许用户修改其设备帐户设置。
- **修改应用程序蜂窝数据设置：** 允许用户修改应用程序使用蜂窝数据的方式。
- **允许网络驱动器连接：** 阻止在“文件”应用程序中连接到网络驱动器。
- **允许 USB 设备连接：** 阻止在“文件”应用程序中连接到任何已连接的 USB 设备。

- **允许查找我的设备：** 禁用“查找”应用中的“**查找我的设备**”选项。
- **允许查找我的朋友设置：** 禁用“查找”应用中的“**查找我的朋友**”选项。
- **修改查找我的朋友设置：** 允许用户更改其“查找我的朋友”设置。
- **与非 Configurator 主机配对：** 允许管理员控制用户设备可以与哪些设备配对。禁用此设置可防止配对，除非是与运行 Apple Configurator 的监督主机配对。如果未配置监督主机证书，则所有配对都将被禁用。
- **预测键盘：** 允许用户设备使用预测键盘在键入时建议单词。在管理标准化测试等情况下禁用此选项，因为您不希望用户访问建议的单词。
- **键盘自动更正：** 允许用户设备使用键盘自动更正。在管理标准化测试等情况下禁用此选项，因为您不希望用户访问自动更正。
- **键盘拼写检查：** 允许用户设备在键入时使用拼写检查。在管理标准化测试等情况下禁用此选项，因为您不希望用户访问拼写检查器。
- **定义查找：** 允许用户设备在键入时使用定义查找。在管理标准化测试等情况下禁用此选项，因为您不希望用户在键入时查找定义。
- **单个应用捆绑包 ID：** 创建一个允许控制设备并防止与其他应用或功能交互的应用列表。 要添加应用，请单击“**添加**”，键入“**应用名称**”，然后单击“**保存**”。对要添加的每个应用重复此过程。
- **新闻：** 允许用户使用“新闻”应用。
- **Apple Music 服务：** 允许用户使用 Apple Music 服务。如果您不允许 Apple Music 服务，则“音乐”应用将以经典模式运行。默认设置为“**开**”。适用于 iOS 9.3 或更高版本。
- **Apple Music 广播：** 允许用户使用 Apple Music 广播。默认设置为“**开**”。适用于 iOS 9.3 或更高版本。
- **通知修改：** 允许用户修改通知设置。
- **受限应用使用：** 允许用户使用所有应用，或者根据您提供的捆绑包 ID 使用或不使用应用。仅适用于受监督的设备。如果您选择“**仅允许某些应用**”，请添加捆绑包 ID 为 `com.apple.webapp` 的应用以允许网页剪辑。

> **注意：**
>
> 从 iOS 11 开始，Apple 对可用于应用限制的策略进行了更改。Apple 不再允许您通过限制相应的 iOS 应用程序捆绑包来移除对“设置”应用和“电话”应用的访问权限。

> 配置“限制设备策略”以阻止某些应用程序并部署策略后：如果您以后想允许部分或全部这些应用程序，更改和部署“限制设备策略”不会更改限制。在这种情况下，iOS 不会将更改应用于 iOS 配置文件。要继续，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”。

如果您将此设置更改为 **仅允许某些应用程序：** 在部署此策略之前，请建议使用 Apple 部署计划注册的设备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。

- **诊断提交修改：** 允许用户在 **设置 > 诊断与用量** 窗格中修改诊断提交和应用程序分析设置。
- **蓝牙修改：** 允许用户修改蓝牙设置。
- **允许听写：** 仅限受监督设备。如果此限制设置为 **关闭**，则不允许听写输入，包括语音转文本。默认设置为 **开启**。
- **修改 Wi-Fi 开启或关闭状态：** 阻止在“设置”或“控制中心”中开启或关闭 Wi-Fi。进入飞行模式也无效。此限制不会阻止选择要使用的 Wi-Fi 网络。
- **仅加入由网络策略安装的 Wi-Fi 网络：** 可选。仅限受监督设备。如果此限制设置为 **开启**，则设备只能加入通过配置配置文件设置的 Wi-Fi 网络。默认设置为 **关闭**。
- **允许课堂应用在不提示的情况下执行 AirPlay 和屏幕共享：** 如果选中此限制，教师可以在学生设备上执行 AirPlay 和屏幕共享，而无需提示权限。默认设置为未选中。适用于受监督的 iOS 设备。
- **允许课堂应用在不提示的情况下锁定到某个应用并锁定设备：** 如果此限制设置为 **开启**，课堂应用会自动将用户设备锁定到某个应用并锁定设备，而无需提示用户。默认设置为 **关闭**。适用于运行 iOS 11（最低版本）的受监督设备。
- **自动加入课堂应用课程，无需提示：** 如果此限制设置为 **开启**，课堂应用会自动将用户加入课程，而无需提示用户。默认设置为 **关闭**。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 **关闭**，用户无法使用 AirPrint 打印。默认设置为 **开启**。当此限制设置为 **开启** 时，将显示这些额外限制。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 用户名和密码将不会存储在钥匙串中。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，则禁用 iBeacon 发现 AirPrint 打印机。此设置可防止虚假的 AirPrint 蓝牙信标进行网络流量钓鱼。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 AirPrint 到具有受信任证书的目标：** 如果选中此限制，用户只能使用 AirPrint 打印到具有受信任证书的目标。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 **关闭**，用户无法创建 VPN 配置。默认设置为 **开启**。适用于运行 iOS 11（最低版本）的受监督设备。
- **修改蜂窝数据套餐设置：** 如果此限制设置为“**关闭**”，用户将无法修改蜂窝数据套餐设置。默认设置为“**开启**”。适用于运行 iOS 11（最低版本）的受监管设备。
- **移除系统应用：** 如果此限制设置为“**关闭**”，用户将无法从其设备中移除系统应用。默认设置为“**开启**”。适用于运行 iOS 11（最低版本）的受监管设备。
- **设置新的附近设备：** 如果此限制设置为“关闭”，用户将无法设置新的附近设备。默认设置为“开启”。适用于运行 iOS 11（最低版本）的受监管设备。
- **允许 USB 受限模式：** 如果设置为“**关闭**”，设备在锁定状态下始终可以连接 USB 配件。默认设置为“**开启**”。仅适用于受监管的 iOS 11.3 及更高版本设备。
- **强制延迟软件更新：** 如果设置为“**开启**”，则会延迟用户看到软件更新的时间。启用此限制后，用户在软件更新发布日期后的指定天数内不会看到软件更新。默认设置为“**关闭**”。仅适用于受监管的 iOS 11.3 及更高版本设备。操作系统更新策略包含更多设置，用于控制设备接收更新的频率。请参阅操作系统更新设备策略。
- **强制软件更新延迟（天）：** 允许您指定设备上软件更新的延迟天数。最大延迟为 **90** 天。默认延迟为 **30** 天。仅适用于受监管的 iOS 11.3 及更高版本设备。
- **强制课堂请求离开课程权限：** 如果设置为“**开启**”，则在 Classroom 中注册了非托管课程的学生在尝试离开课程时必须向老师请求权限。默认设置为“**关闭**”。仅适用于受监管的 iOS 11.3 及更高版本设备。
- **强制自动填充前进行身份验证：** 强制用户在使用自动填充功能前进行身份验证。
- **强制自动日期和时间：** 允许您在受监管设备上自动设置日期和时间。如果设置为“**开启**”，设备用户将无法在“**通用 > 日期与时间**”下取消选中“**自动设置**”。设备上的时区仅在设备能够确定其位置时更新。也就是说，当设备具有蜂窝网络连接或启用了定位服务的 Wi-Fi 连接时。默认设置为“**关闭**”。仅适用于受监管的 iOS 12 及更高版本设备。
- **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“自动强密码”功能。默认设置为“**开启**”。从 iOS 12 开始可用。
- **密码邻近请求：** 可选。如果禁用，用户的设备将不会从附近设备请求密码。默认设置为“**开启**”。从 iOS 12 开始可用。
- **密码共享：** 可选。如果禁用，用户将无法使用“隔空投送密码”功能共享其密码。默认设置为“**开启**”。从 iOS 12 开始可用。

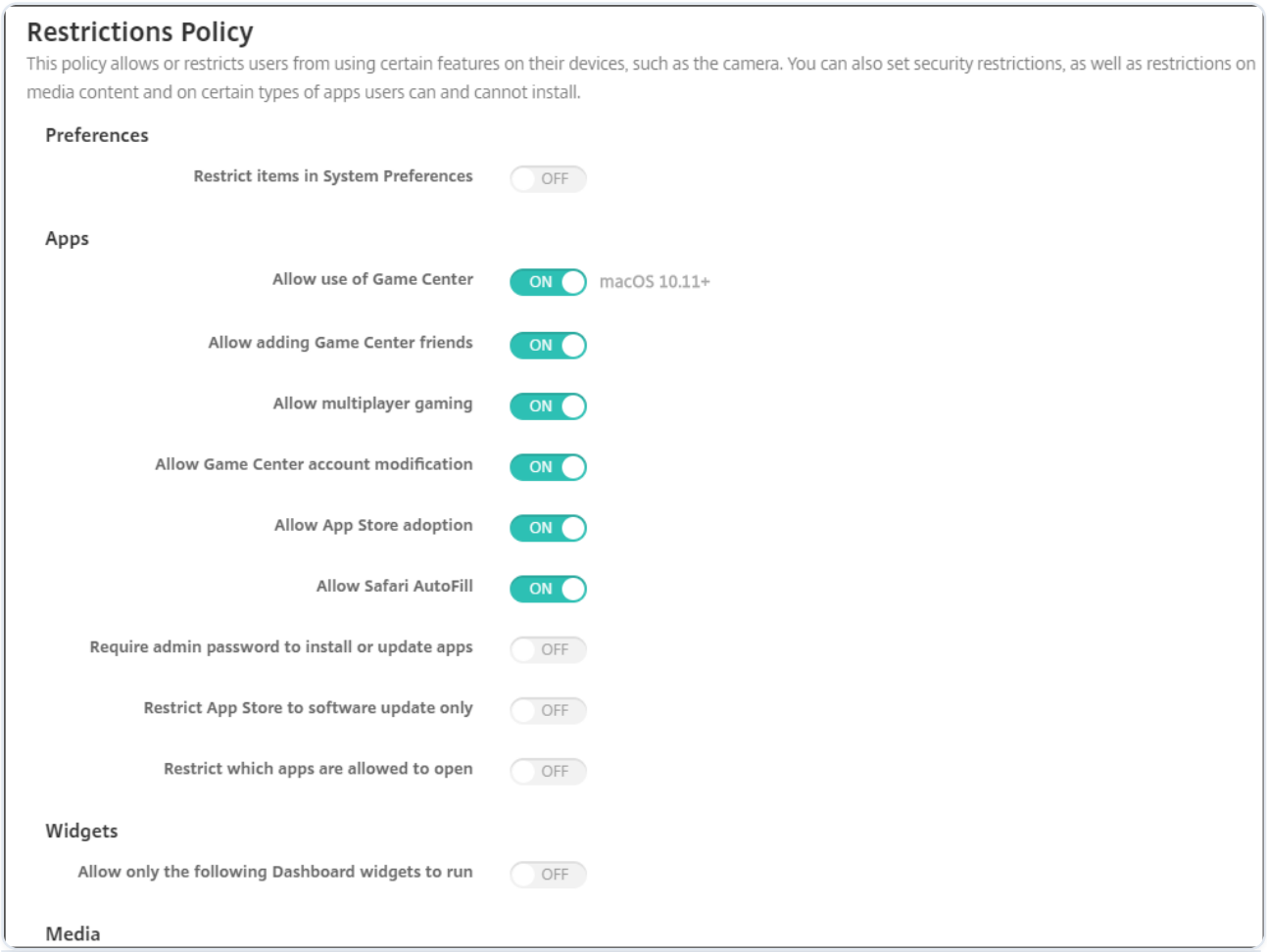
- **允许修改个人热点：** 阻止用户更改个人热点设置。
- **允许未配对设备启动到恢复模式：** 如果设置为“**开启**”，则允许未配对设备将设备启动到恢复模式。默认设置为“**关闭**”。适用于 iOS 14.5 及更高版本。
- **安装快速安全响应：** 如果设置为“**关闭**”，则禁止安装快速安全响应。默认设置为“**开启**”。
- **移除快速安全响应：** 如果设置为“**关**”，则禁止移除快速安全响应。默认设置为“**开**”。
- **允许邮件隐私保护：** 如果设置为“**关**”，则禁用设备上的邮件隐私保护。默认设置为“**开**”。适用于 iOS 15.2 及更高版本。
- **NFC：** 如果设置为“**关**”，则禁用 NFC。默认设置为“**开**”。适用于 iOS 14.2 及更高版本。
- **允许 App Clips**：如果设置为“**关**”，则阻止用户添加任何 App Clips 并移除设备上所有现有的 App Clips。默认设置为“**开**”。适用于 iOS 14.0 及更高版本。
- **Genmoji：** 如果设置为“**关**”，则禁止创建新的 Genmoji。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **图像游乐场：** 如果设置为“**关**”，则禁止使用图像生成功能。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **图像魔杖：** 如果设置为“**关**”，则禁止使用图像魔杖。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **iPhone 镜像：** 如果设置为“**关**”，则禁止使用 iPhone 镜像功能，并阻止 iPhone 镜像到任何 Mac。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **个性化手写结果：** 如果设置为“**关**”，则阻止系统生成用户手写文本。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **书写工具：** 如果设置为“**关**”，则禁用 Apple Intelligence 书写工具。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **通话录音：** 如果设置为“**关**”，则禁用通话录音。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **要隐藏的应用程序：** 如果设置为“**关**”，则阻止用户隐藏应用程序。这不影响将应用程序留在 App 资源库中同时将其从主屏幕移除的功能。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **要锁定的应用程序：** 如果设置为“**关**”，则禁用用户锁定应用程序的功能。由于隐藏应用程序需要锁定它们，因此禁用锁定也会禁用隐藏功能。默认设置为“**开**”。适用于 iOS 18 及更高版本。
- **邮件摘要：** 如果设置为“**关**”，则禁用手动创建电子邮件摘要的功能。这不影响自动摘要生成。默认设置为“**开**”。适用于 iOS 18.1 及更高版本。
- **RCS 消息：** 如果设置为“**关**”，则阻止使用 RCS 消息功能。默认设置为“**开**”。适用于 iOS 18.1 及更高版本。

- **允许外部智能集成：** 如果为“**关闭**”，则禁用 Siri 使用外部基于云的智能服务。默认值为“**开启**”。适用于 iOS 18.2 及更高版本。
- **允许登录外部智能集成：** 如果为“**关闭**”，则强制外部智能提供商进入匿名模式。如果用户已登录外部智能提供商，则应用此限制将在下次尝试请求时导致其退出登录。默认值为“**开启**”。适用于 iOS 18.2 及更高版本。
- **允许邮件智能回复：** 如果为“**关闭**”，则禁用邮件中的智能回复。默认值为“**开启**”。适用于 iOS 18.2 及更高版本。
- **允许备忘录转录：** 如果为“**关闭**”，则禁用备忘录中的转录功能。默认值为“**开启**”。适用于 iOS 18.2 及更高版本。
- **允许 Safari 摘要：** 如果为“**关闭**”，则系统禁用 Safari 中内容摘要功能。默认值为“**开启**”。适用于 iOS 18.4 及更高版本。
- **允许视觉智能摘要：** 如果为“**关闭**”，则系统禁用视觉智能摘要功能。默认值为“**开启**”。适用于 iOS 18.3 及更高版本。
- **允许备忘录转录摘要：** 如果为“**关闭**”，则禁用备忘录中的转录摘要功能。默认值为“**开启**”。适用于 iOS 18.3 及更高版本。
- **允许 Apple 智能报告：** 如果为“**关闭**”，则系统禁用 Apple 智能报告。默认值为“**开启**”。适用于 iOS 18.4 及更高版本。
- **允许修改默认通话应用：** 如果为“**关闭**”，则禁用默认通话应用偏好设置修改。应用此设置后，用于设置默认通话应用偏好设置的 MDM 设置命令仍然有效。默认值为“**开启**”。适用于 iOS 18.4 及更高版本。
- **允许修改默认消息应用：** 如果为“**关闭**”，则禁用默认消息应用偏好设置修改。应用此设置后，用于设置默认消息应用偏好设置的 MDM 设置命令仍然有效。默认值为“**开启**”。适用于 iOS 18.4 及更高版本。
- **允许外部智能工作区 ID：** 一个字符串数组，但目前仅限于单个元素。如果存在，Apple 智能仅允许使用给定的外部集成工作区 ID，并且需要登录才能发出请求；用户将被要求登录支持登录的集成。多个负载使用交集操作组合。这意味着如果多个负载中指定了冲突值，则允许的工作区 ID 集可能变为空集。适用于 iOS 18.3 及更高版本。
  - **外部智能工作区 ID：** 要添加外部智能工作区 ID，请单击“**添加**”，键入“**外部智能工作区 ID**”，然后单击“**保存**”。对要添加的每个工作区 ID 重复此过程。
- **默认浏览器修改：** 如果为“**关闭**”，则禁用默认浏览器偏好设置修改。应用此设置后，用于设置默认浏览器偏好设置的 MDM 设置命令仍然有效。默认值为“**开启**”。适用于 iOS 18.2 及更高版本。

  - **允许实时语音邮件：** 如果为“**关闭**”，则系统禁用设备上的实时语音邮件。默认值为“**开启**”。适用于 iOS 17.2 及更高版本。

- **安全性 - 在锁定屏幕中显示**
  - **控制中心：** 允许在锁定屏幕上访问控制中心。控制中心允许用户轻松修改飞行模式、Wi-Fi、蓝牙、勿扰模式和锁定旋转设置。
  - **通知：** 允许在锁定屏幕上显示通知。
  - **今天视图：** 允许在锁定屏幕上显示“今天视图”，该视图聚合了天气和当天日历项等信息。
- **媒体内容 - 允许**
  - **露骨音乐、播客和 iTunes U 材料：** 允许在用户设备上播放露骨材料。
  - **iBooks 中的露骨性内容：** 允许从 iBooks 下载露骨材料。
  - **评级区域：** 设置获取家长控制评级的区域。在列表中，单击一个国家/地区以设置评级区域。默认值为 **United States**。
  - **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，则可选择设置电影的评级级别。在列表中，单击一个选项以允许或限制设备上的电影。默认值为“允许所有电影”。
  - **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，则可选择设置电视节目的评级级别。在列表中，单击一个选项以允许或限制设备上的电视节目。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，则可选择设置应用程序的评级级别。在列表中，单击一个选项以允许或限制设备上的应用程序。默认值为“允许所有应用程序”。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项为 **Select date** 和 **Duration until removal (in hours)**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。
  - **配置文件范围：** 选择此策略是应用于 **User** 还是整个 **System**。默认值为 **User**。此选项仅适用于 iOS 9.3 及更高版本。

macOS 设置



设置	非受监管	受监管
应用		
允许使用 Game Center	否	是
允许添加 Game Center 好友	否	是
允许多人游戏	否	是
允许修改 Game Center 帐户	是	是
允许采用 App Store	是	是
允许 Safari 自动填充	否	是
安装或更新应用时需要管理员密码	是	是

设置	非受监管	受监管
将 App Store 限制为仅用于软件更新	是	是
限制允许打开的应用	是	是
媒体		
允许隔空投送	否	是
功能		
锁定桌面图片	否	是
允许使用摄像头	否	是
允许使用 Apple Music	否	是
允许使用 Spotlight 建议	是	是
允许查询	是	是
允许将 iCloud 密码用于本地帐户	是	是
允许 iCloud 文档与数据	是	是
允许 iCloud 桌面和文稿	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

设置	非受监管	受监管
允许 iCloud 照片	是	是
允许自动解锁	是	是
允许使用触控 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
图像游乐场	否	是
iPhone 镜像	否	是
写作工具	否	是
允许修改媒体共享	是	是

- **偏好设置**
  - **限制“系统偏好设置”中的项目：** 允许或限制用户访问“系统偏好设置”。默认值为**“关闭”**，这允许用户完全访问“系统偏好设置”。如果启用，请配置以下设置。
    - **系统偏好设置面板：** 选择您选择的设置是启用还是禁用。默认情况下，所有设置都处于启用状态，即默认**开启**。
      - 用户与群组
      - 通用
      - 辅助功能
      - 应用商店
      - 软件更新
      - 蓝牙
      - CD 与 DVD
      - 日期与时间

- 桌面与屏幕保护程序
- 显示器
- 程序坞
- 节能
- 扩展
- 光纤通道
- iCloud
- 墨水
- 互联网帐户
- 键盘
- 语言与文本
- 调度中心
- 鼠标
- 网络
- 通知
- 家长控制
- 打印机与扫描仪
- 描述文件
- 安全性与隐私
- 共享
- 声音
- 听写与语音
- 聚焦搜索
- 启动磁盘
- 时间机器
- 触控板
- 艾克斯安

- **应用**
  - **允许使用 Game Center：**允许用户通过 Game Center 玩在线游戏。默认值为“**开**”。

- **允许添加 Game Center 好友：**允许用户向好友发送通知以玩游戏。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 Game Center 帐户：**允许用户修改其 Game Center 帐户设置。默认值为“**开**”。
- **允许 App Store 采用：**允许或限制 App Store 采用 OS X 中预先存在的应用。默认值为“**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网站上的字段。默认值为“**开**”。
- **安装或更新应用时需要管理员密码：**安装或更新应用时需要管理员密码。默认值为“**关**”，这意味着不需要管理员密码。
- **将 App Store 限制为仅软件更新：**将 App Store 限制为仅更新，这将禁用 App Store 中除“更新”之外的所有选项卡。默认值为“**关**”，这意味着允许完全访问 App Store。
- **限制允许打开的应用：**限制或允许用户可以使用的应用。默认值为“关”，这意味着允许使用所有应用。如果启用，请配置以下设置：
  - **允许的应用程序：** 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，在添加应用程序时使用**程序包 ID** 字段中的 ID。对每个允许启动的应用程序重复此步骤。
  - **不允许的文件夹：** 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**。对所有不希望用户访问的文件夹重复此步骤。
  - **允许的文件夹：** 单击**添加**，键入要授予用户访问权限的文件夹的文件路径，然后单击**保存**。对所有希望用户访问的文件夹重复此步骤。

- **小组件**
  - **仅允许运行以下仪表板小组件：** 如果设置为**开**，用户只能运行在此设置中配置的仪表板小组件。默认设置为**关**，这允许用户运行所有小组件。如果启用，请配置以下设置：
    - **允许的小组件：** 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**。对要在仪表板上运行的每个小组件重复此步骤。
- **媒体**
  - **允许隔空投送：** 允许用户与附近的 iOS 设备共享照片、视频、网站、位置等。
- **共享**
  - **自动启用新的共享服务：** 选择是否自动启用共享服务。
  - **邮件：** 选择是否允许共享邮箱。

- **Facebook：** 选择是否允许共享 Facebook 帐户。
- **视频服务 - Flickr、Vimeo、土豆和优酷：** 选择是否允许共享视频服务。
- **添加到 Aperture：** 选择是否允许共享添加到 Aperture 的功能。
- **新浪微博：** 选择是否允许共享新浪微博帐户。
- **Twitter:** 选择是否允许共享 Twitter 帐户。
- **消息:** 选择是否允许共享消息访问权限。
- **添加到 iPhoto:** 选择是否允许共享添加到 iPhoto 的功能。
- **添加到阅读列表:** 选择是否允许共享添加到阅读列表的功能。
- **隔空投送:** 选择是否允许共享隔空投送帐户。

- **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**关闭**，这意味着用户可以更改桌面图片。
  - **允许使用摄像头:** 选择用户是否可以在其 Mac 上使用摄像头。默认值为**关闭**，这意味着用户无法使用摄像头。
  - **允许 Apple Music:** 允许用户使用 Apple Music 服务 (macOS 10.12 及更高版本)。如果您不允许 Apple Music 服务，则“音乐”应用将以经典模式运行。仅适用于受监督的设备。默认为**开启**。
  - **允许 Spotlight 建议:** 选择用户是否可以使用 Spotlight 建议来搜索其 Mac，并从互联网和 App Store 提供 Spotlight 建议。默认值为**关闭**，这会阻止用户使用 Spotlight 建议。
  - **允许查询:** 选择用户是否可以使用上下文菜单或 Spotlight 搜索菜单查询单词定义。默认值为 Off，这会阻止用户在其 Mac 上使用查询功能。
  - **允许本地帐户使用 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在其 Mac 上的*所有*登录屏幕上仅使用一个 ID 和密码。默认值为**开启**，这允许用户使用其 Apple ID 和 iCloud 密码访问其 Mac。
  - **允许 iCloud 文档和数据:** 选择是否允许用户在其 Mac 上访问存储在 iCloud 中的文档和数据。默认值为**开启**，这会阻止用户在其 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) 默认已选中。
  - **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**开启**。
  - **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**”。

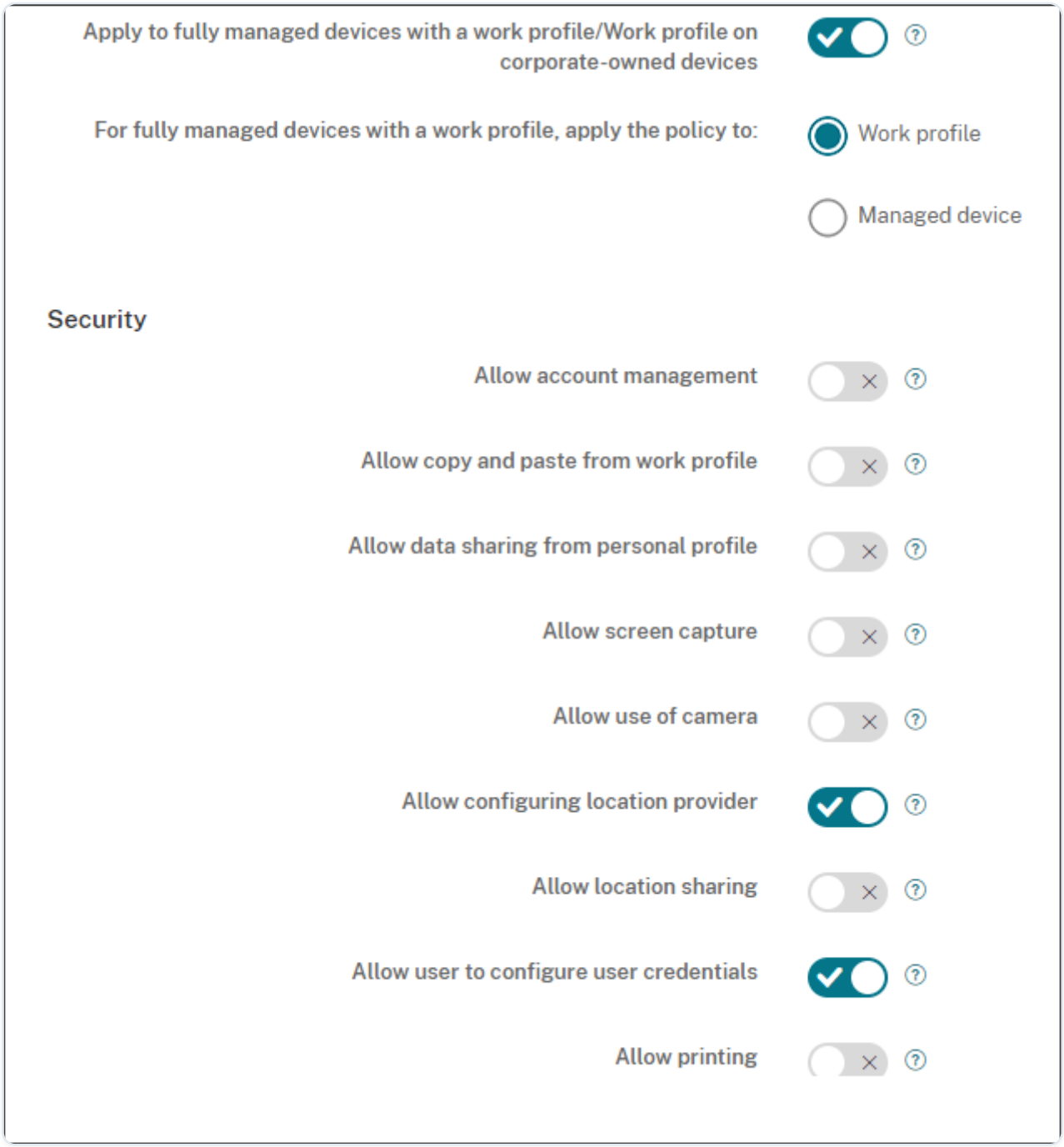
- **允许 iCloud 通讯录：** 允许用户使用 iCloud 通讯录 (macOS 10.12 及更高版本)。默认值为“**开**”。
- **允许 iCloud 日历：** 允许用户使用 iCloud 日历 (macOS 10.12 及更高版本)。默认值为“**开**”。
- **允许 iCloud 提醒事项：** 允许用户使用 iCloud 提醒事项 (macOS 10.12 及更高版本)。默认值为“**开**”。
- **允许 iCloud 书签：** 允许用户与 iCloud 书签同步 (macOS 10.12 及更高版本)。默认值为“**开**”。
- **允许 iCloud 备忘录：** 允许用户使用云备忘录 (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**”，则任何未从 iCloud 照片图库完全下载的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：** 有关此选项和 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**”。
- **允许触控 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：** 如果设置为“**开**”，此设置将延迟用户看到软件更新的时间。用户在软件更新发布日期后的指定天数内不会看到软件更新。默认值为“**关**”。仅适用于运行 macOS 10.13.4 及更高版本的受监督设备。操作系统更新策略具有更多设置，用于控制设备接收更新的频率。请参阅 (/zh-cn/citrix-endpoint-management/policies/control-os-updates.html)。
- **强制软件更新延迟（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，用户的设备不会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，用户无法使用“隔空投送密码”功能共享其密码。默认值为“**开**”。(macOS 10.14 及更高版本)
- **图像游乐场：** 如果设置为“**关**”，则禁止使用图像生成。默认值为“**开**”。仅适用于运行 macOS 15 及更高版本的受监督设备。
- **iPhone 镜像：** 如果设置为 **禁用**，则禁止使用 iPhone 镜像。在 macOS 上使用时，这会阻止 Mac 镜像任何 iPhone。默认值为 **启用**。仅适用于运行 macOS 15 及更高版本的受监管设备。
- **写作工具：** 如果设置为 **禁用**，则禁用 Apple Intelligence 写作工具。默认值为 **启用**。仅适用于运行 macOS 15 及更高版本的受监管设备。

- **允许修改媒体共享：** 如果设置为 **禁用**，则阻止修改媒体共享设置。默认值为 **启用**。适用于 macOS 15.1 及更高版本。

Android 设置

- **摄像头：** 允许用户在其设备上使用摄像头。如果设置为 **禁用**，则摄像头将被禁用。默认值为 **启用**。

安卓企业版设置



当新的或恢复出厂设置的 Android 设备以工作配置文件模式注册时，运行 Android 9.0-10.x 的设备将注册为具有工作配置文件的完全托管设备。运行 Android 11+ 的设备将注册为公司自有设备上的工作配置文件。限制策略可以应用于设备上的工作配置文件或托管设备。

在以公司自有设备上的工作配置文件模式注册的设备上，以下限制不起作用：

- 允许备份服务
- 启用系统应用
- 防止键盘锁锁定设备
- 允许使用状态栏
- 保持设备屏幕常亮
- 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 NFC
- 允许添加用户

默认情况下，当设备以工作配置文件模式注册到 Android Enterprise 时，设备上的 **USB 调试和未知来源**设置处于禁用状态。

观看此视频了解更多信息：



- **应用于具有工作资料的完全托管设备/公司拥有设备上的工作资料：** 允许为具有工作资料的完全托管设备配置限制策略设置。这些设备也称为 COPE（公司拥有个人启用）设备。当此设置为“**开**”时，请选择以下设置之一：

- **工作资料：** 您配置的限制设置仅适用于设备上的工作资料。
- **托管设备：** 您配置的限制设置仅适用于设备。

当此设置为“**关**”时，您配置的凭据设置将应用于设备，但明确适用于工作资料的设置除外。默认值为“**关**”。

当“**应用于具有工作资料的完全托管设备/公司拥有设备上的工作资料**”为“关”时，请配置以下设置：

- **安全性**
  - **允许帐户管理：** 允许将帐户添加到工作资料和托管设备中。默认值为“**关**”。
  - **允许从工作资料复制和粘贴：** 如果为“**开**”，用户可以将数据从工作资料中的应用程序复制并粘贴到个人资料中的应用程序。默认值为“**关**”。
  - **允许从个人资料共享数据：** 如果为“**开**”，用户可以将文件和数据从个人资料中的应用程序复制、粘贴和共享到工作资料中的应用程序。默认值为“**关**”。
  - **允许屏幕捕获：** 允许用户录制或截取设备屏幕。默认值为“**关**”。
  - **允许使用摄像头：** 允许用户使用设备摄像头拍照和录制视频。默认值为“**关**”。
  - **允许 VPN 配置：** 允许用户创建 VPN 配置。适用于运行 Android 6 及更高版本的工作资料设备和完全托管设备。默认值为“**开**”。
  - **允许备份服务：** 允许用户备份其设备上的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、视频或其他内容从其设备发送到另一台设备。适用于 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开启 GPS。适用于 Android API 28 及更高版本。默认值为“**开**”。
  - **允许位置共享：** 对于托管资料，设备所有者可以覆盖此设置。默认值为“**关**”。

> **提示：**
>
> 您可以在 Citrix Endpoint Management 中创建位置设备策略以强制执行地理边界。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：** 如果设置为“**开**”，则此设置允许用户打印到可从用户设备访问的任何打印机。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**”。

- **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。默认值为“**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**”。
    - **系统应用程序列表：** 您要在设备上启用的系统应用程序列表。将“**启用系统应用程序**”设置为“**开**”并添加应用程序包名称。要查找系统应用程序的包名称，可以使用 Android 调试桥 (`adb`) 调用 Android 包管理器 (`pm`) 命令。例如，`adb shell "pm list packages -f name"`，其中“name”是包名称的一部分。有关详细信息，请参阅 `<https://developer.android.com/studio/command-line/adb>`。对于 Android Enterprise 设备，您可以使用Android Enterprise 应用程序权限 策略限制应用程序权限。
  - **禁用应用程序：** 阻止指定列表中的应用程序在设备上运行。默认值为“**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：** 您要阻止的应用程序列表。将“**禁用应用程序**”设置为“**开**”并添加应用程序。键入应用程序包名称。更改和部署应用程序列表会覆盖先前的应用程序列表。例如：如果您禁用 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，则 Citrix Endpoint Management 将启用 com.example.2。
  - **凭据管理器应用程序：** 控制应用程序是否可以充当凭据提供程序。默认值为“**关**”。如果此设置为“**开**”，用户可以选择包策略类型，然后在“**凭据提供程序应用程序列表**”表中单击“**添加**”以按包名称添加应用程序。此功能适用于 Android 14 及更高版本，并且需要 Secure Hub 26.5.0 或更高版本。
    - **包策略类型：** 指定允许或阻止哪些凭据提供程序。默认选项是“**允许列表和系统包**”，它允许访问 OEM 默认凭据提供程序和凭据提供程序的允许列表。其他选项包括“**仅允许列表**”，它将用户可以使用的凭据提供程序限制为策略中的包；以及“**阻止列表**”，它阻止用户使用策略中列出的凭据提供程序。
    - **凭据提供程序应用程序列表：** 要根据包策略类型允许或阻止应用程序作为凭据提供程序，请单击“**添加**”，键入应用程序包名称，然后单击“**保存**”。对要添加的每个应用程序重复此操作。
  - **启用应用程序验证：** 启用操作系统扫描应用程序以检测恶意行为。默认值为“**开**”。
  - **启用 Google 应用程序：** 允许用户从 Google 移动服务下载应用程序到设备。默认值为“**开**”。
  - **允许非 Google Play 应用程序：** 允许从 Google Play 以外的商店安装应用程序。默认值为“**关**”。

- **允许所有配置文件使用非 Google Play 应用：** 如果设置为“**开**”，用户可以在设备上的所有配置文件中安装来自 Google Play 以外商店的应用。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、禁用应用、清除缓存和数据、强制停止任何应用以及清除默认设置。用户可以通过“设置”应用执行这些操作。默认设置为“**关**”。
- **允许应用卸载：** 允许用户从托管的 Google Play 商店中卸载应用。默认设置为“**关**”。

- **BYOD 工作配置文件**
  - **启用连接的应用：** 如果启用，用户可以选择可以在工作和个人配置文件之间通信的应用，同时使用工作和个人数据。启用后，单击“**添加**”，选择所需应用，然后单击“**保存**”。启用此功能需要工作配置文件。默认设置为“**关**”。
  - **允许工作配置文件应用小组件显示在主屏幕上：** 如果此设置为“**开**”，用户可以将工作配置文件应用小组件放置在设备主屏幕上。如果此设置为“**关**”，用户无法将工作配置文件应用小组件放置在设备主屏幕上。默认设置为“**关**”。
    - **允许使用小组件的应用：** 您希望在主屏幕上允许的应用列表。将“**允许工作配置文件应用小组件显示在主屏幕上**”设置为“**开**”并添加应用。单击“**添加**”并从列表中选择一个您希望在主屏幕上允许其小组件的应用。单击“**保存**”。重复此过程以允许更多应用小组件。
  - **允许设备联系人中包含工作配置文件联系人：** 在父配置文件中显示来自托管 Android Enterprise 配置文件的联系人，用于来电（Android 7.0 及更高版本）。默认设置为“**关**”。

- **仅限完全托管设备**
  - **允许添加用户：** 允许用户在设备上添加新用户。默认设置为“**开**”。
  - **允许数据漫游：** 允许用户在漫游时使用蜂窝数据。默认设置为“关”，这将禁用用户设备上的漫游。默认设置为“**关**”。
  - **允许短信：** 允许用户发送和接收短信。默认设置为“**关**”。
  - **允许使用状态栏：** 如果设置为“**开**”，此设置将在托管设备和专用设备（也称为 COSU 设备）上启用状态栏。此设置会禁用通知、快速设置以及其他允许从全屏模式退出的屏幕叠加层。用户可以进入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。默认设置为“**开**”。
    - **允许蓝牙共享：** 如果未选中，用户无法在其设备上建立传出蓝牙共享。默认设置为选中。
  - **允许配置日期和时间：** 允许用户更改其设备上的日期和时间。默认值为 **开**。
  - **允许恢复出厂设置：** 允许用户对其设备执行恢复出厂设置。默认值为 **开**。

- **保持设备屏幕常亮：** 如果此设置设为 **开**，则设备插入电源时屏幕将保持常亮。默认值为 **关**。
- **允许 USB 大容量存储：** 允许通过 USB 连接在用户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：** 允许用户使用其设备上的麦克风。默认值为 **开**。
- **允许网络共享：** 允许用户配置便携式热点和共享数据。默认值为 **关**。
- **防止键盘锁锁定设备：** 如果设为 **开**，此设置将禁用托管设备和专用设备（也称为 COSU 设备）锁定屏幕上的键盘锁。默认值为 **关**。
- **允许更改 Wi-Fi：** 如果设为 **开**，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。默认值为 **关**。

- **三星**
  - **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 密钥对和证书将路由到默认密钥库提供程序进行存储。默认值为 **关**。
  - **允许共享列表：** 允许用户在“共享方式”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：** 启用事件审核日志的创建，以便对设备进行取证分析。默认值为 **关**。
- **三星：仅限完全托管设备**
  - **仅允许紧急呼叫：** 允许用户在其设备上启用“仅限紧急呼叫”模式。默认值为 **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：** 仅允许加密已使用的内存空间。此加密与加密所有数据的全盘加密不同。这些数据包括设置、应用程序数据、下载的文件和应用程序、媒体以及其他文件。默认值为“**开**”。
  - **启用通用标准模式：** 将设备置于通用标准模式。通用标准配置强制执行严格的安全流程。默认值为“**开**”。
  - **启用重启横幅：** 当用户设备重新启动时，显示经 DoD 批准的系统使用通知消息或横幅。默认值为“**关**”。
  - **允许更改设置：** 允许用户在其完全托管的设备上更改设置。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。适用于完全托管的设备。默认值为“**开**”。
  - **允许剪贴板：** 允许用户将数据复制到其设备上的剪贴板。

- **允许剪贴板共享：** 允许用户在其设备和计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。

- **允许主页键：** 允许用户在其完全托管的设备上使用“**主页**”键。默认值为“**开**”。
- **允许模拟位置：** 允许用户伪造其 GPS 位置。适用于完全托管的设备。默认值为“**关**”。
- **NFC：** 允许用户在其完全托管的设备上使用 NFC（MDM 3.0 及更高版本）。默认值为“**开**”。
- **允许关机：** 允许用户关闭其完全托管的设备（MDM 3.0 及更高版本）。默认值为“**开**”。
- **允许 Wi-Fi 直连：** 允许用户通过其 Wi-Fi 连接直接连接到另一台设备。默认值为“**开**”。如果为“**开**”，则必须启用“**允许 Wi-Fi 更改**”设置。
- **允许 SD 卡：** 允许用户在其设备上使用 SD 卡（如果可用）。默认值为“**开**”。
- **允许 USB 主机存储：** 当 USB 设备连接到用户的设备时，允许用户的设备充当 USB 主机。然后，用户的设备会向 USB 设备供电。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 Beam：** 允许用户使用 NFC 和 Wi-Fi Direct 与他人共享内容（MDM 4.0 及更高版本）。默认值为“**开**”。
- **允许 S Voice：** 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 共享网络：** 允许用户使用其 USB 连接与其他设备共享移动数据连接。默认值为“**关**”。如果设置为“**开**”，则“**允许共享网络**”设置也必须为“**开**”。
- **允许蓝牙共享网络：** 允许用户使用其蓝牙连接与其他设备共享移动数据连接。默认值为“**关**”。如果设置为“**开**”，则“**允许共享网络**”设置也必须为“**开**”。

  - **允许蓝牙共享：** 如果未选择，用户无法在其设备上建立出站蓝牙共享。默认值为选中。

- **允许 Wi-Fi 共享网络：** 允许用户使用其 Wi-Fi 连接与其他设备共享移动数据连接。默认值为“**关**”。如果设置为“**开**”，则“**允许共享网络**”设置也必须为“**开**”。
- **允许接收 MMS：** 允许用户接收 MMS 消息。默认值为“**关**”。如果设置为“**开**”，则必须启用“**允许 SMS**”设置。
- **允许发送 MMS：** 允许用户发送 MMS 消息。默认值为“**关**”。如果设置为“**开**”，则必须启用“**允许 SMS**”设置。
- **允许接收 SMS：** 允许用户接收 SMS 消息。默认值为“**关**”。如果设置为“**开**”，则必须启用“**允许 SMS**”设置。

- **允许发送 SMS：** 允许用户发送 SMS 消息。默认值为“**关**”。如果设置为“**开**”，则必须启用“**允许 SMS**”设置。
- **配置移动网络：** 允许用户使用其蜂窝数据连接。默认值为“**关**”。
- **每日限制 (MB)：** 输入用户每天可使用的移动数据量（MB）。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- **每周限制 (MB)：** 输入用户每周可使用的移动数据量（MB）。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- **每月限制 (MB)：** 输入用户每月可使用的移动数据量（MB）。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 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**”。
- **允许录制音频：** 允许用户使用其设备录制音频 (MDM 4.0 及更高版本)。默认值为“**开**”。如果为“**开**”，则必须启用“**允许麦克风**”设置。
- **允许录制视频：** 允许用户使用其设备录制视频 (MDM 4.0 及更高版本)。默认值为“**关**”。如果为“**开**”，则必须启用“**允许使用摄像头**”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。默认值为“**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。默认值为“**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。默认值为“**关**”。如果为“**开**”，则必须启用“**允许数据漫游**”设置。

当“**应用于具有工作资料的完全托管设备/公司拥有设备上的工作资料**”为“开”且“**对于具有工作资料的完全托管设备，将策略应用于**”设置为“**工作资料**”时，请配置以下设置：

- **安全性**
  - **允许帐户管理：** 允许将帐户添加到工作资料和托管设备中。默认值为“**关**”。
  - **允许跨配置文件复制和粘贴：** 如果为“**开**”，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程序之间复制和粘贴。默认值为“**关**”。
  - **允许屏幕捕获：** 允许用户录制或截取设备屏幕。默认值为“**关**”。
  - **允许使用摄像头：** 允许用户使用设备摄像头拍照和录制视频。默认值为“**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。默认值为“**关**”。

> **提示：**
>
> 您可以在 Citrix Endpoint Management 中创建位置设备策略以强制执行地理边界。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：** 如果设置为“**开**”，则此设置允许用户打印到可从用户设备访问的任何打印机。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。默认值为“**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**”。
    - **系统应用程序列表：** 要在设备上启用的系统应用程序列表。将“**启用系统应用程序**”设置为“**开**”并添加应用程序包名称。要查找系统应用程序的包名称，可以使用 Android 调试桥 (`adb`) 调用 Android 包管理器 (`pm`) 命令。例如，`adb shell "pm list packages -f name"`，其中“name”是包名称的一部分。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：** 阻止指定应用程序列表在设备上运行。默认值为“**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：** 要阻止的应用程序列表。将“**禁用应用程序**”设置为“**开**”并添加应用程序。键入应用程序包名称。更改和部署应用程序列表会覆盖之前的应用程序列表。例如：如果禁用 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，Citrix Endpoint Management 将启用 com.example.2。
  - **凭据管理器应用程序：** 控制应用程序是否可以充当凭据提供程序。默认值为“**关**”。如果此设置为“**开**”，用户可以选择包策略类型，然后在“**凭据提供程序应用程序列表**”表中单击“**添加**”以按包名称添加应用程序。此功能适用于 Android 14 及更高版本，并且需要 Secure Hub 26.5.0 或更高版本。
    - **包策略类型：** 指定允许或阻止哪些凭据提供程序。默认选项是“**允许列表和系统包**”，它允许从 OEM 默认凭据提供程序和凭据提供程序的允许列表进行访问。其他选项包括“**仅允许列表**”，它将用户可以使用的凭据提供程序限制为策略中的包；以及“**阻止列表**”，它阻止用户使用策略中列出的凭据提供程序。

    - **凭据提供程序应用程序列表：** 要根据包策略类型允许或阻止应用程序作为凭据提供程序，请单击“**添加**”，键入应用程序包名称，然后单击“**保存**”。对要添加的每个应用程序重复此操作。

  - **启用应用程序验证：** 启用操作系统扫描应用程序以检测恶意行为。默认值为“**开**”。
  - **启用 Google 应用程序：** 允许用户从 Google 移动服务下载应用程序到设备。默认值为“**开**”。
  - **允许非 Google Play 应用程序：** 允许从 Google Play 以外的商店安装应用程序。默认值为“**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。用户通过“设置”应用程序执行这些操作。默认值为“**关**”。
  - **允许应用程序卸载：** 允许用户从托管 Google Play 商店中卸载应用程序。默认值为“**关**”。

- **BYOD 工作配置文件**

  - **允许工作配置文件应用小组件在主屏幕上显示：** 如果此设置为“**开**”，用户可以将工作配置文件应用小组件放置在设备主屏幕上。如果此设置为“**关**”，用户无法将工作配置文件应用小组件放置在设备主屏幕上。默认值为“**关**”。

    - **允许使用小组件的应用：** 您希望在主屏幕上允许的应用列表。将“**允许工作配置文件应用小组件在主屏幕上显示**”设置为“**开**”并添加应用。单击“**添加**”并从列表中选择一个您希望在主屏幕上允许其小组件的应用。单击“**保存**”。重复此过程以允许更多应用小组件。

  - **允许设备联系人中显示工作配置文件联系人：** 在父配置文件中显示来自托管 Android Enterprise 配置文件的联系人，用于来电（Android 7.0 及更高版本）。默认值为“**关**”。

- **三星**

  - **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 密钥对和证书将路由到默认密钥存储提供程序进行存储。默认值为“**关**”。
  - **允许共享列表：** 允许用户在“通过共享”列表中在应用之间共享内容。默认值为“**开**”。
  - **启用审计日志：** 启用事件审计日志的创建，用于设备的取证分析。默认值为“**关**”。

当“**应用于具有工作配置文件的完全托管设备/公司拥有的设备上的工作配置文件**”为“开”且“**对于具有工作配置文件的完全托管设备，将策略应用于**”设置为“**托管设备**”时，请配置以下设置：

- **安全性**

  - **允许帐户管理：** 允许将帐户添加到工作配置文件和托管设备中。默认值为“**关**”。

- **允许跨配置文件复制和粘贴：** 如果为“**开**”，用户可以在 Android Enterprise 配置文件中的应用与个人区域中的应用之间进行复制和粘贴。默认值为“**关**”。
- **允许屏幕截图：** 允许用户录制或截取设备屏幕。默认值为“**关**”。
- **允许使用相机：** 允许用户使用设备相机拍照和录制视频。默认值为“**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和完全托管设备。默认值为“**开**”。
- **允许备份服务：** 允许用户备份其设备上的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、视频或其他内容从其设备发送到另一设备。适用于 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。默认值为“**关**”。

> **提示：**
>
> 您可以在 Citrix Endpoint Management 中创建位置设备策略以强制执行地理边界。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：** 如果设置为“**开**”，则此设置允许用户打印到可从用户设备访问的任何打印机。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**”。

- **应用程序**
  - **启用系统应用程序：** 允许用户运行预装的设备应用程序。默认值为“**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**”。
    - **系统应用程序列表：** 您要在设备上启用的系统应用程序列表。将“**启用系统应用程序**”设置为“**开**”并添加应用程序包名称。要查找系统应用程序的包名称，您可以使用 Android 调试桥 (`adb`) 调用 Android 包管理器 (`pm`) 命令。例如，`adb shell "pm list packages -f name"`，其中“name”是包名称的一部分。有关详细信息，请参阅 `<https://developer.android.com/studio/command-line/adb>`。对于 Android Enterprise 设备，您可以使用Android Enterprise 应用程序权限 策略来限制应用程序权限。

- **禁用应用程序：** 阻止指定列表中的应用程序在设备上运行。默认值为“**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：** 您要阻止的应用程序列表。将“**禁用应用程序**”设置为“**开**”并添加应用程序。键入应用程序包名称。更改和部署应用程序列表会覆盖先前的应用程序列表。例如：如果您禁用 com.example1 和 com.example2，然后稍后将列表更改为 com.example1 和 com.example3，则 Citrix Endpoint Management 会启用 com.example.2。
- **启用应用程序验证：** 使操作系统能够扫描应用程序以检测恶意行为。默认值为“**开**”。
- **启用 Google 应用程序：** 允许用户从 Google 移动服务下载应用程序到设备。默认值为“**开**”。
- **允许非 Google Play 应用程序：** 允许安装来自 Google Play 以外商店的应用程序。默认值为“**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**”。

- **仅限完全托管设备**
  - **允许添加用户**：允许用户在设备上添加新用户。默认设置为“**开**”。
  - **允许数据漫游**：允许用户在漫游时使用蜂窝数据。默认设置为“关”，这会禁用用户设备上的漫游。默认设置为“**关**”。
  - **允许短信**：允许用户发送和接收短信。默认设置为“**关**”。
  - **允许使用状态栏**：如果设置为“**开**”，此设置将在托管设备和专用设备（也称为 COSU 设备）上启用状态栏。此设置会禁用通知、快速设置以及其他允许从全屏模式退出的屏幕叠加层。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。默认设置为“**开**”。
    - **允许蓝牙共享**：如果未选中，用户无法在其设备上建立出站蓝牙共享。默认设置为选中。
  - **允许配置日期和时间**：允许用户更改其设备上的日期和时间。默认设置为“**开**”。
  - **允许恢复出厂设置**：允许用户对其设备执行恢复出厂设置。默认设置为“**开**”。

- **允许恢复出厂设置保护**：如果设置为“**开**”，当设备使用恢复模式重置时，用户必须提供重置前设备上存在的帐户凭据。如果重置前设置了设备锁定，他们也可以提供设备锁定。如果设置为“**关**”，重置后不需要身份验证。默认设置为“**开**”。
- **保持设备屏幕常亮**：如果此设置设置为“**开**”，则设备插入电源时屏幕将保持常亮。默认设置为“**关**”。
- **允许 USB 大容量存储**：允许通过 USB 连接在用户设备和计算机之间传输大型数据文件。默认设置为“**开**”。
- **允许麦克风**：允许用户在其设备上使用麦克风。默认设置为“**开**”。
- **允许网络共享**：允许用户配置便携式热点和共享数据。默认设置为“**关**”。当此设置打开时，以下设置适用于三星设备：
- **防止键盘锁锁定设备：如果设置为开**，此设置将禁用托管设备和专用设备（也称为 COSU 设备）锁定屏幕上的键盘锁。默认设置为**关**。
- **允许更改 Wi-Fi：如果设置为开**，用户可以打开或关闭 Wi-Fi 并连接到 Wi-Fi 网络。默认设置为**开**。
- **允许文件传输：允许通过 USB 进行文件传输。默认设置为关**。

- **三星**
  - **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 密钥对和证书将路由到默认密钥存储提供程序进行存储。默认设置为关**。
  - **允许共享列表：允许用户在“通过共享”列表中在应用程序之间共享内容。默认设置为开**。
  - **启用审核日志：启用事件审核日志的创建，用于设备的取证分析。默认设置为关**。
- **三星：仅限完全托管设备**
  - **仅允许紧急呼叫：允许用户在其设备上启用仅限紧急呼叫模式。默认设置为关**。
  - **允许固件恢复 ：允许用户恢复其设备上的固件。默认设置为开**。
  - **允许快速加密：仅允许加密已使用的内存空间。此加密与完全磁盘加密（加密所有数据）形成对比。这些数据包括设置、应用程序数据、下载的文件和应用程序、媒体以及其他文件。默认设置为开**。
  - **启用通用标准模式：将设备置于通用标准模式。通用标准配置强制执行严格的安全流程。默认设置为开**。
  - **启用重启横幅：当用户设备重启时，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：允许用户更改其完全托管设备上的设置。默认设置为开**。

- **启用后台数据使用：允许应用程序在后台同步数据。适用于完全托管设备。默认设置为开。**
- **允许剪贴板**：允许用户在其设备上将数据复制到剪贴板。默认设置为“**开**”。
  - **允许剪贴板共享**：允许用户在其设备和计算机之间共享剪贴板内容 (MDM 4.0 及更高版本)。
- **允许主页键**：允许用户在其完全托管的设备上使用“**主页**”键。默认设置为“**开**”。
- **允许模拟位置**：允许用户伪造其 GPS 位置。适用于完全托管的设备。默认设置为“**关**”。
- **NFC**：允许用户在其完全托管的设备上使用 NFC (MDM 3.0 及更高版本)。默认设置为“**开**”。
- **允许关机**：允许用户关闭其完全托管的设备 (MDM 3.0 及更高版本)。默认设置为“**开**”。
- **允许 Wi-Fi 直连**：允许用户通过其 Wi-Fi 连接直接连接到另一台设备。默认设置为“**开**”。如果设置为“**开**”，则必须启用“**允许 Wi-Fi 更改**”设置。
- **允许 SD 卡**：允许用户在其设备上使用 SD 卡（如果可用）。默认设置为“**开**”。
- **允许 USB 主机存储**：允许用户的设备在 USB 设备连接到其设备时充当 USB 主机。然后，用户的设备会向 USB 设备供电。默认设置为“**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)。默认设置为“**开**”。
- **允许 S Beam**：允许用户使用 NFC 和 Wi-Fi Direct 与他人共享内容 (MDM 4.0 及更高版本)。默认设置为“**开**”。
- **允许 S Voice**：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)。默认设置为“**开**”。
- **允许 USB 网络共享**：允许用户使用其 USB 连接与其他设备共享移动数据连接。默认设置为“**关**”。如果设置为“**开**”，则“**允许网络共享**”设置也必须设置为“**开**”。
- **允许蓝牙网络共享**：允许用户使用其蓝牙连接与其他设备共享移动数据连接。默认设置为“**关**”。如果设置为“**开**”，则“**允许网络共享**”设置也必须设置为“**开**”。
- **允许 Wi-Fi 网络共享**：允许用户使用其 Wi-Fi 连接与其他设备共享移动数据连接。默认设置为“**关**”。如果设置为“**开**”，则“**允许网络共享**”设置也必须设置为“**开**”。
- **允许接收彩信：** 允许用户接收彩信消息。默认值为“**关闭**”。如果为“**开启**”，则必须开启“**允许短信**”设置。
- **允许发送彩信：** 允许用户发送彩信消息。默认值为“**关闭**”。如果为“**开启**”，则必须开启“**允许短信**”设置。
- **允许接收短信：** 允许用户接收短信消息。默认值为“**关闭**”。如果为“**开启**”，则必须开启“**允许短信**”设置。

- **允许发送短信：** 允许用户发送短信消息。默认值为“**关闭**”。如果为“**开启**”，则必须开启“**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。默认值为“**关闭**”。
- **按天限制 (MB)：** 输入用户每天可使用的移动数据量（MB）。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)：** 输入用户每周可使用的移动数据量（MB）。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)：** 输入用户每月可使用的移动数据量（MB）。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 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“**开启**”。
- **允许录音：** 允许用户使用其设备录制音频 (MDM 4.0 及更高版本)。默认值为“**开启**”。如果为“**开启**”，则必须开启“**允许麦克风**”设置。
- **允许录像：** 允许用户使用其设备录制视频 (MDM 4.0 及更高版本)。默认值为“**关闭**”。如果为“**开启**”，则必须开启“**允许使用摄像头**”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。默认值为“**关闭**”。如果为“**开启**”，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。默认值为“**关闭**”。如果为“**开启**”，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。默认值为“**关闭**”。如果为“**开启**”，则必须启用“**允许数据漫游**”设置。

Windows 桌面或平板电脑设置

设备策略配置屏幕(/en-us/citrix-endpoint-management/media/device-policy-restrictions-winphone.png)

- **Wi-Fi 设置**
  - **允许 Internet 共享：** 允许设备通过将其转换为 Wi-Fi 热点来与其他设备共享其 Internet 连接。
- **连接**
  - **允许蓝牙：** 允许设备通过蓝牙连接。
  - **允许通过蜂窝网络使用 VPN：** 允许设备通过 VPN 连接到蜂窝网络。
  - **允许在漫游时通过蜂窝网络使用 VPN：** 允许设备在蜂窝网络漫游时通过 VPN 连接。

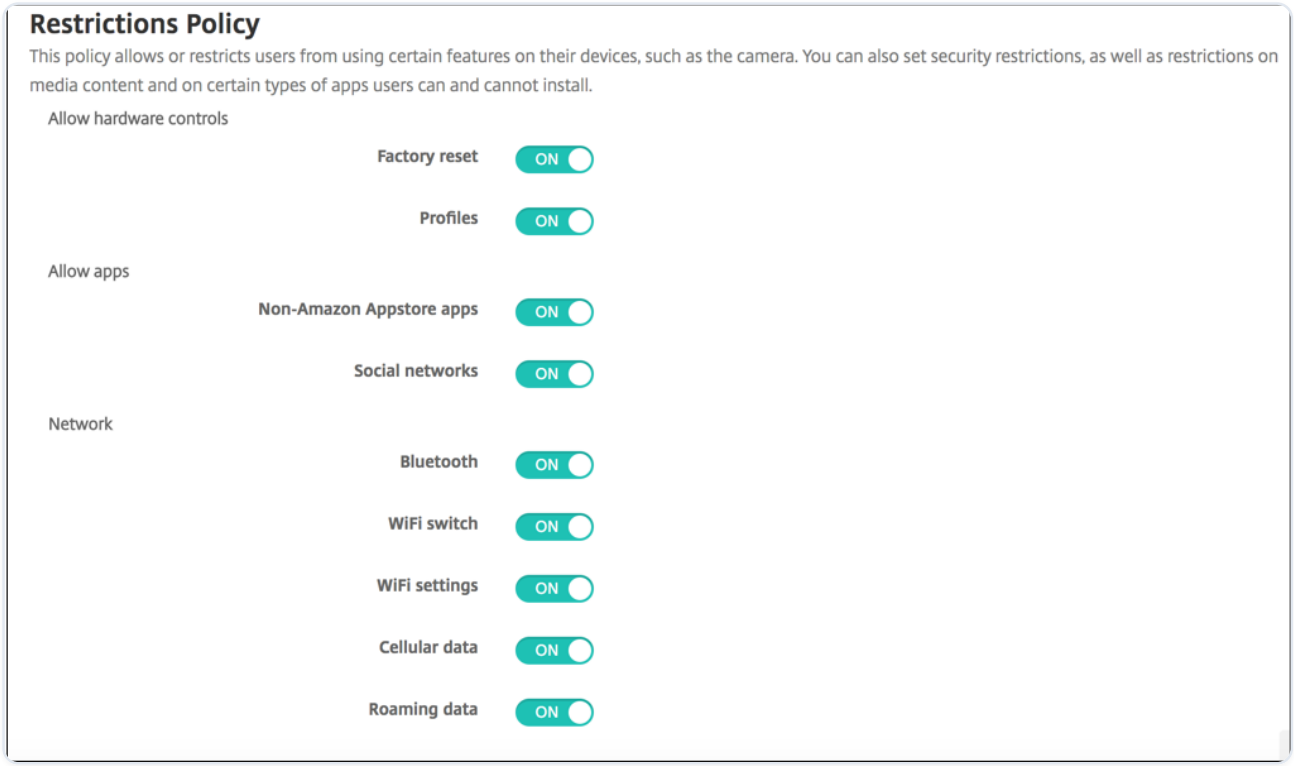
  - **允许蜂窝数据漫游：** 允许用户在漫游时使用蜂窝数据。

- **帐户**
  - **允许 Microsoft 帐户连接：** 允许设备使用 Microsoft 帐户进行非电子邮件相关的连接身份验证和服务。
  - **允许非 Microsoft 电子邮件：** 允许用户添加非 Microsoft 电子邮件帐户。
- **系统**
  - **允许存储卡：** 允许设备使用存储卡。
  - **遥测：** 单击下拉列表中的选项以允许或限制设备发送遥测信息。默认值为 **允许**。其他选项包括 **不允许** 和 **允许，但次要数据请求除外**。
  - **允许应用访问定位服务：** 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。
- **摄像头：** 仅限 Windows 桌面/平板电脑
  - **允许使用摄像头：** 允许用户使用其设备摄像头。
- **蓝牙：** 仅限 Windows 桌面/平板电脑
  - **允许可发现模式：** 允许蓝牙设备发现本地设备。
  - **本地设备名称：** 本地设备的名称。
- **体验：** 仅限 Windows 桌面/平板电脑
  - **允许 Cortana：** 允许用户访问 Cortana，即智能个人助理和知识导航器。
  - **允许设备发现：** 允许网络发现设备。
  - **允许手动 MDM 取消注册：** 允许用户手动将其设备从 Citrix Endpoint Management MDM 中取消注册。
  - **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。
- **锁屏上方：** 仅限 Windows 桌面/平板电脑
  - **允许在锁屏上显示浮动通知：** 允许在锁屏上显示浮动通知。仅限 Windows 桌面/平板电脑
- **应用**
  - **允许应用商店自动更新：** 允许应用商店中的应用自动更新。仅限 Windows 桌面/平板电脑。
- **隐私**：仅限 Windows 桌面/平板电脑

- **允许输入个性化**：允许输入个性化服务运行。输入个性化服务可根据用户输入的内容改进预测性输入，例如笔和触摸键盘。

- **设置**：仅限 Windows 桌面/平板电脑。
  - **允许自动播放**：允许用户更改自动播放设置。
  - **允许数据感知**：允许用户更改数据感知设置。
  - **允许日期时间**：允许用户更改日期和时间设置。
  - **允许语言**：允许用户更改语言设置。
  - **允许电源睡眠**：允许用户更改电源和睡眠设置。
  - **允许区域**：允许用户更改区域设置。
  - **允许登录选项**：允许用户更改登录设置。
  - **允许工作区**：允许用户更改工作区设置。
  - **允许您的帐户**：允许用户更改帐户设置。

Amazon 设置



- **允许硬件控制**
  - **恢复出厂设置：** 允许用户对其设备执行恢复出厂设置。
  - **配置文件：** 允许用户更改其设备上的硬件配置文件。

- **允许应用**
  - **非 Amazon 应用商店应用：** 允许用户在其设备上安装非 Amazon 应用商店应用。
  - **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蜂窝数据。
  - **定位服务：** 允许用户使用 GPS。
- **USB 操作：**
  - **调试：** 允许用户的设备通过 USB 连接到计算机进行调试。

漫游设备策略

您可以在 Citrix Endpoint Management 中添加设备策略，以配置是否允许在受支持的 iOS 设备上进行语音和数据漫游。禁用语音漫游时，数据漫游会自动禁用。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅设备策略。

iOS 设置

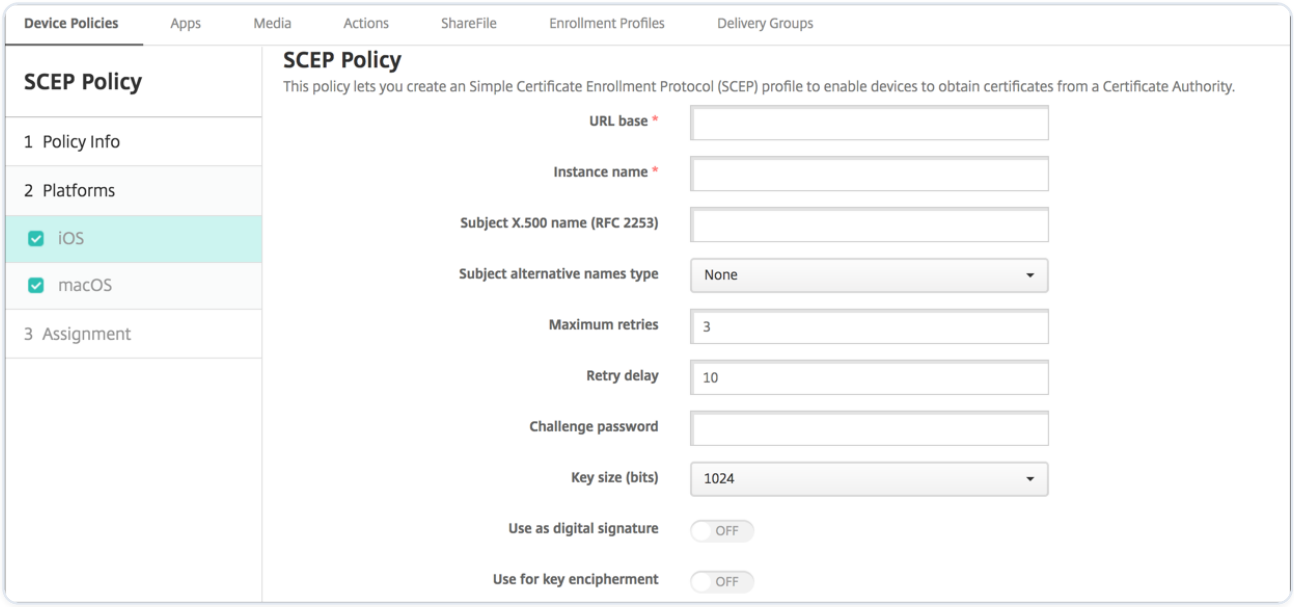
- **禁用语音漫游：** 选择是否禁用语音漫游。启用此选项时，数据漫游会自动禁用。默认值为**关**，表示允许语音漫游。
- **禁用数据漫游：** 选择是否禁用数据漫游。此选项仅在启用语音漫游时可用。默认值为**关**，表示允许数据漫游。

SCEP 设备策略

此策略允许您配置 iOS 和 macOS 设备，以通过简单证书注册协议 (SCEP) 从外部 SCEP 服务器检索证书。要使用 SCEP 从连接到 Citrix Endpoint Management 的 PKI 向设备分发证书，请在分布式模式下创建 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。

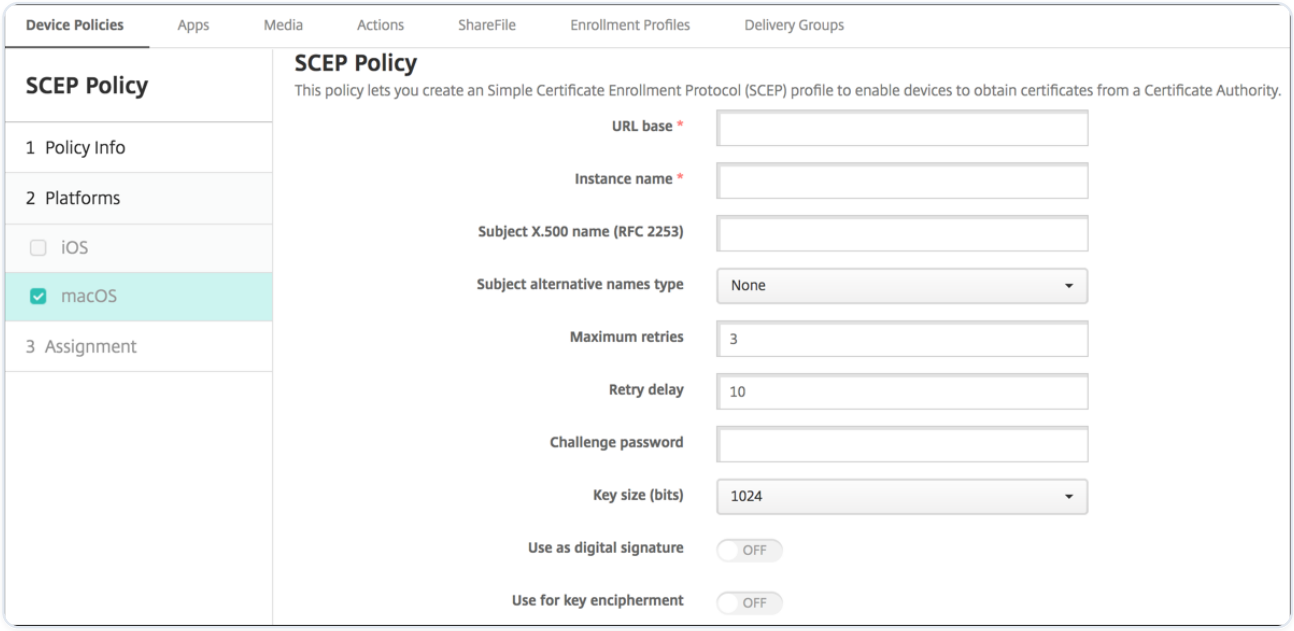
iOS 设置



- **URL 基址：** 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。私钥不会随证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能是安全的。如果一次性密码配置为可重用，请使用 HTTPS 保护密码。此步骤是必需的。
- **实例名称：** 键入 SCEP 服务器可识别的任何字符串。例如，它可以是 example.org 这样的域名。如果 CA 具有多个 CA 证书，则可以使用此字段来区分所需的域。此步骤是必需的。
- **主题 X.500 名称 (RFC 2253)：** 键入 X.500 名称的表示形式，作为对象标识符 (OID) 和值的数组。例如，`/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`，它转换为：`[ [ [“C”, “US”] ], [ [“O”, “Apple Inc.”] ], …, [ [“1.2.5.3”, “bar” ] ] ]`。您可以将 OID 表示为带有点的数字，并使用国家/地区 (C)、地区 (L)、省/市/自治区 (ST)、组织 (O)、组织单位 (OU) 和公用名 (CN) 的快捷方式。
- **主题备用名称类型：** 选择一个备用名称类型。可选的备用名称类型可以提供 CA 颁发证书所需的值。您可以指定**无**、**RFC 822 名称**、**DNS 名称**或 **URI**。
- **最大重试次数：** 键入当 SCEP 服务器发送 PENDING 响应时设备必须重试的次数。默认值为 **3**。
- **重试延迟：** 键入后续重试之间等待的秒数。第一次重试不延迟。默认值为 **10**。
- **质询密码：** 输入预共享密钥。
- **密钥大小（位）：** 选择 **2048** 或更高的密钥大小（位）。
- **用作数字签名：** 选择是否将证书用作数字签名。SCEP 服务器在使用公钥解密哈希之前，会验证证书是否用作数字签名。
- **用于密钥加密：** 选择是否将证书用于密钥加密。服务器首先检查客户端提供的证书是否允许用于密钥加密。然后，服务器使用证书中的公钥来验证数据是否使用私钥加密。如果不是，则操作失败。

- **SHA-256 指纹（十六进制字符串）：** 如果您的 CA 使用 HTTP，请使用此字段提供 CA 证书的指纹。设备使用指纹在注册期间确认 CA 响应的真实性。您可以提供 SHA-256 指纹，也可以选择证书以导入其签名。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

macOS 设置



- **URL 基础：** 键入 SCEP 服务器的地址，以定义 SCEP 请求通过 HTTP 或 HTTPS 发送的位置。私钥不会随证书签名请求 (CSR) 一起发送，因此未加密发送请求可能是安全的。如果一次性密码配置为可重用，请使用 HTTPS 保护密码。此步骤是必需的。
- **实例名称：** 键入 SCEP 服务器可识别的任何字符串。例如，它可以是 example.org 这样的域名。如果 CA 具有多个 CA 证书，则可以使用此字段来区分所需的域。此步骤是必需的。
- **主题 X.500 名称 (RFC 2253)：** 键入 X.500 名称的表示形式，作为对象标识符 (OID) 和值的数组。例如，`/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`，其转换为：`[ [ [“C”, “US”] ], [ [“O”, “Apple Inc.”] ], …, [ [“1.2.5.3”, “bar” ] ] ]`。您可以将 OID 表示为带有点的数字，并使用国家/地区 (C)、地区 (L)、省/市/自治区 (ST)、组织 (O)、组织单位 (OU) 和通用名称 (CN) 的快捷方式。

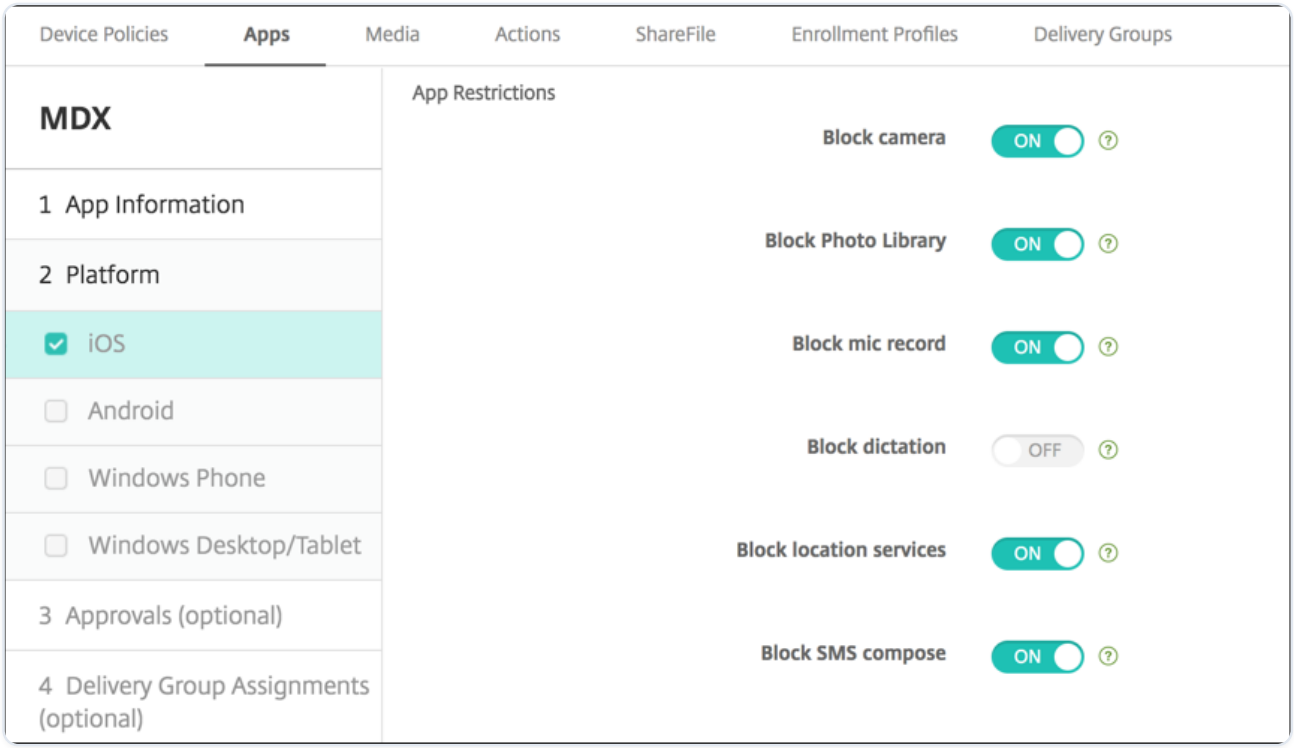
- **主题备用名称类型：** 选择备用名称类型。可选的备用名称类型可以提供 CA 颁发证书所需的值。您可以指定**无**、**RFC 822 名称**、**DNS 名称**或 **URI**。
- **最大重试次数：** 键入当 SCEP 服务器发送 PENDING 响应时设备必须重试的次数。默认值为 **3**。
- **重试延迟：** 键入两次后续重试之间等待的秒数。第一次重试不延迟。默认值为 **10**。
- **质询密码：** 键入预共享密钥。
- **密钥大小（位）：** 选择 **2048** 或更高作为密钥大小（以位为单位）。
- **用作数字签名：** 选择是否将证书用作数字签名。SCEP 服务器在使用公钥解密哈希之前，会验证证书是否用作数字签名。
- **用于密钥加密：** 选择是否将证书用于密钥加密。服务器首先检查客户端提供的证书是否允许用于密钥加密。然后，服务器使用证书中的公钥来验证数据是否使用私钥加密。如果不是，则操作失败。
- **SHA-256 指纹（十六进制字符串）：** 如果您的 CA 使用 HTTP，请使用此字段提供 CA 证书的指纹。设备使用指纹在注册期间确认 CA 响应的真实性。您可以提供 SHA-256 指纹，也可以选择证书以导入其签名。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 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 macOS 10.7 及更高版本。

Siri 和听写策略

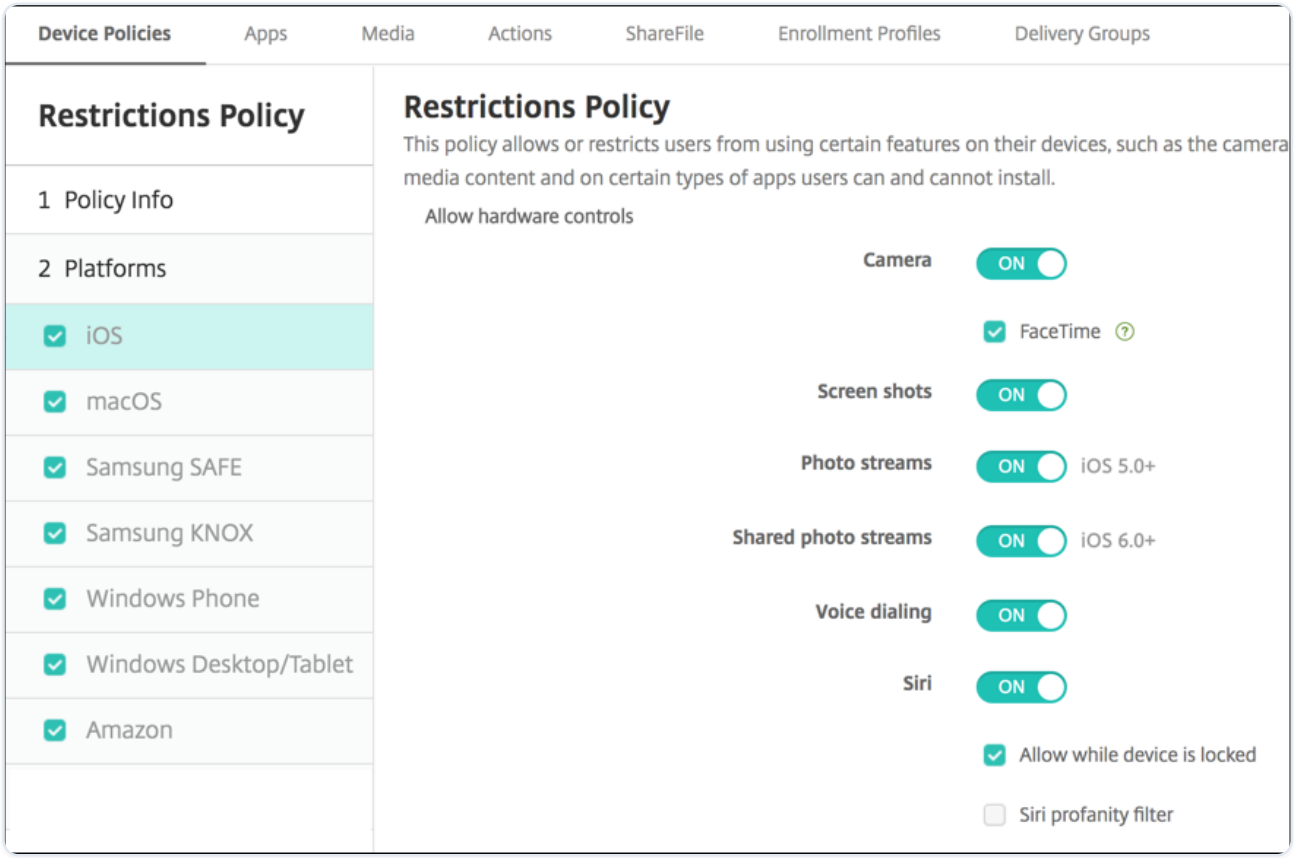
当用户在受管的 iOS 设备上向 Siri 提问或听写文本时，Apple 会收集语音数据以改进 Siri。语音数据会通过 Apple 的云服务，因此存在于安全的 Citrix Endpoint Management 容器之外。但是，听写生成的文本会保留在容器内。

Citrix Endpoint Management 允许您根据安全需求阻止 Siri 和听写服务。

在 MAM 部署中，每个应用的“**阻止听写**”策略默认设置为“**开**”，这会禁用设备的麦克风。如果要允许听写，请将其设置为“**关**”。您可以在 Citrix Endpoint Management 控制台的“**配置 > 应用程序**”中找到此策略。选择应用程序，单击“**编辑**”，然后单击“**iOS**”。



在 MDM 部署中，您还可以通过“**配置 > 设备策略**”中的 Siri 策略禁用 Siri。默认情况下允许使用 Siri。



在决定是否允许 Siri 和听写时，请记住以下几点：

- 根据 Apple 公开的信息，Apple 会将 Siri 和听写语音片段数据保留长达两年。数据会分配一个随机数来代表用户，并且语音文件会与此随机数关联。
- 您可以通过在任何 iOS 设备上转到“**设置 > 通用 > 键盘**”并点击“**启用听写**”下的链接来查看 Apple 隐私策略。

SSO 帐户设备策略

SSO 帐户设备策略允许您在 Citrix Endpoint Management 中创建单点登录 (SSO) 帐户。这些帐户允许用户一次性登录，以从各种应用程序访问 Citrix Endpoint Management 和您的内部公司资源。用户无需在设备上存储任何凭据。SSO 帐户企业用户凭据可用于所有应用程序，包括来自 App Store 的应用程序。此策略旨在与 Kerberos 身份验证后端配合使用。

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

- **帐户名称：**输入显示在用户设备上的 Kerberos SSO 帐户名称。此字段为必填项。
- **Kerberos 主体名称：**输入 Kerberos 主体名称。此字段为必填项。
- **身份凭据（密钥库或 PKI 凭据）：**在下拉列表中单击一个可选的身份凭据，该凭据可用于在无需用户交互的情况下续订 Kerberos 凭据。
- **Kerberos 领域：**输入此策略的 Kerberos 领域。此值通常是您的域名，全部大写（例如，EXAMPLE.COM）。此字段为必填项。
- **允许的 URL：**对于每个需要 SSO 的 URL，单击“**添加**”，然后执行以下操作：
  - **允许的 URL：**输入一个 URL，当用户从 iOS 设备访问该 URL 时，您希望要求 SSO。

    例如，当用户尝试浏览某个站点并且该网站启动 Kerberos 质询时：如果该站点不在 URL 列表中，则 iOS 设备不会通过提供 Kerberos 可能已从之前的 Kerberos 登录缓存到设备上的 Kerberos 令牌来尝试 SSO。匹配必须与 URL 的主机部分完全一致。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，则 URL 仍会回退到标准 HTTP 调用。这可能意味着任何事情，包括标准密码质询或 HTTP 错误（如果 URL 仅配置为使用 Kerberos 进行 SSO）。
  - 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。如果您不添加任何应用程序标识符，则此登录将匹配所有**应用程序标识符。

- **策略设置**
  - **删除策略：** 选择一种安排策略删除的方法。可用选项为“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

应用商店设备策略

您可以在 Citrix 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网络剪辑。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS、安卓 和 Windows 桌面/平板电脑设置

对于您配置的每个平台，请选择应用商店网络剪辑是否显示在用户设备上。默认设置为 **开**。

订阅日历设备策略

您可以在 Citrix Endpoint Management 中添加设备策略，以将订阅日历添加到 iOS 设备上的日历列表。可订阅的公共日历列表可在 Apple 支持网站的“下载”部分中找到。

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。

先决条件

您必须先订阅日历，然后才能将其添加到用户设备上的订阅日历列表。

iOS 设置

- **说明：** 输入日历的说明。此字段为必填项。
- **URL：** 输入日历 URL。您可以输入 `webcal://` URL 或指向 iCalendar 文件 (.ics) 的 `https://` 链接。此字段为必填项。
- **用户名：** 输入用户的登录名。此字段为必填项。
- **密码：** 输入可选的用户密码。

- **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：** 选择安排策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。

条款和条件设备策略

当您希望用户接受公司关于连接到公司网络的特定策略时，您可以在 Citrix Endpoint Management 中创建条款和条件设备策略。当用户使用 Citrix Endpoint Management 注册其设备时，系统会向他们显示条款和条件，他们必须接受这些条款和条件才能注册其设备。拒绝条款和条件将取消注册过程。

如果您的公司有国际用户，并且您希望他们以其母语接受条款和条件，您可以为不同语言的条款和条件创建不同的策略。您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，您必须提供 PDF 文件。对于 Windows 设备，您必须提供文本 (.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**，然后导航到文件位置，选择要导入的条款和条件文件。
- **默认条款和条件：** 选择此文件是否为属于具有不同条款和条件的多个组的用户的默认文档。默认值为**关**。

> **注意：**
>
> 如果 iOS 设备通过设备注册计划 (DEP) 注册，则不显示条款和条件。

Windows 平板电脑设置

- **要导入的文件：** 单击**浏览**，然后导航到文件位置，选择要导入的条款和条件文件。
- **图像：** 单击**浏览**，然后导航到文件位置，选择要导入的图像文件。

- **默认条款和条件：** 选择此文件是否为属于具有不同条款和条件的多个组的用户的默认文档。默认值为**关**。

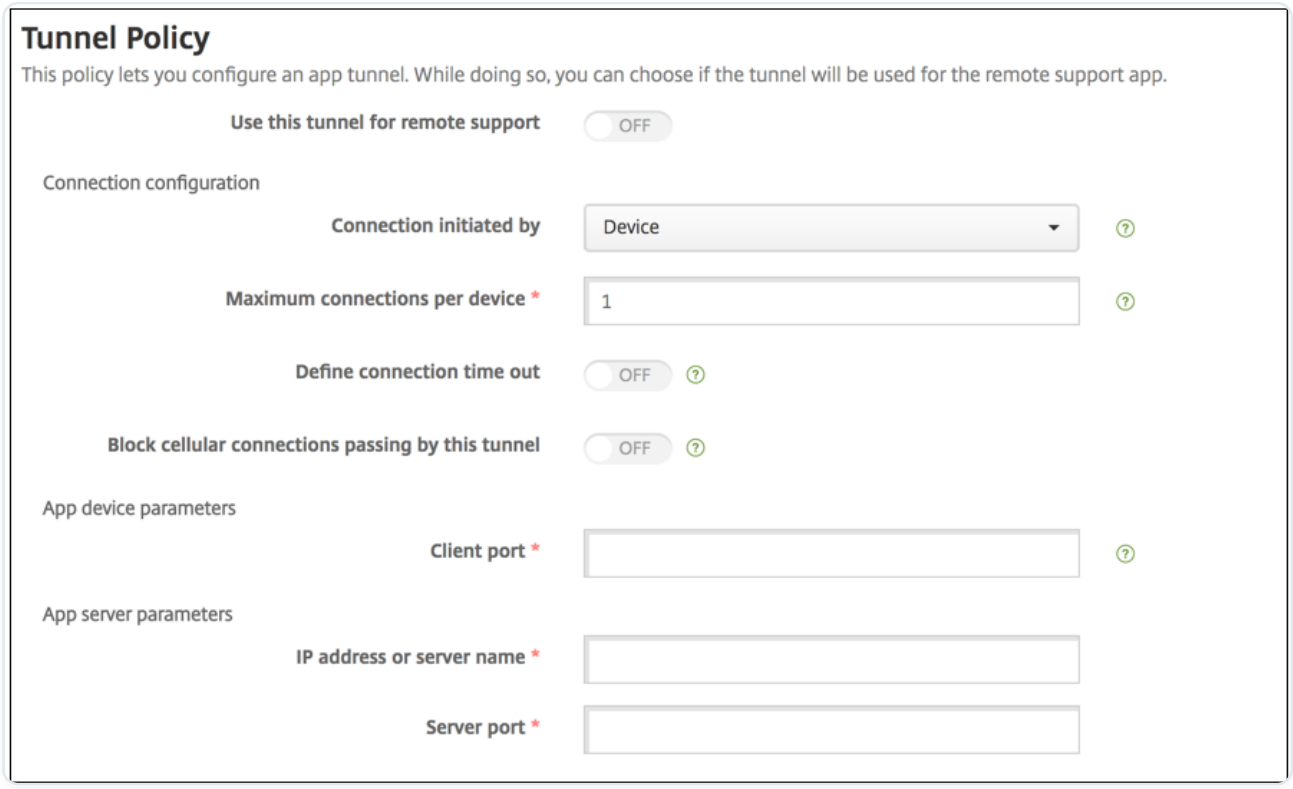
隧道设备策略

应用程序隧道（应用隧道）旨在提高移动应用程序的服务连续性和数据传输可靠性。应用隧道定义了任何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。您可以为 Android 设备配置隧道策略。

通过此策略中定义的隧道发送的任何应用程序流量将通过 Citrix Endpoint Management，然后重定向到运行该应用程序的服务器。

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。

Android 设置



- **连接发起方：** 单击**设备**或**服务器**以指定发起连接的源。
- **每个设备的最大连接数：** 键入一个数字以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：** 选择是否设置应用程序在隧道关闭前可以保持空闲的时间长度。
    - **连接超时：** 如果将**定义连接超时**设置为**开**，请键入应用程序在隧道关闭前可以保持空闲的时间长度（以秒为单位）。

- **阻止通过此隧道的蜂窝连接：** 选择此隧道在漫游时是否被阻止。Wi-Fi 和 USB 连接不会被阻止。
- **客户端端口：** 键入客户端端口号。通常，此值与服务器端口的值相同。
- **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

VPN 设备策略配置虚拟专用网络 (VPN) 设置，使用户设备能够安全地连接到公司资源。您可以为以下平台配置 VPN 设备策略。每个平台都需要一组不同的值，本文将详细介绍这些值。

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。

> **注意：**
>
> 适用于 Android 和 iOS 的 Citrix SSO 现已更名为 Citrix Secure Access。我们正在更新文档以反映此名称更改。

每应用 VPN 的要求

您可以通过 VPN 策略为以下平台配置每应用 VPN 功能：

- iOS
- macOS
- Android（旧版 DA）

对于 Android Enterprise，请使用托管配置设备策略来配置 VPN 配置文件。

每应用 VPN 选项适用于某些连接类型。下表指示何时可以使用每应用 VPN 选项。

平台	连接类型	备注
iOS	思科旧版 AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix SSO 或 自定义 SSL。	

平台	连接类型	备注
macOS	思科 AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA 或 自定义 SSL。	
Android (旧版 DA)	思杰 单点登录	

要使用 Citrix SSO 应用程序为 iOS 和 Android (旧版 DA) 设备创建每应用 VPN，除了 VPN 策略配置之外，您还需要执行额外的步骤。此外，您必须验证是否满足以下先决条件：

- 本地 NetScaler Gateway
- 设备上安装了以下应用程序：
  - 思杰 单点登录
  - 思杰 安全中心

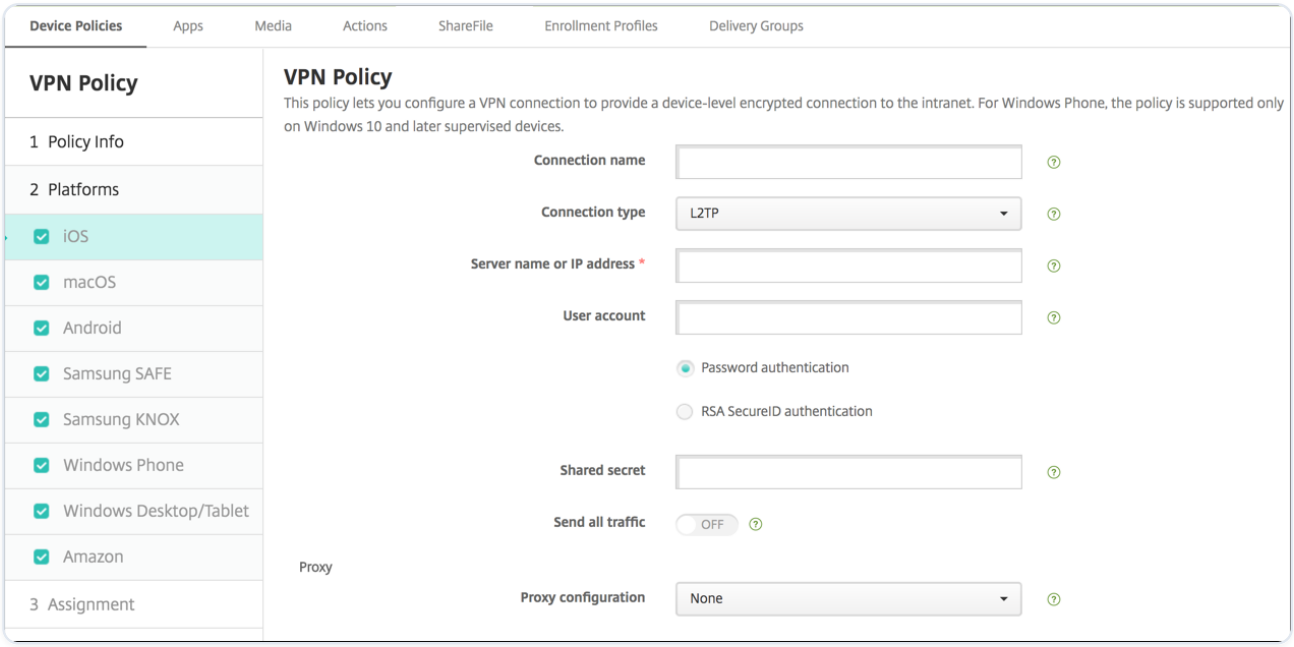
使用 Citrix SSO 应用程序为 iOS 和 Android 设备配置每应用 VPN 的一般工作流程如下所示：

1. 配置 VPN 设备策略，如本文所述。
   - 对于 iOS，请参阅 配置适用于 iOS 的 Citrix SSO 协议。通过 VPN 设备策略配置适用于 iOS 的 Citrix SSO 协议后，您还必须创建应用程序属性策略，以将应用程序与每应用 VPN 策略关联。有关详细信息，请参阅 配置每应用 VPN。
     - 对于“**连接的身份验证类型**”字段，如果您选择“**证书**”，则必须首先为 Citrix 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。
     - 对于“**连接的身份验证类型**”字段，如果您选择“**证书**”或“**密码和证书**”，则必须首先为 Citrix 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. 配置 Citrix ADC 以接受来自每应用 VPN 的流量。有关详细信息，请参阅 在 NetScaler Gateway 上进行完整 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。请执行以下步骤删除现有 VPN 设备策略并创建使用 Citrix SSO 连接类型的 VPN 设备策略：

1. 删除适用于 iOS 的 VPN 设备策略。
2. 添加适用于 iOS 的 VPN 设备策略，并使用以下设置：
   - **连接类型： Citrix SSO**
   - **启用每应用 VPN： 开**
   - **提供程序类型： 数据包隧道**
3. 添加适用于 iOS 的应用程序属性设备策略。对于**每应用 VPN 标识符**，选择 **iOS_VPN**。



- **连接名称：** 键入连接的名称。
- **连接类型：** 在列表中，选择此连接要使用的协议。默认值为 **L2TP**。
  - **L2TP：** 具有预共享密钥身份验证的第 2 层隧道协议。
  - **PPTP：** 点对点隧道协议。
  - **IPSec：** 您的企业 VPN 连接。
  - **Cisco Legacy AnyConnect：** 此连接类型要求用户设备上安装 Cisco Legacy AnyConnect VPN 客户端。Cisco 正在逐步淘汰基于已弃用 VPN 框架的 Cisco Legacy AnyConnect 客户端。

    要使用当前的 Cisco AnyConnect 客户端，请使用**自定义 SSL** 的**连接类型**。有关所需设置，请参阅本节中的“配置自定义 SSL 协议”。
  - **Juniper SSL：** 瞻博网络 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 虚拟互联网访问客户端。
- **IKEv2（仅限 iOS）：** 仅适用于 iOS 的 Internet 密钥交换版本 2。
- **AlwaysOn IKEv2：** 使用 IKEv2 的始终在线访问。
- **AlwaysOn IKEv2 Dual Configuration：** 使用 IKEv2 双重配置的始终在线访问。
- **Citrix SSO：** 适用于 iOS 12 及更高版本的 Citrix SSO 客户端。
- **Custom SSL：** 自定义安全套接字层。此连接类型是 Cisco AnyConnect 客户端所必需的，该客户端的捆绑 ID 为 **com.cisco.anyconnect**。指定**连接名称**为 **Cisco AnyConnect**。您还可以部署 VPN 策略并为 iOS 设备启用网络访问控制 (NAC) 筛选器。该筛选器会阻止安装了不合规应用程序的设备的 VPN 连接。此配置需要 iOS VPN 策略的特定设置，如以下 iOS 部分所述。有关启用 NAC 筛选器所需的其他设置的更多信息，请参阅网络访问控制。

以下各节列出了上述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：** 键入可选的用户帐户。
- 选择**密码身份验证**或 **RSA SecurID 身份验证**。
- **共享密钥：** 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**”。

配置适用于 iOS 的 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：**键入可选的用户帐户。
- 选择“**密码身份验证**”或“**RSA SecurID 身份验证**”。
- **加密级别：**在列表中，选择一个加密级别。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。
  - **最大值 (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**”。

配置适用于 iOS 的 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：**键入可选的用户帐户。
- **连接的身份验证类型：**在列表中，选择“**共享密钥**”或“**证书**”作为此连接的身份验证类型。默认值为“**共享密钥**”。
- 如果启用“**共享密钥**”，请配置以下设置：
  - **组名称：** 键入可选的组名称。
  - **共享密钥：** 键入可选的共享密钥。
  - **使用混合身份验证：** 选择是否使用混合身份验证。使用混合身份验证时，服务器首先向客户端进行身份验证，然后客户端向服务器进行身份验证。默认值为 **关闭**。
  - **提示输入密码：** 选择是否在用户连接到网络时提示他们输入密码。默认值为 **关闭**。
- 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：** 选择是否要求用户在连接到网络时输入其 PIN。默认值为 **关闭**。
  - **启用按需 VPN：** 选择是否在用户连接到网络时触发 VPN 连接。默认值为 **关闭**。有关在 **启用按需 VPN** 为 **开启** 时配置设置的信息，请参阅 配置 iOS 的按需 VPN 设置。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为 **关闭**。
- **按需匹配应用已启用：** 选择当链接到每应用 VPN 服务的应用发起网络通信时，每应用 VPN 连接是否自动触发。默认值为 **关闭**。
- **Safari 域：** 单击 **添加** 以添加 Safari 域名。

配置适用于 iOS 的 Cisco 旧版 AnyConnect 协议

要从 Cisco 旧版 AnyConnect 客户端过渡到新的 Cisco AnyConnect 客户端，请使用自定义 SSL 协议。

- **提供程序捆绑包标识符：** 对于旧版 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**：键入可选的用户帐户。
- **组**：键入可选的组名。
- **连接的身份验证类型**：在列表中，选择此连接的身份验证类型为**密码**或**证书**。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
  - 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**：选择在用户连接到网络时是否提示他们输入 PIN。默认值为**关**。
    - **启用按需 VPN**：选择在用户连接到网络时是否启用触发 VPN 连接。默认值为**关**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置 iOS 的按需 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**：选择是排除本地网络使用此连接，还是允许这些网络使用此连接。默认值为**关**。
- **启用每应用 VPN**：选择是否启用每应用 VPN。默认值为**关**。如果启用此选项，请配置以下设置：
    - **按需匹配应用已启用**：选择当链接到每应用 VPN 服务的应用启动网络通信时，每应用 VPN 连接是否自动触发。默认值为**关**。
    - **提供程序类型**：选择每应用 VPN 是作为**应用代理**还是作为**数据包隧道**提供。默认值为**应用代理**。
    - **Safari 域**：对于要包括的每个可触发每应用 VPN 连接的 Safari 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，或单击“**取消**”以不保存域。

配置适用于 iOS 的 Juniper SSL 协议

- **提供程序捆绑包标识符：** 如果您的每应用 VPN 配置文件具有具有多个相同类型 VPN 提供程序的应用程序的捆绑包标识符，请在此处指定要使用的提供程序。
- **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：** 键入可选的用户帐户。
- **领域：** 键入可选的领域名称。
- **角色：** 键入可选的角色名称。
- **连接的身份验证类型：** 在列表中，选择“**密码**”或“**证书**”作为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**”字段中键入可选的身份验证密码。
- 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他们输入 PIN。默认值为“**关**”。

- **启用按需 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“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅配置适用于 iOS 的按需 VPN 启用设置。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为“**关**”。如果启用此选项，请配置以下设置：
- **按需匹配应用已启用：** 选择当链接到每应用 VPN 服务的应用启动网络通信时，每应用 VPN 连接是否自动触发。默认值为“**关**”。
- **提供程序类型：** 选择按应用 VPN 是作为**应用代理**还是**数据包隧道**提供。默认值为**应用代理**。
- **Safari 域：** 对于要包含的每个可触发按应用 VPN 连接的 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，或单击**取消**以不保存域。

配置适用于 iOS 的 F5 SSL 协议

- **提供程序捆绑包标识符：** 如果您的按应用 VPN 配置文件具有具有多个相同类型 VPN 提供程序的应用程序的捆绑包标识符，请在此处指定要使用的提供程序。
- **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：** 键入可选的用户帐户。
- **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择**密码**或**证书**。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
  - 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：** 选择在用户连接到网络时是否提示他们输入 PIN。默认值为**关闭**。
    - **启用按需 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**关闭**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置适用于 iOS 的按需 VPN 设置。
- **启用按应用 VPN：** 选择是否启用按应用 VPN。默认值为**关闭**。如果启用此选项，请配置以下设置：
  - **按需匹配应用已启用：** 选择当与按应用 VPN 服务关联的应用启动网络通信时，按应用 VPN 连接是否自动触发。

- **提供程序类型：** 选择按应用 VPN 是作为**应用代理**还是作为**数据包隧道**提供。默认值为**应用代理**。
- **Safari 域：** 对于要包含的每个可触发按应用 VPN 连接的 Safari 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，或单击**取消**以不保存域。

配置适用于 iOS 的 SonicWALL 协议

- **提供程序捆绑包标识符：** 如果您的按应用 VPN 配置文件具有具有多个相同类型 VPN 提供程序的应用的捆绑包标识符，请在此处指定要使用的提供程序。
- **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：** 键入可选的用户帐户。
- **登录组或域：** 键入可选的登录组或域。
- **连接的身份验证类型：** 在列表中，选择**密码**或**证书**作为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**字段中键入可选的身份验证密码。
  - 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：** 选择当用户连接到网络时是否提示他们输入 PIN。默认值为**关闭**。
    - **启用按需 VPN：** 选择是否在用户连接到网络时启用触发 VPN 连接。默认设置为“**关**”。有关在“**启用按需 VPN**”设置为“**开**”时配置设置的信息，请参阅配置 iOS 的按需 VPN 启用设置。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认设置为“**关**”。如果将此选项设置为“开”，请配置以下设置：
  - **启用按需匹配应用：** 选择当链接到每应用 VPN 服务的应用启动网络通信时，每应用 VPN 连接是否自动触发。
  - **提供程序类型：** 选择每应用 VPN 是作为“**应用代理**”还是“**数据包隧道**”提供。默认值为“**应用代理**”。
  - **Safari 域：** 对于要包含的每个可以触发每应用 VPN 连接的 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，或单击“**取消**”以不保存域。

为 iOS 配置 Ariba VIA 协议

- **提供程序捆绑包标识符：** 如果您的每应用 VPN 配置文件具有具有多个相同类型 VPN 提供程序的应用的捆绑包标识符，请在此处指定要使用的提供程序。
- **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：** 键入可选的用户帐户。
- **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择“**密码**”或“**证书**”。默认值为“**密码**”。
    - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
    - 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PIN：** 选择用户连接到网络时是否提示输入PIN。默认值为 **关闭**。
        - **启用按需VPN：** 选择用户连接到网络时是否启用触发VPN连接。默认值为 **关闭**。有关在 **启用按需VPN** 为 **开** 时配置设置的信息，请参阅 配置适用于iOS的按需VPN设置。
- **启用每应用VPN：** 选择是否启用每应用VPN。默认值为 **关闭**。如果启用此选项，请配置以下设置：
    - **启用按需匹配应用：** 选择当链接到每应用VPN服务的应用发起网络通信时，每应用VPN连接是否自动触发。
    - **Safari域：** 对于要包含的每个可触发每应用VPN连接的Safari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，或单击 **取消** 以不保存域。

配置适用于iOS的IKEv2协议

本节包含用于IKEv2、始终开启IKEv2和始终开启IKEv2双配置协议的设置。对于始终开启IKEv2双配置协议，请为蜂窝网络和Wi-Fi网络配置所有这些设置。

- **允许用户禁用自动连接：** 适用于始终开启协议。选择是否允许用户在其设备上禁用自动连接到网络。默认值为 **关闭**。
- **服务器主机名或IP地址：** 键入VPN服务器的服务器名称或IP地址。

- **本地标识符：** IKEv2客户端的FQDN或IP地址。此字段为必填项。
- **远程标识符：** VPN服务器的FQDN或IP地址。此字段为必填项。
- **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 **共享密钥**。
  - 如果选择 **共享密钥**，请键入可选的共享密钥。
  - 如果您选择**证书**，请选择要使用的**身份凭据**。默认值为**无**。
  - 如果您选择**基于设备标识符的设备证书**，请选择要使用的**设备身份类型**。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**始终开启 IKEv2**时可用。
- **启用扩展身份验证：** 选择是否启用扩展身份验证协议 (EAP)。如果为**开**，请键入**用户帐户**和**身份验证密码**。
- **死对等体检测间隔：** 选择联系对等设备以确保对等设备保持可达的频率。默认值为**无**。选项包括：
  - **无：** 禁用死对等体检测。
  - **低：** 每 30 分钟联系对等体一次。
  - **中：** 每 10 分钟联系对等体一次。
  - **高：** 每 1 分钟联系对等体一次。
- **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。
- **启用回退：** 如果启用，此设置允许通过蜂窝数据建立隧道，以承载符合 Wi-Fi 辅助条件并需要 VPN 的流量。默认值为**关**。
- **设备休眠时启用 NAT 保活：** 适用于始终开启协议。保活数据包维护 IKEv2 连接的 NAT 映射。当设备处于唤醒状态时，芯片会定期发送这些数据包。如果此设置开启，即使设备处于休眠状态，芯片也会发送保活数据包。默认间隔在 Wi-Fi 上为 20 秒，在蜂窝网络上为 110 秒。您可以通过使用 NAT 保活间隔参数来更改间隔。
- **NAT 保活间隔（秒）：** 默认为 20 秒。
- **启用完全前向保密：** 选择是否启用此功能。
- **DNS 服务器 IP 地址：** 可选。DNS 服务器 IP 地址字符串列表。这些 IP 地址可以包含 IPv4 和 IPv6 地址的混合。单击“**添加**”以键入地址。
- **域名：** 可选。隧道的首要域。

- **搜索域：** 可选。用于完全限定单标签主机名的域字符串列表。
- **将补充匹配域附加到解析器列表：** 可选。确定是否将补充匹配域列表添加到解析器的搜索域列表。默认值为“**开**”。
- **补充匹配域：** 可选。用于确定哪些 DNS 查询使用 DNS 服务器地址中的 DNS 解析器设置的域字符串列表。此项创建拆分 DNS 配置，其中只有特定域中的主机通过使用隧道的 DNS 解析器进行解析。不在此列表中的域中的主机将通过使用系统的默认解析器进行解析。

如果此参数为空字符串，则该字符串是默认域。因此，拆分隧道配置可以在主 DNS 服务器之前将所有 DNS 查询定向到 VPN DNS 服务器。如果 VPN 隧道是网络的默认路由，则列出的 DNS 服务器将成为默认解析器。在这种情况下，将忽略补充匹配域列表。

- **IKE SA 参数**和**子 SA 参数：** 为每个安全关联 (SA) 参数选项配置这些设置：
  - **加密算法：** 在列表中，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 生存期（分钟）：** 键入一个介于 10 到 1440 之间的整数，表示 SA 生存期（重新生成密钥间隔）。默认值为 **1440** 分钟。
- **服务例外：** 适用于始终开启协议。服务例外是指免于始终开启 VPN 的系统服务。配置这些服务例外设置：
  - **语音邮件：** 在列表中，选择如何处理语音邮件例外。默认值为“**允许流量通过隧道**”。
  - **AirPrint：** 在列表中，选择如何处理 AirPrint 例外。默认值为“**允许流量通过隧道**”。
  - **允许来自 VPN 隧道外部强制网络页面的流量：** 选择是否允许用户连接到 VPN 隧道外部的公共热点。默认值为“**关**”。
  - **允许所有强制网络应用流量通过 VPN 隧道外部**：选择是否允许所有热点网络应用通过 VPN 隧道外部。默认值为“**关**”。
  - **强制网络应用捆绑包标识符**：对于用户被允许访问的每个热点网络应用捆绑包标识符，单击“**添加**”并键入热点网络应用“**捆绑包标识符**”。单击“**保存**”以保存应用捆绑包标识符。
- **每应用 VPN**：为 IKEv2 连接类型配置这些设置。
  - **启用每应用 VPN**：选择是否启用每应用 VPN。默认值为“**关**”。
  - **按需匹配应用已启用**：选择当链接到每应用 VPN 服务的应用发起网络通信时，每应用 VPN 连接是否自动触发。默认值为“**关**”。
  - **Safari 域**：单击“**添加**”以添加 Safari 域名。

- **代理配置**：选择 VPN 连接如何通过代理服务器路由。默认值为“**无**”。

配置适用于 iOS 的 Citrix SSO 协议

Citrix SSO 客户端可在 Apple Store 中获取。

- **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**：键入可选的用户帐户。
- **连接的身份验证类型**：在列表中，为该连接的身份验证类型选择“**密码**”或“**证书**”。默认值为“**密码**”。
  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 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 PIN**： 选择是否在用户连接到网络时提示其输入 PIN。默认值为“**关闭**”。
    - **启用按需 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“**关闭**”。有关在“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅配置 iOS 的按需 VPN 设置。
- **启用每应用 VPN**： 选择是否启用每应用 VPN。默认值为“**关闭**”。如果将此选项设置为“开”，请配置以下设置：
  - **启用按需匹配应用**： 选择当链接到每应用 VPN 服务的应用发起网络通信时，每应用 VPN 连接是否自动触发。
  - **提供程序类型**： 选择每应用 VPN 是作为“**应用代理**”还是作为“**数据包隧道**”提供。默认值为“**应用代理**”。
  - **提供程序类型**： 设置为“**数据包隧道**”。
  - **Safari 域**： 对于要包含的每个可触发每应用 VPN 连接的 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，或单击“**取消**”以不保存域。
- **自定义 XML**： 对于要添加的每个自定义 XML 参数，单击“**添加**”并指定键/值对。可用参数如下：
  - **disableL3**： 禁用系统级 VPN。仅允许每应用 VPN。不需要“**值**”。
  - **user agent**： 将此设备策略与面向 VPN 插件客户端的任何 NetScaler Gateway 策略关联。对于由插件启动的请求，此键的“**值**”会自动添加到 VPN 插件中。

为 iOS 配置自定义 SSL 协议

要从 Cisco Legacy AnyConnect 客户端过渡到 Cisco AnyConnect 客户端，请执行以下操作：

1. 使用自定义 SSL 协议配置 VPN 设备策略。将策略部署到 iOS 设备。
2. 从 `<https://apps.apple.com/us/app/cisco-secure-client/id1135064690>` 上传 Cisco AnyConnect 客户端，将应用添加到 Citrix Endpoint Management，然后将应用部署到 iOS 设备。
3. 从 iOS 设备中删除旧的 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相同类型（应用程序代理或数据包隧道）的 VPN 提供程序，则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：** 键入一个可选的用户帐户。
- **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择**密码**或**证书**。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入一个可选的身份验证密码。
  - 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其输入 PIN。默认值为**关**。
    - **启用按需 VPN：** 选择是否在用户连接到网络时触发 VPN 连接。默认值为**关**。有关在**启用按需 VPN** 为**开**时配置设置的信息，请参阅配置 iOS 的按需 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：** 选择是排除本地网络使用此连接还是允许这些网络。默认值为**关**。
- **启用按应用VPN：** 选择是否启用按应用VPN。默认值为**关闭**。如果将此选项设置为“开”，请配置以下设置：
  - **按需匹配应用已启用：** 选择当链接到按应用VPN服务的应用发起网络通信时，按应用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**数据包隧道**。对于代理服务，请选择**应用代理**。对于Cisco AnyConnect客户端，请选择**数据包隧道**。
- **Safari域：** 对于要包含的每个可以触发按应用VPN连接的Safari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，或单击**取消**以不保存域。

- **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，或单击**取消**以不保存参数。

配置VPN设备策略以支持NAC

1. 配置NAC筛选器需要**自定义SSL**的**连接类型**。
2. 指定**VPN**的**连接名称**。
3. 对于**自定义SSL标识符**，键入**com.citrix.NetScalerGateway.ios.app**
4. 对于**提供程序捆绑包标识符**，键入**com.citrix.NetScalerGateway.ios.app.vpnplugin**

步骤 3 和 4 中的值来自 NAC 筛选所需的 Citrix SSO 安装。您无需配置身份验证密码。有关使用 NAC 功能的更多信息，请参阅网络访问控制。

配置 iOS 的按需 VPN 启用选项

- **按需域：** 对于每个域以及用户连接时要执行的相关操作，单击“**添加**”并执行以下操作：
- **域：** 键入要添加的域。
- **操作：** 从列表中选择一个可能的操作：
  - **始终建立：** 该域始终触发 VPN 连接。
  - **从不建立：** 该域从不触发 VPN 连接。
  - **必要时建立：** 如果域名解析失败，该域会触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，就会发生失败。
  - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。
- **按需规则**

- **操作：** 在列表中，选择要执行的操作。默认值为 **EvaluateConnection**。可能的操作包括：
  - **允许：** 允许按需 VPN 在触发时连接。
  - **连接：** 无条件启动 VPN 连接。
  - **断开连接：** 删除 VPN 连接，并且只要规则匹配，就不要按需重新连接。
  - **EvaluateConnection：** 评估每个连接的 ActionParameters 数组。
  - **忽略**：保持任何现有 VPN 连接处于活动状态，但只要规则匹配，就不要按需重新连接。
- **DNS域匹配**：对于要添加的、设备搜索域列表可与之匹配的每个域，单击**添加**并执行以下操作：
  - **DNS 域**：键入域名。您可以使用通配符“*”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，或单击**取消**以不保存域。
- **DNS服务器地址匹配**：对于要添加的、网络中任何指定 DNS 服务器可与之匹配的每个 IP 地址，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。您可以使用通配符“*”后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的任何 DNS 服务器。
  - 单击**保存**以保存 DNS 服务器地址，或单击**取消**以不保存 DNS 服务器地址。
- **接口类型匹配**：在列表中，选择正在使用的主要网络接口硬件类型。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。此选项为默认值。
  - **以太网**：仅匹配以太网网络接口硬件。
  - **Wi-Fi**：仅匹配 Wi-Fi 网络接口硬件。
  - **蜂窝**：仅匹配蜂窝网络接口硬件。
- **SSID匹配**：对于要添加的、与当前网络匹配的每个 SSID，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 SSID 未出现，则匹配失败。将此列表留空以匹配任何 SSID。
  - 单击**保存**以保存 SSID，或单击**取消**以不保存 SSID。
- **URLStringProbe:** 键入要获取的 URL。如果此 URL 在没有重定向的情况下成功获取，则此规则匹配。

- **ActionParameters : Domains:** 对于 EvaluateConnection 检查的每个要添加的域，单击“**添加**”并执行以下操作：
  - **Domain:** 键入要添加的域。
  - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。
- **ActionParameters : DomainAction:** 在列表中，为指定的 **ActionParameters : Domains** 域选择 **VPN 行为**。默认值为 **ConnectIfNeeded**。可能的动作包括：
  - **ConnectIfNeeded:** 如果域名解析失败，该域将触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，就会发生失败。
  - **NeverConnect:** 该域从不触发 VPN 连接。
- **Action Parameters: RequiredDNSServers:** 对于用于解析指定域的每个 DNS 服务器，单击“**添加**”并执行以下操作：
  - **DNS Server:** 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当前网络配置之外。如果 DNS 服务器不可达，则会建立 VPN 连接作为响应。确保 DNS 服务器是内部 DNS 服务器或受信任的外部 DNS 服务器。
  - 单击“**保存**”以保存 DNS 服务器，或单击“**取消**”以不保存 DNS 服务器。
- **ActionParameters : RequiredURLStringProbe:** 可选地，键入一个 HTTP 或 HTTPS（首选）URL 以使用 GET 请求进行探测。如果 URL 的主机名无法解析、服务器不可达或服务器没有响应，则会建立 VPN 连接。仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。
- **OnDemandRules : XML content:** 键入或复制粘贴 XML 按需配置规则。
  - 单击“**检查字典**”以验证 XML 代码。如果 XML 有效，则“**有效 XML**”将显示在“**XML 内容**”文本框下方。如果无效，则会显示一条错误消息描述错误。

- **代理**
  - **Proxy configuration:** 在列表中，选择 VPN 连接如何通过代理服务器路由。默认值为 **None**。
    - 如果启用**手动**，请配置以下设置：
      - **代理服务器主机名或 IP 地址：** 输入代理服务器的主机名或 IP 地址。此字段为必填项。
      - **代理服务器端口：** 输入代理服务器端口号。此字段为必填项。

    - **用户名：** 输入可选的代理服务器用户名。
    - **密码：** 输入可选的代理服务器密码。
  - 如果配置**自动**，请配置以下设置：
    - **代理服务器 URL：** 输入代理服务器的 URL。此字段为必填项。

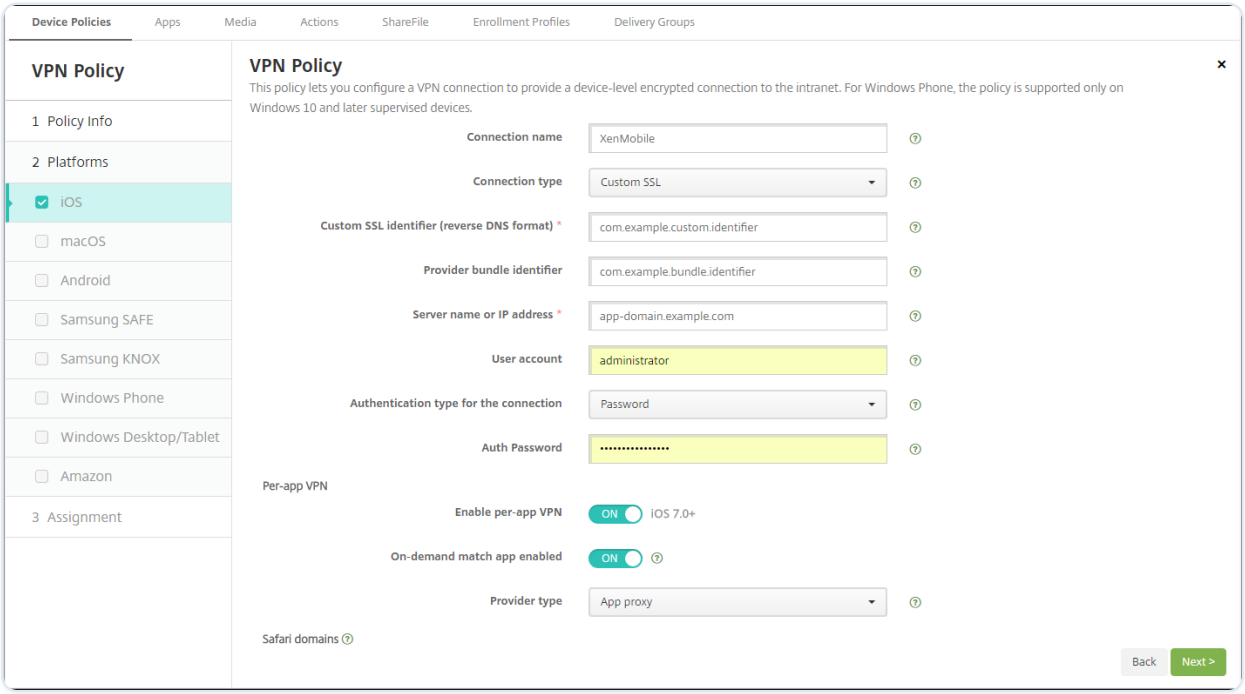
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 输入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。

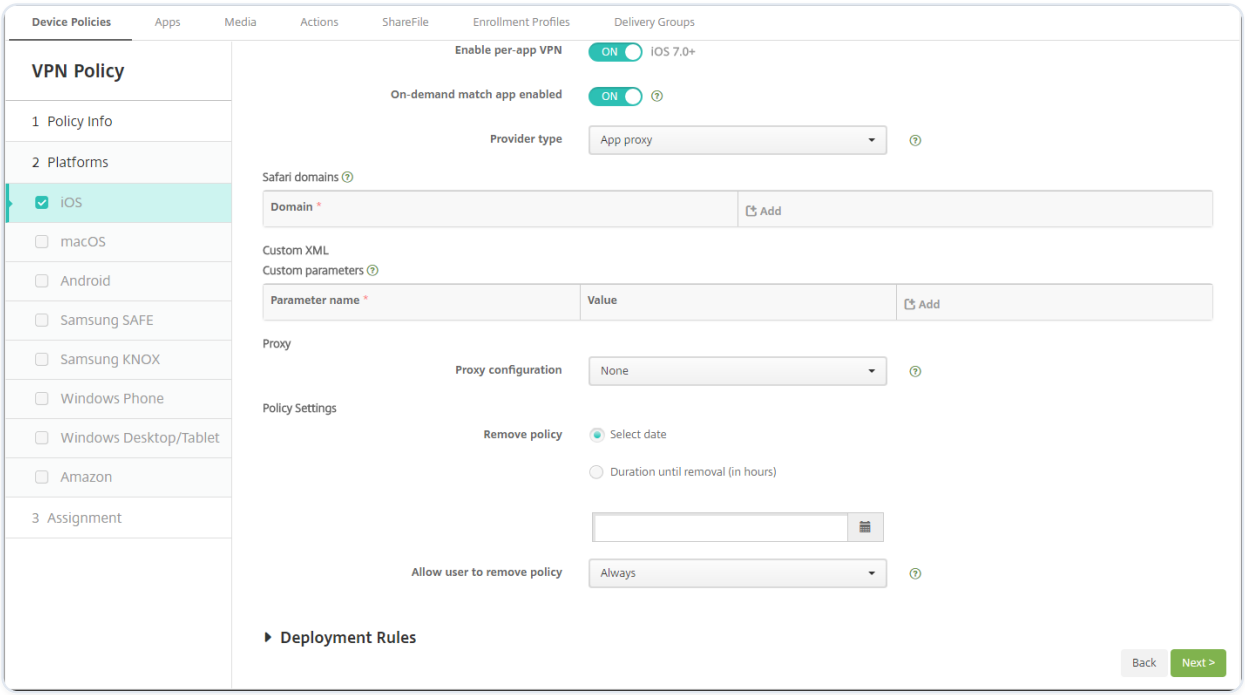
配置每应用 VPN

适用于 iOS 的每应用 VPN 选项可用于以下连接类型：Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix VPN、Citrix SSO 和 Custom SSL。

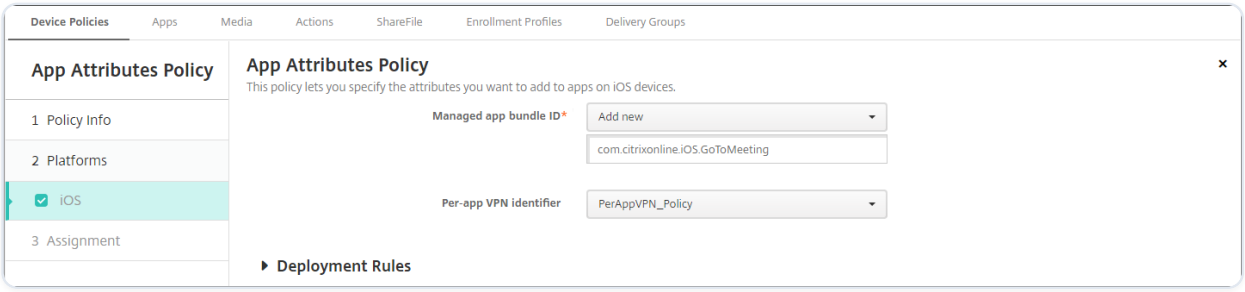
要配置每应用 VPN：

1. 在**配置 > 设备策略**中，创建 VPN 策略。例如：

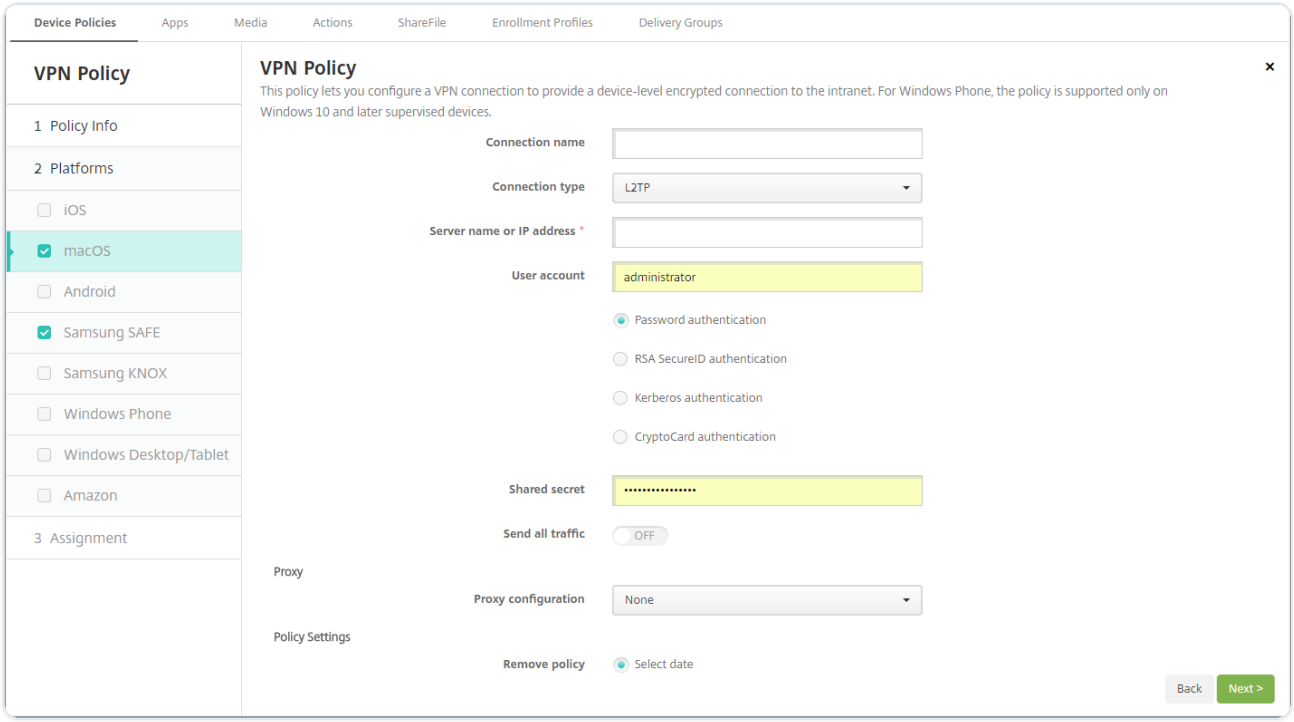




2. 在 **配置 > 设备策略** 中，创建一个应用程序属性策略，以将应用程序与每应用 VPN 策略关联。对于 **每应用 VPN 标识符**，选择在步骤 1 中创建的 VPN 策略的名称。对于 **托管应用程序捆绑包 ID**，从应用程序列表中选择或键入应用程序捆绑包 ID。（如果您部署了 iOS 应用程序清单策略，则应用程序列表将包含应用程序。）



macOS 设置



- **连接名称：** 键入连接的名称。
- **连接类型：** 在列表中，选择此连接要使用的协议。默认值为 L2TP。
  - **L2TP：** 具有预共享密钥身份验证的第 2 层隧道协议。
  - **PPTP：** 点对点隧道。
  - **IPSec：** 您的企业 VPN 连接。
  - **Cisco AnyConnect：** Cisco AnyConnect VPN 客户端。
  - **Juniper SSL：** 瞻博网络 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 虚拟互联网访问客户端。
  - **Citrix VPN**：Citrix VPN 客户端。
  - **自定义 SSL**：自定义安全套接字层。

以下各节列出了上述每种连接类型的配置选项。

配置 macOS 的 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**：键入可选的用户帐户。

- 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**。
- **共享密钥**：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**关闭**。

配置 macOS 的 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**：键入可选的用户帐户。
- 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**。

配置 macOS 的 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**： 键入可选的用户帐户。
- **连接的身份验证类型**： 在列表中，为该连接的身份验证类型选择 **共享密钥** 或 **证书**。默认值为 **共享密钥**。
  - 如果启用 **共享密钥** 身份验证，请配置以下设置：
    - **组名称**： 键入可选的组名称。
    - **共享密钥**： 键入可选的共享密钥。
    - **使用混合身份验证**： 选择是否使用混合身份验证。使用混合身份验证时，服务器首先向客户端进行身份验证，然后客户端向服务器进行身份验证。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他们输入密码。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**： 选择是否要求用户在连接到网络时输入其 PIN。默认值为“**关**”。

  - **启用按需 VPN：** 选择是否在用户连接到网络时触发 VPN 连接。默认值为“**关**”。有关在“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅配置按需 VPN 选项。

配置适用于 macOS 的 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：** 键入可选的用户帐户。
- **组：** 键入可选的组名称。
- **连接的身份验证类型：** 在列表中，选择此连接的身份验证类型为“**密码**”或“**证书**”。默认值为“**密码**”。
  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 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其输入 PIN。默认值为“**关**”。
    - **启用按需 VPN：** 选择是否在用户连接到网络时触发 VPN 连接。默认值为“**关**”。有关在“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅配置按需 VPN 选项。
  - **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为“**关**”。如果启用此选项，请配置以下设置：
    - **启用按需匹配应用：** 选择当链接到每应用 VPN 服务的应用启动网络通信时，每应用 VPN 连接是否自动触发。默认值为“**关**”。
    - **Safari 域：** 对于要包含的每个可触发每应用 VPN 连接的 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，或单击“**取消**”以不保存域。

配置 Juniper SSL 协议（适用于 macOS）

- **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：**键入可选的用户帐户。
- **领域：**键入可选的领域名称。
- **角色：**键入可选的角色名称。
- **连接的身份验证类型：**在列表中，选择此连接的身份验证类型为“**密码**”或“**证书**”。默认值为“**密码**”。

  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 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他们输入 PIN。默认值为“**关**”。
    - **启用按需 VPN：**选择是否在用户连接到网络时触发 VPN 连接。默认值为“**关**”。有关在“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅配置按需 VPN 设置。

- **启用每应用 VPN：**选择是否启用每应用 VPN。默认值为“**关**”。如果启用此选项，请配置以下设置：
  - **按需匹配应用已启用：**选择当链接到每应用 VPN 服务的应用启动网络通信时，是否自动触发每应用 VPN 连接。默认值为“**关**”。
  - **Safari 域：** 对于要包含的、可触发按应用 VPN 连接的每个 Safari 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，或单击“**取消**”以不保存域。

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：** 键入可选的用户帐户。
- **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择“**密码**”或“**证书**”。默认值为“**密码**”。
  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 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：** 选择用户连接到网络时是否提示输入 PIN。默认值为“**关**”。
    - **启用按需 VPN：** 选择用户连接到网络时是否启用触发 VPN 连接。默认值为“**关**”。有关在“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅配置启用按需 VPN 设置。
- **启用按应用 VPN：** 选择是否启用按应用 VPN。默认值为“**关**”。如果启用此选项，请配置以下设置：

- **启用按需匹配应用：** 选择当链接到按应用 VPN 服务的应用开始网络通信时，按应用 VPN 连接是否自动触发。默认值为“**关**”。
- **Safari 域：** 对于要包含的、可触发按应用 VPN 连接的每个 Safari 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，或单击**取消**以不保存域。

配置适用于 macOS 的 SonicWALL Mobile Connect 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：**键入可选的用户帐户。
- **登录组或域：**键入可选的登录组或域。
- **连接的身份验证类型：在列表中，选择密码**或**证书**作为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**字段中键入可选的身份验证密码。
  - 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他们输入 PIN。默认值为关。**
    - **启用按需 VPN：选择是否在用户连接到网络时触发 VPN 连接。默认值为关。**有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置启用按需 VPN 设置。
- **启用每应用 VPN：选择是否启用每应用 VPN。默认值为关。**如果启用此选项，请配置以下设置：
  - **按需匹配应用已启用：选择当链接到每应用 VPN 服务的应用发起网络通信时，每应用 VPN 连接是否自动触发。默认值为关。**
  - **Safari 域：对于要包含的每个可触发每应用 VPN 连接的 Safari 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，或单击“**取消**”以不保存域。

配置适用于 macOS 的 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。
- **用户帐户：** 键入可选的用户帐户。

- **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择“**密码**”或“**证书**”。默认值为“**密码**”。
  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 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：** 选择用户连接到网络时是否提示其输入 PIN。默认值为“**关**”。
    - **启用按需 VPN：** 选择用户连接到网络时是否启用触发 VPN 连接。默认值为“**关**”。有关在“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅配置启用按需 VPN 设置。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为“**关**”。如果启用此选项，请配置以下设置：
  - **启用按需匹配应用：** 选择当链接到每应用 VPN 服务的应用启动网络通信时，每应用 VPN 连接是否自动触发。默认值为“**关**”。
  - **Safari 域：** 对于要包含的每个可触发每应用 VPN 连接的 Safari 域，单击“**添加**”并执行以下操作：
    - **域：** 键入要添加的域。
    - 点击 **保存** 以保存域，或点击 **取消** 以不保存域。

配置 macOS 的自定义 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。此字段为必填项。
- **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。此字段为必填项。
- **用户帐户：** 键入可选的用户帐户。
  - **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择 **密码** 或 **证书**。默认值为 **密码**。
  - 如果启用 **密码**，请在 **身份验证密码** 字段中键入可选的身份验证密码。
  - 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：** 选择在用户连接到网络时是否提示他们输入 PIN。默认值为 **关**。
    - **启用按需 VPN：** 选择在用户连接到网络时是否启用触发 VPN 连接。默认值为 **关**。有关在 **启用按需 VPN** 为 **开** 时配置设置的信息，请参阅 配置按需 VPN 设置。

- **每应用 VPN：** 选择是否启用每应用 VPN。默认值为 **关**。如果启用此选项，请配置以下设置：
  - **按需匹配应用已启用：** 选择当链接到每应用 VPN 服务的应用启动网络通信时，每应用 VPN 连接是否自动触发。
  - **Safari 域：** 对于要包含的每个可触发每应用 VPN 连接的 Safari 域，请单击 **添加** 并执行以下操作：
    - **域：** 键入要添加的域。
    - 点击“**保存**”以保存域，或点击“**取消**”以不保存域。

- **自定义 XML：** 对于要添加的每个自定义 XML 参数，点击“**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。
  - 点击“**保存**”以保存域，或点击“**取消**”以不保存域。

配置启用按需 VPN 选项

- **按需域：** 对于要添加的每个域以及用户连接到这些域时要执行的关联操作，点击“**添加**”并执行以下操作：
  - **域：** 键入要添加的域。
  - **操作：** 在列表中选择以下可能的操作之一：
    - **始终建立：** 该域始终触发 VPN 连接。
    - **从不建立：** 该域从不触发 VPN 连接。
    - **必要时建立：** 如果域名解析失败，该域会触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，就会发生失败。
  - 点击“**保存**”以保存域，或点击“**取消**”以不保存域。

- **按需规则**
  - **操作：** 在列表中，选择要执行的操作。默认值为“**EvaluateConnection**”。可能的操作包括：
    - **允许**：允许按需 VPN 在触发时连接。
    - **连接**：无条件启动 VPN 连接。
    - **断开连接**：删除 VPN 连接，并且只要规则匹配，就不要按需重新连接。
    - **评估连接**：评估每个连接的 **ActionParameters** 数组。

- **忽略**：保持任何现有 VPN 连接处于活动状态，但只要规则匹配，就不要按需重新连接。

- **DNS 域匹配**：对于设备搜索域列表可以匹配的域，单击“**添加**”并执行以下操作：
  - **DNS 域**：键入域名。您可以使用通配符“*”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，或单击“**取消**”以不保存域。
- **DNS 服务器地址匹配**：对于要添加的、网络中任何指定 DNS 服务器可以匹配的每个 IP 地址，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。您可以使用通配符“*”后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的任何 DNS 服务器。
  - 单击“**保存**”以保存 DNS 服务器地址，或单击“**取消**”以不保存 DNS 服务器地址。
- **接口类型匹配**：在列表中，单击正在使用的主要网络接口硬件类型。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。此选项是默认值。
  - **以太网**：仅匹配以太网网络接口硬件。
  - **Wi-Fi**：仅匹配 Wi-Fi 网络接口硬件。
  - **蜂窝网络**： 仅匹配蜂窝网络接口硬件。
- **SSID 匹配**： 对于要添加的每个与当前网络匹配的 SSID，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 SSID 未出现，则匹配失败。将此列表留空以匹配任何 SSID。
  - 单击 **保存** 以保存 SSID，或单击 **取消** 以不保存 SSID。
- **URL 字符串探测**： 键入要获取的 URL。如果此 URL 成功获取且未重定向，则此规则匹配。
- **操作参数：域**： 对于要添加的每个由 EvaluateConnection 检查的域，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，或单击 **取消** 以不保存域。
- **操作参数：域操作**： 在列表中，为指定的 **操作参数：域** 选择 **VPN 行为**。默认值为 **ConnectIfNeeded**。可能的操作包括：
  - **ConnectIfNeeded**： 如果域名解析失败，该域将触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，会发生失败。

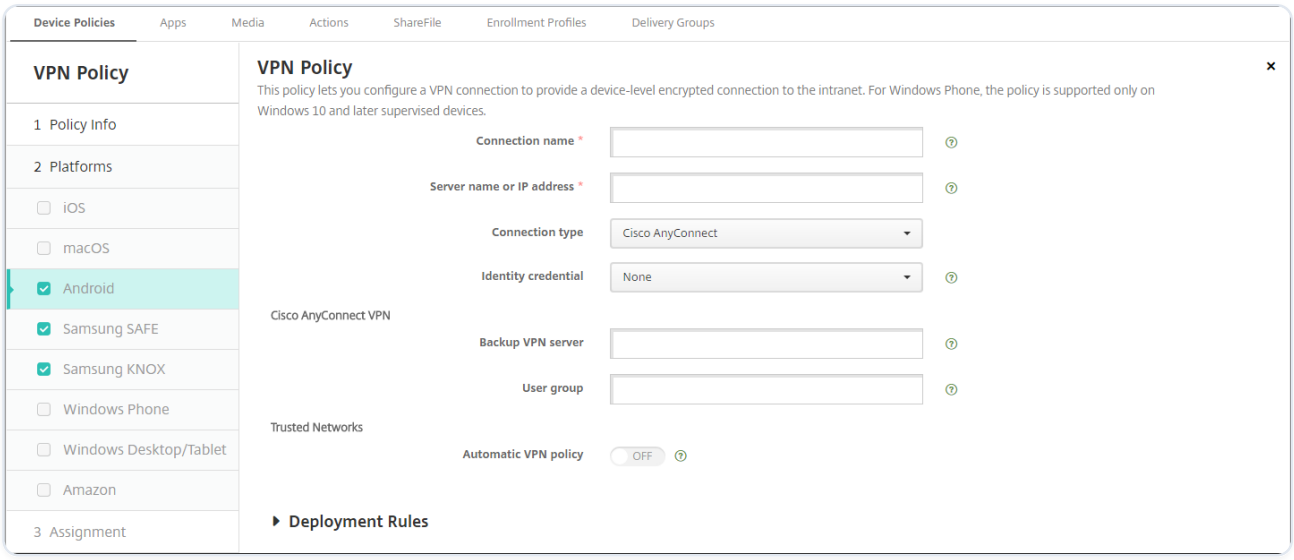
    - **NeverConnect：** 该域从不触发 VPN 连接。
  - **操作参数：所需 DNS 服务器：** 对于用于解析指定域的每个 DNS 服务器，单击 **添加** 并执行以下操作：
    - **DNS 服务器：** 仅当 **操作参数** : **域操作** = **ConnectIfNeeded** 时有效。键入要添加的 DNS 服务器 IP 地址。此服务器可以位于设备当前网络配置之外。如果 DNS 服务器不可达，则会建立 VPN 连接作为响应。此 DNS 服务器必须是内部 DNS 服务器或受信任的外部 DNS 服务器。
    - 单击 **保存** 以保存 DNS 服务器，或单击 **取消** 以不保存 DNS 服务器。
  - **操作参数：所需 URL 字符串探测：** （可选）键入要使用 GET 请求探测的 HTTP 或 HTTPS（首选）URL。如果 URL 的主机名无法解析、服务器不可达或服务器无响应，则会建立 VPN 连接。仅当 **操作参数** : **域操作** = **ConnectIfNeeded** 时有效。
  - **按需规则：XML 内容：**键入或复制并粘贴 XML 按需配置规则。
    - 单击**检查字典**以验证 XML 代码。如果 XML 有效，则**有效 XML**将显示在**XML 内容**文本框下方。如果无效，则会显示一条错误消息描述该错误。

- **代理**
  - **代理配置：在列表中，选择 VPN 连接如何通过代理服务器路由。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。此字段为必填项。
      - **代理服务器端口：**键入代理服务器端口号。此字段为必填项。
      - **用户名：**键入可选的代理服务器用户名。
      - **密码：**键入可选的代理服务器密码。
    - 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。此字段为必填项。

- **策略设置**
  - **删除策略：选择一种计划策略删除的方法。可用选项包括选择日期和删除前持续时间（小时）**
    - **选择日期：**单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），直到策略删除发生。

- **允许用户删除策略：** 您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**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
- **配置文件范围：** 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 macOS 10.7 及更高版本。

Android（旧版设备管理员）设置



配置适用于 Android 的 Cisco AnyConnect VPN 协议

- **连接名称：** 键入 Cisco AnyConnect VPN 连接的名称。此字段为必填项。
- **服务器名称或 IP 地址：** 键入 VPN 服务器的名称或 IP 地址。此字段为必填项。
- **身份凭据：** 在列表中，选择一个身份凭据。
- **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。
- **受信任的网络**
  - **自动 VPN 策略：** 启用或禁用此选项以设置 VPN 对受信任和不受信任网络的反应方式。如果启用，请配置以下设置：
    - **受信任网络策略：** 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：** 客户端在受信任的网络中终止 VPN 连接。此设置为默认值。
      - **连接：** 客户端在受信任的网络中启动 VPN 连接。
      - **不执行任何操作：** 客户端不执行任何操作。

    - **暂停：** 当用户在受信任网络外部建立 VPN 会话，然后进入配置为受信任的网络时，VPN 会话将暂停。当用户再次离开受信任网络时，会话将恢复。此设置消除了离开受信任网络后重新建立 VPN 会话的需要。

  - **不受信任的网络策略：** 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：** 客户端在不受信任的网络中启动 VPN 连接。
    - **不执行任何操作：** 客户端在不受信任的网络中启动 VPN 连接。此选项禁用始终开启的 VPN。

- **受信任的域：** 对于客户端位于受信任网络中时网络接口拥有的每个域后缀，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，或单击 **取消** 以不保存域。

- **受信任的服务器：** 对于客户端位于受信任网络中时网络接口拥有的每个服务器地址，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，或单击 **取消** 以不保存服务器。

配置适用于 Android 的 Citrix SSO 协议

- **连接名称：** 键入 VPN 连接的名称。此字段为必填项。
- **服务器名称或 IP 地址：** 键入 NetScaler 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该类型出现的任何字段：

  - **用户名**和**密码**：为**身份验证类型**为**密码**或**密码和证书**的 VPN 键入您的凭据。可选。如果您不提供 VPN 凭据，Citrix VPN 应用程序会提示输入用户名和密码。
  - **身份凭据**：显示在**身份验证类型**为**证书**或**密码和证书**时。在列表中，选择一个身份凭据。

- **启用每应用 VPN**：选择是否启用每应用 VPN。如果您不启用每应用 VPN，所有流量都将通过 Citrix VPN 隧道。如果您启用每应用 VPN，请指定以下设置。默认值为**关闭**。

  - **允许列表**或**阻止列表**：如果为**允许列表**，则允许列表中的所有应用程序都将通过此 VPN 隧道。如果为**阻止列表**，则除了阻止列表中的应用程序外，所有应用程序都将通过此 VPN 隧道。
  - **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包名称列表。

- **自定义 XML**：单击**添加**，然后键入自定义参数。Citrix Endpoint Management 支持 Citrix VPN 的以下参数：
  - **DisableUserProfiles**：可选。要启用此参数，请为**值**键入**是**。如果启用，Citrix Endpoint Management 不会显示用户添加的 VPN 连接，并且用户无法添加连接。此设置为全局限制，适用于所有 VPN 配置文件。
  - **userAgent**：一个字符串值。您可以指定一个自定义的用户代理字符串，以便在每个 HTTP 请求中发送。指定的自定义用户代理字符串将附加到现有的 Citrix VPN 用户代理。
  - **IsAlwaysOnVpn**：可选。此属性确定 VPN 配置文件是否为“始终开启 VPN”配置文件。设置为**是**表示 VPN 配置文件是“始终开启 VPN”配置文件，默认值为**否**。只有一个 VPN 配置文件可以将此属性设置为**是**，以确保“始终开启 VPN”可靠运行。

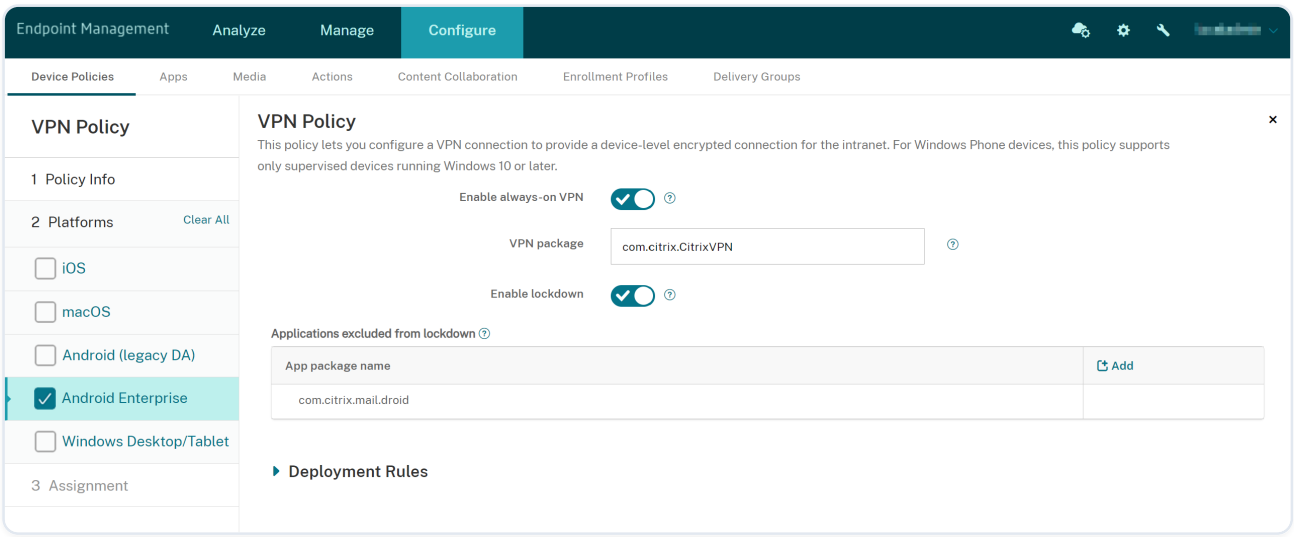
配置 VPN 以支持 NAC

1. 使用**连接类型**为**自定义 SSL**来配置 NAC 筛选器。
2. 指定**连接名称**为**VPN**。
3. 对于**自定义 XML**，单击**添加**并执行以下操作：
   - **参数名称**：键入 **XenMobileDeviceId**。此字段是用于基于 Citrix Endpoint Management 中的设备注册进行 NAC 检查的设备 ID。如果 Citrix Endpoint Management 注册并管理设备，则允许 VPN 连接。否则，在建立 VPN 时将拒绝身份验证。
   - **值**：键入 **DeviceID_${device.id}**，这是参数 **XenMobileDeviceId** 的值。
   - 单击“**保存**”以保存参数。

配置适用于 Android Enterprise 的 VPN

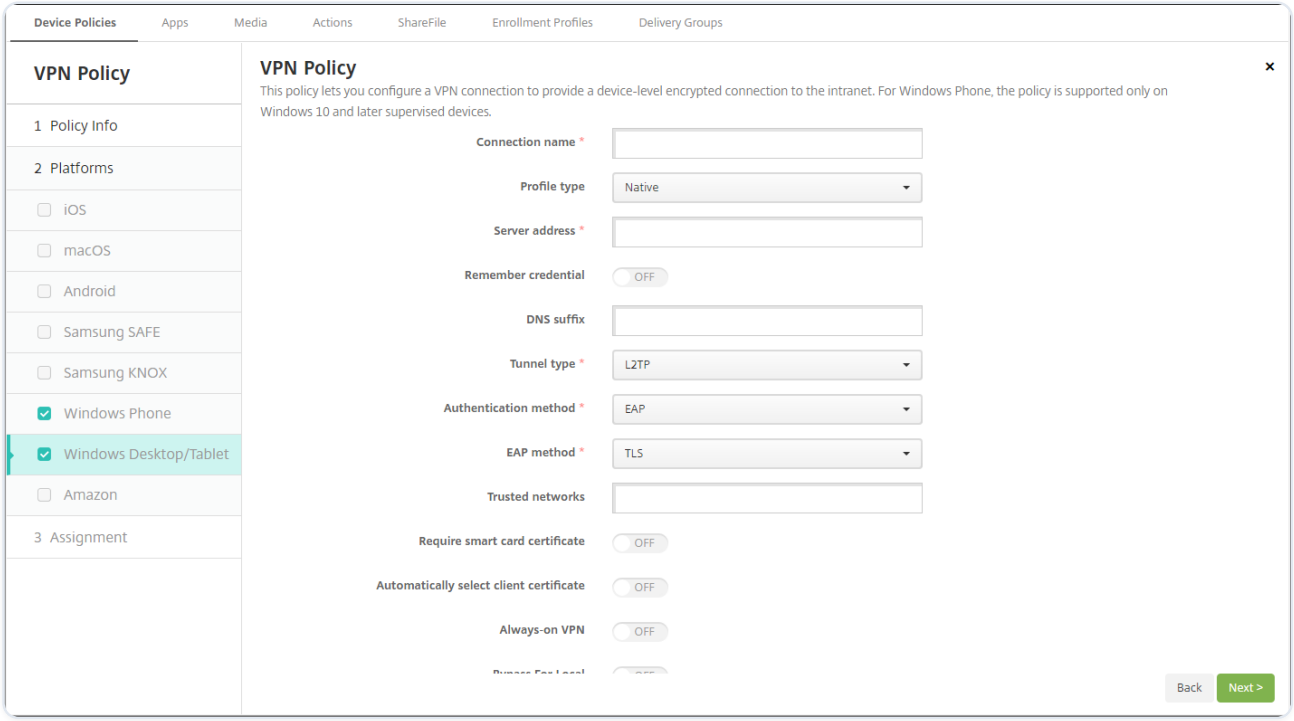
要为 Android Enterprise 设备配置 VPN，请为 Citrix SSO 应用程序创建 Android Enterprise 托管配置设备策略。请参阅配置适用于 Android Enterprise 的 VPN 配置文件。

Android 企业版设置



- **启用始终开启的 VPN：**选择 VPN 是否始终开启。默认值为“**关**”。启用后，VPN 连接将保持开启状态，直到用户手动断开连接。
- **VPN 程序包** 键入设备使用的 VPN 应用程序的程序包名称。
- **启用锁定：**如果禁用，则在 VPN 连接不存在时，任何应用程序都无法访问网络。如果启用，则即使 VPN 连接不存在，您在以下设置中配置的应用程序也可以访问网络。适用于 Android 10 及更高版本的设备。
- **从锁定中排除的应用程序：**单击“**添加**”以键入要绕过锁定设置的应用程序的程序包名称。

视窗桌面/平板电脑设置

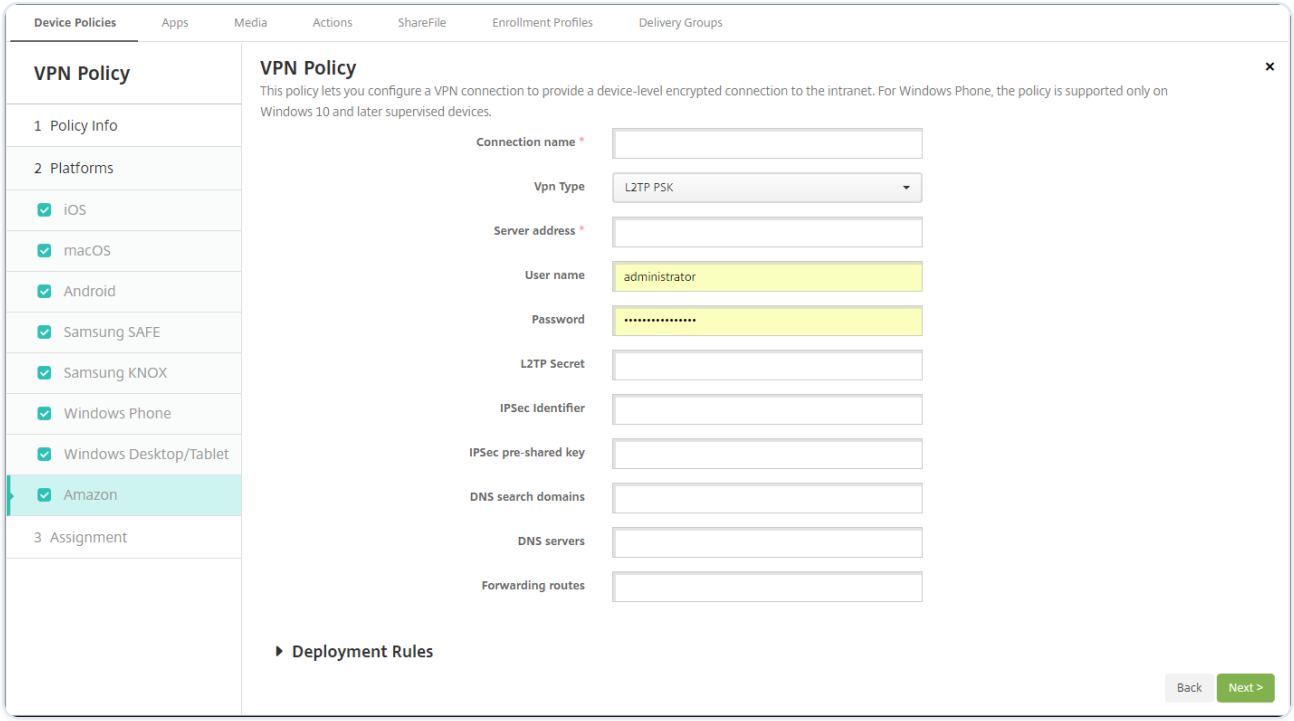


- **连接名称：**输入连接的名称。此字段为必填项。

- **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：**这些设置适用于用户 Windows 设备中内置的 VPN。
  - **服务器地址：**键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填项。
  - **记住凭据：** 选择是否缓存凭据。默认值为“**关**”。启用后，凭据将尽可能缓存。
  - **DNS 后缀：** 键入 DNS 后缀。
  - **隧道类型：** 在列表中，选择要使用的 VPN 隧道类型。默认值为“**L2TP**”。可能的选项包括：
    - **L2TP：** 带预共享密钥身份验证的第 2 层隧道协议。
    - **PPTP：** 点对点隧道协议。
    - **IKEv2：** Internet 密钥交换版本 2。
  - **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：** 可扩展身份验证协议。
    - **MSChapV2：** 使用 Microsoft 质询握手身份验证协议进行相互身份验证。当您为隧道类型选择“**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
  - **受信任的网络：** 键入以逗号分隔的网络列表，这些网络不需要 VPN 连接即可访问。例如，当用户位于公司无线网络上时，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。
  - **始终开启 VPN：** 选择 VPN 是否始终开启。默认值为“**关闭**”。启用后，VPN 连接将保持开启状态，直到用户手动断开连接。
  - **本地绕过：** 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：** 这些设置适用于从 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。此字段为必填项。

- **记住凭据：** 选择是否缓存凭据。默认值为“**关闭**”。启用后，凭据将尽可能缓存。
- **DNS 后缀：** 键入 DNS 后缀。
- **客户端应用 ID：** 键入 VPN 插件的程序包系列名称。
- **插件配置文件 XML：** 通过单击“**浏览**”并导航到文件位置来选择要使用的自定义 VPN 插件配置文件。有关格式和详细信息，请联系插件提供商。
- **受信任的网络：** 键入以逗号分隔的网络列表，这些网络无需 VPN 连接即可访问。例如，当用户位于公司无线网络中时，他们可以直接访问受保护的资源。
- **始终开启 VPN：** 选择 VPN 是否始终开启。默认值为“**关闭**”。启用后，VPN 连接将保持开启状态，直到用户手动断开连接。
- **本地绕过：** 键入地址和端口号以允许本地资源绕过代理服务器。

Amazon 设置



- **连接名称：** 输入连接名称。
- **VPN 类型：** 选择连接类型。可能的选项包括：
  - **L2TP PSK：**带预共享密钥身份验证的二层隧道协议。此设置为默认值。
  - **L2TP RSA：**带 RSA 身份验证的二层隧道协议。
  - **IPSEC XAUTH PSK：**带预共享密钥和扩展身份验证的互联网协议安全。
  - **IPSEC HYBRID RSA：**带混合 RSA 身份验证的互联网协议安全。
  - **PPTP：**点对点隧道协议。

以下各节列出了上述每种连接类型的配置选项。

配置 Amazon 的 L2TP PSK 设置

- **服务器地址：**键入 VPN 服务器的 IP 地址。
- **用户名：**键入可选的用户名。
- **密码：**键入可选的密码。
- **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**：如果您的企业 VPN 服务器支持转发路由，对于要使用的每个转发路由，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，或单击 **取消** 以不保存路由。

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**：键入可选的用户名。
- **密码**：键入可选的密码。
- **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**：如果您的企业 VPN 服务器支持转发路由，对于要使用的每个转发路由，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。
  - 点击 **保存** 以保存路由，或点击 **取消** 以不保存路由。

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：** 键入可选的用户名。
- **密码：** 键入可选的密码。
- **IPSec 标识符：** 键入用户在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：** 如果您的公司 VPN 服务器支持转发路由，则对于要使用的每个转发路由，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。
  - 点击 **保存** 以保存路由，或点击 **取消** 以不保存路由。

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：** 键入可选的用户名。
- **密码：** 输入可选密码。
- **DNS 搜索域：** 输入用户设备的搜索域列表可以匹配的域。
- **DNS 服务器：** 输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：** 如果您的企业 VPN 服务器支持转发路由，则对于要使用的每个转发路由，请单击“**添加**”并执行以下操作：
  - **转发路由：** 输入转发路由的 IP 地址。
  - 单击“**保存**”以保存路由，或单击“**取消**”以不保存路由。

配置 Amazon 的 IPSEC HYBRID RSA 设置

- **服务器地址：** 输入 VPN 服务器的 IP 地址。
- **用户名：** 输入可选用户名。
- **密码：** 输入可选密码。

- **DNS 搜索域：** 输入用户设备的搜索域列表可以匹配的域。
- **DNS 服务器：** 输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：** 如果您的企业 VPN 服务器支持转发路由，则对于要使用的每个转发路由，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，或单击**取消**以不保存路由。

配置 Amazon 的 PPTP 设置

- **服务器地址：** 键入 VPN 服务器的 IP 地址。
- **用户名：** 键入可选的用户名。
- **密码：** 键入可选的密码。
- **DNS 搜索域：** 键入用户设备的搜索域列表可以匹配的域。
- **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) 启用数据加密。默认值为**关**。
- **转发路由：** 如果您的企业 VPN 服务器支持转发路由，则对于要使用的每个转发路由，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，或单击**取消**以不保存路由。

壁纸设备策略

壁纸设备策略允许您添加 .png 或 .jpg 文件，以在 iOS 设备的锁定屏幕、主屏幕或两者上设置壁纸。此策略仅适用于受监管的设备。要在 iPad 和 iPhone 上使用不同的壁纸，您需要创建不同的壁纸策略并将其部署给相应的用户。

下表列出了 Apple 推荐的 iOS 设备图像尺寸。

iPhone

设备	图像尺寸（像素）
苹果手机 12 Pro Max	2778 x 1284

设备	图像尺寸（像素）
iPhone 12 和 iPhone 12 Pro	2532 x 1170
苹果手机 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
苹果手机 XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 第二代	1334 x 750
苹果手机 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
爱疯 8 普拉斯	1334 x 750
iPhone 8	1334 x 750

iPad

设备	图像尺寸（像素）
iPad Pro（第 1、2、3 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

- **应用到：** 在列表中，选择**锁定屏幕**、**主屏幕（图标列表）**或**锁定和主屏幕**以设置壁纸显示位置。
- **壁纸文件：** 要选择壁纸文件，请单击**浏览**，然后导航到文件位置。

Web 内容筛选设备策略

您可以使用 Apple 自动筛选功能，通过添加到允许或阻止列表中的特定站点来筛选 iOS 设备上的 Web 内容。Web 内容筛选设备策略仅适用于处于监督模式的 iOS 设备。有关将 iOS 设备置于监督模式的信息，请参阅使用 Apple Configurator 2 部署设备。

> **注意：**
>
> - Android 设备不支持 Web 内容筛选。
> - 从 iOS 16.5 及更高版本开始，Web 内容筛选设备策略停止识别允许列表中的 `https://localhost`。这会导致某些应用程序无响应。此外，将 URL 的派生形式（例如 `http://localhost:`、`http://localhost:*` 等）添加到允许列表也无法解决此问题。

> 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

- **筛选器类型：** 在下拉列表中单击 **Built-in（内置）** 或 **Plug-in（插件）**，然后按照所选选项的后续步骤操作。默认值为 **Built-in（内置）**。

内置筛选器类型

- **Web 内容筛选器**
  - **自动筛选器已启用：** 是否使用 Apple 自动筛选功能分析网站是否存在不当内容。默认值为 **Off（关）**。
  - **允许的 URL：** 当**自动筛选器已启用**设置为**关**时，此列表将被忽略。当**自动筛选器已启用**设置为**开**时，无论自动筛选器是否允许访问，此列表中的项目始终可访问。对于要添加到允许列表的每个 URL，请单击**添加**并执行以下操作：
    - 键入允许的网站的 URL。您必须在网址前添加 `https://` 或 `https://`。

    - 单击 **Save（保存）** 将网站保存到允许列表，或单击 **Cancel（取消）** 不保存。
  - **阻止的 URL：** 此列表中的项目始终被阻止。对于要添加到阻止列表的每个 URL，请单击**添加**并执行以下操作：
    - 输入要阻止的网站的 URL。您必须在网址前添加 `https://` 或 `https://`。
    - 单击**保存**可将网站保存到阻止列表，或单击**取消**不保存。

- **书签允许列表**
  - **书签允许列表：**指定用户可以访问的站点。要启用对网站的访问，请添加其 URL。
    - **URL：**用户可以访问的每个网站的 URL。例如，要启用对 Citrix Secure Hub 商店的访问，请将 Citrix Endpoint Management 服务器 URL 添加到 **URL** 列表。您必须在网址前添加 `https://` 或 `https://`。此字段为必填项。
    - **书签文件夹：**输入可选的书签文件夹名称。如果此字段留空，则书签将添加到默认书签目录。
    - **标题：**输入网站的描述性标题。例如，对于 URL `https://google.com`，键入“Google”。
    - 单击**保存**可将网站保存到允许列表，或单击**取消**不保存。

插件筛选器类型

- **筛选器名称：**输入筛选器的唯一名称。
- **标识符：**输入提供筛选服务的插件的捆绑包 ID。
- **服务地址：**输入可选的服务器地址。有效格式为 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：在下拉列表中单击一个可选的身份证书，该证书将用于向服务验证用户身份。默认值为无**。
- **筛选 WebKit 流量：**选择是否筛选 WebKit 流量。
- **筛选套接字流量：** 选择是否筛选套接字流量。
- **自定义数据：** 对于要添加到 Web 过滤器的每个自定义密钥，请单击 **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** 以不保存。

- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括 **选择日期** 和 **距离删除的持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **距离删除的持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

Web 剪辑设备策略

您可以将网站快捷方式（即 Web 剪辑）放置在用户设备上，使其与应用程序一同显示。您可以为 iOS、iPadOS、macOS 和 Android 设备指定自己的图标来表示 Web 剪辑。Windows 平板电脑仅需要标签和 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。如果您限制了 iOS 上的应用程序访问，请确保配置限制设备策略以允许 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：** 键入将与 Web 剪辑一同显示的标签。
- **URL：** 键入与 Web 剪辑关联的 URL。URL 必须以协议开头，例如 `https://server`。
- **可移除：** 选择用户是否可以移除 Web 剪辑。默认值为“**关**”。共享 iPad 不支持此选项。
- **要更新的图标：** 通过单击“**浏览**”并导航到文件位置来选择要用于 Web 剪辑的图标。
- **预合成图标：** 选择图标是否应用了效果（圆角、阴影和反光）。默认值为“**关**”，这会添加效果。
- **全屏：** 选择链接的网页是否以全屏模式打开。此设置还允许 iPad 仅打开单个网站。或者，要将 iPad 设置为在 Kiosk 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 配置为自助服务终端。默认值为“**关**”。
- **策略设置**
  - **移除策略：** 选择一种计划策略移除的方法。可用选项包括“**选择日期**”和“**移除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略移除前的持续时间。仅适用于 iOS 6.0 及更高版本。

- **配置文件范围：** 选择策略是应用于用户还是整个系统。默认值为“**系统**”。仅适用于 iOS 9.3 及更高版本。

macOS 设置

- **标签：**键入将与 Web 剪辑一起显示的标签。
- **URL：**键入与 Web 剪辑关联的 URL。URL 必须以协议开头，例如 `https://server`。
- **要更新的图标：**通过单击“浏览”并导航到文件位置来选择要用于 Web 剪辑的图标。
- **策略设置**
  - **删除策略：选择一种计划策略删除的方法。可用选项包括选择日期和删除前持续时间（小时）**
    - **选择日期：**单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：您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、需要密码或从不。**如果选择**需要密码**，请在**删除密码**字段中键入密码。

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：**键入将与 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：如果定义图标为开，**请通过单击**浏览**并导航到文件位置来选择要使用的图标文件。

视窗桌面/平板电脑设置

- **名称：** 键入将与 Web 剪辑一起显示的标签。
- **URL：** 键入与 Web 剪辑关联的 URL。

Windows Agent 设备策略

使用 Windows Agent 设备策略在托管的 Windows 桌面和平板电脑上运行 PowerShell 脚本。您可以指向作为企业应用上传到 Citrix Endpoint Management 的脚本文件以及托管脚本的其他服务器。有关添加企业应用的信息，请参阅添加应用。

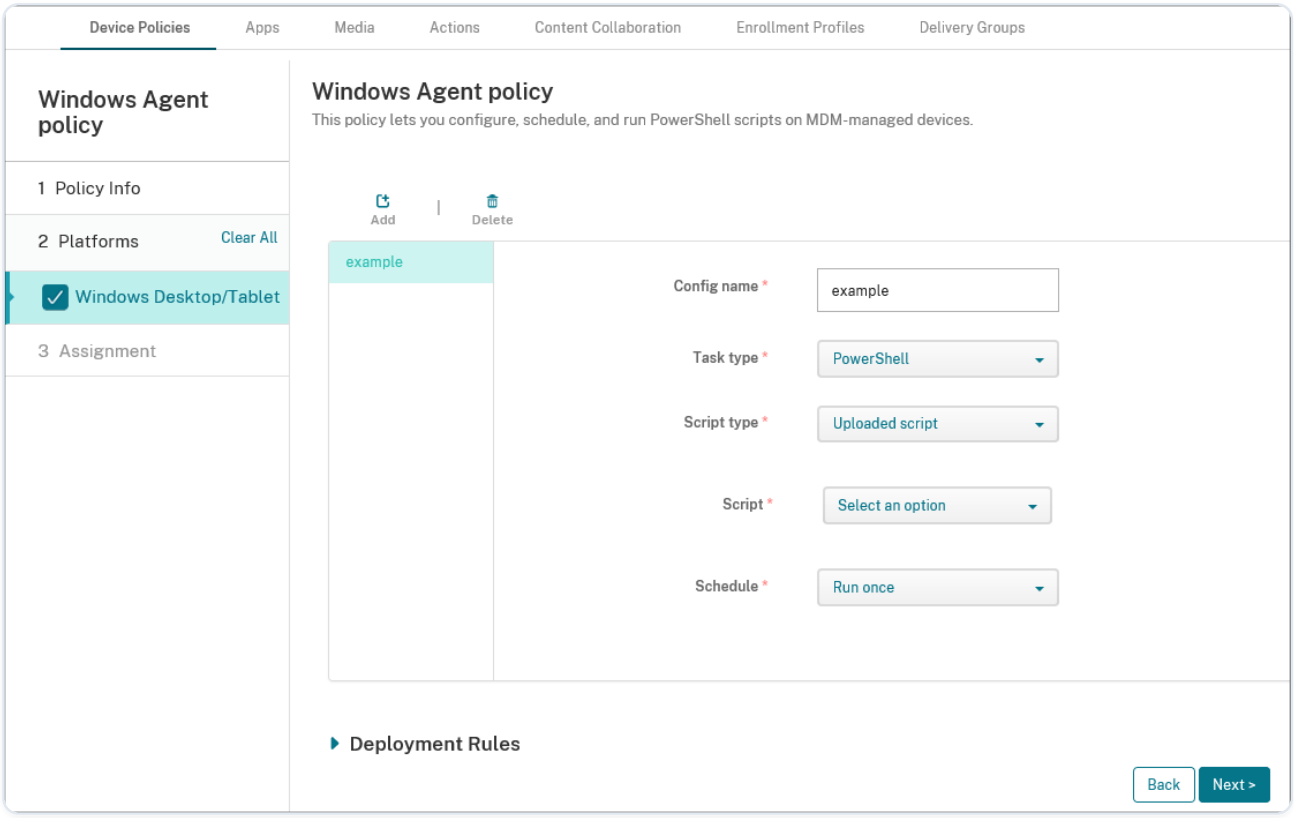
所有脚本都在特权状态下运行，您无需以管理员身份运行脚本。

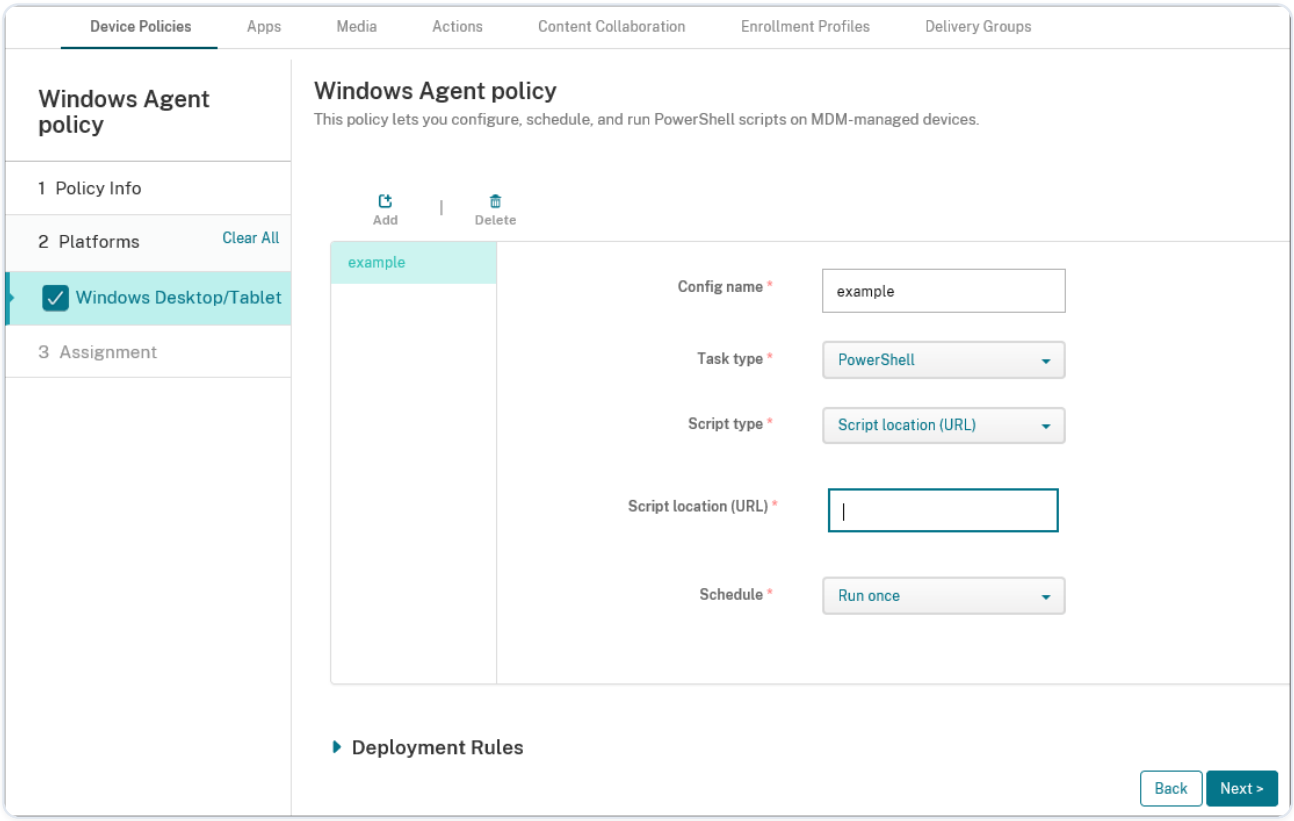
部署并运行脚本后，您可以根据脚本的结果配置自动化操作。例如，您运行一个脚本来监视注册表项并返回结果。根据返回的结果，将运行一个自动化操作。该操作授予或拒绝应用访问权限，将设备标记为不合规，或产生其他影响。

您还可以通过配置指向 .msi 文件和 .mst 文件的 PowerShell 脚本，使用此策略部署自定义 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 桌面和平板电脑设置





- **配置名称：** 为您的配置键入一个描述性名称。
- **任务类型：** 选择 **PowerShell**。
- **脚本类型：** 对于已上传到 Citrix Endpoint Management 的脚本，请选择 **已上传脚本**；对于外部托管的脚本，请选择 **脚本位置 (URL)**。有关如何将脚本上传到 Citrix Endpoint Management 的更多信息，请参阅将 `Win32` 应用添加为企业应用。
    - **选择脚本：** 如果您选择了 **已上传脚本**，请选择要运行的脚本。
    - **脚本位置 (URL)：** 如果您选择了 **脚本位置 (URL)**，请输入要运行的脚本的位置。此 URL 必须以有效负载形式提供脚本。Citrix Endpoint Management 不支持以 JavaScript 下载形式提供脚本的 URL。脚本还必须是公开可用的。
- **计划：** 选择 **运行一次** 以运行所选脚本一次，或选择 **定期运行** 以定期运行脚本。
    - **运行间隔（小时）：** 键入脚本运行之间的小时数。

要检查脚本状态，请在控制台中导航到**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，通过单击**Windows Agent**标题下的**下载**，可以检查脚本的状态。

部署 PowerShell 脚本以触发自动化操作

1. 创建 PowerShell 脚本以监视注册表项。以下 PowerShell 脚本检查防火墙是否已启用。

```
$body = @{}

$firewallEnabled = Get-ItemPropertyValue HKLM:
\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPoli
cy\StandardProfile -Name EnableFirewall

if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"

} else {

$body["firewallEnabled"]="false"

}

$body | ConvertTo-Json -Depth 10
```

此脚本返回的值为

```
{

    "firewallEnabled":  "true"

}
```

或

```
{

    "firewallEnabled":  "false"

}
```

2. 将脚本作为企业应用程序上传到 Citrix Endpoint Management 控制台，或将脚本托管在可访问的 URL 上。
3. 配置本文中介绍的 Windows Agent 设备策略。确保脚本计划立即运行。
4. 脚本运行后，确定脚本状态。

    a. 在控制台中导航到**管理 > 设备**。

b. 选择设备以检查其脚本状态，然后单击**编辑**。

c. 单击**Windows Agent**标题下的**下载**。

5. 根据收到的状态配置自动化操作。有关配置自动化操作的详细信息，请参阅根据 Windows Agent 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 Agent 设备策略创建的特定自动化操作。

Windows GPO 配置设备策略

Windows GPO 配置设备策略允许您执行以下操作：

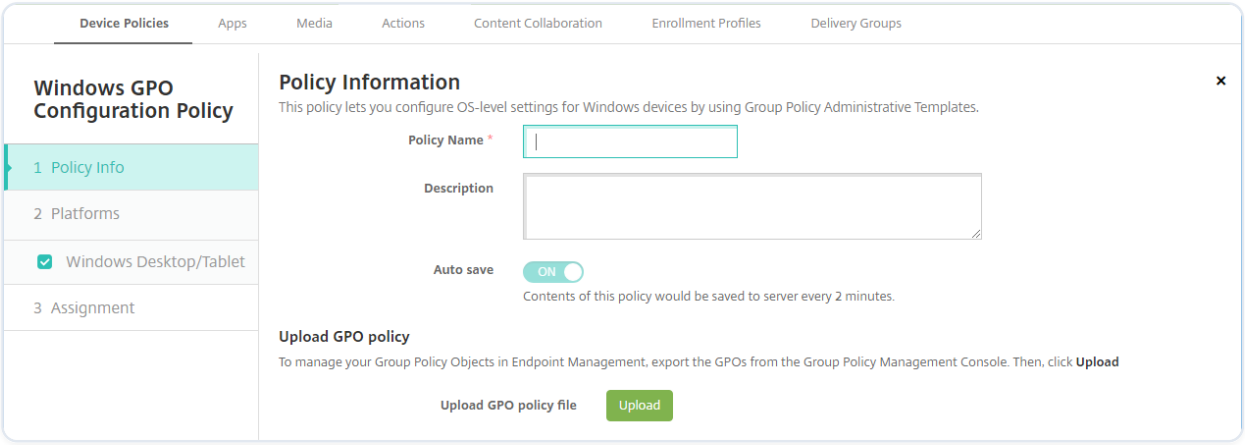
- 使用 Citrix Endpoint Management 控制台导入组策略对象 (GPO) 并将其部署到 Windows 10 和 Windows 11 设备。
- 为 Citrix Workspace Environment Management 支持的任何 Windows 设备配置 GPO。
- 在设备和用户级别配置 GPO。

导入 GPO 以部署到 Windows 10 和 Windows 11 设备

您无需依赖 AD 管理员使用组策略管理控制台来管理 GPO，而是可以通过 Citrix Endpoint Management 控制台导入和部署 GPO。

要在 Citrix Endpoint Management 中创建 GPO 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 并向您提供文件。
2. 在 Citrix Endpoint Management 控制台中，转至 **Configure > Device Policies**（配置 > 设备策略），然后创建 **Windows GPO Configuration**（Windows GPO 配置）策略。
3. 单击 **Upload**（上载），找到文件，然后单击 **Open**（打开）以导入文件。



有关配置 GPO 的信息，请参阅本文中的 Windows 桌面和平板电脑设置。

对 GPO 进行配置，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。Citrix Endpoint Management 将策略推送到 Citrix WEM 服务。然后，WEM 服务通过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。

有关安装 Workspace Environment Management 代理的信息，请参阅 安装和配置。

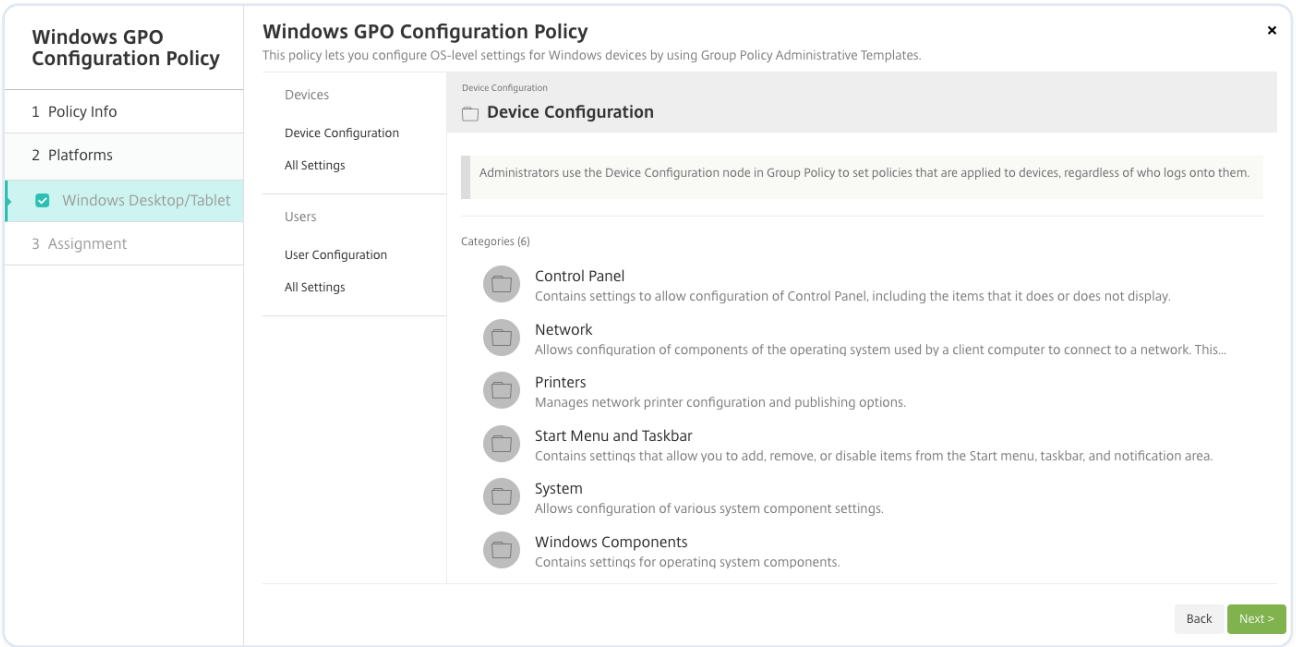
此策略使用所有 Windows OS ADMX 文件。如果要上传第三方 ADMX 文件，请使用应用程序配置设备策略。有关上传第三方 ADMX 文件的更多信息，请参阅 应用程序配置设备策略。

- 您可以将 GPO 配置推送到 WEM 支持的任何设备，即使 Citrix Endpoint Management 不原生支持该设备。有关支持的设备列表，请参阅 操作系统要求。
- 此策略要求设备已安装并配置 WEM 代理。无需对设备进行 MDM 或 MAM 注册。
- Citrix Endpoint Management 通过 WEM 通道推送 GPO 设置。（Microsoft 不支持通过 MDM 通道推送设备级设置。）接收 Windows GPO 配置设备策略的设备在名为 WEM 的 Citrix Endpoint Management 模式下运行。在已注册设备的“**管理 > 设备**”列表中，WEM 管理设备的“**模式**”列显示“**WEM**”。

要添加或配置此策略，请转至“**配置 > 设备策略**”。有关更多信息，请参阅 设备策略。

Windows 桌面和平板电脑设置

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 Windows 设备的 Windows GPO。您可以修改“**设备配置**”和“**用户配置**”。策略以树形结构列出。单击“**所有设置**”以显示所有设置。有关这些设置的信息，请从 Microsoft 下载 GPO 参考表。

要配置设置，您首先需要启用它。在配置过程中，Citrix Endpoint Management 会自动保存更改，以便这些设置能够持久存在。如果您尝试在设置保存之前离开页面，则会弹出一条消息，指示存在未保存的更改。

如果一个设置有两个选项，则会出现单选按钮选择。如果选项多于两个，则会出现菜单。

注意：

如果您需要检查已配置的设置，可以执行以下操作。

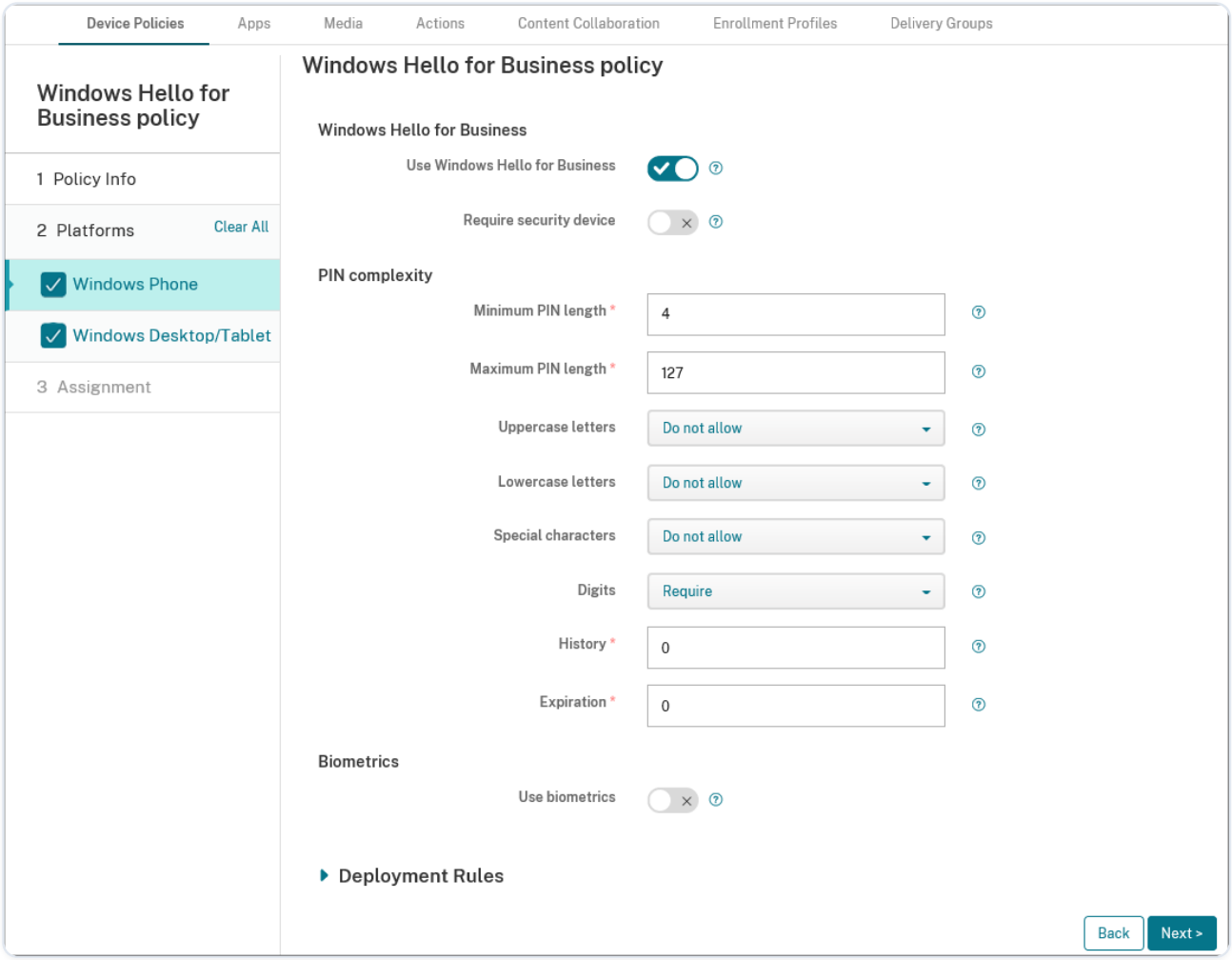
1. 在 Citrix Endpoint Management 控制台中，打开要编辑的“**Windows GPO 配置**”策略。
2. 在“**设备**”或“**用户**”下，选择“**所有设置**”。
3. 按**状态**对表格进行排序，升序排列。所有未配置的策略的状态为**未配置**。您配置的策略会列在顶部。

适用于企业的 Windows Hello 设备策略

适用于企业的 Windows Hello 允许用户使用其 Active Directory 或 Azure Active Directory 帐户登录 Windows 设备。您可以使用**适用于企业的 Windows Hello**设备策略来启用此功能，以便用户可以在其设备上预配适用于企业的 Windows Hello。此策略还允许您配置密码限制和其他安全功能。

转到**配置 > 设备策略**以添加**适用于企业的 Windows Hello**设备策略。配置以下设置：

适用于 Windows 的桌面/平板电脑设置



- **使用适用于企业的 Windows Hello：**启用此功能以允许用户在其设备上预配适用于企业的 Windows Hello。
- **要求使用安全设备：**要求用户拥有受信任的平台模块 (TPM) 才能登录。
- **最小/最大 PIN 长度：**用户 PIN 的最小和最大长度。**最小 PIN 长度**默认为 **4**。**最大 PIN 长度**默认为 **127**。
- **大写字母、小写字母、特殊字符：选择是允许、要求**还是**不允许**每种字符类型。默认为**不允许**。
- **数字：是允许、要求**还是**不允许**数字。默认为**要求**。
- **历史记录：**用户不能重复使用的过去 PIN 的数量。默认为 **0**，表示用户可以重复使用所有 PIN。
- **过期：**用户必须更改其 PIN 之前的天数。默认为 **0**，表示 PIN 不会过期。
- **使用生物识别：**允许使用生物识别代替 PIN 进行用户登录。

添加应用

将应用添加到 Citrix Endpoint Management 可提供移动应用管理 (MAM) 功能。Citrix Endpoint Management 有助于应用交付、软件许可、配置和应用生命周期管理。

启用 MDX 应用是将某些类型的应用分发到用户设备的重要组成部分。有关 MDX 的介绍，请参阅 Citrix Endpoint Management 组件 和 MAM SDK 概述。

- Citrix 建议使用 MAM SDK 启用 MDX 应用。或者，您可以继续 MDX 封装应用，直到 MDX Toolkit 弃用。请参阅 弃用。
- 您不能使用 MDX Toolkit 封装 Citrix 移动生产力应用。从 Citrix 下载中获取移动生产力应用 MDX 文件。

将应用添加到 Citrix Endpoint Management 控制台时，您将：

- 配置应用设置
- （可选）将应用整理到类别中，以便在 Citrix Secure Hub 中进行组织
- （可选）定义工作流，要求在允许用户访问应用之前进行审批
- 将应用部署到用户

本文介绍了添加应用的通用工作流。有关平台特定信息，请参阅以下文章：

- 分发 Android Enterprise 应用
- 分发 Apple 应用

> **重要提示：**
>
> Citrix Endpoint Management 支持添加和维护最多 300 个应用。超出此限制会导致系统不稳定。

应用类型和功能

下表总结了您可以使用 Citrix Endpoint Management 部署的应用类型。

应用类型	来源	备注	请参阅
MDX	您为用户开发的 iOS 和 Android 应用。Citrix 移动生产力应用。	使用 MAM SDK 开发 iOS 或 Android 应用，或使用 MDX Toolkit 封装它们。对于移动生产力应用，请从 Citrix 下载中下载公共应用商店 MDX 文件。然后将应用添加到 Citrix Endpoint Management。	添加 MDX 应用
公共应用商店	来自 Google Play 或 Apple App Store 等公共应用商店的免费或付费应用。	上传应用，启用 MDX 功能，然后将应用添加到 Citrix Endpoint Management。	添加公共应用商店应用
Web 和 SaaS	您的内部网络（Web 应用程序）或公共网络 (SaaS)。	Citrix Endpoint Management 提供从注册到 MDM 的 iOS 和 Android 设备到本机 SaaS 应用程序的移动单点登录。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
企业	未启用 MDX 的私有应用程序，包括 Win32 应用程序。已启用 MDX 的私有 Android Enterprise 应用程序。企业应用程序位于内容分发网络位置或 Citrix Endpoint Management 服务器中。	将应用程序添加到 Citrix Endpoint Management。	添加企业应用程序

应用类型	来源	备注	请参阅
Web 链接	Internet Web 地址、Intranet Web 地址或不需要单点登录的 Web 应用程序。	在 Citrix Endpoint Management 中配置 Web 链接。	添加 Web 链接

规划应用程序分发时，请考虑以下功能：

- 关于静默安装
- 关于必需和可选应用程序
- 关于应用程序类别
- 从 Citrix CDN 交付企业应用
- 启用 Microsoft 365 应用
- 应用工作流
- 应用商店和 Citrix Secure Hub 品牌
- 通过应用商店使用 Citrix Virtual Apps and Desktops™

关于静默安装

Citrix 支持 iOS、Android Enterprise 和 Samsung 应用的静默安装和升级。静默安装意味着用户不会收到安装部署到设备的应用的提示。应用会在后台自动安装。

实施静默安装的先决条件：

- 对于 iOS，请将受管 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，应用将安装在设备上的 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，您可以设置 Samsung MDM 许可证密钥设备策略以生成 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。

关于必需应用和可选应用

将应用添加到交付组时，您可以选择它们是可选的还是必需的。Citrix 建议将应用部署为**必需**。

- 必需应用会在用户设备上静默安装，从而最大程度地减少交互。启用此功能还允许应用自动更新。
- 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 Citrix Secure Hub 手动启动安装。

对于标记为必需的应用程序，用户可以在以下情况下及时收到更新：

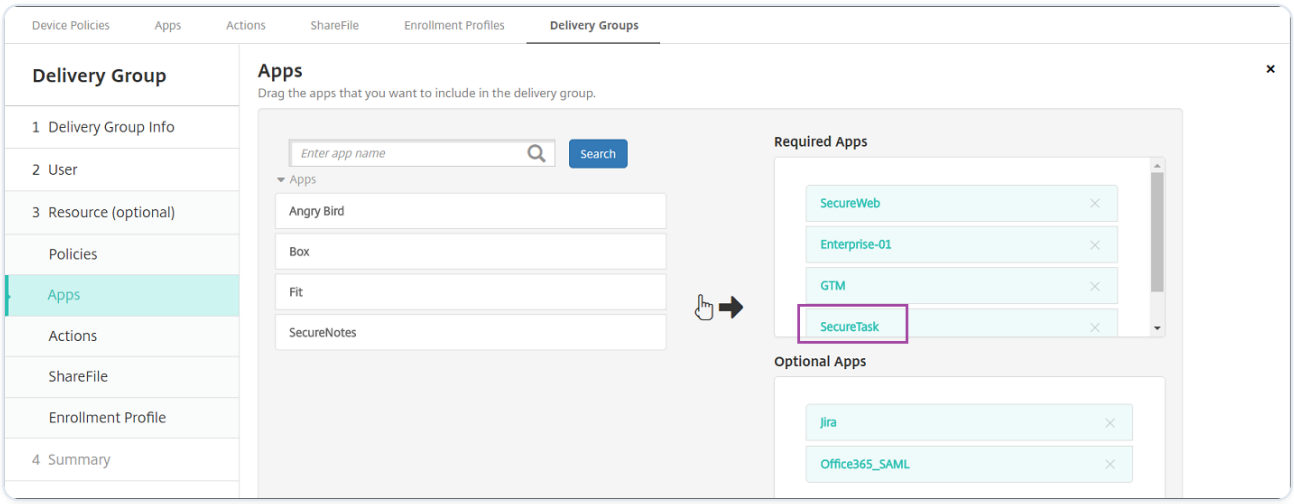
- 您上传了一个新应用程序并将其标记为必需。
- 您将现有应用程序标记为必需。
- 用户删除了一个必需的应用程序。
- Citrix Secure Hub 更新可用。

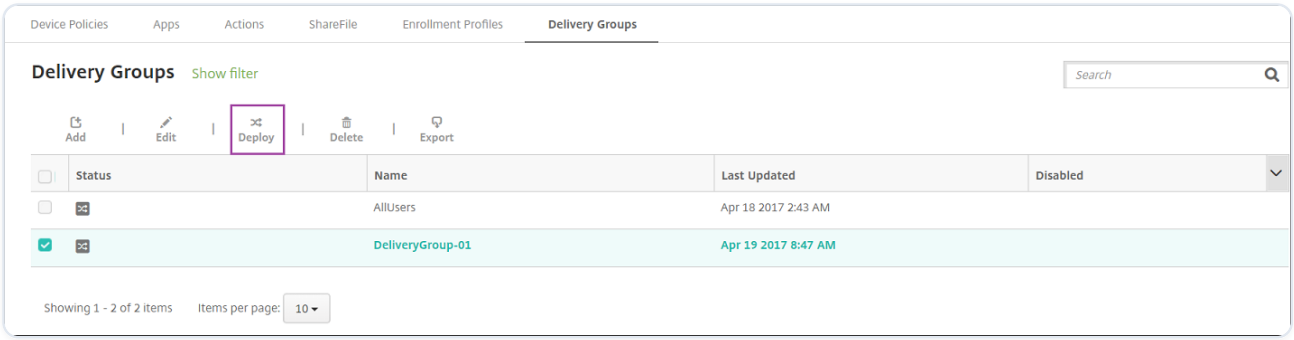
强制部署必需应用程序的要求

- 适用于 iOS 的 Citrix Secure Hub 10.5.15 和适用于 Android 的 10.5.20（最低版本）
- MAM SDK 或 MDX Toolkit 10.6（最低版本）
- 升级 Citrix Endpoint Management 和 Citrix Secure Hub 后：已注册设备的用户必须注销，然后重新登录 Citrix Secure Hub 才能获取所需的应用程序部署更新。

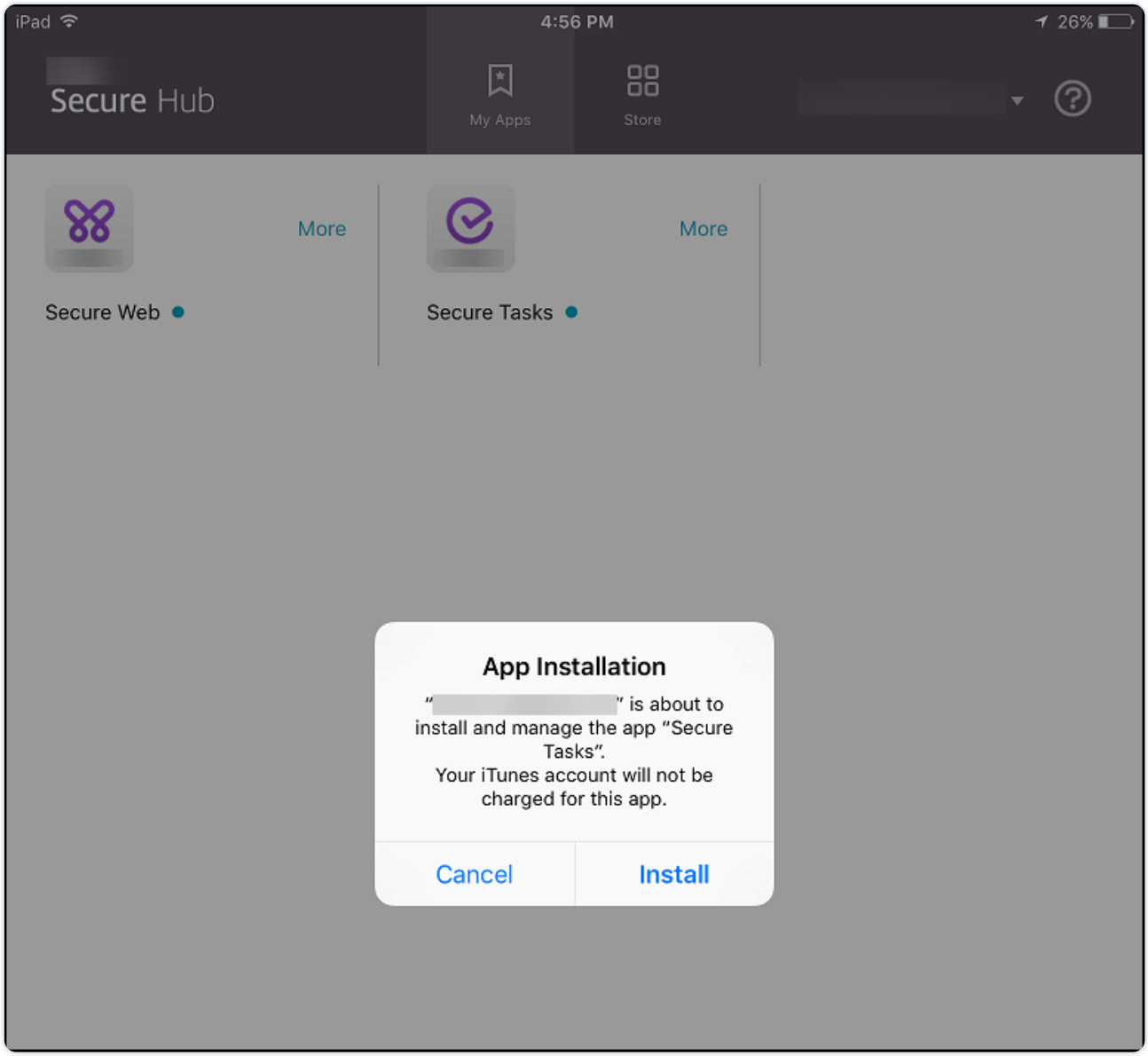
示例

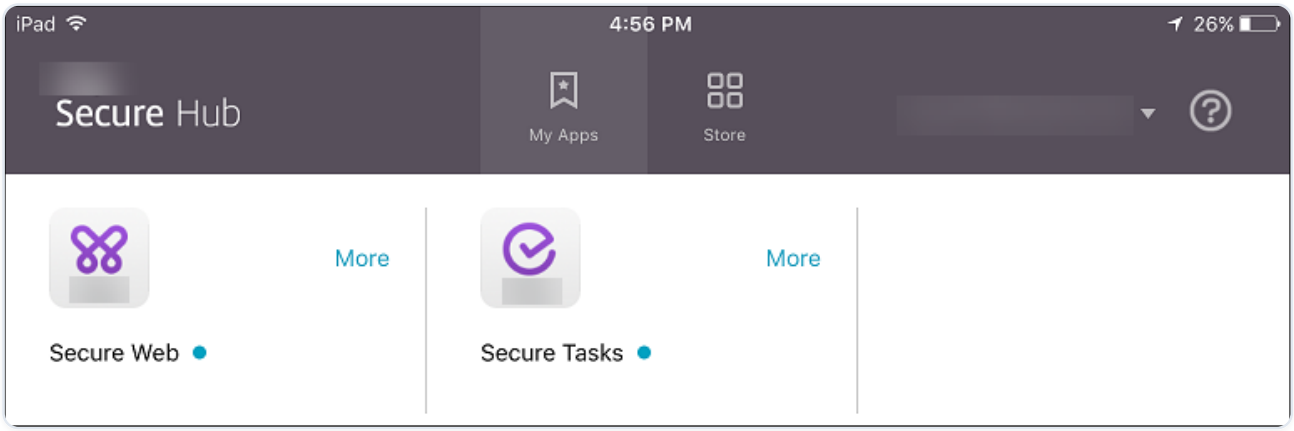
以下示例显示了将名为 Secure Tasks 的应用程序添加到交付组，然后部署该交付组的顺序。





示例应用程序 Secure Tasks 部署到用户设备后，Citrix Secure Hub 会提示用户安装该应用程序。





重要提示：

启用 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）会立即升级。即使您为应用程序更新宽限期配置了 MDX 策略，并且用户选择稍后升级应用程序，此升级也会发生。

适用于企业和公共应用商店应用程序的 iOS 必需应用程序工作流程

1. 在初始注册期间部署移动生产力应用程序。必需应用程序将安装在设备上。
2. 在 Citrix Endpoint Management 控制台上更新应用程序。
3. 使用 Citrix Endpoint Management 控制台部署必需应用程序。
4. 主屏幕上的应用程序已更新。对于公共应用商店应用程序，升级会自动开始。系统不会提示用户更新。
5. 用户从主屏幕打开应用程序。即使您设置了应用程序更新宽限期并且用户选择稍后升级应用程序，应用程序也会立即升级。

适用于企业应用程序的 Android 必需应用程序工作流程

1. 在初始注册期间部署移动生产力应用程序。必需应用程序将安装在设备上。
2. 使用 Citrix Endpoint Management 控制台部署必需应用程序。
3. 应用程序已升级。（Nexus 设备会提示安装更新，但三星设备会静默安装。）
4. 用户从主屏幕打开应用程序。即使您设置了应用程序更新宽限期并且用户选择稍后升级应用程序，应用程序也会立即升级。（三星设备会静默安装。）

Android 公共商店所需应用工作流程

1. 在初始注册期间部署移动生产力应用程序。所需应用程序将安装在设备上。

2. 在 Citrix Endpoint Management 控制台中更新应用程序。
3. 使用 Citrix Endpoint Management 控制台部署所需应用程序。或者，在设备上打开 Citrix Secure Hub 商店。更新图标将显示在商店中。
4. 应用程序升级自动开始。（Nexus 设备会提示用户安装更新。）
5. 在主屏幕上打开应用程序。应用程序已升级。系统不会提示用户宽限期。（三星设备会执行静默安装。）

卸载配置为必需的应用程序

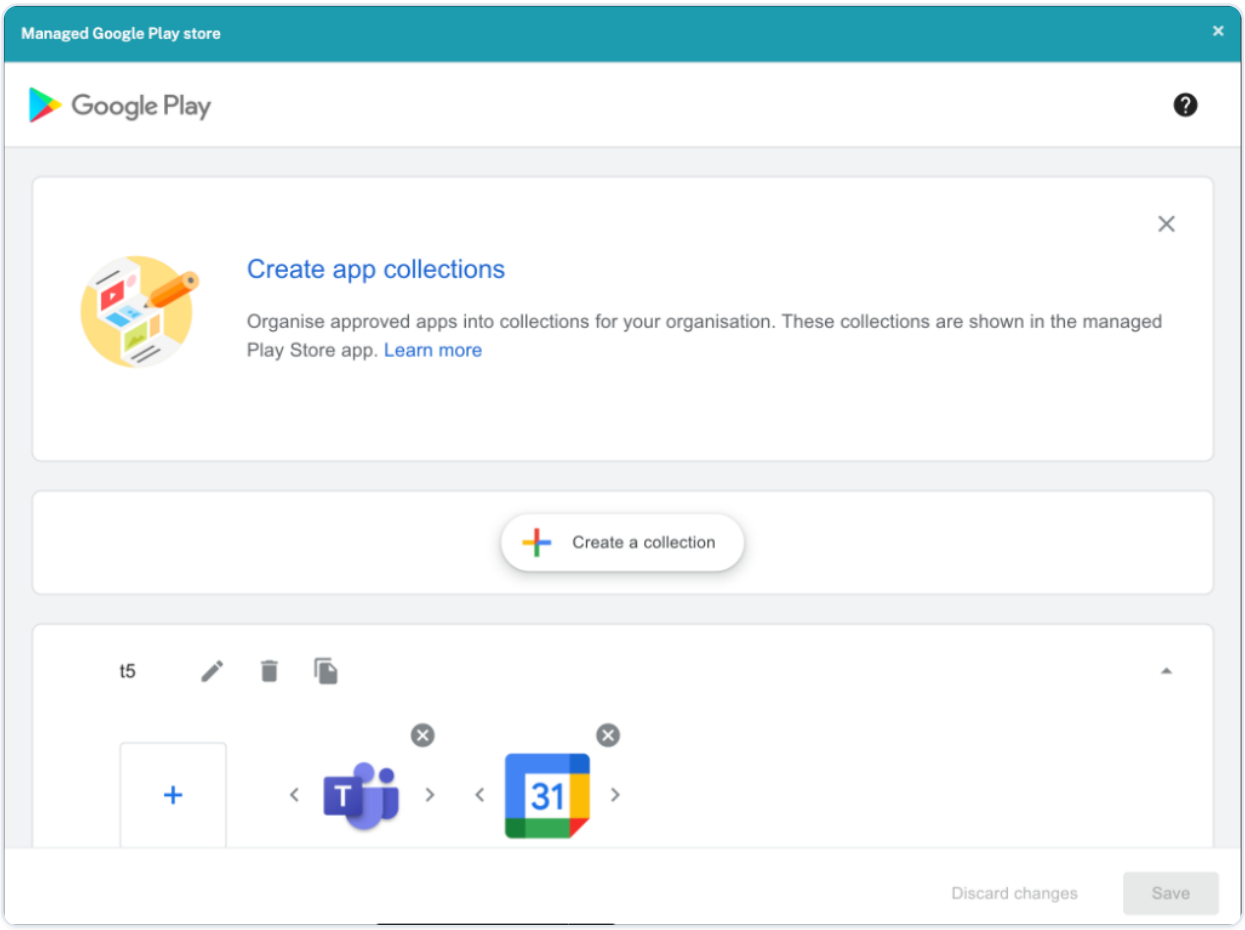
您可以允许用户卸载配置为必需的应用程序。转到 **Configure > Delivery Groups**，然后将应用程序从 **Required Apps** 移动到 **Optional Apps**。

建议： 使用特殊的交付组将应用程序临时更改为可选，以便特定用户可以卸载该应用程序。然后，您可以将现有必需应用程序更改为可选，将该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重新设置为必需。

组织应用程序 (Android Enterprise)

当用户登录到 Citrix Secure Hub 时，他们会收到您在 Citrix Endpoint Management 中设置的应用程序、Web 链接和商店的列表。在 Android Enterprise 中，您可以将这些应用程序组织到集合中，以允许用户仅访问某些应用程序、商店或 Web 链接。例如，您可以创建一个“财务”集合，然后将仅与财务相关的应用程序添加到该集合中。或者，您可以配置一个“销售”集合，并将销售应用程序分配给它。

1. 在 Citrix Endpoint Management 控制台中，单击 **Configure > Apps > Organize Apps**。“**Managed Google Play store**”窗口随即显示。



2. 单击 **Create a collection**，然后选择要添加到该集合的应用程序。
3. 添加完集合后，单击 **Save**。

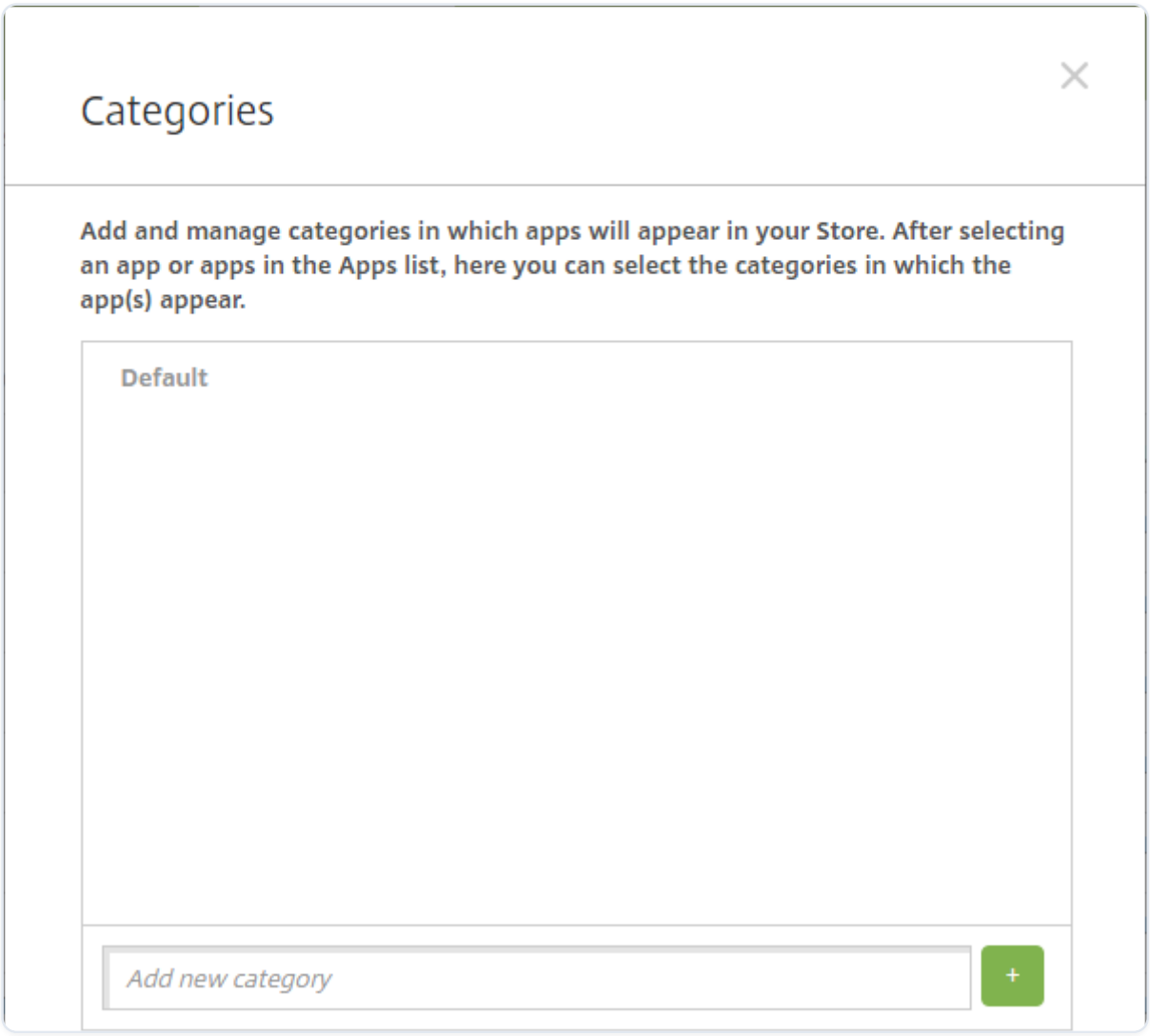
> **注意：**
>
> IT 管理员需要先批准某个应用，然后才能将其添加到“托管 Google Play”窗口上的集合中。IT 管理员可以通过转到 `<https://play.google.com/work>` 来批准应用。在将来的版本中，您无需先批准应用即可将其添加到集合中。

关于应用类别 (iOS 和 MDX)

用户登录 Citrix Secure Hub 时，他们会收到您在 Citrix Endpoint Management 中设置的应用、Web 链接和应用商店的列表。在 iOS 或 MDX 中，您可以使用应用类别让用户仅访问某些应用、应用商店或 Web 链接。例如，您可以创建一个“财务”类别，然后将仅与财务相关的应用添加到该类别中。或者，您可以配置一个“销售”类别，并将销售应用分配给该类别。

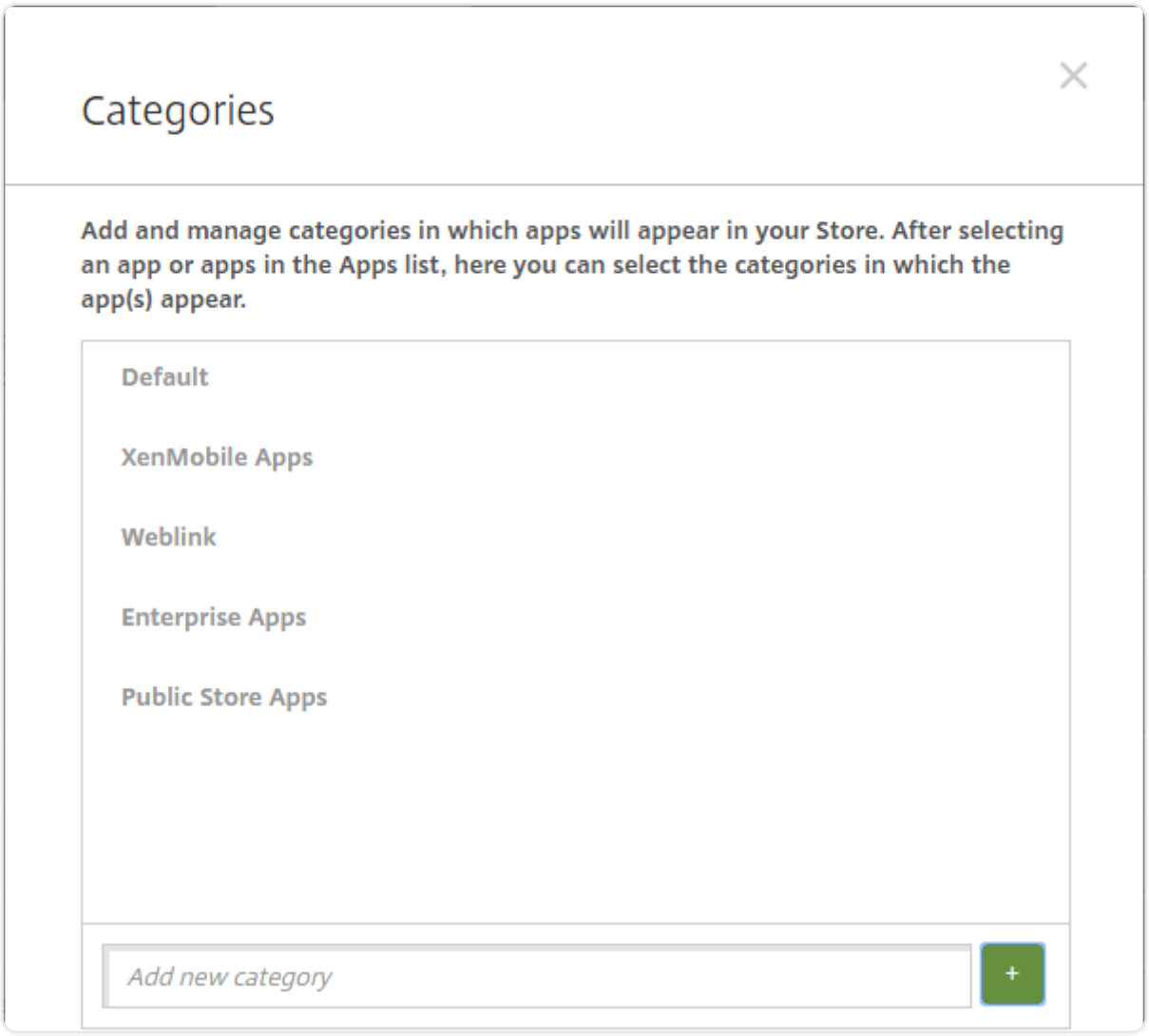
添加或编辑应用、Web 链接或应用商店时，您可以将应用添加到一个或多个已配置的类别中。

1. 在 Citrix Endpoint Management 控制台中，单击“**配置 > 应用 > 类别**”。此时将显示“**类别**”对话框。



2. 对于要添加的每个类别，请执行以下操作：

   - 在对话框底部的“**添加新类别**”字段中键入要添加的类别名称。例如，您可以键入“企业应用”以创建企业应用类别。
   - 单击加号 (+) 以添加类别。新创建的类别随即添加并显示在“**类别**”对话框中。



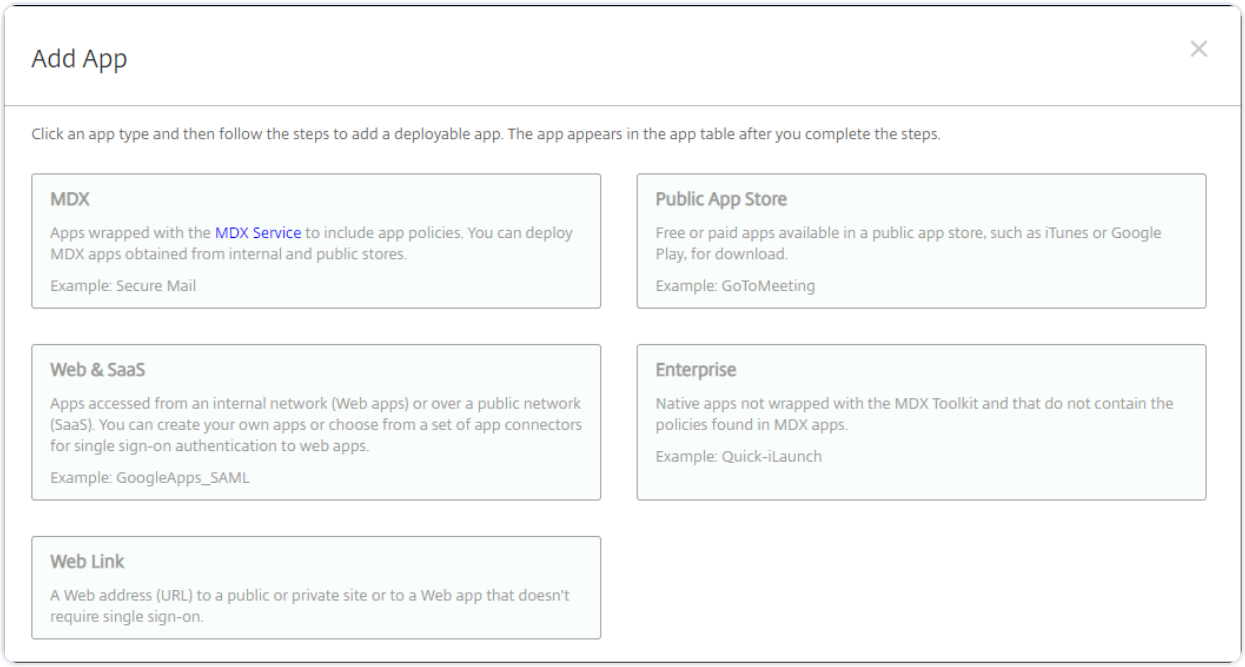
3. 添加完类别后，关闭“**类别**”对话框。
4. 在“**应用**”页面上，您可以将现有应用放入新类别中。
   - 选择要分类的应用。
   - 单击“**编辑**”。此时将显示“**应用信息**”页面。
   - 在“**应用程序类别**”列表中，通过选择类别复选框来应用新类别。清除您不想应用于此应用程序的任何现有类别的复选框。
   - 单击“**交付组分配**”选项卡，或在后续每个页面上单击“**下一步**”以逐步完成其余的应用程序设置页面。
   - 在“**交付组分配**”页面上单击“**保存**”以应用新类别。新类别将应用于该应用程序并显示在“**应用程序**”表中。

添加 MDX 应用程序

当您收到适用于 iOS 或 Android 应用程序的 MDX 文件时，可以将其上传到 Citrix Endpoint Management。上传应用程序后，您可以配置应用程序详细信息和策略设置。有关适用于每种设备平台类型的应用程序策略的信息，请参阅：

- MAM SDK 概述
- MDX 策略一览

1. 对于 Citrix 移动生产力应用程序，请下载公共商店 MDX 文件：转至 `<https://www.citrix.com/downloads>`。导航到“**Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**”。
2. 对于其他类型的 MDX 应用程序，请获取 MDX 文件。
3. 在 Citrix 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。

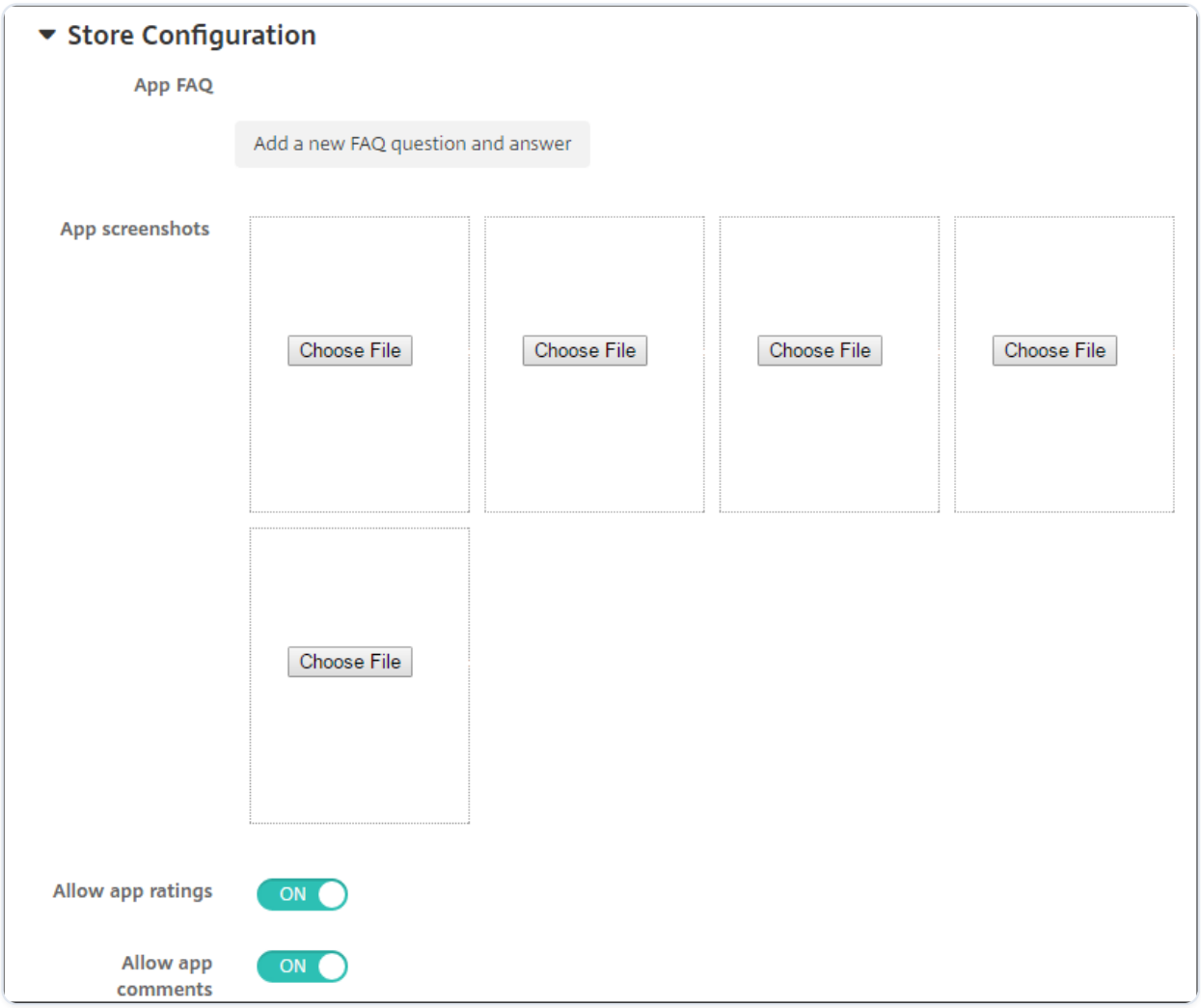


4. 单击“**MDX**”。此时将显示“**MDX 应用程序信息**”页面。
5. 在“**应用程序信息**”窗格中，键入以下信息：
   - “**名称：**”键入应用程序的描述性名称。该名称将显示在“**应用程序**”表中的“**应用程序名称**”下。
   - “**描述：**”键入应用程序的可选描述。
   - **应用程序类别：**（可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的更多信息，请参阅关于应用程序类别。
6. 单击“**下一步**”。此时将显示“**应用程序平台**”页面。

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，请清除其他平台。
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。
    - **应用程序描述：**键入应用程序的描述。
    - **应用程序版本：**（可选）键入应用程序版本号。
    - **程序包 ID：**键入来自托管 Google Play 商店的应用程序的程序包 ID。
    - **最低操作系统版本：**（可选）键入设备可运行以使用此应用程序的最旧操作系统版本。
    - **最高操作系统版本：**（可选）键入设备必须运行以使用此应用程序的最新操作系统版本。
    - **排除的设备：**（可选）键入无法运行此应用程序的设备的制造商或型号。
    - **如果 MDM 配置文件被删除，则删除应用程序：**选择当 MDM 配置文件被删除时是否从 iOS 设备中删除应用程序。默认值为“**开**”。
    - **阻止应用程序数据备份：**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**”。
    - **产品跟踪：**指定要推送到 iOS 设备的产品跟踪。如果您有专为测试设计的跟踪，则可以选择并将其分配给用户。默认值为“**生产**”。
    - **强制应用受管：** 对于作为非受管应用安装的应用，选择是否提示用户允许在非受管 iOS 设备上管理该应用。默认设置为 **开启**。
    - **通过批量购买部署应用：** 选择是否使用 Apple 批量购买部署应用。如果设置为 **开启**，并且您部署了 MDX 版本的应用并使用批量购买来部署该应用，则 Citrix Secure Hub 将仅显示批量购买实例。默认设置为 **关闭**。

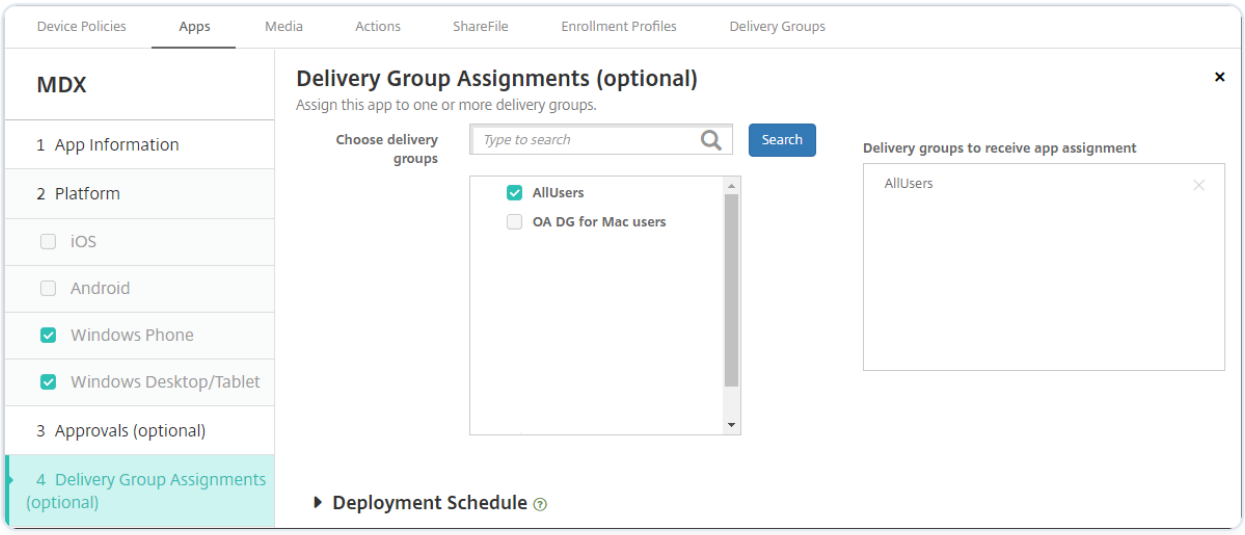
10. 配置 **MDX 策略**。MDX 策略因平台而异，包括身份验证、设备安全和应用限制等策略区域的选项。在控制台中，每个策略都有一个工具提示，用于描述该策略。
11. 配置部署规则。有关信息，请参阅 配置部署规则。
12. 展开 **应用商店配置**。



（可选）您可以配置以下各项：

- **应用常见问题：** 单击 **添加新的常见问题和答案** 为应用创建常见问题。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用评分：** 允许用户在应用商店中对应用进行评分。
- **允许应用评论：** 允许用户在应用商店中对应用发表评论。

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在列表中选择一个或多个组。您选择的组将显示在 **接收应用分配的交付组** 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**：选择是**立即**部署应用程序还是**稍后**部署。如果选择“**稍后**”，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“**仅当以前的部署失败时**”以在设备以前未能接收到应用程序时部署应用程序。默认值为“**每次连接时**”。

    “**始终在线连接部署**”选项在您已在“**设置 > 服务器属性**”中配置了计划后台部署密钥时适用。

    始终在线选项：

    - 不适用于 iOS 设备
    - 不适用于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户
    - 不建议从版本 10.18.19 之前开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户使用

    您配置的部署计划适用于所有平台。您所做的任何更改都适用于所有平台，但“**始终在线连接部署**”除外。
16. 单击“**保存**”。

添加公共应用商店应用程序

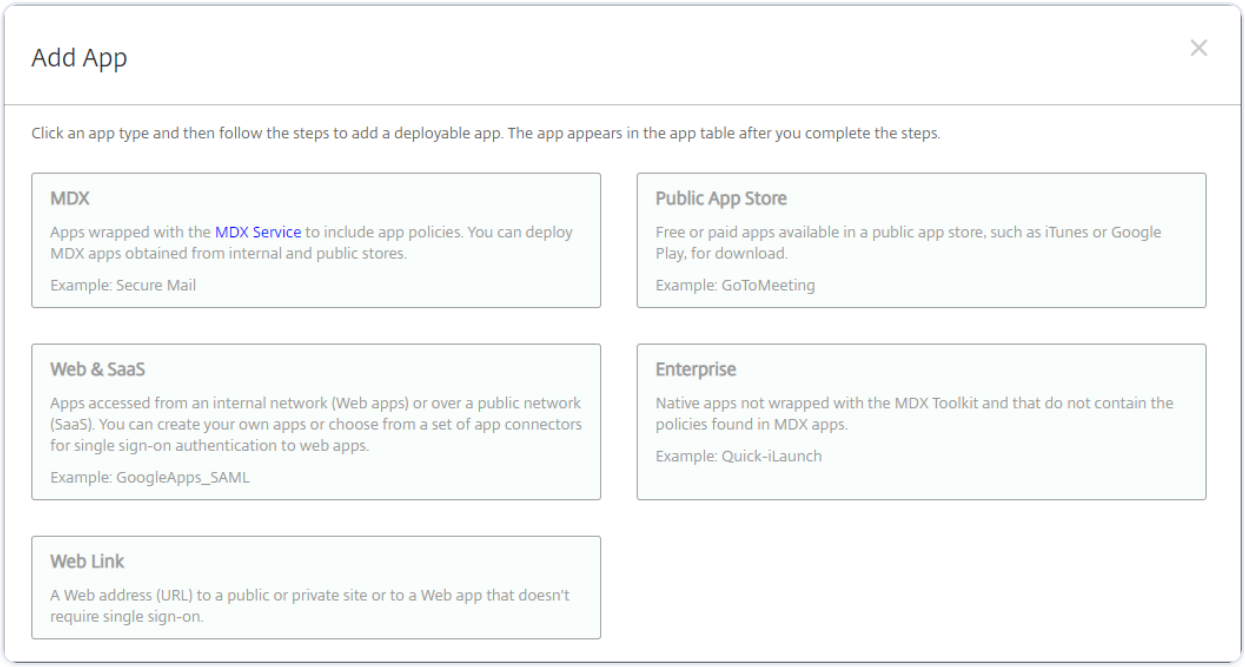
您可以将公共应用商店（例如 Apple App Store）中提供的免费或付费应用程序添加到 Citrix Endpoint Management。

您可以配置设置以从 Apple App Store 检索应用程序名称和说明。当您从商店检索应用程序信息时，Citrix Endpoint Management 会覆盖现有的名称和说明。手动配置 Google Play 商店应用程序信息。

> **注意：**
>
> Google 不再支持通过 Android Enterprise Managed Google Play 提供的 Android 付费应用程序。有关详细信息，请参阅 Managed Google Play 帮助文档。

配置应用程序信息并选择要交付应用程序的平台：

1. 在 Citrix Endpoint Management 控制台中，单击“**配置 > 应用程序 > 添加**”。将显示“**添加应用程序**”对话框。



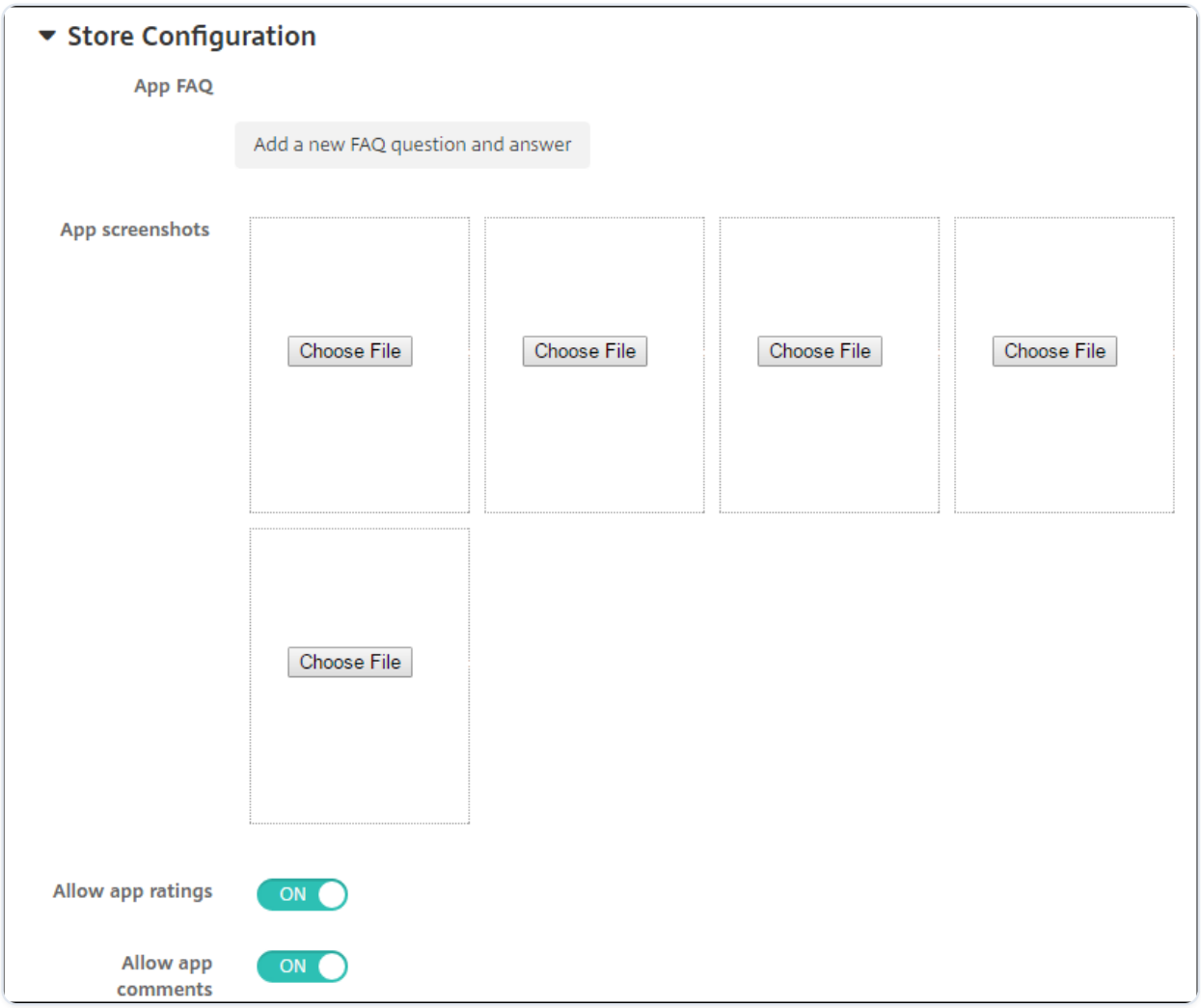
2. 单击“**公共应用商店**”。将显示“**应用程序信息**”页面。
3. 在“**应用程序信息**”窗格中，键入以下信息：
   - **名称：** 键入应用程序的描述性名称。此名称将显示在“**应用程序**”表中的“**应用程序名称**”下。
   - **说明：** 键入应用程序的可选说明。
   - **应用程序类别：** （可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 单击“**下一步**”。将显示“**应用程序平台**”页面。
5. 在“**平台**”下，选择要添加的平台。如果只为一个平台进行配置，请清除其他平台。

接下来，为每个平台配置应用程序设置。请参阅：

- 配置 Google Play 应用程序的应用程序设置
- 托管应用商店应用程序
- 配置 iOS 应用程序的应用程序设置

完成平台设置配置后，设置平台部署规则和应用商店配置。

1. 配置部署规则。有关信息，请参阅配置部署规则。
2. 展开 **商店配置**。



您可以选择配置以下内容：

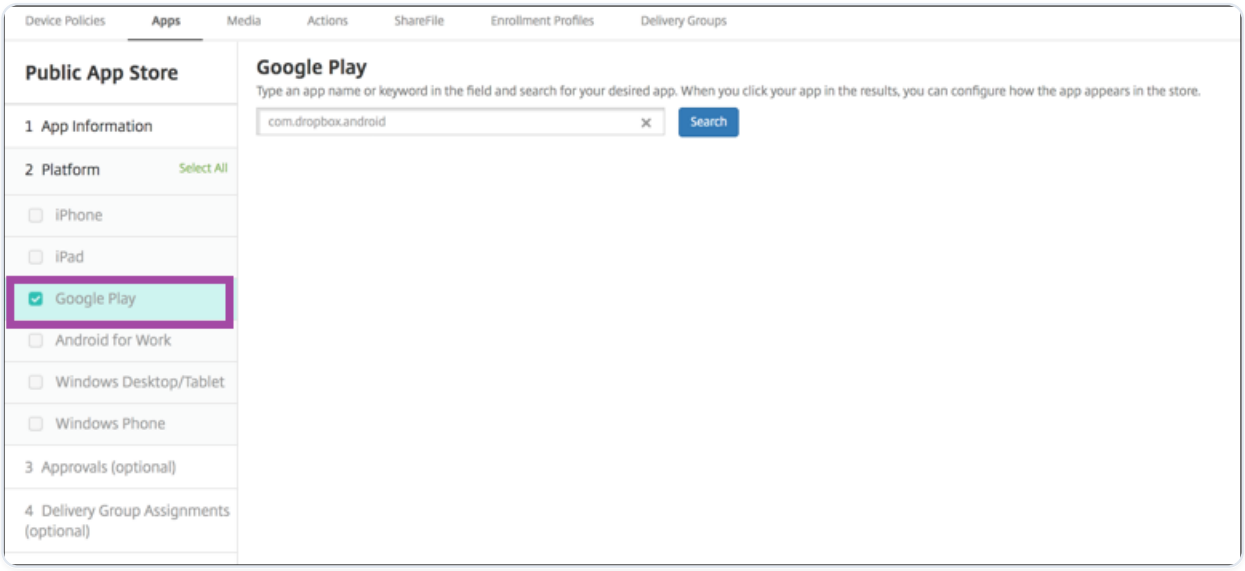
- **应用程序常见问题解答：** 单击 **Add a new FAQ question and answer** 为应用程序创建常见问题解答。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用程序评分：** 允许用户在应用商店中对应用程序进行评分。
- **允许应用程序评论：** 允许用户在应用商店中对应用程序发表评论。

配置 Google Play 应用程序的应用程序设置

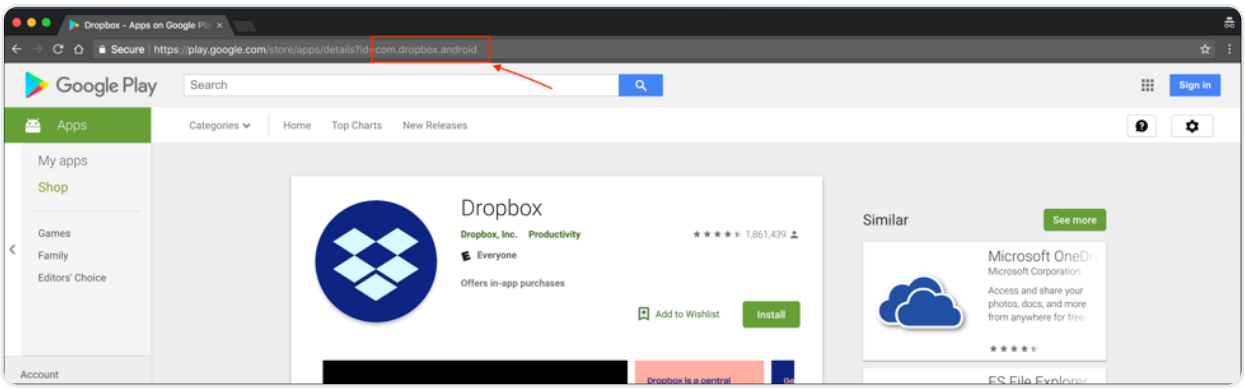
> **注意：**
>
> 要使 Google Play 商店中的所有应用程序都可从托管 Google Play 访问，请使用 **Access all apps in the managed Google Play store** 服务器属性。（请参阅服务器属性。）将此属性设置为 **true** 允许所有 Android Enterprise 用户访问公共 Google Play 商店应用程序。然后，您可以使用限制设备策略来控制对这些应用程序的访问。

> 配置 Google Play 商店应用程序的设置与配置其他平台应用程序的设置不同。请手动配置 Google Play 商店应用程序信息。

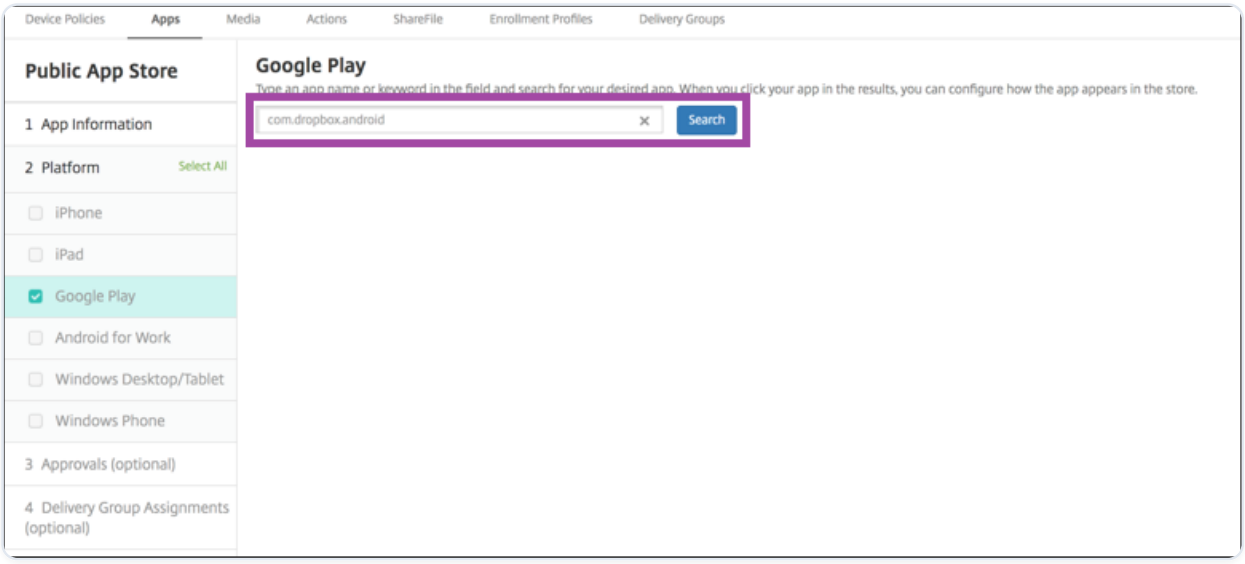
1. 确保在 **Platforms** 下选中 **Google Play**。



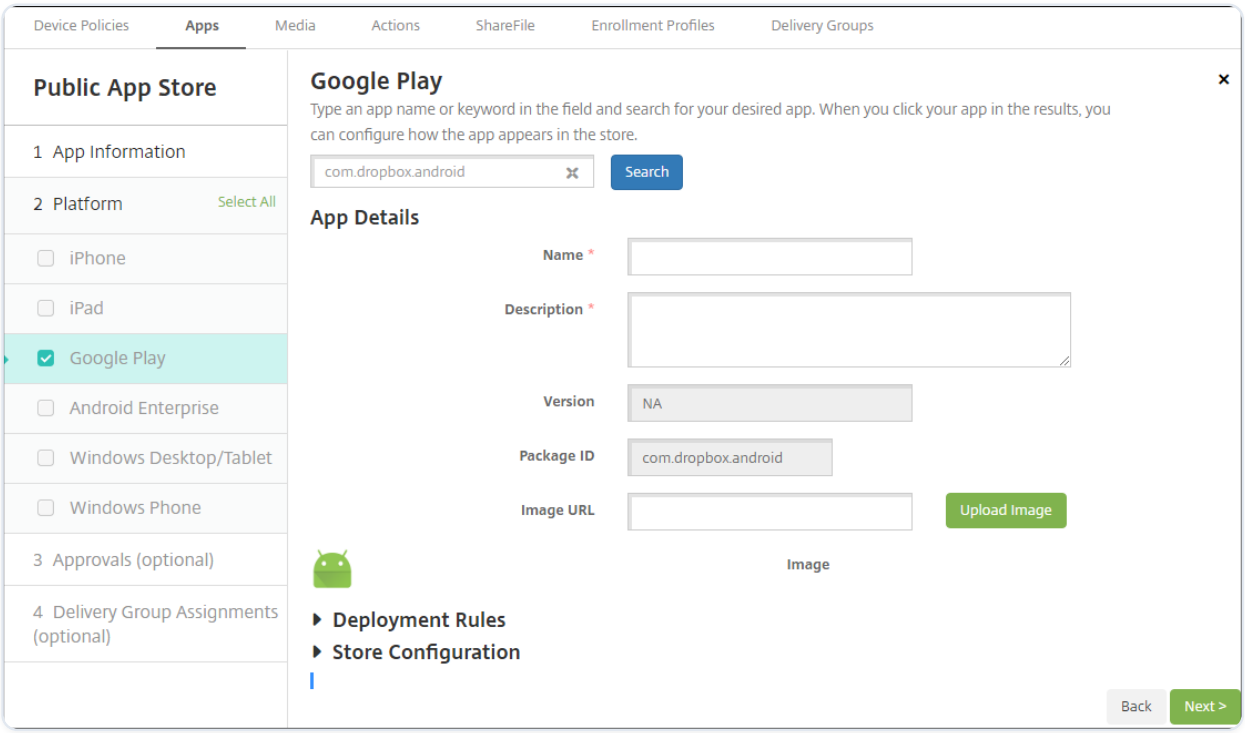
2. 转到 Google Play 商店。从 Google Play 商店复制程序包 ID。该 ID 可以在应用程序的 URL 中找到。



3. 在 Citrix Endpoint Management 控制台中添加公共应用商店应用程序时，将包 ID 粘贴到搜索栏中。单击“**搜索**”。



4. 如果包 ID 有效，将出现一个 UI，允许您输入应用程序详细信息。



5. 您可以配置图像的 URL，使其与应用商店中的应用程序一起显示。要使用 Google Play 商店中的图像：

   a. 转到 Google Play 商店。右键单击应用程序图像并复制图像地址。

   b. 将图像地址粘贴到“**图像 URL**”字段中。

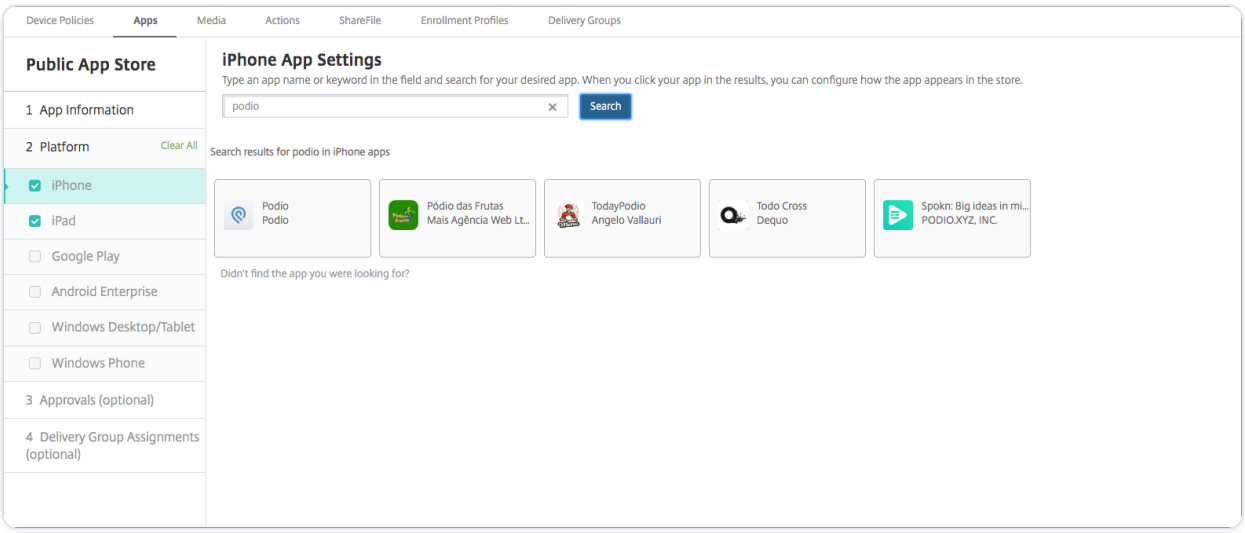
   c. 单击“**上传图像**”。图像将显示在“**图像**”旁边。

如果您不配置图像，应用程序将显示通用 Android 图像。

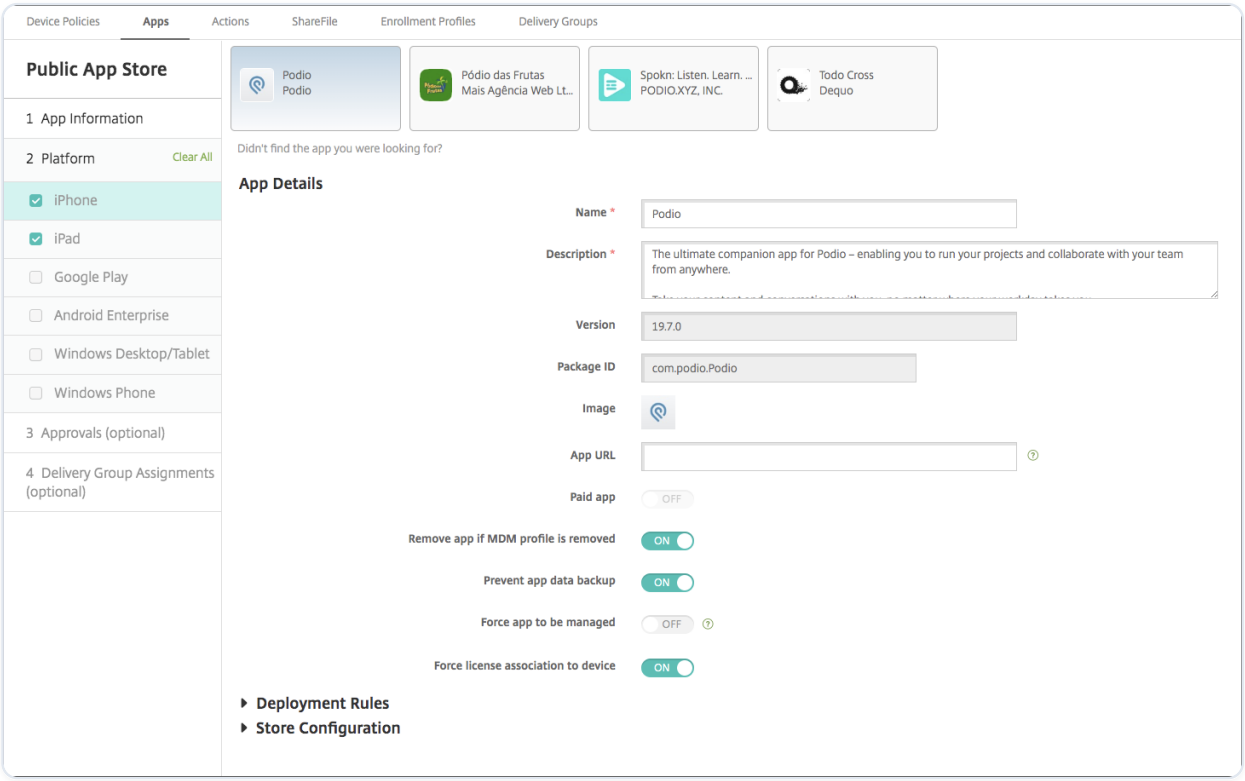
配置 iOS 应用程序的设置

1. 在搜索框中键入应用程序名称并单击“**搜索**”。将显示与搜索条件匹配的应用程序。将显示与搜索条件匹配的应用程序。

   下图显示了在 iPhone 上的应用程序中搜索 **podio** 的结果。



2. 单击要添加的应用程序。
3. “**应用详细信息**”字段会预填充与所选应用相关的信息（包括名称、描述、版本号和关联图像）。

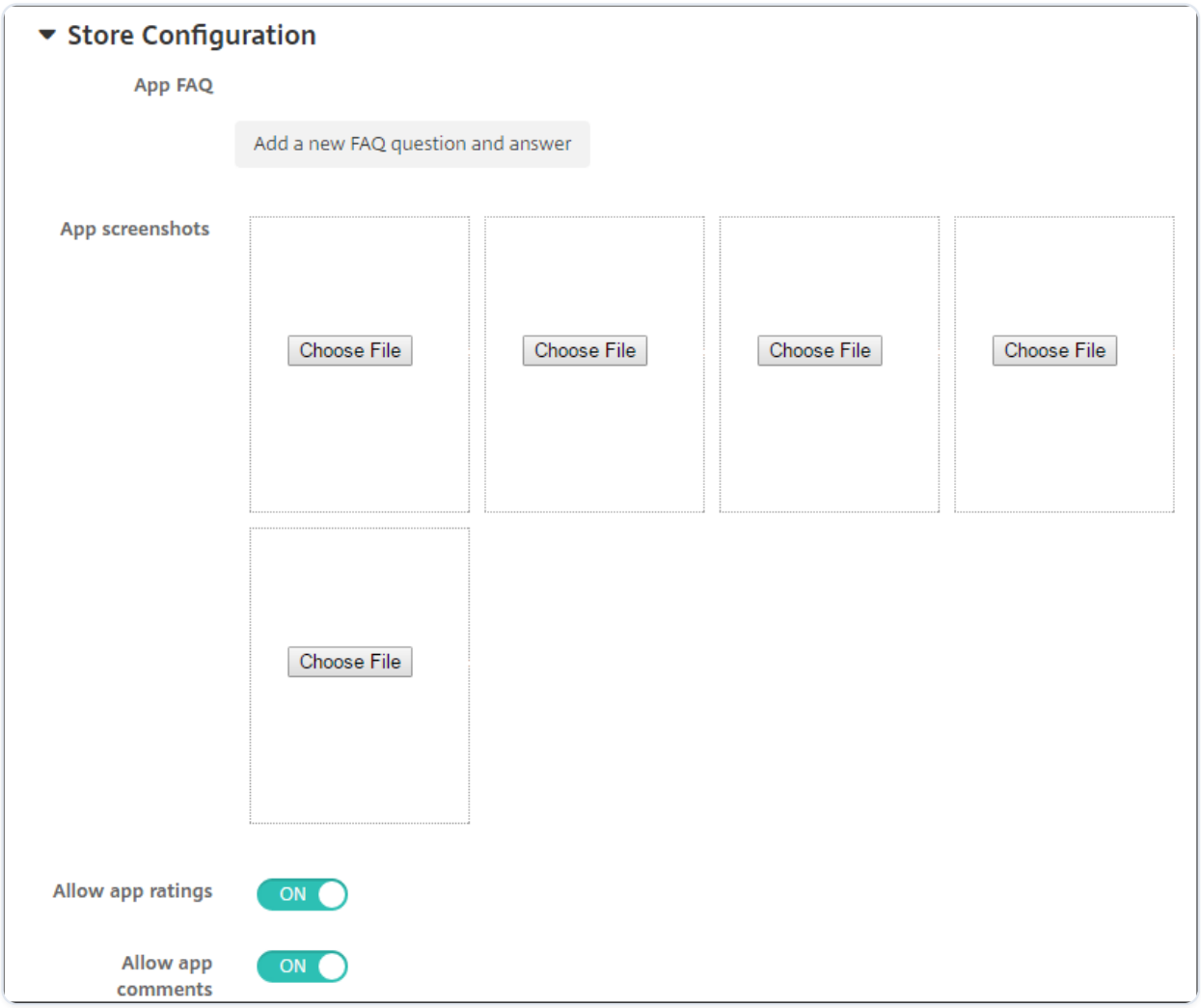


4. 配置设置：

   - 如有必要，更改应用的名称和描述。

- **应用 URL：** 输入以逗号分隔的 URL 列表，以从 Citrix Workspace 应用程序启动您的应用。此字段仅适用于 iPhone 和 iPad 设备。
- **付费应用：** 此字段已预配置，无法更改。
- **如果 MDM 配置文件被删除，则删除应用：** 选择是否在 MDM 配置文件被删除时删除应用。默认值为“**开**”。
- **阻止应用数据备份：** 选择是否阻止应用备份数据。默认值为“**开**”。
- **产品轨道：** 指定要推送到用户设备的产品轨道。如果您有专为测试设计的轨道，则可以选择并将其分配给您的用户。默认值为“**生产**”。
- **强制应用受管理：** 对于作为非托管应用安装的应用，选择是否提示用户允许在非受监管的 iOS 设备上管理应用。默认值为“**关**”。对于通过用户注册注册的 iOS 设备，Citrix Endpoint Management 不会强制执行此设置，也不会提示用户允许应用管理。
- **强制许可证与设备关联：** 选择是将应用（在开发时启用了设备关联）关联到设备而不是用户。如果您选择的应用不支持分配给设备，则无法更改此设置。

5. 配置部署规则。有关信息，请参阅配置部署规则。
6. 展开“**商店配置**”。



或者，您可以配置以下内容：

- **应用常见问题：** 单击 **添加新的常见问题和答案** 为应用创建常见问题。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用评分：** 允许用户在应用商店中对应用进行评分。
- **允许应用评论：** 允许用户在应用商店中对应用发表评论。

7. 对于 iPhone 或 iPad，展开 **批量购买**。

   a. 要使 Citrix Endpoint Management 能够为应用应用批量购买许可证：在 **批量购买许可证** 列表中，单击 **上载批量购买许可证**。

   b. 在出现的对话框中，导入许可证。

      许可证分配表显示应用正在使用的许可证数量，占可用许可证总数。

      您可以取消关联单个用户的批量购买许可证。这样做会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 **应用自动更新**。此设置可确保当 Apple Store 中出现更新时，用户设备上的应用会自动更新。如果应用启用了 **强制应用受管理** 设置，它会在不提示用户的情况下更新。无论应用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 **批准** 页面。

   要使用工作流在允许用户访问应用之前要求批准，请参阅 应用工作流。如果不需要批准工作流，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在列表中选择一个或多个组。您选择的组将显示在 **接收应用分配的交付组** 列表中。
11. 展开 **部署计划**，然后配置以下设置：

    - **部署**：选择是否将应用部署到设备。默认值为**开**。
    - **部署计划**：选择是**立即**部署应用还是**稍后**部署。如果选择**稍后**，请配置部署应用的日期和时间。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。选择**仅当以前的部署失败时**以在设备以前未能接收应用时部署应用。默认值为**每次连接时**。

    始终在线连接部署选项在您已在**设置 > 服务器属性**中配置计划后台部署密钥时适用。

    始终在线选项：

    - 不适用于 iOS 设备
    - 不适用于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户
    - 不建议从版本 10.18.19 之前开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户使用

    您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但**始终在线连接部署**除外。

12. 单击**保存**。

添加 Web 或 SaaS 应用

使用 Citrix Endpoint Management 控制台，您可以为用户提供对企业、Web 和 SaaS 应用的单点登录 (SSO) 授权。

添加 Web 应用或 SaaS 应用时，您可以在 Citrix Endpoint Management 中构建自己的连接器。有关 Citrix Endpoint Management 中可用的连接器类型列表，请参阅应用程序连接器类型。

如果应用仅适用于 SSO：保存设置后，该应用将显示在 Citrix Endpoint Management 控制台的**应用**选项卡上。

1. 在 Citrix Endpoint Management 控制台中，单击**配置 > 应用 > 添加**。此时将显示**添加应用**对话框。

   应用程序配置屏幕(/en-us/citrix-endpoint-management/media/configure-apps-add.png)

2. 单击**Web 和 SaaS**。将显示**应用程序信息**页面。

   应用程序配置屏幕(/en-us/citrix-endpoint-management/media/configure-apps-web-saas.png)

3. 按如下方式配置现有或新的应用程序连接器。

配置现有应用程序连接器

1. 在**应用程序信息**页面中，**从现有连接器中选择**已选中，如前所示。在**应用程序连接器**列表中单击要使用的连接器。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：** 接受预填充的名称或键入新名称。
   - **应用程序描述：** 接受预填充的描述或键入您自己的描述。
   - **URL：** 接受预填充的 URL 或键入应用程序的 Web 地址。根据您选择的连接器，此字段可能包含一个占位符，您必须先替换该占位符才能转到下一页。
   - **域名：** 如果适用，键入应用程序的域名。此字段为必填项。
   - **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 NetScaler Gateway 连接。将此选项设置为**开**会将 VPN 关键字添加到应用程序，并允许用户通过 NetScaler Gateway 连接。默认值为**关**。
   - **应用程序类别：** 在下拉列表中单击一个可选类别以应用于应用程序。
   - **用户帐户预配：** 选择是否为应用程序创建用户帐户。如果使用 Globoforce_SAML 连接器，则必须启用此选项以提供无缝 SSO 集成。
   - 如果启用**用户帐户预配**，请配置以下设置：

     - **服务帐户**

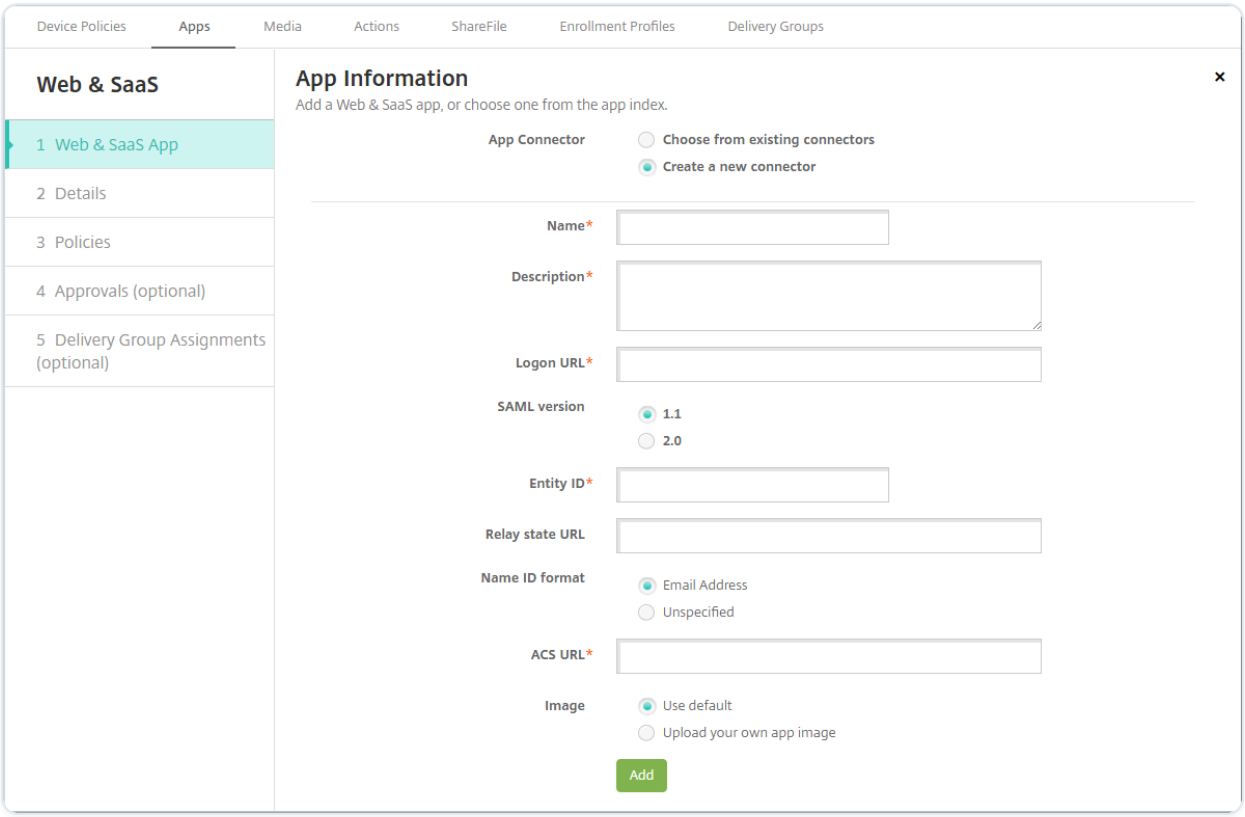
       - **用户名：**键入应用程序管理员的名称。此字段为必填项。
       - **密码：**键入应用程序管理员密码。此字段为必填项。

    - **用户帐户**
        - **用户授权结束时：单击下拉列表中的操作，以在用户不再被允许访问应用程序时执行。默认值为禁用帐户。**
    - **用户名规则**
        - 对于要添加的每个用户名规则，请执行以下操作：
            - **用户属性：**单击下拉列表中的用户属性以将其添加到规则中。
            - **长度（字符）：单击下拉列表中的字符数，以从用户属性中选择要在用户名规则中使用的字符。默认值为全部。**
            - **规则：**您添加的每个用户属性都会自动附加到用户名规则中。

- **密码要求**
    - **长度：键入最小用户密码长度。默认值为8。**
- **密码过期**
    - **有效期（天）：键入密码的有效天数。有效值为0–90。**默认值为 90。
    - **密码过期后自动重置：选择是否在密码过期时自动重置密码。默认值为关闭。**如果未启用此字段，则用户在密码过期后无法打开应用程序。

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**。应用程序连接器字段随即显示。

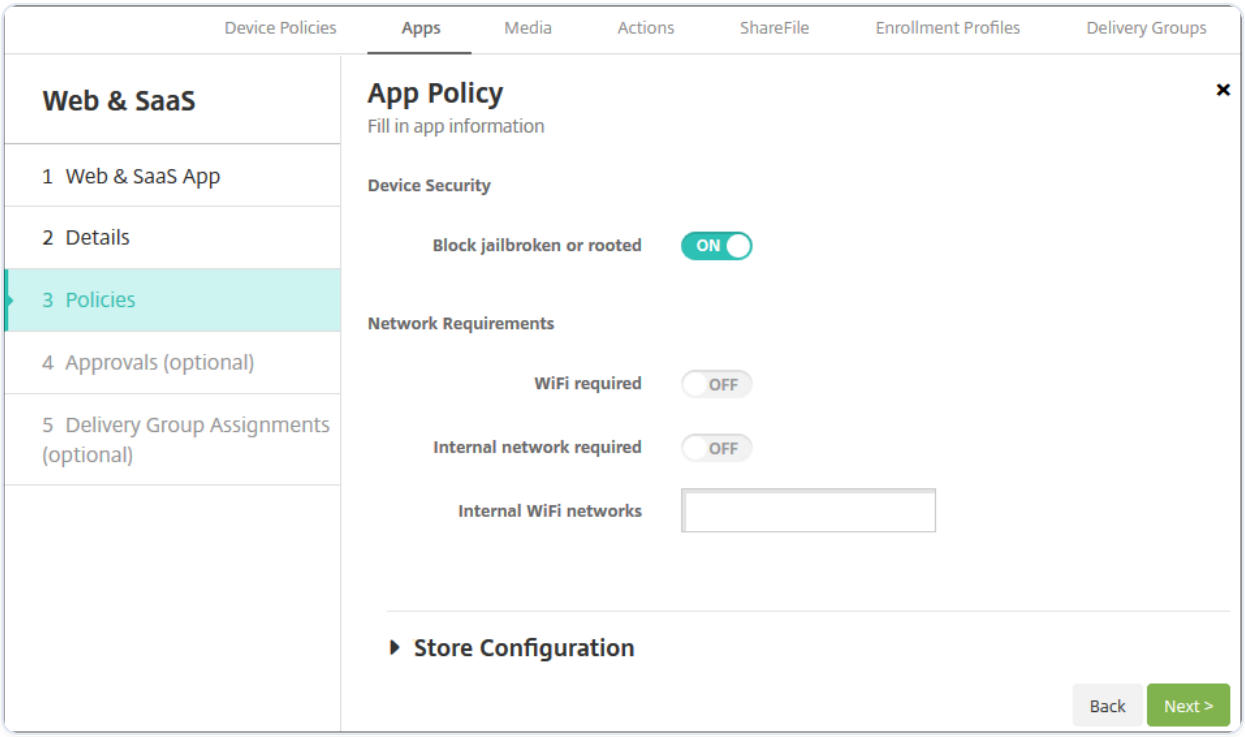


2. 配置以下设置：

   - **名称：**键入连接器的名称。此字段为必填项。
   - **描述：**键入连接器的描述。此字段为必填项。
   - **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具有登录页面，请打开 Web 浏览器并转到该应用程序的登录页面。例如，它可能是 `https://www.example.com/logon`。此字段为必填项。
   - **SAML 版本：**选择 **1.1** 或 **2.0**。默认值为 **1.1**。
   - **实体 ID：**键入 SAML 应用程序的身份。
   - **中继状态 URL：**键入 SAML 应用程序的 Web 地址。中继状态 URL 是应用程序的响应 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程序的断言消费者服务 URL。ACS URL 为用户提供 SSO 功能。
   - **图像：**选择是使用默认的 Citrix 图像还是上传您自己的应用程序图像。默认值为“使用默认图像”。
     - 要上传您自己的图像，请单击**浏览**并导航到文件位置。文件必须是 .PNG 文件。您不能上传 JPEG 或 GIF 文件。添加自定义图形后，您无法再更改它。

3. 完成后，单击**添加**。随即显示**详细信息**页面。

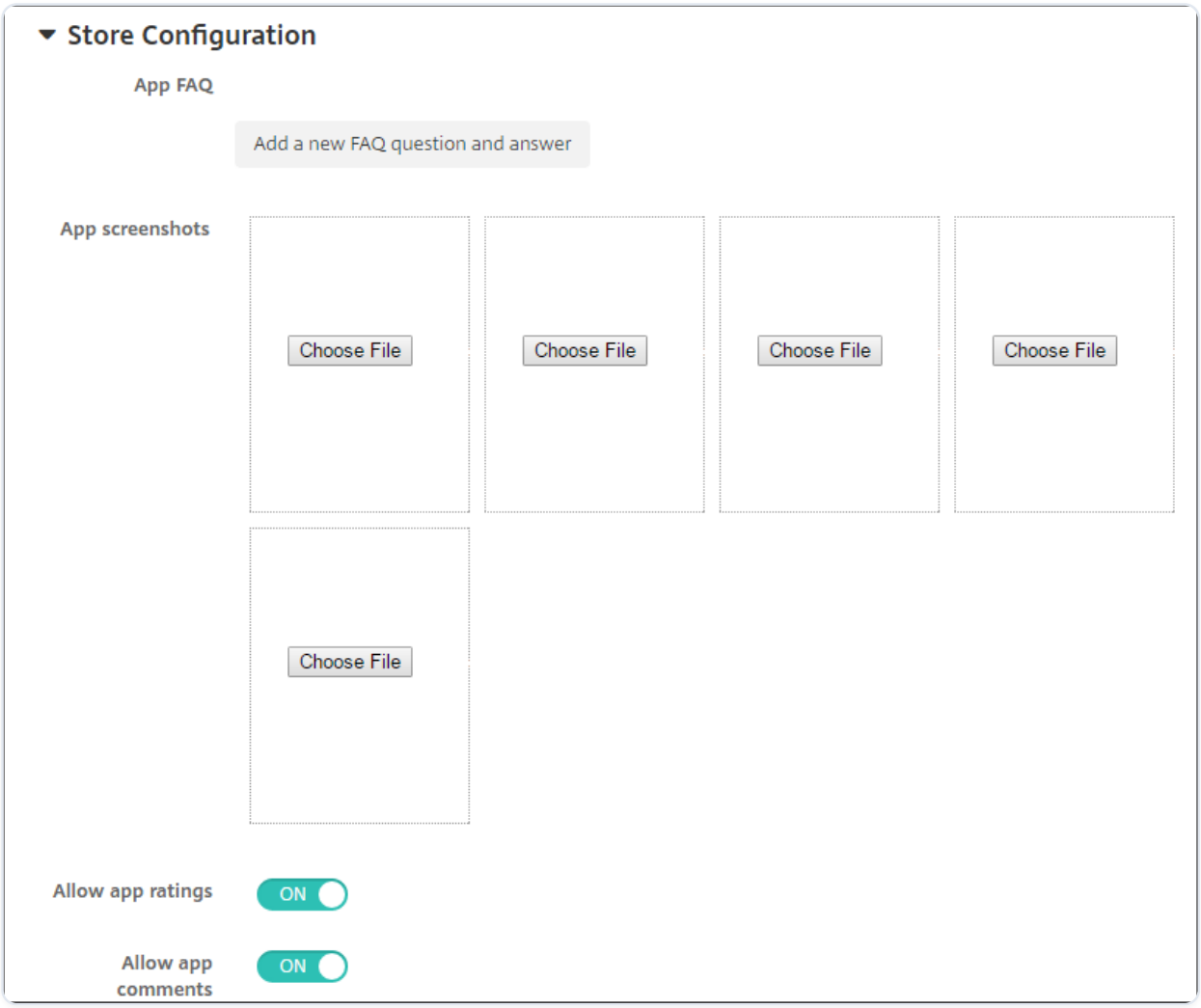
4. 单击**下一步**。**应用程序策略**页面随即显示。



5. 配置以下设置：

   - **设备安全性**
   - **阻止越狱或已获得 root 权限的设备：** 选择是否阻止越狱或已获得 root 权限的设备访问应用程序。默认值为**开**。
   - **网络要求**
   - **需要 WiFi：** 选择运行应用程序是否需要 Wi-Fi 连接。默认值为**关**。
   - **需要内部网络：** 选择运行应用程序是否需要内部网络。默认值为**关**。
   - **内部 WiFi 网络：** 如果启用了**需要 Wi-Fi**，请键入要使用的内部 Wi-Fi 网络。

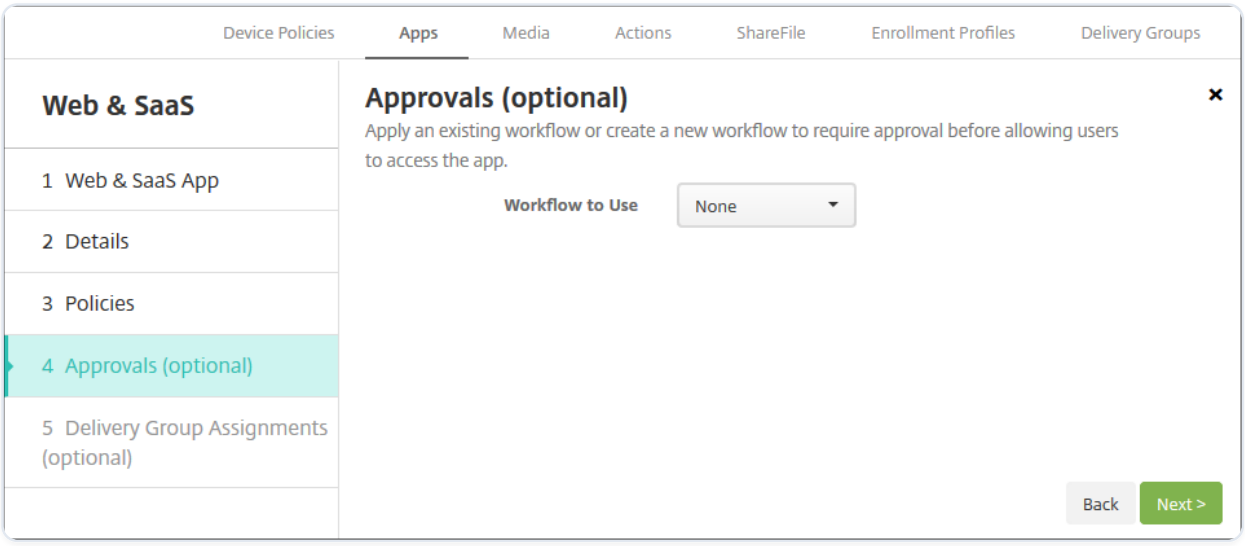
6. 展开**应用商店配置**。



您可以选择配置以下各项：

- **应用程序常见问题解答：** 单击**添加新的常见问题解答**可为应用程序创建常见问题解答。
- **为手机/平板电脑添加屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用程序评分：** 允许用户在应用商店中对应用程序进行评分。
- **允许应用评论：**允许用户在应用商店中对应用发表评论。

7. 单击**下一步**。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审批，请参阅应用工作流。如果不需要审批工作流，请继续执行下一步。

8. 单击**下一步**。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选择一个或多个组。您选择的组将显示在**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：选择是立即**部署应用程序还是**稍后**部署。如果选择**稍后**，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**仅当以前的部署失败时**以在设备以前未能接收到应用程序时部署应用程序。默认值为**每次连接时**。

    当您在**设置 > 服务器属性**中配置了计划后台部署密钥时，**为始终在线连接部署**选项适用。

    始终在线选项：

    - 不适用于 iOS 设备
    - 不适用于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户
    - 不建议从版本 10.18.19 之前开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户使用

    您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但 **Deploy for always-on connection** 除外。

11. 单击“**保存**”。

添加企业应用

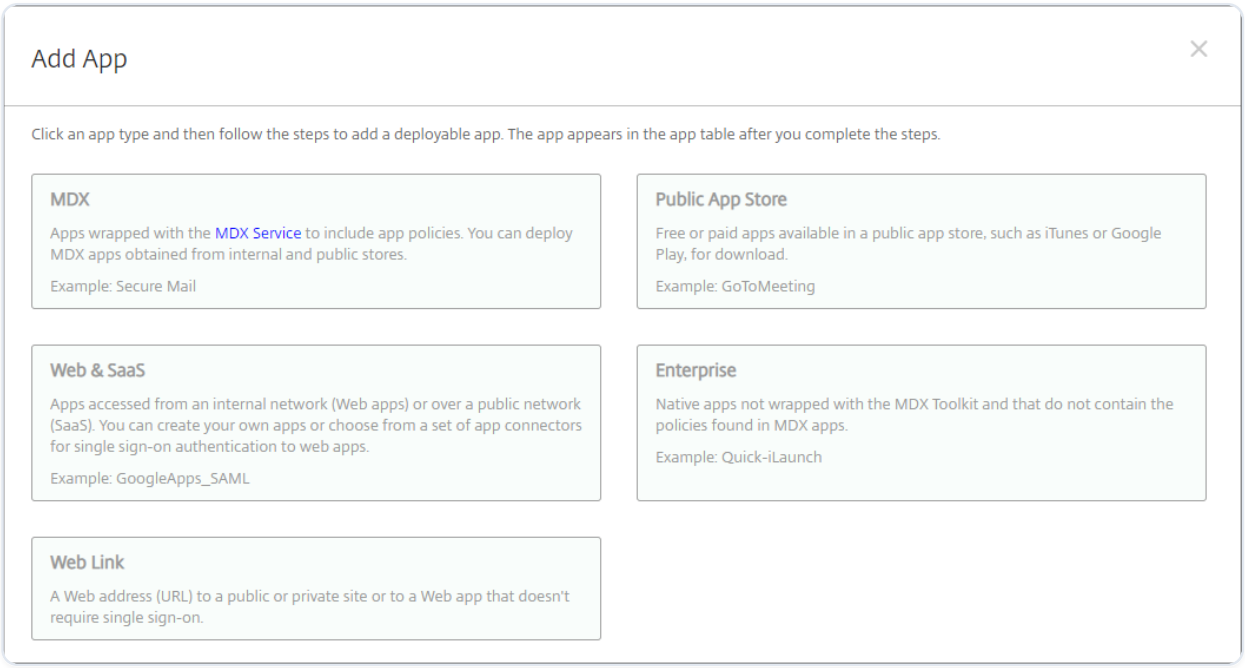
Citrix Endpoint Management 中的企业应用是您开发或从其他来源获取的专用应用。除了作为 MDX 启用应用交付的专用 Android Enterprise 应用外，企业应用不使用 MAM SDK 或 MDX Toolkit 进行准备。您可以在 Citrix Endpoint Management 控制台的“**应用**”选项卡上上传企业应用。企业应用支持以下平台（以及相应的文件类型）：

- iOS（.ipa 文件）
- macOS（.pkg 文件）

  Citrix Endpoint Management 不限制您上传的 PKG 文件的大小，但限制文件上传时间。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）
- 安卓企业版（.apk 文件）
- 另请参阅：将 Win32 应用添加为企业应用
- 另请参阅：MDX 启用的专用应用

不支持将从 Google Play 商店下载的应用添加为企业应用。请改为将 Google Play 商店中的应用添加为公共应用商店应用。请参阅添加公共应用商店应用。

1. 在 Citrix Endpoint Management 控制台中，单击“**配置 > 应用 > 添加**”。此时将显示“**添加应用**”对话框。



2. 单击“**企业**”。此时将显示“**应用信息**”页面。
3. 在“**应用程序信息**”窗格中，键入以下信息：

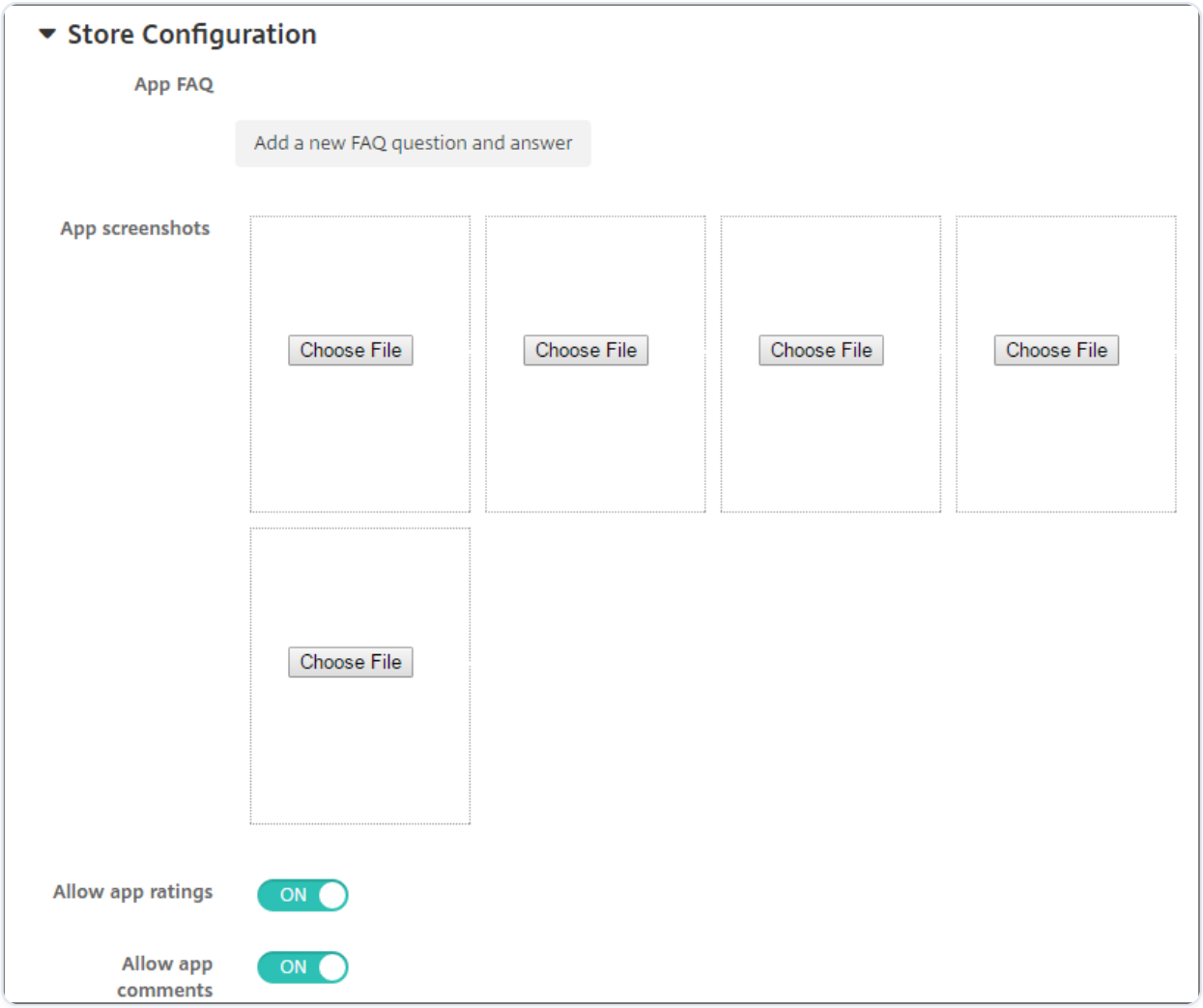
- **名称：** 键入应用程序的描述性名称。此名称将列在“应用程序”表中的“应用程序名称”下。
- **说明：** 键入应用程序的可选说明。
- **应用程序类别：** （可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

4. 单击“**下一步**”。将显示“**应用程序平台**”页面。
5. 在“**平台**”下，选择要添加的平台。如果只为一个平台进行配置，请清除其他平台。
6. 对于您选择的每个平台，通过单击“**上载**”并导航到文件位置来选择要上载的文件。
7. 单击“**下一步**”。将显示该平台的应用程序信息页面。
8. 配置平台类型的设置，例如：

- **文件名：** （可选）为应用程序键入新名称。
- **应用程序说明：** （可选）为应用程序键入新说明。
- **应用程序版本：** 无法更改此字段。
- **最低操作系统版本：** （可选）键入设备可运行以使用此应用程序的最旧操作系统版本。
- **最高操作系统版本：** （可选）键入设备必须运行以使用此应用程序的最新操作系统版本。
- **排除的设备：** （可选）键入无法运行此应用程序的设备的制造商或型号。
- **包 ID**：您的应用程序的唯一标识符。
- **如果 MDM 配置文件被移除，则移除应用程序**：选择当 MDM 配置文件被移除时是否从设备中移除应用程序。默认设置为“**开**”。此设置不适用于 macOS。
- **阻止应用程序数据备份**：选择是否阻止应用程序备份数据。默认设置为“**开**”。此设置不适用于 macOS。
- **强制应用程序受管理**：选择是否在非受监管设备上将应用程序作为受管理应用程序安装。设备类型决定了 Citrix Endpoint Management 在启用此设置时如何处理它。如果启用此设置，应用程序将在不提示用户的情况下更新。无论应用程序是必需的还是可选的，都会进行更新。默认设置为“**关**”。
  - 对于 iOS 设备，如果应用程序已安装，用户会收到提示以允许应用程序受管理。如果您将应用程序部署到不存在该应用程序的设备上，则无论此设置的状态如何，该应用程序都将作为受管理应用程序安装。适用于 iOS 9.0 及更高版本。对于通过用户注册注册的 iOS 设备，Citrix Endpoint Management 不会强制执行此设置，也不会提示用户允许应用程序管理。
  - 对于 macOS 设备，请启用此设置，然后将应用程序部署到设备。应用程序将自动作为受管理应用程序安装。用户不会收到任何提示。如果您将应用程序部署到不存在该应用程

序的设备上，则无论此设置的状态如何，该应用程序都将作为受管理应用程序安装。适用于 macOS 11.0 及更高版本。

9. 配置部署规则。有关信息，请参阅配置部署规则。
10. 展开“**商店配置**”。



或者，您可以配置以下内容：

- **应用程序常见问题**：单击“**添加新的常见问题和答案**”为应用程序创建常见问题。
- **添加手机/平板电脑屏幕截图**：添加显示在应用商店中的屏幕截图。
- **允许应用程序评分**：允许用户在应用商店中对应用程序进行评分。
- **允许应用程序评论**：允许用户在应用商店中对应用程序发表评论。

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。如果不需要批准工作流，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从列表中选择一个或多个组。您选择的组将显示在“**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：** 选择是“**立即**”还是“**稍后**”部署应用程序。如果选择“**稍后**”，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“**仅当以前的部署失败时**”以在设备以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**”。

    当您在“**设置 > 服务器属性**”中配置了计划后台部署密钥时，“**部署用于始终连接**”选项适用。

    始终连接选项：

    - 不适用于 iOS 设备
    - 不适用于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户
    - 不建议从版本 10.18.19 之前开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户使用

    您配置的部署计划适用于所有平台。您所做的任何更改都适用于所有平台，但“**部署用于始终连接**”除外。
15. 单击“**保存**”。

将 Win32 应用程序添加为企业应用程序

您可以将 Win32 应用程序的 MSI、APPX、AppxBundle、PS1 或 EXE 文件上传到 Citrix Endpoint Management，以部署到受管的 Windows 10 和 Windows 11 桌面及平板设备。使用 Citrix Endpoint Management 部署文件后，Windows 设备将按如下方式安装应用程序：

- 如果升级后的应用程序在安装过程中删除了旧版本，则设备将只包含升级后的应用程序。
- 如果升级后的应用程序无法删除旧版本，但新版本可以安装，则设备将包含应用程序的两个版本。Citrix Endpoint Management 不再拥有旧版本的信息。
- 如果存在旧版本时升级后的应用程序无法安装，则新应用程序不会安装。在这种情况下，请首先部署“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 专业版或 Windows 11 专业版
- Windows 10 企业版或 Windows 11 企业版
- 使用 /quiet 选项安装的独立 Win32 MSI 应用程序。对于此部署用例，Microsoft 不支持包含多个应用程序的 MSI、嵌套 MSI 或交互式安装。

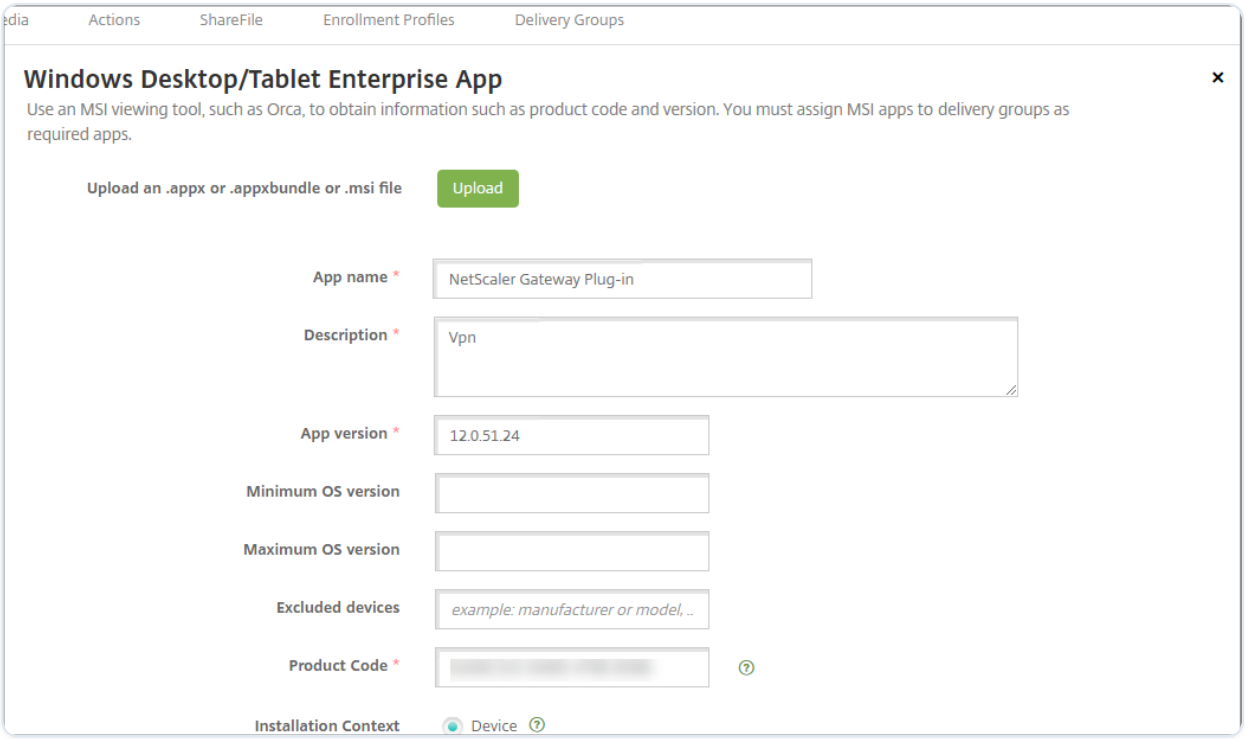
查找元数据

将 Win32 应用程序添加到 Citrix Endpoint Management 时，请指定该应用程序的元数据。要查找元数据，请在 Windows 计算机上使用 Orca 应用程序并记下以下信息：

- 产品代码
- 产品名称
- 产品版本
- 软件包安装类型，按用户或按计算机

将 Win32 应用添加到 Citrix Endpoint Management

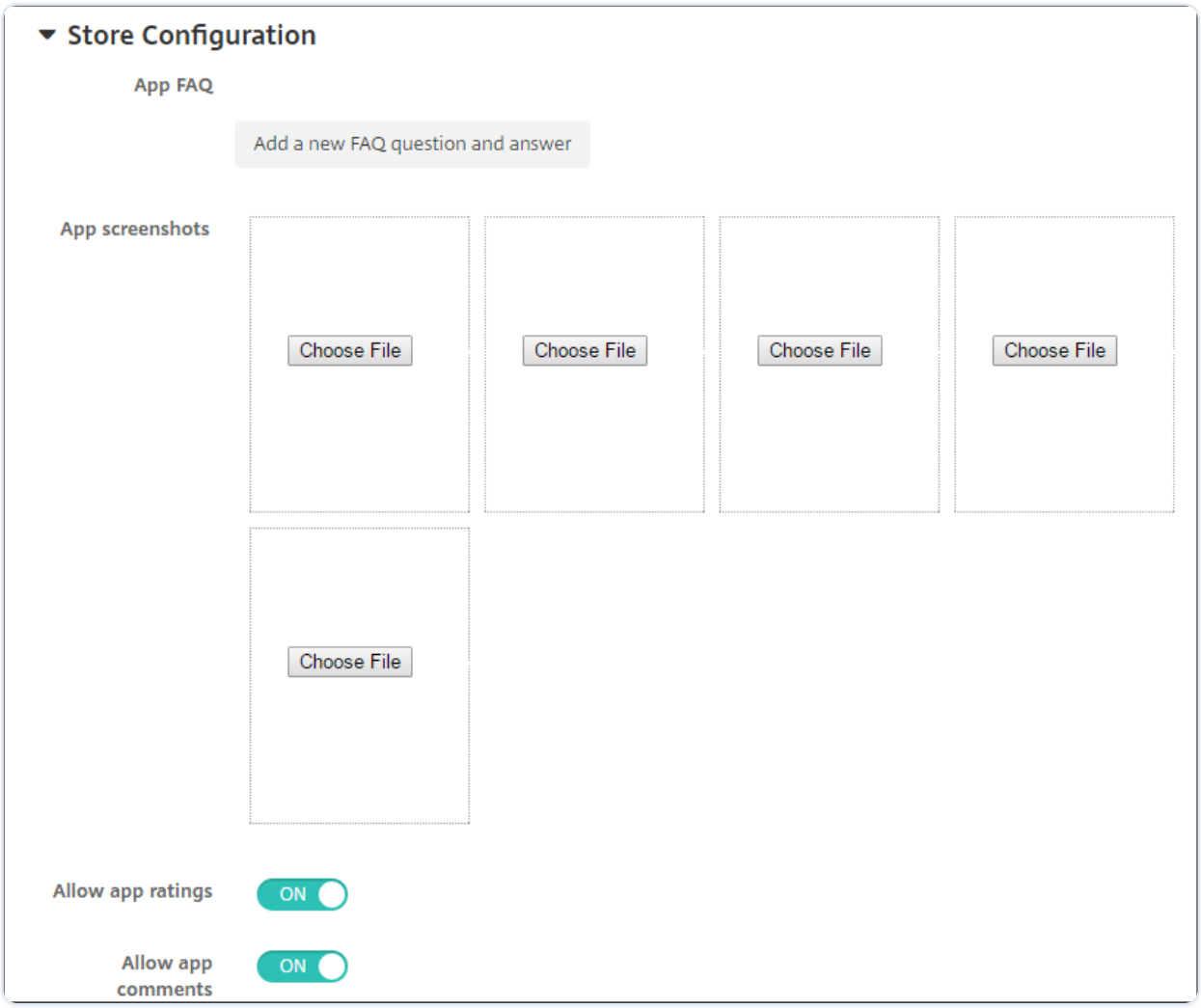
1. 转到**配置 > 应用**，单击**企业**，然后在**应用信息**页面中键入应用的名称。
2. 清除所有平台复选框，但**Windows 桌面/平板电脑**除外。
3. 在**视窗桌面/平板电脑企业应用**页面上，单击**上载**并导航到文件。
4. 配置以下设置：



- **应用名称：** 应用的名称，来自应用元数据。

- **说明：** 应用的说明。
- **应用版本：** 应用的版本号，来自应用元数据。
- **最低操作系统版本：** 可选。设备运行该应用所需的最低操作系统版本。
- **最高操作系统版本：** 可选。设备运行该应用所需的最新操作系统版本。
- **排除的设备：** 可选。无法运行该应用的设备制造商或型号。
- **产品代码：** MSI 应用的产品代码，采用 UUID 格式，来自应用元数据。
- **安装上下文：** 根据应用元数据，选择应用是为设备还是用户安装。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：** 添加用于静默安装 EXE 文件的命令行参数。
- **卸载命令行：** 添加用于静默卸载 EXE 文件的命令行参数。
- **重试次数：** 在将安装标记为失败之前，可以重试下载和安装操作的次数。
- **超时：** 安装程序在将安装解释为失败并停止监视该过程之前，安装过程运行的分钟数。
- **重试间隔：** 两次重试操作之间的分钟数。

5. 配置部署规则。有关信息，请参阅配置部署规则。
6. 展开 **应用商店配置**。



您可以选择配置以下内容：

- **应用程序常见问题：** 单击 **添加新的常见问题及解答** 为应用程序创建常见问题。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用程序评分：** 允许用户在应用商店中对应用程序进行评分。
- **允许应用程序评论：** 允许用户在应用商店中对应用程序发表评论。

7. 单击 **下一步** 直到到达 **摘要** 页面，然后单击 **保存**。
8. 转至 **配置 > 交付组** 并将 Win32 应用程序添加为所需应用程序。
9. 部署应用后，告知用户该应用可用。

升级 Win32 应用

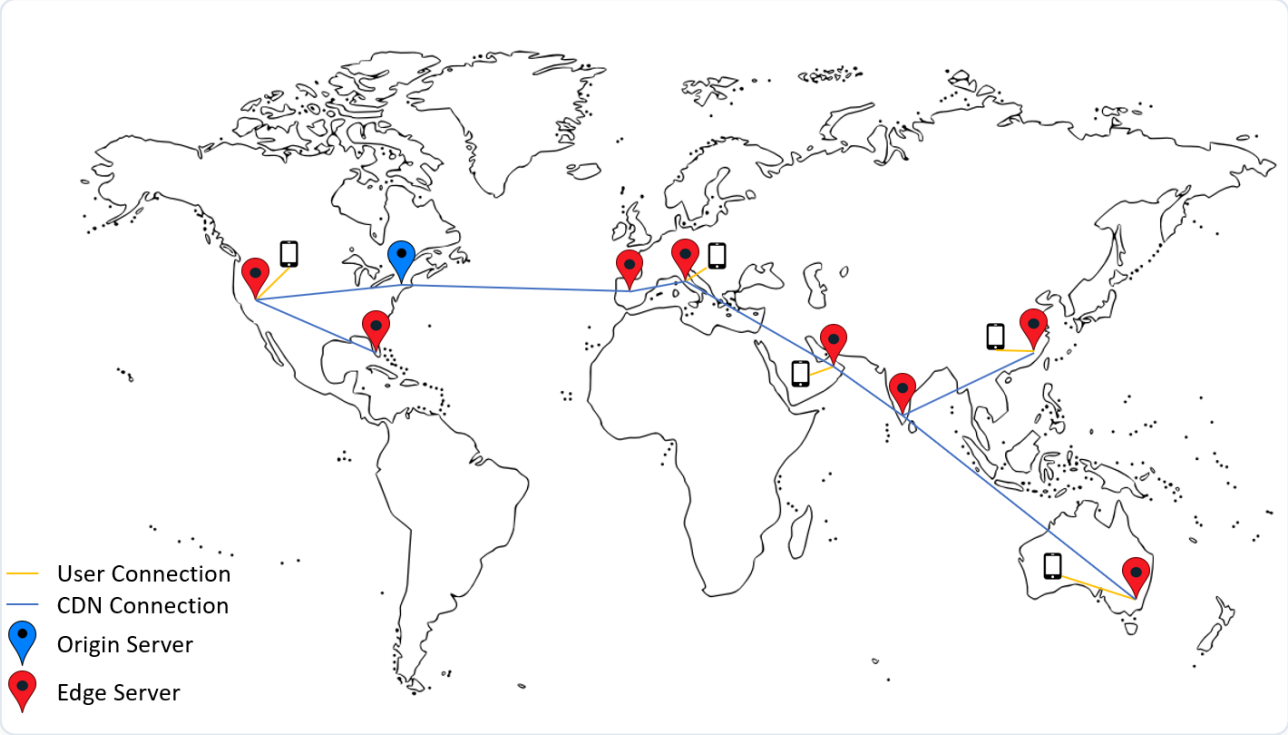
1. 查找应用的元数据，如前面“查找元数据”中所述。
2. 转至 **Configure > Apps** 上传应用的新版本。更新 **App version**。如果应用的新版本具有不同的 **Product Code**，请更新该设置。
3. 提交更改并部署应用。

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。CDN 是指一组地理上分散的服务器，它们协同工作以安全地提供应用程序内容的快速交付。本地服务器将应用交付到移动设备。

CDN 通过将内容分发到地理位置上更接近移动设备的附近 CDN 分发点来缩短应用下载时间。CDN 从距离用户最近的接入点 (POP) 位置交付应用。

下图显示了 CDN 如何将应用分发到距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时，边缘服务器会缓存来自源服务器的内容。



用户可以使用 Citrix Secure Hub 连接到应用。添加应用时，Citrix Endpoint Management 会为其创建应用连接器。

Citrix CDN 对企业应用的支持适用于以下平台：

- iOS（MDM 或 MAM 注册）
- Android（MDM 或 MAM 注册）
- Windows 桌面或平板电脑（MDM 注册）
- macOS (MDM 注册)

Citrix CDN 对 MDX 应用程序的支持适用于以下平台：

- iOS (MDM 或 MAM 注册)
- Android (MDM 或 MAM 注册)

CDN 的工作原理

CDN 服务的核心是，服务器相互连接，旨在更快地交付应用程序。通过将应用程序安全地放置在全球不同的分发点来实现此目标。移动设备在首次连接到 Citrix Endpoint Management 服务器时使用的 DNS 服务器决定了分发点。

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到移动设备。使用 CDN 可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，Citrix Endpoint Management 会将应用程序复制到本地分发点，并将应用程序保留 24 小时，供其他本地设备下载。

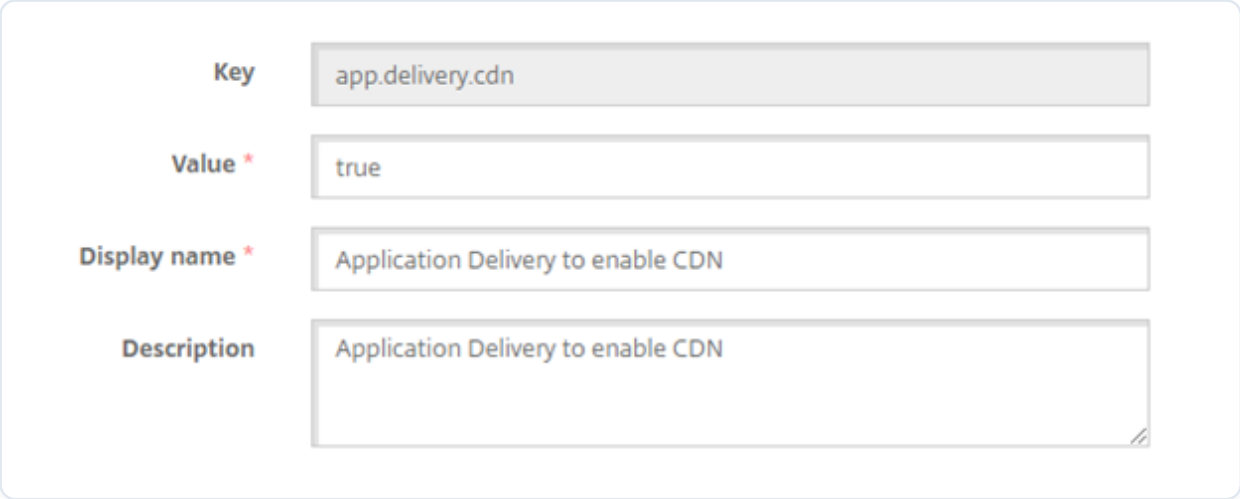
通过 Citrix CDN 交付企业应用程序

从 Citrix Endpoint Management 19.4.1 版本开始，所有新的多租户客户的企业应用程序交付默认使用 CDN 交付。对于此版本之前的现有客户，请按照本节中的说明进行操作。

对于 Citrix Endpoint Management 服务器上已有的企业应用程序，Citrix Endpoint Management 将继续从服务器交付这些应用程序，直到您完成以下步骤后重新上传这些应用程序。

> **重要：**
>
> 只有 Citrix Cloud 管理员才能为帐户启用 CDN。服务器属性 `app.delivery.cdn` 仅在您以 Citrix Cloud 管理员身份登录时才在 Citrix 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 Citrix 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 Citrix Endpoint Management 控制台中，再次上传您的企业应用程序：

   a. 转到 **Configure > Apps**，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 **Edit**，单击 **Next**，然后单击 **Upload**。

   c. 对每个企业应用程序重复上一步。

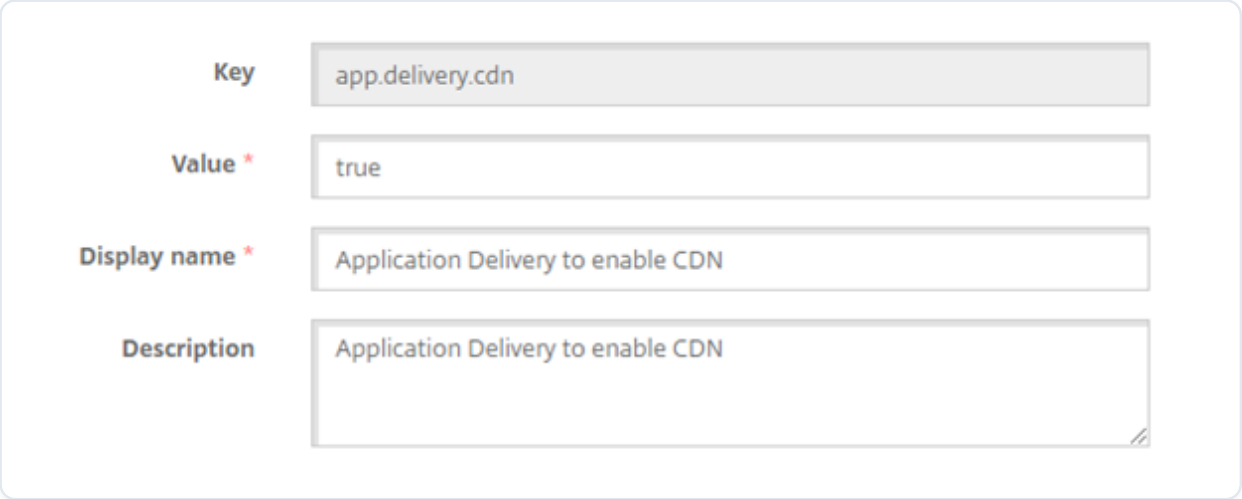
通过 Citrix CDN 交付 MDX 应用程序

从 Citrix Endpoint Management 20.12.0 版本开始，MDX 应用程序交付默认对所有新的多租户客户使用 CDN 交付。对于此版本之前的现有客户，请按照本节中的说明进行操作。

对于 Citrix Endpoint Management 服务器上已有的 MDX 应用程序，Citrix Endpoint Management 将继续从服务器交付这些应用程序，直到您完成以下步骤后重新上传这些应用程序。

> **重要提示：**
>
> 只有 Citrix Cloud 管理员才能为帐户启用 CDN。服务器属性 `app.delivery.cdn` 仅在您以 Citrix Cloud 管理员身份登录时才在 Citrix 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 Citrix Endpoint Management 控制台中：转到 **Settings > Server Properties**。
2. 搜索 `app.delivery.cdn`，然后单击 **Edit**。
3. 将值更改为 **true**。



4. 在 Citrix Endpoint Management 控制台中，再次上传您的 MDX 应用程序：

   a. 转到“**配置 > 应用程序**”，然后按“**类型**”（**MDX**）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“**上传**”。

   c. 对每个 MDX 应用程序重复上一步。

添加 Web 链接

Web 链接是 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。完成 Web 链接配置后，该链接将作为图标显示在应用商店中。当用户使用 Citrix Secure Hub 登录时，该链接会与可用应用程序和桌面列表一起显示。

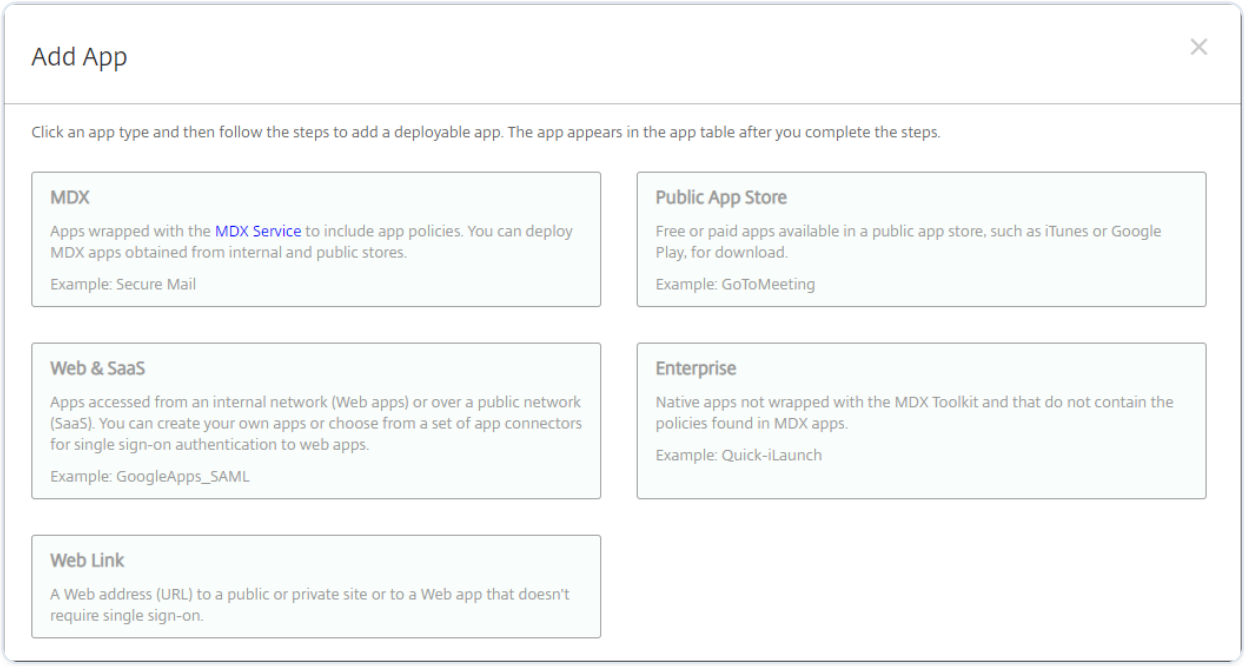
您可以从 Citrix Endpoint Management 控制台的“**应用程序**”选项卡配置 Web 链接。完成 Web 链接配置后，该链接将作为链接图标显示在“**应用程序**”表中的列表中。当用户使用 Citrix Secure Hub 登录时，该链接会与可用应用程序和桌面列表一起显示。

观看此视频了解更多信息：

要添加链接，请提供以下信息：

- 链接名称
- 链接说明
- Web 地址 (URL)
- 类别
- 角色
- PNG 格式的图像（可选）

1. 在 Citrix Endpoint Management 控制台中，单击“**配置 > 应用程序 > 添加**”。将显示“**添加应用程序**”对话框。

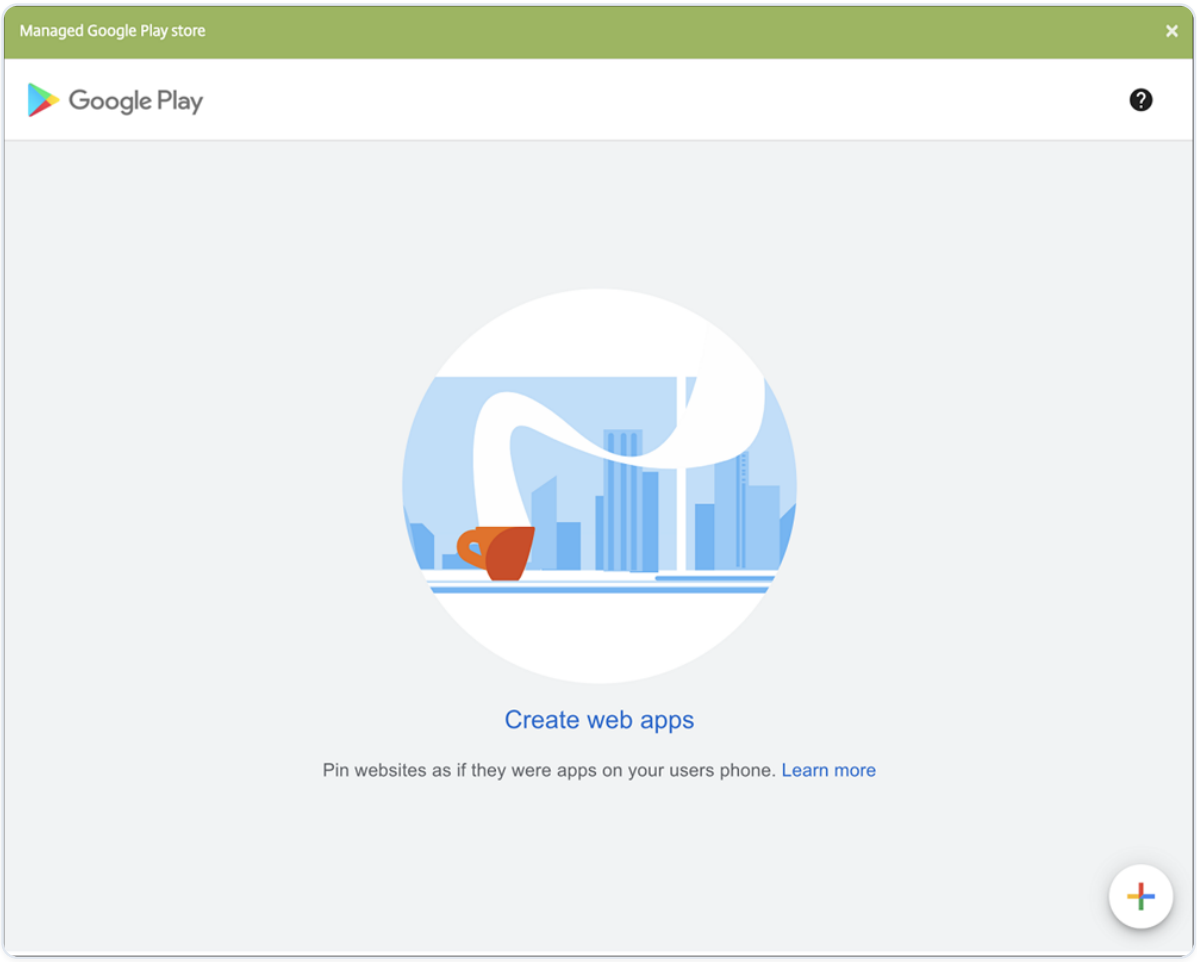


2. 单击“**Web 链接**”。将显示“**应用程序信息**”页面。
3. 在“**应用程序信息**”窗格中，键入以下信息：

   - **名称：** 键入应用程序的描述性名称。此名称将列在“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，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

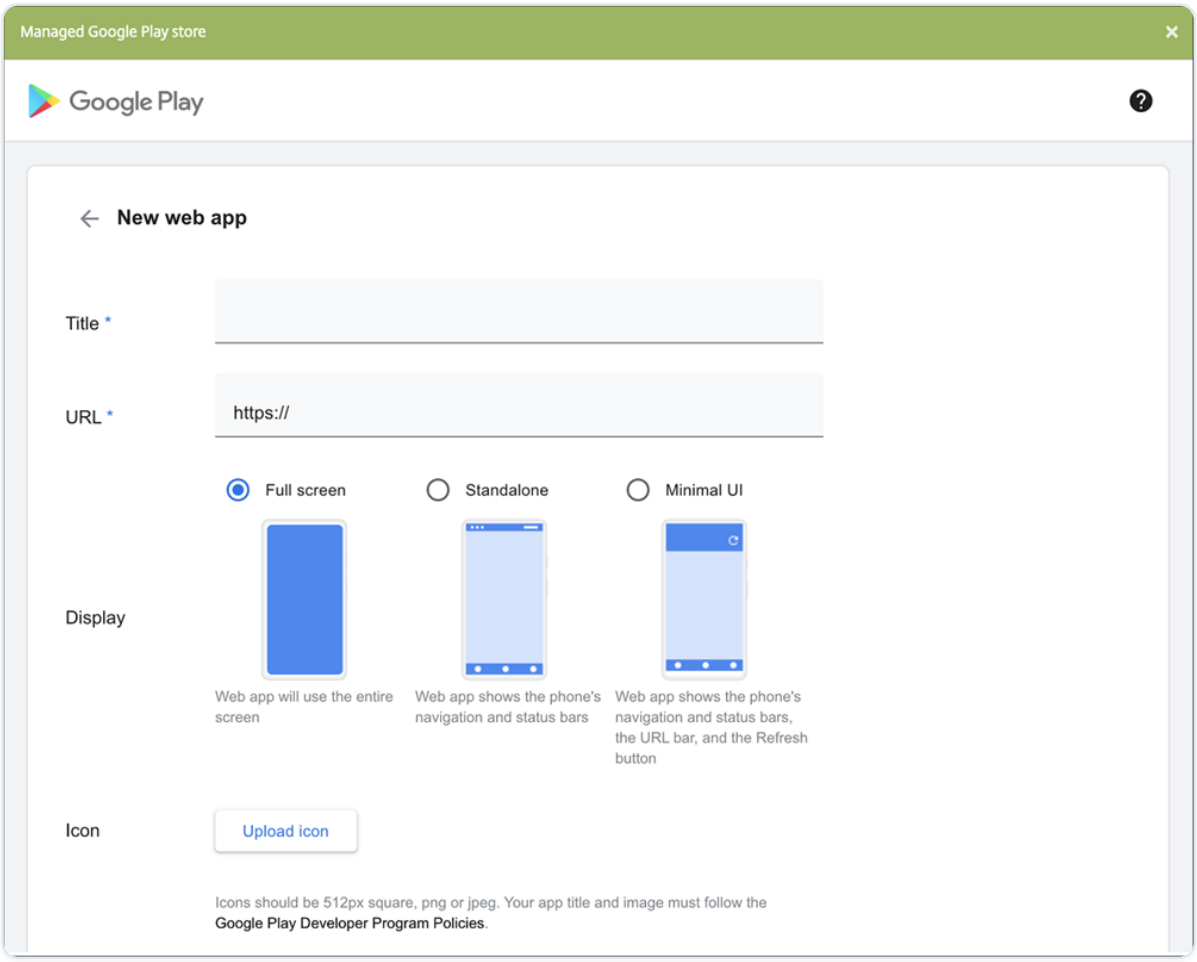
4. 单击“**下一步**”。将显示“**应用程序平台**”页面。
5. 在“**平台**”下，选择“**其他平台**”以添加适用于 iOS、Android（旧版设备管理员）和 Windows 8 的 Web 应用程序，或者选择“**Android Enterprise**”。清除所有不想包含的平台的复选框。

   - 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“**上传**”按钮以打开托管的 Google Play 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。



配置以下设置：

- **标题：** 键入 Web 应用程序的名称。
- **URL：**键入应用程序的网址。
- **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：**上传您自己的 Web 应用程序图像。



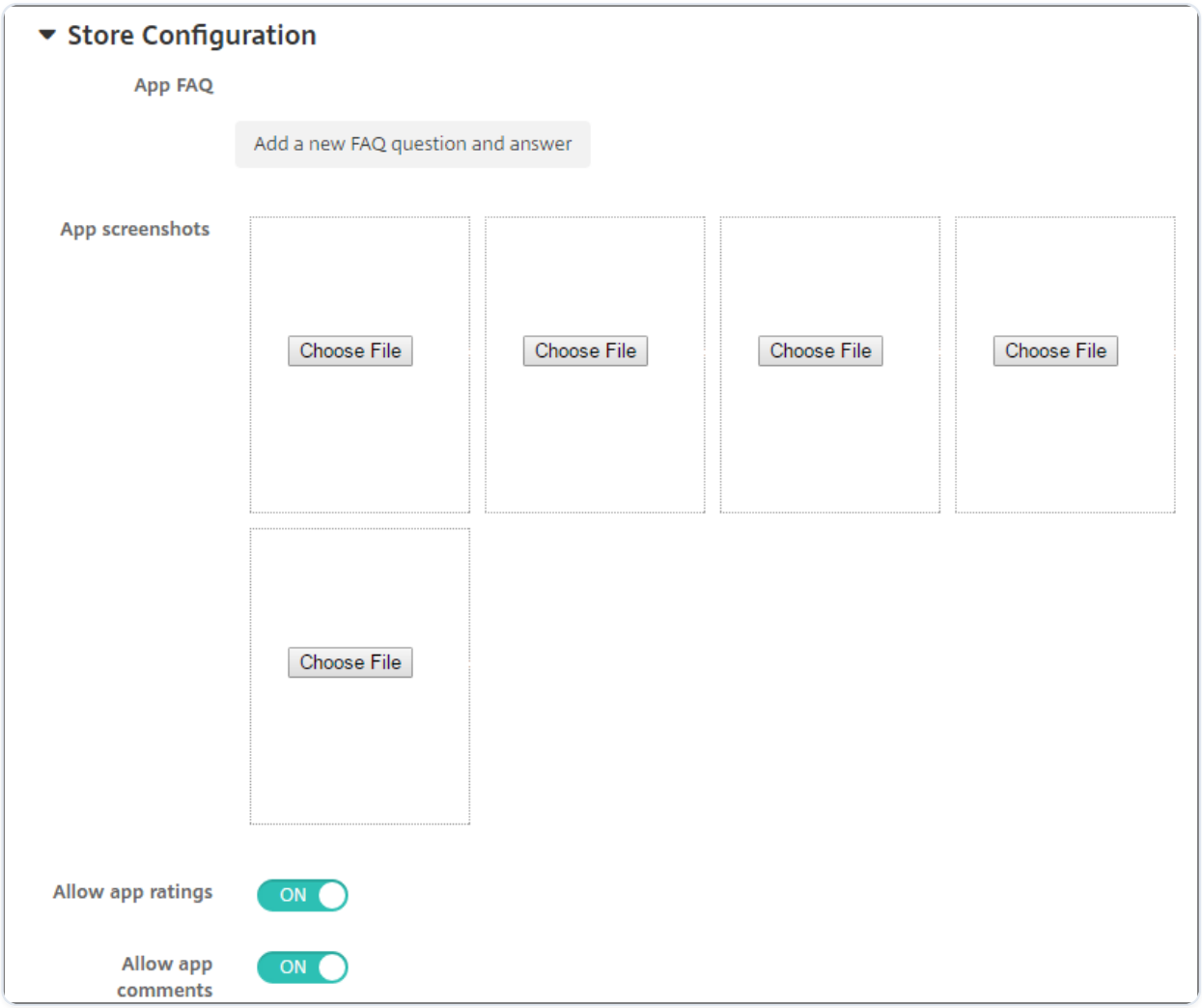
完成后，单击**创建**。您的 Web 应用程序可能需要长达 10 分钟才能发布。

6. 对于 Android Enterprise 以外的平台，请配置以下设置：

   - **应用程序名称：**接受预填充的名称或键入新名称。
   - **应用程序描述：**接受预填充的描述或键入您自己的描述。
   - **URL：**接受预填充的 URL 或键入应用程序的网址。根据您选择的连接器，此字段可能包含一个占位符，您必须先替换该占位符才能转到下一页。
   - **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 NetScaler Gateway 连接。将此选项设置为开**会将 VPN 关键字添加到应用程序，并允许用户通过 NetScaler Gateway 连接。默认值为**关**。
   - **应用程序类别：**在下拉列表中单击一个可选类别以应用于应用程序。
   - **图像：**选择是使用默认的 Citrix 图像还是上传您自己的应用程序图像。默认值为“使用默认值”。
     - 要上传您自己的图像，请单击**浏览**并导航到文件位置。文件必须是 .PNG 文件。您不能上传 JPEG 或 GIF 文件。添加自定义图形后，以后无法更改。

7. 配置部署规则。有关信息，请参阅配置部署规则。

8. 展开**商店配置**。



您可以选择配置以下内容：

- **应用程序常见问题解答：** 单击“**添加新的常见问题解答**”为应用程序创建常见问题解答。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用程序评分：** 允许用户在应用商店中对应用程序进行评分。
- **允许应用程序评论：** 允许用户在应用商店中对应用程序发表评论。

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在列表中选择一个或多个组。您选择的组将显示在“**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：** 选择是“**立即**”还是“**稍后**”部署应用程序。如果选择“**稍后**”，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“**仅当以前的部署失败时**”以在设备以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**”。

  当您在“**设置 > 服务器属性**”中配置了计划后台部署密钥时，“**部署以实现始终连接**”选项适用。

  始终连接选项：

  - 不适用于 iOS 设备
  - 对于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户不可用
  - 对于在版本 10.18.19 之前开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户不推荐

  您配置的部署计划适用于所有平台。您所做的任何更改都将应用于所有平台，但 **部署用于始终在线连接** 除外。

12. 单击 **保存**。

启用 Microsoft 365 应用程序

您可以打开 MDX 容器，以允许 Citrix Secure Mail、Citrix Secure Web 和 Citrix Files 将文档和数据传输到 Microsoft Office 365 应用程序。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

配置以下设置以分配或创建工作流：

- **要使用的工作流：** 在下拉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：** 为工作流键入一个唯一的名称。
  - **描述：** （可选）为工作流键入描述。
  - **电子邮件审批模板：** 在列表中，选择要分配的电子邮件审批模板。当您单击此字段右侧的眼睛图标时，将出现一个对话框，您可以在其中预览模板。
  - **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，选择要用于工作流的相应 Active Directory 域。
- **查找其他必需审批者：** 在搜索字段中键入其他必需人员的姓名，然后单击“**搜索**”。姓名源自 Active Directory。
- 当姓名出现在字段中时，选中姓名旁边的复选框。姓名和电子邮件地址将显示在“**选定的其他必需审批者**”列表中。

  要从“**选定的其他必需审批者**”列表中删除人员，请执行以下操作之一：

  - 单击“**搜索**”以查看所选域中所有人员的列表。
  - 在搜索框中键入完整或部分姓名，然后单击“**搜索**”以限制搜索结果。
  - “**选定的其他必需审批者**”列表中的人员在搜索结果列表中其姓名旁边有复选标记。滚动列表并清除要删除的每个姓名旁边的复选框。

应用商店和 Citrix Secure Hub 品牌

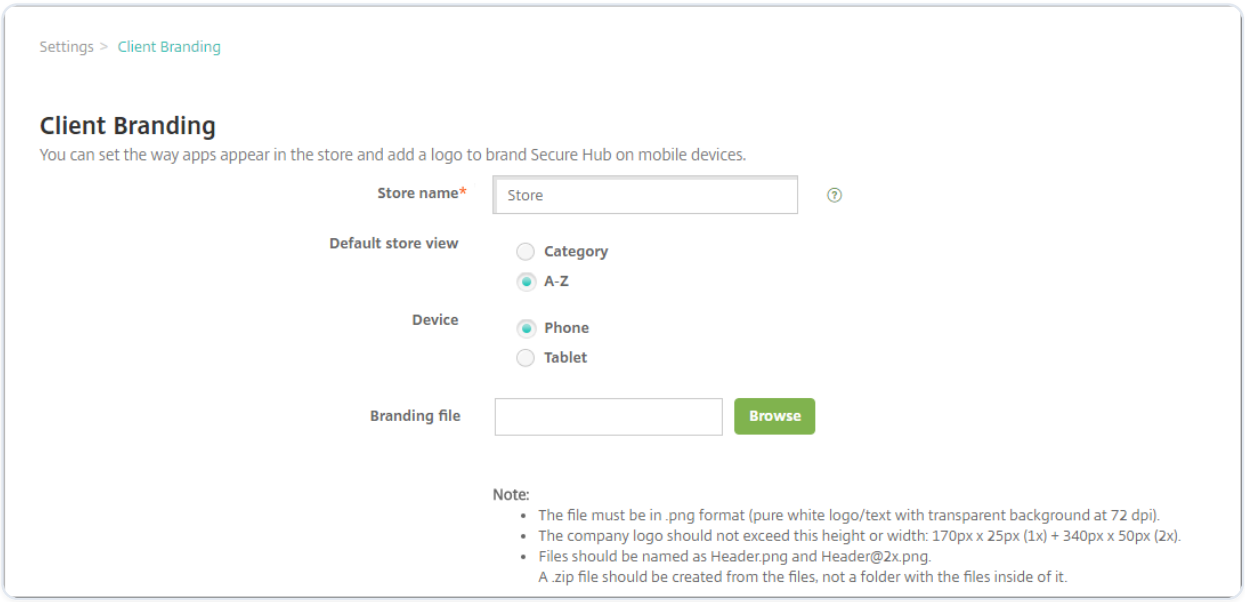
您可以设置应用在商店中的显示方式，并将您的徽标添加到 Citrix Secure Hub 和应用商店。这些品牌功能适用于 iOS 和 Android 设备。

开始之前，请确保您已准备好自定义图像并可访问。

自定义图像必须满足以下要求：

- 文件必须为 .png 格式
- 使用纯白色徽标或文本，背景透明，分辨率为 72 dpi。
- 公司徽标的高度或宽度不能超过：170 像素 x 25 像素 (1x) 和 340 像素 x 50 像素 (2x)。
- 将文件命名为 `Header.png` 和 `Header@2x.png`。
- 从这些文件创建 .zip 文件，而不是包含这些文件的文件夹。

1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。将显示“**设置**”页面。
2. 在“**客户端**”下，单击“**客户端品牌**”。将显示“**客户端品牌**”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。更改名称还会更改用于访问应用商店服务的 URL。通常不需要更改默认名称。

  > **重要：**
  >
  > 应用商店名称只能包含字母数字字符。

- **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“**手机**”或“**平板电脑**”。默认值为“**手机**”。
- **品牌文件：** 要选择品牌图像或图像的 .zip 文件，请单击“**浏览**”并导航到文件位置。

3. 单击“**保存**”。

要将此程序包部署到用户设备，请创建部署程序包，然后部署该程序包。

通过应用商店使用 Citrix Virtual Apps and Desktops

Citrix Endpoint Management 可以从 Citrix Virtual Apps and Desktops 收集应用程序，并在应用商店中向移动设备用户提供这些应用程序。用户可以直接在应用商店中订阅应用程序，并从 Citrix Workspace 启动它们。用户设备上必须安装 Citrix Workspace 应用程序才能启动这些应用程序。

要配置此设置，您需要本地 StoreFront 的完全限定域名 (FQDN) 或 IP 地址和端口号。

1. 在 Citrix 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**虚拟应用程序和桌面**。此时将显示**虚拟应用程序和桌面**页面。

   虚拟应用程序和桌面设置屏幕(/en-us/citrix-endpoint-management/media/settings-virtual-apps-and-desktops.png)

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 和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**以使用 Cloud Connector 连接到 StoreFront 服务器。然后，为连接指定**资源位置**和**允许的相对路径**。
     - **资源位置：**从 Citrix Cloud Connector 中定义的资源位置中选择。
     - **允许的相对路径：**指定资源位置允许的相对路径。每行指定一个路径。您可以使用星号 (*) 通配符。

     假设资源位置是 `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`

     要允许所有使用 URL `https://StoreFront.company.com/Citrix/PNAgent/*` 的请求，请输入此路径：`/Citrix/PNAgent/*`

     Citrix Endpoint Management 会阻止所有其他路径。

4. 单击 **测试连接** 以验证 Citrix Endpoint Management 是否可以连接到指定的 StoreFront 服务器。
5. 单击 **保存**。

应用连接器类型

下表列出了在 Citrix Endpoint Management 中添加 Web 或 SaaS 应用程序时可用的连接器及其类型。您还可以在添加 Web 或 SaaS 应用程序时向 Citrix Endpoint Management 添加连接器。

该表指示连接器是否支持用户帐户管理，这允许您自动创建帐户或通过使用工作流创建帐户。

连接器名称	SSO SAML	支持用户帐户管理
EchoSign_SAML	是	是
Globoforce_SAML		**注意：** 使用此连接器时，必须为预配启用用户管理，以确保无缝 SSO 集成。
GoogleApps_SAML	是	是
GoogleApps_SAML_IDP	是	是
Lynda_SAML	是	是
Office365_SAML	是	是
Salesforce_SAML	是	是
Salesforce_SAML_SP	是	是
SandBox_SAML	是	
SuccessFactors_SAML	是	
ShareFile_SAML	是	
ShareFile_SAML_SP	是	
WebEx_SAML_SP	是	是

Citrix 启动器

Citrix Launcher 允许您为由 Citrix Endpoint Management 部署的 Android Enterprise 设备和旧版 Android 设备自定义用户体验。借助 Citrix Launcher，您可以阻止用户访问某些设备设置，并将设备限制为单个应用或一小组应用。

Citrix Secure Hub 管理 Citrix Launcher 支持的最低 Android 版本为 Android 6.0。

使用**启动器配置策略**来控制以下 Citrix Launcher 功能：

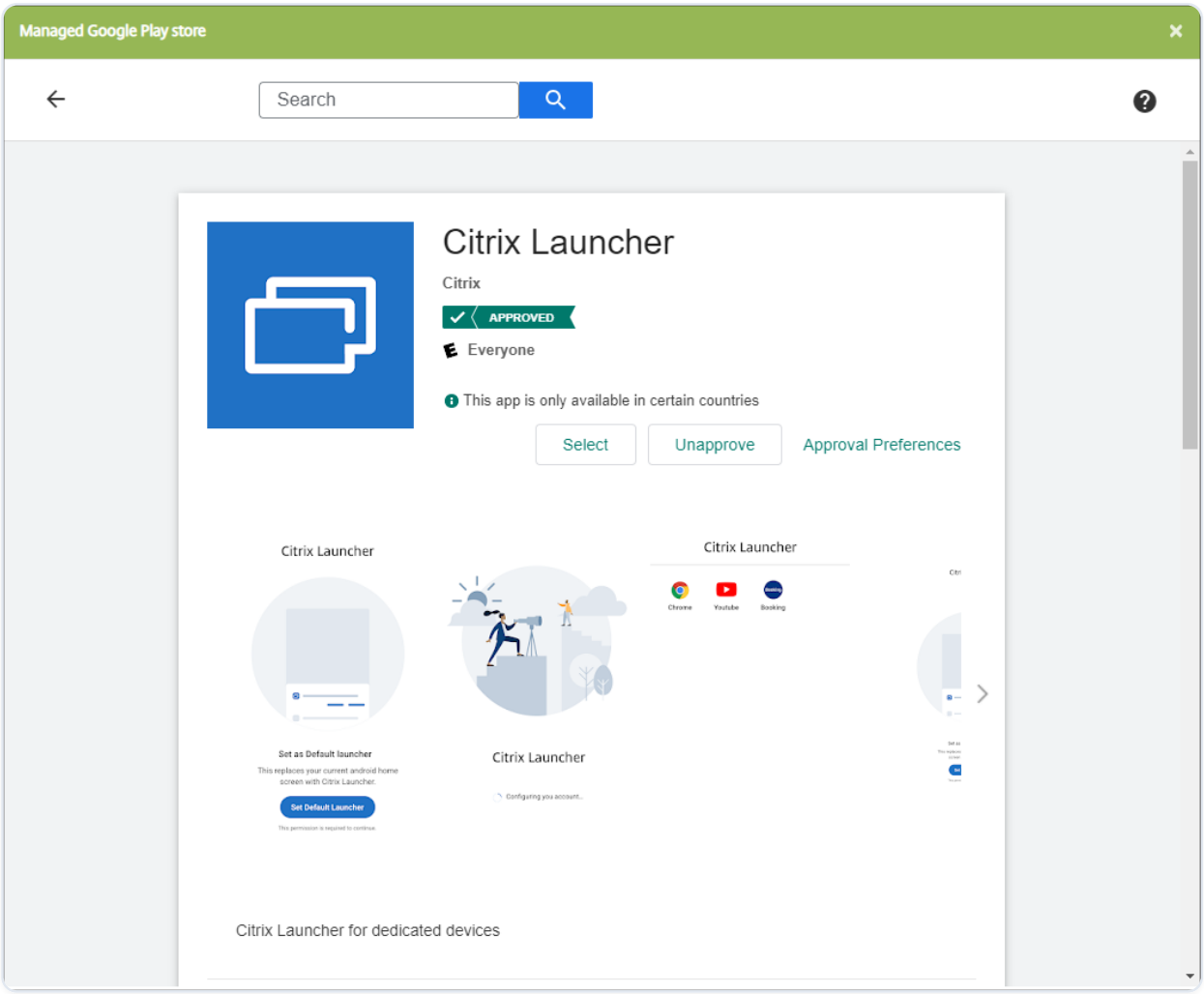
- 管理 Android Enterprise 设备和旧版 Android 设备，以便用户只能访问您指定的应用。
- 可选地为 Citrix Launcher 图标指定自定义徽标图像，并为 Citrix Launcher 指定自定义背景图像。

- 指定用户必须输入才能退出启动器的密码。

Citrix Launcher 并非旨在提供超出设备平台已提供的额外安全层。

为 Android Enterprise 设备设置 Citrix 启动器

1. 将 Citrix Launcher 应用 (com.citrix.launcher.droid) 作为公共应用商店应用添加到 Citrix Endpoint Management。在**配置 > 应用**中，单击**添加**，然后单击**公共应用商店**。有关详细信息，请参阅添加公共应用商店应用。



2. 在 Kiosk 设备策略中，指定哪些应用必须在公司拥有的专用设备（也称为 Android 企业拥有的单用途 (COSU) 设备）上可用。转到**配置 > 设备策略**，单击**添加**，然后选择 **Kiosk**。然后选择 Citrix Launcher 应用和允许列表中的任何其他应用。如果您之前已将应用添加到列表中，则无需再次上传这些应用。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。您无需添加在 Kiosk 策略中指定的所有应用。您必须仅在 Kiosk 策略中添加 Citrix Launcher 应用。有关详细信息，请参阅启动器配置策略。

4. 创建交付组并部署资源。有关详细信息，请参阅本文中的添加交付组和部署资源部分。

在您将 Citrix Launcher 部署到公司拥有的专用 Android Enterprise 设备后，Citrix Endpoint Management 会安装该应用并替换默认的 Citrix Secure Hub 启动器。如果您退出 Citrix Launcher 应用，Citrix Secure Hub 将再次成为默认启动器。

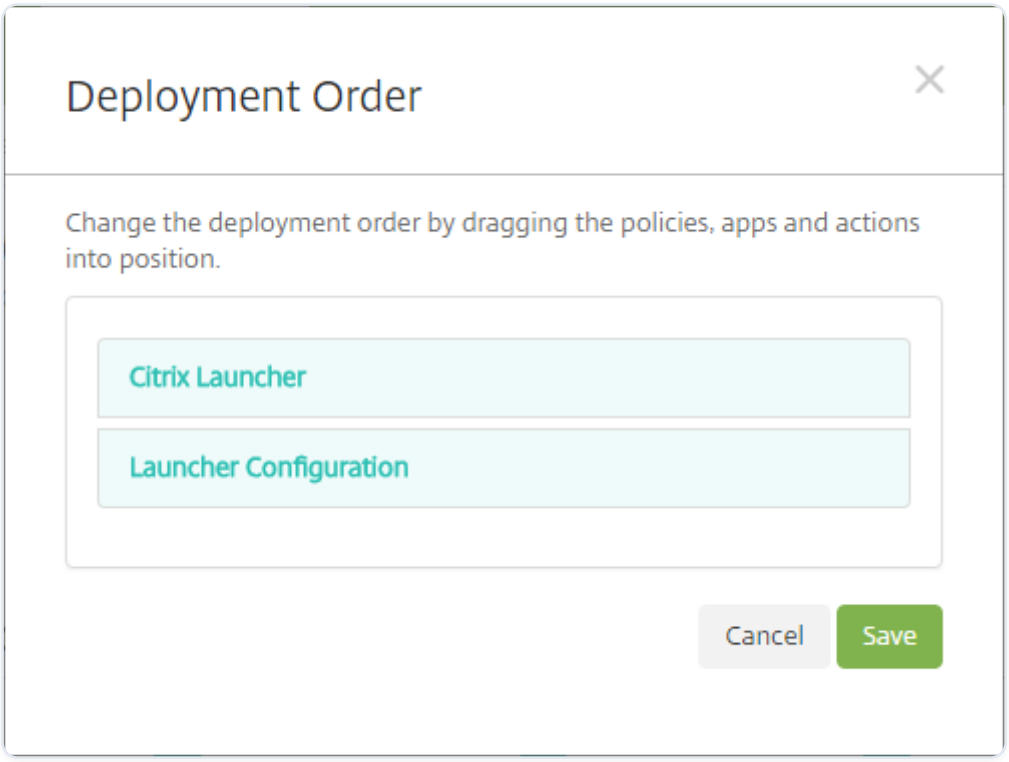
为旧版 Android 设备设置 Citrix Launcher

> **注意：**
>
> 2020 年 8 月，Citrix 弃用了对旧版 Android 设备上 CitrixLauncher.apk 的支持。您可以继续在 Android 设备上使用旧版 Citrix Launcher 应用程序 (com.citrix.launcher)，但不会收到新的功能更新。

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**。下载最新文件。该文件已准备好上传到 Citrix Endpoint Management，无需打包。
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 (/zh-cn/citrix-endpoint-management/policies/launcher-configuration-policy.html)。
3. 将 Citrix Launcher 应用程序作为企业应用程序添加到 Citrix 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 (/zh-cn/citrix-endpoint-management/apps.html#add-an-enterprise-app)。
4. 创建交付组并部署资源。有关详细信息，请参阅本文中的 (/zh-cn/citrix-endpoint-management/apps/citrix-launcher.html#add-a-delivery-group-and-deploy-resources) 部分。

添加交付组并部署资源

1. 在 **配置 > 交付组** 中，使用以下配置为 Citrix Launcher 创建一个交付组。
    - 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**所需应用程序**。
    - 在**摘要**页面上，单击**部署顺序**，并确保 **Citrix Launcher** 应用程序在**启动器配置**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详细信息，请参阅 (/zh-cn/citrix-endpoint-management/deploy-resources.html)。

管理没有 Citrix Launcher 的设备

您可以使用已有的功能，而不是使用 Citrix Launcher。

要预配专用设备：

1. 创建注册配置文件，方法是将**设备所有者模式**设置为**专用设备**。请参阅预配专用 Android Enterprise 设备和注册配置文件。
2. 创建自助服务终端设备策略，以将应用程序添加到允许列表并设置锁定任务模式。如果您之前已将应用程序添加到列表中，则无需再次上传这些应用程序。有关详细信息，请参阅Android Enterprise 设置。
3. 将每个设备注册到您创建的注册配置文件中。

使用 Apple 批量采购添加应用

Apple Business Manager (ABM) 和 Apple School Manager (ASM) 允许您批量购买应用和图书的许可证，并将批量采购信息与 Citrix Endpoint Management 同步。然后，您可以使用 Citrix Endpoint Management 将这些应用和图书部署到 iOS 和 macOS 设备。批量购买内容可简化组织查找、购买和分发应用和图书的过程。

有关使用 ABM 或 ASM 购买内容的更多信息，请参阅 Apple Business Manager 用户指南 或 Apple School Manager 用户指南。本文介绍了如何将批量购买的许可证从 ABM 和 ASM 同步到 Citrix Endpoint Management 以及如何管理这些许可证。

> **注意：**

> Apple 批量采购计划 (VPP) 自 January 14, 2021 起不再可用。批量采购功能已集成到 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 从 Apple 部署计划升级。

关于 Apple 批量采购

使用 ABM 或 ASM 批量购买内容时，请注意以下事项：

- 您可以购买以下内容的许可证：
  - 公共应用和图书
  - 专为您的组织开发的自定义应用
- 您可以将批量购买的应用和图书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。
- 有关分发应用的更多信息，请参阅 分发 Apple 应用。
- 有关已知问题的列表，请参阅知识中心文章 CTX222633。

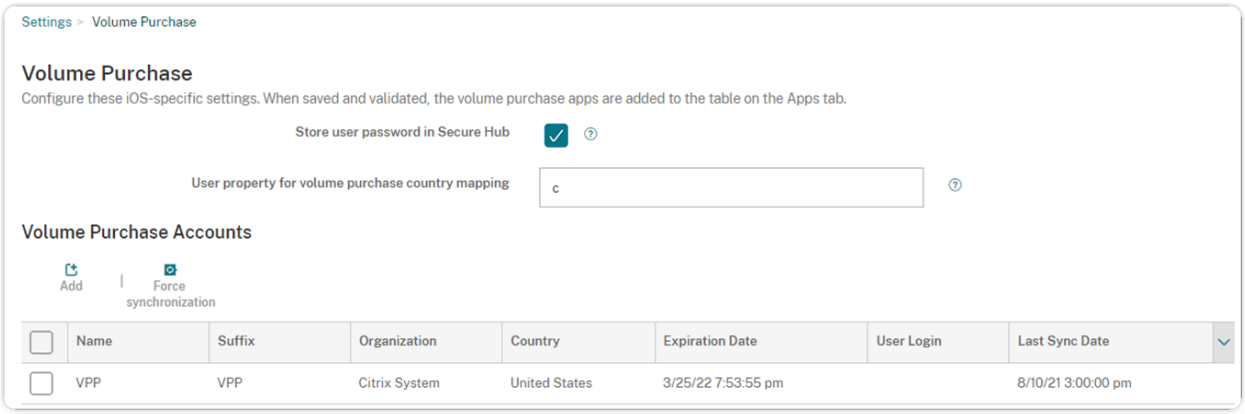
添加批量采购帐户

在 ABM 或 ASM 门户中购买内容后，从门户下载与 Citrix Endpoint Management 关联的内容令牌。接下来，在 Citrix Endpoint Management 中，基于此内容代码创建批量采购帐户。此代码允许 Citrix Endpoint Management 从 ABM 或 ASM 同步内容许可证。

通过批量采购，您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码并希望更改为托管许可证，请参阅 Apple 支持文档。

在 Citrix Endpoint Management 中添加批量采购帐户

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安全位置。
2. 在 Citrix 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“**批量采购**”。此时将显示“**批量采购**”配置页面。

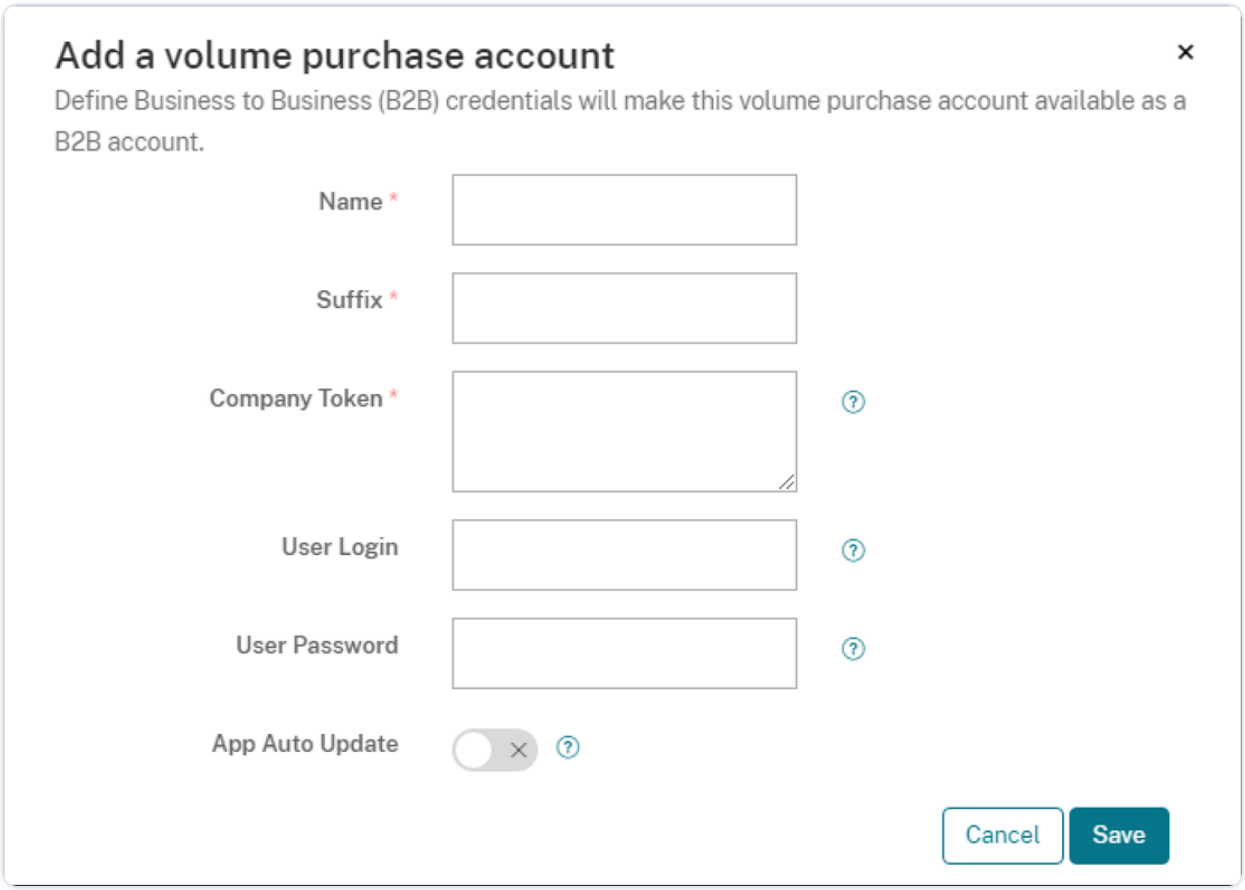


4. 配置以下设置：

   - **在 Citrix Secure Hub 中存储用户密码：** 选择是否在 Citrix Secure Hub 中存储用户名和密码以进行 Citrix Endpoint Management 身份验证。默认值为“**开**”。
   - **用于批量采购国家/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特定国家/地区的应用程序商店下载应用程序。请联系您的内容管理员获取此代码。

     Citrix Endpoint Management 使用国家/地区映射代码来选择批量采购的属性池。例如，如果用户属性是美国，则如果映射代码是英国，用户将无法下载应用程序。

5. 单击“**添加**”。此时将显示“**添加批量采购帐户**”对话框。



6. 配置以下帐户设置：

> **注意：**
>
> 如果您使用 Apple Configurator 1，请按如下方式上载许可证文件：单击“**配置 > 应用程序**”，转到应用程序的平台页面，然后展开“**批量采购**”。

- **名称：**键入帐户的描述性名称。
- **后缀：**键入将与从 Apple Store 继承的应用程序名称一起显示的后缀。例如，如果输入 **VP**，则 **Citrix Secure Mail** 应用程序在应用程序列表中显示为 **Citrix Secure Mail - VP**。
- **公司令牌：**复制并粘贴在步骤 1 中下载的内容令牌。
- **用户登录：**(可选) 键入此批量购买帐户管理员的用户名。如果已配置，则同步批量购买的自定义应用程序到 Citrix Endpoint Management 需要用户名和密码。
- **用户密码：**(可选) 键入您输入的用户名的密码。
- **应用程序自动更新：如果设置为开**，则当有新版本可用时，Citrix Endpoint Management 控制台中的批量购买应用程序和可选应用程序将自动更新。您仍然必须在 Citrix 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。如果此设置设置为**关**，您仍然可以在 Citrix Endpoint Management 控制台中手动更新批量购买的应用程序。应用程序在控制台中更新后，安装了该应用程序的设备也会收到该更新。默认设置为**关**。

成功添加批量帐户后，将显示一条消息，通知您以下内容：

- 在**配置 > 应用程序**页面上，批量购买的应用程序显示在应用程序列表中。应用程序名称将显示您配置的后缀。
- 在**配置 > 媒体**页面上，批量购买的图书显示在媒体列表中。图书名称将显示您配置的后缀。

配置批量购买的应用程序

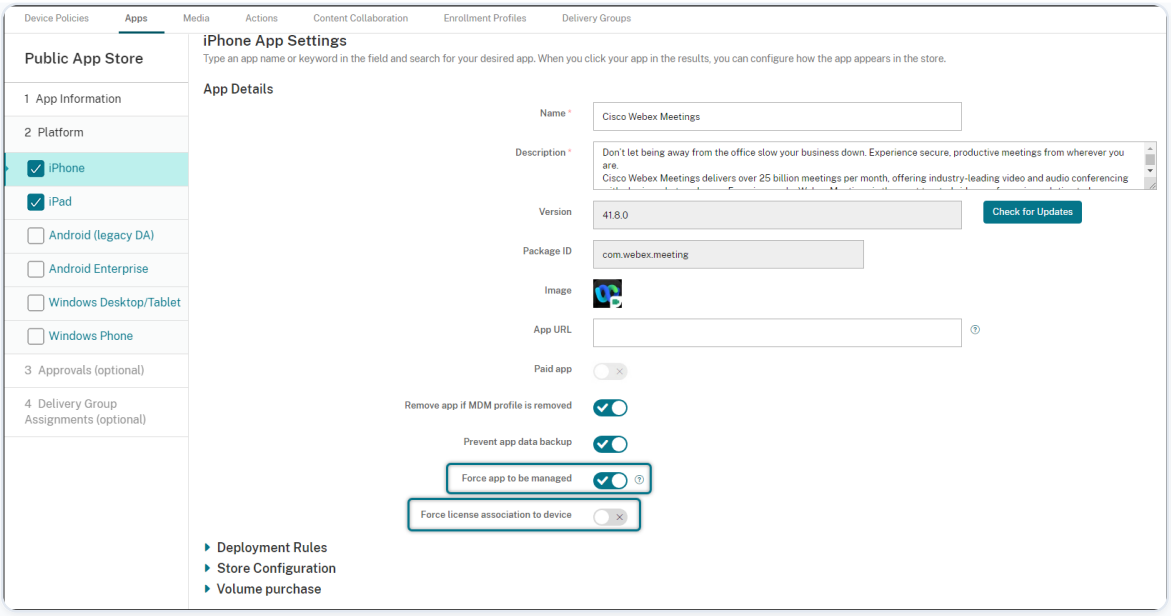
添加批量购买帐户后，应用程序信息将同步到 Citrix Endpoint Management 并显示在**配置 > 应用程序**页面上。您现在可以配置这些应用程序，调整交付组，并为 iOS 和 macOS 设备调整设备策略设置。完成配置后，用户可以注册其设备。

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：
  - 要让 Citrix Endpoint Management 将应用程序部署到设备而不是用户，请打开**强制许可证关联到设备**。启用此设置后，用户无需使用其 Apple ID 即可下载应用程序，而无需登录其 App Store 帐户。

- 我们建议您为应用程序打开**强制应用程序受管**，以便其自动安装为受管应用程序。

> **注意：**
>
> 要使“**强制管理应用**”设置生效，您必须在“**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



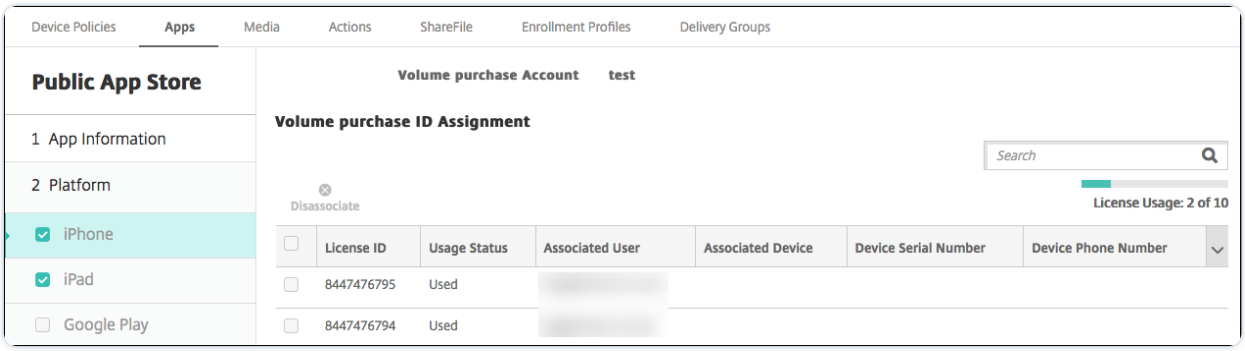
- 在“**配置 > 交付组**”页面上：

  要使应用在用户设备上静默安装且用户交互最少，请转到“**应用**”页面，然后将应用拖动到“**所需应用**”列表。默认情况下，除 Citrix Secure Hub 之外的应用都是“**可选应用**”，这意味着用户必须通过 Citrix Secure Hub 手动启动应用安装。

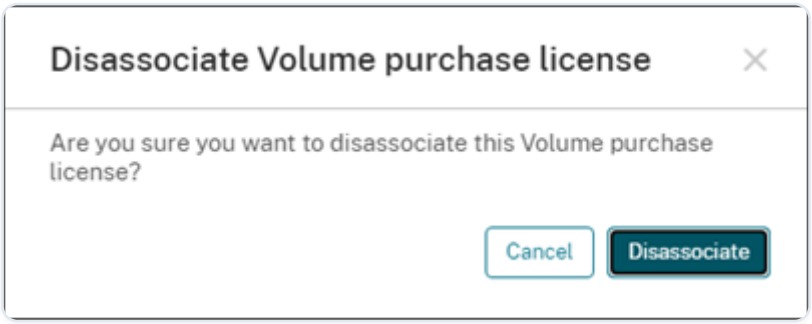
跟踪和管理应用许可证的使用

您可以跟踪应用许可证的使用情况。如果需要，您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**”。
2. 选择一个应用，然后单击“**编辑**”。
3. 转到“**平台**”页面，然后展开“**批量购买**”。 在“**批量购买 ID 分配**”表中，您可以跟踪已使用的许可证数量以及由哪个用户或设备使用。



4. 要收回许可证，请选择该许可证，然后单击“**取消关联**”。



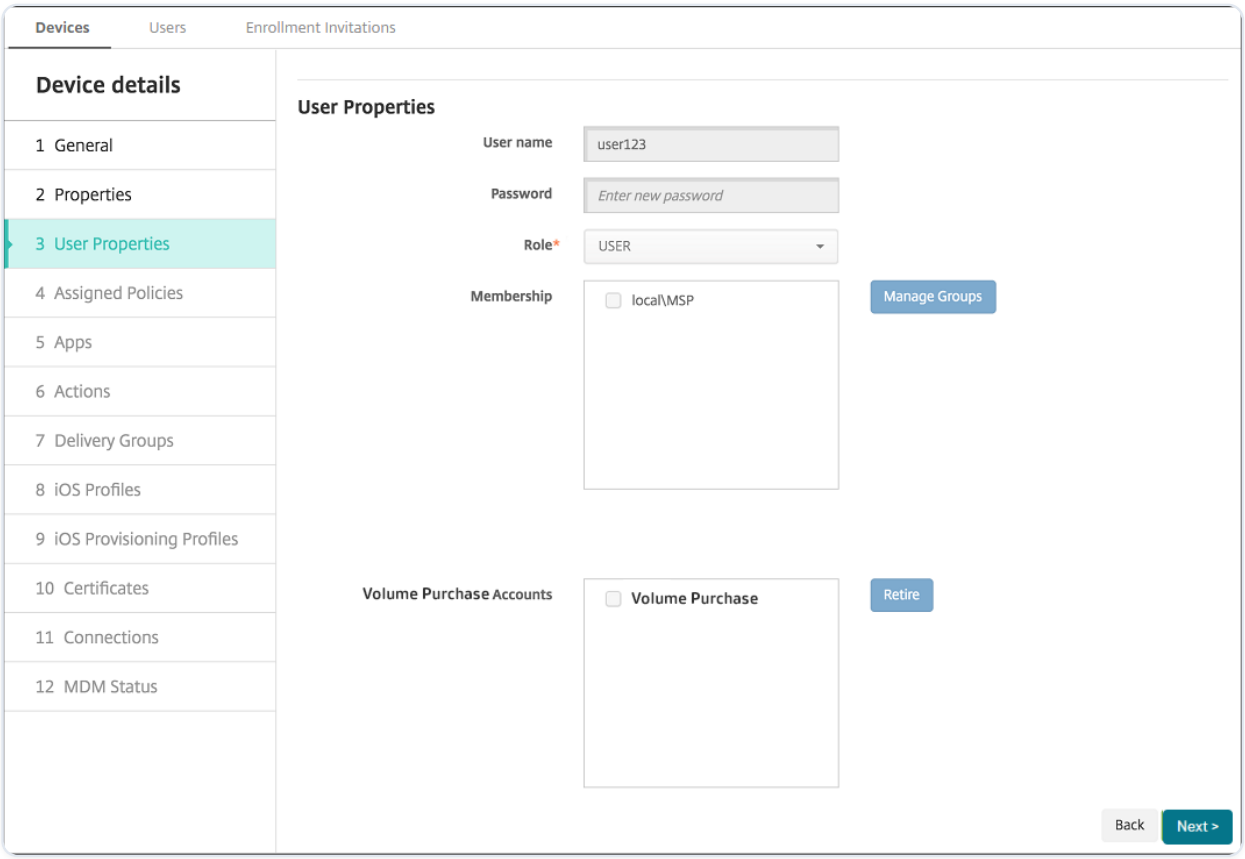
5. 单击“**取消关联**”以确认操作。

从批量购买帐户中停用用户

如果将应用程序许可证与用户关联，则可以从批量购买帐户中停用用户，以收回分配给这些用户的所有许可证。一个用例是当用户离开您的组织时。

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. 转到**用户属性**页面，并根据需要选择批量购买帐户。

4. 单击**停用**。



Citrix Endpoint Management 将从用户处撤销所选批量购买帐户中的应用程序许可证。

同步应用程序信息

Citrix Endpoint Management 会定期将应用程序信息与 ABM 或 ASM 同步。如果需要，您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。此类更改包括您手动从批量购买帐户中删除应用程序的情况。

更改默认同步间隔

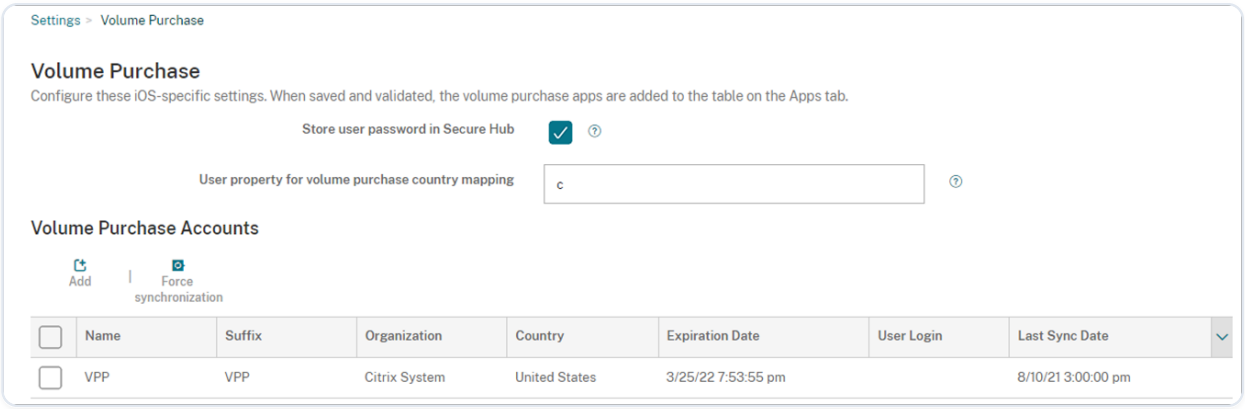
默认情况下，Citrix Endpoint Management 至少每 1440 分钟（24 小时）刷新一次批量购买许可证基线。Citrix Cloud 管理员可以通过服务器属性 `vpp.baseline` 更改默认间隔。有关详细信息，请参阅服务器属性。

手动同步应用程序信息

您可以强制与 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，不选择批量购买帐户，直接单击**强制同步**以同步所有帐户。



3. 确认同步操作。同步开始。

   同步可能需要几分钟，具体取决于批量购买许可证的数量。同步完成后，Citrix 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。

检查应用更新

如果您在添加批量采购帐户时开启了“**应用自动更新**”设置，Citrix Endpoint Management 会定期检查批量采购应用和可选应用的新版本并进行更新。如果需要，您可以手动检查任何应用的新版本，并将应用更新应用于 Citrix Endpoint Management。

Citrix Endpoint Management 收到所需应用的新版本后，它会将新版本推送到设备进行静默安装，而无需提示用户。

检查并应用应用的新版本

1. 单击“**配置 > 应用**”。此时将显示“**应用**”页面。
2. 选择一个应用，然后单击“**编辑**”。
3. 转到“**平台**”页面，然后单击“**版本**”旁边的“**检查更新**”。
4. 在显示的“**更新**”对话框中，如果有新版本可用，请应用更新。

续订批量采购帐户的内容令牌

内容令牌每年到期。当令牌即将到期时，Citrix Endpoint Management 会显示许可证到期警告。请及时续订内容令牌，以防止用户中断。

1. 从 ABM 或 ASM 门户下载更新的令牌。
2. 在 Citrix 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“**批量采购**”。此时将显示批量采购配置页面。

4. 使用更新的令牌信息编辑您的批量采购帐户。

将 ShareFile 与 Citrix Endpoint Management 结合使用

> **免责声明：**
>
> 如果 ShareFile（现为 Progress）停止支持，此功能将被弃用。

> Citrix Endpoint Management 提供了两种与 ShareFile 集成的方法：Citrix Files 和存储区域连接器。

思杰文件

您可以将 Citrix Endpoint Management 配置为提供对您的 ShareFile 帐户的访问。该配置：

- 为移动用户提供对完整 ShareFile 功能集的访问，例如文件共享、文件同步和存储区域连接器。
- 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和全面的访问控制策略。
- 通过 Citrix Endpoint Management 控制台提供 ShareFile 配置、服务级别监控和许可证使用情况监控。

有关为企业帐户配置 Citrix Endpoint Management 的更多信息，请参阅 SAML for single sign-on with Citrix Files。

存储区域连接器

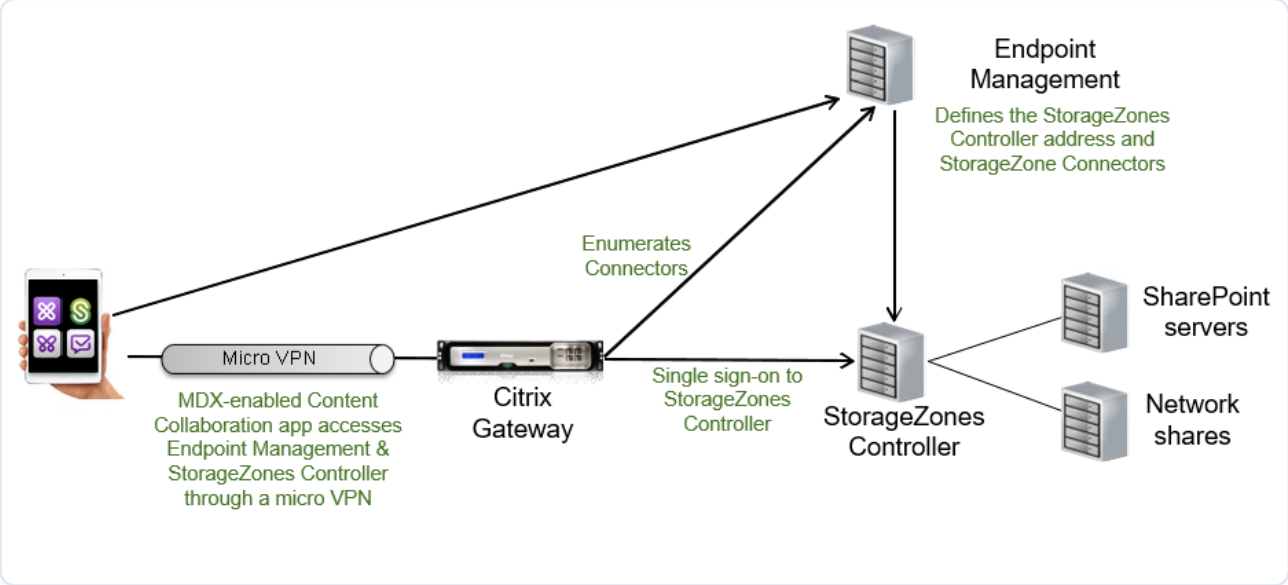
您可以将 Citrix Endpoint Management 配置为仅提供对通过 Citrix Endpoint Management 控制台创建的存储区域连接器的访问。该配置：

- 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 ShareFile 子域或托管 Citrix Files 数据。
- 通过适用于 iOS 和 Android 的 Citrix Files 的 Citrix 移动生产力应用程序，为用户提供对数据的移动访问。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。
- 遵守安全限制，防止用户信息泄露到公司网络之外。
- 通过 Citrix Endpoint Management 控制台提供存储区域连接器的简单设置。如果您以后决定将完整的 Citrix Files 功能与 Citrix Endpoint Management 结合使用，可以在 Citrix Endpoint Management 控制台中更改配置。

对于仅与存储区域连接器集成的 Citrix Endpoint Management：

- ShareFile 使用您的单点登录配置到 NetScaler Gateway，以通过存储区域控制器进行身份验证。
- Citrix Endpoint Management 不通过 SAML 进行身份验证，因为未使用 Citrix Files 控制平面。

下图显示了 Citrix Endpoint Management 与存储区域连接器配合使用的高级架构。



要求

- 最低组件版本：
  - 适用于 iOS 的 ShareFile (MDX) 5.3
  - 适用于 Android 的 ShareFile (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
- 确保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。

适用于 Citrix Files Data 的存储区域和受限存储区域的要求不适用于仅与存储区域连接器集成的 Citrix Endpoint Management。

Citrix Endpoint Management 不支持 Documentum 连接器。

- 要运行 PowerShell 脚本：
  - 在 32 位 (x86) 版本的 PowerShell 中运行脚本。

安装任务

按照所示顺序完成以下任务，以安装和设置存储区域控制器。这些步骤仅适用于 Citrix Endpoint Management 与存储区域连接器的集成。其中一些文章位于存储区域控制器文档中。

1. 为存储区域控制器配置 NetScaler

   您可以将 NetScaler 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。托管受限区域并使用内部地址的存储区域控制器不需要 SSL 证书。

3. 准备服务器

   存储区域连接器需要 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配合使用
6. 为存储区域指定代理服务器

   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。您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

   配置域控制器以支持网络共享或 SharePoint 站点上的 NTLM 或 Kerberos 身份验证。

8. 将辅助存储区域控制器加入存储区域

   要为高可用性配置存储区域，请至少连接两个存储区域控制器。

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. 从 ShareFile 工具/应用程序下载，登录并下载最新的存储区域控制器安装程序。

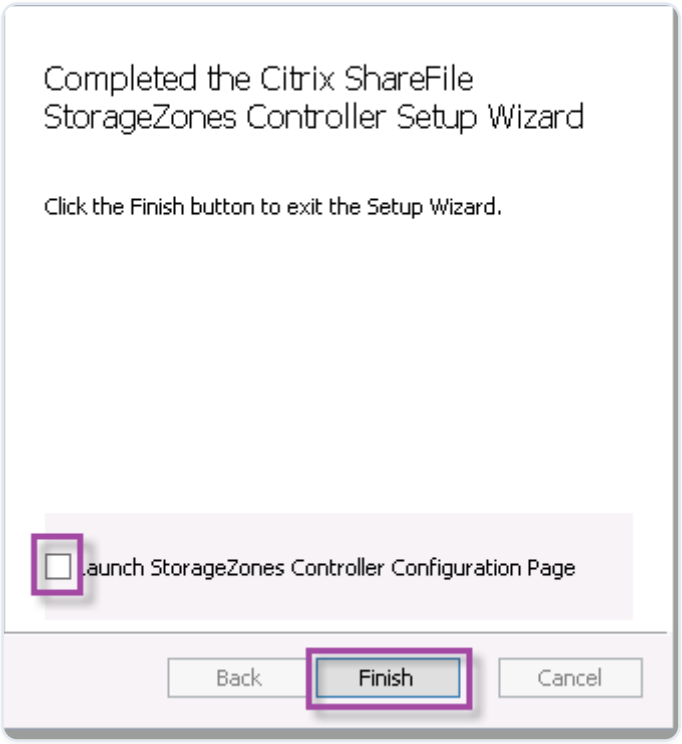
   b. 安装存储区域控制器会将服务器上的默认网站更改为控制器的安装路径。在默认网站上启用**匿名身份验证**。

2. 在要安装存储区域控制器的服务器上，运行 StorageCenter.msi。

   存储区域控制器安装向导启动。

3. 响应提示：

- 在 **目标文件夹** 页面中，如果 Internet Information Services (IIS) 安装在默认位置，请保留默认设置。否则，请浏览到 IIS 安装位置。
- 安装完成后，清除 **启动存储区域控制器配置页面** 复选框，然后单击 **完成**。



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，请考虑改用 HTTP 连接。）如果安装成功，将显示 Citrix Files 徽标。

   如果未显示 Citrix Files 徽标，请清除浏览器缓存，然后重试。

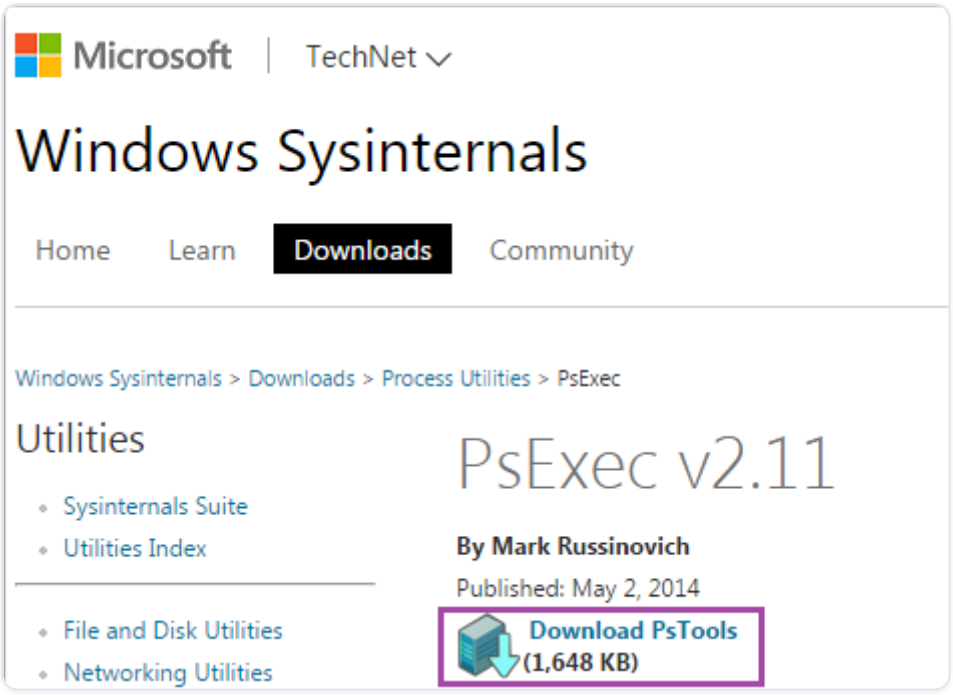
> **重要：**
>
> 如果计划克隆存储区域控制器，请在继续配置存储区域控制器之前捕获磁盘映像。

准备存储区域控制器以仅与存储区域连接器配合使用

对于仅与存储区域连接器集成的部署，您无需使用存储区域控制器管理控制台。该界面需要 Citrix Files 管理员帐户，而此解决方案不需要该帐户。因此，您需要运行 PowerShell 脚本来准备存储区域控制器，使其在没有 Citrix Files 控制平面的情况下使用。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。您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短语。

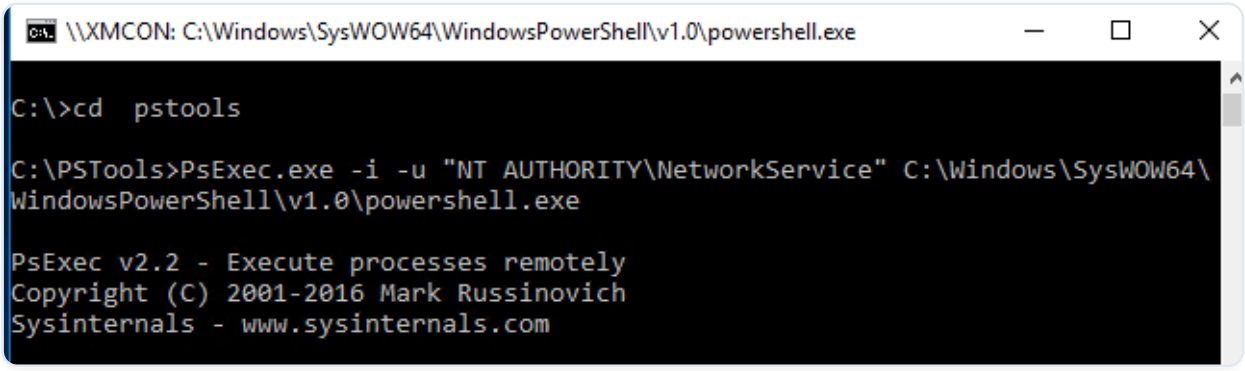
1. 从存储区域控制器服务器下载 PsExec 工具：导航到 Microsoft Windows Sysinternals，然后单击**下载 PsTools**。将该工具解压到 C 盘的根目录。



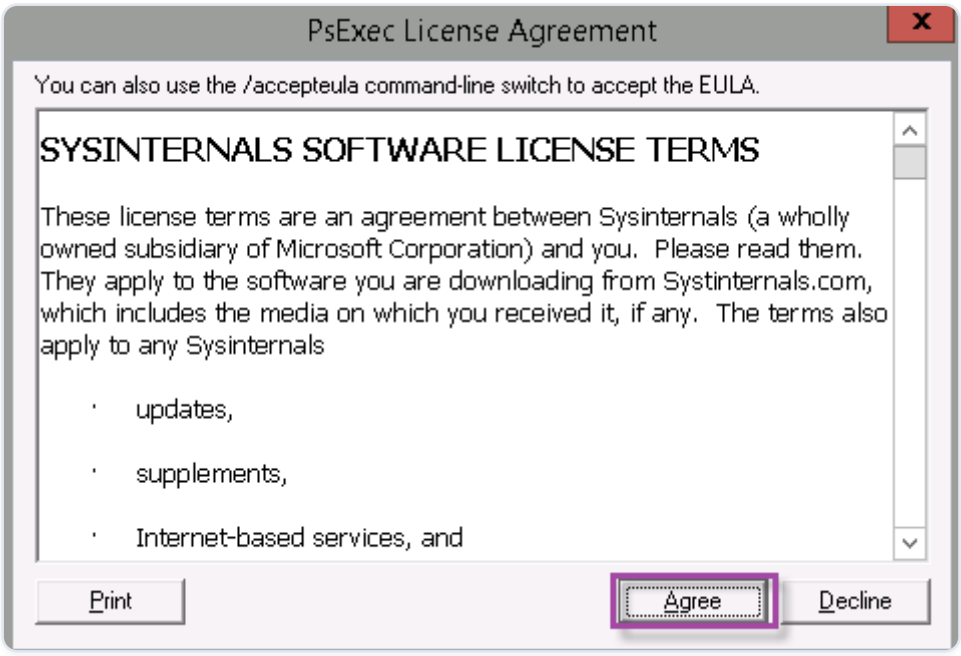
2. 运行 PsExec 工具：以管理员用户身份打开命令提示符，然后键入以下内容：

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. 出现提示时，单击**同意**以运行 Sysinternals 工具。



将打开一个 PowerShell 窗口。

4. 在 PowerShell 窗口中，键入以下内容：

```
```

Import-Module "C:
\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

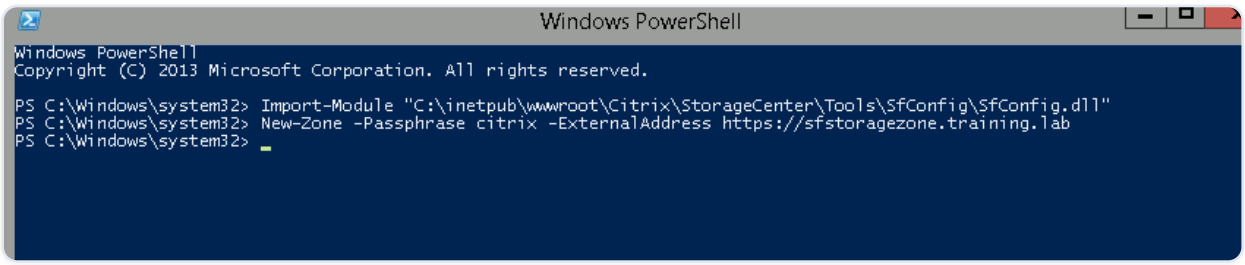
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com

```
```

其中：

密码短语： 是您要分配给站点的密码短语。请记下它。您无法从控制器恢复密码短语。如果您丢失了密码短语，则无法重新安装存储区域、将更多存储区域控制器加入存储区域，或者在服务器发生故障时恢复存储区域。

外部地址： 是存储区域控制器服务器的外部完全限定域名。



您的主存储区域控制器现已就绪。

在登录 Citrix Endpoint Management 以创建存储区域连接器之前：请完成以下配置（如果适用）：

为存储区域指定代理服务器

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，请参阅在 Citrix Endpoint Management 中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

要配置高可用性存储区域，请至少连接两个存储区域控制器。要将辅助存储区域控制器加入某个区域，请在第二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. 在要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，键入以下内容：

```
Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
```

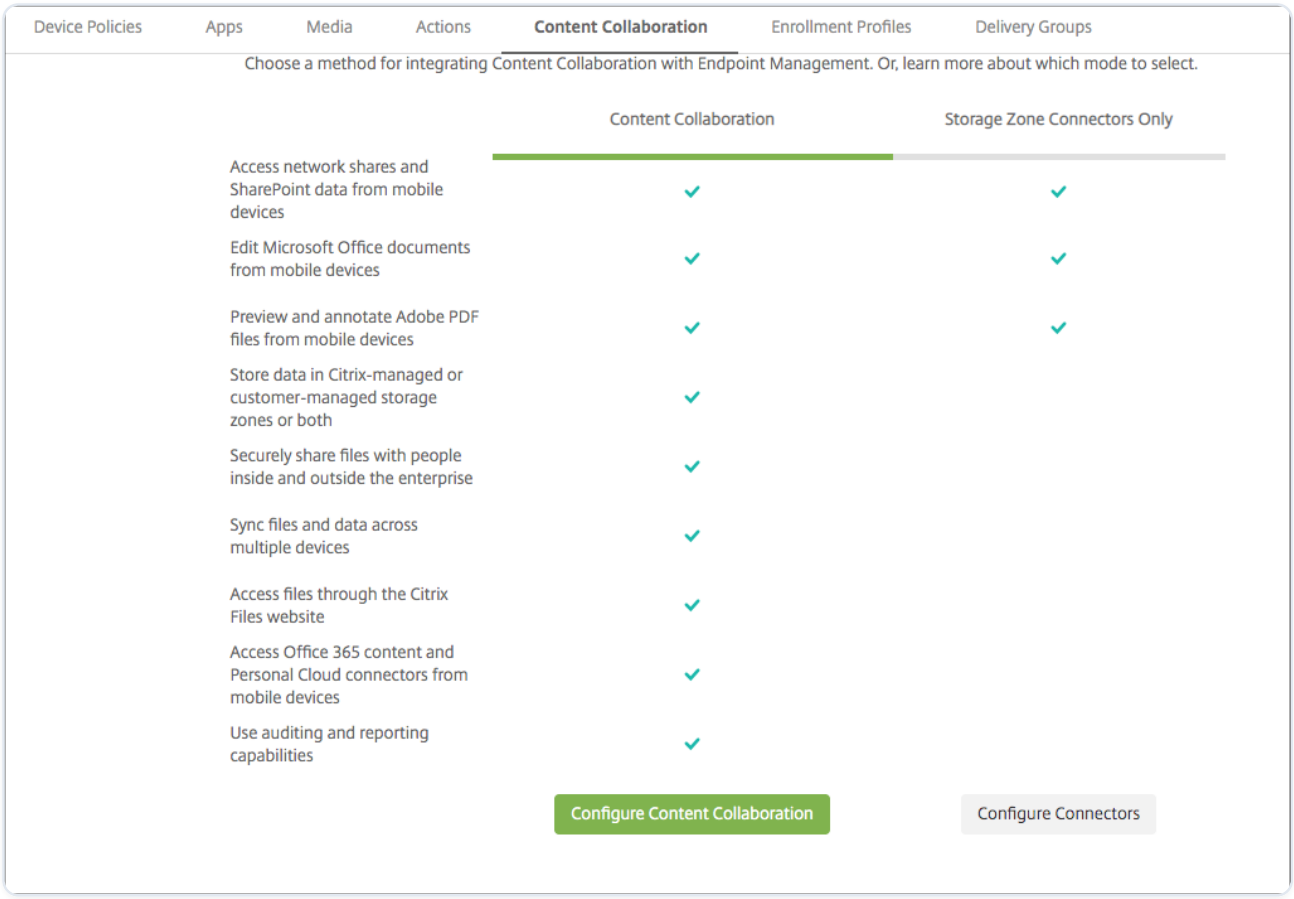
例如：

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

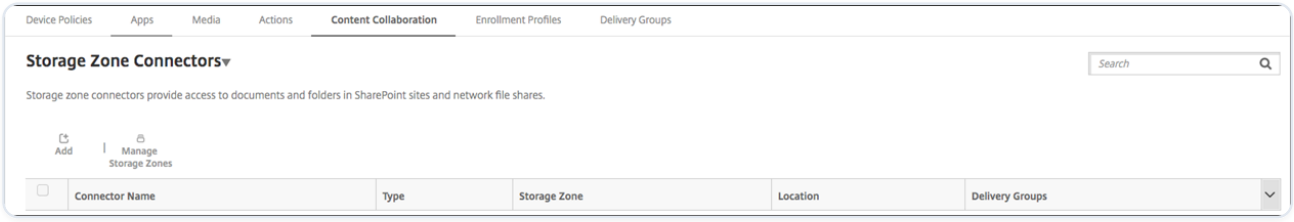
在 Citrix Endpoint Management 中定义存储区域控制器连接

在添加存储区域连接器之前，您需要为每个已启用存储区域连接器的存储区域控制器配置连接信息。您可以按照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。

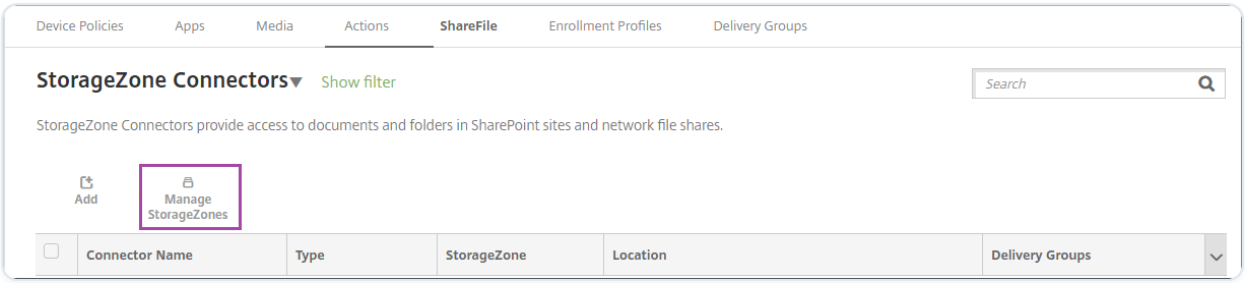
首次访问 **Configure > ShareFile** 页面时，该页面会总结使用 Citrix Endpoint Management 处理企业帐户和存储区域连接器之间的区别。



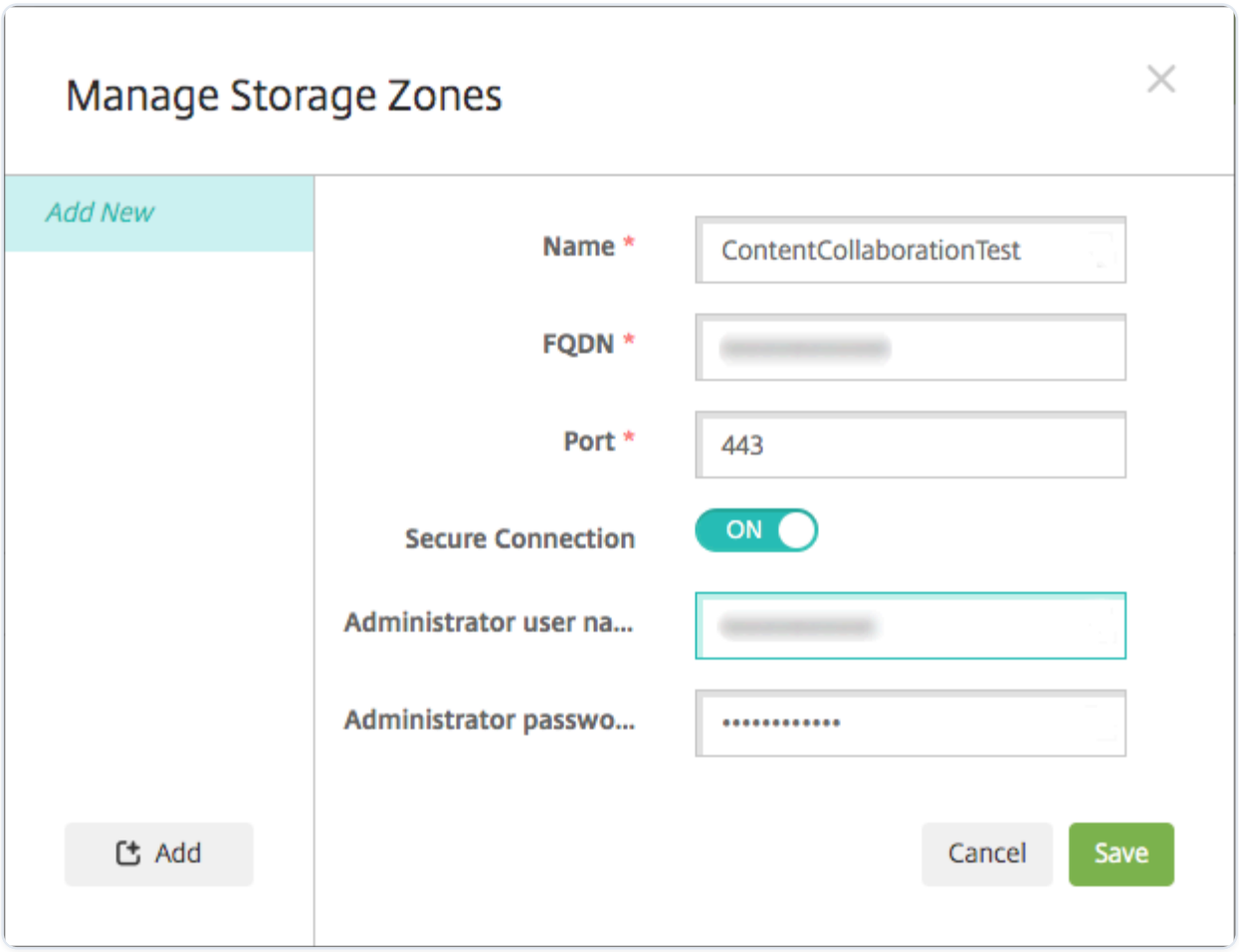
单击 **Configure Connectors** 以继续本文中的配置步骤。



1. 在 **配置 > ShareFile** 中，单击 **管理存储区域**。



2. 在 **Manage Storage Zones** 中，添加连接信息。



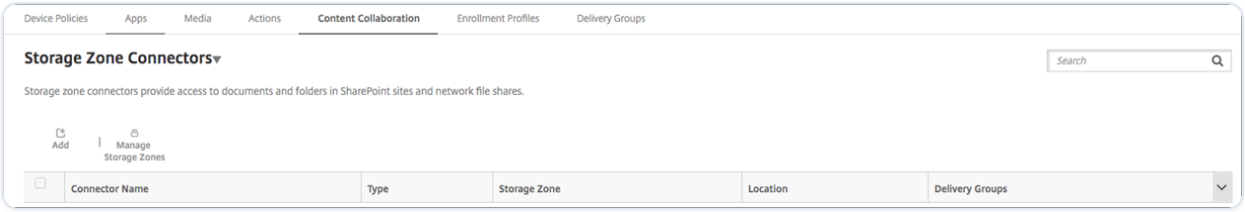
- **名称：** 存储区域的描述性名称，用于在 Citrix Endpoint Management 中标识存储区域。名称中不要包含空格或特殊字符。
- **FQDN 和端口：** 可从 Citrix Endpoint Management 服务器访问的存储区域控制器的完全限定域名和端口号。
- **安全连接：** 如果您使用 SSL 连接到存储区域控制器，请使用默认设置“开”。如果您不使用 SSL 连接，请将此设置更改为“关”。
- **管理员用户名**和**管理员密码**：管理员服务帐户用户名（格式为 domain\\admin）和密码。或者，一个对存储区域控制器具有读写权限的用户帐户。

3. 单击**保存**。
4. 要测试连接，请验证 Citrix Endpoint Management 服务器能否通过端口 443 访问存储区域控制器的完全限定域名。
5. 要定义另一个存储区域控制器连接，请单击**管理存储区域**中的**添加**按钮。

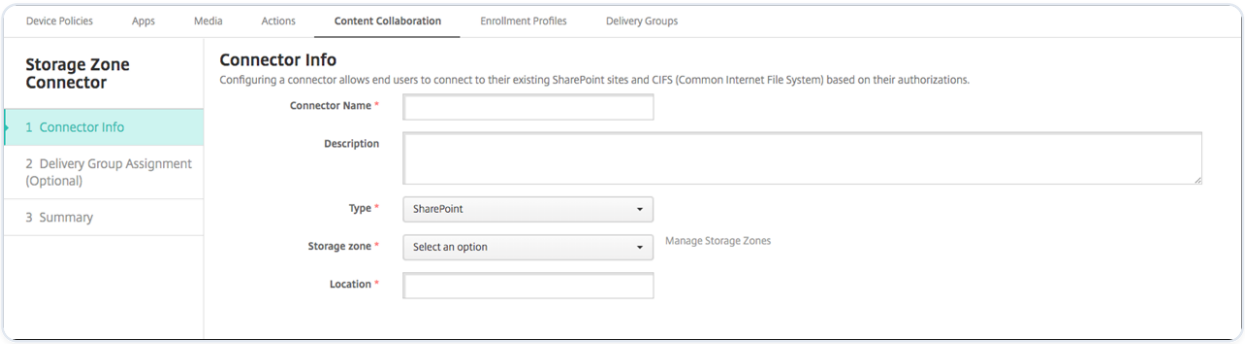
   要编辑或删除存储区域控制器连接的信息，请在**管理存储区域**中选择连接名称。然后，单击**编辑**或**删除**。

在 Citrix Endpoint Management 中添加存储区域连接器

1. 转至**配置 > ShareFile**，然后单击**添加**。

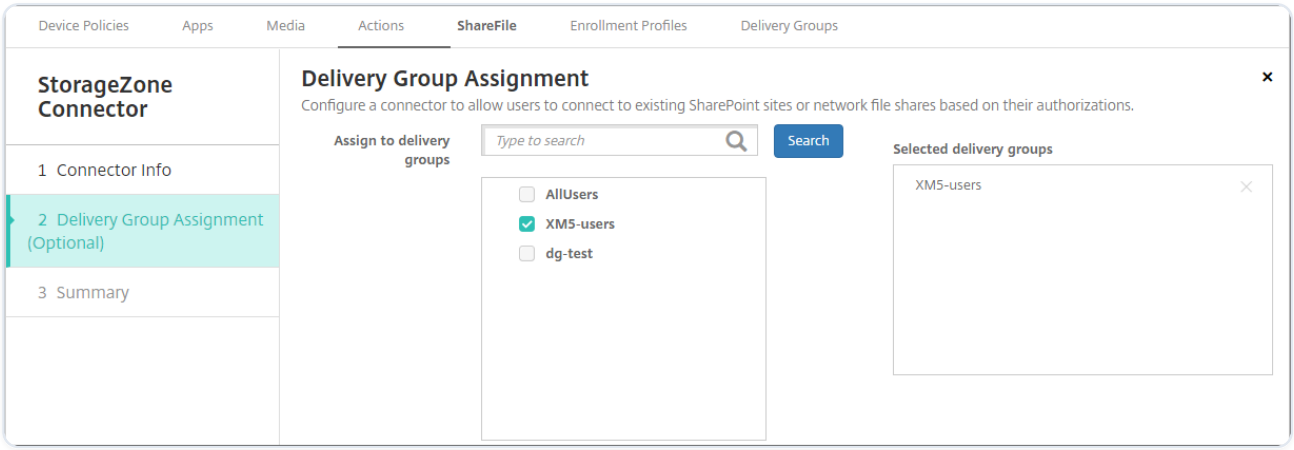


2. 在**连接器信息**页面上，配置以下设置：



   - **连接器名称**：在 Citrix 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。如果未列出存储区域，请单击**管理存储区域**以定义存储区域控制器。
   - **位置**：对于 SharePoint，请指定 SharePoint 根级别站点、站点集或文档库的 URL，格式为 `https://sharepoint.company.com`。对于网络共享，请指定统一命名约定 (UNC) 路径的完全限定域名，格式为 \\\\server\\share。

3. 在**交付组分配**页面上，可以选择将连接器分配给交付组。否则，您可以使用**配置 > 交付组**将连接器与交付组关联。



1. 在**摘要**页面上，您可以查看已配置的选项。要调整配置，请单击**返回**。

2. 单击**保存**以保存连接器。
3. 测试连接器：

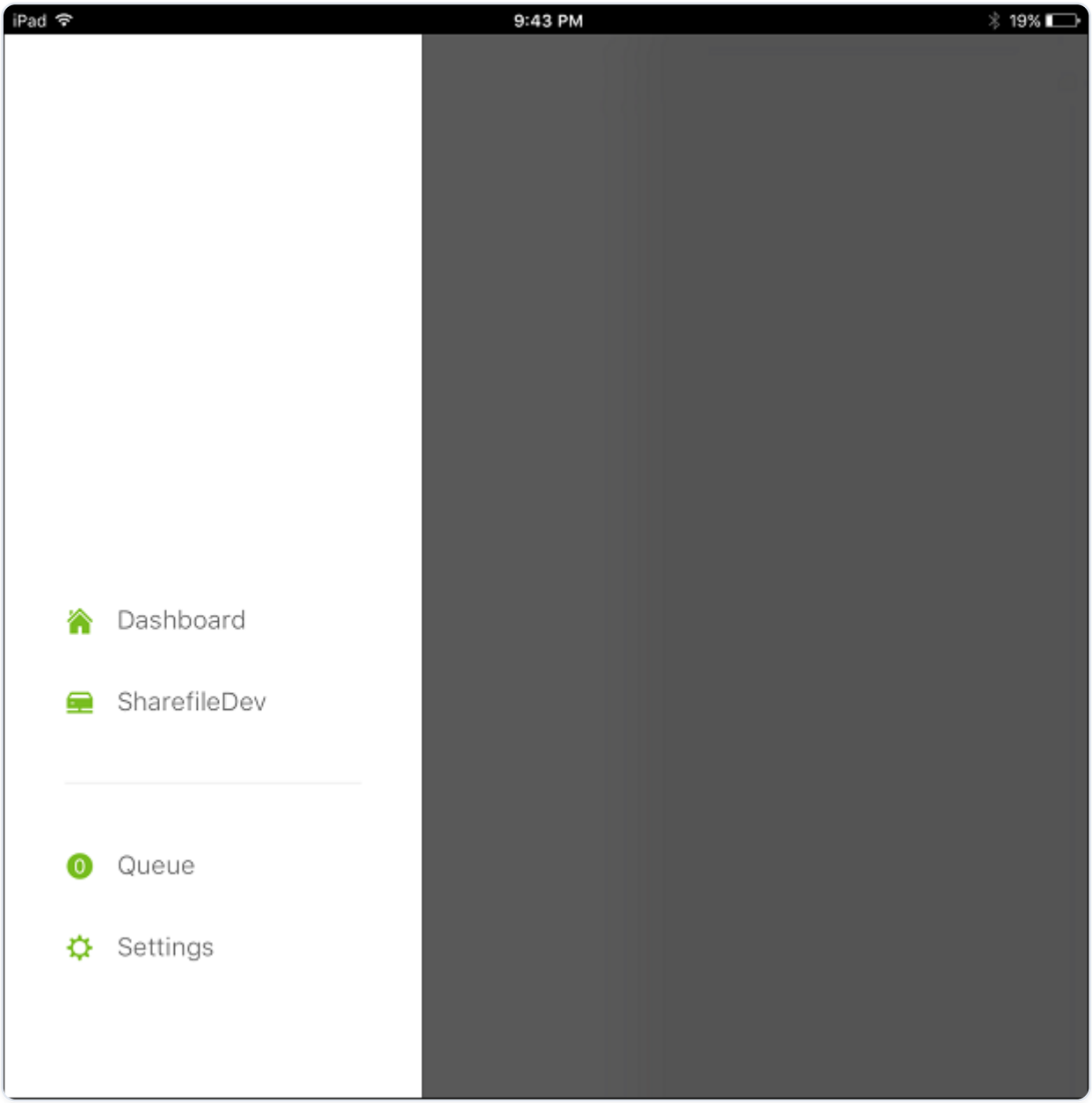
   a. 封装 Citrix Files 客户端时，将网络访问策略设置为**隧道 - Web SSO**。

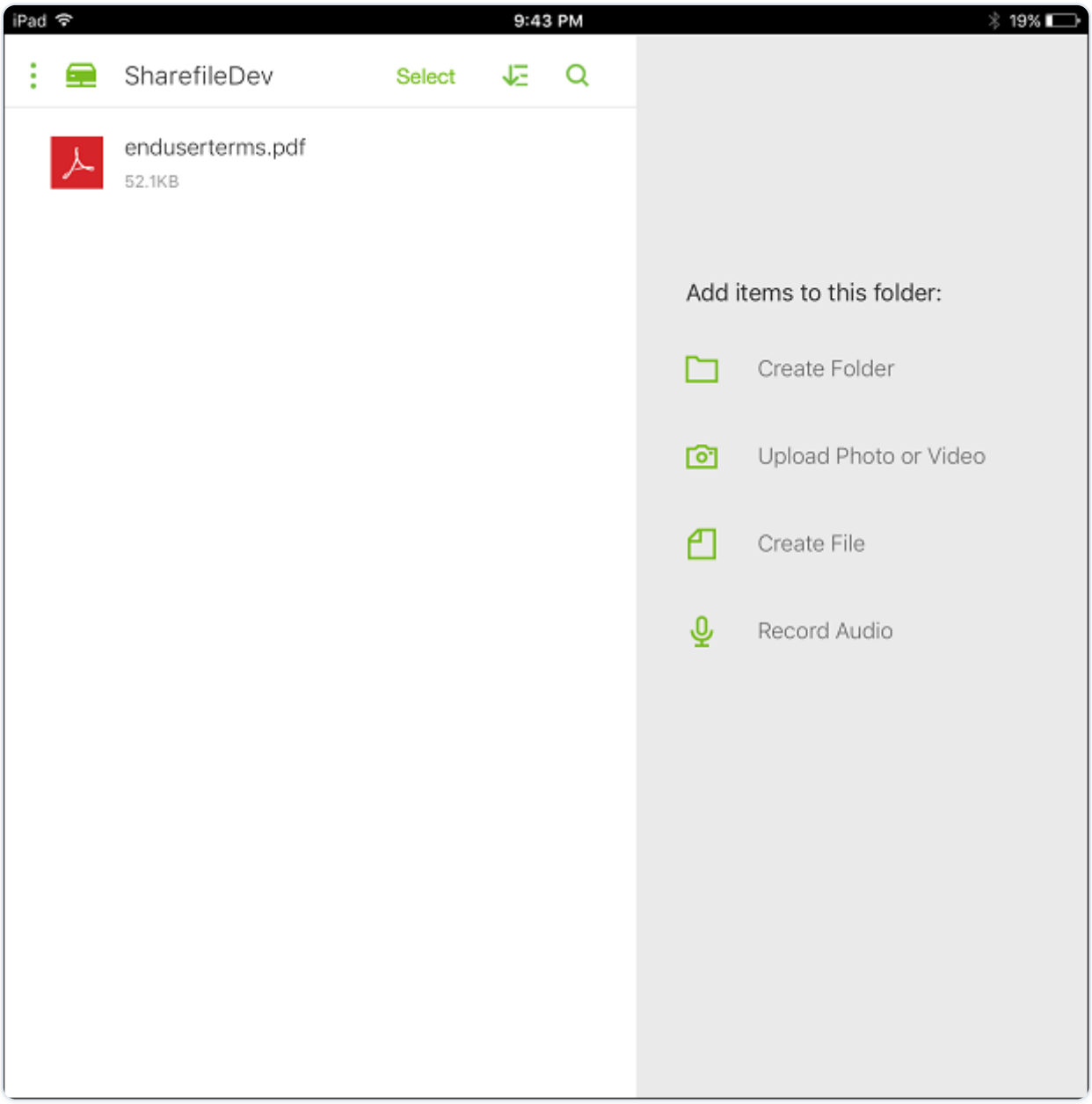
      在此隧道模式下，MDX 框架会终止来自 MDX 应用程序的 SSL/HTTP 流量。然后，MDX 会为用户启动到内部连接的新连接。此策略设置使 MDX 框架能够检测并响应 Web 服务器发出的身份验证质询。

   b. 将 Citrix Files 客户端添加到 Citrix Endpoint Management。有关详细信息，请参阅将 Citrix Files 客户端添加到 Citrix Endpoint Management。

   c. 从受支持的设备，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。

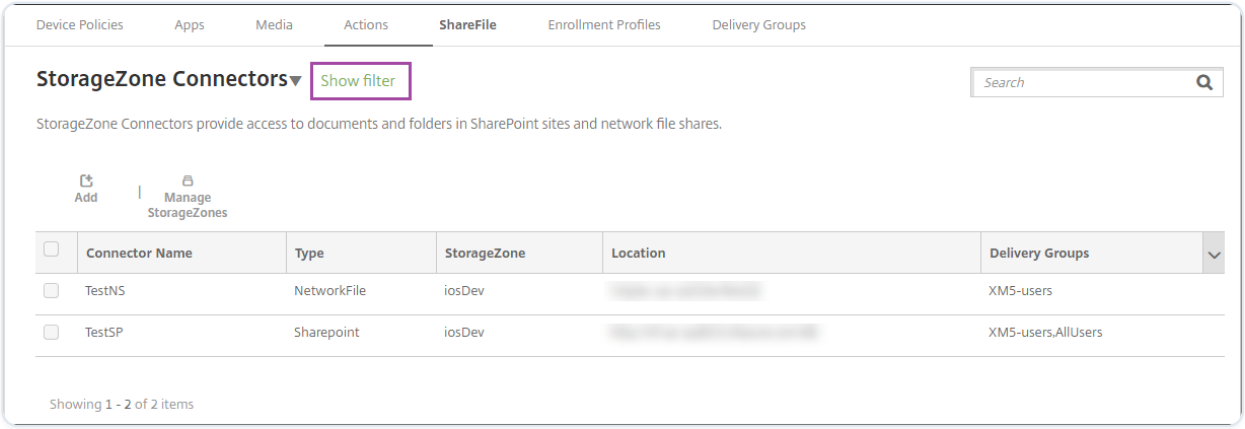




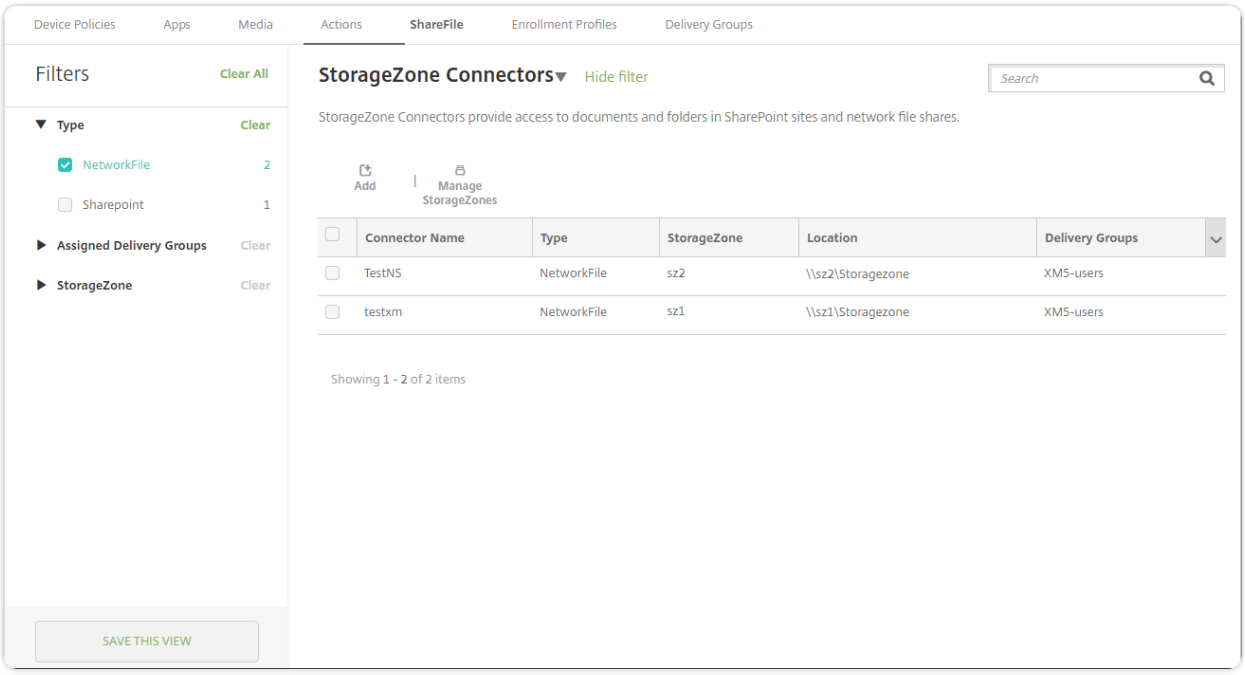
筛选存储区域连接器列表

您可以按连接器类型、分配的交付组和存储区域筛选存储区域连接器列表。

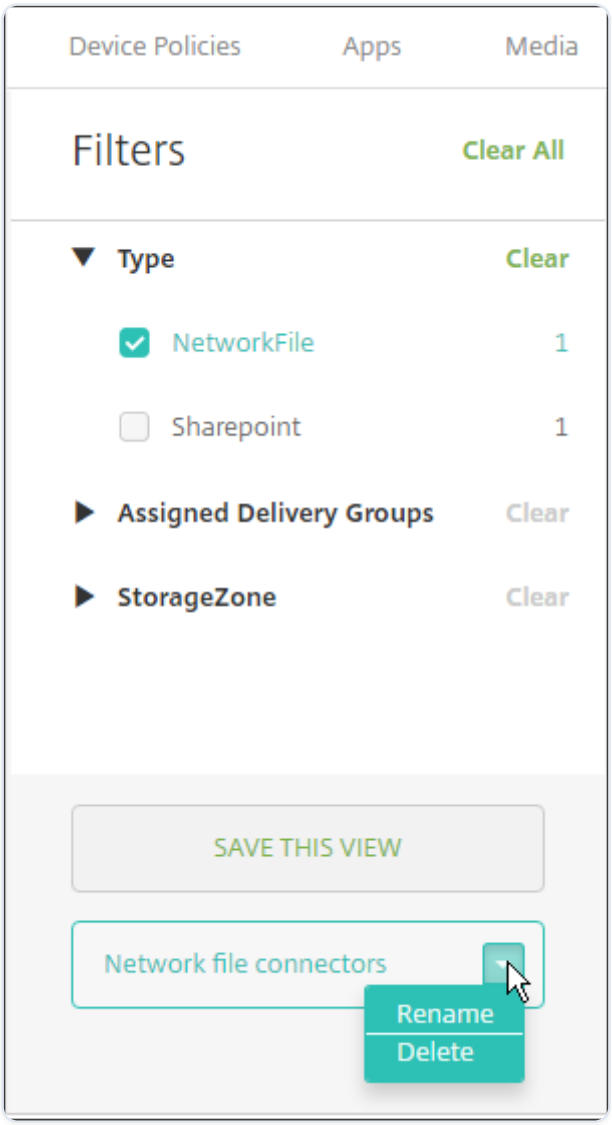
1. 转到**配置 > ShareFile**，然后单击**显示筛选器**。



2. 展开筛选器标题以进行选择。要保存筛选器，请单击“**保存此视图**”，键入筛选器名称，然后单击“**保存**”。



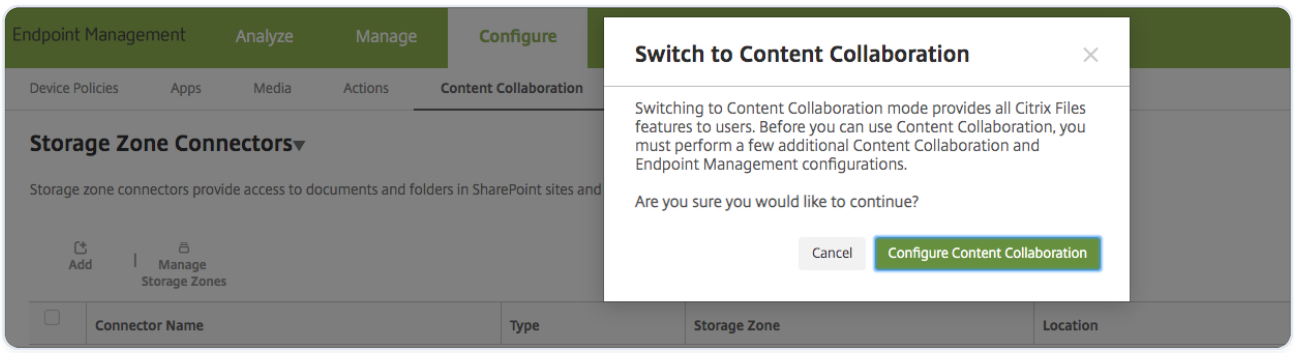
3. 要重命名或删除筛选器，请单击筛选器名称旁边的箭头图标。



切换到企业帐户

将存储区域连接器与 Citrix Endpoint Management 集成后，您可以稍后切换到完整的企业功能集。Citrix Endpoint Management 会保留您现有的存储区域连接器集成设置。

转到“**配置 > ShareFile**”，单击“**存储区域连接器**”下拉菜单，然后单击“**配置 ShareFile**”。



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。

HDX™ 应用程序的 SmartAccess

此功能允许您根据设备属性、设备的用户属性或设备上安装的应用程序来控制对 HDX 应用程序的访问。您可以通过设置自动化操作来使用此功能，将设备标记为不合规以拒绝该设备访问。与此功能一起使用的 HDX 应用程序在 Citrix Virtual Apps and Desktops 中配置，方法是使用 SmartAccess 策略拒绝不合规设备的访问。Citrix Endpoint Management 使用签名加密标签将设备状态传达给 StoreFront。StoreFront 然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，您的部署需要：

- Citrix 虚拟应用和桌面™
- Citrix 端点管理
- 配置了 SAML 证书的 Citrix Endpoint Management，用于签名和加密标签。不带私钥的相同证书将上传到 StoreFront 服务器。

要开始使用此功能：

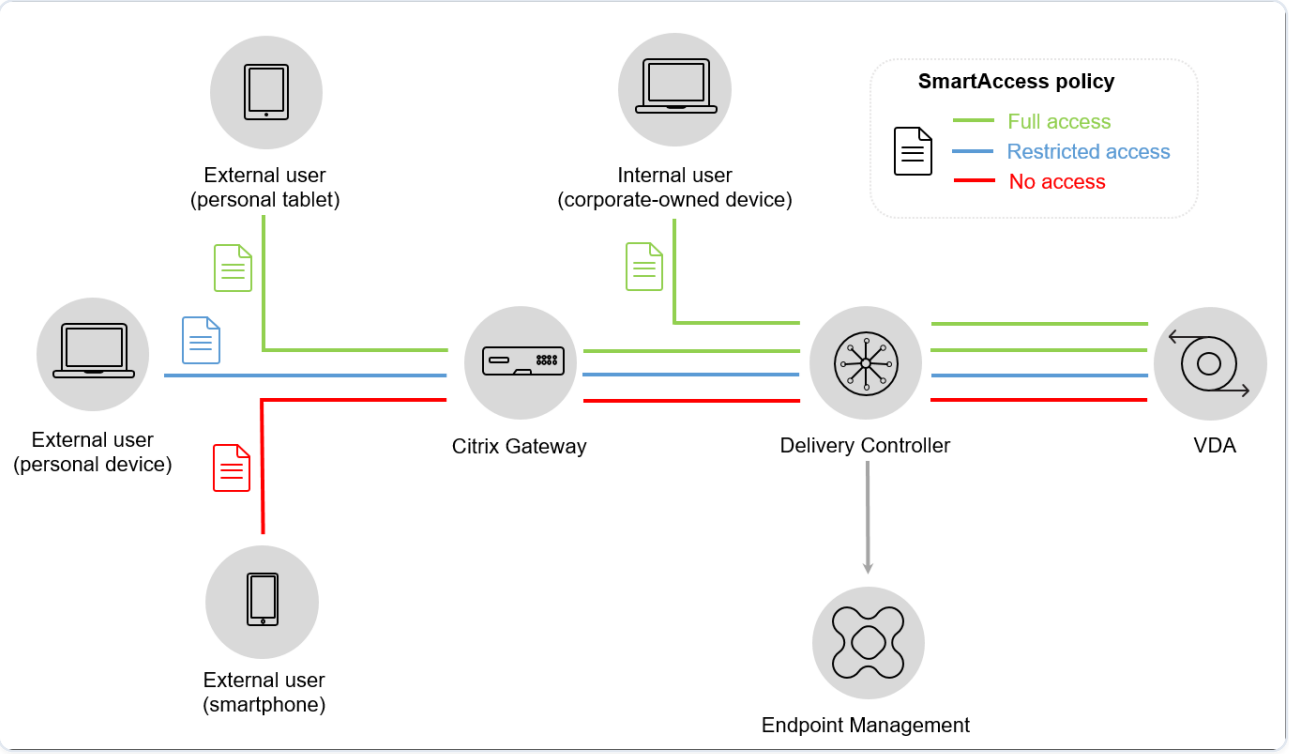
- 将 Citrix Endpoint Management 服务器证书配置到 StoreFront 商店
- 配置至少一个具有所需 SmartAccess 策略的 Citrix Virtual Apps and Desktops 交付组
- 在 Citrix Endpoint Management 中设置自动化操作

适用于端点的 HDX 应用程序的 SmartAccess

借助此功能，您可以应用基于策略的访问控制来限制设备对 HDX 应用程序的访问。您可以将以下访问级别应用于 HDX 应用程序：

- **完全访问**。设备可以访问 Citrix Secure Hub 商店提供的所有 HDX 应用程序。
- **受限访问**。设备可以访问一个或多个（但不是全部）HDX 应用程序。
- **无访问权限**。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。在 Citrix Secure Hub 中尝试启动 HDX 应用程序会触发对 Delivery Controller 的请求。然后，Delivery Controller 将请求转发到 Citrix Endpoint Management 服务器进行验证。验证结果决定了设备拥有的访问级别。例如，如果设备已越狱，则拒绝访问 HDX 应用程序。



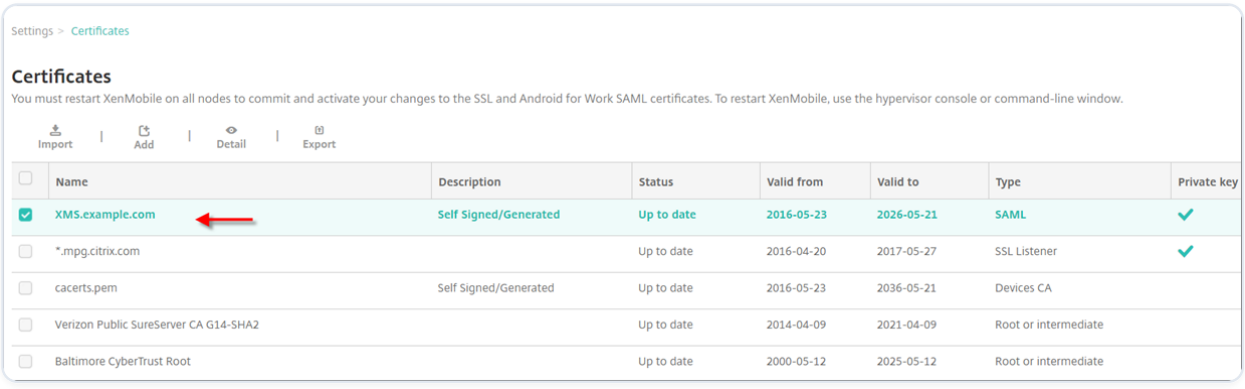
导出并配置 Citrix Endpoint Management 服务器证书，然后将其上传到 StoreFront 商店

SmartAccess 使用签名和加密标签在 Citrix Endpoint Management 和 StoreFront 服务器之间进行通信。要启用该通信，请将 Citrix Endpoint Management 服务器证书添加到 StoreFront 商店。

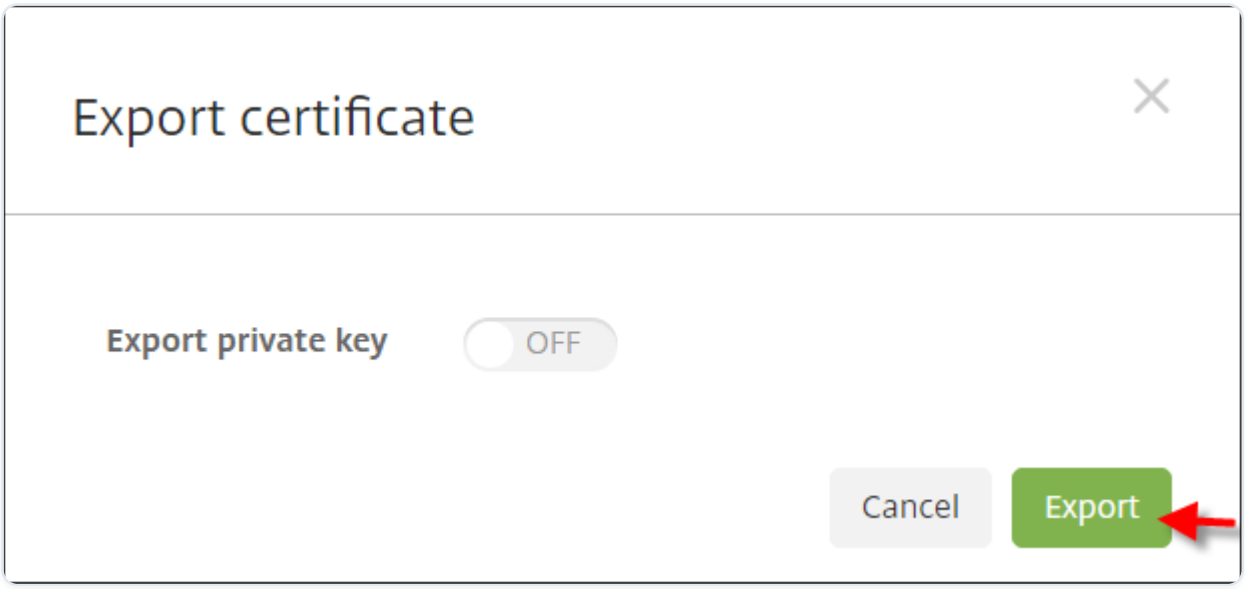
有关在 Citrix Endpoint Management 启用域和基于证书的身份验证时集成 StoreFront 和 Citrix Endpoint Management 的更多信息，请参阅 支持知识中心。

从 Citrix Endpoint Management 导出 SAML 证书

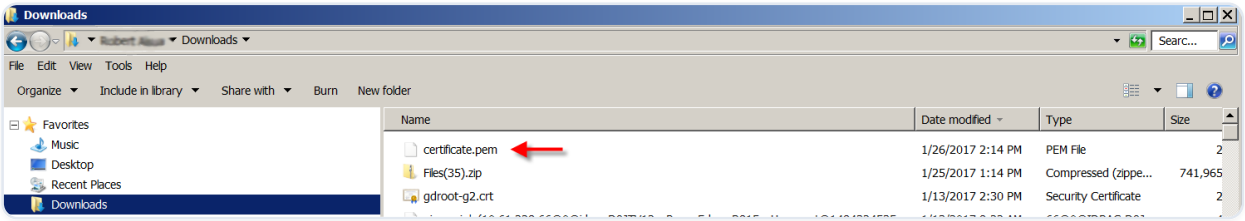
1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示“**设置**”页面。单击“**证书**”。
2. 找到 Citrix Endpoint Management 服务器的 SAML 证书。



3. 确保“**导出私钥**”设置为“**关**”。单击“**导出**”将证书导出到您的下载目录。

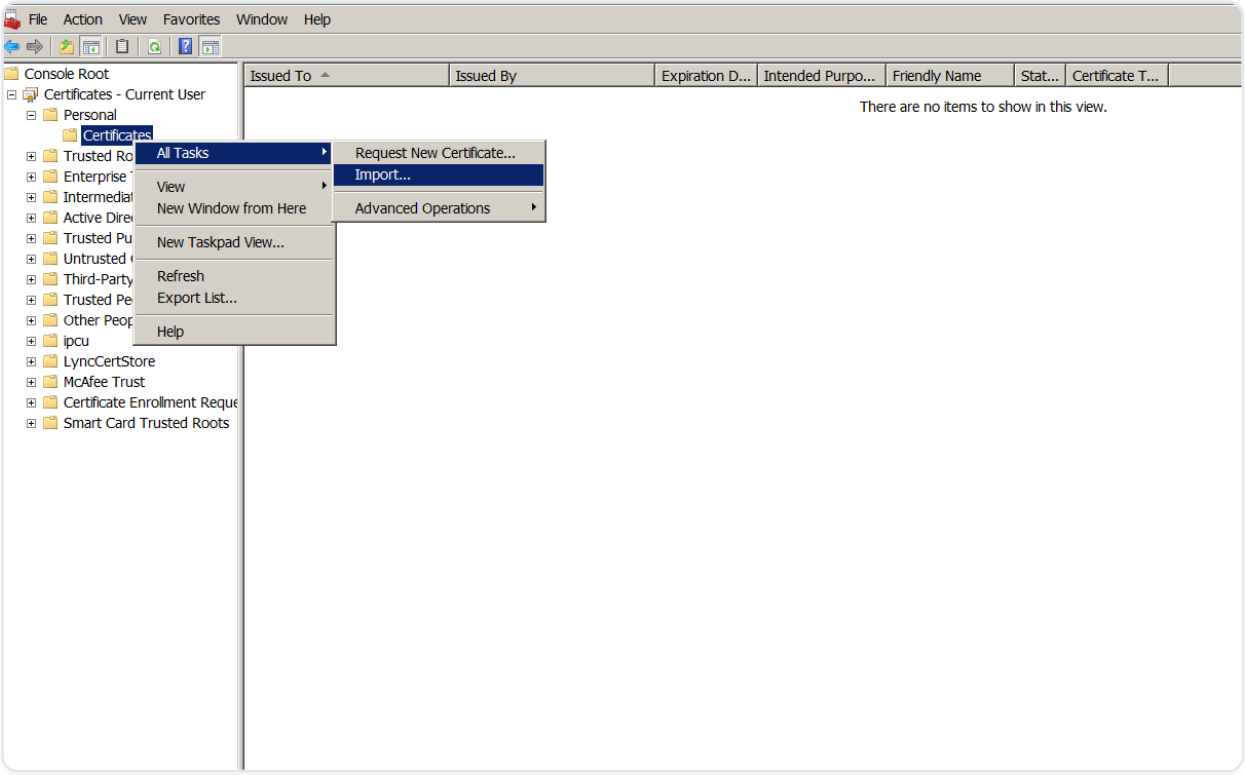


4. 在您的下载目录中找到该证书。该证书采用 PEM 格式。



将证书从 PEM 转换为 CER

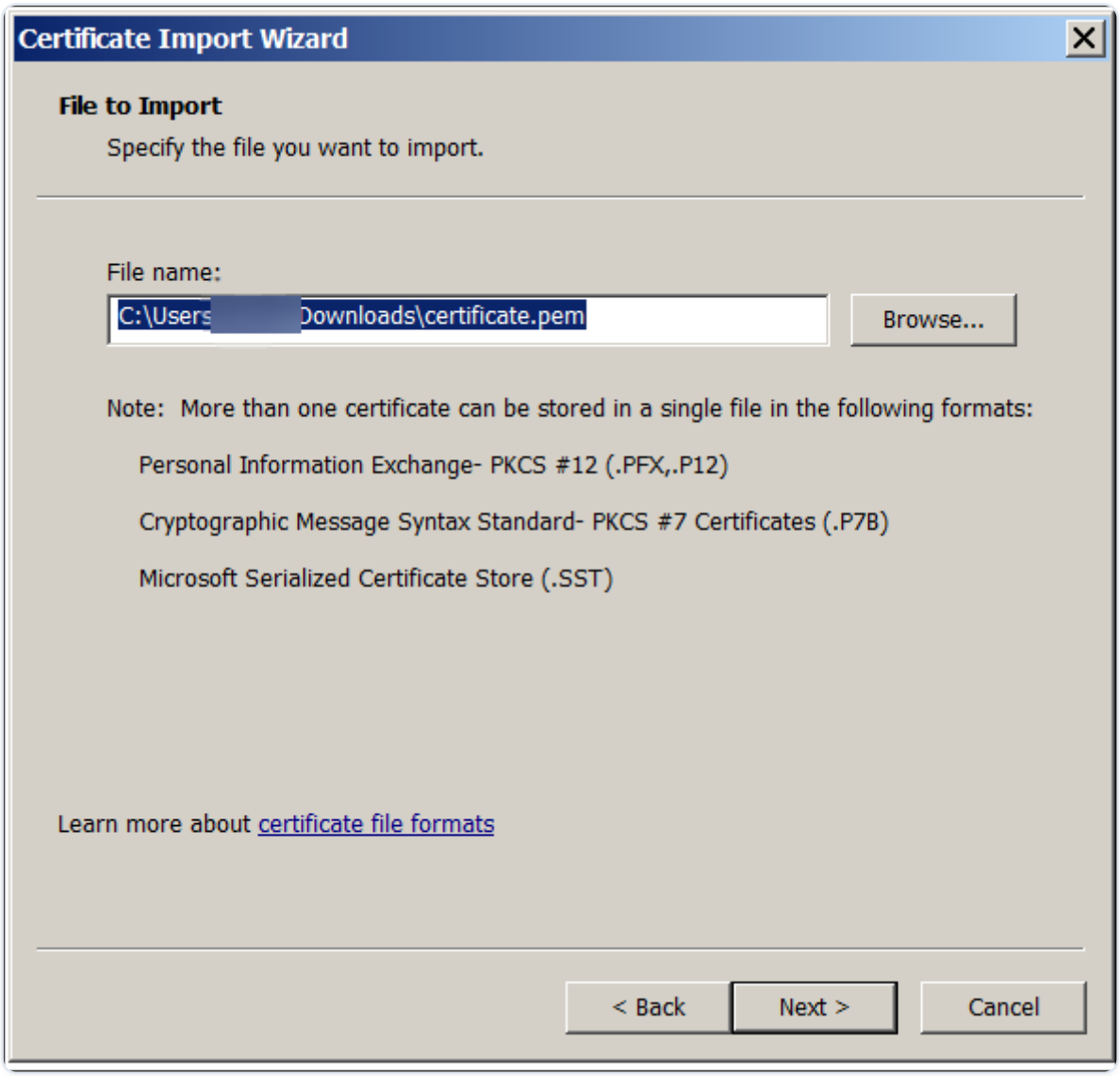
1. 打开 Microsoft 管理控制台 (MMC)，然后右键单击“**证书 > 所有任务 > 导入**”。



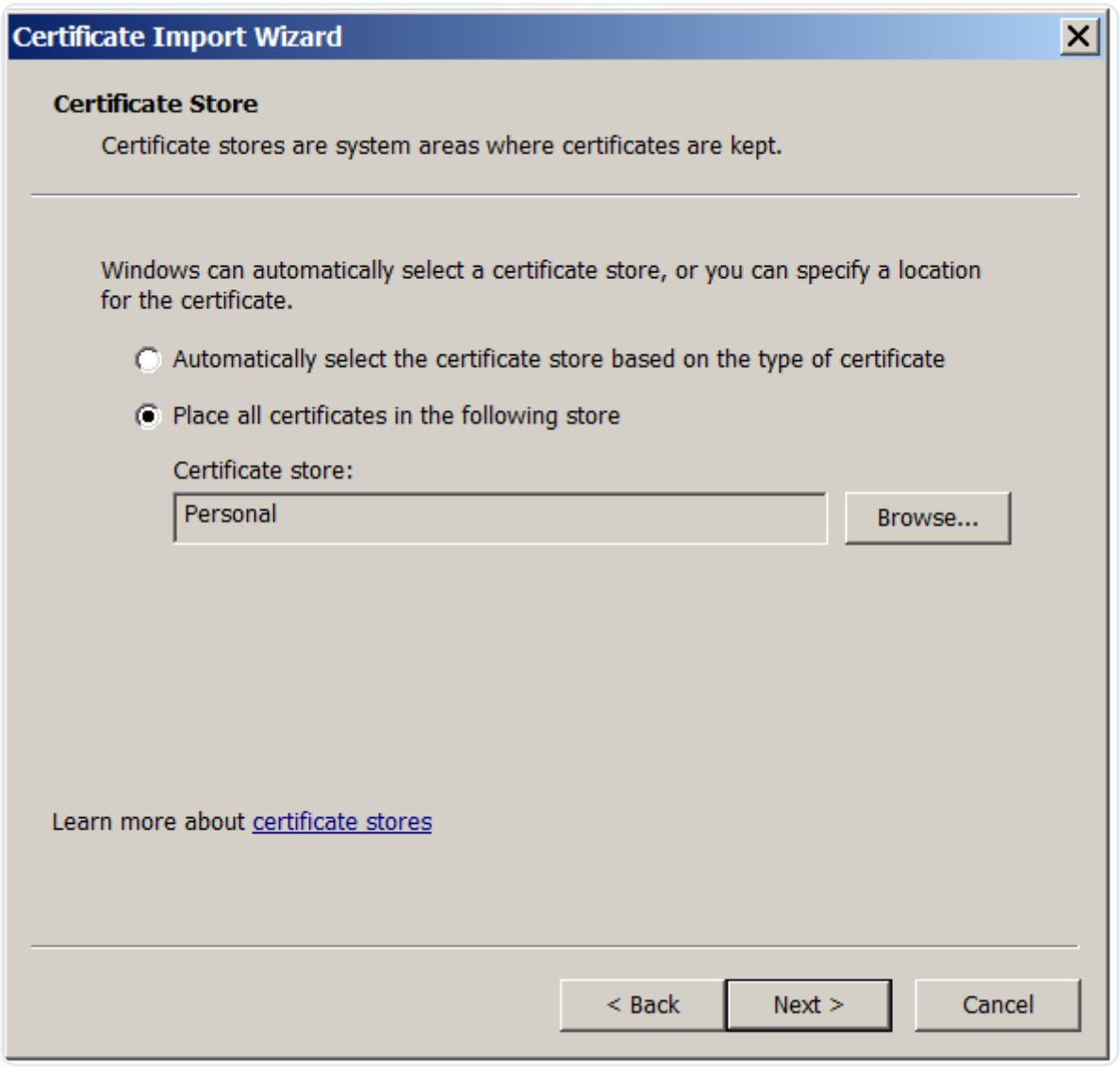
2. 当证书导入向导出现时，单击**下一步**。



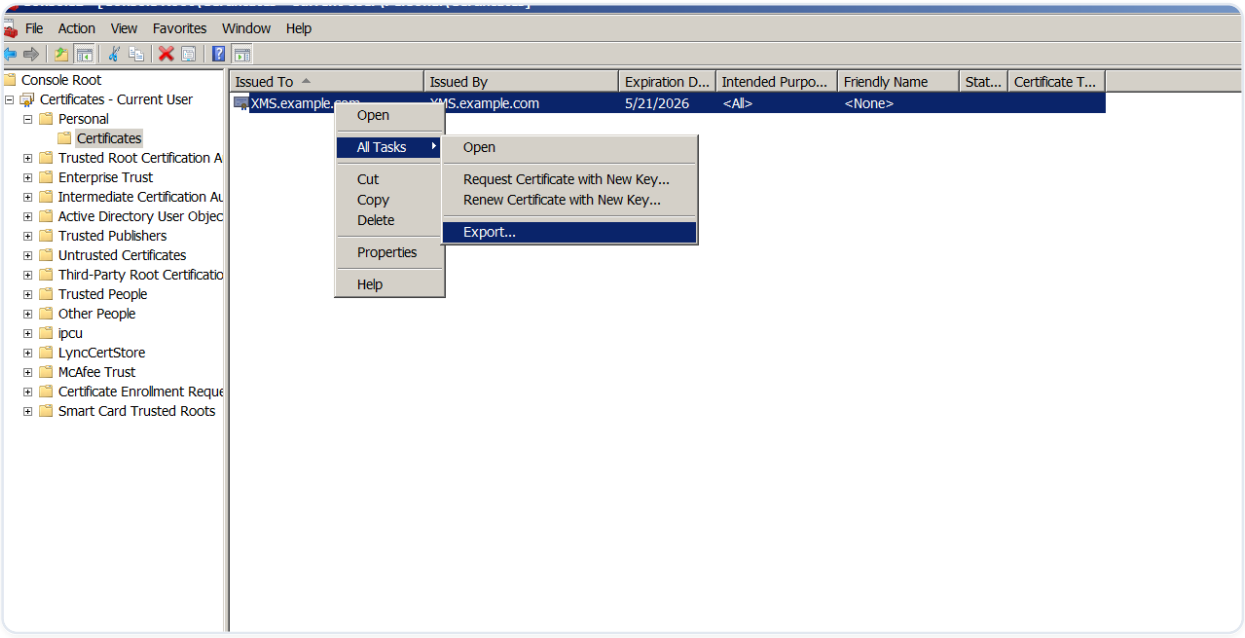
3. 浏览到下载目录中的证书。



4. 选择**将所有证书放入以下存储**，然后选择**个人**作为证书存储。单击**下一步**。



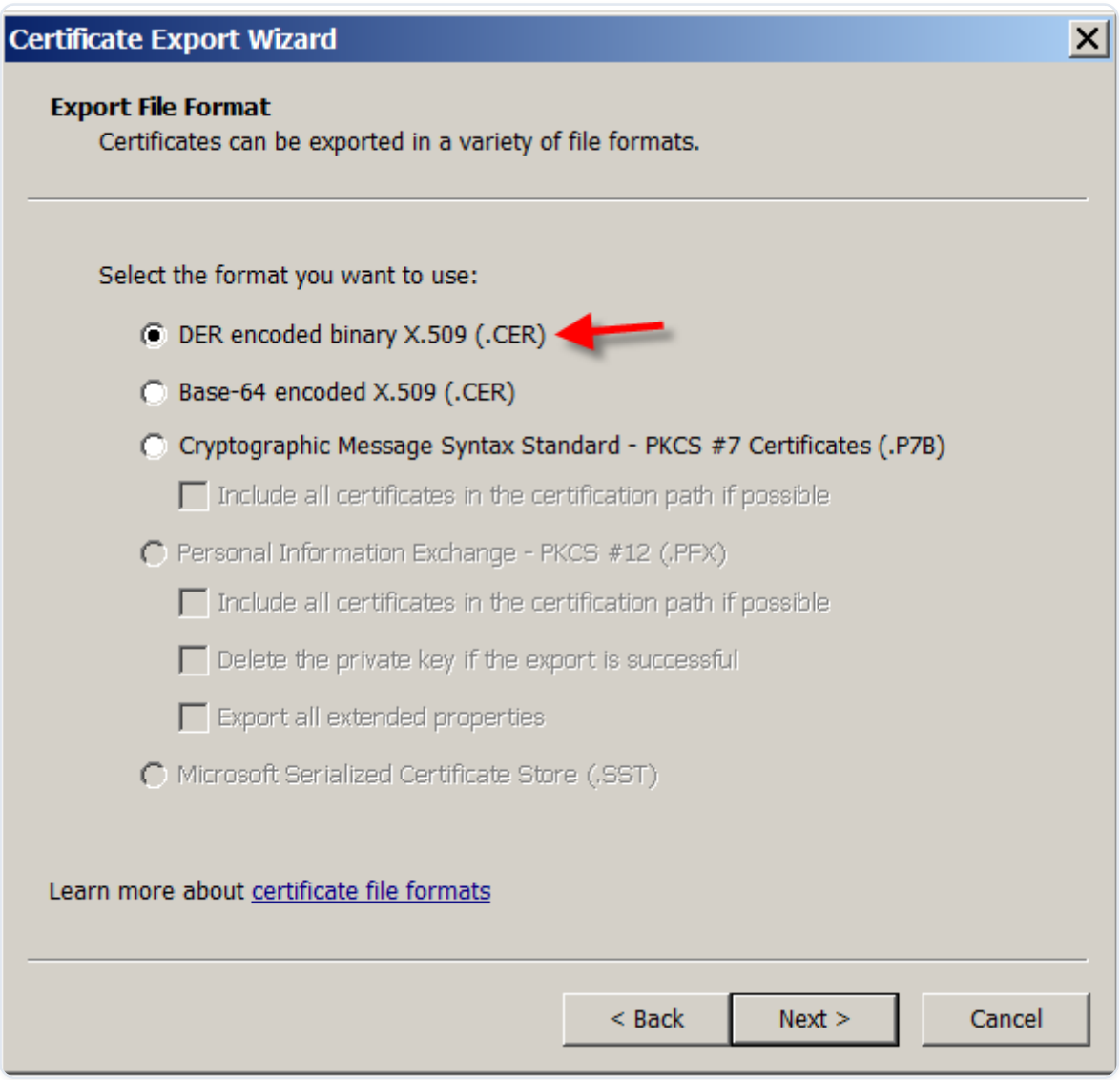
5. 查看您的选择，然后单击**完成**。单击**确定**关闭确认窗口。
6. 在 MMC 中，右键单击证书，然后选择**所有任务 > 导出**。



7. 当证书导出向导出现时，单击**下一步**。



8. 选择格式**DER 编码的二进制 X.509 (.CER)**。单击**下一步**。



9. 浏览到证书。键入证书名称，然后单击**下一步**。

   SmartAccess 配置(/en-us/citrix-endpoint-management/media/mmc-export-certificate-browse.png)

10. 保存证书。

    SmartAccess 配置(/en-us/citrix-endpoint-management/media/mmc-export-certificate-save.png)

11. 浏览到证书，然后单击**下一步**。

    SmartAccess 配置(/en-us/citrix-endpoint-management/media/mmc-export-certificate-browse.png)

12. 查看您的选择，然后单击**完成**。单击**确定**关闭确认窗口。

    SmartAccess 配置(/en-us/citrix-endpoint-management/media/mmc-export-certificate-summary.png)

13. 在下载目录中找到证书。该证书采用 CER 格式。

SmartAccess 配置(/en-us/citrix-endpoint-management/media/certificate-in-download-folder.png)

将证书复制到 StoreFront 服务器

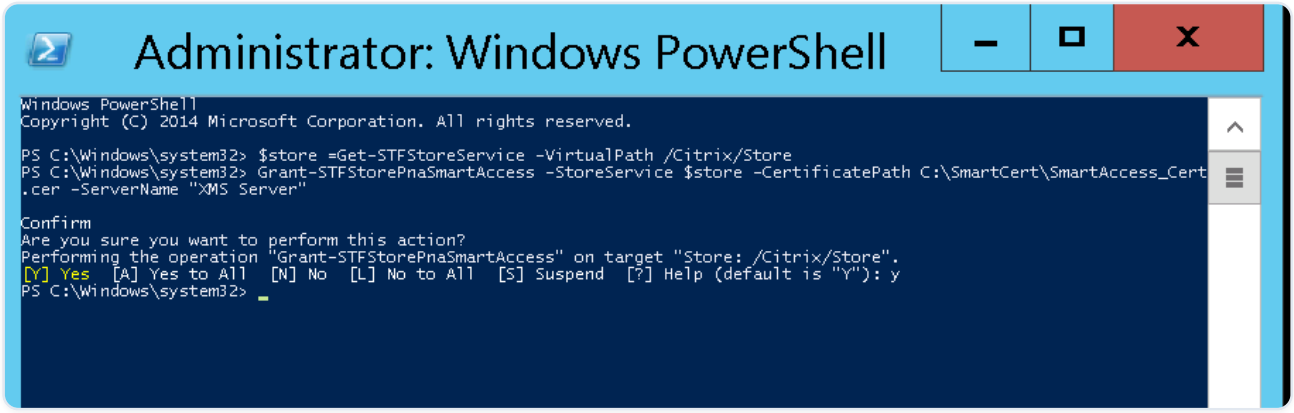
1. 在 StoreFront 服务器上，创建一个名为 **SmartCert** 的文件夹。
2. 将证书复制到 **SmartCert** 文件夹。

SmartAccess 配置(/en-us/citrix-endpoint-management/media/certificate-in-smartcert-folder.png)

在 StoreFront 存储上配置证书

在 StoreFront 服务器上，运行此 PowerShell 命令以在存储上配置转换后的 Citrix Endpoint Management 服务器证书：

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath  “C:\xms\xms.cer” –ServerName “XMS server”
```



如果 StoreFront 存储中有任何现有证书，请运行此 PowerShell 命令以吊销它们：

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```



否则，您可以在 StoreFront 服务器上运行以下任一 PowerShell 命令，以吊销 StoreFront 存储中的现有证书：

- 按名称吊销：

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM
Server"
```

- 按指纹吊销：

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –
CertificateThumbprint "[Thumbprint]
```

- 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]
```

配置 Citrix Virtual Apps and Desktops 的 SmartAccess 策略

要将所需的 SmartAccess 策略添加到交付 HDX 应用程序的交付组：

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. 选择一个交付您要控制访问的应用程序的组。然后在“**操作**”窗格中选择“**编辑交付组**”。
4. 在“**访问策略**”页面上，选择“**通过 NetScaler Gateway 的连接**”和“**满足以下任一条件的连接**”。
5. 单击“**添加**”。
6. 添加访问策略，其中 **场** 为 **XM**，**筛选器** 为 **XMCompliantDevice**。

SmartAccess 配置(/en-us/citrix-endpoint-management/media/delivery-group-app-desktop-access-policy.png)

7. 点击“**应用**”以应用您所做的任何更改并保持窗口打开，或点击“**确定**”以应用更改并关闭窗口。

在 Citrix Endpoint Management 中设置自动化操作

您为 HDX 应用程序在交付组中设置的 SmartAccess 策略会在设备不合规时拒绝设备访问。使用自动化操作将设备标记为不合规。

SmartAccess 配置(/en-us/citrix-endpoint-management/media/actions-out-of-compliance.png)

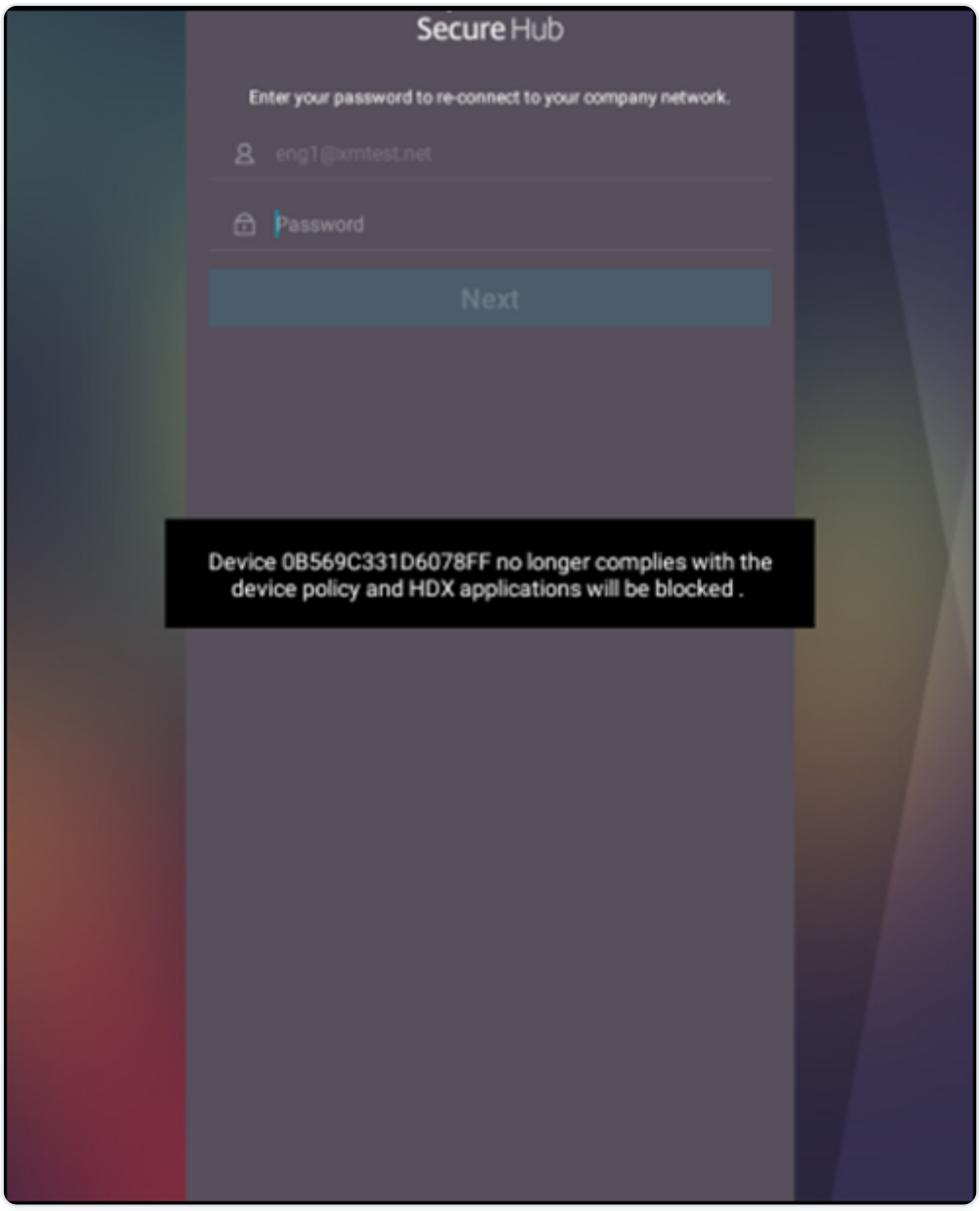
1. 在 Citrix Endpoint Management 控制台中，点击“**配置 > 操作**”。“**操作**”页面随即显示。
2. 点击“**添加**”以添加操作。“**操作信息**”页面随即显示。
3. 在“**操作信息**”页面上，键入操作的名称和描述。
4. 点击“**下一步**”。“**操作详细信息**”页面随即显示。在以下示例中，如果设备具有用户属性名称 **eng5** 或 **eng6**，则会创建一个立即将设备标记为不合规的触发器。

   SmartAccess 配置(/en-us/citrix-endpoint-management/media/configure-actions-trigger-example.png)
5. 在“**触发器**”列表中，选择“**设备属性**”、“**用户属性**”或“**已安装的应用程序名称**”。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“**真**”。
   - 要将操作设置为在触发条件满足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 Citrix Endpoint Management 交付组或多个组。
8. 查看操作摘要。
9. 单击“**下一步**”，然后单击“**保存**”。

当设备被标记为不合规时，HDX 应用程序将不再显示在 Citrix Secure Hub 商店中。用户将不再订阅该应用程序。设备不会收到通知，并且 Citrix Secure Hub 商店中没有任何内容表明 HDX 应用程序以前可用。

如果您希望在设备被标记为不合规时通知用户，请创建通知，然后创建自动化操作以发送该通知。

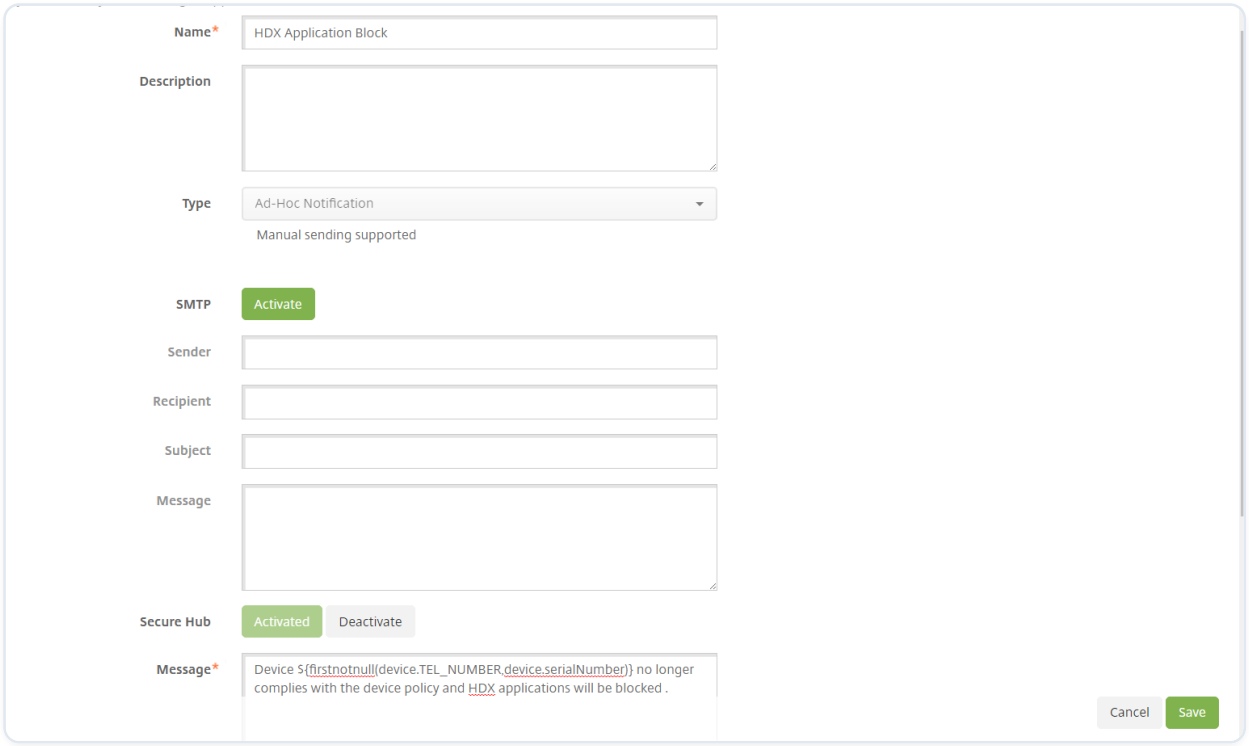
此示例在设备被标记为不合规时创建并发送此通知：“设备序列号或电话号码不再遵循设备策略，并且 HDX 应用程序已被阻止。”



创建设备被标记为不合规时用户看到的通知

1. 在 Citrix Endpoint Management 控制台中，单击控制台右上角的齿轮图标。“**设置**”页面随即显示。
2. 单击“**通知模板**”。“**通知模板**”页面随即显示。
3. 在“**通知模板**”页面上单击“**添加**”以添加。
4. 配置以下设置：
    - **名称：** HDX 应用程序阻止
    - **描述：** 设备不合规时的代理通知

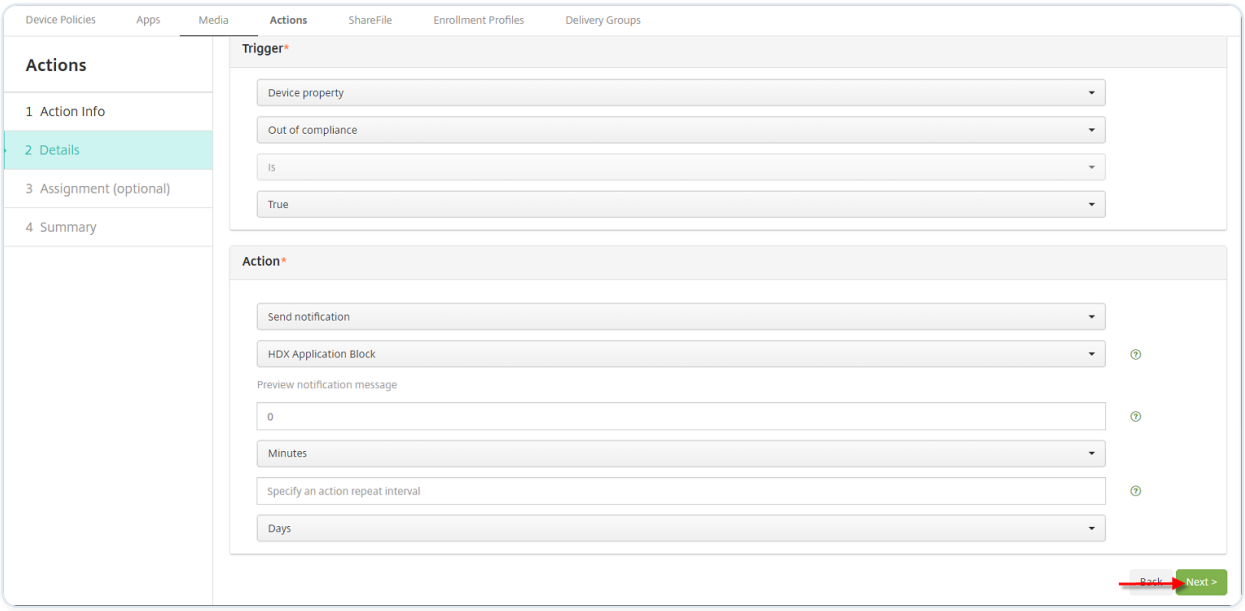
- **类型：** 即时通知
- **Citrix Secure Hub：** 已激活
- **消息：** 设备 `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 不再遵循设备策略，并且 HDX 应用程序已被阻止。



5. 单击**保存**。

创建在设备被标记为不合规时发送通知的操作

1. 在 Citrix Endpoint Management 控制台中，单击**配置 > 操作**。将显示**操作**页面。
2. 单击**添加**以添加操作。将显示**操作信息**页面。
3. 在**操作信息**页面上，输入操作的名称和描述：
   - 名称：HDX 阻止通知
   - **描述：** HDX 阻止通知，因为设备不合规
4. 单击**下一步**。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**。



6. 在 **操作** 列表中，指定满足触发器时执行的操作：
   - 选择 **发送通知**
   - 选择 **HDX 应用程序阻止，您创建的通知**。
   - 选择 **0**。将此值设置为 0 会在满足触发条件时发送通知。
7. 选择要应用此操作的 Citrix Endpoint Management 交付组。在此示例中，选择 **AllUsers**。
8. 查看操作摘要。
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。

用户如何重新获得 HDX 应用程序的访问权限

设备恢复合规性后，用户可以再次访问 HDX 应用程序：

1. 在设备上，转到 Citrix Secure Hub 商店以刷新商店中的应用程序。
2. 转到应用程序并点击 **添加** 到应用程序。

应用添加后，它会出现在“我的应用”中，旁边带有一个蓝点，因为它是一个新安装的应用。

SmartAccess 配置(/en-us/citrix-endpoint-management/media/secure-hub-app-added.png)

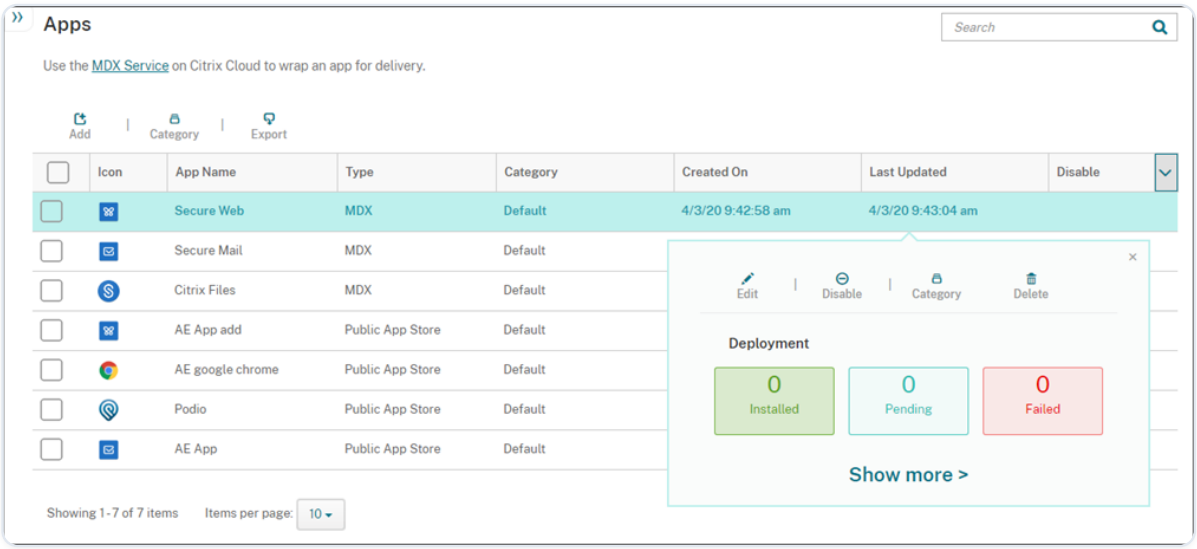
升级 MDX 或企业应用

要在 Citrix Endpoint Management 中升级 MDX 或企业应用，请在 Citrix Endpoint Management 控制台中禁用该应用，然后上传新版本的应用。

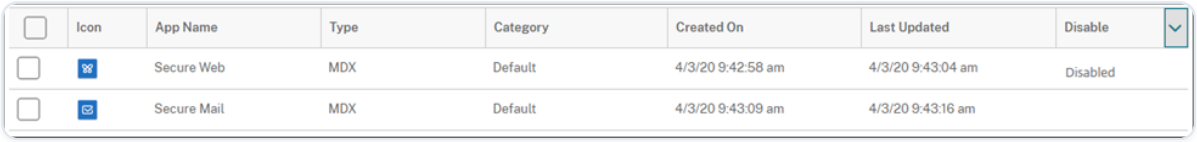
1. 在 Citrix Endpoint Management 控制台中，单击“**配置 > 应用**”。“**应用**”页面随即显示。
2. 对于托管设备（已注册到 Citrix Endpoint Management 以进行移动设备管理的设备），请跳至步骤 3。对于非托管设备（仅为企业应用管理目的而注册到 Citrix Endpoint Management 的设备），请执行以下操作：

   a. 在“**应用**”表中，选中应用旁边的复选框，或单击包含要更新的应用的行。

   b. 在出现的菜单中单击“**禁用**”。



   c. 在确认对话框中单击“**禁用**”。应用的“**禁用**”列中显示“*已禁用*”。



> **注意：**
>
> 应用禁用后，用户注销后无法重新连接到该应用。禁用应用是可选的，但我们建议禁用应用以避免应用功能问题。例如，用户在您上传新版本的同时请求下载应用可能会导致问题。

3. 在“**应用**”表中，单击应用旁边的复选框，或单击包含要更新的应用的行。
4. 在出现的菜单中单击“**编辑**”。“**应用信息**”页面随即显示，其中已选择您最初为该应用选择的平台。
5. 配置以下设置：

   - **名称：** （可选）更改应用名称。

- **说明：**（可选）更改应用说明。
- **应用程序类别：**（可选）更改应用程序类别。

6. 单击**下一步**。将显示第一个选定平台页面。对每个选定平台执行以下操作：

   a. 通过单击**上载**并导航到文件位置来选择要上载的替换文件。应用程序将上载到 Citrix Endpoint Management。

      如果您要上载适用于 Android Enterprise 的应用程序，将显示托管的 Google Play 窗口。在此处上载应用程序的新版本。有关详细信息，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程序商店。有关信息，请参阅添加 MDX 应用程序。

7. 单击**保存**。将显示**应用程序**页面。
8. 如果您在步骤 2 中禁用了应用程序，请执行以下操作：

   a. 在**应用程序**表中，单击以选择您更新的应用程序，然后在显示的菜单中单击**启用**。

   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收到提示他们升级应用程序的通知。

添加媒体

您将媒体添加到 Citrix Endpoint Management，以便可以将媒体部署到用户设备。您可以使用 Citrix Endpoint Management 部署通过 Apple Volume Purchase 获取的 Apple Books。

在 Citrix Endpoint Management 中配置 Volume Purchase 帐户后，您购买的和免费的图书将显示在 **Configure** > **Media** 中。在 **Media** 页面中，通过选择交付组并指定部署规则来配置要部署到 iOS 设备的图书。

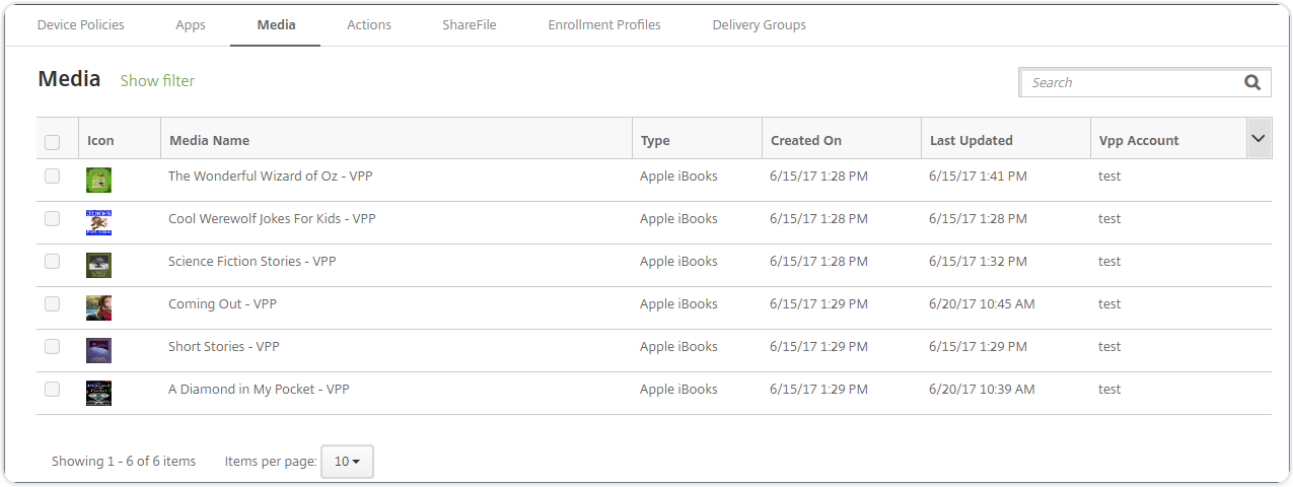
用户首次收到图书并接受 Volume Purchase 许可证后，部署的图书将安装到设备上。这些图书会显示在 Apple Book 应用程序中。您无法将图书许可证与用户解除关联，也无法从设备中删除图书。Citrix Endpoint Management 将图书安装为必需媒体。如果用户从其设备中删除已安装的图书，该图书仍会保留在 Apple Book 应用程序中，可供下载。

先决条件

- iOS 设备
- 在 Citrix Endpoint Management 中配置 Apple Volume Purchase。有关详细信息，请参阅 (/zh-cn/citrix-endpoint-management/apps/apple-volume-purchase.html) 。

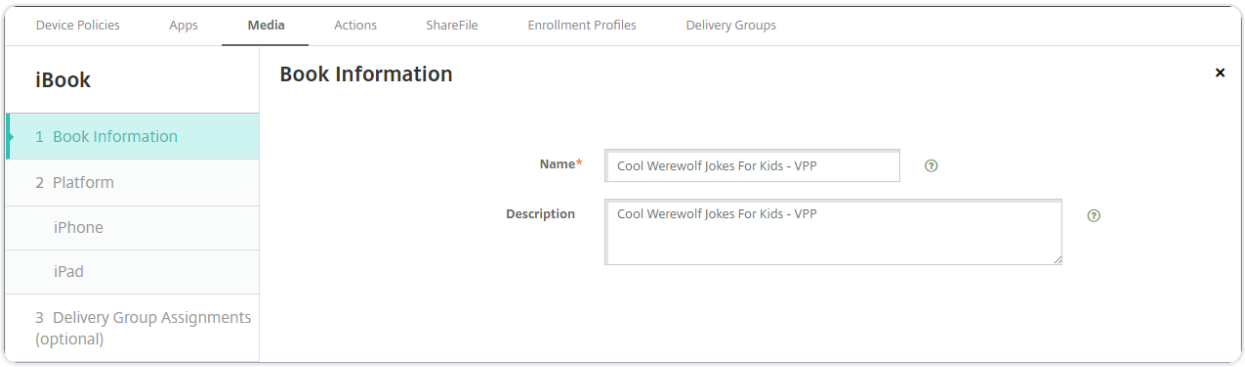
配置图书

通过 Volume Purchase 获取的 Apple Books 将显示在 **Configure** > **Media** 页面上。



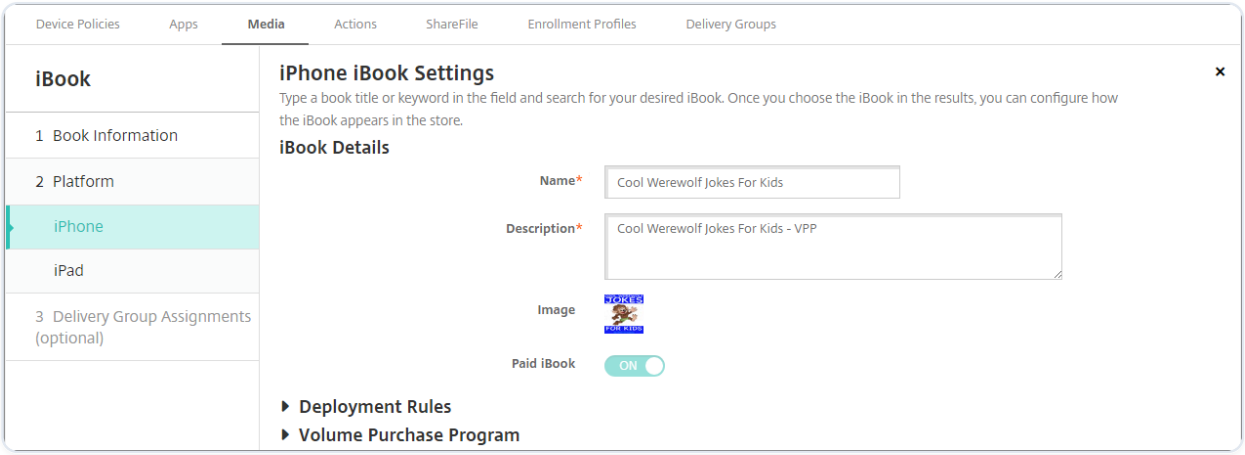
配置要部署的 Apple Book

1. 在 **Configure > Media** 中，选择一本图书，然后单击 **Edit**。此时将显示 **Book Information** 页面。

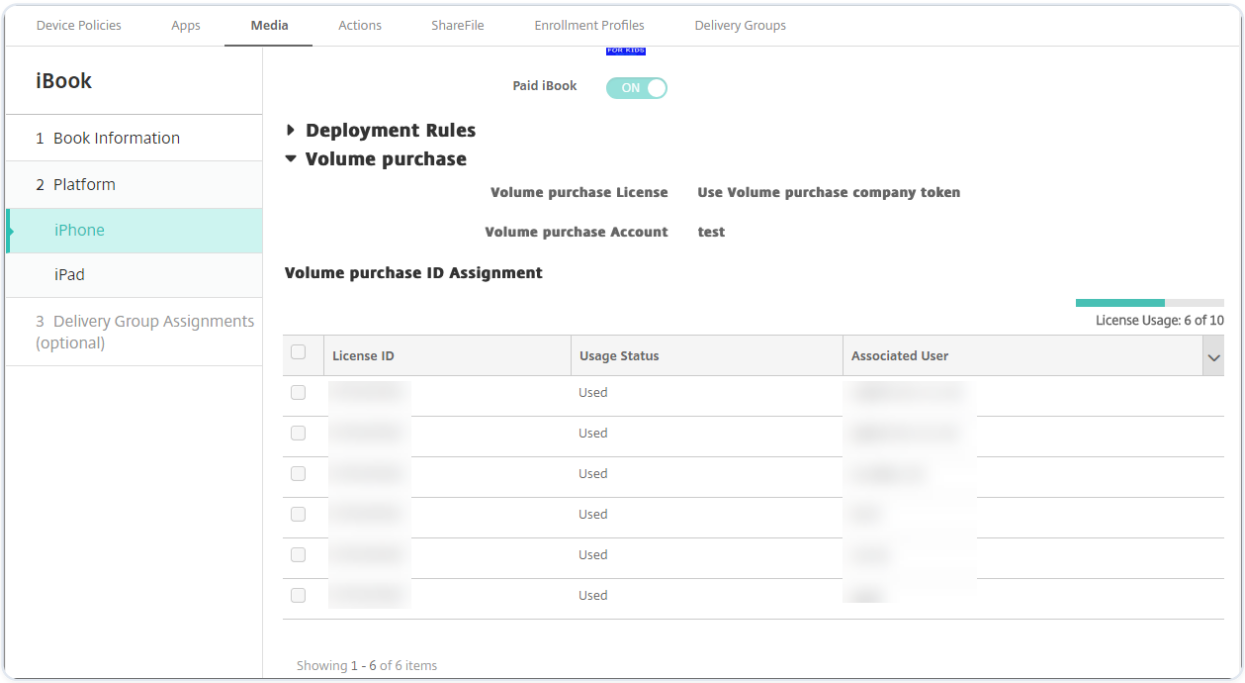


Name 和 **Description** 仅显示在 Citrix Endpoint Management 控制台和日志中。

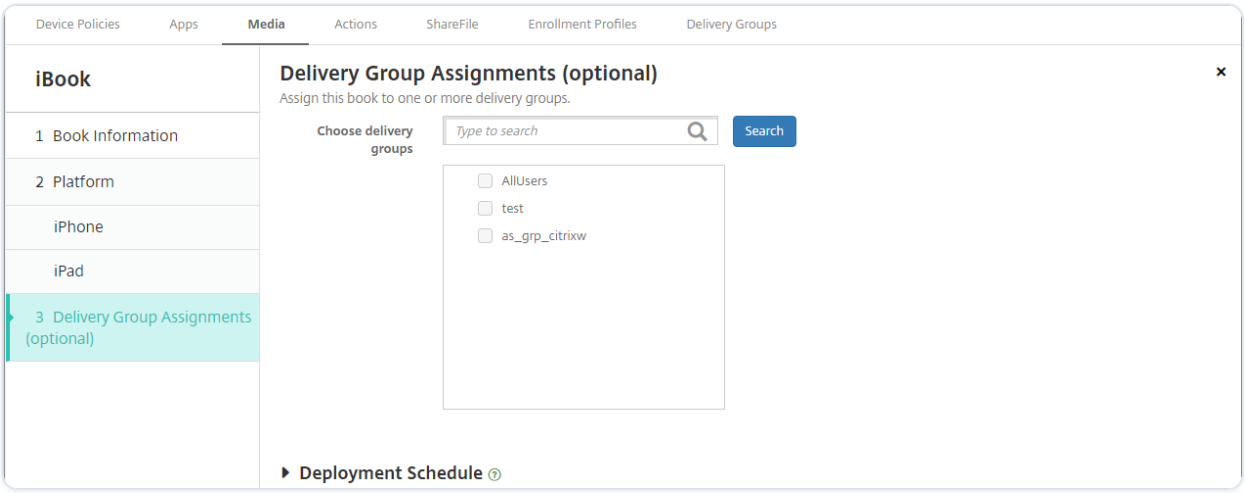
2. 在 **iPhone iBook Settings** 和 **iPad iBook Settings** 页面中：虽然您可以选择更改图书名称和说明，但 Citrix® 建议您不要更改这些设置。该图像仅供参考，不可编辑。**Paid iBook** 表示图书是通过 Apple Volume Purchase 购买的。



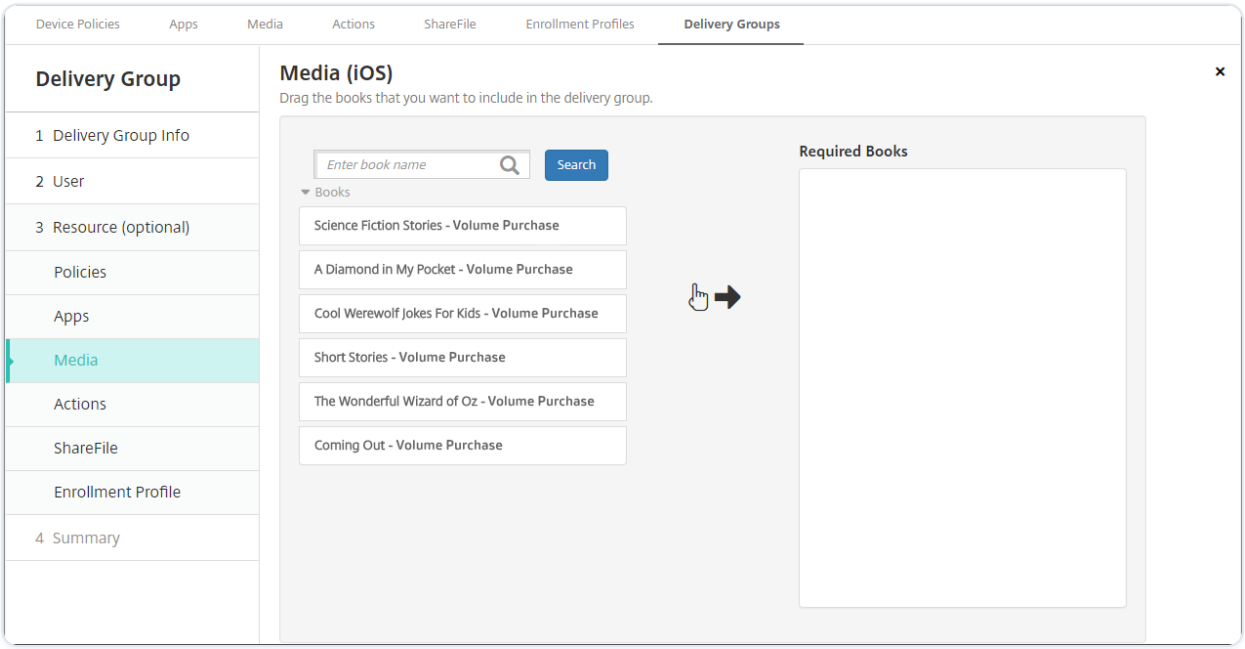
您还可以指定部署规则或查看批量采购信息。



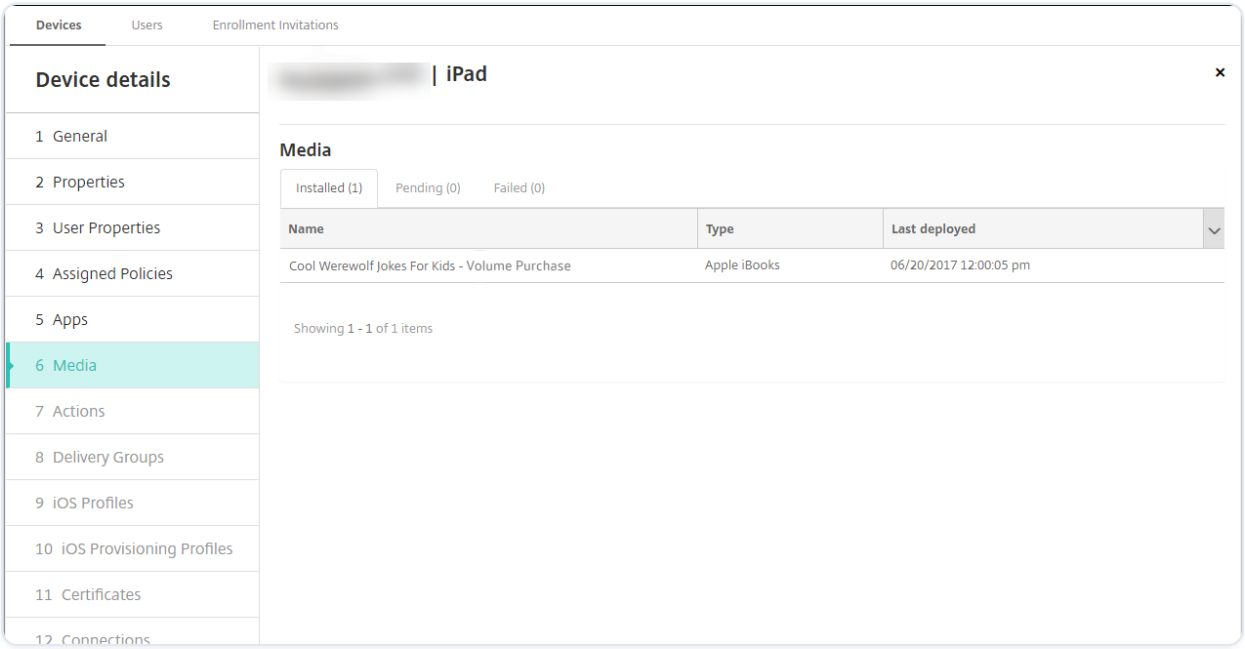
3. （可选）将图书分配给交付组并设置部署计划。



您还可以从**配置 > 交付组**的**媒体**选项卡将图书分配给交付组。Citrix Endpoint Management 仅支持强制图书部署。



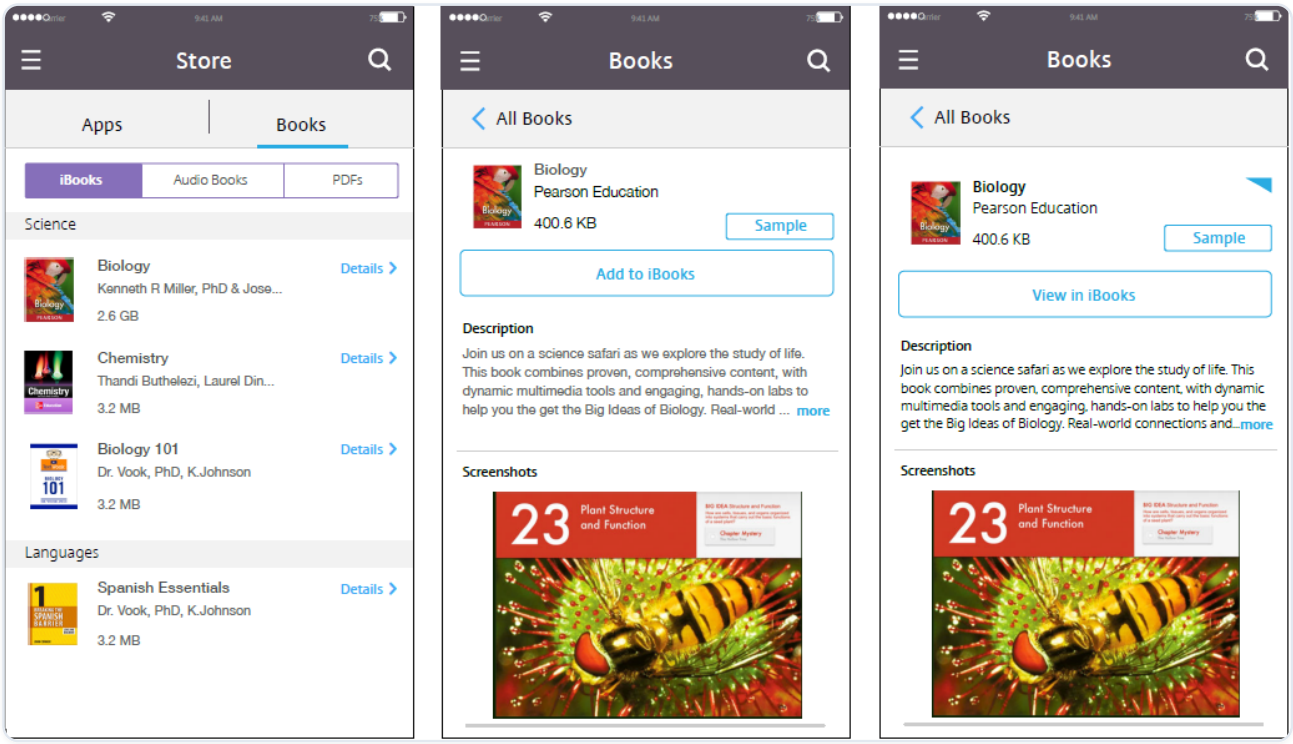
4. 使用**管理 > 设备**的**媒体**选项卡可查看部署状态。



注意：

在**配置** > **媒体**页面上，如果您选择一本图书并单击**删除**，Citrix Endpoint Management 会将该图书从列表中删除。但是，下次 Citrix Endpoint Management 与 Apple 批量采购同步时，除非已从 Apple 批量采购中删除该图书，否则该图书会重新出现在列表中。从列表中删除图书不会从设备中删除图书。

图书在用户设备上的显示方式如下例所示。


Store
Apps
Books
iBooks
Audio Books
PDFs
Science
Biology
Kenneth R Miller, PhD & Jose...
2.6 GB
Details
Chemistry
Thandi Buthelezi, Laurel Din...
3.2 MB
Details
Biology 101
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Languages
Spanish Essentials
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
Add to iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world ... more
Screenshots
23
Plant Structure and Function
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
View in iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world connections and...more
Screenshots
23
Plant Structure and Function

部署资源

设备配置和管理通常涉及在 Citrix 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打包。交付组定义了用户类别，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 Citrix Endpoint Management 控制台，您可以：

- 添加、管理和部署交付组。
- 更改 Citrix Endpoint Management 将交付组中的资源和操作推送到设备的顺序。此顺序称为 *部署顺序*。

  您可以在 Citrix 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，Citrix Endpoint Management 会确定部署顺序。请参阅 计算步骤。

关于交付组

包含在交付组中通常基于用户特征，例如公司、国家/地区、部门、办公地址和职称。交付组使您可以更好地控制谁获得哪些资源以及何时获得这些资源。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 Citrix Endpoint Management 会创建默认交付组 AllUsers。此组包含所有本地用户和 Active Directory 用户。您不能删除 AllUsers 组，但当您不想将资源推送到所有用户时，可以禁用它。有关详细信息，请参阅 启用和禁用 AllUsers 交付组。

当您将资源部署到交付组时，您会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 (APNs) 发送通知。有关详细信息，请参阅 APNs 证书)。对于 Android 设备，请使用 Firebase Cloud Messaging (FCM)。有关详细信息，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：

- 部署顺序： 部署顺序是 Citrix Endpoint Management 将资源（策略、应用程序和媒体）和操作推送到设备的顺序。部署顺序适用于交付组中配置了设备管理 (MDM) 或应用程序管理 (MAM) 和 MDM 组合的注册配置文件的设备。

- 部署规则： Citrix 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，部署规则可能指定当域名与特定值匹配时推送部署包。

  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资源上设置的部署规则。

- **部署计划**： Citrix 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。您可以指定部署立即发生、在设定的日期和时间发生，或者在满足部署条件时发生。您在创建规则时指定计划。请参阅 配置部署规则。

在添加交付组之前，请考虑部署顺序、规则和计划如何与您的部署目标相关联。

部署顺序

部署顺序是 Citrix Endpoint Management 将资源推送到设备的序列。当资源存在先决条件以及资源之间存在依赖关系时，部署顺序非常重要。资源包括策略、应用程序、操作和交付组。

例如，如果您要推送具有基于证书的身份验证的 Wi-Fi 策略，则必须在 Wi-Fi 策略之前推送证书策略。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，可以指定资源部署到设备的顺序。但是，Citrix 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，Citrix Endpoint Management 会计算交付给设备的各项对象以及其执行的操作的部署顺序。

在确定部署顺序时，Citrix Endpoint Management 会将筛选器和控制条件（例如部署规则和部署计划）应用于资源。下表显示了您可以应用于每种资源类型的条件。

资源	设备平台	部署规则	部署计划	用户/组
设备策略	是	是	是	-
应用程序	是	是	是	-
媒体	是	是	是	-
操作	-	是	是	-
交付组	-	是	-	是

计算步骤

当 Citrix Endpoint Management 需要计算部署顺序时，它会执行以下步骤。

> **注意：**
>
> 设备平台不影响计算步骤。

1. 根据用户、组和部署规则的筛选器，确定特定用户的所有交付组。
2. 在选定的交付组中创建所有资源（策略、应用程序、媒体和操作）的有序列表。该列表基于设备平台、部署规则和部署计划的筛选器。排序算法如下：
    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部署顺序的交付组中的资源之前。有关详细信息，请参阅使用用户定义顺序进行计算的示例。
    b. 作为交付组之间的决胜因素，按交付组名称的逆字母顺序对交付组中的资源进行排序。例如，Citrix Endpoint Management 将交付组 B 中的资源置于交付组 A 中的资源之前。
    c. 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，则保持该顺序。否则，按资源名称的字母顺序对该交付组中的资源进行排序。
    d. 如果同一资源出现多次，请删除重复资源。仅交付这些资源中的第一个。

具有管理员定义顺序的资源在没有管理员定义顺序的资源之前部署。

使用管理员定义顺序进行计算的示例

假设您有两个交付组：

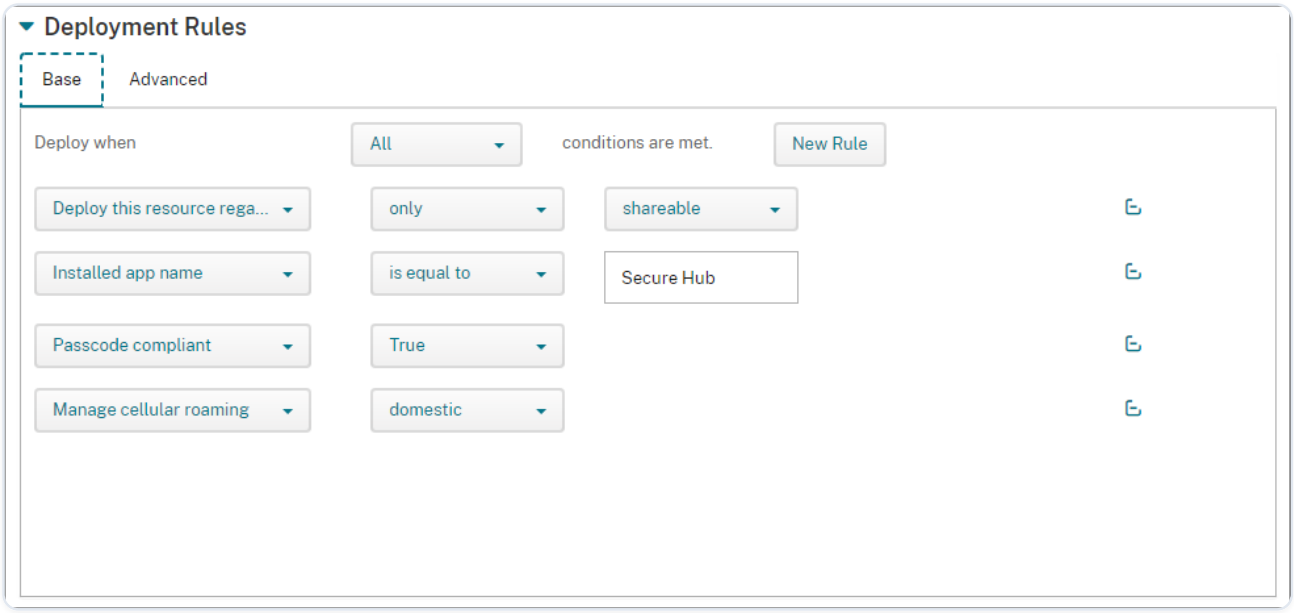
- 交付组客户经理 1：资源的顺序为 *未指定*。包含策略 **网络** 和 **密码**。
- 交付组客户经理 2：资源的顺序为 *已指定*。按顺序包含策略 **连接计划**、**限制**、**密码** 和 **网络**。

如果计算算法仅按名称对部署组进行排序，Citrix Endpoint Management 可能会按此顺序部署，从交付组客户经理 1 开始：**网络**、**密码**、**连接计划** 和 **限制**。Citrix Endpoint Management 可能会忽略来自客户经理 2 交付组的 **密码** 和 **网络**（两者都是重复项）。

但是，客户经理 2 组具有管理员指定的部署顺序。因此，计算算法将客户经理 2 交付组中的资源置于列表中的位置高于客户经理 1 交付组中的资源。结果，Citrix Endpoint Management 按此顺序部署策略：**连接计划**、**限制**、**密码** 和 **网络**。Citrix Endpoint Management 忽略来自客户经理 1 交付组的策略 **网络** 和 **密码**，因为它们是重复项。该算法遵循 Citrix 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。您可以配置基本或高级部署规则。



使用基本编辑器添加部署规则时，首先选择何时部署资源。

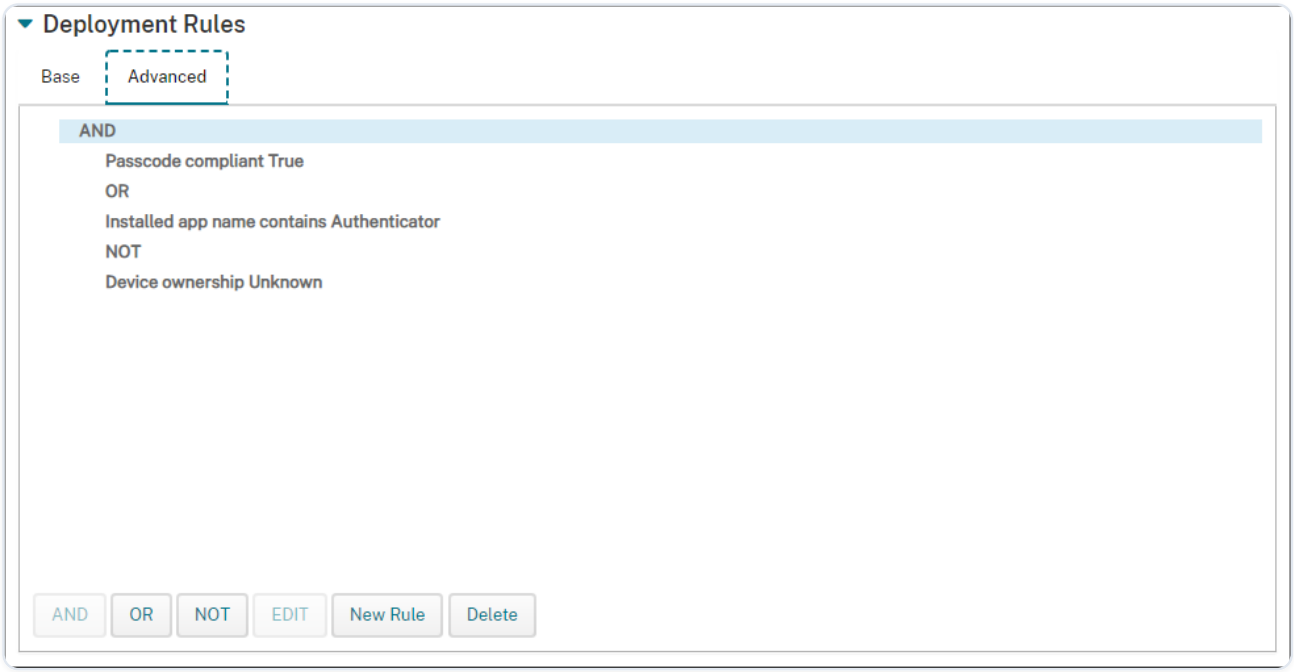
- **全部：**当用户或设备满足您配置的所有条件时，交付资源。
- **任意：**当用户或设备满足您配置的至少一个条件时，交付资源。

单击**新建规则**以从可用规则列表中选择要添加的规则。可用规则因部署的资源以及您配置资源的平台而异。每个规则中都包含条件。

您可以指定在以下情况下部署资源：

- 仅当选定属性存在时，或者除了选定属性存在时。
- 当属性与您键入的文本完全匹配时，属性包含您键入的文本，或者属性与您键入的文本不匹配时。
- 当设备或用户符合您选择的属性时，或者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，并且在创建高级规则时可以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，需要指定是在 Citrix Endpoint Management 中还是在 Citrix Cloud 中管理用户分配。创建交付组后，无法更改此规范。

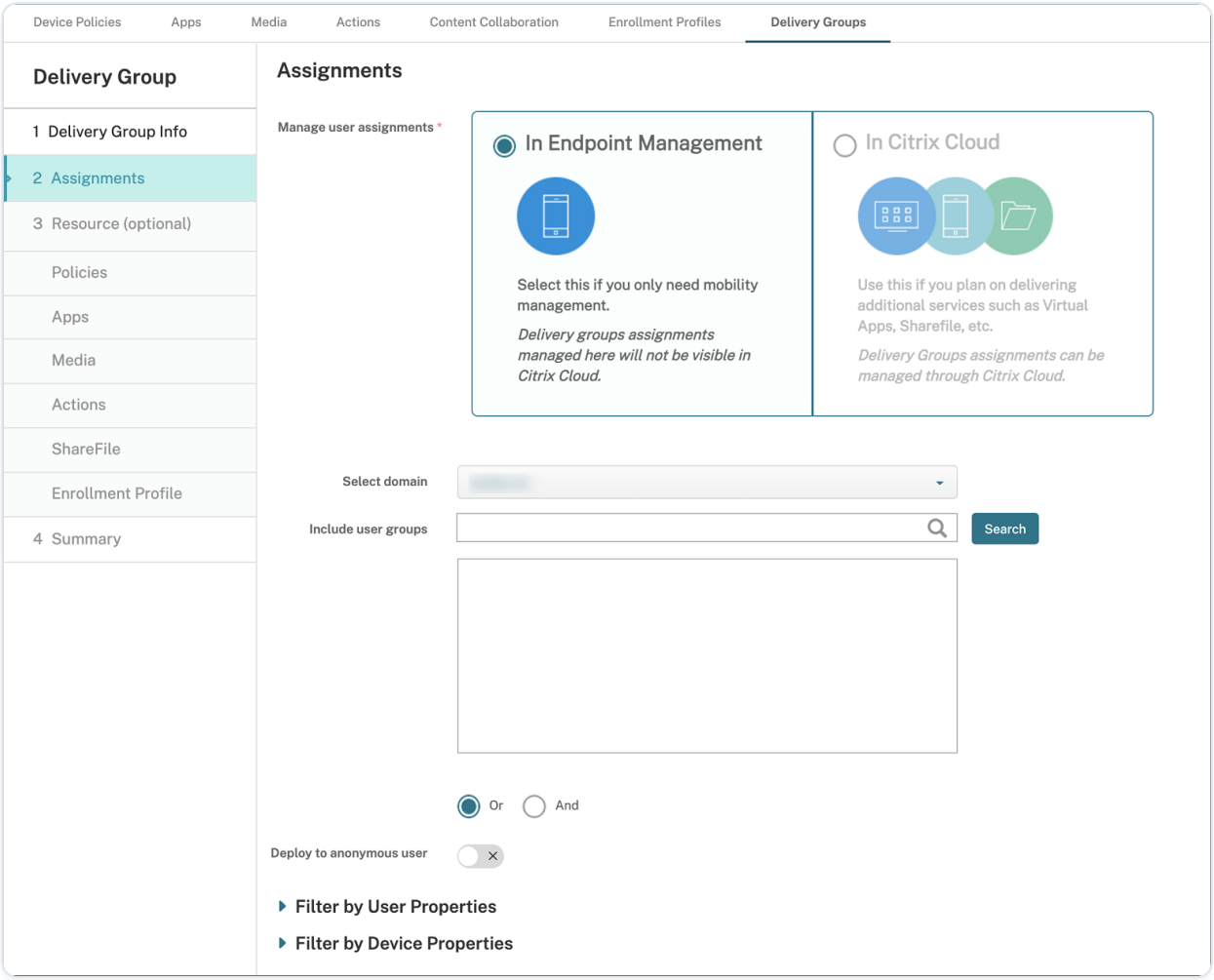
如果您计划使用交付组来交付其他 Citrix Cloud 服务，请指定在 Citrix Cloud 中管理用户分配。其他 Citrix Cloud 服务包括 Citrix Virtual Apps and Desktops、ShareFile 或 Secure Browser Service。您只能将 Active Directory 用户添加到在 Citrix Cloud 中管理的交付组。

如果只需要对用户和应用程序交付组进行移动性管理，请将**管理用户分配**设置为**在 Citrix Endpoint Management 中**。您无法在 Citrix Cloud 中查看在 Citrix Endpoint Management 中管理用户的交付组。因此，您无法使用在 Citrix Endpoint Management 中管理的交付组来交付其他服务。

> **注意：**

> 建议在创建设备策略和注册配置文件之前添加交付组。有关创建这些策略和配置文件的信息，请参阅设备策略和注册配置文件。

1. 在 Citrix Endpoint Management 控制台中，单击**配置 > 交付组**。
2. 在**交付组**页面中，单击**添加**。
3. 在**交付组信息**页面中，键入交付组的名称和描述，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 Citrix Endpoint Management 中：** 如果您计划为仅需要移动性管理的用户和应用程序创建交付组，请选择此选项。您无法在 Citrix Cloud 中查看其用户分配在 Citrix 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：** 如果您计划使用交付组来交付其他服务，请选择此选项。这些服务可能包括 Citrix Virtual Apps and Desktops 或 ShareFile。

5. 将用户添加到交付组。

> **重要提示：**
>
> 创建交付组后，无法更改“**管理用户分配**”设置。

- **选择域：** 从列表中，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。所选组将显示在“**选定的用户组**”列表中。
  - 单击“**搜索**”以查看所选域中所有用户组的列表。您还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“**选定的用户组**”列表中删除用户组，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**”以查看所选域中所有用户组的列表。或者，在单击“**搜索**”以缩小搜索范围之前，键入完整或部分组名称。清除要删除的每个组的复选框。
- **或/和：** 选择用户是属于任何组（或）还是必须属于所有组（和），以便将资源部署给他们。
- **部署到匿名用户：** 选择是否部署到交付组中的未经身份验证的用户。未经身份验证的用户是您无法进行身份验证但仍允许其设备连接到 Citrix Endpoint Management 的用户。

6. 展开“**按用户属性筛选**”或“**按设备属性筛选**”以指定交付组如何管理资源。
   - 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 桌面/平板电脑**
   - 默认情况下显示“**基本**”选项卡。在“**基本**”选项卡下，指定何时部署策略。您可以选择在满足“**所有**”条件或满足“**任何**”条件时部署策略。默认选项设置为“**所有**”。
     - 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。您在“**基本**”选项卡上选择的条件将显示。
     - 单击“**AND**”、“**OR**”或“**NOT**”，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一个条件，然后单击“**编辑**”以更改条件或单击“**删除**”以删除条件。

7. 单击“**下一步**”以转到“**策略**”页面。您可以在此处选择性地为交付组添加策略、应用程序、媒体或操作。有关详细信息，请参阅：

   - 将策略添加到交付组
   - 将应用程序添加到交付组
   - 将媒体添加到交付组
   - 将操作添加到交付组(#add-actions-to-a-delivery-group)

8. 当您对交付组满意时，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。

将策略添加到交付组

1. 在**资源（可选）列表中，单击策略**。
2. 对于要添加的每个策略，请执行以下操作：

   - 滚动浏览可用策略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**。
   - 将要添加的策略拖动到右侧的框中。

   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**以转到**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，请执行以下操作：

   - 滚动浏览可用应用程序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程序名称，然后单击**搜索**。
   - 将应用程序拖动到“**所需应用程序**”框或“**可选应用程序**”框中。

   对于标记为必需的应用程序，用户可以及时收到更新，例如在以下情况下：

   - 您上传了一个新应用并将其标记为必需。
   - 您将现有应用标记为必需。
   - 用户删除了一个必需应用。

- Citrix Secure Hub 更新可用。

有关必需应用的强制部署信息（包括如何启用该功能），请参阅关于必需和可选应用。

要从框中删除应用，请单击应用名称旁边的 **X**。

2. 单击 **Next** 转到 **Media** 页面。

将媒体添加到交付组

1. 对于要添加的每本书，请执行以下操作：

   - 滚动浏览可用书籍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籍名称，然后单击 **Search**。
   - 将要添加的书籍拖到 **Required Books** 框中。

   对于标记为必需的书籍，用户会在以下情况下及时收到更新：

   - 您上传了一本新书并将其标记为必需。
   - 您将现有书籍标记为必需。
   - 用户删除了一本必需书籍。
   - Citrix Secure Hub 更新可用。

   要从框中删除项目，请单击项目名称旁边的 **X**。

2. 单击“**下一步**”转到“**操作**”页面。

将操作添加到交付组

1. 对于要添加的每个操作，请执行以下操作：

   - 滚动可用操作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**”。
   - 将要添加的操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“**ShareFile**”页面。

应用 ShareFile 配置

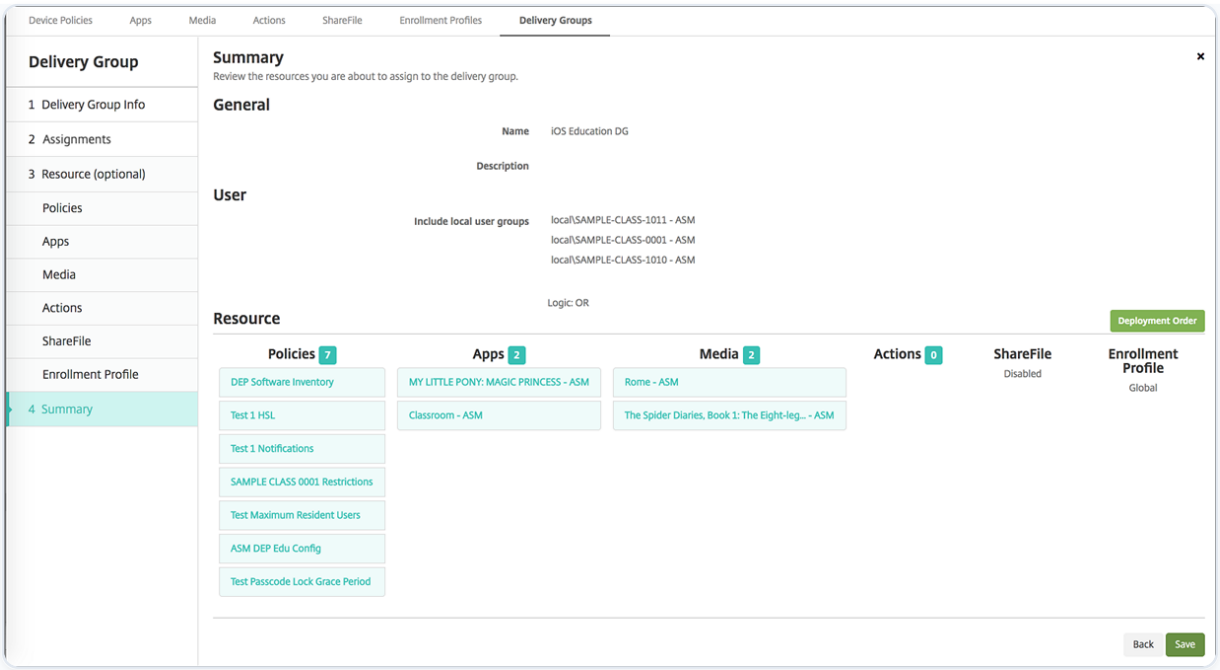
ShareFile 页面因您是为企业帐户还是为存储区域连接器配置了 Citrix Endpoint Management（**配置 > ShareFile**）而异。

- 如果您配置了企业帐户以与 Citrix Endpoint Management 结合使用，请将“**启用 ShareFile**”设置为“**开**”。此设置可为交付组提供对 ShareFile 内容和数据的单点登录访问。
- 如果您配置了存储区域连接器以与 Citrix 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动到右侧的框中。

查看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“**返回**”以返回上一页更改配置。



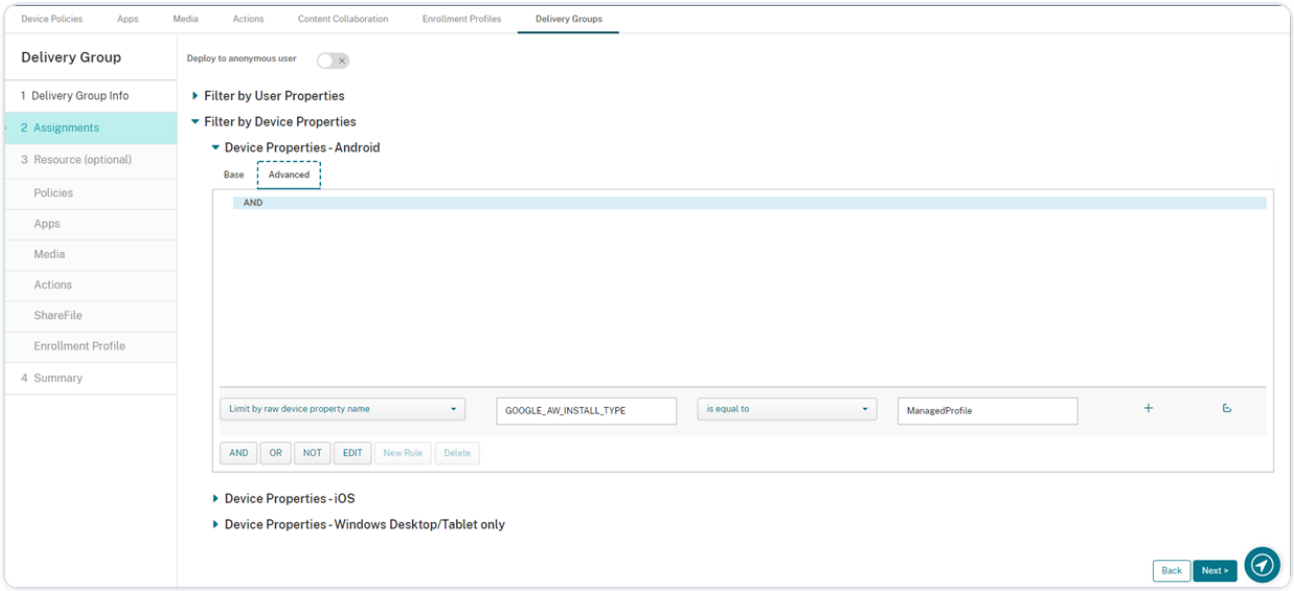
要查看或更改部署顺序：

1. 单击“**部署顺序**”。
2. 在“部署顺序”对话框中，将资源拖动到您要部署它的顺序位置。资源按从上到下的顺序部署。
3. 单击“**保存**”以保存部署顺序。

完成交付组配置后，在“摘要”页面上，单击“**保存**”。

创建规则以将资源部署到 Android Enterprise

您可以使用 Android 设备属性规则来管理交付组到 Android Enterprise 设备的部署。如果您为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。



要使用设备注册模式将交付组部署到 Android Enterprise 设备：

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**”选项卡并单击“**新建规则**”。
4. 在列表中，选择要添加到规则的条件：
   - 对于新的 Android Enterprise 设备，选择“**按原始设备属性名称限制**”并在第一个值字段中键入 **GOOGLE_AW_INSTALL_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，选择 **按已知设备属性名称限制**，并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，键入您的 Android Enterprise 设备的注册模式：
   - **设备管理员：** 指定仅用于工作用途的公司自有设备（也称为设备所有者模式）
   - **托管配置文件：** 指定 BYOD — 注册了工作配置文件管理的个人设备（也称为配置文件所有者模式）
   - **公司自有单用途：** 指定专用设备（以前称为公司自有单用途设备）
   - **公司自有个人启用：** 指定具有工作配置文件的完全托管设备（以前称为公司自有个人启用设备）

6. 按照 添加交付组 中所述完成交付组配置。

   有关详细信息，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：

1. 在 **设备属性 – Android** 中，打开 **高级选项卡** 并单击 **新建规则**。
2. 在列表中，选择 **已安装的应用程序名称** 并输入应用程序包 ID。

编辑交付组

您无法更改现有交付组的名称。要更新其他设置，请转至 **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 是唯一可以启用或禁用的交付组。您无法像删除其他交付组一样删除 AllUsers。

在**交付组**页面上，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**以禁用 AllUsers 交付组。此命令仅在 AllUsers 组已启用（默认）时可用。**已禁用**显示在交付组表中的**已禁用**标题下。
- 单击**启用**以启用 AllUsers 交付组。此命令仅在 AllUsers 组已禁用时可用。**已禁用**不再显示在交付组表中的**已禁用**标题下。

部署到交付组

部署到交付组意味着向所有拥有 Apple、Android 和 Windows 平板电脑设备的用户发送推送通知。

对于拥有其他平台设备的用户，如果这些设备已连接到 Citrix Endpoint Management，他们会立即收到资源。否则，根据其调度策略，他们会在下次连接时收到资源。

要使更新的应用程序显示在 Android 设备应用商店的“可用更新”列表中，请首先向用户设备部署应用程序清单策略。

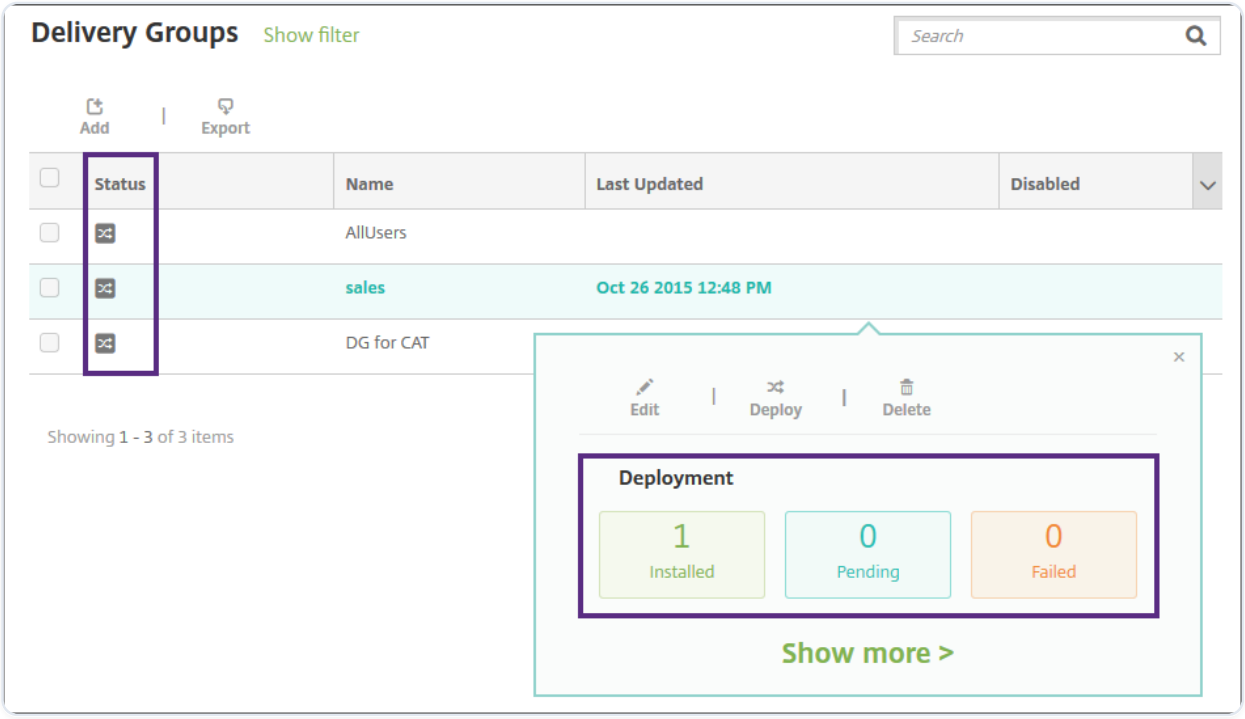
1. 在**交付组**页面上，执行以下操作之一：
   - 要一次部署到多个交付组，请选中要部署的组旁边的复选框。
   - 要部署到单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。
2. 单击**部署**。

   根据您选择单个交付组的方式，**部署**命令会显示在交付组上方或右侧。

验证您要部署应用程序、策略和操作的组是否已列出。然后单击**部署**。应用程序、策略和操作将根据设备平台和调度策略部署到所选组。

您可以通过以下方式之一检查**交付组**页面上的部署状态：

- 查看交付组**状态**标题下的部署图标，该图标指示任何部署失败。
- 点击包含交付组的行以显示一个叠加层，其中显示**已安装**、**待处理**和**失败**的部署。



克隆交付组

当您想要创建与现有交付组类似的交付组时，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。

1. 在 Citrix 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，并（可选）输入说明。
5. 选择**克隆**。

删除交付组

您无法删除 AllUsers 交付组，但当您不想向所有用户推送资源时，可以将其禁用。请参阅启用和禁用 AllUsers 交付组。

> **重要提示：**
>
> 删除操作无法撤消。

1. 在**交付组**页面上，执行以下操作之一：
   - 要一次删除多个交付组，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**命令会显示在交付组上方或右侧。
3. 在**删除**对话框中，单击**删除**。

导出交付组表

1. 单击**交付组**表上方的**导出**。Citrix Endpoint Management 会提取**交付组**表中的信息并将其转换为 .csv 文件。
2. 按照浏览器的常规步骤打开或保存 .csv 文件。

宏

Citrix Endpoint Management 提供宏，用于在以下项目的文本字段中填充用户或设备属性数据：

- 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

Citrix Endpoint Management 会将宏替换为相应的用户或系统值。例如，您可以在一个 Exchange 配置文件中为数千名用户预填充用户的邮箱值。

宏语法

宏可以采用以下形式：

- `${type.PROPERTYNAME}`

- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]}`

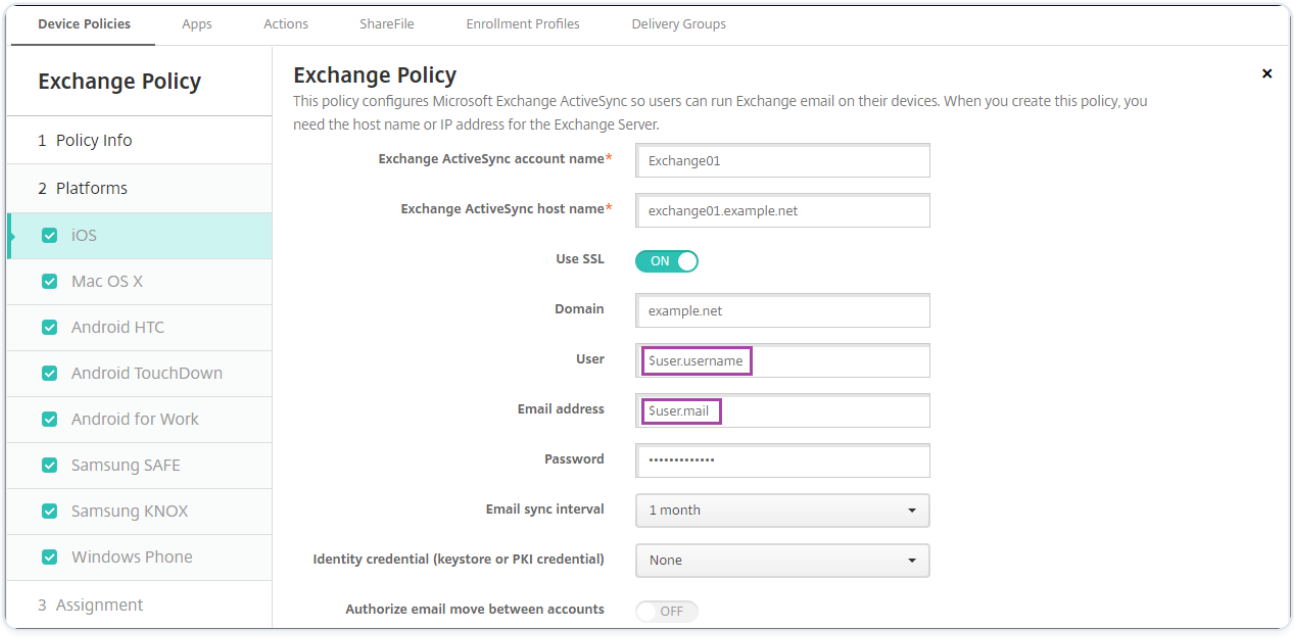
将美元符号 ($) 后面的所有语法用大括号 ({ }) 括起来。

- 限定属性名称引用用户属性、设备属性或自定义属性。
- 限定属性名称由前缀和实际属性名称组成。
- 用户属性采用 `${user.[PROPERTYNAME] (prefix="user.")}` 形式。
- 设备属性采用 `${device.[PROPERTYNAME] (prefix="device.")}` 形式。
- 属性名称区分大小写。
- 函数可以是有限列表，也可以是定义函数的第三方参考链接。此通知消息宏包含函数 `firstnotnull`：

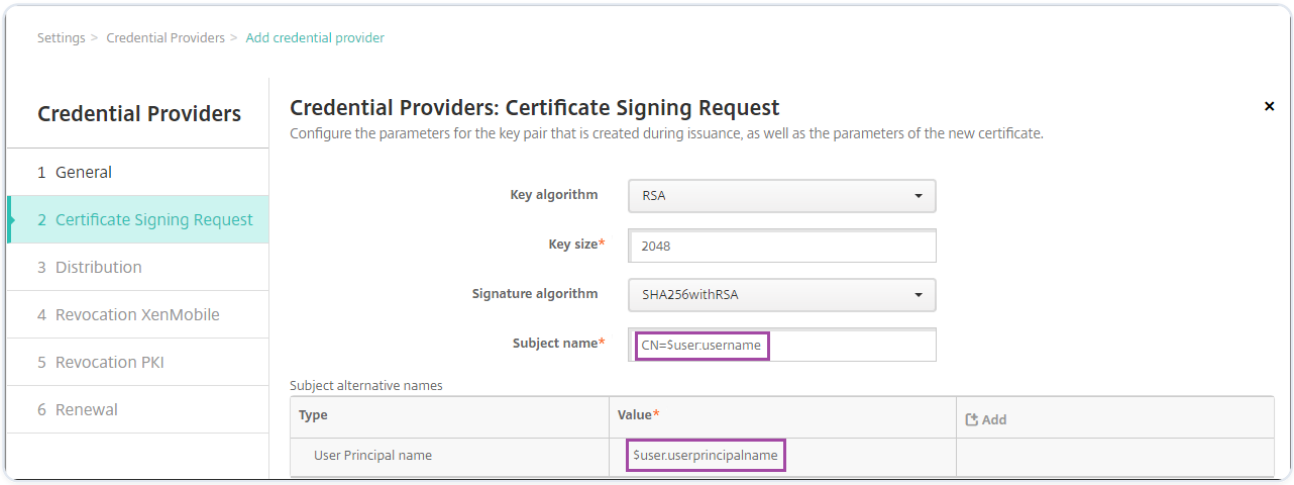
设备 `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 已被阻止...

- 对于自定义宏（您定义的属性），前缀为 `${custom}`。您可以省略此前缀。

以下是一个常用宏的示例，`${user.username}`，它在策略的文本字段中填充用户名值。此宏对于配置 Exchange ActiveSync 配置文件以及许多用户使用的其他配置文件非常有用。以下示例演示了如何在 Exchange 策略中使用宏。**用户**的宏为 `${user.username}`。**电子邮件地址**的宏为 `${user.mail}`。

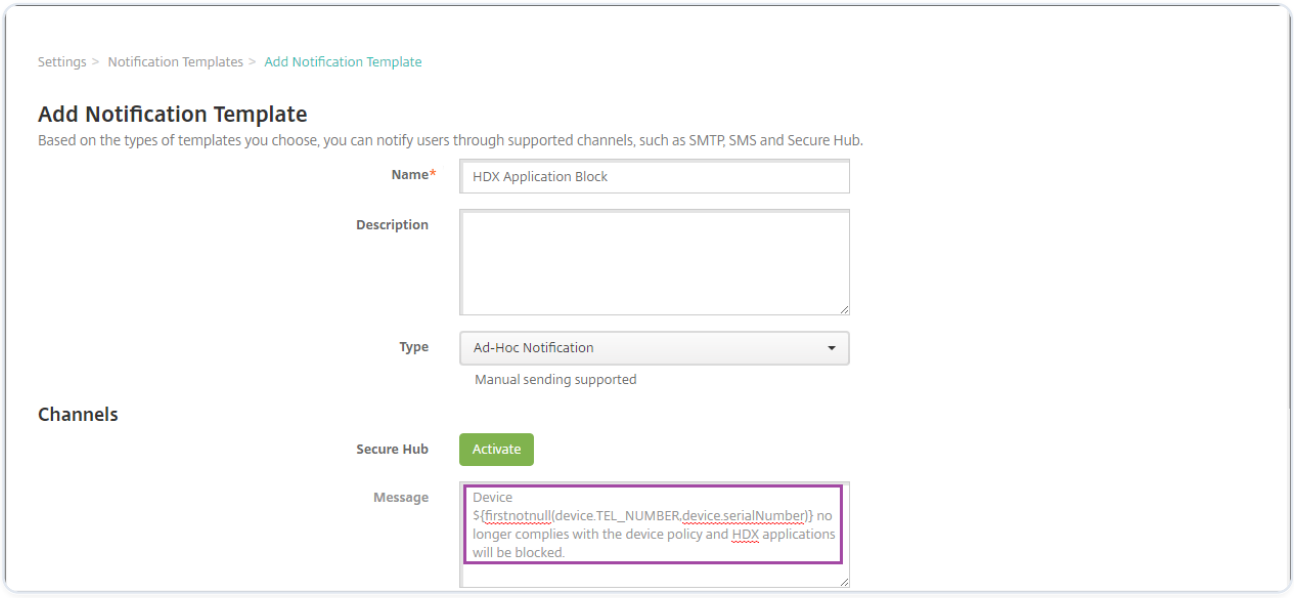


以下示例演示了如何为证书签名请求使用宏。**主题名称**的宏为 **CN=$user.username**。**主题备用名称**的**值**的宏为 **$user.userprincipalname**。



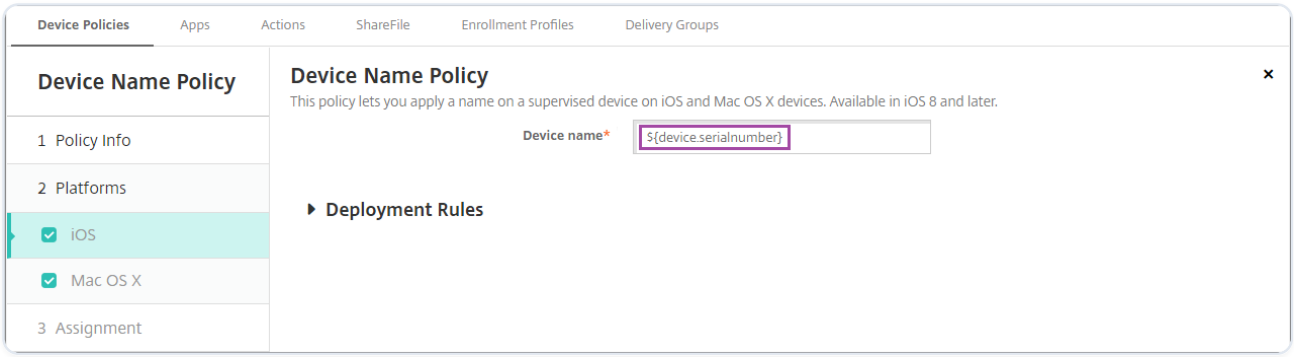
以下示例演示了如何在通知模板中使用宏。该示例模板定义了当 HDX™ 应用程序因设备不合规而被阻止时发送给用户的消息。**消息**的宏为：

设备 `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 不再遵循设备策略，HDX 应用程序已被阻止。



有关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。您可以键入宏、宏组合或宏与文本的组合来唯一命名每个设备。例如，使用 `${device.serialnumber}` 将设备名称设置为每个设备的序列号。使用 `${device.serialnumber} ${ user.username }` 在设备名称中包含用户名。设备名称设备策略适用于受监管的 iOS 和 macOS 设备。



默认通知模板的宏

您可以在默认通知模板中使用以下宏：

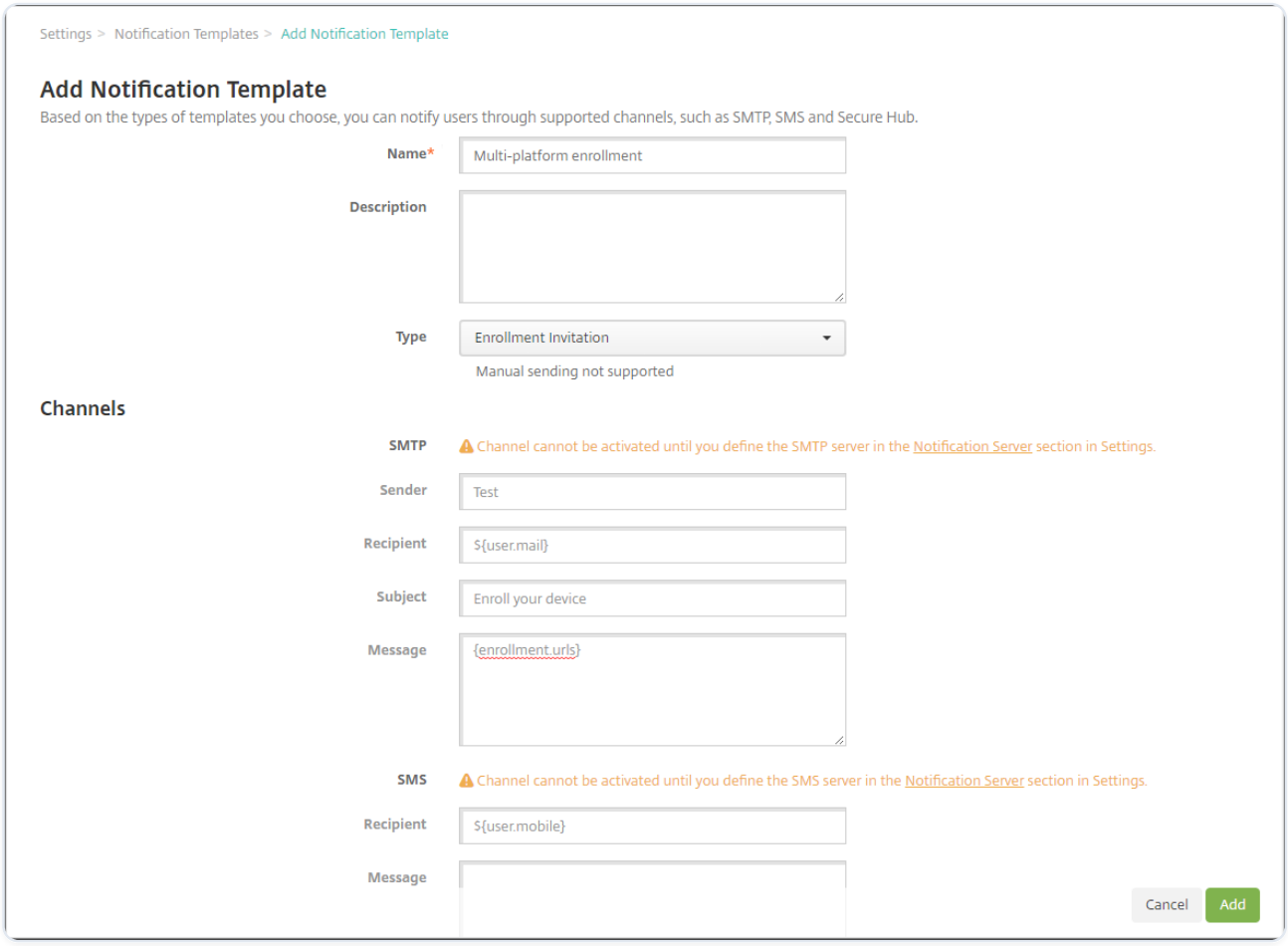
- `${account.SUPPORT_EMAIL}`
- `${applicationName}`
- `${enrollment.andriod.agent.download.url}`
- `${enrollment.ios.agent.download.url}`
- `${enrollment.pin}`
- `${enrollment.url}`
- `${enrollment.urls}`
- `${enrollment.ios.url}`
- `${enrollment.macos.url}`
- `${enrollment.android.url}`
- `${enrollment.ios.platform}`
- `${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：**

> Citrix Endpoint Management 控制台包含“黑名单”和“白名单”术语。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

> 此示例演示如何创建包含许多设备平台的注册 URL 的通知。**消息**的宏为：

${enrollment.urls}



以下示例演示如何为通知创建消息，以提示用户单击其设备平台的注册 URL：

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}
```

示例 2：

```
To enroll an iOS device, click the link ${enrollment.ios.url}.


To enroll a macOS device, click the link ${enrollment.macos.url}.


To enroll an Android device, click the link ${enrollment.android.url}.
```

特定策略的宏

对于设备名称设备策略（适用于 iOS 和 macOS），您可以将这些宏用于**设备名称：**

- `${device.serialnumber}`
- `${user.username}@example.com`
- `${device.serialnumber}`
- `${device.serialnumber}`
- `${user.username}`
- `${enrollment.pin}`
- `${user.dnsroot}`

对于蜂窝设备策略（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，它们会扩展为整数。

对于通过使用**导入 iOS 和 macOS 配置文件**设备策略导入到 Citrix Endpoint Management 中的设备配置 XML 文件，您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，您可以将此宏用于 **ELM 许可证密钥：**

- `${elm.license.key}`

对于 Web 剪辑设备策略，您可以将此宏用于 **URL**：

- `${webeas-url}`

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`

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： 激活锁绕过代码

- **Web 元素：** `ACTIVATION_LOCK_BYPASS_CODE`
- **宏：** `${device.ACTIVATION_LOCK_BYPASS_CODE}`

显示名称： 激活锁已启用

- **Web 元素：** `ACTIVATION_LOCK_ENABLED`
- **宏：** `${device.ACTIVATION_LOCK_ENABLED}`

显示名称： 活跃的 Apple App Store 账户

- **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`
- **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： Android Enterprise 已启用设备？

- **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： 防病毒签名状态

- **Web 元素：** `ANTI_VIRUS_SIGNATURE_STATUS`
- **宏：** `${device.ANTI_VIRUS_SIGNATURE_STATUS}`

显示名称： 防病毒状态

- **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代码

- **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

- **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： 在后台自动下载软件更新

- **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}`

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： 电池充电

- **Web 元素：** `BATTERY_CHARGING_STATUS`
- **宏：** `${device.BATTERY_CHARGING_STATUS}`

显示名称： 电池充电

- **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： 电池运行时长

- **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 server agent ID

- **Web 元素：** `AGENT_ID`
- **宏：** `${device.AGENT_ID}`

显示名称： BES server name

- **Web 元素：** `BES_SERVER`
- **宏：** `${device.BES_SERVER}`

显示名称： BES server version

- **Web 元素：** `BES_VERSION`
- **宏：** `${device.BES_VERSION}`

显示名称： BIOS Info

- **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： 蜂窝网络海拔

- **Web 元素：** `GPS_ALTITUDE_FROM_CELLULAR`
- **宏：** `${device.GPS_ALTITUDE_FROM_CELLULAR}`

显示名称： 蜂窝网络航向

- **Web 元素：** `GPS_COURSE_FROM_CELLULAR`
- **宏：** `${device.GPS_COURSE_FROM_CELLULAR}`

显示名称： 蜂窝网络水平精度

- **Web 元素：** `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`

- **宏：** `${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}`

显示名称： 蜂窝网络纬度

- **Web 元素：** `GPS_LATITUDE_FROM_CELLULAR`
- **宏：** `${device.GPS_LATITUDE_FROM_CELLULAR}`

显示名称： 蜂窝网络经度

- **Web 元素：** `GPS_LONGITUDE_FROM_CELLULAR`
- **宏：** `${device.GPS_LONGITUDE_FROM_CELLULAR}`

显示名称： 蜂窝网络速度

- **Web 元素：** `GPS_SPEED_FROM_CELLULAR`
- **宏：** `${device.GPS_SPEED_FROM_CELLULAR}`

显示名称： 蜂窝网络技术

- **Web 元素：** `CELLULAR_TECHNOLOGY`
- **宏：** `${device.CELLULAR_TECHNOLOGY}`

显示名称： 蜂窝网络时间戳

- **Web 元素：** `GPS_TIMESTAMP_FROM_CELLULAR`
- **宏：** `${device.GPS_TIMESTAMP_FROM_CELLULAR}`

显示名称： 蜂窝垂直精度

- **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}

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： 云备份已启用

- **Web 元素：** `CLOUD_BACKUP_ENABLED`
- **宏：** `${device.CLOUD_BACKUP_ENABLED}`

显示名称： 代码完整性已启用？

- **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`
- **宏：** `${device.CARRIER}`

显示名称： 当前移动国家代码

- **Web 元素：** `CURRENT_MCC`
- **宏：** `${device.CURRENT_MCC}`

显示名称： 当前移动网络代码

- **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： 上次 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： 已分配 Apple 部署计划配置文件

- **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

- **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： 描述

- **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： 勿扰模式已激活

- **Web 元素：** `DO_NOT_DISTURB`
- **宏：** `${device.DO_NOT_DISTURB}`

显示名称： ELAM 驱动程序已加载？

- **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}`

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 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`
- **宏：** `${device.EXTERNAL_STORAGE2_FREE_SPACE}`

显示名称： 外部存储 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： 外部存储已加密

- **Web 元素：** `EXTERNAL_ENCRYPTION`
- **宏：** `${device.EXTERNAL_ENCRYPTION}`

显示名称： FileVault 已启用

- **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 目录别名

- **Web 元素：** `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- **宏：** `${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}`

显示名称： Google 目录姓氏

- **Web 元素：** `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- **宏：** `${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}`

显示名称： Google 目录名称

- **Web 元素：** `GOOGLE_AW_DIRECTORY_NAME`
- **宏：** `${device.GOOGLE_AW_DIRECTORY_NAME}`

显示名称： Google 目录主电子邮件

- **Web 元素：** `GOOGLE_AW_DIRECTORY_PRIMARY`
- **宏：** `${device.GOOGLE_AW_DIRECTORY_PRIMARY}`

显示名称： Google 目录用户 ID

- **Web 元素：** `GOOGLE_AW_DIRECTORY_USER_ID`
- **宏：** `${device.GOOGLE_AW_DIRECTORY_USER_ID}`

显示名称： GPS 海拔

- **Web 元素：** `GPS_ALTITUDE_FROM_GPS`
- **宏：** `${device.GPS_ALTITUDE_FROM_GPS}`

显示名称： GPS 航向

- **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}`

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： 家庭运营商网络

- **Web 元素：** `SIM_CARRIER_NETWORK`
- **宏：** `${device.SIM_CARRIER_NETWORK}`

显示名称： 归属地移动国家代码

- **Web 元素：** `SIM_MCC`
- **宏：** `${device.SIM_MCC}`

显示名称： 归属地移动网络代码

- **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： 身份

- **Web 元素：** `AS_DEVICE_IDENTITY`
- **宏：** `${device.AS_DEVICE_IDENTITY}`

显示名称： IMEI/MEID 号码

- **Web 元素：** `IMEI`
- **宏：** `${device.IMEI}`

显示名称： IMSI

- **Web 元素：** `SIM_ID`
- **宏：** `${device.SIM_ID}`

显示名称： 内部存储已加密

- **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： 越狱/Root

- **Web 元素：** `ROOT_ACCESS`
- **宏：** `${device.ROOT_ACCESS}`

显示名称： 内核调试已启用？

- **Web 元素：** `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- **宏：** `${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}`

显示名称： 信息亭模式

- **Web 元素：** `IS_KIOSK`
- **宏：** `${device.IS_KIOSK}`

显示名称： 上次已知 IP 地址

- **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： 上次计划的软件更新

- **Web 元素：** `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- **宏：** `${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}`

显示名称： 上次计划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： 上次计划的软件更新状态

- **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： 定位器服务已启用

- **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}`

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： MDM 丢失模式已启用

- **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： 手机号码

- **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`

- **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

- **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

- **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： 密码合规

- **Web 元素：** `PASSCODE_IS_COMPLIANT`
- **宏：** `${device.PASSCODE_IS_COMPLIANT}`

显示名称： 密码符合配置

- **Web 元素：** `PASSCODE_IS_COMPLIANT_WITH_CFG`
- **宏：** `${device.PASSCODE_IS_COMPLIANT_WITH_CFG}`

显示名称： 存在密码

- **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： 周边入侵

- **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： 个人热点已激活

- **Web 元素：** `PERSONAL_HOTSPOT_ENABLED`
- **宏：** `${device.PERSONAL_HOTSPOT_ENABLED}`

显示名称： 地理围栏 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 IMEI

- **Web 元素：** `IDENTITY1_IMEI`
- **宏：** `${device.IDENTITY1_IMEI}`

显示名称： 主 SIM IMSI

- **Web 元素：** `IDENTITY1_IMSI`
- **宏：** `${device.IDENTITY1_IMSI}`

显示名称： 主 SIM 漫游

- **Web 元素：** `IDENTITY1_ROAMING`
- **宏：** `${device.IDENTITY1_ROAMING}`

显示名称： 主 SIM 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

- **Web 元素：** `SCREEN_NB_COLORS`
- **宏：** `${device.SCREEN_NB_COLORS}`

显示名称： 屏幕：大小

- **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： 辅助 SIM 卡 IMEI

- **Web 元素：** `IDENTITY2_IMEI`
- **宏：** `${device.IDENTITY2_IMEI}`

显示名称： 辅助 SIM IMSI

- **Web 元素：** `IDENTITY2_IMSI`
- **宏：** `${device.IDENTITY2_IMSI}`

显示名称： 辅助 SIM 漫游

- **Web 元素：** `IDENTITY2_ROAMING`
- **宏：** `${device.IDENTITY2_ROAMING}`

显示名称： 辅助 SIM 漫游合规性

- **Web 元素：** `IDENTITY2_ROAMING_COMPLIANCE`
- **宏：** `${device.IDENTITY2_ROAMING_COMPLIANCE}`

显示名称： 安全启动已启用？

- **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： SecureContainer 已启用

- **Web 元素：** `DLP_ACTIVE`

- **宏：** `${device.DLP_ACTIVE}`

显示名称： 安全补丁级别

- **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： 支持短信

- **Web 元素：** `IS_SMS_CAPABLE`
- **宏：** `${device.IS_SMS_CAPABLE}`

显示名称： 受监管

- **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： 篡改状态

- **Web 元素：** `TAMPERED_STATUS`
- **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： 条款和协议已接受？

- **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： 用户账户控制状态

- **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 #1

- **Web 元素：** `USER_DEFINED_1`
- **宏：** `${device.USER_DEFINED_1}`

显示名称： 用户定义 #2

- **Web 元素：** `USER_DEFINED_2`
- **宏：** `${device.USER_DEFINED_2}`

显示名称： 用户定义 #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

- **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 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}`

显示名称： WinPE 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： Citrix Endpoint Management 代理 ID

- **Web 元素：** `ENROLLMENT_AGENT_ID`
- **宏：** {device.ENROLLMENT_AGENT_ID}`

显示名称： Citrix Endpoint Management 代理修订版

- **Web 元素：** `EW_REVISION`
- **宏：** `${device.EW_REVISION}`

显示名称： Citrix 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 补丁版本

- **Web 元素：** `ZEBRA_PATCH_VERSION`
- **宏：** `${device.ZEBRA_PATCH_VERSION}`

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`（登录名减去域，如果有）	`${user.username}`

所有用户属性的宏

显示名称	WEB 元素	宏
Active Directory 登录失败尝试次数	`badpwdcount`	`${user.badpwdcount}`
ActiveSync 用户电子邮件	`asuseremail`	`${user.asuseremail}`
ASM 数据源	`aspersonsource`	`${user.aspersonsource}`
ASM 部署计划帐户名称	`asmdepaccount`	`${user.asmdepaccount}`
ASM 托管 Apple ID	`aspersonmanagedappleid`	`${user.aspersonmanagedappleid}`
ASM 密码类型	`aspersonpasscodetype`	`${user.aspersonpasscodetype}`
ASM 人员 ID	`aspersonid`	`${user.aspersonid}`
ASM 人员状态	`aspersonstatus`	`${user.aspersonstatus}`
ASM 人员职称	`aspersontitle`	`${user.aspersontitle}`
ASM 人员唯一 ID	`aspersonuniqueid`	`${user.aspersonuniqueid}`

显示名称	WEB 元素	宏
ASM 源系统 ID	`asmpersonsourcesystemid`	`${user.asmpersonsourcesystemid}`
ASM 学生年级	`asmpersongrade`	`${user.asmpersongrade}`
BES 用户电子邮件	`besuseremail`	`${user.besuseremail}`
公司	`company`	`${user.company}`
公司名称	`companyname`	`${user.companyname}`
国家	`c`	`${user.c}`
部门	`department`	`${user.department}`
描述	`description`	`${user.description}`
禁用用户	`disableduser`	`${user.disableduser}`
显示名称	`displayname`	`${user.displayname}`
可分辨名称	`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`	`${user.homestreetaddress}`
家庭城市	`homecity`	`${user.homecity}`
家庭国家	`homecountry`	`${user.homecountry}`
家庭传真	`homefax`	`${user.homefax}`
家庭电话	`homephone`	`${user.homephone}`

显示名称	WEB 元素	宏
家庭省/地区	`homestate`	`${user.homestate}`
家庭邮政编码	`homezip`	`${user.homezip}`
IP 电话	`ipphone`	`${user.ipphone}`
中间名首字母	`middleinitial`	`${user.middleinitial}`
中间名	`middlename`	`${user.middlename}`
手机	`mobile`	`${user.mobile}`
名称	`cn`	`${user.cn}`
办公地址	`physicaldeliveryofficename`	`${user.physicaldeliveryofficename}`
办公城市	`l`	`${user.l}`
办公传真号码	`facsimiletelephonenumber`	`${user.facsimiletelephonenumber}`
办公省/州	`st`	`${user.st}`
办公街道地址	`officestreetaddress`	`${user.officestreetaddress}`
办公电话号码	`telephonenumber`	`${user.telephonenumber}`
办公邮政编码	`postalcode`	`${user.postalcode}`
邮政信箱	`postofficebox`	`${user.postofficebox}`
寻呼机	`pager`	`${user.pager}`
主组 ID	`primarygroupid`	`${user.primarygroupid}`
SAM 帐户	`samaccountname`	`${user.samaccountname}`

显示名称	WEB 元素	宏
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

您可以在 Citrix Endpoint Management 中创建自动化操作，以编程方式响应以下情况：

- 事件
- 用户或设备属性
- 用户设备上应用程序的存在

创建自动化操作时，为该操作定义的触发器决定了用户设备连接到 Citrix Endpoint Management 时会发生什么。当事件被触发时，您可以向用户发送通知以纠正问题，以免采取更严重的措施。

您设置为自动发生的效果包括以下内容：

- 完全或选择性擦除设备。
- 将设备设置为不合规。
- 吊销设备。
- 向用户发送通知以纠正问题，以免采取更严重的措施。

您可以为仅 MAM 模式配置应用程序锁定和应用程序擦除操作。

您可以使用自动化操作将已加入 Azure Active Directory (AD) 的 Windows 10 和 Windows 11 设备标记为 Azure AD 中的不合规设备。

> **注意：**

> 在通知用户之前，您必须在 Citrix Endpoint Management 的 SMTP 设置中配置通知服务器，以便 Citrix Endpoint Management 可以发送消息。有关详细信息，请参阅通知。在继续操作之前，请设置您计划使用的任何通知模板。有关详细信息，请参阅通知。设置 u，请参阅创建和更新通知模板。

示例操作

以下是使用自动化操作的一些示例：

示例一

- 您想要检测之前阻止的应用程序（例如，“Words with Friends”）。您可以指定一个触发器，在检测到“Words with Friends”应用程序后，将用户设备设置为不合规。然后，该操作会通知用户必须删除该应用程序，以使设备恢复合规。您还可以设置一个时间限制，以确定等待用户合规的时间。超过该时间限制后，将执行一个已定义的操作，例如选择性擦除设备。

示例二

- 您想要验证客户是否正在使用最新固件，如果用户必须更新其设备，则阻止其访问资源。您可以指定一个触发器，当用户设备没有最新版本时，将其设置为不合规。您可以使用自动化操作来阻止资源并通知客户。

示例三

- 用户设备处于不合规状态，然后用户修复了该设备。您可以配置策略以部署一个软件包，将设备重置为合规状态。

示例四

- 您希望将长时间不活动的用户设备标记为不合规。您可以按如下方式为不活动设备创建自动化操作：

  a. 在 Citrix Endpoint Management 控制台中，转至**设置 > 网络访问控制**，然后选择**不活动设备**。有关**不活动设备**设置的详细信息，请参阅网络访问控制。

  b. 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**页面上按如下方式配置设置：

     - **触发器**。选择**设备属性**、**不合规**和**True**。
     - **操作**。选择**发送通知**，然后选择您在**设置**中使用**通知模板**创建的模板。然后设置执行操作前的延迟时间（以天、小时或分钟为单位）。设置操作重复的间隔，直到用户解决触发问题。

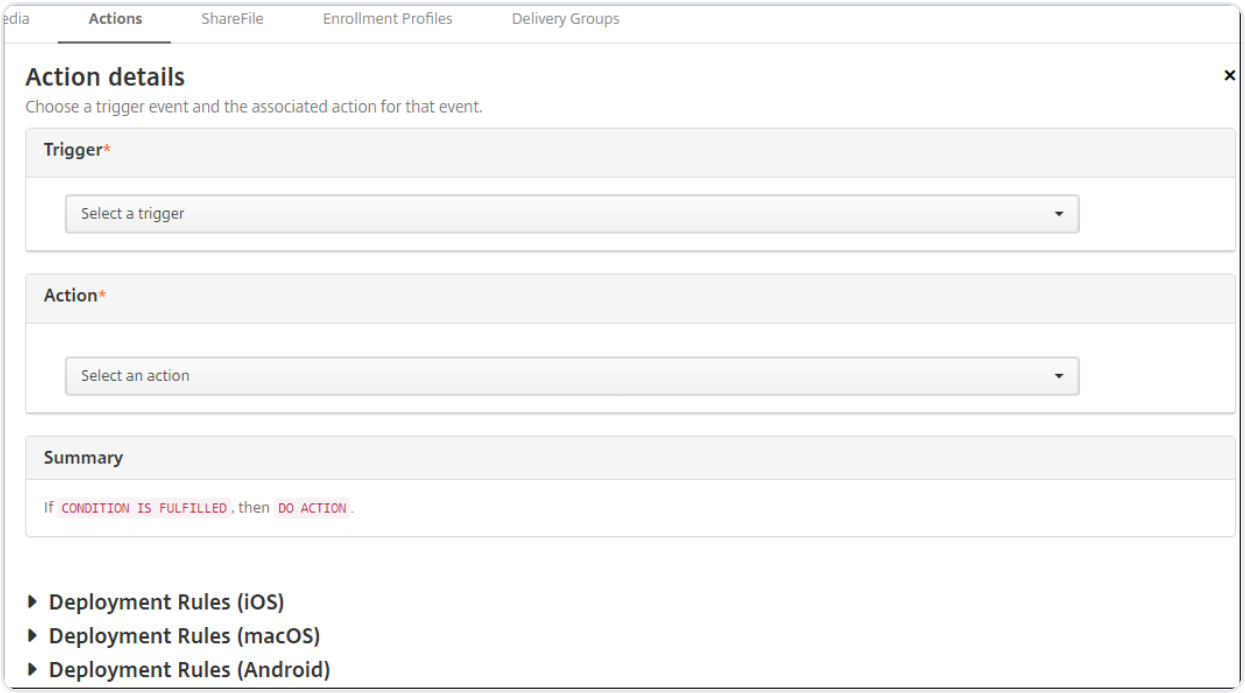
> **提示：**
>
> 要批量删除不活动设备，请使用Citrix Endpoint Management 公共 REST API。您首先手动获取要删除的不活动设备的设备 ID，然后运行删除 API 以批量删除它们。

添加和管理操作

要添加、编辑和筛选自动化操作：

1. 在 Citrix Endpoint Management 控制台中，单击 **Configure > Actions**。将显示 **Actions** 页面。
2. 在 **Actions** 页面上，执行以下操作之一：
   - 单击 **Add** 以添加操作。
   - 选择一个现有操作以编辑或删除。单击要使用的选项。
3. 将显示 **Action Information** 页面。
4. 在 **Action Information** 页面上，输入或修改以下信息：
   - **名称：** 键入一个名称以标识操作。此字段为必填项。
   - **描述：** 描述此操作的预期用途。
5. 单击 **Next**。将显示 **Action details** 页面。

   以下示例显示了如何设置 **Event** 触发器。如果选择不同的触发器，则生成的选项将与此处显示的选项不同。



6. 在 **Action details** 页面上，输入或修改以下信息：

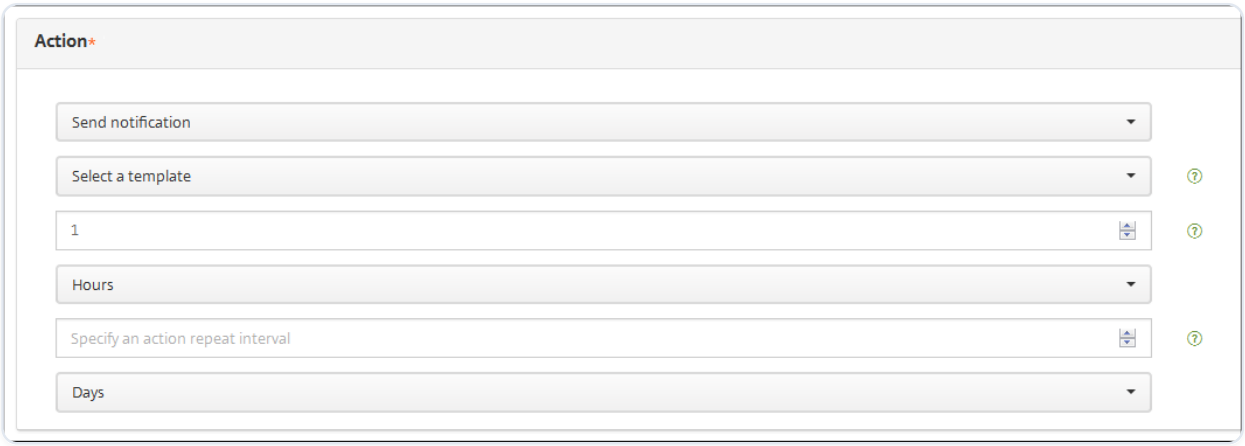
   在 **Trigger** 列表中，单击此操作的事件触发器类型。选择以下触发器之一：
   - **事件：** 检查设备状态是否与您选择的不合规事件匹配，然后对其作出反应。
   - **设备属性：** 检查 MDM 管理设备上的设备属性的特定值，然后做出反应。有关详细信息，请参阅 设备属性名称和值 PDF。
   - **用户属性：** 对用户属性的特定值做出反应，通常来自 Active Directory。

- **已安装应用程序名称：** 对应用程序的安装做出反应。不适用于仅 MAM 模式。需要在设备上启用应用程序清单策略。应用程序清单策略默认在所有平台上启用。有关详细信息，请参阅应用程序清单设备策略。
- **策略返回值：** 检查 PowerShell 脚本返回的值是否符合某些逻辑条件。必须启用并配置 Windows Agent 策略。有关 Windows Agent 策略的详细信息，请参阅 Windows Agent 设备策略。

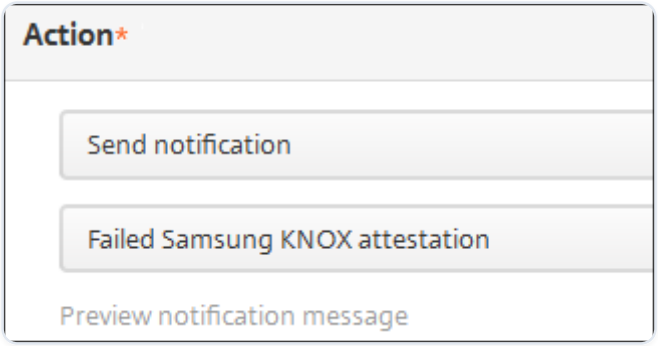
7. 在下一个列表中，单击对触发器的响应。
8. 在“**操作**”列表中，单击在满足触发器条件时要执行的操作。除了“**发送通知**”操作之外，您可以选择一个时间范围，在此时间范围内用户可以解决导致触发器的问题。如果问题未在该时间范围内解决，则会执行所选操作。有关操作的定义，请参阅 安全操作。

   如果选择“**发送通知**”，请使用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。将显示与所选事件相关的通知模板。如果没有适用于此通知类型的模板，系统将提示您配置一个模板，并显示消息：“此事件类型没有模板。请在“**设置**”中使用“**通知模板**”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 Citrix Endpoint Management 可以发送消息。请参阅 通知。此外，在继续之前，请使用“**设置 > 通知模板**”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**”。



10. 在以下字段中，设置执行操作前的延迟（以天、小时或分钟为单位）。设置操作重复的间隔，直到用户解决触发问题。



11. 在“**摘要**”中，验证您是否按预期创建了自动化操作。



12. 配置操作详细信息后，您可以单独配置每个平台的部署规则。为此，请为您选择的每个平台完成步骤 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。

    例如：

    - 设备所有权必须是 **BYOD**。
    - 设备必须符合密码要求。
    - 设备移动国家/地区代码不能仅为安道尔。

14. 完成配置操作的平台部署规则后，单击**下一步**。此时将显示**操作分配**页面，您可以在其中将操作分配给一个或多个交付组。此步骤是可选的。
15. 在**选择交付组**旁边，键入以查找交付组或从列表中选择组。您选择的组将显示在**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**以安排部署，或单击**关**以阻止部署。默认选项设置为**开**。如果您选择**关**，则无需其他选项。
    - 在**部署计划**旁边，单击**立即**或**稍后**。默认选项设置为**立即**。
    - 如果您单击**稍后**，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**仅当上次部署失败时**。默认选项设置为**每次连接时**。
    - 在**为始终连接部署**旁边，单击**开**或**关**。默认选项设置为**关**。

此选项在您已在 **设置 > 服务器属性** 中配置计划后台部署密钥时适用。

> **注意：**
>
> 此选项在您已在 **设置 > 服务器属性** 中配置计划后台部署密钥时适用。
>
> 始终开启选项：
>
> - 不适用于 iOS 设备
> - 不适用于从版本 10.18.19 或更高版本开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户
> - 不建议从版本 10.18.19 之前开始使用 Citrix Endpoint Management 的 Android 和 Android Enterprise 客户使用

> 您配置的部署计划适用于所有平台。您所做的任何更改都适用于所有平台，但 **部署以实现始终开启连接** 除外。

17. 单击 **下一步**。此时将显示 **摘要** 页面，您可以在其中验证操作配置。
18. 单击 **保存** 以保存操作。

仅 MAM 模式下的应用程序锁定和应用程序擦除操作

您可以根据 Citrix Endpoint Management 控制台中列出的所有四类触发器（事件、设备属性、用户属性和已安装的应用程序名称）擦除或锁定设备上的应用程序。

配置自动应用程序擦除或应用程序锁定

1. 在 Citrix 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描述。
4. 在“**操作详细信息**”页面上，选择所需触发器。
5. 在“**操作**”中，选择一个操作。

   对于此步骤，请记住以下条件：

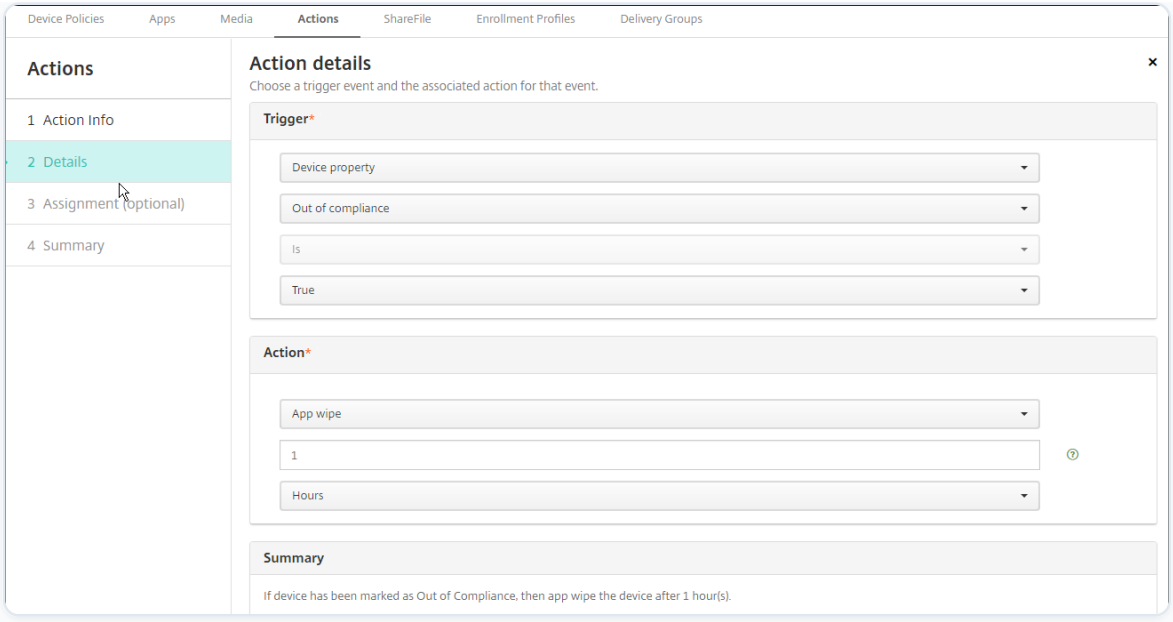
当触发器类型设置为“**事件**”且值不是“**Active Directory 禁用用户**”时，则不显示“**应用程序擦除**”和“**应用程序锁定**”操作。

当触发器类型设置为“**设备属性**”且值为“**MDM 丢失模式已启用**”时，则不显示以下操作：

- 选择性擦除设备
- 完全擦除设备
- 吊销设备

对于每个选项，系统都会自动设置 1 小时延迟，但您可以选择以分钟、小时或天为单位的延迟时间。延迟的目的是让用户在操作发生之前有时间解决问题。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：**
>
> 如果将触发器设置为“**事件**”，则重复间隔自动最短为 1 小时。设备必须刷新策略才能与服务器同步以接收通知。通常，设备会在用户登录或通过 Citrix Secure Hub 手动刷新其策略时与服务器同步。
>
> 在执行任何操作之前，可能会出现大约 1 小时的额外延迟，以允许 Active Directory 数据库与 Citrix 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. 点击 **保存**。

检查应用程序锁定或应用程序擦除状态

1. 转到 **管理 > 设备**，单击一个设备，然后单击 **显示更多**。

   管理设备屏幕(/en-us/citrix-endpoint-management/media/manage-devices-show-more.png)

2. 滚动到 **设备应用擦除** 和 **设备应用锁定**。

   管理设备屏幕(/en-us/citrix-endpoint-management/media/manage-devices-device-details.png)

   设备擦除后，系统会提示用户输入 PIN 码。如果用户忘记了该代码，您可以在“设备详细信息”中查找。

   管理设备屏幕(/en-us/citrix-endpoint-management/media/device-manage-macos-wipe-code.png)

在 Azure AD 中将 Windows 10 和 Windows 11 设备标记为不合规

当已加入 Azure AD 的 Windows 10 和 Windows 11 设备被 Citrix Endpoint Management 标记为不合规时，它们也可以在 Azure AD 中被标记为不合规。要启用此功能，请在 Azure AD 门户中向本地 MDM 应用程序添加权限以访问 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** 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** 以授予权限。

当运行 Windows 10 或 Windows 11 的 Azure AD 注册设备不合规时，Citrix Endpoint Management 也会在 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

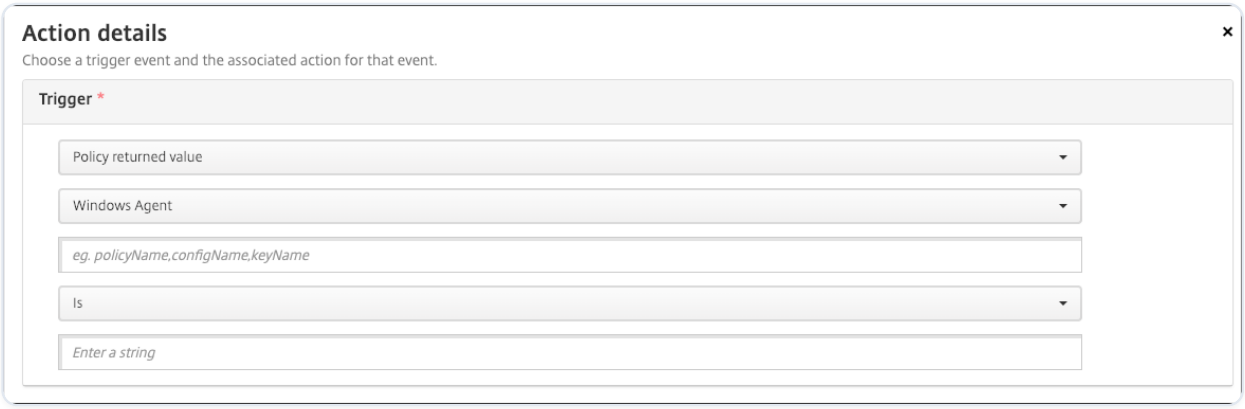
使用 Windows 代理设备策略部署脚本，以监视托管 Windows 桌面和平板电脑上的注册表值。根据脚本返回的值，您可以配置一个自动化操作来运行。

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。

   该文章和本节包含一个基于名为 `EntApp_2019_checkFirewall` 的脚本的示例。相关的 Windows 代理设备策略定义了一个名为 `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 代理设备策略中所述。

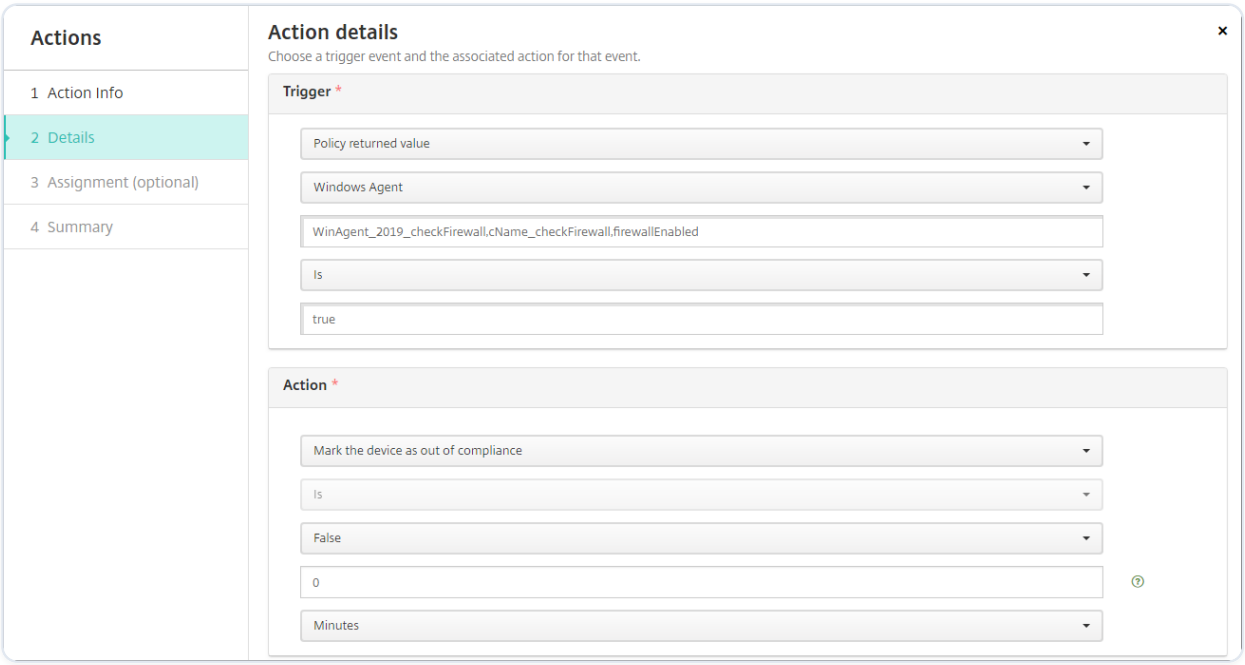
2. 在 Citrix Endpoint Management 控制台中，单击 **配置 > 操作**。
3. 在**操作**页面上，单击**添加**。
4. 在**操作信息**页面上，输入操作的名称和可选描述。
5. 在**操作详细信息**页面上，选择**策略返回值**触发器。



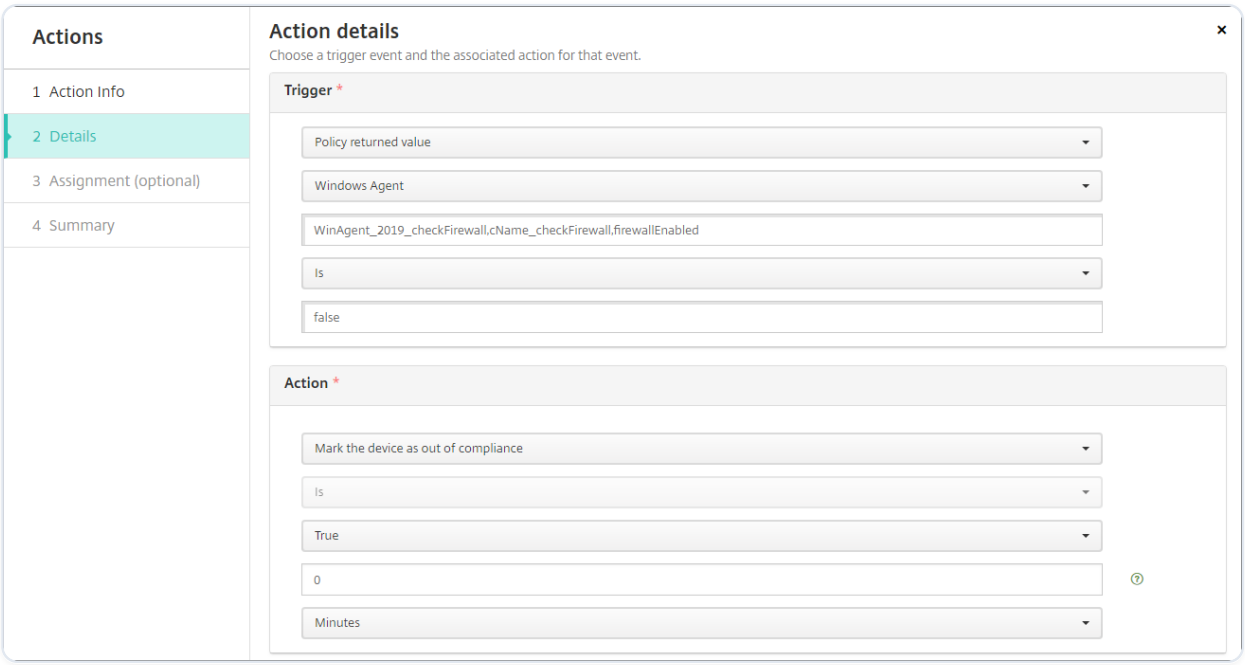
6. 在出现的字段中，定义触发器和操作：

   - **Windows 代理设置：** 输入您创建的 Windows 代理策略的策略名称、配置名称和密钥名称。
   - **下拉菜单：** 选择**是**、**不是**、**包含**或**不包含**逻辑。此逻辑适用于下一个字段，如果逻辑适用，则会触发操作。
   - **输入字符串：** 输入运行您策略中上传的 PowerShell 脚本后生成的字符串。有关查找该字符串的信息，请参阅Windows 代理设备策略。
   - **操作：** 选择一个操作、该操作的值，并选择解决该操作的时间范围。

   在我们的示例中：如果键名 `firewallEnabled` 返回值 `true`，以下操作会将设备标记为合规。



如果键名 `firewallEnabled` 返回值 `false`，以下操作会将设备标记为不合规。



7. 如有需要，设置部署计划并选择交付组。

监控和支持

您可以使用 Citrix Endpoint Management 控制板和 Citrix Endpoint Management 支持页面来监控和排查 Citrix Endpoint Management 服务器的故障。使用 Citrix Endpoint Management 支持页面可访问与支持相关的信息和工具。

在 Citrix Endpoint Management 控制台中，单击右上角的扳手图标。

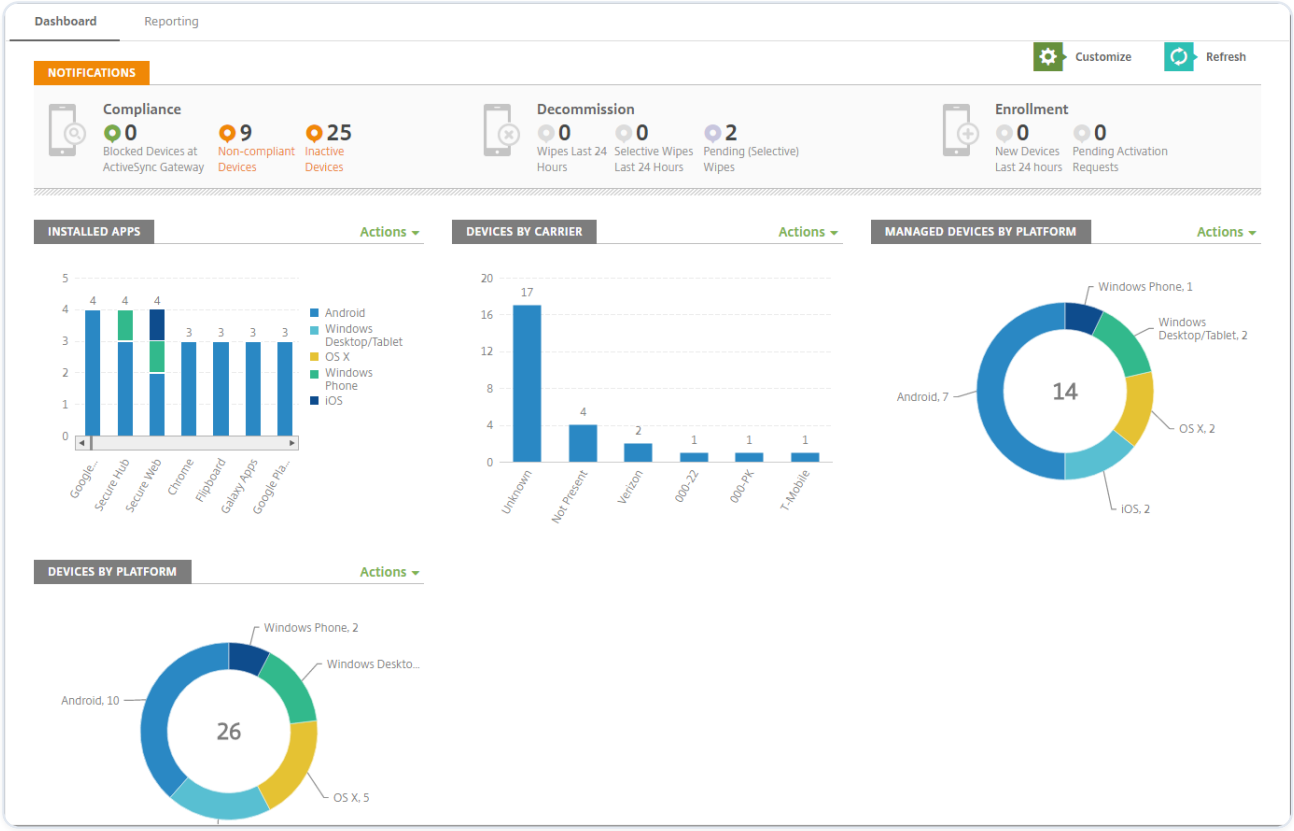


故障排除和支持页面随即显示。

使用 Citrix Endpoint Management **故障排除和支持**页面可执行以下操作：

- 访问诊断。
- 访问 Citrix 产品文档和知识中心链接。
- 访问日志操作。
- 使用高级配置选项。
- 访问一组工具和实用程序。

您还可以通过访问 Citrix Endpoint Management 控制台控制板来一目了然地查看信息。借助此信息，您可以使用小组件快速查看问题和成功。

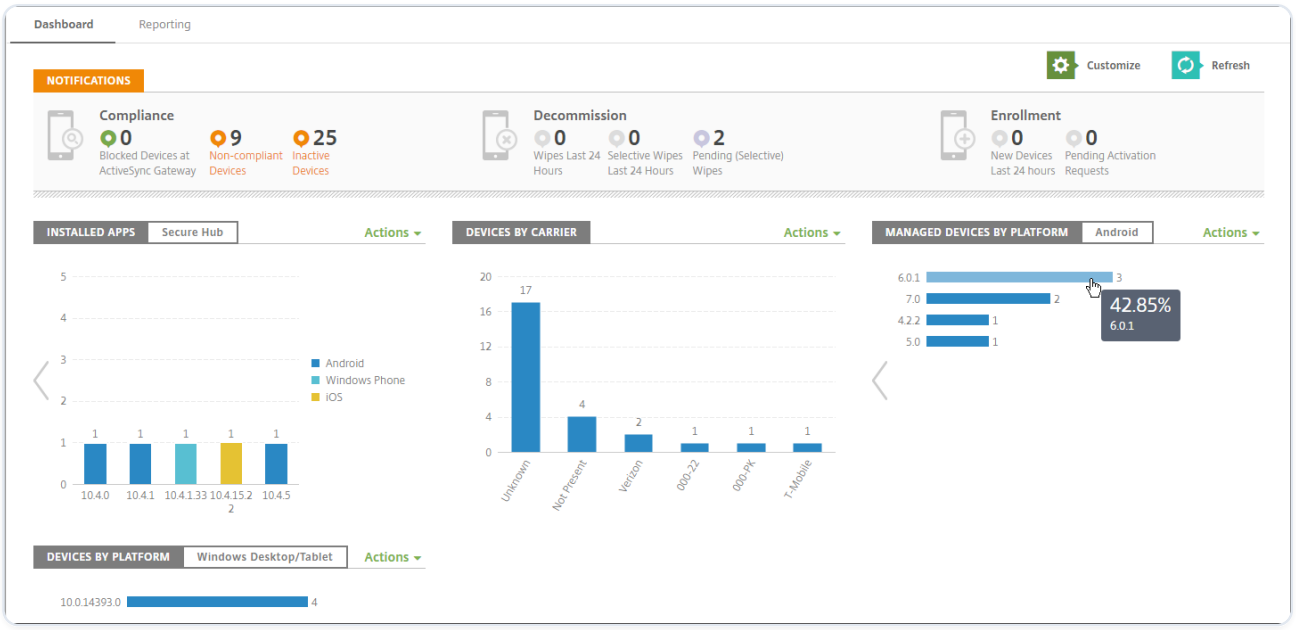


控制板通常是您登录 Citrix Endpoint Management 控制台时首先出现的页面。要从控制台的其他位置访问控制板，请单击**分析**。在控制板上单击**自定义**可编辑页面布局和显示的小组件。

- **我的控制板：** 您最多可以保存四个控制板。您可以单独编辑这些控制板，并通过选择已保存的控制板来查看每个控制板。
- **布局样式：** 在此行中，您可以选择仪表板上显示的微件数量以及微件的布局方式。
- **微件选择：** 您可以选择要在仪表板上显示的信息。
    - **通知：** 勾选左侧数字上方的复选框，可在微件上方添加一个通知栏。此栏显示合规设备、非活动设备以及在过去 24 小时内擦除或注册的设备数量。
    - **按平台划分的设备：** 按平台显示托管和非托管设备的数量。
    - **按运营商划分的设备：** 按运营商显示托管和非托管设备的数量。单击每个条形图可按平台查看详细信息。
    - **按平台划分的托管设备：** 按平台显示托管设备的数量。
    - **按平台划分的非托管设备：** 按平台显示非托管设备的数量。此图表中显示的设备可能已安装代理，但其权限已被撤销或设备已被擦除。
    - **按 ActiveSync 网关状态划分的设备：** 显示按 ActiveSync 网关状态分组的设备数量。信息显示“已阻止”、“已允许”或“未知”状态。您可以单击每个条形图按平台细分数据。
    - **按所有权划分的设备：** 显示按所有权状态分组的设备数量。信息显示公司所有、员工所有或未知所有权状态。

- **失败的交付组部署：** 显示每个软件包的失败部署总数。仅显示有失败部署的软件包。
- **按阻止原因划分的设备：** 显示 ActiveSync 阻止的设备数量
- **已安装的应用：** 输入应用名称以获取应用信息图表。
- **批量采购应用许可证使用情况：** 显示 Apple 批量采购应用的许可证使用统计信息。

对于每个微件，您可以单击各个部分以深入了解更多信息。



您还可以通过单击“**操作**”菜单将信息导出为 .csv 文件。

分析仪表板菜单(/en-us/citrix-endpoint-management/media/analyze-dashboard-actions-menu.png)

帮助台管理员的“监视”页面

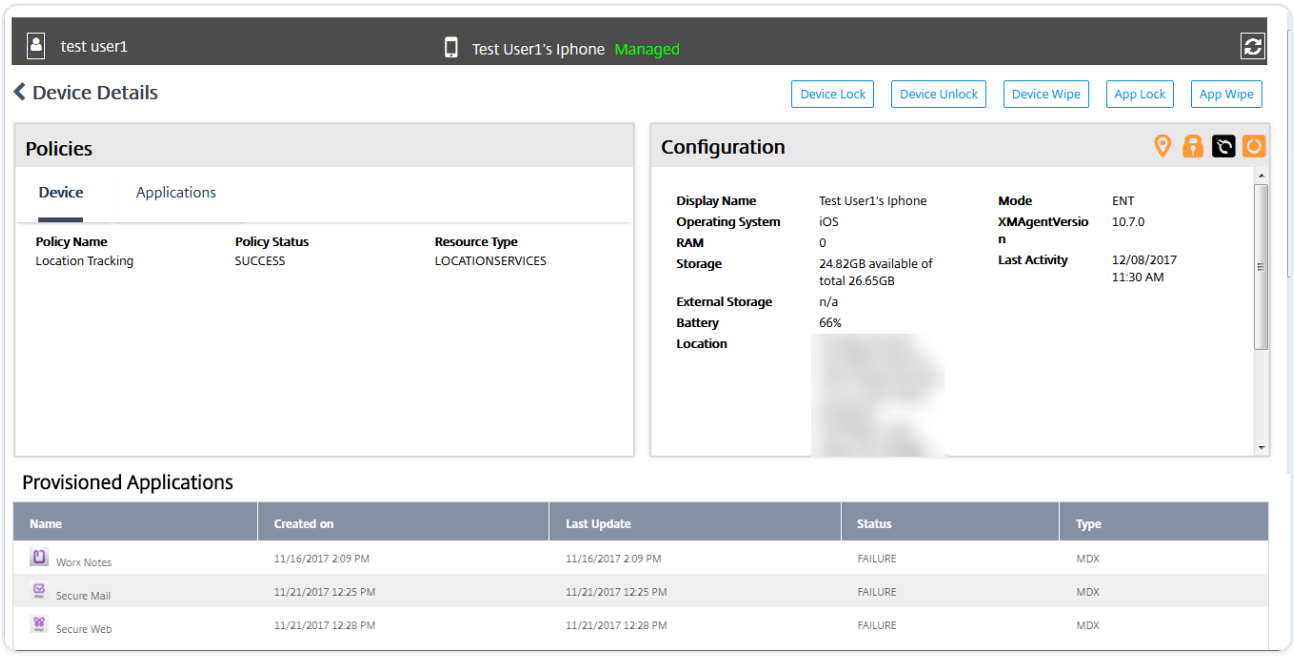
您可以在“**监视**”页面上监视和排查 Citrix Endpoint Management。此界面专为帮助台管理员定制，可高效执行基于用户的故障排除。

帮助台管理员必须具有以下权限才能访问“**监视**”页面和所有可用工作流：

- 授权访问
  - 管理控制台访问
  - 公共 API 访问
- 控制台功能
  - 监控
  - 设备

- 完全擦除设备
- 查看位置
  - 定位设备
  - 跟踪设备
- 锁定设备
- 解锁设备
- 应用程序锁定
- 应用擦除
- 应用

监视页面为您提供了设备策略和配置的组合视图。该视图包括故障排除操作，例如应用锁定/解锁、应用擦除、设备锁定/解锁和设备擦除。



使用**监视**页面可执行以下操作：

- 搜索要进行故障排除的 Active Directory (AD) 用户和设备。
- 分析**设备详细信息**页面，其中包含以下内容：
  - **策略：**显示所选设备和应用的设备和应用策略。有关修改策略的信息，请参阅设备策略和添加应用。
  - **配置：**显示设备配置。此面板包含指示设备是否启用了位置服务、是否已越狱以及是否由 MDM 或 MAM 管理的图标。此面板还显示存储加密状态。
  - **正在运行的应用**表：显示设备上当前正在运行的应用的详细信息。

- 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登录管理员可用的权限：
    - 设备锁定/解锁
    - 设备擦除
    - 应用锁定/解锁（如果设备已注册 MAM，则可用）
    - 应用擦除（如果设备已注册 MAM，则可用）

有关您可以执行的操作的更多信息，请参阅安全操作。

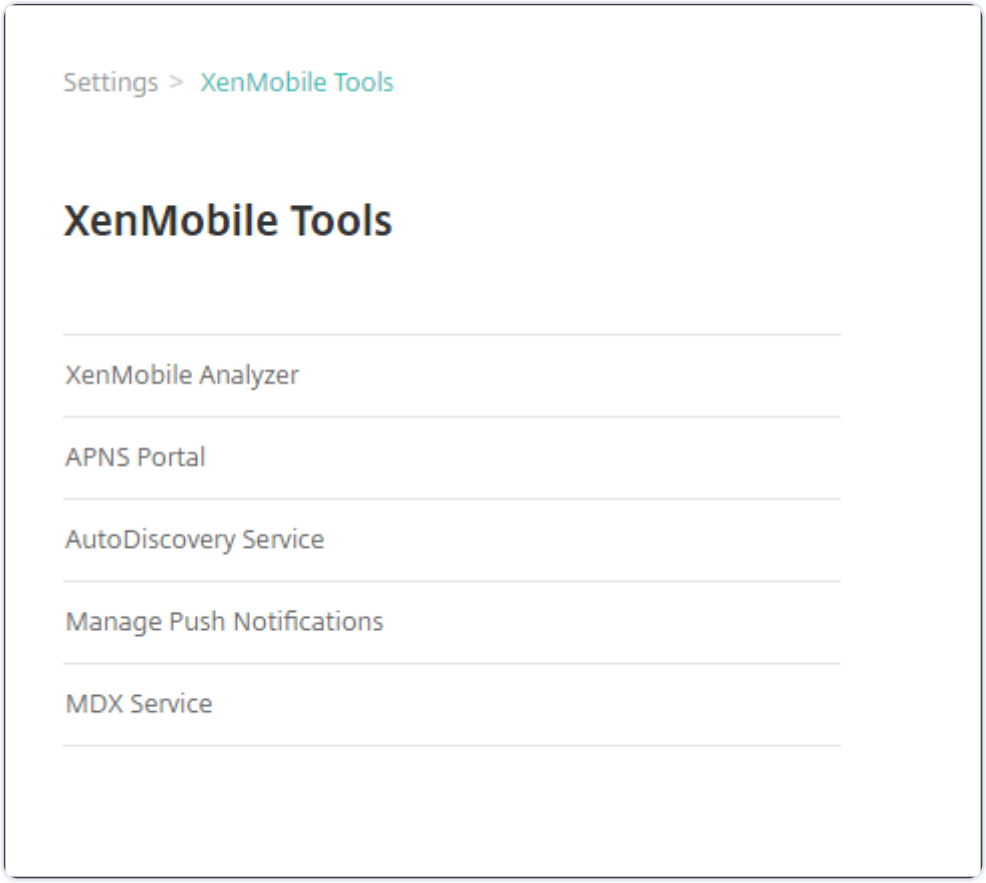
“监视”页面在上次加载后 60 分钟可能无法按预期运行，因为它不处理登录令牌的刷新。作为一种解决方法，请通过重新加载页面来刷新令牌：单击服务控制台上的 **Citrix Cloud** 链接，然后单击 **Citrix Endpoint Management > 管理 > 监视**。

从控制台访问 Citrix Endpoint Management 工具

您可以从 Citrix Endpoint Management 控制台访问以下 Citrix Endpoint Management 工具：

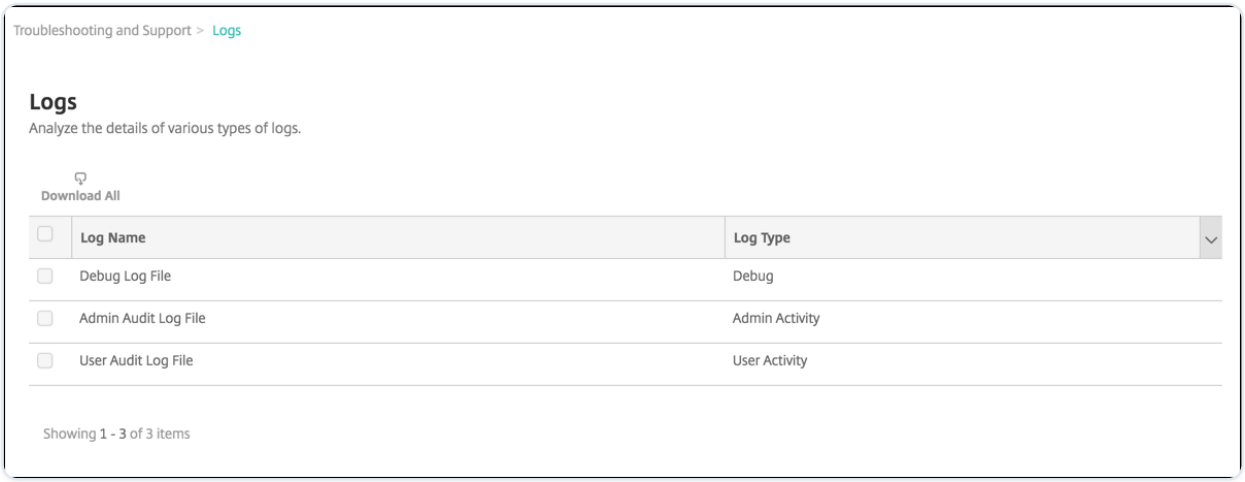
- **APNs 门户** – 向 Citrix 提交请求以签署 APNs 证书，然后将其提交给 Apple。
- **自动发现服务** – 在您的域中请求并配置 Citrix Endpoint Management 的自动发现。
- **管理推送通知** – 管理 iOS 和 Windows 移动应用的推送通知。

要访问这些工具，请转至 **设置 > Citrix Endpoint Management 工具**。此页面适用于具有云管理员或客户管理员角色的用户。



在 Citrix Endpoint Management 中查看和分析日志文件

1. 在 Citrix 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，单击“**日志**”。此时将显示“**日志**”页面。各个日志将显示在一个表中。

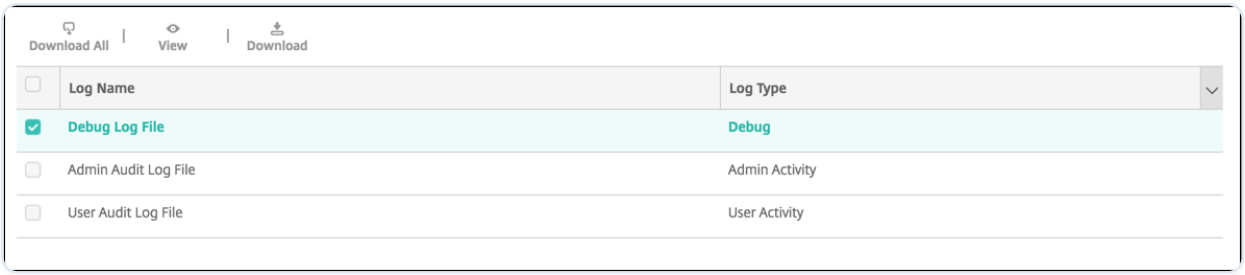


3. 选择要查看的日志：

   - 调试日志文件包含对 Citrix 支持有用的信息，例如错误消息和服务器相关操作。
   - 管理员审计日志文件包含有关 Citrix Endpoint Management 控制台活动的审计信息。

- 用户审计日志文件包含与已配置用户相关的信息。

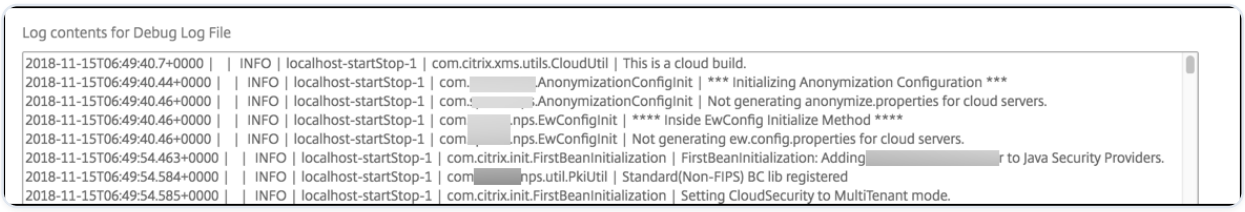
4. 使用表格顶部的操作来下载所有日志、查看日志或下载单个日志。



> **注意：**
>
> 如果您选择多个日志文件，则只有“**下载所有**”可用。

5. 执行以下操作之一：

- **下载所有：** 控制台下载系统中存在的所有日志（包括调试、管理员审计、用户审计、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。控制台还会下载该相同类型的所有存档日志。



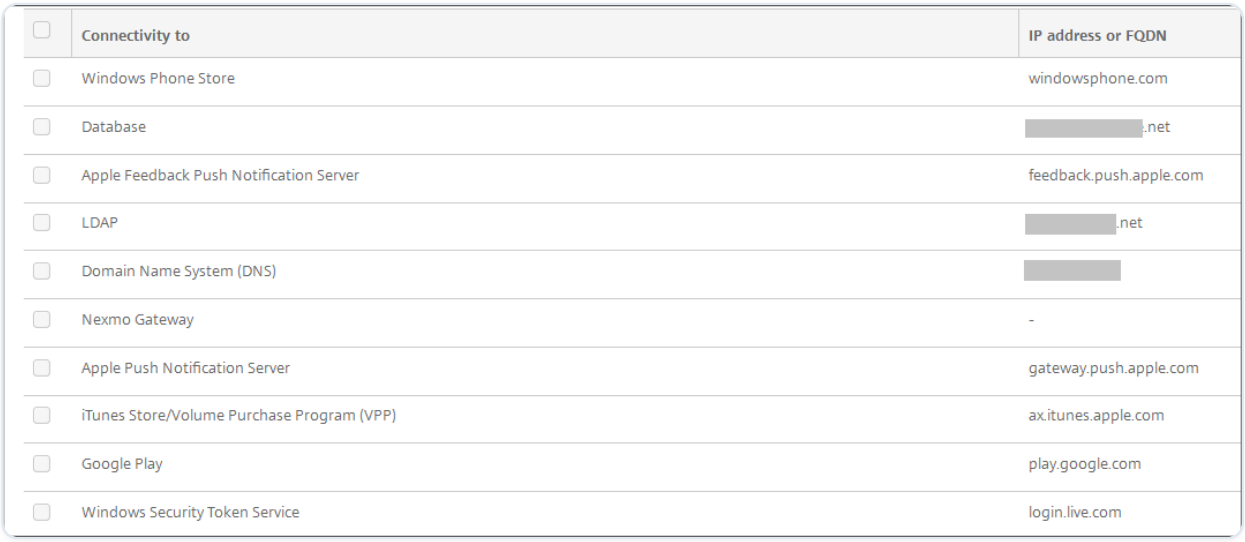
Citrix Endpoint Management 使用 log4j syslog appender 发送 RFC5424 格式的 syslog 消息。syslog 消息数据是纯文本，没有特定格式。

连接性检查

在 Citrix Endpoint Management 的“**故障排除和支持**”页面上，您可以检查 Citrix Endpoint Management 与 NetScaler Gateway 以及其他服务器和位置的连接。要运行 Citrix Endpoint Management 连接性检查，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。有关分配角色的详细信息，请参阅使用 RBAC 配置角色。

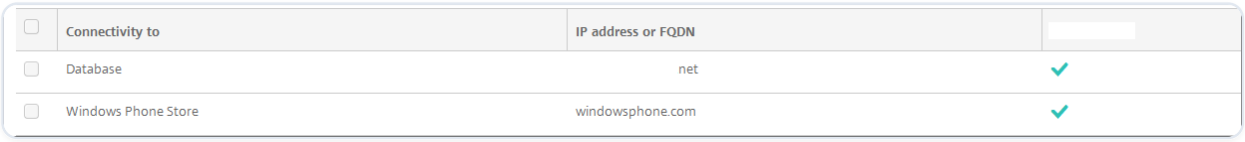
运行 Citrix Endpoint Management 连接性检查

1. 在 Citrix 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“**Citrix Endpoint Management 连接性检查**”。此时将显示“**Citrix Endpoint Management 连接性检查**”页面。如果您的 Citrix Endpoint Management 环境具有群集节点，则会显示所有节点。



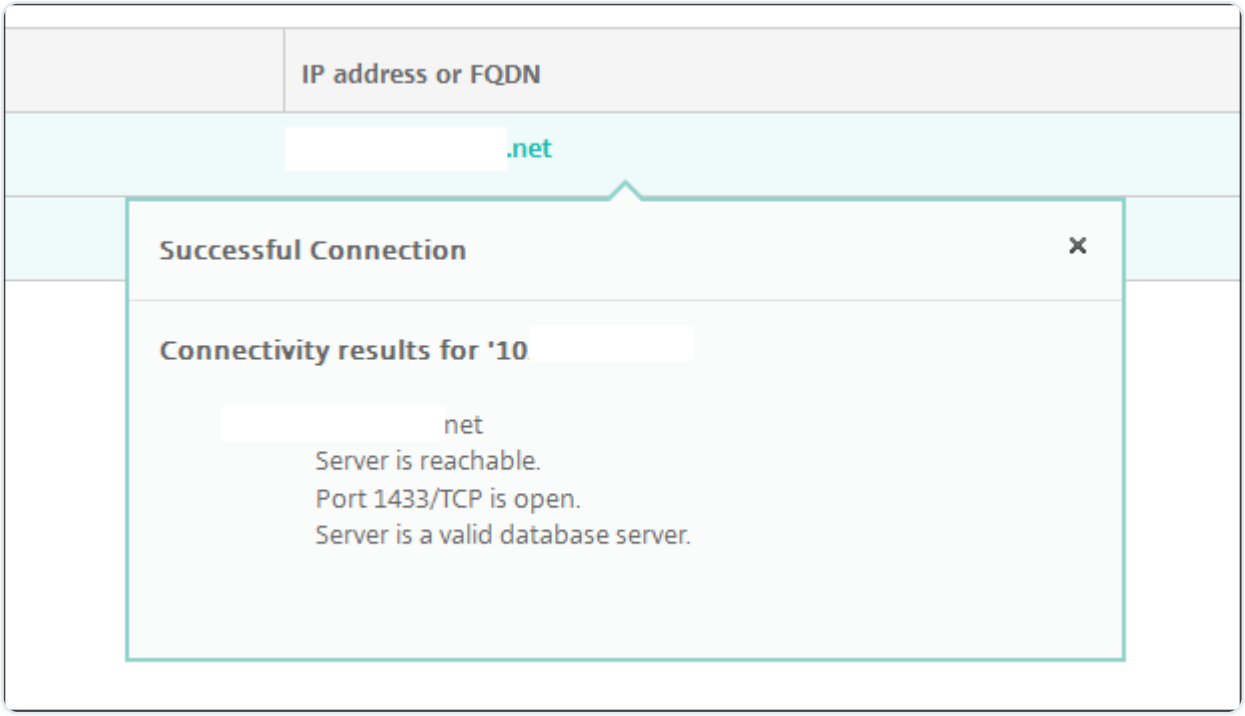
Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	[redacted].net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	[redacted].net
Domain Name System (DNS)	[redacted]
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

3. 选择要包含在连接性测试中的服务器，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	✓

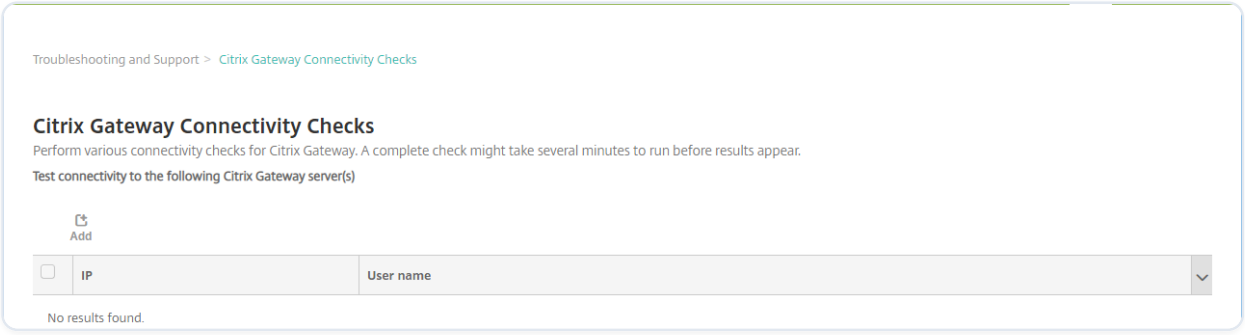
4. 在测试结果表中选择一个服务器，以查看该服务器的详细结果。



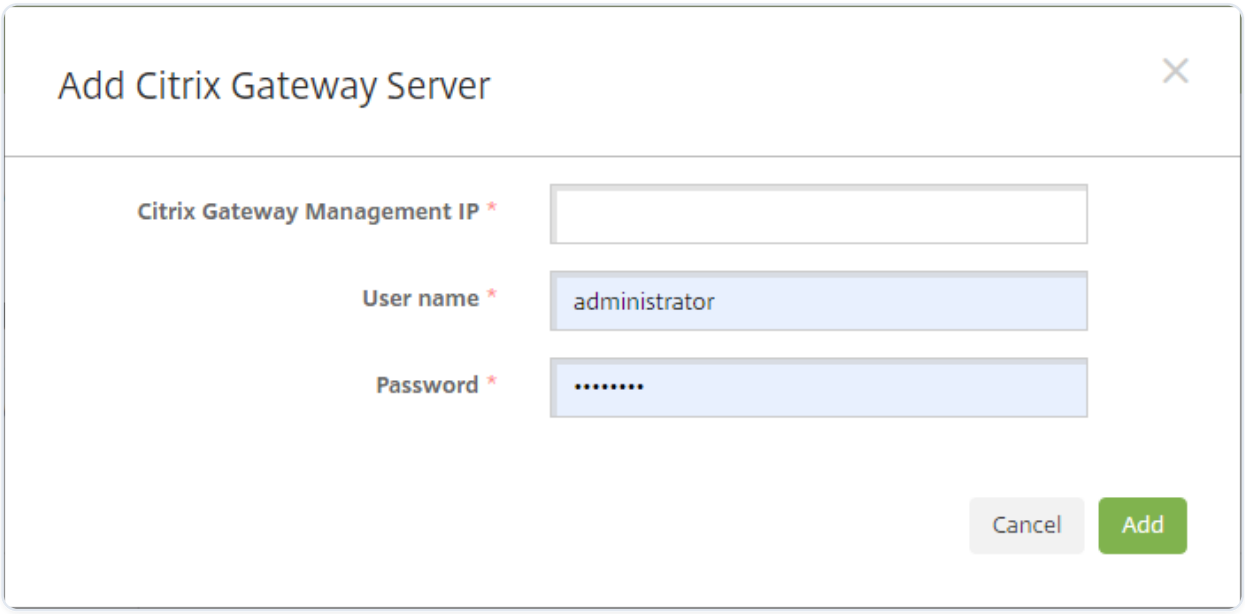
有关 Citrix Endpoint Management 可以执行的连接性检查及其详细信息的更多信息，请参阅连接性检查详细信息。

执行 NetScaler Gateway 连接性检查

1. 在“**故障排除和支持**”页面上，在“**诊断**”下，单击“**NetScaler Gateway 连接性检查**”。此时将显示“**NetScaler Gateway 连接性检查**”页面。如果 Citrix Endpoint Management 与 NetScaler Gateway 之间没有连接，则该表为空。



2. 单击“**添加**”。此时将显示“**添加 NetScaler Gateway 服务器**”对话框。



3. 在 **NetScaler Gateway 管理 IP** 中，键入要测试的运行 NetScaler Gateway 的服务器的管理 IP 地址。

   如果您正在对之前已添加的 NetScaler Gateway 服务器执行连接检查，则会提供 IP 地址。

4. 键入此 NetScaler Gateway 的管理员凭据。

   如果您正在对之前已添加的 NetScaler Gateway 服务器执行连接检查，则会提供用户名。

5. 单击 **添加**。NetScaler Gateway 将添加到 **NetScaler Gateway 连接检查** 页面上的表中。
6. 选择 NetScaler Gateway 服务器，然后单击 **测试连接**。结果将显示在测试结果表中。

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 Citrix Endpoint Management 可以执行的各种连接检查，并包含每个检查的详细信息。

连接到	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 Citrix Endpoint Management 节点之间的连接。Apple 推送通知服务器是向 iOS 和 macOS 设备发送消息所必需的。
Apple 反馈推送通知服务器	feedback.push.apple.com	检查 Apple 反馈服务器与 Citrix Endpoint Management 节点之间的连接。Apple 反馈推送通知服务器提供有关发送到 iOS 和 macOS 设备的失败远程通知的信息。
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 Citrix Endpoint Management 节点之间的连接。运行 Citrix 产品的服务器会联系 Citrix 许可证服务器以获取许可证。
NetScaler 网关	在 Citrix Endpoint Management 中配置的 NetScaler Gateway 的 FQDN	检查 NetScaler Gateway 与 Citrix Endpoint Management 节点之间的连接。Citrix Endpoint Management 客户端应用程序（例如 Citrix Secure Mail 和 Citrix Secure Web）使用 NetScaler Gateway 通过 VPN 服务器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 Citrix Endpoint Management 数据库与 Citrix Endpoint Management 节点之间的连接。

连接到	IP 地址或 FQDN	详细信息
域名系统 (DNS)	在 Citrix Endpoint Management 中配置的 IP 地址	检查 DNS 服务器与 Citrix Endpoint Management 节点之间的连接。
安全票证颁发机构服务	本地主机	检查 Citrix Endpoint Management 节点与身份验证服务、STA（安全票证颁发机构）服务和群集服务的连接。
Firebase 云消息传递 (FCM) 服务器		检查 FCM 服务器与 Citrix 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的电子邮件或其他数据可供同步。您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) 的替代方案。
谷歌应用商店	play.google.com	检查 Google 商店服务器与 Citrix Endpoint Management 节点之间的连接。Google Play 用于提供服务，其中包括托管的私有企业应用程序分发商店。
iTunes Store/批量采购	vpp.itunes.apple.com	检查 Apple Store 服务器与 Citrix Endpoint Management 节点之间的连接。Apple Store 用于提供服务，其中包括托管的私有企业应用程序分发商店。
LDAP	在 Citrix Endpoint Management 中配置的 LDAP 的 IP 地址或 FQDN	检查 LDAP 服务器与 Citrix 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 Citrix Endpoint Management 节点之间的连接。Windows

连接到	IP 地址或 FQDN	详细信息
		通知服务器用于向 Windows 设备发送消息。
ShareFile 服务	在 Citrix Endpoint Management 中配置的 ShareFile 服务的 IP 地址或 FQDN	检查 ShareFile 服务与 Citrix Endpoint Management 之间的连接。ShareFile 服务是一个安全的云平台，供企业存储和共享大型文件。
视窗桌面/平板电脑商店	windows.microsoft.com	检查 Windows 桌面/平板电脑商店与 Citrix Endpoint Management 节点之间的连接。Windows 桌面/平板电脑商店用于提供服务，其中包括托管的私有企业应用交付商店。
Windows 安全令牌服务	login.live.com	检查 Windows 安全令牌服务器与 Citrix Endpoint Management 节点之间的连接。Windows 安全令牌服务支持 Windows 设备的双因素身份验证（域加安全令牌）。

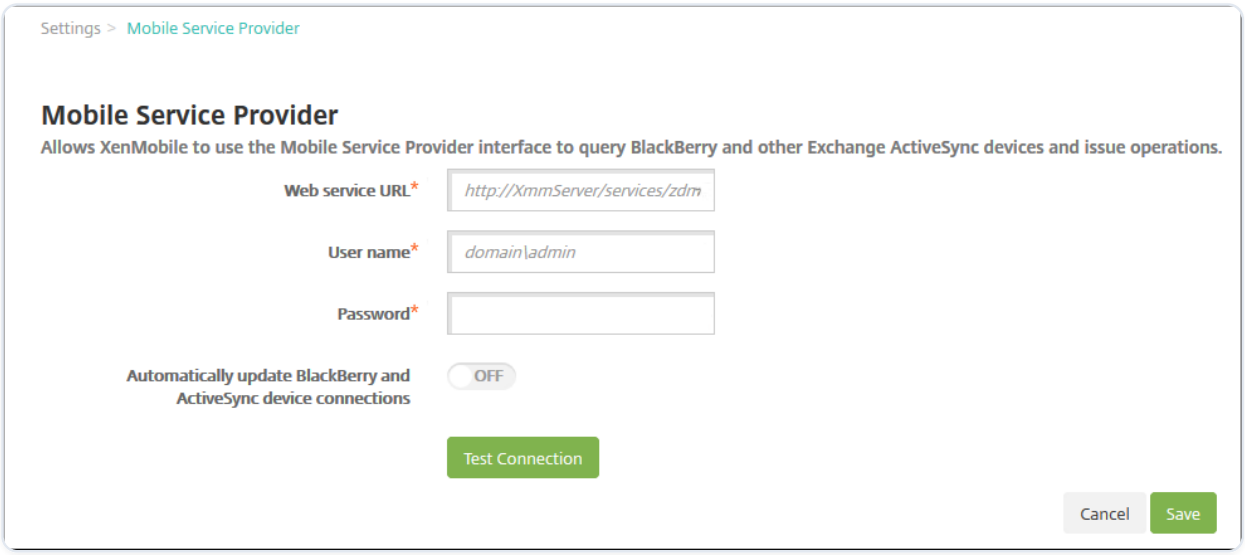
移动服务提供商

您可以启用 Citrix Endpoint Management 使用移动服务提供商界面来查询 BlackBerry 和 Exchange ActiveSync 设备并执行操作。

例如，假设您的组织有 1,000 名用户，并且每位用户使用一台或多台设备。在您指示所有用户将其设备注册到 Citrix Endpoint Management 后，Citrix Endpoint Management 控制台会显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。通过这种方式，您可以执行以下操作：

- 确定是否有任何用户仍需注册其设备。
- 向连接到 Exchange Server 的用户设备发出命令，例如数据擦除。

1. 在 Citrix 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，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：** 键入格式为 `domain\\admin` 的用户名。
   - **密码：** 键入密码。
   - **自动更新 BlackBerry 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。

4. 点击 **保存**。

报告

Citrix Endpoint Management 提供以下预定义报告，可用于分析您的应用程序和设备部署。每个报告都以表格和图表的形式显示。您可以按列对表格进行排序和筛选。您可以从图表中选择元素以获取更详细的信息。

- **应用程序部署尝试总数：** 列出用户尝试在其设备上安装的已部署应用程序。
- **按平台列出的应用程序：** 按设备平台和版本列出应用程序和应用程序版本。
- **按类型列出的应用程序：** 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。
- **非活动设备：** 列出在 Citrix 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。

- **越狱/Root 设备：** 列出已越狱的 iOS 设备和已 Root 的 Android 设备。
- **条款和条件：** 列出已接受和拒绝条款和条件协议的用户。您可以选择图表区域以查看更多详细信息。
- **前 10 个失败的部署：** 列出最多 10 个部署失败的应用程序。
- **按设备和用户列出的已阻止应用程序：** 列出用户设备上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。标准包括设备是否已越狱、正在运行的操作系统版本以及设备是否具有密码。报告还会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，加密列显示“不适用”。

您可以将每个表格中的数据导出为 .csv 格式，该格式可在 Microsoft Excel 等程序中打开。每个报告的图表可以导出为 PDF 格式。

“**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。要获取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，请参阅获取设备信息。

以下方面决定了 Citrix Endpoint Management 如何收集有关部署到托管设备或安装在托管设备上的应用程序的信息：

- 设备类型
- 注册方法
- 是否已部署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。下表指明了 **Android Enterprise** 的应用程序列表位置（**设备详细信息**页面、报告或不可用）。除非另有说明，否则应用程序列表包含所有应用程序。

	MDM+MAM（所有应用程序）	MDM（所有应用程序）
所需应用程序（应用程序清单策略未部署）	**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（应用程序清单策略未部署）	不可用	不可用
所需应用程序（应用程序清单策略已部署）	**设备详细信息**页面和报告	**设备详细信息**页面和报告

	MDM+MAM（所有应用程序）	MDM（所有应用程序）
可选应用（应用清单策略已部署）	企业、MDX、公共和 Web 链接应用；报告	**设备详细信息**页面和报告

下表指示了应用在何处列出，适用于 **Android（旧版设备管理员）**（**设备详细信息**页面、报告或不可用）。应用列表包含所有应用，除非另有说明。

	MDM+MAM（所有应用）	MDM（公共应用和企业应用）	MAM
必需应用（应用清单策略未部署）	**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（应用清单策略未部署）	**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
必需应用（应用清单策略已部署）	**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。下表指示应用程序的列出位置（**设备详细信息**页面或报告）。除非另有说明，否则应用程序列表包含所有应用程序。

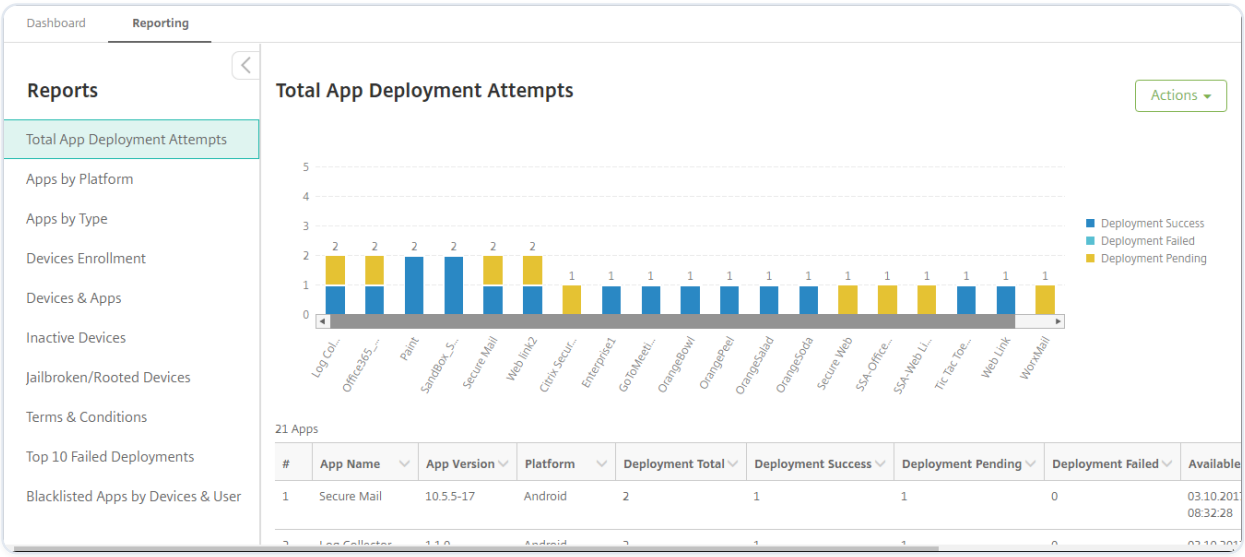
	MDM+MAM（所有应用程序）	MDM（公共和企业应用程序）	MAM（所有应用程序）
所需应用程序（未部署应用程序清单策略）	**设备详细信息**页面和报告	**设备详细信息**页面和报告	**设备详细信息**页面和报告。这些应用程序显示为挂起状态（即使未安装），或者在手动安装后仍保持挂起状态。
可选应用程序（未部署应用程序清单策略）	**设备详细信息**页面和报告	**设备详细信息**页面和报告	Web、SaaS 和 Web 链接应用程序在**设备详细信息**页面上列为已安装应用程序。它们未在报告中列出。

	MDM+MAM（所有应用程序）	MDM（公共和企业应用程序）	MAM（所有应用程序）
			企业、MDX 和公共应用程序在手动安装后不会在**设备详细信息**页面上列出。应用程序在手动安装后不会在报告中列出。
所需应用程序（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	应用程序清单策略无法部署到设备。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待定状态（即使未安装），或者在手动安装后仍处于待定状态。
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	应用程序清单策略无法部署到设备。Web、SaaS 和 Web 链接应用程序在**设备详细信息**页面上列为已安装应用程序。它们未在报告中列出。企业、MDX 和公共应用程序在手动安装后不会在**设备详细信息**页面上列出。应用程序在手动安装后不会在报告中列出。

对于 macOS 和 Windows 设备，Citrix Endpoint Management *仅在*部署应用程序清单策略时才收集应用程序清单。

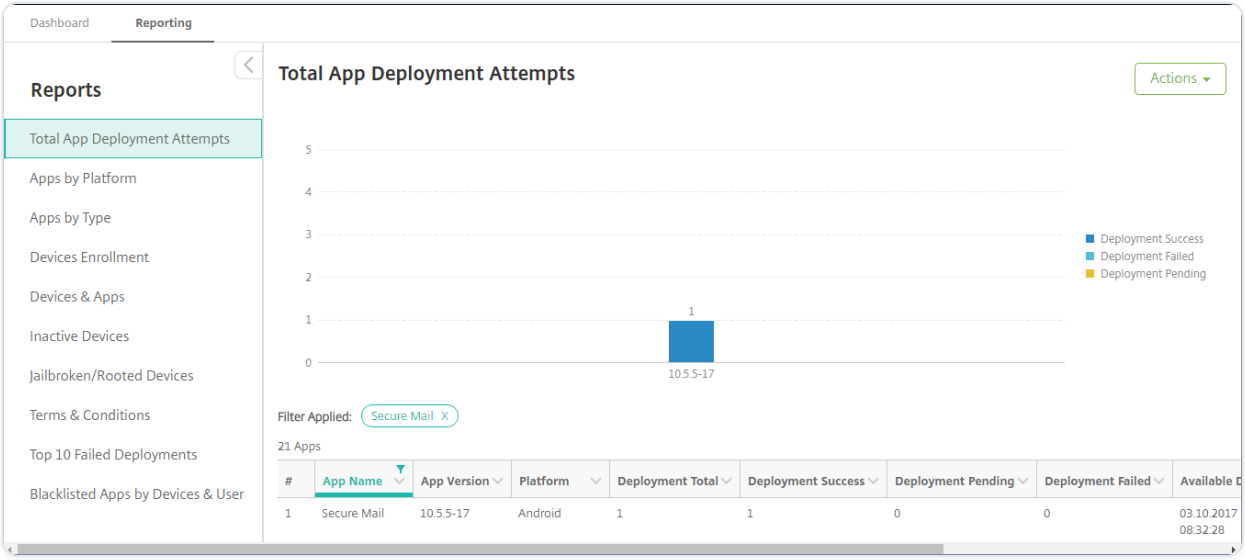
生成报告

1. 在 Citrix 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。

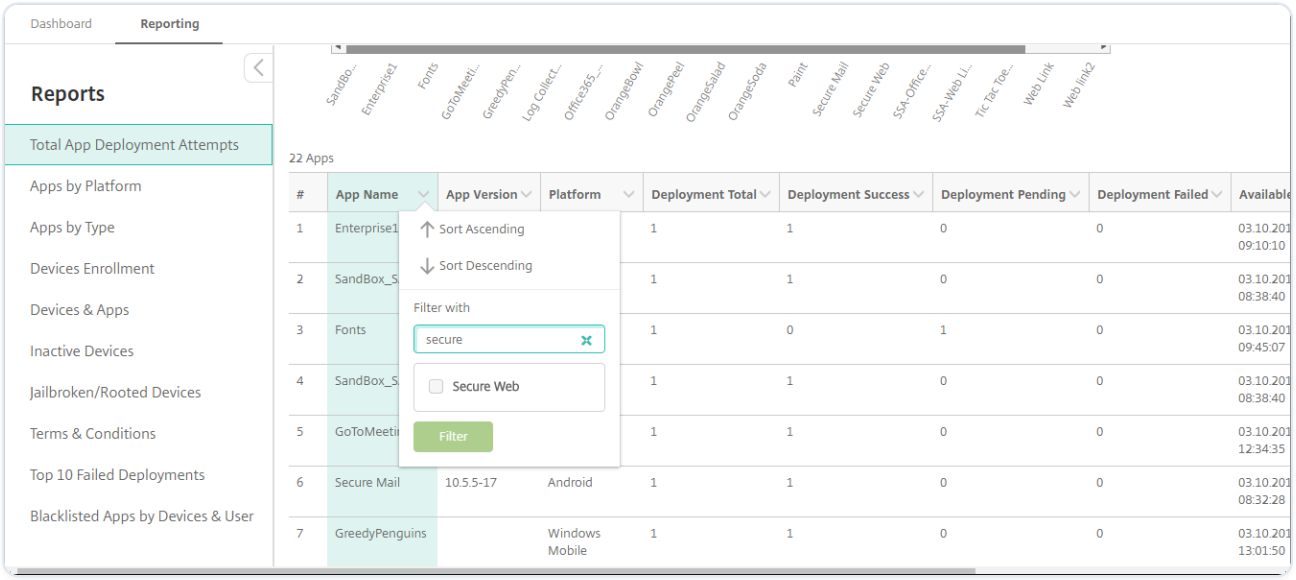


查看报告的更多详细信息

1. 单击图表区域以向下钻取并查看更详细的信息。

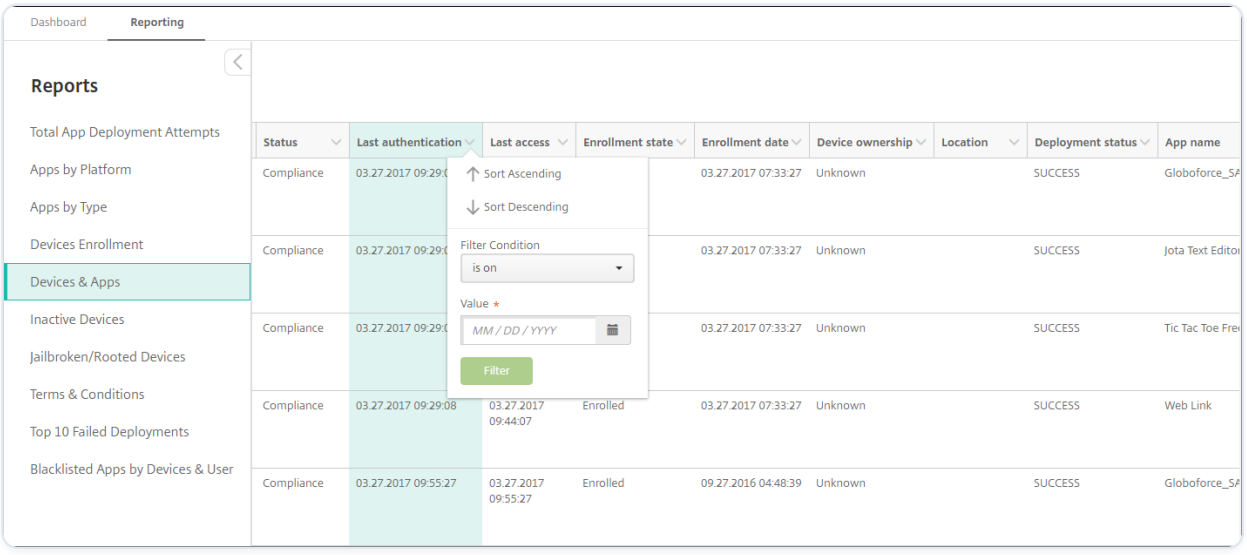


要对表列进行排序、筛选或搜索，请单击列标题

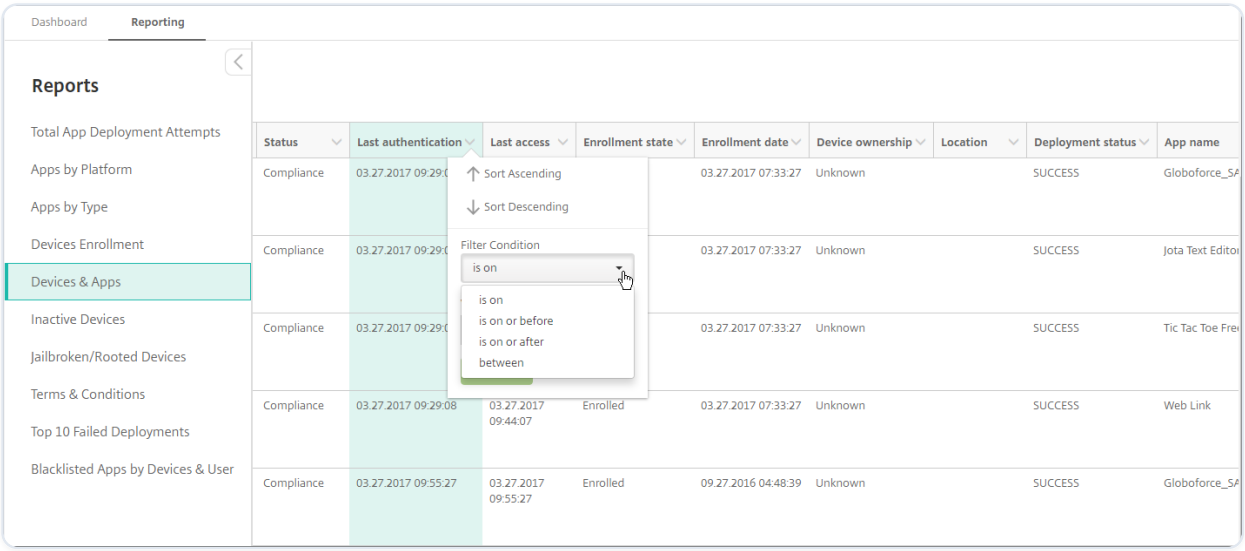


按日期筛选报告

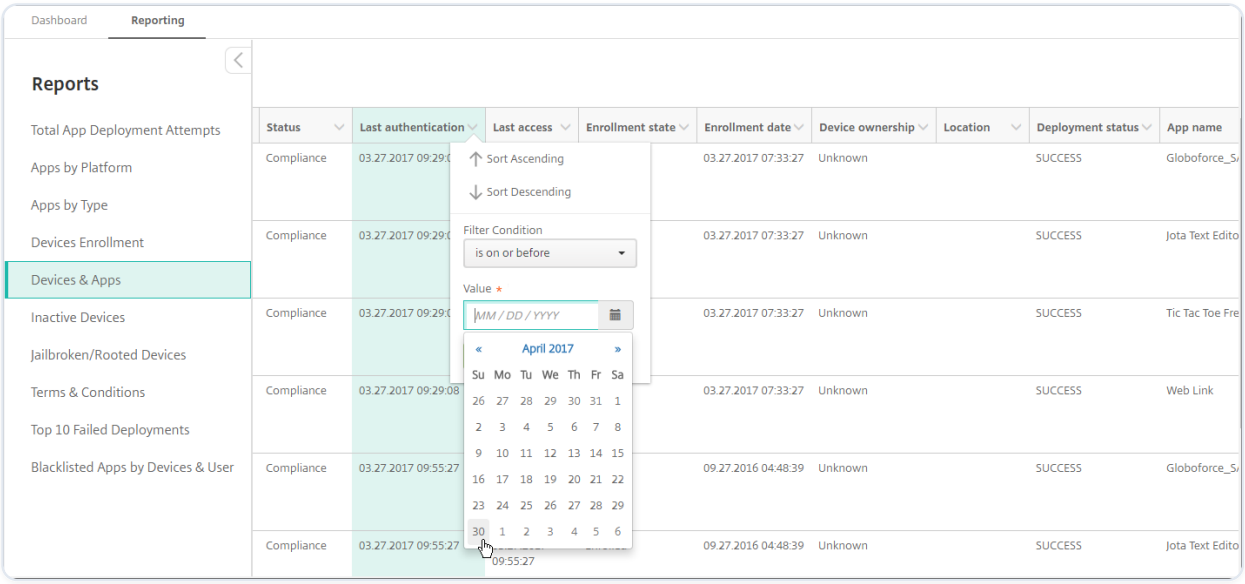
1. 单击列标题以查看筛选器设置。



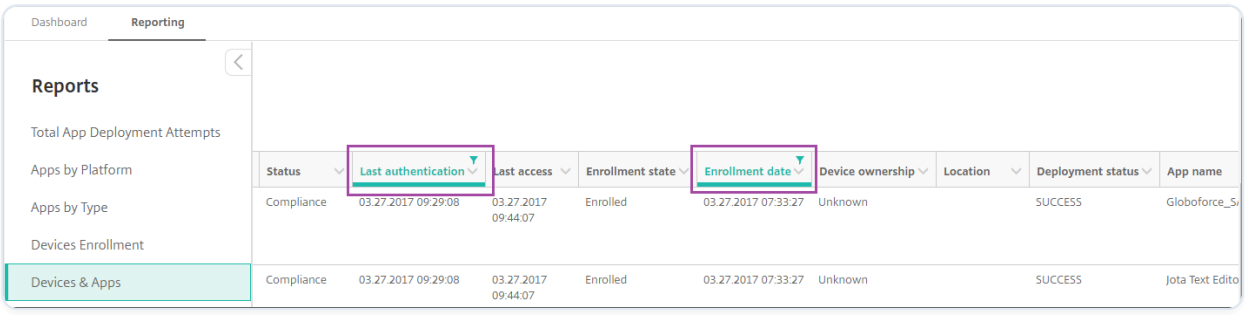
2. 在“**筛选条件**”中，选择您希望如何限制报告的日期。



3. 使用日期选择器指定日期。



4. 带有日期筛选器的列显示方式如下例所示。



5. 要移除筛选器，请单击列标题，然后单击**移除筛选器**

移除筛选器(/en-us/citrix-endpoint-management/media/analyze-reporting-date-filter-remove.png)

导出图表或表格

- 要以 PDF 格式导出图表，请单击**操作**，然后单击**将图表导出为 PDF**。
- 要以 CSV 格式导出表格数据，请单击**操作**，然后单击**将数据导出为 CVS**。

导出图表或表格(/en-us/citrix-endpoint-management/media/reporting-export-snip.png)

REST API

借助 Citrix Endpoint Management REST API，您可以：

- 调用在 Citrix Endpoint Management 控制台中显示的服务
- 使用任何 REST 客户端调用 REST 服务

API 不需要您登录 Citrix Endpoint Management 控制台即可调用服务。

有关可用 API 的完整当前集，请下载 Public API for REST Services PDF。

可以使用 API 来管理您的移动和桌面端点设备，并为您的 Workspace 应用程序配置设置。转至 `<https://developer.cloud.com/citrixworkspace>` 并导航到 **Citrix Endpoint Management > Mobile Application Integration**。

访问 REST API 所需的权限

访问 REST API 需要以下权限之一：

- Citrix Cloud 管理员
- 作为基于角色的访问配置的一部分设置的公共 API 访问权限。有关信息，请参阅 Configuring roles with RBAC。
- 超级用户权限

要使用您的 Citrix Cloud 帐户访问 REST API，请生成 **API** 密钥：

1. 在 Citrix Cloud 菜单中，选择 **身份和访问管理**。
2. 选择 **API 访问 > 安全客户端**。
3. 为您的安全客户端输入一个名称，然后点击**创建客户端**。

Citrix Cloud 随后会创建安全客户端 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 不会存储这些唯一标识符。

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 Advanced REST 客户端。

> **注意：**
>
> 在以下示例中，请更改主机名和端口号以匹配您的环境。

登录

此处显示的示例涵盖了使用通过 Citrix Cloud API 检索到的令牌进行登录。

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

方法类型: POST

内容类型: application/json

请求示例:

```
{

 "bearerToken":
"eyJ0eOiJSUzJiibGcI1AiONiJ9.eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"

}
```

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"

}
```

相关信息

- Citrix 端点管理 REST API

限制电子邮件访问

ActiveSync 网关

ActiveSync 是 Microsoft 开发的一种移动数据同步协议。ActiveSync 可将数据与手持设备和台式机（或笔记本电脑）同步。

您可以在 Citrix Endpoint Management 中配置 ActiveSync 网关规则。ActiveSync 网关会维护 Citrix Endpoint Management 中配置的所有设备的 ActiveSync ID 列表。根据您配置的规则，您可以基于这些 ActiveSync ID 允许或拒绝设备访问 ActiveSync 数据。例如，如果您激活**缺少所需应用程序**规则，Citrix Endpoint Management 会检查应用程序访问策略中所需的应用程序。如果缺少所需的应用程序，该策略会拒绝访问 ActiveSync 数据。对于每条规则，您可以选择**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。

Citrix Endpoint Management 支持以下规则：

匿名设备： 检查设备是否处于匿名模式。当设备尝试重新连接时，如果 Citrix Endpoint Management 无法重新验证用户身份，则此检查可用。

禁用应用程序： 检查设备是否有禁用应用程序，如应用程序访问策略中所定义。

隐式允许和拒绝： 此操作是 ActiveSync 网关的默认设置。网关会创建不符合任何其他筛选规则条件的所有设备的设备列表。然后，网关根据该列表允许或拒绝连接。如果没有规则匹配，则默认设置为**隐式允许**。

非活动设备： 检查设备是否处于非活动状态，具体由**服务器属性**中的**设备非活动天数阈值**设置定义。

缺少所需应用程序： 检查设备是否缺少所需的应用程序，如应用程序访问策略中所定义。

非建议应用程序： 检查设备是否有非建议应用程序，如应用程序访问策略中所定义。

不合规密码： 检查用户密码是否合规。在 iOS 和 Android 设备上，Citrix Endpoint Management 可以确定设备上当前密码是否符合发送到设备的密码策略。例如，在 iOS 上，如果 Citrix Endpoint Management 向设备发送密码策略，用户有 60 分钟的时间来设置密码。在用户设置密码之前，密码可能不合规。

不合规设备： 检查设备是否不合规，基于不合规设备属性。使用 Citrix Endpoint Management API 的自动化操作或第三方通常会更改该属性。

已吊销状态： 检查设备证书是否已吊销。已吊销的设备在再次获得授权之前无法重新注册。

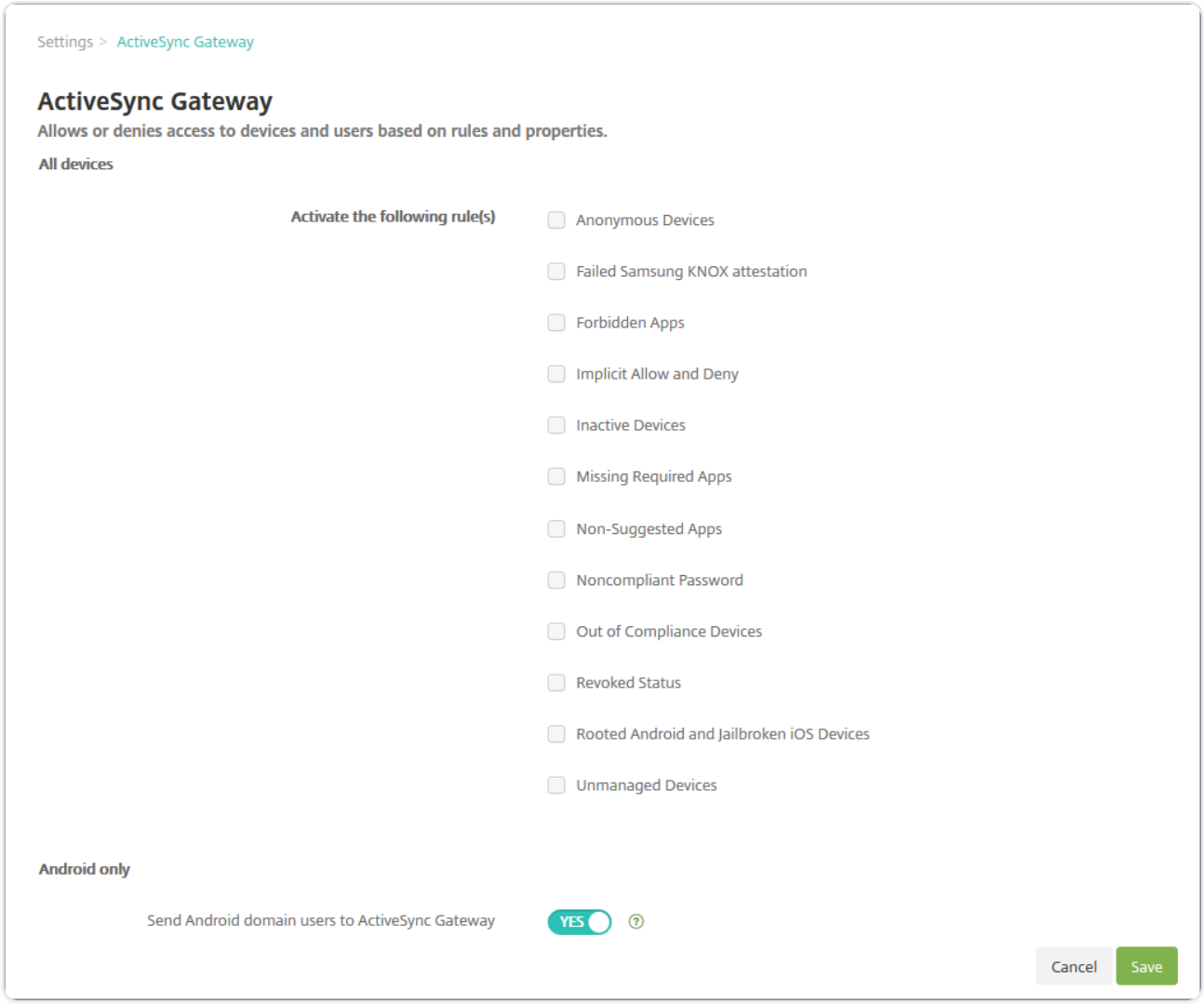
已 Root 的 Android 设备和已越狱的 iOS 设备： 检查 Android 或 iOS 设备是否已越狱。

非托管设备： 检查设备是否仍处于由 Citrix Endpoint Management 控制的托管状态。例如，已注册 MAM 的设备或未注册的设备均不受托管。

将 Android 域用户发送到 ActiveSync Gateway： 单击 **YES** 以使 Citrix Endpoint Management 将 Android 设备所有者的用户名和 ActiveSync ID 发送到 ActiveSync Gateway。除非您正在运行旧版配置，否则请关闭此功能。在较新的配置中，只要与设备关联的用户名存在于网关上，此功能就允许任何设备访问 ActiveSync 数据。

配置 ActiveSync Gateway 设置

1. 在 Citrix 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，单击“**ActiveSync Gateway**”。此时将显示“**ActiveSync Gateway**”页面。



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，在“**将 Android 域用户发送到 ActiveSync Gateway**”中，单击 **YES** 以确保 Citrix Endpoint Management 将 Android 设备信息发送到 ActiveSync Gateway。
3. 点击 **保存**。

用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器

XenMobile Mail Manager 现已成为 Citrix Endpoint Management Exchange ActiveSync 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。

此连接器通过以下方式扩展了 Citrix Endpoint Management 的功能：

- 适用于 Exchange Active Sync (EAS) 设备的动态访问控制。EAS 设备可以自动被允许或阻止访问 Exchange 服务。
- Citrix Endpoint Management 能够访问由 Exchange 提供的 EAS 设备伙伴关系信息。

- Citrix Endpoint Management 能够根据 EAS 状态擦除移动设备。
- Citrix Endpoint Management 能够访问有关 Blackberry 设备的信息，并执行控制操作，例如擦除 (Wipe) 和重置密码 (ResetPassword)。

要根据 EAS 状态擦除设备，请使用 ActiveSync 触发器配置自动化操作。请参阅 自动化操作。

> **重要提示：**

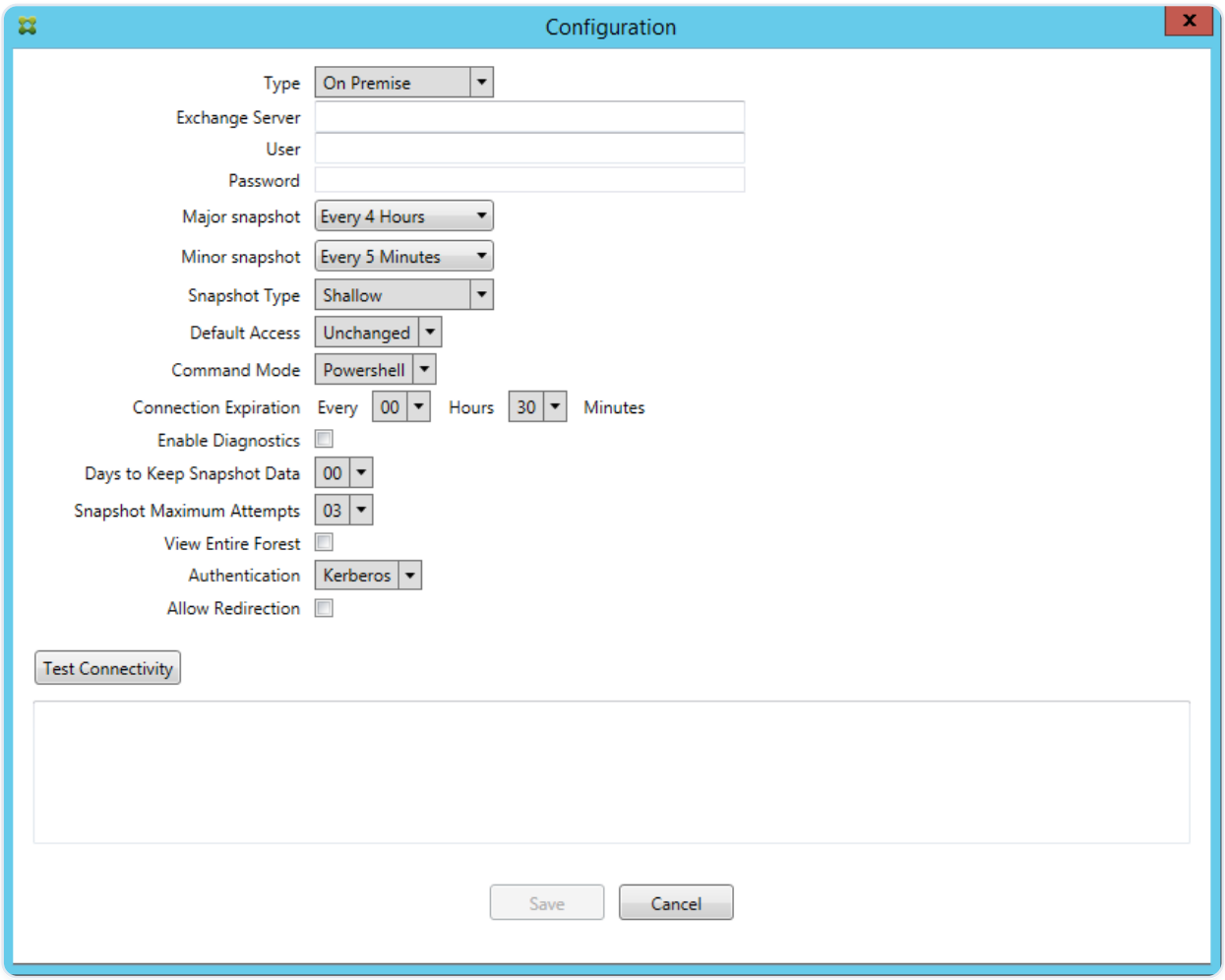
> 自 2022 年 10 月起，鉴于 Microsoft 此处 宣布的身份验证更改，Citrix Endpoint Management 和 NetScaler Gateway 的 Exchange ActiveSync 连接器不再支持 Exchange Online。Citrix Endpoint Management 的 Exchange 连接器将继续与 Microsoft Exchange Server（本地部署）配合使用。

版本 10.1.10 中的新增功能

版本 10.1.10 中修复了以下问题：

- 遇到频繁网络问题的客户可能无法在之前提供的三次尝试内完成快照 (Snapshot)。在此版本中，管理员可以配置最大尝试次数 (1-10)。此修复允许快照在通信中断多次的情况下，无需完全放弃

快照过程。



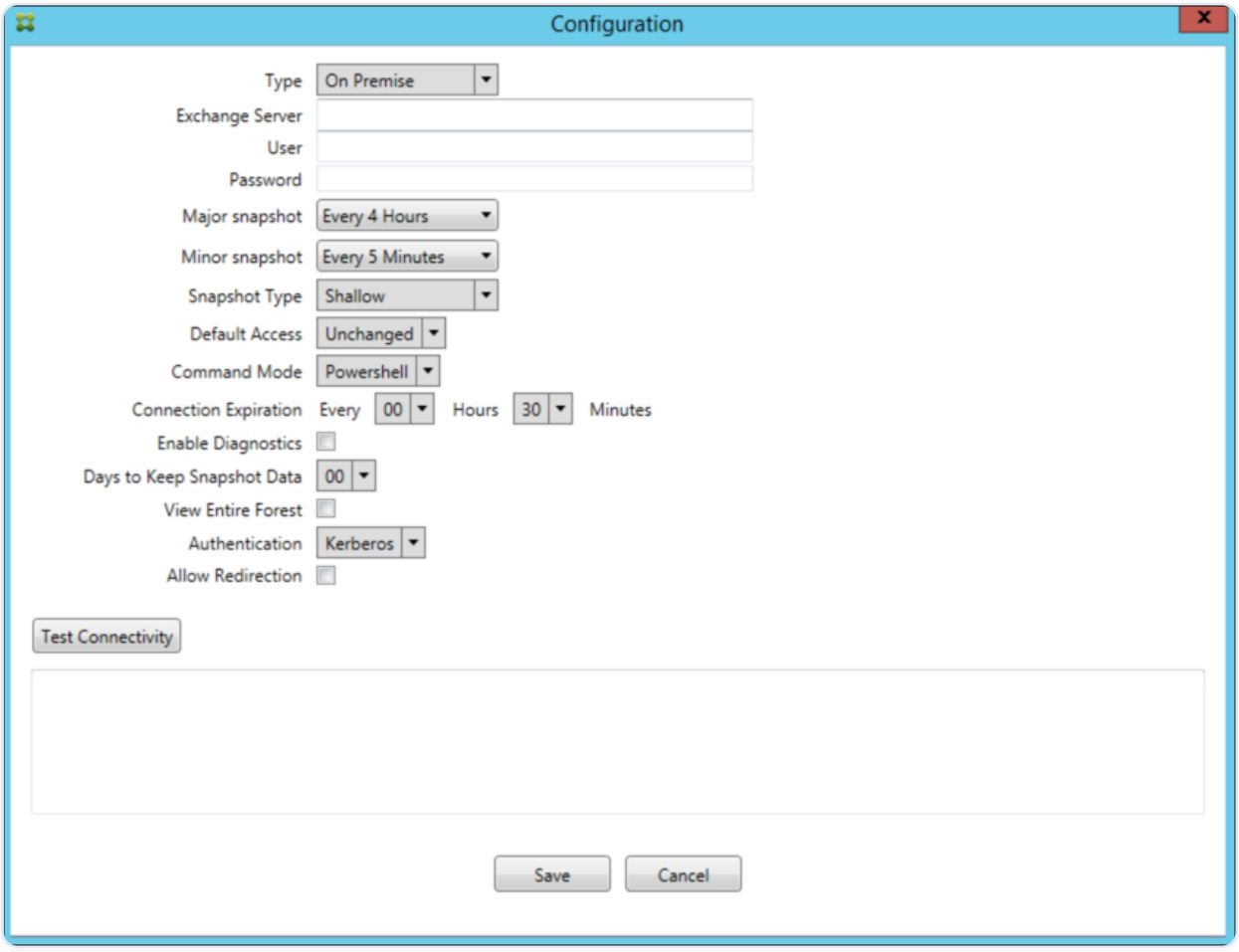
- 在以前的版本中，快照 (Snapshot) 类型未显示在 Exchange 配置列表中。现在，快照类型会显示。
- PowerShell 报告的 PSRemotingTransport 异常表示与 Exchange 的会话不再可用。默认情况下，此状态会添加到配置文件中的“严重错误”列表中。这样，当检测到 PSRemotingTransportException 时，连接将被标记为“错误”状态，以便稍后处理。下一次通信将使用有效连接或创建新连接。
- 保存配置更改时，可能并非所有先前配置的内部组件都在加载新配置之前得到正确处置。此问题可能导致不可预测的行为。行为取决于具体的更改以及更改是否与以前的配置冲突。在此版本中，所有内部组件都在加载新配置之前得到处置。

10.1.9 版中的新增功能

版本 10.1.9 中修复了以下问题：

- 配置更改现在以更一致的方式处理。当服务检测到配置更改时，每个内部子系统都会停止，这意味着任何活动或计划的处理都会中断。接下来，加载新配置并重新启动子系统，这意味着所有计划和其他内部基础结构都将使用新设置重新建立。此问题纠正了 10.1.8 版中的已知问题。

- 在升级过程中，现有数据库配置未合并到新配置文件中。现在，数据库配置已合并到升级后的配置文件中。
- 在快照相关的诊断文件中，缺少列标题。标题已恢复。
- 从以前的版本升级时，配置文件的默认部分会被正在使用的配置文件中的类似部分覆盖。此问题阻止了默认部分的添加或改进在升级后被服务加载。从该版本开始，默认部分始终反映最新的配置。
- 管理员在运行应用程序时无法再通过按 Shift 键访问某些选项。这些选项以前在 Citrix® 许可下可用。现在，某些选项（例如“允许重定向”）已完全可用，而其他选项（例如“挂起检测”和“计数校正”）则已弃用。



早期版本中的新增功能

以下部分列出了 Citrix Endpoint Management connector for Exchange ActiveSync 早期版本中的新功能和已修复问题。

10.1.8 版中的新增功能

- Exchange 可能会限制 Citrix Endpoint Management connector for Exchange ActiveSync 服务过于频繁地发出命令。此问题在连接到 Office 365 时很常见。限制的影响要求服务在发送下一个命令之前暂停指定时间。现在，“配置”控制台会显示暂停的剩余时间。
- 当对配置文件 (config.xml) 的“Watchdog”和/或“SpecialistsDefaults”部分进行修改时，升级后更改不会反映在配置文件中。在此版本中，修改已正确合并到新配置文件中。
- 已向发送到 Google Analytics 的分析数据添加了更多详细信息，特别是关于快照的详细信息。
- Exchange 测试连接功能只会尝试初始化连接一次。由于 Office 365 连接可能会受到限制，因此在受到限制时，测试连接可能会显示失败。Citrix Endpoint Management connector for Exchange ActiveSync 现在最多尝试启动连接三次。
- 为了在 Exchange 上实施策略，Citrix Endpoint Management connector for Exchange ActiveSync 必须编译一个 **Set-CASMailbox** 命令，该命令包含每个邮箱的所有相关设备，分为两个列表：允许和阻止。如果设备未包含在任一列表中，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，则该设备将变得不合规。因此，如果 Exchange 默认访问状态为阻止而应为允许，则用户可能会失去对其电子邮件的访问权限。或者，如果用户的电子邮件访问权限应被阻止，但却被授予了访问权限。Citrix Endpoint Management connector for Exchange ActiveSync 现在确保所有具有有效所需状态的设备都包含在每个 **Set-CasMailbox** 命令中。

版本 10.1.8 中存在以下已知问题：

如果管理员在“配置”应用程序中进行更改以修改配置数据，而服务正在执行长时间操作（例如快照或策略评估），则服务可能会进入不确定状态。可能的症状是策略更改未处理或快照未启动。要使服务恢复到工作状态，必须重新启动服务。您可能需要使用 Windows 服务管理器终止服务进程，然后才能启动服务。

版本 10.1.7 中的新增功能

- XenMobile Mail Manager 现已成为 思杰端点管理 的 Exchange ActiveSync 连接器。
- 我们已弃用 Exchange 配置对话框中的“**禁用管道**”选项。您可以通过在 config.xml 文件中为每个命令配置多个步骤来实现相同的功能。

版本 10.1.7 中修复了以下问题：

- 在“快照历史记录”窗口中，错误消息可能显示上下文不足。现在，错误消息会以其发生位置的上下文作为前缀。
- XmmGoogleAnalytics .dll 没有对应的发布文件版本。

- 为了改进诊断，我们最近更改了用于设置邮箱“允许/阻止”状态的设备 ID 列表的字符串格式。然而，指定过多设备超出了最大字符串大小。现在，我们使用内部数组数据结构。此结构没有大小限制，并且还为诊断目的适当地格式化数据。
- 当检测到与 Exchange 不同步的设备策略时，其命令可能包含不属于相关邮箱的设备。Citrix Endpoint Management connector for Exchange ActiveSync 现在确保发送到 Exchange 的命令仅代表属于其各自邮箱的设备。
- 在某些环境中，Microsoft 程序集不可用。现在，所需的程序集已随应用程序明确安装。
- 如果设备或邮箱的专有名称在属性名称和等号之间有空格，或者在等号之后和值之前有空格，则 Citrix Endpoint Management connector for Exchange ActiveSync 可能无法正确地将设备与其邮箱匹配，反之亦然。结果可能是某些设备和/或邮箱在快照协调期间被拒绝。

> **注意：**
>
> 以下“新增功能”部分将 Citrix Endpoint Management connector for Exchange ActiveSync 称为其旧名称 XenMobile Mail Manager。该名称从版本 10.1.7 开始更改。

版本 10.1.6.20 中的更新

10.1.6 的更新在版本 10.1.6.20 中包含以下修复：

- 当检测到与 Exchange 不同步的设备策略时，其命令可能包含不属于相关邮箱的设备。XenMobile® Mail Manager 现在确保发送到 Exchange 的命令仅代表属于其各自邮箱的设备。

10.1.6 版中的新增功能

XenMobile Mail Manager 10.1.6 版包含以下已修复问题和增强功能：

- 快照历史记录窗口有时会进入不再更新的状态。窗口刷新机制已改进，可更可靠地进行更新。
- 分区快照和非分区快照使用了两种独立的模式和代码路径。由于非分区快照等同于使用单个“*”分区的配置的分区快照，因此已取消非分区快照模式。默认快照模式现在是具有 36 个分区（0–9，A–Z）的分区快照。
- 在“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 提供了两个单独的字段，以便用户可以同时查看状态和错误。
- 连接到 Exchange Online (Office 365) 时，与快照相关的查询可能会导致数据集被截断。当 XenMobile Mail Manager 运行多命令管道脚本时，可能会出现此问题。上游命令无法足够快地将数据传递给下游命令，导致下游命令过早完成工作。结果是数据不完整。XenMobile Mail

Manager 现在可以模拟管道本身，并在上游命令完成后再调用下游命令。此更改应能确保所有数据都得到处理和捕获。

- 如果向 Exchange 发送的策略更新命令中发生无法解决的错误，则同一命令会长时间重复返回到工作队列。这种情况导致命令多次发送到 Exchange。在此版本的 XenMobile Mail Manager 中，导致错误的命令只会返回到工作队列有限的次数。
- 如果特定邮箱的策略更新涉及允许或阻止所有设备：发出的 **Set-CASMailbox** 命令将失败，因为空列表被转换为一个空字符串而不是 **NULL**。现在发送的是正确的数据。
- 处理新设备时，Exchange 可能会在一段时间内（通常为 15 分钟）将状态返回为“DeviceDiscovery”。XenMobile Mail Manager 以前没有专门处理此状态。XenMobile Mail Manager 现在可以处理此状态。在 UI 的“监视器”选项卡中，用户可以筛选处于此状态的设备。
- XenMobile Mail Manager 未检查写入 XenMobile Mail Manager 数据库的能力。因此，如果权限受限，行为可能无法预测。XenMobile Mail Manager 现在从数据库捕获并验证所需的权限。当测试连接（显示消息）或在主“配置”窗口底部的“数据库”指示器（悬停以显示消息）中，XenMobile Mail Manager 会指示权限降低。
- 根据当前工作负载，当收到指令时，XenMobile Mail Manager 服务可能无法及时停止。因此，服务似乎处于无响应状态。改进措施允许中断正在进行的任务，从而实现更优雅的关机。

10.1.5 版中的新增功能

XenMobile Mail Manager 10.1.5 版包含以下已修复问题：

- 当 Exchange 对 XenMobile Mail Manager 活动应用限制时，除了日志之外，没有迹象表明正在发生限制。在此版本中，用户可以将鼠标悬停在活动快照上，然后会出现“限制”状态。此外，当 XenMobile Mail Manager 受到限制时，在 Exchange 解除限制禁令之前，禁止启动主要快照。
- 如果 XenMobile Mail Manager 在主要快照期间受到 Exchange 的限制：在运行下一次快照尝试之前，可能没有足够的时间间隔。此问题会导致进一步的限制和快照失败。XenMobile Mail Manager 现在会等待 Exchange 指定的快照尝试之间的最短时间。
- 启用诊断时，命令文件会显示 **Set-CasMailbox** 命令，这些命令在每个属性名称前缺少连字符。此问题仅发生在诊断文件的格式中，而不是实际发送到 Exchange 的命令。缺少连字符会阻止用户剪切命令并直接将其粘贴到 PowerShell 提示符进行测试或验证。现在已添加连字符。
- 如果邮箱标识符的形式为 `lastname, firstname`，则 Exchange 在从查询返回数据时会在逗号前添加反斜杠。当 XenMobile Mail Manager 使用该标识符查询更多数据时，必须去除此反斜杠。

已知限制

> **注意：**

以下限制已在版本 10.1.6 中解决。

XenMobile Mail Manager 存在一个已知限制，可能导致发送到 Exchange 的命令失败。为了将策略更改应用于 Exchange，XenMobile Mail Manager 会发出 **Set_CASMailbox** 命令。此命令可以接受两个设备列表：一个用于允许，一个用于阻止。该命令应用于与邮箱关联的设备。

这些列表在 Microsoft API 中每个限制为 256 个字符。如果其中一个列表超出限制，则整个命令将失败，从而阻止为该邮箱的这些设备设置策略。XenMobile Mail Manager 日志中报告的错误将如下所示。此示例适用于阻止列表。

“消息：'无法将参数 'ActiveSyncBlockedDeviceIDs' 绑定到目标。设置 "ActiveSyncBlockedDeviceIDs" 时发生异常："属性的长度过长。最大长度为 256，提供的值的长度为 …”

设备 ID 长度可能有所不同，但一个好的指导原则是，同时允许或阻止大约 10 个或更多设备可能会超出限制。尽管与特定邮箱关联如此多的设备很少见，但仍有可能。在 Mail Manager 改进以处理此类情况之前，我们建议您将与用户和邮箱关联的设备数量限制为 10 个或更少。

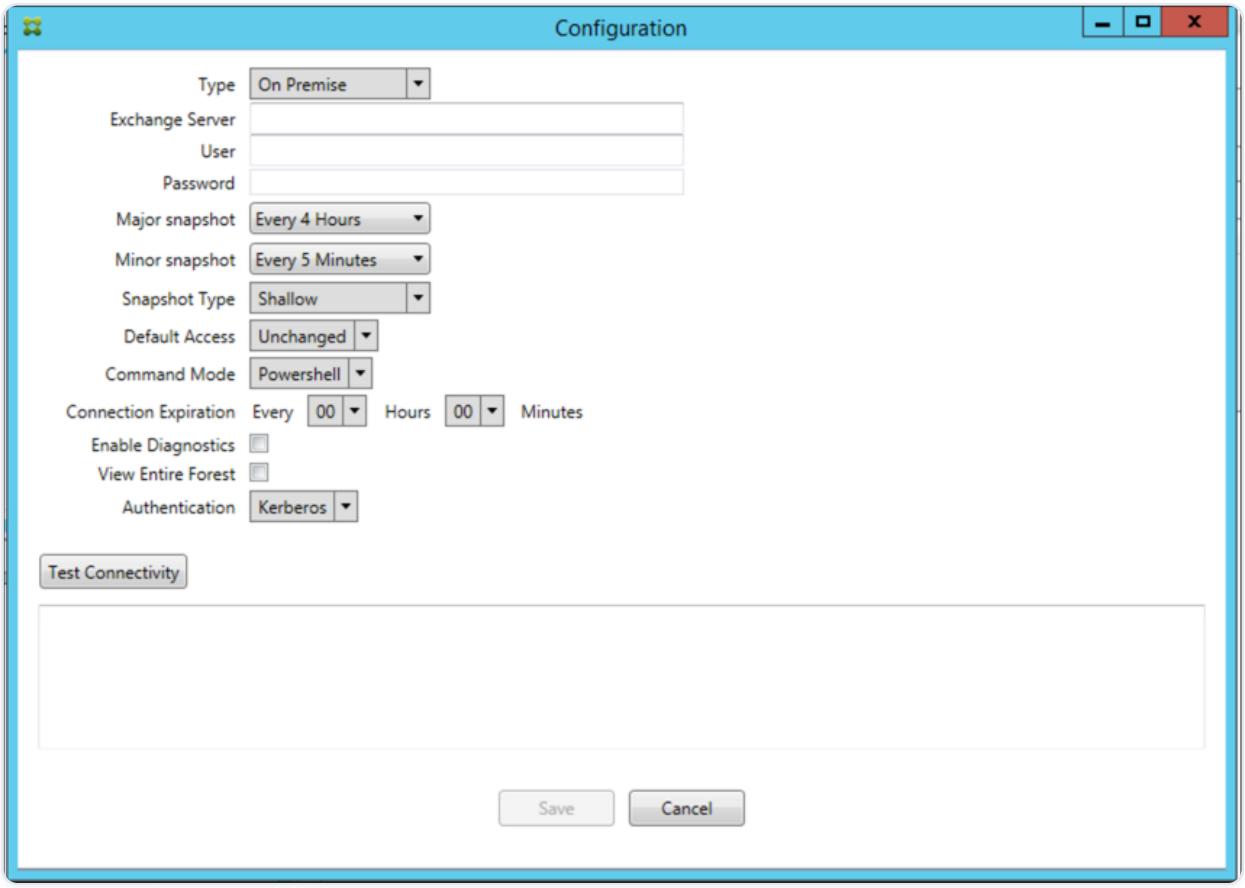
版本 10.1.4 中的新增功能

XenMobile Mail Manager 版本 10.1.4 修复了以下问题：

- 由于其安全性减弱，PCI 委员会正在弃用 TLS 1.0 和 TLS 1.1。XenMobile Mail Manager 中已添加对 1.2 的支持。
- XenMobile Mail Manager 包含一个新的诊断文件。在 Exchange 规范中选择 **Enable Diagnostics** 时，会生成一个新的快照历史文件。每次快照尝试都会在文件中添加一行，其中包含快照结果。
- 在命令诊断文件中，**Set-CASMailbox** 命令未显示允许或阻止的设备列表。相反，文件中显示的是相关参数的内部类名。XenMobile Mail Manager 现在将设备 ID 列表显示为逗号分隔列表。
- 当由于错误的规范而导致尝试获取与 Exchange 的连接失败时：不正确的错误消息会覆盖原始错误消息：“所有连接都在使用中”。现在会显示更具描述性的消息，例如“所有连接都无法操作”、“连接池为空”、“所有连接都受到限制”和“没有可用连接”。
- 有时，允许/阻止/擦除命令会在 XenMobile Mail Manager 内部缓存中多次排队。此问题会导致命令发送到 Exchange 时出现延迟。XenMobile Mail Manager 现在只对每个命令的一个实例进行排队。

版本 10.1.3 中的新增功能

- **Google Analytics 支持：** 我们希望了解您如何使用 XenMobile Mail Manager，以便我们能够专注于改进产品。
- **启用诊断的设置：** “配置”控制台的“**配置**”对话框中显示一个“**启用诊断**”复选框。



版本 10.1.3 中修复的问题

- 在“**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。 有时，XenMobile Mail Manager 无法写入命令诊断文件。发生这种情况时，命令历史记录不会完整记录。
- 当连接发生错误时，该连接可能不会被标记为“出错”。因此，后续命令可能会尝试使用该连接并导致另一个错误。
- 当 Exchange Server 发生限制时，“检查运行状况”例程中可能会抛出异常。因此，已发生错误或已过期的连接可能不会被清除。此外，XenMobile Mail Manager 可能不会创建连接，直到限制时间过期。。
- 当超出 Exchange 的最大会话数时，XenMobile Mail Manager 会报告错误“设备捕获失败”，这不是一个准确的消息。相反，该消息应指示 XenMobile Mail Manager 通常用于 Exchange 通信的两个会话正在使用中。

版本 10.1.2 中的新增功能

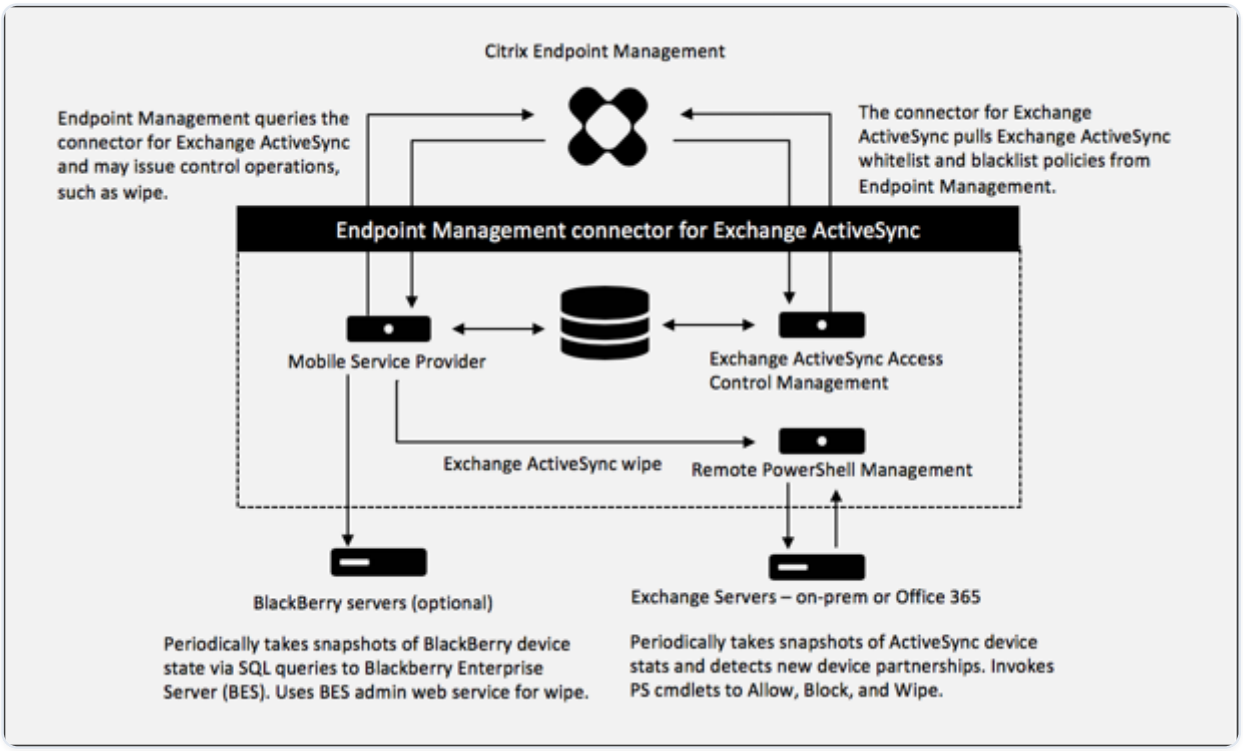
- **改进了与 Exchange 的连接：** XenMobile Mail Manager 使用 PowerShell 会话与 Exchange 通信。PowerShell 会话，尤其是在处理 Office 365 时，一段时间后可能会变得不稳定，从而阻止后续命令成功。XenMobile Mail Manager 现在可以为连接设置一个过期时间。当连接达到其过期时间时，XenMobile Mail Manager 会正常关闭 PowerShell 会话并创建一个新会话。通过这样做，PowerShell 会话变得不稳定的可能性较小，从而显著降低了快照失败的可能性。
- **改进的快照工作流：** 主要快照是一项耗时且占用大量处理资源的操作。如果在快照期间发生错误，XenMobile Mail Manager 现在会尝试多次（最多三次）完成快照。后续尝试不会从头开始。XenMobile Mail Manager 会从上次中断的地方继续。此增强功能通过允许瞬时错误在快照仍在进行时通过，从而提高了快照的总体成功率。
- **改进的诊断：** 现在，通过在快照期间可选生成的三个新诊断文件，快照操作的故障排除变得更加容易。这些文件有助于识别 PowerShell 命令问题、信息缺失的邮箱以及无法与邮箱关联的设备。管理员可以使用这些文件来识别 Exchange 中可能不正确的数据。
- **改进的内存使用：** XenMobile Mail Manager 现在更有效地利用内存。管理员可以安排 XenMobile Mail Manager 自动重启，以便为系统提供一个全新的开始。
- **Microsoft .NET Framework 4.6 先决条件：** Microsoft .NET Framework 的先决条件版本现在是 4.6。

已修复的问题

- 凭据提示错误：Office 365 会话不稳定通常会导致此错误。改进的 Exchange 连接增强功能解决了此问题。(XMHELP-293, XMHELP-311, XMHELP-801)
- 邮箱和设备计数不准确：XenMobile Mail Manager 具有改进的邮箱到设备关联算法。改进的诊断功能有助于识别 XenMobile Mail Manager 认为不在其职责范围内的邮箱和设备。(XMHELP-623)
- 允许/阻止/擦除命令无法识别：修复了一个错误，该错误导致有时 XenMobile 邮件管理器 的允许/阻止/擦除命令无法识别。(XMHELP-489)
- 内存管理：更好的内存管理和缓解措施。(XMHELP-419)

架构

下图显示了 Citrix Endpoint Management connector for Exchange ActiveSync 的主要组件。有关详细的参考体系结构图，请参阅 体系结构。



两个主要组件是：

- **Exchange ActiveSync 访问控制管理：** 与 Citrix Endpoint Management 通信以从 Citrix Endpoint Management 检索 Exchange ActiveSync 策略，并将此策略与任何本地定义的策略合并，以确定应允许或拒绝访问 Exchange 的 Exchange ActiveSync 设备。本地策略允许扩展策略规则，以通过 Active Directory 组、用户、设备类型或设备用户代理（通常是移动平台版本）进行访问控制。
- **远程 PowerShell 管理：** 负责调度和调用远程 PowerShell 命令，以执行由 Exchange ActiveSync 访问控制管理编译的策略。定期对 Exchange ActiveSync 数据库进行快照，以检测新增或更改的 Exchange ActiveSync 设备。

系统要求和先决条件

使用 Citrix Endpoint Management connector for Exchange ActiveSync 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 January 14, 2020 结束，对 Windows Server 2012 R2 的支持将于 October 10, 2023 结束。
- Microsoft SQL Server 2016 服务包 2、SQL Server 2014 服务包 3 或 SQL Server 2012 服务包 4。
- Microsoft .NET 框架 4.6。
- Blackberry Enterprise 服务，版本 5（可选）。

Microsoft Exchange Server 支持的最低版本：

- 微软 Office 365
- Exchange 服务器 2016
- Exchange Server 2013 (支持于 April 11, 2023 结束)
- Exchange Server 2010 Service Pack 3（支持截止日期为 January 14, 2020）

先决条件

- 必须安装 Windows 管理框架。
    - PowerShell V5、V4 和 V3
- 必须通过 Set-ExecutionPolicy RemoteSigned 将 PowerShell 执行策略设置为 RemoteSigned。
- 运行 Exchange ActiveSync 连接器的计算机与远程 Exchange Server 之间必须打开 TCP 端口 80。

设备电子邮件客户端： 并非所有电子邮件客户端都始终为设备返回相同的 ActiveSync ID。由于 Exchange ActiveSync 连接器需要为每个设备提供唯一的 ActiveSync ID，因此仅支持始终为每个设备生成相同且唯一的 ActiveSync ID 的电子邮件客户端。Citrix 已对以下电子邮件客户端进行了测试，且未发现错误：

- 三星原生电子邮件客户端
- iOS 原生电子邮件客户端

Exchange： 运行 Exchange 的本地计算机的要求如下：

Exchange 配置 UI 中指定的凭据必须能够连接到 Exchange Server，并被授予完全访问权限以运行以下 Exchange 特定的 PowerShell cmdlet。

- **对于 Exchange Server 2010 SP2 而言：**
    - `Get-CASMailbox`
    - `Set-CASMailbox`
    - `Get-Mailbox`
    - `Get-ActiveSyncDevice`
    - `Get-ActiveSyncDeviceStatistics`
    - `Clear-ActiveSyncDevice`
    - `Get-ExchangeServer`

  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

- **对于 Exchange 服务器 2013 和 Exchange 服务器 2016：**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- 如果 Exchange ActiveSync 连接器配置为查看整个林，则必须已授予运行以下命令的权限：**Set-AdServerSettings -ViewEntireForest $true**
- 必须已授予所提供的凭据通过远程 Shell 连接到 Exchange Server 的权限。默认情况下，安装 Exchange 的用户拥有此权限。
- 要建立远程连接并运行远程命令，凭据必须对应于远程计算机上的管理员用户。您可以使用 Set-PSSessionConfiguration 来消除管理要求，但该命令的讨论超出了本文档的范围。有关详细信息，请参阅 Microsoft 文章关于会话配置。
- 必须将 Exchange Server 配置为通过 HTTP 支持远程 PowerShell 请求。通常，只需管理员在 Exchange Server 上运行以下 PowerShell 命令即可：WinRM QuickConfig。
- Exchange 有许多限制策略。其中一项策略控制每个用户允许的并发 PowerShell 连接数。在 Exchange 2010 上，每个用户允许的默认并发连接数为 18。当达到连接限制时，Exchange ActiveSync 连接器将无法连接到 Exchange Server。有多种方法可以通过 PowerShell 更改允许的最大并发连接数，但这超出了本文档的范围。如果感兴趣，请研究与 PowerShell 远程管理相关的 Exchange 限制策略。

Office 365 Exchange 的要求

- **权限：** Exchange 配置 UI 中指定的凭据必须能够连接到 Office 365，并被授予完全访问权限以运行以下 Exchange 特定的 PowerShell cmdlet：
  - `Get-CASMailbox`

  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

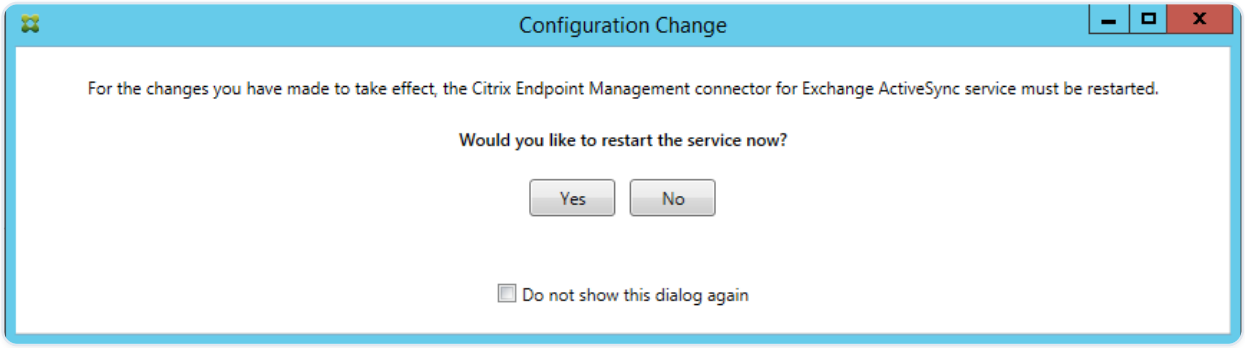
- **权限：** 必须已授予所提供的凭据通过远程 Shell 连接到 Office 365 服务器的权限。默认情况下，Office 365 在线管理员拥有所需的权限。
- **限制策略：** Exchange 有许多限制策略。其中一项策略控制每个用户允许的并发 PowerShell 连接数。在 Office 365 上，每个用户允许的默认并发连接数为三个。当达到连接限制时，Exchange ActiveSync 连接器将无法连接到 Exchange Server。有多种方法可以通过 PowerShell 更改允许的最大并发连接数，但这超出了本文档的范围。如果感兴趣，请研究与 PowerShell 远程管理相关的 Exchange 限制策略。

安装和配置

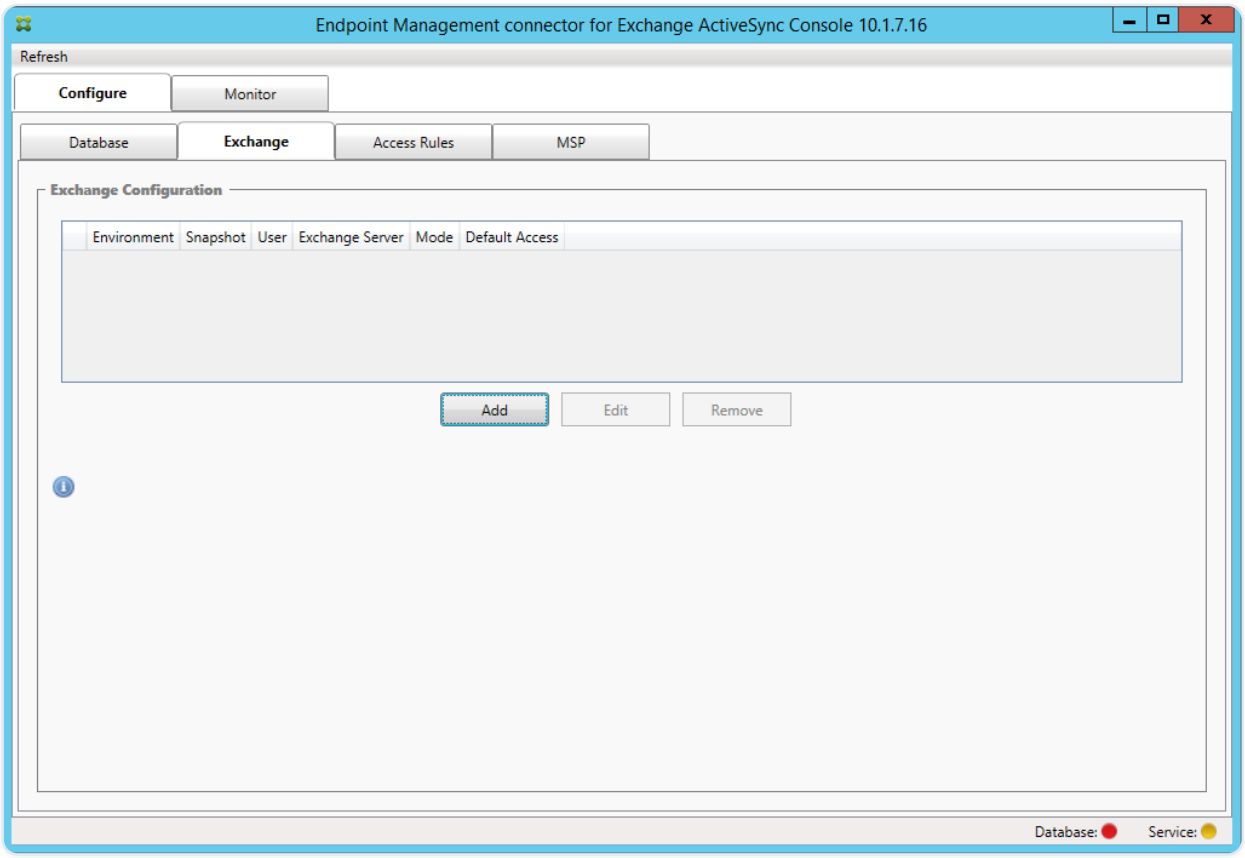
1. 单击 XmmSetup.msi 文件，然后按照安装程序中的提示安装 Citrix Endpoint Management connector for Exchange ActiveSync。
2. 在安装向导的最后一个屏幕中，保持选中“**启动配置实用程序**”。或者，从“**开始**”菜单打开 Exchange ActiveSync 连接器。
3. 配置以下数据库属性：
   - 选择“**配置 > 数据库**”选项卡。
   - 输入 SQL Server 的名称（默认为 localhost）。
   - 将数据库保留为默认的 **CitrixXmm**。
4. 选择以下用于 SQL 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 集成：** 如果选择此选项，则必须将 XenMobile Mail Manager Service 的登录凭据更改为具有访问 SQL Server 权限的 Windows 帐户。为此，请打开“**控制面板 > 管理工具 > 服务**”，右键单击 XenMobile Mail Manager Service 条目，然后单击“**登录**”选项卡。

如果 BlackBerry 数据库连接也选择了 Windows 集成，则此处指定的 Windows 帐户也必须被授予访问 BlackBerry 数据库的权限。

5. 单击“**测试连接**”以检查是否可以连接到 SQL Server，然后单击“**保存**”。
6. 此时会显示一条消息，提示您重新启动服务。单击“**是**”。



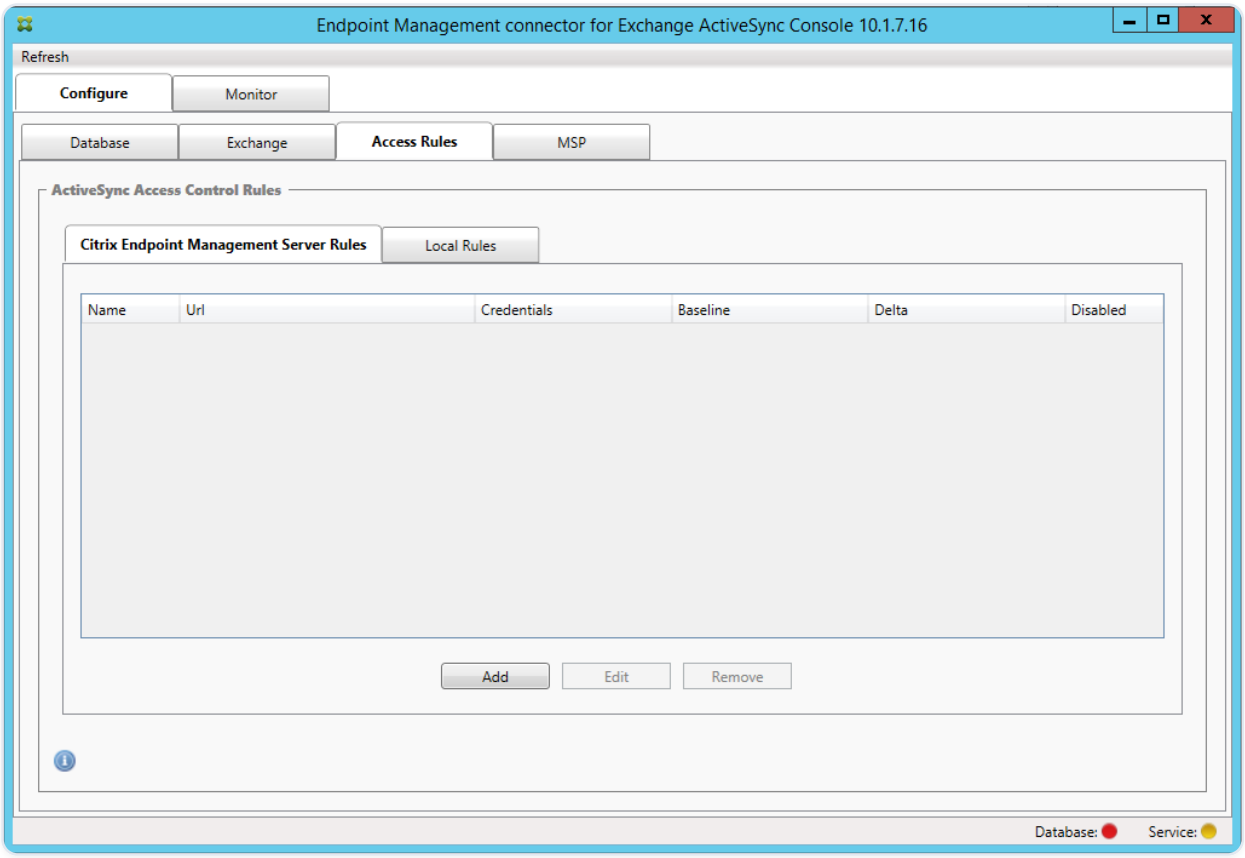
7. 配置一个或多个 Exchange Server：
   - 如果管理单个 Exchange 环境，则仅指定一个服务器。如果管理多个 Exchange 环境，则为每个 Exchange 环境指定一个 Exchange Server。
   - 单击“**配置 > Exchange**”选项卡，然后单击“**添加**”。



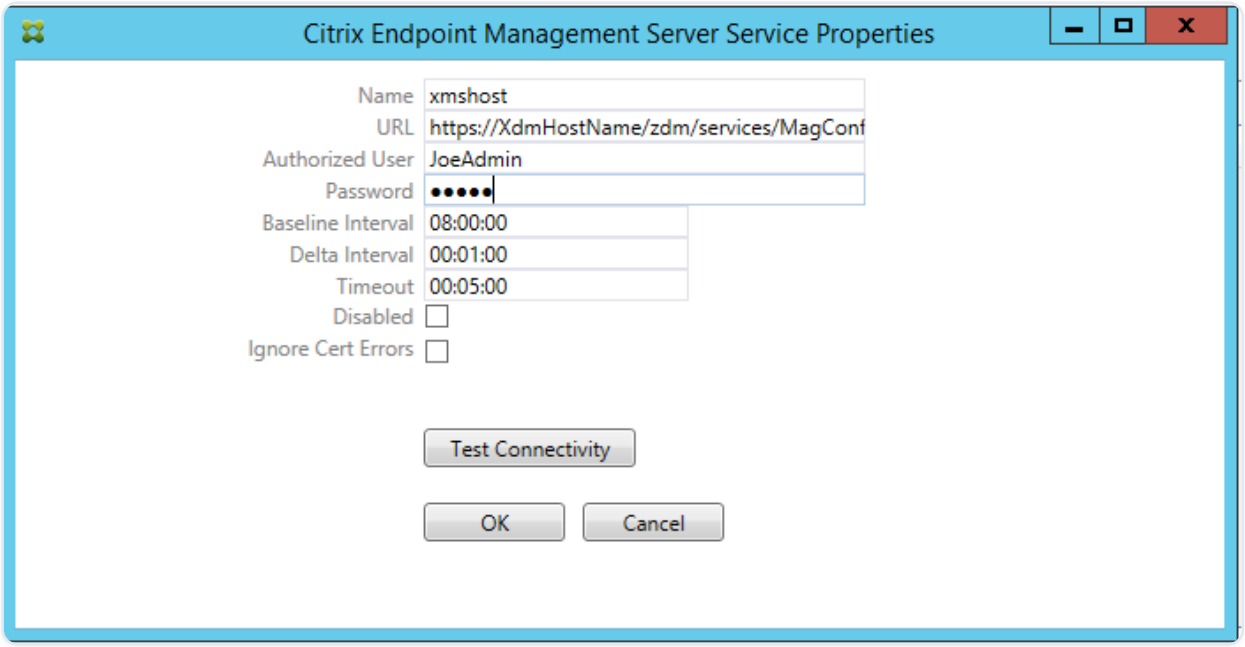
8. 选择 Exchange Server 环境类型：**本地部署**或 **Office 365**。
   - 如果您选择 **本地部署**，请输入用于远程 PowerShell 命令的 Exchange Server 名称。

- 输入在“要求”部分中指定的、在 Exchange Server 上具有相应权限的 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。主要快照会检测每个 Exchange ActiveSync 伙伴关系。
- 选择运行次要快照的计划。次要快照会检测新创建的 Exchange ActiveSync 伙伴关系。
- 选择快照类型：**深度**或**浅度**。浅度快照通常快得多，足以执行 Exchange ActiveSync 连接器所有 Exchange ActiveSync 访问控制功能。
- 选择默认访问权限：**允许**、**阻止**或**不变**。此设置控制除由显式 Citrix Endpoint Management 或本地规则标识的设备之外的所有设备的处理方式。如果您选择**允许**，则允许所有此类设备的 ActiveSync 访问。如果您选择**阻止**，则拒绝访问。如果您选择**不变**，则不进行任何更改。
- 选择 ActiveSync 命令模式：**PowerShell** 或**模拟**。
- 在 **PowerShell** 模式下，Exchange ActiveSync 连接器会发出 PowerShell 命令以实施所需的访问控制。在模拟模式下，Exchange ActiveSync 连接器不会发出 PowerShell 命令，而是将预期的命令和预期结果记录到数据库中。在模拟模式下，用户可以使用**监视器**选项卡查看如果启用了 PowerShell 模式会发生什么。
- 在**连接过期**中，设置连接的生命周期（小时和分钟）。当连接达到指定时长时，该连接将被标记为已过期，因此不会再次使用。当不再使用过期连接时，Exchange ActiveSync 连接器会正常关闭该连接。如果需要再次连接，并且没有可用连接，则会初始化一个新连接。如果未指定，则使用默认值 30 分钟。
- 选择**查看整个林**以配置 Exchange ActiveSync 连接器以查看 Exchange 环境中的整个 Active Directory 林。
- 选择身份验证协议：**Kerberos** 或**基本**。Exchange ActiveSync 连接器支持本地部署的基本身份验证。这使得当连接器服务器不是 Exchange 服务器所在域的成员时，可以使用该连接器。
- 单击**测试连接**以检查是否可以连接到 Exchange Server，然后单击**保存**。
- 消息提示您重新启动服务。单击**是**。

9. 配置访问规则：选择**配置 > 访问规则**选项卡，单击 **Citrix Endpoint Management 规则**选项卡，然后单击**添加**。



10. 在 **Citrix Endpoint Management 服务器服务属性** 页面上，修改 URL 字符串以指向 Citrix Endpoint Management 服务器。例如，如果实例名称为 `zdm`，请输入 `https://<XdmHostName>/zdm/services/MagConfigService`。在此示例中，请将 `XdmHostName` 替换为 Citrix Endpoint Management 服务器的 IP 或 DNS 地址。

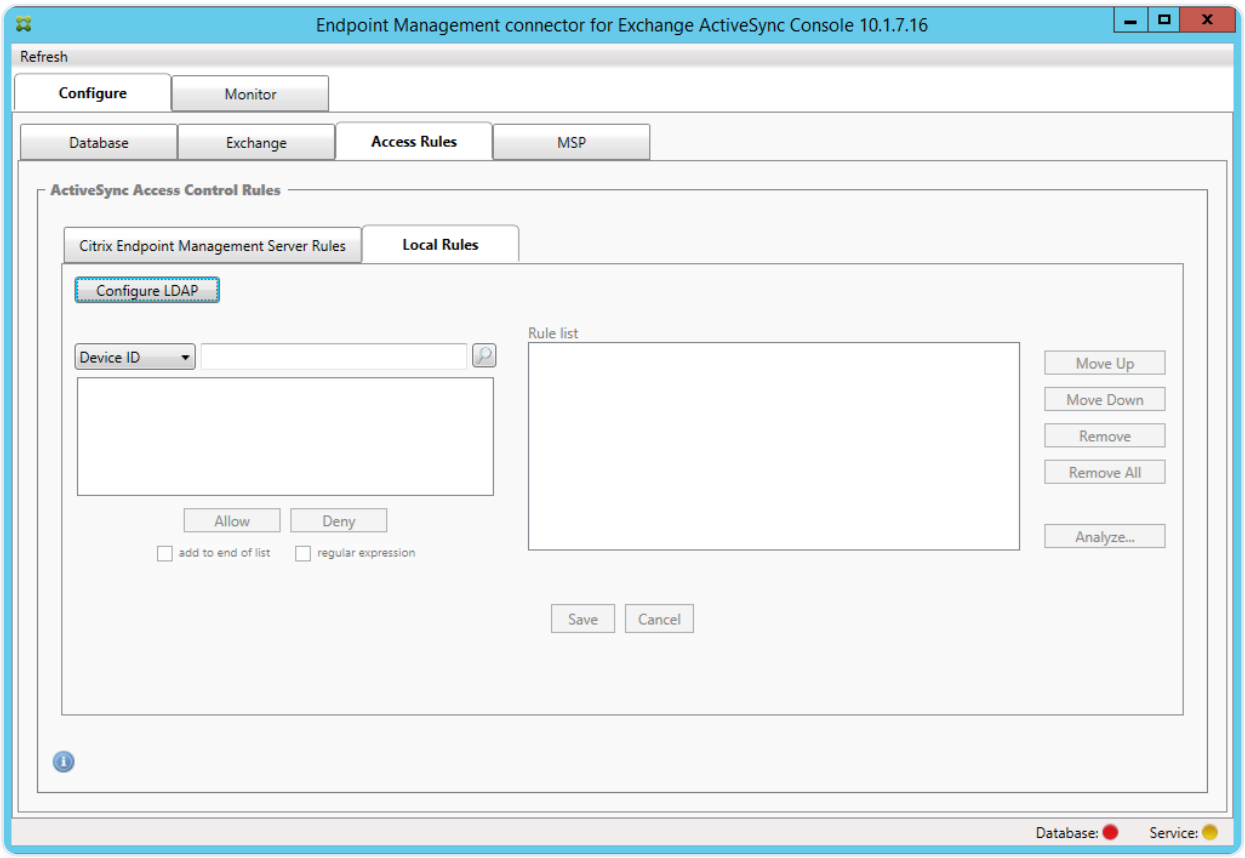


- 输入服务器的授权用户。
- 输入用户的密码。

- 保留 **基线间隔**、**增量间隔** 和 **超时** 值的默认值。
- 单击 **测试连接** 以检查与服务器的连接，然后单击 **确定**。

如果选中了 **禁用** 复选框，则 Citrix Endpoint Management 邮件服务不会从 Citrix Endpoint Management 收集策略。

11. 单击 **本地规则** 选项卡。

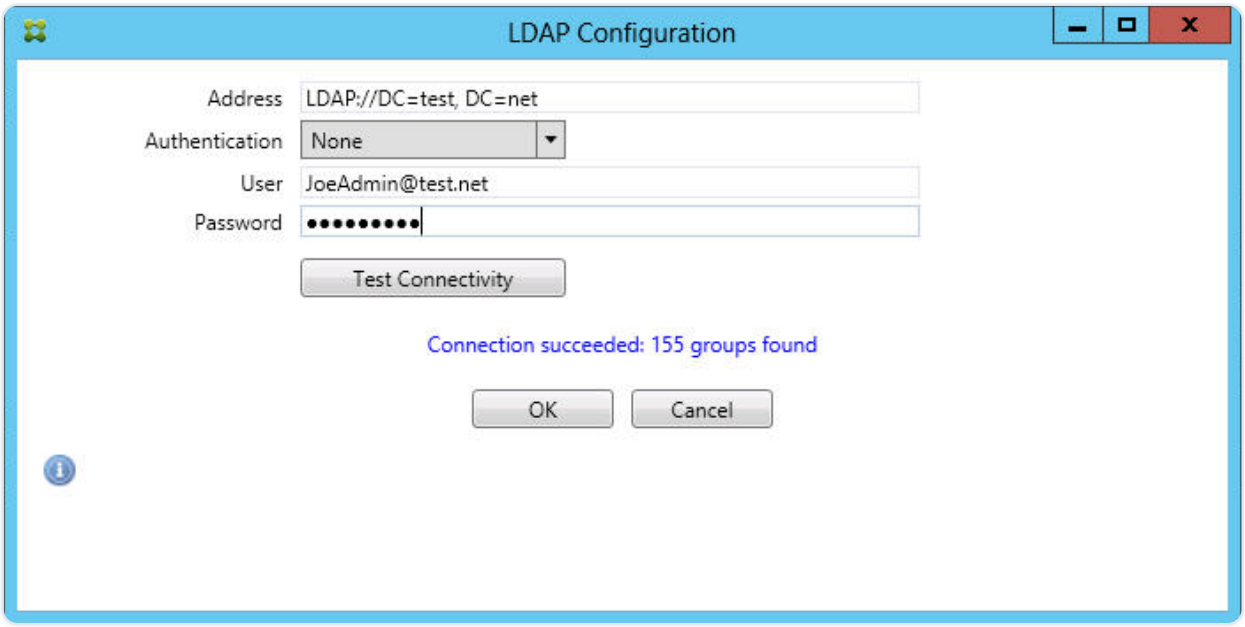


- 您可以根据 ActiveSync 设备 ID、设备类型、AD 组、用户或设备 UserAgent 添加本地规则。在列表中，选择相应的类型。
- 在文本框中输入文本或文本片段。或者，单击查询按钮以查看与该片段匹配的实体。

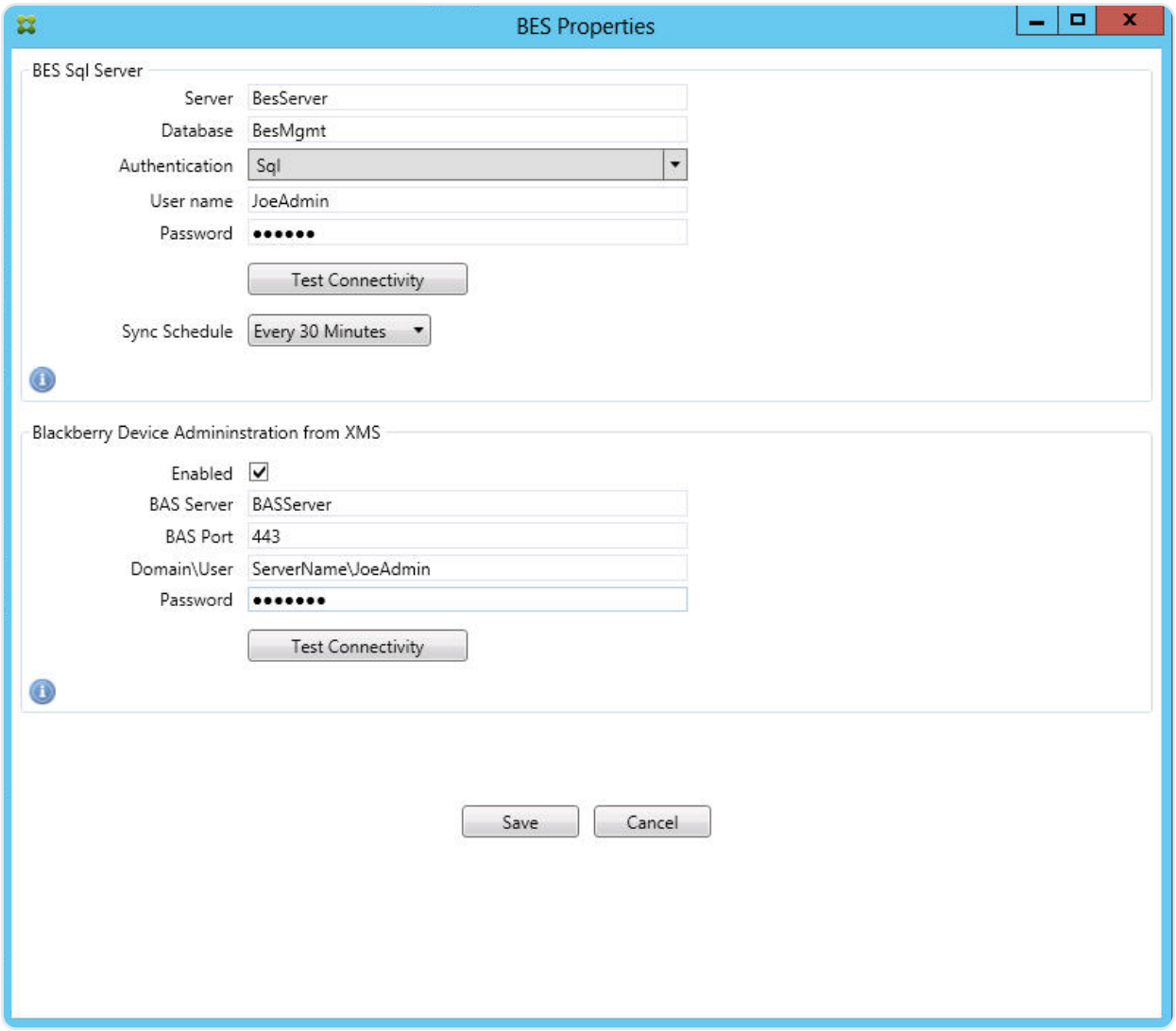
对于除组以外的所有类型，系统都依赖于在快照中找到的设备。因此，如果您刚开始并且尚未完成快照，则没有可用的实体。

- 选择一个文本值，然后单击 **允许** 或 **拒绝** 以将其添加到右侧的 **规则列表** 窗格中。您可以使用 **规则列表** 窗格右侧的按钮更改规则的顺序或将其删除。顺序很重要，因为对于给定的用户和设备，规则将按所示顺序进行评估，并且与较高规则（靠近顶部）的匹配会导致后续规则无效。例如，如果您有一条允许所有 iPad 设备的规则，以及一条后续阻止用户 Matt 的规则，则 Matt 的 iPad 仍将被允许，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查找任何潜在的覆盖、冲突或补充构造，请单击 **分析**，然后单击 **保存**。

12. 如果要构建对 Active Directory 组进行操作的本地规则，请单击 **配置 LDAP**，然后配置 LDAP 连接属性。



13. 可选地，配置一个或多个 BlackBerry Enterprise Server (BES) 实例：单击 **添加**，然后输入 BES SQL Server 的服务器名称

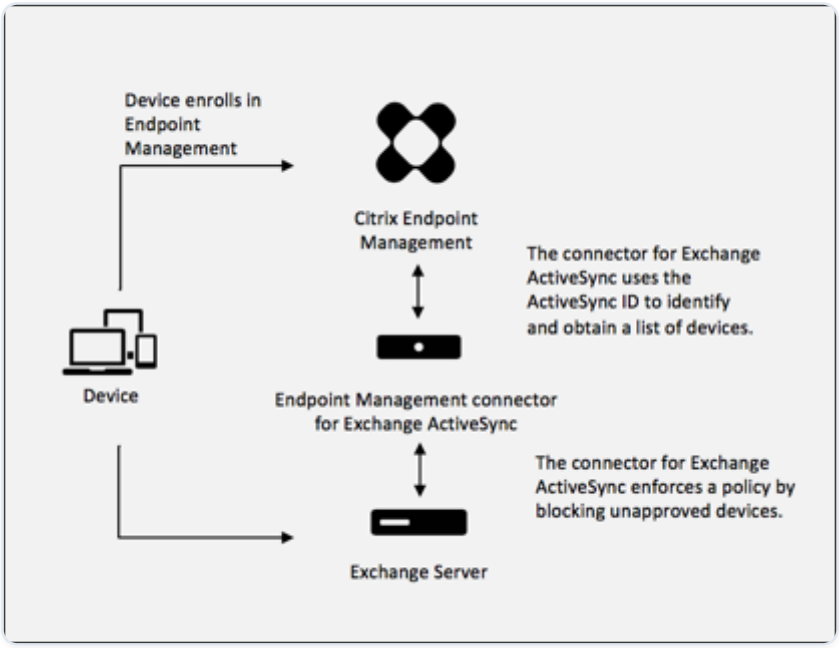


- 输入 BES 管理数据库的数据库名称。
- 选择 **身份验证** 模式。如果选择 Windows 集成身份验证，则用于 Exchange ActiveSync 服务的连接器用户帐户是用于连接到 BES SQL Server 的帐户。如果您还为连接器数据库连接选择 Windows 集成，则此处指定的 Windows 帐户也必须被授予连接器数据库的访问权限。
- 如果选择 **SQL 身份验证**，请输入用户名和密码。
- 设置 **同步计划**。这是用于连接到 BES SQL Server 并检查任何设备更新的计划。
- 单击 **测试连接** 以检查与 SQL Server 的连接。如果选择 Windows 集成，此测试将使用当前登录的用户而不是连接器服务用户，因此无法准确测试 SQL 身份验证。
- 为了支持从 Citrix Endpoint Management 远程擦除和重置 BlackBerry 设备的密码，请选中 **启用** 复选框。
- 输入 BES 完全限定域名 (FQDN)。
- 输入用于管理 Web 服务的 BES 端口。
- 输入 BES 服务所需的完全限定用户和密码。
- 单击 **测试连接** 以测试与 BES 的连接，然后单击 **保存**。

使用 ActiveSync ID 强制执行电子邮件策略

您的公司电子邮件策略可能规定某些设备不被批准用于公司电子邮件。为遵循此策略，您需要确保员工无法从此类设备访问公司电子邮件。Citrix Endpoint Management connector for Exchange ActiveSync 和 Citrix Endpoint Management 协同工作以强制执行此类电子邮件策略。Citrix Endpoint Management 设置公司电子邮件访问策略。当未经批准的设备注册到 Citrix Endpoint Management 时，Exchange ActiveSync 连接器会强制执行该策略。

设备的电子邮件客户端使用设备 ID（也称为 ActiveSync ID）向 Exchange Server（或 Office 365）通告自身，该 ID 用于识别设备。Citrix Secure Hub 获取一个类似的标识符，并在设备注册时将该标识符发送给 Citrix Endpoint Management。通过比较这两个设备 ID，Exchange ActiveSync 连接器可以确定特定设备是否应具有企业电子邮件访问权限。下图说明了此概念：



如果 Citrix Endpoint Management 向 Exchange ActiveSync 连接器发送的 ActiveSync ID 与设备发布到 Exchange 的 ID 不同，则连接器无法向 Exchange 指示如何处理该设备。

ActiveSync ID 匹配在大多数平台上都能可靠运行。但是，Citrix 发现，在某些 Android 实现中，来自设备的 ActiveSync ID 与邮件客户端向 Exchange 通告的 ID 不同。为缓解此问题，您可以执行以下操作：

- 在 Android 平台上，Citrix 建议您使用 Citrix Secure Mail。

为确保正确执行企业电子邮件访问策略，您可以采取防御性安全措施。将 Citrix Endpoint Management 的 Exchange ActiveSync 连接器配置为默认将静态策略设置为 **“拒绝”** 来阻止电子邮件。这意味着，如果员工在 Android 设备上配置了其他电子邮件客户端，并且 ActiveSync ID 检测不起作用，则企业电子邮件会拒绝该员工的访问。

访问控制规则

Citrix Endpoint Management 的 Exchange ActiveSync 连接器提供了一种基于规则的方法，用于动态配置 Exchange ActiveSync 设备的访问控制。连接器访问控制规则由两部分组成：匹配表达式和所需的访问状态（允许或阻止）。可以针对给定的 Exchange ActiveSync 设备评估规则，以确定该规则是否适用于或匹配该设备。匹配表达式有多种类型；例如，规则可以匹配给定设备类型的所有设备、特定的 Exchange ActiveSync 设备 ID 或特定用户的所有设备，等等。

在规则列表中添加、删除和重新排列规则的任何时候，单击 **“取消”** 按钮会将规则列表恢复到首次打开时的状态。除非单击 **“保存”**，否则如果关闭“配置”工具，此窗口所做的任何更改都将丢失。

Citrix Endpoint Management 的 Exchange ActiveSync 连接器有三种类型的规则：本地规则、Citrix Endpoint Management 服务器规则（也称为 XDM 规则）和默认访问规则。

本地规则： 本地规则具有最高优先级：如果设备与本地规则匹配，则规则评估将停止。既不会咨询 Citrix Endpoint Management 服务器规则，也不会咨询默认访问规则。本地规则通过 **“配置”>“访问规则”>“本地规则”** 选项卡在 Exchange ActiveSync 连接器本地配置。支持匹配基于用户在给定 Active Directory 组中的成员身份。支持匹配基于以下字段的正则表达式：

- 活动同步设备 ID
- ActiveSync 设备类型
- 用户主体名称 (UPN)
- ActiveSync 用户代理（通常是设备平台或电子邮件客户端）

只要主要快照已完成并找到设备，您就可以添加普通规则或正则表达式规则。如果主要快照尚未完成，则只能添加正则表达式规则。

Citrix Endpoint Management 服务器规则： Citrix Endpoint Management 服务器规则是对外部 Citrix Endpoint Management 服务器的引用，该服务器提供有关托管设备的规则。Citrix Endpoint Management 服务器可以配置其自身的高级规则，这些规则根据 Citrix Endpoint Management 已知的属性（例如设备是否已越狱或设备是否具有禁用应用程序）来识别允许或阻止的设备。Citrix Endpoint Management 评估高级规则并生成一组允许或阻止的 ActiveSync 设备 ID，然后将其交付给 XenMobile Mail Manager。

默认访问规则： 默认访问规则的独特之处在于它可能匹配所有设备，并且始终最后进行评估。此规则是包罗万象的规则，这意味着如果给定设备不匹配本地或 Citrix Endpoint Management 服务器规则，则设备的所需访问状态由默认访问规则的所需访问状态决定。

- **默认访问 – 允许：** 任何不匹配本地或 Citrix Endpoint Management 服务器规则的设备都将被允许访问。

- **默认访问 – 阻止：** 任何不匹配本地或 Citrix Endpoint Management 服务器规则的设备都将被阻止访问。
- **默认访问 - 未更改：** 任何不匹配本地或 Citrix Endpoint Management 服务器规则的设备，其访问状态都不会被 Exchange ActiveSync 连接器以任何方式修改。如果设备已被 Exchange 置于隔离模式，则不采取任何操作。例如，将设备从隔离模式中移除的唯一方法是使用显式本地或 XDM 规则覆盖隔离。

关于规则评估

对于 Exchange 报告给 Exchange ActiveSync 连接器的每个设备，规则按从高到低的优先级顺序进行评估，如下所示：

- 本地规则
- Citrix Endpoint Management 服务器规则
- 默认访问规则

找到匹配项后，评估停止。例如，如果本地规则匹配给定设备，则不会根据任何 Citrix Endpoint Management 服务器规则或默认访问规则评估该设备。这在给定规则类型中也适用。例如，如果本地规则列表中给定设备有多个匹配项，则在找到第一个匹配项时，评估停止。

当设备属性更改、设备添加或移除，或者规则本身更改时，Exchange ActiveSync 连接器会重新评估当前定义的规则集。主要快照以可配置的间隔获取设备属性更改和移除。次要快照以可配置的间隔获取新设备。

Exchange ActiveSync 也有管理访问的规则。了解这些规则在 Exchange ActiveSync 连接器上下文中的工作方式非常重要。Exchange 可以配置三级规则：个人豁免、设备规则和组织设置。Exchange ActiveSync 连接器通过以编程方式发出远程 PowerShell 请求来影响个人豁免列表，从而实现访问控制自动化。这些是与给定邮箱关联的允许或阻止的 Exchange ActiveSync 设备 ID 列表。部署后，Exchange ActiveSync 连接器有效地接管了 Exchange 中豁免列表功能的管理。请参阅 Microsoft 文章：使用 Exchange 和 Configuration Manager。

在为同一字段定义了多个规则的情况下，分析非常有用。您可以排查规则之间的关系。您从规则字段的角度进行分析。例如，规则根据匹配的字段进行分组分析，例如 ActiveSync 设备 ID、ActiveSync 设备类型、用户、用户代理。

规则术语

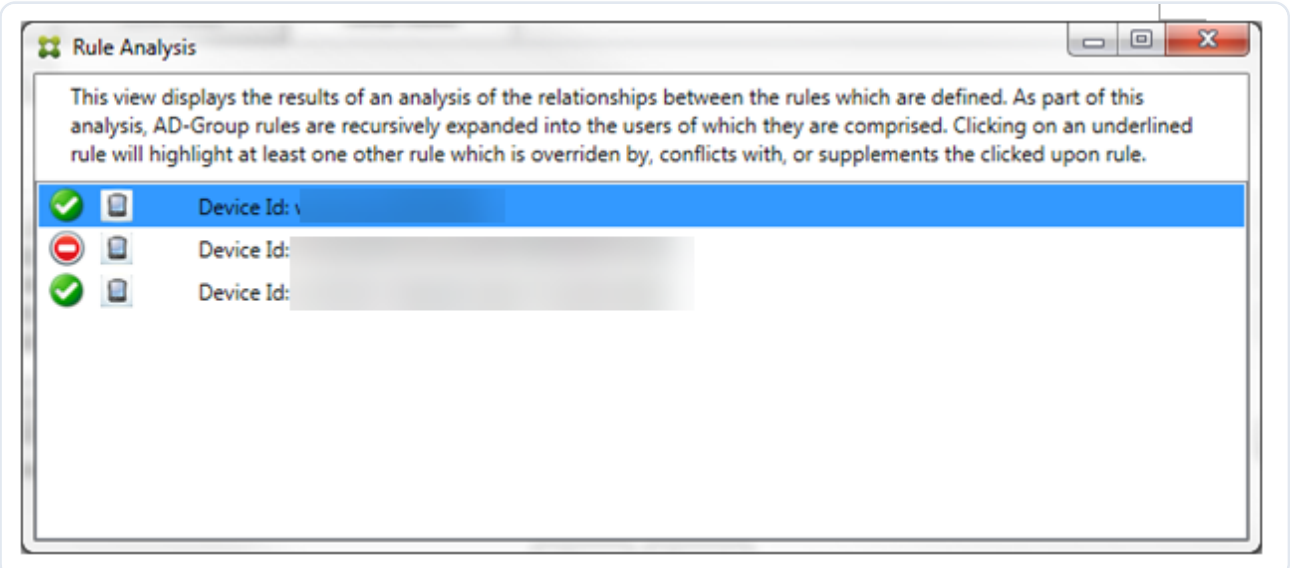
- **覆盖规则：** 当多个规则可以应用于同一设备时，就会发生覆盖。由于规则是按列表中的优先级进行评估的，因此后面可能适用的规则实例可能永远不会被评估。

- **冲突规则：** 当多个规则可以应用于同一设备但访问权限（允许/阻止）不匹配时，就会发生冲突。如果冲突规则不是正则表达式规则，则冲突总是隐式地意味着覆盖。
- **补充规则：** 当多个规则是正则表达式规则时，就会发生补充，因此可能需要确保两个（或更多）正则表达式可以合并为一个正则表达式规则，或者没有重复功能。补充规则也可能在其访问权限（允许/阻止）方面发生冲突。
- **主规则：** 主规则是对话框中已单击的规则。该规则通过其周围的实线边框在视觉上表示。该规则还将有一个或两个向上或向下的绿色箭头。如果箭头向上，则表示主规则之前存在辅助规则。如果箭头向下，则表示主规则之后存在辅助规则。任何时候只能有一个主规则处于活动状态。
- **辅助规则：** 辅助规则通过覆盖、冲突或补充关系与主规则以某种方式相关联。这些规则通过其周围的虚线边框在视觉上表示。对于每个主规则，可以有一个到多个辅助规则。单击任何带下划线的条目时，突出显示的辅助规则始终是从主规则的角度来看的。例如，辅助规则被主规则覆盖，或者辅助规则在其访问权限上与主规则冲突，或者辅助规则补充了主规则。

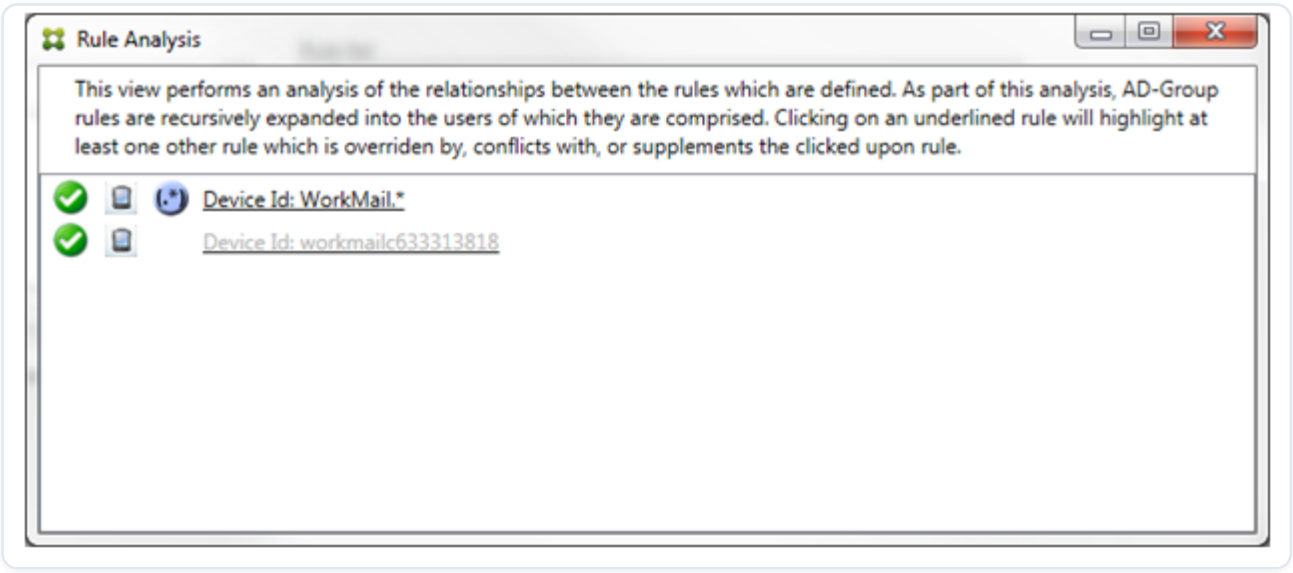
规则类型在“规则分析”对话框中的显示方式

当没有冲突、覆盖或补充时，**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影响；例如，会出现正常的选中项目视觉效果。

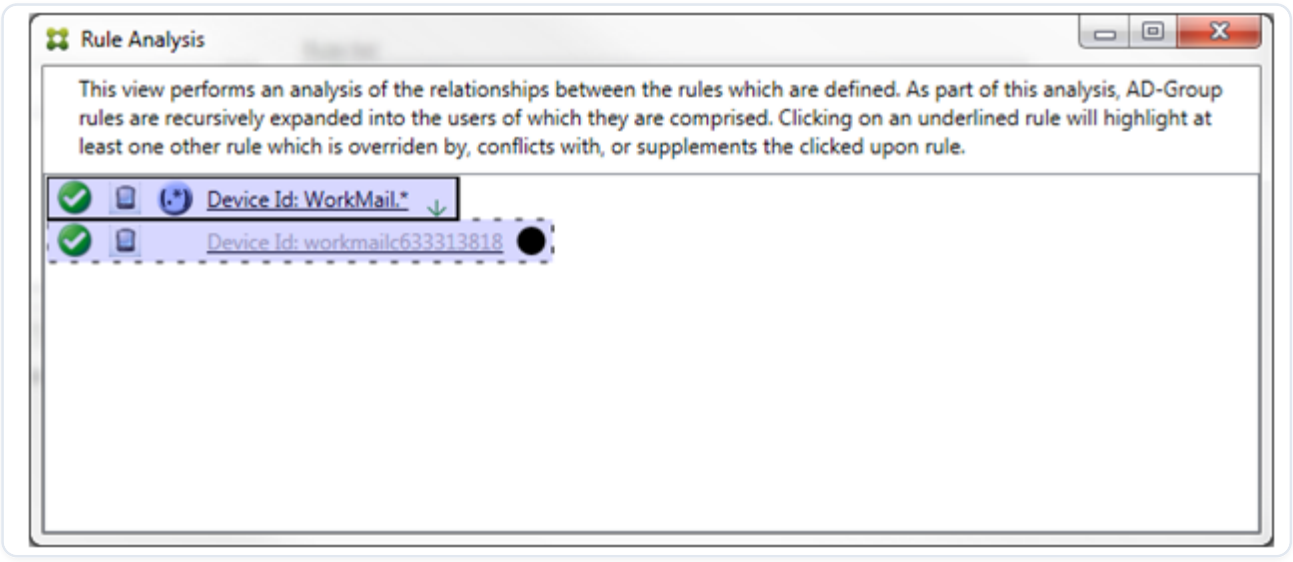
规则分析窗口有一个复选框，选中后，它将仅显示冲突、覆盖、冗余或补充的规则。



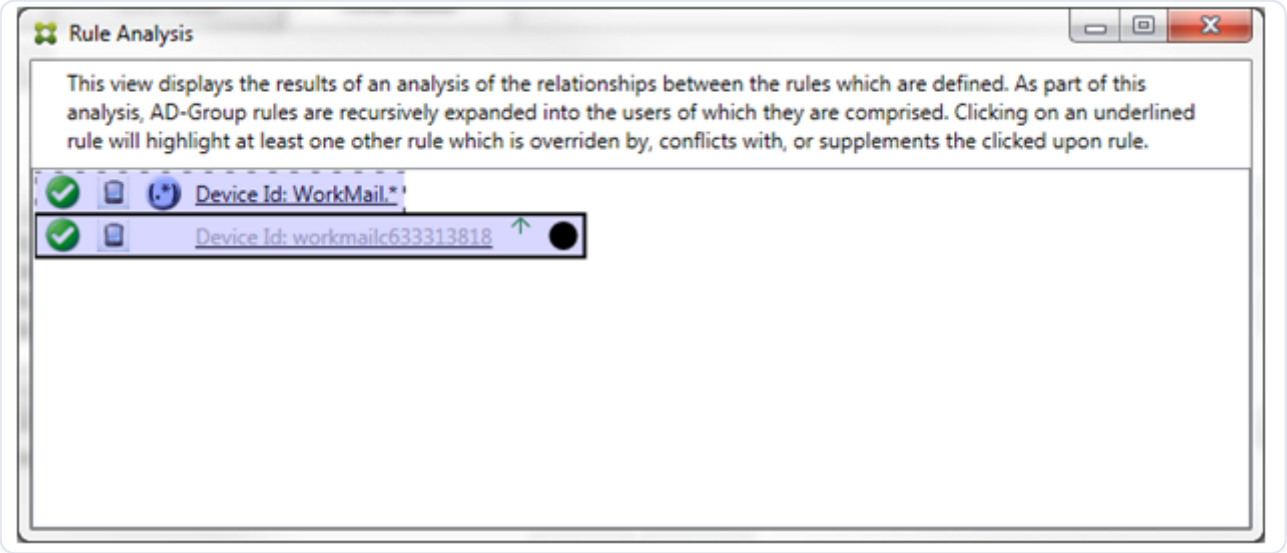
当发生覆盖时，至少有两个规则会带下划线：主规则和辅助规则。至少有一个辅助规则以较浅的字体显示，表示该规则已被更高优先级的规则覆盖。您可以单击被覆盖的规则，以找出哪些规则覆盖了该规则。无论何时，只要被覆盖的规则因其是主规则或辅助规则而被突出显示，其旁边就会出现一个黑圈，作为该规则不活动的进一步视觉指示。例如，在单击规则之前，对话框显示如下：



当您单击最高优先级的规则时，对话框显示如下：

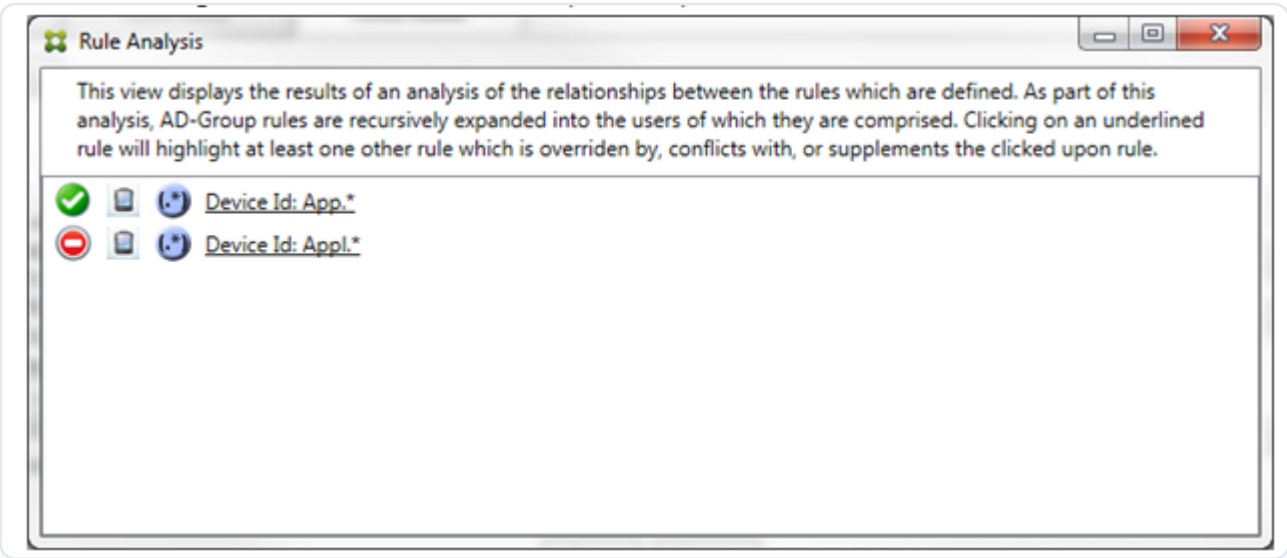


在此示例中，正则表达式规则 `WorkMail.*` 是主规则（由实线边框表示），普通规则 `workmailc633313818` 是辅助规则（由虚线边框表示）。辅助规则旁边的黑点是一个视觉提示，进一步表明该规则不活动（永远不会被评估），因为它前面有一个更高优先级的正则表达式规则。单击被覆盖的规则后，对话框显示如下：

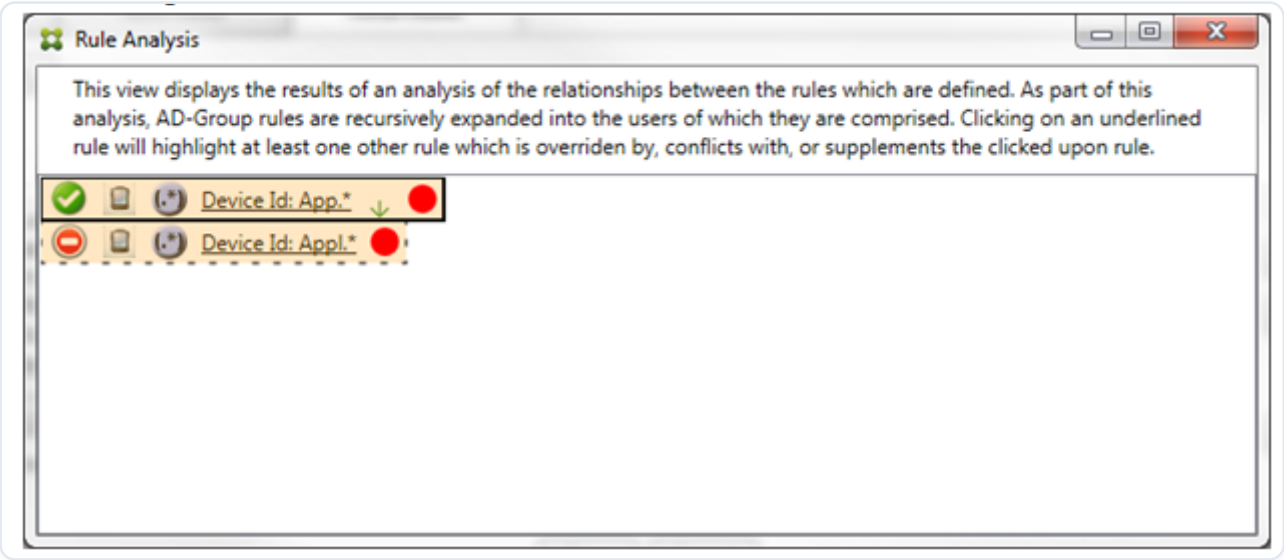


在前面的示例中，正则表达式规则 `WorkMail.*` 是辅助规则（由虚线边框指示），普通规则 `workmailc633313818` 是主要规则（由实线边框指示）。对于这个简单的示例，差异不大。有关更复杂的示例，请参阅本主题后面介绍的复杂表达式示例。在定义了许多规则的场景中，单击被覆盖的规则将快速识别是哪个或哪些规则覆盖了它。

当发生冲突时，至少有两条规则会带下划线，即主要规则和辅助规则（或多条辅助规则）。冲突的规则由红点指示。仅相互冲突的规则只有在定义了两条或更多正则表达式规则时才可能出现。在所有其他冲突场景中，不仅会存在冲突，还会存在覆盖。在简单示例中单击任一规则之前，对话框显示如下：

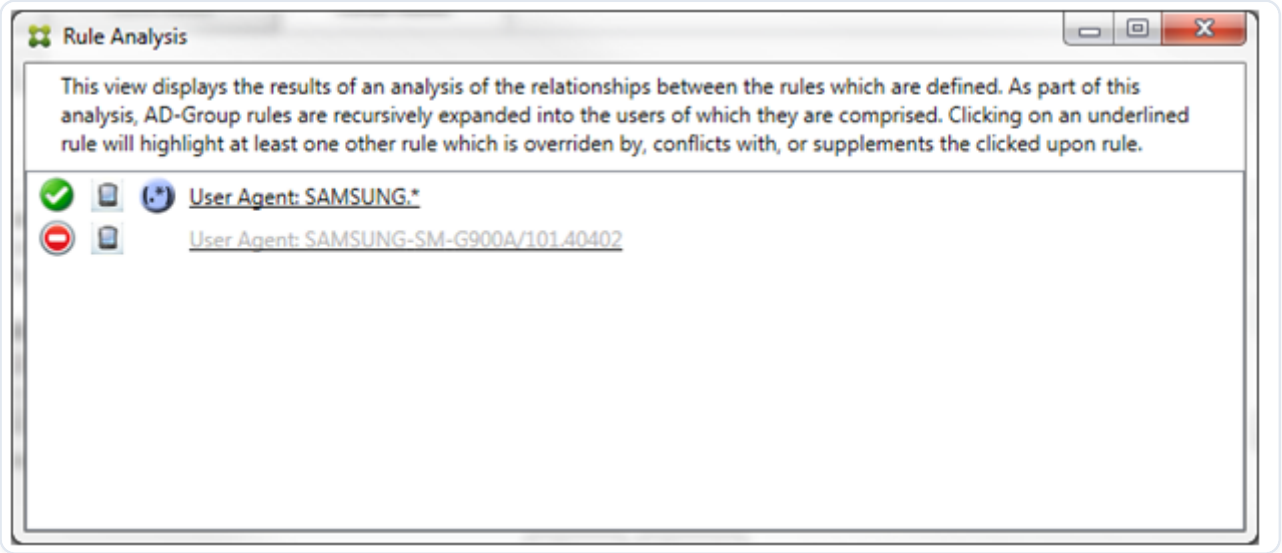


通过检查这两条正则表达式规则，可以明显看出，第一条规则允许所有设备 ID 包含“App”的设备，第二条规则拒绝所有设备 ID 包含 `Appl` 的设备。此外，即使第二条规则拒绝所有设备 ID 包含 `Appl` 的设备，但由于允许规则的优先级更高，因此符合该匹配条件的设备永远不会被拒绝。单击第一条规则后，对话框显示如下：



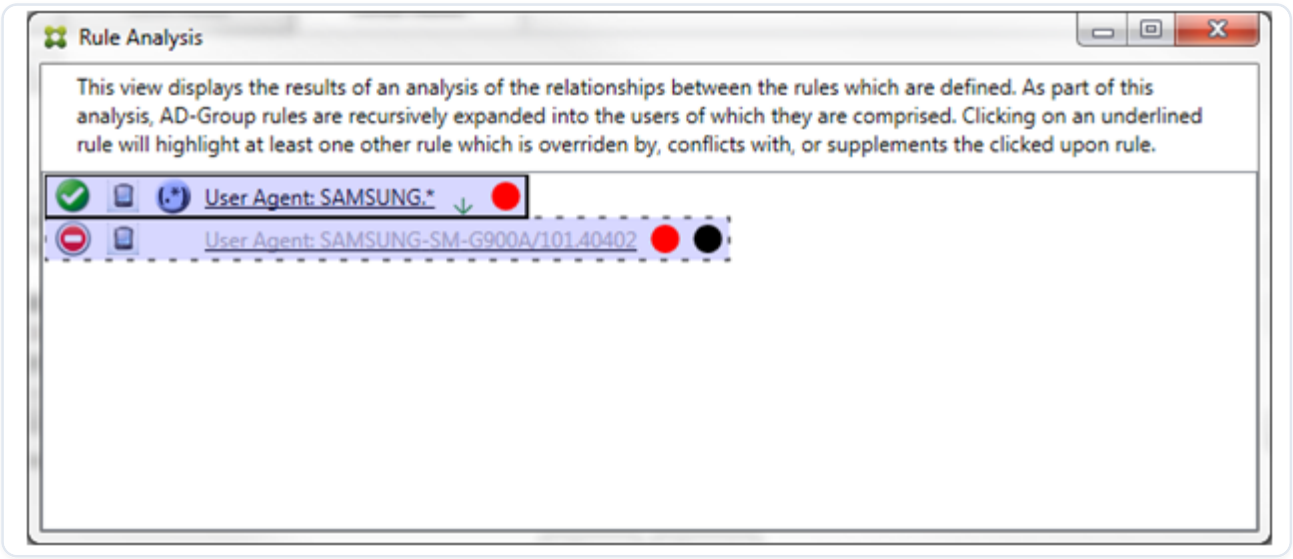
在前面的场景中，主要规则（正则表达式规则 `App.*`）和辅助规则（正则表达式规则 `Appl.*`）都以黄色突出显示。这只是一个视觉警告，提醒您已将多条正则表达式规则应用于单个可匹配字段，这可能意味着冗余问题或更严重的问题。

在同时存在冲突和覆盖的场景中，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.*`）都以黄色突出显示。这只是一个视觉警告，提醒您已将多条正则表达式规则应用于单个可匹配字段，这可能意味着冗余问题或更严重的问题。



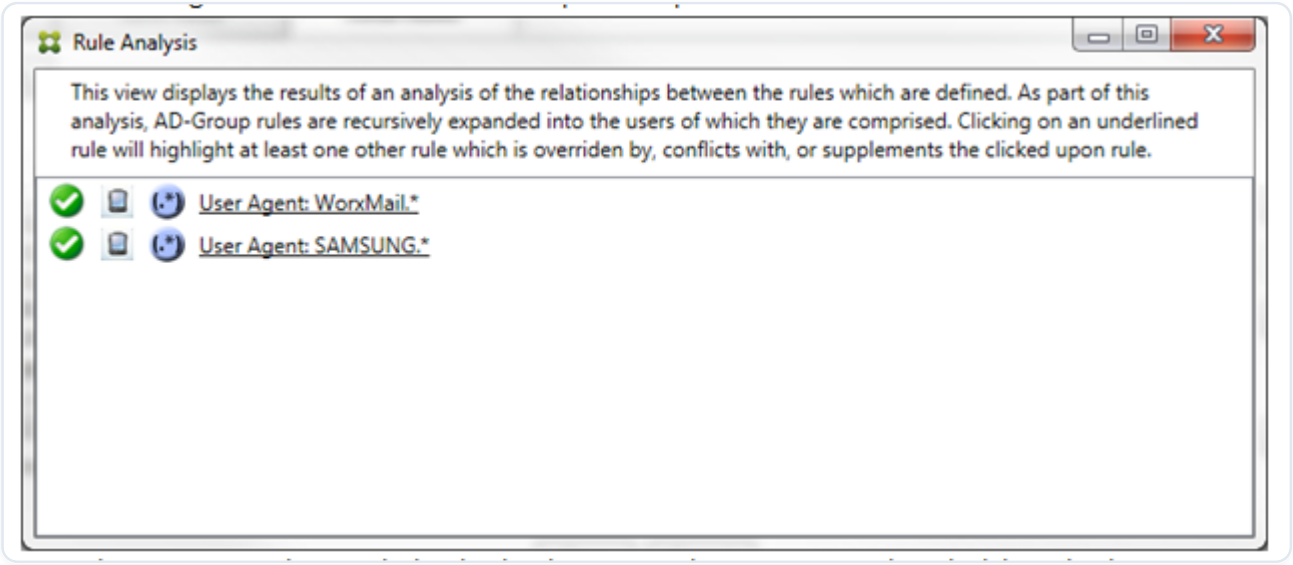
在前面的示例中很容易看出，第一条规则（正则表达式规则 `SAMSUNG.*`）不仅覆盖了下一条规则（普通规则 `SAMSUNG-SM-G900A/101.40402`），而且这两条规则的访问权限不同（主要规则指定“允许”，辅助规则指定“阻止”）。第二条规则（普通规则 `SAMSUNG-SM-G900A/101.40402`）以较浅的文本显示，表示它已被覆盖，因此处于非活动状态。

单击正则表达式规则后，对话框显示如下：

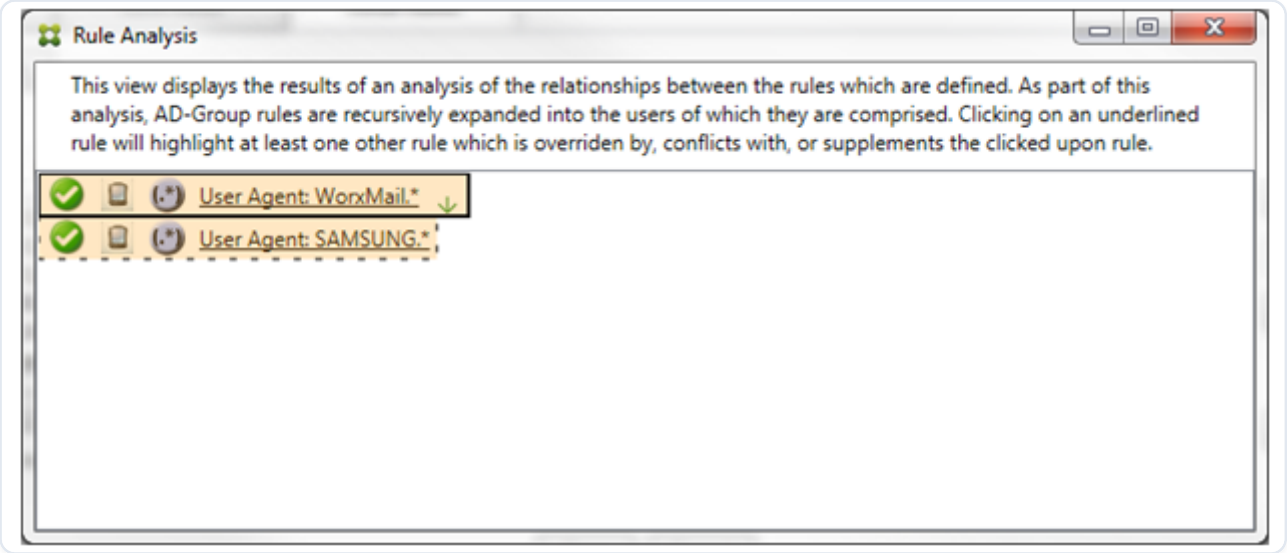


主要规则（正则表达式规则 `SAMSUNG.*`）后面跟着一个红点，表示其访问状态与一个或多个辅助规则冲突。辅助规则（普通规则 `SAMSUNG-SM-G900A/101.40402`）后面跟着一个红点，表示其访问状态与主要规则冲突。该规则后面还跟着一个黑点，表示它已被覆盖，因此处于非活动状态。

至少有两条规则会带下划线，即主要规则和辅助规则（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，它们会以黄色叠加层指示。在简单示例中单击任一规则之前，对话框显示如下：



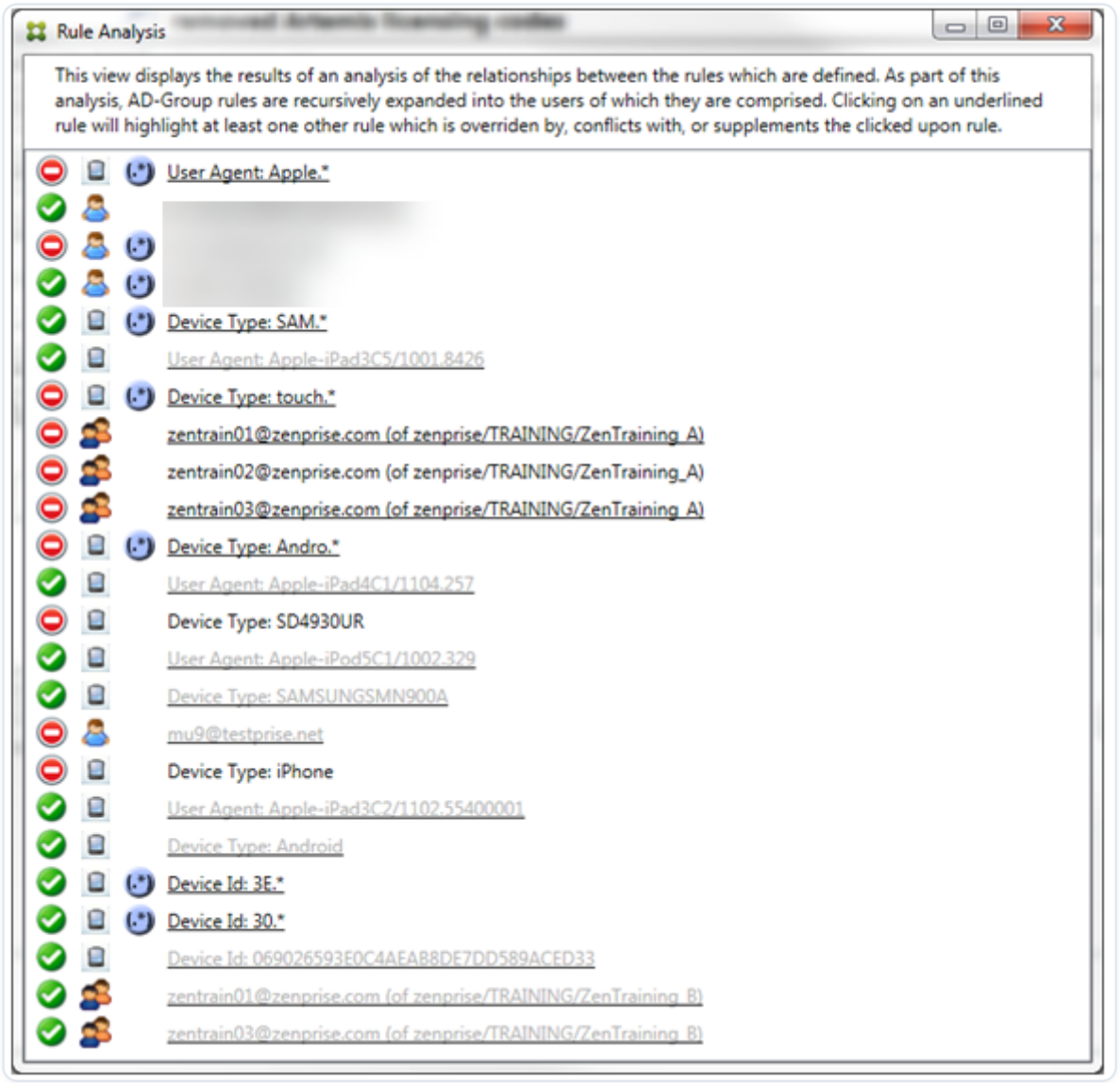
目视检查很容易发现，这两个规则都是正则表达式规则，并且都已应用于 Citrix Endpoint Management 的 Exchange ActiveSync 连接器中的 ActiveSync 设备 ID 字段。单击第一个规则后，对话框如下所示：



主规则（正则表达式规则 `WorkMail.*`）以黄色叠加层突出显示，表示至少存在一个辅助规则，该辅助规则也是正则表达式。辅助规则（正则表达式规则 `SAMSUNG.*`）以黄色叠加层突出显示，表示它和主规则都是应用于 Exchange ActiveSync 连接器中同一字段的正则表达式规则。在这种情况下，该字段是 ActiveSync 设备 ID。正则表达式可能重叠，也可能不重叠。您需要自行决定您的正则表达式是否正确编写。

复杂表达式示例

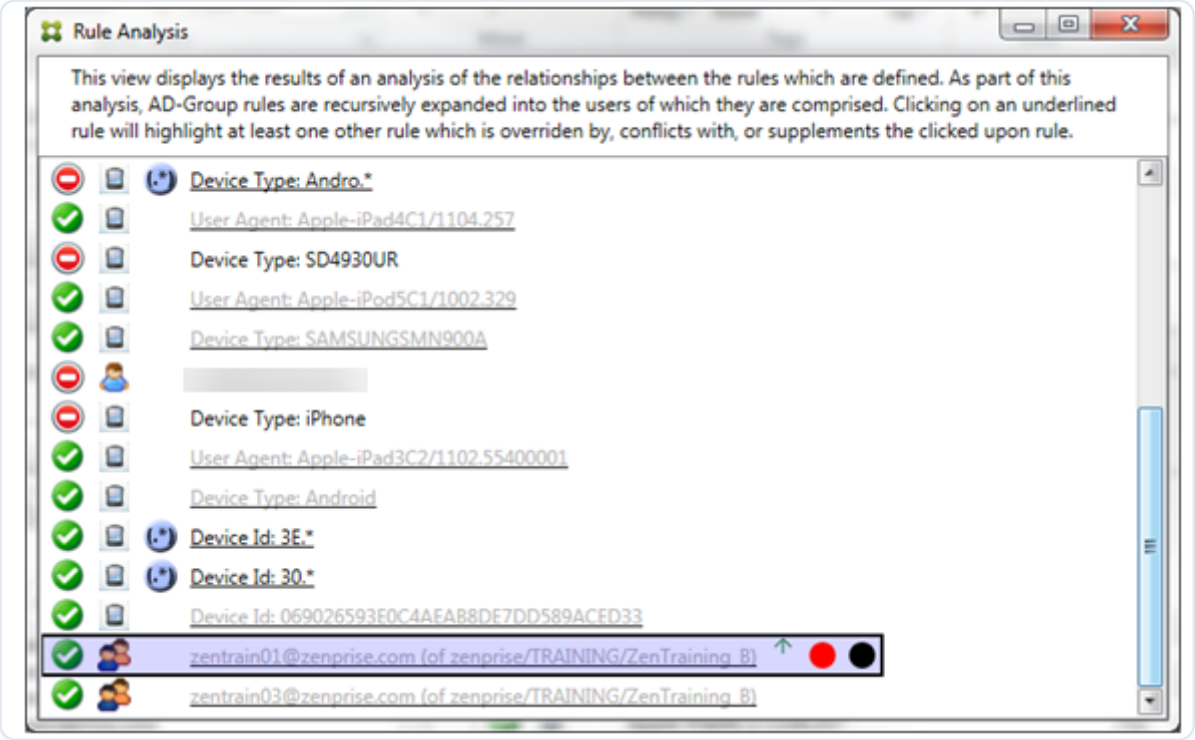
可能会出现许多潜在的覆盖、冲突或补充，因此无法给出所有可能场景的示例。以下示例讨论了不应做的事情，同时也说明了规则分析可视化构造的全部功能。以下图中的大多数项目都带有下划线。许多项目以较浅的字体呈现，这表示相关规则已以某种方式被更高优先级的规则覆盖。列表中还包含一些正则表达式规则，如  图标所示。



如何分析覆盖

要查看哪些规则覆盖了特定规则，请单击该规则。

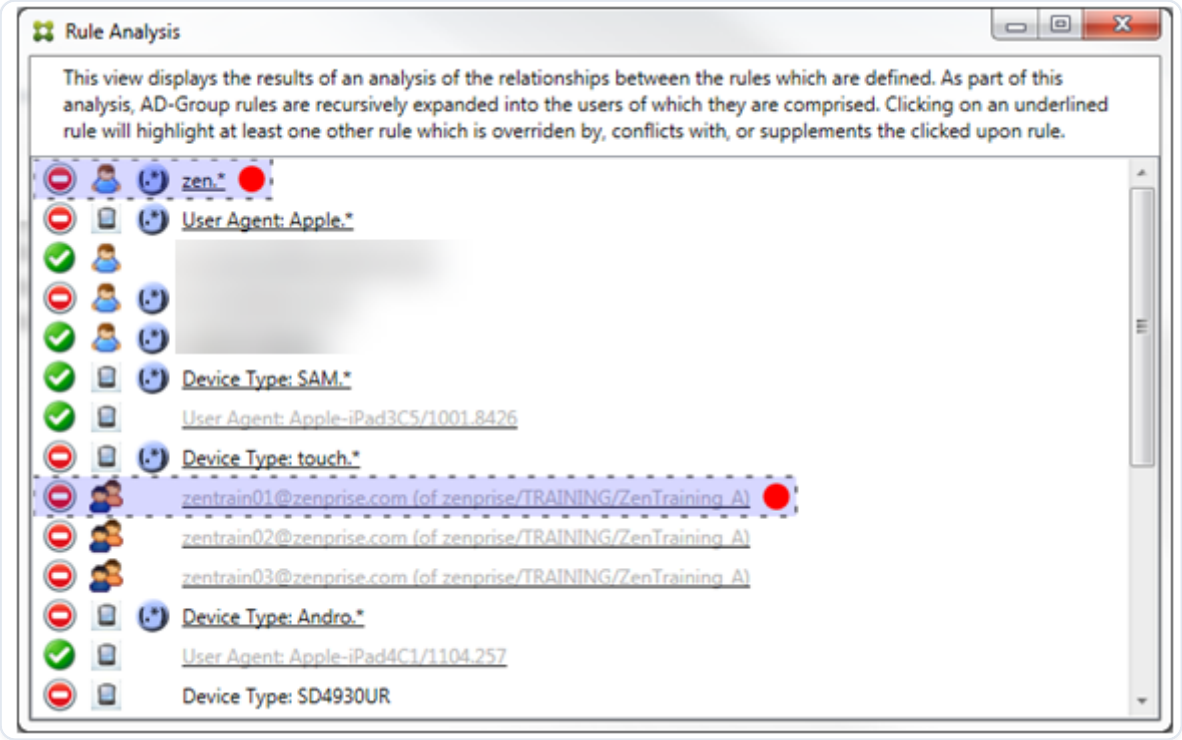
示例 1： 本示例探讨了 `zentrain01@zenprise.com` 被覆盖的原因。



主规则（AD 组规则 `zenprise/TRAINING/ZenTraining B`，其中 `zentrain01@zenprise.com` 是成员）具有以下特征：

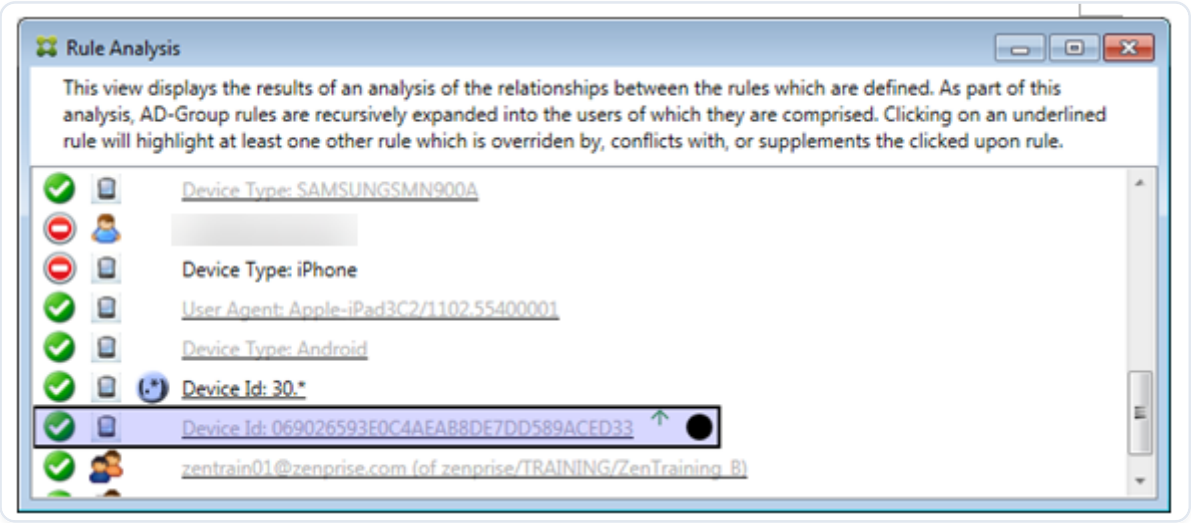
- 以蓝色突出显示并具有实心边框。
- 具有向上指向的绿色箭头（表示所有辅助规则都位于其上方）。
- 后面跟着一个红色圆圈和一个黑色圆圈，分别表示一个或多个辅助规则与其访问权限冲突，以及主规则已被覆盖因此处于非活动状态。

向上滚动时，您会看到以下内容：



在这种情况下，有两个辅助规则覆盖了主规则：正则表达式规则 `zen.*` 和普通规则 `zentrain01@zenprise.com` (属于 `zenprise/TRAINING/ZenTraining A`)。对于后一个辅助规则，发生的情况是 Active Directory 组规则 `ZenTraining A` 包含用户 `zentrain01@zenprise.com`，并且 Active Directory 组规则 `ZenTraining B` 也包含用户 `zentrain01@zenprise.com`。然而，由于辅助规则的优先级高于主规则，因此主规则已被覆盖。主规则的访问权限是“允许”，并且由于两个辅助规则的访问权限都是“阻止”，因此所有规则后面都带有一个红色圆圈，以进一步指示访问冲突。

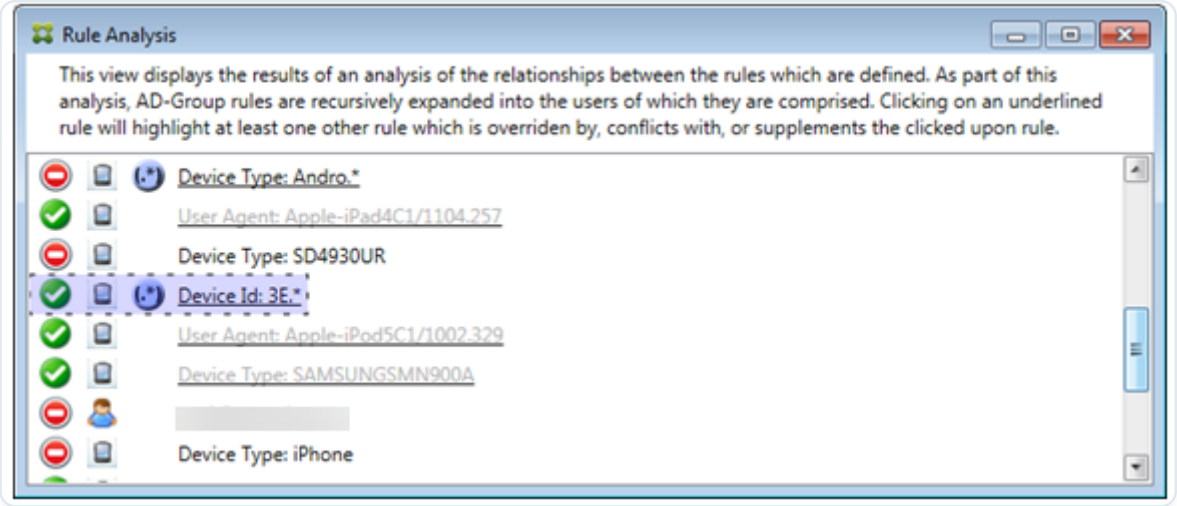
示例 2： 此示例显示了为什么 ActiveSync 设备 ID 为 `069026593E0C4AEAB8DE7DD589ACED33` 的设备已被覆盖：



主规则（普通设备 ID 规则 `069026593E0C4AEAB8DE7DD589ACED33`）具有以下特征：

- 以蓝色突出显示并具有实心边框。

- 有一个向上指向的绿色箭头（表示辅助规则在其上方）。
- 后面跟着一个黑色圆圈，表示辅助规则已覆盖主规则，因此处于非活动状态。

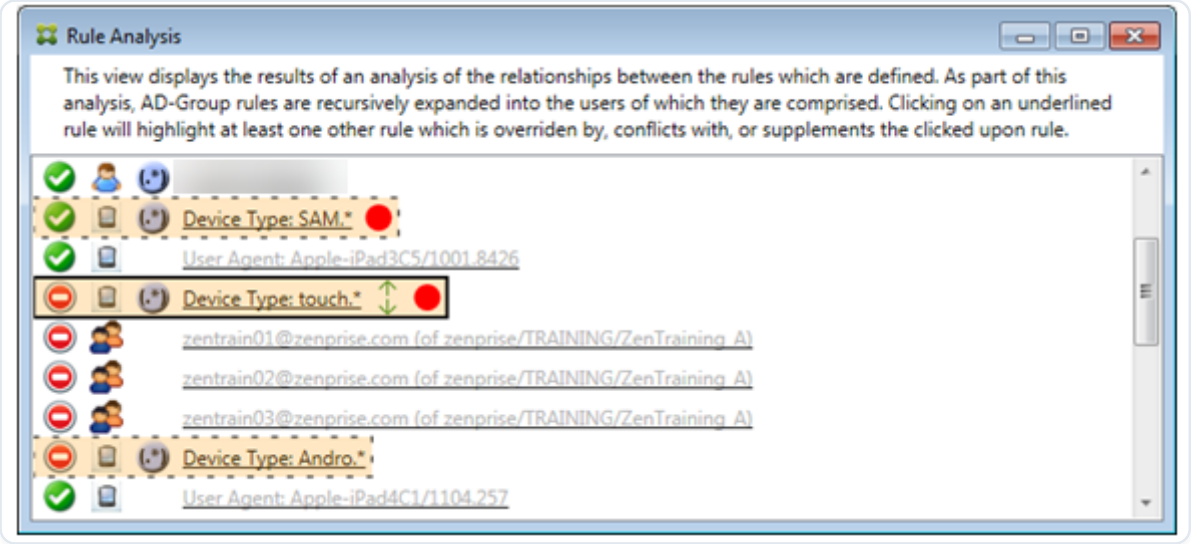


在这种情况下，单个辅助规则覆盖了主规则：正则表达式 ActiveSync 设备 ID 规则是 `3E.*`。因为正则表达式 `3E.*` 将匹配 `069026593E0C4AEAB8DE7DD589ACED33`，所以主规则将永远不会被评估。

如何分析补充和冲突

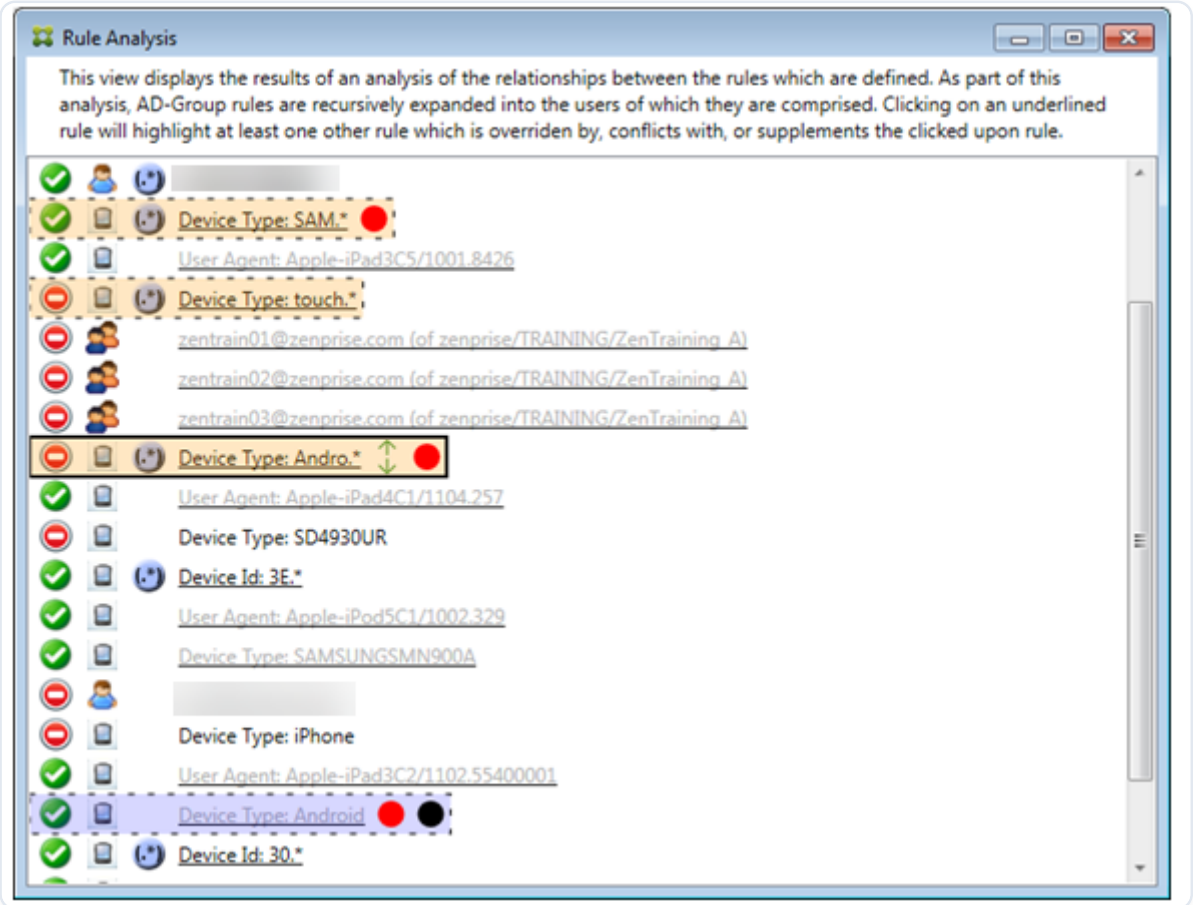
在这种情况下，主规则是正则表达式 ActiveSync 设备类型规则 `touch.*`。其特征如下：

- 由带有黄色叠加层的实心边框指示，作为警告，表示有多个正则表达式规则作用于特定规则字段，在本例中是 ActiveSync 设备类型。
- 两个箭头分别向上和向下，表示至少有一个优先级较高的辅助规则和至少一个优先级较低的辅助规则。
- 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**，这与主规则的访问权限 **阻止** 冲突。
- 有两个辅助规则：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.*`。
- 这两个辅助规则都用破折号边框表示它们是辅助规则。
- 这两个辅助规则都用黄色覆盖，表示它们也应用于 ActiveSync 设备类型的规则字段。
- 在这种情况下，您必须确保其正则表达式规则不是冗余的。



如何进一步分析规则

此示例探讨了规则关系始终从主规则的角度出发。前面的示例展示了如何单击应用于设备类型规则字段的正则表达式规则，其值为 `touch.*`。单击辅助规则 `Andro.*` 会显示一组不同的突出显示的辅助规则。

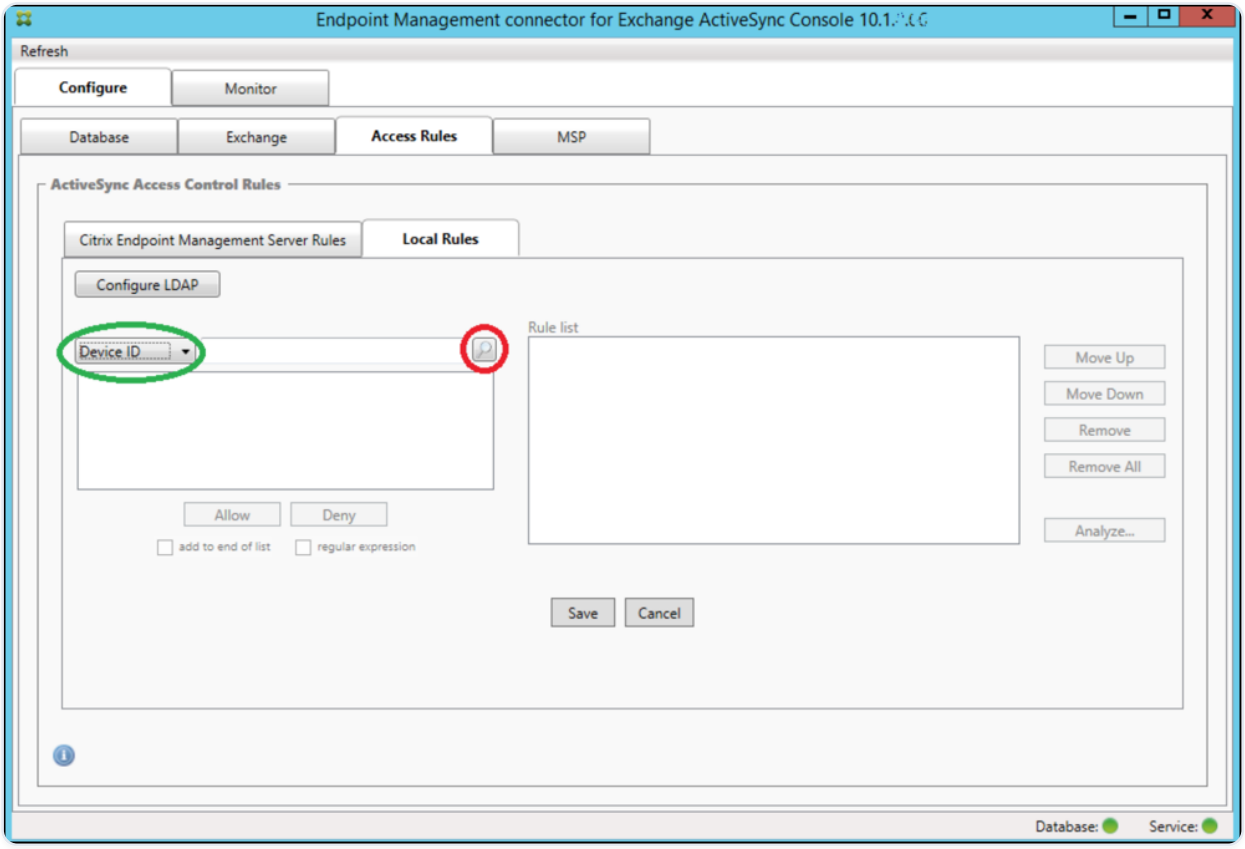


该示例显示了一个包含在规则关系中的被覆盖规则。此规则是正常的 ActiveSync 设备类型规则 `Android`，它已被覆盖（由变淡的字体和旁边的黑圈表示），并且其访问权限与主规则正则表达式 ActiveSync 设备类型规则 `Andro.*` 冲突。该规则在被点击之前曾是辅助规则。在前面的示例中，

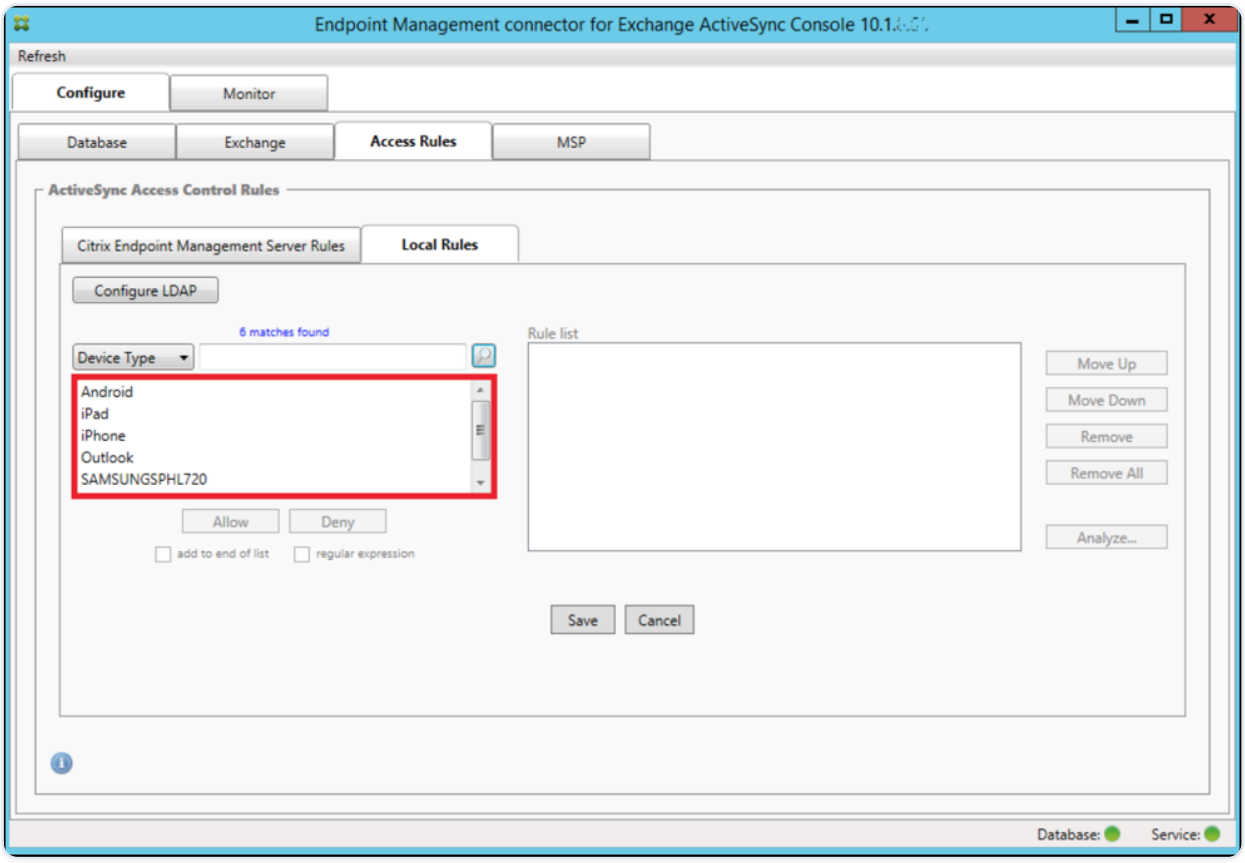
正常的 ActiveSync 设备类型规则 `Android` 未显示为辅助规则，因为从当时的主规则（正则表达式 ActiveSync 设备类型规则 `touch.*`）的角度来看，它与主规则无关。

配置普通表达式本地规则

1. 单击“**访问规则**”选项卡。



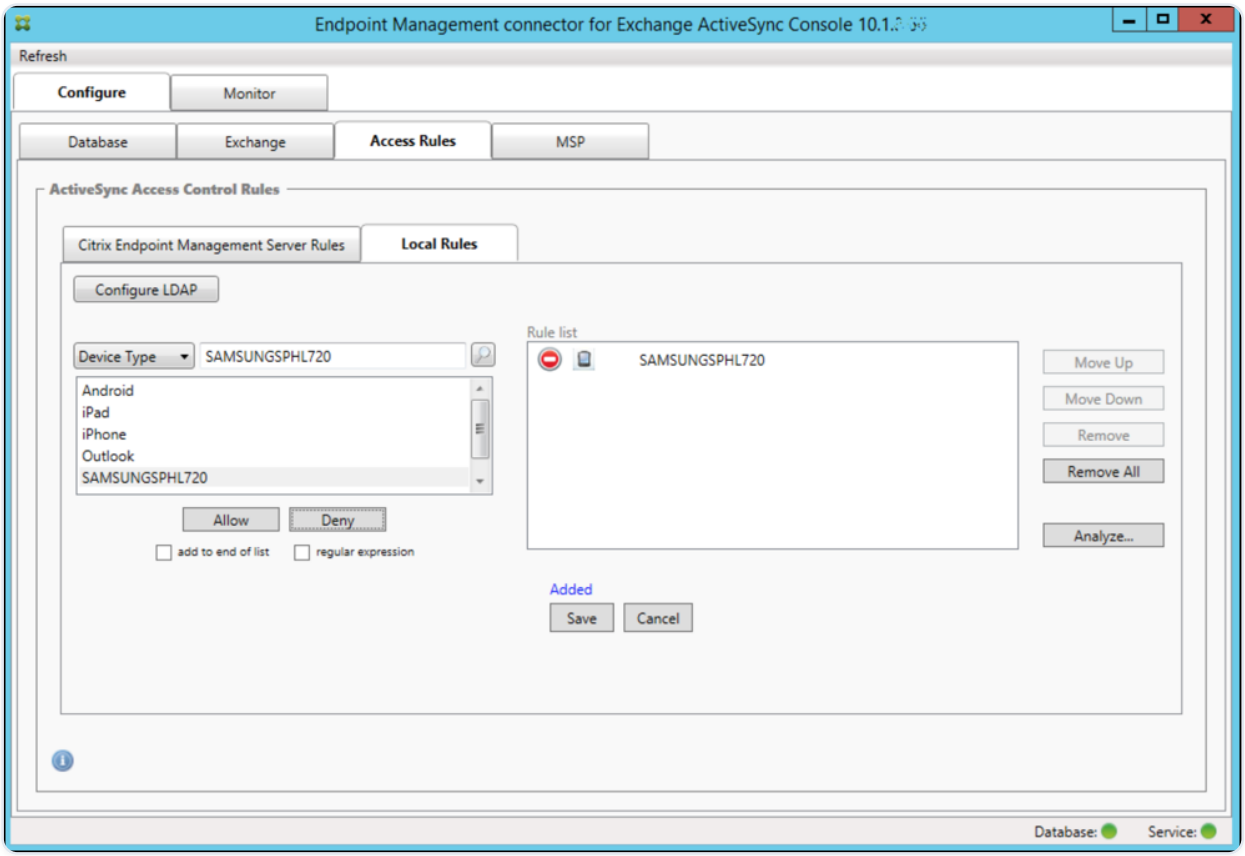
2. 在“**设备 ID**”列表中，选择要为其创建本地规则的字段。
3. 单击放大镜图标以显示所选字段的所有唯一匹配项。在此示例中，已选择“**设备类型**”字段，并且选项显示在以下列表框中：



4. 点击结果列表框中的一个项目，然后点击以下选项之一：

   - **允许**表示 Exchange 将配置为允许所有匹配设备的 ActiveSync 流量。
   - **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，设备类型为 SamsungSPhl720 的所有设备都将被拒绝访问。

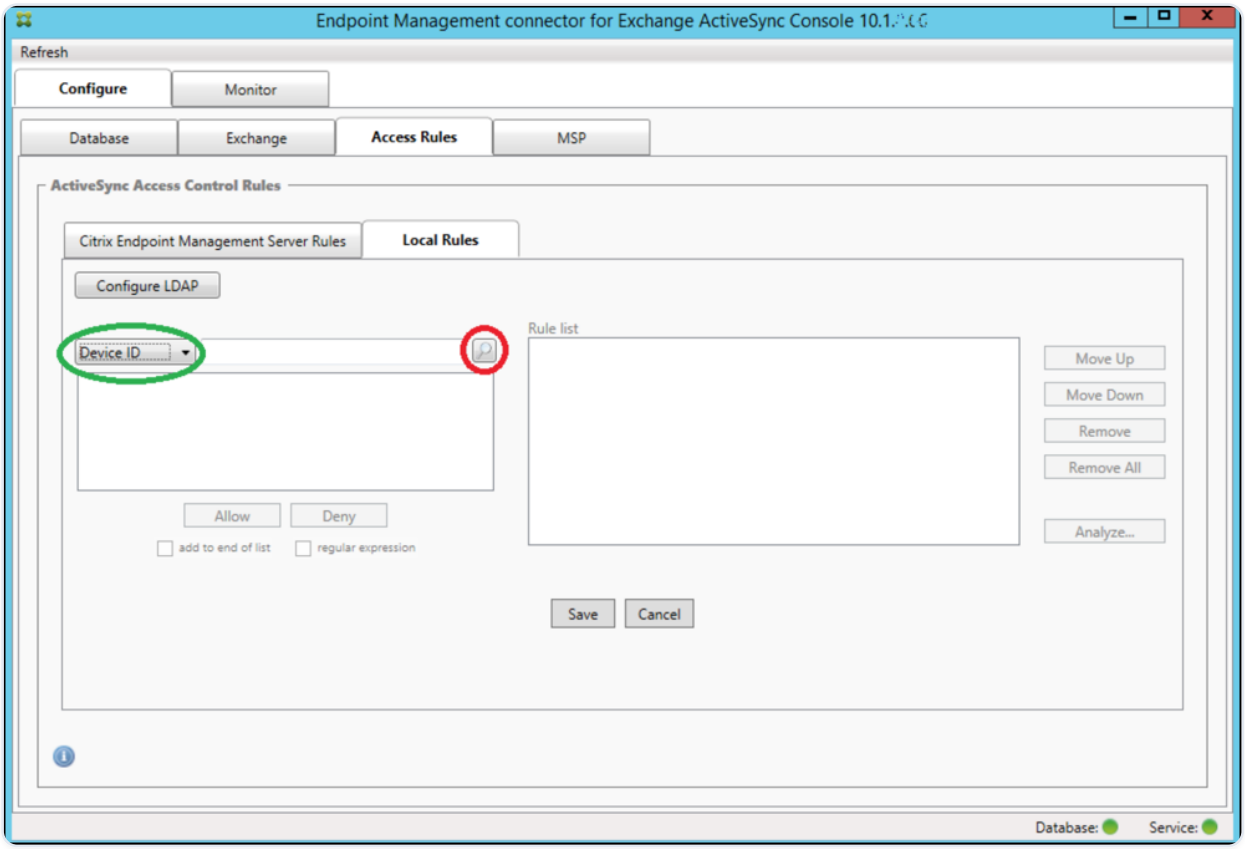


添加正则表达式

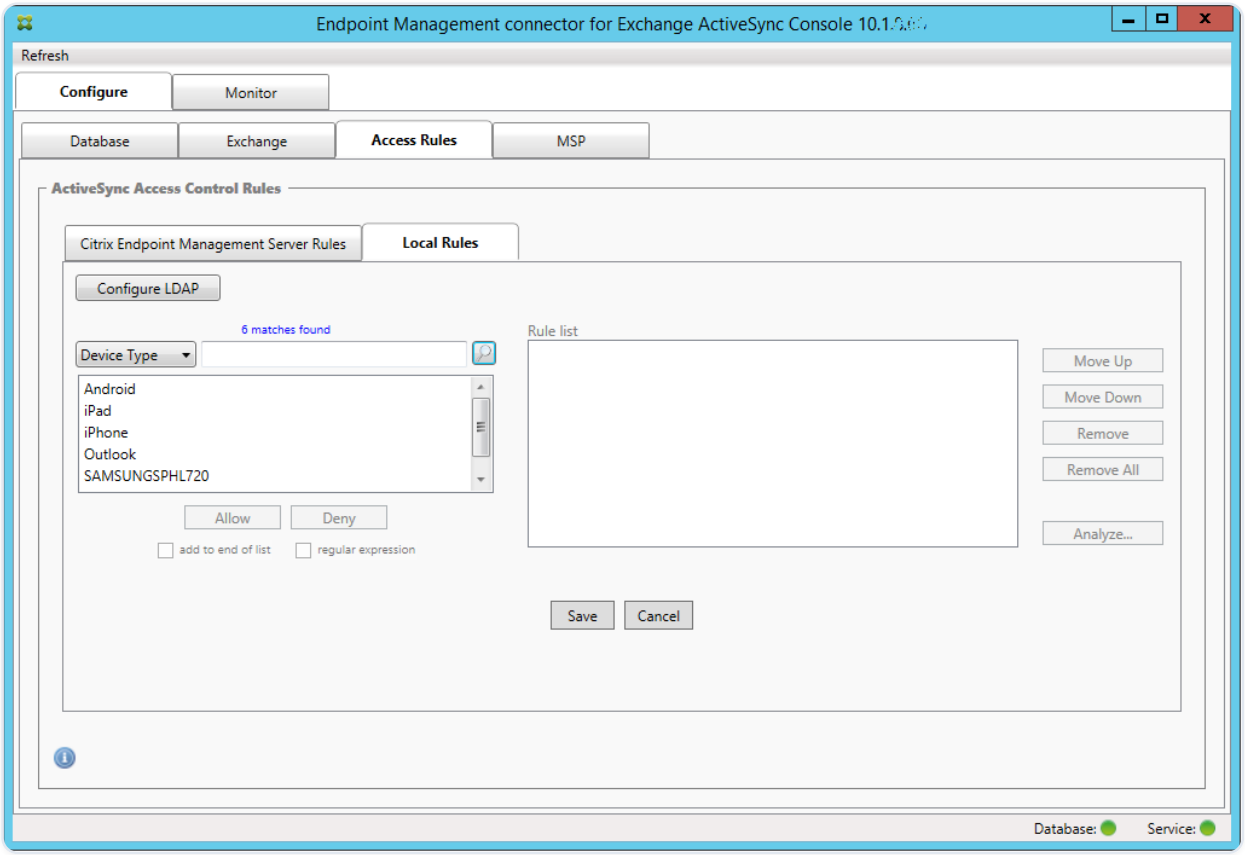
正则表达式本地规则可以通过其旁边的图标来区分 -  。要添加正则表达式规则，您可以从给定字段的结果列表中现有值构建正则表达式规则（只要已完成主要快照），或者您可以直接输入所需的正则表达式。

从现有字段值构建正则表达式

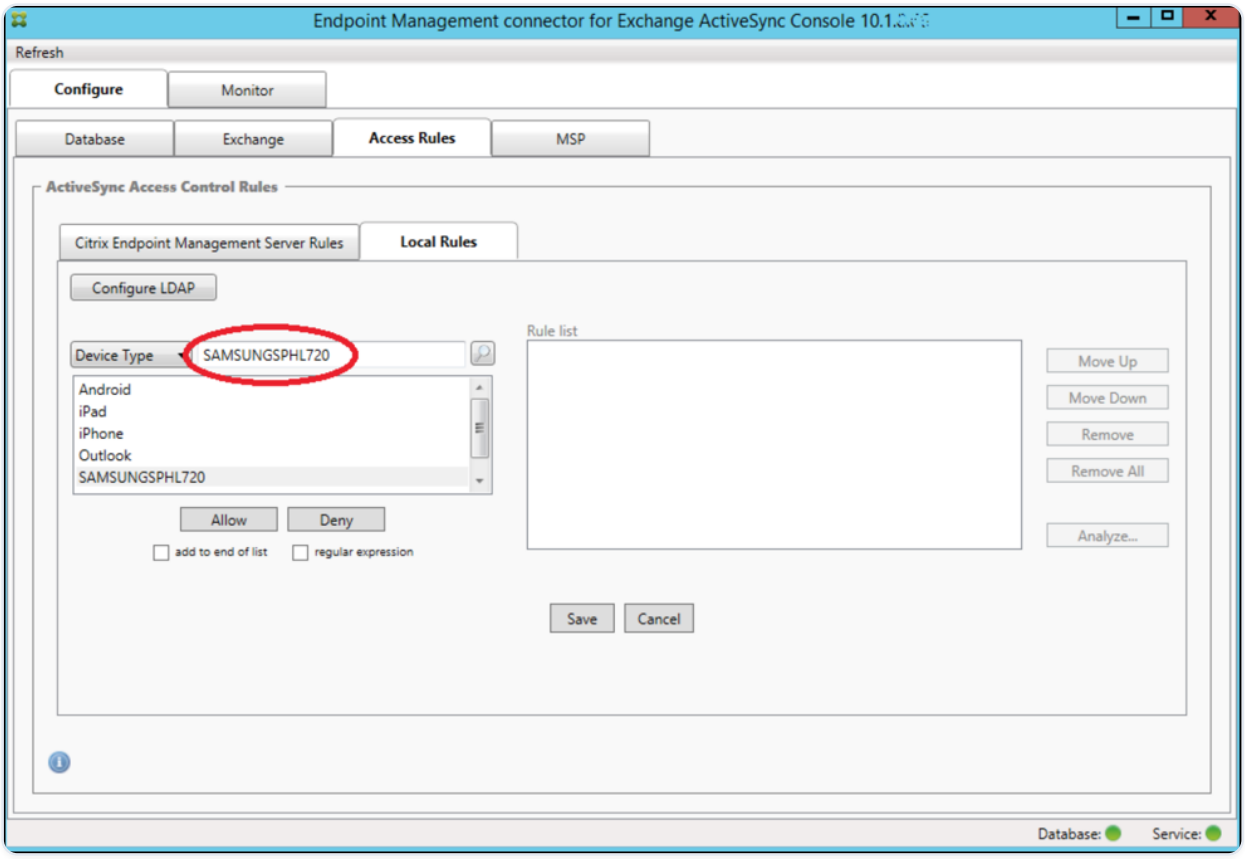
1. 点击**访问规则**选项卡。



2. 在**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. 点击放大镜图标以显示所选字段的所有唯一匹配项。在此示例中，已选择**设备类型**字段，并且选项显示在以下列表框中：



4. 点击结果列表中的一个项目。在此示例中，已选择 **SAMSUNGSPHL720** 并显示在**设备类型**旁边的文本框中。



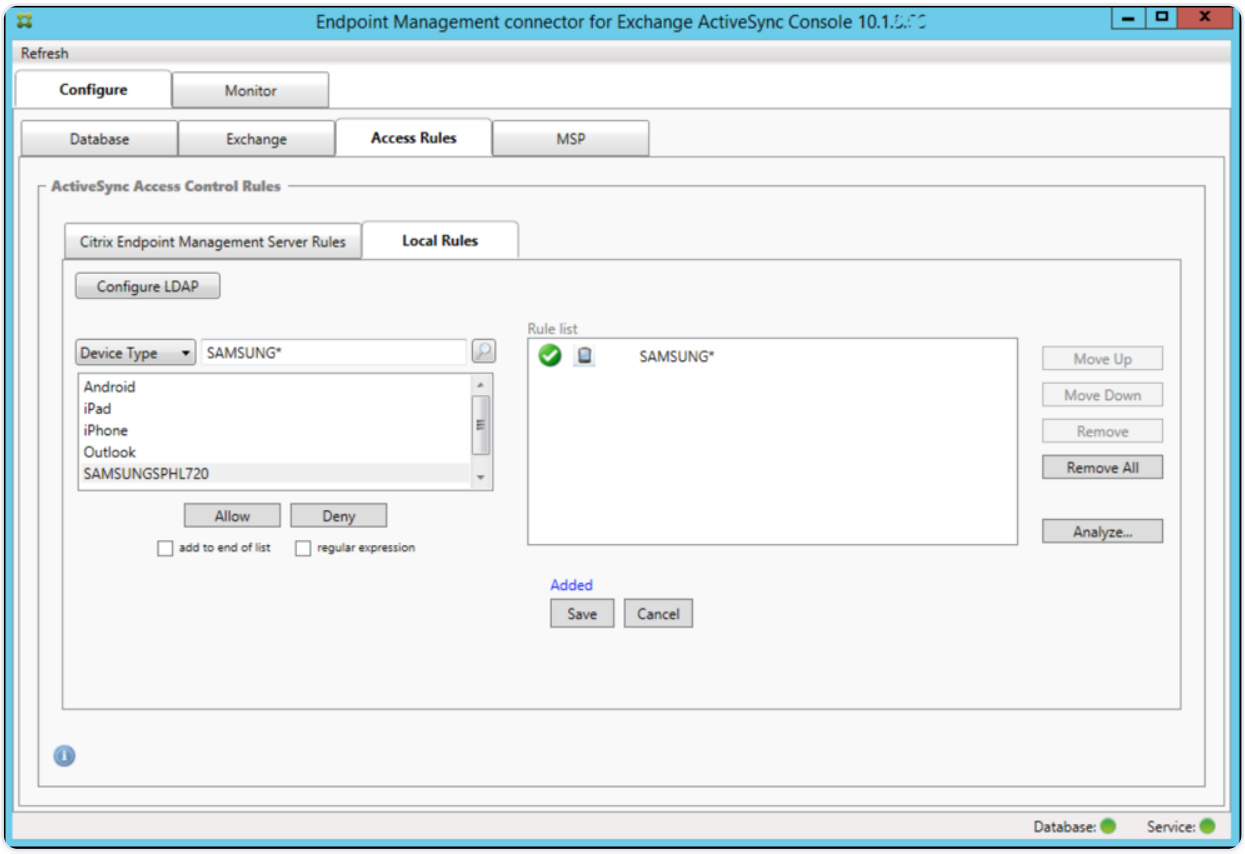
5. 要允许设备类型值中包含“Samsung”的所有设备类型，请按照以下步骤添加正则表达式规则：

   a. 单击选定项目文本框内。

   b. 将文本从 **SAMSUNGSPHL720** 更改为 **SAMSUNG.***。

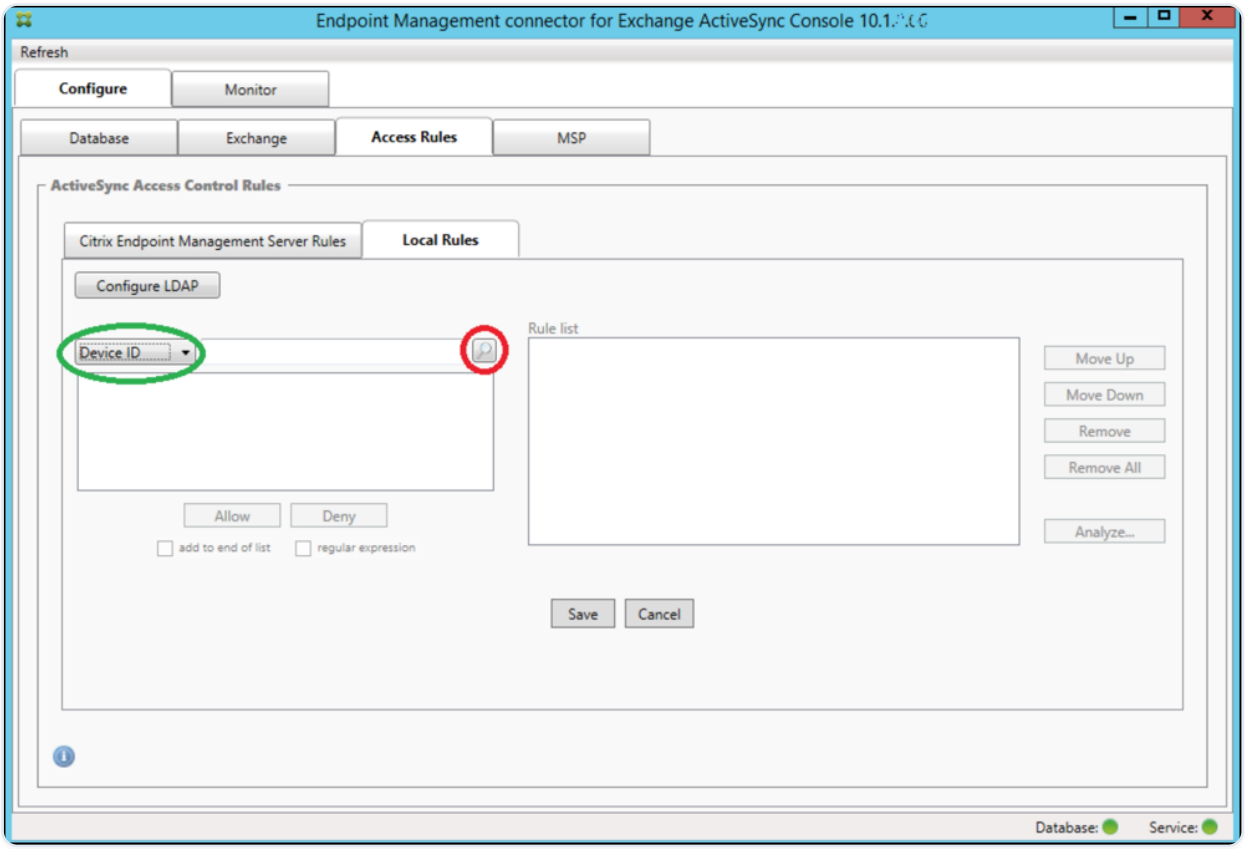
   c. 确保选中正则表达式复选框。

   d. 单击“**允许**”。

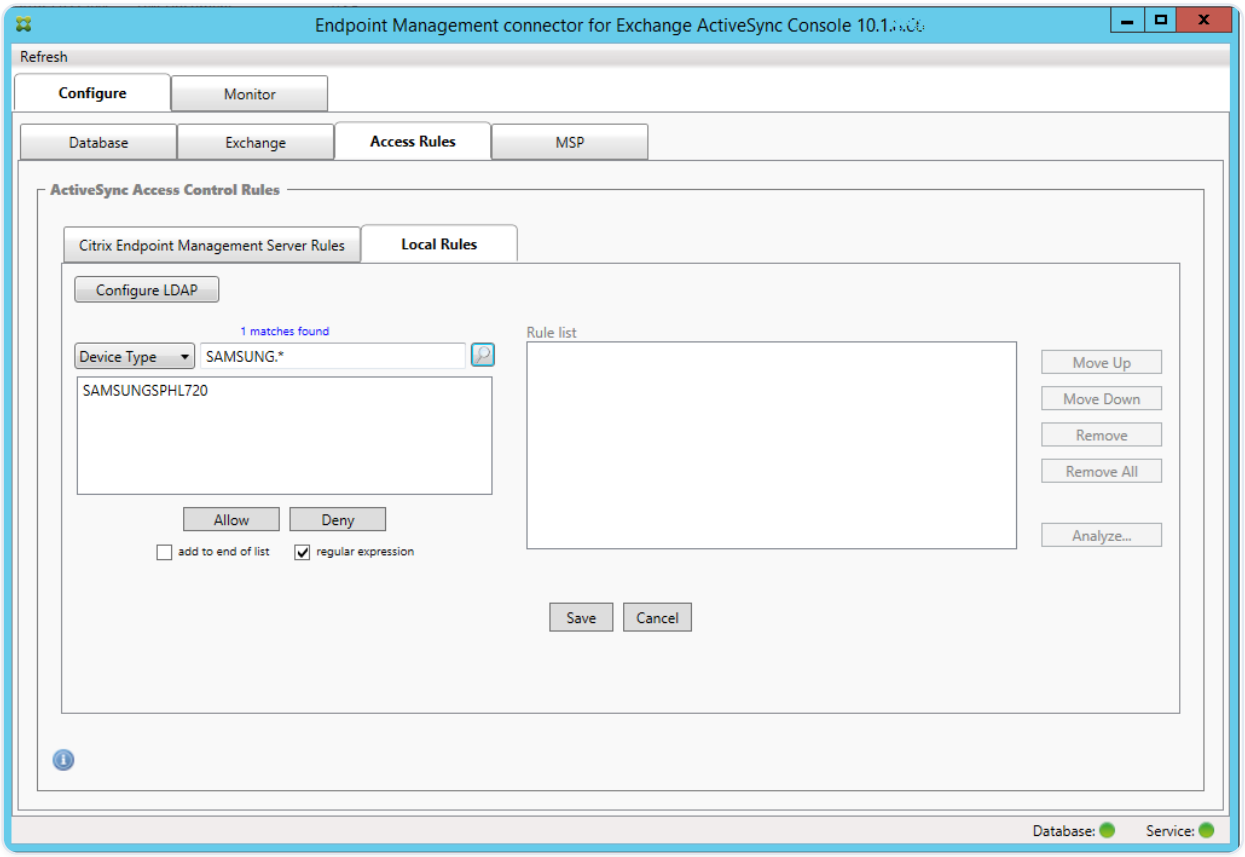


构建访问规则

1. 单击“**本地规则**”选项卡。
2. 要输入正则表达式，您必须同时使用设备 ID 列表和选定项目文本框。



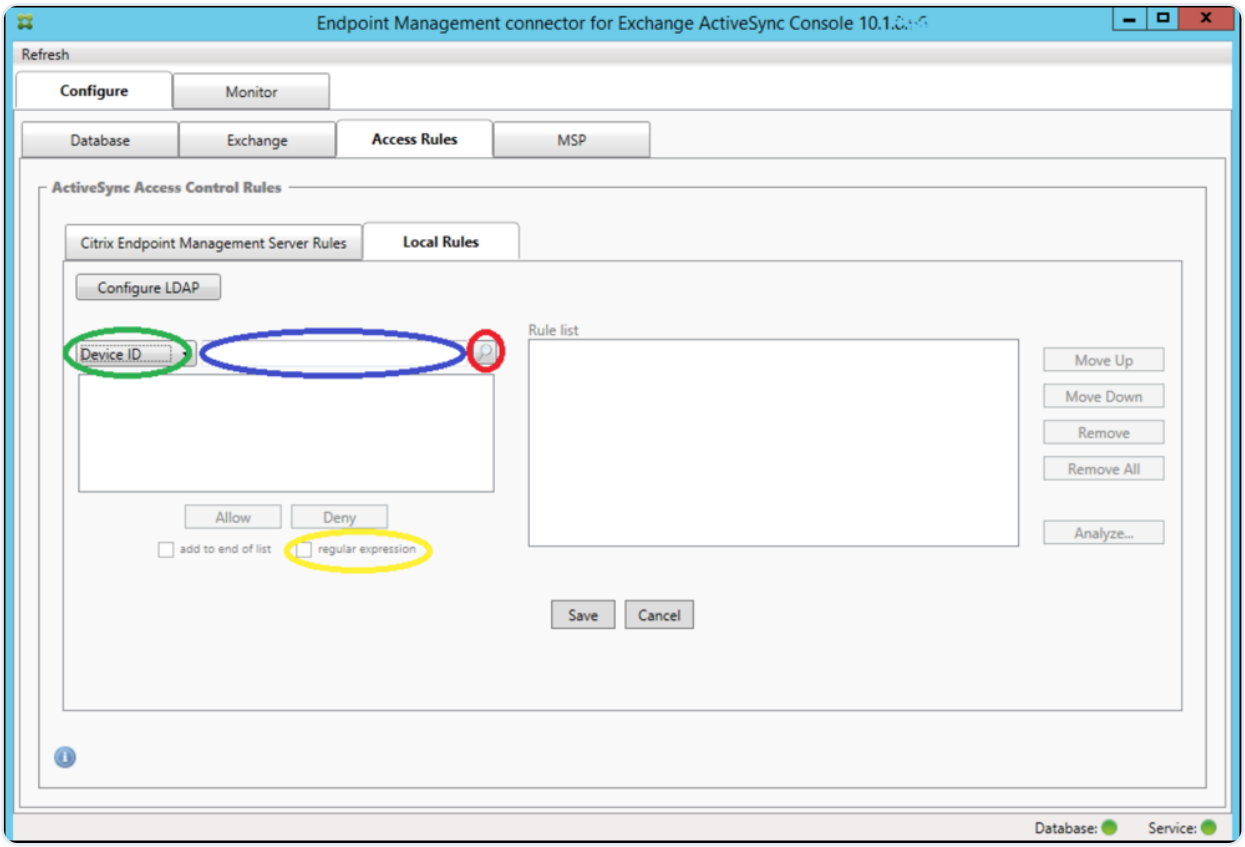
3. 选择要匹配的字段。此示例使用“**设备类型**”。
4. 键入正则表达式。此示例使用 `samsung.*`.
5. 确保选中正则表达式复选框，然后单击“**允许**”或“**拒绝**”。在此示例中，选择设置为“**允许**”。最终结果如下：



查找设备

通过选择正则表达式复选框，您可以搜索与给定表达式匹配的特定设备。此功能仅在主要快照成功完成后可用。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，假设您想查找所有在其 ActiveSync 设备 ID 中包含文本 `workmail` 的设备。为此，请按照以下步骤操作。

1. 单击**访问规则**选项卡。
2. 确保设备匹配字段选择器设置为“设备 ID”（默认值）。



3. 单击选定项目文本框内（如上图蓝色所示），然后键入 `workmail.*`。
4. 确保选中正则表达式复选框，然后单击放大镜图标以显示匹配项，如下图所示。

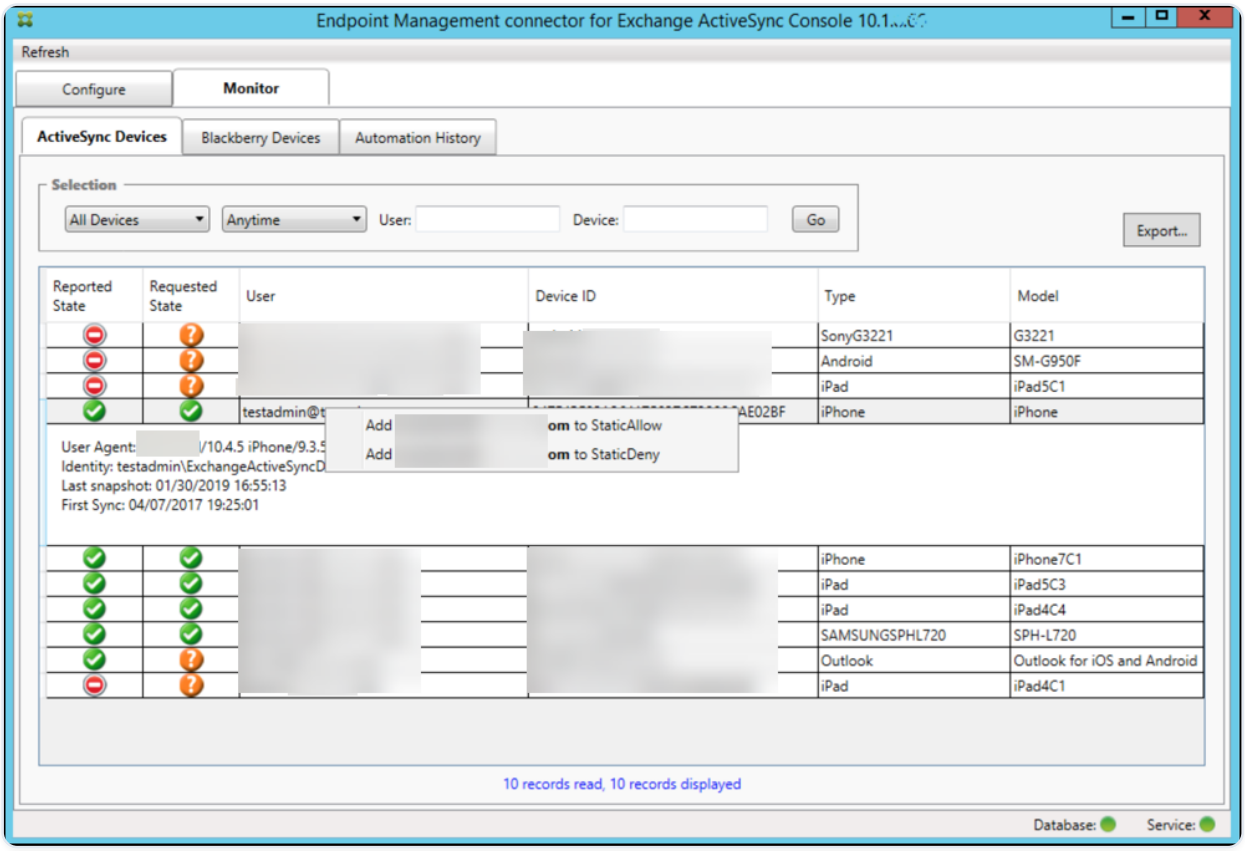
   ](/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-accessrules-localrules-regex.png)

将单个用户、设备或设备类型添加到静态规则

您可以在**ActiveSync 设备**选项卡上根据用户、设备 ID 或设备类型添加静态规则。

1. 单击**ActiveSync 设备**选项卡。
2. 在列表中，右键单击用户、设备或设备类型，然后选择是允许还是拒绝您的选择。

   下图显示了选择 user1 时的“允许/拒绝”选项。



设备监控

Citrix Endpoint Management connector for Exchange ActiveSync 中的**监视**选项卡允许您浏览已检测到的 Exchange ActiveSync 和 BlackBerry 设备以及已发出的自动化 PowerShell 命令的历史记录。**监视**选项卡包含以下三个选项卡：

- **ActiveSync 设备：**
  - 通过单击“**导出**”按钮，可以导出显示的 ActiveSync 设备伙伴关系。
  - 通过右键单击“**用户**”、“**设备 ID**”或“**类型**”列并选择相应的允许或阻止规则类型，可以添加本地（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 设备**
- **自动化历史记录**

“**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、持续时间、检测到的设备数量以及发生的任何错误：

- 在“**Exchange**”选项卡上，单击所需 Exchange Server 的信息图标。

故障排除和诊断

Citrix Endpoint Management connector for Exchange ActiveSync 将错误和其他操作信息记录到其日志文件：*Install Folder*\log\XmmWindowsService.log。Citrix Endpoint Management connector for Exchange ActiveSync 还会将重要事件记录到 Windows 事件日志中。

更改日志记录级别

Citrix Endpoint Management 的 Exchange ActiveSync 连接器包含以下日志级别：Error、Info、Warn、Debug 和 Trace。

> **注意：**
>
> 每个连续级别都会生成更多详细信息（更多数据）。例如，Error 级别提供的详细信息最少，而 Trace 级别提供的详细信息最多。

> 要更改日志记录级别，请执行以下操作：

1. 在 `C:\Program Files\Citrix\Citrix` Citrix Endpoint Management 连接器中，打开 nlog.config 文件。
2. 在 `<rules>` 部分中，将 *minilevel* 参数更改为您首选的日志记录级别。例如：

```
<rules >


<logger name="*" writeTo="file" minlevel="Debug" />


</rules>
```

3. 保存文件。

   更改会立即生效。您无需重新启动 Exchange ActiveSync 连接器。

常见错误

以下列表包含常见错误：

- Exchange ActiveSync 服务的连接器未启动

检查日志文件和 Windows 事件日志以查找错误。典型原因如下：

- Exchange ActiveSync 服务的连接器无法访问 SQL Server。这可能是由以下问题引起的：
  - SQL Server 服务未运行。
  - 身份验证失败。

  如果配置了 Windows 集成身份验证，则 Exchange ActiveSync 服务连接器的用户帐户必须是允许的 SQL 登录名。Exchange ActiveSync 服务连接器的帐户默认为 Local System，但可以更改为具有本地管理员权限的任何帐户。如果配置了 SQL 身份验证，则必须在 SQL 中正确配置 SQL 登录名。

故障排除工具

一组用于故障排除的 PowerShell 实用程序可在 **Support\PowerShell** 文件夹中找到。

故障排除工具可对用户邮箱和设备进行深入分析，检测错误情况和潜在故障区域，并对用户进行深入的 RBAC 分析。它可以将所有 cmdlet 的原始输出保存到文本文件。

用于 Exchange ActiveSync 的 NetScaler Gateway 连接器

XenMobile NetScaler 连接器现已更名为用于 Exchange ActiveSync 的 NetScaler 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。

用于 Exchange ActiveSync 的连接器为 ActiveSync 客户端提供设备级授权服务，以连接到充当 Exchange ActiveSync 协议反向代理的 NetScaler Gateway。您可以通过以下各项的组合来控制授权：

- 您在 Citrix Endpoint Management 中定义的策略
- 由用于 Exchange ActiveSync 的 NetScaler Gateway 连接器本地定义的规则

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 Architecture。

用于 Exchange ActiveSync 的 NetScaler Gateway 连接器的当前版本是 8.5.3。

要下载连接器：

1. 转到 `<https://www.citrix.com/downloads>`。
2. 导航到 **Citrix Endpoint Management（和 Citrix XenMobile Server）> XenMobile Server（本地部署）> 产品软件 > XenMobile Server 10 > 服务器组件**。

3. 在 **NetScaler Gateway 连接器**磁贴上，单击**下载文件**。

要安装连接器，请参阅 安装用于 Exchange ActiveSync 的 NetScaler Gateway 连接器)。

> **重要提示：**
>
> 自 2022 年 10 月起，鉴于 Microsoft 此处 宣布的身份验证更改，用于 Exchange ActiveSync 的 Citrix Endpoint Management 和 NetScaler Gateway 连接器将不再支持 Exchange Online。用于 Exchange 的 Citrix Endpoint Management 连接器将继续与 Microsoft Exchange Server（本地部署）配合使用。

版本 8.5.3 中的新增功能

- 此版本增加了对 ActiveSync 协议 16.0 和 16.1 的支持。
- 已向 Google Analytics 发送的分析数据中添加了更多详细信息，尤其是关于快照的。

早期版本中的新增功能

> **注意：**
>
> 以下“新增功能”部分指的是 Exchange ActiveSync 的 NetScaler Gateway 连接器，其旧名称为 XenMobile NetScaler Connector。该名称从 8.5.2 版本开始更改。

8.5.2 版本中的新增功能

- XenMobile NetScaler Connector 现已更名为 Exchange ActiveSync 的 NetScaler 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了多个条件，并且其中一个条件涉及用户 ID，则可能会出现以下问题：如果用户有多个别名，则在应用规则时不会同时检查这些别名。

8.5.1.11 版本中的新增功能

- **系统要求变更：** 当前版本的 NetScaler Connector 需要 Microsoft .NET Framework 4.5。
- **Google Analytics 支持：** 我们希望了解您如何使用连接器，以便我们能够专注于改进产品的方向。

- **支持 TLS 1.1 和 1.2：** 由于其安全性减弱，PCI Council 正在弃用 TLS 1.0 和 TLS 1.1。XenMobile NetScaler Connector 中已添加对 TLS 1.2 的支持。

监控 Exchange ActiveSync 的 NetScaler Gateway 连接器

Exchange ActiveSync 配置实用程序的 NetScaler Gateway 连接器提供详细的日志记录。使用日志可以查看通过 Exchange Server 的所有流量，这些流量由 Secure Mobile Gateway 允许或阻止。

使用“**日志**”选项卡可查看转发到 Exchange ActiveSync 连接器进行授权的 ActiveSync 请求历史记录。

此外，为确保 Exchange ActiveSync Web 服务的连接器正在运行，请在连接器服务器上的浏览器中加载以下 URL `https://<host:port>/services/ActiveSync/Version`。如果 URL 返回产品版本字符串，则表示 Web 服务响应正常。

使用 Exchange ActiveSync 连接器模拟 ActiveSync 流量

您可以使用 NetScaler Gateway Exchange ActiveSync 连接器通过策略模拟 ActiveSync 流量。在连接器配置实用程序中，单击**模拟器**选项卡。结果显示您的策略如何根据您配置的规则应用。

为 Exchange ActiveSync 连接器选择筛选器

NetScaler Gateway Exchange ActiveSync 连接器筛选器通过分析设备是否存在给定策略违规或属性设置来工作。如果设备符合条件，则该设备将放置在设备列表中。此设备列表既不是允许列表也不是阻止列表。它是符合所定义条件的设备列表。Citrix Endpoint Management 中适用于 Exchange ActiveSync 连接器的筛选器如下。每个筛选器的两个选项是**允许**或**拒绝**。

- **匿名设备：** 允许或拒绝已注册到 Citrix Endpoint Management 但用户身份未知的设备。例如，如果注册用户的 Active Directory 密码已过期或凭据未知，则其身份未知。
- **禁用应用程序：** 根据策略中阻止列表定义的设备列表以及阻止列表中是否存在应用程序来允许或拒绝设备。
- **隐式允许/拒绝：** 创建一个设备列表，其中包含所有不符合任何其他筛选器规则条件的设备，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 Exchange ActiveSync 连接器状态已启用，并显示设备的连接器状态。“隐式允许/拒绝”选项还控制所有其他未选择的连接器筛选器。例如，连接器会拒绝阻止列表上的应用程序。但是，由于“隐式允许/拒绝”选项设置为**允许**，因此连接器会允许所有其他筛选器。
- **非活动设备：** 创建一个设备列表，其中包含在指定时间内未与 Citrix Endpoint Management 通信的设备。这些设备被视为非活动设备。筛选器会相应地允许或拒绝这些设备。
- **缺少所需应用程序：** 当用户注册时，用户会收到一个必须安装的所需应用程序列表。缺少所需应用程序筛选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。

- **非建议应用程序：** 当用户注册时，用户会收到一个要安装的应用程序列表。非建议应用程序筛选器会检查设备中是否存在不在该列表中的应用程序。
- **不合规密码：** 创建一个设备列表，其中包含设备上没有密码的所有设备。
- **不合规设备：** 允许您拒绝或允许符合您内部 IT 合规性标准的设备。合规性是一个任意设置，由名为“不合规”的设备属性定义，该属性是一个布尔标志，可以是**True**或**False**。（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符合特定条件，使用自动化操作在设备上创建此属性。）
  - **不合规 = True：** 如果设备不符合您的 IT 部门设置的合规性标准和策略定义，则该设备不合规。
  - **不合规 = False：** 如果设备符合您的 IT 部门设置的合规性标准和策略定义，则该设备合规。
- **已吊销状态：** 创建一个所有已吊销设备的设备列表，并根据已吊销状态允许或拒绝。
- **Rooted Android/Jailbroken iOS 设备：** 创建所有被标记为已 Root 的设备的设备列表，并根据 Root 状态允许或拒绝访问。
- **未托管设备：** 创建 Citrix Endpoint Management 数据库中所有设备的设备列表。以阻止模式部署移动应用程序网关。

配置与 NetScaler Gateway connector for Exchange ActiveSync 的连接

NetScaler Gateway connector for Exchange ActiveSync 通过 Citrix Secure Web 服务与 Citrix Endpoint Management 和其他远程配置提供程序通信。

1. 在 Exchange ActiveSync 配置实用程序的连接器中，单击“**配置提供程序**”选项卡，然后单击“**添加**”。
2. 在“**配置提供程序**”对话框中，在“**名称**”中输入具有管理权限并用于与 Citrix Endpoint Management 服务器进行基本 HTTP 授权的用户名。
3. 在“**URL**”中，输入 Citrix Endpoint Management GCS 的网址，通常采用 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 格式。*MagConfigService* 名称区分大小写。
4. 在“**密码**”中，输入用于与 Citrix Endpoint Management 服务器进行基本 HTTP 授权的密码。
5. 在“**管理主机**”中，输入 Exchange ActiveSync 服务器名称的连接器。
6. 在“**基线间隔**”中，指定从 Citrix Endpoint Management 拉取新的刷新动态规则集的时间段。
7. 在“**增量间隔**”中，指定拉取动态规则更新的时间段。
8. 在“**请求超时**”中，指定服务器请求超时间隔。
9. 在“**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“**启用事件**”中，如果您希望 Exchange ActiveSync 连接器在设备被阻止时通知 Citrix Endpoint Management，请启用此选项。如果您在任何 Citrix Endpoint Management 自动化操作中使用连接器规则，则此选项是必需的。
11. 单击“**保存**”，然后单击“**测试连接**”以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，或联系您的管理员。
12. 连接成功后，清除“**禁用**”复选框，然后单击“**保存**”。

添加配置提供程序时，Exchange ActiveSync 连接器会自动创建与该提供程序关联的一个或多个策略。`NewPolicyTemplate` 部分中 `config\policyTemplates.xml` 包含的模板定义了这些策略。对于此部分中定义的每个策略元素，都会创建一个新策略。

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，并且标准替换字符串（括在括号中）未被修改。接下来，为提供程序添加新组并更新策略以包含新组。

从 Citrix Endpoint Management 导入策略

1. 在 Exchange ActiveSync 配置实用程序的连接器中，单击“**配置提供程序**”选项卡，然后单击“**添加**”。
2. 在“**配置提供程序**”对话框中，在“**名称**”中，输入用于与 Citrix Endpoint Management 进行基本 HTTP 授权的用户名。该用户必须具有管理权限。
3. 在“**URL**”中，输入 Citrix Endpoint Management 网关配置服务 (GCS) 的网址，通常采用 `https://<xdmHost>/xdm/services/<MagConfigService>` 格式。MagConfigService 名称区分大小写。
4. 在“**密码**”中，输入用于与 Citrix Endpoint Management 服务器进行基本 HTTP 授权的密码。
5. 单击“**测试连接**”以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，或咨询管理员。
6. 成功建立连接后，清除“**禁用**”复选框，然后单击“**保存**”。
7. 在“**管理主机**”中，保留本地主机的默认 DNS 名称。当多个 Forefront Threat Management Gateway (TMG) 服务器配置为阵列时，此设置用于协调与 Citrix Endpoint Management 的通信。

   保存设置后，打开 GCS。

配置 NetScaler Gateway 连接器以用于 Exchange ActiveSync 策略模式

NetScaler Gateway 连接器可用于 Exchange ActiveSync，并可在以下六种模式下运行：

- **允许所有：** 此策略模式授予通过 Exchange ActiveSync 连接器的所有流量的访问权限。不使用其他筛选规则。
- **全部拒绝：** 此策略模式会阻止通过 Exchange ActiveSync 连接器传输的所有流量的访问。不使用其他筛选规则。
- **静态规则：阻止模式：** 此策略模式运行静态规则，并在末尾带有一个隐式拒绝或阻止语句。Exchange ActiveSync 连接器会阻止通过其他筛选规则不允许或未获准的设备。
- **静态规则：允许模式：** 此策略模式运行静态规则，并在末尾带有一个隐式允许语句。通过其他筛选规则未被阻止或拒绝的设备可以通过 Exchange ActiveSync 连接器。
- **静态 + ZDM 规则**：阻止模式。此策略模式首先运行静态规则，然后运行来自 Citrix Endpoint Management 的动态规则，并在末尾带有一个隐式拒绝或阻止语句。设备根据定义的筛选器和 Citrix Endpoint Management 规则获得允许或被拒绝。任何与定义的筛选器和规则不匹配的设备都将被阻止。
- **静态 + ZDM 规则**：允许模式。此策略模式首先运行静态规则，然后运行来自 Citrix Endpoint Management 的动态规则，并在末尾带有一个隐式允许语句。设备根据定义的筛选器和 Citrix Endpoint Management 规则获得允许或被拒绝。任何与定义的筛选器和规则不匹配的设备都将被允许。

Exchange ActiveSync 进程连接器根据从 Citrix Endpoint Management 接收的 iOS 和基于 Windows 的移动设备的唯一 ActiveSync ID 允许或阻止动态规则。Android 设备的行为因制造商而异，有些设备不会轻易公开唯一的 ActiveSync ID。为了弥补这一点，Citrix Endpoint Management 会发送 Android 设备的 用户 ID 信息，以做出允许或阻止的决定。因此，如果用户只有一个 Android 设备，则允许和阻止功能正常。如果用户有多个 Android 设备，则所有设备都将被允许，因为 Android 设备无法区分。如果已知这些设备的 ActiveSyncID，您可以将网关配置为通过 ActiveSyncID 静态阻止这些设备。您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 Configuration 实用程序中执行以下操作：

1. 单击“**路径筛选器**”选项卡，然后单击“**添加**”。
2. 在“**路径属性**”对话框中，从“**策略**”列表中选择一个策略模式，然后单击“**保存**”。

您可以在配置实用程序的“**策略**”选项卡上查看规则。规则在 Exchange ActiveSync 连接器上从上到下进行处理。允许策略显示为绿色复选标记。拒绝策略显示为带斜线的红色圆圈。要刷新屏幕并查看最新规则，请单击“**刷新**”。您还可以修改 config.xml 文件中规则的顺序。

要测试规则，请单击“**模拟器**”选项卡。在字段中指定值。您可以从日志中获取这些值。结果消息会指定“允许”或“阻止”。

配置静态规则

输入静态规则，其中包含 ActiveSync 连接 HTTP 请求的 ISAPI 筛选器读取的值。静态规则使 Exchange ActiveSync 连接器能够根据以下条件允许或阻止流量：

- **用户：** Exchange ActiveSync 连接器使用在设备注册期间捕获的授权用户值和名称结构。该结构通常以 `domain\username` 的形式出现，由通过 LDAP 连接到 Active Directory 的运行 Citrix Endpoint Management 的服务器引用。连接器配置实用程序中的“**日志**”选项卡显示通过连接器的值。如果连接器必须确定值结构或结构不同，则会传递这些值。
- **设备 ID (ActiveSyncID)：** 也称为连接设备的 ActiveSyncID。此值通常在 Citrix Endpoint Management 控制台中的特定设备属性页面中找到。此值也可以从 Exchange ActiveSync 配置实用程序的连接器中的“**日志**”选项卡中筛选出来。
- **设备类型：** Exchange ActiveSync 连接器可以确定设备是 iPhone、iPad 还是其他设备类型，并可以根据该标准允许或阻止访问。与其他值一样，连接器配置实用程序可以显示正在为 ActiveSync 连接处理的所有已连接设备类型。
- **用户代理：** 包含有关所用 ActiveSync 客户端的信息。通常，指定的值对应于移动设备平台的特定操作系统版本和内部版本号。

服务器上运行的 Exchange ActiveSync 配置实用程序的连接器始终管理静态规则。

1. 在 SMG 控制器配置实用程序中，单击“**静态规则**”选项卡，然后单击“**添加**”。
2. 在“**静态规则属性**”对话框中，指定要用作条件的数值。例如，您可以通过输入用户名（例如，AllowedUser）并清除“**禁用**”复选框来输入允许访问的用户。
3. 点击 **保存**。

   静态规则现已生效。此外，您可以使用正则表达式定义值，但必须在 config.xml 文件中启用规则处理模式。

配置动态规则

Citrix Endpoint Management 中的设备策略和属性定义了动态规则，并可以触发 Exchange ActiveSync 过滤器的动态连接器。触发器基于策略违规或属性设置的存在。Exchange ActiveSync 过滤器的连接器通过分析设备的给定策略违规或属性设置来工作。如果设备符合条件，则该设备将放置在设备列表中。此设备列表不是允许列表或阻止列表。它是符合所定义条件的设备列表。以下配置选项使您能够定义是否要使用 Exchange ActiveSync 连接器允许或拒绝设备列表中的设备。

> **注意：**

> 使用 Citrix Endpoint Management 控制台配置动态规则。

1. 在 Citrix 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，单击“**ActiveSync 网关**”。此时将显示 ActiveSync 网关页面。
3. 在“**激活以下规则**”中，选择要激活的一个或多个规则。
4. 仅限 Android，在“**将 Android 域用户发送到 ActiveSync 网关**”中，单击“**是**”以确保 Citrix Endpoint Management 将 Android 设备信息发送到安全移动网关。

   启用此选项后，如果 Citrix Endpoint Management 没有设备用户的 ActiveSync 标识符，则 Citrix Endpoint Management 会将 Android 设备信息发送到连接器。

通过编辑 Exchange ActiveSync XML 文件的连接器来配置自定义策略

您可以在 Exchange ActiveSync 配置实用程序的连接器“**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 XML 配置文件 (config\config.xml) 的 NetScaler Gateway 连接器。

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），请将新的 **Group** 元素添加到 **GroupList** 部分。
3. （可选）您可以通过重新排列 **GroupRef** 元素来更改现有策略中组的顺序。

配置适用于 Exchange ActiveSync 的连接器 XML 文件

适用于 Exchange ActiveSync 的连接器使用 XML 配置文件来规定连接器的操作。除其他条目外，该文件还指定了筛选器在评估 HTTP 请求时所采取的组文件和相关操作。默认情况下，该文件名为 config.xml，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 值标识一个逻辑容器或成员集合，用于匹配特定的用户帐户或设备。action 属性指定筛选器如何处理集合中与规则匹配的成员。例如，与 AllowGroup 集中规则匹

> 配的用户帐户或设备“通过”。通过意味着允许访问 Exchange CAS。与 DenyGroup 集中规则匹配的用户帐户或设备“被拒绝”。被拒绝意味着不允许访问 Exchange CAS。

当特定用户帐户/设备或组合同时满足两个组中的规则时，将使用优先级约定来决定请求的结果。优先级体现在 config.xml 文件中 GroupRef 节点从上到下的顺序。GroupRef 节点按优先级排序。Allow 组中给定条件的规则始终优先于 Deny 组中相同条件的规则。

组节点

此外，config.xml 还定义了组节点。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了筛选规则的基础。

> **注意：**

> 在此版本中，仅支持外部 XML 文件。

> 默认安装在配置中实现两个 XML 文件：allow.xml 和 deny.xml。

配置 NetScaler Gateway 连接器以用于 Exchange ActiveSync

您可以配置 NetScaler Gateway 连接器以用于 Exchange ActiveSync，从而根据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**。

默认配置支持静态组和动态组的组合。您可以使用 SMG 控制器配置实用程序维护静态组。静态组可以由已知类别的设备组成，例如使用给定用户代理的所有设备。

称为网关配置提供程序的外部源维护动态组。Exchange ActiveSync 连接器定期连接这些组。Citrix Endpoint Management 可以将允许和阻止的设备和用户组导出到 Exchange ActiveSync 连接器。

称为网关配置提供程序的外部源维护动态组。Exchange ActiveSync 连接器定期收集动态组。Citrix Endpoint Management 可以将允许和阻止的设备和用户组导出到连接器。

策略是组的有序列表，其中每个组都具有关联的操作（允许或阻止）和组员列表。策略可以包含任意数量的组。策略中的组排序很重要，因为当找到匹配项时，将执行该组的操作，并且不会评估后续组。

成员定义了匹配请求属性的方式。它可以匹配单个属性，例如设备 ID，也可以匹配多个属性，例如设备类型和用户代理。

为 NetScaler Gateway 连接器选择 Exchange ActiveSync 的安全模型

建立安全模型对于任何规模的组织成功部署移动设备都至关重要。通常，默认情况下使用受保护或隔离的网络控制来允许用户、计算机或设备访问。这种做法并非总是理想的。每个管理 IT 安全的组织可能对移动设备的安全有略微不同或量身定制的方法。

同样的逻辑也适用于移动设备安全。由于移动设备的种类和类型繁多、每个用户的移动设备数量以及可用的操作系统平台和应用程序，使用宽松模型是一个薄弱的选择。在大多数组织中，限制性模型是最合乎逻辑的选择。

Citrix 允许将 Exchange ActiveSync 连接器与 Citrix Endpoint Management 集成的配置方案如下：

宽松模型（允许模式）

宽松安全模型的前提是默认情况下所有内容都被允许或授予访问权限。只有通过规则和过滤，才能阻止某些内容并施加限制。宽松安全模型适用于对移动设备安全相对宽松的组织。该模型仅在适当情况下（当策略规则失败时）应用限制性控制来拒绝访问。

限制性模型（阻止模式）

限制性安全模型基于默认情况下不允许或授予任何访问权限的前提。所有通过安全检查点的内容都会被过滤和检查，并且除非通过允许访问的规则，否则将被拒绝访问。限制性安全模型适用于对移动设备有相对严格安全标准的组织。该模式仅在所有允许访问的规则都通过后，才授予使用网络服务的功能和访问权限。

管理 NetScaler Gateway Exchange ActiveSync 连接器

您可以使用 NetScaler Gateway Exchange ActiveSync 连接器来构建访问控制规则。这些规则允许或阻止受管设备发出的 ActiveSync 连接请求。访问权限基于设备状态、应用程序允许或阻止列表以及其他合规性条件。

通过使用 Exchange ActiveSync 配置实用程序的连接器，您可以构建动态和静态规则来强制执行公司电子邮件策略。这些规则和策略允许您阻止违反合规性标准的用户。您还可以设置电子邮件附件加密，以便所有通过 Exchange Server 传输到受管设备的附件都经过加密。只有拥有受管设备的授权用户才能查看加密附件。

卸载 XNC

1. 使用管理员帐户运行 XncInstaller.exe。
2. 按照屏幕上的说明完成卸载。

安装、升级或卸载 Exchange ActiveSync 连接器

1. 使用管理员帐户运行 XncInstaller.exe 以安装 Exchange ActiveSync 连接器，或允许升级或删除现有连接器。
2. 按照屏幕上的说明完成安装、升级或卸载。

安装 Exchange ActiveSync 连接器后，必须手动重新启动 Citrix Endpoint Management 配置服务和通知服务。

安装 NetScaler Gateway Exchange ActiveSync 连接器

您可以将 Exchange ActiveSync 连接器安装在其自己的服务器上，也可以安装在您安装 Citrix Endpoint Management 的同一服务器上。

您可以考虑将 Exchange ActiveSync 连接器安装在其自己的服务器上（与 Citrix Endpoint Management 分开），原因如下：

- 如果您的 Citrix Endpoint Management 服务器远程托管在云中（物理位置）
- 如果您不希望 Citrix Endpoint Management 服务器的重新启动影响 Exchange ActiveSync 连接器（可用性）
- 如果您希望将服务器的系统资源完全用于 Exchange ActiveSync 连接器（性能）

Exchange ActiveSync 连接器对服务器造成的 CPU 负载取决于所管理的设备数量。一般建议是，如果连接器与 Citrix Endpoint Management 部署在同一台服务器上，则额外配置一个 CPU 核心。对于大量设备（超过 50,000 台），如果没有群集环境，可能需要配置更多核心。连接器的内存占用量不足以需要更多内存。

适用于 Exchange ActiveSync 的 NetScaler Gateway 连接器系统要求

适用于 Exchange ActiveSync 的 NetScaler Gateway 连接器通过在 NetScaler Gateway 设备上配置的 SSL 网桥与 NetScaler Gateway 进行通信。该网桥使设备能够将所有安全流量直接桥接到 Citrix Endpoint Management。适用于 Exchange ActiveSync 的连接器具有以下最低系统配置：

组件	要求
计算机和处理器	733 MHz Pentium III 733 MHz 或更高处理器。 2.0 GHz Pentium III 或更高处理器（推荐）
思杰网关	软件版本 10 的 Citrix Gateway 设备
内存	1 GB

组件	要求
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 的支持于 January 14, 2020 结束，对 Windows Server 2012 R2 的支持于 October 10, 2023 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 框架	版本 8.5.1.11 需要 Microsoft .NET Framework 4.5。
显示器	VGA 或更高分辨率的显示器

Exchange ActiveSync 连接器的主机需要以下最低可用硬盘空间：

- **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始终为设备返回相同的 ActiveSync ID。由于 Exchange ActiveSync 连接器需要为每个设备提供唯一的 ActiveSync ID，因此以下情况属实：仅支持始终为每个设备生成相同且唯一的 ActiveSync ID 的电子邮件客户端。Citrix 已测试这些电子邮件客户端，并且这些客户端运行无误：

- 三星原生电子邮件客户端
- iOS 原生电子邮件客户端

部署适用于 Exchange ActiveSync 的 NetScaler Gateway 连接器

适用于 Exchange ActiveSync 的 NetScaler Gateway 连接器使您能够使用 NetScaler Gateway 代理和负载平衡 Citrix Endpoint Management 服务器与 Citrix Endpoint Management 托管设备之间的通信。适用于 Exchange ActiveSync 的连接器会定期与 Citrix Endpoint Management 通信以同步策

略。您可以将适用于 Exchange ActiveSync 的连接器和 Citrix Endpoint Management 进行群集，无论是共同群集还是独立群集。

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 服务接口，NetScaler Gateway 可以调用该接口来确定来自设备的 ActiveSync 请求是否已获得授权。
- **Citrix Endpoint Management 配置服务：** 此服务与 Citrix Endpoint Management 通信，以将 Citrix Endpoint Management 策略更改与适用于 Exchange ActiveSync 的连接器同步。
- **Citrix Endpoint Management 通知服务：** 此服务将未经授权的设备访问通知发送到 Citrix Endpoint Management。通过这种方式，Citrix Endpoint Management 可以采取适当的措施，例如通知用户设备被阻止的原因。
- **Exchange ActiveSync 连接器配置实用程序：** 此应用程序允许管理员配置和监视 Exchange ActiveSync 连接器。

为 NetScaler Gateway Exchange ActiveSync 连接器设置侦听地址

要使 NetScaler Gateway Exchange ActiveSync 连接器接收来自 NetScaler Gateway 的请求以授权 ActiveSync 流量，请执行以下操作。指定 Exchange ActiveSync 连接器侦听 NetScaler Gateway Web 服务调用的端口。

1. 从“**开始**”菜单中，选择 Exchange ActiveSync 配置实用程序的连接器。
2. 单击“**Web 服务**”选项卡，然后键入连接器 Web 服务的侦听地址。您可以选择 **HTTP** 或 **HTTPS**，或两者都选。如果 Exchange ActiveSync 连接器与 Citrix Endpoint Management 共存（安装在同一服务器上），请选择与 Citrix Endpoint Management 不冲突的端口值。
3. 配置值后，单击“**保存**”，然后单击“**启动服务**”以启动 Web 服务。

在 NetScaler Gateway Exchange ActiveSync 连接器中配置设备访问控制策略

要配置要应用于托管设备的访问控制策略，请执行以下操作：

1. 在 Exchange ActiveSync 配置实用程序的连接器中，单击“**路径筛选器**”选项卡。
2. 选择第一行“**Microsoft-Server-ActiveSync 用于 ActiveSync**”，然后单击“**编辑**”。
3. 从“**策略**”列表中，选择所需的策略。对于包含 Citrix Endpoint Management 策略的策略，请选择 **静态 + ZDM: 允许模式或静态 + ZDM: 阻止模式**。这些策略将本地（或静态）规则与 Citrix Endpoint Management 中的规则结合起来。允许模式表示所有未由规则明确标识的设备都允许访问 ActiveSync。阻止模式表示此类设备被阻止。

4. 设置策略后，单击“**保存**”。

配置与 Citrix Endpoint Management 的通信

指定要与 NetScaler Gateway Exchange ActiveSync 连接器和 NetScaler Gateway 配合使用的 Citrix 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 Citrix Endpoint Management。Exchange ActiveSync 配置实用程序使用术语“配置提供程序”来指代 Citrix Endpoint Management。

1. 在 Exchange ActiveSync 配置实用程序的连接器中，单击“**配置提供程序**”选项卡，然后单击“**添加**”。
2. 输入在此部署中使用的 Citrix Endpoint Management 服务器的名称和 URL。如果在多租户部署中部署了多个 Citrix Endpoint Management 服务器，则此名称对于每个服务器实例都必须是唯一的。
3. 在“**URL**”中，输入 Citrix Endpoint Management 全局配置提供程序 (GCP) 的 Web 地址，通常采用 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 格式。*MagConfigService* 名称区分大小写。
4. 在“**密码**”中，输入用于与 Citrix Endpoint Management Web 服务器进行基本 HTTP 授权的密码。
5. 在“**管理主机**”中，输入安装 Exchange ActiveSync 连接器的服务器名称。
6. 在“**基线间隔**”中，指定从 Citrix Endpoint Management 拉取新的刷新动态规则集的时间段。
7. 在“**请求超时**”中，指定服务器请求超时间隔。
8. 在“**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“**启用事件**”中，如果希望 Secure Mobile Gateway 在设备被阻止时通知 Citrix Endpoint Management，请启用此选项。如果在任何 Citrix Endpoint Management 自动化操作中使用 Secure Mobile Gateway 规则，则此选项是必需的。
10. 配置服务器后，单击“**测试连接**”以测试与 Citrix Endpoint Management 的连接。
11. 建立连接后，单击“**保存**”。

部署 NetScaler Gateway Exchange ActiveSync 连接器以实现冗余和可扩展性

为了扩展您的 NetScaler Gateway Exchange ActiveSync 连接器和 Citrix Endpoint Management 部署，您可以在多台 Windows 服务器上安装 Exchange ActiveSync 连接器实例。所有连接器实例都指向同一个 Citrix Endpoint Management 实例。然后，您可以使用 NetScaler Gateway 对服务器进行负载平衡。

Exchange ActiveSync 连接器配置有两种模式：

- 在非共享模式下，每个 Exchange ActiveSync 实例的连接器都与 Citrix Endpoint Management 服务器通信，并保留其自己的策略私有副本。例如，对于 Citrix Endpoint Management 服务器群集，您可以在每个 Citrix Endpoint Management 服务器上运行一个连接器实例。然后，连接器从本地 Citrix Endpoint Management 实例获取策略。
- 在共享模式下，一个 Exchange ActiveSync 节点的连接器被指定为主节点。该连接器与 Citrix Endpoint Management 通信。其他节点通过 Windows 网络共享或通过 Windows（或第三方）复制来共享生成的配置。

整个 Exchange ActiveSync 连接器配置位于单个文件夹中（包含几个 XML 文件）。连接器进程会检测此文件夹中任何文件的更改，并自动重新加载配置。共享模式下，主节点没有故障转移。但是，系统可以容忍主服务器停机几分钟（例如，为了重新启动）。上一个已知良好配置会缓存在连接器进程中。

高级概念

Citrix Endpoint Management 高级概念文章深入探讨了有关 Citrix Endpoint Management 的产品信息。其目的是通过专家技术帮助缩短部署时间。这些文章可能会引用撰写内容的专家。

有关 Citrix Endpoint Management 环境的决策点、建议、常见问题和用例，请参阅本节中的 Citrix Endpoint Management 部署。

有关 Citrix Endpoint Management 的社区支持论坛，请参阅 Citrix Discussions。

思杰端点管理部署

在规划 Citrix Endpoint Management 部署时，有很多因素需要考虑。您选择哪些设备？如何管理它们？如何确保网络安全，同时仍提供良好的用户体验？您需要哪些硬件以及如何对其进行故障排除？本节中的文章旨在帮助回答这些问题。其中包含涵盖您部署关注点的用例和建议。

请记住，指南或建议可能不适用于所有环境或用例。在正式部署 Citrix Endpoint Management 之前，请务必设置测试环境。

本节中的文章涵盖以下领域：

- **评估：** 规划部署时要考虑的常见用例和问题。
- **设计和配置：** 有关设计和配置环境的建议
- **操作和监控：** 确保运行环境的平稳运行。

评估

与任何部署一样，评估您的需求必须是您的首要任务。您对 Citrix Endpoint Management 的主要需求是什么？是需要管理环境中的所有设备、仅应用程序，还是两者兼而有之？您的 Citrix Endpoint Management 环境需要什么级别的安全性？让我们来看看在规划部署时需要考虑的常见用例和问题。

- 管理模式
- 设备要求
- 安全性和用户体验
- 应用程序

- 用户社区
- 电子邮件策略
- 思杰端点管理集成

设计和配置

完成部署需求评估后，您可以决定如何设计和配置您的环境。需要规划的项目包括：

- 选择服务器硬件
- 设置应用程序和设备的策略
- 让用户注册

本节包含针对这些场景及更多场景的用例和建议。

- 与 NetScaler 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

操作和监控

Citrix Endpoint Management 环境启动并运行后，您需要对其进行监控以确保其平稳运行。监控部分讨论了在哪里可以找到 Citrix Endpoint Management 及其组件生成的各种日志和消息，以及如何读取这些日志。本节还包括您可以遵循的各种常见故障排除步骤，以减少客户支持反馈时间。

- 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 Citrix Endpoint Management 支持
- 监视和支持
- Citrix 支持流程

管理模式

管理模式是一个术语，包括移动设备管理 (MDM) 和移动应用程序管理 (MAM)。您可以配置：

- 注册配置文件，用于将 Android 和 iOS 设备注册到 MDM、MAM 或两者兼有 (MDM+MAM)。如果选择 MDM+MAM，可以允许用户选择退出 MDM。
- 注册配置文件，用于将 Windows 10 和 Windows 11 设备注册到 MDM。

您在注册配置文件中指定注册选项，然后将这些配置文件附加到交付组。有关注册选项的信息，请参阅注册配置文件。以下各节重点介绍管理设备和应用程序的注意事项。

移动设备管理 (MDM)

使用 MDM，您可以配置、保护和支持移动设备。MDM 使您能够在系统级别保护设备和设备上的数据。您可以配置策略、操作和安全功能。例如，如果设备丢失、被盗或不合规，您可以选择性地擦除设备。

即使您不选择管理设备上的应用程序，也可以交付移动应用程序，例如公共应用商店应用程序和企业应用程序。

以下是 MDM 的常见用例：

- MDM 是企业自有设备的考虑因素，这些设备需要设备级管理策略或某些限制。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。
- 当用户只需要将电子邮件发送到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，您可以使用 MDM 配置电子邮件交付。
- 当您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商店交付的 MDX 应用程序时。请注意，单独的 MDM 解决方案可能无法阻止设备上应用程序之间机密信息的数据泄露。数据泄露可能发生在 Office 365 应用程序中的复制粘贴或“另存为”操作中。

移动应用程序管理 (MAM)

MAM 保护应用程序数据并允许您控制应用程序数据共享。MAM 还允许独立于个人数据管理公司数据和资源。通过为 MAM 配置的 Citrix Endpoint Management，您可以使用支持 MDX 的移动应用程序来提供每个应用程序的容器化和控制。

通过使用 MDX 策略，Citrix Endpoint Management 提供对网络访问（例如微型 VPN）、应用程序和设备交互以及应用程序访问的应用程序级控制。

MAM 通常适用于自带 (BYO) 设备，因为尽管设备未受管理，但公司数据受到保护。MDX 有许多仅限 MAM 的策略，这些策略不需要 MDM 控制。

MAM 还支持 Citrix 移动生产力应用程序。此支持包括：

- 安全电子邮件交付到 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：

- 您交付移动应用程序，例如在应用程序级别管理的 MDX 应用程序。
- 您无需在系统级别管理设备。

MDM+MAM

Citrix Endpoint Management 允许您指定用户是否可以选择退出设备管理。这种灵活性对于包含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：

- 您有一个需要 MDM 和 MAM 的单一用例。需要 MDM 才能访问您的 MAM 资源。
- 某些用例需要 MDM，而另一些则不需要。
- 某些用例需要 MAM，而有些则不需要。

设备管理和 MDM 注册

Citrix Endpoint Management Enterprise 环境可以包含多种用例，其中一些用例需要通过 MDM 策略进行设备管理，以允许访问 MAM 资源。

在向用户部署 Citrix 移动生产力应用程序之前，请全面评估您的用例并决定是否需要 MDM 注册。如果您以后决定更改 MDM 注册要求，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 NetScaler Gateway 的信息，请参阅与 NetScaler Gateway 和 Citrix ADC 集成。

以下是要求 MDM 注册的优点和缺点（以及缓解措施）的摘要。

当 MDM 注册是可选时

优点

- 用户可以访问 MAM 资源，而无需将其设备置于 MDM 管理之下。此选项可以提高用户采用率。
- 能够安全访问 MAM 资源以保护企业数据。
- MDX 策略（例如**应用程序密码**）可以控制每个 MDX 应用程序的应用程序访问。

- 配置 NetScaler Gateway、Citrix Endpoint Management 和每个应用程序的超时，以及 Citrix PIN，可提供额外的保护层。
- 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。拒绝是基于系统设置，例如越狱或已 root 的设备。
- 用户可以在首次使用时选择是否将其设备注册到 MDM。

缺点

- MAM 资源可用于未注册 MDM 的设备。
- MDM 策略和操作仅适用于已注册 MDM 的设备。

缓解选项

- 让用户同意公司条款和条件，如果他们选择不合规，则需承担责任。让管理员监控未受管理的设备。
- 通过使用应用程序计时器管理应用程序访问和安全性。缩短超时值可提高安全性，但可能会影响用户体验。

何时需要 MDM 注册

优点

- 能够将 MAM 资源的访问权限仅限于 MDM 管理的设备。
- MDM 策略和操作可以按您希望的方式应用于环境中的所有设备。
- 用户无法选择不注册其设备。

缺点

- 要求所有用户注册 MDM。
- 对于反对公司管理其个人设备的用户，可能会降低采用率。

缓解选项

- 向用户说明 Citrix Endpoint Management 实际管理其设备上的哪些内容以及管理员可以访问哪些信息。

设备要求

任何部署都需要考虑的一个重要方面是您计划推出的设备集。在 iOS、Android 和 Windows 平台上，有许多选项。有关 Citrix 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，支持的平台可能混合存在。但是，在告知用户可以注册的设备时，请考虑“支持的设备平台”文章中的限制。即使您的环境中只允许一两台设备，Citrix Endpoint Management 在 iOS、Android 和 Windows 设备上的功能也略有不同。每个平台上都提供不同的功能集。

此外，并非所有应用程序设计都同时针对平板电脑和手机外形。在进行广泛更改之前，请测试应用程序以确保它们适合您要推出的设备屏幕。

您还可以考虑注册因素。Apple 和 Google 提供企业注册计划。通过 Apple Deployment Program 和 Google Android Enterprise，您可以购买预配置好并可供员工使用的设备。

有关注册的更多信息，请参阅 用户注册选项。

安全性和用户体验

安全性对任何组织都很重要，但您需要在安全性与用户体验之间取得平衡。例如，您可能拥有一个高度安全的环境，但用户难以使用。或者，您的环境可能非常用户友好，以至于访问控制不够严格。本虚拟手册中的其他部分详细介绍了安全功能。本文的目的是概述常见的安全问题以及 Citrix Endpoint Management 中可用的安全选项。

以下是每个用例需要牢记的一些关键注意事项：

- 您是想保护某些应用程序、整个设备，还是两者都保护？
- 您希望用户如何验证其身份？您想使用 LDAP、基于证书的身份验证，还是两者的组合？
- 您希望用户会话持续多长时间才超时？请记住，后台服务、Citrix ADC 以及离线访问应用程序都有不同的超时值。
- 您是否希望用户设置设备级密码和应用程序级密码？您希望允许多少次登录尝试？请记住，MAM 可能会实施额外的每应用程序身份验证要求，以及用户可能如何看待这些要求。
- 您还想对用户施加哪些限制？您是否希望用户访问 Siri 等云服务？对于您提供给他们的每个应用程序，他们可以做什么，不能做什么？您是否希望部署企业网络 (Wi-Fi) 策略，以防止在办公室内部使用蜂窝数据套餐？

应用程序与设备

首先要考虑的是您是否要保护：

- 仅某些应用程序（移动应用程序管理，或 MAM）
- 整个设备（移动设备管理，或 MDM）。
- MDM+MAM

最常见的情况是，如果您不需要设备级控制，则只需管理移动应用程序，尤其是在您的组织支持自带设备 (BYOD) 的情况下。

使用 Citrix Endpoint Management 未管理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，而不是通过设备级控制（例如选择性擦除或完全擦除）。根据您设置的值，策略要求设备定期检查 Citrix Endpoint Management，以确认应用程序仍被允许运行。

MDM 允许您保护整个设备，包括清点设备上所有软件的能力。如果设备已越狱、已取得 root 权限或安装了不安全的软件，MDM 允许您阻止注册。然而，这种级别的控制会让用户对允许其个人设备拥有如此大的权力感到担忧，并可能降低注册率。

身份验证

身份验证是用户体验的重要组成部分。如果您的组织已运行 Active Directory，则使用 Active Directory 是让用户访问系统的最简单方法。

身份验证用户体验的另一个重要部分是超时。高安全性环境可能要求用户每次访问系统时都登录。该选项可能不适用于所有组织或用例。

用户熵

为了增强安全性，您可以启用一项名为*用户熵*的功能。Citrix Secure Hub 和其他一些应用程序通常共享密码、PIN 和证书等常见数据，以确保一切正常运行。此信息存储在 Citrix Secure Hub 中的通用保管库中。如果您通过**加密机密**选项启用用户熵，Citrix Endpoint Management 将创建一个名为 UserEntropy 的保管库。Citrix Endpoint Management 会将信息从通用保管库移动到此新保管库中。对于 Citrix Secure Hub 或其他应用程序访问数据，用户必须输入密码或 PIN。

启用用户熵可在多个位置增加一层身份验证。因此，每当应用程序需要访问 UserEntropy 保管库中的共享数据（包括密码、PIN 和证书）时，用户都必须进行身份验证。

您可以通过阅读关于 MDX Toolkit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极大的灵活性，但它们也可能限制用户。在某些情况下，您可能需要这种限制，但策略也可能导致系统无法使用。例如，您可能希望阻止访问 Siri 或 iCloud 等可能将敏感数据发送到外部位置的云应用程序。您可以设置策略来阻止访问这些服务，但请记住，此类策略可能会产生意想不到的后果。例如，iOS 键盘麦克风依赖于云访问。

应用程序

企业移动管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 使组织能够保护和控制移动设备，而 MAM 则简化了应用程序交付和管理。随着 BYOD 的日益普及，您通常可以实施 MAM 解决方案（例如 Citrix Endpoint Management）来协助完成以下任务：

- 应用程序交付
- 软件许可
- 配置
- 应用程序生命周期管理

借助 Citrix Endpoint Management，您可以通过配置特定的 MAM 策略和 VPN 设置来增强这些应用程序的安全性，以防止数据泄露和其他安全威胁。Citrix 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之外，Citrix Endpoint Management 还通过 MDX 技术提供应用程序容器化。MDX 通过独立于平台提供的设备级加密的加密来保护应用程序。您可以擦除或锁定应用程序。应用程序受细粒度基于策略的控制。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，用户使用各种移动应用程序来协助其工作职责。这些应用程序可以包括来自公共应用商店的应用程序、内部开发的应用程序或本机应用程序。Citrix Endpoint Management 将这些应用程序分类如下：

公共应用程序： 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。组织外部的供应商通常会在公共应用商店中提供其应用程序。此选项允许其客户直接从互联网下载应用程序。根据用户的需求，您可能在组织中使用许多公共应用程序。此类应用程序的示例包括 GoToMeeting、Salesforce 和 EpicCare 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 对其进行包装以进行企业分发。要启用 MDX 的第三方应用程序，请联系您的应用程序供应商以获取应用程序二进制文件。您可以使用 MDX Toolkit 包装二进制文件，或将 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部独立开发和分发的应用程序。在某些情况下，一些组织可能还拥有 ISV 提供的应用程序。您可以将此类应用程序部署为本机应用程序，也可以使用 MAM 解决方案（例如 Citrix Endpoint Management）对应用程序进行容器化。例如，医疗保健组织可以创建一个内部应用程序，允许医生在移动设备上查看患者信息。然后，组织可以启用 MAM SDK 或 MDM 包装应用程序，以保护患者信息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： 这些应用程序包括从内部网络（Web 应用程序）或通过公共网络 (SaaS) 访问的应用程序。Citrix Endpoint Management 还允许您使用应用程序连接器列表创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器可以促进对现有 Web 应用程序的单点登录 (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断言标记语言 (SAML) 的 Google Apps SAML 进行单点登录到 Google Apps。

移动生产力应用程序： 移动生产力应用程序是 Citrix 开发的应用程序，包含在 Citrix Endpoint Management 许可证中。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 业务就绪应用程序。ISV 使用移动应用程序 SDK 开发业务就绪应用程序。

HDX 应用程序： HDX 应用程序是您使用 StoreFront 发布的 Windows 托管应用程序。如果您有 Citrix Virtual Apps and Desktops 环境，则可以将应用程序与 Citrix Endpoint Management 集成，以使已注册用户可以使用这些应用程序。

根据您计划使用 Citrix Endpoint Management 部署和管理的移动应用程序类型，底层配置和架构有所不同。假设许多具有不同权限级别的用户组使用单个应用程序。在这种情况下，您可以创建单独的交付组来部署两个版本的应用程序。请确保用户组成员资格互斥，以避免用户设备上的策略不匹配。

您可能还希望使用 Apple 批量采购来管理 iOS 应用程序许可。此选项要求您注册 Apple 批量采购计划。并且，您必须使用 Citrix Endpoint Management 控制台来配置批量采购设置。该配置允许您使用批量采购许可证分发应用程序。各种此类用例使得在实施 Citrix Endpoint Management 环境之前评估和规划您的 MAM 策略变得非常重要。您可以通过定义以下内容来开始规划您的 MAM 策略：

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，还要根据不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。此分类有助于您调整每种应用程序所需的 Citrix Endpoint Management 设置。例如：某些应用程序可能不符合包装条件。或者，少数应用程序可能需要使用移动应用程序 SDK 来启用特殊 API 以与其他应用程序交互。

网络要求： 使用适当的设置配置具有特定网络访问要求的应用程序。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互联网访问才能通过 DMZ 路由访问。要允许此类应用程序连接到所需的网络，您必须相应地配置各种设置。提前定义每个应用程序的网络要求有助于最终确定您的架构决策。这项工作简化了整个实施过程。

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、包装、身份验证、地理围栏、密码或数据共享要求。提前概述这些要求以简化您的部署。

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：

- 已启用基于设备平台的加密
- 设备已受管理
- 设备满足最低操作系统版本要求
- 某些应用程序仅供企业用户使用

提前概述此类要求，以便您可以配置相应的部署规则或操作。

许可要求： 记录与应用程序相关的许可要求。此类说明可帮助您有效地管理许可证使用情况，并决定是否需要在 Citrix Endpoint Management 中配置特定功能以方便许可。例如，如果您部署免费或付费的 iOS 应用程序，Apple 会通过要求用户登录其 Apple Store 帐户来对应用程序强制执行许可要求。您可以注册 Apple 批量采购计划，通过 Citrix Endpoint Management 分发和管理这些应用程序。批量采购允许用户下载应用程序，而无需登录其 Apple Store 帐户。此外，Samsung Knox 等工具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。创建应用程序允许列表，这些应用程序会导致设备不合规。然后，设置策略以在设备不合规时触发。另一方面，某个应用程序可能可以接受使用，但由于某种原因可能属于阻止列表。在这种情况下，您可以将应用程序添加到允许列表，并指出该应用程序可以接受使用，但不是必需的。此外，请记住，新设备上预装的应用程序可能包含一些不属于操作系统的常用应用程序。这些应用程序可能与您的阻止列表策略冲突。

应用程序用例

一家医疗保健组织计划部署 Citrix Endpoint Management，作为其移动应用程序的 MAM 解决方案。移动应用程序将交付给企业用户和 BYOD 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

- **Citrix Secure Hub：** 所有移动设备用于与 Citrix Endpoint Management 通信的客户端。IT 通过 Citrix Secure Hub 客户端将安全设置、配置和移动应用程序推送到移动设备。Android 和 iOS 设备通过 Citrix Secure Hub 注册到 Citrix Endpoint Management。
- **Citrix Workspace 应用程序：** 允许用户在移动设备上打开由 Citrix Virtual Apps 托管的应用程序的移动应用程序。

- **GoToMeeting**：一款在线会议、桌面共享和视频会议客户端，允许用户通过互联网与其他的计算机用户、客户、委托人或同事实时会面。
- **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整合在一起，为任何 Salesforce 用户提供统一的体验。
- **RSA SecurID**：用于双因素身份验证的基于软件的令牌。
- **EpicCare 应用程序**：这些应用程序为医疗保健从业者提供对患者图表、患者列表、日程表和消息的安全便携式访问。
  - **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**：用于电子健康记录管理的 Epic 客户端应用程序。

ISV

- **Vocera**：符合 HIPAA 标准的 IP 语音和消息移动应用程序，可通过 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**：一款应用程序，可帮助撰写加密消息、在内部邮件服务器上搜索地址簿，并使用电子邮件客户端将加密消息发送给联系人。

内部 WEB 应用程序

- **PatientRounding**：用于不同部门记录患者健康信息的 Web 应用程序。
- **Outlook Web Access**： 允许通过 Web 浏览器访问电子邮件。
- **SharePoint**： 用于组织范围内的文件和数据共享。

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 封装	IOS	安卓
Citrix 安全邮件	移动生产力应用程序	版本 10.4.1 及更高版本为否	是	是
Citrix 安全浏览器	移动生产力应用程序	版本 10.4.1 及更高版本不支持	是	是

应用程序名称	应用程序类型	MDX 封装	IOS	安卓
Citrix 文件	移动生产力应用	版本 10.4.1 及更高版本不支持	是	是
思杰安全中心	公共应用	不适用	是	是
Citrix Workspace 应用程序	公共应用	不适用	是	是
GoToMeeting	公共应用	不适用	是	是
SalesForce1	公共应用	不适用	是	是
RSA SecurID	公共应用	不适用	是	是
Epic 海库	公共应用	不适用	是	是
Epic 坎托	公共应用	不适用	是	否
Epic 漫游者	公共应用	不适用	是	否
史诗超空间	HDX™ 应用程序	不适用	是	是
沃西拉	ISV 应用程序	是	是	是
艾尺邮件	内部应用程序	是	是	是
PatientRounding	Web 应用	不适用	是	是
Outlook Web 访问	Web 应用	不适用	是	是
SharePoint	Web 应用	不适用	是	是

下表列出了在 Citrix Endpoint Management 中配置 MAM 策略时可以参考的具体要求。

应用程序名称	需要 VPN	交互（与容器外部的应用程序）	交互（来自容器外部的应用程序）	基于设备平台的加密
思杰安全邮件	是	选择性允许	允许	不需要
思杰安全 Web	是	允许	允许	不需要
Citrix 文件	是	允许	允许	不需要
Citrix 安全中心	是	不适用	不适用	不适用
Citrix 工作区应用程序	是	不适用	不适用	不适用
GoToMeeting	否	不适用	不适用	不适用
SalesForce1	否	不适用	不适用	不适用
RSA SecurID	否	不适用	不适用	不适用
史诗 海库	是	不适用	不适用	不适用
史诗 坎托	是	不适用	不适用	不适用
史诗 漫游者	是	不适用	不适用	不适用
Epic 超空间	是	不适用	不适用	不适用
沃西拉	是	已阻止	已阻止	不需要
HCMail 邮件	是	已阻止	已阻止	必需
PatientRounding	是	不适用	不适用	必需
Outlook Web 访问	是	不适用	不适用	非必需
SharePoint	是	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SDK	最低操作系统版本
思杰安全邮件	必需	不适用	选择性必需	不适用	强制执行
Citrix 安全 Web	必需	不适用	非必需	不适用	强制执行
安全备忘录	必需	不适用	非必需	不适用	强制执行
Citrix 文件	必需	不适用	不需要	不适用	已强制执行
思杰安全中心	不需要	批量购买	不需要	不适用	未强制执行
Citrix Workspace 应用程序	不需要	批量购买	不需要	不适用	未强制执行
GoToMeeting	不需要	批量采购	不需要	不适用	未强制执行
SalesForce1	不需要	批量采购	不需要	不适用	未强制执行
RSA SecurID	不需要	批量采购	不需要	不适用	不强制执行
埃匹克 海库	不需要	批量采购	不需要	不适用	不强制执行
埃匹克 坎托	不需要	批量采购	不需要	不适用	未强制执行
埃匹克 罗孚	不需要	批量购买	不需要	不适用	未强制执行
埃匹克 超空间	不需要	不适用	不需要	不适用	未强制执行
沃西拉	需要	不适用	必需	必需	强制执行
HC邮件	必需	不适用	必需	必需	强制执行
PatientRound-ing	必需	不适用	非必需	不适用	未强制执行

应用程序名称	代理过滤	许可	地理围栏	移动应用SDK	最低操作系统版本
Outlook 网页访问	必需	不适用	非必需	不适用	未强制执行
SharePoint	必需	不适用	非必需	不适用	未强制执行

用户社区

每个组织都由在不同职能角色中运作的多元用户社区组成。这些用户社区使用您通过用户设备提供的各种资源来执行不同的任务和办公职能。用户可能在家中或远程办公室使用您提供的移动设备工作。或者，用户可能拥有自己的移动设备，这些设备允许他们访问受某些安全合规性规则约束的工具。

随着越来越多的用户群开始在工作中利用移动设备，企业移动管理 (EMM) 对于防止数据泄露变得至关重要。EMM 对于强制执行组织的安全限制也至关重要。为了实现高效且更复杂的移动设备管理，您可以对用户群进行分类。这样做可以简化用户到资源的映射，并将适当的安全策略与用户关联起来。

以下示例说明了医疗保健组织的用户群如何为 EMM 进行分类。

用户群用例

这个示例医疗保健组织为许多用户提供技术资源和访问权限，包括网络和附属员工以及志愿者。该组织已选择仅向非执行用户推出 EMM 解决方案。

该组织的用户角色和职能可分为子组，包括：临床、非临床和承包商。选定的用户会收到公司移动设备，而其他用户可以从其个人设备访问有限的公司资源。为了强制执行适当级别的安全限制并防止数据泄露，该组织决定由公司 IT 管理每个注册设备。这些设备可能是公司所有或自带设备 (BYOD)。此外，用户只能注册一台设备。

以下部分概述了每个子组的角色和职能：

临床

- 护士
- 医生（内科医生、外科医生等）
- 专家（营养师、麻醉师、放射科医生、心脏病专家、肿瘤科医生等）
- 外部医生（非雇员医生和在远程办公室工作的办公室职员）
- 家庭医疗服务（为患者上门就诊提供医生服务的办公室和移动工作人员）
- 研究专家（六个研究所的知识工作者和高级用户，从事临床研究以寻找医学问题的答案）

- 教育和培训（教育和培训领域的护士、医生和专家）

非临床

- 共享服务（办公室工作人员执行各种后台职能，包括人力资源、薪资、应付账款和供应链服务）
- 医生服务（办公室工作人员为提供商执行各种医疗保健管理、行政服务和业务流程解决方案，包括：行政服务、分析和商业智能、业务系统、客户服务、财务、管理式医疗管理、患者访问解决方案、收入周期解决方案等）
- 支持服务（办公室工作人员执行各种非临床职能，包括：福利管理、临床整合、通信、薪酬和绩效管理、设施和物业服务、人力资源技术系统、信息服务、内部审计和流程改进等）
- 慈善项目（办公室和移动工作人员执行各种职能以支持慈善项目）

承包商

- 制造商和供应商合作伙伴（通过站点到站点 VPN 在现场和远程连接，提供各种非临床支持功能）

根据上述信息，组织创建了以下实体。有关 Citrix 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 组织单位 = Citrix Endpoint Management 资源：

- OU = 临床；组 =
  - XM-护士
  - XM-医生
  - XM-专家
  - XM-外部医生
  - XM-家庭健康服务
  - XM-研究专家
  - XM-教育与培训
- OU = 非临床；组 =
  - XM-共享服务
  - XM-医生服务
  - XM-支持服务
  - XM-慈善项目

CITRIX ENDPOINT MANAGEMENT 本地用户和组

对于组=承包商，用户 =

- 供应商1
- 供应商2
- 供应商 3
- … 供应商 10

CITRIX 端点管理 交付组

- 临床-护士
- 临床-医生
- 临床-专家
- 临床-外部医生
- 临床-家庭健康服务
- 临床-研究专家
- 临床-教育和培训
- 非临床-共享服务
- 非临床-医生服务
- 非临床-支持服务
- 非临床-慈善项目

交付组和用户组映射

活动目录组	CITRIX 端点管理交付组
XM-护士	临床-护士
XM-医生	临床-医生
XM-专家	临床-专家
XM-外部医生	临床-外部医生
XM-家庭健康服务	临床-家庭健康服务
XM-研究专家	临床-研究专家
XM-教育和培训	临床-教育和培训

活动目录组	CITRIX 端点管理交付组
XM-共享服务	非临床-共享服务
XM-医生服务	非临床-医生服务
XM-支持服务	非临床-支持服务
XM-慈善项目	非临床-慈善项目

交付组和资源映射

以下表格说明了此用例中分配给每个交付组的资源。第一个表格显示了移动应用程序分配。第二个表格显示了公共应用程序、HDX 应用程序和设备管理资源。

思杰端点管理交付组	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-医生			
临床-专家			
临床 - 外部医生	X		
临床 - 家庭健康服务	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 - 医生服务		X	X
非临床支持服务	X	X	X
非临床慈善项目	X	X	X
承包商	X	X	X

思杰端点管理交付组	公共应用：RSA SECURID	公共应用：EPICCARE HAIKU	HDX 应用程序：EPIC HYPERSPACE	密码策略	设备限制	自动化操作	网络策略
临床护士							X
临床医生					X		
临床专家							
临床外部医生							
临床家庭健康服务							
临床研究专家							
临床教育和培训		X	X				
非临床共享服务		X	X				
非临床医生服务		X	X				
非临床支持服务		X	X				

注意事项

- Citrix Endpoint Management 在初始配置期间会创建一个名为“所有用户”的默认交付组。如果您不禁用此交付组，则所有 Active Directory 用户都有权注册到 Citrix Endpoint Management。
- Citrix Endpoint Management 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果用户所属的组未在 Citrix Endpoint Management 中映射，则该用户无法注册。同样，如果用户是多个组的成员，Citrix Endpoint Management 只会将该用户归类为映射到 Citrix Endpoint Management 的组的一部分。

安全要求

与 Citrix Endpoint Management 环境相关的安全考虑范围可能很快变得令人应接不暇。其中有许多相互关联的组件和设置。您可能不知道从何开始，也不知道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 提供了高、更高和最高安全级别的建议，如下表所示。

安全问题并非是设备注册模式（MAM、MDM+MAM（MDM 可选）或 MDM+MAM（MDM 必需））的唯一考虑因素。同样重要的是，还要审查用例要求，并在选择管理模式之前确定是否可以缓解安全问题。

高： 使用这些设置可在保持大多数组织可接受的基本安全级别的同时，提供最佳用户体验。

更高： 这些设置在安全性和可用性之间实现了更强的平衡。

最高： 遵循这些建议可在牺牲可用性和用户采用率的情况下提供高安全级别。

管理模式安全注意事项

下表指定了每个安全级别的管理模式。

高安全性	更高安全性	最高安全性
MAM, MDM+MAM	MDM+MAM	MDM+MAM

注意：

- 根据用例，仅限 MAM 的部署可以满足安全要求并提供良好的用户体验。
- 对于BYOD等用例，如果所有业务和安全要求仅通过应用程序容器化即可满足，Citrix 建议使用仅MAM模式。
- 对于高安全性环境（以及公司发放的设备），Citrix 建议使用MDM+MAM，以利用所有可用的安全功能。

Citrix ADC 和 NetScaler Gateway 安全注意事项

下表列出了针对每个安全级别的 Citrix ADC 和 NetScaler Gateway 建议。

高安全性	更高安全性	最高安全性
建议使用 Citrix ADC。MAM 和 MDM+MAM 需要 NetScaler Gateway。	如果 Citrix Endpoint Management 位于 DMZ 中，则使用 XenMobile 向导配置的标准 NetScaler 和 SSL 桥接。	具有端到端加密的 SSL 卸载

注意：

- 通过 NAT 或现有第三方代理/负载均衡器将 Citrix Endpoint Management 服务器暴露给 Internet 可能是 MDM 的一个选项。但是，在这种情况下，SSL 流量终止于 Citrix Endpoint Management 服务器，这会带来潜在的安全风险。
- 对于高安全性环境，具有默认 Citrix Endpoint Management 配置的 NetScaler Gateway 通常可以满足或超出安全要求。
- 对于具有最高安全需求的 MDM 注册，NetScaler Gateway 上的 SSL 终止使您能够在外围检查流量，同时保持端到端 SSL 加密。
- 定义 SSL/TLS 密码的选项。
- 有关详细信息，请参阅 Integrating with NetScaler Gateway and Citrix ADC。

注册安全注意事项

下表指定了 Citrix ADC 和 NetScaler Gateway 针对每个安全级别的建议。

高安全性	更高安全性	最高安全性
仅限 Active Directory 组成员身份。“所有用户”交付组已禁用。	仅限邀请的注册安全模式。仅限 Active Directory 组成员身份。“所有用户”交付组已禁用	注册安全模式与设备 ID 绑定。仅限 Active Directory 组成员身份。“所有用户”交付组已禁用

注意：

- Citrix 通常建议您将注册限制为仅限于预定义的 Active Directory 组中的用户。此限制要求禁用内置的“所有用户”交付组。

- 您可以使用注册邀请将注册限制为仅限于拥有邀请的用户。注册邀请不适用于 Windows 设备。
- 您可以使用一次性 PIN (OTP) 注册邀请作为双因素身份验证解决方案，并控制用户可以注册的设备数量。（OTP 邀请不适用于 Windows 设备。）

设备密码安全注意事项

下表指定了针对每个安全级别的设备密码建议。

高安全性	更高安全性	最高安全性
建议。设备级加密需要高安全性。可通过 MDM 强制执行。可通过 MDX 策略“不合规设备行为”设置为仅限 MAM 所需。	通过使用 MDM、MAM 或 MDM+MAM 策略强制执行。	通过使用 MDM 和 MDX 策略强制执行。MDM 复杂密码策略。

注意：

- Citrix 建议使用设备密码。
- 您可以通过 MDM 策略强制执行设备密码。
- 您可以使用 MDX 策略将设备密码设置为使用托管应用程序的要求；例如，对于 BYOD 用例。
- Citrix 建议结合使用 MDM 和 MDX 策略选项，以提高 MDM+MAM 注册的安全性。
- 对于具有最高安全要求的环境，您可以配置复杂的密码策略并通过 MDM 强制执行。您可以配置自动操作，以便在设备不遵循密码策略时通知管理员或执行选择性/完全设备擦除。

应用程序

企业移动管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 使组织能够保护和控制移动设备，而 MAM 则有助于应用程序交付和管理。随着 BYOD 的日益普及，您通常可以实施 MAM 解决方案，例如 Citrix Endpoint Management。Citrix Endpoint Management 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。您可以要求或允许用户选择加入 MDM 管理。

借助 Citrix Endpoint Management，您可以通过配置 MAM 策略和 VPN 设置来保护应用程序，以防止数据泄露和其他安全威胁。Citrix Endpoint Management 为组织提供了将设备注册为仅限 MAM 或 MDM+MAM 的灵活性。

除了能够将应用程序交付到移动设备之外，Citrix Endpoint Management 还通过 MDX 技术提供应用程序容器化。这些应用程序受精细的基于策略的控制。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，用户使用各种移动应用程序来协助其工作。这些应用程序可以包括来自公共应用商店的应用程序、内部开发的应用程序或本机应用程序。Citrix Endpoint Management 将这些应用程序分类如下：

- **公共应用程序：** 这些应用程序包括在公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。组织外部的供应商通常会在公共应用商店中提供其应用程序。此选项允许其客户直接从 Internet 下载应用程序。您可能根据用户的需求在组织中使用许多公共应用程序。此类应用程序的示例包括 GoToMeeting、Salesforce 和 EpicCare 应用程序。
  - **如果您使用 MAM SDK：** 从您的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获取应用程序二进制文件。然后，您可以使用 MDX Toolkit 打包这些二进制文件。
- **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部独立开发和分发的应用程序。在某些情况下，一些组织可能还拥有 ISV 提供的应用程序。您可以将此类应用程序部署为本机应用程序，或者使用 MAM 解决方案（例如 Citrix Endpoint Management）对应用程序进行容器化。

  例如，医疗保健组织可能会创建一个内部应用程序，允许医生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保护患者信息并启用对患者数据库的 VPN 访问：
  - MAM SDK
  - MDX 工具包
- **Web 和 SaaS 应用程序：** 这些应用程序包括从内部网络（Web 应用程序）或通过公共网络（SaaS）访问的应用程序。Citrix Endpoint Management 还允许您使用应用程序连接器列表创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器可以促进对现有 Web 应用程序的单点登录 (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断言标记语言 (SAML) 的 Google Apps SAML 进行单点登录到 Google Apps。

- **移动生产力应用程序：** 移动生产力应用程序是 Citrix 开发的应用程序，包含在 Citrix Endpoint Management 许可证中。有关详细信息，请参阅 关于移动生产力应用程序。Citrix 还提供其他由 ISV 使用移动应用程序 SDK 开发的 业务就绪应用程序。
- **HDX 应用程序：** HDX 应用程序是您使用 StoreFront 发布的 Windows 托管应用程序。如果您使用 Citrix Virtual Apps and Desktops 和 Citrix Workspace，则已注册用户可以使用 HDX 应用程序。

根据您计划使用 Citrix Endpoint Management 部署和管理的移动应用程序类型，底层配置可能有所不同。例如，许多具有不同权限级别的用户组可能会使用单个应用程序。在这种情况下，您可以创建单独的交付组来部署同一应用程序的两个不同版本。此外，您必须确保用户组成员资格是互斥的，以避免用户设备上出现策略不匹配。

您还可以通过使用 Apple Volume Purchase 来管理 iOS 应用程序许可。此选项要求您注册 Volume Purchase 计划并在 Citrix Endpoint Management 控制台中配置 Volume Purchase 设置。该配置允许您分发带有 Volume Purchase 许可证的应用程序。在实施 Citrix Endpoint Management 环境之前，各种用例使得评估和规划您的 MAM 策略变得非常重要。您可以通过定义以下内容来开始规划您的 MAM 策略：

- **应用程序类型：** 列出您计划支持的不同类型的应用程序并对其进行分类，例如公共、原生、Web、内部或 ISV 应用程序。此外，还要根据不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。这种分类有助于调整每种应用程序类型所需的各种 Citrix Endpoint Management 设置。例如，某些应用程序可能需要使用移动应用程序 SDK 来启用特殊 API 以便与其他应用程序进行交互。
- **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 访问才能通过 DMZ 路由访问。为了允许此类应用程序连接到所需的网络，您必须相应地配置各种设置。提前定义每个应用程序的网络要求有助于完成您的架构决策，从而简化整个实施过程。
- **安全要求：** 您可以定义安全要求，以应用于单个应用程序或所有应用程序。
    - 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容器化、MDX、身份验证、地理围栏、密码或数据共享要求

  提前概述这些要求以简化您的部署。有关 Citrix Endpoint Management 中安全性的详细信息，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，某些应用程序可能要求设备受管理或设备满足最低操作系统版本。您可能还希望某些应用程序仅供企业用户使用。提前概述此类要求，以便您可以配置适当的部署规则或操作。

- **许可要求：** 记录与应用程序相关的许可要求。您的记录可以帮助您有效管理许可证使用情况，并决定是否在 Citrix Endpoint Management 中配置特定功能以方便许可。例如，如果您部署免费或付费的 iOS 应用程序，Apple 会对该应用程序强制执行许可要求。因此，用户必须登录其 Apple App Store 帐户。

  但是，您可以注册 Apple Volume Purchase，以使用 Citrix Endpoint Management 分发和管理这些应用程序。Volume Purchase 允许用户下载应用程序，而无需登录其 Apple App Store 帐户。

  某些平台在部署这些功能之前需要完成特殊的许可要求。

- **允许列表和阻止列表要求：** 您可能会识别出不希望用户安装或使用的应用程序。创建阻止列表定义了一个不合规事件。然后，您可以设置策略以在事件发生时触发。另一方面，某个应用程序可能可以接受使用，但由于某种原因可能属于阻止列表。在这种情况下，您可以将应用程序添加到允许列表，并指出该应用程序可以接受使用但不是必需的。此外，请记住，新设备上预安装的应用程序可能包含一些不属于操作系统的常用应用程序。此类应用程序可能与您的阻止列表策略冲突。

用例

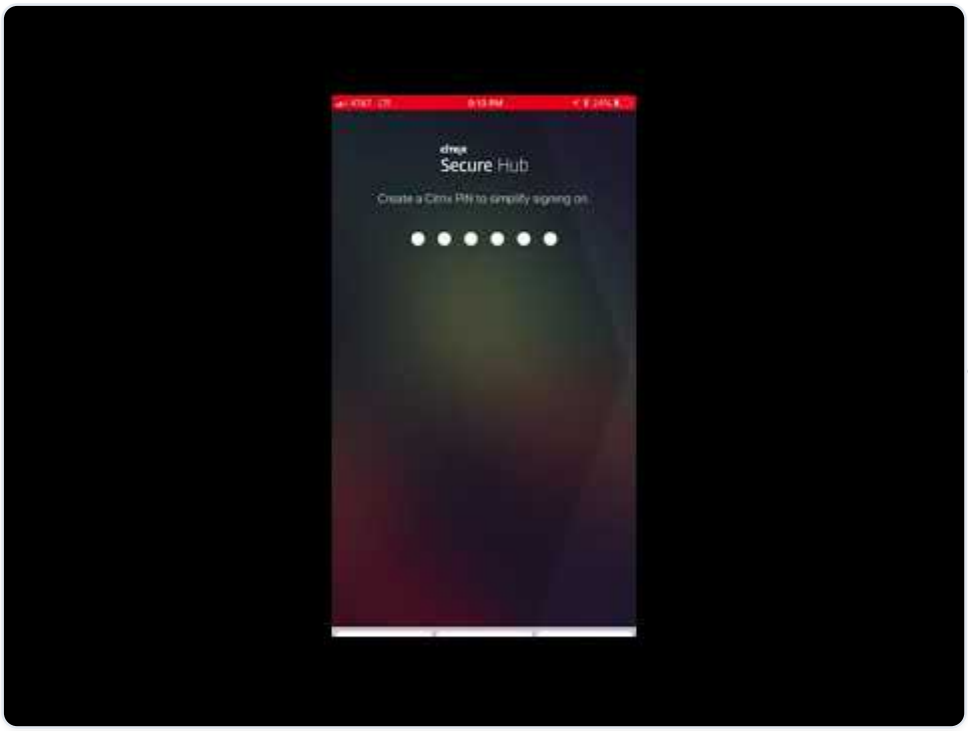
一家医疗保健机构计划部署 Citrix Endpoint Management，以作为其移动应用的 MAM 解决方案。移动应用将交付给企业用户和 BYOD 用户。IT 部门决定交付和管理以下应用：

移动生产力应用： Citrix 提供的 iOS 和 Android 应用。有关详细信息，请参阅移动生产力应用。

Citrix Secure Hub： 对于在 Citrix Endpoint Management 10.18.14 之前加入的客户：您可以使用 Citrix Secure Hub 将安全设置、配置和移动应用推送到移动设备。Android 和 iOS 设备通过 Citrix Secure Hub 注册到 Citrix Endpoint Management。

对于 Citrix Endpoint Management 10.18.14 的新客户：Citrix Secure Hub 支持使用 Workspace 应用商店。打开 Citrix Secure Hub 时，用户将不再看到 Citrix Secure Hub 商店。现在，一个“添加应用”按钮会将用户带到 Workspace 应用商店。

以下视频展示了 iOS 设备使用 Citrix Workspace 应用程序执行 Citrix Endpoint Management 注册的过程。



。

Citrix Workspace 应用程序： Citrix Workspace 应用程序集成了现有的 Citrix Receiver 技术、Citrix Secure Hub 和其他 Citrix Workspace 客户端技术。Citrix Workspace 应用程序为最终用户提供了统一的上下文体验。

GoToMeeting： 一款在线会议、桌面共享和视频会议客户端，允许用户通过 Internet 与其他计算机用户、客户、客户端或同事实时会面。

SalesForce1： Salesforce1 允许用户从移动设备访问 Salesforce，并将所有 Chatter、CRM、自定义应用和业务流程整合到任何 Salesforce 用户的统一体验中。

RSA SecurID： 用于双因素身份验证的基于软件的令牌。

EpicCare 应用： 这些应用为医疗保健从业者提供对患者图表、患者列表、日程和消息的安全便携式访问。

Haiku： 适用于 iPhone 和 Android 手机的移动应用。

Canto： 适用于 iPad 的移动应用

Rover： 适用于 iPhone 和 iPad 的移动应用。

HDX： 这些应用通过 Citrix Workspace 中的 Citrix Virtual Apps 交付。

- **Epic Hyperspace：**用于电子健康记录管理的 Epic 客户端应用程序。

ISV：

- **Vocera：**符合 HIPAA 规范的 IP 语音和消息移动应用程序，可通过 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：**可帮助撰写加密邮件、在内部邮件服务器上搜索地址簿，并使用电子邮件客户端将加密邮件发送给联系人的应用程序。

内部 Web 应用程序：

- **PatientRounding：**用于不同部门记录患者健康信息的 Web 应用程序。
- **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	已启用 MDX	IOS	安卓
思杰安全邮件	移动生产力应用	否	是	是
思杰安全浏览器	移动生产力应用	否	是	是
思杰文件	移动生产力应用	否	是	是
Citrix 安全中心	公共应用	不适用	是	是
Citrix Workspace 应用程序	公共应用	不适用	是	是
GoToMeeting	公共应用	不适用	是	是
SalesForce1	公共应用	不适用	是	是
RSA SecurID	公共应用	不适用	是	是
Epic 俳句	公共应用	不适用	是	是
Epic 坎托	公共应用	不适用	是	否
Epic 漫游者	公共应用	不适用	是	否
Epic 超空间	HDX 应用	不适用	是	是

应用程序名称	应用程序类型	已启用 MDX	IOS	安卓
沃赛拉	ISV 应用	是	是	是
HC邮件	内部应用	是	是	是
PatientRounding	Web 应用	不适用	是	是
Outlook Web 访问	Web 应用	不适用	是	是
SharePoint	Web 应用	不适用	是	是

下表列出了在 Citrix Endpoint Management 中配置 MAM 策略时可以参考的具体要求。

应用程序名称	需要 VPN	交互（与容器外部的应用程序）	交互（来自容器外部的应用程序）	代理过滤	许可	地理围栏	移动应用SDK	最低操作系统版本
Citrix 安全邮件	是	选择性允许	允许	必需	不适用	选择性必需	不适用	强制执行
Citrix 安全浏览器	是	允许	允许	必需	不适用	非必需	不适用	强制执行
Citrix 文件	是	允许	允许	必需	不适用	非必需	不适用	强制执行
思杰安全中心	是	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 Workspace 应用程序	是	不适用	不适用	不需要	批量采购	不需要	不适用	未强制执行

应用程序名称	需要VPN	交互（与容器外部的应用程序）	交互（来自容器外部的应用程序）	代理过滤	许可	地理围栏	移动应用SDK	最低操作系统版本
GoTo Meeting	否	不适用	不适用	不需要	批量采购	不需要	不适用	未强制执行
Sales Force 1	否	不适用	不适用	不需要	批量采购	不需要	不适用	未强制执行
RSA SecurID	否	不适用	不适用	不需要	批量采购	不需要	N/A	未强制执行
艾派克海库	是	N/A	N/A	不需要	批量购买	不需要	N/A	未强制执行
艾派克坎托	是	N/A	N/A	不需要	批量购买	不需要	不适用	未强制执行
Epic罗孚	是	不适用	不适用	不需要	批量购买	不需要	不适用	未强制执行
Epic超空间	是	不适用	不适用	不需要	不适用	不需要	不适用	未强制执行
沃塞拉	是	已阻止	已阻止	必需	不适用	必需	必需	强制
HC邮件	是	已阻止	已阻止	必需	不适用	必需	必需	强制
PatientRound-ing	是	不适用	不适用	必需	不适用	非必需	不适用	未强制执行
Outlook Web访问	是	不适用	不适用	必需	不适用	非必需	不适用	未强制执行

应用程序名称	需要VPN	交互（与容器外部的应用程序）	交互（来自容器外部的应用程序）	代理过滤	许可	地理围栏	移动应用SDK	最低操作系统版本
Share Point	是	不适用	不适用	必需	不适用	非必需	不适用	未强制执行

用户社区

每个组织都由在不同职能角色中运作的多元用户社区组成。这些用户社区通过您提供的用户移动设备执行不同的任务和办公职能，并使用各种资源。用户可能在家中或远程办公室使用您提供的移动设备工作。或者，用户可能使用个人移动设备，这允许他们访问受某些安全合规规则约束的工具。

With more user communities using mobile devices, Enterprise Mobility Management (EMM) becomes critical to prevent a data leak and to enforce organizational security restrictions. For efficient and more sophisticated Mobile Device Management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and makes sure that the right security policies apply to the right users.

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

  Users added to specific Active Directory security groups can receive policies and resources such as apps. Removing users from the Active Directory security groups removes access to previously allowed Citrix Endpoint Management resources.

- Citrix Endpoint Management 本地用户和组

  For users who don't have an account in Active Directory, you can create the users as local Citrix Endpoint Management users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- 思杰端点管理交付组

  如果许多具有不同权限级别的用户组要使用单个应用程序，您可能需要创建单独的交付组。通过单独的交付组，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，也可以是一对多。将基本策略和应用程序分配给一对多交付组映射。将特定于功能的策略和应用程序分配给一对一交付组映射。

- 交付组和应用程序资源映射

  将特定应用程序分配给每个交付组。

- 交付组和 MDM 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，可以按以下任意组合配置交付组：应用程序类型（公共、HDX™ 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。

以下示例说明了医疗保健组织的用户社区是如何为 EMM 分类的。

用例

这个示例医疗保健组织为许多用户（包括网络员工、附属员工和志愿者）提供技术资源和访问权限。该组织已选择仅向非执行用户推出EMM解决方案。

您可以将此组织的用户角色和职能划分为以下子组：临床、非临床和承包商。一部分选定的用户会收到公司移动设备，而其他用户则可以从其个人设备 (BYOD) 访问有限的公司资源。为了实施适当级别的安全限制并防止数据泄露，该组织决定由公司IT管理每个注册设备。此外，用户只能注册一台设备。

以下各节概述了每个子组的角色和职能。

临床

- 护士
- 医生（内科医生、外科医生等）
- 专科医生（营养师、麻醉师、放射科医生、心脏病专家、肿瘤科医生等）
- 外部医生（非雇员医生和在远程办公室工作的办公室职员）
- 家庭医疗服务（为患者上门就诊提供医生服务的办公室和移动工作人员）
- 研究专家（六个研究所的知识工作者和高级用户，从事临床研究以寻找医学问题的答案）
- 教育和培训（教育和培训领域的护士、医生和专家）

非临床

- 共享服务（从事各种后台职能的办公室工作人员，包括：人力资源、薪资、应付账款、供应链服务等）

- 医生服务（从事各种医疗保健管理、行政服务以及为提供商提供业务流程解决方案的办公室工作人员，包括：行政服务、分析和商业智能、业务系统、客户服务、财务、管理式医疗管理、患者访问解决方案、收入周期解决方案等）
- 支持服务（从事各种非临床职能的办公室工作人员，包括：福利管理、临床整合、沟通、薪酬和绩效管理、设施和物业服务、人力资源技术系统、信息服务、内部审计和流程改进等）
- 慈善项目（从事各种职能以支持慈善项目的办公室和移动工作人员）

承包商

- 制造商和供应商合作伙伴（通过站点到站点 VPN 在现场和远程连接，提供各种非临床支持功能）

根据上述信息，组织创建了以下实体。有关 Citrix Endpoint Management 中交付组的更多信息，请参阅 Citrix Endpoint Management 产品文档中的部署资源。

Active Directory 组织单位 (OU) 和组

对于 OU = 思杰端点管理资源

- OU = 临床；组 =
  - XM-护士
  - XM-医生
  - XM-专家
  - XM-外部医生
  - XM-家庭健康服务
  - XM-研究专家
  - XM-教育和培训
- OU = 非临床; 组 =
  - XM-共享服务
  - XM-医生服务
  - XM-支持服务
  - XM-慈善项目

Citrix Endpoint Management 本地用户和组

对于组= 承包商, 用户 =

- 供应商1

- 供应商2
- 供应商3
- … 供应商10

Citrix 端点管理交付组

- 临床护士
- 临床-医生
- 临床-专科医生
- 临床-外部医生
- 临床-家庭健康服务
- 临床-研究专员
- 临床-教育和培训
- 非临床-共享服务
- 非临床-医生服务
- 非临床-支持服务
- 非临床-慈善项目

交付组和用户组映射

活动目录组	CITRIX 端点管理 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-家庭健康服务	临床-家庭健康服务
XM-研究专家	临床-研究专家
XM-教育与培训	临床-教育与培训
XM-共享服务	非临床-共享服务
XM-医师服务	非临床-医生服务

活动目录组	CITRIX 端点管理 交付组
XM-支持服务	非临床-支持服务
XM-慈善项目	非临床-慈善项目

交付组和应用程序的资源映射

	安全邮件	安全 WEB	思杰文件	WORKSPACE 应用	SALESFORCE1	RSA SECURID	EPICCARE 海库	EPIC 超空间
临床-护士	X	X	X					
临床医生								
临床专家								
临床-外部医生	X		X					
临床-家庭健康服务	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

	安全邮件	安全 WEB	思杰文件	WORKSPACE 应用	SALESFORCE1	RSA SECURID	EPICCARE 海库	EPIC 超空间
非临床 - 医生服务							X	X
非临床 - 支持服务	X		X				X	X
非临床 - 慈善项目	X		X				X	X
承包商	X		X	X	X		X	X

MDM 资源的交付组和资源映射

	MDM: 密码策略	MDM: 设备限制	MDM: 自动化操作	MDM: 网络策略
临床-护士				X
临床-医生		X		
临床-专家				
临床-外部医生				
临床-家庭健康服务				
临床-研究专家				
临床-教育和培训				
非临床-共享服务				
非临床-医生服务				

	MDM: 密码策略	MDM: 设备限制	MDM: 自动化操作	MDM: 网络策略
非临床-支持服务				
非临床-慈善项目				
承包商				X

注意事项

- Citrix Endpoint Management 在初始配置期间会创建一个名为“所有用户”的默认交付组。如果您不禁用此交付组，则所有 Active Directory 用户都有权注册到 Citrix Endpoint Management。
- Citrix Endpoint Management 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果用户属于某个未在 Citrix Endpoint Management 中映射的组，则该用户无法注册。同样，如果用户是多个组的成员，Citrix Endpoint Management 只会将用户归类为属于已映射到 Citrix Endpoint Management 的组。

电子邮件策略

从移动设备安全访问电子邮件是任何组织移动性管理计划背后的主要驱动力之一。确定适当的电子邮件策略通常是任何 Citrix Endpoint Management 设计的关键组成部分。Citrix Endpoint Management 提供了多种选项，可根据安全性、用户体验和集成要求来适应不同的用例。本文涵盖了典型的设计决策过程以及选择正确解决方案的注意事项，从客户端选择到邮件流量。

选择您的电子邮件客户端

客户端选择通常是整体电子邮件策略设计中的首要考虑因素。您可以从多种客户端中进行选择：Citrix Secure Mail、特定移动平台操作系统中包含的本机邮件，或通过公共应用商店提供的其他第三方客户端。根据您的需求，您可以使用单个（标准）客户端来支持用户社区，或者可能需要结合使用多种客户端。

下表概述了不同可用客户端选项的一些设计注意事项：

主题	**Citrix 安全邮件**	**本机（例如，iOS 邮件）**	**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。所有其他客户端均被视为第三方客户端。	通常需要用户手动配置。
安全性	设计安全，提供最高安全性。使用 MDX 策略和额外的数据加密级别。Citrix Secure Mail 是通过 MDX 策略完全管理的应用程序。通过 Citrix PIN 增加了一层身份验证。	基于供应商/应用功能集。提供更高的安全性。使用设备加密设置。依赖设备级身份验证来访问应用。	基于供应商/应用功能集。提供高安全性。
集成	默认情况下允许与托管 (MDX) 应用程序交互。使用 Citrix Secure Web 打开 Web URL。将文件保存到 Citrix Files 并从 Citrix Files 附加文件。直接加入 GoToMeeting 并拨入。	默认情况下只能与其他非托管（非 MDX）应用程序交互。	默认情况下只能与其他非托管（非 MDX）应用程序交互。
部署/许可	您可以通过 MDM 直接从公共应用商店推送 Citrix Secure Mail。包含在 Citrix Endpoint Management Advanced 和 Enterprise 许可中。	客户端应用程序随平台操作系统提供。无额外许可要求。	您可以通过 MDM 推送，作为企业应用或直接从公共应用商店推送。相关的许可模式/成本基于应用供应商。
支持	客户端和 EMM 解决方案（Citrix）的单一供应商支持。Citrix Secure Hub/应用调	供应商定义的支援（Apple/Google）。可能需要根据设备平	供应商定义的支援。一个客户端需要支持，前提是第三方客

	试日志记录功能中嵌入了支持联系信息。一个客户端需要支持。	台支持不同的客户端。	户端在所有托管设备平台上都受支持。

邮件流量流和筛选注意事项

本节讨论了 Citrix Endpoint Management 环境中邮件 (ActiveSync) 流量流动的三个主要场景和设计注意事项。

场景 1：暴露的 Exchange

支持外部客户端的环境通常会将 Exchange ActiveSync 服务暴露在互联网上。移动 ActiveSync 客户端通过反向代理（例如 NetScaler Gateway）或边缘服务器，经由这个面向外部的路径进行连接。此选项是使用本机或第三方邮件客户端所必需的，这使得这些客户端成为此场景的流行选择。尽管不常见，但您也可以在此场景中使用 Citrix Secure Mail 客户端。这样做，您将受益于使用 MDX 策略和应用程序管理所提供的安全功能。

场景 2：通过 NetScaler Gateway 隧道连接（微型 VPN 和 STA）

由于其微型 VPN 功能，此场景是使用 Citrix Secure Mail 客户端时的默认设置。在这种情况下，Citrix Secure Mail 客户端通过 NetScaler Gateway 建立到 ActiveSync 的安全连接。本质上，您可以将 Citrix Secure Mail 视为直接从内部网络连接到 ActiveSync 的客户端。Citrix 客户通常将 Citrix Secure Mail 统一为首选的移动 ActiveSync 客户端。这一决定是避免将 ActiveSync 服务暴露在互联网上（如第一个场景所述的暴露的 Exchange Server）的举措的一部分。

只有启用了 MAM SDK 或经过 MDX 封装的应用程序才能使用微型 VPN 功能。如果您使用 MDX 封装，此场景不适用于本机客户端。尽管可能可以使用 MDX 工具包封装第三方客户端，但这种做法并不常见。事实证明，使用设备级 VPN 客户端允许本机或第三方客户端进行隧道访问是繁琐且不可行的解决方案。

场景 3：云托管 Exchange 服务

云托管 Exchange 服务（例如 Microsoft Office 365）正变得越来越流行。在 Citrix Endpoint Management 的背景下，此场景可能与第一个场景以相同的方式处理，因为 ActiveSync 服务也暴露在互联网上。在这种情况下，云服务提供商的要求决定了客户端的选择。这些选择通常包括支持大多数 ActiveSync 客户端，例如 Citrix Secure Mail 以及其他本机或第三方客户端。

Citrix Endpoint Management 可以在此场景的三个方面增加价值：

- 使用 Citrix Secure Mail 的 MDX 策略和应用程序管理客户端
- 通过在受支持的本机电子邮件客户端上使用 MDM 策略进行客户端配置

- 通过使用 Citrix Endpoint Management for Exchange ActiveSync 连接器实现 ActiveSync 筛选选项

邮件流量筛选注意事项

与大多数暴露在互联网上的服务一样，您必须保护路径并为授权访问提供筛选。Citrix Endpoint Management 解决方案包含两个专门设计用于为本机和第三方客户端提供 ActiveSync 筛选功能的组件：NetScaler Gateway for Exchange ActiveSync 连接器和 Citrix Endpoint Management for Exchange ActiveSync 连接器。

NetScaler Gateway Exchange ActiveSync 连接器

NetScaler Gateway 的 Exchange ActiveSync 连接器通过使用 NetScaler Gateway 作为 ActiveSync 流量的代理，在边界提供 ActiveSync 过滤。因此，过滤组件位于邮件流量路径中，拦截进入或离开环境的邮件。Exchange ActiveSync 连接器充当 NetScaler Gateway 和 Citrix Endpoint Management 之间的中介。当设备通过 NetScaler Gateway 上的 ActiveSync 虚拟服务器与 Exchange 通信时，NetScaler Gateway 会向 Exchange ActiveSync 服务的连接器发出 HTTP 调用。然后，该服务会向 Citrix Endpoint Management 检查设备状态。根据设备状态，Exchange ActiveSync 连接器会回复 NetScaler Gateway 以允许或拒绝连接。您还可以配置静态规则，根据用户、代理和设备类型或 ID 过滤访问。

此设置允许将 Exchange ActiveSync 服务公开到互联网，并增加一层安全防护以防止未经授权的访问。设计注意事项包括：

- **Windows Server：** Exchange ActiveSync 组件的连接器需要 Windows Server。
- **过滤规则集：** Exchange ActiveSync 连接器旨在根据设备状态和信息进行过滤，而不是根据用户信息。尽管您可以配置静态规则按用户 ID 进行过滤，但例如，不存在基于 Active Directory 组成员身份进行过滤的选项。如果需要 Active Directory 组过滤，则可以使用 Citrix Endpoint Management 的 Exchange ActiveSync 连接器。
- **NetScaler Gateway 可扩展性：** 鉴于需要通过 NetScaler Gateway 代理 ActiveSync 流量：NetScaler Gateway 实例的适当大小对于支持所有 ActiveSync SSL 连接的额外工作负载至关重要。
- **NetScaler Gateway 集成缓存：** NetScaler Gateway 上的 Exchange ActiveSync 配置连接器使用集成缓存功能来缓存来自连接器的响应。由于此配置，NetScaler Gateway 无需为给定会话中的每个 ActiveSync 事务向连接器发出请求。此配置对于足够的性能和规模也至关重要。集成缓存适用于 NetScaler Gateway Platinum Edition。
- **自定义过滤策略：** 您可能需要创建自定义 NetScaler Gateway 策略，以限制标准原生移动客户端之外的某些 ActiveSync 客户端。此配置需要了解 ActiveSync HTTP 请求和 NetScaler Gateway 响应程序策略的创建。

- **Citrix Secure Mail 客户端：** Citrix Secure Mail 具有微型 VPN 功能，无需在边界进行过滤。通过 NetScaler Gateway 连接时，Citrix Secure Mail 客户端通常可以被视为内部（受信任的）ActiveSync 客户端。如果需要同时支持原生和第三方（使用 Exchange ActiveSync 连接器）以及 Citrix Secure Mail 客户端：Citrix 建议 Citrix Secure Mail 流量不要通过用于连接器的 NetScaler Gateway 虚拟服务器。您可以通过 DNS 实现此流量流，并防止连接器策略影响 Citrix Secure Mail 客户端。

有关 Citrix Endpoint Management 部署中 NetScaler Gateway 的 Exchange ActiveSync 连接器图，请参阅体系结构。

思杰端点管理 的 Exchange ActiveSync 连接器

Citrix Endpoint Management 的 Exchange ActiveSync 连接器是 Citrix Endpoint Management 的一个组件，它在 Exchange 服务级别提供 ActiveSync 过滤。因此，过滤仅在邮件到达 Exchange 服务时发生，而不是在邮件进入 Citrix Endpoint Management 环境时发生。邮件管理器使用 PowerShell 查询 Exchange ActiveSync 以获取设备伙伴关系信息，并通过设备隔离操作控制访问。这些操作根据 Citrix Endpoint Management 的 Exchange ActiveSync 连接器规则标准将设备移入和移出隔离区。

与 NetScaler Gateway 的 Exchange ActiveSync 连接器类似，Exchange ActiveSync 连接器会向 Citrix Endpoint Management 检查设备状态，以根据设备合规性过滤访问。您还可以配置静态规则，根据设备类型或 ID、代理版本和 Active Directory 组成员身份过滤访问。

此解决方案不需要使用 NetScaler Gateway。您可以部署 Exchange ActiveSync 连接器，而无需更改现有 ActiveSync 流量的路由。设计注意事项包括：

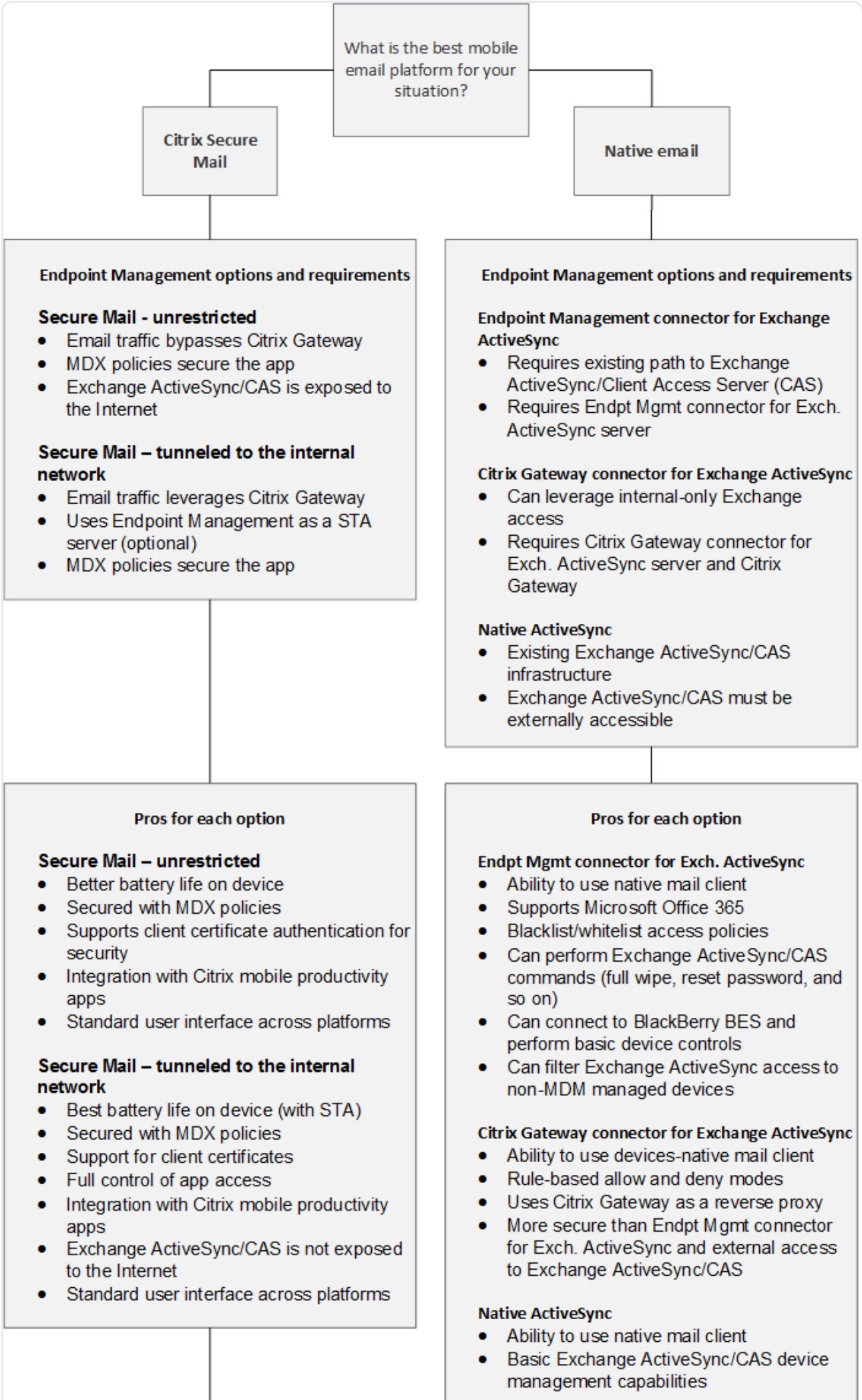
- **Windows Server：** Exchange ActiveSync 连接器要求您部署 Windows Server。
- **过滤规则集：** 与 NetScaler Gateway 的 Exchange ActiveSync 连接器一样，Exchange ActiveSync 连接器包含用于评估设备状态的过滤规则。此外，Exchange ActiveSync 连接器还支持基于 Active Directory 组成员身份进行过滤的静态规则。
- **Exchange 集成：** Exchange ActiveSync 连接器需要直接访问托管 ActiveSync 角色的 Exchange 客户端访问服务器 (CAS)，并控制设备隔离操作。此要求可能会根据环境架构和安全状况带来挑战。您必须预先评估此技术要求。
- **其他 ActiveSync 客户端：** 由于 Exchange ActiveSync 连接器在 ActiveSync 服务级别进行筛选，因此请考虑 Citrix Endpoint Management 环境之外的其他 ActiveSync 客户端。您可以配置 Exchange ActiveSync 连接器静态规则，以避免对其他 ActiveSync 客户端造成意外影响。
- **扩展的 Exchange 功能：** 通过与 Exchange ActiveSync 直接集成，Exchange ActiveSync 连接器使 Citrix Endpoint Management 能够在移动设备上执行 Exchange ActiveSync 擦除。

Exchange ActiveSync 连接器还允许 Citrix Endpoint Management 访问有关 Blackberry 设备的信息并执行其他控制操作。

有关 Citrix Endpoint Management 部署中 Citrix Endpoint Management 的 Exchange ActiveSync 连接器的图示，请参阅体系结构。

电子邮件平台决策树

下图可帮助您区分在 Citrix Endpoint Management 部署中使用本机电子邮件或 Citrix Secure Mail 解决方案的优缺点。每个选择都允许相关的 Citrix Endpoint Management 选项和要求，以启用服务器、网络和数据库访问。优缺点包括有关安全性、策略和用户界面注意事项的详细信息。


What is the best mobile email platform for your situation?
Citrix Secure Mail
Native email
Endpoint Management options and requirements
Secure Mail - unrestricted
Email traffic bypasses Citrix Gateway
MDX policies secure the app
Exchange ActiveSync/CAS is exposed to the Internet
Secure Mail – tunneled to the internal network
Email traffic leverages Citrix Gateway
Uses Endpoint Management as a STA server (optional)
MDX policies secure the app
Endpoint Management options and requirements
Endpoint Management connector for Exchange ActiveSync
Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
Requires Endpt Mgmt connector for Exch. ActiveSync server
Citrix Gateway connector for Exchange ActiveSync
Can leverage internal-only Exchange access
Requires Citrix Gateway connector for Exch. ActiveSync server and Citrix Gateway
Native ActiveSync
Existing Exchange ActiveSync/CAS infrastructure
Exchange ActiveSync/CAS must be externally accessible
Pros for each option
Secure Mail – unrestricted
Better battery life on device
Secured with MDX policies
Supports client certificate authentication for security
Integration with Citrix mobile productivity apps
Standard user interface across platforms
Secure Mail – tunneled to the internal network
Best battery life on device (with STA)
Secured with MDX policies
Support for client certificates
Full control of app access
Integration with Citrix mobile productivity apps
Exchange ActiveSync/CAS is not exposed to the Internet
Standard user interface across platforms
Pros for each option
Endpt Mgmt connector for Exch. ActiveSync
Ability to use native mail client
Supports Microsoft Office 365
Blacklist/whitelist access policies
Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
Can connect to BlackBerry BES and perform basic device controls
Can filter Exchange ActiveSync access to non-MDM managed devices
Citrix Gateway connector for Exchange ActiveSync
Ability to use devices-native mail client
Rule-based allow and deny modes
Uses Citrix Gateway as a reverse proxy
More secure than Endpt Mgmt connector for Exch. ActiveSync and external access to Exchange ActiveSync/CAS
Native ActiveSync
Ability to use native mail client
Basic Exchange ActiveSync/CAS device management capabilities

Citrix 端点管理集成

本文介绍了在规划 Citrix Endpoint Management 如何与您现有网络和解决方案集成时需要考虑的事项。例如，如果您已将 NetScaler Gateway 用于 Citrix Virtual Apps and Desktops：

- 您是想使用现有的 NetScaler Gateway 实例，还是使用新的专用实例？
- 您是否希望将使用 StoreFront 发布的 HDX 应用程序与 Citrix Endpoint Management 集成？
- 您是否计划将 Citrix Files 与 Citrix Endpoint Management 结合使用？
- 您是否有想要集成到 Citrix Endpoint Management 中的网络访问控制解决方案？

NetScaler 网关

Citrix Endpoint Management 需要 NetScaler Gateway。NetScaler Gateway 为访问所有公司资源提供微型 VPN 路径，并提供强大的多重身份验证支持。

您可以将现有 NetScaler Gateway 实例用于 Citrix Endpoint Management，也可以为其设置新实例。以下部分将介绍使用现有或新的专用 NetScaler Gateway 实例的优缺点。

共享的 NetScaler Gateway MPX，其中为 Citrix Endpoint Management 创建了一个 NetScaler Gateway VIP

优点：

- 为所有 Citrix 远程连接（Citrix Virtual Apps、完整 VPN 和无客户端 VPN）使用一个通用的 NetScaler Gateway 实例。
- 使用现有的 NetScaler Gateway 配置，例如用于证书身份验证以及访问 DNS、LDAP 和 NTP 等服务。
- 使用单个 NetScaler Gateway 平台许可证。

缺点：

- 在同一个 NetScaler Gateway 上处理两种不同的用例时，规划扩展性会更困难。
- 有时，Citrix Virtual Apps 用例需要特定的 NetScaler Gateway 版本。同一版本可能对 Citrix Endpoint Management 存在已知问题。或者 Citrix Endpoint Management 可能对 NetScaler Gateway 版本存在已知问题。
- 如果 NetScaler Gateway 已存在，则无法第二次运行 NetScaler for XenMobile 向导来创建 Citrix Endpoint Management 的 NetScaler Gateway 配置。
- 除非 NetScaler Gateway 11.1 或更高版本使用 Platinum 许可证：安装在 NetScaler Gateway 上且 VPN 连接所需的用户访问许可证是共用的。由于这些许可证可用于所有 NetScaler Gateway 虚拟服务器，因此 Citrix Endpoint Management 以外的服务可能会占用它们。

专用 NetScaler Gateway VPX/MPX 实例

优点：

Citrix 建议使用 NetScaler Gateway 的专用实例。

- 更容易规划扩展性，并将 Citrix Endpoint Management 流量与可能已受资源限制的 NetScaler Gateway 实例分离。
- 避免 Citrix Endpoint Management 和 Citrix Virtual Apps 需要不同 NetScaler Gateway 软件版本时出现问题。通常建议为 Citrix Endpoint Management 使用最新兼容的 NetScaler Gateway 版本和内部版本。
- 允许通过内置的 NetScaler for XenMobile 向导配置 Citrix Endpoint Management 的 NetScaler Gateway。
- 服务的虚拟和物理分离。

缺点：

- 需要在 NetScaler Gateway 上设置额外服务以支持 Citrix Endpoint Management 配置。
- 需要另一个 NetScaler Gateway 平台许可证。为每个 NetScaler Gateway 实例授予 NetScaler Gateway 许可证。

有关在 Citrix Endpoint Management 管理模式下集成 NetScaler Gateway 和 Citrix ADC 时要考虑的事项的信息，请参阅与 NetScaler Gateway 和 Citrix ADC 集成。

StoreFront

如果您有 Citrix Virtual Apps and Desktops 环境，可以使用 StoreFront 将 HDX 应用程序与 Citrix Endpoint Management 集成。将 HDX 应用程序与 Citrix Endpoint Management 集成后：

- 应用程序可供已注册 Citrix Endpoint Management 的用户使用。
- 应用程序与其他移动应用程序一起显示在应用商店中。
- Citrix Endpoint Management 通过 StoreFront 上的 Citrix Receiver 进行操作。
- 当 Citrix Workspace 应用程序安装在设备上时，HDX 应用程序将开始使用该应用程序。

StoreFront 存在每个 StoreFront 实例只能有一个服务站点的限制。假设您有许多应用商店，并且希望将其与其他生产用途分开。在这种情况下，Citrix 通常建议您考虑为 Citrix Endpoint Management 部署新的 StoreFront 实例和服务站点。

注意事项包括：

- StoreFront 是否有任何不同的身份验证要求？StoreFront 服务站点需要 Active Directory 凭据才能登录。仅使用基于证书的身份验证的客户无法使用相同的 NetScaler Gateway 通过 Citrix Endpoint Management 枚举应用程序。
- 使用相同的应用商店还是创建新的应用商店？
- 使用相同或不同的 StoreFront 服务器？

以下部分阐述了为 Citrix Workspace 和 Citrix 移动生产力应用程序使用独立或组合的 StoreFront 的优点和缺点。

将现有 StoreFront 实例与 Citrix Endpoint Management 集成

优点：

- 相同的应用商店：Citrix Endpoint Management 无需对 StoreFront 进行额外配置，前提是您使用相同的 NetScaler Gateway VIP 进行 HDX 访问。假设您选择使用相同的应用商店并希望将 Citrix Workspace 访问定向到新的 NetScaler Gateway VIP。在这种情况下，请将相应的 NetScaler Gateway 配置添加到 StoreFront。
- 相同的 StoreFront 服务器：使用现有的 StoreFront 安装和配置。

缺点：

- 相同的应用商店：对 StoreFront 进行任何重新配置以支持 Citrix Virtual Apps and Desktops 工作负载，都可能会对 Citrix Endpoint Management 产生不利影响。
- 相同的 StoreFront 服务器：在大型环境中，请考虑 Citrix Endpoint Management 使用 Citrix Receiver 进行应用程序枚举和启动所带来的额外负载。

使用新的专用 StoreFront 实例与 Citrix Endpoint Management 集成

优点：

- 新的应用商店：对 Citrix Endpoint Management 的 StoreFront 应用商店进行的任何配置更改都不会影响现有的 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 Endpoint Management 使用 Citrix Receiver 进行应用程序枚举和启动之外的负载不会影响可扩展性。

缺点：

- 新的应用商店：StoreFront 应用商店配置。
- 新的 StoreFront 服务器：需要新的 StoreFront 安装和配置。

有关详细信息，请参阅通过应用商店使用 Citrix Virtual Apps and Desktops。

共享文件和思杰文件

> **免责声明：**

> 如果 ShareFile（现为 Progress）停止支持，此功能将被弃用。

> ShareFile 使您能够轻松安全地交换文档、通过电子邮件发送大型文档以及安全地处理向第三方传输文档。Citrix Files 应用程序使用户能够从任何设备访问和同步其所有数据。借助 Citrix Files，用户可以安全地与组织内部和外部的人员共享数据。

Citrix Endpoint Management 为 Citrix Files 提供以下功能：

- 为移动生产力应用程序用户提供单点登录身份验证。
- 基于 Active Directory 的用户帐户预配。
- 全面的访问控制策略。

移动用户可以受益于完整的企业帐户功能集。

或者，您可以将 Citrix Endpoint Management 配置为仅与存储区域连接器集成。通过存储区域连接器，Citrix Files 提供对以下内容的访问：

- 文档和文件夹
- 网络文件共享
- 在 SharePoint 站点中：站点集和文档库。

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。您可以使用 Citrix Endpoint Management 控制台配置与企业帐户或存储区域连接器的集成。有关详细信息，请参阅 适用于 Citrix Endpoint Management 的 Citrix Files。

以下部分列出了在为 Citrix Files 制定设计决策时需要考虑的问题。

与 Citrix Files 集成或仅与存储区域连接器集成

要提出的问题：

- 您是否希望将数据存储在 Citrix 管理的存储区域中？
- 您是否希望为用户提供文件共享和同步功能？
- 您是否希望用户能够访问 Citrix Files 网站上的文件？或者从移动设备访问 Office 365 内容和个人云连接器？

设计决策：

- 如果这些问题中的任何一个答案是“是”，请与企业帐户集成。
- 仅与存储区域连接器集成可为 iOS 用户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。在此配置中，您无需设置 Citrix Files 子域、无需为用户预配 Citrix Files，也无需托管 Citrix Files 数据。将存储区域连接器与 Citrix Endpoint Management 结合使用遵循了防止用户信息泄露到公司网络之外的安全限制。

存储区域控制器服务器位置

要提出的问题：

- 您是否需要本地存储或存储区域连接器等功能？
- 如果使用 Citrix Files 的本地功能，存储区域控制器将位于网络的何处？

设计决策：

- 确定是将存储区域控制器服务器放置在 Citrix Files 云中、您的本地单租户存储系统中，还是支持的第三方云存储中。
- 存储区域控制器需要一定的互联网访问权限才能与 Citrix Files 控制平面通信。您可以通过多种方式连接，包括直接访问或 NAT/PAT 配置。

存储区域连接器

要提出的问题：

- CIFS 共享路径是什么？
- SharePoint URL 有哪些？

设计决策：

- 确定是否需要本地存储区域控制器来访问这些位置。
- 由于存储区域连接器与文件存储库、CIFS 共享和 SharePoint 等内部资源进行通信，Citrix 建议将存储区域控制器部署在 DMZ 防火墙后面的内部网络中，并由 NetScaler Gateway 提供前端访问。

SAML 与 Citrix Endpoint Management 的集成方案

要提出的问题：

- Citrix Files 是否需要 Active Directory 身份验证？
- Citrix Endpoint Management 的 Citrix Files 应用程序首次使用是否需要 SSO？
- 您当前的环境中是否有标准 IdP？

- 使用 SAML 需要多少个域？
- Active Directory 用户是否有许多电子邮件别名？
- 是否有任何 Active Directory 域迁移正在进行中或即将进行？

设计决策：

您可以选择使用 SAML 作为 Citrix Files 的身份验证机制。身份验证选项包括：

- 使用 Citrix Endpoint Management 服务器作为 SAML 的身份提供程序 (IdP)

  此选项可以提供出色的用户体验，自动创建 Citrix Files 帐户，并启用移动应用 SSO 功能。

  Citrix Endpoint Management 服务器已针对此过程进行了增强：它不需要同步 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

  如果您有现有且受支持的 IdP 并且不需要移动应用 SSO 功能，此选项可能最适合您。此选项还需要使用 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）也可能在 Windows 客户端提供 SSO 功能。在选择 Citrix Files SAML IdP 之前，请务必评估用例。
- 或者，要满足这两种用例，请参阅 适用于双身份提供程序的 ShareFile 单点登录配置指南。

移动应用

要提出的问题：

- 您计划使用哪个 Citrix Files 移动应用（公共、MDM、MDX）？

设计决策：

- 您可以从 Apple App Store 和 Google Play Store 分发 Citrix 移动生产力应用。通过这种公共应用商店分发，您可以从 Citrix 下载页面获取封装的应用。
- 如果您的安全要求较低并且不需要容器化，公共 Citrix Files 应用可能不适用。
- 有关详细信息，请参阅 应用 和 适用于 Citrix Endpoint Management 的 Citrix Files。

安全、策略和访问控制

要提出的问题：

- 您对桌面、Web 和移动用户有哪些限制要求？
- 您希望为用户设置哪些标准访问控制设置？

- 您计划使用哪种文件保留策略？

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，Citrix Endpoint Management 策略优先，其次是 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 Citrix Endpoint Management 中启用它们，则外部应用程序将在 Citrix Files 中被禁用。您可以将应用程序配置为 Citrix Endpoint Management 不需要 PIN/密码，但 Citrix Files 应用程序需要 PIN/密码。

标准存储区域与受限存储区域

要提出的问题：

- 您是否需要受限存储区域？

设计决策：

- 标准存储区域用于非敏感数据，并允许员工与非员工共享数据。此选项支持涉及在您的域之外共享数据的工作流。
- 受限存储区域保护敏感数据：只有经过身份验证的域用户才能访问该区域中存储的数据。

访问控制

企业可以在网络内部和外部管理移动设备。Citrix Endpoint Management 等企业移动管理解决方案在为移动设备提供安全性和控制方面表现出色，且不受位置限制。但是，当您将它们与网络访问控制 (NAC) 解决方案结合使用时，您可以为网络内部的设备添加 QoS 和更精细的控制。这种组合使您能够通过 NAC 解决方案扩展 Citrix Endpoint Management 设备安全评估。您的 NAC 解决方案随后可以使用 Citrix Endpoint Management 安全评估来促进和处理身份验证决策。

您可以使用以下任何解决方案来实施 NAC 策略：

- NetScaler 网关
- ForeScout

Citrix 不保证与其他 NAC 解决方案的集成。

NAC 解决方案与 Citrix Endpoint Management 集成的优势包括：

- 为企业网络上的所有端点提供更好的安全性、合规性和控制。
- NAC 解决方案可以：

  - 在设备尝试连接到您的网络时立即检测到它们。
  - 查询 Citrix Endpoint Management 以获取设备属性。
  - 使用该设备信息来确定是允许、阻止、限制还是重定向这些设备。这些决定取决于您选择实施的安全策略。

- NAC 解决方案为 IT 管理员提供了非托管和不合规设备的视图。

有关 Citrix 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 NetScaler Gateway 和 Citrix ADC 集成

与 Citrix Endpoint Management 集成后，NetScaler Gateway 为 MAM 设备提供远程设备访问内部网络的身份验证机制。此集成使 Citrix 移动生产力应用程序能够通过微型 VPN 连接到内网中的公司服务器。Citrix Endpoint Management 会在设备上的应用程序与 NetScaler Gateway 之间创建微型 VPN。NetScaler Gateway 提供微型 VPN 路径以访问所有公司资源，并提供强大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 NetScaler Gateway FQDN 进行注册。

Citrix Cloud Operations 管理 Citrix ADC 负载平衡。

设计决策

以下部分总结了在规划 NetScaler Gateway 与 Citrix Endpoint Management 集成时需要考虑的许多设计决策。

证书

决策详情：

- 您是否需要为注册和访问 Citrix Endpoint Management 环境提供更高级别的安全性？
- LDAP 是否不可用？

设计指导：

Citrix Endpoint Management 的默认配置是用户名和密码身份验证。为了增加注册和访问 Citrix Endpoint Management 环境的安全性，请考虑使用基于证书的身份验证。您可以将证书与 LDAP 结合使用进行双因素身份验证，从而在无需 RSA 服务器的情况下提供更高级别的安全性。

如果您不允许 LDAP 并使用智能卡或类似方法，配置证书可让您向 Citrix Endpoint Management 表示智能卡。用户随后使用 Citrix Endpoint Management 为他们生成的唯一 PIN 进行注册。用户获得

访问权限后，Citrix Endpoint Management 会创建并部署稍后用于向 Citrix Endpoint Management 环境进行身份验证的证书。

Citrix Endpoint Management 仅支持第三方证书颁发机构的证书吊销列表 (CRL)。如果您配置了 Microsoft CA，Citrix Endpoint Management 会使用 NetScaler Gateway 来管理吊销。当您配置基于客户端证书的身份验证时，请考虑是否需要配置 NetScaler Gateway 证书吊销列表 (CRL) 设置 **启用 CRL 自动刷新**。此步骤可确保仅在 MAM 中注册的设备用户无法使用设备上的现有证书进行身份验证。Citrix Endpoint Management 会重新颁发新证书，因为它不限制用户在证书被吊销时生成用户证书。当 CRL 检查过期的 PKI 实体时，此设置会提高 PKI 实体的安全性。

专用或共享 NetScaler Gateway VIP

决策详情：

- 您目前是否将 NetScaler Gateway 用于 Citrix Virtual Apps and Desktops？
- Citrix 端点管理是否会使用与 Citrix 虚拟应用和桌面相同的 NetScaler 网关？
- 两种流量流的身份验证要求是什么？

设计指导：

当您的 Citrix 环境包含 Citrix Endpoint Management 以及 Virtual Apps and Desktops 时，您可以为两者使用相同的 NetScaler Gateway 虚拟服务器。由于可能存在版本冲突和环境隔离，建议为每个 Citrix Endpoint Management 环境使用专用的 NetScaler Gateway。

如果您使用 LDAP 身份验证，Citrix Secure Hub 可以毫无问题地向同一 NetScaler Gateway 进行身份验证。如果您使用基于证书的身份验证，Citrix Endpoint Management 会在 MDX 容器中推送一个证书，Citrix Secure Hub 使用该证书向 NetScaler Gateway 进行身份验证。

您可以考虑此变通方法，它允许您为两个 NetScaler Gateway VIP 使用相同的 FQDN。您可以创建两个具有相同 IP 地址的 NetScaler Gateway VIP。用于 Citrix Secure Hub 的 VIP 使用标准 443 端口，而用于 Citrix Virtual Apps and Desktops（部署 Citrix Workspace 应用程序）的 VIP 使用 444 端口。然后，一个 FQDN 解析到相同的 IP 地址。对于此变通方法，您可能需要将 StoreFront 配置为返回端口 444 的 ICA 文件，而不是默认的端口 443。此变通方法不需要用户输入端口号。

NetScaler Gateway 超时

决策详情：

- 您希望如何为 Citrix Endpoint Management 流量配置 NetScaler Gateway 超时？

设计指导：

NetScaler Gateway 包含“会话超时”和“强制超时”设置。有关详细信息，请参阅 推荐配置。请记住，后台服务、NetScaler Gateway 以及离线访问应用程序的超时值是不同的。

注册 FQDN

> **重要：**
>
> 更改注册 FQDN 需要一个新的 SQL Server 数据库和重建 Citrix Endpoint Management 服务器。

思杰安全网络流量

决策详情：

- 您会将 Citrix Secure Web 限制为仅用于内部网页浏览吗？
- 您会为内部和外部网页浏览启用 Citrix Secure Web 吗？

设计指南：

如果您计划仅将 Citrix Secure Web 用于内部网页浏览，则 NetScaler Gateway 配置非常简单。但是，如果 Citrix Secure Web 默认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 Citrix Secure Web 用于内部和外部浏览，则必须启用 SNIP 以便进行出站 Internet 访问。IT 通常将已注册设备（使用 MDX 容器）视为公司网络的延伸。因此，IT 通常希望 Citrix Secure Web 连接返回到 NetScaler Gateway，通过代理服务器，然后访问 Internet。默认情况下，Citrix Secure Web 访问会隧道连接到内部网络。Citrix Secure Web 使用每个应用程序的 VPN 隧道返回到内部网络以进行所有网络访问，并且 NetScaler Gateway 使用拆分隧道设置。

有关 Citrix Secure Web 连接的讨论，请参阅配置用户连接。

Citrix Secure Mail 的推送通知

决策详情：

- 您会使用推送通知吗？

iOS 的设计指南：

如果您的 NetScaler Gateway 配置包含安全票证颁发机构 (STA) 并且拆分隧道已关闭：NetScaler Gateway 必须允许来自 Citrix Secure Mail 的流量访问 Citrix 侦听器服务 URL。这些 URL 在适用于 iOS 的 Citrix Secure Mail 推送通知中指定。

Android 的设计指南：

使用 Firebase Cloud Messaging (FCM) 控制 Android 设备何时以及如何连接到 Citrix Endpoint Management。配置 FCM 后，任何安全操作或部署命令都会触发向 Citrix Secure Hub 发送推送通知，以提示用户重新连接到 Citrix Endpoint Management 服务器。

HDX™ STA

决策详情：

- 如果集成 HDX 应用程序访问，应使用哪些 STA？

设计指导：

HDX STA 必须与 StoreFront 中的 STA 匹配，并且必须对 Virtual Apps and Desktops 站点有效。

Citrix 文件和 ShareFile

决策详情：

- 您是否会在环境中部署存储区域控制器？
- 您将使用哪个 Citrix Files VIP URL？

设计指导：

如果您的环境中包含存储区域控制器，请确保正确配置以下各项：

- Citrix Files 内容交换 VIP（由 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 Storage zones controller 的文档。

SAML IdP

决策详情：

- 如果 Citrix Files 需要 SAML，您是否希望使用 Citrix Endpoint Management 作为 SAML IdP？

设计指导：

推荐的最佳实践是将 Citrix Files 与 Citrix Endpoint Management 集成，这是一种比配置基于 SAML 的联合更简单的替代方案。Citrix 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。

Citrix Endpoint Management 控制台使您能够执行 Citrix Files 配置，并监控服务级别和许可证使用情况。

Citrix Files 客户端有两种类型：适用于 Citrix Endpoint Management 的 Citrix Files（也称为封装的 Citrix Files）和 Citrix Files 移动客户端（也称为未封装的 Citrix Files）。要了解这些差异，请参阅 How Citrix Files for Citrix Endpoint Management Clients differ from Citrix Files mobile clients。

您可以将 Citrix Endpoint Management 和 Citrix Files 配置为使用 SAML 来提供对以下各项的 SSO 访问：

- 已启用 MAM SDK 或使用 MDX Toolkit 封装的 Citrix Files 应用程序
- 未封装的 Citrix Files 客户端，例如网站、Outlook 插件或同步客户端

如果您希望使用 Citrix Endpoint Management 作为 Citrix Files 的 SAML IdP，请确保已进行适当的配置。有关详细信息，请参阅 SAML for SSO with Citrix Files。

ShareConnect 直接连接

决策详情：

- 用户是否将使用直接连接，从运行 ShareConnect 的计算机或移动设备访问主机计算机？

设计指导：

ShareConnect 允许用户通过 iPad、Android 平板电脑和 Android 手机安全地连接到其计算机，以访问其文件和应用程序。对于直接连接，Citrix Endpoint Management 使用 NetScaler Gateway 提供对本地网络外部资源的访问。有关配置详细信息，请参阅 ShareConnect。

每种管理模式的注册 FQDN

管理模式	注册 FQDN
MDM+MAM（强制 MDM 注册）	Citrix 端点管理服务器 FQDN
MDM+MAM（可选 MDM 注册）	Citrix 端点管理服务器 FQDN
仅限 MAM	思杰端点管理 服务器 FQDN

部署摘要

如果您有多个 Citrix 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 NetScaler Gateway。当您拥有一个正常运行的环境时，请记下设置，然后再尝试为 Citrix Endpoint Management 手动配置 NetScaler Gateway。

一个关键决定是，与 Citrix Endpoint Management 服务器通信时是使用 HTTPS 还是 HTTP。HTTPS 提供安全的后端通信，因为 NetScaler Gateway 和 Citrix Endpoint Management 之间的流量已加密。重新加密会影响 Citrix Endpoint Management 服务器性能。HTTP 提供更好的 Citrix Endpoint Management 服务器性能。NetScaler Gateway 和 Citrix Endpoint Management 之间的流量未加密。下表显示了 NetScaler Gateway 和 Citrix Endpoint Management 的 HTTP 和 HTTPS 端口要求。

HTTPS

Citrix 通常建议将 SSL Bridge 用于 NetScaler Gateway MDM 虚拟服务器配置。对于将 NetScaler Gateway SSL Offload 与 MDM 虚拟服务器结合使用，Citrix Endpoint Management 仅支持端口 80 作为后端服务。

管理模式	NETSCALER GATEWAY 负载平衡方法	SSL 重新加密	CITRIX 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	NETSCALER GATEWAY 负载平衡方法	SSL 重新加密	CITRIX 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 Citrix Endpoint Management 部署中 NetScaler Gateway 的图示，请参阅体系结构。

MDX 应用的 SSO 和代理注意事项

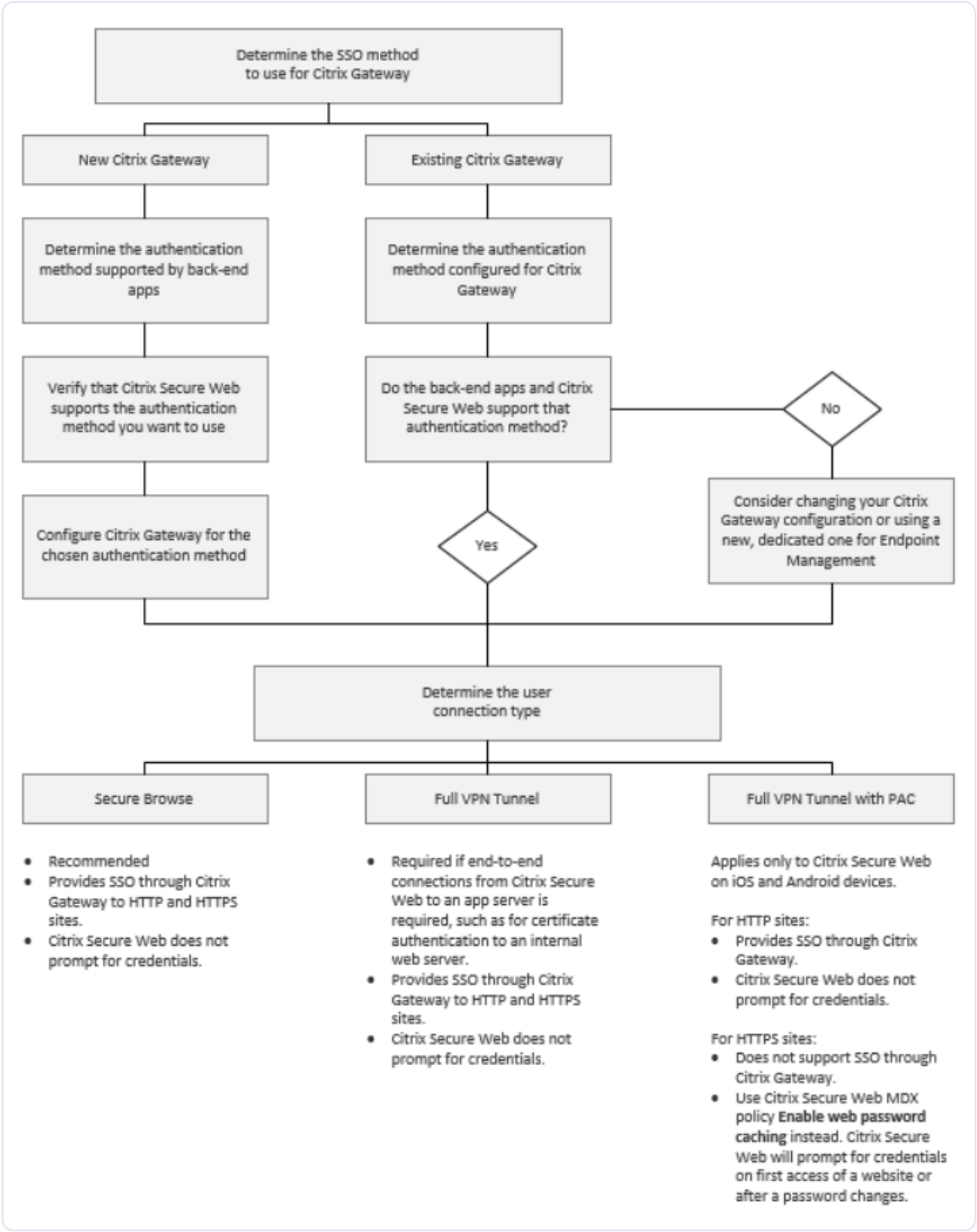
Citrix Endpoint Management 与 NetScaler Gateway 集成，使您能够为用户提供对所有后端 HTTP/HTTPS 资源的单点登录 (SSO)。根据您的 SSO 身份验证要求，将 MDX 应用的用户连接配置为使用安全浏览（隧道式 - Web SSO），这是一种无客户端 VPN。

> **重要提示：**

> Citrix 已弃用对 iOS 和 Android 设备上完整 VPN 隧道以及带有完整 VPN 隧道部署的代理自动配置 (PAC) 文件的支持。有关详细信息，请参阅弃用。

> 如果 NetScaler Gateway 不是在您的环境中提供 SSO 的最佳方式，您可以设置一个 MDX 应用，并使用基于策略的本地密码缓存。本文探讨了各种 SSO 和代理选项，重点关注 Citrix Secure Web。这些概念也适用于其他 MDX 应用。

以下流程图总结了 SSO 和用户连接的决策流程。



NetScaler Gateway 身份验证方法

本节提供有关 NetScaler Gateway 支持的身份验证方法的常规信息。

SAML 身份验证

当您为安全断言标记语言 (SAML) 配置 NetScaler Gateway 时，用户可以连接到支持 SAML 协议的 Web 应用以进行单点登录。NetScaler Gateway 支持 SAML Web 应用的身份提供程序 (IdP) 单点登录。

所需配置：

- 在 NetScaler 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

如果会话配置文件中启用了对 Web 应用程序的 SSO，NetScaler Gateway 会自动执行 NTLM 身份验证。

所需配置：

- 在 NetScaler Gateway 会话或流量配置文件中启用 SSO。

Kerberos 模拟

Citrix Endpoint Management 仅支持 Citrix Secure Web 的 Kerberos。当您为 Kerberos SSO 配置 NetScaler Gateway 时，如果 NetScaler Gateway 可以获取用户密码，则 NetScaler Gateway 会使用模拟。模拟意味着 NetScaler Gateway 使用用户凭据来获取访问服务（例如 Citrix Secure Web）所需的票证。

所需配置：

- 配置 NetScaler Gateway `Worx` 会话策略，以允许其从您的连接中识别 Kerberos 领域。
- 在 NetScaler 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 Citrix Endpoint Management 网关上的流量策略。
- 有关这些和其他配置详细信息，请参阅 Citrix 博客：WorxWeb 和 Kerberos 模拟 SSO。

Kerberos 约束委派

Citrix Endpoint Management 仅支持 Citrix Secure Web 的 Kerberos。当您为 Kerberos SSO 配置 NetScaler Gateway 时，如果 NetScaler Gateway 无法获取用户密码，则 NetScaler Gateway 会使用约束委派。

通过约束委派，NetScaler Gateway 使用指定的管理员帐户为用户和服务获取票证。

所需配置：

- 在 Active Directory 中配置具有所需权限的 KCD 帐户，并在 NetScaler Gateway 上配置 KDC 帐户。
- 在 NetScaler Gateway 流量配置文件中启用 SSO。
- 配置后端网站以进行 Kerberos 身份验证。

表单填充身份验证

当您将 NetScaler Gateway 配置为基于表单的单点登录时，用户可以一次登录以访问网络中的所有受保护应用程序。此身份验证方法适用于使用“隧道 - Web SSO”模式的应用程序。

所需配置：

- 在 NetScaler Gateway 流量配置文件中配置基于表单的 SSO。

摘要式 HTTP 身份验证

如果您在会话配置文件中为 Web 应用程序启用 SSO，NetScaler Gateway 会自动执行摘要式 HTTP 身份验证。此身份验证方法适用于使用“隧道 - Web SSO”模式的应用程序。

所需配置：

- 在 NetScaler Gateway 会话或流量配置文件中启用 SSO。

基本 HTTP 身份验证

如果您在会话配置文件中为 Web 应用程序启用 SSO，NetScaler Gateway 会自动执行基本 HTTP 身份验证。此身份验证方法适用于使用“隧道 - Web SSO”模式的应用程序。

所需配置：

- 在 NetScaler Gateway 会话或流量配置文件中启用 SSO。

安全隧道 - Web SSO

本节介绍 Citrix Secure Web 的 **隧道 - Web SSO** 用户连接类型。

隧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“隧道 - Web SSO”。隧道 - Web SSO 是 Citrix Secure Web **首选 VPN 模式**策略的默认配置。Citrix 建议对需要单点登录 (SSO) 的连接使用隧道 - Web SSO。

在隧道 - Web SSO 模式下，NetScaler Gateway 将 HTTPS 会话分为两部分：

- 从客户端到 NetScaler Gateway
- 从 NetScaler Gateway 到后端资源服务器。

通过这种方式，NetScaler Gateway 可以完全查看客户端和服务器之间的所有事务，从而能够提供 SSO。

在隧道 - Web SSO 模式下使用 Citrix Secure Web 时，您还可以为其配置代理服务器。有关详细信息，请参阅博客 Citrix Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode。

> **注意：**

> Citrix 宣布弃用带 PAC 的完整 VPN 隧道。请参阅 弃用。

> Citrix Endpoint Management 支持 NetScaler Gateway 提供的代理身份验证。PAC 文件包含定义 Web 浏览器如何选择代理以访问给定 URL 的规则。PAC 文件规则可以指定内部和外部站点的处理方式。Citrix Secure Web 解析 PAC 文件规则并将代理服务器信息发送到 NetScaler Gateway。NetScaler Gateway 不知道 PAC 文件或代理服务器。

对于 HTTPS 网站的身份验证：Citrix Secure Web MDX 策略**启用 Web 密码缓存**使 Citrix Secure Web 能够通过 MDX 对代理服务器进行身份验证并提供 SSO。

NetScaler Gateway 分流

在规划 SSO 和代理配置时，您还必须决定是否使用 NetScaler Gateway 分流。Citrix 建议仅在需要时才使用 NetScaler Gateway 分流。本节概述了分流的工作原理：NetScaler Gateway 根据其路由表确定流量路径。当 NetScaler Gateway 分流开启时，Citrix Secure Hub 会区分内部（受保护）网络流量和 Internet 流量。Citrix Secure Hub 根据 DNS 后缀和 Intranet 应用程序进行此确定。然后，Citrix Secure Hub 仅通过 VPN 隧道传输内部网络流量。当 NetScaler Gateway 分流关闭时，所有流量都通过 VPN 隧道。

如果您出于安全考虑希望监控所有流量，请禁用 NetScaler Gateway 分流。这样，所有流量都将通过 VPN 隧道。

NetScaler Gateway 还具有微型 VPN 反向分流模式。此配置支持 IP 地址排除列表，这些 IP 地址不会通过隧道传输到 NetScaler Gateway。相反，这些地址是使用设备 Internet 连接发送的。有关反向分流的更多信息，请参阅 NetScaler Gateway 文档。

Citrix Endpoint Management 包含一个**反向分流排除列表**。要防止某些网站通过 NetScaler Gateway 隧道传输：添加一个逗号分隔的完全限定域名 (FQDN) 或 DNS 后缀列表，这些域名或后缀改为使用 LAN 连接。此列表仅适用于配置为反向分流的 NetScaler Gateway 的隧道 - Web SSO 模式。

身份验证

在 Citrix Endpoint Management 部署中，决定如何配置身份验证时需要考虑多个因素。本节介绍影响身份验证的各种因素：

- 与身份验证相关的主要 MDX 策略、Citrix Endpoint Management 客户端属性和 NetScaler 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。

本文还包括三个推荐配置示例，以提高安全性。

广义上讲，更强的安全性会导致用户体验不佳，因为用户必须更频繁地进行身份验证。如何平衡这些问题取决于您的组织需求和优先级。查看这三个推荐配置，以了解各种身份验证选项之间的相互作用。

身份验证模式

在线身份验证： 允许用户访问 Citrix Endpoint Management 网络。需要 Internet 连接。

离线身份验证： 在设备上进行。用户解锁安全保管库并可以离线访问项目，例如下载的邮件、缓存的网站和笔记。

身份验证方法

单因素

LDAP： 您可以在 Citrix Endpoint Management 中配置与一个或多个符合轻型目录访问协议 (LDAP) 的目录的连接。此方法通常用于为公司环境提供单点登录 (SSO)。您可以选择使用 Citrix PIN 和 Active Directory 密码缓存来改善 LDAP 的用户体验。同时，您可以在注册、密码过期和帐户锁定方面提供复杂密码的安全性。

有关更多详细信息，请参阅 (/zh-cn/citrix-endpoint-management/authentication/authentication-domain-security-token.html)。

客户端证书： Citrix Endpoint Management 可以与行业标准证书颁发机构集成，以使用证书作为唯一的在线身份验证方法。Citrix 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。当使用客户端证书作为主要的身份验证方法时，在仅限客户端证书的环境中需要 Citrix PIN 来保护设备上的证书。

Citrix Endpoint Management 仅支持第三方证书颁发机构的证书吊销列表 (CRL)。如果配置了 Microsoft CA，Citrix Endpoint Management 将使用 NetScaler 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 NetScaler Gateway 证书吊销列表 (CRL) 设置“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。Citrix Endpoint Management 会重新颁发新证书，因为它不限制用户在证书被吊销时生成用户证书。当 CRL 检查过期的 PKI 实体时，此设置可提高 PKI 实体的安全性。

有关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图，请参阅体系结构。

双因素身份验证

LDAP + 客户端证书： 此配置是 Citrix Endpoint Management 安全性和用户体验的最佳组合。同时使用 LDAP 和客户端证书身份验证具有以下优点：

- 具有最佳的 SSO 可能性，并结合了 NetScaler Gateway 提供的双因素身份验证安全性。
- 通过用户知道的信息（其 Active Directory 密码）和用户拥有的信息（其设备上的客户端证书）提供安全性。

Citrix Secure Mail 可以自动配置并提供无缝的首次使用客户端证书身份验证的用户体验。该功能需要正确配置的 Exchange 客户端访问服务器环境。

为了获得最佳可用性，您可以将 LDAP 和客户端证书身份验证与 Citrix PIN 和 Active Directory 密码缓存结合使用。

LDAP + 令牌： 此配置允许使用 RADIUS 协议进行 LDAP 凭据的经典配置以及一次性密码。为了获得最佳可用性，您可以将此选项与 Citrix PIN 和 Active Directory 密码缓存结合使用。

重要的身份验证策略、设置和客户端属性

以下策略、设置和客户端属性适用于以下三种推荐配置：

MDX 策略

应用程序密码： 如果设置为 **On**，则在应用程序启动或在一段时间不活动后恢复时，需要 Citrix PIN 或密码才能解锁应用程序。默认值为 **On**。

要为所有应用程序配置不活动计时器，请在 Citrix Endpoint Management 控制台的**设置**选项卡上的**客户端属性**中，将 INACTIVITY_TIMER 值设置为分钟。默认值为 15 分钟。要禁用不活动计时器，以便仅在应用程序启动时显示 PIN 或密码提示，请将该值设置为零。

需要微型 VPN 会话： 如果设置为 **On**，则用户必须连接到企业网络并具有活动会话才能访问设备上的应用程序。如果设置为 **Off**，则无需活动会话即可访问设备上的应用程序。默认值为 **Off**。

最长离线时间（小时）： 定义了应用程序在不重新确认应用程序授权和不从 Citrix Endpoint Management 刷新策略的情况下可以运行的最长时间。iOS 应用程序在满足以下条件后，可以从 Citrix Endpoint Management 检索 MDX 应用程序的新策略，而不会对用户造成任何中断：

- 您设置了最长离线时间，并且
- 适用于 iOS 的 Citrix Secure Hub 具有有效的 NetScaler Gateway 令牌。

如果 Citrix Secure Hub 没有有效的 NetScaler Gateway 令牌，则用户必须通过 Citrix Secure Hub 进行身份验证，然后才能更新应用程序策略。NetScaler Gateway 令牌可能因 NetScaler Gateway 会话不活动或强制会话超时策略而失效。当用户再次登录 Citrix Secure Hub 时，他们可以继续运行该应用程序。

在期限到期前 30、15 和 5 分钟，系统会提醒用户登录。到期后，应用程序将被锁定，直到用户登录。默认值为 **72 小时（3 天）**。最短期限为 1 小时。

> **注意：**

> 请记住，在用户经常出差并使用国际漫游的情况下，默认的 72 小时（3 天）可能太短。

> **后台服务票证过期：** 后台网络服务票证保持有效的时间段。当 Citrix Secure Mail 通过 NetScaler Gateway 连接到运行 ActiveSync 的 Exchange Server 时，Citrix Endpoint Management 会颁发一个令牌。Citrix Secure Mail 使用该令牌连接到内部 Exchange Server。此属性设置确定 Citrix Secure Mail 可以使用令牌而无需新的令牌进行身份验证和连接到 Exchange Server 的持续时间。当时间限制到期时，用户必须再次登录以生成新令牌。默认值为 **168 小时（7 天）**。当此超时到期时，邮件通知将停止。

微 VPN 会话所需宽限期： 确定用户可以在离线状态下使用应用程序多少分钟，直到在线会话得到验证。默认值为 **0**（无宽限期）。

有关身份验证策略的信息，请参阅：

- 如果您使用 MAM SDK：MAM SDK 概述
- 如果您使用 MDX Toolkit：适用于 iOS 的 Citrix Endpoint Management MDX 策略 和 适用于 Android 的 Citrix Endpoint Management MDX 策略

Citrix Endpoint Management 客户端属性

> **注意：**

> 客户端属性是适用于连接到 Citrix Endpoint Management 的所有设备的全局设置。

> **Citrix PIN：** 为了获得简单的登录体验，您可以选择启用 Citrix PIN。使用 PIN，用户无需重复输入其他凭据，例如其 Active Directory 用户名和密码。您可以将 Citrix PIN 配置为独立的离线身份验证，也可以将 PIN 与 Active Directory 密码缓存结合使用，以简化身份验证，从而实现最佳可用性。您可以在 Citrix Endpoint Management 控制台的**设置 > 客户端 > 客户端属性**中配置 Citrix PIN。

以下是几个重要属性的摘要。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

此密钥允许您启用 Citrix PIN 功能。使用 Citrix PIN 或密码，系统会提示用户定义一个 PIN 以代替其 Active Directory 密码。如果启用了 **ENABLE_PASSWORD_CACHING** 或 Citrix Endpoint Management 正在使用证书身份验证，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

此密钥允许您将用户的 Active Directory 密码缓存在移动设备本地。当您将此密钥设置为 true 时，系统会提示用户设置 Citrix PIN 或密码。当您将此密钥设置为 **true** 时，**ENABLE_PASSCODE_AUTH** 密钥必须设置为 true。

可能的值： **true** 或 **false**

默认值： **false**

PASSCODE_STRENGTH

显示名称： PIN 强度要求

此密钥定义 Citrix PIN 或密码的强度。当您更改此设置时，下次系统提示用户进行身份验证时，会要求他们设置新的 Citrix PIN 或密码。

可能值： **低、中或强**

默认值： **中**

INACTIVITY_TIMER

显示名称： 不活动计时器

此密钥定义了用户可以将其设备置于非活动状态，然后访问应用程序而无需提示输入 Citrix PIN 或密码的时间（以分钟为单位）。要为 MDX 应用程序启用此设置，必须将**应用程序密码**设置设为**开**。如果**应用程序密码**设置设为**关**，则用户将被重定向到 Citrix Secure Hub 以进行完全身份验证。更改此设置后，该值将在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： 启用触控 ID 身份验证

允许使用指纹识别器（仅限 iOS）进行离线身份验证。在线身份验证仍需要主要的身份验证方法。

ENCRYPT_SECRETS_USING_PASSCODE

显示名称： 使用密码加密机密

此密钥允许将敏感数据存储在移动设备上的秘密保管库中，而不是存储在基于平台的本机存储（例如 iOS 钥匙串）中。此配置密钥可实现对关键工件的强加密，但也会增加用户熵（只有用户知道的用户生成的随机 PIN 码）。

可能值： **true** 或 **false**

默认值： **false**

NetScaler Gateway 设置

会话超时： 如果启用此设置，NetScaler Gateway 将在指定的时间间隔内未检测到网络活动时断开会话。此设置对通过 NetScaler Gateway 插件、Citrix Secure Hub 或 Web 浏览器连接的用户强制执行。默认值为 **1440 分钟**。如果将此值设置为零，则此设置将被禁用。

强制超时： 如果启用此设置，无论用户正在执行什么操作，NetScaler Gateway 都会在超时时间间隔结束后断开会话。当超时时间间隔结束后，用户无法采取任何操作来阻止断开连接。此设置对使用 NetScaler Gateway Plug-in、Citrix Secure Hub 或通过 Web 浏览器连接的用户强制执行。如果 Citrix Secure Mail 正在使用 STA（一种特殊的 NetScaler Gateway 模式），则此设置不适用于 Citrix Secure Mail 会话。默认值为无，这意味着会话会因任何活动而延长。

有关 NetScaler Gateway 超时设置的详细信息，请参阅 NetScaler Gateway 文档。

有关提示用户通过在其设备上输入凭据向 Citrix Endpoint Management 进行身份验证的方案的详细信息，请参阅身份验证提示方案。

默认配置设置

这些设置是以下各项提供的默认值：

- NetScaler® for XenMobile 向导
- MAM 软件开发工具包 或 MDX 工具包
- 思杰端点管理控制台

设置	设置位置	默认设置
会话超时	NetScaler 网关	1440 分钟
强制超时	NetScaler 网关	无值 (关闭)
最长离线时间	MDX 策略	72 小时
后台服务票证过期	MDX 策略	168 小时 (7 天)
需要微型 VPN 会话	MDX 策略	关闭
需要微型 VPN 会话的宽限期	MDX 策略	0
应用密码	MDX 策略	开
使用密码加密机密	Citrix Endpoint Management 客户端属性	否
启用 Citrix PIN 身份验证	Citrix Endpoint Management 客户端属性	否
PIN 强度要求	Citrix Endpoint Management 客户端属性	中
PIN 类型	Citrix Endpoint Management 客户端属性	数字
启用用户密码缓存	Citrix Endpoint Management 客户端属性	否
不活动计时器	Citrix Endpoint Management 客户端属性	15
启用触控 ID 身份验证	Citrix Endpoint Management 客户端属性	否

推荐配置

本节提供了三个 Citrix Endpoint Management 配置示例，这些配置的范围从最低安全性、最佳用户体验到最高安全性、更具侵入性的用户体验。这些示例为您提供了有用的参考点，以确定您希望将自己的配置置于哪个级别。修改这些设置可能需要您更改其他设置。例如，最长离线时间不得超过会话超时。

最高安全性

此配置提供了最高级别的安全性，但会牺牲大量可用性。

设置	设置位置	推荐设置	行为影响
会话超时	NetScaler 网关	1440	用户仅在需要在线身份验证时（每 24 小时）输入其 Citrix Secure Hub 凭据。
强制超时	NetScaler 网关	无值	如果存在任何活动，会话将延长。
最长离线时间	MDX 策略	23	需要每天刷新策略。
后台服务票证过期	MDX 策略	72 小时	STA 超时，允许在没有 NetScaler Gateway 会话令牌的情况下进行长时间会话。对于 Citrix Secure Mail，将 STA 超时设置得比会话超时长，可以避免邮件通知停止。在这种情况下，如果用户在会话过期前未打开应用程序，Citrix Secure Mail 不会提示用户。
需要微型 VPN 会话	MDX 策略	关	提供有效的网络连接和 NetScaler Gateway 会话以使用应用程序。

需要微型 VPN 会话宽限期	MDX 策略	0	无宽限期（如果您启用了需要微型 VPN 会话）。
应用程序密码	MDX 策略	开	要求应用程序提供密码。
使用密码加密机密	Citrix Endpoint Management 客户端属性	是	从用户熵派生的密钥保护保管库。
启用 Citrix PIN 身份验证	Citrix Endpoint Management 客户端属性	是	启用 Citrix PIN 以简化身份验证体验。
PIN 强度要求	Citrix Endpoint Management 客户端属性	强	高密码复杂性要求。
PIN 类型	Citrix 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	Citrix Endpoint Management 客户端属性	否	Active Directory 密码不缓存，Citrix PIN 用于脱机身份验证。
不活动计时器	Citrix Endpoint Management 客户端属性	15	如果用户在此期间未使用 MDX 应用程序或 Citrix Secure Hub，则提示进行脱机身份验证。
启用触控 ID 身份验证	Citrix Endpoint Management 客户端属性	否	在 iOS 中禁用触控 ID 以用于脱机身份验证用例。

更高的安全性

这是一种更折中的方法，此配置要求用户更频繁地进行身份验证（最多每 3 天一次，而不是 7 天一次），并提供更强的安全性。身份验证次数的增加会更频繁地锁定容器，从而在设备不使用时提供数据安全性。

设置	设置位置	推荐设置	行为影响
会话超时	NetScaler 网关	4320	用户仅在需要在线身份验证时输入其 Citrix Secure Hub 凭据 - 每 3 天一次
强制超时	NetScaler 网关	无值	如果有任何活动，会话将延长。
最长离线时间	MDX 策略	71	需要每 3 天刷新一次策略。小时差是为了允许在会话超时之前进行刷新。
后台服务票证过期	MDX 策略	168 小时	STA 超时，允许在没有 NetScaler Gateway 会话令牌的情况下进行长时间会话。对于 Citrix Secure Mail，将 STA 超时设置得比会话超时更长，可以避免邮件通知在未提示用户的情况下停止。
需要微型 VPN 会话	MDX 策略	关	提供有效的网络连接和 NetScaler Gateway 会话以使用应用程序。
需要微型 VPN 会话的宽限期	MDX 策略	0	无宽限期（如果您启用了“需要微型 VPN 会话”）。
应用程序密码	MDX 策略	开	为应用程序要求密码。
使用密码加密机密	Citrix Endpoint Management 客户端属性	否	加密保管库时不需要用户熵。

启用 Citrix PIN 身份验证	Citrix Endpoint Management 客户端属性	是	启用 Citrix PIN 以简化身份验证体验。
PIN 强度要求	Citrix Endpoint Management 客户端属性	中等	强制执行中等密码复杂性规则。
PIN 类型	Citrix Endpoint Management 客户端属性	数字	PIN 是一个数字序列。
启用密码缓存	Citrix Endpoint Management 客户端属性	是	用户 PIN 缓存并保护 Active Directory 密码。
不活动计时器	Citrix Endpoint Management 客户端属性	30	如果用户在此期间未使用 MDX 应用程序或 Citrix Secure Hub，则提示进行离线身份验证。
启用触控 ID 身份验证	Citrix Endpoint Management 客户端属性	是	在 iOS 中为离线身份验证用例启用触控 ID。

高安全性

此配置对用户而言最方便，可提供基本级别的安全性。

设置	设置位置	推荐设置	行为影响
会话超时	奈思开勒 网关	10080	用户仅在需要在线身份验证时（每 7 天）输入其 Citrix Secure Hub 凭据
强制超时	奈思开勒 网关	无值	如果有任何活动，会话会延长。

最长离线时间	MDX 策略	167	每周（每 7 天）需要刷新策略。小时差是为了允许在会话超时之前进行刷新。
后台服务票证过期	MDX 策略	240	STA 超时，允许在没有 NetScaler Gateway 会话令牌的情况下进行长时间会话。对于 Citrix Secure Mail，将 STA 超时设置得比会话超时更长可以避免邮件通知停止。在这种情况下，如果用户在会话过期前没有打开应用程序，Citrix Secure Mail 不会提示用户。
需要微型 VPN 会话	MDX 策略	关	提供有效的网络连接和 NetScaler Gateway 会话以使用应用程序。
需要微型 VPN 会话的宽限期	MDX 策略	0	无宽限期（如果您启用了需要微型 VPN 会话）。
应用密码	MDX 策略	开	要求应用程序使用密码。
使用密码加密机密	Citrix Endpoint Management 客户端属性	否	不需要用户熵来加密保管库。
启用 Citrix PIN 身份验证	Citrix Endpoint Management 客户端属性	是	启用 Citrix PIN 以简化身份验证体验。

PIN 强度要求	Citrix Endpoint Management 客户端属性	低	无密码复杂性要求
PIN 类型	Citrix Endpoint Management 客户端属性	数字	PIN 是一个数字序列。
启用密码缓存	Citrix Endpoint Management 客户端属性	是	用户 PIN 缓存并保护 Active Directory 密码。
不活动计时器	Citrix Endpoint Management 客户端属性	90	如果用户在此期间未使用 MDX 应用程序或 Citrix Secure Hub，则提示进行离线身份验证。
启用触控 ID 身份验证	Citrix Endpoint Management 客户端属性	是	在 iOS 中为离线身份验证用例启用触控 ID。

使用升级身份验证

某些应用程序可能需要增强型身份验证。例如，辅助身份验证因素（如令牌）或激进的会话超时。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（可以在相同或不同的 NetScaler Gateway 设备上）。

设置	设置位置	推荐设置	行为影响
备用 NetScaler Gateway	MDX 策略	需要辅助 NetScaler Gateway 设备的 FQDN 和端口。	允许由辅助 NetScaler Gateway 设备身份验证和会话策略控制的增强型身份验证。

如果用户打开使用备用 NetScaler Gateway 的应用程序，则所有其他应用程序都将使用该 NetScaler Gateway 实例与内部网络通信。会话仅在增强安全性的 NetScaler Gateway 实例会话超时后，才会切换回安全性较低的 NetScaler Gateway 实例。

使用所需的微型 VPN 会话

对于某些应用程序（例如 Citrix Secure Web），您可以确保用户仅在拥有经过身份验证的会话时才运行应用程序。此策略强制执行该选项，并允许宽限期，以便用户可以完成其工作。

设置	设置位置	推荐设置	行为影响
需要微型 VPN 会话	MDX 策略	开	确保设备在线并具有有效的身份验证令牌。
需要微型 VPN 会话宽限期	MDX 策略	15	允许 15 分钟的宽限期，之后用户将无法再使用应用程序

服务器属性

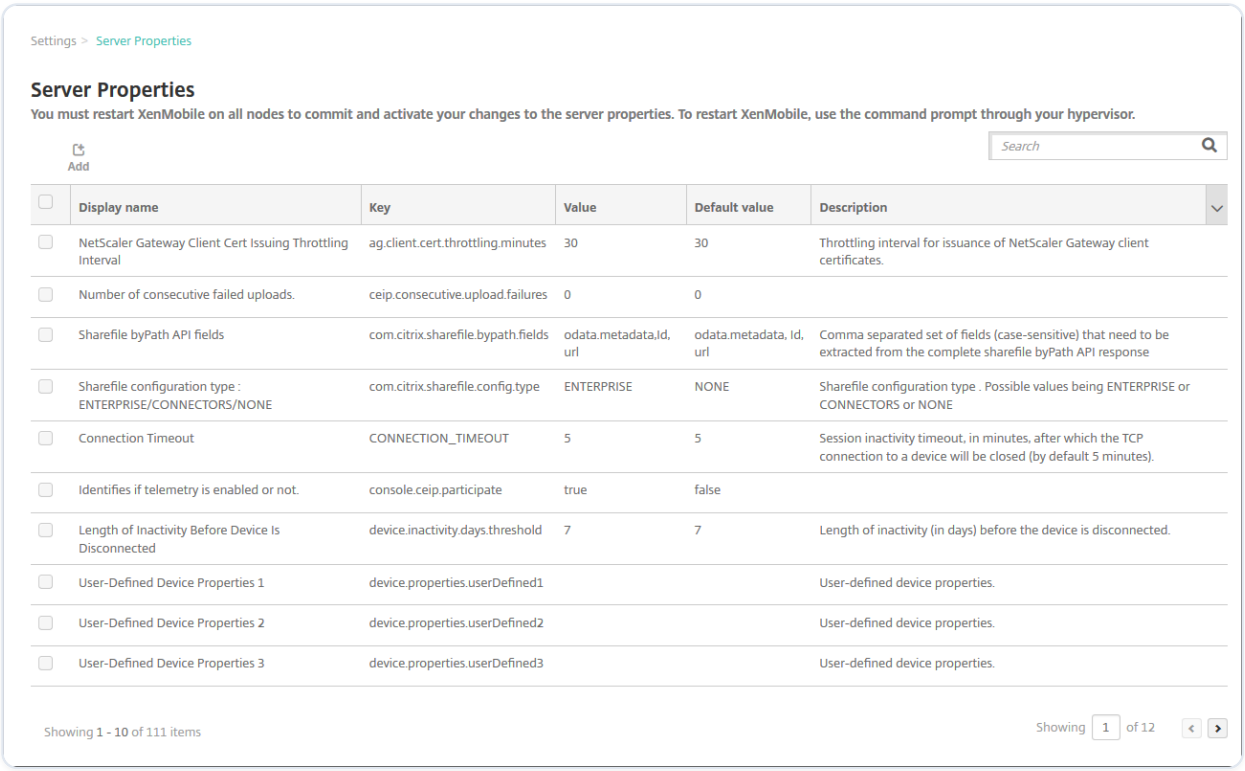
服务器属性是全局属性，适用于整个 Citrix Endpoint Management 实例中的操作、用户和设备。Citrix 建议您评估本文中涵盖的服务器属性以适应您的环境。在更改其他服务器属性之前，请务必咨询 Citrix。

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

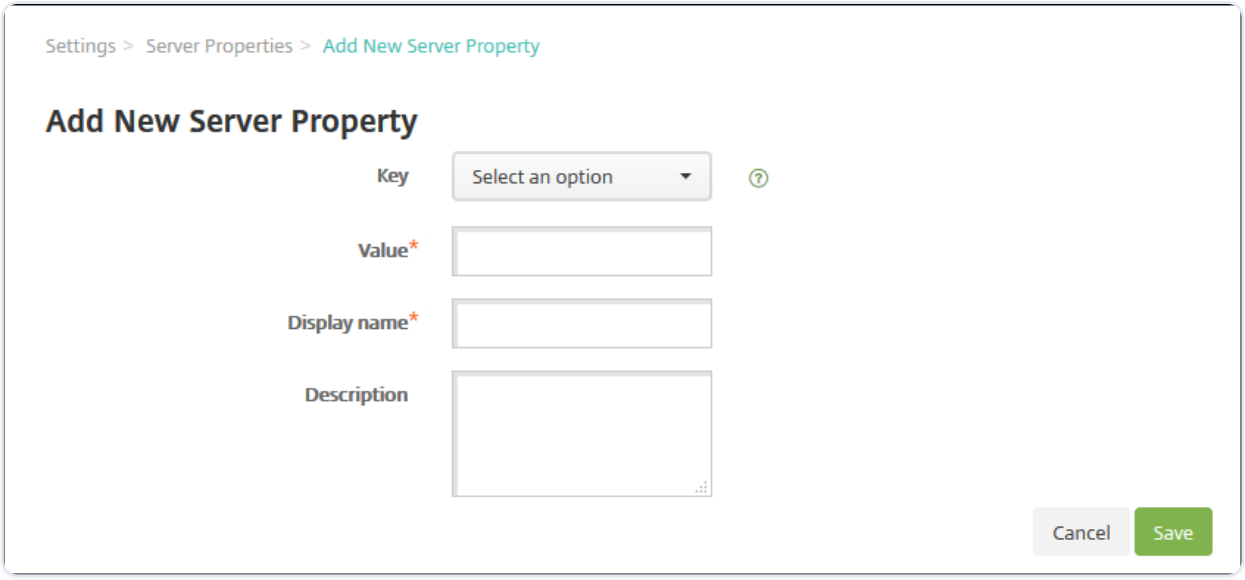
在 Citrix Endpoint Management 中，您可以将属性应用于服务器。

1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。将显示 **设置** 页面。
2. 在 **服务器** 下，单击 **服务器属性**。将显示 **服务器属性** 页面。您可以从此页面添加、编辑或删除服务器属性。



添加服务器属性

1. 单击 **添加**。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，选择相应的密钥。密钥区分大小写。在编辑属性值或请求特殊密钥之前，请联系 Citrix 支持。
   - 值：根据您选择的密钥输入一个值。
   - 显示名称：为新属性值输入一个名称，该名称将显示在 **服务器属性** 表中。
   - 描述：可选，输入新服务器属性的描述。

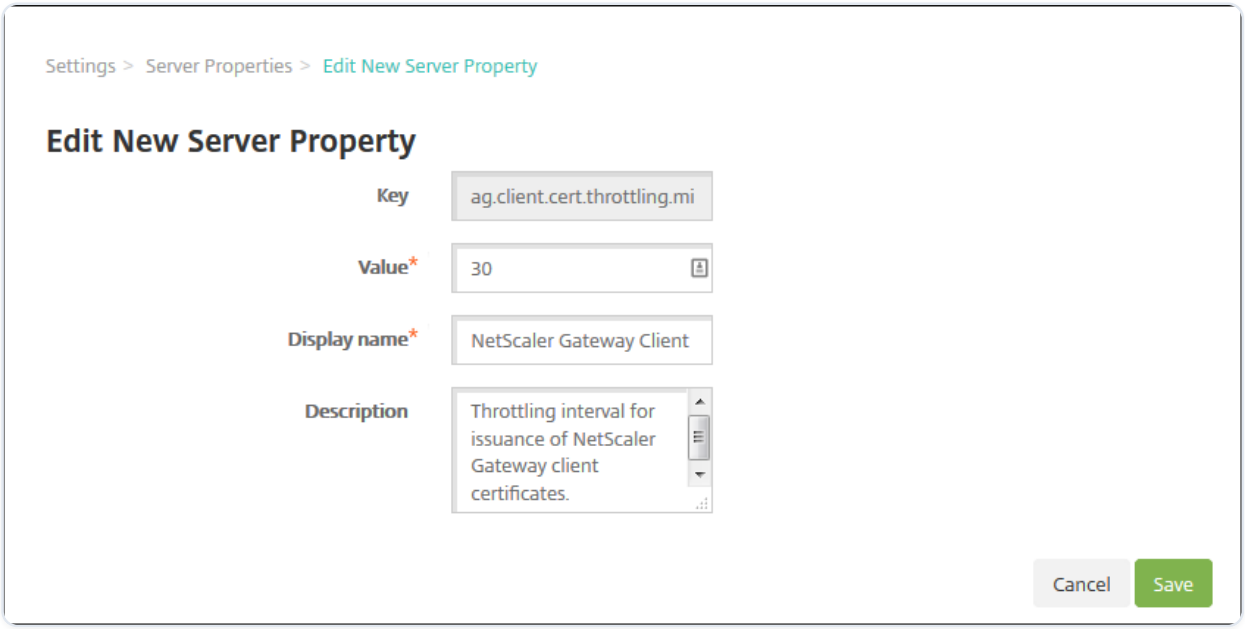
3. 点击 **保存**。

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。

   当您选择服务器属性旁边的复选框时，选项菜单会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. 点击 **编辑**。将显示 **编辑新服务器属性** 页面。



3. 根据需要更改以下信息：

   - 键：您无法更改此字段。
   - 值：属性值。
   - 显示名称：属性名称。
   - 描述：属性描述。

4. 点击 **保存** 以保存更改，或点击 **取消** 以保持属性不变。

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. 点击“**删除**”。出现确认对话框。再次点击“**删除**”。

服务器属性定义

访问托管 Google Play 商店中的所有应用程序

- 如果为 **true**，Citrix Endpoint Management 会使公共 Google Play 商店中的所有应用程序都可从托管 Google Play 商店访问。您可以使用 (/zh-cn/citrix-endpoint-management/policies/restrictions-policy.html#android-enterprise-settings) 来控制对这些应用程序的访问。默认为 **false**。

始终添加设备

- 如果为 **true**，Citrix Endpoint Management 会将设备添加到 Citrix Endpoint Management 控制台，即使设备注册失败。因此，您可以查看哪些设备尝试注册。默认为 **false**。

AG 客户端证书颁发限制间隔

- 生成证书之间的宽限期。此间隔可防止 Citrix Endpoint Management 在短时间内为设备生成大量证书。Citrix 建议您不要更改此值。默认为 **30** 分钟。

允许删除在指定时间段内标记为非活动状态的设备

- 如果为 **true**，在指定时间（以天为单位）内处于非活动状态的设备将从 Citrix Endpoint Management 中删除。活动期限由“**设备在从 CEM 自动删除之前可以处于非活动状态的时间长度**”服务器属性设置。默认为 **true**。要更改此属性的值，请咨询您的 Citrix 代表。

审计日志记录器

- 如果为 **False**，不记录用户界面 (UI) 事件。默认为 **False**。

阻止已 Root 的 Android 设备和已越狱的 iOS 设备注册

当此属性设置为 **true** 时，Citrix Endpoint Management 会阻止已 Root 的 Android 设备和已越狱的 iOS 设备的注册。建议所有安全级别都设置为 **true**。默认为 **true**。

cdn.s3.retry.interval 和 cdn.s3.max.retry

服务器属性 `cdn.s3.retry.interval` 和 `cdn.s3.max.retry` 协同工作，为每个 macOS PKG 文件上传设置最大时间限制。默认情况下，Citrix 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，则上传失败。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 Citrix Endpoint Management 验证文件上传是否成功完成的间隔（以毫秒为单位）。默认值为 `10000`。
- `cdn.s3.max.retry`。允许您定义在上传失败之前最大验证重试次数。默认值为 `10`。

这两个键协同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）。

证书续订（秒）

- 证书过期前 Citrix Endpoint Management 开始续订证书的秒数。例如，当证书于 12 月 30 日过期且此属性设置为 30 天时。如果设备在 12 月 1 日至 12 月 30 日之间连接，Citrix Endpoint Management 会尝试续订证书。默认为 **2592000** 秒（30 天）。

连接超时

- 会话不活动超时（以分钟为单位），在此之后 Citrix Endpoint Management 会关闭与设备的 TCP 连接。会话保持打开状态。适用于 Android 设备。默认为 **5** 分钟。

默认部署通道

- 确定 Citrix Endpoint Management 如何将资源部署到设备：用户级别 (**DEFAULT_TO_USER**) 或设备级别。默认为 **DEFAULT_TO_DEVICE**。

弃用移动服务提供商

- 弃用对用于查询 Blackberry 和其他 Exchange ActiveSync 设备的移动服务提供商接口的支持。启用后，**移动服务提供商**接口将从控制台中隐藏。默认值为 **true**。

设备标记

- 如果将 `enable.device.tagging` 设置为 **true**，Citrix Endpoint Management 会自动按设备类型标记设备。您可以使用设备标记来部署策略和应用程序或配置交付组。Citrix Endpoint Management 会为以下设备应用标记：
    - BYOD 标记
        - iOS 用户注册
        - Android Enterprise 工作配置文件
    - 公司标签
        - Android Enterprise 完全托管的企业设备
        - 批量注册
            - 苹果商务管理设备
            - 苹果校园管理设备
            - Windows AutoPilot 设备
            - Android Enterprise 批量注册

禁用主机名验证

- 默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。当主机名验证失败时，服务器日志中会包含以下错误：“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”。如果主机名验证导致部署中断，请将此属性更改为 **true**。默认为 **false**。

禁用 SSL 服务器验证

- 如果为 **True**，则在满足以下所有条件时禁用 SSL 服务器证书验证：
  - 您已在 Citrix Endpoint Management 上启用基于证书的身份验证
  - Microsoft CA 服务器是证书颁发者
  - 内部 CA（其根证书不受 Citrix Endpoint Management 信任）签署了您的证书。

  默认为 **True**。

启用崩溃报告

- 如果为 **true**，Citrix 会收集崩溃报告和诊断信息，以帮助排查适用于 iOS 和 Android 的 Citrix Secure Hub 的问题。如果为 **false**，则不收集任何数据。默认值为 **true**。

启用/禁用 Hibernate 统计信息日志记录用于诊断

- 如果为 **True**，则启用 Hibernate 统计信息日志记录，以帮助排查应用程序性能问题。Hibernate 是用于 Citrix Endpoint Management 连接到 Microsoft SQL Server 的组件。默认情况下，日志记录处于禁用状态，因为它会影响应用程序性能。仅在短时间内启用日志记录，以避免创建巨大的日志文件。Citrix Endpoint Management 将日志写入 /opt/sas/logs/hibernate_stats.log。默认为 **False**。

启用 macOS OTAE

- 如果为 **false**，则阻止 macOS 设备使用注册链接，这意味着 macOS 用户只能通过注册邀请进行注册。默认为 **true**。

启用通知触发器

- 启用或禁用 Citrix Secure Hub 客户端通知。值为 **true** 时启用通知。默认为 **true**。

完全拉取 ActiveSync 允许和拒绝的用户

- Citrix Endpoint Management 拉取 ActiveSync 允许和拒绝用户的完整列表（基线）的间隔（以秒为单位）。默认为 **28800** 秒。

标识遥测是否已启用

- 标识遥测是否已启用。遥测也称为客户体验改善计划 (CEIP)。您可以在安装或升级 Citrix Endpoint Management 时选择加入 CEIP。如果 Citrix Endpoint Management 连续 15 次上传失败，它将禁用遥测。默认为 **false**。

不活动超时（分钟）

- Citrix 端点管理在非活动用户注销前的分钟数。用户必须已使用 Citrix 端点管理公共 API 访问 Citrix 端点管理控制台或任何第三方应用程序。超时值设置为 **0** 表示非活动用户保持登录状态。对于访问 API 的第三方应用程序，保持登录通常是必需的。默认值设置为 **5**。
- 如果 **WebServices timeout type** 服务器属性为 **INACTIVITY_TIMEOUT**：此属性定义了 Citrix 端点管理在非活动管理员执行以下操作后注销前的分钟数：
  - 使用 REST 服务的公共 API 访问 Citrix 端点管理控制台
  - 使用 REST 服务的公共 API 访问任何第三方应用程序。超时值设置为 **0** 表示非活动用户保持登录状态。

include.device.properties.during.search

- 在设备搜索中包含所有设备属性。默认值为 **Off**，这将搜索范围限制为以下设备属性，以实现快速搜索：
  - 序列号
  - IMEI
  - Wi-Fi MAC 地址
  - 蓝牙 MAC 地址
  - 活动同步 ID
  - 用户名

  当此属性设置为 **On** 时，设备搜索可能需要更长时间。

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- 指定离线 iOS 或 macOS 设备被视为不可达的天数。当 iOS 或 macOS 设备达到指定限制时，它们将停止与 Citrix 端点管理进行检查。这两个属性的默认值均为 **45** 天。

iOS 设备管理注册（如果需要）安装根 CA

- 对于所有 Citrix Endpoint Management 环境，服务器属性 **ios.mdm.enrollment.installRootCalfRequired** 都设置为 **False**。Citrix 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步延迟

- 在设备注册期间，此属性值指定在安装 MDM 配置文件和在设备上启动代理之间等待的时间量。Citrix 建议仅在出现网络延迟或速度问题时编辑此属性。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）。

iOS 设备管理身份交付模式

- 指定 Citrix Endpoint Management 是使用 **SCEP**（出于安全原因推荐）还是 **PKCS12** 将 MDM 证书分发到设备。在 PKCS12 模式下，密钥对在服务器上生成，不进行协商。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 Citrix Endpoint Management iOS 代理身份的私钥大小。默认值为 **2048**。

iOS 设备管理身份续订天数

- 指定在证书过期前多少天 Citrix Endpoint Management 开始续订证书。例如：如果证书在 10 天内过期，并且此属性为 **10** 天：当设备在过期前 9 天连接时，Citrix 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，Citrix Endpoint Management 需要此密码才能将通知推送到 Apple 服务器。

设备断开连接前的非活动时长

- 指定设备在 Citrix Endpoint Management 断开连接之前可以处于非活动状态（包括上次身份验证）的时长。默认值为 **7** 天。

设备在自动从 CEM 中移除前的非活动时长

- 设备在自动从 Citrix Endpoint Management 中移除之前可以处于非活动状态的时间长度（以天为单位）。最短为 **14** 天，默认值为 **30** 天。此属性生效，必须将“**允许删除在指定时间段内标记为非活动的设备**”服务器属性设置为 **true**。

local.user.account.lockout.time

- 指定用户在超出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。默认值设置为 **6**。

mac.dep.admin.passwd.rotate

此服务器属性允许您为通过 Apple Deployment Program 注册的 macOS 设备配置管理员密码轮换间隔。Citrix Endpoint Management 每天检查是否轮换管理员帐户的密码。默认情况下，Citrix 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* Citrix Endpoint Management 轮换密码的间隔（以分钟为单位）。键入一个等于或大于 360（6 小时）的值。Citrix Endpoint Management 会忽略小于 360 的值，并改为每 360 分钟（6 小时）轮换一次密码。
- 显示名称：*管理员定义*
- 描述：*管理员定义*

仅限 MAM 设备最大值

- 此自定义密钥限制每个用户可以注册的仅限 MAM 设备的数量。按如下方式配置密钥。**值**为 **0** 允许无限设备注册。
- 密钥 = **number.of.mam.devices.per.user**
- 值 = **5**
- 显示名称 = **仅限 MAM 设备最大值**
- Description = **限制每个用户可以注册的 MAM 设备数量。**

MaxNumberOfWorker

- 导入大量批量购买许可证时使用的线程数。默认为 **3**。如果需要进一步优化，可以增加线程数。但是，线程数越多会导致 CPU 使用率越高。

NetScaler Gateway (NetScaler) 单点登录

- 如果为 **False**，则在从 NetScaler Gateway 到 Citrix Endpoint Management 的单点登录期间禁用 Citrix Endpoint Management 回调功能。如果 NetScaler Gateway 配置包含回调 URL，Citrix Endpoint Management 将使用回调功能验证 NetScaler Gateway 会话 ID。默认为 **False**。

连续上传失败次数

- 显示客户体验改善计划 (CEIP) 上传期间连续失败的次数。当上传失败时，Citrix Endpoint Management 会增加该值。在 15 次上传失败后，Citrix Endpoint Management 会禁用 CEIP（也称为遥测）。有关详细信息，请参阅服务器属性 **Identifies if telemetry is enabled or not**。当上传成功时，Citrix Endpoint Management 会将该值重置为 **0**。

每设备用户数

- 可以在 MDM 中注册同一设备的最大用户数。值 **0** 表示可以注册同一设备的无限数量的用户。默认为 **0**。

optional.user.identity.attributes

- 此服务器属性允许您自定义可选的 Active Directory 用户属性。

  创建自定义密钥，并在“**值**”字段中编辑用户属性，以定义 Citrix Endpoint Management 可以访问哪些属性来创建用户帐户。有关详细信息，请参阅自定义用户属性。

  - 密钥：**Custom Key**
  - 密钥：**optional.user.identity.attributes**
  - 值：**通用名称, 名, 姓, 显示名称, 街道地址, 城市, 州/省, 国家/地区, 工作电话, 家庭电话, 手机, 公司, 部门, 描述, 员工ID, 传真号码, 姓名首字母, IP电话, 经理, 家庭邮政地址, 其他手机, 寻呼机, 物理交付办公室名称, 邮政编码, 邮政信箱, 职称, 组织, 首选语言**
  - 显示名称：**optional.user.identity.attributes**
  - 描述：**可选的 Active Directory 用户属性**

macOS 和 iOS/iPadOS 注册配置文件中的组织名称

- 您为 `apple.mdm.enrollment.profile.organization.name` 输入的值对应于提供注册配置文件的组织的名称。当用户将其设备注册到 Citrix Endpoint Management 时，将显示该名称。默认显示的名称是 **Citrix Workspace**。

拉取允许和拒绝用户的增量更改

- Citrix Endpoint Management 在运行 PowerShell 命令以获取 ActiveSync 设备的增量时，等待域响应的秒数。默认为 **60** 秒。

Microsoft 认证服务器的读取超时

- Citrix Endpoint Management 在执行读取操作时，等待证书服务器响应的秒数。如果证书服务器速度慢且流量大，您可以将此值增加到 60 秒或更长时间。如果证书服务器在 120 秒后仍无响应，则需要维护。默认为 **15000** 毫秒（15 秒）。

REST Web 服务

- 启用 REST Web 服务。默认为 **true**。

按指定大小分块检索设备信息

- 此值在设备导出期间用于内部多线程处理。如果值较高，则单个线程解析更多设备。如果值较低，则更多线程获取设备。减小此值可能会提高导出和设备列表获取的性能，但可能会减少可用内存。默认为 **1000**。

shp.console.enable

- 如果为 **False**，则阻止访问自助服务门户。在端口 4443 上导航到门户的用户会收到“访问被拒绝”消息。如果为 **True**，则通过端口 443 提供对自助服务门户的访问。

  默认为 **False**。

enable.new.shp

- 如果为 **False**，则阻止用户从自助服务门户启用其设备。如果为 **True**，则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**。

  默认为 **False**。

会话日志清理（天）

- Citrix Endpoint Management 保留会话日志的天数。默认为 **7**。

ShareFile 配置类型

- 指定 Citrix Files 存储类型。**ENTERPRISE** 启用 Citrix Files 企业模式。**CONNECTORS** 仅提供对您通过 Citrix Endpoint Management 控制台创建的存储区域连接器的访问权限。默认为 **NONE**，这将显示“**配置 > Citrix Files**”屏幕的初始视图，您可以在其中选择 Citrix Files Enterprise 和连接器。默认为 **NONE**。

静态超时（分钟）

- 如果 **WebServices timeout type** 服务器属性为 **STATIC_TIMEOUT**：此属性定义了 Citrix Endpoint Management 在管理员使用以下各项后注销管理员的分钟数：
  - 用于访问 Citrix Endpoint Management 控制台的 REST Services 公共 API。
  - 用于访问任何第三方应用程序的 REST Services 公共 API。

  默认为 **60**。

触发代理消息抑制

- 启用或禁用 Citrix Secure Hub 客户端消息传送。值 **false** 启用消息传送。默认为 **true**。

触发代理声音抑制

- 启用或禁用 Citrix Secure Hub 客户端声音。值 **false** 启用声音。默认为 **true**。

适用于 Android 设备的未经身份验证的应用下载

- 如果为 **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 Android Enterprise 选项以在 Google Play 商店中静态提供下载 URL，则 Citrix Endpoint Management 需要此属性。在这种情况下，下载 URL 不能包含一次性票证（由 **XAM One-Time Ticket server** 属性定义），该票证包含身份验证令牌。默认为 **False**。

适用于 Windows 设备的未经身份验证的应用下载

- 仅用于不验证一次性票证的旧版 Citrix Secure Hub。如果为 **False**，则可以从 Citrix Endpoint Management 下载未经身份验证的应用程序到 Windows 设备。默认为 **False**。

使用 ActiveSync ID 执行 ActiveSync 设备擦除

- 如果为 **true**，则 Citrix Endpoint Management 的 Exchange ActiveSync 连接器将 ActiveSync 标识符用作 **asWipeDevice** 方法的参数。默认为 **false**。

仅来自 Exchange 的用户

- 如果为 **true**，则禁用 ActiveSync Exchange 用户的用户身份验证。默认为 **false**。

批量采购基线间隔

- Citrix Endpoint Management 从 Apple 重新导入批量采购许可证的最小间隔。刷新许可证信息可确保 Citrix Endpoint Management 反映所有更改，例如手动从批量采购中删除导入的应用程序时。默认情况下，Citrix Endpoint Management 至少每 **1440** 分钟刷新一次批量采购许可证基线。
    - 如果您安装了大量批量采购许可证（例如，超过 50,000 个）：Citrix 建议您增加基线间隔，以减少导入许可证的频率和开销。
    - 如果您预计 Apple 会频繁更改批量采购许可证：Citrix 建议您降低该值，以使 Citrix Endpoint Management 及时更新这些更改。
    - 两个基线之间的最小间隔为 60 分钟。此外，Citrix Endpoint Management 每 60 分钟执行一次增量导入，以捕获自上次导入以来的更改。因此，如果批量采购基线间隔为 60 分钟，则基线之间的间隔可能会延迟长达 119 分钟。

WebServices 超时类型

- 指定如何使从公共 API 检索到的身份验证令牌过期。
  - 如果是 **STATIC_TIMEOUT**：Citrix Endpoint Management 根据服务器属性 **Static Timeout in Minutes** 的值，将令牌视为已过期。
  - 如果是 **INACTIVITY_TIMEOUT**：Citrix Endpoint Management 根据服务器属性 **Inactivity Timeout in Minutes** 的值，将令牌视为已过期。默认为 **STATIC_TIMEOUT**。

Windows 平板电脑 MDM 证书延长有效期 (5 年)

- MDM 为 Windows 平板电脑颁发的设备证书的有效期。设备在设备管理期间使用设备证书向 MDM 服务器进行身份验证。如果为 **true**，则有效期为五年。如果为 **false**，则有效期为两年。默认为 **true**。

Windows WNS 通道 - 续订前天数

- ChannelURI 的续订频率。默认为 **10** 天。

Windows WNS 心跳间隔

- Citrix Endpoint Management 在每三分钟连接设备五次后，再次连接设备之前等待的时间。默认为 **6** 小时。

XAM 一次性票证

- 一次性身份验证令牌 (OTT) 下载应用程序的有效毫秒数。此属性与属性 **Unauthenticated App download for Android** 和 **Unauthenticated App download for Windows** 协同工作。这些属性指定是否允许未经身份验证的应用程序下载。默认为 **3600000**。

Citrix Endpoint Management MDM 自助服务门户控制台最大非活动间隔（分钟）

- 此属性名称反映了较旧的 Citrix Endpoint Management 版本。该属性控制 Citrix Endpoint Management 控制台的最大非活动间隔。该间隔是指 Citrix Endpoint Management 将非活动用户从 Citrix Endpoint Management 控制台注销的分钟数。超时设置为 **0** 意味着非活动用户将保持登录状态。默认值为 **30**。

从 ABM MDM 服务器取消分配时，从 CEM 中删除 ABM 设备

- 如果 `remove.unassigned.abm.devices` 为 **true**，CEM 会移除不再分配给此服务器的设备。默认为 **false**。

设备和应用策略

Citrix Endpoint Management 设备和应用策略使您能够在以下因素之间优化平衡：

- 企业安全性
- 企业数据和资产保护
- 用户隐私
- 高效且积极的用户体验

这些因素之间的最佳平衡可能有所不同。例如，金融等高度受监管的组织比教育和零售等其他行业需要更严格的安全控制，而在教育和零售行业中，用户生产力是首要考虑因素。

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，以限制对企业内容的恶意使用。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。总体结果是提供了一个解决方案，在确保安全性和管理控制的同时，提高了员工满意度和生产力。

本文主要关注与安全性相关的许多设备和应用策略。

解决安全风险的策略

Citrix Endpoint Management 设备和应用策略解决了许多可能构成安全风险的情况，例如：

- 用户尝试从不受信任的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
- 已离职的用户使用了自己的设备 (BYOD)
- 用户放错了设备
- 用户必须始终安全地访问网络
- 用户拥有自己的受管设备，您必须将工作数据与个人数据分开
- 设备处于空闲状态，需要再次验证用户凭据
- 用户将敏感内容复制并粘贴到未受保护的电子邮件系统中
- 用户在同时包含个人帐户和公司帐户的设备上接收带有敏感数据的电子邮件附件或网页链接

这些情况与保护公司数据时的两个主要关注领域有关，即数据处于以下状态时：

- 静态
- 传输中

Citrix 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。Citrix Endpoint Management 使用 iOS 和 Android 平台提供的设备加密。Citrix Endpoint Management 通过 Citrix MAM SDK 提供的合规性检查等功能补充了基于平台的加密。

Citrix Endpoint Management 中的移动应用程序管理 (MAM) 功能可对 Citrix 移动生产力应用程序、启用 MDX 的应用程序及其关联数据进行全面的管理、安全和控制。

移动应用程序 SDK 通过使用 Citrix MDX 应用程序容器技术，为 Citrix Endpoint Management 部署启用应用程序。容器技术将用户设备上的公司应用程序和数据与个人应用程序和数据分开。数据分离使您能够通过全面的基于策略的控制来保护任何自定义开发、第三方或 BYO 移动应用程序。

Citrix Endpoint Management 还包括应用程序级加密。Citrix Endpoint Management 会单独加密存储在任何启用 MDX 的应用程序中的数据，而无需设备密码，也无需您管理设备来强制执行策略。

- 在 iOS 设备上，Citrix Endpoint Management 使用强大的 FIPS 验证加密服务和库，例如密钥链。
- OpenSSL 为各种设备平台提供 FIPS 验证模块。OpenSSL 进一步保护传输中的数据以及管理和注册设备所需的证书。
- Citrix Endpoint Management 使用 MAM SDK 共享保管库 API 在具有相同密钥链访问组的应用程序之间共享托管内容。例如，您可以通过已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获取证书。
- Citrix Endpoint Management 使用平台提供的设备加密。
- Citrix Endpoint Management 的 MAM 应用程序级控制会执行合规性检查，以验证每次应用程序启动时是否启用了设备加密。

Citrix Endpoint Management 如何保护传输中的数据

用户移动设备与内部网络之间传输的数据称为传输中的数据。MDX 应用程序容器技术通过 NetScaler Gateway 提供对内部网络的应用程序专用 VPN 访问。

假设员工希望从移动设备访问安全企业网络中的以下资源：

- 公司电子邮件服务器
- 托管在公司内网上的启用 SSL 的 Web 应用程序
- 存储在文件服务器或 Microsoft SharePoint 上的文档

MDX 通过应用程序专用微 VPN 允许从移动设备访问所有这些企业资源。每个设备都有自己的专用微 VPN 隧道。

微 VPN 功能不需要设备范围的 VPN，这可能会损害不受信任的移动设备上的安全性。因此，内部网络不会暴露于可能感染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可以在一台设备上共存。

为了提供更强的安全级别，您可以为启用 MDX 的应用程序配置备用 NetScaler Gateway 策略。该策略用于身份验证以及与应用程序的微 VPN 会话。您可以将备用 NetScaler Gateway 与微 VPN 会话所需策略结合使用，以强制应用程序重新向特定网关进行身份验证。此类网关通常可能具有不同的（更高保证的）身份验证要求和流量管理策略。

除了安全功能外，微 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
- 传输以最快速度完成。速度可改善用户体验，这是移动设备普及的关键成功因素。

定期重新评估设备策略，例如在以下情况下：

- 当新版 Citrix Endpoint Management 因设备操作系统更新发布而包含新的或更新的策略时
- 添加设备类型时：

  尽管许多策略对所有设备都通用，但每种设备都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 设备之间存在差异，甚至不同制造商的 Android 设备之间也存在差异。
- 使 Citrix Endpoint Management 操作与企业或行业变化保持同步，例如新的公司安全策略或合规性法规
- 当新版 MAM SDK 包含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，为用户集成新工作流

应用程序策略和用例场景

尽管您可以选择通过 Citrix Secure Hub 提供哪些应用程序，但您可能还需要定义这些应用程序如何与 Citrix Endpoint Management 交互。使用应用程序策略：

- 如果您希望用户在经过一定时间后进行身份验证。
- 如果您希望为用户提供对其信息的离线访问。

以下各节包含一些策略和示例用法。

- 有关可使用 MAM SDK 集成到 iOS 和 Android 应用程序中的第三方策略列表，请参阅 MAM SDK 概述。
- 有关每个平台的 MDX 策略列表，请参阅 MDX 策略一览。

身份验证策略

- **设备密码**

为何使用此策略： 启用设备密码策略，以强制用户仅在设备启用了设备密码的情况下才能访问 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 设备上设置密码，然后才能访问 MDX 应用程序。

- **应用程序密码**

  为何使用此策略： 启用应用程序密码策略，以使 Citrix Secure Hub 在用户打开托管应用程序并访问数据之前提示用户进行身份验证。用户可以使用其 Active Directory 密码、Citrix PIN 或 iOS TouchID 进行身份验证，具体取决于您在 Citrix Endpoint Management 控制台的**设置 > 客户端属性**下配置的内容。您可以在客户端属性中设置一个非活动计时器，以便 Citrix Secure Hub 在计时器到期之前不会提示用户重新对托管应用程序进行身份验证。

  应用程序密码与设备密码不同。通过推送到设备的设备密码策略，Citrix Secure Hub 会提示用户配置密码或 PIN。用户必须在打开设备或非活动计时器到期时解锁其设备。有关详细信息，请参阅 Citrix Endpoint Management 中的身份验证。

  用户示例： 如果非活动期已过期，用户在设备上打开 Citrix Secure Web 应用程序时，必须输入其 Citrix PIN 才能浏览网站。

- **需要微型 VPN 会话**

  为何使用此策略： 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。Citrix Endpoint Management 随后会提示用户连接到企业网络或在使用应用程序之前拥有活动会话。

  用户示例： 当用户尝试打开启用了微型 VPN 会话所需策略的 MDX 应用程序时：他们无法使用该应用程序，直到连接到网络。连接必须使用蜂窝网络或 Wi-Fi 服务。

- **最长脱机期限**

  为何使用此策略： 将此策略用作额外的安全选项。此策略可确保脱机运行应用程序达到指定持续时间的用户必须重新确认应用程序授权并刷新策略。

  用户示例： 如果您为 MDX 应用程序配置了最长脱机期限，则用户可以脱机打开和使用该应用程序，直到脱机计时器期限到期。届时，用户必须通过蜂窝网络或 Wi-Fi 服务重新连接到网络，并在出现提示时重新进行身份验证。

杂项访问策略

- **应用更新宽限期（小时）**

为何使用此策略： 应用更新宽限期是指用户在必须更新应用商店中可用新版本应用之前可用的时间。在宽限期到期时，用户必须更新应用才能访问应用中的数据。设置此值时，请记住您的移动员工的需求，特别是那些在国际旅行时可能长时间离线的用户。

用户示例： 您在应用商店中加载了新版本的 Citrix Secure Mail，然后将应用更新宽限期设置为 6 小时。Citrix Secure Hub 用户有 6 小时的时间来升级 Citrix Secure Mail，之后他们将被重定向到应用商店。

- **活动轮询周期（分钟）**

  为何使用此策略： 活动轮询周期是 Citrix Endpoint Management 检查应用以确定何时执行安全操作（例如应用锁定和应用擦除）的时间间隔。

  用户示例： 如果您将活动轮询周期策略设置为 60 分钟，然后发送应用锁定命令，则锁定将在上次轮询后的 60 分钟内发生。

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。

应用交互策略

为何使用这些策略： 使用应用交互策略来控制文档和数据从 MDX 应用流向设备上其他应用。例如，您可以阻止用户执行以下操作：

- 将数据移动到容器外部的个人应用
- 将数据从容器外部粘贴到容器化应用中

用户示例： 您将应用交互策略设置为“受限”，这意味着用户可以将文本从 Citrix Secure Mail 复制到 Citrix 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，用户可以将 Citrix Secure Mail 中的附件文档打开到 Citrix Files 或 QuickEdit 中。用户无法在容器外部的个人文件查看应用中打开附件文档。

应用限制策略

为何使用这些策略： 使用应用程序限制策略来控制用户在MDX应用程序打开时可以访问的功能。这些限制有助于确保应用程序运行时不会发生恶意活动。应用程序限制策略在iOS和Android之间略有不同。例如，在iOS中，您可以在MDX应用程序运行时阻止访问iCloud。在Android中，您可以在MDX应用程序运行时停止使用NFC。

用户示例： 假设您在MDX应用程序中启用了应用程序限制策略以阻止iOS上的听写功能。因此，用户在MDX应用程序运行时无法使用iOS键盘上的听写功能。这样，用户听写的数据就不会传递给不

安全的第三方云听写服务。当用户在容器外部打开其个人应用程序时，听写选项仍可供用户用于其个人通信。

应用程序网络访问策略

为何使用这些策略： 使用应用程序网络访问策略，允许设备上容器中的MDX应用程序访问公司网络内部的数据。隧道式 - Web SSO选项仅允许HTTP和HTTPS流量的隧道传输。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： 当用户打开启用了隧道功能的MDX应用程序时，浏览器会打开一个内部网站点，而无需用户启动VPN。该应用程序使用微型VPN技术自动访问内部站点。

应用程序地理位置和地理围栏策略

为何使用这些策略： 控制应用程序地理位置和地理围栏的策略包括中心点经度、中心点纬度和半径。这些策略允许MDX应用程序访问特定地理区域的数据。这些策略通过经纬度坐标的半径定义地理区域。如果用户尝试在定义的半径之外使用应用程序，则应用程序将保持锁定状态，用户无法访问应用程序数据。

用户示例： 用户可以在其办公地点访问并购数据。当他们离开办公地点时，这些敏感数据将无法访问。

Citrix Secure Mail 应用程序策略

- **后台网络服务**

  为何使用此策略： Citrix Secure Mail 中的后台网络服务使用安全票证颁发机构 (STA)，它实际上是一个SOCKS5代理，用于通过NetScaler Gateway连接。与微型VPN相比，STA支持长时间连接并提供更好的电池续航时间。因此，STA非常适合需要持续连接的邮件。Citrix建议您为Citrix Secure Mail配置这些设置。适用于XenMobile的NetScaler向导会自动为Citrix Secure Mail设置STA。

  用户示例： 当STA未启用且Android用户打开Citrix Secure Mail时，系统会提示他们打开VPN，该VPN会在设备上保持打开状态。当STA启用且Android用户打开Citrix Secure Mail时，Citrix Secure Mail会无缝连接，无需VPN。

- **默认同步间隔**

  为何使用此策略： 此设置指定用户首次访问Citrix Secure Mail时同步到Citrix Secure Mail的默认邮件天数。两周的邮件同步时间比三天邮件的同步时间长。需要同步的数据越多，用户的设置过程就越长。

  用户示例： 假设用户首次设置Citrix Secure Mail时，默认同步间隔设置为三天。用户可以在收件箱中看到从当前到过去三天内收到的任何电子邮件。如果用户想查看三天前的电子邮件，他们可

以进行搜索。Citrix Secure Mail随后会显示存储在服务器上的旧电子邮件。安装Citrix Secure Mail后，每个用户都可以更改此设置以更好地满足其需求。

设备策略和用例行为

设备策略（有时也称为 MDM 策略）决定了 Citrix Endpoint Management 如何管理设备。尽管许多策略对所有设备都通用，但每台设备都有一组特定于其操作系统的策略。以下列表包含一些设备策略，并讨论了如何使用它们。有关所有设备策略的列表，请参阅 (/zh-cn/citrix-endpoint-management/policies.html) 下的文章。

- **应用程序清单策略**

  为何使用此策略： 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。如果不部署此策略，则只能看到用户从应用商店安装的应用程序，而不能看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： 拥有 MDM 管理设备的用户无法禁用此功能。用户的个人安装应用程序对 Citrix Endpoint Management 管理员可见。

- **应用程序锁定策略**

  为何使用此策略： 适用于 Android 的“应用程序锁定策略”允许您将应用程序置于允许列表或阻止列表。例如，对于允许的应用程序，您可以配置自助服务终端设备。通常，您只将“应用程序锁定策略”部署到公司拥有的设备，因为它限制了用户可以安装的应用程序。您可以设置一个覆盖密码，以向用户提供对被阻止应用程序的访问权限。

  用户示例： 假设您部署了一个阻止“愤怒的小鸟”应用程序的“应用程序锁定策略”。用户可以从 Google Play 安装“愤怒的小鸟”应用程序，但是当他们打开该应用程序时，会收到一条消息，告知他们管理员已阻止该应用程序。

- **连接计划策略**

  为何使用此策略： “连接计划策略”使 Windows Mobile 设备能够连接回 Citrix 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 Citrix Endpoint Management 的连接。计划选项如下：

  - **从不：** 手动连接。用户必须从其设备上的 Citrix Endpoint Management 启动连接。Citrix 不建议将此选项用于生产部署，因为它会阻止您向设备部署安全策略。因此，用户不会收到新的应用程序或策略。默认情况下启用**从不**选项。
  - **每次：** 按选定的时间间隔连接。当您发送安全策略（例如锁定或擦除）时，Citrix Endpoint Management 会在设备下次连接时处理设备上的策略。

  - **定义计划：** Citrix Endpoint Management 会在网络连接丢失后尝试将用户的设备重新连接到 Citrix Endpoint Management 服务器。Citrix 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： 您希望将密码策略部署到已注册的设备。计划策略可确保设备以固定的时间间隔连接回服务器以收集新策略。

- **凭据策略**

  为何使用此策略：凭据策略通常与网络策略结合使用，它允许您部署证书，以便对需要证书身份验证的内部资源进行身份验证。

  用户示例：您部署一个网络策略，用于在设备上配置无线网络。Wi-Fi 网络需要证书进行身份验证。凭据策略部署一个证书，该证书随后存储在操作系统密钥库中。用户连接到内部资源时可以选择该证书。

- **Exchange 策略**

  为何使用此策略：借助 Citrix Endpoint Management，您有两种选项来交付 Microsoft Exchange ActiveSync 电子邮件。

  - **Citrix Secure Mail 应用程序：**通过使用您从公共应用商店或应用商店分发的 Citrix Secure Mail 应用程序来交付电子邮件。
  - **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。您可以使用宏从用户的 Active Directory 属性填充用户数据，例如使用 `${user.username}` 填充用户名，使用 `${user.domain}` 填充用户域。

  用户示例：当您推送 Exchange 策略时，会将 Exchange Server 详细信息发送到设备。Citrix Secure Hub 随后会提示用户进行身份验证，然后其电子邮件开始同步。

- **位置策略**

  为何使用此策略：如果设备为 Citrix Secure Hub 启用了 GPS，位置策略允许您在地图上对设备进行地理定位。部署此策略并从 Citrix Endpoint Management 发送定位命令后，设备会返回位置坐标。

  用户示例：当您部署位置策略且设备上启用了 GPS 时：如果用户放错了设备，他们可以登录 Citrix Endpoint Management 自助服务门户并选择定位选项，以在地图上查看其设备位置。用户选择是否允许 Citrix Secure Hub 使用位置服务。当用户自行注册设备时，您无法强制使用位置服务。使用此策略的另一个考虑因素是对电池续航时间的影响。

- **密码策略**

为何使用此策略：密码策略允许您在托管设备上强制执行 PIN 码或密码。此密码策略允许您设置设备上密码的复杂性和超时时间。

用户示例：当您向托管设备部署密码策略时，Citrix Secure Hub 会提示用户配置密码或 PIN。密码或 PIN 码允许用户在启动时或不活动计时器到期时访问其设备。

- **配置文件删除策略**

  为何使用此策略：假设您向一组用户部署了一个策略，但后来必须从这些用户的一个子集中删除该策略。您可以通过创建配置文件删除策略来为选定用户删除该策略。然后，使用部署规则将配置文件删除策略仅部署到指定用户。

  用户示例： 当您向用户设备部署配置文件删除策略时，用户可能不会注意到此更改。例如，如果配置文件删除策略删除了禁用设备摄像头的限制，则用户不会知道此更改。请考虑在更改影响用户体验时通知用户。

- **限制策略**

  为何使用此策略： 限制策略为您提供了许多选项，用于锁定和控制托管设备上的功能。您可以为受支持的设备启用数百个限制选项。例如，您可以：禁用设备上的摄像头或麦克风、强制执行漫游规则以及强制访问第三方服务（如应用商店）。

  用户示例： 如果您向 iOS 设备部署限制，用户可能无法访问 iCloud 或 Apple App Store。

- **条款和条件策略**

  为何使用此策略： 可能需要告知用户其设备受管理的法律影响。此外，您可能希望确保用户了解将公司数据推送到设备时的安全风险。《条款和条件》文档允许您在用户注册之前发布规则和通知。

  用户示例： 用户在注册过程中会看到“条款和条件”信息。如果他们拒绝接受所述条件，则注册过程将结束，他们将无法访问公司数据。您可以生成报告提供给 HR/法律/合规团队，以显示谁接受或拒绝了这些条款。

- **VPN 策略**

  为何使用此策略： 使用 VPN 策略通过旧版 VPN 网关技术提供对后端系统的访问。此策略支持各种 VPN 提供商，包括 Cisco AnyConnect、Juniper 和 Citrix VPN。如果 VPN 网关支持此选项，还可以将此策略链接到 CA 并启用按需 VPN。

  用户示例： 启用 VPN 策略后，当用户访问内部域时，用户的设备会打开 VPN 连接。

- **Web 剪辑策略**

为何使用此策略： 如果您希望向设备推送一个直接打开网站的图标，请使用 Web 剪辑策略。Web 剪辑包含指向网站的链接，并且可以包含自定义图标。在设备上，Web 剪辑看起来像一个应用程序图标。

用户示例： 用户可以单击 Web 剪辑图标以打开 Internet 站点，从而访问所需服务。使用 Web 链接比在浏览器中键入链接地址更方便。

- **网络策略**

  为何使用此策略： 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）部署到托管设备。

  用户示例：当您部署网络策略时，设备会自动连接到 Wi-Fi 网络并对用户进行身份验证，以便他们可以访问网络。

- **Endpoint Management 应用商店策略**

  为何使用此策略：应用商店是一个统一的应用商店，管理员可以在其中发布用户所需的所有企业应用和数据资源。管理员可以添加：

  - Web 应用、SaaS 应用、以及启用 MAM SDK 的应用或 MDX 封装的应用
  - Citrix 移动生产力应用
  - 本机移动应用，例如 .ipa 或 .apk 文件
  - 苹果应用商店和 Google Play 应用
  - 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 Citrix Endpoint Management 后，他们可以通过 Citrix Secure Hub 应用访问应用商店。用户可以查看所有可用的企业应用和服务。用户可以单击某个应用进行安装、访问数据、对应用进行评分和评论，并从应用商店下载应用更新。

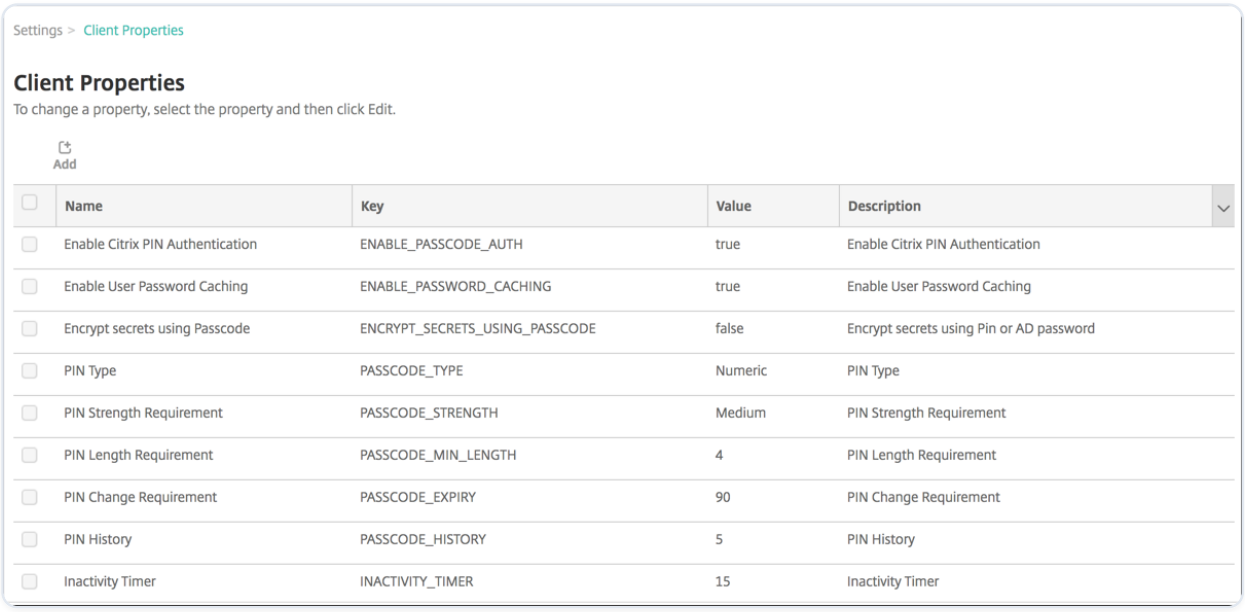
客户端属性

客户端属性包含直接提供给用户设备上的 Citrix Secure Hub 的信息。您可以使用这些属性来配置高级设置，例如 Citrix PIN。您可以从 Citrix 支持获取客户端属性。

客户端属性可能会随 Citrix Secure Hub 的每个版本更改，有时也会随客户端应用程序更改。有关更常用客户端属性的详细信息，请参阅本文后面的客户端属性参考。

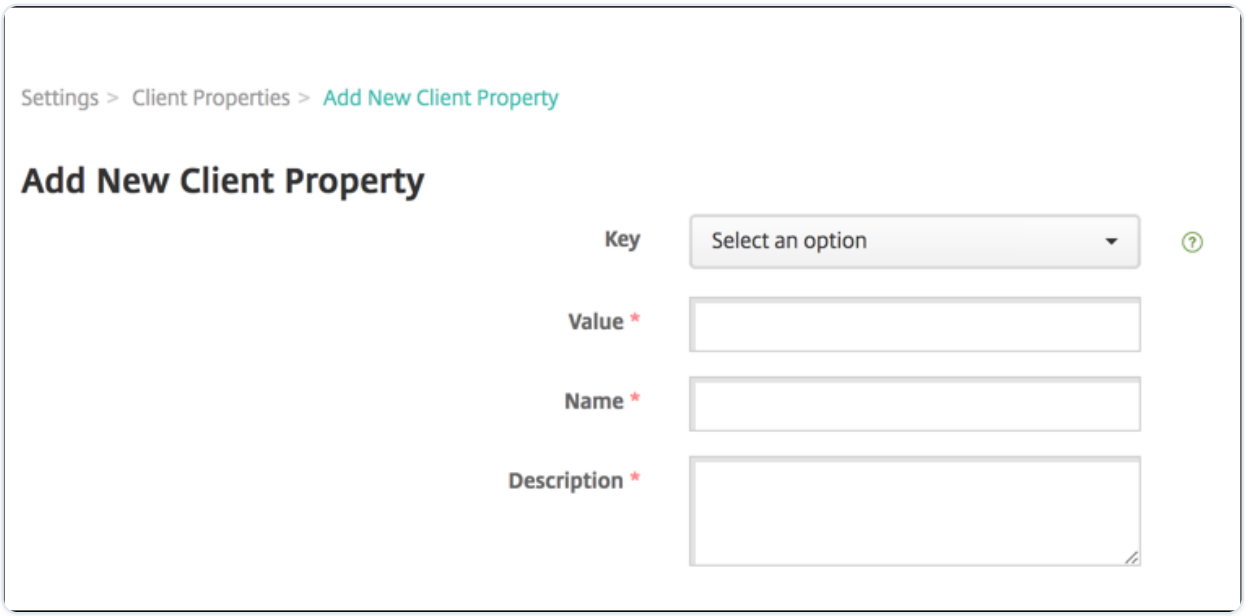
1. 在 Citrix Endpoint Management 控制台中，单击右上角的齿轮图标。此时将显示“**设置**”页面。

2. 在“**客户端**”下，单击“**客户端属性**”。此时将显示“**客户端属性**”页面。您可以从此页面添加、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：

- **密钥：** 从下拉列表中单击要添加的属性密钥。**重要提示：** 在更新设置之前，请联系 Citrix 支持。您可以请求一个特殊密钥。
- **值：** 所选属性的值。
- **名称：** 属性的名称。
- **说明：** 属性的说明。

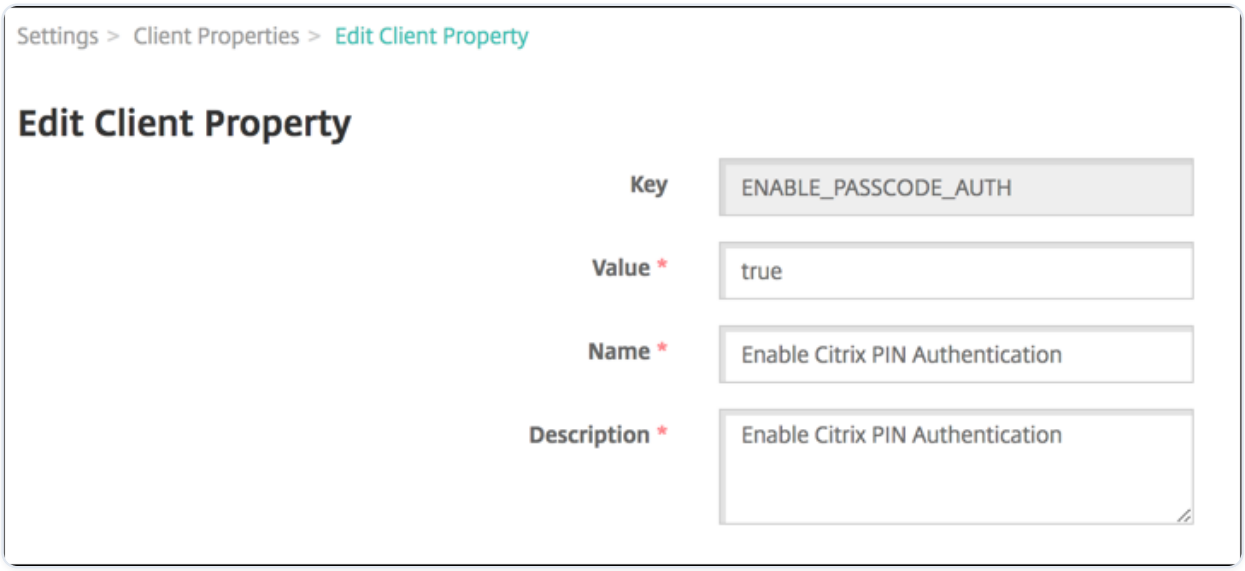
3. 单击“**保存**”。

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以打开列表右侧的选项菜单。

2. 单击**编辑**。此时将显示**编辑客户端属性**页面。



3. 根据需要更改以下信息：

   - **密钥：**您无法更改此字段。
   - **值：**属性值。
   - **名称：**属性名称。
   - **描述：**属性描述。

4. 单击**保存**以保存更改，或单击**取消**以使属性保持不变。

删除客户端属性

1. 在**客户端属性**表中，选择要删除的客户端属性。

   通过选中每个属性旁边的复选框，可以选择多个属性进行删除。

2. 单击**删除**。此时将显示确认对话框。再次单击**删除**。

客户端属性参考

Citrix Endpoint Management 的预定义客户端属性及其默认设置如下：

- **ALLOW_CLIENTSIDE_PROXY**
  - 显示名称：ALLOW_CLIENTSIDE_PROXY
  - 如果您的用户想要使用他们在 iOS 手机上配置的代理，请将此自定义策略设置为默认值 **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 Citrix Secure Hub 未为这些用户打开，请执行以下操作之一：
    - 从设备中删除代理配置，然后重新启动 Citrix Secure Hub。
    - 将设备连接到另一个 Wi-Fi 网络。Citrix 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** 为 **false** 且用户在其设备上配置了代理，则 Citrix Endpoint Management 会检测到该代理。但是，Citrix Secure Hub 不会使用该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，则 Citrix Endpoint Management 不会检测到该代理。为了获得最高安全性，我们建议您使用证书锁定。有关为 Citrix Secure Hub 启用证书锁定的信息，请参阅证书锁定。
  - 要配置此自定义客户端策略，请转至 **“设置”>“客户端属性”**，添加自定义密钥 **ALLOW_CLIENTSIDE_PROXY**，然后设置 **“值”**。
- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 显示名称：MDX 容器自毁期限
  - 自毁功能可在指定天数的不活动后阻止访问 Citrix Secure Hub 和托管应用程序。超过时间限制后，应用程序将无法使用。擦除数据包括清除每个已安装应用程序的应用程序数据，包括应用程序缓存和用户数据。

    不活动时间是指服务器在特定时间长度内未收到用于验证用户的身份验证请求。假设此属性为 30 天。如果用户超过 30 天未使用该应用程序，则该策略将生效。

    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，请转到 **设置 > 客户端属性** 并添加自定义密钥 **CONTAINER_SELF_DESTRUCT_PERIOD**。
  - 值：天数
- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - 显示名称：将设备日志发送到 IT 帮助台
  - 此属性启用或禁用向 IT 帮助台发送日志的功能。

  - 可能的值：**true** 或 **false**
  - 默认值：**false**

- **DISABLE_LOGGING**
  - 显示名称：禁用日志记录
  - 使用此属性可阻止用户从其设备收集和上传日志。此属性会禁用 Citrix Secure Hub 和所有已安装的 MDX 应用程序的日志记录。用户无法从“支持”页面发送任何应用程序的日志。即使显示邮件撰写对话框，日志也不会附加。一条消息指示日志记录已禁用。此设置还会阻止您在 Citrix Endpoint Management 控制台中更新 Citrix Secure Hub 和 MDX 应用程序的日志设置。

    当此属性设置为 **true** 时，Citrix Secure Hub 会将 **阻止应用程序日志** 设置为 **true**。因此，当应用新策略时，MDX 应用程序将停止日志记录。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**（未禁用日志记录）

- **ENABLE_CRASH_REPORTING**
  - 显示名称：启用崩溃报告
  - 如果为 **true**，Citrix 将收集崩溃报告和诊断信息，以帮助排查适用于 iOS 和 Android 的 Citrix Secure Hub 的问题。如果为 **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
  - 启用凭据存储意味着 Android 或 iOS 用户在访问 Citrix 移动生产力应用程序时只需输入一次密码。无论是否启用 Citrix PIN，您都可以使用凭据存储。如果您未启用 Citrix PIN，用户将输入其 Active Directory 密码。Citrix Endpoint Management 仅支持将 Active Directory 密码与凭据存储结合用于 Citrix Secure Hub 和公共应用商店应用程序。如果您将 Active Directory 密码与凭据存储结合使用，Citrix Endpoint Management 不支持 PKI 身份验证。
  - 要在 Citrix 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 **Settings > Client Properties**，添加自定义密钥 **ENABLE_CREDENTIAL_STORE**，并将 **Value** 设置为 **true**。

- **ENABLE_PASSCODE_AUTH**

- 显示名称：启用 Citrix PIN 身份验证
- 此属性允许您启用 Citrix PIN 功能。通过 Citrix PIN 或密码，系统会提示用户定义一个 PIN，以代替其 Active Directory 密码使用。当 ENABLE_PASSWORD_CACHING 启用或 Citrix Endpoint Management 使用证书身份验证时，此设置会自动启用。

  对于离线身份验证，Citrix PIN 在本地进行验证，用户可以访问其请求的应用程序或内容。对于在线身份验证，Citrix PIN 或密码会解锁 Active Directory 密码或证书，然后将其发送给 Citrix Endpoint Management 进行身份验证。

  如果 ENABLE_PASSCODE_AUTH 为 true 且 ENABLE_PASSWORD_CACHING 为 false，则在线身份验证始终会提示输入密码，因为 Citrix Secure Hub 不会保存密码。
- 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
  - 此属性允许 Active Directory 密码在移动设备上本地缓存。当您将此属性设置为 **true** 时，还必须将 **ENABLE_PASSCODE_AUTH** 属性设置为 **true**。启用用户密码缓存后，Citrix Endpoint Management 会提示用户设置 Citrix PIN 或密码。
  - 可能的值: **true** 或 **false**
  - 默认值: **false**
- **ENABLE_TOUCH_ID_AUTH**
  - 显示名称: 启用触控 ID 身份验证
  - 对于支持触控 ID 身份验证的设备，此属性可启用或禁用设备上的触控 ID 身份验证。要求:

    用户设备必须启用 Citrix PIN 或 LDAP。如果 LDAP 身份验证已关闭（例如，因为仅使用基于证书的身份验证），用户必须设置 Citrix PIN。在这种情况下，即使客户端属性 **ENABLE_PASSCODE_AUTH** 为 **false**，Citrix Endpoint Management 也需要 Citrix PIN。

    将 **ENABLE_PASSCODE_AUTH** 设置为 **false**，以便当用户启动应用程序时，他们必须响应提示才能使用触控 ID。
  - 可能的值: **true** 或 **false**
  - 默认值: **false**
- **ENABLE_WORXHOME_CEIP**

- 显示名称: 启用 Citrix Secure Hub CEIP
- 此属性启用客户体验改善计划。该功能会定期向 Citrix 发送匿名配置和使用数据。这些数据有助于 Citrix 提高 Citrix Endpoint Management 的质量、可靠性和性能。
- 值：**true** 或 **false**
- 默认值：**false**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 显示名称：使用密码加密机密
  - 此属性将敏感数据存储在设备上的秘密保管库中，而不是存储在基于平台的本机存储（例如 iOS 钥匙串）中。此属性可对关键工件进行强加密并添加用户熵。用户熵是只有用户知道的用户生成的随机 PIN 码。

    Citrix 建议您启用此属性，以帮助提高用户设备上的安全性。因此，用户会收到更多 Citrix PIN 身份验证提示。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **INACTIVITY_TIMER**
  - 显示名称：不活动计时器
  - 此属性定义了用户可以将设备置于不活动状态多长时间，然后无需提示 Citrix PIN 或密码即可访问应用程序。要为 MDX 应用程序启用此设置，请将“应用程序密码”设置设为“开”。如果“应用程序密码”设置设为“关”，则用户将被重定向到 Citrix Secure Hub 以进行完全身份验证。更改此设置后，该值将在用户下次收到身份验证提示时生效。

    在 iOS 上，“不活动计时器”还控制 MDX 和非 MDX 应用程序对 Citrix Secure Hub 的访问。
  - 可能的值：任何正整数
  - 默认值：**15**（分钟）
- **ON_FAILURE_USE_EMAIL**
  - 显示名称：失败时使用电子邮件将设备日志发送到 IT 帮助台
  - 此属性启用或禁用使用电子邮件将设备日志发送给 IT 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 或密码的有效期，过期后用户将被强制更改其 Citrix PIN 或密码。更改此设置时，新值仅在当前 Citrix PIN 或密码过期时设置。
- 可能的值：建议 **1** 到 **99**。要消除 PIN 重置，请将值设置为一个较大的数字（例如，100,000,000,000）。如果您最初将有效期设置为 1 到 99 天之间，然后在此期间更改为较大的数字：PIN 仍会在初始期限结束时过期，但之后不会再过期。
- 默认值：**90**（天）

- **PASSCODE_HISTORY**
  - 显示名称：PIN 历史记录
  - 此属性定义用户在更改 Citrix PIN 或密码时不能重复使用的先前 Citrix PIN 或密码的数量。更改此设置时，新值将在用户下次重置其 Citrix PIN 或密码时设置。
  - 可能的值：**1** 到 **99**
  - 默认值：**5**
- **PASSCODE_MAX_ATTEMPTS**
  - 显示名称: PIN 尝试次数
  - 此属性定义用户在被提示进行完整身份验证之前可以进行多少次错误的 Citrix PIN 或密码尝试。用户成功完成完整身份验证后，系统会提示他们创建 Citrix PIN 或密码。
  - 可能的值: 任何正整数
  - 默认值: **15**
- **PASSCODE_MIN_LENGTH**
  - 显示名称: PIN 长度要求
  - 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 或密码的强度。更改此设置后，下次提示用户进行身份验证时，系统会提示他们创建 Citrix PIN 或密码。
  - 可能的值: **低**、**中**、**高**或**强**

- 默认值: **中**
- 基于 PASSCODE_TYPE 设置的每个强度设置的密码规则如下所示:

数字密码的规则：

密码强度	数字密码类型的规则	允许	不允许
低	所有数字，允许任何序列	444444, 123456, 654321	
中（默认设置）	所有数字不能相同或连续。	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
高	相邻数字不能相同。	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
强	不要使用相同的数字超过两次。不要使用三个或更多连续的数字。不要使用三个或更多反向连续的数字。	102983, 085085, 824673, 132312	132132, 131313, 902030

字母数字密码规则：

密码强度	字母数字密码类型规则	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
中（默认设置）	除了低密码强度规则外，字母和所有数字不能相同。字母不能连续，数字也不能连续。	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, 或 aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, 或 cba123
高	至少包含一个大写字母和一个小写字母。	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2

密码强度	字母数字密码类型规则	允许	不允许
强	至少包含一个数字、一个特殊符号、一个大写字母和一个小写字母。	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **密码类型**
  - 显示名称：PIN 类型
  - 此属性定义用户是可以使用数字 Citrix PIN 还是字母数字密码。当您选择**数字**时，用户只能使用数字 (Citrix PIN)。当您选择**字母数字**时，用户可以使用字母和数字的组合（密码）。

    如果您更改此设置，用户在下次系统提示其进行身份验证时必须设置新的 Citrix PIN 或密码。
  - 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，Citrix Endpoint Management 每 3 天 ping 一次自动发现服务器 (ADS) 以获取固定的证书。要更改刷新间隔，请转到**设置 > 客户端属性**，添加自定义密钥 **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：您可以将 Citrix Endpoint Management 配置为，使用电子邮件凭据注册 Citrix Secure Hub 的用户将自动注册 Citrix Secure Mail。因此，用户无需提供额外信息或采取额外步骤即可注册 Citrix Secure Mail。
  - 要配置此全局客户端策略，请转到**设置 > 客户端属性**，添加自定义密钥 **SEND_LDAP_ATTRIBUTES**，并按如下方式设置**值**。
  - 值：`userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}`
  - 属性值被指定为宏，类似于 MDM 策略。
  - 以下是此属性的示例帐户服务响应：

```
<property
value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,em
name="SEND_LDAP_ATTRIBUTES"/>
```

  - 对于此属性，Citrix Endpoint Management 将逗号字符视为字符串终止符。因此，如果属性值包含逗号，请在其前面加上反斜杠。反斜杠可防止客户端将嵌入的逗号解释为属性值的结尾。使用 `"\\"` 表示反斜杠字符。

- **HIDE_THREE_FINGER_TAP_MENU**
  - 当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触来访问隐藏功能菜单。隐藏功能菜单允许用户重置应用程序数据。将此属性设置为 **true** 会禁用用户对隐藏功能菜单的访问。
  - 要配置此全局客户端策略，请转至 **Settings > Client Properties**，添加自定义密钥 **HIDE_THREE_FINGER_TAP_MENU** 并设置 **Value**。
- **TUNNEL_EXCLUDE_DOMAINS**
  - 显示名称：隧道排除域
  - 默认情况下，MDX 会从微 VPN 隧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终结点。例如，这些终结点包括不需要通过企业网络路由的服务，例如 Google Analytics、Citrix Cloud™ 服务和 Active Directory 服务。使用此客户端属性可将其他域添加到排除域列表中。
  - 要配置此全局客户端策略，请转至 **Settings > Client Properties**，添加自定义密钥 **TUNNEL_EXCLUDE_DOMAINS** 并设置 **Value**。
  - 值：要从隧道中排除的其他域，请键入一个逗号分隔的域后缀列表。例如：

```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-
test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.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,features.netscalergatewaystaging.net,features.r
```

Citrix Endpoint Management 的自定义客户端属性如下：

ENABLE_MAM_NFACTOR_SSO:

- 此属性允许您在使用 NetScaler® Gateway 中的高级身份验证策略时，在 Secure Hub 的 MAM 注册或登录期间启用或禁用 MAM nFactor SSO。如果值设置为 **true**，则在 Secure Hub 的 MAM 注册或登录期间启用 MAM nFactor SSO。

- 要配置此属性，请转至 **Settings > Client Properties** 并单击 **Add**。在 **Key** 下拉菜单中选择 **Custom Key** 并酌情更新以下信息：
  - 密钥 - ENABLE_MAM_NFACTOR_SSO
  - 值 - true 或 false
  - 名称 - ENABLE_MAM_NFACTOR_SSO
  - 描述 - 添加相关描述

MICROSOFT_CERTIFICATE_STRONG_MAPPING：

- 此属性控制在使用 Secure Mail 和 Microsoft 公钥基础结构 (PKI) 时，是否通过将安全标识符 (SID) 附加到主题备用名称 (SAN) 来续订现有客户端证书，以支持证书强映射功能。如果值设置为 **true**，则现有客户端证书将续订以包含 SAN SID。
- 此属性仅适用于 Microsoft PKI。
- 要配置此属性，请转到“**设置 > 客户端属性**”，然后单击“**添加**”。在“**密钥**”下拉菜单中选择“**自定义密钥**”，并根据需要更新以下信息：
  - 密钥 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - 值 - true 或 false
  - 名称 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - 描述 - 续订客户端证书以包含 SAN SID

aeDeviceCertRenewSupport：

- 此属性控制最终用户是否可以从 Citrix Secure Hub 应用程序查看设备证书运行状况并自动修复证书问题。如果值设置为 **true**，则启用此功能。
- 要配置此属性，请转到“**设置 > 客户端属性**”，然后单击“**添加**”。在“**密钥**”下拉菜单中选择“**自定义密钥**”，并根据需要更新以下信息：
  - 密钥 - aeDeviceCertRenewSupport
  - 值 - true 或 false
  - 名称 - aeDeviceCertRenewSupport
  - 描述 - 启用设备证书健康状态和自动修复证书问题

用户注册选项

您可以通过多种方式让用户将其设备注册到 Citrix Endpoint Management。在考虑具体细节之前，请确定要将哪些设备注册到 MDM+MAM、MDM 或 MAM。有关这些管理模式的更多信息，请参阅管理模式。

在最高级别，有四种注册选项：

- **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。
- **自助服务门户：** 设置一个门户，用户可以访问该门户以下载 Citrix Secure Hub、请求注册和查看设备信息。
- **手动注册：** 发送电子邮件、手册或其他通信，告知用户系统已启动，他们可以注册。然后，用户下载 Citrix Secure Hub 并手动注册其设备。
- **企业：** 设备注册的另一个选项是通过 Apple 部署计划和 Google Android Enterprise。通过这些计划，您可以购买预配置好并可供员工使用的设备。有关详细信息，请参阅 Apple 支持 中的 Apple 部署计划文章和 Android Enterprise 网站 上的 Google Android Enterprise 文档。

注册邀请

您可以向使用 iOS、macOS、Android Enterprise 和旧版 Android 设备的用户发送注册邀请电子邮件。注册邀请不适用于 Windows 设备。

您还可以通过 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。

如果您选择使用注册邀请方法，则可以执行以下操作：

- 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。
- 在 Citrix Endpoint Management 的**设置**页面中启用或禁用这些模式。

有关每个注册安全模式的信息，请参阅配置注册安全模式。

邀请函有多种用途。邀请函最常见的用途是通知用户系统可用，并且他们可以注册。邀请 URL 是唯一的。用户使用邀请 URL 后，该 URL 将不再可用。您可以使用此属性来限制注册到您系统的用户或设备。

配置注册配置文件时，您可以根据 Active Directory 组控制特定用户可以注册的设备数量。例如，您可能只允许财务部门的每个用户注册一台设备。

请注意某些注册选项的额外成本和潜在问题。使用 SMTP 发送邀请需要额外的基础设施。有关此选项的更多信息，请参阅通知。

此外，要通过电子邮件发送邀请，请确保用户可以在 Citrix Secure Hub 之外访问电子邮件。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 密码的替代方案。

自助服务门户

自助服务门户可以通过管理员用于访问 Citrix Endpoint Management 控制台的相同 URL 进行访问。最终用户看到的是自助服务门户，而不是管理控制台。用户可以在自助服务门户中下载 Citrix Secure Hub、请求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。
- `enable.new.shp`：设置为 **True** 以允许用户从自助服务门户启用其设备。

手动注册

通过手动注册，用户可以通过 AutoDiscovery 或输入服务器信息连接到 Citrix Endpoint Management。使用 AutoDiscovery 时，用户只需使用其电子邮件地址或用户主体名称格式的 Active Directory 凭据登录。如果没有 AutoDiscovery，他们必须输入服务器地址和其 Active Directory 凭据。有关设置 AutoDiscovery 的更多信息，请参阅设置 Citrix Endpoint Management AutoDiscovery 服务。

您可以通过多种方式促进手动注册。您可以创建指南，分发给用户，让他们自行注册。您可以让 IT 部门在特定时间段内手动注册用户组。您可以使用任何类似的方法，让用户输入其凭据或服务器信息。

用户入职

设置好环境后，您需要决定如何将用户引入您的环境。本文前面部分讨论了用户注册安全模式的具体细节。本节讨论您联系用户的方式。

开放注册与选择性邀请

在用户入职时，您可以通过两种基本方法允许注册：

- 开放注册。默认情况下，任何拥有 LDAP 凭据和 Citrix Endpoint Management 环境信息的用户都可以注册。
- 受限注册。您可以通过仅允许受邀用户注册来限制用户数量。您还可以通过 Active Directory 组来限制开放注册。

通过邀请方式，您还可以限制用户可以注册的设备数量。在大多数情况下，开放注册是可以接受的，但有几点需要考虑：

- 对于 MAM 注册，您可以通过 Active Directory 组成员身份轻松限制开放注册。

- 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量。如果您的环境中只允许公司设备，则此限制通常不是问题。但是，如果您想限制环境中设备的数量，则在 BYOD 工作场所中可能需要考虑此方法。

选择性邀请通常较少使用，因为它比开放注册需要更多的工作。要让用户在其环境中注册设备，您必须向每个用户发送唯一的邀请。有关如何发送注册邀请的信息，请参阅注册邀请。

为您希望在其环境中注册的每个用户或组发送邀请。此过程可能需要很长时间，具体取决于您的组织规模。可以使用 Active Directory 组批量创建邀请，但您必须分批执行此方法。

首次联系用户

在决定使用开放注册还是选择性邀请并设置好这些环境后，请告知用户其注册选项。

如果您使用选择性邀请方法，电子邮件是该过程的一部分。您也可以通过 Citrix Endpoint Management 控制台发送电子邮件进行开放注册。有关详细信息，请参阅注册邀请。

无论哪种情况，请记住，对于电子邮件，您需要一个 SMTP 服务器。在做出决定时，这些服务器可能需要考虑额外的成本。考虑您希望新用户如何访问信息。如果您希望所有用户通过 Citrix Endpoint Management 访问其电子邮件，则向他们发送邀请电子邮件可能会有问题。

您还可以通过 Citrix Endpoint Management 之外的其他方式为开放注册环境发送通信。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在哪里获取 Citrix Secure Hub 应用程序以及使用哪种方法进行注册。如果已关闭发现功能，还要向用户提供 Citrix Endpoint Management 服务器地址。要了解有关发现的更多信息，请参阅设置 Citrix Endpoint Management 自动发现服务。

应用程序预配和取消预配

应用程序预配围绕移动应用程序生命周期管理展开：在 Citrix Endpoint Management 环境中准备、配置、交付和管理移动应用程序。有时，开发或修改应用程序代码也可能是预配过程的一部分。Citrix Endpoint Management 配备了可用于应用程序预配的各种工具和流程。

在阅读这篇关于应用程序预配的文章之前，我们建议您阅读 应用程序 和 用户社区。当您确定了组织计划向用户交付的应用程序类型后，您就可以概述在整个生命周期中管理这些应用程序的过程。

定义应用程序预配过程时，请考虑以下几点：

- **应用程序分析：** 您的组织可能从少量应用程序开始。但是，随着用户采用率的提高和环境的增长，您管理的应用程序数量可能会迅速增加。预先定义特定的应用程序配置文件，以便于管理应用程序预配。应用程序分析有助于您从非技术角度将应用程序分类到逻辑组中。例如，您可以根据以下因素创建应用程序配置文件：
    - 版本：用于跟踪的应用程序版本

- 实例：为不同用户组部署的多个实例，例如，具有不同访问级别
- 平台：iOS、Android 或 Windows
- 目标受众：标准用户、部门、C 级高管
- 所有权：拥有该应用程序的部门
- 类型：MDX、公共、Web 和 SaaS 或 Web 链接
- 升级周期：应用程序升级的频率
- 许可：许可要求和所有权
- MAM SDK 或 MDX 策略：将 MDX 功能应用于您的移动应用程序
- 网络访问：访问类型，例如，通过单一登录隧道传输 HTTP 和 HTTPS 流量（隧道 - Web SSO）。

示例：

因素	CITRIX 安全邮件	邮件	内部	埃匹克 罗孚
版本	10.1	10.1	X.x	X.x
实例	VIP	医生	临床	临床
平台	iOS	iOS	iOS	iOS
目标用户	VIP 用户	医生	临床用户	临床用户
所有权	IT	IT	IT	IT
类型	MDX	MDX	原生	公共
升级周期	季度	季度	年度	不适用
授权	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	公共

- **应用版本控制：** 维护和跟踪应用版本是预配过程的关键部分。版本控制对用户通常是透明的。他们只会在有新版本应用可供下载时收到通知。从您的角度来看，在非生产环境中审查和测试每个应用版本也至关重要，以避免影响生产站点。

评估是否需要特定升级也很重要。应用升级通常有两种类型：次要升级（例如修复特定错误）或主要版本发布（引入重大更改）。无论哪种情况，都请仔细查看应用的发行说明，以评估升级是否必要。

- **应用开发：** 当您将 MAM SDK 集成到您开发的移动应用中时，您将 MDX 功能应用于这些应用。请参阅 MAM SDK 概述。

  MAM SDK 将取代 MDX Toolkit，后者计划于 2023 年 7 月弃用。有关应用打包的信息，请参阅 MDX Toolkit。打包应用的应用预配过程与标准非打包应用的应用预配过程不同。

- **应用安全性：** 您可以在预配过程中定义单个应用或应用配置文件的安全要求。在部署应用之前，您可以将安全要求映射到特定的 MDM 或 MAM 策略。这种规划简化并加快了应用部署。例如：

  - 您可能以不同的方式部署某些应用。
  - 您可能希望对 Citrix Endpoint Management 环境进行架构更改。这些更改取决于应用所需的安全合规性类型。例如，某个特定应用可能需要端到端 SSL 加密或地理围栏。

- **应用交付：** Citrix Endpoint Management 允许您将应用作为 MDM 应用或 MAM 应用进行交付。MDM 应用会显示在应用商店中。此商店允许您方便地向用户交付公共应用或本机应用。除了强制执行设备级别限制外，不需要其他应用控制。但是，使用 MAM 交付应用可以完全控制应用交付和应用本身。通过 MAM 交付应用通常更合适。

- **应用维护：**

  - 进行初步审计：跟踪生产环境中存在的应用版本以及上次升级周期。记录需要进行升级的特定功能或错误修复。
  - 建立基线：维护每个应用的最新稳定版本列表。如果升级后出现意外问题，请准备好回滚到较早的应用版本。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升级。如果可能，请先将升级部署到部分生产用户，然后再部署到所有用户。
  - 订阅 Citrix® 软件更新通知和任何第三方软件供应商通知：及时了解应用的最新版本至关重要。早期访问版本 (EAR) 可能提前提供用于测试。
  - 制定通知用户的策略：定义当应用升级可用时通知用户的策略。在部署前对用户进行培训。在更新应用之前，考虑发送多个通知。根据应用的不同，最佳通知方法可能是电子邮件通知或网站。

应用生命周期管理涵盖了应用从初始部署到停用的整个生命周期。应用的生命周期包括以下阶段：

1. 规范要求：从业务案例和用户要求开始。
2. 开发：验证应用是否满足业务需求。
3. 测试：识别测试用户、问题和错误。

4. 部署：将应用部署到生产用户。
5. 维护：更新应用版本。在生产环境中更新应用之前，在测试环境中部署应用。

基于控制面板的操作

通过访问您的 Citrix Endpoint Management 控制台控制面板，您可以一目了然地查看信息。利用此信息，您可以使用小组件快速查看问题和成功之处。

控制面板通常是您首次登录 Citrix Endpoint Management 控制台时出现的屏幕。要从控制台的其他位置访问控制面板，请单击 **Analyze**。单击控制面板上的 **Customize** 以编辑页面布局和编辑显示的小组件。

- **我的控制面板：** 您最多可以保存四个控制面板。您可以单独编辑这些控制面板，并通过选择已保存的控制面板来查看每个控制面板。
- **布局样式：** 在此行中，您可以选择控制面板上显示的小组件数量以及小组件的布局方式。
- **小组件选择：** 您可以选择控制面板上显示的信息。
    - **通知：** 勾选左侧数字上方的复选框，可在小组件上方添加一个通知栏。此栏显示合规设备、非活动设备以及在过去 24 小时内擦除或注册的设备数量。
    - **按平台划分的设备：** 按平台显示托管和非托管设备的数量。
    - **按运营商划分的设备：** 按运营商显示托管和非托管设备的数量。单击每个条形图可按平台查看详细信息。
    - **按平台划分的托管设备：** 按平台显示托管设备的数量。
    - **按平台划分的非托管设备：** 按平台显示非托管设备的数量。此图表中显示的设备可能已安装代理，但其权限已被撤销或已被擦除。
    - **按 ActiveSync 网关状态划分的设备：** 显示按 ActiveSync 网关状态分组的设备数量。信息显示“已阻止”、“已允许”或“未知”状态。您可以单击每个条形图以按平台细分数据。
    - **按所有权划分的设备：** 显示按所有权状态分组的设备数量。信息显示“公司所有”、“员工所有”或“未知所有权”状态。
    - **失败的交付组部署：** 显示每个软件包的失败部署总数。仅显示部署失败的软件包。
    - **按阻止原因划分的设备：** 显示 ActiveSync 阻止的设备数量
    - **已安装应用：** 通过使用此小组件，您可以键入应用程序名称，图表将显示有关该应用程序的信息。
    - **批量购买应用许可证使用情况：** 显示 Apple 批量购买应用的许可证使用情况统计信息。

用例

以下是您可以使用仪表板小组件监控环境的多种方式的一些示例。

- 您已部署 Citrix 移动生产力应用程序，并收到有关移动生产力应用程序无法安装在设备上的支持票证。使用**不合规设备**和**已安装应用**小组件查看未安装 Citrix 移动生产力应用程序的设备。
- 您希望监控非活动设备，以便可以从环境中移除这些设备并回收许可证。使用**非活动设备**小组件跟踪此统计信息。
- 您收到有关数据未正确同步的支持票证。您可能希望使用**按 ActiveSync 网关状态列出的设备**和**按阻止原因列出的设备**小组件来确定问题是否与 ActiveSync 相关。

报告

设置好环境并注册用户后，您可以运行报告以了解部署情况。Citrix Endpoint Management 内置了各种报告，可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 Citrix Endpoint Management 支持

Citrix Endpoint Management 使用基于角色的访问控制 (RBAC) 来限制用户和组对 Citrix Endpoint Management 系统功能（例如 Citrix Endpoint Management 控制台、自助服务门户和公共 API）的访问。本文介绍了 Citrix Endpoint Management 中内置的角色，并提供了有关为使用 RBAC 的 Citrix Endpoint Management 确定支持模型的注意事项。

内置角色

您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。有关与每个角色及其默认设置关联的完整访问和功能权限集，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。

管理员角色

默认授予的访问权限：

- 除自助服务门户外，拥有完整的系统访问权限。
- 默认情况下，管理员可以执行一些支持任务，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，您可以编辑管理员角色或添加管理员角色。
- 要进一步限制某些管理员或管理员组的访问权限，请基于管理员模板添加角色并编辑权限。

用户

默认授予的访问权限：

- 访问自助服务门户，允许经过身份验证的用户生成注册链接。这些链接允许他们注册设备或向自己发送注册邀请。
- 对 思杰端点管理控制台 的受限访问：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；使设备响铃；重置容器密码）；添加、删除和发送注册邀请。

注意事项：

- 用户角色使您能够让用户自助服务。
- 为了支持共享设备，请为共享设备注册创建一个用户角色。

Citrix Endpoint Management 支持模型的注意事项

您可以采用的支持模型可能差异很大，并且可能涉及由第三方处理 1 级和 2 级支持，而员工处理 3 级和 4 级支持。无论您如何分配支持负载，请记住本节中针对您的 Citrix Endpoint Management 部署和用户群的特定注意事项。

用户拥有公司设备还是 BYO 设备？ 影响支持的主要问题是您的 Citrix Endpoint Management 环境中用户设备的所有权。如果您的用户拥有公司设备，您可能会提供较低级别的支持，作为锁定设备的一种方式。在这种情况下，您可能会提供一个帮助台，协助用户解决设备问题以及如何使用设备。根据您需要支持的设备类型，请考虑如何为您的帮助台使用 RBAC 设备预配和支持角色。

如果您的用户拥有 BYO 设备，您的组织可能会期望用户自行寻找设备支持来源。在这种情况下，您的组织提供的支持更多是一种围绕 Citrix Endpoint Management 特定问题的管理角色。

您的桌面支持模型是什么？ 考虑您的桌面支持模型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？他们可能需要哪些额外培训？

您是否希望授予用户访问 Citrix Endpoint Management 自助服务门户的权限？ 尽管有些组织倾向于不授予用户访问 Citrix Endpoint Management 的权限，但赋予用户一些自助支持功能可以减轻您的支持组织的负担。如果 RBAC 的默认用户角色包含您不想授予的权限，请考虑创建一个仅包含您希望包含的权限的角色。您可以根据需要创建任意数量的角色以满足您的要求。

Citrix 支持流程

您可以求助于 Citrix 技术支持服务来解决与 Citrix 产品相关的问题。该团队提供变通方法和解决方案，并与开发团队紧密合作以提供解决方案。

Citrix ConsultingSM 服务或 Citrix Education 服务提供与产品培训、产品使用建议、配置、安装或环境设计和架构相关的帮助。

Citrix Consulting 协助处理与 Citrix 产品相关的项目，包括以下内容：

- 概念验证
- 经济影响评估
- 基础设施健康检查
- 设计需求分析
- 架构设计验证
- 集成
- 运营流程开发

Citrix EducationSM 提供关于 Citrix 虚拟化、云和网络技术的一流 IT 培训和认证。

Citrix 建议您在创建支持案例之前充分利用 Citrix 自助资源和建议。例如，您可以通过多种途径访问 Citrix 技术专家撰写的文章和公告，查阅 Citrix 解决方案和产品的产品文档，或者阅读 Citrix 高管、产品团队和技术专家的真知灼见。请分别参阅知识中心、产品文档和博客页面。

如需更多交互式帮助，您可以参与讨论论坛，在其中提问并从其他客户那里获得实际问题的答案；在用户组和兴趣组中分享想法、意见、技术信息和最佳实践；或者与监控 Citrix 支持社交网站的 Citrix 支持工程师互动。请分别参阅支持论坛和Citrix 社区页面。

您还可以访问培训和认证课程以提升您的技能。请参阅Citrix Education。

Citrix Insight Services 为您的 Citrix 环境提供一个简单的在线故障排除平台和健康检查器。适用于 Citrix Endpoint Management、Citrix Virtual Apps and Desktops、Citrix Hypervisor 和 NetScaler Gateway。请参阅 分析工具。

要寻求技术支持，您可以通过电话或网络创建支持案例。对于低严重性和中等严重性问题，您可以使用网络；对于高严重性问题，您可以使用电话选项。要联系 Citrix Endpoint Management 问题的支持，请参阅 Citrix 支持服务。

如果您需要一个训练有素、经验丰富的单一联系点来提供 Citrix 解决方案，Citrix Services 提供技术关系经理。有关 Citrix 服务产品和优势的更多信息，请参阅 Citrix 全球服务。

在 Citrix Endpoint Management 中发送组注册邀请

您可以在 Citrix Endpoint Management 中向组和嵌套组发送注册邀请。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。您还可以标记设备，以便例如区分公司拥有的设备和员工拥有的设备。然后，设置用户设备的身份验证类型。

> **注意：**
>
> 如果您计划使用自定义通知模板，则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 (/zh-cn/citrix-endpoint-management/users/notifications.html#create-and-update-notification-templates)。

> 有关用户帐户、角色以及注册安全模式和邀请的基本配置的详细信息，请参阅 (/zh-cn/citrix-endpoint-management/users.html)。

一般步骤

1. 在 Citrix Endpoint Management 控制台中，导航到 **Manage > Enrollment Invitations**（管理 > 注册邀请）。
2. 单击屏幕左上角的 **Add**（添加），然后单击 **Add Invitation**（添加邀请）。
3. 从 **Recipient**（收件人）菜单中单击 **Group**（组）。

   此步骤允许您选择一个或多个平台。如果您的公司混合使用不同的操作系统平台，请选择所有平台。仅当您确定没有用户使用特定平台时，才清除平台选择。
4. 您可以在邀请过程中选择标记设备。选择 **Corporate**（公司）或 **Employee**（员工）。

   标记可以轻松区分公司拥有的设备和员工拥有的设备。
5. 在 **Domain**（域）列表中，选择组所在的域。
6. 在 **Group**（组）列表中，选择要向其发送邀请的 Active Directory 组。
7. 通过**注册模式**，您可以设置用户首选的注册安全类型。

   - 用户名 + 密码
   - 高安全性
   - 邀请 URL
   - 邀请 URL + PIN
   - 邀请 URL + 密码
   - 双因素
   - 用户名 + PIN

   > **注意：**

> 我们已弃用**高安全性**注册安全模式。要发送注册邀请，您只能使用**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**、**双因素**或**用户名 + PIN** 注册的设备，用户必须下载 Citrix 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，请选择您过去创建的自定义通知模板。或者，选择列出的默认模板。

   对于这些通知模板，请使用您在 Citrix Endpoint Management 中配置的 SMTP 服务器设置。请先设置您的 SMTP 信息，然后再继续。

   > **注意：**
   >
   > **过期时间**和**最大尝试次数**选项会根据您选择的**注册模式**选项而变化。您无法更改这些选项。

9. 选择**发送邀请**的“开”，然后单击**保存并发送**以完成此过程。

嵌套组支持

您可以使用嵌套组发送邀请。通常，嵌套组用于大规模环境，其中具有相似权限的组相互绑定。

导航到 **设置 > LDAP**，然后启用 **支持嵌套组** 选项。

故障排除和已知限制

问题： 即使已从 Active Directory 组中删除用户，邀请仍会发送给他们。

解决方案： 根据您的 Active Directory 环境的大小，更改可能需要长达六小时才能传播到所有服务器。如果用户或嵌套组最近被删除，Citrix Endpoint Management 可能仍会将这些用户视为组的一部分。

因此，最好等待长达六小时，然后再向用户发送另一个组邀请。

配置本地设备健康证明服务器

您可以通过本地 Windows 服务器为 Windows 10 和 Windows 11 移动设备启用设备健康证明 (DHA)。要在本地启用 DHA，您首先需要配置 DHA 服务器。

配置 DHA 服务器后，您需要创建 Citrix Endpoint Management 策略以启用本地 DHA 服务。有关信息，请参阅 设备健康证明设备策略。

DHA 服务器的先决条件

- 运行 Windows Server Technical Preview 5 或更高版本，并使用桌面体验安装选项安装的服务器。
- 一个或多个 Windows 10 和 Windows 11 客户端设备。这些设备必须具有运行最新版本 Windows 的 TPM 1.2 或 2.0。
- 以下证书：
  - **DHA SSL 证书：** 一个 x.509 SSL 证书，链到具有可导出私钥的企业信任根。此证书保护传输中的 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：** 一个 x.509 证书，链到具有可导出私钥的企业信任根。DHA 服务使用此证书进行数字签名。
  - **DHA 加密证书：** 一个 x.509 证书，链到具有可导出私钥的企业信任根。DHA 服务也使用此证书进行加密。
- 选择以下其中一个证书验证模式：
  - **EKCert：** EKCert 验证模式针对未连接到 Internet 的组织中的设备进行了优化。连接到在 EKCert 验证模式下运行的 DHA 服务的设备无法直接访问 Internet。
  - **AIKCert：** AIKCert 验证模式针对具有 Internet 访问权限的操作环境进行了优化。连接到在 AIKCert 验证模式下运行的 DHA 服务的设备必须直接访问 Internet，并且可以从 Microsoft 获取 AIK 证书。

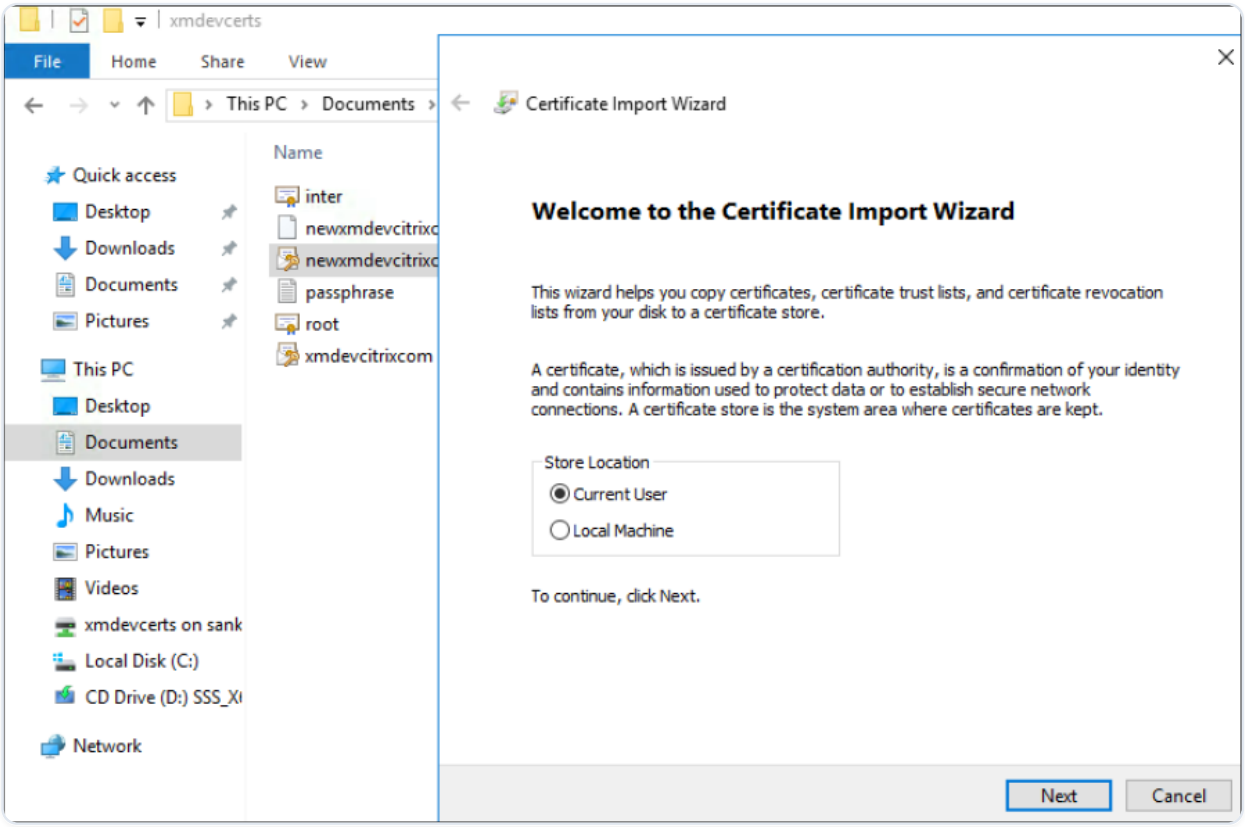
将 DHA 服务器角色添加到 Windows 服务器

1. 在 Windows 服务器上，如果服务器管理器尚未打开，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“**设备健康状况证明**”复选框。
7. 可选：单击“**添加功能**”以安装其他所需的角色服务和功能。
8. 单击“**下一步**”。
9. 在“**选择功能**”页面上，单击“**下一步**”。

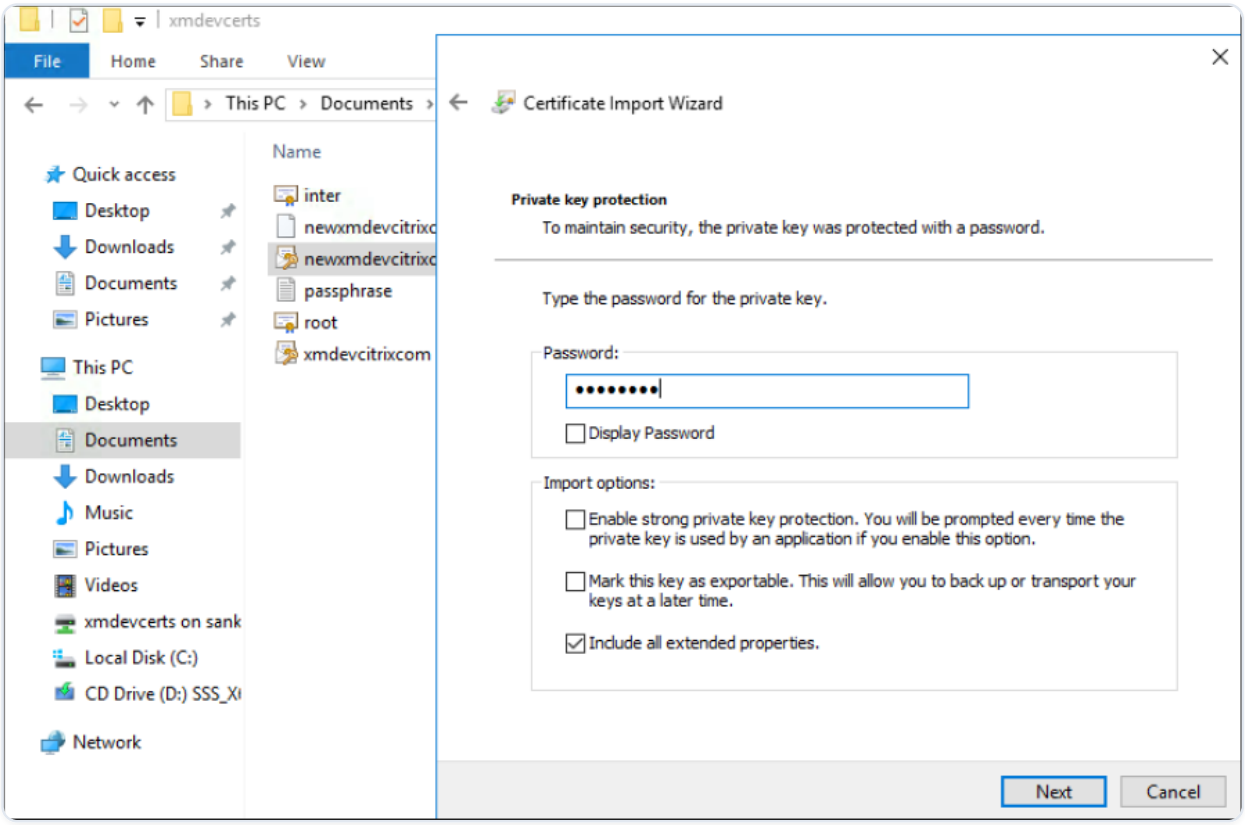
10. 在“**Web 服务器角色 (IIS)**”页面上，单击“**下一步**”。
11. 在“**选择角色服务**”页面上，单击“**下一步**”。
12. 在“**设备健康状况证明服务**”页面上，单击“**下一步**”。
13. 在“**确认安装选择**”页面上，单击“**安装**”。
14. 安装完成后，单击“**关闭**”。

将 SSL 证书添加到服务器的证书存储区

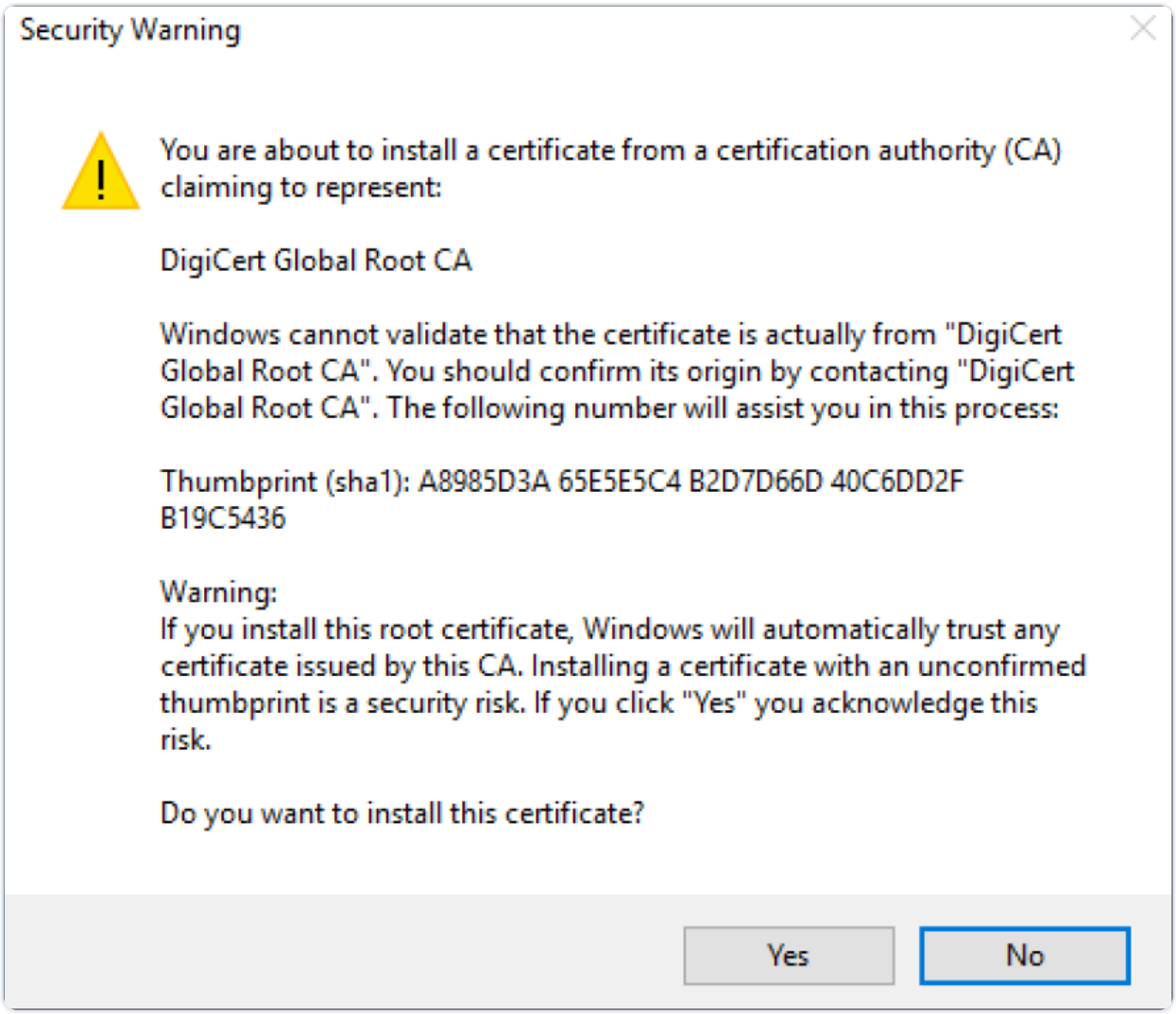
1. 转到 SSL 证书文件并选择它。
2. 对于存储位置，选择 **当前用户**，然后单击 **下一步**。



3. 键入私钥的密码。
4. 确保选中导入选项 **包括所有扩展属性**。单击 **下一步**。



5. 当此窗口出现时，单击 **是**。



6. 确认证书已安装：

   a. 打开“命令提示符”窗口。

   b. 键入 `mmc` 并按 **Enter** 键。要查看本地计算机存储中的证书，您必须具有管理员角色。

   c. 在“文件”菜单上，单击 **添加/删除管理单元**。

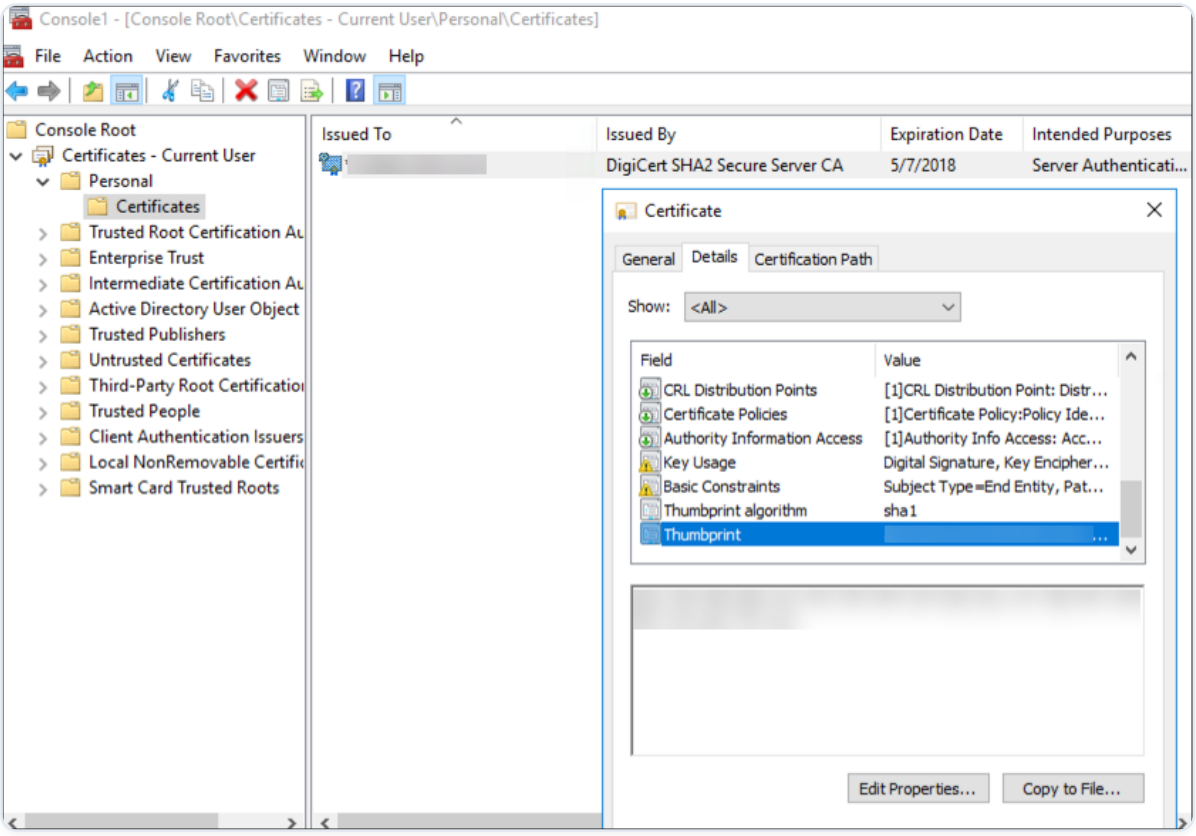
   d. 单击 **添加**。

   e. 在“添加独立管理单元”对话框中，选择 **证书**。

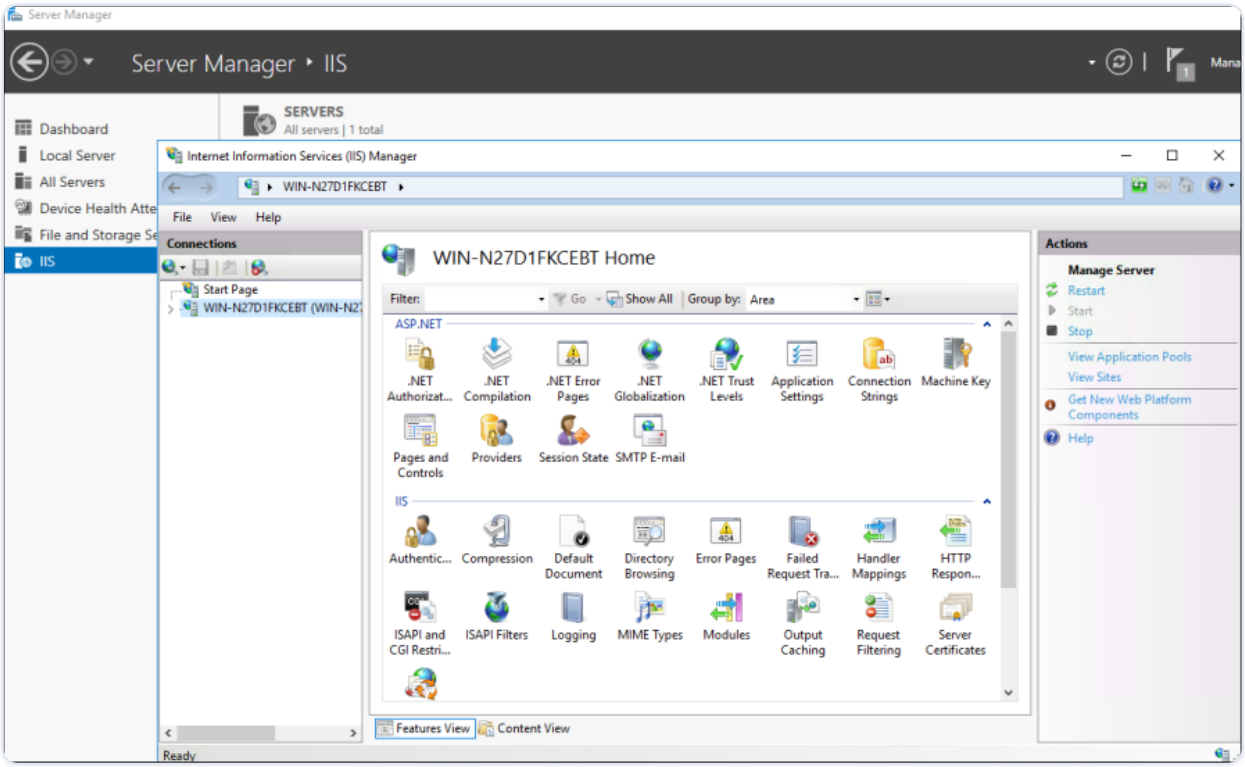
   f. 点击“**添加**”。

   g. 在“证书管理单元”对话框中，选择“**我的用户帐户**”。（如果您以服务帐户持有者身份登录，请选择“**服务帐户**”。）

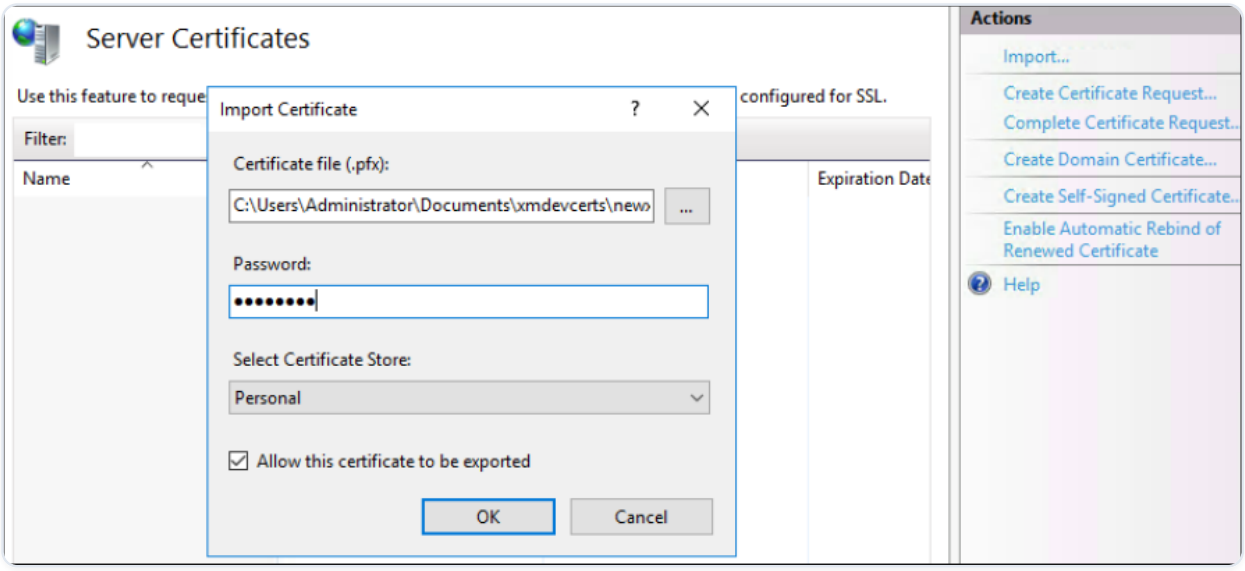
   h. 在“选择计算机”对话框中，点击“**完成**”。



7. 转到“**服务器管理器 > IIS**”，然后从图标列表中选择“**服务器证书**”。

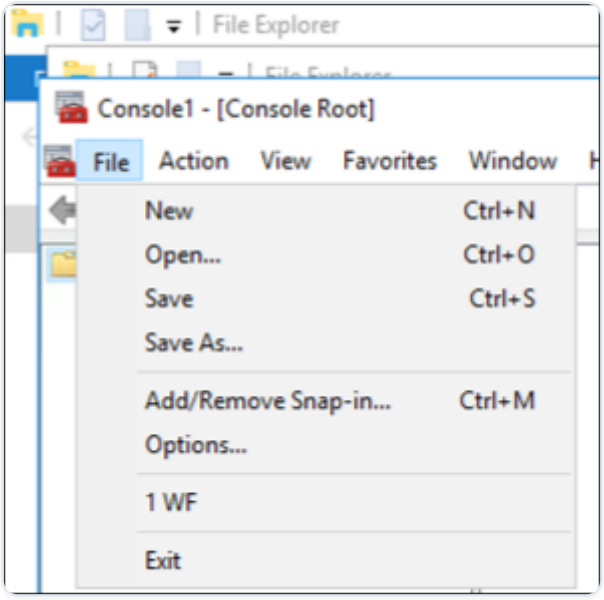


8. 从“操作”菜单中，选择“**导入...**”以导入 SSL 证书。

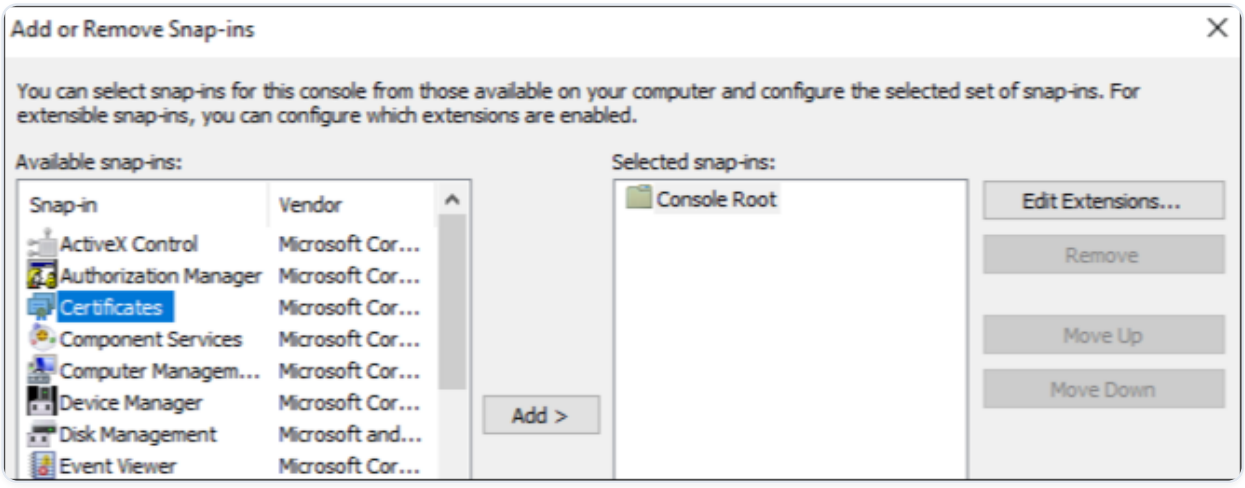


检索并保存证书的指纹

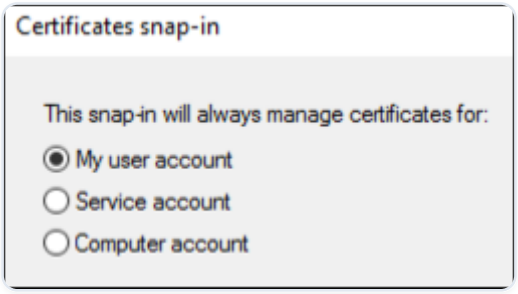
1. 在文件资源管理器搜索栏中，键入 `mmc`。
2. 在“控制台根目录”窗口中，点击“**文件 > 添加/删除管理单元**”。



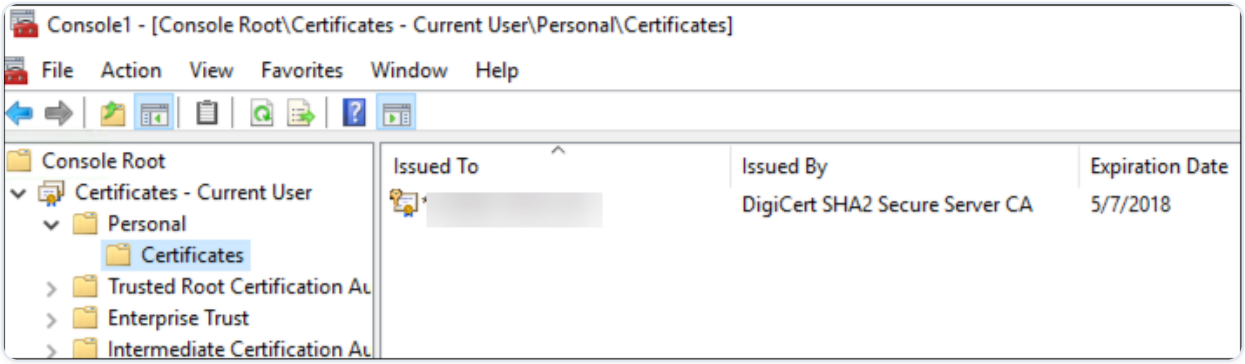
3. 从可用管理单元中选择证书，并将其添加到选定的管理单元中。



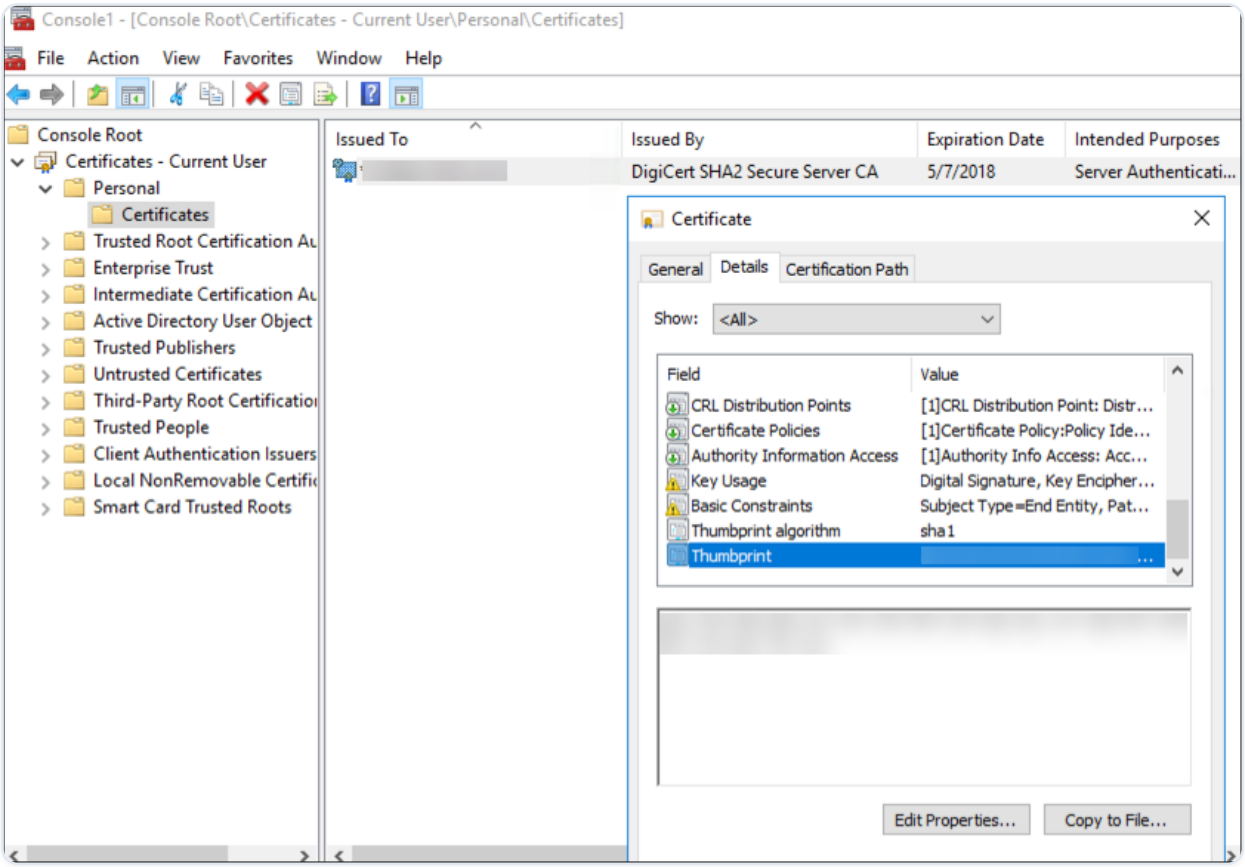
4. 选择“**我的用户帐户**”。



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。



7. 将指纹复制到文件。在 PowerShell 命令中使用指纹时，请删除空格。

安装签名和加密证书

在 Windows 服务器上运行这些 PowerShell 命令以安装签名和加密证书。

替换占位符 ReplaceWithThumbprint，并按所示将其用双引号括起来。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint
-like "ReplaceWithThumbprint"}



$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName



$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
$keyname icacls $keypath /grant IIS_IUSRS`:R
```

提取 TPM 根证书并安装受信任的证书包

在 Windows 服务器上运行以下命令：

```
mkdir .\TrustedTpm



expand -F:\* .\TrustedTpm.cab .\TrustedTpm



cd .\TrustedTpm



.\setup.cmd
```

配置 DHA 服务

在 Windows 服务器上运行此命令以配置 DHA 服务。

替换占位符 ReplaceWithThumbprint。

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
ReplaceWithThumbprint



-SigningCertificateThumbprint ReplaceWithThumbprint



-SslCertificateStoreName My -SslCertificateThumbprint
ReplaceWithThumbprint



-SupportedAuthenticationSchema "AikCertificate"
```

在 Windows 服务器上运行以下命令，为 DHA 服务设置证书链策略：

```
$policy = Get-DHASCertificateChainPolicy



$policy.RevocationMode = "NoCheck"



Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

按如下方式响应这些提示：

```
  Confirm



    Are you sure you want to perform this action?



    Performing the operation "Install-DeviceHealthAttestation" on target
"[Machine Name]".



    [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
```

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，则会显示证书类型（签名）和指纹。

要检查 DHASActiveSigningCertificate 是否处于活动状态，请在服务器上运行以下命令：

替换占位符 ReplaceWithThumbprint，并如所示将其用双引号括起来。

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
-Force

Get-DHASActiveEncryptionCertificate
```

如果证书处于活动状态，则会显示指纹。

要进行最终检查，请访问此 URL：

`https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1`

如果 DHA 服务正在运行，则会显示“Method not allowed”。


Secure
https://dha.[redacted].com/DeviceHealthAttestation/ValidateHealthCertificate/v1
Citrix Access Gateway
AWS Dev
Azure Dev
15Five
Jenkins
FileDiff
Git XM
Nantucket
Service
Method not allowed.

__index__

Android Enterprise 托管配置策略

Android Enterprise 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

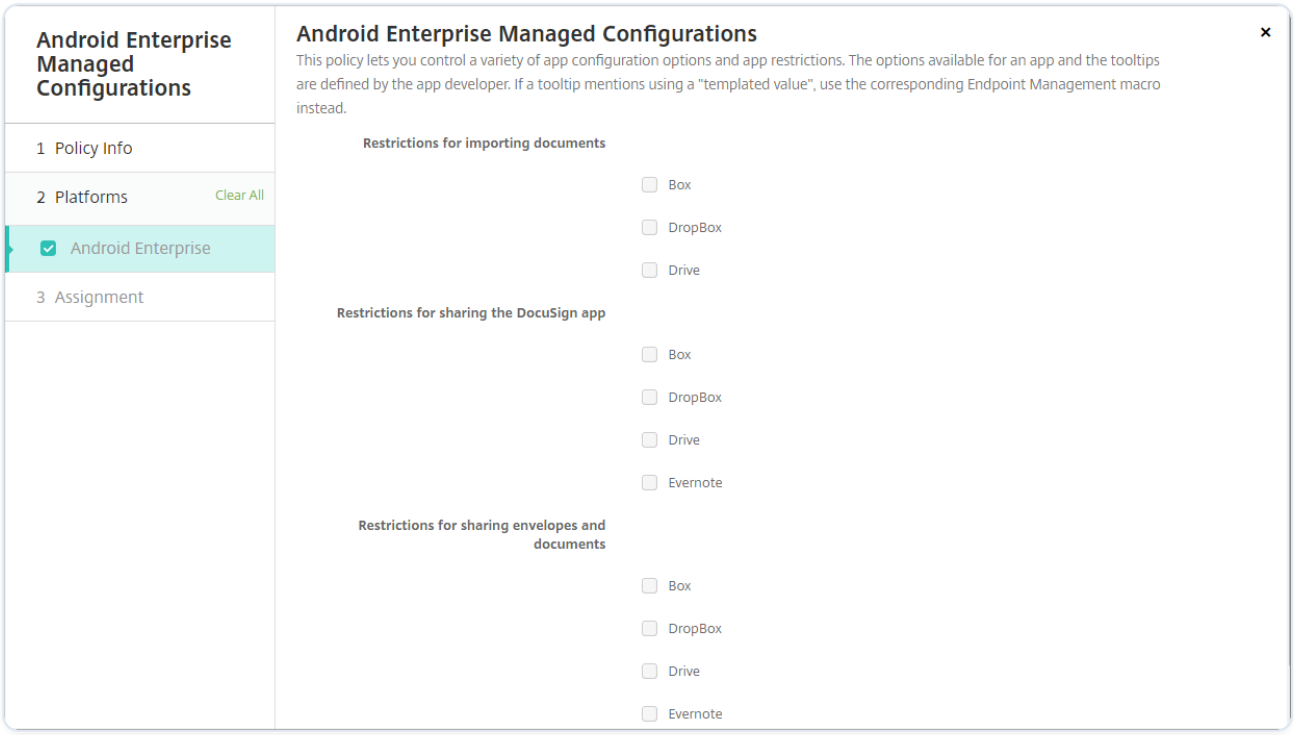
- 在 Google 上完成 Android Enterprise 设置任务，并将 Android Enterprise 连接到托管 Google Play。有关详细信息，请参阅Android Enterprise。
- 将 Android Enterprise 应用程序添加到 Endpoint Management。有关详细信息，请参阅将应用程序添加到 Endpoint Management。

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。

Android Enterprise 设置

选择添加 Android Enterprise 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。

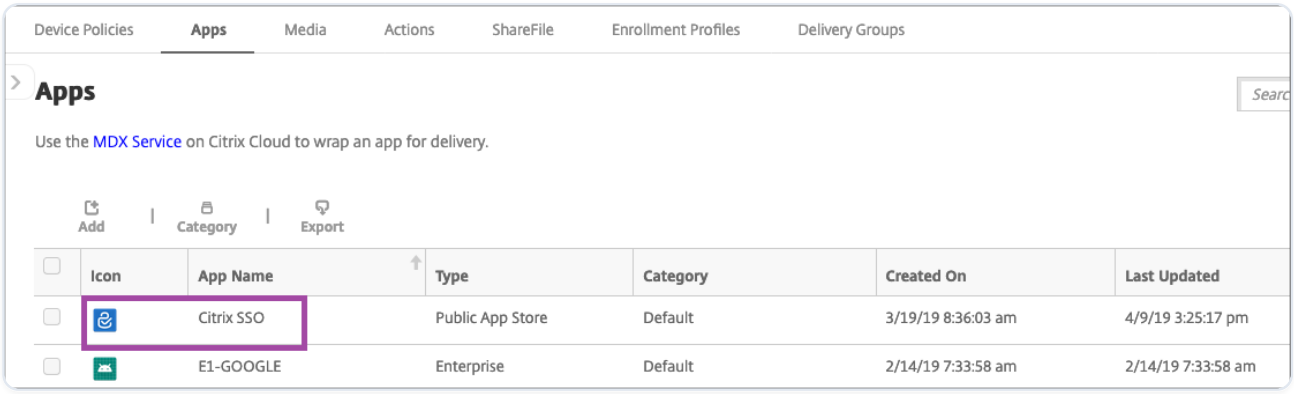
选择应用程序后，配置策略设置。这些设置与每个应用程序特定相关。



为 Android Enterprise 配置 VPN 配置文件

使用 Citrix SSO 应用程序和 Android Enterprise 托管配置设备策略，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。

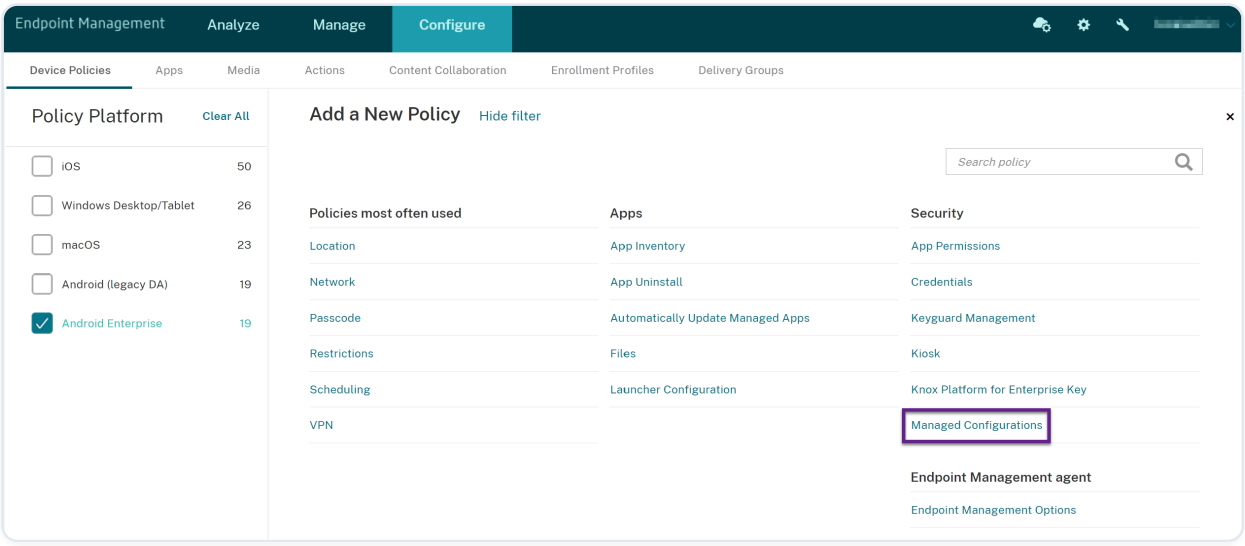


为 Citrix SSO 创建 Android Enterprise 托管配置

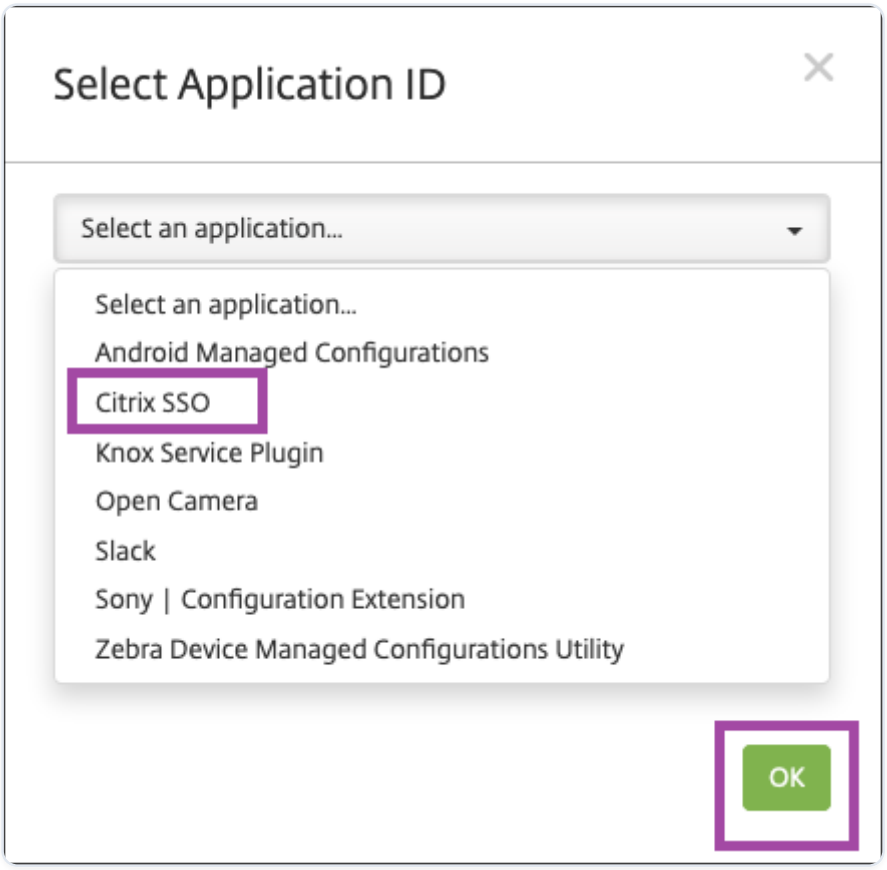
为 Citrix SSO 配置 Android Enterprise 托管配置设备策略以创建 VPN 配置文件。安装了 Citrix SSO 应用程序并部署了策略的设备可以访问您创建的 VPN 配置文件。

您需要您的 Citrix Gateway FQDN 和端口。

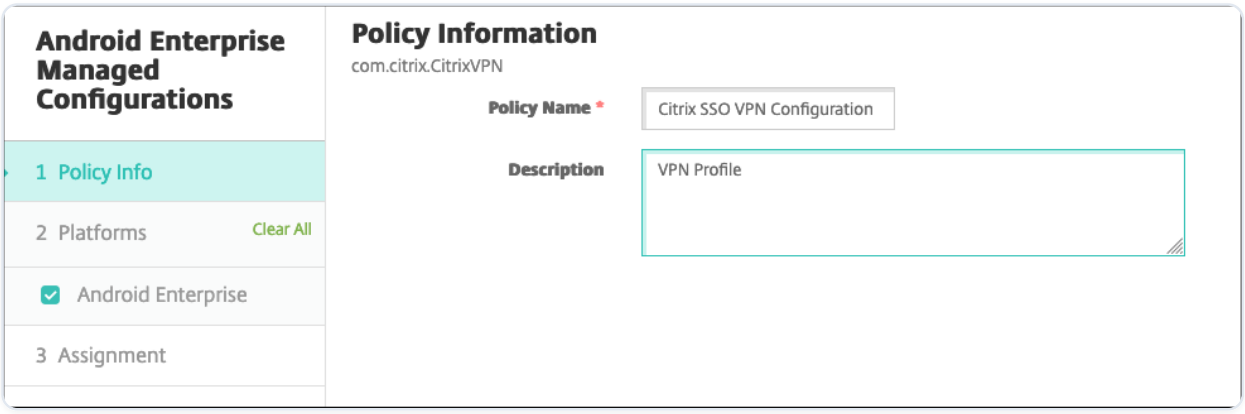
1. 在 Endpoint Management 控制台中，单击**配置 > 设备策略**。单击**添加**。
2. 选择 **Android Enterprise**。单击 **Android Enterprise 托管配置**。



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**。



4. 键入 Citrix SSO VPN 配置的名称和说明。单击**下一步**。

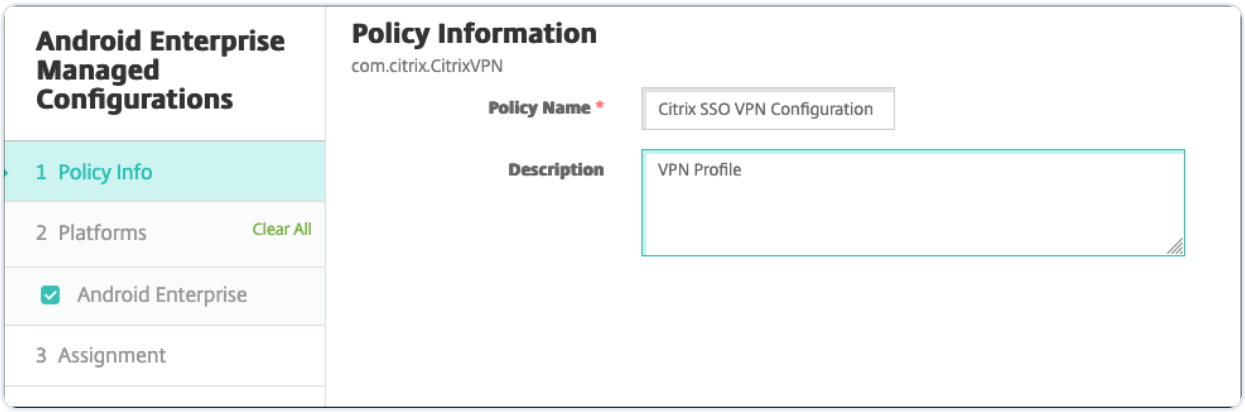


5. 配置 VPN 配置文件参数。

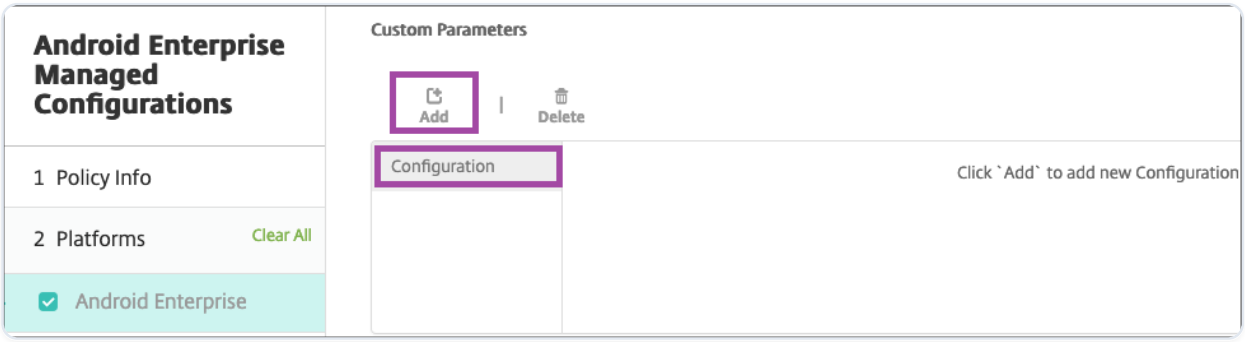
- **VPN 配置文件名称：** 键入 VPN 配置文件的名称。如果要创建多个 VPN 配置文件，请为每个配置文件使用唯一的名称。如果不提供名称，则会将您在**服务器地址**字段中放置的地址用作 VPN 配置文件名称。
- **服务器地址(*)：** 键入您的 Citrix Gateway FQDN。如果 Citrix Gateway 端口不是 443，请键入您的端口。使用 URL 格式。例如，`https://gateway.mycompany.com:8443`。
- **用户名(可选)：** 提供最终用户用于对 Citrix Gateway 进行身份验证的用户名。可以将 Endpoint 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。
- **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**。



   a. 创建自定义参数：

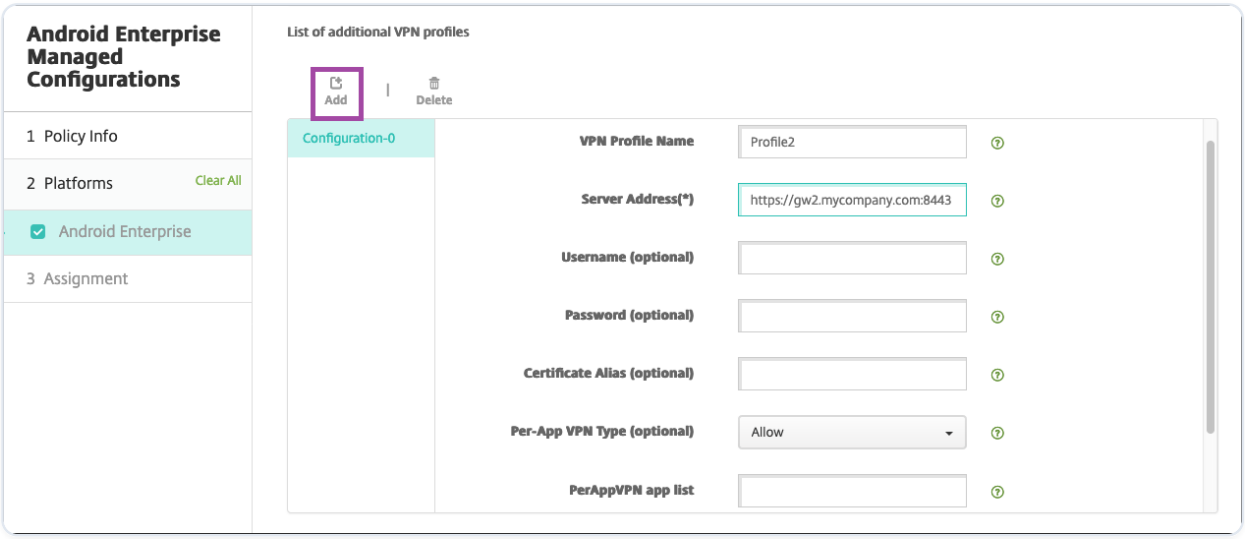
   - **参数名称：** 键入 **XenMobileDeviceId**。此字段是用于根据 Endpoint Management 中的设备注册进行网络访问检查的设备 ID。如果 Endpoint Management 注册并管理设备，则允许建立 VPN 连接。否则，在 VPN 建立时将拒绝身份验证。
   - **参数值** Endpoint Management 用于确定设备的注册和管理状态，XenMobileDeviceID 的值设置为 `DeviceID_${device.id}`。



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。



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。

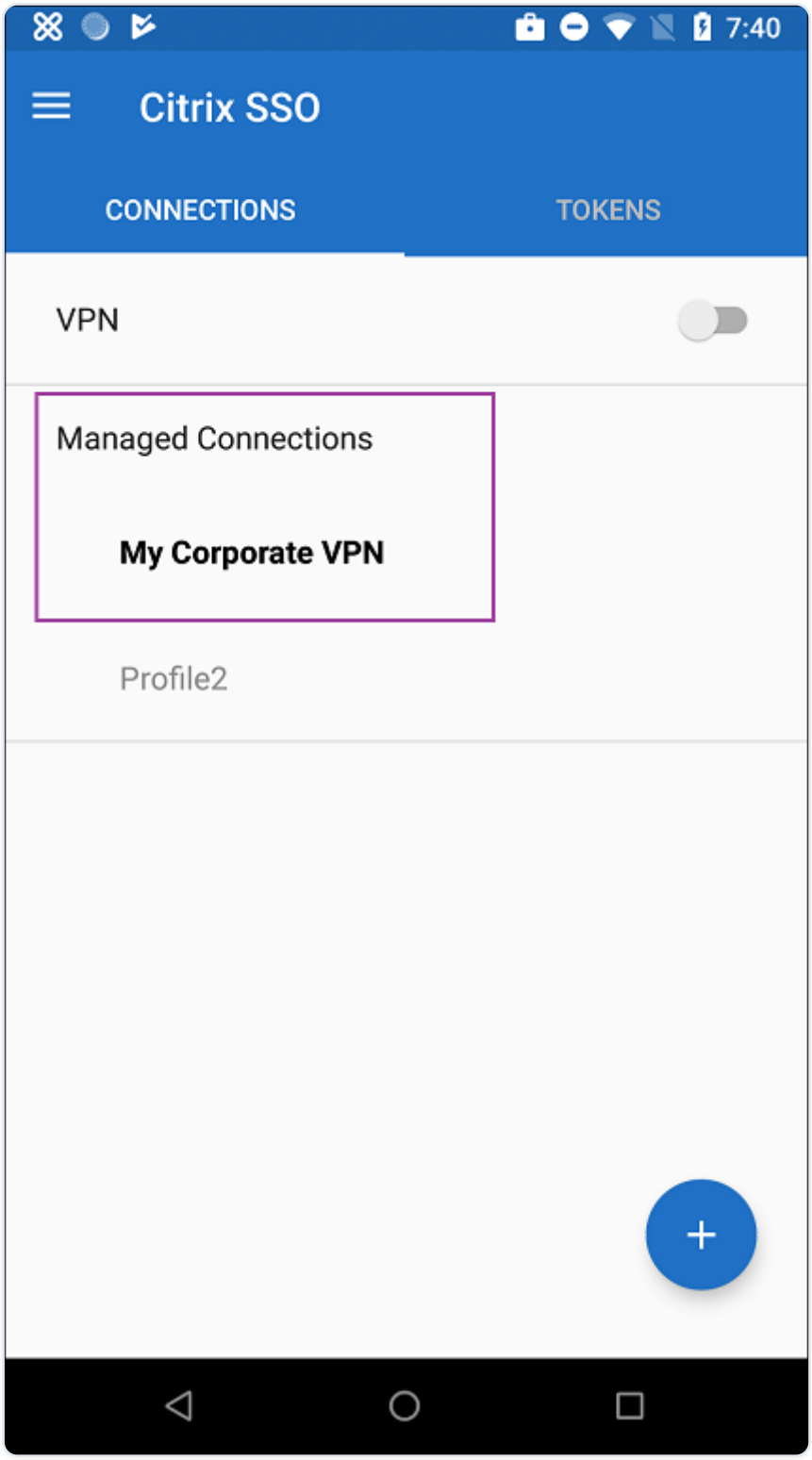
要为您配置的 VPN 配置文件启用始终启用功能，请设置Endpoint Management 选项设备策略。

> **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。



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。

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。

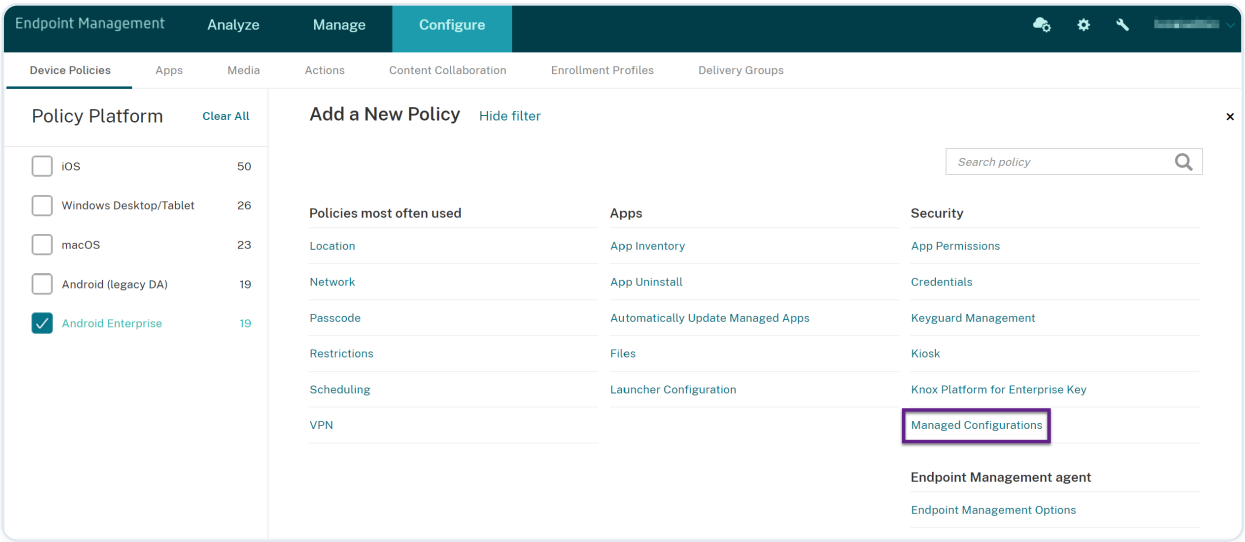
Endpoint Management 支持 Zebra OEMConfig 9.2 及更高版本。有关在设备上安装 Zebra OEMConfig 的系统要求的信息，请参阅 Zebra Technologies Web 站点上的 OEMConfig 设置。

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 Android Enterprise 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 **Android Enterprise 托管配置**。



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**。

Citrix Endpoint Management 文档历史记录

下表介绍了对 Endpoint Management 产品文档所做的重要变更。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	说明
05 Nov 2021	更新了 Endpoint Management 21.11.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.11.0。
22 Oct 2021	更新了 Endpoint Management 21.10.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.10.1。
21 Oct 2021	宣布弃用 Windows 10 设备的“允许自动连接到 Wi-Fi 感应热点”限制	有关信息，请参阅弃用和 Microsoft 文档。
05 Oct 2021	更新了 Endpoint Management 21.10.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.10.0。
24 Sep 2021	宣布不使用 Cloud Connector 的身份提供程序身份验证的公共预览版	有关此功能的详细信息，请参阅不使用 Cloud Connector 的身份提供程序身份验证。
15 Sep 2021	更新了 Endpoint Management 21.9.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.9.1。
06 Sep 2021	更新了 Endpoint Management 21.9.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.9.0。
18 Aug 2021	更新了 Endpoint Management 21.8.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.8.0。

日期	更改	说明
22 Jul 2021	更新了 Endpoint Management 21.7.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.7.1。
09 Jul 2021	宣布在自助服务门户中弃用高安全性注册模式和注册邀请设置	有关信息，请参阅弃用。
06 Jul 2021	更新了 Endpoint Management 21.7.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.7.0。
23 Jun 2021	Android for Workspace 平台作为公共预览版提供。配置 Android for Workspace 后，用户可以使用 Citrix Workspace 应用程序在 Endpoint Management 中注册。	有关详细信息，请参阅 Android for Workspace。
14 Jun 2021	更新了 Endpoint Management 21.6.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.6.0。
24 May 2021	更新了 Endpoint Management 21.5.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.5.1。
11 May 2021	更新了 MDX 共享设备支持的弃用日期	有关详细信息，请参阅弃用。
06 May 2021	更新了 Endpoint Management 21.5.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.5.0。
03 May 2021	添加了已知问题 CXM-89333 的文档。	有关信息，请参阅 Endpoint Management 21.4.0 中的已知问题。
26 Apr 2021	更新了“定位”安全操作的说明	请参阅安全操作。

日期	更改	说明
22 Apr 2021	添加了操作示例	请参阅自动化操作。
21 Apr 2021	宣布弃用使用设备 IMEI 或序列号生成邀请 URL 的功能。	有关信息，请参阅弃用。
20 Apr 2021	添加了与 Azure AD 条件访问的集成	有关信息，请参阅与 Azure AD 条件访问集成（预览版）。
15 Apr 2021	添加了有关共用的 iPad 的文章	请参阅共用的 iPad。
13 Apr 2021	更新了 Endpoint Management 21.4.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.4.0。
31 Mar 2021	添加了对 PerApp VPN 要求的说明	请参阅 VPN 设备策略和托管配置策略。
09 Mar 2021	更新了 Endpoint Management 21.3.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.3.0。
09 Mar 2021	添加了与迁移自动发现服务记录有关的声明	请参阅迁移自动发现服务记录。
24 Feb 2021	添加了关于将端点升级到 iOS 14.5 之前所需准备的公告	请参阅在将端点升级到 iOS 14.5 之前的准备工作。
12 Feb 2021	更新了 Endpoint Management 21.2.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.2.0。
25 Jan 2021	更新了 Endpoint Management 21.1.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.1.1。
06 Jan 2021	更新了 Endpoint Management 21.1.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 21.1.0。

日期	更改	说明
09 Dec 2020	添加了与使用 Azure Android Enterprise 和 Okta 作为身份平台注册 Active Directory 设备有关的预览内容	有关更改的更多详细信息，请参阅 Endpoint Management 20.12.0。
04 Dec 2020	更新了 Endpoint Management 20.12.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.12.0。
10 Nov 2020	添加了 Endpoint Management 可以执行的各种连接检查表	请参阅连接检查详细信息。
06 Nov 2020	更新了 Endpoint Management 20.11.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.11.0。
28 Oct 2020	添加了升级到最新版本的 Citrix ADC 所需的解决方法	请参阅在将本地 Citrix ADC 升级到 13.0-64.35+ 之前的准备工作。
23 Oct 2020	更新了 Endpoint Management 20.10.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.10.1。
22 Oct 2020	为 Android Enterprise 设置添加了高级工作流程	请参阅 Android Enterprise 入门。
22 Oct 2020	添加了详细介绍分发 Android Enterprise 应用程序的不同方法的文章	请参阅分发 Android Enterprise 和 Android for Workspace 应用程序。
07 Oct 2020	更新了 Endpoint Management 20.10.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.10.0。
22 Sep 2020	更新了 Endpoint Management 20.9.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.9.1。

日期	更改	说明
04 Sep 2020	更新了 Endpoint Management 20.9.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.9.0。
20 Aug 2020	更新了 Endpoint Management 20.8.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.8.0。
14 Aug 2020	添加了简化 Windows 设备开箱即用批量注册流程的说明	请参阅批量注册设备开箱即用。
31 Jul 2020	更新了 Windows 设备的批量注册文章	请参阅批量注册 Windows 设备。
23 Jul 2020	更新了 Endpoint Management 20.7.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.7.1。
10 Jul 2020	更新了 Endpoint Management 20.7.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.7.0。
02 Jul 2020	添加了弃用 MDX 加密的时间表和行动计划	请参阅为即将做出的更改准备您的 Android 设备。
25 Jun 2020	更新了 Endpoint Management 20.6.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.6.0。
19 Jun 2020	解决了文档中的术语“黑名单”和“白名单”问题。更改为“阻止列表”和“允许列表”。	Endpoint Management 控制台当前包含术语“黑名单”和“白名单”。我们更新了该文档。我们正在为即将发布的版本更改产品控制台中的术语。
18 Jun 2020	宣布弃用 Samsung SEAMS 容器	请参阅弃用。
09 Jun 2020	添加了 Citrix Cloud Connector 支持用于 Endpoint	请参阅支持的 Active Directory 功能级别。

日期	更改	说明
	Management 的林和域功能级别表	
05 Jun 2020	添加了一篇文章，该文章提供了 Android 和 iOS 设备注册的 Citrix Cloud Connector 加载测试结果	请参阅 Cloud Connector 的扩展和大小注意事项。
02 Jun 2020	更新了 Endpoint Management 20.5.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.5.0。
27 May 2020	扩展了有关发布 Intune 托管应用程序的内容。删除了与封装第三方应用程序有关的内容。	请参阅 Citrix Endpoint Management 与 Microsoft Endpoint Manager 的集成。
13 May 2020	有关 Endpoint Management 用户角色和权限的扩展信息	请参阅使用 RBAC 功能。
05 May 2020	更新了 Endpoint Management 20.4.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.4.1。
04 May 2020	添加了关于 iOS、iPadOS 和 macOS 中受信任的证书的新 TLS 证书要求的说明	请参阅证书。
30 Apr 2020	添加了有关使用 Azure Active Directory 进行身份验证的预览版内容	请参阅通过 Citrix Cloud 使用 Azure Active Directory 进行身份验证。
29 Apr 2020	添加了有关使用 Okta 凭据进行身份验证的 Endpoint Management 支持的预览版文档	请参阅通过 Citrix Cloud 使用 Okta 进行身份验证
13 Apr 2020	更新了 Endpoint Management 20.4.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.4.0。

日期	更改	说明
26 Mar 2020	更新了 Endpoint Management 20.3.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.3.0。
20 Mar 2020	添加了一篇文章，详细介绍了分发不同类型的 iOS 应用程序的步骤	请参阅分发 Apple 应用程序
13 Mar 2020	添加了有关保护企业移动设备免受高级网络攻击的部分	请参阅与 Mobile Threat Defense 软件集成。
13 Feb 2020	更新了 Endpoint Management 20.2.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.2.1。
08 Jan 2020	更新了 Endpoint Management 20.1.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 20.1.0。
03 Dec 2019	更新了 Endpoint Management 19.12.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.12.0。
08 Nov 2019	更新了 Endpoint Management 19.11.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.11.0。
16 Oct 2019	更新了 Endpoint Management 19.10.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.10.0。
16 Oct 2019	添加了有关 Google 向 Android Enterprise 转换的部分	请参阅创建注册配置文件。
25 Sep 2019	更新了 Endpoint Management 19.9.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.9.1。

日期	更改	说明
10 Sep 2019	更新了 Endpoint Management 19.9.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.9.0。
08 Aug 2019	更新了 Endpoint Management 19.8.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.8.0。
07 Aug 2019	更新了 Android Enterprise 一文，以阐明 Android Enterprise 概念。在有关迁移到 Android Enterprise 的文章中增加了迁移建议	请参阅 Android Enterprise 和从设备管理迁移到 Android Enterprise。
31 Jul 2019	添加了有关从 Android 旧版设备管理迁移到 Android Enterprise 的文章	请参阅从设备管理迁移到 Android Enterprise。
16 Jul 2019	更新了 Endpoint Management 19.7.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.7.1。
27 Jun 2019	更新了 Endpoint Management 19.6.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.6.1。
06 Jun 2019	更新了 Endpoint Management 19.6.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.6.0。
24 May 2019	更新了 Android Enterprise 术语以匹配当前的 Google Android Enterprise 文档	更新了文章 Android Enterprise。
20 May 2019	新增关于支持从 iOS 和 Android 设备移动单点登录到本机 SaaS 应用程序的部分	在“添加应用程序”一文中添加了以下部分：配置移动 SSO（预览版）。移动 SSO 适用于启用了 Workspace 的客户。

日期	更改	说明
20 May 2019	新增关于将 Citrix Gateway 服务与 Endpoint Management 集成的部分	Citrix Gateway 服务预览适用于具有 Citrix Gateway 服务订阅并且启用了 Workspace 的客户。在“载入和资源设置”一文中添加了以下部分：将 Citrix Gateway 配置为与 Endpoint Management 结合使用。
10 May 2019	新增关于 Entrust PKI 的部分	在“PKI 实体”一文中添加了以下部分：Entrust PKI 适配器。
09 May 2019	更新了 Endpoint Management 19.5.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.5.0。
01 May 2019	新增有关如何为 Android Enterprise 配置 VPN 的部分：为 Citrix SSO 应用程序创建托管配置设备策略	在“托管配置策略”一文中添加了以下部分：为 Android Enterprise 配置 VPN 配置文件。
17 Apr 2019	更新了 Endpoint Management 19.4.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.4.1。
04 Apr 2019	新增关于零接触配置的部分	在“Android Enterprise”一文中添加了以下部分：零触摸注册。
02 Apr 2019	更新了适用于 Exchange ActiveSync 8.5.3 的网关连接器版本的文章	有关新增功能和更改后的功能的摘要，请参阅版本 8.5.3 中的新增功能。
02 Apr 2019	Endpoint Management 19.3.1 版本的新的已修复的问题	有关信息，请参阅 Endpoint Management 19.3.1 中已修复的问题。
26 Mar 2019	更新了包含升级步骤的 FCM 部分	有关 FCM 的详细信息，请参阅 Firebase Cloud Messaging。

日期	更改	说明
26 Mar 2019	更新了 Secure Hub 应用商店名称语法	在 App Store 和 Citrix Secure Hub 外观方案中添加了与应用商店名称的字母数字要求有关的备注。
11 Mar 2019	更新了 Endpoint Management 19.3.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.3.0。
22 Feb 2019	更新了 Endpoint Management 19.2.1 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.2.1。
11 Feb 2019	更新了 Endpoint Management 19.2.0 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.2.0。
25 Jan 2019	更新了 Endpoint Management 19.1.2 版本的相关文章	有关新增功能和更改后的功能的摘要，请参阅 Endpoint Management 19.1.2。