citrix

XenMobile Server 当前版本

Contents

滚动修补程序的发行说明

January 5, 2022

本部分内容包含最新的 XenMobile Server 滚动修补程序的发行说明。单击下面的链接可查看已修复的问题和已知问题、功能变更以及所需的操作。

最新的滚动修补程序包含同一版本的之前的滚动修补程序中的所有修复。

当前版本的修补程序的发行说明	发布日期
10.14 滚动修补程序 3	Dec 22, 2021
10.14 滚动修补程序 2	Dec 15, 2021
10.14 滚动修补程序 1	Nov 19, 2021

早期版本的修补程序的发行说明	发布日期
10.13 滚动修补程序 6	Dec 21, 2021
10.13 滚动修补程序 5	Dec 15, 2021
10.13 滚动修补程序 4	Aug 11, 2021
10.13 滚动修补程序 3	May 13, 2021
10.13 滚动修补程序 2	Feb 25, 2021
10.13 滚动修补程序 1	Jan 8, 2021
10.12 滚动修补程序 11	Dec 21, 2021
10.12 滚动修补程序 10	Dec 16, 2021
10.12 滚动修补程序 9	Oct 8, 2021
10.12 滚动修补程序 8	Jun 2, 2021
10.12 滚动修补程序 7	Mar 29, 2021
10.12 滚动修补程序 6	Jan 26, 2021
10.11 滚动修补程序 7	Nov 18, 2020
10.10 滚动修补程序 6	Jul 22, 2020

XenMobile Server 10.14 滚动修补程序 3 版本的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 3 的增强功能以及已修复的问题和已知问题。

此版本包括缺陷修复。

有关以前面向 XenMobile Server 10.14.0 的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

XenMobile Server 10.13 滚动修补程序 6 版本的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.13 滚动修补程序 6 的增强功能以及已修复的问题和已知问题。

此版本包括缺陷修复。

有关以前面向 XenMobile Server 10.13.0 的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

XenMobile Server 10.12 滚动修补程序 11 的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.12 滚动修补程序 11 的增强功能以及已修复的问题和已知问题。

此版本包括缺陷修复。

有关以前面向 XenMobile Server 10.12.0 的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

XenMobile Server 10.12 滚动修补程序 10 的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.12 滚动修补程序 10 的增强功能以及已修复的问题和已知问题。

此版本包括缺陷修复。

有关以前面向 XenMobile Server 10.12.0 的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

XenMobile Server 10.14 滚动修补程序 **2** 版本的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 2 的增强功能以及已修复的问题和已知问题。

有关以前面向 XenMobile Server 10.14.0 的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

已修复的问题

在 XenMobile Server 上，您会观察到高峰时段服务器节点上的 CPU 使用率非常高。[CXM-102568]

XenMobile Server 10.13 滚动修补程序 **5** 版本的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.13 滚动修补程序 5 的增强功能以及已修复的问题和已知问题。

新增功能

- 支持 **Windows 11** 台设备。现在，您可以使用 XenMobile Server 来管理 Windows 11 设备。有关详细信息，请参阅操作系统支持列表。[CXM-99998]
- 配置 **macOS** 的连接模式和网络优先级。在 Wi-Fi 设备策略中，启用 macOS 设备的连接模式设置，以选择用户加入网络的方式。设备可以使用系统凭据或在登录窗口中输入的凭据对用户进行身份验证。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。设备选择编号最低的网络。有关详细信息，请参阅 Wi-Fi 设备策略中的 macOS 设置。[CXM-100533]
- XenMobile Server 将无法将组许可证同步到 Google，原因是 Google 已弃用对 Android Enterprise 设备上的组许可证的支持。有关详细信息，请参阅本文。[CXM-101309]

有关以前面向 XenMobile Server 10.13.0 的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

已修复的问题

- 注册 iOS 15 或 macOS 12 设备后，MDM 配置文件将显示为 “未验证”。[CXM-99380]
- 禁用应用程序自动更新设置后，在设备上安装的 Apple 批量购买应用程序将自动更新到最新版本。[CXM-99723]
- 在 XenMobile Server 控制台中，当您修改了某个应用程序的设置以清除所有平台并保存时，该应用程序不会在配置 **>** 应用程序中列出。[CXM-99850]
- 在某些 Android Enterprise 设备上，交付组和分配的策略或应用程序不会间歇性应用。[CXM-101554]
- 在 XenMobile Server 上，您会观察到高峰时段服务器节点上的 CPU 使用率非常高。[CXM-102450]

- 在仅 MDM 模式下注册的 iOS 设备上，您无法通过 Secure Hub 打开的浏览器添加 App Store 中的应用程序。您将收到以下错误消息：您的登录已过期。请重新登录以继续。[CXM-102604]
- 在 XenMobile Server 版本 10.13 中，无法使用仅存储区域连接器连接和配置存储区域控制器。[CXM-102655]
- 在 XenMobile Server 10.13 RP1 及更高版本中，SNMP 监视的 XenMobile 节点间连接陷阱不起作用。[CXM-102788]

XenMobile Server 10.14 滚动修补程序 **1** 版本的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 1 的增强功能以及已修复的问题和已知问题。

新增功能

- 支持 **Windows 11** 台设备。现在，您现在可以使用 XenMobile 来管理 Windows 11 设备。有关详细信息，请参阅操作系统支持列表。[CXM-99999]
- 配置 **macOS** 的连接模式和网络优先级。在 Wi-Fi 设备策略中，启用 macOS 设备的连接模式设置，以选择用户加入网络的方式。设备可以使用系统凭据或在登录窗口中输入的凭据对用户进行身份验证。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。设备选择编号最低的网络。有关详细信息，请参阅 Wi-Fi 设备策略中的 macOS 设置。[CXM-100879]
- XenMobile Server 将无法将组许可证同步到 Google，原因是 Google 已弃用对 Android Enterprise 设备上的组许可证的支持。有关详细信息，请参阅本文。[CXM-101209]

已知问题

从 macOS 11 或更早版本升级到 macOS 12 的已注册设备，或者在 macOS12 中新注册的设备，可能会在设备上的系统偏好设置 **>** 描述文件下显示为 “尚未验证”。有关详细信息和解决方法，请参阅此支持文章。[CXM-101843]

已修复的问题

- 注册 iOS 15 或 macOS 12 设备后，MDM 配置文件将显示为未验证。[CXM-99379]
- 在 XenMobile Server 控制台中，当您修改了某个应用程序的设置以清除所有平台并保存时，该应用程序不会在配置 **>** 应用程序中列出。[CXM-99851]
- 您无法在 Android Enterprise 平台上退出 Citrix Launcher。您将收到以下错误消息：密码不正确。[CXM-100975]
- 在 XenMobile Server 版本 10.14 中，您无法编辑 “导入 iOS 和 macOS 配置文件” 策略。[CXM-102393]

XenMobile Server 10.12 滚动修补程序 9 的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.12 滚动修补程序 9 的增强功能以及已修复的问题和已知问题。

新增功能

支持 **Android 12** XenMobile Server 现在支持在 Android Enterprise 设备上安装 Android 12。有关安全性和隐私优势的摘要，请参阅面向 Android 的 Google 文档。[CXM-97765]

支持 **Windows 11** 台设备。现在，您可以使用 XenMobile Server 来管理 Windows 11 设备。有关详细信息，请参阅操作系统支持列表。[CXM-99995]

已修复的问题

禁用应用程序自动更新设置后，在设备上安装的 Apple 批量购买应用程序将自动更新到最新版本。[CXM-95985]

在 XenMobile Server 10.12 中，访问设备详细信息时出错。当设备属性的值在 **”“** 中时，将出现此错误。[CXM-97953]

在 XenMobile Server 控制台中，当您修改了某个应用程序的设置以取消选中所有平台并保存时，该应用程序不会在配置 **>** 应用程序中列出。[CXM-99708]

XenMobile Server 10.13 滚动修补程序 4 版本的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.13 滚动修补程序 4 的增强功能以及已修复的问题和已知问题。

新增功能

支持 **Android 12** XenMobile Server 现在支持将 Android Enterprise 设备更新到 Android 12。有关安全和隐私好处的摘要，请参阅 Android 文档。

有关以前面向 XenMobile Server 10.13.0 的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

已修复的问题

- 切换到适用于 APNs 的基于 HTTP/2 的 API 时，服务器属性 `ios.mdm.apns.connectionPoolSize` 将处于隐藏状态。[CXM-95479]
- 在 XenMobile Server 10.12 中，无法修改某些应用程序上的 VPP 属性。[CXM-96854]

- 所需的 Web 应用程序无法自动安装在仅 MDM 设备上。[CXM-97477]
- 在 XenMobile Server 10.13 中，在 **CLI** 下配置代理服务器时，无法将通知发送到 iOS 设备上运行的 Secure Hub。[CXM-97807]
- 在 XenMobile Server 10.13 中，访问设备详细信息时出错。当设备属性的值在 **”“** 中时，将出现此错误。[CXM-97951]

XenMobile Server 10.12 滚动修补程序 **8** 的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.12 滚动修补程序 8 的增强功能以及已修复的问题和已知问题。

新增功能

Secure Hub APNs 证书续订。适用于 XenMobile Server 10.12 的 Secure Hub Apple 推送通知服务 (APN) 证书将于 2021 年 6 月 17 日到期。此更新将续订 Secure Hub APNs 证书，该证书将于 2022 年 5 月 7 日到期。[CXM-94513]

已修复的问题

- 注册运行 macOS 10.14+ 的设备后，设备属性并不总是填充到 XenMobile Server 控制台中。设备重新启动后，设备属性将按预期显示。[CXM-94221]
- 在 XenMobile Server 10.12 上，ShareFile 间歇性地无法建立连接。[CXM-95419]

XenMobile Server 10.13 滚动修补程序 **3** 版本的发行说明

January 5, 2022

这些发行说明介绍了 XenMobile Server 10.13 滚动修补程序 3 的增强功能以及已修复的问题和已知问题。

新增功能

Secure Hub APNs 证书续订。适用于 XenMobile Server 10.13 的 Secure Hub Apple 推送通知服务 (APN) 证书将于 2021 年 6 月 17 日到期。此更新将续订 Secure Hub APNs 证书，该证书将于 2022 年 5 月 7 日到期。[CXM-94070]

APNs 通知的备用端口。XenMobile Server 现在支持使用端口 2197 作为端口 443 的备用端口。您使用端口 2197 发送 APNs 通知以及接收来自 `api.push.apple.com` 的反馈。该端口使用基于 HTTP/2 的 APNs 提供程序 API。

服务器属性 `apns.http2.alternate.port.enabled` 的默认值为 **`false`**。要使用备用端口，请更新服务器属性，然后重新启动服务器。[CXM-93911]

已修复的问题

注册运行 macOS 10.14+ 的设备后，设备属性并不总是填充到 XenMobile Server 控制台中。设备重新启动后，设备属性将按预期显示。[CXM-94150]

如果在“限制”策略中同时为同一应用程序启用了启用系统应用程序和禁用应用程序设置，该应用程序将显示在工作配置文件中。[CXM-94097]

将 SNMP 用户添加到 XenMobile Server 控制台时，用户不会显示在 **SNMP** 监视用户列表下，或者 SNMP 代理变为非活动状态。[CXM-93199]

在 XenMobile Server 上，NetScaler Gateway 连接检查不显示结果。[CXM-93134]

在 XenMobile Server 控制台中，不显示正确的根证书过期日期。[CXM-93133]

XenMobile Server 10.14 中的新增功能

January 5, 2022

继续支持 Citrix ADC 中已弃用的经典策略

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

XenMobile Migration Service

如果在本地使用 XenMobile Server，我们的免费 XenMobile Migration Service 可以让您开始使用 Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 不需要重新注册设备。

要开始迁移，请与当地的 Citrix 销售人员或 Citrix 合作伙伴联系。请参阅 XenMobile Migration Service。

弃用声明

有关正在逐步淘汰的 Citrix XenMobile 功能的预先通知，请参阅弃用。

在将端点升级到 **iOS 14.5** 之前的准备工作

在将任何端点升级到 iOS 14.5 之前，Citrix 建议执行以下操作以缓解应用程序崩溃情况：

- 将 Citrix Secure Mail 和 Secure Web 升级到 21.2.X 或更高版本。请参阅升级 MDX 或企业应用程序。
- 如果您使用的是 MDX Toolkit，请使用 MDX Toolkit 21.3.X 或更高版本封装所有第三方 iOS 应用程序。请访问 MDX Toolkit 下载页面以获取最新版本。

升级本地 **Citrix ADC** 之前的准备工作

将本地 Citrix ADC 升级到某个版本会导致出现单点登录错误。在浏览器中通过企业员工登录选项单点登录到 Citrix Files 或 ShareFile 域 URL 会导致出现错误。用户无法登录。

要解决此问题，请执行以下操作：如果您尚未从 Citrix Gateway 上的 ADC CLI 运行以下命令，请运行该命令以启用全局 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（功能阶段）13.0 Build 67.39/67.43
- 影响的 SSO 配置

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

升级到 **XenMobile 10.14**（本地）之前的准备工作

某些系统要求发生了变化。有关信息，请参阅系统要求和兼容性和 XenMobile 兼容性。

1. 如果运行要升级的 XenMobile Server 的虚拟机的 RAM 低于 8 GB，我们建议您将 RAM 增加到至少 8 GB。
2. 请先将您的 Citrix 许可证服务器更新到 11.16 或更高版本，然后再更新到最新版本的 XenMobile Server 10.14。

   最新版本的 XenMobile 需要 Citrix 许可证服务器 11.16（最低版本）。

   > 注意：
   >
   > XenMobile 10.14 中的 Customer Success Services 日期（以前称为专享升级服务日期）为 2021 年 9 月 15 日。Citrix 许可证上的 Customer Success Services 日期必须晚于此日期。
   >
   > 可以在许可证服务器中的许可证旁边查看该日期。如果要将最新版本的 XenMobile 连接到较旧的许可证服务器环境，连接检查将失败，并且您无法配置许可证服务器。

   要续订许可证上的日期，请从 Citrix 门户下载最新的许可证文件并将该文件上载到许可服务器。请参阅 Customer Success Services。

3. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序具有以下要求。如果为 Citrix Gateway 配置了 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
4. 建议：安装 XenMobile 更新之前，请使用 VM 中的功能创建系统的快照。此外，还请备份您的系统配置数据库。如果您在升级过程中遇到问题，请完成允许您还原的备份。

升级

在本版本中，XenMobile 支持 VMware ESXi 7.0。请务必在安装或升级 ESXi 7.0 之前升级到 10.14。

可以从 XenMobile 10.13.x 或 10.12.x 直接升级到 XenMobile 10.14。要执行升级，请下载可用的最新二进制文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server >** 产品软件 **> XenMobile Server 10**。在您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击下载文件。

要上载升级，请使用 XenMobile 控制台中的发布管理页面。请参阅使用“发布管理”页面进行升级。

升级之后需要执行的操作

如果涉及传出连接的功能停止运行，并且您尚未更改自己的连接配置，请在 XenMobile Server 日志中检查是否存在如下所示的错误：“Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”（无法连接到 VPP 服务器: 主机名 192.0.2.0 与对等机提供的证书使用者不匹配）。

- 证书验证错误意味着您必须禁用 XenMobile Server 上的主机名验证。
- 默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。
- 如果主机名验证中断了您的部署，请将服务器属性 `disable.hostname.verification` 更改为 **`true`**。此属性的默认值为 **`false`**。

平台支持更新

- **iOS 15**： XenMobile Server 和 Citrix 移动生产力应用程序与 iOS 15 兼容，但目前不支持任何新 iOS 15 功能。
- **Android 12**：XenMobile Server 支持 Android 12。有关弃用 Google 设备管理 API 如何影响运行 Android 10+ 的设备的信息，请参阅从设备管理迁移到 Android Enterprise。另请参阅此 Citrix 博客。

设备策略

- 我们为所有 Android Enterprise 注册模式增加了两个设置，以便与 Google 设置更加一致并简化配置。
  - 允许蓝牙共享：如果未选择，用户将无法在其设备上建立传出蓝牙共享。
  - 允许卸载应用程序：允许用户从托管的 Google Play Store 中卸载应用程序。

此外，我们将允许无线升级设置从“限制”策略移到了“操作系统更新”策略中。

有关这些更改的详细信息，请参阅限制设备策略和操作系统更新设备策略。

- 为确保清晰易懂，我们已对 Android Enterprise 的限制设置进行重新组织。有时，对设置名称进行了细微更改。有关重新组织的详细信息，请参阅 Android Enterprise 设置。
- 现在可以在 Android Enterprise 设备上自动更新托管应用程序。有关详细信息，请参阅自动更新托管应用程序设备策略。
- 可以配置能使用“文件”设备策略进行上载的文件类型的列表。无法上载以下文件类型，即使您将其添加到此允许列表中也是如此：
  - .cab
  - .appx
  - .ipa
  - .apk
  - .xap
  - .mdx
  - .exe

  有关详细信息，请参阅服务器属性

设备注册

- 现在可以为 iOS 和 Android 设备创建不同的注册配置文件。XenMobile Server 支持多种注册类型不同的注册配置文件。有关详细信息，请参阅注册配置文件。
- 完全托管的 Android 11+ 设备将在企业拥有的设备上的工作配置文件模式下注册。新模式进一步将设备上的个人配置文件和工作配置文件分开。这一改变增强了组织对托管配置文件的控制力度，并且让用户的个人配置文件更加隐私。有关详细信息，请参阅 Android Enterprise 和服务器属性。
- 现在，您可以指定用户在设置 iOS 或 macOS 设备时要跳过的更多设置屏幕。
  - iOS
    - 已完成还原：阻止用户看到还原是否在设置过程中完成。适用于 iOS 14.0 及更高版本。
    - 已完成更新：阻止用户看到软件更新是否在设置过程中完成。适用于 iOS 14.0 及更高版本。
  - macOS
    - 辅助功能：阻止用户自动聆听旁白。仅在设备连接到以太网时可用。适用于 macOS 11 及更高版本。
    - 生物特征识别：阻止用户设置 Touch ID 和面容 ID。适用于 macOS 10.12.4 及更高版本。
    - 原彩：阻止用户设置四通道传感器以动态调整显示器的白平衡。适用于 macOS 10.13.6 及更高版本。
    - **Apple Pay**：阻止用户设置 Apple Pay。如果清除此设置，用户必须设置 Touch ID 和 Apple ID。确保清除 **Apple ID** 和生物特征识别设置。适用于 macOS 10.12.4 及更高版本。
    - 屏幕时间：阻止用户启用屏幕时间。适用于 macOS 10.15 及更高版本。

有关配置设置选项的详细信息，请参阅通过 Apple 部署计划部署设备

显示更新日志文件

故障排除菜单的日志命令行界面中提供了一个名为显示更新日志文件的新选项。使用此选项，可以查看更新日志内容的列表并提高故障排除效率。有关命令行界面工具的详细信息，请参阅命令行界面选项。

错误日志文件

查看故障排除和支持 > 日志中的日志时，现在可以查看显示从调试日志中过滤出的错误的日志。有关详细信息，请参阅在 XenMobile 中查看日志文件。

服务器属性

- 可以通过配置 `afw.allow.legacy.apps` 服务器属性来确定是否将旧版 Android 应用程序交付到 Android Enterprise 应用程序。有关详细信息，请参阅服务器属性。
- XenMobile Server 现在支持使用端口 2197 作为端口 443 的备用端口。您将使用端口 2197 发送和接收来自 `api.push.apple.com` 的 APN 通知。该端口使用基于 HTTP/2 的 APNs 提供程序 API。服务器属性 `apns.http2.alternate.port.enabled` 的默认值为 **`false`**。要使用端口 2197，请更新服务器属性，然后重新启动服务器。
- 密码验证可防止用户使用弱密码。将属性 `enable.password.strength.validation` 设置为 **`true`** 时，无法创建使用弱密码的本地用户。

VPN 虚拟服务器列表增强功能

如果 VPN 服务器名称不包括 `_XM_XenMobileGetway`，则 XenMobile Server 将选择列表中的第一个可用 VPN 虚拟服务器。

支持 **Citrix Launcher**

XenMobile Server 在 Android Enterprise 设备上支持 Citrix Launcher。有关详细信息，请参阅 Launcher 配置设备策略。

针对 **XenMobile Server** 的颜色焕新

XenMobile Server 与更新后的 Citrix 品牌颜色相符。

XenMobile Server 10.13 中的新增功能

January 5, 2022

XenMobile Server 10.13（PDF 下载）

继续支持 Citrix ADC 中已弃用的经典策略

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

XenMobile Migration Service

如果在本地使用 XenMobile Server，我们的免费 XenMobile Migration Service 可以让您开始使用 Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 不需要重新注册设备。

要开始迁移，请与当地的 Citrix 销售人员或 Citrix 合作伙伴联系。请参阅 XenMobile Migration Service。

弃用声明

有关正在逐步淘汰的 Citrix XenMobile 功能的预先通知，请参阅弃用。

在将端点升级到 iOS 14.5 之前的准备工作

Citrix 建议在将任何端点升级到 iOS 14.5 之前，执行以下操作以缓解应用程序崩溃情况：

- 将 Citrix Secure Mail 和 Secure Web 升级到 21.2.X 或更高版本。请参阅升级 MDX 或企业应用程序。
- 如果您使用的是 MDX Toolkit，请使用 MDX Toolkit 21.3.X 或更高版本封装所有第三方 iOS 应用程序。请访问 MDX Toolkit 下载页面以获取最新版本。

升级本地 Citrix ADC 之前的准备工作

将本地 Citrix ADC 升级到某个版本会导致出现单点登录错误。在浏览器中通过企业员工登录选项单点登录到 Citrix Files 或 ShareFile 域 URL 会导致出现错误。用户无法登录。

要解决此问题，请执行以下操作：如果您尚未从 Citrix Gateway 上的 ADC CLI 运行以下命令，请运行该命令以启用全局 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（功能阶段）13.0 Build 67.39/67.43
- 影响的 SSO 配置

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

升级到 **XenMobile 10.13**（本地）之前的准备工作

某些系统要求发生了变化。有关信息，请参阅系统要求和兼容性和 XenMobile 兼容性。

1. 如果运行要升级的 XenMobile Server 的虚拟机的 RAM 低于 8 GB，我们建议您将 RAM 增加到至少 8 GB。
2. 请先将您的 Citrix 许可证服务器更新到 11.16 或更高版本，然后再更新到最新版本的 XenMobile Server 10.13。

   最新版本的 XenMobile 需要 Citrix 许可证服务器 11.16（最低版本）。

   > 注意：
   >
   > XenMobile 10.13 中的 Customer Success Services 日期（以前称为专享升级服务日期）为 2020 年 9 月 29 日。Citrix 许可证上的 Customer Success Services 日期必须晚于此日期。
   >
   > 可以在许可证服务器中的许可证旁边查看该日期。如果要将最新版本的 XenMobile 连接到较旧的许可证服务器环境，连接检查将失败，并且您无法配置许可证服务器。

   要续订许可证上的日期，请从 Citrix 门户下载最新的许可证文件并将该文件上载到许可服务器。请参阅 Customer Success Services。
3. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序具有以下要求。如果为 Citrix Gateway 配置了 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
4. 建议：安装 XenMobile 更新之前，请使用 VM 中的功能创建系统的快照。此外，还请备份您的系统配置数据库。如果您在升级过程中遇到问题，请完成允许您还原的备份。

升级

在本版本中，XenMobile 支持 VMware ESXi 7.0。请务必在安装或升级 ESXi 7.0 之前升级到 10.13。

可以从 XenMobile 10.12.x 或 10.11.x 直接升级到 XenMobile 10.13。要执行升级，请下载可用的最新二进制文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server >** 产品软件 **> XenMobile Server 10**。在您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击下载文件。

要上载升级，请使用 XenMobile 控制台中的发布管理页面。请参阅使用“发布管理”页面进行升级。

升级之后需要执行的操作

如果涉及传出连接的功能停止运行，并且您尚未更改自己的连接配置，请在 XenMobile Server 日志中检查是否存在如下所示的错误：“Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”（无法连接到 VPP 服务器: 主机名 192.0.2.0 与对等机提供的证书使用者不匹配）

- 证书验证错误意味着您必须禁用 XenMobile Server 上的主机名验证。
- 默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。
- 如果主机名验证中断了您的部署，请将服务器属性 `disable.hostname.verification` 更改为 **`true`**。此属性的默认值为 **`false`**。

平台支持更新

- **iOS 14**： XenMobile Server 和 Citrix 移动生产力应用程序与 iOS 14 兼容，但目前不支持任何新 iOS 14 功能。请使用 MDX Toolkit 20.8.5 或更高版本或者使用 MAM SDK 准备这些应用程序。
- **Android 11**：XenMobile Server 支持 Android 11。有关弃用 Google 设备管理 API 如何影响运行 Android 10+ 的设备的信息，请参阅从设备管理迁移到 Android Enterprise。另请参阅此 Citrix 博客。

在单个环境中配置多个设备和应用程序管理模式

现在，您可以将单个 XenMobile 站点配置为支持多种注册配置。注册配置文件的角色扩展为包括设备和应用程序管理的注册设置。

注册配置文件在单个 XenMobile 控制台中支持多个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 注册的功能）
- 将 Android 设备管理员注册迁移到 Android Enterprise 注册（完全托管、工作配置文件、专用设备）

注册配置文件替换现已弃用的服务器属性 `xms.server.mode`。此更改不会影响您的现有交付组和已注册的设备。

如果不需要注册专用设备，则可以通过将服务器属性 `enable.multimode.xms` 设置为 **`false`** 来禁用此功能。请参阅服务器属性。

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：

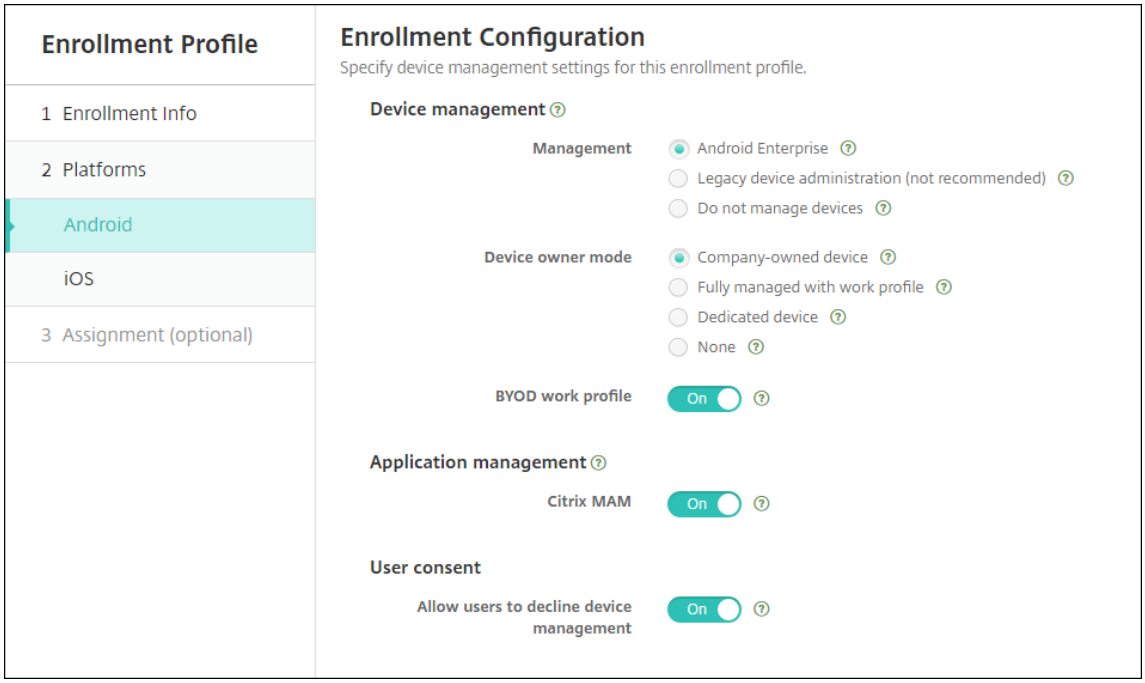
现有服务器属性	新管理模式
ENT 模式 (iOS)	Apple 设备在 Citrix MAM 中的注册
ENT 模式 (Android)	使用 Citrix MAM 的传统设备管理员

现有服务器属性	新管理模式
ENT 模式 (Android Enterprise)	使用 Citrix MAM 的完全托管（以前称为 COPE）设备上的工作配置文件
MAM 模式（iOS 和 Android）	Citrix MAM
MDM 模式 (iOS)	Apple 设备注册
MDM 模式 (Android)	传统设备管理员
MDM 模式 (Android Enterprise)	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。如果未附加注册配置文件，XenMobile 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)** 模式更轻松地迁移到 **Android Enterprise**。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。请参阅 Android Enterprise。



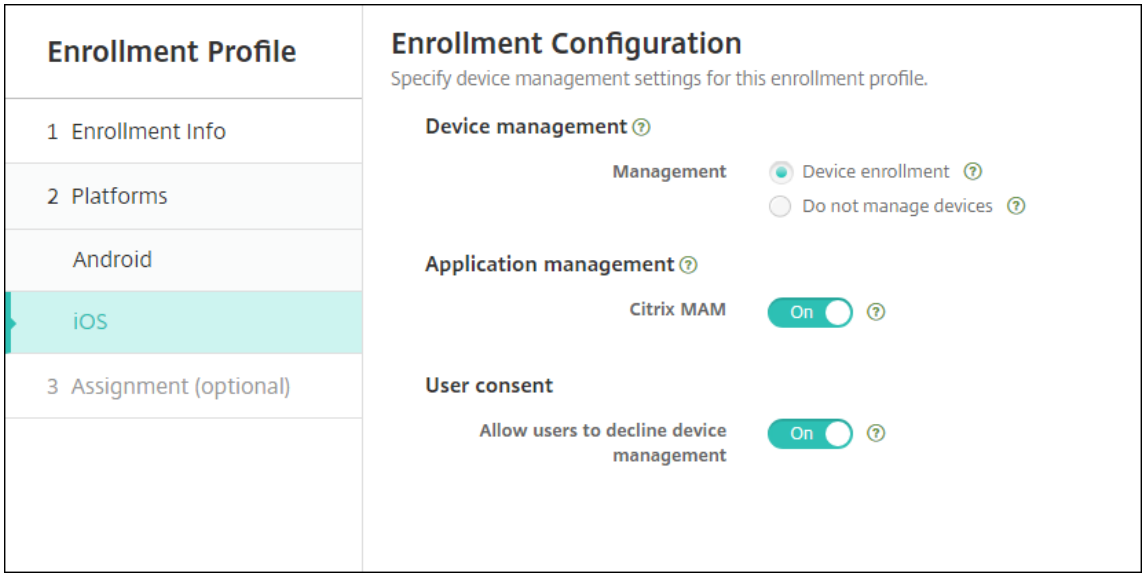
对于此升级，当前服务器模式和设置 **> Android Enterprise** 的 XenMobile 配置映射到新注册配置文件设置，如下所示。

当前配置	管理环境	设备所有者模式设置	Citrix MAM 设置
MDM。托管 Google Play (Android Enterprise)	Android Enterprise	完全托管设备上的工作配置文件	关
MDM；G Suite（传统 DA）	传统 DA	不适用	关
MAM	不管理设备	不适用	开
MDM+MAM。托管 Google Play (Android Enterprise)	Android Enterprise*	完全托管设备上的工作配置文件	开
MDM+MAM; G Suite (传统 DA)	传统 DA*	不适用	开

* 如果需要注册，允许用户拒绝设备管理设置为关。

升级后，您的当前注册配置文件将反映这些映射。请考虑您是否要在从传统 DA 过渡时创建其他注册配置文件来处理任何新用例。

- 更轻松地管理 **iOS**。对于 iOS 设备，设置包括在将设备注册为托管设备或非托管设备之间进行选择。



对于此升级，您之前的配置将映射到新注册配置文件设置，如下所示。

服务器模式	管理环境	Citrix MAM 设置
MDM	设备注册	关
MAM	不管理设备	开

服务器模式	管理环境	Citrix MAM 设置
MDM+MAM	设备注册	开

如果需要注册，允许用户拒绝设备管理设置为关。

增强的注册配置文件存在以下限制：

- 增强的注册配置文件功能不适用于一次性 PIN 或双重身份验证注册邀请。

请参阅注册配置文件。

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文件协议的支持将于 2021 年 3 月 31 日结束。Apple 建议您改为使用基于 HTTP/2 的 APNs 提供程序 API。XenMobile Server 现在支持基于 HTTP/2 的 API。有关更多信息，请参阅 https://developer.apple.com/ 中的新闻更新 “Apple 推送通知服务更新”。有关检查与 APN 的连接的帮助，请参阅连接检查。

默认情况下，以下版本的 XenMobile Server 启用对基于 HTTP/2 的 API 的支持：

- XenMobile Server 10.13
- XenMobile Server 10.12 滚动修补程序 5 及更高版本

如果使用以下版本的 XenMobile Server，则必须添加服务器属性 **apple.apns.http2** 以启用支持：

- XenMobile Server 10.12 滚动修补程序 2-4 及更高版本
- XenMobile Server 10.11 滚动修补程序 5 及更高版本

我们不再支持 XenMobile Server 10.11，建议您升级到最新版本。

在许多 **iOS** 设备上使用基于设备证书的 **IPSec VPN**

无需为每个需要基于设备证书的 IPSec VPN 的 iOS 设备配置 VPN 设备策略和凭据设备策略，自动执行该过程即可。

1. 使用 **Always on IKEv2**（始终启用 IKEv2）连接类型配置 iOS VPN 设备策略。
2. 选择基于设备标识的设备证书作为设备身份验证方法。
3. 选择要使用的设备标识类型。
4. 使用 REST API 批量导入您的设备证书。

有关配置 VPN 设备策略的详细信息，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 批量上载证书。

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）时，您现在可以为所有 iOS 应用启用自动更新。请参阅 Apple 批量购买中的应用程序自动更新设置。

本地用户帐户的密码要求

在 XenMobile 控制台中添加或编辑本地用户帐户时，请务必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。

- 密码要求：在 XenMobile Server 控制台中添加或编辑本地用户帐户时，请遵循最新的密码要求。请参阅添加本地用户帐户。
- 本地用户帐户锁定：如果用户达到连续无效登录尝试的最大次数，则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 XenMobile Server 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。请参阅解锁本地用户帐户。

设备策略

为 Android Enterprise 设备添加了新的设备策略和设备策略设置。

隐藏 **Android Enterprise** 设备上的托盘栏图标

您现在可以选择 Android Enterprise 设备的托盘栏图标是隐藏的还是可见的。请参阅 XenMobile 选项设备策略。

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：

- 配置特定托管应用程序使用的证书。Android Enterprise 的“凭据”设备策略现在包含使用证书的应用程序设置。可以指定要使用在此策略中选择的凭据提供商颁发的用户证书的应用程序。应用程序在运行期间被无提示授予对证书的访问权限。要对所有应用程序使用证书，请将应用程序列表留空。请参阅凭据设备策略。
- 从托管密钥库中无提示删除证书或卸载所有非系统 **CA** 证书。请参阅凭据设备策略。
- 防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，该设置设为开。请参阅限制设备策略。

在 **Android Enterprise** 托管配置中更轻松地使用证书别名

将凭据设备策略中的新证书别名设置与 **Android Enterprise** 托管配置设备策略一起使用。这样做将允许应用程序在 VPN 上进行身份验证，而无需用户操作。您可以创建凭据别名，而非在应用程序日志中查找凭据别名。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中的证书别名设置中键入相同的证书别名。请参阅 Android Enterprise 托管配置策略和凭据设备策略。

控制 **Android Enterprise** 设备上的 **“Use one lock”**（使用一个锁）设置

通过通行码设备策略中的新启用统一通行码设置，您可以控制设备是否需要为设备和工作配置文件提供单独的通行码。在此设置之前，用户使用设备上的 **Use one lock**（使用一个锁）设置来控制此行为。启用统一通行码设置为开时，用户可以对设备使用与工作配置文件相同的通行码。如果启用统一通行码设置为关，用户将无法对设备使用与工作配置文件相同的通行码。默认值为关。**Enable unified lock**（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。请参阅通行码设备策略。

在 **Android Enterprise** 设备上显示不合规的应用程序和快捷方式

Android Enterprise 的通行码设备策略有一项新设置，即在通行码不合规时显示应用程序和快捷方式。启用该设置可在设备通行码不再合规时使应用程序和快捷方式保持可见。Citrix 建议您创建一项自动操作，以便在通行码不合规时将设备标记为不合规。请参阅通行码设备策略。

禁用在 **Android Enterprise** 工作配置文件设备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。请参阅 Android Enterprise 设置。

通过在 **Kiosk** 策略中添加应用程序软件包名称，允许应用程序在专用设备上运行

现在，您可以输入要允许在 Android Enterprise 平台上运行的软件包名称。请参阅 Android Enterprise 设置。

管理面向 **Android Enterprise** 工作配置文件和完全托管设备的键盘锁功能

Android 键盘锁管理设备和工作挑战锁定界面。使用“键盘锁管理”设备策略控制：

- 工作配置文件设备上的键盘锁管理。可以在用户解锁设备键盘锁和工作质询键盘锁之前指定其可用的功能。例如，默认情况下，用户可以使用指纹解锁并在锁定屏幕上查看未编辑的通知。还可以使用键盘锁管理策略来禁用运行 Android 9.0 及更高版本的设备的所有生物特征身份验证。
- 在完全托管设备和专用设备上进行键盘锁管理。可以指定可用的功能，例如信任代理和安全摄像头，然后才能解锁键盘锁屏幕。或者，可以选择禁用所有键盘锁功能。

请参阅键盘锁管理设备策略。

在 **XenMobile** 控制台中发布适用于 **Android Enterprise** 的企业应用程序

添加 Android Enterprise 专用应用程序时，不再需要注册 Google Play 开发者帐户。XenMobile 控制台打开托管 Google Play 应用商店 UI，供您上载和发布 APK 文件。有关详细信息，请参阅添加企业应用程序。

在 **XenMobile** 控制台中发布适用于 **Android Enterprise** 的 **Web** 应用程序

您无需再访问托管 Google Play 或 Google 开发者门户即可发布适用于 XenMobile 的 Android Enterprise Web 应用程序。单击配置 **>** 应用程序 **> Web** 链接中的上载时，将打开一个托管 Google Play 应用商店用户界面，供您上载和保存文件。应用程序审批和发布可能需要 10 分钟。有关详细信息，请参阅添加 Web 链接。

使用 **XenMobile Server REST API** 将证书批量上载到 **iOS** 设备

如果一次上载一个证书并不现实，请使用 XenMobile Server REST API 将证书批量上载到 iOS 设备。

1. 使用 **Always on IKEv2**（始终启用 IKEv2）连接类型配置 iOS VPN 设备策略。
2. 选择基于设备标识的设备证书作为设备身份验证方法。
3. 选择要使用的设备标识类型。
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 将证书批量上载到 iOS 设备。

刷新加密密钥

刷新加密密钥选项将添加到 XenMobile CLI 的高级设置中。可以使用此选项一次刷新一个节点的加密密钥。请参阅系统选项。

ESXi 7.0 支持

在本版本中，XenMobile 支持 VMware ESXi 7.0。请务必在安装或升级 ESXi 7.0 之前升级到 10.13。

新服务器属性

现在可以使用以下服务器属性：

- **Allow hostnames for iOS App Store links**（允许使用 iOS App Store 链接对应的主机名）：要使用公共 API 而非控制台添加适用于 iOS 的公共应用商店应用程序，请根据需要配置允许的主机名列表。
- **Local user account lockout limit**（本地用户帐户锁定限制）：配置本地用户在其帐户被锁定之前的登录尝试次数。
- **Local user account lockout time**（本地用户帐户锁定时间）：配置在登录尝试过多次失败后锁定本地用户的时间长度。
- **Maximum size of file upload restriction enabled**（启用了文件上载的最大大小限制的最大大小）：启用限制上载的文件的最大文件大小。
- **Maximum size of file upload allowed**（允许的文件上载的最大大小）：设置上载的文件的最大文件大小。

有关这些属性的更多详细信息，请参阅服务器属性。

自助磁盘清理

故障排除菜单中提供了一个名为磁盘使用情况的新命令行界面选项。此选项允许您查看核心转储文件和支持包文件的列表。查看该列表后，您可以选择通过命令行删除所有这些文件。有关命令行界面工具的详细信息，请参阅命令行界面选项。

XenMobile Server 10.12 中的新增功能

January 5, 2022

XenMobile Server 10.12（PDF 下载）

XenMobile Migration Service

如果在本地使用 XenMobile Server，我们的免费 XenMobile Migration Service 可以让您开始使用 Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 不需要重新注册设备。

要开始迁移，请与当地的 Citrix 销售人员或 Citrix 合作伙伴联系。有关详细信息，请参阅 XenMobile Migration Service。

弃用声明

有关正在逐步淘汰的 Citrix XenMobile 功能的预先通知，请参阅弃用。

为即将做出的更改准备您的 **Android** 设备

这些先前宣布的弃用会影响您的 Android 和 Android Enterprise 设备：

- Android 10 的设备管理 (DA) 注册：
  - **July 31, 2020**： Citrix 弃用旧版 Android 设备管理的新注册。
  - **November 1, 2020**： Google 弃用旧版设备管理 API。在旧版设备管理模式下运行的 Android 10 设备将不再运行。
- MDX 加密：
  - **August 1, 2020**： Citrix 开始强制 Citrix 移动生产力和第三方 MDX 应用程序从 MDX 加密迁移到平台加密。
  - **2020** 年 **9** 月 **1** 日： MDX 加密达到生命周期结束状态。

适用于在旧版 **DA** 中注册的设备

- 如果不使用 MDX 加密，则无需执行任何操作。

- 如果使用 MDX 加密，请在 2020 年 7 月 31 日之前将 Android 设备迁移到 Android Enterprise。运行 Android 10 的设备必须使用 Android Enterprise 注册或重新注册。此要求包括处于仅 MAM 模式的 Android 设备。请参阅从设备管理迁移到 Android Enterprise。

适用于截至 **7** 月 **31** 日已在 **Android Enterprise** 中注册的设备

- 如果使用 Android Enterprise 平台发布了应用程序，则已通过 Android Enterprise 处理加密。无需任何操作。
- 如果使用旧版 Android 平台发布了应用程序，请在 2020 年 7 月 31 日之前使用 Android Enterprise 重新发布应用程序。

升级到 **XenMobile 10.12**（本地）之前的准备工作

某些系统要求发生了变化。有关信息，请参阅系统要求和兼容性和 XenMobile 兼容性。

1. 请先将您的 Citrix 许可证服务器更新到 11.16 或更高版本，然后再更新到最新版本的 XenMobile Server 10.12。

   最新版本的 XenMobile 需要 Citrix 许可证服务器 11.16（最低版本）。

   > 注意：
   >
   > 如果要使用您自己的许可证进行预览，请知晓 XenMobile 10.12 中的 Customer Success Services 日期（以前称为专享升级服务日期）为 2020 年 1 月 20 日。Citrix 许可证上的 Customer Success Services 日期必须晚于此日期。
   >
   > 可以在许可证服务器中的许可证旁边查看该日期。如果要将最新版本的 XenMobile 连接到较旧的许可证服务器环境，连接检查将失败，并且您无法配置许可证服务器。

   要续订许可证上的日期，请从 Citrix 门户下载最新的许可证文件并将该文件上载到许可服务器。有关详细信息，请参阅 Customer Success Services。

2. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序具有以下要求。如果为 Citrix Gateway 配置了 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
3. 如果运行要升级的 XenMobile Server 的虚拟机的 RAM 低于 4 GB ，请将 RAM 增加到至少 4 GB。请谨记，对于生产环境，建议的最低 RAM 是 8 GB。
4. 建议：安装 XenMobile 更新之前，请使用 VM 中的功能创建系统的快照。此外，还请备份您的系统配置数据库。如果您在升级过程中遇到问题，请完成允许您还原的备份。

升级

可以从 XenMobile 10.11.x 或 10.10.x 直接升级到 XenMobile 10.12。要执行升级，请下载可用的最新二进制文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management (XenMobile) >**

XenMobile Server > 产品软件 **> XenMobile Server 10**。在您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击下载文件。

要上载升级，请使用 XenMobile 控制台中的发布管理页面。有关详细信息，请参阅使用“发布管理”页面进行升级。

升级之后需要执行的操作

升级到 XenMobile 10.12（本地）之后需要执行的操作

如果涉及传出连接的功能停止运行，并且您尚未更改自己的连接配置，请在 XenMobile Server 日志中检查是否存在如下所示的错误：“Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”（无法连接到 VPP 服务器: 主机名 192.0.2.0 与对等机提供的证书使用者不匹配）

证书验证错误指示您需要在 XenMobile Server 上禁用主机名验证。默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。如果主机名验证中断了您的部署，请将服务器属性 `disable.hostname.verification` 更改为 **`true`**。此属性的默认值为 **`false`**。

对 **iOS 13** 的其他支持

XenMobile Server 支持升级到 iOS 13 的设备。升级会影响您的用户，如下所示：

- 在注册过程中，将显示几个新的 iOS 设置助理选项屏幕。Apple 在 iOS 13 中增加了新的 iOS 设置助理选项屏幕。新选项包含在此版本的设置 **> Apple** 设备注册计划 **(DEP)** 页面中。可以将 XenMobile Server 配置为跳过这些屏幕。这些页面显示给 iOS 13 设备上的用户。
- 早期版本的 iOS 的受监督或不受监督设备上可用的某些限制设备策略设置仅适用于 iOS 13+ 的受监督设备。当前 XenMobile Server 控制台工具提示尚未指示这些设置仅适用于 iOS 13+ 的受监管设备。
  - 在允许硬件控制中：
    - FaceTime
    - 安装应用程序
  - 在允许使用应用程序中：
    - iTunes Store
    - Safari
    - Safari > 自动填充
  - 在网络 - 允许执行 iCloud 操作中：
    - iCloud 文档和数据
  - 在仅监管设置 - 允许中：
    - 游戏中心 > 添加好友
    - 游戏中心 > 多人游戏
  - 在媒体内容 - 允许中：
    - 成人音乐、博客及 iTunes U 资料

这些限制适用如下：

- 如果 iOS 12（或更低版本）设备已在 XenMobile Server 中注册，然后升级到 iOS 13，则上述限制将适用于未受监督和受监督的设备。
- 如果未受监督的 iOS 13+ 设备在 XenMobile Server 中注册，上述限制将仅适用于受监督的设备。
- 如果受监督的 iOS 13+ 设备在 XenMobile Server 中注册，上述限制将仅适用于受监督的设备。

Apple 批量购买计划迁移到 **Apple** 商务管理 **(ABM)** 和 **Apple** 校园教务管理 **(ASM)**

使用 Apple 批量购买计划 (VPP) 的公司和机构需要在 2019 年 12 月 1 日之前迁移到 Apple 商务管理或 Apple 校园教务管理中的“应用程序和图书”。

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

如果贵组织或学校仅使用批量购买计划 (VPP)，您可以在 ABM/ASM 中注册，然后邀请现有 VPP 购买者加入新的 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 XenMobile 上的 VPP 帐户，请执行以下操作：

1. 在 XenMobile 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 **iOS** 设置。此时将显示批量购买计划配置页面。
3. 确保您的 ABM 或 ASM 帐户具有与之前的 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 XenMobile 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购买帐户。
    b) 编辑您的 ABM 或 ASM 凭据。请勿更改后缀。
    c) 单击保存两次。

有关详细信息，请参阅：

- Apple 部署计划
- Apple 设备的批量注册

支持 **Android Enterprise COPE** 设备

XenMobile Server 支持具有工作配置文件的 Android Enterprise 完全托管设备，以前称为 COPE（企业拥有但由个人使用）的设备。这些设备是一种同时具有工作配置文件的 Android Enterprise 完全托管设备。您可以将单独的策略设置应用到设备和工作配置文件。对于此版本：

- 可以使用以下设备策略将单独的设置应用到设备和工作配置文件：凭据、通行码和限制。
- 可以将位置设备策略的位置模式设置应用到 COPE 设备本身，但不应用到 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。

- 可以将“锁定”安全操作单独应用到设备或工作配置文件。

设备策略

对于具有工作配置文件的 Android Enterprise 完全托管设备（COPE 设备），某些设备策略可以将单独的设置应用到整个设备和工作配置文件。在 XenMobile Server 控制台中，某些设备策略允许您应用单独的设置。可以使用其他设备策略将设置仅应用到整个设备或仅应用到具有工作配置文件的完全托管设备的工作配置文件。

安全操作

对于具有工作配置文件的 Android Enterprise 完全托管设备（COPE 设备），可以：

- 将“锁定”安全操作单独应用到设备或工作配置文件。
- 将所有其他安全操作应用到设备。

注册配置文件控制 **Android** 设备的注册选项

如果为 XenMobile 部署启用了 Android Enterprise，注册配置文件现在可以控制 Android 设备的注册方式。注册配置文件确定 Android 设备是在默认 Android Enterprise 模式（完全托管或工作配置文件）还是旧版（设备管理员）模式下注册。

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 Enterprise 设备注册为完全托管设备，并将 BYOD ndroid 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。

为 **Android Enterprise** 准备旧版 **Android** 设备作为默认注册

Google 即将弃用设备管理的设备管理员模式，并鼓励客户在设备所有者模式或配置文件所有者模式下管理所有 Android 设备。（请参阅 Google Android Enterprise 开发者指南中的设备管理员弃用。）为了支持此变更，Android Enterprise 现在是 Android 设备的默认注册选项。

此变更意味着，如果为您的 XenMobile 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。

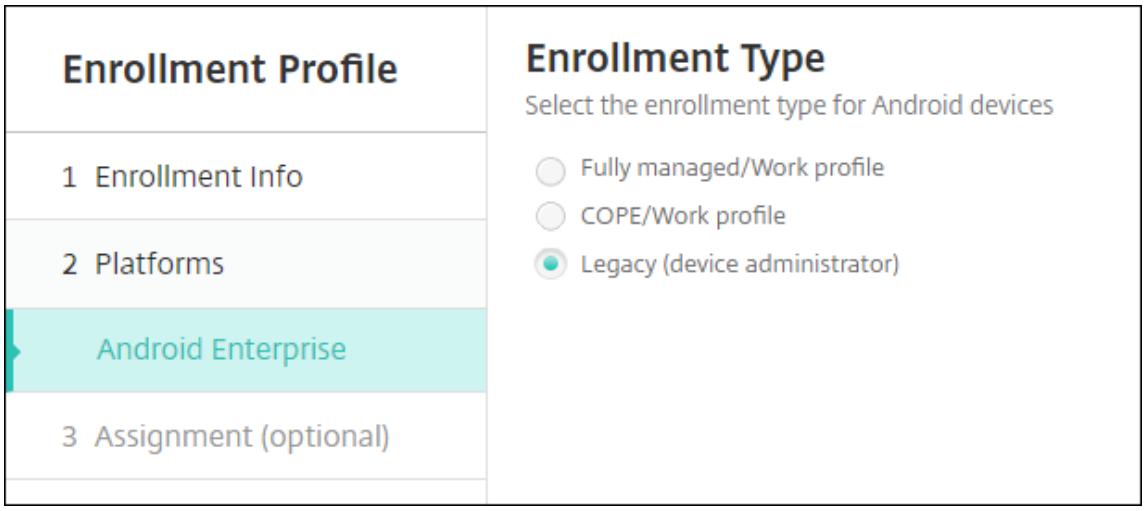
为了准备此变更，XenMobile 现在允许您创建注册配置文件，用于控制 Android 设备的注册方式。

贵组织可能尚未准备好开始在设备所有者模式或配置文件所有者模式下管理旧版 Android 设备。在这种情况下，您可以继续在设备管理员模式下进行管理。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：

1. 在 XenMobile 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。
3. 单击下一步或在平台下选择 **Android Enterprise**。此时将显示“注册配置”页面。

4. 将管理设置为旧版 (设备管理)。单击下一步或选择分配 (选项)。此时将显示交付组分配屏幕。



5. 请选择包含注册专用设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

要在设备管理员模式下继续管理旧版设备，请使用此配置文件注册或重新注册这些设备。可以通过让用户下载 Secure Hub 并提供注册服务器 URL 来注册与工作配置文件设备类似的设备管理员设备。

有关转换到 Android Enterprise 的 Endpoint Management 支持的详细信息，请参阅博客 Android Enterprise as default for Citrix Endpoint Management service (Android Enterprise 作为 Citrix Endpoint Management 服务的默认设置)。

简化了 **Android Enterprise** 的应用程序管理过程

不再需要访问托管 Google Play 或 Google 开发者门户来审批或发布面向 XenMobile Server 的应用程序。因此，应用程序审批和发布大约需要 10 分钟，而非几个小时。

在 **XenMobile Server** 控制台中审批面向公用应用商店的 **Android Enterprise** 应用程序。您现在可以审批托管 Google Play 应用商店应用程序，而无需离开 XenMobile Server 控制台。在搜索字段中输入应用程序名称后，托管 Google Play 应用商店 UI 将打开，其中包含审批和保存应用程序的说明。然后，您的应用程序在结果中填充，以便您配置其详细信息。请参阅添加公共应用商店应用程序。

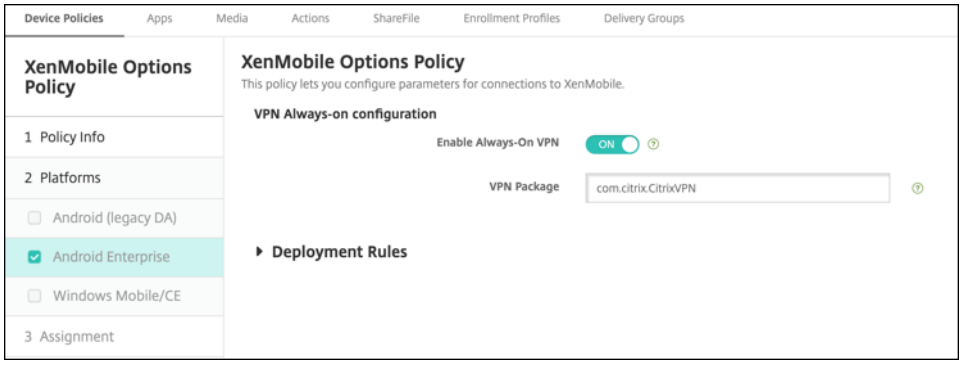
为 **Android Enterprise** 添加 **MDX** 应用程序。XenMobile Server 控制台现在支持将 Android Enterprise 作为 MDX 应用程序部署的平台。请参阅添加 MDX 应用程序。

在 **XenMobile Server** 控制台中审批适用于 **Android Enterprise** 的 **MDX** 应用程序。您现在可以审批适用于 Android Enterprise 的托管 Google Play 应用商店应用程序，而无需离开 XenMobile Server 控制台。上载 MDX 文件后，托管 Google Play 应用商店 UI 将打开，其中包含您审批和保存应用程序的说明。请参阅添加应用程序 MDX。

支持对 **Android Enterprise** 使用使用可用的 **VPN**

现在，XenMobile Server 选项设备策略现在允许您对 Android Enterprise 启用始终可用的 VPN。

为 Android Enterprise 配置 VPN 配置文件时，请在默认 **VPN** 配置文件中键入 VPN 配置文件的名称。用户在 Citrix SSO 应用程序的用户界面中轻按连接开关（而非轻按特定配置文件）时，XenMobile 使用此配置文件。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。



为您的 **Android Enterprise** 应用程序配置产品轨迹

在为 Android Enterprise 添加公共应用商店应用程序或 MDX 应用程序时，请配置要推送到用户设备的产品轨迹。例如，如果您有一个专为测试而设计的轨迹，则可以选择并将其分配给特定的交付组。要了解有关推出版本的更多信息，请参阅 Google Play 帮助中心。有关配置产品跟踪的信息，请参阅添加 MDX 应用程序或添加公共应用商店应用程序。

强制为 **macOS** 用户重置通行码

当 macOS 设备收到包含通行码策略的配置文件时，用户必须提供符合策略设置的通行码。现在，您可以在用户下次进行身份验证时强制重置通行码。在适用于 macOS 的“通行码”设备策略（10.13 及更高版本）中，启用新设置强制重置通行码。有关策略的详细信息，请参阅通行码设备策略。

XenMobile Server 10.11 中的新增功能

January 5, 2022

XenMobile Server 10.11（PDF 下载）

XenMobile Migration Service

如果在本地使用 XenMobile Server，我们的免费 XenMobile Migration Service 可以让您开始使用 Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 不需要重新注册设备。

要开始迁移，请与当地的 Citrix 销售人员或 Citrix 合作伙伴联系。有关详细信息，请参阅 XenMobile Migration Service。

Apple 批量购买计划迁移到 Apple 商务管理 (ABM) 和 Apple 校园教务管理 (ASM)

使用 Apple 批量购买计划 (VPP) 的公司和机构必须在 2019 年 12 月 1 日之前迁移到 Apple 商务管理或 Apple 校园教务管理中的“应用程序和图书”。

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

如果贵组织或学校仅使用批量购买计划 (VPP)，您可以在 ABM/ASM 中注册，然后邀请现有 VPP 购买者加入新的 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 XenMobile 上的批量购买（以前称为 VPP）帐户，请执行以下操作：

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击批量购买。此时将显示批量购买配置页面。
3. 确保您的 ABM 或 ASM 帐户具有与之前的 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 XenMobile 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购买帐户。
    b) 编辑您的 ABM 或 ASM 凭据。请勿更改后缀。
    c) 单击保存两次。

对 iOS 13 的其他支持

> 重要：
>
> 准备将设备升级到 iOS 12+：适用于 iOS 的 VPN 设备策略中的 Citrix VPN 连接类型不支持 iOS 12+。删除您的 VPN 设备策略，然后创建使用 Citrix SSO 连接类型的新 VPN 设备策略。
>
> 删除 VPN 设备策略后，Citrix VPN 连接将继续在以前部署的设备中运行。在用户注册期间，您的新 VPN 设备策略配置将在 XenMobile Server 10.11 中生效。

XenMobile Server 支持升级到 iOS 13 的设备。升级会影响您的用户，如下所示：

- 在注册过程中，将显示几个新的 iOS 设置助理选项屏幕。Apple 在 iOS 13 中增加了新的 iOS 设置助理选项屏幕。新选项不包含在此版本的设置 **> Apple** 设备注册计划 **(DEP)** 页面中。因此，您无法将 XenMobile Server 配置为跳过这些屏幕。这些页面显示给 iOS 13 设备上的用户。
- 早期版本的 iOS 的受监督或不受监督设备上可用的某些限制设备策略设置仅适用于 iOS 13+ 的受监督设备。当前 XenMobile Server 控制台工具提示尚未指示这些设置仅适用于 iOS 13+ 的受监管设备。
    - 在允许硬件控制中：
        * FaceTime
        * 安装应用程序

  - 在允许使用应用程序中：
    * iTunes Store
    * Safari
    * Safari > 自动填充
  - 在网络 - 允许执行 iCloud 操作中：
    * iCloud 文档和数据
  - 在仅监管设置 - 允许中：
    * 游戏中心 > 添加好友
    * 游戏中心 > 多人游戏
  - 在媒体内容 - 允许中：
    * 成人音乐、博客及 iTunes U 资料

这些限制适用如下：

- 如果 iOS 12（或更低版本）设备已在 XenMobile Server 中注册，然后升级到 iOS 13，则上述限制将适用于未受监督和受监督的设备。
- 如果未受监督的 iOS 13+ 设备在 XenMobile Server 中注册，上述限制将仅适用于受监督的设备。
- 如果受监督的 iOS 13+ 设备在 XenMobile Server 中注册，上述限制将仅适用于受监督的设备。

iOS 13 和 **macOS 15** 中对可信证书的要求

Apple 对 TLS 服务器证书有新的要求。验证所有证书都符合 Apple 的新要求。请参阅 Apple 出版物 https://support.apple.com/en-us/HT210176。有关管理证书方面的帮助，请参阅在 XenMobile 中上载证书。

从 **GCM** 升级到 **FCM**

截至 2018 年 4 月 10 日，Google 弃用了 Google Cloud Messaging (GCM)。Google 于 2019 年 5 月 29 日删除了 GCM 服务器和客户端 API。

> 重要要求：
>
> - 升级到最新版本的 XenMobile Server。
> - 升级到最新版本的 Secure Hub。

Google 建议您立即升级到 Firebase Cloud Messaging (FCM) 以开始充分利用 FCM 中提供的新功能。有关 Google 的信息，请参阅https://developers.google.com/cloud-messaging/faq和https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html。

继续支持向您的 Android 设备发送推送通知：如果您将 GCM 与 XenMobile Server 结合使用，请迁移到 FCM。然后，请使用 Firebase Cloud Messaging 控制台提供的新 FCM 密钥更新 XenMobile Server。

使用可信证书时，以下步骤将反映注册工作流程。

升级步骤：

1. 请按照 Google 提供的信息，从 GCM 升级到 FCM。

2. 在 Firebase Cloud Messaging 控制台中，复制新 FCM 密钥。您在下一个步骤中需要该密钥。
3. 在 XenMobile Server 控制台中，转至设置 **> Firebase Cloud Messaging** 并配置设置。

设备下次在 XenMobile Server 中签入并执行策略刷新时将切换到 FCM。要强制 Secure Hub 刷新策略，请执行以下操作：在 Secure Hub 中，转至首选项 **>** 设备信息，然后轻按刷新策略。
有关配置 FCM 的详细信息，请参阅 Firebase Cloud Messaging。

XenMobile Migration Service

如果在本地使用 XenMobile Server，我们的 XenMobile Migration Service 可以让您开始使用 Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 不需要重新注册设备。

要了解详细信息，请联系您的本地 Citrix 销售人员、系统工程师或 Citrix Partner。以下博客探讨了 XenMobile Migration Service：

New XenMobile Migration Service（新 XenMobile Migration Service）

Making the Case for XenMobile in the Cloud（用作云中的 XenMobile 的示例）

升级到 **XenMobile 10.11**（本地）之前的准备工作

某些系统要求发生了变化。有关信息，请参阅系统要求和兼容性和 XenMobile 兼容性。

1. 请先将您的 Citrix 许可证服务器更新到 11.15 或更高版本，然后再更新到最新版本的 XenMobile Server 10.11。

   最新版本的 XenMobile 需要 Citrix 许可证服务器 11.15（最低版本）。

   > 注意：
   >
   > 如果要使用您自己的许可证进行预览，请知晓 XenMobile 10.11 中的 Customer Success Services 日期（以前称为专享升级服务日期）为 2019 年 4 月 9 日。Citrix 许可证上的 Customer Success Services 日期必须晚于此日期。
   >
   > 可以在许可证服务器中的许可证旁边查看该日期。如果要将最新版本的 XenMobile 连接到较旧的许可证服务器环境，连接检查将失败，并且您无法配置许可证服务器。

   要续订许可证上的日期，请从 Citrix 门户下载最新的许可证文件并将该文件上载到许可服务器。有关详细信息，请参阅 Customer Success Services。

2. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序具有以下要求。如果为 Citrix Gateway 配置了 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
3. 如果运行要升级的 XenMobile Server 的虚拟机的 RAM 低于 4 GB ，请将 RAM 增加到至少 4 GB。请谨记，对于生产环境，建议的最低 RAM 是 8 GB。
4. 建议：安装 XenMobile 更新之前，请使用 VM 中的功能创建系统的快照。此外，还请备份您的系统配置数据库。如果您在升级过程中遇到问题，请完成允许您还原的备份。

升级

可以从 XenMobile 10.10.x 或 10.9.x 直接升级到 XenMobile 10.11。要执行升级，请下载可用的最新二进制文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management**（和 **Citrix XenMobile Server**）**> XenMobile Server (**本地**) >** 产品软件 **> XenMobile Server 10**。在您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击下载文件。

要上载升级，请使用 XenMobile 控制台中的发布管理页面。有关详细信息，请参阅使用“发布管理”页面进行升级。

升级之后需要执行的操作

升级到 XenMobile 10.11（本地）之后需要执行的操作

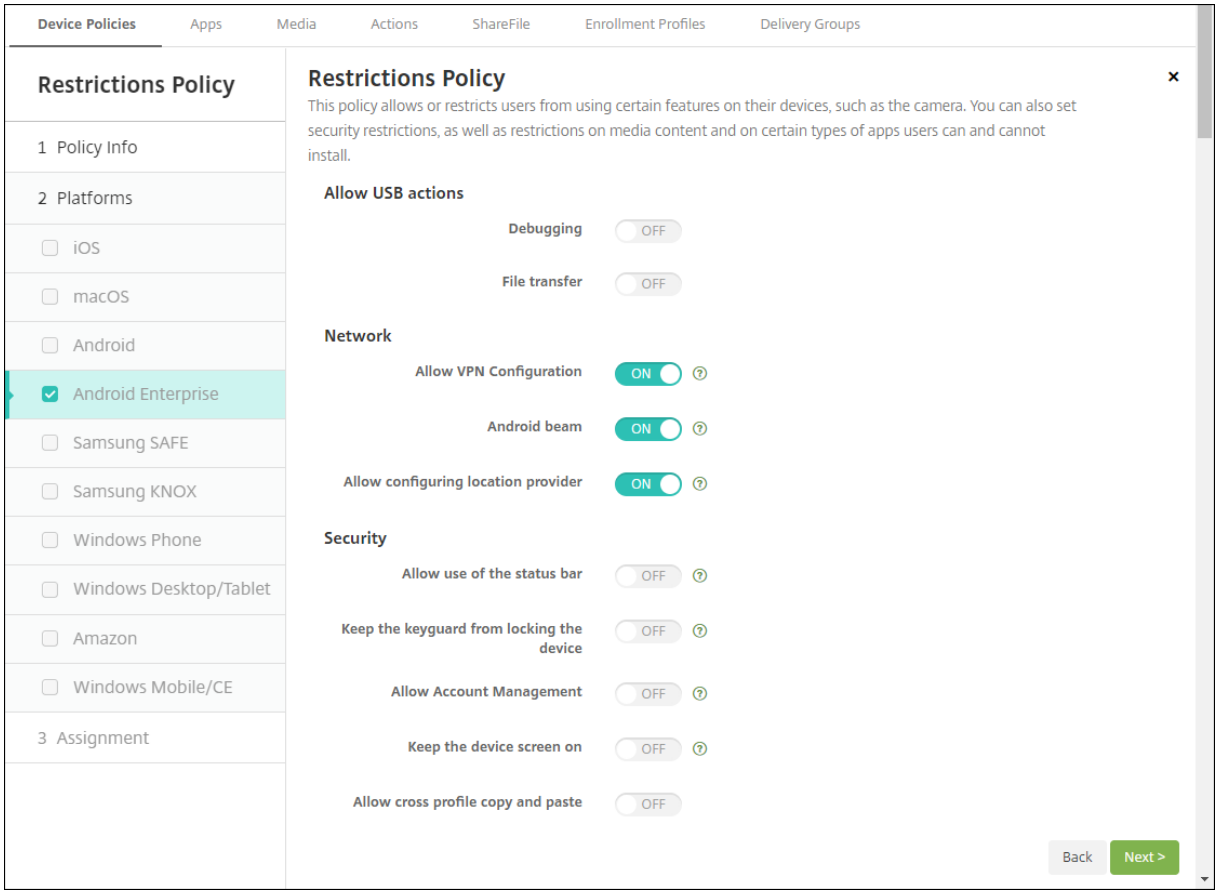
如果涉及传出连接的功能停止运行，并且您尚未更改自己的连接配置，请在 XenMobile Server 日志中检查是否存在如下所示的错误：“Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”（无法连接到 VPP 服务器: 主机名 192.0.2.0 与对等机提供的证书使用者不匹配）

证书验证错误指示您需要在 XenMobile Server 上禁用主机名验证。默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。如果主机名验证中断了您的部署，请将服务器属性 `disable.hostname.verification` 更改为 **`true`**。此属性的默认值为 **`false`**。

适用于 **Android Enterprise** 设备的新设备策略设置和更新后的设备策略设置

Samsung Knox 和 **Android Enterprise** 策略统一。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 将合并为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：

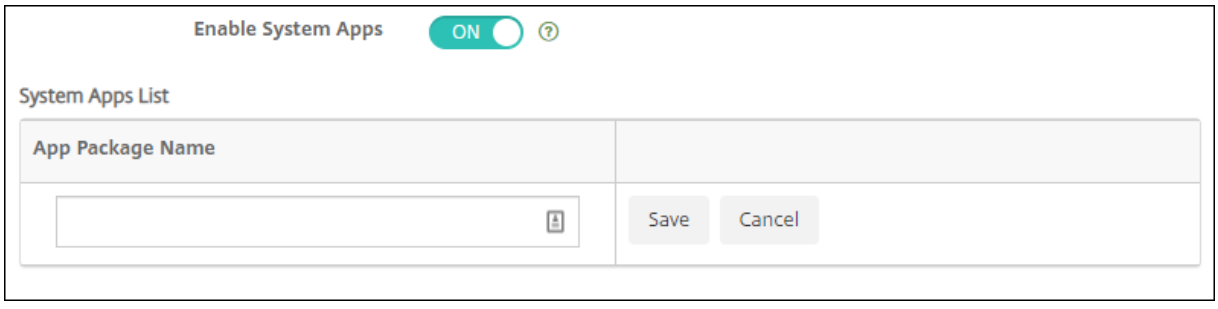
- 操作系统更新设备策略。包括适用于 Samsung Enterprise FOTA 更新的设置。
- 通行码设备策略。
- **Samsung MDM** 许可证密钥设备策略。配置 Knox 许可证密钥。
- **“限制”** 设备策略设置。



适用于 **Android Enterprise** 的应用程序清单设备策略。您现在可以在托管设备上收集 Android Enterprise 应用程序的清单。请参阅应用程序清单设备策略。

访问托管 **Google Play** 应用商店中的所有 **Google Play** 应用程序。访问托管 **Google Play** 应用商店中的所有应用程序服务器属性使得公共 Google Play 应用商店中的所有应用程序可从托管 Google Play 应用商店访问。将此属性设置为 **true** 会将所有 Android Enterprise 用户的公共 Google Play 应用商店应用程序列入允许列表。然后，管理员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。该配置授予用户对默认设备应用程序的访问权限，例如摄像头、库和其他应用程序。要限制对特定应用程序的访问，请使用 Android Enterprise 应用程序权限设备策略设置应用程序权限。



支持 **Android Enterprise** 专用设备。XenMobile 现在支持管理专用设备，以前称为企业拥有、单一用途 (COSU) 设备。

专用 Android Enterprise 设备属于完全托管设备，专门用于满足单个用例。您将这些设备限制为执行此用例需要执行的任务所需的一个应用程序或一小组应用程序。您还将阻止用户启用其他应用程序或在设备上执行其他操作。

有关预配 Android Enterprise 设备的信息，请参阅预配专用 Android Enterprise 设备。

已重命名策略。为了与 Google 术语保持一致，Android Enterprise 应用程序限制设备策略现在称为 Android Enterprise 托管配置。请参阅 Android Enterprise 托管配置设备策略。

锁定和重置 **Android Enterprise** 的密码

XenMobile 现在支持针对 Android Enterprise 设备的锁定和重置密码安全操作。这些设备必须在运行 Android 8.0 及更高版本的工作配置文件模式下注册。

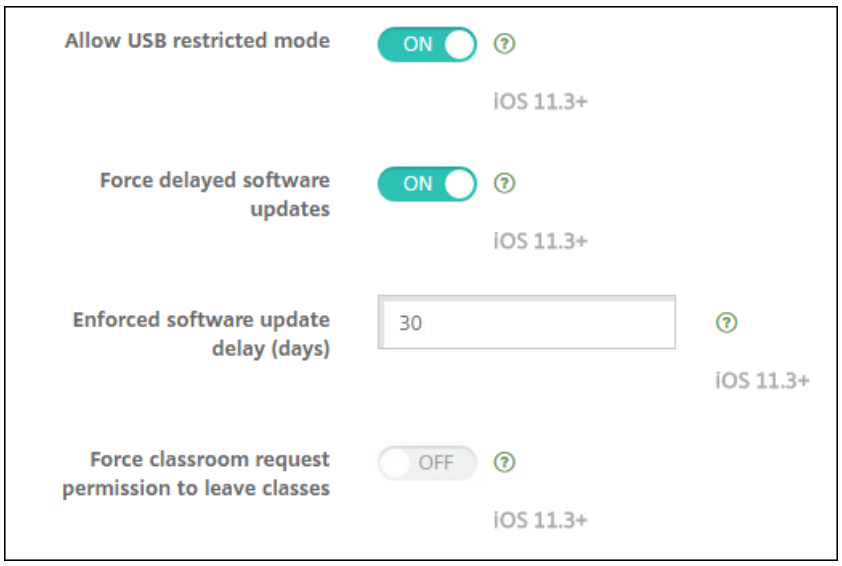
- 发送的密码将锁定工作配置文件。设备不会被锁定。
- 如果未发送通行码或发送的通行码不符合通行码要求：
  - 并且尚未在工作配置文件中设置通行码，设备将被锁定。
  - 并且已在工作配置文件中设置密码，工作配置文件将锁定，但设备不锁定。

有关锁定和重置通行码安全操作的详细信息，请参阅安全操作。

面向 **iOS** 和 **macOS** 的新 **“限制”** 设备策略

- 非托管应用程序读取托管联系人：可选。仅当非托管应用程序中来自托管应用程序的文档处于禁用状态时才可用。如果启用，则非托管应用程序可以读取托管帐户的联系人数据。默认值为关。截至 iOS 12 适用。
- 托管应用程序写入非托管联系人：可选。如果启用，则允许托管应用程序将联系人写入非托管帐户的联系人。如果非托管应用程序中来自托管应用程序的文档处于启用状态，则此限制无效。默认值为关。截至 iOS 12 适用。
- 密码自动填充：可选。如果禁用，用户将无法使用 “自动填充密码” 或 “自动使用强密码” 功能。默认值为开。截至 iOS 12 和 macOS 10.14 适用。
- 密码邻近请求：可选。如果禁用，用户的设备将不从附近的设备请求密码。默认值为开。截至 iOS 12 和 macOS 10.14 适用。
- 密码共享：可选。如果禁用，用户将无法使用 “AirDrop 密码” 功能共享其密码。默认值为开。截至 iOS 12 和 macOS 10.14 适用。
- 强制自动填写日期和时间：受监督。如果启用，用户将无法禁用选项常规 **>** 日期和时间 **>** 自动设置。默认值为关。截至 iOS 12 适用。
- 允许 **USB** 受限模式：仅适用于受监管的设备。如果设置为 “关”，设备在锁定状态下可以始终连接到 USB 附属设施。默认值为开。截至 iOS 11.3 可用。
- 强制执行延迟的软件更新：仅适用于受监管的设备。如果设置为开，则延迟软件更新的用户可见性。设置此限制后，用户在软件更新发布日期后的指定天数之后才能看到软件更新。默认值为关。截至 iOS 11.3 和 macOS 10.13.4 适用。

- 强制执行的软件更新延迟 **(**天**)**：仅适用于受监管的设备。此限制允许管理员设置在设备上延迟软件更新的时间长度。最大值为 90 天，默认值为 **30** 天。截至 iOS 11.3 和 macOS 10.13.4 适用。
- 强制课堂申请离开课程的权限：仅适用于受监督的设备。如果设置为开，通过“课堂”应用程序在非托管课程中注册的学生在尝试离开课程时将向教师申请权限。默认值为关。截至 iOS 11.3 可用。



请参阅限制设备策略。

面向 **iOS** 或 **macOS** 的 **“Exchange”** 设备策略更新

自 **iOS 12** 起，更多 **S/MIME“Exchange”** 签名和加密设置。“Exchange”设备策略现在包括用于配置 S/MIME 签名和加密的设置。

对于 S/MIME 签名：

- 签署身份凭据：选择要使用的签名凭据。
- **S/MIME** 签名用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 签名。默认值为关。
- **S/MIME** 签名证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中选择要使用的签名凭据。默认值为关。

对于 S/MIME 加密：

- 加密身份凭据：选择要使用的加密凭据。
- 启用 **“**为消息单独设置 **S/MIME”** 开关：设置为开时，向用户显示一个选项，用于为其撰写的每条消息打开或关闭 S/MIME 加密。默认值为关。
- 默认 **S/MIME** 加密用户可替代：如果设置为 **“**开**”**，用户可以在其设备的设置中选择 **S/MIME** 是否默认处于打开状态。默认值为关。
- **S/MIME** 加密证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 加密身份和加密。默认值为关。

自 **iOS 12** 起，**Exchange OAuth** 设置。您现在可以将与 Exchange 的连接配置为使用 OAuth 进行身份验证。

自 **macOS 10.14** 起，**Exchange OAuth** 设置。您现在可以将与 Exchange 的连接配置为使用 OAuth 进行身份验证。对于使用 OAuth 进行身份验证，可以为不使用自动发现的设置指定登录 URL。

请参阅 Exchange 设备策略。

面向 **iOS** 的 **“**邮件**”** 设备策略更新

自 **iOS 12** 起，更多 **S/MIME“Exchange”** 签名和加密设置。“邮件”设备策略包括用于配置 S/MIME 签名和加密的更多设置。

对于 S/MIME 签名：

- 启用 **S/MIME** 签名：选择此帐户是否支持 S/MIME 签名。默认值为开。设置为开时，将显示以下两个字段。
  - **S/MIME** 签名用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 签名。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - **S/MIME** 签名证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中选择要使用的签名凭据。默认值为关。此选项适用于 iOS 12.0 及更高版本。

对于 S/MIME 加密：

- 启用 **S/MIME** 加密：选择此帐户是否支持 S/MIME 加密。默认值为关。设置为开时，将显示以下两个字段。
  - 启用 **“**为消息单独设置 **S/MIME”** 开关：设置为开时，向用户显示一个选项，用于为其撰写的每条消息打开或关闭 S/MIME 加密。默认值为关。
  - 默认 **S/MIME** 加密用户可替代：如果设置为 **“**开**”**，用户可以在其设备的设置中选择 **S/MIME** 是否默认处于打开状态。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - **S/MIME** 加密证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 加密身份和加密。默认值为关。此选项适用于 iOS 12.0 及更高版本。

请参阅邮件设备策略。

面向 **iOS** 的 **“**应用程序通知**”** 设备策略更新

以下应用程序通知设置自 iOS 12 起可用。

- 在 **CarPlay** 中显示：如果设置为开，通知将在 Apple CarPlay 中显示。默认值为开。
- 启用严重警报：如果设置为开，应用程序可以将通知标记为忽略“请勿打扰”和铃声设置的关键通知。默认值为关。

请参阅应用程序通知设备策略

支持用于 **Apple** 教育的共用 **iPad**

XenMobile 与 Apple 教育的集成功能现在支持共用的 iPad。课堂中的多个学生可以共享一个 iPad，学习一位或多位教师教授的不同学科。

您或教师注册共用的 iPad，然后将设备策略、应用程序和媒体部署到这些设备。之后，学生提供其托管 Apple ID 凭据以登录共用的 iPad。如果您以前为学生部署了“教育配置”策略，这些学生将不再以“其他用户”身份登录共享设备。

共用的 iPad 的必备条件：

- 任意 iPad Pro、iPad 第五代、iPad Air 2 或更高版本以及 iPad mini 4 或更高版本
- 至少 32 GB 存储空间
- 受监督

有关详细信息，请参阅配置共用的 iPad。

基于角色的访问控制 (RBAC) 权限更改

RBAC 权限“添加/删除本地用户”现在分为两种权限：“添加本地用户”和“删除本地用户”。

有关详细信息，请参阅使用 RBAC 配置角色。

第三方声明

January 5, 2022

此版本的 XenMobile 可能包含根据以下文档定义的条款获得许可的第三方软件：

XenMobile 第三方声明

弃用

January 5, 2022

本文的声明旨在提前通知您正在逐渐淘汰的 XenMobile Server 功能。我们提供此信息，以便您能够及时做出业务决策。Citrix 将监视客户使用情况和反馈以确定其退出时间。在后续版本中声明可能会有更改，可能不会包括每个弃用的特性或功能。有关产品生命周期支持的详细信息，请参阅 Product Lifecycle Support Policy（产品生命周期支持策略）一文。

弃用和删除

下面的列表显示了已弃用或已删除的 XenMobile Server 功能。

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

在 XenMobile Server 中，已删除的项目已被删除或不再受支持。

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

项目	说明	宣布弃用	删除的功能	备选方法
Knox Mobile Enrollment（旧版 DA）	已弃用在所有 Android 版本中的旧版设备管理员模式下对 Knox Mobile Enrollment (KME) 的支持。	May 4, 2021	目标：June 30, 2021	使用 KME 在 Android Enterprise 模式下注册。Android 8、9、10、11 支持 Android Enterprise。
适用于 Android 7.x 和 iOS 12.x 的 Citrix 移动应用程序和 Workspace 应用程序	弃用了对 Android 7.x 和 iOS 12.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持。	2021 年 4 月	目标：June 2021	请每个主操作系统平台的当前版本和早期版本（最低版本）。较旧的设备保持注册状态。但是，Citrix 不测试也不支持旧设备。
派生凭据	弃用了对派生凭据和 Citrix Derived Credentials Manager 应用程序的支持。	March 25, 2021	目标：2021 年第 2 季度	有关 iOS 支持的身份验证类型的列表，请参阅 iOS。
Internet Explorer 11	弃用了对在 XenMobile Server 控制台中使用 Internet Explorer 的支持。	January 2021	January 2021	请使用以下 Web 浏览器的最新版本：Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari
适用于 Android 的 RSA 软令牌支持	弃用了对将 RSA 软令牌直接导入 Secure Hub for Android 的支持。	January 2021	February 2021	可以在 Google Play 中提供的 RSA Secure ID 应用程序中导入 RSA 软令牌。然后，可以使用该令牌进行 Citrix Gateway 身份验证。

项目	说明	宣布弃用	删除的功能	备选方法
Android - Sony	弃用了对 Android Sony 设备和 SONY 特定的策略的支持。	January 2021	February 2021	使用 Android Enterprise
Android - HTC	弃用了对 Android HTC 设备和 HTC 特定的策略的支持。	January 2021	February 2021	使用 Android Enterprise
XenMobile 控制板的第三方组件	我们将弃用作为 XenMobile 空孩子般的一部分的第三方组件。	December 2020	January 2021	要继续使用控制板，请升级到 XenMobile 10.12 或更高版本
在 Android Enterprise 设备上为旧版设备管理员模式发布的应用程序	我们不再将为旧版 DA 平台发布的应用程序发布到在 Android Enterprise 中注册的设备。	October 2020	November 2020	对于 Android Enterprise 设备，请发布适用于 Android Enterprise 平台的应用程序。要继续将旧版 DA 应用程序发布到 DA 模式下的设备，请为这些应用程序创建单独的交付组。
APNs 传出端口	Apple 对 APNs 旧版二进制文件协议的支持将于 2021 年 3 月 31 日结束。Apple 建议您改为使用基于 HTTP/2 的 APNs 提供程序 API。作为此更改的一部分，我们将弃用对用于向 `*.push.apple.com` 发送 APNs 通知的端口 2195 和 2196 的支持。	October 2020	目标：April 2021	请改为使用端口 443 或 2197。请参阅打开 XenMobile 端口以管理设备。

项目	说明	宣布弃用	删除的功能	备选方法
Samsung SEAMS 容器	弃用了对 Samsung SEAMS 容器的支持。	June 2020	August 2020	使用适用于 Android Enterprise 的 Samsung Knox 服务插件 (KSP) 应用程序。请参阅添加 Knox 服务插件应用程序。
自签名安全套接字层 (SSL) 证书	已弃用对所有设备平台的自签名 SSL 证书的支持。	May 2020		使用知名证书颁发机构 (CA) 颁发的可信 SSL 证书替换现有的自签名证书。
基于证书的身份验证签名算法（非 FIPS 和弱密码）	已弃用对以下签名算法的支持：SHA1withRSA、SHA224withRSA、SHA1withECDSA、SHA224withECDSA、SHA1withDSA、RIPEMD160withRS RIPEMD128withRS RIPEMD256withRS	May 2020	January 2021	在 XenMobile 控制台（设置 > 凭据提供程序 > 证书签名请求）中为凭据提供程序创建 CSR 时，请选择较强的密码。
数据库服务器	已弃用对 Microsoft SQL Server 2014 及更早版本的支持。	October 2021	August 2022	请将系统更新到以下受支持的版本之一：Microsoft SQL Server 2016 SP2、Microsoft SQL Server 2017 CU 13 或 Microsoft SQL Server 2019 CTP 3.2。请参阅系统要求和兼容性中的受支持服务器列表。

项目	说明	宣布弃用	删除的功能	备选方法
虚拟机管理程序	已弃用对 Citrix XenServer 6.5.x 及更早版本、VMware ESXi 5.5 Update 3 及更早版本以及 Hyper-V 2012 的支持。	May 2020	August 2020	请将系统更新为以下收支持的版本之一：Citrix Hypervisor 8.0 及更高版本、Citrix XenServer 7.0 及更高版本、VMware（ESXi 6.0、ESXi 6.5.0 Update 3、ESXi 6.7 Update 2 Patch 10 或 ESXi 7.0）或 Hyper-V (Windows Server 2016 或 Windows Server 2019)。
Citrix Launcher	弃用了对 Citrix Launcher 应用程序的支持。	May 2020	August 2020（从应用商店中删除）	将设备预配为网亭（专用设备）。有关详细信息，请参阅 Citrix Launcher 替代产品。
适用于 Android 6.x 和 iOS 11.x 的 Citrix 移动应用程序和 Workspace 应用程序	弃用了对 Android 6.x 和 iOS 11.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持。	April 2020	June 2020	请每个主操作系统平台的当前版本和早期版本（最低版本）。

项目	说明	宣布弃用	删除的功能	备选方法
MDX Toolkit 和 MDX Service	弃用了对支持移动应用程序管理 (MAM) SDK 的 MDX Toolkit 和 MDX Service 的支持。在过渡期间，您可以同时使用 MDX 打包的应用程序和 MAM SDK 开发的应用程序。	March 2020	目标：2022 年 3 月（适用于 MDX Toolkit）和 2021 年 9 月（适用于 MDX Service）	要继续管理您的企业应用程序，请使用 MAM SDK。
MDX：备用网关服务器	弃用了适用于 iOS 和 Android 设备的递升式身份验证。	March 2020	目标：September 2021	无备选
MDX：Micro VPN（完整通道模式）	弃用了适用于 iOS 和 Android 设备的完整虚拟专用网络 (VPN) 通道。	March 2020	目标：September 2021	使用 MAM SDK Web SSO 模式或使用 Citrix SSO 连接类型创建 PerApp VPN 策略。
MDX：PAC 文件支持	对 iOS 和 Android 设备的完整 VPN 通道部署使用代理自动配置 (PAC) 文件的支持已弃用。	March 2020	目标：September 2021	使用 Citrix Gateway 通过代理服务器进行连接以访问内部网络。
MDX 共享设备支持	弃用了对 MDX 应用程序的共享设备支持。	March 2020	目标：September 2021	对于 Android Enterprise，请使用 MDM 的共享设备支持。对于 iOS，请使用 Apple 校园教务管理或 GroundControl。
适用于 Android 10 的新设备管理员注册	已禁用在 Android 10 设备上对新注册或重新注册到旧版设备管理员模式的支持。已注册的设备将继续工作。	February 2020	September 2020	将新 Android 10+ 设备注册到 Android Enterprise。

项目	说明	宣布弃用	删除的功能	备选方法
适用于 Android 10 设备的旧版设备管理员模式	Google 弃用了一些设备管理员 API。自升级到针对 Android API 级别 29 的 Citrix Secure Hub 起，Citrix 将不支持注册到设备管理员模式的 Android 10 设备。	February 2020	November 2020	将 Android 10 设备迁移到 Android Enterprise。
MDX 加密	弃用了 XenMobile 控制台中的 MDX 加密和 MDX 加密功能。	October 2019	September 2020	使用我们的加密管理功能启用 iOS 或 Android 平台加密，并增加合规性检查。确保您已在 2020 年 7 月之前测试并计划从 MDX 加密迁移。
密码设备策略：适用于 Android Enterprise 的无限制设置	运行 Android 7 或更高版本的 Android Enterprise 设备仅支持创建的带字符限制的通行码。如果您以前将需含字符设置为无限制，此更新将该值更改为仅限数字。	February 2019	April 2019	此更改不会影响当前用户的登录体验。
远程支持	弃用了面向群集化的本地 XenMobile Server 部署的远程支持客户端。	January 2019	August 2020	无备选

项目	说明	宣布弃用	删除的功能	备选方法
适用于 iOS 的 Secure Hub 网络扩展	自 Secure Hub release 20.3.0 起，弃用了允许您为 iOS 设备自定义网络连接功能的网络扩展框架。	October 2018	March 2020	无备选
TLS 版本 1.0 和 1.1	为了提高 XenMobile 的安全性，Citrix 现在会阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的任何通信。由于安全性削弱，PCI 委员会将弃用 TLS 1.0 和 TLS 1.1。	June 2018	March 2019	升级到 TLS 1.2。
Windows Mobile/CE	弃用了对 Windows Mobile/CE 设备的支持。	April 2018	September 2020	使用 Windows 10 Desktop 和 Laptop。
Android TouchDown	DigiCert 已停止支持 Android TouchDown。Citrix 将从 Exchange 设备策略中删除 Android TouchDown 平台页面。	July 2018	2021	建议：使用 Citrix Secure Mail。

已修复的问题

October 13, 2021

XenMobile 10.14 包含以下已修复的问题：

- 升级到 XMS 10.12 时，XenMobile Server 控制台上的控制板视图出现问题。[CXM-88918]
- 配置通用 PKI 后，无法在 Apple 设备上注册 Apple 部署计划（以前称为 DEP）。[CXM-89978]

- 当您使用基于角色的访问控制 (RBAC) 登录时，需要其他权限才能编辑注册配置文件。[CXM-89985]
- 在 XenMobile Server 控制台上，您将无法为 Chrome 应用程序编辑 **Android Enterprise** 托管配置策略。[CXM-89986]
- 在 iOS 平台上，编辑连接类型为 **AlwaysOn IKEv2** 双配置的 VPN 策略时，您将收到错误。[CXM-90010]
- 无法使用 **SamAccountName** 注册 Android Enterprise 设备，您将收到以下错误："Work profile deleted, wiping profile"（已删除工作配置文件，正在擦除配置文件）。[CXM-90049]
- 数据库不接受以小写 "u" 开头的用户名。[CXM-90722]
- XenMobile Server 控制台将为未插入 SIM 卡的设备显示集成电路卡 ID (ICCID)。[CXM-90845]
- 无法在运行 iOS 14 的设备上注册 Apple 设备注册计划 (DEP) 失败。[CXM-91697]
- 在 XenMobile Server 控制台中，不显示正确的根证书过期日期。[CXM-91961]
- 在 XenMobile Server 上，NetScaler Gateway 连接检查不显示结果。[CXM-93129]
- 将 SNMP 用户添加到 XenMobile Server 控制台时，用户不会显示在 *SNMP* 监视用户列表下，或者 SNMP 代理变为非活动状态。[CXM-93197]
- 如果在限制设备策略中同时为同一应用程序启用启用系统应用程序和禁用应用程序设置，则该应用程序仍将显示在工作配置文件中。[CXM-93671]
- 切换到适用于 APNs 的基于 HTTP/2 的 API 时，服务器属性 `ios.mdm.apns.connectionPoolSize` 将处于隐藏状态。[CXM-95478]
- 在 XenMobile Server 10.12 中，无法修改某些应用程序上的 VPP 属性。[CXM-96796]
- 禁用应用程序自动更新设置后，在设备上安装的 Apple 批量购买应用程序将自动更新到最新版本。[CXM-96855]
- 在 XenMobile Server 10.13 中，在 **CLI** 下配置代理服务器时，无法将通知发送到 iOS 设备上运行的 Secure Hub。[CXM-97609]
- 在 XenMobile Server 10.13 中，访问设备详细信息时出错。当设备属性的值在 **"“** 中时，将出现此错误。[CXM-97952]
- 有关版本 10.13.0 滚动修补程序版本中已修复的问题，请参阅：
  - XenMobile Server 10.13.0 滚动修补程序 4
  - XenMobile Server 10.13.0 滚动修补程序 3
  - XenMobile Server 10.13.0 滚动修补程序 2

相关信息

- XenMobile 支持知识中心

平台支持更新

已知问题

January 5, 2022

XenMobile 10.14 包括以下已知问题：

- 将 XenMobile Server 10.8 或 10.9 映像导入到 VMware ESXi 6.7 或 6.5 Update 2 之后：重新启动 VM 后，配置应用程序无法启动，XenMobile 服务器进入恢复模式，并且 IP 设置被清除。要解决此问题，请使用 VMXNET3 NIC 构建新的 VM，然后将该 VM 加入到已进入恢复模式 VM 的数据库。[CXM-54581]
- 注册 iOS 15 或 macOS 12 设备后，MDM 配置文件将显示为 “未验证”。[CXM-98525]
- 升级到 Android 12 后，在工作配置文件模式下重新注册的设备会在设备管理表中显示两次。[CXM-99712]
- 将定位命令发送到运行 Android 12 且由 MDM 注册的设备后，用户将在启动 Secure Hub 时遇到无限期加载的白屏。[CXM-99878]
- 有关与移动生产力应用程序相关的已知问题，请参阅 Secure Hub、Secure Mail 和 Secure Web。
- 有关最新版本 10.13.0 滚动修补程序版本中的已知问题，请参阅：
  - XenMobile Server 10.13 滚动修补程序 4 版本的发行说明

相关信息

- XenMobile 支持知识中心

体系结构

January 5, 2022

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

- Citrix Gateway 向用户授予对移动应用程序的远程访问权限以及跟踪用户设备类型。
- 您可以在 XenMobile 中管理这些应用程序和设备。

部署 XenMobile 组件：可以部署 XenMobile 组件以允许用户通过以下方式连接到内部网络中的资源：

- 与内部网络的连接。如果您的用户为远程用户，则可以使用 VPN 或 Micro VPN 连接通过 Citrix Gateway 进行连接。通过该连接可以访问内部网络中的应用程序和桌面。
- 设备注册。用户可以在 XenMobile 中注册移动设备，这样一来，您便可以在 XenMobile 控制台中管理连接到网络资源的设备。

- Web、SaaS 和移动应用程序。用户可以从 XenMobile 通过 Secure Hub 访问其 Web、SaaS 和移动应用程序。
- 基于 Windows 的应用程序和虚拟桌面。用户可以通过 Citrix Receiver 或 Web 浏览器进行连接，以从 StoreFront 或 Web Interface 访问基于 Windows 的应用程序和虚拟桌面。

要在本地 XenMobile Server 上实现其中任何功能，Citrix 建议按以下顺序部署 XenMobile 组件：

- Citrix Gateway。可以使用快速配置向导在 Citrix Gateway 中配置设置，以实现与 XenMobile、StoreFront 或 Web Interface 的通信。在 Citrix Gateway 中使用快速配置向导前，必须先安装以下组件之一才能建立通信：XenMobile、StoreFront 或 Web Interface。
- XenMobile。安装 XenMobile 后，可以在 XenMobile 控制台中配置策略和设置，以允许用户注册其移动设备。您也可以配置移动应用程序、Web 应用程序和 SaaS 应用程序。移动应用程序可以包括 Apple App Store 或 Google Play 中的应用程序。用户还可以连接到您通过 MDX Toolkit 打包并上载到控制台的移动应用程序。
- MAM SDK 或 MDX Toolkit。MDX 封装技术计划于 2022 年 3 月达到生命周期结束 (EOL) 状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

  移动应用程序管理 (MAM) SDK 提供了 iOS 和 Android 平台不涵盖的 MDX 功能。可以启用 MDX 并保护 iOS 或 Android 应用程序。您可以在内部应用商店或公共应用商店中提供这些应用程序。请参阅 MDX 应用程序 SDK。
- StoreFront（可选）。可以通过连接到 Receiver 从 StoreFront 提供对基于 Windows 的应用程序和虚拟桌面的访问权限。
- Citrix Files（可选）。如果部署 Citrix Files，您可以通过 XenMobile 启用企业目录集成，XenMobile 的作用是安全声明标记语言 (SAML) 身份提供程序。有关为 Citrix Content Collaboration 配置身份提供程序的详细信息，请参阅 Content Collaboration 支持站点。

XenMobile 通过 XenMobile 控制台提供设备管理和应用程序管理。本节介绍 XenMobile 部署的参考体系结构。

在生产环境中，Citrix 建议采用群集配置部署 XenMobile 解决方案，以实现可扩展性和服务器冗余。此外，利用 Citrix ADC SSL 卸载功能可以进一步降低 XenMobile Server 的负载，并增加吞吐量。有关如何通过在 Citrix ADC 上配置两个负载平衡虚拟 IP 地址来为 XenMobile 设置群集的详细信息，请参阅群集。

有关为灾难恢复部署配置 XenMobile 的详细信息，请参阅部署手册中的灾难恢复一文。这篇文章包括了体系结构图。

以下各节说明了 XenMobile 部署的不同参考体系结构。有关参考体系结构图，请参阅《XenMobile 部署手册》文章面向本地部署的参考体系结构和体系结构。有关端口的完整列表，请参阅端口要求（本地部署）和端口要求（云）。

移动设备管理 (MDM) 模式

> 重要：
>
> 如果配置了 MDM 模式，之后更改为 ENT 模式，请务必使用相同的 (Active Directory) 身份验证。XenMobile 不支持在用户注册后更改身份验证模式。有关详细信息，请参阅从 XenMobile MDM Edition 升级到 Enterprise Edition。

XenMobile MDM Edition 提供移动设备管理。有关平台支持，请参阅支持的设备操作系统。如果您计划只使用 XenMobile 的 MDM 功能，请在 MDM 模式下部署 XenMobile。例如，如果您要执行以下操作。

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

在建议的模型中，XenMobile Server 位于 DMZ 中，可选 Citrix ADC 位于前端，后者为 XenMobile 提供更多的保护。

移动应用程序管理 (MAM) 模式

MAM（也称为仅 MAM 模式）提供移动应用程序管理。有关平台支持，请参阅支持的设备操作系统。如果您计划只使用 XenMobile 的 MAM 功能而不要求设备进行 MDM 注册，请在 MDM 模式下部署 XenMobile。例如，如果您要执行以下操作。

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

设备不能进行 MDM 注册。

在此部署模型中，XenMobile Server 与 Citrix Gateway 位于前端，后者为 XenMobile 提供更多的保护。

MDM+MAM 模式

同时使用 MDM 和 MAM 模式可以提供移动应用程序和数据管理以及移动设备管理功能。有关平台支持，请参阅支持的设备操作系统。如果您计划使用 XenMobile 的 MDM+MAM 功能，请在 ENT（企业）模式下部署 XenMobile。例如，如果您希望：

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

在建议的部署模型中，XenMobile Server 位于 DMZ 中，Citrix Gateway 位于前端，后者为 XenMobile 提供更多的保护。

XenMobile 在内部网络中：另一种部署方案是将本地 XenMobile Server 放置在内部网络中，而不是放置在 DMZ 中。如果您的安全策略要求只能将网络设备放置到 DMZ 中，请使用此部署。在此部署中，XenMobile Server 不在 DMZ 中。因此，不需要打开内部防火墙中的端口即可允许从 DMZ 访问 SQL Server 和 PKI 服务器。

系统要求和兼容性

January 5, 2022

> 注意：
>
> 本文介绍了 XenMobile Server 10.14 的系统要求和兼容性。有关 Endpoint Management 系统要求，请参阅系统要求。

有关更多要求和兼容性信息，请参阅以下文章：

- XenMobile 兼容性
- 支持的设备操作系统
- 端口要求
- 可扩展性
- 许可
- FIPS 140-2 合规性
- 语言支持

要运行 XenMobile 10.14，需要满足以下最低系统要求：

- 以下其中一种：
  - Citrix Hypervisor 8.1 或 8.0 或者 Citrix XenServer（支持的版本：7.0、7.1、7.2、7.3、7.4、7.5、7.6、8.0、8.1、8.2）；有关详细信息，请参阅 XenServer
  - VMware（支持的版本：ESXi 6.0、ESXi 6.5.0 Update 3 或 ESXi 6.7 Update 2 修补程序 10、ESXi 7.0 Update 2a）；有关详细信息，请参阅ESXi 6.7 解决方法和 VMware
  - Hyper-V（支持的版本：Windows Server 2016 和 Windows Server 2019）；有关详细信息，请参阅 Hyper-V
- 适用于 Exchange ActiveSync 的 Endpoint Management 连接器 10.1.10 或适用于 Exchange ActiveSync 的 Citrix Gateway 连接器 8.5.3.19
- 双核处理器
- 4 个虚拟 CPU
- 对于生产环境：8 GB RAM；对于概念验证和测试环境：4 GB RAM
- 50 GB 磁盘空间
- Citrix 许可证服务器 11.16。

  请在升级 XenMobile Server 之前更新您的 Licensing 服务器。

ESXi 6.7 解决方法

为使 ESXi 6.7 正常工作，必须采用以下解决方法。

1. 使用 VMware 提供的 OVF 工具，提取从 citrix.com 下载的 OVA 文件。从 VMware 的页面 (https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491) 获取 OVF 工具。
2. 将提取的三个文件中的.vmdk 文件上载到您的数据存储中。
3. 创建新虚拟机。
   a) 为该虚拟机命名，并选择 **ESX/ESXi 4.x virtual machine**（ESX/ESXi 4.x 虚拟机）作为兼容性选项。
   b) 对于来宾操作系统系列，选择 **Linux**。
   c) 对于来宾操作系统版本，选择 **Other 2.6.x Linux (64-bit)**（其他 2.6.x Linux (64 位)）。
   d) 对于数据存储，选择 **Default**（默认值）。
   e) 在自定义期间，删除默认硬盘、USB 控制器和 CD/DVD 驱动器。
   f) 在“Network”（网络）下，选择 **VMXNET3** 作为适配器类型。
   g) 在 ESXi 上，如果您的磁盘是本地磁盘，请选择 **SCSI Controller**（SCSI 控制器）和 **LSI Logic Parallel**（LSI 逻辑并行）。如果您使用的是共享磁盘，请选择 **VMware Paravirtual**（VMware 半虚拟化）。
   h) 单击“Next”（下一步）完成 VM 创建。
4. 导航到您的数据存储，并复制之前上载的.vmdk 文件。将其复制到您为 XenMobile 创建的 VM 目录中。
5. 从 ESXi Web 界面，选择 VM，然后编辑设置。
6. 单击 **Add Hard disk**（添加硬盘）。
7. 选择之前复制的.vmdk 文件并将其附加到 VM。
8. 单击保存。
9. 打开 VM 电源。

Citrix Gateway 系统要求

要在 XenMobile 10.14 中运行 Citrix Gateway，需要满足以下最低系统要求。

- Citrix Gateway（本地）支持的版本：12.1 或更高版本
- 您还必须能够与 Active Directory 通信，这需要使用服务帐户。您只需具有查询和读取权限。

XenMobile 10.14 的数据库要求

XenMobile 需要使用以下数据库之一：

- Microsoft SQL Server

  XenMobile 支持运行以下其中一个受支持的版本的 Microsoft SQL Server 数据库。有关 Microsoft SQL Server 数据库及其硬件要求的详细信息，请参阅 Microsoft 文档。

  - Microsoft SQL Server 2014 SP3
  - Microsoft SQL Server 2016 SP2
  - Microsoft SQL Server 2017 CU 25
  - Microsoft SQL Server 2019 CU 12

您的 Microsoft SQL Server 数据库要求还取决于部署的大小。有关您的部署大小的 Microsoft SQL Server 数据库要求的详细信息，请参阅可扩展性。

XenMobile 支持 SQL Basic 可用性组（AlwaysOn 可用性组）和 SQL 群集以实现数据库高可用性。

Citrix 建议远程使用 Microsoft SQL。

有关升级 Microsoft SQL 的信息，请参阅 Microsoft 文章升级 SQL Server。

- PostgreSQL（仅适用于测试环境）。PostgreSQL 随附在 XenMobile 中。您可以在测试环境中本地或远程使用。不支持数据库迁移。不能将在测试环境中创建的数据库移动到生产环境。

  所有 XenMobile 版本都支持适用于 Windows 的 Remote PostgreSQL 9.5.1 和 9.5.11，但存在以下限制：不建议用于生产环境。最多支持 300 个设备。对于超出 300 个设备的情况，可使用本地 SQL Server。不支持群集。

SQL Server 服务帐户要求

确保要用于 XenMobile 的 SQL Server 服务帐户具有 `DBcreator` 角色权限。记录在 XenMobile Server 安装期间指定的 SQL Server 帐户密码。如果您需要在 XenMobile Server 恢复期间克隆 XenMobile 数据库，需要该密码。

使用透明数据加密 (Transparent Data Encryption, TDE) 保护 SQL Server 数据库。不允许对 SQL Server 端口进行外部访问，如面向本地部署的参考体系结构中的参考体系结构所示。

有关 SQL Server 服务帐户的详细信息，请参阅 Microsoft 文档站点上的以下页面。这些链接提供有关 SQL Server 2014 的信息。如果您使用的是其他版本，请从 **Other Versions**（其他版本）列表中选择您的服务器版本：

- Configure Windows Service Accounts and Permissions（配置 Windows 服务帐户和权限）
- Server-Level 角色

Virtual Apps and Desktops 兼容性

- Virtual Apps and Desktops 7.15 LTSR CU3
- Virtual Apps and Desktops 7.1811
- Virtual Apps and Desktops 7 1906
- Virtual Apps and Desktops 7 1909
- Virtual Apps and Desktops 7 2006

StoreFront 兼容性

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

其他兼容性

- 适用于 Exchange ActiveSync 10.1.10 的 Endpoint Management 连接器
  - 早期版本未进行测试
- 适用于 Exchange ActiveSync 8.5.3.19 的 Citrix Gateway 连接器
  - 早期版本未进行测试

XenMobile 兼容性

January 5, 2022

> 注意：
>
> 本文涵盖 XenMobile Server 的兼容性。有关使用 Endpoint Management 测试过的组件，请参阅 Endpoint Management 兼容性。

要使用新功能、修复和策略更新，Citrix 建议您安装以下组件的最新版本：

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

  MDX Toolkit 计划于 2022 年 3 月达到生命周期已结束 (EOL) 状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

本文概述了可以集成的受支持的 XenMobile 组件的版本。

兼容性和升级路径

最新版本的 Secure Hub、MDX Toolkit 和移动生产力应用程序与最新版本和早期版本的 XenMobile Server 兼容。

最新版本的移动生产力应用程序要求使用最新版本的 Secure Hub。这两个版本的应用程序与最新版本的 Secure Hub 兼容。有关详细信息，请参阅 Citrix Product Matrix（Citrix 产品列表）。

Citrix 仅支持从公共应用商店分发 XenMobile 生产力应用程序。

XenMobile Server（本地）

- Citrix 支持从最后两个版本的 XenMobile Server 进行升级。
- XenMobile Server 的最新版本：XenMobile Server 10.14
- 从以下版本升级：
  - XenMobile Server 10.13.x
  - XenMobile Server 10.12.x

移动生产力应用程序

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

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

MAM SDK

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

MDX Toolkit

MDX 封装技术计划于 2021 年 9 月达到生命周期结束 (EOL) 状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

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

浏览器支持

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

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

支持的设备操作系统

January 5, 2022

> 注意：
>
> 本文介绍了 XenMobile Server 10.13 支持的设备操作系统。有关 Endpoint Management 支持的操作系统，请参阅支持的设备操作系统。

XenMobile 支持对运行以下平台和操作系统的设备进行企业移动性管理，包括应用程序和设备管理。由于平台限制和安全功能，XenMobile 并不在所有平台上支持所有功能。

本文中受支持设备平台的信息也适用于适用于 Exchange ActiveSync 的 XenMobile 连接器和适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。

有关移动生产力应用程序的最新版本以及支持的 MDX 加密设备，请参阅支持移动生产力应用程序。

> 注意：
>
> Citrix 最低支持每个主操作系统平台的当前版本和早期版本。并非 Endpoint Management 较新版本的所有功能都能在较旧的平台版本上运行。
>
> 有关弃用通知，请参阅弃用。

操作系统支持列表

Citrix XenMobile 支持以下操作系统：

> 注意：
>
> 对 Android 7.x 和 iOS 12.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持已于 2021 年 4 月结束。

- **Android**：8.x、9.x、10.x、11.x、12.x

  有关 Android 10+，请参阅 Android 注意事项。

- **iOS**：13.x、14.x、15.x

  XenMobile 和 Citrix 移动应用程序与 iOS 14.x 兼容，但目前不支持所有新 iOS 14.x 功能。要封装适用于 iOS 14.x 的内部企业应用程序，请使用 MDX Toolkit 21.8.5 或更高版本或者使用 MAM SDK 准备这些应用程序。

- **iPadOS**：13.x、14.x、15.x

  XenMobile 和 Citrix 移动应用程序与 iPadOS 14.x 兼容，但目前不支持所有新 iPadOS 14.x 功能。

- **macOS**：10.13x、10.14x、10.15x、11.x

  XenMobile 和 Citrix 移动应用程序与 macOS 11 兼容，但目前不支持所有新 macOS 11 功能。

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

- **Windows Phone**：（仅限 MDM）。Windows Phone 8.1、Windows Phone 10、Windows 10 RS4 和 RS5

- **Windows Mobile/CE**：（仅限 MDM）。从 2018 年第二季度开始，对 Windows Mobile/CE 设备的支持将不再可用。

- **Samsung SAFE** 和 **Knox**：在兼容的 Samsung 设备上，XenMobile 可同时支持和扩展 Samsung for Enterprise (SAFE) 和 Samsung Knox 策略。XenMobile 要求您先启用 SAFE API，然后再部署 SAFE 策略和限制。为此，应将内置 Samsung Enterprise License Management (ELM) 密钥部署到设备。请参阅 Samsung MDM 许可证密钥设备策略。

Android 注意事项

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

- Citrix 建议您避免在旧设备管理模式下注册 Android 10 设备。Google 正在逐步弃用设备管理 API，这会影响运行 Android 10+ 的设备。在 API 被弃用后，在旧设备管理模式下注册 Android 10+ 设备将失败。Citrix 不支持在设备管理模式下注册 Android 11 设备。
- Citrix 建议对 Android 10 设备使用 Android Enterprise。有关详细信息，请参阅从设备管理迁移到 Android Enterprise。
- Google API 更改不会影响在仅 MAM 模式下注册的设备。

升级之前：

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

端口要求

January 5, 2022

要使设备和应用程序能够与 XenMobile 通信，应在防火墙中打开特定端口。以下各表列出了必须打开的端口。

为 **Citrix Gateway** 和 **XenMobile** 打开端口以管理应用程序

打开下列端口以允许用户通过 Citrix Gateway 从 Citrix Secure Hub、Citrix Receiver、Citrix Gateway 插件连接到以下组件：

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- 适用于 Exchange ActiveSync 的 Citrix Gateway 连接器
- 其他内部网络资源，例如 Intranet Web 站点

要实现从 Citrix ADC 到 Launch Darkly 的通信，可以使用此支持知识中心文章中所述的 IP 地址。

有关 Citrix Gateway 的详细信息，请参阅 Citrix Gateway 文档。该文档包括有关 Citrix ADC IP (NSIP) 虚拟服务器 IP (VIP) 和子网 IP (SNIP) 地址的信息。

TCP 端口	说明	源	目标
21 或 22	用于将支持包发送到 FTP 或 SCP 服务器。	XenMobile	FTP 或 SCP 服务器
53（TCP 和 UDP）	用于 DNS 连接。	Citrix Gateway、XenMobile	DNS 服务器
80	Citrix Gateway 通过第二个防火墙将 VPN 连接传递到内部网络资源。用户使用 Citrix Gateway 插件登录时，通常会发生此情况。	Citrix Gateway	Intranet Web 站点
80 或 8080，443	用于枚举、票证记录和身份验证的 XML 和 Secure Ticket Authority (STA) 端口。Citrix 建议使用端口 443。	StoreFront 和 Web Interface XML 网络流量，Citrix Gateway STA	虚拟应用程序或桌面
123（TCP 和 UDP）	用于网络时间协议 (NTP) 服务。	Citrix Gateway；XenMobile	NTP 服务器
389	用于非安全 LDAP 连接	Citrix Gateway；XenMobile	LDAP 身份验证服务器或 Microsoft Active Directory
443	用于从 Citrix Receiver 连接到 StoreFront 或从 Receiver for Web 连接到 Virtual Apps and Desktops。	Internet	Citrix Gateway
443	用于连接到 XenMobile 以实现 Web、移动和 SaaS 应用程序交付。	Internet	Citrix Gateway
443	用于与 XenMobile Server 的一般设备通信。	XenMobile	XenMobile
443	注册时用于从移动设备到 XenMobile 的连接。	Internet	XenMobile

TCP 端口	说明	源	目标
443	用于从 XenMobile 连接到适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。	XenMobile	适用于 Exchange ActiveSync 的 Citrix Gateway 连接器
443	用于从适用于 Exchange ActiveSync 的 Citrix Gateway 连接器连接到 XenMobile。	适用于 Exchange ActiveSync 的 Citrix Gateway 连接器	XenMobile
443	用于在未进行证书身份验证的部署中的回调 URL。	XenMobile	Citrix Gateway
514	用于 XenMobile 与 Syslog 服务器之间的连接。	XenMobile	Syslog 服务器
636	用于安全 LDAP 连接。	Citrix Gateway；XenMobile	LDAP 身份验证服务器或 Active Directory
1494	用于与内部网络中基于 Windows 应用程序的 ICA 连接。Citrix 建议保持此端口处于打开状态。	Citrix Gateway	虚拟应用程序或桌面
1812	用于 RADIUS 连接。	Citrix Gateway	RADIUS 身份验证服务器
2598	用于使用会话可靠性连接到内部网络中基于 Windows 的应用程序。Citrix 建议保持此端口处于打开状态。	Citrix Gateway	虚拟应用程序或桌面
3268	用于 Microsoft Global Catalog 非安全 LDAP 连接。	Citrix Gateway；XenMobile	LDAP 身份验证服务器或 Active Directory
3269	用于 Microsoft Global Catalog 安全 LDAP 连接。	Citrix Gateway；XenMobile	LDAP 身份验证服务器或 Active Directory

TCP 端口	说明	源	目标
9080	用于传输 Citrix ADC 和适用于 Exchange ActiveSync 的 Citrix Gateway 连接器之间的 HTTP 流量。	Citrix ADC	适用于 Exchange ActiveSync 的 Citrix Gateway 连接器
30001	HTTPS 服务的初始分段的管理 API	内部 LAN	XenMobile Server
9443	用于传输 Citrix ADC 和适用于 Exchange ActiveSync 的 Citrix Gateway 连接器之间的 HTTPS 流量。	Citrix ADC	适用于 Exchange ActiveSync 的 Citrix Gateway 连接器
45000、80	用于部署在群集中的两个 XenMobile VM 之间的通信。端口 80 用于节点间通信和 SSL 卸载。	XenMobile	XenMobile
8443	用于注册、XenMobile Store 和移动应用程序管理 (MAM)。	XenMobile、Citrix Gateway、设备、Internet	XenMobile
4443	用于管理员通过浏览器访问 XenMobile 控制台。还用于从一个节点为所有 XenMobile 群集节点下载日志和支持包。	接入点（浏览器）、XenMobile	XenMobile
27000	用于访问外部 Citrix 许可证服务器的默认端口。	XenMobile	Citrix 许可证服务器
7279	用于签入和签出 Citrix 许可证的默认端口。	XenMobile	Citrix 供应商守护程序
161	用于使用 UDP 协议的 SNMP 流量。	SNMP 管理器	XenMobile
162	用于从 XenMobile 向 SNMP 管理器发送 SNMP 陷阱警报。来源为 XenMobile，目标为 SNMP 管理器。	XenMobile	SNMP 管理器

打开 **XenMobile** 端口以管理设备

打开以下端口以允许 XenMobile 在网络中通信。

TCP 端口	说明	源	目标
25	用于 XenMobile 通知服务的 SMTP 端口。如果 SMTP 服务器使用其他端口，请确保防火墙不会阻止该端口。	XenMobile	SMTP 服务器
80 和 443	与 Apple iTunes App Store、Google Play（必须使用 80）或 Windows Phone 应用商店的企业应用商店连接。用于 Apple 批量购买。用于从 iOS 中的应用商店、Secure Hub for Android 或 Secure Hub for Windows Phone 发布应用程序。	XenMobile	ax.apps.apple.com 和 *.mzstatic.com, vpp.itunes.apple.com, login.live.com, *.notify.windows.com, play.google.com, android.clients.google.com, android.l.google.com
80 或 443	用于 XenMobile 与 Nexmo SMS Notification Relay 之间的出站连接。	XenMobile	Nexmo SMS Relay 服务器
389	用于非安全 LDAP 连接。	XenMobile	LDAP 身份验证服务器或 Active Directory
443	用于 Android 和 Windows Mobile 的注册和代理安装。	Internet	XenMobile
443	用于 Android 和 Windows 设备以及 MDM 远程支持客户端的注册和代理安装。	Internet LAN 和 Wi-Fi	XenMobile
1433	默认用于与远程数据库服务器的连接（可选）。	XenMobile	SQL Server

TCP 端口	说明	源	目标
443 或 2197	用于将 APNs 通知发送到 `*.push.apple.com`	XenMobile	Internet（使用公用 IP 地址 17.0.0.0/8 的 APNs 主机
5223	用于从 iOS 设备到 `*.push.apple.com` 的 APNs 出站连接。	iOS 设备	Internet（使用公用 IP 地址 17.0.0.0/8 的 APNs 主机）
8081	用于来自可选 MDM 远程支持客户端的应用程序通道。默认值为 8081。	远程支持客户端	XenMobile
8443	用于 iOS 和 Windows Phone 设备注册。	Internet，LAN 和 Wi-Fi	XenMobile

自动发现服务连接的端口要求

此端口配置可确保从 Secure Hub for Android 连接的 Android 设备能够从内部网络访问 Citrix AutoDiscovery Service (ADS)。您需要访问 ADS 以下载通过 ADS 提供的安全更新。

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

如果您希望启用证书固定，应满足以下必备条件：

- 收集 **XenMobile Server** 和 **Citrix ADC** 证书。证书必须采用 PEM 格式，并且必须是公用证书，而非私钥。
- 联系 **Citrix** 技术支持并请求启用证书固定功能。在此过程中，系统会要求您提供证书。

证书固定功能要求设备先连接到 ADS，然后再注册。此要求可确保最新的安全信息对 Secure Hub 可用。为了 Secure Hub 注册设备，该设备必须访问 ADS。因此，在内部网络中打开 ADS 访问功能对启用设备注册非常重要。

要允许访问 Secure Hub for Android 的 ADS，请为以下 FQDN 和 IP 地址打开端口 443：

FQDN	IP 地址	端口	IP 和端口用法
`ads.xm.cloud.com`	34.194.83.188	443	Secure Hub - ADS 通信
`ads.xm.cloud.com`	34.193.202.23	443	Secure Hub - ADS 通信

> 注意：
>
> 对于 10.6.15 之前的 Secure Hub 版本，FQDN 为 `discovery.mdm.zenprise.com`。为 IP 地址 52.5.138.94 和 52.1.30.122 打开端口 443。

Android Enterprise 网络要求

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

XenMobile 的端口要求

以下目标主机必须能够从网络访问，才能创建托管 Google Play Enterprise 并访问 Managed Google Play iFrame（托管 Google Play iFrame）。Google 为 EMM 开发人员提供了托管 Play iFrame，以简化应用程序的搜索和审批。您访问 XenMobile 控制台所使用的浏览器必须能够访问 Google Play，才能使用托管 Play iFrame。

目标主机	端口	说明
play.google.com	TCP/443	用于 Google Play 应用商店，Play Enterprise 注册
*.googleapis.com	TCP/443	用于 Google Mobile Management、Google API、Google Play 应用商店 API
accounts.youtube.com、accounts.google.com	TCP/443	用于帐户身份验证
apis.google.com	TCP/443	用于 GCM 和其他 Google Web 服务
ogs.google.com	TCP/443	用于 iFrame UI 元素
notifications.google.com	TCP/443	用于桌面和移动通知
fonts.googleapis.com、*.gstatic.com、*.googleusercontent.com	TCP/443	用于 Google 字体用户生成的内容。例如，应用商店中的应用程序图标
cri.pki.goog、ocsp.pki.goog	TCP/443	用于证书验证

可扩展性和性能

January 5, 2022

理解扩展 XenMobile 基础结构在确定如何部署和配置 XenMobile 方面起着重要作用。本文包含来自针对小型到大型本地 XenMobile 企业部署的可扩展性测试的数据，以及有关如何针对这些部署来确定性能和可扩展性方面的基础结构要求。

可扩展性在本文中是根据已在部署中注册的设备同时重新连接到部署的能力来定义的。

- 可扩展性定义为在部署中注册的最大设备数。
- 登录速率定义为现有设备可以重新连接到部署的最大速率。

本文中的数据源自对规模范围从 10000 到 75000 台设备的部署的测试。测试中的移动设备使用已知工作负载。

所有测试都是在 XenMobile Enterprise Edition 上完成。

测试是使用 Citrix Gateway 8200 进行的。预计具有相似或更高容量的 Citrix ADC 设备可以获得相似或更高的可扩展性和性能。

可扩展性测试结果摘要如下所示。

最多 **75000** 台设备的部署的可扩展性测试结果摘要

登录速率（现有用户的重新连接速率）- 每小时最多 9375 台设备

使用的配置：

- Citrix Gateway
- MPX 8200
- XenMobile Enterprise Edition
- XenMobile Server 7 节点群集
- 数据库：Microsoft SQL Server 外部数据库

测试结果（按设备数量和硬件配置）

设备数量	12500	30000	60000	75000
每小时现有设备的重新连接速率	1250	3750	7500	9375
XenMobile Server - 模式	独立	群集	群集	群集
XenMobile Server - 群集	不适用	3	5	7
XenMobile Server - 虚拟设备	内存 = 8 GB RAM；vCPU = 4	内存 = 16 GB RAM；vCPU = 6	内存 = 24 GB RAM；vCPU = 8	内存 = 24 GB RAM；vCPU = 8
Active Directory	内存 = 4 GB RAM；vCPU = 2	内存 = 8 GB RAM；vCPU = 4	内存 = 16 GB RAM；vCPU = 4	内存 = 16 GB RAM；vCPU = 4

设备数量	12500	30000	60000	75000
Microsoft SQL Server 外部数据库	内存 = 8 GB RAM；vCPU = 4	内存 = 16 GB RAM；vCPU = 8	内存 = 24 GB RAM；vCPU = 16	内存 = 24 GB RAM；vCPU = 16

可扩展性配置文件

Active Directory 配置	使用的配置文件
用户	100000
组	200000
嵌套级别	5

XenMobile Server 配置	总数	每个用户
策略	20	20
应用程序	270	50
公共应用程序	200	0
MDX	50	30
Web 和 SaaS 应用程序	20	20
操作	50	
交付组	20	
每个交付组的 Active Directory 组数	10	
SQL		
数据库数	1	

设备连接和应用程序活动

这些可扩展性测试按部署中注册的设备在 8 小时的时间段内重新连接的能力来收集数据。

测试模拟了重新连接时间间隔，在这段时间里，进行重新连接的设备获得所有授权安全策略，导致 XenMobile Server 节点需要承受的负载情况高于一般情况。在后续重新连接过程中，只有更改的策略或新策略推送至 iOS 设备，从而减轻 XenMobile Server 节点上的负载。

这些测试混合使用了 50% 的 iOS 设备和 50% 的 Android 设备。

这些测试假定进行重新连接的 Android 设备接收了以前的 GCM 通知。

在 8 小时的测试时间间隔内，发生了以下应用程序相关活动：

- Secure Hub 打开了一次以列举获得授权的应用程序
- 打开了 2 个 SAML Web 应用程序
- 下载了 4 个 MAM 应用程序
- 生成了 1 个 STA 以供 Secure Mail 使用
- 240 次 STA 票据验证，每个通过 Micro VPN 的 Secure Mail 重新连接事件执行一次验证。

参考体系结构

有关这些可扩展性测试中使用的部署的参考体系结构，请参阅 Reference Architecture for On-Premises Deployments（适用于本地部署的参考体系结构）中的“Core MAM+MDM Reference Architecture”（核心 MAM+MDM 参考体系结构）。

附加说明和限制

考虑本文中的可扩展性测试结果时请注意以下内容：

- 未测试 Windows 平台。
- 针对 iOS 和 Android 设备测试了策略推送功能。
- 每个 XenMobile Server 节点最多同时支持 12000 台设备。

许可

January 5, 2022

> 重要：
>
> 自 2020 年 11 月 4 日起，返回和修改 Citrix 许可证的过程发生了变化。有关对 Citrix.com 上的“Manage Licenses”（管理许可证）门户和合作伙伴中心上的“My Licensing Tools”（我的许可工具）所做的更改的信息，请参阅 Citrix 支持文章 https://support.citrix.com/article/CTX285157。

XenMobile 使用 Citrix Licensing 管理许可证。XenMobile Server 和 Citrix Gateway 需要许可证。

有关 Citrix Gateway 许可的详细信息，请参阅 Citrix Gateway 文档。有关 Citrix Licensing 的详细信息，请参阅 The Citrix Licensing System（Citrix Licensing 系统）。

购买 XenMobile Server 时，您会收到一封订单确认电子邮件，其中包含用于激活许可证的说明。新客户必须先注册加入许可证计划才能下订单。有关 XenMobile 许可模式和计划的详细信息，请参阅 XenMobile licensing（XenMobile 许可）。

要求

- 请先将您的 Citrix 许可证服务器更新到 11.16.x 或更高版本，然后再更新到最新版本的 XenMobile Server。早期许可证服务器版本不支持最新版本的 XenMobile。
- 必须先安装 Citrix Licensing，然后再下载 XenMobile 许可证。需要安装了 Citrix Licensing 的服务器的名称才能生成许可证文件。安装 XenMobile 时，默认在服务器上安装 Citrix Licensing。您也可以使用现有 Citrix Licensing 部署管理 XenMobile 许可证。有关安装、部署和管理 Citrix Licensing 的详细信息，请参阅许可使用本产品。
- 如果打算将 XenMobile 的节点或实例群集在一起，必须在远程服务器上使用 Citrix Licensing。
- Citrix 建议您保留收到的所有许可证文件的一份本地副本。保存配置文件的备份副本时，所有许可证文件都包含在备份中。但是，如果您在未提前备份配置文件的情况下重新安装 XenMobile，则需要使用原始许可证文件。

XenMobile 许可注意事项

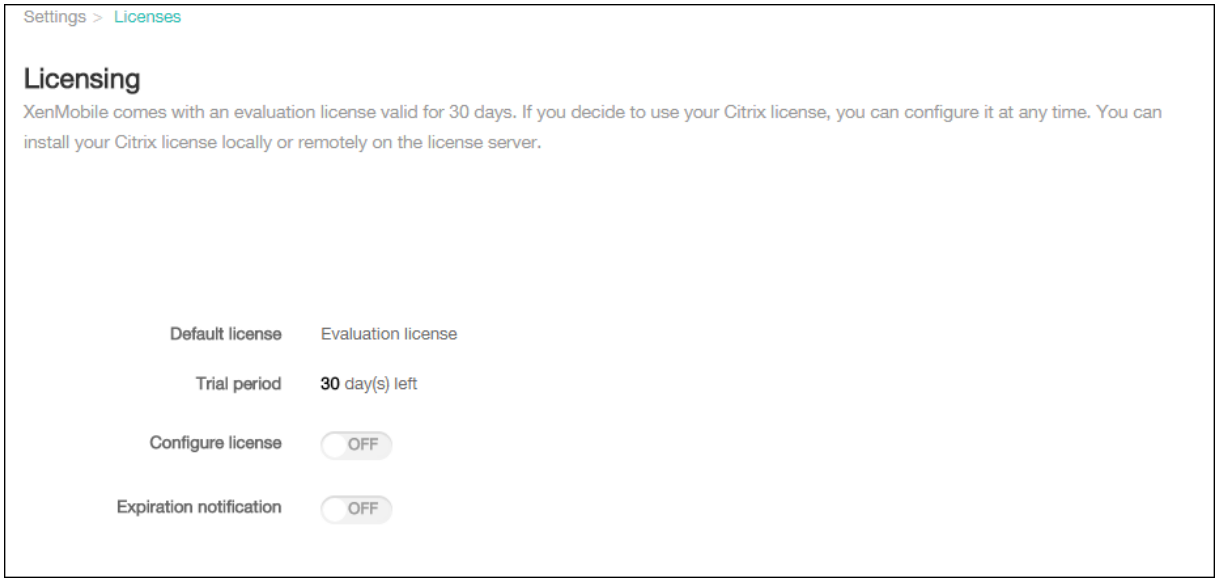
在不提供许可证的情况下，XenMobile 将在宽限期为 30 天的试用模式下运行，功能齐全。此试用模式只能使用一次，期限为从安装 XenMobile 开始持续 30 天。无论是否有可用的有效 XenMobile 许可证，均不会阻止对 XenMobile Web 控制台的访问。在 XenMobile 控制台中，您可以看到试用期剩余的天数。

尽管 XenMobile 允许上载多个许可证，但同一时间只能激活一个许可证。

XenMobile 许可证过期后，您将无法再执行任何设备管理功能。例如，新用户或设备将无法注册，部署到已注册设备的应用程序和配置将无法更新。有关 XenMobile 许可模式和计划的详细信息，请参阅 XenMobile licensing (XenMobile 许可)。

在 XenMobile 控制台上查找 “Licensing”（许可）页面

安装 XenMobile 后首次显示许可页面时，许可证设置为默认 30 天的试用模式，并且尚未配置。可以在此页面上添加和配置许可证。



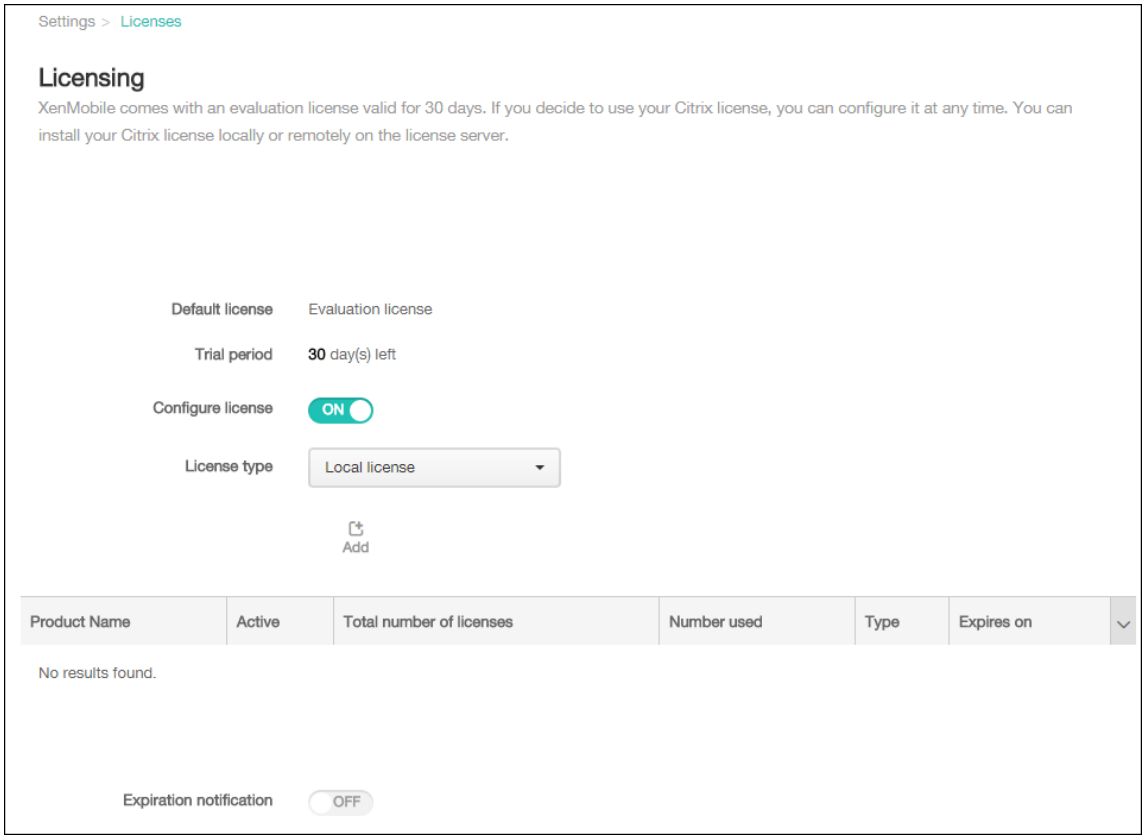
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击许可。此时将显示许可页面。

添加本地许可证

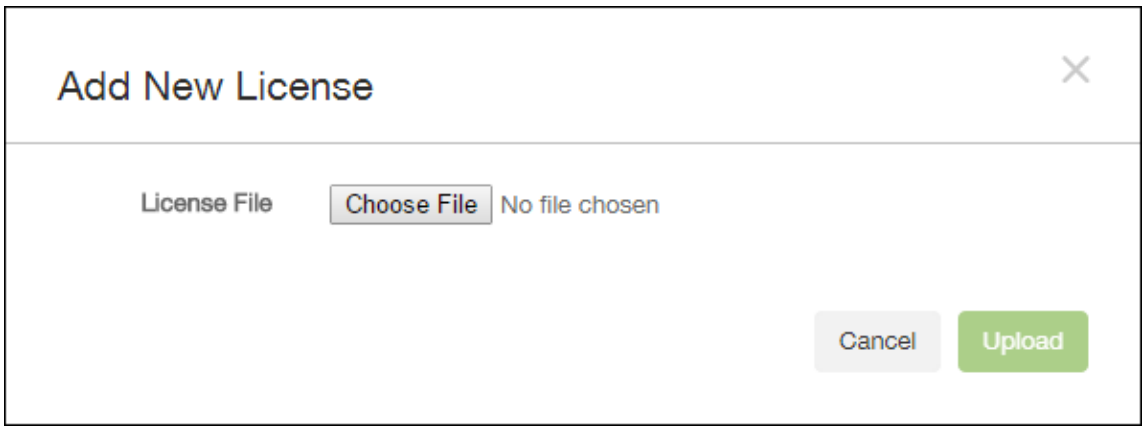
添加新许可证时，它们将显示在表中。添加的第一个许可证自动被激活。如果添加同一类别（如企业）和类型的多个许可证，这些许可证将显示在表格的同一行中。在这些情况下，许可证总数和使用的数量反映公共许可证的总数。过期日期显示公共许可证中的最新过期日期。

通过 XenMobile 控制台管理所有本地许可证。

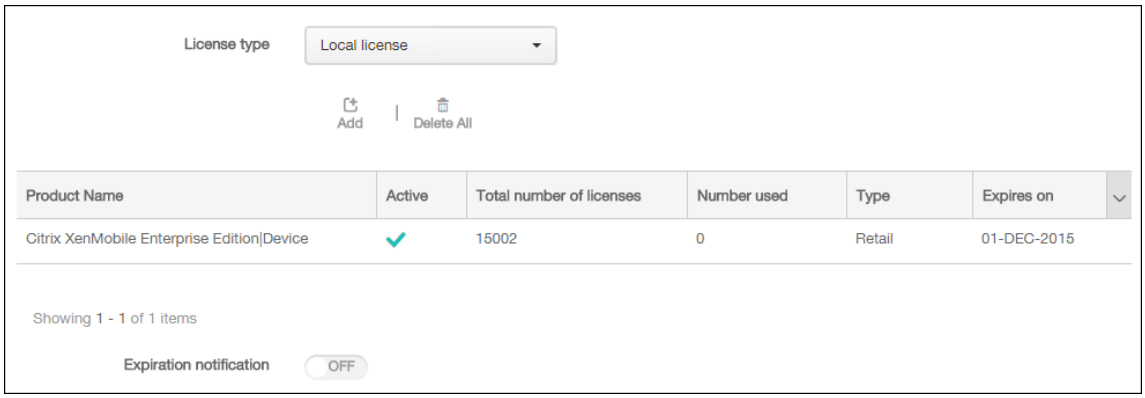
1. 从 Simple License Service 获取许可证文件，方法是通过许可证管理控制台或直接利用您在 Citrix.com 上的帐户。有关详细信息，请参阅 Citrix Licensing 文档。
2. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
3. 单击许可。此时将显示许可页面。
4. 将配置许可证设置为开。在许可证类型列表中，单击添加按钮，将显示许可表。许可表中包含已用于 XenMobile 的许可证。如果尚未添加任何 Citrix 许可证，此表为空。



5. 确保将许可证类型设置为本地许可证，然后单击添加。此时将显示添加新许可证对话框。



6. 在添加新许可证对话框中，单击选择文件，然后浏览到许可证文件的位置。
7. 单击上载。许可证将上载到本地并显示在表格中。



8. 许可证显示在许可页面上的表格中以后，请将其激活。如果此许可证是表格中的第一个许可证，则会自动激活此许可证。

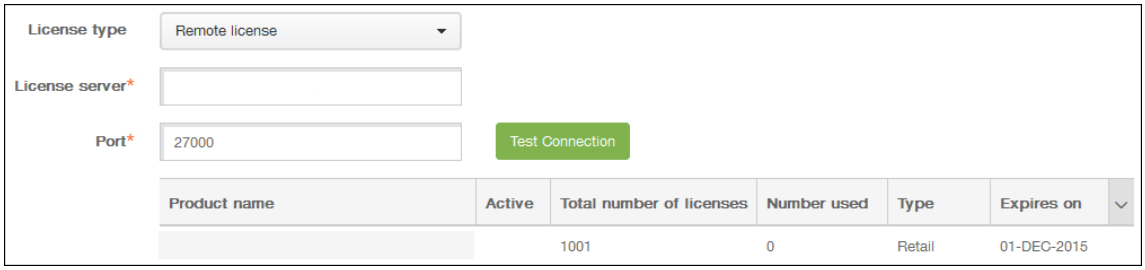
添加远程许可证

如果使用的是远程 Citrix Licensing 服务器，可使用 Citrix Licensing 服务器来管理所有许可活动。有关详细信息，请参阅许可使用本产品。

1. 将许可证服务器证书导入到 XenMobile Server 中（设置 **>** 证书）。
2. 默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。如果主机名验证中断了您的部署，请将服务器属性 **disable.hostname.verification** 更改为 **true**。此属性的默认值为 **false**。

   主机名验证失败时，服务器日志将包括错误，例如：“Unable to connect to the volume purchase Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”（无法连接到批量购买服务器: 主机名 192.0.2.0 与对等机提供的证书使用者不匹配）
3. 在许可页面上，将配置许可证设置为开。在许可证类型列表中，单击添加按钮，将显示许可表。许可表中包含已用于 XenMobile 的许可证。如果尚未添加任何 Citrix 许可证，此表为空。

4. 将许可证类型设置为远程许可证。许可证服务器和端口字段以及测试连接按钮将替换添加按钮。



5. 配置以下设置：

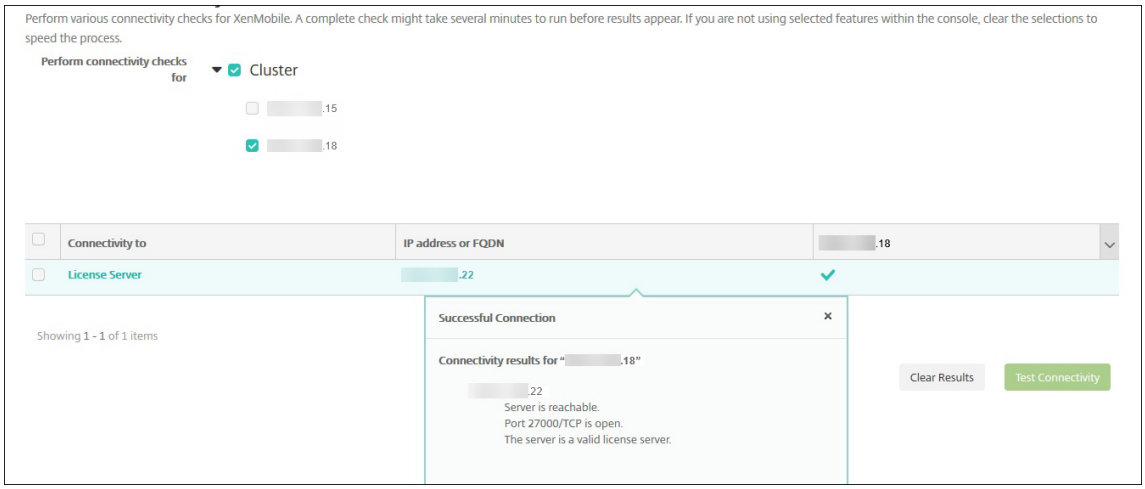
   - 许可证服务器：键入远程许可服务器的 IP 地址或完全限定的域名 (FQDN)。
   - 端口：接受默认端口或键入用于与许可服务器通信的端口号。

6. 单击测试连接。如果连接成功，XenMobile 将与许可服务器连接，并且在许可表中填充可用的许可证。如果只有一个许可证，会自动激活此许可证。

   单击测试连接时，XenMobile 将确认以下信息：

   - XenMobile 可以与许可证服务器通信。
   - 许可证服务器上的许可证有效。
   - 许可证服务器与 XenMobile 兼容。

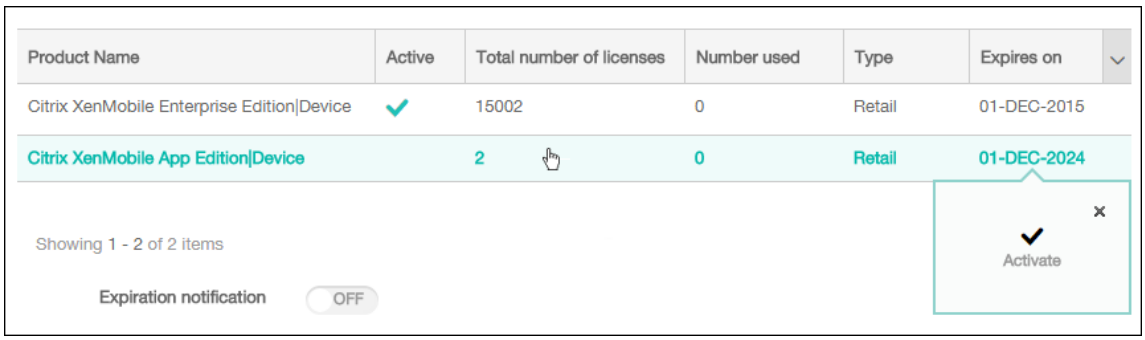
   如果连接不成功，请检查显示的错误消息，进行必要的更正，然后单击测试连接。



激活其他许可证

如果您有多个许可证，可以选择要激活的许可证。但是，同一时间只能激活一个许可证。

1. 在许可页面的许可表中，单击要激活的许可证所在的行。行旁边将显示激活确认框。



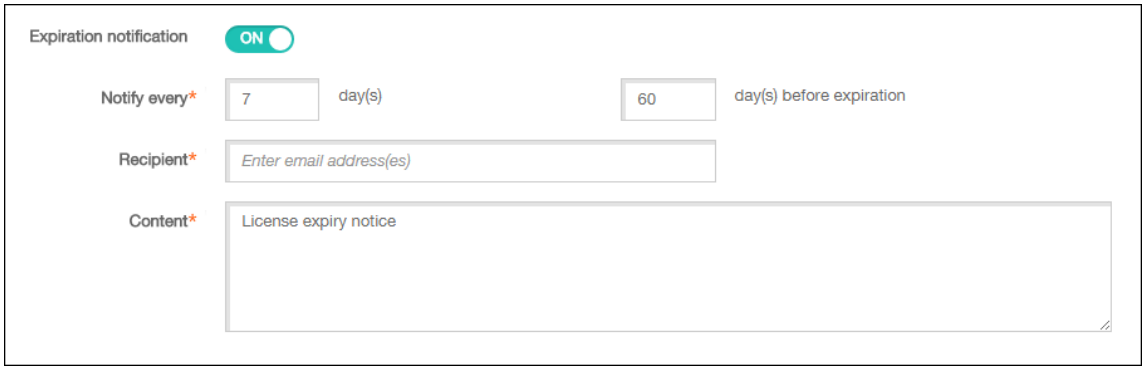
2. 单击激活。将显示激活对话框。
3. 单击激活。所选许可证现已激活。

> 重要：
>
> 如果激活所选许可证，当前激活的许可证将取消激活。

自动化过期通知

激活远程或本地许可证后，可以将 XenMobile 配置为在临近许可证过期日期时通知您，或配置一个委派。

1. 在许可页面上，将到期通知设置为开。将显示新的与通知相关的字段。



2. 配置以下设置：
   - 通知时间间隔：键入：
   - 发送通知的频率，例如每 **7** 天一次。
   - 开始发送通知的时间，如在许可证过期前 60 天发送。
   - 收件人：键入您的电子邮件地址或许可证负责人的电子邮件地址。
   - 内容：键入收件人在通知中看到的过期通知消息。
3. 单击保存。根据您的设置，XenMobile 开始向您在收件人中键入的收件人发送电子邮件，其中包含您在内容中键入的文本。通知按照您设置的频率发送。

FIPS 140-2 合规性

January 5, 2022

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

> 重要：
>
> - 只可以在初始安装时启用 XenMobile FIPS 模式。
> - 如果未使用任何 HDX 应用程序，XenMobile 仅移动设备管理、XenMobile 仅移动应用程序管理和 XenMobile MDM+MAM 都与 FIPS 兼容。

在 iOS 上执行的所有静态数据 (data-at-rest) 和传输中数据 (data-in-transit) 加密操作使用 Citrix 和 Apple 提供的经 FIPS 验证的加密模块。在 Android 上，所有静态数据加密操作都使用设备制造商提供的平台的加密模块提供的经 FIPS 验证的加密模块。有关设备制造商的模块的详细信息，请与 Citrix 代表联系。

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

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

MDX Vault 使用 FIPS 验证的加密模块加密 iOS 和 Android 设备上 MDX 打包的应用程序以及关联静态数据。

语言支持

November 12, 2020

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

本文列出了最新版本的 XenMobile 支持的语言。

XenMobile 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

移动生产力应用程序

X 表示应用程序可在该特定语言中使用。

iOS 和 Android

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

Windows

语言	Secure Hub	Secure Mail	Secure Web
法语	X	X	X
德语	X	X	X
西班牙语	X	X	X
意大利语	X	X	X
丹麦语	X	X	X
瑞典语	X	X	X

对从右至左书写的语言的支持

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

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

安装和配置

January 5, 2022

开始之前的准备工作

可以使用以下预安装核对表记录在本地安装 XenMobile 的必备条件和设置。每项任务或记录都包含一列，指明适用此要求的组件或功能。

规划 XenMobile 部署有多个注意事项。有关您的完整 XenMobile 环境的建议、常见问题和用例，请参阅 XenMobile 部署手册。

有关安装步骤，请参阅本文后面的安装 XenMobile 部分。

预安装核对表

基本网络连接

以下是 XenMobile 解决方案需要的网络设置。

必备条件或设置	组件或功能	记录设置
——————–	———–	——-
记录远程用户连接到的完全限定的域名 (FQDN)。	XenMobile 和 Citrix Gateway
记录公用和本地 IP 地址。
您需要这些 IP 地址来配置防火墙以设置网络地址转换 (NAT)。	XenMobile 和 Citrix Gateway	
记录子网掩码。	XenMobile 和 Citrix Gateway	
记录 DNS IP 地址。	XenMobile 和 Citrix Gateway	
记下 WINS 服务器 IP 地址（如果适用）。	Citrix Gateway	
识别并记下 Citrix Gateway 主机名。| Citrix Gateway	此项不是 FQDN。FQDN 位于绑定到用户所连接的虚拟服务器的已签名服务器证书中。您可以使用 Citrix Gateway 中的安装向导来配置主机名。| Citrix Gateway	
记录 XenMobile 的 IP 地址。如果安装一个 XenMobile 实例，请保留一个 IP 地址。如果配置群集，请记录需要的所有 IP 地址。	XenMobile	
Citrix Gateway 上配置的一个公用 IP 地址	Citrix Gateway	
Citrix Gateway 的一个外部 DNS 条目	Citrix Gateway
记录 Web 代理服务器 IP 地址、端口、代理主机列表以及管理员用户名和密码。如果您在网络中部署代理服务器，这些设置是可选的（如果适用）。| Citrix Gateway	配置 Web 代理的用户名时，可以使用 sAMAccountName 或用户主体名称 (UPN)。| XenMobile 和 Citrix Gateway	
记录默认网关 IP 地址。	XenMobile 和 Citrix Gateway	
记录系统 IP (NSIP) 地址和子网掩码。	Citrix Gateway	
记下子网 IP (SNIP) 地址和子网掩码。	Citrix Gateway	
记录证书中的 Citrix Gateway 虚拟服务器 IP 地址和 FQDN。要配置多个虚拟服务器，请记录证书中的所有虚拟 IP 地址和 FQDN。	Citrix Gateway	
记录用户可通过 Citrix Gateway 访问的内部网络。例如：10.10.0.0/24。输入用户在以下情况下需要访问的所有内部网络和网段：通过 Secure Hub 或 Citrix Gateway 插件连接时，拆分通道设置为 “开” 时。	Citrix Gateway	
确保 XenMobile Server、Citrix Gateway、外部 Microsoft SQL Server 与 DNS 服务器之间的网络连接良好。	XenMobile 和 Citrix Gateway	

许可

XenMobile 要求您购买 Citrix Gateway 和 XenMobile 的许可选项。有关 Citrix Licensing 的详细信息，请参阅 The Citrix Licensing System（Citrix Licensing 系统）。

必备条件	组件	记录位置
从 Citrix Web 站点获取通用许可证。有关详细信息，请参阅 Citrix Gateway 文档中的“许可”。	Citrix Gateway、XenMobile 和 Citrix 许可证服务器	

证书

XenMobile 和 Citrix Gateway 需要使用证书来启用用户设备与其他 Citrix 产品和应用程序的连接。有关详细信息，请参阅 XenMobile 文档中的证书和身份验证部分。

必备条件	组件	备注
获取并安装所需的证书。	XenMobile 和 Citrix Gateway	

端口

打开端口以允许与 XenMobile 组件通信。

必备条件	组件	备注
打开用于 XenMobile 的端口	XenMobile 和 Citrix Gateway	

数据库

XenMobile 需要数据库连接配置。XenMobile 存储库要求 Microsoft SQL Server 数据库在系统要求和兼容性中记录的受支持版本之一上运行。Citrix 建议远程使用 Microsoft SQL。PostgreSQL 随附在 XenMobile 中。仅在测试环境中本地或远程使用 PostgreSQL。

默认情况下，XenMobile 使用 jTDS 数据库驱动程序。要对 XenMobile Server 的本地安装使用 Microsoft JDBC 驱动程序，请参阅 SQL Server 驱动程序。

必备条件	组件	备注
Microsoft SQL Server IP 地址和端口。确保要用于 XenMobile 的 SQL Server 服务帐户具有 DBcreator 角色权限。	XenMobile	

Active Directory 设置

必备条件	组件	备注
————	———	————
记录主服务器和辅助服务器的 Active Directory IP 地址和端口。如果使用端口 636，请在 XenMobile 上安装 CA 的根证书，并将使用安全连接选项设置为是。	XenMobile 和 Citrix Gateway
记录 Active Directory 域名。	XenMobile 和 Citrix Gateway
记录 Active Directory 服务帐户，该帐户需要用户 ID、密码和域别名。
Active Directory 服务帐户是 XenMobile 用来查询 Active Directory 的帐户。	XenMobile 和 Citrix Gateway
记录用户基础 DN，这是用户所在的目录级别。例如：`cn=users,dc=ace,dc=com`。Citrix Gateway 和 XenMobile 使用用户基础 DN 来查询 Active Directory。	XenMobile 和 Citrix Gateway	
记录组基础 DN，这是组所在的目录级别。Citrix Gateway 和 XenMobile 使用此 DN 来查询 Active Directory。	XenMobile 和 Citrix Gateway	

XenMobile 与 **Citrix Gateway** 之间的连接

必备条件	组件	记录设置
记录 XenMobile 主机名。	XenMobile	
记录 XenMobile 的 FQDN 或 IP 地址。	XenMobile	
识别用户可以访问的应用程序。	Citrix Gateway	
记录回调 URL。	XenMobile	

用户连接：访问 **Citrix Virtual Apps and Desktops** 和 **Citrix Secure Hub**

Citrix 建议在 Citrix ADC 中使用快速配置向导来配置 XenMobile 与 Citrix Gateway 之间以及 XenMobile 与 Secure Hub 之间的连接设置。可以创建第二个虚拟服务器以允许用户从 Citrix Receiver 和 Web 浏览器建立连接。这些连接是与 Virtual Apps and Desktops 中基于 Windows 的应用程序和虚拟桌面建立的。Citrix 建议您同时在 Citrix ADC 中使用快速配置向导来配置这些设置。

必备条件	组件	记录设置
记录 Citrix Gateway 主机名和外部 URL。外部 URL 是用户用来进行连接的 Web 地址。	XenMobile	
记录 Citrix Gateway 回调 URL。	XenMobile	

必备条件	组件	记录设置
记录虚拟服务器的 IP 地址和子网掩码。	Citrix Gateway	
记录 Program Neighborhood Agent 或 Virtual Apps and Desktops 站点的路径。	Citrix Gateway 和 XenMobile	
记录运行 Secure Ticket Authority (STA) 的 Citrix Virtual Apps and Desktops 服务器的 FQDN 或 IP 地址（仅限 ICA 连接）。	Citrix Gateway	
记录 XenMobile 的公共 FQDN。	Citrix Gateway	
记录 Secure Hub 的公共 FQDN。	Citrix Gateway	

XenMobile 部署的流程图

可以使用此流程图指导您完成部署 XenMobile 的主要步骤。图后面提供每个步骤的主题链接。

1：系统要求和兼容性

2：安装和配置

3 和 4：预安装核对表（本文）

5：在命令提示窗口中配置 XenMobile（本文）

6：在 Web 浏览器中配置 XenMobile（本文）

7：配置 XenMobile 环境的设置

8：端口要求

安装 XenMobile

XenMobile 虚拟机 (VM) 在 Citrix XenServer、VMware ESXi 或 Microsoft Hyper-V 上运行。可以使用 XenCenter 或 vSphere 管理控制台安装 XenMobile。

> 注意：
>
> 确保使用正确的时间配置虚拟机管理程序（使用 NTP 服务器或手动配置），因为 XenMobile 会使用该时间。如果您在将 XenMobile 时间与虚拟机管理程序同步时遇到时区问题，可以通过将 XenMobile 指向 NTP 服务器来避免这些问题。为此，请使用 XenMobile CLI，如命令行接口选项中所述。

XenServer 或 **VMware ESXi** 必备条件。在 XenServer 或 VMware ESXi 上安装 XenMobile 之前，必须执行以下操作。有关详细信息，请参阅 XenServer 或 VMware 文档。

- 在硬件资源充足的计算机上安装 XenServer 或 VMware ESXi。
- 在单独的计算机上安装 XenCenter 或 vSphere。托管 XenCenter 或 vSphere 的计算机通过网络连接 XenServer 或 VMware ESXi 主机。

Hyper-V 必备条件。在 Hyper-V 上安装 XenMobile 之前，必须执行以下操作。有关详细信息，请参阅 Hyper-V 文档。

- 在具有充足系统资源的计算机上安装 Windows Server 2008 R2、Windows Server 2012 或已启用 Hyper-V 和角色的 Windows Server 2012 R2。安装 Hyper-V 角色时，请确保在服务器上指定 Hyper-V 用来创建虚拟网络的 NIC。可以保留某些 NIC 供主机使用。
- 删除 Virtual Machines/<*build-specific UUID*>.xml 文件
- 将 Legacy/<*build-specific UUID*>.exp 文件移到虚拟机内

如果安装 Windows Server 2008 R2 或 Windows Server 2012，请执行以下操作：

由于有两个不同版本的 Hyper-V 清单文件可以表示 VM 配置 (.exp and .xml)，因此这些步骤 X 分必要。Windows Server 2008 R2 和 Windows Server 2012 版本仅支持.exp。对于这些版本，您在安装前必须只具有.exp 清单文件。

Windows Server 2012 R2 不要求执行这些额外步骤。

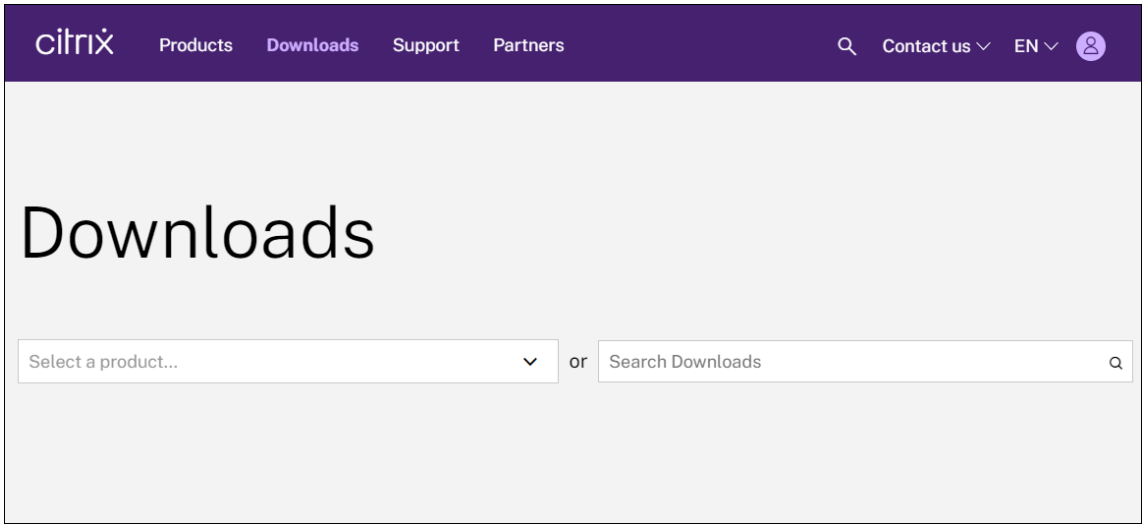
FIPS 140-2 模式。要在 FIPS 模式下安装 XenMobile Server，请完成一组必备条件，如在 XenMobile 中配置 FIPS 中所述。

下载 **XenMobile** 产品软件

可以从 Citrix Web 站点下载产品软件。登录该站点，然后使用“下载”链接导航到包含要下载的软件的页面。

下载 **XenMobile** 的软件

1. 访问 Citrix Web 站点。
2. 在“搜索”框旁边，单击登录，然后登录您的帐户。
3. 单击下载选项卡。
4. 在“下载”页面上，从选择产品列表中，单击 **Citrix Endpoint Management (**和 **Citrix XenMobile Server)**。Citrix Endpoint Management（和 Citrix XenMobile Server）页面将自动显示。



5. 展开 **XenMobile Server (**本地**)**。
6. 展开 **Product Software**（产品软件）。
7. 单击 **XenMobile Server 10**。
8. 单击 **Jump to Download**（跳至下载）菜单，选择要用于安装 XenMobile 的相应虚拟映像。此外，可以向下滚动页面以找到要安装的映像对应的 **Download File**（下载文件）按钮。
9. 按照屏幕上的说明下载软件。

下载 **Citrix Gateway** 的软件

可以执行以下过程来下载 Citrix Gateway 虚拟设备或现有 Citrix Gateway 设备的软件升级。

1. 访问 Citrix Web 站点。
2. 如果尚未登录 Citrix Web 站点，请在“搜索”框旁边，单击登录，然后登录您的帐户。
3. 单击下载选项卡。
4. 在“下载”页面上，从选择产品列表中，单击 **Citrix Gateway**。
5. 单击转到。此时将显示 Citrix Gateway 页面。
6. 在 Citrix Gateway 页面上，展开您运行的 Citrix Gateway 版本。
7. 在 **Firmware**（固件）下方，单击要下载的设备软件版本。

   > 注意：
   >
   > 还可以单击 **Virtual Appliances**（虚拟设备）以下载 Citrix ADC VPX。选择此选项时，将显示适用于每个虚拟机管理程序所对应的虚拟机的软件列表。

8. 单击要下载的设备软件版本。
9. 在要下载的版本对应的设备软件页面上，单击相应的虚拟设备对应的 **Download**（下载）。

10. 按照屏幕上的说明下载软件。

为首次使用配置 XenMobile

1. 要为 XenMobile 配置 IP 地址和子网掩码、默认网关和 DNS 服务器，请使用 XenCenter 或 vSphere 命令行控制台。

   > 注意：
   >
   > 使用 vSphere Web Client 时，我们建议您在 **Customize template**（自定义模板）页面上部署 OVF 模板过程中不要配置网络连接属性。因此，在高可用性配置中，您可以避免克隆并重新启动第二个 XenMobile 虚拟机时 IP 地址出现问题。

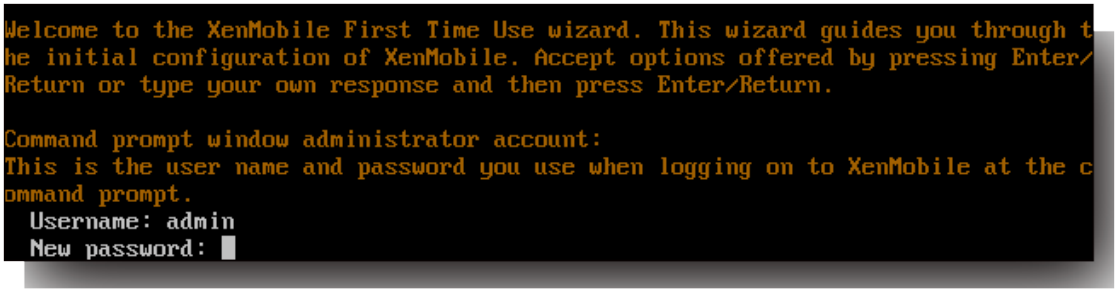
2. 只能通过 XenMobile Server 的完全限定域名或节点的 IP 地址访问 XenMobile 管理控制台。
3. 登录并按照初始登录屏幕上的步骤进行操作。

在命令提示窗口中配置 XenMobile

1. 将 XenMobile 虚拟机导入 Citrix XenServer、Microsoft Hyper-V 或 VMware ESXi 中。有关详细信息，请参阅 XenServer、Hyper-V 或 VMware 文档。
2. 在虚拟机管理程序中，选择导入的 XenMobile 虚拟机，然后启动命令提示窗口视图。有关详细信息，请参阅您的虚拟机管理程序的文档。
3. 从虚拟机管理程序的控制台页面，通过在命令提示窗口中键入管理员用户名和密码，为 XenMobile 创建管理员帐户。

   创建或更改命令提示窗口管理员帐户、公钥基础结构 (PKI) 服务器证书和 FIPS 的密码时，XenMobile 针对除 Active Directory 用户（其密码在 XenMobile 外部管理）之外的所有用户强制执行以下规则。

   - 密码的长度至少为八个字符。
   - 密码必须至少满足以下复杂条件中的三项：
     - 大写字母（A 至 Z）
     - 小写字母（a 至 z）
     - 数字（0 至 9）
     - 特殊字符（如！ ## $ %）



键入新密码时，不会显示任何字符，例如星号。

4. 提供以下网络信息，然后键入 **y** 以提交设置：

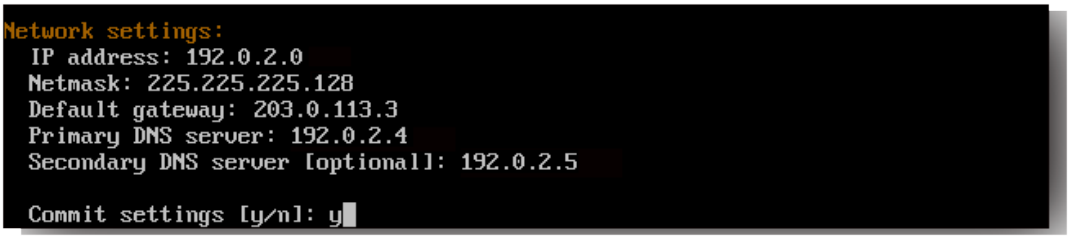
   a) XenMobile Server 的 IP 地址

   b) 网络掩码

   c) Default gateway（默认网关），即 DMZ 中默认网关的 IP 地址

   d) Primary DNS server（主 DNS 服务器），即 DNS 服务器的 IP 地址

   e) Secondary DNS server（辅助 DNS 服务器）（可选）



> 注意：
>
> 本图片和后面的图片中显示的地址并不可用，仅作为示例提供。

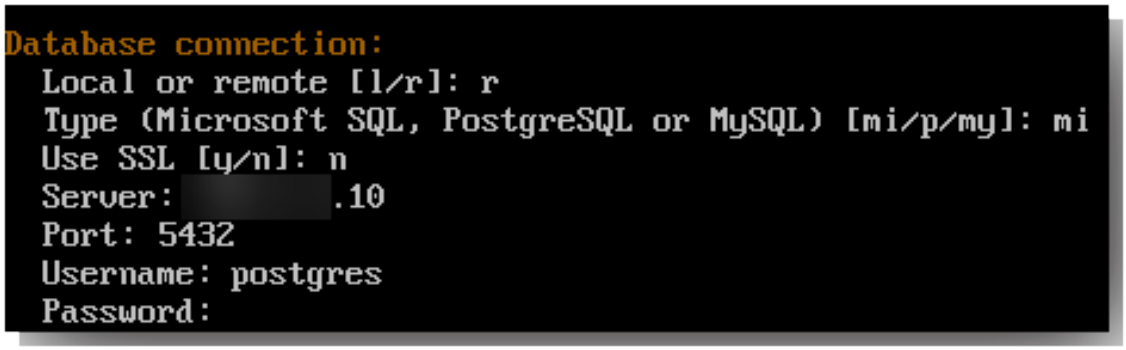
5. 键入 **y** 可通过生成随机的加密密码增加安全性，或者键入 **n** 提供自己的密码。Citrix 建议键入 **y** 以生成随机密码。

   密码是加密密钥（用于保护敏感数据）保护措施的一部分。密码哈希存储在服务器文件系统中，用于在加密数据和解密数据过程中提取密钥。无法查看密码。

> 注意：
>
> 如果打算扩展您的环境并配置更多服务器，请提供您自己的密码。如果选择随机密码，则不能查看。

6. （可选）启用联邦信息处理标准 (FIPS)。有关 FIPS 的详细信息，请参阅 FIPS。此外，请务必完成一组必备条件，如在 XenMobile 中配置 FIPS 中所述。

7. 提供以下信息以配置数据库连接。



- 数据库可以是本地数据库或远程数据库。键入 **l** 表示本地数据库，键入 **r** 表示远程数据库。
- 选择数据库类型。键入 **mi** 表示 Microsoft SQL，键入 **p** 表示 PostgreSQL。

  > 重要：
  >
  > – Citrix 建议远程使用 Microsoft SQL。PostgreSQL 随附在 XenMobile 中。仅在测试环境中本地或远程使用 PostgreSQL。
  > – 不支持数据库迁移。在测试环境下创建的数据库不能移动到生产环境中。

- （可选）键入 **y** 以对数据库使用 SSL 身份验证。
- 提供托管 XenMobile 的服务器的完全限定的域名 (FQDN)。此单个主机服务器同时提供设备管理服务和应用程序管理服务。
- 键入数据库端口号（如果数据库端口号与默认端口号不同）。Microsoft SQL 的默认端口为 1433，PostgreSQL 的默认端口为 5432。
- 键入您的数据库管理员用户名。
- 键入您的数据库管理员密码。
- 键入数据库名称。
- 按 **Enter** 键提交数据库设置。

8. （可选）键入 **y** 以启用群集 XenMobile 节点或实例。

   > 重要：
   >
   > 如果启用 XenMobile 群集，完成系统配置后，请打开端口 80，以便在群集成员之间启用实时通信。请在所有群集节点上完成该设置。

9. 键入 XenMobile Server 完全限定的域名 (FQDN)。

10. 按 **Enter** 键提交设置。

11. 识别通信端口。有关端口及其用法的详细信息，请参阅端口要求。

    > 注意：
    >
    > 通过按 **Enter**（在 Mac 上为 Return）接受默认端口。

    ```
    HTTP [80]: 80
    HTTPS with certificate authentication [443]: 443
    HTTPS with no certificate authentication [8443]: 8443
    HTTPS for management [4443]: 4443
    ```

12. 由于您是首次安装 XenMobile，请跳过下一个关于从之前的 XenMobile 版本进行升级的问题。

13. 如果要对每个公钥基础结构 (PKI) 证书使用相同密码，请键入 **y**。有关 XenMobile PKI 功能的详细信息，请参阅上载证书。

    ```
    The wizard will now generate an internal Public Key Infrastructure (PKI):
     - A root certificate
     - An intermediate certificate to issue device certificates during enrollment
     - An intermediate certificate to issue an SSL certificate
     - An SSL certificate for your connectors
      Do you want to use the same password for all the certificates of the PKI [y]:
      New password:
      Re-enter new password:
    ```

    > 重要：
    >
    > 如果打算将 XenMobile 的节点或实例群集在一起，请为后续节点提供完全相同的密码。

14. 键入新密码，然后重新输入新密码以确认。

    键入新密码时，不会显示任何字符，例如星号。

15. 按 **Enter** 键提交设置。

16. 创建管理员帐户以便使用 Web 浏览器登录 XenMobile 控制台。请务必记录这些凭据，供以后使用。

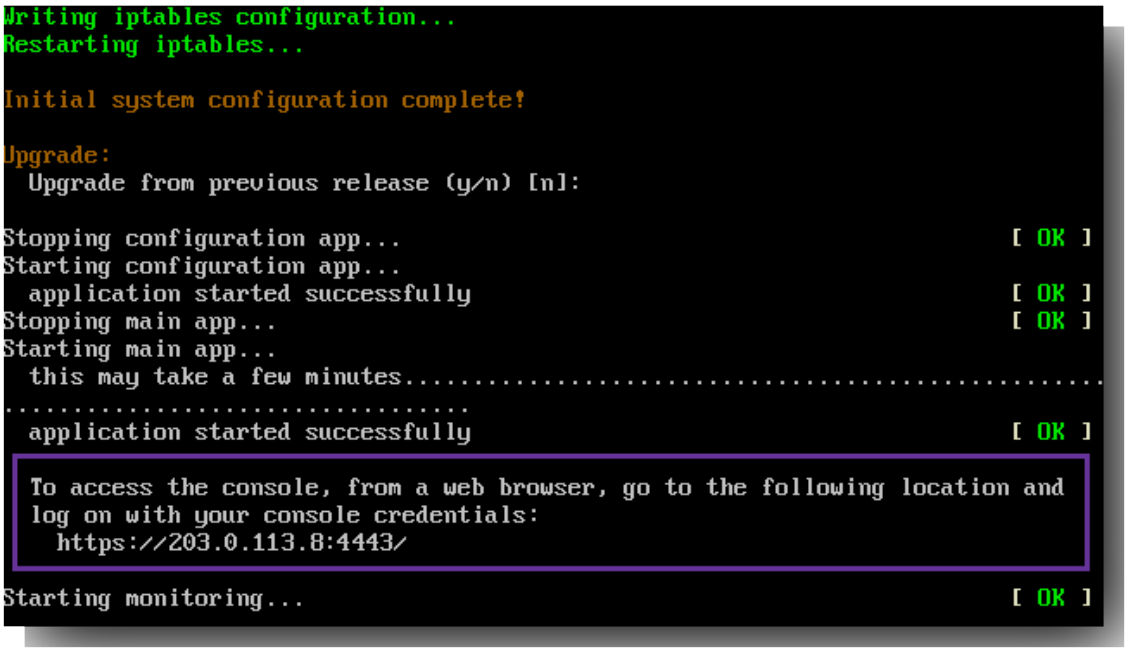
    ```
    XenMobile console administrator account:
    This is the user name and password you use when logging on to the XenMobile cons
    ole through a web browser.
      Username [administrator]: administrator
      Password:
      Re-enter new password:
    ```

    > 注意：
    >
    > 键入新密码时，不会显示任何字符，例如星号。

17. 按 **Enter** 键提交设置。此时已保存初始系统配置。

18. 当询问是否升级时，请键入 **n**，因为这是全新安装。

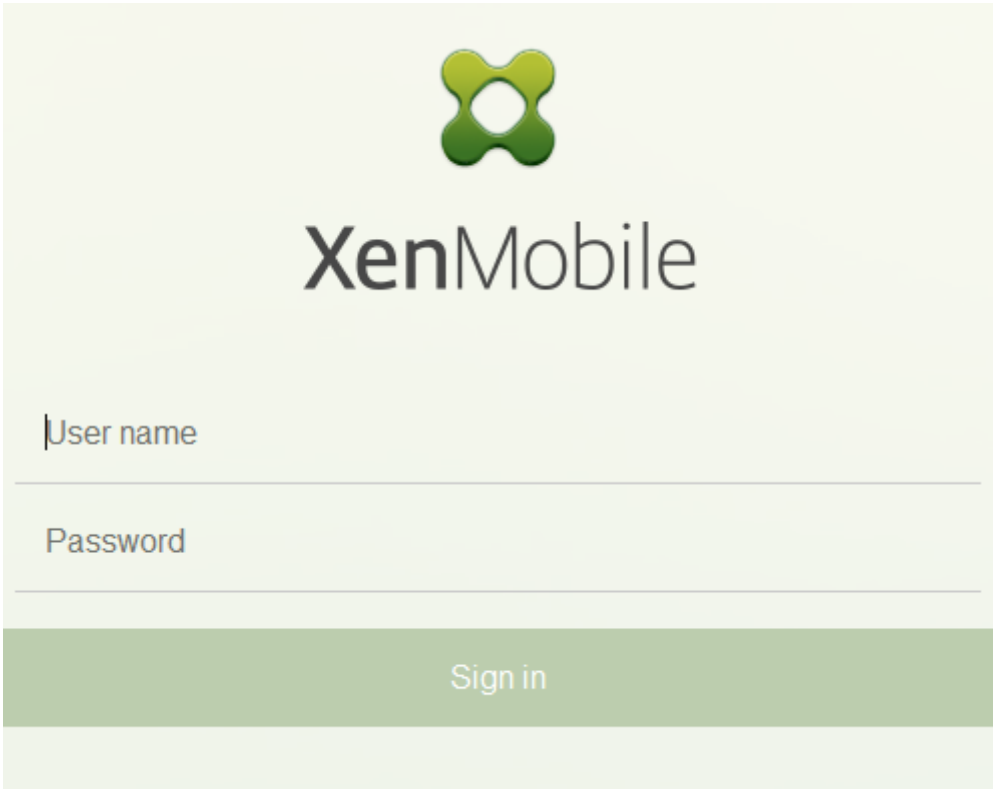
19. 完整复制屏幕上显示的 URL，并在 Web 浏览器中继续此初始 XenMobile 配置。



在 **Web** 浏览器中配置 **XenMobile**

在虚拟机管理程序命令提示窗口中完成 XenMobile 配置的初始部分后，在 Web 浏览器中完成该过程。

1. 在 Web 浏览器中，导航到命令提示窗口配置的结论部分提供的位置。
2. 键入在命令提示窗口中创建的 XenMobile 控制台管理员帐户的用户名和密码。



3. 在“开始”页面上，单击开始。此时将显示许可页面。
4. 配置许可证。如果未上载许可证，则使用有效期为 30 天的评估版许可证。有关添加和配置许可证以及配置过期通知的详细信息，请参阅许可。

   > 重要：
   >
   > 如果打算通过添加 XenMobile 的群集节点或实例来使用 XenMobile 群集，必须在远程服务器上使用 Citrix Licensing。

5. 在证书页面上，单击导入。此时将显示导入对话框。
6. 导入您的 APNs 和 SSL 侦听器证书。iOS 设备管理需要 APNs 证书。有关使用证书的详细信息，请参阅证书。

   > 注意：
   >
   > 此步骤需要重新启动服务器。

7. 如果适用于环境，请配置 Citrix Gateway。有关配置 Citrix Gateway 的详细信息，请参阅 Citrix Gateway 和 XenMobile 以及配置 XenMobile 环境的设置。

   > 注意：
   >
   > - 可以在您的内部网络（或 Intranet）外围部署 Citrix Gateway。在部署中，您可以安全地单点访问内部网络中驻留的服务器、应用程序和其他网络资源。在此部署中，所有远程用户必须先连接到 Citrix Gateway，才能访问内部网络中的任何资源。
   > - 尽管 Citrix Gateway 为可选设置，但在页面上输入数据后，必须清除或完成必填字段，才能离开页

> 面。

8. 完成 LDAP 配置，以便从 Active Directory 访问用户和组。有关配置 LDAP 连接的详细信息，请参阅 LDAP 配置。
9. 配置能够向用户发送消息的通知服务器。有关通知服务器配置的详细信息，请参阅通知。

后续条件。重新启动 XenMobile Server 以激活您的证书。

在 **XenMobile** 中配置 **FIPS**

January 5, 2022

XenMobile 中的联邦信息处理标准 (Federal Information Processing Standards, FIPS) 模式通过对所有加密操作仅使用通过 FIPS 140-2 认证的库来支持美国联邦政府客户。在 FIPS 模式下安装 XenMobile Server 可确保 XenMobile 客户端与服务器的数据完全符合 FIPS 140-2。该合规性适用于静态数据和传输中的数据。

在 FIPS 模式下安装 XenMobile Server 之前，应完成以下必备条件。

- 必须对 XenMobile 数据库使用外部 SQL Server 2014。还必须配置 SQL Server 以实现安全 SSL 通信。有关配置与 SQL Server 的安全 SSL 通信的说明，请参阅 Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)（启用与数据库引擎 (SQL Server Configuration Manager) 的加密连接）。
- 安全 SSL 通信要求您在 SQL Server 上安装来自众所周知的证书颁发机构 (CA) 的可信 SSL 证书。请注意，SQL Server 2014 无法接受通配符证书。因此，Citrix 建议您通过 SQL Server 的 FQDN 请求 SSL 证书。

配置 **FIPS** 模式

可以在对 XenMobile Server 进行初始设置过程中启用 FIPS 模式。安装完成后则无法启用 FIPS。因此，如果您打算使用 FIPS 模式，则必须在开始时在 FIPS 模式下安装 XenMobile Server。此外，对于 XenMobile 群集，所有群集节点都必须启用 FIPS。不能在同一个群集中混合使用 FIPS 和非 FIPS XenMobile Server。

XenMobile 命令行接口中存在一个不用于生产的 **Toggle FIPS mode**（切换 FIPS 模式）选项。此选项专用于非生产诊断，在生产型 XenMobile Server 上不受支持。

1. 在初始设置过程中，启用 **FIPS mode**（FIPS 模式）。
2. 上载 SQL Server 的根 CA 证书。
3. 指定 SQL Server 的服务器名称和端口，用于登录 SQL Server 的凭据以及要为 XenMobile 创建的数据库名称。

> 注意：

> 可以使用 SQL 登录帐户或 Active Directory 帐户访问 SQL Server，但您使用的登录帐户必须具有 DBcreator 角色。

4. 要使用 Active Directory 帐户，请以 domain\username 格式输入凭据。
5. 完成这些步骤后，请继续执行 XenMobile 初始设置。

要确认 FIPS 模式是否已成功配置，请登录 XenMobile 命令行接口。登录横幅中将显示短语 **In FIPS Compliant Mode**（处于 FIPS 兼容模式）。

导入证书

以下步骤介绍了如何通过导入证书在 XenMobile 上配置 FIPS，使用 VMware 虚拟机管理程序时需要使用该模式。

SQL 必备条件

1. 从 XenMobile 到 SQL 实例的连接必须安全，且必须是 SQL Server 2012 或 SQL Server 2014。要确保连接安全，请参阅 How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console（如何使用 Microsoft 管理控制台为 SQL Server 的实例启用 SSL 加密）。
2. 如果该服务未正确重新启动，请检查以下项：打开 **Services.msc**。
   a) 复制用于 SQL Server 服务的登录帐户信息。
   b) 在 SQL Server 上打开 MMC.exe。
   c) 转至文件 **>** 添加/删除管理单元，然后双击证书项以添加证书管理单元。在向导中的两个页面上选择计算机帐户和本地计算机。
   d) 单击确定。
   e) 展开证书 **(**本地计算机**) >** 个人 **>** 证书，找到导入的 SSL 证书。
   f) 右键单击导入的证书（在 SQL Server 配置管理器中进行选择），然后单击所有任务 **>** 管理私钥。
   g) 在组或用户名下方，单击添加。
   h) 输入在之前的步骤中复制的 SQL 服务帐户名称。
   i) 取消选中允许完全控制选项。默认情况下，该服务帐户将被同时授予完全控制和读取权限，但只需要能够读取私钥。
   j) 关闭 **MMC** 并启动 SQL 服务。
3. 确保 SQL 服务已正确启动。

Internet Information Services (IIS) 必备条件

1. 下载根证书 (base 64)。

2. 将根证书复制到 IIS 服务器上的默认站点 C:\inetpub\wwwroot。
3. 选中默认站点的身份验证复选框。
4. 将匿名设置为已启用。
5. 选中失败请求跟踪规则复选框。
6. 确保.cer 不被阻止。
7. 从本地服务器浏览到 Web 浏览器中的.cer 的位置 `https://localhost/certname.cer`。根证书文本将显示在浏览器中。
8. 如果根证书未显示在您的 Web 浏览器中，请务必按如下所示在 IIS 服务器上启用 ASP。
   a) 打开服务器管理器。
   b) 在管理 **>** 添加角色和功能中导航到向导。
   c) 在服务器角色中，依次展开 **Web** 服务器 **(IIS)**、**Web** 服务器和应用程序开发，然后选择 **ASP**。
   d) 完成安装后，单击下一步。
9. 浏览到 `https://localhost/cert.cer`。

   有关详细信息，请参阅 Web 服务器 (IIS)。

   > 注意：
   >
   > 在此过程可以使用 CA 的 IIS 实例。

在初始 **FIPS** 配置过程中导入根证书

在命令行控制台中完成首次配置 XenMobile 的步骤时，必须完成以下设置才能导入根证书。有关安装步骤的详细信息，请参阅安装 XenMobile。

- 启用 FIPS：是
- 上载根证书：是
- 复制 (c) 或导入 (i)：i
- 输入 HTTP URL 以导入：`https://<FQDN of IIS server>/cert.cer`
- 服务器：*SQL Server* 的 *FQDN*
- 端口：1433
- 用户名：可以创建数据库的服务帐户 (`domain\username`)。
- 密码：服务帐户的密码。
- 数据库名称：您选择的名称。

在移动设备上启用 **FIPS** 模式

默认情况下，FIPS 模式在移动设备上处于禁用状态。要启用 FIPS 模式，请转至设置 **>** 客户端属性，编辑启用 **FIPS** 模式属性，然后将值设置为 **true**。有关详细信息，请参阅客户端属性。

配置群集

December 14, 2020

要配置群集，请在 Citrix ADC 上配置下面两个负载平衡虚拟 IP 地址。

- 移动设备管理 **(MDM)** 负载平衡虚拟 **IP** 地址：与群集中配置的 XenMobile 节点进行通信需要使用 MDM 负载平衡虚拟 IP 地址。此负载平衡在 SSL 桥接模式下完成。
- 移动应用程序管理 **(MAM)** 负载平衡虚拟 **IP** 地址： Citrix Gateway 与群集中配置的 XenMobile 节点进行通信需要使用 MAM 负载平衡虚拟 IP 地址。在 XenMobile 中，默认情况下，来自 Citrix Gateway 的所有流量在端口 8443 上路由到负载平衡虚拟 IP 地址。

本文中的过程介绍了如何创建新 XenMobile 虚拟机 (VM) 以及将新 VM 加入现有 VM。这些步骤将创建群集设置。

必备条件

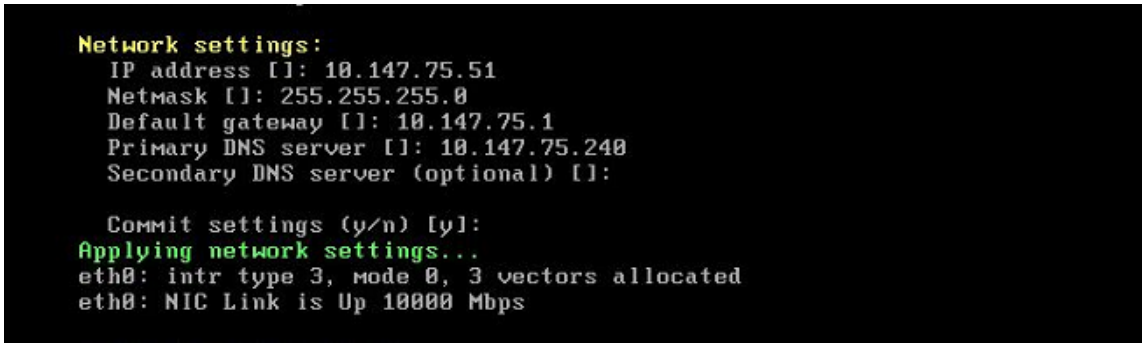
- 已完整配置所需的 XenMobile 节点。
- 在所有群集节点上和 XenMobile 数据库中配置 NTP。要使群集正常工作，所有服务器的时间都必须相同。
- 一个用于 MDM 负载平衡器的公用 IP 地址和一个用于 MAM 的专用 IP 地址。
- 服务器证书。
- 一个用作 Citrix Gateway 虚拟 IP 地址的可用 IP。
- 在群集设置中以及仅 MDM 或企业模式 (MDM+MAM) 下部署了 XenMobile 的情况下：将您的 Citrix ADC 负载平衡器配置修改为对所有 Citrix ADC MDM 负载平衡器（即，为端口 8443 和 443 设置的虚拟服务器）使用 **Source IP persistence**（源 IP 暂留）。请在用户设备升级到 iOS 11 之前完成该配置。有关详细信息，请参阅此 Citrix 知识中心文章：https://support.citrix.com/article/CTX227406。
- 必须在 XenMobile Server 上启用端口 80，才能在 iOS 11 设备上从 XenMobile Store 中安装应用程序。

有关群集配置中 XenMobile 10.x 的参考体系结构图，请参阅体系结构。

安装 **XenMobile** 群集节点

根据您需要的节点数，创建 XenMobile VM。将新 VM 指向相同的数据库并提供相同的 PKI 证书密码。

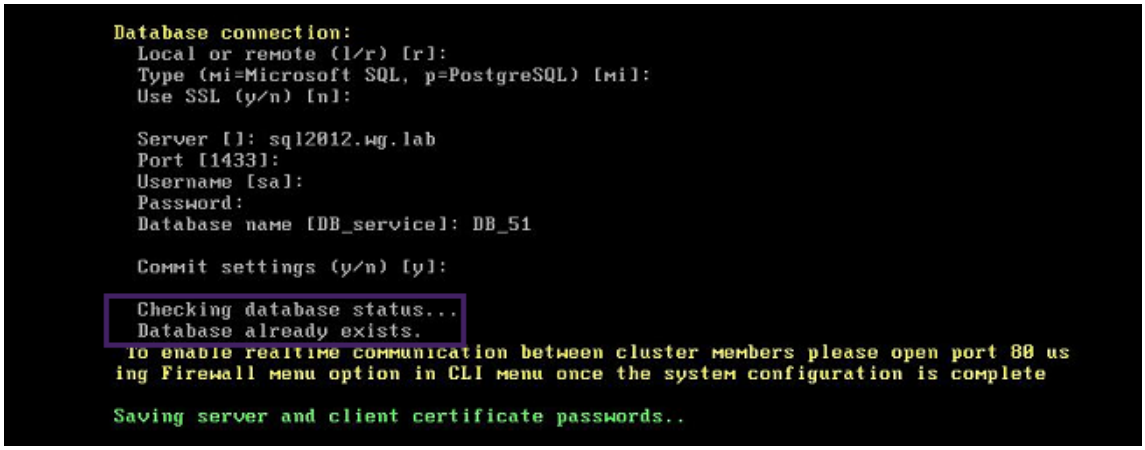
1. 打开新 VM 的命令行控制台，然后输入管理员帐户的新密码。
2. 提供网络配置详细信息，如下图所示。



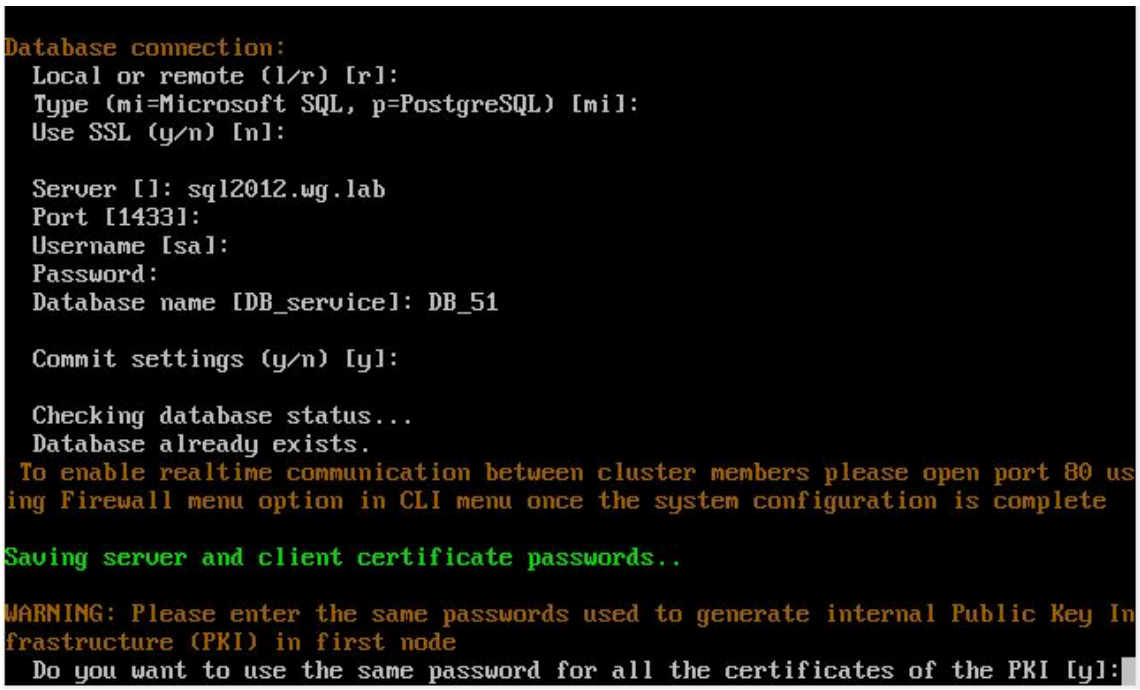
3. 如果要使用默认密码进行数据保护，请键入 **y**；否则，请键入 **n**，然后输入新密码。

4. 如果要使用 FIPS，请键入 **y**；否则，请键入 **n**。

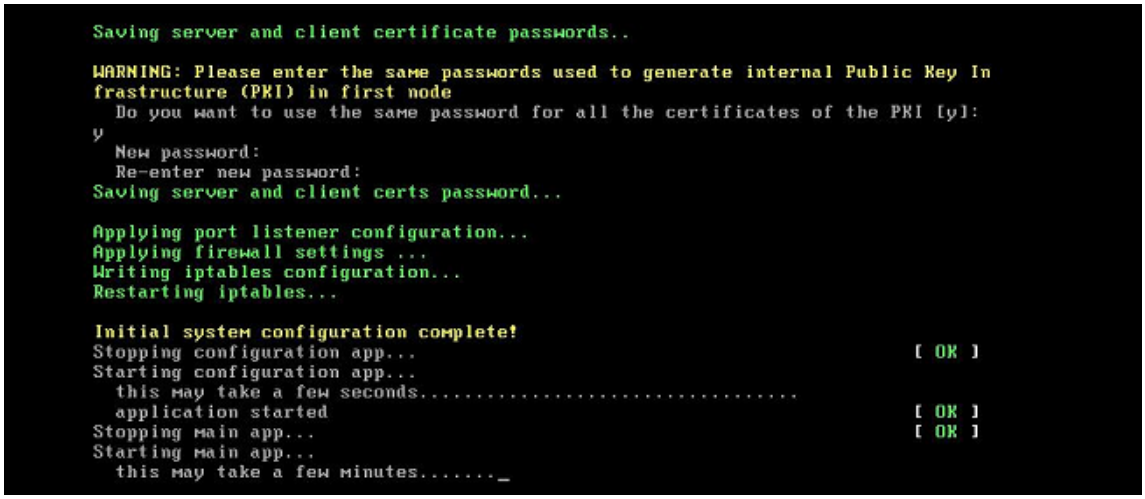
5. 配置数据库，以便指向之前完整配置的 VM 所指向的同一个数据库。将显示以下消息：Database already exists（数据库已经存在）。



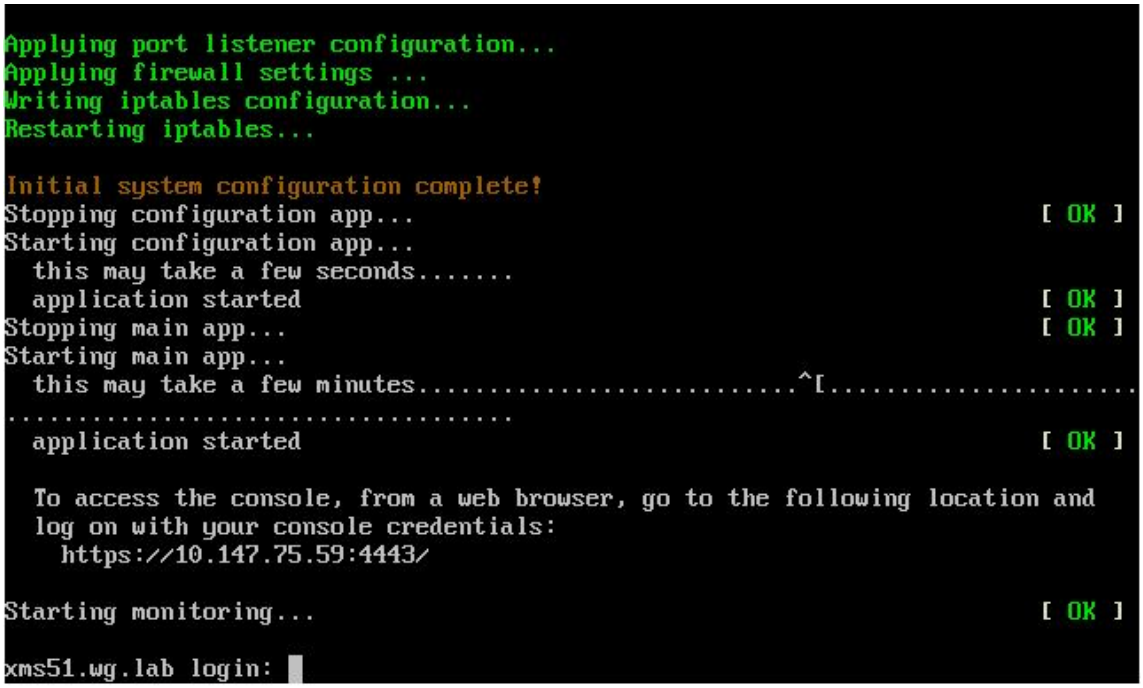
6. 输入与为第一个 VM 提供的证书相同的密码。



输入密码后，第二个节点上的初始配置将完成。



7. 完成配置后，服务器将重新启动，并将显示登录对话框。

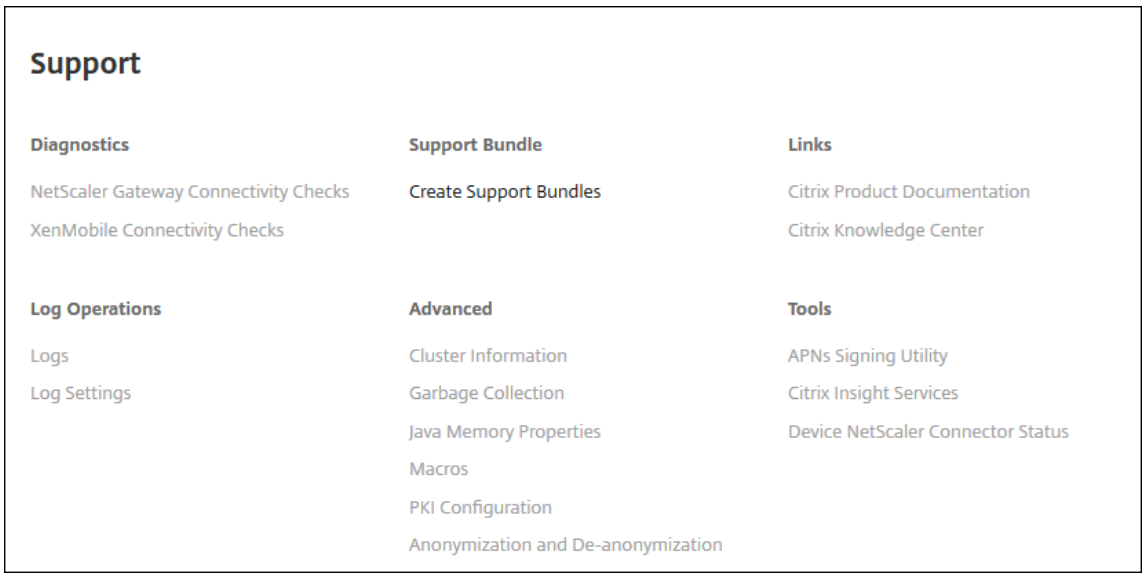


> 注意：
>
> 登录对话框与第一个 VM 的登录对话框相同。这种相同是供您确认两个 VM 使用相同的数据库服务器的一种途径。

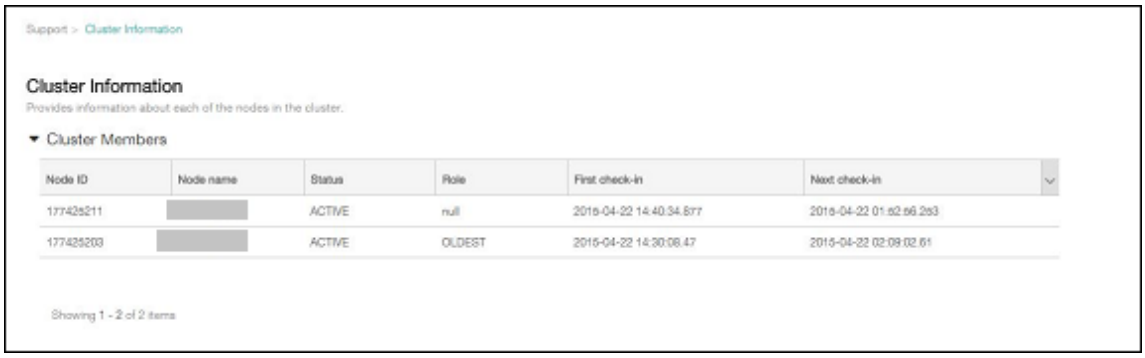
8. 使用 XenMobile 的完全限定的域名 (FQDN) 在 Web 浏览器中打开 XenMobile 控制台。
9. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。

此时将打开支持页面。

10. 在高级下方，单击群集信息。



将显示关于此群集的所有信息，包括群集成员、设备连接信息、任务等。新节点现在属于群集的成员。

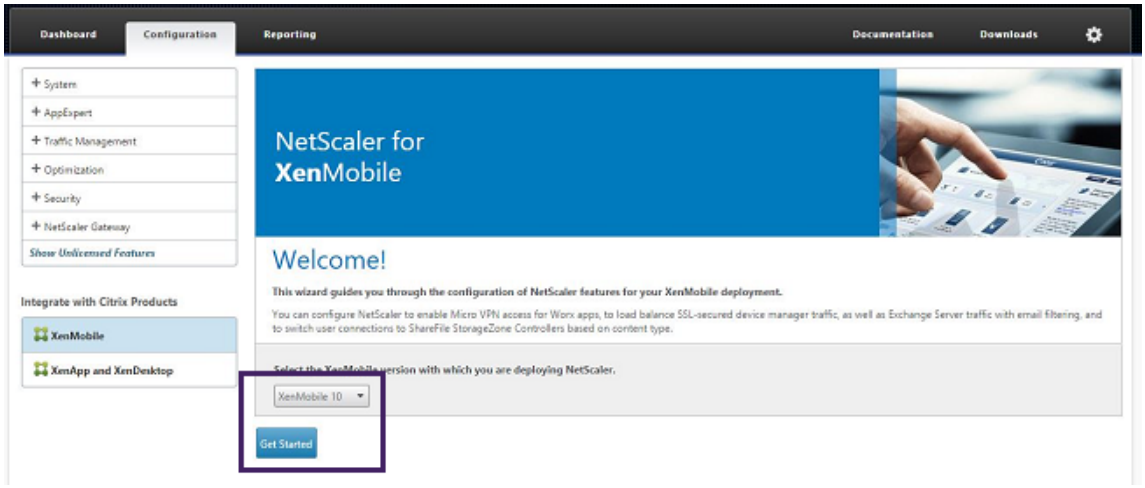


您可以按照相同的步骤添加其他节点。添加到群集的第一个节点的角色为最早。在其后添加的节点的角色为无或空。

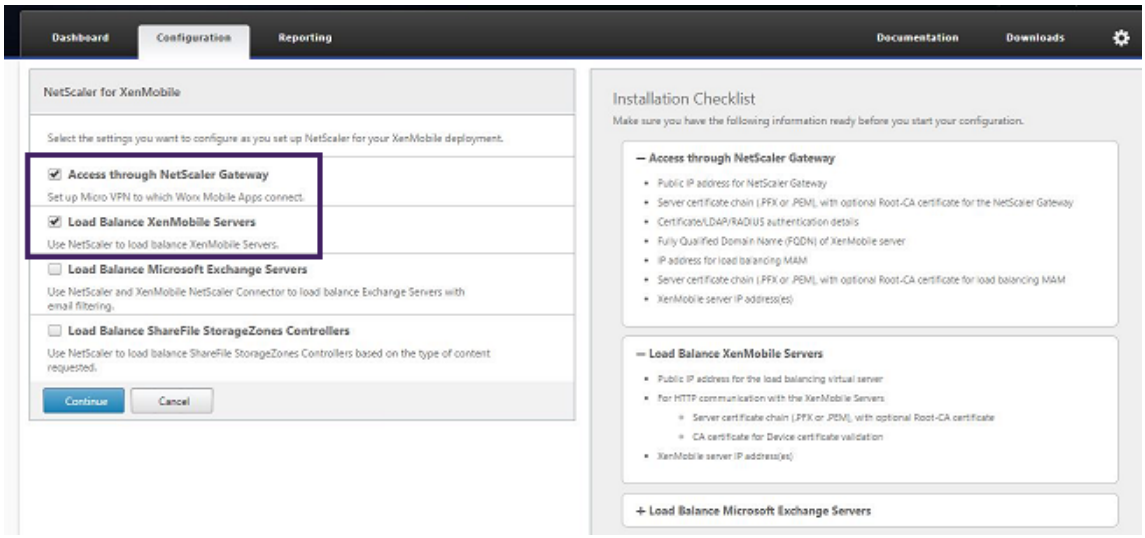
在 **Citrix ADC** 中为 **XenMobile** 群集配置负载平衡

将所需节点添加为 XenMobile 群集的成员后，对节点进行负载平衡，以便可以访问群集。负载平衡通过运行 Citrix ADC 中提供的 XenMobile 向导完成。以下步骤介绍了如何通过运行该向导对 XenMobile 进行负载平衡。

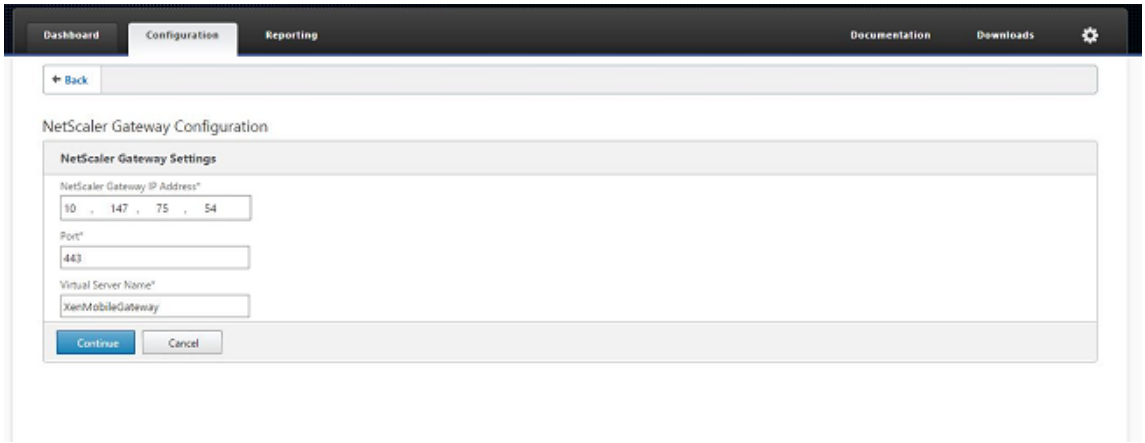
1. 登录到 Citrix ADC。
2. 在“Configuration”（配置）选项卡上，单击 **XenMobile**，然后单击 **Get Started**（开始）。



3. 选中 **Access through Citrix Gateway**（通过 Citrix Gateway 访问）复选框和 **Load Balance XenMobile Servers**（对 XenMobile Server 进行负载平衡）复选框，然后单击 **Continue**（继续）。



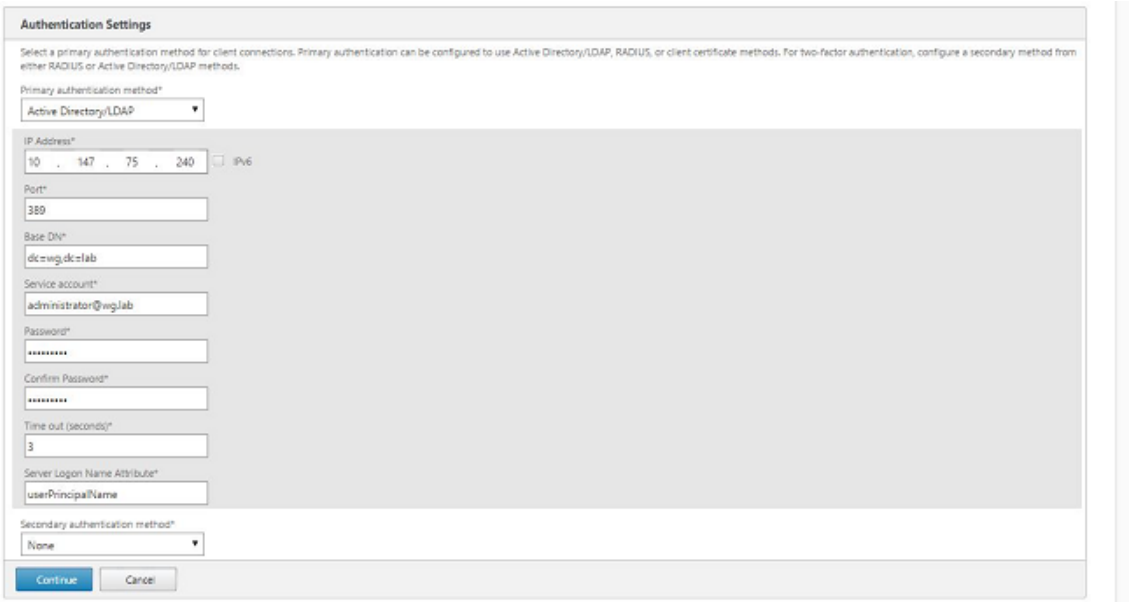
4. 输入 Citrix Gateway 的 IP 地址，然后单击 **Continue**（继续）。



5. 执行以下操作之一将服务器证书绑定到 Citrix Gateway 虚拟 IP 地址，然后单击 **Continue**（继续）。

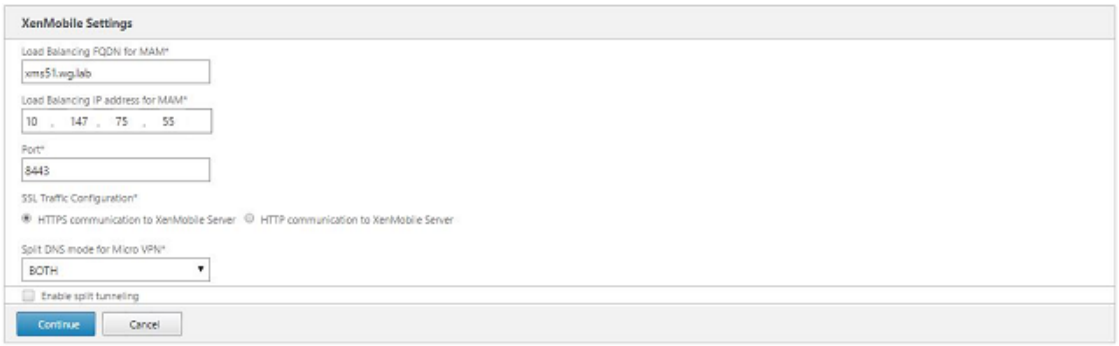
- 在 **Use existing certificate**（使用现有证书），从列表中选择服务器证书。
- 单击 **Install Certificate**（安装证书）选项卡以上载新的服务器证书。

6. 输入身份验证服务器详细信息，然后单击 **Continue**（继续）。



> 注意：
>
> 请确保“Server Logon Name Attribute”（服务器登录名称属性）与您在 XenMobile LDAP 配置中提供的相同。

7. 在“XenMobile Settings”（XenMobile 设置）下方的“Load Balancing FQDN for MAM”（MAM 的负载平衡 FQDN）中输入值，然后单击 **Continue**（继续）。



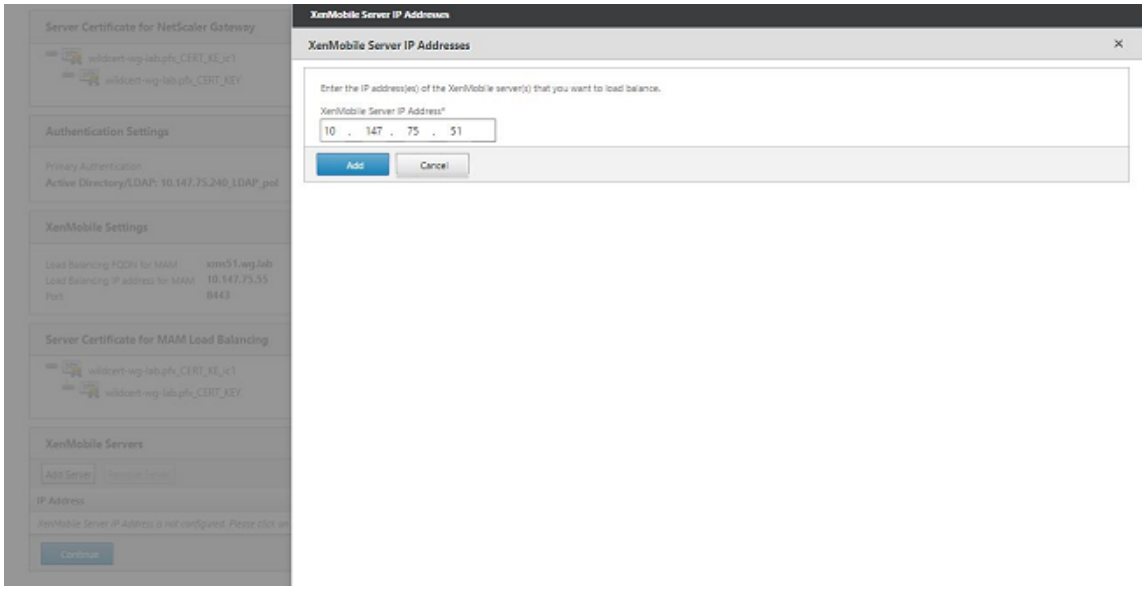
> 注意：
>
> 请确保 MAM 负载平衡虚拟 IP 地址的 FQDN 与 XenMobile 的 FQDN 相同。

8. 如果要使用 SSL 桥接模式 (HTTPS)，请选择 **HTTPS communication to XenMobile Server**（与 XenMobile Server 进行 HTTPS 通信）。但是，如果要使用 SSL 卸载，请选择 **HTTP communication to XenMobile Server**（与 XenMobile Server 进行 HTTP 通信），如上图所示。为实现本文的目的，请选择 SSL 桥接模式 (HTTPS)。

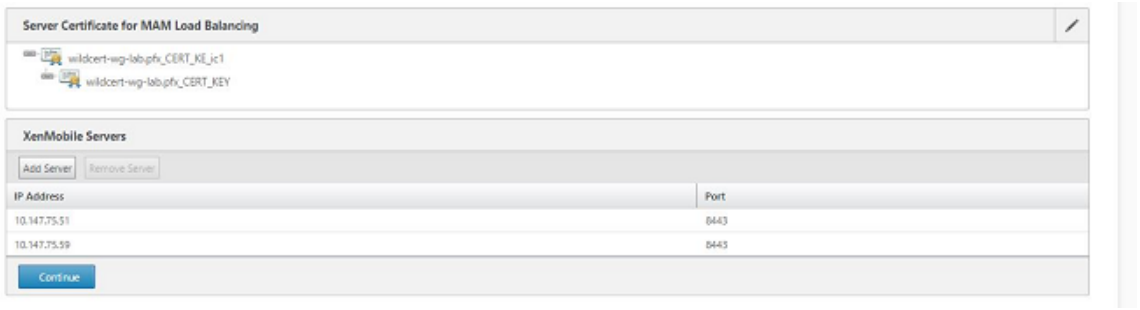
9. 为 MAM 负载平衡虚拟 IP 地址绑定服务器证书，然后单击 “Continue”（继续）。

10. 在 “XenMobile Servers”（XenMobile Server）下方，单击 **Add Server**（添加服务器）以添加 XenMobile 节点。

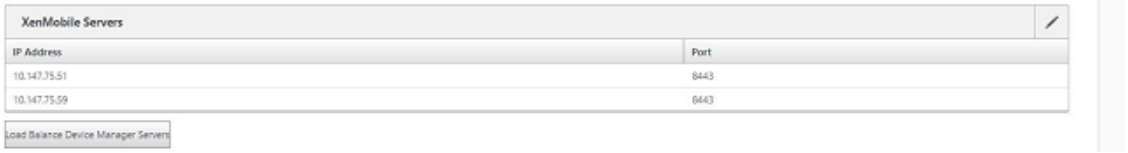
11. 输入 XenMobile 节点的 IP 地址，然后单击 “Add”（添加）。



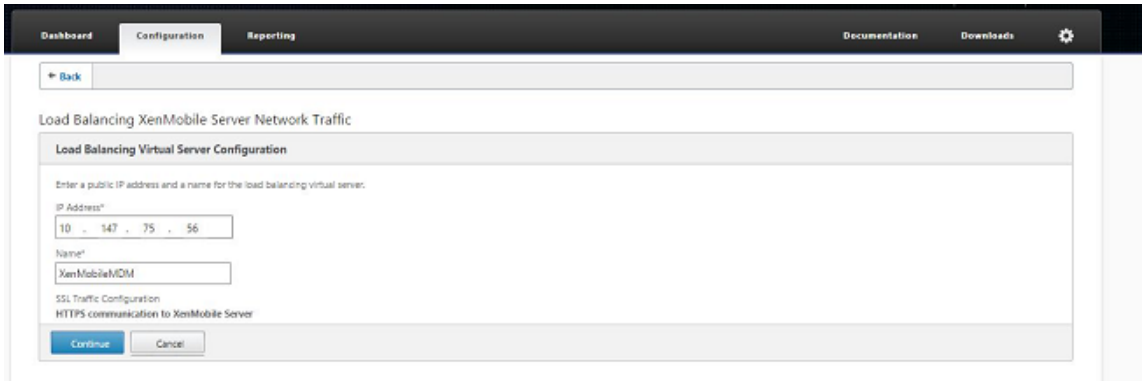
12. 重复步骤 10 和 11 以添加更多 XenMobile 节点，作为 XenMobile 群集的一部分。您将看到已添加的所有 XenMobile 节点。单击继续。



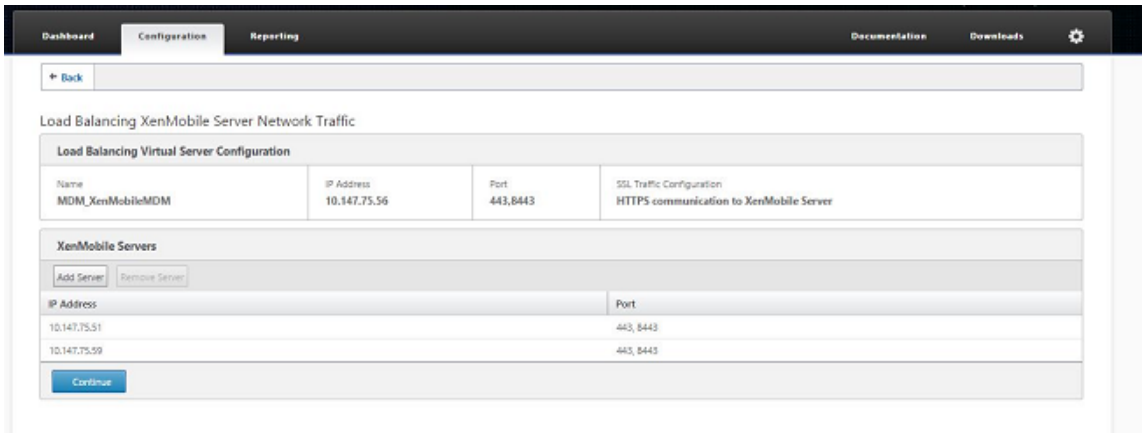
13. 单击 **Load Balance Device Manager Servers**（Device Manager 服务器负载平衡）以继续执行 MDM 负载平衡配置。



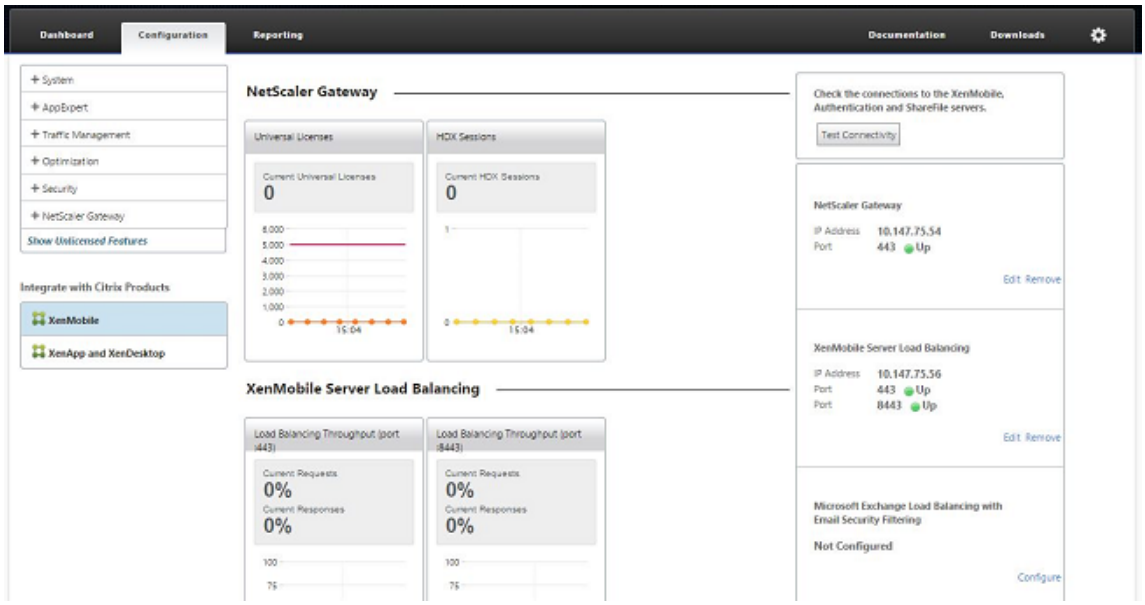
14. 输入要用作 MDM 负载平衡 IP 地址的 IP 地址，然后单击 **Continue**（继续）。



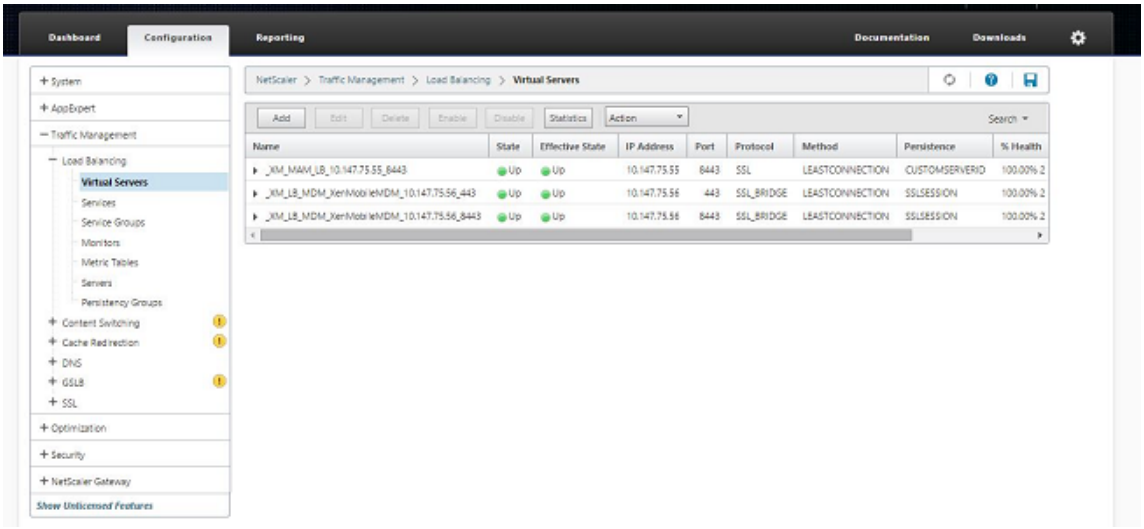
15. 列表中显示 XenMobile 节点后，单击 **Continue**（继续），然后单击“Done”（完成）以完成该过程。



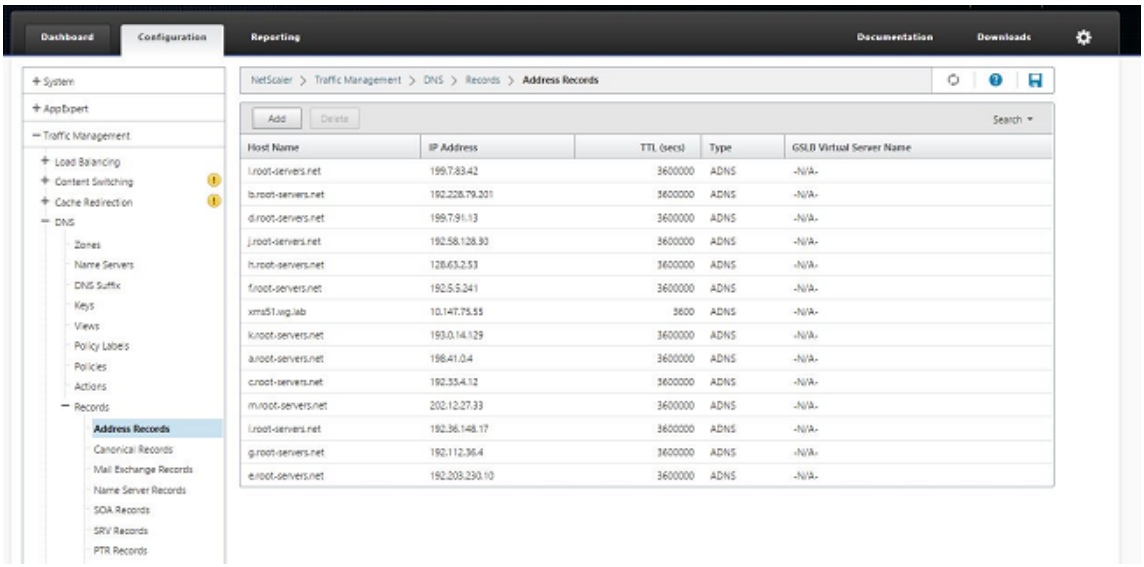
您将在 XenMobile 页面上看到虚拟 IP 地址状态。



16. 要确认虚拟 IP 地址是否已启用并运行，请单击“Configuration”（配置）选项卡，然后导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Virtual Servers**（虚拟服务器）。



您将看到 Citrix ADC 中的 DNS 条目指向 MAM 负载平衡虚拟 IP 地址。



灾难恢复指南

January 5, 2022

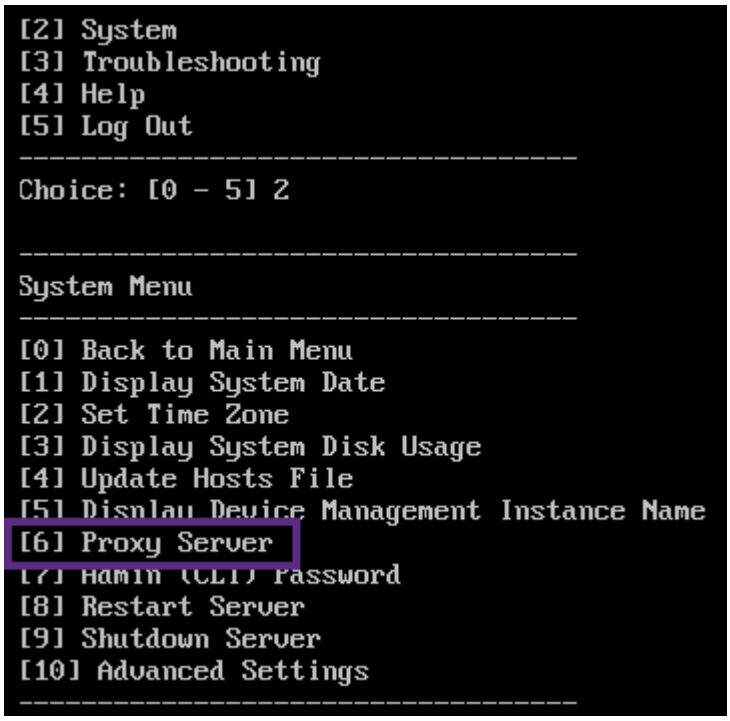
可以设计使用主-被故障转移策略的灾难恢复的多个站点的 XenMobile 部署的架构并配置该部署。有关详细信息，请参阅《XenMobile 部署手册》中的灾难恢复一文。

启用代理服务器

January 5, 2022

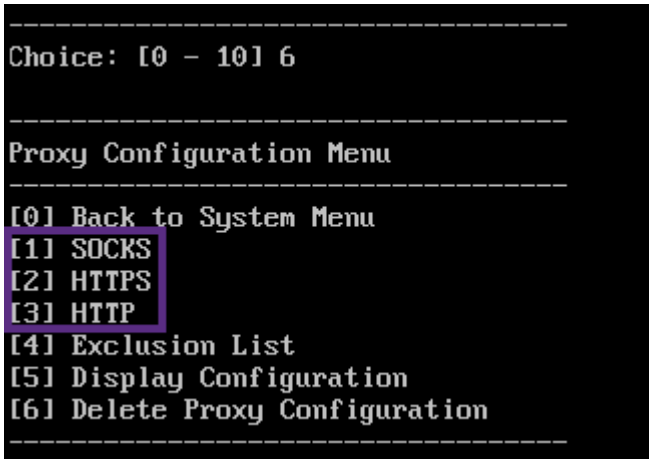
要控制出站 Internet 流量，可以在 XenMobile 中设置代理服务器来传输该流量。可通过命令行接口 (CLI) 设置代理服务器。设置代理服务器需要重新启动系统。

1. 在 XenMobile CLI 主菜单中，键入 **2** 以选择 “System Menu”（系统菜单）。
2. 在 “System Menu”（系统菜单）中，键入 **6** 以选择 “Proxy Server”（代理服务器）菜单。



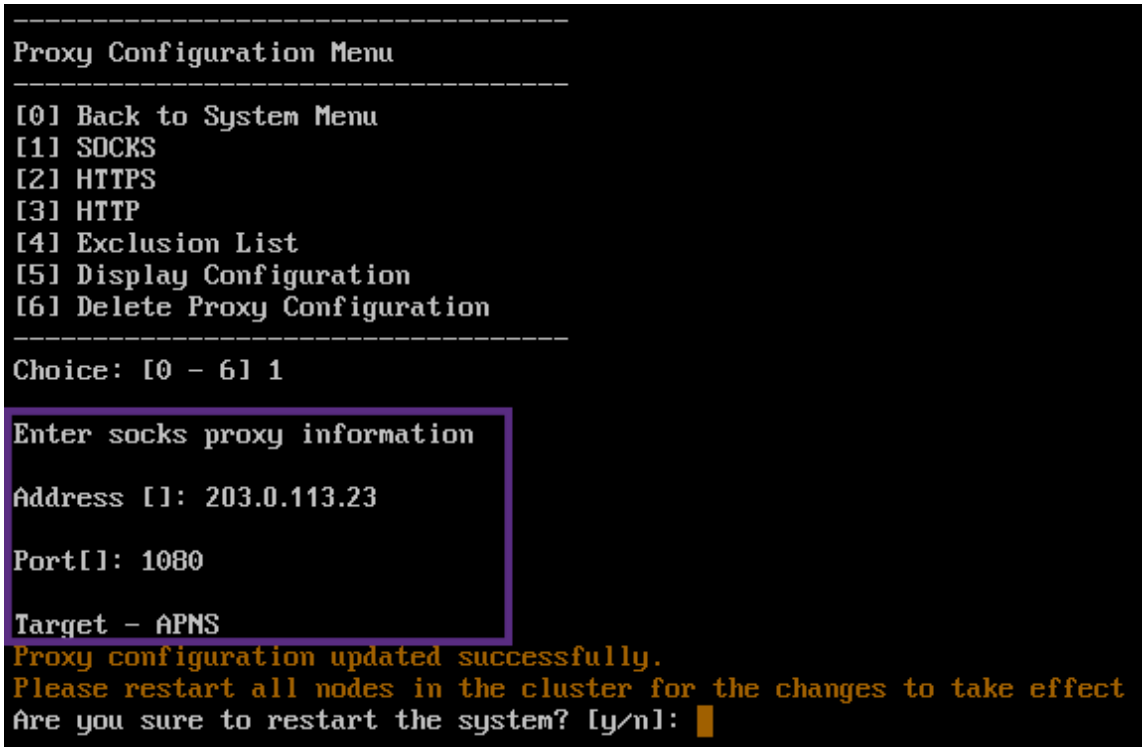
3. 在 “Proxy Configuration Menu”（代理配置菜单）中，键入 **1** 以选择 SOCKS。

   在保存此设置之前，还必须配置 HTTPS。除非您将 SOCKS 和 HTTPS 设置保存在相同的配置中，否则代理将无法正常运行。

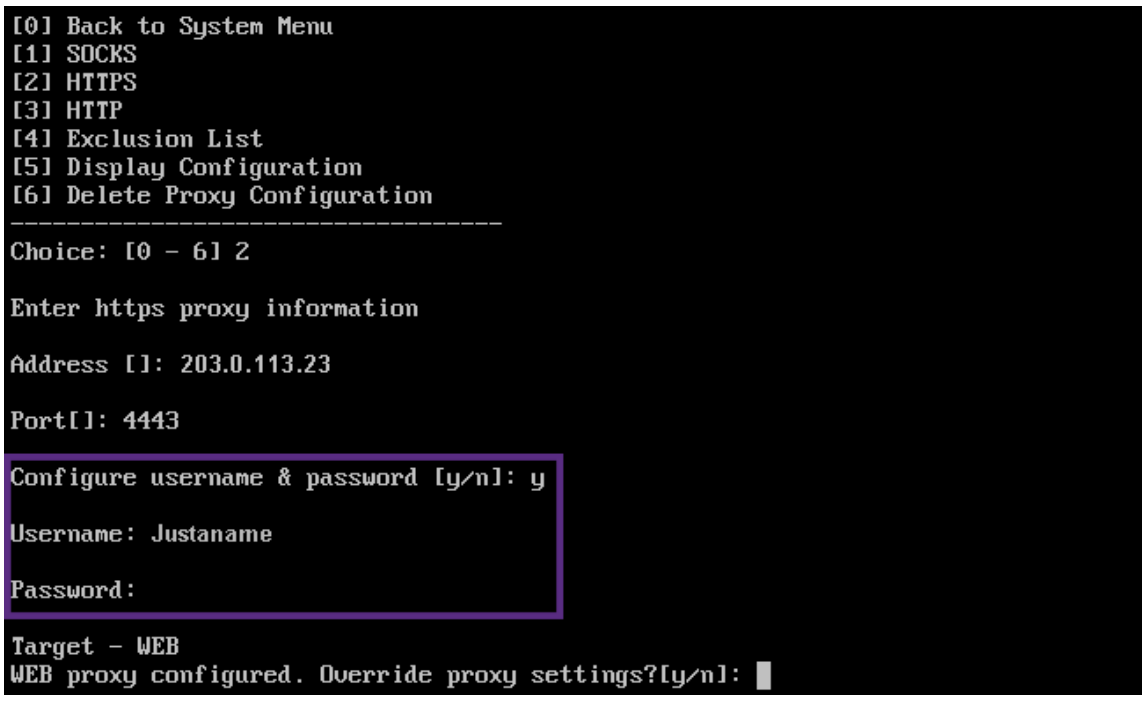


4. 键入代理服务器 IP 地址、端口号和目标。有关每种代理服务器类型支持的目标类型，请参阅下表。

代理类型	支持的目标
SOCKS	APNS
HTTP	APNS、Web、PKI
HTTPS	Web、PKI
HTTP 并进行身份验证	Web、PKI
HTTPS 并进行身份验证	Web、PKI



5. 键入 **n**，键入 **2** 以选择 HTTPS，然后键入您的代理服务器 IP 地址、端口号和目标。
6. 如果选择在代理服务器上配置用户名和密码以进行身份验证，请键入 **y**，然后键入用户名和密码。



7. 键入 **y** 以保存设置。

配置 SQL Server

January 5, 2022

对于从本地 XenMobile Server 到 SQL Server 的连接，可以使用以下任意驱动程序：

- 默认驱动程序
- jTDS
- Microsoft Java 数据库连接 (JDBC) 驱动程序

在执行以下操作时，jTDS 驱动程序是默认的驱动程序：

- 在本地安装 XenMobile Server。
- 从配置为使用 jTDS 驱动程序的 XenMobile Server 升级。

对于这两种驱动程序，XenMobile 支持 SQL Server 身份验证或 Windows 身份验证。对于身份验证和驱动程序的这些组合，可以打开或关闭 SSL。

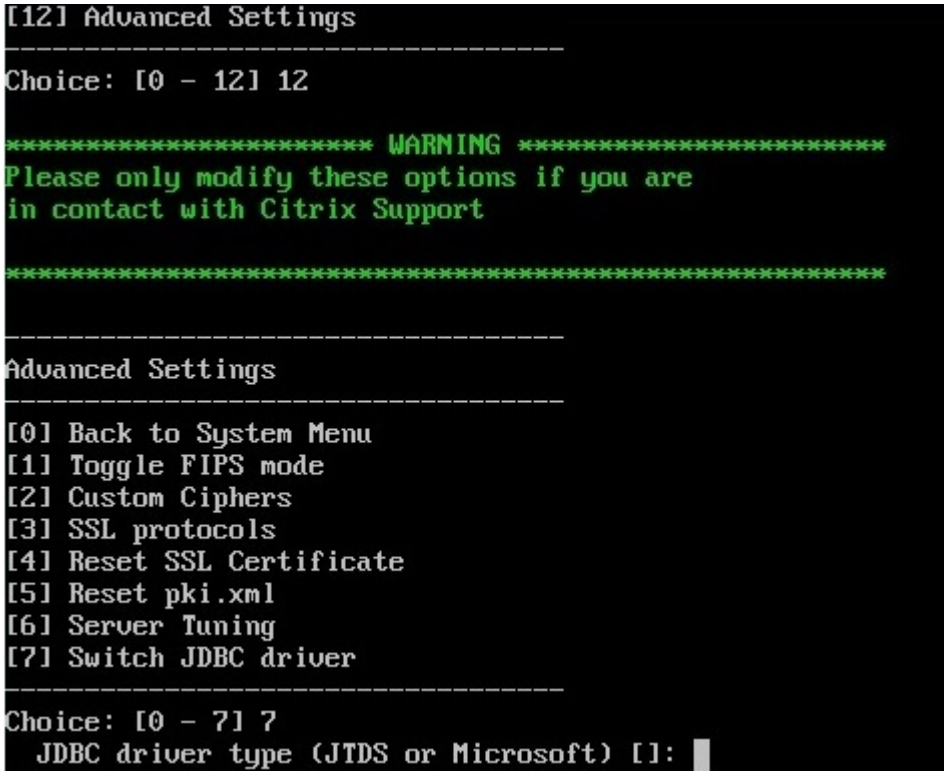
使用 Windows 身份验证和 Microsoft JDBC 驱动程序时，驱动程序会将集成身份验证与 Kerberos 结合使用。XenMobile 将联系 Kerberos 以获取 Kerberos 密钥发行中心 (KDC) 详细信息。如果所需的详细信息未提供，XenMobile CLI 将提示输入 Active Directory 服务器的 IP 地址。

要从 jTDS 驱动程序切换到 JDBC 驱动程序，请通过 SSH 连接到您的所有 XenMobile Server 节点并使用 XenMobile CLI 进行配置。执行的步骤因您当前的 jTDS 驱动程序配置而异，如下所示。

切换到 **Microsoft JDBC**（**SQL Server** 身份验证）

要完成这些步骤，您需要提供 SQL Server 用户名和密码。

1. 通过 SSH 连接到所有 XenMobile Server 节点。
2. 在 XenMobile CLI 主菜单中，键入 **2** 以选择 **System Menu**（系统菜单）。
3. 键入 **12** 选择 “Advanced Settings”（高级设置）。
4. 键入 **7** 选择 “Switch JDBC driver”（切换 JDBC 驱动程序），然后键入 **m** 表示选择 Microsoft。



5. 系统提示时，请键入 **y** 选择 SQL 身份验证，然后键入 SQL Server 用户名和密码。
6. 对每个 XenMobile Server 节点重复执行上述步骤。
7. 重新启动每个 XenMobile Server 节点。

切换到 **Microsoft JDBC**（**SSL** 关闭；**Windows** 身份验证）

要完成这些步骤，您需要 Active Directory 用户名和密码、Kerberos KDC 领域以及 KDC 用户名。

1. 通过 SSH 连接到所有 XenMobile Server 节点。
2. 在 XenMobile CLI 主菜单中，键入 **2** 以选择 **System Menu**（系统菜单）。
3. 键入 **12** 选择 “Advanced Settings”（高级设置）。
4. 键入 **7** 选择 “Switch JDBC driver”（切换 JDBC 驱动程序），然后键入 **m**。
5. 系统提示是否要使用 SQL Server 身份验证时，键入 **n**。
6. 系统提示时，请键入为 SQL Server 配置的 Active Directory 用户名和密码。
7. 如果 XenMobile 不自动发现 Kerberos KDC 领域，系统将提示输入 KDC 详细信息，包括 SQL Server FQDN。
8. 系统提示是否要使用 SSL 时，键入 **n**。XenMobile 将保存配置。如果 XenMobile 由于出错而无法保存配置，则将显示一条错误消息以及您输入的详细信息。
9. 对每个 XenMobile Server 节点重复执行上述步骤。
10. 重新启动每个 XenMobile Server 节点。

更改 **XenMobile** 数据库密码

更改 XenMobile 数据库密码时（例如，当 Citrix 支持指示您更改密码时），请遵循以下指导。

如果您的 SQL Server 使用 Windows 身份验证，请在 Windows Active Directory 中更改数据库密码。然后，请刷新数据库服务器上的数据库管理员帐户以同步密码更改。然后，您可以在 XenMobile 中更改密码，如下所示。

> 重要：
>
> - 在 XenMobile 中为更改数据库密码安排定期维护时段。必须在系统停机时更改密码。
> - 更改密码时，确保所有 XenMobile 节点都连接到网络。更改密码后，重新启动 XenMobile。
>
>   If you don't restart XenMobile after a password change, XenMobile goes into recovery mode. In that case, revert to the old password in SQL server, restart XenMobile, and change the password again.

1. 验证所有 XenMobile Server 节点是否正在运行。对于群集环境，要提取所有节点。
2. 通过禁用虚拟服务器阻止在 Citrix ADC 负载平衡器上向 XenMobile 传输传入设备流量。
3. 要在 SQL Server 中更改数据库密码，请登录 XenMobile CLI，导航到 **Configuration**（配置）**> Database**（数据库），在系统提示时输入更改后的密码：

```
Server []: <ipAddress>
Port [1433]: 1433
Username [sa]: <userName>
Password: <****>
<!--NeedCopy-->
```

4. 选择 **Y** 重新启动服务器。
5. 对于群集中的所有其他节点重复执行步骤 3 和 4。
6. 通过启用虚拟服务器取消阻止在 Citrix ADC 负载平衡器上传输传入设备流量。

服务器属性

January 5, 2022

XenMobile 具有多个适用于服务器范围内的操作的属性。本文将介绍多个服务器属性，并详细说明如何添加、编辑或删除服务器属性。

一些属性是自定义键。要添加自定义键，请单击添加，然后从键中选择自定义键。

有关通常配置的属性的信息，请参阅《XenMobile 虚拟手册》中的服务器属性。

服务器属性定义

始终添加设备

- 如果设置为 **true**，XenMobile 将向 XenMobile 控制台中添加设备，即使注册失败亦如此，因此，您能够看到尝试注册的设备。默认值为 **false**。

AG 客户端证书颁发限制时间间隔

- 两次生成证书之间的宽限期。此时间间隔阻止 XenMobile 在短时间内为某个设备生成多个证书。Citrix 建议不要更改此值。默认值为 **30** 分钟。

审核日志清理执行时间

- 启动审核日志清理的时间，格式为 HH:MM AM/PM。示例：04:00 AM。默认值为 **02:00 AM**。

审核日志清理时间间隔 **(**天**)**

- XenMobile Server 保留审核日志的天数。默认值为 **1**。

Audit Logger（审核记录器）

- 如果设置为 **False**，则不记录用户界面 (UI) 事件。默认值为 **False**。

审核日志保留期限 **(**天**)**

- XenMobile Server 保留审核日志的天数。默认值为 **7**。

auth.ldap.connect.timeout and auth.ldap.read.timeout

- 为了补偿 LDAP 响应慢的情况，Citrix 建议为以下自定义键添加服务器属性。
  - 键：自定义键
  - 键：**auth.ldap.connect.timeout**
  - 值：**60000**
  - 显示名称：**auth.ldap.connect.timeout**
  - 说明：**LDAP** 连接超时
  - 键：自定义键
  - 键：**auth.ldap.read.timeout**

- 值：**60000**
- 显示名称：**auth.ldap.read.timeout**
- 说明：**LDAP** 读取超时

证书续订 **(**秒**)**

- XenMobile 在证书过期之前开始续订证书的秒数。例如，如果证书将于 12 月 30 日过期，并且此属性设置为 30 天：如果设备在 12 月 1 日到 12 月 30 日之间连接，XenMobile 会尝试续订证书。默认值为 **2592000** 秒（30 天）。

连接超时

- 会话不活动超时（分钟），在这段时间之后 XenMobile 关闭与设备的 TCP 连接。会话保持打开状态。适用于 Android 和 Windows CE 设备及远程支持。默认值为 **5** 分钟。

与 **Microsoft** 证书服务器连接超时

- XenMobile 等待来自证书服务器的响应的秒数。如果证书服务器速度缓慢，并且具有大量流量，可将此值增加到 60 秒或更长时间。在 120 秒后不响应的证书服务器需要维护。默认值为 **15000** 毫秒（15 秒）。

默认部署渠道

- 确定 XenMobile 将资源部署到设备的方式：在用户级别 (**DEFAULT_TO_USER**) 或设备级别。默认值为 **DEFAULT_TO_DEVICE**。

部署日志清理时间 **(**天**)**

- XenMobile Server 保留部署日志的天数。默认值为 **7**。

禁用主机名验证

- 默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。主机名验证失败时，服务器日志将包括错误，例如：“Unable to connect to the volume purchase Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”（无法连接到批量购买服务器: 主机名 192.0.2.0 与对等机提供的证书使用者不匹配）。如果主机名验证中断了您的部署，请将此属性更改为 **true**。默认值为 **false**。

禁用 **SSL** 服务器验证

- 如果为 **True**，则在满足所有以下条件时禁用 SSL 服务器证书验证：
  - 在 XenMobile Server 上启用了基于证书的身份验证

  - Microsoft CA 服务器是证书颁发者
  - 其根 XenMobile Server 不信任的内部 CA 已为您的证书签名。

默认值为 **True**。

启用控制台

- 如果设置为 **true**，则允许用户访问自助服务门户控制台。默认值为 **true**。

启用崩溃报告

- 如果设置为 **true**，Citrix 将收集崩溃报告和诊断信息以帮助对 Secure Hub for iOS 和 Secure Hub for Android 相关问题进行故障排除。如果设置为 **false**，则不收集任何数据。默认值为 **true**。

启用/禁用休眠统计信息日志记录以进行诊断

- 如果设置为 **True**，则启用休眠统计日志记录，以协助对应用程序性能问题进行故障排除。休眠是用于 XenMobile 与 Microsoft SQL Server 的连接的组件。默认情况下，此日志记录功能已禁用，因为它会影响应用程序的性能。只应在短时间内启用日志记录功能，以避免生成巨大的日志文件。XenMobile 将此日志写入 /opt/sas/logs/hibernate_stats.log。默认值为 **False**。

启用 **macOS OTAE**

- 如果设置为 **false**，则阻止在 macOS 设备上使用注册链接，这意味着 macOS 用户只能使用注册邀请进行注册。默认值为 **true**。

启用通知触发器

- 启用或禁用 Secure Hub 客户端通知. 值 **true** 表示启用通知。默认值为 **true**。

force.server.push.required.apps

- 诸如以下情况下在 Android 和 iOS 设备上启用所需应用程序的强制部署：
  - 上载新应用程序并根据需要对其进行标记。
  - 根据需要标记现有应用程序。
  - 用户删除所需的应用程序。
  - Secure Hub 更新可用。

默认情况下，必需应用程序的强制部署设置为 **false**。创建自定义键并将值设置为 **true** 以启用强制部署。强制部署期间，启用了 MDX 的必需应用程序（包括企业应用程序和公共应用商店应用程序）将立即升级。即使您配置了应用程序更新宽限期 MDX 策略并且用户选择以后升级应用程序，也会升级。

- 键：自定义键
- 键：**force.server.push.required.apps**
- 值：**false**
- 显示名称：**force.server.push.required.apps**
- 说明：强制部署必需应用程序

完全拉取 **ActiveSync** 允许和拒绝的用户

- XenMobile 拉取 ActiveSync 允许和拒绝的用户的完整列表（基准）的时间间隔（秒）。默认值为 **28800** 秒。

hibernate.c3p0.idle_test_period

- 此 XenMobile Server 属性（即“自定义键”）确定自动验证连接之前的空闲时间（秒）。按如下所示配置键。默认值为 **30**。
- 键：自定义键
- 键：**hibernate.c3p0. idle_test_period**
- 值：**30**
- 显示名称：**hibernate.c3p0. idle_test_period =*nnn***
- 说明：休眠空闲测试时间段

hibernate.c3p0.max_size

- 此自定义键确定 XenMobile 可以打开的与 SQL Server 数据库的最大连接数。XenMobile 使用您为此自定义键指定的值作为上限。仅当需要连接时才会打开连接。设置基于数据库服务器的容量。有关详细信息，请参阅优化 XenMobile 操作。按如下所示配置键。默认值为 **1000**。
- 键：**hibernate.c3p0.max_size**
- 值：**1000**
- 显示名称：**hibernate.c3p0.max_size**
- 说明：**DB** 与 **SQL** 的连接数

hibernate.c3p0.min_size

- 此自定义键确定 XenMobile 打开的与 SQL Server 数据库的最小连接数。按如下所示配置键。默认值为 **100**。
- 键：**hibernate.c3p0.min_size**
- 值：**100**
- 显示名称：**hibernate.c3p0.min_size**

- 说明：**DB** 与 **SQL** 的连接数

hibernate.c3p0.timeout

- 此自定义键确定空闲超时时间（秒）。默认值为 **120**。
- 键：自定义键
- 键：**hibernate.c3p0.timeout**
- 值：**120**
- 显示名称：**hibernate.c3p0.timeout**
- 说明：数据库空闲超时

确定是否已启用遥测

- 确定是否已启用遥测（客户体验改善计划，或 CEIP）。您可以在安装或升级 XenMobile 时选择加入 CEIP。如果 XenMobile 有 15 次连续失败的上载，则会禁用遥测。默认值为 **false**。

不活动超时 **(**分钟**)**

- 如果 **Web** 服务超时类型服务器属性为 **INACTIVITY_TIMEOUT**：此属性定义分钟数，超过此时间后，XenMobile 注销执行了以下操作的不活动管理员：
  - 使用适用于 REST 的 XenMobile 公共 API 服务访问 XenMobile 控制台
  - 使用适用于 REST 的 XenMobile 公共 API 服务来访问任何第三方应用程序。超时为 **0** 意味着不活动用户保持登录状态。

默认值为 **5**。

已启用 **iOS** 设备管理注册自动安装

- 如果设置为 true，此属性可以减少设备注册过程中所需的用户干预数量。用户必须单击 **Root CA install**（根 CA 安装）（如果需要）和 **MDM Profile install**（MDM 配置文件安装）。

iOS 设备管理注册第一个步骤延迟

- 用户在设备注册过程中输入其凭据后，此值指定在提示提供根 CA 之前等待的时间长度。Citrix 建议仅针对网络延迟或速度问题编辑此属性。在这种情况下，请勿将该值设置为超过 5000 毫秒（5 秒）。默认值为 **1000** 毫秒（1 秒）。

iOS 设备管理注册最后一个步骤延迟

- 在设备注册过程中，此属性的值指定在设备上安装 MDM 配置文件与启动代理之间需等待的时间量。Citrix 建议仅针对网络延迟或速度问题编辑此属性。在这种情况下，请勿将该值设置为超过 5000 毫秒（5 秒）。默认值为 **1000** 毫秒（1 秒）。

iOS 设备管理身份交付模式

- 指定 XenMobile 使用 **SCEP**（出于安全原因而推荐使用）还是 **PKCS12** 向设备分发 MDM 证书。在 PKCS12 模式下，密钥对在服务器上生成，并且不执行任何协商。默认值为 **SCEP**。

iOS 设备管理身份密钥大小

- 定义 MDM 身份、iOS 配置文件服务和 XenMobile iOS 代理身份的私钥的大小。默认值为 **1024**。

iOS 设备管理身份续订天数

- 指定 XenMobile 在证书过期之前开始续订证书的天数。例如：如果证书将于 10 天后过期，并且此属性设置为 **10** 天，当设备在过期之前 9 天连接时，XenMobile 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，XenMobile 向 Apple 服务器推送通知需要该密码。

设备断开连接之前不活动的时长

- 指定设备在 XenMobile 将其断开连接之前可以保持不活动状态的时长，包括最后一次身份验证。默认值为 **7** 天。

MAM Only Device Max（仅 **MAM** 设备最大值）

- 此自定义键限制每个用户可以注册的仅 MAM 设备数。按如下所示配置键。值为 **0** 表示设备注册数不受限制。
- 键 = **number.of.mam.devices.per.user**
- 值 = **5**
- 显示名称 = 仅 **MAM** 设备最大值
- 说明 = 限制每个用户可以注册的 **MAM** 设备数。

MaxNumberOfWorker

- 导入许多批量购买许可证时使用的线程数量。默认值为 **3**。如果需要进一步优化，可以增加线程的数量。但是，如果使用数量较大的线程，例如 6 个，批量购买导入会导致 CPU 使用率非常高。

Citrix ADC 单点登录

- 如果设置为 **False**，则会在从 Citrix ADC 单点登录到 XenMobile 时禁用 XenMobile 回调功能。如果 Citrix Gateway 配置包括回调 URL，则 XenMobile 使用回调功能验证 Citrix Gateway 会话 ID。默认值为 **False**。

连续失败的上载次数

- 显示客户体验改善计划 (CEIP) 上载过程中连续失败的次数。XenMobile 会在上载失败时增加该值。上载失败 15 次后，XenMobile 将禁用 CEIP（又称为遥测）。有关详细信息，请参阅服务器属性确定是否已启用遥测。XenMobile 在上载成功时将该值重置为 **0**。

每个设备的用户数

- 能够在 MDM 中注册相同设备的用户的最大数量。值 **0** 表示能够注册相同设备的用户数量不受限制。默认值为 **0**。

提取允许和被拒绝的用户的增量更改

- XenMobile 在执行 PowerShell 命令以获取 ActiveSync 设备的增量时等待来自域的响应的秒数。默认值为 **60** 秒。

从 **Microsoft** 证书服务器读取超时

- XenMobile 在执行读取时等待来自证书服务器的响应的秒数。如果证书服务器速度缓慢，并且具有大量流量，您可以将此值增加到 60 秒或更长时间。在 120 秒后不响应的证书服务器需要维护。默认值为 **15000** 毫秒（15 秒）。

REST Web 服务

- 启用 REST Web 服务。默认值为 **true**。

以指定大小的块检索设备信息

- 此值在内部用于设备导出期间的多线程处理。如果该值较高，则单个线程解析较多的设备。如果该值较低，则有较多的线程提取设备。降低该值可能会提高导出和设备列表提取的性能，但可能会减少可用内存。默认值为 **1000**。

会话日志清理时间 **(**天**)**

- XenMobile Server 保留会话日志的天数。默认值为 **7**。

服务器模式

- 确定 XenMobile 在 MAM、MDM 还是 ENT（企业）模式下运行，这三个值分别对应于应用程序管理、设备管理或应用程序和设备管理。请根据所需的设备注册方式设置“服务器模式”属性，如下表所示。无论许可证类型为何，“服务器模式”都默认为 **ENT**。

如果您具有 XenMobile MDM Edition 许可证，不管您在“服务器属性”中如何设置服务器模式，有效服务器模式始终为 MDM。如果您具有 MDM Edition 许可证，则无法通过将“服务器模式”设置为“MAM”或“ENT”来启用应用程序管理。

您的许可证为此版本	您希望设备在此模式下注册	将 **“服务器模式”** 属性设置为
Enterprise/Advanced	MDM 模式	MDM
Enterprise/Advanced	MDM+MAM 模式	ENT
MDM	MDM 模式	MDM

有效服务器模式是许可证类型和服务器模式的组合。对于 MDM 许可证，无论服务器模式的设置为何，有效服务器模式始终为 MDM。对于 Enterprise 和 Advanced 许可证，如果“服务器模式”为 **ENT** 或 **MDM**，有效服务器模式与服务器模式一致。如果“服务器模式”为 **MAM**，则有效服务器模式为 ENT。

XenMobile 会在服务器日志中为以下每个活动添加服务器模式：激活某个许可证、删除某个许可证以及在“服务器属性”中更改服务器模式。有关创建和查看日志文件的信息，请参阅日志和在 XenMobile 中查看和分析日志文件。

Content Collaboration 配置类型

- 指定 Citrix Files 存储类型。**ENTERPRISE** 表示启用 Citrix Files Enterprise 模式。**CONNECTORS** 表示仅提供对通过 XenMobile 控制台创建的存储区域连接器的访问权限。默认值为 **NONE**，此时显示配置 **> ShareFile** 屏幕的初始视图，在该屏幕中可以选择“ShareFile Enterprise”与“Citrix Files 连接器”。默认值为 **NONE**。

静态超时（分钟）

- 如果 **Web** 服务超时类型服务器属性为 **STATIC_TIMEOUT**：此属性定义分钟数，超过此时间后，XenMobile 注销执行了以下操作的管理员：
  - 使用适用于 REST 的 XenMobile 公共 API 服务访问 XenMobile 控制台。
  - 使用适用于 REST 的 XenMobile 公共 API 服务访问任何第三方应用程序。

默认值为 **60**。

触发代理消息抑制

- 启用或禁用 Secure Hub 客户端消息传递。值 **false** 表示启用消息传递。默认值为 **true**。

触发代理声音抑制

- 启用或禁用 Secure Hub 客户端声音。值 **false** 表示启用声音。默认值为 **true**。

Android 设备的未经身份验证的应用程序下载

- 如果设置为 **True**，则可以将自托管应用程序下载到运行 Android Enterprise 的 Android 设备。如果启用了在 Google Play 应用商店中静态提供下载 URL 的 Android Enterprise 选项，XenMobile 将需要此属性。在这种情况下，下载 URL 不能包括带有身份验证令牌的一次性票据（由 **XAM** 一次性票据服务器属性定义）。默认值为 **False**。

Windows 设备的未经身份验证的应用程序下载

- 仅适用于不验证一次性票证的较旧 Secure Hub 版本。如果设置为 **False**，则可以将未经身份验证的应用程序从 XenMobile 下载到 Windows 设备。默认值为 **False**。

使用 **ActiveSync ID** 对 **ActiveSync** 擦除设备执行操作

- 如果为 **true**，适用于 Exchange ActiveSync 的 Endpoint Management 连接器将使用 ActiveSync 标识符作为 asWipeDevice 方法的参数。默认值为 **false**。

用户定义的设备属性 **N**

- 仅用于 Windows CE 设备。此自定义键允许您获取在 Windows CE 设备的注册表中创建的属性。这些属性保存在 XenMobile 数据库中之后，您可以根据这些属性的值创建部署规则。
- 键：自定义键
- 键：**device.properties.userDefinedN**
- 值：管理员定义
- 显示名称：管理员定义
- 说明：由管理员定义

仅限来自 **Exchange** 的用户

- 如果设置为 **true**，则禁用针对 ActiveSync Exchange 用户的用户身份验证。默认值为 **false**。

VP 基准时间间隔

- XenMobile 重新导入 Apple 提供的批量购买许可证的最小时间间隔。刷新许可证信息可确保 XenMobile 反映所有更改，例如，手动从批量购买中删除导入的应用程序时。默认情况下，XenMobile 按每 **720** 分钟的最小时间间隔为基准刷新批量购买许可证。

如果您安装了许多批量购买许可证（例如，超过 50000）：Citrix 建议增加基准时间间隔以降低导入许可证的频率和开销。如果您预计 Apple 会频繁更改批量购买许可证：Citrix 建议降低该值以使更改及时更新到 XenMobile 中。两个基准之间的最小时间间隔为 60 分钟。此外，XenMobile 每隔 60 分钟执行一次增量导入，以捕获自上次导入后所做的更改。因此，如果批量购买基准时间间隔为 60 分钟，则基准之间的时间间隔可能会最长延迟 119 分钟。

Web 服务超时类型

- 指定如何使从公共 API 中获取的身份验证令牌过期。如果设置为 **STATIC_TIMEOUT**，XenMobile 会在静态超时 **(**分钟**)** 服务器属性中指定的值之后将身份验证令牌视为已过期。

如果设置为 **INACTIVITY_TIMEOUT**，XenMobile 会在令牌不活动的时间为在不活动超时 **(**分钟**)** 服务器属性中指定的值之后将身份验证令牌视为已过期。默认值为 **STATIC_TIMEOUT**。

Windows Phone MDM 证书延长的有效期 **(5** 年**)**

- MDM 为 Windows Phone 和 Tablet 颁发的设备证书的有效期。在设备管理过程中，设备使用设备证书向 MDM 服务器进行身份验证。如果设置为 **true**，有效期为五年。如果设置为 **false**，有效期为两年。默认值为 **true**。

Windows WNS 通道 **-** 续订之前的天数

- ChannelURI 的续订频率。默认值为 **10** 天。

Windows WNS 检测信号时间间隔

- XenMobile 在以每五分钟三次的速率连接到某个设备之后再次连接到该设备之前等待的时间。默认值为 **6** 小时。

XAM 一次性票据

- 一次性身份验证令牌 (OTT) 对下载应用程序有效的毫秒数。此属性与 **Android** 设备的未经身份验证的应用程序下载属性和 **Windows** 设备的未经身份验证的应用程序下载属性一起使用。这些属性指定是否允许进行未经身份验证的应用程序下载。默认值为 **3600000**。

XenMobile MDM Self Help Portal console max inactive interval (minutes)（**XenMobile MDM** 自助服务门户控制台最长不活动时间间隔 **(**分钟**)**）

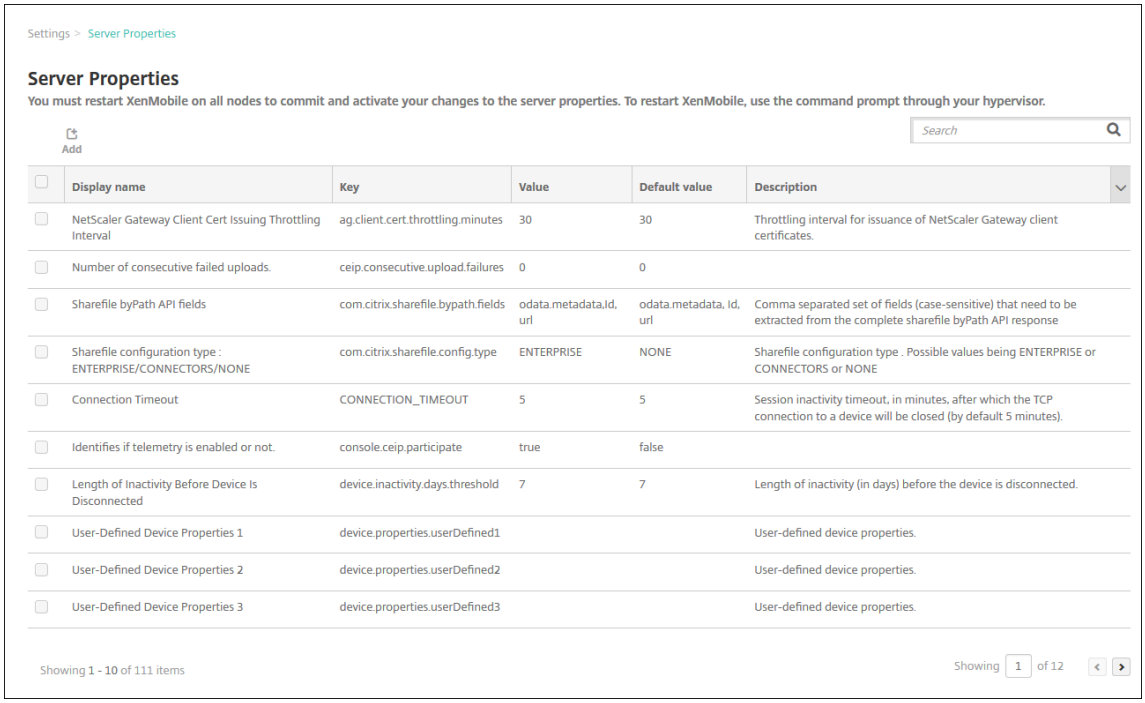
- XenMobile 从 XenMobile 自助服务门户注销不活动用户之前的分钟数。超时值 **0** 表示不活动用户保持登录状态。默认值为 **30**。

添加、编辑或删除服务器属性

在 XenMobile 中，可以将属性应用到服务器。更改后，务必在所有节点上重新启动 XenMobile 以提交并激活更改。

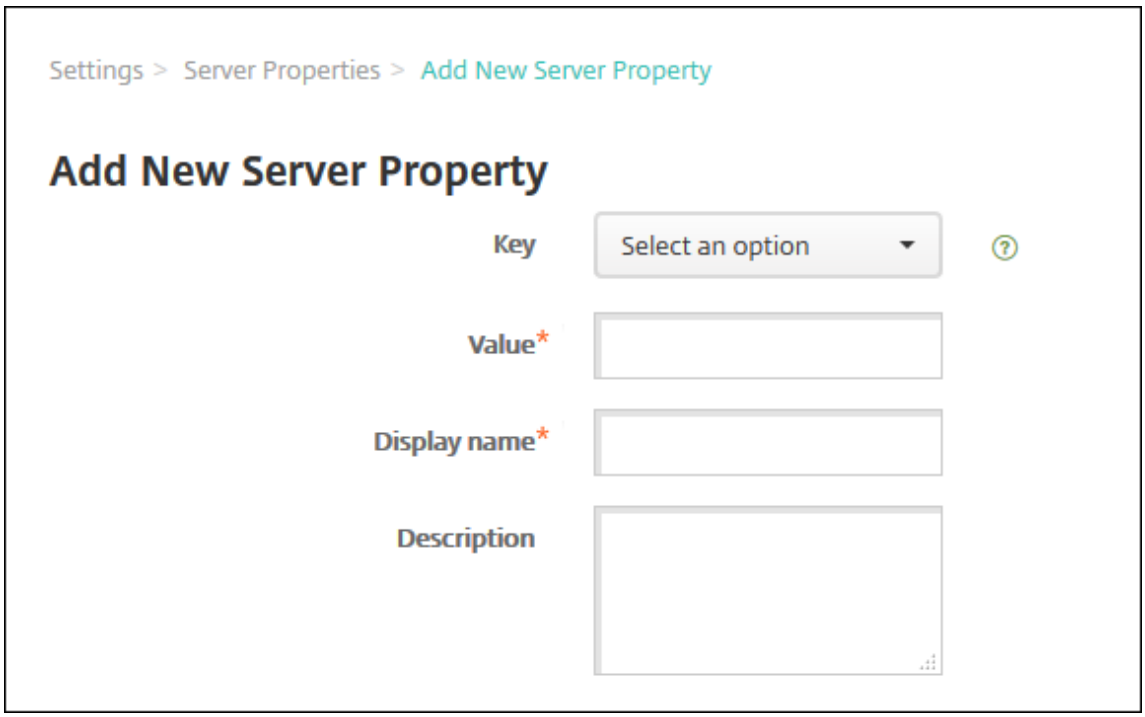
> 注意：
>
> 要重新启动 XenMobile，请通过虚拟机管理程序使用命令提示窗口。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击服务器属性。此时将显示服务器属性页面。可以从此页面添加、编辑和删除服务器属性。



添加服务器属性

1. 单击添加。此时将显示添加新服务器属性页面。



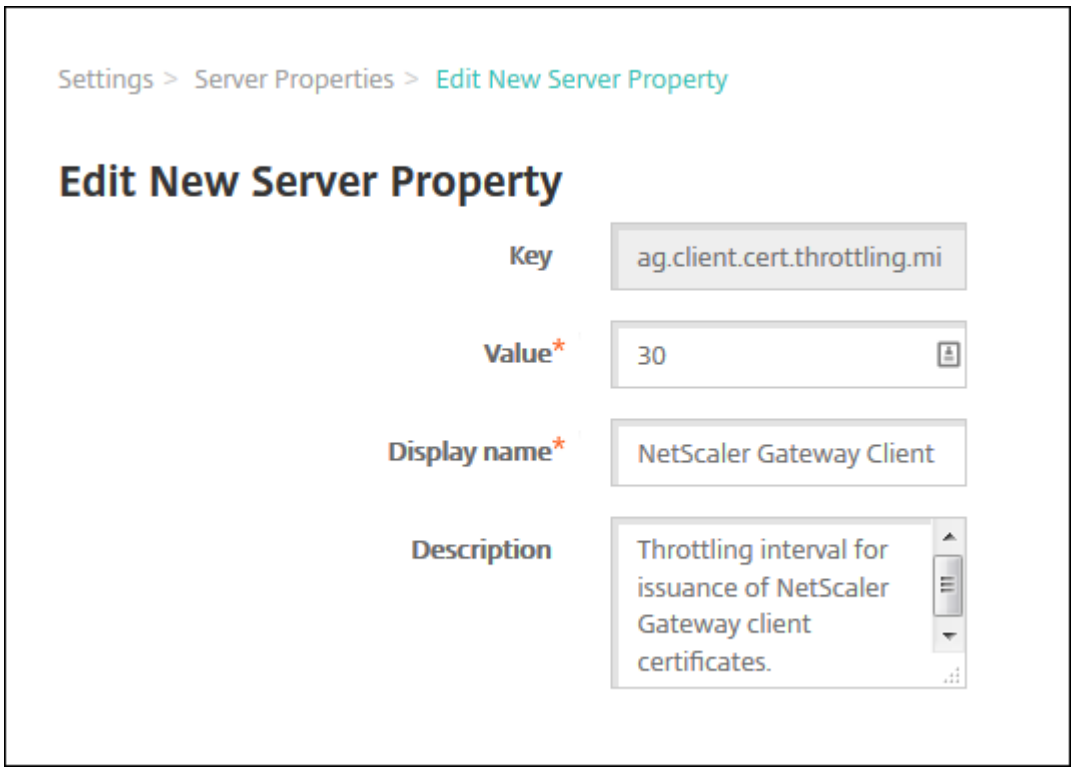
2. 配置以下设置：
   - 密钥：在列表中，选择合适的密钥。键区分大小写。如果要编辑属性值或申请特殊密钥，请联系 Citrix 支持。
   - 值：根据选择的键输入一个值。
   - 显示名称：输入新属性值显示在服务器属性表中的名称。
   - 说明：（可选）键入新服务器属性的说明。
3. 单击保存。

编辑服务器属性

1. 在服务器属性表中，选择要编辑的服务器属性。

   选中服务器属性旁边的复选框时，选项菜单将显示在服务器属性列表上方。单击列表中的其他任意位置可在列表右侧打开选项菜单。

2. 单击编辑。此时将显示编辑新服务器属性页面。



3. 适当更改以下信息：
   - 键：无法更改此字段。
   - 值：属性值。
   - 显示名称：属性名称。
   - 说明：属性说明。
4. 单击保存以保存您所做更改，或单击取消保留属性不变。

删除服务器属性

1. 在服务器属性表中，选择要删除的服务器属性。

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

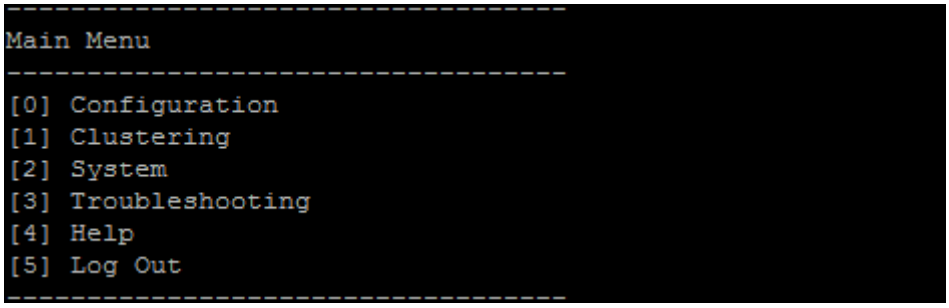
命令行接口选项

January 5, 2022

对于本地安装的 XenMobile Server，您可以按如下所示访问 CLI 选项：

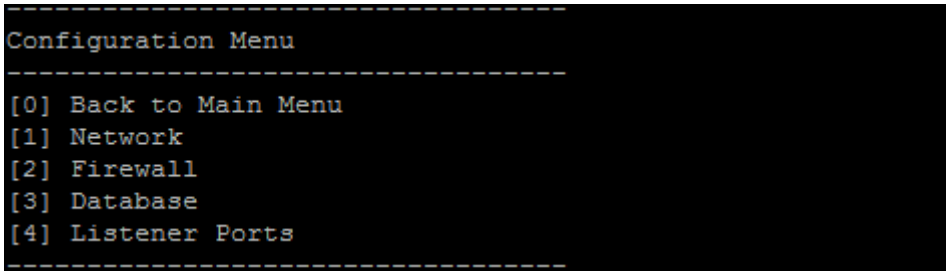
- 从安装了 **XenMobile** 的虚拟机管理程序：在虚拟机管理程序中，选择导入的 XenMobile 虚拟机，启动命令提示窗口视图，然后登录您的 XenMobile 管理员帐户。有关详细信息，请参阅您的虚拟机管理程序的文档。
- 如果在防火墙中启用了 **SSH**，则使用 **SSH**：登录您的 XenMobile 管理员帐户。

可以使用 CLI 执行各种配置和故障排除任务。下图显示了 CLI 的顶层菜单。

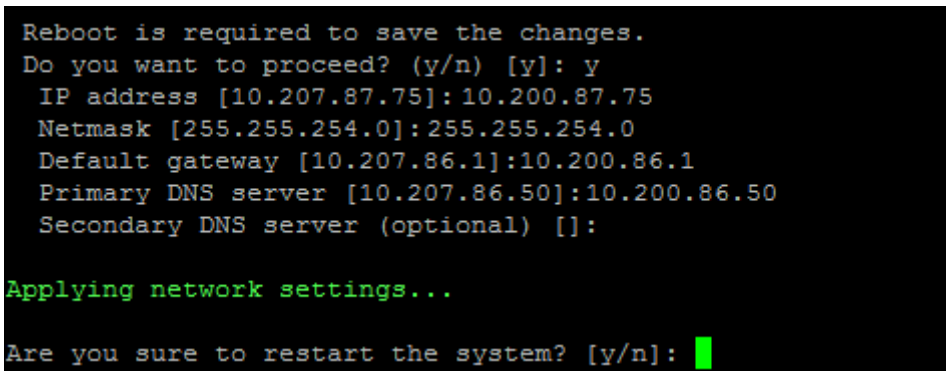


配置选项

下面是 **Configuration Menu**（配置菜单）以及每个选项显示的设置的示例。



[1] Network（网络）



[2] Firewall（防火墙）

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction
 - enter c as value to clear list

  HTTP service
    Port: 80
    Enable access (y/n) [y]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  SSH service
    Port [22]:
    Enable access (y/n) [y]:
    Access white list []:

  Management API (for initial staging) HTTPS service
    Port [30001]:
    Enable access (y/n) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```

[3] Database（数据库）

```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```


[4] Listener Ports（侦听器端口）

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

群集选项

下面是 **Clustering Menu**（群集菜单）以及每个选项显示的设置的示例。

```
-----------------------------------
Clustering Menu
-----------------------------------
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----------------------------------
```

[1] Show Cluster Status（显示群集状态）

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```

[2] Enable/Disable cluster（启用/禁用群集）

选择启用群集时，将显示以下消息：

```
To enable real-time communication between cluster members, please open port
 80 using the Firewall menu option in CLI menu. Also configure Access white
 list under Firewall settings for restricted access.
```

选择禁用群集时，将显示以下消息：

```
You have chosen to disable clustering. Access to port 80 is not needed.
Please disable it.
```


[3] Cluster member white list（群集成员白名单）

```
Current White List:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction


Please enter hosts or networks to be white listed:
```

[4] Enable or disable SSL offload（启用或禁用 **SSL** 卸载）

选择启用或禁用 SSL 卸载时，将显示以下消息：

```
Enabling SSL offload opens port 80 for everyone. Please configure Access
white list under Firewall settings for restricted access.
```

[5] Display Hazelcast Cluster（显示 **Hazelcast** 群集）

选择显示 Hazelcast 群集时，将显示以下选项：

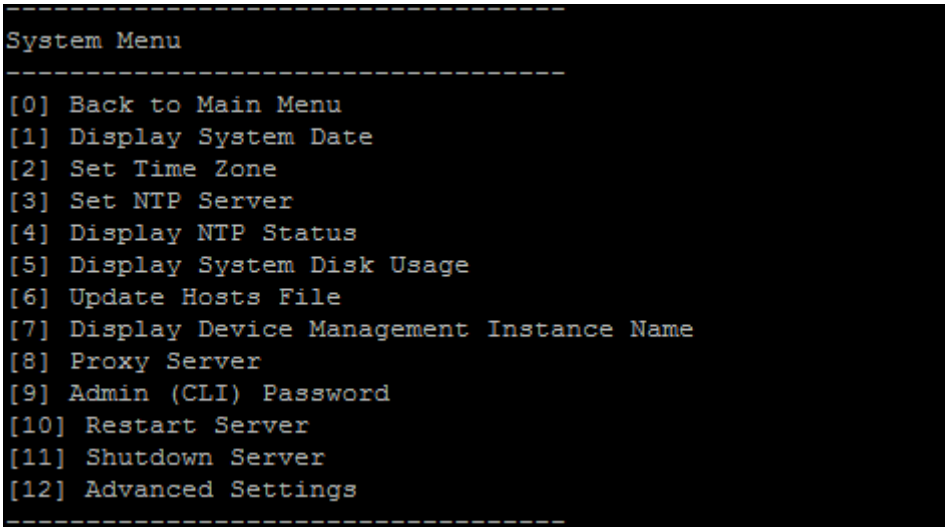
Hazelcast Cluster Members:（Hazelcast 群集成员:）

[列出 IP 地址]

> 注意：
>
> 如果所配置的某个节点不属于群集，请重新启动该节点。

系统选项

在 **System Menu**（系统菜单）中，您可以显示或设置系统级信息、重新启动或关闭服务器，或者访问 **Advanced Settings**（高级设置）。



通过“Set NTP Server”（设置 NTP 服务器），可以指定 NTP 服务器信息。如果您在将 XenMobile 时间与虚拟机管理程序同步时遇到时区问题，可以通过将 XenMobile 指向 NTP 服务器来避免这些问题。请在更改此选项后重新启动所有群集服务器。

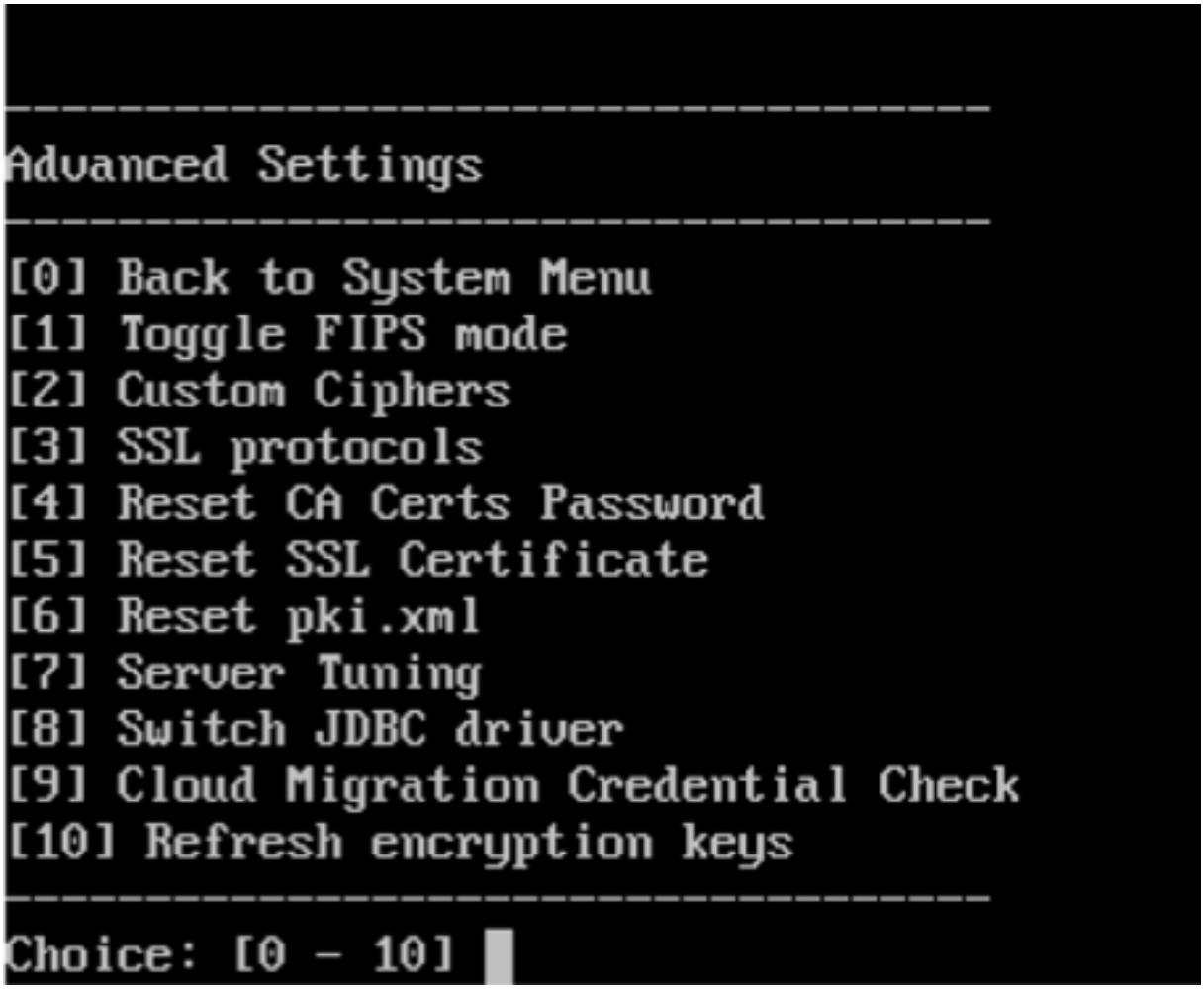
您还可以通过查看 **[5]** 显示系统磁盘使用情况菜单项来检查磁盘空间。

关于关闭服务器节点

关闭群集中的单个服务器节点时，其他节点通常可以处理工作负载，前提是其满足可扩展性和性能中记录的要求。产生的影响可能会因同时关闭的节点数量、用户总数以及节点关闭的时间长度而有所差别。

- 用户仍然可以访问 Secure Hub 和应用商店。
- 如果可用节点能够处理用户数量，则用户仍然可以访问和启动已部署的托管应用程序。连接速度可能较慢，导致设备签入速度较慢。
- 除非所有节点都关闭，否则设备策略将继续有效。策略的部署速度可能会更慢，具体取决于资源和设备数量。

[12] Advanced Settings（高级设置）



SSL protocols（SSL 协议）选项默认设置为允许使用的所有协议。显示 **New SSL protocols to enable**（要启用的新 SSL 协议）提示后，键入要启用的协议。XenMobile 将禁用不包括在您的响应中的所有协议。例如：要禁用 TLSv1，请键入 `TLSv1.2,TLSv1.1`，然后键入 **y** 以重新启动 XenMobile Server。

Server Tuning（服务器优化）选项包括“server connection timeout”（服务器连接超时）、“maximum connections (by port)”（最大连接数 (按端口)）和“maximum threads (by port)”（最大线程数 (按端口)）。

Switch JDBC driver（切换 JDBC 驱动程序）选项为 **jTDS** 和 **Microsoft** JDBC。默认驱动程序为 jTDS。有关切换到 Microsoft JDBC 驱动程序的信息，请参阅 SQL Server 驱动程序。

故障排除选项

下面是 **Troubleshooting Menu**（故障排除菜单）以及每个选项显示的设置的示例。


```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

[1] Network Utilities（网络实用程序）

```
---------------------------------
Network Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
---------------------------------
```

[2] 日志

```
 -------------------------------------
 Logs Menu
 -------------------------------------
 [0] Back to Troubleshooting Menu
 [1] Display debug log file
 [2] Display update log file
```

[3] 支持包

```
-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----------------------------------
```

[4] 磁盘使用情况

```
-------------------------------------
Troubleshooting Menu
-------------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-------------------------------------
Choice: [0 - 4] 4
```

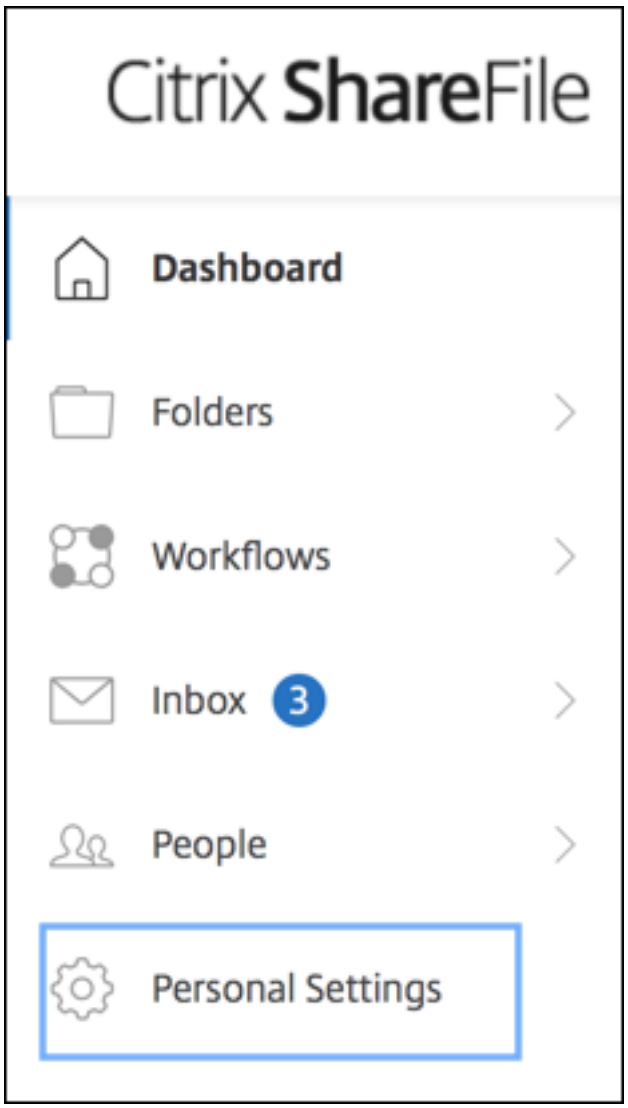
使用 **Citrix Files** 作为 **FTP** 站点来上载支持包

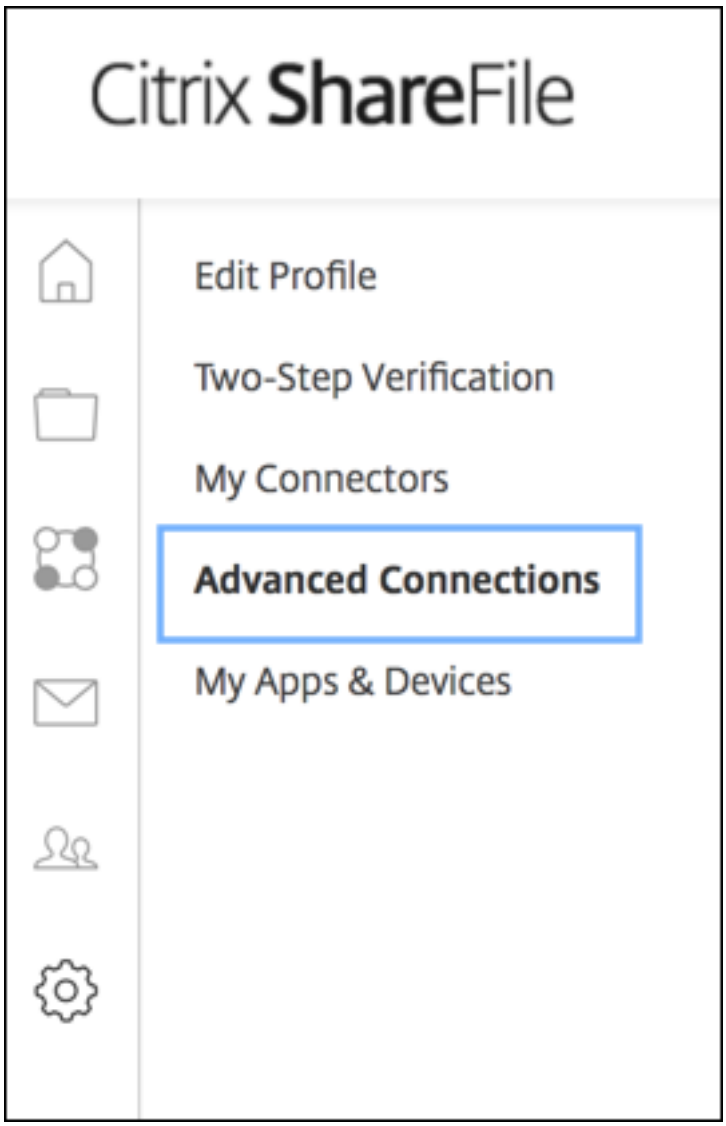
启动支持包上载之前，请在 Citrix Files 上配置以下必备条件：

1. 验证 FTP 登录详细信息。

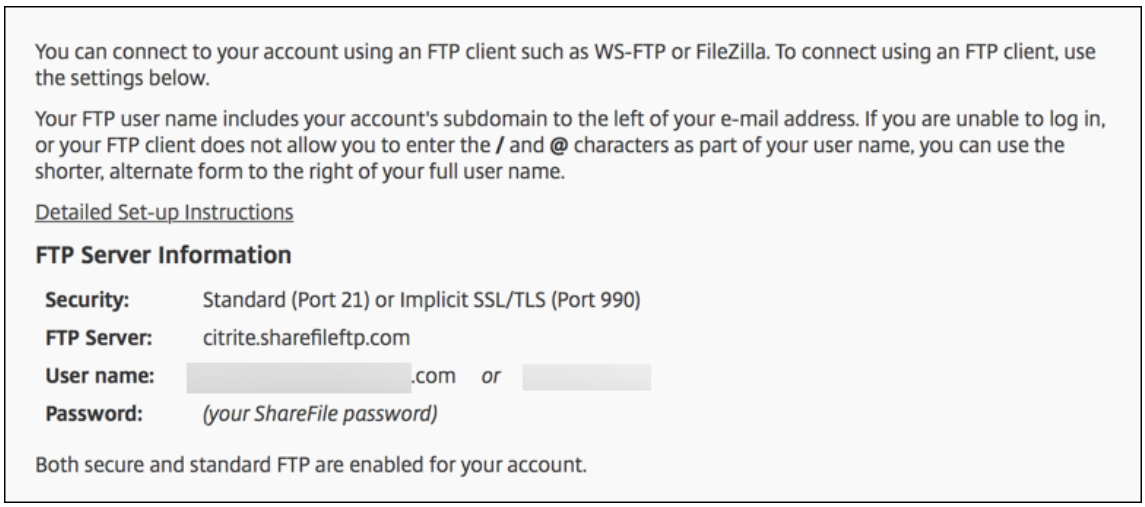
   a. 在 Web 浏览器中，打开 https://citrix.sharefile.com。

   b. 单击个人设置，然后单击高级连接。





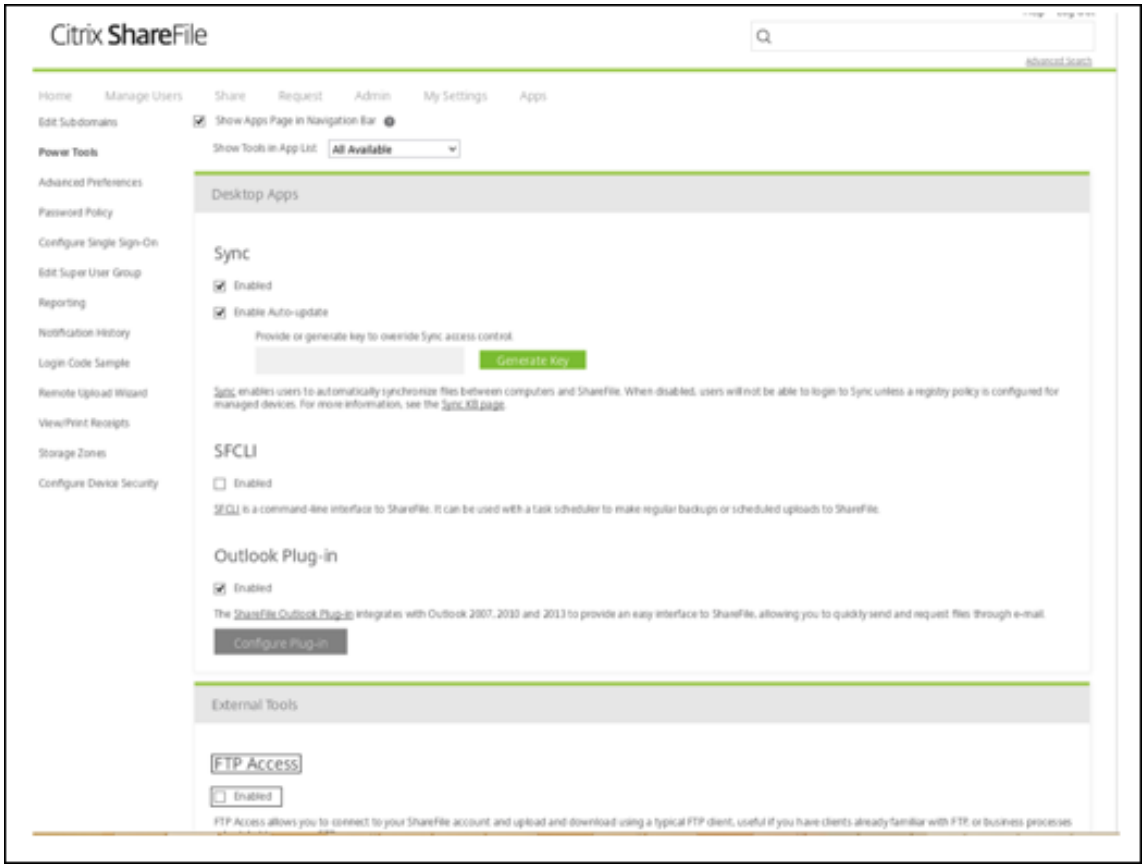
c. 在“FTP 服务器信息”中，对于“用户名”，确认显示的用户 ID 为字母数字形式，并显示默认子域/用户名详细信息。



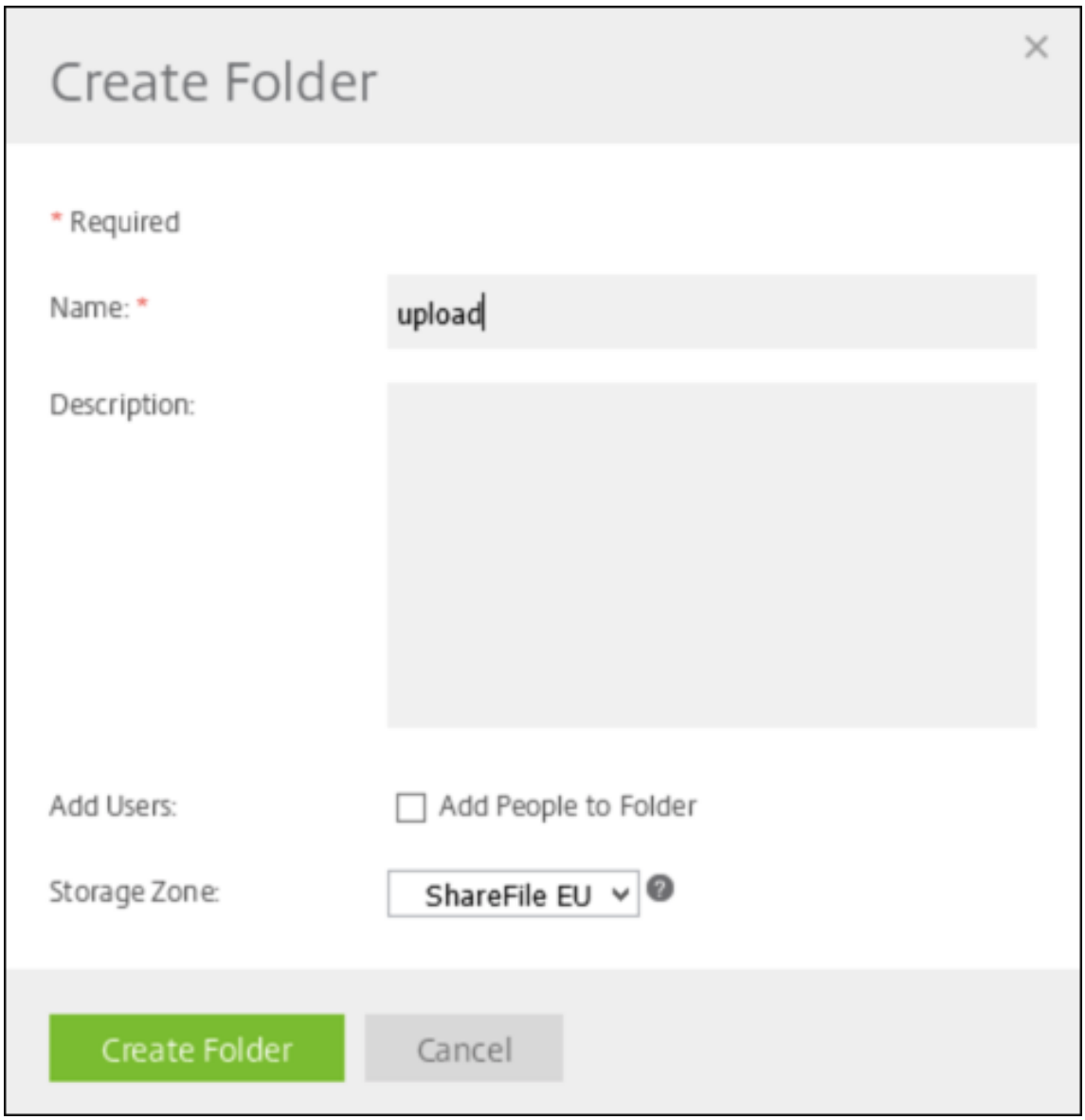
> 备注：
>
> - 您正在从 XenMobile 上载的文件是一个基于 Linux CLI 的 FTP 客户端。因此，不能输入反斜杠 () 和 @ 字符作为用户名的一部分。
> - 如果您看到的用户 ID 不是字母数字形式，可以向您的 Content Collaboration 管理员或 Content Collaboration 支持人员申请此用户 ID。

2. 验证是否已为 Citrix Files 服务器启用 FTP 通信以及 FTPS 通信。理想情况下，Content Collaboration 管理员允许通过 FTP 通信打开用户帐户。但是，有时仅允许进行 FTPS 通信。

   具有管理员权限的用户可以验证并启用此设置，方法是依次单击设置、管理员设置、高级首选项，然后单击启用 **ShareFile** 工具。在外部应用程序、**FTP** 访问中，验证是否已选中启用复选框。



3. 为 FTP 客户端创建用作文件上载目录的共享文件夹。依次单击主页、文件夹，然后单击个人文件夹。
4. 在最右侧，单击加号 (+) 图标，单击创建文件夹，然后输入该文件夹的名称。



5. 在 XenMobile Server CLI 中的主菜单上，选择故障排除 **>** 支持包。然后，在支持包菜单上，选择 **Generate Support Bundle**（生成支持包）。

> 注意：
>
> 如果存在支持包，则在系统提示时，请键入 **y** 以覆盖该支持包。

6. 将支持包上载到 FTP 服务器：

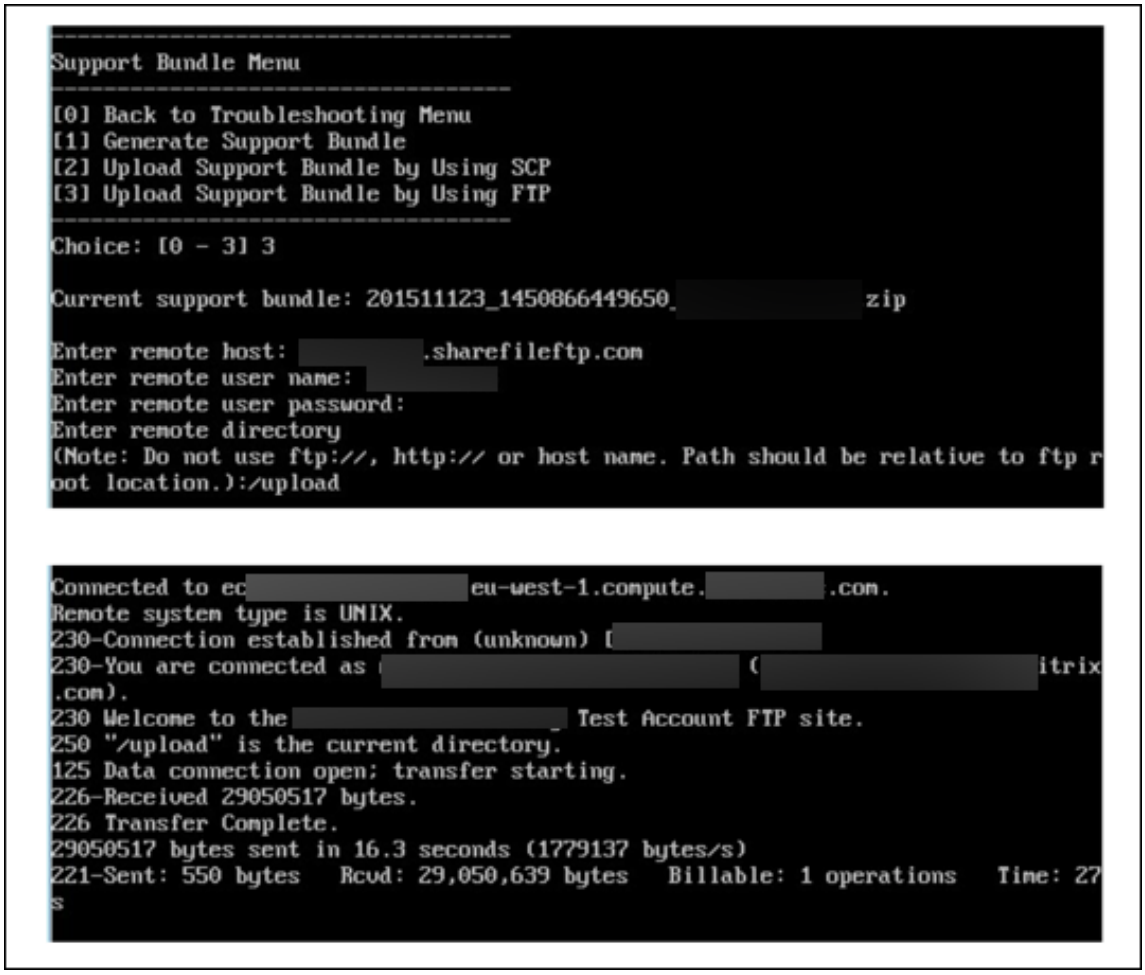
   a. 选择 **Upload Support Bundle by using FTP**（使用 FTP 上载支持包）。

   b. 输入远程主机：在系统提示时，键入 FTP 服务器名称。当 Citrix Files 用作 FTP 服务器时，键入您的公司名称，后跟 Citrix Files FTP 站点名称。例如 citrix.sharefileftp.com。

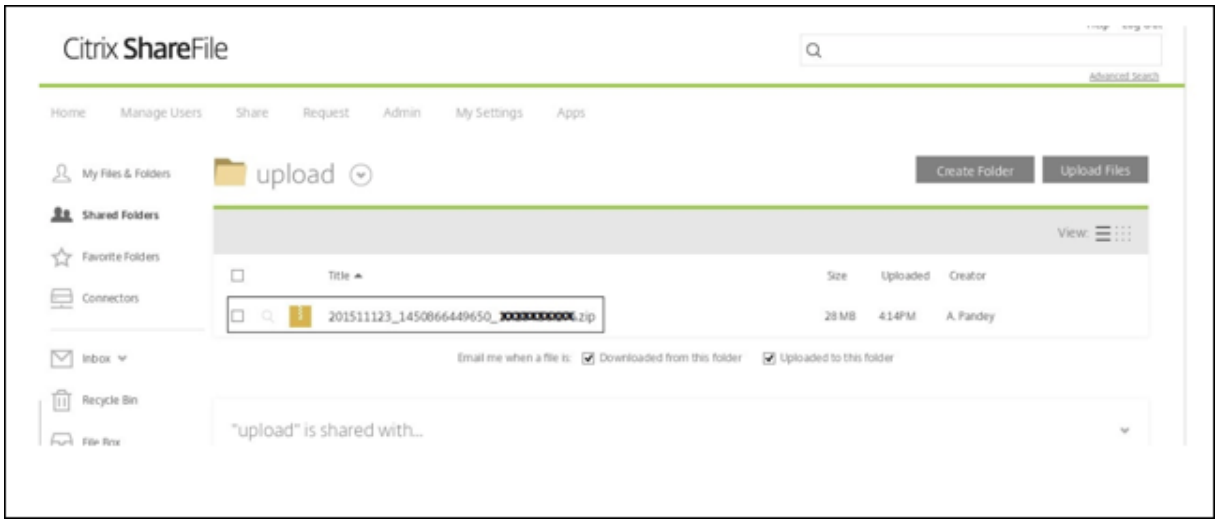
   c. 输入远程用户名：在系统提示时，键入字母数字形式的用户 ID。

d. 输入远程用户密码：在系统提示时，输入您的密码。

e. 输入远程目录：在系统提示时，输入在 Citrix Files 中创建的共享文件夹名称，然后按 **Enter** 键。



可以在于 Citrix Files 中创建的共享文件夹中查看上载的支持包。



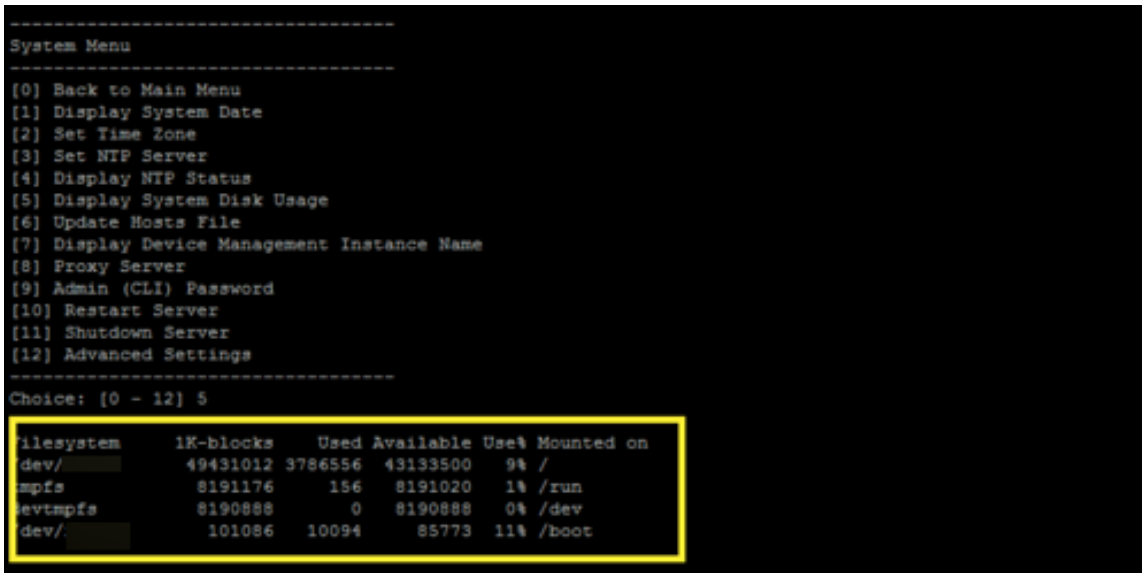
有关 Citrix Files FTP 的详细信息，请参阅 Citrix 支持知识中心文章。

检查磁盘空间

您可以按如下所示在 CLI 中检查系统磁盘空间：

1. 在主菜单中，选择系统菜单。
2. 在系统菜单中，选择显示系统磁盘使用情况选项。

   此时将显示文件系统信息。



执行自助磁盘清理

可以按如下所示在 CLI 中清理磁盘：

1. 在故障排除菜单中，选择磁盘使用情况。磁盘使用情况菜单具有以下选项：

2. 键入 1 列出核心转储文件和支持包文件类型。如果不存在任何文件，您将收到以下消息：**No core dump and support bundles found**（找不到核心转储和支持包）。

3. 键入 2 清除扫描的核心转储文件和支持包文件。

XenMobile 控制台工作流入门

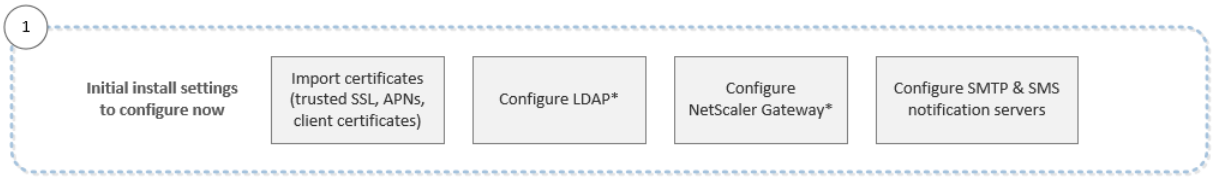
January 5, 2022

XenMobile 控制台是 XenMobile 中的统一管理工具。本文假设您已安装了 XenMobile，并准备好使用此控制台。如果有待安装 XenMobile，请参阅安装 XenMobile。有关 XenMobile 控制台的浏览器支持的详细信息，请参阅“XenMobile 兼容性”一文。

初始设置工作流

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。您无法返回到初始配置屏幕。如果您跳过了某些安装配置，可以在控制台中配置以下设置。开始添加用户、应用程序和设备之前，请考虑完成这些安装设置。开始时，请单击控制台右上角的齿轮图标。

> 注意：
>
> 带星号的项目为可选项目。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章和各节：

- 身份验证
- Citrix Gateway 和 XenMobile
- 通知

必须具有以下帐户相关设置，才能支持 Android、iOS 和 Windows 平台。

Android

- 创建 Google Play 凭据。有关详细信息，请参阅 Google Play 启动。
- 创建一个 Android Enterprise 管理员帐户。有关详细信息，请参阅 Android Enterprise。
- 通过 Google 验证您的域名。有关详细信息，请参阅 Verify your domain for Google Workspace（验证您的 Google Workspace 域）。
- 启用 API 并为 Android Enterprise 创建一个服务帐户。有关详细信息，请参阅 Android 企业版帮助。

iOS

- 创建一个 Apple ID 和开发人员帐户。有关详细信息，请参阅 Apple Developer Program（Apple 开发者计划）Web 站点。
- 创建一个 Apple 推送通知服务 (APNs) 证书。如果您打算通过 XenMobile Server 部署管理 iOS 设备，则需要使用 Apple APNS 证书。如果您为您的 Secure Mail 部署使用推送通知，您还需要 Apple APNs 证书。有关获取 Apple APNs 证书的详细信息，请参阅 Apple Push Certificates Portal。有关 XenMobile 和 APNs 的详细信息，请参阅 APNs 证书和 Secure Mail for iOS 的推送通知。
- 创建批量购买公司令牌。有关详细信息，请参阅 Apple Volume Purchasing Program。

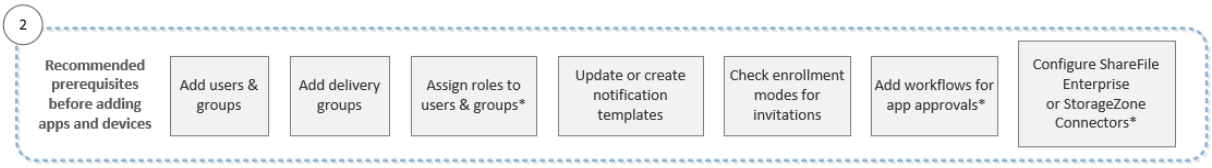
Windows

- 创建一个 Microsoft Windows 应用商店开发人员帐户。有关详细信息，请参阅帐户类型、位置和费用。
- 获取一个 Microsoft Windows 应用商店发布者 ID。有关详细信息，请参阅管理帐户设置和个人资料信息。
- 从 DigiCert 获取一个企业证书。有关详细信息，请参阅适用于 Windows Phone 的公司应用程序分发。
- 如果计划在注册 Windows Phone 时使用 XenMobile 自动发现功能，请确保您具有可用的公用 SSL 证书。有关详细信息，请参阅 XenMobile AutoDiscovery Service。
- 创建一个应用程序注册令牌 (AET)。有关详细信息，请参阅如何生成适用于 Windows Phone 的应用程序注册令牌。

控制台必备条件工作流

此工作流显示在添加应用程序和设备之前要配置的必备条件。

> 注意：
>
> 带星号的项目为可选项目。



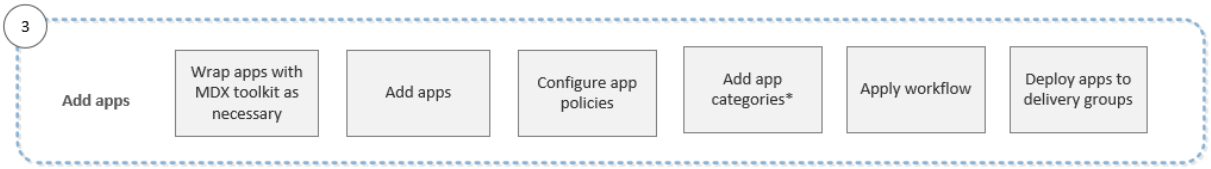
有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章和各节：

- 用户帐户、角色和注册
- 部署资源
- 使用 RBAC 配置角色
- 通知
- 应用工作流
- 将 Citrix Content Collaboration 与 XenMobile 结合使用

添加应用程序工作流

此工作流显示了向 XenMobile 中添加应用程序时应遵循的建议顺序。

> 注意：
>
> 带星号的项目为可选项目。



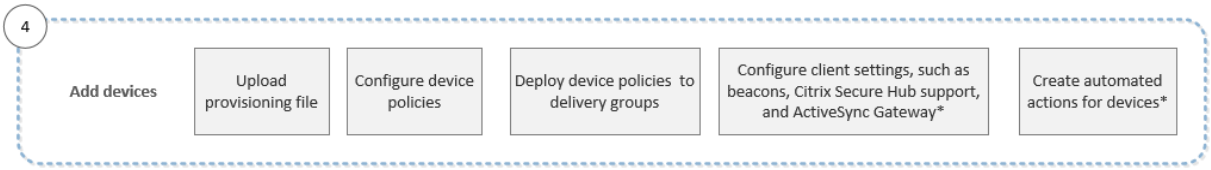
有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章和各节：

- 关于 MDX Toolkit
- 添加应用程序
- MDX 策略概览
- 应用工作流
- 部署资源

添加设备工作流

此工作流显示了向 XenMobile 中添加和注册设备时应遵循的建议顺序。

> 注意：
>
> 带星号的项目为可选项目。

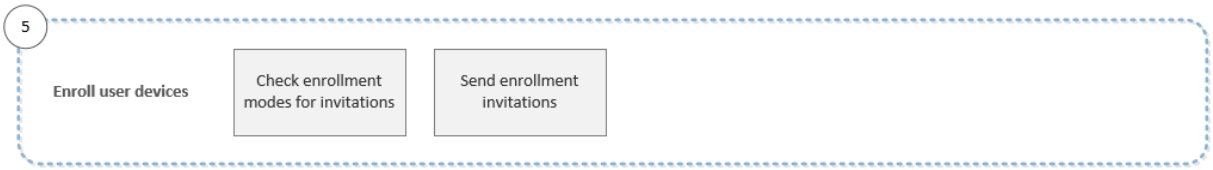


有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章和各节：

- 设备
- 支持的设备操作系统
- 部署资源
- 监视和支持
- 自动化操作

注册用户设备工作流

此工作流显示了在 XenMobile 中注册用户设备时应遵循的建议顺序。



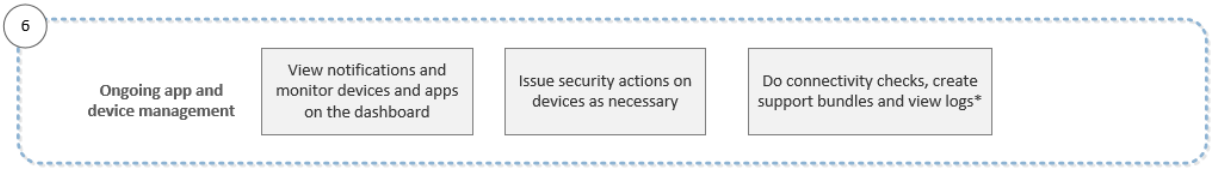
有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 用户帐户、角色和注册
- 通知

正在进行的应用程序和设备管理工作流

此工作流显示您可以在控制台中执行的应用程序和设备管理活动。

> 注意：
>
> 带星号的项目为可选项目。



有关通过单击控制台右上角的扳手图标找到的支持选项的详细信息，请参阅监视和支持。

证书和身份验证

January 5, 2022

在 XenMobile 操作期间，若干组件都会参与身份验证：

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

Secure Hub 还有助于使用 MDX 安全容器：Secure Hub 会推送策略，在应用程序超时后与 Citrix ADC 建立会话，以及定义 MDX 超时和身份验证体验。Secure Hub 还可执行越狱检测、地理定位检查以及您应用的所有策略。

- **MDX** 策略： MDX 策略会在设备上创建数据保管库。MDX 策略会将 Micro VPN 连接引导回 Citrix ADC，强制执行脱机模式限制，以及强制执行超时等客户端策略。

有关配置身份验证的详细信息，包括单重身份验证方法和双重身份验证方法概述，请参阅《部署手册》文章身份验证。

使用 XenMobile 中的证书创建安全连接并对用户进行身份验证。本文余下部分将介绍证书。有关其他配置详细信息，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
- PKI 实体
- 凭据提供程序
- APNs 证书
- SAML 单点登录与 Citrix Files
- Microsoft Azure Active Directory 服务器设置
- 要将证书发送到设备以对 Wi-Fi 服务器进行身份验证，请执行以下操作：Wi-Fi 设备策略
- 要推送未用于身份验证的唯一证书，例如内部根证书颁发机构 (CA) 证书或特定策略（证书设备策略），请执行以下操作：

证书

XenMobile 在安装过程中生成自签名安全套接字层 (SSL) 证书，用于确保与服务器之间的通信流安全。必须使用知名 CA 发布的可信 SSL 证书替换此 SSL 证书。

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

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

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

下表显示了每个 XenMobile 组件的证书格式和类型：

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

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

XenMobile 支持位长度为 4096、2048 和 1024 的 SSL 侦听器证书和客户端证书。1024 位证书很容易被盗用。

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

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

在 **XenMobile** 中上载证书

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

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

私钥要求

XenMobile 可能会处理给定证书的私钥，但也可能不会进行此项处理。同样，XenMobile 可能需要也可能不需要所上载证书的私钥。

上载证书

您有两个用于上载证书的选项：

- 将证书单独上载到控制台。
- 使用 REST API 将证书批量上载到 iOS 设备。

将证书上载到控制台的主要方式有两种：

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

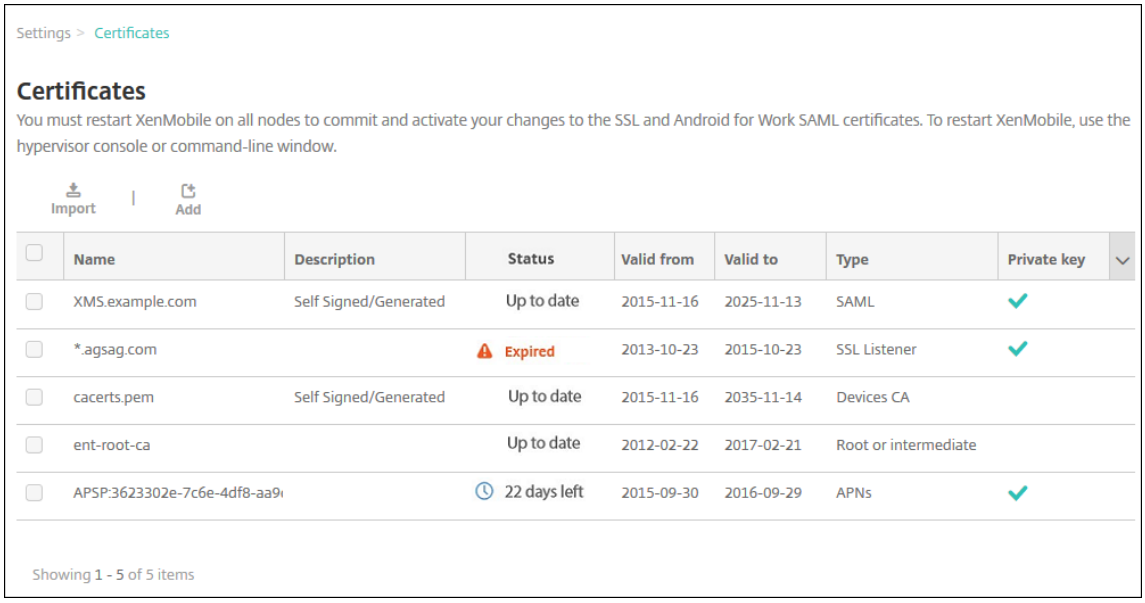
您可以上载 CA 用于对请求进行签名的 CA 证书（不带私钥）。您还可以上载用于客户端身份验证的 SSL 客户端证书（带私钥）

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

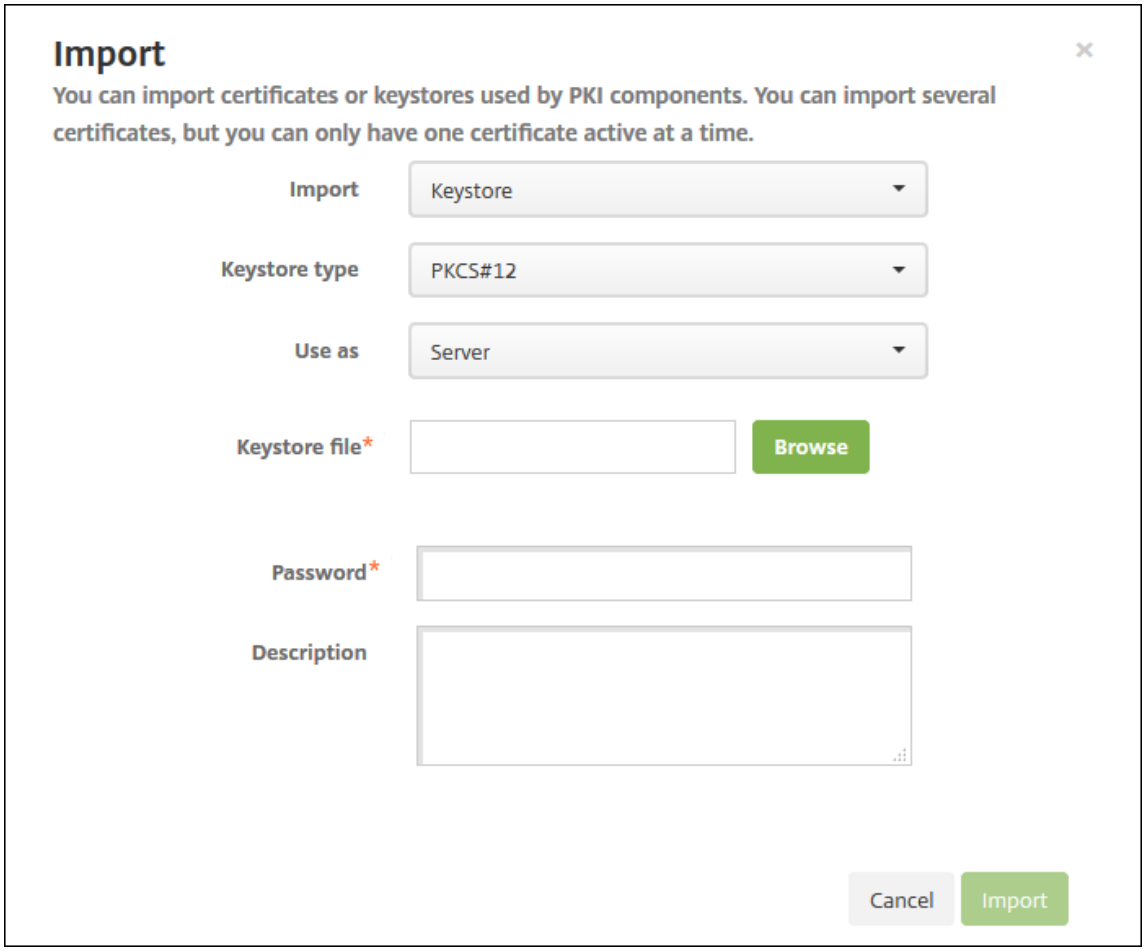
导入密钥库

按照设计，密钥库（安全证书的存储库）可以包含多个条目。因此，从密钥库加载时，系统会提示您指定条目别名，用于识别要加载的条目。如果未指定别名，将加载库中的第一个条目。由于 PKCS #12 文件通常仅包含一个条目，当选择 PKCS #12 作为密钥库类型时，不会显示别名字段。

1. 在 XenMobile 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. 单击证书。此时将显示证书页面。



3. 单击导入。此时将显示导入对话框。
4. 配置以下设置：
    - 导入：在列表中，单击密钥库。导入对话框将更改以反映可用的密钥库选项。



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

5. 单击导入。密钥库将添加到证书表中。

导入证书

从文件或密钥库条目导入证书时，XenMobile 将尝试基于输入内容构建证书链。XenMobile 将导入该链中的所有证书来为每个证书创建一个服务器证书条目。仅当文件或密钥库条目中的证书形成链时，才可执行此操作。例如，如果链中每个后续证书是前一个证书的颁发者。

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

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击证书。
2. 在证书页面上，单击导入。此时将显示导入对话框。
3. 在导入对话框的导入中，如果尚未选择，请单击证书。
4. 导入对话框将更改以反映可用的证书选项。在用作中，选择您计划使用密钥库的方式。可用选项如下：
   - 服务器。服务器证书是 XenMobile Server 功能性使用的证书，这些证书上载到 XenMobile Web 控制台中。这些证书包括 CA 证书、RA 证书以及用于您基础结构其他组件的客户端身份验证的证书。此外，您还可以使用服务器证书来存储您要部署到设备的证书。此选项特别适用于在设备上建立信任所使用的 CA。
   - **SAML**。安全声明标记语言 (SAML) 认证允许您提供对服务器、Web 站点和应用程序的单点登录 (SSO) 访问权限。
   - **SSL** 侦听器。安全套接字层 (SSL) 侦听器向 XenMobile 通知 SSL 加密活动。
5. 浏览查找要导入的文件类型为.p12 （在基于 Windows 的计算机上为.pfx）的密钥库。
6. 浏览以查找证书的可选私钥文件。私钥用于与证书一起使用以便进行加密和解密。
7. 键入证书的说明（可选），以帮助您将其与其他证书区分开。
8. 单击导入。证书将添加到证书表中。

使用 **REST API** 将证书批量上载到 **iOS** 设备

如果一次上载一个证书并不现实，则可以使用 REST API 将证书批量上载到 iOS 设备。此方法支持.p12 格式的证书。有关 REST API 的详细信息，请参阅 REST API。

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

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

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

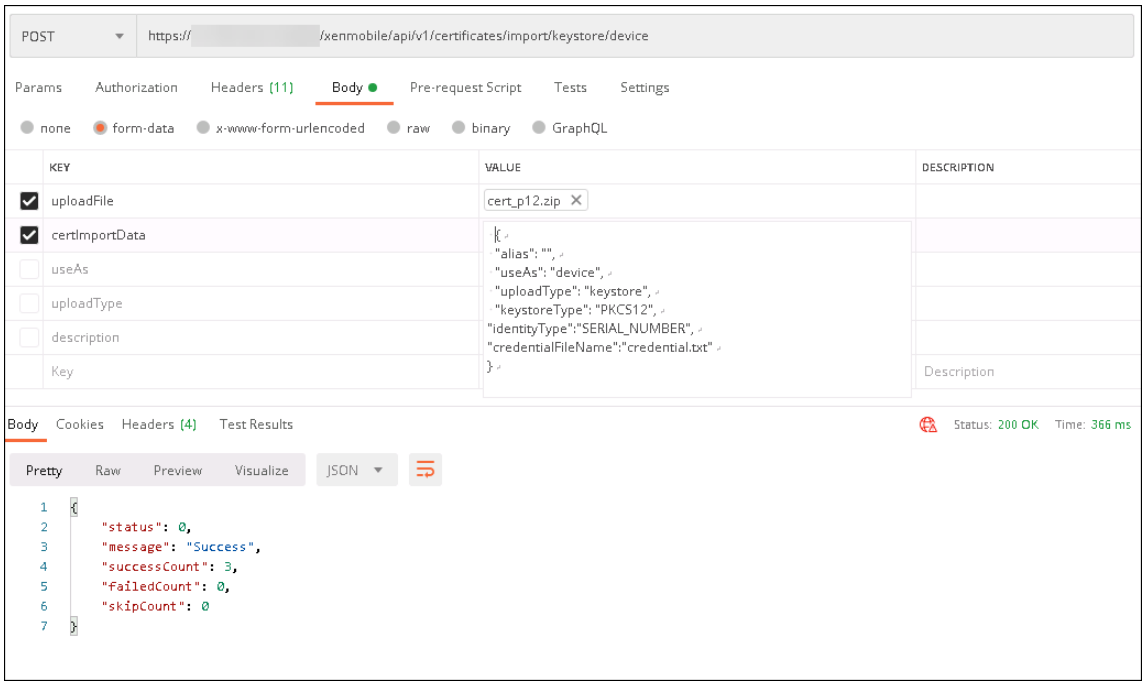
   ```
   A12BC3D4EFGH.p12=password1!
   A12BC3D4EFIJ.p12=password2@
   A12BC3D4EFKL.p12=password3#
   <!--NeedCopy-->
   ```

3. 将所有证书和您创建的文本文件打包到.zip 文件中。

4. 启动 REST API 客户端，登录 XenMobile，然后获取身份验证令牌。

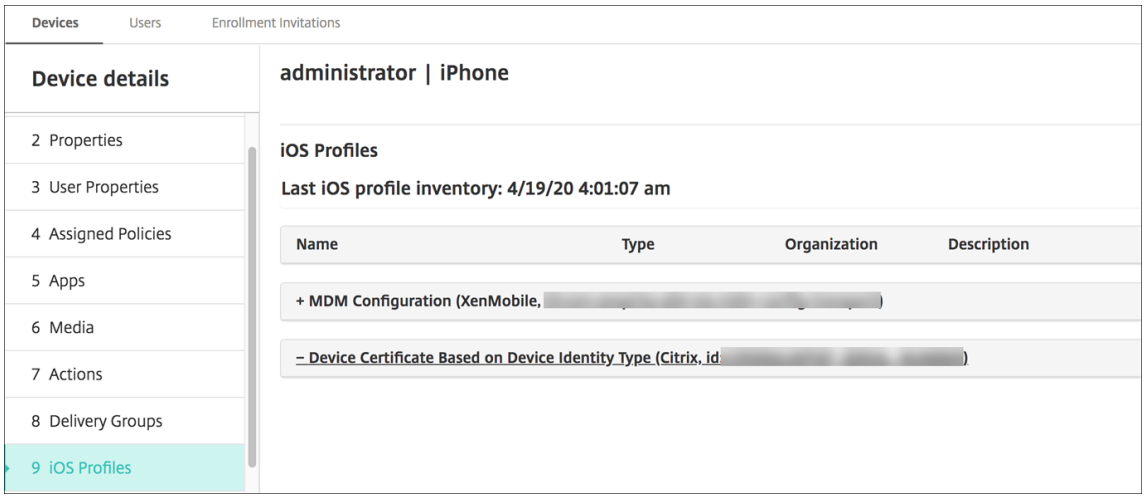
5. 导入您的证书，确保您将以下内容放入消息正文中：

```
{

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

<!--NeedCopy-->
```



6. 使用凭据类型 **Always on IKEv2**（始终启用 IKEv2）和设备身份验证方法基于设备标识的设备证书创建 VPN 策略。选择您的证书文件名中使用的设备标识类型。请参阅 VPN 设备策略。

7. 注册 iOS 设备并等待部署 VPN 策略。通过检查设备上的 MDM 配置来确认证书安装。还可以在 XenMobile 控制台中检查设备详细信息。

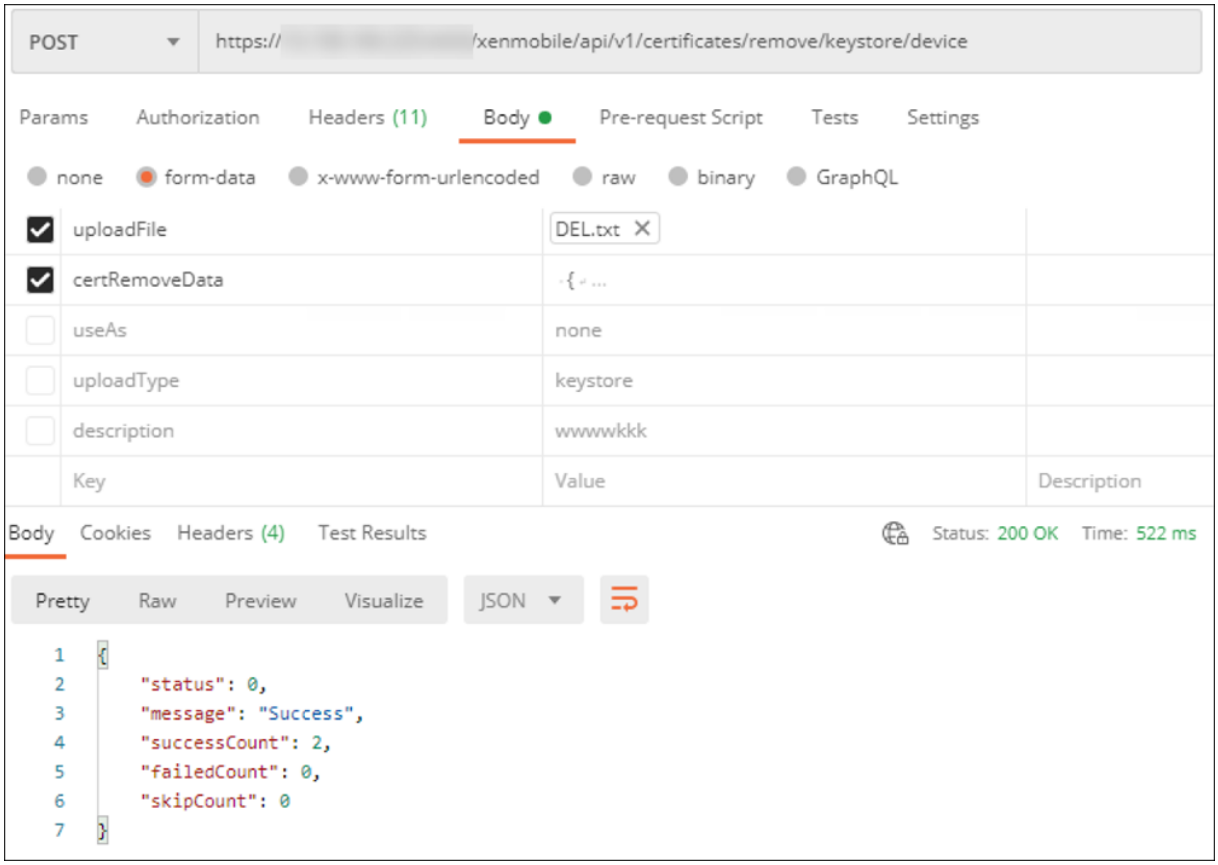


还可以通过创建一个包含为每个要删除的证书列出的 device_identity_value 的文本文件来批量删除证书。在 REST API 中，调用删除 API 并使用以下请求，将 device_identity_value 替换为适当的标识符：

```
```
{

    "identityType"="device_identity_value"
 }

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

 
```



更新证书

XenMobile 只允许系统中每个公钥一次存在一个证书。如果您尝试为已导入证书的同一密钥对导入证书：您可以替换现有条目或将其删除。

要最有效地更新您的证书，请在 XenMobile 控制台上执行以下操作。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。在导入对话框中，导入新证书。

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

续签证书

XenMobile Server 在内部将以下证书颁发机构用于 PKI：根 CA、设备 CA、服务器 CA。这些 CA 分类为一个逻辑组并提供一个组名称。预配新的 XenMobile Server 实例时，会生成这三个 CA 并为其提供组名称 “default”。

您可以使用 XenMobile Server 控制台或公用 REST API 为支持的 iOS、macOS 和 Android 设备续订 CA。对于注册的 Windows 设备，用户必须重新注册其设备才能接收新的设备 CA。

以下 API 可用于在 XenMobile Server 中续订或重新生成内部 PKI CA，以及续订这些证书颁发机构颁发的设备证书。

- 创建组证书颁发机构 (CA)。

- 激活新 CA 和取消激活旧 CA。
- 在一组配置的设备上续订设备证书。已注册的设备继续运行而不会中断。设备重新连接到服务器时颁发设备证书。
- 返回仍使用旧 CA 的设备列表。
- 所有设备都拥有新 CA 后删除旧 CA。

有关信息，请参阅 Public API for REST Services（适用于 REST 的公共 API 服务）PDF：

- 第 3.16.58 节 “Renew Device Certificate”（续订设备证书）
- 第 3.23 节，内部 PKI CA 组

管理设备控制台包括用于续订设备上的注册证书的安全操作证书续订。

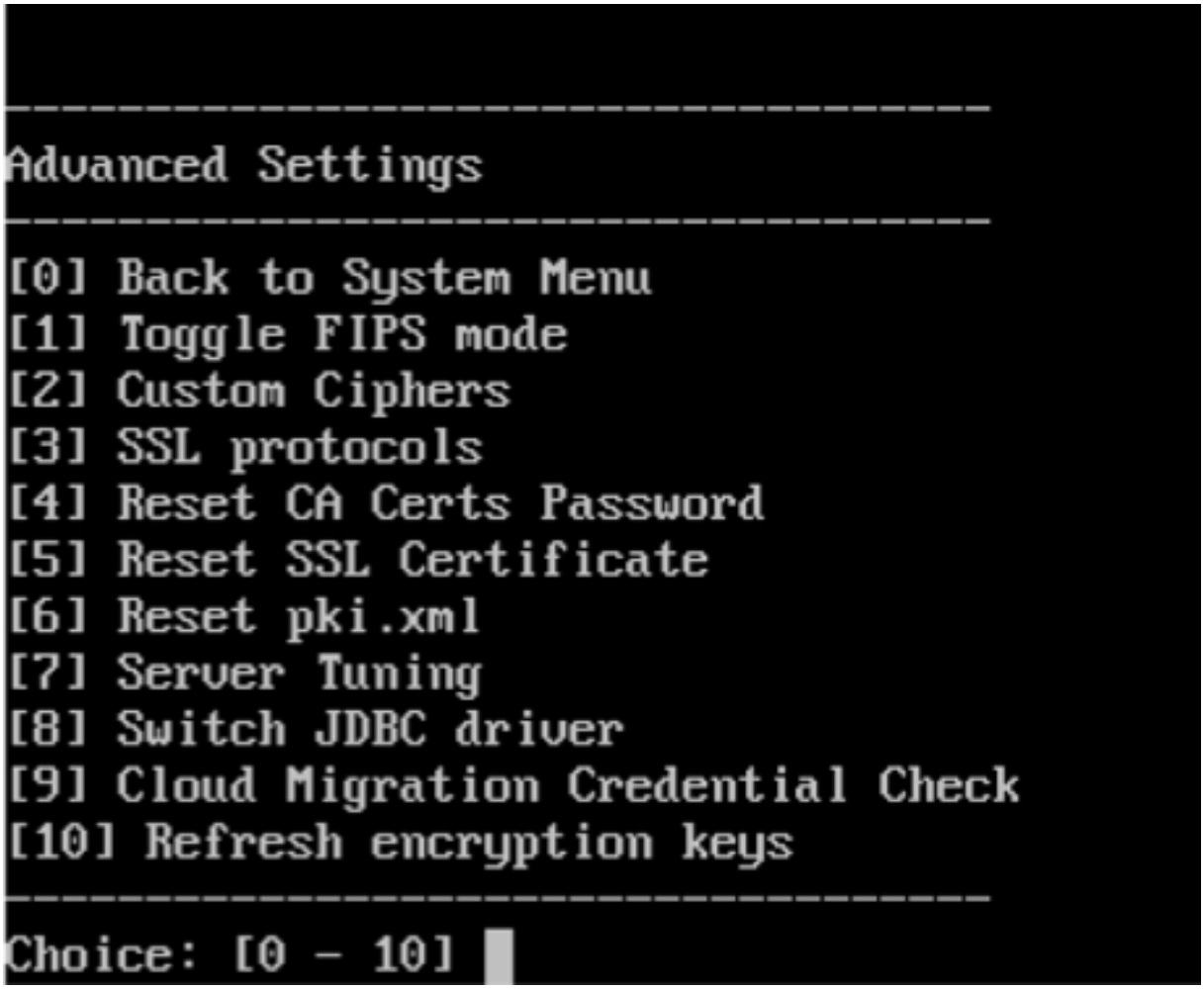
必备条件

- 默认情况下，此证书刷新功能处于禁用状态。要激活证书刷新功能，请将服务器属性 **refresh.internal.ca** 的值设置为 **True**。

> 重要：
>
> 如果您的 Citrix ADC 设置了 SSL 卸载，则在生成新证书时，请确保使用新的 cacert.perm 来更新您的负载平衡器。有关 Citrix Gateway 设置的详细信息，请参阅为 Citrix ADC VIP 使用 SSL 卸载模式。

用于为群集节点重置服务器 **CA** 证书密码的 **CLI** 选项

在一个 XenMobile Server 节点上生成服务器 CA 证书后，可使用 XenMobile CLI 在其他群集节点上重置证书密码。在 CLI 主菜单中，选择系统 **>** 高级设置 **>** 重置 **CA** 证书密码。如果在没有任何新的 CA 证书时重置密码，XenMobile 不会重置密码。



XenMobile 证书管理

我们建议您列出在您的 XenMobile 部署中使用的证书，尤其是证书的过期日期和关联的密码。本节旨在帮助您更轻松地在 XenMobile 中进行证书管理。

您的环境中可能包含以下部分或所有证书：

- XenMobile Server
  - 用于 MDM FQDN 的 SSL 证书
  - SAML 证书（适用于 Citrix Files）
  - 用于以上证书和任何其他内部资源（StoreFront/代理等）的根证书和中间 CA 证书
  - 用于 iOS 设备管理的 APN 证书
  - 用于 XenMobile Server Secure Hub 通知的内部 APNs 证书
  - 用于连接到 PKI 的 PKI 用户证书
- MDX Toolkit
  - Apple 开发人员证书

  - Apple 预配配置文件（按应用程序）
  - Apple APNs 证书（用于 Citrix Secure Mail）
  - Android 密钥库文件
  - Windows Phone - DigiCert 证书

  MAM SDK 不封装应用程序，因此不需要证书。

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

XenMobile 证书过期策略

如果允许证书过期，证书则会无效。您不能再在您的环境中运行安全事务，也不能访问 XenMobile 资源。

> 注意：
>
> 证书颁发机构 (CA) 会在过期日期之前提示您续订 SSL 证书。

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

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

用于 **iOS** 设备管理的 **APNs** 证书

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

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

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

```
1 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.
2
```



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

Thank You,

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

MDX Toolkit（iOS 分发证书）

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

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

要验证您的 iOS 分发证书是否有效，请执行以下操作：

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

要确认所有 XenMobile Server 证书是否有效，请执行以下操作：

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

Android 密钥库

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

DigiCert 提供的用于 Windows Phone 的企业证书

DigiCert 是用于 Microsoft 应用程序中心服务的代码签名证书的独家提供商。开发者和软件发行者加入应用程序中心来分发 Windows Phone 和 Xbox 360 应用程序，以便通过 Windows Marketplace 下载。有关详细信息，请参阅 DigiCert 文档中的 DigiCert Code Signing Certificates for Windows Phone（适用于 Windows Phone 的 DigiCert 代码签名证书）。

如果证书过期，Windows Phone 用户将无法注册。用户无法安装公司发布和签名的应用程序，也不能启动手机上安装的公司应用程序。

Citrix ADC

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

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

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

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

Citrix Gateway 和 XenMobile

January 5, 2022

使用 XenMobile 配置 Citrix Gateway 时，为远程设备访问内部网络建立身份验证机制。利用此功能，移动设备上的应用程序可以访问位于 Intranet 上的企业服务器。XenMobile 在设备上的应用程序与 Citrix Gateway 之间创建一个 Micro VPN。

您通过从 Citrix Gateway 上运行的 XenMobile 中导出一个脚本，将 Citrix Gateway 配置为与 XenMobile 结合使用。

使用 Citrix Gateway 配置脚本的必备条件

Citrix ADC 要求：

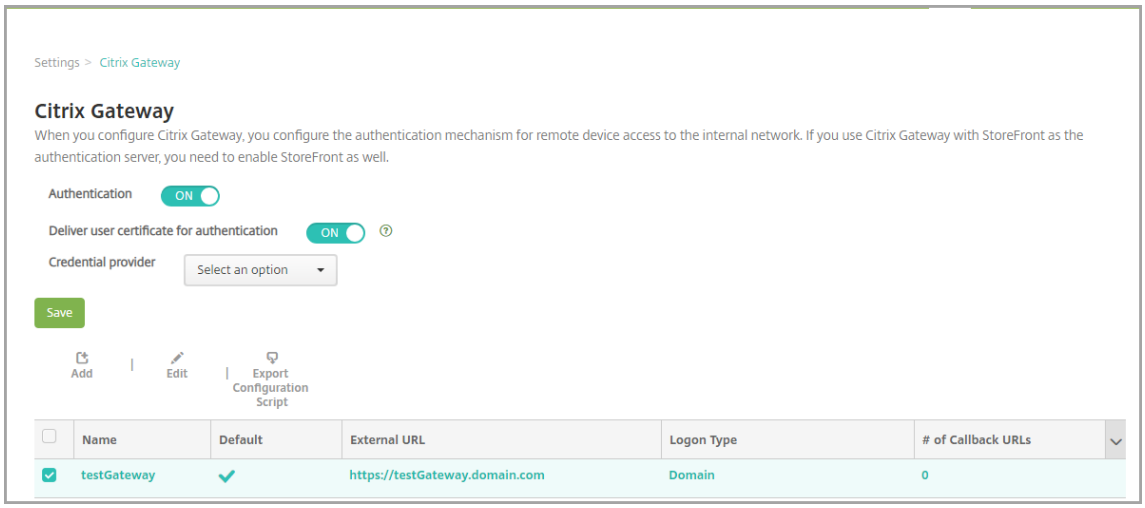
- Citrix ADC（最低版本 11.0，内部版本号 70.12）。
- Citrix ADC IP 地址已配置并且连接到 LDAP 服务器（平衡了 LDAP 的负载时除外）。
- Citrix ADC 子网 (SNIP) IP 地址已配置，连接到必需的后端服务器，并且能够通过端口 8443/TCP 访问公用网络。
- DNS 可以解析公共域。
- Citrix ADC 已通过平台/通用许可证或试用版许可证获得许可。有关信息，请参阅 https://support.citrix.com/article/CTX126049。
- Citrix Gateway SSL 证书已上载并安装在 Citrix ADC 上。有关信息，请参阅 https://support.citrix.com/article/CTX136023。

XenMobile 的要求：

- XenMobile Server（最低版本 10.6）。
- LDAP 服务器已配置。

配置身份验证以便远程设备能够访问内部网络

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

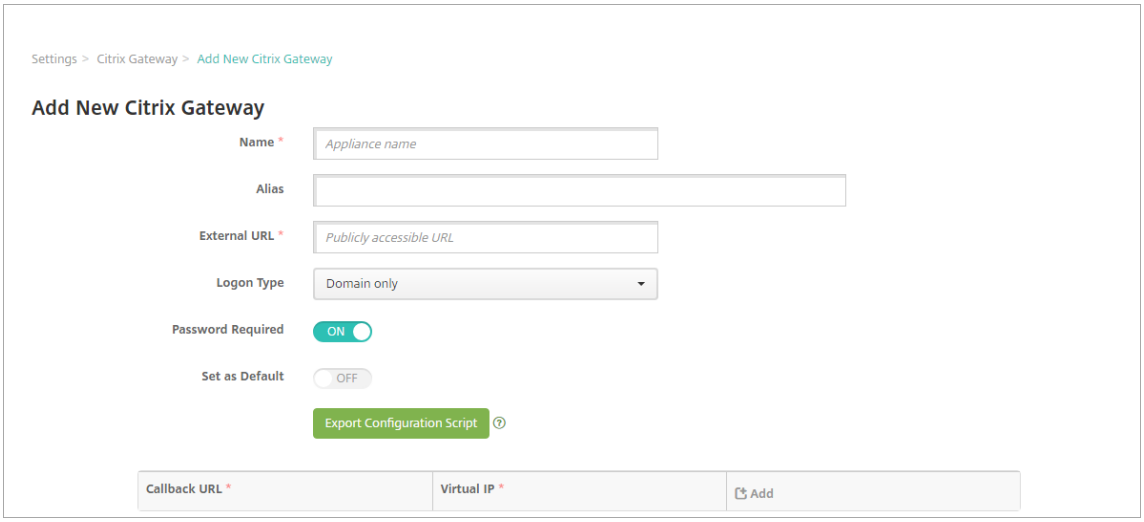


3. 配置以下设置：
   - 身份验证：选择是否启用身份验证。默认值为开。
   - 向用户提供用于身份验证的证书：选择是否希望 XenMobile 与 Secure Hub 共享身份验证证书，以使 Citrix Gateway 能够处理客户端证书身份验证。默认值为关。
   - 凭据提供程序：在列表中，单击要使用的凭据提供程序。有关详细信息，请参阅凭据提供程序。
4. 单击保存。

添加 **Citrix Gateway** 实例

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

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将打开设置页面。
2. 在服务器下方，单击 **Citrix Gateway**。此时将显示 **Citrix Gateway** 页面。
3. 单击添加。此时将显示添加新的 **Citrix Gateway** 页面。



4. 配置以下设置：

   - 名称：键入 Citrix Gateway 实例的名称。
   - 别名：（可选）包括 Citrix Gateway 的别名。
   - 外部 **URL**：键入 Citrix Gateway 的可公开访问的 URL。例如，`https://receiver.com`。
   - 登录类型：选择登录类型。类型包括仅限域、仅限安全令牌、域和安全令牌、证书、证书和域以及证书和安全令牌。需要密码字段的默认设置会根据所选登录类型发生变化。默认值为仅限域。

   如果您有多个域，请使用证书和域。有关为 XenMobile 和 Citrix Gateway 配置多域身份验证的详细信息，请参阅为多个域配置身份验证。

   如果使用证书和安全令牌，则需要在 Citrix Gateway 上设置一些其他配置才能支持 Secure Hub。有关信息，请参阅为 XenMobile 配置证书和安全令牌身份验证。

   有关详细信息，请参阅部署手册中的身份验证。

   - 需要密码：选择是否要求使用密码身份验证。默认值因会根据所选登录类型发生变化。
   - 设为默认值：选择是否将此 Citrix Gateway 用作默认值。默认值为关。
   - 导出配置脚本：单击此按钮可导出您上载到 Citrix Gateway 以通过 XenMobile 设置对其进行配置的配置包。有关信息，请参阅这些步骤后面的“配置本地 Citrix Gateway 以与 XenMobile Server 配合使用”。
   - 回调 **URL** 和虚拟 **IP**：请在添加这些字段之前保存您的设置。有关信息，请参阅本文中的添加回调 URL 和 Citrix Gateway VPN 虚拟 IP。

5. 单击保存。

   此时 Citrix Gateway 已添加并显示在表格中。要编辑或删除实例，请单击列表中的名称。

配置 **Citrix Gateway** 以与 **XenMobile Server** 配合使用

要配置本地 Citrix Gateway 以与 XenMobile 结合使用，请执行本文中详细介绍的以下常规步骤：

1. 从 XenMobile Server 下载一个脚本以及相关的文件。请参阅脚本附带的自述文件了解最新的详细说明。
2. 确认您的环境是否满足必备条件。
3. 更新脚本使其适用您的环境。
4. 在 Citrix ADC 上运行脚本。
5. 测试配置。

该脚本配置 XenMobile 所需的以下 Citrix Gateway 设置：

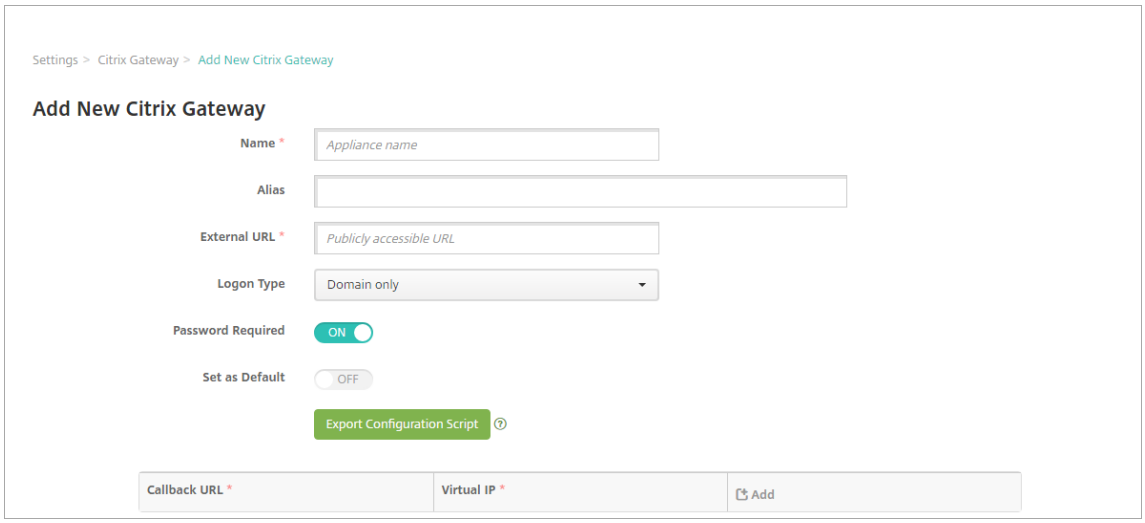
- MDM 和 MAM 需要的 Citrix Gateway 虚拟服务器
- Citrix Gateway 虚拟服务器的会话策略
- XenMobile Server 详细信息
- Citrix Gateway 虚拟服务器的身份验证策略和操作。
  该脚本描述了 LDAP 配置设置。
- 代理服务器的流量操作和策略
- 无客户端访问配置文件
- Citrix ADC 上的静态本地 DNS 记录
- 其他绑定：服务策略、CA 证书

该脚本不处理以下配置：

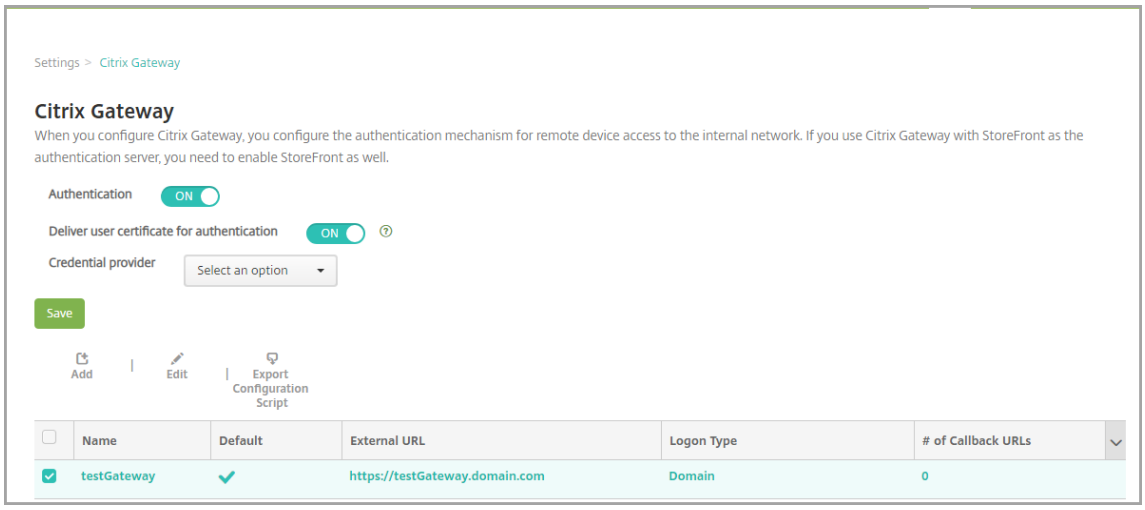
- Exchange 负载平衡
- Citrix Files 负载平衡
- ICA 代理配置
- SSL 卸载

下载、更新和运行脚本

1. 如果要添加 Citrix Gateway，请单击添加新 **Citrix Gateway** 页面上的导出配置脚本。



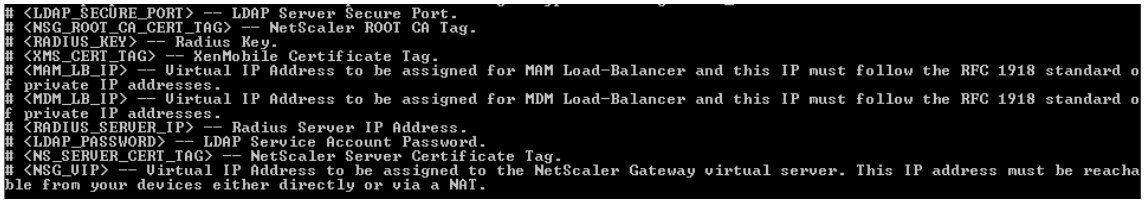
或者，如果您在导出脚本之前添加了一个 Citrix Gateway 实例并单击保存，请返回设置 **> Citrix Gateway**，选择“Citrix ADC”，单击导出配置脚本，然后单击下载。



单击导出配置脚本后，XenMobile 将创建一个.tar.gz 脚本包。脚本包中包括：

- 包含详细说明的 readme 文件
- 包含用于在 Citrix ADC 中配置所需组件的 Citrix ADC CLI 命令的脚本
- XenMobile Server 的公用根 CA 证书和中间 CA 证书（这些证书用于 SSL 卸载，不是当前版本必需的证书）
- 包含用于删除 Citrix ADC 配置的 Citrix ADC CLI 命令的脚本

2. 编辑脚本 (NSGConfigBundle_CREATESCRIPT.txt) 以将所有占位符替换为您的环境中的详细信息。



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

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



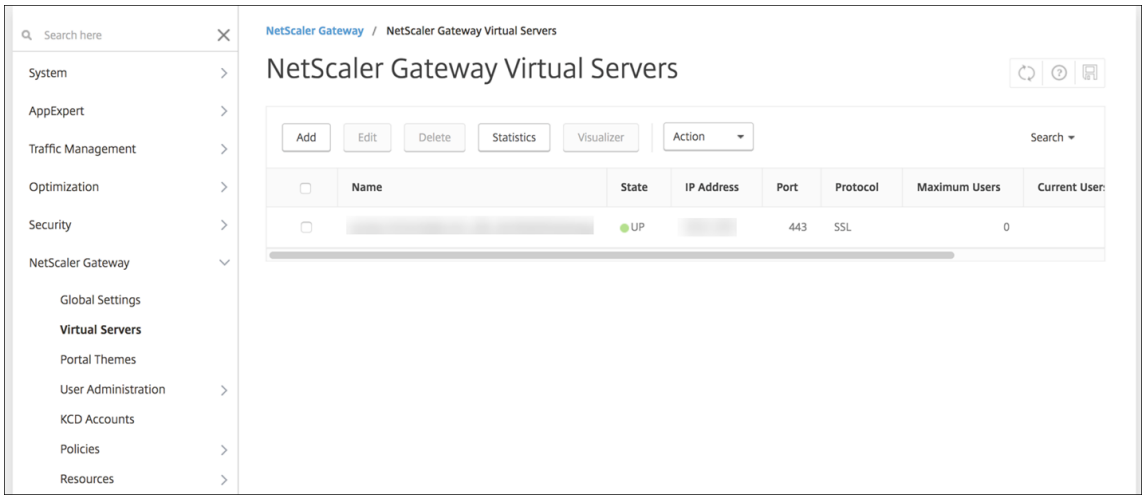
```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

脚本完成后，将显示以下行。

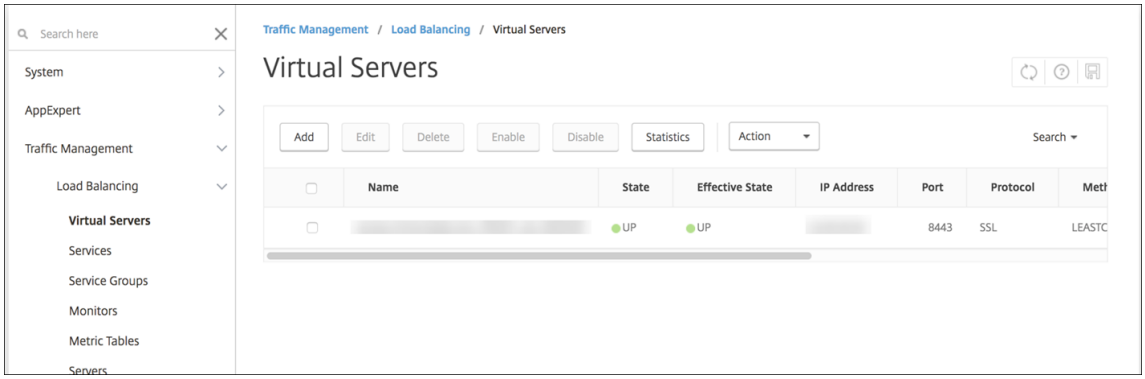
```
exec: save ns config
 Done
 Done
root@ns#
```

测试配置

1. 验证 Citrix Gateway 虚拟服务器显示的状态是否为运行。



2. 验证代理负载平衡虚拟服务器显示的状态是否为运行。



3. 打开 Web 浏览器，连接到 Citrix Gateway URL，并尝试进行身份验证。如果身份验证失败，将显示以下消息：HTTP 状态 404 - 未找到
4. 注册设备，并确保其获取 MDM 和 MAM 注册。

添加回调 **URL** 和 **Citrix Gateway VPN** 虚拟 **IP**

添加 Citrix Gateway 实例后，可以添加一个回调 URL 并指定 Citrix Gateway 虚拟 IP 地址。这些设置是可选设置，但是可以进行配置以增强安全性，尤其是当 XenMobile Server 在 DMZ 中时。

1. 在设置 **> Citrix Gateway** 中，选择 Citrix Gateway，然后单击编辑。
2. 在表格中，单击添加。
3. 对于回调 **URL**，键入完全限定的域名 (FQDN)。回调 URL 验证请求是否来自 Citrix Gateway。

   请确保回调 URL 解析为可从 XenMobile Server 访问的 IP 地址。回调 URL 可以是外部 Citrix Gateway URL 或某些其他 URL。
4. 键入 Citrix Gateway 虚拟 **IP** 地址，然后单击保存。

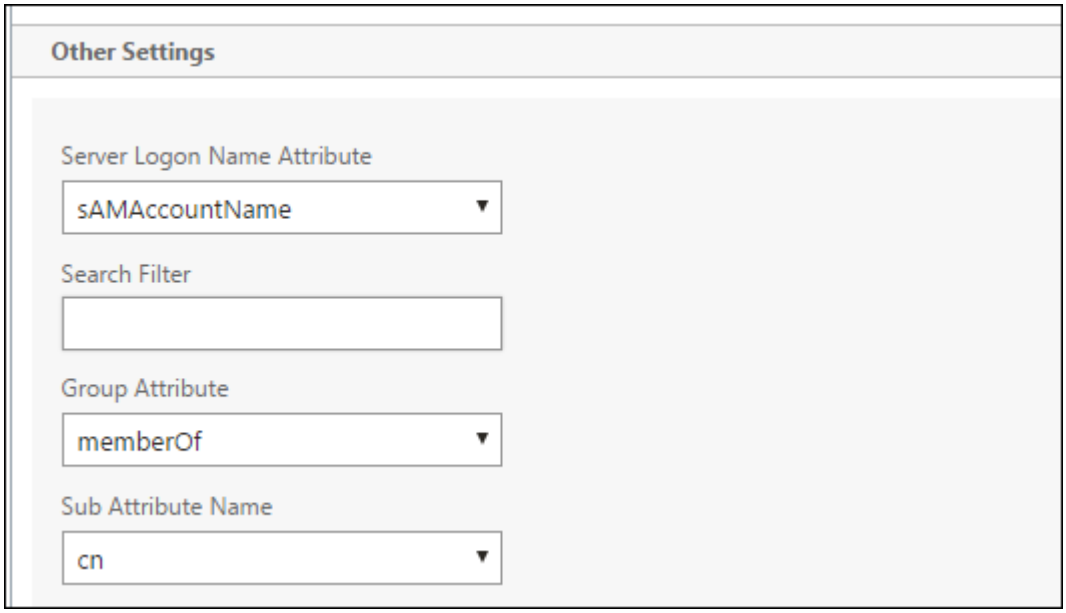
为多个域配置身份验证

如果您有多个 XenMobile Server 实例（例如，用于测试、开发和生产环境），则必须手动为其他环境配置 Citrix Gateway。（只能运行一次适用于 XenMobile 的 Citrix ADC 向导。）

Citrix Gateway 配置

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

1. 在 Citrix Gateway 配置实用程序中的配置选项卡上，展开 **Citrix Gateway >** 策略 **>** 身份验证。
2. 在导航窗格中，单击 **LDAP**。
3. 单击后即可编辑 LDAP 配置文件。将服务器登录名称属性更改为 **userPrincipalName** 或您想要用于执行搜索操作的属性。记下您指定的属性，以便在 XenMobile 控制台中配置 LDAP 设置时具有该属性。

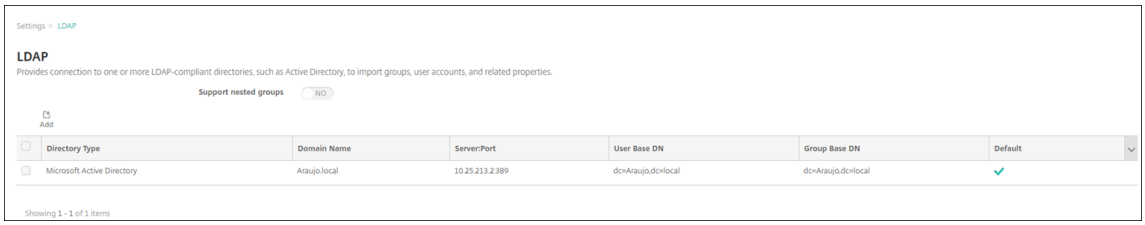


4. 针对每个 LDAP 策略重复以上步骤。每个域均需要一个单独的 LDAP 策略。
5. 在绑定到 Citrix Gateway 虚拟服务器的会话策略中，导航到编辑会话配置文件 **>** 已发布的应用程序。请确保单点登录域为空。

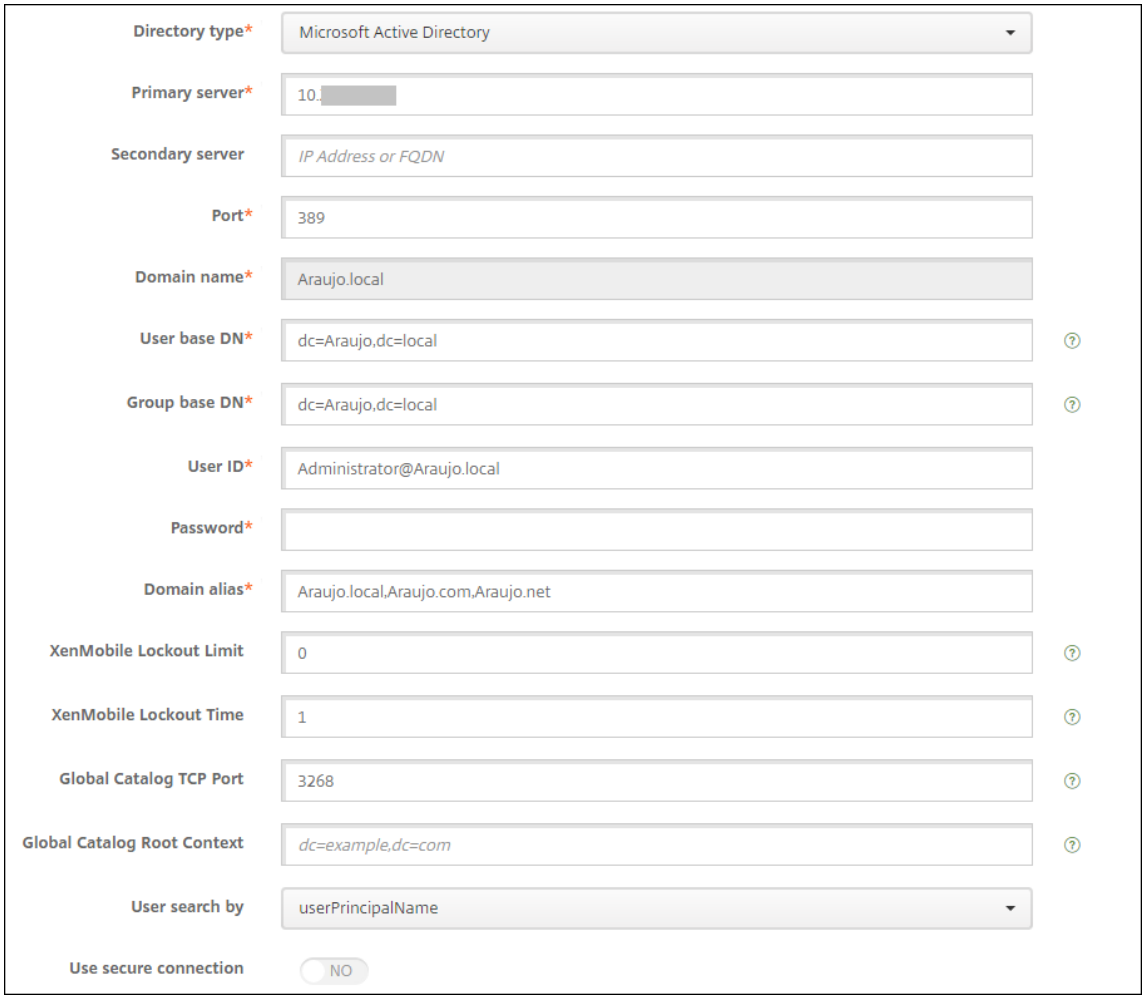
XenMobile Server 配置

要为多域 XenMobile 环境配置 LDAP，请执行以下操作：

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



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



删除对特定 **URL** 的入站连接请求

如果您的环境中的 Citrix Gateway 是为 SSL 卸载配置的，您可能希望网关删除对特定 URL 的入站连接请求。

如果您更偏好额外的安全性，请在 Citrix Gateway 上配置两个 MDM 负载平衡器虚拟服务器（一个用于端口 443，一个用于端口 8443）。请将以下信息用作您的设置的模板。

> 重要：
>
> 以下更新仅适用于为 SSL 卸载配置的 Citrix Gateway。

1. 创建名为 `XMS_DropURLs` 的模式集。

```
add policy patset XMS_DropURLs
<!--NeedCopy-->
```

2. 将以下 URL 添加到新模式集。根据需要自定义此列表。

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6
```



```
2
3 bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5
4
5 bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4
6
7 bind policy patset XMS_DropURLs /zdm/log.jsp -index 3
8
9 bind policy patset XMS_DropURLs /zdm/login.jsp -index 2
10
11 bind policy patset XMS_DropURLs /zdm/console -index 1
12 <!--NeedCopy-->
```

3. 除非连接请求来自指定的子网，否则请创建一个策略以删除传输到这些 URL 的所有流量。

```
1 add responder policy XMS_DROP_pol  “CLIENT.IP.SRC.IN_SUBNET
     (192.168.0.0/24).NOT &&
2 HTTP.REQ.URL.CONTAINS_ANY(” XMS_DropURLs” )”  DROP -comment "Allow
     only subnet 192.168.0.0/24 to access these URLs. All other
     connections are DROPed"
3 <!--NeedCopy-->
```

4. 将新策略绑定到两个 MDM 负载平衡器虚拟服务器（端口 443 和 8443）。

```
1 bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
     XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
     REQUEST
2
3 bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
     XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
     REQUEST
4 <!--NeedCopy-->
```

域或域加安全令牌身份验证

March 2, 2021

XenMobile 支持对一个或多个（与轻型目录访问协议 (LDAP) 兼容的）目录执行基于域的身份验证。您可以在 XenMobile 中配置与一个或多个目录的连接，然后使用 LDAP 配置导入组、用户帐户和相关属性。

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

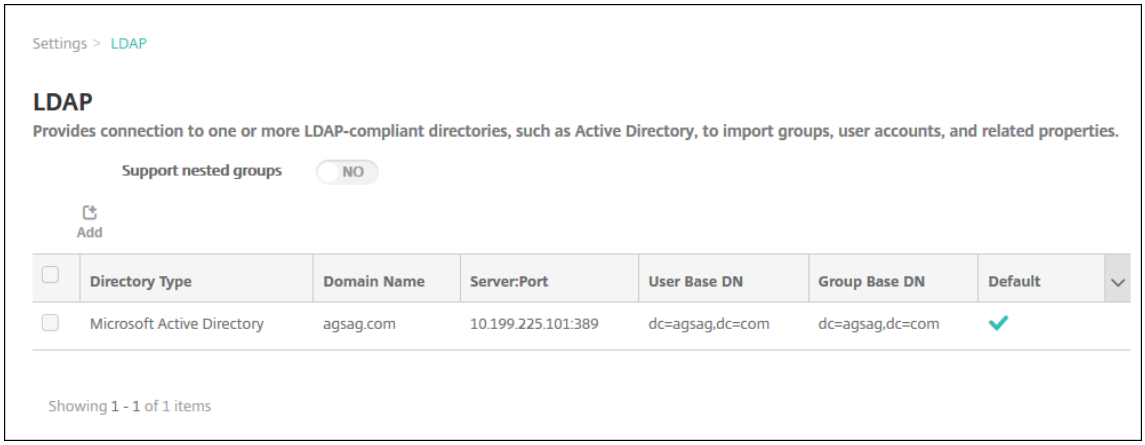
LDAP 的常见用处是为用户提供单点登录 (SSO)，即每个用户在多项服务之间共享一个密码。通过单点登录，用户登录一次公司 Web 站点，可对公司 Intranet 进行经过身份验证访问。

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

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

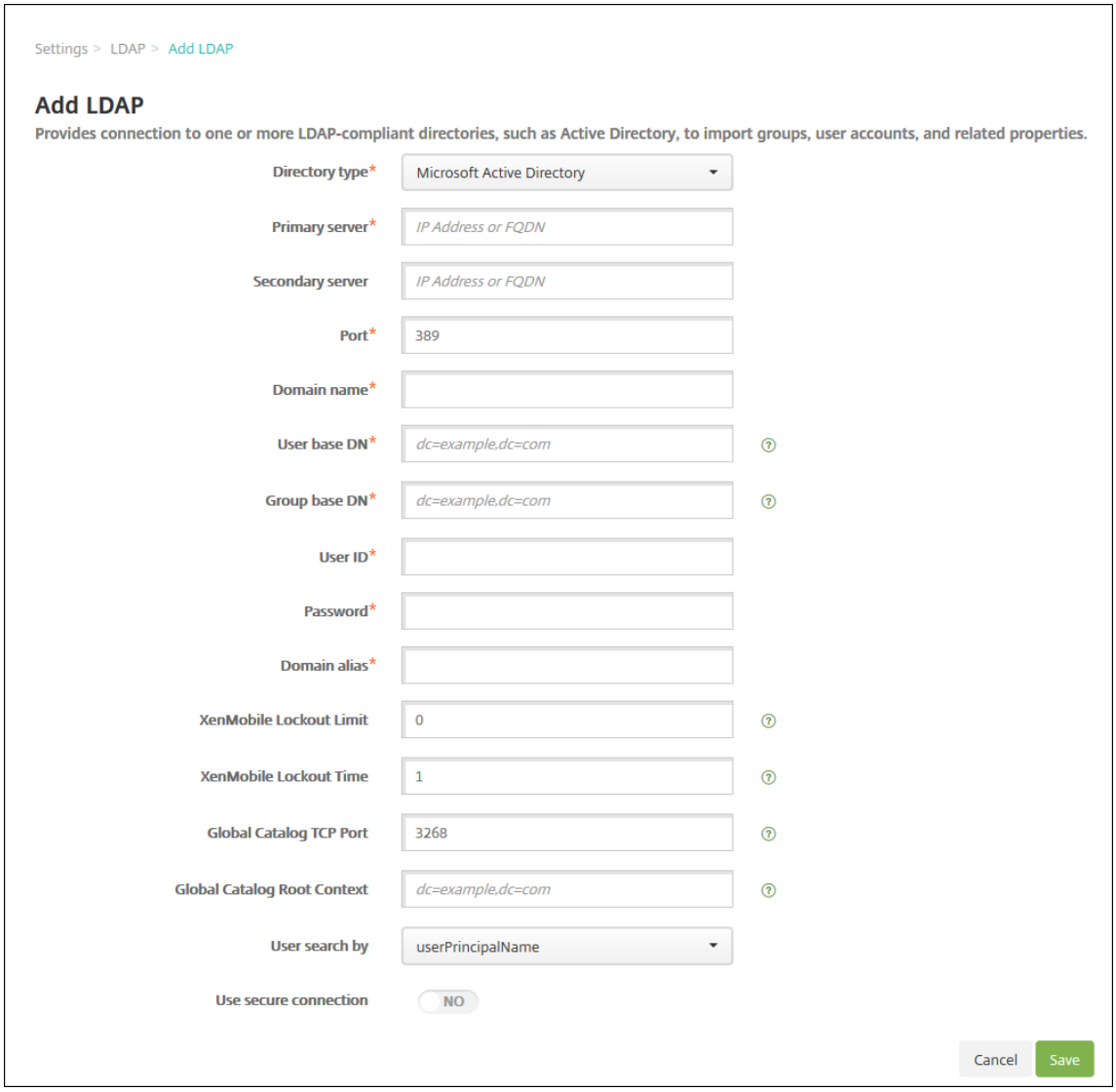
在 **XenMobile** 中添加 **LDAP** 连接

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **LDAP**。此时将显示 **LDAP** 页面。可以添加、编辑或删除 LDAP 兼容目录，如本文中所述。



添加 **LDAP** 兼容目录

1. 在 **LDAP** 页面上，单击添加。此时将显示添加 **LDAP** 页面。



2. 配置以下设置：

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

- 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。
- **XenMobile** 锁定限制：键入 **0** 到 **999** 之间的数字，表示失败登录尝试次数。值为 **0** 表示 XenMobile 从不根据失败登录尝试次数锁定用户。
- **XenMobile** 锁定时间：键入 **0** 到 **99999** 之间的数字，表示用户超过锁定限制后必须等待的分钟数。值为 **0** 表示不强制用户在锁定后等待。
- 全局目录 **TCP** 端口：键入全局目录服务器的 TCP 端口号。默认情况下，TCP 端口号设置为 **3268**；对于 SSL 连接，使用端口号 **3269**。
- 全局目录根上下文：（可选）键入用于在 Active Directory 中启用全局目录搜索的全局根上下文值。此搜索是除标准 LDAP 搜索之外的方法，可在任何域中使用，无需指定实际的域名。
- 用户搜索依据：在此列表中，单击 **userPrincipalName** 或 **sAMAccountName**。默认值为 **userPrincipalName**。如果在注册后通过设置更改用户搜索，用户必须重新注册。
- 使用安全连接：选择是否使用安全连接。默认值为否。

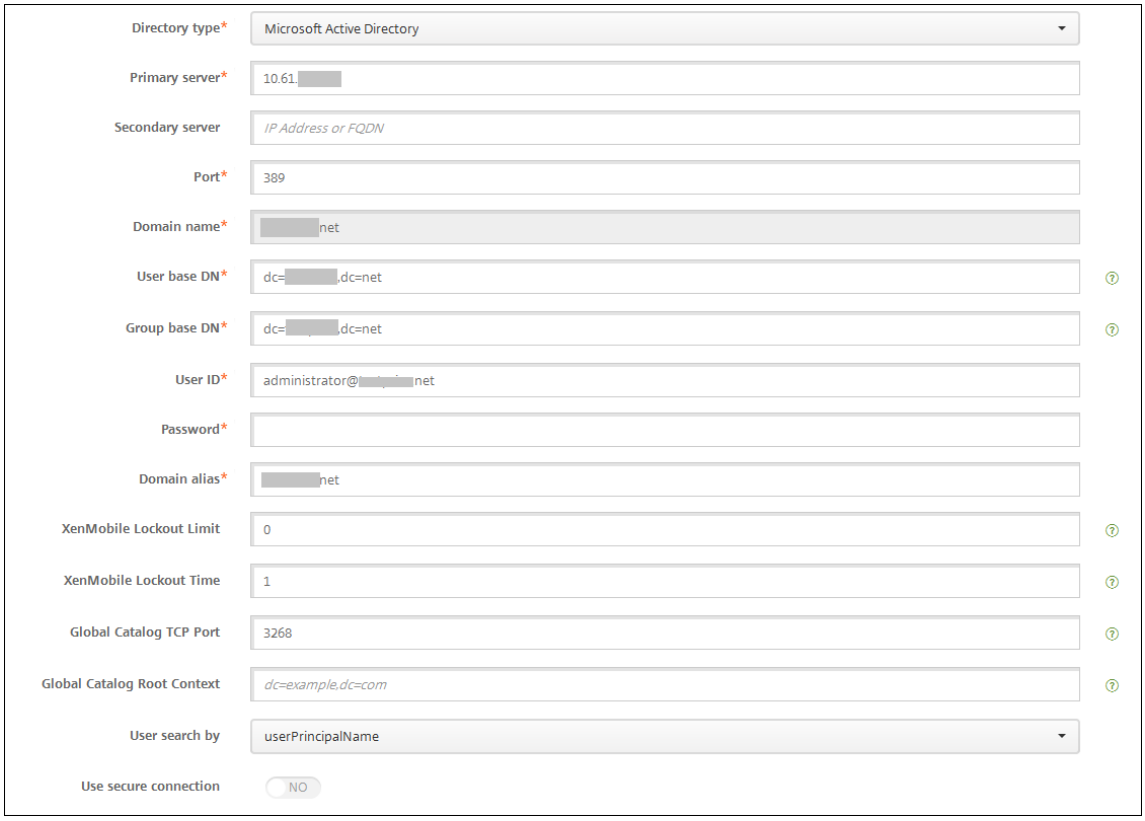
3. 单击保存。

编辑 **LDAP** 兼容目录

1. 在 **LDAP** 表中，选择要编辑的目录。

   选中某个目录旁边的复选框时，选项菜单将显示在 LDAP 列表上方。单击列表中的其他任意位置，选项菜单将显示在列表右侧。

2. 单击编辑。此时将显示编辑 **LDAP** 页面。



3. 适当更改以下信息：

- 目录类型：在列表中，单击相应的目录类型。
- 主服务器：键入用于 LDAP 的主服务器；可以输入 IP 地址或完全限定的域名 (FQDN)。
- 辅助服务器：（可选）键入辅助服务器的 IP 地址或 FQDN（如果配置了辅助服务器）。
- 端口：键入 LDAP 服务器使用的端口号。默认情况下，对于不安全的 LDAP 连接，端口号设置为 **389**。对安全的 LDAP 连接使用端口号 **636**，对 Microsoft 不安全 LDAP 连接使用 **3268**，或者对 Microsoft 安全 LDAP 连接使用 **3269**。
- 域名：无法更改此字段。
- 用户基础 **DN**：通过唯一标识符在 Active Directory 中键入用户的位置。语法示例包括：`ou=users`、`dc=example` 或 `dc=com`。
- 组基础 **DN**：键入组基础 DN 组名称，以 `cn=groupname` 的形式指定。例如，`cn=users`，`dc=servername`，`dc=net`，其中 `cn=users` 为组名称。`DN` 和 `servername` 表示运行 Active Directory 的服务器的名称。
- 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。
- **XenMobile** 锁定限制：键入 **0** 到 **999** 之间的数字，表示失败登录尝试次数。值为 **0** 表示 XenMobile 从不根据失败登录尝试次数锁定用户。
- **XenMobile** 锁定时间：键入 **0** 到 **99999** 之间的数字，表示用户超过锁定限制后必须等待的分钟数。值为 **0** 表示不强制用户在锁定后等待。

- 全局目录 **TCP** 端口：键入全局目录服务器的 TCP 端口号。默认情况下，TCP 端口号设置为 **3268**；对于 SSL 连接，使用端口号 **3269**。
- 全局目录根上下文：（可选）键入用于在 Active Directory 中启用全局目录搜索的全局根上下文值。此搜索是除标准 LDAP 搜索之外的方法，可在任何域中使用，无需指定实际的域名。
- 用户搜索依据：在此列表中，单击 **userPrincipalName** 或 **sAMAccountName**。如果在注册后通过设置更改用户搜索，用户必须重新注册。
- 使用安全连接：选择是否使用安全连接。

4. 单击保存以保存您所做更改，或单击取消保留属性不变。

删除 **LDAP** 兼容目录

1. 在 **LDAP** 表中，选择要删除的目录。

   可以通过选中每个属性旁边的复选框，选择多个要删除的属性。

2. 单击删除。此时将显示确认对话框。再次单击删除。

为多个域配置身份验证

要将 XenMobile Server 配置为在 LDAP 配置中使用多个域后缀，请参阅 Citrix Endpoint Management 文档为多个域配置身份验证中的过程。这些步骤在本地版本的 XenMobile Server 和 Endpoint Management 云版本中相同。

配置域加安全令牌身份验证

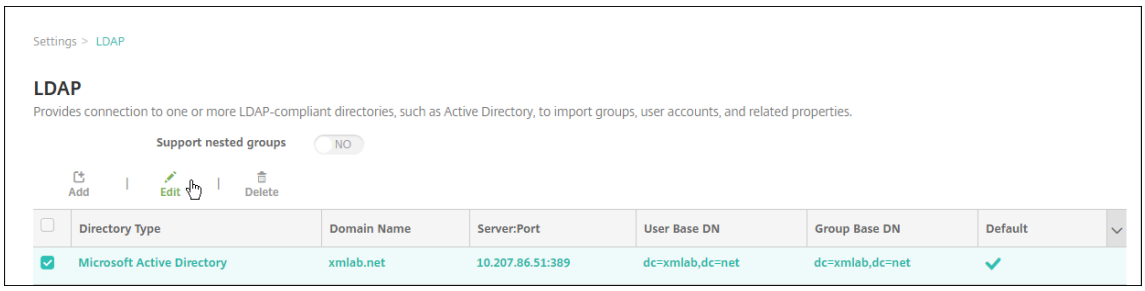
可以将 XenMobile 配置为要求用户通过 RADIUS 协议使用其 LDAP 凭据以及一次性密码进行身份验证。

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

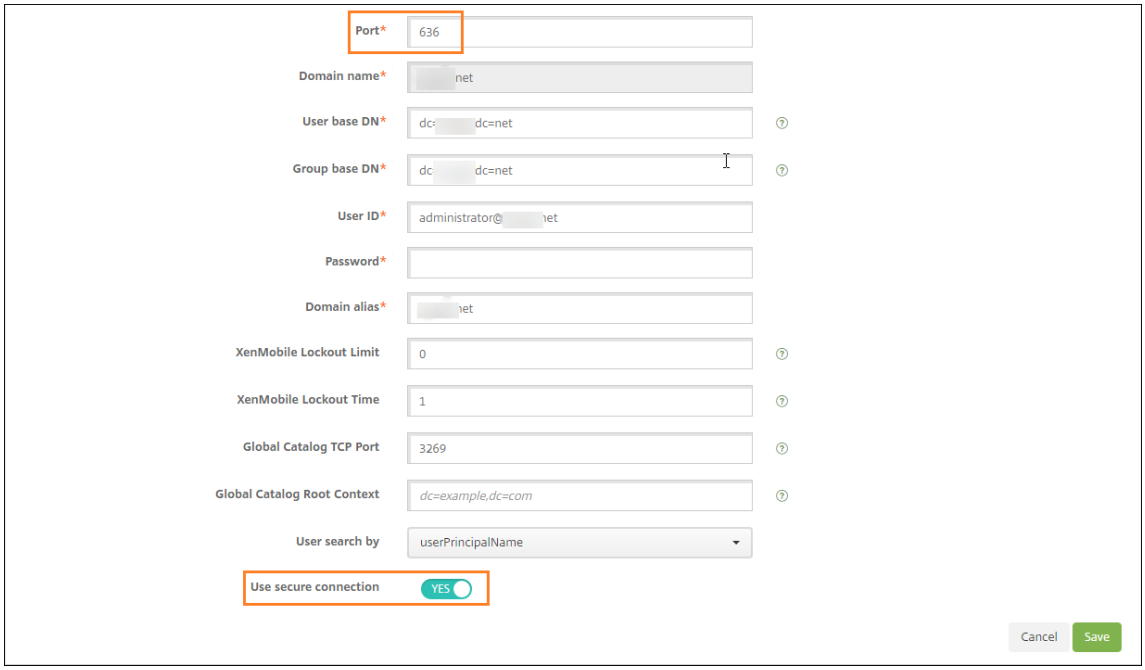
配置 **LDAP** 设置

使用 LDAP 进行身份验证要求您在 XenMobile 上安装证书颁发机构颁发的 SSL 证书。有关信息，请参阅在 XenMobile 中上载证书。

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



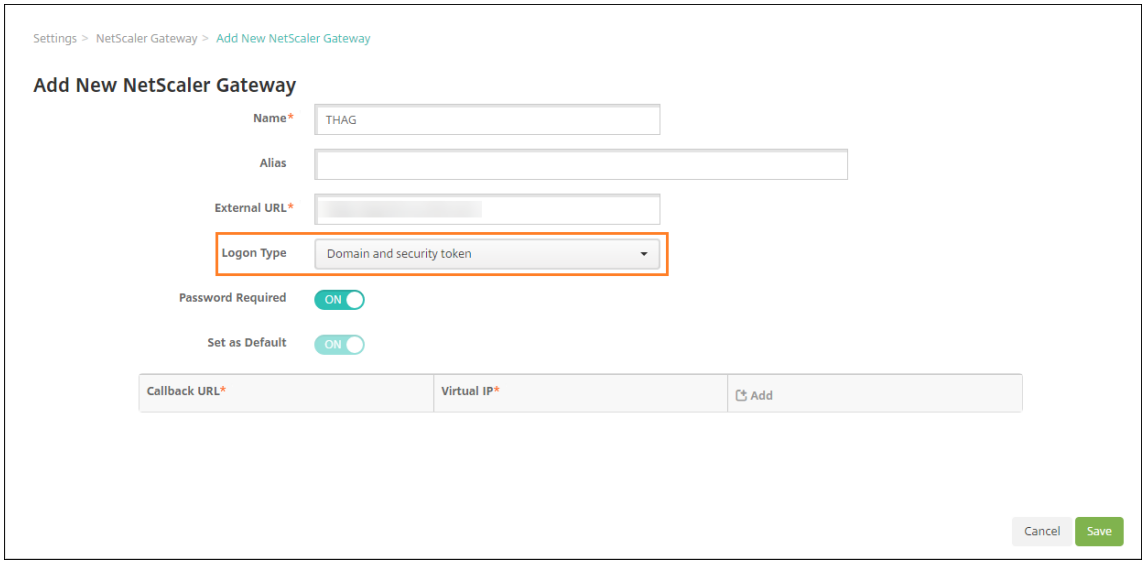
3. 确认“端口”为 **636**（用于安全 LDAP 连接）还是 **3269**（用于 Microsoft 安全 LDAP 连接）。
4. 将使用安全连接更改为是。



配置 **Citrix Gateway** 设置

以下步骤假定您已向 XenMobile 中添加 Citrix Gateway 实例。要添加 Citrix Gateway 实例，请参阅添加 Citrix Gateway 实例。

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



启用 **Citrix PIN** 和用户密码缓存

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

配置 **Citrix Gateway** 以进行域和安全令牌身份验证

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

客户端证书或证书加域身份验证

January 5, 2022

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

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

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

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

使用 Citrix ADC 仅证书身份验证或证书加域身份验证时，可以使用适用于 XenMobile 的 Citrix ADC 向导设置 XenMobile 所需的配置。只能运行一次适用于 XenMobile 的 Citrix ADC 向导。

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

客户端证书身份验证适用于 XenMobile MAM 模式（仅 MAM）和 ENT 模式（当用户注册到 MDM 时）。当用户注册到旧版 MAM 模式时，客户端证书身份验证不适用于 XenMobile ENT 模式。必须依次配置 Microsoft 服务器、XenMobile Server 和 Citrix Gateway，才能对 XenMobile ENT 和 MAM 模式使用客户端证书身份验证。执行本文所述的如下常规步骤。

在 Microsoft 服务器上：

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

在 XenMobile Server 上：

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

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

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

必备条件

- 创建 Microsoft 证书服务实体模板时，通过排除特殊字符来避免已注册的设备可能会出现的身份验证问题。例如，请勿在模板名称中使用以下字符：`: ! $ ()## % + * ~ ? | { } []`
- 对于使用证书身份验证和 SSL 卸载的 Windows Phone 8.1 设备，在 Citrix ADC 中的两个负载平衡虚拟服务器上对端口 443 禁用 SSL 会话重用。为此，请在虚拟服务器上对端口 443 运行以下命令：

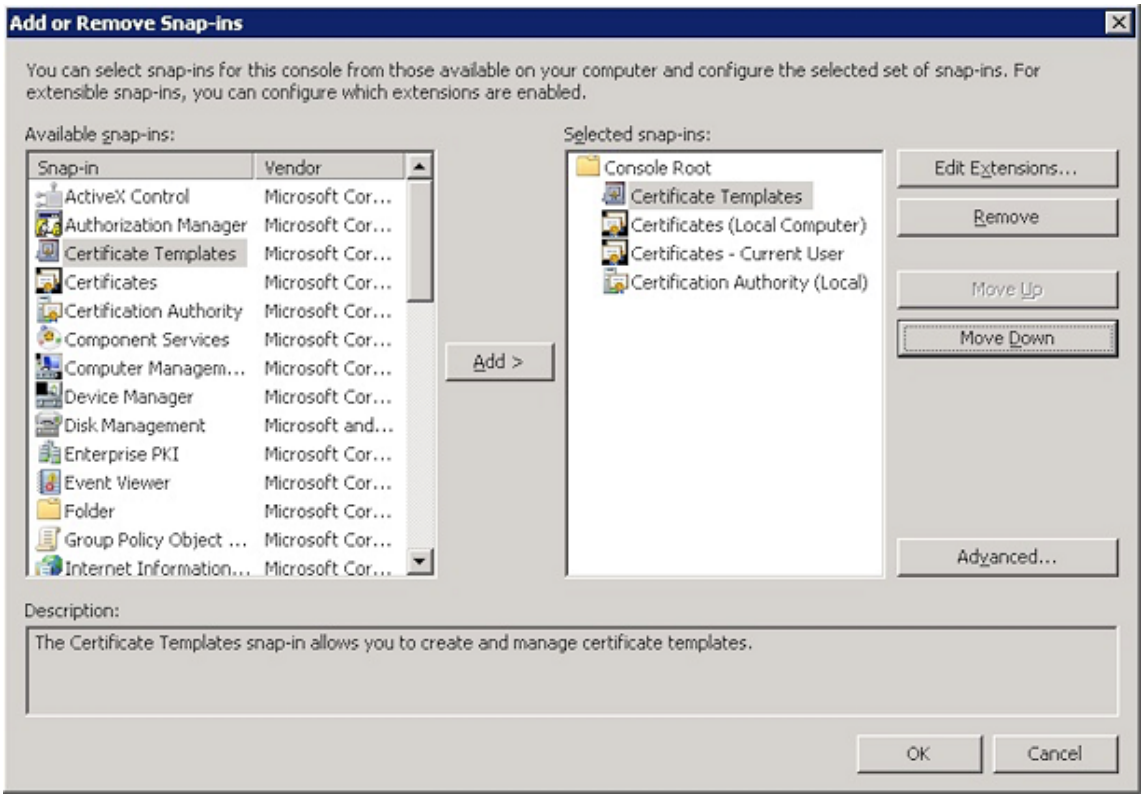
  ```
  set ssl vserver <ssl lb vserver> sessReuse DISABLE
  ```

  如果禁用 SSL 会话重用，还将禁用 Citrix ADC 提供的某些优化功能，这可能会导致 Citrix ADC 上的性能下降。

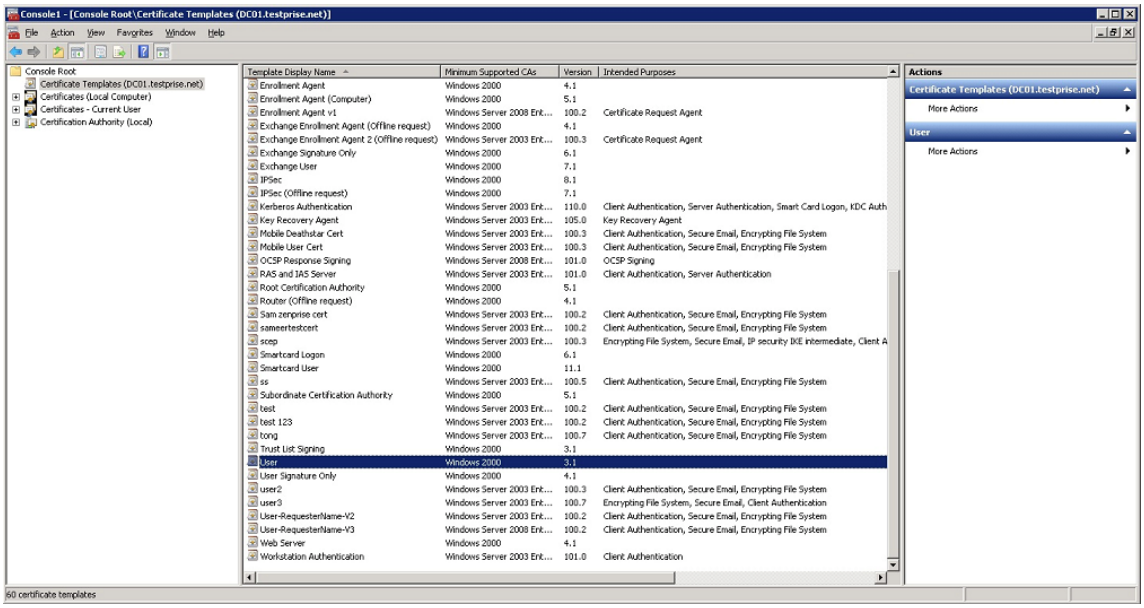
- 要为 Exchange ActiveSync 配置基于证书的身份验证，请参阅此 Microsoft 博客。为 Exchange ActiceSync 配置证书颁发机构 (CA) 服务器站点以要求客户端证书。
- 如果使用专用服务器证书来确保流向 Exchange Server 的 ActiveSync 流量安全，请确保移动设备具有所有必需的根证书/中间证书。否则，在 Secure Mail 中设置邮箱时，基于证书的身份验证将失败。在 Exchange IIS 控制台中，必须执行以下操作：
  - 添加一个 Web 站点以供 XenMobile 和 Exchange 使用，并绑定 Web 服务器证书。
  - 使用端口 9443。
  - 对于该 Web 站点，必须添加两个应用程序，一个用于 Microsoft-Server-ActiveSync，一个用于 EWS。对于这两个应用程序，请在 **SSL Settings**（SSL 设置）下方选择 **Require SSL**（需要 SSL）。

向 **Microsoft** 管理控制台添加证书管理单元

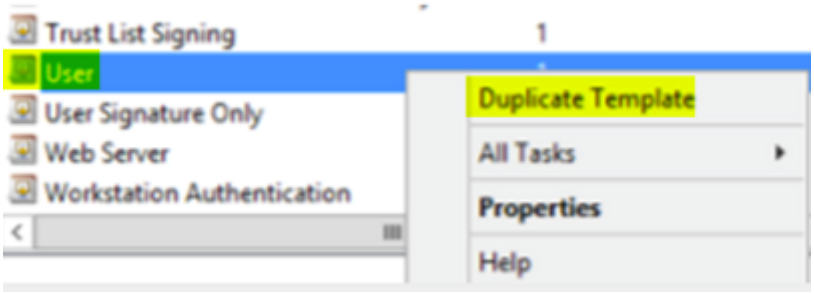
1. 打开该控制台，然后单击添加/删除管理单元。
2. 添加以下管理单元：
   - 证书模板
   - 证书 (本地计算机)
   - 证书 - 当前用户
   - 证书颁发机构 (本地)



3. 展开证书模板。



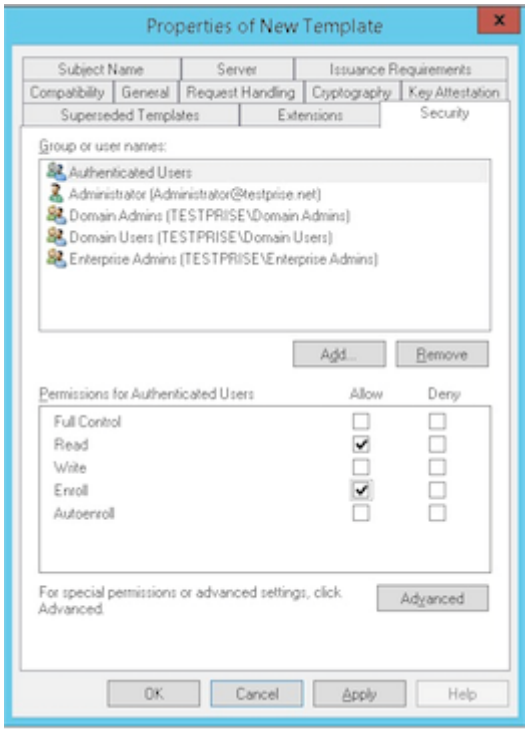
4. 依次选择用户模板和复制模板。



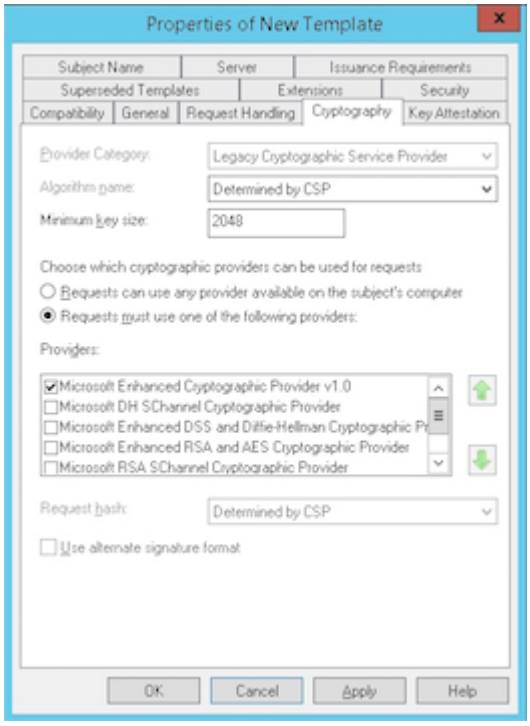
5. 提供模板显示名称。

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

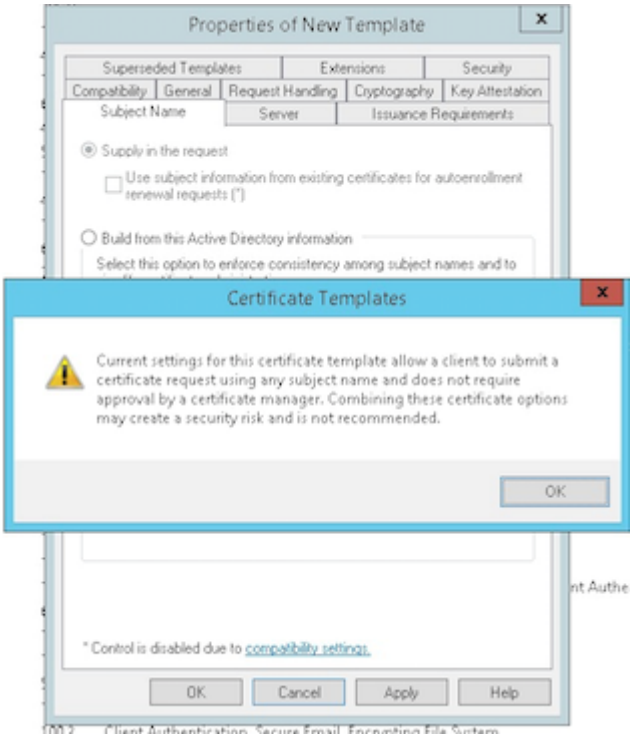
6. 选择 **Windows 2003 Server** 作为模板类型。在 Windows 2012 R2 Server 中，在兼容性下选择证书颁发机构，然后设置接受方 **Windows 2003**。
7. 在安全下方，针对已通过身份验证的用户在允许列中选择注册选项。



8. 在加密下方，务必提供密钥大小。以后可以在配置 XenMobile 时输入密钥大小。

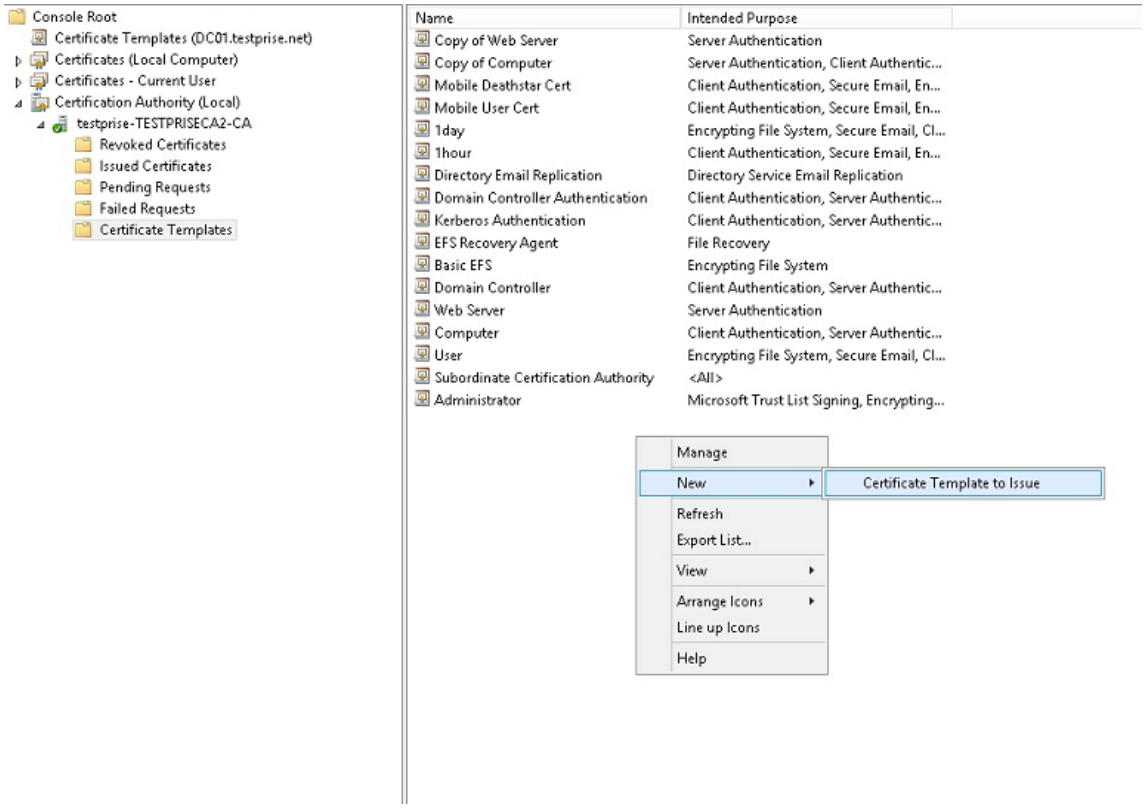


9. 在使用者名称下方，选择在请求中提供。应用更改并保存。

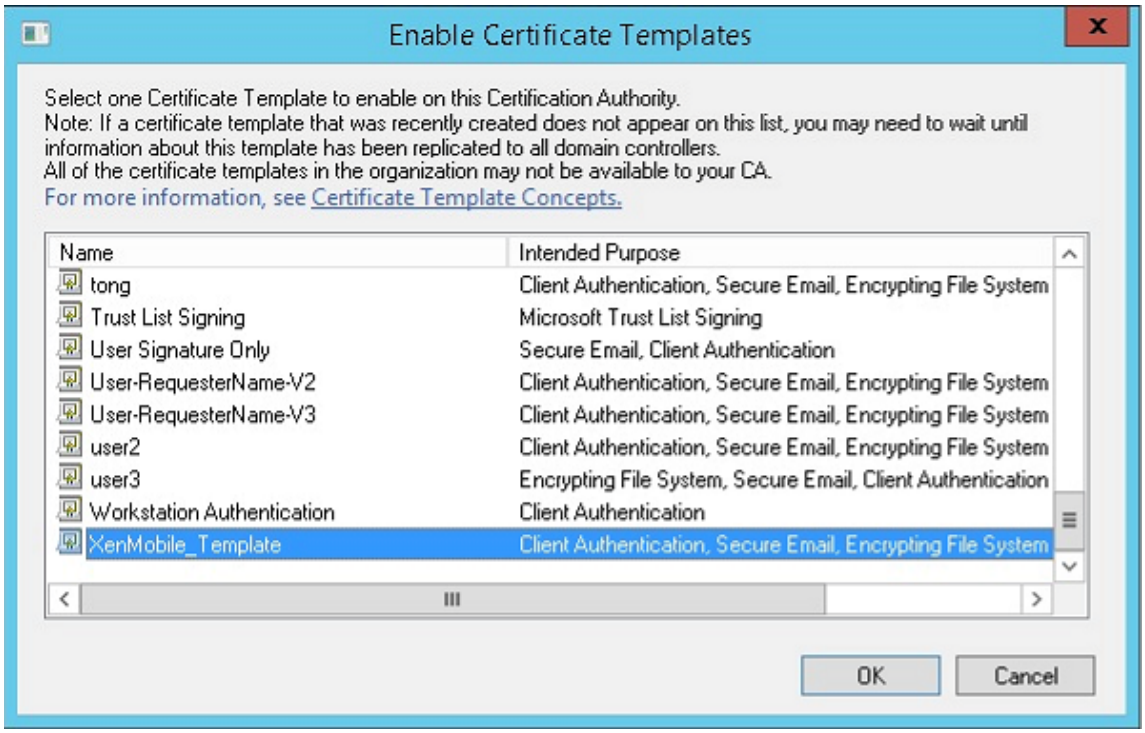


向证书颁发机构添加模板

1. 转至证书颁发机构并选择证书模板。
2. 在右侧窗格中单击鼠标右键，然后选择新建 **>** 要颁发的证书模板。

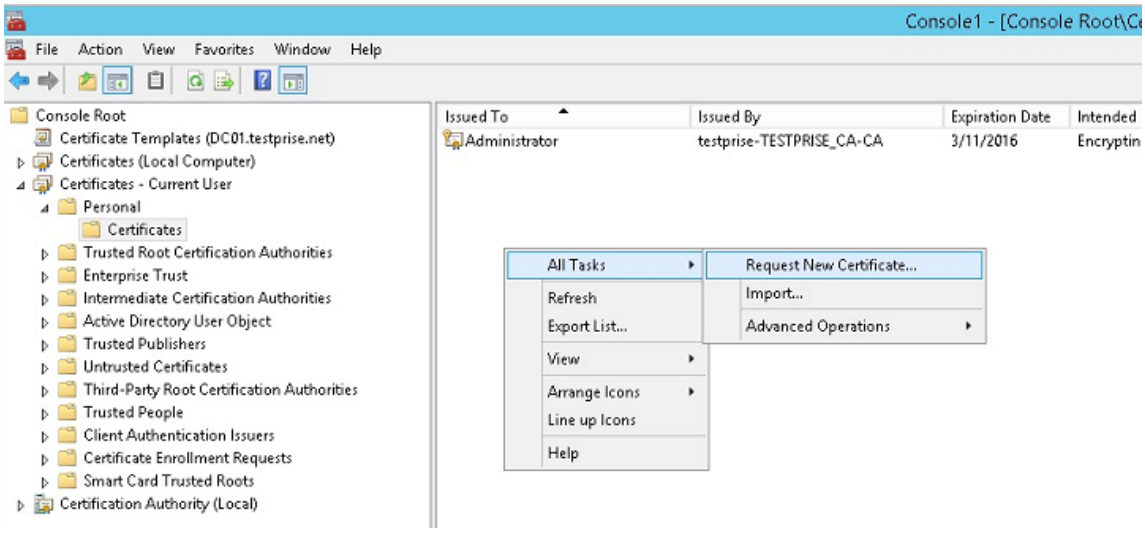


3. 选择在上一步中创建的模板，然后单击确定将其添加到证书颁发机构。

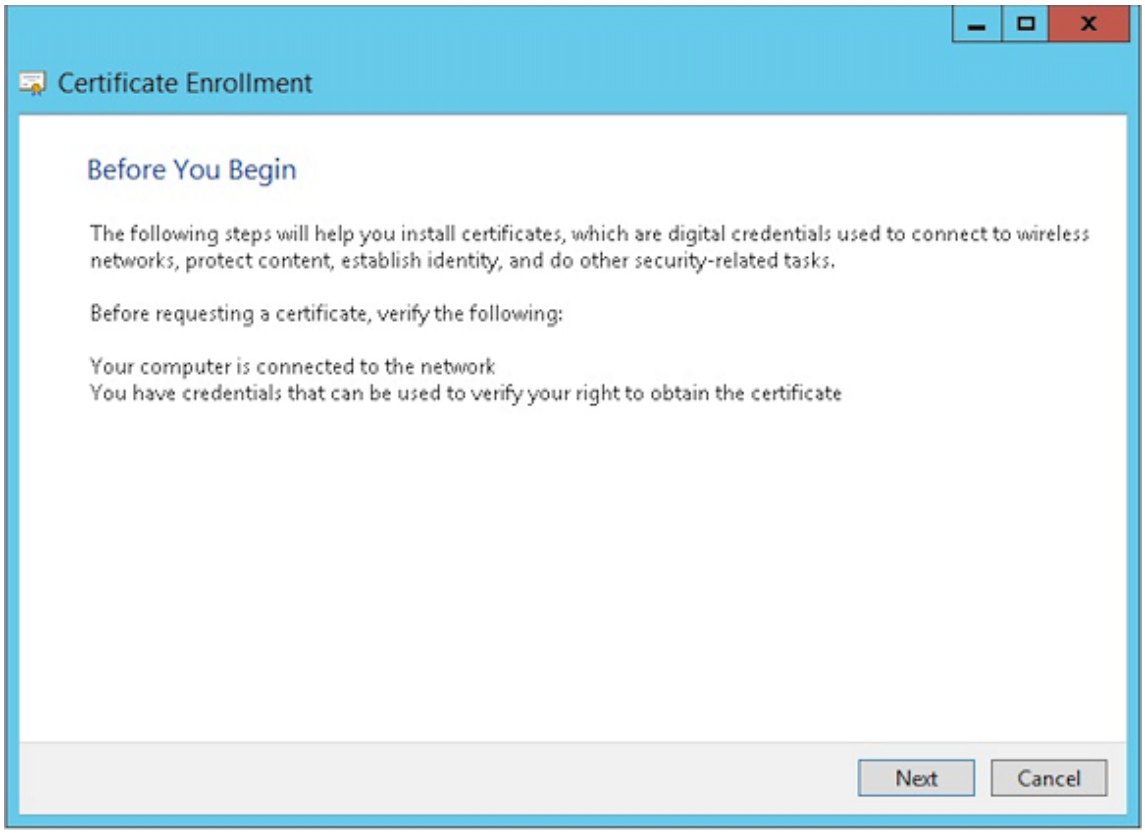


从 **CA** 服务器创建 **PFX** 证书

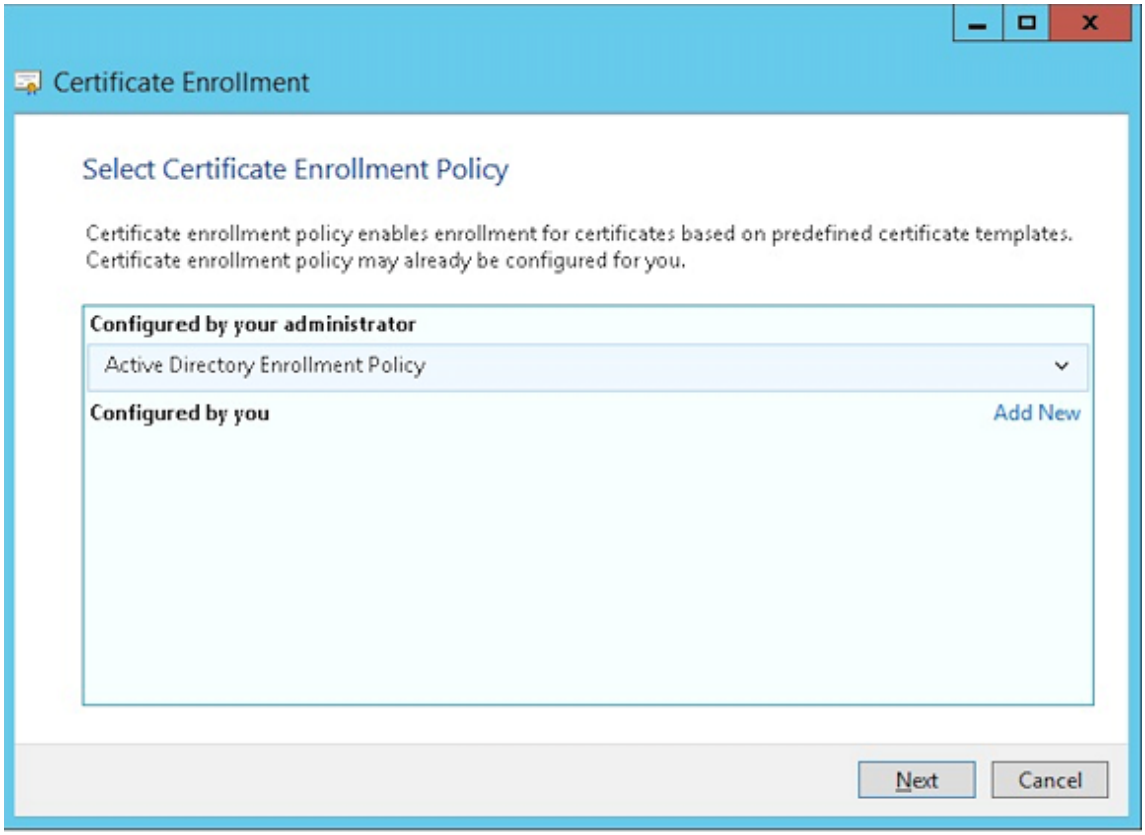
1. 使用登录时使用的服务帐户创建用户.pfx 证书。该.pfx 将上载到 XenMobile，之后 XenMobile 将代表注册其设备的用户申请用户证书。
2. 在当前用户下方，展开证书。
3. 在右侧窗格中单击鼠标右键，然后单击申请新证书。



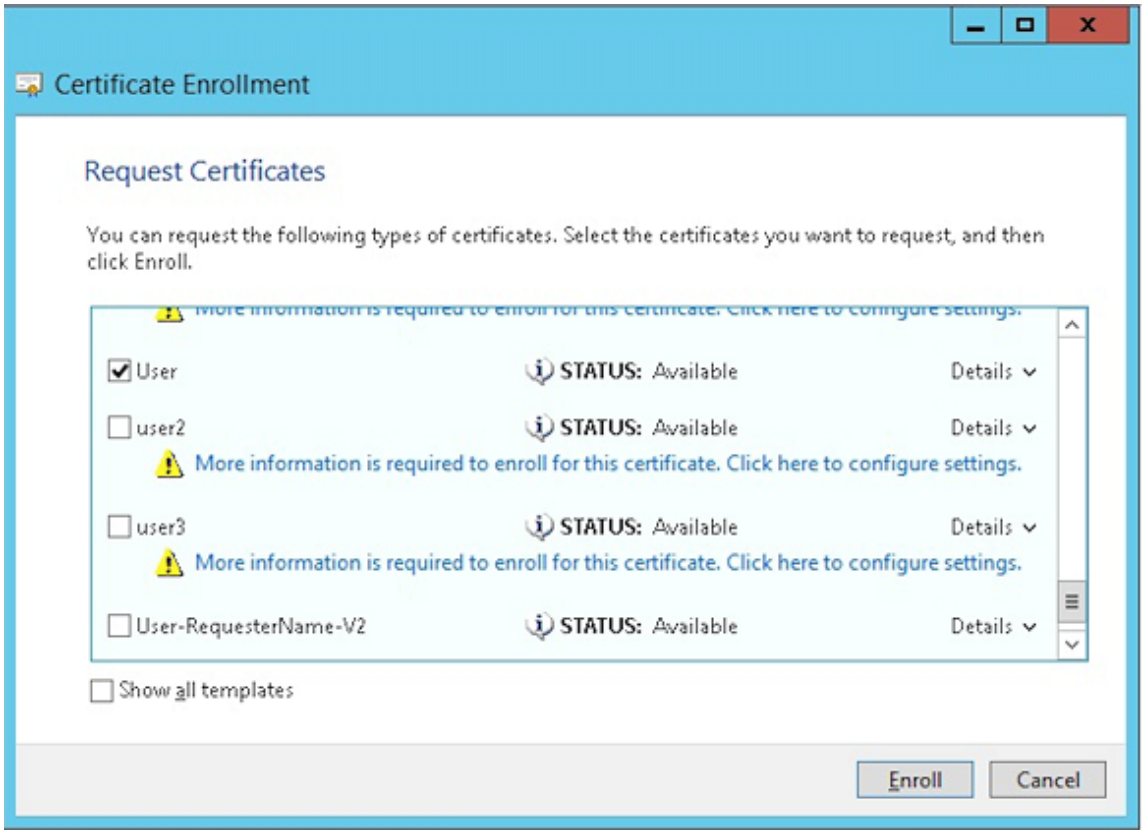
4. 此时将显示证书注册屏幕。单击 **Next**（下一步）。



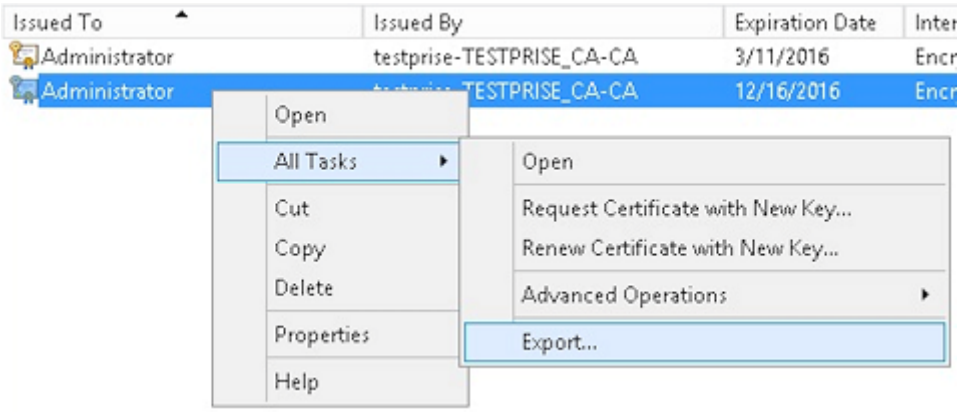
5. 选择 **Active Directory** 注册策略，然后单击下一步。



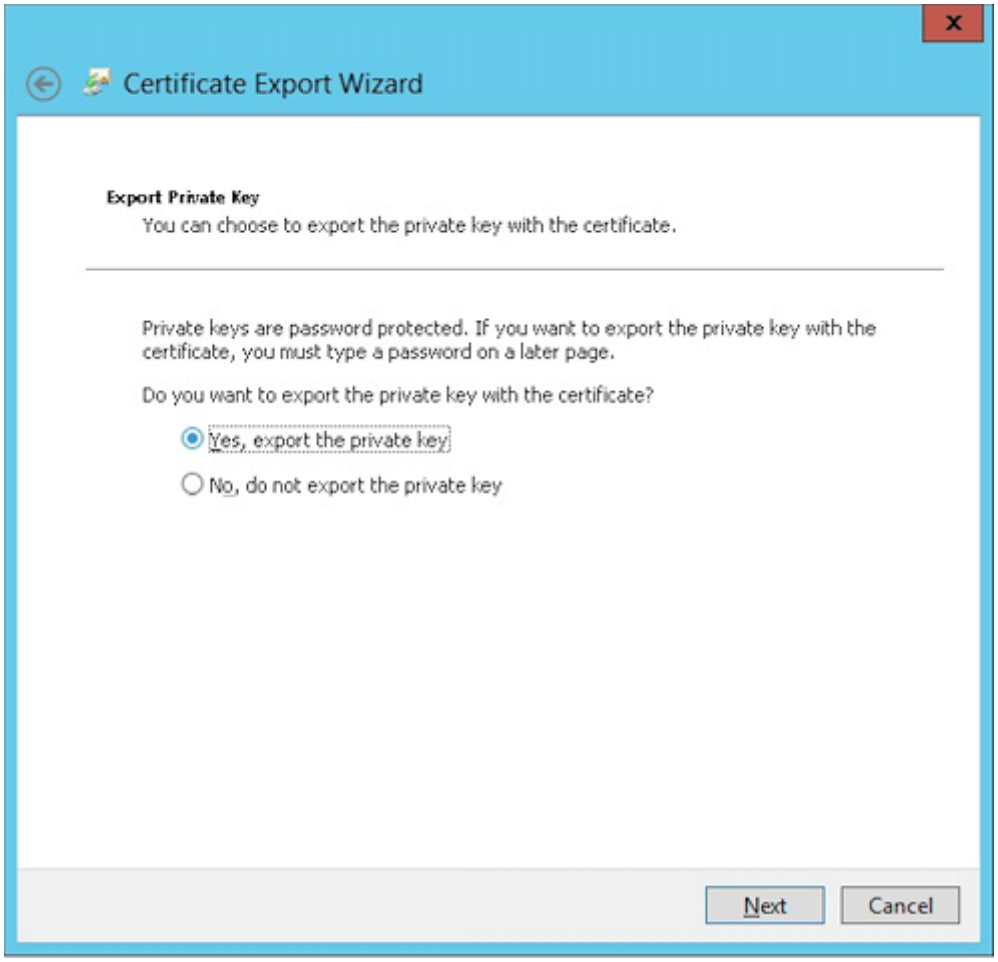
6. 选择用户模板，然后单击注册。



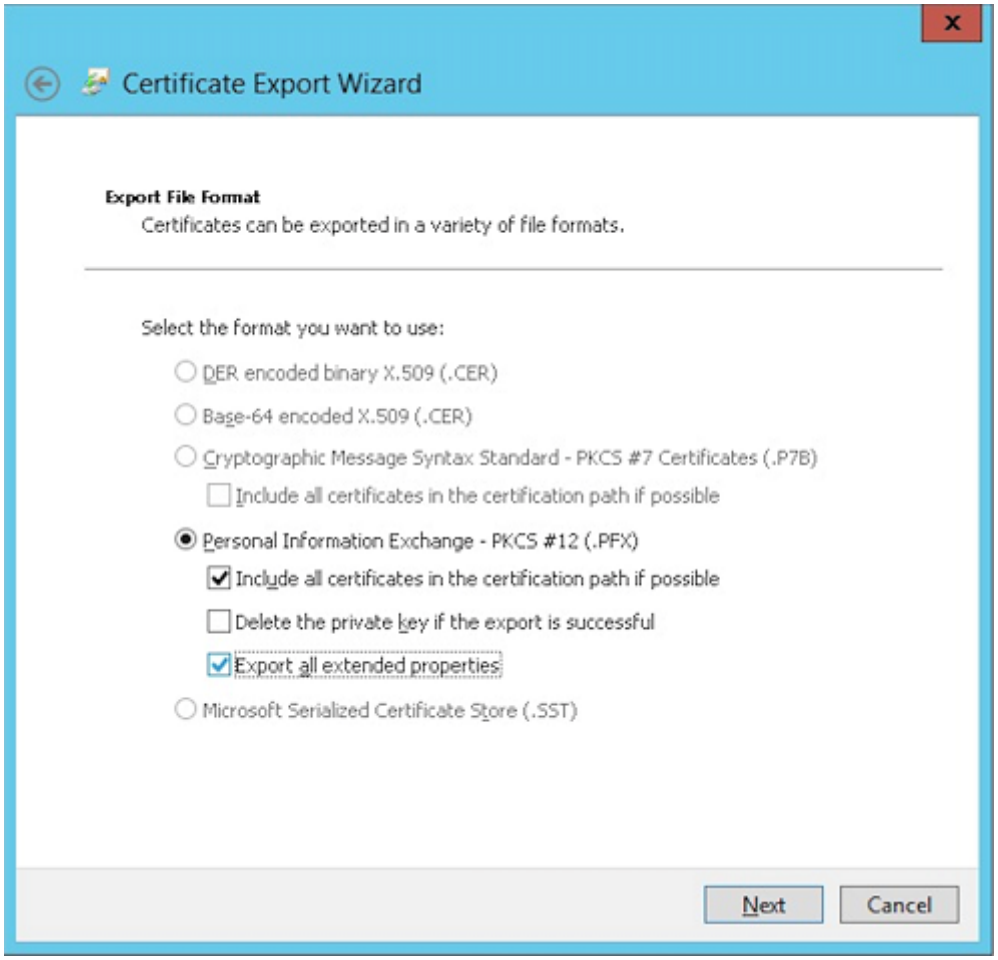
7. 导出在上一步中创建的.pfx 文件。



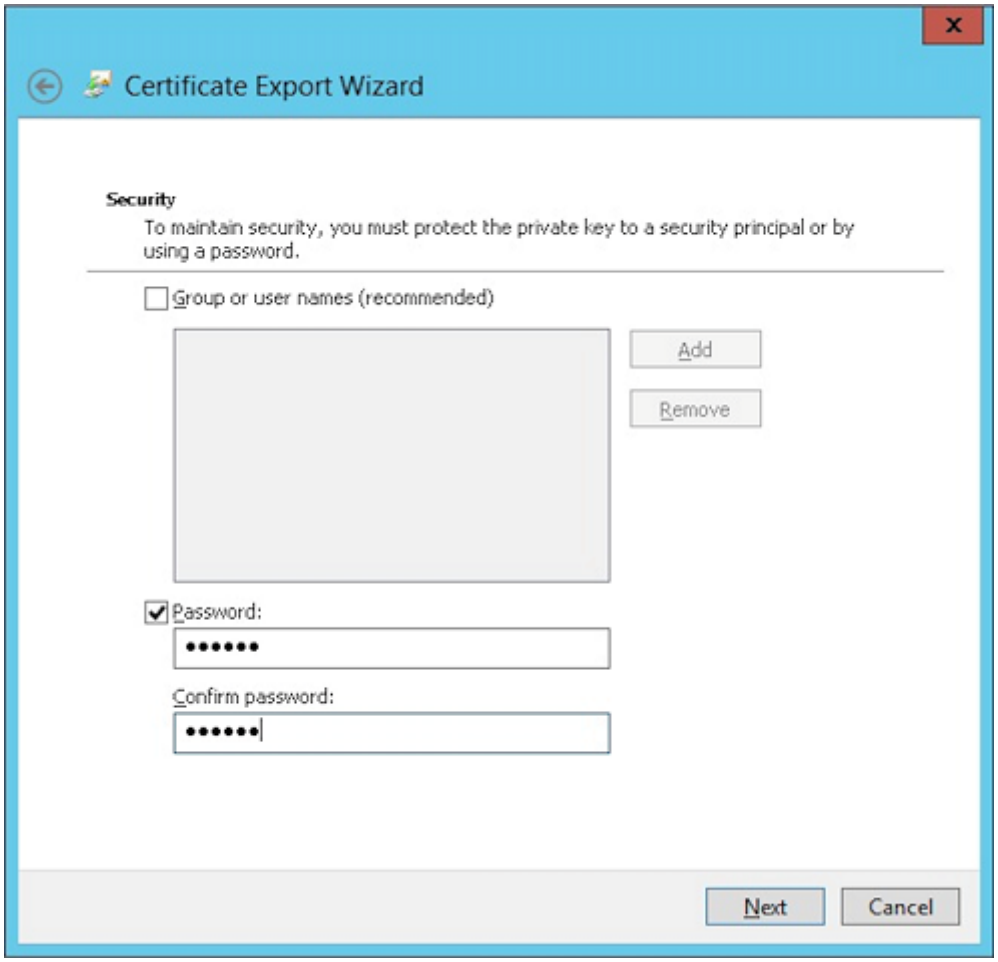
8. 单击是，导出私钥。



9. 选中如果可能，则包括证书路径中的所有证书和导出所有扩展属性复选框。



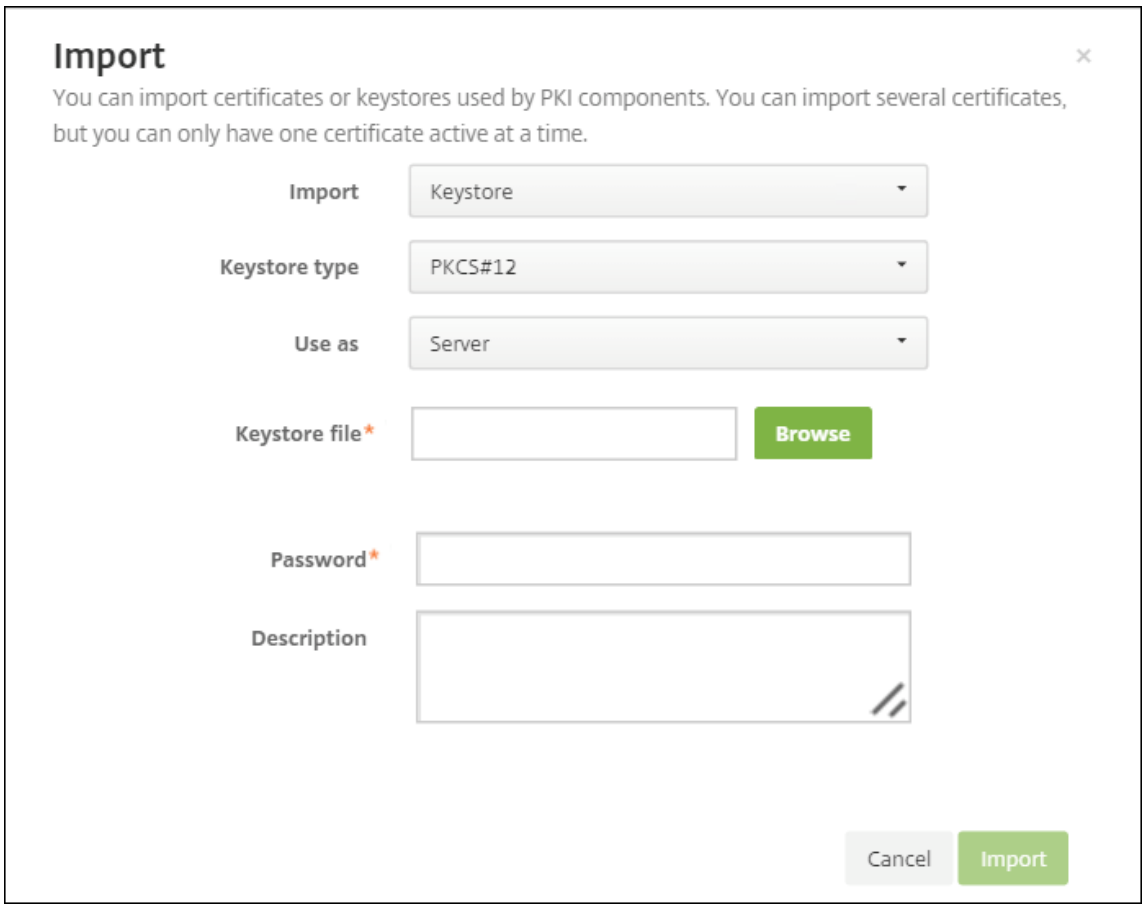
10. 设置在将此证书上载到 XenMobile 中时要使用的密码。



11. 将证书保存到您的硬盘驱动器。

将证书上载到 **XenMobile**

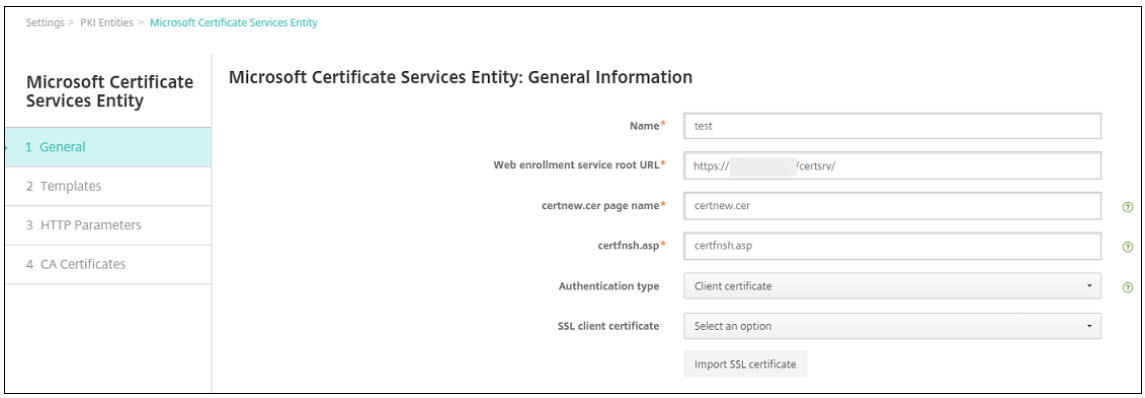
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置屏幕。
2. 依次单击证书和导入。
3. 输入以下参数：
   - 导入：密钥库
   - 密钥库类型： PKCS #12
   - 用作：服务器
   - 密钥库文件：单击浏览选择创建的 `.pfx` 证书。
   - 密码：输入为此证书创建的密码。



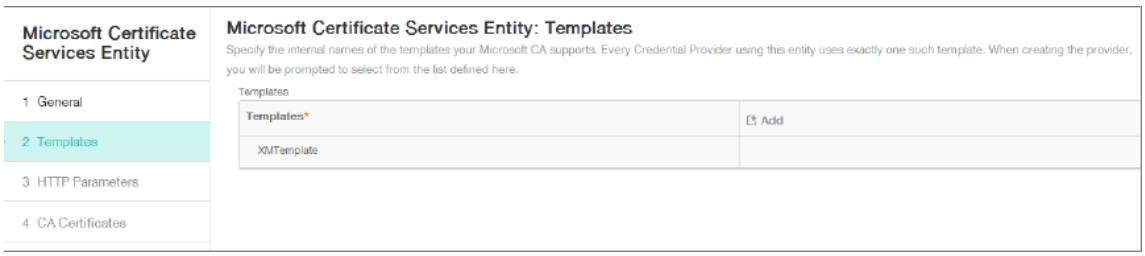
4. 单击导入。
5. 验证是否已正确安装证书。正确安装的证书将显示为用户证书。

为基于证书的身份验证创建 **PKI** 实体

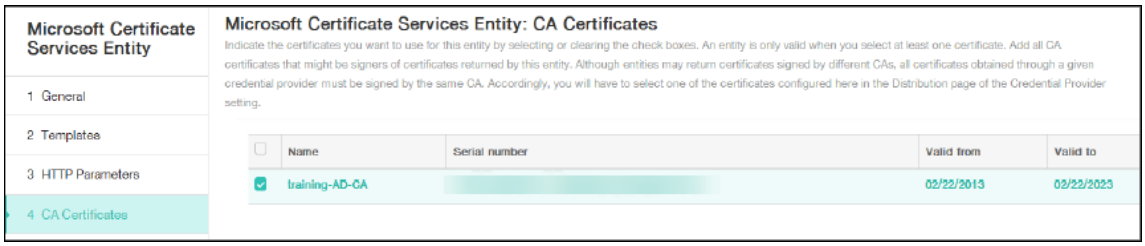
1. 在设置中，转至更多 **>** 证书管理 **> PKI** 实体。
2. 依次单击添加和 **Microsoft** 证书服务实体。此时将显示 **Microsoft** 证书服务实体**:** 常规信息屏幕。
3. 输入以下参数：
   - 名称：键入任意名称
   - **Web** 注册服务根 **URL**： `https://RootCA-URL/certsrv/` （请务必在 URL 路径结尾添加一个斜杠 /。）
   - **certnew.cer** 页面名称： certnew.cer（默认值）
   - **certfnsh.asp**： certfnsh.asp（默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



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



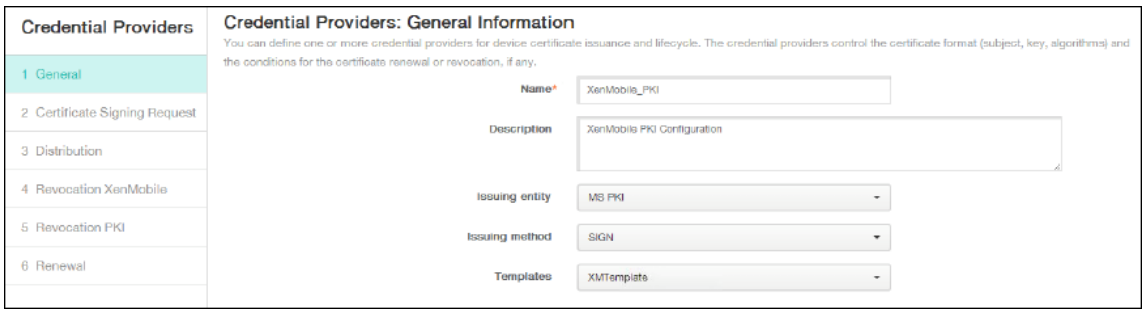
5. 跳过“HTTP 参数”，然后单击 **CA** 证书。
6. 选择与您的环境对应的根 CA 名称。此根 CA 属于从 XenMobile 客户端证书中导入的链的一部分。



7. 单击保存。

配置凭据提供程序

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



4. 单击证书签名请求，然后输入以下参数：

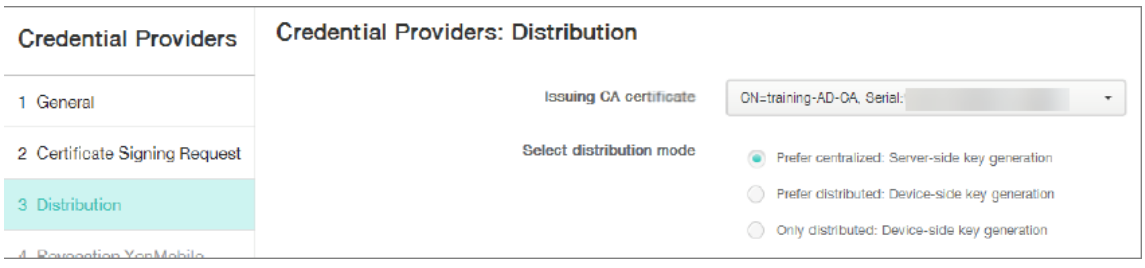
   - 密钥算法： RSA
   - 密钥大小： 2048
   - 签名算法： SHA256withRSA
   - 使用者名称： `cn=$user.username`

   对于使用者备用名称，请单击添加，然后输入以下参数：

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

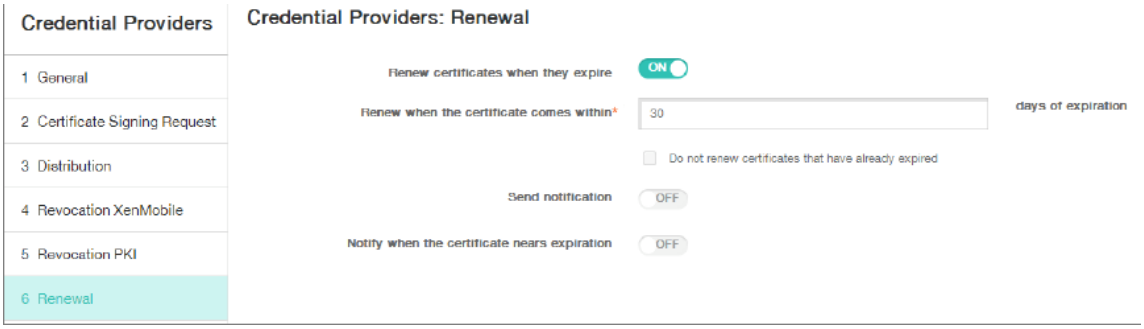
5. 单击分发并输入以下参数：

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



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

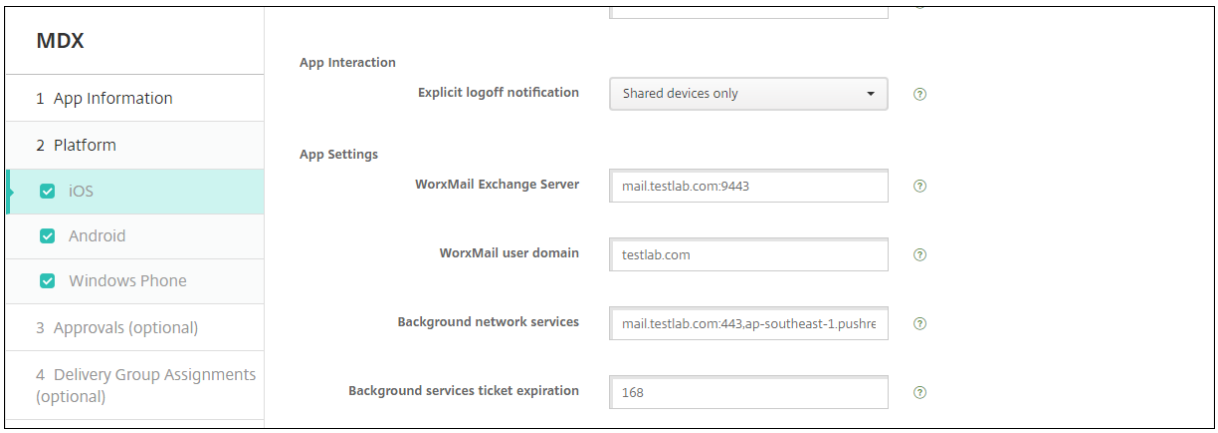
8. 对于在证书过期时续订，选择开。
9. 让所有其他设置保留为默认设置，或者根据需要进行更改。



10. 单击保存。

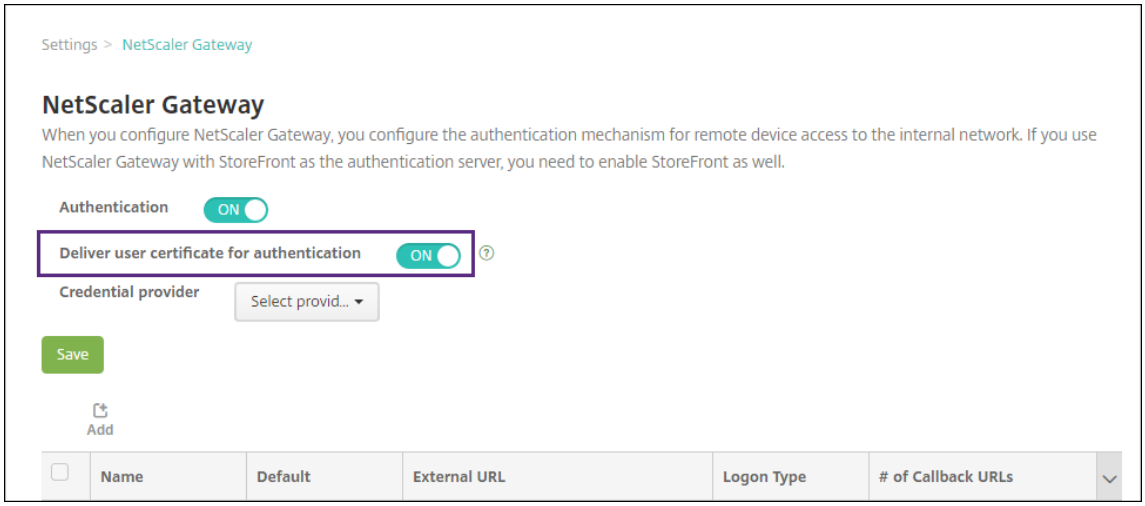
将 **Secure Mail** 配置为使用基于证书的身份验证

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

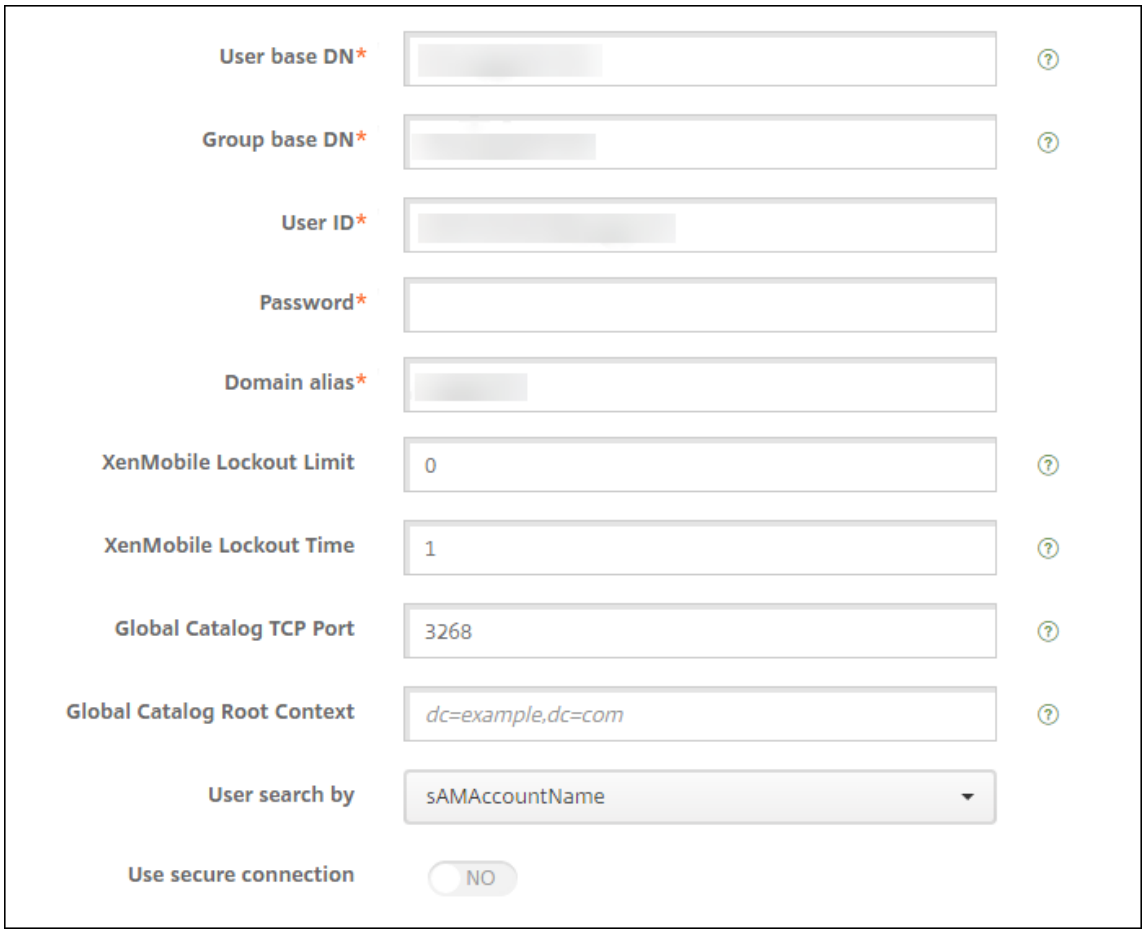


在 **XenMobile** 中配置 **Citrix ADC** 证书交付

1. 登录到 XenMobile 控制台并单击右上角的齿轮图标。此时将显示设置屏幕。
2. 在服务器下方，单击 **Citrix Gateway**。
3. 如果尚未添加 Citrix Gateway，请单击添加并指定以下设置：
   - 外部 **URL**： `https://YourCitrixGatewayURL`
   - 登录类型：证书和域
   - 需要密码：关
   - 设为默认值：开
4. 对于向用户提供用于身份验证的证书，选择开。



5. 对于凭据提供程序，选择一个提供程序，然后单击保存。
6. 要使用用户证书中的 sAMAccount 属性作为用户主体名称 (UPN) 的备用名称，请按如下所示在 XenMobile 中配置 LDAP 连接器：转至设置 **> LDAP**，选择目录并单击编辑，然后在用户搜索依据中选择 **sAMAccountName**。



启用 **Citrix PIN** 和用户密码缓存

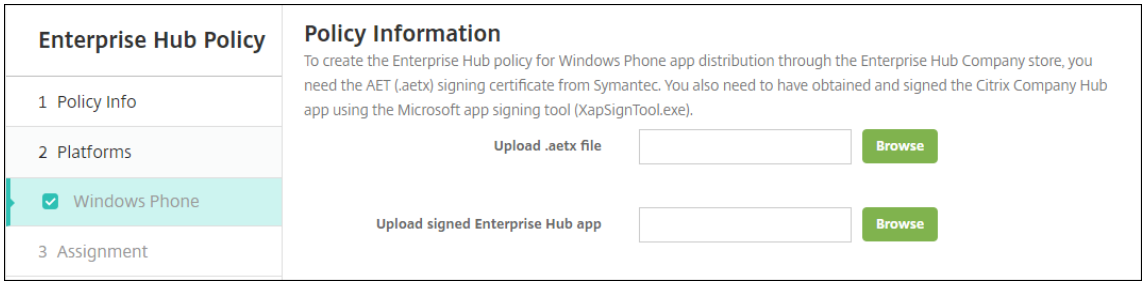
要启用 Citrix PIN 和用户密码缓存，请转至设置 **>** 客户端属性，然后选中这些复选框：启用 **Citrix PIN** 身份验证和启用用户密码缓存。有关详细信息，请参阅客户端属性。

为 **Windows Phone** 创建企业中心策略

对于 Windows Phone 设备，必须创建企业中心设备策略才能交付 AETX 文件和 Secure Hub 客户端。

> 注意：
>
> 请确保 AETX 和 Secure Hub 文件都使用：
>
> - 证书提供程序提供的相同企业证书。
> - 来自 Windows 应用商店开发人员帐户的相同发布者 ID。

1. 在 XenMobile 控制台中，单击配置 **>** 设备策略。
2. 单击添加，然后在更多 **> XenMobile Agent** 下方单击企业中心。
3. 命名该策略后，请务必为企业中心选择正确的 **.**AETX 文件和签名 Secure Hub 应用程序。



4. 将该策略分配给交付组并保存。

客户端证书配置故障排除

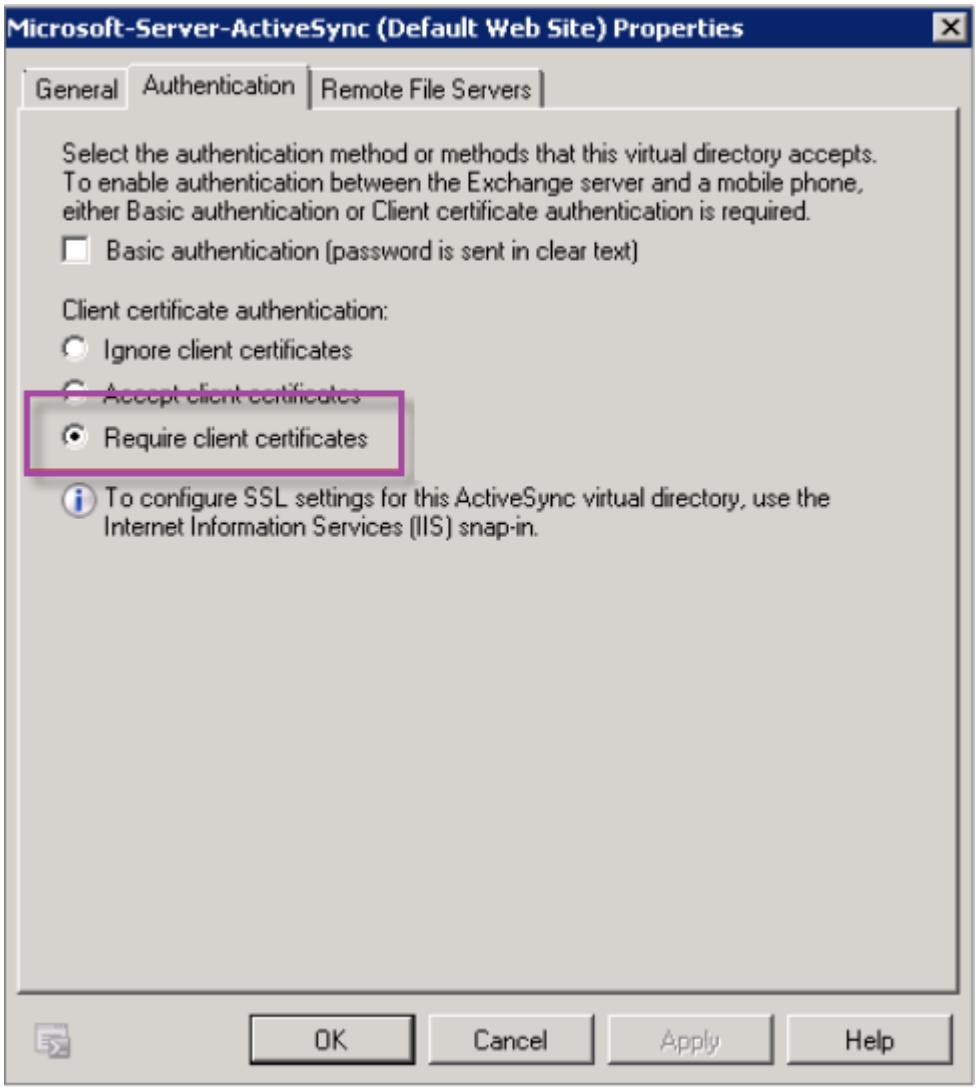
成功配置前述配置及 Citrix Gateway 配置后，用户工作流如下：

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

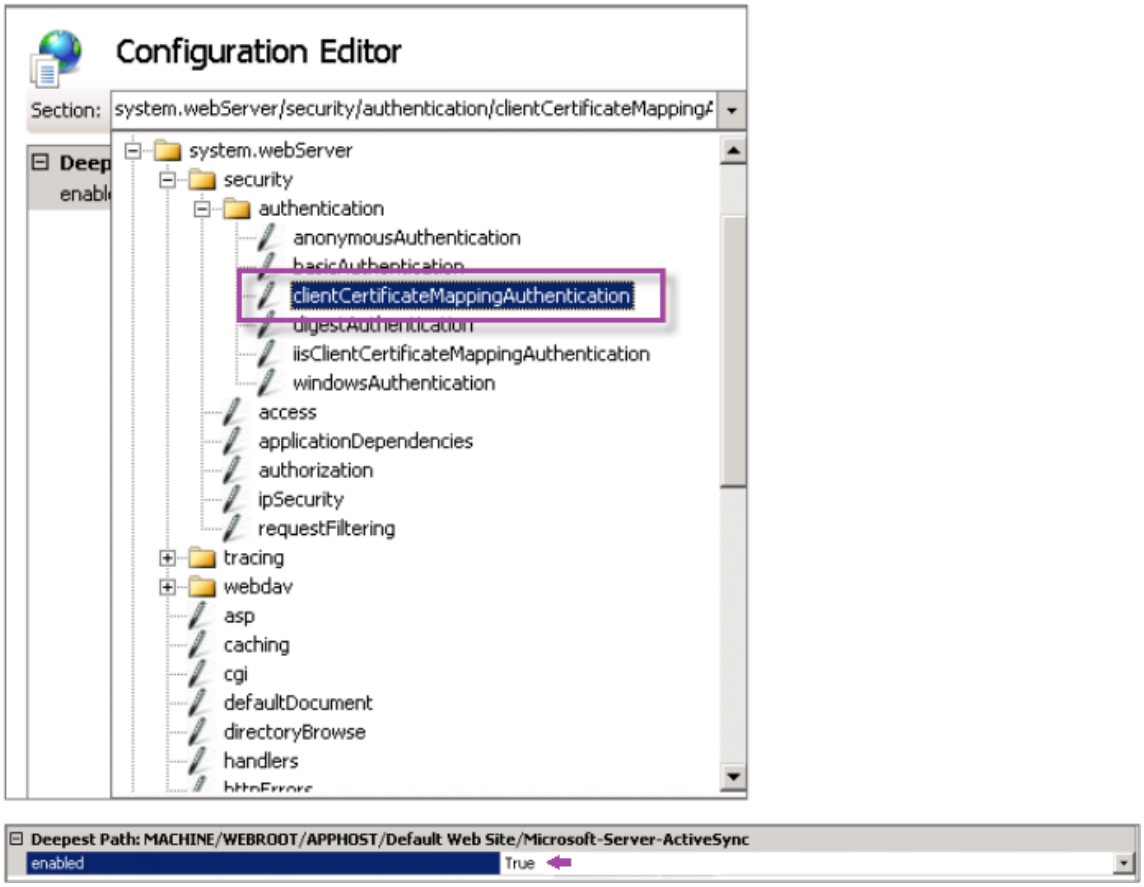
如果用户能够下载并安装 Secure Mail，但邮箱配置过程中 Secure Mail 无法完成配置：

1. 如果 Microsoft Exchange Server ActiveSync 使用专用 SSL 服务器证书来确保流量安全，请验证是否已在移动设备上安装根证书/中间证书。

2. 验证为 ActiveSync 选择的身份验证类型是否为要求提供客户端证书。



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



选择 **True** 后，请务必单击应用以使更改生效。

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

确定是否已向移动设备提供客户端证书

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

   Citrix Gateway Credentials: Requested credential, CertId=

验证是否已启用客户端证书协商

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

   ```
   netsh http show sslcert
   ```

2. 如果 **Negotiate Client Certificate**（协商客户端证书）的值为 **Disabled**（已禁用），请运行以下命令将其启用：


```
netsh http delete sslcert ipport=0.0.0.0:443

netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={
 app_id } certstorename=store_name verifyclientcertrevocation=Enable
 VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable
clientcertnegotiation=Enable
```

例如：

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c54
 appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam
 verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

如果无法通过 XenMobile 向 Windows Phone 8.1 设备提供根证书/中间证书，请执行以下操作：

- 通过电子邮件将根证书/中间证书 (.cer) 文件发送到 Windows Phone 8.1 设备并直接安装。

如果无法在 Windows Phone 8.1 上成功安装 Secure Mail，请验证以下项：

- 应用程序注册令牌（.AETX 文件）是否已使用企业中心设备策略通过 XenMobile 提供。
- 创建应用程序注册令牌时使用的证书提供程序提供的企业证书是否与用于封装 Secure Mail 并为 Secure Hub 应用程序签名的企业证书相同。
- 是否使用相同的发布者 ID 签名并封装 Secure Hub、Secure Mail 和应用程序注册令牌。

PKI 实体

January 5, 2022

XenMobile 公钥基础结构 (PKI) 实体配置代表执行实际 PKI 操作（颁发、吊销和状态信息）的组件。这些组件是 XenMobile 的内部组件或外部组件。内部组件称为自主组件。外部组件属于企业基础结构的组成部分。

XenMobile 支持以下类型的 PKI 实体：

- 通用 PKI (GPKI)

  XenMobile Server GPKI 支持包括 DigiCert 托管 PKI。

- Microsoft 证书服务
- 任意证书颁发机构 (CA)

XenMobile 支持以下 CA 服务器：

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

常见 **PKI** 概念

无论何种类型，每个 PKI 实体均拥有下列功能的子集：

- 签名：基于证书签名请求 (CSR) 颁发新证书。
- 提取：恢复现有证书和密钥对。
- 吊销：吊销客户端证书。

关于 **CA** 证书

配置 PKI 实体时，请向 XenMobile 指明哪个 CA 证书将成为该实体所颁发（或从该实体恢复）的证书的签署者。该 PKI 实体可以返回任意多个不同 CA 签名（提取或新签名）的证书。

请在 PKI 实体配置过程中提供其中每个 CA 的证书。为此，请将证书上载到 XenMobile，然后在 PKI 实体中引用这些证书。对于任意 CA，证书实际上是签名 CA 证书。对于外部实体，必须手动指定该证书。

> 重要：
>
> 创建 Microsoft 证书服务实体模板时，为避免已注册的设备可能会出现的身份验证问题：请勿在模板名称中使用特殊字符。例如，请勿使用：`! : $ ( )## % + * ~ ? | { } [ ]`

通用 **PKI**

通用 PKI (GPKI) 协议是 XenMobile 专有协议，在 SOAP Web 服务层之上运行，用于实现与各种 PKI 解决方案的统一交互。GPKI 协议定义以下三个基本 PKI 操作：

- 签名：适配器可以接收 CSR，将其传输到 PKI 并返回新签名的证书。
- 提取：适配器能够从 PKI 检索（恢复）现有证书和密钥对（取决于输入参数）。
- 吊销：适配器会导致 PKI 吊销给定证书。

GPKI 协议的接收端是 GPKI 适配器。该适配器将基本操作转换为其构建所针对的特定类型的 PKI。例如，存在适用于 RSA 和 Entrust 的 GPKI 适配器。

作为 SOAP Web 服务端点，GPKI 适配器可发布自我描述的 Web 服务描述语言 (WSDL) 定义。创建 GPKI PKI 实体相当于通过 URL 或上载文件本身为 XenMobile 提供该 WSDL 定义。

可以选择是否支持适配器中的各个 PKI 操作。如果适配器支持某个给定操作，可以称之为拥有相应功能（签名、提取或吊销）。这些功能中的每一项均可与一组用户参数相关联。

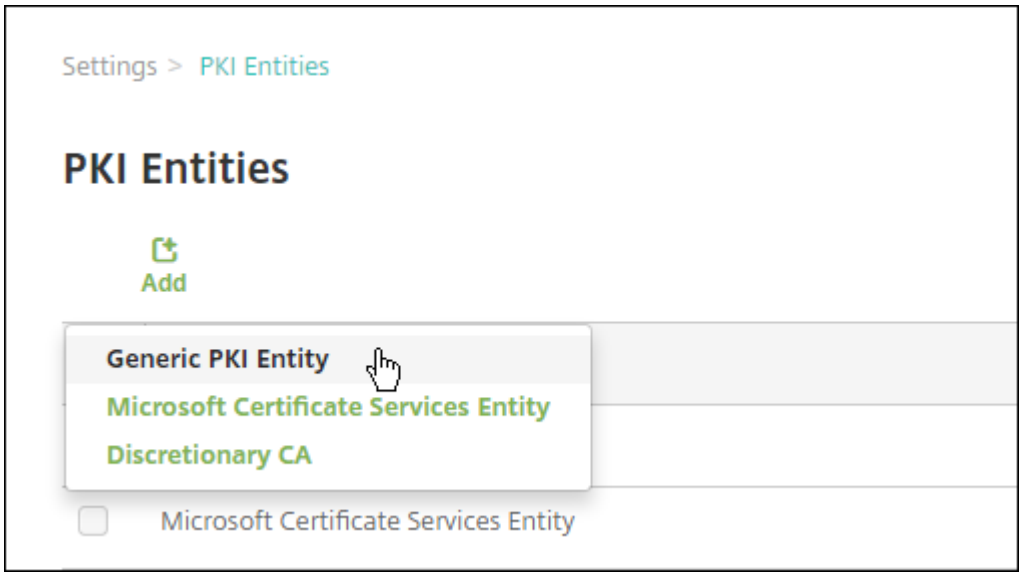
用户参数是指 GPKI 适配器针对特定操作定义的参数，您必须向 XenMobile 提供这些参数的值。XenMobile 通过解析 WSDL 文件来确定适配器支持的操作以及适配器针对每个操作所需的参数。如果选择此项，则使用 SSL 客户端身份验证保护 XenMobile 与 GPKI 适配器之间的连接。

添加通用 **PKI**

1. 在 XenMobile 控制台中，单击设置 **> PKI** 实体。

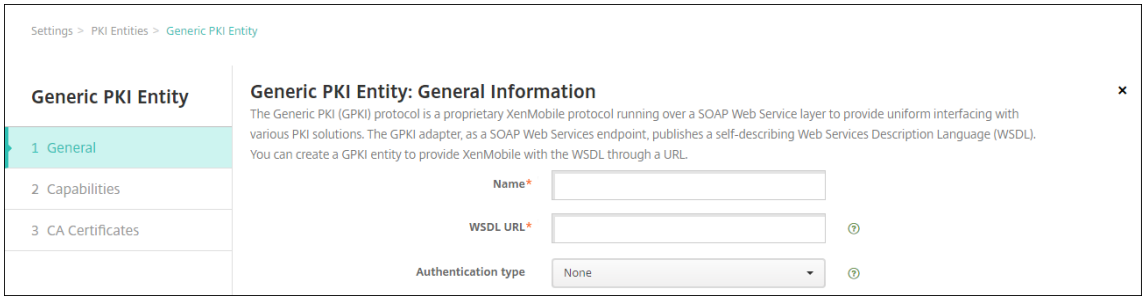
2. 在 **PKI** 实体页面上，单击添加。

   此时将显示一个 PKI 实体类型菜单。



3. 单击通用 **PKI** 实体。

   此时将显示“通用 PKI 实体: 常规信息”页面。



4. 在通用 **PKI** 实体**:** 常规信息页面上，执行以下操作：

   - 名称：键入 PKI 实体的描述性名称。
   - **WSDL URL**：键入描述适配器的 WSDL 的位置。
   - 身份验证类型：单击要使用的身份验证方法。
   - 无
   - **HTTP Basic**：提供连接到适配器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。

5. 单击 **Next**（下一步）。

   此时将显示“通用 PKI 实体: 适配器功能”页面。

6. 在通用 **PKI** 实体**:** 适配器功能页面上，检查与适配器关联的功能和参数，然后单击下一步。

   此时将显示通用 **PKI** 实体**:** 颁发 **CA** 证书页面。

7. 在“通用 PKI 实体: 颁发 CA 证书”页面上，选择要用于此实体的证书。

   尽管实体可能会返回不同 CA 签名的证书，但通过给定证书提供程序获取的所有证书必须由同一个 CA 签名。因此，在配置凭据提供程序设置时，在分发页面上，选择在此处配置的证书之一。

8. 单击保存。

   实体将显示在 PKI 实体表格中。

DigiCert 托管 PKI

XenMobile Server GPKI 支持包括 DigiCert 托管 PKI（也称为 MPKI）。本节介绍如何为 DigiCert 托管 PKI 设置 Windows Server 和 XenMobile Server。

必备条件

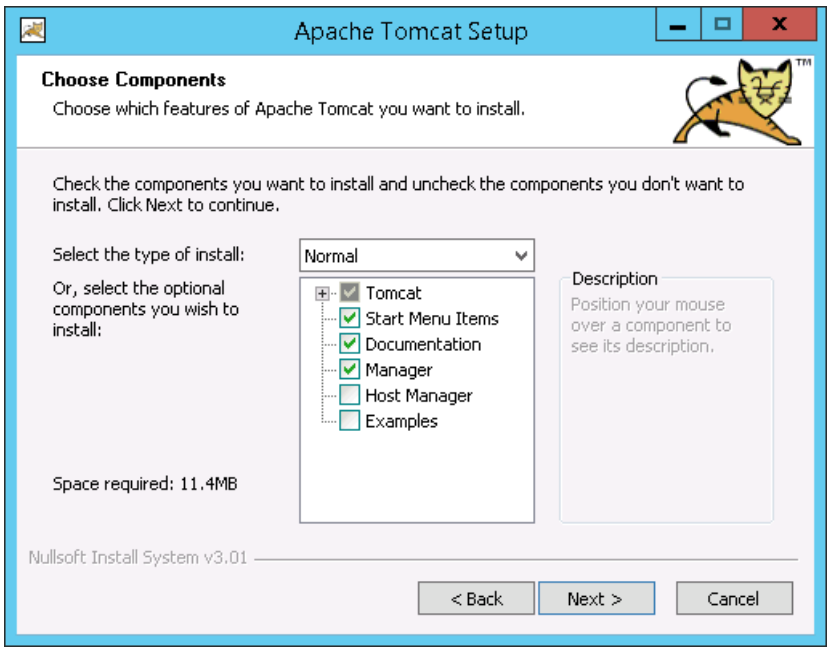
- 访问 DigiCert 托管 PKI 基础结构
- 安装了以下组件的 Windows Server 2012 R2 服务器，如本文中所述：
  - Java
  - Apache Tomcat
  - DigiCert PKI 客户端
  - Portecle
- 访问 XenMobile 下载站点

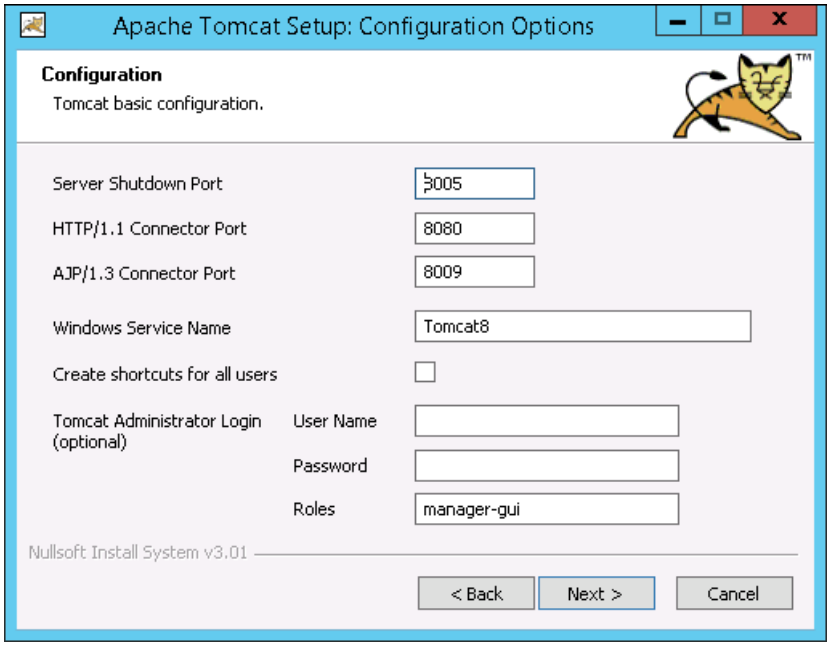
在 Windows Server 上安装 Java

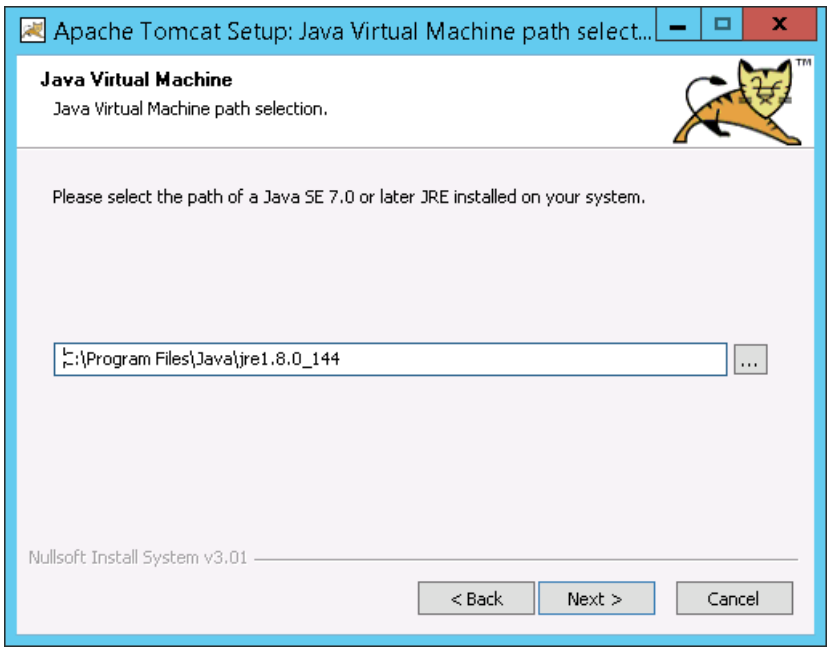
从https://java.com/en/download/faq/java_win64bit.xml 下载 Java 并安装。在“安全警告”对话框中，单击运行。

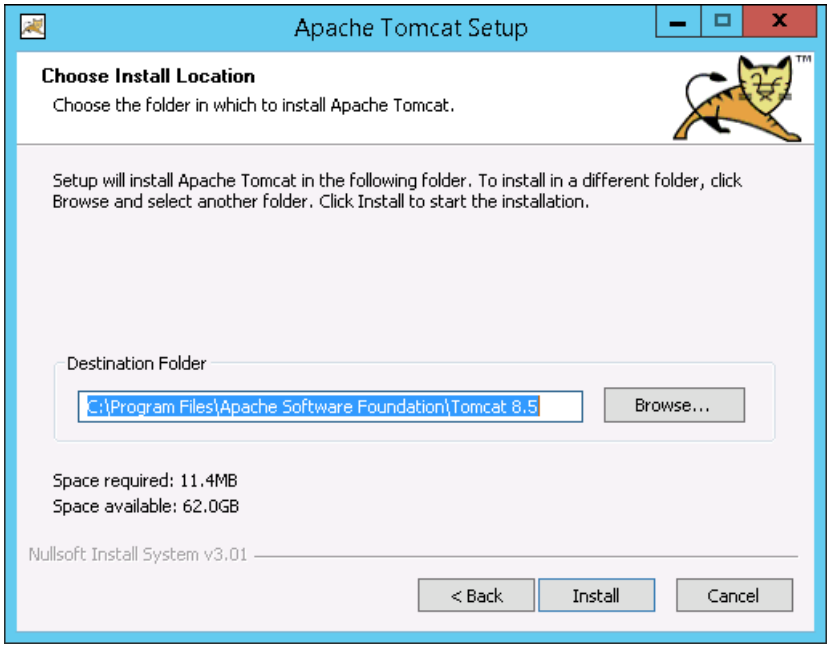
在 Windows Server 上安装 Apache Tomcat

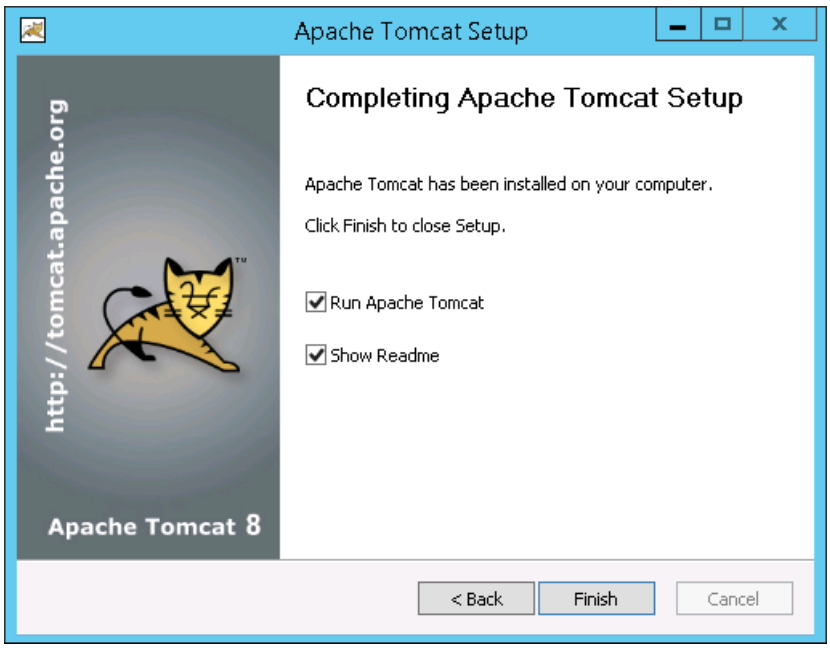
从 https://tomcat.apache.org/download-80.cgi 下载 Apache Tomcat 32 位/64 位 Windows 服务安装程序并安装。在“安全警告”对话框中，单击运行。使用下面的示例作为指南，完成 Apache Tomcat 安装。



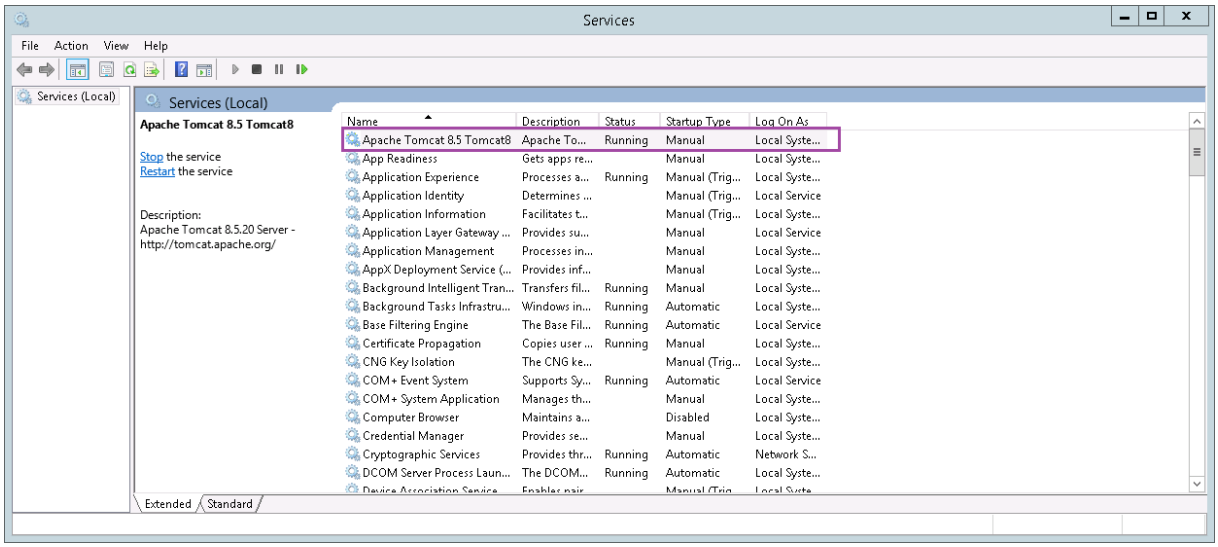


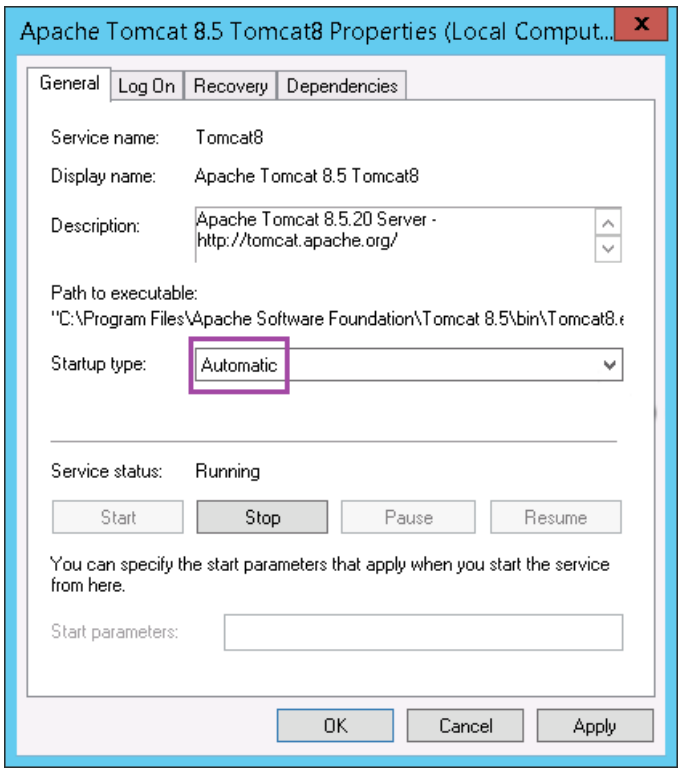






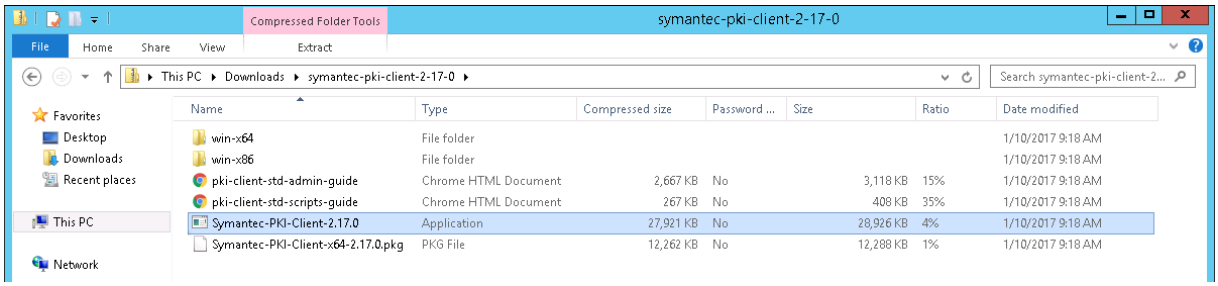
下一步，转至 Windows“Services”（服务）并将 **Startup Type**（启动类型）从 **Manual**（手动）更改为 **Automatic**（自动）。

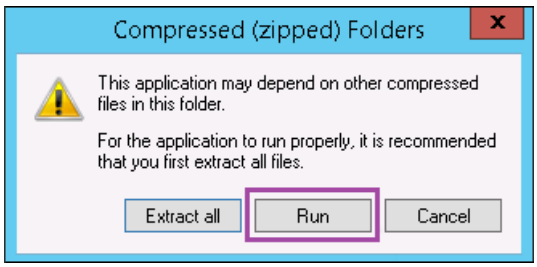




在 **Windows Server** 上安装 **DigiCert PKI** 客户端

从 PKI Manager 控制台下载安装程序。如果您无权访问该控制台，请从 DigiCert 支持页面 How to download DigiCert PKI Client（如何下载 DigiCert PKI 客户端）下载安装程序。解压并运行该安装程序。





在“安全警告”对话框中，务必单击运行。按照安装程序中的说明完成安装。安装程序完成时，系统将提示您重新启动。

在 **Windows Server** 上安装 **Portecle**

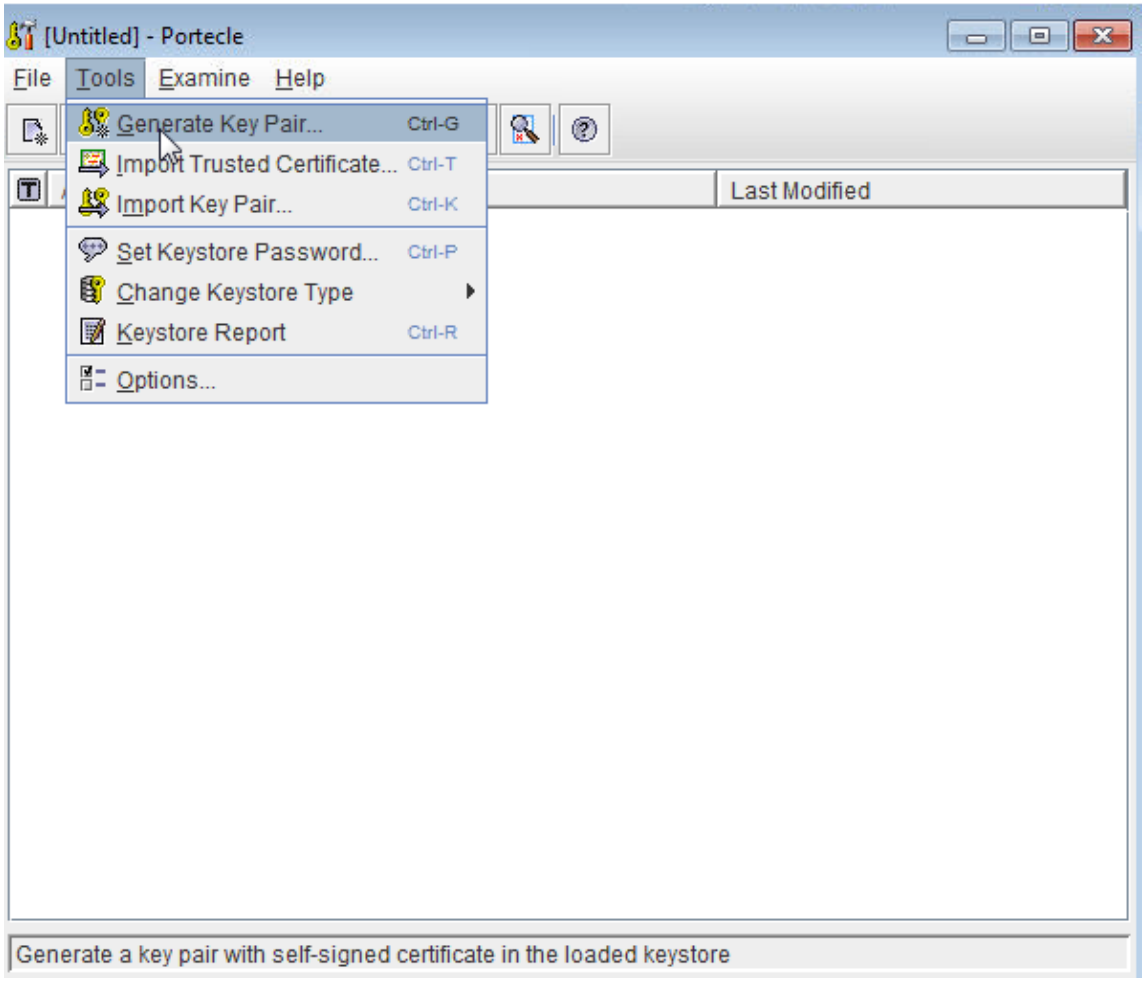
从 https://sourceforge.net/projects/portecleinstall/files/ 下载安装程序，然后解压并运行该安装程序。

为 **DigiCert** 托管 **PKI** 生成注册机构 **(RA)** 证书

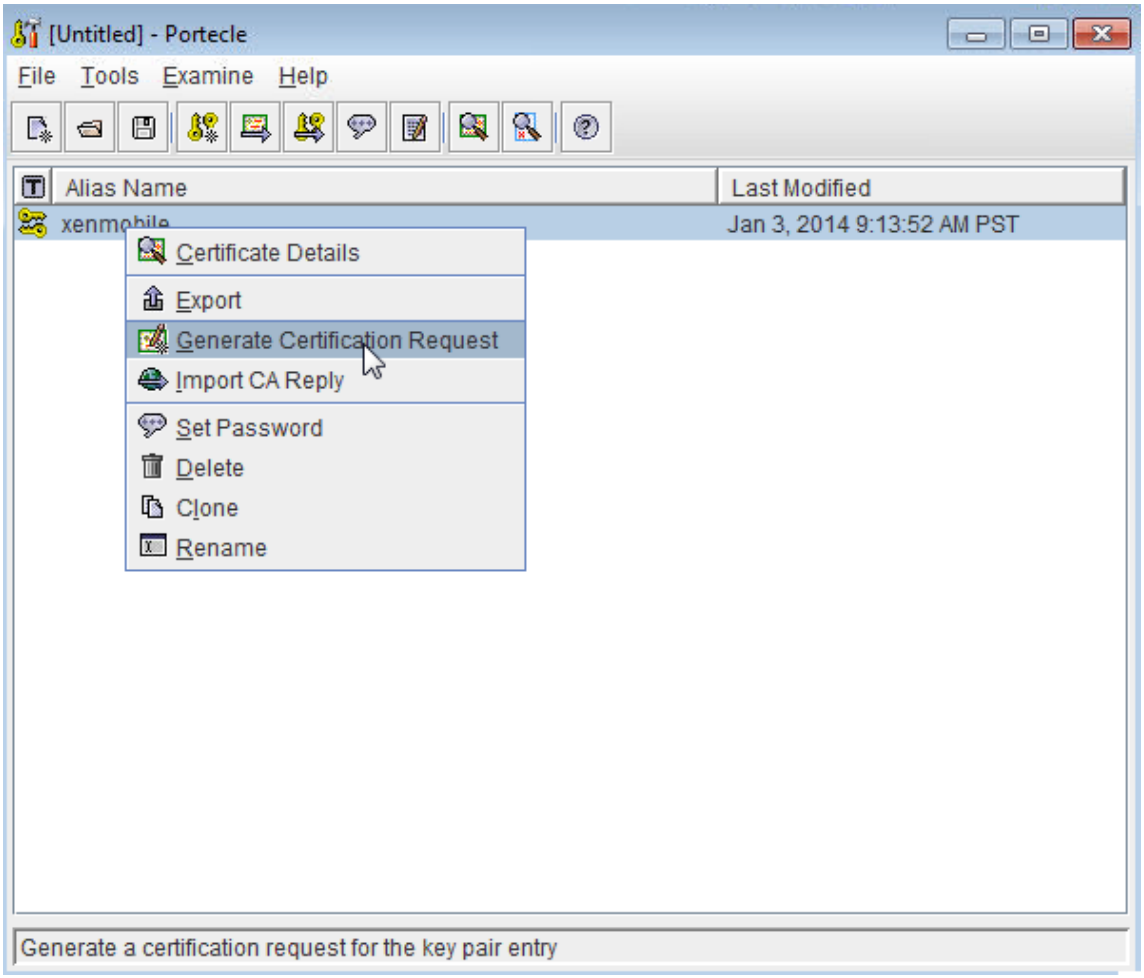
客户端证书身份验证的密钥库包含在注册机构 (RA) 证书中，名为 RA.jks。以下步骤说明了如何使用 Portecle 生成该证书。也可以使用 Java CLI 生成 RA 证书。

本文还说明了如何上载 RA 证书和公用证书。

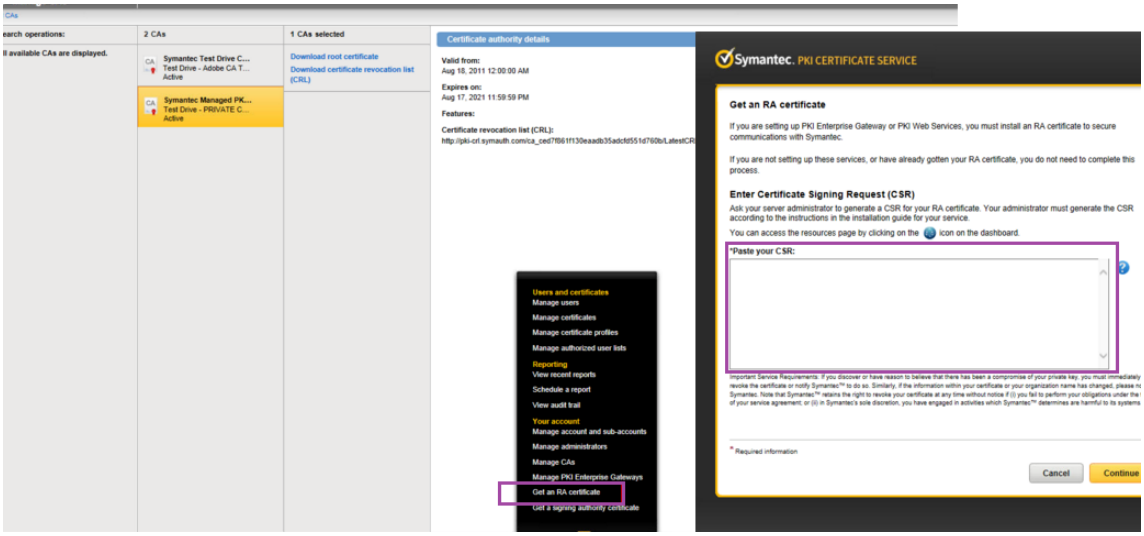
1. 在 Portecle 中，转至 **Tools**（工具）**> Generate Key Pair**（生成密钥对），提供所需信息，然后生成密钥对。



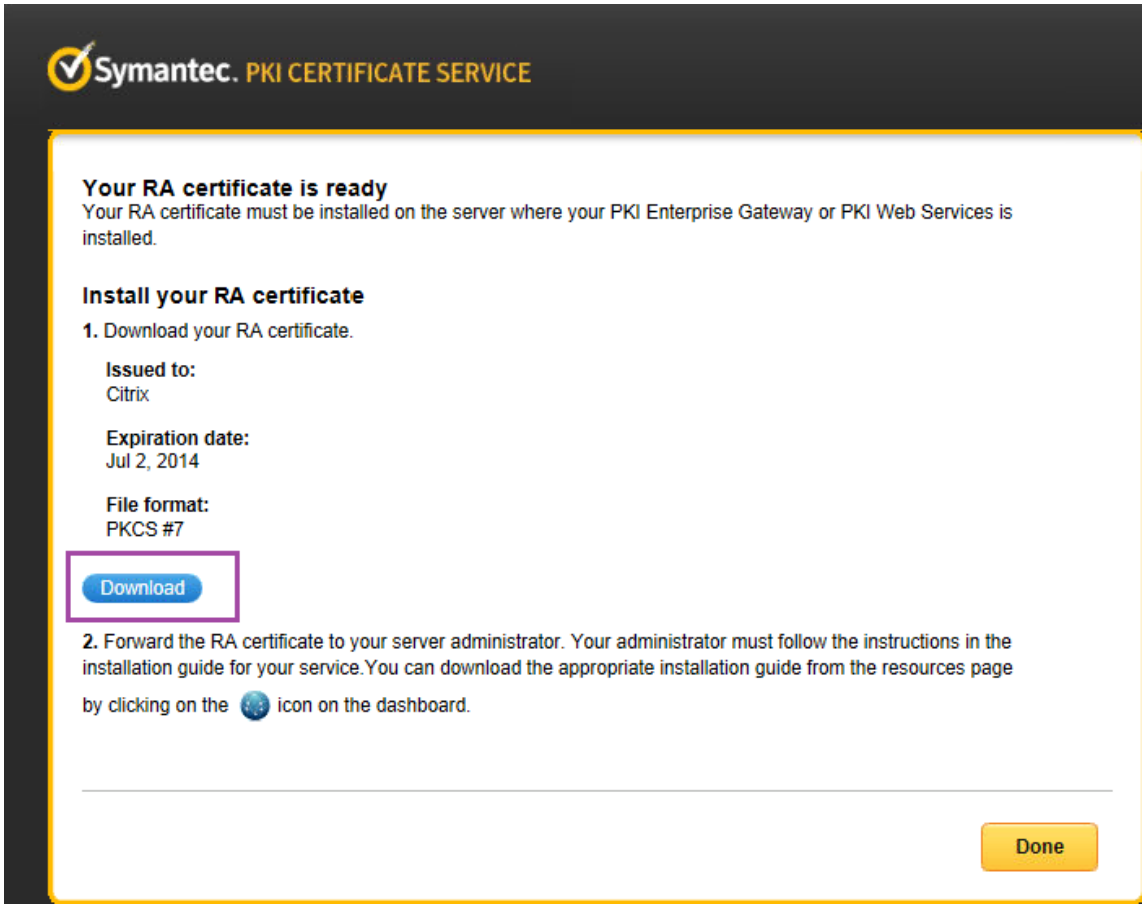
2. 右键单击该密钥对，然后单击 **Generate Certification Request**（生成证书请求）。



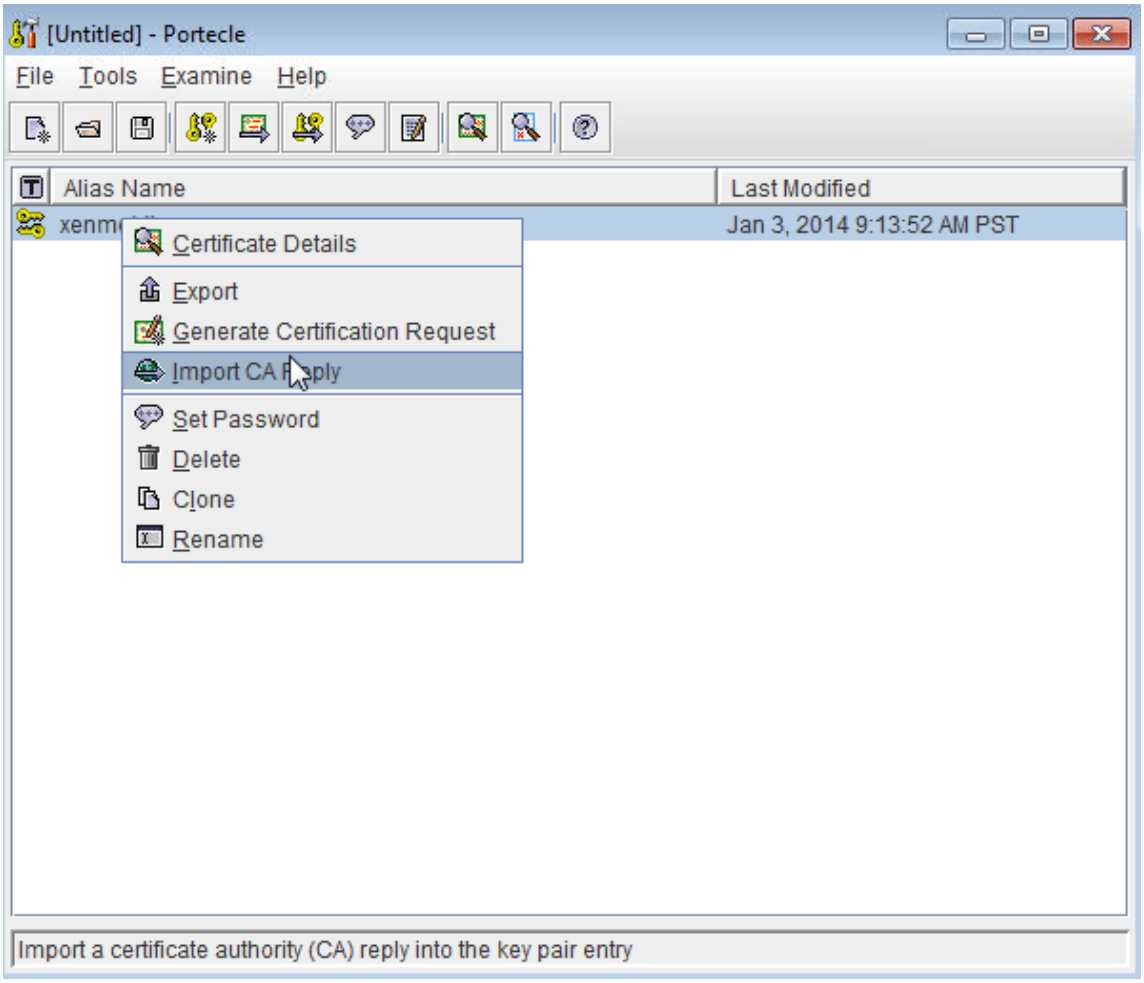
3. 复制 CSR。
4. 在 DigiCert PKI Manager 中，生成 RA 证书：依次单击 **Settings**（设置）和 **Get a RA Certificate**（获取 RA 证书），粘贴 CSR，然后单击 **Continue**（继续）。



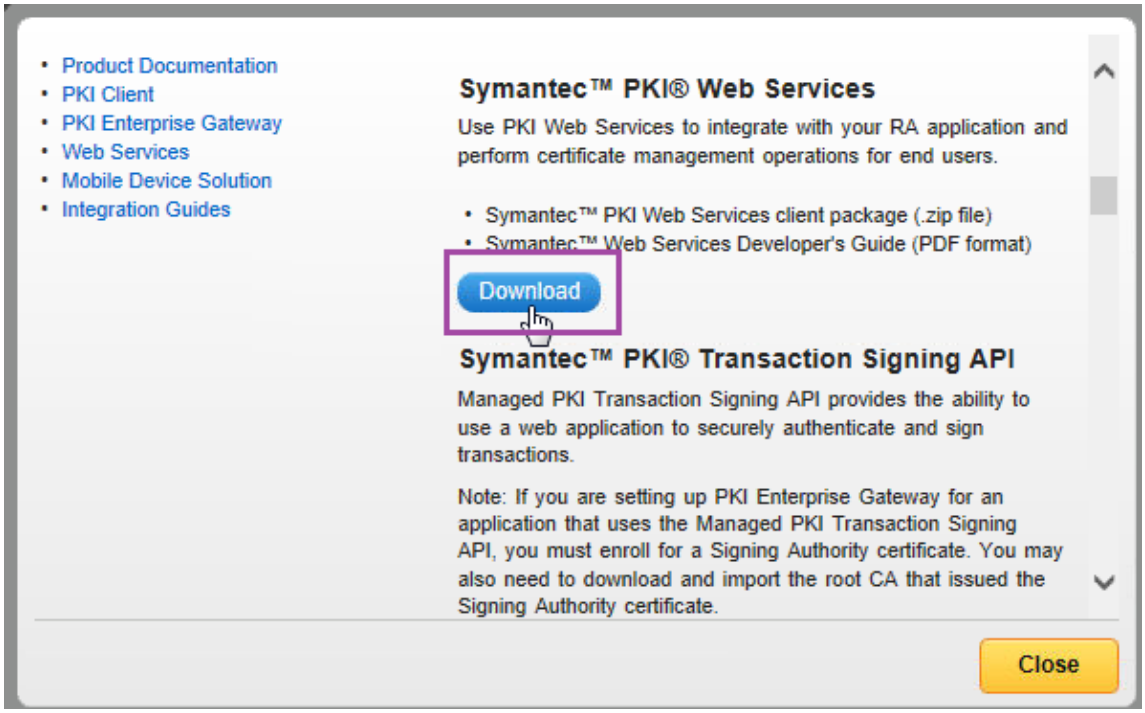
5. 单击 **Download**（下载）以下载生成的 RA 证书。



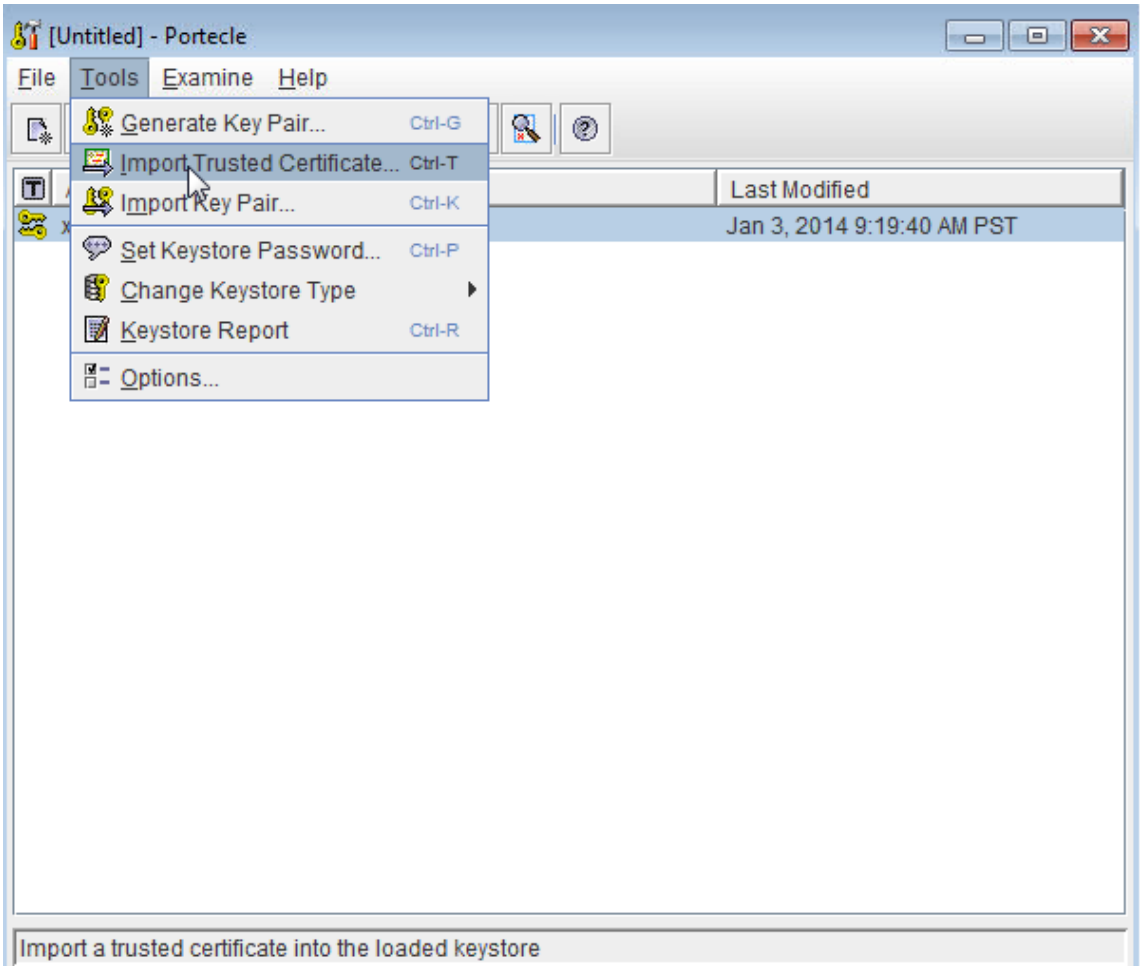
6. 在 Portecle 中，导入 RA 证书：右键单击密钥对，然后单击 **Import CA Reply**（导入 CA 答复）。



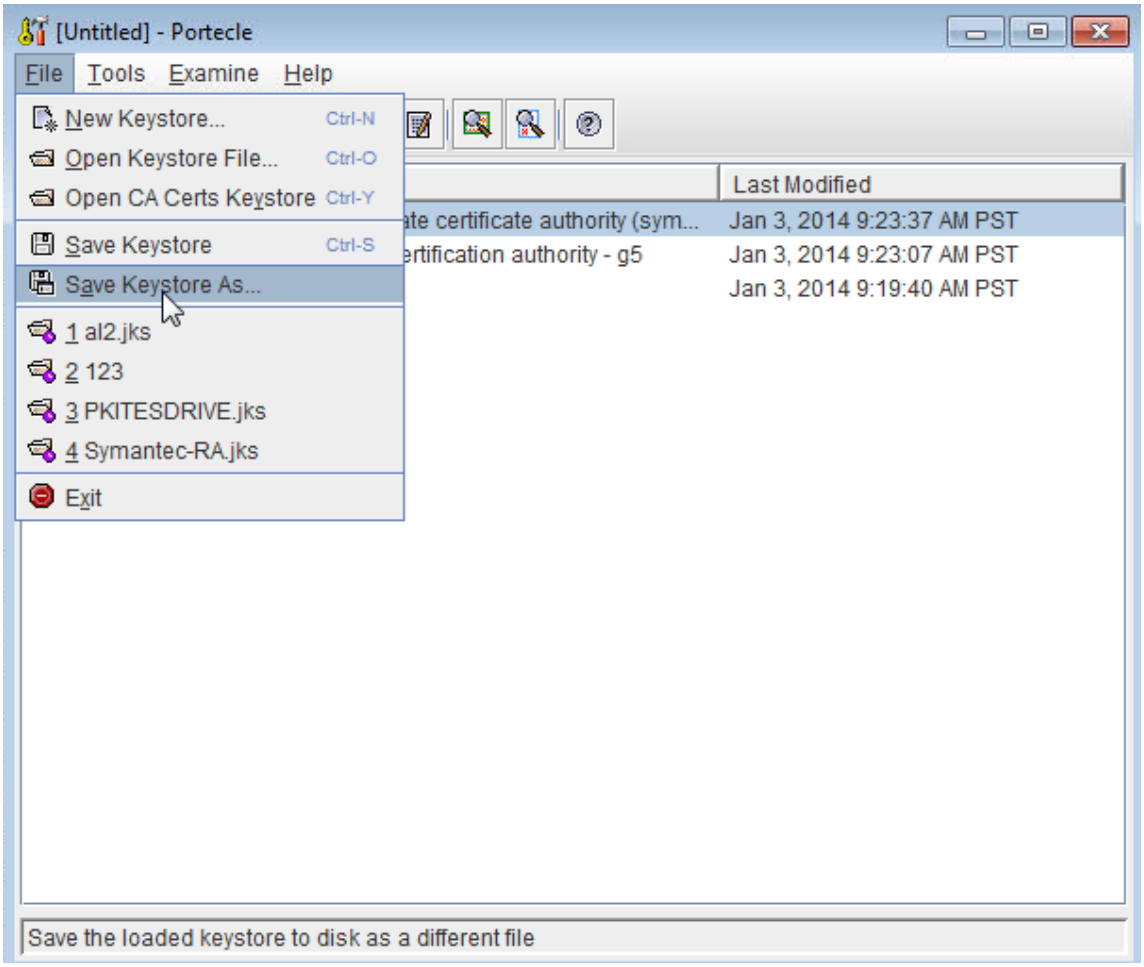
7. 在 DigiCert PKI Manager 中：转至 **Resources**（资源）**> Web Services**（**Web** 服务），然后下载 CA 证书。



8. 在 Portecle 中，将 RA 中间证书和根证书导入到密钥库中：转至 **Tools**（工具）**> Import Trusted Certificates**（导入可信证书）。



9. 导入 CA 后，在 Windows Server 上的 C:\DigiCert 文件夹下将密钥库保存为 RA.jks。



在 **Windows Server** 上配置 **DigiCert PKI** 适配器

1. 以管理员身份登录 Windows Server。
2. 上载您在前面部分中生成的 RA.jks 文件。此外，还请上载适用于您的 Symantec MPKI 服务器的公用证书 (cacerts.jks)。
3. 下载 Symantec PKI Adapter 文件：
   a) 转到 https://www.citrix.com/downloads。
   b) 导航到 **Citrix Endpoint Management**（和 **Citrix XenMobile Server**）**> XenMobile Server (**本地**) >** 产品软件 **> XenMobile Server 10 >** 工具。
   c) 在 **Symantec PKI Adapter** 磁贴上，单击下载文件。
   d) 解压该文件并将这些文件复制到 Windows Server C: 驱动器：
      - custom_gpki_adapter.properties
      - Symantec.war

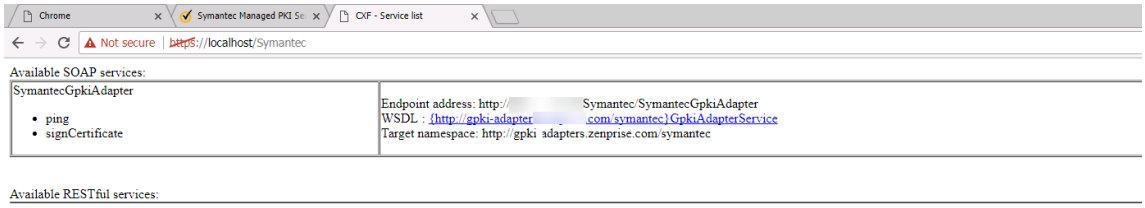
4. 在记事本中打开 custom_gpki_adapter.properties 并编辑以下值：

```
Gpki.CaSvc.Url=https://<managed PKI URL>

# keystore for client-cert auth

keyStore=C:\Symantec\RA.jks

# truststore for server with self-signed root CA

trustStore=C:\Symantec\cacerts.jks
<!--NeedCopy-->
```

5. 在文件夹 <tomcat dir>\webapps 下复制 Symantec.war，然后启动 Tomcat。
6. 验证是否已部署应用程序：打开 Web 浏览器并导航到 https://localhost/Symantec。
7. 导航到该文件夹 <tomcat dir>\webapps\Symantec\WEB-INF\classes 并编辑 gpki_adapter.properties。修改属性 **CustomProperties**，使其指向 C:\Symantec 文件夹下的 custom_gpki_adapter 文件：

   ```
   CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties
   ```

8. 重新启动 Tomcat，导航到 https://localhost/Symantec，然后复制端点地址。在下一部分中，请在配置 PKI 适配器时粘贴该地址。

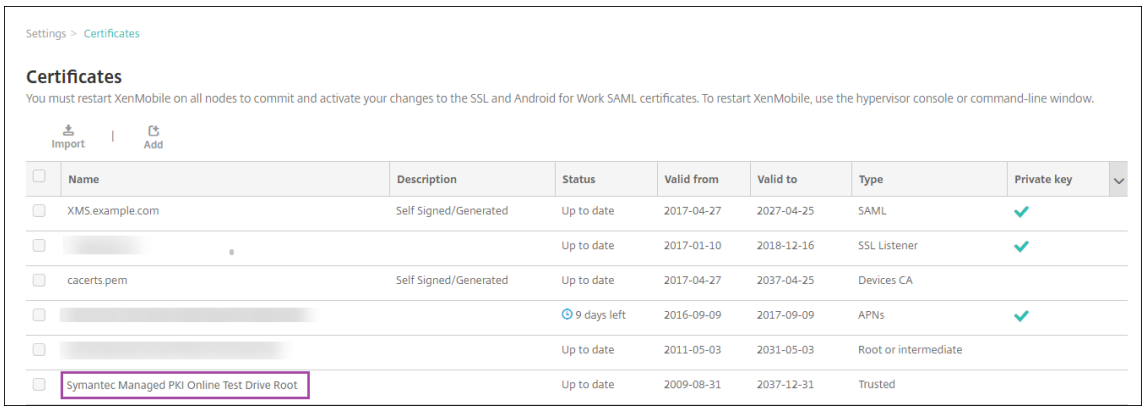


为 **DigiCert** 托管 **PKI** 配置 **XenMobile Server**

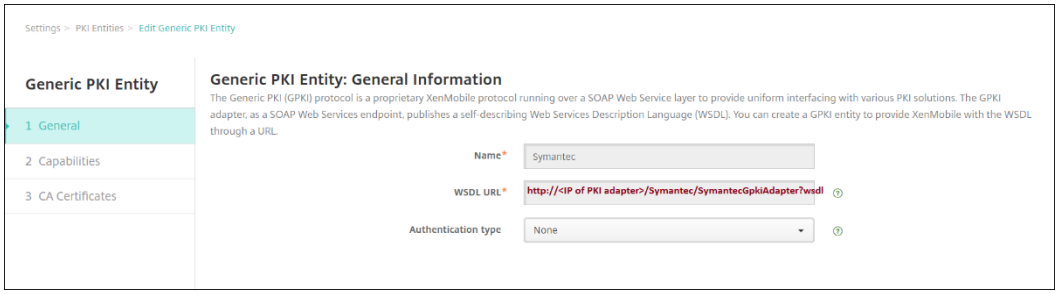
请先完成 Windows Server 设置，然后再执行以下 XenMobile Server 配置。

导入 **DigiCert CA** 证书并配置 **PKI** 实体

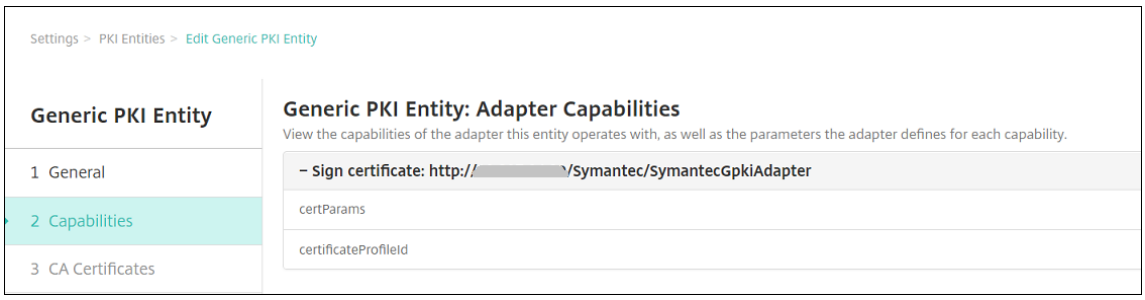
1. 导入颁发最终用户证书的 DigiCert CA 证书：在 XenMobile Server 控制台中，转至设置 **>** 证书并单击导入。



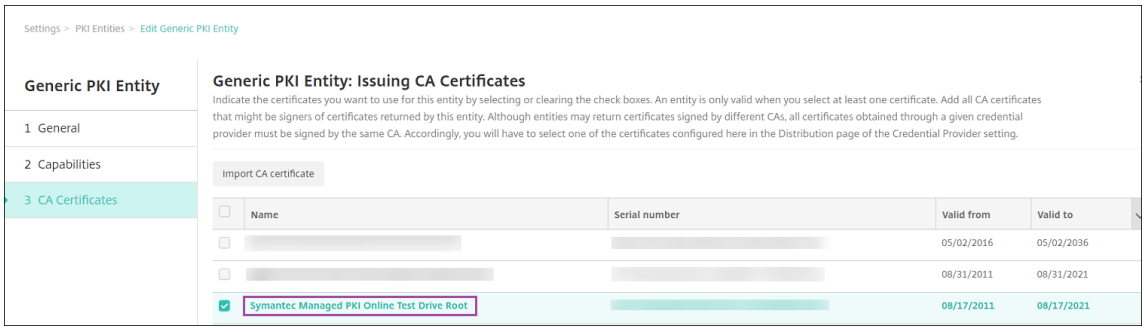
2. 添加并配置 PKI 实体：转至设置 **> PKI** 实体，单击添加，然后选择通用 **PKI** 实体。在 **WSDL URL** 中，粘贴您在上一部分中配置 PKI 适配器时复制的端点地址，然后按如下所示附加 ?wsdl。



3. 单击 **Next**（下一步）。XenMobile 将从 WSDL 中填充参数名称。



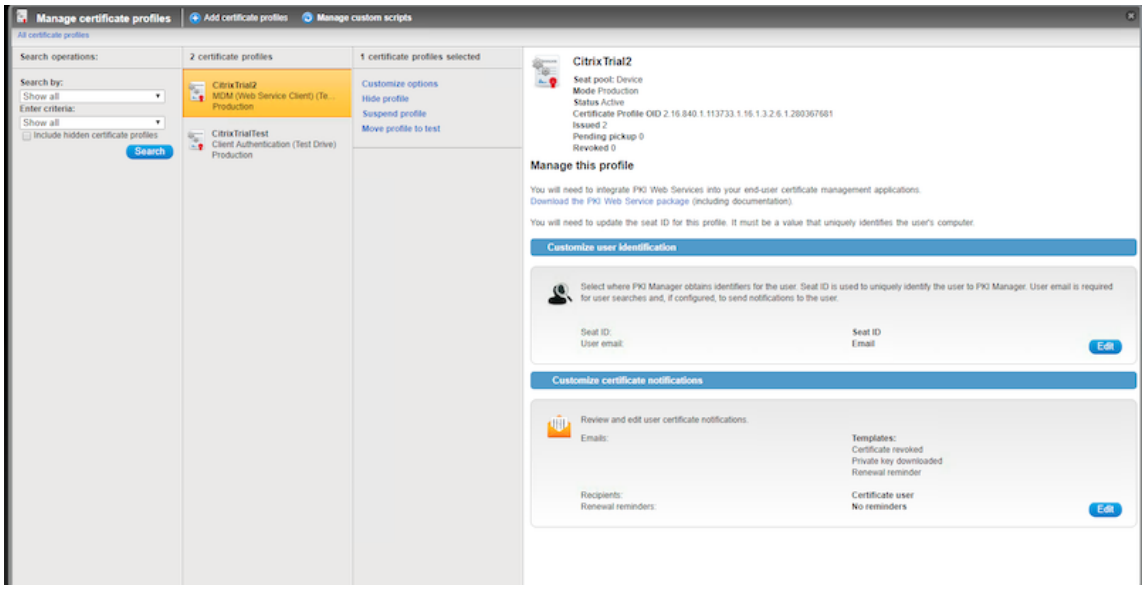
4. 单击下一步，选择正确的 CA 证书，然后单击保存。



5. 在设置 **> PKI** 实体页面上，确认您添加的 PKI 实体的状态为有效。

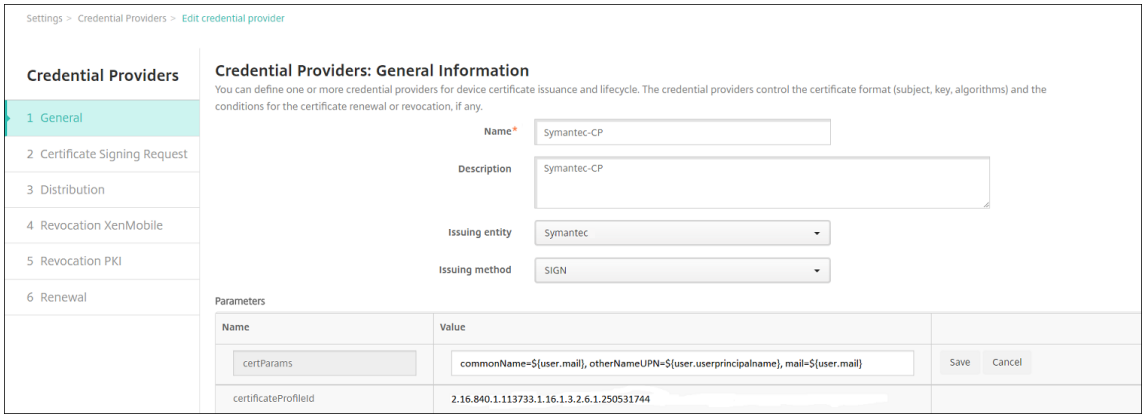
为 **DigiCert** 托管 **PKI** 创建凭据提供程序

1. 在 DigiCert PKI Manager 控制台中，从证书模板中复制证书配置文件 **OID**。



2. 在 XenMobile Server 控制台中，转至设置 **>** 凭据提供程序，单击添加，然后按如下所示配置设置。

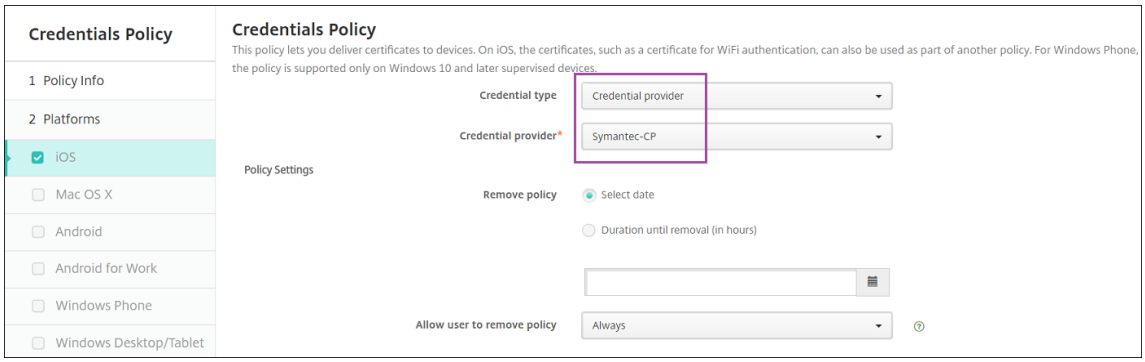
   - 名称：为新提供程序配置键入唯一名称。此名称用于在 XenMobile 控制台的其他部分引用该配置。
   - 说明：凭据提供程序的说明。尽管此字段为可选字段，但当您需要有关凭据提供程序的详细信息时，说明很有用。
   - 颁发实体：选择证书颁发实体。
   - 颁发方法：选择签名作为系统用于从已配置的实体中获取客户端证书的方法。
   - **certParams**：添加以下值：**commonName=${user.mail},otherNameUPN=${user.userprincipalname},**
   - **certificateProfileid**：粘贴您在步骤 1 中复制的证书配置文件 OID。



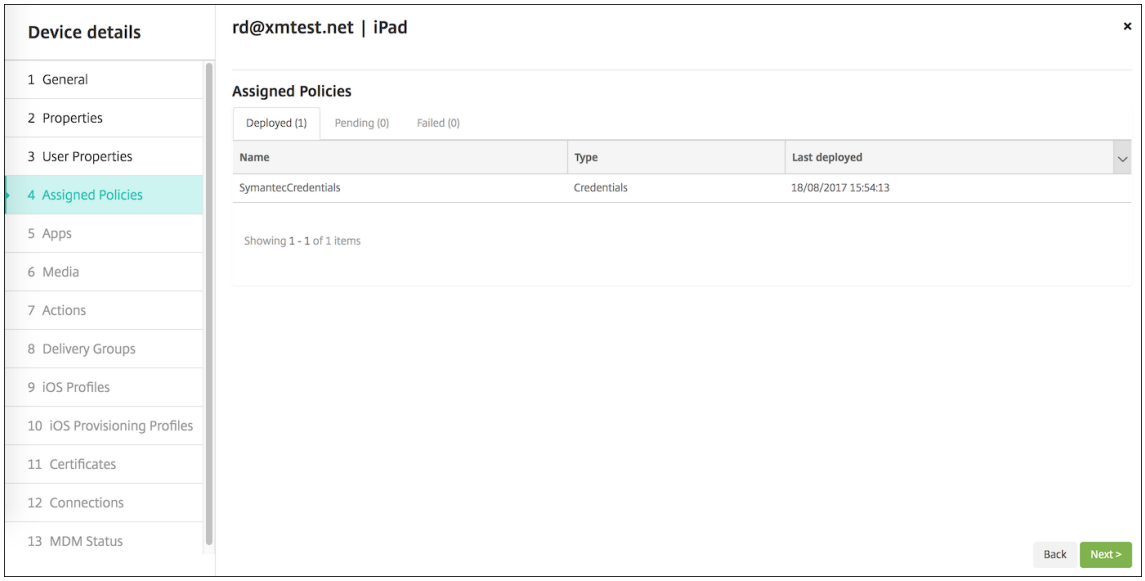
3. 单击 **Next**（下一步）。在其余的每个页面（“证书签名请求”到“续订”）上，接受默认设置。完成后，单击保存。

测试配置和对配置进行故障排除

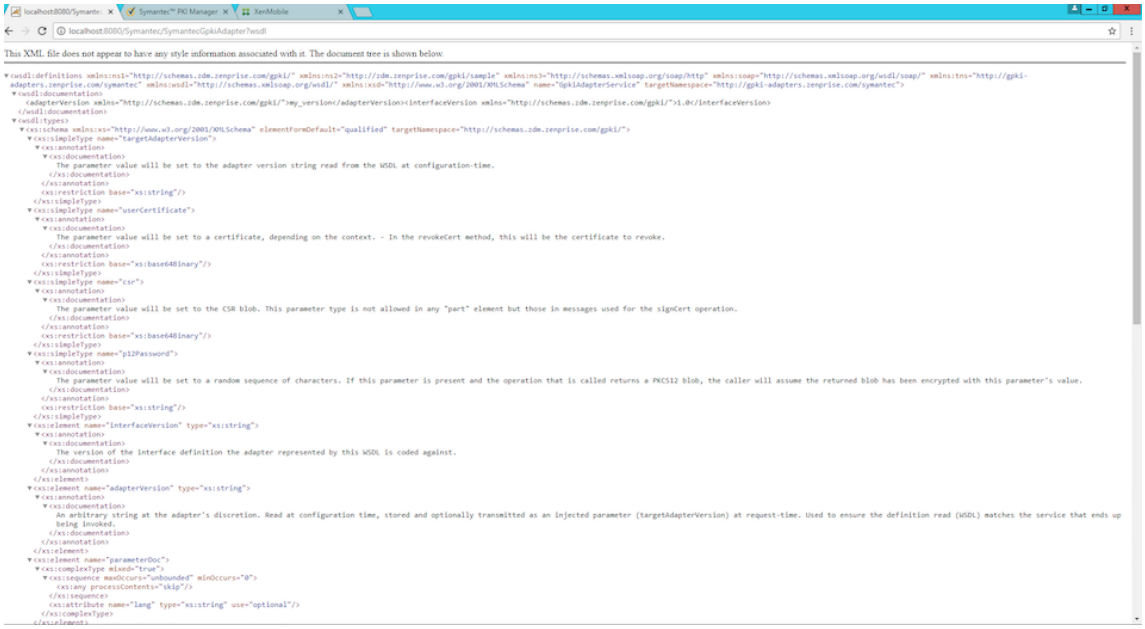
1. 创建凭据设备策略：转至配置 **>** 设备策略，单击添加，开始键入凭据，然后单击凭据。
2. 指定策略名称。
3. 按如下所示配置平台设置：
   - 凭据类型：选择凭据提供程序。
   - 凭据提供程序：选择 DigiCert 提供程序。



4. 完成平台设置后，转至分配页面，将策略分配给交付组，然后单击保存。
5. 要检查策略是否已部署到设备，请转至管理 **>** 设备，选择设备，单击编辑，然后单击已分配的策略。以下示例显示了一个成功的策略部署。



如果该策略未部署，请登录 Windows Server 并检查 WSDL 是否正确加载。



有关故障排除详细信息，请查看 <tomcat dir>\logs\catalina.<current date> 中的 Tomcat 日志。

Entrust PKI 适配器

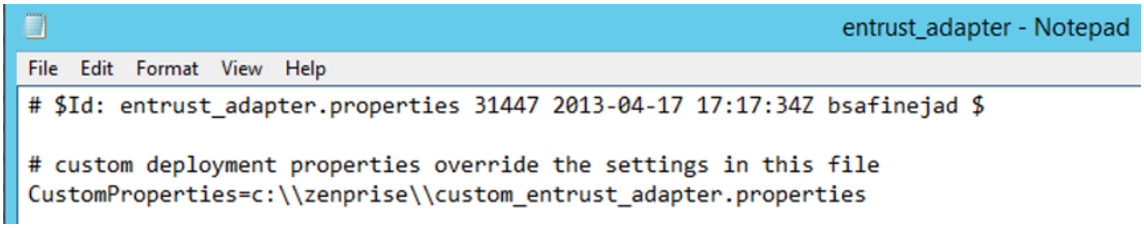
作为 DigiCert 托管 PKI 的替代方案，您可以安装 Entrust PKI 适配器。在安装适配器之前，请参阅本文的DigiCert 托管 PKI 部分中有关在 Windows Server 上安装 Java 和 Apache Tomcat 的步骤。

安装 Entrust PKI 适配器

1. 下载 Entrust PKI Adapter 文件：

a) 转到 https://www.citrix.com/downloads。
b) 导航到 **Citrix Endpoint Management**（和 **Citrix XenMobile Server**）**> XenMobile Server > 产品软件 > XenMobile Server 10 >** 工具。
c) 在 **Entrust PKI Adapter** 磁贴上，单击下载文件。
d) 从下载的.zip 文件中提取 entrust.war 文件，并将其放置在 C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps 目录中。

2. 在 C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes 中，编辑 entrust_adapter.properties 并将 CustomProperties 设置为 `c:\\zenprise\\custom_entrust_adapter.properties`。



3. 在 C: 驱动器中，创建 zenprise 目录和一个名为 custom_entrust_adapter.properties 的新文件。
4. 使用以下内容编辑文件，并注意适当替换 Entrust.MdmSvc.URL、AdminUserId 和 AdminPassword。

~

# 对于 AS/IG
Entrust.MdmSvc.Url=`https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8`，请将以下内容设置为正确的 URL

```
# set to 1 or true to force user creation from passed user and group parameters if using IG and user does not exist
CreateUser=

# set the credentials for the endpoint
AdminUserId=`[User ID]`
AdminPassword=`[password]`


# keystore for client-cert auth
#keyStore=
#keyStorePassword=
#keyStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and .jks files

# truststore for server with self-signed root CA
#trustStore=
#trustStorePassword=
#trustStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and .jks files
```



```
18  ~
```

5. 重新启动 Tomcat 服务。导航到 C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\logs 并打开 Catalina_201x-MM-DD.log。验证没有错误并显示以下行：
   `13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf.endpoint.ServerImpl.initDestination Setting the server's publish address to be /EntrustGpkiAdapter`
6. 导航到 `http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl` 或服务器的公用 URL，并验证 XML 正确显示。

为 **Entrust PKI** 适配器配置 **XenMobile**

1. 登录到 XenMobile 控制台并导航到设置 **>** **PKI** 实体。单击添加 **>** 通用 **PKI** 实体。
2. 输入以下信息：
   - 名称：输入 PKI 实体的名称。
   - **WSDL URL**：输入您的服务器的公共 URL。
   - 身份验证类型：选择要使用的身份验证方法。
     - 无
     - **HTTP Basic**：键入连接所需的用户名和密码。
     - 客户端证书：选择正确的 SSL 客户端证书。
   - 资源位置：选择我的资源位置。
   - 允许使用的相对路径：输入 `/Entrust/*`。
3. 完成配置 PKI 实体后，返回到设置页面并添加凭据提供程序。
4. 在常规选项卡上，选择您的 Entrust 实体作为颁发实体，选择 **SIN** 作为颁发方法。

5. 在证书签名请求选项卡上，按如下所示配置设置：
   - 密钥算法： **RSA**。
   - 密钥大小： 2048。
   - 签名算法 **SHA256withRSA**。
   - 使用者名称： cn=$user.username
   - 使用者备用名称：可选。我们的建议如下：
     - 类型：用户主体名称。
     - 值： $user.userprincipalname

     > 注意：
     >
     > 如果更改适配器上的任何设置，请按照以下步骤重新配置凭据提供程序。
6. 完成配置证书提供程序后，导航到配置 **>** 设备策略并添加证书策略。
7. 为您计划使用的操作系统配置策略。在每个操作系统配置页面上，对于凭据类型，请选择凭据提供程序。对于凭据提供程序菜单，请选择之前配置的凭据提供程序。

Microsoft 证书服务

XenMobile 通过其 Web 注册界面与 Microsoft Certificate Services 交互。XenMobile 仅支持通过该界面颁发新证书（相当于 GPKI 签名功能）。如果 Microsoft CA 生成 Citrix Gateway 用户证书，Citrix Gateway 将支持续订和吊销这些证书。

要在 XenMobile 中创建 Microsoft CA PKI 实体，必须指定证书服务 Web 界面的基本 URL。如果选择此项，则使用 SSL 客户端身份验证保护 XenMobile 与证书服务 Web 界面之间的连接。

添加 **Microsoft** 证书服务实体

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击 **PKI** 实体。
2. 在 **PKI** 实体页面上，单击添加。

   此时将显示一个 PKI 实体类型菜单。
3. 单击 **Microsoft** 证书服务实体。

   此时将显示 **Microsoft** 证书服务实体**:** 常规信息页面。
4. 在 **Microsoft** 证书服务实体**:** 常规信息页面上，配置以下设置：
   - 名称：为新实体键入名称，此名称以后将用于指代该实体。实体名称必须唯一。
   - **Web** 注册服务根 **URL**： 键入 Microsoft CA Web 注册服务的基本 URL，例如 `https://192.0.2.13/certsrv/`。该 URL 可能会使用纯 HTTP 或 HTTP-over-SSL。
   - **certnew.cer** 页面名称： certnew.cer 页面的名称。若非因为某些原因重命名了此页面，请使用默认名称。
   - **certfnsh.asp**： certfnsh.asp 页面的名称。若非因为某些原因重命名了此页面，请使用默认名称。
   - 身份验证类型：选择要使用的身份验证方法。

- 无
- **HTTP Basic**：键入连接所需的用户名和密码。
- 客户端证书：选择正确的 SSL 客户端证书。

5. 单击测试连接以确保服务器可以访问。如果不可访问，则会显示一条消息，指出连接失败。请检查配置设置。
6. 单击 **Next**（下一步）。

   此时将显示 **Microsoft** 证书服务实体**:** 模板页面。在此页面上，指定 Microsoft CA 所支持模板的内部名称。创建凭据提供程序时，从此处定义的列表中选择模板。使用此实体的每个凭据提供程序仅使用一个此类模板。

   有关 Microsoft 证书服务模板的要求，请参阅您的 Microsoft Server 版本对应的 Microsoft 文档。除了证书中所述的证书格式要求外，XenMobile 对其分发的证书并无其他要求。

7. 在 **Microsoft** 证书服务实体**:** 模板页面上，单击添加，键入模板的名称，然后单击保存。为要添加的每个模板重复执行此步骤。
8. 单击 **Next**（下一步）。

   此时将显示 **Microsoft** 证书服务实体**: HTTP** 参数页面。在此页面上，您可以指定自定义参数以供 XenMobile 添加到向 Microsoft Web 注册界面发送的 HTTP 请求。自定义参数仅对 CA 上运行的自定义脚本有用。

9. 在 **Microsoft** 证书服务实体**: HTTP** 参数页面上，单击添加，键入要添加的 HTTP 参数的名称和值，然后单击下一步。

   此时将显示 **Microsoft** 证书服务实体**: CA** 证书页面。在此页面上，必须将系统通过此实体获取的证书的签署者告知 XenMobile。续订 CA 证书后，将在 XenMobile 中对其进行更新。XenMobile 以透明方式将更改应用于实体。

10. 在 **Microsoft** 证书服务实体**: CA** 证书页面上，选择要用于此实体的证书。
11. 单击保存。

    实体将显示在 PKI 实体表格中。

Citrix ADC 证书吊销列表 **(CRL)**

XenMobile 仅支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，XenMobile 将使用 Citrix ADC 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 Citrix ADC 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh**（启用 CRL 自动刷新）。此步骤可确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证。

XenMobile 将重新颁发新证书，因为吊销用户证书后，XenMobile 不会限制用户生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

任意 CA

向 XenMobile 提供 CA 证书及关联的私钥时，将创建任意 CA。XenMobile 将根据您指定的参数，在内部处理证书颁发、吊销和状态信息。

配置任意 CA 时，可以为该 CA 激活联机证书状态协议 (OCSP) 支持。当且仅当启用了 OCSP 支持时，CA 才会向该 CA 颁发的证书中添加 `id-pe-authorityInfoAccess` 扩展。该扩展指向以下位置处的 XenMobile 内部 OCSP 响应者：

`https://<server>/<instance>/ocsp`

配置 OCSP 服务时，请为相关任意实体指定 OCSP 签名证书。可以将 CA 证书本身用作签署者。要避免 CA 私钥的不必要暴露（建议避免），请创建一个由 CA 证书签名并包含 `id-kp-OCSPSigning extendedKeyUsage` 扩展的委派 OCSP 签名证书。

XenMobile OCSP Responder Service 支持在请求中使用基本 OCSP 响应及以下散列算法：

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

响应通过 SHA-256 及签名证书的密钥算法（DSA、RSA 或 ECDSA）进行签名。

添加任意 CA

1. 在 XenMobile 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。

   此时将显示一个 PKI 实体类型菜单。
3. 单击任意 **CA**。

   此时将显示任意 **CA:** 常规信息页面。
4. 在任意 **CA:** 常规信息页面上，执行以下操作：
   - 名称：键入任意 CA 的描述性名称。
   - 用于对证书请求进行签名的 **CA** 证书：单击任意 CA 用于为证书请求签名的证书。

     此证书列表是根据您通过配置 **>** 设置 **>** 证书上载到 XenMobile 的 CA 证书（带私钥）生成的。
5. 单击 **Next**（下一步）。

   此时将显示任意 **CA:** 参数页面。
6. 在任意 **CA:** 参数页面上，执行以下操作：

- 序列号生成器：任意 CA 为其颁发的证书生成序列号。从此列表中，单击按顺序或不按顺序以确定序列号的生成方式。
- 下一个序列号：键入一个用于确定颁发的下一个序列号的值。
- 证书有效期：键入证书有效的天数。
- 密钥用法：通过将相应的密钥设置为开，标识任意 CA 所颁发证书的目的。设置后，CA 仅限于为这些目的颁发证书。
- 扩展密钥用法：要添加更多参数，请单击添加，键入密钥名称，然后单击保存。

7. 单击 **Next**（下一步）。

   此时将显示任意 **CA:** 分发页面。

8. 在任意 **CA:** 分发页面上，选择分发模式：

   - 集中式**:** 服务器端密钥生成。Citrix 建议使用集中选项。在服务器上生成并存储私钥，然后分发到用户设备。
   - 分布式**:** 设备端密钥生成。私钥在用户设备上生成。此分布式模式使用 SCEP 并需要采用 **keyUsage keyEncryption** 扩展的 RA 加密证书和采用 **keyUsage digitalSignature** 扩展的 RA 签名证书。同一个证书可以同时用于加密和签名。

9. 单击 **Next**（下一步）。

   此时将显示任意 **CA:** 联机证书状态协议 **(OCSP)** 页面。

   在任意 **CA:** 联机证书状态协议 **(OCSP)** 页面上，执行以下操作：

   - 如果要向此 CA 签名的证书添加 `AuthorityInfoAccess` (RFC2459) 扩展，请将为此 **CA** 启用 **OCSP** 支持设置为开。此扩展指向位于 `https://<server>/<instance>/ocsp` 的 CA OCSP 响应者。
   - 如果启用了 OCSP 支持，请选择 OSCP 签名 CA 证书。此证书列表使用您上载到 XenMobile 的 CA 证书生成。

10. 单击保存。

    任意 CA 将显示在 PKI 实体表格中。

凭据提供程序

January 5, 2022

凭据提供程序是在 XenMobile 系统的各个部分中使用的实际证书配置。凭据提供程序定义证书的来源、参数和生命周期。无论这些证书是设备配置的一部分还是独立的配置（即，按原样推送到设备），都是这样。

设备注册约束证书生命周期。也就是说，XenMobile 在注册前不颁发证书，尽管 XenMobile 可能会在注册的过程中颁发某些证书。此外，在某个注册环境下从内部 PKI 颁发的证书会在注册被吊销时吊销。管理关系终止后，不保留任何有效证书。

一个凭据提供程序配置可用于多个位置，从而达到通过一个配置同时控制任意多个证书的效果。这时，其唯一性在于部署资源和部署。例如，如果凭据提供程序 P 作为配置 C 的一部分部署到设备 D：P 的颁发设置将决定部署到 D 的证书。同样，在更新 C 时将应用 D 的续订设置。并且，删除 C 或吊销 D 时将应用 D 的吊销设置。

根据这些规则，XenMobile 中的凭据提供程序配置确定以下各项：

- 证书的来源。
- 获取证书的方法：签发新证书还是提取（恢复）现有证书和密钥对。
- 用于颁发或恢复的参数。例如，密钥大小、密钥算法和证书扩展名等证书签名请求 (CSR) 参数。
- 将证书交付给设备的方式。
- 吊销条件。尽管在管理关系终止后 XenMobile 中的所有证书都将被吊销，但该配置可以指定在更早时间吊销。例如，配置可以指定在删除关联设备配置时吊销证书。此外，在某些情况下，XenMobile 中关联证书的吊销可能会发送给后端公钥基础结构 (PKI)。也就是说，在 XenMobile 中吊销证书可能导致在 PKI 上吊销证书。
- 续订设置。通过指定凭据提供程序获取的证书可以在即将过期时自动续订。或者采用与之不同的方式，在接近过期时由系统发送通知。

配置选项的可用性主要取决于为凭据提供程序选择的 PKI 实体的类型和颁发方法。

证书颁发方法

可以通过两种方式（称为“颁发方法”）获取证书：

- 签名：利用此方法，颁发包括创建新私钥、创建 CSR 以及将 CSR 提交给证书颁发机构 (CA) 进行签名。XenMobile 支持对三种 PKI 实体（MS 证书服务实体、通用 PKI 和任意 CA）使用该签名方法。
- 提取：利用此方法，用于 XenMobile 的颁发是指恢复现有密钥对。XenMobile 仅支持对通用 PKI 使用提取方法。

凭据提供程序使用签名或提取颁发方法。所选方法会影响可用配置选项。具体而言，仅当颁发方法为签名时，才可以使用 CSR 配置和分散交付。提取的证书始终作为 PKCS #12 发送给设备，相当于签名方法的集中交付模式。

证书交付

XenMobile 中可用的证书交付模式共有两种：集中和分散。分布式模式使用简单证书注册协议 (SCEP)，并且只有在客户端支持该协议时方可使用（仅限 iOS）。在某些情况下，必须采用分布式模式。

对于支持分散式（SCEP 辅助）交付的凭据提供程序，需要特殊的配置步骤：设置注册机构 (RA) 证书。需要 RA 证书是因为，使用 SCEP 协议时，XenMobile 充当实际证书颁发机构的委派者（注册者）。XenMobile 必须向客户端证实自己有权执行此类操作。通过向 XenMobile 上载上述证书，可以建立该机构。

需要两种不同的证书角色（尽管同一证书即可满足这两项要求）：RA 签名和 RA 加密。这些角色的限制如下：

- RA 签名证书必须拥有 X.509 密钥用法数字签名。
- RA 加密证书必须拥有 X.509 密钥用法密钥加密。

要配置凭据提供程序的 RA 证书，请先将证书上载到 XenMobile，然后在凭据提供程序中链接到这些证书。

仅当凭据提供程序为证书角色配置了证书时，才可将凭据提供程序视为支持分散式交付。可以将每个凭据提供程序配置为首选集中式模式、首选分布式模式或要求分布式模式。实际结果取决于具体环境：如果环境不支持分布式模式，但是凭据提供程序要求使用该模式，部署将失败。同样，如果环境要求使用分布式模式，但凭据提供程序不支持该模式，部署也将失败。在所有其他情况下，将会应用首选设置。

下面显示了 SCEP 在整个 XenMobile 的分布：

上下文	支持 SCEP	需要 SCEP
iOS 配置文件服务	是	是
iOS 移动设备管理注册	是	否
iOS 配置文件	是	否
SHTP 注册	否	否
SHTP 配置	否	否
Windows Phone 和 Windows Tablet 注册	否	否
Windows Phone 和 Windows Tablet 配置	否，Wifi 设备策略除外，后者支持 Windows Phone 8.1、Windows 10 和 Windows 11。	否

证书吊销

有三种类型的吊销。

- 内部吊销：内部吊销影响由 XenMobile 维护的证书状态。重新评估提供的证书时，或者提供证书的 OCSP 状态信息时，XenMobile 会考虑此状态。凭据提供程序配置决定在各种条件下此状态受到的影响。例如，凭据提供程序可以指定从设备中删除证书后将这些证书标记为已吊销。
- 外部传播的吊销：又称“吊销 XenMobile”，这种类型的吊销适用于从外部 PKI 获取的证书。在凭据提供程序配置定义的条件下，XenMobile 在内部吊销证书时也会在 PKI 上吊销该证书。用于执行吊销的调用需要使用支持吊销的通用 PKI (GPKI) 实体。
- 外部引起的吊销：又称“吊销 PKI”，这种类型的吊销也仅适用于从外部 PKI 获取的证书。每次 XenMobile 评估指定证书的状态时，XenMobile 都将向 PKI 查询该状态。如果证书已吊销，XenMobile 将在内部吊销该证书。此机制使用 OCSP 协议。

这三种类型并不互斥，而是可以一起应用。外部吊销或独立查询结果可能会导致内部吊销。内部吊销会潜在影响外部吊销。

证书续订

证书续订由吊销现有证书和颁发另一个证书两个过程组成。

XenMobile 将首先尝试获取新证书，然后再吊销之前的证书，以避免在颁发失败时造成服务中断。如果采用分散式（支持 SCEP）交付，仅当证书成功安装到设备后再进行吊销。否则，将在新证书发送给设备之前进行吊销。这种吊销与证书是否安装成功无关。

配置吊销时，需要指定特定的持续时间（天）。如果设备已连接，服务器将验证证书的 “`NotAfter`” 日期是否晚于当前日期减去指定的持续时间。如果证书满足该条件，XenMobile 将尝试续订该证书。

创建凭据提供程序

凭据提供程序的配置方式有多种，主要取决于为其选择的颁发实体和颁发方法。可以将使用内部实体或外部实体的凭据提供程序区分开来：

- 任意实体属于内部实体，位于 XenMobile 内部。任意实体的颁发方法始终为签名。签名意味着，在执行每个颁发操作时，XenMobile 都将使用为该实体选择的 CA 证书给新密钥对签名。该密钥对是在设备上生成还是在服务器上生成取决于所选的分发方法。
- 外部实体包括 Microsoft CA 或 GPKI，属于企业基础结构的一部分。

有关设置 DigiCert 托管 PKI（包括创建凭据提供程序）的详细信息，请参阅 PKI 实体中的 “DigiCert 托管 PKI”。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标，然后单击设置 **>** 凭据提供程序。
2. 在凭据提供程序页面上，单击添加。

   此时将显示凭据提供程序**:** 常规信息页面。
3. 在凭据提供程序**:** 常规信息页面上，执行以下操作：
   - 名称：为新提供程序配置键入唯一名称。此名称之后将用于在 XenMobile 控制台的其他部分标识该配置。
   - 说明：凭据提供程序的说明。尽管此字段为可选字段，但说明可以提供有关此凭据提供程序的有用详细信息。
   - 颁发实体：单击凭据颁发实体。
   - 颁发方法：单击签名或提取以选择系统用于从已配置的实体获取证书的方法。对于客户端证书身份验证，请使用签名。
   - 如果模板列表可用，请为凭据提供程序选择您在 PKI 实体下添加的模板。

     在设置 **> PKI** 实体中添加 Microsoft 证书服务实体时，这些模板将变为可用。
4. 单击 **Next**（下一步）。

   此时将显示凭据提供程序**:** 证书签名请求页面。
5. 在凭据提供程序**:** 证书签名请求页面上，根据您的证书配置来配置以下各项：
   - 密钥算法：选择用于获取新密钥对的密钥算法。可用值为 **RSA**、**DSA** 和 **ECDSA**。
   - 密钥大小：键入密钥对的大小（以位为单位）。此字段为必填字段。

允许的值取决于密钥类型。例如，DSA 密钥的最大大小为 1024 位。为避免出现错误的负值（取决于基础硬件和软件），XenMobile 不强制实施密钥大小。应始终先在测试环境中测试凭据提供程序配置，然后在生产环境中激活这些配置。

- 签名算法：单击用于新证书的值。值取决于密钥算法。
- 使用者名称：必填。键入新证书使用者的标识名 (DN)。例如：`CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \ endquotation`

  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
  - 使用者名称： `cn=$user.username`
- 要向使用者备用名称表中添加新条目，请单击添加。选择备用名称的类型，然后在第二列中键入一个值。

  对于客户端证书身份验证，请指定以下设置：

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

    与“使用者名称”相同，可以在值字段中使用 XenMobile 宏。

6. 单击 **Next**（下一步）。

   此时将显示凭据提供程序**:** 分发页面。

7. 在凭据提供程序**:** 分发页面上，执行以下操作：

   - 在颁发 **CA** 证书列表中，单击提供的 CA 证书。由于凭据提供程序使用任意 CA 实体，因此该凭据提供程序的 CA 证书将始终为在该实体上配置的 CA 证书。CA 证书在此显示是为了与使用外部实体的配置保持一致。
   - 在选择分发模式中，单击以下生成和分发密钥方式中的一种：
     - 首选集中式**:** 服务器端密钥生成： Citrix 建议采用此集中式选项。它支持 XenMobile 支持的所有平台，并且在使用 Citrix Gateway 身份验证时也需要使用此模式。在服务器上生成并存储私钥，然后分发到用户设备。
     - 首选分布式**:** 设备端密钥生成：在用户设备上生成并存储私钥。此分布式模式使用 SCEP 并需要采用 keyUsage keyEncryption 的 RA 加密证书和采用 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可以同时用于加密和签名。
     - 仅限分布式**:** 设备端密钥生成：此选项与“首选分布式: 设备端密钥生成”的工作方式相同，但是此选项是“仅限”而非“首选”，当设备端生成密钥失败或不可用时，没有其他选项可用。

   如果选择首选分布式**:** 设备端密钥生成或仅限分布式**:** 设备端密钥生成，请单击 RA 签名证书和 RA 加密证书。同一个证书可用于这两个目的。此时将显示有关这些证书的新字段。

8. 单击 **Next**（下一步）。

此时将显示凭据提供程序**:** 吊销 **XenMobile** 页面。在此页面上，配置 XenMobile 在内部将通过此提供程序配置颁发的证书标记为吊销的条件。

9. 在凭据提供程序**:** 吊销 **XenMobile** 页面上，执行以下操作：
   - 在吊销已颁发的证书中，选择一个表明何时应吊销证书的选项。
   - 要指示 XenMobile 在吊销证书时发送通知，请将发送通知的值设置为开并选择通知模板。
   - 要在从 XenMobile 吊销证书后在 PKI 上吊销该证书，请将吊销 **PKI** 上的证书设置为开，并在实体列表中，单击某个模板。实体列表将显示具有吊销功能的所有可用 GPKI 实体。从 XenMobile 吊销证书后，吊销调用将发送给在实体列表中选择的 PKI。
10. 单击 **Next**（下一步）。

    此时将显示凭据提供程序**:** 吊销 **PKI** 页面。请在此页面上指出吊销证书时应对 PKI 执行的操作。您还可以选择创建通知消息。
11. 在凭据提供程序**:** 吊销 **PKI** 页面上，如果要从 PKI 吊销证书，请执行以下操作：
    - 将启用外部吊销检查设置更改为开。此时将显示更多与吊销 PKI 相关的字段。
    - 在 **OCSP** 响应者 **CA** 证书列表中，单击证书使用者的标识名 (DN)。

      可以为 DN 字段值使用 XenMobile 宏。例如：`CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \ endquotation`
    - 在吊销证书时列表中，单击吊销证书时对 PKI 实体执行的以下操作之一：
      - 不执行任何操作。
      - 续订证书。
      - 吊销和擦除设备。
    - 要指示 XenMobile 在吊销证书时发送通知，请将发送通知的值设置为开。

      可以从两个通知选项中选择：
    - 如果选择选择通知模板，则可以选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
    - 如果选择输入通知详细信息，则可以自行编写通知消息。除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。
12. 单击 **Next**（下一步）。

    此时将显示凭据提供程序**:** 续订页面。在此页面上，您可以配置 XenMobile 以使其执行以下操作：
    - 续订证书。可以选择在续订时发送通知，以及选择从操作中排除已过期的证书。
    - 为即将过期的证书发送通知（续订前通知）。
13. 在凭据提供程序**:** 续订页面上，如果要在证书过期时进行续订，请执行以下操作：

    将在证书过期时续订设置为开。此时将显示更多字段。

- 在证书在此时间内提供时续订字段中，键入在过期前多少天续订证书。
- （可选）选择不续订已过期的证书。在此情况下，“已过期”表示证书的“NotAfter”日期在过去，不是指证书已被吊销。在内部吊销证书后，XenMobile 不会续订这些证书。

要指示 XenMobile 在续订证书时发送通知，请将发送通知设置为开。要指示 XenMobile 在证书接近过期时发送通知，请将证书即将过期时通知设置为开。
对于其中任一选择方式，可以从两个通知选项中选择：

- 选择通知模板：选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
- 输入通知详细信息：自行编写通知消息。提供收件人电子邮件地址、消息和频率，以便发送通知。

在证书在此时间内提供时通知字段中，键入在证书过期前多少天发送通知。

14. 单击保存。

    凭据提供程序将显示在“凭据提供程序”表中。

APNs 证书

January 5, 2022

> 重要：
>
> Apple 对 APNs 旧版二进制文件协议的支持将于 2021 年 3 月 31 日结束。Apple 建议您改为使用基于 HTTP/2 的 APNs 提供程序 API。自版本 10.13.0 起，XenMobile Server 支持基于 HTTP/2 的 API。有关更多信息，请参阅 https://developer.apple.com/ 中的新闻更新 “Apple 推送通知服务更新”。有关检查与 APN 的连接的帮助，请参阅连接检查。

要在 XenMobile 中注册并管理 iOS 和 macOS 设备，应设置 Apple 提供的 Apple 推送通知服务 (APNs) 证书。

工作流程摘要：

- 步骤 **1**：通过以下任一方法创建证书签名请求 (CSR)：
  - 在 macOS 上使用钥匙串访问创建 CSR（Citrix 推荐使用）
  - 使用 Microsoft IIS 创建 CSR
  - 使用 OpenSSL 创建 CSR
- 步骤 **2**：在 XenMobile Tools 中为 CSR 签名
- 步骤 **3**： 将已签名的 CSR 提交到 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：
  - 在 macOS 上使用钥匙串访问创建 PKCS #12 文件
  - 使用 Microsoft IIS 创建 PKCS #12 文件
  - 使用 OpenSSL 创建 PKCS #12 文件

- 步骤 **5**：将 APNs 证书导入 XenMobile
- 步骤 **6**：续订 APNs 证书

创建证书签名请求

我们建议您在 macOS 上使用钥匙串访问来创建 CSR。还可以通过 Microsoft IIS 或 OpenSSL 创建 CSR。

> 重要：
>
> - 对于用于创建证书的 Apple ID：
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.
>   - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device reenrollment.
> - 如果您无意或有意吊销了该证书，则无法管理自己的设备。
> - 如果使用 iOS Developer Enterprise Program 创建移动设备管理器推送证书：请务必在 Apple Push Certificates Portal 中处理面向迁移的证书的任何操作。

在 **macOS** 上使用钥匙串访问创建 **CSR**

1. 在运行 macOS 的计算机上，在应用程序 **>** 实用工具下方，启动钥匙串访问应用程序。
2. 打开钥匙串访问菜单，然后单击证书助理 **>** 从证书颁发机构请求证书。
3. “证书助理”将提示您输入以下信息：
   - 电子邮件地址：负责管理证书的个人或角色帐户的电子邮件地址。
   - 公用名：负责管理证书的个人或角色帐户的公用名。
   - **CA** 电子邮件地址：证书颁发机构的电子邮件地址。
4. 选择存储到磁盘和让我指定密钥对信息选项，然后单击继续。
5. 输入 CSR 文件的名称，在您的计算机上保存此文件，然后单击保存。
6. 指定密钥对信息：选择密钥大小 2048 位以及 **RSA** 算法，然后单击继续。作为 APNs 证书流程的一部分，CSR 文件已可供上载。
7. 证书助理完成 CSR 流程后，单击完成。
8. 要继续，请为 CSR 签名。

使用 **Microsoft IIS** 创建 **CSR**

生成 APNs 证书请求的第一步是创建证书签名请求 (CSR)。对于 Windows，请通过使用 Microsoft IIS 生成 CSR。

1. 打开 Microsoft IIS。
2. 双击 IIS 的服务器证书图标。
3. 在服务器证书窗口中，单击创建证书申请。

4. 键入相应的标识名 (DN) 信息，然后单击下一步。
5. 为加密服务提供程序选择 **Microsoft RSA SChannel Cryptographic Provider**，并为位长度选择 **2048**，然后单击下一步。
6. 输入文件名并指定 CSR 的保存位置，然后单击完成。
7. 要继续，请为 CSR 签名。

使用 **OpenSSL** 创建 **CSR**

如果无法使用 macOS 设备或 Microsoft IIS 生成 CSR，请使用 OpenSSL。可以从 OpenSSL Web 站点下载并安装 OpenSSL。

1. 在安装了 OpenSSL 的计算机上，从命令提示窗口或 Shell 执行以下命令。

```
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.
csr -newkey rsa:2048
```

2. 此时将显示以下要求证书命名信息的消息。根据请求输入信息。

```
1  You are about to be asked to enter information that will be
       incorporated into your certificate request.
2  What you are about to enter is what is called a Distinguished Name
       or a DN.
3  There are quite a few fields but you can leave some blank
4  For some fields there will be a default value,
5  If you enter '.', the field will be left blank.
6  -----
7  Country Name (2 letter code) [AU]:US
8  State or Province Name (full name) [Some-State]:CA
9  Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
       Customer
11 Organizational Unit Name (eg, section) [:Marketing
12 Common Name (eg, YOUR name) []:John Doe
13 Email Address []:john.doe@customer.com
14 <!--NeedCopy-->
```

3. 在下一条消息中，输入 CSR 私钥的密码。

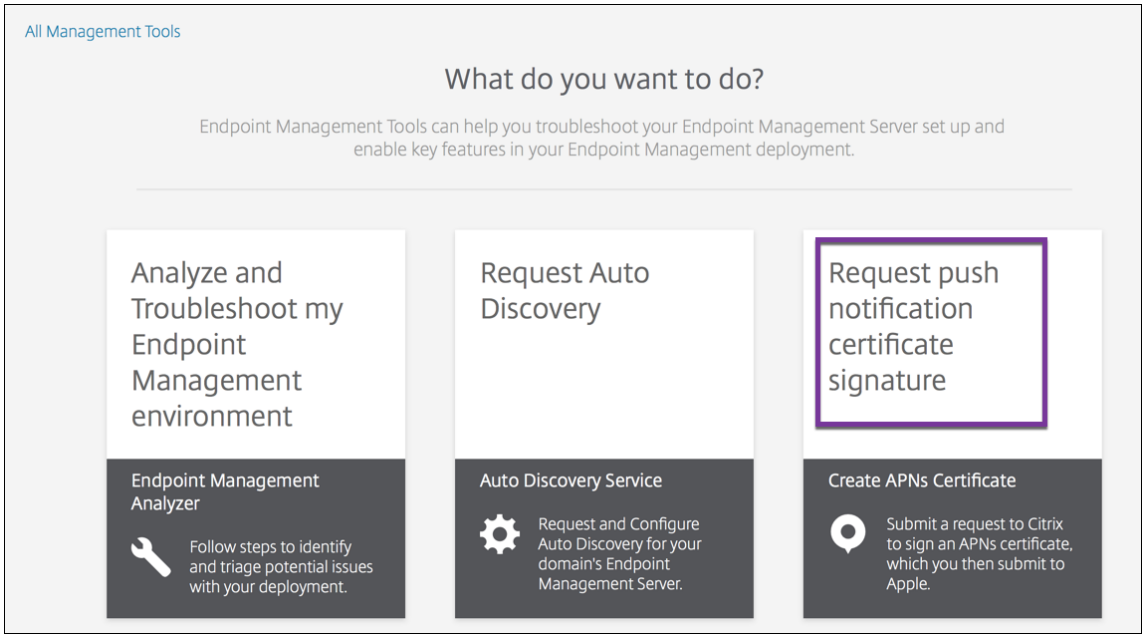
```
1  Please enter the following 'extra' attributes
2  to be sent with your certificate request
3  A challenge password []:
4  An optional company name []:
5  <!--NeedCopy-->
```

4. 要继续，请按照下一节中的说明为 CSR 签名。

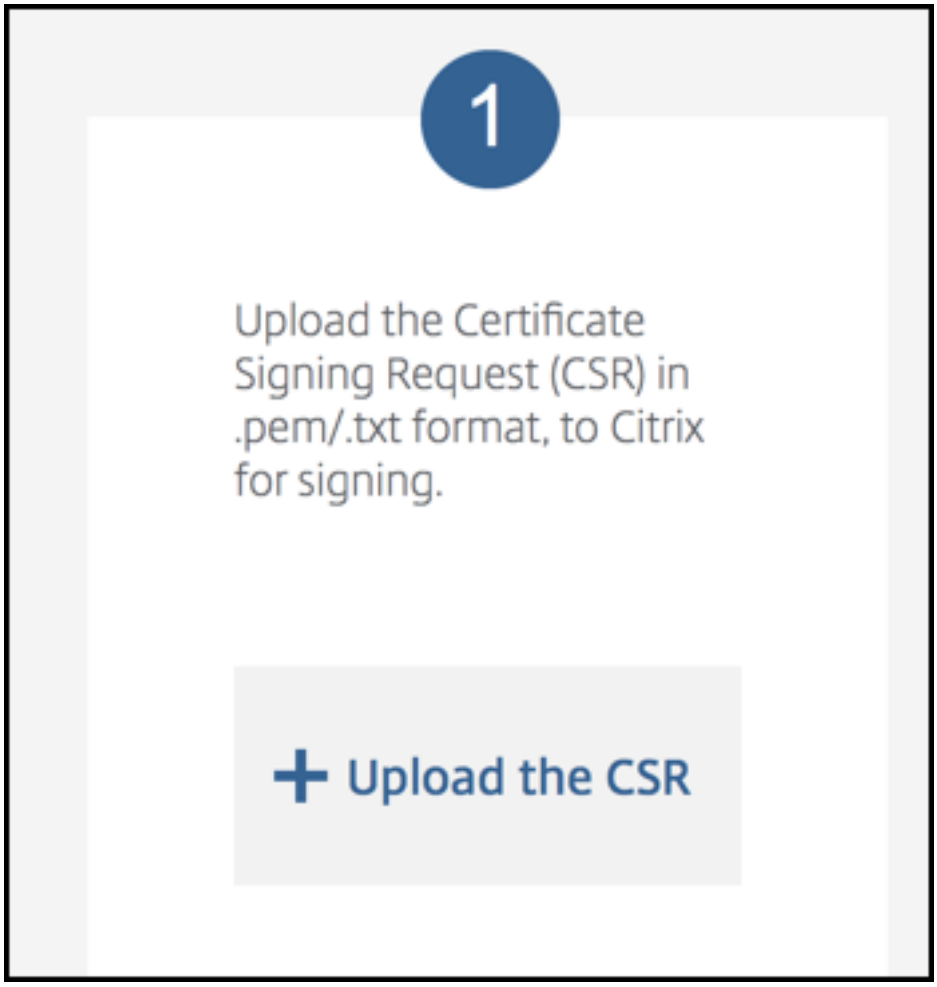
为 **CSR** 签名

要将证书与 XenMobile 一起使用，请将其提交给 Citrix 进行签名。Citrix 使用其移动设备管理签名证书给 CSR 签名并返回 `.plist` 格式的已签名文件。

1. 在浏览器中，转至 Endpoint Management Tools Web 站点，然后单击 **Request push notification certificate signature**（申请推送通知证书签名）。



2. 在创建新证书页面上，单击上载 **CSR**。



3. 浏览并选择证书。

   证书必须采用.pem/txt 格式。

4. 在 **Endpoint Management APNs CSR Signing**（Endpoint Management APNs CSR 签名）页面上，单击 **Sign**（签名）。将为 CSR 签名并将签名后的 CSR 自动保存到已配置的下载文件夹。

5. 要继续，请按照下一节中的说明提交签名的 CSR。

将签名后的 **CSR** 提交给 **Apple** 以获取 **APNs** 证书

从 Citrix 收到已签名的证书签名请求 (CSR) 后，将 CSR 提交给 Apple，以获取导入到 XenMobile 所需的 APNs 证书。

> 注意：
>
> 有些用户报告登录 Apple 推送门户时遇到问题。或者，登录 Apple 开发人员门户，然后按照以下步骤进行操作。

1. 在浏览器中，转到 Apple Push Certificates Portal。
2. 单击 **Create a Certificate**（创建证书）。

3. 首次使用 Apple 创建证书：选中 **I have read and agree to these terms and conditions**（我已阅读并同意这些条款和条件）复选框，然后单击 **Accept**（接受）。
4. 单击 **Choose File**（选择文件），浏览到计算机上已签名的 CSR，然后单击 **Upload**（上载）。此时将显示一条确认消息，指示上载成功。
5. 单击 **Download**（下载）以检索.pem 证书。
6. 要继续，请完成 CSR 并导出 PKCS #12 文件，如下一节中所述。

完成 **CSR** 并导出 **PKCS #12** 文件

收到 Apple 提供的 APNs 证书后，返回到钥匙串访问、Microsoft IIS 或 OpenSSL 以将证书导出到 PCKS #12 文件中。

PCKS #12 文件包含 APNs 证书文件和您的私钥。PFX 文件的扩展名通常为.pfx 或.p12。可以互换使用.pfx 和.p12 文件。

> 重要：
>
> Citrix 建议您保存或导出本地系统中的个人密钥和公钥。您需要密钥来访问 APNs 证书以便重复使用。如果没有相同的密钥，您的证书无效，您必须重复执行整个 CSR 和 APNs 过程。

在 **macOS** 上使用钥匙串访问创建 **PKCS #12** 文件

> 重要：
>
> 在此任务中使用的 macOS 设备应与生成 CSR 时使用的 macOS 设备相同。

1. 在设备上，找到从 Apple 收到的生产标识 (.pem) 证书。
2. 启动钥匙串访问应用程序并导航到登录 **>** 我的证书选项卡。将产品标识证书拖放到打开的窗口中。
3. 单击证书并展开左箭头以验证证书是否包含关联的私钥。
4. 要开始将证书导出到 PCKS #12 (.pfx) 证书中，请选择证书和私钥，单击鼠标右键，然后选择导出 **2** 个项目。
5. 为证书文件提供唯一的名称以用于 XenMobile。请勿在名称中包含空格字符。然后，为保存的证书选择一个文件夹位置，选择.pfx 文件格式，然后单击保存。
6. 输入用于导出证书的密码。Citrix 建议使用具有唯一性的强密码。还要确保证书和密码的安全性，以供以后使用和引用。
7. 钥匙串访问应用程序将提示您输入登录密码或选定的钥匙串。键入密码，然后单击确定。保存的证书现在即可用于 XenMobile Server。
8. 要继续操作，请参阅将 APNs 证书导入到 XenMobile。

使用 **Microsoft IIS** 创建 **PKCS #12** 文件

> 重要：
>
> 在此任务中使用的 IIS 服务器应与生成 CSR 时使用的 IIS 服务器相同。

1. 打开 Microsoft IIS。
2. 单击服务器证书图标。
3. 在服务器证书窗口中，单击完成证书申请。
4. 浏览至来自 Apple 的 Certificate.pem 文件。然后，键入友好名称或证书名称，并单击确定。请勿在名称中包含空格字符。
5. 选择在步骤 4 中找到的证书，然后单击导出。
6. 指定.pfx 证书的位置和文件名以及密码，然后单击确定。

   您需要证书的密码才能将其导入 XenMobile。
7. 将.pfx 证书复制到计划安装 XenMobile 的服务器上。
8. 要继续操作，请参阅将 APNs 证书导入到 XenMobile。

使用 **OpenSSL** 创建 **PKCS #12** 文件

如果您使用 OpenSSL 创建 CSR，还可以使用 OpenSSL 创建.pfx APNs 证书。

1. 在命令提示符或 shell 下，执行以下命令。`Customer.privatekey.pem` 为来自 CSR 的私钥。`APNs_Certificate.pem` 为您刚从 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。记住此密码，因为在将证书上载到 XenMobile 时要再次使用该密码。
3. 记下.pfx 证书文件的位置。然后，将该文件复制到 XenMobile Server 中，以便可以使用控制台上载文件。
4. 要继续，请将 APNs 证书导入 XenMobile，如下一节中所述。

将 **APNs** 证书导入到 **XenMobile**

在收到新 APNs 证书后：将 APNs 证书导入 XenMobile，以便首次添加该证书或者替换证书。

1. 在 XenMobile 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 XenMobile 中的证书的详细信息，请参阅证书和身份验证。

续订 **APNs** 证书

> 重要：
>
> 如果您在续订过程中使用其他 Apple ID，则必须重新注册用户设备。

要续订 APNs 证书，请执行创建证书的步骤，然后转到 Apple Push Certificates Portal。使用该门户上载新证书。登录后，将显示您的现有证书或者从您之前的 Apple 开发人员帐户导入的证书。

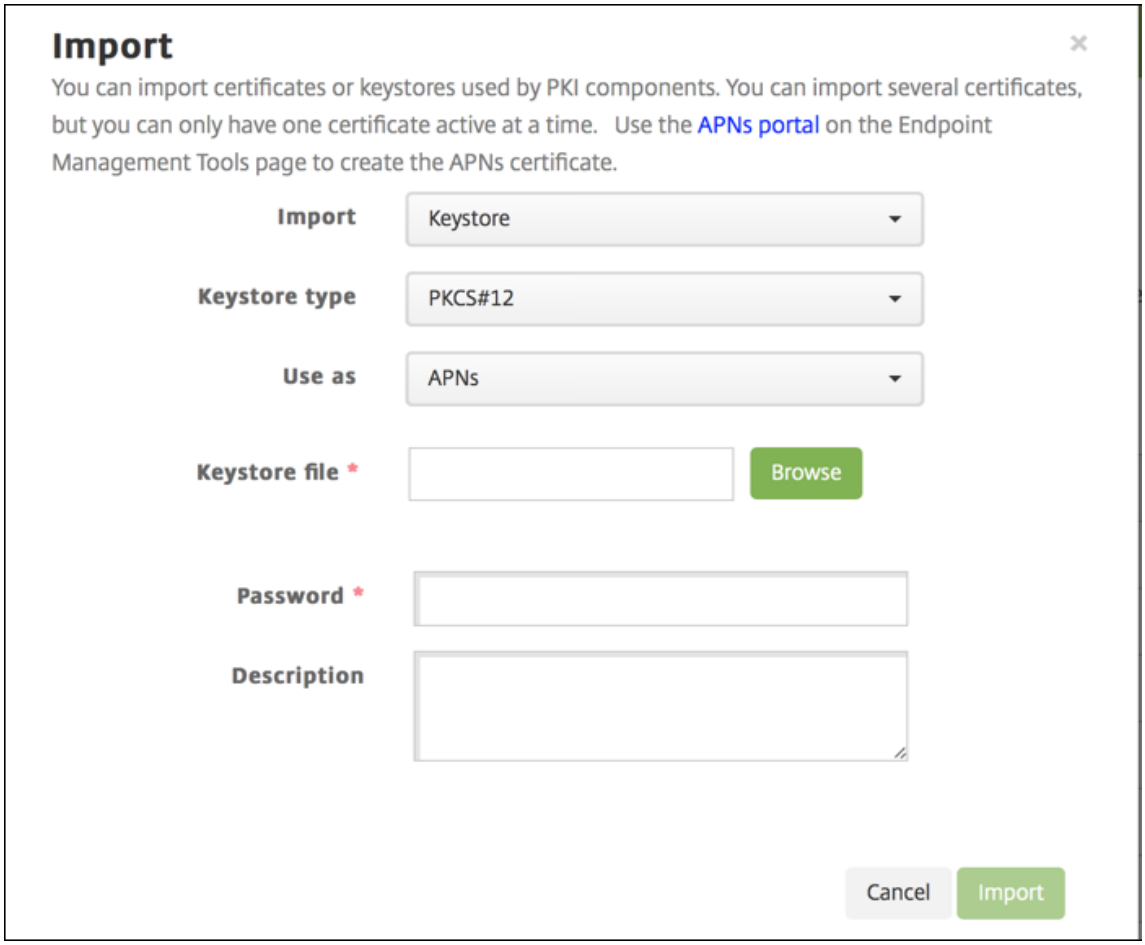
在 Certificates Portal 中，续订证书的唯一区别是要单击 **Renew**（续订）。您必须在 Certificates Portal 上拥有开发人员帐户才能访问该站点。要续订证书，请使用相同的组织名称和 Apple ID。

要确定 APNs 证书的过期时间，请在 XenMobile 控制台中转至设置 **>** 证书。如果证书过期，请不要吊销。

1. 使用 Microsoft IIS、钥匙串访问 (macOS) 或 OpenSSL 生成 CSR。有关生成 CSR 的详细信息，请参阅创建证书签名请求。
2. 在浏览器中，转到 XenMobile Tools。然后，单击 **Request push notification certificate signature**（申请推送通知证书签名）。
3. 单击 **+ Upload the CSR**（+ 上载 CSR）。
4. 在对话框中，导航到 CSR，单击 **Open**（打开），然后单击 **Sign**（签名）。
5. 收到 `.plist` 文件时，将其保存。
6. 在步骤 3 标题中，单击 **Apple Push Certificates Portal** 并登录。
7. 选择要续订的证书，然后单击 **Renew**（续订）。
8. 上载 `.plist` 文件。您将收到输出文件.pem。保存.pem 文件。
9. 使用该.pem 文件完成 CSR（根据您在步骤 1 中创建 CSR 时使用的方法）。
10. 将证书导出为.pfx 文件。

在 XenMobile 控制台中，导入.pfx 文件并按如下所示完成配置：

1. 转到设置 **>** 证书 **>** 导入。
2. 在导入菜单中，选择密钥库。
3. 在密钥库类型菜单中，选择 **PKCS #12**。
4. 在用作中，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. 键入可选说明。
8. 单击导入。

XenMobile 将您重定向回证书页面。名称、状态、有效期开始时间和有效期结束时间字段将更新。

SAML 单点登录与 Citrix Files

January 5, 2022

可以将 XenMobile 和 Citrix Content Collaboration 配置为使用安全声明标记语言 (SAML) 来提供对 Citrix Files 移动应用程序的单点登录 (SSO) 访问。此功能包括：

- 使用 MDX Toolkit 启用或封装 MAM SDK 的 Citrix Files 应用程序
- 未封装的 Citrix Files 客户端，例如 Web 站点、Outlook 插件或同步客户端

- 适用于打包的 **Citrix Files** 应用程序。通过 Citrix Files 移动应用程序登录 Citrix Files 的用户将被重定向到 Secure Hub 进行用户身份验证以及获取 SAML 令牌。成功进行身份验证后，Citrix Files 移动应用程序会将 SAML 令牌发送到 Content Collaboration。初始登录后，用户可以通过 SSO 访问 Citrix Files 移动应用程序。还可以将附件从 Content Collaboration 附加到 Secure Mail 邮件，而不需要每次都登录。
- 对于未打包的 **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 XenMobile。XenMobile 对用户进行身份验证，然后用户获取发送到 Content Collaboration 的 SAML 令牌。初始登录后，用户可以通过 SSO 访问 Citrix Files 客户端，而不需要每次都登录。

要将 XenMobile 作为 SAML 身份提供程序 (IdP) 用于 Content Collaboration，必须将 XenMobile 配置为使用企业帐户，如本文中所述。或者，可以将 XenMobile 配置为只与存储区域连接器一起使用。有关详细信息，请参阅将 Citrix Content Collaboration 与 XenMobile 结合使用。

有关详细的参考体系结构图，请参阅体系结构。

必备条件

先完成以下必备条件，才能对 XenMobile 和 Citrix Files 应用程序配置 SSO：

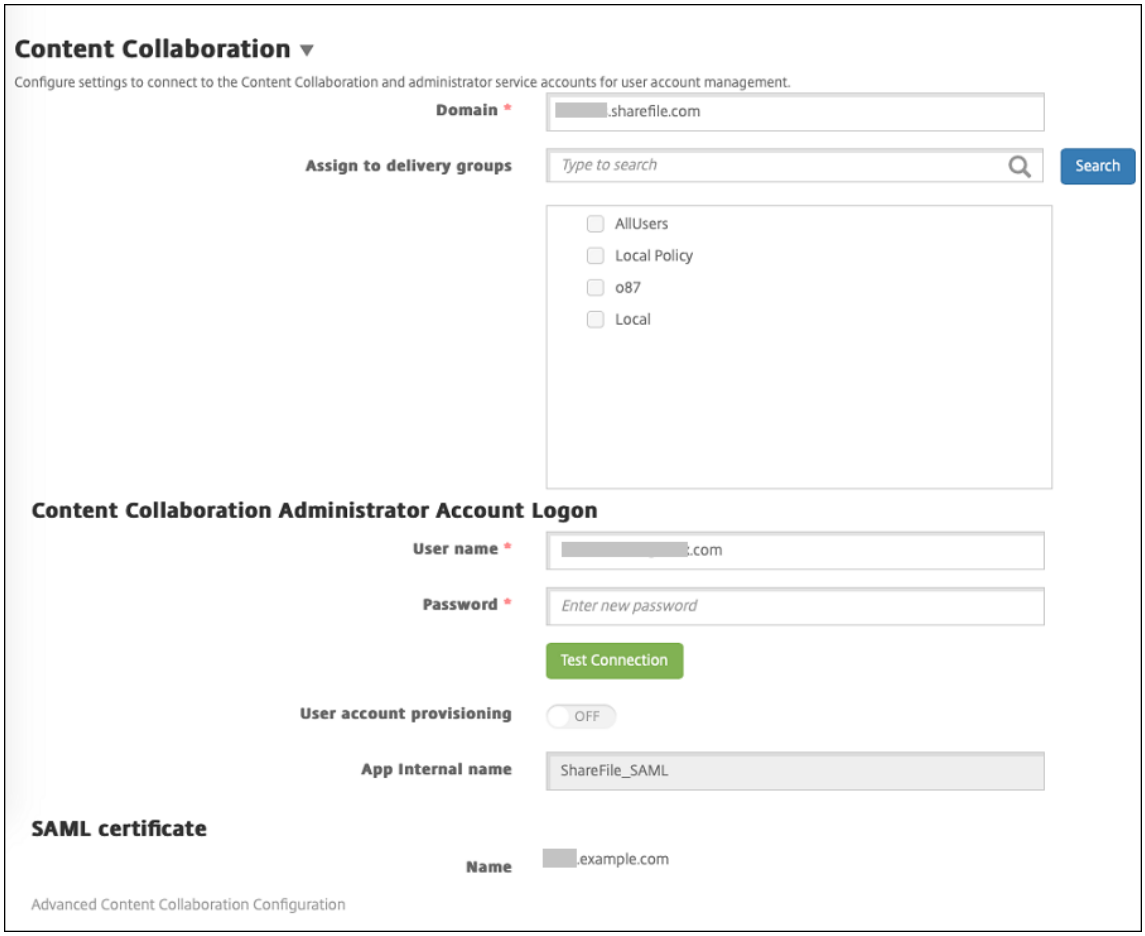
- MAM SDK 或兼容版本的 MDX Toolkit（适用于 Citrix Files 移动应用程序）。

  有关详细信息，请参阅 XenMobile 兼容性。
- 兼容版本的 Citrix Files 移动应用程序和 Secure Hub。
- Content Collaboration 管理员帐户。
- 通过验证的 XenMobile 与 Content Collaboration 之间的连接。

配置 **Content Collaboration** 访问权限

在为 Content Collaboration 设置 SAML 之前，请按以下方式提供 Content Collaboration 访问信息：

1. 在 XenMobile Web 控制台中，单击配置 **> ShareFile**。此时将显示 **ShareFile** 配置页面。您的控制台可能会显示术语 Content Collaboration，而非 ShareFile。



2. 配置以下设置：
   - 域：键入您的 Content Collaboration 子域名。例如：`example.sharefile.com`。
   - 分配给交付组：选择或搜索希望能够对 Content Collaboration 使用 SSO 的交付组。
   - **ShareFile** 管理员帐户登录
   - 用户名：键入 Content Collaboration 管理员用户名。此用户必须具有管理员权限。
   - 密码：键入 Content Collaboration 管理员密码。
   - 用户帐户预配：保留此设置处于禁用状态。使用 Citrix Content Collaboration 用户管理工具进行用户预配。请参阅预配用户帐户和通讯组。
3. 单击测试连接按钮以确认 Content Collaboration 管理员帐户的用户名和密码是否可以向指定的 Content Collaboration 帐户进行身份验证。
4. 单击保存。
   - XenMobile 将与 Content Collaboration 同步并更新 Content Collaboration 设置 **ShareFile** 颁发者/实体 **ID** 和登录 **URL**。
   - 配置 **> ShareFile** 页面显示应用程序内部名称。您需要该名称才能完成后面在修改 Citrix Files.com SSO 设置中介绍的步骤。

为封装的 **Citrix Files MDX** 应用程序设置 **SAML**

对于包含封装的 Citrix Files MDX 应用程序的单点登录配置，您无需使用 Citrix Gateway。要为未封装的 Citrix Files 客户端（例如 Web 站点、Outlook 插件或同步客户端）配置访问权限，请参阅为其他 Citrix Files 客户端配置 Citrix Gateway。

以下步骤适用于 iOS 和 Android 应用程序和设备。要为封装的 Citrix Files MDX 应用程序配置 SAML，请执行以下操作：

1. 使用 MDX Toolkit 打包 Citrix Files 移动应用程序。有关使用 MDX Toolkit 打包应用程序的详细信息，请参阅使用 MDX Toolkit 打包应用程序。
2. 在 XenMobile 控制台中，上载打包的 Citrix Files 移动应用程序。有关上载 MDX 应用程序的信息，请参阅向 XenMobile 中添加 MDX 应用程序。
3. 验证 SAML 设置：使用在前面配置的管理员用户名和密码登录 Content Collaboration。
4. 确认为 Content Collaboration 和 XenMobile 配置了相同的时区。确保 XenMobile 按配置的时区显示正确时间。如果不正确，SSO 可能会失败。

验证 **Citrix Files** 移动应用程序

1. 在用户设备上，安装和配置 Secure Hub。
2. 从 XenMobile Store 下载并安装 Citrix Files 移动应用程序。
3. 启动 Citrix Files 移动应用程序。Citrix Files 将启动，但不提示输入用户名和密码。

使用 **Secure Mail** 验证

1. 在用户设备上，如果尚未安装和配置 Secure Hub，请进行安装和配置。
2. 从 XenMobile Store 下载、安装并设置 Secure Mail。
3. 打开新的电子邮件窗体，并轻按从 **Citrix Files** 附加。此时将显示可以附加到电子邮件中的文件，但不提示输入用户名或密码。

为其他 **Citrix Files** 客户端配置 **Citrix Gateway**

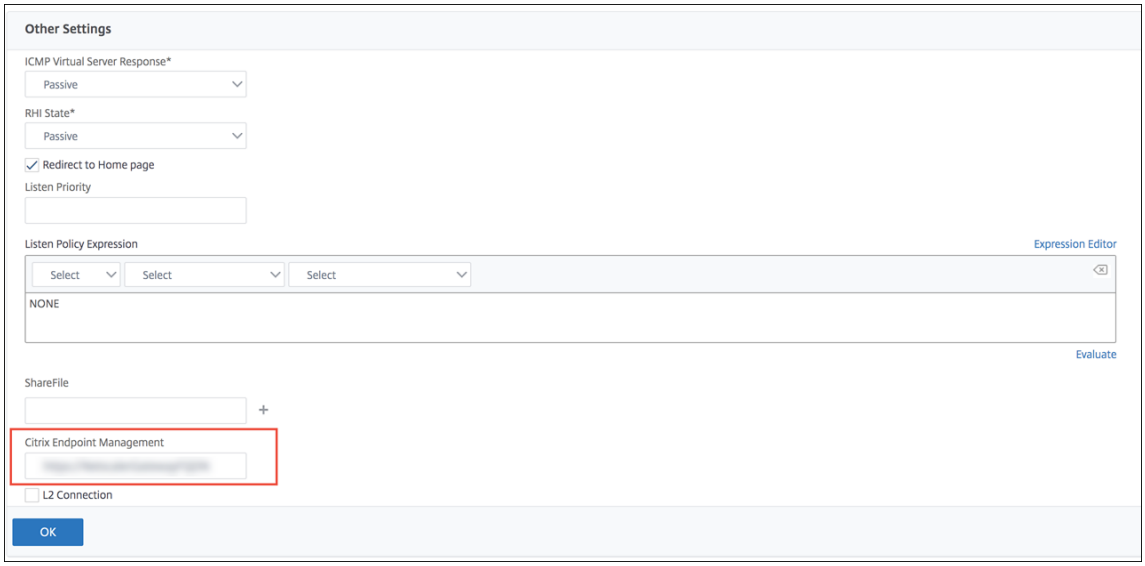
要配置对未打包的 Citrix Files 客户端（例如 Web 站点、Outlook 插件或同步客户端）的访问，请将 Citrix Gateway 配置为支持将 XenMobile 用作 SAML 身份提供程序，如下所示。

- 禁用主页重定向。
- 创建 Citrix Files 会话策略和配置文件。
- 在 Citrix Gateway 虚拟服务器上配置策略。

禁用主页重定向

对通过 /cginfra 路径发出的请求禁用默认行为。执行该操作后，用户将看到最初请求的内部 URL，而非配置的主页。

1. 编辑用于 XenMobile 登录的 Citrix Gateway 虚拟服务器的设置。在 Citrix ADC 中，转至 **Other Settings**（其他设置），然后取消选中标签为 **Redirect to Home Page**（重定向到主页）的复选框。



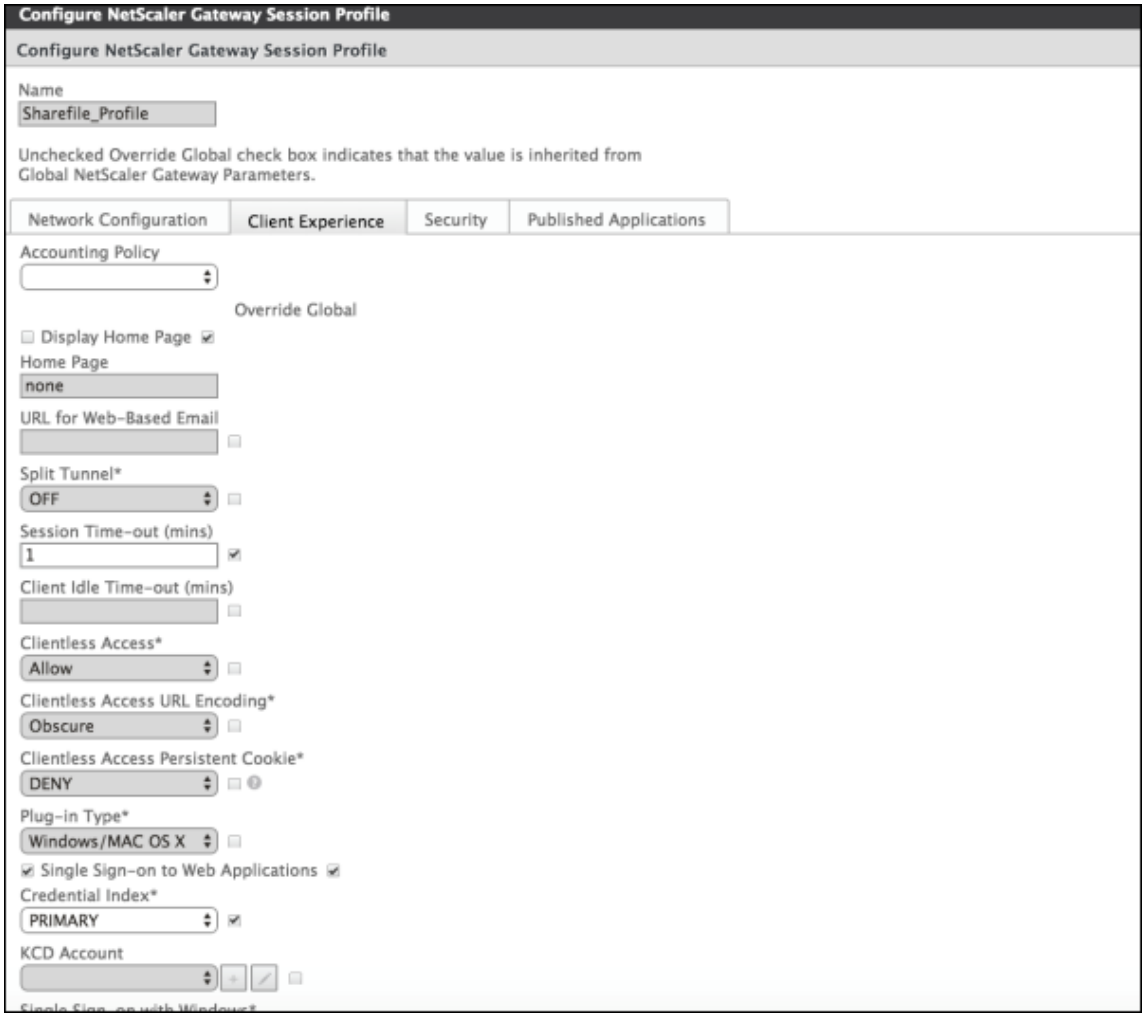
2. 在 **ShareFile**（现在称为 Content Collaboration）下方，键入 XenMobile 内部服务器的名称和端口号。
3. 在 **Citrix Endpoint Management** 下，键入您的 XenMobile URL。您的 Citrix Gateway 版本可能会引用较旧的产品名称 **AppController**。

   此配置授权您向通过 /cginfra 路径输入的 URL 发送请求。

创建 **Citrix Files** 会话策略并请求配置文件

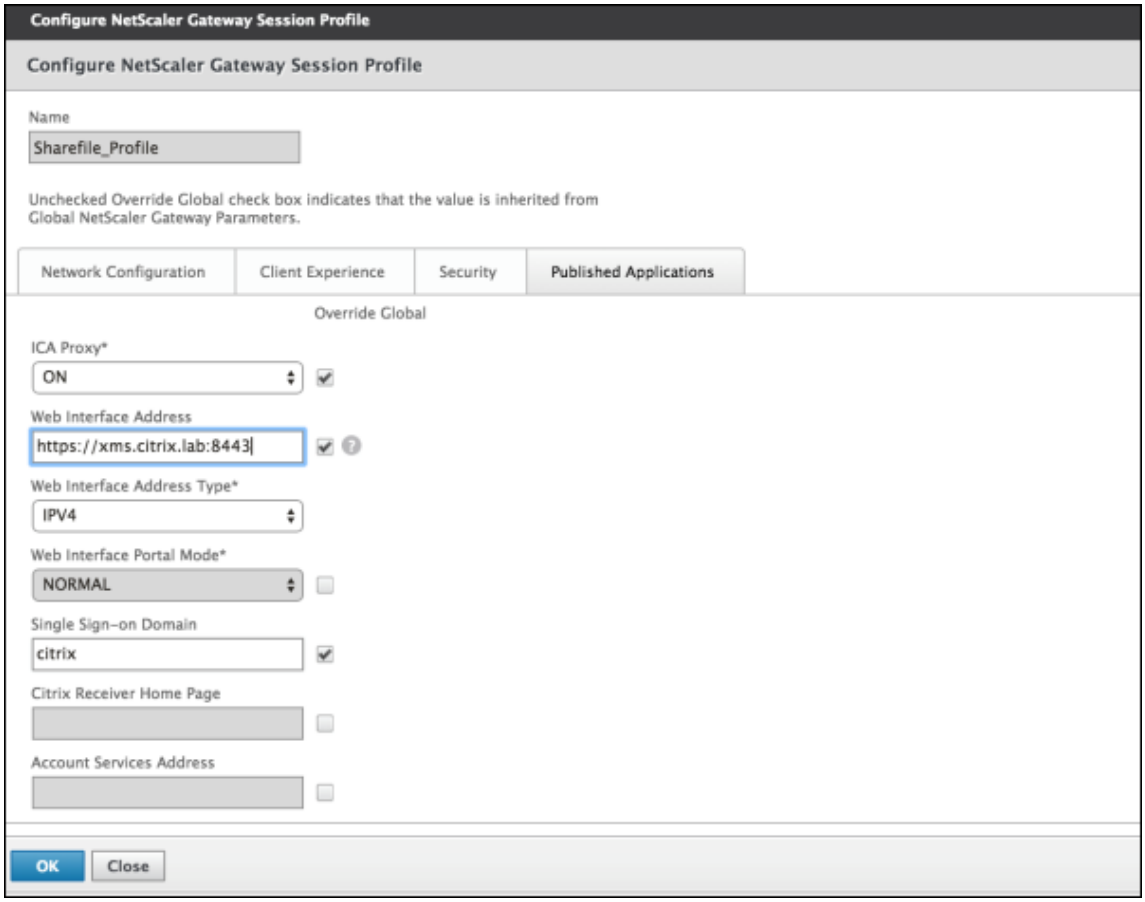
请配置以下设置以创建 Citrix Files 会话策略并请求配置文件：

1. 在 Citrix Gateway 配置实用程序的左侧导航窗格中单击 **Citrix Gateway > Policies**（策略）**> Session**（会话）。
2. 创建会话策略。在 **Policies**（策略）选项卡上，单击 **Add**（添加）。
3. 在 **Name**（名称）字段中，键入 **ShareFile_Policy**。
4. 单击 **+** 按钮创建操作。此时将显示 **Create Session Profile**（创建会话配置文件）页面。



配置以下设置：

- **Name**（名称）：键入 **ShareFile_Profile**。
- 单击 **Client Experience**（客户端体验）选项卡，然后配置以下设置：
  - **Home Page**（主页）：键入 **none**（无）。
  - **Session Time-out (mins)**（会话超时 **(**分钟**)**）：键入 **1**。
  - **Single Sign-on to Web Applications**（单点登录到 **Web** 应用程序）：选择此设置。
  - **Credential Index**（凭据索引）：单击 **PRIMARY**（主要）。
- 单击 **Published Applications**（已发布的应用程序）选项卡。

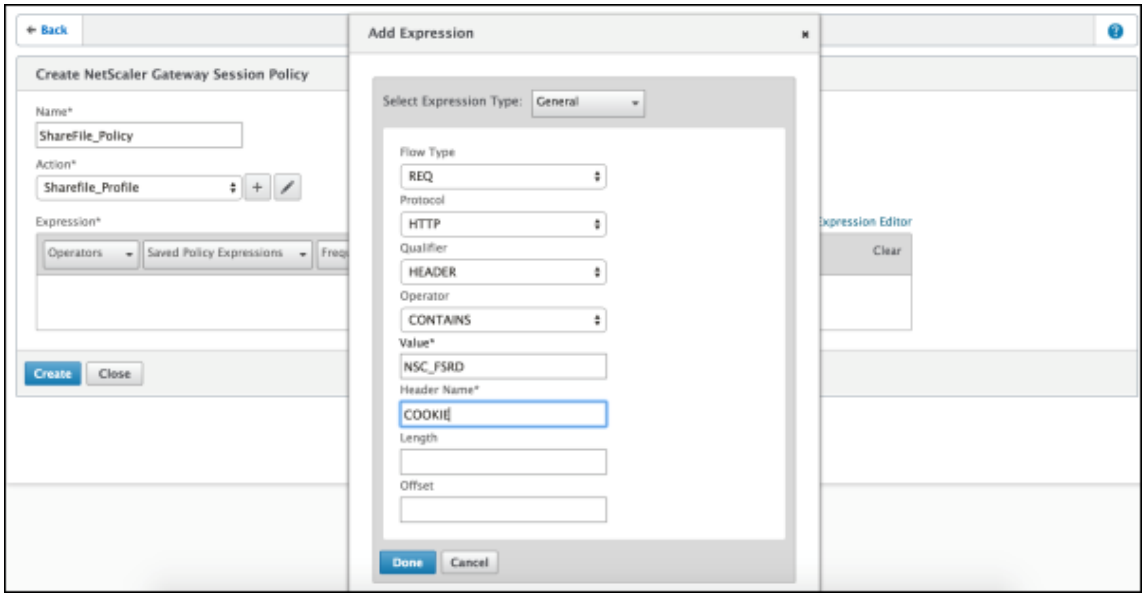


配置以下设置：

- **ICA Proxy**（**ICA** 代理）：单击 **ON**（开）。
- **Web Interface Address**（**Web Interface** 地址）：键入 XenMobile Server 的 URL。
- **Single Sign-on Domain**（单点登录域）：键入 Active Directory 的域名。

  配置 Citrix Gateway 会话配置文件时，**Single Sign-on Domain**（单点登录域）的域后缀必须与在 LDAP 中定义的 XenMobile 域别名匹配。

5. 单击 **Create**（创建）以定义会话配置文件。
6. 单击 **Expression Editor**（表达式编辑器）。



配置以下设置：

- **Value**（值）：键入 **NSC_FSRD**。
- **Header Name**（标头名称）：键入 **COOKIE**。

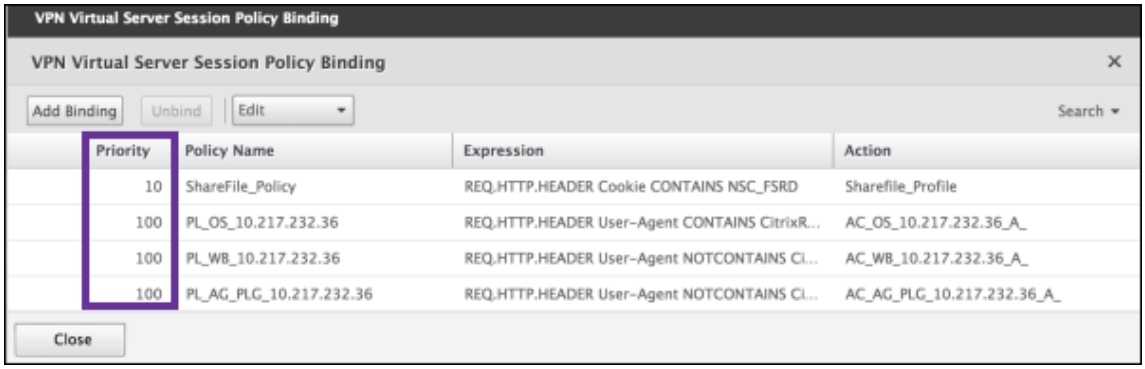
7. 单击 **Create**（创建），然后单击 **Close**（关闭）。

在 **Citrix Gateway** 虚拟服务器上配置策略

在 Citrix Gateway 虚拟服务器上配置以下设置。

1. 在 Citrix Gateway 配置实用程序的左侧导航窗格中单击 **Citrix Gateway > Virtual Servers**（虚拟服务器）。
2. 在 **Details**（详细信息）窗格中，单击 Citrix Gateway 虚拟服务器。
3. 单击编辑。
4. 单击 **Configured policies**（已配置的策略）**> Session policies**（会话策略），然后单击 **Add binding**（添加绑定）。

5. 选择 **ShareFile_Policy**。
6. 编辑为选定策略自动生成的 **Priority**（优先级）编号，以便与列出的任何其他策略相比，其优先级最高（编号最小）。例如：



7. 单击 **Done**（完成），然后保存运行的 Citrix ADC 配置。

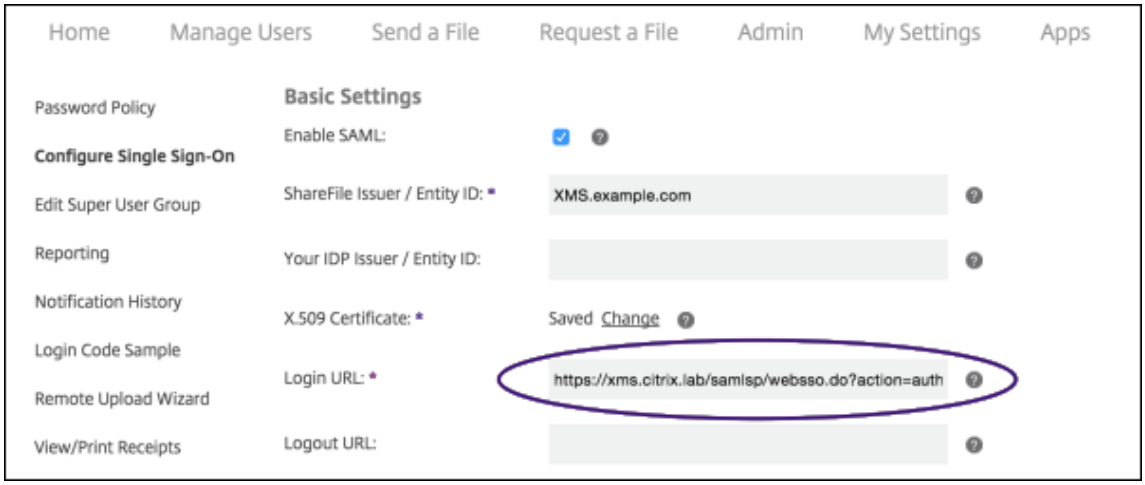
修改 **Citrix Files.com SSO** 设置

针对 MDX 和非 MDX Citrix Files 应用程序进行以下更改。

> 重要：
>
> 内部应用程序名称附加了一个新编号：
>
> - 每次编辑或重新创建 Citrix Files 应用程序时
> - 每次更改 XenMobile 中的 Content Collaboration 设置时
>
> 因此，您还必须在 Citrix Files Web 站点中更新登录 URL，以反映更新后的应用程序名称。

1. 以 Content Collaboration 管理员身份登录到您的 Content Collaboration 帐户 (`https://<subdomain>.sharefile.com`)。
2. 在 Content Collaboration Web 界面中，单击 **Admin**（管理），然后选择 **Configure Single Sign-on**（配置单点登录）。
3. 按如下所示编辑 **Login URL**（登录 URL）：

   下面是编辑之前的 **Login URL**（登录 URL）示例：`https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`。



- 在 XenMobile Server 的 FQDN 前面插入 Citrix Gateway 虚拟服务器的外部 FQDN 和 **/cginfra/https/**，然后在 XenMobile 的 FQDN 后面添加 **8443**。

  下面是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

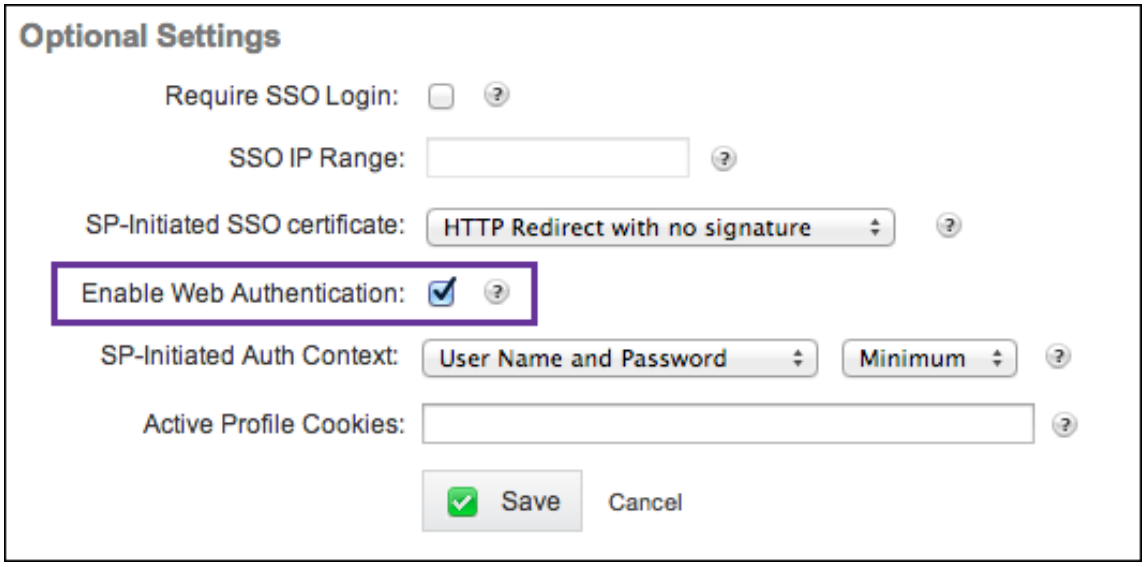
- 将参数 &app=ShareFile_SAML_SP 更改为内部 Citrix Files 应用程序名称。默认情况下，内部名称为 ShareFile_SAML。但是，每次更改配置时，都会向内部名称附加一个数字（ShareFile_SAML_2、ShareFile_SAML_3 等）。可以在配置 **> ShareFile** 页面上查找应用程序内部名称。

  下面是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- 向 URL 的末尾添加 &nssso=**true**。

  下面是最终 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`。

4. 在 **Optional Settings**（可选设置）下方，选中 **Enable Web Authentication**（启用 Web 身份验证）复选框。



验证配置

请执行以下配置以验证设置。

1. 在浏览器中访问 `https://<subdomain>sharefile.com/saml/login`。

   系统会将您重定向到 Citrix Gateway 登录表单。如果未被重定向，请验证前面的配置设置。

2. 输入所配置的 Citrix Gateway 和 XenMobile 环境的用户名和密码。

   此时将在 `<subdomain>.sharefile.com` 下显示您的 Citrix Files 文件夹。如果未显示您的 Citrix Files 文件夹，请确保您输入了正确的登录凭据。

将 **Azure Active Directory** 用作 **IdP**

January 5, 2022

将 Azure Active Directory (AAD) 配置为您的身份提供程序 (IdP) 将允许用户使用其 Azure 凭据在 XenMobile 中注册。

支持 iOS、Android、Windows 10 和 Windows 11 设备。iOS 和 Android 设备通过 Secure Hub 注册。此身份验证方法仅适用于通过 Citrix Secure Hub 在 MDM 中注册的用户。在 MAM 中注册设备时无法使用 AAD 凭据进行身份验证。要将 Secure Hub 与 MDM+MAM 结合使用，请将 XenMobile 配置为使用 Citrix Gateway 进行 MAM 注册。有关详细信息，请参阅 Citrix Gateway 和 XenMobile。

可在设置 **>** 身份验证 **> IDP** 下将 Azure 配置为您的 IdP。**IDP** 页面是此版本的 XenMobile 的新页面。在早期版本的 XenMobile 中，是在设置 **> Microsoft Azure** 下配置 Azure。

要求

- 版本和许可证
  - 要注册 iOS 或 Android 设备，需要 Secure Hub 10.5.5。
  - 要注册 Windows 10 和 Windows 11 设备，需要 Microsoft Azure Premium 许可证。
- 目录服务和身份验证
  - 必须将 XenMobile Server 配置为进行基于证书的身份验证。
  - 如果使用 Citrix ADC 进行身份验证，则必须将 Citrix ADC 配置为进行基于证书的身份验证。
  - Secure Hub 身份验证使用 Azure AD 并遵从在 Azure AD 上定义的身份验证模式。
  - XenMobile Server 必须使用 LDAP 连接到 Windows Active Directory (AD)。将您的本地 LDAP 服务器配置为与 Azure AD 同步。

身份验证流程

设备通过 Secure Hub 注册，并且 XenMobile 配置为使用 Azure 作为其 IdP 时：

1. 用户在自己的设备上在 Secure Hub 中显示的 Azure Active Directory 登录屏幕中输入用户名和密码。
2. Azure AD 验证该用户并发送一个 ID 令牌。
3. Secure Hub 将该 ID 令牌与 XenMobile Server 共享。
4. XenMobile 验证该 ID 令牌以及 ID 令牌中出现的用户信息。XenMobile 返回一个会话 ID。

Azure 帐户设置

要使用 Azure AD 作为 IdP，请先登录您的 Azure 帐户并做以下更改：

1. 注册自定义域并验证域。有关详细信息，请参阅 Add your own domain name to Azure Active Directory（将自己的域名添加到 Azure Active Directory）。
2. 使用目录集成工具，将本地目录扩展到 Azure Active Directory。有关详细信息，请参阅目录集成。

要使用 Azure AD 注册 Windows 10 和 Windows 11 设备，请对您的 Azure 帐户做以下更改：

1. 将 MDM 设为 Azure AD 的可信部分。为此，请单击 **Azure Active Directory >** 应用程序，然后单击添加。
2. 选择从库中添加应用程序。转至移动设备管理，然后选择本地 **MDM** 应用程序。保存设置。

   即使注册加入了 Citrix XenMobile Cloud，也选择本地应用程序。在 Microsoft 术语中，任何非多租户应用程序都属于本地 MDM 应用程序。
3. 在应用程序中，配置 XenMobile Server 发现、端点使用条款和应用程序 ID URI：
   - **MDM** 发现 **URL**： `https://<FQDN>:8443/<instanceName>/wpe`
   - **MDM** 使用条款 **URL**： `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - 应用程序 **ID URI**： `https://<FQDN>:8443/`

4. 选择您在步骤 2 中创建的本地 MDM 应用程序。启用 **Manage devices for these users**（管理这些用户的设备）选项，以便为所有用户或任何特定用户组启用 MDM 管理。

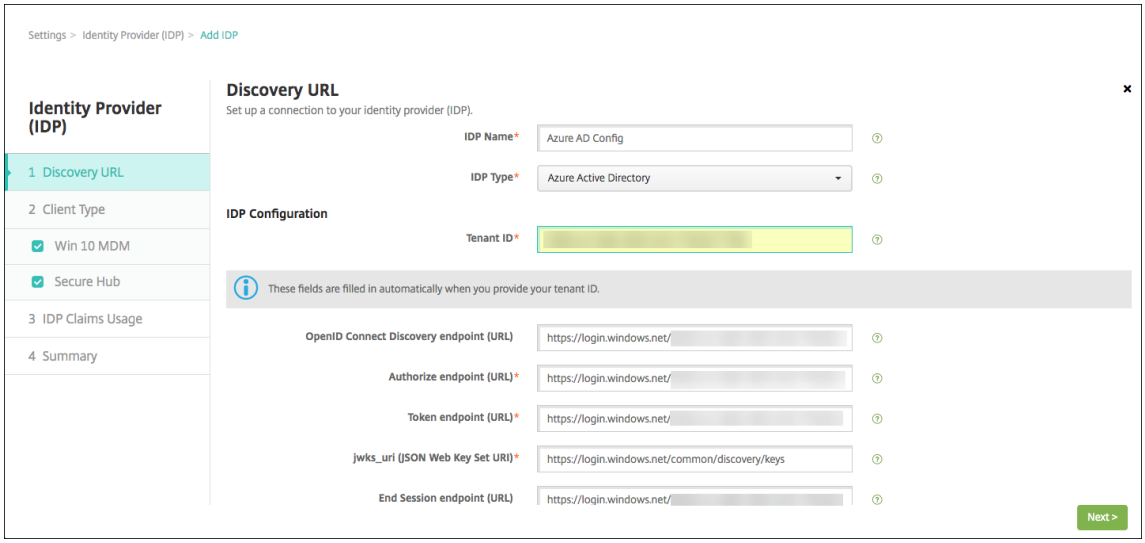
   有关对 Windows 10 和 Windows 11 设备使用 Azure AD 的详细信息，请参阅 Microsoft 文章 Azure Active Directory integration with MDM（Azure Active Directory 与 MDM 的集成）。

将 **Azure AD** 配置为您的 **IdP**

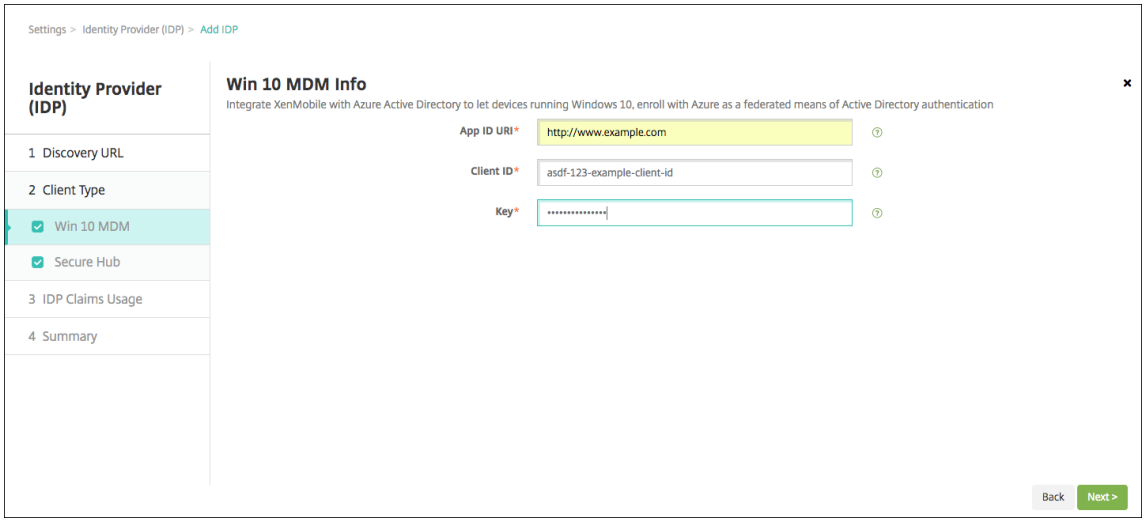
1. 在您的 Azure 帐户中查找或记录所需的信息：
   - 来自 Azure 应用程序设置页面的租户 ID。
   - 如果要使用 Azure AD 注册 Windows 10 和 Windows 11 设备，您还需要：
     - 应用程序 **ID URI**：运行 XenMobile 的服务器的 URL。
     - 客户端 **ID**：“Azure 配置”页面中您的应用程序的唯一标识符。
     - 密钥：来自 Azure 应用程序设置页面。
2. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
3. 在身份验证下方，单击身份提供程序 **(IDP)**。此时将显示身份提供程序页面。

4. 单击添加。此时将显示 **IDP** 配置页面。
5. 配置与您的 IdP 有关的以下信息：
   - **IDP** 名称：键入要创建的 IdP 连接的名称。
   - **IDP** 类型：选择 Azure Active Directory 作为您的 IdP 类型。
   - 租户 **ID**：从 Azure 应用程序设置页面复制此值。在浏览器地址栏中，复制由数字和字母组成的部分。

   例如，在 `https://manage.windowszaure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...` 中，租户 ID 为：`abc123-abc123-abc123`。



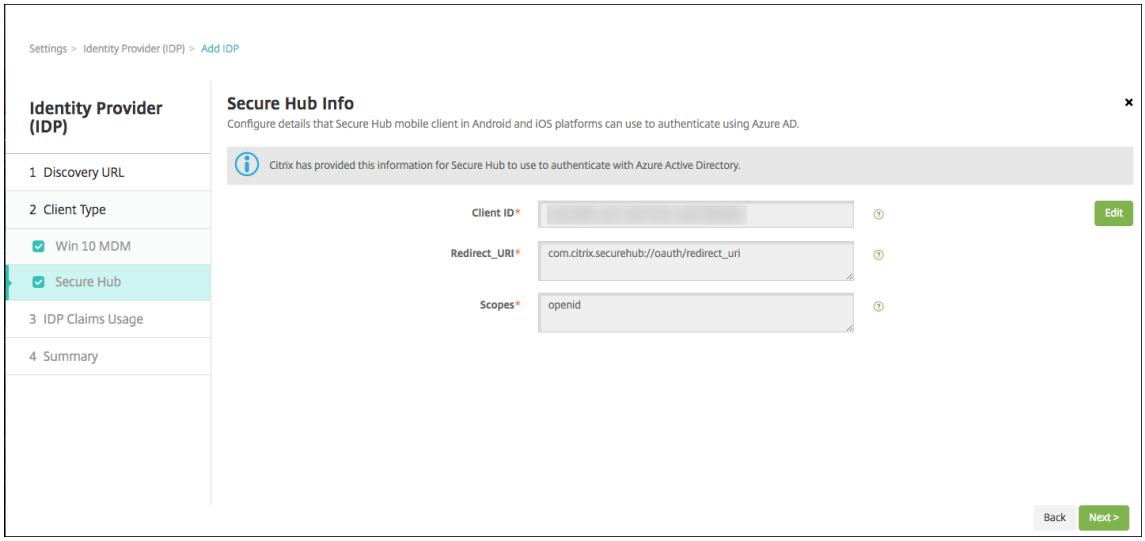
6. 其余的字段将自动填充。填充了这些字段时，单击下一步。
7. 要继续将 XenMobile 配置为使用 Azure AD 注册 Windows 10 和 Windows 11 设备以完成 MDM 注册，请配置以下设置。要跳过此可选步骤，请清除 **Windows MDM**。
   - 应用程序 **ID URI**：键入您在配置 Azure 设置时输入的 XenMobile Server 的 URL。
   - 客户端 **ID**：从 “Azure 配置” 页面复制并粘贴此值。客户端 ID 是您的应用程序的唯一标识符。
   - 密钥：从 Azure 应用程序设置页面复制此值。在密钥下方，从列表中选择一个持续时间并保存设置。然后，可以复制此密钥并将其粘贴到此字段中。应用程序在 Microsoft Azure AD 中读写数据时需要密钥。



8. 单击 **Next**（下一步）。

   Citrix 已在 Microsoft Azure 中注册 Secure Hub 并维护该信息。此屏幕显示 Secure Hub 与 Azure Active Directory 通信时使用的详细信息。如果其中的任何信息需要变更，将来都会使用此页面。仅当 Citrix 建议时才能编辑此页面。

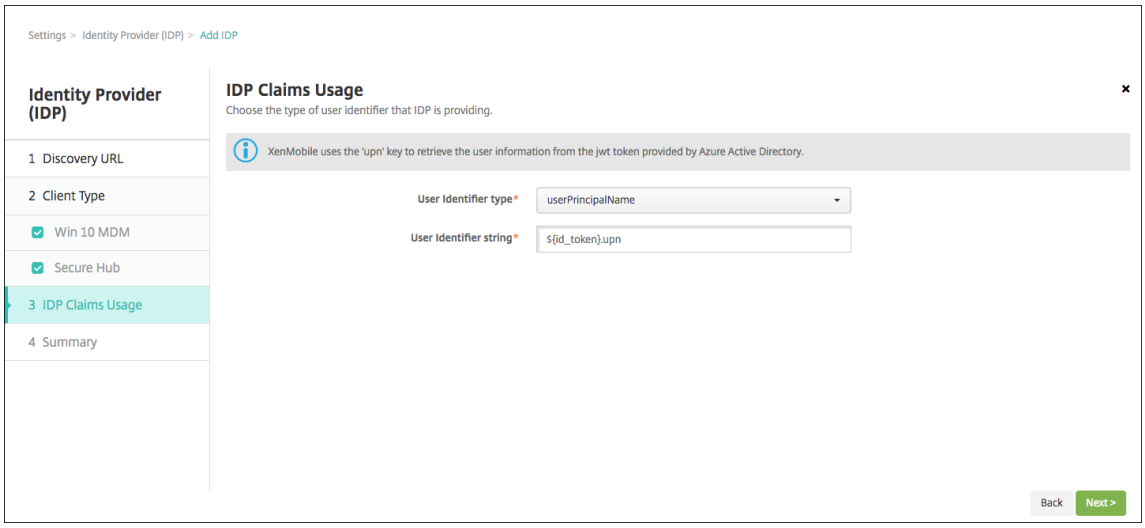
9. 单击 **Next**（下一步）。



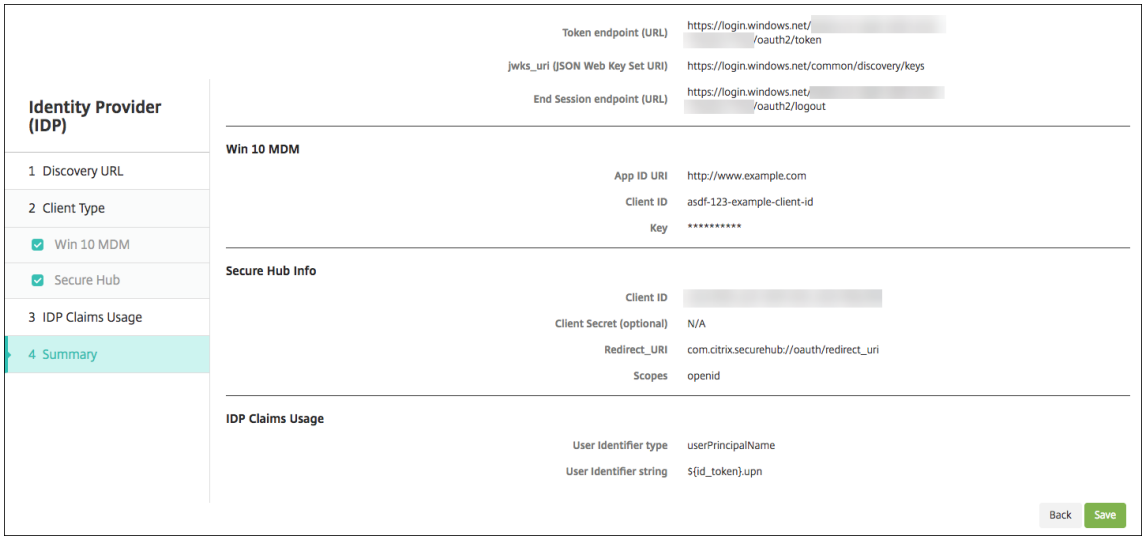
10. 配置 IdP 提供的用户标识符的类型：

    - 用户标识符类型：从下拉列表中选择 **userPrincipalName**。
    - 用户标识符字符串：此字段自动填充。

11. 单击 **Next**（下一步）。

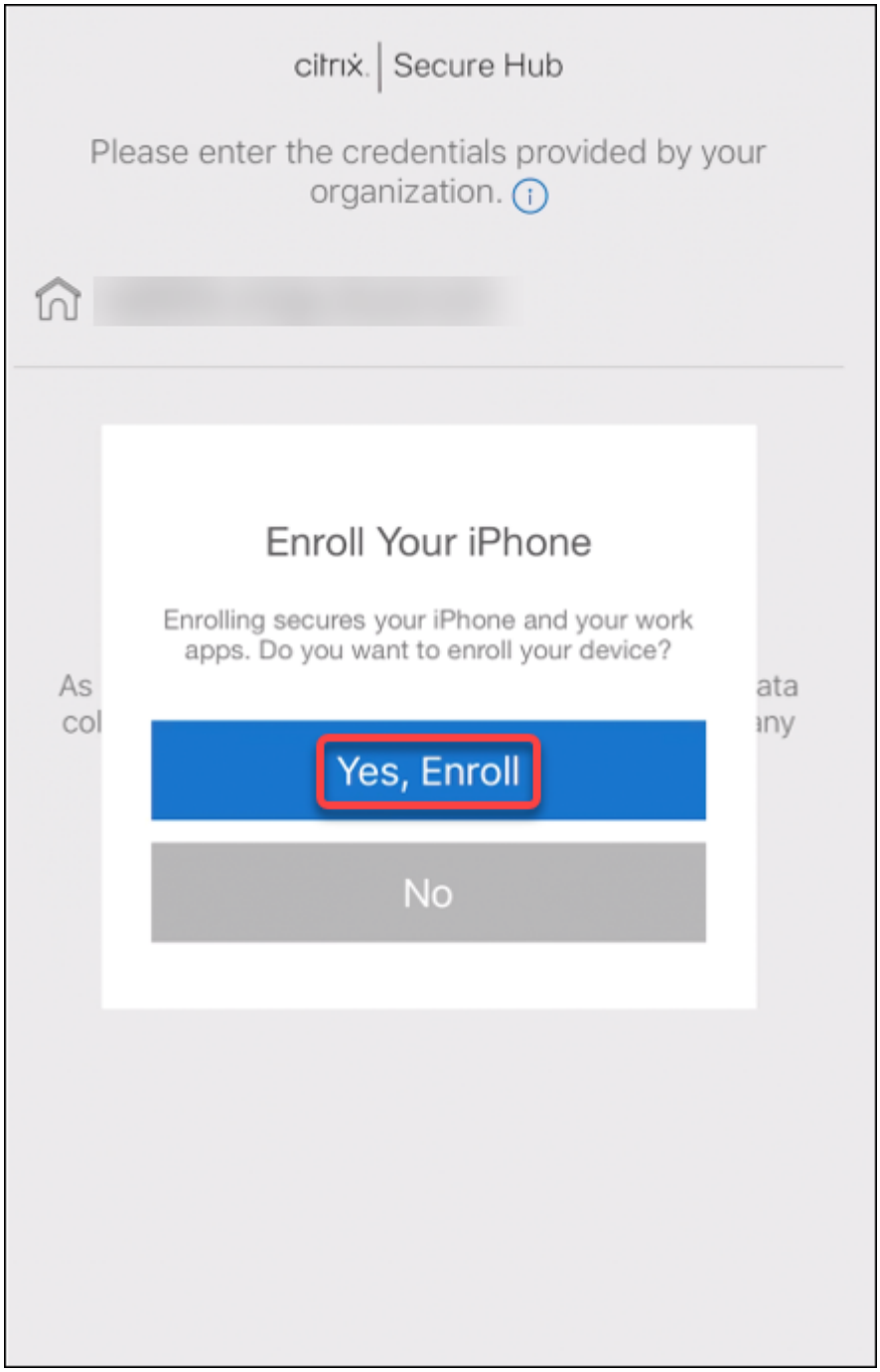


12. 检查摘要页面并单击保存。

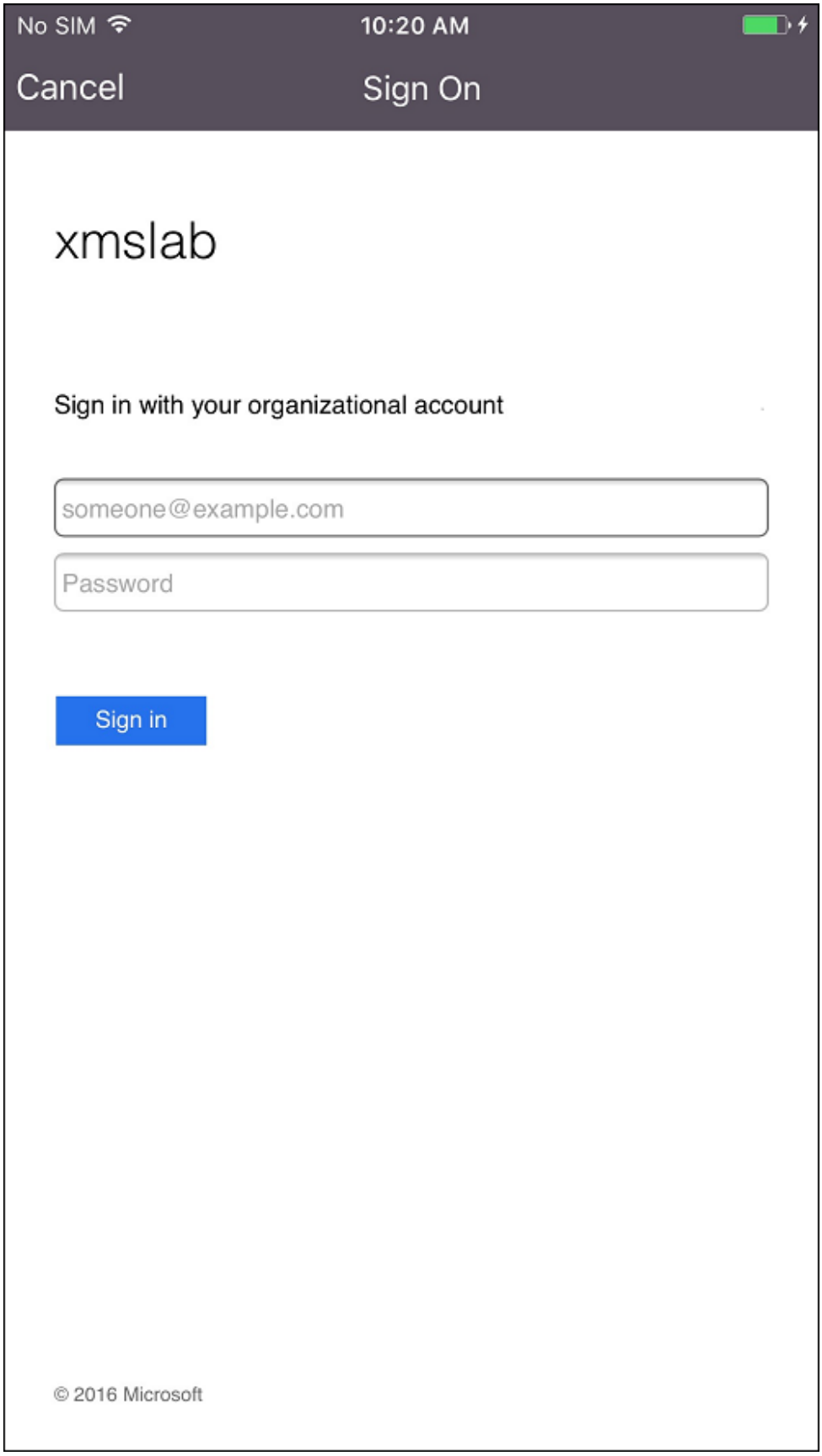


用户体验到的过程

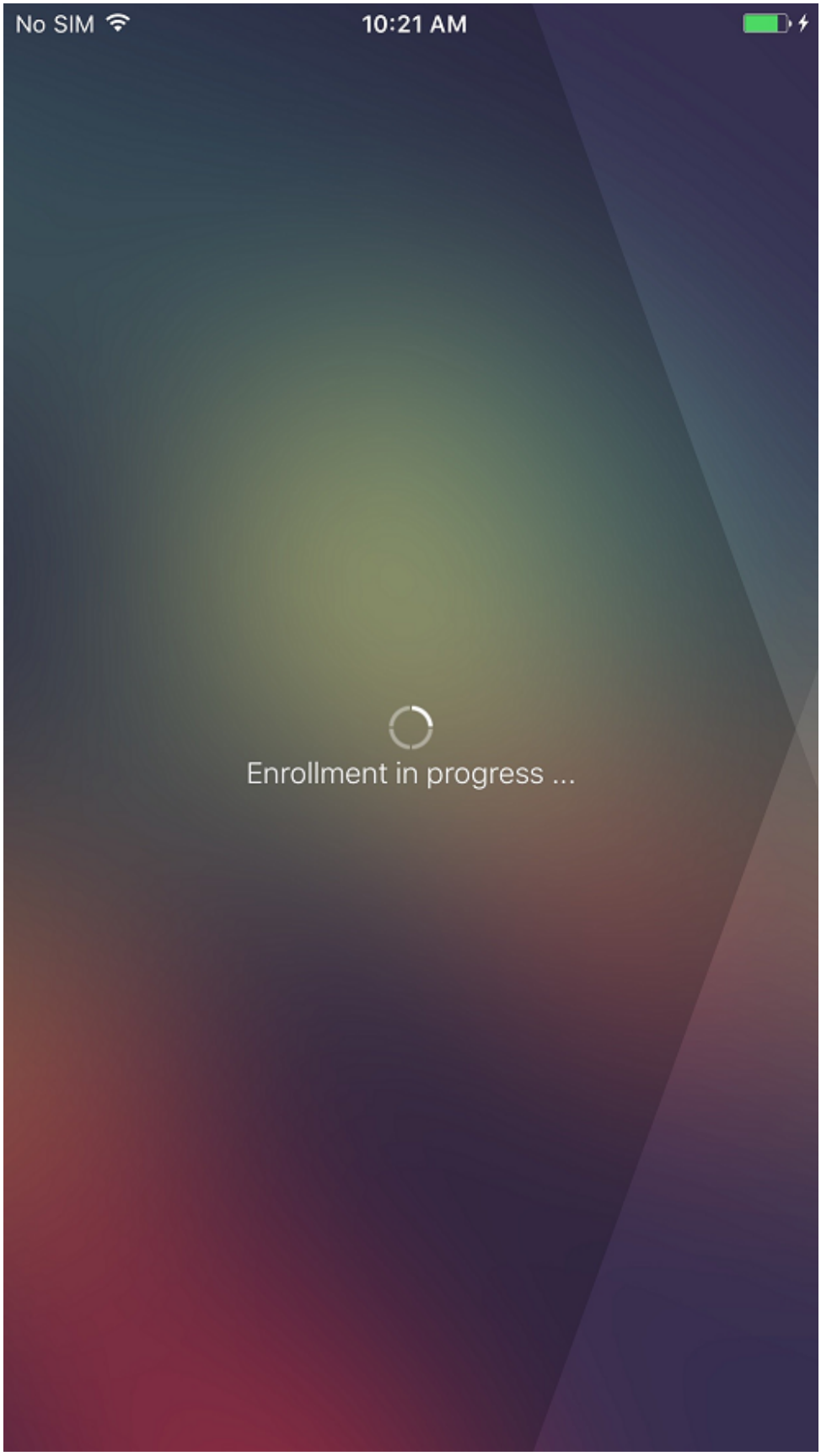
1. 用户启动 Secure Hub。用户随后输入 XenMobile Server 的完全限定域名 (FQDN)、用户主体名称 (UPN) 或电子邮件地址。

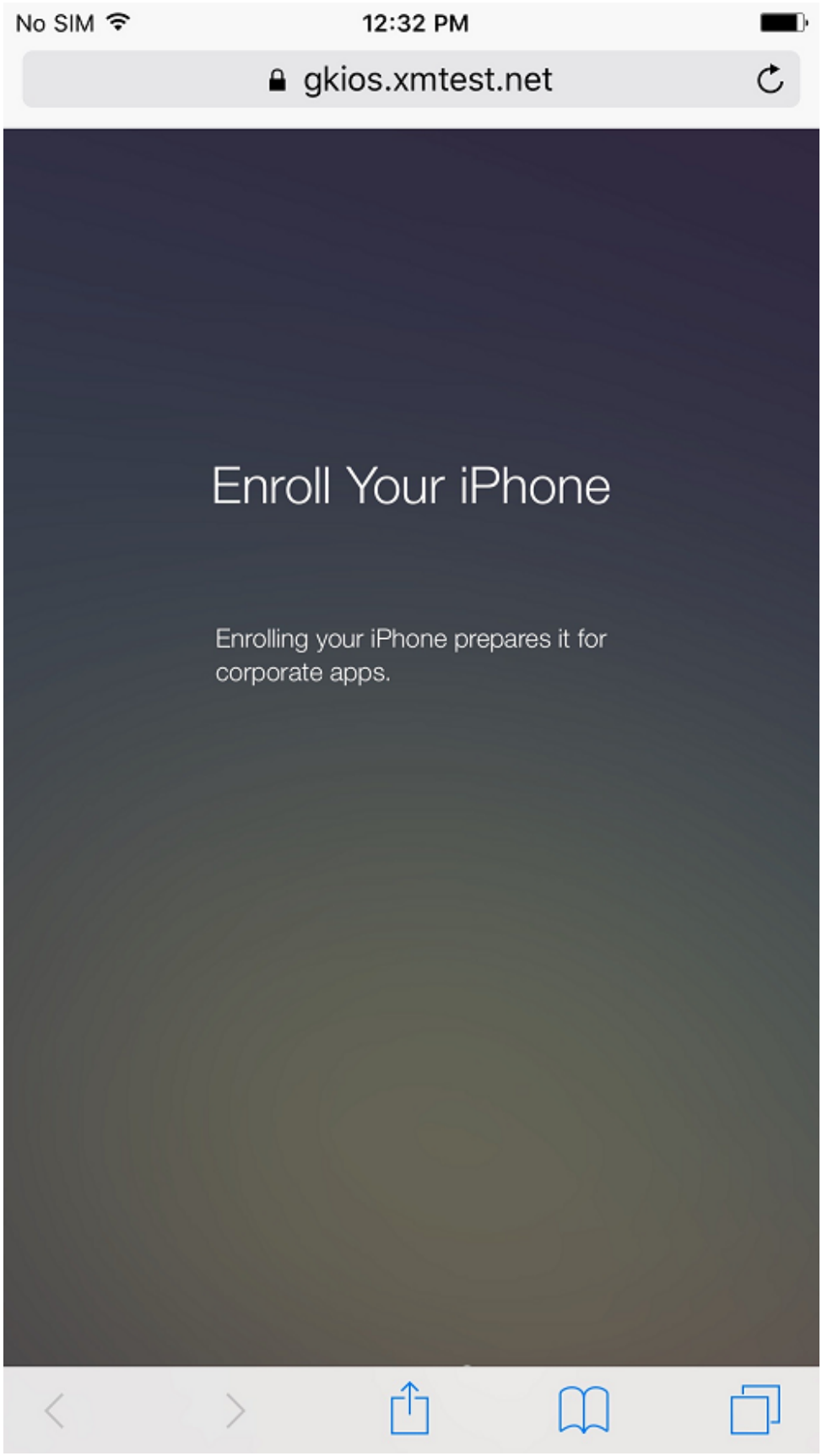


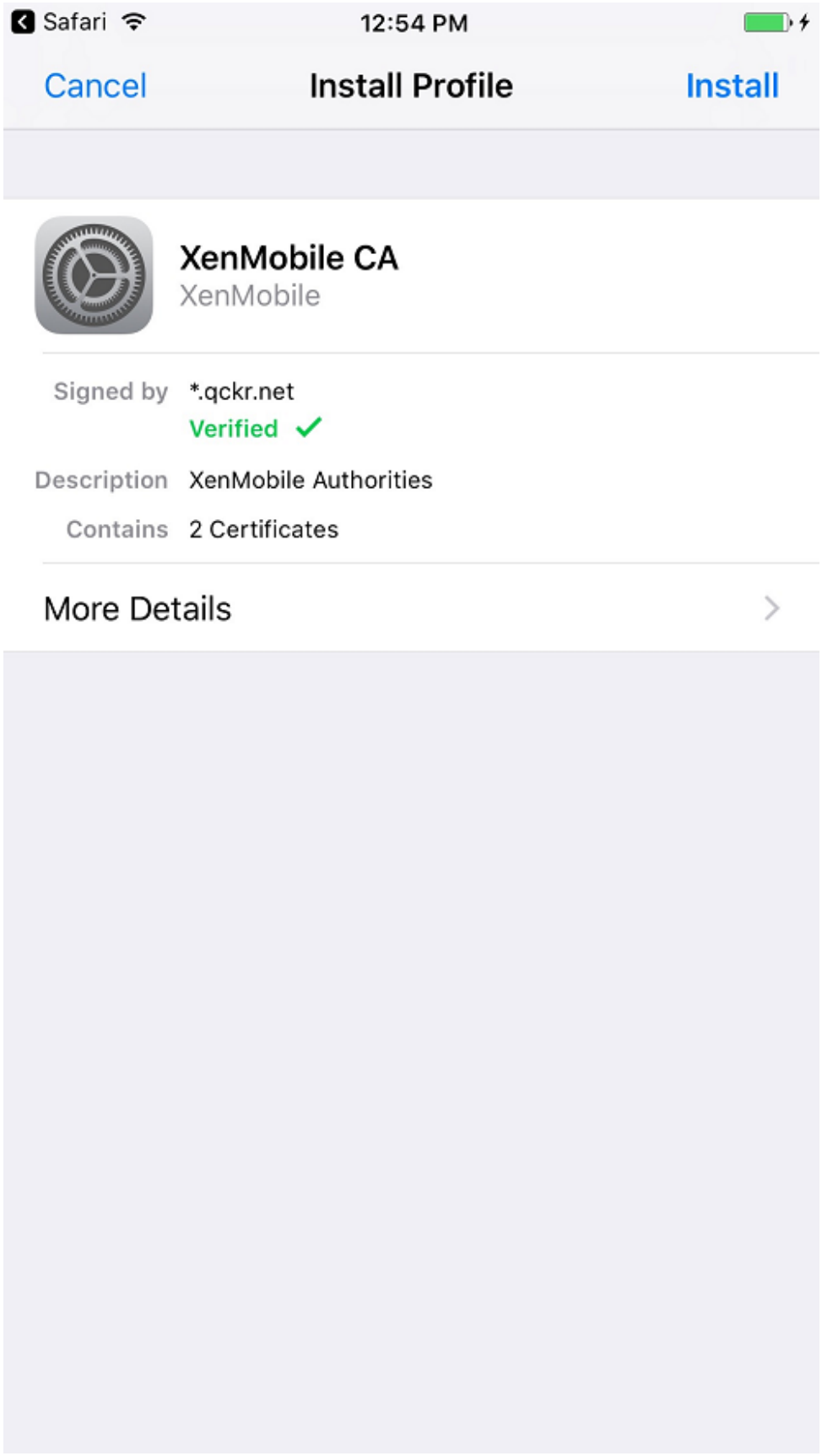
2. 用户随后单击是，注册。



3. 用户使用其 Azure AD 凭据登录。







4. 用户完成注册步骤，方式与通过 Secure Hub 执行的任何其他注册相同。

> 注意：
>
> XenMobile 不支持通过 Azure AD 针对注册邀请完成身份验证。如果您向用户发送了一个包含注册 URL 的注册邀请，用户将通过 LDAP 进行身份验证，而非通过 Azure AD。

派生凭据

March 31, 2021

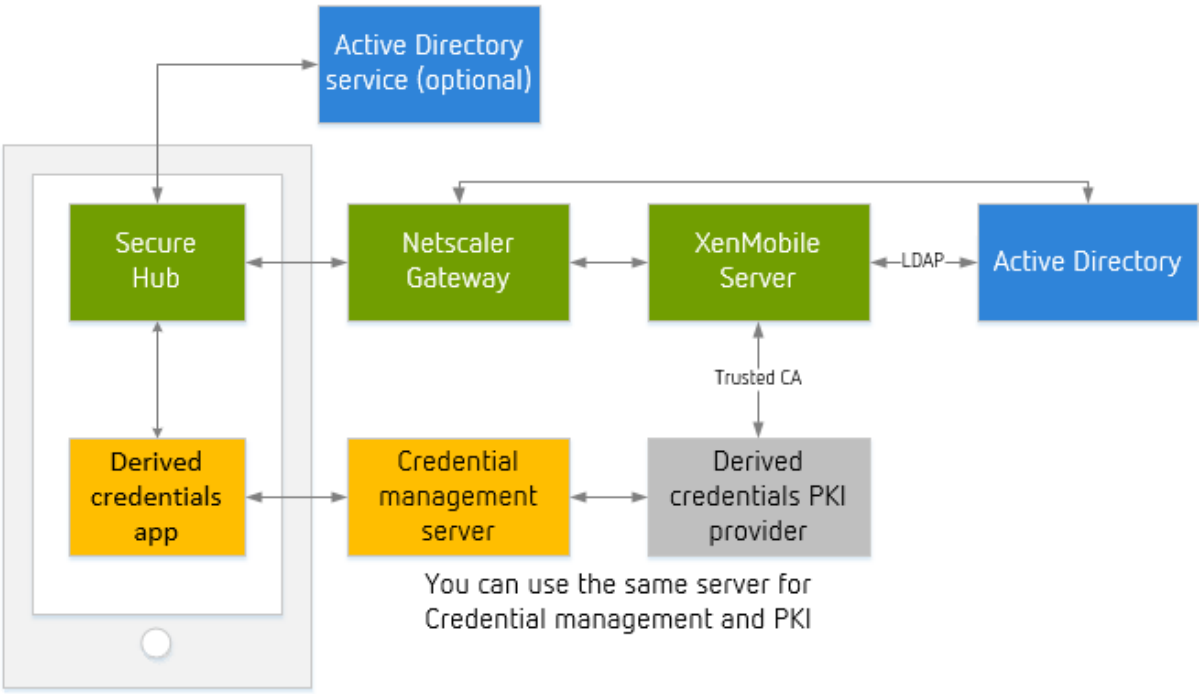
派生凭据提供适用于移动设备的加强的身份验证。智能卡提供凭据，提供的凭据驻留在移动设备上，而非智能卡上。智能卡为个人身份验证 (Personal Identity Verification, PIV) 卡。

派生凭据为包含用户标识符（例如 UPN）的注册证书。XenMobile 将从凭据提供程序获取的凭据保存在设备上一个安全的保管库中。

XenMobile 可以将派生凭据用于设备注册和身份验证。如果配置为使用派生凭据，XenMobile 将不支持注册邀请或其他注册安全模式。Citrix 支持在 iOS 注册过程中使用派生凭据应用程序。

体系结构

进行注册时，XenMobile Server 将连接到各组件，如下图所示。

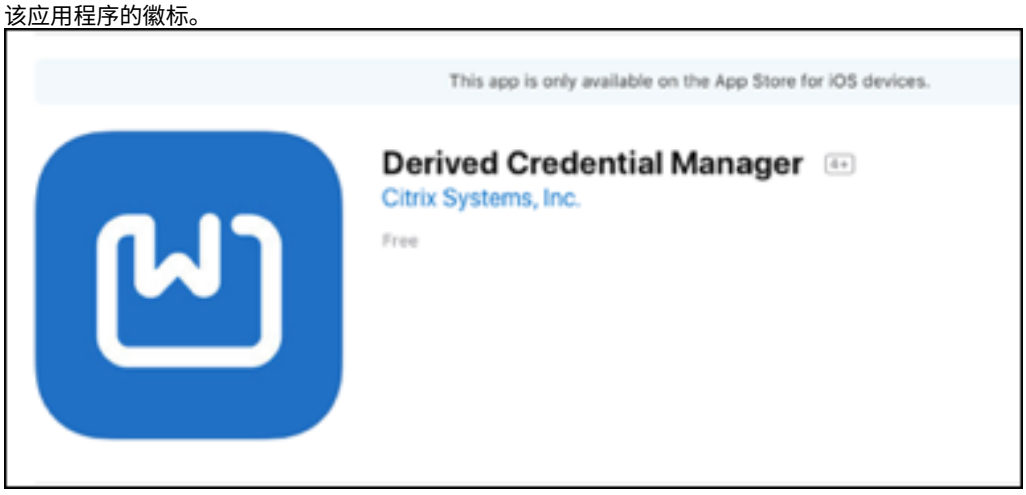


- 设备注册期间，Secure Hub 从派生凭据应用程序获取证书。

- 派生凭据应用程序在注册过程中与凭据管理服务器进行通信。
- 可以为凭据管理服务器和第三方 PKI 提供程序使用相同或不同的服务器。
- XenMobile Server 连接到您的第三方 PKI 服务器以获取证书。

要求

- 下载并安装 Citrix Secure Hub。
- 根据您的派生凭据解决方案，下载并配置应用程序：
  - 对于 **Entrust Datacard**：
    * 在 XenMobile 中注册之前，在您的设备上下载并安装 Citrix Derived Credential Manager 应用程序。Derived Credentials Manager 应用程序是面向 Citrix 的身份提供程序应用程序。下面是该应用程序的徽标。



    * Citrix Derived Credential Manager 应用程序仅支持新注册。设备用户必须重新注册。
      · XenMobile Server 10.8 或更高版本。
      · 需要在 MDM+MAM 下注册设备。
  - 其他派生凭据提供程序：虽然大多数其他凭据解决方案可能都与 XenMobile 兼容，但请在将其部署到生产环境之前测试集成。
- 必须具有向凭据提供程序服务器颁发证书的颁发机构的根证书。该设置使 XenMobile 在注册过程中能够接受数字签名的证书。有关添加证书的信息，请参阅证书和身份验证。
  - 如果用户电子邮件域与 LDAP 域不同，请在设置 **> LDAP** 下的域别名设置中包括该电子邮件域。例如，如果电子邮件地址的域为 `citrix.com`，LDAP 域名为 `sample.com`，请将域别名设置为 **`sample.com`, `citrix.com`**。
  - XenMobile 不支持对共享设备使用派生凭据。
- 用户标识证书：
  - “使用者备用名称”字段中的用户名的格式必须为 SubjectAltName 扩展的 otherName、rfc822Name 或 dNSName 字段。其他字段不受支持。有关使用者备用名称的详细信息，请参阅 RFC https://www.ietf.org/rfc/rfc5280.txt。

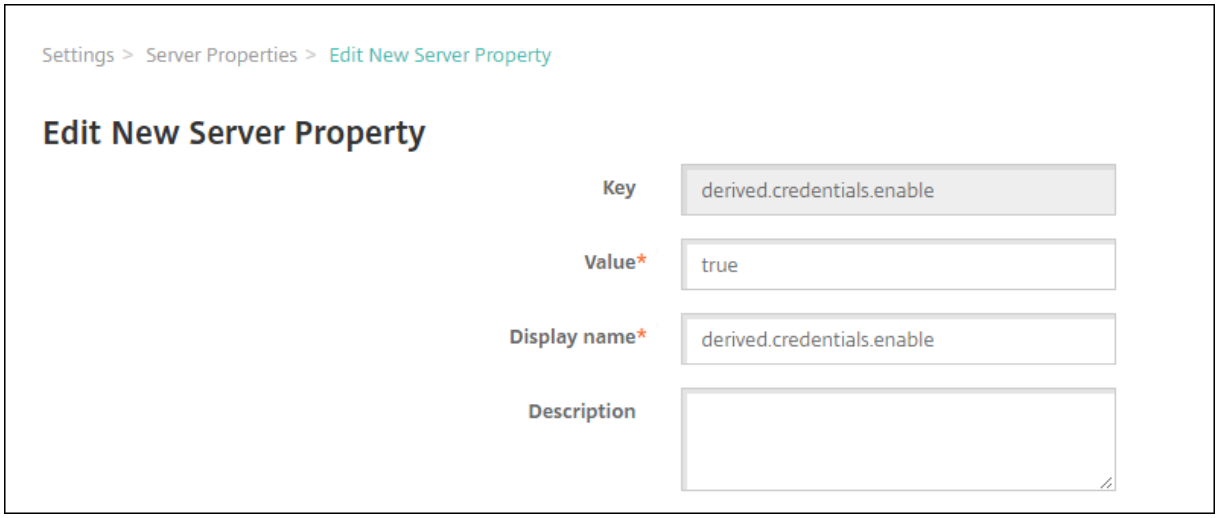
  - “电子邮件”或“CN”中“使用者”字段中的用户标识不受支持。
- Citrix Gateway 配置为进行证书身份验证或证书加安全令牌身份验证

启用派生凭据

默认情况下，XenMobile 控制台不包括设置 **>** 派生凭据页面。

要为派生凭据启用接口，请执行以下操作：

- 转至设置 **>** 服务器属性，添加 **derived.credentials.enable** 作为服务器属性并将该属性值设置为 **true**。

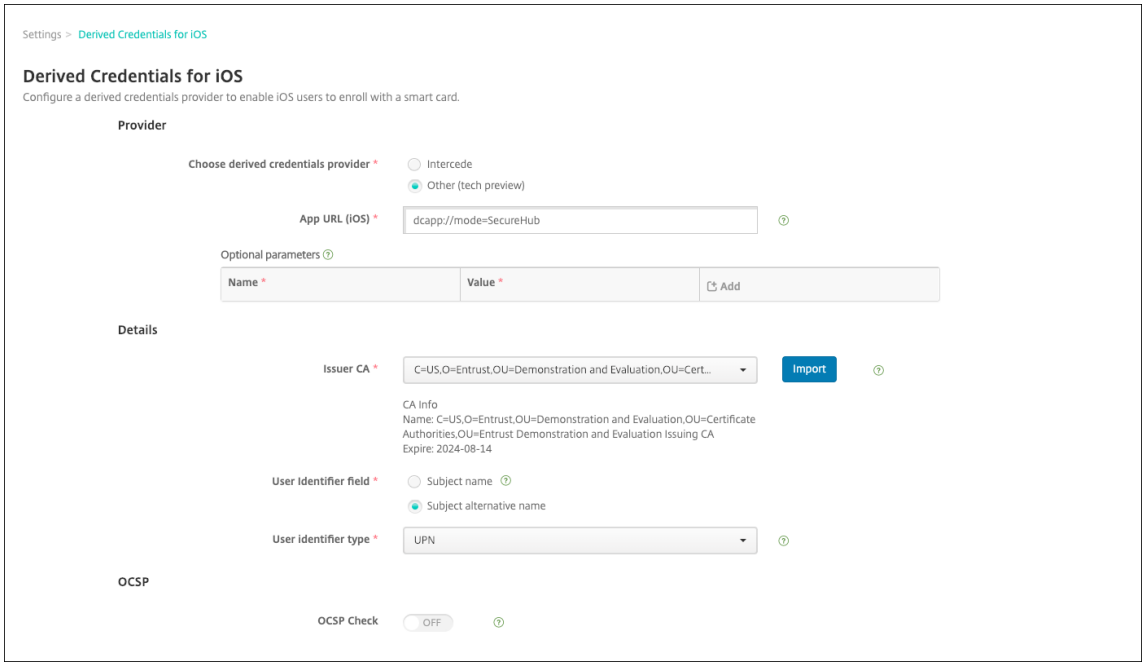


配置派生凭据

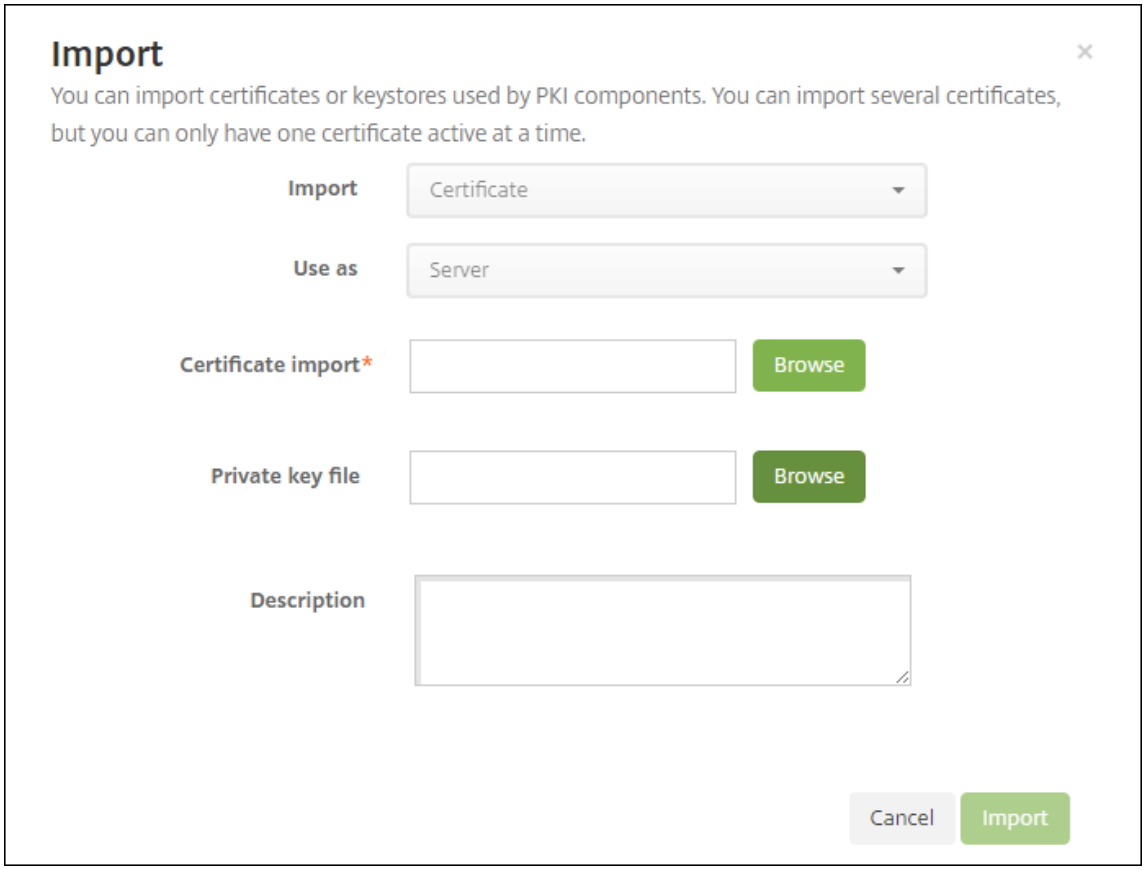
这假定您的计划与 XenMobile 集成的派生凭据提供程序具有有效配置。可以将 XenMobile 配置为与该服务器进行通信。也可以选择已添加到 XenMobile 的派生凭据 CA 证书或导入证书。

可以激活对该 CA 证书的联机证书状态协议 (OCSP) 支持。有关 OCSP 的详细信息，请参阅 PKI 实体中的“任意 CA”。

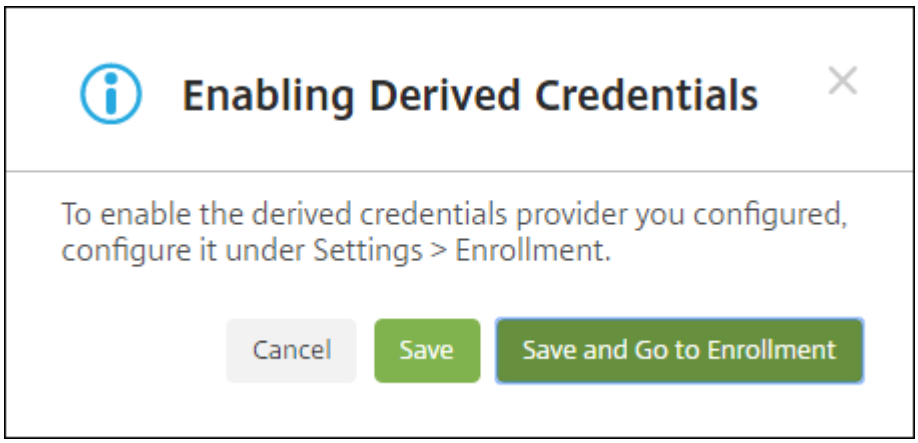
1. 在 XenMobile 控制台中，转至设置 **>** 适用于 **iOS** 的派生凭据。
2. 对于选择派生凭据提供程序，请选择其他（针对 Entrust Datacard）。在应用程序 **URL (iOS)** 中键入 `dcapp://mode=SecureHub`。



3. 可选参数：某些派生凭据提供程序可能要求您提供连接参数。例如，某个供应商可能要求您指定后端服务器的 URL。单击添加可提供参数。
4. 指定派生凭据的证书：如果证书已上载到 XenMobile，请从颁发者 **CA** 中选择该证书。否则，请单击导入以添加证书。此时将显示导入证书对话框。
5. 在导入证书对话框中，单击浏览导航到该证书。然后单击浏览导航到私钥文件。

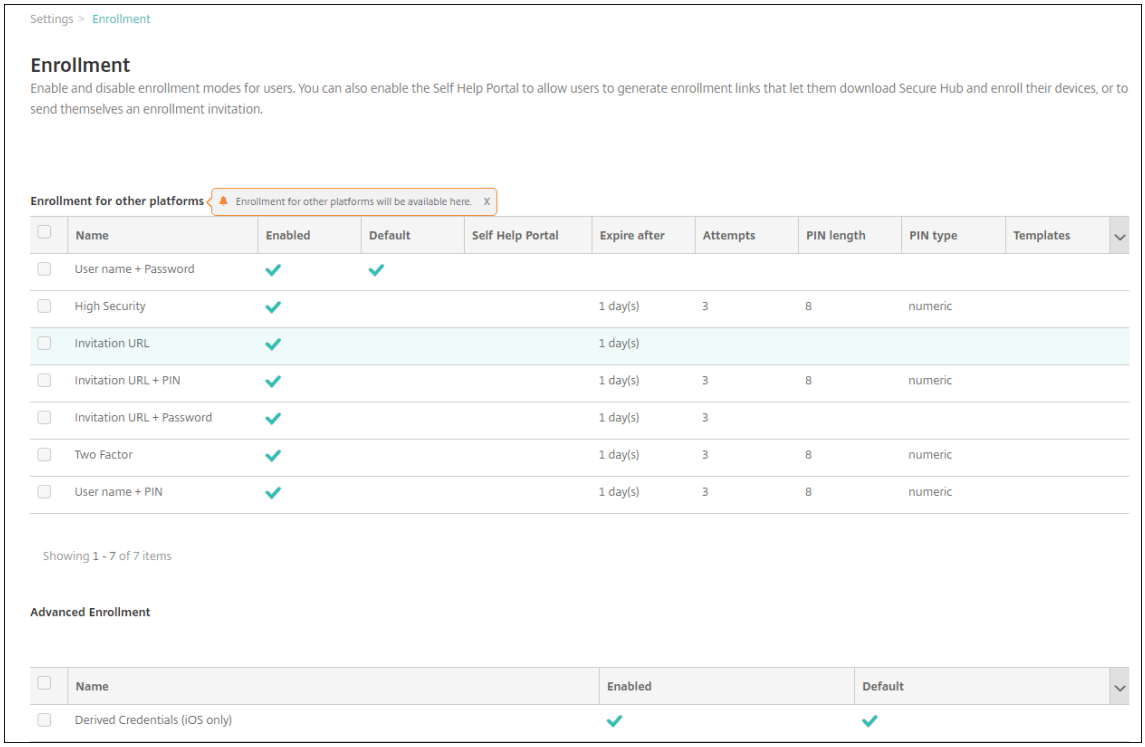


6. 配置设置。
   - 对于 Citrix Derived Credential Manager 应用程序：用户标识符字段为使用者备用名称，用户标识符类型为 **userPrincipalName**。
   - 请联系其他派生凭据提供商以获取其信息。
7. 可以选择性使用 OCSP 响应者执行证书吊销检查。出于安全目的，Citrix 建议您使用 OCSP 响应者。默认情况下，OSP 检查设置为关。
   - 如果要激活对该 CA 证书的 OCSP 支持，请选择使用自定义 **OCSP URL** 对应的选项。默认情况下，XenMobile 从证书中提取 OCSP URL（使用证书定义进行吊销选项）。要指定响应者 URL，请单击使用自定义并键入 URL。
   - 响应者 **CA**：在响应者 **CA** 中，选择一个证书。或者，单击导入，然后使用导入证书对话框查找证书。
8. 单击保存。此时将显示启用派生凭据对话框。

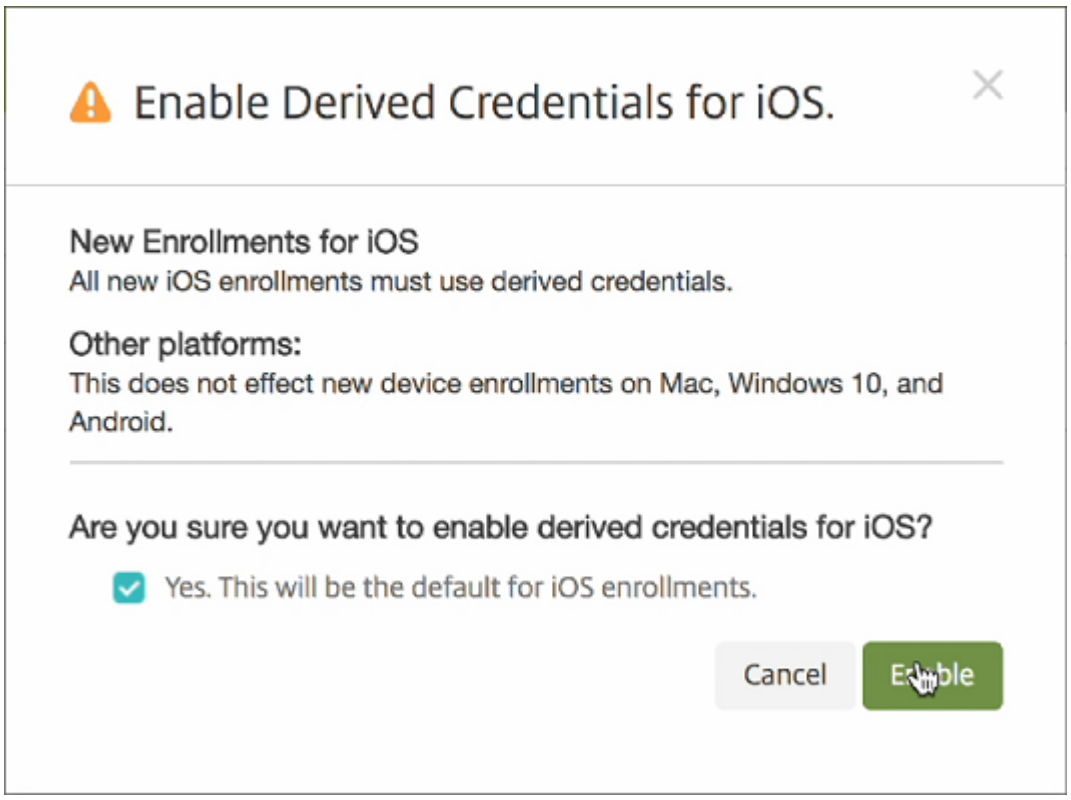


- 要启用派生凭据配置，请单击保存。还必须配置注册设置才能使用派生凭据。
- 要启用派生凭据配置，然后立即转至设置 **>** 注册，请单击保存并转至 **“**注册**”**。

9. 要为注册启用派生凭据，请在设置 **>** 注册页面上的高级注册下，选择派生凭据 **(**仅限 **iOS)**，然后单击启用。



10. 此时将显示确认对话框。要启用派生凭据，请选中该复选框，然后单击启用。



11. 要编辑派生凭据注册的选项，请转至设置 **>** 注册，选择派生凭据 **(**仅限 **iOS)**，然后单击编辑。

启用派生凭据后：在设备注册报告中，注册模式列显示 **derived_credentials**。

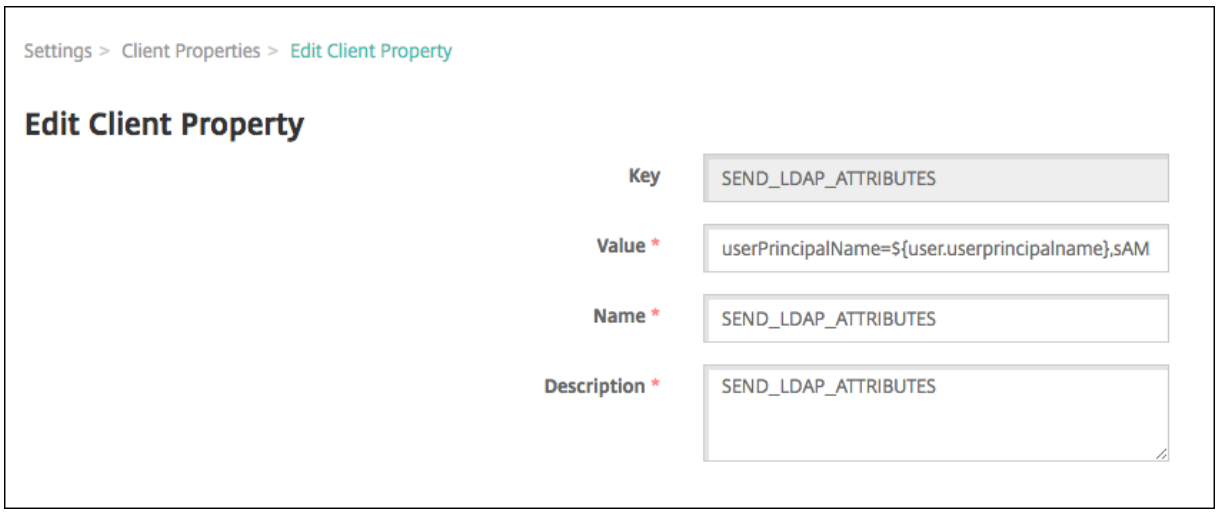
> 重要：
>
> 添加派生凭据提供程序后，重新启动您的 XenMobile Server。

为 **Secure Mail** 配置 **XenMobile Server**

要启用 Secure Mail 以支持派生凭据，请添加 `SEND_LDAP_ATTRIBUTES` 客户端属性。有关添加客户端属性的信息，请参阅客户端属性。

请对客户端属性使用以下信息：

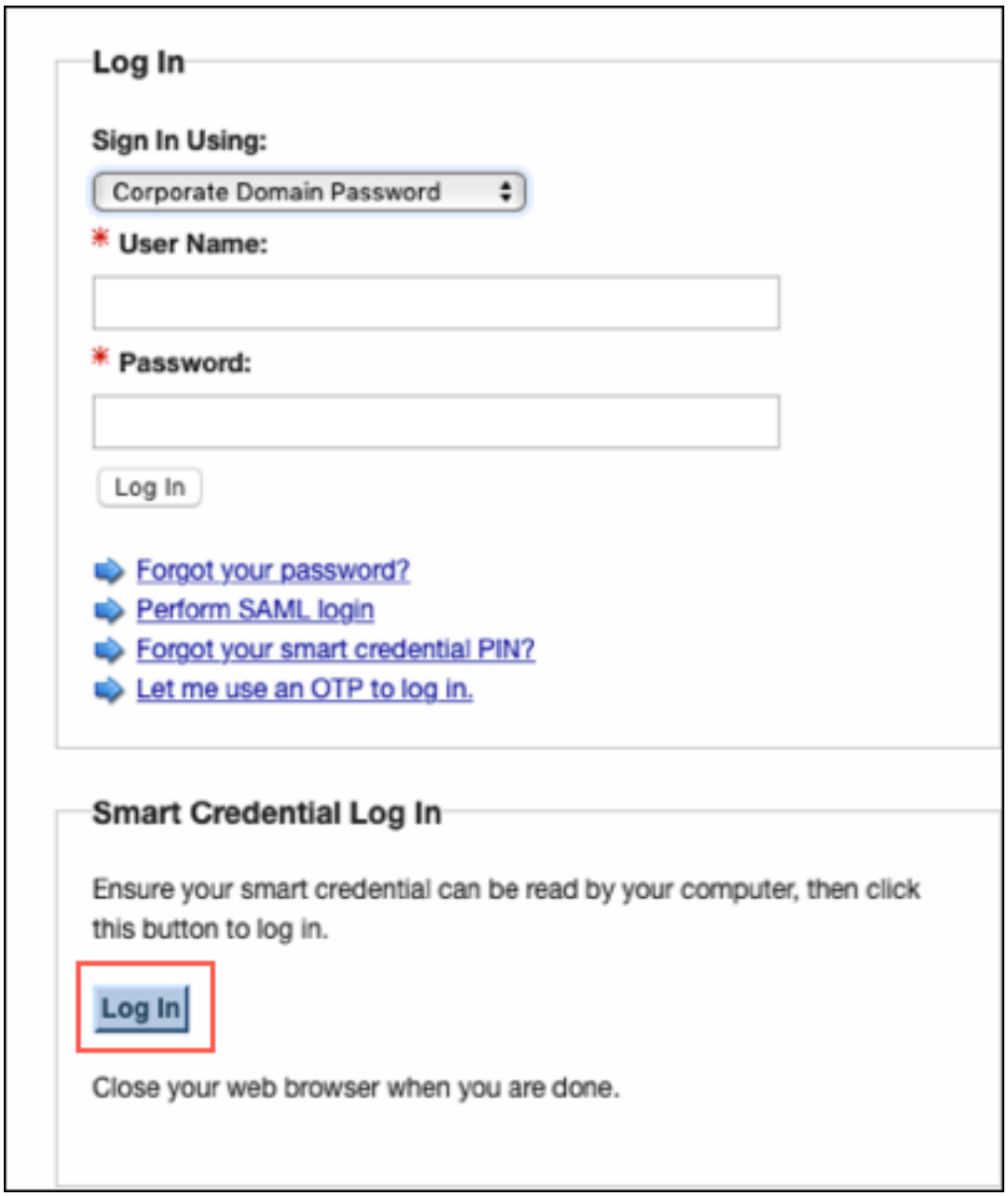
- 注册表项：`SEND_LDAP_ATTRIBUTES`
- 值：`userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



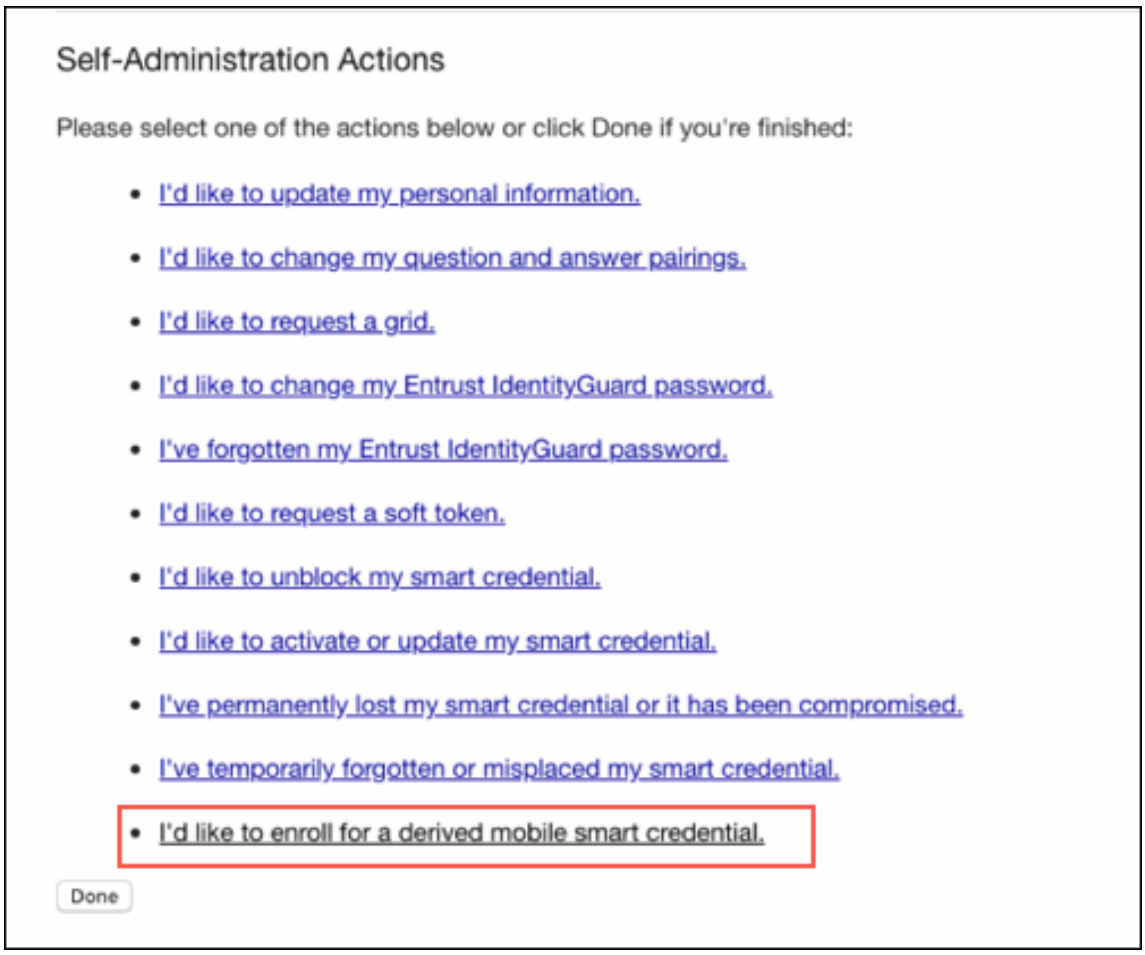
在 **iOS** 设备上激活 **Entrust Datacard** 派生凭据

> 注意：
>
> 使用 Entrust Web 站点时，请在更改 PIV 卡时清除浏览器缓存。

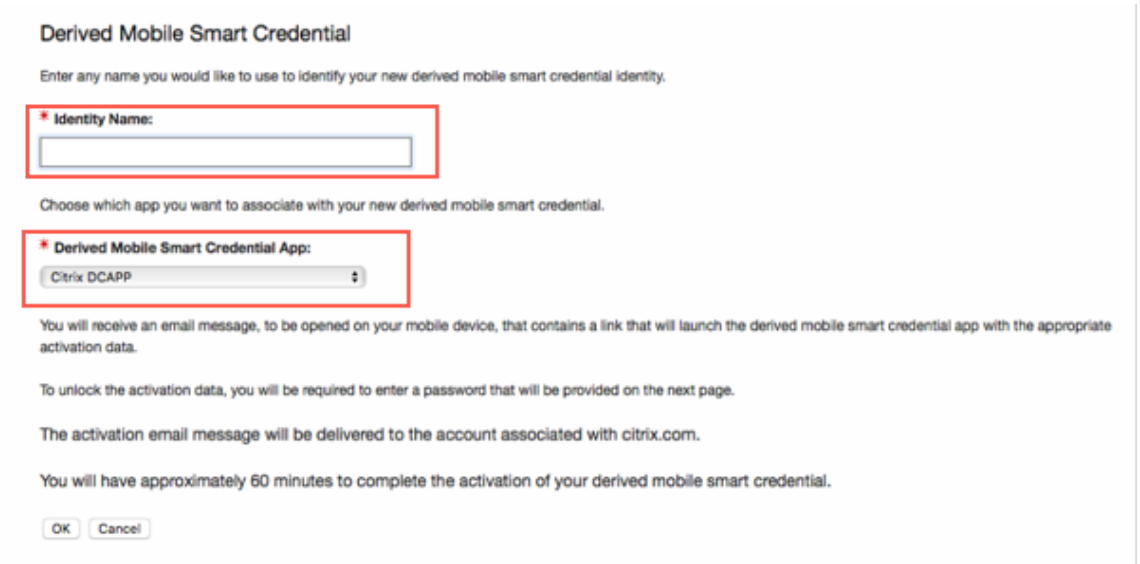
1. 要申请新的智能凭据，请使用桌面或任何设备登录 Entrust 站点。使用页面底部的智能凭据登录按钮登录。用户将智能卡插入连接到其桌面的读卡器。



2. 在 **Self-Administration Actions**（自助管理操作）中，选择 **I'd like to enroll for a derived mobile smart credential**（我希望注册以获取派生的移动智能凭据）并单击 **Done**（完成）。



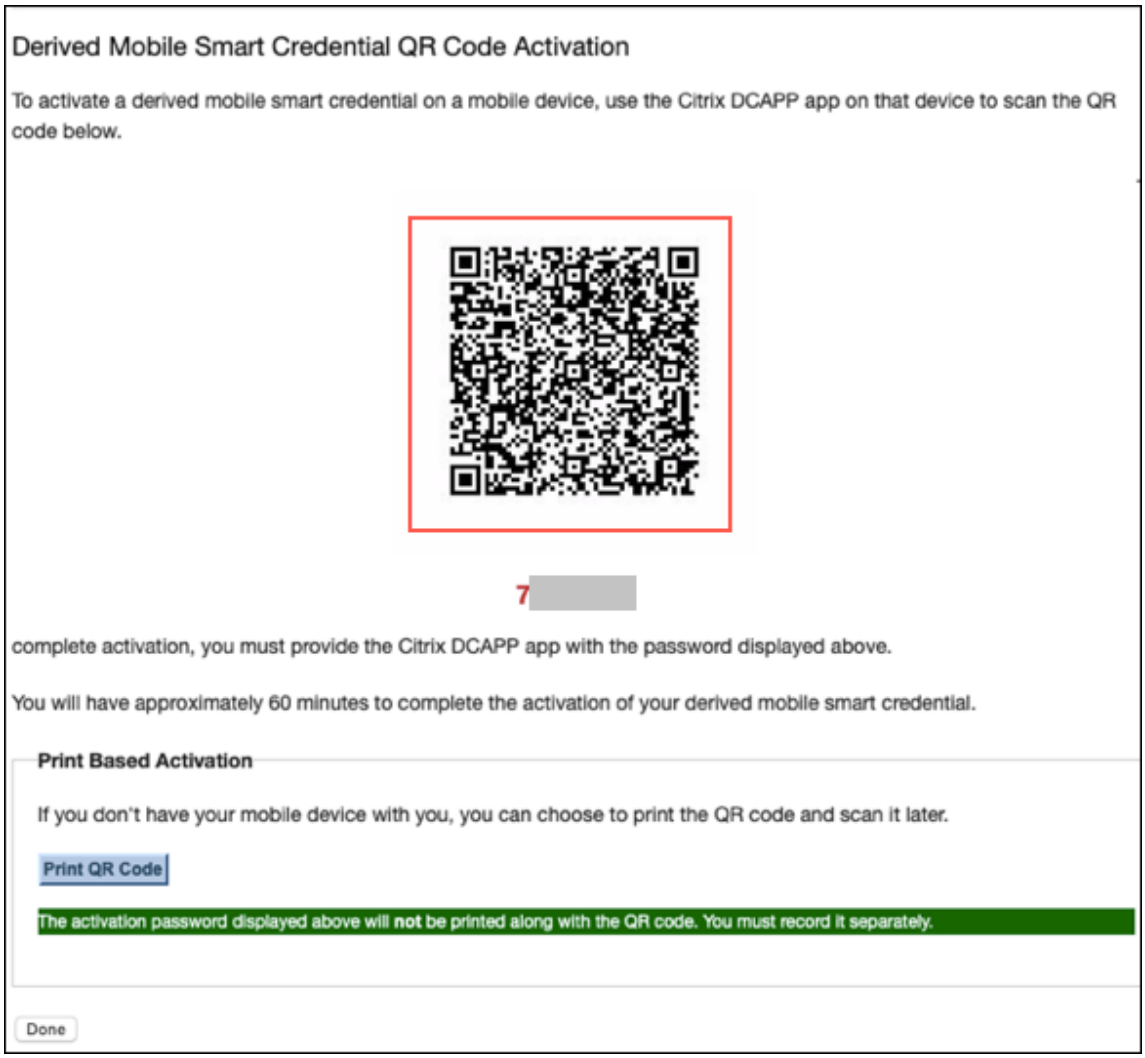
3. 在 **Derived Mobile Smart Credential**（派生移动智能凭据）屏幕上，提供 **Identity Name**（身份名称）。用户可以选择一个唯一的名称，例如用户名或 ID 号。
4. 从 “Derived credential”（派生凭据）应用程序菜单中，选择 **Citrix DCAPP** 并单击 **OK**（确定）。



此时将显示“QR code Activation”（QR 代码激活）屏幕，并提示用户使用其移动设备扫描代码。

> 注意：
>
> 默认情况下，派生凭据 QR 代码在 3 分钟内过期。

5. 在设备上使用 **Derived Credential Manager** 应用程序扫描 QR 代码以完成激活。

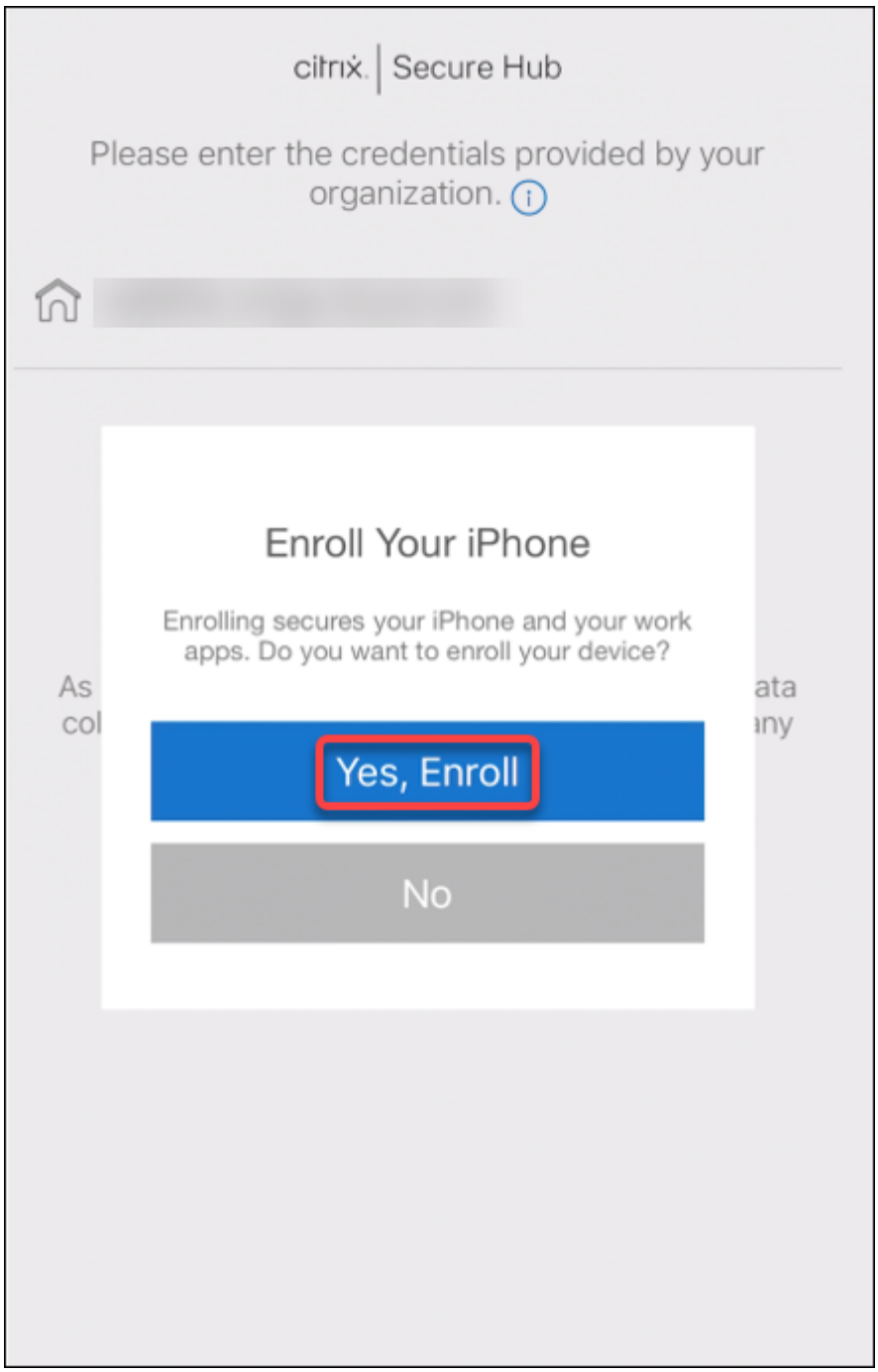


设备注册

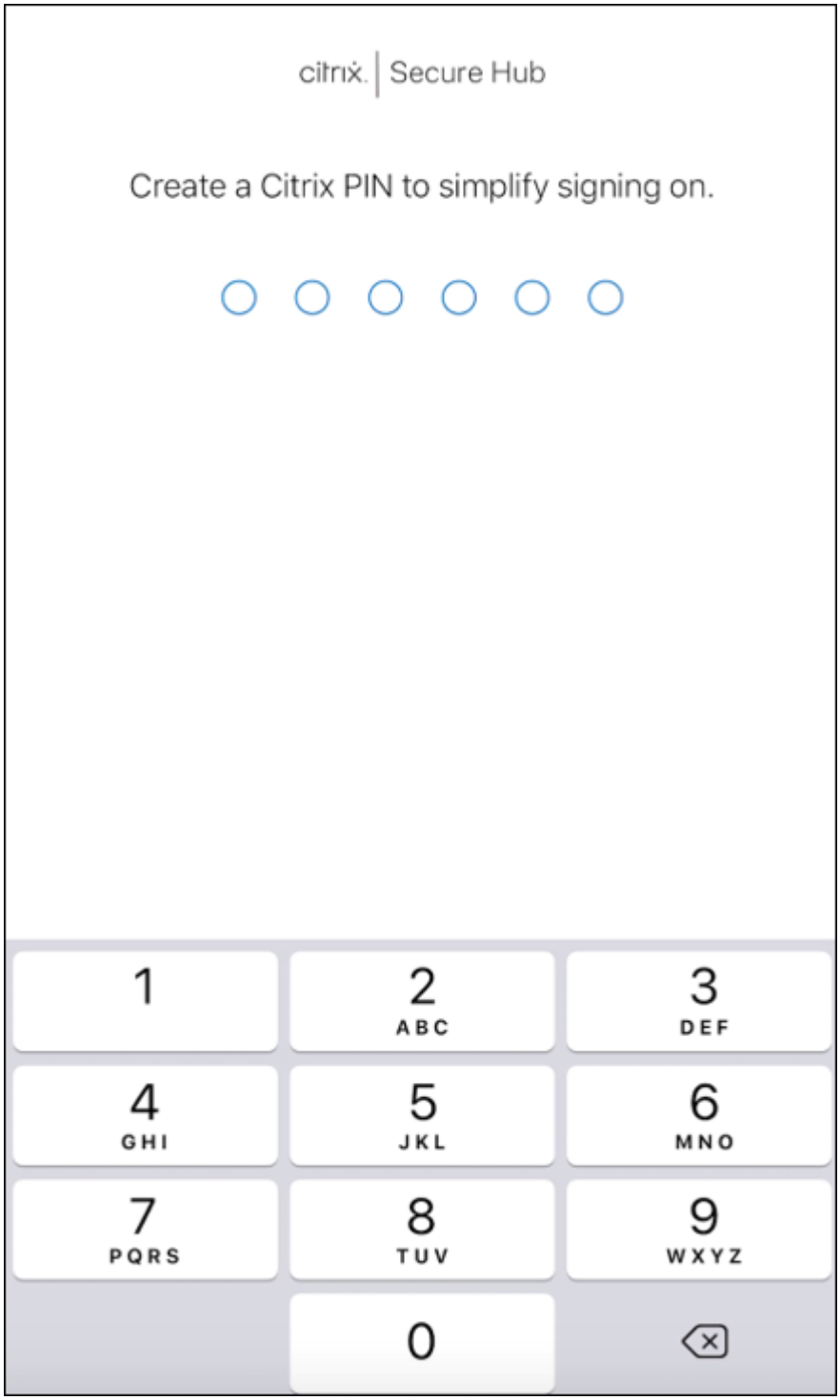
完成本文中前面所述的设置后，用户可以使用派生凭据注册其设备。

> 注意：
>
> 本部分中的屏幕截图以 Entrust Datacard 为例。

1. 轻按以打开 **Secure Hub**。系统提示时，键入 XenMobile Server 的完全限定域名，然后单击下一步。
2. 单击是，注册。在 Secure Hub 中的设备注册将开始运行。

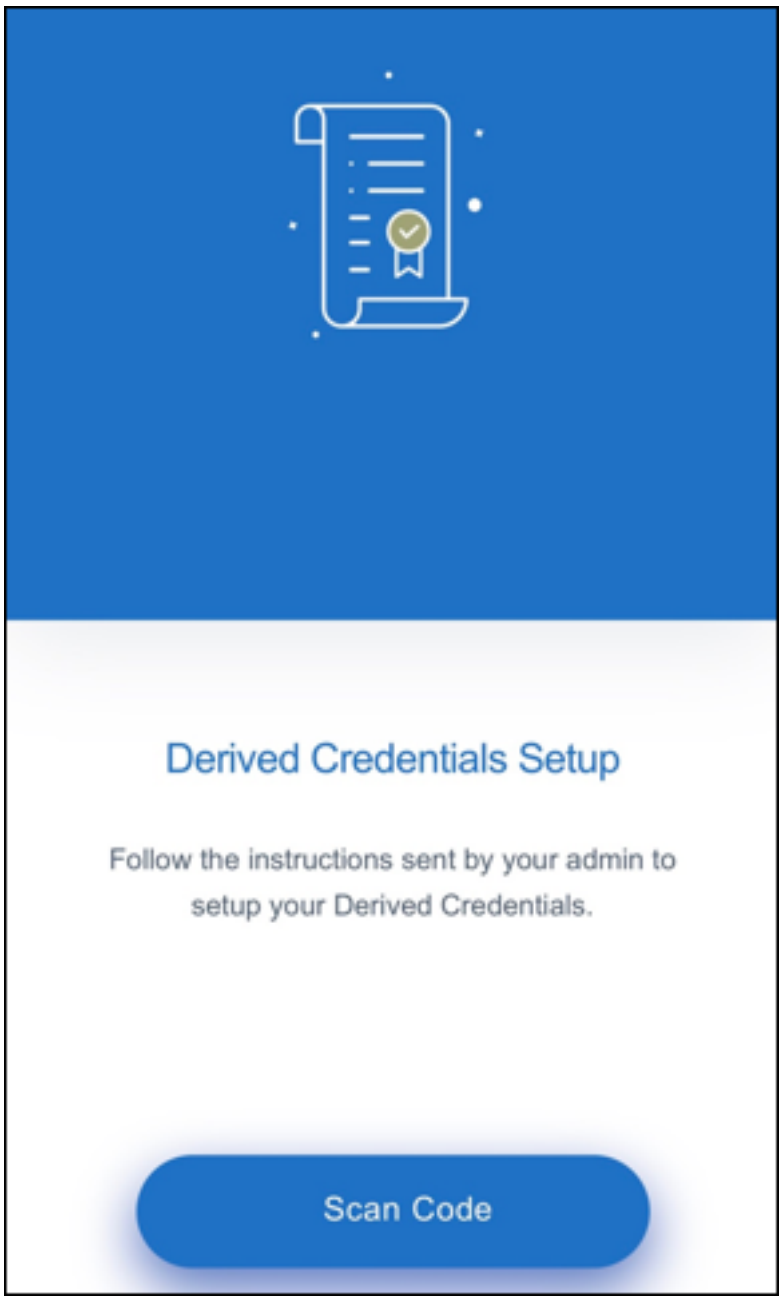


如果 XenMobile Server 支持派生凭据，Secure Hub 将提示用户创建并确认 Citrix PIN。



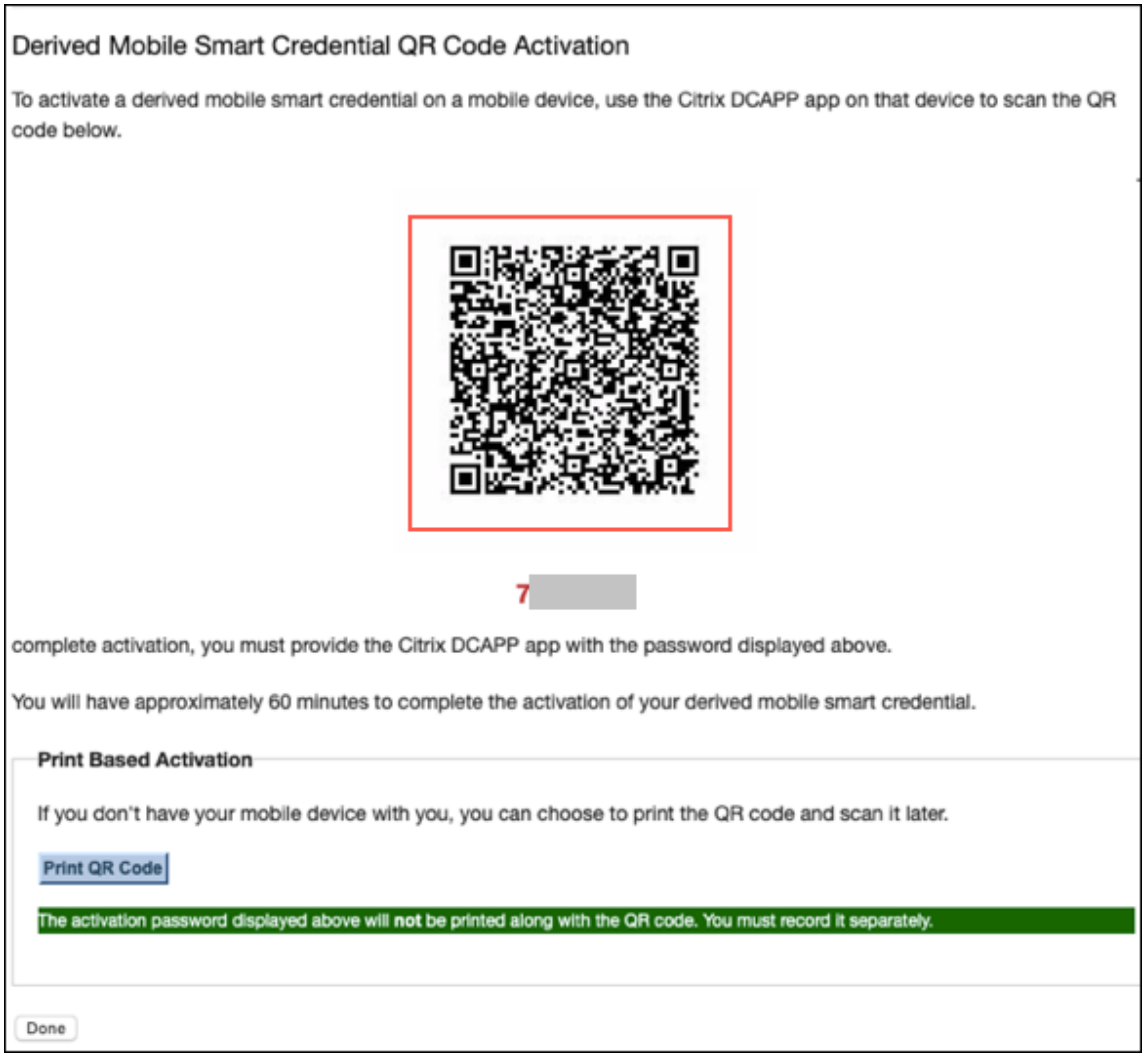
确认 Citrix PIN 后，将显示派生凭据安装程序初始屏幕。请按照说明进行操作，激活智能凭据。

3. 轻按扫描代码。移动电话相机将激活。

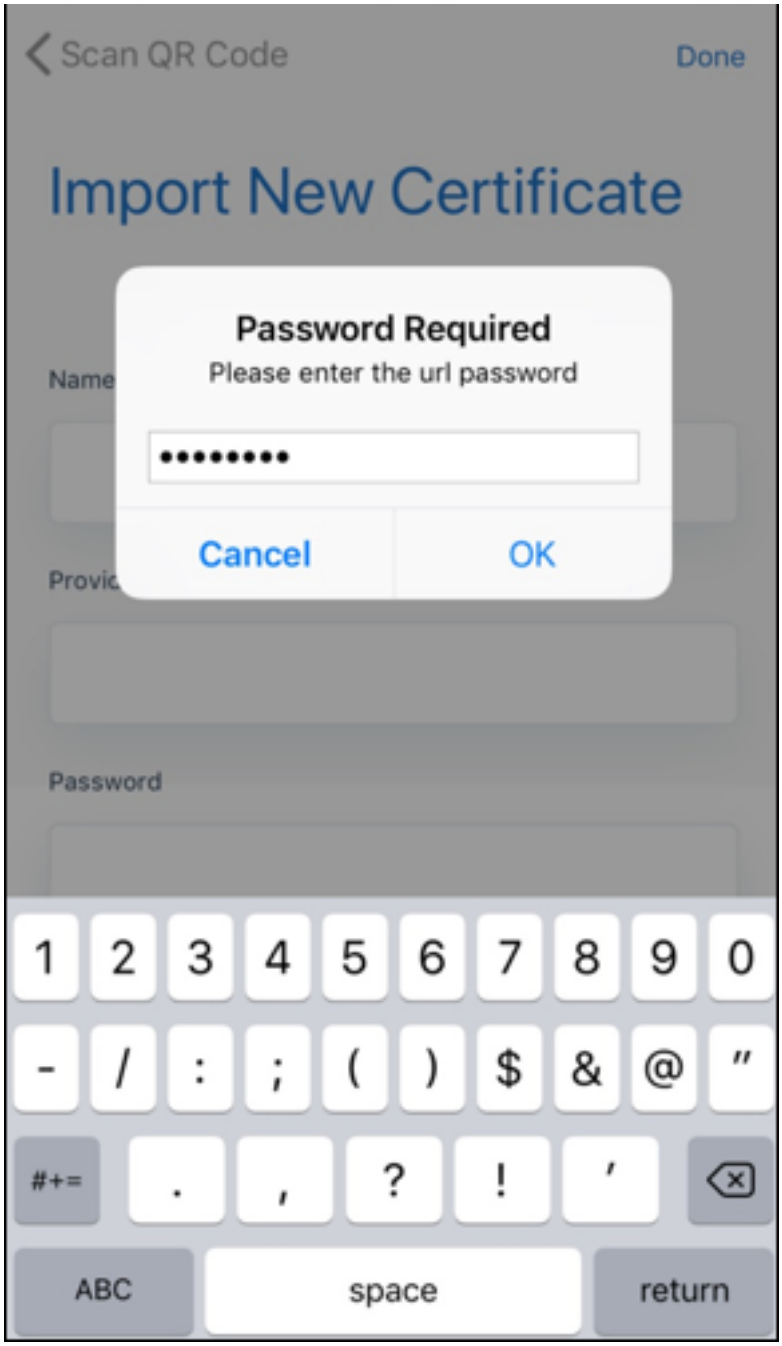


> 注意：
>
> 要扫描 QR 代码，请确保您的相机和麦克风处于启用状态，并且具有所需的访问权限。

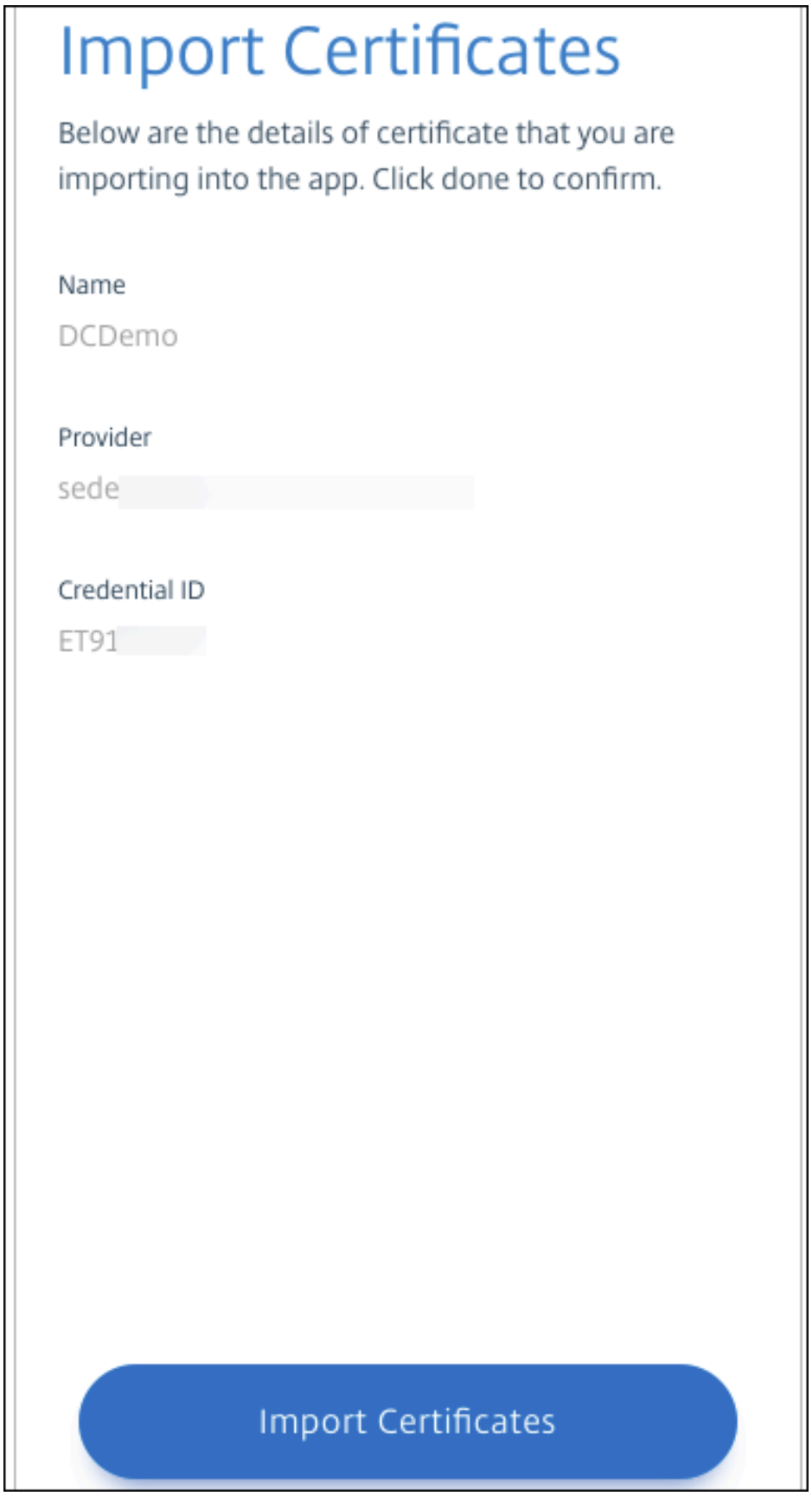
4. 在派生凭据应用程序中，扫描在前述步骤中创建的 QR 代码。



5. 扫描 QR 代码后，在导入新证书屏幕中将显示一个密码对话框，请输入密码并单击确定。



此时将显示导入新证书屏幕，其中的字段已自动填充。



6. 成功添加证书后，在派生凭据屏幕中单击 **Continue to Secure Hub**（继续进入 Secure Hub）。

7. 在 Secure Hub 中，系统提示时输入新 PIN。

   对该 PIN 进行身份验证后，Secure Hub 将下载证书。请按照提示进行操作，完成注册。

要在 XenMobile 控制台中查看设备信息，请执行以下操作：

- 转至管理 > 设备，然后选择一个设备以显示命令框。单击显示更多。
- 转至分析 > 控制板。

升级

January 5, 2022

> 提示：**XenMobile Migration Service**
>
> 如果在本地使用 XenMobile Server，我们的免费 XenMobile Migration Service 可以让您开始使用 Endpoint Management。从 XenMobile Server 迁移到 Citrix Endpoint Management 不需要重新注册设备。
>
> 要了解详细信息，请联系您的本地 Citrix 销售人员、系统工程师或 Citrix Partner。以下博客探讨了 XenMobile Migration Service：
>
> New XenMobile Migration Service（新 XenMobile Migration Service）
>
> Making the Case for XenMobile in the Cloud（用作云中的 XenMobile 的示例）

升级到 **XenMobile 10.14** 之前的准备工作

1. 请先将您的 Citrix 许可证服务器更新到 11.16 或更高版本，然后再更新到最新版本的 XenMobile Server 10.14。

   最新版本的 XenMobile 需要 Citrix 许可证服务器 11.16（最低版本）。

   XenMobile 10.14 中的 Customer Success Services 日期（以前称为专享升级服务日期）为 2021 年 9 月 15 日。Citrix 许可证上的 Customer Success Services 日期必须晚于此日期。可以在许可证服务器中的许可证旁边查看该日期。如果要将最新版本的 XenMobile 连接到较旧的许可证服务器环境，连接检查将失败，并且您无法配置许可证服务器。

   要续订许可证上的日期，请从 Citrix 门户下载最新的许可证文件并将该文件上载到许可服务器。有关详细信息，请参阅 Customer Success Services。

2. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序具有以下要求。如果为 Citrix Gateway 配置了 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
3. 如果运行要升级的 XenMobile Server 的虚拟机的 RAM 低于 8 GB，我们建议您将 RAM 增加到至少 8 GB。

4. 建议：安装 XenMobile 更新之前，请使用 VM 中的功能创建系统的快照。此外，还请备份您的系统配置数据库。如果您在升级过程中遇到问题，请完成允许您还原的备份。

升级

可以从 XenMobile 10.13.x 或 10.12.x 直接升级到 XenMobile 10.14。要执行升级，请下载可用的最新二进制文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server >** 产品软件 **> XenMobile Server 10**。在您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击下载文件。要上载升级，请使用 XenMobile 控制台中的发布管理页面。

使用“发布管理”页面进行升级

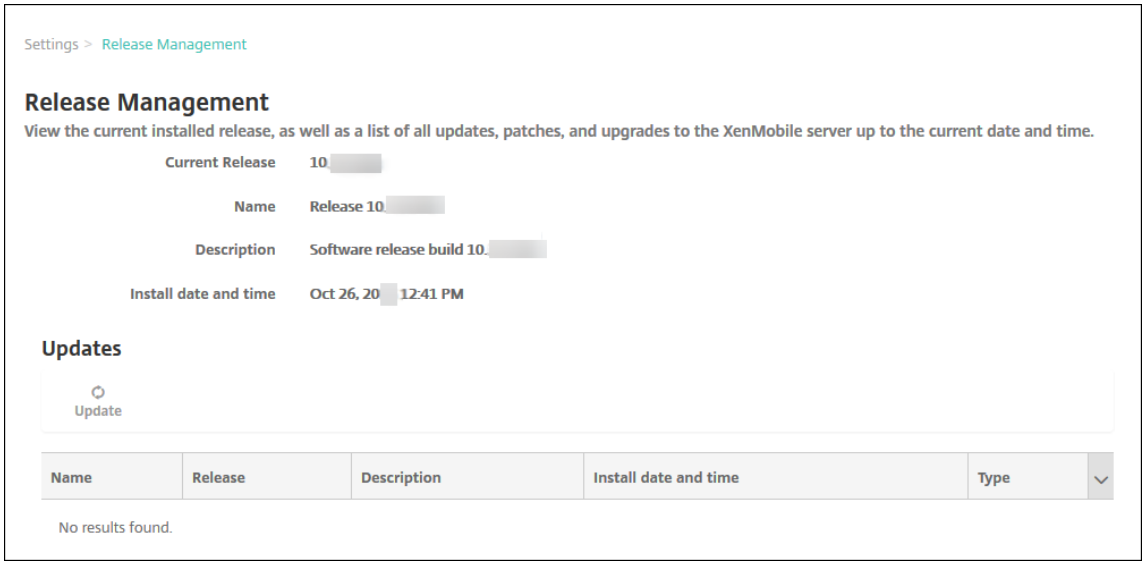
使用发布管理页面可升级到最新版本的 XenMobile Server 。

必备条件：

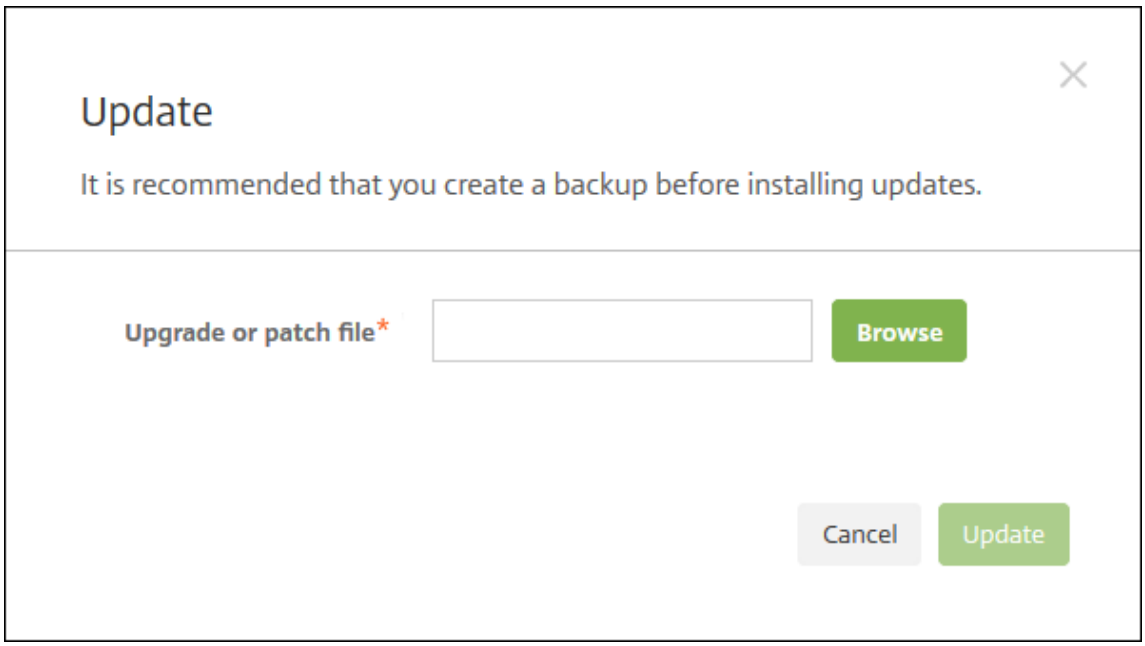
- 检查系统要求。

如果您有群集部署，请参阅本文结尾处的说明。

1. 下载可用的最新二进制文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management**（和 **Citrix XenMobile Server**）**> XenMobile Server (**本地**) >** 产品软件 **> XenMobile Server 10**。在您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击下载文件。
2. 在 XenMobile 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。
3. 单击发布管理。此时将显示发布管理页面。



4. 在更新下方，单击更新。此时将显示更新对话框。



5. 单击浏览并导航到从 Citrix.com 下载的 XenMobile 升级文件所在位置，选择此文件。
6. 单击更新，然后在收到提示时，重新启动 XenMobile。

   如果由于某些原因，更新未能成功完成，会显示一条错误消息以指出问题。系统会恢复到尝试更新之前的状态。

升级之后需要执行的操作

升级后，XenMobile 需要重新启动。可使用 XenMobile CLI 重新启动 XenMobile Server。系统重新启动后清除浏览器缓存非常重要。

如果涉及传出连接的功能停止运行，并且您尚未更改自己的连接配置，请在 XenMobile Server 日志中检查是否存在如下所示的错误：“Unable to connect to the VPP Server: Host name ‘192.0.2.0’ does not match the certificate subject provided by the peer”（无法连接到 VPP 服务器: 主机名 192.0.2.0 与对等机提供的证书使用者不匹配）

证书验证错误指示您需要在 XenMobile Server 上禁用主机名验证。默认情况下，主机名验证对除 Microsoft PKI 服务器以外的传出连接启用。如果主机名验证中断了您的部署，请将服务器属性 **disable.hostname.verification** 更改为 **true**。此属性的默认值为 **false**。

Citrix 将 XenMobile 的新版本或重要更新发布到 Citrix.com。同时，向每个客户的在案联系人发送通知。

升级群集 **XenMobile** 部署

> 重要：
>
> 安装 XenMobile 更新前，请使用虚拟机 (VM) 中的功能创建系统的快照。此外，还请备份您的系统配置数据库。如果您在升级过程中遇到问题，请完成允许您还原的备份。

如果系统是在群集模式下配置的，请按照以下步骤从 XenMobile 10 版本更新每个节点：

1. 在所有节点上从设置 **>** 发布管理上载.bin 文件。
2. 在 CLI 中从 **System Menu**（系统菜单）关闭所有节点。
3. 在 CLI 中从 **System Menu**（系统菜单）提取一个节点，并检查服务是否正在运行。
4. 按顺序逐一提取其他节点。

   如果 XenMobile 无法成功完成更新，会显示一条错误消息以指出问题。XenMobile 随后将系统还原到尝试更新之前的状态。

从 **XenMobile MDM Edition** 升级到 **Enterprise Edition**

对于 iOS 和 Android 设备，可以将 XenMobile MDM Edition 升级到 XenMobile Enterprise Edition。

必备条件

- 正确的 Enterprise 许可证。
- Citrix Gateway 已配置。

升级

1. 转至设置 **>** 许可并验证是否已上载正确的 Enterprise Edition 许可证类型。
2. 转至设置 **>** 服务器属性并将服务器模式属性从 **MDM** 更改为 **ENT**。
3. 转至设置 **> Citrix Gateway** 并配置 Citrix Gateway 详细信息。将身份验证模式设置为与 MDM Edition 相同，即，域 (Active Directory) 身份验证。XenMobile 不支持在用户注册后更改身份验证模式。
4. 可选：转至设置 **>** 客户端属性并启用 Citrix PIN 身份验证。

完成这些步骤后，用户必须执行以下步骤以将设备切换到企业模式。

iOS 用户

1. 关闭 Secure Hub：轻按设备主页按钮两次（快速）并向上滑动 Secure Hub 应用程序。
2. 打开 Secure Hub。

Android 用户

1. 打开 Secure Hub。
2. 转至首选项 **>** 设备信息。
3. 单击刷新策略。

如果启用了 Citrix PIN 身份验证，Secure Hub 将提示用户创建 PIN。用户创建 PIN 后，XenMobile 将在企业模式下配置设备。在 XenMobile 控制台中，管理 **>** 设备页面上设备的 MDM 和 MAM 随后同时显示为活动状态。

用户帐户、角色和注册

October 13, 2021

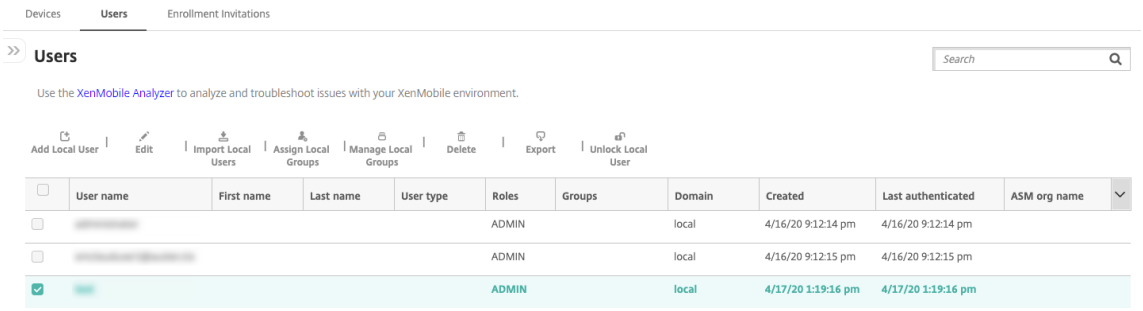
可以在 XenMobile 控制台中的管理选项卡和设置页面上配置用户帐户、角色和注册。除非另有说明，否则本文提供完成以下任务的步骤。

- 用户帐户和组：
  - 从管理 **>** 用户，手动添加用户帐户或使用.csv 预配文件导入帐户并管理本地组。
  - 从设置 **>** 工作流，使用工作流对用户帐户的创建和删除进行管理。
- 用户帐户和组的角色
  - 从设置 **>** 基于角色的访问控制，向用户和组分配预定义角色或权限集合。这些权限控制用户对系统功能的访问级别。有关详细信息，请参阅使用 RBAC 配置角色。
  - 从设置 **>** 通知模板，创建或更新用于自动化操作、注册和发送给用户的标准通知消息的通知模板。配置通知模板以通过三种不同的通道发送消息：Secure Hub、SMTP 或 SMS。有关详细信息，请参阅：创建和更新通知模板。
- 注册安全模式和邀请
  - 从设置 **>** 注册，配置最多七种注册安全模式并发送注册邀请。每种注册安全模式均具有自己的安全级别和用户注册自己的设备必须采取的步骤。
  - 在 XenMobile 中为用户注册启用自动发现

添加、编辑、解锁或删除本地用户帐户

可以手动向 XenMobile 中添加本地用户帐户，也可以使用预配文件导入帐户。有关从预配文件导入用户的步骤，请参阅导入用户帐户。

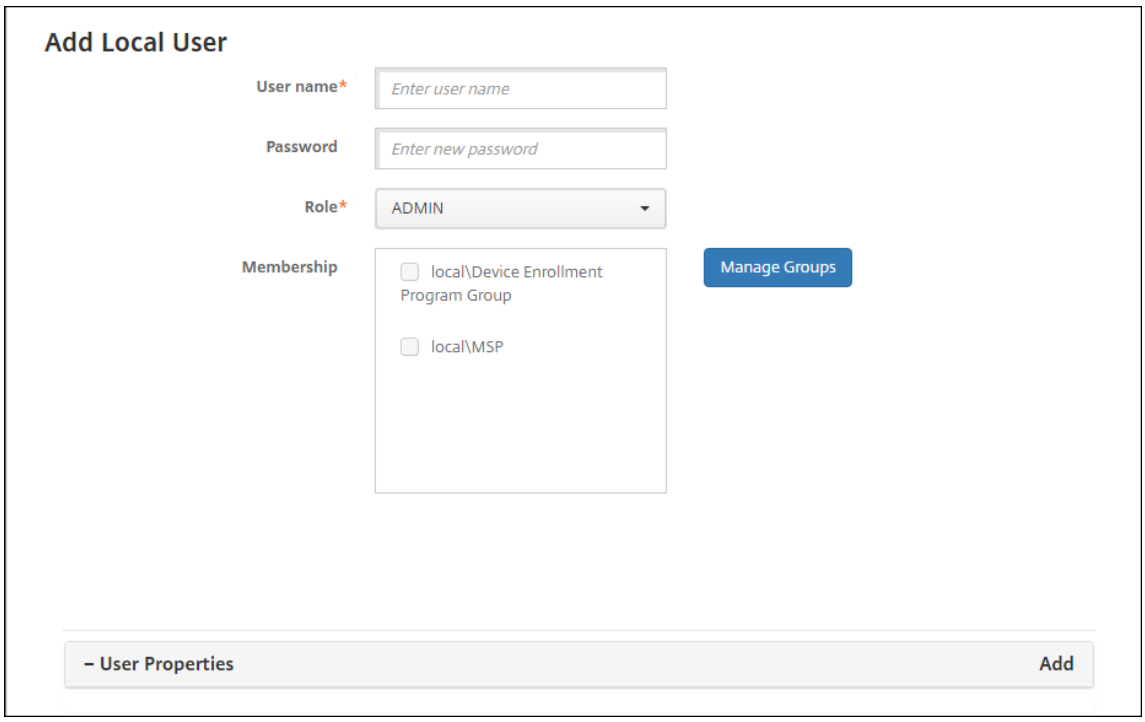
1. 在 XenMobile 控制台中，单击管理 **>** 用户。此时将显示用户页面。



2. 单击显示过滤器以过滤列表。

添加本地用户帐户

1. 在用户页面上，单击添加本地用户。此时将显示添加本地用户页面。



2. 配置以下设置：

   - 用户名：键入名称，这是必填字段。可以在名称中包含空格，也可以包含大写和小写字母。
   - 密码：键入可选用户密码。密码的长度至少为 14 个字符，并且必须满足以下全部条件：
     - 至少包含两个数字
     - 至少包含一个大写字母和一个小写字母
     - 至少包含一个特殊字符
     - 不要包含字典单词或限制单词，例如 Citrix 用户名或电子邮件地址
     - 不要包含三个以上的连续字符和重复字符或键盘模式，例如 1111、1234 或 asdf
   - 角色：在列表中，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
   - 成员身份：在列表中，单击要添加此用户的一个或多个组。
   - 用户属性：添加可选用户属性。对于要添加的每个用户属性，单击添加，然后执行以下操作：
     - 用户属性：在列表中，单击某个属性，然后在该属性旁边的字段中键入用户属性。
     - 单击完成保存用户属性或单击取消。

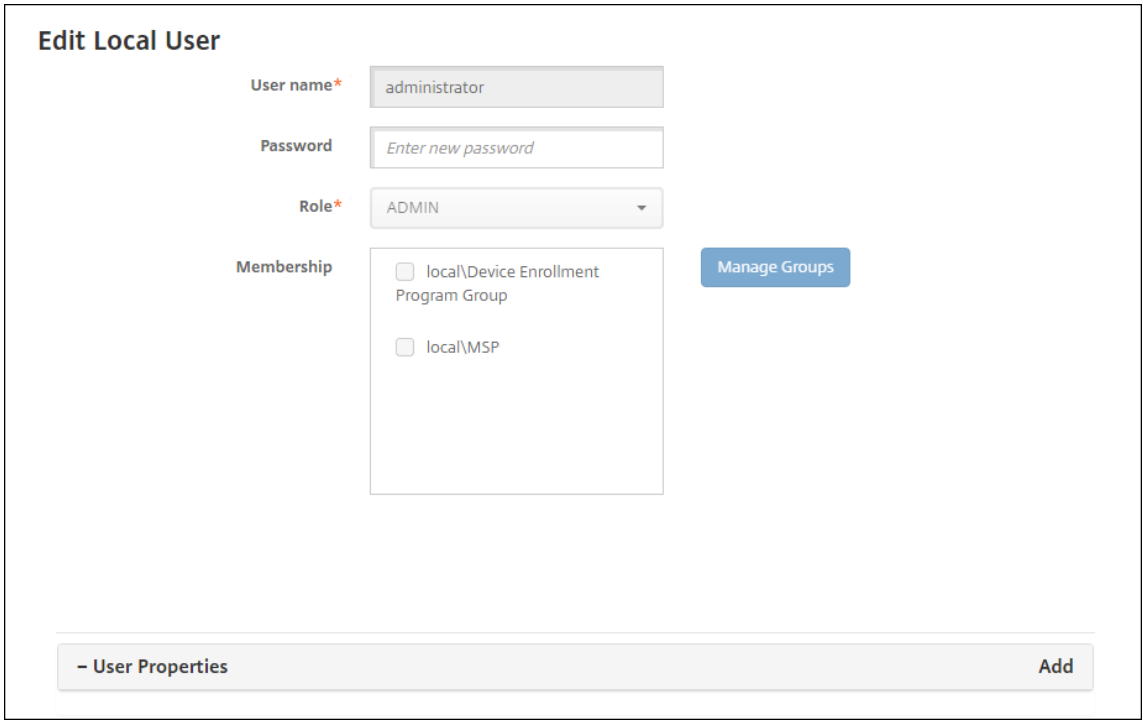
   要删除现有用户属性，请将鼠标悬停在包含此属性的行上，然后单击右侧的 X。属性立即被删除。

   要编辑现有用户属性，请单击属性并进行更改。单击完成保存更改后的列表，或者单击取消保留列表不变。

3. 单击保存。

编辑本地用户帐户

1. 在用户页面上的用户列表中，通过单击选择某个用户，然后单击编辑。此时将显示编辑本地用户页面。



2. 适当更改以下信息：

   - 用户名：无法更改用户名。
   - 密码：更改或添加用户密码。
   - 角色：在列表中，单击用户角色。
   - 成员身份：在列表中，单击要添加或编辑用户帐户的一个或多个组。要从组中删除用户帐户，请取消选中组名称旁边的复选框。
   - 用户属性：请执行以下操作之一：
     - 对于您要更改的各个用户属性，请单击属性并进行更改。单击完成保存更改后的列表，或者单击取消保留列表不变。
     - 对于要添加的每个用户属性，单击添加，然后执行以下操作：
       * 用户属性：在列表中，单击某个属性，然后在该属性旁边的字段中键入用户属性。
       * 单击完成保存用户属性或单击取消。
     - 对于要删除的每个现有用户属性，请将鼠标悬停在包含此属性的行上，然后单击右侧的 **X**。属性立即被删除。

3. 单击保存以保存您所做的更改，或者单击取消保留用户不变。

解锁本地用户帐户

1. 在用户页面上的用户帐户列表中，通过单击选择某个用户帐户。

2. 单击解锁本地用户。此时将显示确认对话框。
3. 单击解锁以解锁用户帐户，或者单击取消保持用户不变。

删除本地用户帐户

1. 在用户页面上的用户帐户列表中，通过单击选择某个用户帐户。

可以通过选中每个用户帐户旁边的复选框，选择多个要删除的用户帐户。

1. 单击删除。此时将显示确认对话框。
2. 单击删除以删除用户帐户或单击取消。

删除 **Active Directory** 用户

要一次删除一个或多个 Active Directory 用户，请选择这些用户，然后单击删除。

如果要删除的用户具有已注册的设备，而您希望重新注册这些设备，请先删除这些设备，然后再重新注册。要删除某个设备，请转至管理 **>** 设备，选择该设备，然后单击删除。

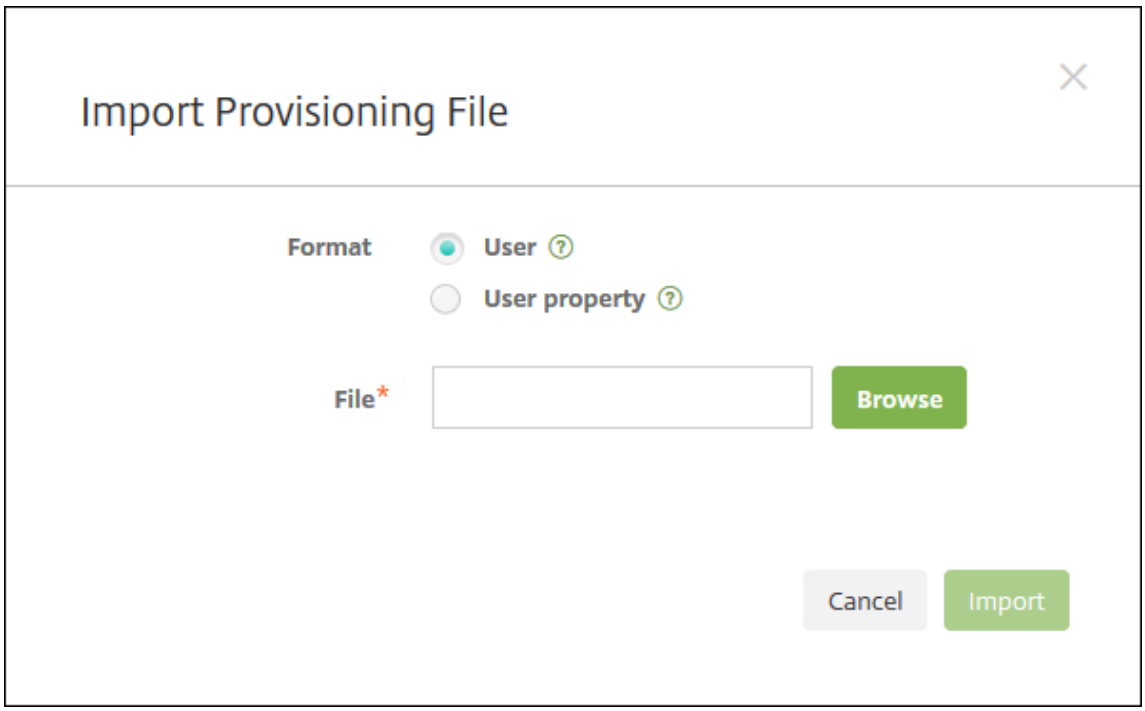
导入用户帐户

您可以从称为预配文件的.csv 文件导入本地用户帐户和属性，该文件可以手动创建。有关设置预配文件格式的详细信息，请参阅预配文件的格式。

> 注意：
>
> - 对于本地用户，请使用域名以及导入文件中的用户名。例如，指定 username@domain。如果在 XenMobile 中将创建或导入的本地用户用于托管域，则用户无法使用对应的 LDAP 凭据进行注册。
> - 如果将用户帐户导入到 XenMobile 内部用户目录，请禁用默认域以加快导入过程的速度。请谨记，禁用域会影响注册，因此，请在内部用户导入完成后重新启用默认域。
> - 本地用户可以采用用户主体名称 (UPN) 格式。但是，Citrix 建议您不要使用托管域。例如，如果 example.com 处于托管状态，请勿使用以下 UPN 格式创建本地用户：user@example.com。

准备好预配文件后，请按照以下步骤将此文件导入到 XenMobile 中。

1. 在 XenMobile 控制台中，单击管理 **>** 用户。此时将显示用户页面。
2. 单击导入本地用户。此时将显示导入预配文件对话框。



3. 对于要导入的预配文件的格式，选择用户或属性。
4. 通过单击浏览并导航到要使用的预配文件所在位置，选择此文件。
5. 单击导入。

预配文件的格式

可以手动创建预配文件，以便将用户帐户和属性导入到 XenMobile 中。有效格式如下：

- 用户置备文件字段：`user;password;role;group1;group2`
- 用户属性置备文件字段：`user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> 注意：
>
> - 使用分号 (;) 分隔预配文件中的字段。如果某个字段的某一部分包含分号，请使用反斜杠字符 (\) 进行转义。例如，在预配文件中以 `propertyV\\;test\\;1\\;2` 格式键入属性 `propertyV;test;1;2`。
> - 角色的有效值为预定义的角色 USER、ADMIN、SUPPORT 和 DEVICE_PROVISIONING 以及您定义的任何其他角色。
> - 使用句点字符（.）作为分隔符来创建组层次结构。请勿在组名称中使用句点。
> - 属性预配文件中的属性使用小写。数据库区分大小写。

用户预配内容示例

条　目　`user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` 表示：

- 用户：user01
- 密码：pwd;01
- 角色：USER
- 组：
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

另一个示例 AUser0;1.password;USER;ActiveDirectory.test.net 表示：

- 用户：AUser0
- 密码：1.password
- 角色：USER
- 组：ActiveDirectory.test.net

用户属性预配内容示例

条目 user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value 表示：

- 用户：user01
- 属性 **1**
  - **name**：propertyN
  - 值：propertyV;test;1;2
- 属性 **2**：
  - **name**：prop 2
  - 值：prop2 value

配置注册安全模式

配置设备注册安全模式以在 XenMobile 中为设备注册指定安全级别和通知模板。

XenMobile 提供七种注册安全模式，每种均具有自己的安全级别和用户注册其设备必须执行的步骤。在 XenMobile Server 控制台的设置 **>** 注册页面配置注册安全模式。

您可以在自助服务门户上提供某些模式。用户可以从门户中生成允许其注册自己的设备的注册链接。iOS、iPadOS、macOS、Android Enterprise 和旧版 Android 用户可以选择从门户向自己发送注册邀请。注册邀请不适用于 Windows 设备。

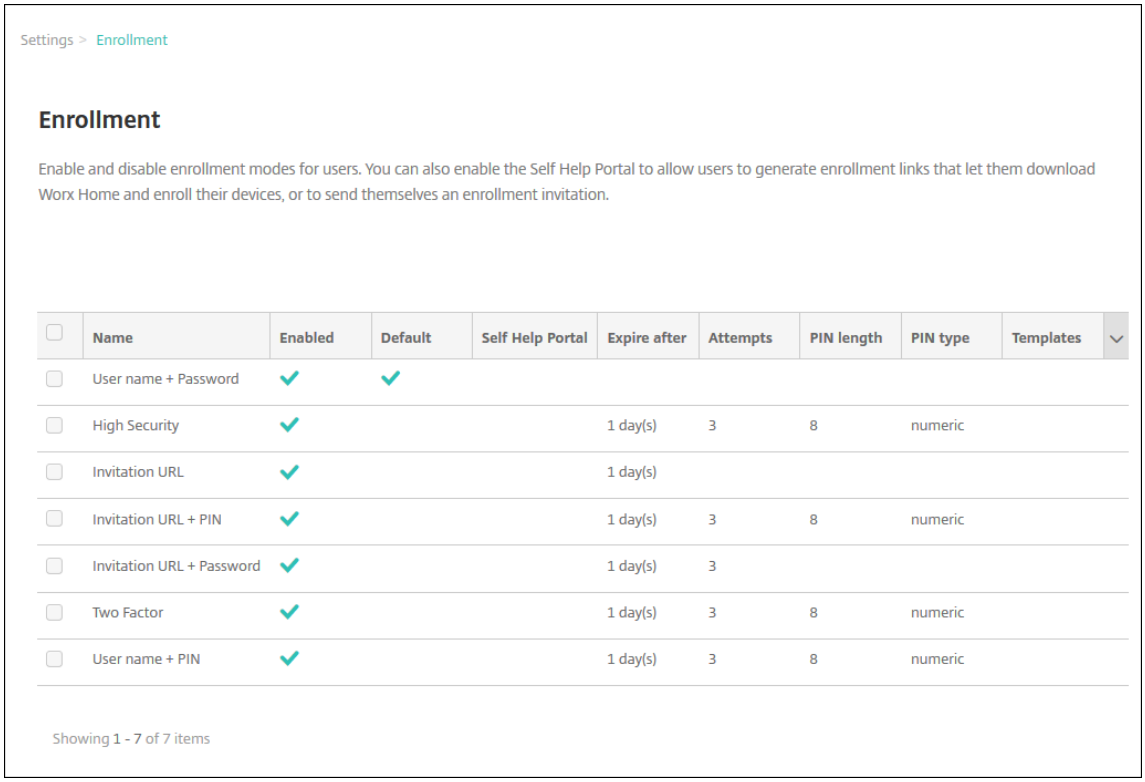
从管理 **>** 注册邀请页面发送注册邀请。有关信息，请参阅发送注册邀请。

> 注意：
>
> 如果您打算使用自定义通知模板，必须在配置注册安全模式之前设置模板。有关通知模板的详细信息，请参阅创建或更新通知模板。

1. 在 XenMobile 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. 单击注册。此时将显示注册页面，其中包含所有可用注册安全模式的表格。默认情况下，启用所有注册安全模式。
3. 在列表中选择任何注册安全模式以对其进行编辑。然后将该模式设置为默认模式、禁用该模式或允许用户通过自助服务门户访问。

> 注意：
>
> 选中注册安全模式旁边的复选框时，选项菜单将显示在注册安全模式列表上方。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。



可从这些注册安全模式中选择：

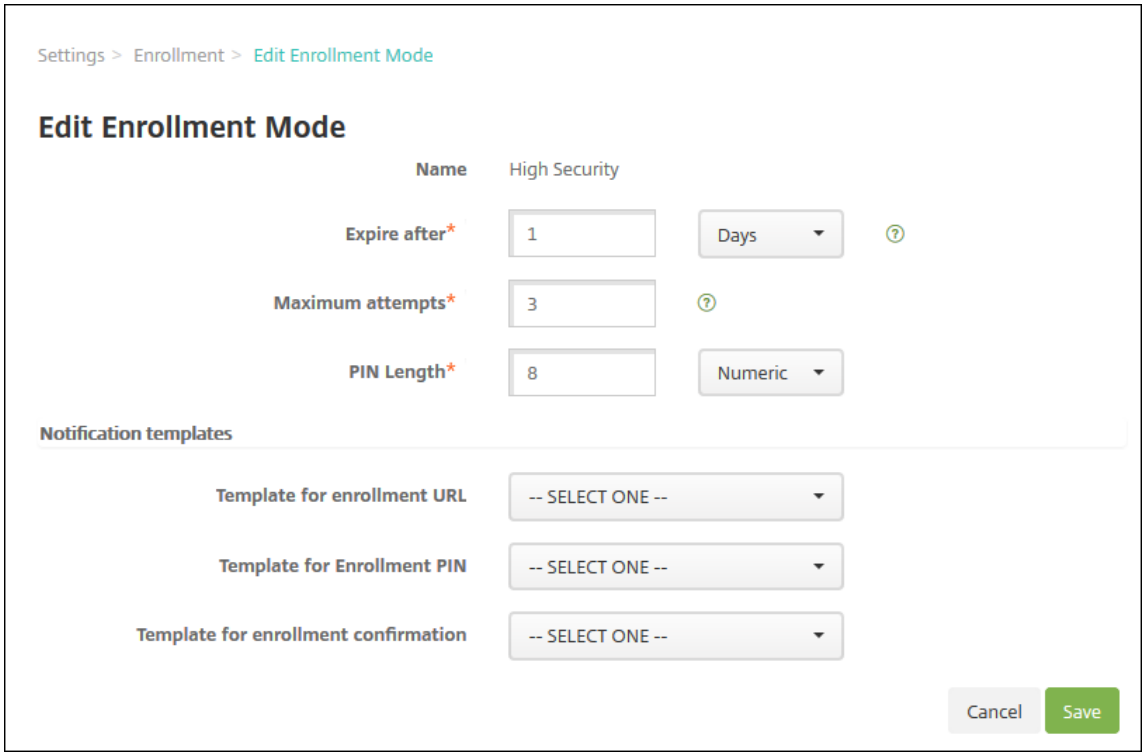
- 用户名 + 密码
- 高安全性
- 邀请 URL
- 邀请 URL + PIN
- 邀请 URL + 密码
- 双重身份验证
- 用户名 + PIN

您可以使用注册邀请来限制仅收到邀请的用户可以注册。要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。对于使用用户名 **+** 密码、双重身份验证或用户名 **+ PIN** 注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

您可以使用一次性 PIN (OTP) 注册邀请作为双重身份验证解决方案。OTP 注册邀请控制用户可以注册的设备数。OTP 邀请不适用于 Windows 设备。

编辑注册安全模式

1. 在注册列表中，选择注册安全模式，然后单击编辑。此时将显示编辑注册模式页面。您选择的模式决定了显示的选项。



2. 适当更改以下信息：

   - 此时间后过期：键入过期期限，过了此期限后用户将无法注册其设备。此值显示在用户和组注册邀请配置页面。

     键入 **0** 可防止邀请过期。

   - 天：在列表中，单击天或小时，对应于您在此时间后过期中输入的过期期限。
   - 最大尝试次数：键入用户可以尝试注册的次数，超出此次数后用户将被锁定，无法进行注册过程。此值显示在用户和组注册邀请配置页面。

     键入 **0** 表示尝试次数不受限制。

   - **PIN** 长度：键入用于设置生成的 PIN 的长度的数字。
   - 数字：在列表中，单击数字或字母数字以选择 PIN 类型。
   - 通知模板：
     - 注册 **URL** 模板：在列表中，单击用于注册 URL 的模板。例如，注册邀请模板向用户发送电子邮件或 SMS。方法取决于您是如何配置用于允许用户在 XenMobile 中注册其设备的模板。有关通知模板的详细信息，请参阅创建或更新通知模板。
     - 注册 **PIN** 模板：在列表中，单击用于注册 PIN 的模板。

- 注册确认模板：在列表中，单击用于向用户通知已成功注册的模板。

3. 单击保存。

将注册安全模式设为默认模式

将注册安全模式设为默认模式后，若不选择其他注册安全模式，此模式将用于所有设备注册请求。如果未将任何注册安全模式设为默认模式，必须为每个设备注册创建注册请求。

> 注意：
>
> 可以用作默认注册模式的注册安全模式只能是仅限用户名 **+** 密码、双重或用户名 **+ PIN**。

1. 选择默认注册安全模式：用户名 **+** 密码、双重或用户名 **+ PIN**。

   要将某个模式用作默认模式，请先启用它。

2. 单击默认值。所选模式现已成为默认模式。如果将任何其他注册安全模式设为默认模式，此模式将不再作为默认模式。

禁用注册安全模式

禁用注册安全模式将使此模式不可供用户使用，既不可用于组注册邀请，也不可在自助服务门户中提供。通过禁用一种注册安全模式并启用另一种注册模式，可以更改用户能够注册其设备的方式。

1. 选择注册安全模式。

   不能禁用默认注册安全模式。如果要禁用默认注册安全模式，必须首先删除其默认状态。

2. 单击禁用。注册安全模式不再处于启用状态。

在自助服务门户上启用注册安全模式

通过在自助服务门户上启用注册安全模式，可允许用户单独在 XenMobile 中注册其设备。

> 注意：
>
> - 注册安全模式必须启用并绑定通知模板，才能在自助服务门户上提供。
> - 同一时间只能在自助服务门户上启用一种注册安全模式。

1. 选择注册安全模式。
2. 单击自助服务门户。此注册安全模式现已在自助服务门户上提供，可供用户使用。已经在自助服务门户上启用的任何模式均不再可供用户使用。

添加或删除组

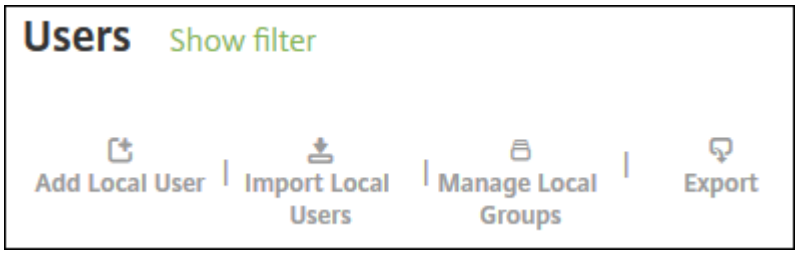
在 XenMobile 控制台中以下页面上的管理组对话框中管理组：用户、添加本地用户或编辑本地用户。没用组编辑命令。

如果删除组，请谨记删除组不影响用户帐户。删除组只是删除用户与该组的关联。用户还会丧失此组关联的交付组提供的应用程序或配置文件的访问权限，但是其他组关联性不受影响。如果用户不与任何其他本地组关联，它们将在顶层关联。

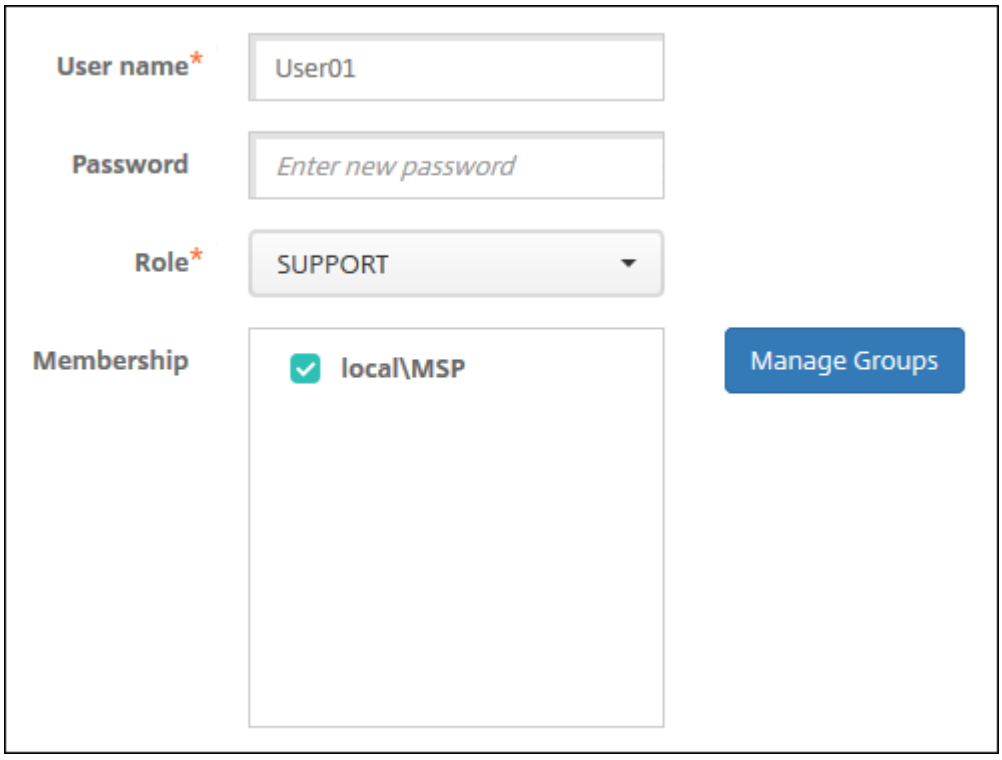
添加本地组

1. 执行以下操作之一：

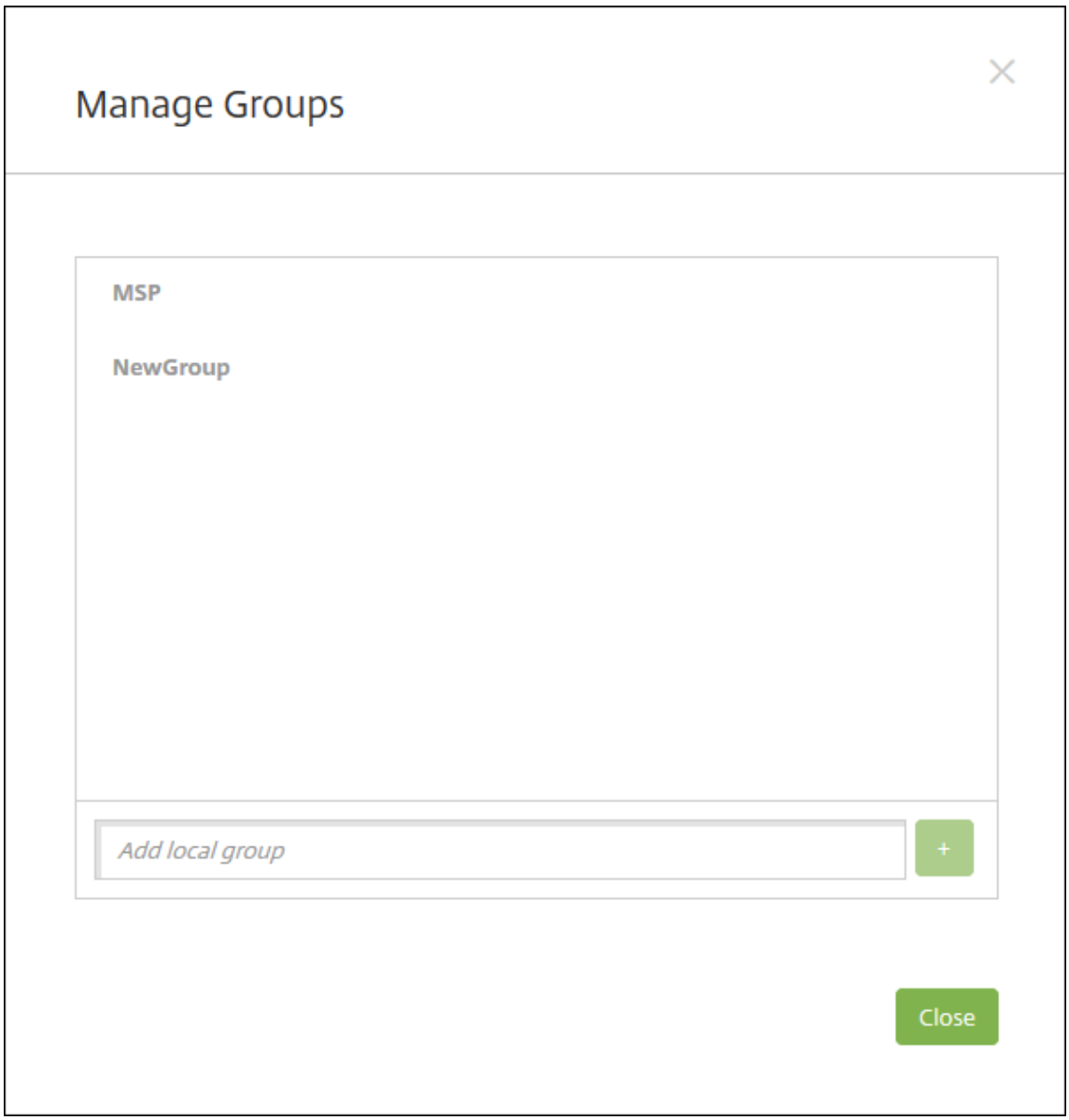
   - 在用户页面上，单击管理本地组。



   - 在添加本地用户页面或编辑本地用户页面上，单击管理组。



   此时将显示管理组对话框。



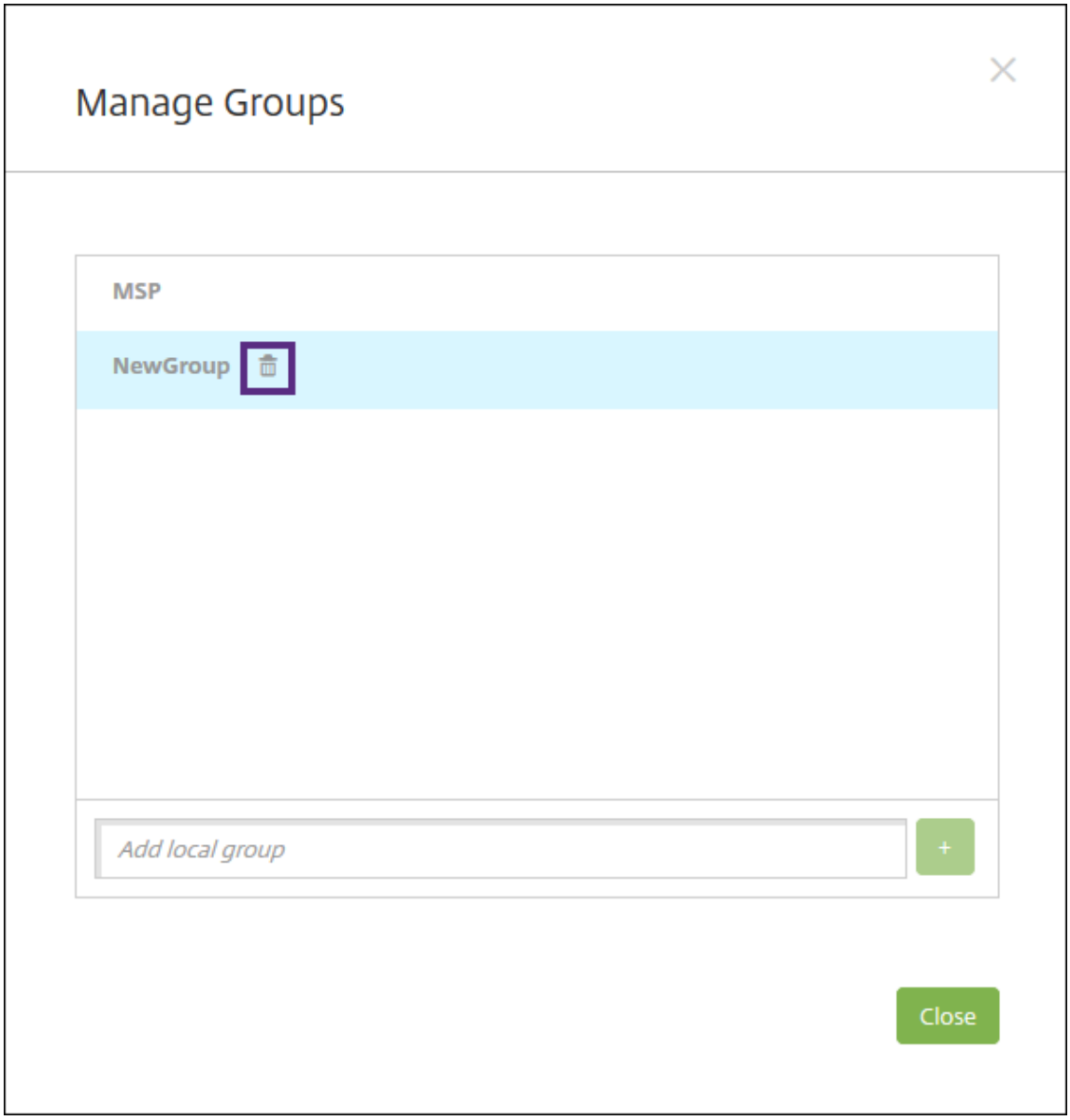
2. 在组列表下方，键入组名称，然后单击加号 (**+**)。用户组已添加到列表中。
3. 单击关闭。

删除组

删除组不会影响用户帐户。删除组只会删除用户与该组的关联。用户还会丧失该组关联的交付组提供的应用程序或配置文件的访问权限。但是，任何其他组关联仍保持不变。如果用户不与任何其他本地组关联，它们将在顶层关联。

1. 执行以下操作之一：
   - 在用户页面上，单击管理本地组。
   - 在添加本地用户页面或编辑本地用户页面上，单击管理组。

此时将显示管理组对话框。



2. 在管理组对话框上，单击要删除的组。
3. 单击组名称右侧的垃圾桶图标。此时将显示确认对话框。
4. 单击删除以确认操作并删除该组。

   > 重要：
   >
   > 此操作无法撤消。

5. 在管理组对话框上，单击关闭。

创建和管理工作流

可以使用工作流对用户帐户的创建和删除进行管理。应先确定组织中有权批准用户帐户请求的人员，才能使用工作流。然后可以使用工作流模板创建和批准用户帐户请求。

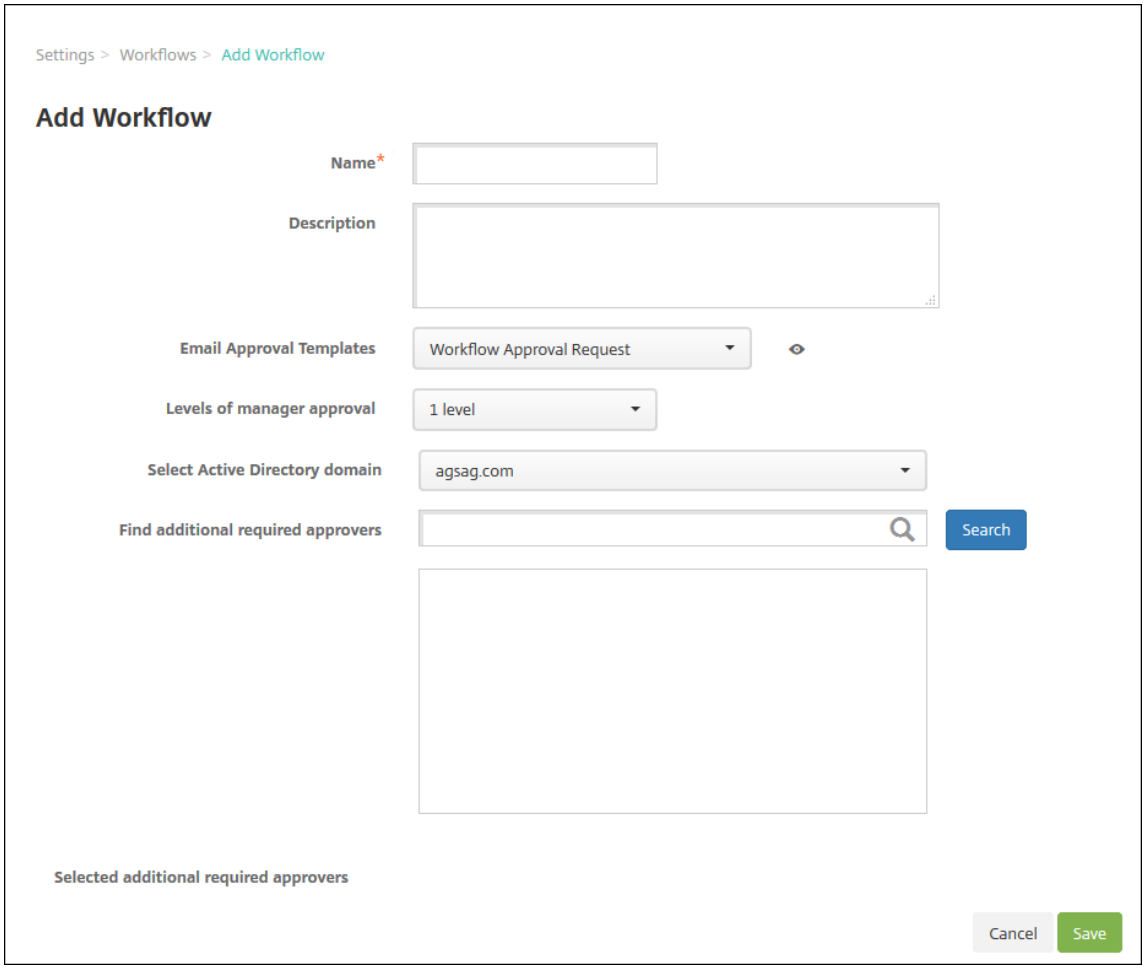
首次设置 XenMobile 时，要配置工作流电子邮件设置，您必须先配置此设置才能使用工作流。随时可以更改工作流电子邮件设置。这些设置包括电子邮件服务器、端口、电子邮件地址以及创建用户帐户的请求是否需要进行审批。

可以在 XenMobile 中的两个位置配置工作流：

- 在 XenMobile 控制台中的工作流页面上。在工作流页面上，可以配置多个用于应用程序配置的工作流。在“工作流”页面上配置工作流时，可以在配置应用程序时选择工作流。
- 配置应用程序连接器时，在应用程序中提供工作流名称，然后配置可以审批用户帐户请求的人员。请参阅向 XenMobile 添加应用程序。

可以为用户帐户分配最多三个经理审批级别。如果需要其他人员批准用户帐户，可以使用其姓名或电子邮件地址搜索和选择这些人员。XenMobile 找到相应的人员时，您可以将其添加到工作流中。工作流中的所有人员都将收到电子邮件，以批准或拒绝新用户帐户。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击工作流。此时将显示工作流页面。
3. 单击添加。此时将显示添加工作流页面。



4. 配置以下设置：

- 名称：键入工作流的唯一名称。
- 说明：（可选）键入工作流的说明。
- 电子邮件审批模板：在列表中，选择要指定的电子邮件审批模板。在 XenMobile 控制台中设置下方的通知模板部分创建电子邮件模板。单击此字段右侧的眼睛图标，即可预览正在配置的模板。
- 经理审批级别：在列表中，选择此工作流所需的经理审批级别数。默认值为 **1** 级。可能的选项包括：
  - 不需要
  - 1 级
  - 2 级
  - 3 级
- 选择 **Active Directory** 域：在列表中，选择用于工作流的合适 Active Directory 域。
- 查找所需的其他审批者：在搜索字段中键入姓名，然后单击搜索。源于 Active Directory 的姓名。
- 姓名显示在此字段中后，选中姓名旁边的复选框。姓名和电子邮件地址显示在选定的其他所需审批者列表中。
  - 要从列表中删除某个姓名，请执行以下操作之一：
    * 单击搜索以查找选定域中的所有人员列表。

    * 在搜索框中键入完整姓名或部分姓名，然后单击搜索以限制搜索结果。
    * 在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。滚动列表，并取消选中要删除的各个姓名旁边的复选框。

5. 单击保存。已创建的工作流显示在工作流页面上。

创建工作流后，您可以查看工作流详细信息，查看与工作流相关的应用程序，或者删除工作流。工作流创建后无法进行编辑。如果需要使用不同审批级别或审批者的工作流，请创建另一个工作流。

查看详细信息和删除工作流

1. 在工作流页面上的现有工作流列表中，选择一个特定的工作流。为此，请单击列表中的行，或者选中工作流旁边的复选框。
2. 要删除工作流，请单击删除。此时将显示确认对话框。再次单击删除。

> 重要：
>
> 此操作无法撤消。

注册配置文件

January 5, 2022

注册配置文件指定以下内容：

- 适用于 Android 和 iOS 设备的设备管理注册选项。对于 Android，可用于 MDM+MAM (ENT) 服务器模式的注册选项与可用于 MDM 模式的选项不同。
- 适用于 Android 和 iOS 设备的应用程序管理注册选项。
- 其他注册选项：
  - 是否限制用户可以注册的设备数量。
    如果达到设备限制，则将显示一条错误消息，通知用户已超出设备注册限制。
  - 是否允许用户拒绝设备管理。

可以使用注册配置文件在单个 XenMobile Server 控制台中合并多个用例和设备迁移路径。一些用例包括：

- 移动设备管理（仅 MDM）
- MDM+ 移动应用程序管理 (MAM)
- 仅 MAM
- 公司拥有的注册
- BYOD 注册（选择退出 MDM 注册的功能）
- 将 Android 设备管理员注册迁移到 Android Enterprise 注册（完全托管、工作配置文件、专用设备）

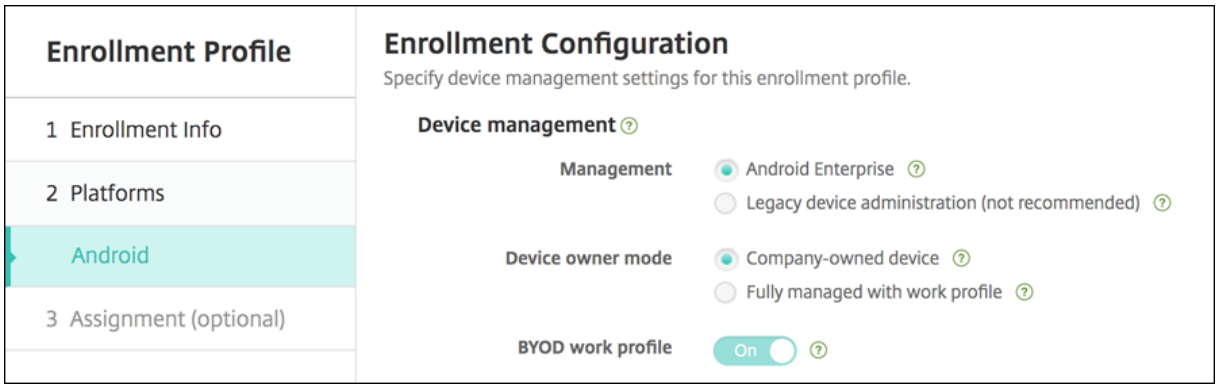
创建交付组时，可以使用名为 Global 的默认注册配置文件或者指定不同的注册配置文件。

按平台划分的注册配置文件功能包括以下内容。

- 对于 **Android** 设备：指定设备所有者模式。例如：完全托管、使用工作配置文件完全托管和 BYOD 工作配置文件。仅当您拥有 XenMobile 的 Enterprise 或 Advanced 许可证时，才会显示专用设备选项。默认情况下，新设备会在 Android Enterprise 和应用程序管理中注册。注册安全模式用户名 **+ PIN**、邀请 **URL**、邀请 **URL + PIN** 以及邀请 **URL +** 密码不适用于 Android Enterprise。
- 对于 **iOS** 设备：指定设备注册类型：“设备注册”或“不管理设备”。仅当您拥有适用于 XenMobile 的企业或高级许可证时，iOS 设置才会显示。默认情况下，新设备在 Apple 设备管理和应用程序管理中注册。

如果您不需要为 Android 设备注册专用设备，也不需要为 Android 或 iOS 设备注册仅 MAM 设备，则可以禁用服务器属性 `enable.multimode.xms`。但是，保持此属性处于启用状态意味着您只需要一个 XenMobile Server 即可处理所有类型的注册配置文件。请参阅服务器属性。

禁用 `enable.multimode.xms` 时，只有此屏幕截图中的设置可用：

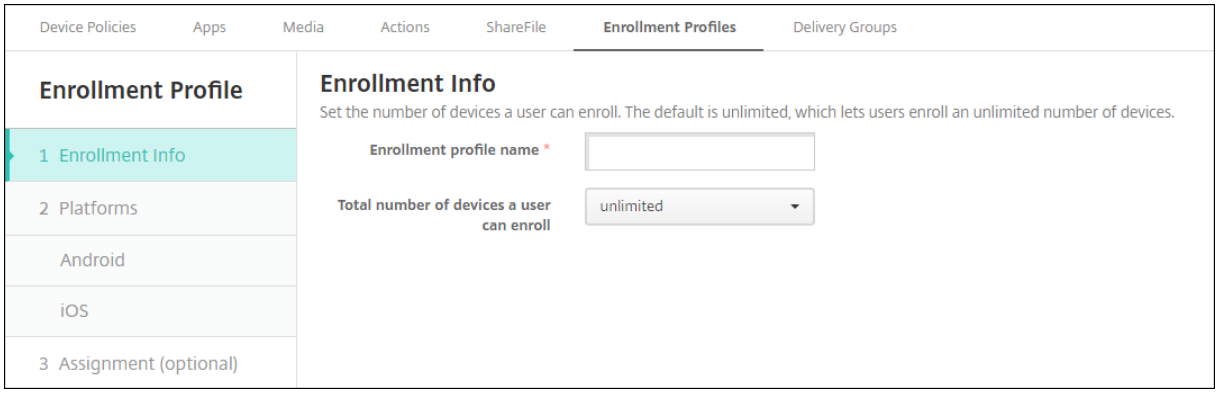


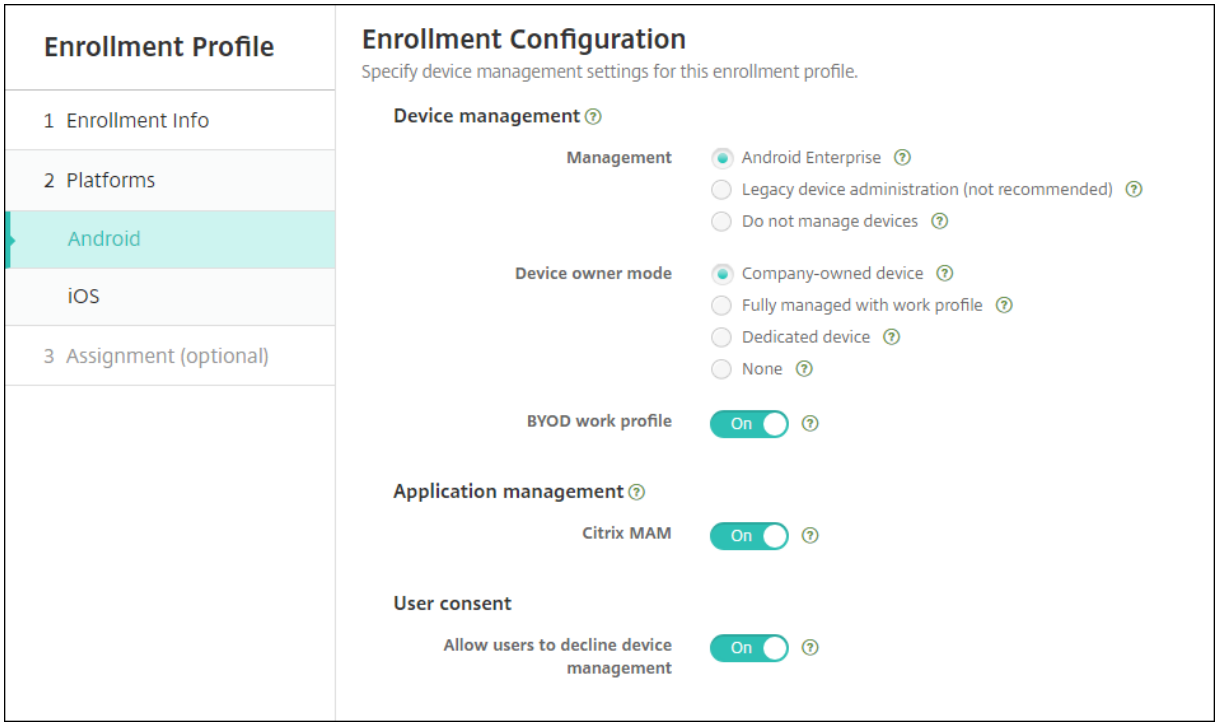
有关这些设置的更多详细信息，请参阅 Android Enterprise。

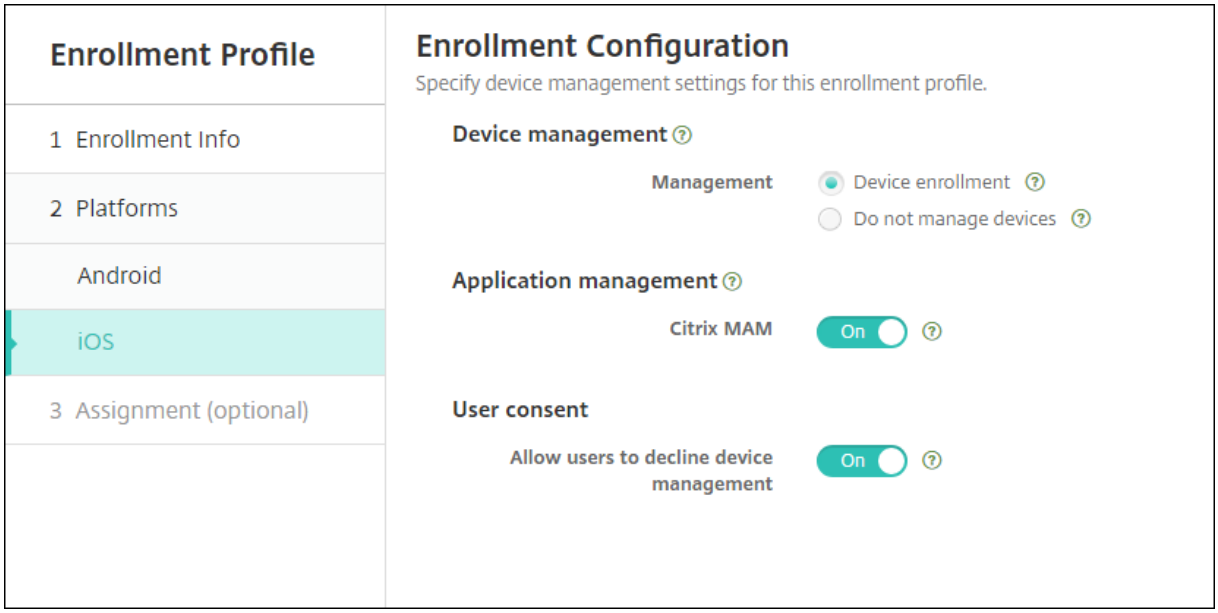
全局注册配置文件

默认注册配置文件的名称为 Global。在您有机会创建注册配置文件之前，全局配置文件对测试非常有用。

以下屏幕截图显示了全局注册配置文件的默认设置。







注册配置文件、交付组和注册

注册配置文件和交付组按如下所示进行交互：

- 可以将注册配置文件附加到一个或多个交付组。
- 如果用户属于具有不同注册配置文件的多个交付组，该交付组的名称决定使用的注册配置文件。XenMobile Server 选择按字母顺序排列的交付组列表中最后显示的交付组。例如，假设您有以下对象：
  - 两个注册配置文件，名为 “EP1” 和 “EP2”。

  - 两个交付组，名为“DG1”和“DG2”。
  - “DG1”与“EP1”相关联。
  - “DG2”与“EP2”相关联。

  如果注册用户同时位于“DG1”和“DG2”交付组中，XenMobile Server 将使用“EP2”注册配置文件来确定用户的注册类型。

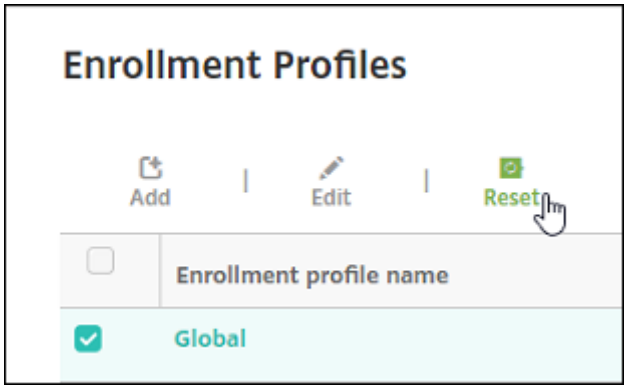
- 部署顺序仅适用于交付组中具有为 MDM（设备管理）配置的注册配置文件的设备。
- 设备注册后，对注册配置文件所做的某些更改需要重新注册：
  - 将 MAM 添加到为 MDM 配置的注册配置文件。
  - 将注册到 MDM 中的设备移动到配置为执行 MDM+MAM 的交付组。该更改仅影响新设备注册。现有设备注册不受影响。
  - 将 MDM 添加到为 MAM 配置的注册配置文件。
- 切换到其他注册配置文件不会影响现有的已注册设备。但是，用户必须先取消注册然后重新注册这些设备，才能使更改生效。

创建注册配置文件

1. 在 XenMobile Server 控制台中，转到配置 **>** 注册配置文件。
2. 在注册信息页面上，键入配置文件的描述性名称。默认情况下，用户可以注册的设备数不受限制。选择一个值以限制每个用户的设备数量。此限制适用于用户注册的 MAM 或 MDM 托管 Android 和 iOS 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
   - iOS：支持的注册方法
4. 在分配页面上，将一个或多个交付组附加到注册配置文件。

   用户可能属于具有不同注册配置文件的多个交付组。在这种情况下，交付组的名称决定使用的注册配置文件。XenMobile 选择按字母顺序排列的交付组列表中最后显示的交付组。要创建交付组，请转到配置 **>** 交付组。

您的注册配置文件列表显示在配置 **>** 注册配置文件页面上。要编辑全局配置文件或将其重置为原始默认设置，请选择全局配置文件对应的行，然后单击重置。您无法删除全局配置文件。



使用 RBAC 配置角色

January 5, 2022

每个基于角色的访问控制 (RBAC) 预定义角色都具有某些关联的访问权限和功能权限。本文描述其中的每个权限可以执行的操作。要获取每个内置角色的默认权限的完整列表，请下载基于角色的访问控制默认设置。

应用权限时，您将定义 RBAC 角色有权管理的用户组。默认管理员无法更改应用的权限设置。默认情况下，所应用的权限适用于所有用户组。

进行分配时，要向组分配 RBAC 角色，以便用户组拥有 RBAC 管理员权限。

> 重要：
>
> 在“设置”权限下，RBAC 权限向管理员用户授予完全访问权限，包括分配自己的权限的能力。请仅向打算提供控制 Endpoint Management 系统中的所有对象的功能的用户授予此访问权限。

本文包含以下各节：

管理角色

具有预定义管理员角色的用户具有或不具有 XenMobile 中以下功能的访问权限。默认情况下，启用授权访问（自助服务门户除外）、控制台功能以及应用权限。

授权访问

管理控制台访问	管理员有权访问 XenMobile 控制台上的所有功能。
自助门户访问	管理员不具有自助门户访问权限。
共享的设备注册程序	管理员不具有“共享设备注册人员”访问权限。此功能适用于需要注册共享设备的用户。
远程支持访问	管理员拥有远程支持访问权限。*
公共 API 访问	管理员有权访问公共 API，以便以编程方式执行可以在 XenMobile 控制台上执行的操作。这些操作包括管理证书、应用程序、设备、交付组和本地用户。

COSU 设备注册器	如果未使用注册配置文件配置此功能，则为管理员提供注册专用 Android Enterprise 设备（又称为 COSU 设备）的方法。

* 通过 Remote Support，您的技术支持代表能够远程控制托管的 Windows CE 和 Android 移动设备。屏幕录像功能仅在 Samsung Knox 设备上受支持。远程支持不适用于本地群集 XenMobile Server 部署。自 2019 年 1 月 1 日起，远程支持功能不再向新客户提供。现有客户可以继续使用此产品，但 Citrix 将不提供增强功能或修复。

控制台功能

管理员对 XenMobile 控制台具有不受限制的访问权限。

控制板	控制板是管理员在登录 XenMobile 控制台后看到的第一个页面。控制板显示有关通知和设备的基本信息。
报告	分析 **>** 报告页面提供预定义的报告，您可以利用这些报告分析应用程序和设备部署情况。
设备	在管理 **>** 设备页面中，可以管理用户设备。可以在此页面上逐个添加设备，也可以通过导入设备预配文件一次添加多个设备。
本地用户和组	在管理 **>** 用户页面中，可以添加、编辑或删除本地用户和本地用户组。
注册	在管理 **>** 注册邀请页面中，可以管理如何邀请用户在 XenMobile 中注册其设备。
策略	在配置 **>** 设备策略页面中，可以管理 VPN 和 Wi-Fi 等设备策略。
应用程序	在配置 **>** 应用程序页面中，可以管理用户能够在其设备上安装的各种应用程序。
媒体	在配置 **>** 媒体页面中，可以管理用户能够在其设备上安装的各种媒体。
操作	在配置 **>** 操作页面中，可以管理触发事件的响应。
注册配置文件	在配置 **>** 注册配置文件页面中，可以配置注册配置文件（模式）以允许用户注册其设备。
交付组	在配置 **>** 交付组页面中，可以管理交付组以及与其关联的资源。
设置	在设置页面中，可以管理系统设置，例如，客户端和服务器属性、证书和凭据提供程序。重要：这些设置包括 RBAC 权限。RBAC 权限向管理员授予完全访问权限，包括分配自己的权限的能力。请仅向打算提供控制 Endpoint Management 系统中的所有对象的功能的用户授予此访问权限。
支持	在故障排除和支持页面中，可以执行运行诊断和生成日志等故障排除活动。

设备

管理员可以通过设置设备限制、设置并向设备发送通知、管理设备上的应用程序等操作，访问控制台各处的设备功能。

完全擦除设备	擦除设备上的所有数据和应用程序，包括内存卡（如果设备具有内存卡）。
清除限制	删除一项或多项设备限制。
选择性擦除设备	擦除设备上的所有公司数据和应用程序，保留个人数据和应用程序。
查看位置	查看设备的位置以及在设备上设置地理区域限制。包括：定位设备、查看设备的位置、跟踪设备、跟踪设备位置随时间的变化。
锁定设备	远程锁定设备，使用户无法使用设备。
解锁设备	远程解锁设备，使用户可以使用设备。
锁定容器	远程锁定设备上的企业容器。
解锁容器	远程解锁设备上的企业容器。
重置容器密码	重置企业容器密码。
启用 ASM DEP/绕过激活锁	启用激活锁时，在受监督的 iOS 设备上存储绕过码。如果需要擦除该设备，请使用此代码自动清除激活锁。
使设备响铃	远程使 Windows 设备以最高音量响铃 5 分钟。
重新启动设备	从 XenMobile 控制台重新启动 Windows 设备。
部署到设备	向设备发送应用程序、通知、限制等。
编辑设备	更改设备上的设置。
通知设备	向设备发送通知。
添加/删除设备	从 XenMobile 添加或删除设备。
设备导入	通过文件向 XenMobile 导入一组设备。
导出设备表	从“设备”页面收集设备信息，并将其导出到.csv 文件。
吊销设备	禁止设备连接到 XenMobile。
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 XenMobile。在 iOS 中，用户可以登录，但无法访问应用程序。
应用程序擦除	在 Android 上，此操作将删除用户的 XenMobile 帐户。在 iOS 上，此操作将删除用户访问 XenMobile 功能所需的加密密钥。
查看软件清单	查看设备上安装的软件。

请求使用 AirPlay 镜像	请求启动 AirPlay 流。
停止使用 AirPlay 镜像	停止 AirPlay 流。
启用丢失模式	在管理 **>** 设备上，可以将受监督的设备置于丢失模式，以阻止锁屏界面上的受监督设备。丢失模式还允许您在设备丢失或被盗时定位设备。
禁用丢失模式	在管理 **>** 设备上，可以禁用设置为丢失模式的设备的丢失模式。
操作系统更新设备	可以在设备中部署“控制操作系统更新”设备策略。
关闭设备	从 XenMobile 控制台关闭 iOS 设备。
重新启动设备	从 XenMobile 控制台重新启动 iOS 设备。

本地用户和组

管理员在 XenMobile 中的管理 **>** 用户页面上管理本地用户和本地用户组。

添加本地用户
删除本地用户
编辑本地用户
导入本地用户
导出本地用户
本地用户组
获取本地用户锁 ID
删除本地用户锁

注册

管理员可以添加和删除注册邀请、向用户发送通知以及将注册表导出到.csv 文件。

添加/删除注册	添加或删除向一个或一组用户发送的注册邀请。
通知用户	向一个或一组用户发送注册邀请。

导出注册邀请表	从“注册”页收集注册信息并将其导出到.csv 文件。

策略

添加/删除策略	添加或删除设备策略或应用程序策略。
编辑策略	更改设备策略或应用程序策略。
上载策略	上载设备策略或应用程序策略。
克隆策略	复制设备策略或应用程序策略。
禁用策略	禁用现有应用程序策略。
导出策略	从“设备策略”页面收集设备策略信息，并将其导出到.csv 文件。
分配策略	将设备策略分配给一个或多个交付组。

应用程序

管理员在 XenMobile 中的配置 **>** 应用程序页面上管理应用程序。

添加/删除应用商店或企业应用程序	添加或删除公共应用商店应用程序或企业应用程序（未启用 MDX）。
编辑应用商店或企业应用程序	更改公共应用商店应用程序或企业应用程序（未启用 MDX）。
添加/删除 MDX、Web 和 SaaS 应用程序	在 XenMobile 中添加或删除启用了 MDX 的应用程序、内部网络中的应用程序（Web 应用程序）或公共网络中的应用程序 (SaaS)。
添加 MDX、Web 和 SaaS 应用程序	更改启用了 MDX 的应用程序、内部网络中的应用程序（Web 应用程序）或从公共网络连接到 XenMobile 的应用程序 (SaaS)。
添加/删除类别	添加或删除应用程序在 XenMobile Store 中可以归属的类别。

将公共/企业应用程序分配给交付组	将公共应用商店应用程序或启用了 MDX 的应用程序分配给交付组以便部署。
将 MDX/WebLink/SaaS 应用程序分配给交付组	将启用了 MDX、不需要单点登录 (WebLink) 或来自公共网络 (SaaS) 的应用程序分配给交付组。
导出应用程序表	从“应用程序”页收集应用程序信息并将其导出到.csv 文件。

媒体

管理从公共应用商店或通过批量购买许可证获取的媒体。

添加/删除应用商店或企业书籍
将公共/企业书籍分配给交付组
编辑应用商店或企业书籍

操作

添加/删除操作	添加或删除通过触发器（事件、设备或用户属性、已安装的应用程序名称）定义的操作及其关联响应。
编辑操作	更改通过触发器（事件、设备或用户属性、已安装的应用程序名称）定义的操作及其关联响应。
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”页收集操作信息并将其导出到.csv 文件。

交付组

管理员在配置 **>** 交付组页面上管理交付组。

添加/删除交付组	创建或删除交付组，即添加指定用户和可选策略、应用程序和操作。
编辑交付组	更改现有交付组，即修改用户和可选策略、应用程序和操作。
部署交付组	使交付组可供使用。
导出交付组	从“交付组”页收集交付组信息并将其导出到.csv 文件。

注册配置文件

管理注册配置文件。

添加/删除注册配置文件
编辑注册配置文件
将注册配置文件分配给交付组

设置

管理员在设置页面上配置各种设置。

RBAC	RBAC 分配、分配角色。重要：此权限向管理员授予完全访问权限，包括分配自己的权限的能力。请仅向打算提供控制 Endpoint Management 系统中的所有对象的功能的用户授予此访问权限。
LDAP	管理一个或多个 LDAP 兼容目录（例如 Active Directory），以导入组、用户帐户和相关属性。
许可证	适用于本地 XenMobile Server。管理您的 Citrix 许可证。
注册	为用户和自助门户启用注册安全模式。
发布管理	查看当前安装的版本。包括：发布管理更新
证书	编辑 APNS 证书、证书 SSL 侦听器

通知模板	创建要在自动执行的操作、注册以及对用户的标准通知消息交付中使用的通知模板。
工作流	管理用于应用程序配置的用户帐户的创建、审批和删除。
凭据提供程序	添加一个或多个授权颁发设备证书的凭据提供程序。凭据提供程序控制证书格式以及续订或吊销证书的条件。
PKI 实体	管理公钥基础结构实体（通用、Microsoft Certificate Services 或任意 CA）。
测试 PKI 连接	使用设置 **> PKI** 实体页面上的“测试连接”按钮可确保服务器可访问。
客户端属性	管理用户设备上的各种属性，例如通行码类型、长度或过期日期。
客户端支持	设置用户联系支持服务的方式（电子邮件、电话或支持票证电子邮件）。
客户端外观方案	为 XenMobile Store 创建自定义的应用商店名称和默认应用商店视图。添加在 XenMobile Store 或 Secure Hub 中显示的自定义徽标。
运营商 SMS 网关	设置运营商 SMS 网关以配置 XenMobile 通过运营商 SMS 网关发送的通知。
通知服务器	设置用于向用户发送电子邮件的 SMTP 网关服务器。
ActiveSync Gateway	通过规则和属性，管理用户对用户和设备的访问权限。
Apple 部署计划	在 XenMobile 中添加一个 Apple 部署计划帐户。
Apple Configurator 设备注册	在 XenMobile 中配置 Apple Configurator 设置。
iOS/批量购买设置	添加 Apple 批量购买帐户。
移动服务提供商	使用移动服务提供商界面查询 BlackBerry 及其他 Exchange ActiveSync 设备并发布操作。
Citrix Gateway	适用于本地 XenMobile Server。添加 Citrix Gateway。选择是否启用身份验证以及是否推送用户证书以进行身份验证。选择凭据提供程序。
网络访问控制	设置确定设备不兼容并因此拒绝访问网络的条件。
Samsung Knox	启用或禁用 XenMobile 查询 Samsung Knox 认证服务器 REST API。
服务器属性	添加或修改服务器属性。需要在所有节点上重新启动 XenMobile。

Syslog	适用于本地 XenMobile Server。使用服务器主机名或 IP 地址将日志文件发送到系统日志 (syslog) 服务器。
XenApp 和 XenDesktop	允许用户通过 Secure Hub 添加 Virtual Apps and Desktops。
Citrix Files	将 XenMobile 与 Enterprise 帐户结合使用时：配置连接到 Content Collaboration 帐户和管理员服务帐户以管理用户帐户的设置。需要使用现有 Citrix Files 域和管理员凭据。在 XenMobile 中使用存储区域连接器时：将 XenMobile 配置为指向在存储区域连接器中定义的网络共享和 SharePoint 位置。
体验改善计划	适用于本地 XenMobile Server。选择是否参与向 Citrix 发送匿名统计数据和使用信息。
Microsoft Azure	适用于本地 XenMobile Server。将 XenMobile 与 Microsoft Azure 相集成。
Android Enterprise	配置 Android Enterprise 服务器设置
身份提供程序 (IdP)	配置身份提供程序。
XenMobile Tools	访问 “XenMobile Tools” 页面。
SNMP 配置	为 XenMobile Server 节点启用 SNMP。编辑或添加监视用户、设置显示陷阱通知的 SNMP 管理器以及配置陷阱时间间隔和阈值。

支持

管理员可以执行各种支持任务。

Citrix Gateway 连接检查	通过 IP 地址执行 Citrix Gateway 的各种连接检查。需要用户名和密码。
XenMobile 连接检查	为选定的 XenMobile 功能（如数据库、DNS 或 Google Plan）执行连接检查。
创建支持包	适用于本地 XenMobile Server。创建一个文件，以发送给 Citrix 支持用于进行故障排除。该文件中包含系统信息、日志、数据库信息、内核信息、跟踪文件以及 XenMobile 或 Citrix Gateway 的最新配置信息。

Citrix 产品文档	访问公共 Citrix XenMobile 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	访问并分析用于调试、管理员审核和用户审核的日志文件详细信息。
群集信息	适用于本地 XenMobile Server。访问群集环境中关于每个节点的信息。
垃圾回收	适用于本地 XenMobile Server。访问不再使用的内存对象的信息。
Java 内存属性	适用于本地 XenMobile Server。访问 Java 内存使用情况、内存详细信息和内存池详细信息的快照。
宏	在配置文件、策略、通知或注册模板的文本字段内填充用户或设备属性数据。配置一个策略并将其部署到较大的用户群，并为每个目标用户显示特定于用户的值。
PKI 配置	导入和导出 PKI 配置信息。
APNS 签名实用程序	提交 Apple 推送网络签名 (Apple Push Network signing, APNs) 证书请求，或上载适用于 iOS 的 Secure Mail APNs 证书。
Citrix Insight Services	将日志上载到 Citrix Insight Services (CIS)，以帮助解决各种问题。
发送到适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的设备状态	根据设备 ActiveSync ID 向 XenMobile 查询发送到适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的设备状态。
匿名和取消匿名	适用于本地 XenMobile Server。在 XenMobile 中创建支持包时，默认情况下会将敏感用户、服务器和网络数据设为匿名。可以在高级下的支持 **>** 匿名和取消匿名中更改此行为。
日志设置	自定义日志级别或添加自定义调试器。

限制组访问

管理员用户可以应用所有用户组的权限。

设备预配角色

> 重要：
>
> “设备预配角色”仅适用于 Windows CE 设备。

具有预定义的设备预配角色的用户对控制台功能具有有限访问权限。默认情况下，用户的权限设置为所有用户组，他们不能更改此设置。

控制台功能

设备预配用户具有 XenMobile 控制台的以下有限访问权限。默认情况下，以下各功能均处于启用状态。

设备

编辑设备	更改设备上的设置。
添加/删除设备	从 XenMobile 添加或删除设备。

设置

设备预配用户可以访问设置页面，但无权配置功能。

支持角色

具有支持角色的用户可以访问远程支持。默认情况下，其权限适用于所有用户，并且他们无法编辑此设置。

用户角色

具有用户角色的用户具有 XenMobile 的以下有限访问权限。

授权访问

自助服务门户	用户在 XenMobile 中仅具有自助服务门户的访问权限。

控制台功能

用户具有 XenMobile 控制台的以下有限访问权限。

设备

完全擦除设备	擦除设备上的所有数据和应用程序，包括内存卡（如果设备具有内存卡）。
选择性擦除设备	擦除设备上的所有公司数据和应用程序，保留个人数据和应用程序。
查看位置	查看设备的位置以及在设备上设置地理区域限制。包括：定位设备、查看设备的位置、跟踪设备、跟踪设备位置随时间的变化。
锁定设备	远程锁定设备，使其无法使用。
解锁设备	远程解锁设备，使其可以使用。
锁定容器	远程锁定设备上的企业容器。
解锁容器	远程解锁设备上的企业容器。
重置容器密码	重置企业容器密码。
启用 ASM DEP/绕过激活锁	启用激活锁时，在受监督的 iOS 设备上存储绕过码。如果需要擦除该设备，请使用此代码自动清除激活锁。
使设备响铃	远程使 Windows 设备以最高音量响铃 5 分钟。
重新启动设备	重新启动 Windows 设备。
查看软件清单	查看设备上安装的软件。

注册

添加/删除注册	添加或删除向一个或一组用户发送的注册邀请。
通知用户	向一个或一组用户发送注册邀请。

限制组访问

对于所有四种默认角色，此权限在默认情况下设置，并且可应用于所有用户组。您无法编辑此角色。

使用 **RBAC** 配置角色

通过 XenMobile 中基于角色的访问控制 (RBAC) 功能，可以向用户和组分配预定义的角色（或称权限集）。这些权限控制用户对系统功能的访问级别。

XenMobile 实现四种默认用户角色，用于在逻辑上区分系统功能的访问权限：

- 管理员：授予完整系统访问权限。
- 设备预配：授予访问针对 Windows CE 设备的基本设备管理的权限。
- 支持：授予访问远程支持的权限。
- 用户：供可以注册设备和访问自助服务门户的用户使用。

还可以将默认角色用作自定义的用于创建用户角色的模板。可以分配角色权限，以访问默认角色定义的功能以外的特定系统功能。

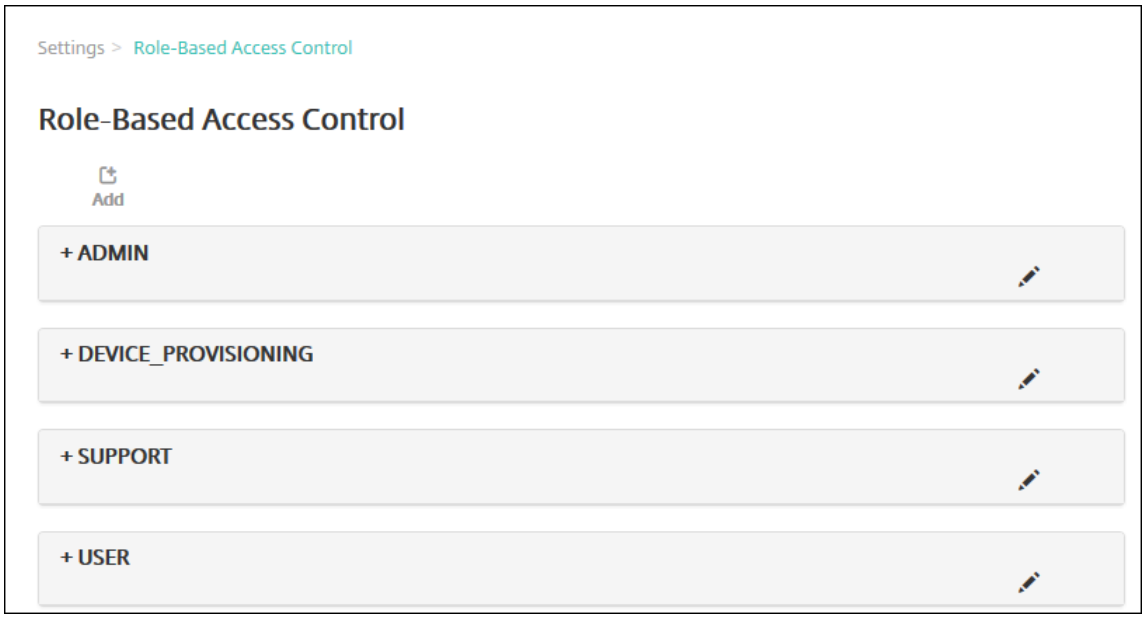
角色可以分配给本地用户（在用户级别）或 Active Directory 组（此组中的所有用户具有相同的权限）。如果用户属于多个 Active Directory 组，则所有权限合并起来，以定义该用户的权限。例如，假设 ADGroupA 用户可以定位经理的设备，而 ADGroupB 用户可以擦除员工的设备。在这种情况下，属于两个组的用户可以找到并擦除经理和员工的设备。

> 注意：
>
> 只能为本地用户分配一个角色。

可以使用 XenMobile 中的 RBAC 功能执行以下操作：

- 创建角色。
- 将组添加到角色。
- 向本地用户分配角色。

1. 在 XenMobile 控制台中，转到设置 **>** 基于角色的访问控制。此时将显示基于角色的访问控制页面，其中显示了四种默认用户角色以及您之前添加的所有角色。



如果单击某个角色旁边的加号 (+)，角色将展开以显示此角色的所有权限，如下图所示。

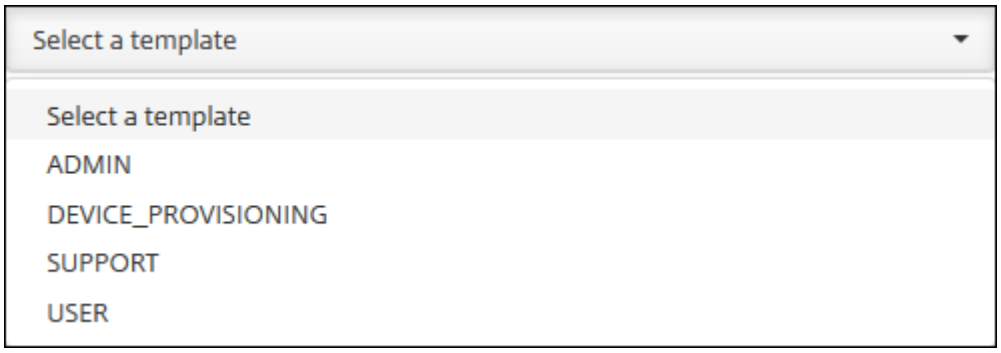
2. 单击添加添加一个新用户角色。要编辑该角色，请单击现有角色右侧的笔图标。要删除角色，请单击角色右侧的垃圾桶图标。无法删除默认用户角色。

   - 单击添加或铅笔图标时，将显示添加角色或编辑角色页面。
   - 单击垃圾桶图标时，将显示一个确认对话框。单击删除可删除选定的角色。

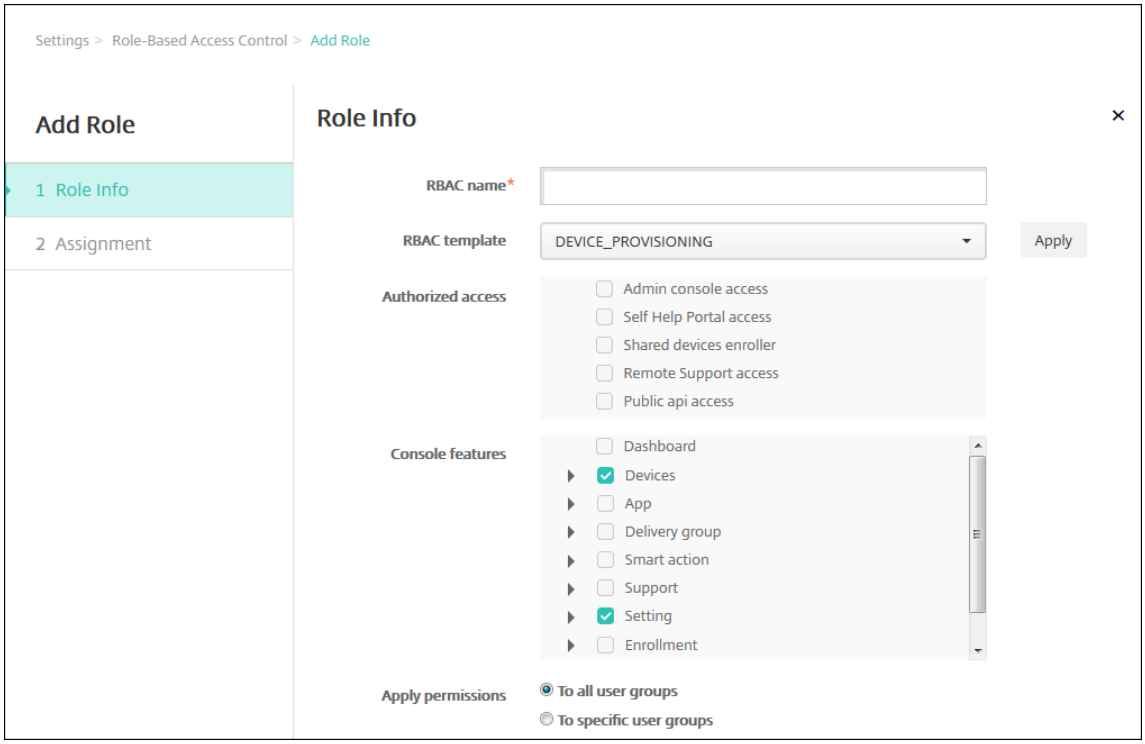
3. 输入以下信息以创建或编辑用户角色：

   - **RBAC** 名称：输入新用户角色的描述性名称。无法更改现有角色的名称。
   - **RBAC** 模板：（可选）单击某个模板以将其作为新角色的起点。如果正在编辑现有角色，则无法选择模板。

   RBAC 模板是默认用户角色。它们定义与此角色关联的用户对系统功能的访问权限。选择某个 RBAC 模板后，可以在授权访问和控制台功能字段看到与该角色关联的所有权限。可以选择使用模板。可以直接在授权访问和控制台功能字段中选择要分配给角色的选项。

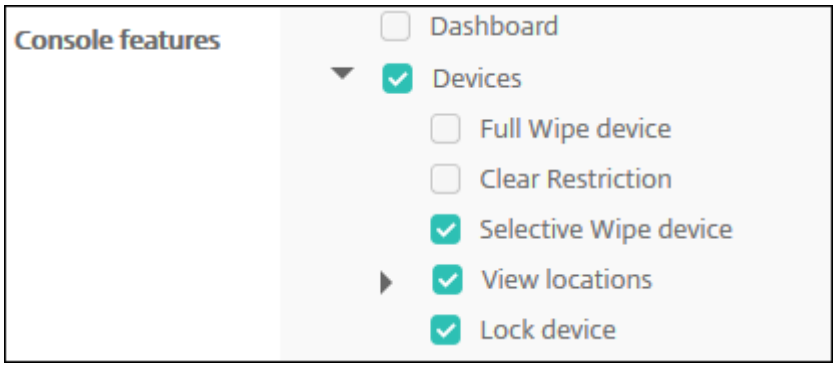


4. 单击选定的 **RBAC** 模板字段旁边的应用以使用预定义的访问权限和功能权限填充授权访问和控制台功能。



5. 选中或取消选中授权访问和控制台功能复选框可自定义角色。

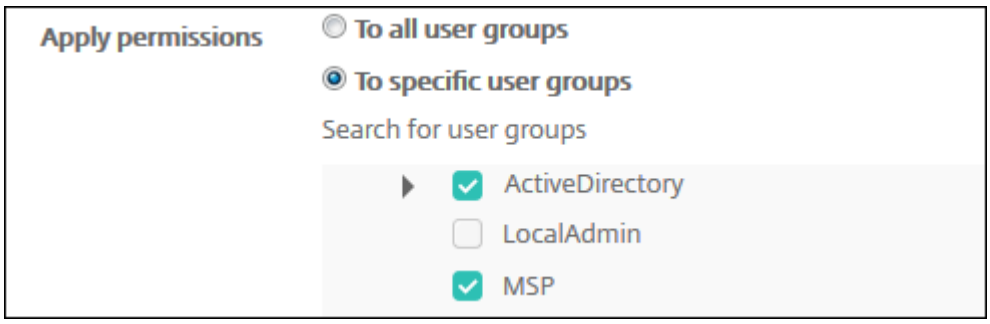
   如果单击某项控制台功能旁边的三角形，将显示特定于此功能的权限，您可以选中或取消选中相应的权限。单击顶层复选框禁止访问该控制台区域的权限。选择顶层下方的单个选项可启用这些选项。例如，在下图中，不会为分配给角色的用户显示完全擦除设备和清除限制选项。确实会出现选中的选项。



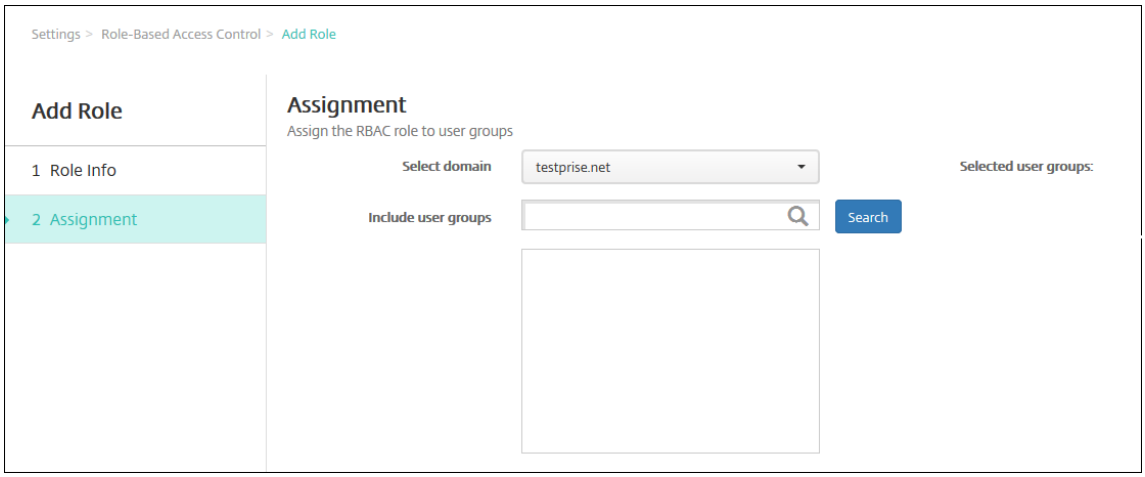
6. 应用程序权限：选择一个或多个用户组，以限制管理员可以管理的组。如果单击至特定用户组，将显示组列表，您可以从中选择一个或多个组。

   例如，如果 RBAC 管理员具有对 ActiveDirectory 和 MSP 用户组的权限：

   - 管理员只能访问 ActiveDirectory 组、MSP 组或这两个组中的用户的信息。
   - 管理员无法查看任何其他本地或 AD 用户。管理员可以查看属于这些组的子组成员的用户。
   - 管理员可以发送邀请至：
     - 权限组及其子组
     - 属于权限组及其子组的成员的用户

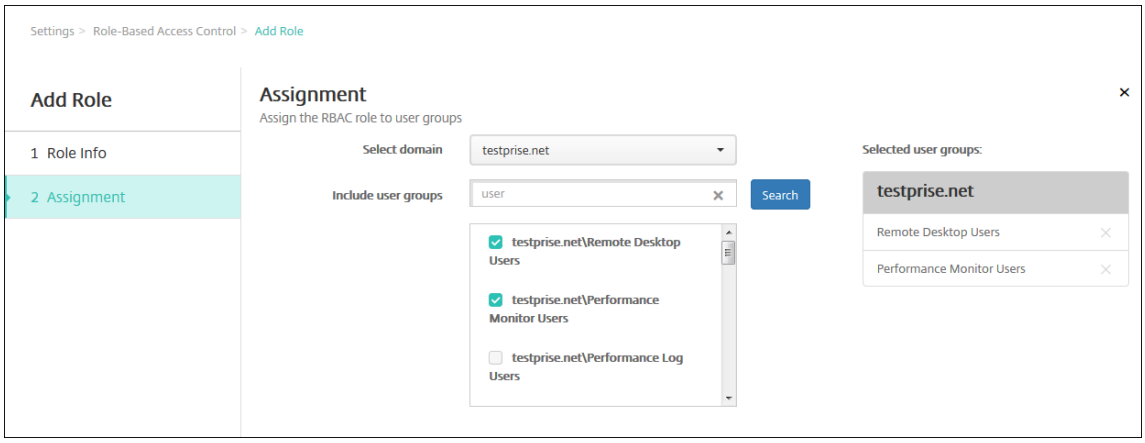


7. 单击 **Next**（下一步）。此时将显示分配页面。



8. 输入下列信息，以将角色分配给用户组。

   - 选择域：在列表中，单击某个域。
   - 包括用户组：单击“搜索”以查看所有可用组的列表，或键入完整或部分组名称以将列表限制为仅显示具有该名称的组。
   - 在显示的列表中，选择要向其分配角色的用户组。选择某个用户组后，此组将显示在选定用户组列表中。



> 注意：
>
> 要从选定用户组列表中删除用户组，请单击用户组名称旁边的 X。

9. 单击保存。

通知

January 5, 2022

可以将 XenMobile 中的通知用于以下目的：

- 与选择的用户组通信以使用多个系统相关功能。也可以将这些通知发送给特定用户。例如，使用 iOS 设备的所有用户、设备不合规的用户、使用员工自带设备的用户等。
- 注册用户及其设备
- 满足某些条件时自动通知用户（使用自动化操作）。例如：
  - 由于合规性问题阻止用户设备访问企业域时。
  - 设备已被越狱或获得 Root 权限时。

有关自动化操作的详细信息，请参阅自动化操作。

要使用 XenMobile 发送通知，必须配置网关和通知服务器。可以在 XenMobile 中设置通知服务器，以配置简单邮件传输协议 (SMTP) 和短信服务 (SMS) 网关服务器，以便向用户发送电子邮件和文本 (SMS) 通知。可以使用通知经两种不同的通道发送消息：SMTP 或 SMS。

- SMTP 是面向连接的文本协议，邮件发送方通常通过传输控制协议 (TCP) 发布命令字符串并提供必需的数据，从而与邮件接收方通信。SMTP 会话包括来自 SMTP 客户端（邮件发送人员）的命令和来自 SMTP 服务器的相应响应。
- SMS 是手机、Web 或移动通信系统的文本消息服务组件。SMS 使用标准化通信协议，使固定线路或移动电话设备可以交换短文本消息。

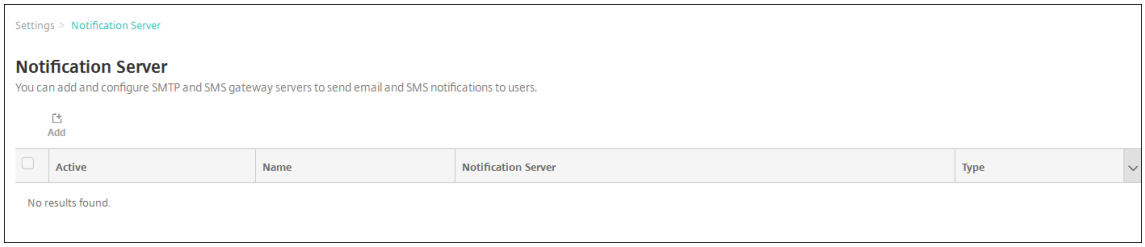
还可以在 XenMobile 中设置运营商 SMS 网关，以配置通过运营商的 SMS 网关发送的通知。运营商使用 SMS 网关发送和接受来往于电信网络的 SMS 传输。这些基于文本的消息使用标准化通信协议，允许固定线路或移动电话设备交换短文本消息。

必备条件

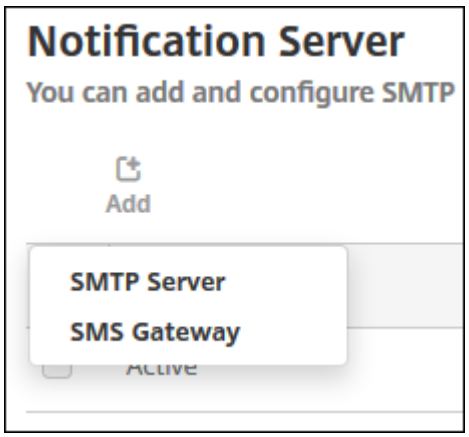
- 配置 SMS 网关之前，请咨询系统管理员以确定服务器信息。了解 SMS 服务器是否托管在内部企业服务器上或者服务器是否属于托管电子邮件服务至关重要。在这种情况下，您需要服务提供商 Web 站点上的信息
- 可配置 SMTP 通知服务器以向用户发送消息。如果此服务器托管在内部服务器上，请联系系统管理员以获取配置信息。如果此服务器是托管的邮件服务，请在服务提供商的 Web 站点上查找适当的配置信息。
- 可以同时使用一个活动的 SMTP 服务器和一个活动的 SMS 服务器。这两个通信渠道都允许一种活动配置。
- 从位于网络的 DMZ 中的 XenMobile 打开端口 25 以指回内部网络上的 SMTP 服务器。这样，XenMobile 能够成功发送通知。

配置 **SMTP** 服务器和 **SMS** 网关

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在通知下方，单击通知服务器。此时将显示通知服务器页面。

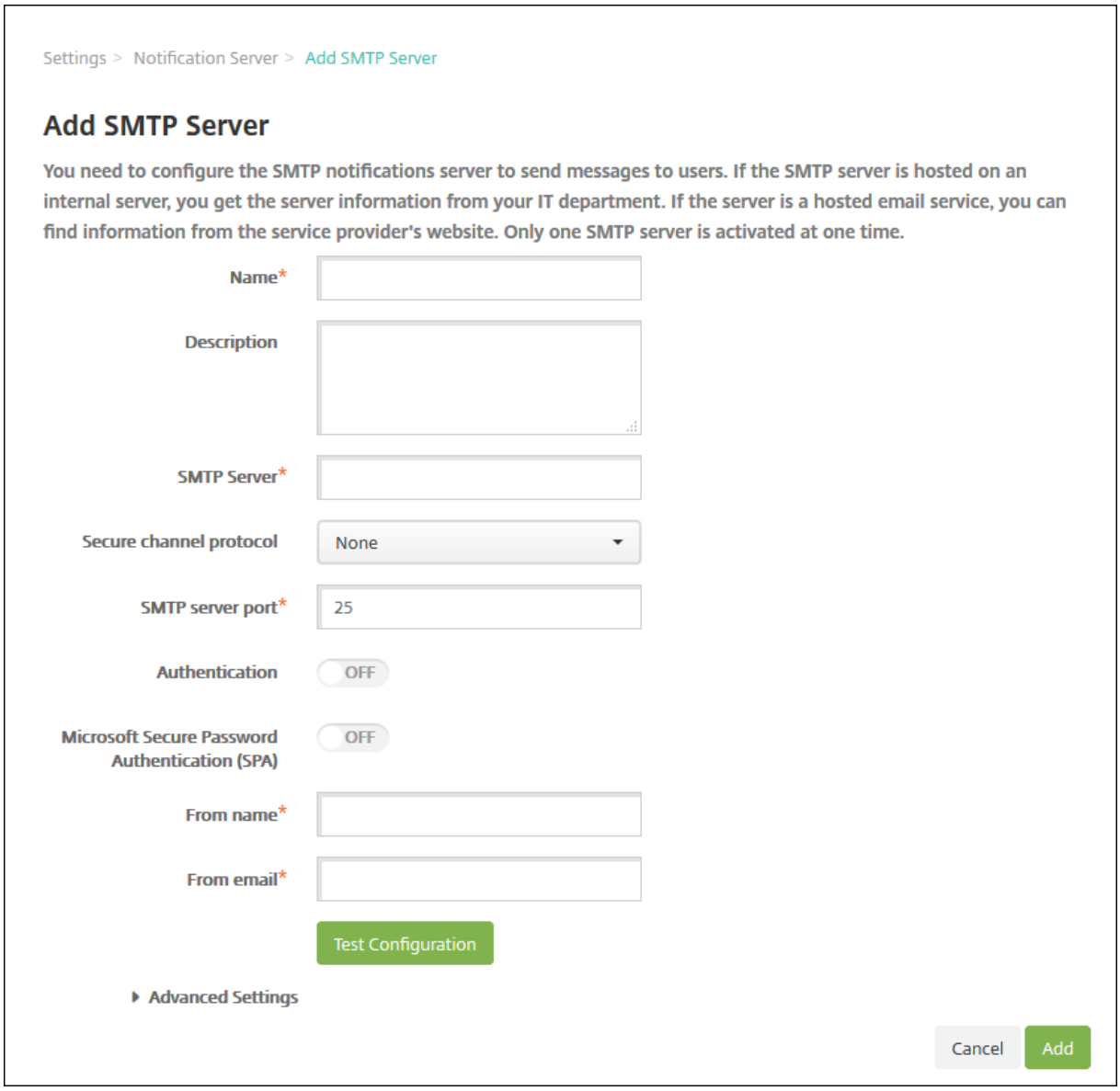


3. 单击添加。显示一个包含用于配置 SMTP 服务器或 SMS 网关的选项的菜单。



   - 要添加 SMTP 服务器，请单击 **SMTP** 服务器，然后参阅添加 SMTP 服务器了解配置此设置的步骤。
   - 要添加 SMS 网关，请单击 **SMS** 网关，然后参阅添加 SMS 网关了解配置此设置的步骤。

添加 **SMTP** 服务器



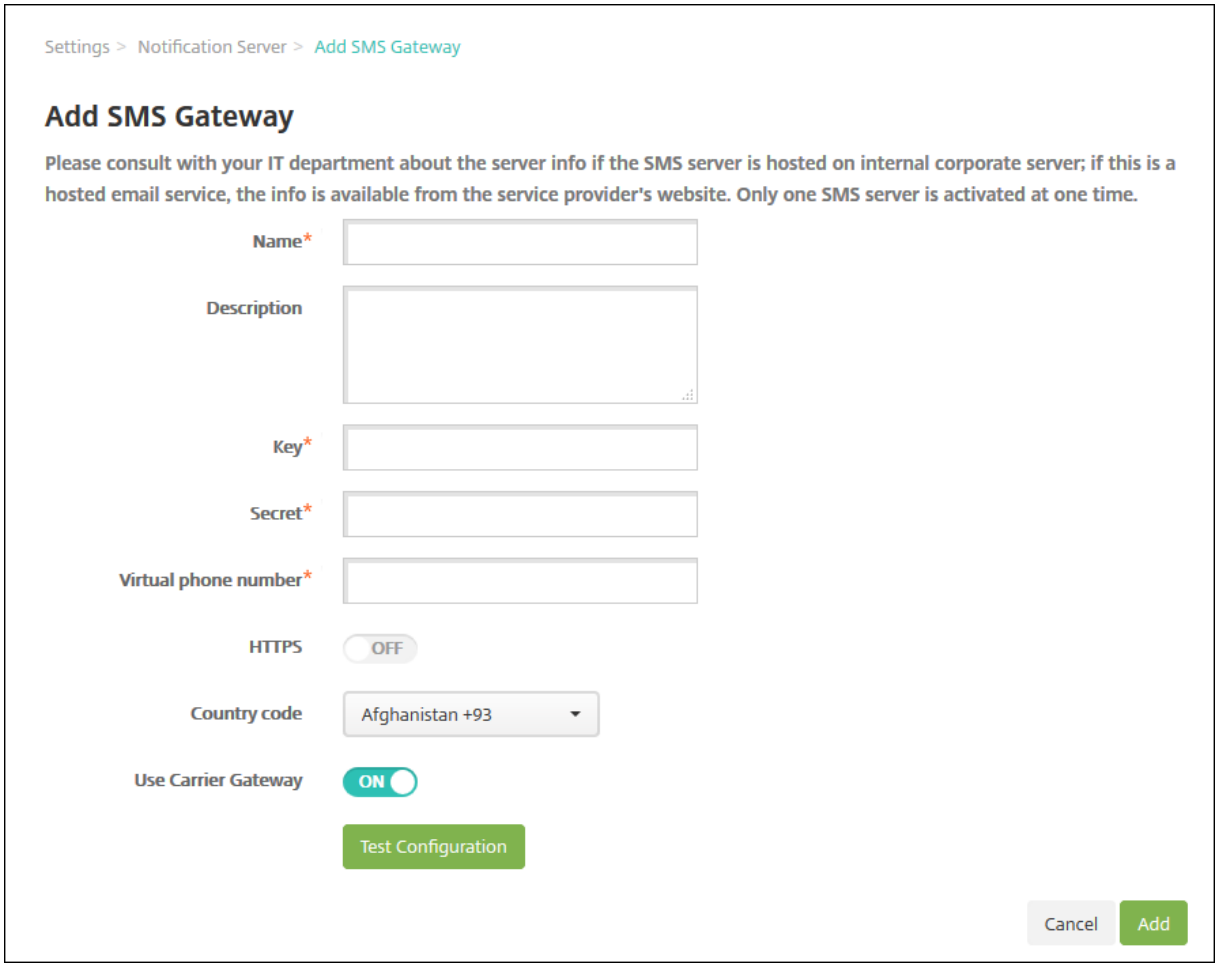
1. 配置以下设置：

   - 名称：键入与此 SMTP 服务器帐户关联的名称。
   - 说明：（可选）输入服务器的说明。
   - **SMTP** 服务器：键入服务器的主机名。主机名可以是完全限定的域名 (FQDN) 或 IP 地址。
   - 安全通道协议：在列表中，单击 **SSL**、**TLS** 或无选择服务器使用的安全通道协议（如果服务器配置为使用安全身份验证）。默认设置为无。
   - **SMTP** 服务器端口：键入 SMTP 服务器使用的端口。默认情况下，此端口设置为 25；如果 SMTP 连接使用 SSL 安全通道协议，则此端口设置为 465。
   - 身份验证：选择开或关。默认值为关。
   - 如果启用身份验证，请配置以下设置：

  - 用户名：键入进行身份验证时使用的用户名。
  - 密码：键入身份验证用户的密码。
- **Microsoft** 安全密码身份验证 **(SPA)**：如果 SMTP 服务器使用的是 SPA，请单击开。默认值为关。
- 发件人姓名：键入客户端接收来自此服务器的通知电子邮件时，显示在发件人框中的姓名。例如，公司 IT。
- 发件人电子邮件：键入电子邮件收件人回复 SMTP 服务器发送的通知时使用的电子邮件地址。

2. 单击测试配置以发送测试电子邮件通知。
3. 展开高级设置，然后配置以下设置：
   - **SMTP** 重试次数：键入 SMTP 服务器发送邮件失败的重试次数。默认值为 5。
   - **SMTP** 超时：键入发送 SMTP 请求时等待的持续时间（秒）。如果频繁出现因超时导致消息发送失败的情况，请增加此值。降低此值时请格外小心；此操作可增加超时次数和未送达的消息。默认值为 30 秒。
   - **SMTP** 收件人数量上限：键入 SMTP 服务器发送的每封电子邮件的收件人数量上限。默认值为 100。
4. 单击添加。

添加 **SMS** 网关



> 注意：
>
> XenMobile 仅支持 Nexmo SMS 消息传递。如果还没有使用 Nexmo 消息传递的帐户，请访问其 Web 站点以创建帐户。

1. 配置以下设置：
   - 名称：键入 SMS 网关配置的名称。此字段为必填字段。
   - 说明：（可选）键入配置的说明。
   - 密钥：键入系统管理员在激活帐户时提供的数字标识符。此字段为必填字段。
   - 密码：键入系统管理员提供的密码 (secret)，当密码 (password) 丢失或被盗时用于访问您的帐户。此字段为必填字段。
   - 虚拟电话号码：向北美电话号码（前缀为 +1）发送时使用此字段。在此字段中，必须键入 Nexmo 虚拟电话号码，且只能使用数字。可以在 Nexmo Web 站点上购买虚拟电话号码。
   - **HTTPS**：选择是否使用 HTTPS 将 SMS 请求传输到 Nexmo。默认值为关。

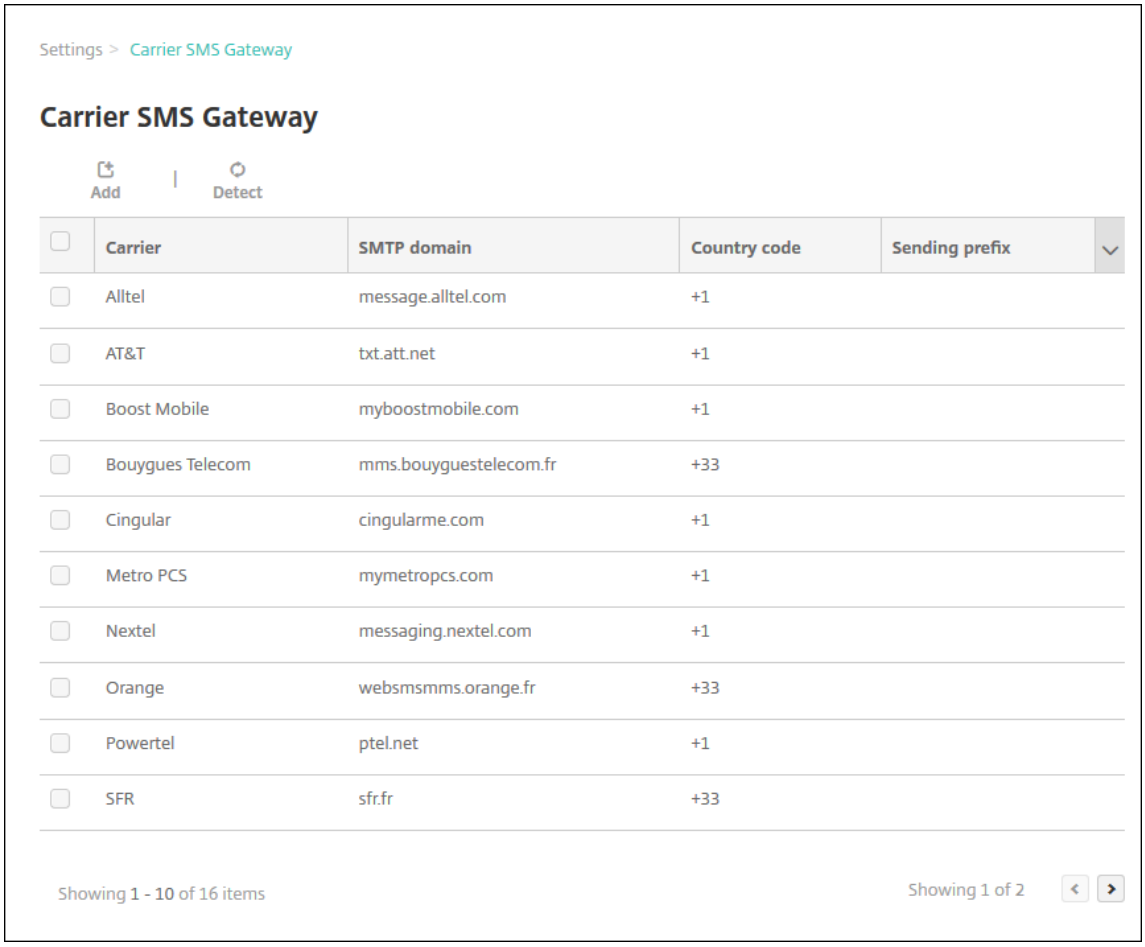
     > 重要：
     >
     > 保留 HTTPS 设置为开，除非 Citrix 技术支持指示您将其改为关。

   - 国家/地区代码：在此列表中，单击贵组织中收件人的默认 SMS 国家/地区代码前缀。此字段始终以 + 符号开头。默认值为阿富汗 **+93**。
2. 单击测试配置以使用当前配置发送测试消息。系统将立即检测并显示连接错误，如身份验证或虚拟电话号码错误。接收消息的时间范围与移动电话之间发送消息的时间范围相同。
3. 单击添加。

添加运营商 **SMS** 网关

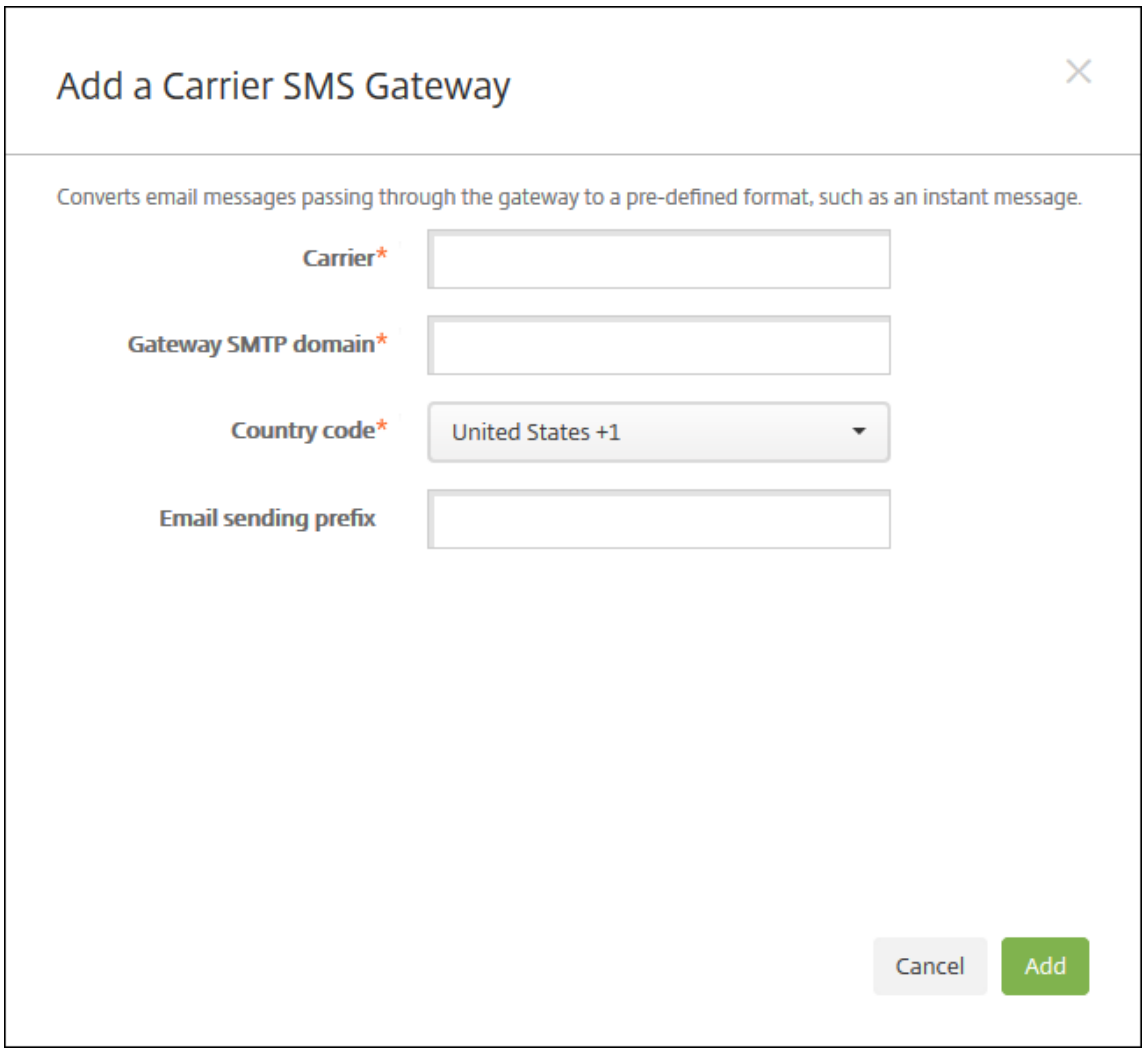
您可以在 XenMobile 中设置运营商 SMS 网关，以配置通过运营商的 SMS 网关发送的通知。运营商使用短信服务 (SMS) 网关发送或接受来往于电信网络的 SMS 传输。这些基于文本的消息使用标准化通信协议，允许固定线路或移动电话设备交换短文本消息。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在通知下方，单击运营商 **SMS** 网关。此时将显示运营商 **SMS** 网关页面。



3. 执行以下操作之一：

   - 单击检测以自动发现网关。此时将显示一个对话框，指出没有检测到新的运营商或列出在已注册设备中间检测到的新运营商。
   - 单击添加。此时将显示添加运营商 **SMS** 网关对话框。



> 注意：
>
> XenMobile 仅支持 Nexmo SMS 消息传递。如果还没有使用 Nexmo 消息传递的帐户，请访问其 Web 站点以创建帐户。

4. 配置以下设置：
   - 运营商：键入运营商的名称。
   - 网关 **SMTP** 域：键入与 SMTP 网关关联的域。
   - 国家/地区代码：在列表中，单击运营商的国家/地区代码。
   - 电子邮件发送前缀：（可选）指定电子邮件发送前缀。
5. 单击添加以添加新运营商，或单击取消不添加新运营商。

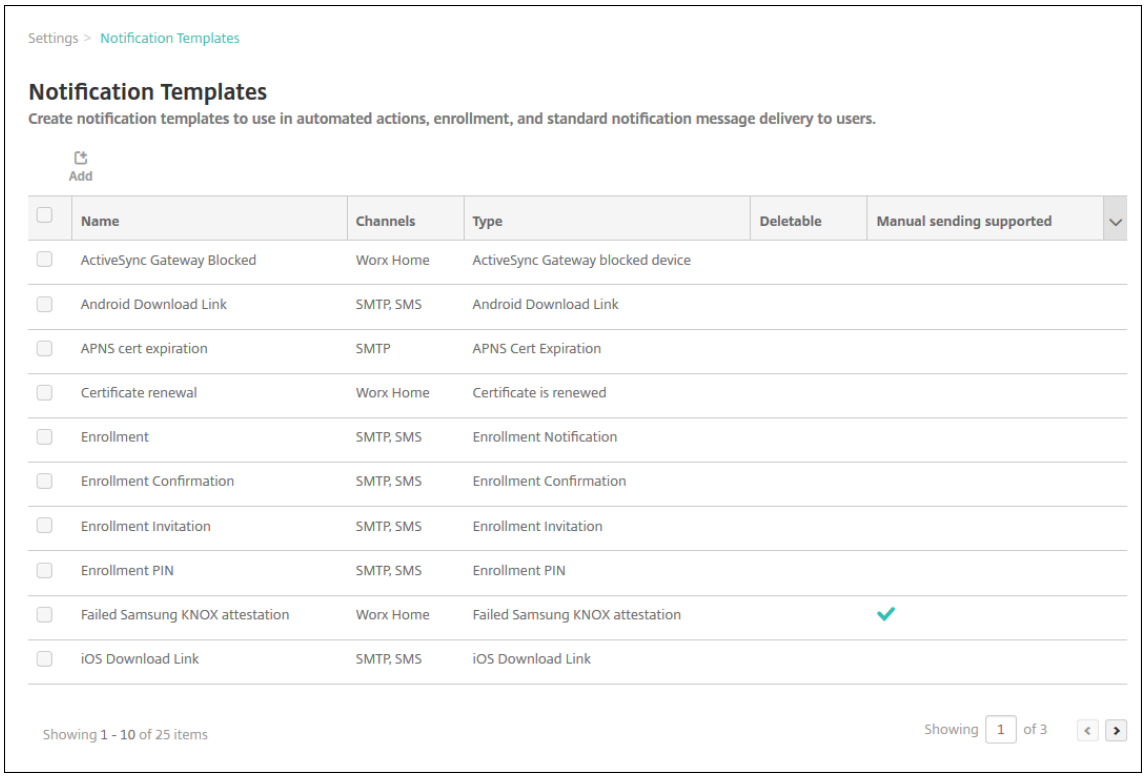
创建和更新通知模板

可以在 XenMobile 中创建或更新用于自动化操作、注册和发送给用户的标准通知消息的通知模板。配置通知模板以通过三种不同的通道发送消息：Secure Hub、SMTP 或 SMS。

XenMobile 包含很多反应不同事件类型的预定义通知模板，XenMobile 会自动针对这些事件类型向系统中的每个设备发出响应。

> 注意：
>
> 如果计划使用 SMTP 或 SMS 通道向用户发送通知，必须设置通道后才能将其激活。如果尚未设置通道，当添加通知模板时，XenMobile 会提示您设置通道。

1. 在 XenMobile 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。如果尚未设置任何 SMS 网关或 SMTP 服务器，会显示一条关于使用 SMS 和 SMTP 通知的消息。可以选择立即或稍后设置 SMTP 服务器或 SMS 网关。

   如果选择立即设置 SMS 或 SMTP 服务器设置，将重定向到设置页面上的通知服务器页面。设置了要使用的通道后，可以返回通知模板页面，继续添加或修改通知模板。

   > 重要：
   >
   > 如果选择稍后设置 SMS 或 SMTP 服务器设置，将无法在添加或编辑通知模板时激活这些通道，这意味着这些通道将不能用于发送用户通知。

2. 配置以下设置：

   - 名称：键入模板的描述性名称。

- 说明：键入模板的说明。
- 类型：在列表中，单击通知类型。仅显示选定类型支持的通道。仅允许一个 APNS 证书过期模板，此为预定义模板。这表示您无法添加此类型的新模板。

> 注意：
>
> 对于某些模板类型，类型的下面会显示短语支持手动发送。这表示此模板会显示在控制板和设备页面上的通知列表中，允许您手动向用户发送模板。在“主题”或“消息”字段中使用以下宏的任何模板在任何通道上均不可以使用手动发送。

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}

  > 注意：
  >
  > XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

- ${outofcompliance.reason(smg_block)}

3. 在通道下方，配置用于此通知的每个通道的信息。可以选择任何通道或所有通道。您选择的通道取决于您希望发送通知的方式。

   - 如果选择 **Secure Hub**，则仅 iOS 和 Android 设备接收通知，通知将显示在设备的通知托盘中。
   - 如果选择 **SMTP**，大多数用户应该可以接收邮件，因为他们已使用其电子邮件地址注册。
   - 如果选择 **SMS**，则仅使用的设备带有 SIM 卡的用户接收通知。

   Secure Hub：

   - 激活：单击以启用通知通道。
   - 消息：键入要发送给用户的消息。如果使用的是 Secure Hub，此字段为必填字段。有关在消息中使用宏的信息，请参阅宏。
   - 声音文件：在列表中，单击用户收到通知时听到的通知声音。

   SMTP：

   - 激活：单击以启用通知通道。

     只能在设置 SMTP 服务器后，才能激活 SMTP 通知。

   - 发件人：键入通知的可选发件人，可以是姓名或/和电子邮件地址。
   - 收件人：此字段包含除临时通知以外的所有通知的预置宏，以确保通知发送到正确的 SMTP 收件人地址。Citrix 建议您不要修改模板中的宏。除了用户，您还可以通过添加以分号 (;) 分隔的收件人地址，添加其他收件人（如企业管理员）。要发送临时通知，可以在此页面上输入特定收件人，也可以从管理 **>** 设备页面选择设备并从此处发送通知。有关详细信息，请参阅设备。
   - 主题：键入通知的描述性主题。此字段为必填字段。
   - 消息：键入要发送给用户的消息。有关在消息中使用宏的信息，请参阅宏。

   SMS：

- 激活：单击以启用通知通道。

  只能在设置 SMTP 服务器后，才能激活 SMTP 通知。

- 收件人：此字段包含除临时通知以外的所有通知的预置宏，以确保通知发送到正确的 SMS 收件人地址。Citrix 建议您不要修改模板中的宏。要发送临时通知，可以输入特定收件人，也可以从管理 **>** 设备页面选择设备。

- 消息：键入要发送给用户的消息。此字段为必填字段。有关在消息中使用宏的信息，请参阅宏。

4. 单击添加。正确配置所有通道后，通道将按照以下顺序显示在通知模板页面：SMTP、SMS 和 Secure Hub。未正确配置的通道将在经过正确配置后显示。

编辑通知模板

1. 选择通知模板。此时将显示该模板特定的编辑页面，您可以在此页面上更改类型字段以外的所有内容，以及激活或取消激活通道。
2. 单击保存。

删除通知模板

您只能删除自己添加的通知模板。不能删除预定义的通知模板。

1. 选择现有通知模板。
2. 单击删除。此时将显示确认对话框。
3. 单击删除以删除通知模板，或单击取消以取消删除通知模板。

设备

January 5, 2022

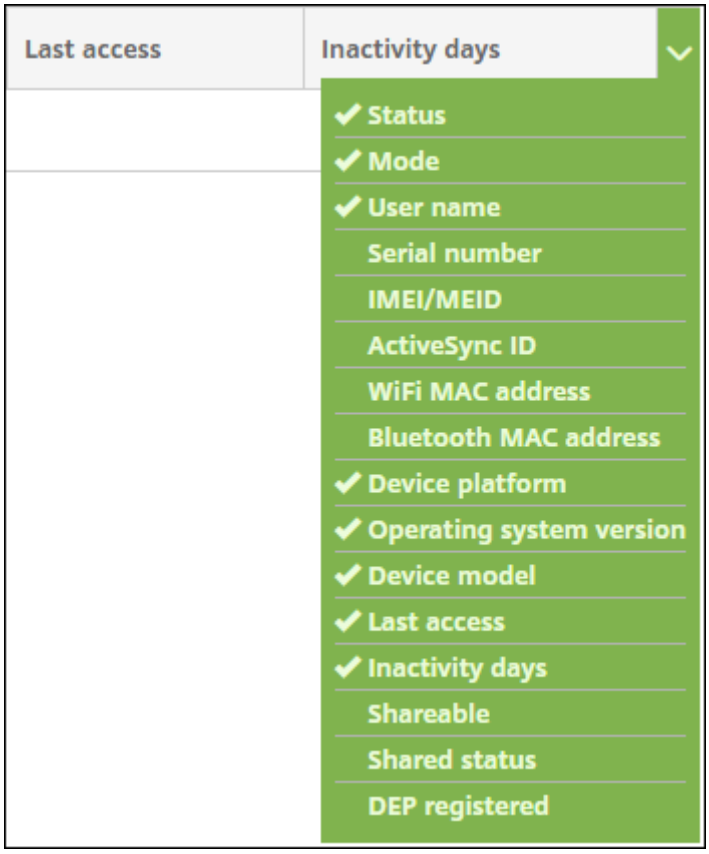
Citrix XenMobile 可以在单个管理控制台中预配和管理各种设备类型、保护其安全以及将其列入清单。

XenMobile Server 数据库存储移动设备的列表。唯一的序列号或国际移动设备标识 (IMEI)/移动设备标识符 (MEID) 标识唯一地定义每个移动设备。要将设备填充到 XenMobile 控制台中，可以手动添加设备或从文件导入设备列表。有关设备预配文件格式的详细信息，请参阅本文中稍后介绍的设备预配文件格式。

XenMobile 控制台中的设备页面列出每个设备以及以下信息：

- 状态：图标指示设备是否已越狱、是否托管，Active Sync Gateway 是否可用以及部署状态
- 模式：设备模式是 MDM、MAM 还是两者
- 与设备有关的其他信息，例如，用户名、设备平台、操作系统版本、设备型号、上次访问时间以及不活动天数。这些标题是显示的默认标题。

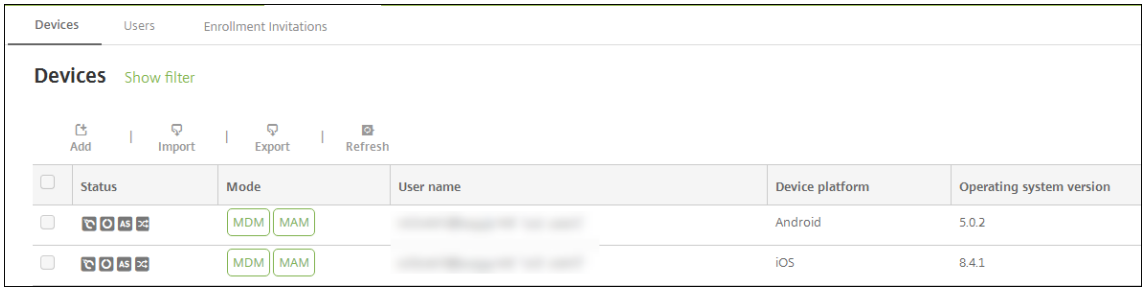
要自定义设备表，请单击最后一个标题上的向下箭头。然后选择要在表格中看到的其他标题，或者清除要删除的所有标题。



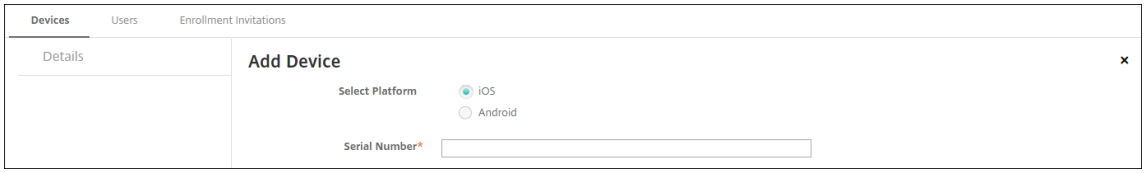
可以手动添加设备、从设备预配文件中导入设备、编辑设备详细信息、执行安全操作以及向设备发送通知。还可以将所有设备表数据导出到.csv 文件，以创建自定义报告。服务器将导出所有设备属性。如果应用过滤器，XenMobile 会在创建.csv 文件时使用这些过滤器。

手动添加设备

1. 在 XenMobile 控制台中，单击管理 **>** 设备。此时将显示设备页面。



2. 单击添加。此时将显示添加设备页面。



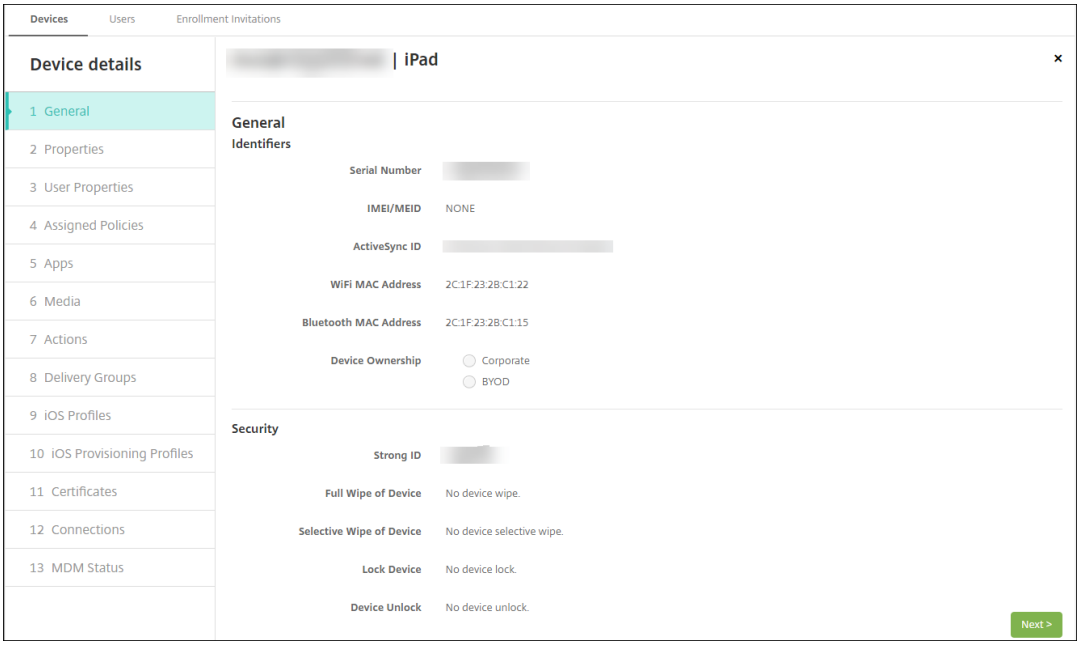
3. 配置以下设置：

   - 选择平台：单击 **iOS** 或 **Android**。
   - 序列号：键入设备序列号。
   - **IMEI/MEID**：（可选，仅限 Android 设备）键入设备的 IMEI/MEID 信息。

4. 单击添加。设备将添加到所显示设备表的列表底部。选择已添加的设备，然后在显示的菜单中，单击编辑以查看并确认设备详细信息。

   > 注意：
   >
   > 选中某个设备旁边的复选框时，选项菜单将在设备列表上方显示。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。

   - 在企业 (XME) 或 MDM 模式下配置的 XenMobile Server
   - 已配置 LDAP
   - 如果使用本地组和本地用户：
     - 一个或多个本地组。
     - 分配给本地组的本地用户。
     - 交付组与本地组相关联。
   - 如果使用 Active Directory：
     - 交付组与 Active Directory 组相关联。



5. 常规页面列出设备标识符，例如，序列号、ActiveSync ID 以及平台类型的其他信息。对于设备所有权，请选择公司或 **BYOD**。

   常规页面还列出了设备安全属性，例如，强 ID、锁定设备、激活锁绕过和平台类型的其他信息。完全擦除设备字段包括用户的 PIN 代码。擦除设备后，用户必须输入该代码。如果用户忘记了该代码，您可以在此处查找。

6. 属性页面列出了 XenMobile 要预配的设备属性。此列表显示了用于添加设备的预配文件中包含的任何设备属性。要添加属性，请单击添加，然后从列表中选择一种属性。有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

   添加属性时，它最初将显示在添加了该属性的类别下方。单击下一步，然后返回属性页面后，属性将显示在相应列表中。

   要删除某个属性，请将鼠标悬停在列表上方，然后单击右侧的 **X**。XenMobile 将立即删除该项目。

7. 其余的设备详细信息部分包含设备的摘要信息。

   - 用户属性：显示用户的 RBAC 角色、组成员身份、批量购买帐户和属性。可以从此页面停用批量购买帐户。
   - 已分配的策略：显示已分配策略的数量，包括已部署、挂起和失败的策略数量。提供每个策略的策略名称、类型和上次部署信息。
   - 应用程序：显示上一个清单的已安装、挂起和失败的应用程序部署数量。提供应用程序名称、标识符、类型和其他信息。
   - 媒体：显示上一个清单的已部署、挂起和失败的媒体部署数量。
   - 操作：显示已部署、挂起和失败的操作数量。提供上一个部署的操作名称和时间。
   - 交付组：显示成功、挂起和失败的交付组数量。对于每个部署，提供交付组的名称和部署时间。选择一个交付组以查看更多详细信息，包括状态、操作以及通道或用户。
   - **iOS** 配置文件：显示上一个 iOS 配置文件清单，包括名称、类型、组织和说明。
   - **iOS** 预配配置文件：显示企业分发预配配置文件信息，例如 UUID、过期日期以及是否托管。
   - 证书：显示有效证书、已过期证书或已吊销证书信息，例如，类型、提供程序、颁发者、序列号、过期之前

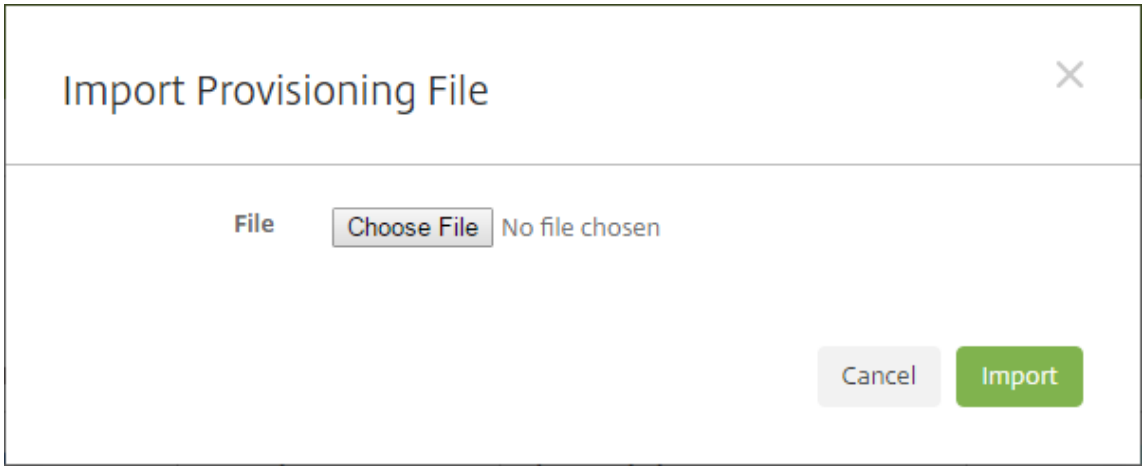
的剩余天数。

- 连接：显示第一个连接状态和最后一个连接状态。提供每个连接的用户名、倒数第二次身份验证和上次身份验证时间。
- **MDM** 状态：显示 MDM 状态、上次推送时间以及上次设备答复时间等信息。

从预配文件导入设备

您可以导入移动运营商或设备制造商支持的文件，或创建自己的设备预配文件。有关详细信息，请参阅本文中后面的设备预配文件格式。

1. 转至管理 **>** 设备，然后单击导入。此时将显示导入预配文件对话框。

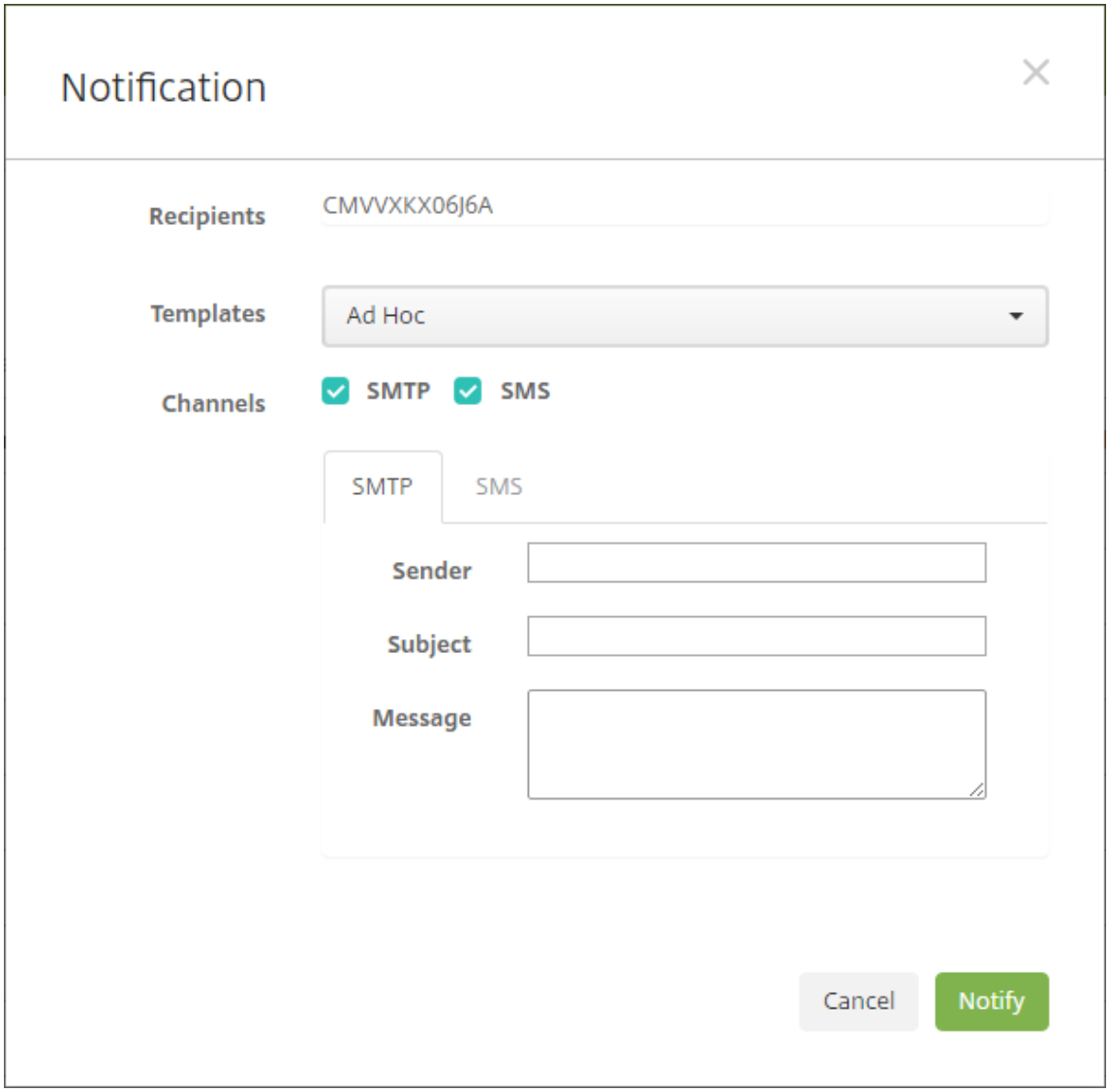


2. 单击选择文件，然后导航到要导入的文件。
3. 单击导入。设备表将列出导入的文件。
4. 要编辑设备信息，请将其选中，然后单击编辑。有关设备详细信息页面的信息，请参阅手动添加设备。

向设备发送通知

您可以从设备页面向设备发送通知。有关通知的详细信息，请参阅通知。

1. 在管理 **>** 设备页面上，选择要向其发送通知的一个或多个设备。
2. 单击通知。将显示通知对话框。收件人字段列出要接收通知的所有设备。



3. 配置以下设置：
   - 模板：在列表中，单击要发送的通知类型。对于除临时外的每个模板，主题和消息字段将显示为所选模板配置的文本。
   - 通道：选择消息的发送方式。默认值为 **SMTP** 和 **SMS**。单击选项卡以查看每个通道的消息格式。
   - 发件人：输入可选发件人。
   - 主题：输入临时消息的主题。
   - 消息：输入临时消息的消息。
4. 单击通知。

导出设备表

1. 根据您希望在导出文件中显示的内容过滤设备表。

2. 单击设备表上方的导出按钮。XenMobile 将提取过滤后的设备表中的信息，并将其转换为.csv 文件。
3. 系统提示时，打开或保存.csv 文件。

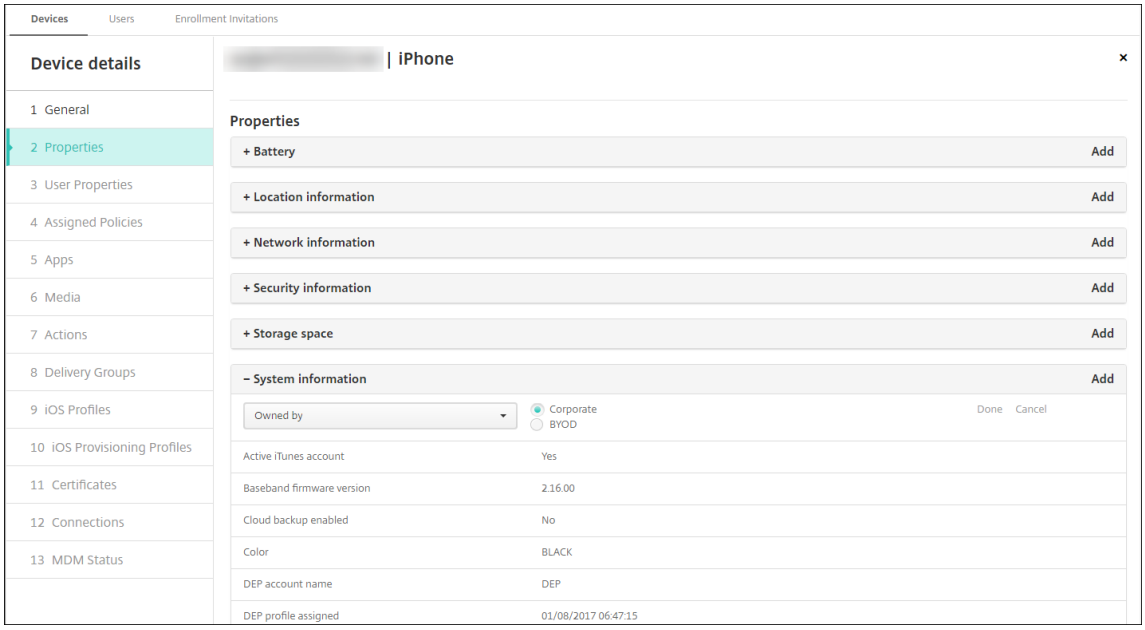
手动标记用户设备

可以在 XenMobile 中通过以下方式手动标记设备：

- 在基于邀请的注册过程中。
- 在自助服务门户注册过程中。
- 通过添加设备所有权作为设备属性

您可以选择将设备标记为公司拥有或员工拥有。使用自助服务门户自助注册设备时，可以将设备标记为公司拥有或员工拥有。也可以手动标记设备，如下所示。

1. 在 XenMobile 控制台中，从设备选项卡向设备添加属性。
2. 添加名为所有者的属性，然后选择公司或 **BYOD**（员工拥有）。



设备预配文件格式

许多移动运营商或设备制造商都会提供授权移动设备的列表。可以使用这些列表来避免手动输入长长的移动设备列表。XenMobile 支持以下三个受支持设备类型通用的导入文件格式：Android、iOS 和 Windows。

手动创建并用于将设备导入 XenMobile 的预配文件必须采用以下格式：

序列号;IMEI; 操作系统系列; 属性名 1; 属性值 1; 属性名 2; 属性值 2; … 属性名 N; 属性值 N

请紧急以下几点：

- 有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

- 使用 UTF-8 字符集。
- 使用分号 (;) 分隔预配文件中的字段。如果某个字段的某一部分包含分号，请使用反斜杠字符 (\) 进行转义。

  例如，对于此属性：

  ```
  propertyV;test;1;2
  ```

  按如下所示对其进行转义：

  ```
  propertyV\;test\;1\;2
  ```

- 对于 iOS 设备，必须提供序列号，因为序列号是 iOS 设备标识符。
- 对于其他设备平台，必须包括序列号或 IMEI。
- **OperatingSystemFamily** 的有效值为 **WINDOWS**、**ANDROID** 或 **iOS**。

设备预配文件示例：

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;
4050BF3F5173010816100655105903 93;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

文件中的每行都描述一个设备。上述示例中第一个条目的含义如下：

- 序列号：1050BF3F5173010816100655105903 91
- IMEI：15244201625379901
- 操作系统系列：WINDOWS
- 属性名称：propertyN
- 属性值：propertyV\;test\;1\;2;prop 2

ActiveSync Gateway

January 5, 2022

ActiveSync 是 Microsoft 开发的移动数据同步协议。ActiveSync 与手持设备和台式（便携式）计算机同步数据。

可以在 XenMobile 中配置 ActiveSync Gateway 规则。根据这些规则，可以允许或拒绝设备访问 ActiveSync 数据。例如，如果激活“缺少必备应用程序”规则，XenMobile 将检查应用程序访问策略中是否存在必备应用程序，如果缺少必备应用程序，则会拒绝对 ActiveSync 数据的访问。对于每个规则，可以选择允许或拒绝。默认设置为允许。

有关应用程序访问设备策略的详细信息，请参阅应用程序访问设备策略。

XenMobile 支持以下规则：

匿名设备：检查设备是否处于匿名模式。如果在设备尝试重新连接时 XenMobile 无法重新对用户进行身份验证，则可以执行此检查。

Samsung KNOX 认证失败：检查设备是否无法通过 Samsung KNOX 认证服务器的查询。

禁止的应用程序：检查设备是否具有应用程序访问策略中定义的禁止的应用程序。

隐式允许和拒绝：这是 ActiveSync Gateway 的默认操作。网关创建不满足其他任何过滤器规则条件的所有设备的设备列表，并根据该列表允许或拒绝连接。如果任何规则均不匹配，则默认为隐式允许。

不活动设备：按照服务器属性中“Device Inactivity Days Threshold”（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。

缺少所需的应用程序：检查设备是否缺少在应用程序访问策略中定义的所需应用程序。

非推荐应用程序：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码：检查用户密码是否合规。在 iOS 和 Android 设备上，XenMobile 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。例如，在 iOS 设备上，如果 XenMobile 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规设备”属性检查设备是否不合规。该属性通常由自动化操作进行更改，或由第三方利用 XenMobile API 进行更改。

吊销状态：检查设备证书是否已吊销。再次授权之前，已吊销的设备无法重新注册。

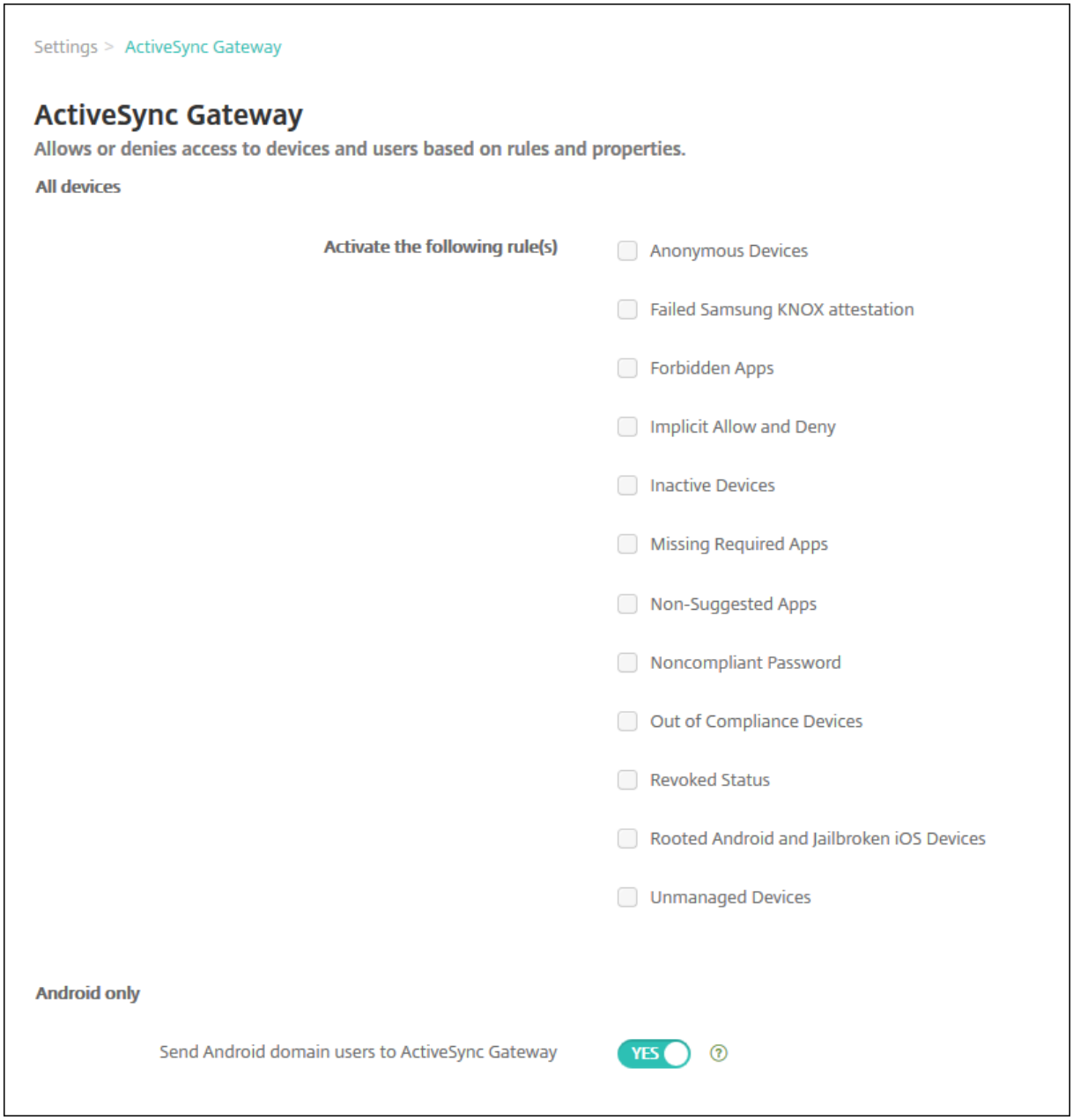
已获得 **root** 权限的 **Android** 设备和已越狱的 **iOS** 设备：检查 Android 设备或 iOS 设备是否已被越狱。

非托管设备：检查设备是否仍处于托管状态，受 XenMobile 控制。例如，在 MAM 下注册的设备或已取消注册的设备为非托管设备。

将 **Android** 域用户发送到 **ActiveSync Gateway**：单击是可确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。

配置 **ActiveSync Gateway** 设置

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **ActiveSync Gateway**。此时将显示 **ActiveSync Gateway** 页面。



1. 在激活以下规则中，选择要激活的一个或多个规则。
2. 在仅限 **Android** 中的将 **Android** 域用户发送到 **ActiveSync Gateway** 中，单击是以确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。
3. 单击保存。

从设备管理迁移到 **Android Enterprise**

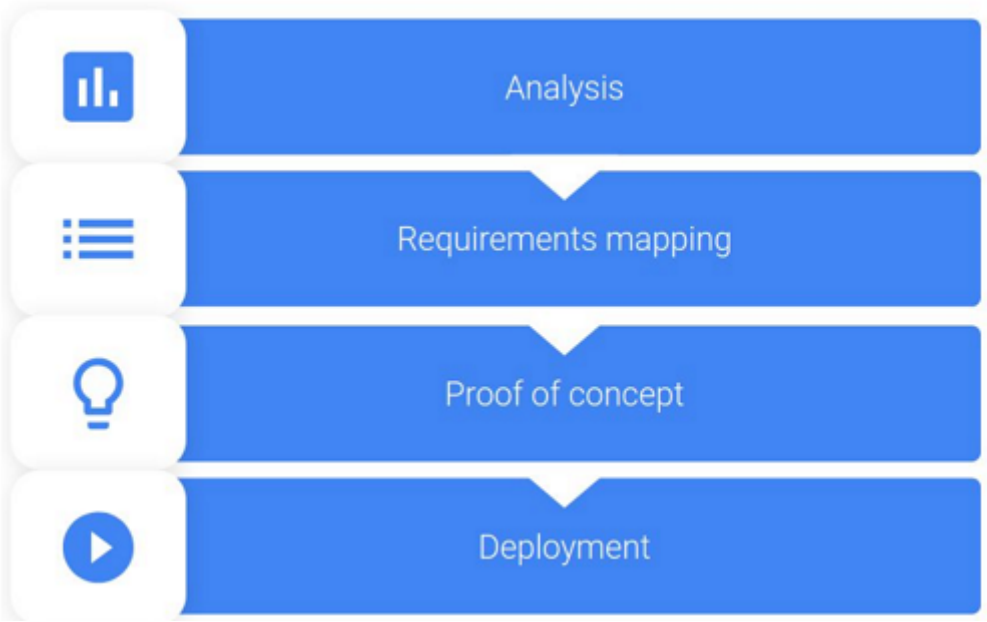
January 5, 2022

本文探讨了从旧版 Android 设备管理迁移到 Android Enterprise 的注意事项和建议。Google 即将弃用 Android 设备管理 API。该 API 支持 Android 设备上的企业应用程序。Android Enterprise 是 Google 和 Citrix 推荐的现代化管理解决方案。

XenMobile 正在更改为 Android Enterprise 作为 Android 设备的默认注册方法。Google 弃用 API 后，在设备管理模式下 Android Q 设备的注册将失败。

Android Enterprise 支持完全托管和工作配置文件设备模式。Google 出版物 Android Enterprise Migration Bluebook（《Android Enterprise 迁移蓝皮书》）详细解释了旧版设备管理与 Android Enterprise 的不同之处。我们建议您阅读 Google 提供的迁移信息。

该出版物还介绍了设备管理迁移的四个阶段，并包括下图。本文包括针对迁移阶段的 XenMobile 特定的建议。



> Android Enterprise Migration Bluebook（《Android Enterprise 迁移蓝皮书》）中的示意图
> 在 Google 的许可下重新发布。

设备管理弃用的影响

Google 将弃用以下设备管理 API。升级 Secure Hub 以 Android Q API 级别为目标，这些 API 将无法在运行 Android Q 的设备上运行：

- 禁用相机头：控制对设备相机的访问。
- 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。

弃用的 API 不会对在 Citrix 仅 MAM 模式下注册的设备产生任何影响。

建议

以下建议适用于已在 Android 旧版设备管理模式下注册的设备、未注册的设备以及在 Citrix 仅 MAM 模式下注册的设备。

设备注册状态	建议的操作
现有设备已在设备管理模式下注册，并可升级到 Android Q。	将设备升级到 Android Q 之前，请从设备管理模式迁移到 Android Enterprise。
现有设备在设备管理模式下注册。设备无法升级到 Android Q。	设备可以保持设备管理模式。但是，计划在设备刷新时将设备移动到 Android Enterprise。
现有设备已在设备管理模式下注册，并升级到 Android Q。	在 Google 弃用 API 之前，从设备管理模式迁移到 Android Enterprise。XenMobile 控制台中将显示有关这些设备的警告消息。
与 Android Q 一起交付的新设备，并在设备管理模式下注册。	在 Google 弃用 API 之前，从设备管理模式迁移到 Android Enterprise。XenMobile 控制台中将显示有关这些设备的警告消息。
随 Android Q 一起交付或可升级到 Android Q 的新设备。设备未注册。	使用 Android Enterprise 的任何新设备。
Google 弃用 API 后，Android Q 上的新设备或现有设备将在设备管理模式下注册。	为了避免弃用的 Google API 的影响，Citrix 建议在 Google 弃用 API 之前迁移到 Android Enterprise。在该日期之后，这些设备的注册将失败。
在 Citrix 仅 MAM 模式下注册的新设备或现有设备	无需采取任何操作。弃用的 Google API 不会对仅 MAM 模式下的设备产生任何影响。

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，以便您可以将旧版功能映射到 Android Enterprise 功能

建议的分析

1. 在 XenMobile 上评估 Android Enterprise：完全托管，通过工作配置文件、专用设备、工作配置文件 (BYOD) 进行完全托管。
2. 根据 Android Enterprise 分析您当前的设备管理功能。
3. 记录您的设备管理用例。

要记录您的设备管理用例，请执行以下操作：

1. 在 XenMobile 控制台中创建电子表格并列出当前的策略组。
2. 基于现有策略组创建单独的用例。
3. 对于每个用例，请记录以下内容：
    - 名称
    - 企业所有者
    - 用户身份模型
    - 设备要求
        - 安全性
        - 管理
        - 可用性
    - 设备清单
        - 制造商和型号
        - 操作系统版本
    - 应用程序
4. 对于每个应用程序，请列出：
    - 应用程序名称
    - 软件包名称
    - 托管方法
    - 应用程序是公用还是专用
    - 应用程序是否具有强制性 (true/false)

要求映射

根据完成的分析，确定您的 Android Enterprise 功能要求。

建议的要求映射

1. 确定管理模式和注册方法：
    - 工作配置文件 (BYOD)：需要重新注册。无需重置出厂设置。
    - 完全托管：需要恢复出厂设置。使用 QR 码、近场通信 (NFC) 碰撞、设备策略控制器 (DPC) 标识符、零触摸方式注册设备。
2. 创建应用程序迁移策略。
3. 将用例要求映射到 Android Enterprise 功能。记录与要求最匹配的每个设备要求及其相应的 Android 版本的功能。
4. 根据功能要求（7.0、8.0、9.0）确定最低 Android 操作系统。

5. 选择身份模型：
   - 建议：托管 Google Play 帐户
   - 仅当您是 Google Cloud Identity 客户时才使用 Google G-Suite 帐户
6. 创建设备策略：
   - 无操作：如果设备满足最低操作系统级别
   - 升级：如果设备支持且可以更新到支持的操作系统
   - 替换：如果设备无法更新到支持的操作系统级别

推荐的应用程序迁移策略

完成需求映射后，将应用程序从 Android 平台移动到 Android Enterprise 平台。有关发布应用程序的详细信息，请参阅添加应用程序。

- 公共应用商店应用程序
  1. 选择要迁移的应用程序，然后编辑应用程序以清除 Google Play 设置，然后选择 **Android Enterprise** 作为平台。
  2. 选择交付组。如果某个应用程序是必需的，请将该应用程序移动到交付组中的必需应用程序列表。

  保存应用程序后，该应用程序将显示在 Google Play 应用商店中。如果您有工作配置文件，应用程序将显示在工作配置文件中的 Google Play 应用商店中。
- 专用（企业）应用程序

  专用应用程序由内部开发人员或第三方开发人员开发。我们建议您使用 Google Play 发布专用应用程序。
  1. 选择要迁移的应用程序，然后编辑应用程序以选择 **Android Enterprise** 作为平台。
  2. 上载 APK 文件，然后配置应用程序设置。
  3. 将应用程序发布到所需的交付组。
- MDX 应用程序
  1. 选择要迁移的应用程序，然后编辑应用程序以选择 **Android Enterprise** 作为平台。
  2. 上载 MDX 文件。完成应用程序审批流程。
  3. 选择 MDX 策略。

  对于企业 MDX 应用程序，我们建议将其更改为 MDX SDK 模式打包的应用程序：
  - 选项 1：使用专门分配给贵组织的开发人员帐户在 Google Play 中托管 APK。在 XenMobile 中发布 MDX 文件。
  - 选项 2：从 XenMobile 发布应用程序作为企业应用程序。在 XenMobile 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 和 Android Enterprise 平台的策略：请编辑策略并选择平台 **Android Enterprise**。

对于 Android Enterprise，请考虑注册模式。某些策略选项仅适用于处于工作配置文件模式或完全托管模式的设备。

概念证明

将应用程序迁移到 Android Enterprise 后，可以设置迁移测试以验证功能是否按预期运行。

推荐的概念证明设置

1. 设置部署基础结构：
    - 为您的 Android Enterprise 测试创建交付组。
    - 在 XenMobile 中配置 Android Enterprise。
2. 设置用户应用程序。
3. 配置 Android Enterprise 功能。
4. 将策略分配给 Android Enterprise 交付组。
5. 测试和确认功能。
6. 完成每个用例的设备设置流程。
7. 记录用户设置步骤。

部署

现在，您可以部署 Android Enterprise 设置并准备用户进行迁移。

建议的部署策略

Citrix 推荐的部署策略是为 Android Enterprise 测试所有生产系统，然后在以后完成设备迁移。

- 在这种情况下，用户继续使用旧设备与其当前配置。可以为 Android Enterprise 管理设置新设备。
- 请仅在需要升级或更换时迁移现有设备。
- 在常规生命周期结束时将现有设备迁移到 Android Enterprise 管理中。或者，在这些设备因丢失或损坏而需要更换时，迁移这些设备。

Android Enterprise

January 5, 2022

Android Enterprise 是一套由 Google 提供的作为 Android 设备的企业管理解决方案工具和服务。借助 Android Enterprise：

- 可以使用 XenMobile 管理公司拥有的 Android 设备以及携带自己的 (BYOD) Android 设备。
- 可以管理整个设备或设备上的单独配置文件。这一单独的配置文件将企业帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。
- 还可以管理专用于单一用途的设备，例如库存管理。有关 Google 提供的 Android Enterprise 功能的概述，请参阅 Android Enterprise Management。

资源：

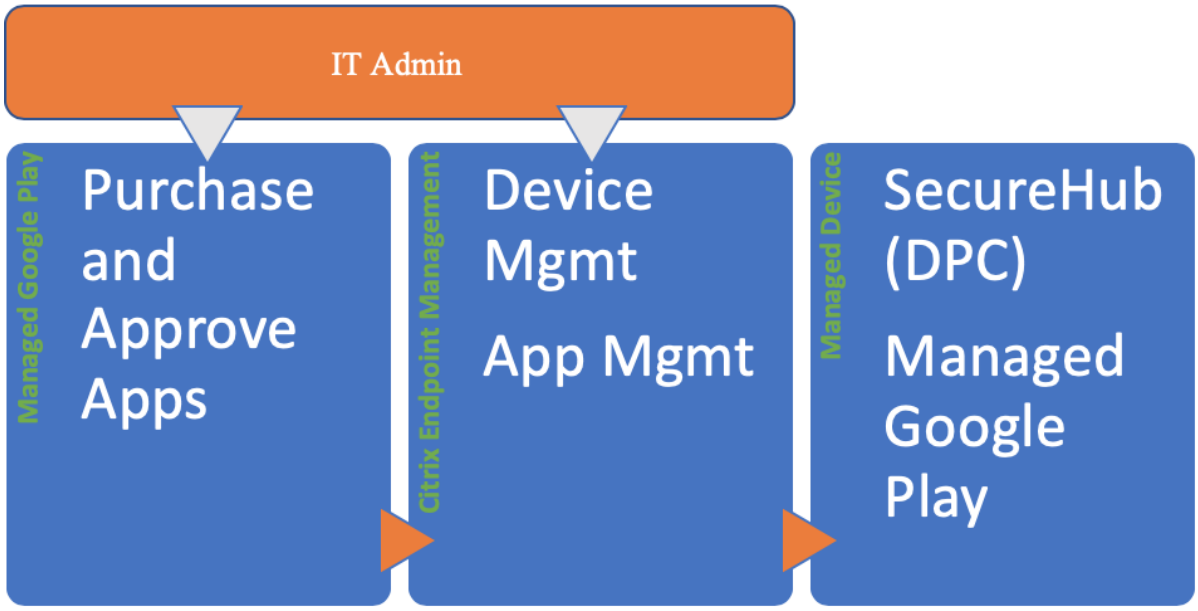
- 有关与 Android Enterprise 相关的术语和定义的列表，请参阅 Google Android Enterprise 开发人员指南中的 Android Enterprise terminology（Android Enterprise 术语）。Google 经常更新这些术语。
- 有关 XenMobile 支持的 Android 操作系统，请参阅支持的设备操作系统。
- 有关为 Android Enterprise 设置网络环境时要考虑的出站连接的信息，请参阅 Google 支持文章 Android Enterprise Network Requirements（Android Enterprise 网络要求）。

将 XenMobile 与托管 Google Play 相集成以使用 Android Enterprise 时，可以创建一个企业。Google 将企业定义为组织与企业移动管理 (EMM) 解决方案之间的绑定。组织通过您的解决方案管理的所有用户和设备都属于其企业。

适用于 Android Enterprise 的企业有三个组件：EMM 解决方案、设备策略控制器 (DPC) 应用程序和 Google 企业应用程序平台。当您将 XenMobile 与 Android Enterprise 相集成时，完整的解决方案包含以下组件：

- **XenMobile**： Citrix EMM。XenMobile 是用于安全数字工作区的统一 XenMobile 解决方案。XenMobile 为 IT 管理员提供了为其组织管理设备和应用程序的方法。
- **Citrix Secure Hub**： Citrix DPC 应用程序。Secure Hub 是 XenMobile 的启动板。Secure Hub 在设备上强制执行策略。
- 托管 **Google Play**：与 XenMobile 集成的 Google 企业应用程序平台。Google Play EMM API 设置应用程序策略并分发应用程序。

下图显示了管理员如何与这些组件进行交互，以及组件之间如何交互：



将托管 **Google Play** 与 **XenMobile** 结合使用

> 注意：
>
> 可以使用托管 Google Play 或 Google Workspace 将 Citrix 注册为您的 EMM 提供商。本文讨论了使用 Android Enterprise 与托管 Google Play。如果贵组织使用 Google Workspace 提供对应用程序的访问权限，您可以将其用于 Android Enterprise。请参阅适用于 Google Workspace（以前称为 G Suite）客户的旧版 Android Enterprise。

使用托管 Google Play 时，您将为设备和最终用户预配托管 Google Play 帐户。托管 Google Play 帐户提供对托管 Google play 的访问，以允许用户安装和使用您提供的应用程序。如果贵组织使用第三方身份服务，您可以将托管 Google Play 帐户与您的现有身份帐户链接。

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

对于 XenMobile 管理员，托管 Google Play 将 Google Play 的用户体验和应用商店功能与为企业设计的一组管理功能相结合。使用托管 Google Play 可添加、购买和审批应用程序，以便部署到设备上的 Android Enterprise 工作区。可以使用 Google Play 部署您的公共应用程序、专用应用程序和第三方应用程序。

对于托管设备的用户，托管 Google Play 是企业应用商店。用户可以浏览应用程序、查看应用程序详细信息以及安装这些应用程序。与 Google Play 的公共版本不同，用户只能从您为其提供的托管 Google Play 安装应用程序。

设备部署方案和操作模式

设备部署方案是指谁拥有您所部署的设备以及如何管理这些设备。设备配置文件是指 DPC 如何在设备上管理和强制执行策略。

工作配置文件将企业帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。有关工作配置文件的更多详细信息，请参阅 Google Android Enterprise 帮助主题 What is a work profile（工作配置文件是什么）。

> 重要：
>
> 当 Android Enterprise 设备更新到 Android 11 时，Google 会将作为“使用工作配置文件的完全托管”进行托管的设备迁移到新的安全性增强的工作配置文件体验。有关详细信息，请参阅使用工作配置文件进行完全托管的 Android Enterprise 的未来更改。

设备管理	用例	工作配置文件	个人资料	备注
公司拥有的设备（完全托管）	仅供工作使用的公司拥有的设备	否	是。DPC 可以执行设备范围的操作，例如配置设备范围的连接、配置全局设置和执行出厂重置。	仅适用于新设备或恢复出厂设置的设备。
通过工作配置文件完全托管	供工作和个人使用的公司拥有的设备	是	是。两个 DPC 副本在这些设备上运行：一个在设备所有者模式下管理设备，另一个在配置文件所有者模式下管理工作配置文件。您可以将单独的策略应用到设备和工作配置文件。	以前称为企业拥有但由个人使用 (COPE) 的设备。
专用设备 *	为单个用例配置的公司拥有的设备，例如数字标牌或票证打印	否	是。可以仅提供所需的应用程序，并阻止用户添加其他应用程序。	以前称为公司拥有、单一用途 (COSU) 的设备。
BYOD 工作配置文件 **	在工作配置文件模式下注册的个人设备（又称为配置文件所有者模式）	是	是。DPC 仅管理工作配置文件，不管理整个设备。	这些设备不需要是新设备或恢复出厂设置的设备。

* 用户可以共享专用设备。当用户登录到专用设备上的应用程序时，其工作状态与应用程序一致，而非与设备一致。

** 在 BYOD 工作配置文件模式下，XenMobile 不支持 Zebra 设备。XenMobile 支持 Zebra 设备作为完全托管设备并且处于设备旧模式（也称为设备管理模式）。

有关从旧模式迁移到设备所有者或配置文件所有者模式的信息，请参阅从设备管理迁移到 Android Enterprise。

身份验证方法

注册配置文件确定 Android 设备在 MAM、MDM 还是 MDM+MAM 中注册，并提供供用户选择退出 MDM 的选项。

有关指定安全级别和所需注册步骤的信息，请参阅配置注册安全模式。

XenMobile 支持对在 MDM+MAM 中注册的 Android 设备使用以下身份验证方法。有关信息，请参阅证书和身份验证下的文章。

- 域
- 域加安全令牌
- 客户端证书
- 客户端证书加域
- 身份提供程序：
  - Azure Active Directory
  - Citrix 身份提供程序

另一种罕见的身份验证方法是客户端证书加安全令牌。有关信息，请参阅 https://support.citrix.com/article/CTX215200。

要求

在开始使用 Android Enterprise 之前，您需要：

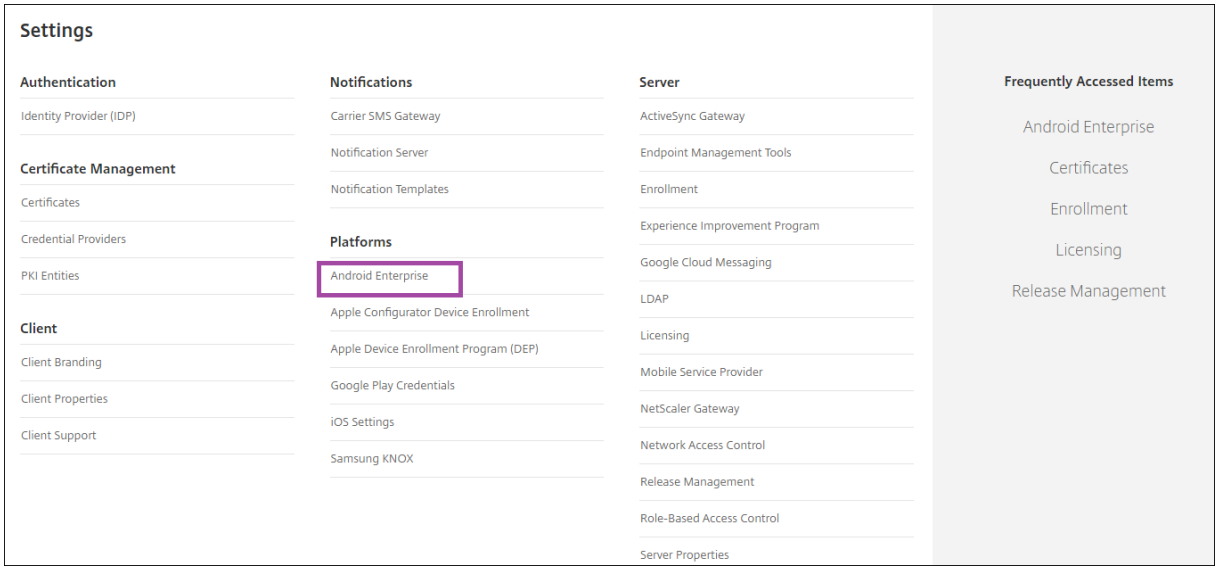
- 帐户和凭据：
  - 要通过托管 Google Play 设置 Android Enterprise，则需要企业 Google 帐户
  - 要下载最新的 MDX 文件，则需要 Citrix 客户帐户
  - 要部署专用应用程序（可选），则需要 Google 开发人员帐户
- 针对 XenMobile 配置的 Firebase Cloud Messaging (FCM)。有关说明，请参阅 Firebase Cloud Messaging。
- 对于 Samsung Knox 移动注册（可选），则需要 Knox 高级许可证。

将 **XenMobile** 连接到 **Google Play**

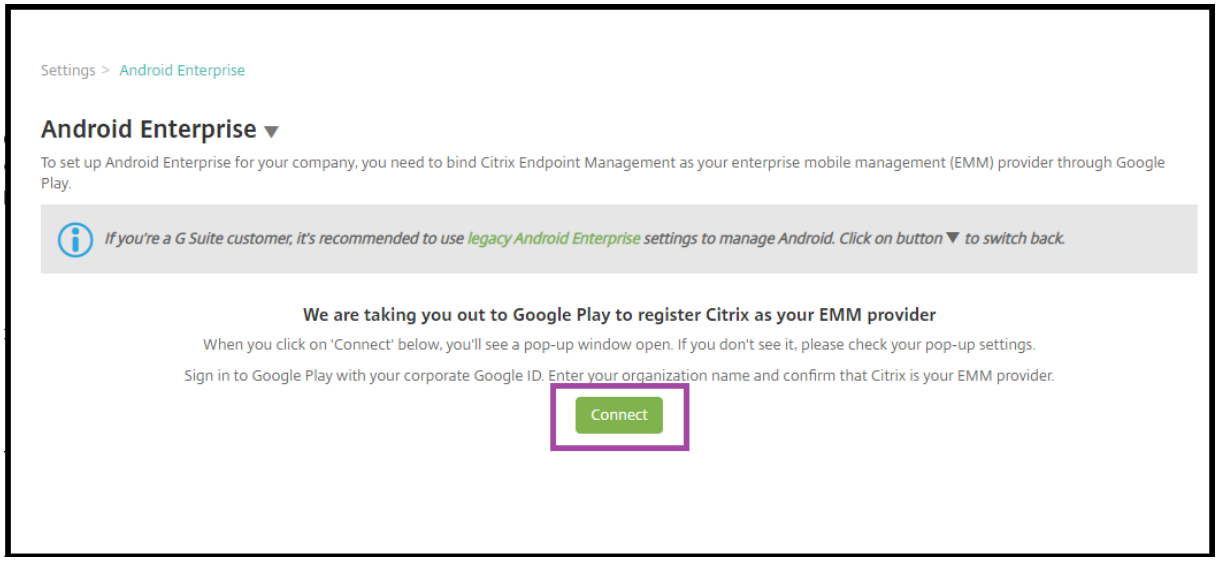
要为贵组织设置 Android Enterprise，请通过托管 Google Play 将 Citrix 注册为 EMM 提供商。该设置将托管 Google Play 连接到 XenMobile，并在 XenMobile 中为 Android Enterprise 创建一个企业。

您需要一个企业 Google 帐户才能登录 Google Play。

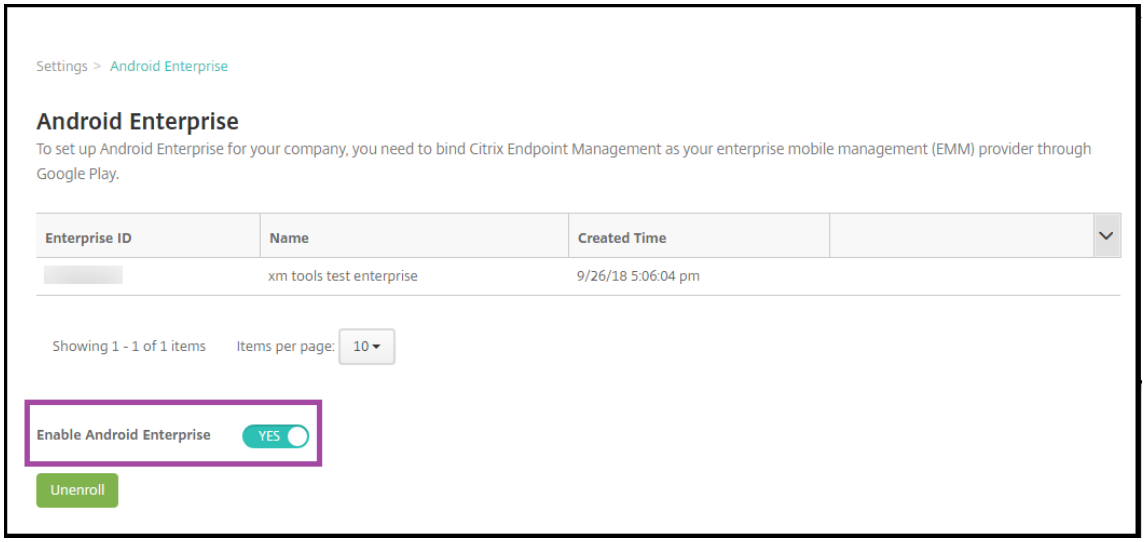
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 转至设置 **> Android Enterprise**。



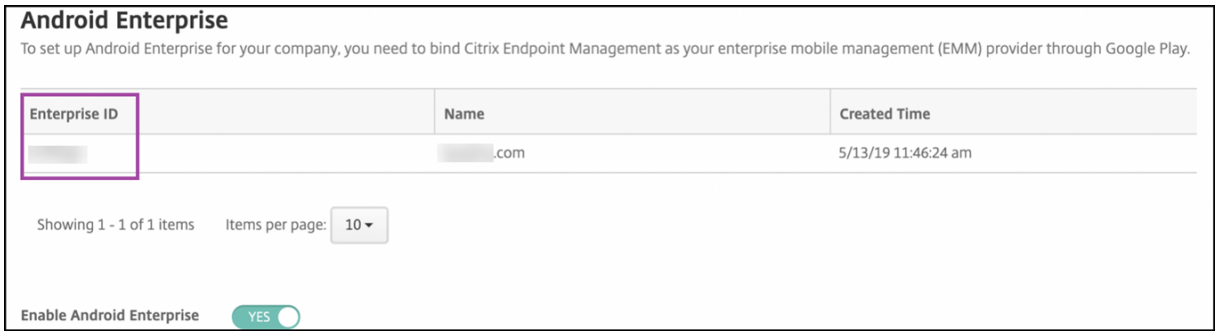
1. 单击连接。Google Play 将打开。



1. 使用您的企业 Google 帐户凭据登录 Google Play。输入贵组织的名称并确认 Citrix 是您的 EMM 提供商。
2. 将为 Android Enterprise 添加企业 ID。要启用 Android Enterprise，请将启用 **Android Enterprise** 滑动到是。



您的企业 ID 将显示在 XenMobile 控制台中。



您的环境已连接到 Google，并准备好管理设备。您现在可以为用户提供应用程序。

XenMobile 可用于为用户提供 Citrix 移动生产力应用程序、MDX 应用程序、公共应用商店应用程序、Web 和 SaaS 应用程序、企业应用程序和 Web 链接。有关这些类型的应用程序以及向用户提供这些应用程序的详细信息，请参阅添加应用程序。

下面的部分介绍了如何提供移动生产力应用程序。

向 **Android Enterprise** 用户提供 **Citrix** 移动生产力应用程序

为 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. 为用户用于访问其设备上的工作配置文件的安全质询配置规则。请参阅配置安全质询策略。

您发布的应用程序可用于在 Android Enterprise 企业中注册的设备。

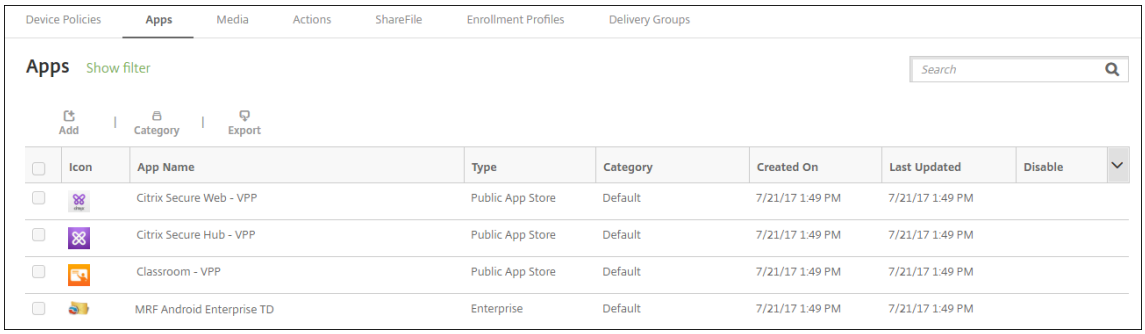
> 注意：

> 将 Android Enterprise 公共应用商店应用程序部署给 Android 用户时，该用户将自动在 Android Enterprise 中注册。

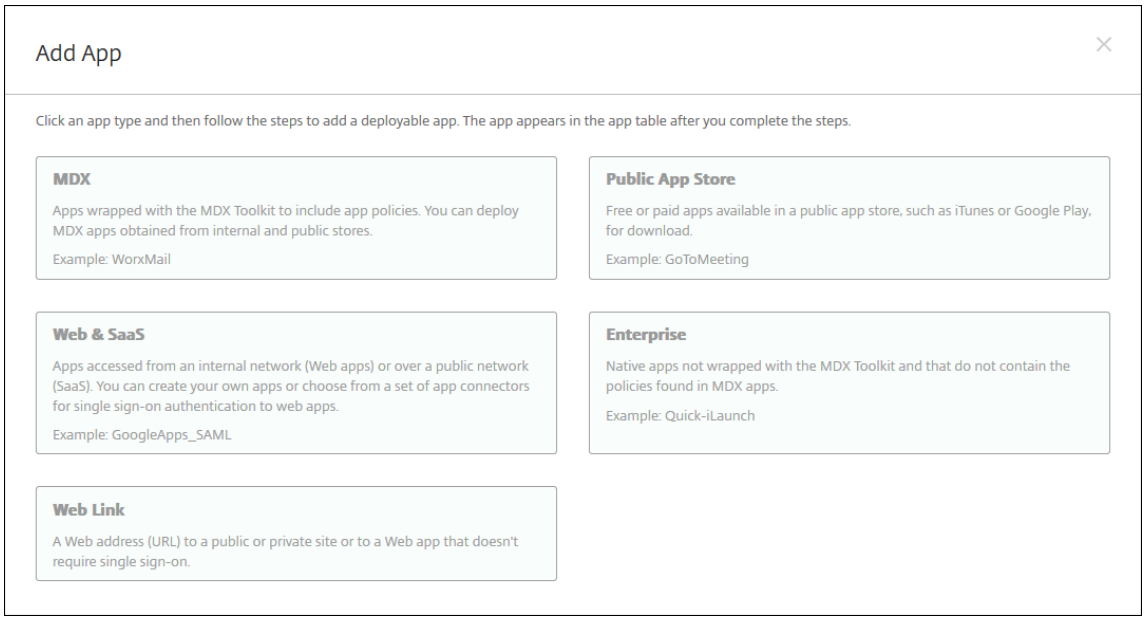
将应用程序配置为 **MDX** 应用程序

要将 Citrix 生产力应用程序配置为适用于 Android Enterprise 的 MDX 应用程序，请执行以下操作：

1. 在 XenMobile 控制台中，单击配置 **>** 应用程序。此时将显示应用程序页面。

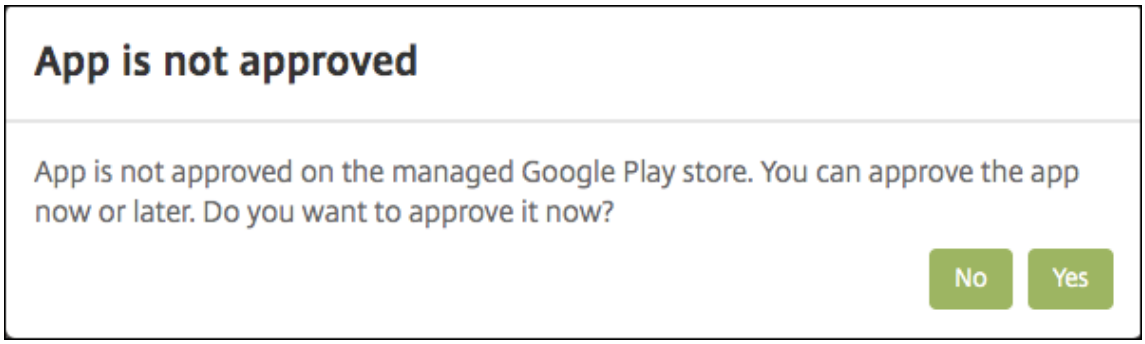


2. 单击添加。此时将显示添加应用程序对话框。

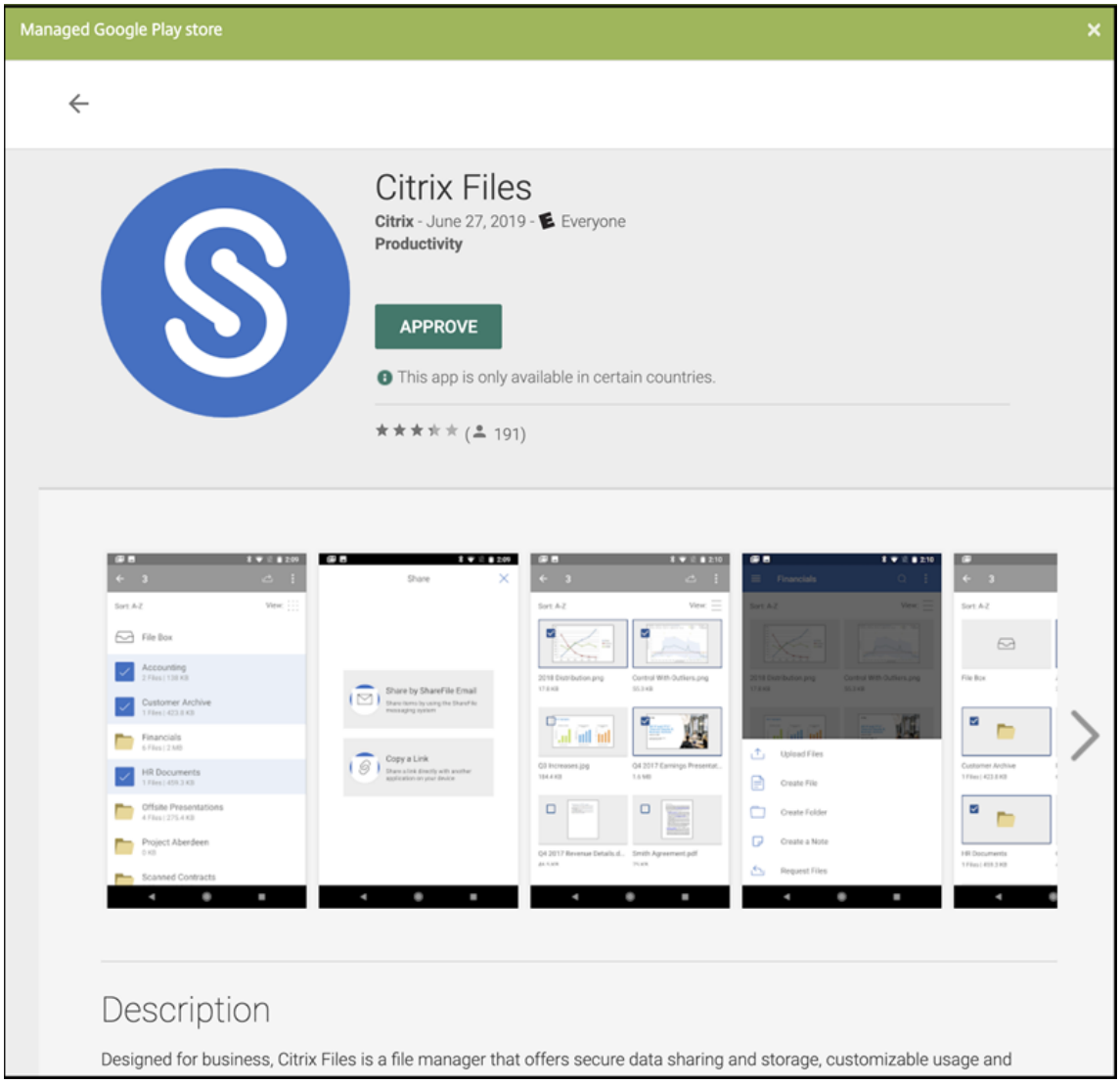


3. 单击 **MDX**。此时将显示应用程序信息页面。
4. 在页面左侧，选择 **Android Enterprise** 作为平台。
5. 在应用程序信息页面中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在应用程序表中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

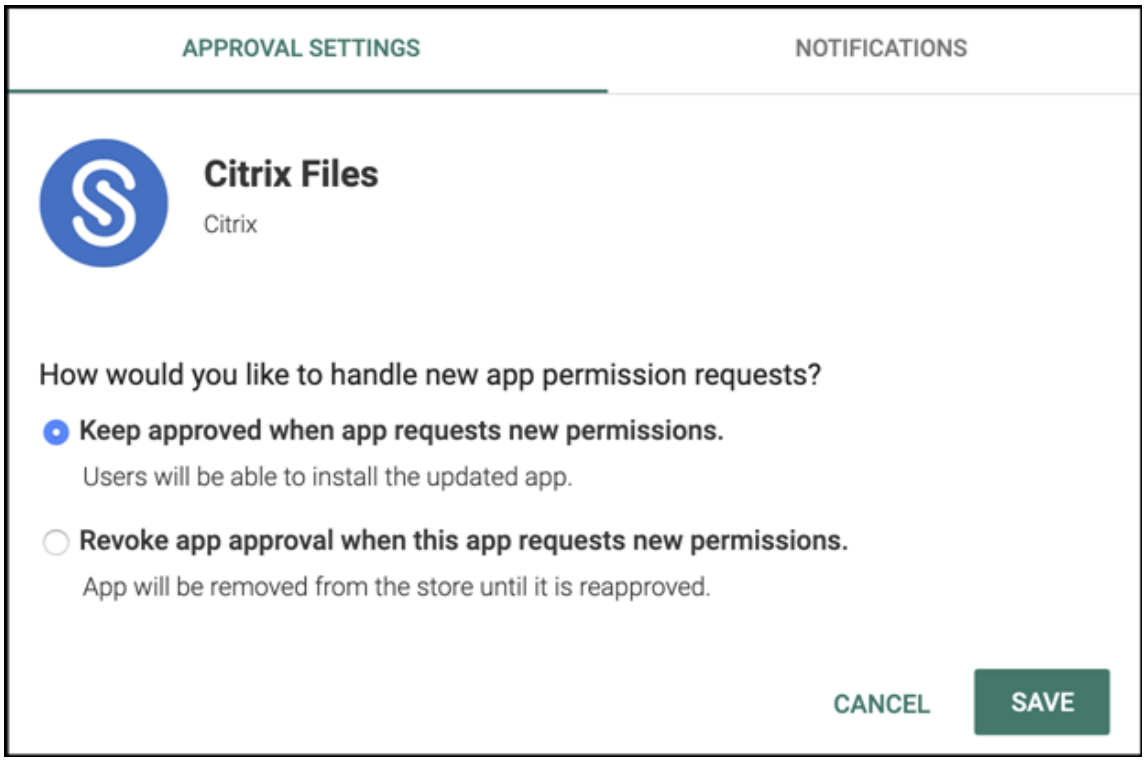
6. 单击 **Next**（下一步）。此时将显示 **Android Enterprise MDX** 应用程序页面。
7. 单击上载并导航到应用程序的.mdx 文件的文件位置。选择该文件，然后单击打开。
8. UI 会通知您附加的应用程序是否需要从托管 Google Play 应用商店获得批准。要在不离开 XenMobile 控制台的情况下审批应用程序，请单击是。



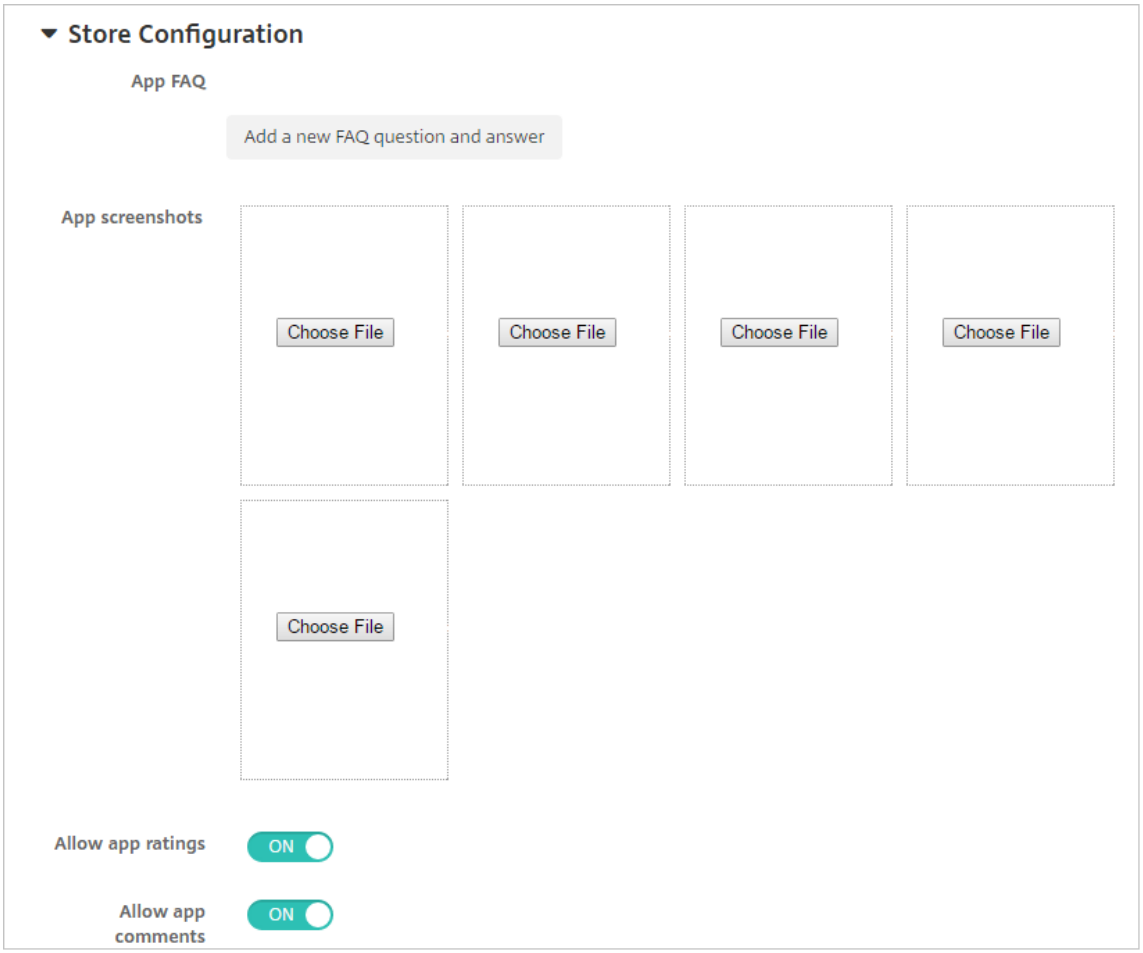
9. 当托管 Google Play 应用商店页面打开时，单击批准。



10. 再次单击 **Approve**（批准）。
11. 选择 **Keep approved when app requests new permissions**（在应用程序请求新权限时保持已批准）。单击保存。



12. 当应用程序获得批准并保存后，页面上会显示更多设置。配置以下设置：
    - 文件名：键入与应用程序关联的文件名。
    - 应用程序说明：键入应用程序的说明。
    - 产品轨迹：指定要推送到用户设备的产品轨迹。如果您有一个专为测试而设计的轨迹，则可以选择并将其分配给您的用户。默认值为生产。
    - 应用程序版本：（可选）键入应用程序版本号。
    - 软件包 **ID**： Google Play 应用商店中的应用程序的 URL。
    - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
    - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
    - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
13. 配置 **MDX** 策略。有关 MDX 应用程序的应用程序策略的详细信息，请参阅 MDX 策略概览和 MAM SDK 概览。
14. 配置部署规则。有关信息，请参阅部署资源。
15. 展开应用商店配置。此设置不适用于仅出现在托管 Google Play 中的 Android Enterprise 应用程序。

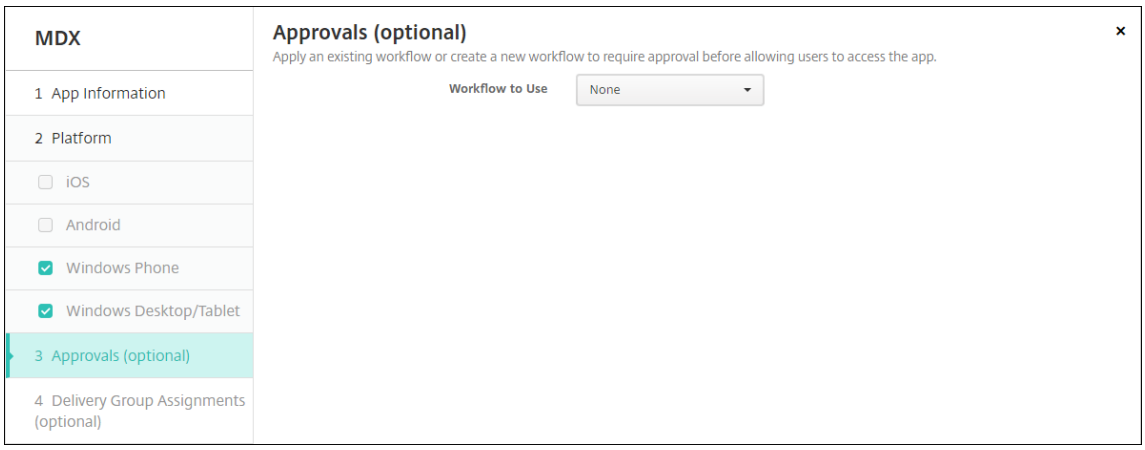


（可选）可以添加应用程序的常见问题解答或显示在应用商店中的屏幕截图。还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - 应用程序常见问题解答：添加应用程序的常见问题和答案。
  - 应用程序屏幕截图：添加屏幕截图以帮助在应用商店中对应用程序进行分类。上载的图形必须为 PNG 格式。不能上载 GIF 或 JPEG 图片。
  - 允许对应用程序评分：选择是否允许用户对应用程序进行评分。默认值为开。

    允许评价应用程序：选择是否允许用户评价选定的应用程序。默认值为开。

16. 单击 **Next**（下一步）。此时将显示审批页面。

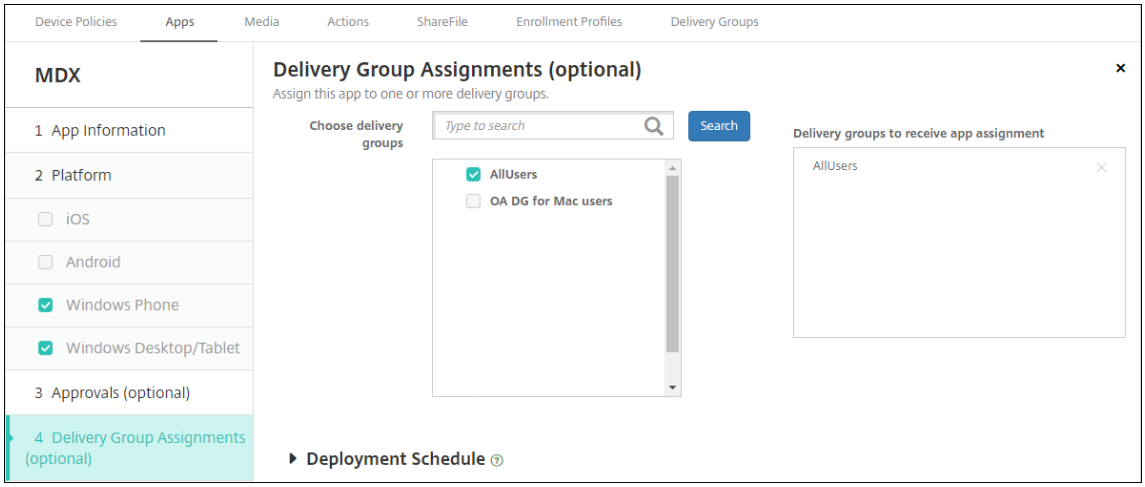


创建用户帐户时如果需要审批则使用工作流。如果不想设置审批工作流，可以跳至步骤 15。

要指定或创建工作流，请配置以下设置：

- 要使用的工作流：在此列表中，单击现有工作流或单击创建新工作流。默认设置为无。
- 如果选择创建新工作流，请配置以下设置。有关详细信息，请参阅应用工作流。
- 名称：键入工作流的唯一名称。
- 说明：（可选）键入工作流的说明。
- 电子邮件审批模板：在列表中，选择要指定的电子邮件审批模板。单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
- 经理审批级别：在列表中，选择此工作流所需的经理审批级别数。默认值为 1 级。可能的选项包括：
  - 不需要
  - 1 级
  - 2 级
  - 3 级
- 选择 **Active Directory** 域：在列表中，选择用于工作流的合适 Active Directory 域。
- 查找所需的其他审批者：在搜索字段中键入其他所需人员的姓名，然后单击搜索。源于 Active Directory 的姓名。
- 姓名显示在此字段中后，选中姓名旁边的复选框。姓名和电子邮件地址显示在选定的其他所需审批者列表中。
  - 要从选定的其他所需审批者列表中删除人员，请执行以下操作之一：
    * 单击搜索以查找选定域中的所有人员列表。
    * 在搜索框中键入完整姓名或部分姓名，然后单击搜索以限制搜索结果。
    * 在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。滚动列表，并取消选中要删除的各个姓名旁边的复选框。

17. 单击 **Next**（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者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。
19. 展开部署计划，然后配置以下设置：
    - 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。
    - 在“部署计划”旁边，单击立即或以后。默认选项为立即。
    - 如果单击以后，请单击日历图标，然后选择部署的日期和时间。
    - 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
    - 在为始终启用的连接部署旁边，确保选择了关。默认选项为关。如果您开始使用版本为 10.18.19 或更高版本的 XenMobile，则始终启用的连接将不适用于 Android Enterprise。我们不建议开始使用 10.18.19 版之前的 XenMobile 的客户使用这些连接。

      如果在设置 > 服务器属性中配置了计划后台部署密钥，则适用此选项。

      配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。
20. 单击保存。

重复上述步骤，为每个移动生产力应用程序配置 MDX 应用程序。

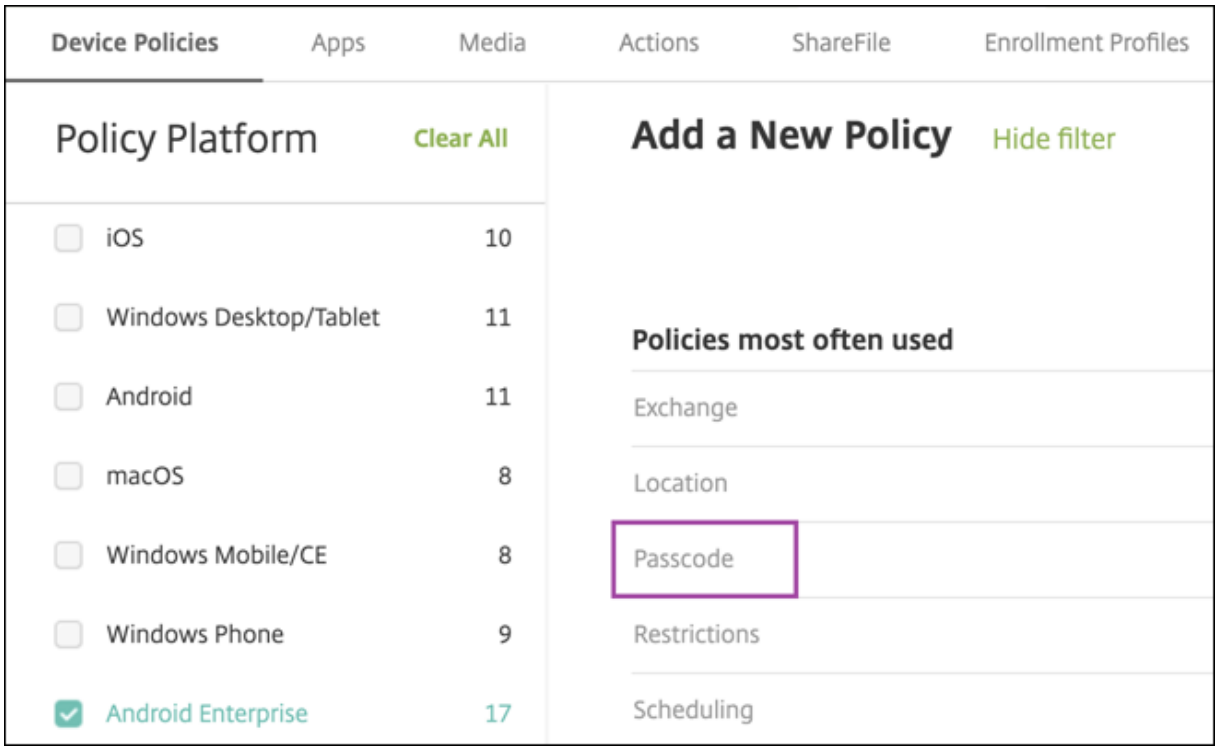
配置安全质询策略

XenMobile 通行码设备策略为用户访问其设备或其设备上的 Android Enterprise 工作配置文件的安全质询配置一组规则。安全质询可能是通行码或生物特征识别。有关通行码策略的详细信息，请参阅通行码设备策略。

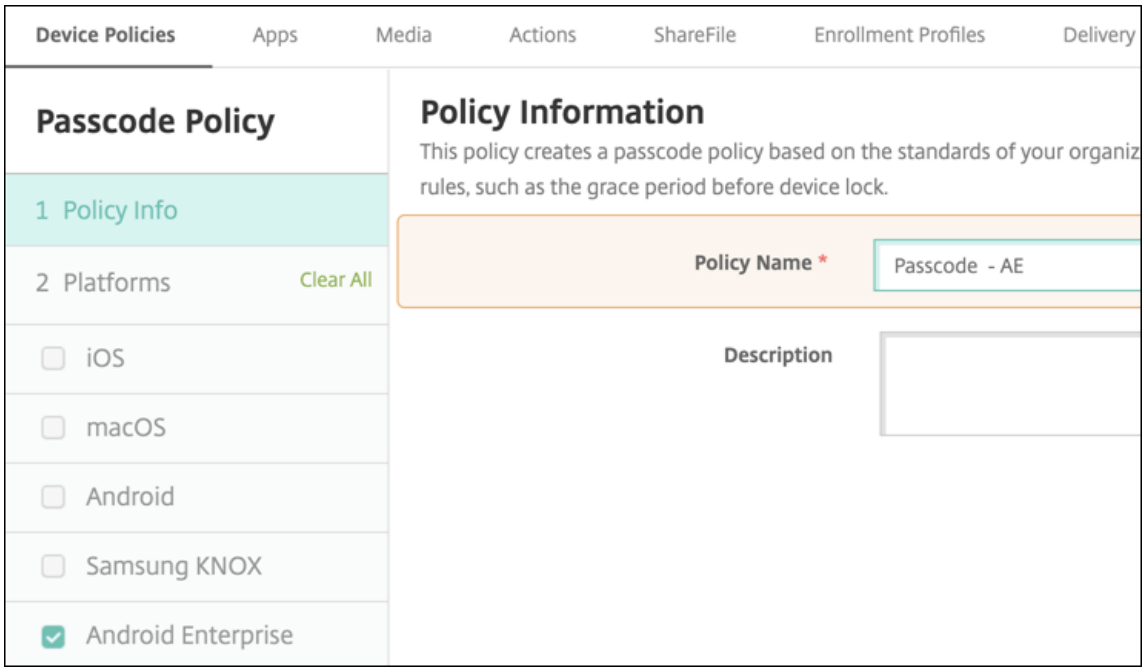
- 如果您的 Android Enterprise 部署包含 BYOD 设备，请为工作配置文件配置通行码策略。
- 如果您的部署包括公司拥有的完全托管设备，请为设备本身配置通行码策略。
- 如果您的部署包括两种类型的设备，请配置两种类型的通行码策略。

要配置通行码策略，请执行以下操作：

1. 在 XenMobile 控制台中，转至配置 **>** 设备策略。
2. 单击添加。
3. 单击显示过滤器以显示策略平台窗格。在策略平台窗格中，选择 **Android Enterprise**。
4. 单击右侧窗格上的通行码。



1. 输入策略名称。单击 **Next**（下一步）。



2. 配置通行码策略设置。
    - 将需要设备通行码设置为开，以查看设备本身的安全质询可用的设置。
    - 将工作配置文件安全质询设置为开，以查看可用于工作配置文件安全质询的设置。
3. 单击 **Next**（下一步）。
4. 将策略分配给一个或多个交付组。
5. 单击保存。

创建注册配置文件

如果为 XenMobile 部署启用了 Android Enterprise，注册配置文件可以控制 Android 设备的注册方式。创建注册配置文件以注册 Android Enterprise 设备时，可以配置注册配置文件以将新设备和重置为出厂设置的设备注册为：

- 完全托管设备
- 专用设备（COSU 设备）
- 使用工作配置文件的完全托管设备（COPE 设备）

还可以配置其中每个 Android Enterprise 注册配置文件以将 BYOD Android 设备注册为工作配置文件设备。

如果为您的 XenMobile 部署启用了 Android Enterprise，则所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。默认情况下，全局注册配置文件会将新的和恢复出厂设置的 Android 设备注册为完全托管设备，并将 BYOD Android 设备注册为工作配置文件设备。

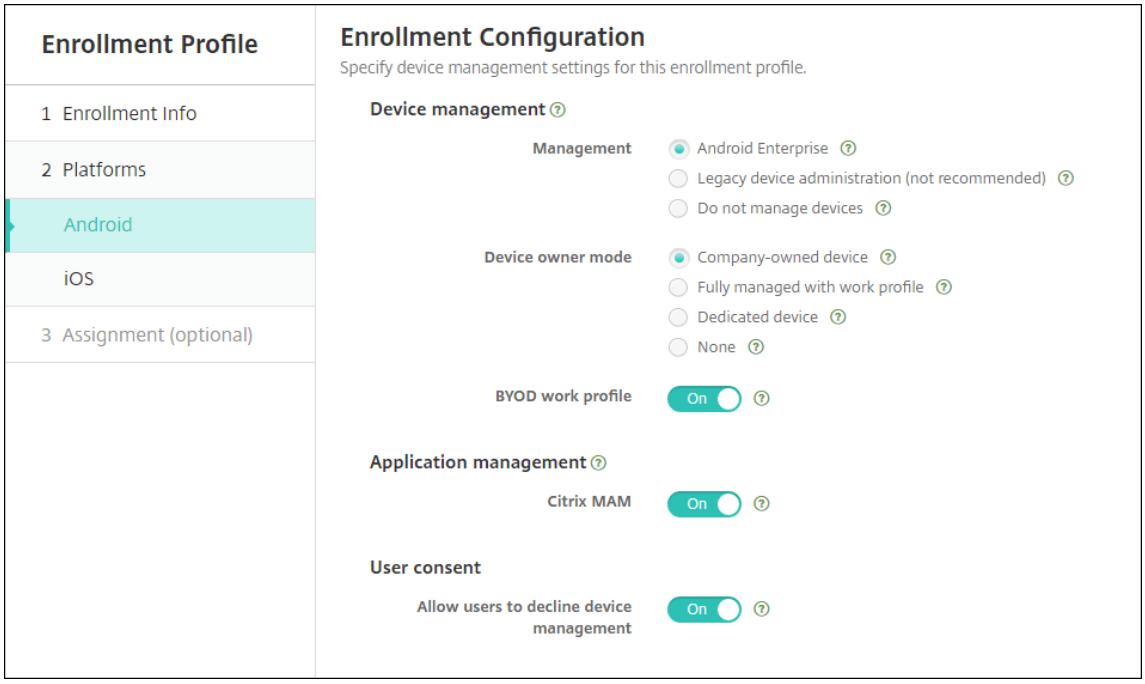
创建注册配置文件时，需要为其分配交付组。如果用户属于具有不同注册配置文件的多个交付组，该交付组的名称决定使用的注册配置文件。XenMobile 选择按字母顺序排列的交付组列表中最后显示的交付组。有关详细信息，请参阅注册配置文件。

可以使用注册配置文件来组合多个用例，例如仅 MDM、MDM+MAM 和仅 MAM。您的 XenMobile Server 许可证类型（反映在服务器属性 `xms.server.mode` 中）决定了配置 **>** 注册配置文件中的可用设置。

为完全托管设备添加注册配置文件

默认情况下，全局注册配置文件将注册完全托管设备，但您可以创建更多注册配置文件以注册完全托管设备。

1. 在 XenMobile 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置使用此配置文件的成员可以注册的设备数量。
4. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。
5. 将管理设置为 **Android Enterprise**。
6. 将设备所有者模式设置为公司拥有的设备。



7. **BYOD** 工作配置文件允许您配置注册配置文件以将 BYOD 设备注册为工作配置文件设备。将新设备和重置为出厂设置的设备注册为完全托管设备。

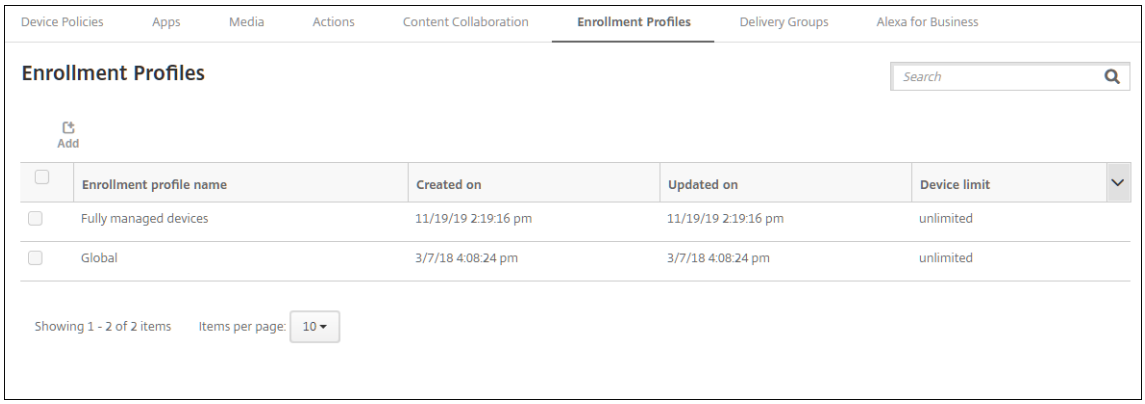
   - 将 **BYOD** 工作配置文件设置为开，以允许将 BYOD 设备注册为工作配置文件设备。默认值为开。
   - 将 **BYOD** 工作配置文件设置为关，以限制对完全托管设备的注册。

8. 选择是否在 Citrix MAM 中注册设备。
9. 如果将 **BYOD** 工作配置文件设置为开，请配置用户同意书。要允许 BYOD 工作配置文件设备的用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。

   如果 **BYOD** 工作配置文件设置为开，则允许用户拒绝设备管理的默认值为开。如果 **BYOD** 工作配置文件设置为关，则禁用允许用户拒绝设备管理。

10. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
11. 请选择包含注册完全托管设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

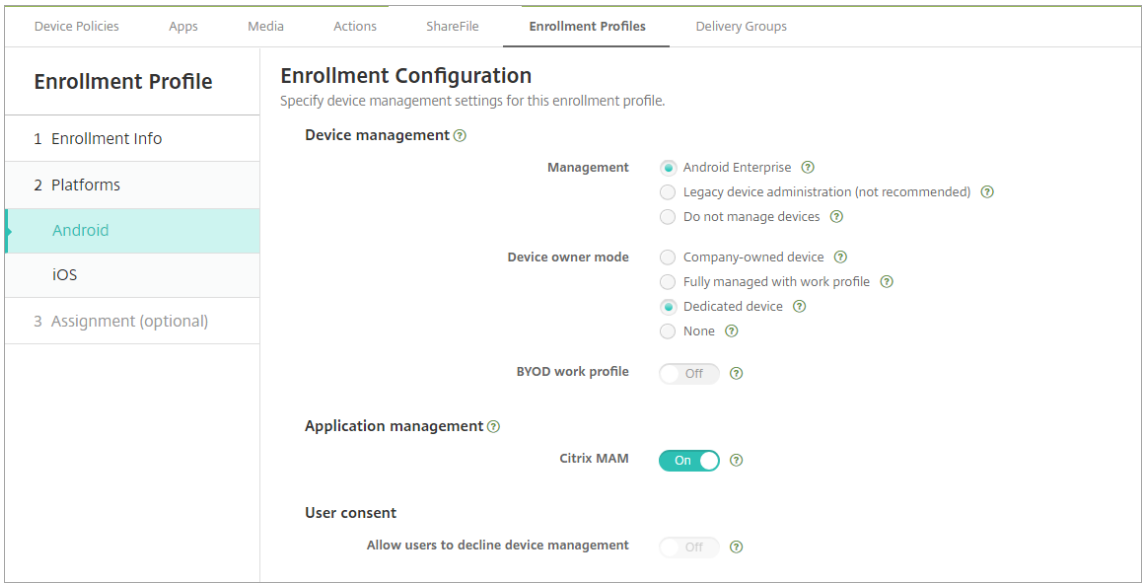
    显示的“注册配置文件”页面中添加了您的配置文件。



添加专用的注册配置文件

当您的 XenMobile 部署包括专用设备时，单个 XenMobile 管理员或一小组管理员将注册多个专用设备。要确保这些管理员能够注册所需的所有设备，请为其创建一个允许每个用户无限制注册设备的注册配置文件。

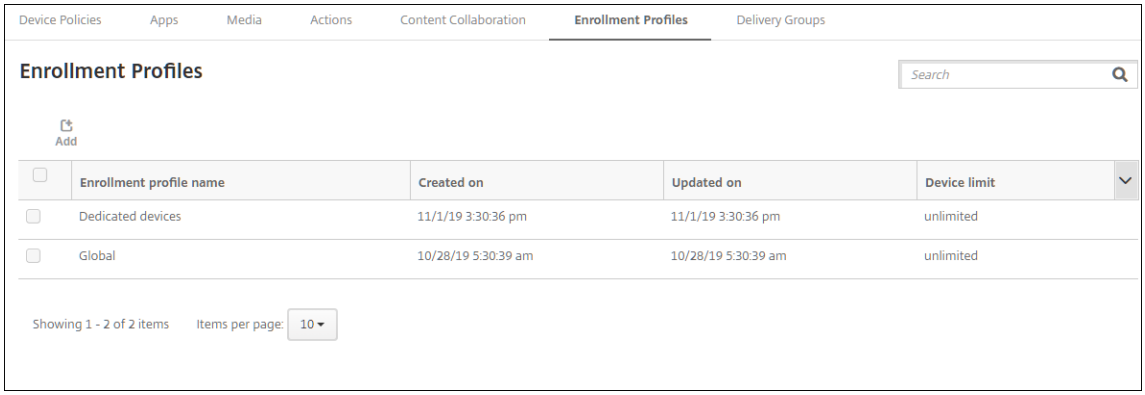
1. 在 XenMobile 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。请确保使用此配置文件可以注册的设备数量设置为无限制。
3. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。
4. 将管理设置为 **Android Enterprise**。
5. 将设备所有者模式设置为专用设备。



6. **BYOD** 工作配置文件允许您配置注册配置文件以将 BYOD 设备注册为工作配置文件设备。将新设备和重置为出厂设置的设备注册为专用设备。将 **BYOD** 工作配置文件设置为开，以允许将 BYOD 设备注册为工作配置文件设备。将 **BYOD** 工作配置文件设置为关，以限制对公司拥有的设备的注册。默认值为开。
7. 选择是否在 Citrix MAM 中注册设备。
8. 如果将 **BYOD** 工作配置文件设置为开，请配置用户同意书。要允许 BYOD 工作配置文件设备的用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。

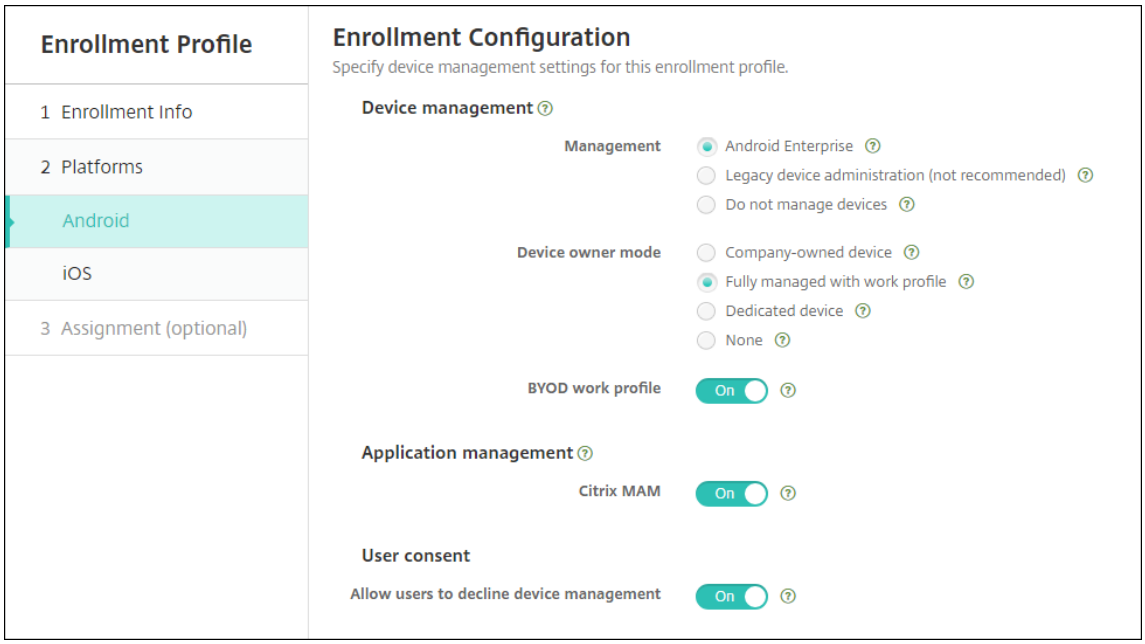
   如果 **BYOD** 工作配置文件设置为开，则允许用户拒绝设备管理的默认值为开。如果 **BYOD** 工作配置文件设置为关，则禁用允许用户拒绝设备管理。
9. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
10. 请选择包含注册专用设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

    显示的“注册配置文件”页面中添加了您的配置文件。



为使用工作配置文件的完全托管设备添加注册配置文件

1. 在 XenMobile 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置使用此配置文件的成员可以注册的设备数量。
4. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。
5. 将管理设置为 **Android Enterprise**。将设备所有者模式设置为通过工作配置文件完全托管。



6. **BYOD** 工作配置文件允许您配置注册配置文件以将 BYOD 设备注册为工作配置文件设备。新设备和重置为出厂设备的设备注册为使用工作配置文件的完全托管设备。将 **BYOD** 工作配置文件设置为开，以允许将 BYOD 设备注册为工作配置文件设备。将 **BYOD** 工作配置文件设置为关，以限制对专用设备的注册。默认值为关。
7. 选择是否在 Citrix MAM 中注册设备。

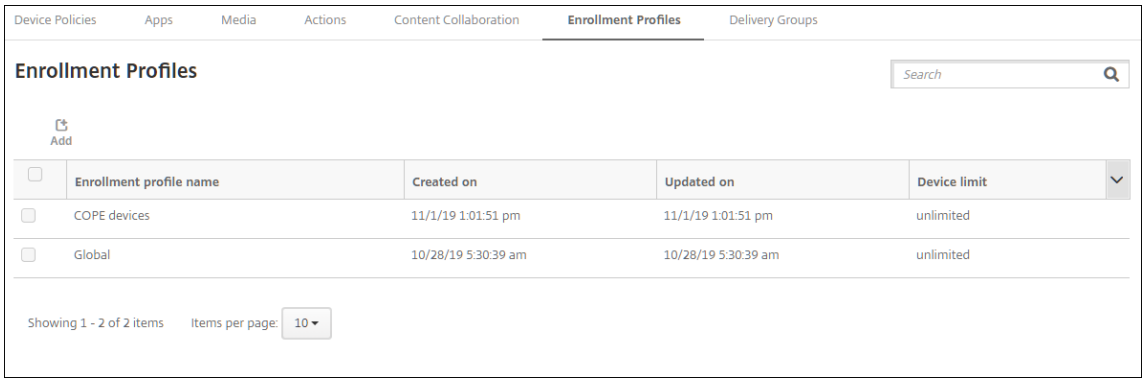
8. 如果将 **BYOD** 工作配置文件设置为开，请配置用户同意书。要允许 BYOD 工作配置文件设备的用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。

   如果 **BYOD** 工作配置文件设置为开，则允许用户拒绝设备管理的默认值为开。如果 **BYOD** 工作配置文件设置为关，则禁用允许用户拒绝设备管理。

9. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。

10. 请选择包含注册使用工作配置文件的完全托管设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

    显示的“注册配置文件”页面中添加了您的配置文件。



为旧版设备添加注册配置文件

Google 将逐步弃用设备管理的设备管理员模式。Google 鼓励客户在设备所有者模式或配置文件所有者模式下管理所有 Android 设备。【请参阅 Google Android Enterprise 开发人员指南中的 Device admin deprecation（设备管理员弃用）。】

要支持此更改，请执行以下操作：

- Citrix 将 Android Enterprise 设置为 Android 设备的默认注册选项。
- 如果为您的 XenMobile 部署启用了 Android Enterprise，则所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。

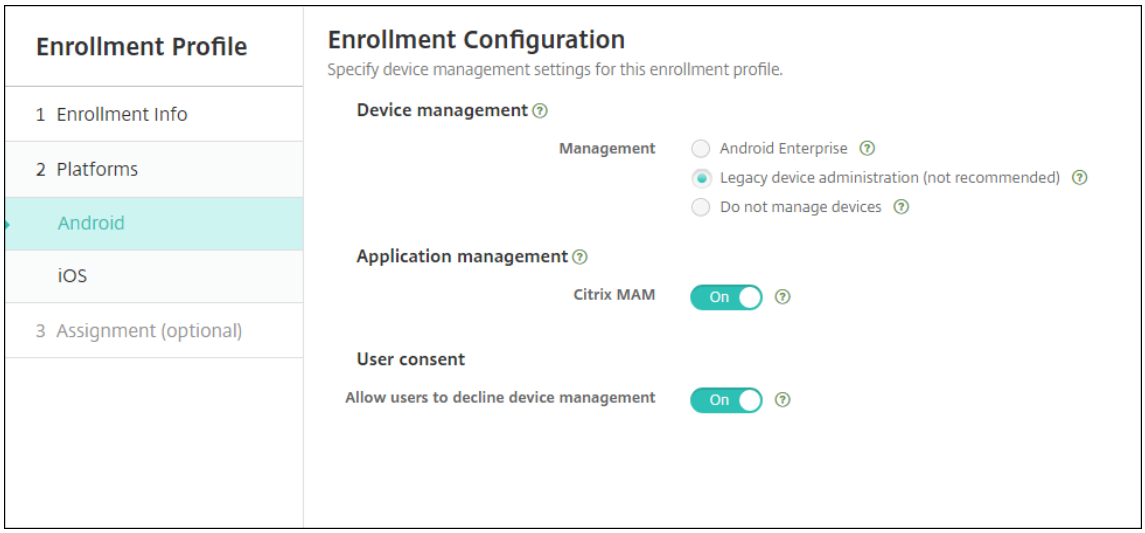
贵组织可能尚未准备好开始使用 Android Enterprise 管理旧版 Android 设备。在这种情况下，您可以继续在设备管理员模式下进行管理。对于已在设备管理员模式下注册的设备，XenMobile 将继续以设备管理员模式管理这些设备。

为旧版设备创建注册配置文件，以允许新 Android 设备注册使用设备管理员模式。

要为旧版设备创建注册配置文件：

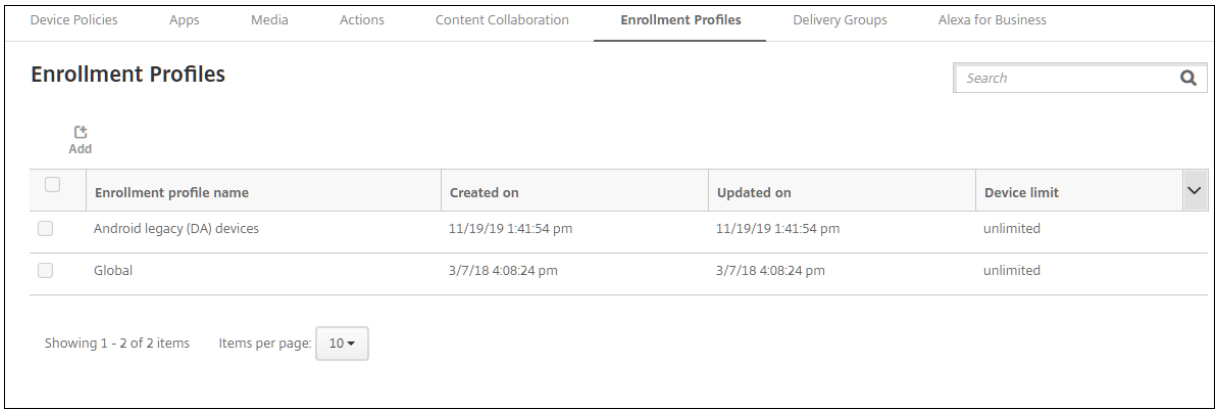
1. 在 XenMobile 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置使用此配置文件的成员可以注册的设备数量。
4. 在平台下选择 **Android**，或者单击下一步。此时将显示“注册配置”页面。

5. 将管理设置为旧版设备管理 **(**不推荐**)**。单击 **Next**（下一步）。



6. 选择是否在 Citrix MAM 中注册设备。
7. 要允许用户在注册其设备时拒绝设备管理，请将允许用户拒绝设备管理设置为开。默认值为开。
8. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
9. 请选择包含注册专用设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

显示的“注册配置文件”页面中添加了您的配置文件。



要在设备管理员模式下继续管理旧版设备，请使用此配置文件注册或重新注册这些设备。可以通过让用户下载 Secure Hub 并提供注册服务器 URL 来注册与工作配置文件设备类似的设备管理员设备。

预配 **Android Enterprise** 工作配置文件设备

Android Enterprise 工作配置文件设备在配置文件所有者模式下注册。这些设备不需要是新设备或恢复出厂设置的设备。BYOD 设备作为工作配置文件设备注册。注册体验与 XenMobile 中的 Android 注册体验相似。用户将从 Google Play 下载 Secure Hub 并注册其设备。

默认情况下，如果某个设备在 Android Enterprise 中注册为工作配置文件设备，**USB** 调试和未知来源设置在该设备上将处于禁用状态。

在 Android Enterprise 中将设备注册为工作配置文件设备时，将始终转至 Google Play。在该应用商店中，允许 Secure Hub 在用户的个人配置文件中显示。

预配 **Android Enterprise** 完全托管设备

可以在前面的部分中设置的部署中注册完全托管设备。完全托管设备是公司拥有的设备，在设备所有者模式下注册。在设备所有者模式下，只能注册新设备或恢复出厂设置的设备。

可以使用以下任何注册方法在设备所有者模式下注册设备：

- **DPC** 标识符令牌：如果使用此注册方法，用户在设置设备时将输入字符`afw##xenmobile`。`afw##xenmobile` 为 Citrix DPC 标识符令牌。此令牌将设备标识为由 XenMobile 托管并从 Google Play 应用商店下载 Secure Hub。请参阅使用 Citrix DPC 标识符令牌注册设备。
- 近场通信 **(NFC)** 碰撞： NFC 碰撞注册方法通过在两个设备之间使用近场通信来传输数据。蓝牙、Wi-Fi 和其他通信模式在新设备或恢复出厂设置的设备上处于禁用状态。NFC 是此状态下设备可以使用的唯一通信协议。请参阅通过 NFC 碰撞注册设备。
- **QR** 代码： QR 代码注册可用于注册不支持 NFC 的分布式设备队列（例如平板电脑）。QR 代码注册方法通过扫描设置向导中的 QR 代码来设置并配置设备配置文件模式。请参阅使用 QR 代码注册设备。
- 零触摸：零触摸注册允许您将设备配置为在首次打开电源时自动注册。某些运行 Android 8.0 或更高版本的 Android 设备支持零触摸注册。请参阅零接触注册。
- **Google** 帐户：用户输入其 Google 帐户凭据以启动预配过程。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

用户在打开新设备或恢复出厂重置的设备以进行初始设置后输入 Google 帐户时输入 `afw##xenmobile`。此操作将下载并安装 Secure Hub。用户随后将按照 Secure Hub 设置提示进行操作，完成注册过程。

对于大多数客户，建议使用此注册方法，因为是从 Google Play 应用商店下载最新版本的 Secure Hub。与其他注册方法不同，您不用提供要从 XenMobile Server 下载的 Secure Hub。

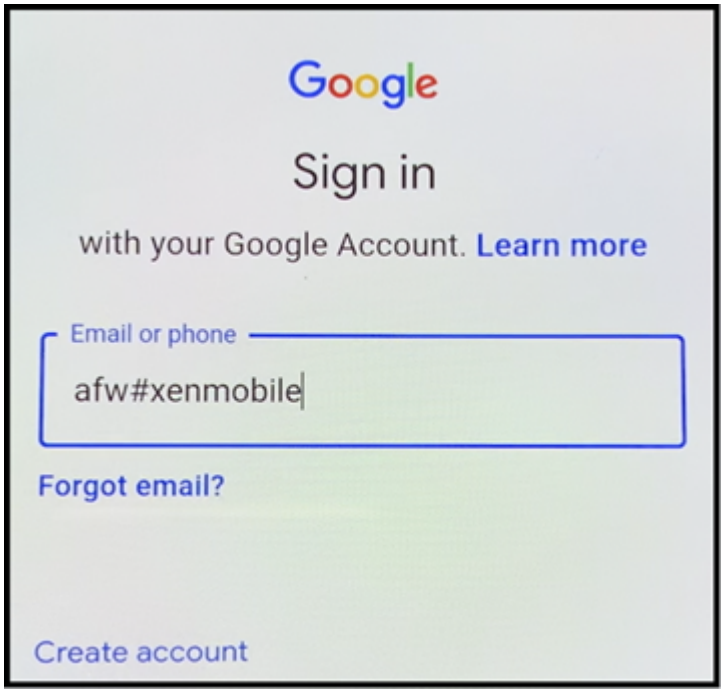
系统要求

- 在运行 Android OS 的所有 Android 设备上均受支持。

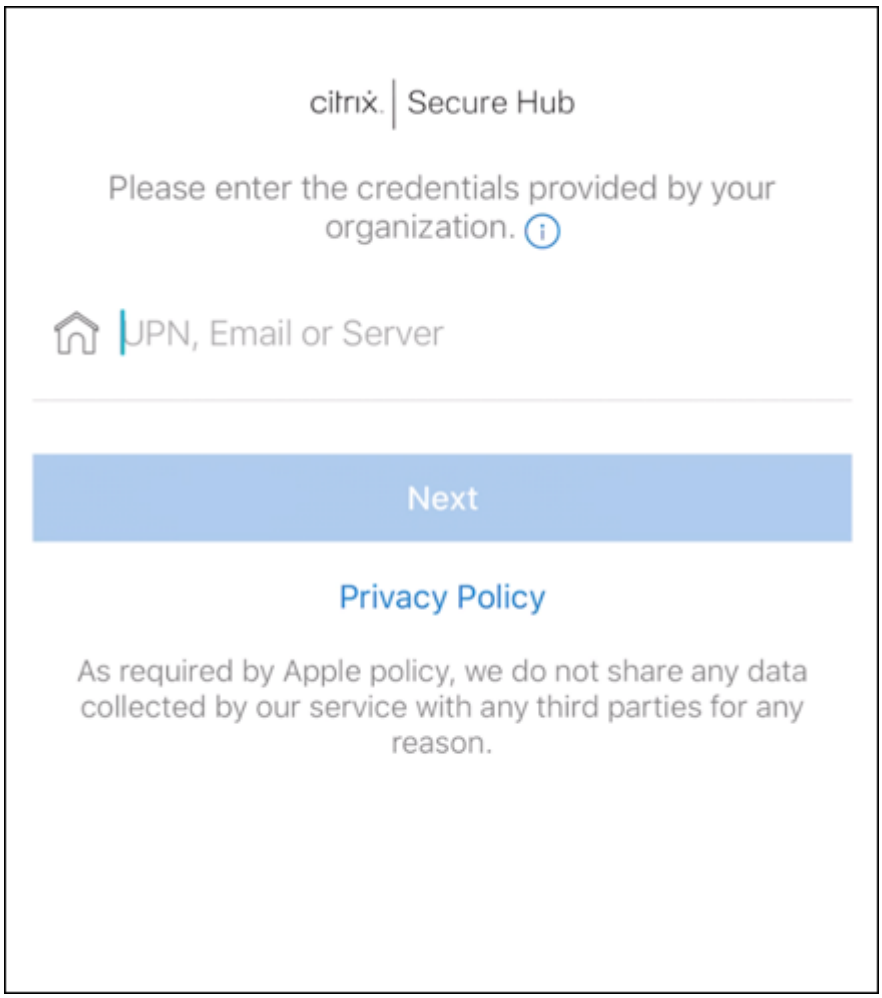
注册设备

1. 打开新设备或恢复出厂设置的设备的电源。
2. 初始设备设置加载并提示您输入 Google 帐户。如果设备加载设备的主屏幕，请检查通知栏中是否显示完成设置通知。

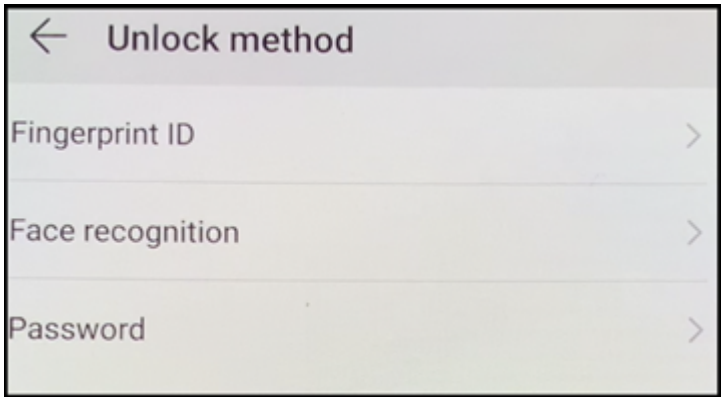
3. 在电子邮件或电话字段中输入 `afw##xenmobile`。



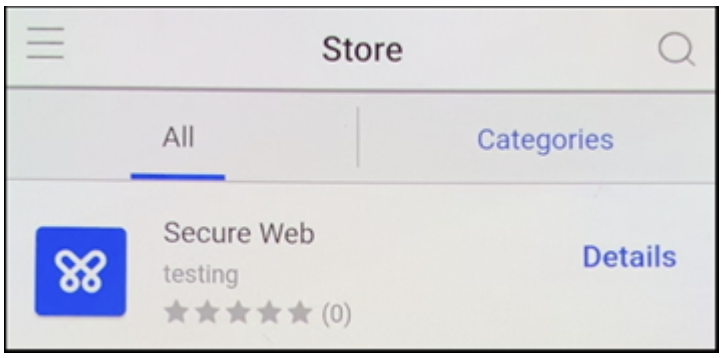
4. 在 Android Enterprise 屏幕上轻按安装，提示安装 Secure Hub。
5. 在 Secure Hub 安装程序屏幕上轻按安装。
6. 对所有应用程序权限申请轻按允许。
7. 轻按接受并继续以安装 Secure Hub 并允许其管理设备。
8. Secure Hub 现在已安装，并位于默认注册屏幕上。在此示例中，未设置自动发现。如果是，用户可以输入其用户名/电子邮件，并为其找到一个服务器。相反，请输入环境的注册 URL，然后轻按下一步。



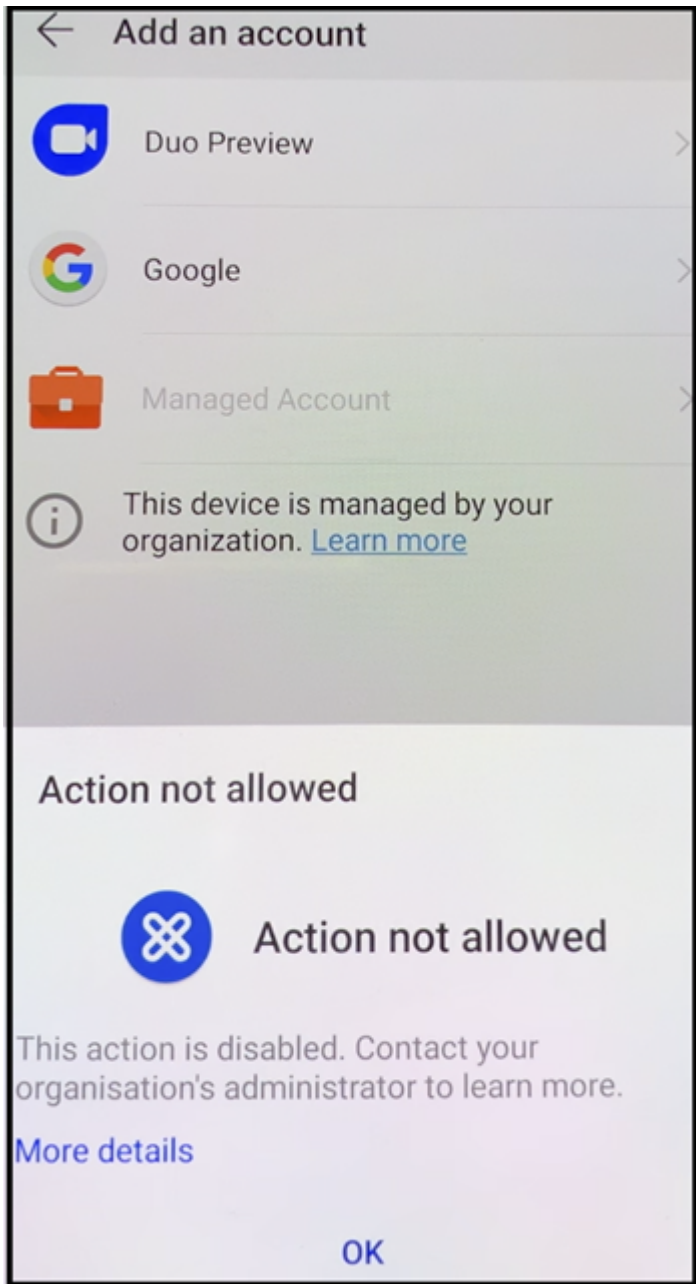
9. XenMobile 的默认配置允许用于选择其使用 MAM 还是 MDM+MAM。如果以这种方式提示，请轻按是，注册以选择 MDM+MAM。
10. 输入用户名和密码，然后轻按下一步。
11. 系统将提示用户配置设备通行码。轻按设置并输入通行码。
12. 系统会提示用户配置工作配置文件解锁方法。在此示例中，轻按密码，轻按 **PIN**，然后输入 PIN。



13. 设备现在位于 Secure Hub 我的应用程序登录屏幕上。轻按从应用商店中添加应用程序。
14. 要添加 Secure Web，请轻按 **Secure Web**。



15. 轻按添加。
16. Secure Hub 引导用户访问 Google Play 应用商店以安装 Secure Web。轻按安装。
17. 安装 Secure Web 后，轻按打开。在地址栏中输入来自内部站点的 URL，并验证页面是否加载。
18. 转到设备上的设置 **>** 帐户。注意无法修改托管帐户。用于共享屏幕或远程调试的开发人员选项也被阻止。



通过 **NFC** 碰撞注册设备

要使用 NFC 碰撞功能将设备注册为完全托管设备，需要两个设备：一个已恢复出厂设置的设备，以及一个运行 XenMobile Provisioning Tool 的设备。

系统要求和必备条件

- 支持的 Android 设备。

- 新的或恢复出厂设置的设备，为 Android Enterprise 预配为完全托管设备。可以在本文中查找完成此必备条件的步骤。
- 另一个设备具有 NFC 功能，运行已配置的 Provisioning Tool。Provisioning Tool 在 Secure Hub 或 Citrix 下载页面上提供。

每个设备只能有一个 Android Enterprise 配置文件，即托管 Secure Hub。每台设备上只允许一个配置文件。尝试添加第二个 DPC 应用程序将删除已安装的 Secure Hub。

通过 **NFC** 碰撞传输数据

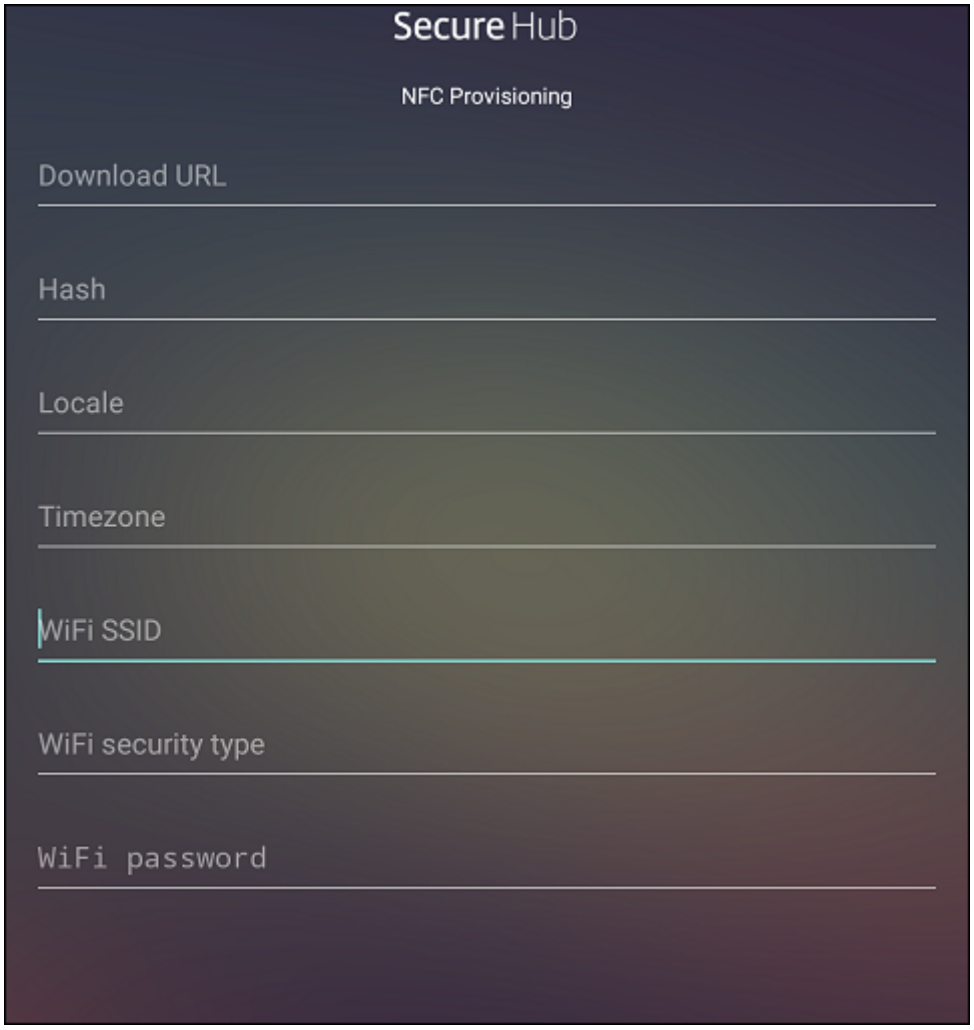
预配恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以初始化 Android Enterprise：

- 要作为设备所有者（在此示例中为 Secure Hub）的 DPC 应用程序的包名称。
- 设备可以从中下载 DPC 应用程序的 Intranet/Internet 位置。
- 用于验证下载是否成功的 DPC 应用程序的 SHA1 哈希。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备能够连接和下载 DPC 应用程序。注意：Android 现在不支持在此步骤中使用 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

碰撞两个设备时，来自 Provisioning Tool 的数据将发送到恢复出厂设置的设备。该数据随后用于下载使用管理员设置的 Secure Hub。如果未输入时区和位置值，Android 将在新设备上自动配置值。

配置 **XenMobile Provisioning Tool**

执行 NFC 碰撞之前，必须配置 Provisioning Tool。此配置随后在 NFC 碰撞过程中被传输到恢复出厂设置的设备。



可以将数据键入到必填字段中，或者使用文本文件进行填充。下一个过程中的步骤介绍了如何配置文本文件，并且包含每个字段的说明。键入后，该应用程序将不保存信息，因此，您可能希望创建一个文本文件以保留该信息供将来使用。

使用文本文件配置 **Provisioning Tool**

将文件命名为 nfcprovisioning.txt 并将其放置在设备的 SD 卡中的 /sdcard/ 文件夹下。该应用程序随后可以读取文本文件并填充值。

文本文件必须包含以下数据：

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>

此行为 EMM 提供程序应用程序的 Intranet/Internet 位置。恢复出厂设置的设备在进行 NFC 碰撞后连接到 Wi-Fi 之后，该设备必须有权访问此位置才能进行下载。该 URL 为常规 URL，不需要特殊格式。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>

此行是 EMM 提供程序应用程序的校验和。此校验和用于验证下载是否成功。本文中后面的内容介绍了获取校验和的步骤。

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

此行是运行 Provisioning Tool 的设备的已连接 Wi-Fi SSID。

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

支持的值为 WEP 和 WPA2。如果 Wi-Fi 未受保护，此字段必须留空。

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

如果 Wi-Fi 未受保护，此字段必须留空。

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

输入语言和国家/地区代码。语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请键入 en_US 表示在美国所讲的英语。如果未输入任何代码，则会自动填充国家/地区和语言。

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

设备运行时所在的时区。请键入区域/位置形式的 Olson 名称。例如，America/Los_Angeles 表示太平洋时间。如果未输入名称，则将自动填充时区。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

不需要此数据，因为值 Secure Hub 被硬编码到应用程序中。在本文中提及的目的只是为了保持完整性。

如果存在通过使用 WPA2 保护的 Wi-Fi，完整的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

如果存在不受保护的 Wi-Fi，完整的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d
```



```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

获取 **Citrix Secure Hub** 的校验和

Secure Hub 的校验和是一个常数值：qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM。要下载适用于 Secure Hub 的 APK 文件，请使用以下 Google Play 应用商店链接：https://play.google.com/managed/downloadManagingApp?identifier=xenmobile。

获取应用程序校验和

必备条件：

- 来自 Android SDK Build Tools 的 **apksigner** 工具
- OpenSSL 命令行

要获取任何应用程序的校验和，请按照下列步骤进行操作：

1. 从 Google Play 应用商店下载应用程序的 APK 文件。
2. 在 OpenSSL 命令行中，导航到 **apksigner** 工具：android-sdk/build-tools/<version>/apksigner 并键入以下内容：

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

   该命令返回有效的校验和。

3. 要生成 QR 码，请在 PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM 字段中输入校验和。例如：

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
```



```
7
8         "serverURL": "https://supportablility.xm.cloud.com"
9       }
10
11    }
12
13  <!--NeedCopy-->
```

使用的库

Provisioning Tool 在其源代码中使用以下库：

- Google 遵循 Apache License 2.0 提供的 v7 `appcompat` 库、Design Support Library 以及 v7 Palette 库

  有关信息，请参阅 Support Library Features Guide（支持库功能指南）。

- Jake Wharton 遵循 Apache License 2.0 提供的 Butter Knife

使用 **QR** 代码注册设备

要使用 QR 代码注册完全托管设备，请通过创建一个 JSON 并将该 JSON 转换为 QR 代码来生成 QR 代码。将使用设备相机扫描 QR 代码以注册设备。

系统要求

- 在运行 Android 8.0 及更高版本的所有 Android 设备上均受支持。

从 **JSON** 创建 **QR** 代码

创建包含以下字段的 JSON。

以下字段均为必填项：

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

值：com.zenprise/com.zenprise.configuration.AdminFunction

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

值：qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

值：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

以下字段为选填字段：

- **android.app.extra.PROVISIONING_LOCALE**：输入语言和国家/地区代码。

  语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请输入 en_US 表示在美国所讲的英语。

- **android.app.extra.PROVISIONING_TIME_ZONE**：设备运行时所在的时区。

  请键入区域/位置形式的 Olson 名称。例如，America/Los_Angeles 表示太平洋时间。如果未输入，则将自动填充时区。

- **android.app.extra.PROVISIONING_LOCAL_TIME**：从 Epoch 开始经过的时间（毫秒）。

  Unix epoch（或 Unix 时间、POSIX 时间或 Unix 时间戳）是指从 1970 年 1 月 1 日（午夜，UTC/GMT）开始经过的秒数。该时间不包括闰秒（在 ISO 8601 中为：1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION**：设置为 **true** 将在配置文件创建期间跳过加密。设置为 **false** 将在配置文件创建期间强制加密。

典型的 JSON 如下：

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "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
}
```

使用任意 JSON 验证工具（例如 https://jsonlint.com）验证创建的 JSON。然后使用任意联机 QR 代码生成器（例如 https://www.qr-code-generator.com）将该 JSON 字符串转换为 QR 代码。

恢复出厂设置的设备将扫描此 QR 代码以将设备注册为完全托管设备。

注册设备

打开新设备或恢复出厂设置的设备的电源后：

1. 在欢迎屏幕上轻按该屏幕六次以启动 QR 代码注册流程。
2. 系统提示时，连接到 Wi-Fi。QR 代码（JSON 编码）中 Secure Hub 的下载位置可以通过此 Wi-Fi 网络访问。

   设备成功连接到 Wi-Fi 后，将从 Google 下载一个 QR 代码读取器并启动摄像头。

3. 将摄像头对准 QR 代码以扫描该代码。

   Android 将从 QR 代码中的下载位置下载 Secure Hub，验证签名证书的签名，安装 Secure Hub 并将其设置为设备所有者。

有关详细信息，请参阅此面向 Android EMM 开发人员的 Google 指南：https://developers.google.com/android/work/prov-devices#qr_code_method。

零接触注册

零触摸注册允许您将设备设置为首次打开电源时将自身预配为完全托管设备。

您的设备经销商在 Android 零触摸门户网站上为您创建一个帐户，这是一个可让您将配置应用到设备的联机工具。使用 Android 零触摸门户，您可以创建一个或多个零触摸注册配置，并将这些配置应用到分配给您的帐户的设备。当用户为这些设备打开电源时，这些设备将自动注册到 XenMobile 中。分配给设备的配置定义了其自动注册过程。

系统要求

- 对零触摸注册的支持自 Android 8.0 开始。

您的经销商提供的设备和帐户信息

- 符合零触摸注册条件的设备可从企业经销商或 Google 合作伙伴处购买。有关 Android Enterprise 零触摸合作伙伴的列表，请参阅 Android website（Android Web 站点）。
- 由您的经销商创建的 Android Enterprise 零触摸门户帐户。
- Android Enterprise 零触摸门户帐户登录信息，由您的经销商提供。

创建零触摸配置

创建零触摸配置时，请包含一个自定义 JSON 以指定配置的详细信息。

使用此 JSON 可配置要在指定的 XenMobile Server 上注册的设备。在此示例中，将服务器的 URL 替换为 “URL”。

```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL",
7            }
8
9         }
10
11 <!--NeedCopy-->
```

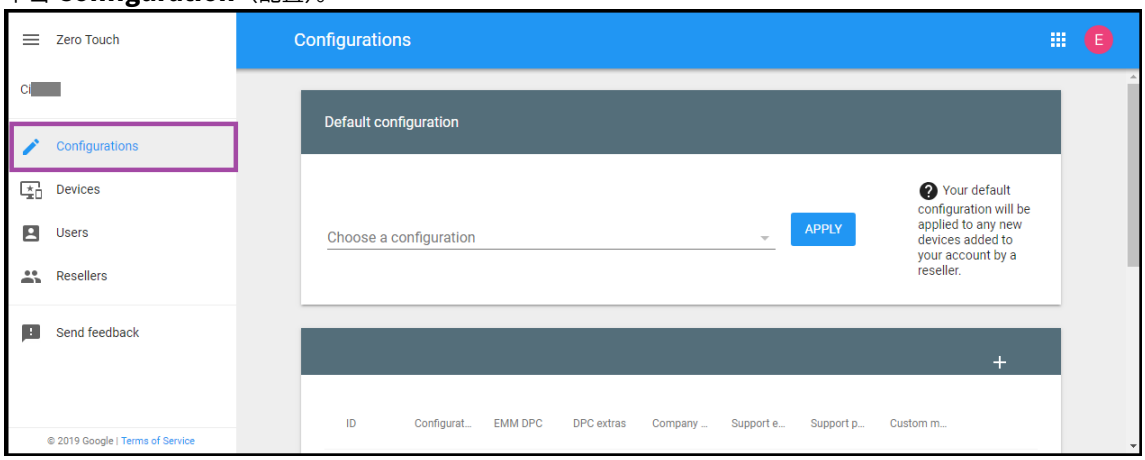
可以使用具有更多参数的可选 JSON 来进一步自定义您的配置。此示例指定 XenMobile Server 以及使用此配置的设备用于登录服务器的用户名和密码。

```
1       {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4            {
```

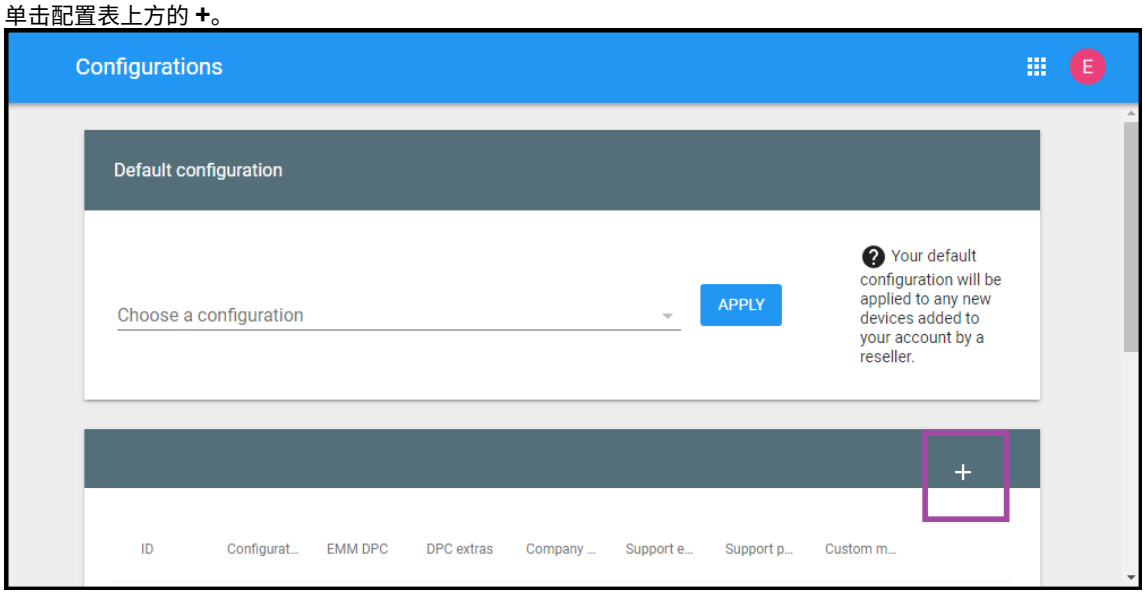


```
5
6                "serverURL":"URL",
7                "xm_username":"username",
8                "xm_password":"password"
9             }
10
11              }
12
13    <!--NeedCopy-->
```

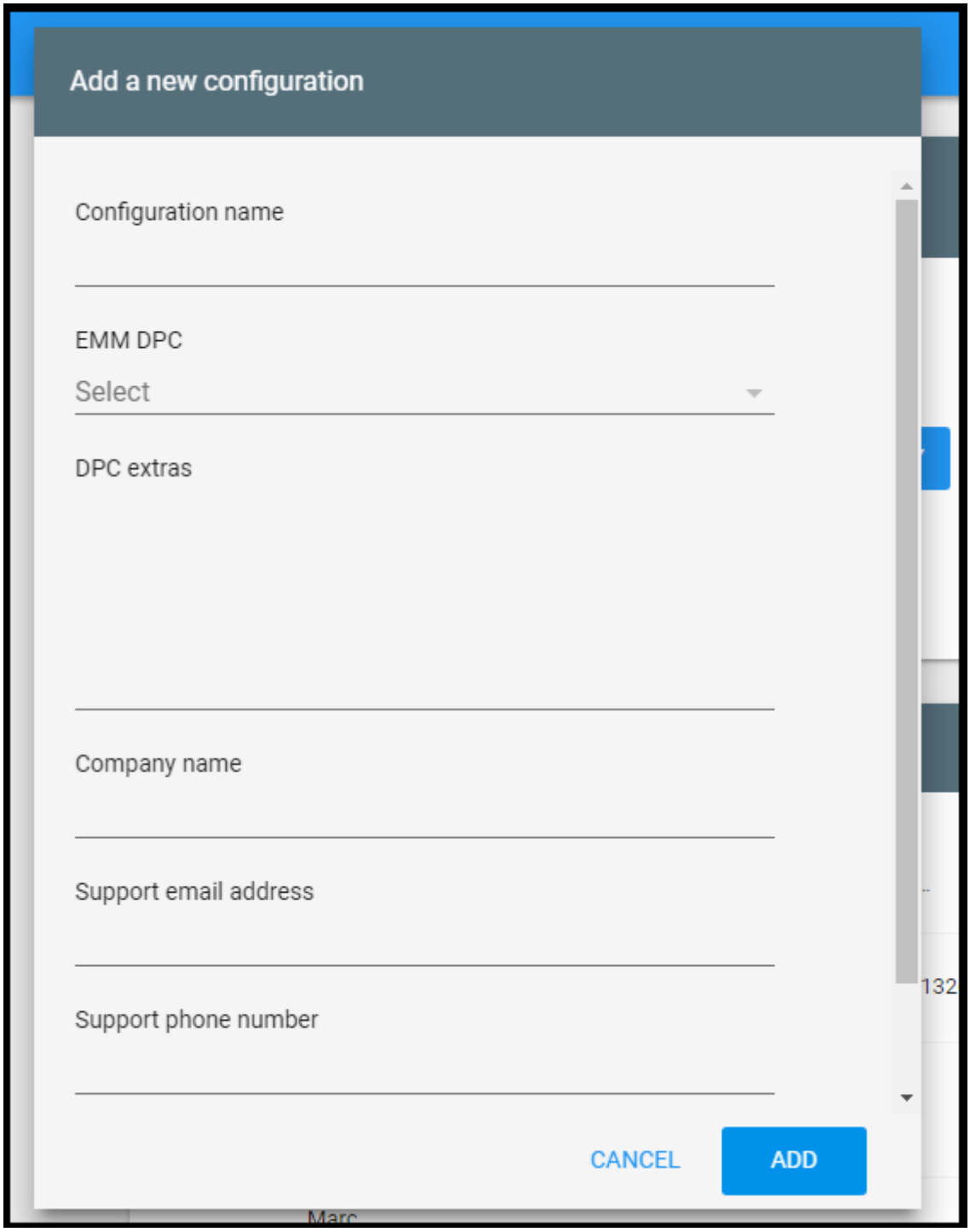
1. 转至 Android 零触摸门户，网址为 https://partner.android.com/zerotouch。使用您的零触摸设备经销商提供的帐户信息登录。
2. 单击 **Configuration**（配置）。



3. 单击配置表上方的 **+**。



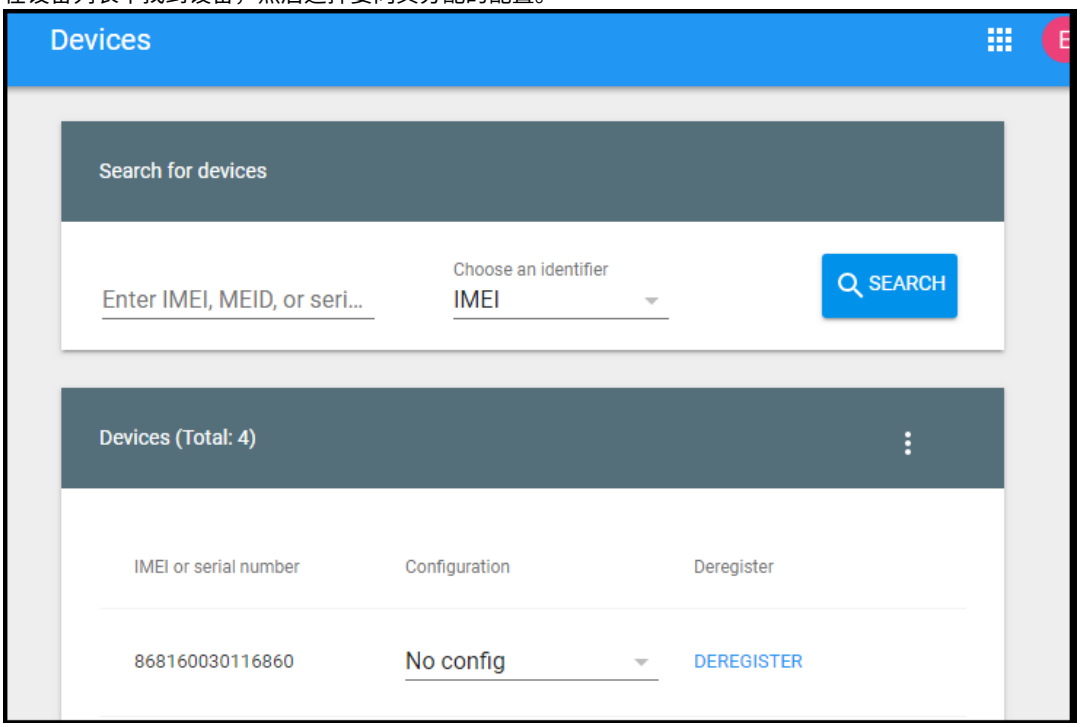
4. 在显示的配置窗口中输入您的配置信息。



- 配置名称：键入您为此配置选择的名称。
- **EMM DPC**：选择 **Citrix Secure Hub**。
- **DPC** 附加程序：在此字段中粘贴您的自定义 JSON 文本。
- 公司名称：键入您希望在设备预配过程中在 Android Enterprise 零触摸设备上显示的名称。
- 支持电子邮件地址：键入用户可以联系以寻求帮助的电子邮件地址。此地址会在设备预配之前显示在 Android Enterprise 零触摸设备上。

- 支持电话号码：键入您的用户可以联系以寻求帮助的电话号码。设备预配之前，此电话号码会显示在 Android Enterprise 零触摸设备上。
- 自定义消息：（可选）添加一个或两个句子，以帮助您的用户与您联系，或者为其提供有关其设备发生的情况的更多详细信息。此自定义消息会在设备预配之前显示在 Android Enterprise 零触摸设备上。

5. 单击添加。
6. 要创建更多配置，请重复步骤 2 到 4。
7. 要将配置应用到设备，请执行以下操作：
   a) 在 Android 零触摸门户中，单击设备。
   b) 在设备列表中找到设备，然后选择要向其分配的配置。



   c) 单击更新。

可以使用 CSV 文件将配置应用到许多设备。

有关如何将配置应用到许多设备的信息，请参阅 Android Enterprise 帮助主题 Zero-touch enrollment for IT admins（面向 IT 管理员的零触摸注册）。此 Android Enterprise 帮助主题包含有关如何管理配置并将其应用到设备的详细信息。

预配专用 **Android Enterprise** 设备

专用 Android Enterprise 设备属于完全托管设备，专门用于满足单个用例。专用设备又称为公司拥有、单一用途 (COSU) 的设备。您将这些设备限制为执行此用例需要执行的任务所需的一个应用程序或一小组应用程序。您还将阻止用户启用其他应用程序或在设备上执行其他操作。

使用用于其他完全托管设备的任何注册方法注册专用设备，如预配 Android Enterprise 完全托管设备。预配专用设备需要在注册之前进行更多设置。

要预配专用设备，请执行以下操作：

- 为允许在您的 XenMobile 部署中注册专用设备的 XenMobile 管理员创建注册配置文件。请参阅创建注册配置文件。
- 允许运行希望专用设备访问的应用程序。
- 或者，将允许运行的应用程序设置为允许锁定任务模式。当某个应用程序处于锁定任务模式时，用户打开时该应用程序将固定到设备屏幕。此时将不显示任何主页按钮，并且返回按钮处于禁用状态。用户使用编程到该应用程序中的一项操作退出该应用程序，例如注销。
- 在您添加的注册配置文件中注册每个设备。

系统要求

- 对注册专用设备的支持自 Android 6.0 起启用。

允许运行应用程序并设置锁定任务模式

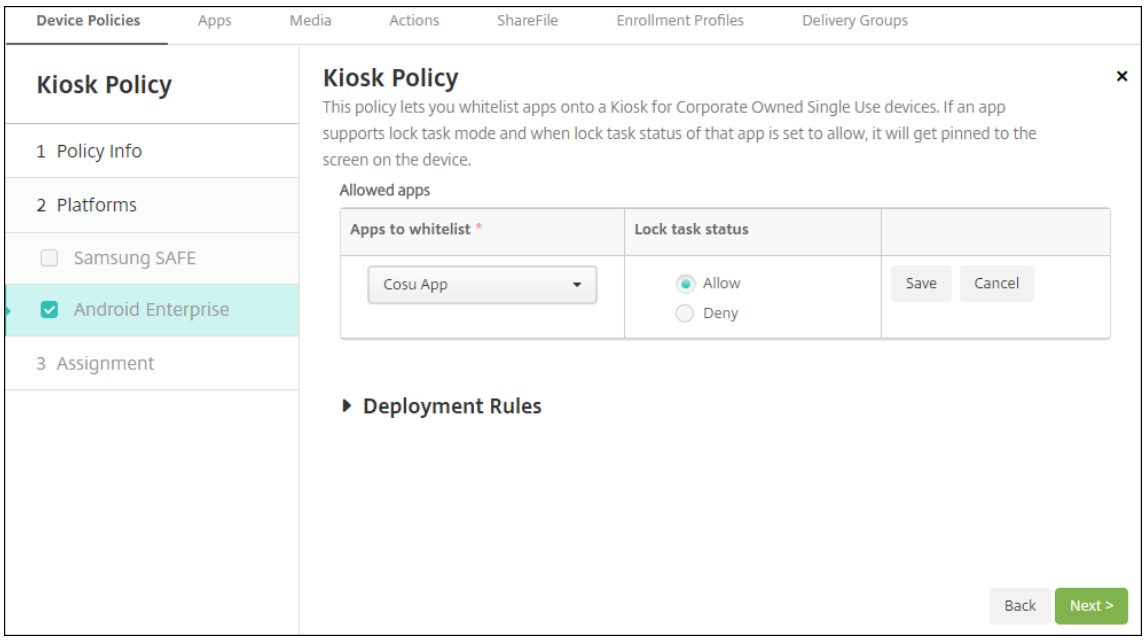
展台设备策略允许您允许运行应用程序以及设置锁定任务模式。默认情况下，允许运行 Secure Hub 和 Google Play 服务。

要添加展台策略，请执行以下操作：

1. 在 XenMobile 控制台中，单击配置 **>** 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在“安全性”下，单击展台。此时将显示展台策略页面。
4. 在“平台”下，选择 **Android Enterprise**。清除其他平台。
5. 在“策略信息”窗格中，键入策略名称和可选说明。
6. 单击下一步，然后单击添加。
7. 要允许运行某个应用程序并允许或拒绝该应用程序的锁定任务模式，请执行以下操作：

   从列表中选择要允许运行的应用程序。

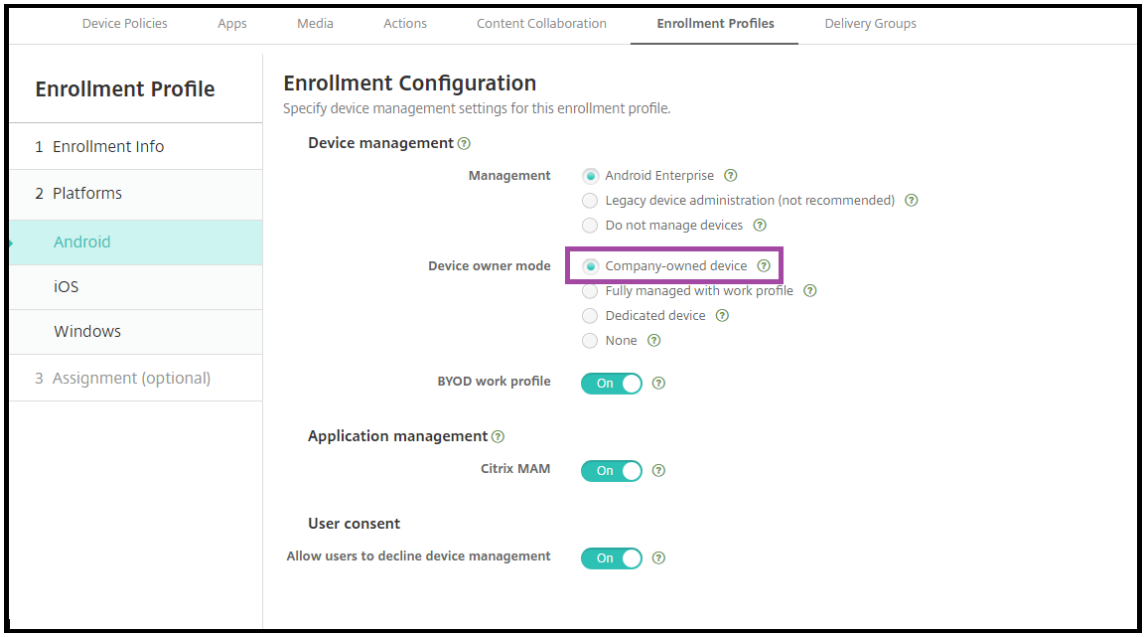
   选择允许可设置要在用户启动应用程序时固定到设备屏幕的应用程序。选择拒绝可设置不固定的应用程序。默认设置为允许。



8. 单击保存。
9. 要允许运行另一个应用程序并允许或拒绝该应用程序的锁定任务模式，请单击添加。
10. 配置部署规则并选择交付组。有关详细信息，请参阅设备策略。

注册设备

1. 单击下一步或在平台下选择 **Android** 。此时将显示“注册配置”页面。
2. 将管理设置为 **Android Enterprise**。
3. 将设备所有者模式设置为公司拥有的设备。



4. 选择分配 **(**选项**)**。此时将显示交付组分配屏幕。
5. 请选择包含注册专用设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

如果在注册配置文件中启用了 **BYOD** 工作配置文件，则非新设备或重置为出厂设置的设备将注册为工作配置文件设备。请参阅预配 Android Enterprise 工作配置文件设备。

使用工作配置文件预配 **Android Enterprise** 完全托管设备（**COPE** 设备）

使用工作配置文件的完全托管设备（以前称为 COPE 设备）是公司拥有的设备，既用于工作目的，也用于个人目的。贵组织负责管理整个设备。可以将一组策略应用到设备，另一组策略应用到工作配置文件。

在 XenMobile 控制台中，具有工作配置文件的完全托管设备将显示以下术语：

- 设备所有权为“企业”。
- 设备 Android Enterprise 安装类型为“企业所有者但由个人使用”。

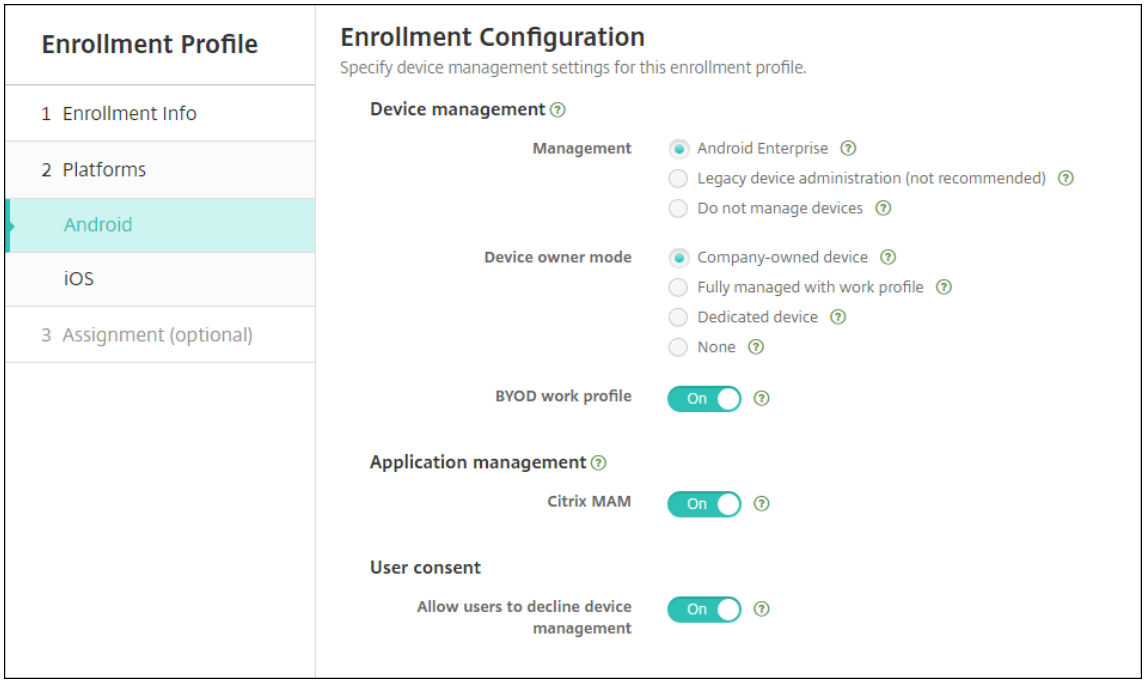
系统要求

- 从 Android 8.0 到 Android 10.x 开始，支持注册具有工作配置文件的完全托管设备。

为具有工作配置文件的完全托管设备添加注册配置文件

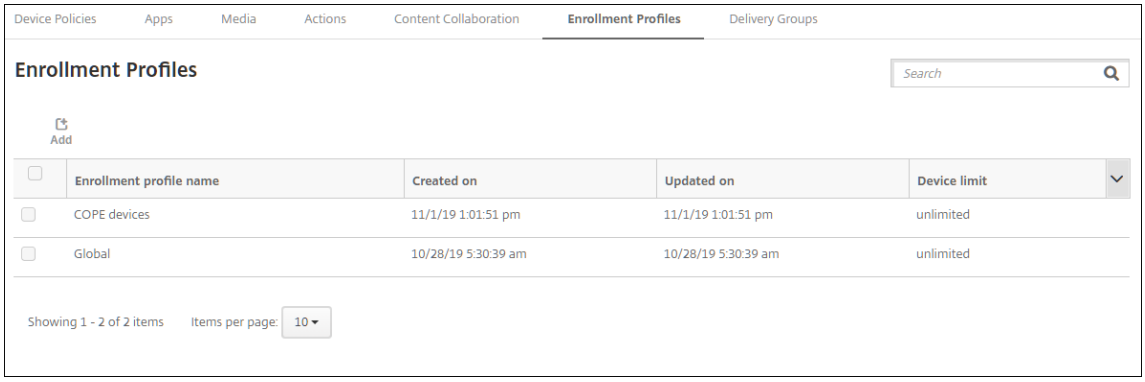
为注册具有工作配置文件的完全托管设备创建注册配置文件。分配给此注册配置文件的交付组中的管理员可以注册具有工作配置文件的完全托管设备。要确保这些管理员能够注册所需的所有设备，请为其创建一个允许每个用户无限制注册设备的注册配置文件。将此配置文件分配给包含注册具有工作配置文件的完全托管设备的管理员的交付组。

1. 在 XenMobile 控制台中，转到配置 **>** 注册配置文件。
2. 要添加注册配置文件，请单击添加。在“注册信息”页面中，键入注册配置文件的名称。请确保使用此配置文件可以注册的设备数量设置为无限制。
3. 单击下一步或在平台下选择 **Android Enterprise**。此时将显示“注册配置”页面。
4. 将注册类型设置为以下选项之一：
    - 完全托管**/**工作配置文件：新设备或重置为出厂设置的设备注册完全托管。BYOD 设备仅使用您管理的工作配置文件进行注册。
    - **COPE/**工作配置文件：新设备或重置为出厂设置的设备注册具有工作配置文件的完全托管设备。BYOD 设备仅使用您管理的工作配置文件进行注册。



5. 选择分配 **(**可选**)** 或单击下一步。此时将显示交付组分配屏幕。
6. 请选择包含注册专用设备的管理员的一个或多个交付组。然后单击 **Save**（保存）。

   显示的“注册配置文件”页面中添加了您的配置文件。



如果用户属于具有不同注册配置文件的多个交付组，该交付组的名称决定使用的注册配置文件。XenMobile 选择按字母顺序排列的交付组列表中最后显示的交付组。

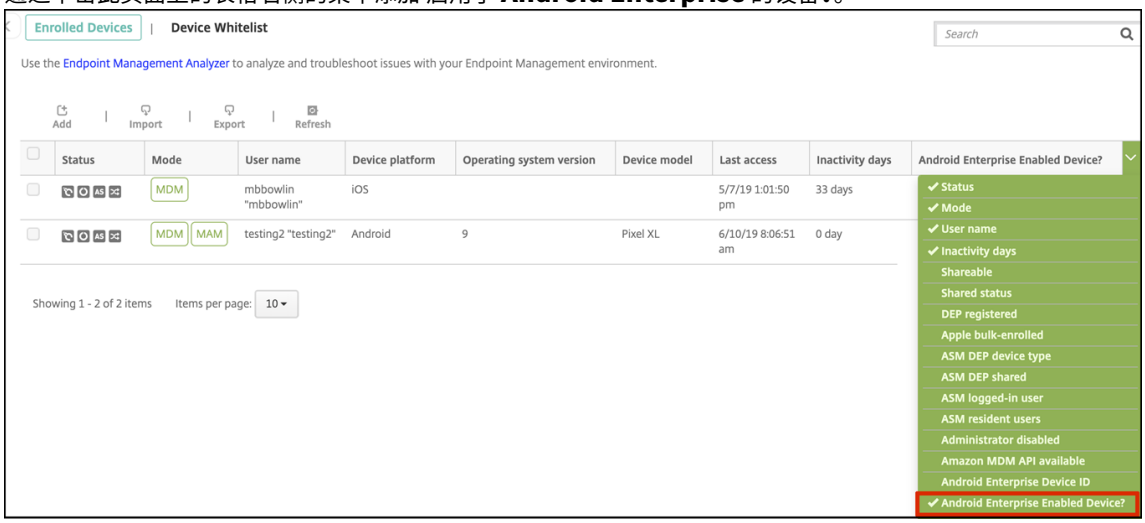
注册设备

新设备和重置为出厂设置的设备使用 DPC 标识符令牌、近场通信 (NFC) 碰撞或 QC 代码方法注册为具有工作配置文件的完全托管设备。请参阅使用 Citrix DPC 标识符令牌注册设备、通过 NFC 碰撞注册设备或使用 QR 代码注册设备。

非新设备或重置为出厂设置的设备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 **XenMobile** 控制台中查看 **Android Enterprise** 设备

1. 在 XenMobile 控制台中，转至管理 **>** 设备。
2. 通过单击此页面上的表格右侧的菜单添加 启用了 **Android Enterprise** 的设备**?**。



3. 要查看可用的安全操作，请选择完全托管设备，然后单击安全。设备完全托管时，完全擦除操作可用，但选择性擦除不可用。该差别是因为设备仅允许来自托管 Google Play 应用商店的应用程序。用户没有从公共应用商店安装应用程序的选项。贵组织负责管理设备上的所有内容。

配置 **Android Enterprise** 设备和应用程序策略

有关在设备和应用程序级别控制的策略的概述，请参阅 Android Enterprise 支持的设备策略和 MDX 策略。

关于策略需要了解以下内容：

- **Data loss protection**（数据丢失保护）：XenMobile MAM 容器技术使用加密和其他移动数据丢失防护 (DLP) 技术保护应用程序。对启用了 MDX 的应用程序、使用 Citrix MAM SDK 或 MDX Toolkit。
- 设备限制：数十种设备限制允许您控制以下功能：
  - 使用设备摄像头
  - 在工作配置文件与个人配置文件之间使用复制和粘贴
- **PerApp VPN**：使用“托管配置”设备策略为 Android Enterprise 配置 VPN 配置文件。
- 电子邮件策略：我们建议使用“托管配置”设备策略来配置应用程序。

下表列出了适用于 Android Enterprise 设备的所有设备策略。

> 重要：
>
> 对于在 Android Enterprise 中注册并使用 MDX 应用程序的设备：可以通过 MDX 和 Android Enterprise 控制某些设置。对 MDX 使用限制性最低的策略设置，并通过 Android Enterprise 控制策略。

Android Enterprise 应用程序权限	Android Enterprise 托管配置	应用程序清单
应用程序卸载	自动更新托管应用程序	控制操作系统更新
凭据	自定义 XML	Exchange
文件	键盘锁管理	kiosk
位置	通行码	限制
Samsung MDM 许可证密钥	计划	Wi-Fi
XenMobile 选项		

适用于具有工作配置文件的完全托管设备的设备策略（**COPE** 设备）

对于具有工作配置文件的完全托管设备（COPE 设备），可以使用某些设备策略将单独的设置应用到整个设备和工作配置文件。可以使用其他设备策略将设置仅应用到整个设备或仅应用到具有工作配置文件的完全托管设备的工作配置文件。

策略	适用对象
Android Enterprise 应用程序权限	工作配置文件
Android Enterprise 托管配置	工作配置文件
应用程序清单	工作配置文件
应用程序卸载	工作配置文件

策略	适用对象
自动更新托管应用程序	工作配置文件
控制操作系统更新	不适用
凭据	工作配置文件
自定义 XML	不适用
Exchange	不适用
文件	工作配置文件
键盘锁管理	设备和工作配置文件
kiosk	不适用
位置	设备（仅限定位模式）
通行码	设备和工作配置文件
限制	设备和工作配置文件（为设备和工作配置文件创建单独的策略）
Samsung MDM 许可证密钥	不适用
计划	工作配置文件
Wi-Fi	设备
XenMobile 选项	工作配置文件

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	否	是
查找	是	是
锁定	是	是
锁定并重置密码	否	是
通知（响铃）	是	是

安全操作	工作配置文件	完全托管
吊销	是	是
选择性擦除	是	否

安全操作说明

- 除非“位置”设备策略将设备的位置模式设置为高精度或电池节能，否则定位安全操作将失败。请参阅位置设备策略。
- 在运行 Android 8.0 之前版本的 Android 的工作配置文件设备上：
  - 不支持锁定和重置密码操作。
- 在 Android 8.0 或更高版本的工作配置文件设备上：
  - 发送的密码将锁定工作配置文件。设备本身不锁定。
  - 如果未在工作配置文件上设置通行码：
    - 如果未发送通行码或发送的通行码不符合通行码要求：设备处于锁定状态。
  - 如果在工作配置文件上设置了通行码：
    - 如果未发送通行码，或者发送的通行码不符合通行码要求：工作配置文件将锁定，但设备本身不锁定。
- 在使用工作配置文件的完全托管设备（COPE 设备）上：
  - 可以将“锁定”安全操作单独应用到设备或工作配置文件

取消注册 **Android Enterprise** 企业

如果您不想再使用 Android Enterprise 企业，则可以取消注册该企业。

> 警告：
>
> 取消注册企业后，通过其注册的设备上的 Android Enterprise 应用程序将重置为其默认状态。Google 不再管理设备。如果您注册到新的 Android Enterprise 企业，则必须从托管 Google Play 审批新组织的应用程序。然后，可以从 XenMobile 控制台更新这些应用程序。

取消注册 Android Enterprise 企业后：

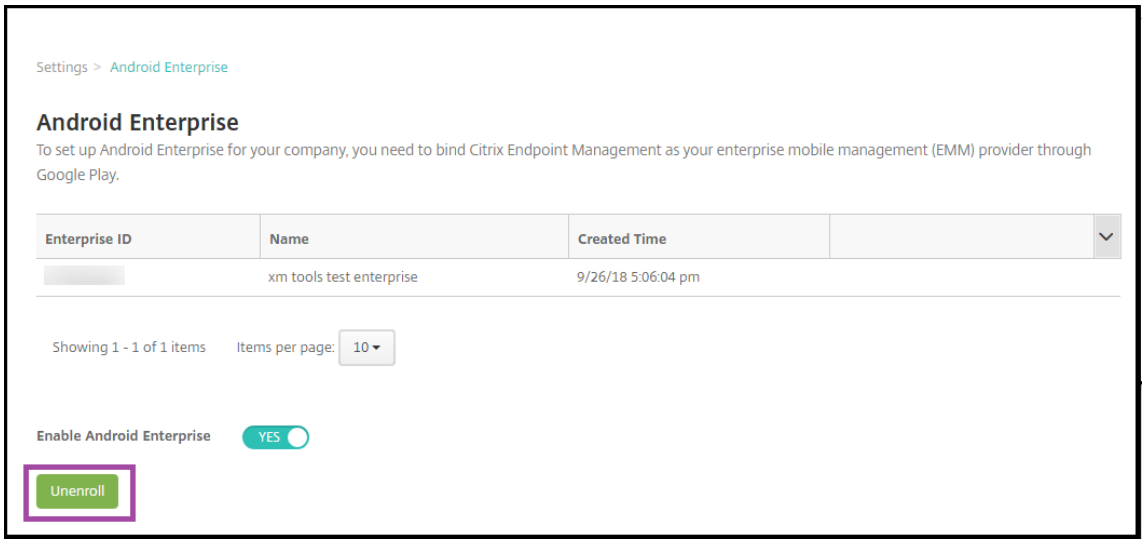
- 通过企业注册的设备和用户会将 Android Enterprise 应用程序重置到其默认状态。以前应用的 Android Enterprise 托管配置策略不再影响操作。
- XenMobile 负责管理通过企业注册的设备。从 Google 角度来看，这些设备是非托管设备。您不能添加新的 Android Enterprise 应用程序。您无法应用 Android Enterprise 托管配置策略。可以将其他策略（例如“计划”、“密码”和“限制”）应用到这些设备。
- 如果尝试在 Android Enterprise 中注册设备，这些设备将注册为 Android 设备，而非 Android Enterprise 设备。

使用 XenMobile Server 控制台和 XenMobile Tools 取消注册 Android Enterprise 企业。

执行此任务时，XenMobile 将打开 XenMobile Tools 的弹出窗口。开始之前，请确保 XenMobile 有权在您使用的浏览器中打开弹出窗口。某些浏览器（例如 Google Chrome）要求禁用弹出窗口阻止功能并将 XenMobile 站点的地址添加到弹出窗口阻止允许列表中。

要取消注册 Android Enterprise 企业，请执行以下操作：

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在“设置”页面上，单击 **Android Enterprise**。
3. 单击取消注册。



分发 **Android Enterprise** 应用程序

January 5, 2022

XenMobile 管理部署到设备的应用程序。可以组织和部署以下类型的 Android Enterprise 应用程序。

- 托管应用商店应用程序：这些应用程序包括托管 Google Play 应用商店中提供的免费或付费应用程序。例如，GoToMeeting。
- **MDX**：使用 MAM SDK 准备的应用程序或使用 MDX Toolkit 封装的应用程序。这些应用程序包括 MDX 策略。您可以从内部来源和公共应用商店获取 MDX 应用程序。将 Citrix 移动生产力应用程序作为 MDX 应用程序部署。
- 企业：您开发或从其他来源获取的专用应用程序。可以通过托管 Google Play 应用商店向用户提供这些应用程序。托管 Google Play 应用商店是 Google 企业应用商店。
- **MDX-enabled private apps**（启用了 MDX 的专用应用程序）：使用 MAM SDK 准备或通过 MDX Toolkit 封装的企业应用程序。

可以通过两种不同的方式添加企业应用程序和启用了 MDX 的专用应用程序。

- 将应用程序作为企业应用程序添加到 XenMobile 控制台，如本文中的企业应用程序和启用了 MDX 的专用应用程序部分中所述。
- 使用您的 Google 开发者帐号将应用程序直接发布到托管 Google Play 应用商店。然后将应用程序添加到 XenMobile 控制台作为托管应用商店应用程序。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 XenMobile 控制台，则应用程序的所有权会有所不同。在这种情况下，请在两个位置管理您的应用程序。Citrix 建议使用一种或另一种方法添加应用程序。

如果您需要从托管 Google Play 应用商店中删除自助管理的应用程序，请向 Google 开立一个票证。开发者可以禁用但不能删除托管 Google Play 应用商店中的应用程序。

以下各部分内容提供了有关 Android Enterprise 应用程序配置的详细信息。有关分发应用程序的信息，请参阅添加应用程序。该文包含：

- 用于添加 Web 和 SaaS 应用程序或 Web 链接的一般工作流程
- 面向企业和公共应用商店应用程序的必需应用程序工作流
- 如何通过适用于企业应用程序的 Citrix 内容交付网络 (CDN) 交付企业应用程序

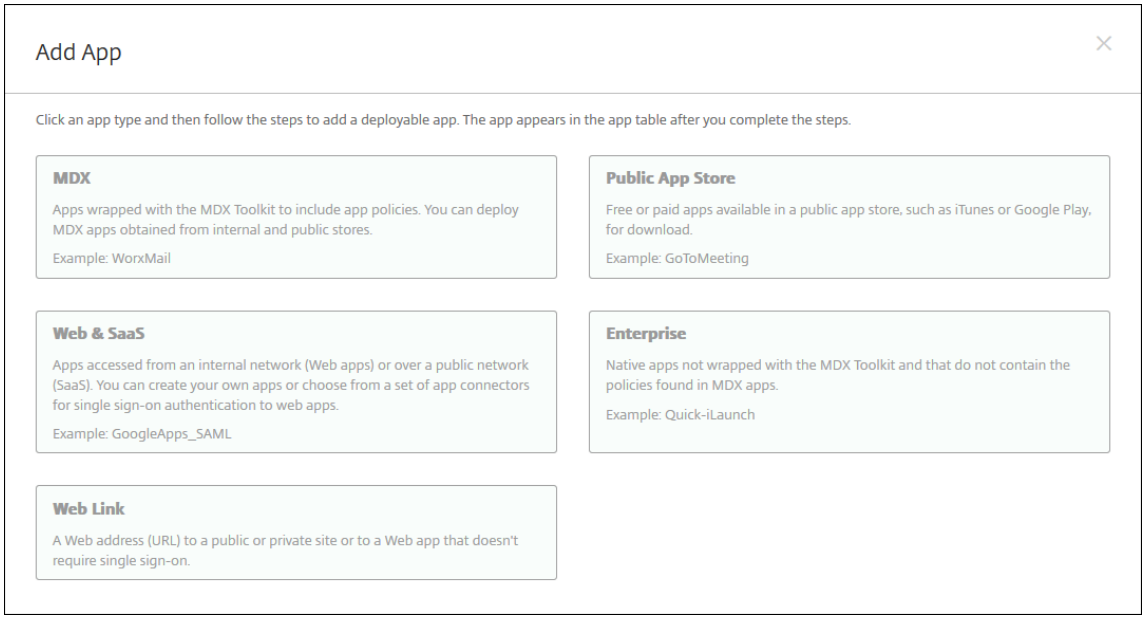
托管应用商店应用程序

可以将托管 Google Play 应用商店中可用的免费和付费应用程序添加到 XenMobile。

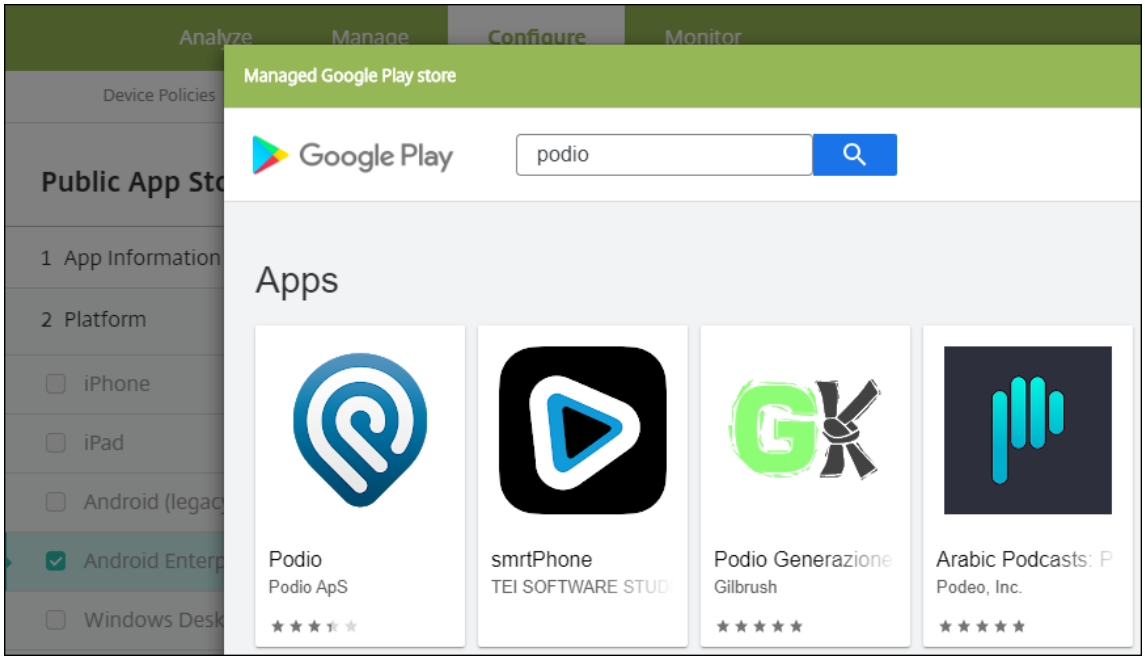
> 注意：
>
> 要使可从托管 Google Play 访问的 Google Play 应用商店中的所有应用程序，请使用访问托管 **Google Play** 应用商店中的所有应用程序服务器属性。请参阅服务器属性。将此属性设置为 **true** 会允许所有 Android Enterprise 用户访问公共 Google Play 应用商店应用程序。然后，您可以使用限制设备策略来控制对这些应用程序的访问。

步骤 **1**：添加和配置应用程序

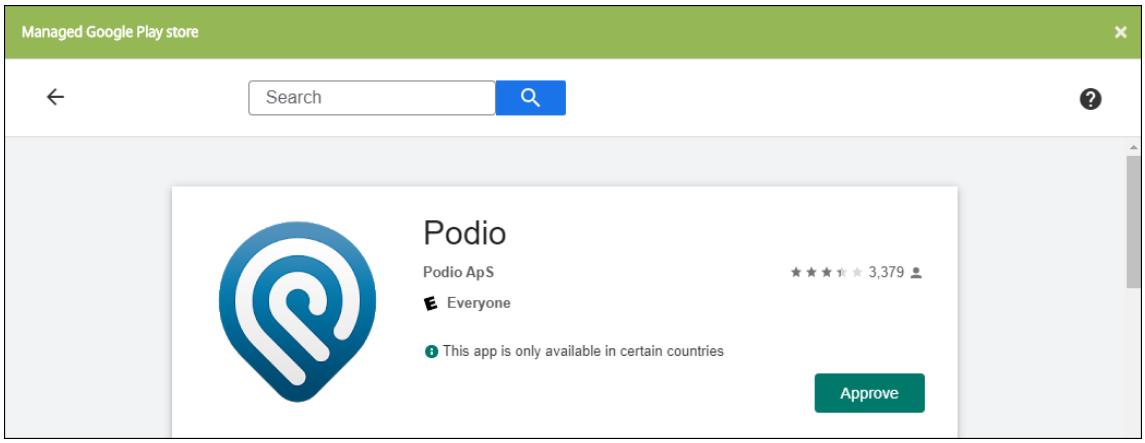
1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击公共应用商店。



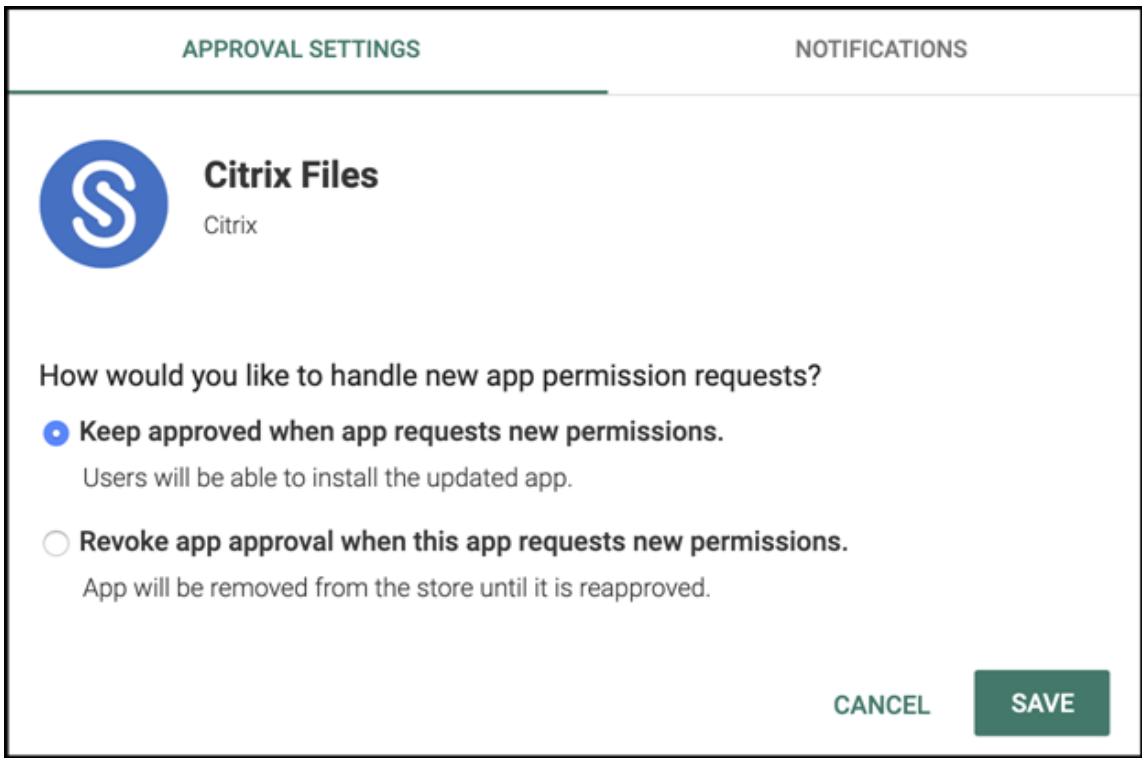
3. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。该名称将显示在应用程序表中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 选择 **Android Enterprise** 作为平台。
5. 在搜索框中键入应用程序名称或软件包 ID，然后单击搜索。可以在 Google Play 应用商店中找到软件包 ID。该 ID 位于应用程序的 URL 中。例如，`com.Slack` 为 `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US` 中的软件包 ID。



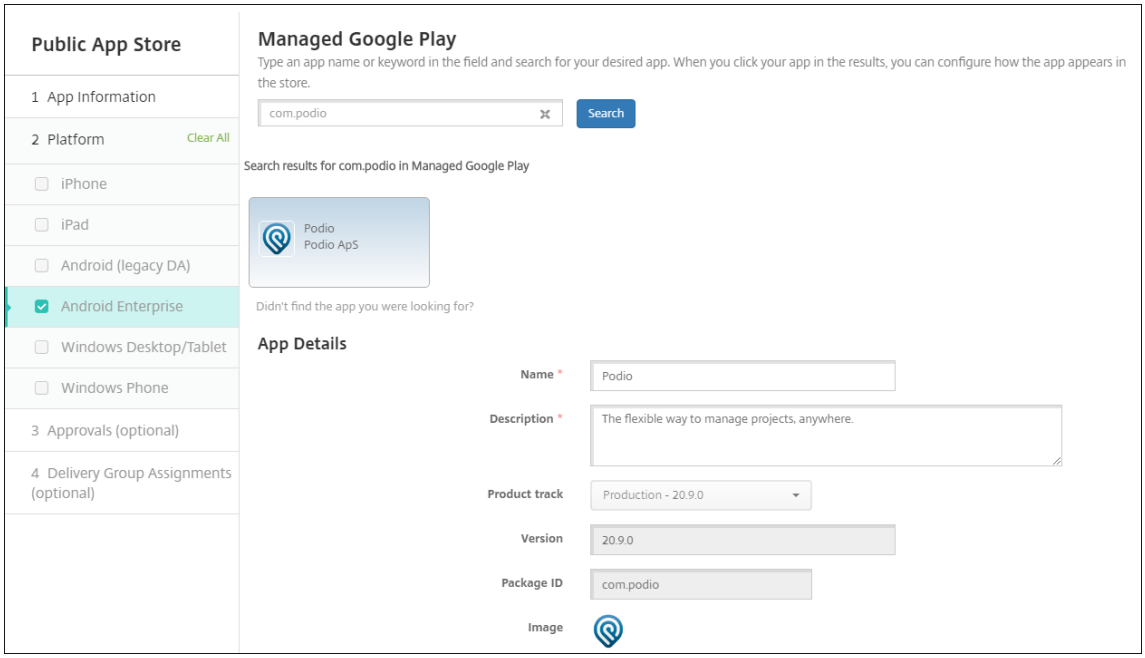
6. 此时将显示符合搜索条件的应用程序。单击所需应用程序，然后单击 **Approve**（审批）。



7. 再次单击 **Approve**（批准）。
8. 选择 **Keep approved when app requests new permissions**（在应用程序请求新权限时保持已批准）。单击保存。



9. 单击应用程序图标并配置应用程序名称和说明。

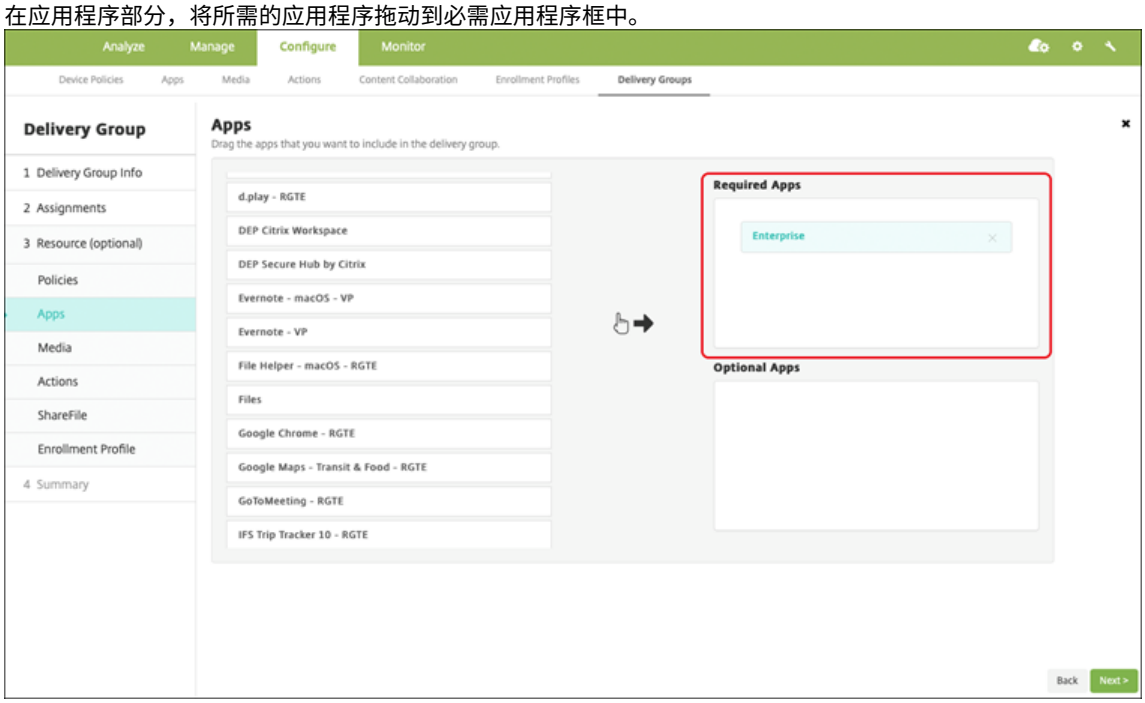


10. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

步骤 **2**：配置应用程序部署

1. 导航到配置 **>** 交付组，然后选择您配置的交付组。单击编辑。

2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



3. 在摘要页面上，单击保存。
4. 在交付组页面上，选择交付组，然后单击部署。

MDX 应用程序

将 MDX 文件添加到 XenMobile 并配置应用程序详细信息和策略设置。要为 Android Enterprise 配置 Citrix 移动生产力应用程序，请将其添加为 MDX 应用程序。有关每种设备平台类型可用的应用程序策略的信息，请参阅：

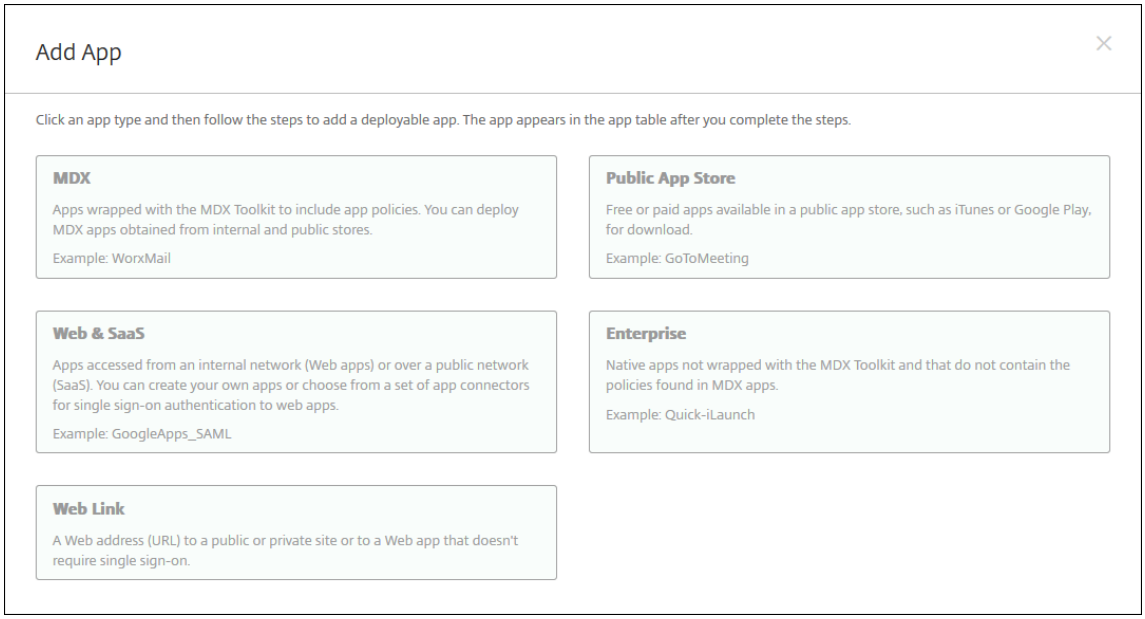
- MAM SDK 概述
- MDX 策略概览

步骤 **1**：添加和配置应用程序

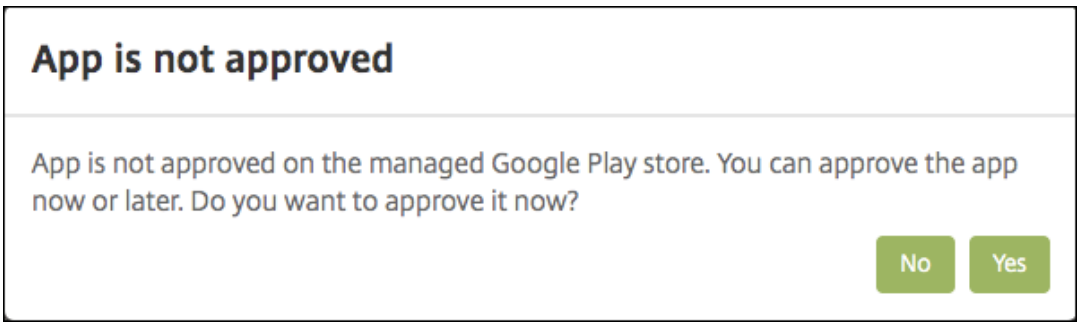
1. 对于 Citrix 移动生产力应用程序，请下载公共应用商店 MDX 文件：转到 https://www.citrix.com/downloads。导航到 **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management** 生产力应用程序。

   对于其他类型的 MDX 应用程序，请获取 MDX 文件。

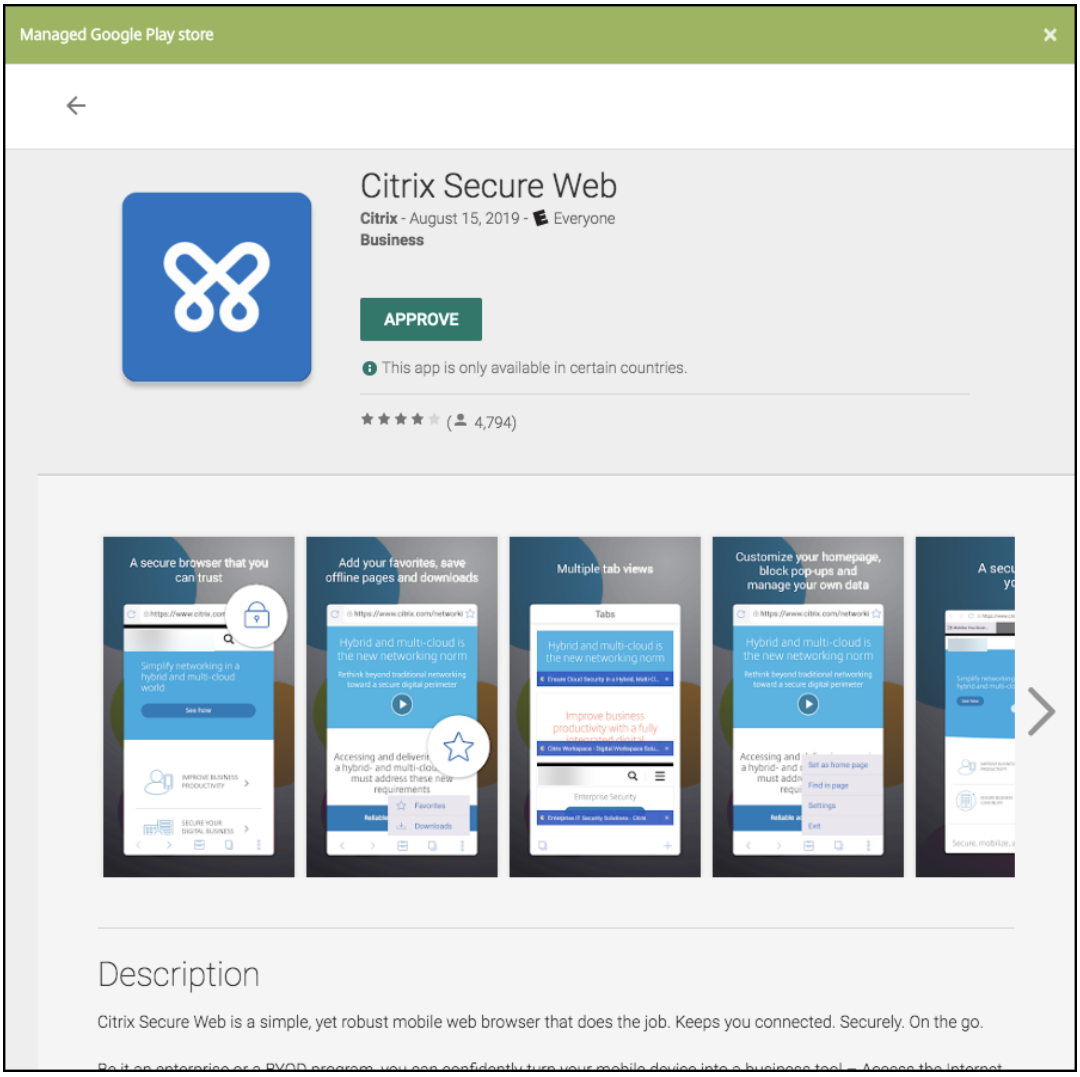
2. 在 XenMobile 控制台中，单击配置 **>** 应用程序。单击添加。此时将显示添加应用程序对话框。



3. 单击 **MDX**。此时将显示 **MDX** 应用程序信息页面。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。该名称将显示在应用程序表中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 选择 **Android Enterprise** 作为平台。
5. 单击上载并导航到 MDX 文件。Android Enterprise 仅支持使用 MAM SDK 或 MDX Toolkit 准备的应用程序。
   - UI 会通知您附加的应用程序是否需要从托管 Google Play 应用商店获得批准。要在不离开 XenMobile 控制台的情况下审批应用程序，请单击是。



   在托管 Google Play 应用商店打开后，按照说明审批并保存应用程序。



成功添加应用程序后，将显示应用程序详细信息页面。

6. 配置以下设置：

   - 文件名：键入与应用程序关联的文件名。
   - 应用程序说明：键入应用程序的说明。
   - 应用程序版本：（可选）键入应用程序版本号。
   - 软件包 **ID**：键入从托管的 Google Play 商店获取的应用程序包 ID。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。

7. 配置 **MDX** 策略。MDX 策略因平台而异，并且包含面向策略区域的选项，包括身份验证、设备安全和应用程序限制。在控制台中，每种策略都具有介绍此策略的提示。有关每种设备平台类型可用的应用程序策略的信息，请参阅：

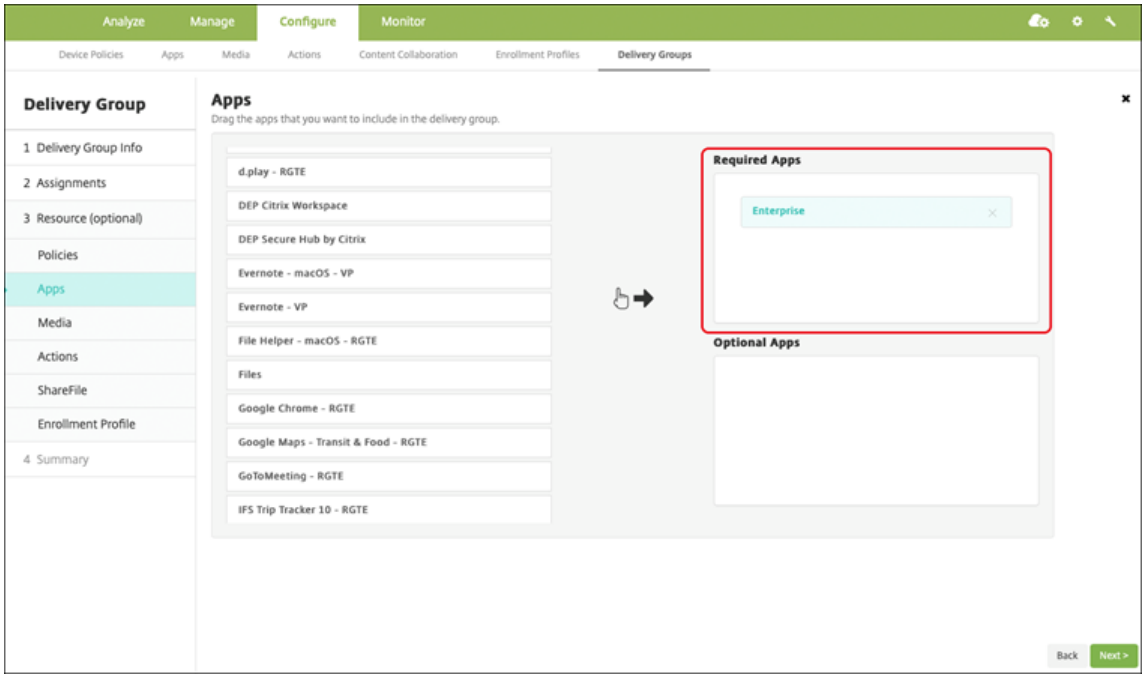
   - MAM SDK 概述

- MDX 策略概览

8. 配置部署规则和应用商店配置。
9. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

步骤 **2**：配置应用程序部署

1. 导航到配置 **>** 交付组，然后选择您配置的交付组。单击编辑。
2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



3. 在摘要页面上，单击保存。
4. 在交付组页面上，选择交付组，然后单击部署。

企业应用程序

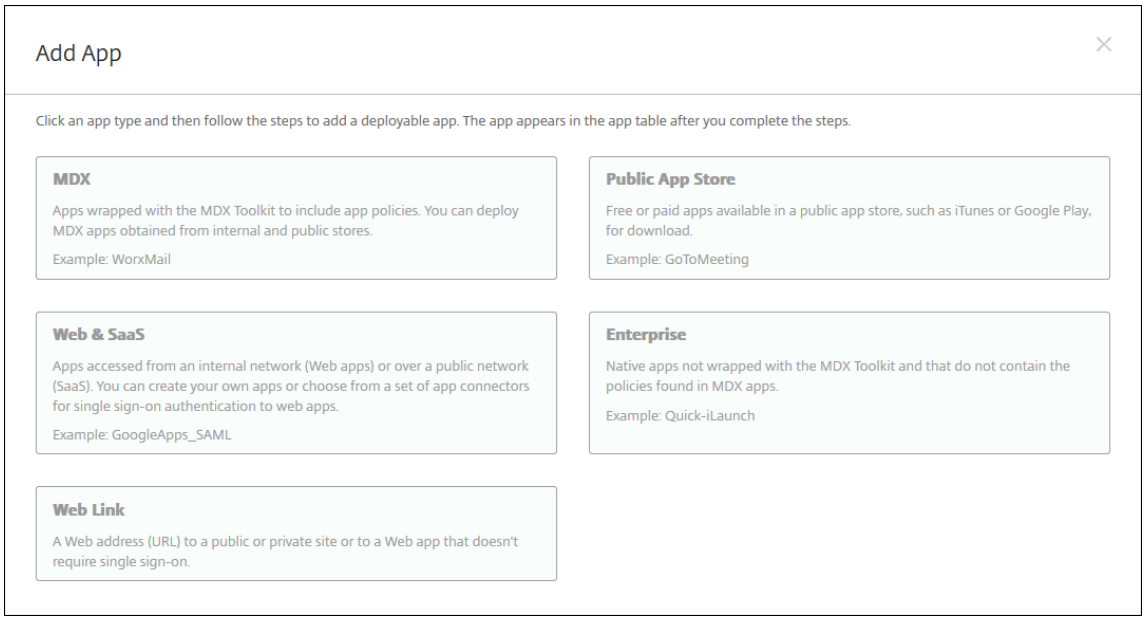
XenMobile 应用程序表示未使用 MAM SDK 或 MDX Toolkit 准备的专用应用程序。可以自己开发这些应用程序或直接从其他来源获取。要添加企业应用程序，您需要与该应用程序关联的 APK 文件。请务必关注 Google Best practices for private apps（专用应用程序的最佳实践）。

步骤 **1**：添加和配置应用程序

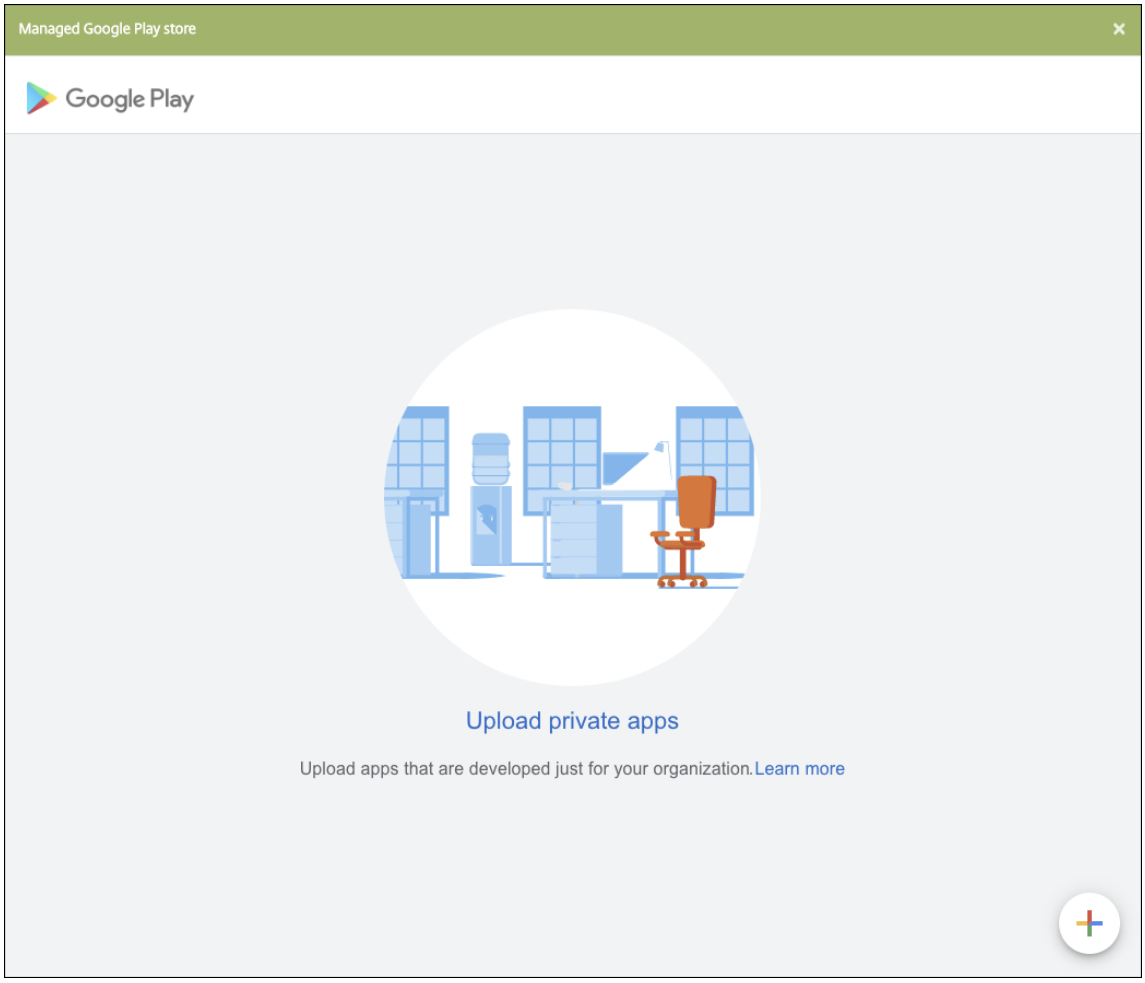
通过以下两种方法之一添加应用程序：

- 将应用程序直接发布到托管 Google Play 应用商店，然后将其作为托管 Play 应用商店应用程序添加到 XenMobile 控制台。请参照 Google 文档，了解如何发布专用应用程序，然后按照托管应用商店应用程序部分中的步骤进行操作。
- 将应用程序作为企业应用程序添加到 XenMobile 控制台。请执行以下步骤：

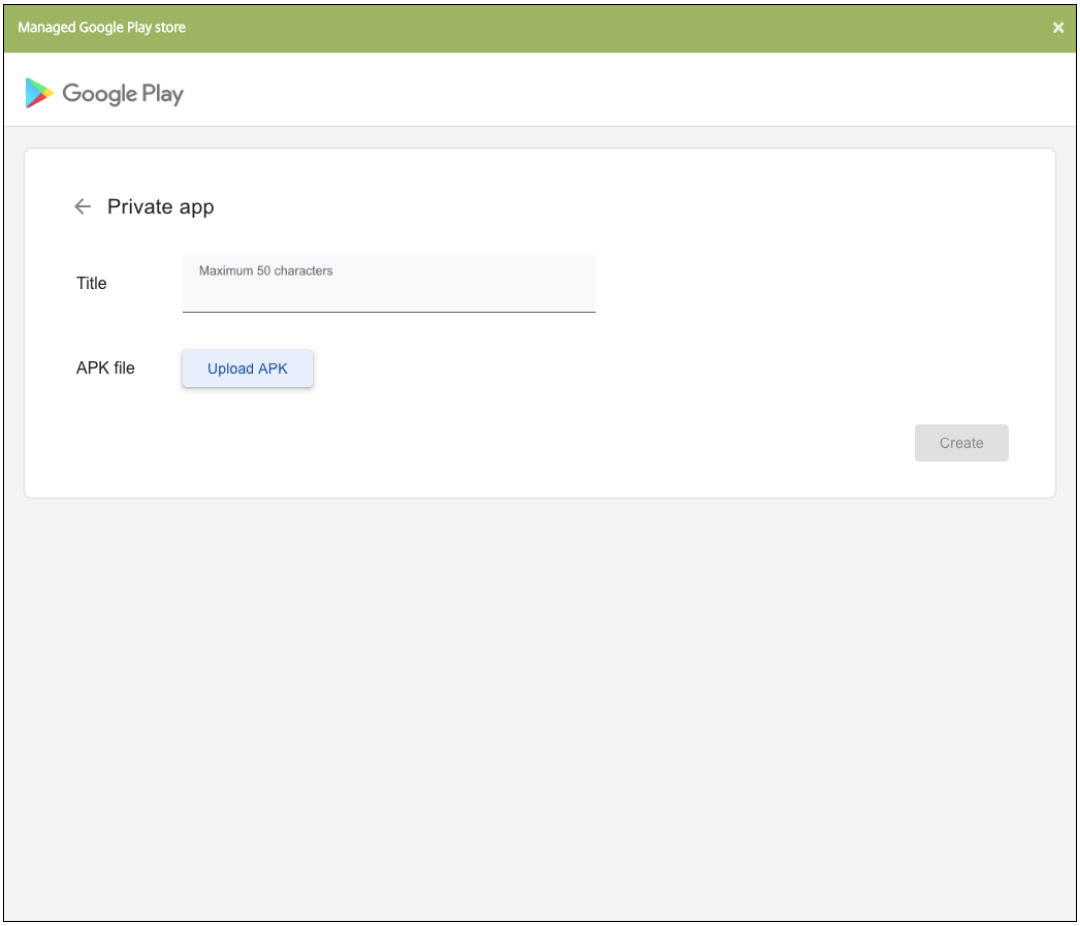
1. 在 XenMobile 控制台中，单击配置 **>** 应用程序。单击添加。此时将显示添加应用程序对话框。



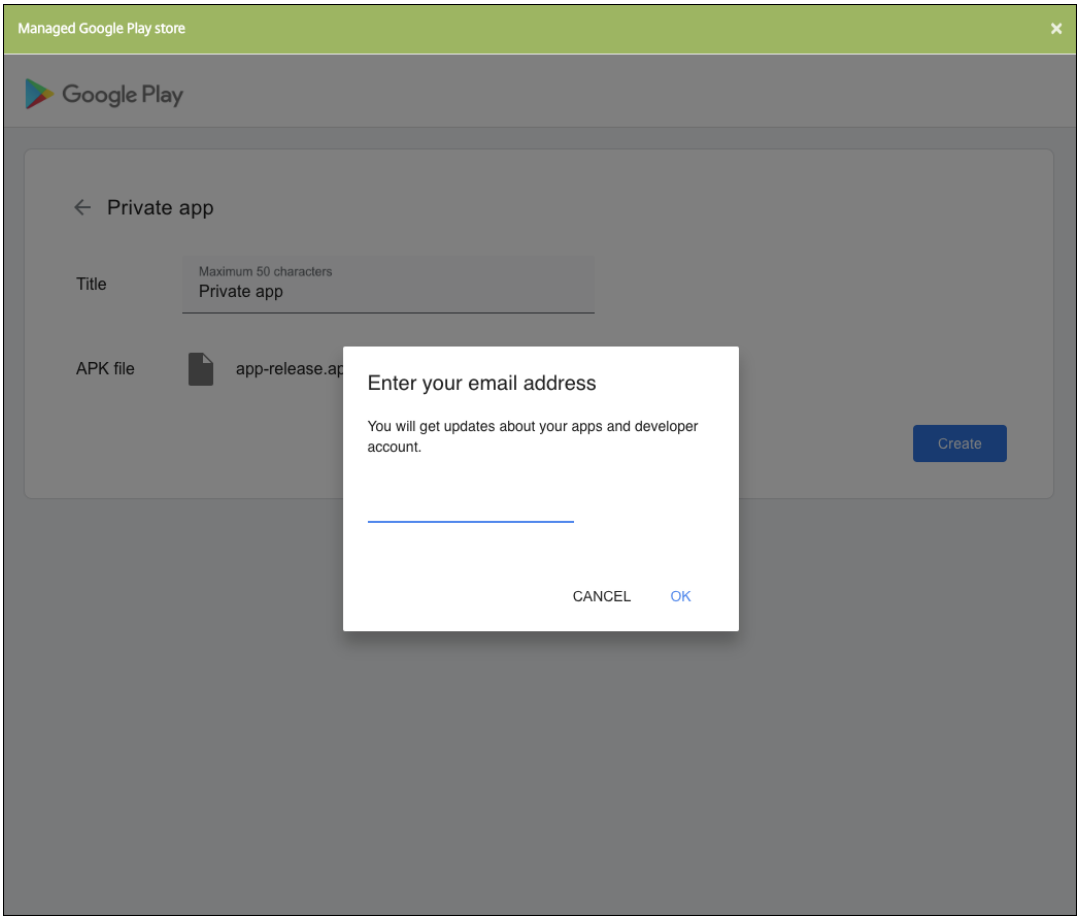
2. 单击企业。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
3. 选择 **Android Enterprise** 作为平台。
4. 上载按钮将打开托管 Google Play 应用商店。您无需注册开发者帐户即可发布专用应用程序。单击右下角的加号图标以继续。



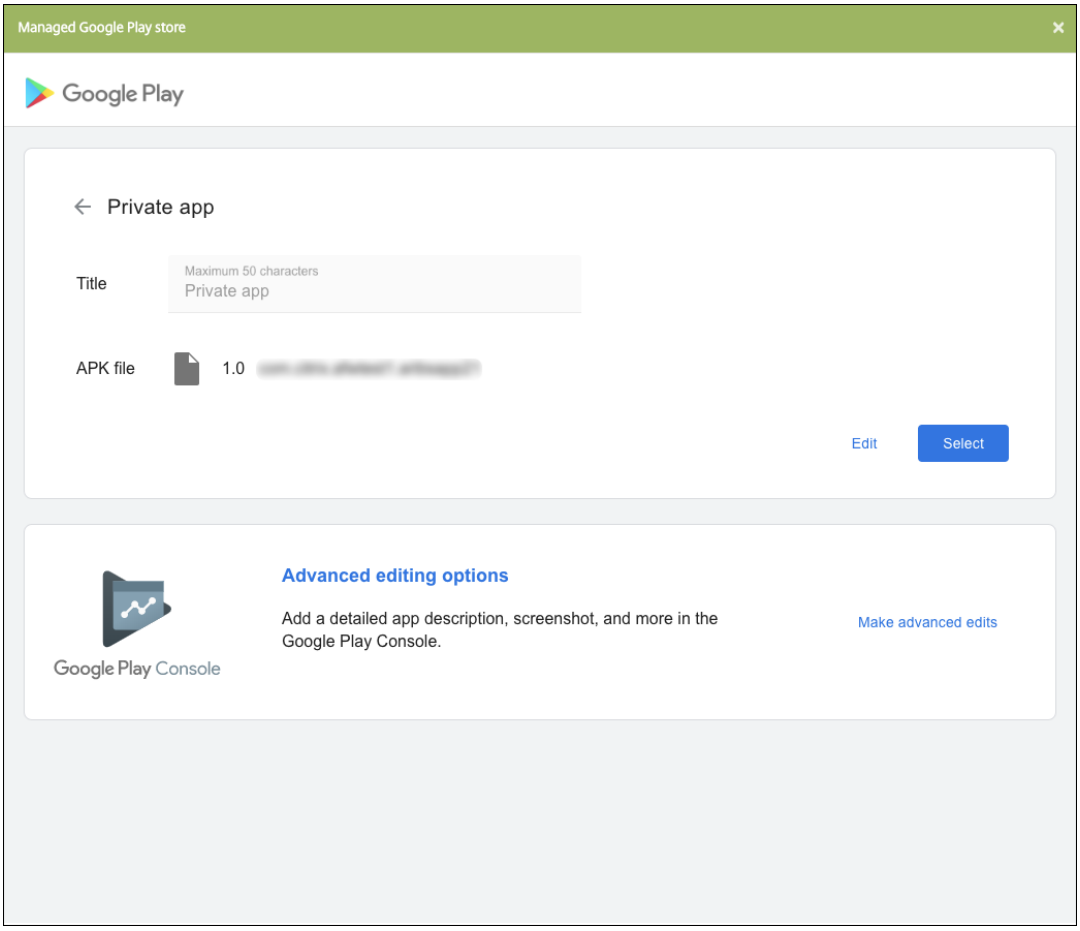
a) 键入应用程序的名称并上载.apk 文件。完成后，单击创建。您的专用应用程序最多可能需要 10 分钟才能发布。



b) 输入电子邮件地址以获取有关您的应用程序的更新。



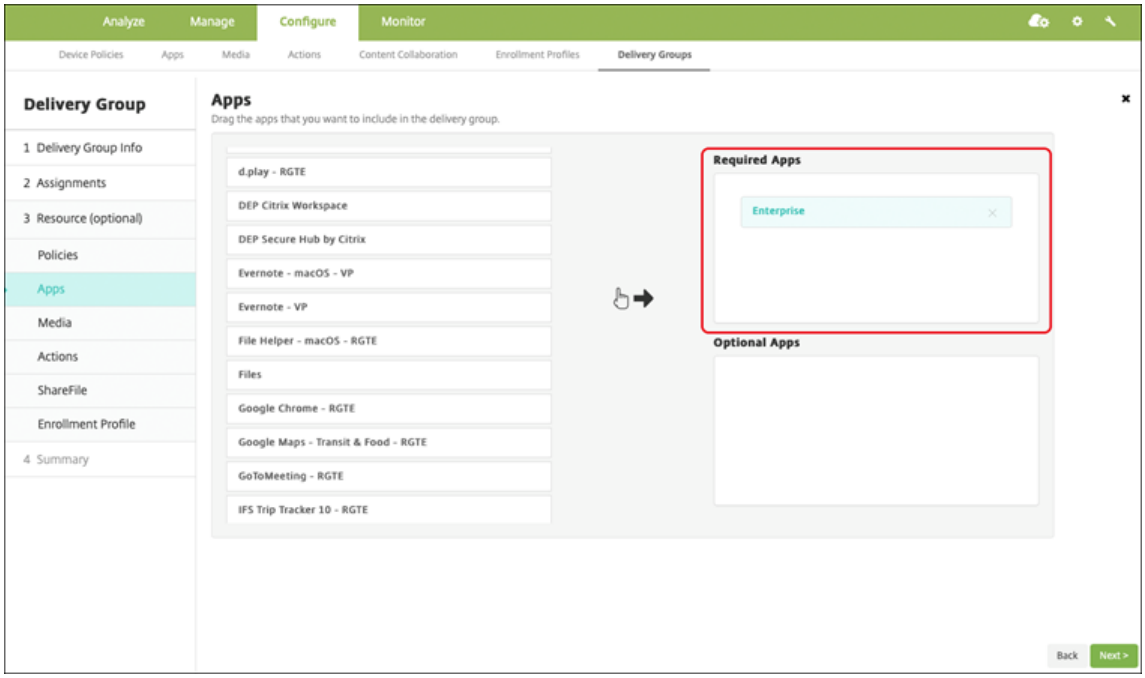
c) 发布应用程序后，单击专用应用程序的图标。如果要添加应用程序说明、更改应用程序图标以及执行其他操作，请单击 **Make advanced edits**（进行高级编辑）。否则，请单击选择以打开应用程序信息页面。



5. 单击 **Next**（下一步）。此时将显示平台的应用程序信息页面。
6. 为平台类型配置设置，例如：
   - 文件名：（可选）键入应用程序的新名称。
   - 应用程序说明：（可选）键入应用程序的新说明。
   - 应用程序版本：无法更改此字段。
   - 软件包 **ID**：应用程序的唯一标识符。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
7. 配置部署规则和应用商店配置。
8. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

步骤 **2**：配置应用程序部署

1. 导航到配置 **>** 交付组，然后选择您配置的交付组。单击编辑。
2. 在应用程序部分，将所需的应用程序拖动到必需应用程序框中。



3. 在摘要页面上，单击保存。
4. 在交付组页面上，选择交付组，然后单击部署。

启用了 **MDX** 的专用应用程序

要将 Android Enterprise 应用程序添加为启用了 MDX 的企业应用程序，请执行以下操作：

1. 创建专用 Android Enterprise 应用程序并为应用程序启用 MDX。
2. 将应用程序添加到 XenMobile 控制台。
   - 在托管 Google Play 应用商店中托管和发布应用程序。
   - 将应用程序添加到 XenMobile 控制台作为企业应用程序。
3. 将 MDX 文件添加到 XenMobile。

如果您决定通过 Google Play 应用商店托管和发布应用程序，请不要选择使用 Google 证书签名。请使用用于通过 MDX 启用应用程序的相同证书对应用程序进行签名。有关发布应用程序的详细信息，请参阅 Publishing your app（发布您的应用程序）和 Signing your app（对您的应用程序进行签名）上的 Google 文档。MAM SDK 不封装应用程序，因此它不需要用于开发应用程序的证书以外的证书。

有关通过 Google Play 控制台发布专用应用程序的详细信息，请参阅有关如何从 Play 控制台发布专用应用程序的 Google 文档。

要通过 XenMobile 发布应用程序，请参阅以下部分。

准备一个专用 **Android Enterprise** 应用程序

创建专用 Android Enterprise 应用程序时，请务必遵循 Google Best practices for private apps（面向专用应用程序的最佳做法）。

创建专用 Android Enterprise 应用程序后，请将 MAM SDK 与应用程序集成，或使用 MDX Toolkit 封装应用程序。然后，将生成的文件添加到 XenMobile。

可以通过上载更新后的.apk 文件来更新应用程序。以下步骤介绍了通过 MDX Toolkit 封装应用程序的过程。

1. 创建您的专用 Android Enterprise 应用程序并生成一个签名的.apk 文件。
2. 以下示例文件包含所有已知策略，其中一些策略可能不适用于您的环境。任何不可用的设置都将被忽略。使用以下参数创建 XML 文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
            NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
        <ActivePollPeriod>60</ActivePollPeriod>
        <PublicFileAccessLimitsList/>
        <CutAndCopy>Unrestricted</CutAndCopy>
        <Paste>Unrestricted</Paste>
        <DocumentExchange>Unrestricted</DocumentExchange>
        <OpenInExclusionList/>
        <InboundDocumentExchange>Unrestricted</
            InboundDocumentExchange>
        <InboundDocumentExchangeWhitelist/>
        <connectionSecurityLevel>TLS</connectionSecurityLevel>
```



```
        <DisableCamera>false</DisableCamera>
        <DisableGallery>false</DisableGallery>
        <DisableMicrophone>false</DisableMicrophone>
        <DisableLocation>false</DisableLocation>
        <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>
<!--NeedCopy-->
```

3. 使用 MDX Toolkit 封装应用程序。有关使用 MDX Toolkit 的信息，请参阅封装 Android 移动应用程序。

   将 **apptype** 参数设置为 **Premium**。在下面介绍的命令中使用上一步中的 XML 文件。

   如果您知道应用程序的应用商店 URL，请将 **storeURL** 参数设置为应用商店 URL。发布应用程序后，用户将从应用商店 URL 下载应用程序。

   下面是用于封装名为 SampleAEapp 的应用程序的 MDX Toolkit 命令的示例：

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

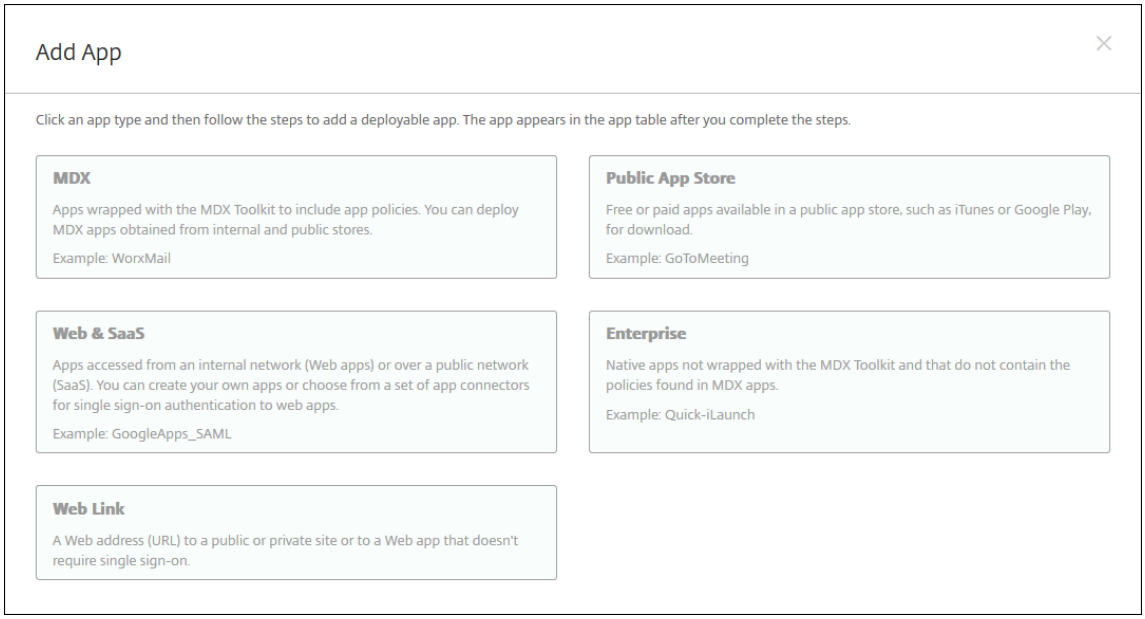
封装应用程序会生成一个封装的.apk 文件和一个.mdx 文件。

添加封装的**.apk** 文件

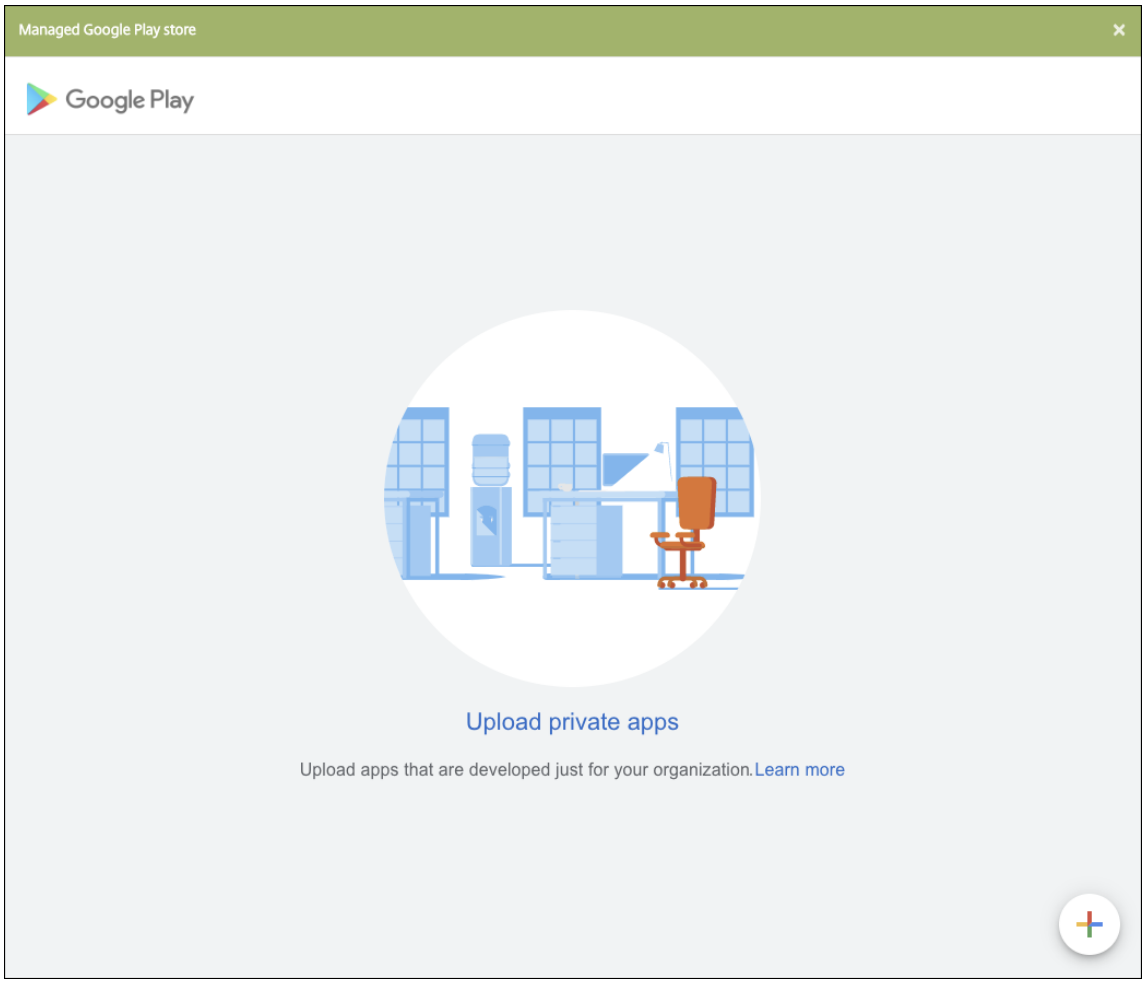
通过以下两种方法之一添加应用程序：

- 将应用程序直接发布到托管 Google Play 应用商店，然后将其作为托管 Play 应用商店应用程序添加到 XenMobile 控制台。请参照 Google 文档，了解如何发布专用应用程序，然后按照托管应用商店应用程序部分中的步骤进行操作。
- 将应用程序作为企业应用程序添加到 XenMobile 控制台。请执行以下步骤：

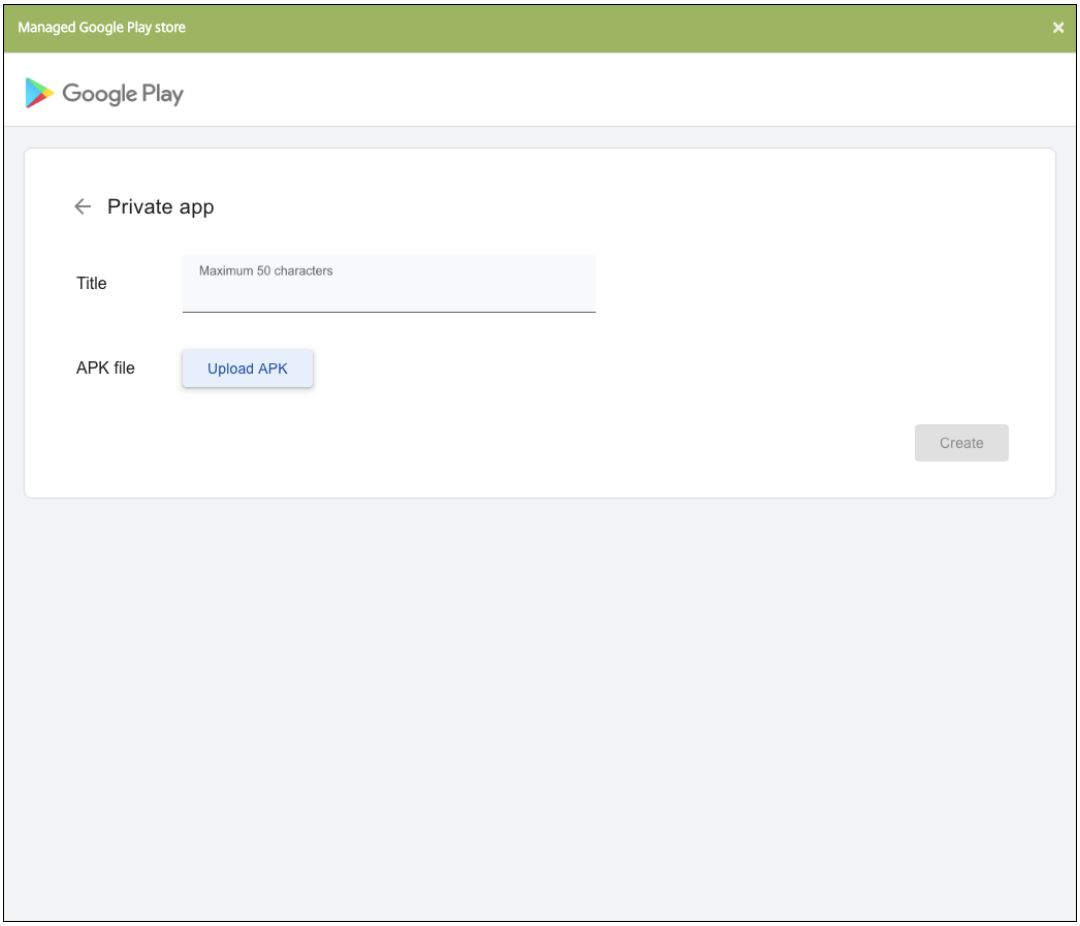
1. 在 XenMobile 控制台中，单击配置 **>** 应用程序。此时将打开应用程序页面。
2. 单击添加。此时将显示添加应用程序对话框。



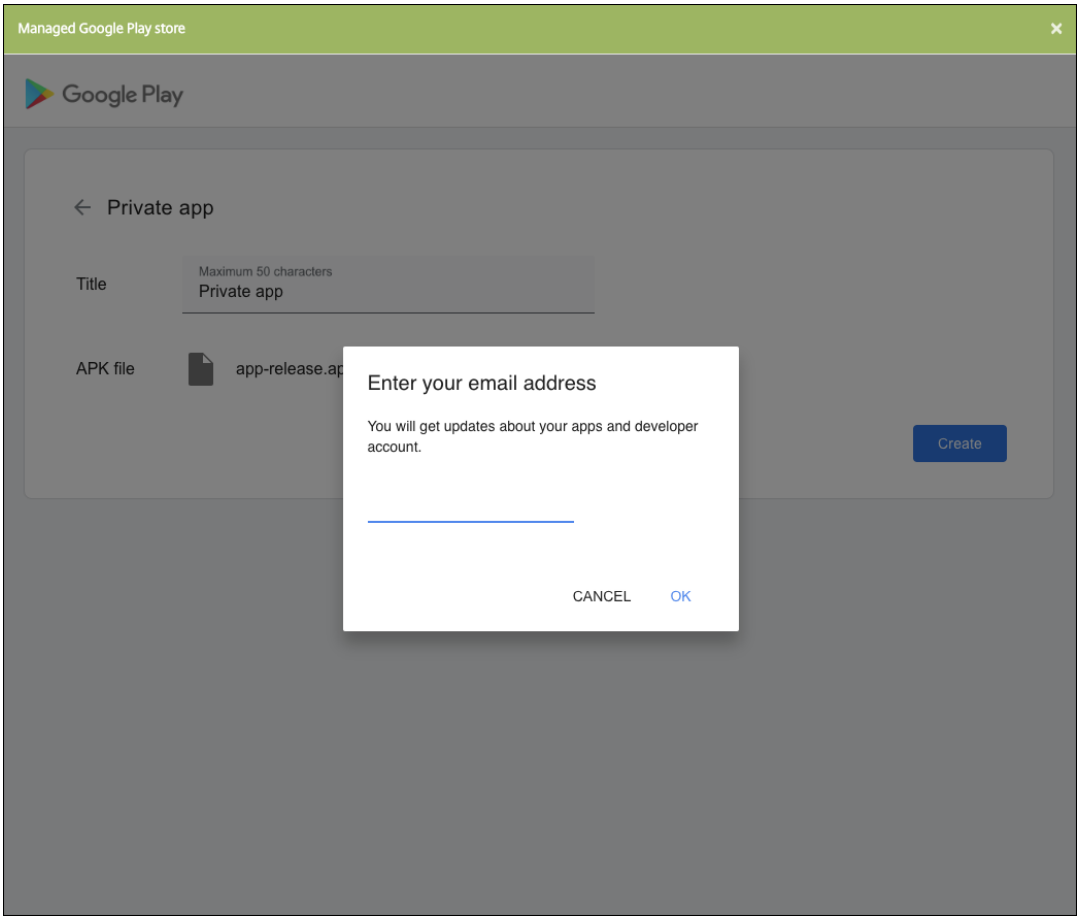
3. 单击企业。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 选择 **Android Enterprise** 作为平台。
5. 上载按钮将打开托管 Google Play 应用商店。您无需注册开发者帐户即可发布专用应用程序。单击右下角的加号图标以继续。



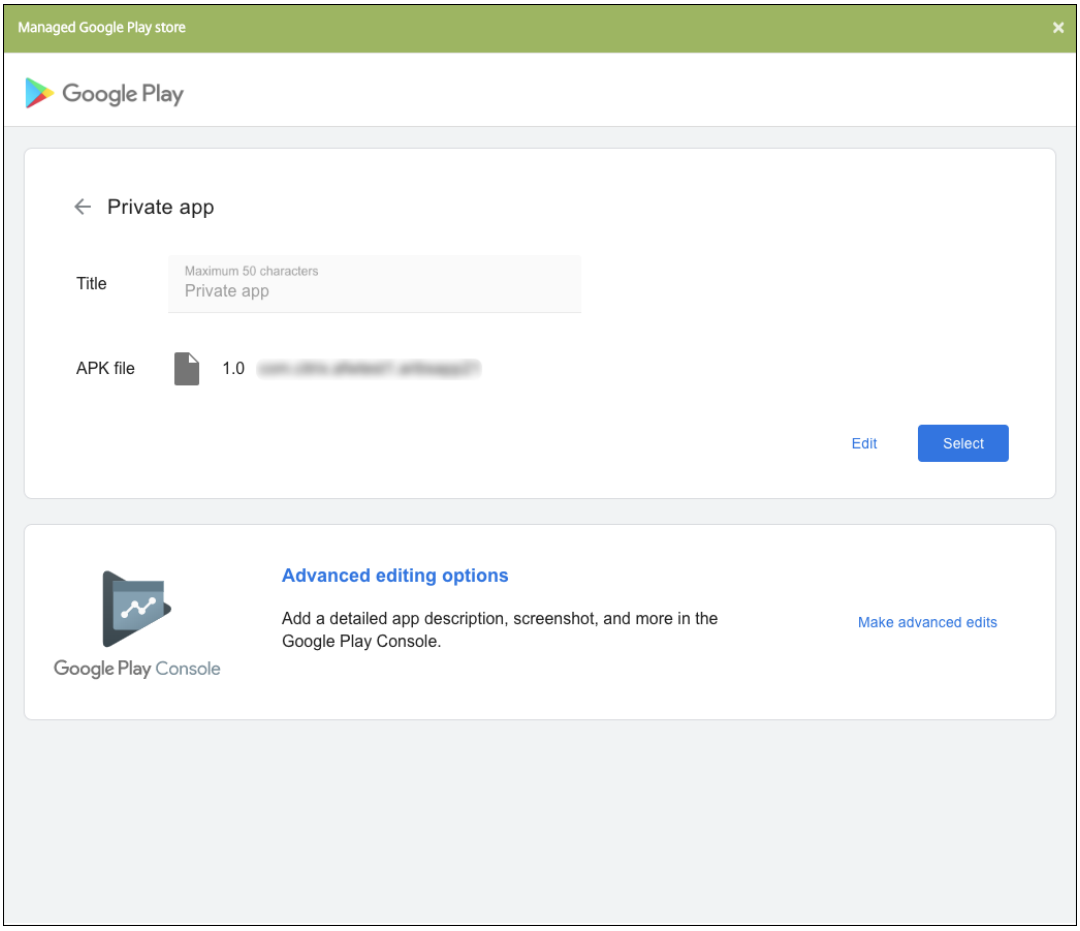
   a) 键入应用程序的名称并上载.apk 文件。完成后，单击创建。您的专用应用程序最多可能需要 10 分钟才能发布。



b) 输入电子邮件地址以获取有关您的应用程序的更新。



c) 发布应用程序后，单击专用应用程序的图标，然后单击选择以打开应用程序信息页面。



6. 单击 **Next**（下一步）。此时将显示平台的应用程序信息页面。
7. 为平台类型配置设置，例如：
   - 文件名：（可选）键入应用程序的新名称。
   - 应用程序说明：（可选）键入应用程序的新说明。
   - 应用程序版本：无法更改此字段。
   - 软件包 **ID**：应用程序的唯一标识符。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
8. 配置部署规则和应用商店配置。
9. 在 **Android Enterprise** 企业应用程序页面中，单击下一步。此时将显示审批页面。

   要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果无需审批工作流，可以跳至步骤 13。
10. 单击 **Next**（下一步）。
11. 此时将显示交付组分配页面。无需在此页面上执行任何操作。添加.mdx 文件时，可以为此应用程序配置交付组

和部署计划。单击保存。

可选：添加或更改应用商店 **URL**

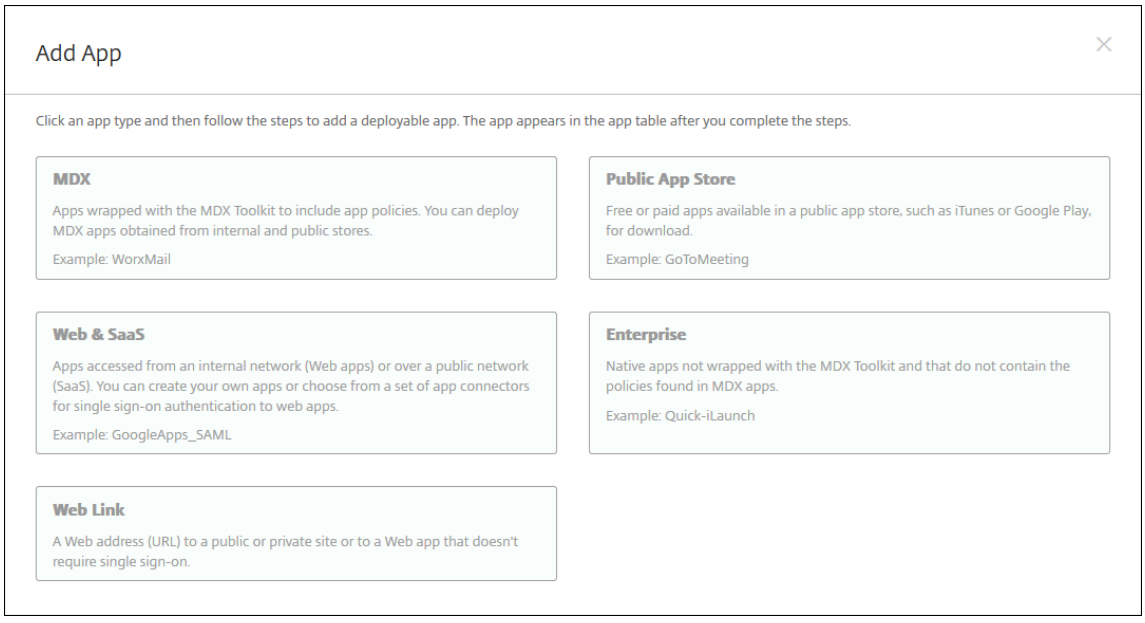
如果您在封装应用程序时不知道应用商店 URL，请立即添加应用商店 URL。

1. 查看托管 Google Play 应用商店中的应用程序。选择应用程序时，应用商店 URL 将显示在浏览器的地址栏中。从 URL 表单中复制应用程序的软件包名称。例如：`https://play.google.com/store/apps/details?id=SampleAEappPackage`。您复制的 URL 可能以 `https://play.google.com/work/` 开头。确保将 `work` 更改为 `store`。
2. 使用 MDX Toolkit 将应用商店 URL 添加到.mdx 文件中：

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
    SampleAEappPackage"
<!--NeedCopy-->
```

添加**.mdx** 文件

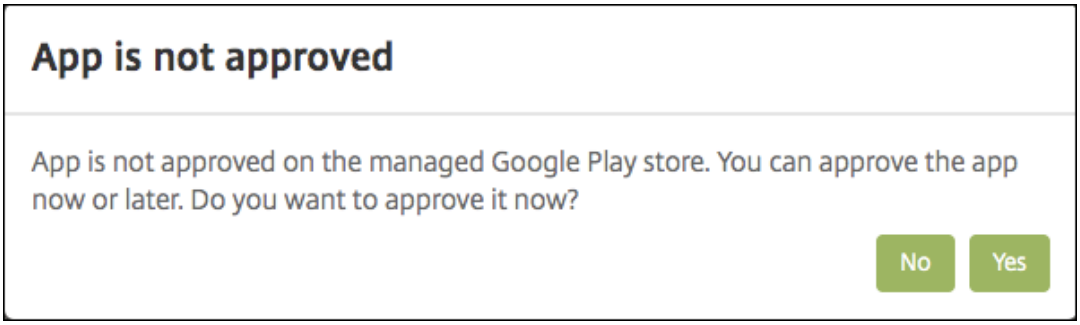
1. 在 XenMobile 控制台中，单击配置 **>** 应用程序。单击添加。此时将显示添加应用程序对话框。



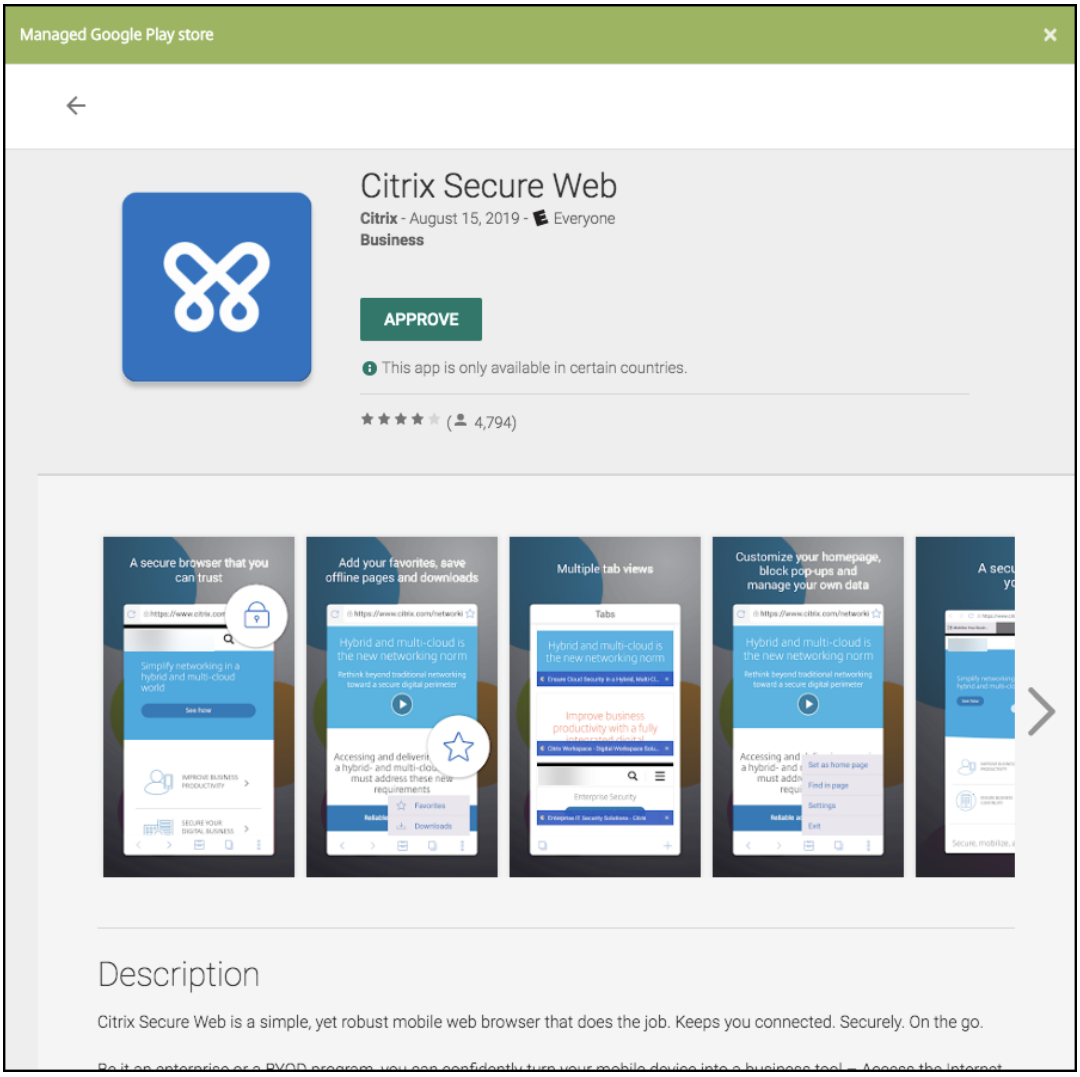
2. 单击 **MDX**。此时将显示 **MDX** 应用程序信息页面。在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。该名称将显示在应用程序表中的应用程序名称下。
   - 说明：键入应用程序的可选说明。

- 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

3. 选择 **Android Enterprise** 作为平台。
4. 单击上载并导航到 MDX 文件。Android Enterprise 仅支持使用 MDX Toolkit 封装的应用程序。
   - UI 会通知您附加的应用程序是否需要从托管 Google Play 应用商店获得批准。要在不离开 XenMobile 控制台的情况下审批应用程序，请单击是。



   在托管 Google Play 应用商店打开后，按照说明审批并保存应用程序。



成功添加应用程序后，将显示应用程序详细信息页面。

5. 配置以下设置：

   - 文件名：键入与应用程序关联的文件名。
   - 应用程序说明：键入应用程序的说明。
   - 应用程序版本：（可选）键入应用程序版本号。
   - 软件包 **ID**：键入从托管的 Google Play 商店获取的应用程序包 ID。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。

6. 配置 **MDX** 策略。MDX 策略因平台而异，并且包含面向策略区域的选项，包括身份验证、设备安全和应用程序限制。在控制台中，每种策略都具有介绍此策略的提示。有关每种设备平台类型可用的应用程序策略的信息，请参阅：

   - MAM SDK 概述

- MDX 第三方应用程序策略概览

7. 配置部署规则和应用商店配置。

   如果在设置 > 服务器属性中配置了计划后台部署密钥，则为始终启用的连接部署适用。

   始终启用选项：

   - 不适用于开始使用 10.18.19 或更高版本的 Endpoint Management 的 Android Enterprise 客户
   - 不建议开始使用版本 10.18.19 之前的 Endpoint Management 的 Android Enterprise 客户使用

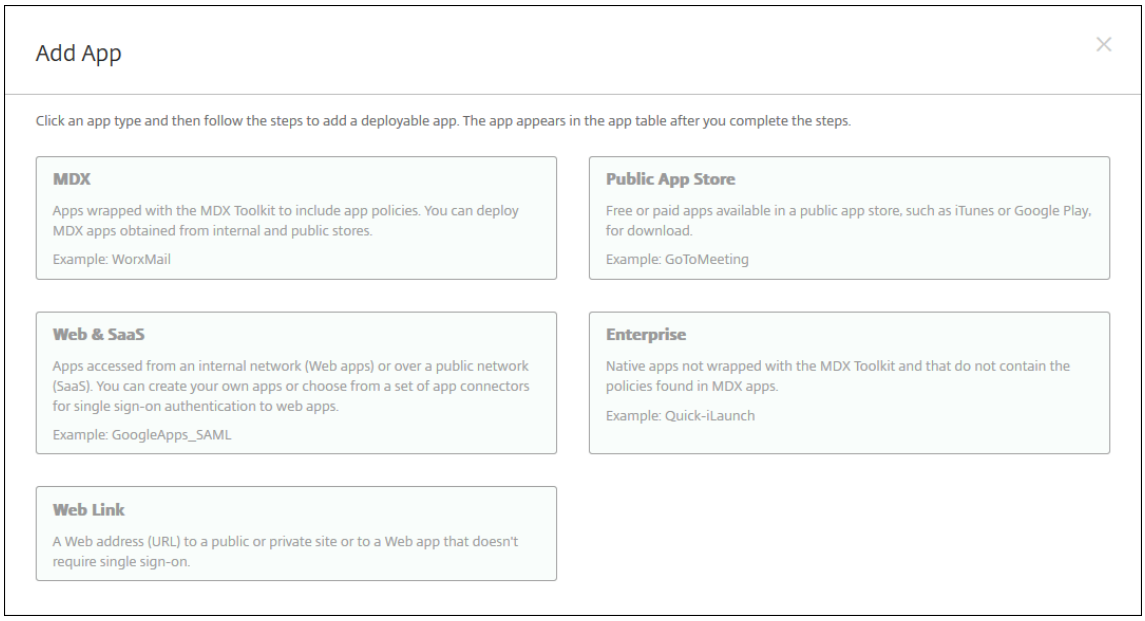
   配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

8. 将任何交付组分配给应用程序，然后单击保存。有关信息，请参阅部署资源。

更新应用程序

要更新 Android Enterprise 应用程序，请封装并上载更新后的.apk 文件：

1. 使用 MAM SDK 或 MDX Toolkit 封装更新后的应用程序的.apk 文件。
2. 在 XenMobile 控制台中，单击配置 > 应用程序。此时将打开应用程序页面。

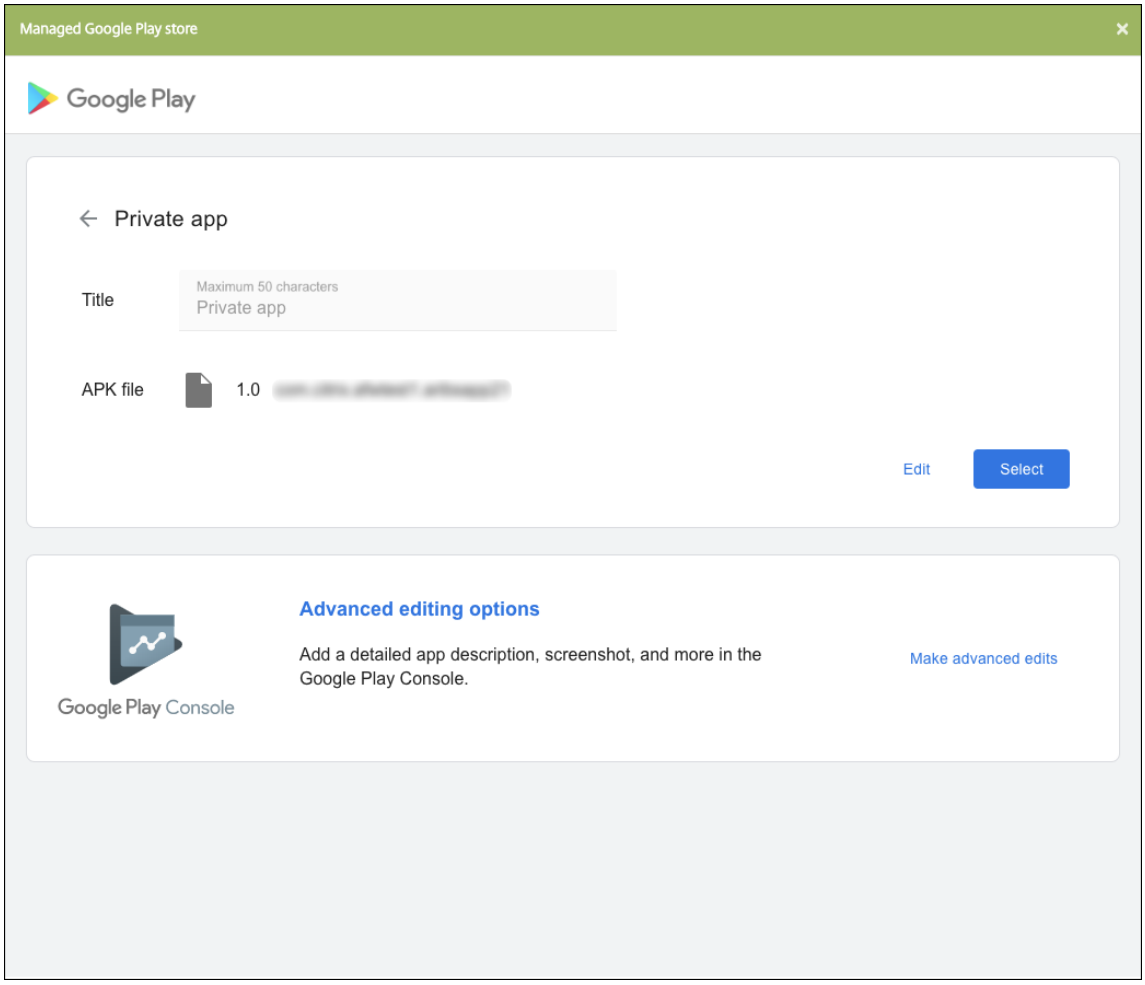


3. 单击添加。此时将显示添加应用程序对话框。
4. 单击企业。在应用程序信息窗格中，键入以下信息：

   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

5. 选择 **Android Enterprise** 作为平台。

6. 单击 **Next**（下一步）。此时将显示 **Android Enterprise** 企业应用程序页面。
7. 单击上载。
8. 在托管 Google Play 应用商店页面中，选择要更新的应用程序。
9. 在应用程序信息页面中，单击.apk 文件名旁边的编辑。



10. 导航到新.apk 文件并上载该文件。
11. 在托管 Google Play 应用商店页面中，单击保存。

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

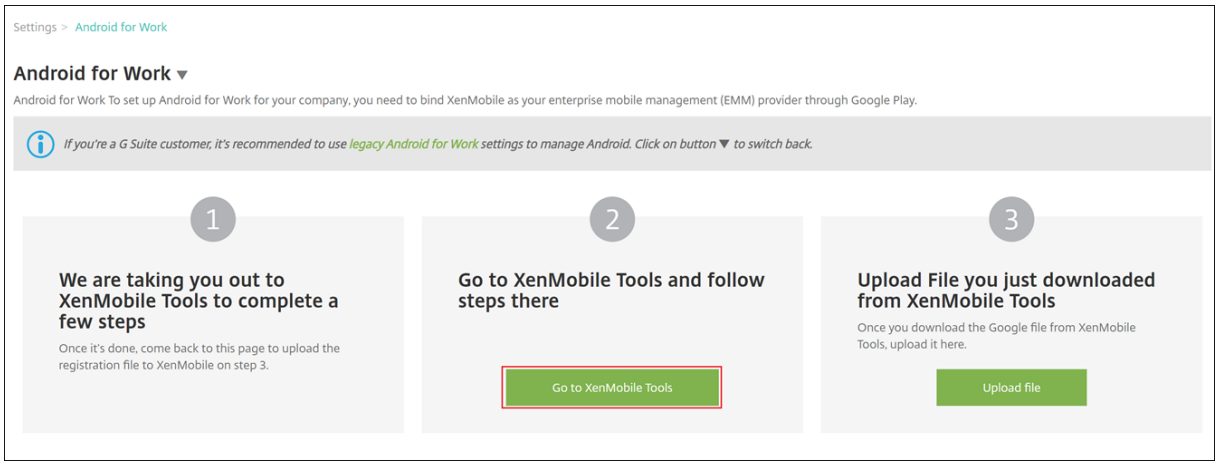
January 5, 2022

要配置旧版 Android Enterprise，Google Workspace（以前称为 G Suite）客户必须使用旧版 Android Enterprise 设置。

旧版 Android Enterprise 的要求：

- 可公开访问的域
- Google 管理员帐户
- 支持托管配置文件并且运行 Android 5.0+ Lollipop 的设备
- 安装了 Google Play 的 Google 帐户
- 用户设备上设置的工作配置文件

要开始配置旧版 Android Enterprise，请单击 XenMobile“设置”的 **Android Enterprise** 页面中的旧版 **Android Enterprise**。



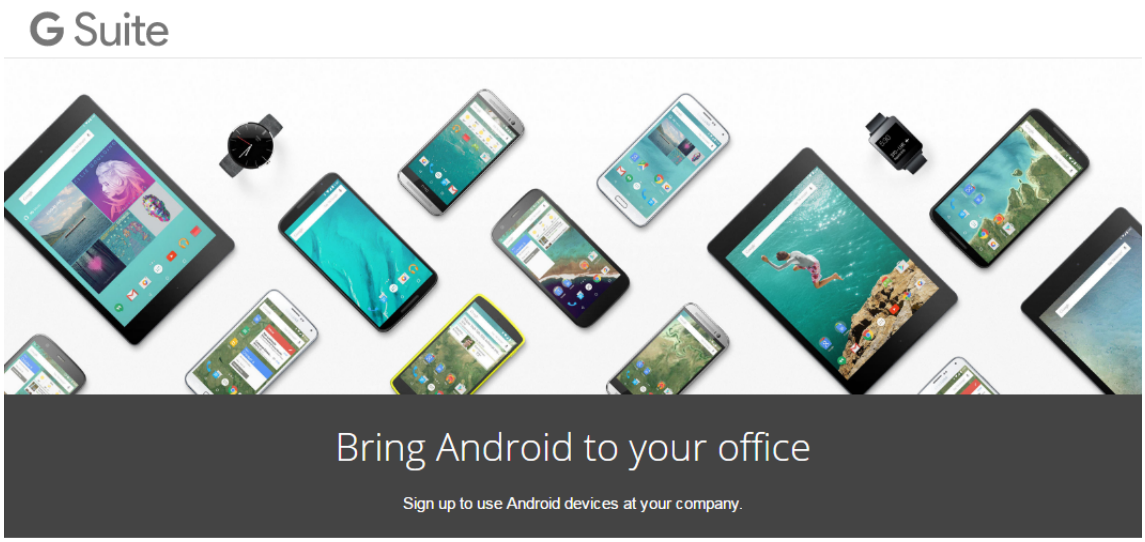
创建 **Android Enterprise** 帐户

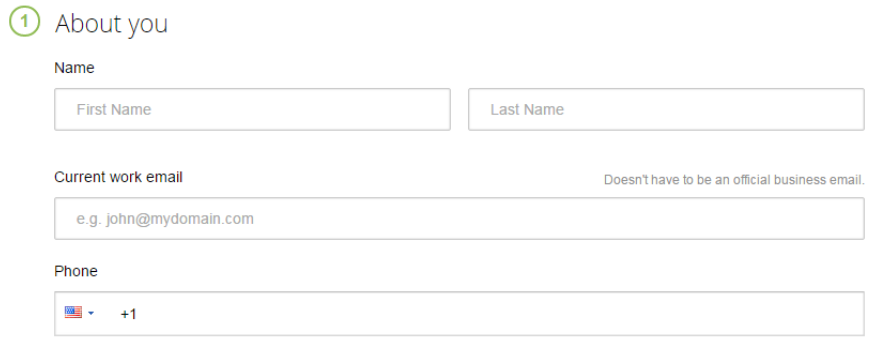
要设置 Android Enterprise 帐户，必须向 Google 验证您的域名。

如果已向 Google 验证您的域名，可以跳至此步骤：设置 Android Enterprise 服务帐户并下载 Android Enterprise 证书。

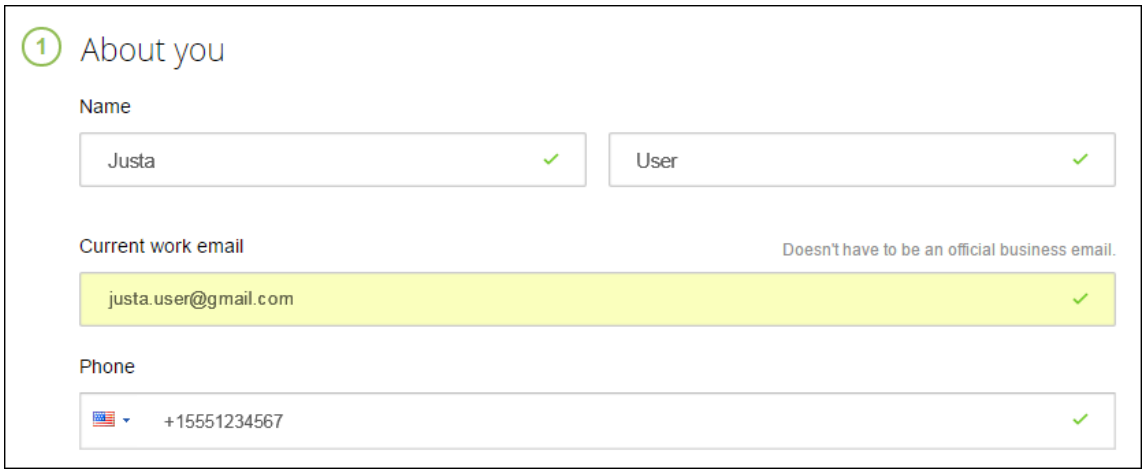
1. 导航到 https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK。

   此时将显示以下页面，您可以在此页面中键入管理员和公司信息。

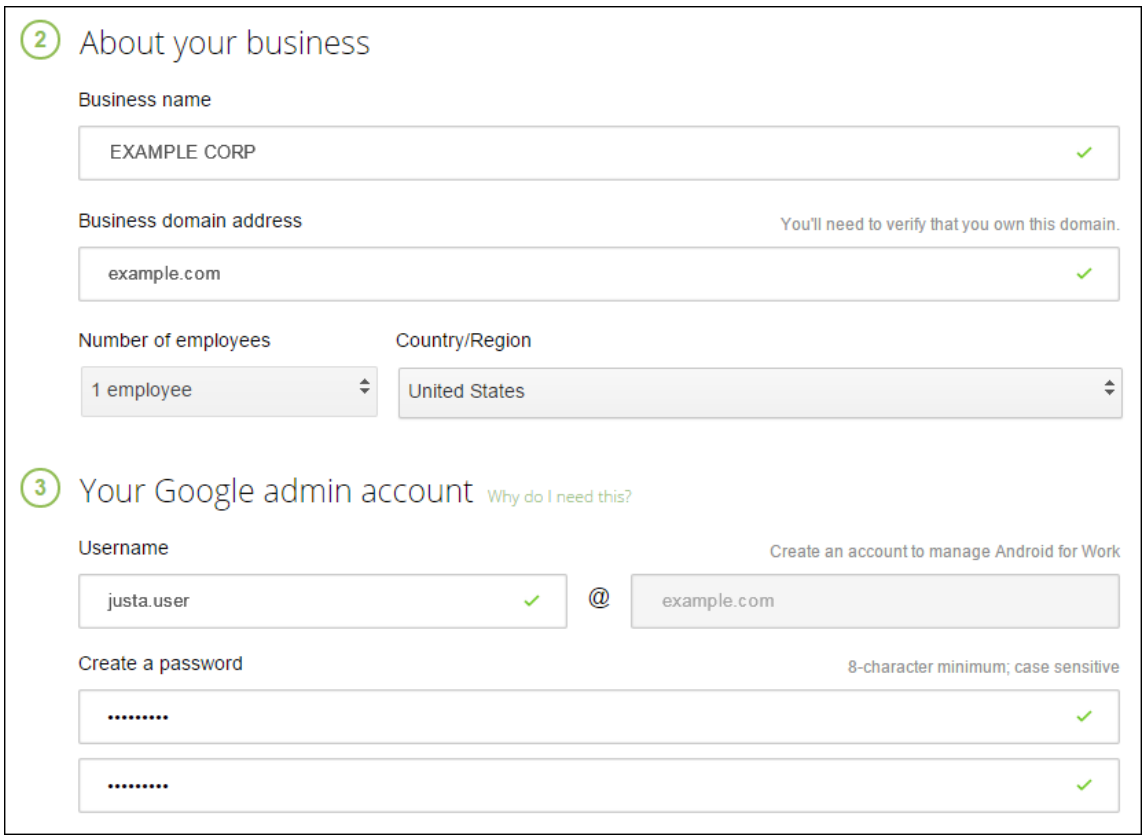




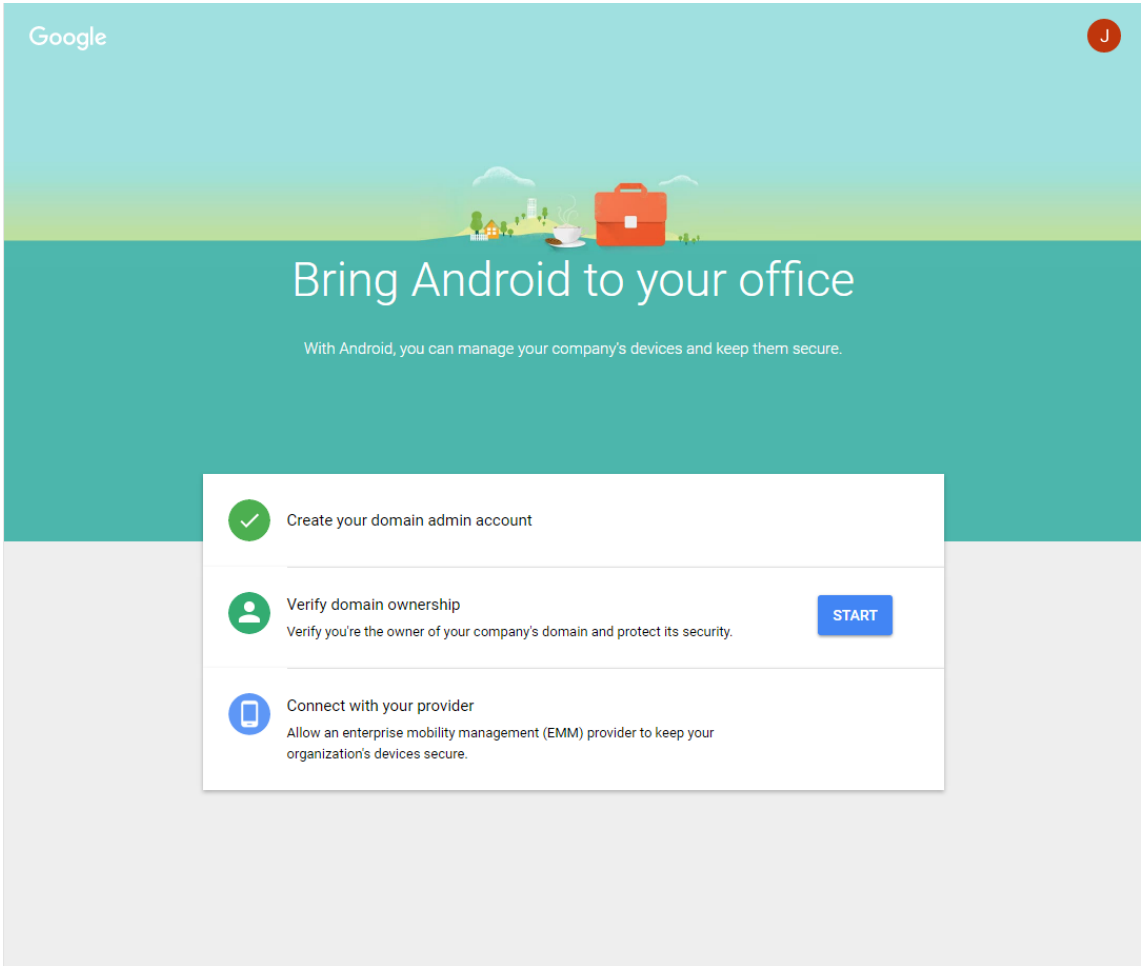
2. 键入管理员用户信息。



3. 键入您的公司信息（管理员帐户信息除外）。



此过程中的第一个步骤已完成，请继续查看下面的页面。



验证域所有权

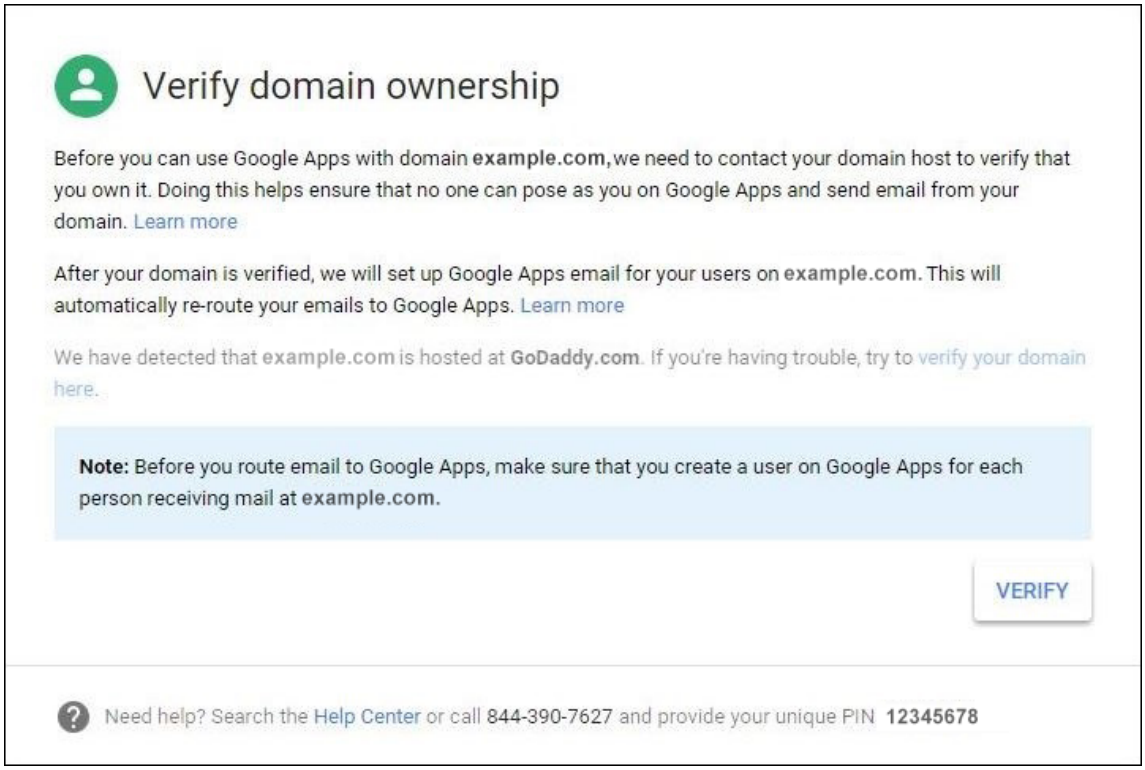
允许 Google 通过以下方式之一验证您的域：

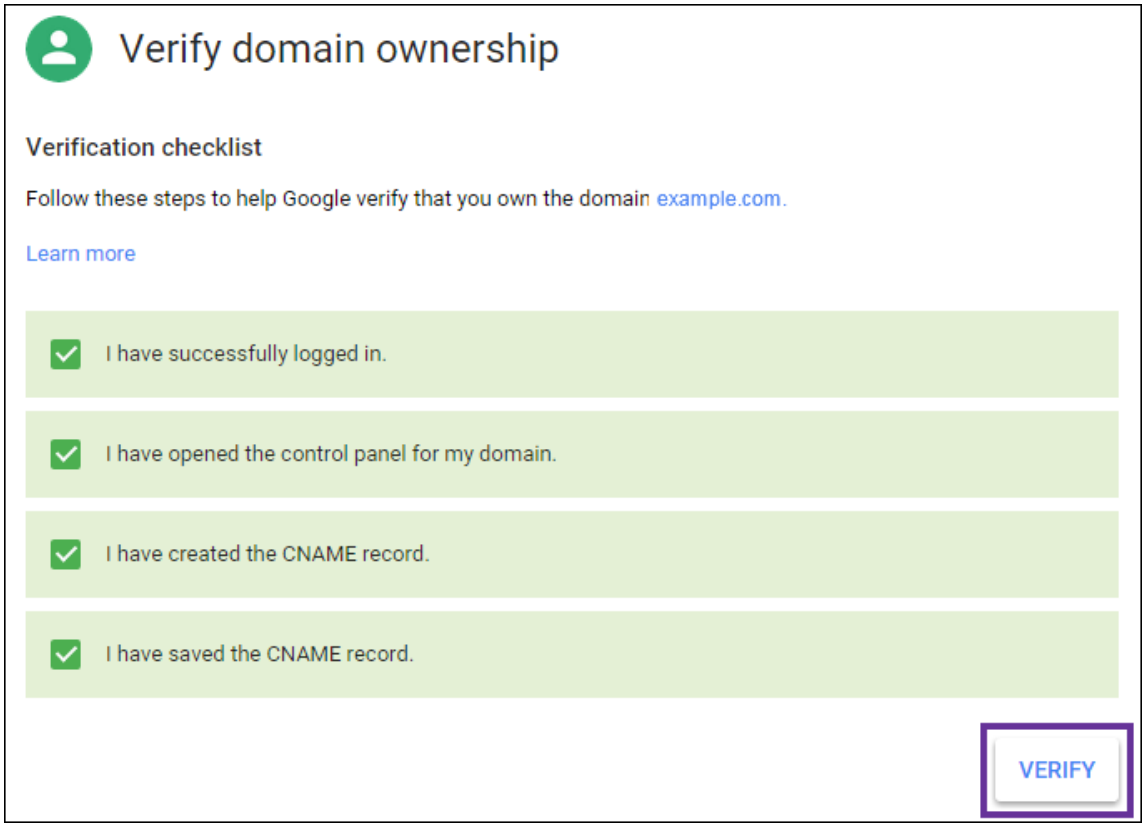
- 将 TXT 或 CNAME 记录添加到域主机的 Web 站点。
- 向域的 Web 服务器上载 HTML 文件。
- 向您的主页添加 <meta> 标记。Google 建议使用第一种方法。本文不包含验证域所有权的步骤，但您可以从以下网址找到所需的信息：https://support.google.com/a/answer/6248925。

1. 单击 **Start**（开始）开始验证您的域。

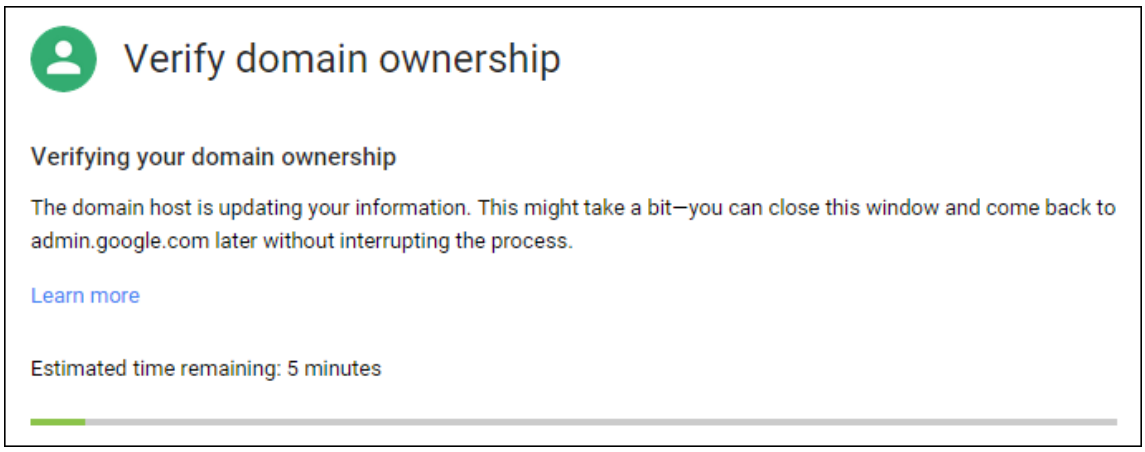
   此时将显示 **Verify domain ownership**（验证域所有权）页面。请按照此页面上显示的说明验证您的域。

2. 单击 **Verify**（验证）。

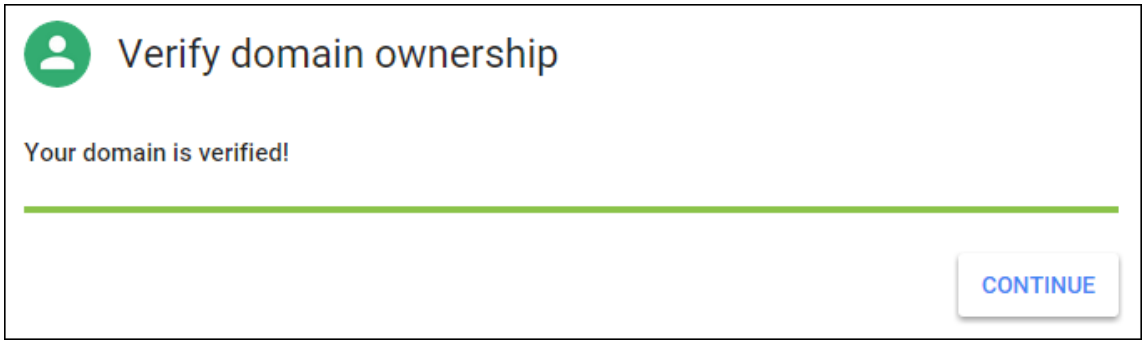




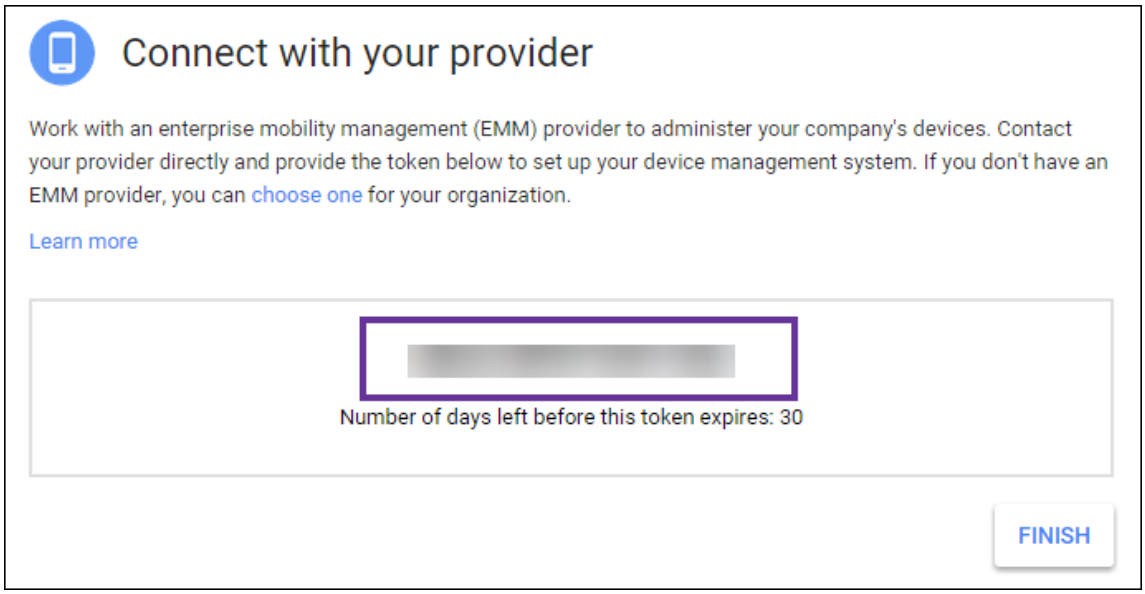
3. Google 验证您的域所有权。



4. 成功验证后，将显示以下页面。单击继续。



5. Google 创建一个需要向 Citrix 提供的 EMM 绑定令牌，您在配置 Android Enterprise 设置时需要使用该令牌。复制并保存该令牌；稍后的设置过程中需要使用该令牌。



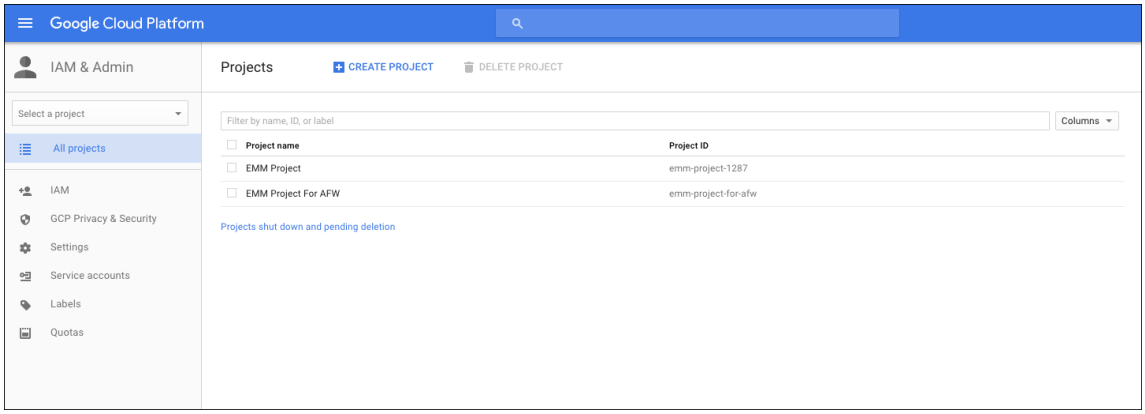
6. 单击 **Finish**（完成）以完成 Android Enterprise 设置。此时将显示一个页面，指示您已成功验证您的域。

创建 Android Enterprise 服务帐户后，可以登录 Google 管理控制台管理您的移动性管理设置。

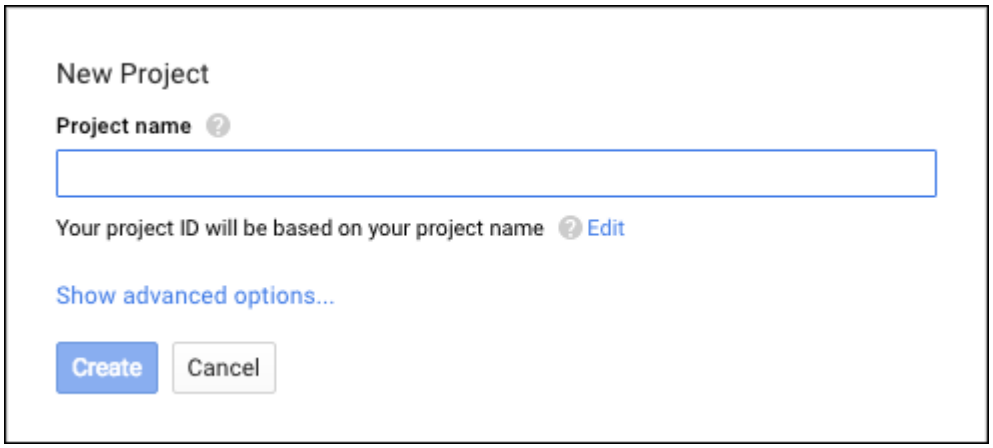
设置 **Android Enterprise** 服务帐户并下载 **Android Enterprise** 证书

要允许 XenMobile 联系 Google Play 和 Directory 服务，必须使用面向开发人员的 Google 项目门户创建新服务帐户。此服务帐户用于 XenMobile 与适用于 Android 的 Google 服务之间的服务器至服务器通信。有关使用的身份验证协议的详细信息，请访问 https://developers.google.com/identity/protocols/OAuth2ServiceAccount。

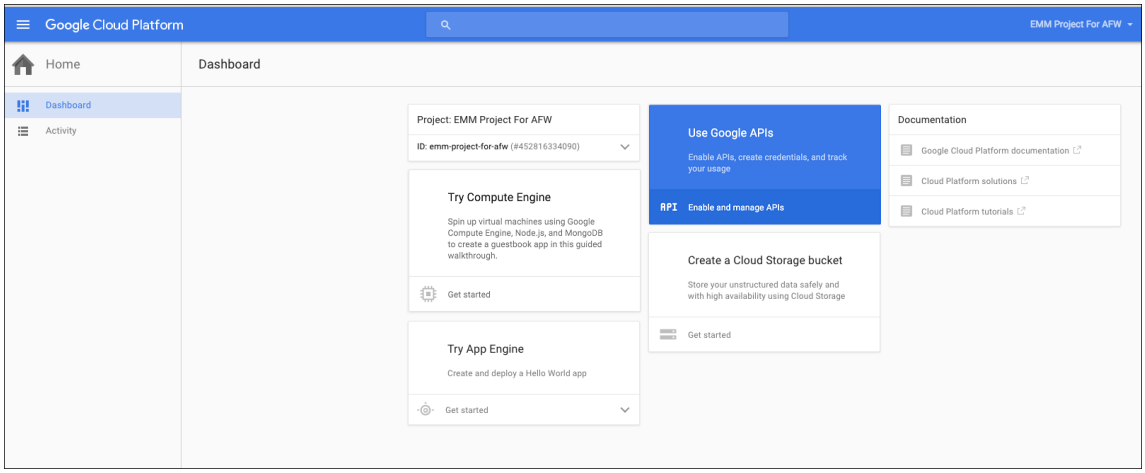
1. 在 Web 浏览器中，访问 https://console.cloud.google.com/project 并使用您的 Google 管理员凭据登录。
2. 在 **Projects**（项目）列表中，单击 **Create Project**（创建项目）。



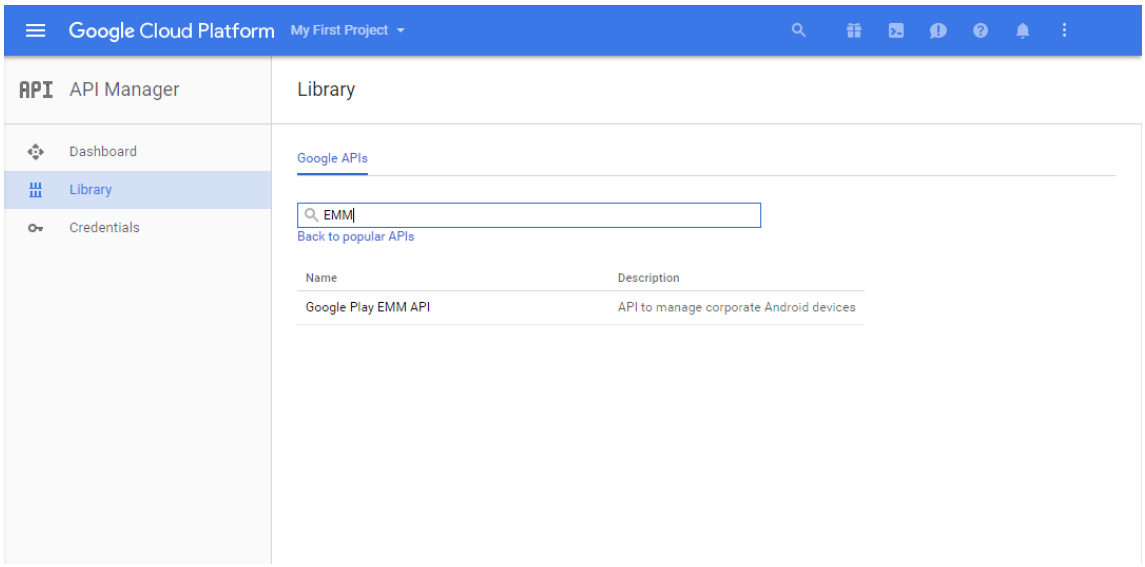
3. 在 **Project name**（项目名称）中，键入项目的名称。



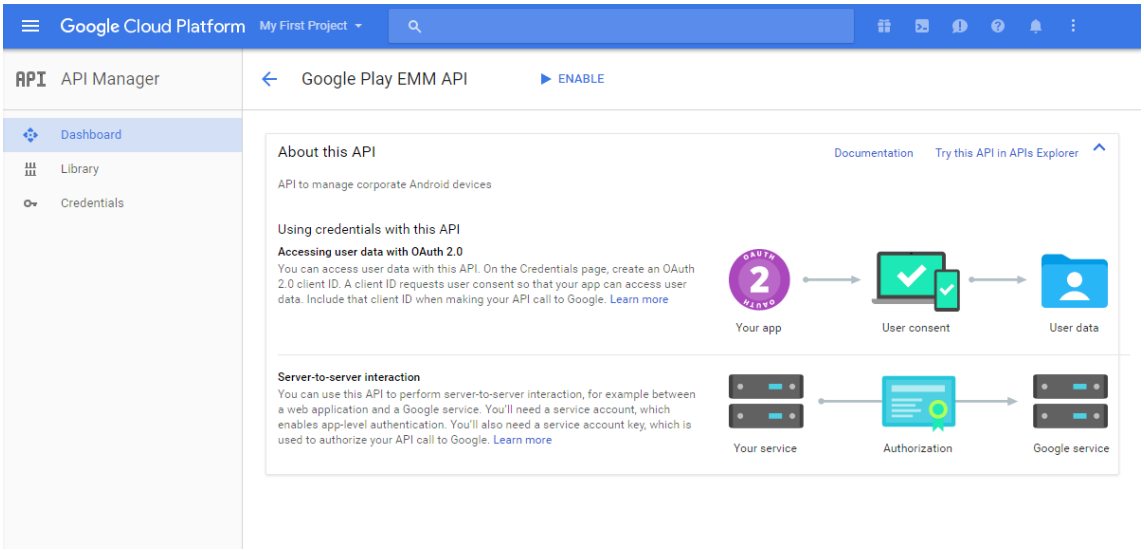
4. 在“Dashboard”（控制板）上，单击 **Use Google APIs**（使用 Google API）。



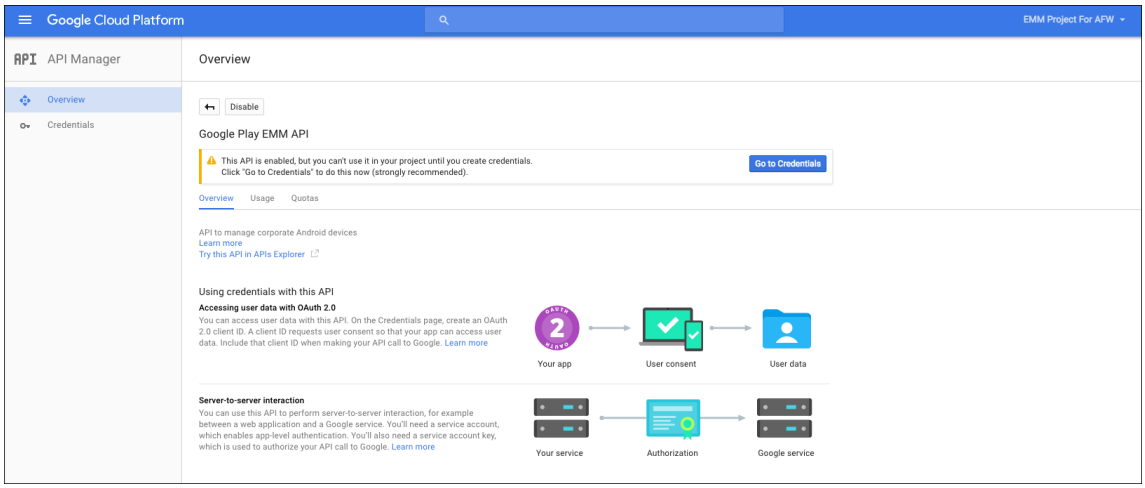
5. 单击 **Library**（库），在 **Search**（搜索）中，键入 **EMM**，然后单击搜索结果。



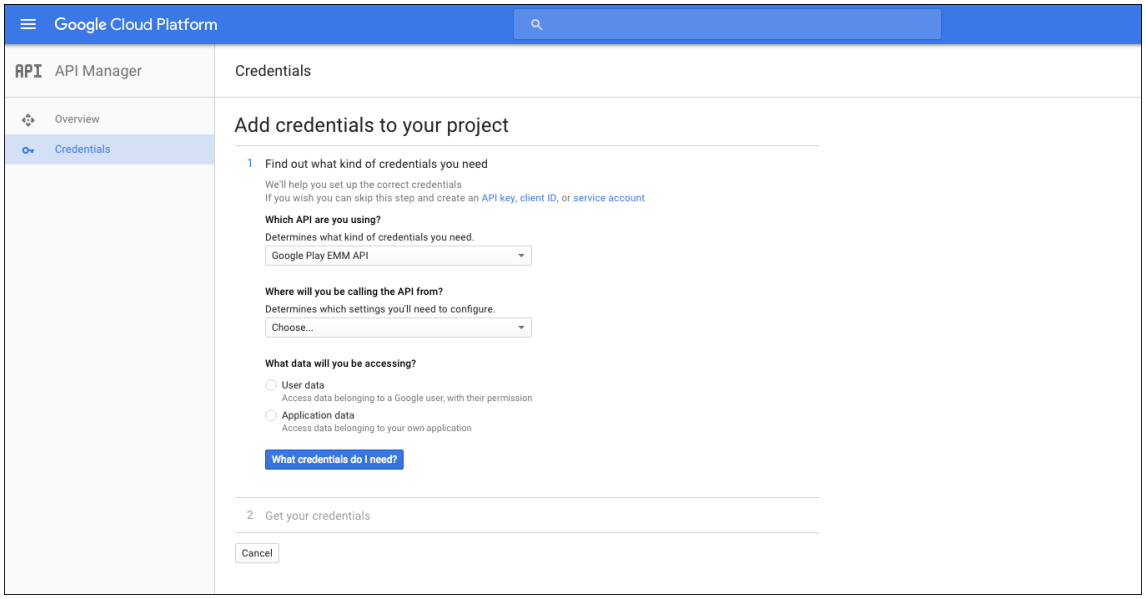
6. 在 **Overview**（概览）页面上，单击 **Enable**（启用）。



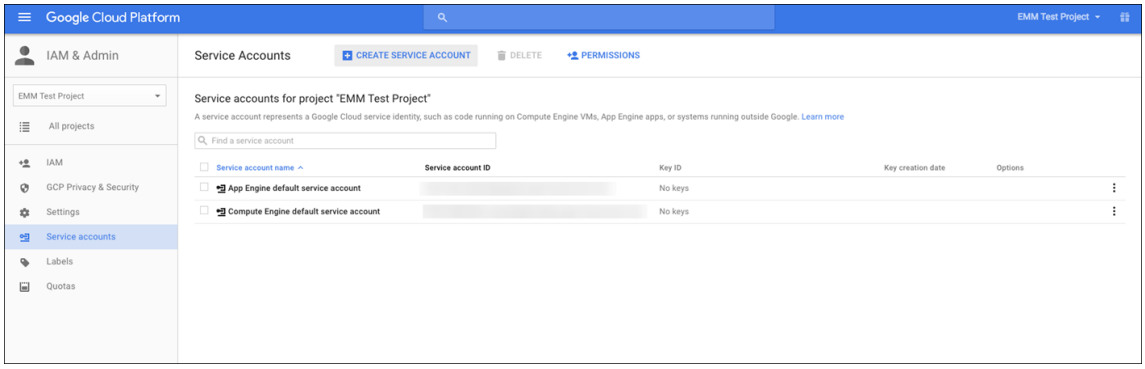
7. 在 **Google Play EMM API** 旁边，单击 **Go to Credentials**（转至凭据）。



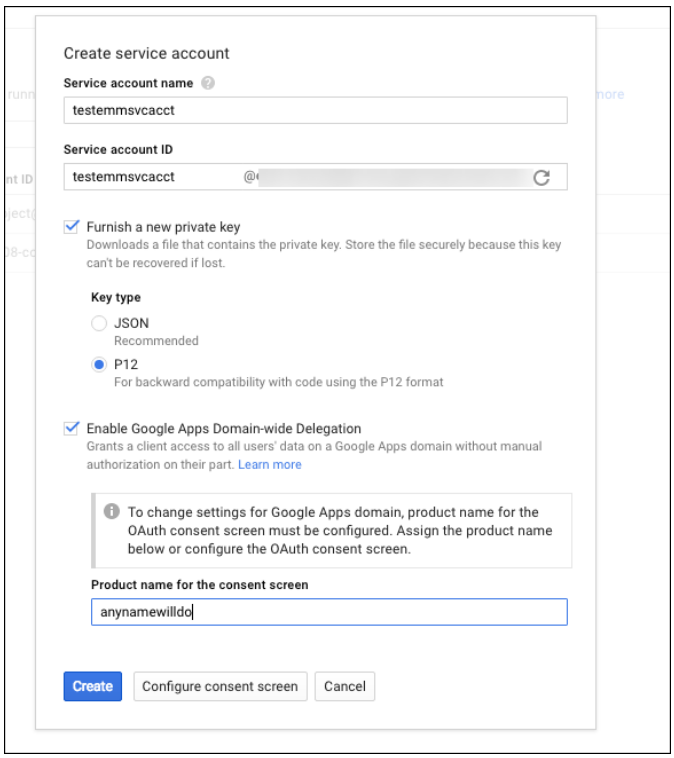
8. 在 **Add credentials to our project**（向我们的项目中添加凭据）列表中，在步骤 1 中单击 **service account**（服务帐户）。



9. 在 **Service Accounts**（服务帐户）页面上，单击 **Create Service Account**（创建服务帐户）。

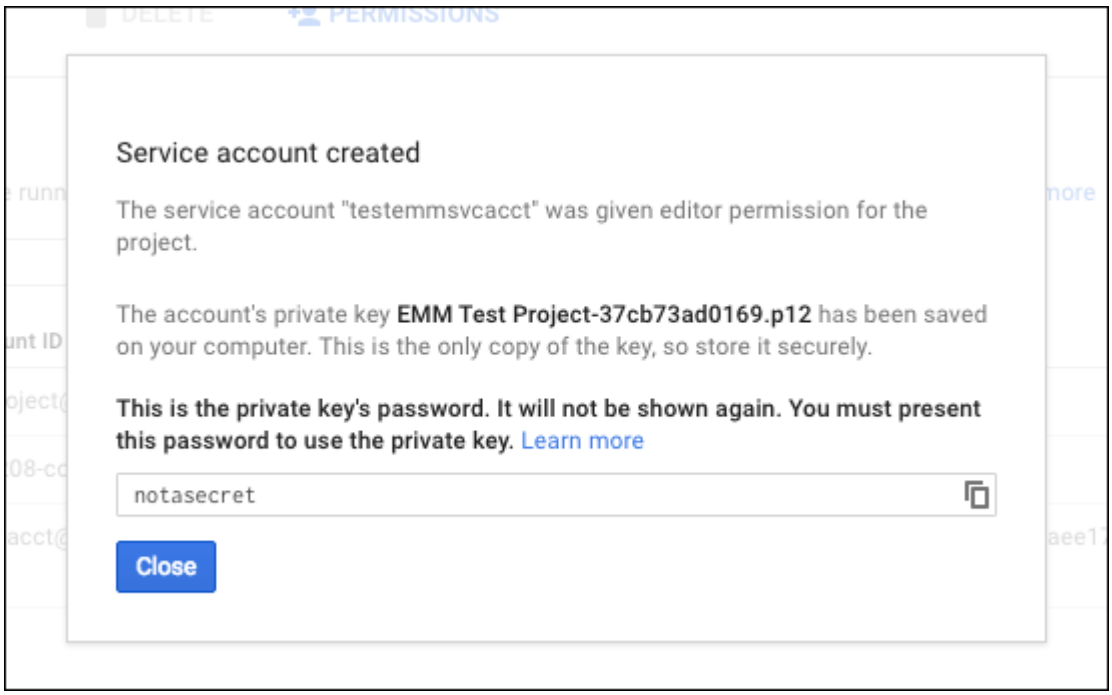


10. 在 **Create service account**（创建服务帐户）中，命名该帐户，然后选中 **Furnish a new private key**（提供新私钥）复选框。单击 **P12**，选中 **Enable Google Apps Domain-wide Delegation**（启用 Google Apps 域范围的委派）复选框，然后单击 **Create**（创建）。

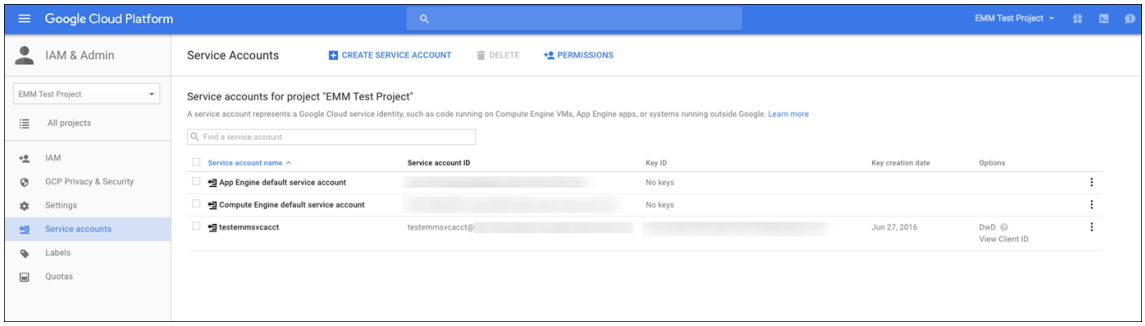


证书（P12 文件）将下载到您的计算机。请务必将该证书保存到一个安全的位置。

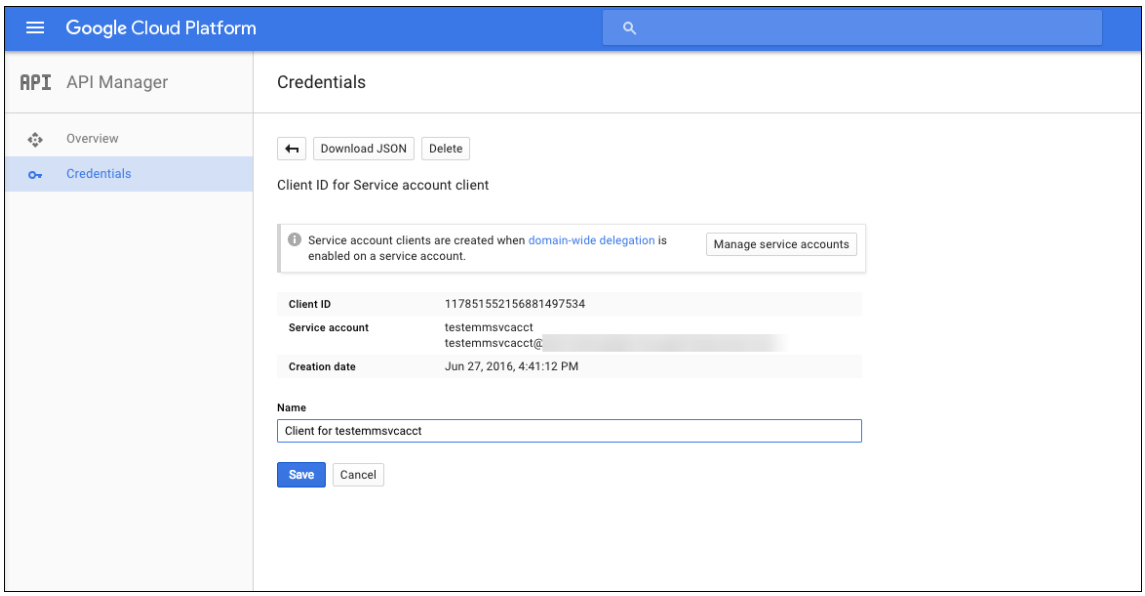
11. 在 **Service account created**（已创建服务帐户）确认屏幕上，单击 **Close**（关闭）。



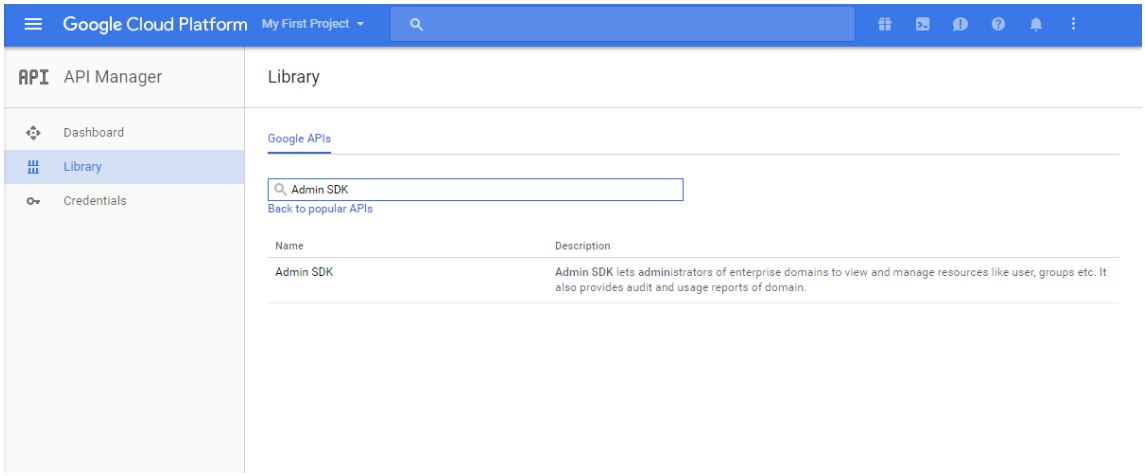
12. 在 **Permissions**（权限）中，单击 **Service accounts**（服务帐户），然后在您的服务帐户对应的 **Options**（选项）下方，单击 **View Client ID**（查看客户端 ID）。



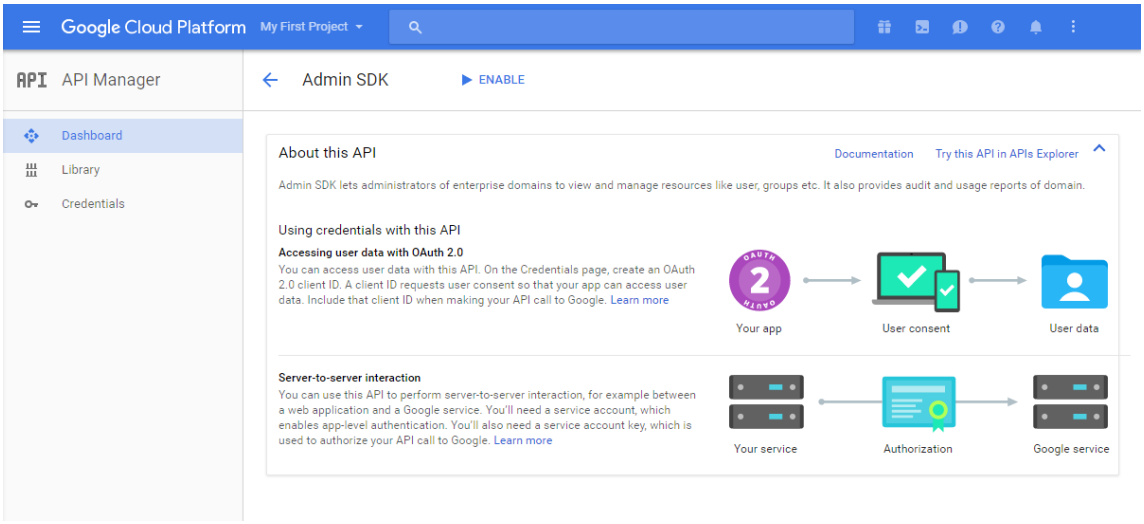
13. 此时将显示 Google 管理控制台上的帐户授权所需的详细信息。将 **Client ID**（客户端 ID）和 **Service account**（服务帐户）ID 复制到以后能够从中检索该信息的位置。需要提供此信息以及域名，才能发送给 Citrix 技术支持以便允许运行。



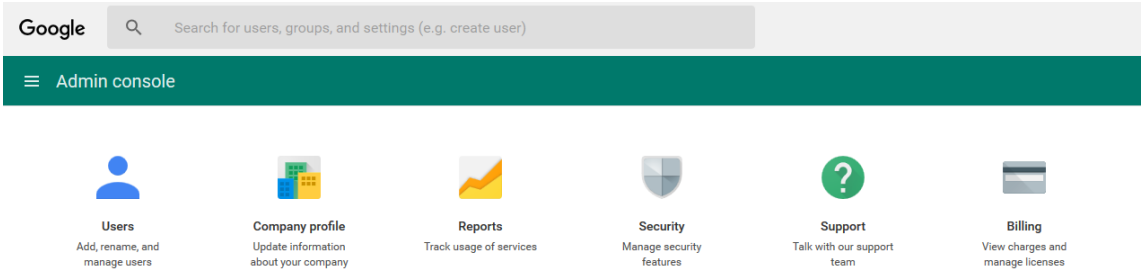
14. 在 **Library**（库）页面上，搜索 **Admin SDK**（管理 SDK），然后单击搜索结果。



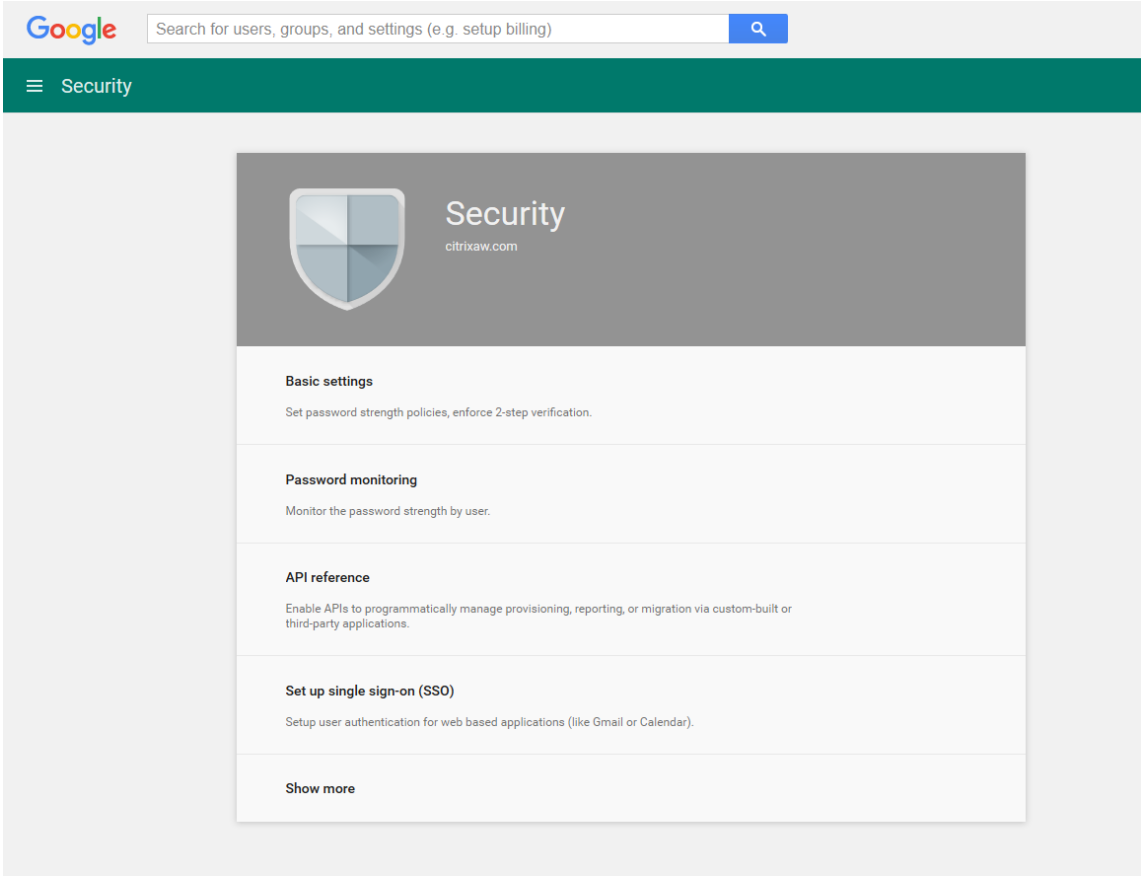
15. 在 **Overview**（概览）页面上，单击 **Enable**（启用）。

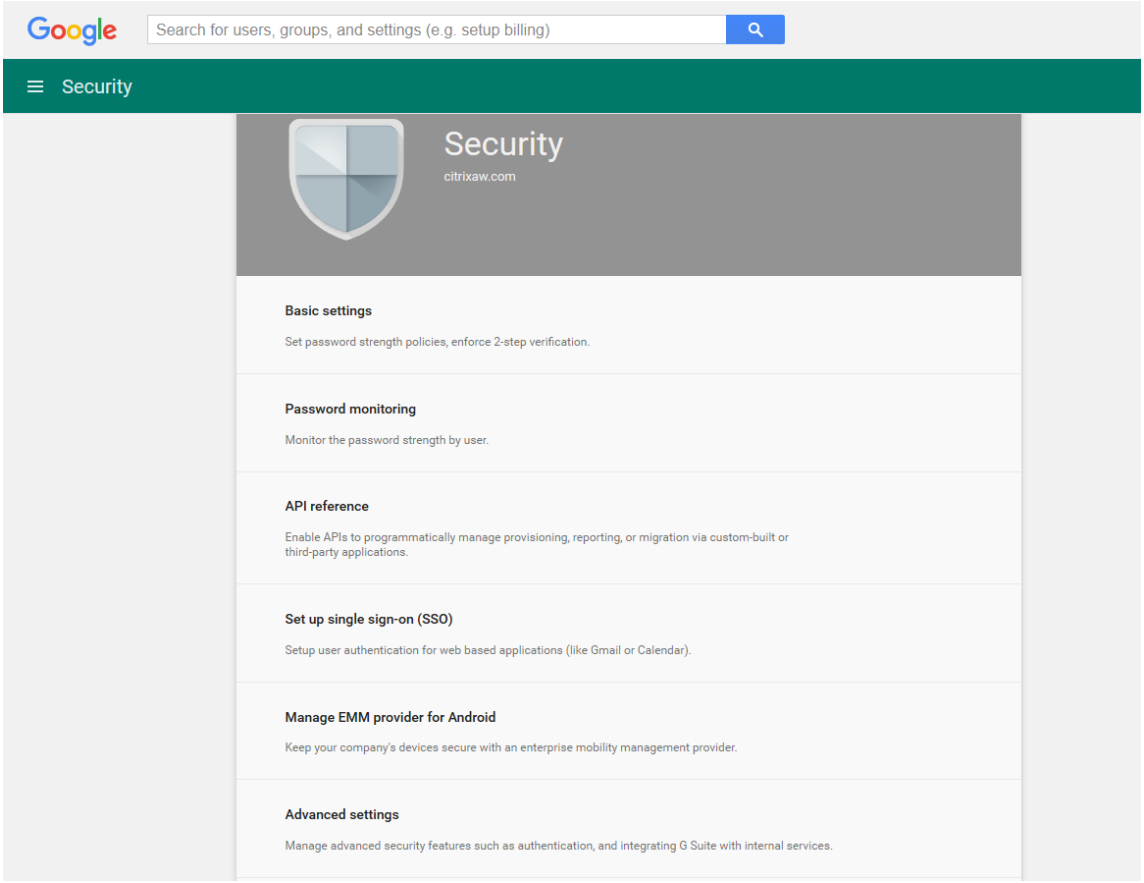


16. 打开您的域对应的 Google 管理控制台，然后单击 **Security**（安全）。

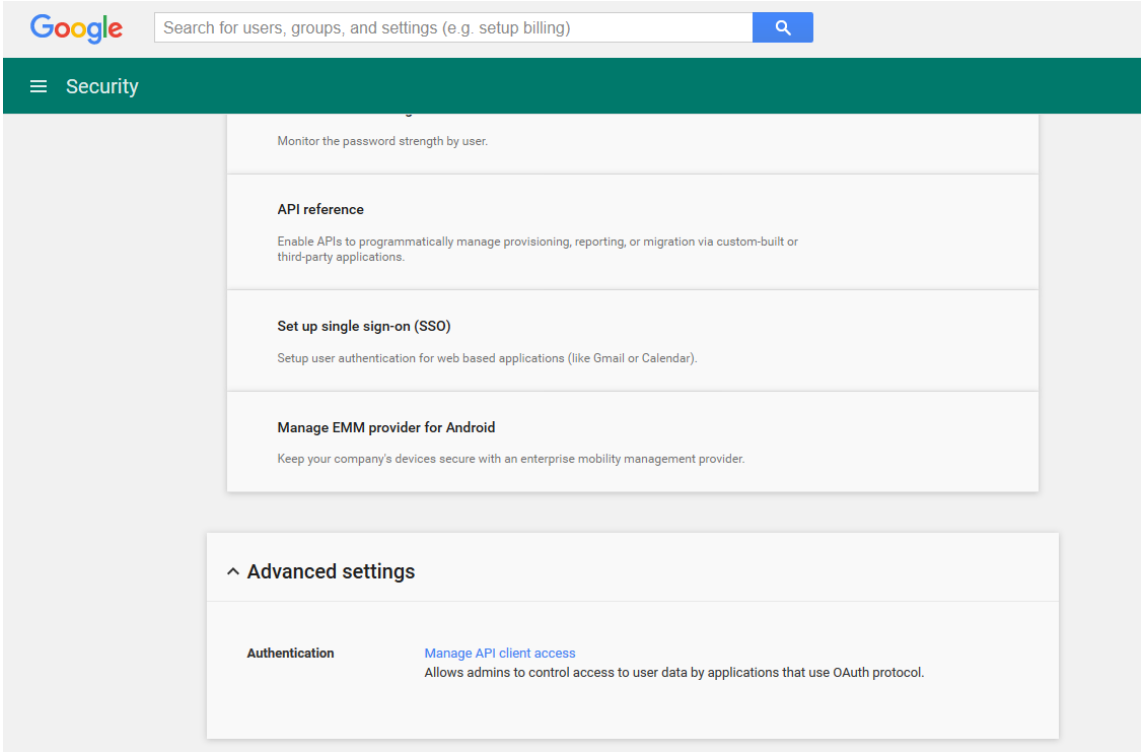


17. 在 **Settings**（设置）页面上，单击 **Show more**（显示更多），然后单击 **Advanced settings**（高级设置）。

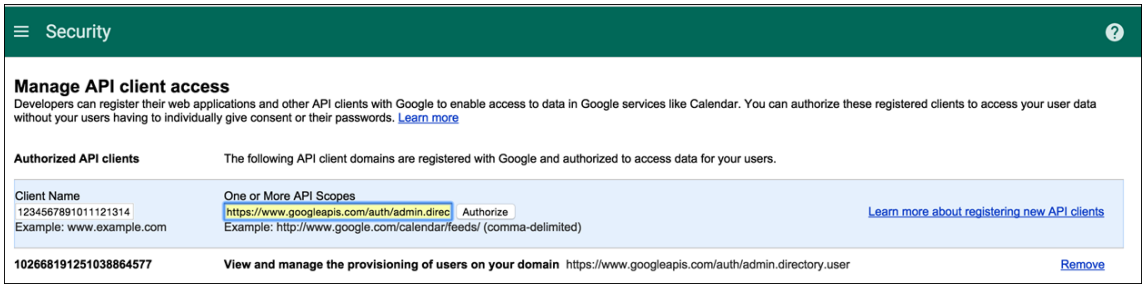




18. 单击 **Manage API client Access**（管理 API 客户端访问）。



19. 在 **Client Name**（客户端名称）中，输入您之前保存的客户端 ID，在 **One or More API Scopes**（一个或多个 API 作用域）中，键入 `https://www.googleapis.com/auth/admin.directory.user`，然后单击 **Authorize**（授权）。



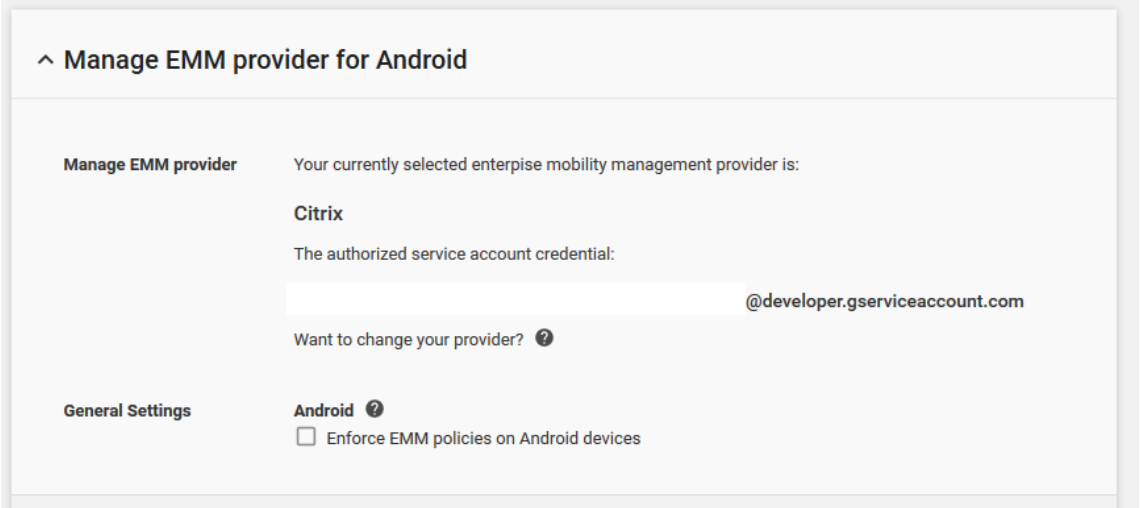
绑定到 **EMM**

必须先联系 Citrix 技术支持并提供您的域名、服务帐户和绑定令牌，才能使用 XenMobile 管理您的 Android 设备。Citrix 会将该令牌绑定到 XenMobile 作为企业移动性管理 (EMM) 提供程序。有关 Citrix 技术支持的联系信息，请参阅 Citrix 技术支持。

1. 要确认绑定，请登录 Google 管理门户，然后单击 **Security**（安全）。
2. 单击 **Manage EMM provider for Android**（管理适用于 Android 的 EMM 提供程序）。

   您将看到自己的 Google Android Enterprise 帐户绑定到 Citrix，用作 EMM 提供程序。

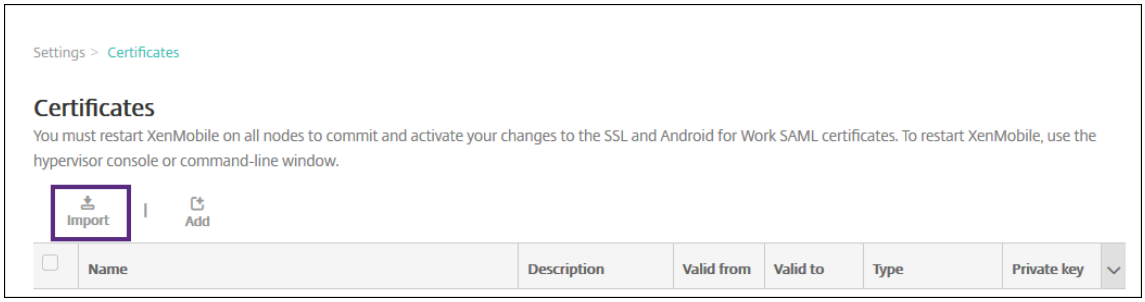
   确认令牌绑定后，可以开始使用 XenMobile 控制台管理您的 Android 设备。导入在步骤 14 中生成的 P12 证书。设置 Android Enterprise 服务器设置，启用基于 SAML 的单点登录 (SSO)，并至少定义一个 Android Enterprise 设备策略。



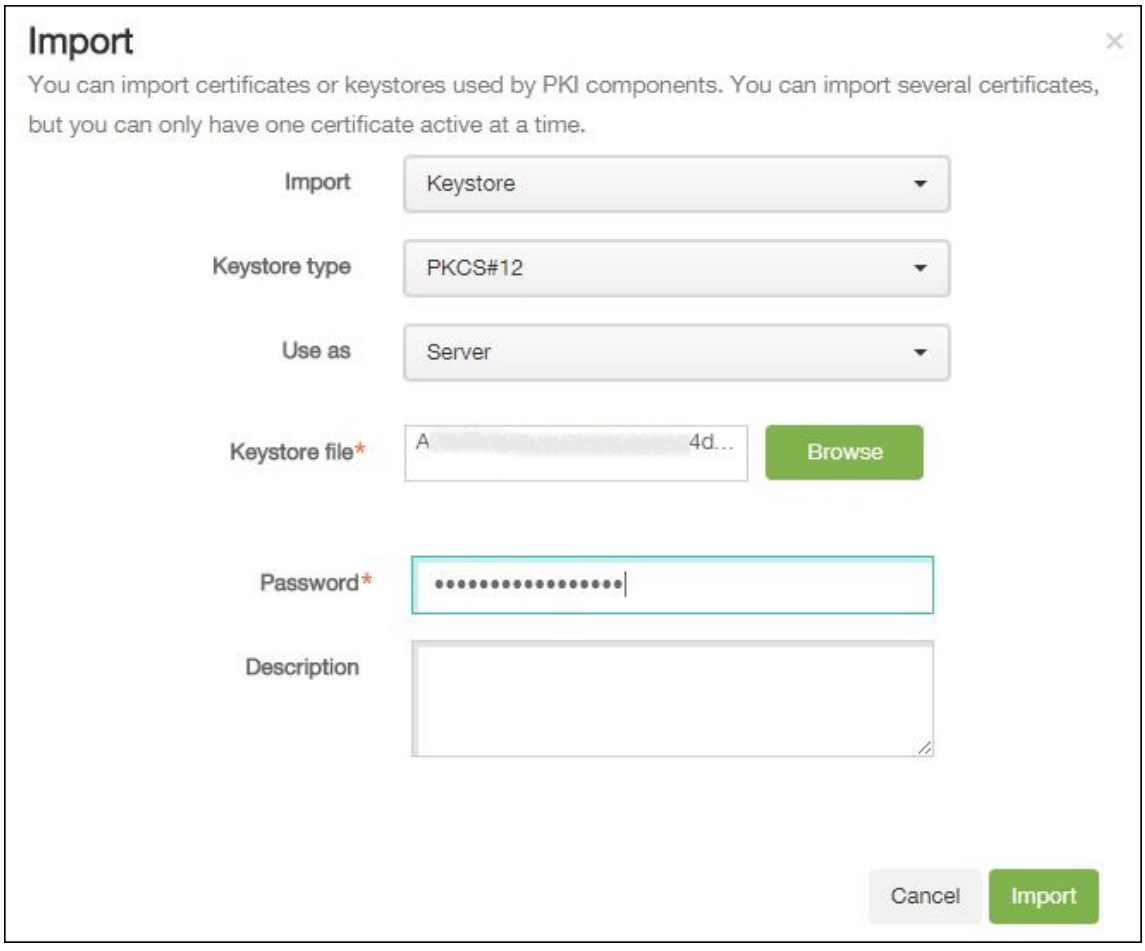
导入 **P12** 证书

请按照以下步骤导入 Android Enterprise P12 证书：

1. 登录 XenMobile 控制台。
2. 单击控制台右上角的齿轮图标以打开设置页面，然后单击证书。此时将显示证书页面。



3. 单击导入。此时将显示导入对话框。



配置以下设置：

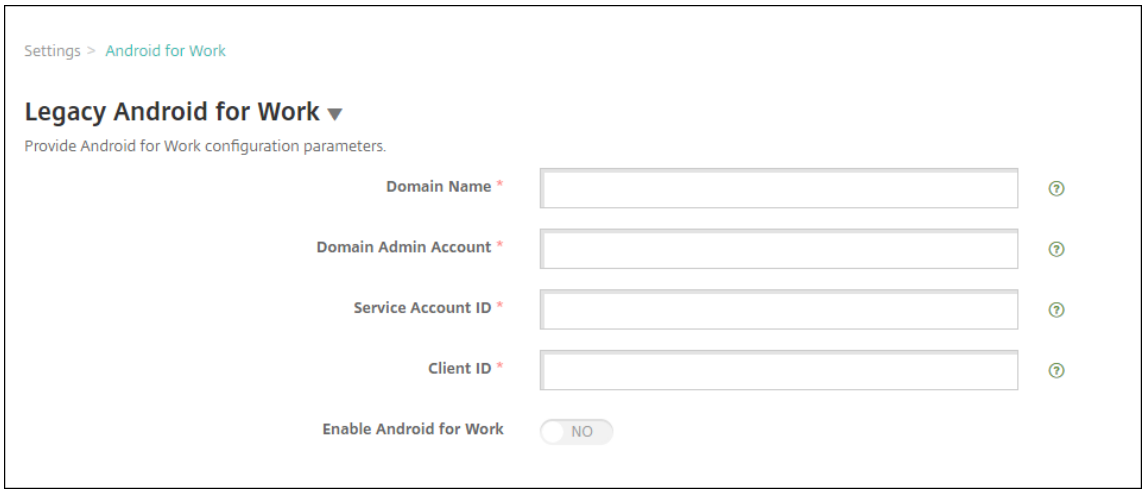
- 导入：在列表中，单击密钥库。
- 密钥库类型：在列表中，单击 **PKCS#12**。
- 用作：在列表中，单击服务器。
- 密钥库文件：单击浏览，然后导航到 P12 证书。
- 密码：键入密钥库密码。

- 说明：（可选）键入证书的说明。

4. 单击导入。

设置 **Android Enterprise** 服务器设置

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **Android Enterprise**。此时将显示 **Android Enterprise** 页面。

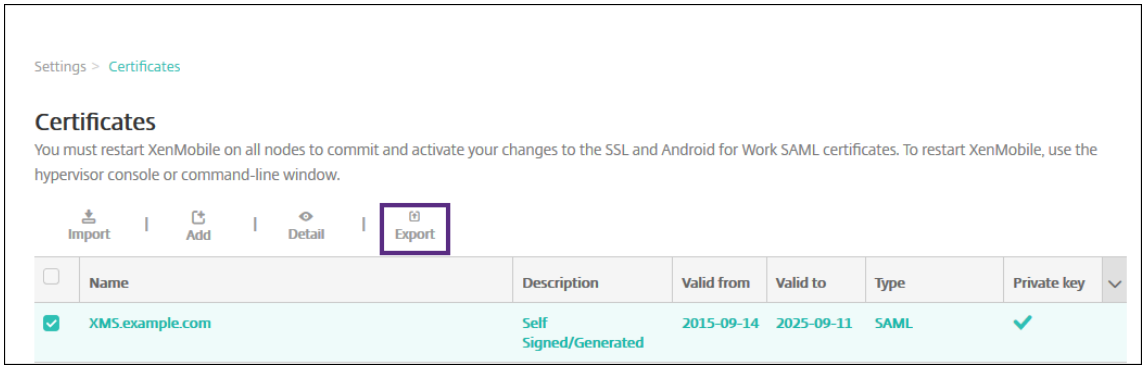


配置以下设置，然后单击保存。

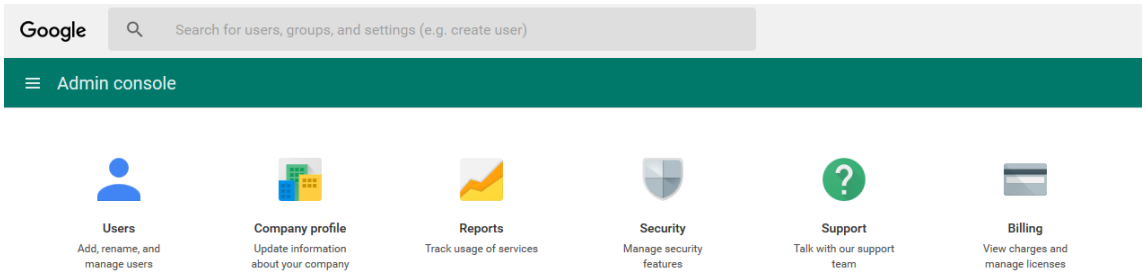
- 域名：键入您的 Android Enterprise 域名，例如 domain.com。
- 域管理员帐户：键入您的域管理员的用户名，例如，用于 Google 开发人员门户的电子邮件帐户。
- 服务帐户 **ID**:键入您的服务帐户 ID,例如,Google 服务帐户中关联的电子邮件 (serviceaccountemail@xxxxxxx.iam.gserviceaccount.com)。
- 客户端 **ID**：键入您的 Google 服务帐户的数字客户端 ID。
- 启用 **Android Enterprise**：选择启用或禁用 Android Enterprise。

启用基于 **SAML** 的单点登录

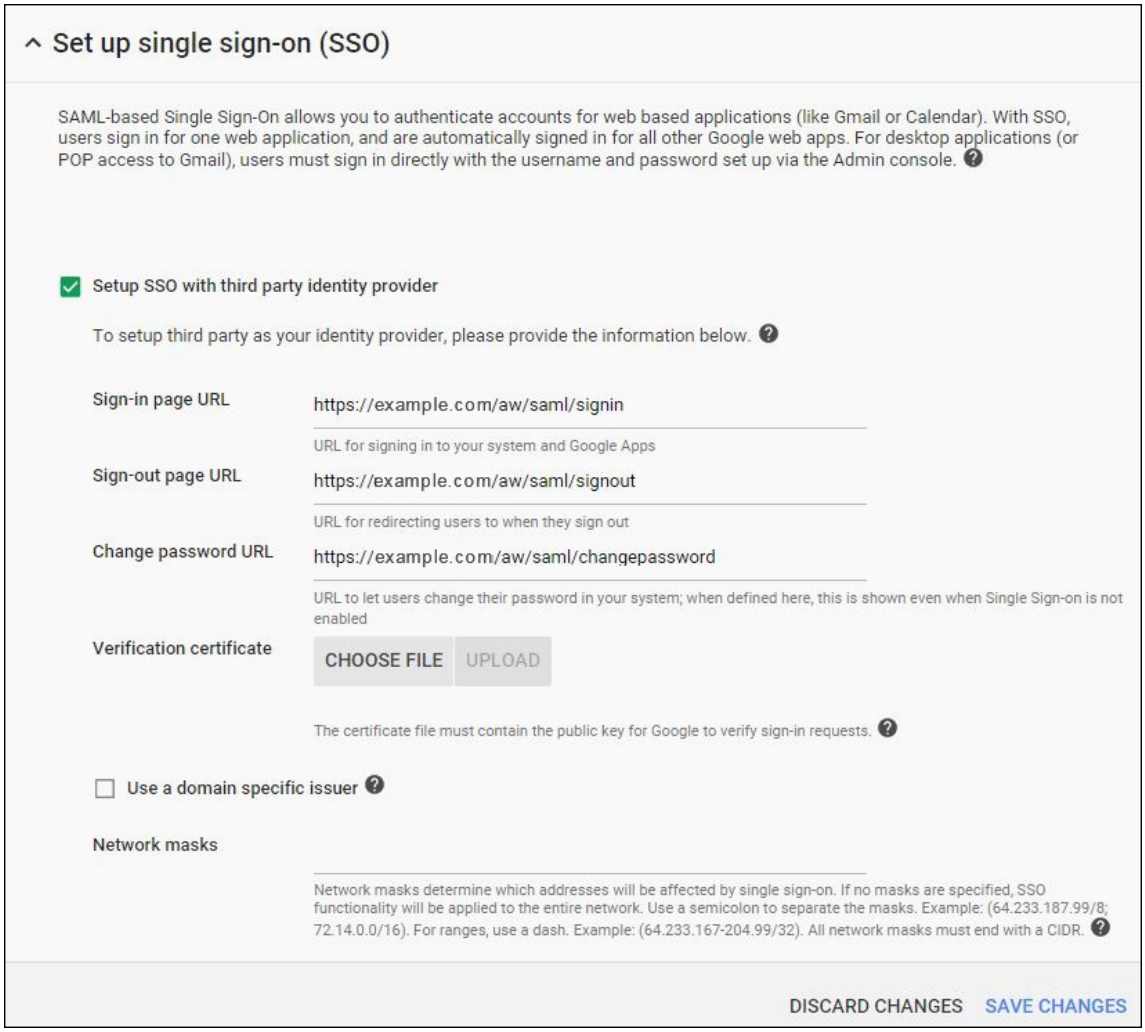
1. 登录 XenMobile 控制台。
2. 单击控制台右上角的齿轮图标。此时将显示设置页面。
3. 单击证书。此时将显示证书页面。



4. 在证书列表中，单击 SAML 证书。
5. 单击导出并将证书保存到您的计算机。
6. 使用您的 Android Enterprise 管理员凭据登录 Google 管理门户。有关门户的访问权限，请参阅 Google 管理门户。
7. 单击 **Security**（安全）。



8. 在 **Security**（安全）下方，单击 **Set up single sign-on** (SSO)（设置单点登录 (SSO)），然后配置以下设置。

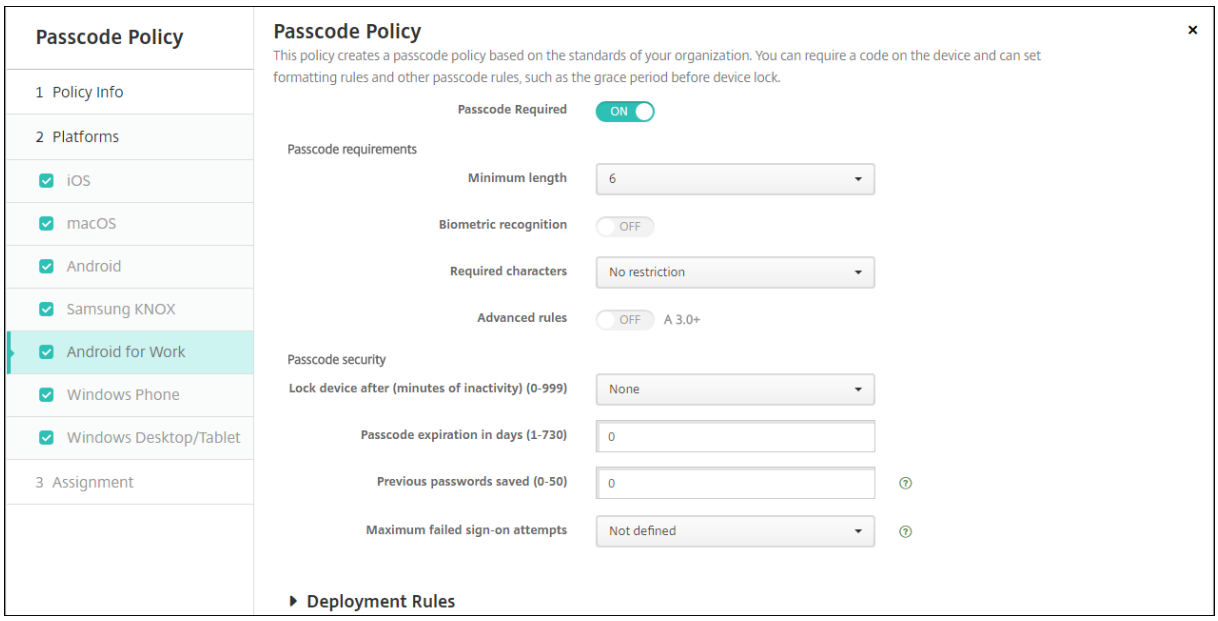


- **Sign-in page URL**（登录页面 **URL**）：键入用户登录您的系统和 Google Apps 使用的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/signin`。
- **Sign out page URL**（注销页面 **URL**）：键入用户注销时被定向到的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/signout`。
- **Change password URL**（更改密码 **URL**）：键入 URL 以允许用户更改其系统中的密码。例如：`https://<Xenmobile-FQDN>/aw/saml/changepassword`。如果定义了此字段，用户将看到此提示，即使 SSO 不可用时也是如此。
- **Verification certificate**（验证证书）：单击 **CHOOSE FILE**（选择文件），然后导航到从 XenMobile 导出的 SAML 证书。

9. 单击 **SAVE CHANGES**（保存更改）。

设置 **Android Enterprise** 设备策略

设置通行码策略，以便用户在首次注册时必须在其设备上创建通行码。



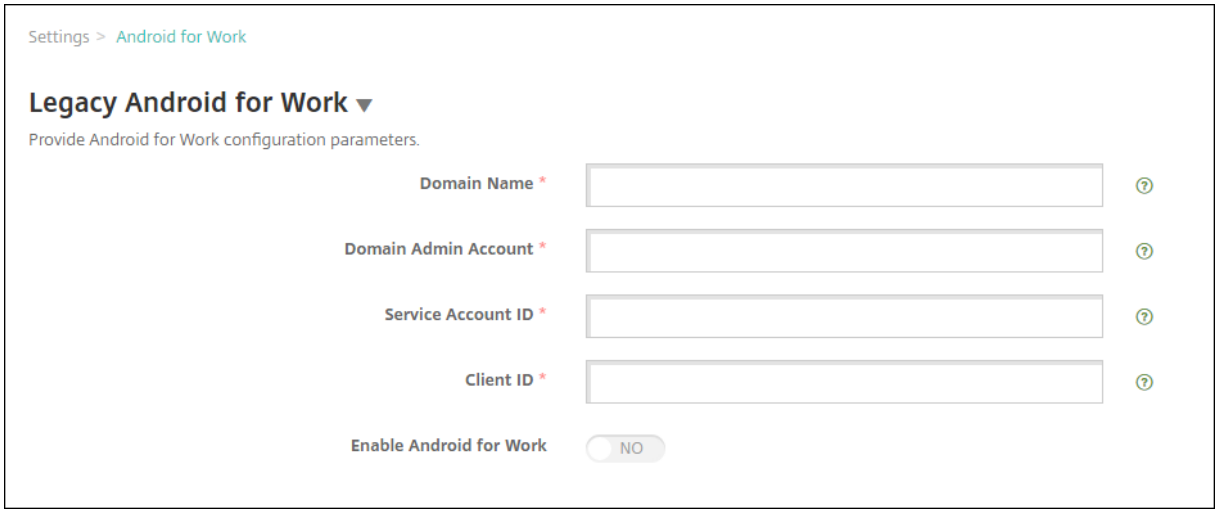
设置任何设备策略的基本步骤如下。

1. 登录 XenMobile 控制台。
2. 单击配置，然后单击设备策略。
3. 单击添加，然后在添加新策略对话框中选择要添加的策略。在此示例中，请单击通行码。
4. 完成策略信息页面。
5. 单击 **Android Enterprise** 并配置策略设置。
6. 将策略分配到交付组。

配置 **Android Enterprise** 帐户设置

必须在 XenMobile 中设置 Android Enterprise 域和帐户信息，才能开始管理设备上的 Android 应用程序和策略。首先，请在 Google 上完成 Android Enterprise 设置任务以设置域管理员，并获取服务帐户 ID 和绑定令牌。

1. 在 XenMobile 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. 在服务器下方，单击 **Android Enterprise**。此时将显示 **Android Enterprise** 配置页面。



1. 在 **Android Enterprise** 页面上，配置以下设置：
   - 域名：键入域名。
   - 域管理员帐户：键入您的域管理员用户名。
   - 服务帐户 **ID**：键入您的 Google 服务帐户 ID。
   - 客户端 **ID**：键入您的 Google 服务帐户的客户端 ID。
   - 启用 **Android Enterprise**：选择是否启用 Android Enterprise。
2. 单击保存。

为 **XenMobile** 设置 **Google Workspace** 合作伙伴访问权限

Chrome 的某些端点管理功能使用 Google 合作伙伴 API 在 XenMobile 与您的 Google Workspace 域之间进行通信。例如，XenMobile 要求对管理隐身模式和来宾模式等 Chrome 功能的设备策略使用 API。

要启用合作伙伴 API，请在 XenMobile 控制台中设置您的 Google Workspace 域，然后配置 Google Workspace 帐户。

在 **XenMobile** 中设置 **Google Workspace** （以前称为 **G Suite**）域

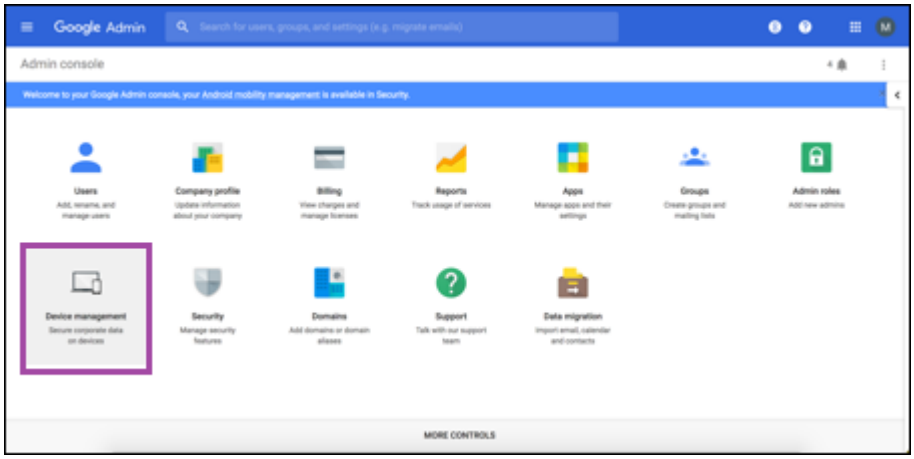
要允许 XenMobile 在您的 Google Workspace 域中与 API 进行通信，请转至设置 **> Google Chrome** 配置并配置设置。

- **G Suite** 域：托管 XenMobile 所需的 API 的 Google Workspace 域。
- **G Suite** 管理员帐户： G Suite 域的管理员帐户。
- **G Suite** 客户端 **ID**： Citrix 的客户端 ID。请使用此值为您的 Google Workspace 域配置合作伙伴访问权限。
- **G Suite** 企业 **ID**：您的帐户的客户端 ID，从您的 Google 企业帐户填充。

启用对您的 **Google Workspace** 域中的设备和用户的合作伙伴访问权限

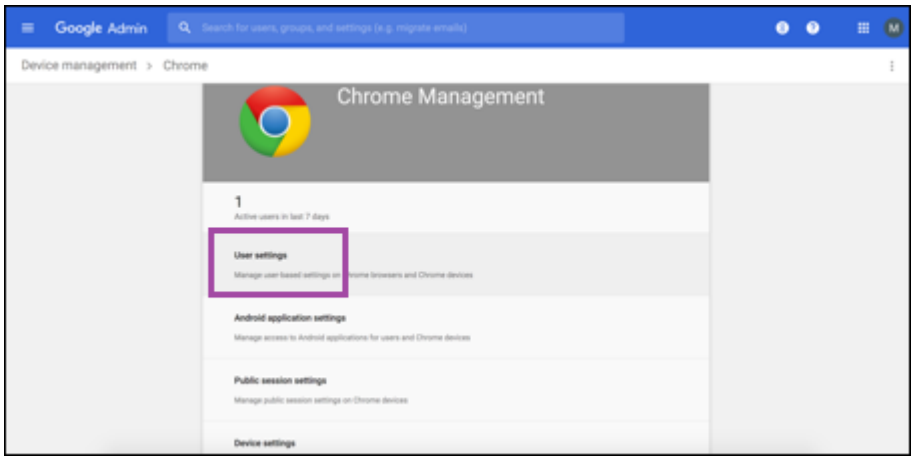
1. 登录 Google 管理控制台：https://admin.google.com

2. 单击 **Device Management**（设备管理）。



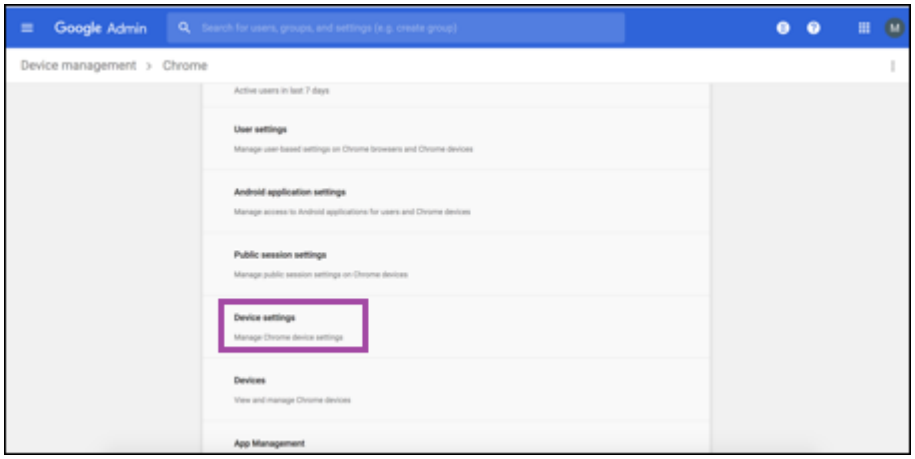
3. 单击 **Chrome management**（Chrome 管理）。

4. 单击 **User settings**（用户设置）。

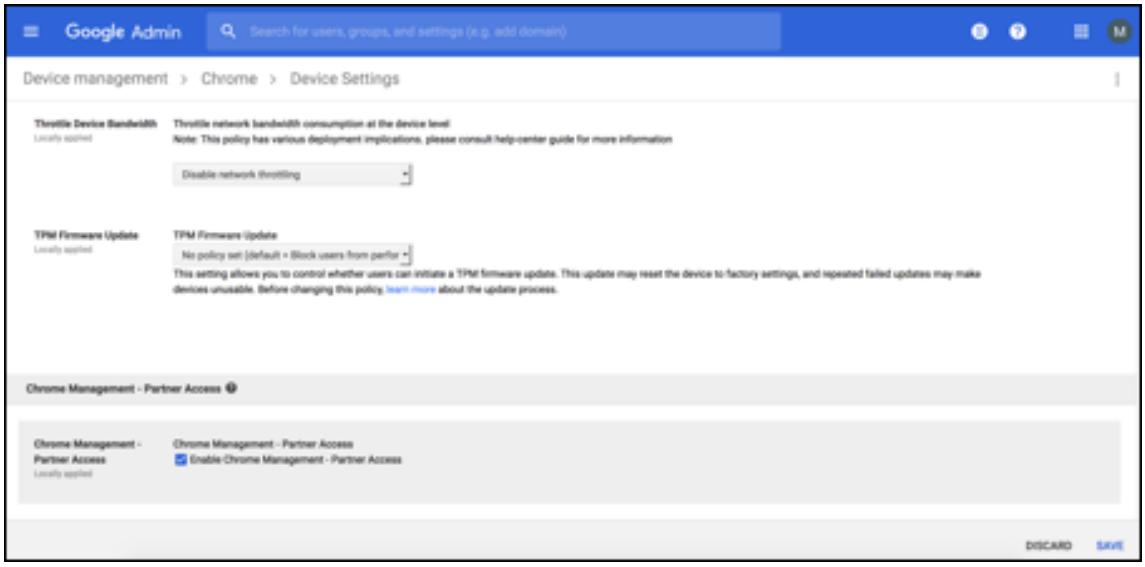


5. 搜索 **Chrome Management - Partner Access**（Chrome 管理 - 合作伙伴访问权限）。

6. 选中 **Enable Chrome Management - Partner Access**（启用 Chrome 管理 - 合作伙伴访问权限）复选框。
7. 同意您理解并希望启用合作伙伴访问权限。单击保存。
8. 在 Chrome 管理页面中，单击 **Device Settings**（设备设置）。



9. 搜索 **Chrome Management - Partner Access**（Chrome 管理 - 合作伙伴访问权限）。

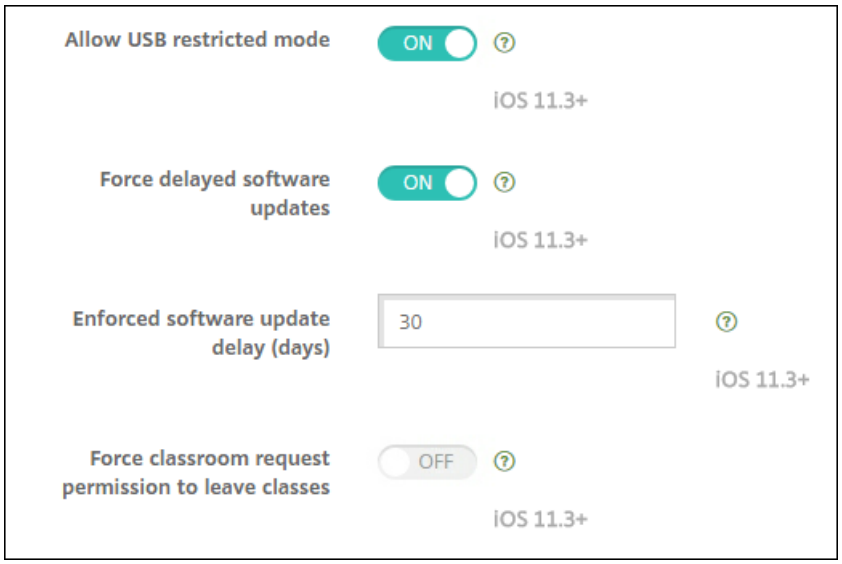


10. 选中 **Enable Chrome Management - Partner Access**（启用 Chrome 管理 - 合作伙伴访问权限）复选框。
11. 同意您理解并希望启用合作伙伴访问权限。单击保存。
12. 转至 **Security**（安全）页面，然后单击 **Advanced Settings**（高级设置）。

13. 单击 **Manage API client Access**（管理 API 客户端访问）。
14. 在 XenMobile 控制台中，转至设置 **> Google Chrome** 配置并复制 Google Workspace 客户端 ID 的值。然后，返回到 **Manage API client Access**（管理 API 客户端访问）页面并将复制的值粘贴到 **Client Name**（客户端名称）字段中。
15. 在 **One or More API Scopes**（一个或多个 API 范围）中，添加 URL：`https://www.googleapis.com/auth/chromedevicemanagementapi`

16. 单击 **Authorize**（授权）。

    此时将显示消息 “Your settings have been saved”（已保存您的设置）。



注册 **Android Enterprise** 设备

如果您的设备注册过程要求用户输入用户名或用户 ID，接受的格式取决于将 XenMobile Server 配置为按用户主体名称 (UPN) 还是 SAM 帐户名称来搜索用户。

如果 XenMobile Server 配置为按 UPN 搜索用户，用户必须按以下格式输入 UPN：

- 用户名 @ 域

如果 XenMobile Server 配置为按 SAM 搜索用户，用户必须按以下格式之一输入 SAM：

- 用户名 @ 域
- 域\用户名

要确定为您的 XenMobile Server 配置的用户名类型，请执行以下操作：

1. 在 XenMobile Server 控制台中，单击右上角的齿轮图标。此时将显示设置页面。

2. 单击 **LDAP** 以查看 LDAP 连接的配置。
3. 在靠近页面底部的位置，查看用户搜索依据字段：
    - 如果设置为 **userPrincipalName**，XenMobile Server 将设置为按 UPN 搜索。
    - 如果设置为 **sAMAccountName**，XenMobile Server 将设置为按 SAM 搜索。

取消注册 **Android Enterprise** 企业

可以使用 XenMobile Server 控制台和 XenMobile Tools 取消注册 Android Enterprise 企业。

执行此任务时，XenMobile Server 将打开 XenMobile Tools 的弹出窗口。开始之前，请确保 XenMobile Server 有权在您使用的浏览器中打开弹出窗口。某些浏览器（例如 Google Chrome）要求禁用弹出窗口阻止功能并将 XenMobile 站点的地址添加到弹出窗口阻止允许列表中。

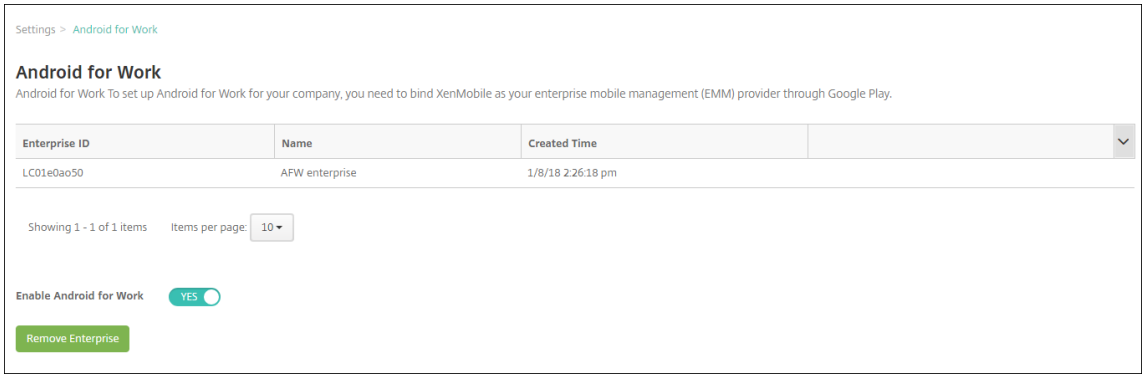
> 警告：
>
> 取消注册企业后，通过其注册的设备上的 Android Enterprise 应用程序将重置到其默认状态。这些设备将不再由 Google 托管。如果未进一步进行配置，在 Android Enterprise 企业中重新注册这些设备可能不会恢复以前的功能。

取消注册 Android Enterprise 企业后：

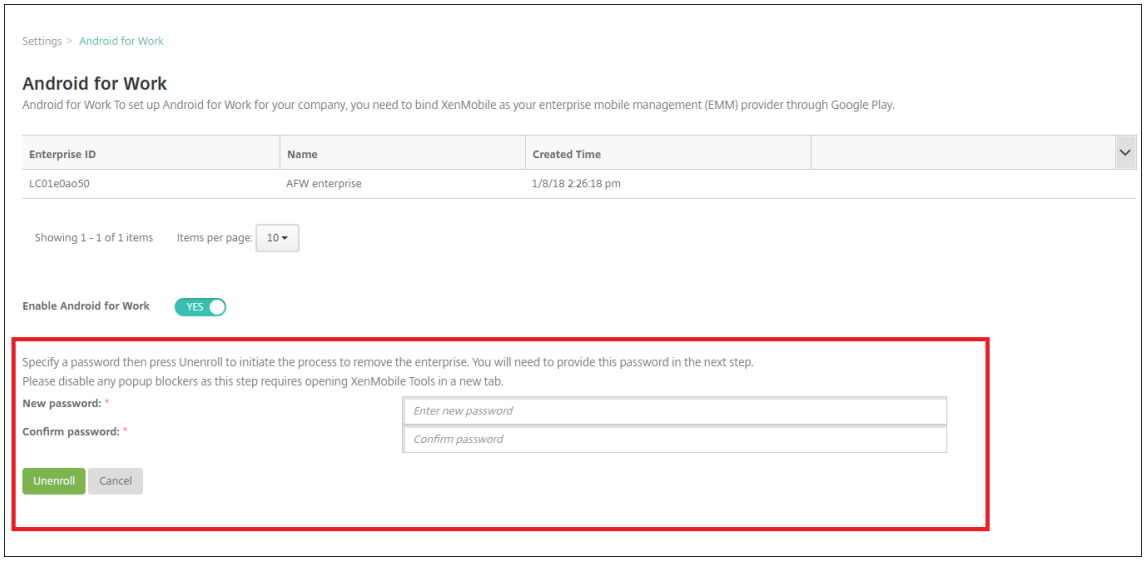
- 通过企业注册的设备和用户会将 Android Enterprise 应用程序重置到其默认状态。以前应用的 “Android Enterprise 应用程序权限” 和 “Android Enterprise 应用程序限制” 策略不再有效。
- 通过企业注册的设备由 XenMobile 托管，但在 Google 看来未托管。无法添加任何新的 Android Enterprise 应用程序。无法应用任何 “Android Enterprise 应用程序权限” 或 “Android Enterprise 应用程序限制” 策略。仍然可以将其他策略（例如 “计划”、“密码” 和 “限制”）应用于这些设备。
- 如果尝试在 Android Enterprise 中注册设备，这些设备将注册为 Android 设备，而非 Android Enterprise 设备。

要取消注册 Android Enterprise 企业，请执行以下操作：

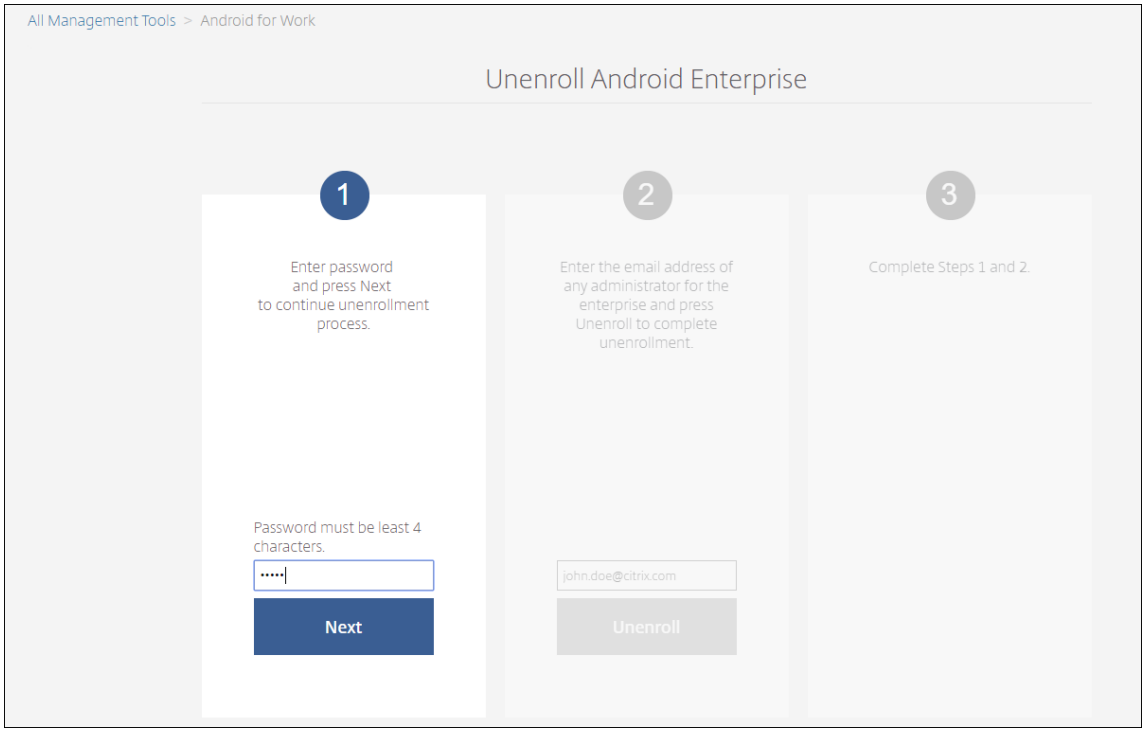
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在 “设置” 页面上，单击 **Android Enterprise**。
3. 单击删除企业。



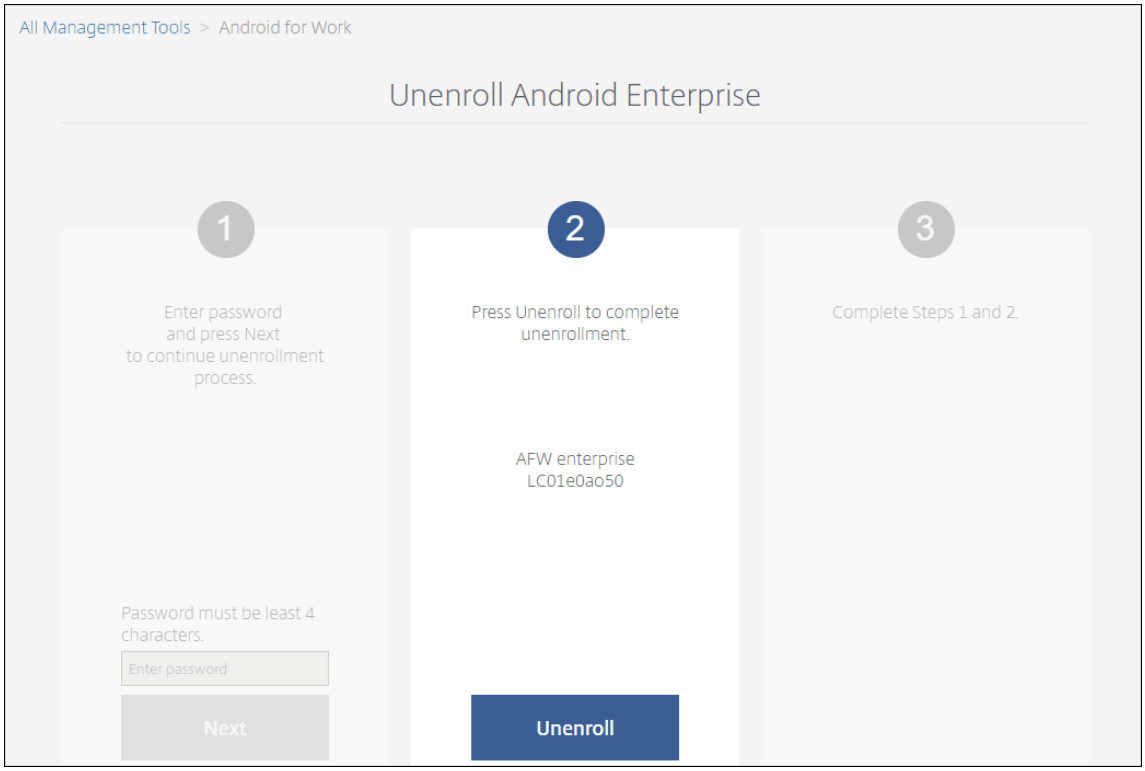
4. 指定一个密码。您在执行下一步骤时需要此密码才能完成取消注册操作。然后单击取消注册。



5. “XenMobile Tools” 页面打开时，请输入您在上一步骤中创建的密码。



6. 单击取消注册。



在 **Android Enterprise** 中预配完全托管设备

只有公司拥有的设备可以是适用于 Android Enterprise 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。

XenMobile 支持对完全托管设备使用以下注册方法：

- **afw#xenmobile**：如果使用此注册方法，用户在设置设备时将输入字符 afw#xenmobile。此令牌将设备标识为由 XenMobile 托管并下载 Secure Hub。
- **QR** 代码：QR 代码预配是预配不支持 NFC 的分布式设备队列（例如平板电脑）的简便方式。可以在已恢复出厂设置的队列设备上使用 QR 代码注册方法。QR 代码注册方法通过扫描设置向导中的 QR 代码来设置并配置完全托管设备。
- 近场通信 **(NFC)** 碰撞：可以在已重置为出厂设置的队列设备上使用 NFC 碰撞注册方法。NFC 碰撞通过在两个设备之间使用近场通信来传输数据。蓝牙、Wi-Fi 和其他通信模式在恢复出厂设置的设备上处于禁用状态。NFC 是此状态下设备可以使用的唯一通信协议。

afw#xenmobile

此注册方法在打开新设备或恢复出厂设置的设备以便进行初始设置后使用。系统提示输入 Google 帐户时，用户输入 afw#xenmobile。此操作将下载并安装 Secure Hub。用户随后将按照 Secure Hub 设置提示进行操作，完成注册过程。

对于大多数客户，建议使用此注册方法，因为是从 Google Play 应用商店下载最新版本的 Secure Hub。与其他注册方法不同，您不用提供要从 XenMobile Server 下载的 Secure Hub。

必备条件：

- 在运行 Android 5.0 及更高版本的所有 Android 设备上均受支持。

QR 代码

要使用 QR 代码在设备模式注册设备，请通过创建一个 JSON 并将该 JSON 转换为 QR 代码来生成 QR 代码。将使用设备相机扫描 QR 代码以注册设备。

必备条件：

- 在运行 Android 7.0 及更高版本的所有 Android 设备上均受支持。

从 JSON 创建 QR 代码

创建包含以下字段的 JSON。

以下字段均为必填项：

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

值：com.zenprise/com.zenprise.configuration.AdminFunction

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

值：qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

值：`https://path/to/securehub.apk`

> 注意：
>
> 如果将 Secure Hub 上载到 Citrix XenMobile Server 作为企业应用程序，则可以从 `https://<fqdn>:4443/*instanceName*/worxhome.apk` 下载该应用程序。Secure Hub APK 路径应该能够通过设备在预配期间连接到的 Wi-Fi 连接进行访问。

以下字段为选填字段：

- **android.app.extra.PROVISIONING_LOCALE**：输入语言和国家/地区代码。

  语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请输入 en_US 表示在美国所讲的英语。

- **android.app.extra.PROVISIONING_TIME_ZONE**：设备运行时所在的时区。

  请输入区域/位置形式的 Olson 名称。例如，America/Los_Angeles 表示太平洋时间。如果未输入，则将自动填充时区。

- **android.app.extra.PROVISIONING_LOCAL_TIME**：从 Epoch 开始经过的时间（毫秒）。

  Unix epoch（或 Unix 时间、POSIX 时间或 Unix 时间戳）是指从 1970 年 1 月 1 日（午夜，UTC/GMT）开始经过的秒数。该时间不包括闰秒（在 ISO 8601 中为：1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION**：设置为 **true** 将在配置文件创建期间跳过加密。设置为 **false** 将在配置文件创建期间强制加密。

典型的 JSON 如下：

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "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
}
```

使用任意 JSON 验证工具（例如 https://jsonlint.com）验证创建的 JSON。然后使用任意联机 QR 代码生成器（例如 https://goqr.me）将该 JSON 字符串转换为 QR 代码。

恢复出厂设置的设备将扫描此 QR 代码以在工作托管设备模式下注册设备。

注册设备

要将设备注册为完全托管设备，该设备必须处于已恢复出厂设置状态。

1. 在欢迎屏幕上轻按该屏幕六次以启动 QR 代码注册流程。
2. 系统提示时，连接到 Wi-Fi。QR 代码（JSON 编码）中 Secure Hub 的下载位置可以通过此 Wi-Fi 网络访问。

   设备成功连接到 Wi-Fi 后，将从 Google 下载一个 QR 代码读取器并启动摄像头。

3. 将摄像头对准 QR 代码以扫描该代码。

   Android 将从 QR 代码中的下载位置下载 Secure Hub，验证签名证书的签名，安装 Secure Hub 并将其设置为设备所有者。

有关详细信息，请参阅此面向 Android EMM 开发人员的 Google 指南：https://developers.google.com/android/work/prov-devices#qr_code_method。

NFC 碰撞

要使用 NFC 碰撞功能将设备注册为完全托管设备，需要两个设备：一个已恢复出厂设置的设备，以及一个运行 XenMobile Provisioning Tool 的设备。

必备条件：

- 在运行 Android 5.0、Android 5.1、Android 6.0 及更高版本的所有 Android 设备上均受支持。
- 为 Android Enterprise 启用的 XenMobile Server 10.4。
- 新的或恢复出厂设置的设备，为 Android Enterprise 预配为完全托管设备。可以在本文中查找完成此必备条件的步骤。

- 另一个设备具有 NFC 功能，运行已配置的 Provisioning Tool。Provisioning Tool 在 Secure Hub 10.4 或 Citrix 下载页面上提供。

每个设备只能配备一个 Android Enterprise 配置文件，通过企业移动性管理 (EMM) 应用程序管理。在 XenMobile 中，Secure Hub 为 EMM 应用程序。仅允许在每个设备上配备一个配置文件。尝试添加第二个 EMM 应用程序将删除第一个 EMM 应用程序。

通过 **NFC** 碰撞传输数据

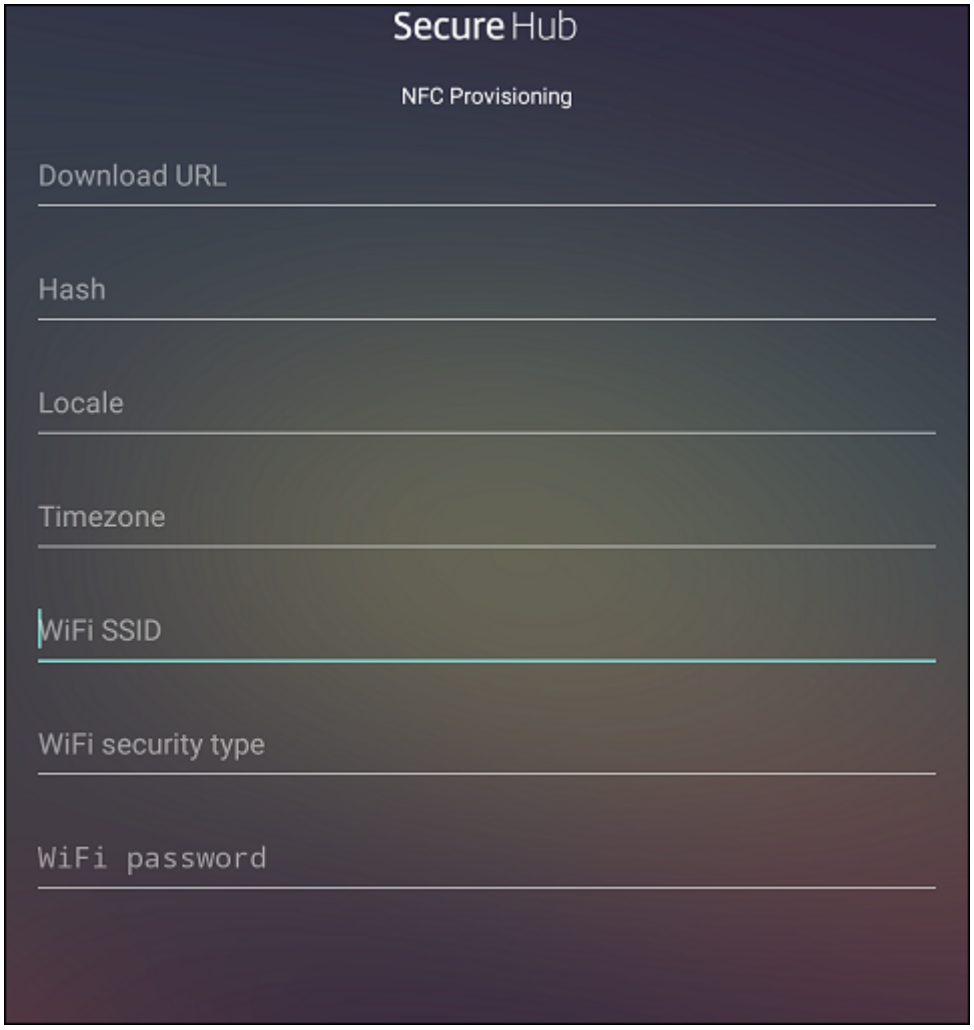
预配恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以初始化 Android Enterprise：

- 要作为设备所有者（在此示例中为 Secure Hub）的 EMM 提供程序应用程序的包名称。
- 设备可以从中下载 EMM 提供程序应用程序的 Intranet/Internet 位置。
- 用于验证下载是否成功的 EMM 提供程序应用程序的 SHA1 哈希。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备能够连接和下载 EMM 提供程序应用程序。注意：Android 现在不支持在此步骤中使用 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

碰撞两个设备时，来自 Provisioning Tool 的数据将发送到恢复出厂设置的设备。该数据随后用于下载使用管理员设置的 Secure Hub。如果未输入时区和位置值，Android 将在新设备上自动配置值。

配置 **XenMobile Provisioning Tool**

执行 NFC 碰撞之前，必须配置 Provisioning Tool。此配置随后在 NFC 碰撞过程中被传输到恢复出厂设置的设备。



可以将数据键入到必填字段中，或者通过文本文件进行填充。下一个过程中的步骤介绍了如何配置文本文件，并且包含每个字段的说明。键入后，该应用程序将不保存信息，因此，您可能希望创建一个文本文件以保留该信息供将来使用。

使用文本文件配置 **Provisioning Tool**

将文件命名为 nfcprovisioning.txt 并将其放置在设备的 SD 卡中的 /sdcard/ 文件夹下。该应用程序随后可以读取文本文件并填充值。

文本文件必须包含以下数据：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<
download_location>
```

此行为 EMM 提供程序应用程序的 Intranet/Internet 位置。恢复出厂设置的设备在进行 NFC 碰撞后连接到 Wi-Fi 之后，该设备必须有权访问此位置才能进行下载。该 URL 为常规 URL，不需要特殊格式。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```


此行是 EMM 提供程序应用程序的校验和。此校验和用于验证下载是否成功。本文中后面的内容介绍了获取校验和的步骤。

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

此行是运行 Provisioning Tool 的设备的已连接 Wi-Fi SSID。

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

支持的值为 WEP 和 WPA2。如果 Wi-Fi 未受保护，此字段必须留空。

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

如果 Wi-Fi 未受保护，此字段必须留空。

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

输入语言和国家/地区代码。语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请键入 en_US 表示在美国所讲的英语。如果未输入任何代码，则会自动填充国家/地区和语言。

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

设备运行时所在的时区。请键入区域/位置形式的 Olson 名称。例如，America/Los_Angeles 表示太平洋时间。如果未输入名称，则将自动填充时区。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

不需要此数据，因为值 Secure Hub 被硬编码到应用程序中。在本文中提及的目的只是为了保持完整性。

如果存在通过使用 WPA2 保护的 Wi-Fi，完整的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

如果存在不受保护的 Wi-Fi，完整的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d
```



```
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 **Secure Hub** 校验和

要获取任何应用程序的校验和，请添加该应用程序作为企业应用程序。

1. 在 XenMobile 控制台中，转至配置 **>** 应用程序，然后单击添加。

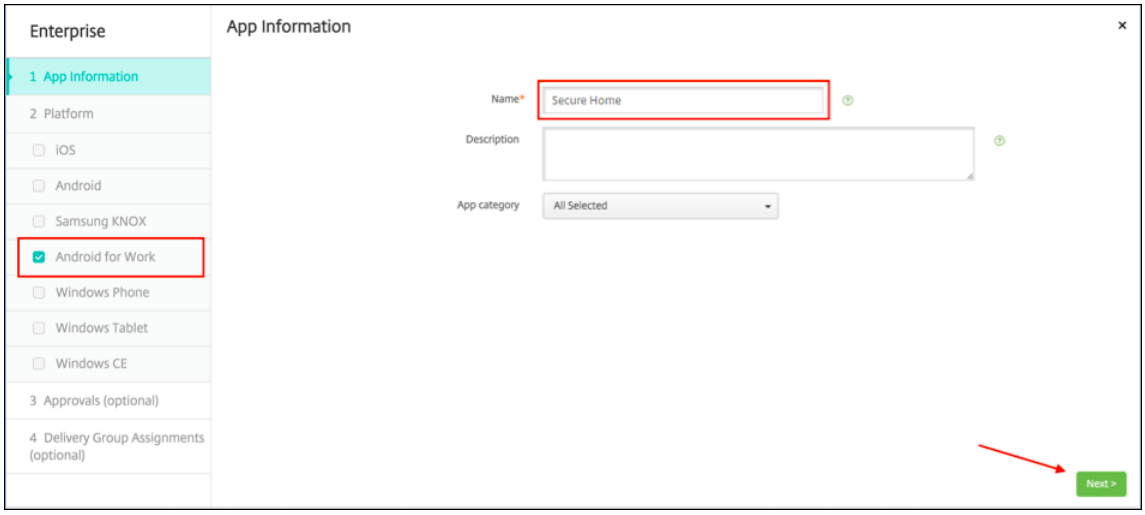
   此时将显示添加应用程序窗口。

2. 单击企业。

   此时将显示应用程序信息页面。

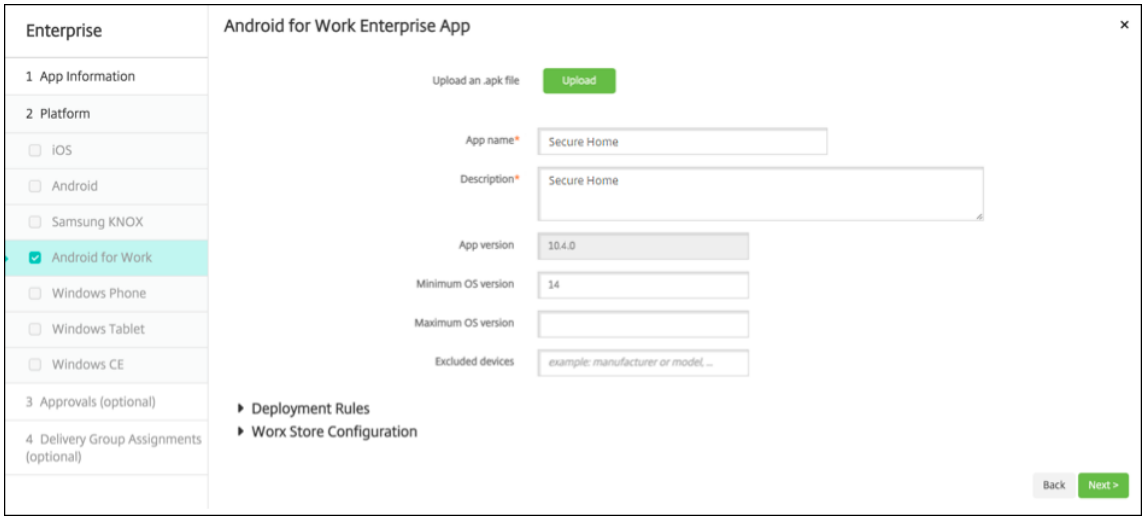
3. 选择以下配置并单击下一步。

   此时将显示 **Android Enterprise** 企业应用程序页面。



4. 提供.apk 的路径，然后单击下一步以上载文件。

   上载完成后，系统将显示上载的软件包的详细信息。



5. 单击下一步以打开下载 JSON 文件的页面，随后可以在该页面中上载到 Google Play。对于 Secure Hub，不需要上载到 Google Play，但需要 JSON 文件才能从中读取 SHA1 值。

   典型的 JSON 文件格式如下：

6. 复制 **file_sha1_base64** 值并在 Provisioning Tool 中的 **Hash**（哈希）字段中使用。

   > 注意：
   >
   > 该哈希必须是 URL 安全哈希。

   - 将任何 **+** 符号转换为 **-**
   - 将任何 **/** 符号转换为 **_**
   - 将尾随 **\u003d** 替换为 **=**

   如果您将哈希值存储在设备的 SD 卡上的 nfcprovisioning.txt 文件中，该应用程序将执行安全转换。但是，如果选择手动键入哈希值，您将负责确保其 URL 的安全性。

使用的库

Provisioning Tool 在其源代码中使用以下库：

- Google 遵循 Apache License 2.0 提供的 v7 appcompat 库、Design Support Library 以及 v7 Palette 库

  有关信息，请参阅 Support Library Features Guide（支持库功能指南）。

- Jake Wharton 遵循 Apache License 2.0 提供的 Butter Knife

在 **Android Enterprise** 中预配工作配置文件设备

在 Android Enterprise 中的工作配置文件设备上，您安全地分隔了设备上的企业区域与个人区域。例如，BYOD 设备可以是工作配置文件设备。工作配置文件设备的注册体验与 XenMobile 中的 Android 注册体验相似。用户将从 Google Play 下载 Secure Hub 并注册其设备。

默认情况下，如果某个设备在 Android Enterprise 中注册为工作配置文件设备，USB 调试和未知来源设置在该设备上将处于禁用状态。

> 提示：
>
> 在 Android Enterprise 中将设备注册为工作配置文件设备时，将始终转至 Google Play。在该应用商店中，允许 Secure Hub 在用户的个人配置文件中显示。

iOS

January 5, 2022

要在 XenMobile Server 中管理 iOS 设备，请设置 Apple 提供的 Apple 推送通知服务 (APNs) 证书。有关信息，请参阅 APNs 证书。

注册配置文件确定 iOS 设备是否在 MDM+MAM 模式下注册，并带有用户可选择退出 MDM 的选项。XenMobile Server 支持对处于 MDM+MAM 模式的 iOS 设备使用以下身份验证类型。有关信息，请参阅证书和身份验证下的文章。

- 域
- 域加安全令牌
- 客户端证书
- 客户端证书加域

> **iOS 13** 中对可信证书的要求：
>
> Apple 对 TLS 服务器证书有新的要求。验证所有证书都符合 Apple 的新要求。请参阅 Apple 出版物 https://support.apple.com/en-us/HT210176。有关管理证书方面的帮助，请参阅在 XenMobile Server 中上载证书。

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

XenMobile Server 和 Citrix 移动应用程序与 iOS 14 兼容，但目前不支持新的 iOS 14 功能。

对于受监督的 iOS 设备，您最多可以将软件升级延迟 90 天。在适用于 iOS 的“限制”设备策略中，请使用以下设置：

- 强制执行延迟的软件更新
- 强制执行的软件更新延迟

请参阅 iOS 设置。这些设置不适用于用户注册模式或非监督（完全 MDM）模式下的设备。

必须保持公开状态的 Apple 主机名

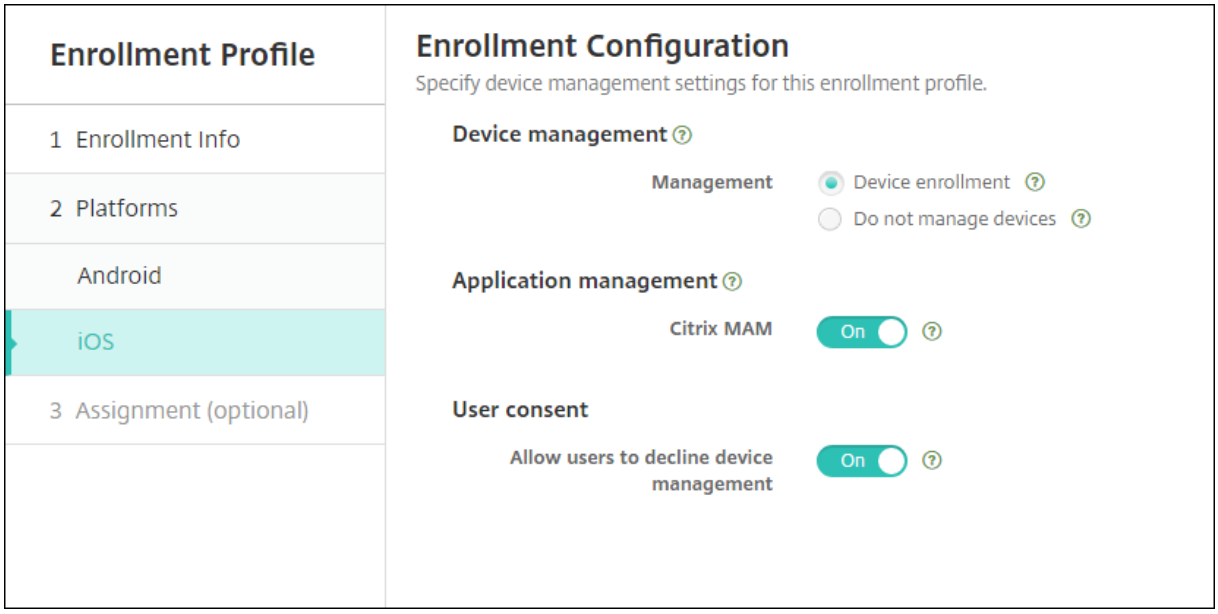
某些 Apple 主机名必须保持打开状态，以确保 iOS、macOS 和 Apple App Store 的正常运行。阻止这些主机名可能会影响以下对象的安装、更新和正确操作：iOS、iOS 应用程序、MDM 操作以及设备和应用程序注册。有关详细信息，

请参阅 https://support.apple.com/en-us/HT201999。

支持的注册方法

可以在注册配置文件中指定如何管理 iOS 设备。可以选择设备注册或不注册 MDM。

要为 iOS 设备配置注册设置，请转到配置 **>** 注册配置文件 **> iOS**。



下表列出了 XenMobile Server 支持 iOS 设备的注册方法：

方法	支持
Apple 部署计划	是
Apple 校园教务管理	是
Apple Configurator	是
手动注册	是
注册邀请	是

Apple 制定了面向企业和教育帐户的设备注册计划。对于企业帐户，需要在 “Apple 部署计划” 中注册才能使用 Apple 设备注册计划在 XenMobile Server 中注册和管理设备。该计划面向 iOS 和 macOS 设备。请参阅通过 Apple 部署计划部署设备。

对于教育帐户，需要创建一个 Apple 校园教务管理帐户。Apple 校园教务管理统一了部署计划和批量购买。Apple 校园教务管理的类型为教育 Apple 部署类型。请参阅与 Apple 教育功能相集成。

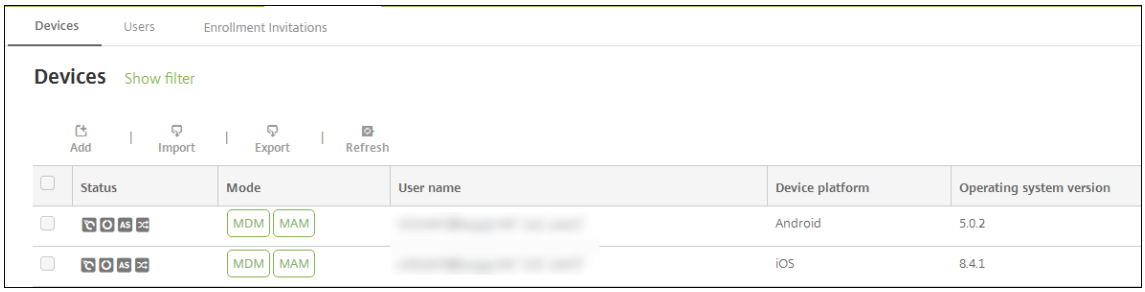
可以使用 Apple 部署计划批量注册 iOS 和 macOS 设备。可以直接从 Apple 、参与计划的 Apple 授权经销商或运营

商处购买这些设备。无论您是否直接从 Apple 购买 iOS 设备，都可以使用 Apple Configurator 注册这些设备。请参阅Apple 设备的批量注册。

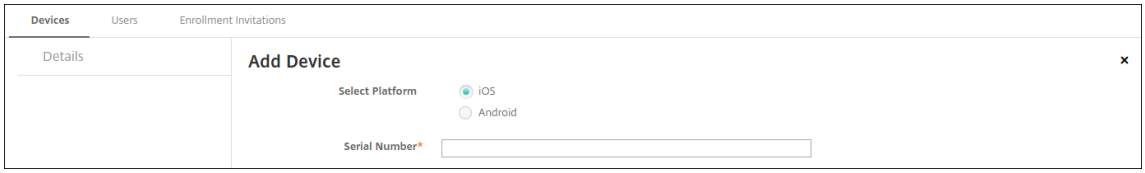
手动添加 iOS 设备

如果要手动添加 iOS 设备（例如用于测试目的），请按照以下步骤进行操作。

1. 在 XenMobile Server 控制台中，单击管理 > 设备。此时将显示设备页面。



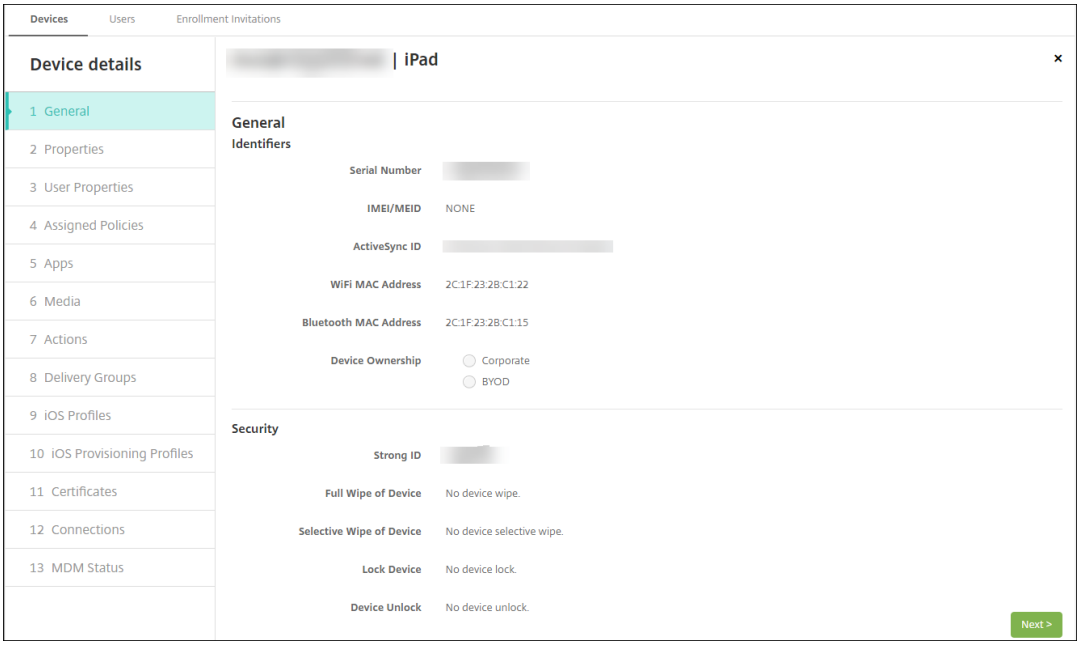
2. 单击添加。此时将显示添加设备页面。



3. 配置以下设置：
   - 选择平台：单击 **iOS**。
   - 序列号：键入设备序列号。
4. 单击添加。设备将添加到所显示设备表的列表底部。要查看并确认设备详细信息，请执行以下操作：选择已添加的设备，然后在显示的菜单中，单击编辑。

> 注意：
>
> 选中某个设备旁边的复选框时，选项菜单将在设备列表上方显示。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。

   - 已配置 LDAP
   - 如果使用本地组和本地用户：
     - 一个或多个本地组。
     - 分配给本地组的本地用户。
     - 交付组与本地组相关联。
   - 如果使用 Active Directory：
     - 交付组与 Active Directory 组相关联。



5. 常规页面列出设备标识符，例如，序列号和平台类型的其他信息。对于设备所有权，请选择公司或 **BYOD**。

   常规页面还列出了设备安全属性，例如，强 ID、锁定设备、激活锁绕过和平台类型的其他信息。完全擦除设备字段包括用户的 PIN 代码。擦除设备后，用户必须输入该代码。如果用户忘记了该代码，您可以在此处查找。

6. 属性页面列出了 XenMobile Server 要预配的设备属性。此列表显示了用于添加设备的预配文件中包含的任何设备属性。要添加属性，请单击添加，然后从列表中选择一种属性。有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

   添加属性时，它最初将显示在添加了该属性的类别下方。单击下一步，然后返回属性页面后，属性将显示在相应列表中。

   要删除某个属性，请将鼠标悬停在列表上方，然后单击右侧的 **X**。XenMobile Server 将立即删除该项目。

7. 其余的设备详细信息部分包含设备的摘要信息。

   - 用户属性：显示用户的 RBAC 角色、组成员身份、批量购买帐户和属性。可以从此页面停用批量购买帐户。
   - 已分配的策略：显示已分配策略的数量，包括已部署、挂起和失败的策略数量。提供每个策略的策略名称、类型和上次部署信息。
   - 应用程序：显示上一个清单的已安装、挂起和失败的应用程序部署数量。提供应用程序名称、标识符、类型和其他信息。有关 iOS 和 macOS 清单密钥（例如 **HasUpdateAvailable**）的说明，请参阅移动设备管理 (MDM) 协议。
   - 媒体：显示上一个清单的已部署、挂起和失败的媒体部署数量。
   - 操作：显示已部署、挂起和失败的操作数量。提供上一个部署的操作名称和时间。
   - 交付组：显示成功、挂起和失败的交付组数量。对于每个部署，提供交付组的名称和部署时间。选择一个交付组以查看更多详细信息，包括状态、操作以及通道或用户。
   - **iOS** 配置文件：显示上一个 iOS 配置文件清单，包括名称、类型、组织和说明。
   - **iOS** 预配配置文件：显示企业分发预配配置文件信息，例如 UUID、过期日期以及托管状态。

- 证书：显示有效证书、已过期证书或已吊销证书信息，例如，类型、提供程序、颁发者、序列号、过期之前的剩余天数。
- 连接：显示第一个连接状态和最后一个连接状态。提供每个连接的用户名、倒数第二次身份验证和上次身份验证时间。
- **MDM** 状态：显示 MDM 状态、上次推送时间以及上次设备答复时间等信息。

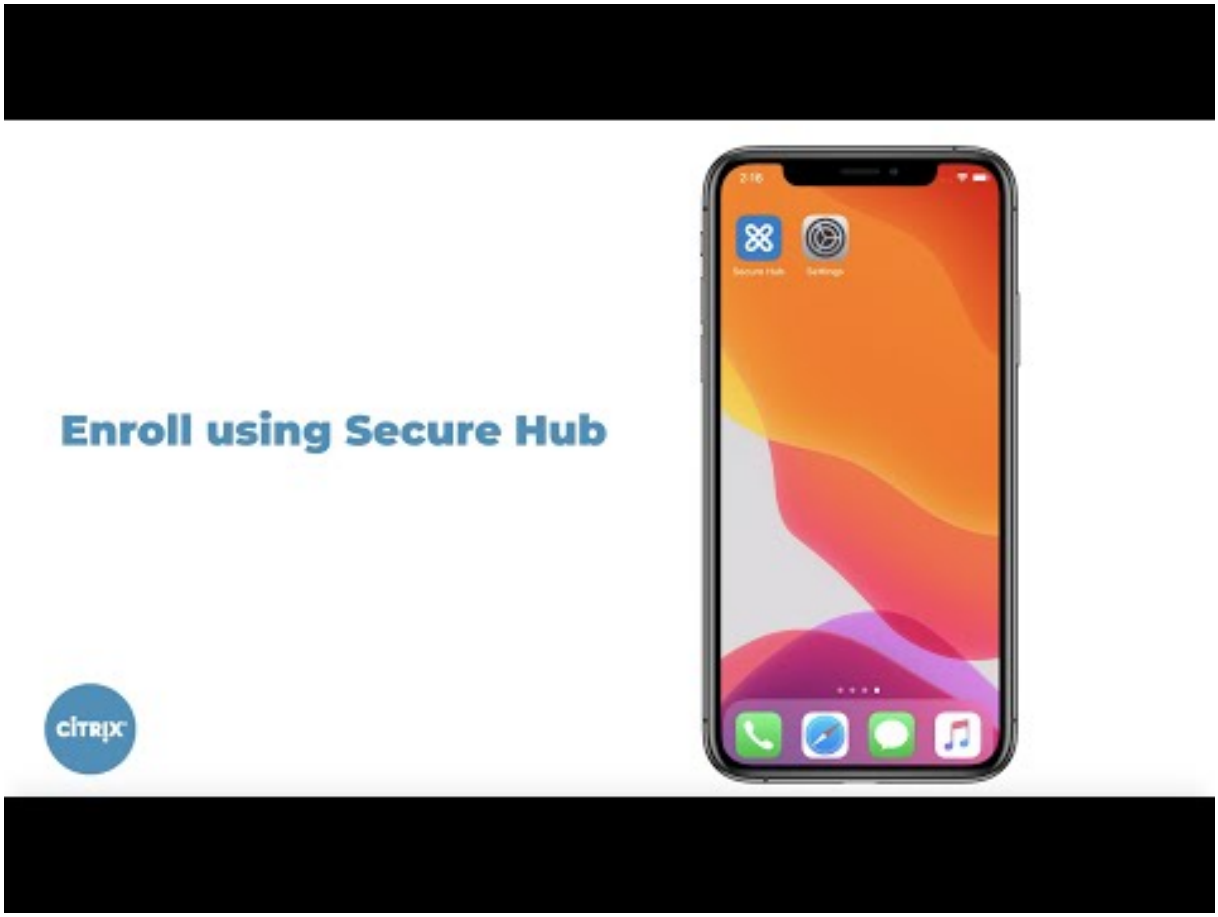
配置 iOS 设备策略

使用这些策略可配置 XenMobile Server 与运行 iOS 的设备的交互方式。下表列出了适用于 iOS 设备的所有设备策略。

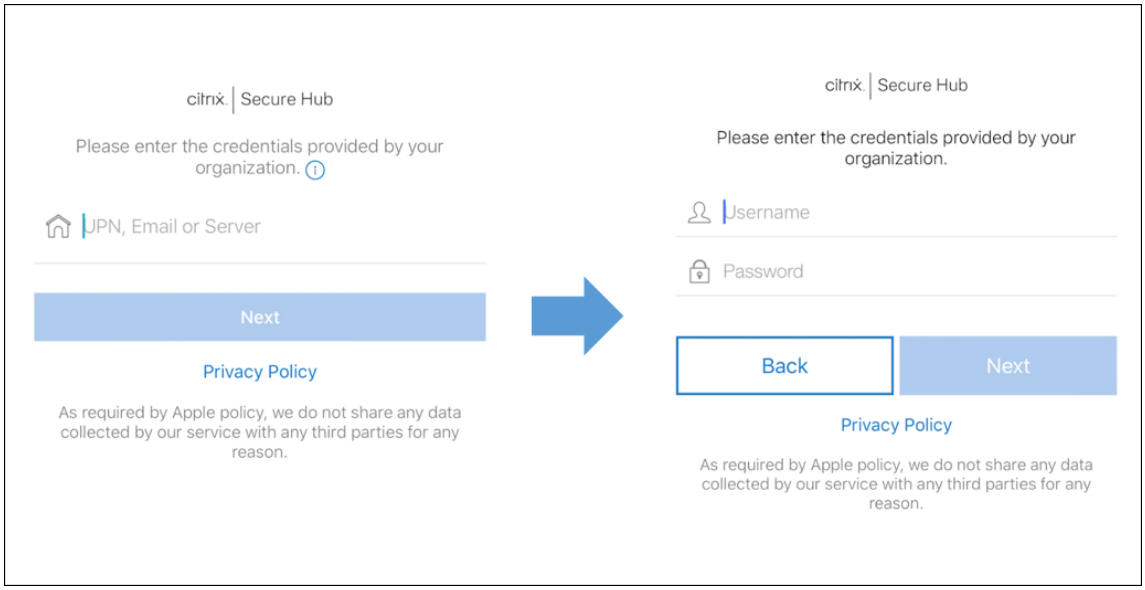
AirPlay 镜像	AirPrint	APN
应用程序访问	应用程序属性	应用程序配置
应用程序清单	应用程序锁定	应用程序网络使用
应用程序卸载	应用程序通知	日历 (CalDav)
手机网络	联系人 (CardDAV)	控制操作系统更新
凭据	设备名称	教育配置
Exchange	字体	主屏幕布局
导入 iOS 和 macOS 配置文件	LDAP	位置
邮件	托管域	MDM 选项
组织信息	通行码	个人热点
配置文件删除	预配配置文件	删除预配配置文件
代理	限制	漫游
SCEP	共用的 iPad - 最大常驻用户数	共用的 iPad - 通行码锁宽限期
SSO 帐户	存储	已订阅的日历
条款和条件	VPN	壁纸
Web 内容过滤器	Web 剪辑	WiFi

注册 iOS 设备

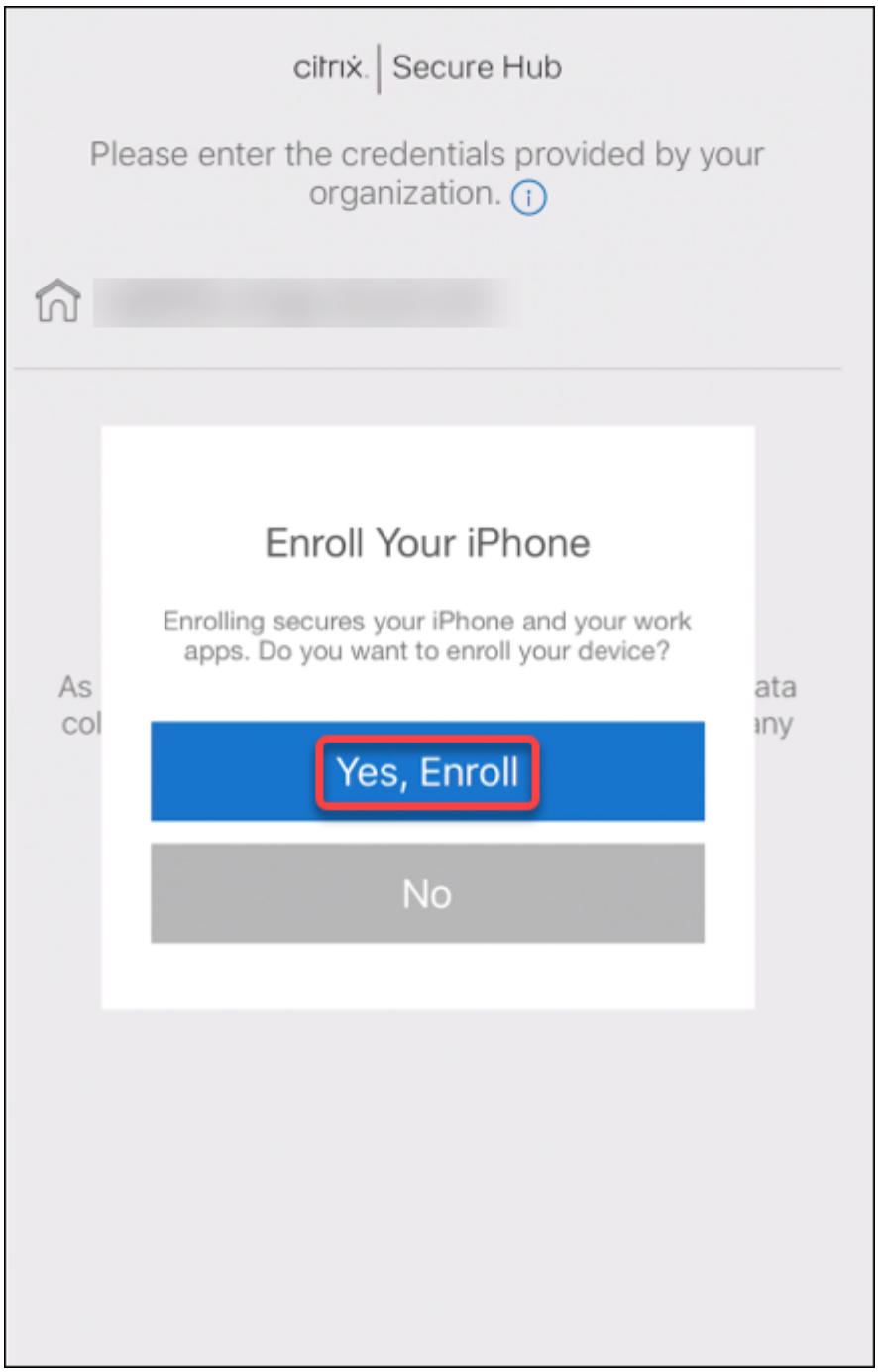
本部分内容介绍用户如何将 iOS 设备（12.2 或更高版本）注册到 XenMobile Server。有关 iOS 注册的详细信息，请打开以下视频：



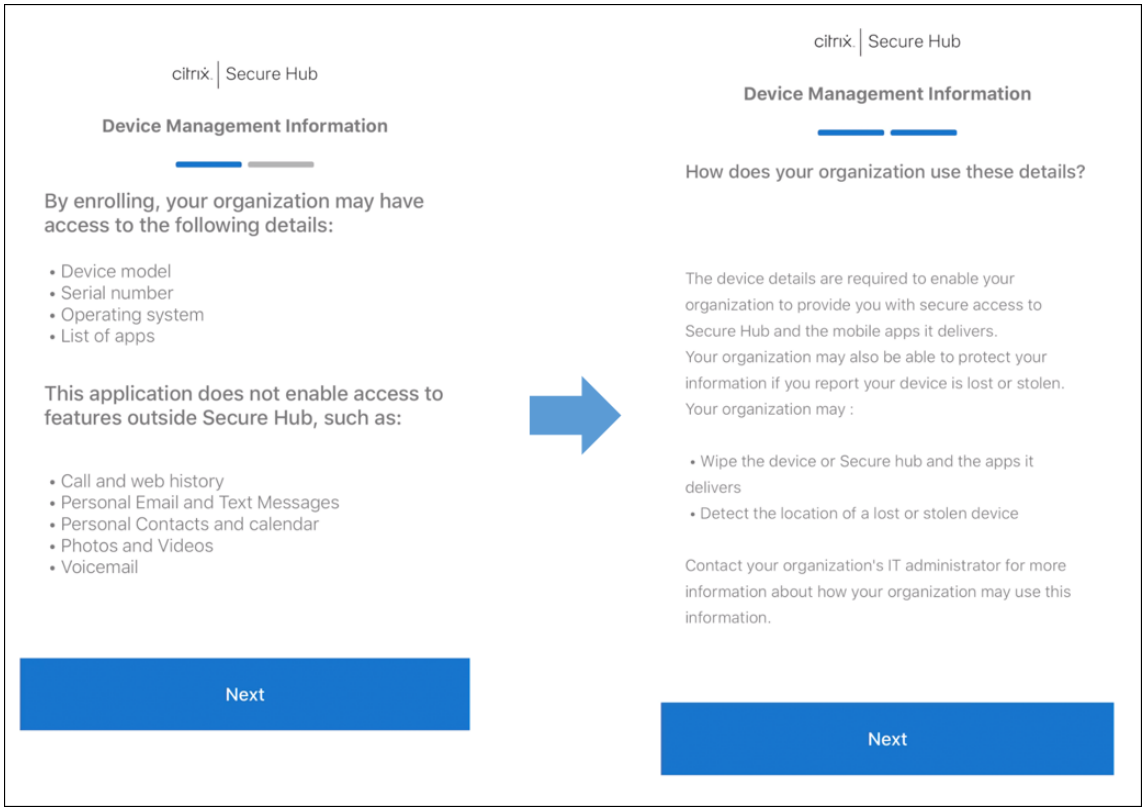
1. 在 iOS 设备上转到 Apple 应用商店，下载 Citrix Secure Hub 应用程序，然后轻按该应用程序。
2. 当系统提示安装应用程序时，轻按下一步，然后轻按安装。
3. 安装 Secure Hub 后，轻按打开。
4. 输入您的企业凭据，例如 XenMobile Server 服务器名称、用户主体名称 (UPN) 或电子邮件地址。然后，单击下一步。



5. 轻按是，注册以注册 iOS 设备。

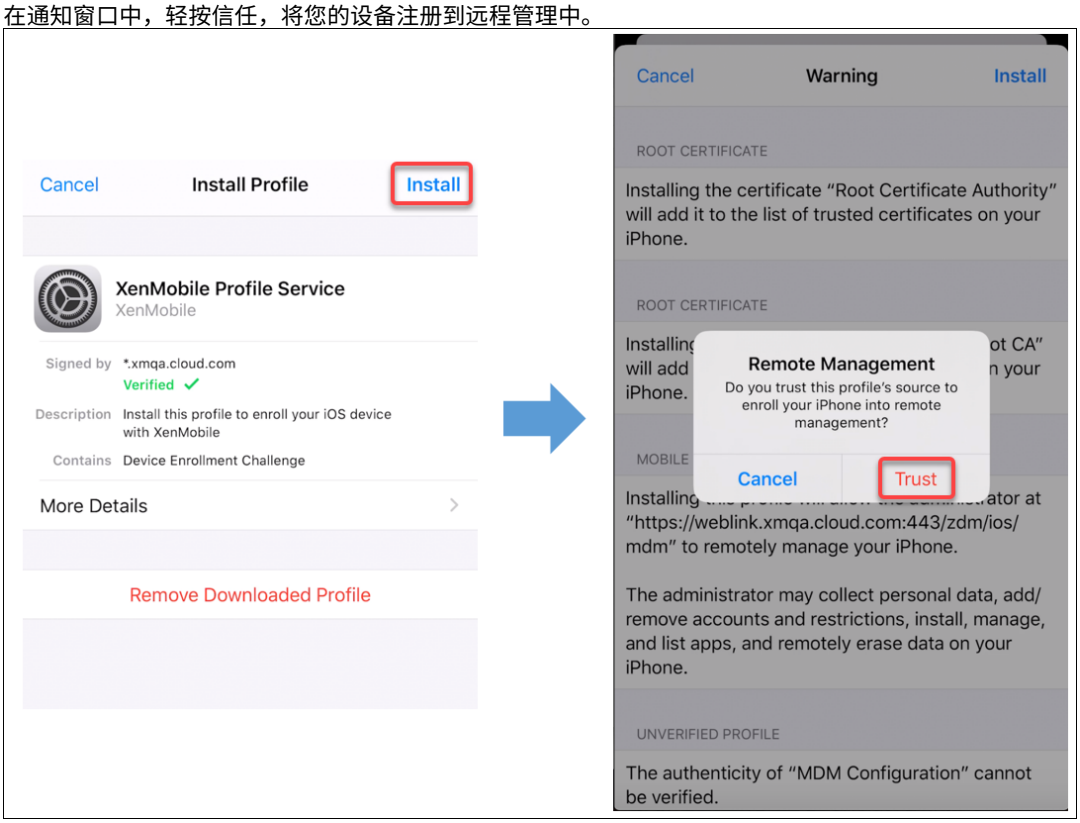


6. 此时将显示 XenMobile Server 收集的数据列表。单击 **Next**（下一步）。显示组织如何使用该数据的说明。单击 **Next**（下一步）。



7. 键入凭据后，在出现提示时轻按允许以下载配置文件。下载配置文件后，轻按关闭。

8. 在设备设置中，安装 iOS 证书并将设备添加到可信列表中。
   - 转到设置 > 常规 > 配置文件 > **XenMobile** 配置文件服务，然后轻按安装以添加配置文件。
   - 在通知窗口中，轻按信任，将您的设备注册到远程管理中。



9. 注册成功后，打开 Secure Hub。如果要注册到 MDM+MAM：验证凭据后，在出现提示时创建并确认您的 Citrix PIN。
10. 工作流程完成后，注册设备。随后即可访问应用商店来查看您安装在 iOS 设备上的应用程序。

安全操作

iOS 支持以下安全操作。有关每个安全操作的说明，请参阅安全操作。

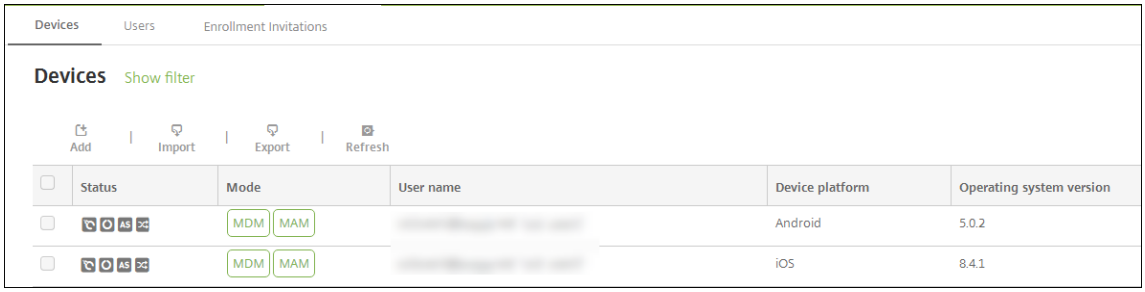
激活锁绕过	应用程序锁定	应用程序擦除
ASM 激活锁	证书续订	清除限制
启用/禁用丢失模式	启用/禁用跟踪	完全擦除
查找	锁定	响铃
请求使用/停止使用 AirPlay 镜像	重新启动/关闭	吊销/授权
选择性擦除	解锁	

锁定 **iOS** 设备

您可以锁定丢失的 iOS 设备，同时在设备锁屏界面上显示消息和电话号码。

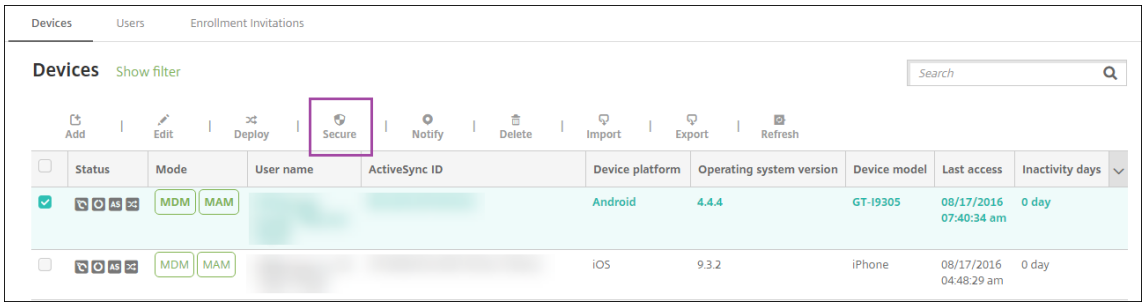
要在锁定的设备上显示消息和电话号码，请在 XenMobile Server 控制台中将通行码策略设置为 **true**。用户也可以手动在设备上启用通行码。

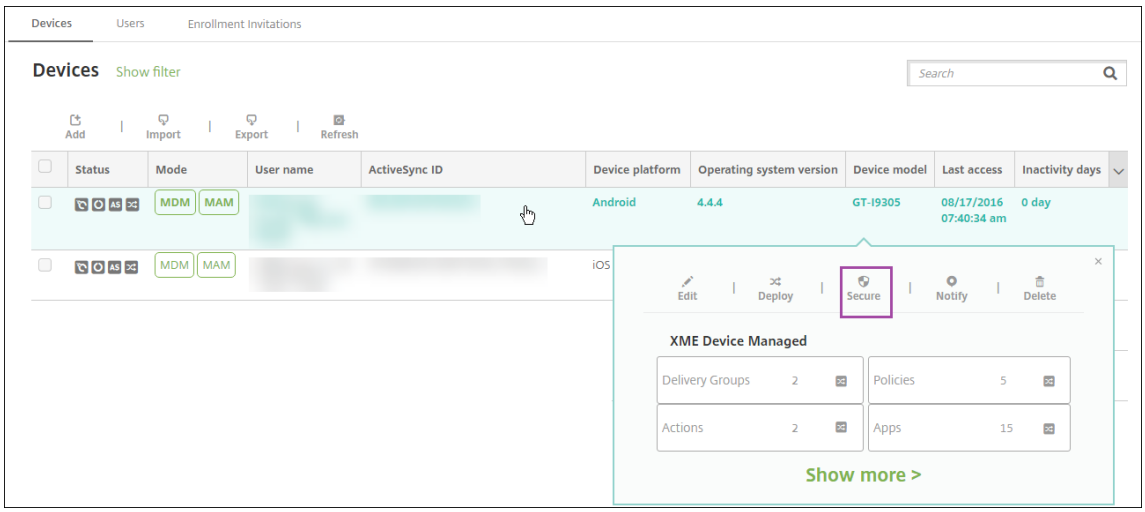
1. 单击管理 **>** 设备。此时将显示设备页面。



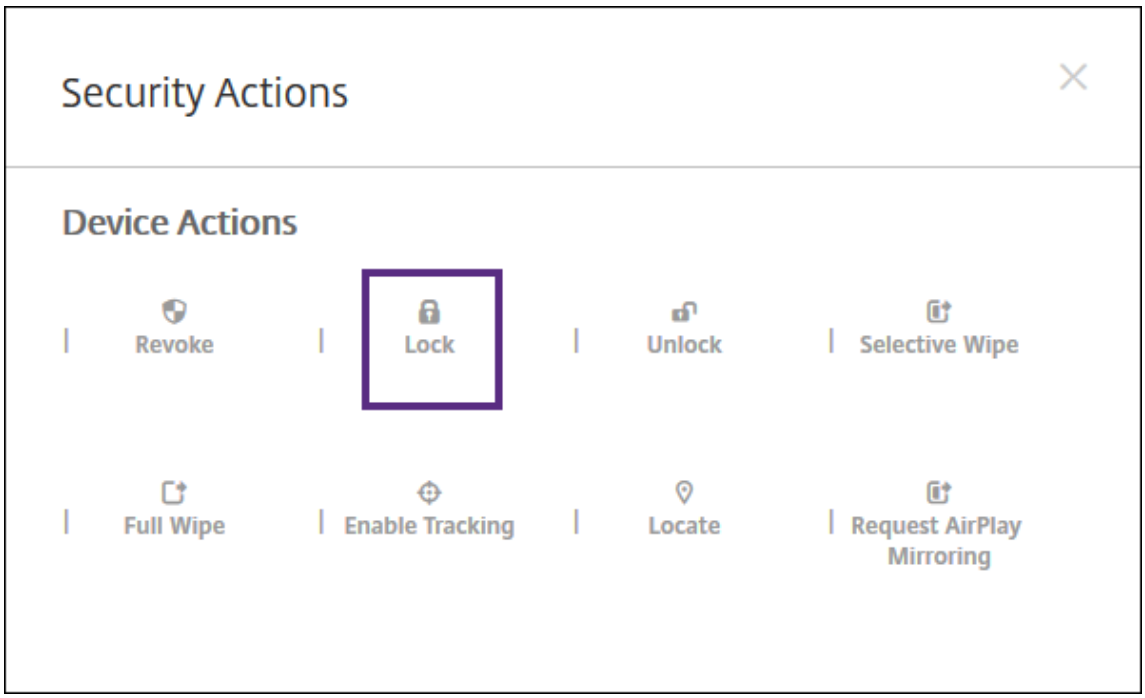
2. 选择要锁定的 iOS 设备。

   选中设备旁边的复选框以显示设备列表上方的选项菜单。单击列表中的其他任意位置可在列表右侧显示选项菜单。

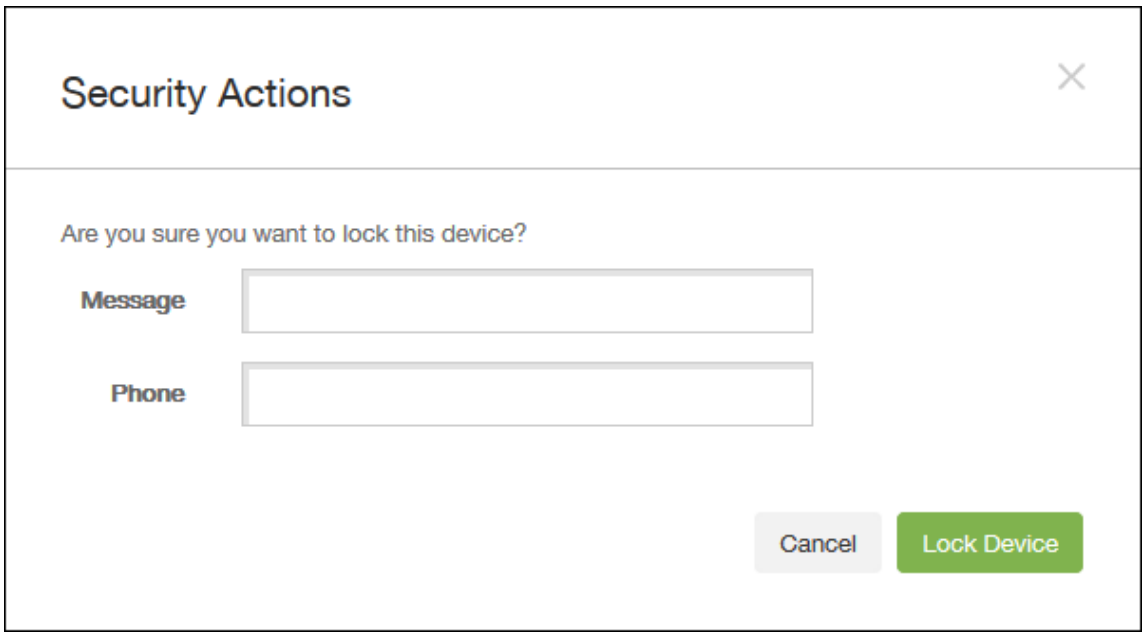




3. 在选项菜单中，选择安全。此时将显示安全操作对话框。



4. 单击锁定。此时将显示安全操作确认对话框。



5. （可选）键入将显示在设备锁屏界面上的消息和电话号码。

   iOS 会将 “丢失的 iPad” 字样附加到您在消息字段中键入的内容后。

   如果将消息字段留空，并提供电话号码，Apple 将在设备锁屏界面上显示消息 “呼叫所有者”。

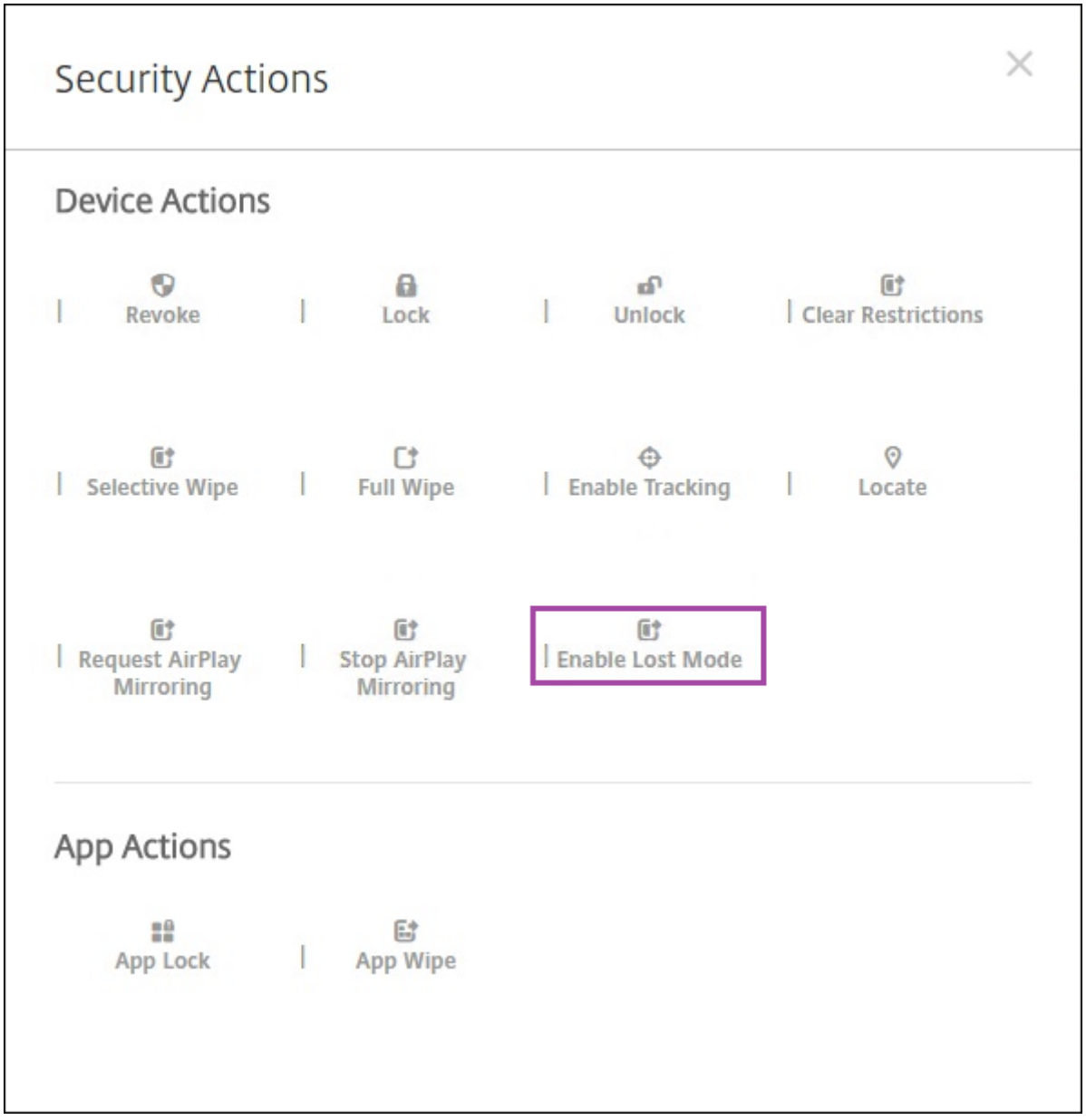
6. 单击锁定设备。

将 **iOS** 设备置于丢失模式

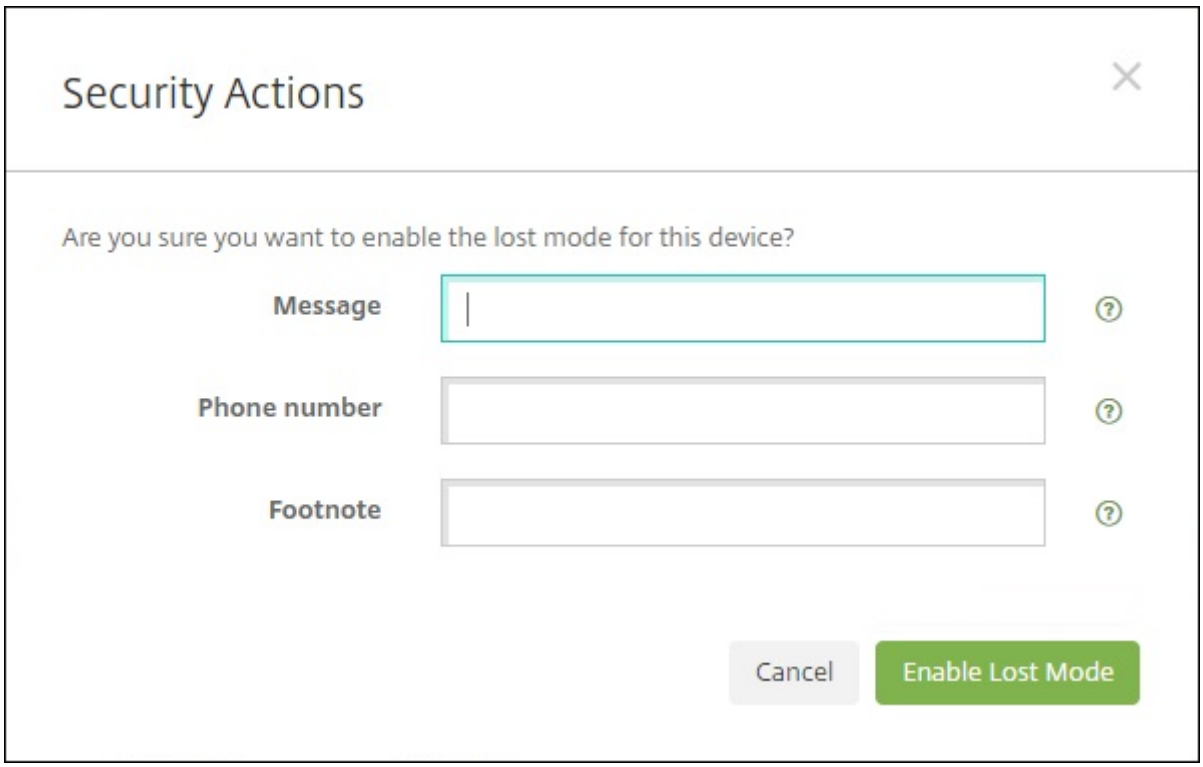
XenMobile Server 丢失模式设备属性将 iOS 设备置于丢失模式。与 Apple 托管丢失模式不同，XenMobile Server 丢失模式不要求用户执行以下任一操作来启用定位其设备：配置查找我的 **iPhone/iPad** 设置或为 Citrix Secure Hub 启用定位服务。

在 XenMobile Server 丢失模式下，只有 XenMobile Server 能够解锁设备。（与此相反，如果您使用 XenMobile Server 设备锁定功能，用户可以使用您提供的 PIN 代码直接解锁设备。

要启用或禁用丢失模式，请转至管理 **>** 设备，选择受监督的 iOS 设备，并单击安全。然后，单击启用丢失模式或禁用丢失模式。

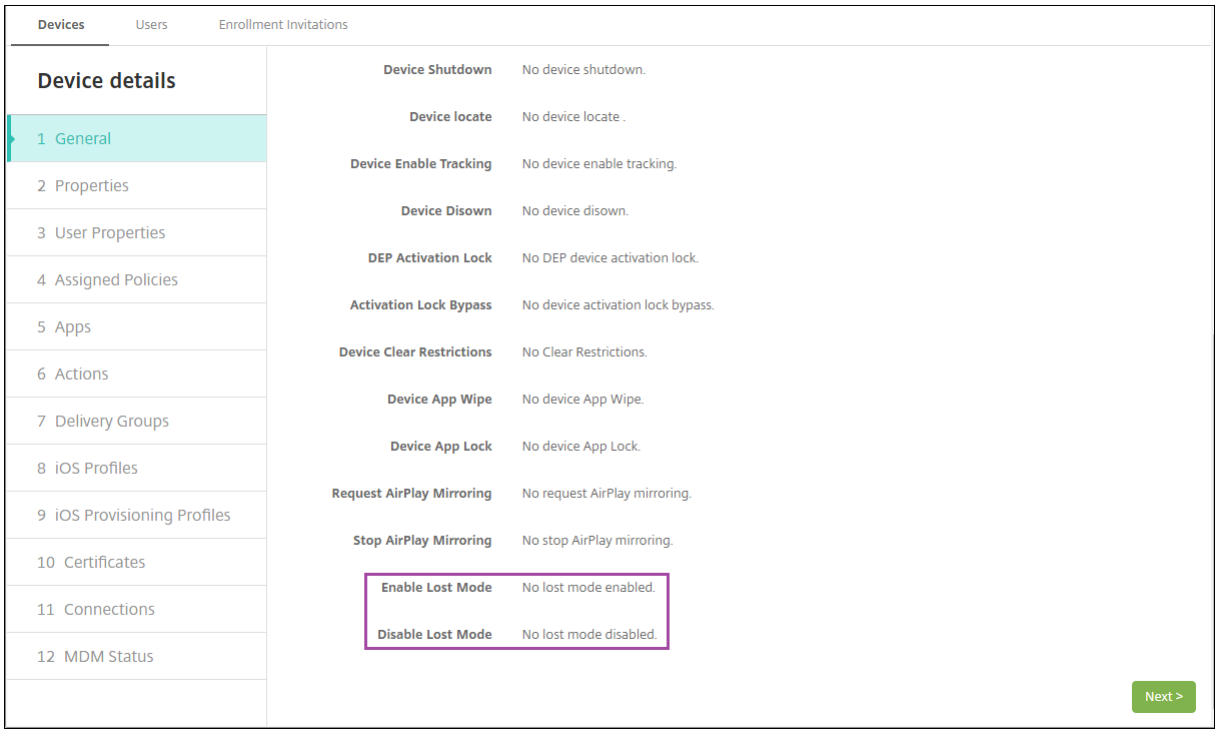


如果单击启用丢失模式，请键入设备处于丢失模式时要在设备上显示的信息。

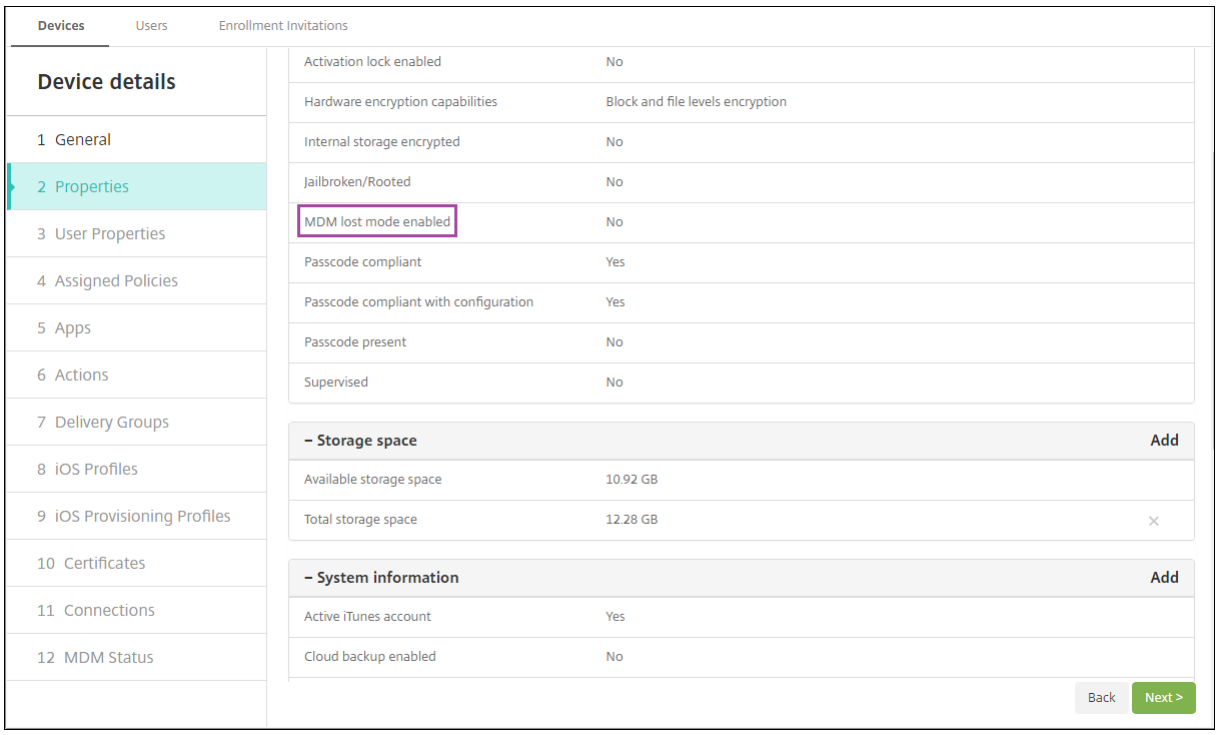


可使用以下任何方法来检查丢失模式状态：

- 在安全操作窗口中，确认按钮是否为禁用丢失模式。
- 在管理 **>** 设备中常规选项卡上的安全下方，查看最后一次“启用丢失模式”或“禁用丢失模式”操作。



- 在管理 **>** 设备中的属性选项卡上，确认已启用 **MDM** 丢失模式设置的值是否正确。



如果在 iOS 设备上启用 XenMobile Server 丢失模式，XenMobile Server 控制台也会更改，如下所示：

- 在配置 **>** 操作中，操作列表不包括这些自动化操作：吊销设备、选择性擦除设备和完全擦除设备。
- 在管理 **>** 设备中，安全操作列表不再包括吊销和选择性擦除设备的操作。您仍可以根据需要使用安全操作来执行完全擦除操作。

iOS 会将 “丢失的 iPad” 字样附加到您在安全操作屏幕的消息中输入的内容后。

如果将消息留空，并提供电话号码，Apple 将在设备锁屏界面上显示消息 “呼叫所有者”。

绕过 **iOS** 激活锁

激活锁是一项 “查找我的 iPhone/iPad” 功能，用于阻止重新激活丢失或被盗的受监督设备。激活锁需要用户的 Apple ID 和密码，之后用户才能执行以下操作：关闭 “查找我的 iPhone/iPad”、擦除设备或重新激活设备。对于组织拥有的设备，绕过激活锁是（例如）重置或重新分配设备的必要操作。

要启用激活锁，请配置并部署 XenMobile Server MDM 选项设备策略。之后可以从 XenMobile Server 控制台管理设备，而不需要用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 XenMobile Server 控制台发出 “激活锁绕过” 安全操作。

例如，如果用户在执行完全擦除操作之前或之后归还了丢失的手机或设置了设备：手机提示输入 Apple App Store 帐户凭据时，可以通过从 XenMobile Server 控制台发出 “激活锁绕过” 安全操作来绕过该设置。

激活锁绕过的设备要求

- 通过 Apple Configurator 或 Apple 部署计划进行监督

- 配置了 iCloud 帐户
- 已启用 “查找我的 iPhone/iPad”
- 已在 XenMobile Server 中注册
- “MDM 选项” 设备策略（启用了激活锁）已部署到设备

要在发出设备的完全擦除操作之前绕过激活锁，请执行以下操作：

1. 转至管理 **>** 设备，选择设备，单击安全，然后单击激活锁绕过。
2. 擦除设备。激活锁屏幕在设备设置过程中不显示。

要在发出设备的完全擦除操作之后绕过激活锁，请执行以下操作：

1. 重置或擦除设备。激活锁屏幕在设备设置过程中显示。
2. 转至管理 **>** 设备，选择设备，单击安全，然后单击激活锁绕过。
3. 轻按设备上的 “返回” 按钮。此时将显示主屏幕。

请紧急以下几点：

- 建议您的用户不要关闭 “查找我的 iPhone/iPad”。请勿从设备执行完全擦除操作。在这些情况下，系统将提示用户输入 iCloud 帐户密码。验证帐户后，用户在擦除所有内容和设置后将看不到 “激活 iPhone/iPad” 屏幕。
- 对于具有生成的激活锁绕过码并且启用了激活锁的设备：如果在执行完全擦除操作后无法绕过 “激活 iPhone/iPad” 页面，则不需要从 XenMobile Server 中删除设备。您或用户可以联系 Apple 技术支持人员来直接解锁设备。
- 确认硬件清单过程中，XenMobile Server 将查询设备中是否存在激活锁绕过码。如果绕过码可用，设备会将其发送到 XenMobile Server。之后，要从设备中删除绕过码，请从 XenMobile Server 控制台发送 “激活锁绕过” 安全操作。此时，XenMobile Server 和 Apple 将具有解锁设备所需的绕过码。
- “激活锁绕过” 安全操作依赖 Apple 服务的可用性。如果该操作无法运行，您可以按如下所示解锁设备。在设备上，手动输入 iCloud 帐户的凭据。或者，将 “用户名” 字段留空，并在 “密码” 字段中键入绕过码。要查找绕过码，请转至管理 **>** 设备，选择设备，单击编辑，然后单击属性。激活锁绕过码显示在安全信息下。

macOS

January 5, 2022

要在 XenMobile 中管理 macOS 设备，请设置 Apple 提供的 Apple 推送通知服务 (APNs) 证书。有关信息，请参阅 APNs 证书。

XenMobile 将 macOS 设备注册到 MDM 中。XenMobile 支持对 MDM 中的 macOS 设备使用以下注册身份验证类型。

- 域
- 域名加一次性密码
- 邀请 URL 加一次性密码

> **macOS 15** 中对可信证书的要求：
>
> Apple 对 TLS 服务器证书有新的要求。验证所有证书都符合 Apple 的新要求。请参阅 Apple 出版物 https://support.apple.com/en-us/HT210176。有关管理证书方面的帮助，请参阅在 XenMobile 中上载证书。

启动 macOS 设备管理的一般工作流程如下：

1. 配置 macOS 设备策略。
2. 注册 macOS 设备。
3. 设置设备和应用程序安全操作。请参阅安全操作。

有关支持的操作系统，请参阅支持的设备操作系统。

必须保持公开状态的 **Apple** 主机名

某些 Apple 主机名必须保持打开状态，以确保 iOS、macOS 和 Apple App Store 的正常运行。阻止这些主机名可能会影响以下对象的安装、更新和正确操作：iOS、iOS 应用程序、MDM 操作以及设备和应用程序注册。有关详细信息，请参阅 https://support.apple.com/en-us/HT201999。

支持的注册方法

下表列出了 XenMobile 支持的 macOS 设备的注册方法：

方法	支持
Apple 部署计划	是
Apple 校园教务管理	是
Apple Configurator	否
手动注册	是
注册邀请	是

Apple 制定了面向企业和教育帐户的设备注册计划。对于企业帐户，需要在 “Apple 部署计划” 中注册才能使用 Apple 设备注册计划在 XenMobile 中注册和管理设备。该计划面向 iOS 和 macOS 设备。请参阅通过 Apple 部署计划部署设备。

对于教育帐户，需要创建一个 Apple 校园教务管理帐户。Apple 校园教务管理统一了部署计划和批量购买。Apple 校园教务管理的类型为教育 Apple 部署类型。请参阅与 Apple 教育功能相集成。

可以使用 Apple 部署计划批量注册 iOS 和 macOS 设备。可以直接从 Apple 、参与计划的 Apple 授权经销商或运营商处购买这些设备。

配置 **macOS** 设备策略

使用这些策略可配置 XenMobile 与运行 macOS 的设备的交互方式。下表列出了适用于 macOS 设备的所有设备策略。

AirPlay 镜像	应用程序清单	日历 (CalDav)
联系人 (CardDAV)	控制操作系统更新	凭据
设备名称	Exchange	FileVault
防火墙	字体	导入 iOS 和 macOS 配置文件
LDAP	邮件	通行码
配置文件删除	限制	SCEP
VPN	Web 剪辑	Wi-Fi

注册 **macOS** 设备

XenMobile 提供两种方法来注册运行 macOS 的设备。这两种方法都使 macOS 用户能够直接从其设备无线注册。

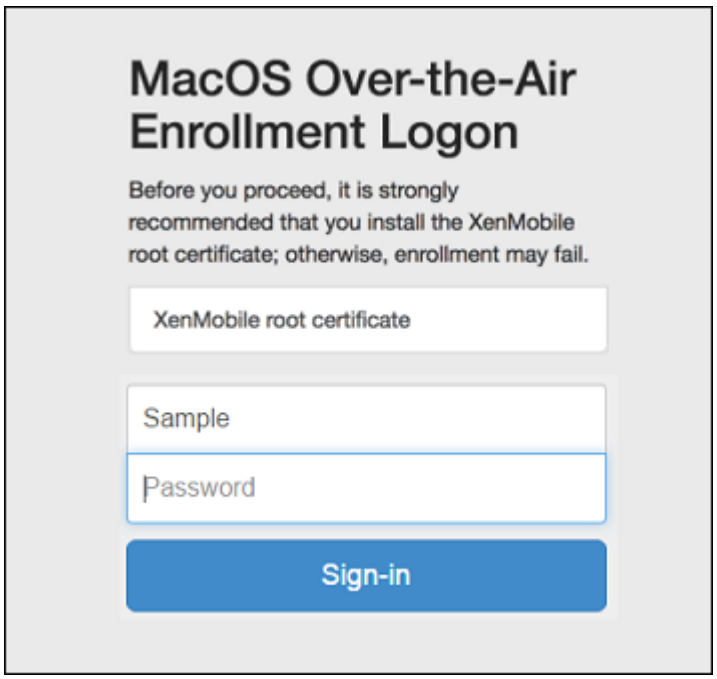
- 向用户发送注册邀请：此注册方法允许您为 macOS 设备设置以下任意注册安全模式：
  - 用户名 + 密码
  - 用户名 + PIN
  - 双重身份验证

  用户按照注册邀请中的说明进行操作时，将显示一个填写了用户名的登录屏幕。
- 向用户发送注册链接：此注册方法适用于 macOS 设备，向用户发送一个注册链接，用户可以在 Safari 或 Chrome 浏览器中打开该链接。用户随后通过提供其用户名和密码进行注册。

  要阻止对 macOS 设备使用注册链接，请将服务器属性启用 **macOS OTAE** 设置为 **false**。因此，macOS 用户只能使用注册邀请进行注册。

向 **macOS** 用户发送注册邀请

1. 添加面向 macOS 用户注册的邀请。请参阅创建注册邀请。
2. 用户收到邀请并单击链接后，以下屏幕将在 Safari 浏览器中显示。XenMobile 填写用户名。如果您为注册安全模式选择双重，则将显示另一个字段。



3. 用户根据需要安装证书。用户是否会收到安装证书的提示取决于您是否为 macOS 配置了以下证书：公众信任的 SSL 证书和公众信任的数字签名证书。有关证书的信息，请参阅证书和身份验证。
4. 用户提供请求的凭据。

   安装 Mac 设备策略。现在即可以像管理移动设备一样使用 XenMobile 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 XenMobile 的服务器的完全限定域名 (FQDN)。
   - 端口 **8443** 为默认安全端口。如果已配置其他端口，请使用该端口替换 8443。
   - **instanceName**（通常显示为 `zdm`）为在服务器安装过程中指定的名称。

   有关发送安装链接的详细信息，请参阅发送注册邀请。
2. 用户根据需要安装证书。如果您为 iOS 和 macOS 配置了公众信任的 SSL 证书和数字签名证书，用户将看到安装证书的提示。有关证书的信息，请参阅证书和身份验证。
3. 用户登录其 Mac 设备。

   安装 Mac 设备策略。现在即可以像管理移动设备一样使用 XenMobile 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。

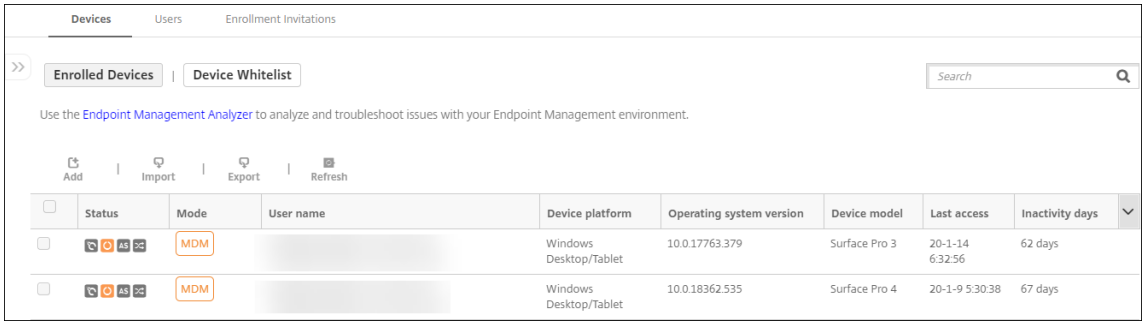
吊销	锁定	选择性擦除
完全擦除	证书续订	

锁定 **macOS** 设备

可以远程锁定丢失的 macOS 设备。XenMobile 锁定设备。它随之生成一个 PIN 代码并在设备中进行设置。要访问设备，用户需要键入该 PIN 代码。使用取消锁定可从 XenMobile 控制台中删除锁定。

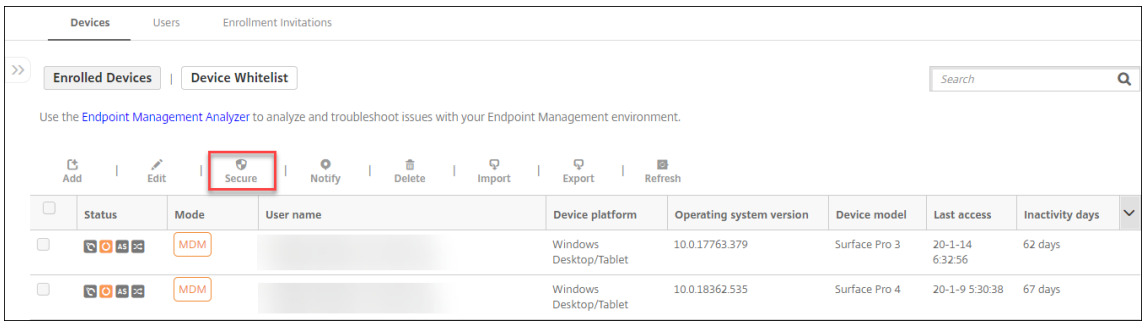
可以使用通行码设备策略配置与 PIN 代码关联的更多设置。有关详细信息，请参阅 macOS 设置。

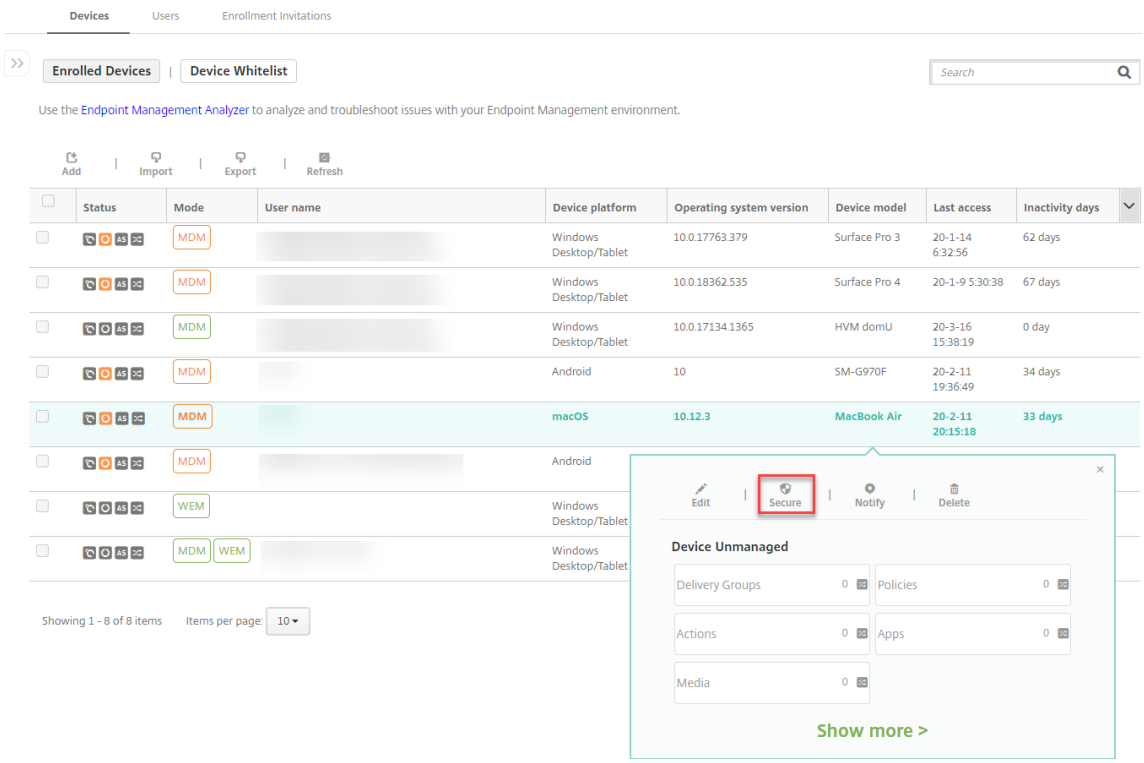
1. 单击管理 **>** 设备。此时将显示设备页面。



2. 选择要锁定的 macOS 设备。

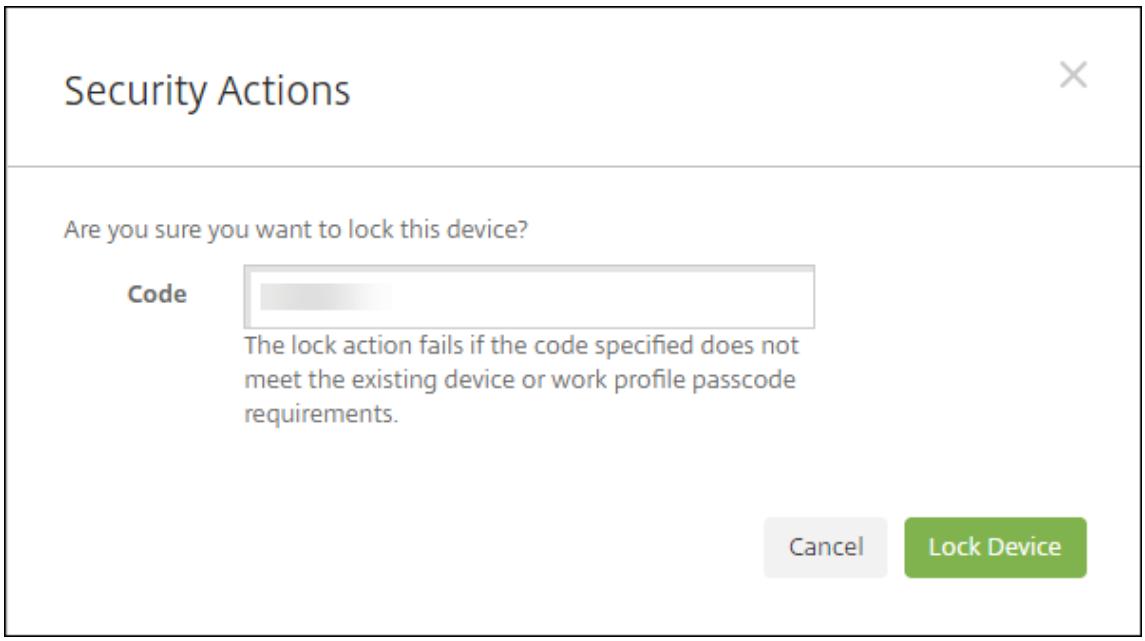
   选中设备旁边的复选框以显示设备列表上方的选项菜单。也可以单击列出的项目上的其他任何位置，以在此列表的右侧显示选项菜单。





3. 在选项菜单中，选择安全。此时将显示安全操作对话框。

4. 单击锁定。此时将显示安全操作确认对话框。



5. 单击锁定设备。

> 重要：
>
> 还可以指定密码，而不是使用 XenMobile 生成的代码。如果指定的代码不符合设备或现有工作配置文件的代码要求，锁定操作将失败。

Apple 设备的批量注册

January 5, 2022

可以通过两种方式在 XenMobile 中注册大量 iOS、iPadOS 和 macOS 设备。

- 请使用 Apple 部署计划注册您直接从 Apple、Apple 授权经销商或运营商处购买的 iOS、iPadOS 和 macOS 设备。该支持包括共享 iPad。XenMobile 支持对 Apple 部署计划使用 Apple 商务管理 (ABM)，对教育行业使用 Apple 校园教务管理 (ASM)。本文介绍如何将多台设备与您的 ABM 帐户集成。有关在 ABM 中注册以及将 ABM 帐户与 XenMobile 关联的信息，请参阅通过 Apple 部署计划部署设备。有关 Apple 校园教务管理帐户的信息，请参阅与 Apple 教育功能相集成。

  对于 macOS 设备的注册，XenMobile 要求设备运行 macOS 10.10 或更高版本。

- 还可以使用 Apple Configurator 2 注册 iOS 设备，无论这些设备是否直接从 Apple 购买，皆可注册。

通过 ABM：

- 您不需要触摸或准备设备。只需通过提交设备序列号或采购订单编号，即可配置并注册设备。
- XenMobile 注册设备后，可以将其提供给能够立即使用这些设备的用户。通过 ABM 设置设备时，可以不执行用户在首次启动设备时需要完成的某些设置助理步骤。

- 有关设置 ABM 的详细信息，请参阅 Apple 商务管理中提供的文档。

使用 Apple Configurator 2：

- 需要将 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 Apple 计算机。请通过 Apple Configurator 2 准备 iOS 设备并配置策略。
- 为设备预配所需的策略后，首次将设备连接到 XenMobile 时，这些设备将从 XenMobile 接收策略。您之后可以开始管理设备。
- 有关使用 Apple Configurator 2 的详细信息，请参阅 Apple Configurator 帮助。

必备条件

打开所需的端口以在 XenMobile 与 Apple 之间建立连接。有关详细信息，请参阅端口要求。

将 **Apple** 商务管理帐户与 **XenMobile** 相集成

如果您没有使用 XenMobile 设置 ABM 帐户，请完成通过 Apple 部署计划部署设备中的以下步骤。

- 在 Apple 商务管理中注册。
- 将您的 Apple 商务管理帐户与 XenMobile 相关联。
- 启用了订单部署计划的设备。
- 管理启用了部署程序的设备。

为批量注册设置默认服务器

要将 iOS、iPadOS 和 macOS 设备的大量订单分配给 MDM 服务器，可以将 XenMobile 设置为默认服务器。

1. 使用管理员或设备注册管理员帐户登录到 Apple 商务管理。
2. 在边栏中，单击设置 **>** 设备管理设置。
3. 选择现有的 MDM 服务器。在 **Default Device Assignment**（默认设备分配）下，单击 **Change**（更改）。为每种设备类型选择默认的 XenMobile Server。单击完成。

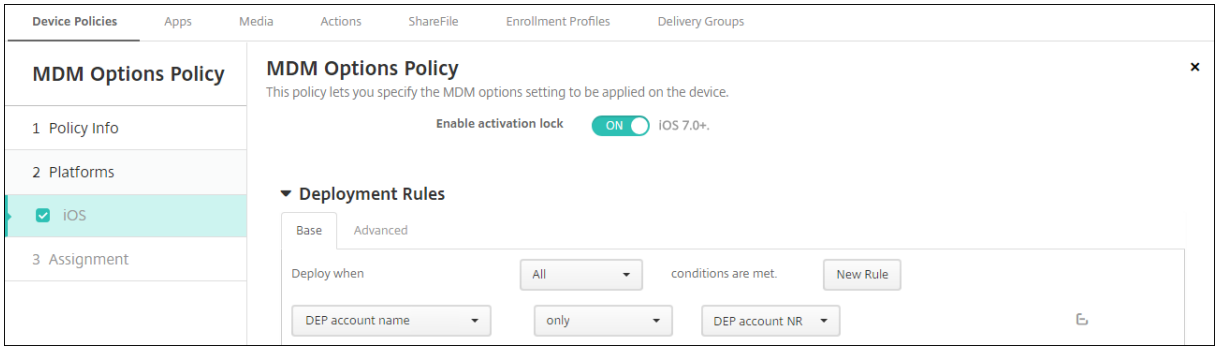
配置 **ABM** 帐户的设备策略和应用程序的部署规则

可以使用配置 **>** 设备策略和配置 **>** 应用程序下的部署规则部分将 ABM 帐户与不同的设备策略和应用程序关联。可以指定某个策略或应用程序：

- 仅针对特定的 ABM 帐户部署。
- 针对除所选帐户外的所有 ABM 帐户部署。

ABM 帐户的列表仅包括状态为已启用或已禁用的帐户。如果 ABM 帐户已禁用，ABM 设备将不属于该帐户。因此，XenMobile 不会将应用程序或策略部署到该设备。

在以下示例中，设备策略仅针对 ABM 帐户名称为 “ABM Account NR” 的设备进行部署。

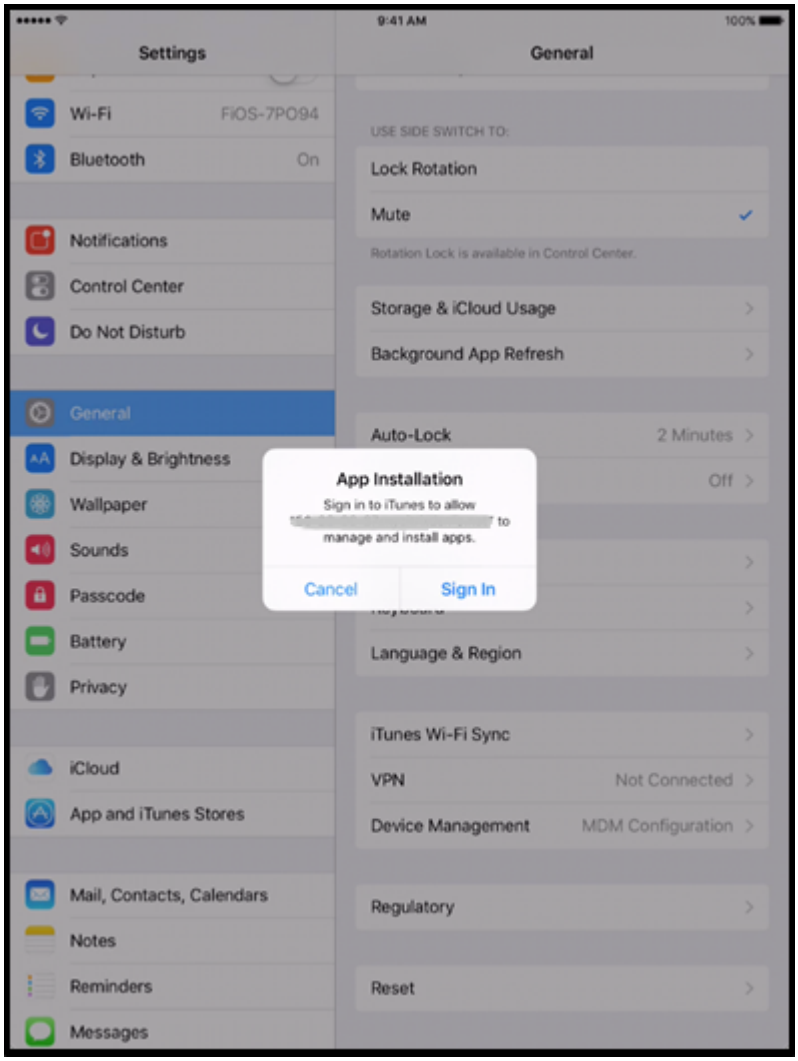


注册启用了 **Apple** 部署计划的设备时的用户体验

用户注册启用了 Apple 部署计划的设备时，其体验如下。

1. 用户启动启用了 Apple 部署计划的设备。
2. XenMobile 将您在 XenMobile 控制台中配置的 Apple 部署计划配置提交至启用了 Apple 部署计划的设备。
3. 用户在其设备上配置初始设置。
4. 该设备将自动启动 XenMobile 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 XenMobile 配置为使用基于设备的批量购买应用程序分配来部署 Secure Hub 应用程序，则此步骤是可选步骤。在这种情况下，不需要创建 Apple App Store 帐户，也不需要使用现有帐户。



7. 用户打开 Secure Hub 并键入其凭据。如果策略要求，系统可能会提示用户创建并验证 Citrix PIN。

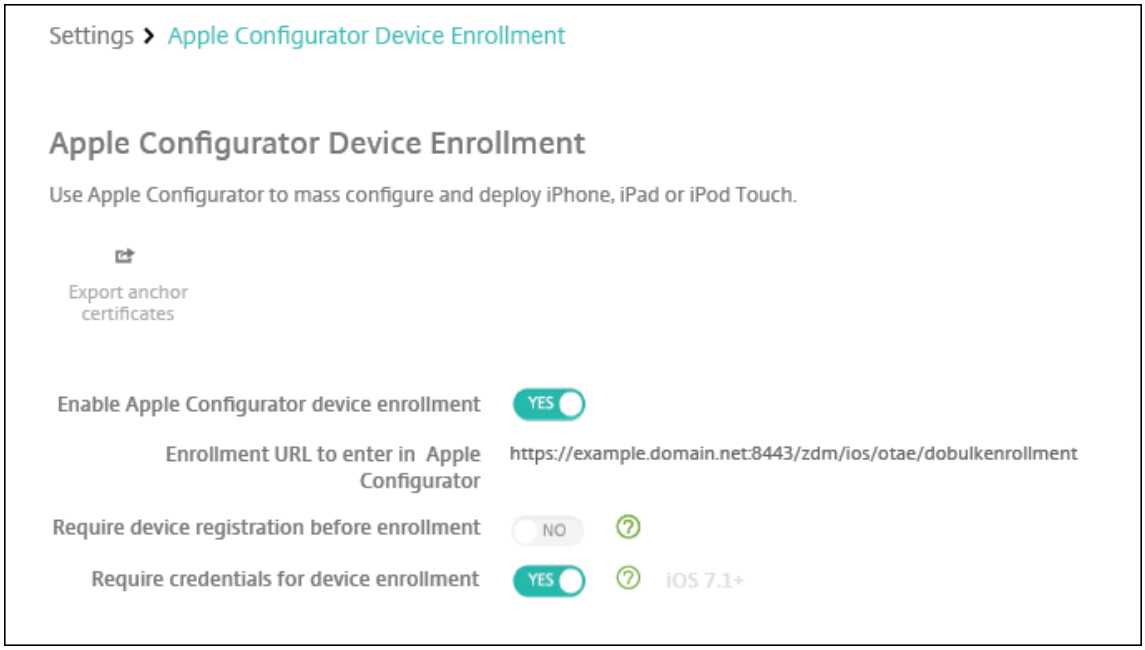
   XenMobile 将任何其余必备应用程序部署到设备。

配置 **Apple Configurator 2** 设置

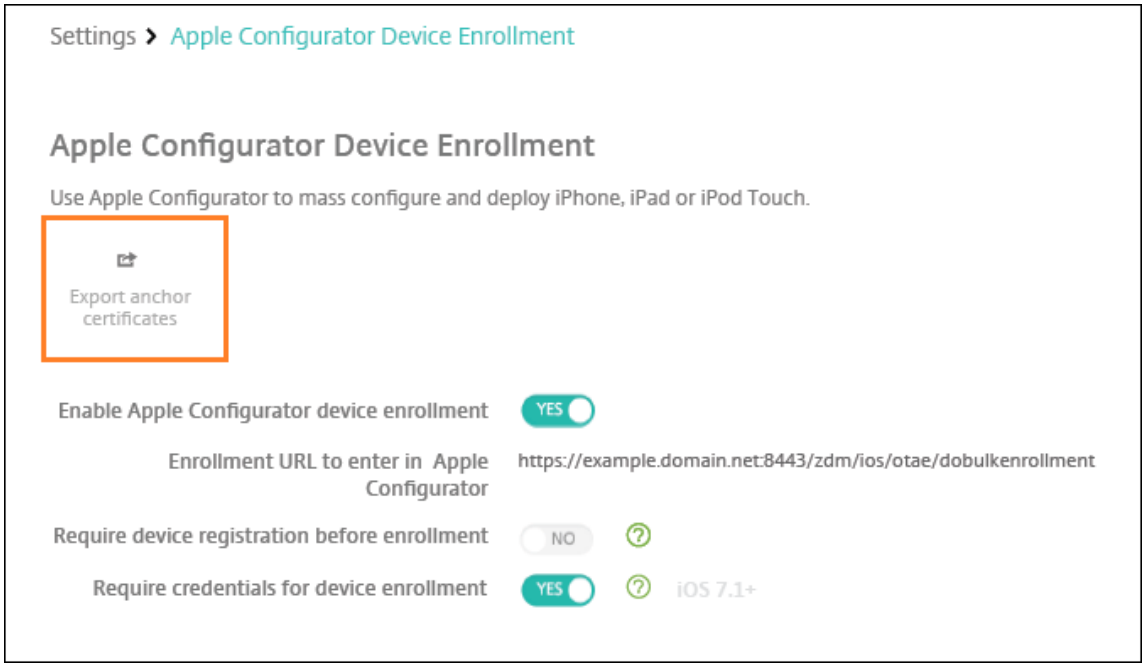
可以使用 Apple Configurator 2 而非 Apple 商务管理批量配置和部署 iPhone 和 iPad 设备。

步骤 **1**：在 **XenMobile** 中配置设置

1. 在 XenMobile 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. **Enrollment URL to enter in Apple Configurator**（要在 Apple Configurator 中输入的注册 URL）为只读字段。此设置提供 XenMobile Server 与 Apple 通信时使用的 URL。请在 Apple Configurator 2 中配置设置时复制并粘贴此 URL。注册 URL 是指 XenMobile Server 的完全限定域名 (FQDN)（例如 `mdm.server.url.com`）或 IP 地址。
4. 要防止注册未知设备，请将要求在注册之前注册设备设置为是。注意：如果此设置为是，必须先在 XenMobile 中手动或通过 CSV 文件将配置的设备添加到管理 **>** 设备，然后再进行注册。
5. 请将需要提供凭据才能完成设备注册设置为是，才能要求使用 iOS 设备的用户在注册时输入其凭据。默认为不要求提供注册凭据。
6. 注意：如果 XenMobile Server 使用的是可信 SSL 证书，请跳过此步骤。单击导出锚点证书，然后将 certchain.pem 文件保存到 macOS 钥匙串中（登录或系统）。



步骤 **2**：在 **Apple Configurator 2** 中配置设置

1. 从 App Store 安装 Apple Configurator 2。
2. 使用 Dock 连接器到 USB 电缆将设备连接到运行 Apple Configurator 2 的 Mac。最多可以同时配置 30 台已连接的设备。如果没有基座接口，请使用一个或多个有源 USB 2.0 高速集线器连接设备。
3. 启动 Apple Configurator 2。该配置器会显示您能够准备监督的任何设备。
4. 准备设备以进行监督：
   - 如果您打算通过定期重新应用配置来保留对设备的控制权，请选择 **Supervise devices**（监督设备）。单击 **Next**（下一步）。

     > 重要：
     >
     > 将设备置于受监督模式时，系统将会在设备上安装所选版本的 iOS，同时完全擦除设备上以前存储的任何用户数据或应用程序。

   - 在 iOS 中，单击 **Latest**（最新），获取您要安装的最新版本的 iOS。
5. 在在 **MDM** 服务器中注册中，选择 MDM 服务器。要添加新服务器，请单击下一步
6. 在定义 **MDM** 服务器中，提供服务器的名称，然后从 XenMobile 控制台粘贴 MDM 服务器 URL。
7. 在分配给组织中，选择要监督设备的组织。

   有关通过 Apple Configurator 2 准备设备的详细信息，请参阅 Apple Configurator 帮助页面准备设备。
8. 在配置每个设备的过程中，请将其打开以启动 iOS 设置助理，以便为首次使用准备好设备。

将 **Apple Configurator 2** 中的设备分配给 **Apple** 商务管理

可以将 Apple Configurator 2 中的 iPhone 和 iPad 设备与您的 Apple 商务管理帐户相关联。添加设备时，它们将显示在设备部分中。这些设备不再包含通过 Apple Configurator 2 分配的注册设置。有关详细信息，请参阅将从 Apple Configurator 2 添加的设备分配给 Apple 商务管理。

使用 **Apple** 部署计划时续订或更新证书

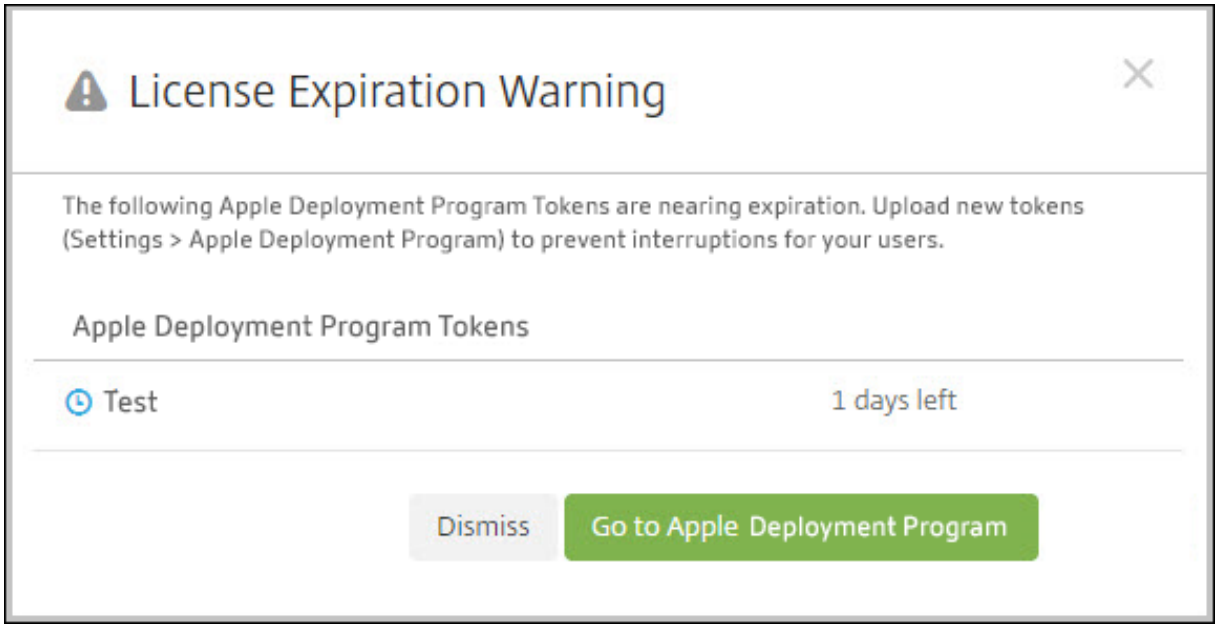
续订 XenMobile 安全套接字层 (SSL) 证书时，请在 XenMobile 控制台的设置 **>** 证书中上载新证书。在导入对话框的用作中，单击 **SSL** 侦听器，以便将该证书用于 SSL。重新启动服务器后，XenMobile 将使用新 SSL 证书。有关 XenMobile 中的证书的详细信息，请参阅在 XenMobile 中上载证书。

续订或更新 SSL 证书时，不需要在 Apple 部署计划与 XenMobile 之间重新建立信任关系。但是，可以按照本文中之前的步骤随时重新配置 **Apple** 部署计划设置。

有关 Apple 部署计划的详细信息，请参阅 Apple 文档。

续订 **Apple** 部署计划与 **XenMobile** 之间的连接

自动设备注册服务器令牌过期时，XenMobile 会显示许可证过期警告。



更换 Apple 校园教务管理/Apple 商务管理的令牌。

步骤 **1**：从 **XenMobile Server** 下载公钥

1. 在 XenMobile 控制台中，转至设置 **> Apple** 部署计划以下载新公钥。

步骤 **2**：在您的 **Apple** 帐户中创建并下载服务器令牌文件

1. 登录 Apple 商务管理以下载令牌。
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，上载您从 XenMobile 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 **XenMobile** 中上载服务器令牌文件

1. 在 Citrix XenMobile 中，转到设置 **> Apple** 部署计划。
2. 选择部署计划帐户，单击编辑，然后上载您的服务器令牌文件。
3. 单击下一步保存更改。

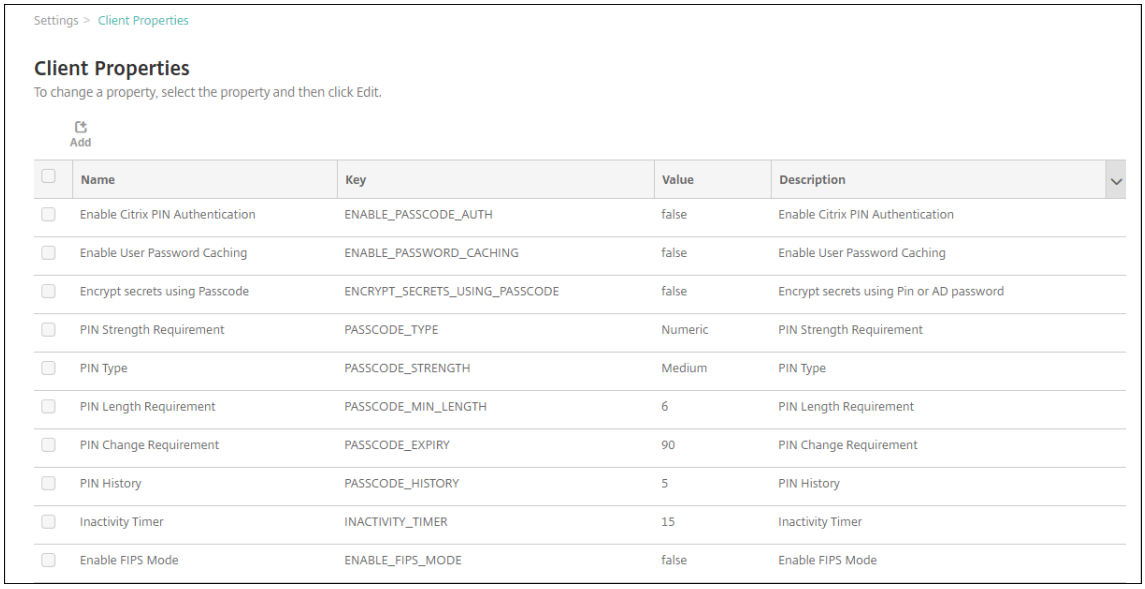
客户端属性

January 5, 2022

客户端属性包含用户设备上直接提供给 Secure Hub 的信息。可以使用这些属性配置高级设置，如 Citrix PIN。从 Citrix 支持获取客户端属性。

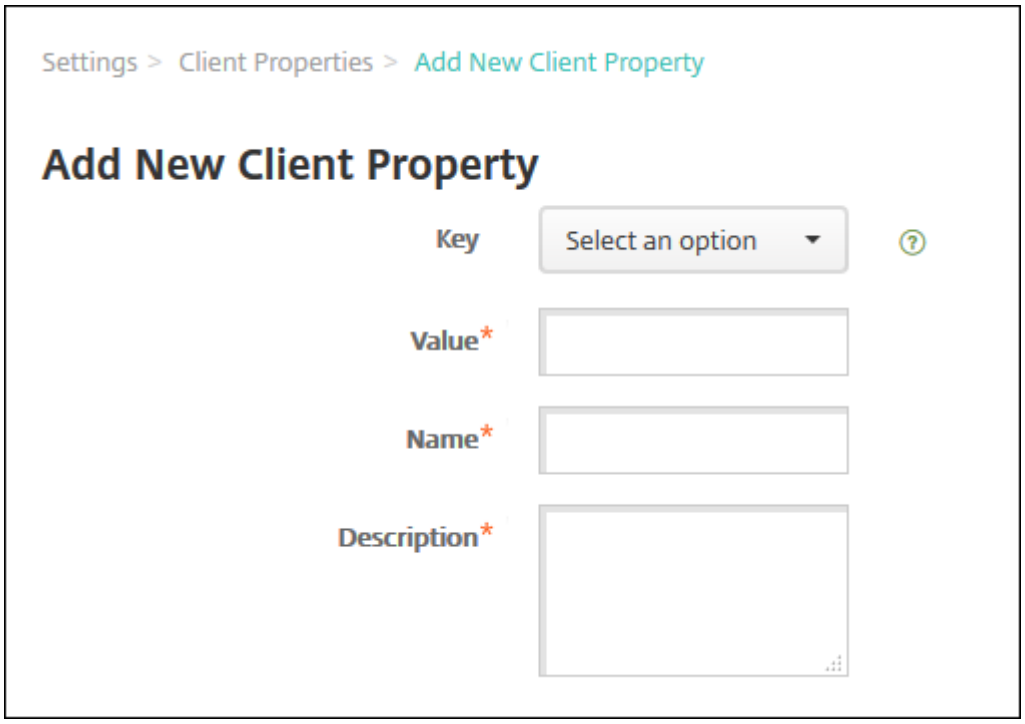
每次发布 Secure Hub 以及有时发布客户端应用程序时，均会更改客户端属性。有关通常要配置的客户端属性的详细信息，请参阅本文末尾的客户端属性参考。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在客户端下方，单击客户端属性。此时将显示客户端属性页面。可以从此页面添加、编辑和删除客户端属性。



添加客户端属性

1. 单击添加。此时将显示添加新客户端属性页面。



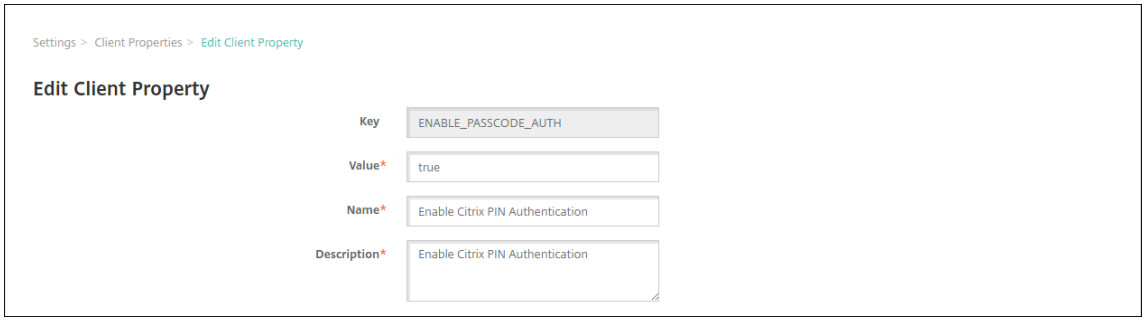
2. 配置以下设置：
   - 键：在列表中，单击要添加的属性键。重要：更新这些设置之前，请联系 Citrix 技术支持。您可以申请一个特殊键。
   - 值：选定属性的值。
   - 名称：属性的名称。
   - 说明：属性的说明。
3. 单击保存。

编辑客户端属性

1. 在客户端属性表格中，选择要编辑的客户端属性。

   选中客户端属性旁边的复选框时，选项菜单将显示在客户端属性列表上方。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。

2. 单击编辑。此时将显示编辑客户端属性页面。



3. 适当更改以下信息：
   - 键：无法更改此字段。
   - 值：属性值。
   - 名称：属性名称。
   - 说明：属性说明。
4. 单击保存以保存您所做更改，或单击取消保留属性不变。

删除客户端属性

1. 在客户端属性表格中，选择要删除的客户端属性。

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

客户端属性参考

XenMobile 预定义的客户端属性及其默认设置如下所示。

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 显示名称：MDX 容器自毁期限
  - 自毁功能阻止在经过指定天数的非活动状态后访问 Secure Hub 和托管应用程序。超过该时间限制后，应用程序将不再可用。擦除数据包括清除已安装的各应用程序的应用程序数据，包括应用程序缓存和用户数据。

    不活动时间是指在经过特定时间长度后，服务器不接收身份验证请求以验证用户。例如，如果此属性为 30 天，并且用户不使用应用程序的时间超过 30 天，此策略将生效。

    此全局安全策略适用于 iOS 和 Android 平台，是对现有应用程序锁定和擦除策略的增强。
  - 要配置此全局策略，请转至设置 > 客户端属性，然后添加自定义键 **CONTAINER_SELF_DESTRUCT_PERIOD**。
  - 值：天数
- **DEVICE_LOGS_TO_IT_HELP_DESK**

- 显示名称：向 IT 技术支持人员发送设备日志
- 此属性启用或禁用向 IT 技术支持人员发送日志的功能。
- 可能的值：**true** 或 **false**
- 默认值：**false**

- **DISABLE_LOGGING**
  - 显示名称：禁用日志记录
  - 使用此属性可阻止用户从其设备收集和上载日志。此属性禁用 Secure Hub 以及已安装的所有 MDX 应用程序的日志记录功能。用户无法从“支持”页面发送任何应用程序的日志。即使显示了邮件撰写对话框，也不附加日志。此时将显示一条消息，指示日志记录功能已禁用。此设置还阻止您在 XenMobile 控制台中更新 Secure Hub 和 MDX 应用程序的日志设置。

    此属性设置为 **true** 时，Secure Hub 会将阻止应用程序日志设置为 **true**。因此，应用新策略时，MDX 应用程序将停止日志记录。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**（不禁用日志记录）

- **ENABLE_CRASH_REPORTING**
  - 显示名称：启用崩溃报告
  - 如果设置为 **true**，Citrix 将收集崩溃报告和诊断信息以帮助对 Secure Hub for iOS 和 Secure Hub for Android 相关问题进行故障排除。如果设置为 **false**，则不收集任何数据。
  - 可能的值：**true** 或 **false**
  - 默认值：**true**

- **ENABLE_CREDENTIAL_STORE**
  - 显示名称：启用凭据存储区
  - 启用凭据存储区意味着 Android 或 iOS 用户在访问移动生产力应用程序时输入一次其密码。可以使用凭据存储区，无论是否启用 Citrix PIN。如果不启用 Citrix PIN，用户输入其 Active Directory 密码。XenMobile 只对 Secure Hub 和公共应用商店应用程序支持将 Active Directory 密码用于凭据存储区。如果您将 Active Directory 密码用于凭据存储区，XenMobile 将不支持 PKI 身份验证。
  - 要在 Secure Mail 中自动注册，需要将此属性设置为 **true**。
  - 要配置此自定义客户端策略，请转至设置 > 客户端属性，添加自定义键 **ENABLE_CREDENTIAL_STORE**，并将值设置为 **true**。

- **ENABLE_FIPS_MODE**
  - 显示名称：启用 FIPS 模式
  - 此属性在移动设备上启用或禁用 FIPS 模式。更改此值后，Secure Hub 会在执行下一次联机身份验证时将新值传递到设备。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**

- **ENABLE_PASSCODE_AUTH**
  - 显示名称：启用 Citrix PIN 身份验证
  - 此属性允许您打开 Citrix PIN 功能。启用 Citrix PIN 或通行码后，系统将提示用户定义要使用的 PIN（而非其 Active Directory 密码）。如果启用了 ENABLE_PASSWORD_CACHING，或者如果 XenMobile 使用证书身份验证，此设置将自动启用。

    执行脱机身份验证时，Citrix PIN 将在本地验证，并且允许用户访问请求的应用程序或内容。执行联机身份验证时，Citrix PIN 或通行码将解锁 Active Directory 密码或证书，随后将发送该密码或证书以通过 XenMobile 执行身份验证。

    如果 ENABLE_PASSCODE_AUTH 设置为 true，ENABLE_PASSWORD_CACHING 设置为 false，联机身份验证将始终提示输入密码，因为 Secure Hub 不保存该密码。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **ENABLE_PASSWORD_CACHING**
  - 显示名称：启用用户密码缓存
  - 此属性允许在移动设备上本地缓存 Active Directory 密码。将此属性设置为 **true** 时，还必须将 **ENABLE_PASSCODE_AUTH** 属性设置为 **true**。如果启用了用户密码缓存，XenMobile 将提示用户设置 Citrix PIN 或通行码。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **ENABLE_TOUCH_ID_AUTH**
  - 显示名称：启用 Touch ID 身份验证
  - 对于支持 Touch ID 身份验证的设备，此属性将在设备上启用或禁用 Touch ID 身份验证。要求：

    用户设备必须启用 Citrix PIN 或 LDAP。如果 LDAP 身份验证处于关闭状态（例如，因为使用了仅基于证书的身份验证），则用户必须设置 Citrix PIN。在这种情况下，XenMobile 要求使用 Citrix PIN，即使客户端属性 **ENABLE_PASSCODE_AUTH** 为 **false** 也是如此。

    将 **ENABLE_PASSCODE_AUTH** 设置为 **false**，以便用户启动应用程序时，他们必须响应提示以使用 Touch ID。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **ENABLE_WORXHOME_CEIP**
  - 显示名称：启用 Worx Home CEIP
  - 此属性将打开客户体验改善计划。该功能会定期向 Citrix 发送匿名配置和使用数据。该数据将帮助 Citrix 提高 XenMobile 的品质、可靠性和性能。
  - 值：**true** 或 **false**

- 默认值：**false**

- **ENABLE_WORXHOME_GA**
  - 显示名称：在 Worx Home 中启用 Google Analytics
  - 此属性将启用或禁用在 Secure Hub 中使用 Google Analytics 收集数据的功能。更改此设置时，仅当用户下次登录 Secure Hub（以前称为 Worx Home）时才设置新值。
  - 可能的值：**true** 或 **false**
  - 默认值：**true**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 显示名称：使用通行码加密机密
  - 此属性将敏感数据存储在设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串。此属性允许使用强加密的密钥，但还会添加用户熵。用户熵是用户生成的只有自己知道的随机 PIN 代码。

    Citrix 建议您启用此属性以帮助提高用户设备的安全性。因此，用户将遇到多个要求输入 Citrix PIN 的身份验证提示。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**

- **INACTIVITY_TIMER**
  - 显示名称：不活动计时器
  - 此属性定义用户可以保持其设备处于不活动状态且之后访问应用程序不会提示输入 Citrix PIN 或通行码的时间长度。要为 MDX 应用程序启用此设置，请将“应用程序通行码”设置设为“开”。如果“应用程序通行码”设置设为关，用户将被重定向到 Secure Hub 以执行完全身份验证。更改此设置时，该值将在系统下次提示用户进行身份验证时生效。

    在 iOS 上，不活动计时器还将管理 MDX 应用程序和非 MDX 应用程序对 Secure Hub 的访问。
  - 可能的值：任意正整数
  - 默认值：**15**（分钟）

- **ON_FAILURE_USE_EMAIL**
  - 显示名称：失败时使用电子邮件向 IT 技术支持人员发送设备日志
  - 此属性启用或禁用使用电子邮件向 IT 发送设备日志的功能。
  - 可能的值：**true** 或 **false**
  - 默认值：**true**

- **PASSCODE_EXPIRY**
  - 显示名称：PIN 更改要求
  - 此属性定义 Citrix PIN 或通行码的有效时间长度，超过此时间后，系统将强制用户更改其 Citrix PIN 或通行码。更改此设置时，仅在当前 Citrix PIN 或通行码过期时才设置新值。

- 可能的值：**1** 到 **99**（建议）。为了永远不重置 PIN，请将该值设置为一个非常大的数值（例如 100000000000）。如果最初设置的过期期限介于 1 到 99 天之间，然后在该时间段内更改为更大的数值，PIN 在初始期限结束时仍会过期，但之后永不过期。
- 默认值：**90**（天）

- **PASSCODE_HISTORY**
  - 显示名称：PIN 历史记录
  - 此属性定义之前使用的 Citrix PIN 或通行码的数量，用户在更改其 Citrix PIN 或通行码时不能重用。如果更改此设置，用户下次重置其 Citrix PIN 或通行码时将设置新值。
  - 可能的值：**1** 到 **99**
  - 默认值：**5**
- **PASSCODE_MAX_ATTEMPTS**
  - 显示名称：PIN 尝试次数
  - 此属性定义用户可以尝试输入错误 Citrix PIN 或通行码的次数，之后系统将提示用户进行完全身份验证。用户成功执行完全身份验证后，系统将提示其创建 Citrix PIN 或通行码。
  - 可能的值：任意正整数
  - 默认值：**15**
- **PASSCODE_MIN_LENGTH**
  - 显示名称：PIN 长度要求
  - 此属性定义 Citrix PIN 的最小长度。
  - 可能的值：**4** 到 **10**
  - 默认值：**6**
- **PASSCODE_STRENGTH**
  - 显示名称：PIN 强度要求
  - 此属性定义 Citrix PIN 或通行码的强度。更改此设置时，系统将在下次提示用户进行身份验证时提示其创建 Citrix PIN 或通行码。
  - 可能的值：低、中、高或强
  - 默认值：中
  - 每种强度设置的密码规则如下所示，具体取决于 PASSCODE_TYPE 设置：

数字通行码的规则：

通行码强度	数字通行码类型的规则	允许	不允许
低	所有数字，允许使用任意顺序	444444、123456、654321	
中（默认设置）	所有数字不能相同，也不能连续。	444333、124567、136790、555556、788888	444444、123456、654321

通行码强度	数字通行码类型的规则	允许	不允许
高	相邻的数字不能相同。	123512、134134、132312、131313、987456	080080、112233、135579、987745、919199
强	请勿使用同一编号超过两次。请勿连续使用三个或更多连续数字。请勿按相反的顺序使用三个或更多连续的数字。	102983、085085、824673、132312	132132、131313、902030

字母数字通行码的规则：

通行码强度	字母数字通行码类型的规则	允许	不允许
低	必须至少包含一个数字和一个字母	aa11b1、Abcd1#、Ab123~、aaaa11、aa11aa	AAAaaa、aaaaaa、abcdef
中（默认设置）	除“低”通行码强度的规则外，字母和所有数字都不能相同。字母和数字都不能连续。	aa11b1、aaa11b、aaa1b2、abc145、xyz135、sdf123、ab12c3、a1b2c3、Abcd1#、Ab123~	aaaa11、aa11aa 或 aaa111；abcd12、bcd123、123abc、xy1234、xyz345 或 cba123
高	至少包括一个大写字母和一个小写字母。	Abcd12、jkrtA2、23Bc#、AbCd	abcd12、DFGH2
强	至少包括一个数字、一个特殊符号、一个大写字母以及一个小写字母。	Abcd1#、Ab123~、xY12#3、Car12#、AAbc1#	abcd12、Abcd12、dfgh12、jkrtA2

- **PASSCODE_TYPE**
  - 显示名称：PIN 类型
  - 此属性定义用户能够定义数字型 Citrix PIN 还是字母数字型通行码。选择数字时，用户只能定义数字 (Citrix PIN)。选择字母数字时，用户可以使用字母和数字的组合（通行码）。

    如果更改此设置，用户必须在系统下次提示进行身份验证时设置新 Citrix PIN 或通行码。
  - 可能的值：数字或字母数字
  - 默认值：数字

- **REFRESHINTERVAL**
  - 显示名称：REFRESHINTERVAL
  - 默认情况下，XenMobile 每隔 3 天会对 Auto Discovery Server (ADS) 执行 ping 命令查找固定证书。要更改刷新时间间隔，请转至设置 **>** 客户端属性，添加自定义键 **REFRESHINTERVAL**，并将值设置为小时数。
  - 默认值：**72** 小时（3 天）
- **SEND_LDAP_ATTRIBUTES**
  - 对于 Android、iOS 或 macOS 设备的仅 MAM 部署：可以配置 XenMobile，以便使用电子邮件凭据在 Secure Hub 中注册的用户能够自动在 Secure Mail 中注册。因此，用户不需要提供额外的信息或执行额外的步骤即可在 Secure Mail 中注册。
  - 要配置此全局客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **SEND_LDAP_ATTRIBUTES**，并按如下所示设置值。
  - 值：`userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
  - 与 MDM 策略类似，属性值会指定为宏。
  - 以下示例介绍了帐户服务如何响应此属性：

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName=
    eng1,displayName=user\,test1,email=user@site.com\,user@site.com"
    name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - 对于此属性，XenMobile 会将逗号字符视为字符串终止符。因此，如果属性值包括一个逗号，请在其前面添加一个反斜杠。反斜杠将阻止客户端将嵌入的逗号解释为属性值的结尾。反斜杠字符表示为 `"\\"`。
- **HIDE_THREE_FINGER_TAP_MENU**
  - 此属性未设置或设置为 **false** 时，用户可以通过在其设备上执行三指轻按操作来访问隐藏的功能菜单。隐藏的功能菜单允许用户重置应用程序数据。将此属性设置为 **true** 将禁止用户访问隐藏的功能菜单。
  - 要配置此全局客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **HIDE_THREE_FINGER_TAP_MENU**，然后设置值。
- **TUNNEL_EXCLUDE_DOMAINS**
  - 显示名称：通道排除域
  - 默认情况下，MDX 将从 Micro VPN 通道中排除 XenMobile SDK 和应用程序用于各种功能的某些服务端点。例如，这些端点包括不需要通过企业网络路由的服务，例如 Google Analytics、Citrix Cloud Services 和 Active Directory 服务。可使用此客户端属性覆盖排除的默认域列表。
  - 要配置此全局客户端策略，请转至设置 **>** 客户端属性，添加自定义键 **TUNNEL_EXCLUDE_DOMAINS**，并设置值。

- 值：要将默认列表替换为要从通道中排除的域，请键入以逗号分隔的域后缀列表。要在通道中包括所有域，请键入 **none**。默认值：

  app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com

通过 **Apple** 部署计划部署设备

January 5, 2022

Apple 制定了面向企业和教育帐户的设备注册计划。对于企业帐户，需要在 “Apple 部署计划” 中注册才能使用 Apple 商务管理 (ABM) 或 Apple 校园教务管理 (ASM) 在 XenMobile 中注册和管理设备。该计划面向 iOS、iPadOS 和 macOS 设备。

Apple 部署计划面向组织而非个人提供。您必须提供大量企业详细信息以及创建 Apple 部署计划帐户所需的信息。因此，可能需要一些时间才能完成帐户申请并收到帐户审批结果。

对于教育帐户，需要创建一个 Apple 校园教务管理帐户。ASM 统一了 Apple 部署计划和 Apple 批量购买。要创建 Apple 校园教务管理帐户，请访问 Apple 校园教务站点。

注册 **Apple** 部署计划

要在 Apple 商务管理中注册，请转至 business.apple.com。单击立即注册申请新帐户。最佳做法是使用贵组织的电子邮件地址，例如 deployment@company.com。注册过程可能需要几天时间。收到登录凭据后，请按照 Apple 商务管理中提供的步骤创建帐户。

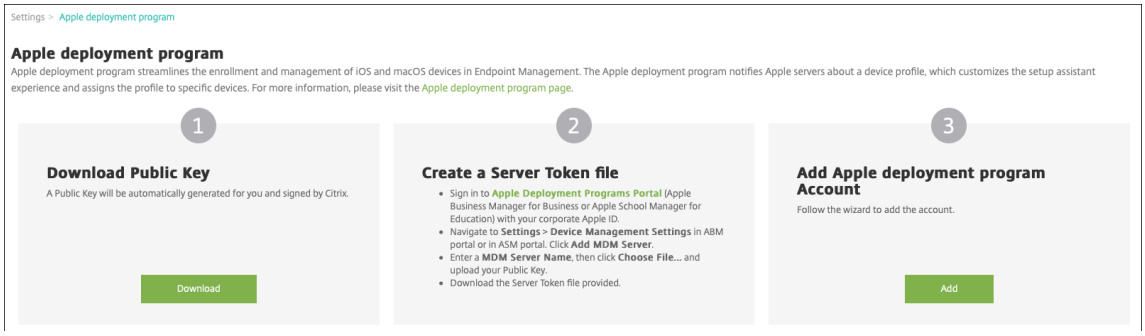
> 注意：
>
> 对于教育帐户，请参阅与 Apple 教育功能相集成。

将您的 **Apple** 商务管理帐户与 **XenMobile** 相关联

要将 Apple 商务管理帐户与 XenMobile 部署相关联，请在 XenMobile 控制台和 Apple 商务管理中输入信息。请按照以下步骤进行操作：

步骤 **1**：从 **XenMobile Server** 下载公钥

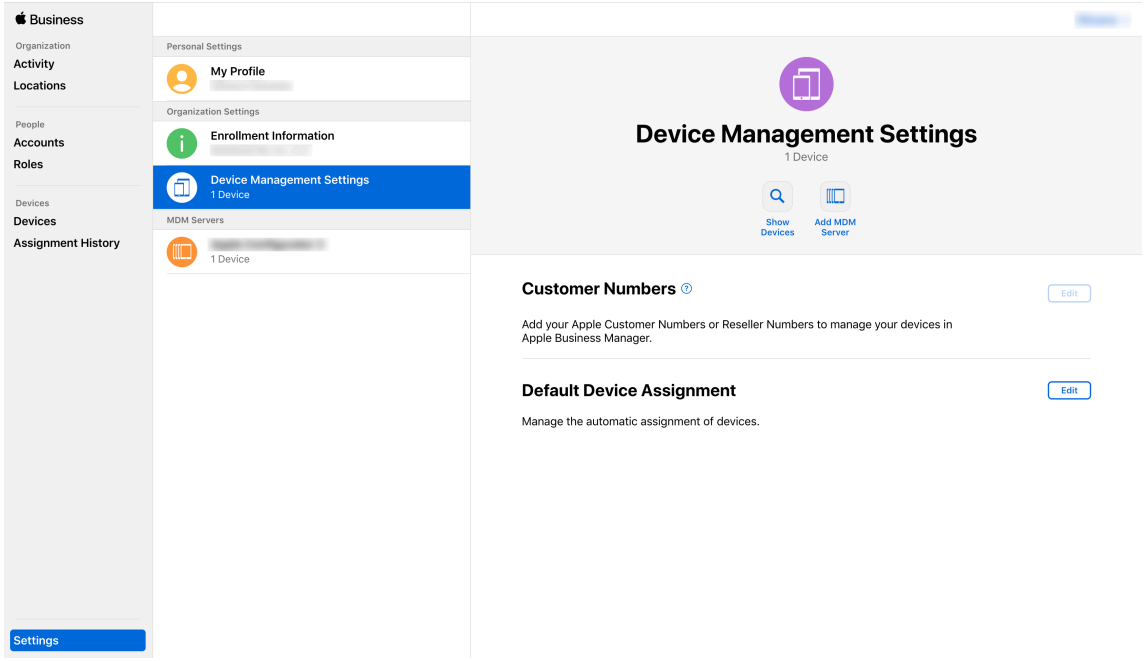
1. 在 XenMobile 控制台中，转至设置 **> Apple** 部署计划。



2. 在下载公钥下，单击下载。

步骤 **2**：在您的 **Apple** 帐户中创建并下载服务器令牌文件

1. 使用管理员或设备注册管理员帐户登录到 Apple 商务管理。
2. 在边栏底部，单击设置，然后单击设备管理设置 **>** 添加 **MDM** 服务器。



3. 在 **MDM** 服务器名称设置中，键入 XenMobile Server 的名称。键入的服务器名称仅供参考。它不是服务器的 URL 或名称。
4. 在 **Upload Public Key**（上载公钥）下，单击 **Choose File**（选择文件）。上载从 XenMobile 下载的公钥，然后保存更改。
5. 单击 **Download Token**（下载令牌）以将服务器令牌文件下载到您的计算机。

   必须在向 XenMobile 中添加 ABM 帐户时上载服务器令牌文件。导入令牌文件后，您的 ABM 令牌信息将在 XenMobile 控制台中显示。

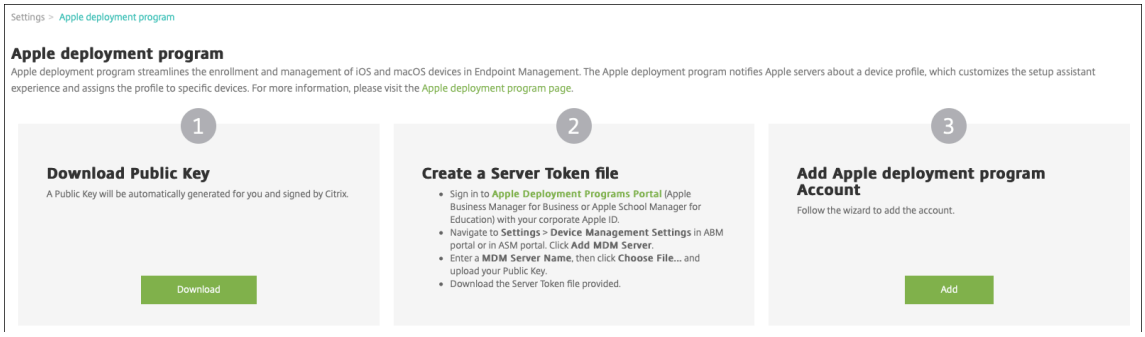
6. 在 **Default Device Assignment**（默认设备分配）下，单击 **Change**（更改）。选择设备的分配方式，然后提供所需的信息。有关信息，请参阅《ABM 用户指南》。

步骤 3：向 XenMobile 中添加 ABM 帐户

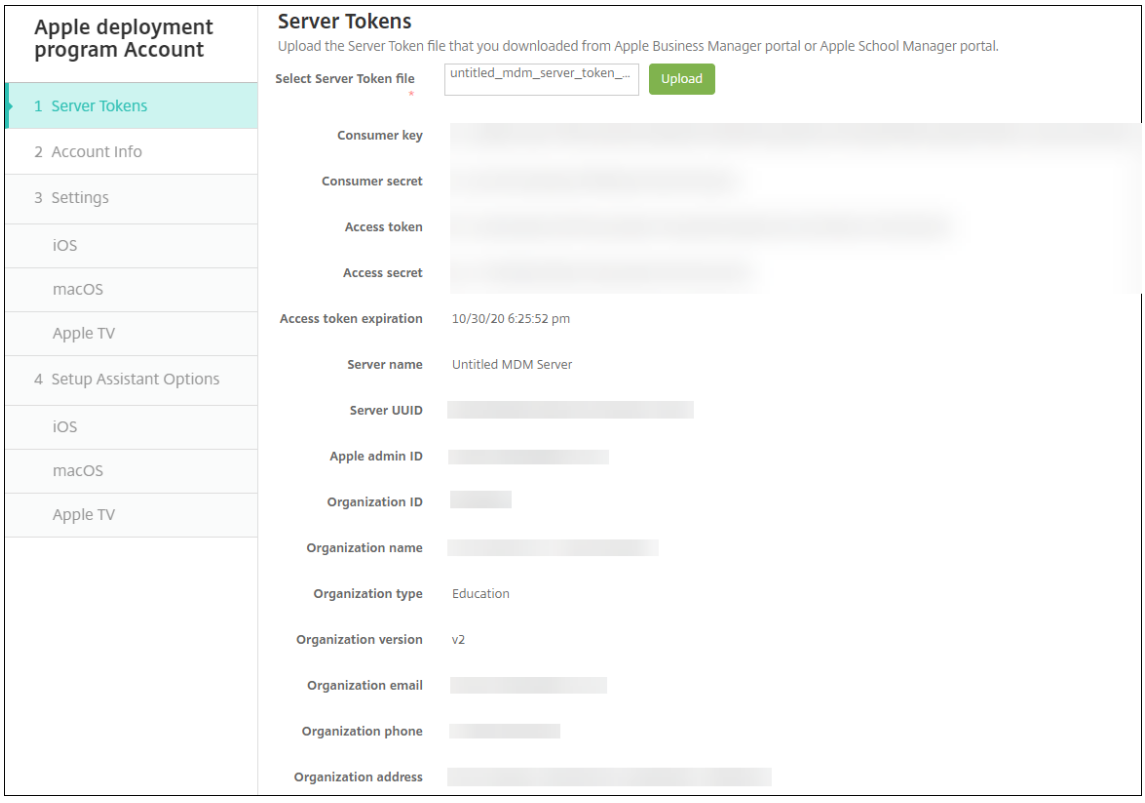
可以向 XenMobile 中添加多个 ABM 帐户。有了此功能，可以按国家/地区和部门等使用不同的注册设置和设置助理选项。然后将 ABM 帐户与不同的设备策略相关联。

例如，可以将来自不同国家/地区的所有 ABM 帐户集中在同一 XenMobile Server 上，以导入和监督所有 ABM 设备。通过按部门、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，策略将在整个组织中提供合适的功能，用户将获得恰当的帮助。

1. 在 XenMobile 控制台中，转至设置 **> Apple** 部署计划，然后在添加 **Apple** 部署计划帐户下，单击添加。

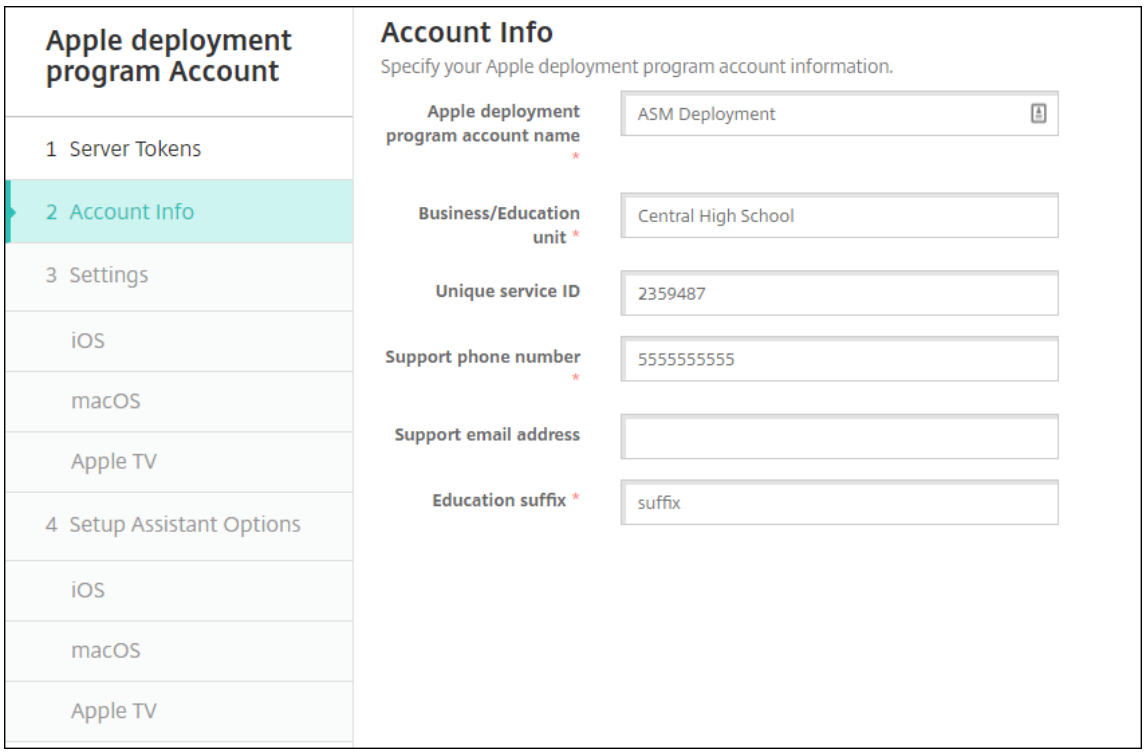


2. 在服务器令牌页面中，指定您的服务器令牌文件，然后单击上载。



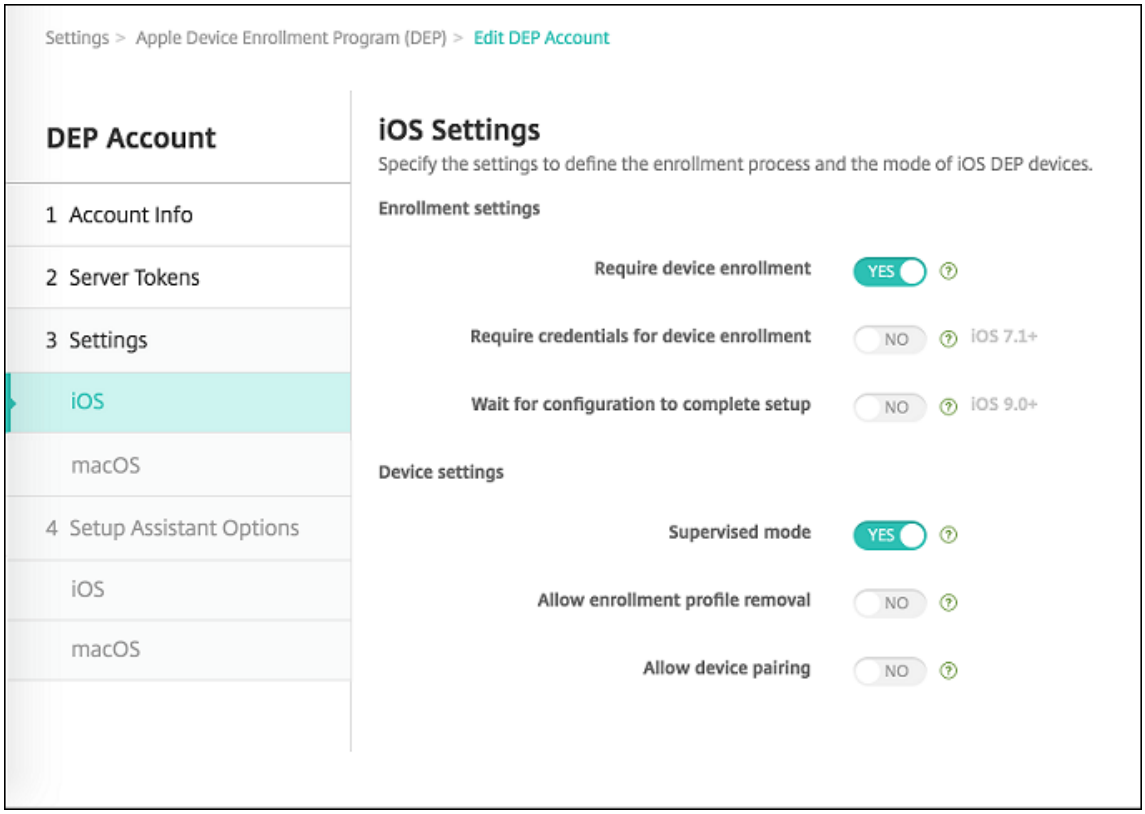
此时将显示您的服务器令牌信息。

3. 在帐户信息页面中，指定以下设置：



- **Apple** 部署计划帐户名称：此 Apple 部署计划帐户的唯一名称。请使用反映您如何组织 Apple 部署计划帐户（例如按国家/地区或组织层次结构）的名称。
- 业务/教育单位：将设备分配到的业务单位或部门。此字段为必填字段。
- 唯一服务 **ID**：有助于您进一步识别帐户的可选唯一 ID。
- 支持电话号码：支持电话号码，用户在设置期间拨打此号码寻求帮助。此字段为必填字段。
- 支持电子邮件地址：向最终用户提供的可选支持电子邮件地址。

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。默认值为是。
- 需要提供凭据才能完成设备注册： ABM 设置过程中是否需要用户输入其凭据。Citrix 建议您要求所有用户在设备注册期间输入其凭据，从而仅允许授权用户注册设备。默认值为是。

  如果您在首次设置之前启用 ABM 但不选择此选项，XenMobile 将创建 ABM 组件。此创建包括 ABM 用户、Secure Hub、软件清单和 ABM 部署组等组件。如果未选择此选项，XenMobile 将不创建这些组件。因此，如果您在以后清除此选项，则尚未输入其凭据的用户将无法在 ABM 中注册，因为这些 ABM 组件不存在。在这种情况下，要添加 ABM 组件，请禁用并启用 ABM 帐户。
- 等待完成配置设置：是否要求用户的设备一直保持在“设置助理”模式，直到将所有 MDM 资源部署到设备。此设置适用于处于受监督模式的设备。默认值为否。
- Apple 文档指出，当设备处于“设置助手”模式时，以下命令可能无法使用：
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

设备设置：

- 受监督模式：如果要使用 Apple Configurator 管理 ABM 注册的设备或启用了等待完成配置设置，必须设置为是。默认值为是。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 将 iOS 设备置于受监督模式。
- 允许删除注册配置文件：是否允许设备使用能够远程删除的配置文件。默认值为否。
- 允许设备配对：是否允许通过 ABM 注册的设备通过 Apple Music 和 Apple Configurator 进行管理。默认值为否。

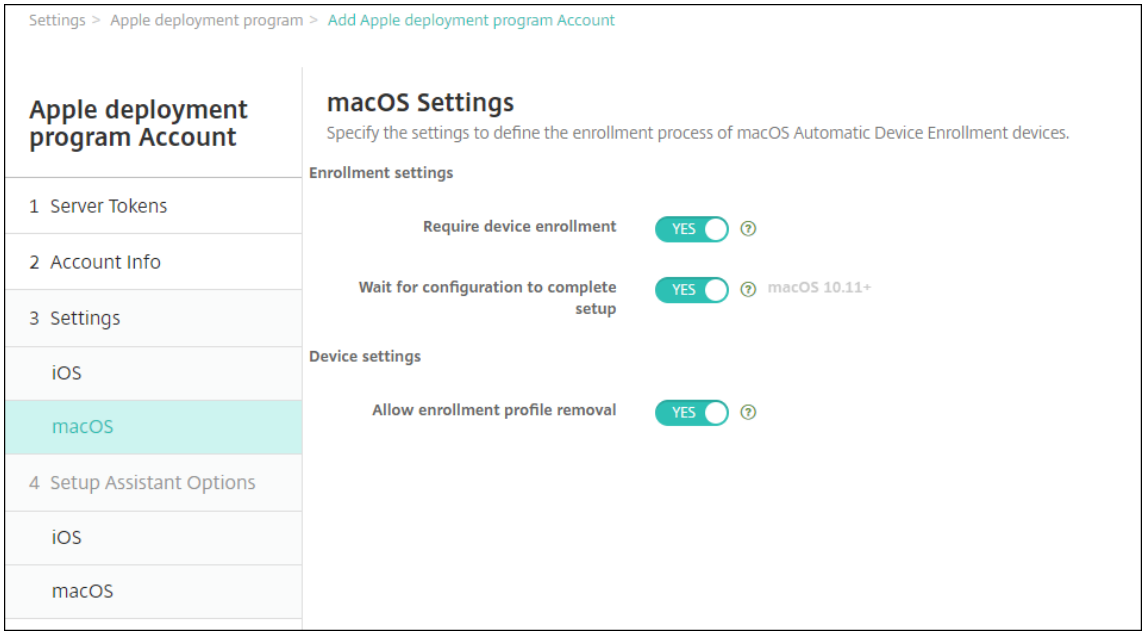
监督身份

如果使用 GroundControl 工具，则可以添加证书以执行以下操作：

- 覆盖配对限制，以避免显示“信任此主机”提示。
- 通过 USB 上报托管设备操作以执行配置文件安装等活动，而无需用户交互。这样做将允许 GroundControl 启用单应用程序模式和设备锁定以进行签出。
- 将备份还原到 ABM 设备。

有关 GroundControl 的详细信息，请参阅 GroundControl Web 站点。

5. 在 **macOS** 设置中，指定以下设置：



注册设置：

- 要求设备注册：是否要求用户注册其设备。默认值为是。
- 等待完成配置设置：如果选择是，macOS 设备将不继续在“设置助理”下操作，直到将 MDM 资源通行码部署到设备。该部署在创建本地帐户之前进行。此设置适用于 macOS 10.11 及更高版本的设备。默认值为否。

设备设置：

- 允许删除注册配置文件：是否允许设备使用能够远程删除的配置文件。默认值为否。

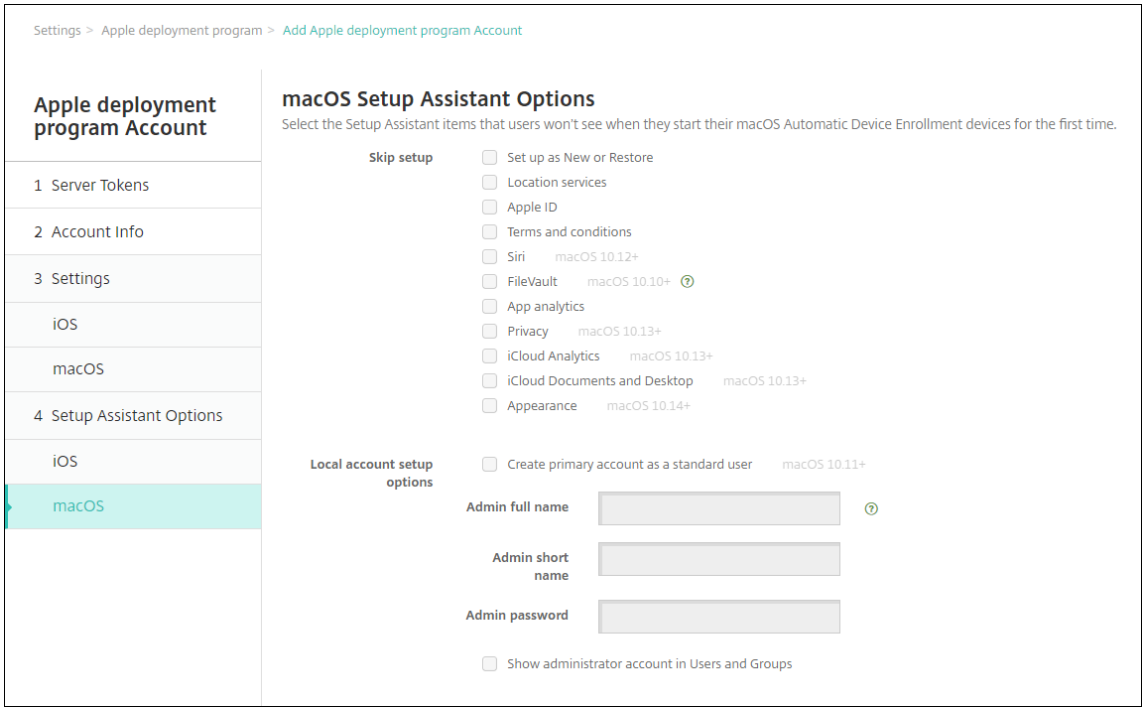
6. 在 **iOS** 设置助手选项中，选择用户在首次启动其设备时 iOS 设置助手跳过的步骤。跳过屏幕时，相关功能将使用默认设置。用户可以在设置完成后配置已跳过的功能，除非您完全限制对这些功能的访问。有关限制对功能的访问的信息，请参阅限制设备策略。所有项目的默认设置为未选中。以下说明解释了选择某项设置时发生的情况。

- 定位服务：阻止用户在设备上设置定位服务。
- **Touch ID**：阻止用户在 iOS 设备上设置 Touch ID 或面容 ID。
- 通行码锁定：阻止用户为设备设置通行码。如果不存在通行码，用户将无法使用 Touch ID 或 Apple Pay。
- 设置为新设备或还原：阻止用户将设备设置为新设备或从 iCloud 或 Apple App Store 备份还原。
- 从 **Android** 移动：阻止用户将数据从 Android 设备传输到 iOS 设备。此选项仅在已选择设置为新对象或还原时可用（即跳过相应步骤）。
- **Apple ID**：阻止用户为设备设置托管 Apple ID 帐户。
- 条款和条件：阻止用户阅读并接受条款和条件以使用设备。
- **Apple Pay**：阻止用户设置 Apple Pay。如果清除此设置，用户必须设置 Touch ID 和 Apple ID。请确保清除这些设置。
- **Siri**：阻止用户配置 Siri。
- 应用程序分析：阻止用户设置是否与 Apple 共享崩溃数据和使用情况统计信息。
- 显示缩放：阻止用户在 iOS 设备上设置显示分辨率（标准或缩放）。
- 原彩：阻止用户设置四通道传感器以动态调整显示器的白平衡。
- 主页按钮：阻止用户设置反馈的主页按钮样式。
- 新功能亮点：阻止用户看到显示 Apple 软件新增功能信息的屏幕。
- 隐私：阻止用户看到数据和隐私窗格。适用于 iOS 11.3 及更高版本。
- 软件更新：阻止用户将 iOS 更新到最新版本。适用于 iOS 12.0 及更高版本。
- 屏幕时间：阻止用户启用屏幕时间。适用于 iOS 12.0 及更高版本。
- **SIM** 设置：阻止用户设置手机网络套餐。适用于 iOS 12.0 及更高版本。
- **iMessage** 和 **FaceTime**：阻止用户启用 iMessage 和 FaceTime。适用于 iOS 12.0 及更高版本。
- 外观：阻止用户选择外观模式。适用于 iOS 13.0 及更高版本。
- 欢迎：阻止用户看到入门屏幕。适用于 iOS 13.0 及更高版本。

- 已完成还原：阻止用户看到还原是否在设置过程中完成。适用于 iOS 14.0 及更高版本。
- 已完成更新：阻止用户看到软件更新是否在设置过程中完成。适用于 iOS 14.0 及更高版本。

ABM 帐户显示在设置 **> Apple** 部署计划上。

7. 在 **macOS** 设置助手选项中，选择用户在首次启动其设备时 macOS 设置助手跳过的步骤。跳过屏幕时，相关功能将使用默认设置。用户可以在设置完成后配置已跳过的功能，除非您完全限制对这些功能的访问。有关限制对功能的访问的信息，请参阅限制设备策略。所有项目的默认设置为未选中。以下说明解释了选择某项设置时发生的情况。



- 设置为新设备或还原：阻止用户将设备设置为新设备或从“时间机器”备份还原或执行系统迁移。
- 定位服务：阻止用户在设备上设置定位服务。适用于 macOS 10.11 及更高版本。
- **Apple ID**：阻止用户为设备设置托管 Apple ID 帐户。
- 条款和条件：阻止用户阅读并接受条款和条件以使用设备。
- **Siri**：阻止用户配置 Siri。适用于 macOS 10.12 及更高版本。
- **FileVault**：使用 FileVault 加密启动磁盘。如果系统具有一个本地用户帐户并且该帐户已登录到 iCloud，XenMobile 将仅应用 FileVault 设置。

  可以使用 macOS FileVault 磁盘加密功能通过加密系统卷的内容 (https://support.apple.com/en-us/HT204837) 来保护系统卷。如果您在未打开 FileVault 功能的新型便携式 Mac 上运行设置助理，系统可能会提示您打开此功能。该提示在新系统以及升级到 OS X 10.10 或 10.11 的系统中显示，但仅当系统具有一个本地管理员帐户并且该帐户已登录到 iCloud 时显示。
- 应用程序分析：阻止用户设置是否与 Apple 共享崩溃数据和使用情况统计信息。

- 隐私：阻止用户看到数据和隐私窗格。适用于 macOS 10.13 及更高版本。
- **iCloud** 分析：阻止用户选择是否向 Apple 发送诊断 iCloud 数据。适用于 macOS 10.13 及更高版本。
- **iCloud** 文档和桌面：阻止用户设置 iCloud 桌面和文档。适用于 macOS 10.13 及更高版本。
- 外观：阻止用户选择外观模式。适用于 macOS 10.14 及更高版本。
- 辅助功能：阻止用户自动聆听旁白。仅在设备连接到以太网时可用。适用于 macOS 11 及更高版本。
- 生物特征识别：阻止用户设置 Touch ID 和面容 ID。适用于 macOS 10.12.4 及更高版本。
- 原彩：阻止用户设置四通道传感器以动态调整显示器的白平衡。适用于 macOS 10.13.6 及更高版本。
- **Apple Pay**：阻止用户设置 Apple Pay。如果清除此设置，用户必须设置 Touch ID 和 Apple ID。确保清除 **Apple ID** 和生物特征识别设置。适用于 macOS 10.12.4 及更高版本。
- 屏幕时间：阻止用户启用屏幕时间。适用于 macOS 10.15 及更高版本。
- 本地帐户设置选项：指定在设备上创建管理员帐户的设置。用户使用此信息登录其 macOS 设备。XenMobile 将使用指定的信息来创建帐户。
  - 创建主帐户作为标准用户： XenMobile 创建具有标准权限的用户，而非授予此用户对设备的管理员权限。由于 macOS 需要管理员帐户，因此 XenMobile 首先创建一个管理员帐户，然后创建一个新的标准帐户并将其设置为主帐户。
  - 管理员全名：键入系统为管理员帐户显示的名称。
  - 管理员短名称：键入设备为主文件夹显示的名称和在 shell 中显示的名称。
  - 管理员密码：键入管理员帐户的安全密码。
  - 显示用户和组中的管理员帐户：如果清除此选项，管理员帐户不会显示在 macOS 设置中的用户和组中。如果您创建主帐户作为标准用户，请启用此设置以隐藏 XenMobile 首先创建的管理员帐户。

启用了订单部署计划的设备

可以直接从 Apple 或启用了部署计划的授权经销商或运营商处订购启用了部署计划的设备。要从 Apple 订购，请在 Apple 部署计划门户中提供您的 Apple 客户 ID。Apple 可以通过您的客户 ID 将您购买的设备与您的 Apple 部署计划帐户关联。

要从经销商或运营商处订购，请联系 Apple 经销商或运营商，确认其是否加入了 Apple 部署计划。购买设备时，请要求提供经销商的 Apple 部署计划 ID。您将您的 Apple 部署计划经销商添加到您的 Apple 部署计划帐户时，Apple 要求提供此信息。添加经销商的 Apple 部署计划 ID 后，您将收到部署计划客户 ID。请向经销商提供部署计划客户 ID，经销商将使用该 ID 将您购买的设备的相关信息提交给 Apple。有关详细信息，请参阅此 Apple 使用设备注册站点。

管理启用了部署程序的设备

订单发货后，您可以将 iOS、iPadOS 和 macOS 设备与 XenMobile Server 相关联。

1. 使用管理员或设备注册管理员帐户登录到 Apple 商务管理。

2. 在边栏中，单击设备。直接从 Apple 购买的设备会自动显示。要将设备从 Apple Configurator 2 分配给 Apple 商务管理，请参阅《Apple 商务管理用户指南》。
3. 在列表中，选择一个设备或设备总数，然后单击编辑设备管理。您有两种选择：
   - 要将设备分配给 MDM 服务器，请在 **Assign to Server**（分配给服务器）下选择您的 XenMobile 服务器的名称。单击继续。

     要将新设备批量分配给 Apple 商务管理，请设置默认 XenMobile Server 以进行部署。有关详细信息，请参阅为批量注册设置默认服务器。
   - 要从 XenMobile Server 取消分配设备，请选择取消分配。

您的 Apple 部署计划设备现在已与选定 XenMobile Server 相关联。

如果使用 iOS、iPadOS 或 macOS 设备提供服务，则需要从 Apple 商务管理中删除该设备。收回提供服务的设备后，必须将该设备重新分配给 XenMobile Server。更换设备时，可以使用订单号将新设备分配给 XenMobile Server。

要查看已分配的设备的历史记录，请执行以下操作：

1. 使用管理员或设备注册管理员帐户登录到 Apple 商务管理。
2. 在边栏中，单击分配历史记录。然后选择一个分配以查看更多信息。
3. 单击下载以下载 CSV 文件，其中包含所有已分配和未分配的设备的序列号。

如果设备已出售、被盗或无法维修，则可以从 Apple 商务管理中删除 iOS、iPadOS 和 macOS 设备。

1. 使用管理员或设备注册管理员帐户登录到 Apple 商务管理。
2. 在边栏中，单击设备并搜索设备。
3. 选择设备，然后单击 **Release Device**（释放设备）。在对话框中，确认您为从程序中删除设备所做的更改。要重新添加 iOS 和 iPadOS 设备，请使用 Apple Configurator 2。您无法使用 Apple Configurator 2 添加 macOS 设备。

注册设备

January 5, 2022

为了安全地远程管理用户设备，请在 XenMobile 中注册这些设备。将 XenMobile 客户端软件安装在用户设备上并验证用户的身份。然后，安装 XenMobile 和用户配置文件。之后，您可以在 XenMobile 控制台中执行设备管理任务。可以应用策略、部署应用程序、将数据推送到设备以及锁定、擦除和定位丢失或被盗的设备。

iOS、Android 和 Windows 10 和 Windows 11 设备支持 Azure Active Directory 注册。有关将 Azure 配置为身份提供程序 (IDP) 的详细信息，请参阅 XenMobile 与作为 IDP 的 Azure Active Directory 的集成。

> 注意：
>
> 必须先申请 APNs 证书才能注册 iOS 设备用户。有关详细信息，请参阅证书和身份验证。

要针对用户和设备更新配置选项，请转至管理 **>** 注册邀请页面。有关详细信息，请参阅本文中的发送注册邀请。

Android 设备

> 注意：
>
> 有关注册 Android Enterprise 设备的信息，请参阅 Android Enterprise。

1. 在 Android 设备上转到 Google Play 应用商店，下载 Citrix Secure Hub 应用程序，然后轻按该应用程序。
2. 系统提示安装应用程序时，单击下一步，然后单击安装。
3. 安装 Secure Hub 后，轻按打开。
4. 输入您的企业凭据，例如 XenMobile Server 名称、用户主体名称 (UPN) 或电子邮件地址。然后，单击下一步。
5. 在 **Activate device administrator**（激活设备管理员）屏幕中，轻按激活。
6. 输入公司密码，然后轻按登录。
7. 系统可能会要求您创建一个 Citrix PIN，具体取决于 XenMobile 的配置方式。可以使用该 PIN 登录 Secure Hub 或其他启用了 XenMobile 的应用程序，例如 Secure Mail 和 Citrix Files。请输入 Citrix PIN 两次。在 **Create Citrix PIN**（创建 Citrix PIN）屏幕上，输入一个 PIN。
8. 重新输入 PIN。此时会打开 Secure Hub。这时即可访问 XenMobile Store 来查看您可以安装在 Android 设备上的应用程序。
9. 如果您在注册后将 XenMobile 配置为自动向设备推送应用程序，系统将提示用户安装这些应用程序。此外，您在 XenMobile 中配置的策略将部署到设备。轻按安装以安装应用程序。

取消注册和重新注册 Android 设备

用户可以从 Secure Hub 内部取消注册。用户通过以下过程取消注册时，设备将仍然在 XenMobile 控制台的设备清单中显示。但您无法在设备上执行操作。无法跟踪设备，也无法监视设备合规性。

1. 轻按以打开 Secure Hub 应用程序。
2. 执行以下操作，具体取决于您拥有的是手机还是平板电脑：

   在手机上：

   - 从屏幕左侧轻扫以打开设置窗格。
   - 依次轻按首选项、帐户和删除帐户。

   在平板电脑上：

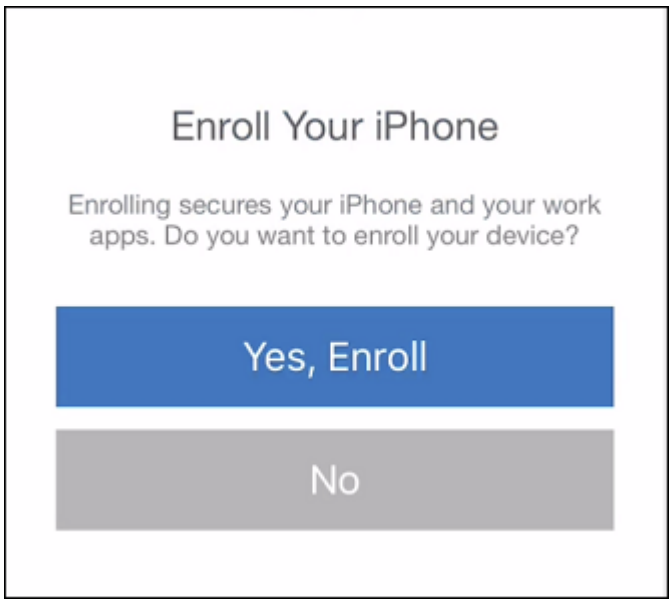
   - 轻按右上角的电子邮件地址旁边的箭头。
   - 依次轻按首选项、帐户和删除帐户。
3. 轻按重新注册。将显示一条消息，提示您确认是否要重新注册自己的设备。
4. 轻按确定。

   您的设备将取消注册。
5. 请按照屏幕上的说明重新注册设备。

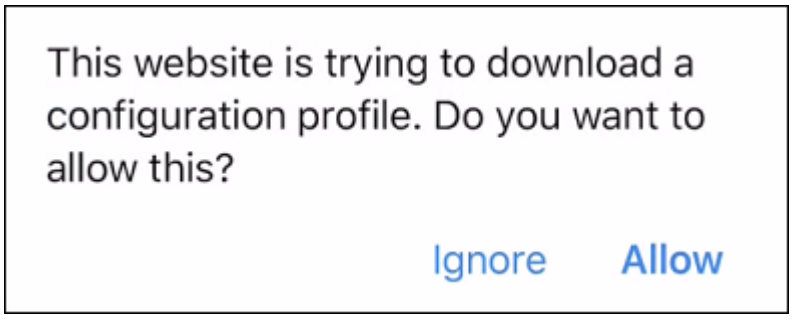
注册 **iOS** 设备

本部分内容介绍用户如何将 iOS 设备（12.2 或更高版本）注册到 XenMobile Server。有关 iOS 注册的详细信息，请打开以下视频：

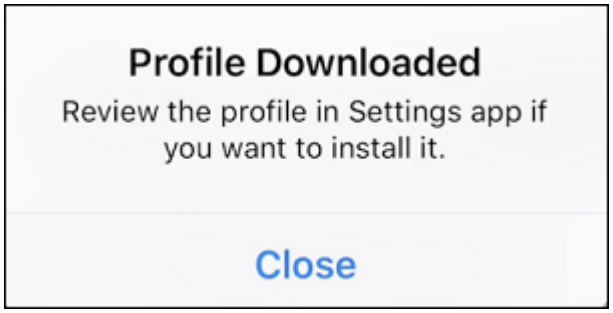
1. 在 iOS 设备上转到 Apple 应用商店，下载 Citrix Secure Hub 应用程序，然后轻按该应用程序。
2. 当系统提示安装应用程序时，轻按下一步，然后轻按安装。
3. 安装 Secure Hub 后，轻按打开。
4. 输入您的企业凭据，例如 XenMobile Server 名称、用户主体名称 (UPN) 或电子邮件地址。然后，单击下一步。
5. 轻按是，注册以注册 iOS 设备。



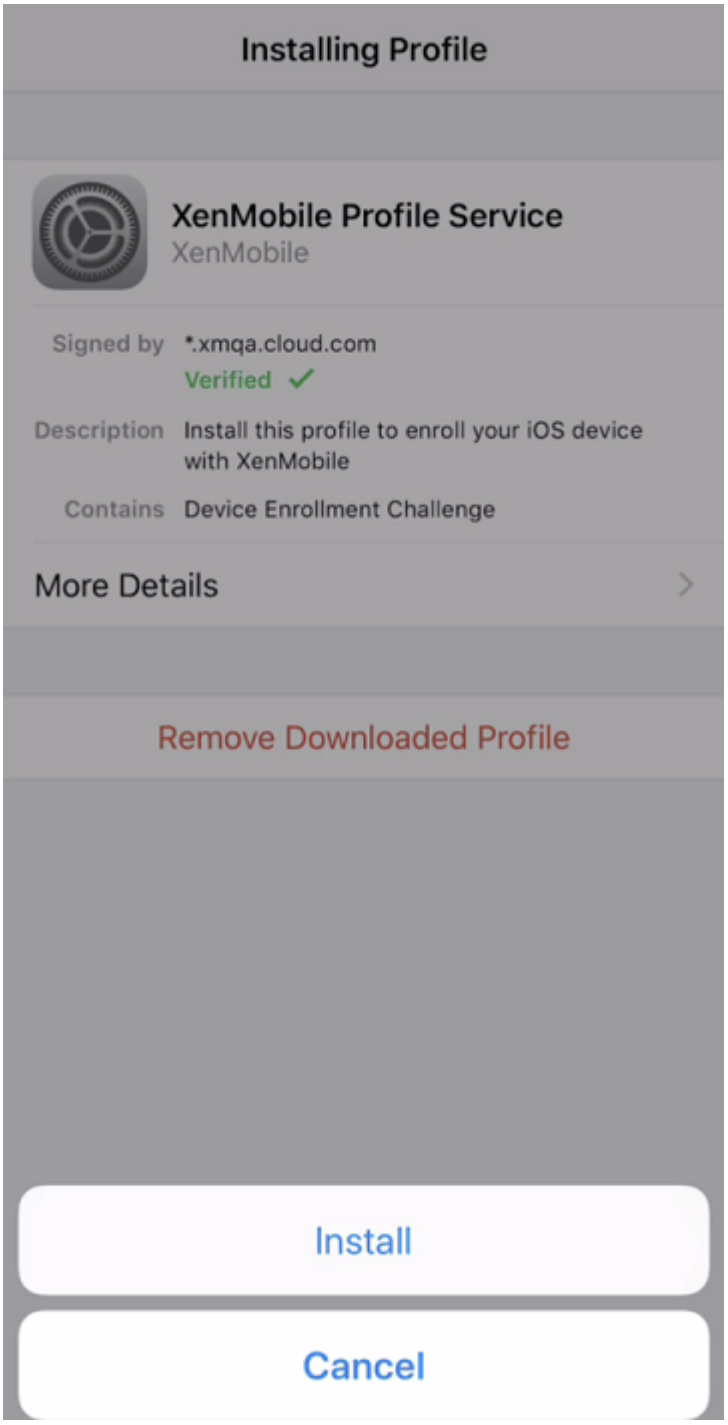
6. 键入凭据后，在出现提示时轻按允许以下载配置文件。



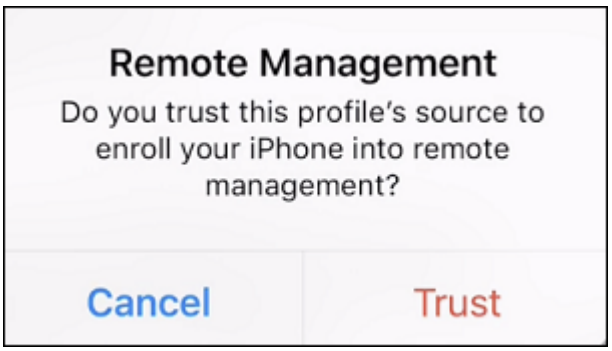
7. 下载配置文件后，轻按关闭。



8. 在设备设置中，安装 iOS 证书并将设备添加到可信列表中。
   - 转到设置 **>** 常规 **>** 配置文件 **> XenMobile** 配置文件服务，然后轻按安装以添加配置文件。



- 在通知窗口中，轻按信任，将您的设备注册到远程管理中。



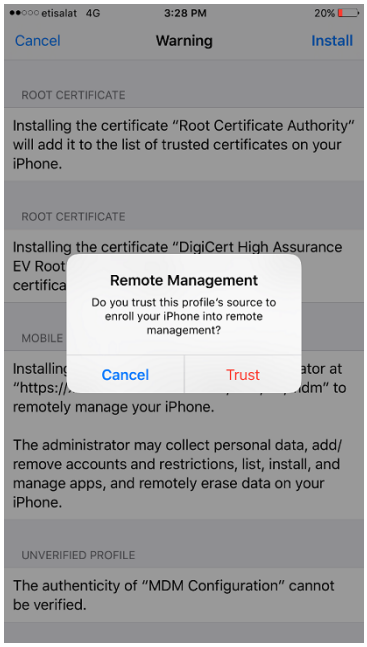
9. 登录到 Secure Hub。如果要注册到 MDM+MAM：验证凭据后，在出现提示时创建并确认您的 Citrix PIN。
10. 工作流程完成后，注册设备。随后即可访问应用商店来查看您安装在 iOS 设备上的应用程序。

iOS 设备

1. 从设备上的 Apple iTunes App Store 下载 Secure Hub 应用程序，然后在设备上安装该应用程序。
2. 在 iOS 设备主屏幕上，轻按 Secure Hub 应用程序。
3. Secure Hub 应用程序打开时，输入技术支持人员提供的服务器地址。

   显示的屏幕可能因这些示例而异，具体取决于 XenMobile 的配置方式。
4. 系统提示时，输入您的用户名和密码或 PIN。单击 **Next**（下一步）。
5. 系统提示注册时，单击是，注册，然后在收到提示时输入您的凭据。
6. 轻按安装以安装 Citrix Profile Service。

7. 轻按信任。



8. 轻按打开，然后输入您的凭据。

macOS 设备

XenMobile 提供两种方法来注册运行 macOS 的设备。这两种方法都使 macOS 用户能够直接从其设备无线注册。

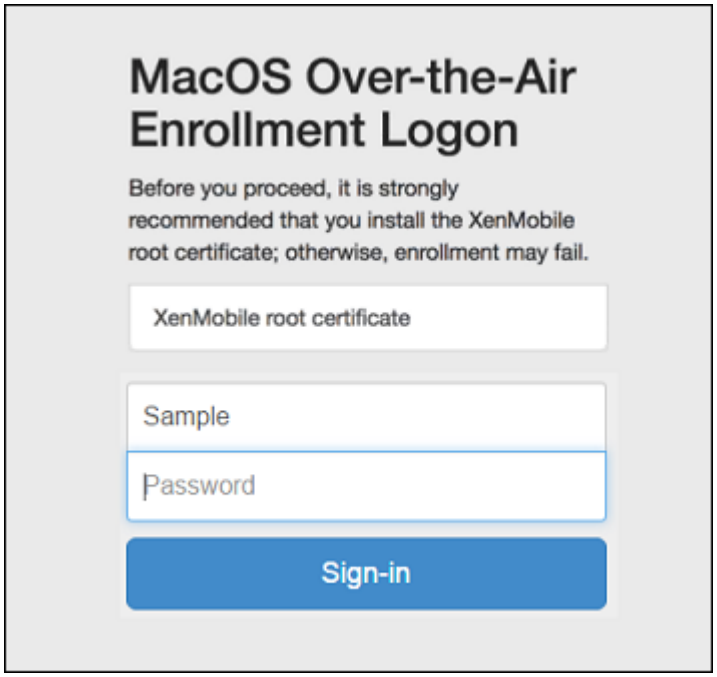
- 向用户发送注册邀请：此注册方法允许您为 macOS 设备设置以下任意注册安全模式：
  - 用户名 + 密码
  - 用户名 + PIN
  - 双重

  用户按照注册邀请中的说明进行操作时，将显示一个填写了用户名的登录屏幕。
- 向用户发送安装链接：此注册方法适用于 macOS 设备，向用户发送一个注册链接，用户可以在 Safari 或 Chrome 浏览器中打开该链接。用户随后通过提供其用户名和密码进行注册。

  要阻止对 macOS 设备使用注册链接，请将服务器属性启用 **macOS OTAE** 设置为 **false**。因此，macOS 用户只能使用注册邀请进行注册。

向用户发送注册邀请

1. （可选）在 XenMobile 控制台中设置 macOS 设备策略。有关设备策略的详细信息，请参阅设备策略。
2. 添加面向 macOS 用户注册的邀请。有关详细信息，请参阅本文中的发送注册邀请。
3. 用户收到邀请并单击链接后，以下屏幕将在 Safari 浏览器中显示。XenMobile 填写用户名。如果您为注册安全模式选择双重，则将显示另一个字段。



4. 用户根据需要安装证书。用户是否会收到安装证书的提示取决于您是否为 macOS 配置了以下证书：公众信任的 SSL 证书和公众信任的数字签名证书。有关证书的详细信息，请参阅证书和身份验证。
5. 用户提供请求的凭据。

   安装 Mac 设备策略。现在即可以像管理移动设备一样使用 XenMobile 管理 Mac。

向用户发送安装链接

1. （可选）在 XenMobile 控制台中设置 macOS 设备策略。有关设备策略的详细信息，请参阅设备策略。
2. 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 XenMobile 的服务器的完全限定域名 (FQDN)。
   - 端口 **8443** 为默认安全端口。如果已配置其他端口，请使用该端口替换 8443。
   - **instanceName**（通常显示为 zdm）为在服务器安装过程中指定的名称。

   有关发送安装链接的详细信息，请参阅发送安装链接。
3. 用户根据需要安装证书。如果您为 iOS 和 macOS 配置了公众信任的 SSL 证书和数字签名证书，用户将看到安装证书的提示。有关证书的详细信息，请参阅证书和身份验证。
4. 用户登录其 Mac 设备。

   安装 Mac 设备策略。现在即可以像管理移动设备一样使用 XenMobile 管理 Mac。

Windows 设备

> 注意：
>
> 本节包括对 Windows Phone 8.1 设备的引用，Microsoft 已将该设备的支持结束日期移至 2017 年 7 月 11 日。XenMobile 仅支持对 Windows Phone 8.1 设备执行 MDM 注册。

Windows 10 和 Windows 11 设备通过 Azure 注册作为 Active Directory 身份验证的联合方式。可以采用下列方法之一将 Windows 10 和 Windows 11 设备连接到 Microsoft Azure AD：

- 首次打开设备电源时在 Azure AD 联接启用过程中在 MDM 中注册。
- 配置设备后，从 “Windows 设置” 页面执行 Azure AD 联接过程中在 MDM 中注册。

可以在 XenMobile 中注册运行以下 Windows 操作系统的设备：

- Windows 10 Phone
- Windows 10
- Windows 11
- Windows Phone 8.1

用户可以直接通过其设备注册。

> 注意：
>
> 对于 Windows 10 RS2 Phone 和 Tablet，重新注册过程中，系统不提示用户提供服务器 URL。要解决此问题，请重新启动设备。或者，在电子邮件地址屏幕上，轻按正在连接到服务中的 X 以转至服务器 URL 页面。这是第三方问题。

必须为用户注册配置自动发现和 Windows 发现服务，才能启用对受支持的 Windows 设备的管理。

必须先在 XenMobile 中配置 Microsoft Azure 服务器，Windows 设备用户才能使用 Azure 进行注册。有关详细信息，请参阅 Microsoft Azure Active Directory 服务器设置。

在配置自行发现的情况下注册 **Windows** 设备

要对 Windows 设备进行管理，Citrix 建议您配置 AutoDiscovery Service 和 Windows 发现服务。有关详细信息，请参阅 XenMobile AutoDiscovery Service。

1. 在设备上，找到并安装所有可用的 Windows 更新。
2. 对于 Windows 10 和 Windows 11：在超级按钮菜单中，轻按设置，然后轻按帐户 **>** 访问工作单位或学校 **>** 连接到工作单位或学校。对于 Windows 8.1 Phone：轻按电脑设置 **>** 网络 **>** 工作区。
3. 对于 Windows 10 和 Windows 11：输入贵公司的电子邮件地址，然后轻按继续。对于 Windows 8.1：轻按 **Turn on device management**（打开设备管理）。要注册为本地用户，请输入带有正确域名的不存在的电子邮件地址（例如 `foo@mydomain.com`）。这将允许您绕过已知 Microsoft 限制，即注册由 Windows 上的内置设备管理执行；在正在连接到服务对话框中，输入与本地用户关联的用户名和密码。设备即会自动发现 XenMobile Server 并开始注册过程。
4. 输入您的密码。使用与某帐户相关的密码，该帐户应该是 XenMobile 中用户组的一部分。
5. 对于 Windows 10 和 Windows 11：在使用条款对话框中，指明您同意托管自己的设备，然后轻按接受。对于 Windows 8.1：在允许 **IT** 管理员提供的应用和服务对话框中，指明您同意托管自己的设备，然后轻按打开。

在不配置自行发现的情况下注册 **Windows** 设备

可以在不配置自动发现的情况下注册 Windows 设备。但是，Citrix 建议您配置自动发现。由于在不配置自动发现的情况下进行注册会导致在连接到所需的 URL 前调用端口 80，因此，这不是用于生产部署的最佳做法。Citrix 建议您仅在测试环境和概念验证部署中使用此过程。

1. 在设备上，找到并安装所有可用的 Windows 更新。
2. 对于 Windows 10 和 Windows 11：在超级按钮菜单中，轻按设置，然后轻按帐户 **>** 访问工作单位或学校 **>** 连接到工作单位或学校。对于 Windows 8.1：轻按电脑设置 **>** 网络 **>** 工作区。
3. 输入企业电子邮件地址。
4. 对于 Windows 10 和 Windows 11：如果未配置自动发现，则将显示一个选项，您可以在此处输入服务器详细信息，如步骤 5 中所述。对于 Windows 8.1：如果自动检测服务器地址设置为开，请轻按以关闭此选项。
5. 对于 Windows 10 和 Windows 11：在输入服务器地址字段中，键入地址：`https://serverfqdn:8443/serverInstance/wpe`。

   如果用于未经身份验证 SSL 连接的端口不是 8443，请使用相应的端口号替换此地址中的 8443。

   对于 Windows 8.1：按以下格式键入服务器地址：`https://serverfqdn:8443/serverInstance/Discovery.svc`。

   如果用于未经身份验证 SSL 连接的端口不是 8443，请使用相应的端口号替换此地址中的 8443。
6. 键入密码。

7. 对于 Windows 10 和 Windows 11：在使用条款对话框中，指明您同意托管自己的设备，然后轻按接受。对于 Windows 8.1：在允许 **IT** 管理员提供的应用和服务对话框中，指明您同意托管自己的设备，然后轻按打开。

注册 **Windows Phone** 设备

要在 XenMobile 中注册 Windows Phone 设备，用户需要使用其 Active Directory 或内部网络电子邮件地址和密码。如果未设置自动发现，用户还需要 XenMobile Server 的服务器 Web 地址。然后，他们需要按照此过程在设备上完成注册。

> 注意：
>
> 如果您计划通过 Windows Phone 公司应用商店来部署应用程序，则在用户注册前，请确保您已配置企业中心策略（具有签名的 Secure Hub、适用于您支持的每个平台的 Windows Phone 应用程序）。

1. 在 Windows Phone 的主屏幕上，轻按设置图标。
   - 对于 Windows 10 和 Windows 11：轻按帐户 **>** 访问工作单位或学校 **>** 连接到工作单位或学校，或轻按帐户 **>** 工作单位访问权限 **>** 注册移动设备管理，具体取决于您使用的版本。
   - 对于 Windows 8.1：轻按电脑设置 **>** 网络 **>** 工作区，然后轻按添加帐户。
2. 在下一屏幕上，输入电子邮件地址和密码，然后轻按登录。

   如果为域配置了自动发现，随后几个步骤中所需的信息将会自动填充。继续执行步骤 8。

   如果没有为域配置自动发现，请继续执行下一步。要注册为本地用户，请输入带有正确域名的不存在的电子邮件地址（例如 `foo@mydomain.com`）。这将允许您绕过已知 Microsoft 限制；在正在连接到服务对话框中，输入与本地用户关联的用户名和密码。
3. 在下一屏幕上，输入 XenMobile Server 的 Web 地址，例如：`https://<xenmobile_server>:<portnumber>/<instancename>/wpe`。例如，`https://mycompany.mdm.com:8443/zdm/wpe`。

   > 注意：
   >
   > 必须将端口号调整为适用于您的实现。该端口必须与您用于 iOS 注册的端口相同。
4. 如果通过用户名和域进行身份验证，请输入用户名和域，然后轻按登录。
5. 在 Windows Phone 8.1 上，添加帐户时，可以选择 **Install company app**（安装公司应用程序）。如果管理员已配置 Company App Store，请选中此选项，然后轻按完成。如果取消选中此选项，您需要重新注册设备才能接收 Company App Store。
6. 在 Windows Phone 8.1 上，在已添加帐户屏幕上，轻按完成。
7. 要强制连接到某一服务器，请轻按“刷新”图标。如果设备没有手动连接到服务器，XenMobile 会尝试重新连接。XenMobile 会每 3 分钟连续 5 次连接设备，然后间隔改为 2 小时。您可以在服务器属性中的 **Windows WNS** 检测信号间隔中修改此连接率。注册完成后，Secure Hub 将在后台注册。安装完成时不会提示。在所有应用程序屏幕中，轻按 Secure Hub。

发送注册邀请

在 XenMobile 控制台中，可以向使用 iOS、macOS、Android Enterprise 和旧 Android 设备的用户发送注册邀请。此外，还可以向使用 iOS、Android Enterprise 或旧 Android 设备的用户发送安装链接。

注册邀请的发送方式如下所示：

- 如果注册邀请面向本地用户或 Active Directory 用户：用户将通过您指定的电话号码和运营商收到来自 SMS 的邀请。
- 如果注册邀请面向组：用户将收到来自 SMS 的邀请。如果 Active Directory 用户在 Active Directory 中具有电子邮件地址和移动电话号码，则会收到该邀请。本地用户将通过在用户属性中指定的电子邮件和电话号码收到邀请。

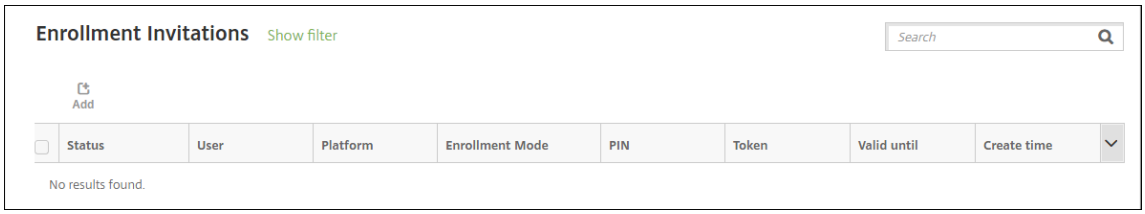
用户注册后，其设备在管理 **>** 设备上将显示为托管设备。邀请 URL 的状态显示为已兑换。

必备条件

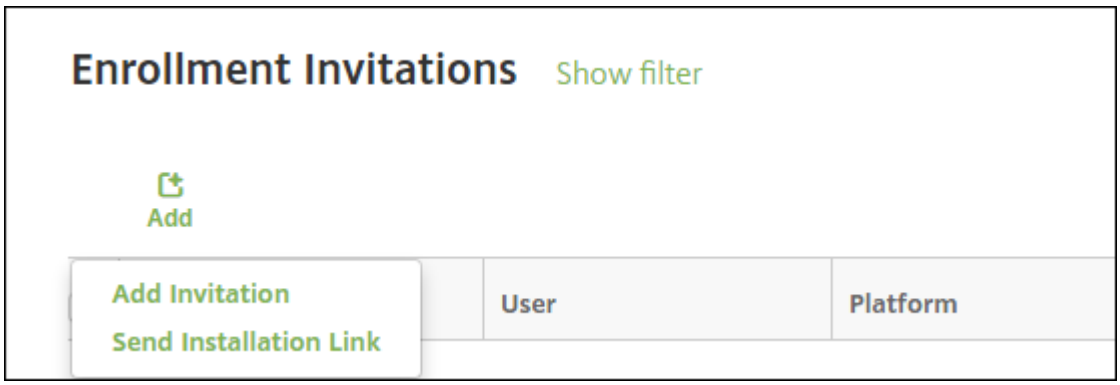
- 在企业 (XME) 或 MDM 模式下配置的 XenMobile Server
- 已配置 LDAP
- 如果使用本地组和本地用户：
  - 一个或多个本地组。
  - 分配给本地组的本地用户。
  - 交付组与本地组相关联。
- 如果使用 Active Directory：
  - 交付组与 Active Directory 组相关联。

创建注册邀请

1. 在 XenMobile 控制台中，单击管理 **>** 注册邀请。此时将显示注册邀请页面。



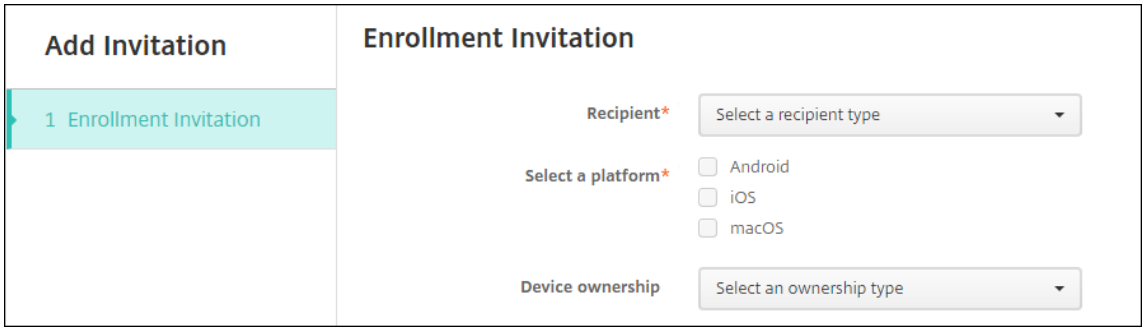
2. 单击添加。此时将显示一个注册选项菜单。



- 要向用户或组发送注册邀请，请单击添加邀请。
- 要通过 SMTP 或 SMS 向收件人列表发送注册安装链接，请单击发送安装链接。

如何发送注册邀请和安装链接将在这些步骤之后进行介绍。

3. 单击添加邀请。将显示注册邀请屏幕。



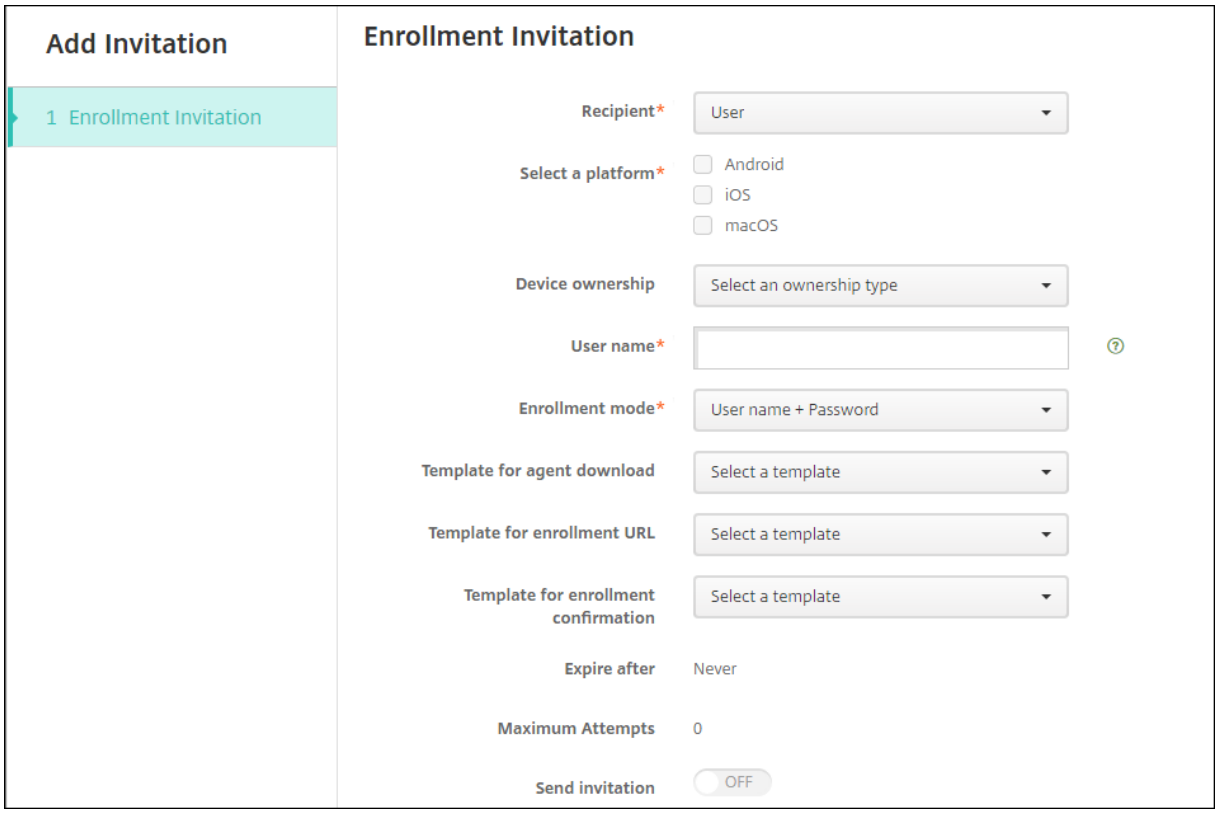
4. 配置以下设置：

   - 收件人：选择组或用户。
   - 选择平台：如果收件人为组，则默认选择所有平台。可以更改所选平台。如果收件人为用户，则不选择任何平台。选择平台。

     要为 Android Enterprise 设备创建注册邀请，请选择 **Android > Android Enterprise**。
   - 设备所有权：选择公司或员工。

   此时将显示用户或组的设置，如以下各节中所述。

向用户发送注册邀请



1. 配置以下用户设置：

   - 用户名：键入用户名。用户必须作为本地用户或 Active Directory 中的用户存在于 XenMobile Server 中。如果用户是本地用户，请务必设置用户的电子邮件属性，以便能够向该用户发送通知。如果用户在 Active Directory 中，请务必配置 LDAP。
   - 设备信息：如果您选择了多个平台，或者仅选择了 macOS，此设置将不显示。选择序列号、**UDID** 或 **IMEI**。选择某个选项后，将显示一个字段，您可以在此处键入设备的相应值。
   - 电话号码：如果您选择了多个平台，或者仅选择了 macOS，此设置将不显示。（可选）键入用户的电话号码。
   - 运营商：如果您选择了多个平台，或者仅选择了 macOS，此设置将不显示。选择要与用户的电话号码关联的运营商。
   - 注册模式：为用户选择注册安全模式。默认值为用户名 **+** 密码。下面某些选项不对所有平台可用：
     - 用户名 + 密码
     - 高安全性
     - 邀请 URL
     - 邀请 URL + PIN
     - 邀请 URL + 密码
     - 双重
     - 用户名 + PIN

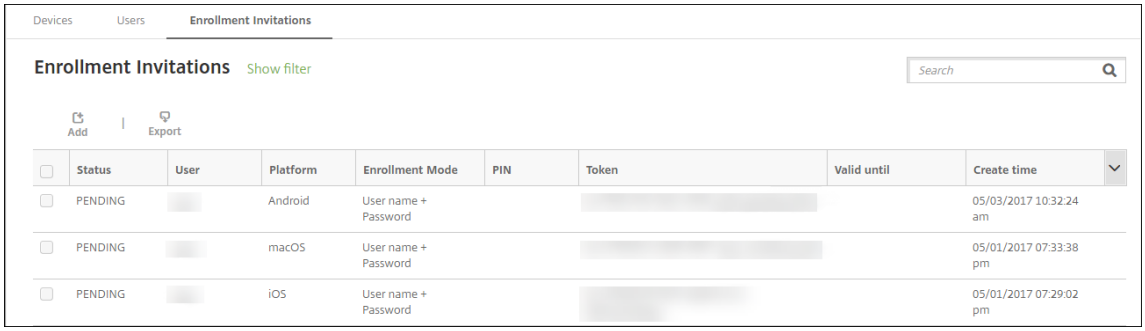
要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。对于使用用户名 **+** 密码、双重或用户名 **+ PIN** 注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

用于注册的 PIN 又称为一次性 PIN。此类 PIN 仅在用户注册时有效。

> 注意：
>
> 选择包含 PIN 的任意注册安全模式时，会显示注册 **PIN** 模板字段，在此可单击注册 **PIN**。

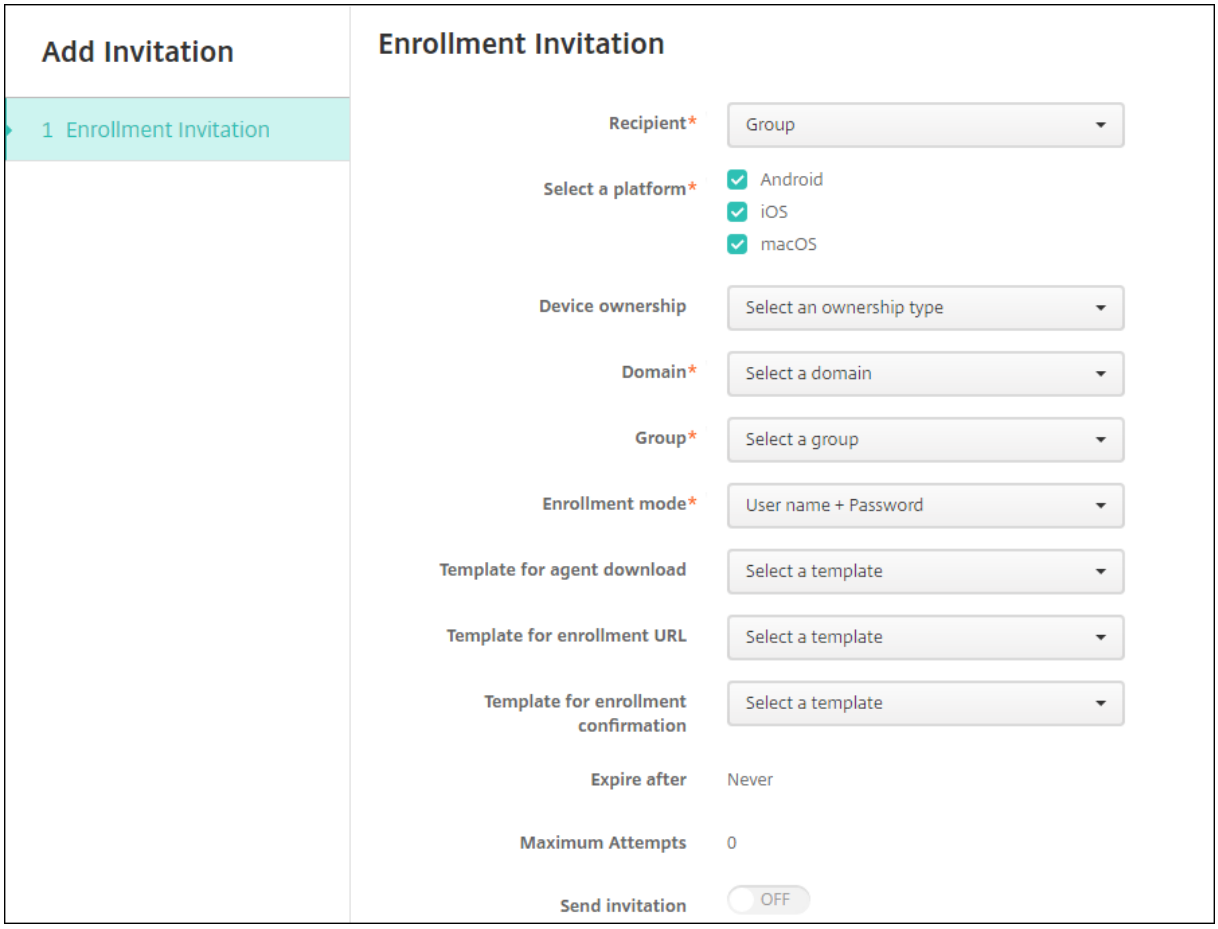
- 代理下载模板：选择名为下载链接的下载链接模板。该模板适用于受支持的所有平台。
- 注册 **URL** 模板：选择注册邀请。
- 注册确认模板：选择注册确认。
- 此时间后过期：此字段在配置注册模式时设置，用于指出注册的过期时间。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- 最大尝试次数：此字段将在配置注册模式时设置，用于指出注册过程发生的最大次数。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- 发送邀请：选择开将立即发送邀请。选择关将向注册邀请页面上的表格中添加邀请，但不发送。

2. 如果已启用发送邀请，请单击保存并发送。否则，请单击保存。邀请将显示在注册邀请页面上的表格中。



向组发送注册邀请

下图中显示了用于配置向组发送的注册邀请的设置。



1. 配置以下设置：

   - 域：选择要接收邀请的组的域。
   - 组：选择要接收邀请的组。
   - 注册模式：选择希望组中的用户采用的注册方式。默认值为用户名 **+** 密码。下面某些选项不对所有平台可用：
     - 用户名 + 密码
     - 高安全性
     - 邀请 URL
     - 邀请 URL + PIN
     - 邀请 URL + 密码
     - 双重
     - 用户名 + PIN

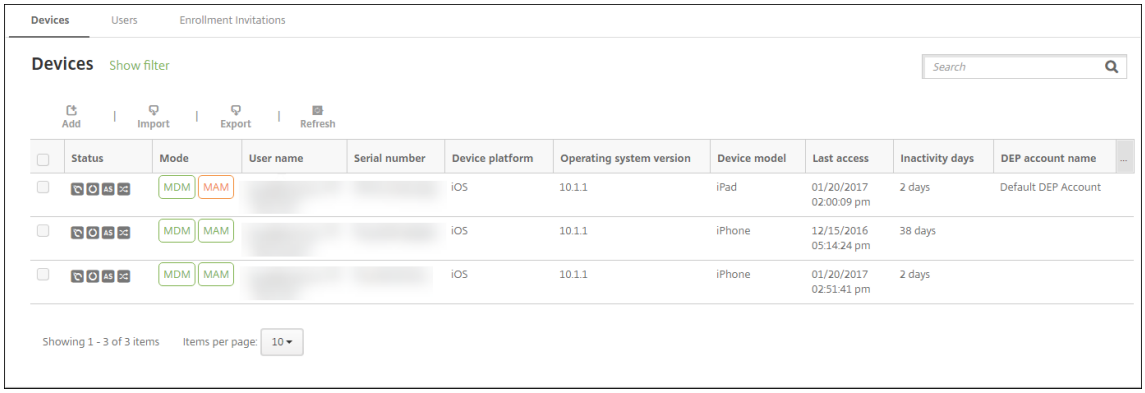
   要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。对于使用用户名 **+** 密码、双重或用户名 **+ PIN** 注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

   仅显示对每个选定的平台有效的注册安全模式。

> 注意：
>
> 选择包含 PIN 的任意注册安全模式时，会显示注册 **PIN** 模板字段，在此可单击注册 **PIN**。

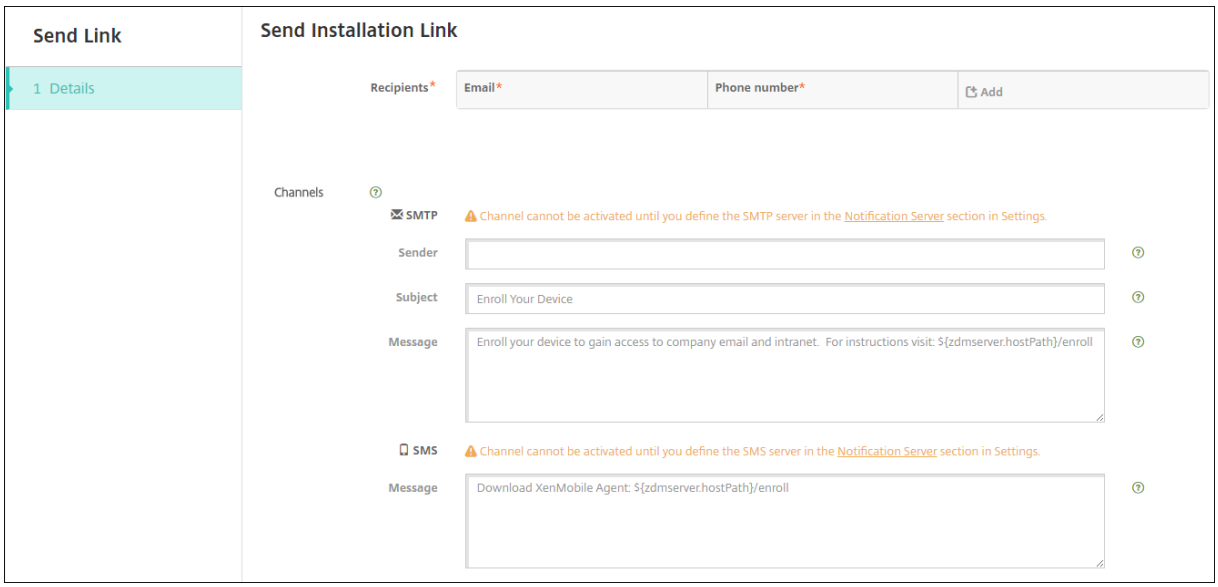
- 代理下载模板：选择名为下载链接的下载链接模板。该模板适用于受支持的所有平台。
- 注册 **URL** 模板：选择注册邀请。
- 注册确认模板：选择注册确认。
- 此时间后过期：此字段在配置注册模式时设置，用于指出注册的过期时间。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- 最大尝试次数：此字段将在配置“注册模式”时设置，用于指出注册过程发生的最大次数。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- 发送邀请：选择开将立即发送邀请。选择关将向注册邀请页面上的表格中添加邀请，但不发送。

2. 如果已启用发送邀请，请单击保存并发送。否则，请单击保存。邀请将显示在注册邀请页面上的表格中。



发送安装链接

您必须通过设置页面在通知服务器上配置通道（SMTP 或 SMS），才能发送注册安装链接。有关详细信息，请参阅 [通知] (/zh-cn/xenmobile/server/users/notifications.html



1. 配置这些设置，然后单击保存。

   - 收件人：对于要添加的每个收件人，单击添加，然后执行以下操作：
     - 电子邮件：键入收件人的电子邮件地址。此字段为必填字段。
     - 电话号码：键入收件人的电话号码。此字段为必填字段。

     > 注意：
     >
     > 要删除现有收件人，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾桶图标。此时将显示确认对话框。单击删除以删除列表，或单击取消以保留列表。
     >
     > 要编辑现有收件人，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。更新列表，然后单击保存以保存更改后的列表，或单击取消以保留列表不变。

   - 通道：选择用于发送注册安装链接的通道。可以通过 **SMTP** 或 **SMS** 发送通知。在通知服务器的设置页面上配置服务器设置后，才能激活这些通道。有关详细信息，请参阅通知。
   - **SMTP**：配置以下可选设置。如果不在这些字段中键入任何内容，将使用为所选平台配置的通知模板中指定的默认值：
     - 发件人：键入可选发件人。
     - 主题：键入消息的可选主题。例如，“注册您的设备”。
     - 消息：键入要发送给收件人的可选消息。例如，“注册您的设备以获取组织应用程序和电子邮件的访问权限。”
   - **SMS**：配置以下设置。如果不在此字段中键入任何内容，将使用为所选平台配置的通知模板中指定的默认值：
     - 消息：键入要发送给收件人的消息。对于基于 SMS 的通知，这是必填字段。

> 注意：在北美，超过 160 个字符的 SMS 消息将通过多条消息发送。

2. 单击发送。

> 注意：
>
> 如果您的环境使用 sAMAccountName：在用户收到邀请并单击链接后，必须编辑用户名才能完成身份验证。用户名以 sAMAccountName@domainname.com 格式显示。用户必须删除 @domain-name.com 部分。

注册安全模式（按平台）

下表显示了可用于注册用户设备的安全模式。在该表中，是表示哪些设备平台支持使用不同注册配置文件的特定注册和管理模式。

MDM 注册安全模式	Citrix Gate-way 上的 MAM 注册安全模式	管理模式	支持不同的注册配置文件	Android（旧版）	Android Enter-prise	iOS（用户注册模式）	iOS	macOS	Windows
Azure AD 和 Okta 可通过 Citrix Cloud 作为身份提供程序	客户端证书	MDM+MA 或 MDM	是	是	是	是	是	否	否

MDM 注册安全模式	Citrix Gateway 上的 MAM 注册安全模式	管理模式	支持不同的注册配置文件	Android（旧版）	Android Enterprise	iOS（用户注册模式）	iOS	macOS	Windows
用户名 + 密码	LDAP、LDAP + 客户端证书和仅客户端证书	MDM+MAM、MDM 或 MAM（仅 MAM 模式在 Citrix Gateway 上不支持客户端证书）	是	是	是	是	是	是	是
邀请 URL	客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	否	否
邀请 URL + PIN	客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	否	否
邀请 URL + 密码	LDAP、LDAP + 客户端证书和仅客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	否	否
双重身份验证（用户名 + 密码 + PIN）	LDAP、LDAP + 客户端证书和仅客户端证书	MDM+MAM 或 MDM	是	是	是	否	是	是	否

MDM 注册安全模式	Citrix Gateway 上的 MAM 注册安全模式	管理模式	支持不同的注册配置文件	Android（旧版）	Android Enterprise	iOS（用户注册模式）	iOS	macOS	Windows
用户名 + PIN	客户端证书	MDM+M/ 或 MDM	是	是	是	否	是	是	否

下面介绍了注册安全模式在 iOS、Android 和 Android Enterprise 设备上的行为方式：

- 用户名 **+** 密码（默认设置）
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Secure Hub 将打开。然后，用户会键入用户名和密码以在 XenMobile 中注册设备。
- 邀请 **URL**
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Secure Hub 将打开。此时将显示 XenMobile 服务器名称和是，注册按钮。用户可以轻按是，注册以在 XenMobile 中注册设备。
- 邀请 **URL + PIN**
  - 向用户发送以下电子邮件：
    - 包含注册 URL 的电子邮件，该邮件允许用户通过 Secure Hub 在 XenMobile 中注册设备。
    - 包含一次性 PIN（用户在注册设备时必须键入该 PIN）以及用户的 Active Directory（或本地）密码的电子邮件。
  - 在此模式下，用户只能通过使用通知中的注册 URL 进行注册。如果用户丢失了通知邀请，用户将无法注册。但是，您可以发送其他邀请。
- 邀请 **URL +** 密码
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Secure Hub 将打开。此时将显示 XenMobile 服务器名称，以及允许用户键入密码的字段。
- 双重
  - 向用户发送包含注册 URL 和一次性 PIN 码的单个通知。当用户单击 URL 时，Secure Hub 将打开。此时将显示 XenMobile 服务器名称，以及允许用户键入密码和 PIN 码的两个字段。
- 用户名 **+ PIN**
  - 向用户发送以下电子邮件：
    - 包含注册 URL 的电子邮件，该邮件允许用户下载并安装 Secure Hub。Secure Hub 打开后，系统将提示用户键入用户名和密码，以便在 XenMobile 中注册设备。
    - 包含一次性 PIN（用户在注册设备时必须键入该 PIN）以及用户的 Active Directory（或本地）密码的电子邮件。
  - 如果用户丢失了通知邀请，用户将无法注册。但是，您可以发送其他邀请。

下面介绍了注册安全模式在 macOS 设备上的行为方式：

- 用户名 **+** 密码
  - 向用户发送包含注册 URL 的单个通知。当用户单击 URL 时，Safari 浏览器将打开。此时将显示一个登录页面，提示用户键入用户名和密码，以便在 XenMobile 中注册设备。
- 双重
  - 向用户发送包含注册 URL 和一次性 PIN 码的单个通知。当用户单击 URL 时，Safari 浏览器将打开。此时将显示一个登录页面，其中显示两个允许用户键入密码和 PIN 码的字段。
- 用户名 **+ PIN**
  - 向用户发送以下电子邮件：
    - 包含注册 URL 的电子邮件。当用户单击 URL 时，Safari 浏览器将打开。此时将显示一个登录页面，提示用户键入用户名和密码，以便在 XenMobile 中注册设备。
    - 包含一次性 PIN（用户在注册设备时必须键入该 PIN）以及用户的 Active Directory（或本地）密码的电子邮件。
  - 如果用户丢失了通知邀请，用户将无法注册。但是，您可以发送其他邀请。

您不能向 Windows 设备发送注册邀请。Windows 用户直接通过其设备注册。

Firebase Cloud Messaging

January 5, 2022

> 注意：
>
> Firebase Cloud Messaging (FCM) 的前称为 Google Cloud Messaging (GCM)。某些 XenMobile 控制台标签和消息会使用术语 GCM。

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

完成本文中的配置步骤且某个设备签入后，该设备将注册到 XenMobile Server 中的 FCM 服务。该连接允许通过使用 FCM 在 XenMobile 服务与您的设备之间实现近乎实时的通信。FCM 注册适用于新设备注册和以前注册的设备。

当 XenMobile 需要启动与设备的连接时，它将连接到 FCM 服务。然后，FCM 服务将通知该设备进行连接。这种类型的连接与 Apple 用于其推送通知服务的连接类似。

必备条件

- 最新版本 Secure Hub 客户端
- Google 开发人员帐户凭据
- 在启用了 FCM 的 Android 设备上安装的 Google Play 服务

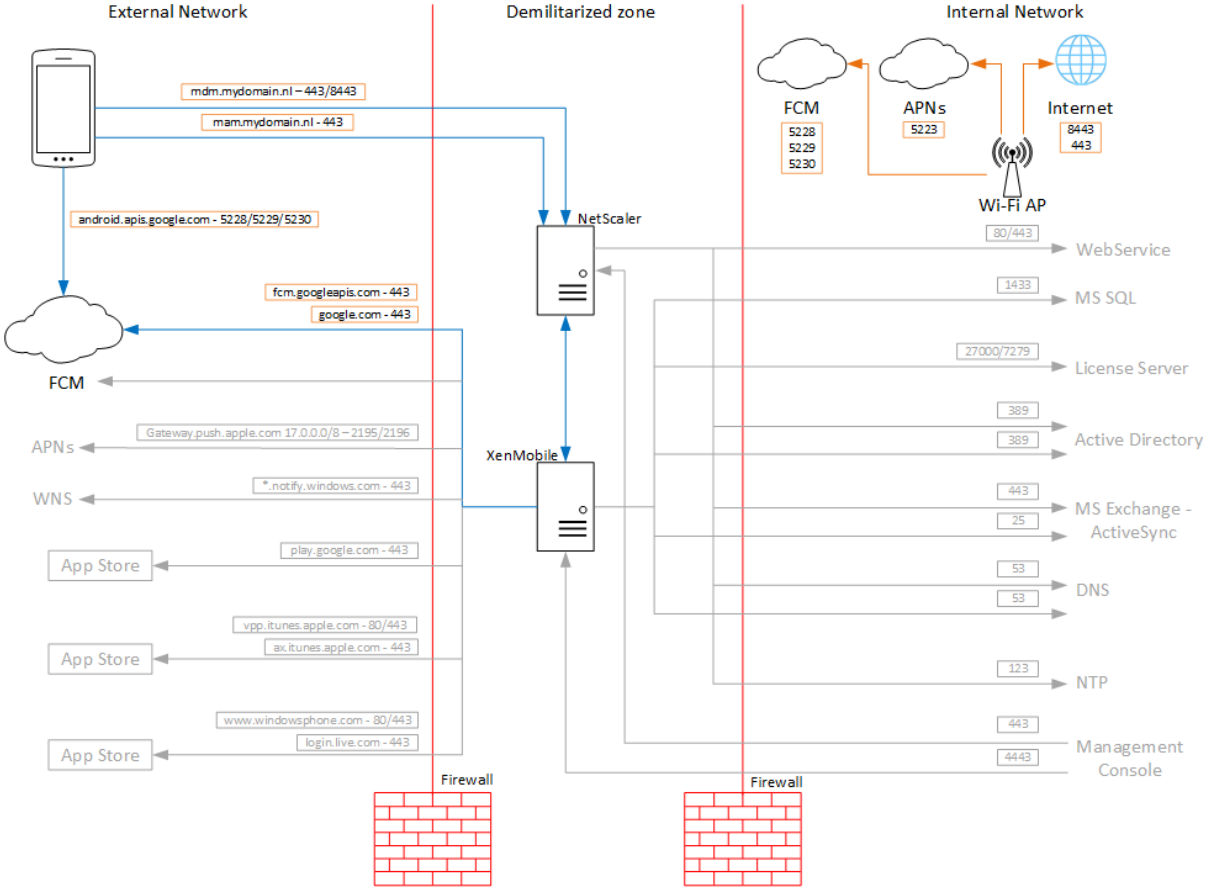
防火墙端口

- 在 XenMobile 上打开指向 `fcm.googleapis.com` 和 `Google.com` 的端口 443。
- 在端口 5228、5229 和 5230 上为设备 Wi-Fi 打开传出 Internet 通信。
- 要允许传出连接，FCM 建议允许使用端口 5228 到 5230，且无任何 IP 限制。但是，如果您需要 IP 限制，FCM 建议允许使用 IPv4 和 IPv6 块中的所有 IP 地址。这些块将在 Google ASN 15169 中列出。每月更新该列表。

有关详细信息，请参阅端口要求。

体系结构

此图显示了外部和内部网络中 FCM 的通信流。

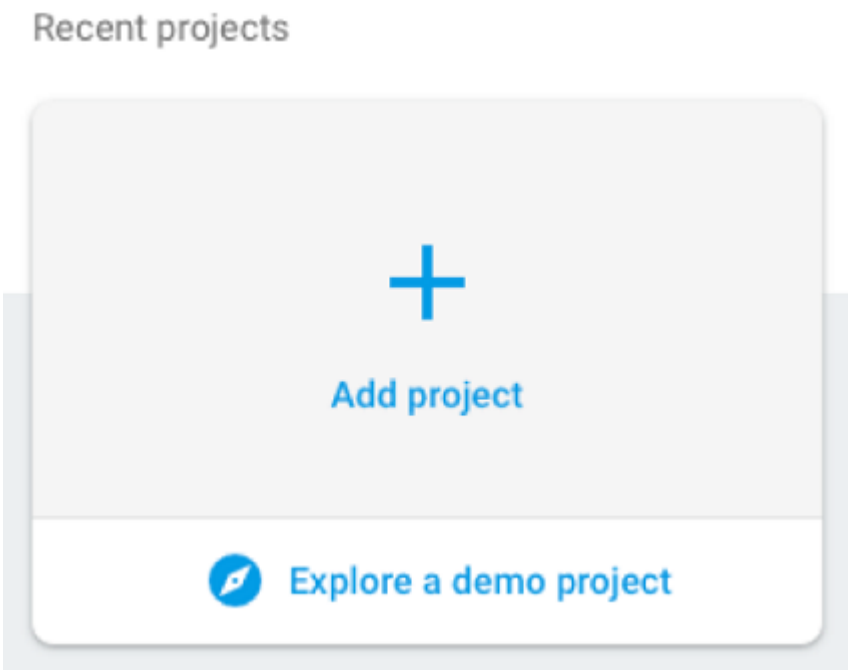


为 **FCM** 配置 **Google** 帐户

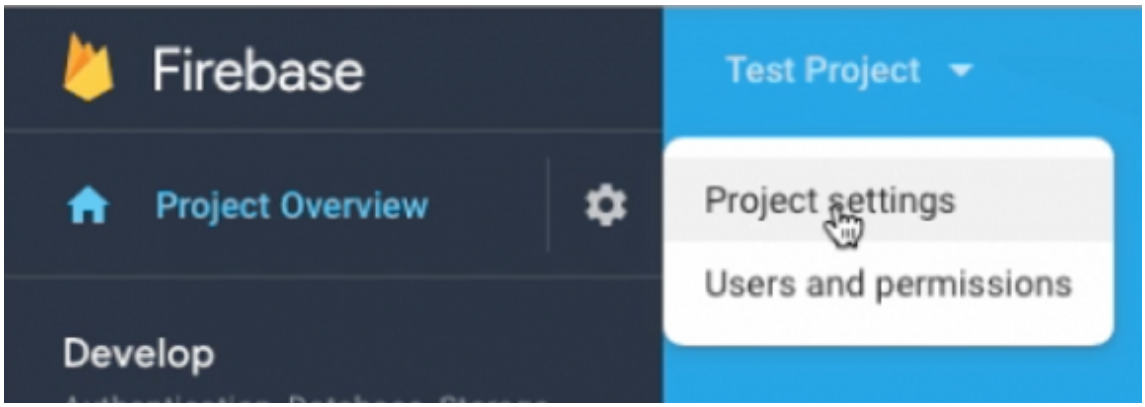
1. 使用您的 Google 开发人员帐户凭据登录以下 URL：

   https://console.firebase.google.com/

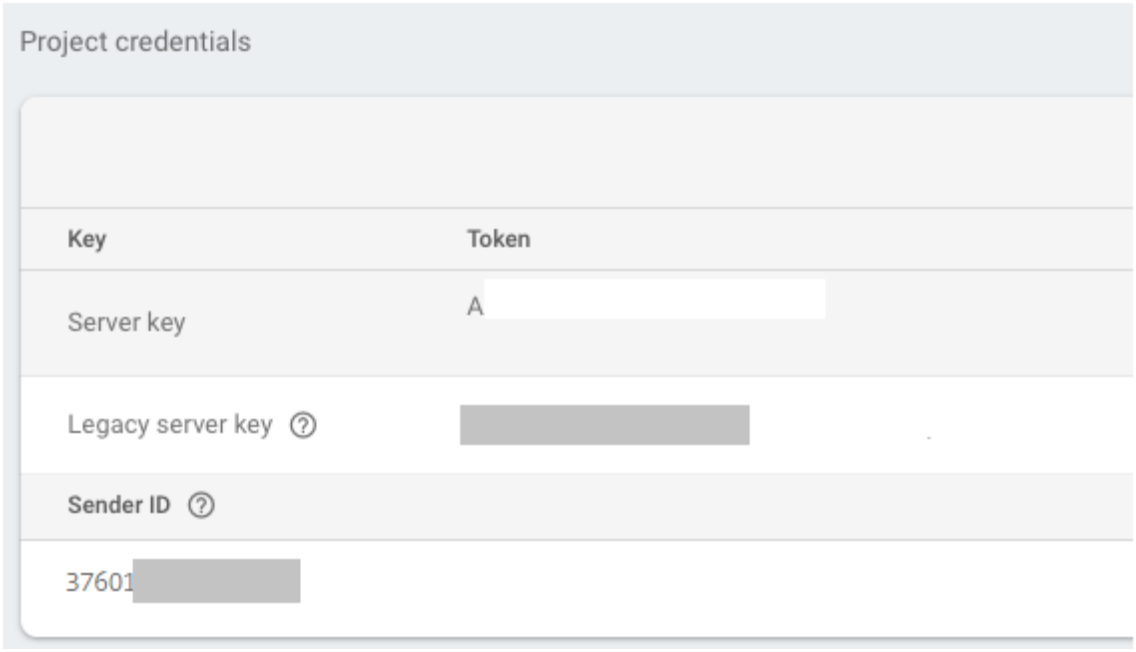
2. 单击添加项目。



3. 创建项目后，单击项目设置。



4. 单击 **Cloud Messaging** 选项卡。复制服务器密钥和发件人 **ID** 值。在下一个过程中，可以将这些值粘贴到 XenMobile 控制台中。截至 2016 年 10 月，必须在 Firebase 控制台中创建服务器密钥。

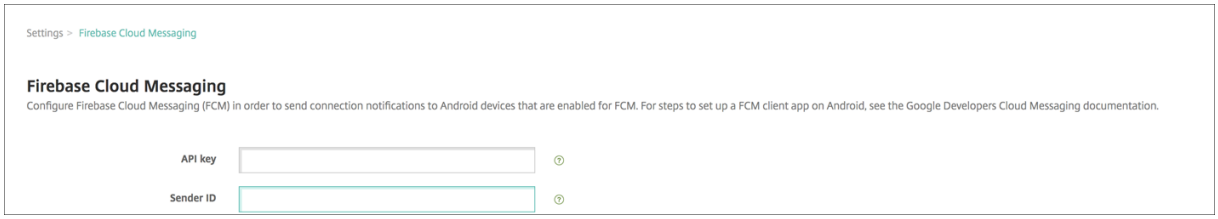


有关在 Android 上设置 FCM 客户端应用程序的步骤，请参阅此 Google Developers Cloud Messaging 文章：https://firebase.google.com/docs/cloud-messaging/android/client。

为 **FCM** 配置 **XenMobile**

在 XenMobile 控制台中，转至设置 **> Firebase Cloud Messaging**。

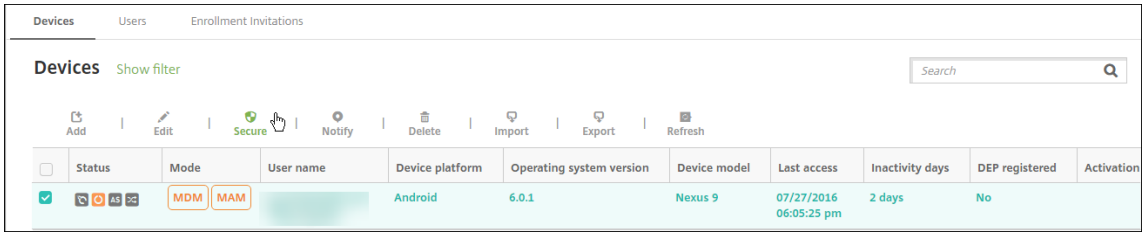
- 编辑 **API** 密钥，并键入在 Firebase Cloud Messaging 配置的最后一步中复制的 Firebase Cloud Messaging 服务器密钥。
- 编辑发件人 **ID**，并键入在之前的过程中复制的发件人 **ID** 值。



完成设置后，可以删除计划设备策略，也可以将该策略更改为降低连接频率。

测试您的配置

1. 注册 Android 设备。
2. 保持设备在一段时间内处于空闲状态，以使其与 XenMobile 断开连接。
3. 登录 XenMobile 控制台，单击管理，选择 Android 设备，然后单击安全。



4. 在设备操作下方，单击选择性擦除。

成功配置后，即可在设备上执行选择性擦除。

与 **Apple** 教育功能相集成

January 5, 2022

在使用 Apple 教育功能的环境中，可以使用 XenMobile 作为您的移动设备管理 (MDM) 解决方案。XenMobile 支持包括 Apple 校园教务管理 (ASM) 和面向 iPad 的课堂应用程序。XenMobile 的教育配置设备策略配置教师和学生的设备以供 Apple 教育功能使用。

您负责向教师和学生提供预配置并且受监督的 iPad。该配置包括 XenMobile 中的 ASM 注册、配置了新密码的管理式 Apple ID 帐户以及必需的批量购买应用程序和 iBooks。

下面是 XenMobile 对 Apple 教育功能的支持的几点重要事项。

Apple 校园教务管理

ASM 是一项服务，通过该服务，您可以设置、部署和管理教育机构使用的 iOS (iPadOS) 设备和 macOS 便携式计算机。ASM 包括一个基于 Web 的门户，在该门户中，IT 管理员可以执行以下操作：

- 向不同的 MDM 服务器分配 Apple 部署计划设备。

- 购买适用于各种应用程序和 iBooks 的批量购买许可证
- 批量创建管理式 **Apple ID**。这些自定义的 Apple ID 提供对各项 Apple 服务的访问权限，例如在 iCloud Drive 中存储文档以及在 Apple App Store 课程中注册。

可以向 XenMobile 中添加多个 ASM 帐户。例如，借助此功能，您可以按教育单位或部门使用不同的注册设置和设置助手选项。然后将 ASM 帐户与不同的设备策略相关联。

向 XenMobile 控制台中添加 ASM 帐户后，XenMobile 将检索班级和名单信息。设备设置过程中，XenMobile 将执行以下操作：

- 注册设备。
- 安装您为部署配置的资源，例如设备策略（教育配置、主屏幕布局等）。
- 此外，还将安装通过批量购买购买的应用程序和 iBooks。

您随后向教师和学生提供预配置的设备。如果设备丢失或被盗，可以使用 MDM 丢失模式功能锁定和定位设备。

适用于 **iPad** 的 **“**课堂**”** 应用程序

通过适用于 iPad 的 “课堂” 应用程序，教师可以连接到学生的设备以及对其进行管理。可以查看设备屏幕、在 iPad 上打开应用程序以及共享和打开 Web 链接。

“课堂” 应用程序在 App Store 中免费提供。您需要将该应用程序上载到 XenMobile 控制台。随后使用教育配置设备策略配置 “课堂” 应用程序（将该应用程序部署到教师的设备）。

有关 Apple 教育功能的详细信息，请参阅 Apple 教育站点和来自同一站点的 Apple《教育部署指南》。

必备条件

- Citrix Gateway
- 为 MDM+MAM 配置的注册配置文件。
- 安装了 iOS 9.3（最低版本）的 Apple iPad 第三代（最低版本）或 iPad Mini

> 注意：
>
> XenMobile 不针对 LDAP 或 Active Directory 验证 ASM 用户帐户。但是，可以将 XenMobile 连接到 LDAP 或 Active Directory 以便管理与 ASM 教师或学生无关的用户和设备。例如，可以使用 Active Directory 将 Secure Mail 和 Secure Web 提供给其他 Apple ASM 成员，例如 IT 管理员和经理。
>
> 由于 Apple ASM 教师和学生都是本地用户，因此，不需要向其设备部署 Citrix Secure Hub。
>
> 包括 Citrix Gateway 身份验证的 MAM 注册不支持本地用户（仅支持 Active Directory 用户）。因此，XenMobile 仅向教师和学生设备部署必需的批量购买应用程序和 iBooks。

共用的 **iPad** 的必备条件

- 任意 iPad Pro、iPad 第五代、iPad Air 2 或更高版本以及 iPad mini 4 或更高版本
- 至少 32 GB 存储空间
- 受监督

配置 **Apple** 校园教务管理和 **XenMobile**

从 Apple 或 Apple 授权经销商或运营商处购买 iPad 后，请按照本节介绍的工作流程设置您的 Apple ASM 帐户和设备。此工作流程包括您在 ASM 门户和 XenMobile 控制台中执行的步骤。

请按照这些说明为您在一对一模式（每个学生一个 iPad）下使用的任何 iPad 或教师 iPad（非共享）配置集成。要配置公用的 iPad，请参阅配置公用的 iPad。

步骤 **1**：创建 **Apple** 校园教务管理帐户并完成设置助手

如果要从 Apple 部署计划升级，请参阅 Apple 支持文章 Upgrade your institution to ASM（将您的机构升级到 ASM）。要创建 Apple 校园教务管理帐户，请转至 https://school.apple.com/并按照说明进行注册。首次登录 ASM 时，设置助手将打开。

- 有关 ASM 必备条件、设置助手和管理任务的信息，请参阅 Apple School Manager User Guide（《Apple 校园教务管理用户指南》）。
- 设置 Apple ASM 时，请使用与 Active Directory 的域名不同的域名。例如，请在 ASM 的域名中添加 `appleid` 之类的前缀。
- 将 ASM 连接到您的名单数据时，ASM 将为教师和学生创建管理式 Apple ID。名单数据包括教师、学生和班级。有关向 ASM 添加名单数据的信息，请参阅前面引用的《ASM 用户指南》。
- 可以为您的机构自定义管理式 Apple ID 格式，如前文引用的 “ASM 用户指南” 中所述。

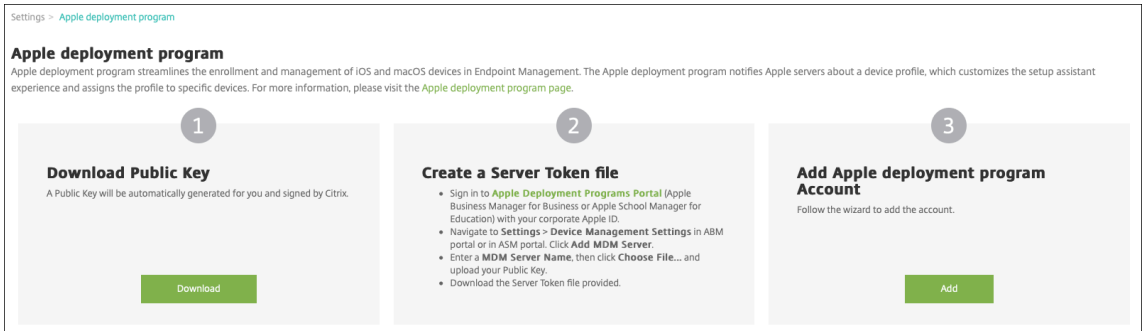
  > 重要：
  >
  > 将 ASM 信息导入 XenMobile 后，请勿更改托管 Apple ID。

- 如果您是通过经销商或运营商购买的设备，请将这些设备链接到 Apple ASM。有关信息，请参阅前面引用的《ASM 用户指南》。

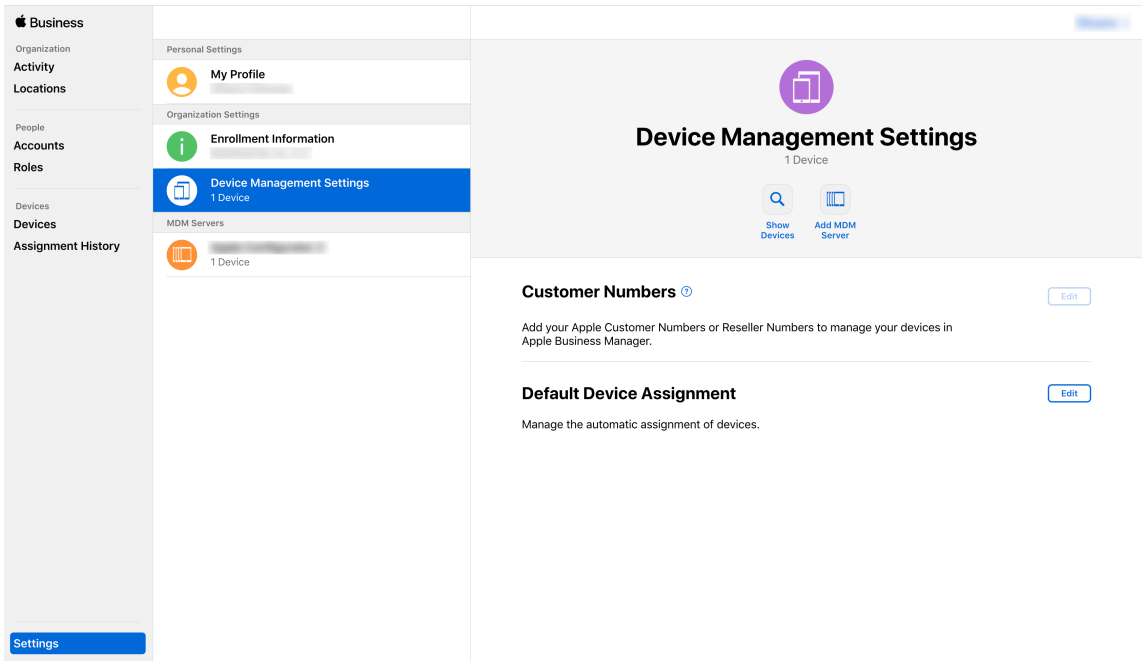
步骤 **2**：将 **XenMobile** 配置为 **Apple** 校园教务管理的 **MDM** 服务器并配置设备分配

ASM 门户包括 **MDM** 服务器选项卡。需要使用 XenMobile 中的公钥文件才能完成该设置。

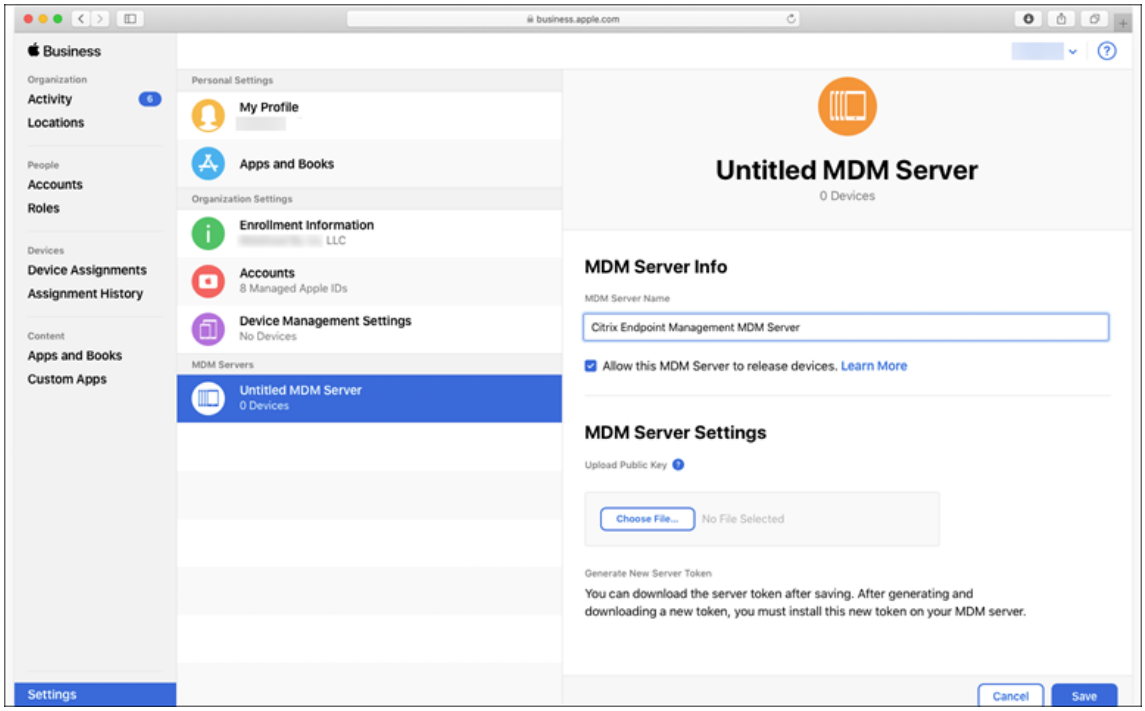
1. 将您的 XenMobile 的公钥下载到您的本地计算机：在 XenMobile 控制台中，转至设置 **> Apple** 部署计划。



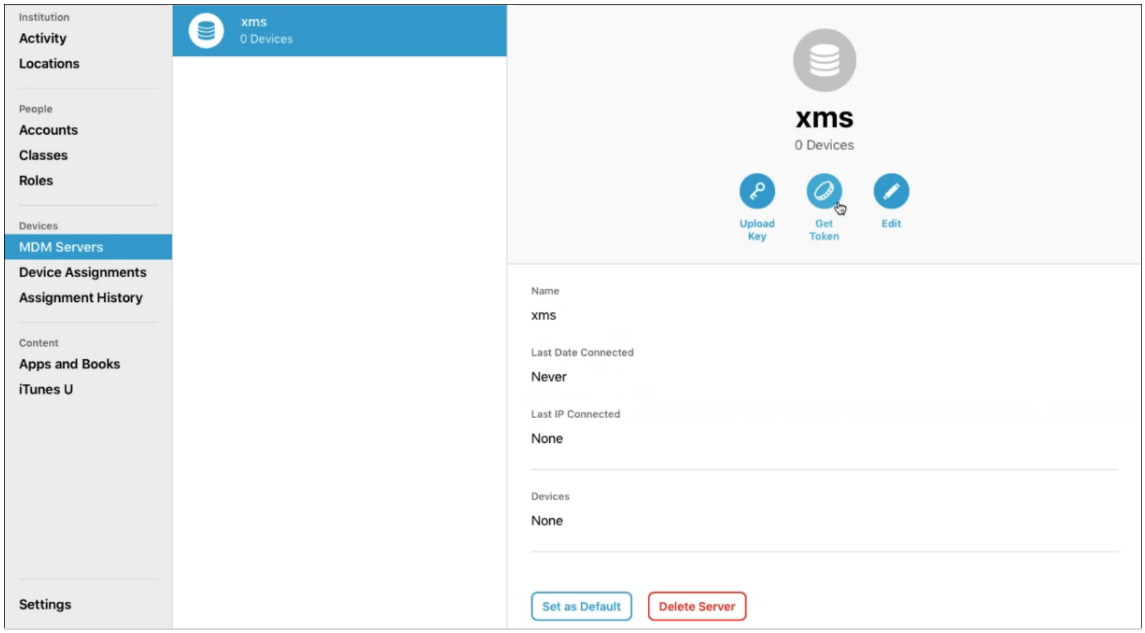
2. 在下载公钥下，单击下载，然后保存 PEM 文件。
3. 在 **Apple** 校园教务管理门户中，单击设置，然后单击设备管理设置。单击 **Add MDM Server**（添加 MDM 服务器）。



4. 键入 XenMobile 的名称。键入的服务器名称仅供参考，并不是服务器 URL 或名称。在 **Upload Public Key**（上载公钥）下，单击 **Choose File**（选择文件）。



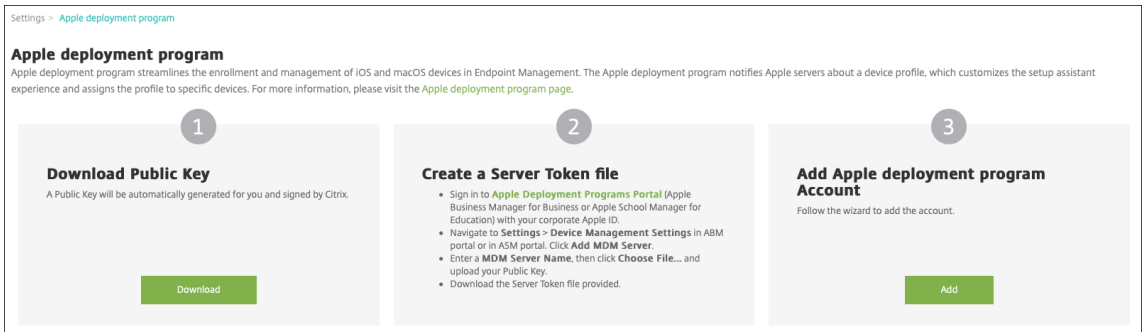
5. 上载您从 XenMobile 下载的公钥，然后单击 **Save**（保存）。
6. 生成服务器令牌：单击 **Download Token**（下载令牌）以将服务器令牌文件下载到您的计算机。



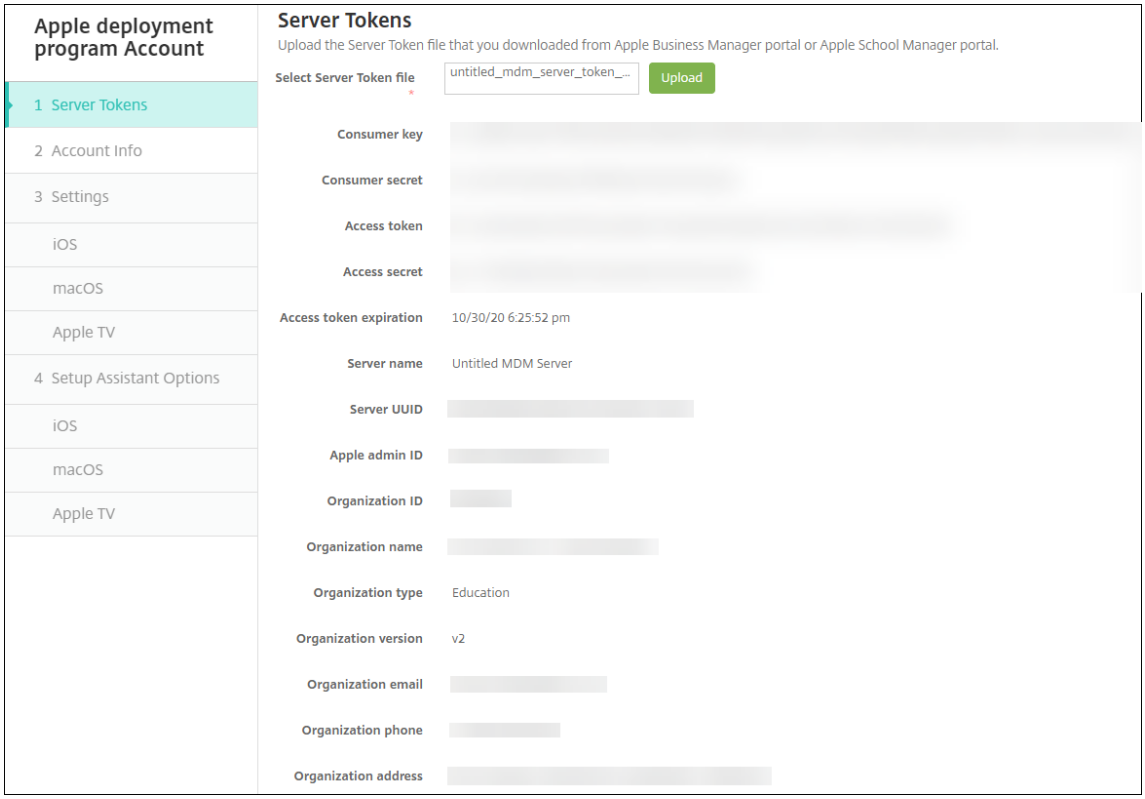
7. 在 **Default Device Assignment**（默认设备分配）下，单击 **Change**（更改）。选择设备的分配方式，然后提供所需的信息。有关信息，请参阅《ASM 用户指南》。

步骤 **3**：向 **XenMobile** 中添加 **Apple** 校园教务管理帐户

1. 在 XenMobile 控制台中，转至设置 **> Apple** 部署计划，然后在添加 **Apple** 部署计划帐户下，单击添加。



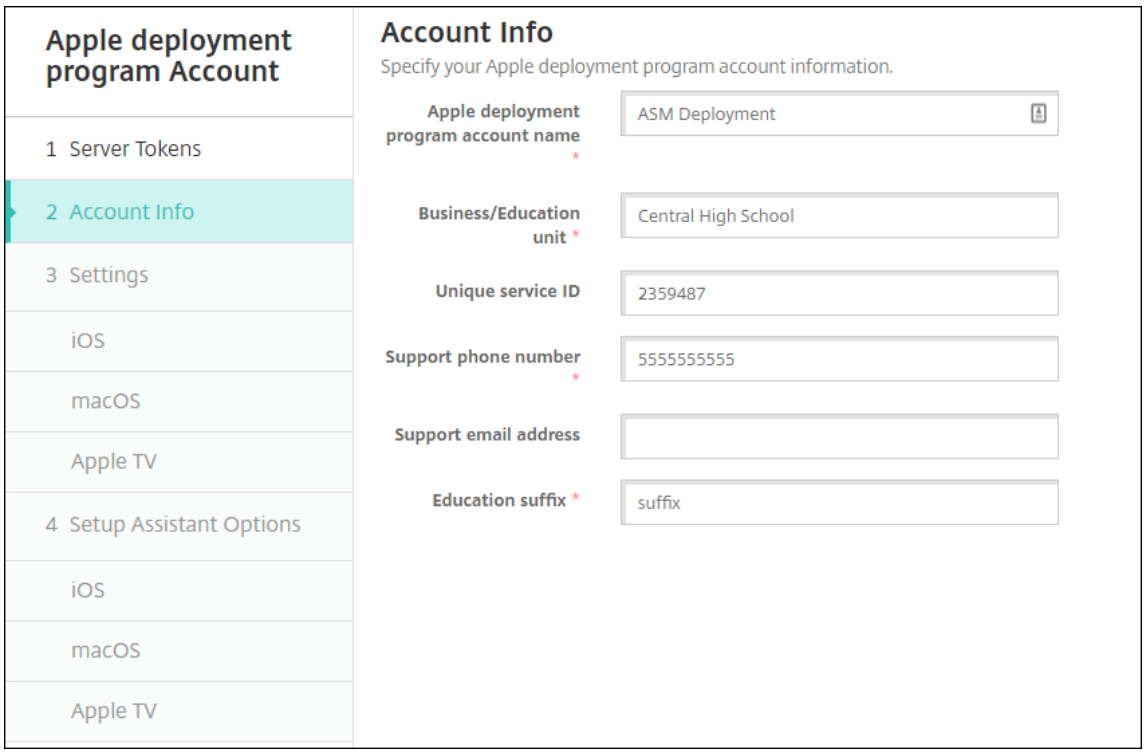
2. 在服务器令牌页面中，单击上载，然后选择您从 Apple ASM 门户下载的服务器令牌（P7M 文件）文件。此时将显示令牌信息。



备注：

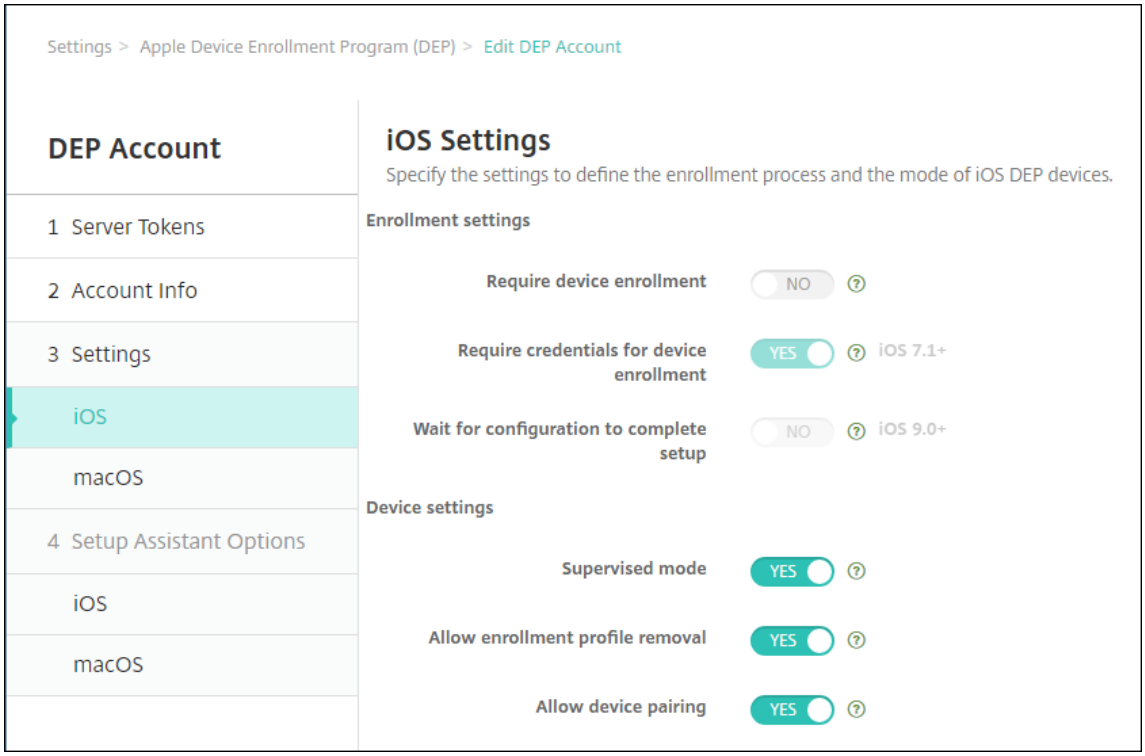
- 组织 **ID** 为 Apple 部署计划的客户 ID。
- ASM 帐户的组织类型为教育，组织版本为 **v2**。

3. 在帐户信息页面中，指定以下设置。



- **Apple** 部署计划帐户名称：此 Apple 部署计划帐户的唯一名称。请使用反映您如何组织 Apple 部署计划帐户（例如按国家/地区或组织层次结构）的名称。
- 业务/教育单位：设备分配的教育单位或部门。此字段为必填字段。
- 唯一服务 **ID**：有助于您进一步识别帐户的可选唯一 ID。
- 支持电话号码：支持电话号码，用户可以在设置期间拨打此号码寻求帮助。此字段为必填字段。
- 支持电子邮件地址：向最终用户提供的可选支持电子邮件地址。
- 教育后缀：为给定 ASM 部署计划帐户对班级设置标志。（批量购买后缀标记给定批量购买帐户的应用程序和 iBooks。）建议对两个帐户、ASM 部署计划和 ASM 批量购买使用相同的后缀。

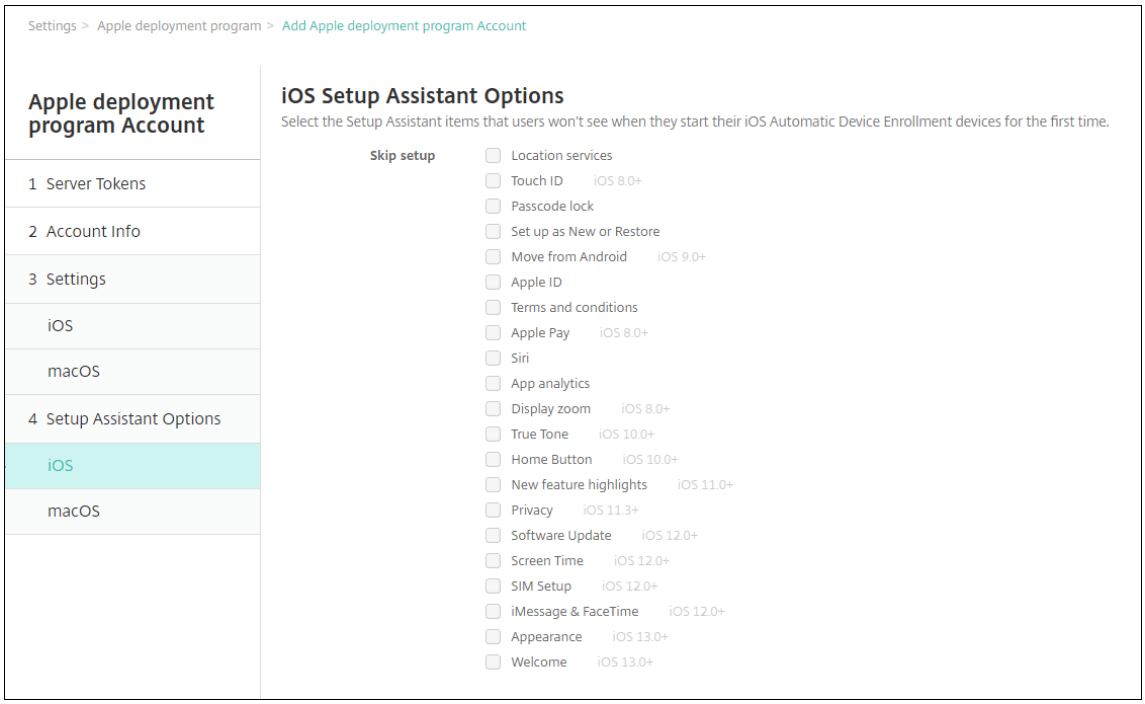
4. 单击 **Next**（下一步）。在 **iOS** 设置中，指定以下设置。



- 注册设置
  - 要求设备注册：要求用户注册其设备。请将此设置更改为否。
  - 需要提供凭据才能完成设备注册：要求用户在 Apple 部署计划设置过程中输入其凭据。对于 ASM 与 XenMobile 的集成，默认情况下，此设置为是，不能更改。Apple 部署计划需要凭据才能注册设备。
  - 等待完成配置设置：是否要求用户设备一直保持在“设置助理”模式，直到将所有 MDM 资源部署到设备。对于 ASM 与 XenMobile 的集成，默认情况下，此设置为否。根据 Apple 文档，当设备处于“设置助手”模式时，以下命令可能不起作用：
    - InviteToProgram
    - InstallApplication
    - InstallMedia
    - ApplyRedemptionCode
- 设备设置
  - 受监督模式：将 iOS 设备置于受监督模式。请勿更改默认值是。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 将 iOS 设备置于受监督模式。
  - 共享模式：在 iPad 上启用共享模式。不满足最低要求的设备无法共享。
  - 允许删除注册配置文件：对于 ASM 集成，允许用户从设备中删除注册配置文件。请将此设置更改为是。
  - 允许设备配对：对于 Apple 校园教务管理集成，允许设备配对以便您能够通过 Apple App Store 和 Apple Configurator 管理这些设备。请将此设置更改为是。

5. 在 **iOS** 设置助手选项中，选择用户在首次启动其设备时跳过的 iOS 设置助手步骤。默认情况下，设置助手包括所有步骤。请注意，从设置助手中删除步骤将简化用户体验。

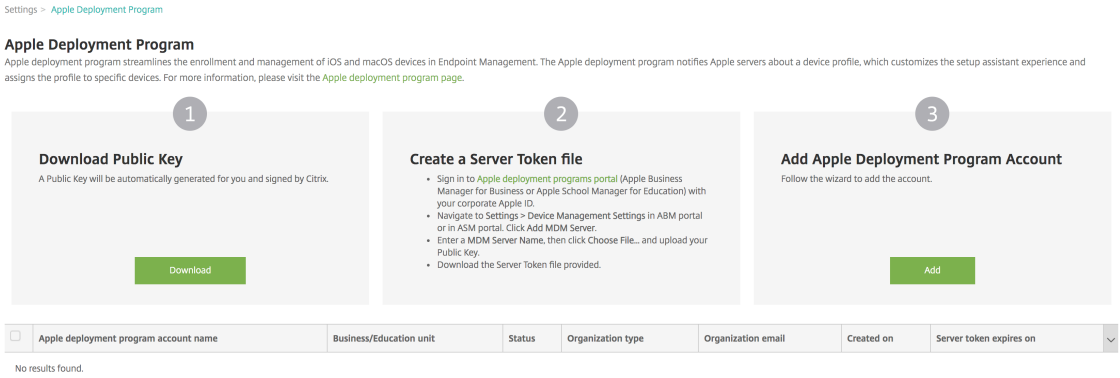
> 重要：
>
> Citrix 强烈建议您包括 **Apple ID** 以及条款和条件步骤。这些步骤将使教师和学生能够提供新的管理式 Apple ID 密码并接受必要的条款和条件。



- 定位服务：在设备上设置定位服务。
- **Touch ID**：在 iOS 设备上设置 Touch ID。
- 通行码锁：为设备创建通行码。
- 设置为新对象或还原：将设备设置为新设备或从 iCloud 或 Apple App Store 备份设置设备。
- 从 **Android** 移动：启用从 Android 设备向 iOS 设备传输数据。此选项仅在已选择设置为新对象或还原（即跳过此步骤）时可用。
- **Apple ID**：设置设备的 Apple ID 帐户。Citrix 建议您选中包括此步骤的复选框。
- 条款和条件：要求用户接受条款和条件才能使用设备。Citrix 建议您选中包括此步骤的复选框。
- **Apple Pay**：在 iOS 设备上设置 Apple Pay。
- **Siri**：是否在设备上使用 Siri。
- 应用程序分析：设置是否与 Apple 共享崩溃数据和使用情况统计信息。
- 显示缩放：在 iOS 设备上设置显示分辨率（标准或缩放）。
- **True Tone**：在 iOS 设备上设置 True Tone 显示。
- 主页按钮：设置“主页按钮”屏幕敏感度。
- 新增功能亮点：在 iOS 11.0 设备（最低版本）上设置入门信息屏幕、从任意位置访问 Dock 以及在最近使用的应用程序之间切换。
- 隐私：阻止用户在 Apple 部署计划设备设置过程中看到数据和隐私窗格。适用于 iOS 11.3 及更高版本。

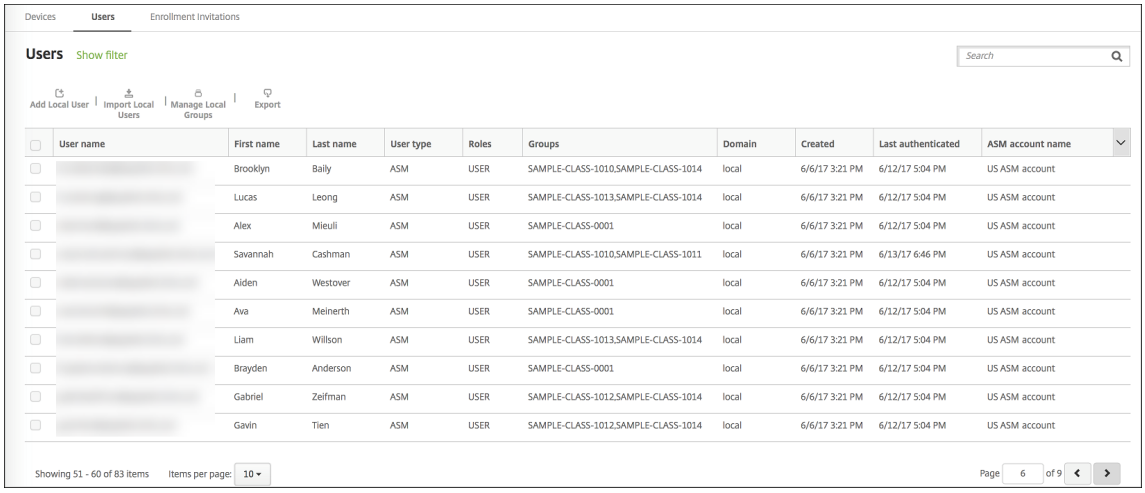
- 软件更新：阻止用户在 Apple 部署计划设备设置过程中看到强制软件更新屏幕。适用于 iOS 12.0 及更高版本。
- 屏幕时间：阻止用户在 Apple 部署计划设备设置过程中看到“屏幕时间”屏幕。适用于 iOS 12.0 及更高版本。
- **SIM** 卡设置：阻止用户在 Apple 部署计划设备设置过程中看到“添加手机网络规划”屏幕。适用于 iOS 12.0 及更高版本。
- **iMessage** 和 **FaceTime**：阻止用户在 Apple 部署计划设备设置过程中看到“iMessage 和 FaceTime”屏幕。适用于 iOS 12.0 及更高版本。

6. 该帐户显示在设置 **> Apple** 部署计划上。要测试 XenMobile 与您的 ASM 帐户之间的连接，请选择该帐户并单击测试连接。



此时将显示一条状态消息。

几分钟后，ASM 中的用户帐户将显示在管理 **>** 用户页面上。XenMobile 根据导入的每个用户的管理式 Apple ID 创建本地用户帐户。在以下示例中，用户帐户的自定义 Apple ID 的域名前缀为 `appleid`。

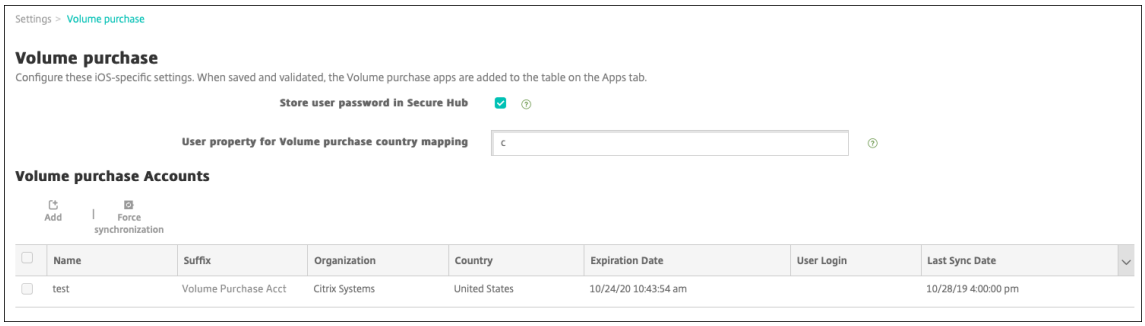


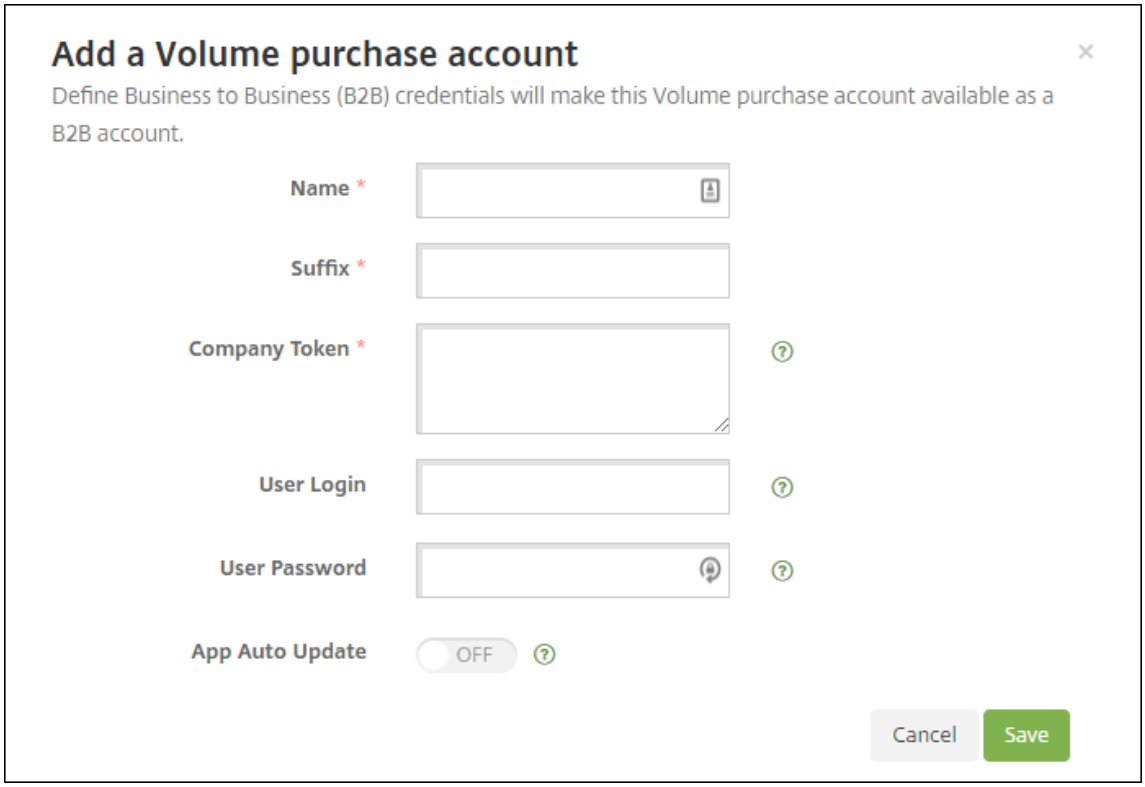
要查找给定 ASM 帐户的所有用户，请在每个用户搜索过滤器中键入帐户名称。

步骤 **4**：为 **Apple** 校园教务管理配置教育批量购买帐户

在本节中，您将 XenMobile 指向用于为应用程序和 iBooks 购买批量购买许可证的批量购买帐户。

1. 要为 ASM 配置教育批量购买帐户，请按照 Apple 批量购买中的说明进行操作。“添加批量购买帐户”屏幕要求您提供公司令牌。请直接从您的教育批量购买帐户下载令牌并将其粘贴到添加批量购买帐户屏幕中。





2. 等待几分钟，直至批量购买许可证导入到 XenMobile 中。

步骤 **5**：为 **Apple** 校园教务管理用户添加密码

添加 ASM 帐户后，XenMobile 将从 ASM 导入类和用户。XenMobile 将班级视为本地组，并在控制台中使用术语“组”。如果某个班级在 ASM 中具有组名称，XenMobile 会将该组名称分配给班级。否则，XenMobile 将为组名称使用源系统 ID。XenMobile 不为班级名称使用课程名称，因为 ASM 中的课程名称不唯一。

XenMobile 使用管理式 Apple ID 创建用户类型为 **ASM** 的本地用户。这些用户属于本地用户，因为 ASM 创建的凭据与所有外部数据源都无关。因此，XenMobile 不使用目录服务器对这些新用户进行身份验证。

ASM 不会向 XenMobile 发送临时用户密码。可以从 CSV 文件导入或手动添加这些密码。要导入临时用户密码，请执行以下操作：

1. 获取 ASM 在创建管理式 Apple ID 临时密码时生成的 CSV 文件。
2. 编辑 CSV 文件，将临时密码替换为用户在 XenMobile 中注册时提供的新密码。为实现这一目的，不对密码类型设置任何限制。

   CSV 文件中的条目格式如下所示：`user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

   其中：

   用户：`user@appleid.citrix.com`

名字：`Firstname`

中间名：`Middle`

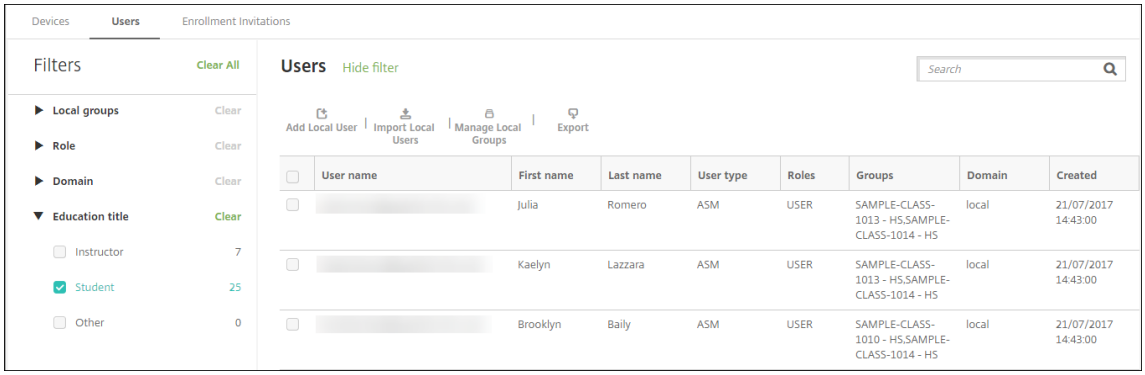
姓氏：`Lastname`

密码：`Password123!`

3. 在 XenMobile 控制台中，单击管理 **>** 用户。此时将显示用户页面。

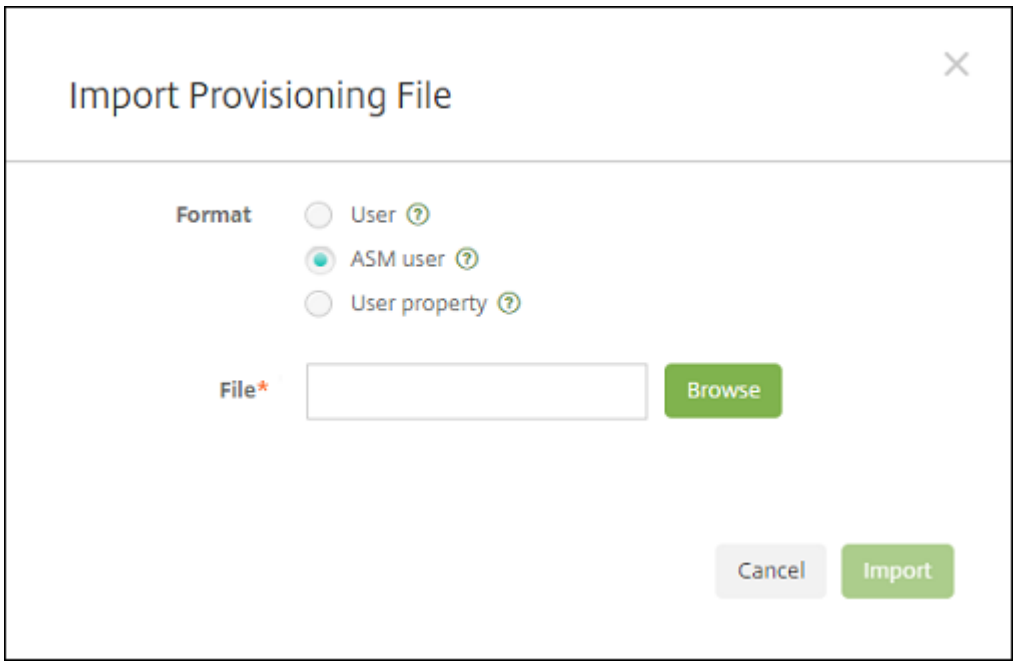
   下面的管理 **>** 用户屏幕示例显示了从 ASM 中导入的用户的列表。在用户列表中：

   - 用户名显示管理式 Apple ID。
   - 用户类型为 **ASM**，指示源自 ASM 的帐户。
   - 组显示班级。

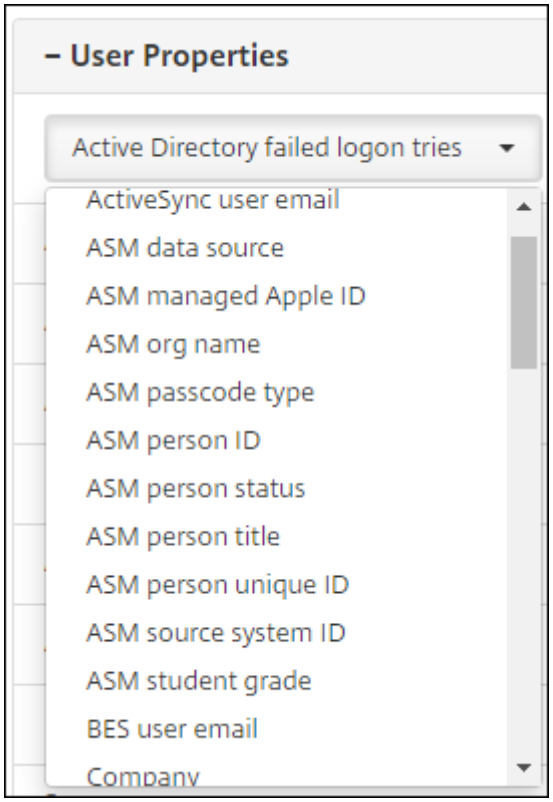


4. 单击导入本地用户。此时将显示导入预配文件对话框。

5. 对于格式，请选择 **ASM** 用户，导航到您在步骤 2 中准备的 CSV 文件，然后单击导入。



6. 要查看某个本地用户的属性，请选择该用户，然后单击编辑。



除名称属性外，还可以使用以下 ASM 属性：

- **ASM** 数据源：班级的数据源，例如 **CSV** 或 **SFTP**。
- **ASM** 管理式 **Apple ID**：管理式 Apple ID 可能包括您的机构名称和 `appleid`。例如，该 ID 可能类似于 johnappleseed@appleid.myschool.edu。XenMobile 需要使用管理式 Apple ID 进行身份验证。
- **ASM** 组织名称：您在 XenMobile 中为帐户指定的名称。
- **ASM** 通行码类型：人员的密码策略：复杂（包含 8 个或更多数字和字母的非学生用密码）、**four**（4）（数字）或 **six**（6）（数字）。
- **ASM** 人员的唯一 **ID**：用户的标识符。
- **ASM** 人员状态：指定管理式 Apple ID 的状态为活动还是不活动。用户提供其管理式 Apple ID 帐户的新密码后，此状态将变为活动。
- **ASM** 人员职称：“教师”、“学生”或“其他”。
- **ASM** 人员的唯一 **ID**：用户的唯一标识符。
- **ASM** 源系统 **ID**：系统源的标识符。
- **ASM** 学生年级：学生的年级信息（教师不使用）。

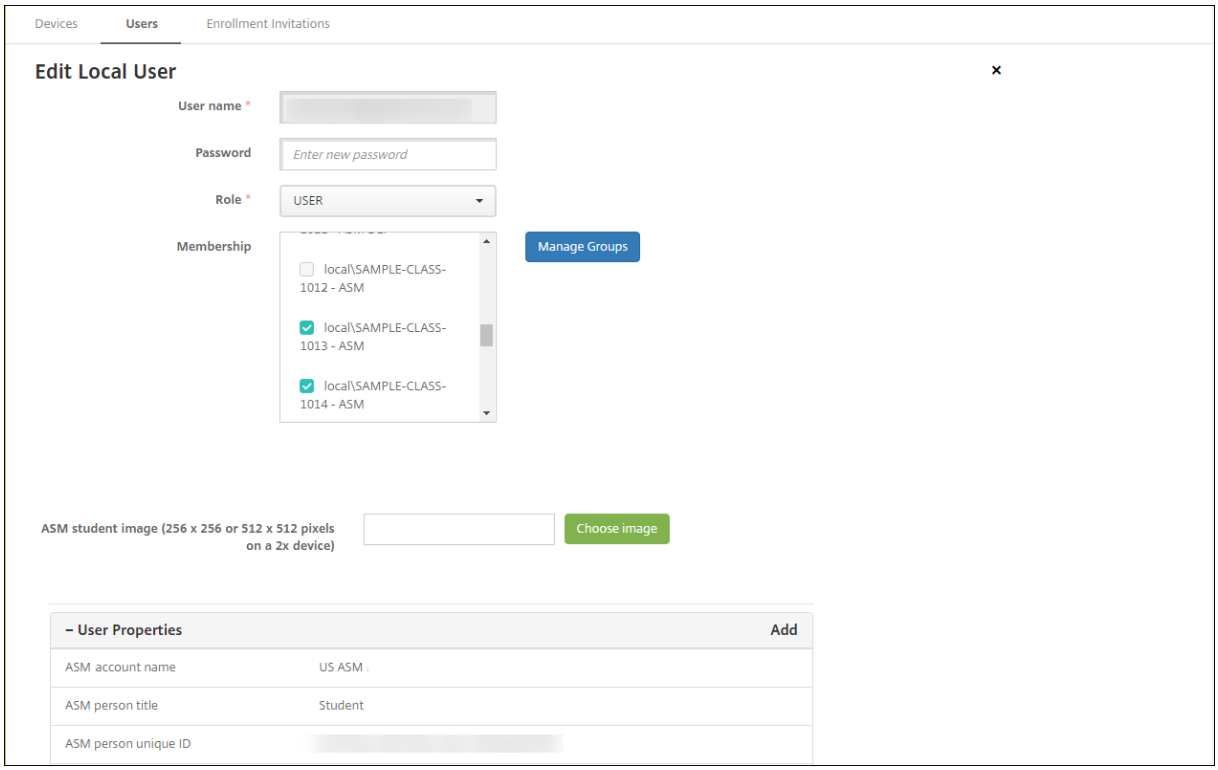
步骤 **6**：（可选）添加学生的照片

可以添加每个学生的照片。如果教师使用 Apple“课堂”应用程序，照片将在此应用程序中显示。

照片建议：

- 分辨率：256 x 256 像素（在 2x 设备上建议 512 x 512 像素）
- 格式：JPEG、PNG 或 TIFF

要添加照片，请转至管理 **>** 用户，选择某个用户，单击编辑，然后单击选择图像。



步骤 **7**：规划和添加资源和交付组至 **XenMobile**

交付组指定要部署到各类别的用户的资源。例如，可以为教师和学生创建一个交付组。或者，可以创建多个交付组，以便您能够自定义发送给不同教师或学生的应用程序、媒体和策略。可以为每个班级创建一个或多个交付组。还可以为管理员（教育机构中的其他员工）创建一个或多个交付组。

部署到用户设备的资源包括设备策略、批量购买应用程序和 iBooks。

- 设备策略：

  如果教师使用“课堂”应用程序，则需要配置教育配置设备策略。请务必检查其他设备策略，以确定您希望如何配置和限制教师和学生的 iPad。

- 批量购买应用程序：

  XenMobile 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。XenMobile 不支持将此类批量购买应用程序作为可选应用程序进行部署。

  如果您使用 Apple“课堂”应用程序，请仅将其部署到教师的设备。

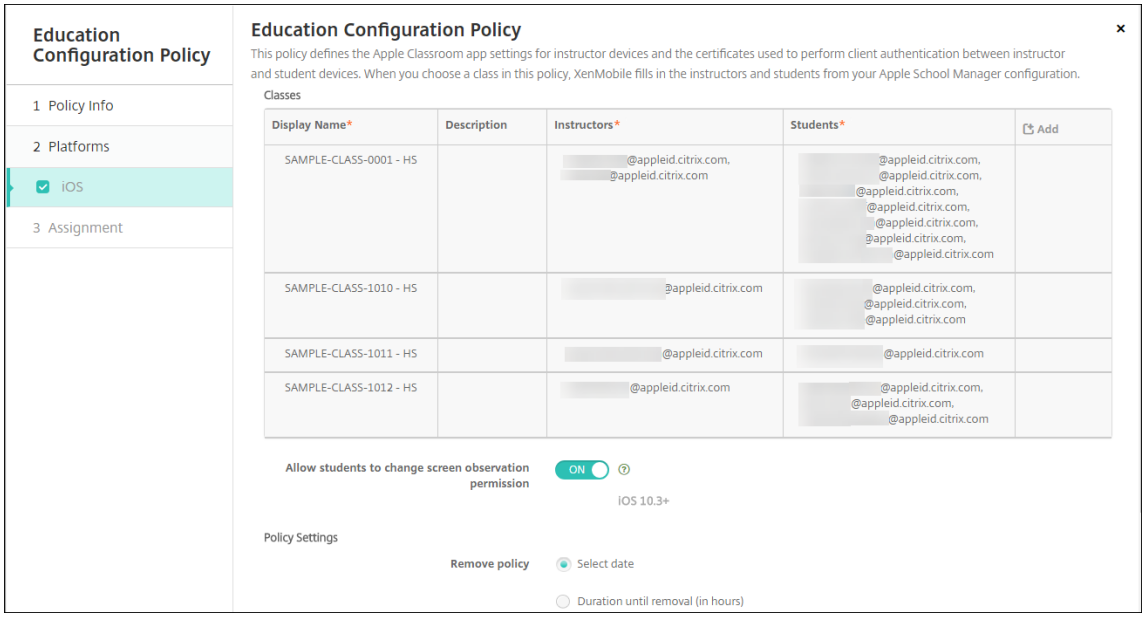
  部署要提供给教师或学生的任何其他应用程序。此解决方案不使用 Citrix Secure Hub 应用程序，因此，不需要为教师或学生部署。

- 批量购买 iBooks：

  XenMobile 连接到您的 ASM 帐户后，您购买的 iBooks 将显示在 XenMobile 控制台的配置 **>** 媒体中。该页面上列出的 iBooks 可以添加到交付组中。XenMobile 仅支持将 iBooks 添加为必需媒体。

为教师和学生规划资源和交付组后，可以在 XenMobile 控制台中创建这些项目。

1. 创建要为教师或学生设备部署的任何设备策略。有关教育配置设备策略的信息，请参阅教育配置设备策略。

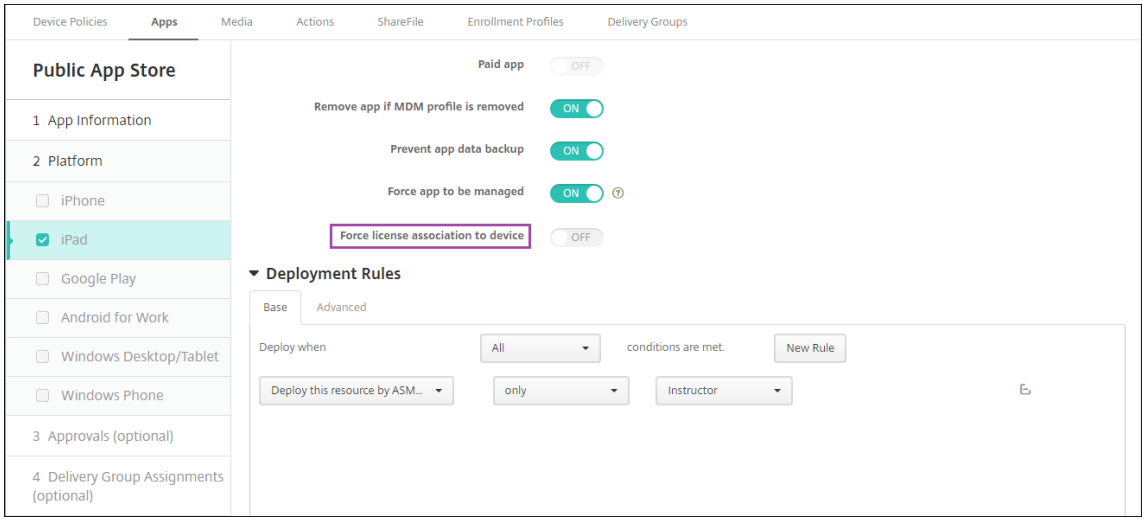


   有关设备策略的信息，请参阅设备策略以及各策略文章。

2. 配置应用程序（配置 **>** 应用程序）和 iBooks（配置 **>** 媒体）：

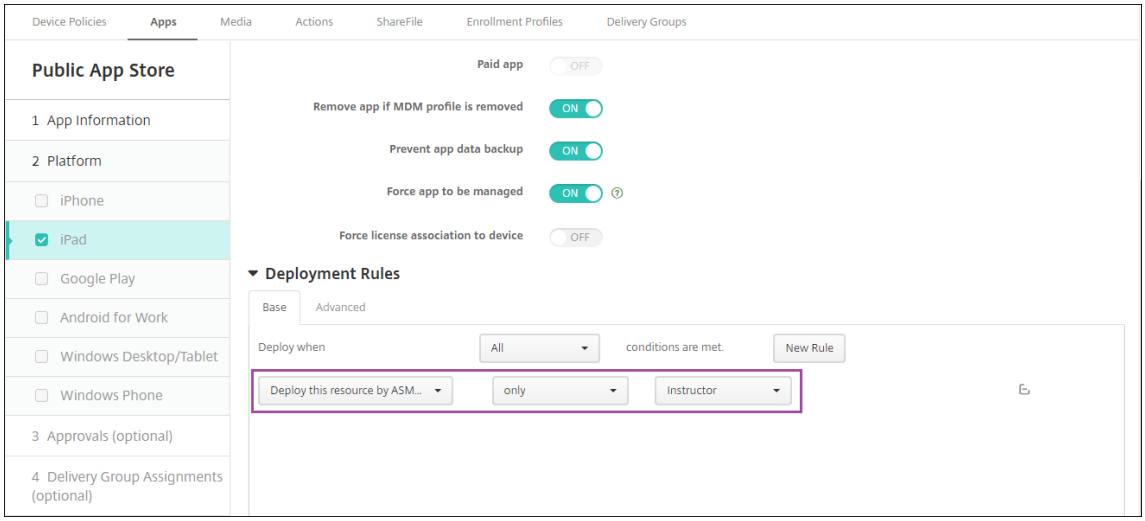
   - 默认情况下，XenMobile 在用户级别分配应用程序和 iBooks。首次部署过程中，教师和学生将收到一条提示注册参加 ASM 的提示。接受邀请后，用户会在接下来的部署中（6 个小时内）收到其 ASM 应用程序和 iBooks。Citrix 建议您强制为新 ASM 用户部署应用程序和 iBooks。为此，请选择交付组并单击部署。

     可以选择在设备级别分配应用程序（而非 iBooks）。为此，请将强制与设备建立许可证关联设置更改为开。在设备级别分配应用程序时，用户不会收到加入 Apple 批量购买的邀请。



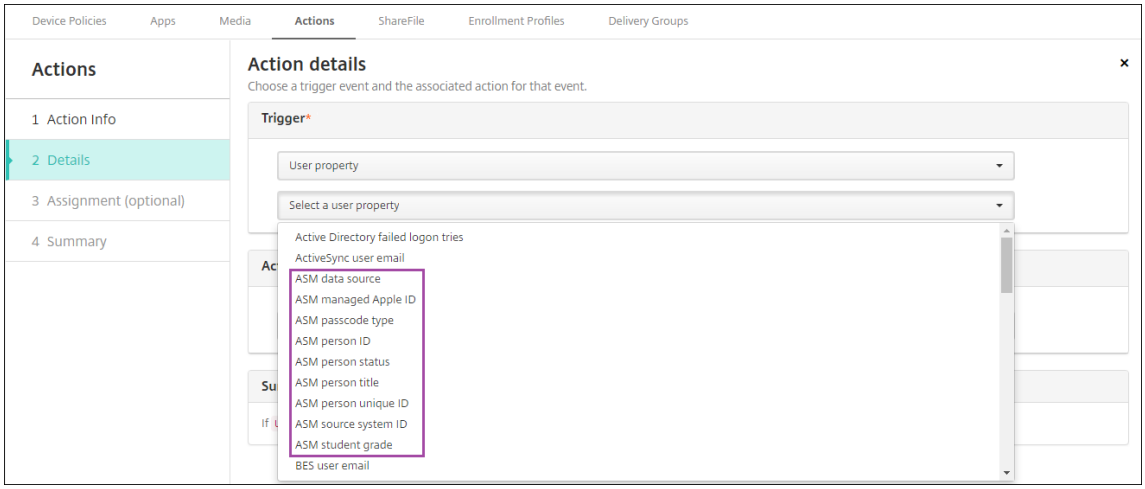
- 要仅为教师部署应用程序，请选择仅包括教师的交付组，或者使用以下部署规则：

```
Deploy this resource by ASM device type
only
Instructor
<!--NeedCopy-->
```



- 有关添加批量购买应用程序的帮助，请参阅添加公共应用商店应用程序。

3. 可选。根据 ASM 用户属性创建操作。例如，您可能会创建在新应用程序安装时向学生设备发送通知的操作。或者，可以创建用户属性触发的操作，如以下示例中所示。

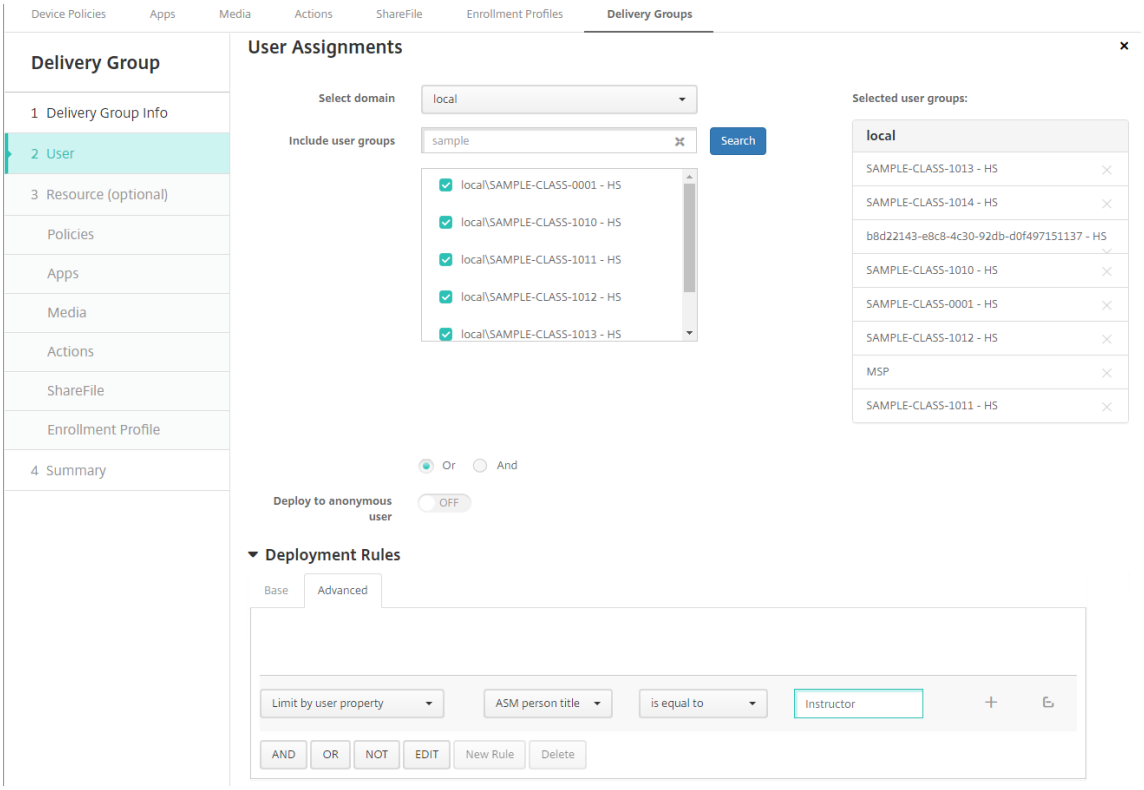


要创建操作，请转至配置 **>** 操作。有关配置操作的信息，请参阅自动化操作。

4. 在配置 **>** 交付组中，为教师和学生创建交付组。选择从 ASM 中导入的班级。此外，请为教师和学生创建部署规则。

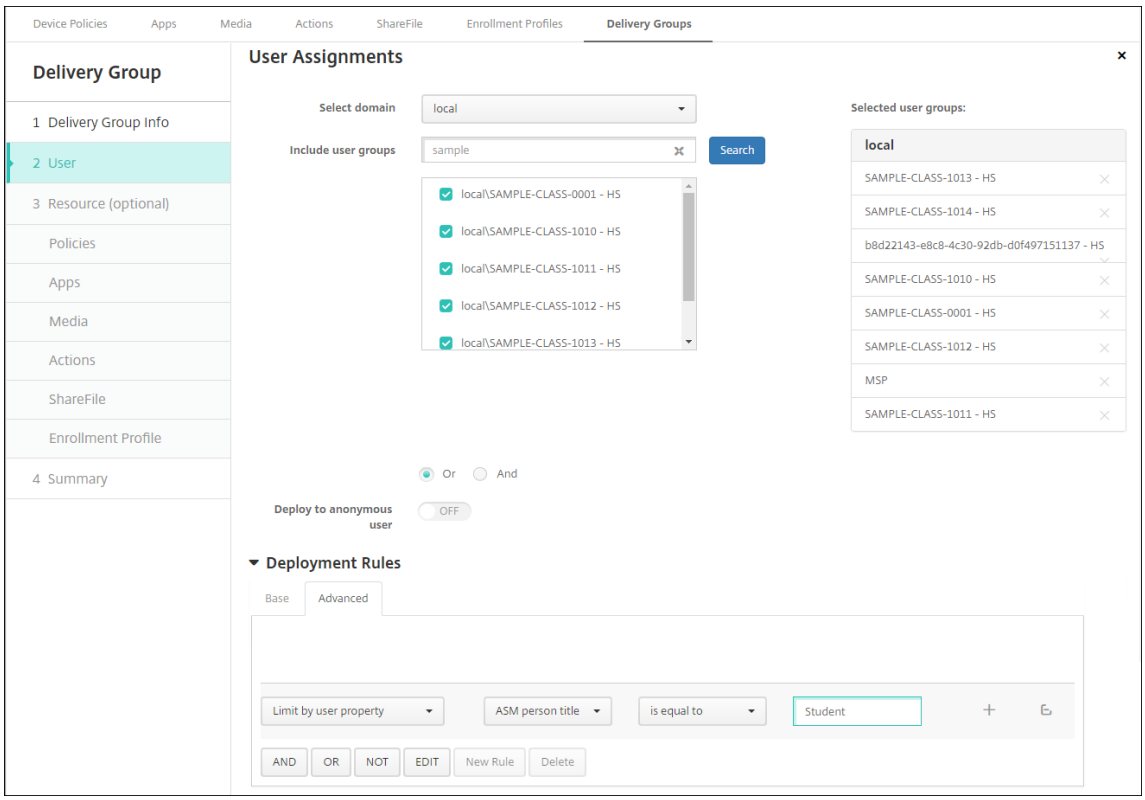
   例如，以下用户分配针对教师。部署规则为：

```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

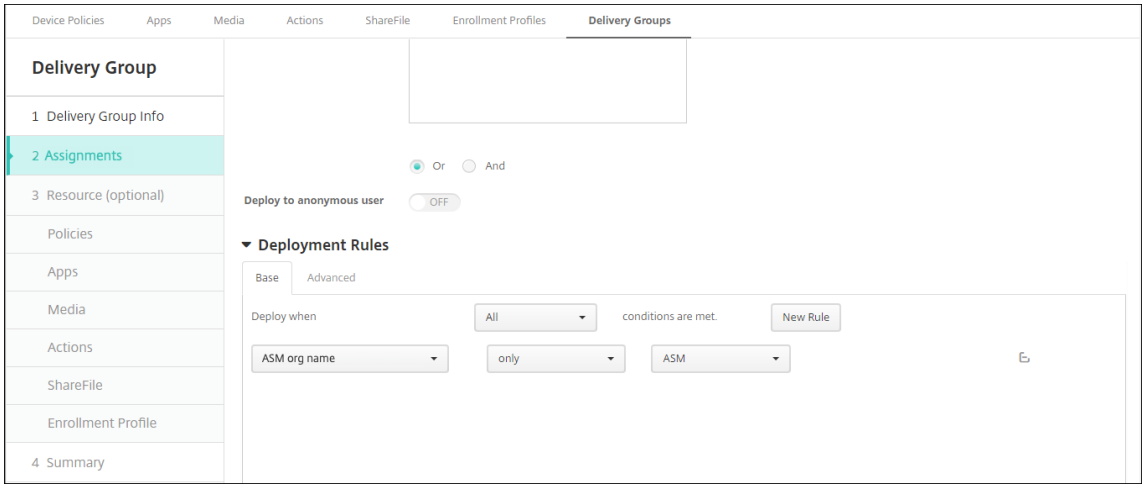



以下用户分配针对学生。部署规则为：

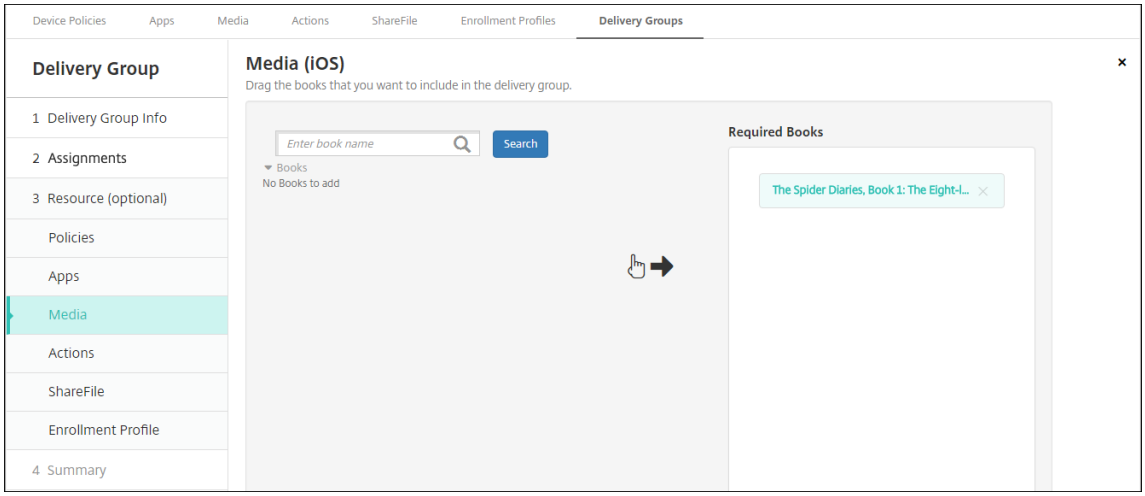
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

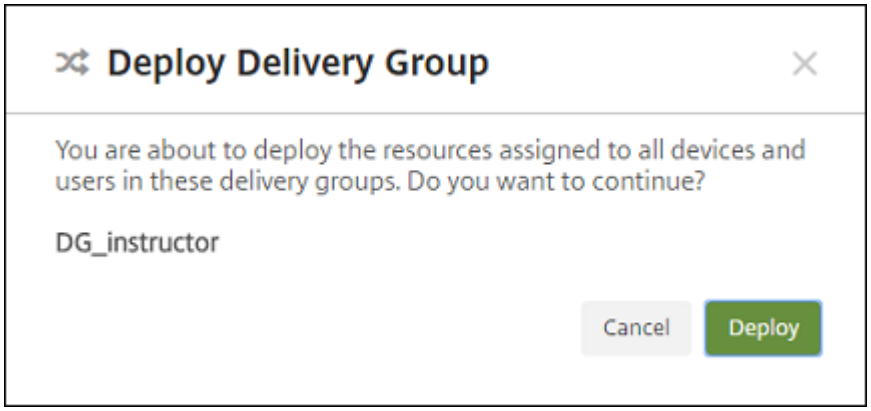
还可以使用基于 ASM 组织名称的部署规则过滤交付组。



5. 将资源分配给交付组。以下示例显示了交付组中包含的 iBook。



以下示例显示了在您选择交付组并单击部署时显示的确认对话框。



有关详细信息，请参阅部署资源中的“编辑交付组”和“部署到交付组”。

步骤 **8**：测试教师和学生的设备注册

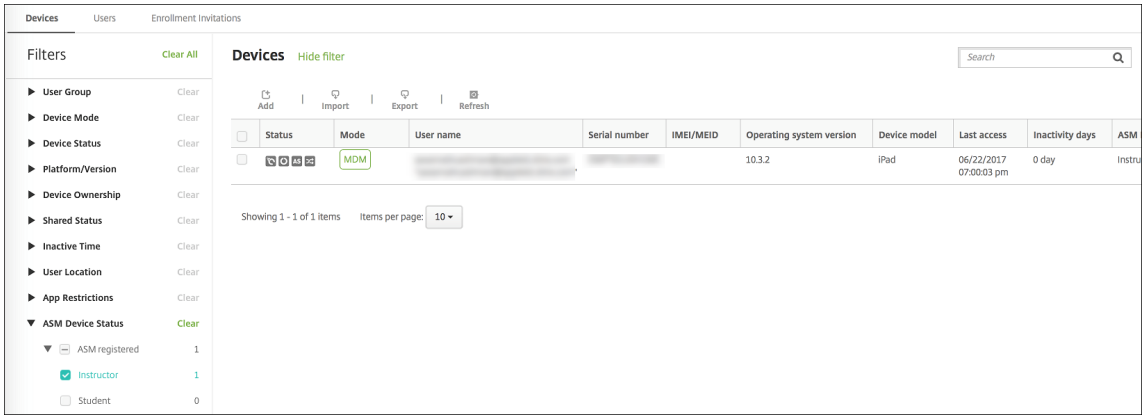
可以通过以下方法之一注册设备：

- 学校管理员可以使用您能够在 XenMobile 控制台中设置的用户密码注册教师和学生设备。因此，可以向用户提供设置了应用程序和媒体的设备。
- 收到设备时，用户使用您向其提供的用户密码进行注册。注册完成后，XenMobile 将向设备发送设备策略、应用程序和媒体。

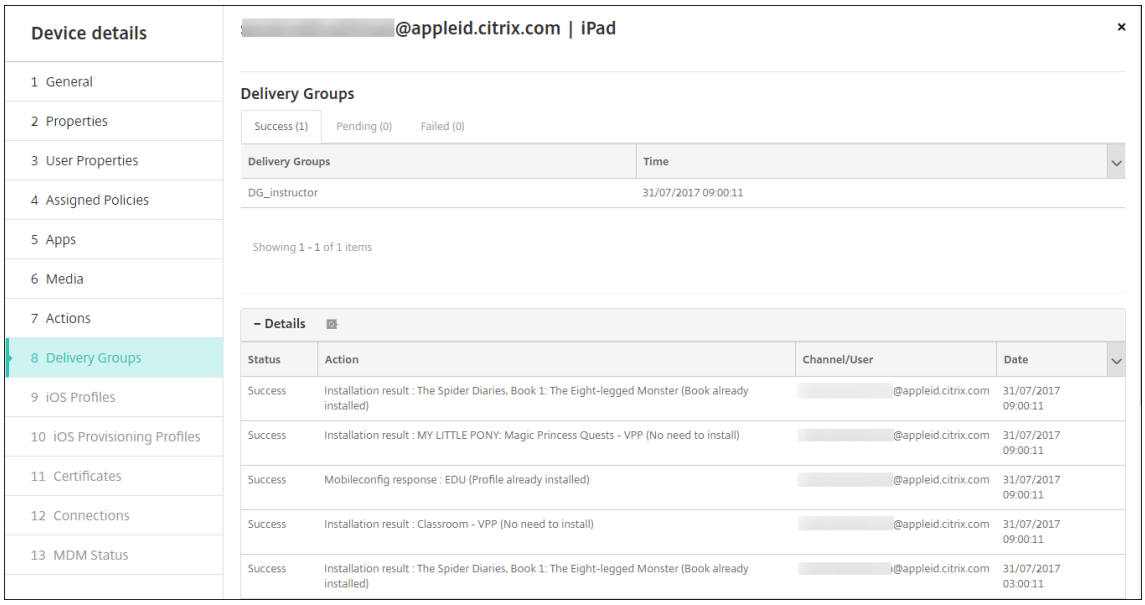
要测试注册，请使用链接到 ASM 的 Apple 部署计划设备。

1. 如果设备未链接到 ASM，请通过执行硬重置来擦除设备内容和设置。
2. 将 ASM 设备注册给教师。然后，将 ASM 设备注册给学生。
3. 在管理 **>** 设备页面中，检查 ASM 设备是否在仅 MDM 模式下注册。

   可以按 ASM 设备状态过滤设备页面：已注册 **ASM**、已共享 **ASM**、教师和学生。



4. 要验证是否为每个设备正确部署了 MDM 资源，请执行以下操作：选择设备，单击编辑，然后检查各页面。



步骤 **9**：分发设备

Apple 建议您举办活动，以便能够将设备分发给教师和学生。

如果未分发预注册的设备，还需要向这些用户提供以下各项内容：

- 用于注册的 XenMobile 密码
- 管理式 Apple ID 的 ASM 临时密码。

首次用户体验如下所示。

1. 用户在硬重置后首次启动其设备时，XenMobile 将在注册屏幕中提示用户注册其设备。
2. 用户提供用于对 XenMobile 进行身份验证的管理式 Apple ID 和 XenMobile 密码。
3. 在 Apple ID 设置步骤中，设备将提示用户提供其管理式 Apple ID 和 ASM 的临时密码。这些项目将对 Apple 服务验证用户的身份。

4. 设备提示用户为其管理式 Apple ID 创建密码，用于保护 iCloud 中的数据。
5. 在设置助手结束时，XenMobile 将开始向设备中安装策略、应用程序和媒体。对于在用户级别分配的应用程序和 iBooks，设置助手将提示教师和学生注册参加批量购买。接受邀请后，用户会在接下来的部署中（6 个小时内）收到其批量购买应用程序和 iBooks。

配置共用的 iPad

课堂中的多个学生可以共享一个 iPad，学习一位或多位教师教授的不同学科。

您或教师注册共用的 iPad，然后将设备策略、应用程序和媒体部署到这些设备。之后，学生提供其管理式 Apple ID 凭据以登录共用的 iPad。如果您以前为学生部署了“教育配置”策略，这些学生将不再以“其他用户”身份登录共享设备。

XenMobile 对共用的 iPad 使用两个通信通道：面向设备所有者（教师）的系统通道和面向当前常驻用户（学生）的用户通道。XenMobile 使用这些通道为 Apple 支持的资源发送恰当的 MDM 命令。

通过系统通道部署的资源如下：

- 设备策略，例如教育配置、锁屏界面消息、最大常驻用户数和通行码锁宽限期
- 基于设备的批量购买应用程序

  Apple 不支持在共用的 iPad 上使用企业应用程序或基于用户的批量购买应用程序。共用的 iPad 上安装的应用程序是设备的全局应用程序，不基于用户。

- 基于用户的批量购买 iBooks

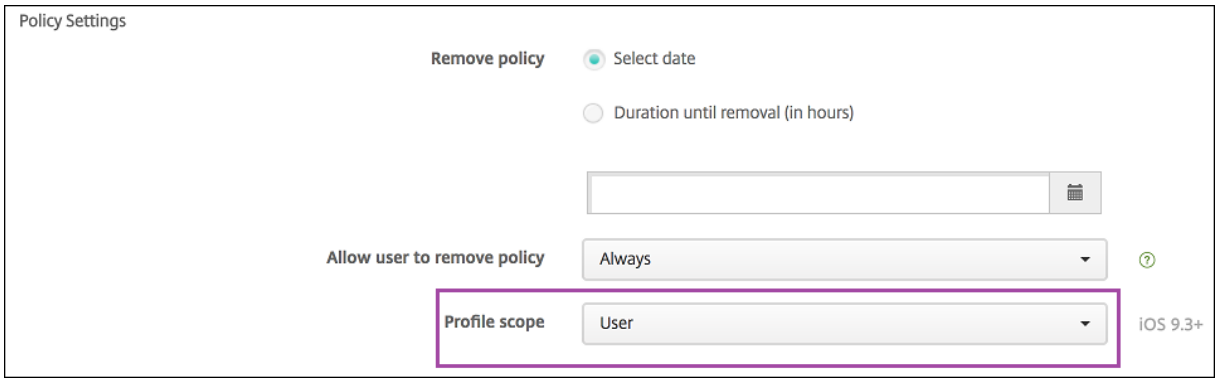
  Apple 支持在共用的 iPad 上分配基于用户的批量购买 iBook。

通过用户通道部署的资源如下：

- 设备策略：应用程序通知、主屏幕布局和限制

  XenMobile 仅支持通过用户通道部署这些设备策略。

配置设备策略时，可以在策略设置配置文件作用域中指定部署通道。



要删除通过用户通道部署的设备策略，请务必为“配置文件删除”策略选择部署范围为用户。

常规工作流程

通常情况下，您负责向教师提供预配置并且受监督的共用的 iPad。教师之后将这些身份分发给学生。如果您未向教师分发预先注册的共用的 iPad：请务必向教师提供其 XenMobile Server 密码，以便能够注册其设备。

配置和注册共用的 iPad 的常规工作流程如下。

1. 使用 XenMobile Server 控制台添加启用了共享模式的 ASM 帐户（设置 **> Apple** 部署计划）。有关详细信息，请参阅接下来的“为共用的 iPad 管理 ASM 帐户”。
2. 如本部分内容中所述，请向 XenMobile 中添加所需的设备策略、应用程序和媒体。将这些资源分配给交付组。
3. 请教师在共用的 iPad 上执行硬重置。此时将显示面向注册的“远程管理”屏幕。
4. 教师注册共用的 iPad。
   XenMobile 将所配置的资源部署到每个已注册的共用的 iPad。自动重新启动后，教师可以与学生共享这些设备。此时 iPad 上将显示登录页面。
5. 学生选择班级，然后输入其管理式 Apple ID 和临时 ASM (ASM) 密码。
   共用的 iPad 对 ASM 进行身份验证，并提示学生创建 ASM 密码。对于下次登录共用的 iPad，学生将提供新 ASM 密码。
6. 正在共用的 iPad 的另一个学生之后可以通过重复上述步骤进行登录。

为共用的 **iPad** 管理 **ASM** 帐户

如果已将 XenMobile 与 Apple 教育功能结合使用：您有在 XenMobile 中为未共享的设备（例如教师使用的设备）配置的现有 ASM 帐户。可以同时为共享和非共享设备使用相同的 ASM 和相同的 XenMobile Server。

XenMobile 支持以下部署场景：

- 每个班级一组共用的 iPad

  在此场景中，您将共用的 iPad 分配给一个班级的学生。iPad 留在课堂中。在该班级中教授不同学科的教师使用一组相同的 iPad。

- 每个教师一组共用的 iPad

  在此场景中，您将共用的 iPad 分配给教师，教师为教授的各个班级使用这些 iPad。

将共用的 **iPad** 组织整理到设备组中

ASM 允许您通过创建多个 MDM 服务器将设备组织整理到多个组中。将共用的 iPad 分配给 MDM 服务器时，请按班级或按教师为每个共用的 iPad 创建一个设备组：

- 共用的 iPad 组 1 > 设备组 1 MDM 服务器
- 共用的 iPad 组 2 > 设备组 2 MDM 服务器
- 共用的 iPad 组 N > 设备组 N MDM 服务器

为每个设备组添加 **ASM** 帐户

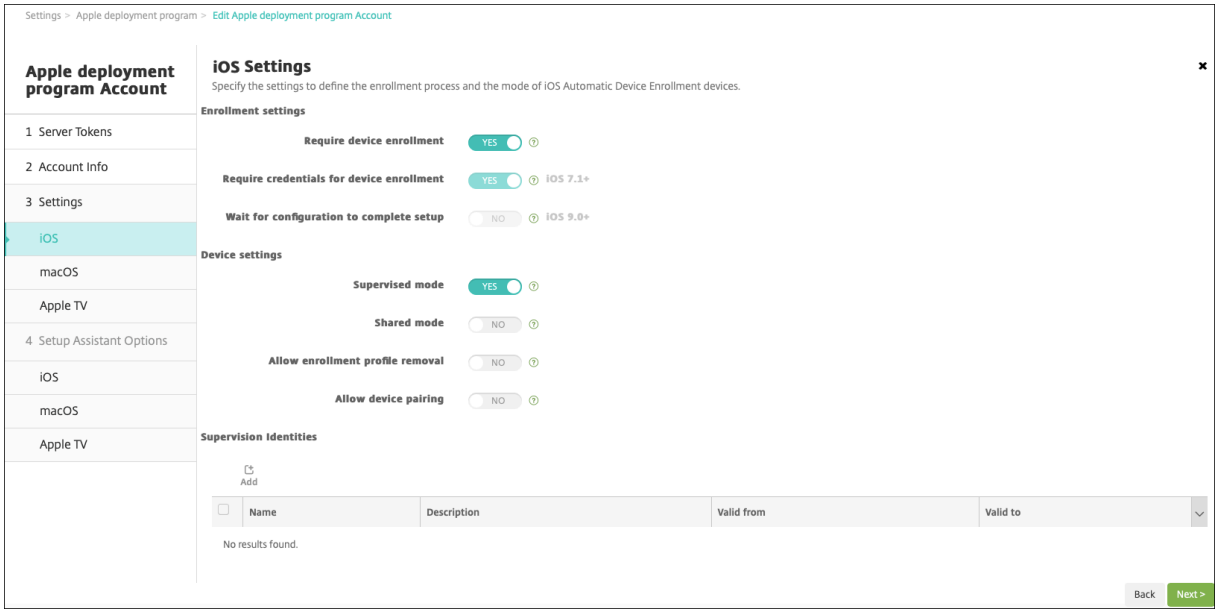
从 XenMobile Server 控制台创建多个 ASM 帐户时，您将自动导入多个共用的 iPad 组（每个班级或教师一个组）：

- 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

共用的 iPad 的特定要求如下：

- 每个设备组一个 ASM 帐户，并启用以下设置：
  - 要求注册设备
  - 受监督模式
  - 共享模式
- 对于指定的教育机构，请务必为所有 ASM 帐户使用相同的教育后缀。

要添加帐户，请转至设置 **> Apple** 部署计划。

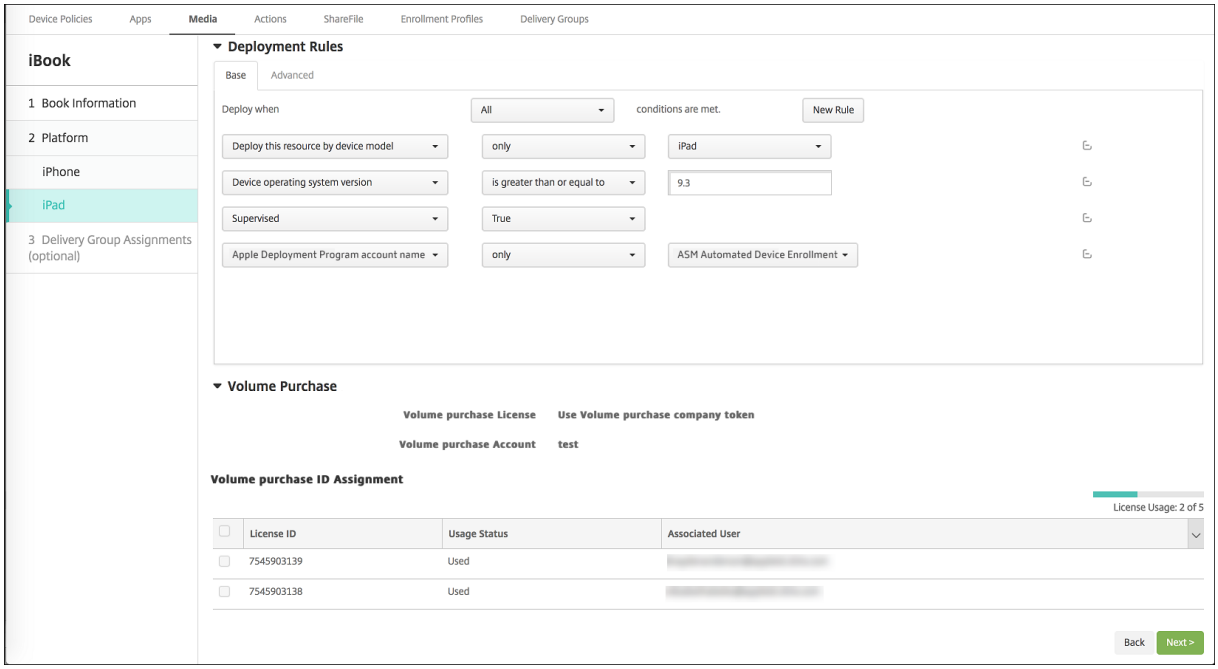


共用的 **iPad** 的应用程序

共用的 iPad 支持分配基于设备的批量购买应用程序。在共用的 iPad 上部署应用程序之前，XenMobile 将向 Apple 批量购买服务器发送一个请求以将批量购买许可证分配到设备。要检查批量购买分配，请转至配置 **>** 应用程序 **> iPad** 并展开批量购买。

共用的 **iPad** 的媒体

共用的 iPad 支持分配基于用户的批量购买 iBook。在共用的 iPad 上部署 iBook 之前，XenMobile 将向 Apple 批量购买服务器发送一个请求以将批量购买许可证分配给学生。要检查批量购买分配，请转至配置 **>** 媒体 **> iPad** 并展开批量购买。



共用的 **iPad** 的部署规则

对于共用的 iPad 部署，在交付组级别的规则不适用，应为这些规则与用户属性有关。要为每个设备组过滤策略、应用程序和媒体，请执行以下操作：根据帐户名称为资源添加部署规则。例如：

- 对于设备组 1 帐户，请设置此部署规则：

```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```

- 对于设备组 2 帐户，请设置此部署规则：

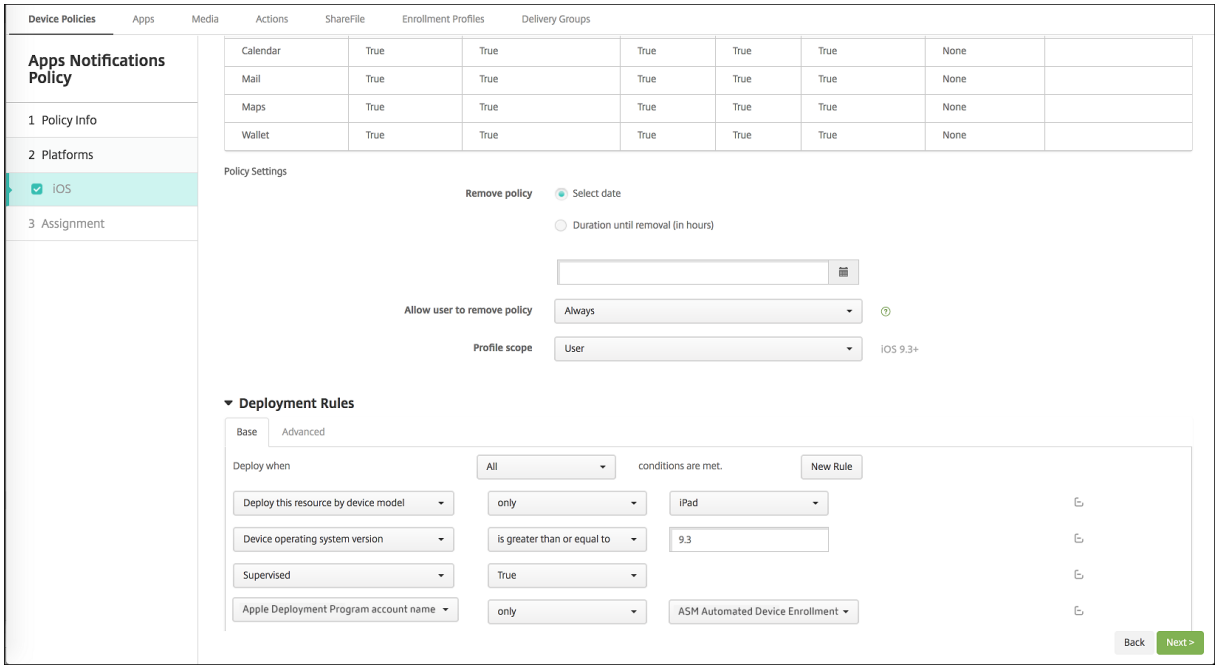
```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- 对于设备组 N 帐户，请设置此部署规则：

```
Apple Deployment Program account name
Only
Device Group N account

```



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

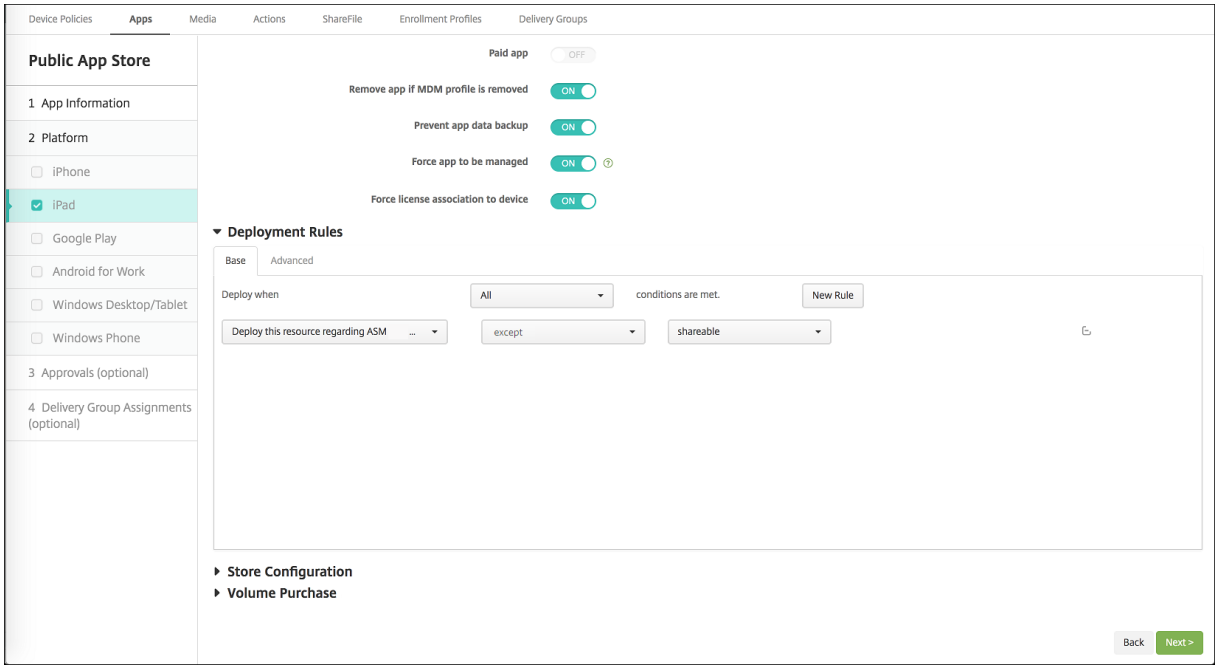


要仅对教师（使用非共用的 iPad）部署 Apple 课堂应用程序，请按 ASM 共享状态通过以下部署规则过滤资源：

```
Deploy this resource regarding ASM shared mode
only
unshared

<!--NeedCopy-->
```

或：

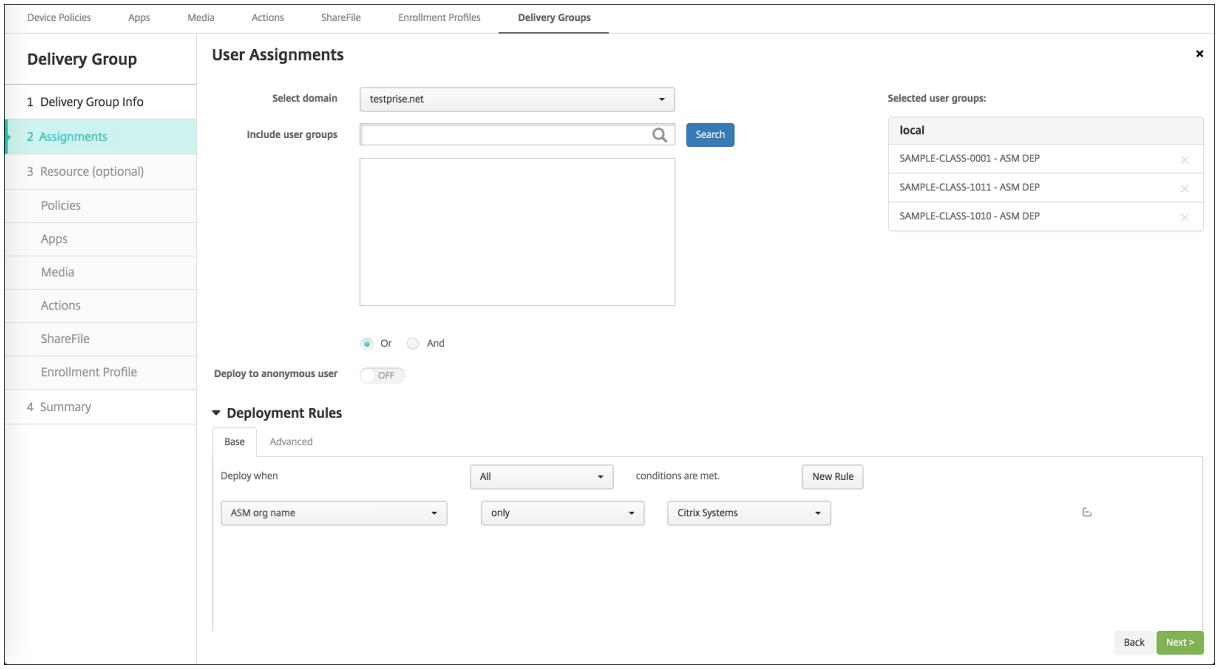
```
Deploy this resource regarding ASM shared mode
except
shareable

<!--NeedCopy-->
```

共用的 **iPad** 的交付组

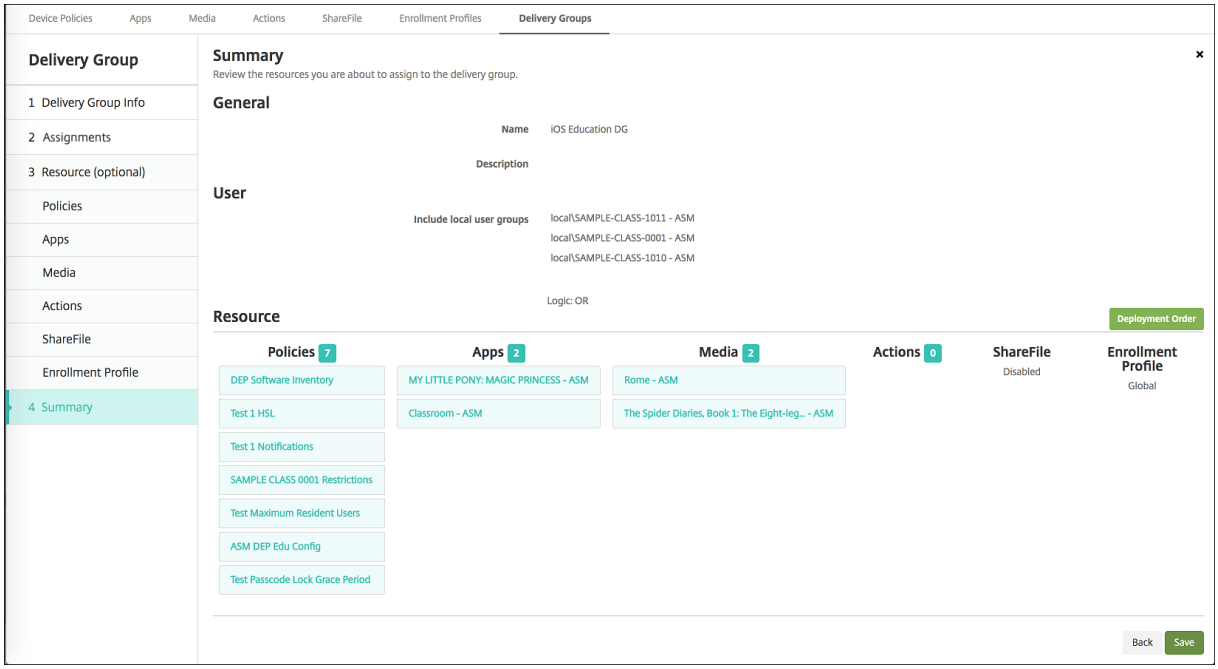
对于每个教师的每个设备组：

- 配置一个交付组。对于教师，请分配“教育配置”策略定义的所有班级。



- 该交付组必须包括以下 MDM 资源：
  - 设备策略：
    - 教育配置

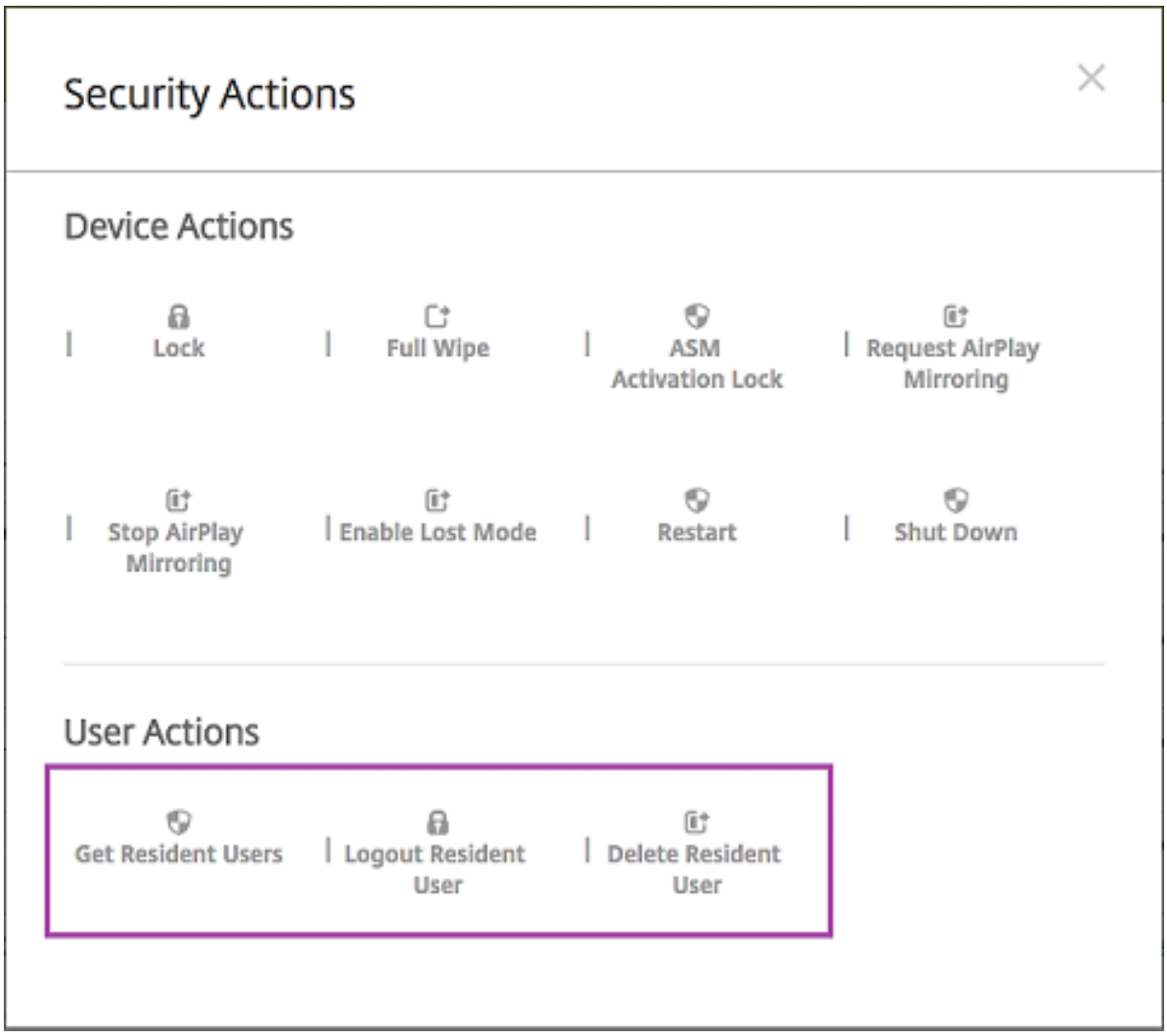
    * 锁屏界面消息
    * 应用程序通知
    * 主屏幕布局
    * 限制
    * 最大常驻用户数
    * 通行码锁宽限期
  - 必需的批量购买应用程序
  - 必须的批量购买 iBooks



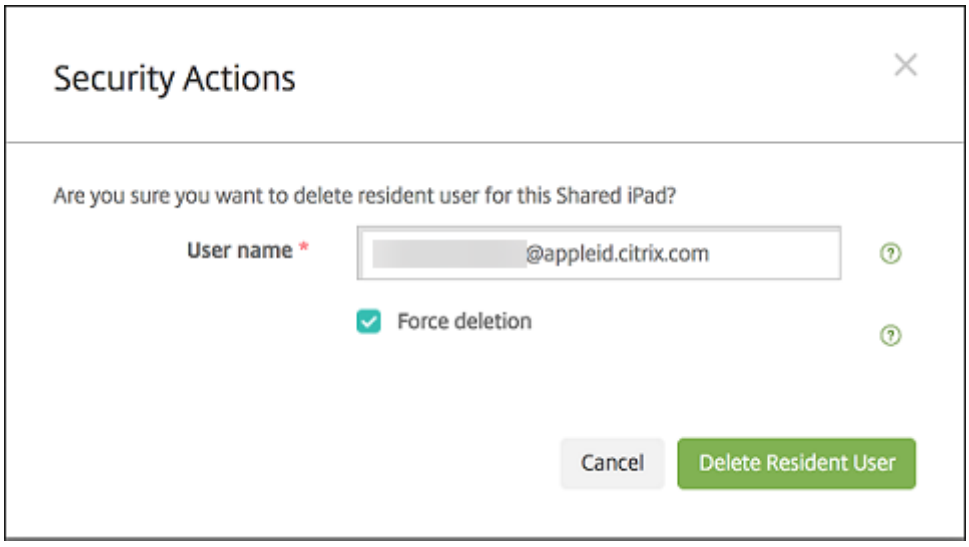
共用的 **iPad** 的安全操作

除现有安全操作外，可以对共用的 iPad 使用以下安全操作：

- 获取常驻用户：列出在当前设备上具有活动帐户的用户。此操作将强制在设备与 XenMobile 控制台之间进行同步。
- 注销常驻用户：强制注销当前用户。
- 删除常驻用户：删除特定用户的当前会话。该用户可以重新登录。



单击删除常驻用户后，可以指定用户名。

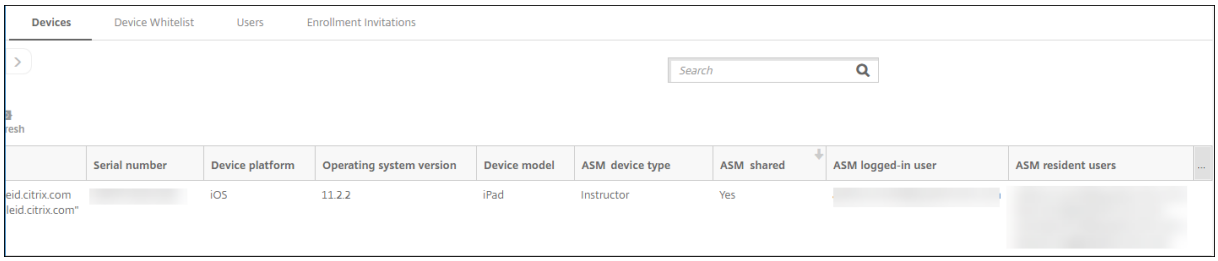


安全操作的结果在管理 > 设备 > 常规和管理 > 设备 > 交付组页面上显示。

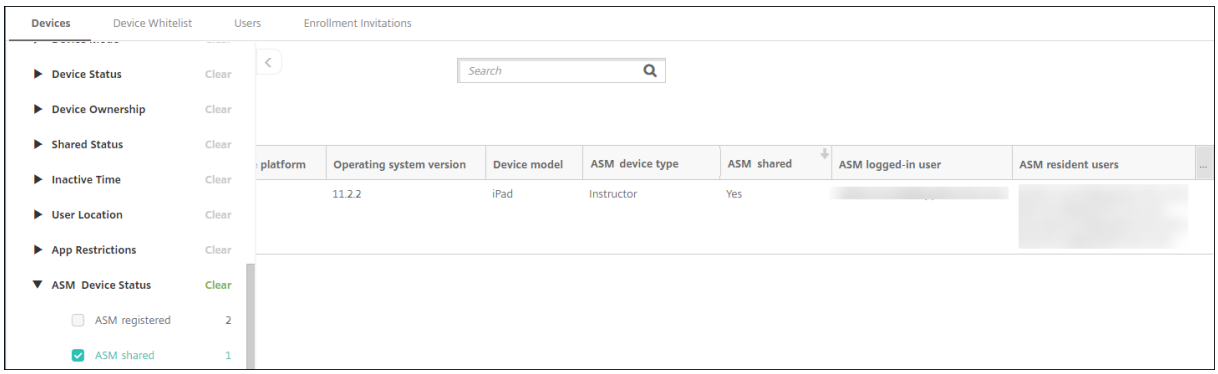
获取与共用的 iPad 有关的信息

请在管理 > 设备页面上查找共用的 iPad 特有的信息：

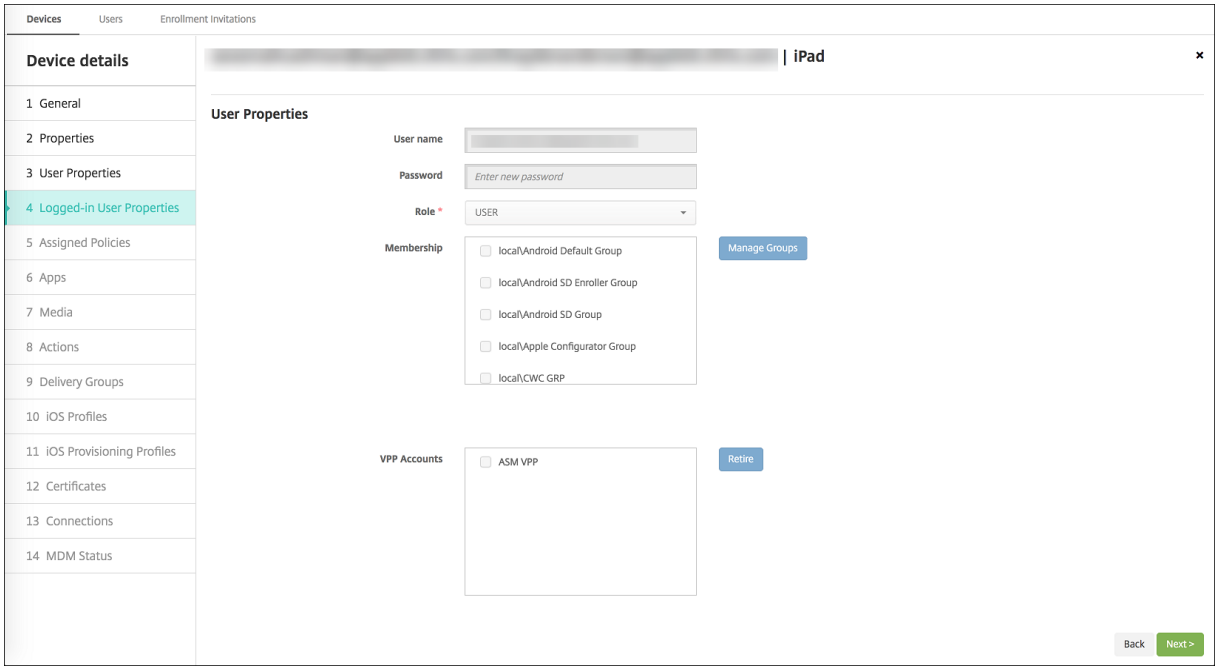
- 请查找：
  - 设备是否共用（**ASM** 共用）
  - 登录到共用设备的用户（已登录 **ASM** 的用户）
  - 分配给共用设备的所有用户（**ASM** 常驻用户）

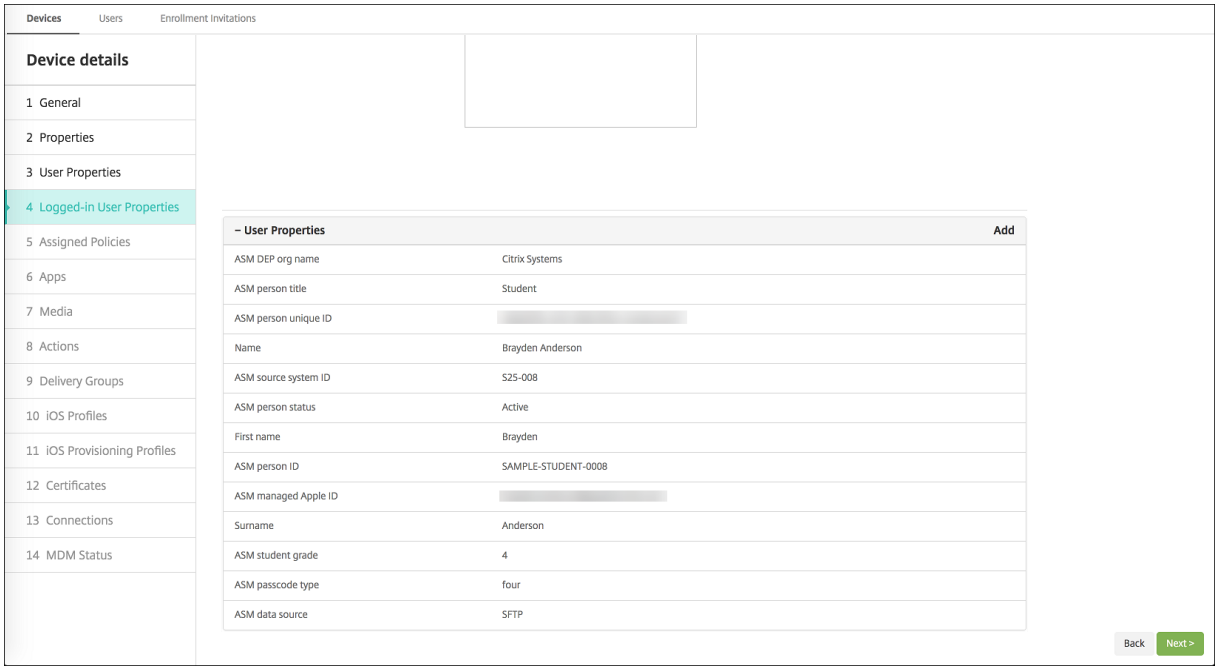


- 请按 **ASM** 设备状态过滤设备列表：

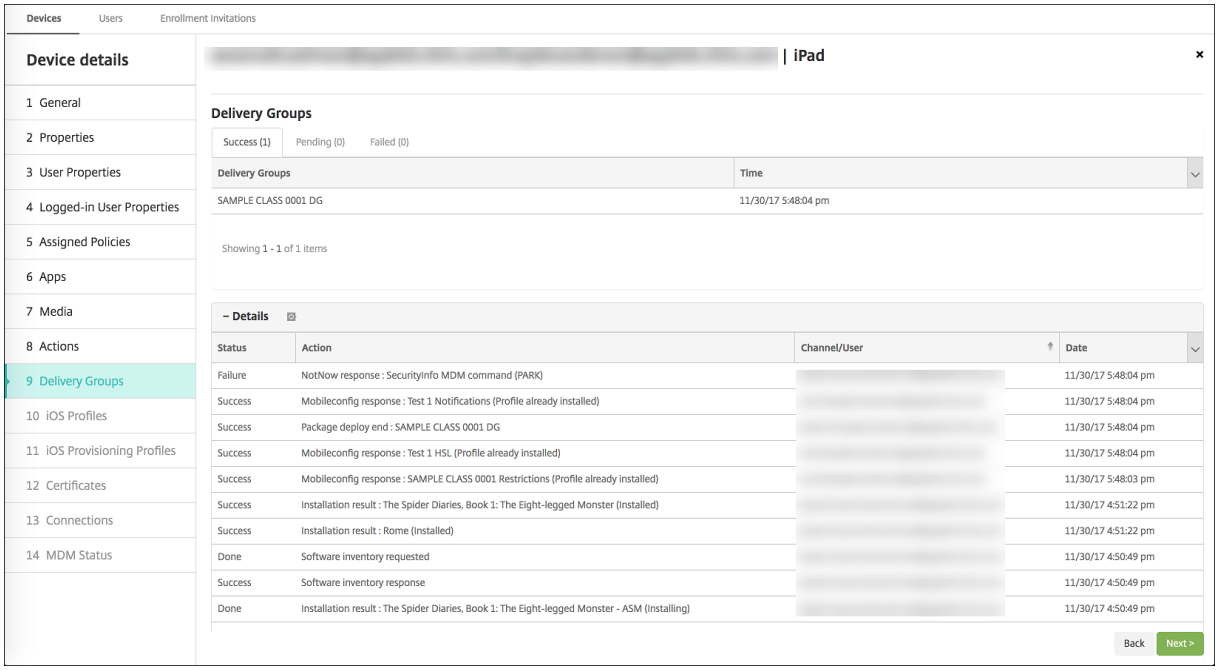


- 在管理 > 设备 > 已登录用户的属性页面上查看与登录到共用的 iPad 的用户有关的详细信息。

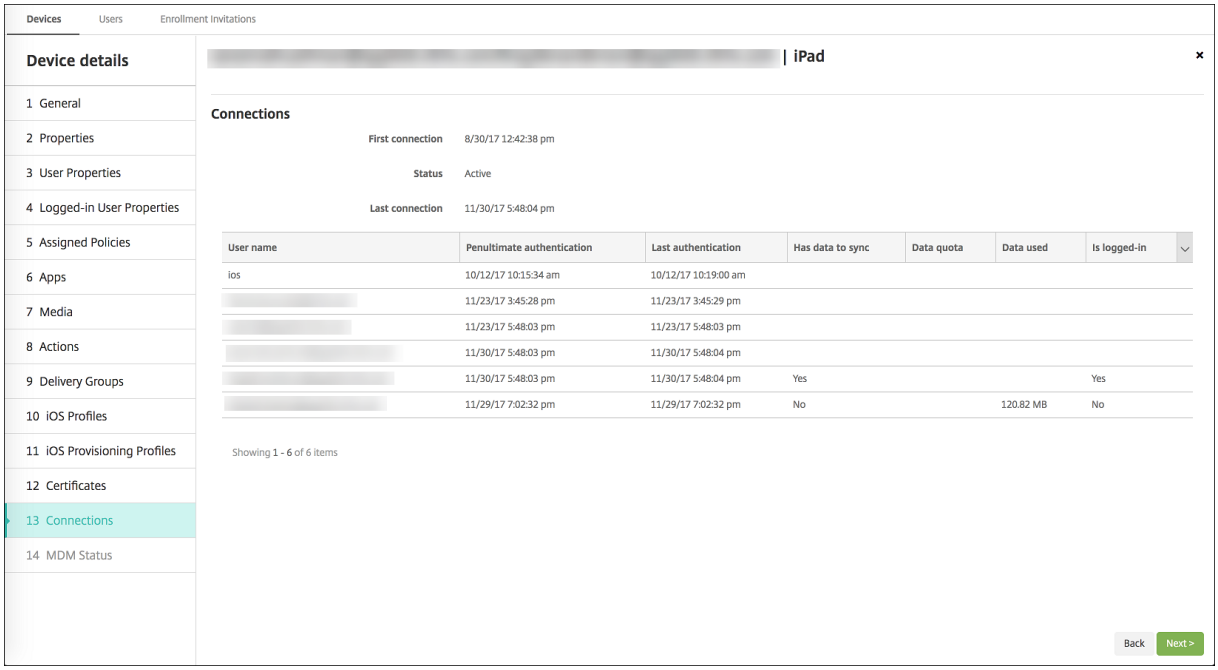




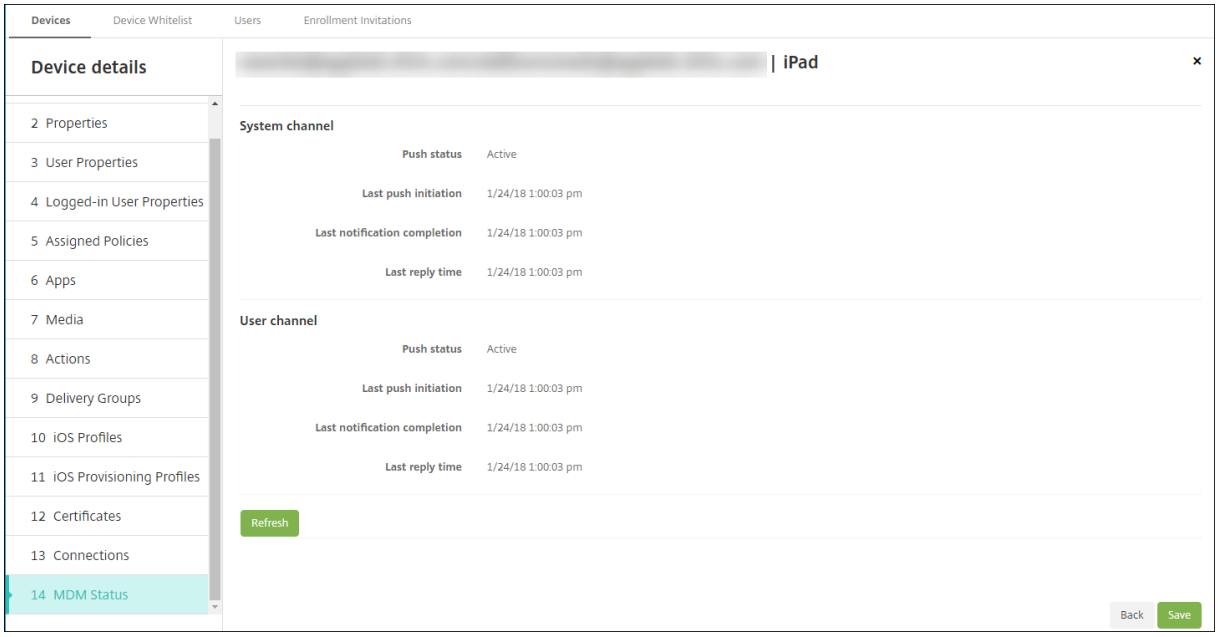
- 在管理 **>** 设备 **>** 交付组页面上查看用于向交付组中的教师和用户部署资源的通道。通道/用户列显示类型（系统或用户）和收件人（教师或学生）。



- 获取与常驻用户有关的信息：
  - 有要同步的数据：用户是否具有要同步到云的数据。
  - 数据配额：为用户设置的数据配额，单位为字节。如果用户配额暂时关闭或不强制对用户实施，配额可能不会显示。
  - 已使用的数据：用户使用的数据量，单位为字节。如果系统收集信息过程中出现错误，值可能不会显示。
  - 已登录：用户是否已登录设备。



- 查看两个通道的推送状态。



管理教师、学生和班级数据

管理教师、学生和班级数据时，请注意以下事项：

- 将 ASM 信息导入 XenMobile 后，请勿更改托管 Apple ID。XenMobile 还使用 ASM 用户标识符来识别用户。
- 如果您在创建一个或多个“教育配置”设备策略后在 ASM 中添加或更改了班级数据，请编辑策略，然后重新部署这些策略。
- 如果班级的教师在您部署教育配置设备策略后发生了变化，请检查策略以确保其在 XenMobile 控制台进行了更新，然后重新部署该策略。
- 如果您在 ASM 门户中更新了用户属性，XenMobile 还将在控制台中更新这些属性。但是，XenMobile 不通过与接收其他属性相同的方式接收 ASM 人员职务属性，即“教师”、“学生”或“其他”。因此，如果您在 ASM 中更改了 ASM 人员职务，请完成以下步骤以在 XenMobile 中反映该更改。

要管理数据，请执行以下操作：

1. 在 ASM 门户中，更新学生年级并清除教师年级。
2. 如果您将学生帐户更改为教师帐户，请将该用户从班级中的学生列表中删除。然后，将该用户添加到同一班级或其他班级中的教师列表中。

   如果您将教师帐户更改为学生帐户，请将该用户从班级中删除。然后，将该用户添加到同一班级或其他班级中的学生列表中。您的更新将在下次同步时在 XenMobile 控制台中显示（默认时间间隔为每隔 5 分钟）或提取（默认时间间隔为每隔 24 小时）。
3. 编辑教育配置设备策略以应用更改并重新部署。
   - 如果您从 ASM 门户中删除了某个用户，XenMobile 也将在提取后从 XenMobile 控制台中删除该用户。

可以通过更改以下服务器属性值来缩短两个基线之间的时间间隔：**bulk.enrollment.fetchRosterInfoDelay**（默认值为 **1440** 分钟）。

- 部署资源后：如果学生加入了某个班级，请创建仅包含该学生的交付组，并为该学生部署资源。
- 如果某个学生或教师丢失了临时密码，请其联系 ASM 管理员。管理员可以提供临时密码或生成一个新密码。

管理在 **Apple** 校园教务管理 **Apple** 部署计划中注册的丢失或被盗设备

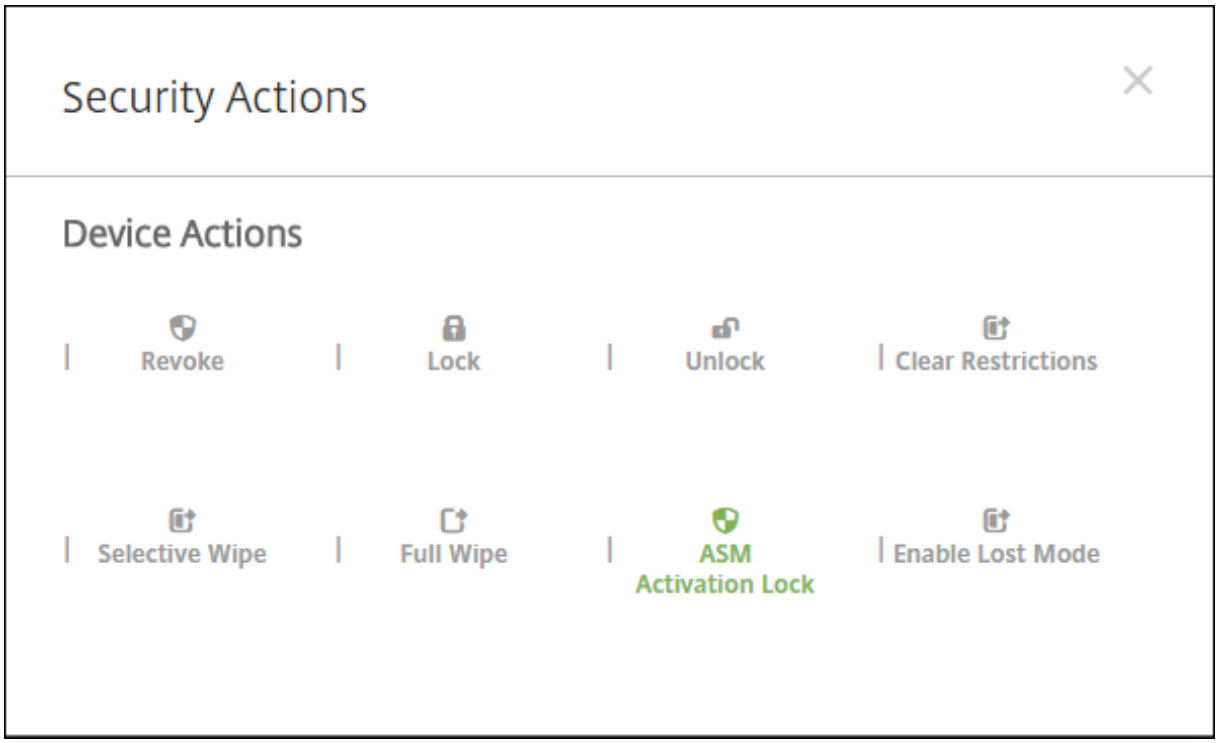
Apple 的“查找我的 iPhone/iPad”服务包括激活锁功能。激活锁可防止未授权的用户使用或转售在 Apple 部署计划中注册的丢失或被盗设备。

XenMobile 包括 **ASM** 激活锁安全操作，使您能够将锁定代码发送到已注册 ASM Apple 部署计划的设备。

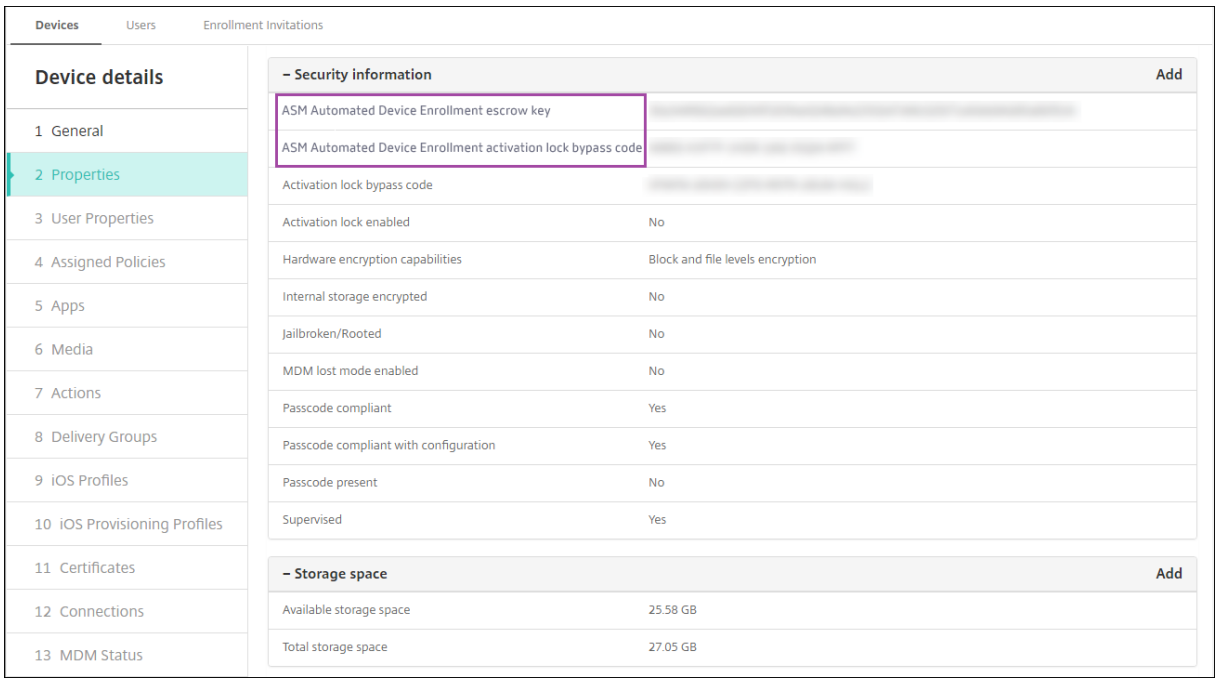
使用 **ASM** 激活锁安全操作时，XenMobile 不需要用户启用“查找我的 iPhone/iPad”服务即可定位设备。ASM 设备被硬重置或完全擦除后，用户需要提供其管理式 Apple ID 和密码才能解锁该设备。

要从控制台中释放锁定，请单击安全操作激活锁绕过。有关绕过激活锁的信息，请参阅绕过 iOS 激活锁。用户还可以将登录保留为空，并键入 **ASM** 激活锁绕过码作为密码。该信息在属性选项卡上的设备详细信息中提供。

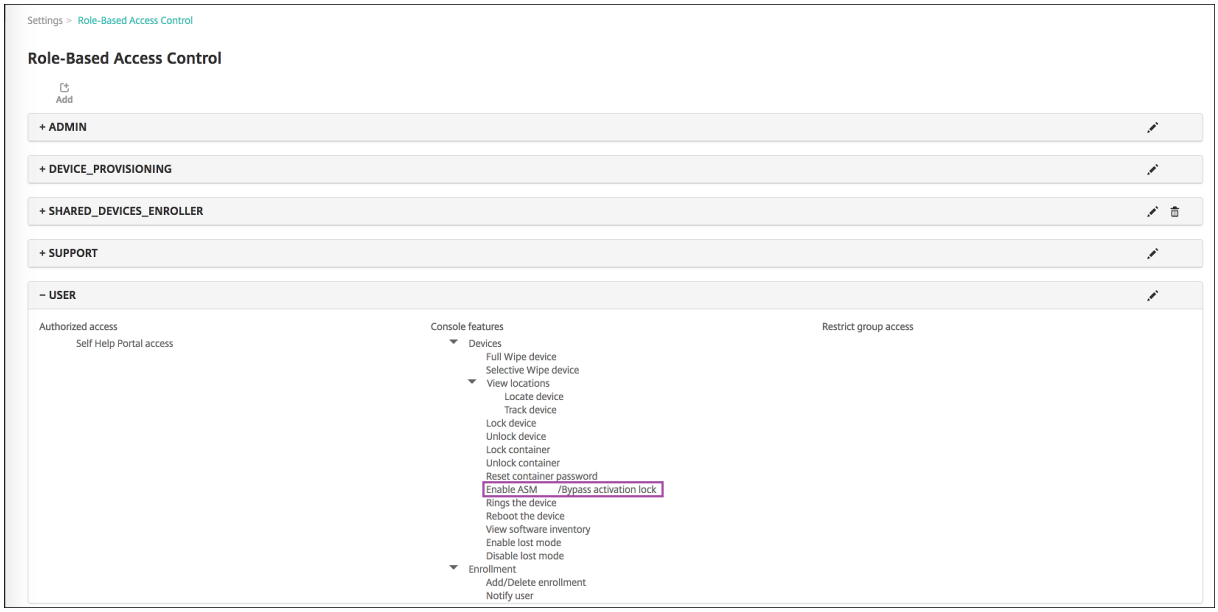
要设置激活锁，请转至管理 **>** 设备，选择设备，单击安全性，然后单击 **ASM** 激活锁。



属性 **ASM** 托管密钥和 **ASM** 激活锁绕过码显示在设备详细信息中。



ASM 激活锁的 RBAC 权限为设备 **>** 启用 **ASM** 绕过激活锁。



分发 **Apple** 应用程序

January 5, 2022

XenMobile 管理部署到设备的应用程序。您可以组织和部署以下类型的 iOS/iPadOS 和 macOS 应用程序。

- 公共应用商店 **(**仅限 **iOS/iPadOS)**：这些应用程序包括公共应用商店（例如 Apple App Store 或 Google

Play）中提供的免费或付费应用程序。例如，GoToMeeting。

- 企业 **(iOS/iPadOS/macOS)**：未启用 MDX 且不包含与 MDX 应用程序关联的策略的本机应用程序。
- **MDX (**仅限 **iOS/iPadOS)**：使用 MAM SDK 准备的应用程序或使用 MDX Toolkit 封装的应用程序。这些应用程序包括 MDX 策略。您可以从内部来源和公共应用商店获取 MDX 应用程序。
- 批量购买 **(iOS/iPadOS/macOS)**：具有通过 Apple 批量购买计划管理的许可证的应用程序。
- **iOS** 自定义应用程序 **(**仅限 **iOS/iPadOS)**：在内部或第三方开发的专有企业对企业应用程序。

有关不同类型的应用程序的详细信息，请参阅添加应用程序。

某些部署需要 Apple 商务管理 (ABM) 或 Apple 校园教务管理 (ASM) 帐户。有关详细信息，请参阅以下部分。

对于每种类型的应用程序和分发方法，Citrix 建议采用一组配置实践。有关为其他平台分发应用程序的信息，请参阅添加应用程序。以下各部分内容提供了有关 iOS 应用程序配置的详细信息。

应用程序分发的一般步骤

场景	步骤 1：链接帐户	步骤 2：添加和配置应用程序	步骤 3：配置交付组并部署应用程序
公共应用商店应用程序，包括 Citrix 移动应用程序	不适用	在 **XenMobile** 中：在配置 **>** 应用程序中，添加适用于 iPhone 或 iPad 的公共应用商店应用程序。配置应用程序并将其分配给交付组。	在 **XenMobile** 中：使用交付组配置和部署应用程序。
通过 Apple 批量购买提供的公共应用商店应用程序，包括 Citrix 移动应用程序	在 Apple 部署计划中注册在 **XenMobile** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 或 **ASM** 中：从“应用程序”和“书籍”购买和添加应用程序。在 **XenMobile** 中：转到配置 **>** 应用程序，配置应用程序，然后将其分配给交付组。	在 **XenMobile** 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 **XenMobile** 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 **XenMobile** 中：使用交付组配置和部署应用程序。

场景	步骤 1：链接帐户	步骤 2：添加和配置应用程序	步骤 3：配置交付组并部署应用程序
MDX 应用程序	不适用	在 **XenMobile** 中：转到配置 **>** 应用程序。单击添加，然后单击 **MDX**。确保您为平台选择了 **iPad**/**iPhone**。上载 MDX 文件。配置应用程序并将其分配给交付组。	在 **XenMobile** 中：使用交付组配置和部署应用程序。
使用 Apple 批量购买分发的 MDX 应用程序	在 Apple 部署计划中注册在 **XenMobile** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 中：从“应用程序”和“书籍”购买和添加 MDX 应用程序。将应用程序链接到您的 ABM 帐户。在 **XenMobile** 中：转到配置 **>** 应用程序，配置应用程序，然后将其分配给交付组。	在 **XenMobile** 中：使用交付组配置和部署应用程序。
自定义应用程序	在 Apple 部署计划中注册在 **XenMobile** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 中：将您的应用程序作为私人应用程序添加到应用商店中。请将应用程序链接到您的 ABM 帐户。在 **XenMobile** 中：转到配置 **>** 应用程序，配置应用程序，然后将其分配给交付组。	在 **XenMobile** 中：使用交付组配置和部署应用程序。
启用了 MDX 的自定义应用程序	在 Apple 部署计划中注册在 **XenMobile** 中：转到设置 **>** 批量购买以添加批量购买帐户。	在 **ABM** 中：将您的应用程序作为私人应用程序添加到应用商店中。请将应用程序链接到您的 ABM 帐户。在 **XenMobile** 中：转到配置 **>** 应用程序并上载 MDX 文件。配置应用程序并将其分配给交付组。	在 **XenMobile** 中：使用交付组配置和部署应用程序。

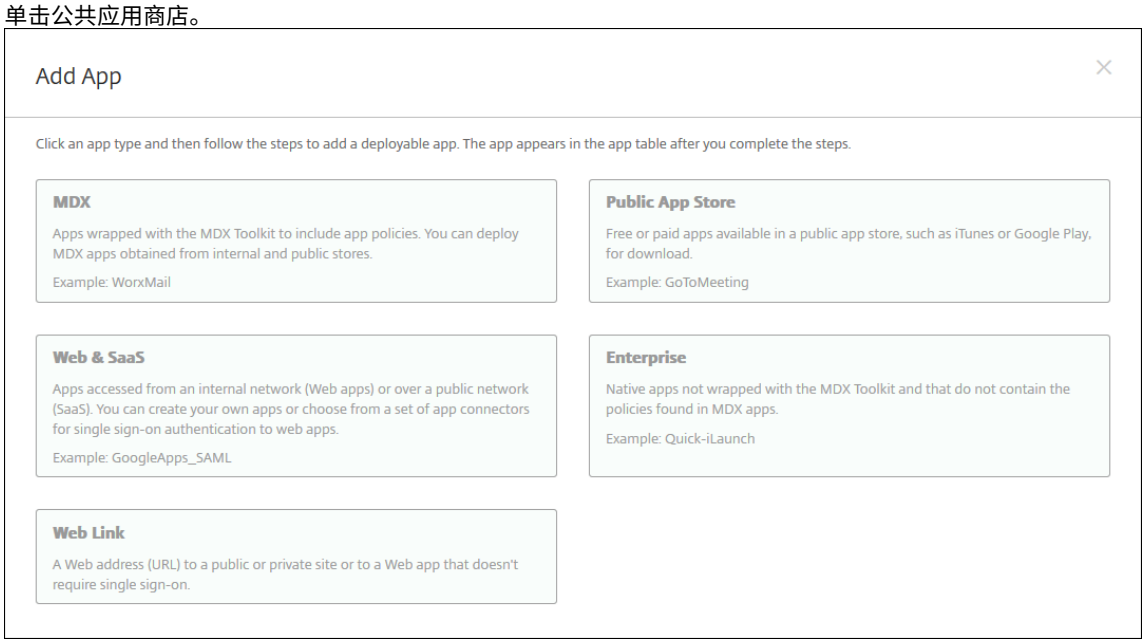
公共应用商店应用程序

可以将 App Store 中提供的免费和付费应用程序添加到 XenMobile 中。

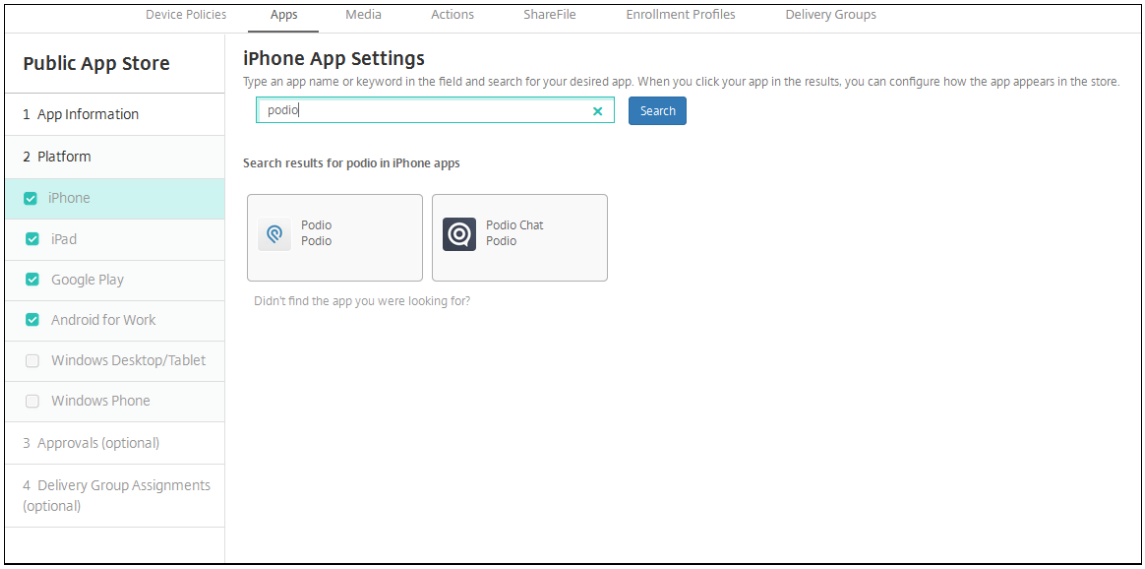
功能可用性	
需要监督设备	否
适用于用户注册模式	否
有效日期	iOS/iPadOS

步骤 **1**：添加和配置应用程序

1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击公共应用商店。



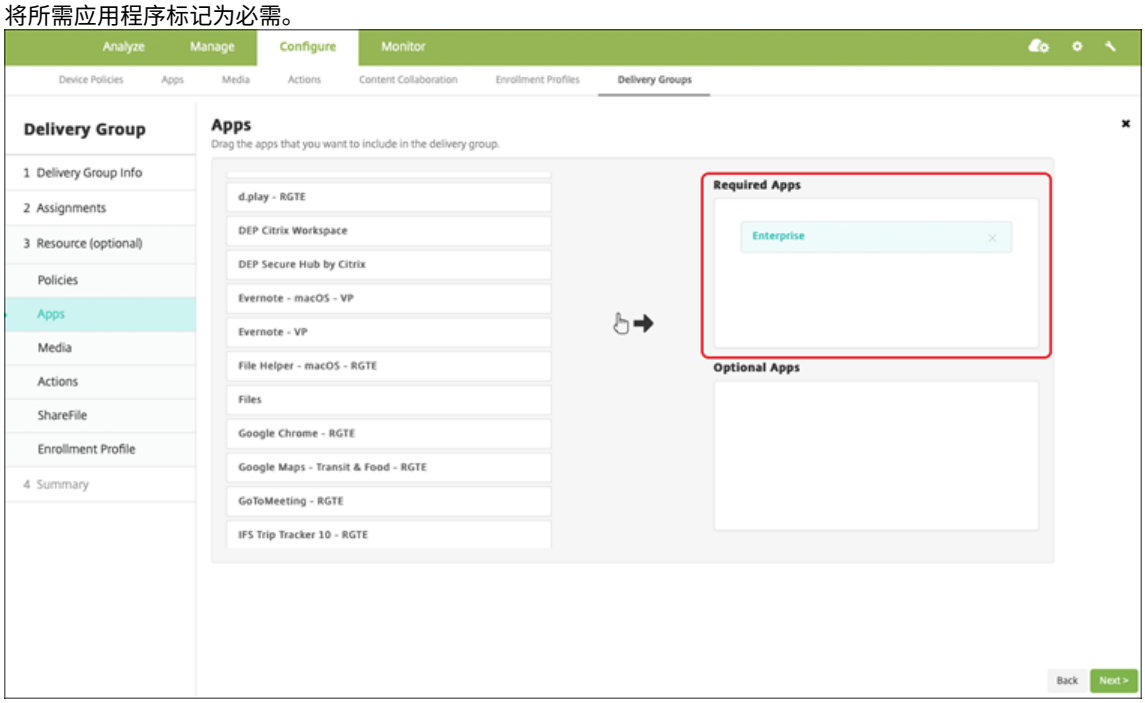
3. 为平台选择 **iPhone** 或 **iPad**
4. 在搜索框中键入应用程序名称，然后单击搜索。



5. 此时将显示符合搜索条件的应用程序。单击所需的应用程序。
6. 将交付组分配给应用程序，然后单击保存。

步骤 **2**：配置应用程序部署

1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。
2. 选择要配置的应用程序，然后单击编辑。
3. Citrix 建议启用强制管理应用程序功能。
4. 分配任何交付组，然后单击保存。
5. 导航到配置 **>** 交付组 **>** 应用程序。
6. 将所需应用程序标记为必需。



7. 导航回配置 **>** 交付组。
8. 选择交付组并单击部署。
9. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

通过 **Apple** 批量购买提供的公共应用商店应用程序

可以通过 Apple 批量购买计划管理 iOS/iPadOS 应用程序许可证。请按照以下步骤将批量购买应用程序添加到 XenMobile。

功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS/macOS

步骤 **1**：链接帐户

1. 设置 Apple 商务管理 (ABM) 或 Apple 校园教务管理 (ASM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 XenMobile 相关联。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。

3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应用程序会自动更新。

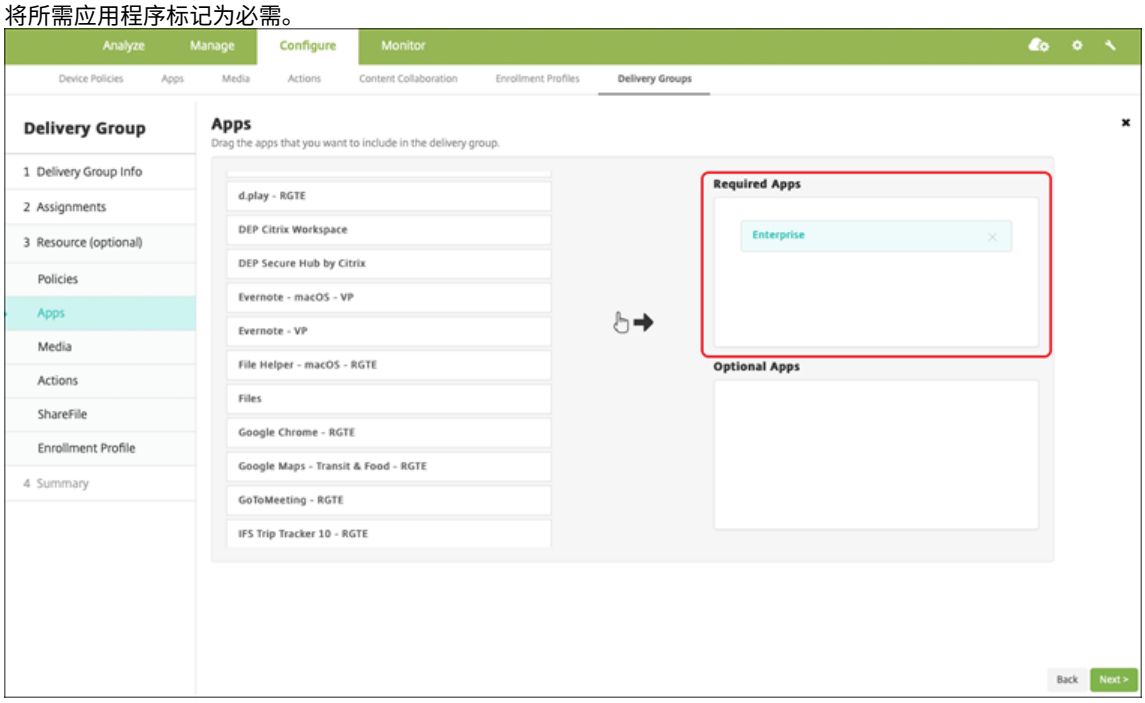
步骤 **2**：从 **Apple** 获取应用程序和许可证

在您的 ABM/ASM 帐户中添加应用程序。可以从 Apple App Store 或 Apple 书籍添加购买内容（仅限 iOS/iPadOS）。请记住，您必须购买所有应用程序，即使它们是免费的亦如此。

有关如何使应用程序可供您的企业使用的信息，请参阅 Apple 文档。

步骤 **3**：配置应用程序部署

1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。
2. 选择要配置的批量购买应用程序，然后单击编辑。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. Citrix 建议启用强制管理应用程序功能（仅限 iOS/iPadOS）。
5. 分配任何交付组，然后单击保存。
6. 导航到配置 **>** 交付组 **>** 应用程序。
7. 将所需应用程序标记为必需。



8. 导航回配置 **>** 交付组。
9. 选择交付组并单击部署。
10. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

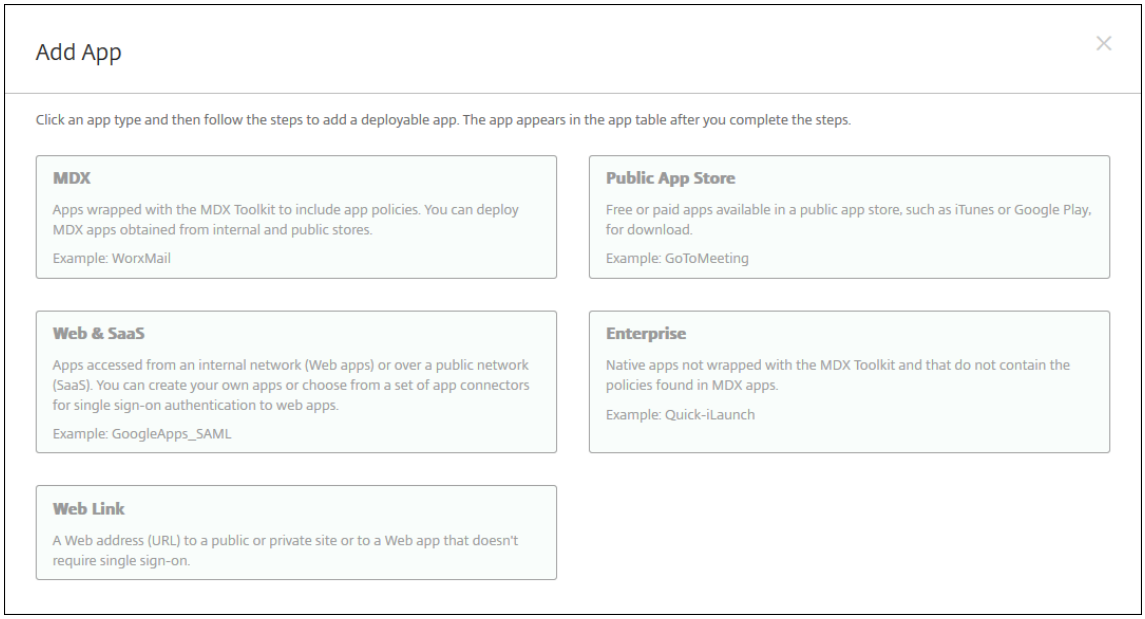
企业应用程序

还可以添加没有关联任何 MDX 策略的本机应用程序。请按照以下步骤添加 App Store 上不存在的应用程序。

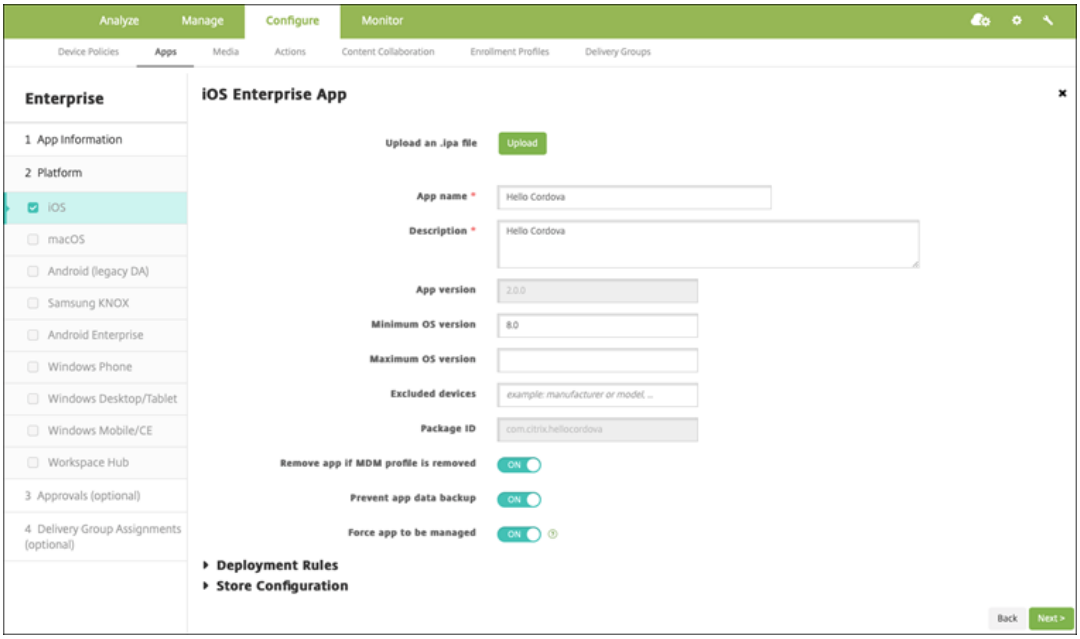
功能可用性	
需要监督设备	否
适用于用户注册模式	是
操作系统	iOS/iPadOS/macOS

步骤 **1**：添加和配置应用程序

1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击企业。



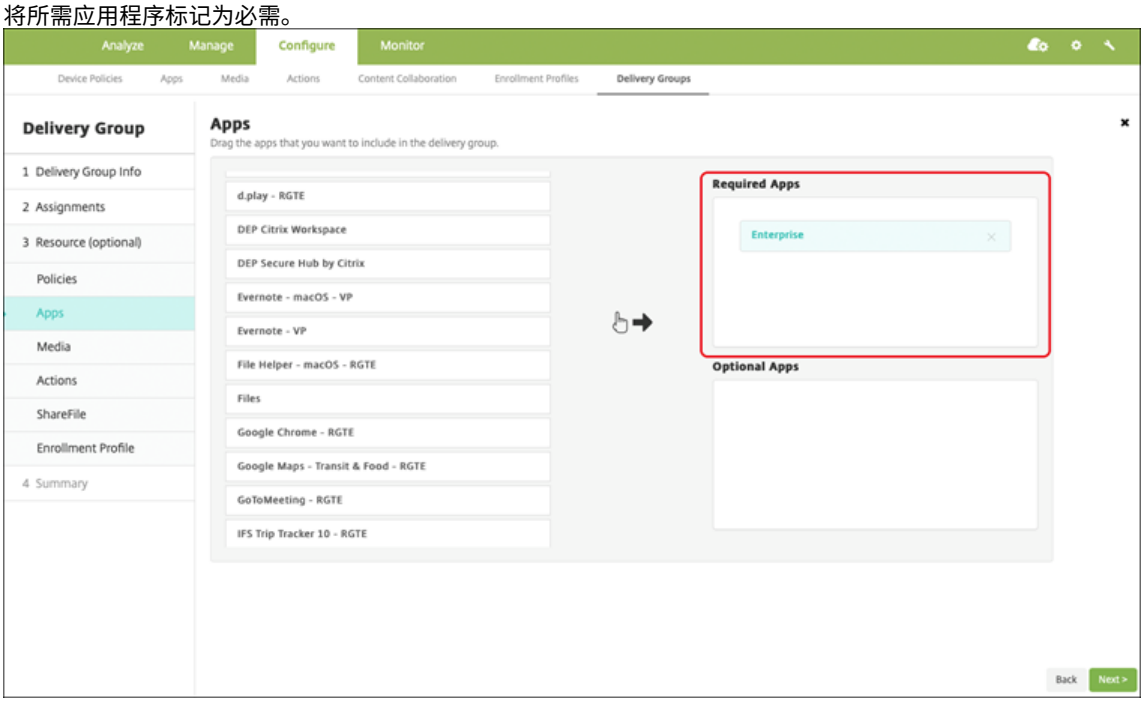
3. 在应用程序信息页面上，配置以下设置：
   - 名称：键入应用程序的描述性名称。该名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中，单击要将应用程序添加到的类别。
4. 单击 **Next**（下一步）。此时将显示应用程序平台页面。
5. 选择平台：**iPhone**、**iPad** 或 **macOS**。
6. 上载 IPA 文件 (iOS/iPadOS) 或上载 PKG 文件 (macOS)
7. 单击 **Next**（下一步）。此时将显示应用程序详细信息页面。
8. 配置以下设置：
   - 文件名：（可选）键入应用程序的新名称。
   - 应用程序说明：（可选）键入应用程序的新说明。
   - 应用程序版本：无法更改此字段。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
   - 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否从设备中删除应用程序。默认值为“开”。（仅限 iOS/iPadOS）
   - 阻止备份应用程序数据：选择是否阻止应用程序备份数据。默认值为“开”。（仅限 iOS/iPadOS）
   - 强制管理应用程序：安装非托管应用程序时，如果希望不受监督设备上的用户看到允许管理应用程序的提示，请选择开。如果用户接受提示，则将托管应用程序。（仅限 iOS/iPadOS）



9. 将交付组分配给应用程序，然后单击保存。

步骤 **2**：配置应用程序部署

1. 在 XenMobile 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. 将所需应用程序标记为必需。



3. 导航到配置 **>** 交付组。
4. 选择交付组并单击部署。
5. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

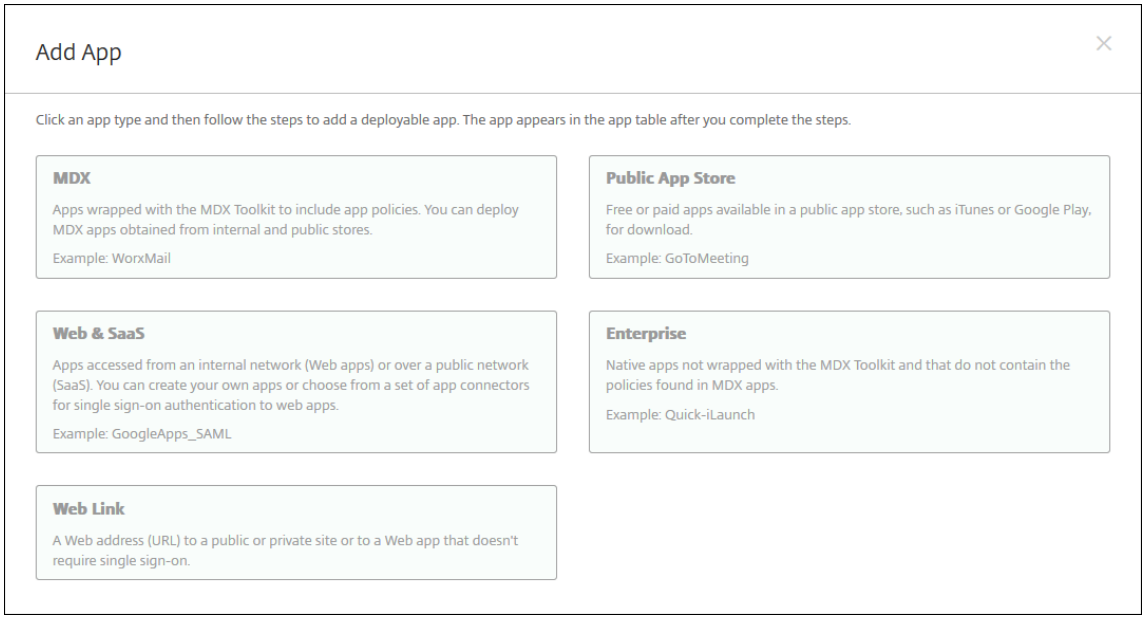
MDX 应用程序

要使用 MDX 策略和安全功能，请添加启用了 MAM SDK 或 MDX 封装的应用程序。可以使用批量购买或不使用批量购买来部署 MDX 应用程序。

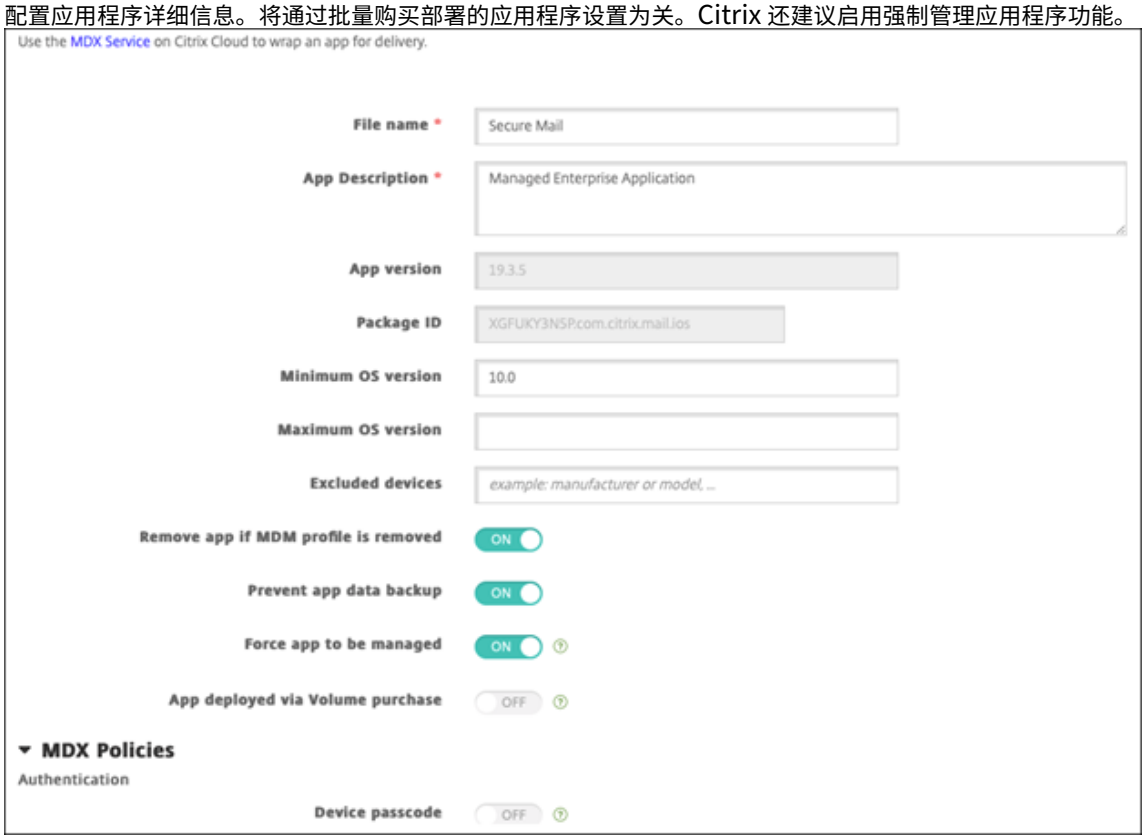
功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

步骤 **1**：添加和配置应用程序

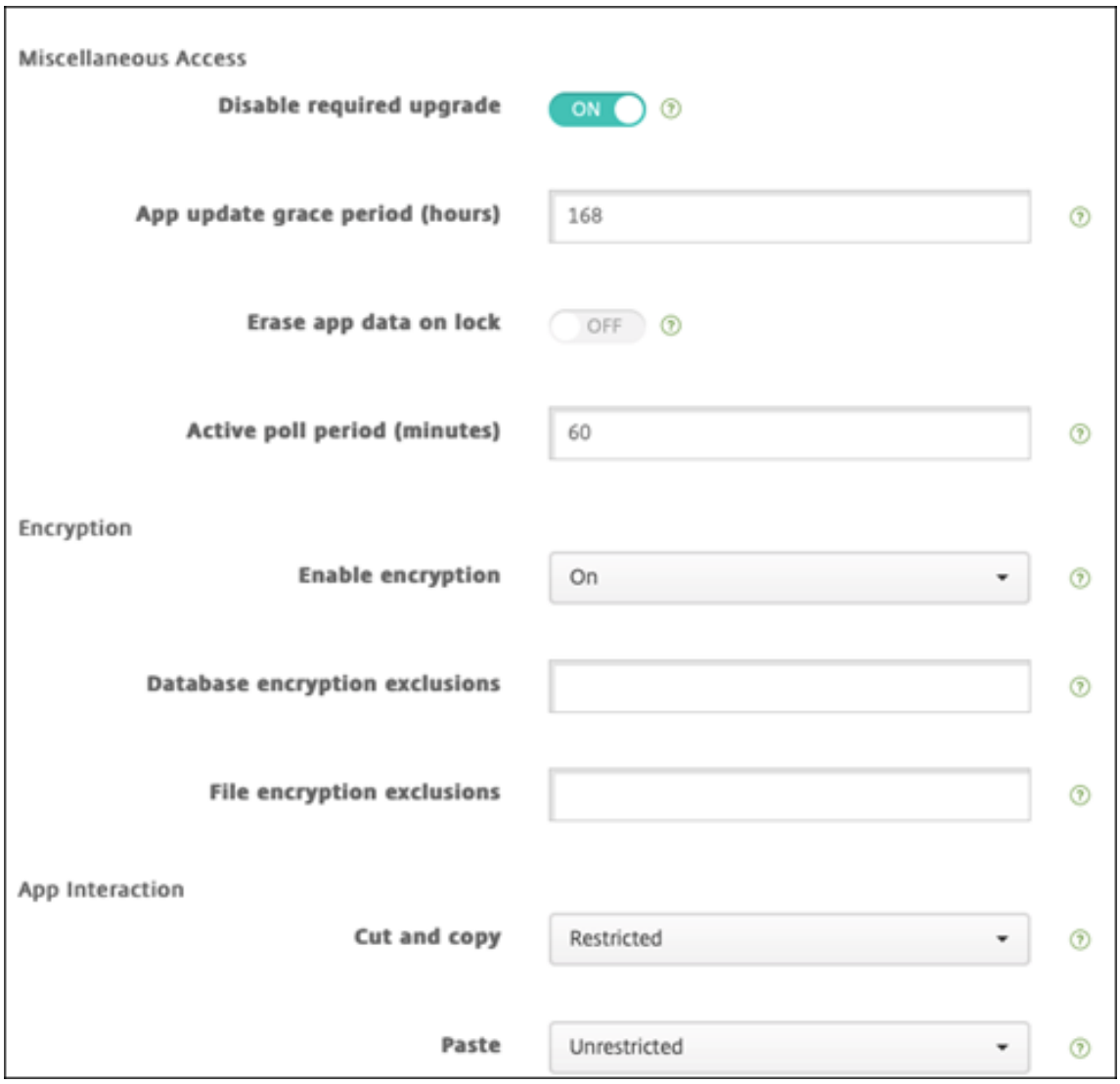
1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击 **MDX**。



3. 为平台选择 **iPhone** 或 **iPad**。
4. 上载 MDX 文件。
5. 配置应用程序详细信息。将通过批量购买部署的应用程序设置为关。Citrix 还建议启用强制管理应用程序功能。



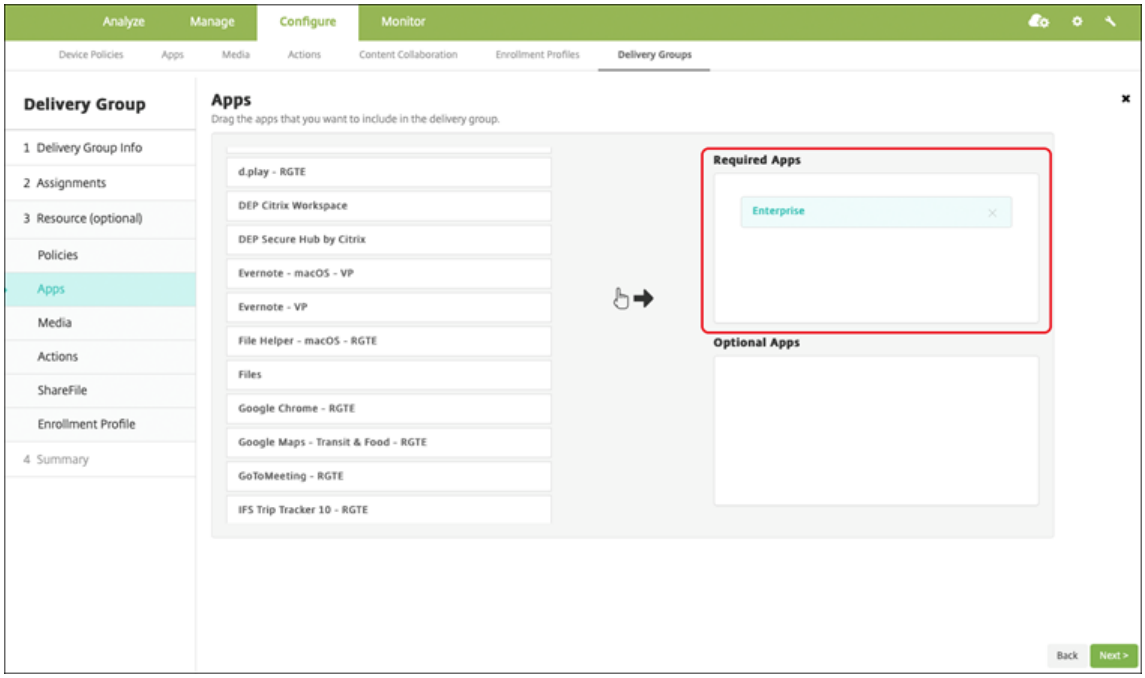
6. 配置 MDX 策略。将禁用所需的升级设置为开。



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 XenMobile 控制台中，导航到配置 **>** 交付组 **>** 应用程序。
2. 将所需应用程序标记为必需。



3. 导航到配置 **>** 交付组。
4. 选择交付组并单击部署。
5. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

使用 **Apple** 批量购买分发的 **MDX** 应用程序

要使用 MDX 策略和安全功能，请添加启用了 MAM SDK 或 MDX 封装的应用程序。要使用批量购买部署应用程序，这些应用程序必须存在于应用商店中。

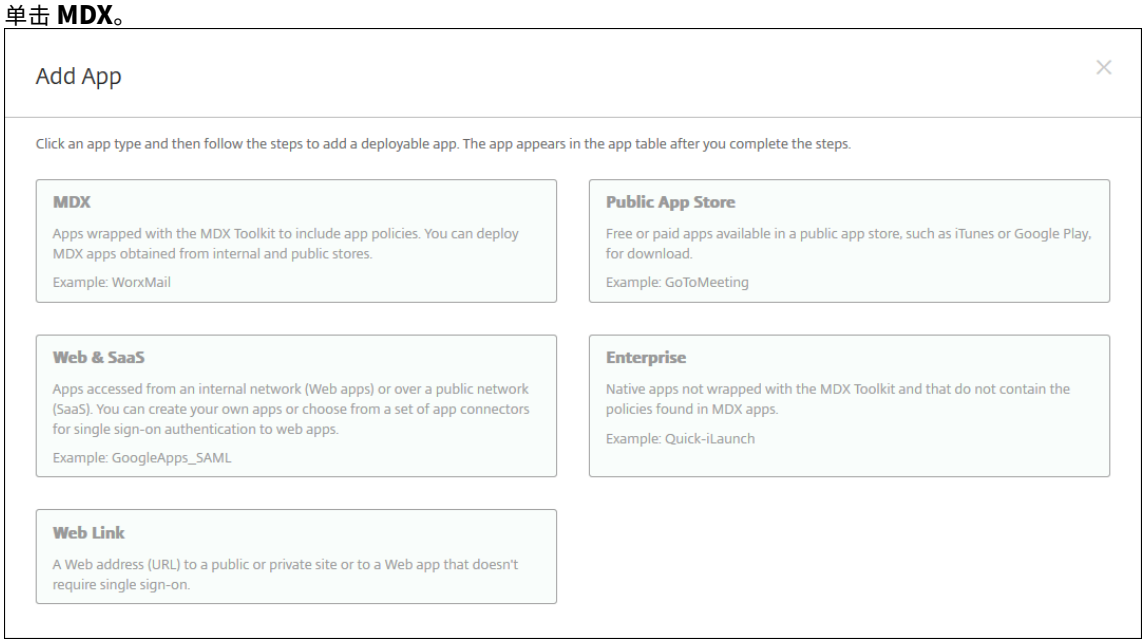
功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

步骤 **1**：链接帐户

1. 设置 Apple 商务管理 (ABM) 或 Apple 校园教务管理 (ASM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 XenMobile 相关联。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应用程序会自动更新。

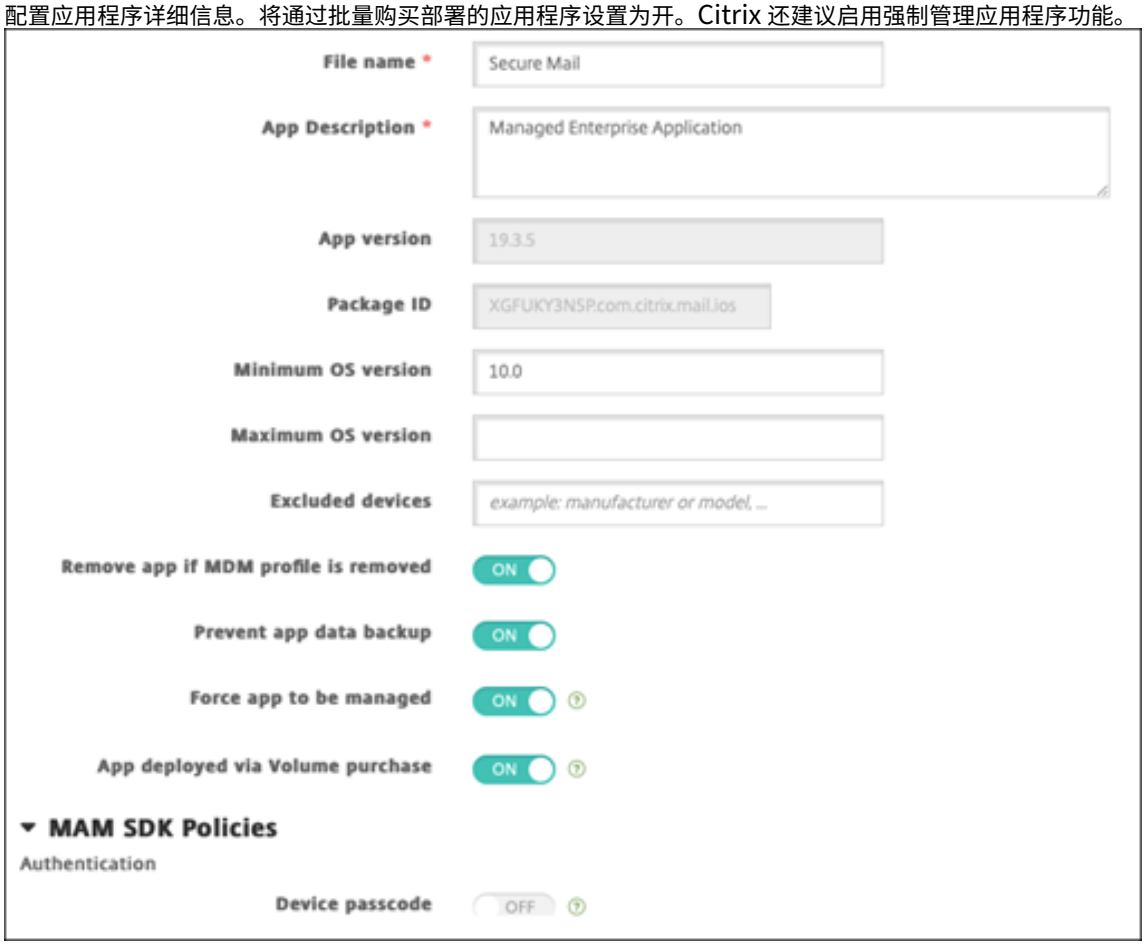
步骤 **2**：添加和配置应用程序

1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击 **MDX**。

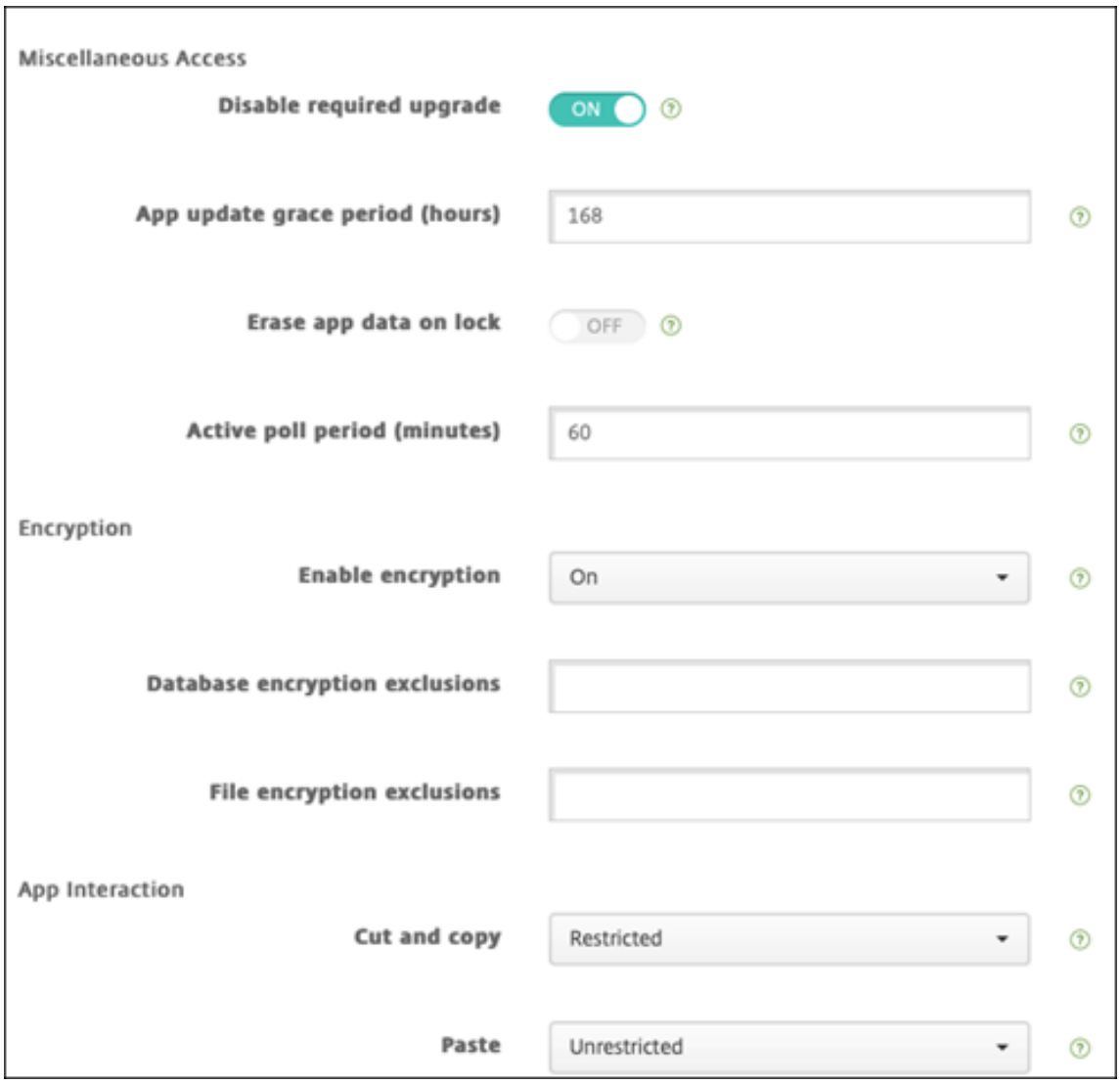


3. 为平台选择 **iPhone** 或 **iPad**。
4. 上载 MDX 文件。

5. 配置应用程序详细信息。将通过批量购买部署的应用程序设置为开。Citrix 还建议启用强制管理应用程序功能。



6. 配置 MDX 策略。将禁用所需的升级设置为开。

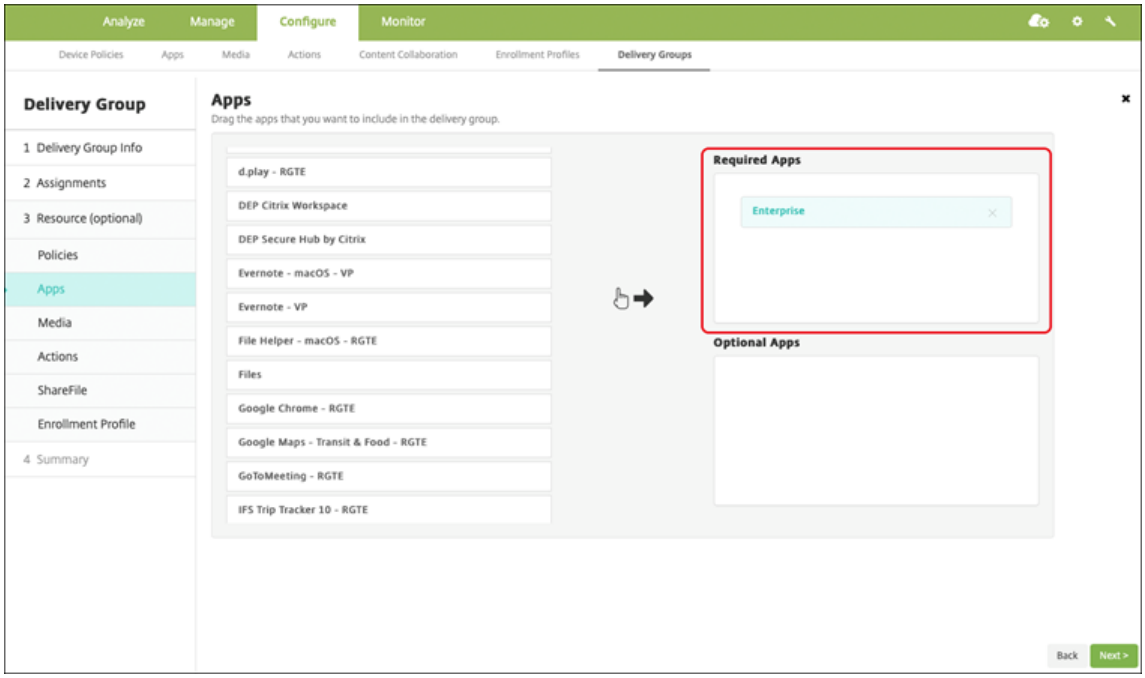


7. 将交付组分配给每个平台的应用程序，然后单击保存。

此配置将导致在应用程序列表中为此应用程序列出两个条目。选择要配置的应用程序时，请选择类型为 **MDX** 的应用程序。

步骤 **3**：配置应用程序部署

1. 在 XenMobile 控制台中，导航到配置 **>** 交付组 **>** 应用程序。
2. 将所需的批量购买应用程序标记为必需。



3. 导航到配置 **>** 交付组。
4. 选择交付组并单击部署。
5. 用户收到安装应用程序的请求，并在用户接受后在后台安装应用程序。

自定义应用程序

自定义应用程序是专有的企业对企业应用程序。可以使用 XenMobile 和 Apple 批量购买来私下安全地分发专有应用程序。可以将应用程序分发给特定的合作伙伴、客户、特许经营商和内部员工。

功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

自定义应用程序的要求

- Apple 商务管理或 Apple 校园教务管理帐户
- Apple 批量购买帐户（需要安装了 iOS 7 或更高版本的设备）
- 使用以下 Apple 注册模式之一在 XenMobile 中注册设备：
  - 自动化设备注册
  - 设备注册
  - 用户注册

步骤 **1**：链接帐户

要使用批量购买部署自定义应用程序，请将批量购买帐户链接到 XenMobile。

1. 设置 Apple 商务管理 (ABM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 XenMobile 相关联。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应用程序会自动更新。

步骤 **2**：在 **ABM** 上配置应用程序

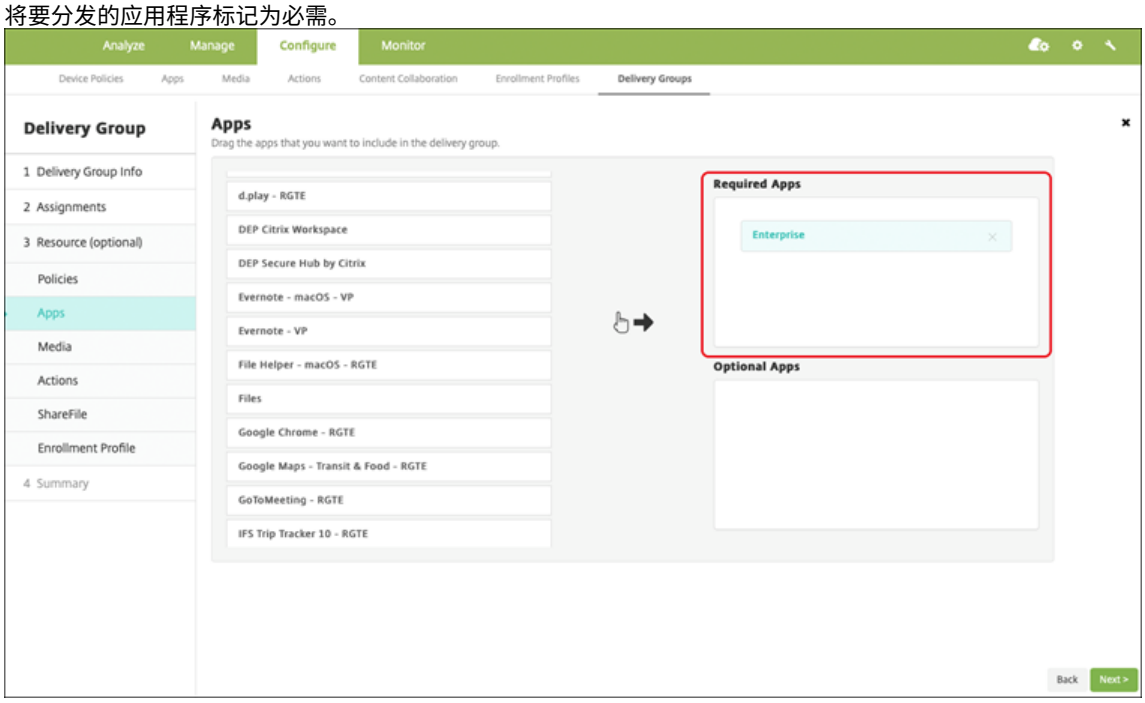
在 ABM 帐户中添加应用程序。可以上载和分发您自己的自定义应用程序，或者从其他组织购买自定义应用程序的许可证。有关在 ABM 上添加和启用自定义应用程序的详细信息，请参阅 Apple 文档。

步骤 **3**：在 **XenMobile** 中添加和配置应用程序

1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。批量购买应用程序将显示在应用程序列表中。
2. 选择要配置的应用程序。单击编辑。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. 选择要向其分发应用程序的交付组。单击保存。

步骤 **4**：配置应用程序部署

1. 在 XenMobile 控制台中，导航到配置 **>** 交付组 **>** 应用程序。
2. 将要分发的应用程序标记为必需。



3. 导航回配置 **>** 交付组。
4. 选择要部署的交付组，然后单击部署。
5. 用户会收到部署应用程序的请求。应用程序在用户接受后在后台安装。

启用了 **MDX** 的自定义应用程序

要使用 MDX 策略和安全功能，请添加启用了 MAM SDK 或 MDX 封装的自定义应用程序。

功能可用性	
需要监督设备	否
适用于用户注册模式	是
有效日期	iOS/iPadOS

步骤 **1**：链接帐户

要使用批量购买部署自定义应用程序，请将批量购买帐户链接到 XenMobile。

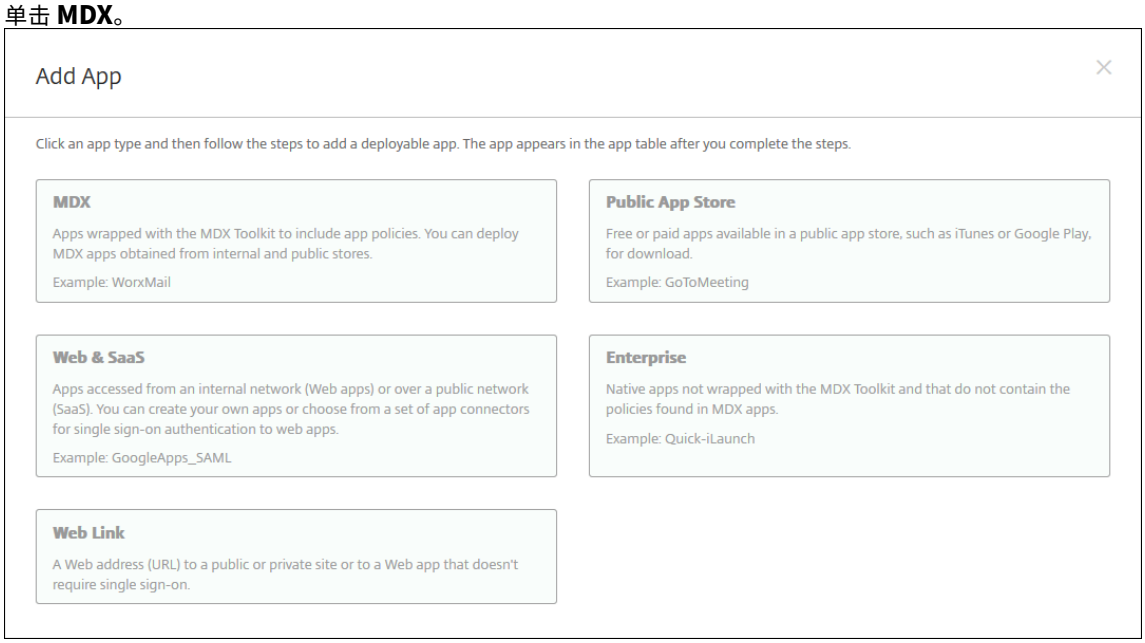
1. 设置 Apple 商务管理 (ABM) 并在其中注册。有关这些计划的详细信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 XenMobile 相关联。有关链接批量购买帐户的详细信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用应用程序自动更新。此设置可确保当 Apple 应用商店中出现更新时，用户设备上的应用程序会自动更新。

步骤 **2**：在 **ABM** 上配置应用程序

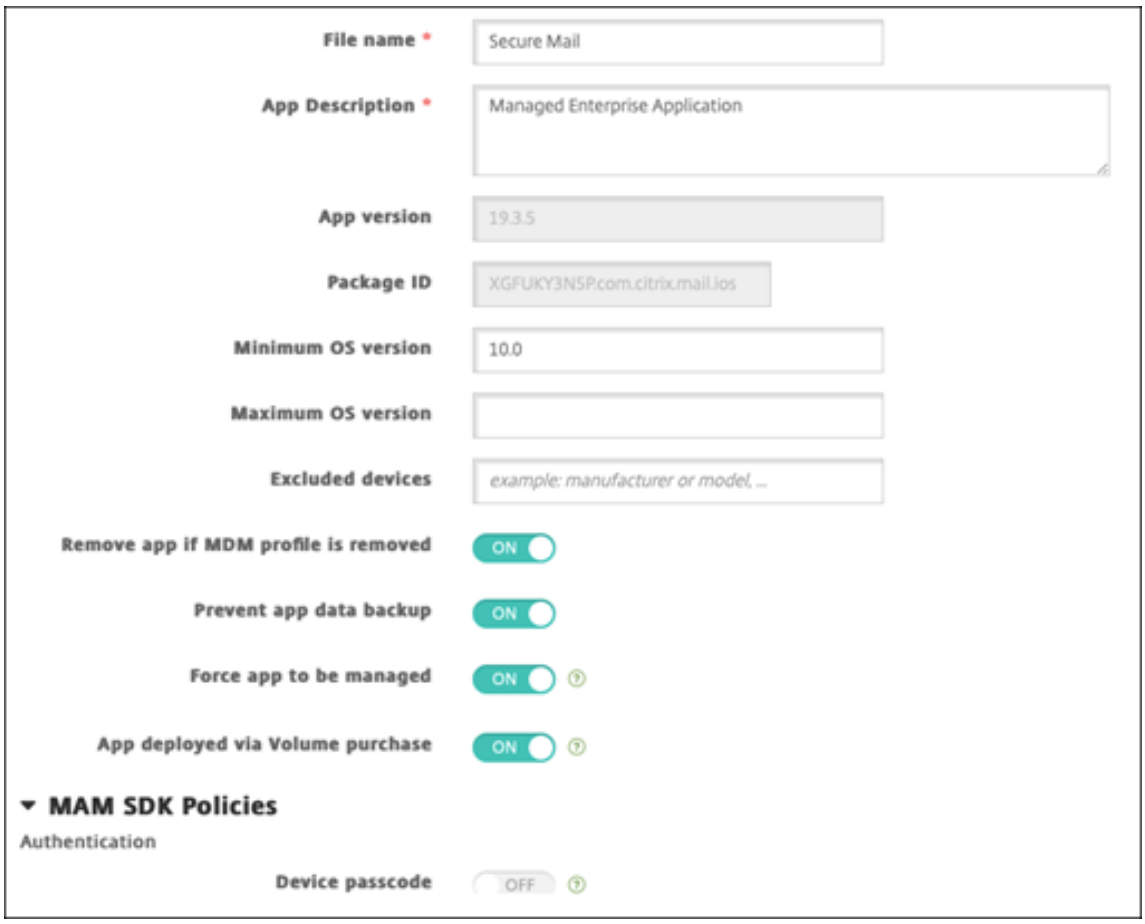
在 ABM 帐户中添加应用程序。可以上载和分发您自己的自定义应用程序，或者从其他组织购买自定义应用程序的许可证。有关在 ABM 上添加和启用自定义应用程序的详细信息，请参阅 Apple 文档。

步骤 **3**：在 **XenMobile** 中添加和配置应用程序

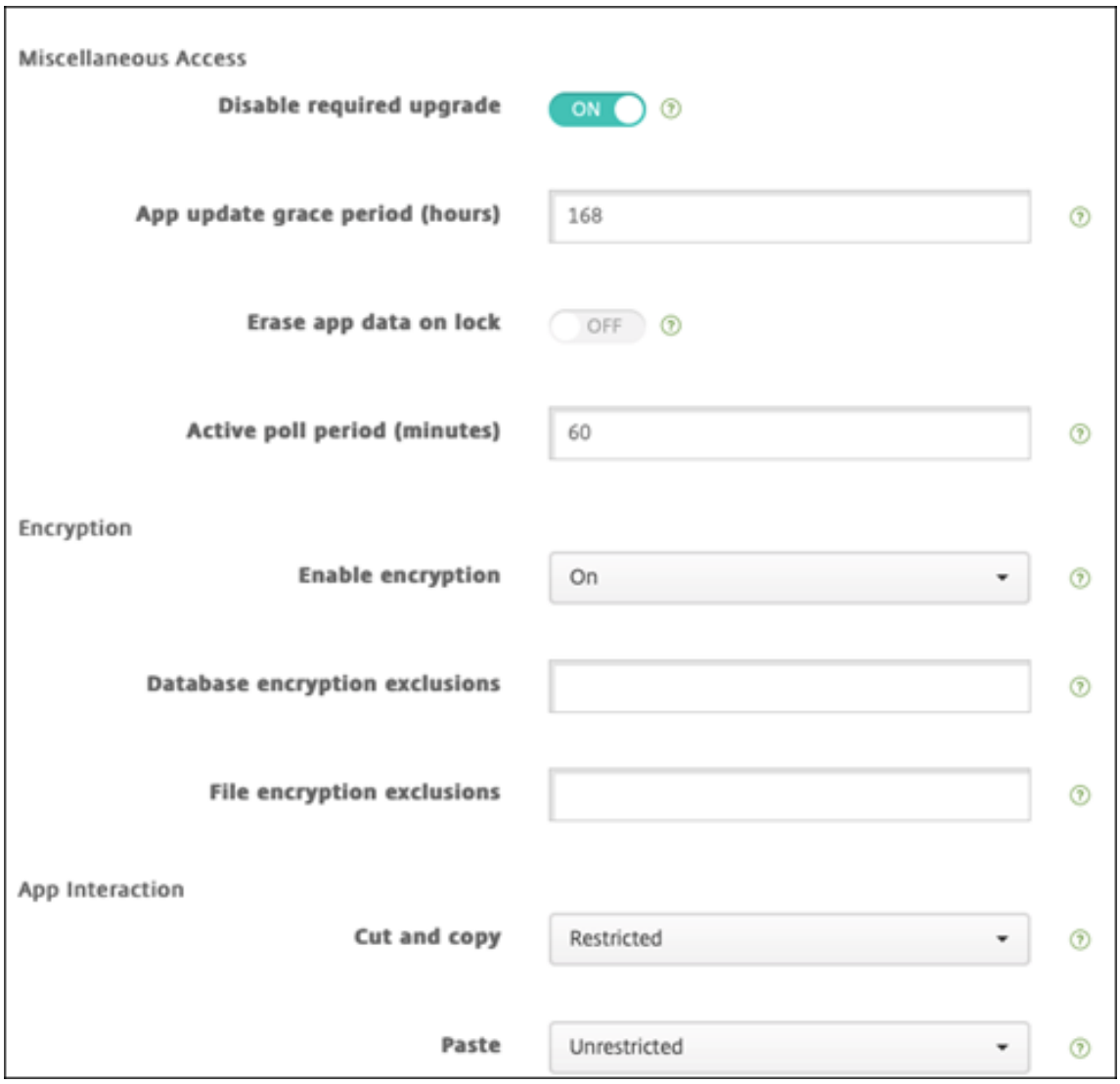
1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。单击添加。
2. 单击 **MDX**。



3. 选择 **iPhone** 或 **iPad** 平台。
4. 上载要添加的应用程序的 MDX 文件。
5. 配置应用程序详细信息。将通过批量购买部署的应用程序设置为开。Citrix 还建议启用强制管理应用程序功能。



6. 配置 MDX 策略。将禁用所需的升级设置为开。

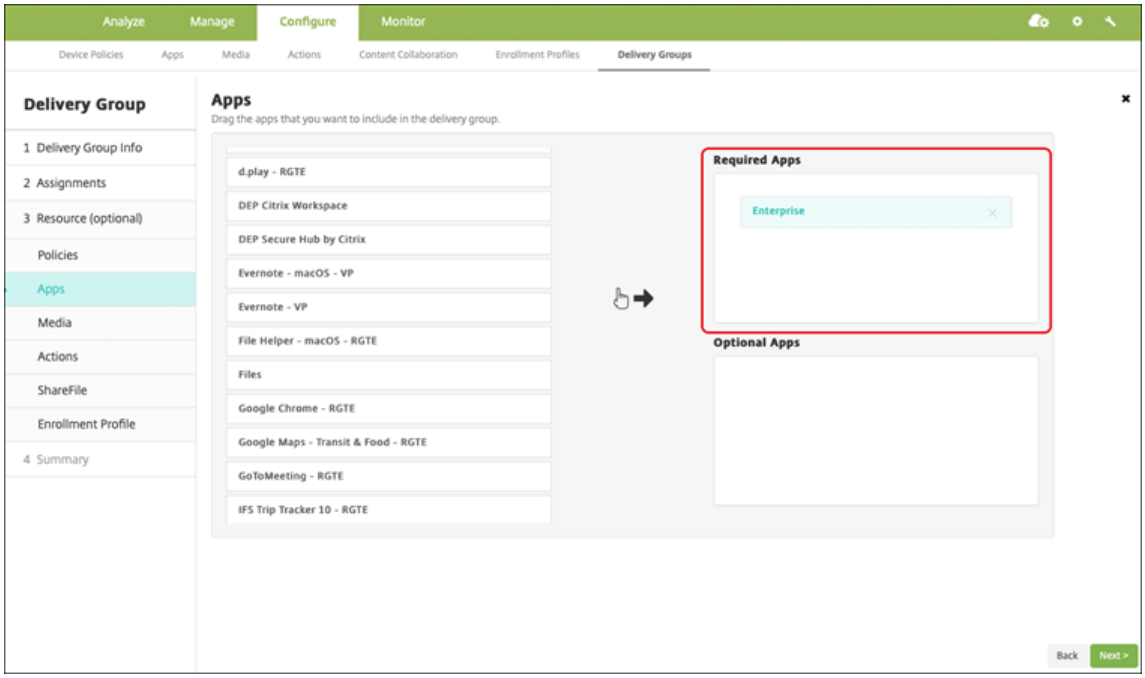


7. 将交付组分配给应用程序，然后单击保存。

此配置将导致在应用程序列表中为此应用程序列出两个条目。选择要配置的应用程序时，请选择类型为 **MDX** 的应用程序。

步骤 **4**：配置应用程序部署

1. 在 XenMobile 控制台中，导航到配置 **>** 应用程序。批量购买应用程序将显示在应用程序列表中。
2. 选择要配置的应用程序。单击编辑。
3. 选择要在每个平台上向其分发应用程序的交付组。单击保存。
4. 导航回配置 **>** 交付组 **>** 应用程序。
5. 将要分发的应用程序标记为必需。



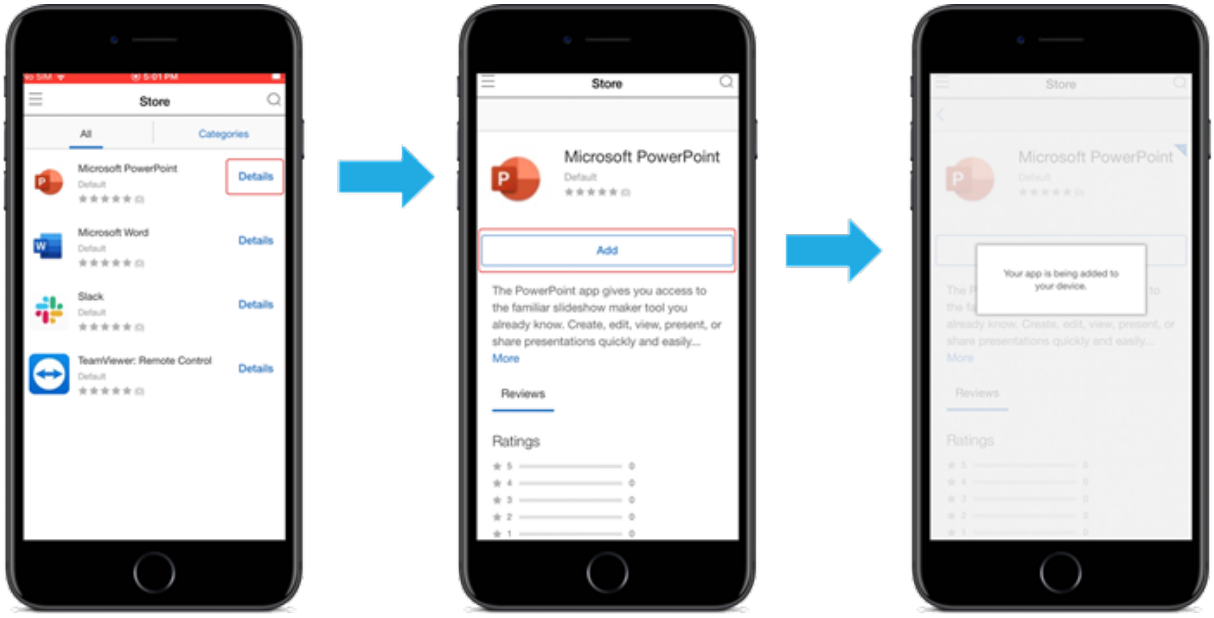
6. 导航回配置 **>** 交付组。
7. 选择要部署的交付组，然后单击部署。
8. 用户会收到部署应用程序的请求。应用程序在用户接受后在后台安装。

可选应用程序（仅限 **iOS/iPadOS**）

Citrix 建议根据需要部署应用程序。所需的应用程序以无提示方式安装在用户设备上，从而最大限度地减少交互。启用此功能还将允许应用程序自动更新。

可选应用程序允许用户选择要安装的应用程序，但用户必须通过 Secure Hub 手动启动安装。

要安装可选应用程序，用户必须启动 Secure Hub，转到应用商店，为所需应用程序选择详细信息，然后单击添加。



网络访问控制

January 5, 2022

可以使用网络访问控制 (NAC) 解决方案扩展 Android 和 Apple 设备的 Endpoint Management 设备安全评估。您的 NAC 解决方案将使用 XenMobile 安全评估帮助制定和处理身份验证决策。配置 NAC 设备后，将强制执行在 XenMobile 中配置的设备策略和 NAC 过滤器。

将 XenMobile 与 NAC 解决方案结合使用可提高 QoS，并对网络内部的设备进行更精细的控制。有关将 NAC 与 XenMobile 集成的优势的摘要，请参阅访问控制。

Citrix 支持以下与 XenMobile 集成的解决方案：

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix 不保证其他 NAC 解决方案的集成。

使用网络中的 NAC 设备：

- XenMobile 支持 NAC 作为 iOS、Android Enterprise 和 Android 设备的端点安全功能。
- 可以在 XenMobile 中启用过滤器，以便根据规则或属性将设备设置为对 NAC 合规或不合规。例如：
  - 如果 XenMobile 中的托管设备不符合指定的条件，XenMobile 会将该设备标记为不合规。NAC 设备会阻止网络中的不合规设备。
  - 如果 XenMobile 中的托管设备安装了不合规的应用程序，NAC 过滤器可以阻止建立 VPN 连接。因此，不合规的用户设备无法通过 VPN 访问应用程序或 Web 站点。
  - 如果将 Citrix Gateway 用于 NAC，则可以启用拆分隧道，以防止 Citrix Gateway 插件向 Citrix Gateway 发送不必要的网络流量。有关拆分隧道的详细信息，请参阅配置拆分隧道。

支持的 **NAC** 合规性过滤器

XenMobile Server 支持以下 NAC 合规性过滤器：

匿名设备：检查设备是否处于匿名模式。如果在设备尝试重新连接时 XenMobile 无法重新对用户进行身份验证，则可以执行此检查。

Samsung Knox 认证失败：检查设备是否无法通过 Samsung Knox 认证服务器的查询。

禁止的应用程序：检查设备是否具有“应用程序访问”设备策略中定义的禁止的应用程序。有关该策略的信息，请参阅应用程序访问设备策略。

不活动设备：按照服务器属性中 **Device Inactivity Days Threshold**（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。有关详细信息，请参阅服务器属性。

缺少所需的应用程序：检查设备是否缺少在应用程序访问策略中定义的任何所需的应用程序。

非推荐应用程序：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码：检查用户密码是否合规。在 iOS 和 Android 设备上，XenMobile 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。例如，在 iOS 设备上，如果 XenMobile 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规设备”属性检查设备是否不合规。通常情况下，使用 XenMobile API 的自动操作或第三方会更改该设备属性。

吊销状态：检查设备证书是否已吊销。再次授权之前，已吊销的设备无法重新注册。

已获得 **root** 权限的 **Android** 设备和已越狱的 **iOS** 设备：检查 Android 设备或 iOS 设备是否已被越狱。

非托管设备：检查设备是否仍处于托管状态，受 XenMobile 控制。例如，在 MAM 下注册的设备或已取消注册的设备为非托管设备。

> 注意：
>
> “隐式合规/不合规”过滤器仅在 XenMobile 管理的设备上设置默认值。例如，任何安装了阻止的应用程序或未注册的设备都将被标记为“不合规”。NAC 设备会阻止您的网络中的这些设备。

配置概述

我们建议您按照列出的顺序配置 NAC 组件。

1. 配置设备策略以支持 NAC：

   对于 **iOS** 设备：请参阅配置 VPN 设备策略以支持 NAC。

   对于 **Android Enterprise** 设备：请参阅为 Citrix SSO 创建 Android Enterprise 托管配置。

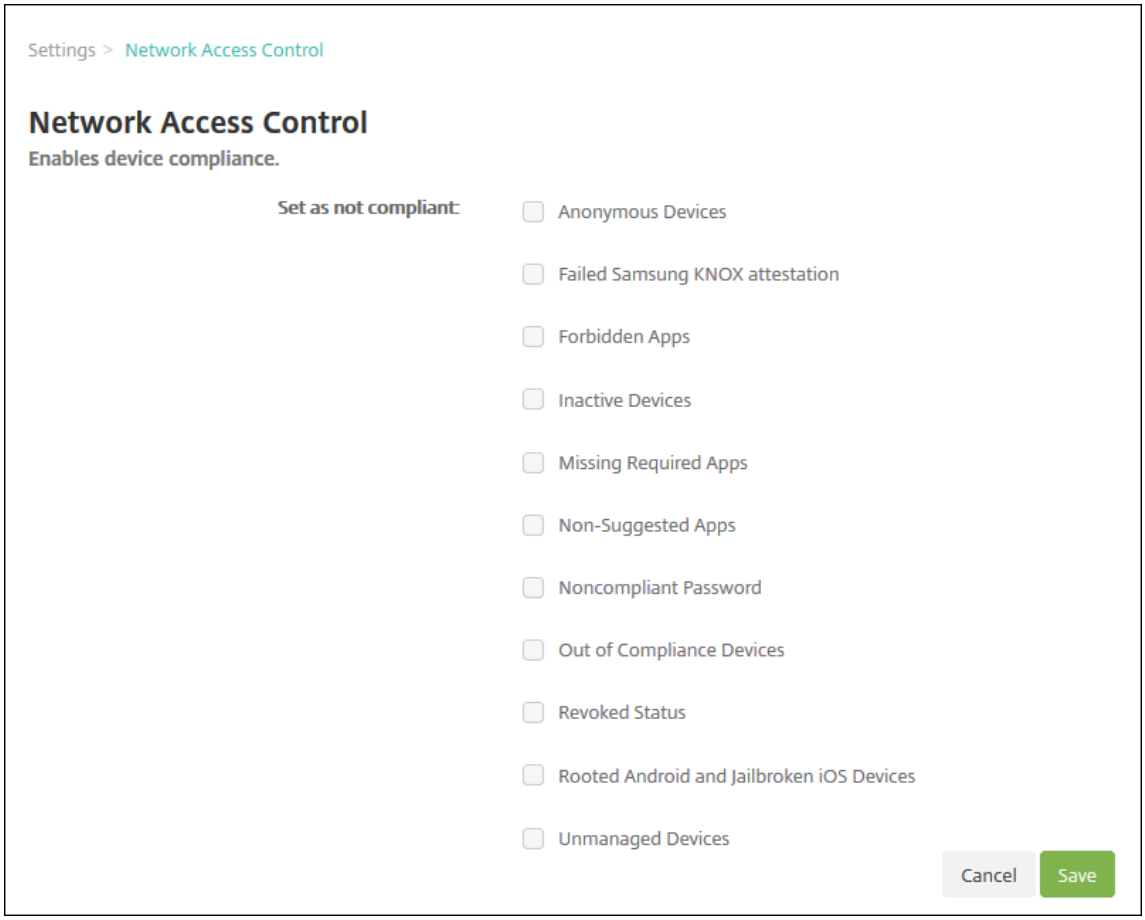
   对于 **Android** 设备：请参阅为 Android 配置 Citrix SSO 协议。

2. 在 XenMobile 中启用 NAC 过滤器。
3. 配置 NAC 解决方案：
   - Citrix Gateway，详见更新 Citrix Gateway 策略以支持 NAC。

     要求您在设备上安装 Citrix SSO。请参阅 Citrix Gateway 客户端。
   - Cisco ISE：请参阅 Cisco 文档。
   - ForeScout：请参阅 ForeScout 文档。

在 **XenMobile** 中启用 **NAC** 过滤器

1. 在 XenMobile 控制台中，转到设置 **>** 网络访问控制。



2. 选中要启用的设为不合规过滤器旁边的复选框。
3. 单击保存。

更新 **Citrix Gateway** 策略以支持 **NAC**

必须在 VPN 虚拟服务器上配置高级（非传统）身份验证和 VPN 会话策略。

以下步骤使用以下任一特性更新 Citrix Gateway：

- 与 XenMobile Server 环境集成。
- 或者，针对 VPN 设置，而非 XenMobile Server 环境的一部分，并且可以访问 XenMobile。

在您的虚拟 VPN 服务器上，从控制台窗口中执行以下操作：命令和示例中的 IP 地址是虚构的。

1. 如果要在您的 VPN 虚拟服务器上使用经典策略，请删除并取消绑定所有经典策略。要进行检查，请键入：

   ```
   show vpn vserver <VPN_VServer>
   ```

   删除包含单词 Classic 的所有结果。例如：`VPN Session Policy Name: PL_OS_10.10.1.1 Type : Classic Priority: 0`

   要删除策略，请键入：


```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. 请通过键入以下命令创建相应的高级会话策略。

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   例如：`add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. 请通过键入以下命令将策略绑定到您的 VPN 虚拟服务器。

   ```
   bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
   ```

4. 请通过键入以下命令创建身份验证虚拟服务器。

   ```
   add authentication vserver <authentication vserver name> <service type>
    <ip address>
   ```

   例如：`add authentication vserver authvs SSL 0.0.0.0`
   在此示例中，`0.0.0.0` 表示身份验证虚拟服务器不面向公众开放。

5. 请通过键入以下命令将 SSL 证书与虚拟服务器绑定在一起。

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver
   certificate>
   ```

   例如：`bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. 请从 VPN 虚拟服务器将身份验证配置文件关联到身份验证虚拟服务器。首先，请通过键入以下命令创建身份验证配置文件。

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication
    vserver name>
   ```

   例如：

   ```
   add authentication authnProfile xm_nac_prof -authnVsName authvs
   ```

7. 请通过键入以下命令将身份验证配置文件与 VPN 虚拟服务器关联。

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   例如：

   ```
   set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. 请通过键入以下命令检查从 Citrix Gateway 到设备的连接。

   ```
   curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --
   header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   例如，此查询通过获取在环境中注册的第一台设备 (`deviceid_1`) 的合规性状态来验证连接性：

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-
   Citrix-VPN-Device-ID: deviceid_1"
   ```

   成功的结果与以下示例类似。


```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. 上一个步骤成功时，请创建对 XenMobile 的 Web 身份验证操作。首先，请创建一个策略表达式以从 iOS VPN 插件中导出设备 ID。键入以下命令。

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
   TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. 请通过键入以下命令向 XenMobile 发送请求。在此示例中，XenMobile Server IP 为 10.207.87.82，FQDN 为 example.em.server.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.server.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\")"
    ```

    XenMobile NAC 的成功输出为 HTTP status 200 OK。X-Citrix-Device-State 标头的值必须为 Compliant。

11. 请通过键入以下命令创建一个要将操作关联到的身份验证策略。

    ```
    add authentication Policy <policy name> -rule <rule> -action <web
    authentication action>
    ```

    例如：add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER (\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac

12. 请通过键入以下命令将现有 LDAP 策略转换为高级策略。

    ```
    add authentication Policy <policy_name> -rule <rule> -action <LDAP
    action name>
    ```

    例　　如：add authentication Policy ldap_xm_test_pol -rule **true** -action 10.10.1.1_LDAP

13. 请通过键入以下命令添加要将 LDAP 策略关联到的策略标签。

    ```
    add authentication policylabel <policy_label_name>
    ```

    例如：add authentication policylabel ldap_pol_label

14. 请通过键入以下命令将 LDAP 策略关联到策略标签。


```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol
 -priority 100 -gotoPriorityExpression NEXT
```

15. 请连接合规设备以执行 NAC 测试，以确认成功的 LDAP 身份验证。键入以下命令。

```
bind authentication vserver <authentication vserver> -policy <web
authentication policy> -priority 100 -nextFactor <ldap policy label> -
gotoPriorityExpression END
```

16. 添加 UI 以与身份验证虚拟服务器相关联。请键入以下命令以检索设备 ID。

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -
action lschema_single_factor_deviceid
```

17. 请通过键入以下命令绑定身份验证虚拟服务器。

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority
 100 -gotoPriorityExpression END
```

18. 创建 LDAP 高级身份验证策略以启用 Secure Hub 连接。键入以下命令。

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority
110 -gotoPriorityExpression NEXT
```

Samsung Knox

January 5, 2022

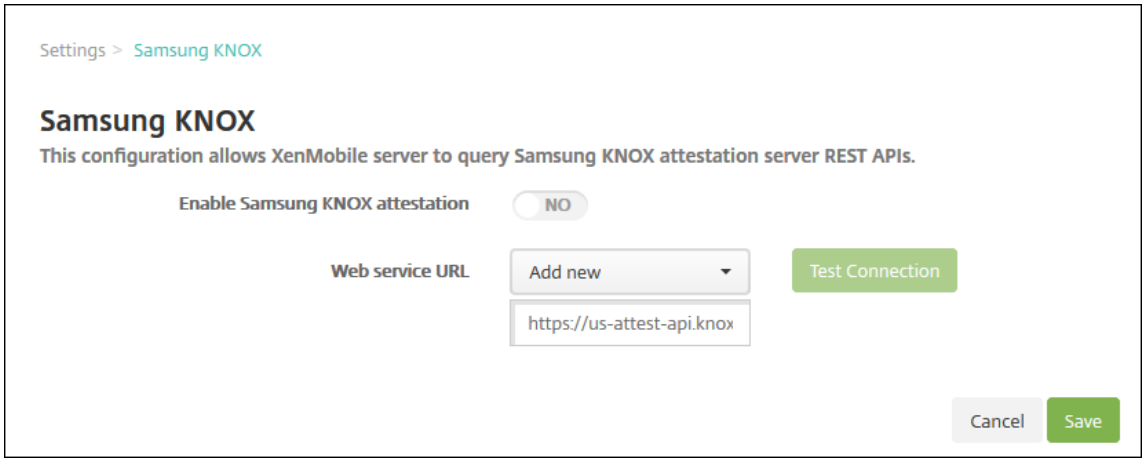
Samsung 提供了与 XenMobile Server 兼容的几种解决方案。

- XenMobile 在兼容的 Samsung 设备上支持和扩展 Samsung Knox 策略。
- Knox 服务插件 (KSP) 是支持一部分适用于企业的 Knox 平台 (KPE) 功能的应用程序。有关 Samsung 提供的有关 KPE 的信息，请参阅 Configure Knox Platform for Enterprise（为企业配置 Knox 平台）和 Overview（概述）。

可以配置 XenMobile 以查询 Samsung Knox 认证服务器 REST API。

Samsung Knox 利用为操作系统和应用程序提供多级别保护的硬件安全功能。其中一种安全级别驻留在通过认证的平台上。认证服务器提供移动设备的核心系统软件（例如，引导加载程序和内核）验证。该验证基于在可信引导期间收集的数据在运行时进行。

1. 在 XenMobile 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. 在平台下方，单击 **Samsung KNOX**。此时将显示 **Samsung KNOX** 页面。



3. 在启用 **Samsung KNOX** 认证中，选择是否启用 Samsung Knox 认证。默认值为否。
4. 将启用 **Samsung KNOX** 认证设置为是时，将启用 **Web** 服务 **URL** 选项。然后在列表中执行以下操作之一：
   - 单击适当的认证服务器。
   - 单击新增，然后输入 Web 服务 URL。
5. 单击测试连接以验证连接。将显示成功或失败消息。
6. 单击保存。

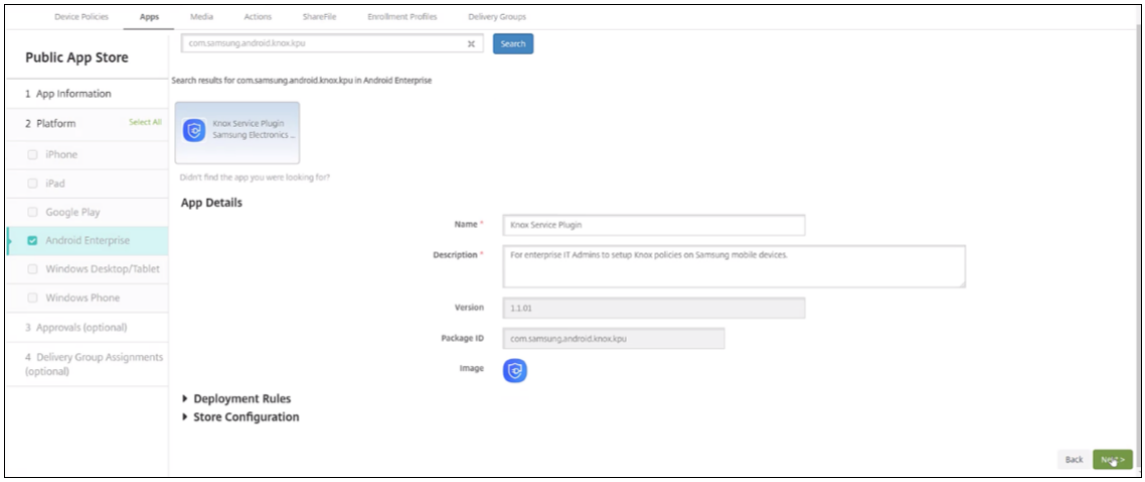
> 注意：
>
> 可以使用 Samsung Knox Mobile Enrollment 将多个 Samsung Knox 设备注册到 XenMobile（或任何移动设备管理器）中，无需手动配置每个设备。有关信息，请参阅 Samsung Knox 批量注册。

添加 **Knox** 服务插件应用程序

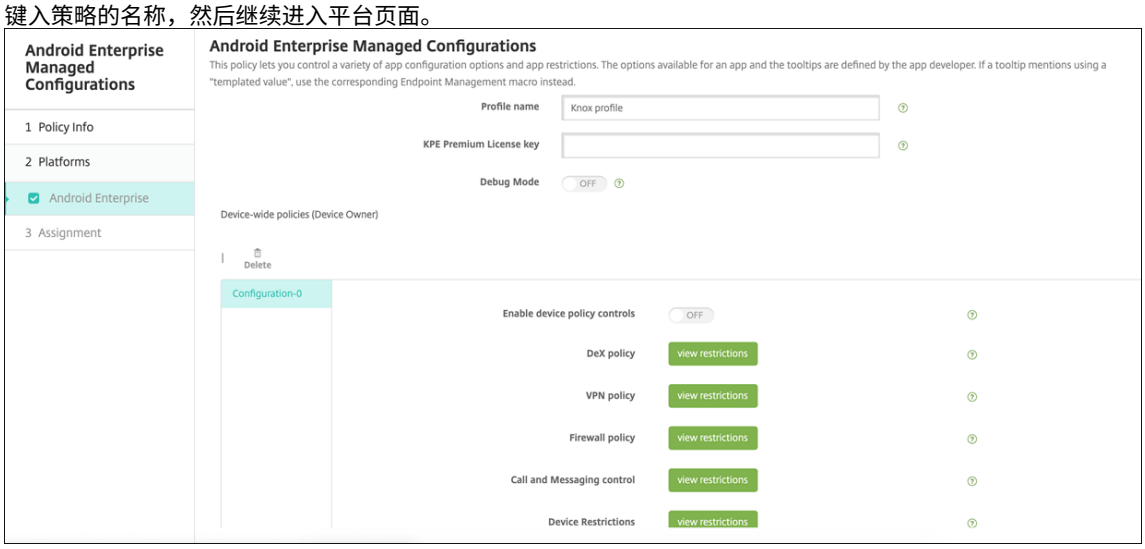
如果您计划将 Android Enterprise 与 Knox 结合使用，请将 Knox 服务插件 (KSP) 添加到 XenMobile。KSP 应用程序使用 AndroidOEMConfig 来支持安全策略、灵活的 VPN 配置和生物特征识别身份验证控制等功能。AndroidOEMConfig 使 OEM 和端点移动性管理器 (EMM) 能够支持自定义 OEM API。这些 API 涵盖了 Android Enterprise 不支持的用例。

有关 KSP 的详细信息，请参阅 Knox Service Plug-in Admin Guide（《Knox 服务插件管理指南》）。

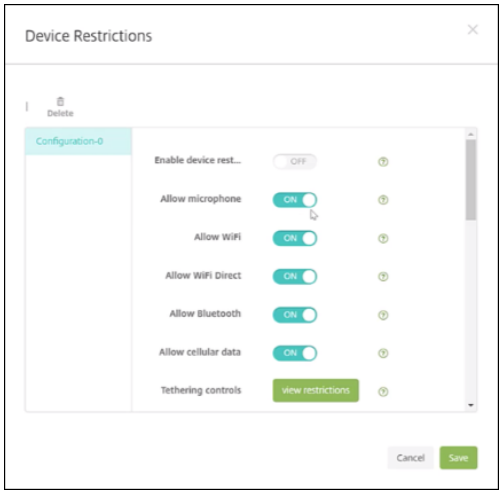
1. 登录您的 Google 帐户并导航到 `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`。批准 Knox 服务插件应用程序。
2. 登录到 XenMobile 控制台，并将 Knox 服务插件添加为公共应用商店应用程序。有关添加公共应用商店应用程序的详细信息，请参阅添加公共应用商店应用程序。



3. 在 XenMobile 控制台中，导航到配置 **>** 设备策略。单击添加。
4. 单击 **Android Enterprise** 托管配置。在显示的对话框中，从菜单中选择 **Knox Service Plugin**（Knox 服务插件）。有关 Android Enterprise 托管配置策略的详细信息，请参阅 Android Enterprise 托管配置策略。
5. 键入策略的名称，然后继续进入平台页面。



6. 在平台页面上，键入 Knox 配置文件的配置文件名称，然后输入 Samsung 提供的 **KPE Premium License key**（KPE 高级许可证密钥）。这些字段下方显示的策略来自您的 Knox 部署。有关 Knox 策略的详细信息，请参阅本部分前面引用的《Knox 服务管理插件指南》。



7. 单击下一步并配置策略的部署规则。
8. 单击保存。

Samsung Knox 批量注册

January 5, 2022

要将多个 Samsung Knox 设备注册到 XenMobile（或任何移动设备管理器）中，但不手动配置每个设备，请使用 Knox Mobile Enrollment。首次使用时或恢复出厂设置后会进行注册。管理员还可以将用户名和密码直接传递到设备，以便用户不需要在注册时输入任何信息。

> 注意：
>
> Knox Mobile Enrollment 的设置与 XenMobile Knox 容器无关。有关 Knox Mobile Enrollment 的详细信息，请参阅 Knox Mobile Enrollment Admin Guide（《Knox Mobile Enrollment 管理指南》）。

Knox Mobile Enrollment 的先决条件

- XenMobile 必须已配置（包括许可证和证书）且正在运行。
- Secure Hub APK 文件。设置 Knox Mobile Enrollment 时，您将上载此文件。
- 有关 KME 要求的列表，请参阅 Knox Mobile Enrollment Introduction（Knox Mobile Enrollment 简介）。
- 适用于企业的 Samsung Knox 平台 (PKE) 许可证，需要应用设备策略。在 XenMobile 设备策略“适用于企业的 Knox 平台”中提供许可证密钥。

下载 Secure Hub APK 文件

转到 Google Play 应用商店下载 Citrix Secure Hub for Android 文件。

配置防火墙例外

要访问 Knox Mobile Enrollment，请配置以下防火墙例外。其中有些防火墙例外是所有设备必需的，而有些例外则特定于设备的地理区域。

设备区域	URL	端口	目标
全部	https://gslb.secb2b.com	443	适用于 Knox Mobile Enrollment 启动的全局负载平衡器
全部	https://gslb.secb2b.com	80	适用于某些受限旧设备上的 Knox Mobile Enrollment 启动的全局负载平衡器
全部	umc-cdn.secb2b.com	443	Samsung 代理更新服务器
全部	bulkenrollment.s3.amazonaws.com	80	Knox Mobile Enrollment 客户 EULA
全部	eula.secb2b.com	443	Knox Mobile Enrollment 客户 EULA
全部	us-be-api-mssl.samsungknox.com	443	用于 IMEI 验证的 Samsung 服务器
美国	https://us-segd-api.secb2b.com	443	适用于美国的 Samsung 企业网关
欧洲	https://eu-segd-api.secb2b.com	443	适用于欧洲地区的 Samsung 企业网关
中华人民共和国	https://china-segd-api.secb2b.com	443	适用于中国的 Samsung 企业网关

> 注意：
>
> 可以在 Knox Mobile Enrollment Admin Guide（《Knox Mobile Enrollment 管理指南》）中找到防火墙例外的完整列表。

获取对 **Knox Mobile Enrollment** 的访问权限

按照 Samsung 文档获取 Knox Mobile Enrollment 的访问权限，网址为 Get started with KME（KME 入门）。

设置 **Knox Mobile Enrollment**

访问 Knox Mobile Enrollment 后，请登录 Knox 门户。

注册过程遵循以下常规步骤。

1. 使用您的 MDM 控制台信息和设置创建一个 MDM 配置文件。

   MDM 配置文件指示您的设备如何连接到 MDM。

2. 将设备添加到您的 MDM 配置文件。

   可以上载包含设备信息的 CSV 文件，也可以从 Google Play 安装和使用 Knox 部署应用程序。

3. Samsung 在验证设备所有权时向您发出警报。

4. 向用户提供 MDM 凭据。指导用户使用 Wi-Fi 连接到 Internet 以及接受注册其设备的提示。

创建 **MDM** 配置文件

请按照配置文件配置上的 Samsung 文档中概述的步骤进行操作。

遇到以下字段或步骤时，请按照说明进行配置：

- **Pick your MDM**（选择您的 MDM）：从菜单中选择 **Citrix**。仅适用于设备所有者配置文件。
- **MDM Agent APK**(MDM 代理 APK):仅适用于设备所有者配置文件。键入 Secure Hub APK 下载 URL:`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

  APK 文件可以驻留在设备在注册过程中能够访问的任何服务器上。在注册过程中，设备：

  - 从 APK 下载 URL 下载 Secure Hub
  - 安装 Secure Hub
  - 然后打开 Secure Hub，其中包含下面描述的自定义 JSON 数据。

  .apk 文件名的大写必须与您输入的 URL 一致。例如，如果文件名全部小写，则在 URL 中也必须全部小写。

- **MDM** 服务器 **URI**：请勿指定 MDM 服务器 URI。XenMobile 不使用 Samsung MDM 协议。
- 自定义 **JSON** 数据： Secure Hub 需要 XenMobile Server 地址以及用户名和密码才能进行注册。可以在 JSON 中提供该数据，以便 Secure Hub 不提示用户输入该数据。仅当 JSON 忽略该字段时，Secure Hub 才会提示用户输入服务器地址、用户名或密码。

  自定义 JSON 数据的格式为：

  ```
  { "serverURL": "URL", "xm_username":"Username", "xm_password":"Password
  "}
  ```

  在此示例中，通常对于批量注册而言，Secure Hub 不会在注册期间提示用户输入服务器地址或其凭据：

  ```
  { "serverURL":"https://example.com/zdm", "xm_username":"userN", "
  xm_password":"password1234"}
  ```



```
{ "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2"
, "xm_password":"password7890"}
```

在此示例中，通常对于基于展台的设备而言，Secure Hub 会提示用户输入其凭据：

```
{ "serverURL":"https://example.com/zdm"}
```

还可以为 Android Enterprise 的零接触注册输入自定义 JSON。

```
1       {
2
3           "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4           {
5
6               "serverURL":"URL","xm_username":"username","
                   xm_password":"password"
7            }
8
9        }
10
11  <!--NeedCopy-->
```

设备开始注册时，设备将从给定的 URL 下载 Secure Hub，安装 Secure Hub，然后打开 Secure Hub。

进一步配置

有关配置的详细信息，请参阅以下 Samsung 文档页面：

- 设备配置：批量添加设备。
- Samsung Knox 部署应用程序：通过蓝牙、NFC 或 Wi-Fi Direct 注册注册设备。
- Knox Mobile Enrollment：浏览 Samsung 文档，了解有关 Samsung Knox 的更多信息。

注册正在运行版本 **2.4** 之前的 **Knox API** 的设备

在 Knox API 的版本低于 2.4 的设备上，在初始设备设置期间不会开始执行批量注册。相反，用户必须启动注册过程。为此，用户将转到 Samsung 站点以下载新的 Mobile Enrollment 客户端并开始注册。

下载的注册客户端使用的 MDM 配置文件和 APK 与在 Knox 批量注册门户中为 Knox 2.4/2.4.1 设备配置的 MDM 配置文件和 APK 相同。

用户通常按照以下步骤进行操作：

1. 打开设备并连接到 Wi-Fi。如果 Mobile Enrollment 未启动或者 Wi-Fi 不可用，请执行下列操作：
   a) 转至 Samsung Knox Mobile Enrollment。
   b) 轻按 **Next**（下一步按钮使用移动数据注册设备。

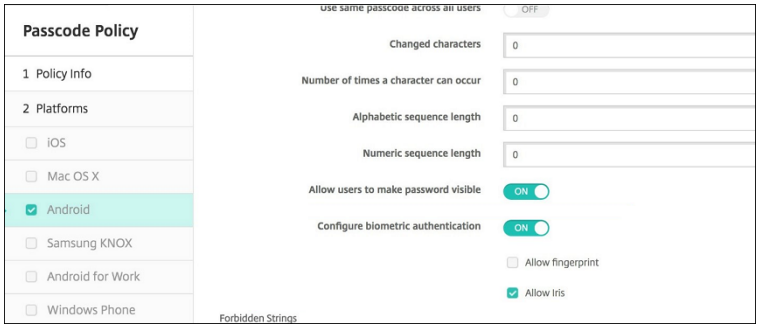
2. 出现提示 **Enroll with Knox**（通过 Knox 注册）时，轻按 **Continue**（继续）。
3. 阅读 EULA（如果有）。轻按下一步。
4. 如果出现提示，请输入 IT 管理员提供的 **User ID**（用户 ID）和 **Password**（密码）。

此时将验证用户凭据并在贵组织的企业 IT 环境中注册其设备。

对 **Samsung** 设备启用和禁用生物特征身份验证

XenMobile 支持指纹和虹膜扫描身份验证，又称为生物特征识别身份验证。可以对 Samsung 设备启用和禁用生物特征识别身份验证，而无需用户执行任何操作。如果在 XenMobile 中禁用了生物特征身份验证，用户和第三方应用程序将无法启用此功能。

1. 在 XenMobile 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页面。
3. 单击通行码。此时将显示通行码策略信息页面。
4. 在策略信息窗格中，输入以下信息：
   - 策略名称：键入策略的描述性名称。
   - 说明：（可选）键入策略的说明。
5. 单击 **Next**（下一步）。此时将显示平台页面。
6. 在平台下，选择 **Android** 或 **Samsung Knox**。
7. 将配置生物特征身份验证设置为开。
8. 如果选择 **Android**，请在 **Samsung SAFE** 下选择允许指纹、允许虹膜，或者两者。



安全操作

January 5, 2022

可以从管理 > 设备页面执行设备和应用程序安全操作。设备操作包括吊销、锁定、解锁及擦除。应用程序安全操作包括应用程序锁定和应用程序擦除。

- 激活锁绕过：设备激活之前从受监督的 iOS 设备中删除激活锁。此命令不需要用户的个人 Apple ID 或密码。
- 应用程序锁定：拒绝访问设备上的所有应用程序。在 Android 中，应用程序锁定后，用户将无法登录 XenMobile。在 iOS 中，用户可以登录，但无法访问任何应用程序。
- 应用程序擦除：从 Secure Hub 中删除用户帐户并取消注册设备。在执行应用程序取消擦除操作之前，用户无法重新注册。
- **ASM** 部署计划激活锁：为在 Apple 校园教务管理 DEP 中注册的 iOS 设备创建激活锁绕过码。
- 清除限制：在受监督的 iOS 设备中，此命令允许 XenMobile 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。第二次发送此命令将使设备脱离丢失模式。
- 启用跟踪：在 Android 或 iOS 设备上，此命令允许 XenMobile 以您定义的频率轮询特定设备的位置。要在地图上查看设备坐标和位置，请转到管理 **>** 设备，选择一个设备，然后单击编辑。设备信息位于安全下的常规选项卡上。使用启用跟踪可持续跟踪设备。Secure Hub 会在设备运行时定期报告位置。
- 完全擦除：立即从设备中（包括从任何内存卡中）擦除所有数据和应用程序。
  - 对于 Android 设备，此请求还可以包括用于擦除内存卡的选项。
  - 对于使用工作配置文件（COPE 设备）的 Android Enterprise 完全托管设备，您可以在选择性擦除操作删除工作配置文件后执行完全擦除。
  - 对于 iOS 和 macOS 设备，擦除操作将立即发生，即使设备处于锁定状态亦如此。对于 iOS 11 设备（最低版本）：确认完全擦除时，可以选择在设备上保留手机网络流量套餐。
  - 对于 Windows Phone 设备，完全擦除操作会删除所有 XenMobile 信息和所有用户数据。此数据包括应用程序、电子邮件、联系人和媒体等个人内容。
  - 对于运行 Windows Mobile 6 或更早版本的 Windows 移动设备：擦除后，可能需要将设备送回制造商处，以重新加载初始操作系统和/或软件。
  - 如果设备用户在删除内存卡内容之前关闭了设备，用户可能仍然对设备数据具有访问权限。
  - 可以在将擦除请求发送到设备之前取消该请求。
- 定位：在管理 **>** 设备页面上的设备详细信息 **>** 常规下定位设备并报告设备位置（包括地图）。定位是一次性操作。使用定位可显示执行该操作时的当前设备位置。要在一段时间内持续跟踪设备，请使用启用跟踪。
  - 将此操作应用到 Android（Android Enterprise 除外）设备或 Android Enterprise（企业拥有或 BYOD）设备时，请注意以下行为：
    * 定位要求用户在注册期间授予位置权限。用户可以选择不授予定位权限。如果用户在注册过程中不授予该权限，XenMobile 会在发送定位命令时再次申请定位权限。
  - 将此功能应用到 iOS 或 Android Enterprise 设备时，请注意以下限制：
    * 对于 Android Enterprise 设备，除非位置设备策略已将设备的位置模式设置为高精度或省电，否则此请求将失败。
    * 对于 iOS 设备，仅当设备处于 MDM 丢失模式时，此命令才会成功。

- 锁定：远程锁定设备。当您丢失设备且不知道设备是否被盗时此操作非常有用。XenMobile 随之生成一个 PIN 代码并在设备中进行设置。要访问设备，用户需要键入该 PIN 代码。使用取消锁定可从 XenMobile 控制台中删除锁定。
- 锁定并重置密码：远程锁定设备并重置密码。
  - 不支持在工作配置文件模式下于 Android Enterprise 中注册且运行低于 Android 8.0 的 Android 版本的设备。
  - 在工作配置文件模式下于 Android Enterprise 中注册且运行 Android 8.0 或更高版本的设备上：
    * 发送的密码将锁定工作配置文件。设备不会被锁定。
    * 如果未发送密码，或者发送的密码不符合密码要求，并且尚未对工作配置文件设置任何密码：设备将被锁定。
    * 如果未发送密码，或者发送的密码不符合密码要求，但已对工作配置文件设置密码：工作配置文件将被锁定，但设备不会被锁定。
- 通知 **(**响铃**)**：在 Android 设备上播放声音。
- 重新启动：重新启动 Windows 10 和 Windows 11 设备。对于 Windows Tablet 和 PC，此时将显示消息“System will reboot soon”（系统很快将重新启动），重新启动将在之后的 5 分钟内发生。对于 Windows Phone，重新启动将在几分钟后发生，并且不向用户显示任何警告消息。
- 请求使用**/**停止使用 **AirPlay** 镜像：在受监督的 iOS 设备上启动和停止 AirPlay 镜像。
- 重新启动**/**关闭：立即重新启动或关闭受监督的 iOS 设备。
- 吊销：禁止设备连接到 XenMobile Server。
- 吊销**/**授权 **(iOS**、**macOS)**：执行与“选择性擦除”相同的操作。吊销后，可以重新向设备授权以进行重新注册。
- 响铃：如果设备处于丢失模式，响铃将在受监督的 iOS 设备上播放声音。声音将持续播放，直至您将设备从丢失模式中删除或者用户禁用声音。
- 选择性擦除：擦除设备上的所有公司数据和应用程序，保留个人数据和应用程序。选择性擦除后，用户可以重新注册设备。
  - 选择性擦除 Android 设备不会断开设备与 Device Manager 及企业网络的连接。要阻止设备访问 Device Manager，还必须吊销设备证书。
  - 选择性擦除 Android 设备也会吊销设备。只有在重新授权设备或从控制台中删除设备后，才能重新注册设备。
  - 对于使用工作配置文件（COPE 设备）的 Android Enterprise 完全托管设备，您可以在选择性擦除操作删除工作配置文件后执行完全擦除。或者，也可以使用相同的用户名重新注册设备。重新注册设备会重新创建工作配置文件。
  - 如果启用了 Samsung Knox API，选择性擦除设备还将删除 Samsung Knox 容器。
  - 对于 iOS 和 macOS 设备，此命令将删除通过 MDM 安装的任何配置文件。
  - 在 Windows 设备上执行的选择性擦除还将删除当时已登录的任何用户的配置文件文件夹的内容。选择性擦除不会删除您通过配置向用户提供的任何 Web 剪辑。要删除 Web 剪辑，用户需要手动取消注册其设备。不能重新注册选择性擦除的设备。

  - 选择性擦除 Windows Phone 设备会删除允许 XenMobile 在设备上安装应用程序的企业令牌。该擦除操作还将删除为设备部署的所有 XenMobile 证书和配置。不能重新注册选择性擦除的 Windows Phone 设备。

- 解锁：清除设备被锁定时向其发送的通行码。此命令不解锁设备。

在管理 **>** 设备中，设备详细信息页面还将列出设备安全属性。这些属性包括“强 ID”、“锁定设备”、“激活锁绕过”以及平台类型的其他信息。完全擦除设备字段包括用户的 PIN 代码。擦除设备后，用户必须输入该代码。如果用户忘记了该代码，您可以在此处查找。

Android 设备的安全操作

安全操作	Android（Android Enterprise 设备除外）	Android Enterprise (BYOD)	Android Enterprise（公司拥有）
应用程序锁定	是	否	否
应用程序擦除	是	否	否
完全擦除	是	否	是
查找	是：对于运行 Android 6.0+ 的设备，定位操作要求用户在注册过程中授予定位权限。用户可以选择不授予定位权限。如果用户在注册过程中不授予该权限，XenMobile 会在发送定位命令时再次申请定位权限。	是：对于运行 Android 6.0+ 的设备，定位操作要求用户在注册过程中授予定位权限。用户可以选择不授予定位权限。如果用户在注册过程中不授予该权限，XenMobile 会在发送定位命令时再次申请定位权限。	是：对于运行 Android 6.0+ 的设备，定位操作要求用户在注册过程中授予定位权限。用户可以选择不授予定位权限。如果用户在注册过程中不授予该权限，XenMobile 会在发送定位命令时再次申请定位权限。
锁定	是	是	是
锁定并重置密码	是	否	是
通知（响铃）	是	是	是
吊销	是	是	是
选择性擦除	是	是	否

iOS 和 **macOS** 设备的安全操作

安全操作	**iOS**	**macOS**
激活锁绕过	是	否

安全操作	iOS	macOS
应用程序锁定	是	否
应用程序擦除	是	否
ASM 部署计划激活锁	是	否
清除限制	是	否
启用/禁用丢失模式	是	否
启用/禁用跟踪	是	否
完全擦除	是	是
查找	是	否
锁定	是	是
响铃	是	是
请求使用/停止使用 AirPlay 镜像	是	否
重新启动/关闭	是	否
吊销/授权	是	是
选择性擦除	是	是
解锁	是	否

Windows 设备的安全操作

安全操作	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
查找	是	是	否
锁定	是	是	是
锁定并重置密码	是	否	是
重新启动	是	是	否
吊销	是	是	是
响铃	是	否	是
选择性擦除	是	是	是
擦除	是	是	是

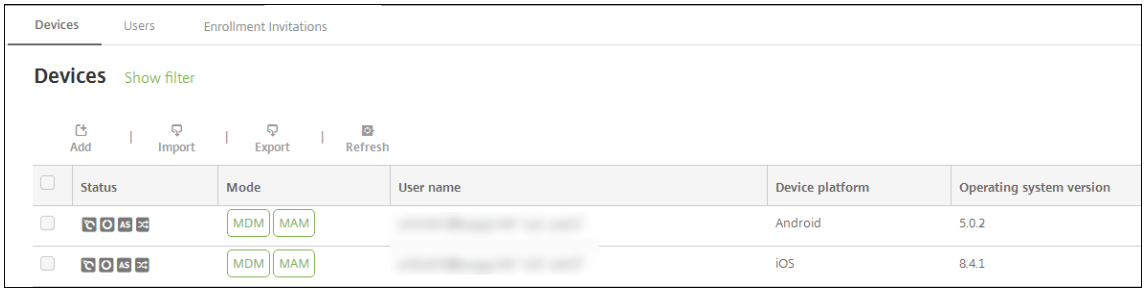
本文的其余部分提供执行各种安全操作的步骤。也可以自动执行某些操作。有关详细信息，请参阅自动化操作。

锁定 **iOS** 设备

您可以锁定丢失的 iOS 设备，同时在设备锁屏界面上显示消息和电话号码。运行 iOS 7 及更高版本的设备支持此功能。

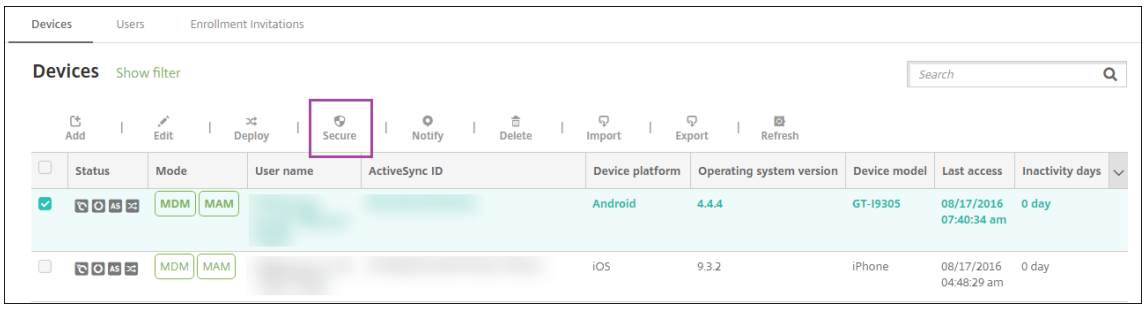
要在锁定的设备上显示消息和电话号码，请在 XenMobile 控制台中将通行码策略设置为 **true**。用户也可以手动在设备上启用通行码。

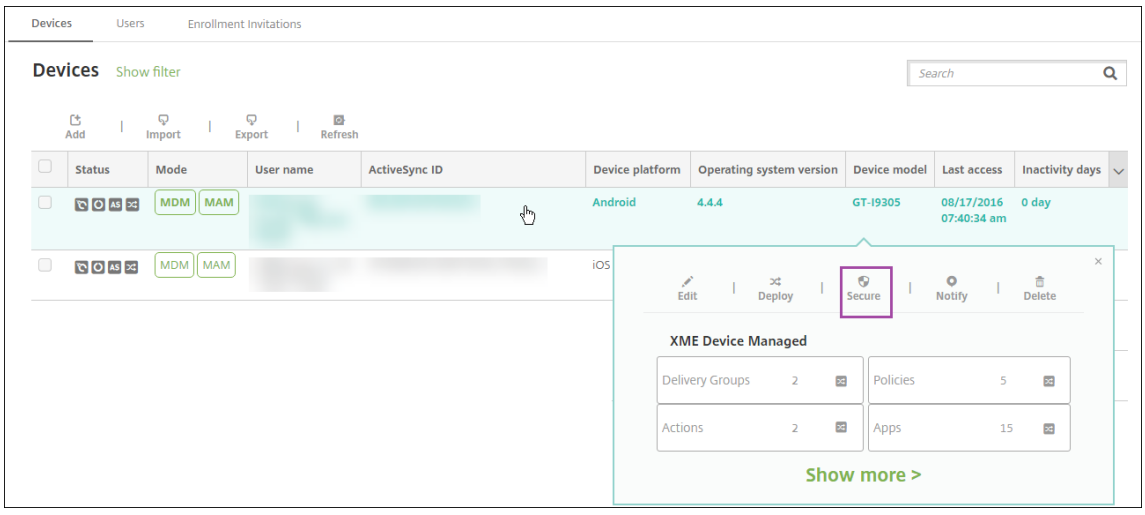
1. 单击管理 **>** 设备。此时将显示设备页面。



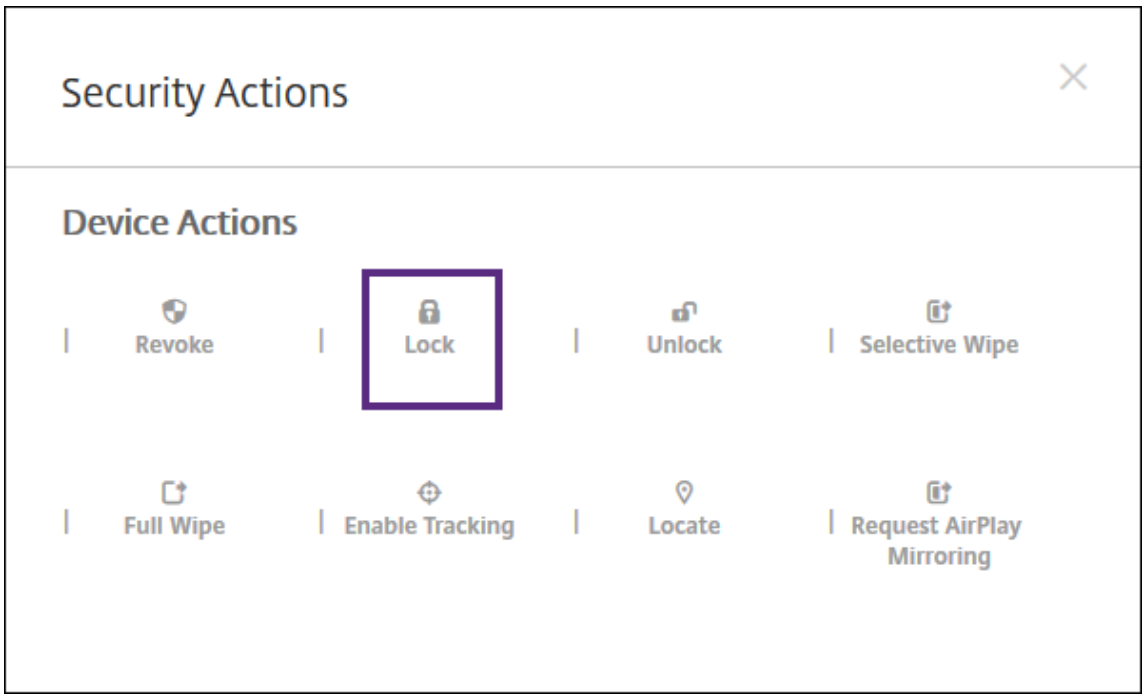
2. 选择要锁定的 iOS 设备。

   选中某个设备旁边的复选框时，选项菜单将在设备列表上方显示。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。

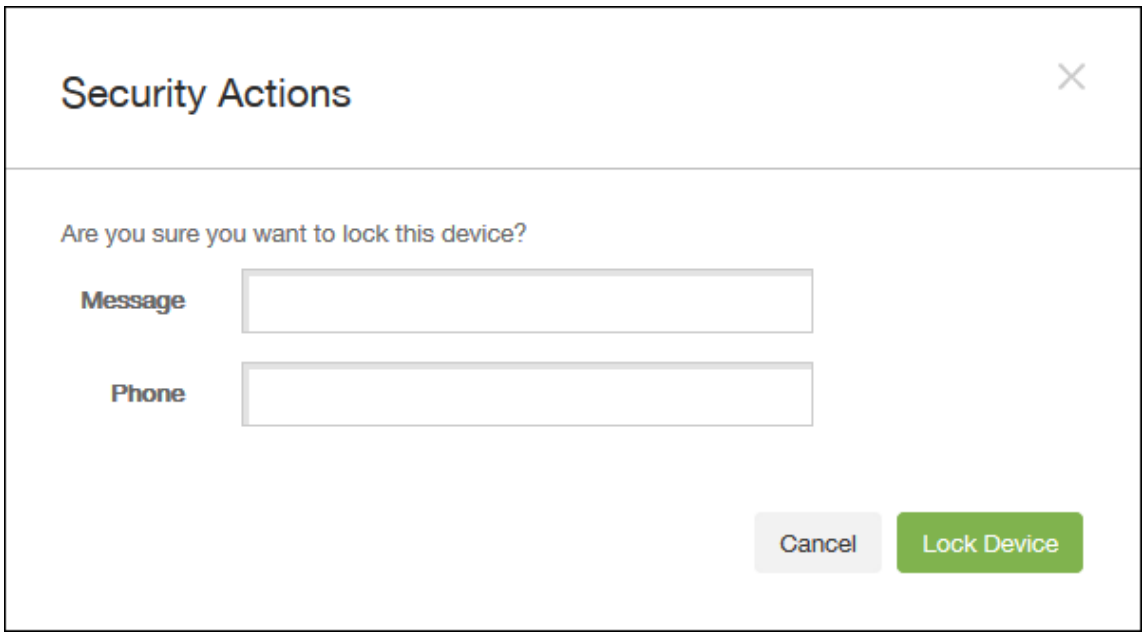




3. 在选项菜单中，选择安全。此时将显示安全操作对话框。



4. 单击锁定。此时将显示安全操作确认对话框。



5. （可选）键入将显示在设备锁屏界面上的消息和电话号码。

   对于运行 iOS 7 及更高版本的 iPad：iOS 会将“丢失的 iPad”字样附加到您在消息字段中键入的内容后。

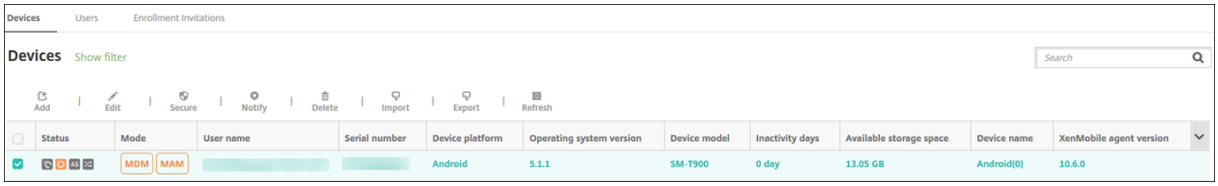
   对于运行 iOS 7 及更高版本的 iPhone：如果将消息字段留空，并提供电话号码，Apple 将在设备锁屏界面上显示消息“呼叫所有者”。

6. 单击锁定设备。

从 **XenMobile** 控制台中删除设备

> 重要：
>
> 从 XenMobile 控制台中删除设备时，托管应用程序和数据仍保留在设备上。要从设备中删除托管应用程序和数据，请参阅本文后面的“删除设备”部分。

要从 XenMobile 控制台中删除某个设备，请转至管理 > 设备，选择一个托管设备，然后单击删除。



选择性擦除设备

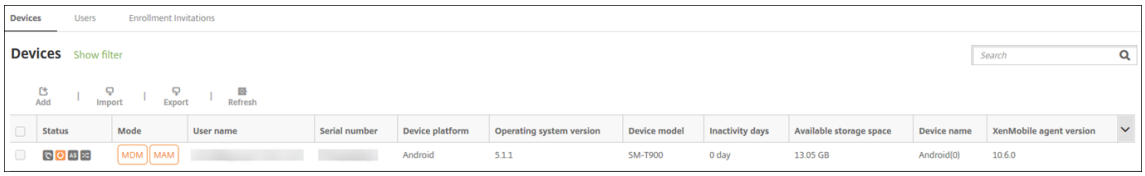
1. 转至管理 > 设备，选择一个托管设备，然后单击安全。
2. 在安全操作中，单击选择性擦除。
3. 仅限 Android 设备：要断开设备与企业网络的连接，请在擦除设备后，在安全操作中，单击吊销。

   要在擦除之前撤回选择性擦除请求，请在安全操作中，单击取消选择性擦除。

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 XenMobile 控制台的设备列表中删除设备。可以使用 Endpoint Management 公共 REST API 批量删除设备。

1. 转至管理 > 设备，选择一个托管设备，然后单击安全。
2. 单击选择性擦除。系统提示时，单击执行选择性擦除。
3. 要验证擦除命令是否成功，请刷新管理 > 设备。在模式列中，琥珀色的 MDM 和 MAM 指示擦除命令成功。



4. 在管理 > 设备中，选择设备，然后单击删除。系统提示时，再次单击删除。

锁定、解锁、擦除或取消擦除应用程序

1. 转至管理 > 设备，选择一个托管设备，然后单击安全。
2. 在安全操作中，单击应用程序操作。

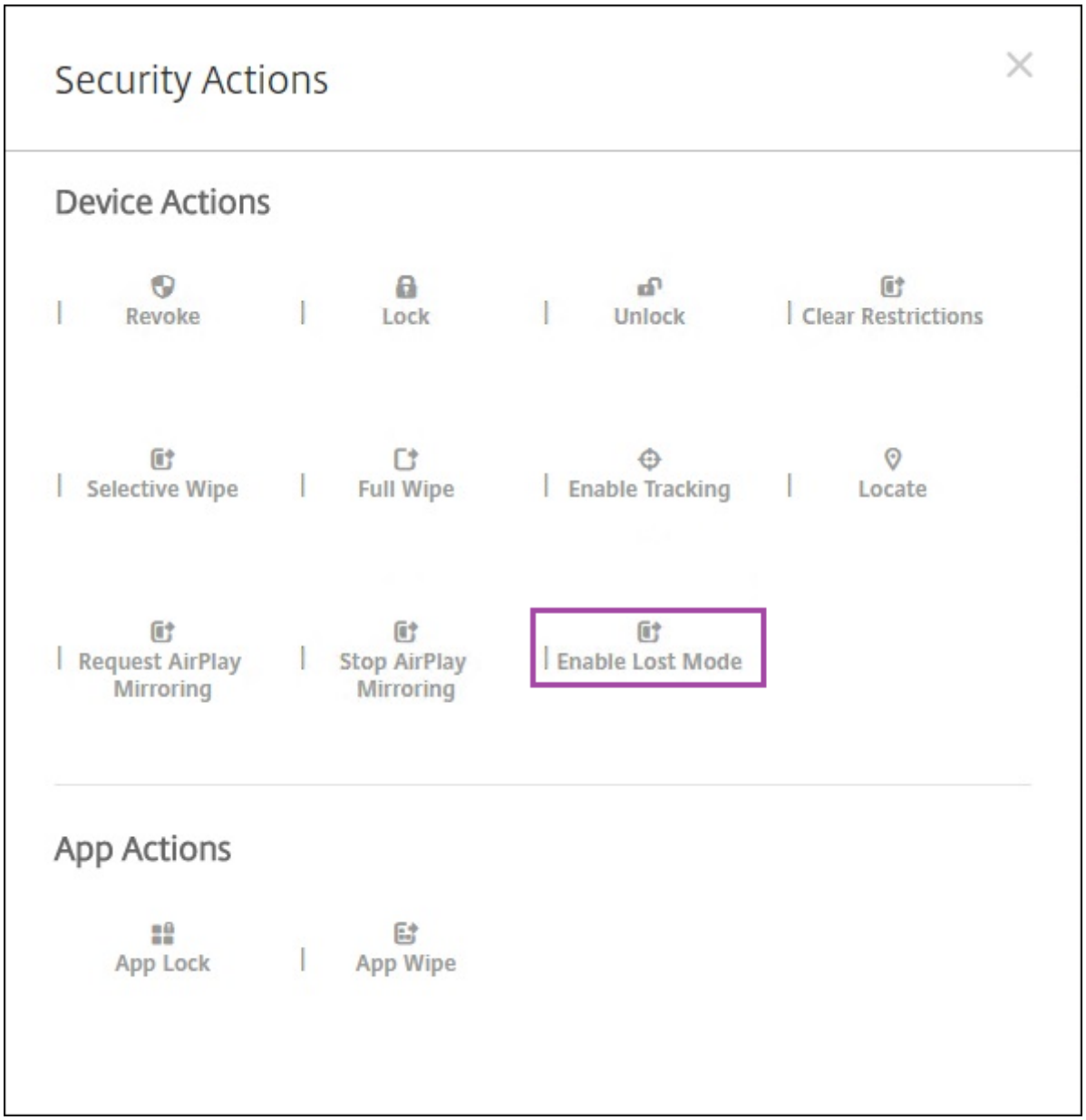
   还可以使用安全操作对话框检查已禁用或从 Active Directory 中删除其帐户的用户的设备状态。如果存在“应用程序解锁”操作或“应用程序取消擦除”操作，则表明应用程序已被锁定或擦除。

将 **iOS** 设备置于丢失模式

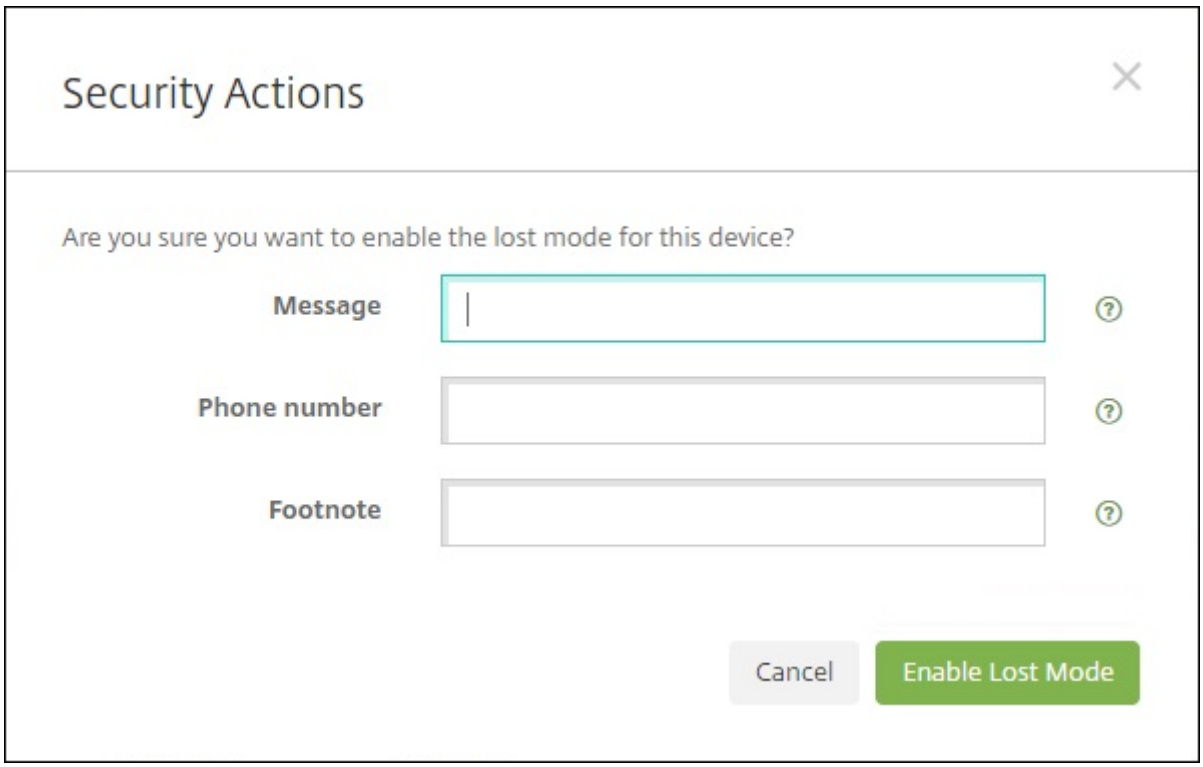
XenMobile 丢失模式设备属性将 iOS 设备置于丢失模式。与 Apple 托管丢失模式不同，XenMobile 丢失模式不要求用户执行以下任一操作来启用定位其设备：配置查找我的 **iPhone/iPad** 设置或为 Citrix Secure Hub 启用定位服务。

在 XenMobile 丢失模式下，只有 XenMobile Server 能够解锁设备。（与此相反，如果您使用 XenMobile 设备锁定功能，用户可以使用您提供的 PIN 代码直接解锁设备。

要启用或禁用丢失模式，请转至管理 **>** 设备，选择受监督的 iOS 设备，并单击安全。然后，单击启用丢失模式或禁用丢失模式。

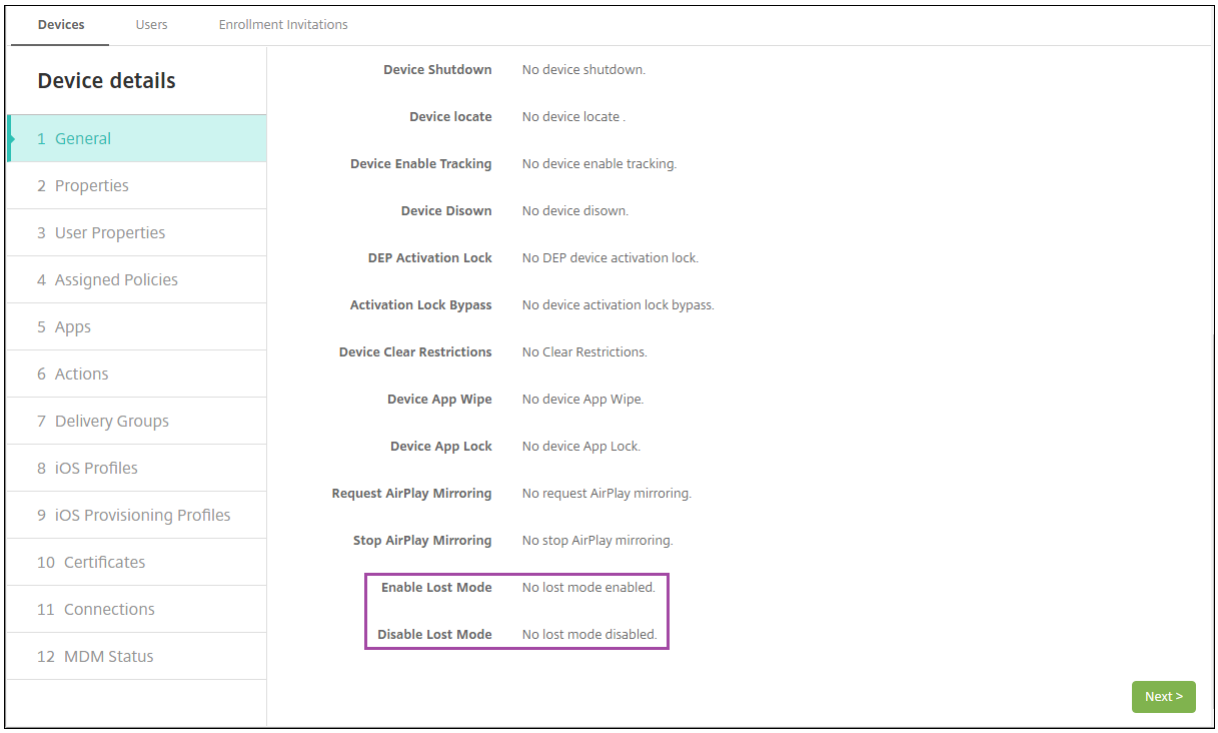


如果单击启用丢失模式，请键入设备处于丢失模式时要在设备上显示的信息。

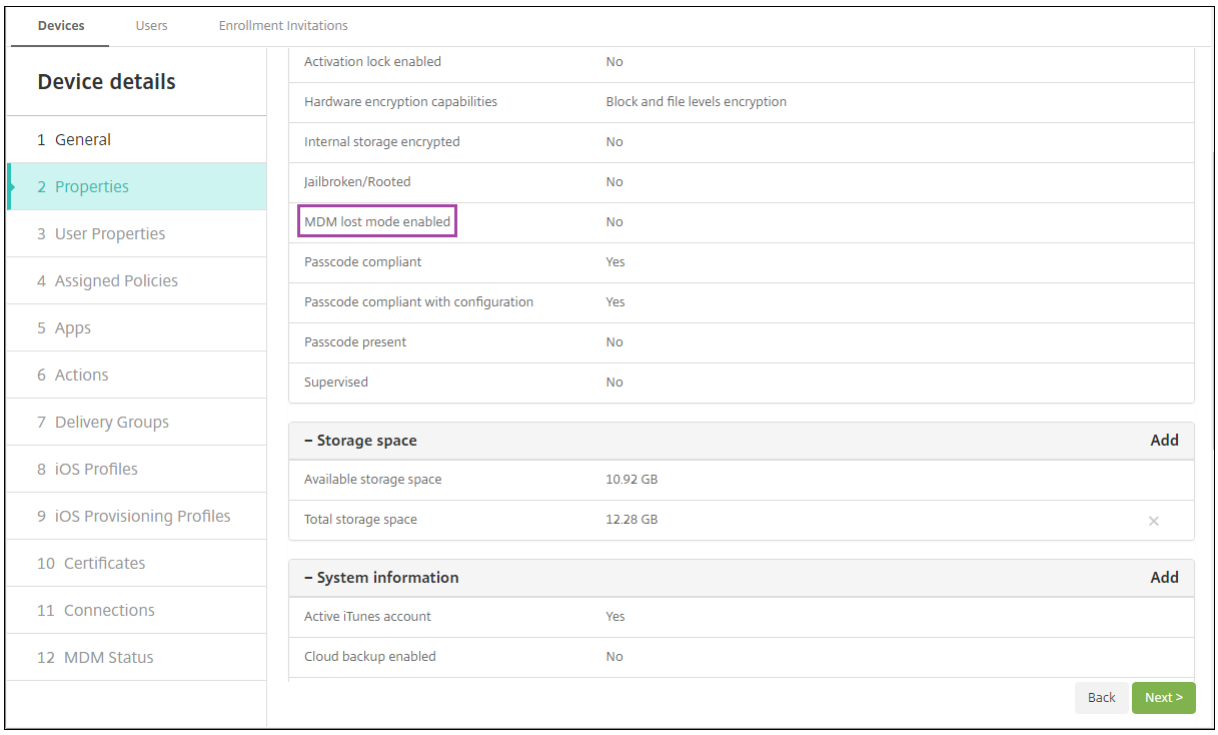


可使用以下任何方法来检查丢失模式状态：

- 在安全操作窗口中，确认按钮是否为禁用丢失模式。
- 在管理 **>** 设备中常规选项卡上的安全下方，查看最后一次“启用丢失模式”或“禁用丢失模式”操作。



- 在管理 **>** 设备中的属性选项卡上，确认已启用 **MDM** 丢失模式设置的值是否正确。



如果在 iOS 设备上启用 XenMobile 丢失模式，XenMobile 控制台也会更改，如下所示：

- 在配置 **>** 操作中，操作列表不包括这些自动化操作：吊销设备、选择性擦除设备和完全擦除设备。
- 在管理 **>** 设备中，安全操作列表不再包括吊销和选择性擦除设备的操作。您仍可以根据需要使用安全操作来执行完全擦除操作。

对于运行 iOS 7 及更高版本的 iPad：iOS 会将 “丢失的 iPad” 字样附加到您在安全操作屏幕的消息中输入的内容后。

对于运行 iOS 7 及更高版本的 iPhone：如果将消息留空，并提供一个电话号码，Apple 将在设备锁屏界面上显示消息 “呼叫所有者”。

绕过 **iOS** 激活锁

激活锁是一项 “查找我的 iPhone/iPad” 功能，用于阻止重新激活丢失或被盗的受监督设备。激活锁需要用户的 Apple ID 和密码，之后用户才能禁用 “查找我的 iPhone/iPad”、擦除设备或重新激活设备。对于组织拥有的设备，绕过激活锁是（例如）重置或重新分配设备的必要操作。

要启用激活锁，请配置并部署 XenMobile MDM 选项设备策略。之后可以从 XenMobile 控制台管理设备，而不需要用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 XenMobile 控制台发出 “激活锁绕过” 安全操作。

例如，如果用户在执行完全擦除操作之前或之后归还了丢失的手机或设置了设备：手机提示输入 iTunes 帐户凭据时，可以通过从 XenMobile 控制台发出 “激活锁绕过” 安全操作来绕过该设置。

激活锁绕过的设备要求

- iOS 7.1（最低版本）

- 通过 Apple Configurator 或 Apple DEP 进行监督
- 配置了 iCloud 帐户
- 已启用 “查找我的 iPhone/iPad”
- 已在 XenMobile 中注册
- “MDM 选项” 设备策略（启用了激活锁）已部署到设备

要在发出设备的完全擦除操作之前绕过激活锁，请执行以下操作：

1. 转至管理 **>** 设备，选择设备，单击安全，然后单击激活锁绕过。
2. 擦除设备。激活锁屏幕在设备设置过程中不显示。

要在发出设备的完全擦除操作之后绕过激活锁，请执行以下操作：

1. 重置或擦除设备。激活锁屏幕在设备设置过程中显示。
2. 转至管理 **>** 设备，选择设备，单击安全，然后单击激活锁绕过。
3. 轻按设备上的 “返回” 按钮。此时将显示主屏幕。

请紧急以下几点：

- 建议您的用户不要禁用 “查找我的 iPhone/iPad”。请勿从设备执行完全擦除操作。在这些情况下，系统将提示用户输入 iCloud 帐户密码。验证帐户后，用户在擦除所有内容和设置后将看不到 “激活 iPhone/iPad” 屏幕。
- 对于具有生成的激活锁绕过码并且启用了激活锁的设备：如果在执行完全擦除操作后无法绕过 “激活 iPhone/iPad” 页面，则不需要从 XenMobile 中删除设备。您或用户可以联系 Apple 技术支持人员来直接解锁设备。
- 确认硬件清单过程中，XenMobile 将查询设备中是否存在激活锁绕过码。如果绕过码可用，设备会将其发送到 XenMobile。之后，要从设备中删除绕过码，请从 XenMobile 控制台发送 “激活锁绕过” 安全操作。此时，XenMobile Server 和 Apple 将具有解锁设备所需的绕过码。
- “激活锁绕过” 安全操作依赖 Apple 服务的可用性。如果该操作无法运行，您可以按如下所示解锁设备。在设备上，手动输入 iCloud 帐户的凭据。或者，将 “用户名” 字段留空，并在 “密码” 字段中键入绕过码。要查找绕过码，请转至管理 **>** 设备，选择设备，单击编辑，然后单击属性。激活锁绕过码显示在安全信息下。

共享设备

January 5, 2022

XenMobile 允许您配置可由多个用户共享的设备。例如，利用共享设备功能，医院的临床医生可以使用附近的任何设备访问应用程序和数据，而无需随身携带特定设备。您可能还希望执法、零售和制造等领域的工作者转向使用共享设备，以降低装备成本。

关于共享设备的要点

可以将支持的任何 iOS 和 Android 设备用作共享设备。有关支持的设备列表，请参阅支持的设备操作系统。

MDM 注册

- 可在 iOS 和 Android 平板电脑和手机上使用。不支持面向 XenMobile Enterprise 共享设备的基本 Apple 部署计划注册。使用经过授权的 Apple 部署计划在此模式下注册共享设备。
- 不支持客户端证书身份验证、Citrix PIN、Touch ID、用户熵和双重身份验证。

MDM+MAM 注册

- 仅适用于 iOS 和 Android 设备。
- 仅支持 Active Directory 用户名和密码身份验证。
- 不支持客户端证书身份验证、Secure Hub 通行码、Touch ID、用户熵和双重身份验证。
- 不支持仅 MAM 注册。设备必须在 MDM 下注册。
- 仅支持 Secure Mail、Secure Web 和 ShareFile 移动应用程序。不支持 HDX 应用程序。
- 仅支持 Active Directory 用户。不支持本地用户和组。
- 要更新为 MDM+MAM，需要重新注册现有的仅 MDM 共享设备。
- 用户无法共享设备上的本机应用程序。
- 在首次注册期间下载后，移动生产力应用程序不会在用户登录期间再次下载。
- 在 Android 上，出于安全考虑，要隔离每个用户的数据，请在 XenMobile 控制台中将 **Disallow rooted devices**（不允许已获得 Root 权限的设备）策略设置为开。

注册共享设备的必备条件

您必须先执行以下操作，才能注册共享设备：

- 创建共享设备注册用户角色。请参阅使用 RBAC 配置角色。
- 创建共享设备用户。请参阅添加、编辑、解锁或删除本地用户帐户。
- 创建包含要应用到共享设备用户的基本策略、应用程序和操作的交付组。请参阅部署资源。

MDM+MAM 注册的必备条件

1. 创建 Active Directory 组。为其指定描述性名称，例如共享设备注册程序。
2. 将注册共享设备的 Active Directory 用户添加到此组。如果要使用一个专用于注册共享设备的新帐户，请创建新的 Active Directory 用户（例如 **sdenroll**），并将该用户添加到 Active Directory 组。

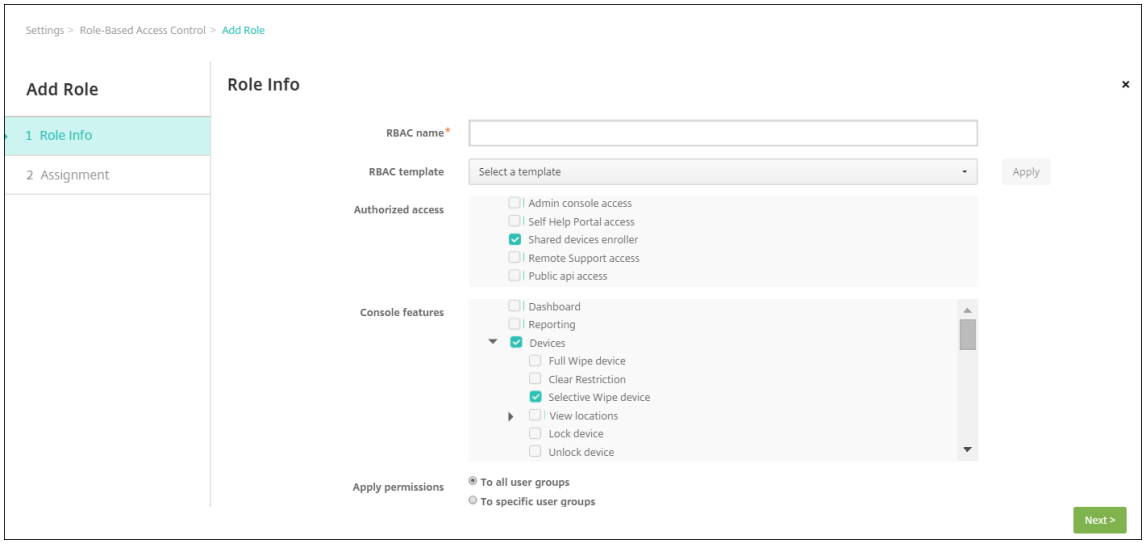
配置共享设备

按照以下步骤配置共享设备。

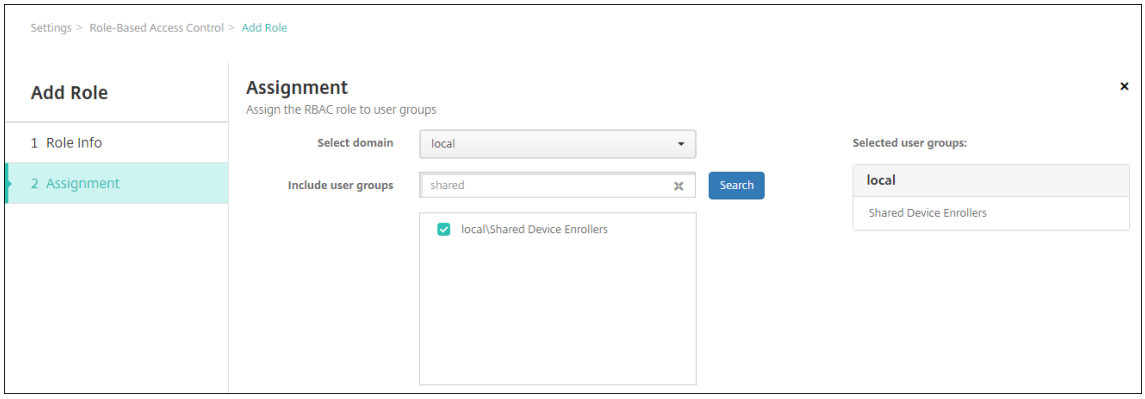
1. 从 XenMobile 控制台，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击基于角色的访问控制，然后单击添加。此时将显示添加角色屏幕。

3. 创建一个名为共享设备注册用户的共享设备注册用户角色，并在授权访问下选择共享设备注册人员权限。请务必在控制台功能中展开设备，然后选择选择性擦除设备。此设置可确保在取消注册设备后，可通过 Secure Hub 删除使用共享设备注册人员帐户预配的应用程序和策略。

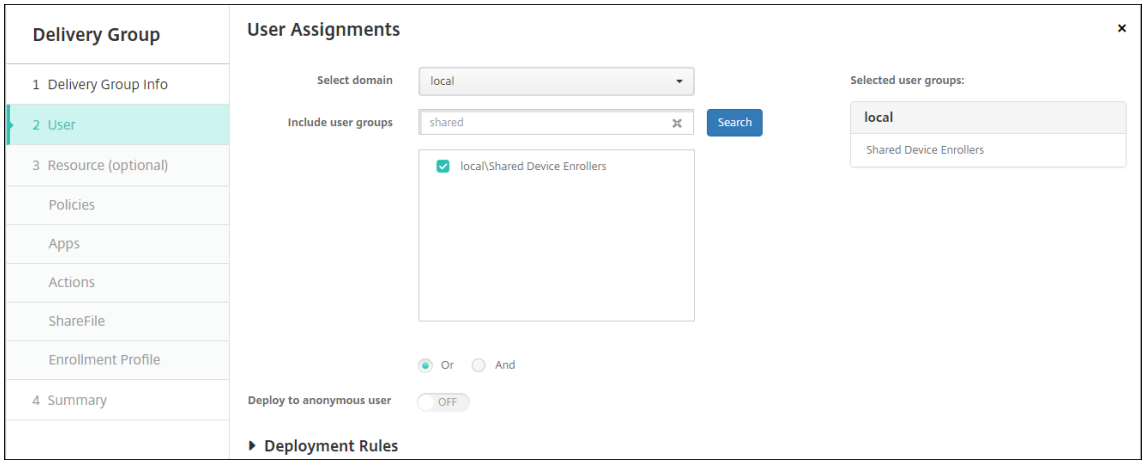
   对于应用权限，保留默认设置至所有用户组，或使用至特定用户组向特定 Active Directory 用户组分配权限。



   单击下一步以转至分配屏幕。将共享设备注册角色分配给在“必备条件”下的步骤 1 中为共享设备注册用户创建的 Active Directory 组。在下图中，**citrix.lab** 是 Active Directory 域，共享设备注册人员是 Active Directory 组。



4. 创建一个交付组，其中包含在用户未登录时要应用于设备的基本策略、应用程序和操作。然后，将该交付组与共享设备注册用户的 Active Directory 组关联。



5. 在共享设备上安装 Secure Hub，然后使用共享设备注册用户帐户将其注册到 XenMobile 中。现在即可通过 XenMobile 控制台查看并管理设备。有关详细信息，请参阅注册设备。
6. 要应用不同的策略或为已通过身份验证的用户提供更多应用程序，必须创建与这些用户关联且仅部署到共享设备的交付组。在创建交付组时，请配置相应的部署规则，以确保将软件包部署到共享设备。有关详细信息，请参阅部署资源。
7. 要停止共享设备，请执行选择性擦除操作，以从设备中删除共享设备注册用户帐户。删除部署到设备的所有应用程序和策略。

共享设备用户体验

MDM 注册

用户只会看到他们可用的资源，而且在每个共享设备上都能获得同样的使用体验。共享设备注册策略和应用程序会始终保留在设备上。当未在共享设备中注册的用户登录到 Secure Hub 时，该用户的策略和应用程序将部署到设备中。当该用户注销时，系统将删除不属于共享设备注册的任何策略和应用程序。共享设备注册资源则完好无损。

MDM+MAM 注册

Secure Mail 和 Secure Web 将在由共享设备注册用户注册后部署到设备中。用户数据会安全地保留在设备上。当其他用户登录到 Secure Mail 或 Secure Web 时，系统不会将这些数据公开给这些用户。

一次只能有一个用户登录到 Secure Hub。上一个用户必须注销，下一个用户才能登录。出于安全原因，Secure Hub 不在共享设备上存储用户凭据，因此用户必须在每次登录时输入其凭据。Secure Hub 会阻止新登录，直至其删除与之前用户关联的策略、应用程序和数据。

共享设备注册不会更改应用程序升级过程。您可以照常将升级推送给共享设备的用户，而共享设备的用户可以直接在其设备上升级应用程序。

建议的 **Secure Mail** 策略

- 为了获得最佳 Secure Mail 性能，请根据要共享设备的用户数设置 **Max sync period**（最长同步期限）。不建议允许无限同步。

共享设备的用户数量	建议的最长同步期限
21–25	1 周或更短
6–20	2 周或更短
5 或更少	1 个月或更短

- 阻止启用联系人导出以避免向共享设备的其他用户公开用户的联系人。
- 在 iOS 上，只能基于用户设置以下设置。所有其他设置都是共享该设备的用户通用的：
  - 通知
  - 签名
  - 外出
  - 同步邮件期限
  - S/MIME
  - 检查拼写

XenMobile 自动发现服务

January 5, 2022

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

使用自动发现服务，用户可以：

- 可以使用公司网络凭据注册其设备。
- 无需输入有关 XenMobile Server 地址的详细信息。
- 以用户主体名称 (UPN) 格式输入其用户名。例如，`user@mycompany.com`。

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

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

必备条件

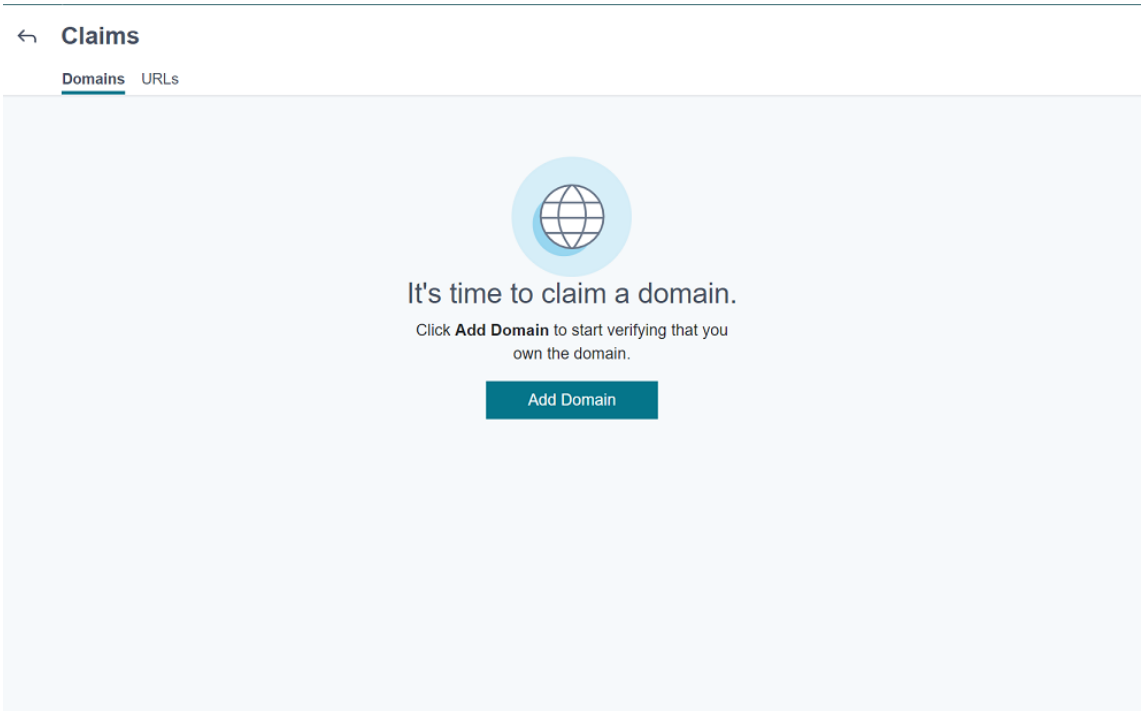
- Citrix Cloud 中的新自动发现服务需要最新版本的 Secure Hub：
  - 对于 iOS，Secure Hub 版本 21.6.0 或更高版本
  - 对于 Android，Secure Hub 版本 21.8.5 或更高版本

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

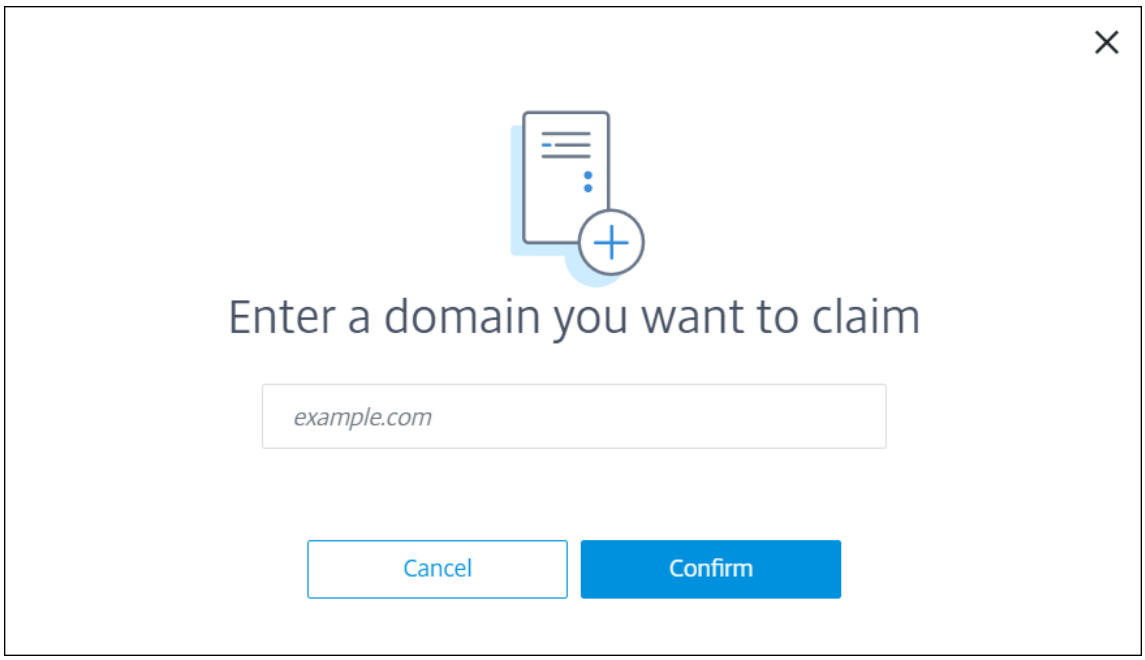
  Citrix 在不中断服务的情况下将所有现有的自动发现记录迁移到 Citrix Cloud。迁移的记录不会自动显示在新控制台中。必须在新的自动发现服务中回收域才能证明所有权。有关详细信息，请参阅 CTX312339。
- 在开始将自动发现服务用于 Endpoint Management 部署之前，请验证并声明您的域。最多可以声明 10 个域。该声明将已验证的域与自动发现服务相关联。要声明超过 10 个域，请开立 SRE 票证或联系 Citrix 技术支持。
- 请使用 MAM 端口设置（而非 Citrix Gateway FQDN）将 MAM 流量定向到您的数据中心。如果输入完全限定的域名以及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

声明域

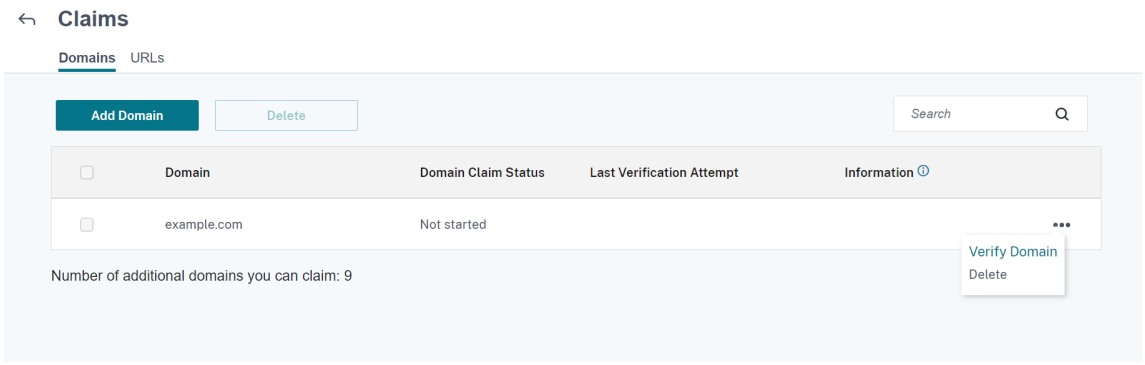
1. 在声明 **>** 域选项卡上，单击添加域。



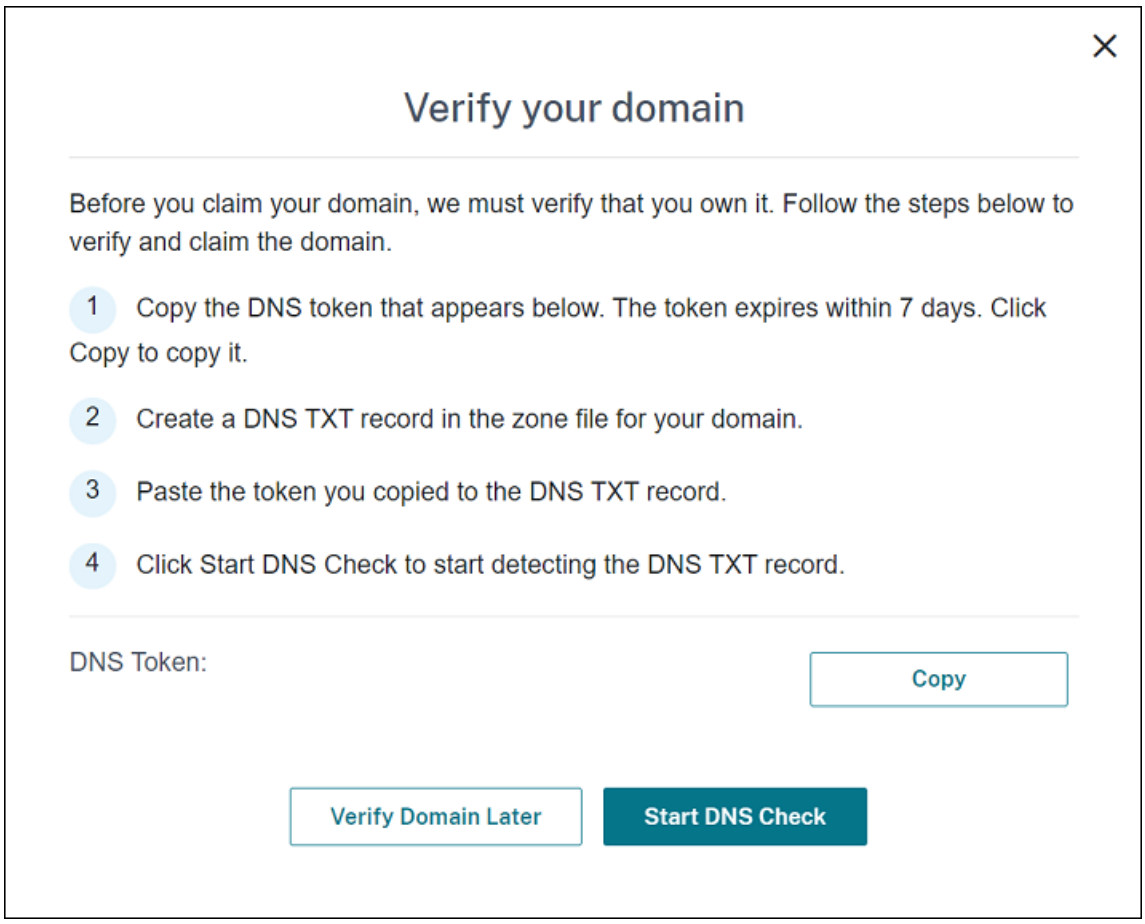
2. 在显示的对话框中，输入 XenMobile 环境的域名，然后单击确认。您的域名将显示在声明 **>** 域中。



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



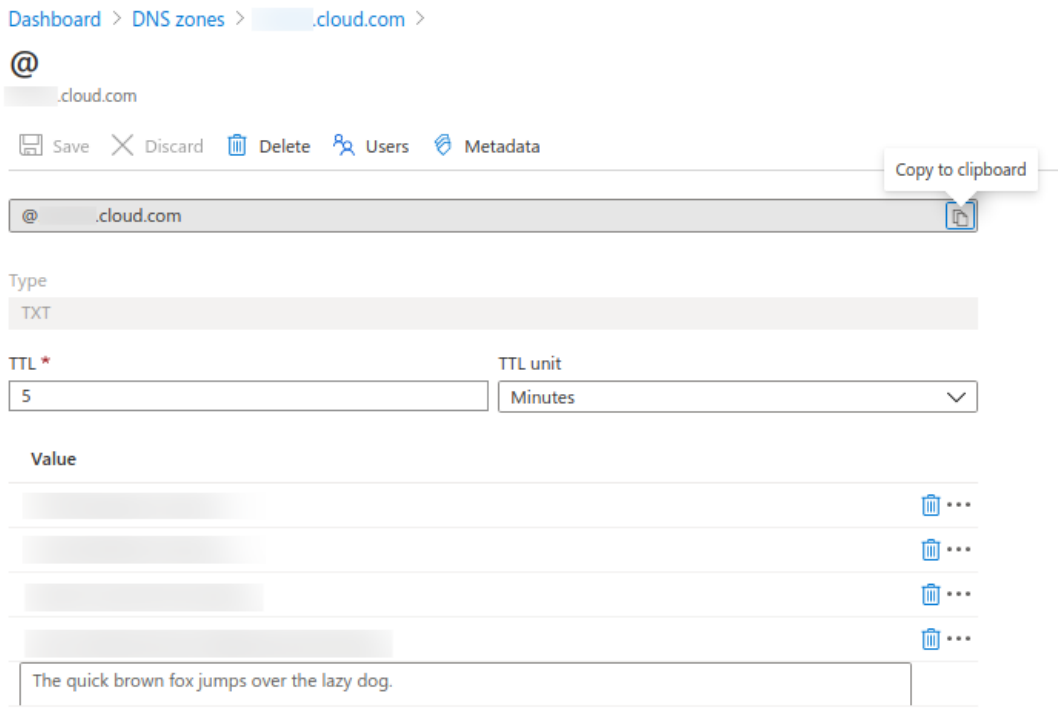
4. 在 **Verify your domain**（验证您的域）页面上，按照说明进行操作以验证您是否拥有该域。



a) 单击 **Copy**（复制）将 DNS 令牌复制到剪贴板。

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

下面的屏幕截图显示了托管提供商门户网站的域。您的门户可能看起来有所差别。



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

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

配置完成后，域的状态将从挂起更改为已验证。

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

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

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

请求 **Windows** 设备的自动发现

如果计划注册 Windows 设备，请执行以下操作：

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

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

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

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

   - 提供 XenMobile Server 的详细信息。
   - 指示设备向 XenMobile 请求有效证书。

此时，您可以注册所有受支持的设备。继续下一部分，准备向设备提供资源。

设备策略

January 5, 2022

可以通过创建策略，配置 XenMobile 与您的设备的交互方式。尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。因此，您可能会发现平台之间的差异，甚至 Android 设备的不同制造商之间的差异。

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 设备配置 XenMobile 设备策略时，请记住以下规则。如果已注册的一台或多

> 台设备上的某个策略冲突，则优先应用与 GPO 对应的策略。

要查看 Android Enterprise 容器支持的策略，请参阅 Android Enterprise。

必备条件

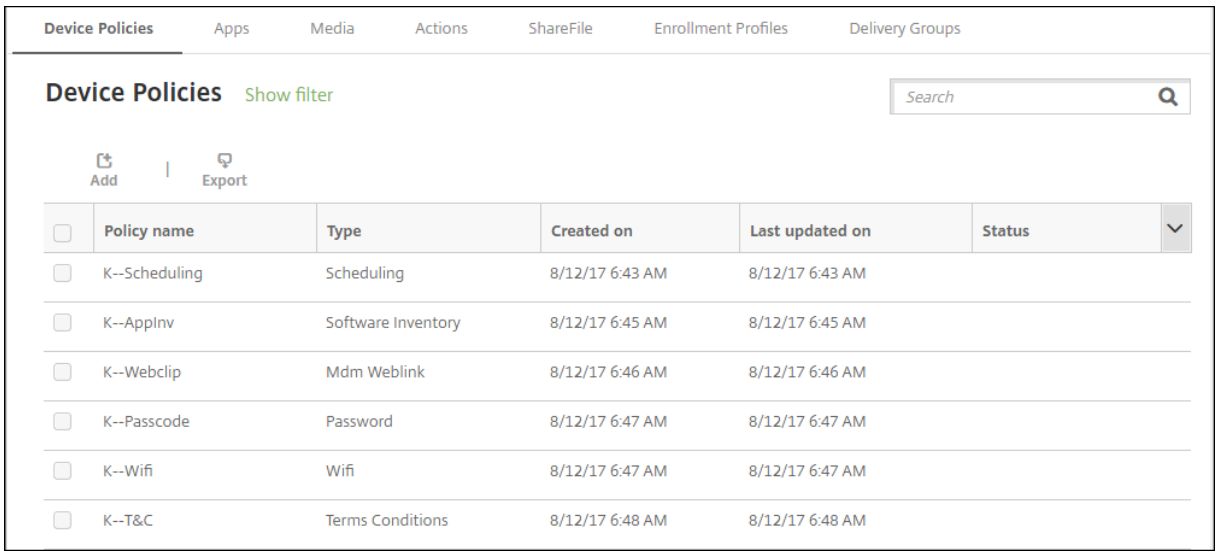
- 创建计划使用的交付组。
- 安装所有必需的 CA 证书。

添加设备策略

创建设备策略的基本步骤如下：

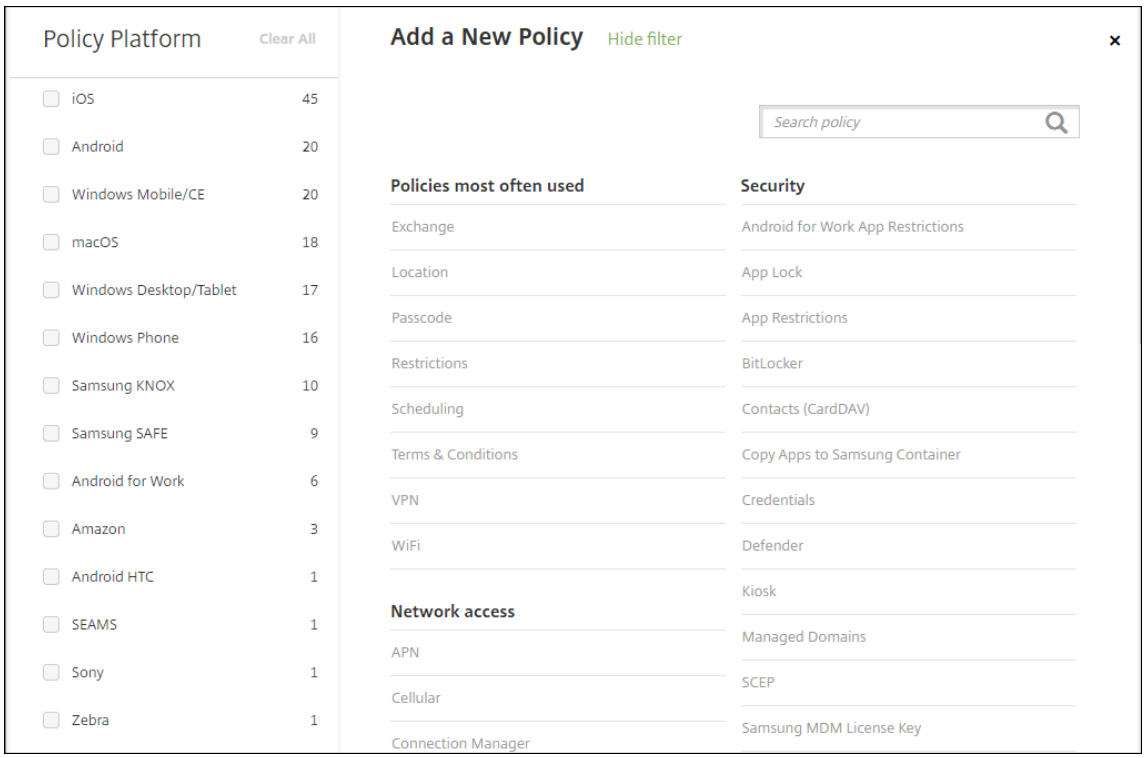
1. 为策略命名并添加说明。
2. 为一个或多个平台配置策略。
3. 创建部署规则（可选）。
4. 将策略分配到交付组。
5. 配置部署计划（可选）。

要创建和管理设备策略，请转到配置 **>** 设备策略。

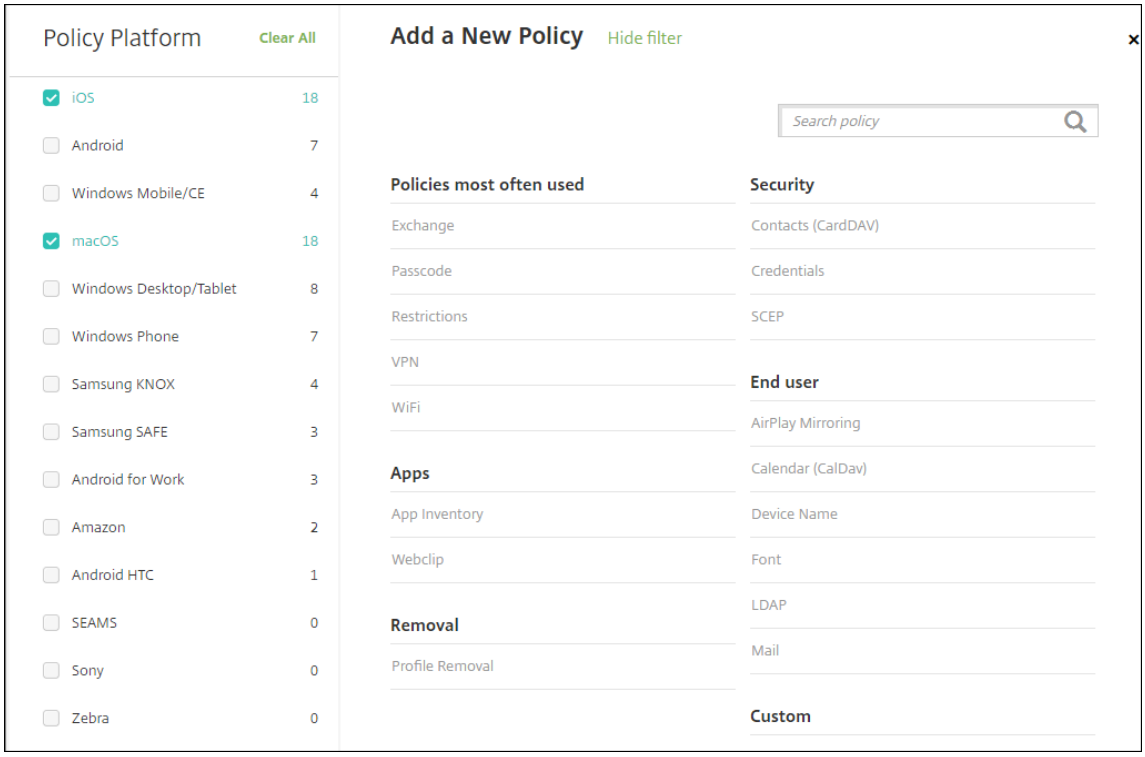


要添加策略，请执行以下操作：

1. 在设备策略页面上，单击添加。将显示添加新策略页面。



2. 单击一个或多个平台可查看适用于选定平台的设备策略的列表。单击某个策略名称可继续添加该策略。



还可以在搜索框中键入策略的名称。随着键入，将显示可能的匹配项。如果列表中存在您的策略，请单击此策略。只有选中的策略保留在结果中。单击此策略以打开其策略信息页面。

3. 选择要包含在策略中的平台。选定平台的配置页面显示在步骤 5 中。
4. 完成策略信息页面，然后单击下一步。策略信息页面收集策略名称等信息，以帮助您识别和跟踪自己的策略。此页面在所有策略之间相似。
5. 完成平台页面。显示在步骤 3 选择的每个平台的平台页面。这些页面因策略而异。策略可能会因平台而异。并非所有策略都适用于所有平台。

   一些页面包括项目表。要删除现有项目，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾桶图标。在确认对话框中，单击删除。

   要编辑现有项目，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。

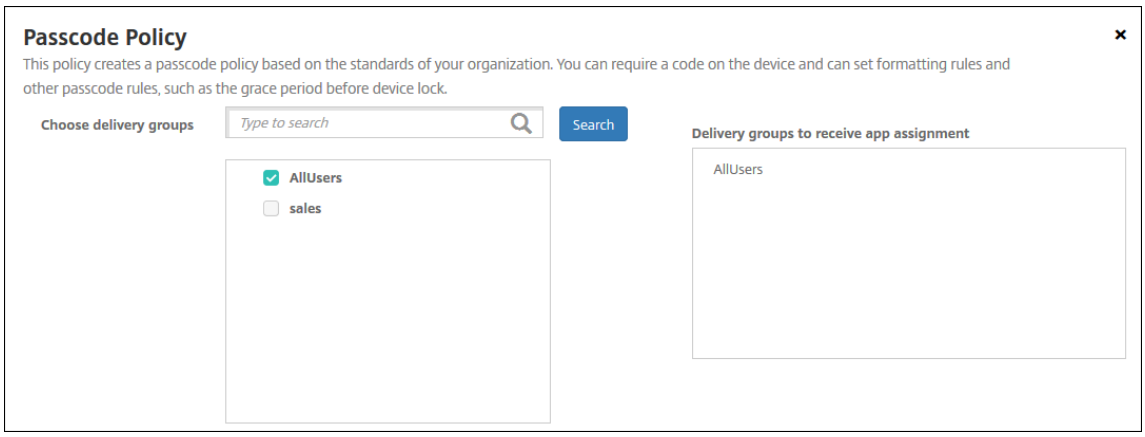
配置部署规则、分配和计划

有关配置部署规则的详细信息，请参阅部署资源。

1. 在平台页面上，展开部署规则，然后配置以下设置。默认情况下将显示基础选项卡。
   - 在此列表中，单击选项以确定部署策略的时间。可以选择在满足全部条件时部署策略，或在满足任意条件时部署策略。默认选项为全部。
   - 单击新建规则以定义条件。
   - 在列表中，单击条件，例如设备所有权和 **BYOD**。
   - 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。此时将显示您在基础选项卡上选择的条件。
3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   - 单击与、或或非。
   - 在列表中，选择要添加到规则的条件。然后单击右侧的加号 (**+**) 向规则添加条件。

     您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   - 单击新建规则添加其他条件。
4. 单击下一步移到下一个平台页面，或者在完成所有平台页面后移到分配页面。
5. 在分配页面上，选择要应用策略的交付组。如果单击某个交付组，此组将显示在用于接收应用程序分配的交付组框中。

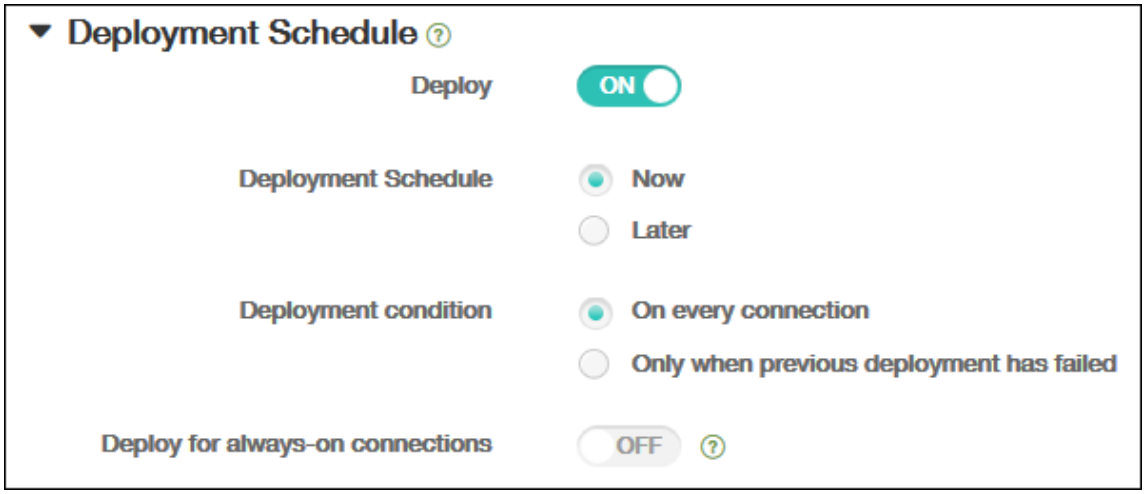
   用于接收应用程序分配的交付组在您选择某个交付组之后才显示。



6. 在分配页面上，展开部署计划，然后配置以下设置：

   - 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。
   - 在部署计划旁边，单击立即或以后。默认选项为立即。
   - 如果单击以后，请单击日历图标，然后选择部署的日期和时间。
   - 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
   - 在为始终启用的连接部署旁边，单击开或关。默认选项为关。

     > 注意：
     >
     > 如果在设置 > 服务器属性中配置了计划后台部署密钥，则适用此选项。始终启用选项不适用于 iOS 设备。
     >
     > 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。



7. 单击保存。

   该策略显示在设备策略表中。

从设备中删除设备策略

从设备中删除设备策略的步骤取决于平台。

- Android

  要从 Android 设备中删除设备策略，请使用 XenMobile 卸载设备策略。有关信息，请参阅 XenMobile 卸载设备策略。

- iOS 和 macOS

  要从 iOS 或 macOS 设备中删除设备策略，请使用“配置文件删除”设备策略。在 iOS 和 macOS 设备上，所有策略都属于 MDM 配置文件的一部分。因此，可以仅针对要删除的策略创建“配置文件删除”设备策略。策略和配置文件的其余部分仍保留在设备上。有关信息，请参阅“配置文件删除”设备策略。

- Windows 10 和 Windows 11

  不能直接从 Windows Desktop 或 Tablet 设备中删除设备策略。但是，可以使用以下方法之一：

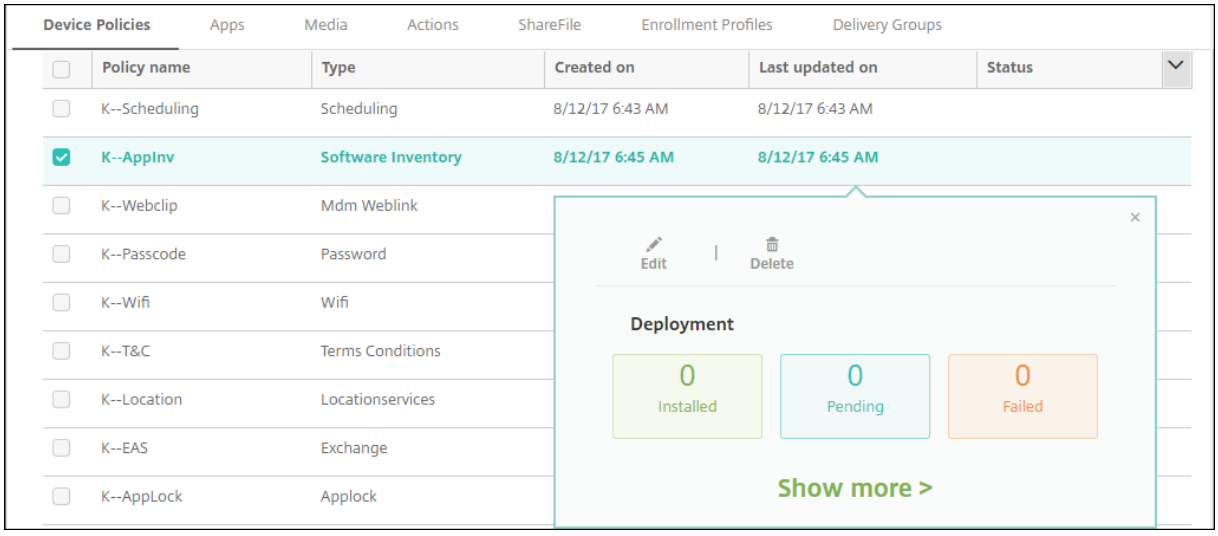
  - 取消注册设备，然后将新的一组策略推送到设备。用户随后将重新注册以继续。
  - 推送安全操作以选择性擦除特定设备。该操作将从设备中删除所有企业应用程序和数据。然后从仅包含该设备的交付组中删除设备策略，并将该交付组推送给设备。用户随后将重新注册以继续。

- Chrome OS

  要从 Chrome OS 设备中删除某个设备策略，可以从仅包含该设备的交付组中删除该设备策略。您随后将该交付组推送给设备。

编辑设备策略

要编辑某个策略，请选中策略旁边的复选框，以在策略列表上方显示选项菜单。或者单击列表中的某个策略，以在此列表右侧显示选项菜单。



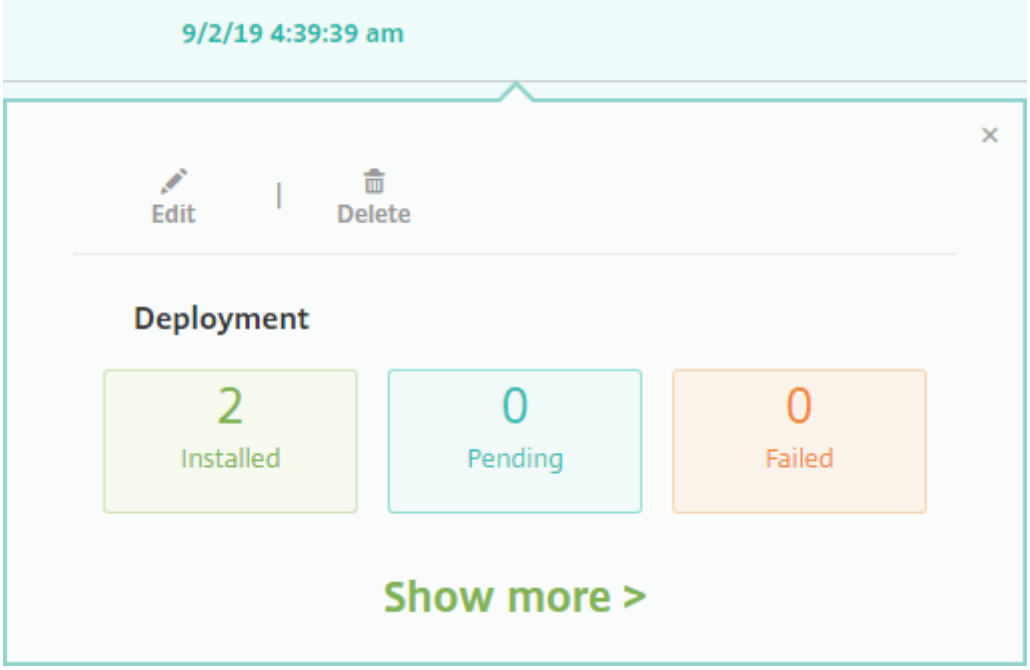
要查看策略详细信息，请单击显示更多。

要编辑某个设备策略的所有设置，请单击编辑。

如果单击删除，将显示确认对话框。再次单击删除以删除策略。

检查策略部署状态

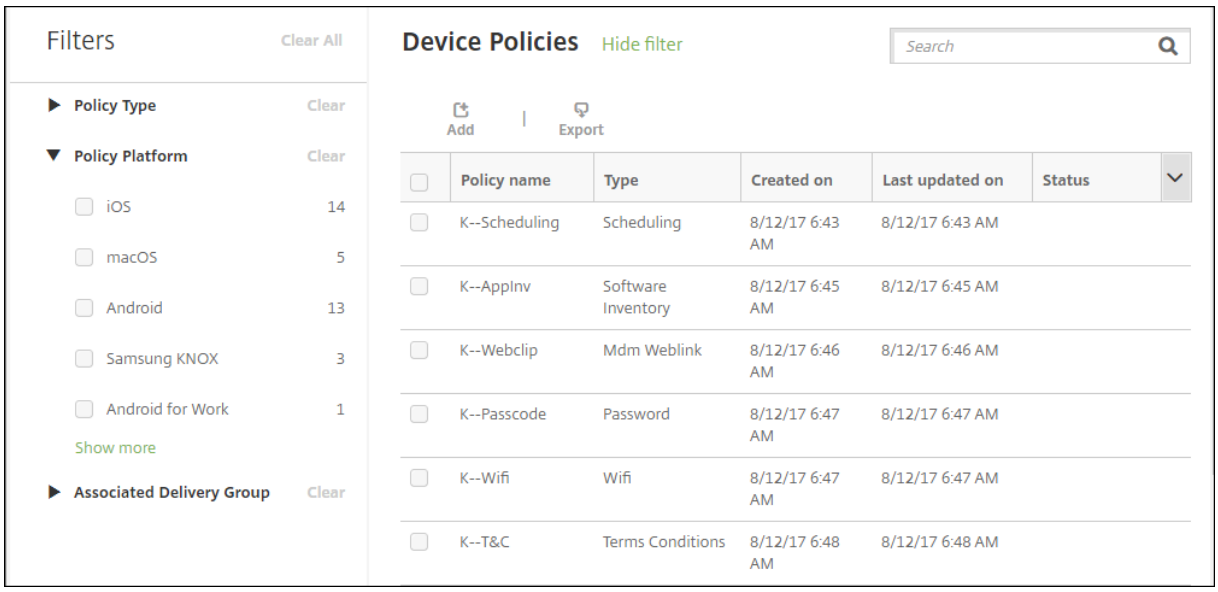
单击配置 **>** 设备策略页面上的策略行以检查其部署状态。



当策略部署处于挂起状态时，用户可以通过轻按首选项 **>** 设备信息 **>** 刷新策略从 Secure Hub 刷新策略。

过滤已添加的设备策略列表

可以按策略类型、平台和关联的交付组过滤已添加的策略列表。在配置 **>** 设备策略页面上，单击显示过滤器。在列表中，选择您要查看的项对应的复选框。



单击保存此视图以保存过滤器。之后过滤器的名称显示在保存此视图按钮下面的一个按钮中。

设备策略摘要

设备策略名称	设备策略说明
AirPlay 镜像	将特定 AirPlay 设备（例如其他 Mac 计算机）添加到 iOS 设备。还可以使用用于将设备添加到受监督设备的允许列表中的选项。该选项仅将用户限制到允许列表中的 AirPlay 设备。
AirPrint	将 AirPrint 打印机添加到 iOS 设备上的 AirPrint 打印机列表。通过此策略可以更加轻松地为打印机和设备位于不同子网的环境提供支持。
Android Enterprise 应用程序权限	配置对工作配置文件内部的 Android Enterprise 应用程序的请求如何处理 Google 称作 “危险” 权限的权限。
Android Enterprise 应用程序限制	更新与 Android 应用程序相关联的限制。
APN	确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。大多数新式电话中已定义此设置。如果贵组织不使用使用者 APN 从移动设备连接到 Internet，请使用此策略。
应用程序访问	定义设备上的必需、可选或受阻止应用程序的列表。然后，可以创建自动化操作，以使设备符合此应用程序列表。

设备策略名称	设备策略说明
应用程序属性	为 iOS 设备指定各种属性，例如托管应用程序捆绑包 ID 或 PerApp VPN 标识符。
应用程序配置	远程配置支持托管配置的应用程序的各种设置和行为。为此，您要将 XML 配置文件（称为属性列表或 plist）部署到 iOS 设备。或者，您可以为 Windows 10 Phone 或者运行 Windows 10 或 Windows 11 的台式机或平板电脑设备部署键/值对。
应用程序清单	收集托管设备上的应用程序清单。之后 XenMobile 将清单与部署到这些设备的任何应用程序访问策略进行比较。这样一来，便可以检测应用程序访问允许列表或阻止列表中的应用程序，然后采取相应操作。
应用程序锁定	定义用户可以或无法在 iOS 或某些 Android 设备上运行的应用程序列表。
应用程序网络使用	设置网络使用规则，以指定 iOS 设备上托管应用程序如何使用网络（例如手机网络数据网络）。规则仅适用于托管应用程序。托管应用程序是指您通过 XenMobile 部署到用户设备的应用程序。
应用程序限制	创建您要阻止用户在 Samsung KNOX 设备上执行安装操作的应用程序的阻止列表。还可以为用户能够安装的应用程序创建允许列表。
应用程序卸载	从用户设备中删除应用程序。
应用程序卸载限制	指定用户可以或无法卸载的应用程序。
应用程序通知	控制 iOS 用户如何从指定的应用程序接收通知。
自动更新托管应用程序	控制 Android Enterprise 设备上安装的托管应用程序的更新方式。
BitLocker	配置在 Windows 10 和 Windows 11 设备上的 BitLocker 界面中可用的设置。
浏览器	定义用户设备是否可以使用浏览器或设备可以使用的浏览器功能。
日历 (CalDav)	将日历 (CalDAV) 帐户添加到 iOS 或 macOS 设备。使用 CalDAV 帐户，用户可以将计划数据与支持 CalDAV 的任何服务器同步。
手机网络	配置手机网络设置。

设备策略名称	设备策略说明
连接管理器	为自动连接到 Internet 和专用网络的应用程序指定连接设置。此策略仅适用于 Windows Pocket PC。
联系人 (CardDAV)	将 iOS 联系人 (CardDAV) 帐户添加到 iOS 或 macOS 设备。使用 CardDAV 帐户，用户可以将联系人数据与支持 CardDAV 的任何服务器同步。
控制操作系统更新	将最新的操作系统更新部署到支持的受监督设备。
将应用程序复制到 Samsung 容器	将已在设备上安装的应用程序复制到受支持的 Samsung 设备上的 KNOX 容器。复制到 KNOX 容器的应用程序仅当用户登录 KNOX 容器时可用。
凭据	启用使用 XenMobile 中的 PKI 配置进行集成身份验证。例如，使用 PKI 实体、密钥库、凭据提供程序或服务器证书。
自定义 XML	自定义设备预配、设备功能启用、设备配置和故障管理等功能。
Defender	配置 Windows 10 和 Windows 11 台式机和平板电脑的 Windows Defender 设置。
删除文件和文件夹	从 Windows Mobile/CE 设备中删除特定的文件或文件夹。
删除注册表项和值	从 Windows Mobile/CE 设备中删除特定的注册表项和值。
设备运行状况证明	需要 Windows 10 和 Windows 11 设备报告其运行状况的状态。为此，它们向 Health Attestation Service (HAS) 发送特定数据和运行时信息以供分析。HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 XenMobile。XenMobile 收到运行状况证明证书后，根据该证书的内容，部署您设置的自动操作。
设备名称	在 iOS 和 macOS 设备上设置名称，以便您可以轻松识别设备。可以使用宏、文本或二者的组合定义设备名称。
教育配置	配置教师和学生的设备以供 Apple 教育使用。如果教师使用“课堂”应用程序，则需要配置教育配置设备策略。

设备策略名称	设备策略说明
企业中心	通过企业中心公司应用商店将应用程序分发到 Windows Phone。对于一种 Windows Phone Secure Hub 模式，XenMobile 仅支持一种企业中心策略。例如，不要使用不同版本的 Secure Home for XenMobile Enterprise Edition 创建多个企业中心策略。只能在设备注册过程中部署初始企业中心策略。
Exchange	为设备上的本机电子邮件客户端启用 ActiveSync 电子邮件。
文件	将为用户执行某些功能的脚本文件添加到 XenMobile。或者，您可以添加您希望 Android 设备用户能够在其设备上访问的文档文件。添加文件时，还可以指定设备上要存储该文件的目录。
FileVault	此策略允许您在已注册的 macOS 设备上启用 FileVault 设备加密。还可以控制用户在登录过程中可以跳过 FileVault 设置的次数。适用于 macOS 10.7 或更高版本。
防火墙	配置防火墙设置。提供要在设备上允许或阻止的 IP 地址、端口和主机名。还可以配置代理和代理重新路由设置。
字体	在 iOS 和 macOS 设备上添加字体。字体必须是 TrueType (.TTF) 字体或 OpenType (.OFT) 字体。XenMobile 不支持字体集合（.TTC 或.OTC)。
主屏幕布局	指定 iOS 9.3 及更高版本的受监督设备上的 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 文件导入到 XenMobile 中。此文件包含您通过使用 Apple Configurator 准备的设备安全策略和限制。
键盘锁管理	控制用户在解锁设备键盘锁和工作质询键盘锁之前可用的功能。还可以控制完全托管设备和专用设备的设备键盘锁功能。例如，您可以禁用锁屏功能，例如指纹解锁、信任代理和通知。
kiosk	限制应用程序在 Samsung SAFE 设备上的使用。您可以将可用应用程序限于特定的一个或多个应用程序。此策略对计划仅运行特定类型或类别的应用程序的企业设备很有用。此策略还允许您针对 Kiosk 模式选择设备主屏幕和锁屏界面墙纸使用的自定义图片。

设备策略名称	设备策略说明
Launcher 配置	指定 Android 设备上的 Citrix Launcher 的设置，例如允许的应用程序以及 Launcher 图标的自定义徽标图像。
LDAP	提供与要用于 iOS 设备的 LDAP 服务器有关的信息，包括任何必要的帐户信息（例如 LDAP 服务器主机名）。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。
位置	允许您在地图上对设备进行地理定位（假定该设备已为 Secure Hub 启用 GPS）。将此策略部署到设备之后，可以从 XenMobile Server 发送定位命令。之后设备会返回其位置坐标。XenMobile 还支持地理围栏和跟踪策略。
邮件	在 iOS 或 macOS 设备上配置电子邮件帐户。
托管域	定义应用于电子邮件和 Safari 浏览器的托管域。托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护公司数据。对于 iOS 8 及更高版本的受监管设备，可以指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。
MDM 选项	在受监督的 iOS 7.0 及更高版本的手机设备上管理 “查找我的 iPhone 和 iPad 激活锁”。
组织信息	为 XenMobile 部署到 iOS 设备的警报消息指定组织信息。
通行码	在托管设备上强制使用 PIN 代码或密码。您可以为设备上的通行码设置复杂性和超时。
个人热点	允许用户不在 WiFi 网络的范围内时连接到 Internet。用户通过其 iOS 设备上手机网络数据连接并使用个人热点功能进行连接。
配置文件删除	从 iOS 或 macOS 设备中删除应用程序配置文件。
预配配置文件	指定要发送到设备的企业分发预配配置文件。在开发 iOS 企业应用程序以及为其进行代码签名时，通常会包括预配配置文件。Apple 要求应用程序的配置文件在 iOS 设备上运行。如果预配配置文件缺失或已过期，用户轻按应用程序以将其打开时，应用程序将崩溃。
删除预配配置文件	删除 iOS 预配配置文件。

设备策略名称	设备策略说明
代理	为运行 Windows Mobile/CE 和 iOS 的设备指定全局 HTTP 代理设置。只能为每个设备部署一个全局 HTTP 代理策略。
注册表	定义允许您管理 Windows Mobile/CE 设备的注册表项和值。Windows Mobile/CE 注册表存储关于应用程序、驱动器、用户首选项和配置设置的数据。
远程支持	向您提供远程访问 Samsung KNOX 设备的权限。自 2019 年 1 月 1 日起，远程支持功能不再向新客户提供。现有客户可以继续使用此产品，但 Citrix 将不提供增强功能或修复。
限制	提供在托管设备上执行锁定和控制功能的数百种选项。限制选项示例：禁用相机或麦克风、强制执行漫游规则以及强制访问第三方服务（例如应用商店）。
漫游	配置在 iOS 和 Windows Mobile/CE 设备上是否允许语音和数据漫游。如果禁用语音漫游，会自动禁用数据漫游。
Samsung MDM 许可证密钥	指定内置 Samsung Enterprise License Management (ELM) 密钥，必须先将该密钥部署到设备，才能部署 SAFE 策略和限制。XenMobile 还支持 Samsung Enterprise Firmware-Over-The-Air (E-FOTA) 服务。XenMobile 支持并扩展了 Samsung for Enterprise (SAFE) 和 Samsung KNOX 策略。
计划	必需策略，用于使 Android 和 Windows Mobile 设备重新连接到 XenMobile Server 以进行 MDM 管理、应用程序推送和策略部署。如果不向设备发送此策略并且未启用 Google FCM，设备将无法重新连接回服务器。
SCEP	将 iOS 和 macOS 设备配置为从外部 SCEP 服务器检索证书。您还可以使用 SCEP 从连接到 XenMobile 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。
SSO 帐户	创建单点登录 (SSO) 帐户，以便用户只需登录设备一次，即可访问 XenMobile 和内部公司资源。用户无需在设备上存储任何凭据。XenMobile 跨应用程序（包括 App Store 中的应用程序）使用 SSO 帐户的企业用户凭据。此策略与 Kerberos 身份验证兼容。适用于 iOS。

设备策略名称	设备策略说明
存储加密	加密内部和外部存储。对于某些设备，此策略可防止用户在其设备上使用存储卡。
已订阅的日历	将订阅的日历添加到 iOS 设备上的日历列表。请务必先订阅某个日历，才能将其添加到用户设备上已订阅的日历列表中。
条款和条件	要求用户接受贵公司控制与企业网络的连接的特定策略。当用户在 XenMobile 中注册其设备时，必须接受这些条款和条件才能注册其设备。拒绝这些条款和条件会取消注册过程。
通道	仅用于远程支持。通过 Remote Support，您的技术支持代表能够远程控制托管的 Windows CE 和 Android 移动设备。远程支持不适用于本地群集 XenMobile Server 部署。自 2019 年 1 月 1 日起，远程支持功能不再向新客户提供。现有客户可以继续使用此产品，但 Citrix 将不提供增强功能或修复。
VPN	提供对使用传统 VPN 网关技术的后端系统的访问权限。此策略用于提供可以部署到设备的 VPN 网关连接的详细信息。XenMobile 支持多个 VPN 提供商，包括 Cisco AnyConnect、Juniper 及 Citrix VPN。如果您的 VPN 网关支持此选项，您可以将此策略链接到 CA 并按需启用 VPN。
壁纸	添加.png 或.jpg 文件，以设置 iOS 设备锁屏界面、主屏幕或二者的墙纸。要在 iPad 和 iPhone 上使用不同的墙纸，请创建不同的墙纸策略并将其部署到相应的用户。
Web 内容过滤器	过滤 iOS 设备上的 Web 内容。XenMobile 使用 Apple 自动过滤功能和您添加到允许列表和阻止列表的站点。仅适用于受监督的 iOS 设备。
Web 剪辑	在 Web 站点中放置快捷方式或 Web 剪辑，以便其与应用程序一起出现在用户设备上。您可以指定自己的图标来表示 iOS、macOS 和 Android 设备的 Web 剪辑。Windows 平板电脑只需要一个标签和一个 URL。
WiFi	允许管理员将 WiFi 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。

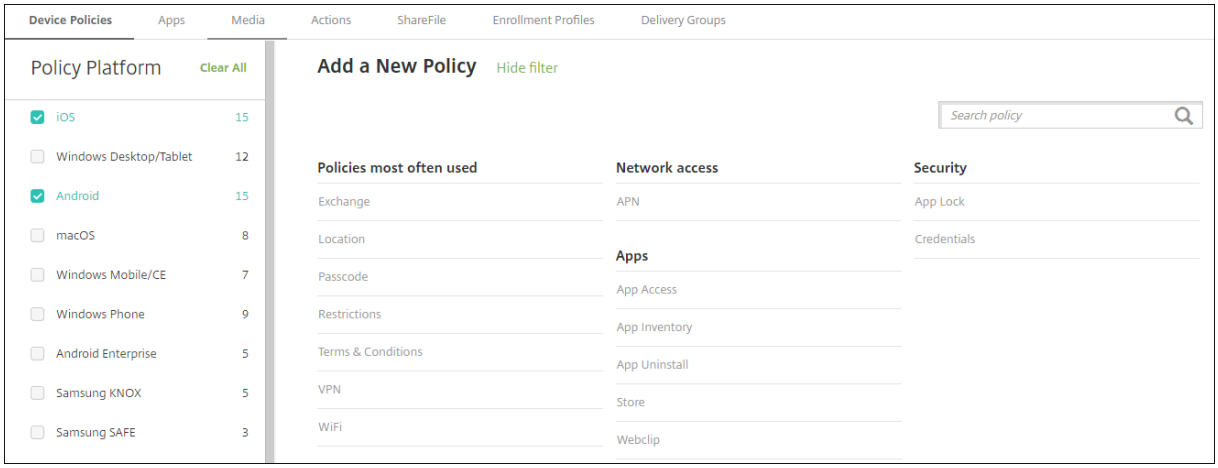
设备策略名称	设备策略说明
Windows CE 证书	从外部 PKI 创建 Windows Mobile/CE 证书并将其交付到用户设备。
Windows 信息保护	指定在您为策略设置的强制级别需要 Windows 信息保护的应用程序。此策略适用于 Windows 10 和 Windows 11 受监督设备。
XenMobile Store	指定 XenMobile Store Web 剪辑是否显示在用户设备的主屏幕上。
XenMobile 选项	配置在从 Android 和 Windows Mobile/CE 设备连接到 XenMobile 时 Secure Hub 的行为。
XenMobile 卸载	从 Android 和 Window Mobile/CE 设备中卸载 XenMobile。部署此策略时，它将从部署组中的所有设备上删除 XenMobile。

设备策略（按平台）

January 5, 2022

要查看对每个平台可用的策略，请执行以下操作：

1. 在 XenMobile 控制台中，转至配置 **>** 设备策略。
2. 单击添加。
3. 每个设备平台显示在策略平台窗格中的列表中。如果该窗格未打开，请单击显示过滤器。
4. 要查看适用于某个平台的所有策略的列表，请选择该平台。要查看适用于多个平台的策略的列表，请选择所有这些平台。仅当策略适用于选择的每个平台时，才会显示在列表中。



最新版本的 XenMobile 支持适用于以下平台的设备策略：

- Amazon
- Android
- Android Enterprise
- Android Zebra
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Windows 10 和 Windows 11 Desktop/Tablet
- Windows 10 Phone
- Windows Mobile/CE

有关最新版本的 XenMobile 中的支持设备的详细信息，请参阅支持的设备平台。

> 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 XenMobile 设备策略时，请记住以下规则。如果已注册的一台或多台设备上的某个策略冲突，则优先应用与 GPO 对应的策略。

AirPlay 镜像设备策略

April 22, 2021

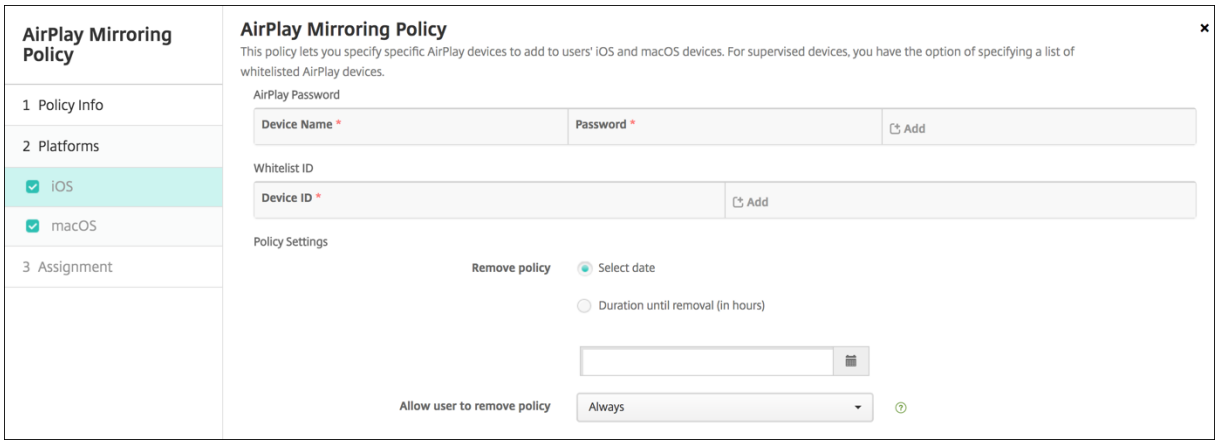
Apple AirPlay 功能允许用户将设备显示器上的内容准确镜像到另一台 Mac 计算机。

可以在 XenMobile 中添加一个设备策略，用于将特定 AirPlay 设备（例如其他 Mac 计算机）添加到 iOS 设备。您还可以将设备添加到受监督设备的允许列表，从而使用户仅限于使用允许列表上的 AirPlay 设备。有关将设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

> 注意：
>
> 继续操作前，请确保您具有要添加的所有设备的设备 ID 和任何密码。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

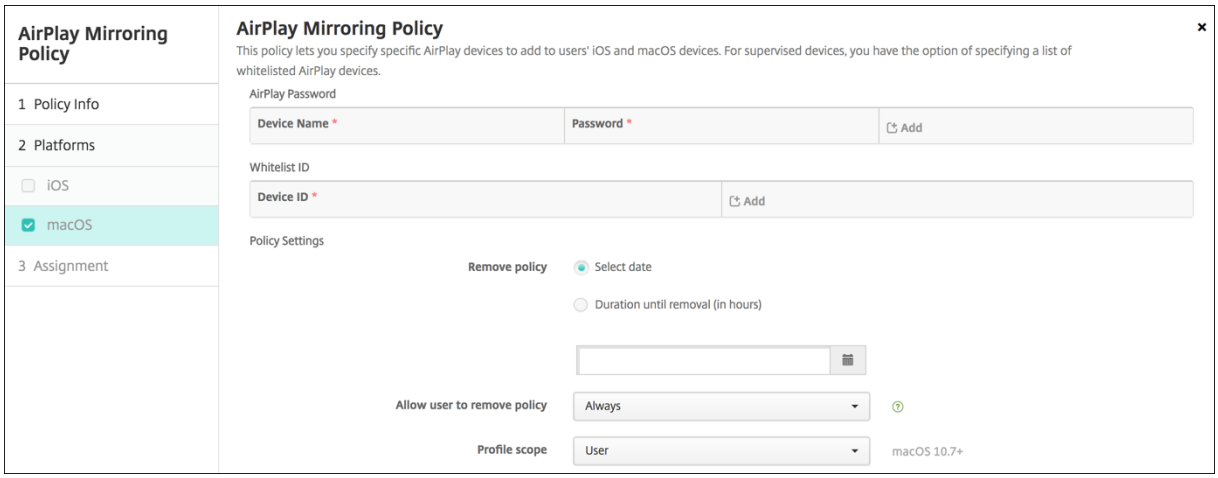


- **AirPlay** 密码：对于要添加的每个设备，单击添加，然后执行以下操作：
  - 设备 **ID**：以 xx:xx:xx:xx:xx:xx 格式输入硬件地址（Mac 地址）。此字段不区分大小写。
  - 密码：输入设备的可选密码。
  - 单击添加以添加设备，或单击取消以取消添加设备。
- 白名单 **ID**：对于未受监督的设备，忽略此列表。此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。对于要添加到列表的每个 AirPlay 设备，单击添加，然后执行以下操作：

  > 注意：
  >
  > XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

  - 设备 **ID**：以 xx:xx:xx:xx:xx:xx 格式键入设备 ID。此字段不区分大小写。
  - 单击添加以添加设备，或单击取消以取消添加设备。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。

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 **ID**：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。
- 白名单 **ID**：对于未受监督的设备，忽略此列表。此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。对于要添加到列表的每个 AirPlay 设备，单击添加，然后执行以下操作：
  - 设备 **ID**：以 xx:xx:xx:xx:xx:xx 格式键入设备 ID。此字段不区分大小写。
  - 单击添加以添加设备，或单击取消以取消添加设备。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

AirPrint 设备策略

April 14, 2020

可以在 XenMobile 中添加一个设备策略，用于在 iOS 设备上向 AirPrint 打印机列表中添加 AirPrint 打印机。通过此策略可以更加轻松地为打印机和设备位于不同子网的环境提供支持。

此策略适用于 iOS 7.0 及更高版本。

> 注意：
>
> 请确保知道每个打印机的 IP 地址和资源路径。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- **AirPrint** 目标：对于您要添加的各个 AirPrint 目标，单击添加，然后执行以下操作：
  - **IP** 地址：输入 AirPrint 打印机 IP 地址。
  - 资源路径：输入与打印机关联的资源路径。此值与 _ipps.tcp Bonjour 记录的参数相对应。例如，printers/Canon_MG5300_series 或 printers/Xerox_Phaser_7600。
  - 单击保存以添加打印机，或单击取消以取消添加打印机。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

Android Enterprise 托管配置策略

January 5, 2022

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。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 XenMobile 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：

- 应用程序电子邮件设置
- 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 XenMobile。有关详细信息，请参阅向 XenMobile 添加应用程序。

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。

PerApp VPN 的要求

要为 AE 创建 PerApp VPN，则除了配置 Android Enterprise 托管配置策略外，您还需要执行额外的步骤。此外，必须验证是否满足以下必备条件：

- 本地 Citrix Gateway
- 设备上安装了以下应用程序：
  - Citrix SSO
  - Citrix Secure Hub

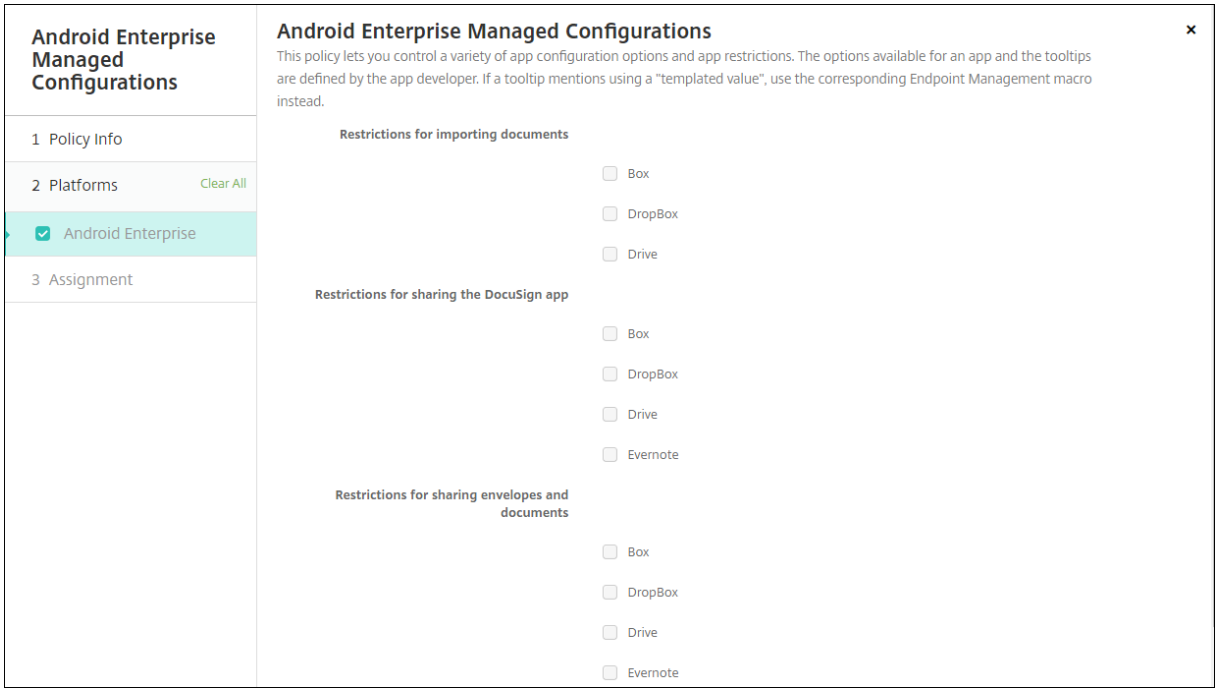
为 AE 设备配置 PerApp VPN 的一般工作流程如下：

1. 按本文中所述配置 VPN 配置文件。
2. 将 Citrix ADC 配置为接受来自 PerApp VPN 的流量。有关详细信息，请参阅 Citrix Gateway 上的完整 VPN 设置。

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 XenMobile 中的 Android Enterprise 应用程序，将无法继续操作。

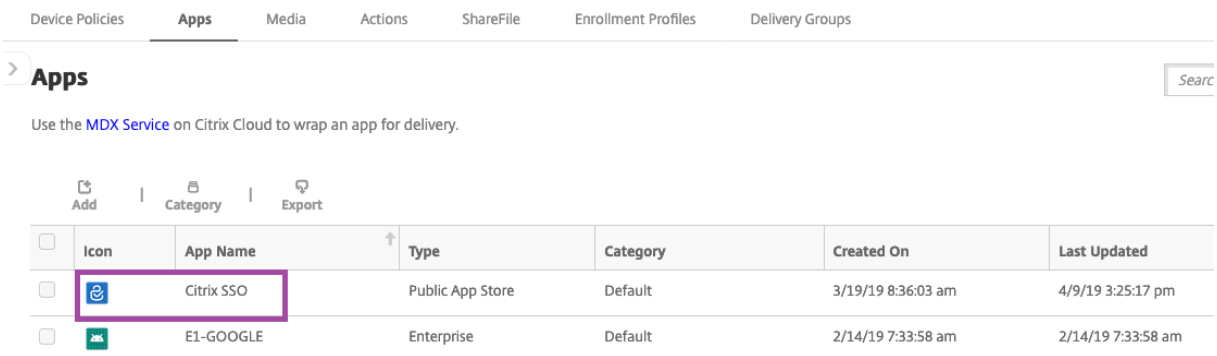
选择应用程序后，配置策略设置。这些设置与每个应用程序特定相关。



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 XenMobile 控制台中。请参阅添加公共应用商店应用程序。

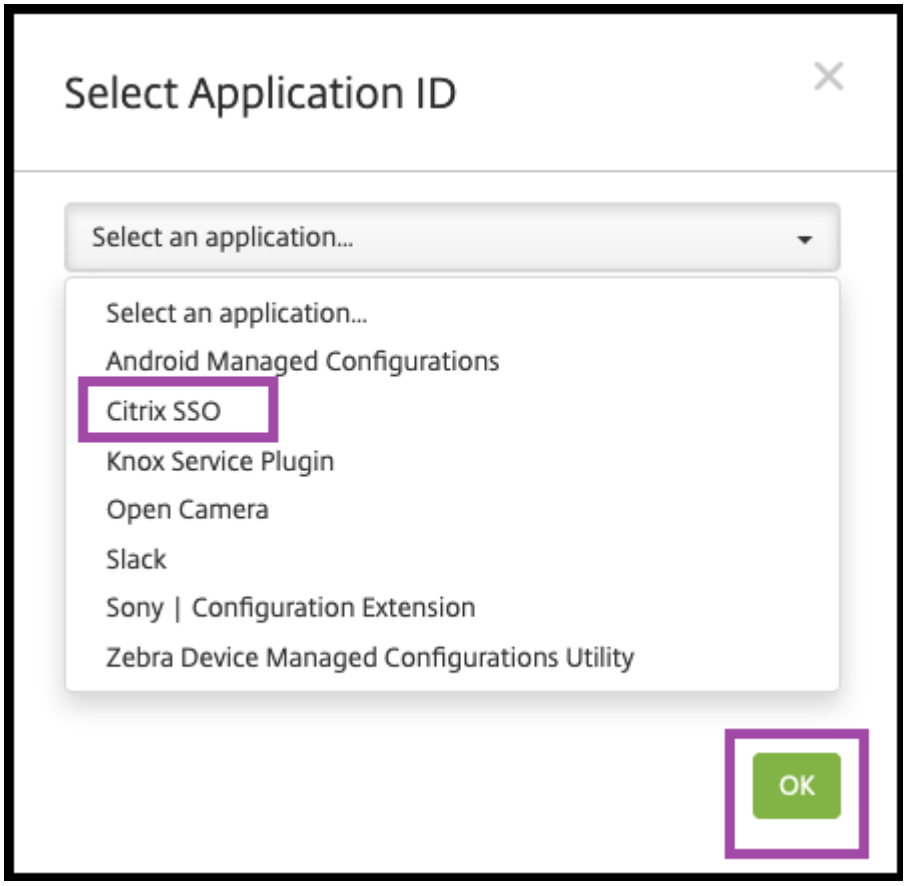


为 **Citrix SSO** 创建 **Android Enterprise** 托管配置

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 XenMobile 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。



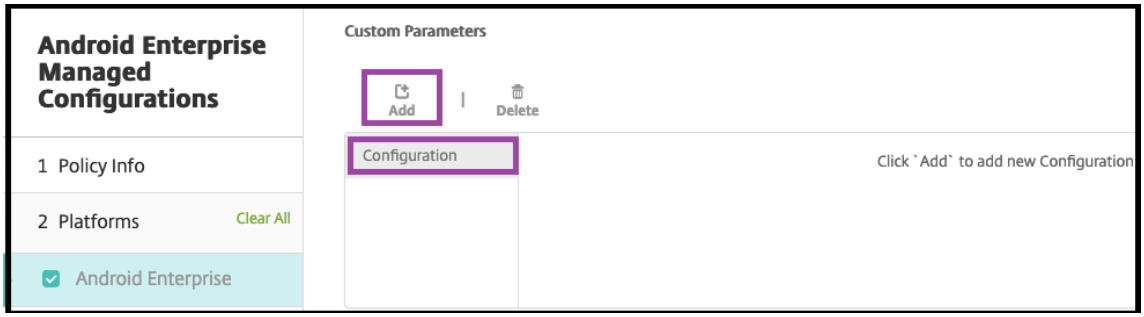
4. 键入 Citrix SSO VPN 配置的名称和说明。单击 **Next**（下一步）。

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。

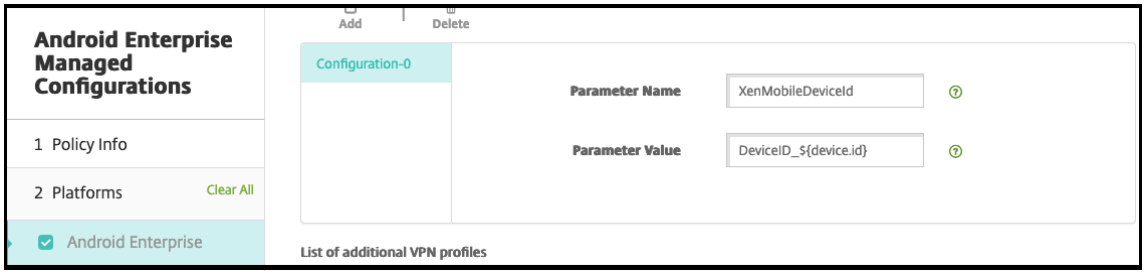
- 服务器地址 **(*)**。键入您的 Citrix Gateway FQDN。如果 Citrix Gateway 端口不是 443，请键入您的端口。使用 URL 格式。例如，`https://gateway.mycompany.com:8443`。
- 用户名 **(**可选**)**。提供最终用户用于对 Citrix Gateway 进行身份验证的用户名。可以将 XenMobile 宏 {user.username} 用于此字段。（请参阅宏。）如果不提供用户名，系统会在连接到 Citrix Gateway 时提示用户提供用户名。
- 密码 **(**可选**)**。提供最终用户用于对 Citrix 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 应用程序的用户界面中轻按连接开关（而非轻按特定配置文件）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。为 Citrix Gateway 使用自签名证书时，或颁发 Citrix Gateway 证书的 CA 的根证书不在系统 CA 列表中时，此设置设为“关”。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：

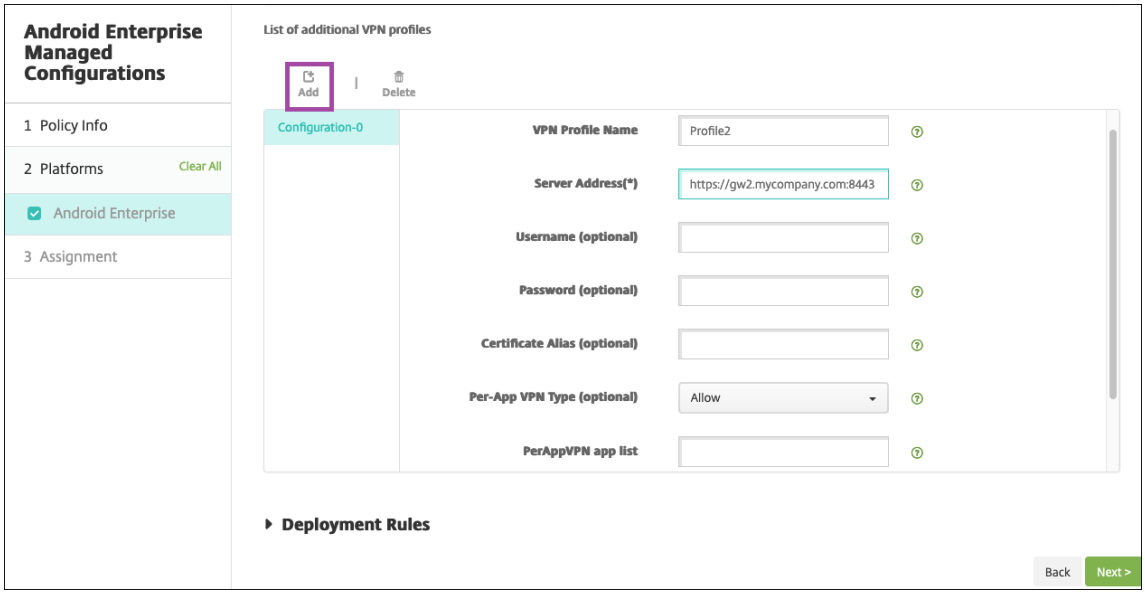
- 参数名称。键入 **XenMobileDeviceId**。此字段是用于根据 XenMobile 中的设备注册进行网络访问检查的设备 ID。如果 XenMobile 注册并管理设备，则允许建立 VPN 连接。否则，在 VPN 建立时将拒绝身份验证。
- 参数值 XenMobile 用于确定设备的注册和管理状态，XenMobileDeviceID 的值设置为 `DeviceID_${ device.id }`。



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。

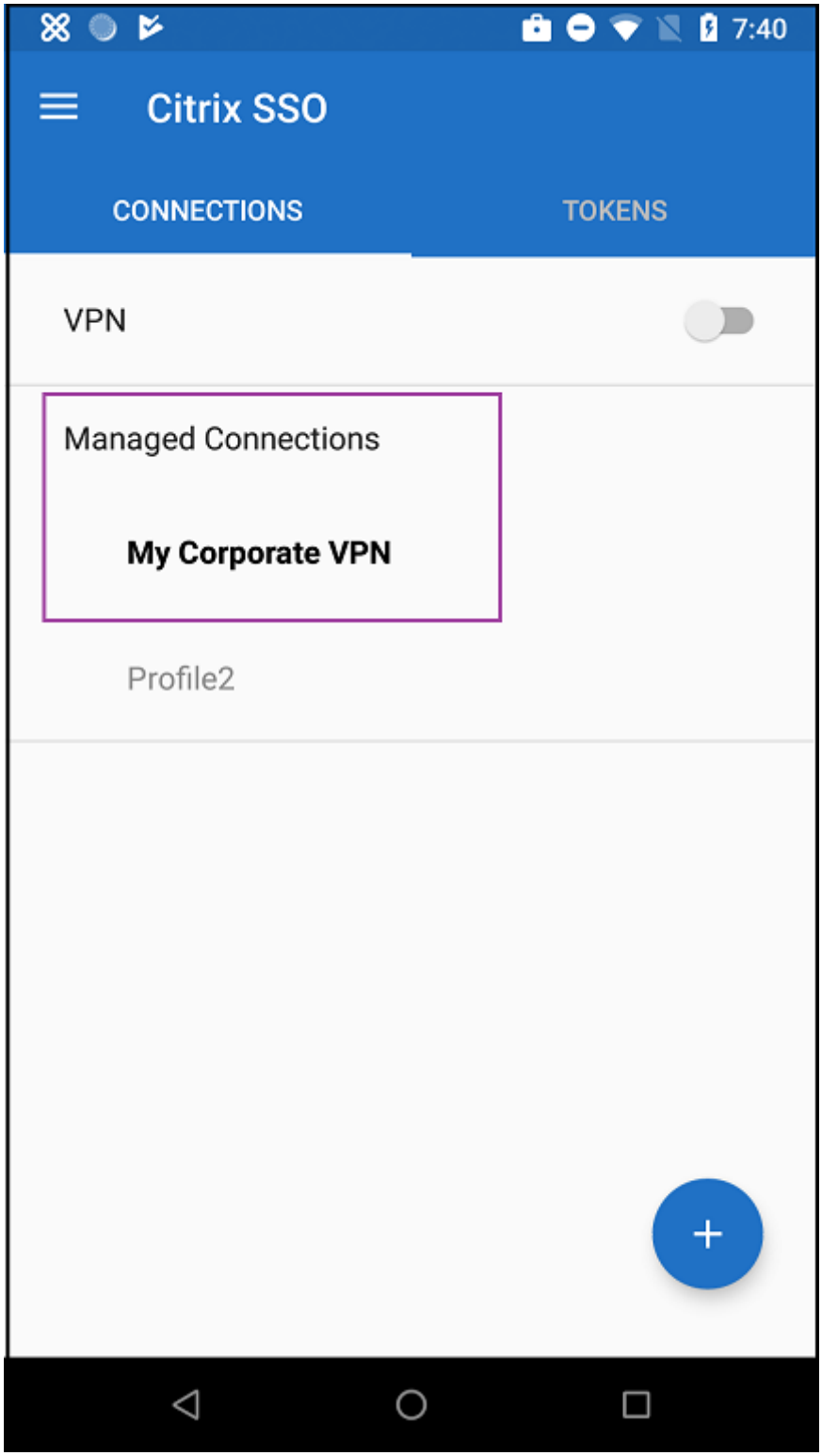
要为您配置的 VPN 配置文件启用始终启用功能，请设置 XenMobile 选项设备策略。

> 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。

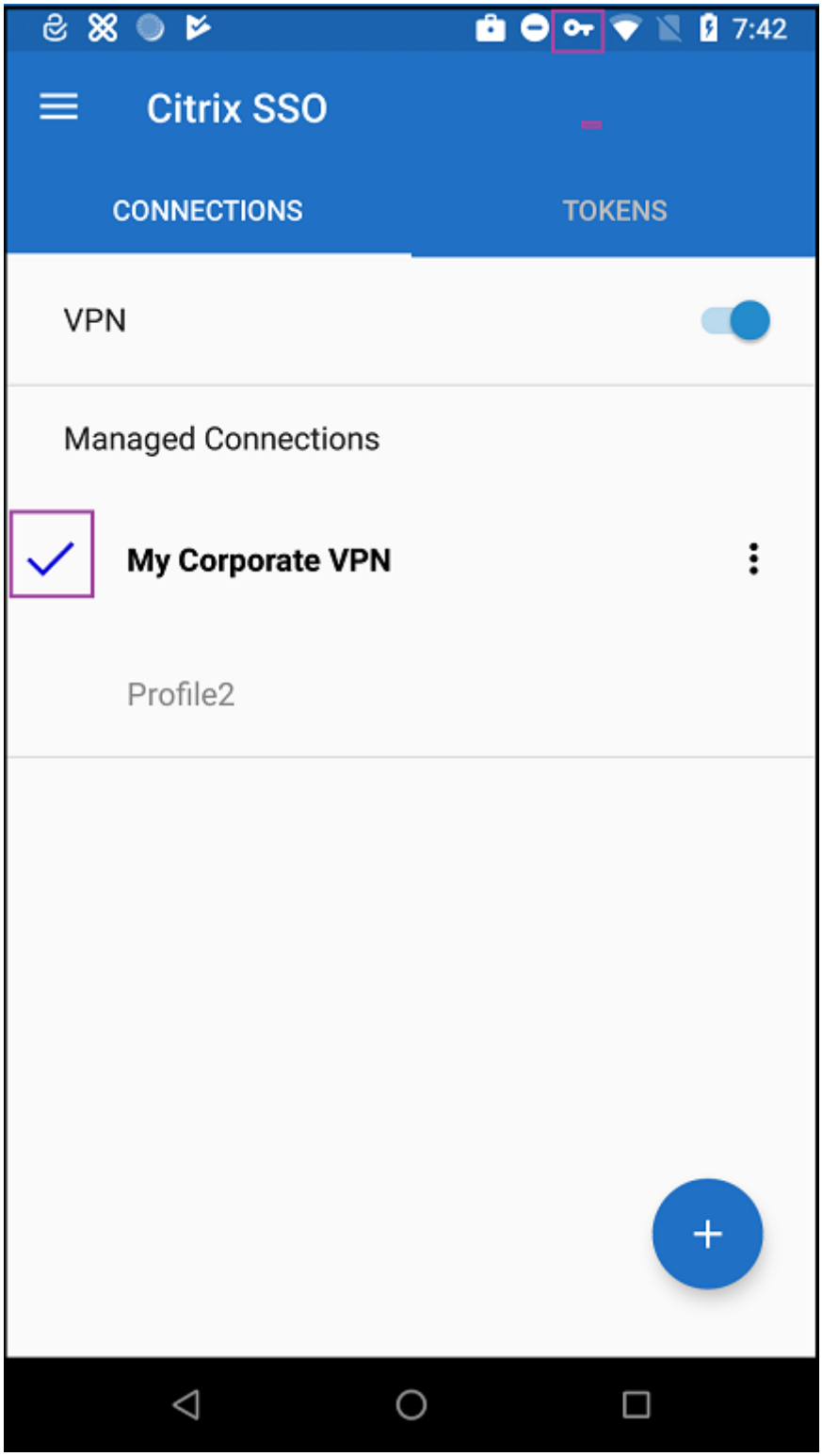
从设备访问 **VPN** 配置文件

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。

XenMobile 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。

首先将 Zebra OEMConfig 应用程序作为 Google Play 应用商店应用程序添加到 XenMobile 控制台中。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 XenMobile 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 **Next**（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**（适用于 12 小时制格式）或 **24**（适用于 24 小时制格式）。

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。

Android Enterprise 应用程序权限

January 5, 2022

您可以配置对（工作配置文件内部的）Android Enterprise 应用程序的请求如何处理 Google 称作“危险”权限的权限。您负责控制是否提示用户授予或拒绝来自应用程序的权限申请。此功能适用于运行 Android 7.0 及更高版本的设备。

Google 将危险权限定义为允许应用程序访问涉及用户的私人信息或者可能会影响用户已存储的数据或其他应用程序的操作的数据或资源的权限。例如，读取用户的联系人的能力属于危险权限。

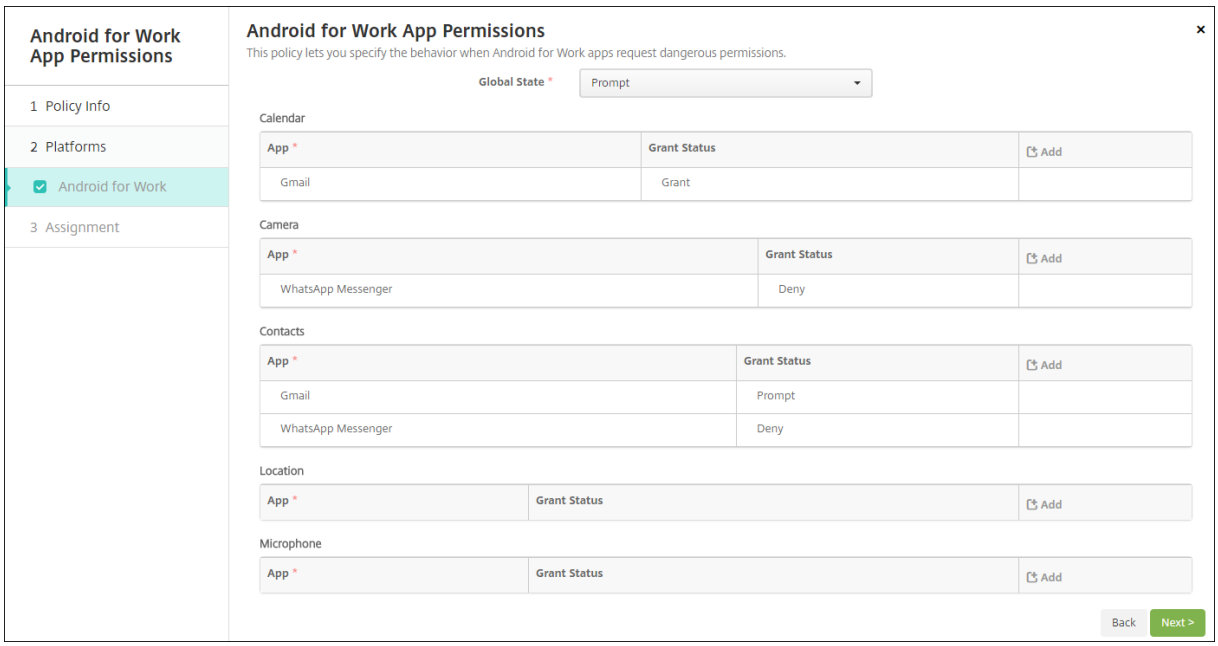
可以配置一个全局状态，用于控制对工作配置文件内部的 Android Enterprise 应用程序的所有危险权限申请的行为。还可以针对每个应用程序控制单个权限组的危险权限申请的行为，如 Google 所定义。这些单个设置将覆盖全局状态。

有关 Google 如何定义权限组的信息，请参阅本 Android developers guide（《Android 开发人员指南》）中的“Permission groups”（权限组）。

默认情况下，系统将提示用户授予或拒绝危险权限申请。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Android Enterprise 设置



- 全局状态：控制所有危险权限申请的行为。在列表中，单击提示、授予或拒绝。
  - 提示：系统提示用户授予或拒绝危险权限申请。
  - 授予：授予所有危险权限申请。系统不提示用户。
  - 拒绝：拒绝所有危险权限申请。系统不提示用户。

  默认值为提示。
- 针对每个应用程序设置每个权限组的单个行为。要配置某个权限组的行为，请单击添加，然后在应用程序下方从列表中选择一个应用程序。如果配置 Android Enterprise 系统应用程序，请单击新增功能，然后在“限制”设备策略中输入启用的应用程序包名称。在“Grant State”（授予状态）下方，选择提示、授予或拒绝。此授予状态将替代全局状态。

  - 提示：系统提示用户针对此应用程序授予或拒绝来自此权限组的危险权限申请。
  - 授予：针对此应用程序授予来自此权限组的危险权限申请。系统不提示用户。
  - 拒绝：针对此应用程序拒绝来自此权限组的危险权限申请。系统不提示用户。

  默认值为提示。

- 单击应用程序和授予状态旁边的保存。
- 要为权限组添加更多应用程序，请再次单击添加并重复执行这些步骤。
- 为要进行设置的所有权限组设置了授予状态后，单击下一步。

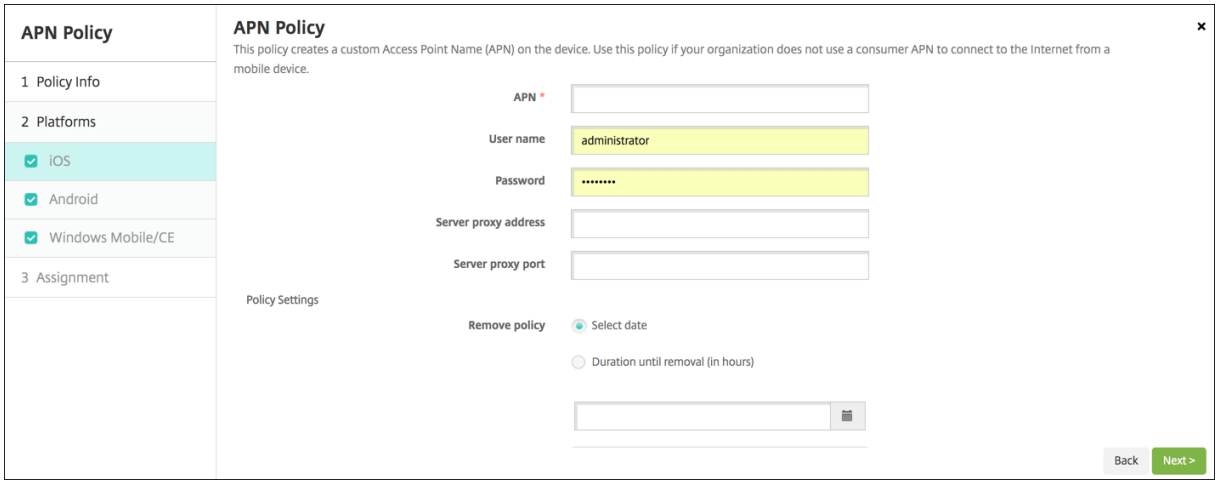
APN 设备策略

January 5, 2022

可以为 iOS、Android 和 Windows Mobile/CE 设备添加接入点名称 (APN) 设备策略。如果贵组织不使用客户 APN 从移动设备连接到 Internet，可以使用此策略。APN 策略确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。大多数新式电话中已经定义此设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

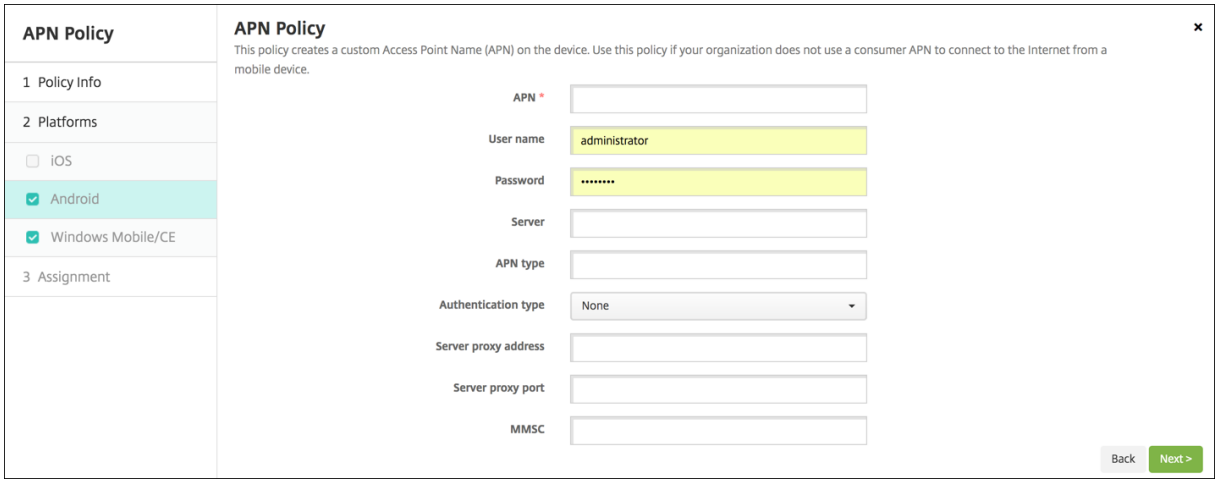
iOS 设置



- **APN**：键入接入点的名称。此信息必须与接受的某个 iOS APN 匹配，否则策略将失败。
- 用户名：此字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- 密码：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- 服务器代理地址： APN 代理的 IP 地址或 URL。
- 服务器代理端口： APN 代理的端口号。如果已输入服务器代理地址，则此字段为必填字段。
- 在策略设置下方的删除策略旁边，单击选择日期或删除前的持续时间 **(**小时**)**。

  - 如果单击选择日期，请单击日历以选择具体删除日期。
  - 在允许用户删除策略列表中，单击始终、需要密码或从不。
  - 如果单击需要密码，在 **Removal password**（删除密码）旁边，键入必需的密码。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

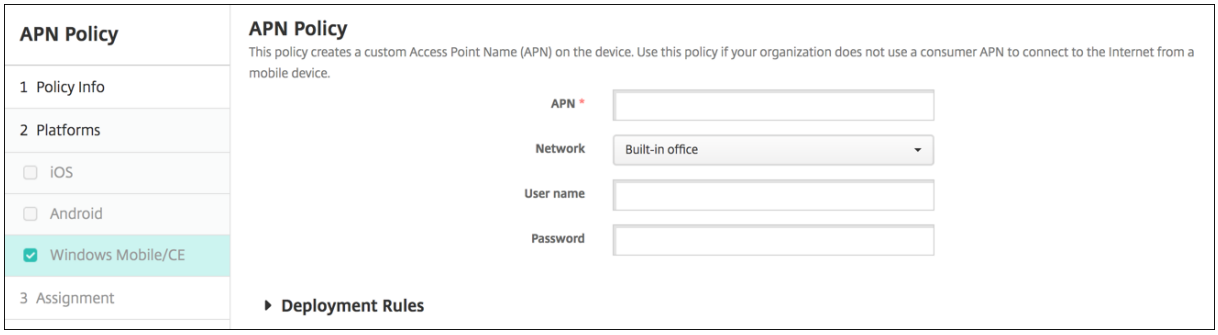
Android 设置



- **APN**：键入接入点的名称。此信息必须与接受的某个 Android APN 匹配，否则策略将失败。
- 用户名：此字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- 密码：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- 服务器：此设置在智能手机之前出现，通常为空。它是指无法访问或显示标准 Web 站点的手机的无线应用协议 (WAP) 网关服务器。
- **APN** 类型：此设置必须匹配运营商的接入点用途。它是 APN 服务说明符的逗号分隔字符串，必须与无线运营商的发布定义匹配。示例包括：
  - *。所有流量均通过此接入点。
  - mms。多媒体流量通过此接入点。
  - default（默认）。包括多媒体在内的所有流量均通过此接入点。
  - supl。与 GPS 关联的安全用户层面定位 (Secure User Plane Location)
  - dun。拨号网络已经过时，很少使用。
  - hipri。高优先级网络。
  - fota。无线固件升级用于接收固件更新。
- 身份验证类型：在列表中，单击要使用的身份验证类型。默认值为 “无”。
- 服务器代理地址：运营商的 APN HTTP 代理的 IP 地址或 URL。
- 服务器代理端口： APN 代理的端口号。如果已输入服务器代理地址，则此字段为必填字段。

- **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：指用于 MMS 流量的多媒体消息服务服务器。MMS 使得 SMS 可以发送包含多媒体内容（如图片或视频）的大型消息。这些服务器需要特定的协议（如 MM1、... MM11)。
- **MMS** 端口：用于 MMS 代理的端口。

Windows Mobile/CE 设置



- **APN**：键入接入点的名称。此信息必须与接受的某个 Android APN 匹配，否则策略将失败。
- 网络：在列表中，单击要使用的网络类型。默认值为内置办公网络。
- 用户名：此字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- 密码：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。

应用程序访问设备策略

March 27, 2020

利用 XenMobile 中的应用程序访问设备策略，可以定义需要安装到设备上、可以安装到设备上或不得安装到设备上的应用程序列表。然后，可以创建自动化操作，以使设备符合此应用程序列表。可以创建适用于 iOS、Android 和 Windows Mobile/CE 设备的应用程序访问策略。

一次只能配置一种类型的访问策略。可以针对必选的应用程序列表、推荐的应用程序列表或禁止的应用程序列表添加策略，但不能在一个应用程序访问策略中混合这些应用程序列表。如果为每种列表类型创建一个策略，建议谨慎地为每个策略命名，以便于了解 XenMobile 中的哪项策略适用于哪种应用程序列表。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

平台设置

- 访问策略：单击必填、建议或禁止。默认值为必填。
- 要向列表中添加一个或多个应用程序，请单击添加，然后执行以下操作：
  - 应用程序名称：输入应用程序的名称。

- 应用程序标识符：输入可选的应用程序标识符。
- 单击保存或取消。
- 对要添加的每个应用程序重复这些步骤。

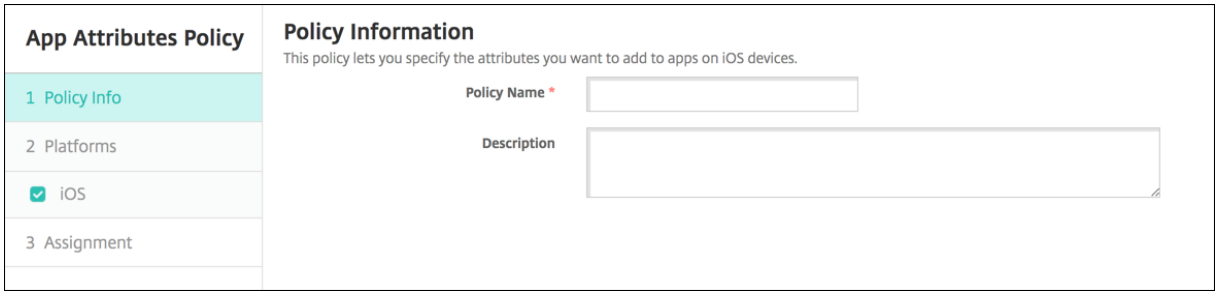
应用程序属性设备策略

March 27, 2020

在应用程序属性设备策略中可以为 iOS 设备指定各种属性，例如托管应用程序捆绑包 ID 或 PerApp VPN 标识符。

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



- 托管应用程序捆绑包 **ID**：在列表中，单击某个应用程序捆绑包 ID 或单击新增。
  - 如果单击新增，请在显示的字段中键入应用程序捆绑包 ID。
- **PerApp VPN** 标识符：在列表中，单击 “PerApp VPN 标识符”。

应用程序配置设备策略

January 5, 2022

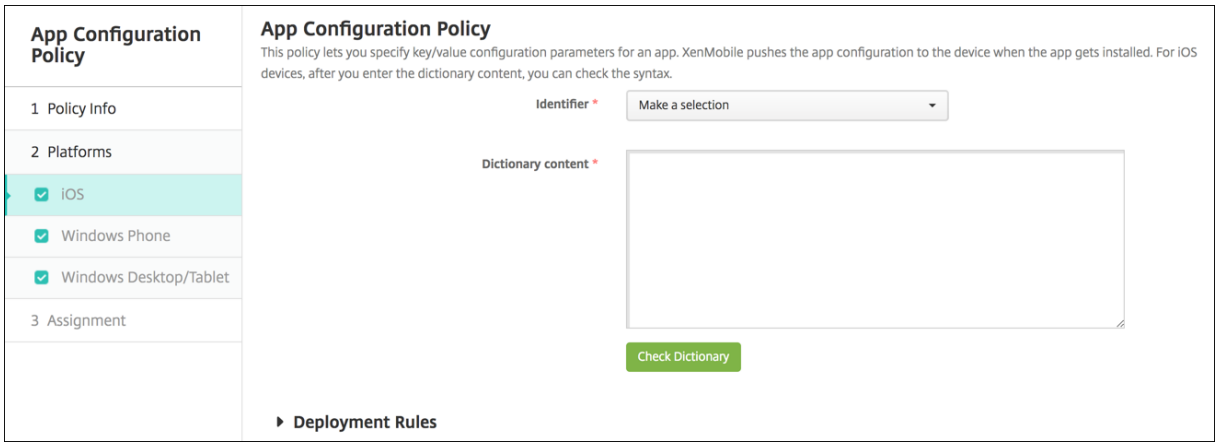
您可以执行以下操作来远程配置支持托管配置的应用程序：

- 将 XML 配置文件（称为属性列表或 plist）部署到 iOS 设备
- 或者，为 Windows 10 Phone 或者运行 Windows 10 或 Windows 11 的平板电脑或台式机设备部署键/值对。

配置指定应用程序中的各种设置和行为。XenMobile 在用户安装应用程序时将配置推送到设备。可以配置的实际设置和行为取决于应用程序，不在本文的探讨范围之内。

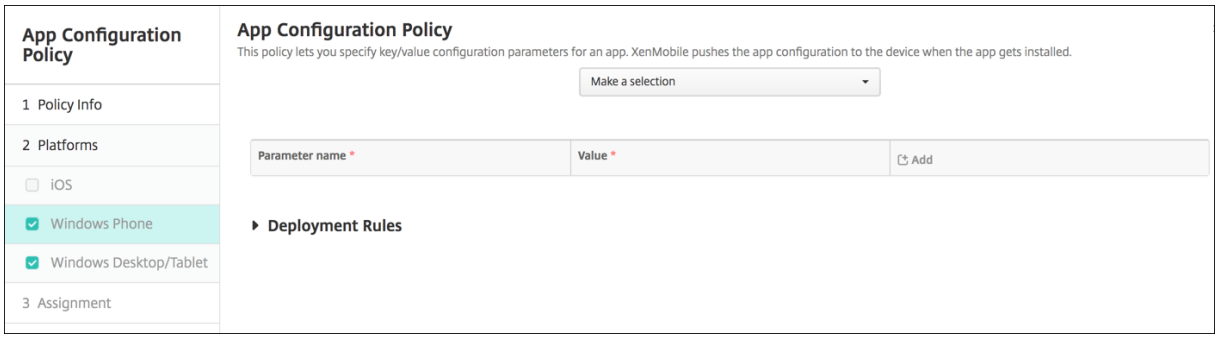
要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

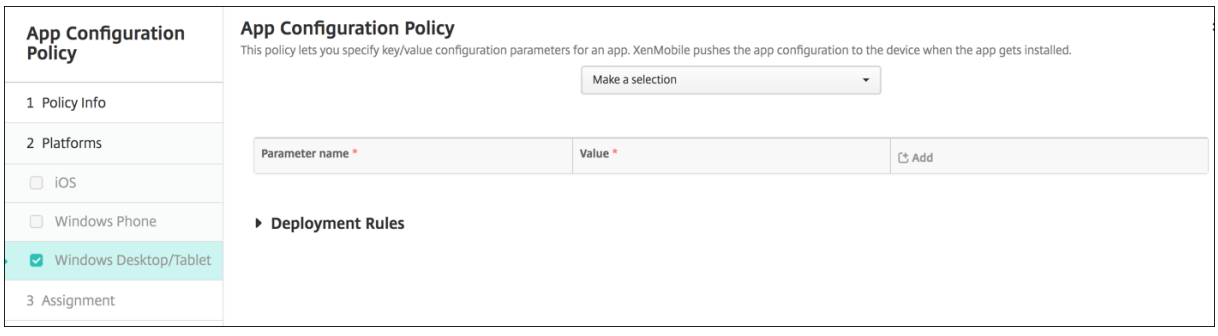
iOS 设置



- 标识符：在列表中，单击要配置的应用程序，或单击新增向列表中添加新应用程序。
  - 如果单击新增，请在显示的字段中键入应用程序标识符。
- 字典内容：键入或复制并粘贴 XML 属性列表 (plist) 配置信息。
- 单击检查字典。XenMobile 验证 XML。如果没有错误，内容框下面将显示有效 **XML**。如果内容框下面显示语法错误，必须纠正这些错误，然后才能继续操作。

Windows Phone 或 Desktop/Tablet 设置





- 在做出选择列表中，单击要配置的应用程序，或单击新增向列表中添加新应用程序。
  - 如果单击新增，请在显示的字段中键入软件包系列名称。
- 对于要添加的每个配置参数，单击添加，然后执行以下操作：

- 参数名称：为 Windows 设备输入应用程序设置的键名称。有关 Windows 应用程序设置的信息，请参阅 Microsoft 文档。
- 值：输入指定参数的值。
- 单击添加以添加参数，或单击取消以取消添加参数。

应用程序清单设备策略

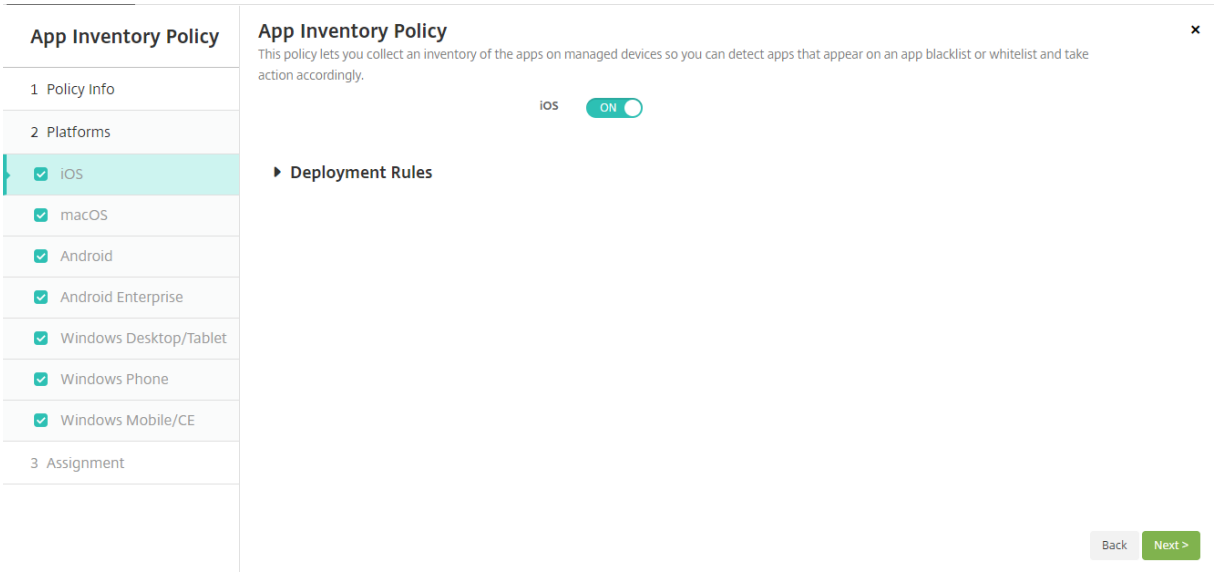
July 7, 2020

应用程序清单策略用于收集托管设备上的应用程序清单。之后 XenMobile 可以将清单与部署到这些设备的任何应用程序访问策略进行比较。这样一来，便可以检测应用程序允许列表或阻止列表中的应用程序，然后采取相应操作。

可以为 iOS、macOS、Android、Android Enterprise、Windows Desktop/Tablet、Windows Phone 和 Windows Mobile/CE 设备创建应用程序访问策略。

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。

平台设置



- 对于所选的每个平台，保留默认设置或将设置更改为关。默认值为开。

应用程序锁定设备策略

January 5, 2022

应用程序锁定设备策略定义允许在设备上运行的应用程序列表，或阻止在设备上运行的应用程序列表。可以同时为 iOS 和 Android 设备配置此策略，但策略具体的执行方式则因平台而异。例如，不能阻止在 iOS 设备上运行多个应用程序。

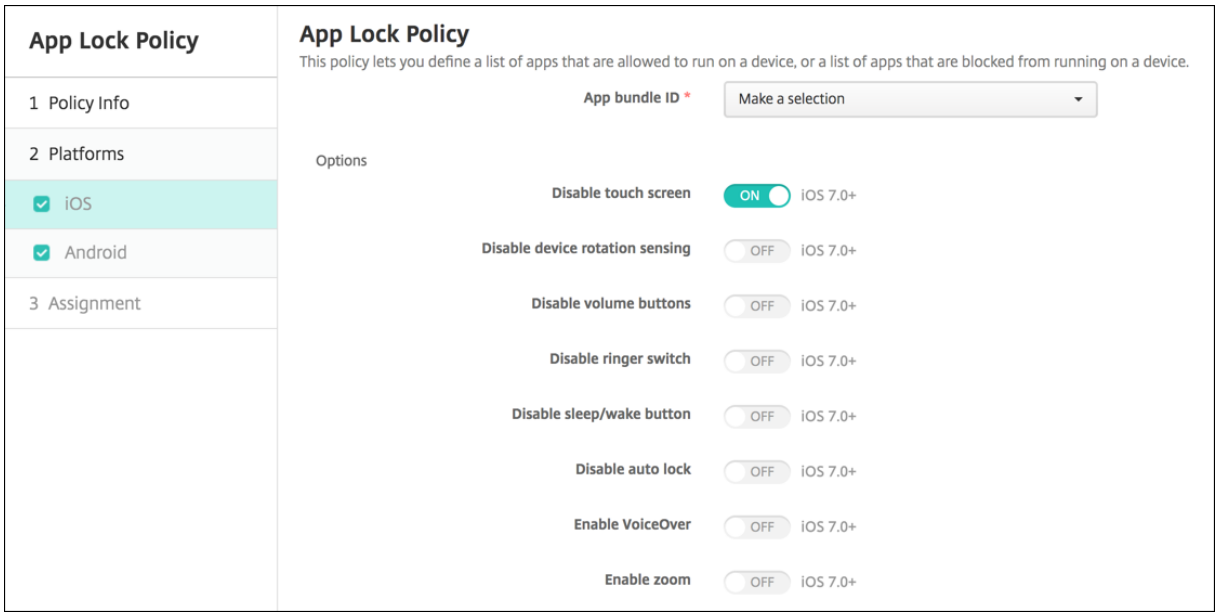
同样，对于 iOS 设备，每个策略只能选择一个 iOS 应用程序。这表示用户只能使用其设备运行单个应用程序。在强制执行应用程序锁定策略时，用户无法在设备上执行除您明确允许的选项之外的任何其他活动。

此外，必须监督 iOS 设备才能推送应用程序锁定策略。

虽然设备策略适用于大多数 Android L 和 M 设备，但是，由于 Google 弃用了所需的 API，因此，应用程序锁定不适用于 Android N 或更高版本的设备。

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。

iOS 设置



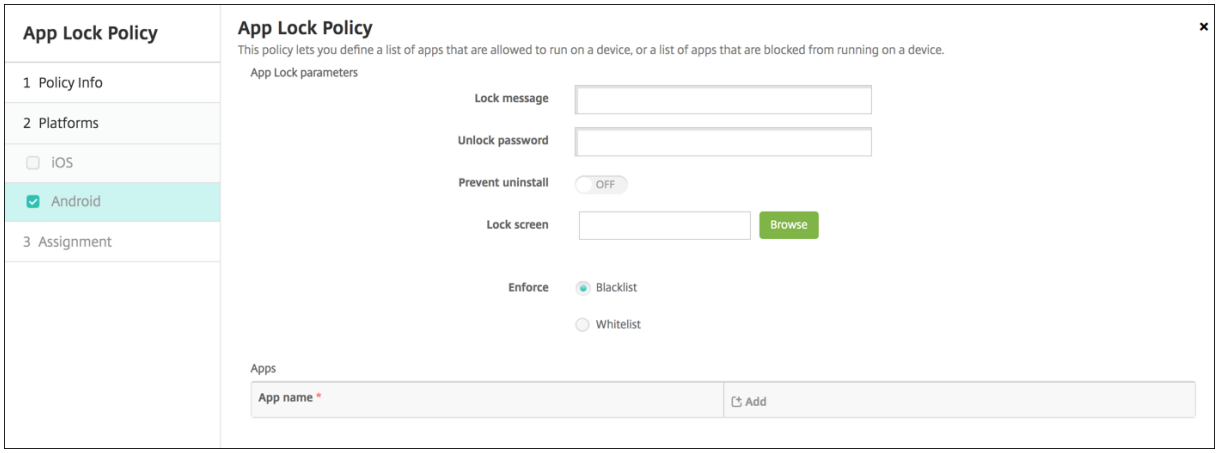
- 应用程序捆绑包 **ID**：在列表中，单击应用此策略的应用程序，或单击新增向列表中添加新应用程序。如果选择新增，请在显示的字段中键入应用程序名称。
- 选项：以下各选项仅适用于 iOS 7.0 或更高版本。对于每个选项，除“禁用触摸屏”默认值为开之外，默认值均为关。
  - 禁用触摸屏
  - 禁用设备旋转感应
  - 禁用音量按钮
  - 禁用铃声开关

    “禁用铃声开关”设置为开时，铃声行为取决于首次禁用时开关所处的位置。
  - 禁用睡眠/唤醒按钮
  - 禁用自动锁定
  - 禁用 VoiceOver
  - 启用缩放

  - 启用反转颜色
  - 启用 AssistiveTouch
  - 启用朗读所选内容
  - 启用单声道音频
- 用户已启用的选项：以下各选项仅适用于 iOS 7.0 或更高版本。每个选项的默认值均为关。
  - 允许 VoiceOver 调整
  - 允许缩放调整
  - 允许反转颜色调整
  - 允许 AssitiveTouch 调整
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

Android 设置

> 注意：
>
> 不能使用“应用程序锁定”设备策略阻止 Android 的“设置”应用程序。



- 应用程序锁定参数
  - 锁定消息：键入用户尝试打开锁定的应用程序时看到的消息。
  - 解锁密码：键入用于解锁应用程序的密码。
  - 阻止卸载：选择是否允许用户卸载应用程序。默认值为关。
  - 锁定屏幕：单击“浏览”并导航到显示在设备锁屏界面上的图像文件所在位置，选择此图像。
  - 强制执行：单击黑名单以创建不允许在设备上运行的应用程序的列表，或单击白名单以创建允许在设备上运行的应用程序的列表。

    > 注意：
    >
    > XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

- 应用程序：单击添加，然后执行以下操作：
  - 应用程序名称：在列表中，单击要添加到允许列表或阻止列表的应用程序的名称，或单击新增向可用应用程序列表中添加新应用程序。
  - 如果选择新增，请在显示的字段中键入应用程序名称。
  - 单击保存或取消。
  - 为要添加到允许列表或阻止列表中的每个应用程序重复执行这些步骤。

应用程序网络使用设备策略

January 5, 2022

您可以设置网络使用规则，以指定 iOS 设备上托管应用程序使用网络（如手机网络数据网络）的方式。规则仅适用于托管应用程序。托管应用程序是您通过 XenMobile 部署到用户设备的应用程序。其中不包括用户直接下载到设备上且未通过 XenMobile 部署的应用程序，或者在设备向 XenMobile 注册时已经安装到设备上的应用程序。

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。

iOS 设置

- 允许手机网络数据漫游：选择指定的应用程序是否可以在漫游时使用手机网络数据连接。默认值为关。
- 允许手机网络数据：选择指定的应用程序是否可以使用手机网络数据连接。默认值为关。
- 应用程序标识符匹配：对于要添加到此列表中的每个应用程序，单击添加，然后执行以下操作：
  - 应用程序标识符：输入应用程序标识符。
  - 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。

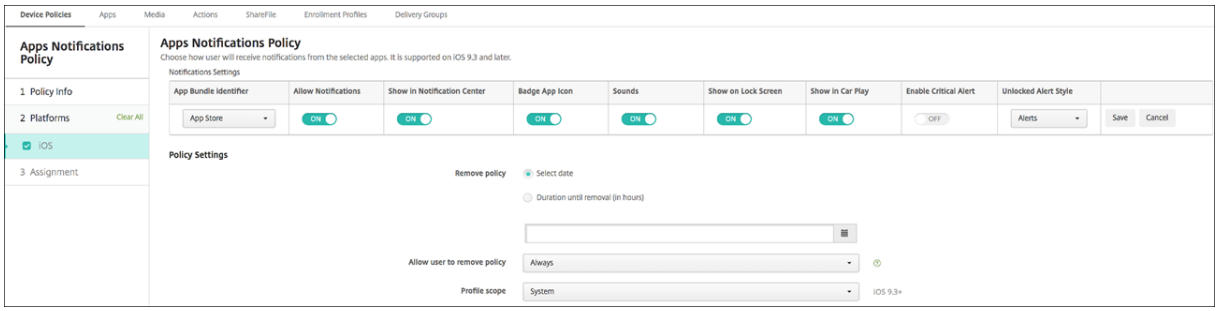
应用程序通知设备策略

April 14, 2020

通过应用程序通知策略，您可以控制 iOS 用户如何从指定的应用程序接收通知。此策略在运行 iOS 9.3 或更高版本的设备上受支持。

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



- 应用程序捆绑包标识符：指定要应用此策略的应用程序。
- 允许通知：选择开将允许通知。
- 在通知中心中显示：选择开将在用户设备的通知中心显示通知。
- 徽章应用程序图标：选择开将在通知中显示徽章应用程序图标。
- 声音：选择开将在通知中包含声音。
- 在锁屏界面中显示：选择开将在用户设备的锁屏界面中显示通知。
- 在 **CarPlay** 中显示：如果设置为开，通知将在 Apple CarPlay 中显示。在 iOS 12 及更高版本中可用。默认值为开。
- 启用严重警报：如果设置为开，应用程序可以将通知标记为忽略“请勿打扰”和铃声设置的关键通知。在 iOS 12 及更高版本中可用。默认值为关。
- 解锁的警报样式：在列表中，选择无、横幅或警报来配置解锁的警报的外观。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅适用于 iOS 9.3 及更高版本。

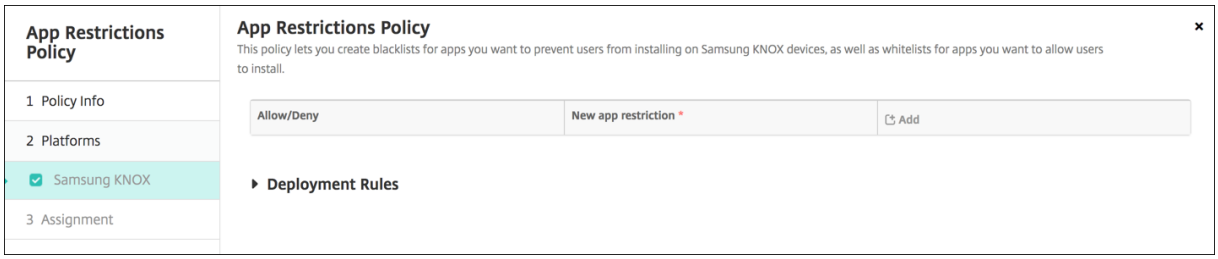
应用程序限制设备策略

July 7, 2020

可以创建您要阻止用户在 Samsung KNOX 设备上安装的应用程序的阻止列表。还可以创建要允许用户安装的应用程序的允许列表。

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。

Samsung KNOX 设置



对于要添加到“允许/拒绝”列表中的每个应用程序，单击添加，然后执行以下操作：

- 允许/拒绝：选择是否允许用户安装应用程序。
- 新应用程序限制：键入应用程序软件包 ID，例如 com.kmdm.af.crackle。
- 单击保存将应用程序保存到“允许/拒绝”列表，或单击取消不将应用程序保存到“允许/拒绝”列表中。

应用程序通道设备策略

January 5, 2022

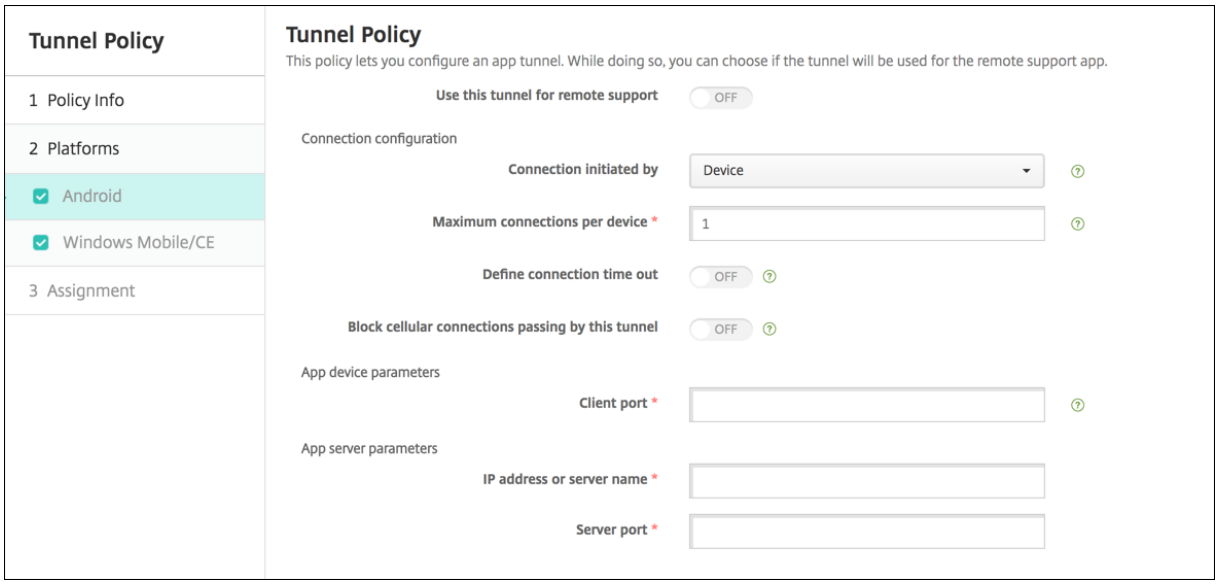
> 重要：
>
> 应用程序通道策略仅用于远程支持。有关远程支持的信息，请参阅支持选项和远程支持。自 2019 年 1 月 1 日起，远程支持功能不再向新客户提供。现有客户可以继续使用此产品，但 Citrix 将不提供增强功能或修复。

应用程序通道旨在提高移动应用程序的服务连续性及数据传输可靠性。应用程序通道定义移动设备应用程序的客户端组件与应用程序服务器组件之间的代理参数。还可以使用应用程序通道创建设备的远程支持通道以使用管理支持。可以为 Android 和 Windows Mobile/CE 设备配置应用程序通道策略。

通过在此策略中定义的通道发送的任何应用程序流量均先通过 XenMobile，然后再被重定向到运行此应用程序的服务器。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

Android 设置



- 使用此通道进行远程支持：选择是否将此通道用于远程支持。

  根据是否选择远程支持，配置步骤会有所不同。

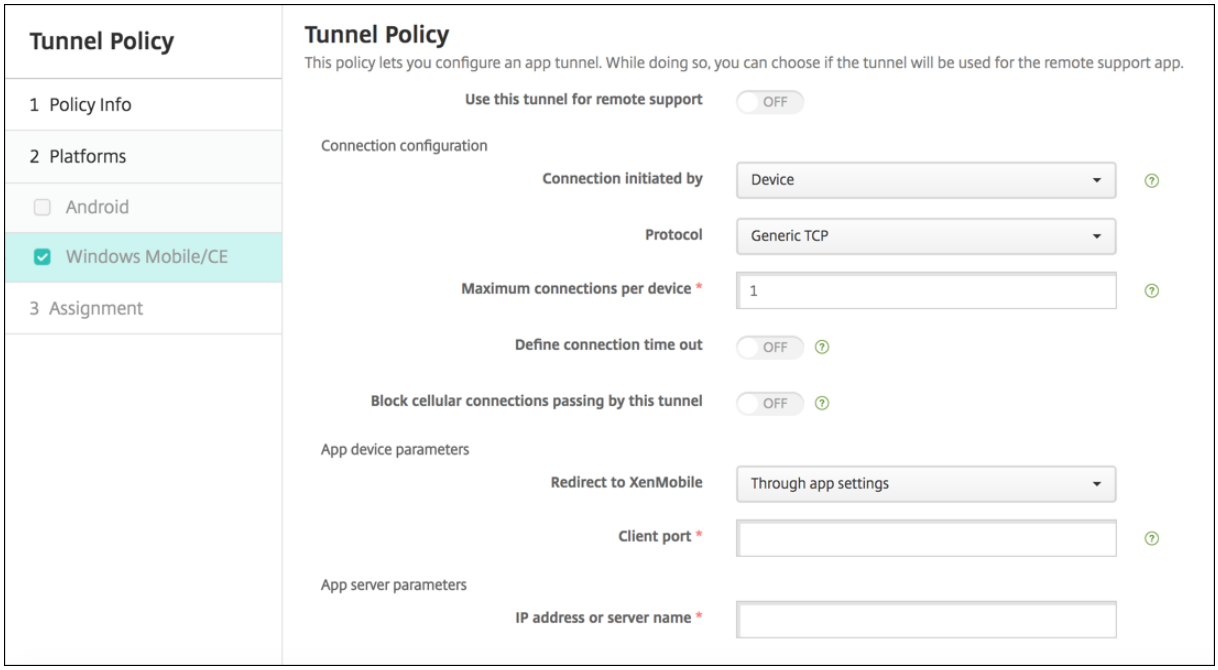
- 如果不选择远程支持，请执行以下操作：
  - 连接发起者：单击设备或服务器以指定发起连接的源。
  - 每台设备最大连接数：键入一个数字，用于指定应用程序可以建立的并发 TCP 连接数。此字段仅适用于设备发起的连接。
  - 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - 连接超时：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度（秒）。
  - 阻止手机网络连接通过此通道：选择是否在漫游时阻止此通道。

    > 注意：
    >
    > 不会阻止 WiFi 和 USB 连接。

  - 客户端端口：键入客户端端口号。在大多数情况下，此值与服务器端口相同。
  - **IP** 地址或服务器名称：键入应用程序服务器的 IP 地址或名称。此字段仅适用于设备发起的连接。
  - 服务器端口：键入服务器端口号。
- 如果选择远程支持，请执行以下操作：
  - 使用此通道进行远程支持：设置为开。
  - 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - 连接超时：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度（秒）。
  - 使用 **SSL** 连接：选择是否对此通道使用安全 SSL 连接。

- 阻止手机网络连接通过此通道：选择是否在漫游时阻止此通道。此设置不会阻止 WiFi 和 USB 连接。

Windows Mobile/CE 设置



- 使用此通道进行远程支持：选择是否将此通道用于远程支持。

根据是否选择远程支持，配置步骤会有所不同。

- 如果不选择远程支持，请执行以下操作：
  - 连接发起者：单击设备或服务器以指定发起连接的源。
  - 协议：在列表中，单击要使用的协议。默认值为通用 **TCP**。
  - 每台设备最大连接数：键入一个数字，用于指定应用程序可以建立的并发 TCP 连接数。此字段仅适用于设备发起的连接。
  - 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - 连接超时：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度（秒）。
  - 阻止手机网络连接通过此通道：选择是否在漫游时阻止此通道。

    > 注意：
    > 不会阻止 WiFi 和 USB 连接。

  - 重定向到 **XenMobile**：在列表中，单击设备连接到 XenMobile 的方式。默认值为通过应用程序设置。
    - 如果选择使用本地别名，请在本地别名中键入别名。默认值为 **localhost**。
    - 如果选择 **IP** 地址范围，请在 **IP** 地址范围起点中键入起始 IP 地址，在 **IP** 地址范围终点中键入结束 IP 地址。
  - 客户端端口：键入客户端端口号。在大多数情况下，此值与服务器端口相同。
  - **IP** 地址或服务器名称：键入应用程序服务器的 IP 地址或名称。此字段仅适用于设备发起的连接。
  - 服务器端口：键入服务器端口号。

- 如果选择远程支持，请执行以下操作：
  - 使用此通道进行远程支持：设置为开。
  - 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - 连接超时：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度（秒）。
  - 使用 **SSL** 连接：选择是否对此通道使用安全 SSL 连接。
  - 阻止手机网络连接通过此通道：选择是否在漫游时阻止此通道。不会阻止 WiFi 和 USB 连接。

应用程序卸载设备策略

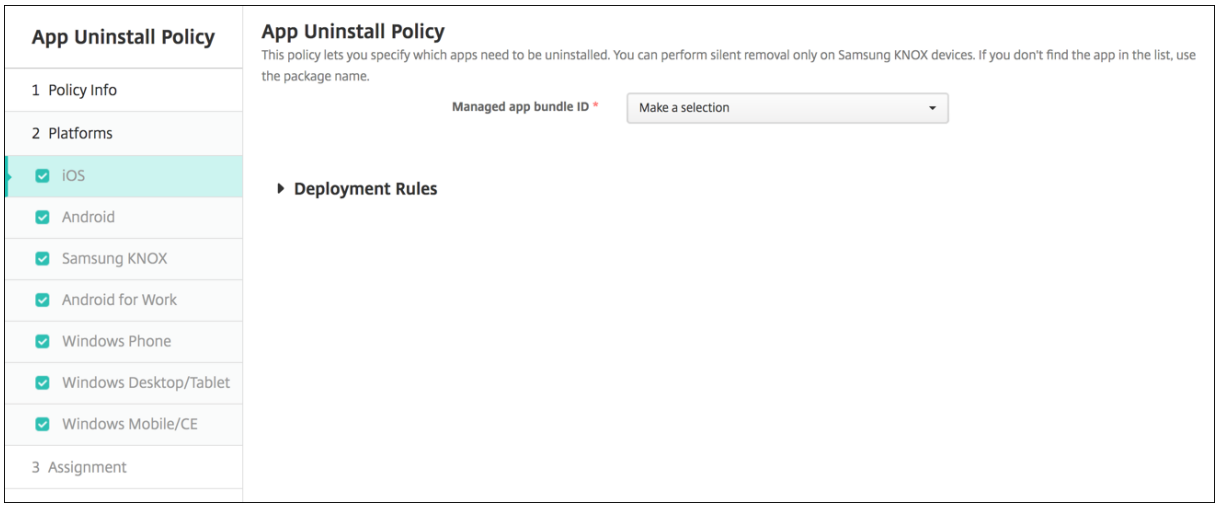
March 27, 2020

您可以为 iOS、Android、Samsung KNOX、Android Enterprise、Windows Desktop/Tablet 和 Windows Mobile/CE 平台创建应用程序卸载策略。通过应用程序卸载策略，您可以因任意多种原因从用户设备中删除应用程序。原因可以是您不再想要支持某些应用程序，贵公司可能要将现有应用程序替换为其他供应商的类似应用程序等等。

当此策略部署到用户设备时，应用程序被删除。除 Samsung KNOX 设备外，用户会收到卸载应用程序的提示。Samsung KNOX 设备用户不会收到卸载应用程序的提示。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- 托管应用程序捆绑包 **ID**：在列表中，单击现有应用程序或单击新增。如果此平台没有配置应用程序，该列表将是空的，您必须添加新的应用程序。
  - 单击添加时，将显示一个字段，您可以在其中键入应用程序名称。

所有其他平台设置

- 要卸载的应用程序：对于您要添加的每个应用程序，单击添加，然后执行以下操作：

- 应用程序名称：在列表中，单击现有应用程序，或单击新增输入新的应用程序名称。如果此平台没有配置应用程序，该列表将是空的，您必须添加新的应用程序。
- 单击添加以添加应用程序，或单击取消以取消添加应用程序。

在安装相应的公共应用商店应用程序后自动卸载企业应用程序

可以将 XenMobile 配置为在安装公共应用商店版本时删除 Citrix 应用程序的企业版本。此功能可防止用户设备在安装公共应用商店版本后具有两个相同的应用程序图标。

“应用程序卸载”设备策略的部署条件将触发 XenMobile 在安装新版本时从用户设备中删除较旧的应用程序。此功能仅适用于在企业模式 (XME) 下连接到 XenMobile Server 的托管 iOS 设备。

要通过“已安装应用程序的名称”条件配置一条部署规则，请执行以下操作：

- 指定企业应用程序的托管应用程序捆绑包 **ID**。
- 添加规则：单击新建规则，然后（如示例中所示）选择已安装应用程序的名称和等于。键入公共应用商店应用程序的应用程序捆绑包 ID。

在示例中，公共应用商店应用程序 (com.citrix.mail.ios) 安装在指定交付组中的设备上时，XenMobile 将删除企业版本 (com.citrix.mail)。

应用程序卸载限制设备策略

March 27, 2020

可以指定用户在 Samsung SAFE 或 Amazon 设备上可以卸载或不能卸载的应用程序。

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。

Samsung SAFE 或 **Amazon** 设置

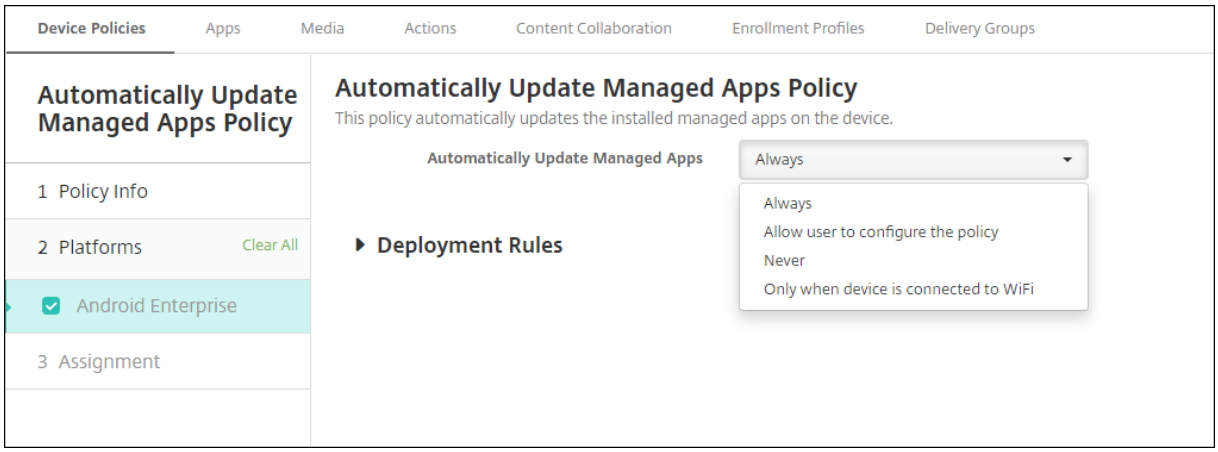
- 应用程序卸载限制设置：对于要添加的每个应用程序规则，单击添加，然后执行以下操作：
  - 应用程序名称：在列表中，单击某个应用程序，或单击新增以添加新应用程序。
  - 规则：选择用户是否可以卸载应用程序。默认值为允许卸载。
  - 单击保存或取消。

自动更新托管应用程序设备策略

January 21, 2021

此策略控制 Android Enterprise 设备上安装的托管应用程序的更新方式。可以限制用户允许自动更新其设备上的应用程序的能力。如果您允许用户控制其设备上的应用程序的自动更新，这些用户会在托管 Google Play 应用商店中设置自动应用程序更新策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。



设置自动更新托管应用程序。

- 始终：启用自动应用程序更新。始终为默认设置。
- 允许用户配置策略：允许用户在托管 Google Play 应用商店中为设备配置自动应用程序更新策略。
- 从不：禁用自动应用程序更新。
- 仅当设备连接到 **Wi-Fi** 时：仅当设备连接到 Wi-Fi 时，才允许自动更新应用程序。

BitLocker 设备策略

January 5, 2022

Windows 10 和 Windows 11 中包括一项名为 BitLocker 的磁盘加密功能，该功能提供针对丢失或被盗的 Windows 设备的未授权访问的额外文件和系统保护。要获取更多保护，可以对受信任的平台模块 (TPM) 芯片版本 1.2 或更高版本使用 BitLocker。TPM 芯片处理加密操作、生成和存储加密密钥以及限制对加密密钥的使用。

自 Windows 10 Build 1703 起，MDM 策略可以控制 BitLocker。可以在 XenMobile 中使用 BitLocker 设备策略配置在 Windows 10 和 Windows 11 设备上的 BitLocker 向导中可用的设置。例如，在启用了 BitLocker 的设备上，BitLocker 可以提示用户如何在启动时解锁其设备、如何备份其恢复密钥以及如何解锁固定驱动器。BitLocker 设备策略还配置是否：

- 在没有 TPM 芯片的设备上启用 BitLocker。
- 在 BitLocker 界面中显示恢复选项。
- 拒绝在未启用 BitLocker 时对固定驱动器或可移动驱动器的写入访问。

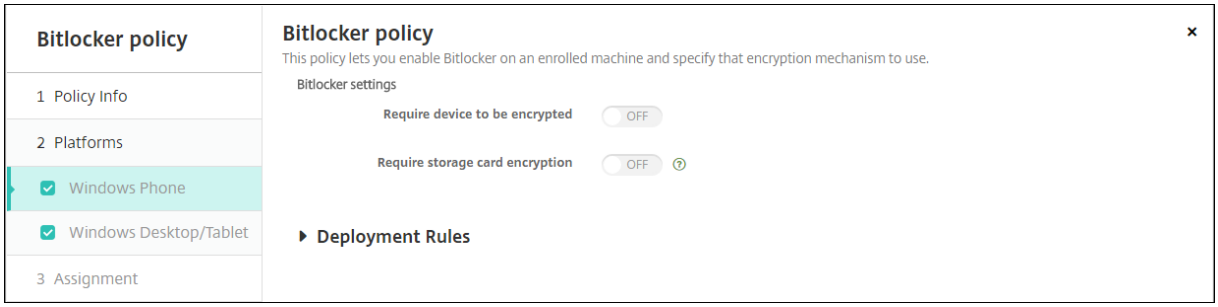
> 注意：
>
> BitLocker 加密在设备上启动后，您将无法再继续通过部署更新后的 BitLocker 设备策略来更改设备上的 BitLocker 设置。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

要求

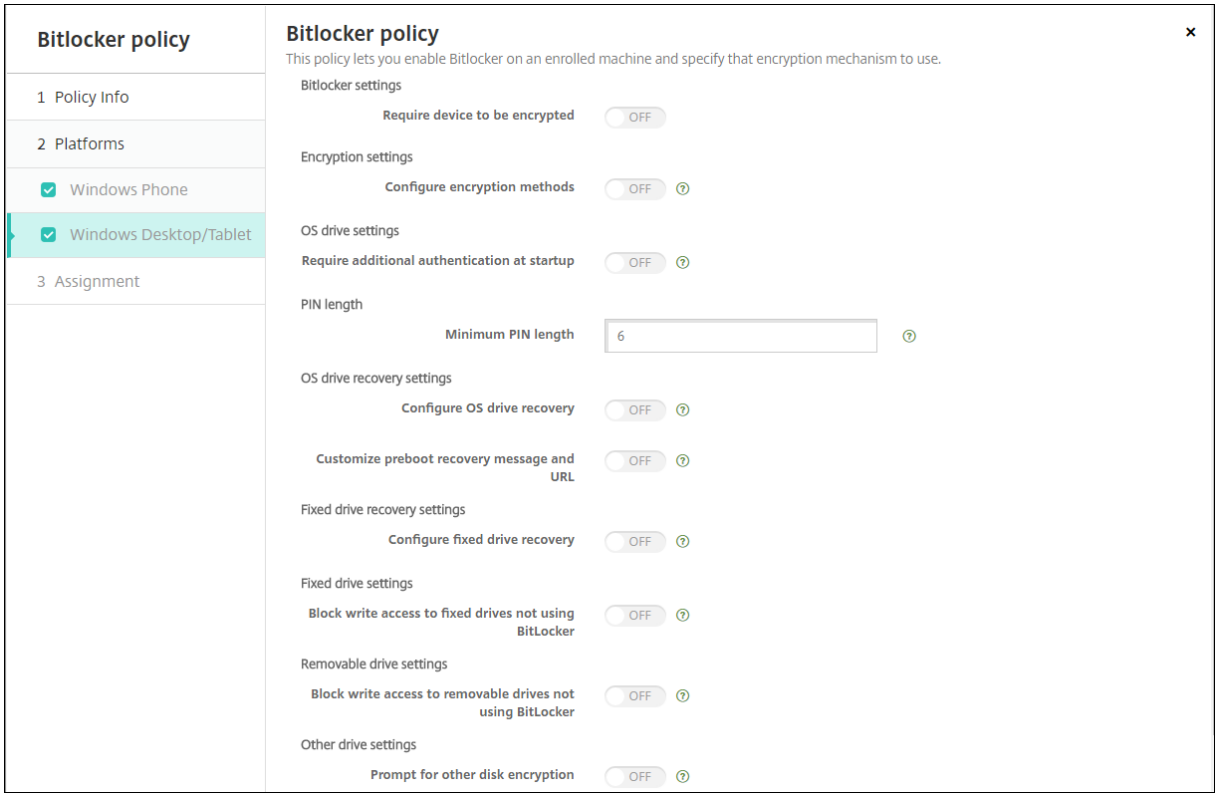
- BitLocker 设备策略需要 Windows 10 或 Windows 11 Enterprise Edition。
- 部署 BitLocker 设备策略之前，请准备您的环境以便使用 BitLocker。有关 Microsoft 提供的详细信息（包括 BitLocker 系统要求和设置），请参阅 BitLocker 以及该节点下的文章。

Windows Phone 设置



- 要求加密设备：确定是否提示用户在 Windows Phone 系统卡上启用 BitLocker 加密。如果设置为开，设备将在注册完成后显示一条消息，指出企业要求设备加密。如果用户选择不进行设备加密，用户将不会被授予对系统卡的写入访问权限。如果设置为关，系统将不会提示用户，并且 BitLocker 策略将决定是否加密设备。默认值为关。
- 要求存储卡加密：确定是否提示用户在 Windows Phone 存储卡上启用 BitLocker 加密。如果设置为开，则需要存储卡加密才能获取对卡的写入权限。默认值为关。

Windows Desktop 和 Tablet 设置



- 要求加密设备：确定是否提示用户在 Windows Desktop 或 Tablet 上启用 BitLocker 加密。如果设置为开，设备将在注册完成后显示一条消息，指出企业要求设备加密。如果设置为关，系统将不提示用户，并且 BitLocker 将使用策略设置。默认值为关。
- 配置加密方法：确定要对特定设备类型使用的加密方法。如果设置为关，BitLocker 向导将提示用户指定要对某种驱动器类型使用的加密方法。所有驱动器的加密方法都默认为 XTS-AES 128 位。可移动驱动器的加密方法默认为 AES-CBC 128 位。如果设置为开，BitLocker 将使用在策略中指定的加密方法。如果设置为开，将显示以下额外的设置：操作系统驱动器、固定驱动器和可移动驱动器。选择每种驱动器类型的默认加密方法。默认值为关。
- 启动时需要额外的身份验证：指定在设备启动过程中需要额外进行一次身份验证。此外，还指定是否允许在没有 TPM 芯片的设备上启用 BitLocker。如果设置为关，没有 TPM 的设备将无法使用 BitLocker 加密。有关 TPM 的信息，请参阅 Microsoft 文章 Trusted Platform Module Technology Overview（受信任的平台模块技术概览）。如果设置为开，将显示以下额外的设置。默认值为关。
  - 在没有 **TPM** 芯片的设备上阻止 **BitLocker**：在没有 TPM 芯片的设备上，BitLocker 要求用户创建解锁密码或启动密钥。启动密钥存储在 USB 驱动器中，用户必须在启动之前将该驱动器连接到设备。解锁密码最少包含 8 个字符。默认值为关。
  - **TPM** 启动：在配备了 TPM 的设备上，存在四种解锁模式：“仅 TPM”、“TPM + PIN”、“TPM + 密钥”以及 “TPM + PIN + 密钥”。TPM 启动面向 “仅 TPM” 模式，在该模式下，加密密钥存储在 TPM 芯片中。此模式不要求用户提供额外的解锁数据。用户设备在重新启动过程中使用 TPM 芯片中的加密密钥自动解

锁。默认值为允许 **TPM**。

- **TPM** 启动 **PIN**：此设置为 “TPM + PIN” 解锁模式。PIN 最多可以包含 20 个数字。使用最小 **PIN** 长度设置可指定最小 PIN 长度。用户将在 BitLocker 设置过程中配置 PIN，并在设备启动过程中提供 PIN。
- **TPM** 启动密钥：此设置为 “TPM + 密钥” 解锁模式。启动密钥存储在 USB 或其他可移动驱动器中，用户必须在启动之前将该驱动器连接到设备。
- **TPM** 启动密钥和 **PIN**：此设置为 “TPM + PIN + 密钥” 解锁模式。

  如果解锁成功，操作系统将开始加载。如果解锁失败，设备将进入恢复模式。

- 最小 **PIN** 长度：TPM 启动 PIN 的最小长度。默认值为 **6**。
- 配置操作系统驱动器恢复：如果解锁步骤失败，BitLocker 将提示用户提供已配置的恢复密钥。此设置将配置对用户可用的操作系统驱动器恢复选项（如果用户没有解锁密码或 USB 启动密钥）。默认值为关。
  - 允许基于证书的数据恢复代理：指定是否允许启用基于证书的数据恢复代理。从公钥策略中添加数据恢复代理，该代理位于组策略管理控制台 (GPMC) 或本地组策略编辑器中。有关数据恢复代理的详细信息，请参阅 Microsoft 文章 BitLocker Group Policy settings（BitLocker 组策略设置）。默认值为关。
  - 为操作系统驱动器恢复创建 **48** 位恢复密码：指定是否允许或要求用户使用恢复密码。BitLocker 生成密码并将其存储在文件中或 Microsoft 云帐户中。默认值为允许 **48** 位密码。
  - 创建 **256** 位恢复密钥：指定是否允许或要求用户使用恢复密钥。恢复密钥为 BEK 文件，该文件存储在 USB 驱动器中。默认值为允许 **256** 位恢复密钥。
  - 隐藏操作系统驱动器恢复选项：指定在 BitLocker 界面中显示还是隐藏恢复选项。如果设置为开，则不在 BitLocker 界面中显示任何恢复选项。在这种情况下，请将设备注册到 Active Directory 中，将恢复选项保存到 Active Directory 中，并将将恢复信息保存到 **AD DS** 中设置为开。默认值为关。
  - 将恢复信息保存到 **AD DS** 中：指定是否将恢复选项保存到 Active Directory 域服务中。默认值为关。
  - 配置存储在 **AD DS** 中的恢复信息：指定在 Active Directory 域服务中存储 BitLocker 恢复密码还是恢复密码和密钥包。存储密钥包将支持从物理损坏的驱动器中恢复数据。默认值为备份恢复密码。
  - 将恢复信息存储到 **AD DS** 后启用 **BitLocker**：指定是否阻止用户启用 BitLocker，但设备已连接到域，并且 BitLocker 恢复信息已成功备份到 Active Directory 时除外。如果设置为开，设备必须在启动 BitLocker 之前加入域。默认值为关。
- 自定义预引导恢复消息和 **URL**：指定 BitLocker 是否在恢复屏幕上显示自定义的消息和 URL。如果设置为开，将显示以下额外的设置：使用默认恢复消息和 **URL**、使用空恢复消息和 **URL**、使用自定义恢复消息和使用自定义恢复 **URL**。如果设置为关，将显示默认恢复消息和 URL。默认值为关。
- 配置固定驱动器恢复：为用户配置用于 BitLocker 加密的固定驱动器的恢复选项。BitLocker 不向用户显示与固定驱动器加密有关的消息。要在启动过程中解锁驱动器，用户需要提供密码或智能卡。用户在固定驱动器上启用了 BitLocker 加密时，启动解锁设置（不在此策略中）将在 BitLocker 界面上显示。有关相关设置的信息，请参阅此列表中前面部分的配置操作系统驱动器恢复。默认值为关。

- 阻止对不使用 **BitLocker** 的固定驱动器进行写入访问：如果设置为开，则仅当固定驱动器通过 BitLocker 加密时，用户才能向这些驱动器写入数据。默认值为关。
- 阻止对不使用 **BitLocker** 的可移动驱动器进行写入访问：如果设置为开，则仅当可移动驱动器通过 BitLocker 加密时，用户才能向这些驱动器写入数据。请根据贵组织是否允许在其他组织可移动的驱动器上具有访问权限来配置此设置。默认值为关。
- 其他磁盘加密提示：允许您禁用对设备上的其他磁盘加密的警告提示。默认值为关。

浏览器设备策略

March 27, 2020

可以创建适用于 Samsung SAFE 或 Samsung KNOX 设备的浏览器设备策略，以定义用户设备是否可以使用浏览器，或限制用户设备可以使用的浏览器功能。

在 Samsung 设备上，可以完全禁用浏览器，也可以启用或禁用弹出消息、JavaScript、Cookie、自动填充和是否强制显示欺诈警告。

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。

Samsung SAFE 和 **Samsung KNOX** 设置

- 禁用浏览器：选择是否在用户设备上完全禁用 Samsung 浏览器。默认值为关，表示允许用户使用此浏览器。禁用此浏览器后，将不再显示以下选项。
- 禁用弹出窗口：选择是否允许在此浏览器上显示弹出消息。
- 禁用 **JavaScript**：选择是否允许在此浏览器上运行 JavaScript。
- 禁用 **Cookie**：选择是否允许 Cookie。
- 禁用自动填充：选择是否允许用户启用此浏览器的自动填充功能。
- 强制显示欺诈警告：选择在用户访问欺诈性或存在漏洞的 Web 站点时是否显示警告。

日历 **(CalDav)** 设备策略

April 14, 2020

可以在 XenMobile 中添加一个设备策略，用于向用户的 iOS 或 macOS 设备添加日历 (CalDAV) 帐户，使用户可以将其计划数据与任何支持 CalDAV 的服务器同步。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CalDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CalDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。
- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CalDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CalDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。
- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

手机网络设备策略

April 14, 2020

此策略允许您在 iOS 设备上配置手机网络设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 附加 **APN**
  - 名称：此配置的名称。
  - 身份验证类型：在清单上，单击“质询握手身份验证协议” (**CHAP**) 或密码身份验证协议 (**PAP**)。默认值为 **PAP**。
  - 用户名和密码：用于身份验证的用户名和密码。
- **APN**
  - 名称：接入点名称 (APN) 配置的名称。
  - 身份验证类型：在列表中，单击 **CHAP** 或 **PAP**。默认值为 **PAP**。
  - 用户名和密码：用于身份验证的用户名和密码。
  - 代理服务器：代理服务器网络地址。
  - 代理服务器端口：代理服务器端口。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

连接管理器设备策略

March 27, 2020

在 XenMobile 中，可以为自动连接到 Internet 的应用程序指定连接设置并提供网络。此策略仅适用于 Windows Pocket PC。

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 Mobile/CE 设置

> 注意：
>
> 内置办公网络表示所有连接均指向公司的 Intranet。内置 **Internet** 表示所有连接均指向 Internet。

- 自动连接到专用网络的应用程序使用：在列表中，单击内置办公网络或内置 **Internet**。默认值为内置办公网络。

- 自动连接到 **Internet** 的应用程序使用：在列表中，单击内置办公网络或内置 **Internet**。默认值为内置办公网络。

连接计划设备策略

January 5, 2022

> 重要：
>
> Citrix 建议使用 Firebase Cloud Messaging (FCM) 来控制从 Android、Android Enterprise 和 Chrome OS 设备连接到 XenMobile Server。有关使用 FCM 的信息，请参阅 Firebase Cloud Messaging。

如果选择不使用 FCM，可以创建连接计划策略，用于控制用户设备如何及何时连接到 XenMobile Server。

可以指定用户需要手动连接其设备或设备在定义的时间范围内进行连接。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

平台设置

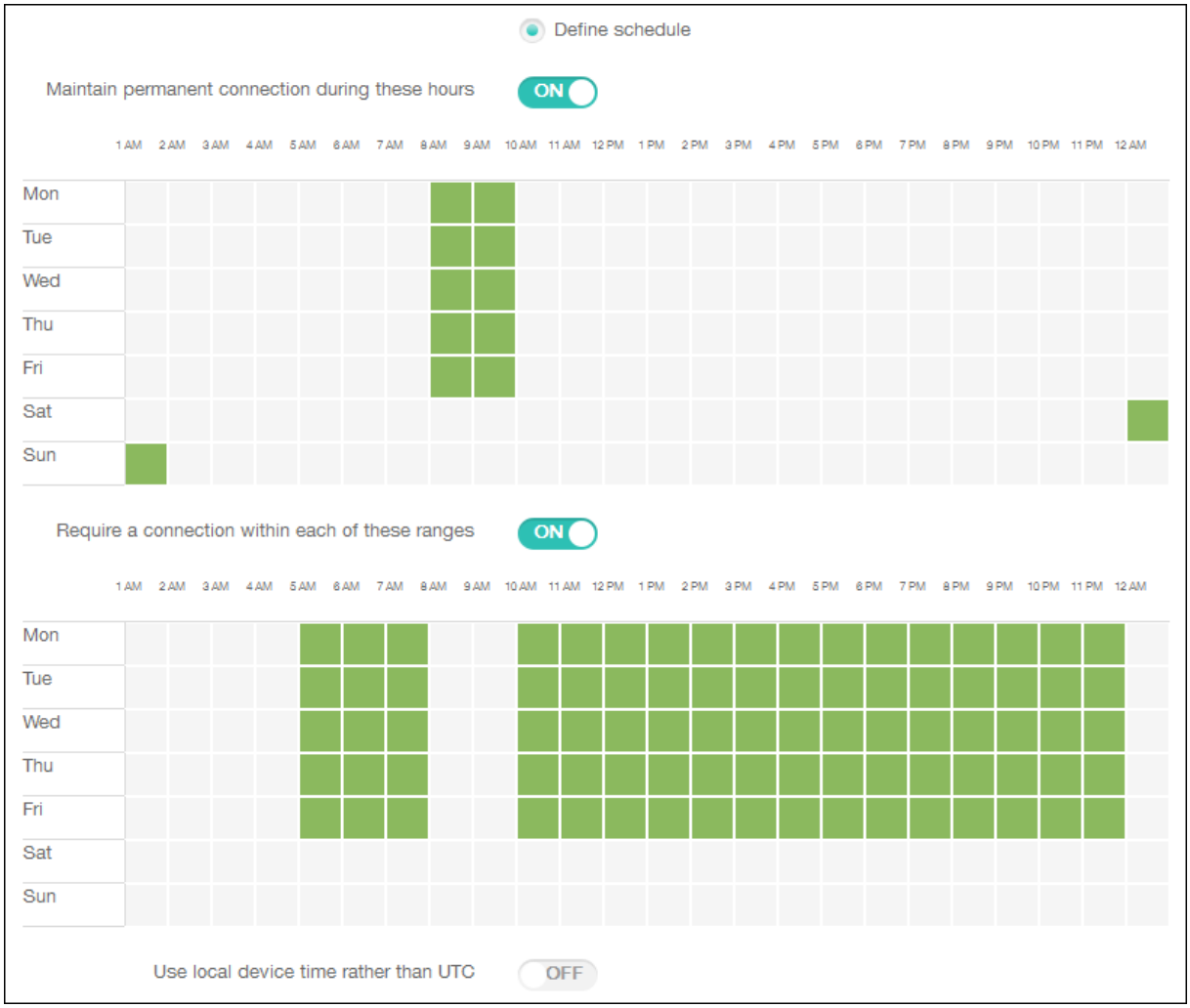
- 需要连接设备：单击要为此计划设置的选项。
  - 总是：连接永久保持活动状态。在丢失网络连接后，用户设备上的 XenMobile 尝试重新连接到 XenMobile Server，并通过以固定间隔传输控制数据包监视连接。Citrix 建议使用此选项以优化安全性。如果选择总是，还要对设备通道策略使用定义连接超时设置以确保连接不会耗尽电池电量。通过保持连接处于活动状态，您可以根据需要将擦除或锁定等安全命令推送到设备。此外，还必须在部署到设备的每个策略中选择部署计划选项为始终启用的连接部署。
  - 从不：手动进行连接。用户必须从其设备上的 XenMobile 启动连接。Citrix 建议不要对生产部署使用此选项，因为这会阻止您将安全策略部署到设备，因此，用户从不会收到任何新应用程序或策略。
  - 每隔：按照指定间隔进行连接。如果此选项生效，则当您发送锁定或擦除等安全策略时，XenMobile 将在下次设备连接时在设备上处理该操作。选择此选项后，将显示每隔 **N** 分钟连接一次字段，您必须在其中输入设备必须进行重新连接的间隔分钟数。默认值为 **20**。
  - 定义计划：启用后，在网络连接断开后，用户设备上的 XenMobile 尝试重新连接到 XenMobile Server，并在您定义的时间范围内通过以固定间隔传输控制数据包监视连接。有关如何定义连接时间范围的信息，请参阅下文中的“定义连接的时间范围”。
    - 在这些时段内保持永久连接：在定义的时间范围内，用户设备必须连接。
    - 要求每个范围内存在一个连接：在定义的任一时间范围内用户设备必须至少连接一次。
    - 使用本地设备时间而非 **UTC**：将定义的时间范围与本地设备时间而非协调世界时 (UTC) 同步。

定义连接的时间范围

启用下列选项时，将显示一个时间表，您可以利用此时间表设置所需的时间范围。您可以启用其中一个选项，也可以同时启用两个选项，以满足在指定时间需要永久连接或在特点时限内需要连接的需求。时间表中的每个方格代表 30 分钟，

因此，如果您希望在每个工作日的上午 8:00 到上午 9:00 之间连接，应单击时间表上每个工作日的上午 8:00 到上午 9:00 之间的两个方格。

例如，下图中的两个时间表需要在每个工作日的上午 8:00 到上午 9:00 之间进行永久连接，在周六上午 12:00 到周日上午 1:00 之间进行永久连接，在每个工作日的上午 5:00 到上午 8:00 或上午 10:00 到下午 11:00 点之间至少有一个连接。



联系人 **(CardDAV)** 设备策略

April 14, 2020

可以在 XenMobile 中添加一个设备策略，用于向用户的 iOS 或 macOS 设备添加 iOS 联系人 (CardDAV) 帐户，使用户可以将其联系人数据与任何支持 CardDAV 的服务器同步。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CardDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CardDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。
- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- 帐户说明：键入帐户说明。此字段为必填字段。
- 主机名：键入 CardDAV 服务器的地址。此字段为必填字段。
- 端口：键入连接到 CardDAV 服务器时使用的端口。此字段为必填字段。默认值为 **8443**。
- 主体 **URL**：键入用户日历的基本 URL。
- 用户名：键入用户的登录名称。此字段为必填字段。
- 密码：键入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为开。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

控制操作系统更新设备策略

October 13, 2021

通过控制操作系统更新设备策略，可以：

- 将最新的操作系统更新部署到受监督的 iOS 设备。

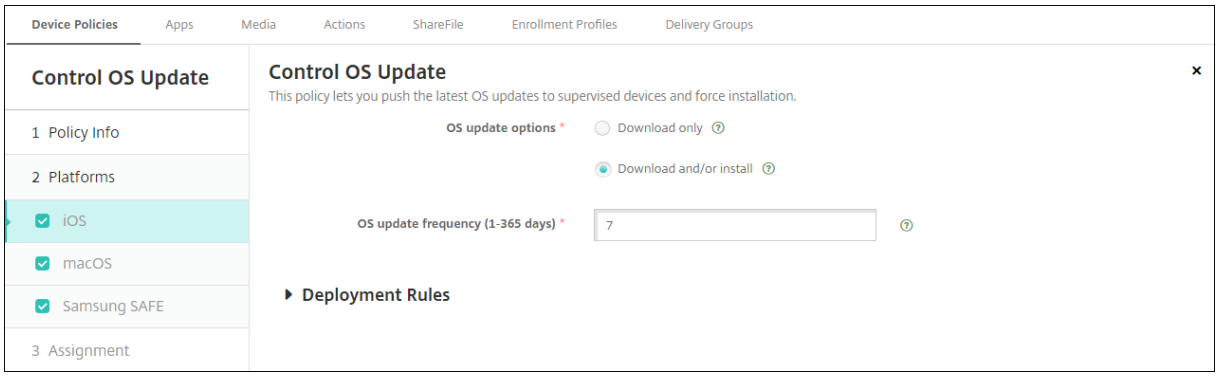
  “操作系统更新” 设备策略仅适用于在 Apple 部署计划中注册的受监督设备。

- 将最新的操作系统和应用程序更新部署到注册了 DEP 并且运行 macOS 10.11.5 及更高版本的 macOS 设备。
- 将最新的操作系统更新部署到受监督的 Samsung SAFE 设备。

  对于 Samsung SAFE 设备，XenMobile 会将控制操作系统更新策略发送到 Secure Hub，后者随后会将该策略应用于设备。XenMobile Server 发送策略时以及设备接收策略时，都会显示管理 **>** 设备页面。

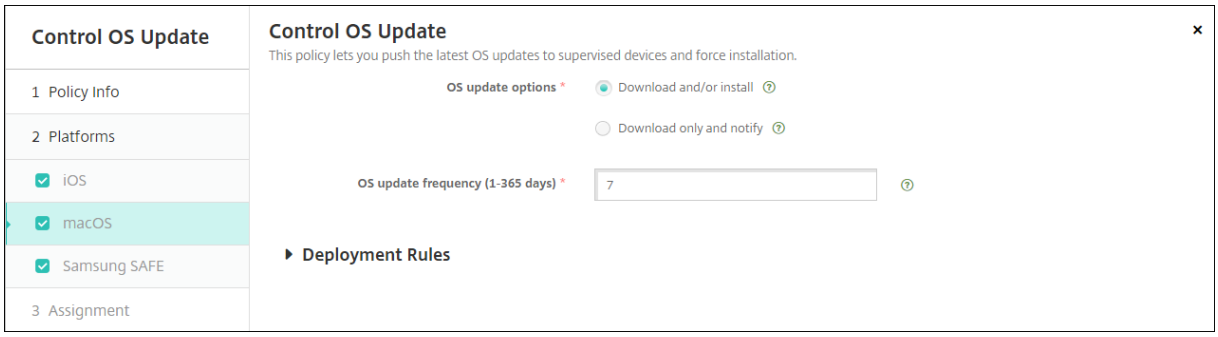
要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- 操作系统更新选项：这两个选项都将根据操作系统更新频率将最新的操作系统更新下载到受监督的设备。设备将提示用户安装更新。提示在用户解锁设备后可见。
- 操作系统更新频率：确定 XenMobile 检查和更新设备操作系统的频率。默认值为 **7** 天。

macOS 设置



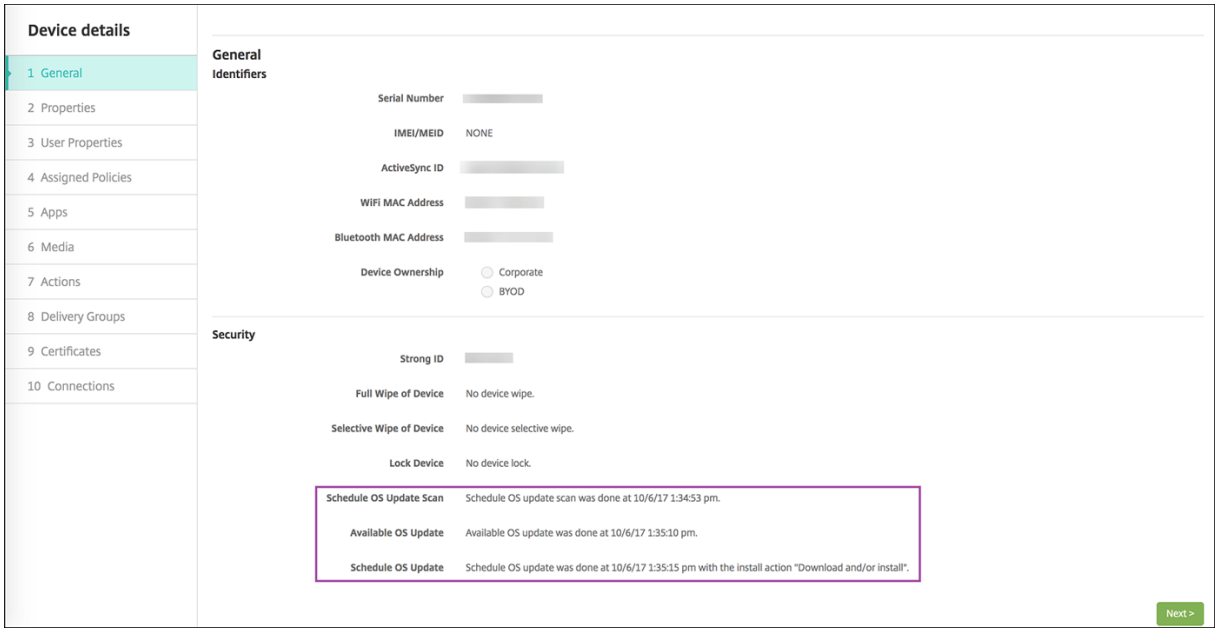
- 操作系统更新选项：这两个选项都将根据操作系统更新频率下载最新的 macOS 更新。可以选择通过提供更新的 App Store 来安装更新或通知用户。
- 操作系统更新频率：确定 XenMobile 检查和更新设备操作系统的频率。默认值为 **7** 天。

获取 **iOS** 和 **macOS** 更新操作的状态

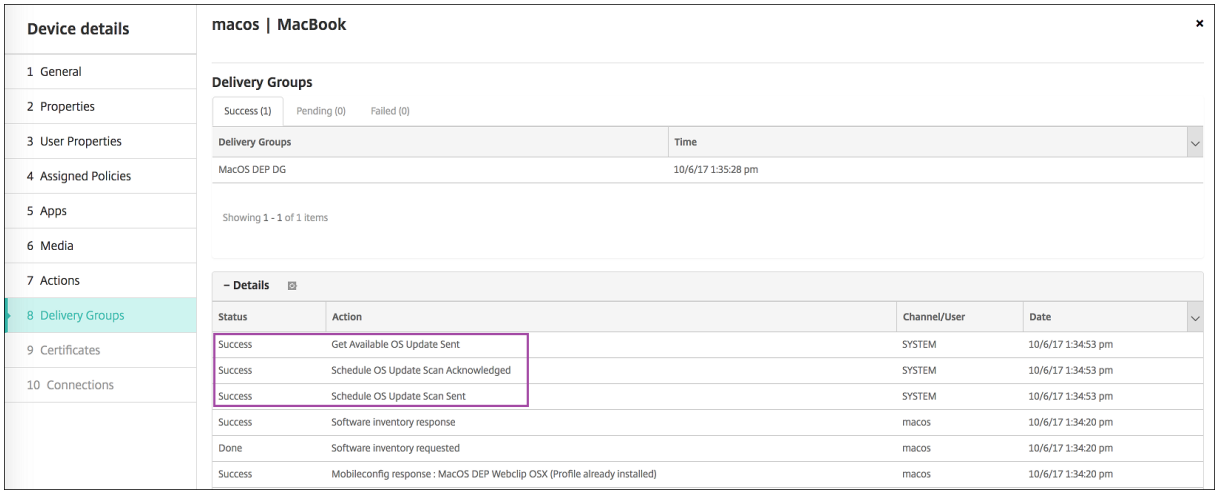
对于 iOS 和 macOS，XenMobile 不向设备部署控制操作系统更新策略。相反，XenMobile 将使用该策略向设备发送以下 MDM 命令：

- 安排操作系统更新扫描：请求设备在后台扫描操作系统更新。（对 iOS 是可选的）
- 可用的操作系统更新：查询设备中的可用操作系统更新列表。
- 安排操作系统更新：请求设备执行 macOS 更新、应用程序更新或两者。因此，设备操作系统负责确定何时应下载或安装操作系统和应用程序更新。

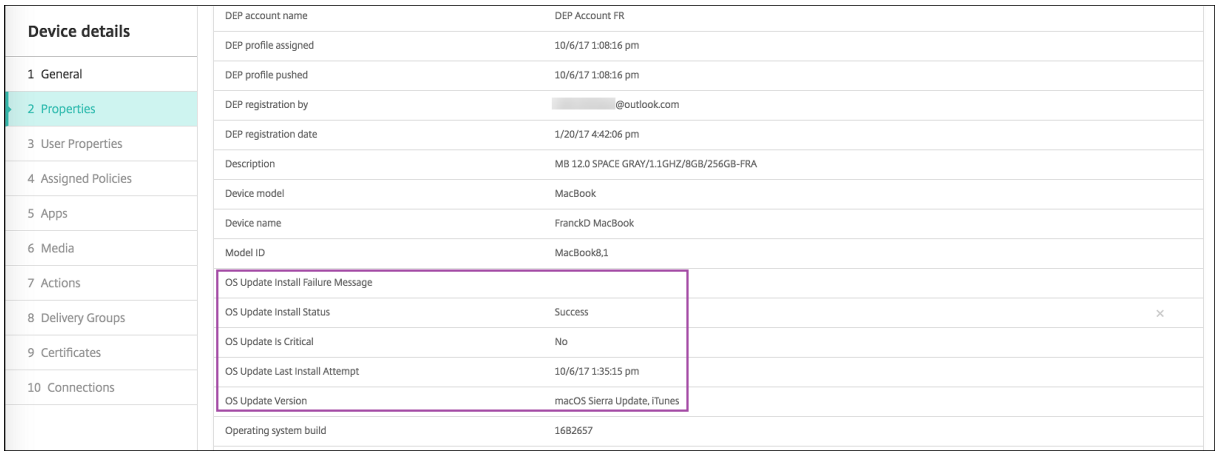
管理 **>** 设备 **>** 设备详细信息 **(**常规**)** 页面显示安排的和可用的操作系统更新扫描以及安排的 macOS 和应用程序更新的状态。

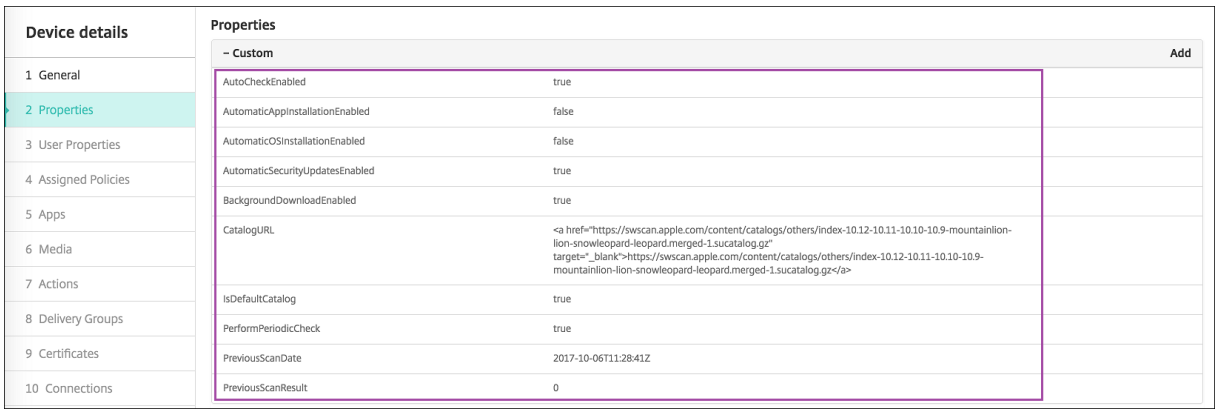


有关更新操作的状态的更多详细信息，请转至管理 **>** 设备 **>** 设备详细信息 **(**交付组**)** 页面。



有关可用的操作系统更新和最后一次安装尝试等详细信息，请转至管理 **>** 设备 **>** 设备详细信息 **(**属性**)** 页面。





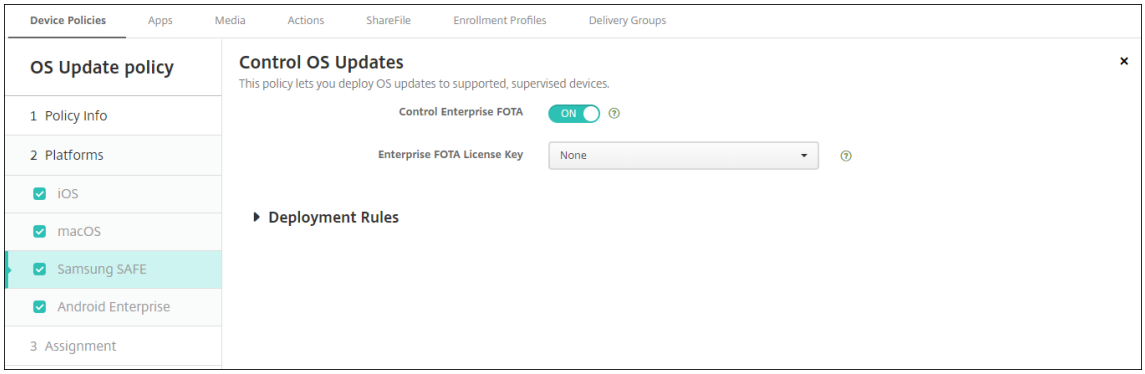
Samsung SAFE 设置

Samsung Enterprise FOTA（也称为 E-FOTA）允许您确定设备更新的时间以及要使用的固件版本。要使用 E-FOTA，请执行以下操作：

1. 使用您从 Samsung 接收的密钥和许可证信息创建 Samsung MDM 许可证密钥设备策略。有关详细信息，请

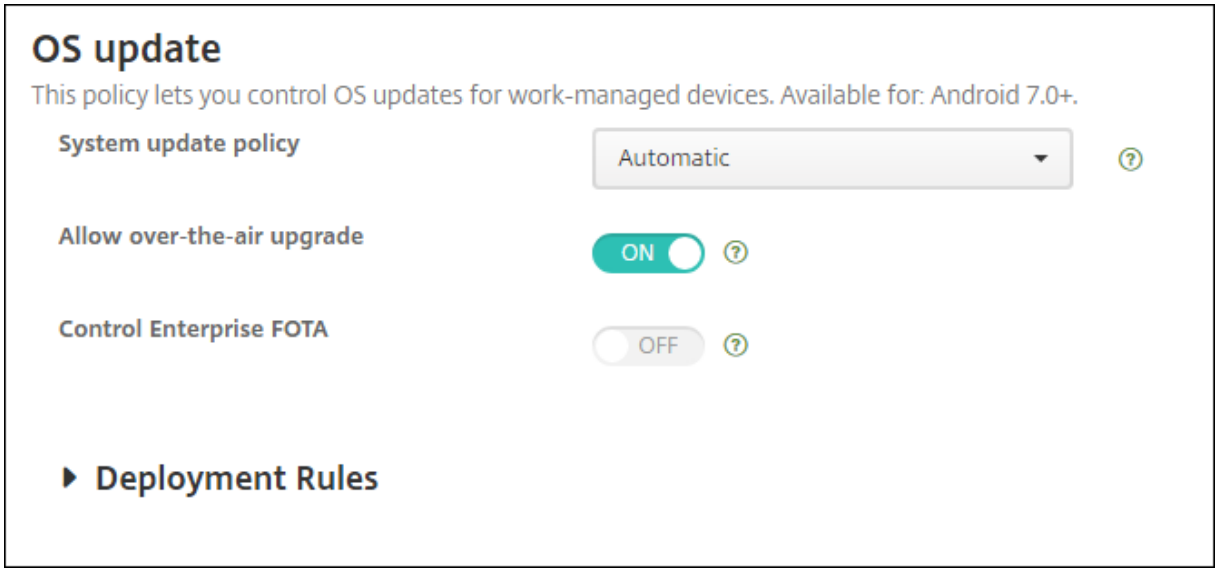
参阅 Samsung MDM 许可证密钥设备策略。

2. 创建控制操作系统更新设备策略以启用 Enterprise FOTA。



- 启用 **Enterprise FOTA**：设置为开。
- **Enterprise FOTA** 许可证密钥：选择 Samsung MDM 许可证密钥设备策略名称。

Android Enterprise 设置



- 系统更新策略：确定系统更新的发生时间。如果启用控制 **Enterprise FOTA** 设置，则无论此设置的配置为何，更新都会自动进行。
  - 自动：在更新可用时自动安装更新。
  - 窗口化：在开始时间和结束时间中指定的每日维护时段内自动安装更新。
    * 开始时间：维护时段的开始时间，测量方式为在设备本地时间从午夜开始的分钟数 (**0** - **1440**)。默认值为 **0**。
    * 结束时间：维护时段的结束时间，测量方式为在设备本地时间从午夜开始的分钟数 (**0** - **1440**)。默认值为 **120**。
  - 推迟：允许用户将更新最长推迟 30 天。

- 允许无线升级：如果禁用，用户设备将无法以无线方式接收软件更新。默认值为开。
- 控制 **Enterprise FOTA**：如果启用，Samsung 设备将检查并自动安装最新更新。禁用后，用户可以检查更新并进行手动安装。适用于运行 Samsung Knox 3.0 或更高版本的 Android Enterprise 设备。默认值为关。
  - **Enterprise FOTA** 许可证密钥：选择检查更新时要使用的许可证密钥。可以在 Samsung MDM 许可证密钥策略中配置此设置。适用于运行 Samsung Knox 3.0 或更高版本的 Android Enterprise 设备。默认值为无。可以使用 **Samsung MDM** 许可证密钥设备策略设置密钥。请参阅 Samsung MDM 许可证密钥设备策略。

将应用程序复制到 **Samsung** 容器设备策略

January 5, 2022

对于已安装在设备上的应用程序，您可以指定将应用程序复制到受支持的 Samsung 设备上的 KNOX 容器。有关受支持的设备的信息，请参阅 Samsung 文章 Devices built on Knox（在 Knox 上构建的设备）。

复制到 KNOX 容器的应用程序仅当用户登录 KNOX 容器时可用。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

必备条件

- 在 XenMobile 中注册设备。
- 部署 Samsung MDM 密钥（ELM 和 KLM）。有关操作方法，请参阅 Samsung MDM 许可证密钥设备策略。
- 在设备上安装应用程序。
- 在设备上初始化 KNOX 以将应用程序复制到 KNOX 容器。

平台设置

- 新建应用程序：对于要添加到此列表中的每个应用程序，请单击添加，然后执行以下操作：
  - 键入软件包 ID，例如，对于 LacingArt 应用程序，键入 com.mobiwolf.lacingart。
  - 单击保存或取消。

凭据设备策略

January 5, 2022

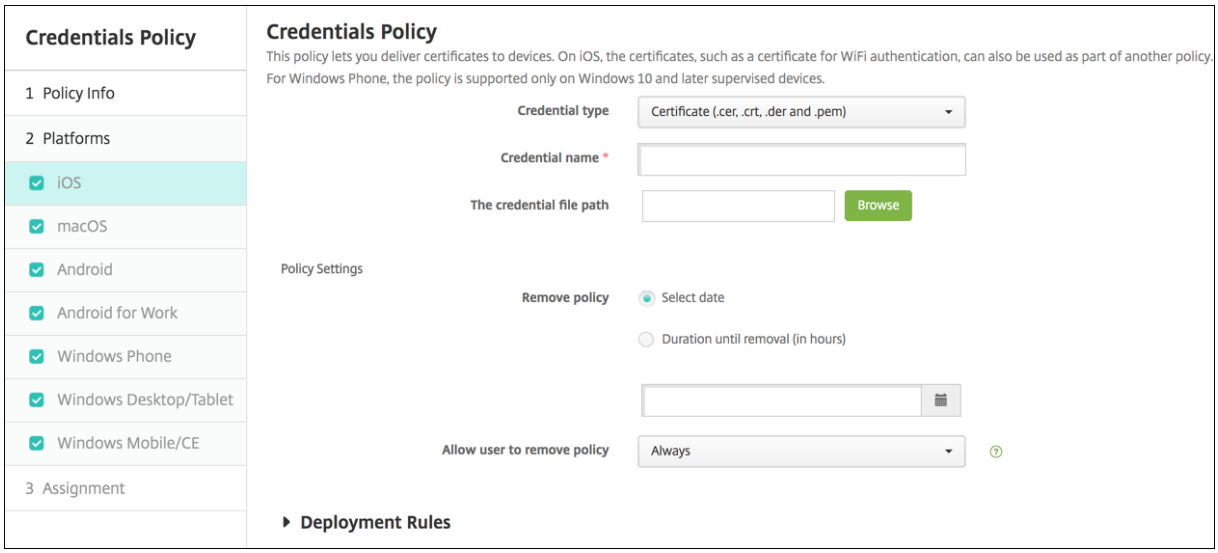
凭据设备策略指向在 XenMobile 中配置的 PKI。例如，您的 PKI 配置可能包括 PKI 实体、密钥库、凭据提供程序或服务器证书。有关凭据的详细信息，请参阅证书和身份验证。

每个受支持的平台都需要一组不同的值，本文将对此进行介绍。

> 注意：
>
> 创建此策略前，需要具有计划用于各平台的凭据信息，以及任何证书和密码。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

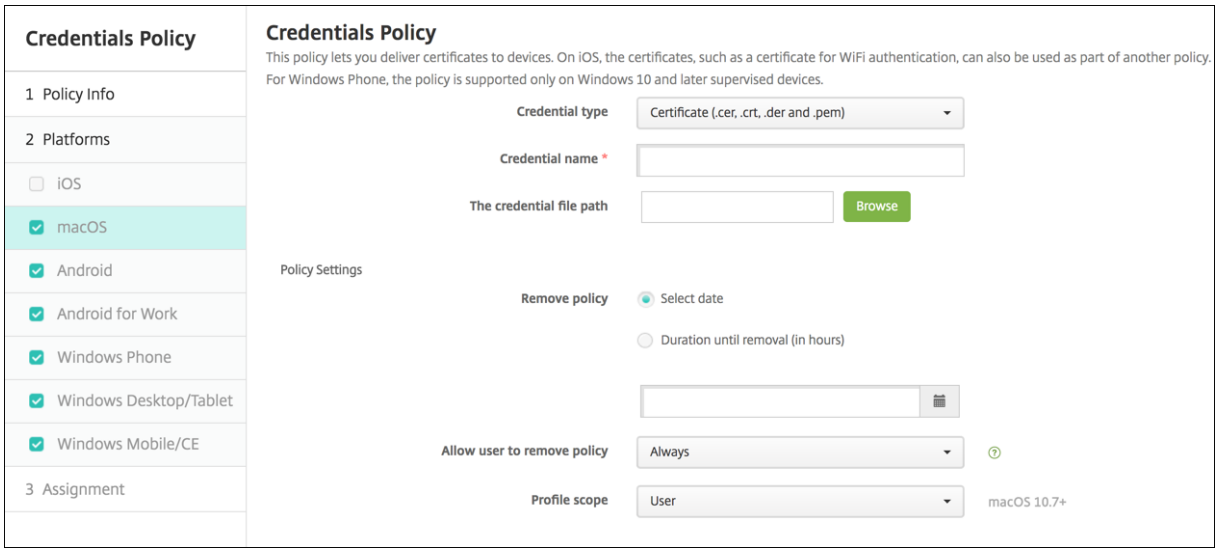
iOS 设置



配置以下设置：

- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：单击“浏览”并导航到凭据文件所在位置，选择此文件。
  - 密钥库
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：单击“浏览”并导航到凭据文件所在位置，选择此文件。
    - 密码：输入凭据的密钥库密码。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

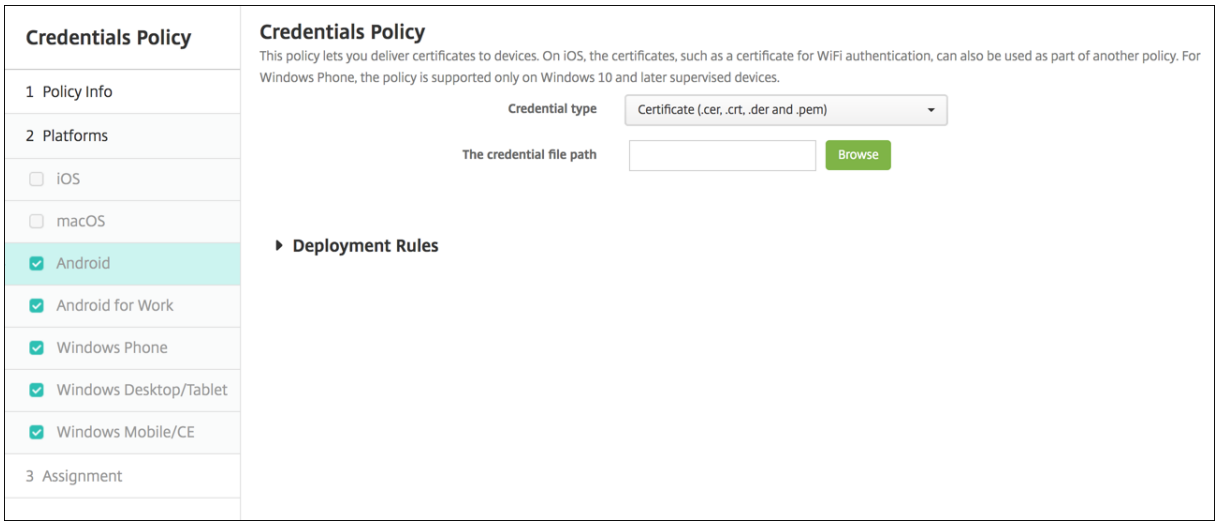
macOS 设置



配置以下设置：

- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
  - 密钥库
    - 凭据名称：输入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
    - 密码：输入凭据的密钥库密码。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

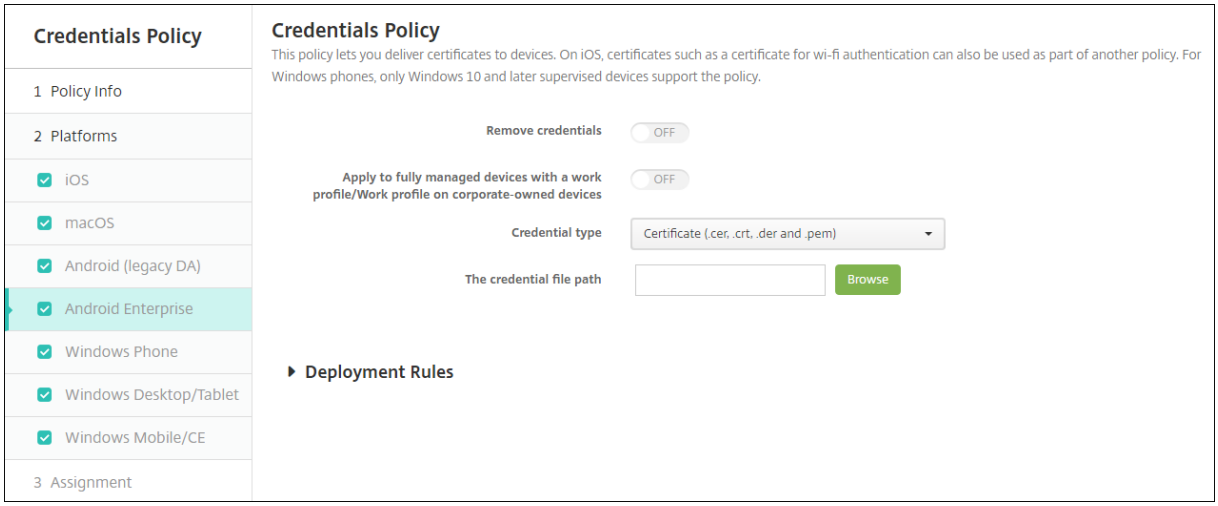
Android 设置



配置以下设置：

- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：单击“浏览”并导航到凭据文件所在位置，选择该文件。
  - 密钥库
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
    - 密码：键入凭据的密钥库密码。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。

Android Enterprise 设置



配置以下设置以确定 XenMobile 如何应用凭据设置：

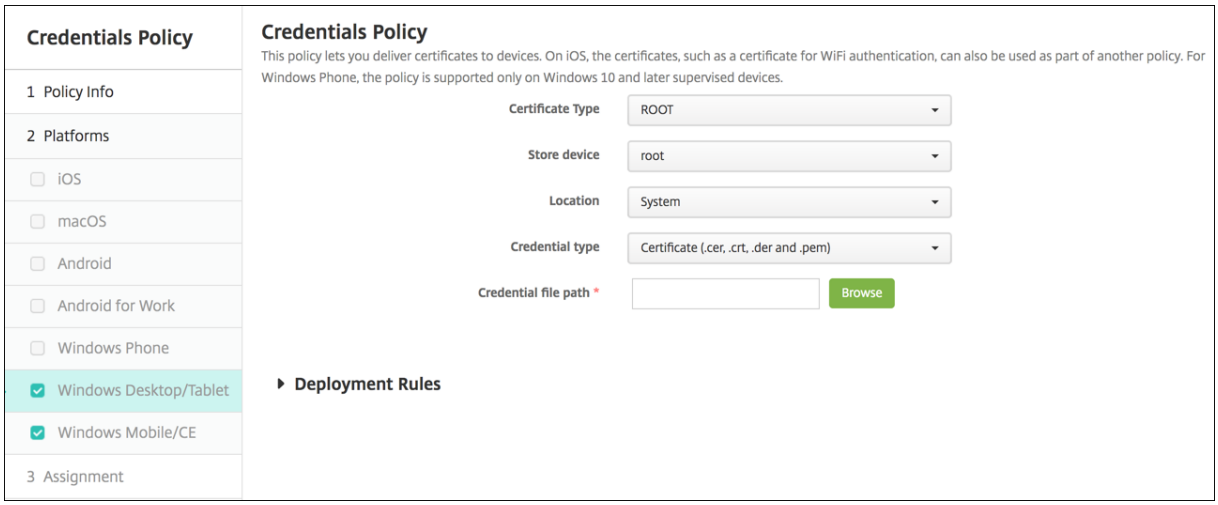
- 删除凭据：设置为开可配置以下设置。默认值为关。
  - 删除用户凭据：从托管密钥库中删除证书。默认值为关。
  - 删除受信任的根证书：卸载所有非系统 CA 证书。默认值为关。
- 应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备：允许您为具有工作配置文件的完全托管设备配置凭据策略设置。当此设置设为关时，您配置的凭据设置将仅应用于工作配置文件。当此设置设为关时，您配置的凭据设置将仅应用到设备。默认值为关。

配置凭据设置：

- 凭据类型：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - 证书
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
  - 密钥库
    - 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择此文件。
    - 证书别名：证书别名使应用程序能够更轻松地访问证书。在“Android Enterprise 托管配置”设备策略中配置证书别名。然后，在“凭据”设备策略中的证书别名字段中键入别名。应用程序将检索证书并对 VPN 进行身份验证，而无需用户执行任何操作。
    - 密码：键入凭据的密钥库密码。
  - 服务器证书
    - 服务器证书：在列表中，单击要使用的证书。
  - 凭据提供程序
    - 证书别名：证书别名使应用程序能够更轻松地访问证书。在“Android Enterprise 托管配置”设备策略中配置证书别名。然后，在“凭据”设备策略中的证书别名字段中键入别名。应用程序将检索证书并对 VPN 进行身份验证，而无需用户执行任何操作。
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。
    - 要使用证书的应用程序：指定对来自此提供程序的凭据具有静默访问权限的应用程序：单击添加，选

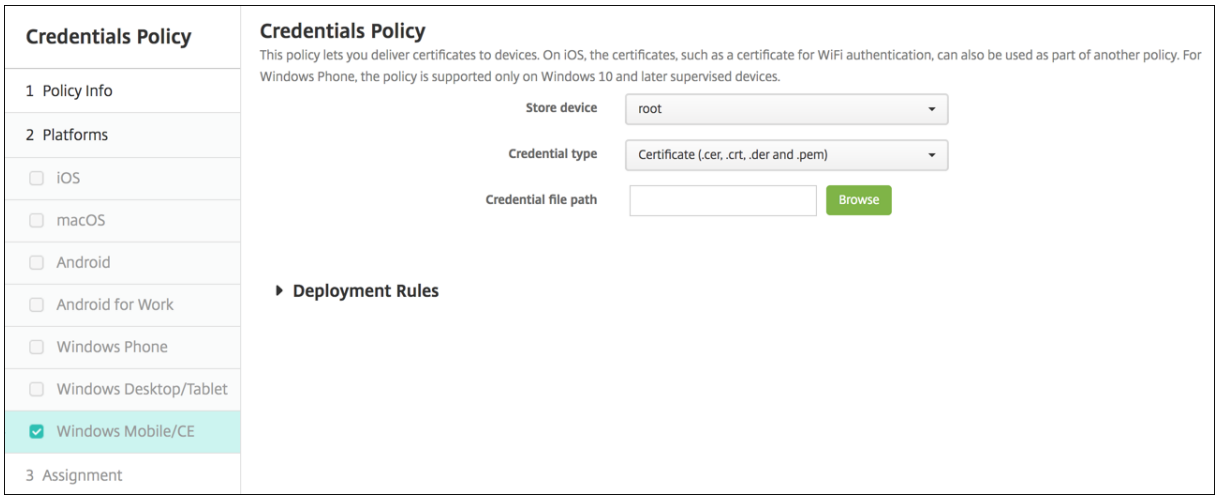
择一个应用程序，然后单击保存。

Windows Desktop/Tablet 设置



- 证书类型：在列表中，单击根证书或客户端证书。
- 如果单击根证书，则配置以下设置：
  - 存储设备：在列表中，单击根、我的或 **CA** 以选择凭据的证书存储位置。如果选择我的，则证书将存储在用户的证书存储中。
  - 位置：对于 Windows 10 和 Windows 11 Tablet，系统是唯一的位置。
  - 凭据类型：对于 Windows 10 和 Windows 11 Tablet，证书是唯一的凭据类型。
  - 凭据文件路径：单击浏览并导航到证书文件所在位置，选择此证书文件。
- 如果单击客户端证书，则配置以下设置：
- 位置：对于 Windows 10 和 Windows 11 Tablet，系统是唯一的位置。
- 凭据类型：对于 Windows 10 和 Windows 11 Tablet，密钥库是唯一的凭据类型。
- 凭据名称：键入凭据的名称。此字段为必填字段。
- 凭据文件路径：单击浏览并导航到证书文件所在位置，选择此证书文件。
- 密码：键入与凭据关联的密码。此字段为必填字段。

Windows Mobile/CE 设置



- 存储设备：在列表中，单击凭据的证书存储位置。默认值为根。选项包括：
  - 特许执行信任颁发机构：使用属于此存储的证书签名的应用程序将在特许信任级别下运行。
  - 非特许执行信任颁发机构：使用属于此存储的证书签名的应用程序将在一般信任级别下运行。
  - **SPC(**软件发行程序证书**)**：软件发行程序证书 (SPC) 用于签名.cab 文件。
  - 根：包含根证书的证书存储。
  - **CA**：包含加密信息（包括中间证书颁发机构）的证书存储。
  - 我的：包含最终用户个人证书的证书存储。
- 凭据类型：证书是适用于 Windows Mobile/CE 设备的唯一凭据类型。
- 凭据文件路径：单击浏览并导航到凭据文件所在位置，选择该文件。

自定义 XML 设备策略

January 5, 2022

可以在 XenMobile 中创建自定义 XML 策略，以在受支持的 Windows、Zebra Android 以及 Android Enterprise 设备上自定义以下功能：

- 预配，包括配置设备以及启用或禁用功能
- 设备配置，包括允许用户更改设置和设备参数
- 软件升级，包括提供要加载到设备中的新软件或缺陷修复（包括应用程序和系统软件）
- 故障管理，包括接收来自设备的错误和状态报告

> 注意：
>
> 创建 XML 内容时，请谨慎使用% 字符。% 字符是 XML 保留字符，仅用于转义 XML 特殊字符。要在名称中使用%，请将其编码为%25。

对于 Windows 设备：可以在 Windows 中使用 Open Mobile Alliance Device Management (OMA DM) API 创

建自己的自定义 XML 配置。本主题中不介绍如何使用 OMA DM API 创建自定义 XML。有关使用 OMA DM API 的详细信息，请参阅 Microsoft Developer Network 站点上的 OMA Device Management（OMA 设备管理）。

对于 Zebra Android 和 Android Enterprise 设备：请使用 MX Management System (MXMS) 创建自定义 XML 配置。使用 MXMS API 创建自定义 XML 不在本文的探讨范围之内。有关使用 MXMS 的详细信息，请参阅 Zebra 站点上的 About MX（关于 MX）。

> 注意：
>
> 对于 Windows 10 RS2 Phone：用于禁用 Internet Explorer 的自定义 XML 策略或限制策略部署到 Phone 后，浏览器将保持已启用。要解决此问题，请重新启动 Phone。这是第三方问题。

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。

Windows Phone、Windows Desktop/Tablet、Zebra Android 和 Android Enterprise 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，XenMobile 将检查 XML 内容语法。内容框下将显示所有语法错误。请先修复所有错误，然后再继续操作。

  如果没有语法错误，将显示自定义 **XML** 策略分配页面。

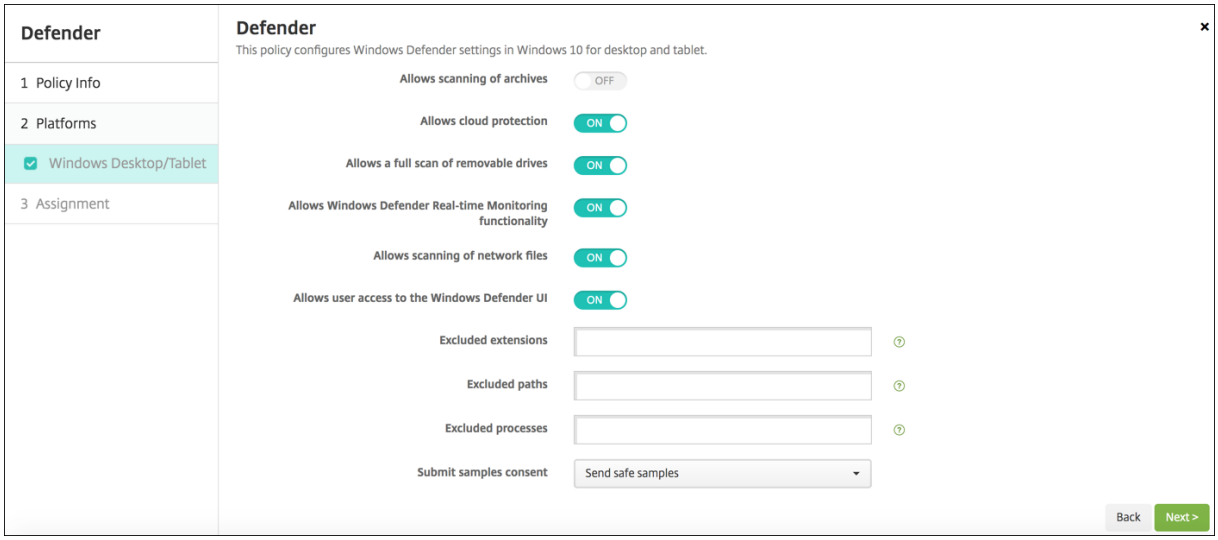
Defender 设备策略

January 5, 2022

Windows Defender 是 Windows 10 和 Windows 11 附带的恶意软件防护功能。可以使用 XenMobile 设备策略 Defender 来为台式机和平板电脑配置适用于 Windows 10 和 Windows 11 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 Desktop 和 Tablet 设置



- 允许扫描存档：允许或不允许 Defender 扫描存档的文件。默认值为关。
- 允许启用云保护：允许或不允许 Defender 向 Microsoft 发送有关恶意软件活动的信息。默认值为开。
- 允许完全扫描可移动驱动器：允许或不允许 Defender 扫描可移动驱动器，例如 U 盘。默认值为开。
- 允许启用 **Windows Defender** 实时监视功能：默认值为开。
- 允许扫描网络文件：允许或不允许 Defender 扫描网络文件。默认值为开。
- 允许用户访问 **Windows Defender UI**：指定用户是否可以访问 Windows Defender 用户界面。此设置在下次启动用户设备时生效。如果此设置设为关，则用户不会收到任何 Windows Defender 通知。默认值为开。
- 排除的扩展名：要从实时扫描或计划的扫描中排除的扩展名。要分隔扩展名，请使用 | 字符。例如，“lib | obj”。
- 排除的路径：要从实时扫描或计划的扫描中排除的路径。要分隔路径，请使用 | 字符。例如，“C:\Example|C:\Example1”。
- 排除的进程：要从实时扫描或计划的扫描中排除的进程。要分隔进程，请使用 | 字符。例如，“C:\Example.exe|C:\Example1.exe”。
- 提交示例许可：控制是否向 Microsoft 发送可能需要进一步分析以确定是否是恶意的文件。选项：始终提示、发送安全示例、从不发送、发送所有示例。默认值为发送安全示例。

删除文件和文件夹设备策略

March 27, 2020

可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的文件或文件夹。

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 Mobile/CE 设置

- 要删除的文件和文件夹：对于要删除的每个文件或文件夹，单击“添加”，然后执行以下操作：
  - 路径：键入文件或文件夹的路径。
  - 类型：在列表中，单击“文件”或“文件夹”。默认值为“文件”。
  - 单击保存以保存文件或文件夹，或单击取消不保存文件夹或文件夹。

删除注册表项和值设备策略

March 27, 2020

可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的注册表项和值。

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。

Windows Mobile/CE 设置

- 要删除的注册表项和值：对于要删除的每个注册表项和值，单击添加，然后执行以下操作：
  - 注册表项：键入注册表项路径。这是必填字段。注册表项路径应以 HKEY_CLASSES_ROOT\ 或 HKEY_CURRENT_USER\ or HKEY_LOCAL_MACHINE\ 或 HKEY_USERS\ 开头。
  - 值：键入要删除的值名称，或让此字段留空以删除整个注册表项。
  - 单击保存以保存注册表项和值，或单击取消不保存注册表项和值。

设备运行状况证明设备策略

January 5, 2022

在 XenMobile 中，您可以要求 Windows 10 和 Windows 11 设备报告其运行状况，方法是让这些设备将特定数据和运行时信息发送给 Health Attestation Service (HAS) 进行分析。HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 XenMobile。XenMobile 收到运行状况证明证书后，根据运行状况证明证书的内容，部署您之前设置的自动操作。

HAS 验证的数据包括：

- AIK 是否存在
- Bit Locker 状态
- 启动调试是否已启用
- 启动管理器修订列表版本
- 代码完整性是否已启用
- 代码完整性修订列表版本

- Apple 部署计划策略
- ELAM 驱动程序是否已加载
- 颁发时间
- 内核调试是否已启用
- PCR
- 重置计数
- 重新启动计数
- 安全模式是否已启用
- SBCP 哈希
- 安全启动是否已启用
- 测试签名是否已启用
- 已启用 VSM
- 已启用 WinPE

有关详细信息，请参阅 Microsoft 设备 HealthAttestation CSP 页面。

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。

使用 **Microsoft** 云配置 **DHA**

添加一个设备运行状况证明策略，并为您选择的每个平台配置此设置：

- 启用设备运行状况证明：选择是否需要设备运行状况证明。默认值为关。

使用本地 **Windows DHA** 服务器配置 **DHA**

要在本地启用 DHA，请先配置一个 DHA 服务器。然后创建 XenMobile Server 策略以启用本地 DHA 服务。

1. 要配置 DHA 服务器，请在运行 Windows Server 2016 技术预览版 5 或更高版本的计算机上安装 DHA 服务器角色。有关说明，请参阅配置本地设备运行状况证明服务器。
2. 添加一个设备运行状况证明策略，并配置以下设置：
   - 启用设备运行状况证明：设置为开。
   - 配置本地 **Health Attestation Service**：设置为开。
   - 本地 **DHA** 服务 **FQDN**：键入您设置的 DHA 服务器的完全限定域名。
   - 本地 **DHA API** 版本：选择 DHA 服务器上安装的 DHA 服务版本。

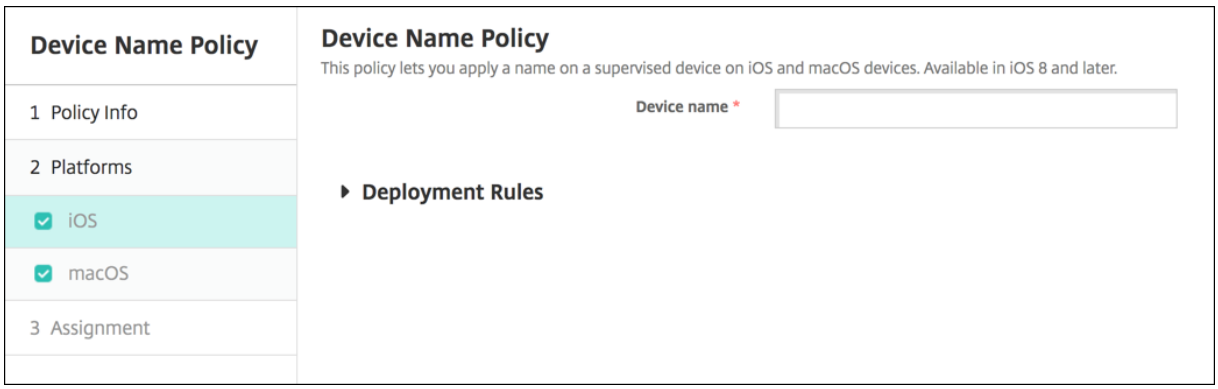
设备名称设备策略

January 5, 2022

可以在受监督的 iOS 和 macOS 设备上设置名称，以便轻松识别设备。可以使用宏、文本或二者的组合定义设备的名称。例如，要将设备名称设置为设备的序列号，可以使用 ${device.serialnumber}。要将设备的名称设置为用户名和域的组合，可以使用 ${user.username}@example.com。有关宏的详细信息，请参阅 XenMobile 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、宏组合或宏和文本组合，为每个设备指定唯一名称。例如，使用 ${device.serialnumber} 将设备名称设置为每个设备的序列号，或使用 ${device.serialnumber} ${ user.username } 使设备名称中包含用户名。

教育配置设备策略

January 5, 2022

教育配置设备策略定义以下对象：

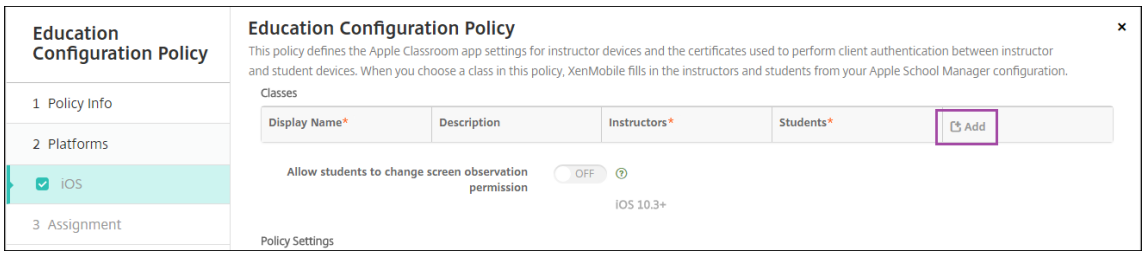
- 面向教师设备的 Apple“课堂”应用程序设置。
- 用于在教师与学生设备之间执行客户端身份验证的证书。

在此策略中选择一个班级时，XenMobile 控制台将填写您的 Apple 校园教务管理配置中的教师和学生。如果此策略中的 Apple“课堂”应用程序设置对所有班级都相同，请创建一个策略。

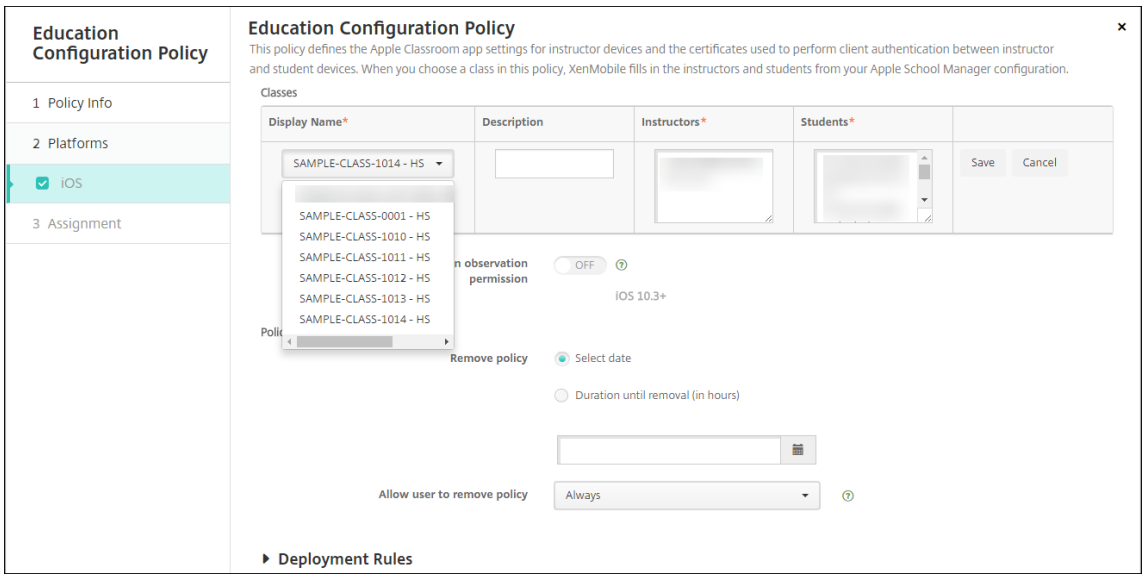
要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

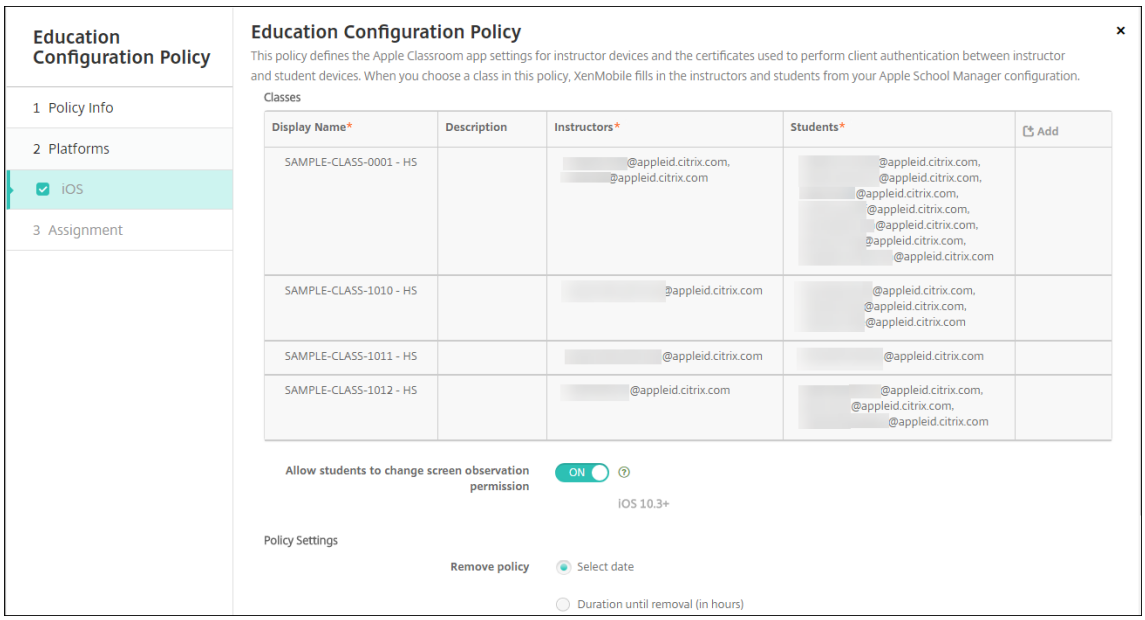
- 课程：要添加课程，请单击添加。



然后，单击显示名称列表。此时将显示从您的已连接 Apple 校园教务管理帐户中获取的班级列表。



从显示名称中选择班级时，XenMobile 将填写教师和学生。继续添加班级。



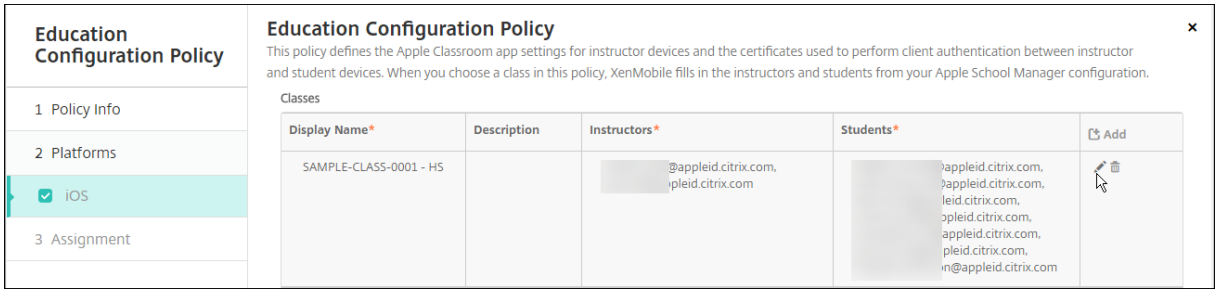
- 允许学生更改屏幕观察权限：如果设置为开，则注册参加托管课程的学生可以选择是否允许教师观察其设备屏幕。默认值为关。

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。

编辑策略中的班级信息

可以向班级添加说明（“课堂”应用程序中的“显示名称”）。还可以添加或删除教师和学生。XenMobile 不保存对您的 Apple 校园教务管理帐户所做的此类更改。有关详细信息，请参阅与 Apple 教育功能相集成中的“管理教师、学生和班级数据”。

将鼠标悬停在要编辑的班级的添加列上，然后单击铅笔图标。



要从策略中删除班级，请将鼠标悬停在要删除的班级的添加列上，然后单击垃圾桶图标。

企业中心设备策略

March 27, 2020

面向 Windows Phone 的企业中心设备策略允许您通过企业中心公司应用商店分发应用程序。

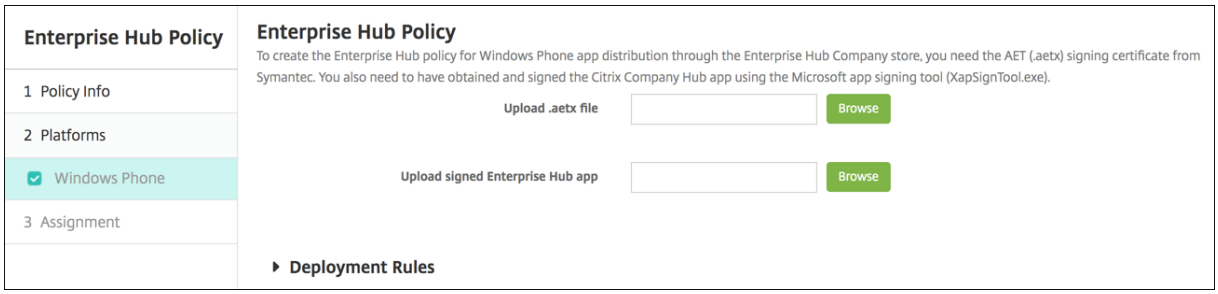
需要具备以下各项才能创建策略：

- 来自 DigiCert 的 AET (.aetx) 签名证书
- 使用 Microsoft 应用程序签名工具 (XapSignTool.exe) 签名的 Citrix Company Hub 应用程序

> 注意：
>
> 对于一种 Windows Phone Secure Hub 模式，XenMobile 仅支持一种企业中心策略。例如，要上载 Windows Phone Secure Hub for XenMobile Enterprise Edition，不应该使用不同版本的 Work Home for XenMobile Enterprise Edition 创建多个企业中心策略。设备注册期间只能部署初始企业中心策略。

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 Phone 设置



- 上载**.aetx** 文件：单击浏览并导航到.aetx 文件所在位置，选择此文件。
- 上载签名的企业中心应用程序：单击浏览并导航到企业中心应用程序所在位置，选择此应用程序。

Exchange 设备策略

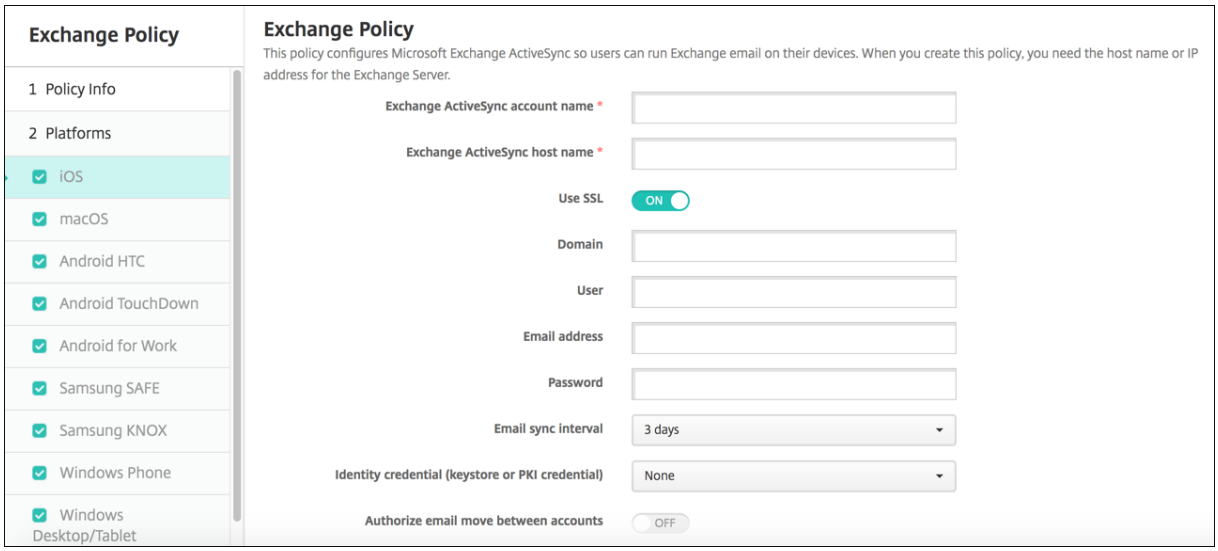
January 5, 2022

可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以允许其访问 Exchange 上托管的企业电子邮件。可以为 iOS、macOS、Android Enterprise、Samsung SAFE、Samsung KNOX、Windows Phone 和 Windows Tablet 创建策略。每个平台都需要一组不同的值，这些值将在以下各节中详细说明。

要创建此策略，需要 Exchange Server 的主机名或 IP 地址。有关 ActiveSync 设置的信息，请参阅 Microsoft 文章 ActiveSync CSP。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

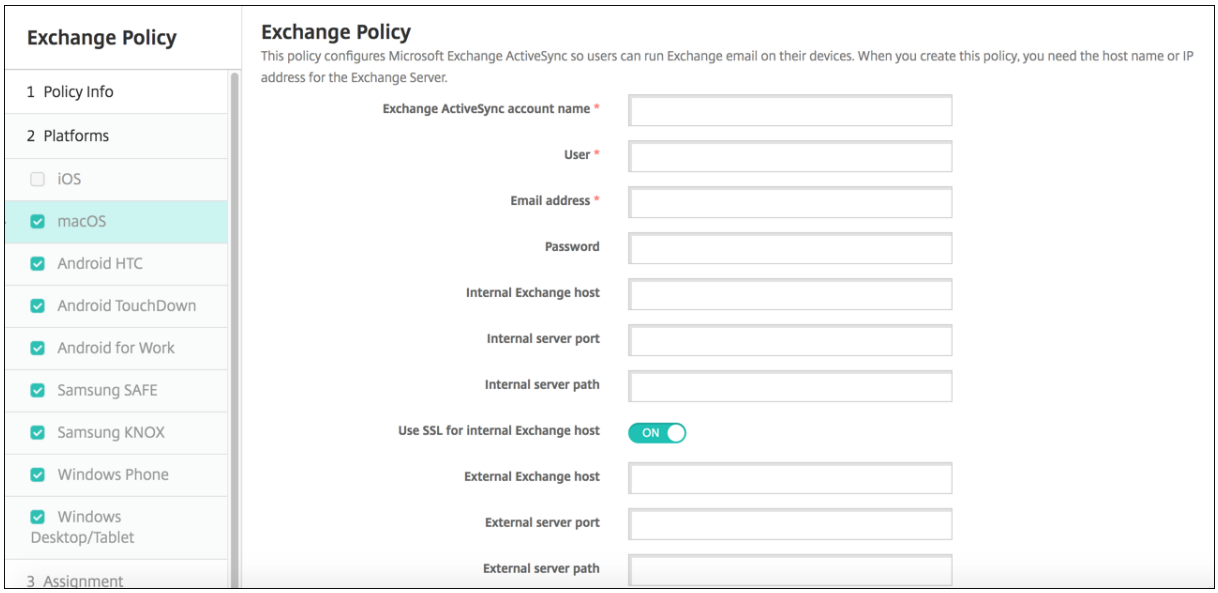
iOS 设置



- **Exchange ActiveSync** 帐户名称：键入显示在用户设备上的电子邮件帐户的说明。

- **Exchange ActiveSync** 主机名：键入电子邮件服务器的地址。
- 使用 **SSL**：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为开。
- 域：输入 Exchange Server 所在的域。可以在此字段中使用系统宏 $user.domainname 自动查找用户的域名。
- 用户：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 $user.username 自动查找用户名。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 $user.mail 自动查找用户的电子邮件帐户。
- 使用 **OAuth**：如果设置为开，连接将使用 OAuth 进行身份验证。默认值为关。此选项适用于 iOS 12.0 及更高版本。
- 密码：输入 Exchange 用户帐户的可选密码。使用 **OAuth** 设置为于时不会显示此设置。
- 电子邮件同步时间间隔：在列表中，选择电子邮件与 Exchange Server 同步的频率。默认值为 **3** 天。
- 身份凭据 **(**密钥库或 **PKI)**：如果为 XenMobile 配置了身份提供程序，则在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。默认设置为无。
- 授权电子邮件在帐户之间移动：选择是否允许用户将电子邮件从此帐户移出到另一个帐户以及从其他帐户转发和答复。默认值为关。
- 仅从电子邮件应用程序发送电子邮件：选择是否限制用户只能从 iOS 邮件应用程序发送电子邮件。默认值为关。
- 禁用最新电子邮件同步：选择是否阻止用户同步最近使用的地址。默认值为关。此选项仅适用于 iOS 6.0 及更高版本。
- 启用 **S/MIME** 签名：选择此帐户是否支持 S/MIME 签名。默认值为开。设置为开时，将显示以下两个字段。
  - 签署身份凭据：选择要使用的签名凭据。
  - **S/MIME** 签名用户可覆盖：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 签名。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - **S/MIME** 签名证书 **UUID** 用户可覆盖：如果设置为开，用户可以在其设备的设置中选择要使用的签名凭据。默认值为关。此选项适用于 iOS 12.0 及更高版本。
- 启用 **S/MIME** 加密：选择此帐户是否支持 S/MIME 加密。默认值为关。设置为开时，将显示以下两个字段。
  - 加密身份凭据：选择要使用的加密凭据。
  - 启用 **“**为消息单独设置 **S/MIME”** 开关：设置为开时，向用户显示一个选项，用于为其撰写的每条消息打开或关闭 S/MIME 加密。默认值为关。
  - 默认 **S/MIME** 加密用户可替代：如果设置为 **“**开**”**，用户可以在其设备的设置中选择 **S/MIME** 是否默认处于打开状态。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - **S/MIME** 加密证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 加密身份和加密。默认值为关。此选项适用于 iOS 12.0 及更高版本。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

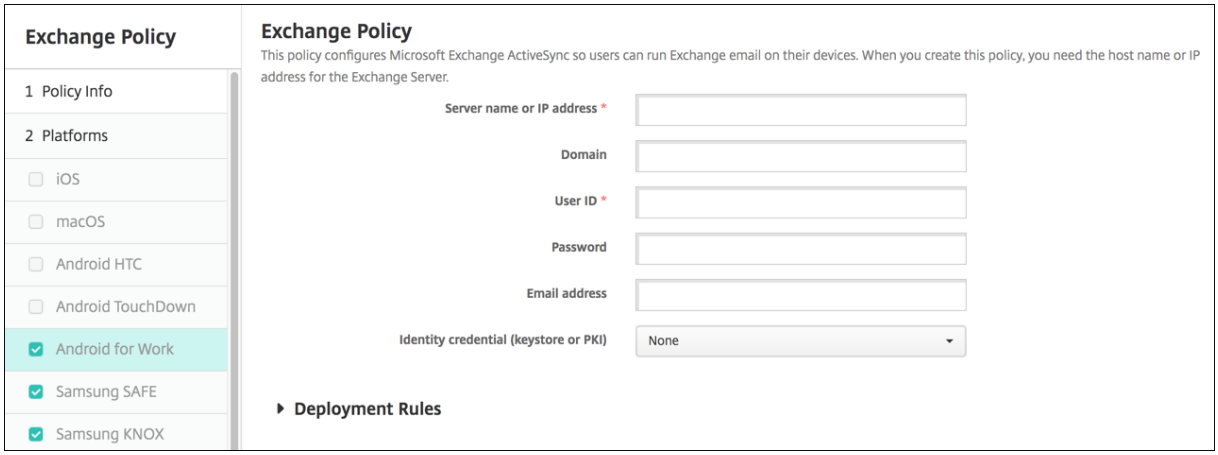
macOS 设置



- **Exchange ActiveSync** 帐户名称：键入显示在用户设备上的电子邮件帐户的说明。
- 用户：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 $user.username 自动查找用户名。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 $user.mail 自动查找用户的电子邮件帐户。
- 使用 **OAuth**：如果设置为开，连接将使用 OAuth 进行身份验证。默认值为关。此选项适用于 macOS 10.14 及更高版本。
- **OAuth** 登录 **URL**：指定在不使用自动发现服务时要加载到 Web 视图中以使用 OAuth 进行身份验证的 URL。使用 **OAuth** 设置为开时将显示此字段。
- 密码：输入 Exchange 用户帐户的可选密码。使用 **OAuth** 设置为于时不会显示此设置。
- 内部 **Exchange** 主机：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选内部 Exchange 主机名。
- 内部服务器端口：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选内部 Exchange Server 端口。
- 内部服务器路径：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选内部 Exchange Server 路径。
- 对内部 **Exchange** 主机使用 **SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。默认值为开。
- 外部 **Exchange** 主机：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选外部 Exchange 主机名。
- 外部服务器端口：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选外部 Exchange Server 端口号。

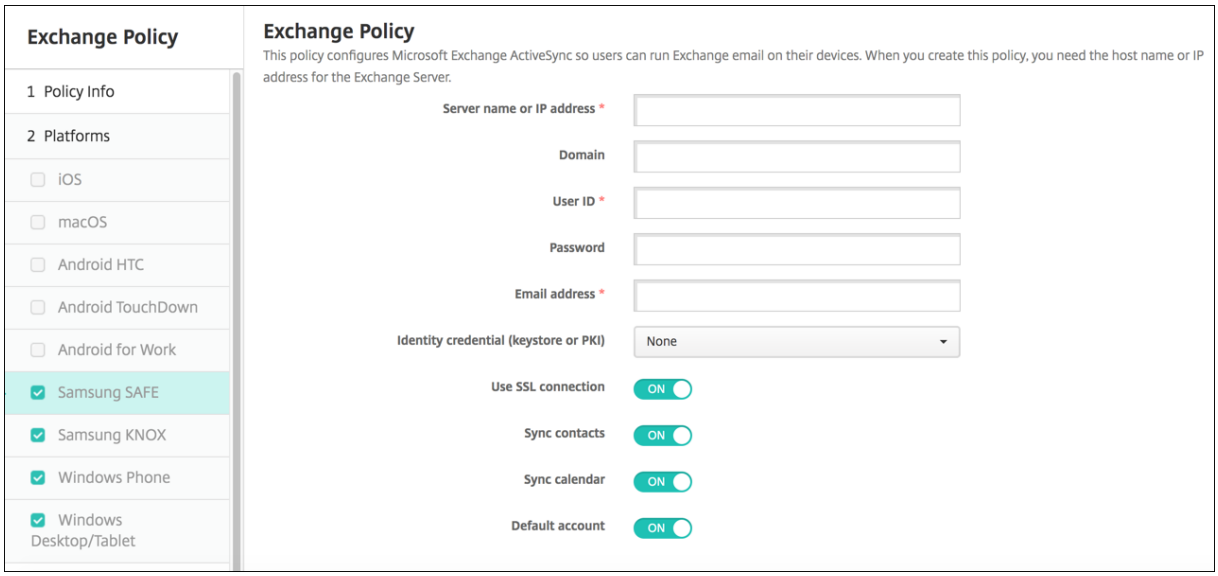
- 外部服务器路径：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选外部 Exchange Server 路径。
- 对外部 **Exchange** 主机使用 **SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。默认值为开。
- 允许投递邮件：选择是否允许用户在两个 Mac 之间以无线方式共享文件，且无需连接到现有网络。默认值为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Android Enterprise



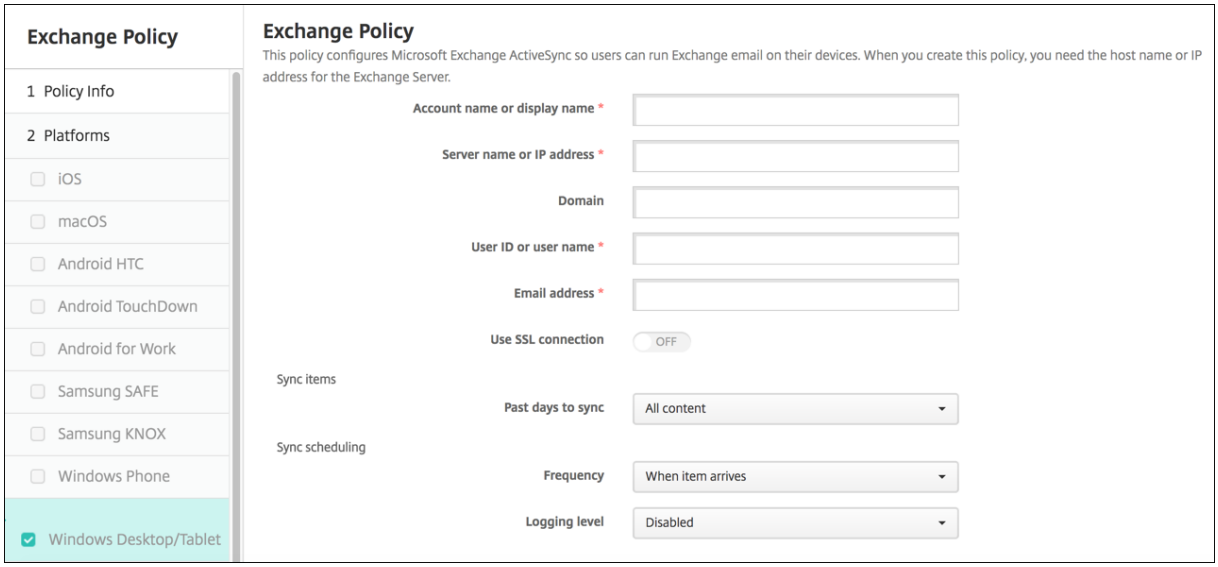
- 服务器名称或 **IP** 地址：键入 Exchange Server 的主机名或 IP 地址。
- 域：键入 Exchange Server 所在的域。可以在此字段中使用系统宏 $user.domainname 自动查找用户的域名。
- 用户 **ID**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 $user.username 自动查找用户名。
- 密码：键入 Exchange 用户帐户的可选密码。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 $user.mail 自动查找用户的电子邮件帐户。
- 身份凭据 **(**密钥库或 **PKI)**：如果为 XenMobile 配置了身份提供程序，则在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。默认设置为无。

Samsung SAFE 和 Samsung KNOX 设置



- 服务器名称或 **IP** 地址：键入 Exchange Server 的主机名或 IP 地址。
- 域：键入 Exchange Server 所在的域。可以在此字段中使用系统宏 $user.domainname 自动查找用户的域名。
- 用户 **ID**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 $user.username 自动查找用户名。
- 密码：键入 Exchange 用户帐户的可选密码。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 $user.mail 自动查找用户的电子邮件帐户。
- 身份凭据 **(**密钥库或 **PKI)**：如果为 XenMobile 配置了身份提供程序，则在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。
- 使用 **SSL** 连接：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为开。
- 同步联系人：选择是否在用户设备与 Exchange Server 之间启用用户联系人的同步。默认值为开。
- 同步日历：选择是否在用户设备与 Exchange Server 之间启用用户日历的同步。默认值为开。
- 默认帐户：选择是否将用户的 Exchange 帐户设置为默认帐户，用于从其设备发送电子邮件。默认值为开。

Windows Phone 和 Windows Desktop/Tablet 设置



> 注意：
>
> 此策略不允许您设置用户密码。用户在推送策略后必须从其设备设置该参数。

- 帐户名称或显示名称：键入 Exchange ActiveSync 帐户名称。
- 服务器名称或 **IP** 地址：键入 Exchange Server 的主机名或 IP 地址。
- 域：输入 Exchange Server 所在的域。可以在此字段中使用系统宏 $user.domainname 自动查找用户的域名。
- 用户 **ID** 或用户名：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 $user.username 自动查找用户名。
- 电子邮件地址：指定完整的电子邮件地址。可以在此字段中使用系统宏 $user.mail 自动查找用户的电子邮件帐户。
- 使用 **SSL** 连接：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为关。
- 要同步的过去天数：在列表中，单击要将设备上过去多少天内的所有内容与 Exchange Server 同步。默认值为所有内容。
- 频率：在列表中，单击同步从 Exchange Server 发送到设备的数据时要使用的计划。默认值为项目到达时。
- 日志记录级别：在列表中，单击已禁用、基本或高级以指定记录 Exchange 活动时的详细级别。默认值为已禁用。

文件设备策略

April 30, 2021

可以添加和部署文件，以便用户在其 Android 和 Android Enterprise 设备上访问。可以指定要在设备上存储文件的目录。例如，您希望用户收到公司文档或.pdf 文件。将文件部署到设备，让用户知道文件的位置。

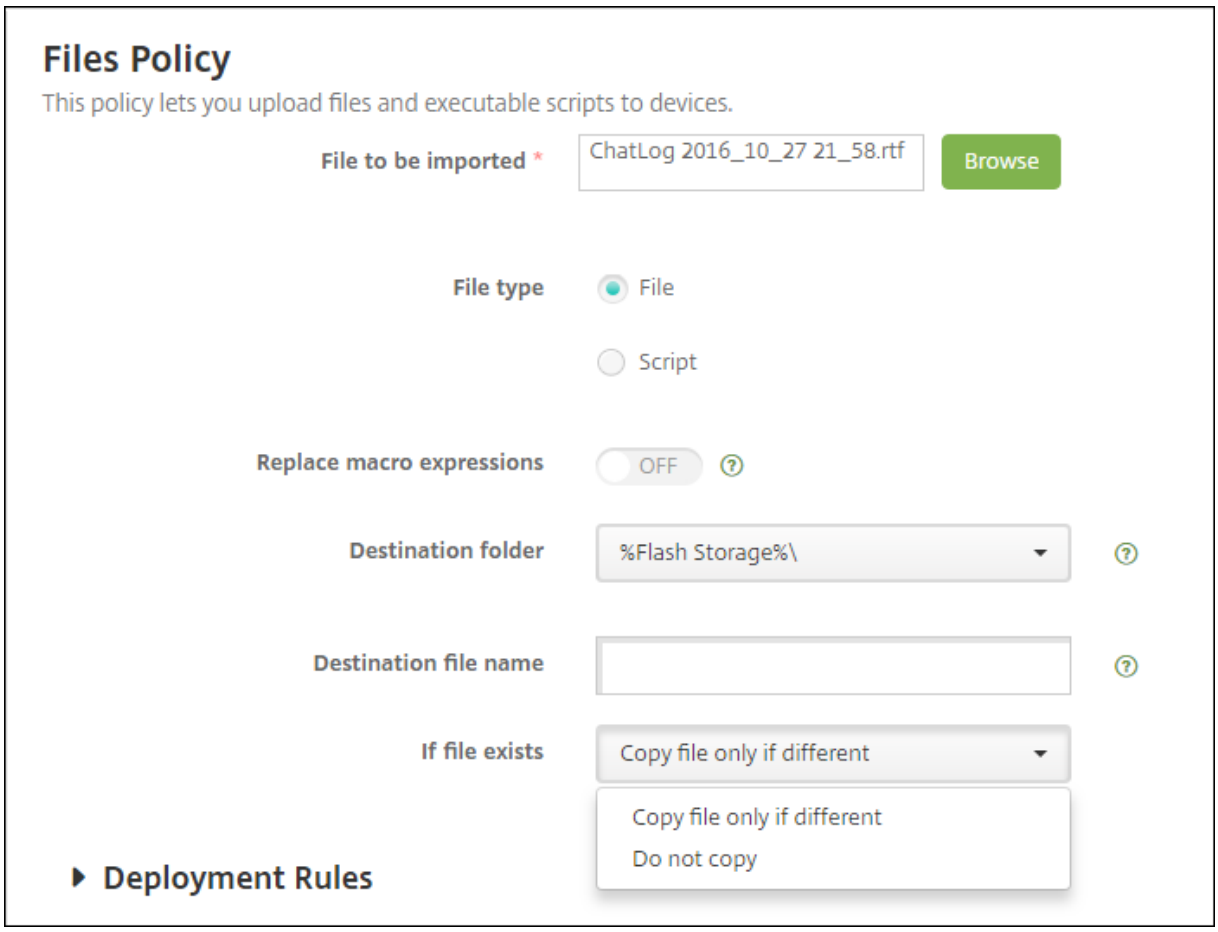
Android 设备不支持本机运行脚本。用户需要第三方软件来运行脚本。

利用此策略可以添加以下文件类型：

- 文本文件（.xml、.html、.py 等）
- 其他文件，如文档、图片、电子表格或演示文稿
- 仅适用于 Windows Mobile 和 Windows CE：通过 MortScript 创建的脚本文件

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。

Android Enterprise 设置



- 要导入的文件：要选择要导入的文件，请单击浏览并导航到文件所在的位置。
- 文件类型：选择文件或脚本。
- 立即执行：选择脚本后，将显示立即执行选项。启用此设置时没有反应。用户必须手动运行脚本。- 替换宏表达式：选择是否将脚本中的宏令牌名称替换为设备或用户属性。有关宏语法，请参阅“宏”。默认值为关。
- 目标文件夹：在列表中，选择存储已上载文件的位置，或单击新增选择未列出的文件位置。可以使用宏%XenMobile Folder%\ 或%Flash Storage%\ 作为任何路径标识符的开头。
- 目标文件名：可选。如果必须在部署到设备之前更改文件名，请键入文件名。
- 如果文件存在：在列表中，选择是否复制现有文件。默认值为仅在存在差异时复制文件。

Android 设置

- 要导入的文件：单击浏览并导航到要导入的文件所在位置，选择此文件。
- 文件类型：选择文件或脚本。
- 立即执行：选择脚本后，将显示立即执行选项。启用此设置时没有反应。用户必须手动运行脚本。- 替换宏表达式：选择是否将脚本中的宏令牌名称替换为设备或用户属性。默认值为关。
- 目标文件夹：在列表中，选择存储已上载文件的位置，或单击新增选择未列出的文件位置。此外，还可以使用宏%XenMobile Folder%\ 或%Flash Storage%\ 作为路径标识符的开头。
- 目标文件夹名：（可选）如果必须在部署到设备上之前更改文件名，请键入一个不同名称。
- 仅在不同时复制文件：在列表中，选择是否在与现有文件不同时复制文件。默认值为仅在文件存在差异时复制文件

Windows Mobile/CE 设置

- 要导入的文件：单击“浏览”并导航到要导入的文件所在位置，选择此文件。
- 文件类型：选择文件或脚本。
- 立即执行：选择脚本后，将显示立即执行。选择是否在上载文件后立即执行脚本。默认值为关。
- 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。默认值为关。
- 目标文件夹：在列表中，选择存储已上载文件的位置，或单击新增选择未列出的文件位置。此外，还可以使用以下宏作为路径标识符的开头：
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- 目标文件夹名：（可选）如果必须在部署到设备上之前更改文件名，请键入一个不同名称。
- 仅在不同时复制文件：在列表中，选择是否在与现有文件不同时复制文件。默认值为仅在文件存在差异时复制文件
- 只读文件：选择文件是否为只读文件。默认值为关。
- 隐藏文件：选择文件是否显示在文件列表中。默认值为关。

FileVault 设备策略

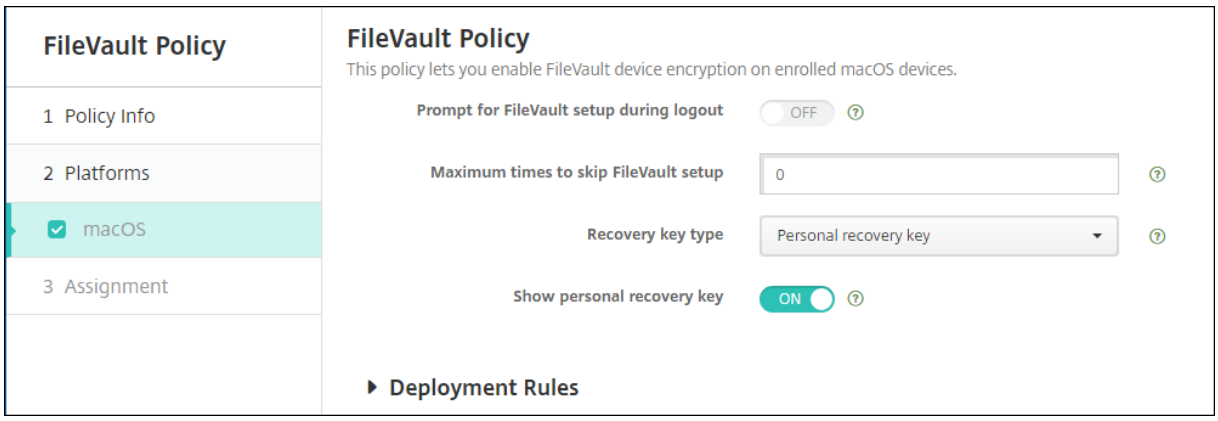
January 5, 2022

macOS FileVault 磁盘加密功能通过加密系统卷的内容来保护系统卷。如果在 macOS 设备上启用了 FileVault，每次设备启动时，用户都将使用其帐户密码进行登录。如果用户丢失了自己的密码，可以通过恢复密钥来解锁磁盘并重置密码。

XenMobile 设备策略 “FileVault” 将启用 FileVault 用户设置屏幕并配置恢复密钥等设置。有关 FileVault 的详细信息，请参阅 Apple 支持站点 https://support.apple.com 。

要添加 FileVault 策略，请转至配置 **>** 设备策略。

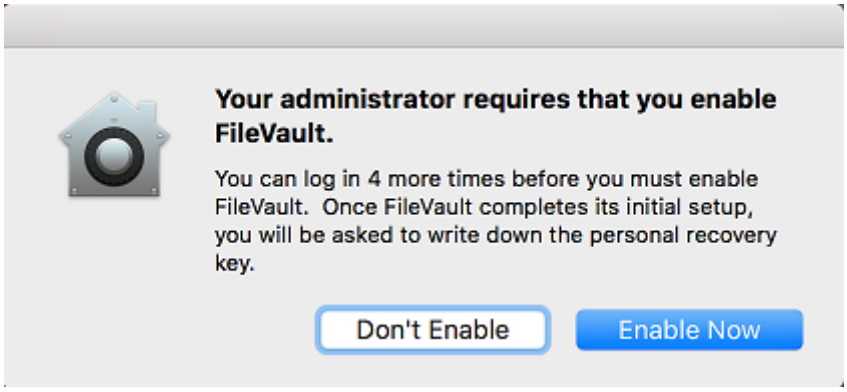
macOS 设置



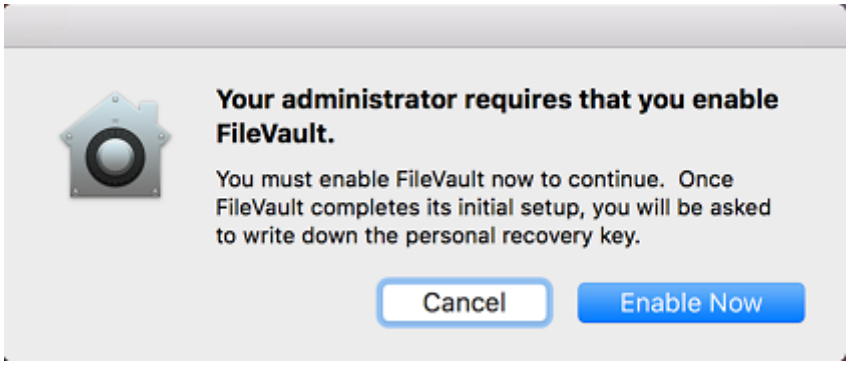
- 注销过程中提示设置 **FileVault**：如果设置为开，则将在接下来的 N 次注销过程中提示用户启用 FileVault，如选项跳过 **FileVault** 设置的最大次数指定。如果设置为关，将不显示 FileVault 密码提示。

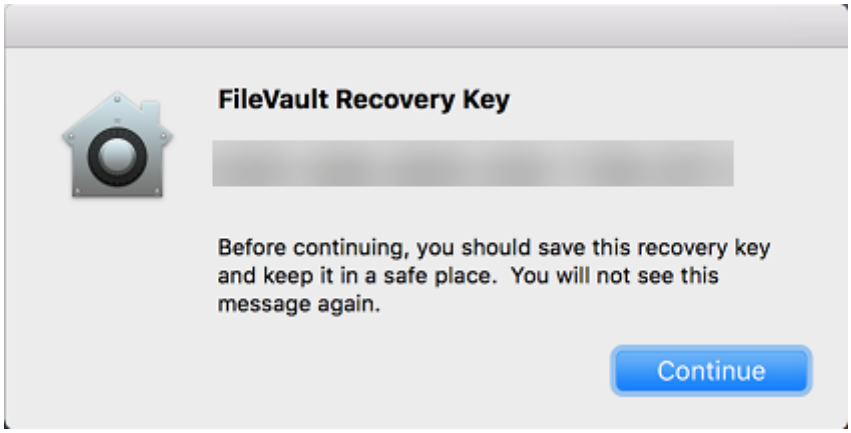
在启用了此设置的情况下部署 FileVault 策略后，用户注销设备时将显示以下屏幕。此屏幕向用户提供用于在注销前启用 FileVault 的选项。

如果跳过 **FileVault** 设置的最大次数值不为 0：在关闭了此设置的情况下部署 FileVault 策略并且用户登录后，将显示以下屏幕。



如果跳过 **FileVault** 设置的最大次数值为 0，或者用户已跳过设置最大次数，则将显示以下屏幕。





字体设备策略

April 14, 2020

可以在 XenMobile 中添加一个设备策略，用于向 iOS 和 macOS 设备添加其他字体。字体必须是 TrueType (.ttf) 字体或 OpenType (.oft) 字体。不支持字体集合（.ttc 或.otc）。

对于 iOS，此策略仅适用于 iOS 7.0 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

- 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：单击浏览并导航到要添加到用户设备的字体文件所在位置，选择此文件。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- 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：单击浏览并导航到要添加到用户设备的字体文件所在位置，选择此文件。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

主屏幕布局设备策略

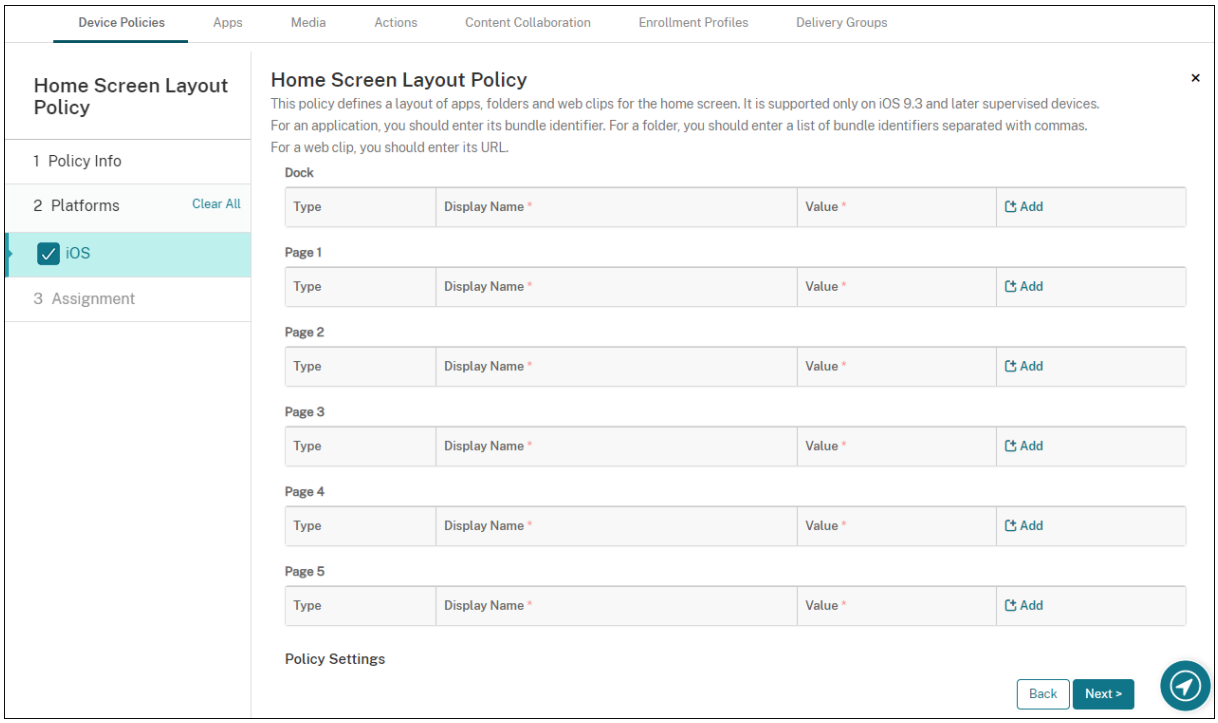
January 5, 2022

可以为 iOS 主屏幕指定应用程序和文件夹的布局。主屏幕布局设备策略适用于 iOS 9.3 及更高版本的受监督设备。

> 重要：
>
> 向设备部署多个主屏幕布局策略会导致在设备上产生 iOS 错误。无论是通过此 XenMobile 策略还是通过 Apple Configurator 定义主屏幕，都存在此限制。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

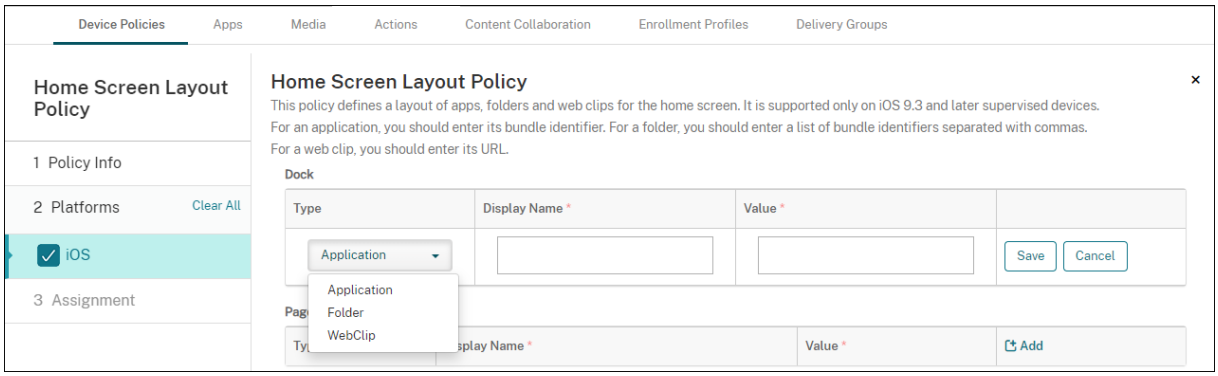
iOS 设置



- 对于要配置的每个屏幕区域（例如，基站或第 **1** 页），单击添加。
- 类型：选择应用程序、文件夹或 **Web** 剪辑。

  “限制”设备策略中的受限应用程序使用 **>** 仅允许部分应用程序设置可以阻止 Web 剪辑在主屏幕上正确显示。为了正确显示 Web 剪辑，请执行以下任一操作：

  - 将受限应用程序使用设置为允许所有应用或不允许某些应用程序。
  - 将受限应用程序使用设置为仅允许部分应用程序后，添加捆绑包 ID 为 `com.apple.webapp` 的应用程序以允许 Web 剪辑。



- 显示名称：应用程序或文件夹在主屏幕上显示的名称。
- 值：对于应用程序，请键入捆绑包标识符。对于文件夹，请键入捆绑包标识符列表（以逗号分隔）。对于 Web 剪辑，请键入捆绑包 ID `com.apple.webClip.managed` 并在 Web 剪辑策略中配置 Web 剪辑的 URL。如果同一个 URL 存在多个 Web 剪辑值，该行为在 iOS 11.3 及更高版本的设备上未定义。

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 (小时)
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅适用于 iOS 9.3 及更高版本。

导入 iOS 和 macOS 配置文件设备策略

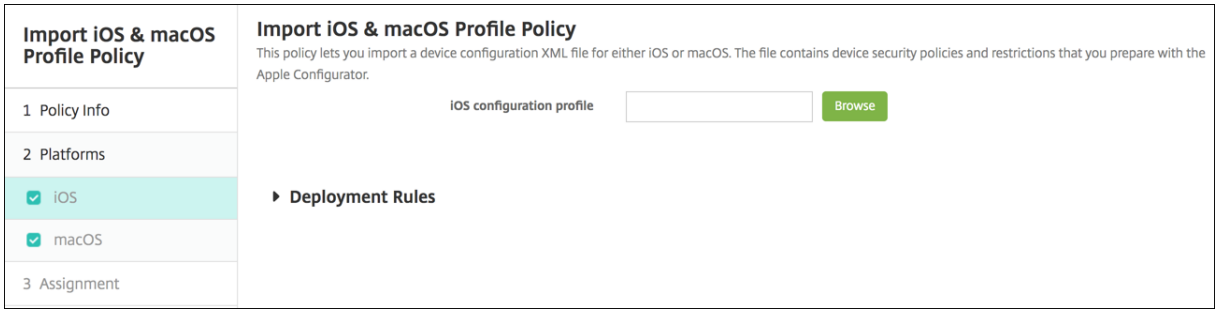
March 27, 2020

可以将 iOS 和 macOS 设备的设备配置 XML 文件导入到 XenMobile 中。此文件包含您使用 Apple Configurator 准备的设备安全策略和限制。

您可使用 Apple Configurator 将 iOS 设备置于受监督模式，如本文稍后所述。有关使用 Apple Configurator 创建配置文件的详细信息，请参阅 Apple Configurator 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 和 macOS 设置



- **iOS** 配置文件或 **macOS** 配置文件：要选择要导入的配置文件，请单击浏览并导航到此文件所在位置。

使用 Apple Configurator 将 iOS 设备置于受监督模式

要使用 Apple Configurator，需要一台运行 macOS 10.7.2 或更高版本的 Apple 计算机。

> 重要：
>
> 将设备置于受监督模式时，系统将会在设备上安装所选版本的 iOS，同时完全擦除设备上以前存储的任何用户数据或应用程序。

1. 从 iTunes 安装 Apple Configurator。
2. 将 iOS 设备连接到 Apple 电脑。

3. 启动 Apple Configurator。Configurator 显示您有一台设备需要进行监督前的准备工作。
4. 设备监督前准备工作：
    a) 将 **Supervision**（监督）控件值切换到 **On**（开）。如果您打算通过定期重新应用配置来随时维护对设备的控制，Citrix 建议您选择此设置。
    b) 提供设备的名称（可选）。
    c) 在 iOS 中，单击 **Latest**（最新），获取您要安装的最新版本的 iOS。
5. 当您准备进行设备监督前的准备工作时，请单击 **Prepare**（准备）。

键盘锁管理设备策略

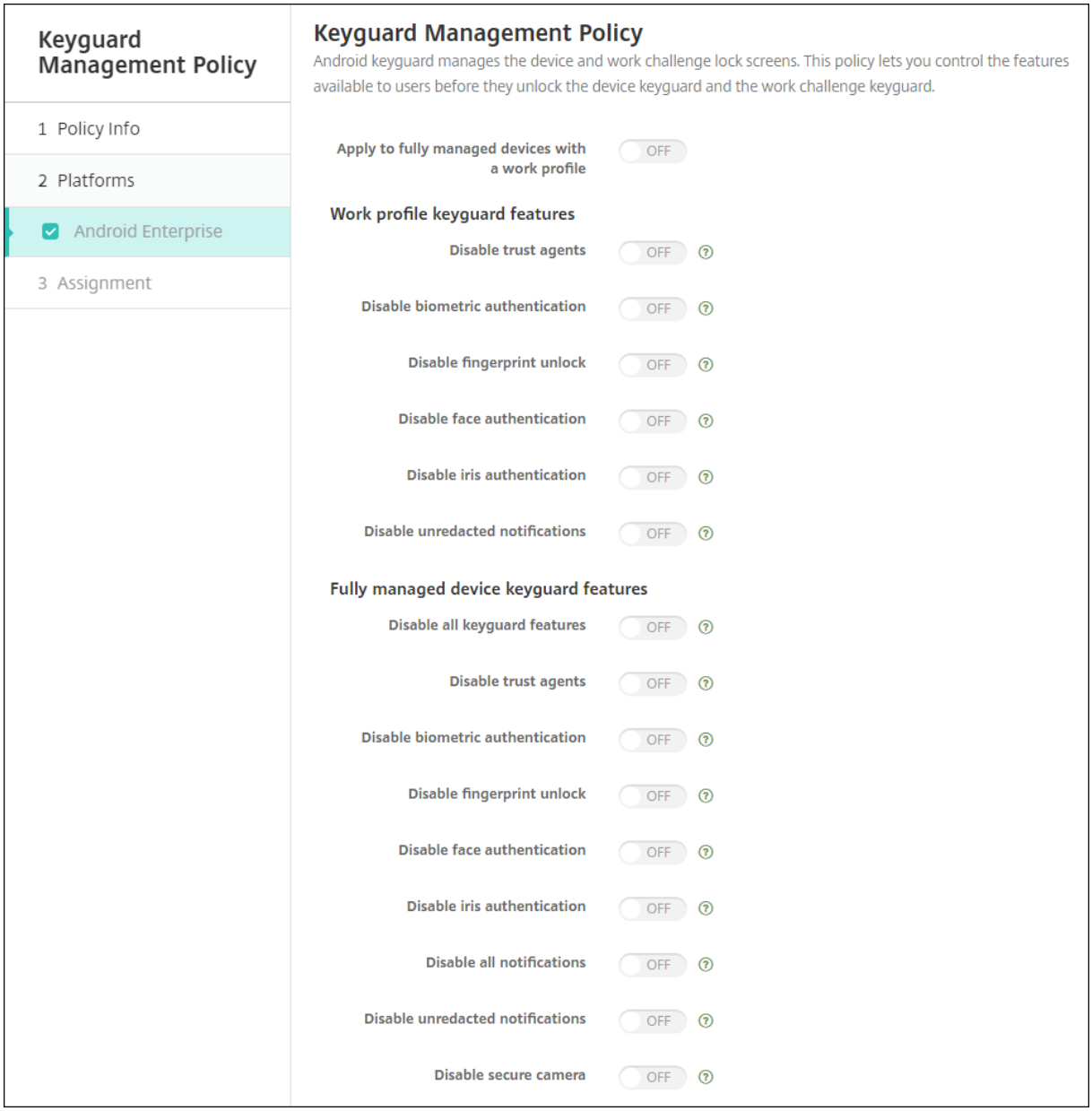
January 5, 2022

Android 键盘锁管理设备和工作挑战锁定界面。此策略允许您管理 Android Enterprise 工作配置文件键盘锁和高级设备键盘锁的功能。您可以控制：

- 工作配置文件设备上的键盘锁管理。可以在用户解锁设备键盘锁和工作质询键盘锁之前指定其可用的功能。例如，默认情况下，用户可以使用指纹解锁并在锁定屏幕上查看未编辑的通知。
- 在完全托管设备和专用设备上进行键盘锁管理。可以指定可用的功能，例如信任代理和安全摄像头，然后才能解锁键盘锁屏幕。或者，可以选择禁用所有键盘锁功能。
- 具有工作配置文件的完全托管设备上的键盘锁管理。可以使用一个键盘锁管理策略将单独的设置应用到设备和工作配置文件。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Android Enterprise 设置



- 应用到使用工作配置文件的完全托管设备：允许您为具有工作配置文件的完全托管设备配置键盘锁管理设备策略。

  当此设置设为开时，您可以将单独的设置应用到设备或具有工作配置文件的完全托管设备上的工作配置文件。

  当此设置设为关时，您可以将设置应用到工作配置文件设备或完全托管设备。为工作配置文件配置的设置仅适用于工作配置文件设备。为完全托管设备配置的设置仅适用于完全托管设备。

  默认值为关。

- 工作配置文件键盘锁功能：控制在用户解锁工作配置文件键盘锁（锁屏界面）之前以下功能是否可用。

  - 禁用信任代理：如果设置为关，则在工作配置文件中设置了质询时，信任代理可以在安全的键盘锁屏幕上运行。设置为开将在工作配置文件中禁用所有信任代理。默认值为关。

- 禁用生物特征身份验证：如果设置为关，则在工作配置文件中设置了质询时，可以在安全的键盘锁屏幕上使用生物特征识别身份验证。设置为开将在工作配置文件中禁用生物特征识别身份验证。此设置将禁用指纹解锁、人脸身份验证和虹膜身份验证。默认值为关。适用于 Android 9.0 及更高版本。
- 禁用指纹解锁：如果设置为开，则在工作配置文件中设置了质询时，不能在安全的键盘锁屏幕上使用指纹解锁。设置为关将在工作配置文件中启用指纹解锁。默认值为关。
- 禁用人脸身份验证：如果设置为关，则在工作配置文件中设置了质询时，可以在安全的键盘锁屏幕上使用人脸身份验证。设置为开将在工作配置文件中禁用人脸身份验证。默认值为关。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，则在工作配置文件中设置了质询时，可以在安全的键盘锁屏幕上使用虹膜身份验证。设置为开将在工作配置文件中禁用虹膜身份验证。默认值为关。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，已遍及的通知和未编辑的通知将显示在安全的键盘锁屏幕上。设置为开将禁用未编辑的通知并仅显示已编辑的通知。默认值为关。

- 完全托管设备键盘锁功能：控制在用户解锁设备键盘锁（锁屏界面）之前以下功能是否可用。这些功能适用于完全托管设备或专用设备。
  - 禁用所有键盘锁功能：如果设置为关，则可以在安全的键盘锁屏幕上使用所有当前和将来的键盘锁自定义设置。设置为开将禁用所有键盘锁自定义设置。默认值为关。
  - 禁用信任代理：如果设置为关，信任代理可以在安全的键盘锁屏幕上运行。设置为开将禁用信任代理。默认值为关。
  - 禁用生物特征身份验证：如果设置为关，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用生物特征识别身份验证。设置为开将在设备上禁用生物特征识别身份验证。此设置将禁用指纹解锁、人脸身份验证和虹膜身份验证。默认值为关。适用于 Android 9.0 及更高版本。
  - 禁用指纹解锁：如果设置为关，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用指纹解锁。设置为开将在设备上禁用指纹解锁。默认值为关。
  - 禁用人脸身份验证：如果设置为关，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用人脸身份验证。设置为开将在设备上禁用人脸身份验证。默认值为关。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，则在设备上设置了质询时，可以在安全的键盘锁屏幕上使用虹膜身份验证。设置为开将在设备上禁用虹膜身份验证。默认值为关。适用于 Android 9.0 及更高版本。
  - 禁用所有通知：如果设置为关，所有通知都将显示在安全的键盘锁屏幕上。设置为开将显示所有通知。默认值为关。
  - 禁用未编辑的通知：如果设置为关，已遍及的通知和未编辑的通知将显示在安全的键盘锁屏幕上。设置为开将禁用未编辑的通知并仅显示已编辑的通知。默认值为关。
  - 禁用安全摄像头：如果设置为关，可以在安全的键盘锁屏幕上使用安全摄像头。设置为开将禁用安全摄像头。默认值为关。

展台设备策略

January 5, 2022

展台策略允许您通过限制可运行的应用程序，将设备限制为展台策略。XenMobile 不控制设备的哪部分锁定在展台模式。部署策略后，该设备将管理展台模式设置。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

将 **Samsung SAFE** 设备置于 **Kiosk** 模式

1. 在移动设备上启用 Samsung SAFE API 密钥，如 Samsung MDM 许可证密钥设备策略中所述。此步骤允许您在 Samsung SAFE 设备上启用策略。
2. 为 Android 设备启用 Firebase Cloud Messaging，如 Firebase Cloud Messaging 中所述。此步骤允许 Android 设备连接回 XenMobile。
3. 添加 Kiosk 设备策略，如下一节所述。
4. 将这三个设备策略分配给恰当的交付组。考虑是否要在这些交付组中包括其他策略，例如“应用程序清单”。

   要从 Kiosk 模式中删除设备，请创建一个 **Kiosk** 模式设置为禁用的新 Kiosk 设备策略。更新交付组以删除启用了 Kiosk 模式的 Kiosk 策略以及添加禁用了 Kiosk 模式的 Kiosk 策略。

添加 **Kiosk** 设备策略

为 Kiosk 模式指定的所有应用程序必须已安装在用户设备上。

某些选项仅适用于 Samsung Mobile Device Management API (MDM) 4.0 及更高版本。

Samsung SAFE 设置

可以指定只能使用一个或多个特定的应用程序。此策略对旨在仅运行特定类型或类别的应用程序的企业设备非常有用。此策略还允许您为设备选择处于 Kiosk 模式时设备主屏幕和锁屏界面墙纸使用的自定义图片。

- **Kiosk** 模式：单击启用或禁用。默认值为启用。单击禁用时，以下所有选项都将消失。
- **Launcher** 软件包：除非您开发了内部启动程序以使用户能够打开一个或多个 Kiosk 应用程序，否则，Citrix 建议您将此字段留空。如果使用内部启动程序，请输入启动程序应用程序软件包的完整名称。
- 紧急电话号码：输入可选电话号码。任何人都可以使用此号码与贵公司联系，以查找丢失的设备。仅适用于 MDM 4.0 及更高版本。
- 允许使用导航栏：选择是否允许用户在处于 Kiosk 模式时看到和使用导航栏。仅适用于 MDM 4.0 及更高版本。默认值为开。
- 允许多窗口模式：选择是否允许用户在处于 Kiosk 模式时使用多个窗口。仅适用于 MDM 4.0 及更高版本。默认值为开。

- 允许使用状态栏：选择是否允许用户在处于 Kiosk 模式时看到状态栏。仅适用于 MDM 4.0 及更高版本。默认值为开。
- 允许使用系统栏：选择是否允许用户在处于 Kiosk 模式时看到系统栏。默认值为开。
- 允许使用任务管理器：选择是否允许用户在处于 Kiosk 模式时看到和使用任务管理器。默认值为开。
- 更改通用 **SAFE** 通行码：此设置有助于防止无意中更改“通用 SAFE 通行码”字段。此设置设为关时，您将无法更改“通用 SAFE 通行码”字段。默认值为关。
- 通用 **SAFE** 通行码：如果您为所有 Samsung SAFE 设备设置了一个通用通行码策略，请在此字段中输入该可选通行码。
- 墙纸
  - 定义主页墙纸：选择是否在处于 Kiosk 模式时对主屏幕使用自定义图片。默认值为关。
    - 主页图片：启用定义主页墙纸时，单击浏览并导航到图片文件所在位置，选择此文件。
  - 定义锁定墙纸：选择是否在处于 Kiosk 模式时对锁屏界面使用自定义图片。默认值为关。仅适用于 MDM 4.0 及更高版本。
    - 锁屏图片：启用定义锁屏墙纸时，单击浏览并导航到图片文件所在位置，选择此文件。
- 应用程序：对于要添加到 Kiosk 模式的每个应用程序，单击添加，然后执行以下操作：
  - 要添加的新应用程序：输入要添加的应用程序的完整名称。例如，com.android.calendar 允许用户使用 Android 日历应用程序。
  - 单击保存以添加应用程序，或单击取消以取消添加应用程序。

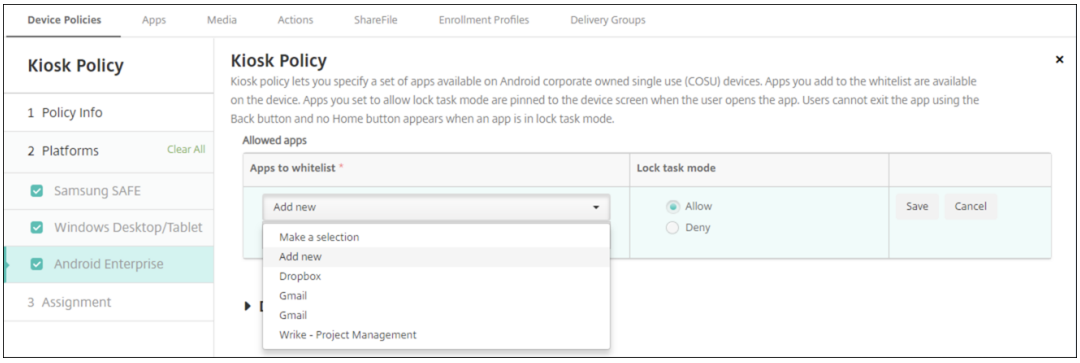
Android Enterprise 设置

对于专用 Android Enterprise 设备（又称为企业拥有，单一用途 (COSU) 设备），可以允许运行应用程序并设置锁定任务模式。默认情况下，Secure Hub 和 Google Play 服务都在允许列表中。

要允许运行应用程序，请单击添加。可以允许运行多个应用程序。有关详细信息，请参阅 Android Enterprise。

> 注意：
>
> XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

- 要加入白名单的应用程序：输入要加入白名单的应用程序的软件包名称，或者从列表中选择应用程序。
  - 单击新增以输入已批准显示在列表中的应用程序的软件包名称。
  - 从列表中选择现有应用程序。该列表显示了在 XenMobile Server 中上载的应用程序。默认情况下，Secure Hub 和 Google Play 服务都列入白名单。



- 锁定任务模式：选择允许可设置要在用户启动应用程序时固定到设备屏幕的应用程序。选择拒绝可设置不固定的应用程序。默认情况下，允许运行 Secure Hub 和 Google Play 服务。默认设置为允许。

当某个应用程序处于锁定任务模式时，用户打开时该应用程序将固定到设备屏幕。此时将不显示任何主页按钮，并且返回按钮处于禁用状态。用户使用编程到该应用程序中的一项操作退出该应用程序，例如注销。

Launcher 配置设备策略

October 13, 2021

使用 Citrix Launcher 可以自定义由 XenMobile 部署的 Android 设备的用户体验。Citrix Launcher 和 Launcher 配置设备策略与 Android Enterprise 不兼容。

您可以添加 Launcher 配置策略来控制以下 Citrix Launcher 功能：

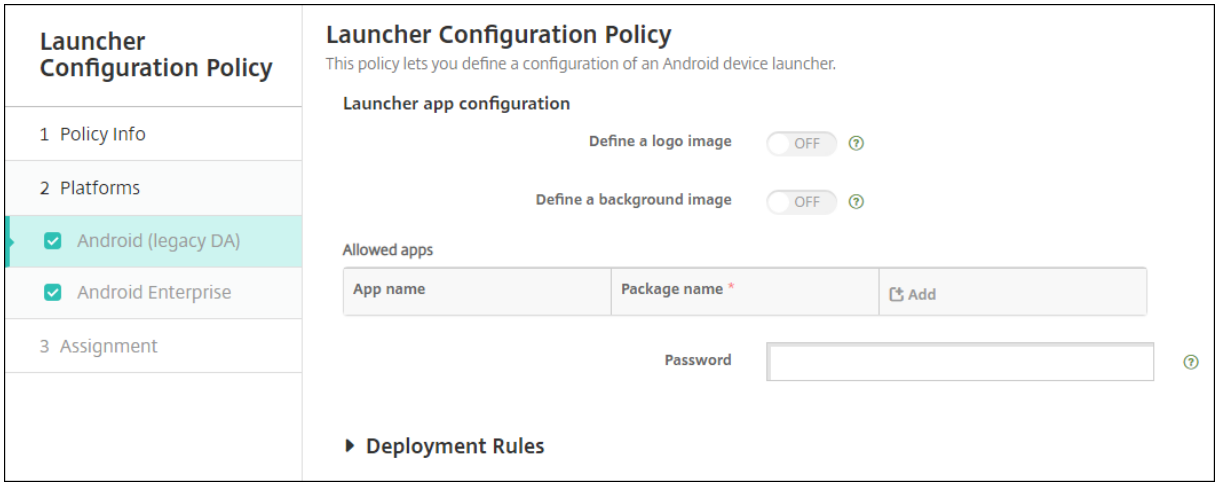
- 管理 Android 设备，确保用户只能访问指定的应用程序。
- （可选）为 Citrix Launcher 图标指定自定义徽标图片以及为 Citrix Launcher 指定自定义背景图片。
- 指定用户在退出启动程序前必须输入的密码。

尽管使用 Citrix Launcher 可以应用这些设备级别限制，但 Citrix Launcher 也为用户提供了所需的操作灵活性，允许他们通过内置访问途径配置设备设置，例如 WiFi 设置、蓝牙设置和设备通行码设置。Citrix Launcher 并不是设备平台在已提供的安全层之外额外提供的一个安全层。

部署 Citrix Launcher 后，XenMobile 会安装它，取代默认 Android 启动程序。

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。

Android（旧 **DA**）和 **Android Enterprise** 设置



- 定义徽标图片：选择是否对 Citrix Launcher 图标使用自定义徽标图片。默认值为关。
- 徽标图片：启用定义徽标图片时，单击浏览并导航到图片文件所在位置，选择此文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- 定义背景图片：选择是否对 Citrix Launcher 背景使用自定义图片。默认值为关。
- 背景图片：启用定义背景图片时，单击浏览并导航到图片文件所在位置，选择此文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- 允许的应用程序：对于要在 Citrix Launcher 中允许使用的每个应用程序，单击添加，然后执行以下操作：
  - 要添加的新应用程序：输入要添加的应用程序的完整名称。例如，com.android.calendar 表示 Android 日历应用程序。
  - 单击保存以添加应用程序，或单击取消以取消添加应用程序。
- 密码：用户退出 Citrix Launcher 时必须输入的密码。

LDAP 设备策略

April 14, 2020

可以在 XenMobile 中为 iOS 设备创建 LDAP 策略，用于提供与要使用的 LDAP 服务器有关的信息，包括任何必要的帐户信息。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。

配置此策略之前，您需要提供 LDAP 主机名。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 帐户说明：输入可选帐户说明。
- 帐户用户名：输入可选用户名。

- 帐户密码：输入可选密码。此字段仅适用于加密的配置文件。
- **LDAP** 主机名：输入 LDAP 服务器的主机名。此字段为必填字段。
- 使用 **SSL**：选择是否使用安全套接字层连接到 LDAP 服务器。默认值为开。
- 搜索设置：添加查询 LDAP 服务器时要使用的搜索设置。可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。单击添加，然后执行以下操作：
  - 说明：输入搜索设置的说明。此字段为必填字段。
  - 范围：选择基础、一级或子树以定义搜索 LDAP 树的深度。默认值为基础。
    - 基础搜索“搜索基础”指向的节点。
    - 一级搜索基础节点及其下一级节点。
    - 子树搜索基础节点及其所有子节点，而无论深度为何。
  - 搜索基础：输入开始搜索时所在节点的路径。例如 ou=people 或 0=example corp。此字段为必填字段。
  - 单击保存添加搜索设置，或单击取消以取消添加搜索设置。
  - 为要添加的每个搜索设置重复执行这些步骤。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- 帐户说明：输入可选帐户说明。
- 帐户用户名：输入可选用户名。
- 帐户密码：输入可选密码。此字段仅适用于加密的配置文件。
- **LDAP** 主机名：输入 LDAP 服务器的主机名。此字段为必填字段。
- 使用 **SSL**：选择是否使用安全套接字层连接到 LDAP 服务器。默认值为开。
- 搜索设置：添加查询 LDAP 服务器时要使用的搜索设置。可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。单击添加，然后执行以下操作：
  - 说明：输入搜索设置的说明。此字段为必填字段。
  - 范围：选择基础、一级或子树以定义搜索 LDAP 树的深度。默认值为基础。
    - 基础搜索“搜索基础”指向的节点。
    - 一级搜索基础节点及其下一级节点。
    - 子树搜索基础节点及其所有子节点，而无论深度为何。
  - 搜索基础：输入开始搜索时所在节点的路径。例如 ou=people 或 0=example corp。此字段为必填字段。
  - 单击保存添加搜索设置，或单击取消以取消添加搜索设置。
  - 为要添加的每个搜索设置重复执行这些步骤。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。

如果选择需要通行码，请在删除通行码字段中键入通行码。

– 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

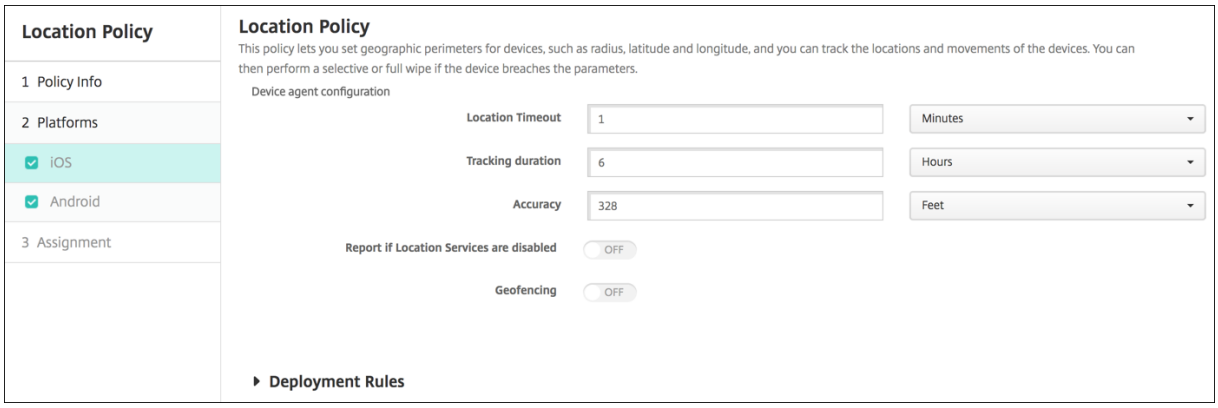
位置设备策略

January 5, 2022

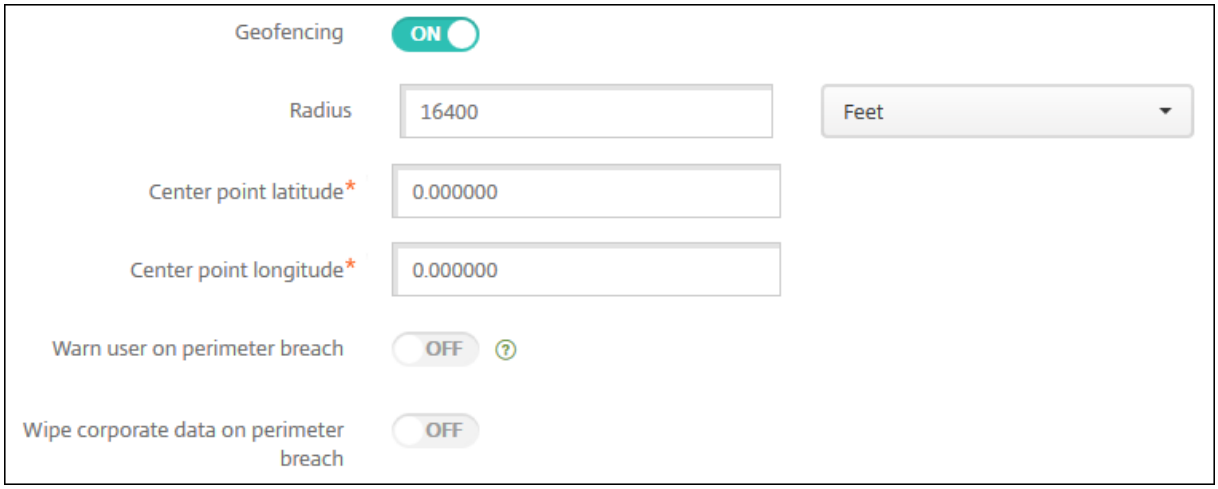
可以在 XenMobile 中创建定位设备策略以强制实施地理边界。用户超出定义的边界（也称为地理围栏）时，XenMobile 可以执行某些操作。例如，您可以配置策略以在用户超出定义的外围时向用户发出警告消息。您还可以配置策略以在用户超出外围时立即或延迟一段时间后擦除用户的公司数据。有关安全操作的信息（例如，启用跟踪和定位设备），请参阅安全操作。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



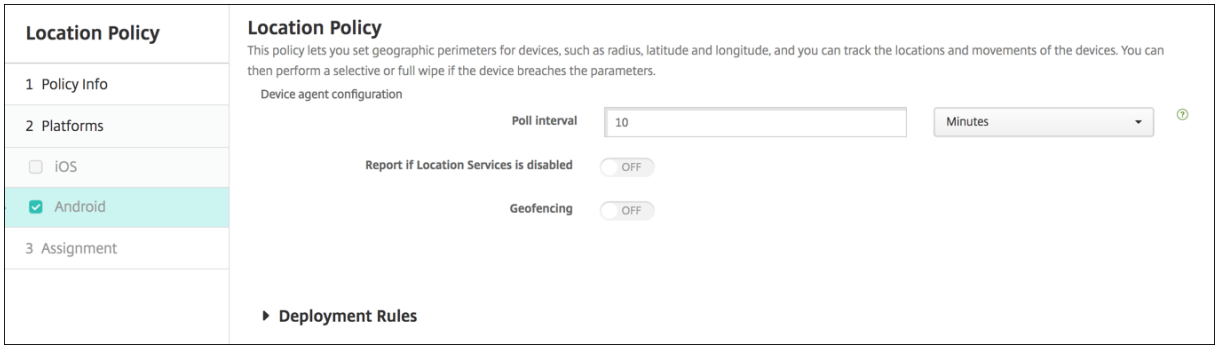
- 定位超时：键入数值，然后在列表中单击秒或分钟以设置 XenMobile 尝试修复设备位置的频率。有效值为 60-900 秒或 1-15 分钟。默认值为 1 分钟。
- 跟踪持续时间：键入数值，然后在列表中单击小时或分钟以设置 XenMobile 跟踪设备的时间长度。有效值为 1-6 小时或 10-360 分钟。默认值为 6 小时。
- 准确度：键入数值，然后在列表中单击米、英尺或码以设置 XenMobile 跟踪设备的接近程度。有效值为 10–5000 码或米，或者 30–15000 英尺。默认值为 328 英尺。
- 禁用定位服务时报告：选择禁用 GPS 时设备是否向 XenMobile 发送报告。默认值为关。
- 地理围栏



启用地理围栏后，请配置以下设置：

- 半径：键入数值，然后在列表中单击要用于度量半径的单位。默认值为 16,400 英尺。半径的有效值如下：
  - 164–164000 英尺
  - 50-50000 米
  - 54-54680 码
  - 1-31 英里
- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- 超出边界时警告用户：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 XenMobile 即可显示警告消息。
- 超出边界时擦除公司数据：选择当用户超出边界时是否擦除用户设备。默认值为关。启用此选项时，将显示本地擦除延迟字段。
  - 键入数值，然后在列表中单击秒或分钟以设置擦除用户设备中的公司数据之前延迟的时长。此设置使用户有机会在 XenMobile 选择性擦除其设备之前返回到允许的位置。默认值为 0 秒。

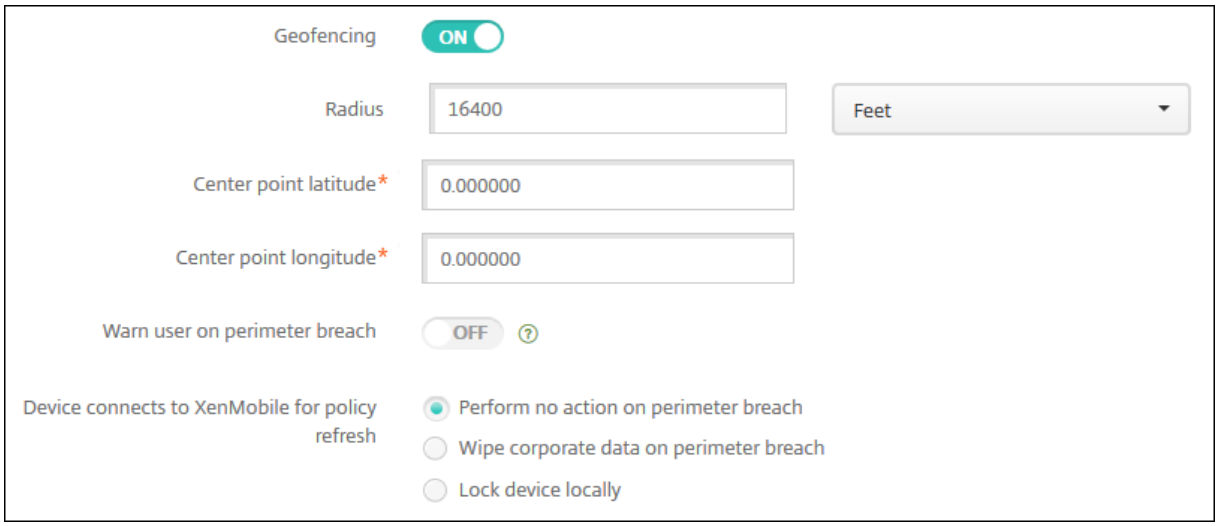
Android 设置



- 轮询间隔：键入数值，然后在列表中单击分钟、小时或天以设置 XenMobile 尝试修复设备位置的频率。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寿

命产生不利影响。

- 禁用定位服务时报告：选择禁用 GPS 时设备是否向 XenMobile 发送报告。默认值为关。
- 地理围栏



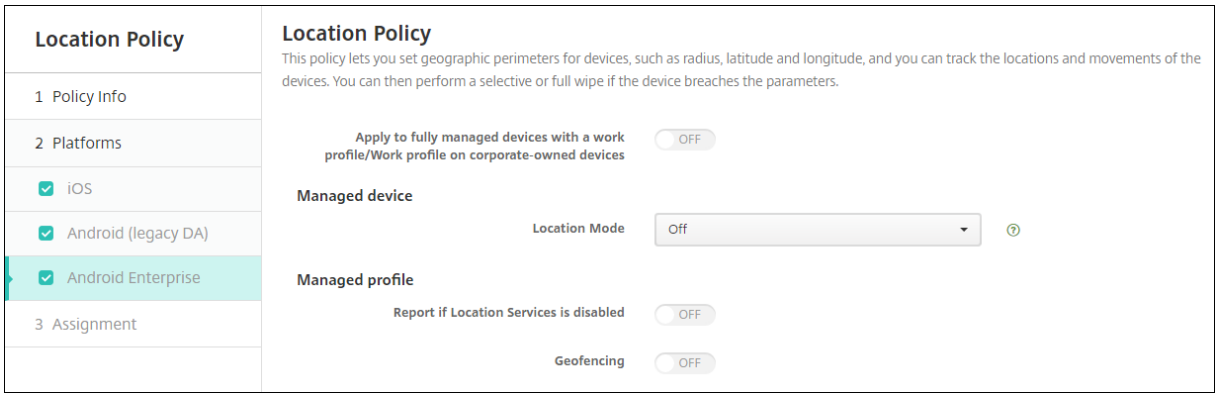
启用地理围栏后，请配置以下设置：

- 半径：键入数值，然后在列表中单击要用于度量半径的单位。默认值为 16,400 英尺。半径的有效值如下：
  - 164–164000 英尺
  - 1-50 千米
  - 50-50000 米
  - 54-54680 码
  - 1-31 英里
- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- 超出边界时警告用户：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 XenMobile 即可显示警告消息。
- 设备连接到 **XenMobile** 以刷新策略：针对用户超出边界时选择以下选项之一：
  - 超出边界时不执行任何操作：不执行任何操作。这是默认设置。
  - 超出边界时擦除公司数据：在指定的时间长度后擦除公司数据。启用此选项时，将显示本地擦除延迟字段。
    - 键入数值，然后在列表中单击“秒”或“分钟”以设置擦除用户设备中的公司数据之前延迟的时间长度。此设置使用户有机会在 XenMobile 选择性擦除其设备之前返回到允许的位置。默认值为 0 秒。
  - 锁定延迟：在指定的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。
    - 键入数值，然后在列表中单击“秒”或“分钟”以设置锁定用户设备之前延迟的时间长度。此设置使用户有机会在 XenMobile 锁定其设备之前返回到允许的位置。默认值为 0 秒。

Android Enterprise 设置

要使 Android 位置跟踪起作用，请确保满足以下要求：

- Android 8.5 或更高版本
- 在 Android Enterprise 的“限制设备”策略中启用了“允许位置共享”设置
- 连接计划（推荐使用 Firebase Cloud Messaging）



应用到使用工作配置文件的完全托管设备

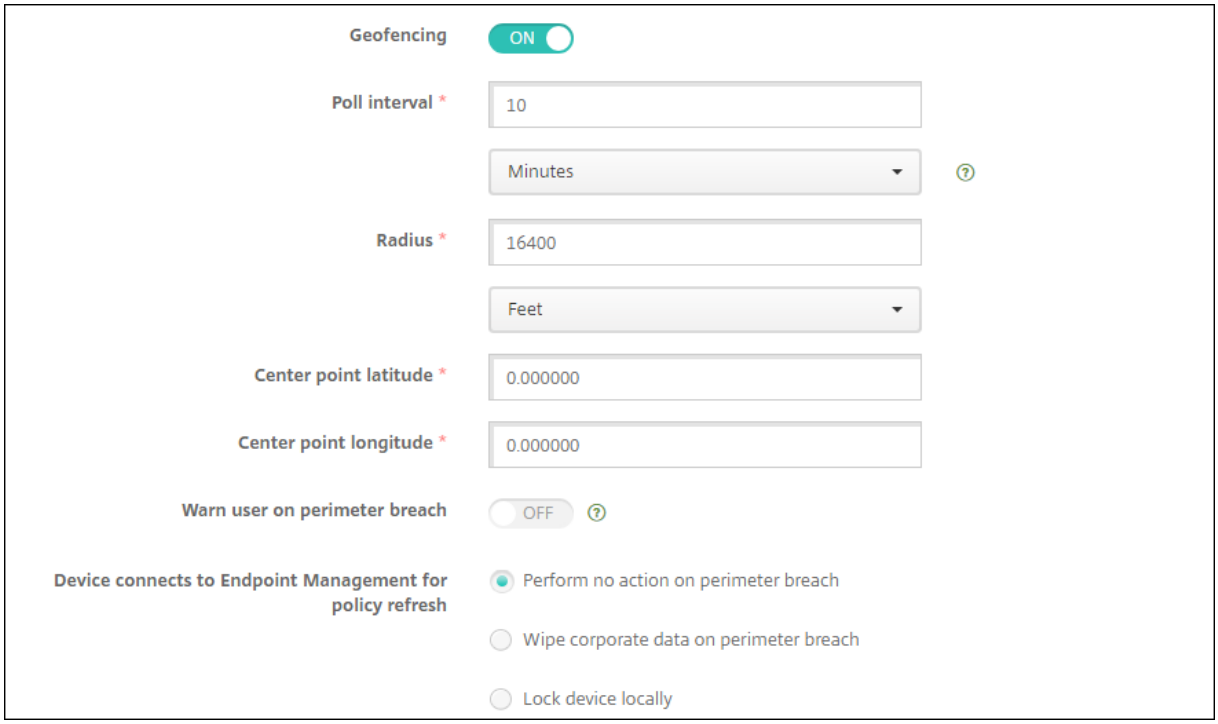
对于具有工作配置文件的完全托管设备，只有位置模式设置可用。

- 应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备：允许您为具有工作配置文件的完全托管设备配置位置模式。启用此设置后，请为工作配置文件配置位置模式设置：
  - 禁用定位服务时报告：选择当用户关闭 GPS 时设备是否向 XenMobile Server 发送报告。默认值为关。
  - 地理围栏：请参阅本文中托管设备下的设置。

当应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备设置为“关”时，设置将应用到托管设备和工作配置文件，如以下部分中所示。默认值为关。

托管设备

- 位置模式：指定要启用的位置检测程度。仅当位置模式设置为高精度或电池节能时，可以使用“定位”安全操作。默认值为高精度。
  - 高精度：启用所有位置检测方法，包括 GPS、网络和其他传感器。
  - 仅限传感器：仅启用 GPS 和其他传感器。
  - 电池节能：仅启用网络位置提供程序。
  - 关：禁用位置检测。
- 地理围栏：



启用地理围栏后，请配置以下设置：

- 轮询间隔：键入数值，然后单击分钟、小时或天以设置 XenMobile Server 尝试修复设备位置的频率。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寿命产生不利影响。
- 半径：键入数值，然后单击要用于度量半径的单位。默认值为 **16400** 英尺（**5000** 米）。半径的有效值如下：
  - 164–164000 英尺
  - 1-50 千米
  - 50-50000 米
  - 54-54680 码
  - 1-31 英里
- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。要查找值，请转至管理 **>** 设备，选择设备，单击安全，然后单击定位。定位设备后，XenMobile Server 会在安全性下的设备详细信息 **>** 常规页面中报告设备位置。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- 超出边界时警告用户：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 XenMobile Server 即可显示警告消息。
- 设备连接到 **XenMobile Server** 以刷新策略：针对用户超出边界时选择以下选项之一：
  - 超出边界时不执行任何操作：不执行任何操作。这是默认设置。
  - 超出边界时擦除公司数据：在指定的时间长度后擦除公司数据。启用此选项时，将显示本地擦除延迟字段。

    * 键入数值，然后单击秒或分钟以设置擦除用户设备中的公司数据之前延迟的时间长度。此延迟使用户有机会在 XenMobile Server 选择性擦除其设备之前返回到允许的位置。默认值为 **0** 秒。
  - 本地锁定设备：在指定的时间长度后锁定用户的设备。启用此选项时，将显示锁定延迟字段。
    * 键入数值，然后单击秒或分钟以设置锁定用户设备之前延迟的时间长度。此延迟使用户有机会在 XenMobile Server 锁定其设备之前返回到允许的位置。默认值为 **0** 秒。

托管配置文件

- 禁用定位服务时报告：选择当用户关闭 GPS 时设备是否向 XenMobile Server 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。

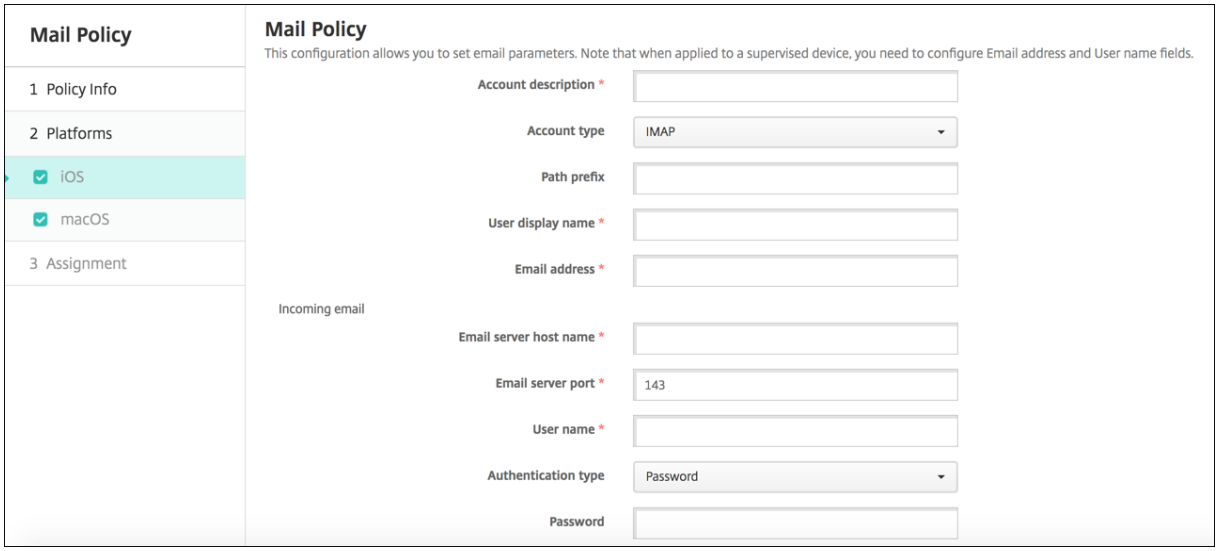
邮件设备策略

January 5, 2022

可以在 XenMobile 中添加邮件设备策略以在用户的 iOS 或 macOS 设备上配置电子邮件帐户。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 和 macOS 设置



- 帐户说明：键入在邮件和设置应用程序中显示的帐户说明。此字段为必填字段。
- 帐户类型：选择 **IMAP** 或 **POP** 以选择要用于用户帐户的协议。默认值为 **IMAP**。选择 **POP** 时，以下路径前缀选项将消失。
- 路径前缀：键入 **INBOX** 或您的 IMAP 邮件帐户路径前缀。此字段为必填字段。
- 用户显示名称：键入要用于邮件及其他用途的完整用户名。此字段为必填字段。
- 电子邮件地址：键入帐户的完整电子邮件地址。此字段为必填字段。

- 传入电子邮件设置
  - 电子邮件服务器主机名：键入传入电子邮件服务器主机名或 IP 地址。此字段为必填字段。
  - 电子邮件服务器端口：键入传入邮件服务器端口号。默认值为 **143**。此字段为必填字段。
  - 用户名：键入电子邮件帐户的用户名。此名称通常与电子邮件地址中 @ 字符前面的部分相同。此字段为必填字段。
  - 身份验证类型：选择要使用的身份验证类型。默认值为密码。选择无时，以下密码字段将消失。
  - 密码：键入传入邮件服务器的可选密码。
  - 使用 **SSL**：选择传入邮件服务器是否使用安全套接字层身份验证。默认值为关。
- 传出电子邮件设置
  - 电子邮件服务器主机名：输入传出邮件服务器主机名或 IP 地址。此字段为必填字段。
  - 电子邮件服务器端口：键入传出邮件服务器端口号。如果未输入端口号，将使用指定协议的默认端口。
  - 用户名：键入电子邮件帐户的用户名。此名称通常与电子邮件地址中 @ 字符前面的部分相同。此字段为必填字段。
  - 身份验证类型：选择要使用的身份验证类型。默认值为密码。
  - 密码：键入传出邮件服务器的可选密码。
  - 传出密码和传入密码相同：选择传入密码和传出密码是否相同。默认值为关，表示密码不相同。
  - 使用 **SSL**：选择传出邮件服务器是否使用安全套接字层身份验证。默认值为关。
- 策略
  - 授权电子邮件在帐户之间移动：选择是否允许用户将电子邮件从此帐户移出到另一个帐户以及从其他帐户转发和答复。默认值为关。
  - 仅从邮件应用程序发送电子邮件：选择是否限制用户只能从 iOS 邮件应用程序发送电子邮件。
  - 禁用最新邮件同步：选择是否阻止用户同步最近使用的地址。默认值为关。此选项仅适用于 iOS 6.0 及更高版本。
  - 允许投递邮件：选择是否允许对运行 iOS 9.2 及更高版本的设备使用 Apple 投递邮件。默认值为关。
  - 启用 **S/MIME** 签名：选择此帐户是否支持 S/MIME 签名。默认值为开。设置为开时，将显示以下两个字段。
    - 签署身份凭据：选择要使用的签名凭据。
    - **S/MIME** 签名用户可覆盖：如果设置为开，用户可以在其设备的设置中打开和关闭 S/MIME 签名。默认值为关。此选项适用于 iOS 12.0 及更高版本。
    - **S/MIME** 签名证书 **UUID** 用户可覆盖：如果设置为开，用户可以在其设备的设置中选择要使用的签名凭据。默认值为关。此选项适用于 iOS 12.0 及更高版本。
  - 启用 **S/MIME** 加密：选择此帐户是否支持 S/MIME 加密。默认值为关。设置为开时，将显示以下两个字段。
    - 加密身份凭据：选择要使用的加密凭据。
    - 启用 **“**为消息单独设置 **S/MIME”** 开关：设置为开时，向用户显示一个选项，用于为其撰写的每条消息打开或关闭 S/MIME 加密。默认值为关。
    - 默认 **S/MIME** 加密用户可替代：如果设置为 **“**开**”**，用户可以在其设备的设置中选择 **S/MIME** 是否默认处于打开状态。默认值为关。此选项适用于 iOS 12.0 及更高版本。
    - **S/MIME** 加密证书 **UUID** 用户可替代：如果设置为开，用户可以在其设备的设置中打开和关闭

S/MIME 加密身份和加密。默认值为关。此选项适用于 iOS 12.0 及更高版本。

- 策略设置
  - 删除策略：要稍后删除策略，可以将此设置配置为在选择日期或删除前的持续时间 (小时) 后删除策略。
  - 允许用户删除策略：允许用户始终删除邮件策略，仅使用需要通行码或从不删除。
  - 配置文件作用域：仅适用于 macOS，选择策略是适用于每个用户级别还是适用于整个系统。

托管域设备策略

January 5, 2022

可以定义应用到电子邮件和 Safari 浏览器的托管域。托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护公司数据。

对于 iOS 8 及更高版本的受监管设备，请指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。对于 iOS 9.3 及更高版本的受监督设备，可以在 Safari 中指定用户能够从中保存密码的 URL。

有关将 iOS 设备置于受监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

用户向域不在托管电子邮件域列表上的收件人发送电子邮件时，在用户的设备上此邮件将带有标记，以警告用户正在向企业域外部的人员发送邮件。

对于文档、附件或下载内容等项目：当用户使用 Safari 从位于托管 Web 域列表上的 Web 域打开某个项目（文档、附件或下载内容）时，将由合适的企业应用程序打开此项目。如果此项目所在的 Web 域不在托管 Web 域列表上，用户无法使用合适的企业应用程序打开此项目。必须使用未托管的个人应用程序打开。

对于受监督的设备，即使您未指定 Safari 密码自动填充域：如果设备配置为暂时多用户，用户将无法保存密码。但是，如果设备未配置为暂时多用户，用户可以保存所有密码。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

指定域：

格式	说明
`example.com`	将 `example.com` 下面的所有路径视为已托管，但 `site.example.com/` 除外。
`foo.example.com`	将 `foo.example.com` 下面的所有路径视为已托管，但 `example.com/` 和 `bar.example.com/` 除外。
`\*.example.com`	将 `foo.example.com` 或 `bar.example.com` 下面的所有路径视为已托管，但 `example.com/` 除外。

格式	说明
example.com/sub	将 example.com/sub 及其下面的所有路径视为已托管，但 example.com/ 除外。
foo.example.com/sub	将 foo.example.com/sub 下面的所有路径视为已托管，但 example.com、example.com/sub、foo.example.com/ 和 bar.example.com/sub 除外。
*.example.com/sub	将 foo.example.com/sub 或 bar.example.com/sub 下面的所有路径视为已托管，但 example.com 和 foo.example.com/ 除外。

规则：

- 比较域时，会忽略 URL 中的前导 “www.” 和尾部斜线。
- 如果条目包含端口号，只有指定此端口号的地址才被视为托管。否则，仅将标准端口视为托管（http 为端口 80，https 为端口 443）。例如，模式 *.example.com:8080 匹配 https://site.example.com:8080/page.html，但不匹配 https://site.example.com/page.html，而模式 *.example.com 匹配 https://site.example.com/page.html 和 https://site.example.com/page.html，但不匹配 https://site.example.com:8080/page.html。
- 托管 Safari Web 域定义具有累计性。所有托管 Safari Web 域负载定义的模式用于匹配 URL 请求。

设置：

- 托管域
  - 取消标记电子邮件域：对于要包含在列表中的每个电子邮件域，单击添加，然后执行以下操作：
    - 托管电子邮件域：键入电子邮件域。
    - 单击保存以保存电子邮件域，或单击取消不保存电子邮件域。
  - 托管 **Safari Web** 域：对于要包含在列表中的每个 Web 域，单击添加，然后执行以下操作：
    - 托管 **Web** 域：键入 Web 域。
    - 单击保存以保存 Web 域，或单击取消不保存 Web 域。
  - **Safari** 密码自动填充域：对于要包含在列表中的每个自动填充域，单击添加，然后执行以下操作：
    - **Safari** 密码自动填充域：键入自动填充域。
    - 单击保存以保存自动填充域，或单击取消不保存自动填充域。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

MDM 选项设备策略

January 5, 2022

可以在 XenMobile 中创建一个设备策略，用于在受监督的 iOS 7.0 及更高版本的手机设备上管理“查找我的 iPhone/iPad 激活锁”。有关将 iOS 设备置于受监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

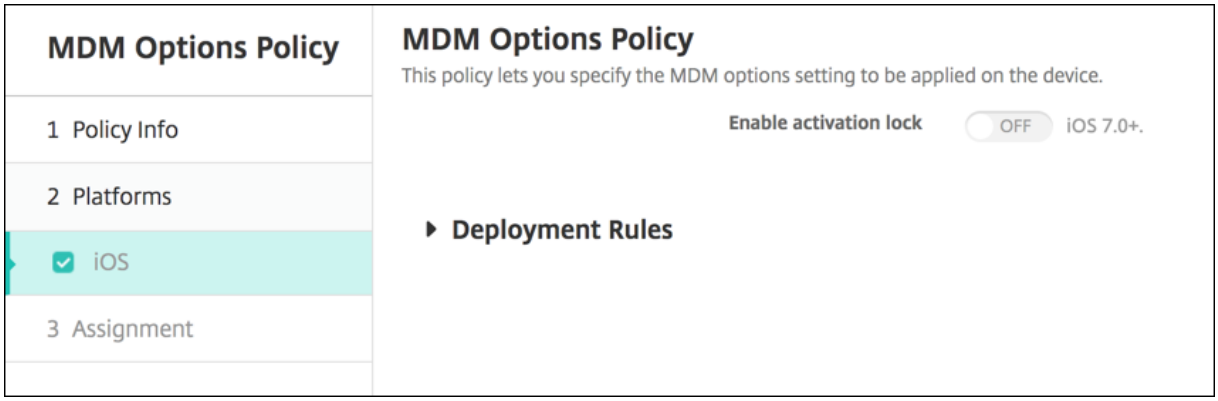
激活锁是一项“查找我的 iPhone/iPad”功能，用于阻止重新激活丢失或被盗的受监督设备。激活锁需要用户的 Apple ID 和密码，之后用户才能关闭“查找我的 iPhone/iPad”、擦除设备或重新激活设备。对于组织拥有的设备，绕过激活锁是（例如）重置或重新分配设备的必要操作。

要启用激活锁，请配置并部署 XenMobile MDM 选项设备策略。之后可以从 XenMobile 控制台管理设备，而不需要用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 XenMobile 控制台发出“激活锁绕过”安全操作。

例如，如果用户在执行完全擦除操作之前或之后归还了丢失的手机或设置了设备：手机提示输入 iTunes 帐户凭据时，可以通过从 XenMobile 控制台发出“激活锁绕过”安全操作来绕过该设置。

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- 启用激活锁：选择是否要在部署此策略的设备上启用激活锁。默认值为关。

通过部署 MDM 选项设备策略启用激活锁后：当您在管理 > 设备页面上选择这些设备并单击安全时，将显示安全操作激活锁绕过。通过“激活锁绕过”，可以在设备激活之前从受监督的设备中删除激活锁，而不需要知晓设备用户的 Apple ID 和密码。可以在执行完全擦除操作之前或之后向设备发送“激活锁绕过”安全操作。有关详细信息，请参阅“安全操作”一文中的绕过 iOS 激活锁。

组织信息设备策略

March 27, 2020

可以在 XenMobile 中添加一个设备策略，用于指定贵组织从 XenMobile 推送到 iOS 设备的警报消息信息。此策略适用于 iOS 7 及更高版本的设备。

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。

iOS 设置

- 名称：键入运行 XenMobile 的组织的名称。
- 地址：键入组织的地址。
- 电话：键入组织的支持电话号码。
- 电子邮件：键入支持电子邮件地址。
- 魔术字：键入用于描述组织托管的服务的单词或短语。

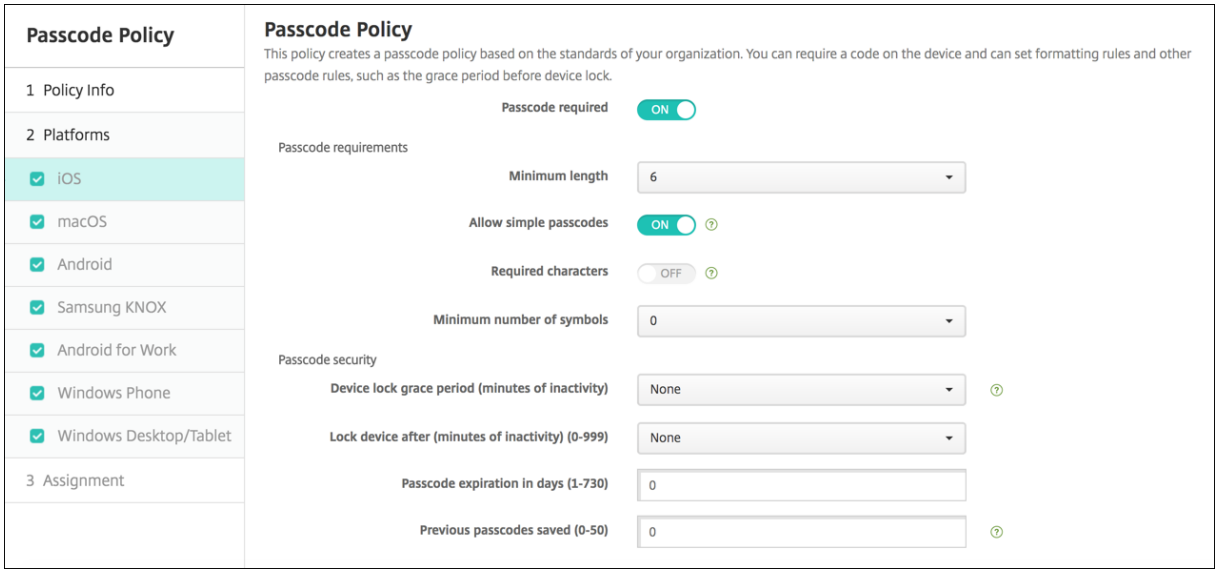
通行码设备策略

January 5, 2022

可以根据贵组织的标准在 XenMobile 中创建通行码策略。可以要求在用户设备上输入通行码，并且可以设置各种格式和通行码规则。您可以为 iOS、macOS、Android、Samsung KNOX、Android Enterprise、Windows Phone 和 Windows Desktop/Tablet 创建策略。每种平台需要一组不同的值，本文将对此进行介绍。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

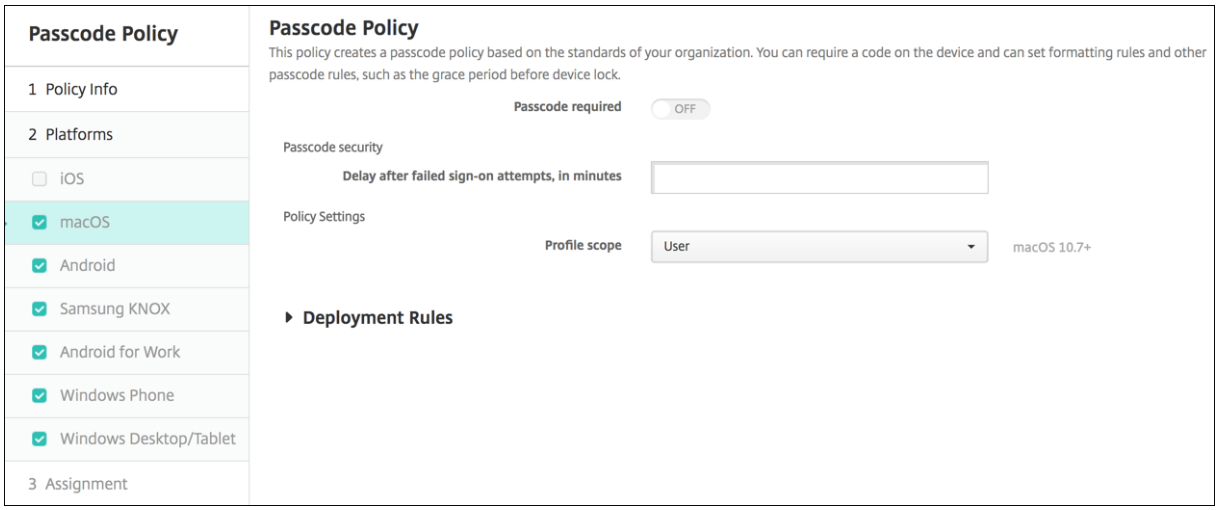
iOS 设置



- 需要通行码：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。

- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 **6**。
  - 允许使用简单通行码：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为开。
  - 需含字符：选择是否要求通行码至少包含一个字母。默认值为关。
  - 符号数下限：在列表中，单击通行码必须包含的符号数量。默认值为 **0**。
- 通行码安全
  - 设备锁定宽限期 **(**不活动分钟**)**：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。默认设置为无。
  - 此时间后锁定设备 **(**不活动分钟数**)**：在列表中，单击设备在锁定之前可以不活动的时间长度。默认设置为无。
  - 通行码有效期限 **(1 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 失败登录尝试次数上限：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被完全擦除。默认值为未定义。

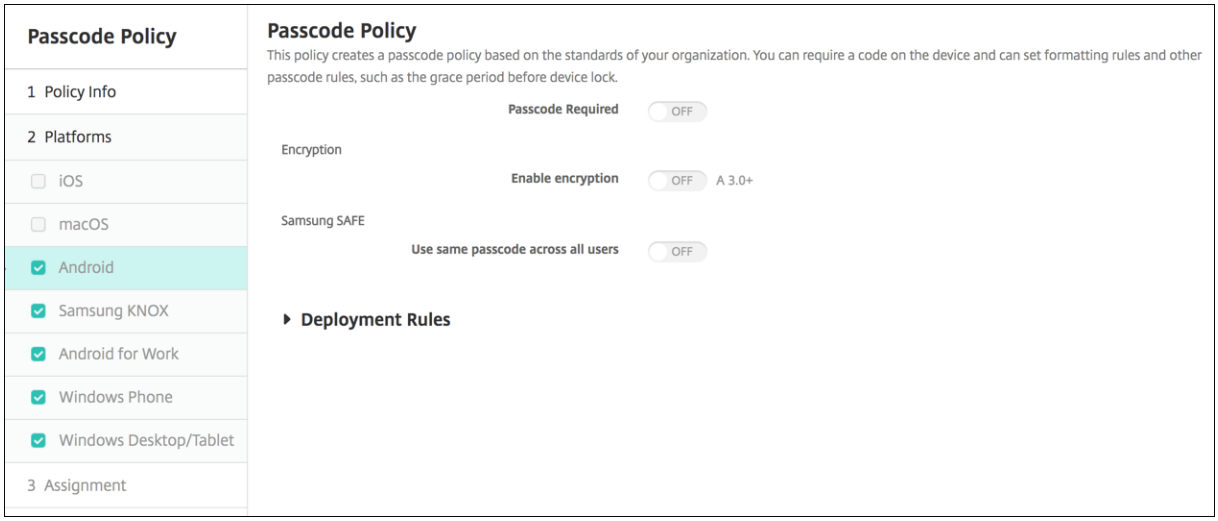
macOS 设置



- 需要通行码：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。
- 如果未启用需要通行码，请在尝试登录失败后的延迟时间 **(**分钟**)** 旁边，键入允许用户重新输入其通行码之前延迟的分钟数。
- 如果启用了需要通行码，请配置以下设置：
- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 **6**。
  - 允许使用简单通行码：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为开。
  - 需含字符：选择是否要求通行码至少包含一个字母。默认值为关。

  - 符号数下限：在列表中，单击通行码必须包含的符号数量。默认值为 **0**。
- 通行码安全
  - 设备锁定宽限期 **(**不活动分钟**)**：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。默认设置为无。
  - 此时间后锁定设备 **(**不活动分钟数**)**：在列表中，单击设备在锁定之前可以不活动的时间长度。默认设置为无。
  - 通行码有效期限 **(1 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 失败登录尝试次数上限：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被锁定。默认值为未定义。
  - 尝试登录失败后的延迟时间 **(**分钟**)**：键入允许用户重新输入其通行码之前延迟的分钟数。
  - 强制重置通行码：用户下次进行身份验证时，必须重置通行码。
- 策略设置
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Android 设置



> 注意：
>
> Android 的默认值为关。

- 需要通行码：选择此选项以要求输入通行码并显示 Android 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性、加密和 Samsung SAFE 的相关设置。
- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 6。

  - 生物特征识别：选择是否启用生物特征识别。如果启用此选项，需含字符字段将隐藏。默认值为关。
  - 需含字符：在列表中，单击“无限制”、“数字和字母”、“仅限数字”或“仅限字母”以配置通行码的组成方式。默认值为无限制。
  - 高级规则：选择是否应用高级通行码规则。此选项适用于 Android 3.0 及更高版本。默认值为关。
  - 启用高级规则时，请在下面每个列表中，单击通行码必须包含的每种字符类型的最小数量：
    * 符号：符号的最小数量。
    * 字母：字母的最小数量。
    * 小写字母：小写字母的最小数量。
    * 大写字母：大写字母的最小数量。
    * 数字或符号：数字或符号的最小数量。
    * 数字：数字的最小数量。

- 通行码安全
  - 此时间后锁定设备 **(**不活动分钟数**)**：在列表中，单击设备在锁定之前可以不活动的时间长度。默认值为无
  - 通行码有效期限 **(1 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 失败登录尝试次数上限：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被擦除。默认值为未定义。

- 加密
  - 启用加密：选择是否启用加密。此选项适用于 Android 3.0 及更高版本。无论需要通行码设置为何，此选项都可用。

    要加密其设备，用户必须首先具有充电电池并将此设备接通电源一个小时或更长时间，以便进行加密。如果中断加密过程，可能会丢失其设备上的部分或全部数据。设备加密后，过程无法逆转，除非执行出厂重置，但这样会擦除设备上的所有数据。

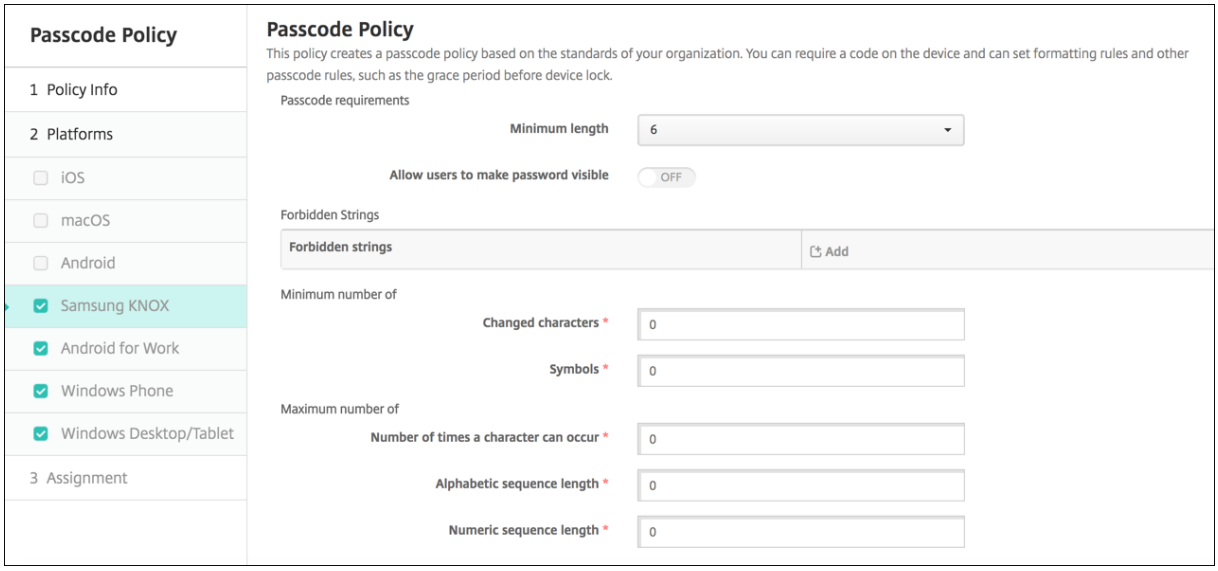
- **Samsung SAFE**

  > 注意：
  >
  > 在 Samsung SAFE 设备上禁用面部或虹膜识别的解决方法：为 Samsung SAFE 创建限制设备策略。在“限制策略”中，打开禁用应用程序，并将 `com.samsung.android.bio.face.service` 或 `com.samsung.android.server.iris` 添加到表中。然后部署限制策略。

  - 对所有用户使用相同的通行码：选择是否对所有用户使用相同的通行码。默认值为关。此设置仅适用于 Samsung SAFE 设备，无论需要通行码设置为何，此设置都可用。
  - 启用对所有用户使用相同的通行码时，请在通行码字段键入供所有用户使用的通行码。
  - 启用需要通行码时，请配置以下 Samsung SAFE 设置：
    * 更改的字符：键入用户必须在以前的通行码中更改的字符数量。默认值为 **0**。
    * 字符可以出现的次数：键入某个字符可以在通行码中出现的最大次数。默认值为 **0**。

* 字母序列长度：键入通行码中字母序列的最大长度。默认值为 **0**。
* 数字序列长度：键入通行码中数字序列的最大长度。默认值为 **0**。
* 允许用户将密码设为可见：选择用户是否可以将通行码设为可见。默认值为开。
* 配置生物特征身份验证。选择是否启用生物特征身份验证。默认值为关。如果将其设置为开，则可以设置以下选项：
  - 允许指纹。选择是否允许用户使用指纹进行身份验证。
  - 允许虹膜。选择是否允许用户使用虹膜进行身份验证。
* 禁止的字符：可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。对于要拒绝的每个字符串，单击添加，然后执行以下操作：
  - 禁止的字符：键入用户不能使用的字符串。
  - 单击保存以添加字符串，或单击取消以取消添加字符串。

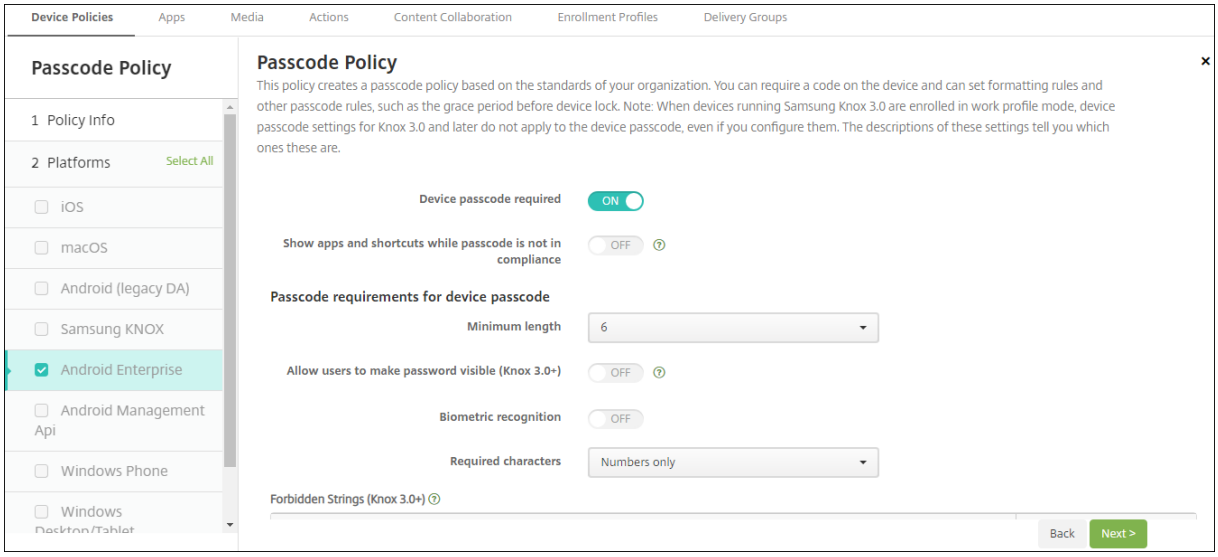
Samsung KNOX 设置



- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 **6**。
  - 允许用户将密码设为可见：选择是否允许用户将密码设为可见。
  - 禁止的字符：可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。对于要拒绝的每个字符串，单击添加，然后执行以下操作：
    * 禁止的字符：键入用户不能使用的字符串。
    * 单击保存以添加字符串，或单击取消以取消添加字符串。
- 数量下限
  - 更改的字符：键入用户必须在以前的通行码中更改的字符数量。默认值为 **0**。
  - 符号：键入通行码中所需符号的最小数量。默认值为 **0**。
- 数量上限
  - 字符可以出现的次数：键入某个字符可以在通行码中出现的最大次数。默认值为 **0**。

  - 字母序列长度：键入通行码中字母序列的最大长度。默认值为 **0**。
  - 数字序列长度：键入通行码中数字序列的最大长度。默认值为 **0**。
- 通行码安全
  - 此时间后锁定设备 **(**不活动分钟数**)**：在列表中，单击设备在锁定之前可以不活动的秒数。默认设置为无。
  - 通行码有效期限 **(1 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 如果超过失败登录尝试次数，设备将锁定：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被锁定。默认值为未定义。
  - 如果超过失败登录尝试次数，设备将被擦除：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，将从设备中擦除 KNOX 容器（以及 KNOX 数据）。在擦除后，用户需要重新初始化 KNOX 容器。默认值为未定义。

Android Enterprise 设置



对于 Android Enterprise 设备，可以要求设备的通行码或 Android Enterprise 工作配置文件的安全质询或两者。

对于运行 Android 8.0 或更高版本以及 Samsung Knox 3.0 及更高版本的设备，请在 **Android Enterprise** 页面上为 Samsung Knox 配置设置。对于运行早期版本的 Android 或 Samsung Knox 的设备，请使用 **Samsung Knox** 页面。

> 注意：
>
> 当运行 Samsung Knox 3.0 的设备注册为工作配置文件设备时，Knox 3.0 及更高版本的设备通行码设置也不适用于设备通行码，即使您对其进行了配置亦如此。

- 需要设备通行码：需要设备上的通行码。当此设置设为开时，请配置设备通行码的通行码要求和设备通行码的通行码安全性下的设置。默认值为关。

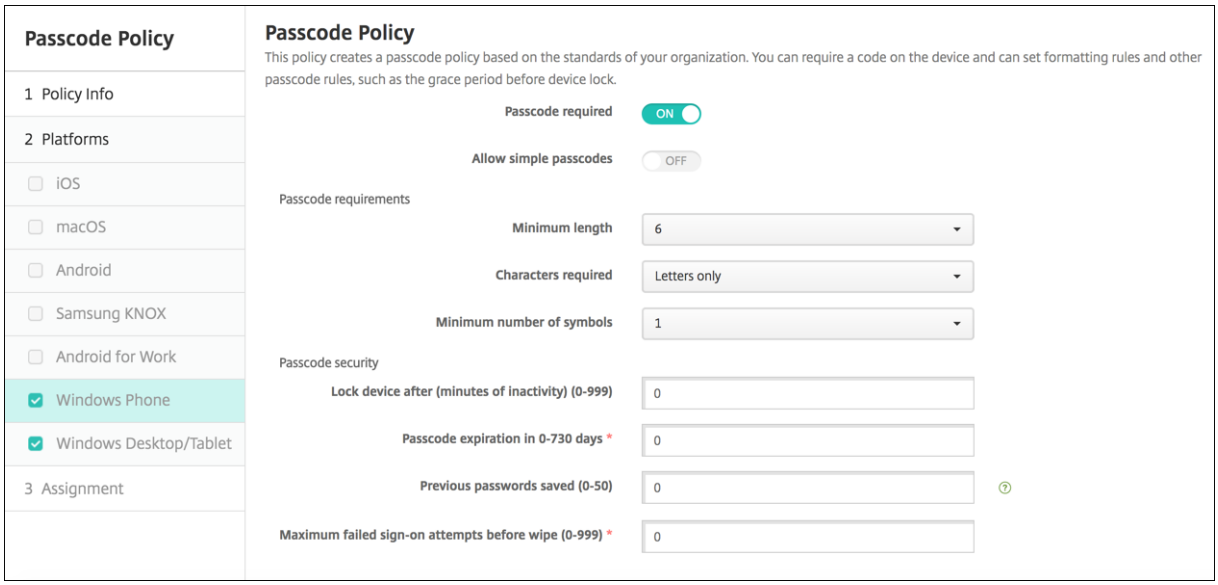
- **Show apps and shortcuts while passcode is not in compliance**（在通行码不合规时显示应用程序和快捷方式）：如果此设置为开，设备上的应用程序和快捷方式也不会被隐藏，即使通行码不合规亦如此。当此设置设为关时，如果通行码不合规，应用程序和快捷方式将被隐藏。如果启用此设置，Citrix 建议您创建一项自动操作，以便在通行码不合规时将设备标记为不合规。默认值为关。
- 设备通行码的通行码要求：
  - 最小长度：指定通行码的最小长度。默认值为 6。
  - 允许用户将密码设为可见：适用于运行 Samsung Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作配置文件设备的设备。允许用户将密码设为可见。默认值为关。
  - 生物特征识别：启用生物特征识别。如果此设置设为开，则隐藏需含字符字段。默认值为关。
  - 需含字符：指定通行码所需的字符类型。在列表中，选择无限制、数字和字母、仅数字或仅字母。请仅对运行 Android 7.0 的设备使用无限制。Android 7.1 及更高版本不遵守无限制设置。默认值为数字和字母。
  - 禁止的字符串：适用于运行 Samsung Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作配置文件设备的设备。指定用户不能用作通行码的字符串。可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。对于要拒绝的每个字符串：单击添加；键入您不希望用户使用的字符串；单击保存以添加字符串，或单击取消以取消添加字符串。
  - 高级规则：对可能出现在通行码中的字符类型应用高级规则。当此设置设为开时，请在数量下限和数量上限下配置设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为关。
  - 数量下限：
    - 符号：指定符号的最小数量。默认值为 **0**。
    - 字母：指定字母的最小数量。默认值为 **0**。
    - 小写字母：指定小写字母的最小数量。默认值为 **0**。
    - 大写字母：指定大写字母的最小数量。默认值为 **0**。
    - 数字或符号：指定数字或符号的最小数量。默认值为 **0**。
    - 数字：指定数字的最小数量。默认值为 **0**。
    - 更改的字符：适用于运行 Samsung Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作配置文件设备的设备。指定用户必须在以前的通行码中更改的字符数量。默认值为 **0**。
  - 数量上限：适用于运行 Samsung Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作配置文件设备的设备。
    - 字符可以出现的次数：指定某个字符可以在通行码中出现的最大次数。默认值为 **0**，这意味着没有上限。
    - 字母序列长度：指定通行码中字母序列的最大长度。默认值为 **0**，这意味着没有上限。
    - 数字序列长度：指定通行码中数字序列的最大长度。默认值为 **0**，这意味着没有上限。
- 设备通行码的通行码安全性：
  - 此次数后擦除设备 **(**失败登录尝试次数**)**：指定用户可以登录失败的次数，超过此次数后，设备将被完全擦除。默认值为未定义。
  - 此时间后锁定设备 **(**不活动分钟数**) (0-999)**：指定设备在锁定之前可以不活动的分钟数。默认设置为无。

  - 通行码有效期限 **(1 - 730** 天**)**：指定有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：指定要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 此次数后锁定设备 **(**失败登录尝试次数**)**：适用于运行 Samsung Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作配置文件设备的设备。指定用户可以登录失败的次数，超过此次数后，设备将被锁定。默认值为未定义。
- 工作配置文件安全质询：要求用户完成安全质询才能访问 Android Enterprise 工作配置文件中运行的应用程序。适用于运行 Android 7.0 及更高版本的设备。当此设置设为开时，请配置工作配置文件安全质询的通行码要求和工作配置文件安全质询的通行码安全性下的设置。默认值为关。
- 工作配置文件安全质询的通行码要求：
  - 最小长度：指定通行码的最小长度。默认值为 6。
  - 允许用户将密码设为可见：适用于运行 Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。允许用户将密码设为可见。默认值为关。
  - 生物特征识别：启用生物特征识别。如果此设置设为开，则隐藏需含字符字段。默认值为关。
  - 需含字符：指定通行码所需的字符类型。在列表中，选择无限制、数字和字母、仅数字或仅字母。请仅对运行 Android 7.0 的设备使用无限制。Android 7.1 及更高版本不遵守无限制设置。默认值为数字和字母。
  - 禁止的字符串：适用于运行 Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。指定用户不能用作通行码的字符串。可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。对于要拒绝的每个字符串：单击添加；键入您不希望用户使用的字符串；单击保存以添加字符串，或单击取消以取消添加字符串。
  - 高级规则：对可能出现在通行码中的字符类型应用高级规则。当此设置设为开时，请在数量下限和数量上限下配置设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为关。
  - 数量下限：
    * 符号：指定符号的最小数量。默认值为 **0**。
    * 字母：指定字母的最小数量。默认值为 **0**。
    * 小写字母：指定小写字母的最小数量。默认值为 **0**。
    * 大写字母：指定大写字母的最小数量。默认值为 **0**。
    * 数字或符号：指定数字或符号的最小数量。默认值为 **0**。
    * 数字：指定数字的最小数量。默认值为 **0**。
    * 更改的字符：适用于运行 Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。指定用户必须在以前的通行码中更改的字符数量。默认值为 **0**。
  - 数量上限：适用于运行 Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。
    * 字符可以出现的次数：指定某个字符可以在通行码中出现的最大次数。默认值为 **0**，这意味着没有上限。
    * 字母序列长度：指定通行码中字母序列的最大长度。默认值为 **0**，这意味着没有上限。
    * 数字序列长度：指定通行码中数字序列的最大长度。默认值为 **0**，这意味着没有上限。
  - 启用统一通行码：如果设置为开，则用户将一个通行码用于其设备和工作配置文件。如果设置为关：
    * 用户必须对其设备和工作配置文件使用不同的通行码。

    * 设备上的 **Use one lock**（使用一个锁）设置（如果用户希望为其设备和工作配置文件使用一个通行码）已禁用。用户无法启用该设置。
    * 如果工作配置文件安全质询的通行码要求比设备通行码更复杂：系统将提示启用了 **Use one lock**（使用一个锁）设置的用户更改其工作配置文件通行码。

  默认值为关。自 Android 9.0 起可用。
- 工作配置文件安全质询的通行码安全性
  - 此次数后擦除容器 **(**失败登录尝试次数**)**：指定用户可以登录失败的次数，超过此次数后，工作配置文件及其数据将从设备中擦除。擦除后，用户需要重新初始化工作配置文件。默认值为未定义。
  - 此时间后锁定容器 **(**不活动分钟数**)**：指定在锁定工作配置文件之前设备可以不活动的分钟数。默认设置为无。
  - 通行码有效期限 **(1 - 730** 天**)**：指定有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：指定要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 此次数后锁定容器 **(**失败登录尝试次数**)**：适用于运行 Knox 3.0 及更高版本并且配置了有效的 Knox 许可证密钥的设备。指定用户可以登录失败的次数，超过此次数后，设备将被锁定。默认值为未定义。

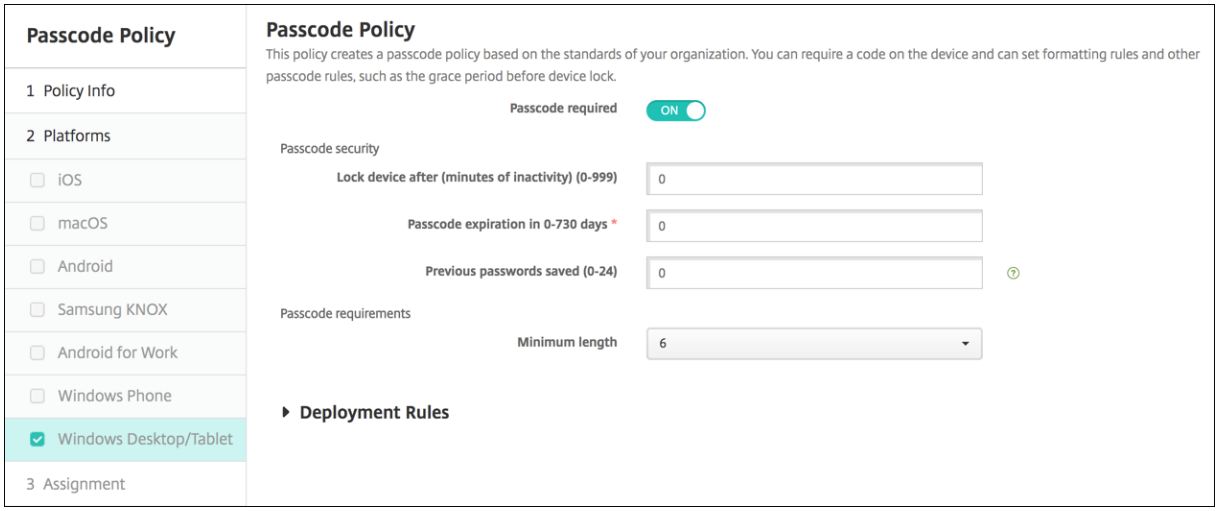
Windows Phone 设置



- 需要通行码：选择此选项将不要求提供 Windows Phone 设备的通行码。默认值为开，表示需要提供通行码。禁用此设置时，页面折叠，不再显示以下选项。
- 允许使用简单通行码：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为关。
- 通行码要求
  - 最小长度：在列表中，单击通行码的最小长度。默认值为 **6**。
  - 需含字符：在列表中单击数字或字母数字、仅限字母或仅限数字以配置通行码的组成方式。默认值为仅限字母。

  - 符号数下限：在列表中，单击通行码必须包含的符号数量。默认值为 **1**。
- 通行码安全
  - 此时间后锁定设备 **(**不活动分钟数**)**：键入设备在锁定之前可以不活动的分钟数。默认值为 **0**。
  - 通行码在 **0 - 730** 天内有效：键入有效天数，超过此天数后，通行码将过期。有效值为 0-730。默认值为 **0**，表示通行码永不过期。
  - 保存的以前用过的密码数量 **(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
  - 擦除前的最大失败登录尝试次数 **(0 - 999)**：键入用户在成功登录之前可以失败的次数，超过此次数后，将从设备中擦除公司数据。默认值为 **0**。

Windows Desktop/Tablet 设置



- 不允许便捷登录：选择是否允许用户使用图片密码或生物特征识别登录访问其设备。默认值为关。
- 最小通行码长度：在列表中，单击通行码的最小长度。默认值为 **6**。
- 擦除前的通行码尝试次数上限：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，将从设备中擦除公司数据。默认值为 **4**。
- 通行码有效期限 **(0 - 730** 天**)**：键入有效天数，超过此天数后，通行码将过期。有效值为 0-730。默认值为 **0**，表示通行码永不过期。
- 通行码历史记录**: (1-24)**：键入要保存的使用过的通行码数量。用户无法使用在此列表中找到的任何通行码。有效值为 1-24。必须在此字段中输入介于 1 到 24 之间的数值。默认值为 **0**。
- 设备锁定前的最长不活动时间 **(1 - 999** 分钟**)**：输入设备在锁定之前可以不活动的时间长度（分钟）。有效值为 1-999。必须在此字段中输入介于 1 到 999 之间的数值。默认值为 **0**。

个人热点设备策略

March 27, 2020

当用户不在 WiFi 网络范围内，可以允许用户通过其 iOS 设备的个人热点功能，使用手机网络数据连接来连接到 Internet。适用于 iOS 7.0 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

- 禁用个人热点：选择是否在用户设备上禁用个人热点功能。默认值为关，表示在用户设备上关闭个人热点。此策略不禁用该功能。用户仍可以在其设备上使用个人热点，但是部署此策略后，将关闭个人热点功能，因此默认情况下不打开此功能。

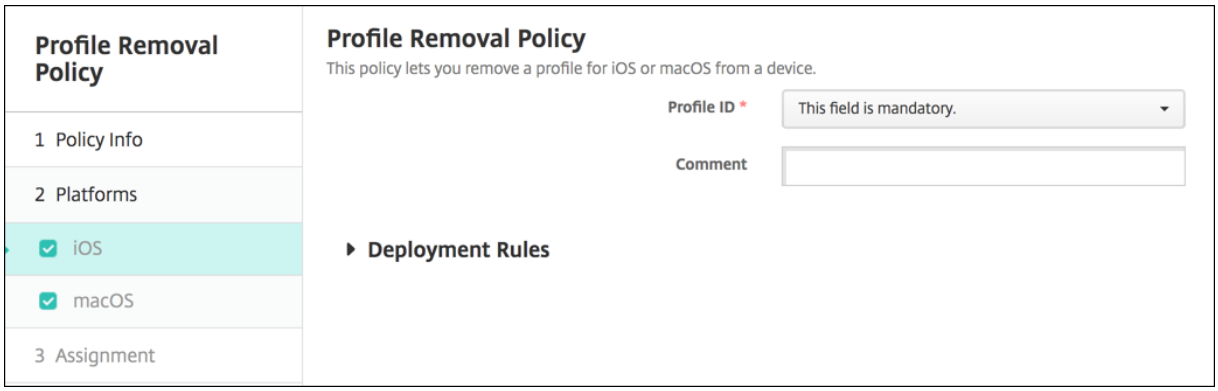
配置文件删除设备策略

March 27, 2020

可以在 XenMobile 中创建应用程序配置文件删除设备策略。此策略在部署时，将从用户的 iOS 或 macOS 设备删除应用程序配置文件。

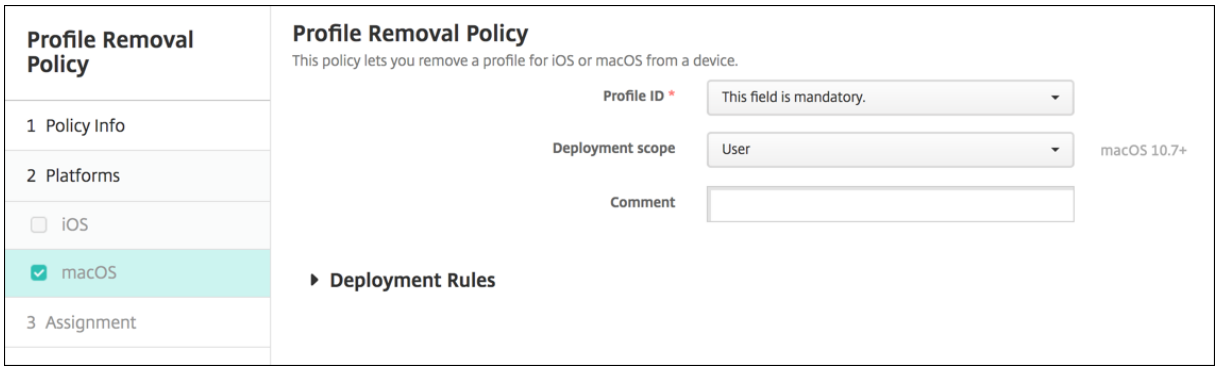
要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- 配置文件 **ID**：在列表中，单击应用程序配置文件 ID。此字段为必填字段。
- 备注：键入可选备注。

macOS 设置



- 配置文件 **ID**：在列表中，单击应用程序配置文件 ID。此字段为必填字段。
- 部署范围：在列表中，单击用户或系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。
- 备注：键入可选备注。

预配配置文件设备策略

January 5, 2022

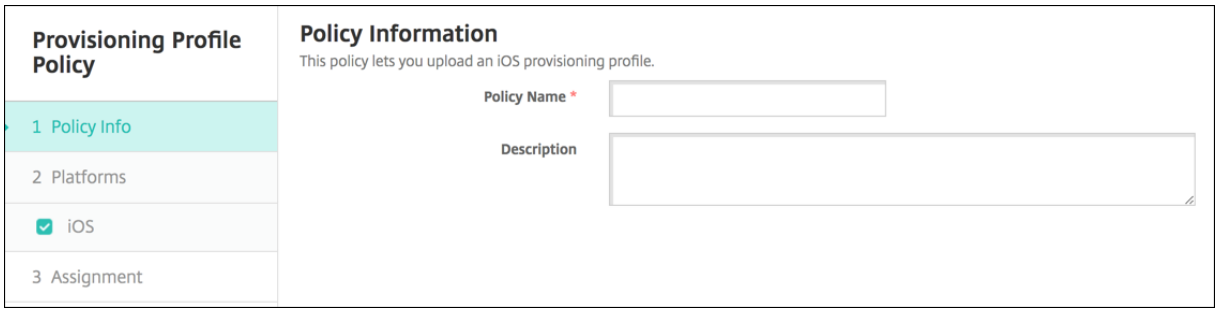
开发或代码签名 iOS 企业应用程序时，通常包含企业分发预配配置文件，Apple 需要此配置文件才能允许应用程序在 iOS 设备上运行。如果预配配置文件缺失或已过期，用户轻按应用程序以将其打开时，应用程序将崩溃。

预配配置文件的主要问题是，它们在 Apple 开发人员门户上生成一年之后将过期，您必须跟踪用户注册的所有 iOS 设备上的所有预配配置文件的过期日期。跟踪过期日期不仅涉及到跟踪实际的过期日期，还要跟踪每个用户正在使用的应用程序版本。两种解决方案分别为通过电子邮件将预配配置文件发送给用户或者将其置于 Web 门户中以供下载和安装。这些解决方案可行，但容易出错，因为需要用户响应电子邮件中的说明，或访问 Web 门户并下载正确的配置文件，然后再进行安装。

要使此过程对用户透明，您可以在 XenMobile 使用设备策略来安装和删除预配配置文件。在必要时删除缺失或过期的预配配置文件并在用户设备上安装最新的配置文件，这样一来，只需轻按应用程序，即可将其打开并使用。

创建预配配置文件策略之前，必须创建预配配置文件。有关详细信息，请参阅 Apple 在 Apple 开发人员站点上发布的关于如何创建开发预配配置文件的文章。

iOS 设置



- **iOS** 预配配置文件：单击浏览并导航到要导入的预配配置文件所在位置，选择此文件。

删除预配配置文件设备策略

January 5, 2022

您可以通过设备策略删除 iOS 预配配置文件。有关预配配置文件的详细信息，请参阅预配配置文件设备策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- **iOS** 预配配置文件：在列表中，单击要删除的预配配置文件。
- 备注：（可选）添加备注。

代理设备策略

January 5, 2022

可以在 XenMobile 中添加一个设备策略，用于为运行 Windows Mobile/CE 和 iOS 6.0 或更高版本的设备指定全局 HTTP 代理设置。只能为每个设备部署一个全局 HTTP 代理策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

必备条件

在部署此策略之前，请务必将要为其设置全局 HTTP 代理的所有 iOS 设备设置为受监督模式。有关详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式或通过 Apple 部署计划部署设备。

将代理策略发送到设备之前，设置部署规则以注册设备。

iOS 设置

- 代理配置：单击手动或自动以设置在用户设备上配置代理的方式。
  - 如果单击手动，可以配置以下设置：
    - 代理服务器的主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
    - 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。
    - 用户名：键入向代理服务器进行身份验证的可选用户名。
    - 密码：键入向代理服务器进行身份验证的可选密码。
  - 如果单击自动，可以配置以下设置：
    - 代理 **PAC URL**：键入用于定义代理配置的 PAC 文件的 URL。
    - 允许在无法访问 **PAC** 时直接连接：选择是否允许用户在无法访问 PAC 文件时直接连接到目标。默认值为开。此选项仅适用于 iOS 7.0 及更高版本。
- 允许旁路代理以访问俘获型网络：选择是否允许旁路代理以访问俘获型网络。默认值为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

Windows Mobile/CE 设置

- 网络：在列表中，单击要使用的网络类型。默认值为内置办公网络。可能的选项包括：
  - 用户定义的办公网络
  - 用户定义的 Internet
  - 内置办公网络
  - 内置 Internet
- 网络：在列表中，单击要使用的网络连接协议。默认值为 **HTTP**。可能的选项包括：
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- 代理服务器的主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
- 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。默认值为 **80**。
- 用户名：键入向代理服务器进行身份验证的可选用户名。
- 密码：键入向代理服务器进行身份验证的可选密码。
- 域名：键入可选域名。
- 启用：选择是否启用代理。默认值为开。

注册表设备策略

March 27, 2020

Windows Mobile/CE 注册表存储关于应用程序、驱动器、用户首选项和配置设置的数据。在 XenMobile 中，可以定义用于管理 Windows Mobile/CE 设备的注册表项和值。

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。

Windows Mobile/CE 设置

对于要添加的每个注册表项或注册表项/值对，单击添加，然后执行以下操作：

- 注册表项路径：键入注册表项的完整路径。例如，键入 **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows** 以指定从 HKEY_LOCAL_MACHINE 根注册表项到 Windows 注册表项的路由。
- 注册表值的名称：键入注册表项值的名称。例如，键入 **ProgramFilesDir** 将该值名称添加到注册表项路径 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion。如果将此字段留空，表示将添加注册表项而非注册表项/值对。
- 类型：在列表中，单击值的数据类型。默认值为 **DWORD**。可能的选项包括：
  - **DWORD**： 32 位无符号整数。
  - 字符串：任意字符串。
  - 扩展字符串：可以包含环境变量（例如%TEMP% 或%USERPROFILE%）的字符串值。
  - 二进制：任意二进制数据。
- 值：键入与注册表值名称关联的值。例如，要指定 ProgramFilesDir 的值，请键入 **C:\Program Files**。
- 单击保存以保存注册表项信息，或单击取消不保存注册表项信息。

远程支持设备策略

January 5, 2022

> 注意：
>
> 对于本地 XenMobile Server 部署：通过远程支持，您的技术支持代表能够远程控制托管的 Windows CE 和 Android 移动设备。屏幕录像功能仅在 Samsung KNOX 设备上受支持。
>
> 远程支持不支持本地群集 XenMobile Server 部署。
>
> 有关详细信息，请参阅支持选项和远程支持。

可以在 XenMobile 中创建远程支持策略以授予您远程访问受支持的 Windows 和 Android 设备的权限。可以配置两种类型的支持：

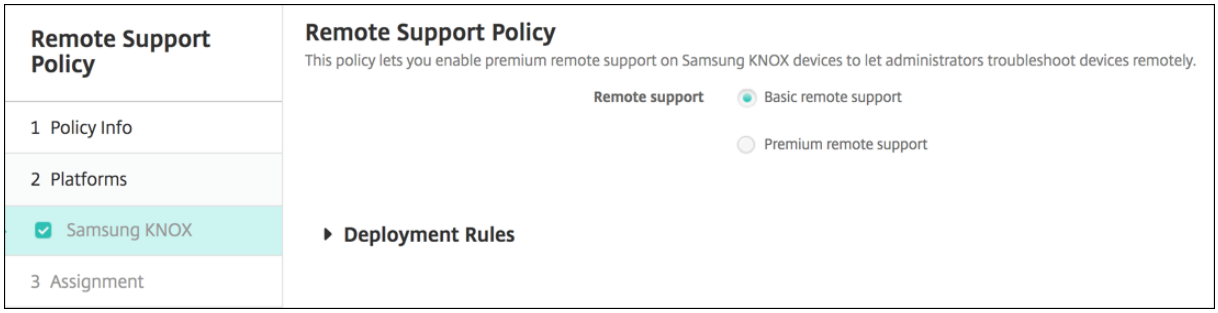
- 基本，用于查看有关设备的诊断信息（如系统信息）、正在运行的进程、任务管理器（内存和 CPU 使用率）、已安装的软件文件夹内容等。
- 高级，用于远程控制设备屏幕，其中包括：
  - 控制颜色（在主窗口或独立的浮动窗口中）
  - 在技术支持人员与用户之间建立 IP 语音会话 (VoIP)
  - 配置设置
  - 在技术支持人员与用户之间建立聊天会话。

要实施此策略，必须执行以下操作：

- 在您的环境中安装 XenMobile Remote Support 应用程序。
- 配置远程支持应用程序通道。有关详细信息，请参阅应用程序通道设备策略。
- 按本主题中所述配置 Samsung KNOX 远程支持设备策略。
- 同时对用户设备部署应用程序通道远程支持策略和 Samsung KNOX 远程支持策略。

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。

Android 和 **Windows CE** 设置



- 远程支持：选择基本远程支持或高级远程支持。默认值为基本远程支持。

限制设备策略

January 5, 2022

限制设备策略允许或限制用户设备上的某些特性或功能，例如相机。您还可以设置安全限制、对媒体内容的限制以及对用户能够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。主要的例外情况是 iOS 安全 - 强制功能和所有 Windows Tablet 功能，其默认值为关或限制。

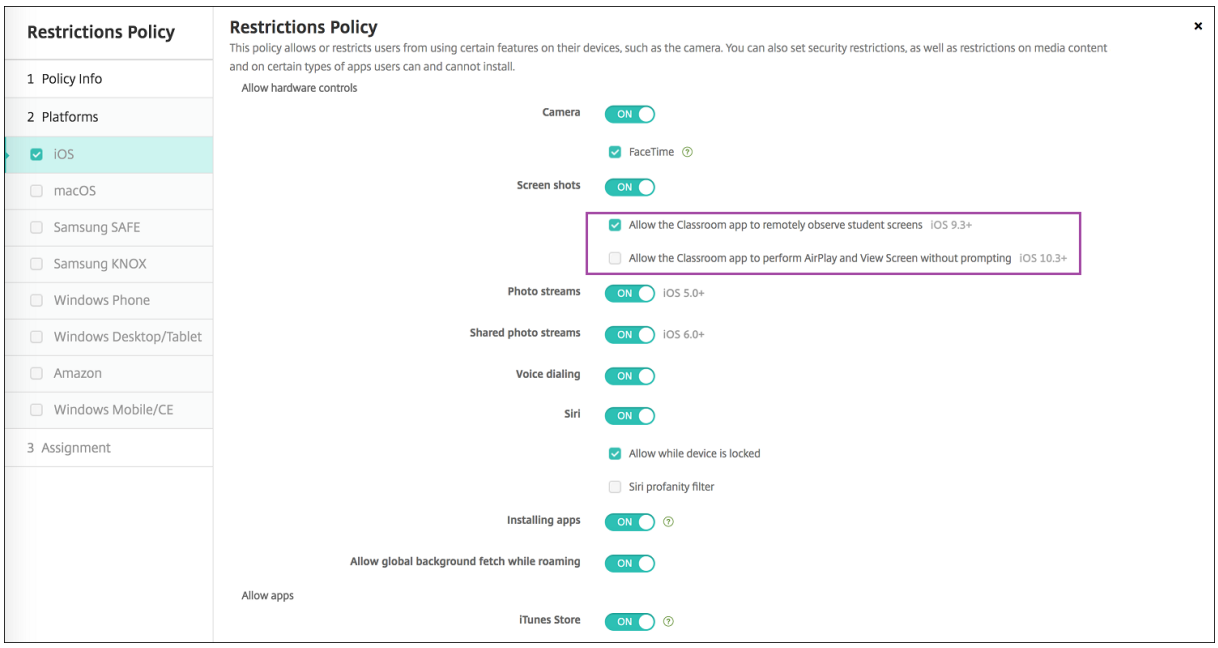
对于 Windows 10 RS2 Phone：用于禁用 Internet Explorer 的自定义 XML 策略或限制策略部署到 Phone 后，浏览器将保持已启用。要解决此问题，请重新启动 Phone。这是第三方问题。

> 提示：
>
> 如果您为任何选项选择开，则意味着用户可以执行该操作或使用该功能。例如：

> 相机。如果设置为开，用户将可以在其设备上使用相机。如果设置为关，用户将无法在其设备上使用相机。
>
> 屏幕截图。如果设置为开，用户可以在其设备上截取屏幕截图。如果设置为关，用户将无法在设备上截取屏幕截图。

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，如此处和 XenMobile 控制台限制策略页面中所述。

当设备在用户注册模式、未受监督（完全 MDM）模式或受监督模式下注册时，iOS 限制策略设置可能适用。下表显示了适用于 iOS 13 及更高版本的每个限制策略设置的注册模式。

如表中所示，自 iOS 13 起，以前在未受监督和监督模式下可用的某些设置仅在监督模式下可用。以下规则适用：

- 如果受监督的 iOS 13+ 设备在 XenMobile 中注册，这些设置将应用到该设备。
- 如果未受监督的 iOS 13+ 设备在 XenMobile 中注册，这些设置将不应用到该设备。
- 如果 iOS 12（或更低版本）的设备已在 XenMobile 中注册，然后升级到 iOS 13，则不会发生任何变化。这些设置与升级之前一样应用到设备。

有关将 iOS 设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

设置	用户注册	不受监督	受监督
允许硬件控制			
相机	否	是	是
FaceTime	否	否（iOS 13 中的新增功能）	是

设置	用户注册	不受监督	受监督
屏幕截图	是	否	是
允许“课堂”应用程序远程观察学生的屏幕	否	否	是
允许“课堂”应用程序运行 AirPlay 和查看屏幕而不提示	否	否	是
照片流	否	是	是
共享照片流	否	是	是
语音拨号	否	是	是
Siri	是	是	是
设备锁定时允许	是	是	是
Siri 猥亵语言过滤器	否	否	是
安装应用程序	否	否（iOS 13 中的新增功能）	是
允许在漫游时执行全局后台获取	否	是	是
允许使用应用程序			
iTunes Store	否	否（iOS 13 中的新增功能）	是
应用内购买	否	是	是
所有购买均需使用 iTunes 密码	否	是	是
Safari	否	否（iOS 13 中的新增功能）	是
自动填充	否	否（iOS 13 中的新增功能）	是
强制显示欺诈警告	是	是	是
启用 JavaScript	否	是	是
阻止弹出窗口	否	是	是
接受 Cookie	否	是	是
网络 - 允许执行 **iCloud** 操作			

设置	用户注册	不受监督	受监督
iCloud 文档和数据	否	否（iOS 13 中的新增功能）	是
iCloud 备份	否	是	是
iCloud 照片钥匙链	否	是	是
iCloud 照片库	否	是	是
安全 - 强制			
加密备份	是	是	是
有限广告跟踪	否	是	是
首次 AirPlay 配对时输入通行码	是	是	是
需要配对的 Apple Watch 才能使用腕部监测	是	是	是
使用 AirDrop 共享托管文档	是	是	是
安全 - 允许			
接受不可信 SSL 证书	否	是	是
自动更新证书信任设置	否	是	是
在非托管应用程序中使用托管应用程序的文档	是	是	是
非托管应用程序读取托管联系人	否	否	是
托管应用程序写入非托管联系人	否	否	是
在托管应用程序中使用非托管应用程序的文档	是	是	是
诊断结果提交到 Apple	是	是	是
通过 Touch ID 解锁设备	否	是	是
锁定时接收 Passbook 通知	否	是	是
提交	否	是	是
托管应用程序的 iCloud 同步	是	是	是

设置	用户注册	不受监督	受监督
企业书籍备份	是	是	是
企业书籍的笔记和重点同步	是	是	是
Spotlight 中的 Internet 结果	否	是	是
企业应用程序信任	否	是	是
仅监管设置 - 允许			
擦除所有内容和设置	否	否	是
配置限制	否	否	是
播客	否	否	是
安装配置文件	否	否	是
修改指纹	否	否	是
从设备安装应用程序	否	否	是
键盘快捷方式	否	否	是
已配对 Apple Watch	否	否	是
修改通行码	否	否	是
修改设备名称	否	否	是
修改壁纸	否	否	是
自动下载应用程序	否	否	是
AirDrop	否	否	是
iMessage	否	否	是
Siri 用户生成的内容	否	否	是
iBooks	否	否	是
删除应用程序	否	是	是
游戏中心	否	否（iOS 13 中的新增功能）	是
添加好友	否	否	是
多人游戏	否	否（iOS 13 中的新增功能）	是
修改帐户设置	否	否	是

设置	用户注册	不受监督	受监督
修改应用程序手机网络数据设置	否	否	是
修改应用程序手机网络数据设置	否	否	是
修改“查找我的好友”设置	否	否	是
与非 Configurator 主机配对	否	否	是
预测键盘	否	否	是
键盘自动更正	否	否	是
键盘拼写检查	否	否	是
定义查找	否	否	是
单应用程序捆绑 **ID**			
新闻	否	否	是
Apple 音乐服务	否	否	是
iTunes 电台	否	否	是
通知修改	否	否	是
受限应用程序使用	否	否	是
诊断提交修改	否	否	是
蓝牙修改	否	否	是
允许听写	否	否	是
仅加入通过 Wi-Fi 策略安装的 Wi-Fi 网络	否	否	是
允许“课堂”应用程序运行 AirPlay 和查看屏幕而不提示	否	否	是
允许“课堂”应用程序锁定到应用程序以及锁定设备而不提示	否	否	是
自动加入“课堂”应用程序课程而不提示	否	否	是
允许 AirPrint	否	否	是

设置	用户注册	不受监督	受监督
允许在钥匙串中存储 AirPrint 凭据	否	否	是
允许使用 iBeacon 发现 AirPrint 打印机	否	否	是
仅允许通过 AirPrint 打印到证书受信任的目标打印机	否	否	是
添加 VPN 配置	否	否	是
修改手机网络套餐设置	否	否	是
删除系统应用程序	否	否	是
设置新的附近的设备	否	否	是
允许 USB 受限模式	否	否	是
强制执行延迟的软件更新	否	否	是
强制执行的软件更新延迟	否	否	是
强制课堂申请离开课程的权限	否	否	是
强制自动填写日期和时间	否	否	是
密码自动填充	否	否	是
密码邻近请求	否	否	是
密码共享	否	否	是
安全 - 在锁屏界面中显示			
控制中心	是	是	是
通知	是	是	是
“今天” 视图	是	是	是
媒体内容 - 允许			
成人音乐、博客及 iTunes U 资料	否	否（iOS 13 中的新增功能）	是
iBooks 中暴露的性内容	否	是	是
评级地区	否	是	是
电影	否	是	是

设置	用户注册	不受监督	受监督
电视节目	否	是	是
应用程序	否	是	是

- 允许硬件控制
  - 相机：允许用户在其设备上使用相机。
    - **FaceTime**：允许用户在其设备上使用 FaceTime。适用于受监督的 iOS 设备。
  - 屏幕截图：允许用户在其设备上截取屏幕截图。
    - 允许 **“课堂”** 应用程序远程观察学生的屏幕：如果未选中此限制，教师将无法使用“课堂”应用程序远程观察学生的屏幕。默认设置为选中，教师可以使用“课堂”应用程序观察学生的屏幕。允许 **“课堂”** 应用程序运行 **AirPlay** 和查看屏幕而不提示的设置确定学生是否接收向教师授予权限的提示。适用于受监督的 iOS 设备。
    - 允许 **“课堂”** 应用程序运行 **AirPlay** 和查看屏幕而不提示：如果选中此限制，教师可以在学生的设备上执行 AirPlay 和查看屏幕操作，而不提示授予权限。默认设置为未选中。适用于受监督的 iOS 设备。
  - 照片流：允许用户使用 MyPhotoStream 通过 iCloud 与其所有 iOS 设备共享照片。
  - 共享照片流：允许用户使用 iCloud Photo Sharing 与同事、朋友和家人共享照片。
  - 语音拨号：在用户设备上启用拨号。
  - **Siri**：允许用户使用 Siri。
    - 设备锁定时允许：允许用户在其设备锁定时使用 Siri。
    - **Siri** 猥亵语言过滤：启用 Siri 猥亵语言过滤。默认为限制此功能，也就是说不会进行猥亵语言过滤。有关 Siri 和安全性的详细信息，请参阅 Siri 和听写策略。
  - 安装应用程序：允许用户安装应用程序。适用于受监督的 iOS 设备。
  - 允许在漫游时执行全局后台获取：允许设备在漫游时自动向 iCloud 同步邮件帐户。设置为关时，在 iOS 手机漫游时将禁用全局后台获取活动。默认值为开。
- 允许使用应用程序
  - **iTunes Store**：允许用户访问 iTunes Store。适用于受监督的 iOS 设备。
  - 应用程序内购买：允许用户进行应用程序内购买。
    - 所有购买均需使用 **iTunes** 密码：需要密码才能进行应用程序内购买。默认为限制此功能，也就是说进行应用程序内购买无需密码。
  - **Safari**：允许用户访问 Safari。适用于受监督的 iOS 设备。
    - 自动填充：允许用户在 Safari 上设置用户名和密码自动填充功能。
    - 强制显示欺诈警告：如果启用此设置，则当用户访问可疑网络钓鱼 Web 站点时，Safari 会向用户发出警报。默认为限制此功能，也就是说不会发出警报。
    - 启用 **JavaScript**：允许在 Safari 上运行 JavaScript。
    - 阻止弹出窗口：查看 Web 站点时阻止弹出窗口。默认为限制此功能，也就是说不阻止弹出窗口。
  - 接受 **Cookie**：设置为接受 Cookie 的程度。在列表中，选择某个选项以允许或限制 Cookie。默认选项

为总是，即允许所有 Web 站点在 Safari 中保存 Cookie。其他选项为仅限当前 **Web** 站点、从不和仅来自访问的 **Web** 站点。

- 网络 **-** 允许执行 **iCloud** 操作
  - **iCloud** 文档和数据：允许用户将文档和数据同步到 iCloud。适用于受监督的 iOS 设备。
  - **iCloud** 备份：允许用户向 iCloud 备份其设备。
  - **iCloud** 钥匙串：允许用户在 iCloud 钥匙串中存储密码、Wi-Fi 网络信息、信用卡信息以及其他信息。
  - 云照片库：允许用户访问其 iCloud 照片库。
- 安全 **-** 强制

  默认为限制以下功能，即不启用任何安全功能。
  - 加密备份：强制加密到 iCloud 的备份。
  - 有限广告跟踪：阻止有针对性的广告跟踪。
  - 首次 **AirPlay** 配对时输入通行码：需要使用屏幕上显示的一次性代码验证已启用 AirPlay 的设备才可以使用 AirPlay。
  - 需要配对的 **Apple Watch** 才能使用腕部监测：需要配对的 Apple Watch 才能使用腕部监测。
  - 使用 **AirDrop** 共享托管文档：将此选项设置为开会使 AirDrop 显示为非托管放置目标。
- 安全 **-** 允许
  - 接受不可信 **SSL** 证书：允许用户接受 Web 站点的不可信 SSL 证书。
  - 自动更新证书信任设置：允许自动更新可信证书。
  - 在非托管应用程序中使用托管应用程序中的文档：允许用户将托管（企业）应用程序中的数据移动到非托管（私人）应用程序。
  - 在托管应用程序中使用非托管应用程序中的文档：允许用户将非托管（私人）应用程序中的数据移动到托管（企业）应用程序。
  - 将诊断结果提交给 **Apple**：允许将有关用户设备的匿名诊断数据发送给 Apple。
  - 通过 **Touch ID** 解锁设备：允许用户使用其指纹解锁其设备。
  - 锁定时接收 **Passbook** 通知：允许 Passbook 通知显示在锁屏界面上。
  - **Handoff**：允许用户从一台 iOS 设备向附近的另一台 iOS 设备转移活动。
  - 托管应用程序的 **iCloud** 同步：允许用户向 iCloud 同步托管应用程序。
  - 企业通讯簿备份：允许将企业通讯簿备份到 iCloud。
  - 企业书籍的笔记和重点同步：允许用户添加到企业书籍的笔记和重点同步到 iCloud。
  - 企业应用程序信任：允许信任企业应用程序。企业应用程序是指为贵组织自定义的任何应用程序。这些产品可以在内部开发，也可以从外部供应商处开发并购买。有关其他信息，请参阅 Install custom enterprise apps on iOS（在 iOS 上安装自定企业级应用）。
  - **Spotlight** 中的 **Internet** 结果：允许 Spotlight 显示来自 Internet 以及设备的搜索结果。
  - 非托管应用程序读取托管联系人：可选。仅当非托管应用程序中来自托管应用程序的文档处于禁用状态时才可用。如果启用，则非托管应用程序可以读取托管帐户的联系人数据。默认值为关。截至 iOS 12 适用。
  - 托管应用程序写入非托管联系人：可选。如果启用，则允许托管应用程序将联系人写入非托管帐户的联系人。如果非托管应用程序中来自托管应用程序的文档处于启用状态，则此限制无效。默认值为关。截至

iOS 12 适用。

- 仅监管设置 - 允许

  这些设置仅适用于受监管设备。有关将 iOS 设备置于受监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

  - 擦除所有内容和设置：允许用户擦除其设备中的所有内容和设置。
  - 配置限制：允许用户在其设备上配置家长控制。
  - 播客：允许用户下载和同步播客。
  - 安装配置文件：允许用户安装并非由您部署的配置文件。
  - 修改指纹：允许用户更改或删除其 Touch ID 指纹。
  - 从设备安装应用程序：允许用户安装应用程序。禁用此设置将阻止最终用户安装新应用程序。App Store 处于禁用状态，其图标将从主屏幕中删除。
  - 键盘快捷方式：允许用户为其常用的字词或短语创建自定义键盘快捷方式。
  - 配对的 **Apple Watch**：允许用户将 Apple Watch 与受监督的设备配对。
  - 修改通行码：允许用户在受监督的设备上更改通行码。
  - 修改设备名称：允许用户更改其设备的名称。
  - 修改壁纸：允许用户在更改其设备上的壁纸。
  - 自动下载应用程序：允许下载应用程序。
  - **AirDrop**：允许用户与附近的 iOS 设备共享照片、视频、Web 站点、位置及其他信息。
  - **iMessage**：允许用户使用 iMessage 通过 Wi-Fi 传递文本消息。
  - **Siri** 用户生成的内容：允许 Siri 从 Web 查询用户生成的内容。用户，而非传统新闻记者；生成用户生成的内容。例如，在 Twitter 或 Facebook 上找到的内容是用户生成的。
  - **iBooks**：允许用户使用 iBooks 应用程序。
  - 删除应用程序：允许用户从其设备中删除应用程序。
  - 游戏中心：允许用户在其设备上通过游戏中心在线玩游戏。
    - 添加好友：允许用户向好友发送玩游戏通知。
    - 多人游戏：允许用户在其设备上启动多人游戏。
  - 修改帐户设置：允许用户修改其设备帐户设置。
  - 修改应用程序手机网络数据设置：允许用户修改使用手机网络数据的方式。
  - 修改 **“查找我的好友”** 设置：允许用户更改其“查找我的好友”设置。
  - 与非 **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。禁用此设置将阻止配对，与运行 Apple Configurator 的监督主机配对除外。如果未配置任何监督主机证书，将禁用所有配对。

- 预测键盘：允许用户设备使用预测键盘，在用户键入时提供建议单词。如果要管理标准化测试，不允许用户访问建议的单词，在此类情况下可以禁用此选项。
- 键盘自动更正：允许用户设备使用键盘自动更正。如果要管理标准化测试，不允许用户访问自动更正，在此类情况下可以禁用此选项。
- 键盘拼写检查：在键入时允许用户设备使用拼写检查。如果要管理标准化测试，不允许用户访问拼写检查，在此类情况下可以禁用此选项。
- 定义查找：在键入时允许用户设备使用定义查找。如果要管理标准化测试，不允许用户在键入时查找定义，在此类情况下可以禁用此选项。
- 单应用程序捆绑包 **ID**：创建允许保留设备的控制权并阻止与其他应用程序或功能进行交互的应用程序的列表。
  要添加应用程序，请单击添加，键入应用程序名称，然后单击保存。对要添加的每个应用程序重复该过程。
- 新闻：允许用户使用新闻应用程序。
- **Apple** 音乐服务：允许用户使用 Apple 音乐服务。如果您不允许使用 Apple 音乐服务，则音乐应用程序以经典模式运行。
- **iTunes Radio**：允许用户使用 iTunes Radio。
- 修改通知：允许用户修改通知设置。
- 受限应用程序使用：允许用户使用所有应用程序或者使用或不使用某些应用程序，具体取决于您提供的捆绑包 ID。仅适用于受监督的设备。如果选择仅允许某些应用程序，请添加捆绑包 ID 为 `com.apple.webapp` 的应用程序以允许 Web 剪辑。

  > 注意：
  >
  > 自 iOS 11 起，Apple 引入了对适用于应用程序限制的策略所做的更改。Apple 不再允许您通过限制适当的 iOS 应用程序包来删除对“设置”应用程序和“电话”应用程序的访问权限。

  配置限制设备策略以阻止某些应用程序，然后部署了该策略之后：如果以后要允许这些应用程序中的一些或全部，更改并部署限制设备策略不会更改显示。在这种情况下，iOS 不会将更改应用于 iOS 配置文件。要继续操作，请使用配置文件删除策略删除 iOS 配置文件，然后部署更新的限制设备策略。

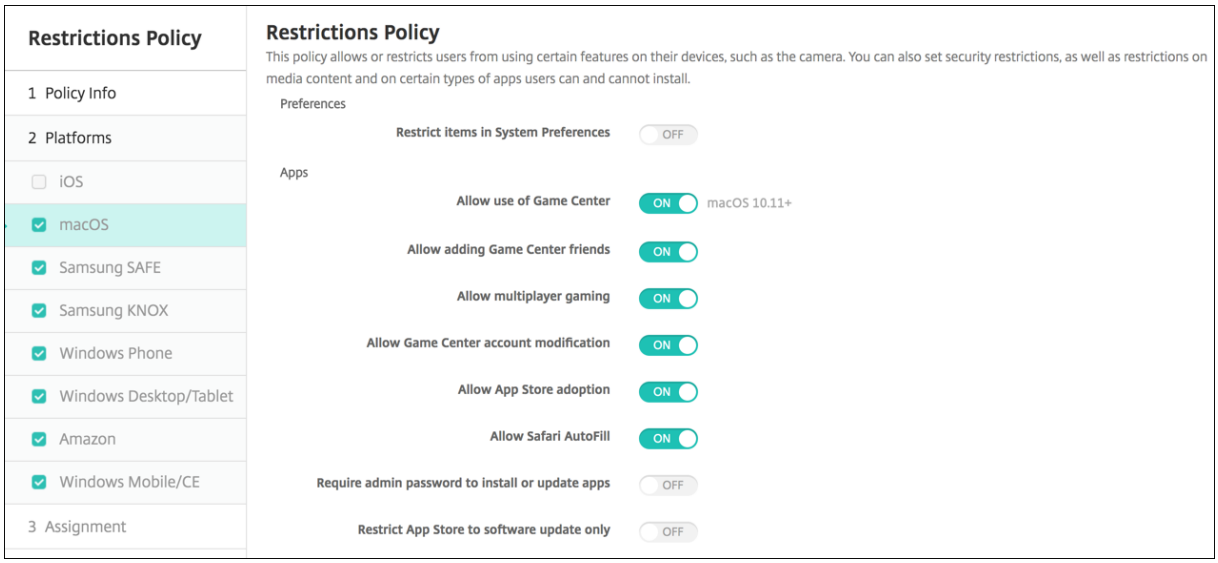
  如果将此设置更改为仅允许某些应用程序：部署此策略之前，建议使用 Apple 部署计划注册的设备的用户从设置助理登录其 Apple 帐户。否则，用户可能必须在其设备上禁用双重身份验证，才能登录其 Apple 帐户并访问允许的应用程序。
- 修改诊断提交：允许用户在设置 **> Diagnostics & Usage**（诊断和使用）窗格中修改诊断提交和应用程序分析设置。
- 修改蓝牙：允许用户修改蓝牙设置。
- 允许听写：仅在监督下使用。如果此限制设置为关，则不允许听写输入，包括语音转换为文本。默认设置为开。

- 仅加入通过 **WiFi** 策略安装的 **WiFi** 网络：可选。仅在监督下使用。如果此限制设置为开，则仅在 Wi-Fi 网络是通过配置文件设置的情况下设备才能加入这些网络。默认设置为关。
- 允许 **"**课堂**"** 应用程序运行 **AirPlay** 和查看屏幕而不提示：如果选中此限制，教师可以在学生的设备上执行 AirPlay 和查看屏幕操作，而不提示授予权限。默认设置为未选中。适用于受监督的 iOS 设备。
- 允许 **"**课堂**"** 应用程序锁定到应用程序以及锁定设备而不提示：如果此限制设置为开，"课堂" 应用程序会自动将用户设备锁定到某个应用程序并锁定设备，而不提示用户。默认设置为关。适用于运行 iOS 11（最低版本）的受监督设备。
- 自动加入 **"**课堂**"** 应用程序课程而不提示：如果此限制设置为开，"课堂" 应用程序会自动将用户加入到课程中，而不提示用户。默认设置为关。适用于运行 iOS 11（最低版本）的受监督设备。
- 允许 **AirPrint**：如果此限制设置为关，用户将无法通过 AirPrint 打印。默认设置为开。此限制设置为开时，将显示这些额外的限制。适用于运行 iOS 11（最低版本）的受监督设备。
  - 允许在钥匙串中存储 **AirPrint** 凭据：如果未选中此限制，AirPrint 用户名和密码将不存储在钥匙串中。默认设置为选中。适用于运行 iOS 11（最低版本）的受监督设备。
  - 允许使用 **iBeacon** 发现 **AirPrint** 打印机：如果未选中此限制，则禁止 iBeacon 发现 AirPrint 打印机。这将阻止虚假 AirPrint 蓝牙信标对网络流量进行网络钓鱼。默认设置为选中。适用于运行 iOS 11（最低版本）的受监督设备。
  - 仅允许通过 **AirPrint** 打印到证书受信任的目标打印机：如果选中此限制，用户可以使用 AirPrint 仅打印到证书受信任的目标打印机。默认设置为未选中。适用于运行 iOS 11（最低版本）的受监督设备。
- 添加 **VPN** 配置：如果此限制设置为关，用户将无法创建 VPN 配置。默认设置为开。适用于运行 iOS 11（最低版本）的受监督设备。
- 修改手机网络套餐设置：如果此限制设置为关，用户将无法修改手机网络套餐设置。默认设置为开。适用于运行 iOS 11（最低版本）的受监督设备。
- 删除系统应用程序：如果此限制设置为关，用户将无法从其设备中删除系统应用程序。默认设置为开。适用于运行 iOS 11（最低版本）的受监督设备。
- 设置新的附近的设备：如果此限制设置为 "关"，用户将无法设置新的附近的设备。默认设置为开。适用于运行 iOS 11（最低版本）的受监督设备。
- 允许 **USB** 受限模式：如果设置为关，设备在锁定状态下可以始终连接到 USB 附属设施。默认值为开。仅适用于 iOS 11.3 及更高版本的受监督设备。
- 强制执行延迟的软件更新：如果设置为开，则延迟软件更新对用户的可见性。设置此限制后，用户在软件更新发布日期后的指定天数之后才能看到软件更新。默认值为关。仅适用于 iOS 11.3 及更高版本的受监督设备。
- 强制执行的软件更新延迟 **(**天**)**：允许您指定在设备上延迟软件更新的天数。最长延迟时间为 **90** 天。默认值为 **30** 天。仅适用于 iOS 11.3 及更高版本的受监督设备。
- 强制课堂申请离开课程的权限：如果设置为开，通过 "课堂" 应用程序在非托管课程中注册的学生在尝试离开课程时将向教师申请权限。默认值为关。仅适用于 iOS 11.3 及更高版本的受监督设备。

- 强制自动填写日期和时间：允许您在受监督设备上自动设置日期和时间。如果设置为开，设备用户将无法在常规 **>** 日期和时间下关闭自动设置。仅当设备可以确定其位置时，设备上的时区才会更新。也就是说，当设备启用了手机网络连接或启用了带定位服务的 Wi-Fi 连接时。默认值为关。仅适用于 iOS 12 及更高版本的受监督设备。
- 密码自动填充：可选。如果禁用，用户将无法使用“自动填充密码”或“自动使用强密码”功能。默认值为开。截至 iOS 12 适用。
- 密码邻近请求：可选。如果禁用，用户的设备将不从附近的设备请求密码。默认值为开。截至 iOS 12 适用。
- 密码共享：可选。如果禁用，用户将无法使用“AirDrop 密码”功能共享其密码。默认值为开。截至 iOS 12 适用。

- 安全 **-** 在锁屏界面中显示
  - 控制中心：允许访问锁屏界面上的控制中心。控制中心允许用户轻松修改飞行模式、Wi-Fi、蓝牙、请勿打扰模式和锁定旋转设置。
  - 通知：允许在锁屏界面上显示通知。
  - **“**今天**”** 视图：允许在锁屏界面上显示“今天”视图，此视图汇总了天气及当天的日历项目等信息。
- 媒体内容 **-** 允许
  - 成人音乐、博客及 **iTunes U** 资料：允许用户设备上出现成人资料。
  - **iBooks** 中暴露的性内容：允许从 iBooks 下载成人资料。
  - 评分地区：设置从其获得家长控制评分的地区。在列表中，单击某个国家/地区以设置评分地区。默认值为美国。
  - 电影：设置是否允许在用户设备上播放电影。如果允许播放电影，可以选择为电影设置评分级别。在列表中，单击某个选项以允许或限制在设备上播放电影。默认值为“允许所有电影”。
  - 电视节目：设置是否允许在用户设备上播放电视节目。如果允许播放电视节目，可以选择为电视节目设置评分级别。在列表中，单击某个选项以允许或限制在设备上播放电视节目。默认值为“允许所有电视节目”。
  - 应用程序：设置是否允许在用户设备上使用应用程序。如果允许使用应用程序，可以选择为应用程序设置评分级别。在列表中，单击某个选项以允许或限制在设备上使用应用程序。默认值为“允许所有应用程序”。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅适用于 iOS 9.3 及更高版本。

macOS 设置



- 首选项
  - 限制系统首选项中的项目：允许或限制用户访问系统首选项。默认值为关，表示完全允许用户访问系统首选项。如果启用，可以配置以下设置。
    - 系统首选项窗格：选择是启用还是禁用选择的设置。默认为启用所有设置，即默认情况下为开。
      - 用户和组
      - 常规
      - 辅助工具
      - App Store
      - 软件更新
      - 蓝牙
      - CD 和 DVD
      - 日期和时间
      - 桌面和屏幕保护程序
      - 显示
      - 基站
      - 节能程序
      - 扩展
      - 光纤通道
      - iCloud
      - Ink
      - Internet 帐户
      - 键盘
      - 语言和文字
      - Mission Control
      - 鼠标

- 网络
- 通知
- 家长控制
- 打印机和扫描仪
- 配置文件
- 安全和隐私
- 共享
- 声音
- 用词和语音
- Spotlight
- 启动磁盘
- Time Machine
- 触控板
- Xsan

- 应用程序
  - 允许使用游戏中心：允许用户通过游戏中心在线玩游戏。默认值为开。
  - 允许添加游戏中心好友：允许用户向好友发送玩游戏通知。默认值为开。
  - 允许多人游戏：允许用户发起多人游戏。默认值为开。
  - 允许修改游戏中心帐户：允许用户修改其游戏中心帐户设置。默认值为开。
  - 允许应用商店采用：允许或限制应用商店采用 OS X 中预先存在的应用程序。默认设置为开。
  - 允许 **Safari** 自动填充：允许 Safari 自动使用其存储的密码、地址和其他基本信息填充 Web 站点上的字段。默认值为开。
  - 需要提供管理员密码才能安装或更新应用程序：需要提供管理员密码才能安装或更新应用程序。默认值为关，表示无需提供管理员密码。
  - 将应用商店限制为仅提供软件更新：将应用商店限制为仅提供更新，这样会在应用商店中禁用除“更新”之外的所有选项卡。默认值为关，即允许完整的应用商店访问。
  - 限制允许打开的应用程序：限制或允许用户可以使用的应用程序。默认值为“关”，表示所有应用程序均可以使用。如果启用，请配置以下设置：
    * 允许运行的应用程序：单击添加，输入允许启动的应用程序的名称和捆绑包 ID，然后单击保存。为允许启动的每个应用程序重复此步骤。
    * 不允许使用的文件夹：单击添加，键入限制用户访问的文件夹的文件路径（例如，/Applications/Utilities），然后单击保存。为不希望用户访问的所有文件夹重复此步骤。
    * 允许使用的文件夹：单击添加，键入要允许用户访问的文件夹的文件路径，然后单击保存。为希望用户可以访问的所有文件夹重复此步骤。
- 小组件
  - 仅允许运行以下控制板小组件：允许或限制用户可以运行的控制板小组件，如世界时钟或计算器。默认值为关，表示允许用户运行所有小组件。如果启用，可以配置以下设置：
    * 允许运行的小组件：单击添加，键入允许运行的小组件的名称和 ID，然后单击保存。为希望在控制板上运行的每个小组件重复执行此步骤。

- 媒体
  - 允许 **AirDrop**：允许用户与附近的 iOS 设备共享照片、视频、Web 站点、位置及其他信息。
- 共享
  - 自动启用新共享服务：选择是否自动启用共享服务。
  - 邮件：选择是否允许使用共享的邮箱。
  - **Facebook**：选择是否允许使用共享的 Facebook 帐户。
  - 视频服务 **- Flickr**、**Vimeo**、**Tudou** 和 **Youku**：选择是否允许使用共享的视频服务。
  - 添加到 **Aperture**：选择是否允许将共享功能添加到 Aperture。
  - 新浪微博：选择是否允许使用共享的新浪微博微博客帐户。
  - **Twitter**：选择是否允许使用共享的 Twitter 帐户。
  - 消息：选择是否允许对消息进行共享访问。
  - 添加到 **iPhoto**：选择是否允许将共享功能添加到 iPhoto。
  - 添加到阅读列表：选择是否允许将共享功能添加到阅读列表。
  - **AirDrop**：选择是否允许使用共享的 AirDrop 帐户。
- 功能
  - 锁定桌面图片：选择用户是否可以更改桌面图片。默认值为关，表示用户可以更改桌面图片。
  - 允许使用相机：选择用户是否可以在其 Mac 上使用相机。默认值为关，表示用户无法使用相机。
  - 允许 **Apple** 音乐：允许用户使用 Apple 音乐服务（macOS 10.12 及更高版本）。如果您不允许使用 Apple 音乐服务，则音乐应用程序以经典模式运行。仅适用于受监督的设备。默认值为开。
  - 允许 **Spotlight** 推荐：选择用户是否可以使用 Spotlight 推荐搜索其 Mac 并提供来自 Internet、iTunes 和 App Store 的 Spotlight 推荐。默认值为关，表示阻止用户使用 Spotlight 推荐。
  - 允许查找：选择用户是否可以使用上下文菜单或 Spotlight 搜索菜单查找字词的定义。默认值为“关”，表示阻止用户在其 Mac 上使用查找。
  - 允许使用本地帐户的 **iCloud** 密码：选择用户是否可以使用其 Apple ID 和 iCloud 密码登录其 Mac。启用此策略意味着用户对其 Mac 上的所有登录屏幕仅使用一个 ID 和密码。默认值为开，表示允许用户使用其 Apple ID 和 iCloud 密码访问其 Mac。
  - 允许使用 **iCloud** 文档和数据：选择是否允许用户在其 Mac 上访问存储在 iCloud 上的文档和数据。默认值为关，表示阻止用户在其 Mac 上使用 iCloud 文档和数据。
    - 允许 **iCloud** 桌面和文档：（macOS 10.12.4 及更高版本）默认选中。
  - 允许 **iCloud** 钥匙串同步：允许 iCloud 钥匙串同步（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 邮件：允许用户使用 iCloud 邮件（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 通讯录：允许用户使用 iCloud 通讯录（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 日历：允许用户使用 iCloud 日历（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 提醒事项：允许用户使用 iCloud 提醒事项（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 书签：允许用户与 iCloud 书签同步（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 备忘录：允许用户使用 iCloud 备忘录（macOS 10.12 及更高版本）。默认值为开。
  - 允许 **iCloud** 照片：如果将此设置更改为关，未完全从 iCloud 照片库中下载的所有照片都将从本地设备存储中删除（macOS 10.12 及更高版本）。默认值为开。
  - 允许自动解锁：有关此选项及 Apple Watch 的信息，请参阅 https://www.imore.com/auto-unlock

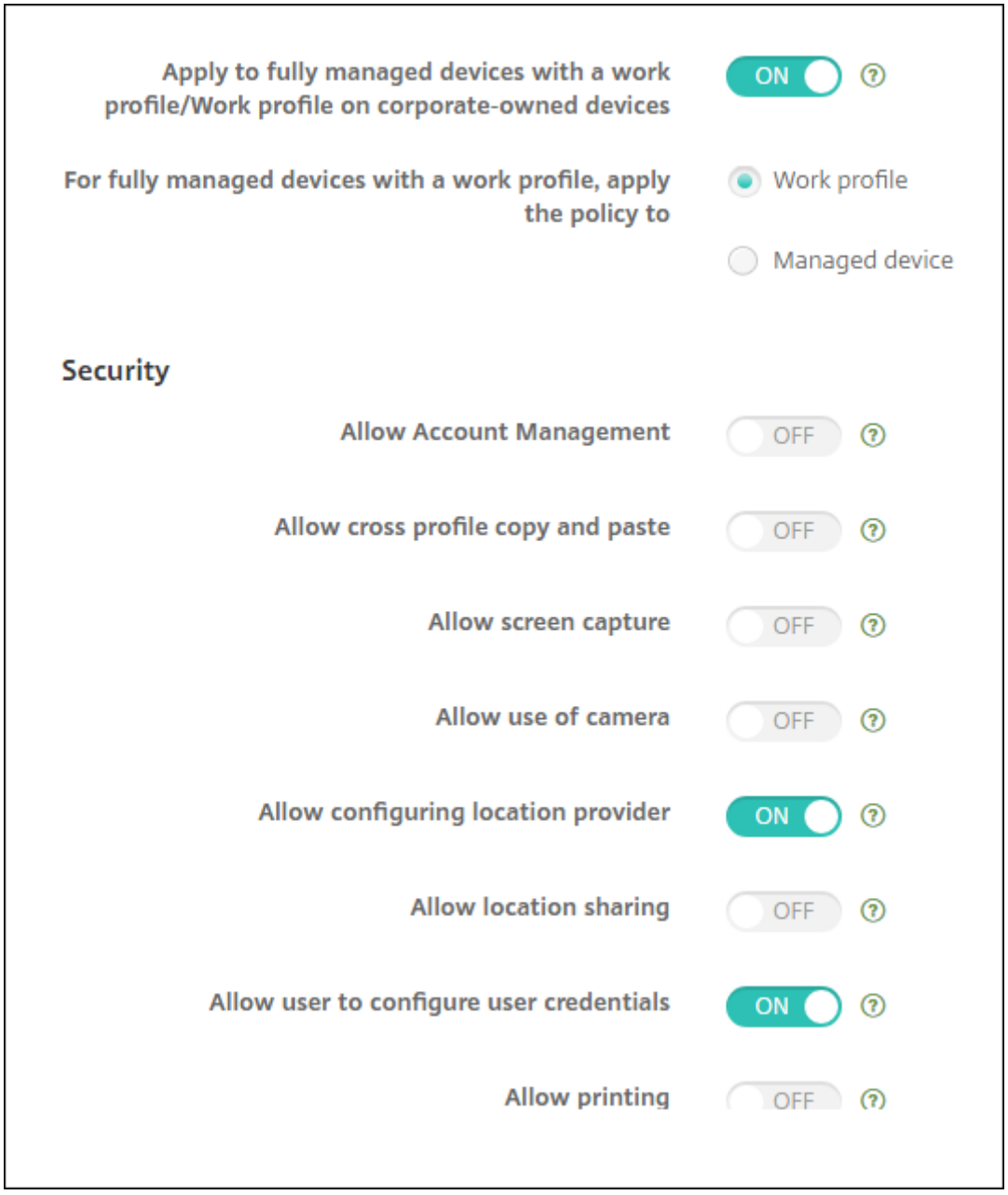
（macOS 10.12 及更高版本）。默认值为开。

- 允许 **Touch ID** 解锁 **Mac**：（macOS 10.12.4 及更高版本）。默认值为开。
- 强制执行延迟的软件更新：如果设置为开，此设置将延迟软件更新对用户的可见性。用户在软件更新发布日期后的指定天数之后才能看到软件更新。默认值为关。仅适用于运行 macOS 10.13.4 及更高版本的受监督设备。
- 强制执行的软件更新延迟 **(**天**)**：指定在设备上延迟软件更新的天数。最大值为 90 天。默认值为 **30**。仅适用于运行 macOS 10.13.4 及更高版本的受监督设备。
- 密码自动填充：可选。如果禁用，用户将无法使用“自动填充密码”或“自动使用强密码”功能。默认值为开。截至 macOS 10.14 可用。
- 密码邻近请求：可选。如果禁用，用户的设备将不从附近的设备请求密码。默认值为开。截至 macOS 10.14 可用。
- 密码共享：可选。如果禁用，用户将无法使用“Airdrop 密码”功能共享其密码。默认值为开。截至 macOS 10.14 可用。

Android 设置

- 相机：允许用户在其设备上使用相机。如果设置为关，则将禁用相机。默认值为开。

Android Enterprise 设置



当新的或已恢复出厂设置的 Android 设备在工作配置文件模式下注册时，运行 Android 8.0-10.x 的设备会注册为具有工作配置文件的完全托管设备。运行 Android 11+ 的设备将注册为企业拥有的设备上的工作配置文件。限制策略可以应用到设备上的工作配置文件，也可以应用到托管设备。

在企业拥有的设备上的工作配置文件模式下注册的设备上，以下限制仅适用于工作配置文件：

- 允许备份服务
- 启用系统应用程序
- 保持键盘锁不锁定设备

- 允许使用状态栏
- 保持设备屏幕处于打开状态
- 允许用户控制应用程序设置
- 允许用户配置用户凭据
- 允许 VPN 配置
- 允许 USB 大容量存储
- 允许恢复出厂设置
- 允许卸载应用程序
- 允许使用非 Google Play 应用程序
- 允许跨配置文件复制和粘贴
- 启用应用程序验证
- 允许帐户管理
- 允许打印
- 允许使用 NFC
- 允许添加用户

默认情况下，如果某个设备是在工作配置文件模式下在 Android Enterprise 中注册的，**USB** 调试和未知来源设置在该设备上将处于禁用状态。

对于运行 Android 8.0-10.x 和 Samsung Knox 3.0 及更高版本的设备，请在 **Android Enterprise** 页面上为 Samsung Knox 和 Samsung SAFE 配置设置。对于运行早期版本的 Android 或 Samsung Knox 的设备，请使用 **Samsung Knox** 和 **Samsung SAFE** 页面。

Samsung 限制不会应用到在企业拥有的设备上的工作配置文件模式下注册的设备。使用 Knox 服务插件 (KSP) 将 Samsung 限制应用到这些设备。有关详细信息，请参阅 Samsung 文档。

建议您使用 Samsung Knox 3.4 或更高版本来获得最新的 Samsung Knox 管理功能。

- 应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备：允许为具有工作配置文件的完全托管设备配置凭据策略设置。当此设置设为开时，选择以下设置之一：
  - 工作配置文件：您配置的限制设置仅适用于设备上的工作配置文件。
  - 管理设备：您配置的限制设置仅适用于设备。

  当此设置设为关时，您配置的凭据设置将应用到设备，但明确应用于工作配置文件的设置除外。默认值为关。

当应用到具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备处于关闭状态时，请配置以下设置：

- 安全性
  - 允许帐户管理：允许在工作配置文件和托管设备中向帐户中添加对象。默认值为关。
  - 允许跨配置文件复制粘贴：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执行复制和粘贴操作。默认值为关。
  - 允许屏幕捕获：允许用户记录或捕获设备屏幕的屏幕拍图。默认值为关。
  - 允许使用相机：允许用户使用设备摄像头拍照并制作视频。默认值为关。

- 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以及完全托管设备。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。
- 允许使用 **NFC**：允许用户使用近场通信 (NFC) 从其设备向其他设备发送 Web 页面、照片、视频或其他内容。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：
  >
  > 可以在 XenMobile 中创建定位设备策略以强制实施地理边界。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：如果为开，则此设置允许用户打印到任何可通过用户设备访问的打印机。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，请单击系统应用程序列表表中的添加。
    - 系统应用程序列表：要在设备上启用的系统应用程序的列表。将启用系统应用程序设置为开并添加应用程序包名称。要查找系统应用程序的软件包名称，可以使用 Android Debug Bridge (adb) 调用 Android 软件包管理器 (pm) 命令。例如，`adb shell "pm list packages -f name"`，其中 “name” 为软件包名称的一部分。有关详细信息，请参阅 https://developer.android.com/studio/command-line/adb。对于 Android Enterprise 设备，可以使用 Android Enterprise 应用程序权限策略限制应用程序权限。
  - 禁用应用程序：阻止列出的指定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，请将该设置更改为开，然后单击应用程序列表表中的添加。
    - 应用程序列表：要阻止的应用程序的列表。请将禁用应用程序设置为开并添加应用程序。请键入应用程序软件包名称。更改和部署某个应用程序列表将覆盖之前的应用程序列表。例如：如果禁用了 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，XenMobile 将启用 com.example.2。
  - 启用应用程序验证：允许操作系统扫描应用程序以检测恶意行为。默认值为开。
  - 启用 **Google** 应用程序：允许用户将 Google Mobile Services 中的应用程序下载到设备中。默认值为开。
  - 允许使用非 **Google Play** 应用程序：允许从 Google Play 之外的应用商店安装应用程序。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。用户将从 “设置” 应用程序执行这些操作。默认值为关。

- 允许卸载应用程序：允许用户从托管的 Google Play Store 中卸载应用程序。默认值为关。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的详细信息，请参阅服务器属性。

- **BYOD** 工作配置文件
  - 允许在主屏幕上显示工作配置文件应用程序小组件：如果此设置设为开，则用户可以将工作配置文件应用程序小组件放置在设备主屏幕上。如果此设置设为关，则用户无法将工作配置文件应用程序小组件放置在设备主屏幕上。默认值为关。
    - **Apps with allowed widgets**（具有允许的小组件的应用程序）：要允许显示在主屏幕上的应用程序的列表。将允许在主屏幕上显示工作配置文件应用程序小组件设置为开并添加应用程序。单击添加并从列表中选择希望允许在主屏幕上显示其小组件的应用程序。单击保存。重复该过程将允许更多应用程序小组件。
  - 允许在设备联系人中添加工作配置文件联系人：在家长配置文件中显示托管 Android Enterprise 配置文件中的联系人，以便接收传入呼叫（Android 7.0 及更高版本）。默认值为关。

- 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。默认值为开。
  - 允许数据漫游：允许用户在漫游时使用手机网络数据。默认值为“关”，即在用户设备上禁用漫游。默认值为关。
  - 允许短信：允许用户发送和接收短消息。默认值为关。
  - 允许使用状态栏：如果为开，此设置将在托管设备和专用设备（又称为 COSU 设备）上启用状态栏。此设置将禁用通知、快速设置以及其他促使退出全屏模式的屏幕叠加。用户可以转到系统设置并查看通知。适用于 Android 6.0 及更高版本。默认值为关。
  - 允许使用蓝牙：允许用户使用蓝牙。默认值为开。
    - 允许蓝牙共享：如果未选择，用户将无法在其设备上建立传出蓝牙共享。默认处于选中状态。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的详细信息，请参阅服务器属性。
  - 允许配置日期和时间：允许用户在其设备上更改日期和时间。默认值为开。
  - 允许恢复出厂设置：允许用户在其设备上恢复出厂设置。默认值为开。
  - 保持设备屏幕处于打开状态：如果此设置设为开，设备插入时设备屏幕保持打开状态。默认值为关。
  - 允许 **USB** 大容量存储：允许通过 USB 连接在用户的设备与计算机之间传输大型数据文件。默认值为开。
  - 允许使用麦克风：允许用户在其设备上使用麦克风。默认值为开。
  - 允许网络共享：允许用户配置便携式热点和网络共享数据。默认值为关。
  - 保持键盘锁不锁定设备：如果为开，此设置将在托管设备和专用设备（又称为 COSU 设备）上的锁屏界面上禁用键盘锁。默认值为关。
  - 允许更改 **Wi-Fi**：如果为开，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 进行文件传输。默认值为关。

- **Samsung**
  - 启用 **TIMA** 密钥库： TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书路由到默认密钥库提供商进行存储。默认值为关。

- 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。

- **Samsung:** 仅限完全托管设备
  - 启用 **ODE** 可信引导验证：使用 ODE 可信引导验证建立从引导加载程序到系统映像的信任链。默认值为开。
  - 仅允许紧急呼叫：允许用户在其设备上启用“仅限紧急呼叫”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：允许仅加密已使用的内存空间。此加密与完全磁盘加密（用于加密所有数据）完全不同。该数据包括设置、应用程序数据、已下载的文件和应用程序、媒体及其他文件。默认值为开。
  - 启用通用准则模式：将设备置于通用准则模式。通用准则配置强制执行严苛的安全流程。默认值为开。
  - 启用重新启动横幅：当用户的设备重新启动时，显示 DoD 批准的系统使用通知消息或横幅。默认值为关。
  - 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，适用于完全托管设备。默认值为开。
  - 允许使用剪贴板：允许用户在其设备上将数据复制到剪贴板。
    - 允许剪贴板共享：允许用户在其设备和某个计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。
  - 允许使用 **Home** 键：允许用户在其完全托管设备上使用 **Home** 键。默认值为开。
  - 允许模拟位置：允许用户伪造其 GPS 位置。适用于完全托管设备。默认值为关。
  - **NFC**：允许用户在其完全托管设备上使用 NFC（MDM 3.0 及更高版本）。默认值为开。
  - 允许关闭电源：允许用户关闭其完全托管设备（MDM 3.0 及更高版本）的电源。默认值为开。
  - 允许使用 **Wi-Fi Direct**：允许用户通过其 Wi-Fi 连接直接连接到其他设备。默认值为开。如果为开，则必须启用允许更改 **Wi-Fi** 设置。
  - 允许使用 **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，用户的设备为 USB 设备提供电源。默认值为开。
  - 允许使用语音拨号器：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 与其他人共享内容（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手和知识导航器（MDM 4.0 及更高版本）。默认值为开。
  - 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。默认值为关。如果为开，则允许网络共享设置也必须为开。
  - 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。默认值为关。如果为开，则允许网络共享设置也必须为开。
    - 允许蓝牙共享：如果未选择，用户将无法在其设备上建立传出蓝牙共享。默认处于选中状态。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的详细信息，请参阅服务器属性。
  - 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。默认值为关。如果为开，则允许网络共享设置也必须为开。
  - 允许传入 **MMS**：允许用户接收 MMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。

- 允许传出 **MMS**：允许用户发送 MMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。
- 允许传入 **SMS**：允许用户接收 SMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。
- 允许传出 **SMS**：允许用户发送 SMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。
- 配置移动网络：允许用户使用其手机网络数据连接。默认值为关。
- 按天限制 **(MB)**：输入移动数据用户每天可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按周限制 **(MB)**：输入移动数据用户每周可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按月限制 **(MB)**：输入移动数据用户每月可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 仅允许建立安全的 **VPN** 连接：允许用户仅使用安全连接（MDM 4.0 及更高版本）。默认值为开。
- 允许录制音频：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，则必须打开允许使用麦克风设置。
- 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，则必须打开允许使用相机设置。
- 允许漫游时推送消息：允许用户使用手机网络数据进行推送。默认值为关。如果为开，则必须启用允许数据漫游设置。
- 允许漫游时自动同步：允许用户使用手机网络数据进行同步。默认值为关。如果为开，则必须启用允许数据漫游设置。
- 允许漫游时语音通话：允许用户使用手机网络数据进行语音通话。默认值为关。如果为开，则必须启用允许数据漫游设置。

- **Samsung**：**Knox** 容器**/**完全托管设备
  - 启用吊销检查：启用对已吊销证书的检查。默认值为关。
- **Samsung**：仅限 **Knox** 容器
  - 将应用程序移至容器：允许用户在其设备上的 Knox 容器与个人区域之间移动应用程序。默认值为开。
  - 强制执行多重身份验证：用户必须使用指纹和另一种身份验证方法（密码或 PIN）才能打开设备。默认值为开。
  - 强制对容器执行身份验证：使用与用于解锁设备以打开 KNOX 容器的方法不同的身份验证方法。默认值为开。
  - 允许使用安全小键盘：强制用户在 Knox 容器内使用安全小键盘。默认值为开。
- **Samsung**：**DeX**
  - 启用 **Samsung DeX**：允许支持启用了 Knox 的设备在 Samsung DeX 模式下运行。需要 Samsung Knox 3.1（最低版本）。默认值为开。有关 Samsung DeX 设备要求和设置 Samsung DeX 的信息，请参阅 Samsung 开发人员文档。
    - **Allow Ethernet in DeX mode only**（仅允许在 DeX 模式下使用以太网）：允许在 Samsung DeX 模式下使用以太网。手机网络数据、Wi-Fi 和网络共享（Wi-Fi、蓝牙和 USB）在 DeX 模式下受到限制。默认处于未选中状态。
    - 上载 **Dex** 徽标图像：选择此设置可指定一个.png 图像，以用作 Samsung DeX 的图标。

    * **DeX screen timeout (seconds)**（DeX 屏幕超时 (秒)）：指定空闲时间（以秒为单位），超过此时间后，DeX 屏幕将关闭。要禁用超时，请键入 **0**。默认值为 **1200** 秒（20 分钟）。
    * 在 **Samsung DeX** 中添加应用程序快捷方式：指定应用程序包名称以将应用程序的快捷方式添加到 DeX。要查找应用程序软件包名称，请转到 Google Play 并选择该应用程序。URL 包括软件包名称：`https://play.google.com/store/apps/details?id=<package.name><!--NeedCopy-->`。
    * 删除 **Samsung DeX** 中的应用程序快捷方式：指定应用程序包名称以从 DeX 中删除快捷方式。转到 Google Play 查找应用程序软件包名称。
    * 在 **DeX** 中禁用的应用程序包：指定要从 Samsung DeX 模式中阻止的应用程序包的逗号分隔列表。例如：`"com.android.chrome", "com.google.android.gm"<!--NeedCopy-->`。

当应用到使用工作配置文件的完全托管设备设置为“开”且对于具有工作配置文件的完全托管设备，请将策略应用到设置为工作配置文件时，请配置以下设置：

- 安全性
    - 允许帐户管理：允许在工作配置文件和托管设备中向帐户中添加对象。默认值为关。
    - 允许跨配置文件复制粘贴：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执行复制和粘贴操作。默认值为关。
    - 允许屏幕捕获：允许用户记录或捕获设备屏幕的屏幕拍图。默认值为关。
    - 允许使用相机：允许用户使用设备摄像头拍照并制作视频。默认值为关。
    - 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：
      >
      > 可以在 XenMobile 中创建定位设备策略以强制实施地理边界。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：如果为开，则此设置允许用户打印到任何可通过用户设备访问的打印机。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，请单击系统应用程序列表表中的添加。
        * 系统应用程序列表：要在设备上启用的系统应用程序的列表。将启用系统应用程序设置为开并添加应用程序包名称。要查找系统应用程序的软件包名称，可以使用 Android Debug Bridge (adb) 调用 Android 软件包管理器 (pm) 命令。例如，`adb shell "pm list packages -f name"`，其中 “name” 为软件包名称的一部分。有关详细信息，请参阅 https://developer.android.com/studio/command-line/adb。对于 Android Enterprise 设备，可以使用 Android Enterprise 应用程序权限策略限制应用程序权限。

  - 禁用应用程序：阻止列出的指定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，请将该设置更改为开，然后单击应用程序列表表中的添加。
    * 应用程序列表：要阻止的应用程序的列表。请将禁用应用程序设置为开并添加应用程序。请键入应用程序软件包名称。更改和部署某个应用程序列表将覆盖之前的应用程序列表。例如：如果禁用了 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，XenMobile 将启用 com.example.2。
  - 启用应用程序验证：允许操作系统扫描应用程序以检测恶意行为。默认值为开。
  - 启用 **Google** 应用程序：允许用户将 Google Mobile Services 中的应用程序下载到设备中。默认值为开。
  - 允许使用非 **Google Play** 应用程序：允许从 Google Play 之外的应用商店安装应用程序。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。用户将从“设置”应用程序执行这些操作。默认值为关。
  - 允许卸载应用程序：允许用户从托管的 Google Play Store 中卸载应用程序。默认值为关。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的详细信息，请参阅服务器属性。

- **BYOD** 工作配置文件
  - 允许在主屏幕上显示工作配置文件应用程序小组件：如果此设置设为开，则用户可以将工作配置文件应用程序小组件放置在设备主屏幕上。如果此设置设为关，则用户无法将工作配置文件应用程序小组件放置在设备主屏幕上。默认值为关。
    * **Apps with allowed widgets**（具有允许的小组件的应用程序）：要允许显示在主屏幕上的应用程序的列表。将允许在主屏幕上显示工作配置文件应用程序小组件设置为开并添加应用程序。单击添加并从列表中选择希望允许在主屏幕上显示其小组件的应用程序。单击保存。重复该过程将允许更多应用程序小组件。
  - 允许在设备联系人中添加工作配置文件联系人：在家长配置文件中显示托管 Android Enterprise 配置文件中的联系人，以便接收传入呼叫（Android 7.0 及更高版本）。默认值为关。

- **Samsung**
  - 启用 **TIMA** 密钥库： TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书路由到默认密钥库提供商进行存储。默认值为关。
  - 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。

- **Samsung**：**Knox** 容器**/**完全托管设备
  - 启用吊销检查：启用对已吊销证书的检查。默认值为关。

- **Samsung**：仅限 **Knox** 容器
  - 将应用程序移至容器：允许用户在其设备上的 Knox 容器与个人区域之间移动应用程序。默认值为开。
  - 强制执行多重身份验证：用户必须使用指纹和另一种身份验证方法（密码或 PIN）才能打开设备。默认值为开。

- 强制对容器执行身份验证：使用与用于解锁设备以打开 KNOX 容器的方法不同的身份验证方法。默认值为开。
- 允许使用安全小键盘：强制用户在 Knox 容器内使用安全小键盘。默认值为开。

当应用到使用工作配置文件的完全托管设备设置为“开”且对于具有工作配置文件的完全托管设备，请将策略应用到设置为托管设备时，请配置以下设置：

- 安全性
  - 允许帐户管理：允许在工作配置文件和托管设备中向帐户中添加对象。默认值为关。
  - 允许跨配置文件复制粘贴：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执行复制和粘贴操作。默认值为关。
  - 允许屏幕捕获：允许用户记录或捕获设备屏幕的屏幕拍图。默认值为关。
  - 允许使用相机：允许用户使用设备摄像头拍照并制作视频。默认值为关。
  - 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以及完全托管设备。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。
  - 允许使用 **NFC**：允许用户使用近场通信 (NFC) 从其设备向其他设备发送 Web 页面、照片、视频或其他内容。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：
    >
    > 可以在 XenMobile 中创建定位设备策略以强制实施地理边界。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：如果为开，则此设置允许用户打印到任何可通过用户设备访问的打印机。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，请单击系统应用程序列表表中的添加。
    - 系统应用程序列表：要在设备上启用的系统应用程序的列表。将启用系统应用程序设置为开并添加应用程序包名称。要查找系统应用程序的软件包名称，可以使用 Android Debug Bridge (`adb`) 调用 Android 软件包管理器 (`pm`) 命令。例如，`adb shell "pm list packages -f name"`，其中“name”为软件包名称的一部分。有关详细信息，请参阅 https://developer.android.com/studio/command-line/adb。对于 Android Enterprise 设备，可以使用 Android Enterprise 应用程序权限策略限制应用程序权限。

- 禁用应用程序：阻止列出的指定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，请将该设置更改为开，然后单击应用程序列表表中的添加。
  - 应用程序列表：要阻止的应用程序的列表。请将禁用应用程序设置为开并添加应用程序。请键入应用程序软件包名称。更改和部署某个应用程序列表将覆盖之前的应用程序列表。例如：如果禁用了 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，XenMobile 将启用 com.example.2。
- 启用应用程序验证：允许操作系统扫描应用程序以检测恶意行为。默认值为开。
- 启用 **Google** 应用程序：允许用户将 Google Mobile Services 中的应用程序下载到设备中。默认值为开。
- 允许使用非 **Google Play** 应用程序：允许从 Google Play 之外的应用商店安装应用程序。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。用户将从“设置”应用程序执行这些操作。默认值为关。
- 允许卸载应用程序：允许用户从托管的 Google Play Store 中卸载应用程序。默认值为关。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的详细信息，请参阅服务器属性。

- 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。默认值为开。
  - 允许数据漫游：允许用户在漫游时使用手机网络数据。默认值为“关”，即在用户设备上禁用漫游。默认值为关。
  - 允许短信：允许用户发送和接收短消息。默认值为关。
  - 允许使用状态栏：如果为开，此设置将在托管设备和专用设备（又称为 COSU 设备）上启用状态栏。此设置将禁用通知、快速设置以及其他促使退出全屏模式的屏幕叠加。用户可以转到系统设置并查看通知。适用于 Android 6.0 及更高版本。默认值为关。
  - 允许使用蓝牙：允许用户使用蓝牙。默认值为开。
    - 允许蓝牙共享：如果未选择，用户将无法在其设备上建立传出蓝牙共享。默认处于选中状态。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的详细信息，请参阅服务器属性。
  - 允许配置日期和时间：允许用户在其设备上更改日期和时间。默认值为开。
  - 允许恢复出厂设置：允许用户在其设备上恢复出厂设置。默认值为开。
  - 保持设备屏幕处于打开状态：如果此设置设为开，设备插入时设备屏幕保持打开状态。默认值为关。
  - 允许 **USB** 大容量存储：允许通过 USB 连接在用户的设备与计算机之间传输大型数据文件。默认值为开。
  - 允许使用麦克风：允许用户在其设备上使用麦克风。默认值为开。
  - 允许网络共享：允许用户配置便携式热点和网络共享数据。默认值为关。启用此设置时，这些设置适用于 Samsung 设备：
  - 保持键盘锁不锁定设备：如果为开，此设置将在托管设备和专用设备（又称为 COSU 设备）上的锁屏界面上禁用键盘锁。默认值为关。
  - 允许更改 **Wi-Fi**：如果为开，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 进行文件传输。默认值为关。

- **Samsung**

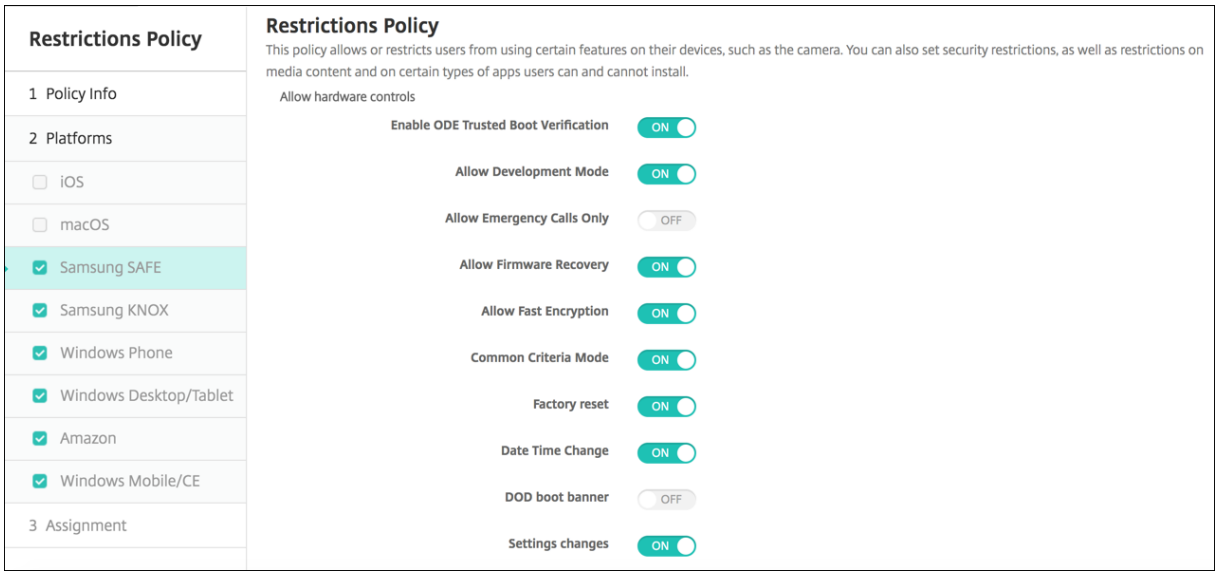
- 启用 **TIMA** 密钥库： TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书路由到默认密钥库提供商进行存储。默认值为关。
- 允许共享列表：允许用户在“共享方式”列表中的应用程序之间共享内容。默认值为开。
- 启用审核日志：启用事件审核日志的创建，以便对设备进行取证分析。默认值为关。

- **Samsung:** 仅限完全托管设备
  - 启用 **ODE** 可信引导验证：使用 ODE 可信引导验证建立从引导加载程序到系统映像的信任链。默认值为开。
  - 仅允许紧急呼叫：允许用户在其设备上启用“仅限紧急呼叫”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：允许仅加密已使用的内存空间。此加密与完全磁盘加密（用于加密所有数据）完全不同。该数据包括设置、应用程序数据、已下载的文件和应用程序、媒体及其他文件。默认值为开。
  - 启用通用准则模式：将设备置于通用准则模式。通用准则配置强制执行严苛的安全流程。默认值为开。
  - 启用重新启动横幅：当用户的设备重新启动时，显示 DoD 批准的系统使用通知消息或横幅。默认值为关。
  - 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，适用于完全托管设备。默认值为开。
  - 允许使用剪贴板：允许用户在其设备上将数据复制到剪贴板。默认值为开。
    - 允许剪贴板共享：允许用户在其设备和某个计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。
  - 允许使用 **Home** 键：允许用户在其完全托管设备上使用 **Home** 键。默认值为开。
  - 允许模拟位置：允许用户伪造其 GPS 位置。适用于完全托管设备。默认值为关。
  - **NFC**：允许用户在其完全托管设备上使用 NFC（MDM 3.0 及更高版本）。默认值为开。
  - 允许关闭电源：允许用户关闭其完全托管设备（MDM 3.0 及更高版本）的电源。默认值为开。
  - 允许使用 **Wi-Fi Direct**：允许用户通过其 Wi-Fi 连接直接连接到其他设备。默认值为开。如果为开，则必须启用允许更改 **Wi-Fi** 设置。
  - 允许使用 **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，用户的设备为 USB 设备提供电源。默认值为开。
  - 允许使用语音拨号器：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 与其他人共享内容（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手和知识导航器（MDM 4.0 及更高版本）。默认值为开。
  - 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。默认值为关。如果为开，则允许网络共享设置也必须为开。
  - 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。默认值为关。如果为开，则允许网络共享设置也必须为开。
  - 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。默认值为关。如果为开，则允许网络共享设置也必须为开。
  - 允许传入 **MMS**：允许用户接收 MMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。
  - 允许传出 **MMS**：允许用户发送 MMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。

- 允许传入 **SMS**：允许用户接收 SMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。
- 允许传出 **SMS**：允许用户发送 SMS 消息。默认值为关。如果为开，则必须打开允许 **SMS** 设置。
- 配置移动网络：允许用户使用其手机网络数据连接。默认值为关。
- 按天限制 **(MB)**：输入移动数据用户每天可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按周限制 **(MB)**：输入移动数据用户每周可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 按月限制 **(MB)**：输入移动数据用户每月可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 仅允许建立安全的 **VPN** 连接：允许用户仅使用安全连接（MDM 4.0 及更高版本）。默认值为开。
- 允许录制音频：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，则必须打开允许使用麦克风设置。
- 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，则必须打开允许使用相机设置。
- 允许漫游时推送消息：允许用户使用手机网络数据进行推送。默认值为关。如果为开，则必须启用允许数据漫游设置。
- 允许漫游时自动同步：允许用户使用手机网络数据进行同步。默认值为关。如果为开，则必须启用允许数据漫游设置。
- 允许漫游时语音通话：允许用户使用手机网络数据进行语音通话。默认值为关。如果为开，则必须启用允许数据漫游设置。

- **Samsung**：**Knox** 容器**/**完全托管设备
  - 启用吊销检查：启用对已吊销证书的检查。默认值为关。
- **Samsung**：仅限 **Knox** 容器
  - 将应用程序移至容器：允许用户在其设备上的 Knox 容器与个人区域之间移动应用程序。默认值为开。
  - 强制执行多重身份验证：用户必须使用指纹和另一种身份验证方法（密码或 PIN）才能打开设备。默认值为开。
  - 强制对容器执行身份验证：使用与用于解锁设备以打开 KNOX 容器的方法不同的身份验证方法。默认值为开。
  - 允许使用安全小键盘：强制用户在 Knox 容器内使用安全小键盘。默认值为开。

Samsung SAFE 设置



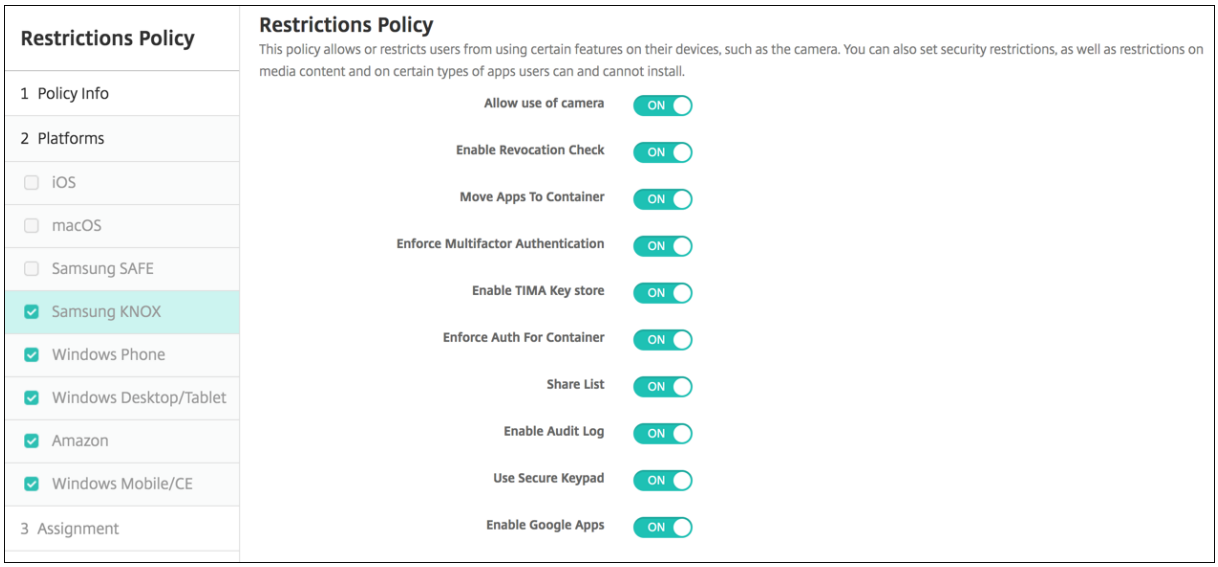
某些选项仅适用于特定的 Samsung Mobile Device Management API。这些选项上会标记相关的版本信息。

- 允许硬件控制
  - 启用 **ODE** 可信引导验证：使用 ODE 可信引导验证建立从引导加载程序到系统映像的信任链。
  - 允许使用开发模式：允许用户在其设备上启用开发人员设置。
  - 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。
  - 允许固件恢复：允许用户在其设备上恢复固件。
  - 允许快速加密：允许仅加密已使用的内存空间。此选项相对于完全磁盘加密，即加密所有数据，包括设置、应用程序数据、已下载的文件和应用程序、媒体及其他文件。
  - 通用准则模式：将设备置于通用准则模式。通用准则配置强制执行严苛的安全流程。
  - 恢复出厂设置：允许用户在其设备上恢复出厂设置。
  - 日期时间更改：允许用户在其设备上更改日期和时间。
  - **DOD** 重新启动横幅：用户的设备重新启动时，显示 DoD 批准的系统使用通知消息或横幅。
  - 设置更改：允许用户在其设备上更改设置。
  - 备份：允许用户备份其设备上的应用程序和系统数据。
  - 通过无线传输技术升级：允许用户设备无线接收软件更新（MDM 3.0 及更高版本）。
  - 后台数据：允许应用程序在后台同步数据。
  - 相机：允许用户在其设备上使用相机。
  - 剪贴板：允许用户在其设备上将数据复制到剪贴板。
    - 剪贴板共享：允许用户在其设备和某个计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。
  - **Home** 键：允许用户在其设备上使用 Home 键。
  - 麦克风：允许用户在其设备上使用麦克风。
  - 伪装位置：允许用户伪装其 GPS 位置。
  - **NFC**：允许用户在其设备（MDM 3.0 及更高版本）上使用 NFC（近场通信）。
  - 关机：允许用户关闭其设备（MDM 3.0 及更高版本）。

  - 屏幕截图：允许用户在其设备上截取屏幕截图。
  - **SD** 卡：允许用户在其设备上使用 SD 卡（如果可用）。
  - 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）。
  - **SBeam**：允许用户使用 NFC 和 Wi-Fi Direct 与其他人共享内容（MDM 4.0 及更高版本）。
  - **SVoice**：允许用户在其设备上使用智能个人助手和知识导航器（MDM 4.0 及更高版本）。
  - 允许多个用户：允许多个用户使用一个设备（MDM 4.0 及更高版本）。默认值为关。
- 允许使用应用程序
  - 浏览器：允许用户使用 Web 浏览器。
  - **Youtube**：允许用户访问 YouTube。
  - **Google Play/Marketplace**：允许用户访问 Google Play 和 Google Apps Marketplace。
  - 允许使用非 **Google Play** 应用程序：允许用户从 Google Play 和 Google Apps Marketplace 之外的站点下载应用程序。如果设置为开，用户可以在其设备上使用安全设置信任来自未知来源的应用程序。
  - 停止系统应用程序：允许用户禁用预安装的系统应用程序（MDM 4.0 及更高版本）。
  - 禁用应用程序：如果设置为开，则将阻止指定的应用程序列表在 Samsung SAFE 设备上运行。
- 网络
  - 传入 **MMS**：允许用户接收 MMS 消息。
  - 传入 **SMS**：允许用户接收 SMS 消息。
  - 传出 **MMS**：允许用户发送 MMS 消息。
  - 传出 **SMS**：允许用户发送 SMS 消息。
  - 用户添加配置文件 **VPN**：
  - 蓝牙：允许用户使用蓝牙。
    - 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。
  - **WiFi**：允许用户连接到 WiFi 网络。
    - 网络共享：允许用户使用其 WiFi 连接与其他设备共享移动数据连接。
    - 直接：允许用户通过其 WiFi 连接直接连接到其他设备（MDM 4.0 及更高版本）。
    - 状态更改：允许应用程序更改 WiFi 连接状态。
    - 用户策略更改：允许用户更改 WiFi 策略。如果不选择，则用户只能更改 WiFi 用户名和密码。如果选择此选项，用户可以更改所有 WiFi 策略。
  - 网络共享：允许用户与其他设备共享移动数据连接。
  - 手机网络数据：允许用户使用其手机网络连接获取数据。
  - 允许漫游：允许用户在漫游时使用手机网络数据。默认值为“关”，即在用户设备上禁用漫游。
  - 仅允许安全连接：允许用户仅使用安全连接（MDM 4.0 及更高版本）。
  - **Android Beam**：允许用户使用 NFC 从其设备向其他设备发送 Web 页面、照片、视频或其他内容（MDM 4.0 及更高版本）。
  - 音频录制：允许用户使用其设备录制音频（MDM 4.0 及更高版本）。
  - 视频录制：允许用户使用其设备录制视频（MDM 4.0 及更高版本）。
  - 定位服务：允许用户在其设备上打开 GPS。
  - 按天限制 **(MB)**：输入移动数据用户每天可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。

  - 按周限制 **(MB)**：输入移动数据用户每周可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
  - 按月限制 **(MB)**：输入移动数据用户每月可以使用的 MB 数。默认值为 0，表示禁用此功能（MDM 4.0 及更高版本）。
- 允许执行 **USB** 操作：允许在用户设备与计算机之间建立 USB 连接。
  - 调试：允许通过 USB 调试。
  - 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，用户的设备为 USB 设备提供电源。
  - 大容量存储设备：允许通过 USB 连接在用户的设备与计算机之间传输大型数据文件。
  - **Kies** 媒体播放器：允许用户使用 Samsung Kies 工具在其设备与计算机之间同步文件。
  - 网络共享：允许用户通过 USB 连接与其他设备共享移动数据连接。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Samsung KNOX 设置

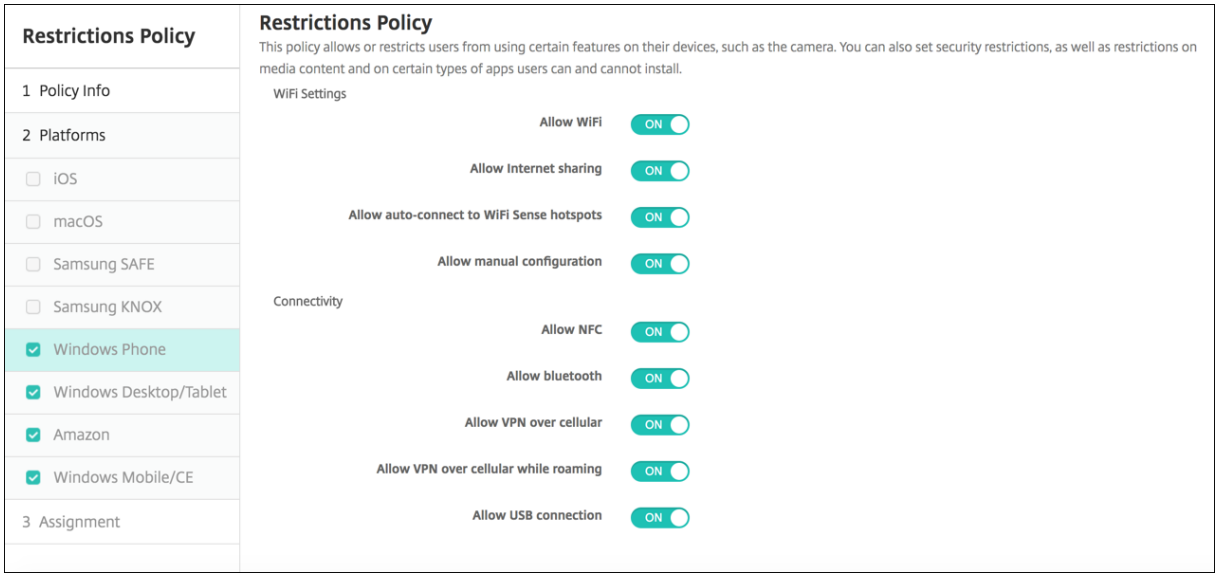


这些选项仅适用于 Samsung KNOX Premium (KNOX 2.0)。

- 允许使用相机：允许用户在其设备上使用相机。
- 允许执行吊销检查：启用已吊销证书检查。
- 将应用程序移至容器：允许用户在其设备上在 KNOX 容器与个人区域之间移动应用程序。

- 强制执行多重身份验证：用户必须使用指纹和另一种身份验证方法（密码或 PIN）才能打开设备。
- 启用 **TIMA** 密钥库： TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书路由到默认密钥库提供商进行存储。
- 强制对容器执行身份验证：使用不同的单独身份验证来打开 KNOX 容器，通过该容器来解锁设备。
- 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。
- 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。
- 使用安全小键盘：强制用户在 KNOX 容器内使用安全小键盘。
- 启用 **Google Apps**：允许用户将 Google Mobile Services 中的应用程序下载到 KNOX 容器中。
- 身份验证智能卡浏览器：在配备有智能卡读卡器的设备上启用浏览器身份验证。

Windows Phone 和 **Windows Desktop/Tablet** 设置

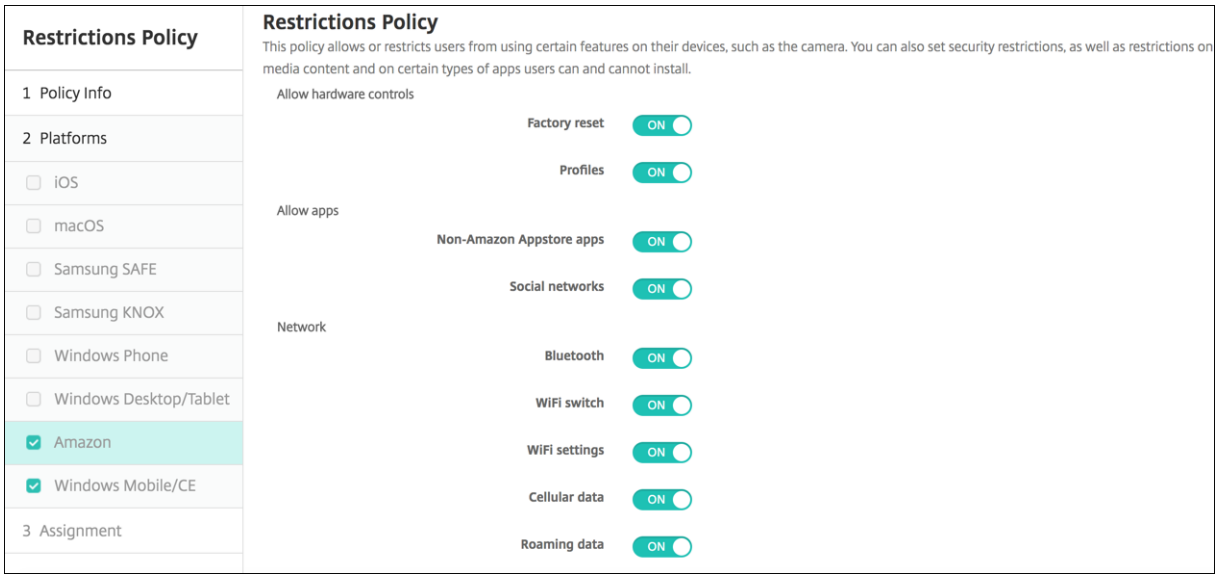


- **WiFi** 设置
  - 允许使用 **WiFi**：允许设备连接到 Wi-Fi 网络。仅限 Windows Phone。
  - 允许 **Internet** 共享：允许设备通过将其设为 WiFi 热点与其他设备共享其 Internet 连接。
  - 允许自动连接到 **WiFi** 感应热点：允许设备自动连接到 WiFi 感应热点。必须启用定位服务才能使用此选项。有关 WiFi 感应的详细信息，请参阅 Windows Phone“WiFi 感知”常见问题解答。
  - 允许手动配置：允许用户手动配置 WiFi 连接。仅限 Windows Phone。
- 连接
  - 允许 **NFC**：允许设备与 NFC（近场通信）标记或另一台启用了 NFC 的传输设备通信。仅限 Windows Phone。
  - 允许使用蓝牙：允许设备通过蓝牙进行连接。仅限 Windows Phone。
  - 允许通过手机网络使用 **VPN**：允许设备通过 VPN 连接到手机网络。
  - 允许在漫游时通过手机网络使用 **VPN**：允许设备在通过手机网络漫游时使用 VPN。
  - 允许 **USB** 连接：允许桌面通过 USB 连接访问设备的存储。仅限 Windows Phone。
  - 允许使用手机网络数据漫游：允许用户在漫游时使用手机网络数据。

- 帐户
  - 允许使用 **Microsoft** 帐户连接：允许设备使用 Microsoft 帐户进行与电子邮件无关的连接身份验证和服务。
  - 允许使用非 **Microsoft** 电子邮件：允许用户添加非 Microsoft 电子邮件帐户。
- 搜索：仅限 Windows Phone。
  - 允许搜索使用定位服务：允许搜索使用设备的定位服务。
  - 过滤成人内容：允许成人内容。默认值为关，表示不过滤成人内容。
  - 允许 **Bing** 影像存储捕获的图片：允许 Bing 影像存储执行 Bing 影像搜索时捕获的图片。
- 系统
  - 允许使用存储卡：允许设备使用存储卡。
  - 遥测：在列表中，单击某个选项以允许或限制设备发送遥测信息。默认值为允许。其他选项为不允许和允许，次要数据请求除外。
  - 允许使用定位服务：允许使用定位服务。
  - 允许预览内部版本：允许用户预览 Microsoft 内部版本。
- 相机：仅限 Windows Desktop/Tablet
  - 允许使用相机：允许用户使用其设备相机。
- 蓝牙：仅限 Windows Desktop/Tablet
  - 允许使用可发现模式：允许蓝牙设备查找本地设备。
  - 本地设备名称：本地设备的名称。
- 安全性：仅限 Windows Phone
  - 允许手动安装根证书：允许用户手动安装根证书。
  - 要求设备加密：要求设备加密。请注意，在设备上启用加密后，无法将其禁用。默认值为关。
  - 允许复制粘贴：允许用户在其设备上复制和粘贴数据。
  - 允许屏幕捕获：允许用户在其设备上捕获屏幕。
  - 允许录制音频：允许用户在其设备上使用音频录制功能。
  - 允许使用 **“**另存为**”** 保存 **Office** 文件：允许用户使用“另存为”保存 Office 文件。
  - 允许显示操作中心通知：允许在设备锁屏界面上显示操作中心通知。
  - 允许使用 **Cortana**：允许用户访问 Cortana（智能个人助手和知识导航器）。
  - 允许同步设备设置：允许用户在漫游时在 Windows Phone 8.1 设备之间同步设置。
- 体验：仅限 Windows Desktop/Tablet
  - 允许使用 **Cortana**：允许用户访问 Cortana（智能个人助手和知识导航器）。
  - 允许发现设备：允许对设备进行网络发现。
  - 允许手动取消注册 **MDM**：允许用户手动从 XenMobile MDM 中取消注册其设备。
  - 允许同步设备设置：允许用户在漫游时在 Windows 10 和 Windows 11 设备之间同步设置。
- 超出锁定范围：仅限 Windows Desktop/Tablet
  - 允许显示 **Toast**：允许在锁屏界面上显示 Toast 通知。仅限 Windows Desktop/Tablet
- 应用程序
  - 允许访问应用商店：允许用户访问 Microsoft 应用商店。仅限 Windows Phone。
  - 允许开发人员解锁：允许用户向 Microsoft 注册其设备以及开发或安装 Windows Phone 应用商店之外

的应用程序。仅限 Windows Phone。
  - 允许使用 **Web** 浏览器访问：允许在设备上使用 Internet Explorer。仅限 Windows Phone。
  - 允许应用商店自动更新：允许应用商店中的应用程序自动更新。仅限 Windows Desktop/Tablet。
- 隐私：仅限 Windows Desktop/Tablet
  - 允许输入个性化：允许运行输入个性化服务，以改进基于用户键入内容的预测输入（例如手写笔和触摸键盘）。
- 设置：仅限 Windows Desktop/Tablet。
  - 允许自动播放：允许用户更改自动播放设置。
  - 允许使用流量感知：允许用户更改流量感知设置。
  - 允许设置日期时间：允许用户更改日期和时间设置。
  - 允许设置语言：允许用户更改语言设置。
  - 允许设置电源睡眠：允许用户更改电源和睡眠设置。
  - 允许设置区域：允许用户更改区域设置。
  - 允许设置登录选项：允许用户更改登录设置。
  - 允许设置工作区：允许用户更改工作区设置。
  - 允许使用您的帐户：允许用户更改帐户设置。

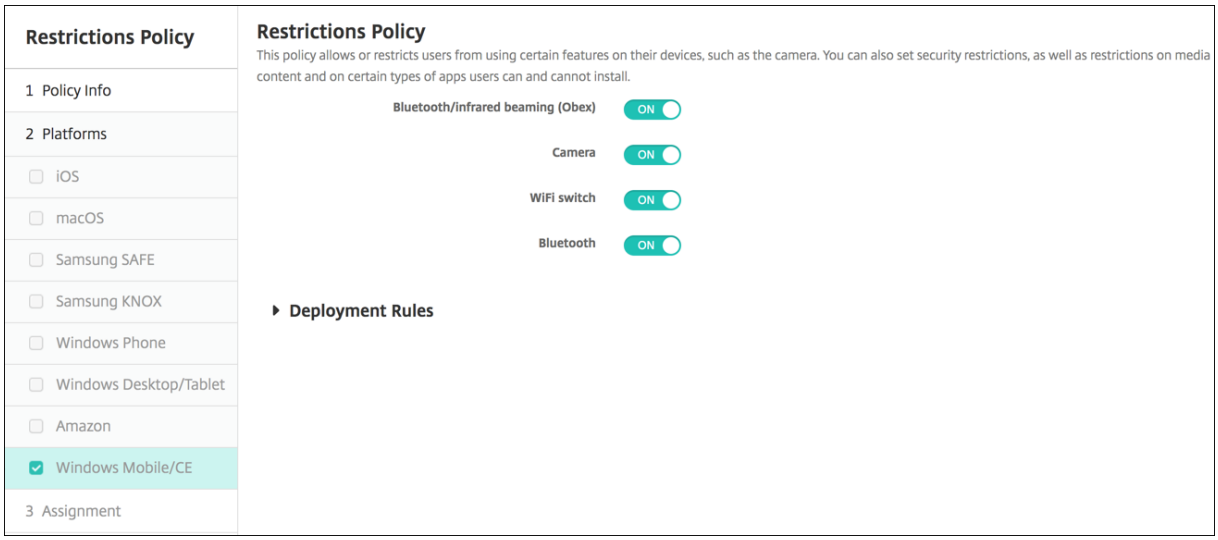
Amazon 设置



- 允许硬件控制
  - 恢复出厂设置：允许用户在其设备上恢复出厂设置
  - 配置文件：允许用户在其设备上更改硬件配置文件。
- 允许使用应用程序
  - 非 **Amazon** 应用商店应用程序：允许用户在其设备上安装非 Amazon 应用商店应用程序。
  - 社交网络：允许用户从其设备访问社交网络。
- 网络

  - 蓝牙：允许用户使用蓝牙。
  - **WiFi** 开关：允许应用程序更改 WiFi 连接状态。
  - **WiFi** 设置：允许用户更改 WiFi 设置。
  - 手机网络数据：允许用户使用其手机网络连接获取数据。
  - 漫游数据：允许用户在漫游时使用手机网络数据。
  - 定位服务：允许用户使用 GPS。
- **USB** 操作：
  - 调试：允许用户设备通过 USB 连接到计算机以进行调试。

Windows Mobile/CE 设置



- 蓝牙/红外收发 **(Obex)**：通过 Bluetooth 或红外线启用 OBEX（OBject EXchange 协议）以在设备之间交换数据。
- 相机：在用户设备上启用相机。
- **WiFi** 开关：允许用户切换 WiFi 网络。
- 蓝牙：在用户设备上启用蓝牙。
- 相机：在用户设备上启用相机。
- **WiFi** 开关：允许用户切换 WiFi 网络。
- 蓝牙：在用户设备上启用蓝牙。

漫游设备策略

March 27, 2020

可以在 XenMobile 中添加一个设备策略，用于配置是否允许在用户 iOS 和 Windows Mobile/CE 设备上进行语音和数据漫游。禁用语音漫游时，会自动禁用数据漫游。对于 iOS，此策略仅适用于 iOS 5.0 及更高版本的设备。

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。

iOS 设置

- 禁用语音漫游：选择是否禁用语音漫游。启用此选项时，会自动禁用数据漫游。默认值为关，表示允许语音漫游。
- 禁用数据漫游：选择是否禁用数据漫游。此选项仅在启用语音漫游时可用。默认值为关，表示允许数据漫游。

Windows Mobile/CE 设置

- 漫游时
  - 只使用按需连接：如果用户在其设备上手动触发连接，或者如果移动应用程序请求强制进行连接（例如，在已相应设置 Exchange Server 时的推送邮件请求），设备才会连接到 XenMobile。请注意，此选项会临时禁用默认设备连接计划策略。
  - 阻止所有手机网络连接，但 **XenMobile** 管理的连接除外：除了在 XenMobile 应用程序通道或其他 XenMobile 设备管理任务中正式声明的数据流量外，该设备不会发送或接收任何其他数据。例如，此选项将禁用所有通过设备的 Web 浏览器到 Internet 的连接。
  - 阻止 **XenMobile** 管理的所有手机网络连接：所有通过 XenMobile 通道传输的应用程序数据都将被阻止（包括 XenMobile Remote Support）。但是，不会阻止与纯“设备管理”相关的数据流量。
  - 阻止与 **XenMobile** 的所有手机网络连接：在这种情况下，除非设备通过 USB、WiFi 或其默认移动运营商手机网络重新进行连接，否则在设备和 XenMobile 之间不会传输任何流量。
- 国内漫游时
  - 忽略国内漫游：用户在国内漫游时不阻止任何数据。

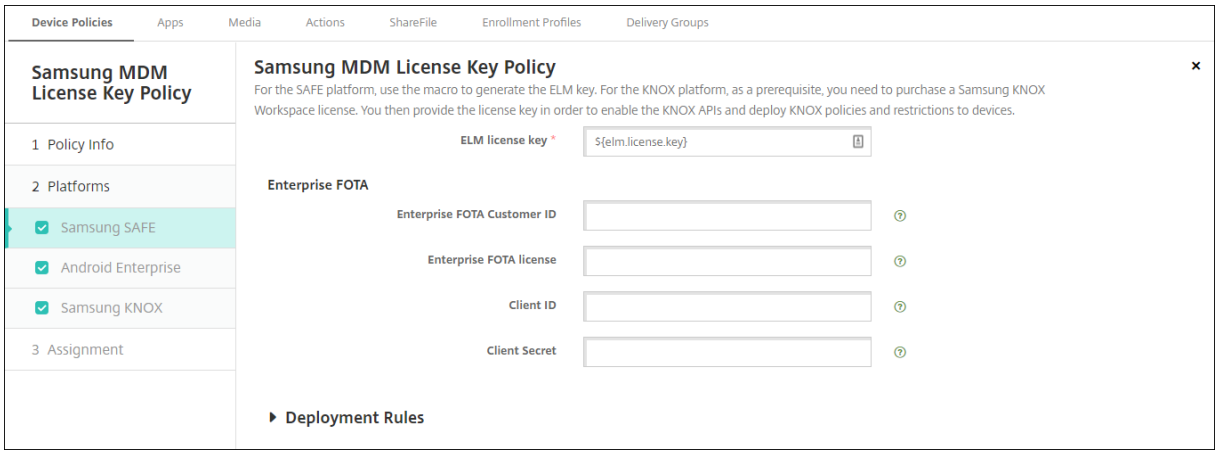
Samsung MDM 许可证密钥设备策略

January 5, 2022

指定内置 Samsung Enterprise License Management (ELM) 密钥，必须先将该密钥部署到设备，才能部署 SAFE 策略和限制。XenMobile 还支持 Samsung Enterprise Firmware-Over-The-Air (E-FOTA) 服务。XenMobile 支持并扩展了 Samsung for Enterprise (SAFE) 和 Samsung KNOX 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。

Samsung SAFE 设置



- **ELM** 许可证密钥：XenMobile 使用生成 ELM 许可证密钥的宏预填充此字段。如果此字段为空，请键入以下宏：${elm.license.key}

配置 Samsung E-FOTA 设置

Samsung Enterprise FOTA (E-FOTA) 允许您确定设备更新的时间以及要使用的固件版本。E-FOTA 允许您在部署更新之前对其进行测试，以确保更新与您的应用程序兼容。可以强制设备使用可用的最新固件版本进行更新，而不要求用户交互。

Samsung 支持对运行授权固件的 Samsung Knox 2.7.1 设备（最低版本）使用 E-FOTA。

XenMobile 支持将设备从 XenMobile 控制台添加到 Knox E-FOTA One。有关从 XenMobile 导出设备列表的详细信息，请参阅导出设备表。有关将设备添加到 Knox E-FOTA One 的详细信息，请参阅 Samsung 文档。

XenMobile 不支持 MDM 上的 Knox E-FOTA 解决方案。

要配置 E-FOTA 策略，请执行以下操作：

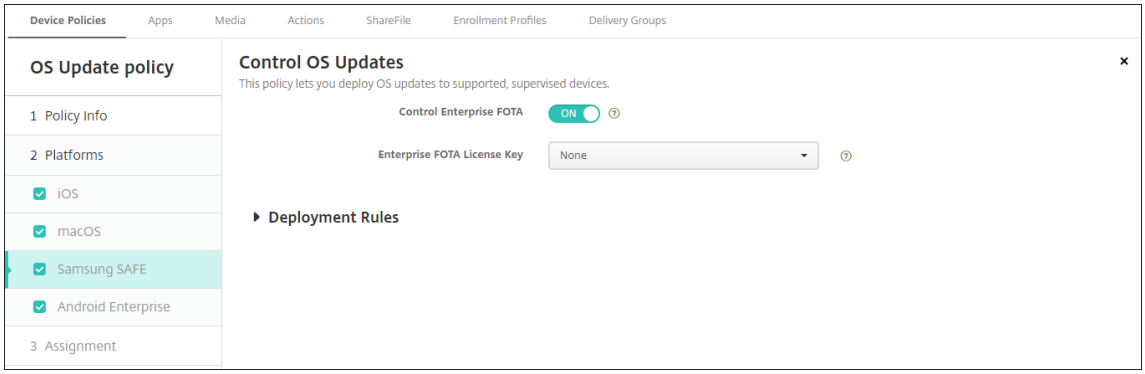
1. 使用您从 Samsung 接收的密钥和许可证信息创建 Samsung MDM 许可证密钥设备策略。XenMobile Server 随后将验证该信息并进行注册。如果 XenMobile 检测到 E-FOTA 问题，则会显示一条错误消息来指示该问题。请使用提供的代码来解决问题。有关详细信息，请参阅 Developer Guides（《开发人员指南》）。

   键入 **ELM** 许可证密钥：XenMobile 使用生成 ELM 许可证密钥的宏预填充此字段。如果此字段为空，请键入以下宏：${elm.license.key}

   键入 Samsung 在您购买 E-FOTA 软件包时提供的以下信息：

   - **Enterprise FOTA** 客户 **ID**
   - **Enterprise FOTA** 许可证
   - 客户端 **ID**
   - 客户端密码

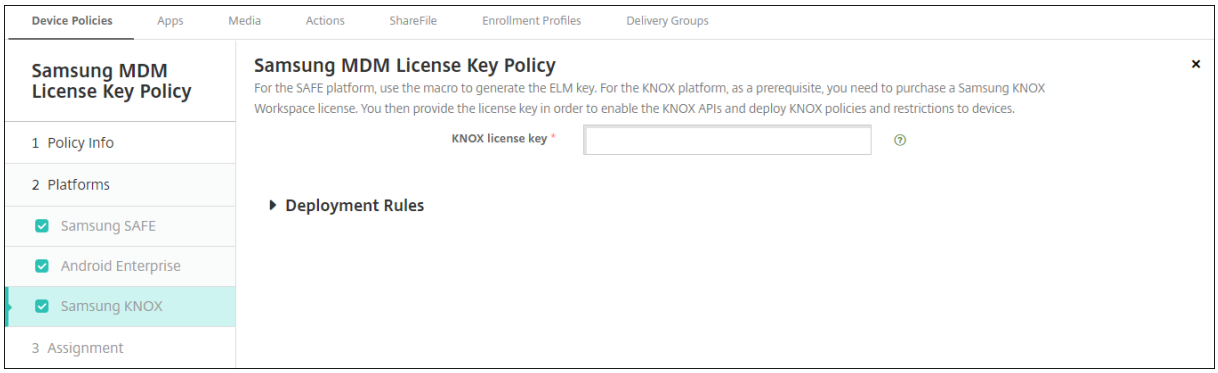
2. 或者，创建“控制操作系统更新”设备策略。



- 启用 **Enterprise FOTA**：设置为开。
- **Enterprise FOTA** 许可证密钥：选择您在步骤 1 中创建的 Samsung MDM 许可证密钥策略名称。

3. 将控制操作系统更新策略部署到 Secure Hub。

Android Enterprise 和 **Samsung KNOX** 设置



- **KNOX** 许可证密钥：键入从 Samsung 获取的 KNOX 许可证密钥。

Samsung SAFE 防火墙设备策略

July 7, 2020

此策略允许您为 Samsung 设备配置防火墙设置。输入要允许或阻止的 IP 地址、端口和主机名。还可以配置代理和代理重新路由设置。

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。

Samsung SAFE 设置

- 允许/拒绝主机：对于希望允许访问或拒绝访问的每个主机，单击添加并配置以下设置：
  - 主机名/**IP** 范围：希望影响的站点的主机名或 IP 地址范围。

  - 端口/端口范围：端口或端口范围。
  - 允许/拒绝规则过滤：单击白名单以允许访问站点或单击黑名单以拒绝访问站点。

    > 注意：
    > XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

- 重新路由配置：对于要配置的每个代理，单击添加并配置以下设置：
  - 主机名/**IP** 范围：代理重新路由的主机名或 IP 地址范围。
  - 端口/端口范围：代理重新路由的端口或端口范围。
  - 代理 **IP**：代理重新路由的代理 IP 地址。
  - 代理端口：代理重新路由的代理端口。
- 代理配置
  - 代理 **IP**：代理服务器的 IP 地址。
  - 端口：代理服务器端口。

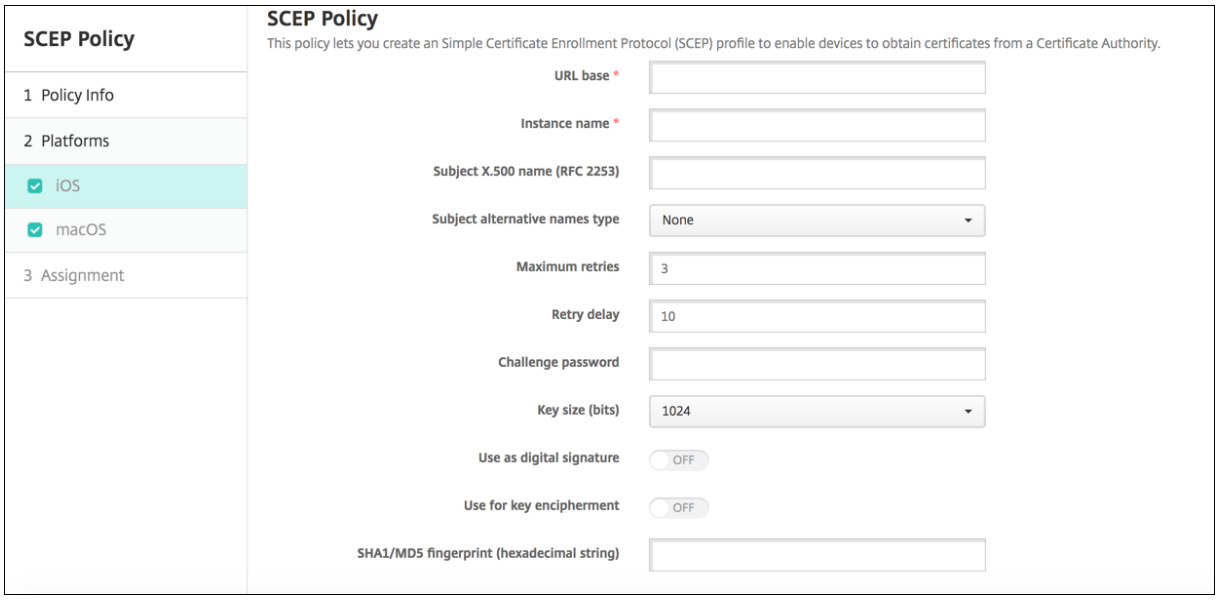
SCEP 设备策略

January 5, 2022

通过此策略，可以将 iOS 和 macOS 设备配置为使用简单证书注册协议 (SCEP) 从外部 SCEP 服务器检索证书。如果希望从连接到 XenMobile 的 PKI 向使用 SCEP 的设备交付证书，应采用分布式模式创建 PKI 实体和 PKI 提供程序。有关详细信息，请参阅 PKI 实体。

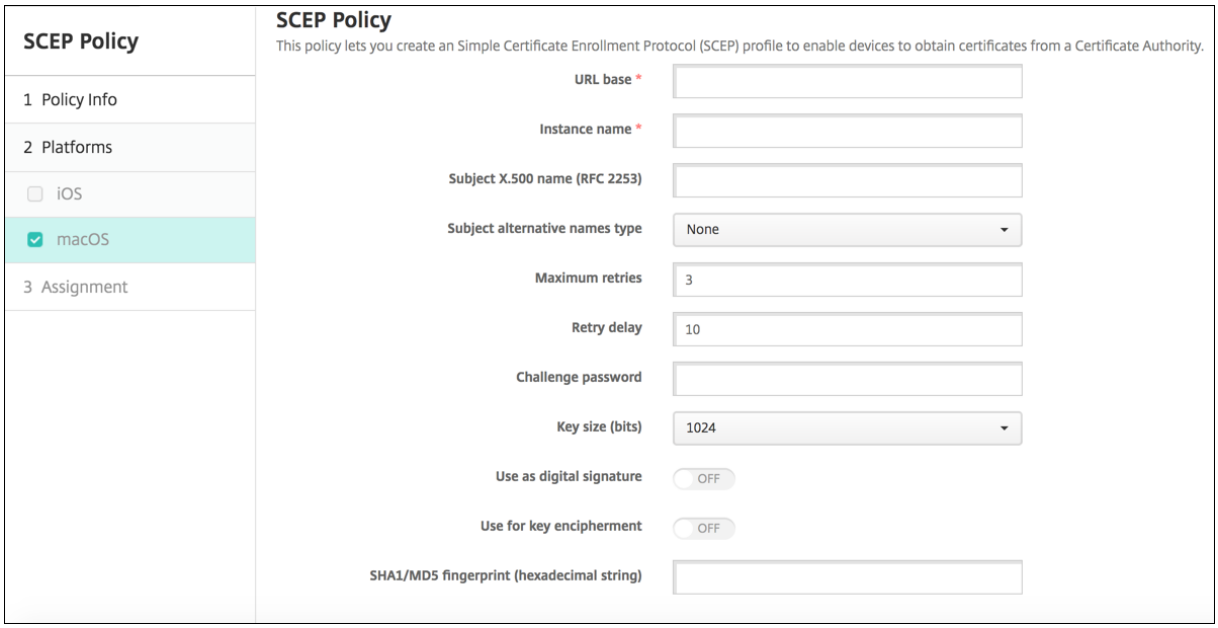
要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置



- **URL** 基：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。但是，如果允许重复使用一次性密码，则应该使用 HTTPS 来保护密码。此步骤不是必需步骤。
- 实例名称：键入 SCEP 服务器可以识别的任何字符串。例如，可以是类似 example.org 的域名。如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。此步骤不是必需步骤。
- 使用者 **X.500** 名称 **(RFC 2253)**：键入表示为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。例如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 将转换为：[[[“C”, “US”]], [[“O”, “Apple Inc.”]], …, [[“1.2.5.3”, “bar”]]]。OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。
- 使用者备用名称类型：在列表中，单击备用名称类型。SCEP 策略可指定可选的备用名称类型，用于提供 CA 颁发证书所需的值。可以指定无、**RFC 822** 名称、**DNS** 名称或 **URI**。
- 最大重试次数：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。默认值为 **3**。
- 重试延迟：键入执行下次重试之前需要等待的秒数。第一次重试尝试没有延迟。默认值为 **10**。
- 质询密码：输入预共享密钥。
- 密钥大小 **(**位**)**：选择 **2048** 或更大值作为密钥大小，单位为位。
- 用作数字签名：指定是否要将证书用作数字签名。如果有人使用证书来验证数字签名，如验证证书是否由 CA 颁发，SCEP 服务器将在使用公钥解密哈希之前确认该证书是否可以用于此目的。
- 用于密钥加密：指定是否要将证书用于密钥加密。如果服务器正在使用客户端提供的证书中包含的公钥来验证数据段是否使用私钥进行加密，服务器将首先检查证书是否可用于密钥加密。否则，操作将失败。
- **SHA1/MD5** 指纹 **(X** 六进制字符串**)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹，供设备在注册期间用于确认 CA 响应的真实性。可以输入 SHA1 或 MD5 指纹，或选择证书来导入其签名。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置



- **URL** 基：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。但是，如果允许重复使用一次性密码，则应该使用 HTTPS 来保护密码。此步骤不是必需步骤。
- 实例名称：键入 SCEP 服务器可以识别的任何字符串。例如，可以是类似 example.org 的域名。如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。此步骤不是必需步骤。
- 使用者 **X.500** 名称 **(RFC 2253)**：键入表示为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。例如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 将转换为：[[[“C”, “US”]], [[“O”, “Apple Inc.”]], …, [[“1.2.5.3”, “bar”]]]。OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。
- 使用者备用名称类型：在列表中，单击备用名称类型。SCEP 策略可指定可选的备用名称类型，用于提供 CA 颁发证书所需的值。可以指定无、**RFC 822** 名称、**DNS** 名称或 **URI**。
- 最大重试次数：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。默认值为 **3**。
- 重试延迟：键入执行下次重试之前需要等待的秒数。第一次重试尝试没有延迟。默认值为 **10**。
- 质询密码：键入预共享密钥。
- 密钥大小 **(**位**)**：选择 **2048** 或更大值作为密钥大小，单位为位。
- 用作数字签名：指定是否要将证书用作数字签名。如果有人使用证书来验证数字签名，如验证证书是否由 CA 颁发，SCEP 服务器将在使用公钥解密哈希之前确认该证书是否可以用于此目的。
- 用于密钥加密：指定是否要将证书用于密钥加密。如果服务器正在使用客户端提供的证书中包含的公钥来验证数据段是否使用私钥进行加密，服务器将首先检查证书是否可用于密钥加密。否则，操作将失败。

- **SHA1/MD5** 指纹 **(X** 六进制字符串**)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹，供设备在注册期间用于确认 CA 响应的真实性。可以输入 SHA1 或 MD5 指纹，或选择证书来导入其签名。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

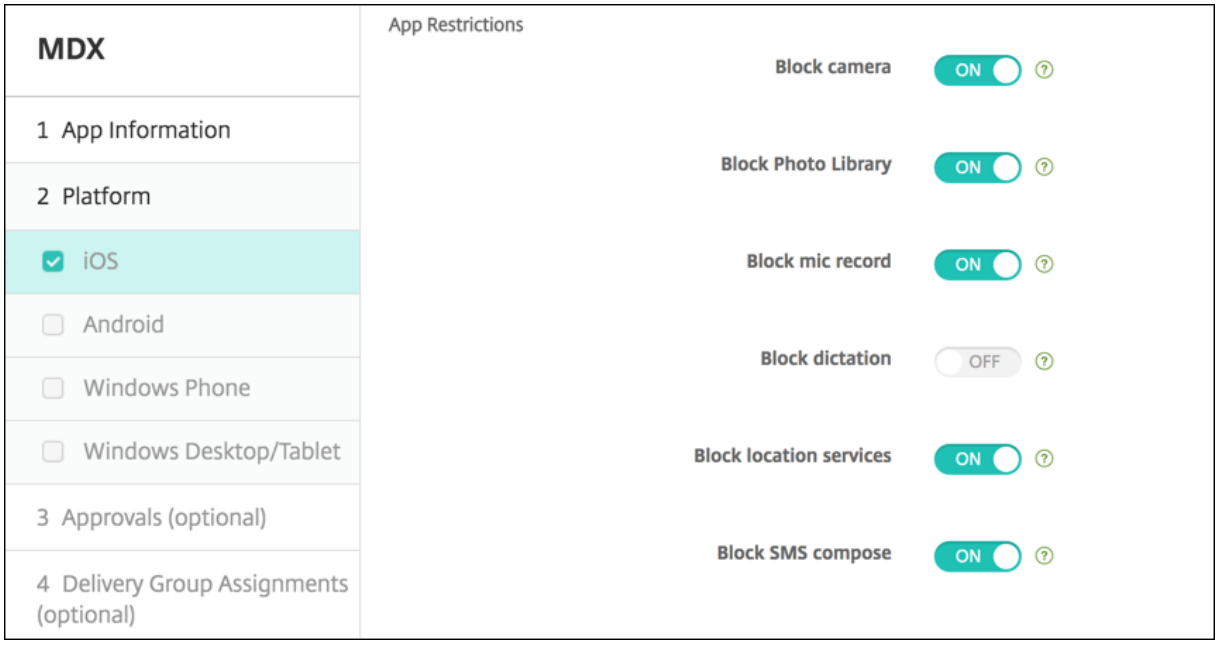
Siri 和听写策略

January 5, 2022

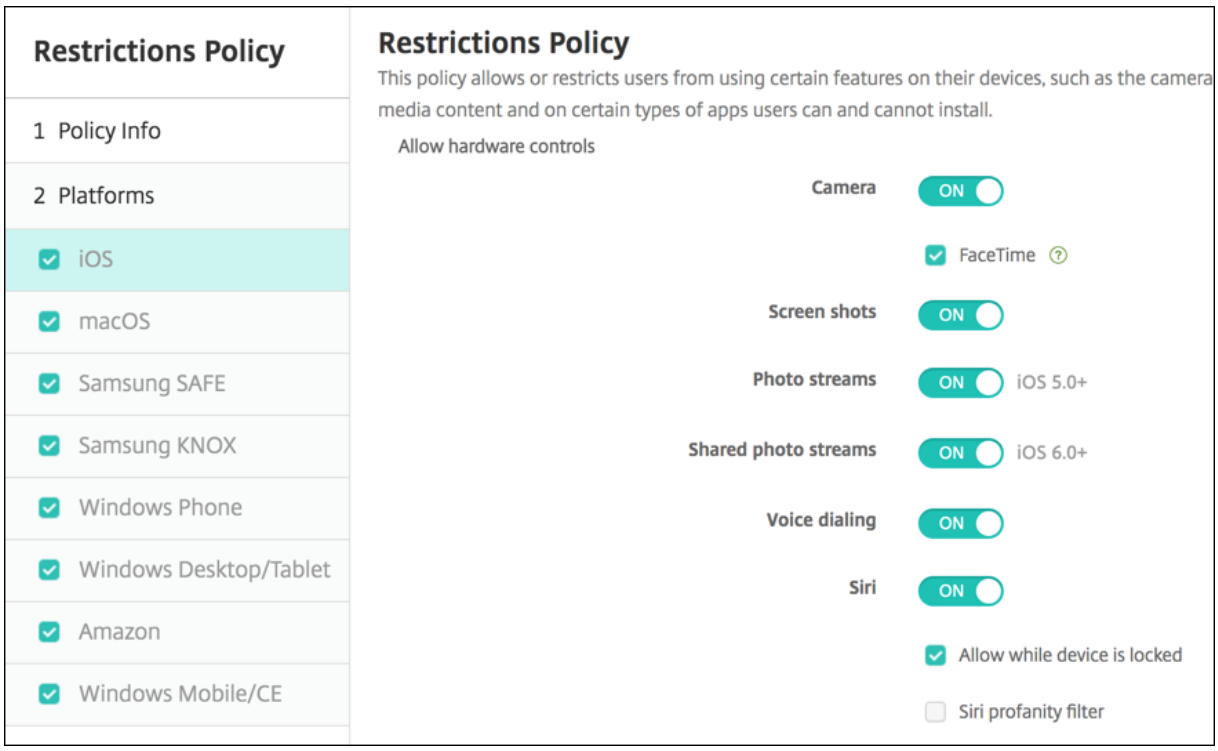
用户向 Siri 提问时或在托管 iOS 设备上听写文本时，Apple 将收集语音数据以改进 Siri 的功能。语音数据通过 Apple 的基于云的服务传输，因此存在于安全的 XenMobile 容器外部。但是，由听写产生的文本仍保留在容器内部。

XenMobile 允许您根据安全性要求阻止 Siri 和听写服务。

在 MAM 部署中，默认情况下，每个应用程序的阻止听写策略均为开，表示禁用设备的麦克风。如果要允许听写，则将其设置为关。可以在 XenMobile 控制台中的配置 **>** 应用程序下找到该策略。选择应用程序，单击编辑，然后单击 **iOS**。



在 MDM 部署中，还可以通过配置 **>** 设备策略下的 Siri 策略禁用 Siri。默认允许使用 Siri。



决定是否允许使用 Siri 和听写服务时，需要谨记以下几点事项：

- 根据 Apple 公开发布的信息，Apple 最长将保留 Siri 和听写语音数据两年时间。该数据将被分配一个随机编号以代表用户，并且语音文件与此随机编号相关联。有关详细信息，请参阅此 Wired 文章 Apple reveals how long Siri keeps your data（Apple 揭示 Siri 保留数据的时长）。
- 可以在任何 iOS 设备上转至设置 **>** 常规 **>** 键盘并轻按启用听写下方的链接来查看 Apple 隐私政策。

SSO 帐户设备策略

January 5, 2022

可在 XenMobile 中创建单点登录 (SSO) 帐户，使用户只需登录设备一次，即可从各种应用程序访问 XenMobile 和内部的公司资源。用户无需在设备上存储任何凭据。可以跨应用程序（包括 App Store 中的应用程序）使用此 SSO 帐户企业用户凭据。此策略专为 Kerberos 身份验证后端设计。

此策略仅适用于 iOS 7.0 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

- 帐户名称：输入显示在用户设备上的 Kerberos SSO 帐户名称。此字段为必填字段。
- **Kerberos** 主体名称：输入 Kerberos 主体名称。此字段为必填字段。

- 身份凭据 **(**密钥库或 **PKI** 凭据**)**：在此列表中，单击可用于在无需用户交互的情况下续订 Kerberos 凭据的可选身份凭据。
- **Kerberos** 领域：输入此策略的 Kerberos 领域。这通常是您的域名，所有字母均大写（例如，EXAMPLE.COM）。此字段为必填字段。
- 允许访问的 **URL**：对于需要 SSO 的每个 URL，单击添加，然后执行以下操作：
  - 允许访问的 **URL**：输入当用户从 iOS 设备访问时需要 SSO 的 URL。
    例如，当用户尝试浏览某个站点，且该 Web 站点发起 Kerberos 质询时：如果该站点不在此 URL 列表中，iOS 设备将不会通过提供 Kerberos 在以前的 Kerberos 登录中缓存到设备上的 Kerberos 令牌来尝试 SSO。URL 的主机部分必须完全匹配。例如，`https://shopping.apple.com` 有效，但 `https://*.apple.com` 无效。
    此外，如果 Kerberos 未基于主机匹配激活，URL 将仍然回退到标准 HTTP 调用。如果 URL 仅配置为使用 Kerberos 实现 SSO，这可能意味着一切，包括标准密码质询或 HTTP 错误。
  - 单击添加以添加 URL，或单击取消以取消添加 URL。
- 应用程序标识符：对于允许使用此登录的每个应用程序，单击添加，然后执行以下操作：
  - 应用程序标识符：输入允许使用此登录的应用程序的应用程序标识符。如果不添加任何应用程序标识符，此登录将匹配所有应用程序标识符。
  - 单击添加以添加应用程序标识符，或单击取消以取消添加应用程序标识符。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

存储加密设备策略

January 21, 2021

在 XenMobile 中创建存储加密设备策略，以加密内部存储和外部存储，并根据设备阻止用户在其设备上使用存储卡。

可以为 Samsung SAFE 和 Windows Phone 设备创建策略。每种平台需要一组不同的值，本文将对此进行详细介绍。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

必备条件

对于 Samsung SAFE 设备，请确保在配置此策略之前满足以下要求：

- 在用户设备上设置“锁屏”选项。
- 为用户设备插上电源并至少充电到 80%。
- 确保设备要求使用包含数字和字母或符号的密码。

配置 **Samsung SAFE** 设置

- 加密内部存储：选择是否加密用户设备上的内部存储。内部存储包括设备内存和内部存储器。默认值为开。
- 加密外部存储：选择是否加密用户设备上的外部存储。默认值为开。

Windows Phone 设置

- 要求设备加密：选择是否加密用户的设备。默认值为关。
- 禁用存储卡：选择是否阻止用户在其设备上使用存储卡。默认值为关。

应用商店设备策略

March 27, 2020

可以在 XenMobile 中创建一个策略，用于指定 iOS、Android 或 Windows Tablet 设备是否在设备的主屏幕上显示 XenMobile Store Web 剪辑。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

平台设置

对于配置的每个平台，选择是否在用户设备上显示 XenMobile Store Web 剪辑。默认值为开。

已订阅的日历设备策略

January 5, 2022

可以在 XenMobile 中添加一个设备策略，用于在 iOS 设备上将已订阅的日历添加日历列表中。www.apple.com/downloads/macosx/calendars 提供了您可以订阅的公共日历列表。

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。

必备条件

必须已经订阅某个日历，才能在用户设备上将其添加到已订阅的日历列表中。

iOS 设置

- 说明：输入日历的说明。此字段为必填字段。

- **URL**：输入日历 URL。可以输入 iCalendar 文件 (.ics) 的 `webcal://` URL 或 `https://` 链接。此字段为必填字段。
- 用户名：输入用户的登录名称。此字段为必填字段。
- 密码：输入可选用户密码。
- 使用 **SSL**：选择是否使用安全套接字层连接到日历。默认值为关。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

条款和条件设备策略

January 5, 2022

如果希望用户接受贵公司用于控制企业网络连接的特定政策，可以在 XenMobile 中创建条款和条件设备策略。当用户向 XenMobile 注册其设备时，系统会向其显示条款和条件，用户必须接受这些条款和条件才能注册其设备。拒绝这些条款和条件会取消注册过程。

如果贵公司具有国际用户，并且希望用户接受采用其本地语言描述的条款和条件，则可以采用不同的语言创建不同的条款和条件策略。必须为计划部署的每个平台和语言组合提供一个文件。对于 Android 和 iOS 设备，必须提供 PDF 文件。对于 Windows 设备，必须提供文本 (.txt) 文件和随附的图像文件。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 和 **Android** 设置

- 要导入的文件：单击浏览并导航到要导入的条款和条件文件所在位置，选择此文件。
- 默认条款和条件：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。默认值为关。

Windows Phone 和 **Windows Tablet** 设置

- 要导入的文件：单击浏览并导航到要导入的条款和条件文件所在位置，选择此文件。
- 图片：单击浏览并导航到要导入的图片文件所在位置，选择此文件。
- 默认条款和条件：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。默认值为关。

VPN 设备策略

January 5, 2022

VPN 设备策略用于配置虚拟专用网络 (VPN) 设置，这些设置使用户设备能够安全地连接到企业网络。可以为以下平台配置 VPN 设备策略。每种平台需要一组不同的值，本文将对此进行详细介绍。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

PerApp VPN 的要求

可以通过 VPN 策略为以下平台配置 PerApp VPN 功能：

- iOS
- macOS
- Android（旧版 DA）
- Samsung SAFE
- Samsung Knox

要为 Android Enterprise 设备配置 VPN，请为 Citrix SSO 应用创建 Android Enterprise 托管的配置设备策略。请参阅为 Android Enterprise 配置 VPN 配置文件。

PerApp VPN 选项可用于某些连接类型。下表显示了 PerApp VPN 选项何时可用。

平台	连接类型	备注
iOS	Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix SSO 或 Custom SSL。	
macOS	Cisco AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA 或 Custom SSL。	
Android（旧版 DA）	Citrix SSO	
Samsung SAFE	IPSEC、SSL	VPN 类型设置为通用
Samsung Knox	IPSEC、SSL	VPN 类型设置为通用

要使用 Citrix SSO 应用程序为 iOS 和 Android（旧版 DA）设备创建 PerApp VPN，则除了 VPN 策略配置外，您还需要执行额外的步骤。此外，必须验证是否满足以下必备条件：

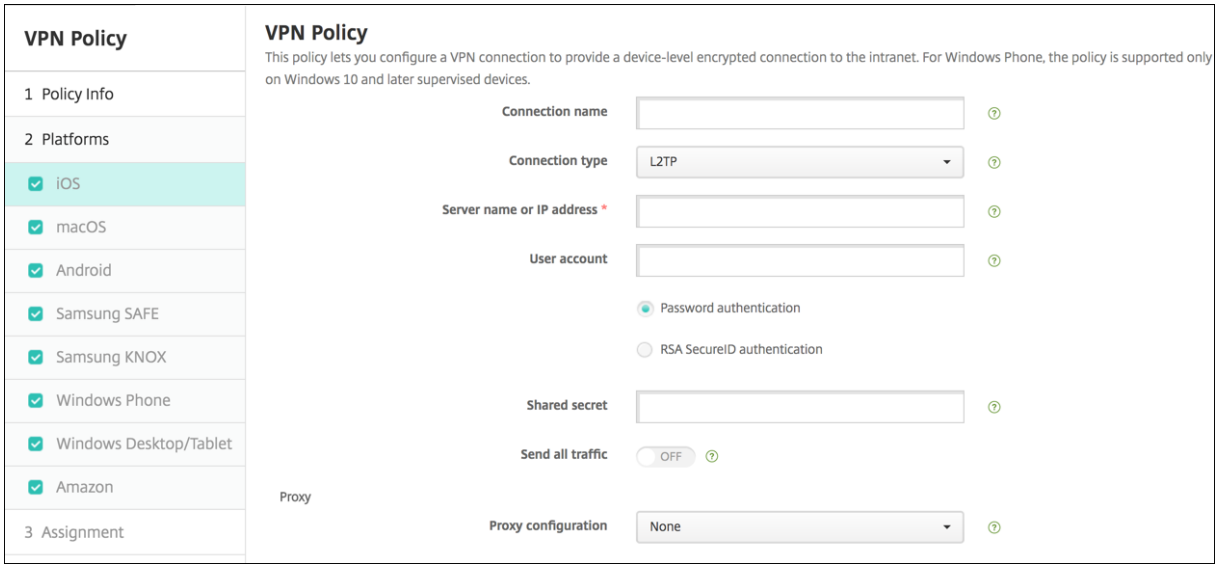
- 本地 Citrix Gateway
- 设备上安装了以下应用程序：
  - Citrix SSO
  - Citrix Secure Hub

使用 Citrix SSO 应用程序为 iOS 和 Android 设备配置 PerApp VPN 的一般工作流程如下：

1. 按本文中所述配置 VPN 设备策略。
   - 对于 *iOS*，请参阅为 iOS 配置 Citrix SSO 协议。通过 VPN 设备策略为 iOS 配置 Citrix SSO 协议后，还需要创建应用程序属性策略以将应用程序与 PerApp VPN 策略相关联。有关详细信息，请参阅配置 PerApp VPN。
     - 对于连接的身份验证类型字段，如果选择证书，则必须首先为 Endpoint Management 配置基于证书的身份验证。请参阅客户端证书或证书加域身份验证。
   - 对于 *Android*（旧版 *DA*），请参阅为 Android 配置 Citrix SSO 协议。
     - 对于连接的身份验证类型字段，如果选择证书或密码和证书，则必须首先为 Endpoint Management 配置基于证书的身份验证。请参阅客户端证书或证书加域身份验证。
2. 将 Citrix ADC 配置为接受来自 PerApp VPN 的流量。有关详细信息，请参阅 Citrix Gateway 上的完整 VPN 设置。

iOS 设置

> 准备将设备升级到 **iOS 12+**：
>
> 适用于 iOS 的 VPN 设备策略中的 Citrix VPN 连接类型不支持 iOS 12+。执行以下步骤可删除现有 VPN 设备策略并使用 Citrix SSO 连接类型创建 VPN 设备策略：
>
> 1. 删除适用于 iOS 的 VPN 设备策略。
> 2. 添加适用于 iOS 的 VPN 设备策略。重要设置：
>   - **Connection type** = **Citrix SSO**
>   - **Enable per-app VPN** = **On**
>   - **Provider type** = **Packet tunnel**
> 3. 添加适用于 iOS 的“应用程序属性”设备策略。对于 **PerApp VPN** 标识符，请选择 **iOS_VPN**。



- 连接名称：键入连接的名称。
- 连接类型：在列表中，选择将用于此连接的协议。默认值为 **L2TP**。
  - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
  - **PPTP**：点对点通道。
  - **IPSec**：企业 VPN 连接。
  - **Cisco Legacy AnyConnect**：此连接类型要求在用户设备上安装 Cisco Legacy AnyConnect VPN 客户端。Cisco 正在分阶段淘汰基于现已弃用的 VPN 框架的 Cisco Legacy AnyConnect 客户端。有关详细信息，请参阅支持文章 https://support.citrix.com/article/CTX227708。
    要使用当前的 Cisco AnyConnect 客户端，请使用连接类型自定义 **SSL**。对于必需的设置，请参阅本节中的“配置自定义 SSL 协议”。
  - **Juniper SSL**： Juniper Networks SSL VPN 客户端。
  - **F5 SSL**： F5 Networks SSL VPN 客户端。
  - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。
  - **Ariba VIA**： Ariba Networks Virtual Internet Access 客户端。
  - **IKEv2**（仅限 **iOS**）：仅限适用于 iOS 的 Internet 密钥交换 2 版。
  - **AlwaysOn IKEv2**：总是使用 IKEv2 进行访问。
  - **AlwaysOn IKEv2** 双配置：总是使用 IKEv2 双配置进行访问。
  - **Citrix SSO**：适用于 iOS 12 及更高版本的 Citrix SSO 客户端。
  - 自定义 **SSL**：自定义安全套接字层。捆绑包 ID 为 **com.cisco.anyconnect** 的 Cisco AnyConnect 客户端需要使用此连接类型。指定连接名称为 **Cisco AnyConnect**。还可以部署 VPN 策略并为 iOS 设备启用网络访问控制 (NAC) 过滤器。该过滤器阻止安装了不合规应用程序的设备建立 VPN 连接。配置需要 iOS VPN 策略的特定设置，如下面的 iOS 部分中所述。有关启用 NAC 过滤器所需的其他设置的详细信息，请参阅网络访问控制。

以下各节列出了前面每种连接类型的配置选项。

为 **iOS** 配置 **L2TP** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 选择密码身份验证或 **RSA SecurID** 身份验证。
- 共享机密：键入 IPsec 共享密钥。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **iOS** 配置 **PPTP** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 选择密码身份验证或 **RSA SecurID** 身份验证。
- 加密级别：在列表中，选择一种加密级别。默认设置为无。
  - 无：不使用加密。
  - 自动：使用服务器支持的最强加密级别。
  - 最大 **(128** 位**)**：始终使用 128 位加密。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **iOS** 配置 **IPsec** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择共享机密或证书以选择此连接的身份验证类型。默认值为共享机密。
- 如果启用共享机密，请配置以下设置：
  - 组名称：键入可选组名称。
  - 共享机密：键入可选共享密钥。
  - 使用混合身份验证：选择是否使用混合身份验证。利用混合身份验证，服务器首先向客户端验证自己的身份，然后客户端向服务器验证自己的身份。默认值为关。
  - 提示输入密码：选择是否在用户连接到网络时提示用户输入其密码。默认值为关。
- 如果启用证书，请配置以下设置：
  - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
  - 连接时提示输入 **PIN**：选择是否在连接到网络时需要用户输入其 PIN。默认值为关。
  - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。
- 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
- **Safari** 域：单击添加可添加 Safari 域名。

为 **iOS** 配置 **Cisco** 旧版 **AnyConnect** 协议

要从 Cisco 旧版 AnyConnect 客户端转换到新的 Cisco AnyConnect 客户端，请使用自定义 SSL 协议。

- 提供程序捆绑包标识符：对于 Legacy AnyConnect 客户端，捆绑包 ID 为 com.cisco.anyconnect.gui。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 组：键入可选组名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **Juniper SSL** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 领域：键入可选领域名称。
- 角色：键入可选角色名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN

连接是否自动触发。默认值为关。

- 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
- **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
  - 域：键入要添加的域。
  - 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **F5 SSL** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **SonicWALL** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 登录组或域：键入可选登录组或域。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。

        * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
        * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果将此选项设置为“开”，请配置以下设置：
    - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
    - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
    - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
        * 域：键入要添加的域。
        * 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **Ariba VIA** 协议

- 提供程序捆绑包标识符：如果您的 PerApp VPN 配置文件包含具有相同类型的多个 VPN 提供程序的应用程序的捆绑包标识符，请指定要在此处使用的提供程序。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
    - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
    - 如果启用证书，请配置以下设置：
        * 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
        * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
        * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
    - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
    - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
        * 域：键入要添加的域。
        * 单击保存以保存域，或者单击取消不保存域。

为 **iOS** 配置 **IKEv2** 协议

本节包括用于 IKEv2、AlwaysOn IKEv2 和 AlwaysOn IKEv2 双配置协议的设置。对于 AlwaysOn IKEv2 双配置协议，请为手机网络和 Wi-Fi 网络配置所有这些设置。

- 允许用户禁用自动连接：面向 AlwaysOn 协议。选择是否允许用户关闭与其设备上的网络的自动连接。默认值为关。
- 服务器的主机名或 **IP** 地址：键入 VPN 服务器的主机名或 IP 地址。

- 本地标识符： IKEv2 客户端的 FQDN 或 IP 地址。此字段为必填字段。
- 远程标识符： VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
- 设备身份验证：选择共享机密、证书或基于设备标识符的设备证书作为此连接的身份验证类型。默认值为共享机密。
  - 如果选择共享机密，请键入可选共享密钥。
  - 如果选择证书，请选择要使用的身份凭据。默认设置为无。
  - 如果选择基于设备标识符的设备证书，请选择要使用的设备标识类型。默认值为 **IMEI**。要使用此选项，请使用 REST API 批量导入证书。请参阅使用 REST API 将证书批量上载到 iOS 设备。仅当您选择 **Always On IKEv2**（始终启用 IKEv2）时才可用。
- 已启用扩展身份验证：选择是否启用扩展身份验证协议 (EAP)。如果选择开，请键入用户帐户和身份验证密码。
- 失效对等体检测时间间隔：选择联系对等设备以确保对等设备仍可访问的频率。默认设置为无。选项包括：
  - 无：禁用失效对等体检测。
  - 低：每 30 分钟联系一次对等体。
  - 中：每 10 分钟联系一次对等体。
  - 高： 1 分钟联系一次对等体。
- 禁用移动性和多宿主：选择是否禁用此功能。
- 使用 **IPv4/IPv6** 内部子网属性：选择是否启用此功能。
- 禁用重定向：选择是否禁用重定向。
- 设备在睡眠状态下启用 **NAT** 保持连接：面向 AlwaysOn 协议。保持连接数据包维护 IKEv2 连接的 NAT 映射。芯片在设备处于唤醒状态时定期发送这些数据包。如果此设置设为开，即使设备处于睡眠状态时，芯片也会发送保持连接数据包。通过 Wi-Fi 传输时，默认时间间隔为 20 秒，通过手机网络传输时为 110 秒。可以使用 NAT 保持连接时间间隔参数更改时间间隔。
- **NAT** 保持连接时间间隔 **(**秒**)**：默认值为 20 秒。
- 启用完全向前保密：选择是否启用此功能。
- **DNS** 服务器 **IP** 地址：可选。DNS 服务器 IP 地址字符串的列表。这些 IP 地址可以包括 IPv4 和 IPv6 地址的混合。单击添加可键入地址。
- 域名：可选。通道的主域。
- 搜索域：可选。用于完全限定单标签主机名的域字符串的列表。
- 将补充匹配域附加到解析程序列表：可选。确定是否将补充匹配域列表添加到解析程序的搜索域列表。默认值为开。

- 补充匹配域：可选。用于确定要使用 DNS 服务器地址中包含的 DNS 解析程序设置的 DNS 查询的域字符串的列表。此键将创建一个拆分 DNS 配置，在该配置中，只有某些域中的主机才能使用通道的 DNS 解析程序进行解析。不在此列表的其中一个域中的主机将使用系统的默认解析程序进行解析。

如果此参数包含一个空字符串，该字符串将为默认域。这说明了拆分通道配置如何将所有 DNS 查询先定向到 VPN DNS 服务器，然后再定向到主 DNS 服务器。如果 VPN 通道为网络的默认路由，列出的 DNS 服务器将成为默认解析程序。在这种情况下，补充匹配域列表将被忽略。

- **IKE SA** 参数和 **Child SA** 参数。为每个安全关联 (SA) 参数选项配置以下设置：
  - 加密算法：在此列表中，选择要使用的 IKE 加密算法。默认值为 **3DES**。
  - 完整性算法：在列表中，选择要使用的完整性算法。默认值为 **SHA1-96**。
  - **Diffie Hellman** 组：在列表中，选择 Diffie Hellman 组号。默认值为 **2**。
  - **IKE** 生存时间 **(**分钟**)**：键入 10 至 1440 之间的整数，表示 SA 生存时间（重新生成密钥时间间隔）。默认值为 **1440** 分钟。
- 服务异常：面向 AlwaysOn 协议。服务异常是指不通过 AlwaysOn VPN 运行的系统服务。请配置以下服务异常设置：
  - 语音邮件：在列表中，选择处理语音邮件异常的方式。默认值为允许通过通道传输流量。
  - **AirPrint**：在列表中，选择处理 AirPrint 异常的方式。默认值为允许通过通道传输流量。
  - 允许在 **VPN** 通道外部传输来自强制 **Web** 表格的流量：选择是否允许用户在 VPN 通道外部连接到公共热点。默认值为关。
  - 允许在 **VPN** 通道外部传输来自所有强制联网应用程序的流量：选择是否允许在 VPN 通道外部打开所有热点网络应用程序。默认值为关。
  - 强制联网应用程序捆绑包标识符：对于允许用户访问的每个热点网络应用程序捆绑包标识符，单击添加并键入热点网络应用程序捆绑包标识符。单击保存以保存该应用程序捆绑包标识符。
- **PerApp VPN**。为 IKEv2 连接类型配置这些设置。
  - 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：单击添加可添加 Safari 域名。
- 代理配置：选择 VPN 连接通过代理服务器进行路由的方式。默认值为无。

为 **iOS** 配置 **Citrix SSO** 协议

Citrix SSO 客户端可从 Apple Store（网址为 https://apps.apple.com/us/app/citrix-sso/id1333396910）获取。

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。

- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果将此选项设置为“开”，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
  - 提供程序类型：选择 PerApp VPN 是作为应用程序代理还是作为数据包通道提供。默认设置为应用程序代理。
  - 提供程序类型：设置为数据包通道。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。
- 自定义 **XML**：对于要添加的每个自定义 XML 参数，请单击添加并指定键/值对。可用参数如下：
  - **disableL3**：禁用系统级 VPN。仅允许使用 PerApp VPN。不需要任何值。
  - **useragent**：将目标为 VPN 插件客户端的任何 Citrix Gateway 策略与此设备策略相关联。对于插件发起的请求，此键的值会自动添加到 VPN 插件。

为 **iOS** 配置自定义 **SSL** 协议

要从 Cisco Legacy AnyConnect 客户端转换为 Cisco AnyConnect 客户端，请执行以下操作：

1. 通过自定义 SSL 协议配置 VPN 设备策略。将该策略部署到 iOS 设备。
2. 从 https://apps.apple.com/us/app/cisco-anyconnect/id1135064690 上载 Cisco AnyConnect 客户端，将该应用程序添加到 XenMobile，然后再将其部署到 iOS 设备。
3. 从 iOS 设备中删除旧 VPN 设备策略。

设置：

- 自定义 **SSL** 标识符 **(**反向 **DNS** 格式**)**：设置为捆绑包标识符。对于 Cisco AnyConnect 客户端，请使用 **com.cisco.anyconnect**。
- 提供程序捆绑包标识符：如果在自定义 **SSL** 标识符中指定的应用程序具有多个类型相同（应用程序代理或数据包通道）的 VPN 提供程序，请指定此捆绑包标识符。对于 Cisco AnyConnect 客户端，请使用 **com.cisco.anyconnect**。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。

  - 如果启用证书，请配置以下设置：
    * 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅为 iOS 配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果将此选项设置为“开”，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
  - 提供程序类型：提供程序类型指示提供程序是 VPN 服务还是代理服务。对于 VPN 服务，请选择数据包通道。对于代理服务，请选择应用程序代理。对于 Cisco AnyConnect 客户端，请选择数据包通道。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。
- 自定义 **XML**：对于要添加的每个自定义 XML 参数，请单击添加并执行以下操作：
  - 参数名称：键入要添加的参数的名称。
  - 值：键入与参数名称关联的值。
  - 单击保存以保存参数，或者单击取消不保存参数。

配置 **VPN** 设备策略以支持 **NAC**

1. 配置 NAC 过滤器所需的连接类型为自定义 **SSL**。
2. 指定连接名称为 **VPN**。
3. 对于自定义 **SSL** 标识符，请键入 **com.citrix.NetScalerGateway.ios.app**
4. 对于提供程序捆绑包标识符，请键入 **com.citrix.NetScalerGateway.ios.app.vpnplugin**

步骤 3 和 4 中的值来自 NAC 过滤所需的 Citrix SSO 安装。请勿配置身份验证密码。有关使用 NAC 功能的详细信息，请参阅网络访问控制。

为 **iOS** 配置 **“按需启用 VPN”** 选项

- 按需域：对于每个域以及当用户连接时要执行的关联操作，请单击添加并执行以下操作：
- 域：键入要添加的域。
- 操作：在列表中，选择其中一项可能采取的操作：
  - 始终建立：域始终触发 VPN 连接。
  - 从不建立：域从不触发 VPN 连接。
  - 必要时建立：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。
  - 单击保存以保存域，或者单击取消不保存域。
- 按需规则
  - 操作：在列表中，选择要采取的操作。默认值为 **EvaluateConnection**。可能的操作包括：

    * 允许：允许在触发时 VPN 按需进行连接。
    * 连接：无条件启动 VPN 连接。
    * 断开连接：删除 VPN 连接并且在规则匹配时不按需重新连接。
    * **EvaluateConnection**：评估每个连接的 ActionParameters 阵列。
    * 忽略：保持任何现有 VPN 连接，并且在规则匹配时不按需重新连接。
- **DNSDomainMatch**：对于要添加且设备的搜索域列表可以与之匹配的每个域，请单击添加并执行以下操作：
    * **DNS** 域：键入域名。可以使用通配符 “*” 前缀来匹配多个域。例如，*.example.com 匹配 mydomain.example.com、yourdomain.example.com 和 herdomain.example.com。
    * 单击保存以保存域，或者单击取消不保存域。
- **DNSServerAddressMatch**：对于要添加且网络的任何指定 DNS 服务器可以匹配的每个 IP 地址，请单击添加并执行以下操作：
    * **DNS** 服务器地址：键入要添加的 DNS 服务器地址。可以使用通配符 “*” 后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的所有 DNS 服务器。
    * 单击保存以保存 DNS 服务器地址，或者单击取消不保存 DNS 服务器地址。
- **InterfaceTypeMatch**：在列表中，选择使用的主要网络接口硬件的类型。默认值为未指定。可能的值包括：
    * 未指定：匹配任何网络接口硬件。此选项是默认选项。
    * 以太网：仅匹配以太网网络接口硬件。
    * **WiFi**：仅匹配 Wi-Fi 网络接口硬件。
    * 手机网络：仅匹配手机网络网络接口硬件。
- **SSIDMatch**：对于要添加且匹配当前网络的每个 SSID，请单击添加并执行以下操作。
    * **SSID**：键入要添加的 SSID。如果网络不是 Wi-Fi 网络，或者如果 SSID 未出现，匹配将失败。将此列表留空可匹配任何 SSID。
    * 单击保存以保存 SSID，或单击取消不保存 SSID。
- **URLStringProbe**：键入要提取的 URL。如果此 URL 在未经重定向的情况下成功提取，此规则匹配。
- **ActionParameters : Domains**：对于要添加且 EvaluateConnection 检查的每个域，请单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。
- **ActionParameters : DomainAction**：在列表中，选择指定的 **ActionParameters : Domains** 域的 **VPN** 行为。默认值为 **ConnectIfNeeded**。可能的操作包括：
    * 需要时连接：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。
    * **NeverConnect**：域从不触发 VPN 连接。
- **ActionParameters: RequiredDNSServers**：对于要用于解析指定域的每个 DNS 服务器 IP 地址，请单击添加并执行以下操作：
    * **DNS** 服务器：仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。键入要添加的 DNS 服务器。此服务器不需要属于设备的当前网络配置。如果无法访问 DNS 服务器，作

为响应，将建立 VPN 连接。此 DNS 服务器应该为内部 DNS 服务器或可信的外部 DNS 服务器。

* 单击保存以保存 DNS 服务器，或者单击取消不保存 DNS 服务器。

– **ActionParameters : RequiredURLStringProbe**：（可选）键入使用 GET 请求探查的 HTTP 或 HTTPS（首选）URL。如果无法解析 URL 的主机名、服务器无法访问或者服务器不响应，则建立 VPN 连接。仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。

– **OnDemandRules : XML content**：键入或复制并粘贴 XML 按需配置规则。

* 单击检查字典验证 XML 代码。如果 XML 有效，您将在 **XML** 内容文本框下方看到绿色文本的有效 XML。如果无效，您会看到一条用橙色文本描述错误的错误消息。

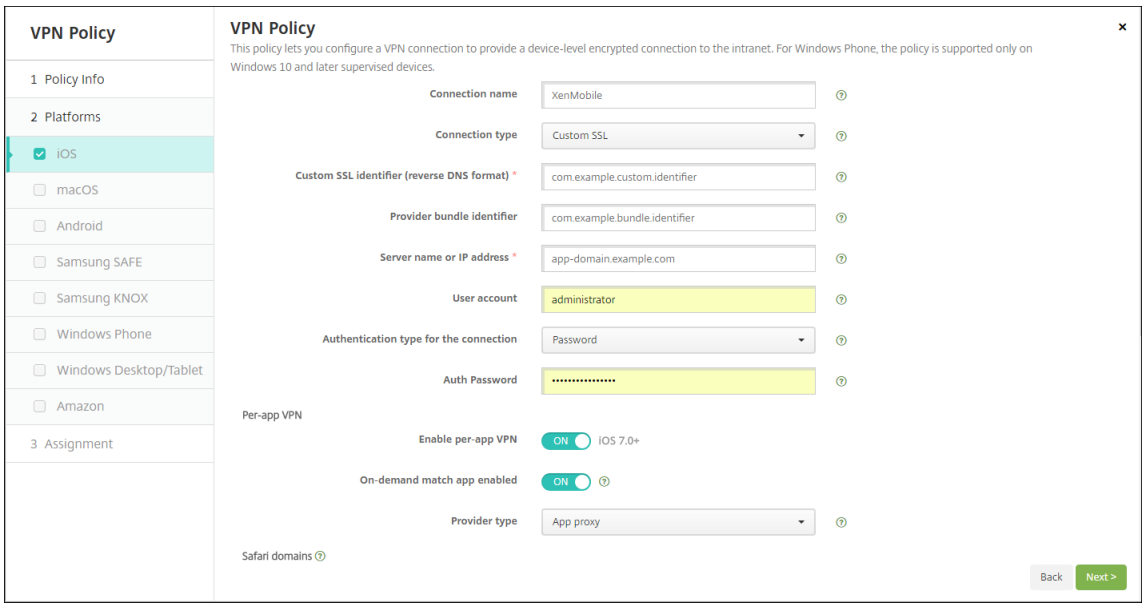
- 代理
  – 代理配置：在列表中，选择 VPN 连接通过代理服务器进行路由的方式。默认设置为无。
    * 如果启用手动，请配置以下设置：
      · 代理服务器的主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
      · 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。
      · 用户名：键入可选代理服务器用户名。
      · 密码：键入可选代理服务器密码。
    * 如果配置自动，请配置以下设置：
      · 代理服务器 **URL**：键入代理服务器的 URL。此字段为必填字段。
- 策略设置
  – 在策略设置下方的删除策略旁边，选择选择日期或删除前的持续时间 **(**小时**)**。
  – 如果选择选择日期，请单击日历以选择具体删除日期。
  – 在允许用户删除策略列表中，选择始终、需要密码或从不。
  – 如果选择需要密码，在 **Removal password**（删除密码）旁边，键入必需的密码。

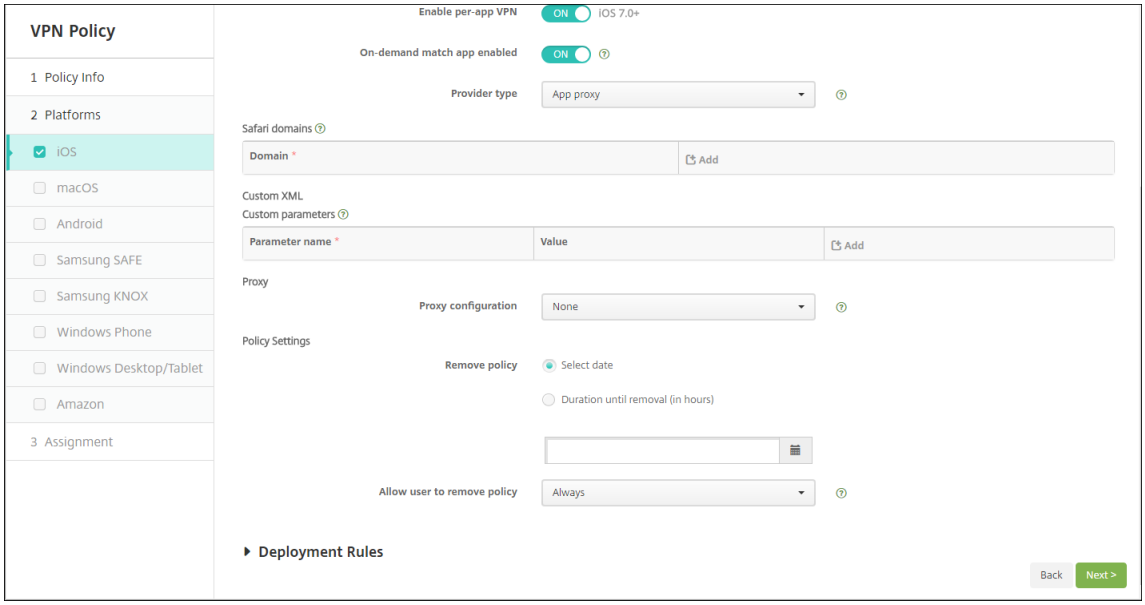
配置 **PerApp VPN**

iOS 的 PerApp VPN 选项适用于以下连接类型：Cisco 旧版 AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix VPN、Citrix SSO 和自定义 SSL。

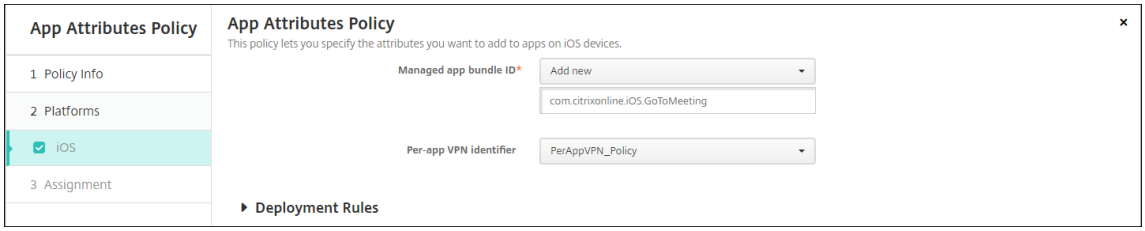
要配置 PerApp VPN，请执行以下操作：

1. 在配置 **>** 设备策略中，创建 VPN 策略。例如：





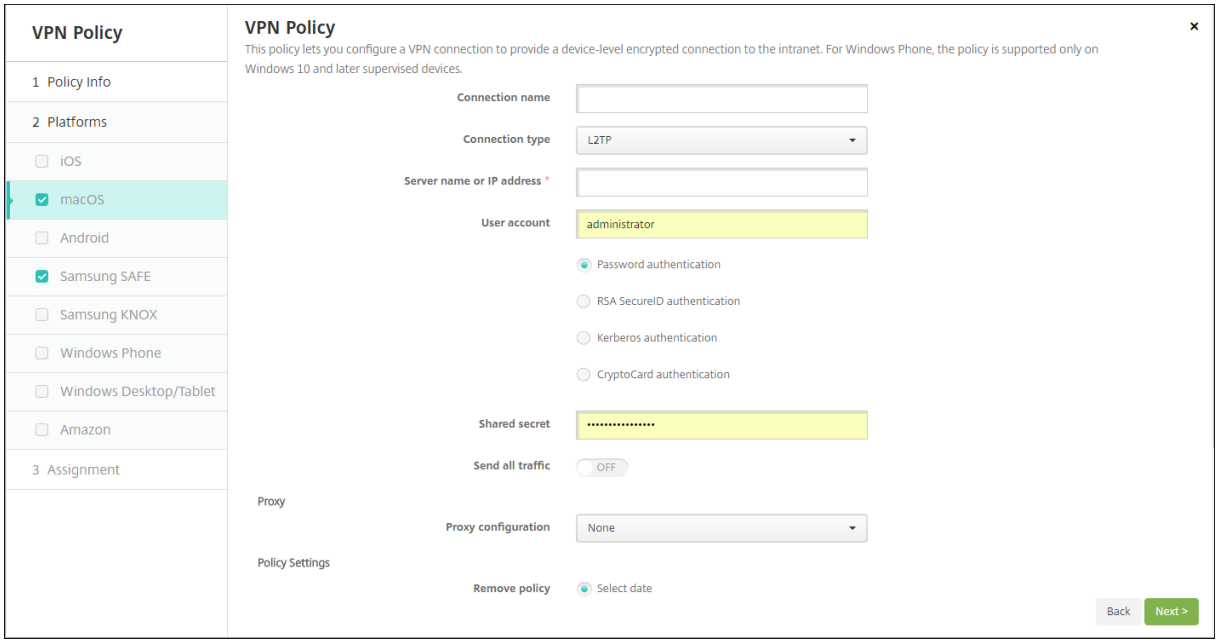
2. 在配置 **>** 设备策略中，创建应用程序属性策略以将应用程序与 PerApp VPN 策略相关联。对于 **PerApp VPN** 标识符，请选择在步骤 1 中创建的 VPN 策略的名称。对于托管应用程序捆绑包 **ID**，请从应用程序列表中进行选择，或者键入应用程序捆绑包 ID。（如果部署了 iOS 的应用程序清单策略，应用程序列表将包含应用程序。）



- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**

* 选择日期：单击日历可选择具体删除日期。
* 删除前的持续时间 (小时)：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置



- 连接名称：键入连接的名称。
- 连接类型：在列表中，选择将用于此连接的协议。默认值为 L2TP。
  - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
  - **PPTP**：点对点通道。
  - **IPSec**：企业 VPN 连接。
  - **Cisco AnyConnect**： Cisco AnyConnect VPN 客户端。
  - **Juniper SSL**： Juniper Networks SSL VPN 客户端。
  - **F5 SSL**： F5 Networks SSL VPN 客户端。
  - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。
  - **Ariba VIA**： Ariba Networks Virtual Internet Access 客户端。
  - **Citrix VPN**： Citrix VPN 客户端。
  - 自定义 **SSL**：自定义安全套接字层。

以下各节列出了前面每种连接类型的配置选项。

为 macOS 配置 L2TP 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。

- 选择密码身份验证、**RSA SecurID** 身份验证、**Kerberos** 身份验证或 **CryptoCard** 身份验证。默认值为密码身份验证。
- 共享机密：键入 IPsec 共享密钥。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **macOS** 配置 **PPTP** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 选择密码身份验证、**RSA SecurID** 身份验证、**Kerberos** 身份验证或 **CryptoCard** 身份验证。默认值为密码身份验证。
- 加密级别：选择所需的加密级别。默认设置为无。
  - 无：不使用加密。
  - 自动：使用服务器支持的最强加密级别。
  - 最大 **(128** 位**)**：始终使用 128 位加密。
- 发送所有流量：选择是否通过 VPN 发送所有流量。默认值为关。

为 **macOS** 配置 **IPsec** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择共享机密或证书以选择此连接的身份验证类型。默认值为共享机密。
  - 如果启用共享机密身份验证，请配置以下设置：
    - 组名称：键入可选组名称。
    - 共享机密：键入可选共享密钥。
    - 使用混合身份验证：选择是否使用混合身份验证。利用混合身份验证，服务器首先向客户端验证自己的身份，然后客户端向服务器验证自己的身份。默认值为关。
    - 提示输入密码：选择是否在用户连接到网络时提示用户输入其密码。默认值为关。
  - 如果启用证书身份验证，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    - 连接时提示输入 **PIN**：选择是否在连接到网络时需要用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置“按需启用 VPN”选项。

为 **macOS** 配置 **Cisco AnyConnect** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 组：键入可选组名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。

- 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
- 如果启用证书，请配置以下设置：
  - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
  - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
  - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置“按需启用 VPN”选项。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置 **Juniper SSL** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 领域：键入可选领域名称。
- 角色：键入可选角色名称。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    - 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    - 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    - 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置 **F5 SSL** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：

        * 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
        * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
        * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
    - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
    - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
        * 域：键入要添加的域。
        * 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置 **SonicWALL** 移动连接协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 登录组或域：键入可选登录组或域。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
    - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
    - 如果启用证书，请配置以下设置：
        * 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
        * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
        * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
    - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
    - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
        * 域：键入要添加的域。
        * 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置 **Ariba VIA** 协议

- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。
- 用户帐户：键入可选用户帐户。
- 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
    - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
    - 如果启用证书，请配置以下设置：
        * 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
        * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。

        * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置“按需启用 VPN”设置。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
  - 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。默认值为关。
  - **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
    * 域：键入要添加的域。
    * 单击保存以保存域，或者单击取消不保存域。

为 **macOS** 配置自定义 **SSL** 协议

- 自定义 **SSL** 标识符 **(**反向 **DNS** 格式**)**：以反向 DNS 格式键入 SSL 标识符。此字段为必填字段。
- 服务器名称或 **IP** 地址：键入 VPN 服务器的服务器名称或 IP 地址。此字段为必填字段。
- 用户帐户：键入可选用户帐户。
  - 连接的身份验证类型：在列表中，选择密码或证书以选择此连接的身份验证类型。默认值为密码。
  - 如果启用密码，请在身份验证密码字段中键入可选身份验证密码。
  - 如果启用证书，请配置以下设置：
    * 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
    * 连接时提示输入 **PIN**：选择是否在用户连接到网络时提示用户输入其 PIN。默认值为关。
    * 按需启用 **VPN**：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关。有关在按需启用 **VPN** 设置为开时配置设置的信息，请参阅配置“按需启用 VPN”设置。
  - **PerApp VPN**：选择是否启用 PerApp VPN。默认值为关。如果启用此选项，请配置以下设置：
    * 按需匹配应用程序已启用：选择当链接到 PerApp VPN 服务的应用程序发起网络通信时，PerApp VPN 连接是否自动触发。
    * **Safari** 域：对于要包含的可以触发 PerApp VPN 连接的每个 Safari 域，单击添加并执行以下操作：
      · 域：键入要添加的域。
      · 单击保存以保存域，或者单击取消不保存域。
- 自定义 **XML**：对于要添加的每个自定义 XML 参数，请单击添加并执行以下操作：
  - 参数名称：键入要添加的参数的名称。
  - 值：键入与参数名称关联的值。
  - 单击保存以保存域，或者单击取消不保存域。

配置 **“**按需启用 **VPN”** 选项

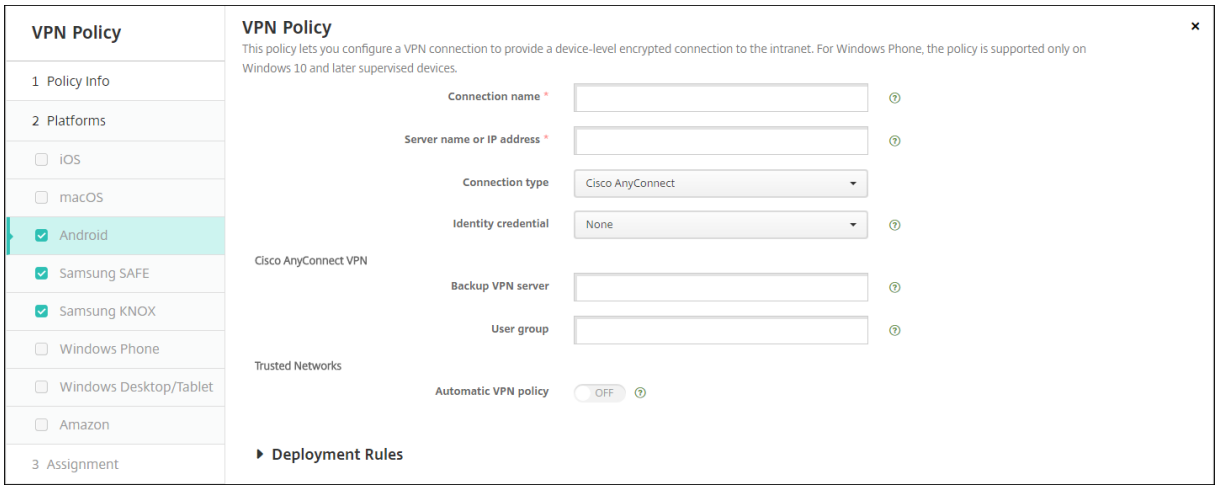
- 按需域：对于要添加的每个域以及当用户与之连接时要执行的关联操作，请单击添加并执行以下操作：
  - 域：键入要添加的域。
  - 操作：在列表中，选择其中一项可能采取的操作：
    * 始终建立：域始终触发 VPN 连接。
    * 从不建立：域从不触发 VPN 连接。

    - 必要时建立：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。
  - 单击保存以保存域，或者单击取消不保存域。
- 按需规则
  - 操作：在列表中，选择要采取的操作。默认值为 **EvaluateConnection**。可能的操作包括：
    - 允许：允许在触发时 VPN 按需进行连接。
    - 连接：无条件启动 VPN 连接。
    - 断开连接：删除 VPN 连接并且在规则匹配时不按需重新连接。
    - **EvaluateConnection**：评估每个连接的 **ActionParameters** 阵列。
    - 忽略：保持任何现有 VPN 连接，并且在规则匹配时不按需重新连接。
  - **DNSDomainMatch**：对于要添加且用户设备的搜索域列表可以与之匹配的每个域，请单击添加并执行以下操作：
    - **DNS** 域：键入域名。可以使用通配符 “*” 前缀来匹配多个域。例如，*.example.com 匹配 mydomain.example.com、yourdomain.example.com 和 herdomain.example.com。
    - 单击保存以保存域，或者单击取消不保存域。
  - **DNSServerAddressMatch**：对于要添加且网络的任何指定 DNS 服务器可以匹配的每个 IP 地址，请单击添加并执行以下操作：
    - **DNS** 服务器地址：键入要添加的 DNS 服务器地址。可以使用通配符 “*” 后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的所有 DNS 服务器。
    - 单击保存以保存 DNS 服务器地址，或者单击取消不保存 DNS 服务器地址。
  - **InterfaceTypeMatch**：在列表中，单击使用的主要网络接口硬件的类型。默认值为未指定。可能的值包括：
    - 未指定：匹配任何网络接口硬件。此选项是默认选项。
    - 以太网：仅匹配以太网网络接口硬件。
    - **WiFi**：仅匹配 Wi-Fi 网络接口硬件。
    - 手机网络：仅匹配手机网络网络接口硬件。
  - **SSIDMatch**：对于要添加且匹配当前网络的每个 SSID，请单击添加并执行以下操作。
    - **SSID**：键入要添加的 SSID。如果网络不是 Wi-Fi 网络，或者如果 SSID 未出现，匹配将失败。将此列表留空可匹配任何 SSID。
    - 单击保存以保存 SSID，或单击取消不保存 SSID。
  - **URLStringProbe**：键入要提取的 URL。如果此 URL 在未经重定向的情况下成功提取，此规则匹配。
  - **ActionParameters : Domains**：对于要添加且 EvaluateConnection 检查的每个域，请单击添加并执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。
  - **ActionParameters : DomainAction**：在列表中，选择指定的 **ActionParameters : Domains** 域的 **VPN** 行为。默认值为 **ConnectIfNeeded**。可能的操作包括：
    - 需要时连接：如果域名解析失败，域将触发 VPN 连接尝试。如果 DNS 服务器无法解析域、重定向到其他服务器或超时，则会失败。

    * **NeverConnect**：域从不触发 VPN 连接。
  - **ActionParameters: RequiredDNSServers**：对于要用于解析指定域的每个 DNS 服务器 IP 地址，请单击添加并执行以下操作：
    * **DNS** 服务器：仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。键入要添加的 DNS 服务器。此服务器不需要属于设备的当前网络配置。如果无法访问 DNS 服务器，作为响应，将建立 VPN 连接。此 DNS 服务器必须为内部 DNS 服务器或可信的外部 DNS 服务器。
    * 单击保存以保存 DNS 服务器，或者单击取消不保存 DNS 服务器。
  - **ActionParameters : RequiredURLStringProbe**：（可选）键入使用 GET 请求探查的 HTTP 或 HTTPS（首选）URL。如果无法解析 URL 的主机名、服务器无法访问或者服务器不响应，则建立 VPN 连接。仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。
  - **OnDemandRules : XML** 内容：键入或复制并粘贴 XML 按需配置规则。
    * 单击检查字典验证 XML 代码。如果 XML 有效，您将在 **XML** 内容文本框下方看到绿色文本的有效 XML。如果无效，您会看到一条用橙色文本描述错误的错误消息。

- 代理
  - 代理配置：在列表中，选择 VPN 连接通过代理服务器进行路由的方式。默认设置为无。
    * 如果启用手动，请配置以下设置：
      · 代理服务器的主机名或 **IP** 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
      · 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。
      · 用户名：键入可选代理服务器用户名。
      · 密码：键入可选代理服务器密码。
    * 如果配置自动，请配置以下设置：
      · 代理服务器 **URL**：键入代理服务器的 URL。此字段为必填字段。

Android 设置



为 **Android** 配置 **Cisco AnyConnect VPN** 协议

- 连接名称：输入 Cisco AnyConnect VPN 连接的名称。此字段为必填字段。

- 服务器名称或 **IP** 地址：键入 VPN 服务器的名称或 IP 地址。此字段为必填字段。
- 身份凭据：在列表中，选择身份凭据。
- 备份 **VPN** 服务器：键入备份 VPN 服务器信息。
- 用户组：键入用户组信息。
- 可信网络
  - 自动 **VPN** 策略：启用或禁用此选项，以设置 VPN 响应可信网络和不可信网络的方式。如果启用，请配置以下设置：
    - 可信网络策略：在列表中，选择所需的策略。默认值为断开连接。可能的选项包括：
      - 断开连接：客户端终止可信网络中的 VPN 连接。这是默认设置。
      - 连接：客户端在可信网络中启动 VPN 连接。
      - 不执行任何操作：客户端不执行任何操作。
      - 暂停：用户在可信网络外部建立 VPN 会话，然后进入配置为可信的网络时，VPN 会话将挂起。用户再次离开可信网络时，会话恢复。此设置无需在离开可信网络后建立新的 VPN 会话。
    - 不可信网络策略：在列表中，选择所需的策略。默认值为连接。可能的选项包括：
      - 连接：客户端在不可信网络中启动 VPN 连接。
      - 不执行任何操作：客户端在不可信网络中启动 VPN 连接。此选项将禁用始终启用 VPN。
  - 可信域：对于客户端位于可信网络时网络接口拥有的每个域后缀，请单击添加以执行以下操作：
    - 域：键入要添加的域。
    - 单击保存以保存域，或者单击取消不保存域。
  - 可信服务器：对于客户端位于可信网络时网络接口拥有的每个服务器地址，请单击添加并执行以下操作：
    - 服务器：键入要添加的服务器。
    - 单击保存以保存服务器，或者单击取消不保存服务器。

为 **Android** 配置 **Citrix SSO** 协议

- 连接名称：键入 VPN 连接的名称。此字段为必填字段。
- 服务器名称或 **IP** 地址：键入 Citrix Gateway 的 FQDN 或 IP 地址。
- 连接的身份验证类型：选择身份验证类型并填写针对该类型显示的以下字段中的任何字段：
  - 用户名和密码：键入身份验证类型密码或密码和证书的 VPN 凭据。可选。如果未提供 VPN 凭据，Citrix VPN 应用程序将提示输入用户名和密码。
  - 身份凭据：针对身份验证类型证书或密码和证书显示。在列表中，选择身份凭据。
- 启用 **PerApp VPN**：选择是否启用 PerApp VPN。如果未启用 PerApp VPN，所有流量都将通过 Citrix VPN 通道传输。如果启用 PerApp VPN，请指定以下设置。默认值为关。
  - 白名单或黑名单：如果选择白名单，所有允许运行的应用程序都将通过此 VPN 传输。如果选择黑名单，除阻止列表通道中的应用程序以外的所有应用程序都将通过此 VPN 传输。

> 注意：
>
> XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

  - 应用程序列表：指定允许或阻止的应用程序。单击添加，然后键入以逗号分隔的应用程序软件包名称的列表。

- 自定义 **XML**：单击添加，然后键入自定义参数。XenMobile 支持 Citrix VPN 的以下参数：
  - 禁用用户配置文件：可选。要启用此参数，请键入 **Yes** 作为值。如果启用了此参数，XenMobile 将不显示用户添加的 VPN 连接，并且用户无法添加连接。此设置属于全局限制，适用于所有 VPN 配置文件。
  - **userAgent**：字符串值。可以指定要在每个 HTTP 请求中发送的自定义用户代理字符串。指定的用户代理字符串附加到现有 Citrix VPN 用户代理。

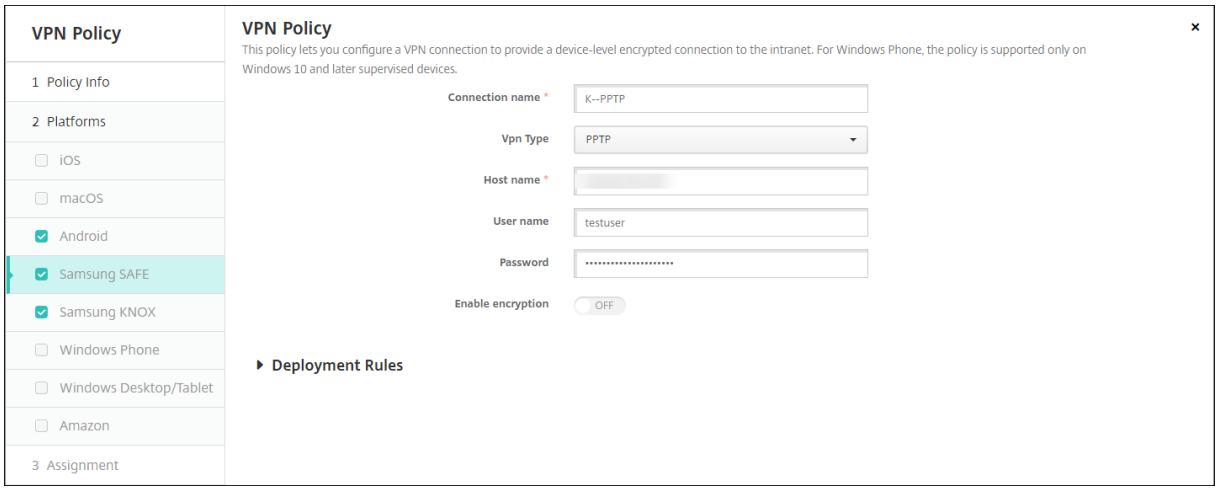
配置 **VPN** 以支持 **NAC**

1. 使用连接类型自定义 **SSL** 配置 NAC 过滤器。
2. 指定连接名称为 **VPN**。
3. 对于自定义 **XML**，请单击添加并执行以下操作：
   - 参数名称：键入 **XenMobileDeviceId**。此字段是用于根据 XenMobile 中的设备注册进行 NAC 检查的设备 ID。如果 XenMobile 注册并管理设备，则允许建立 VPN 连接。否则，在 VPN 建立时将拒绝身份验证。
   - 值：键入 **DeviceID_${device.id}**，该值是参数 **XenMobileDeviceId** 的值。
   - 单击保存保存参数。

为 **Android Enterprise** 配置 **VPN**

要为 Android Enterprise 设备配置 VPN，请为 Citrix SSO 应用创建 Android Enterprise 托管的配置设备策略。请参阅为 Android Enterprise 配置 VPN 配置文件。

Samsung SAFE 设置



- 连接名称：键入连接的名称。
- **VPN** 类型：在列表中，选择将用于此连接的协议。默认值为使用预共享密钥的 **L2TP**。可能的选项包括：
  - 使用预共享密钥的 **L2TP**：使用预共享密钥身份验证的第二层通道协议。这是默认设置。
  - 使用证书的 **L2TP**：使用证书的第二层通道协议。
  - **PPTP**：点对点通道。
  - 企业：企业 VPN 连接。适用于 SAFE 2.0 之前的版本。
  - 通用：通用 VPN 连接。适用于 SAFE 2.0 或更高版本。

为 Samsung SAFE 配置使用预共享密钥的 L2TP 协议

- 主机名：键入 VPN 主机的名称。必须使用此选项。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- 预共享密钥：键入预共享密钥。必须使用此选项。

为 Samsung SAFE 配置使用证书的 L2TP 协议

- 主机名：键入 VPN 主机的名称。必须使用此选项。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。

为 Samsung SAFE 配置 PPTP 协议

- 主机名：键入 VPN 主机的名称。必须使用此选项。
- 用户名：键入可选用户名。
- 密码：键入可选密码。

- 启用加密：选择是否在 VPN 连接上启用加密。

为 **Samsung SAFE** 配置企业协议

- 主机名：键入 VPN 主机的名称。必须使用此选项。
- 启用备份服务器：选择是否启用备份 VPN 服务器。如果启用，请在备份 **VPN** 服务器上，键入备份 VPN 服务器的 FQDN 或 IP 地址。
- 启用用户身份验证：选择是否需要进行用户身份验证。如果启用，请配置以下设置：
  - 用户名：键入用户名。
  - 密码：键入用户密码。
- 组名称：键入可选组名称。
- 身份验证方法：在列表中，选择要使用的身份验证方法。可能的选项包括：
  - 证书：使用证书身份验证。这是默认设置。如果选择此选项，请在身份凭据列表中，选择要使用的凭据。默认设置为无。
  - 预共享密钥：使用预共享密钥。如果选择此选项，请在预共享密钥字段中，键入共享密钥。
  - 混合 **RSA**：使用采用 RSA 证书的混合身份验证。
  - **EAP MD5**： EAP 对等体向 EAP 服务器进行身份验证，但是不相互验证身份。
  - **EAP MSCHAPv2**：使用 Microsoft 的质询-握手身份验证相互验证身份。
- **CA** 证书：在列表中，选择要使用的证书。默认设置为无。
- 启用默认路由：选择是否启用到 VPN 服务器的默认路由。默认值为关。
- 启用智能卡身份验证：选择是否允许用户使用智能卡进行身份验证。默认值为关。
- 启用移动选项：选择是否启用移动选项。默认值为关。
- **Diffie-Hellman** 组值 **(**密钥强度**)**：在列表中，选择要使用的密钥强度。默认值为 0。
- 拆分通道类型：在列表中，选择要使用的拆分通道类型。默认值为自动。可能的选项包括：
  - 自动：自动使用拆分通道。
  - 手动：通过在 VPN 服务器上指定的 IP 地址和端口使用拆分通道。
  - 已禁用：不使用拆分通道。
- **SuiteB** 类型：在列表中，选择要使用的 NSA Suite B 加密级别。默认值为 **GCM-128**。可能的选项包括：
  - **GCM-128**：使用 128 位 AES-GCM 加密。
  - **GCM-256**：使用 256 位 AES-GCM 加密。
  - **GMAC-128**：使用 128 位 AES-GMAC 加密。
  - **GMAC-256**：使用 256 位 AES-GMAC 加密。
  - 无：不使用加密。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

为 **Samsung SAFE** 配置通用协议

- 主机名：键入 VPN 主机的名称。必须使用此选项。

- 启用用户身份验证：选择是否需要进行用户身份验证。如果启用，请在密码中，键入用户密码。
- 用户名：键入用户名。
- 包名称代理 **VPN**：在设备上安装的 VPN 的包名称或 ID，例如 Mocana 或 Pulse Secure。
- **VPN** 连接类型：在列表中，选择 **IPSEC** 或 **SSL** 以选择要使用的连接类型。默认值为 **IPSEC**。以下各节介绍了每种连接类型的配置设置。

为 **Samsung SAFE** 配置 **IPSEC** 连接类型设置

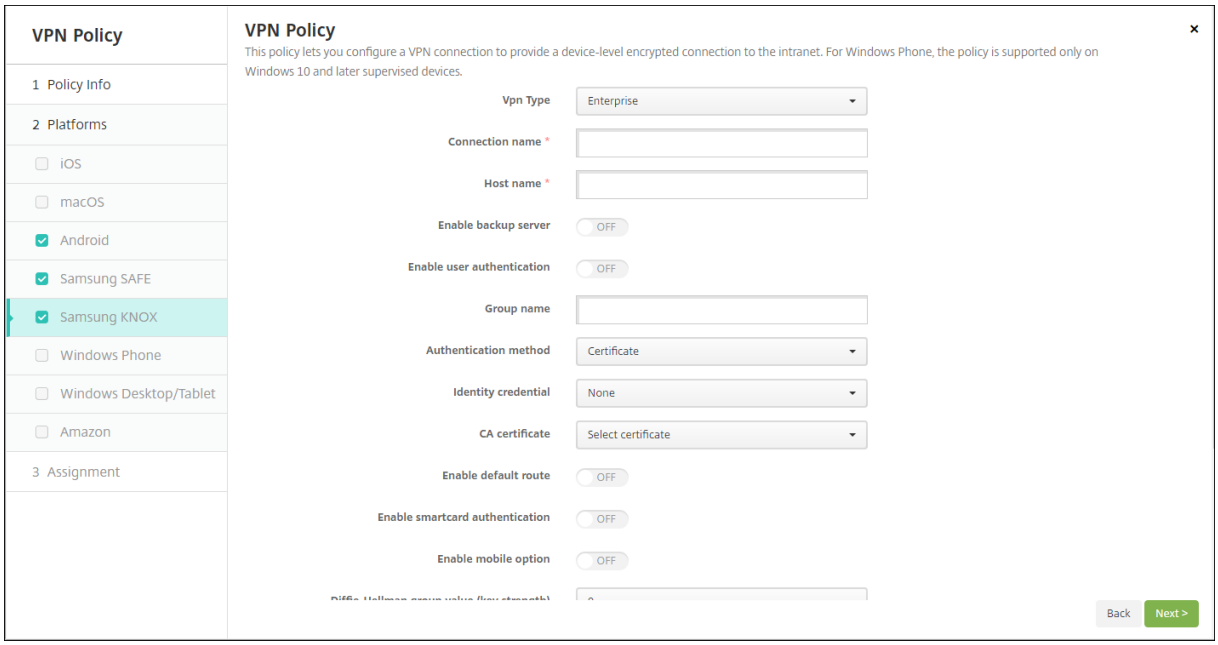
- 标识：键入此配置的可选标识符。
- **IPsec** 组 **ID** 类型：在列表中，选择要使用的 IPsec 组 ID 类型。默认值为默认值。可能的选项包括：
  - 默认值
  - **IPv4** 地址
  - 完全限定域名 **(FQDN)**
  - 用户 **FQDN**
  - **IKE** 密钥 **ID**
- **IKE** 版本：在列表中，选择要使用的 Internet 密钥交换版本。默认值为 **IKEv1**。
- 身份验证方法：在列表中，选择要使用的身份验证方法。默认值为证书。可能的选项包括：
  - 证书：使用证书身份验证。如果选择此选项，请在身份凭据列表中，选择要使用的凭据。默认设置为无。
  - 预共享密钥：使用预共享密钥。如果选择此选项，请在预共享密钥字段中，键入共享密钥。
  - 混合 **RSA**：使用采用 RSA 证书的混合身份验证。
  - **EAP MD5**： EAP 对等体向 EAP 服务器进行身份验证，但是不相互验证身份。
  - **EAP MSCHAPv2**：使用 Microsoft 的质询-握手身份验证相互验证身份。
  - 基于 **CAC** 的身份验证：使用通用访问卡 (CAC) 进行身份验证。
- 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
- **CA** 证书：在列表中，选择要使用的证书。
- 启用失效对等体检测：选择是否联系对等体以确定其仍然有效。默认值为关。
- 启用默认路由：选择是否启用到 VPN 服务器的默认路由。
- 启用移动选项：选择是否启用移动选项。
- **IKE** 生存时间 **(**分钟**)**：键入必须重新建立 VPN 连接之前经过的分钟数。默认值为 1440 分钟（24 小时）。
- **ipsec** 生存时间 **(**分钟**)**：键入必须重新建立 VPN 连接之前经过的分钟数。默认值为 1440 分钟（24 小时）。
- **Diffie-Hellman** 组值 **(**密钥强度**)**：在列表中，选择要使用的密钥强度。默认值为 **0**。
- **IKE** 阶段 **1** 密钥交换模式：选择主模式或积极模式作为 IKE 阶段 1 协商模式。默认值为主模式。
  - 主模式：协商期间不会向潜在攻击者泄露任何信息，但是速度低于积极模式。
  - 积极模式：协商期间会向潜在攻击者泄露某些信息（例如，协商对等体的身份），但是速度高于主模式。
- 完全向前保密 **(PFS)** 值：选择是否使用 PFS 以要求使用新密钥交换重新协商连接。
- 拆分通道类型：在列表中，选择要使用的拆分通道类型。可能的选项包括：
  - 自动：自动使用拆分通道。
  - 手动：通过在 VPN 服务器上指定的 IP 地址和端口使用拆分通道。
  - 已禁用：不使用拆分通道。
- **IPSEC** 加密算法： IPsec 协议使用的 VPN 配置。

- **IKE** 加密算法： IPsec 协议使用的 VPN 配置。
- **IKE** 完整性算法： IPsec 协议使用的 VPN 配置。
- 供应商：与 Knox API 通信的通用代理的个人配置文件。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。
- **PerApp VPN**：对于要添加的每个 PerApp VPN，请单击添加并执行以下操作：
  - **PerApp VPN**：应用程序进行通信时使用的 VPN 配置。
  - 单击保存以保存 PerApp VPN，或者单击取消不保存 PerApp VPN。

为 **Samsung SAFE** 配置 **SSL** 连接类型设置

- 身份验证方法：在列表中，选择要使用的身份验证方法。默认值为不适用。可能的选项包括：
  - 不适用
  - 证书：使用证书身份验证。如果选择此选项，请在身份凭据列表中，选择要使用的凭据。默认设置为无。
  - 基于 **CAC** 的身份验证：使用通用访问卡 (CAC) 进行身份验证。
- **CA** 证书：在列表中，选择要使用的证书。
- 启用默认路由：选择是否启用到 VPN 服务器的默认路由。
- 启用移动选项：选择是否启用移动选项。
- 拆分通道类型：在列表中，选择要使用的拆分通道类型。可能的选项包括：
  - 自动：自动使用拆分通道。
  - 手动：通过在 VPN 服务器上指定的 IP 地址和端口使用拆分通道。
  - 已禁用：不使用拆分通道。
- **SSL** 算法：键入用于客户端-服务器协商的 SSL 算法。
- 供应商：与 Knox API 通信的通用代理的个人配置文件。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。
- **PerApp VPN**：对于要添加的每个 PerApp VPN，请单击添加并执行以下操作：
  - **PerApp VPN**：应用程序进行通信时使用的 VPN 配置。
  - 单击保存以保存 PerApp VPN，或者单击取消不保存 PerApp VPN。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Samsung Knox 设置



为 Samsung Knox 配置任何策略时，策略仅在 Samsung Knox 容器内应用。

- **VPN** 类型：在列表中，选择要配置的 VPN 连接类型。连接可以是企业（适用于 Knox 2.0 之前的版本）或通用（适用于 Knox 2.0 或更高版本）。默认值为企业。

以下各节列出了前面每种连接类型的配置选项。

为 Samsung Knox 配置企业协议

- 连接名称：键入连接的名称。此字段为必填字段。
- 主机名：键入 VPN 主机的名称。必须使用此选项。
- 启用备份服务器：选择是否启用备份 VPN 服务器。如果启用，请在备份 **VPN** 服务器上，键入备份 VPN 服务器的 FQDN 或 IP 地址。
- 启用用户身份验证：选择是否需要进行用户身份验证。如果启用，请配置以下设置：
  - 用户名：键入用户名。
  - 密码：键入用户密码。
- 组名称：键入可选组名称。
- 身份验证方法：在列表中，选择要使用的身份验证方法。可能的选项包括：
  - 证书：使用证书身份验证。对于证书身份验证，还要从身份凭据列表中选择要使用的凭据。
  - 预共享密钥：使用预共享密钥。如果选择此选项，请在预共享密钥字段中，键入共享密钥。
  - 混合 **RSA**：使用采用 RSA 证书的混合身份验证。
  - **EAP MD5**： EAP 对等体向 EAP 服务器进行身份验证，但是不相互验证身份。
  - **EAP MSCHAPv2**：使用 Microsoft 的质询-握手身份验证相互验证身份。
- **CA** 证书：在列表中，选择要使用的证书。

- 启用默认路由：选择是否启用到 VPN 服务器的默认路由。
- 启用智能卡身份验证：选择是否允许用户使用智能卡进行身份验证。默认值为关。
- 启用移动选项：选择是否启用移动选项。
- **Diffie-Hellman** 组值 **(**密钥强度**)**：在列表中，选择要使用的密钥强度。默认值为 **0**。
- 拆分通道类型：在列表中，选择要使用的拆分通道类型。可能的选项包括：
  - 自动：自动使用拆分通道。
  - 手动：通过在 VPN 服务器上指定的 IP 地址和端口使用拆分通道。
  - 已禁用：不使用拆分通道。
- **SuiteB** 类型：在列表中，选择要使用的 NSA Suite B 加密级别。可能的选项包括：
  - **GCM-128**：使用 128 位 AES-GCM 加密，此设置为默认设置。
  - **GCM-256**：使用 256 位 AES-GCM 加密。
  - **GMAC-128**：使用 128 位 AES-GMAC 加密。
  - **GMAC-256**：使用 256 位 AES-GMAC 加密。
  - 无：不使用加密。
- 转发路由：如果您的企业 VPN 服务器支持多个路由表，请单击添加以添加其他可选转发路由。

为 **Samsung Knox** 配置通用协议

- 连接名称：键入连接的名称。此字段为必填字段。
- 包名称代理 **VPN**：在设备上安装的 VPN 的包名称或 ID，例如 Mocana 或 Pulse Secure。
- 主机名：键入 VPN 主机的名称。必须使用此选项。
- 启用用户身份验证：选择是否需要进行用户身份验证。如果启用，请配置以下设置：
  - 用户名：键入用户名。
  - 密码：键入用户密码。
- 标识：键入此配置的可选标识符。仅在 **VPN** 连接类型 **= IPSEC** 时适用。
- **VPN** 连接类型：在列表中，选择 **IPSEC** 或 **SSL** 以选择要使用的连接类型。默认值为 **IPSEC**。以下各节介绍了每种连接类型的配置设置。
- 配置 **IPSEC** 连接设置
  - **IPsec** 组 **ID** 类型：在列表中，选择要使用的 IPsec 组 ID 类型。默认值为默认值。可能的选项包括：
    - 默认值
    - **IPv4** 地址
    - 完全限定域名 **(FQDN)**
    - 用户 **FQDN**
    - **IKE** 密钥 **ID**
  - **IKE** 版本：在列表中，选择要使用的 Internet 密钥交换版本。默认值为 **IKEv1**。
  - 身份验证方法：在列表中，选择要使用的身份验证方法。默认值为证书。可能的选项包括：
    - 证书：使用证书身份验证。如果选择此选项，请在身份凭据列表中，选择要使用的凭据。默认设置为无。
    - 预共享密钥：使用预共享密钥。如果选择此选项，请在预共享密钥字段中，键入共享密钥。
    - 混合 **RSA**：使用采用 RSA 证书的混合身份验证。

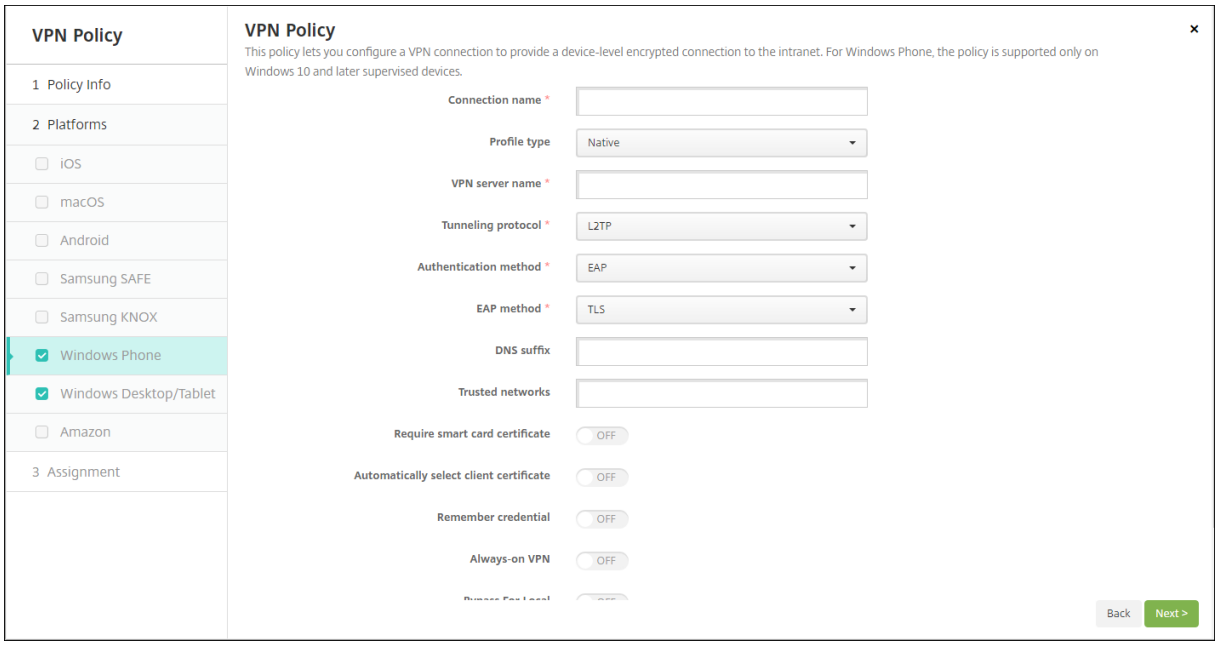
        * **EAP MD5**： EAP 对等体向 EAP 服务器进行身份验证，但是不相互验证身份。
        * **EAP MSCHAPv2**：使用 Microsoft 的质询-握手身份验证相互验证身份。
        * 基于 **CAC** 的身份验证：使用通用访问卡 (CAC) 进行身份验证。
    - **CA** 证书：在列表中，选择要使用的证书。
    - 启用失效对等体检测：选择是否联系对等体以确定其仍然有效。默认值为关。
    - 启用默认路由：选择是否启用到 VPN 服务器的默认路由。
    - 启用移动选项：选择是否启用移动选项。
    - **IKE** 生存时间 **(**分钟**)**：键入必须重新建立 VPN 连接之前经过的分钟数。默认值为 1440 分钟（24 小时）。
    - **ipsec** 生存时间 **(**分钟**)**：键入必须重新建立 VPN 连接之前经过的分钟数。默认值为 1440 分钟（24 小时）。
    - **Diffie-Hellman** 组值 **(**密钥强度**)**：在列表中，选择要使用的密钥强度。默认值为 **0**。
    - **IKE** 阶段 **1** 密钥交换模式：选择主模式或积极模式作为 IKE 阶段 1 协商模式。默认值为主模式。
        * 主模式：协商期间不会向潜在攻击者泄露任何信息，但是速度低于积极模式。
        * 积极模式：协商期间会向潜在攻击者泄露某些信息（例如，协商对等体的身份），但是速度高于主模式。
    - 完全向前保密 **(PFS)** 值：选择是否使用 PFS 以要求使用新密钥交换重新协商连接。
    - 拆分通道类型：在列表中，选择要使用的拆分通道类型。可能的选项包括：
        * 自动：自动使用拆分通道。
        * 手动：通过在 VPN 服务器上指定的 IP 地址和端口使用拆分通道。
        * 已禁用：不使用拆分通道。
    - **SuiteB** 类型：在列表中，选择要使用的 NSA Suite B 加密级别。默认值为 **GCM-128**。可能的选项包括：
        * **GCM-128**：使用 128 位 AES-GCM 加密。
        * **GCM-256**：使用 256 位 AES-GCM 加密。
        * **GMAC-128**：使用 128 位 AES-GMAC 加密。
        * **GMAC-256**：使用 256 位 AES-GMAC 加密。
        * 无：不使用加密。
    - **IPSEC** 加密算法： IPsec 协议使用的 VPN 配置。
    - **IKE** 加密算法： IPsec 协议使用的 VPN 配置。
    - **IKE** 完整性算法： IPsec 协议使用的 VPN 配置。
    - **Knox**：仅适用于 Samsung Knox 的配置。
    - 供应商：与 Knox API 通信的通用代理的个人配置文件。
    - 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
        * 转发路由：键入转发路由的 IP 地址。
        * 单击保存以保存路由，或者单击取消不保存路由。
    - **PerApp VPN**：对于要添加的每个 PerApp VPN，请单击添加并执行以下操作：
        * **PerApp VPN**：应用程序进行通信时使用的 VPN 配置。
        * 单击保存以保存 PerApp VPN，或者单击取消不保存 PerApp VPN。
- 配置 **SSL** 连接设置
    - 身份验证方法：在列表中，单击要使用的身份验证方法。可能的选项包括：
        * 不适用：不应用任何身份验证方法。这是默认设置。
        * 证书：使用证书身份验证。这是默认设置。如果选择此选项，请在身份凭据列表中，选择要使用的凭

据。默认设置为无。

  * 基于 **CAC** 的身份验证：使用通用访问卡 (CAC) 进行身份验证。

- **CA** 证书：在列表中，选择要使用的证书。
- 启用默认路由：选择是否启用到 VPN 服务器的默认路由。
- 启用移动选项：选择是否启用移动选项。
- 拆分通道类型：在列表中，选择要使用的拆分通道类型。可能的选项包括：
  * 自动：自动使用拆分通道。
  * 手动：通过指定的 IP 地址和端口使用拆分通道。
  * 已禁用：不使用拆分通道。
- **SuiteB** 类型：在列表中，选择要使用的 NSA Suite B 加密级别。默认值为 GCM-128。可能的选项包括：
  * **GCM-128**：使用 128 位 AES-GCM 加密。
  * **GCM-256**：使用 256 位 AES-GCM 加密。
  * **GMAC-128**：使用 128 位 AES-GMAC 加密。
  * **GMAC-256**：使用 256 位 AES-GMAC 加密。
  * 无：不使用加密：键入用于客户端-服务器协商的 SSL 算法。
- **SSL** 算法：键入用于客户端-服务器协商的 SSL 算法。
- **Knox**：仅适用于 Samsung Knox 的配置。
- 供应商：与 Knox API 通信的通用代理的个人配置文件。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  * 转发路由：键入转发路由的 IP 地址。
  * 单击保存以保存路由，或者单击取消不保存路由。
- **PerApp VPN**：对于要添加的每个 PerApp VPN，请单击添加并执行以下操作：
  * **PerApp VPN**：应用程序进行通信时使用的 VPN 配置。
  * 单击保存以保存 PerApp VPN，或者单击取消不保存 PerApp VPN。

Windows Phone 设置

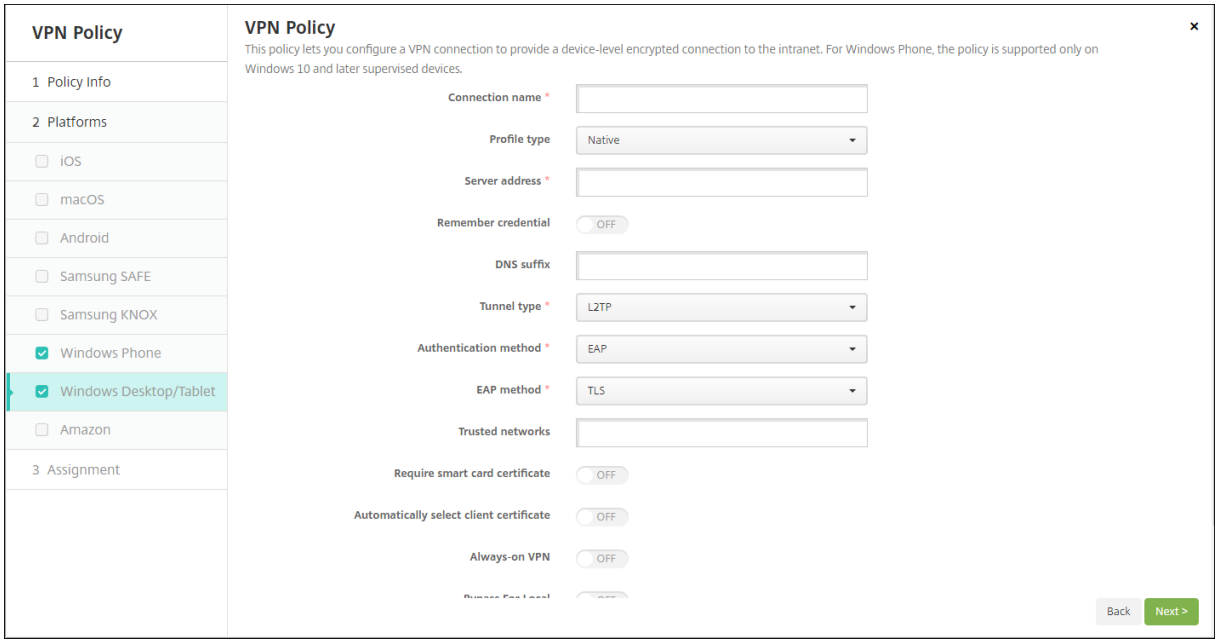


这些设置仅在 Windows 10 及更高版本的受监督手机上受支持。

- 连接名称：输入连接的名称。此字段为必填字段。
- 配置文件类型：在列表中，选择本机或插件。默认值为本机。以下各节介绍了其中每个选项的设置。
- 配置本机配置文件类型设置：这些设置适用于内置于用户 Windows Phone 的 VPN。
  - **VPN** 服务器名称：键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
  - 通道协议：在列表中，选择要使用的 VPN 通道的类型。默认值为 **L2TP**。可能的选项包括：
    - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
    - **PPTP**：点对点通道。
    - **IKEv2**： Internet 密钥交换第 2 版。
  - 身份验证方法：在列表中，选择要使用的身份验证方法。默认值为 **EAP**。可能的选项包括：
    - **EAP**：扩展身份验证协议。
    - **MSChapV2**：使用 Microsoft 的质询-握手身份验证相互验证身份。当您选择通道类型 IKEv2 时，此选项不可用。选择 MSChapV2 时，会显示自动使用 **Windows** 凭据选项。默认值为关。
  - **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
  - **DNS** 后缀：键入 DNS 后缀。
  - 可信网络：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - 需要智能卡证书：选择是否需要智能卡证书。默认值为关。
  - 自动选择客户端证书：选择是否自动选择用于身份验证的客户端证书。默认值为关。启用需要智能卡证书时此选项不可用。

  - 记住凭据：选择是否缓存凭据。默认值为关。启用后，会在合适的时候缓存凭据。
  - 始终启用 **VPN**：选择是否始终启用 VPN。默认值为关。启用后，VPN 连接保持可用，直到用户手动断开连接。
  - 绕过本地地址：键入地址和端口号，以允许本地资源绕过代理服务器。
- 配置插件协议类型：这些设置应用于从 Windows 应用商店获取并安装在用户设备上的 VPN 插件。
  - 服务器地址：键入 VPN 服务器的 URL、主机名或 IP 地址。
  - 客户端应用程序 **ID**：键入 VPN 插件的软件包系列名称。
  - 插件配置文件 **XML**：单击浏览并导航到要使用的自定义 VPN 插件配置文件所在位置，选择此文件。有关格式及详细信息，请联系插件提供商。
  - **DNS** 后缀：键入 DNS 后缀。
  - 可信网络：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - 记住凭据：选择是否缓存凭据。默认值为关。启用后，会在合适的时候缓存凭据。
  - 始终启用 **VPN**：选择是否始终启用 VPN。默认值为关。启用后，VPN 连接保持可用，直到用户手动断开连接。
  - 绕过本地地址：键入地址和端口号，以允许本地资源绕过代理服务器。

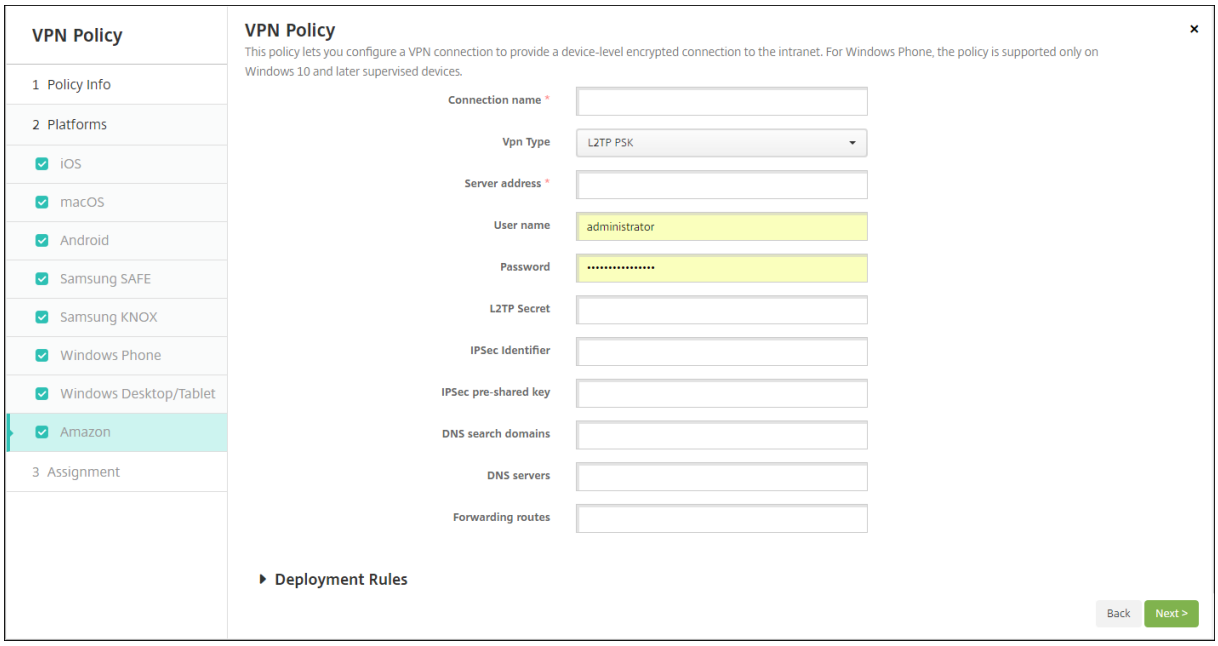
Windows Desktop/Tablet 设置



- 连接名称：输入连接的名称。此字段为必填字段。
- 配置文件类型：在列表中，选择本机或插件。默认值为本机。
- 配置本机配置文件类型：这些设置应用于内置于用户 Windows 设备上的 VPN。
  - 服务器地址：键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
  - 记住凭据：选择是否缓存凭据。默认值为关。启用后，会在合适的时候缓存凭据。

  - **DNS** 后缀：键入 DNS 后缀。
  - 通道类型：在列表中，选择要使用的 VPN 通道类型。默认值为 **L2TP**。可能的选项包括：
    * **L2TP**：使用预共享密钥身份验证的第二层通道协议。
    * **PPTP**：点对点通道。
    * **IKEv2**： Internet 密钥交换第 2 版。
  - 身份验证方法：在列表中，选择要使用的身份验证方法。默认值为 **EAP**。可能的选项包括：
    * **EAP**：扩展身份验证协议。
    * **MSChapV2**：使用 Microsoft 的质询-握手身份验证相互验证身份。当您选择通道类型 **IKEv2** 时，此选项不可用。
  - **EAP** 方法：在列表中，选择要使用的 EAP 方法。默认值为 **TLS**。启用 MSChapV2 身份验证时此字段不可用。可能的选项包括：
    * **TLS**：传输层安全性
    * **PEAP**：受保护的可扩展身份验证协议
  - 可信网络：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - 需要智能卡证书：选择是否需要智能卡证书。默认值为关。
  - 自动选择客户端证书：选择是否自动选择用于身份验证的客户端证书。默认值为关。启用需要智能卡证书时此选项不可用。
  - 始终启用 **VPN**：选择是否始终启用 VPN。默认值为关。启用后，VPN 连接保持可用，直到用户手动断开连接。
  - 绕过本地地址：键入地址和端口号，以允许本地资源绕过代理服务器。
- 配置插件配置文件类型：这些设置应用于从 Windows 应用商店获取并安装在用户设备上的 VPN 插件。
  - 服务器地址：键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
  - 记住凭据：选择是否缓存凭据。默认值为关。启用后，会在合适的时候缓存凭据。
  - **DNS** 后缀：键入 DNS 后缀。
  - 客户端应用程序 **ID**：键入 VPN 插件的软件包系列名称。
  - 插件配置文件 **XML**：单击浏览并导航到要使用的自定义 VPN 插件配置文件所在位置，选择此文件。有关格式及详细信息，请联系插件提供商。
  - 可信网络：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - 始终启用 **VPN**：选择是否始终启用 VPN。默认值为关。启用后，VPN 连接保持可用，直到用户手动断开连接。
  - 绕过本地地址：键入地址和端口号，以允许本地资源绕过代理服务器。

Amazon 设置



- 连接名称：输入连接的名称。
- **VPN** 类型：选择连接类型。可能的选项包括：
  - **L2TP PSK**：使用预共享密钥身份验证的第二层通道协议。这是默认设置。
  - **L2TP RSA**：使用 RSA 身份验证的第二层通道协议。
  - **IPSEC XAUTH PSK**：使用预共享密钥和扩展身份验证的 Internet 协议安全性。
  - **IPSEC HYBRID RSA**：使用混合 RSA 身份验证的 Internet 协议安全性。
  - **PPTP**：点对点通道。

以下各节列出了前面每种连接类型的配置选项。

为 Amazon 配置 L2TP PSK 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **L2TP** 密钥：键入共享密钥。
- **IPSec** 标识符：键入用户连接时在其设备上看到的 VPN 连接的名称。
- **IPSec** 预共享密钥：键入密钥。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

配置适用于 **Amazon** 的 **L2TP RSA** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **L2TP** 密钥：键入共享密钥。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 服务器证书：在列表中，选择要使用的服务器证书。
- **CA** 证书：在列表中，选择要使用的 CA 证书。
- 身份凭据：在列表中，选择要使用的身份凭据。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

为 **Amazon** 配置 **IPSEC XAUTH PSK** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **IPSec** 标识符：键入用户连接时在其设备上看到的 VPN 连接的名称。
- **IPSec** 预共享密钥：键入共享密钥。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

为 **Amazon** 配置 **IPSEC AUTH RSA** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 服务器证书：在列表中，选择要使用的服务器证书。
- **CA** 证书：在列表中，选择要使用的 CA 证书。
- 身份凭据：在列表中，选择要使用的身份凭据。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。

  - 单击保存以保存路由，或者单击取消不保存路由。

为 **Amazon** 配置 **IPSEC HYBRID RSA** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- 服务器证书：在列表中，选择要使用的服务器证书。
- **CA** 证书：在列表中，选择要使用的 CA 证书。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

配置适用于 **Amazon** 的 **PPTP** 设置

- 服务器地址：键入 VPN 服务器的 IP 地址。
- 用户名：键入可选用户名。
- 密码：键入可选密码。
- **DNS** 搜索域：键入用户设备的搜索域列表可以与之匹配的域。
- **DNS** 服务器：键入用于解析指定域的 DNS 服务器的 IP 地址。
- **PPP** 加密 **(MPPE)**：选择是否使用 Microsoft 点对点加密 (MPPE) 进行数据加密。默认值为关。
- 转发路由：如果企业 VPN 服务器支持转发路由，对于要使用的每种转发路由，请单击添加并执行以下操作：
  - 转发路由：键入转发路由的 IP 地址。
  - 单击保存以保存路由，或者单击取消不保存路由。

墙纸设备策略

August 18, 2021

您可以添加.png 或.jpg 文件，以设置 iOS 设备锁屏界面或/和主屏幕的墙纸。仅在 iOS 7.1.2 及更高版本中针对受监督的设备提供。要在 iPad 和 iPhone 上使用不同的墙纸，需要创建不同的墙纸策略并将其部署到相应的用户。

下表列出了 Apple 建议的用于 iOS 设备的图片尺寸。

iPhone

设备	图片尺寸（像素）
iPhone 12 Pro Max	2778 x 1284
iPhone 12 和 iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X、XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 第二代	1334 x 750
iPhone 7 PLus、8 PLus	2208 x 1242
iPhone 7、8	1334 x 750
iPhone 8 PLus	1334 x 750
iPhone 8	1334 x 750

iPad

设备	图片尺寸（像素）
iPad Pro（第一代、第二代和第三代 12.9 英寸）	2732 x 2048
iPad Pro 10.5 英寸	2224 x 1668
iPad Pro（9.7 英寸）	1536 x 2048
iPad Air 2	2048 x 1536

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 适用于：在列表中，选择锁屏界面、主 **(**图标列表**)** 屏幕或锁屏界面和主屏幕以设置墙纸的显示位置。
- 墙纸文件：单击浏览并导航到墙纸文件所在位置，选择此文件。

Web 内容过滤器设备策略

January 5, 2022

可以在 XenMobile 中添加一个设备策略，用于通过结合使用 Apple 的自动过滤功能和添加到允许列表和阻止列表中的特定站点，在 iOS 设备上过滤 Web 内容。此策略仅适用于采用受监督模式的 iOS 7.0 及更高版本。有关将 iOS 设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 过滤器类型：在列表中，单击内置或插件，然后按照所选选项后面的步骤操作。默认值为内置。

内置过滤器类型

- **Web** 内容过滤器
  - 启用自动过滤：是否使用 Apple 自动过滤功能来分析 Web 站点是否包含不合适的内容。默认值为关。
  - 允许访问的 **URL**：启用自动过滤设置为关时将忽略此列表。启用自动过滤设置为开时，无论自动过滤器是否允许访问，始终可以访问此列表中的项目。对于要添加到允许列表中的每个 URL，单击添加，然后执行以下操作：
    * 键入允许访问的 Web 站点的 URL。必须在 Web 地址前添加 `http://` 或 `https://`。
    * 单击保存将 Web 站点保存到允许列表中，或单击取消不保存此站点。
  - 加入黑名单的 **URL**：始终阻止此列表中的项目。对于要添加到阻止列表中的每个 URL，单击添加，然后执行以下操作：
    * 输入要阻止的 Web 站点的 URL。必须在 Web 地址前添加 `http://` 或 `https://`。
    * 单击保存将 Web 站点保存到阻止列表中，或单击取消不保存此站点。

      > 注意：
      > XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。
- 书签白名单
  - 书签白名单：指定用户可以访问的站点。要启用对 Web 站点的访问，请添加其 URL。
    * **URL**：用户可以访问的每个 Web 站点的 URL。例如，要启用对 Secure Hub 应用商店的访问，请将 XenMobile Server URL 添加到 **URL** 列表中。必须在 Web 地址前添加 `http://` 或 `https://`。此字段为必填字段。
    * 书签文件夹：输入可选书签文件夹名称。如果将此字段留空，书签将添加到默认书签目录。
    * 标题：输入 Web 站点的描述性标题。例如，为 URL `https://google.com` 输入“Google”。
    * 单击保存将 Web 站点保存到允许列表中，或单击取消不保存此站点。

插件过滤器类型

- 过滤器名称：输入过滤器的唯一名称。
- 标识符：输入提供过滤器服务的插件的捆绑包 ID。
- 服务地址：输入可选服务器地址。有效格式包括 IP 地址、主机名或 URL。
- 用户名：输入服务的可选用户名。
- 密码：输入服务的可选密码。
- 证书：在列表中，单击用于向服务验证用户身份的可选身份证书。默认设置为无。
- 过滤 **WebKit** 流量：选择是否过滤 WebKit 流量。
- 过滤 **Socket** 流量：选择是否过滤套接字流量。
- 自定义数据：对于要添加到 Web 过滤器的每个自定义密钥，单击添加，然后执行以下操作：
  - 密钥：键入自定义密钥。
  - 值：键入自定义密钥的值。
  - 单击保存以保存自定义密钥，或单击取消不保存此密钥。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

Web 剪辑设备策略

January 5, 2022

可以向 Web 站点中放置快捷方式或 Web 剪辑，以与应用程序一起出现在用户的设备上。可以指定自己的图标来表示 iOS、iPadOS、macOS 和 Android 设备的 Web 剪辑。Windows 平板电脑只需要一个标签和一个 URL。对于 iOS 和 iPadOS 设备，请配置主屏幕布局设备策略以组织您创建的 Web 剪辑。如果限制对 iOS 上的应用程序的访问，请务必将限制设备策略配置为允许 Web 剪辑。有关配置这些策略的信息，请参阅主屏幕布局设备策略和“限制”设备策略。

要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

iOS 设置

- 标签：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。URL 的开头必须为协议，例如 `https://server`。
- 可删除：选择用户是否可以删除 Web 剪辑。默认值为关。
- 待更新的图标：单击浏览并导航到要用于 Web 剪辑的图标文件所在位置，选择此图标。
- 复合图标：选择此图标是否应用某些效果（圆角、阴影和光照反射）。默认值为关，表示添加效果。
- 全屏：选择链接的 Web 页面是否以全屏模式打开。默认值为关。

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- 标签：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。URL 的开头必须为协议，例如 `https://server`。
- 待更新的图标：单击“浏览”并导航到要用于 Web 剪辑的图标文件所在位置，选择此图标。

Android 设置

- 规则：选择此策略是添加还是删除 Web 剪辑。默认值为添加。
- 标签：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。
- 定义图标：选择是否使用图标文件。默认值为关。
- 图标文件：如果定义图标设置为开，请单击浏览并导航到要使用的图标文件所在位置，选择此文件。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Windows Desktop/Tablet 设置

- 名称：键入与 Web 剪辑一起显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。

Wi-Fi 设备策略

January 5, 2022

可通过使用配置 > 设备策略页面，在 XenMobile 中创建新的 WiFi 设备策略或编辑现有 Wi-Fi 设备策略。借助 Wi-Fi 策略，您可以通过定义以下项目来管理用户将其设备连接到 Wi-Fi 网络的方式：

- 网络名称和类型
- 身份验证和安全策略
- 代理服务器使用
- 与 WiFi 有关的其他详细信息

要添加或配置此策略，请转至配置 > 设备策略。有关详细信息，请参阅设备策略。

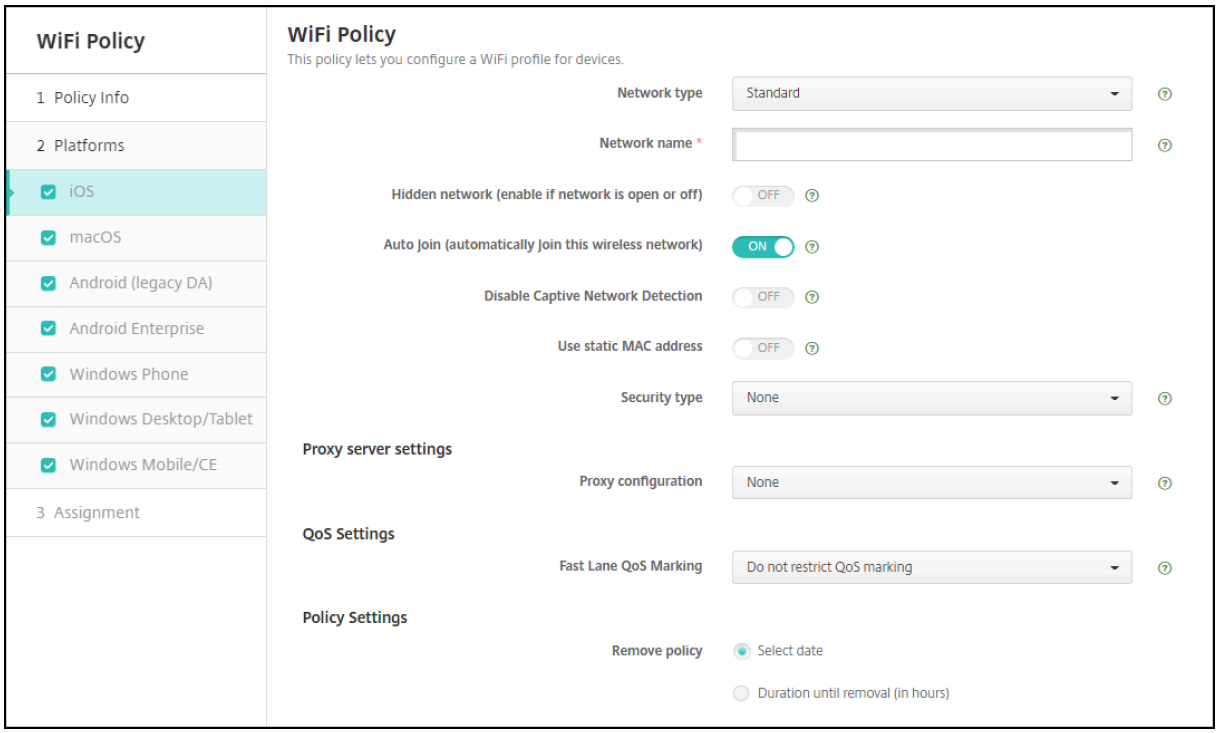
必备条件

在创建策略之前，请务必完成以下步骤：

- 创建计划使用的任何交付组。
- 了解网络名称和类型。
- 了解计划使用的任何身份验证或安全类型。
- 了解可能需要的任何代理服务器信息。
- 安装所有必需的 CA 证书。
- 具有所有必需共享密钥。
- 为基于证书的身份验证创建 PKI 实体。
- 配置凭据提供程序。

有关详细信息，请参阅身份验证及文中各节。

iOS 设置



- 网络类型：在列表中，选择标准、传统热点或 **Hotspot 2.0** 以设置您计划使用的网络类型。
- 网络名称：键入显示在设备的可用网络列表中的 SSID。不适用于 **Hotspot 2.0**。
- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。
- 自动加入 **(**自动加入此无线网络**)**：选择是否自动加入网络。如果 iOS 设备已连接到另一个网络，则不会加入此网络。在设备自动连接之前，用户必须断开与以前的网络的连接。默认值为开。
- 使用静态 **MAC** 地址： MAC 地址是设备在网络中传输的唯一标识符。为了提高隐私性，iOS 和 iPadOS 设备每次连接到网络时都可以使用不同的 MAC 地址。如果设置为开，设备在连接到此网络时将始终使用相同的 MAC 地址。如果设置为关，设备每次连接到此网络时都将使用不同的 MAC 地址。默认值为关。
- 安全类型：在列表中，选择您计划使用的安全类型。不适用于 **Hotspot 2.0**。
  - 无 - 无需进一步配置。
  - WEP
  - WPA/WPA2 Personal
  - 任何 (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise：需要配置简单证书注册协议 (Simple Certificate Enrollment Protocol , SCEP) 才能使用 WPA-2 Enterprise。XenMobile 之后可以将证书发送到设备以对 Wi-Fi 服务器进行身份验证。要配置 SCEP，请转到设置 **>** 凭据提供程序的“分发”页面。有关详细信息，请参阅凭据提供程序。
  - 任何 (Enterprise)

以下各节列出了要为上述各个连接类型配置的选项。

适用于 **iOS** 的 **“WPA”**、**“WPA Personal”**、**“**任何 **(Personal)”** 设置

密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。

适用于 **iOS** 的 **“WEP Enterprise”**、**“WPA Enterprise”**、**“WPA2 Enterprise”**、**“**任何 **(Enterprise)”** 设置

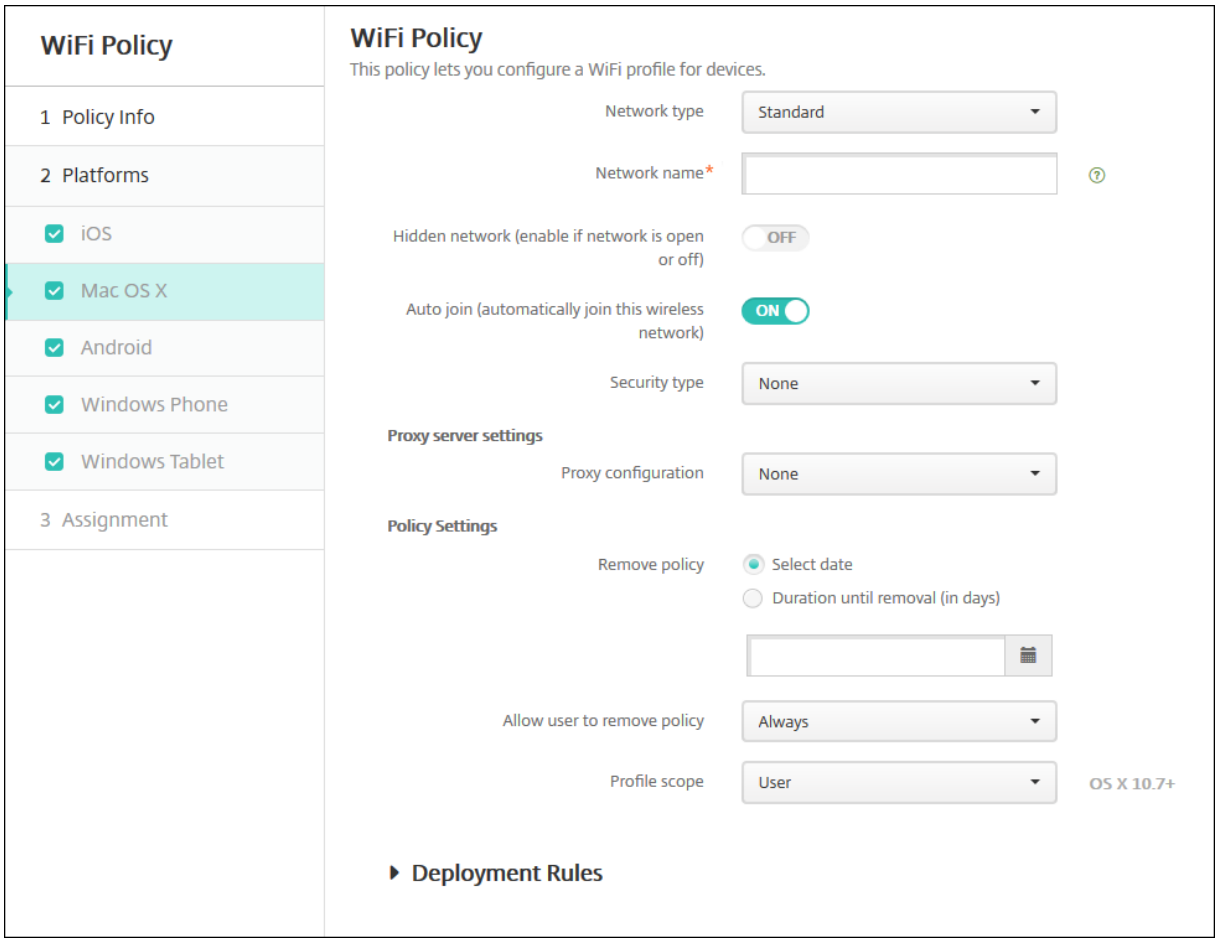
选择其中的任何设置时，其设置将在代理服务器设置后面列出。

- 协议，接受 **EAP** 类型：启用要支持的 EAP 类型，然后配置相关设置。每个可用 EAP 类型的默认值为关。
- 内部身份验证 **(TTLS)**：仅在启用 *TTLS* 时需要。在列表中，选择要使用的内部身份验证方法。选项包括：**PAP**、**CHAP**、**MSCHAP** 或 **MSCHAPv2**。默认值为 **MSCHAPv2**。
- 协议，**EAP-FAST**：选择是否使用受保护的访问凭据 (PAC)。
  - 如果选择使用 **PAC**，请选择是否要使用预配 PAC。
    - 如果选择预配 **PAC**，请选择是否允许在最终用户客户端与 XenMobile 之间建立匿名 TLS 握手。
      - 匿名预配 **PAC**
- 身份验证：
  - 用户名：键入用户名。
  - 为连接单独设置密码：选择用户是否在每次登录时都需要提供密码。
  - 密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。
  - 身份凭据 **(**密钥库或 **PKI** 凭据**)**：在列表中，选择身份凭据的类型。默认设置为无。
  - 外部标识：仅在启用 **PEAP**、**TTLS** 或 **EAP-FAST** 时需要。键入外部可见的用户名。您可以通过键入 “anonymous” 等通用术语以使用户名不可见来增加安全性。
  - 需要 **TLS** 证书：选择是否需要 TLS 证书。
- 信任
  - 可信证书：要添加可信证书，请单击添加，然后，针对要添加的各个证书执行以下操作：
    - 应用程序：在列表中，单击要添加的应用程序。
    - 单击保存以保存证书，或者单击取消。
  - 可信服务器证书名称：要添加可信服务器证书公用名，请单击添加，然后针对要添加的名称执行以下操作：
    - 证书：键入服务器证书的名称。可以使用通配符指定名称，如 wpa.*.example.com。
    - 单击保存以保存证书名称，或者单击取消。
- 允许信任例外：选择当证书不可信时是否在用户设备上显示证书信任对话框。默认值为开。
- 代理服务器设置
  - 代理配置：在列表中，选择无、手动或自动以设置 VPN 连接通过代理服务器路由的方式，然后配置任何其他选项。默认值为无，表示无需进一步配置。
  - 如果选择手动，请配置以下设置：
    - 主机名**/IP** 地址：键入代理服务器的主机名或 IP 地址。
    - 端口：键入代理服务器端口号。
    - 用户名：键入向代理服务器进行身份验证的可选用户名。
    - 密码：键入向代理服务器进行身份验证的可选密码。
  - 如果选择自动，请配置以下设置：
    - 服务器 **URL**：键入用于定义代理配置的 PAC 文件的 URL。

    * 允许在无法访问 **PAC** 时直接连接：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。默认值为开。此选项仅适用于 iOS 7.0 及更高版本。

- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    * 选择日期：单击日历可选择具体删除日期。
    * 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。仅适用于 iOS 6.0 及更高版本。

macOS 设置



- 网络类型：在列表中，选择标准、传统热点或 **Hotspot 2.0** 以设置您计划使用的网络类型。
- 网络名称：键入显示在设备的可用网络列表中的 SSID。不适用于 **Hotspot 2.0**。
- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。
- 自动加入 **(**自动加入此无线网络**)**：选择是否自动加入网络。如果设备已连接到另一个网络，则不会加入此网络。在设备自动连接之前，用户必须断开与以前的网络的连接。默认值为开。
- 安全类型：在列表中，选择您计划使用的安全类型。不适用于 **Hotspot 2.0**。
  - 无 - 无需进一步配置。
  - WEP
  - WPA/WPA2 Personal

  - 任何 (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - 任何 (Enterprise)

以下各节列出了要为上述各个连接类型配置的选项。

适用于 **macOS** 的 **“WPA”**、**“WPA Personal”**、**“WPA 2 Personal”**、**“**任何 **(Personal)”** 设置

- 密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。

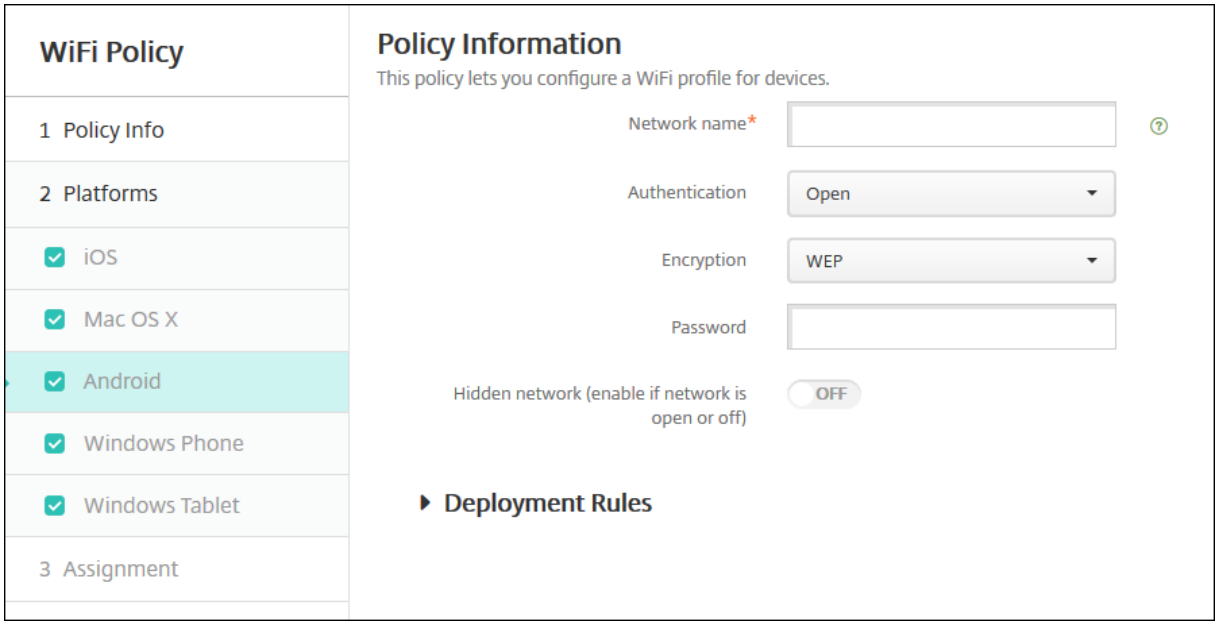
适用于 **macOS** 的 **“WEP Enterprise”**、**“WPA Enterprise”**、**“WPA2 Enterprise”**、**“**任何 **(Enterprise)”** 设置

选择其中的任何设置时，其设置将在代理服务器设置后面列出。

- 协议，接受 **EAP** 类型：启用要支持的 EAP 类型，然后配置相关设置。每个可用 EAP 类型的默认值为关。
- 内部身份验证 **(TTLS)**：仅在启用 *TTLS* 时需要。在列表中，选择要使用的内部身份验证方法。选项包括：**PAP**、**CHAP**、**MSCHAP** 或 **MSCHAPv2**。默认值为 **MSCHAPv2**。
- 协议，**EAP-FAST**：选择是否使用受保护的访问凭据 (PAC)。
  - 如果选择使用 **PAC**，请选择是否使用预配 PAC。
    - 如果选择预配 **PAC**，请选择是否允许在最终用户客户端与 XenMobile 之间建立匿名 TLS 握手。
      - 匿名预配 **PAC**
- 身份验证：
  - 用户名：键入用户名。
  - 为连接单独设置密码：选择用户是否在每次登录时都需要提供密码。
  - 密码：键入可选密码。如果将此字段留空，用户登录时可能会收到输入其密码提示。
  - 身份凭据 **(**密钥库或 **PKI** 凭据**)**：在列表中，选择身份凭据的类型。默认设置为无。
  - 外部标识：仅在启用 **PEAP**、**TTLS** 或 **EAP-FAST** 时需要。键入外部可见的用户名。您可以通过键入 “anonymous” 等通用术语以使用户名不可见来增加安全性。
  - 需要 **TLS** 证书：选择是否需要 TLS 证书。
- 信任
  - 可信证书：要添加可信证书，请单击添加，然后，针对要添加的各个证书执行以下操作：
    - 应用程序：在列表中，单击要添加的应用程序。
    - 单击保存以保存证书，或者单击取消。
  - 可信服务器证书名称：要添加可信服务器证书公用名，请单击添加，然后针对要添加的名称执行以下操作：
    - 证书：键入要添加的服务器证书的名称。可以使用通配符指定名称，如 wpa.*.example.com。
    - 单击保存以保存证书名称，或者单击取消。
- 允许信任例外：选择当证书不可信时是否在用户设备上显示证书信任对话框。默认值为开。
- 用作登录窗口配置：选择是否使用在登录窗口中输入的同一凭据对用户进行身份验证。
- 代理服务器设置

- 代理配置：在列表中，选择无、手动或自动以设置 VPN 连接通过代理服务器路由的方式，然后配置任何其他选项。默认值为无，表示无需进一步配置。
- 如果选择手动，请配置以下设置：
  - 主机名/**IP** 地址：键入代理服务器的主机名或 IP 地址。
  - 端口：键入代理服务器端口号。
  - 用户名：键入向代理服务器进行身份验证的可选用户名。
  - 密码：键入向代理服务器进行身份验证的可选密码。
- 如果选择自动，请配置以下设置：
  - 服务器 **URL**：键入用于定义代理配置的 PAC 文件的 URL。
  - 允许在无法访问 **PAC** 时直接连接：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。默认值为开。此选项仅适用于 iOS 7.0 及更高版本。

Android 设置



- 网络名称：键入在用户设备上的可用网络列表中的 SSID。
- 身份验证：在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - 共享虚拟机
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下各节列出了要为上述各个连接类型配置的选项。

适用于 **Android** 的 **“开放”**、**“共享”** 设置

- 加密：在列表中，选择已禁用或 **WEP**。默认值为 **WEP**。
- 密码：键入可选密码。

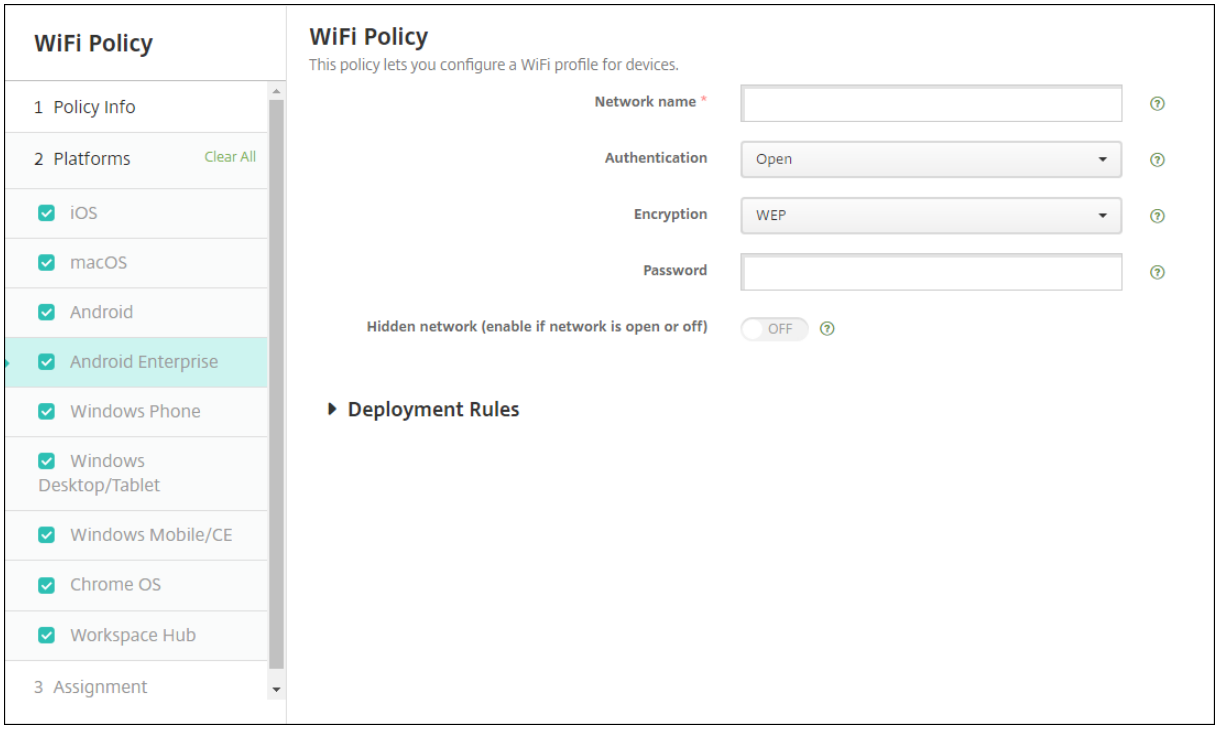
适用于 **Android** 的 **“WPA”**、**“WPA-WPA2”**、**“WPA2-PSK”** 设置

- 加密：在列表中，选择 **TKIP** 或 **AES**。默认值为 **TKIP**。
- 密码：键入可选密码。

适用于 **Android** 的 **802.1x** 设置

- **EAP** 类型：在列表中，选择 **PEAP**、**TLS** 或 **TTLS**。默认值为 **PEAP**。
- 密码：键入可选密码。
- 身份验证阶段 **2**：在列表中，选择无、**PAP**、**MSCHAP**、**MSCHAPPv2** 或 **GTC**。默认值为 **PAP**。
- 身份：键入可选用户名和域。
- 匿名：键入外部可见的可选用户名。您可以通过键入 “anonymous” 等通用术语以使用户名不可见来增加安全性。
- **CA** 证书：在列表中，选择要使用的证书。
- 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。

Android Enterprise 设置



- 网络名称：键入在用户设备上的可用网络列表中的 SSID。
- 身份验证：在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - 共享虚拟机
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下各节列出了要为上述各个连接类型配置的选项。

适用于 **Android** 的 **“**开放**”**、**“**共享**”** 设置

- 加密：在列表中，选择已禁用或 **WEP**。默认值为 **WEP**。
- 密码：键入可选密码。

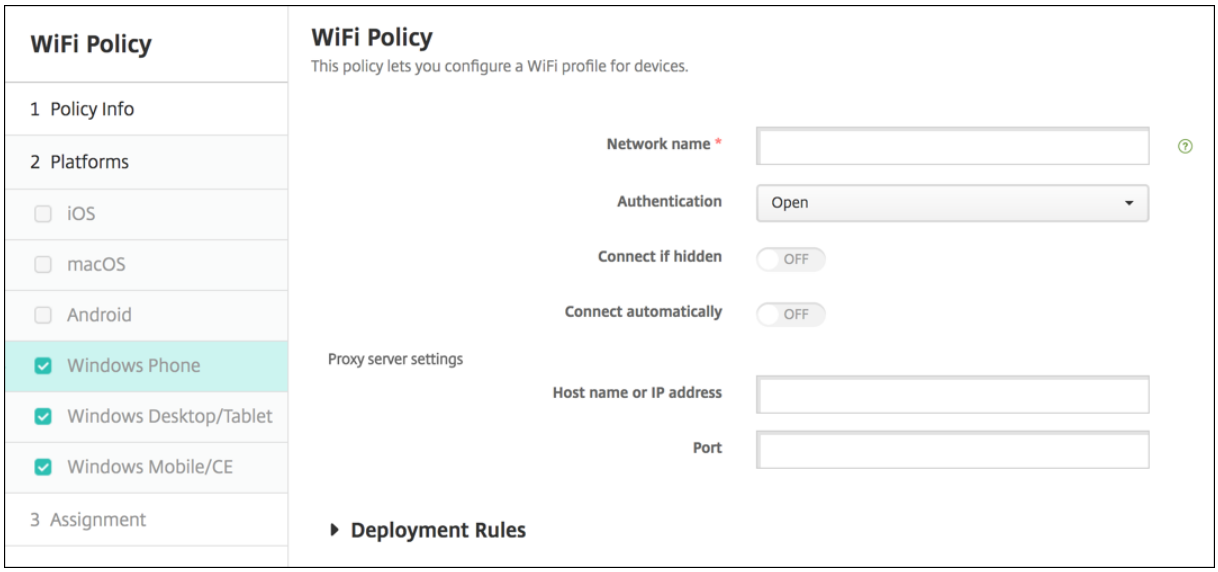
适用于 **Android** 的 **“WPA”**、**“WPA-WPA2”**、**“WPA2-PSK”** 设置

- 加密：在列表中，选择 “TKIP” 或 “AES”。默认值为 TKIP。
- 密码：键入可选密码。

适用于 **Android** 的 **802.1x** 设置

- **EAP** 类型：在列表中，选择 **PEAP**、**TLS** 或 **TTLS**。默认值为 **PEAP**。
- 密码：键入可选密码。
- 身份验证阶段 **2**：在列表中，选择无、**PAP**、**MSCHAP**、**MSCHAPPv2** 或 **GTC**。默认值为 **PAP**。
- 身份：键入可选用户名和域。
- 匿名：键入外部可见的可选用户名。可以通过键入 “anonymous” 等通用术语以使用户名不可见来增加安全性。
- **CA** 证书：在列表中，选择要使用的证书。
- 身份凭据：在列表中，选择要使用的身份凭据。默认设置为无。
- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。

Windows Phone 设置



- 网络名称：键入在用户设备上的可用网络列表中的 SSID。
- 身份验证：在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise：需要配置 SCEP 才能使用 WPA-2 Enterprise。通过 SCEP 配置，XenMobile 可以将证书发送到设备以对 Wi-Fi 服务器进行身份验证。要配置 SCEP，请转到设置 > 凭据提供程序的分发页面。有关详细信息，请参阅凭据提供程序。

以下各节列出了要为上述各个连接类型配置的选项。

适用于 Windows Phone 的 “开放” 设置

- 即使隐藏，也进行连接：选择在网络隐藏时是否进行连接。
- 自动连接：选择是否自动连接到网络。

适用于 Windows Phone 的 “WPA Personal”、“WPA-2 Personal” 设置

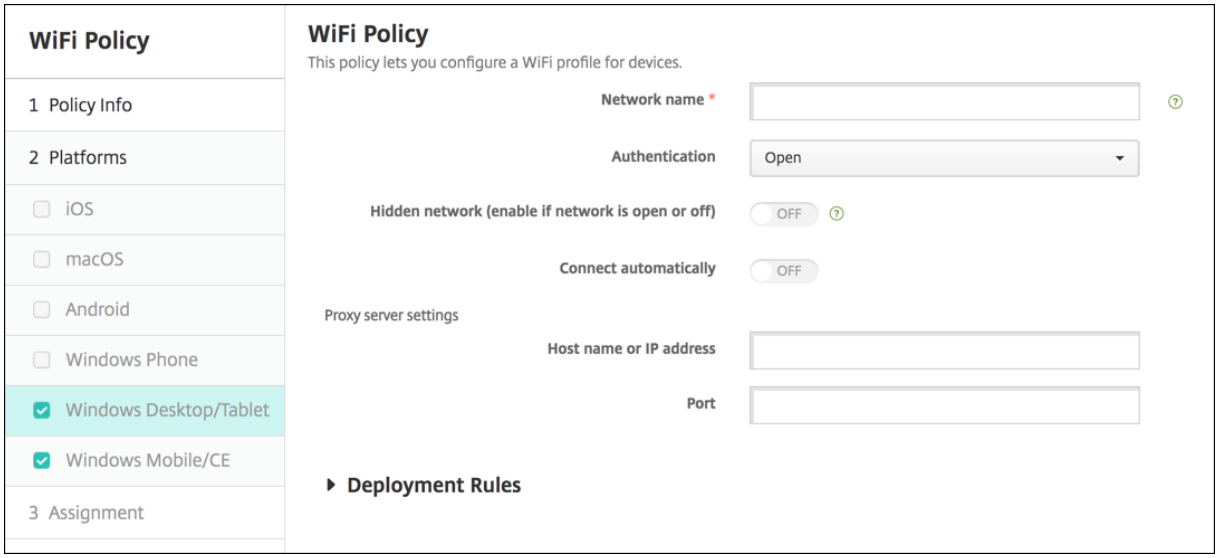
- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- 即使隐藏，也进行连接：选择在网络隐藏时是否进行连接。
- 自动连接：选择是否自动连接到网络。

适用于 Windows Phone 的 “WPA-2 Enterprise” 设置

- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- **EAP** 类型：在列表中，选择 **PEAP-MSCHAPv2** 或 **TLS** 以设置 EAP 类型。默认值为 **PEAP-MSCHAPv2**。

- 即使隐藏，也进行连接：选择在网络隐藏时是否进行连接。
- 自动连接：选择是否自动连接到网络。
- 通过 **SCEP** 推送证书：选择是否通过简单证书注册协议 (SCEP) 将证书推送到用户设备。
- **SCEP** 的凭据提供程序：在列表中，选择 SCEP 凭据提供程序。默认设置为无。
- 代理服务器设置
  - 主机名或 **IP** 地址：键入代理服务器的名称或 IP 地址。
  - 端口：键入代理服务器的端口号。
- 策略设置
  - 删除策略：选择计划删除策略的方法。可用选项包括选择日期和删除前的持续时间 **(**小时**)**
    - 选择日期：单击日历可选择具体删除日期。
    - 删除前的持续时间 **(**小时**)**：键入发生策略删除操作之前的小时数。
  - 允许用户删除策略：可以选择用户何时可以从其设备中删除策略。从菜单中选择始终、需要通行码或从不。如果选择需要通行码，请在删除通行码字段中键入通行码。
  - 配置文件作用域：选择此策略是应用于用户还是整个系统。默认值为用户。此选项仅在 macOS 10.7 及更高版本中可用。

Windows 10 和 **Windows 11** 设置



- 身份验证：在列表中，单击用于 Wi-Fi 连接的安全类型。
  - 开放
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise：需要配置 SCEP 才能使用 WPA-2 Enterprise。通过 SCEP 配置，XenMobile 可以将证书发送到设备以对 Wi-Fi 服务器进行身份验证。要配置 SCEP，请转到设置 **>** 凭据提供程序的分发页面。有关详细信息，请参阅凭据提供程序。

以下各节列出了要为上述各个连接类型配置的选项。

打开 **Windows 10** 和 **Windows 11** 的设置

- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。

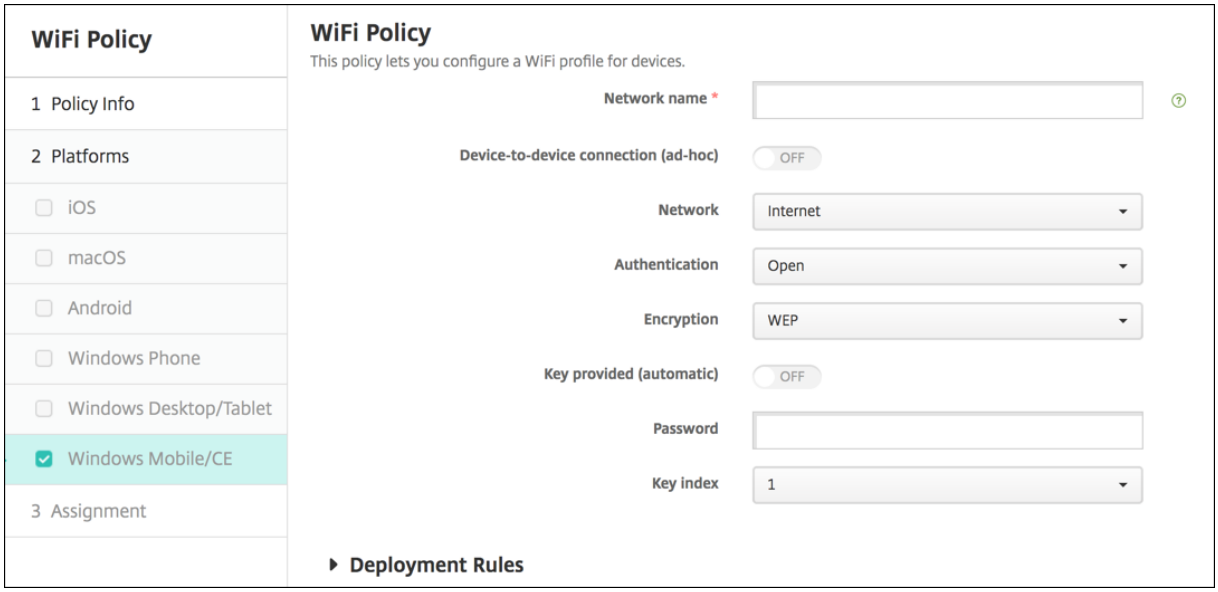
适用于 **Windows 10** 和 **Windows 11** 的 **“WPA Personal”**、**“WPA-2 Personal”** 设置

- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。

适用于 **Windows 10** 和 **Windows 11** 的 **“WPA-2 Enterprise”** 设置

- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- **EAP** 类型：在列表中，选择 **PEAP-MSCHAPv2** 或 **TLS** 以设置 EAP 类型。默认值为 **PEAP-MSCHAPv2**。
- 即使隐藏，也进行连接：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。
- 通过 **SCEP** 推送证书：选择是否使用简单证书注册协议 (SCEP) 将证书推送到用户设备。
- **SCEP** 的凭据提供程序：在列表中，选择 SCEP 凭据提供程序。默认设置为无。

Windows Mobile/CE 设置



- 网络名称：键入在用户设备上的可用网络列表中的 SSID。
- 设备到设备连接 **(**临时**)**：允许两个设备直接连接。默认值为关。

- 网络：选择设备是连接到外部 Internet 来源还是官方 Intranet。
- 身份验证：在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise

以下各节列出了要为上述各个连接类型配置的选项。

适用于 **Windows Mobile/CE** 的 **“开放”** 设置

- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。

适用于 **Windows Mobile/CE** 的 **“WPA Personal”**、**“WPA-2 Personal”** 设置

- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- 隐藏的网络 **(**网络打开或关闭时启用**)**：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。

适用于 **Windows Mobile/CE** 的 **“WPA-2 Enterprise”** 设置

- 加密：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- **EAP** 类型：在列表中，选择 **PEAP-MSCHAPv2** 或 **TLS** 以设置 EAP 类型。默认值为 **PEAP-MSCHAPv2**。
- 即使隐藏，也进行连接：选择是否隐藏网络。
- 自动连接：选择是否自动连接到网络。
- 通过 **SCEP** 推送证书：选择是否使用简单证书注册协议 (SCEP) 将证书推送到用户设备。
- **SCEP** 的凭据提供程序：在列表中，选择 SCEP 凭据提供程序。默认设置为无。
- 提供的密钥 **(**自动**)**：选择是否自动提供密钥。默认值为关。
- 密码：在此字段中键入密码。
- 密钥索引：选择密钥索引。可用选项包括 **1**、**2**、**3** 和 **4**。

Windows CE 证书设备策略

January 5, 2022

可以在 XenMobile 中创建一个设备策略，以从外部 PKI 创建 Windows Mobile/CE 证书并将其交付到用户设备。有关证书和 PKI 实体的详细信息，请参阅证书。

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 CE 设置

- 凭据提供程序：在列表中，单击凭据提供程序。默认设置为无。
- 生成的 **PKCS#12** 的密码：键入用于加密凭据的密码。
- 目标文件夹：在列表中，单击凭据的目标文件夹或单击新增以添加列表中尚未存在的文件夹。预定义选项为：
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- 目标文件名：键入凭据文件的名称。

Windows 信息保护设备策略

January 5, 2022

Windows 信息保护 (WIP) 以前称为企业数据保护 (EDP)，是一项防止出现潜在企业数据泄漏的 Windows 技术。数据泄漏会通过与非企业保护的应用程序、在应用程序之间或在组织网络外部共享企业数据发生。有关详细信息，请参阅 Protect your enterprise data using Windows Information Protection (WIP)（使用 Windows 信息保护 (WIP) 保护您的企业数据）。

可以在 XenMobile 创建一条设备策略以指定在您设置的强制级别需要 Windows 信息保护的应用程序。“Windows 信息保护” 策略适用于运行 Windows 10 或 Windows 11 的受监督 Phone、Tablet 和 Desktop。

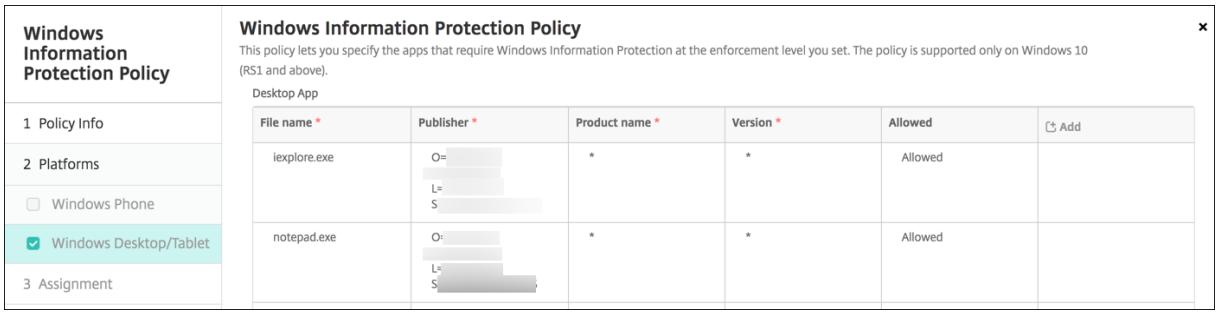
XenMobile 包括一些常用应用程序，并且您可以添加其他应用程序。您为策略指定影响用户体验的强制级别。例如，您可以：

- 阻止任何不恰当的数据共享。
- 警告不恰当的数据共享并允许用户覆盖策略。
- 登录并允许不恰当的数据共享过程中无提示运行 WIP。

要将应用程序从 Windows 信息保护中排除，请在 Microsoft AppLocker XML 文件中定义这些应用程序，然后将这些文件导入到 XenMobile 中。

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 10 和 Windows 11 设置



- 桌面应用程序（Windows 10 或 Windows 11 Desktop）、应用商店应用程序（Windows 10 Phone、Windows 10 或 Windows 11 Tablet）：XenMobile 包括一些常用应用程序，如上例中所示。您可以根据需要编辑或删除这些应用程序。

  要添加其他应用程序，请在桌面应用程序或应用商店应用程序表中，单击添加并提供应用程序信息。

  允许的应用程序可以读取、创建和更新企业数据。禁止的应用程序不能访问企业数据。例外应用程序可以读取企业数据，但不能创建或修改这些数据。

  - **AppLocker XML**： Microsoft 提供存在与 WIP 有关的已知兼容性问题的 Microsoft 应用程序的列表。要从 WIP 中排除这些应用程序，请单击浏览以上载该列表。XenMobile 在发送到设备的策略中将上载的 AppLocker XML 与配置的桌面和应用商店应用程序组合在一起。有关详细信息，请参阅 Recommended deny list for Windows Information Protection（针对 Windows 信息保护的建议拒绝列表）。
  - 强制级别：选择一个选项以指定您希望 Windows 信息保护功能保护和管理数据共享的方式。默认值为关。
    - **0-**关闭： WIP 已关闭，不保护或审核您的数据。
    - **1-**无提示： WIP 无提示运行，记录不恰当的数据共享，并且不阻止任何操作。您可以通过报告 CSP 访问日志。
    - **2-**替代： WIP 向用户警告潜在的不安全数据共享。用户可以替代警告并共享数据。此模式在您的审核日志中记录操作，包括用户替代操作。
    - **3-**阻止： WIP 阻止用户完成潜在的不安全数据共享。
  - 受保护的域名：您的企业用于其用户身份的域。此托管标识域列表以及主域组成了您的托管企业的标识。列表中的第一个域是在 Windows UI 中使用的主企业标识。请使用 “|” 分隔列表项。例如：`domain1.com | domain2.com`
  - 数据恢复证书：单击浏览，然后选择一个用于加密文件的数据恢复的恢复证书。此证书与用于加密文件系统 (EFS) 的数据恢复代理 (DRA) 证书相同，仅通过 MDM 提供，不通过组策略提供。如果恢复证书不可用，请进行创建。有关信息，请参阅本节中的 “创建数据恢复证书”。
  - 网络域名称：组成了企业边界的域的列表。WIP 保护传输到此列表中的完全限定域的所有流量。此设置以及 **IP** 范围设置用于检测专用网络中的网络端点是企业端点还是个人端点。请使用逗号分隔列表项。例如：corp.example.com,region.example.com

- **IP** 范围：定义企业网络中的计算机的企业 IPv4 和 IPv6 范围的列表。WIP 将这些位置视为企业数据共享的安全位置。请使用逗号分隔列表项。例如：

  ```
  10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:
  ffff:ffff
  ```

- **IP** 范围列表具有权威性：要阻止 Windows 自动检测 IP 范围，请将此设置更改为开。默认值为关。
- 代理服务器：企业可以用于公司资源的代理服务器的列表。如果在您的网络中使用代理，则需要此设置。如果未设置代理服务器，则当客户端位于代理后面时，企业资源可能不可用。例如，可能无法从宾馆和饭店的某些 WiFi 热点访问资源。请使用逗号分隔列表项。例如：

  ```
  proxy.example.com:80;157.54.11.118:443
  ```

- 内部代理服务器：您的设备通过其访问云资源的代理服务器的列表。使用此服务器类型指示您要连接到的云资源属于企业资源。请勿在此列表中包括代理服务器设置中的任何服务器，这些服务器用于非 WIP 保护的流量。请使用逗号分隔列表项。例如：

  ```
  example.internalproxy1.com;10.147.80.50
  ```

- 云资源： WIP 保护的云资源的列表。对于每种云资源，您还可以选择在代理服务器列表中指定一个代理服务器，用于路由此云资源的流量。通过代理服务器路由的所有流量都被视为企业流量。请使用逗号分隔列表项。例如：

  ```
  domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
  domain2.com
  ```

- 设置锁定情况下需要保护：仅限 Windows 10 Phone。如果设置为开，还需要设置通行码设备策略。否则，Windows 信息保护策略部署将失败。此外，如果此策略设置为开，则将显示需要锁定保护设置。默认值为关。
- 需要锁定保护：仅限 Windows 10 Phone。指定是否在锁定设备上使用不受员工 PIN 保护的密钥加密企业数据。应用程序不能读取锁定设备上的公司数据。默认值为开。
- 取消注册时吊销 **WIP** 证书：指定从 Windows 信息保护中取消注册用户设备时是否从该用户设备中吊销本地加密密钥。吊销加密密钥后，用户将无法访问加密的公司数据。如果设置为关，取消注册后将不吊销这些密钥，并且用户可以继续有权访问受保护的文件。默认值为开。
- 显示覆盖图标：指定是否在资源管理器中的公司文件以及“开始”菜单中的仅企业应用程序磁贴中包括 Windows 信息保护图标叠加。默认值为关。

创建数据恢复证书

要启用 **Windows** 信息保护策略，需要数据恢复证书。

1. 在运行 XenMobile 控制台的计算机上，打开一个命令提示窗口并导航到要在其中创建证书的文件夹（Windows\System32 除外）。

2. 运行以下命令：

   ```
   cipher /r:ESFDRA
   ```

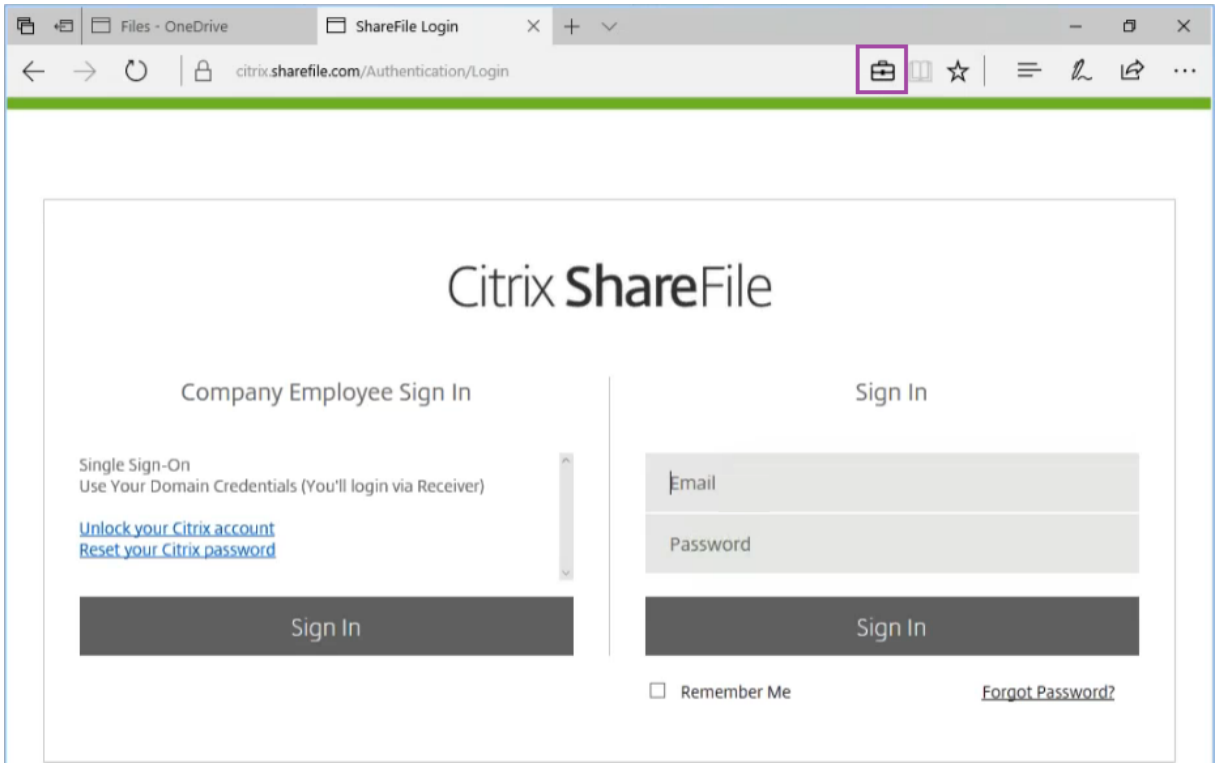
3. 系统提示时，请输入一个用于保护私钥文件的密码。

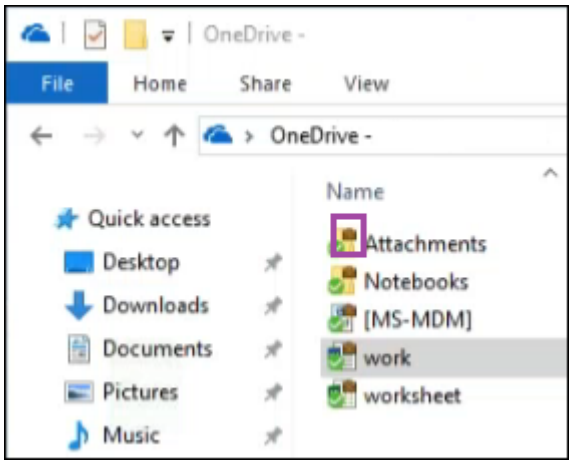
   cipher 命令将创建一个.cer 和.pfx 文件。

4. 在 XenMobile 控制台中，转至设置 **>** 证书并导入.cer 文件，该文件应用于 Windows 10 和 Windows 11 Tablet 和 Windows 10 Phone。

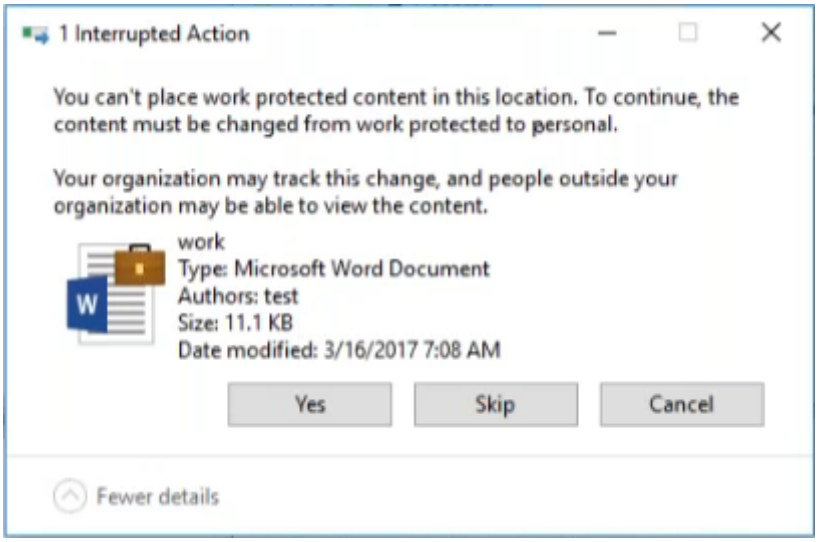
用户体验

当 Windows 信息保护生效时，应用程序和文件将包括一个图标：





如果用户复制受保护的文件或者将其保存到不受保护的位置，则将显示以下通知，具体取决于所配置的强制级别。



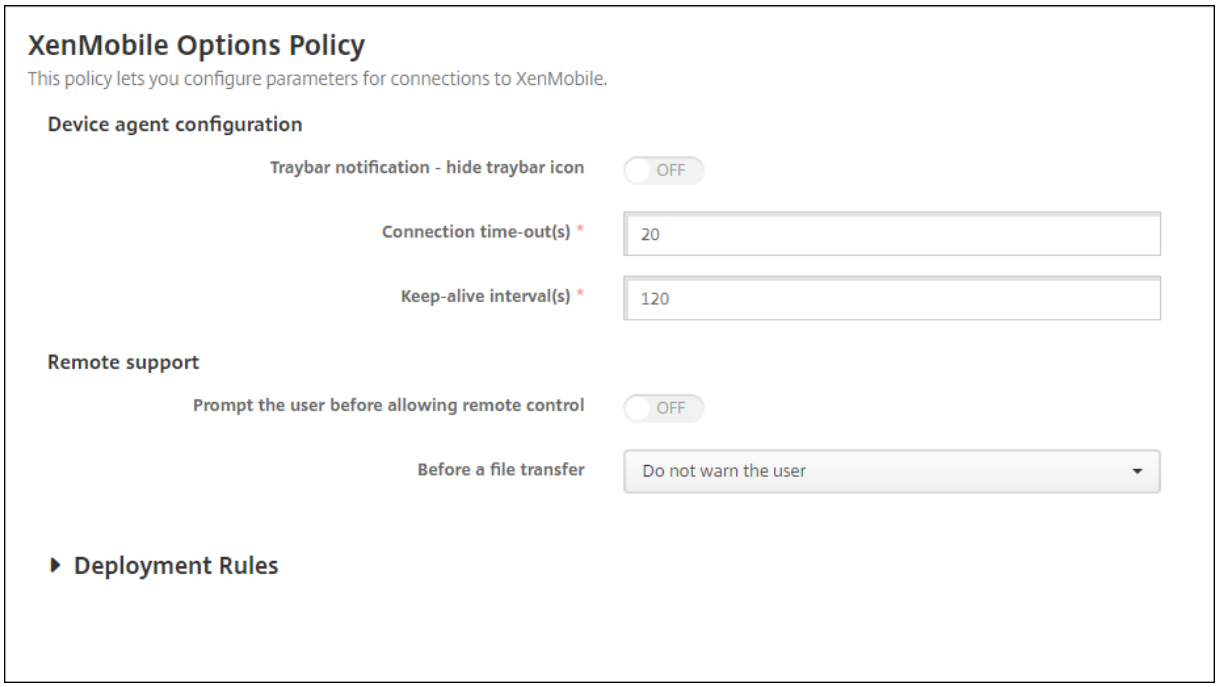
XenMobile 选项设备策略

November 12, 2020

添加 XenMobile 选项策略，用于配置在从 Android 和 Windows Mobile/CE 设备连接到 XenMobile 时 Secure Hub 的行为。

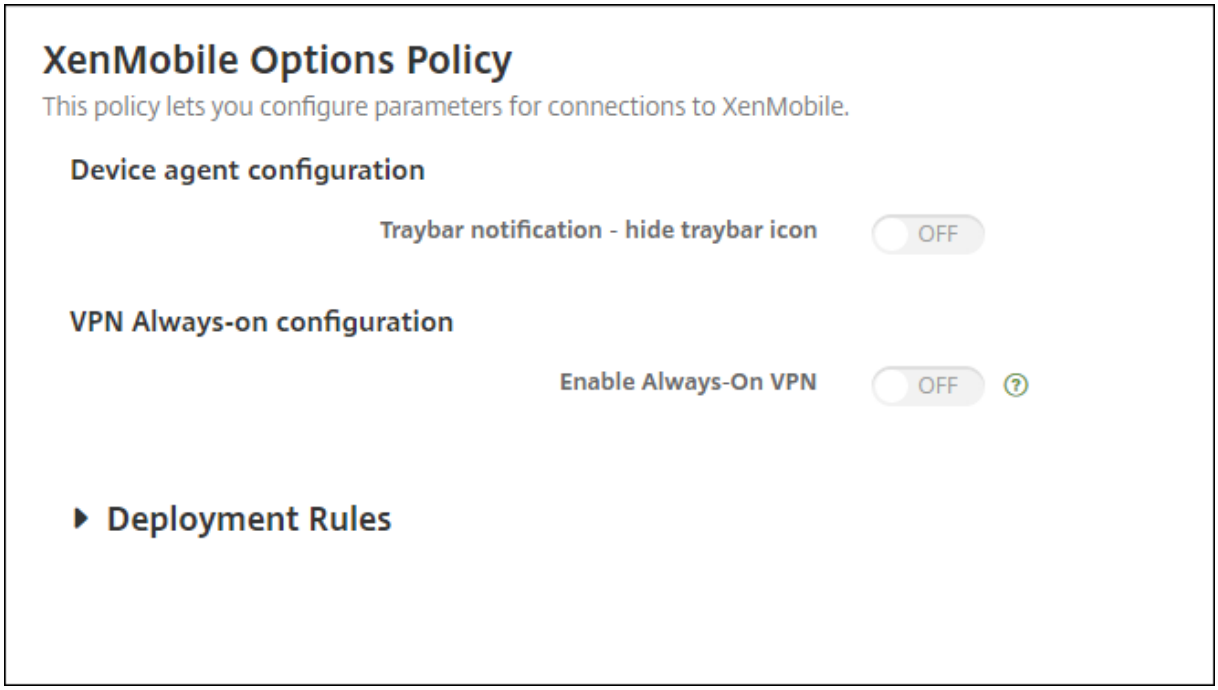
要添加或配置此策略，请转至配置 **>** 设备策略。有关详细信息，请参阅设备策略。

Android 设置



- 托盘栏通知 - 隐藏托盘栏图标：选择是隐藏还是显示托盘栏图标。默认值为关。
- 连接超时 (秒)：键入连接超时前连接可以空闲的时间长度（秒）。默认值为 20 秒。
- 保持连接时间间隔 (秒)：键入保持连接打开的时间长度（秒）。默认值为 120 秒。
- 在允许远程控制前提示用户：选择是否在允许远程支持控制前提示用户。默认值为关。
- 在文件传输前：在列表中，单击是否向用户警告文件传输，或是否请求用户许可。可用值：不警告用户、警告用户和请求用户许可。默认值为不警告用户。

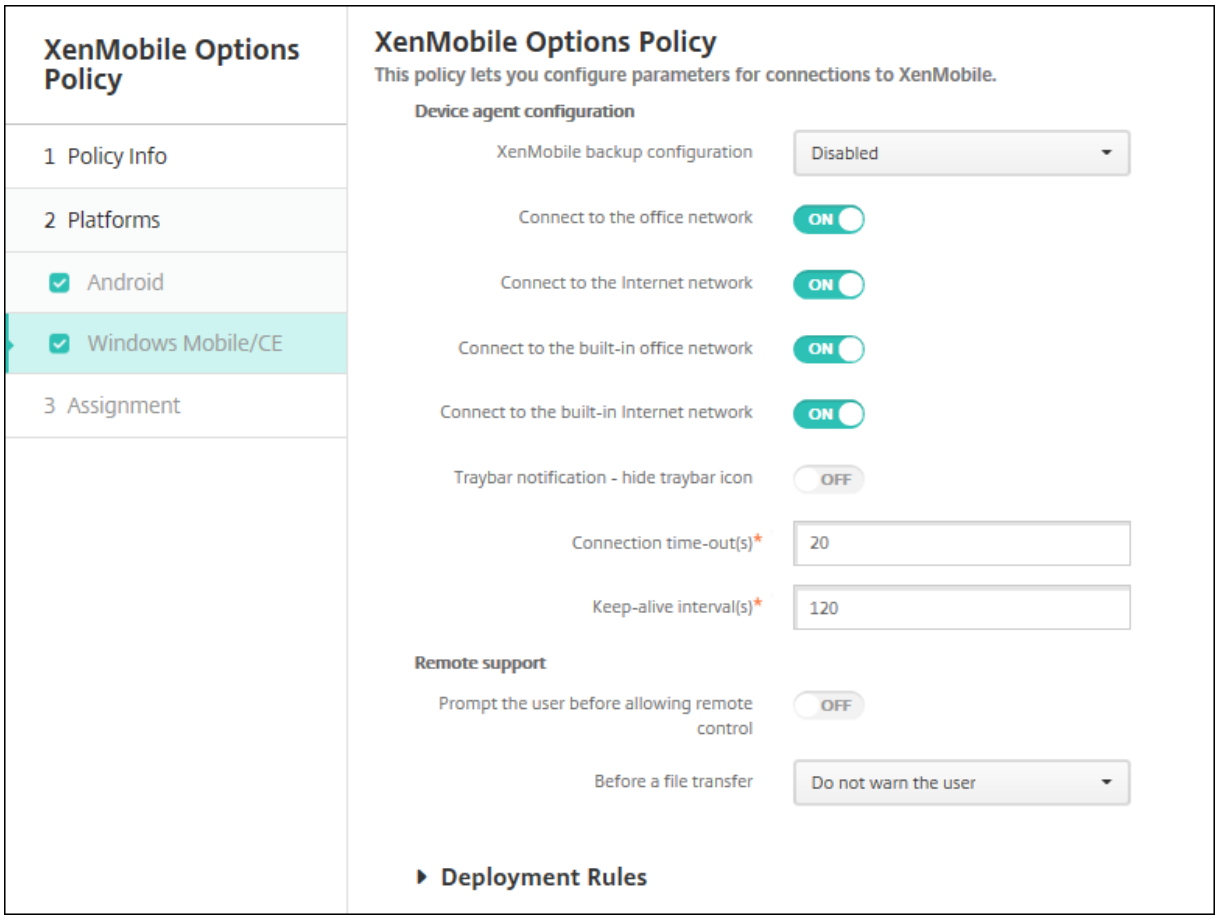
Android Enterprise 设置



支持从 Android 版本 7 开始。

- 托盘栏通知 **-** 隐藏托盘栏图标：选择是隐藏还是显示托盘栏图标。默认值为关。
- 启用始终可用的 **VPN**。选择是否启用始终可用的 VPN。当此设置设为开时，VPN 服务将在设备打开电源时启动，并在设备打开时继续运行。默认值为关。
- **VPN** 包。键入设备使用的 VPN 应用程序的软件包名称。默认情况下，Citrix SSO 应用程序的软件包名称 **com.citrix.CitrixVPN** 将在此字段中自动填充。

Windows Mobile/CE 设置



- 设备代理配置
  - **XenMobile** 备份配置：在列表中，单击用于在用户设备上备份 XenMobile 配置的选项。默认值为已禁用。可用选项包括：
    - 已禁用
    - 安装 XenMobile 后首次连接时
    - 每次设备重新启动后首次连接时
  - 连接到办公网络
  - 连接到 **Internet** 网络
  - 连接到内置办公网络：设置为开时，XenMobile 将自动检测网络。
  - 连接到内置 **Internet** 网络：设置为开时，XenMobile 将自动检测网络。
  - 托盘栏通知 **-** 隐藏托盘栏图标：选择是隐藏还是显示托盘栏图标。默认值为关。
  - 连接超时 **(**秒**)**：键入连接超时前连接可以空闲的时间长度（秒）。默认值为 20 秒。
  - 保持连接时间间隔 **(**秒**)**：键入保持连接打开的时间长度（秒）。默认值为 120 秒。
- 远程支持
  - 在允许远程控制前提示用户：选择是否在允许远程支持控制前提示用户。默认值为关。
  - 在文件传输前：在列表中，单击是否向用户警告文件传输，或是否请求用户许可。可用值：不警告用户、警告用户和请求用户许可。默认值为不警告用户。

XenMobile 卸载设备策略

January 5, 2022

可以在 XenMobile 中添加一个设备策略，用于从 Android 和 Window Mobile/CE 设备卸载 XenMobile。部署此策略时，它将从部署组中的所有设备上删除 XenMobile。

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。

配置 **Android** 和 **Windows Mobile/CE** 设置

- 从设备中卸载 **XenMobile**：选择是否从部署此策略的每个设备中卸载 XenMobile。默认值为关。

添加应用程序

January 5, 2022

将应用程序添加到 XenMobile 可提供移动应用程序管理 (MAM) 功能。XenMobile 可协助进行应用程序交付、软件许可、配置和应用程序生命周期管理。

启用了 MDX 的应用程序是准备大多数类型的应用程序以分发到用户设备的重要组成部分。有关 MDX 的简介，请参阅关于 MDX Toolkit 和 MAM SDK 概述。

- Citrix 建议对启用了 MDX 的应用程序使用 MAM SDK。或者，您可以继续使用 MDX 封装应用程序，直至弃用 MDX Toolkit。请参阅弃用。
- 不能使用 MDX Toolkit 封装 Citrix 移动生产力应用程序。从 Citrix 下载获取移动生产力应用程序 MDX 文件。

将应用程序添加到 XenMobile 控制台时，您可以：

- 配置应用程序设置
- （可选）将应用程序划分为多种类别，以便在 Secure Hub 对其进行组织整理
- （可选）定义工作流，以便在允许用户访问应用程序之前要求批准
- 向用户部署应用程序

本文介绍了添加应用程序的一般工作流程。有关平台详细信息，请参阅以下文章：

- 分发 Android Enterprise 应用程序
- 分发 Apple 应用程序

应用程序类型和功能

下表总结了可以使用 XenMobile 部署的应用程序类型。

应用程序类型	来源	备注	请参阅
MDX	您为用户开发的 iOS 和 Android 应用程序。Citrix 移动生产力应用程序	使用 MAM SDK 开发 iOS 或 Android 应用程序，或者使用 MDX Toolkit 封装。对于移动生产力应用程序，请从 Citrix 下载中下载公共应用商店 MDX 文件。然后，将应用程序添加到 XenMobile。	添加 MDX 应用程序
公共应用商店	Google Play 或 Apple App Store 等公共应用商店提供的免费或付费应用程序。	上载应用程序，为这些应用程序启用 MDX，然后将这些应用程序添加到 XenMobile。	添加公共应用商店应用程序
Web 和 SaaS 应用程序	您的内部网络（Web 应用程序）或公共网络 (SaaS)。	Citrix Workspace 从在 MDM 中注册的 iOS 和 Android 设备向本机 SaaS 应用程序提供移动单点登录功能。或者，使用安全断言标记语言 (SAML) 应用程序连接器	添加 Web 或 SaaS 应用程序
Enterprise	未启用 MDX 的专用应用程序，包括 Win32 应用程序。启用了 MDX 的专用 Android Enterprise 应用程序。企业应用程序驻留在内容交付网络位置或 XenMobile Server 中。	将应用程序添加到 XenMobile。	添加企业应用程序
Web 链接	不需要单点登录的 Internet Web 地址、内联网 Web 地址或 Web 应用程序。	在 XenMobile 中配置 Web 链接。	添加 Web 链接

在规划应用程序分发时，请考虑以下功能：

- 关于无提示安装
- 关于必需应用程序和可选应用程序
- 关于应用程序类别
- 启用 Microsoft 365 应用程序

- 应用工作流
- 应用商店和 Citrix Secure Hub 外观方案

关于无提示安装

Citrix 支持 iOS、Android Enterprise 和 Samsung 应用程序的无提示安装和升级。无提示安装意味着系统不会提示用户安装您部署到设备的应用程序。应用程序将在后台自动安装。

实施无提示安装的必备条件：

- 对于 iOS，请将托管 iOS 设备置于受监督模式。有关详细信息，请参阅导入 iOS 和 macOS 配置文件设备策略。
- 对于 Android Enterprise，应用程序会安装在设备上的 Android 工作配置文件中。有关详细信息，请参阅 Android Enterprise。
- 对于 Samsung 设备，请在设备上启用 Samsung Knox。

  为此，请设置 Samsung MDM 许可证密钥设备策略以生成 Samsung ELM 和 Knox 许可证密钥。有关详细信息，请参阅 Samsung MDM 许可证密钥设备策略。

关于必需应用程序和可选应用程序

向交付组中添加应用程序时，请选择这些应用程序是可选应用程序还是必需应用程序。Citrix 建议根据需要部署应用程序。

- 所需的应用程序以无提示方式安装在用户设备上，从而最大限度地减少交互。启用此功能还将允许应用程序自动更新。
- 可选应用程序允许用户选择要安装的应用程序，但用户必须通过 Secure Hub 手动启动安装。

对于标记为必需的应用程序，用户在诸如以下情况下能够立即收到更新：

- 上载新应用程序并根据需要对其进行标记。
- 根据需要标记现有应用程序。
- 用户删除所需的应用程序。
- Secure Hub 更新可用。

必需应用程序的强制部署要求

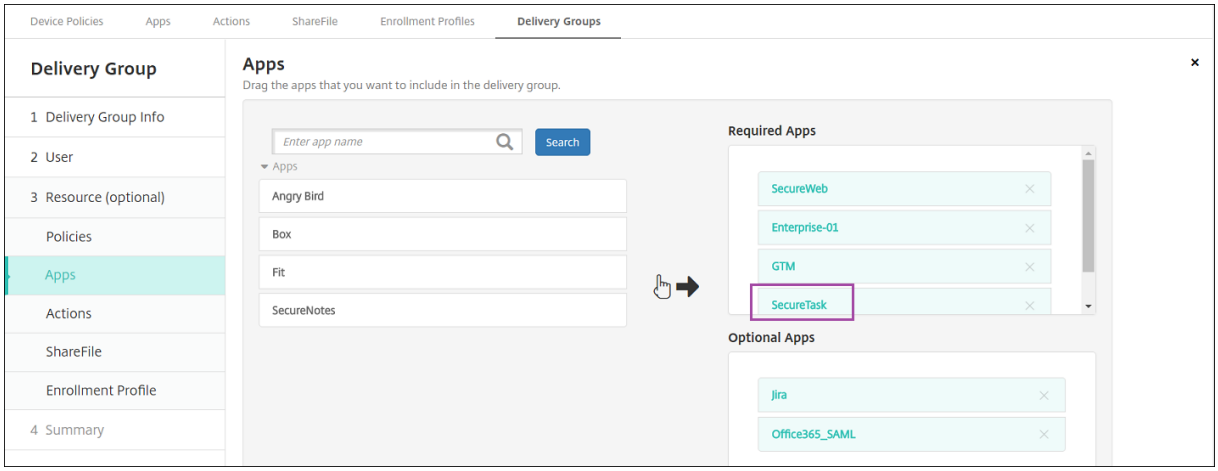
- XenMobile Server 10.6（最低版本）
- Secure Hub 10.5.15 for iOS 和 Secure Hub 10.5.20 for Android（最低版本）
- MAM SDK 或 MDX Toolkit 10.6（最低版本）
- 自定义服务器属性 force.server.push.required.apps

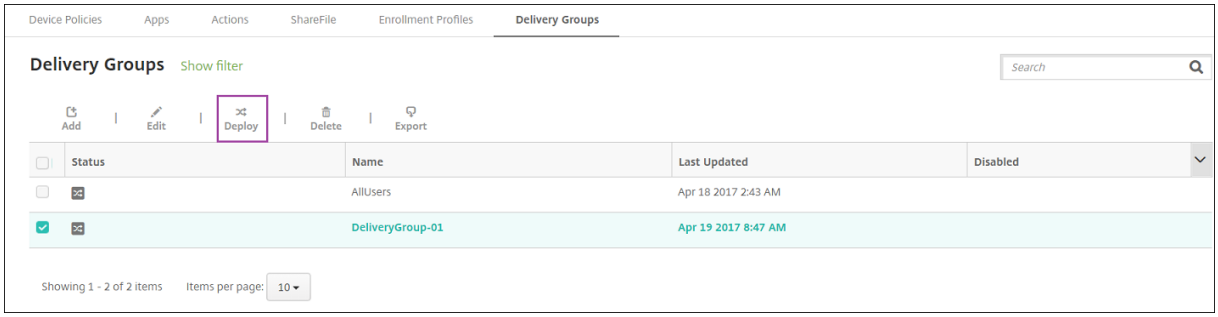
  默认情况下，所需应用程序的强制部署处于禁用状态。要启用该功能，请创建一个“自定义密钥”服务器属性。将密钥和显示名称设置为 **force.server.push.required.apps**，将值设置为 **true**。

- 升级 XenMobile Server 和 Secure Hub 后：使用已注册的设备的用户必须注销并登录 Secure Hub 一次，以获取所需的应用程序部署更新。

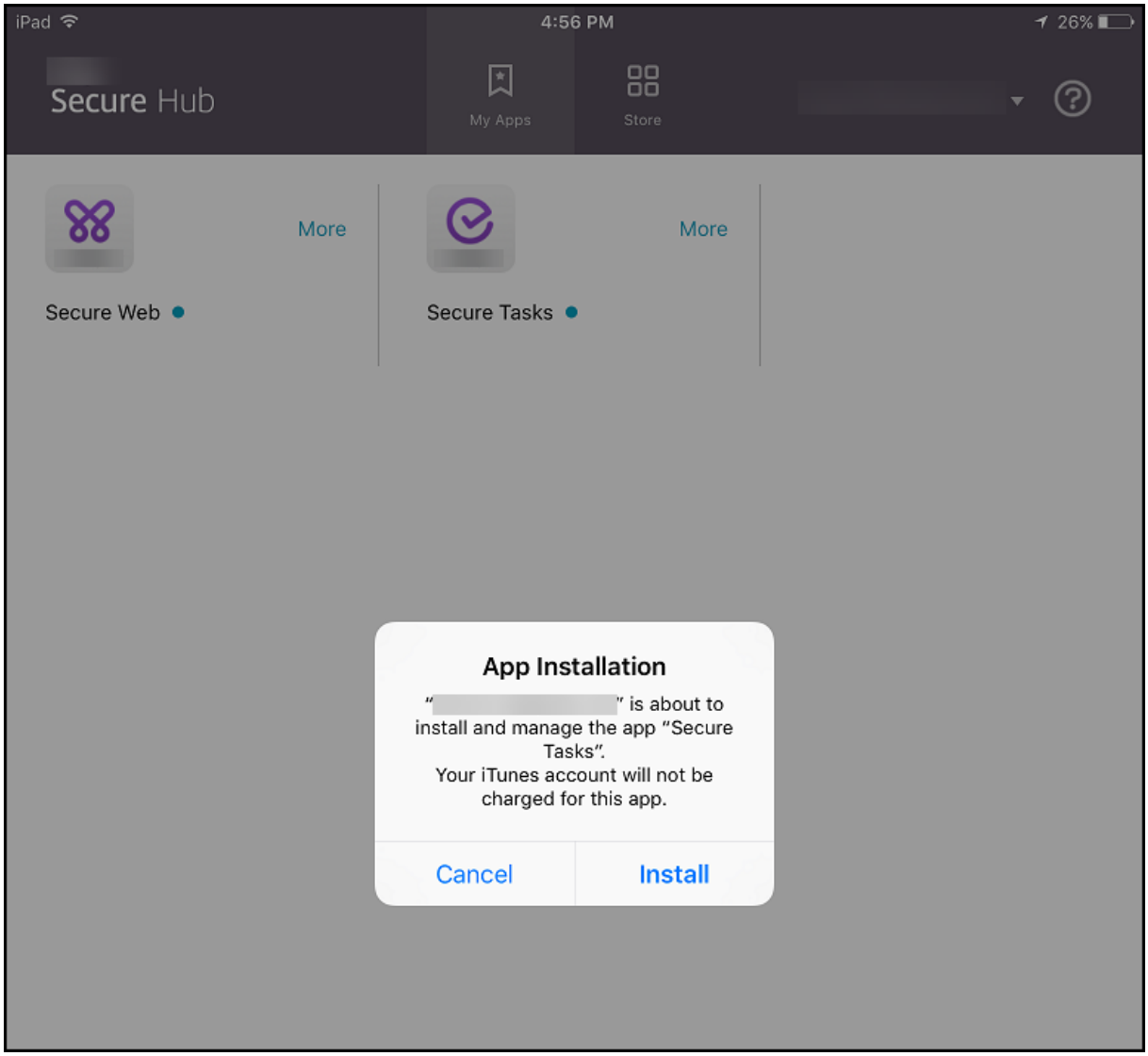
示例

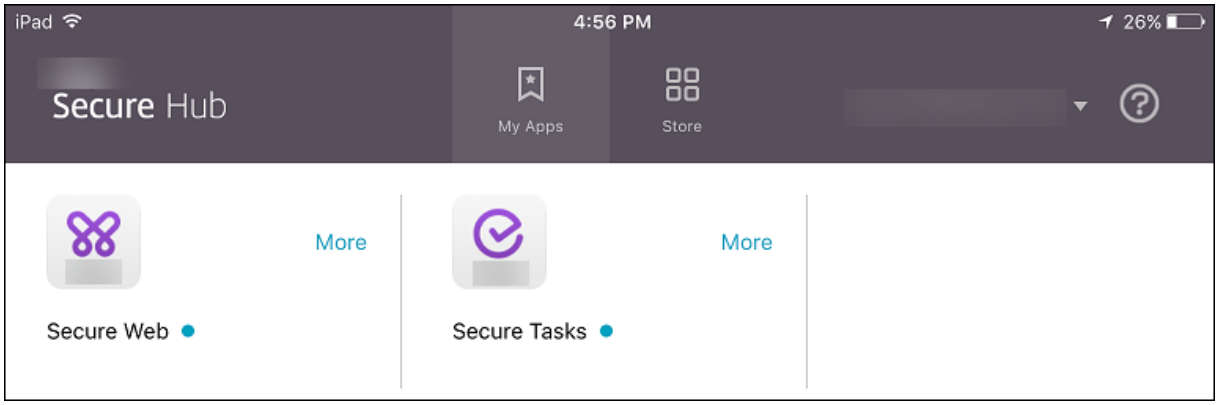
以下示例显示了向交付组添加名为 Secure Tasks 的应用程序并部署交付组的顺序。





示例应用程序 Secure Tasks 部署到用户设备后，Secure Hub 将提示用户安装该应用程序。





> 重要：
>
> 启用了 MDX 的必需应用程序（包括企业应用程序和公共应用商店应用程序）将立即升级。即使您配置了应用程序更新宽限期 MDX 策略并且用户选择以后升级应用程序，也会升级。

面向企业和公共应用商店应用程序的 **iOS** 必需应用程序工作流

1. 首次注册期间部署 XenMobile Apps。必需应用程序安装在设备上。
2. 在 XenMobile 控制台上更新应用程序。
3. 使用 XenMobile 控制台部署必需应用程序。
4. 主屏幕上的应用程序将更新。并且，对于公共应用商店应用程序，升级将自动启动。系统不提示用户进行更新。
5. 用户从主屏幕中打开应用程序。即使您设置了应用程序更新宽限期并且用户以后轻按即可升级应用程序，应用程序也会立即升级。

面向企业应用程序的 **Android** 必需应用程序工作流

1. 首次注册期间部署 XenMobile Apps。必需应用程序安装在设备上。
2. 使用 XenMobile 控制台部署必需应用程序。
3. 应用程序已升级。（Nexus 设备提示安装更新，但 Samsung 设备执行无提示安装。）
4. 用户从主屏幕中打开应用程序。即使您设置了应用程序更新宽限期并且用户以后轻按即可升级应用程序，应用程序也会立即升级。（Samsung 设备执行无提示安装。）

面向公共应用商店应用程序的 **Android** 必需应用程序工作流

1. 首次注册期间部署 XenMobile Apps。必需应用程序安装在设备上。
2. 在 XenMobile 控制台上更新应用程序。
3. 使用 XenMobile 控制台部署必需应用程序。或者，在设备上打开 Secure Hub Store。更新图标在应用商店中显示。
4. 应用程序升级自动启动。（Nexus 设备将提示用户安装更新。）
5. 在主屏幕中打开应用程序。应用程序已升级。系统不提示用户宽限期。（Samsung 设备执行无提示安装。）

根据需要配置应用程序时卸载应用程序

可以允许用户根据需要卸载配置的应用程序。转到配置 **>** 交付组，然后将应用程序从必需应用程序移动到可选应用程序。

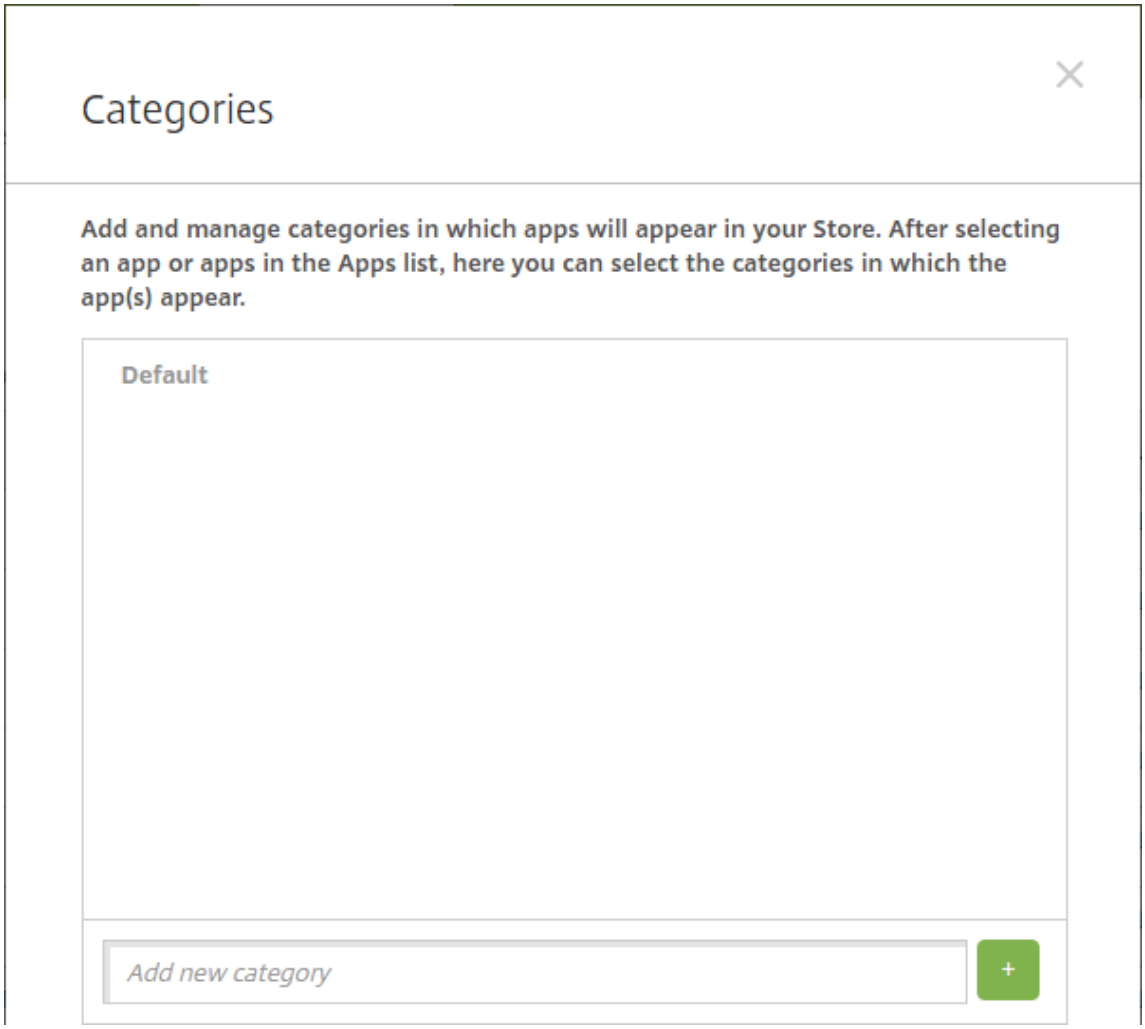
建议：请使用特殊交付组临时将应用程序更改为可选，以便特定用户可以卸载该应用程序。然后，您可以将现有的必需应用程序更改为可选，将应用程序部署到该交付组，然后从这些设备中卸载该应用程序。之后，如果您希望该交付组的未来注册需要该应用程序，则可以将该应用程序设置回必需。

关于应用程序类别

用户登录 Secure Hub 时，会收到您已在 XenMobile 中设置的应用程序、Web 链接和应用商店的列表。您可以使用应用程序类别实现只允许用户访问某些应用程序、应用商店或 Web 链接的目的。例如，您可以创建“财务”类别，然后向其中添加仅与财务相关的应用程序。您也可以配置“销售”类别，并向其分配销售应用程序。

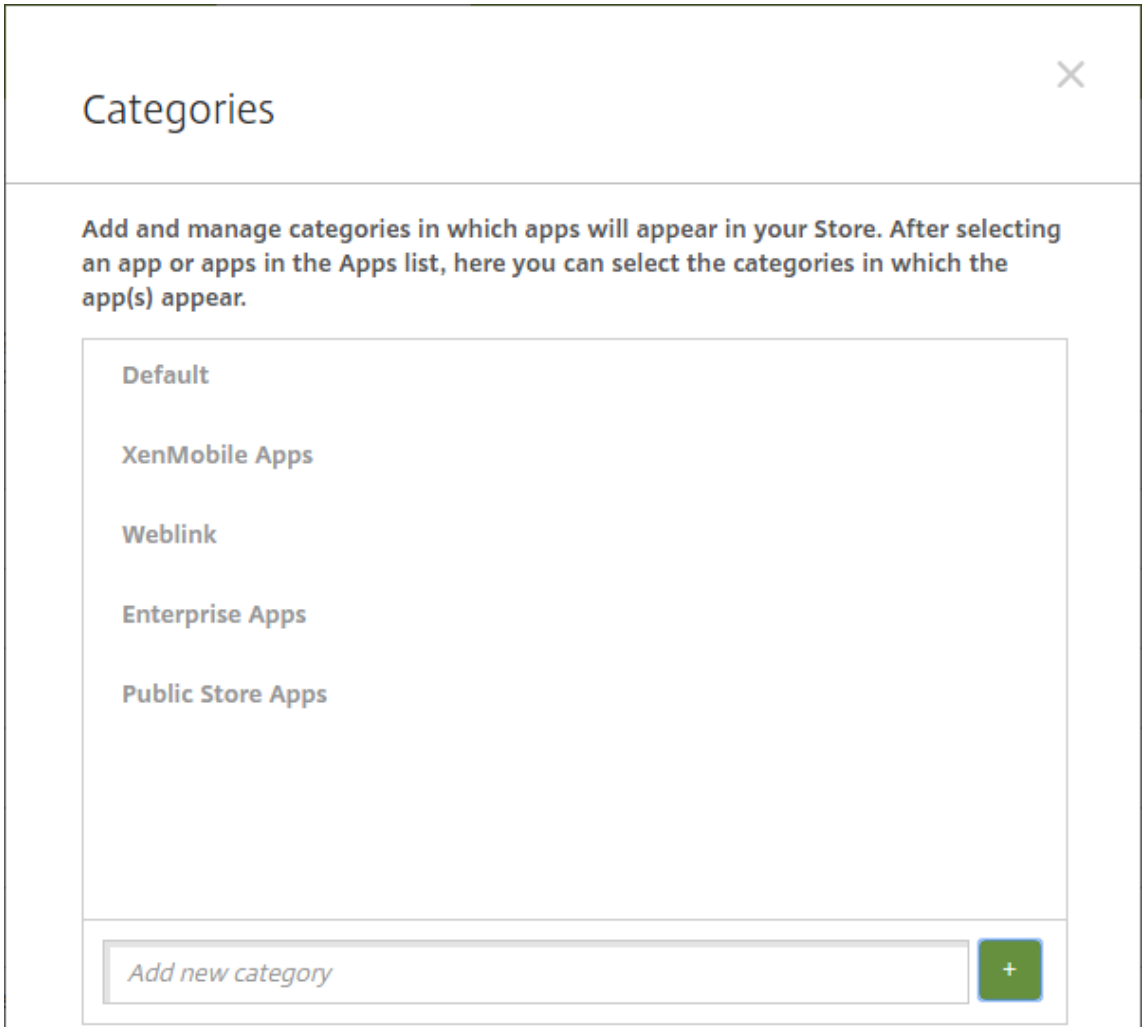
添加或编辑应用程序、Web 链接或应用商店时，可以将应用程序添加到您所配置的一个或多个类别中。

1. 在 XenMobile 控制台中，单击配置 **>** 应用程序 **>** 类别。此时将显示类别对话框。



2. 对于要添加的每个类别，执行以下操作：

   - 在对话框底部的添加新类别字段中键入要添加的类别的名称。例如，可以键入企业应用程序以创建企业应用程序类别。
   - 单击加号 (+) 以添加类别。此时已添加新创建的类别并显示在类别对话框中。



3. 添加完类别后，关闭类别对话框。
4. 在应用程序页面上，可以将现有应用程序放到新类别中。
   - 选择要分类的应用程序。
   - 单击编辑。此时将显示应用程序信息页面。
   - 在应用程序类别列表中，通过选中新类别的复选框应用新类别。对于您不想应用于应用程序的现有类别，可以取消选中其对应的复选框。
   - 单击交付组分配选项卡或单击后面各页面上的下一步完成剩余的应用程序设置页面。
   - 单击交付组分配页面上的保存以应用新类别。新类别将应用于应用程序并显示在应用程序表中。

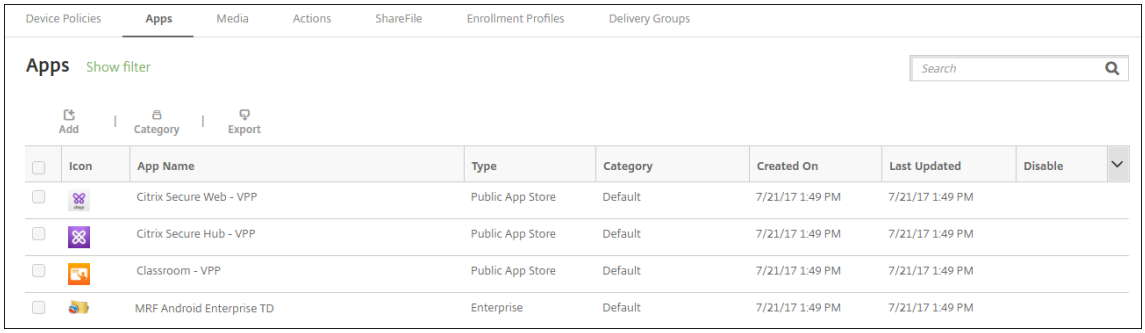
添加 **MDX** 应用程序

收到适用于 iOS 或 Android 应用程序的 MDX 文件时，可以将应用程序上载到 XenMobile。上载应用程序后，可以配置应用程序详细信息和策略设置。有关每种设备平台类型可用的应用程序策略的详细信息，请参阅：

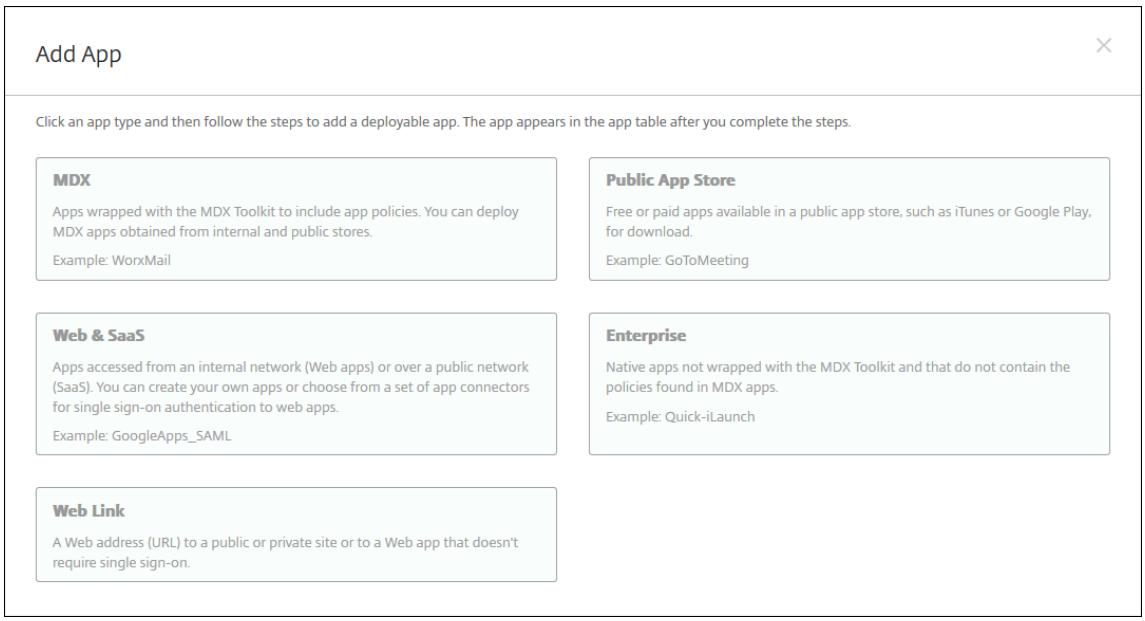
- MAM SDK 概述

- MDX 策略概览

1. 在 XenMobile 控制台中，单击配置 **>** 应用程序。此时将显示应用程序页面。



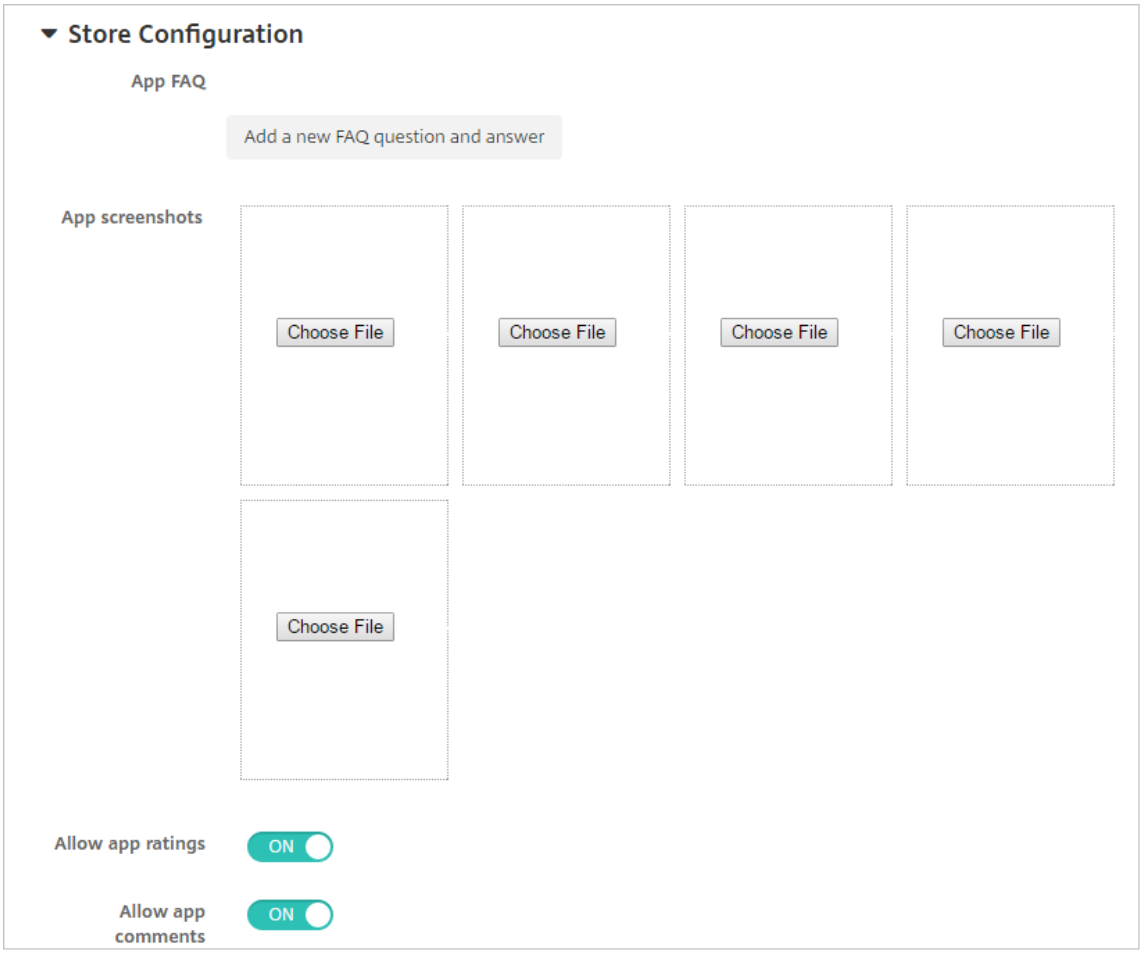
2. 单击添加。此时将显示添加应用程序对话框。



3. 单击 **MDX**。此时将显示 **MDX** 应用程序信息页面。
4. 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。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
5. 单击 **Next**（下一步）。此时将显示应用程序平台页面。
6. 在平台下，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。
7. 要选择要上载的 MDX 文件，请单击上载并导航到文件所在位置。
8. 在应用程序详细信息页面中，配置以下设置：
   - 文件名：键入与应用程序关联的文件名。

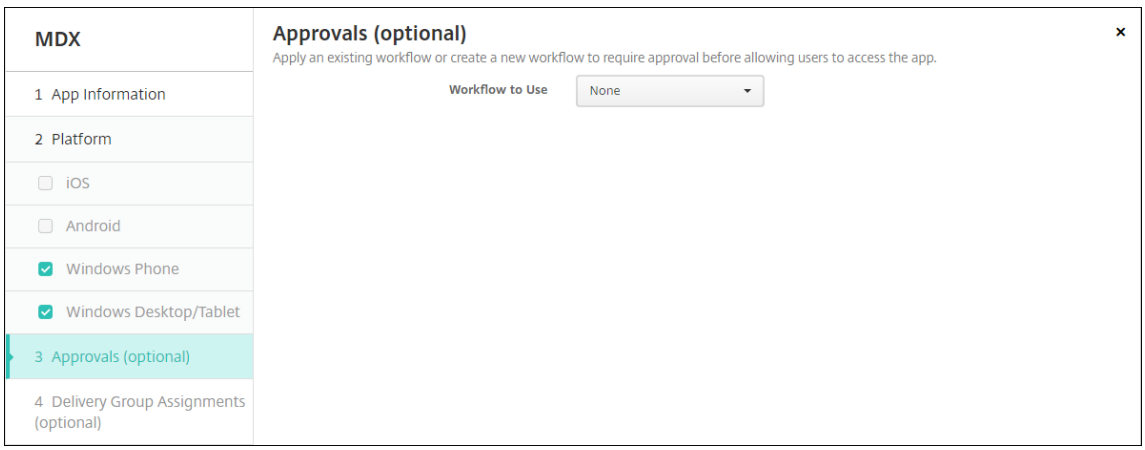
- 应用程序说明：键入应用程序的说明。
- 应用程序版本：（可选）键入应用程序版本号。
- 软件包 **ID**：键入从托管的 Google Play 商店获取的应用程序包 ID。
- 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
- 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
- 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
- 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否从 iOS 设备中删除应用程序。默认值为开。
- 阻止备份应用程序数据：选择是否阻止用户在 iOS 设备上备份应用程序数据。默认值为开。
- 产品轨迹：指定要推送到 iOS 设备的产品轨迹。如果您有一个专为测试而设计的轨迹，则可以选择并将其分配给您的用户。默认值为生产。
- 强制管理应用程序：对于安装为非托管的应用程序，请选择是否提示用户允许在未受监督的 iOS 设备上管理此应用程序。默认值为开。
- 通过批量购买部署的应用程序：选择是否使用 Apple 批量购买部署应用程序。如果设置为开，并且您部署了应用程序的 MDX 版本并使用批量购买部署该应用程序，Secure Hub 将仅显示批量购买实例。默认值为关。

9. 配置 **MDX** 策略。MDX 策略因平台而异，并且包含面向诸如身份验证、设备安全和应用程序限制的策略区域。在控制台中，每种策略都具有介绍此策略的提示。
10. 配置部署规则。有关信息，请参阅部署规则。
11. 展开应用商店配置。



- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

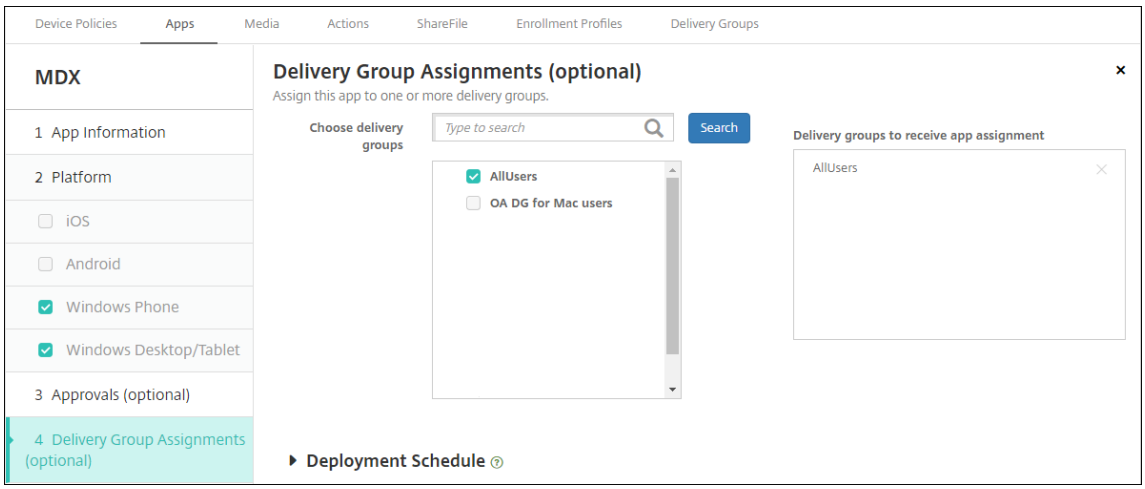
12. 单击 **Next**（下一步）。此时将显示审批页面。



要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果您不想设置审批工作流程，请继

续下一步。

13. 单击 **Next**（下一步）。此时将显示交付组分配页面。



14. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。

15. 展开部署计划，然后配置以下设置：

    - 部署：选择是否将应用程序部署到设备。默认值为开。
    - 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
    - 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

    如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则为始终启用的连接部署选项适用。

    配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

16. 单击保存。

添加公共应用商店应用程序

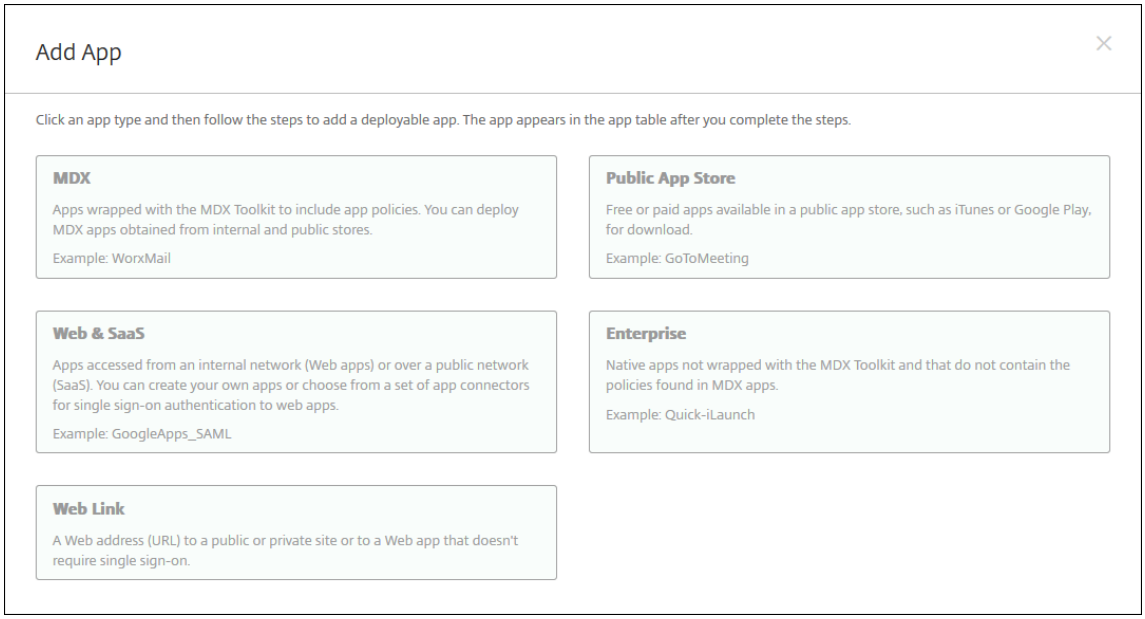
可以向 XenMobile 中添加公共应用商店（如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。

可通过相关设置将系统配置为从 Apple App Store 中检索应用程序名称和说明。在应用商店中检索应用程序信息时，XenMobile 会覆盖现有名称和说明。手动配置 Google Play 应用商店应用程序信息。

添加面向 Android Enterprise 的付费公共应用商店应用程序时，可以查看批量购买许可状态。该状态显示可用许可证总数、当前正在使用的数量以及占用这些许可证的每个用户的电子邮件地址。面向 Android Enterprise 的批量购买计划简化了组织批量查找、购买和分发应用程序及其他数据的过程。

配置应用程序信息并选择用于交付应用程序的平台，以：

1. 在 XenMobile 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。



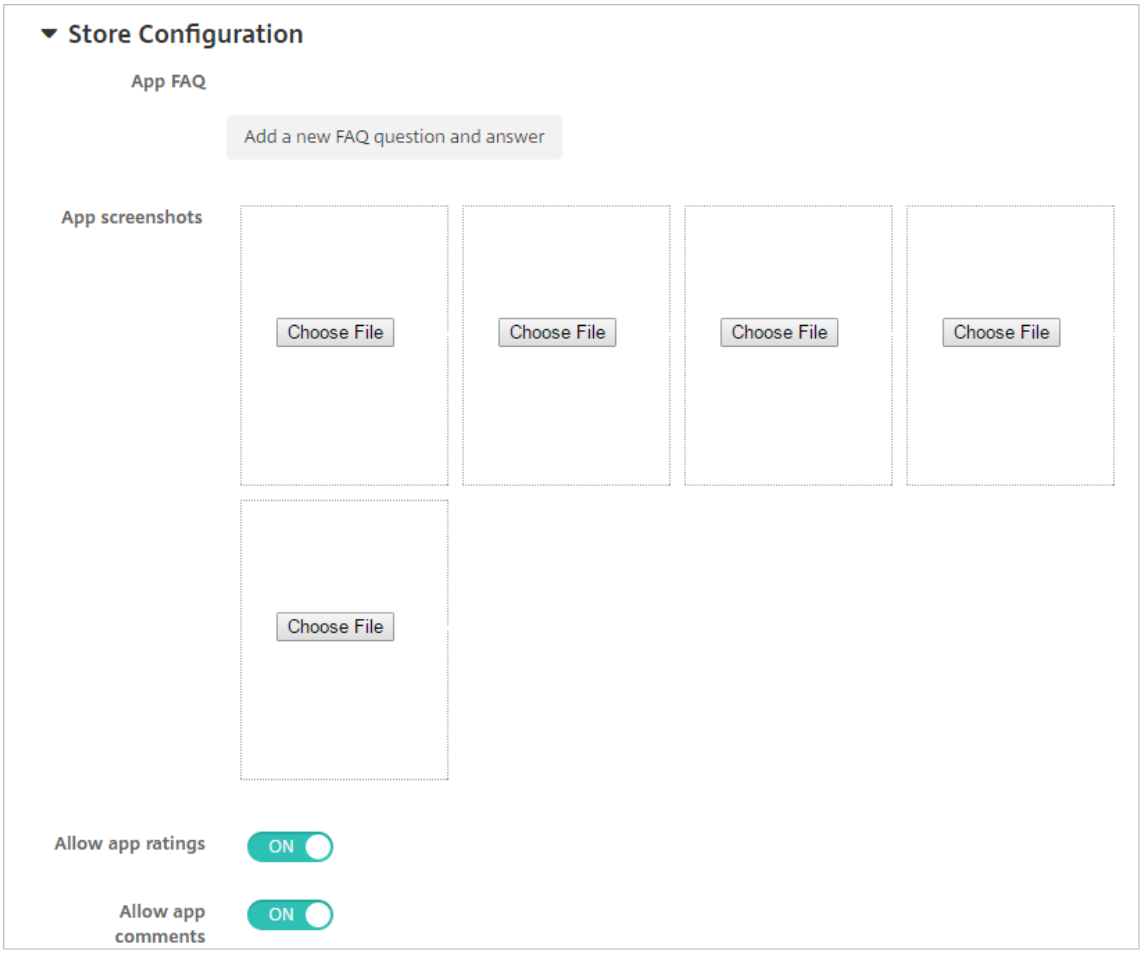
2. 单击公共应用商店。此时将显示应用程序信息页面。
3. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在应用程序表中的应用程序名称下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 单击 **Next**（下一步）。此时将显示应用程序平台页面。
5. 在平台下，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

下一步，请为每个平台配置应用程序设置。请参阅：

- 为 Google Play 应用程序配置应用程序设置
- 托管应用商店应用程序
- 配置 iOS 应用程序的应用程序设置

完成为平台配置设置后，请设置平台部署规则和应用商店配置。

1. 配置部署规则。有关信息，请参阅部署规则。
2. 展开应用商店配置。



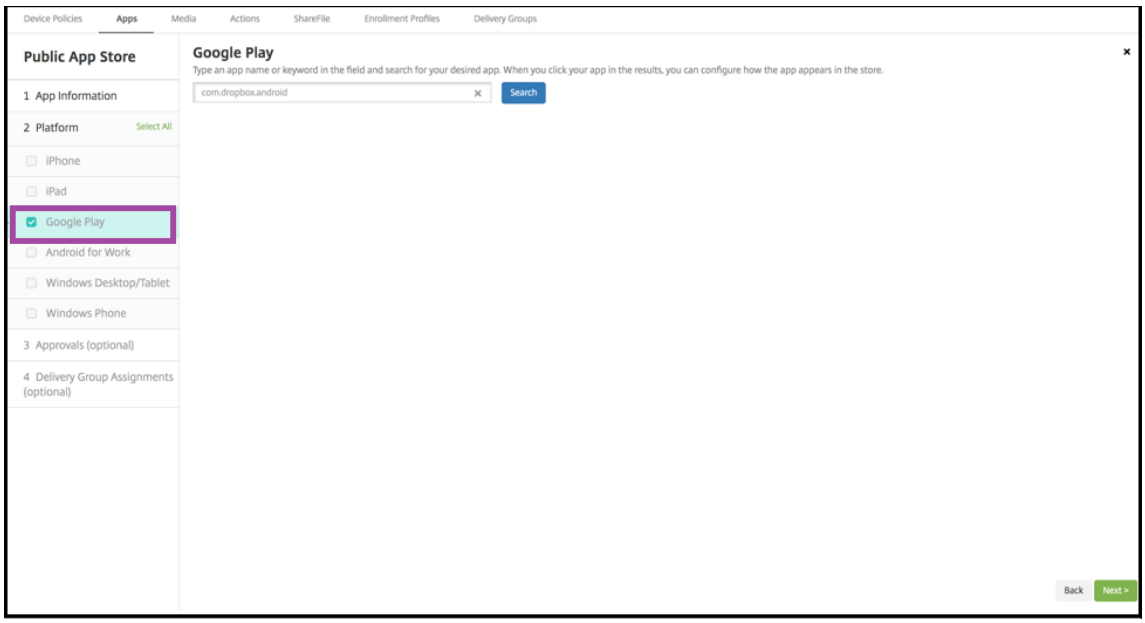
- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

为 **Google Play** 应用程序配置应用程序设置

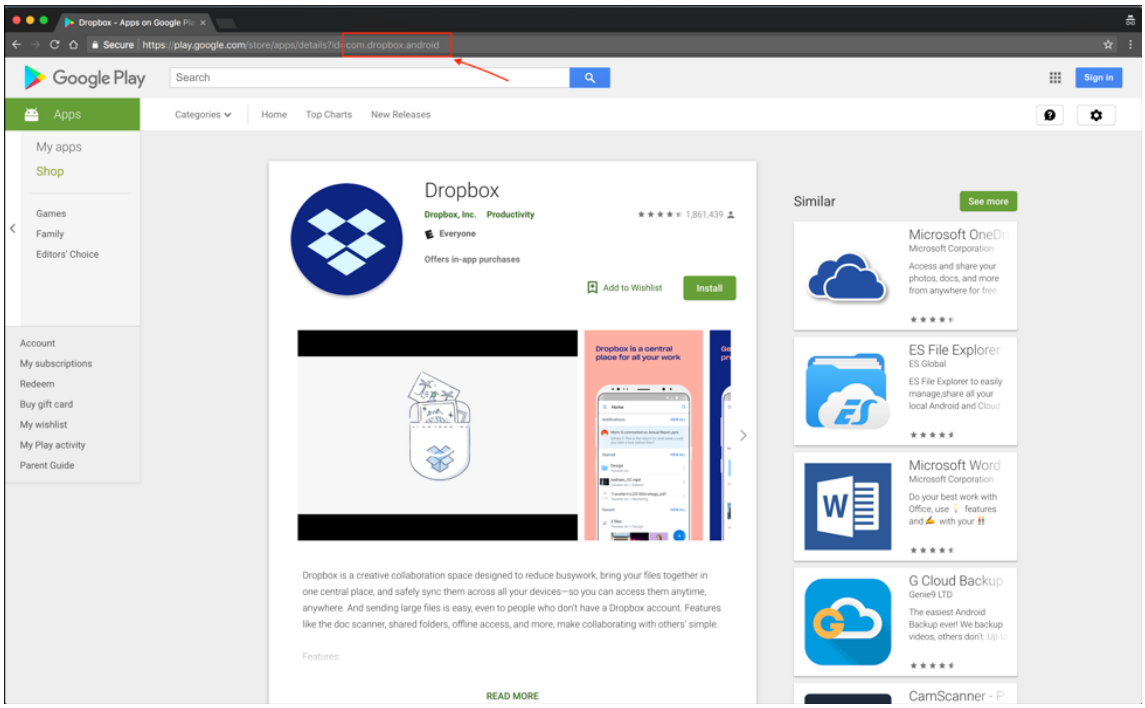
> 注意：
>
> 要使可从托管 Google Play 访问的 Google Play 应用商店中的所有应用程序，请使用访问托管 **Google Play** 应用商店中的所有应用程序 XenMobile Server 属性。请参阅服务器属性。将此属性设置为 **true** 会将所有 Android Enterprise 用户的公共 Google Play 应用商店应用程序列入允许列表。然后，您可以使用限制设备策略来控制对这些应用程序的访问。

配置 Google Play 应用商店应用程序设置要求执行的步骤与适用于其他平台的应用程序不同。必须手动配置 Google Play 应用商店应用程序信息。

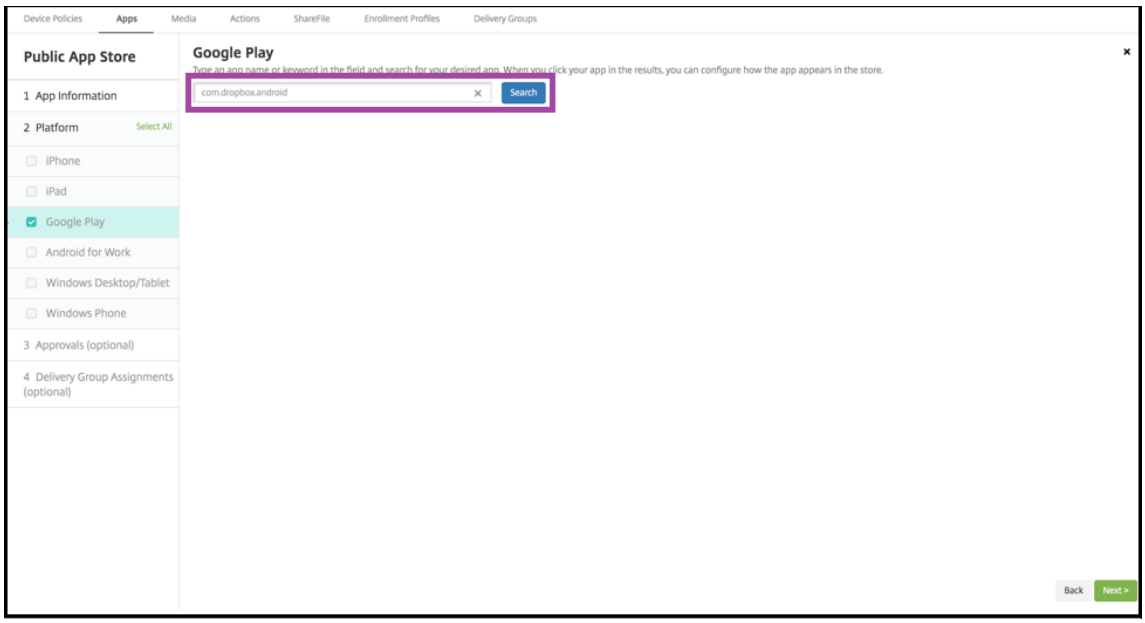
1. 确保在平台下选择 **Google Play**。



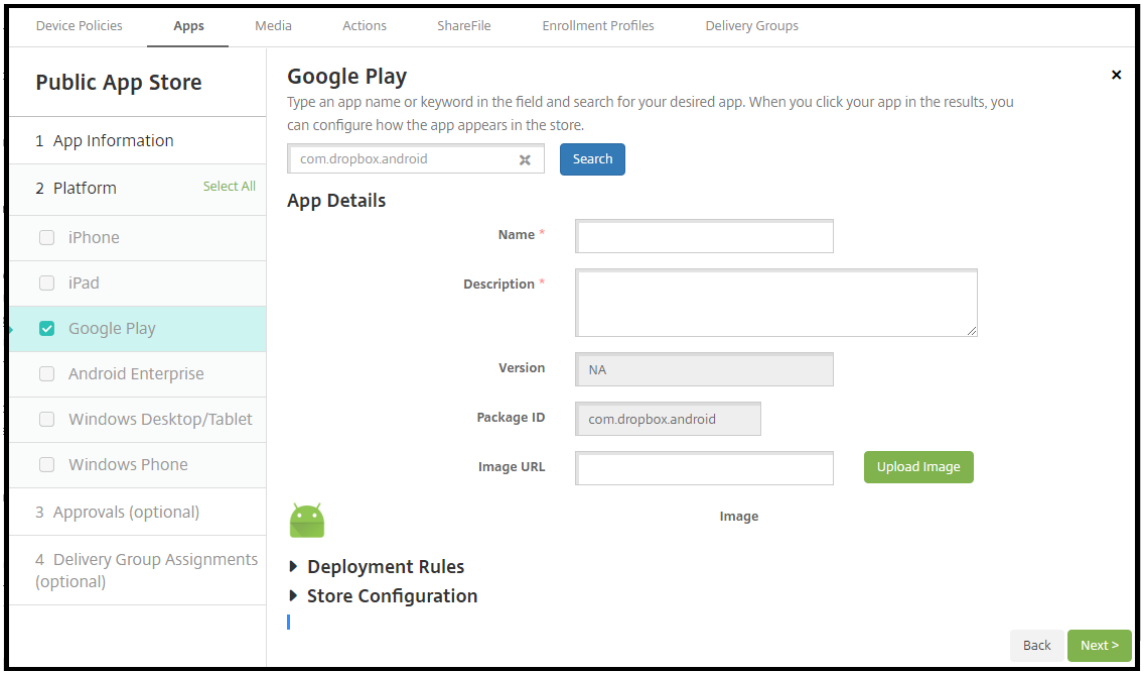
2. 转至 Google Play 应用商店。从 Google Play 应用商店复制软件包 ID。可以在应用程序的 URL 中找到 ID。



3. 在 XenMobile Server 控制台中添加公共应用商店应用程序时，将软件包 ID 粘贴到搜索栏中。单击搜索。



4. 如果软件包 ID 有效，将显示一个 UI，允许您输入应用程序详细信息。



5. 可以为要随应用商店中的应用程序显示的映像配置 URL。要使用 Google Play 应用商店中的映像，请执行以下操作：

   a) 转至 Google Play 应用商店。右键单击该应用程序映像并复制映像地址。

   b) 将映像地址粘贴到映像 **URL** 字段中。

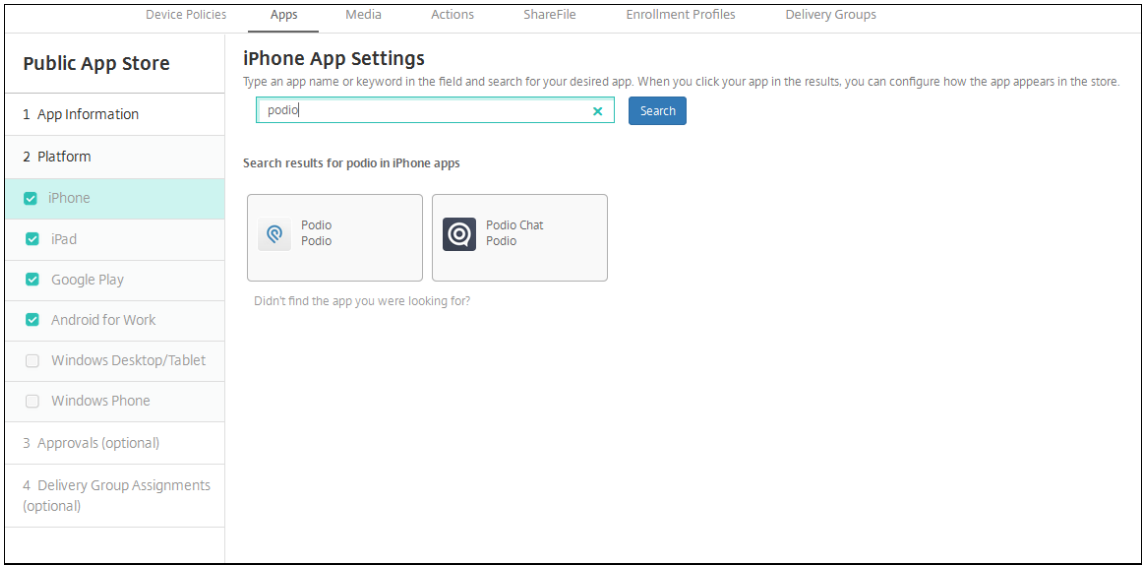
   c) 单击 **Upload image**（上载映像）。该映像将显示在 **Image**（映像）旁边。

如果未配置映像，通用 Android 映像将随应用程序显示。

配置 **iOS** 应用程序的应用程序设置

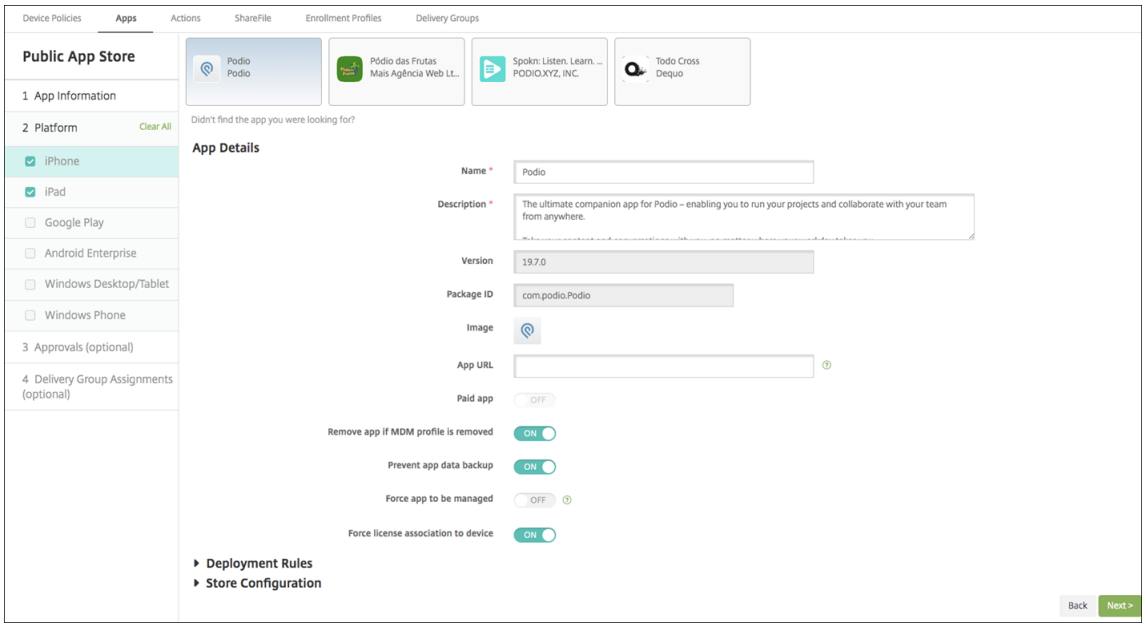
1. 在搜索框中键入应用程序名称，然后单击搜索。此时将显示符合搜索条件的应用程序。此时将显示符合搜索条件的应用程序。

   下图显示了 iPhone 上的应用程序中的 **podio** 的搜索结果。



2. 单击要添加的应用程序。

3. 应用程序详细信息字段预填充了与所选应用程序相关的信息（包括名称、说明、版本号和关联的图像）。



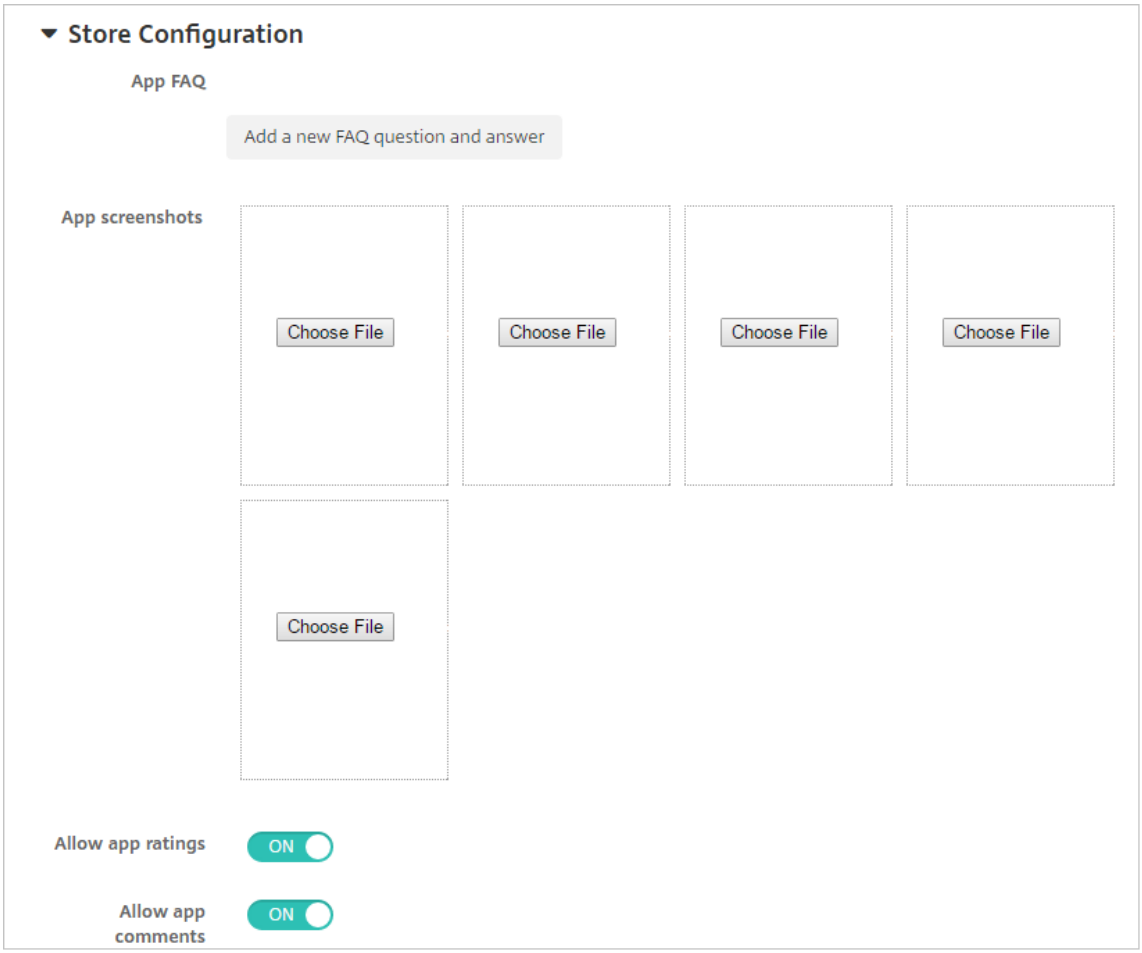
4. 配置以下设置：

   - 如有需要，可更改应用程序的名称和说明。
   - 付费应用程序：此字段已预配置，并且无法更改。

- 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否删除应用程序。默认值为开。
- 阻止备份应用程序数据：选择是否阻止应用程序备份数据。默认值为开。
- 产品轨迹：指定要推送到用户设备的产品轨迹。如果您有一个专为测试而设计的轨迹，则可以选择并将其分配给您的用户。默认值为生产。
- 强制管理应用程序：选择当安装的应用程序未托管时，是否提示用户允许在未受监督的设备上管理此应用程序。默认值为关。在 iOS 9.0 及更高版本中可用。
- 强制与设备建立许可证关联：选择是否将开发时启用设备关联的应用程序与设备而非用户关联。在 iOS 9 及更高版本中可用。如果所选应用程序不支持分配到设备，则您无法更改此字段。

5. 配置部署规则。有关信息，请参阅部署规则。

6. 展开应用商店配置。



- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

7. 对于 iPhone 或 iPad，展开批量购买。

   a) 要启用 XenMobile 以为应用程序应用批量购买许可证，请执行以下操作：在批量购买许可证列表中，单

击上载批量购买许可证。

b) 在显示的对话框中，导入许可证。

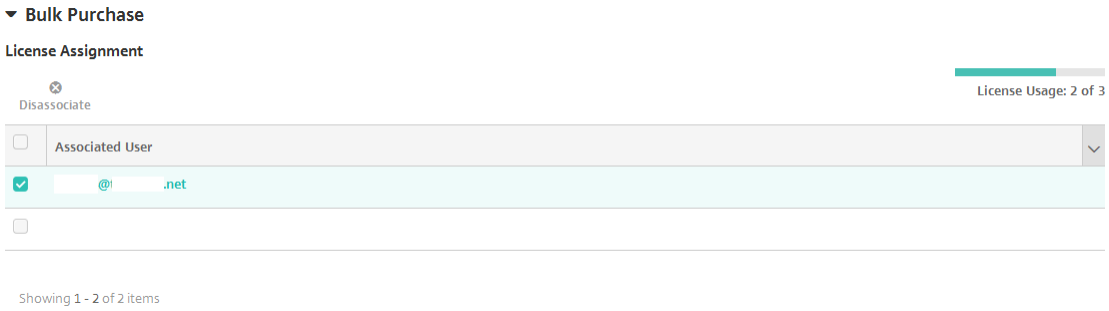
“许可协议”表显示应用程序正在使用的许可证数量以及可用的许可证总数。

可以取消单个用户的批量购买许可证的关联。这样将终止许可证分配并释放许可证。

8. 对于 Android Enterprise，请展开批量购买部分。

“许可协议”表显示应用程序正在使用的许可证数量以及可用的许可证总数。

可以选择一个用户，然后单击解除关联以结束其许可证分配，释放一个许可证以供其他用户使用。但是，如果该用户不属于包含特定应用程序的交付组的一部分，您将只能取消该许可证的关联。



9. 完成批量购买或批量购买设置后，单击下一步。此时将显示审批页面。

要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果您不需要审批工作流程，请继续执行下一步。

10. 单击 **Next**（下一步）。此时将显示交付组分配页面。

11. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。

12. 展开部署计划，然后配置以下设置：

- 部署：选择是否将应用程序部署到设备。默认值为开。
- 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
- 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则为始终启用的连接部署适用。

配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

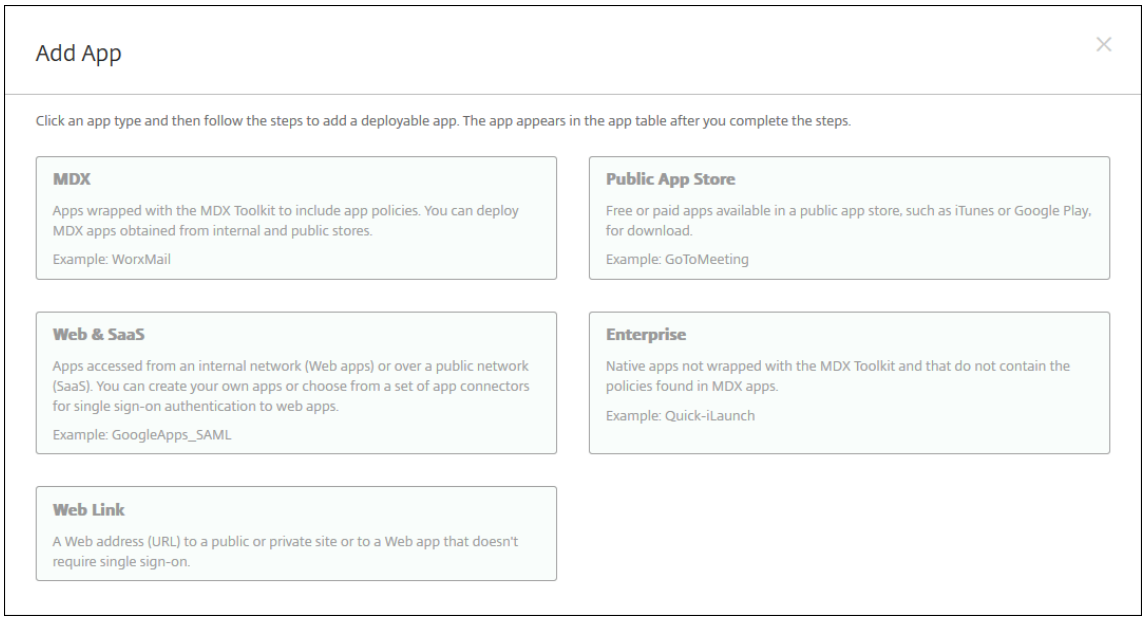
13. 单击保存。

添加 **Web** 或 **SaaS** 应用程序

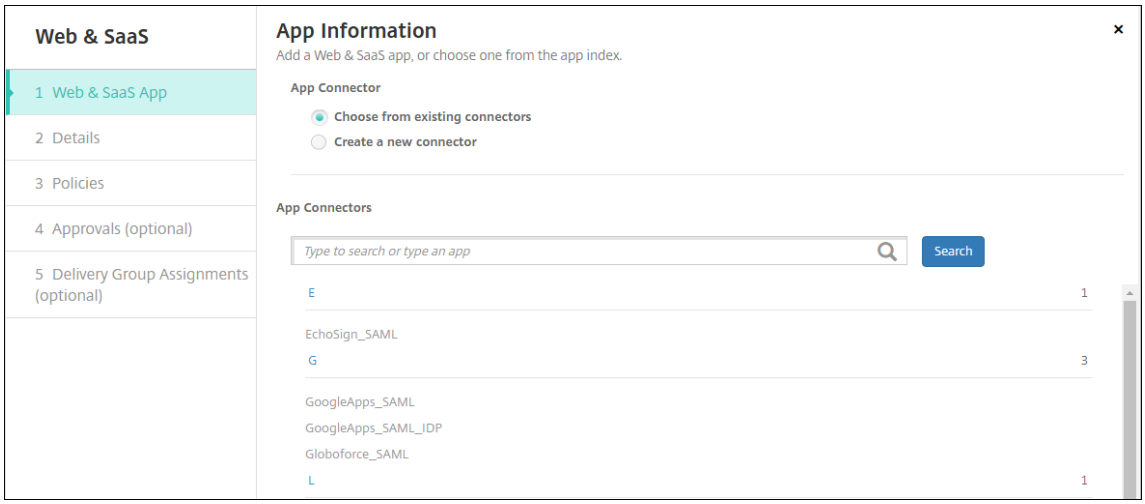
使用 XenMobile 控制台，可以向用户提供对移动应用程序、企业应用程序、Web 应用程序和 SaaS 应用程序的单点登录 (SSO) 授权。可以通过使用应用程序连接器模板，为应用程序启用 SSO。有关 XenMobile 中可用连接器类型的列表，请参阅应用程序连接器类型。还可以在添加 Web 或 SaaS 应用程序时在 XenMobile 中构建自己的连接器。

如果应用程序仅可进行 SSO：保存设置后，应用程序将显示在 XenMobile 控制台的应用程序选项卡中。

1. 在 XenMobile 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。



2. 单击 **Web** 和 **SaaS**。此时将显示应用程序信息页面。



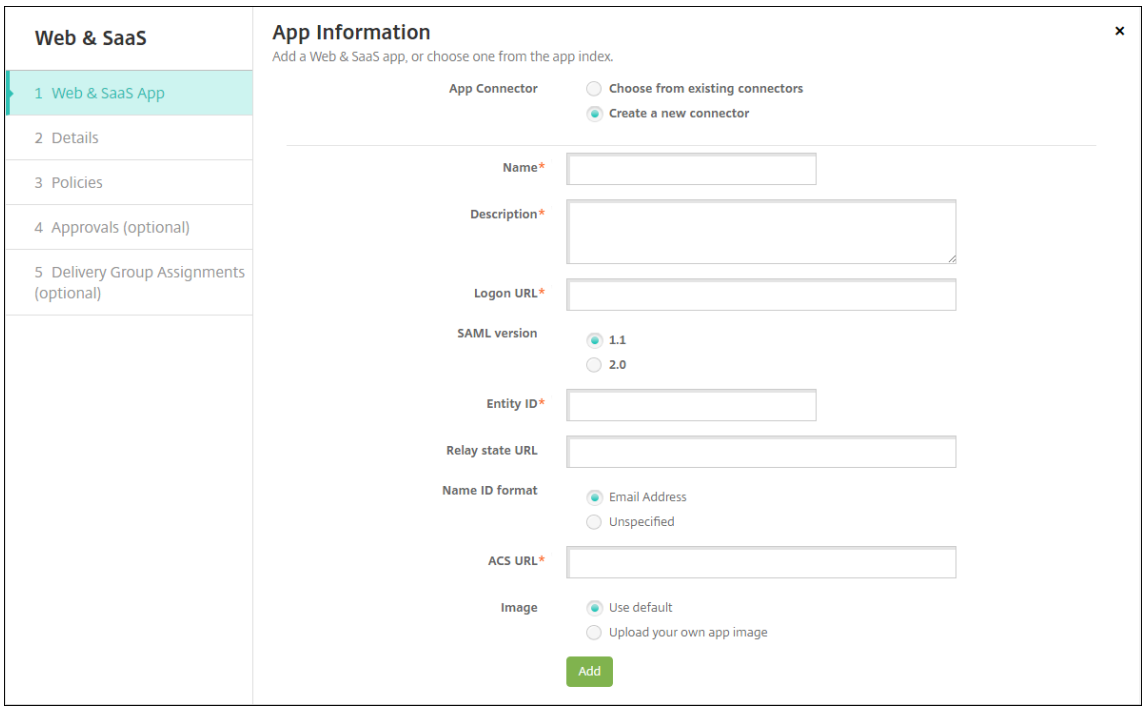
3. 配置现有或新的应用程序连接器，如下所示。

配置现有的应用程序连接器

1. 在应用程序信息页面中，从现有连接器中选择已选中，如上文所示。在应用程序连接器列表中单击要使用的连接器。此时将显示应用程序连接器信息。
2. 配置以下设置：
    - 应用程序名称：接受预先填充的名称或键入新名称。
    - 应用程序说明：接受预先填充的说明或键入自己的说明。
    - **URL**：接受预先填充的 URL 或键入应用程序的 Web 地址。根据您选择的连接器，此字段可能包含占位符，您必须替换占位符才能前进到下一个页面。
    - 域名：如果适用，键入应用程序的域名。此字段为必填字段。
    - 应用程序托管在内部网络中：选择应用程序是否在内部网络中的服务器上运行。如果用户从远程位置连接到内部应用程序，则必须通过 Citrix Gateway 进行连接。将此选项设置为开将向应用程序添加 VPN 关键字，并允许用户通过 Citrix Gateway 连接。默认值为关。
    - 应用程序类别：在此列表中，单击要应用于应用程序的可选类别。
    - 用户帐户预配：选择是否为应用程序创建用户帐户。如果使用 Globoforce_SAML 连接器，必须启用此选项以确保无缝 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。此字段为必填字段。
            - 密码：键入应用程序管理员密码。此字段为必填字段。
        - 用户帐户
            - 用户授权结束时：在列表中，单击不再允许用户访问应用程序时采取的操作。默认值为禁用帐户。
        - 用户名规则
            - 对于要添加的每项用户名规则，请执行以下操作：
                - 用户属性：在列表中，单击要添加到规则中的用户属性。
                - 长度 **(**字符数**)**：在列表中，单击要在用户名规则中使用的用户属性字符数。默认值为全部。
                - 规则：您添加的每个用户属性自动附加到用户名规则中。
    - 密码要求
        - 长度：键入用户密码最小长度。默认值为 **8**。
    - 密码过期时间
        - 有效期 **(**天**)**：键入密码有效的天数。有效值为 **0–90**。默认值为 90。
        - 过期后自动重置密码：选择是否在密码过期时自动重置密码。默认值为关。如果不启用此字段，用户在其密码过期后将无法打开应用程序。

配置新的应用程序连接器

1. 在应用程序信息页面中，选择创建新连接器。此时将显示应用程序连接器字段。

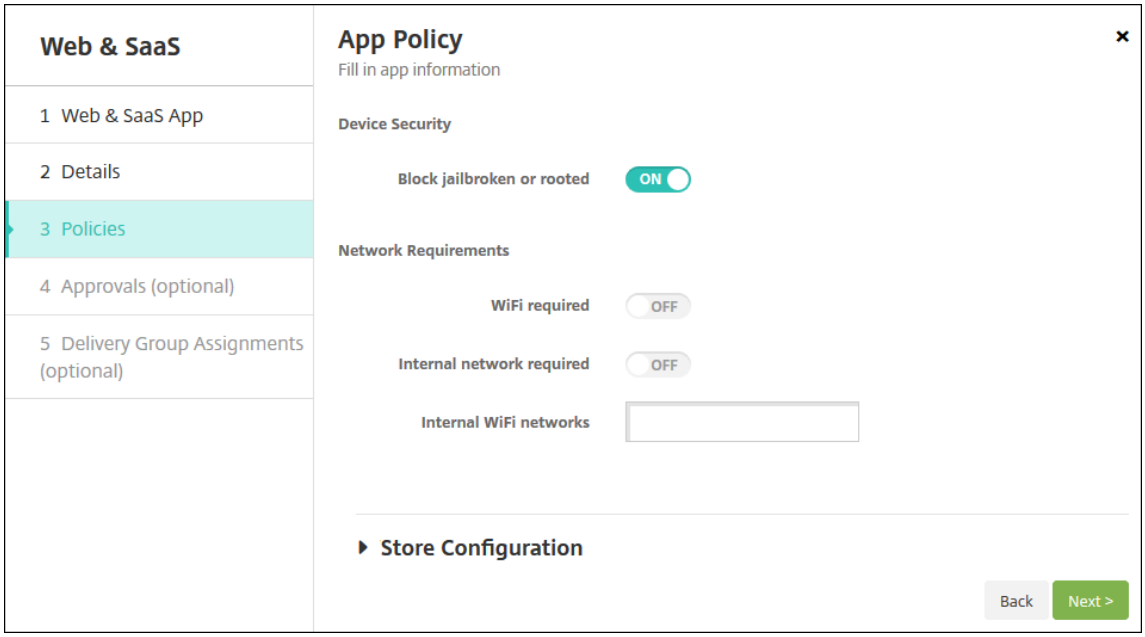


2. 配置以下设置：

   - 名称：键入连接器的名称。此字段为必填字段。
   - 说明：键入连接器的说明。此字段为必填字段。
   - 登录 **URL**：键入或复制并粘贴用户登录站点的 URL。例如，如果您要添加的应用程序有登录页面，请打开 Web 浏览器并访问该应用程序的登录页面。例如，它可能是 `https://www.example.com/logon`。此字段为必填字段。
   - **SAML** 版本：选择 **1.1** 或 **2.0**。默认值为 **1.1**。
   - 实体 **ID**：键入 SAML 应用程序的标识。
   - 中继状态 **URL**：键入 SAML 应用程序的 Web 地址。中继状态 URL 是来自应用程序的响应 URL。
   - 名称 **ID** 格式：选择电子邮件地址或未指定。默认值为电子邮件地址。
   - **ACS URL**：键入身份提供程序或服务提供商的声明使用者服务 URL。ACS URL 为用户提供 SSO 功能。
   - 图片：选择是使用默认 Citrix 图片还是上载您自己的应用程序图片。默认值为“使用默认值”。
     - 要上载自己的图片，请单击浏览并导航到文件所在位置。该文件必须是.PNG 文件。不能上载 JPEG 或 GIF 文件。如果添加自定义图形，以后将无法进行更改。

3. 完成后，单击添加。此时将显示详细信息页面。

4. 单击 **Next**（下一步）。此时将显示应用程序策略页面。

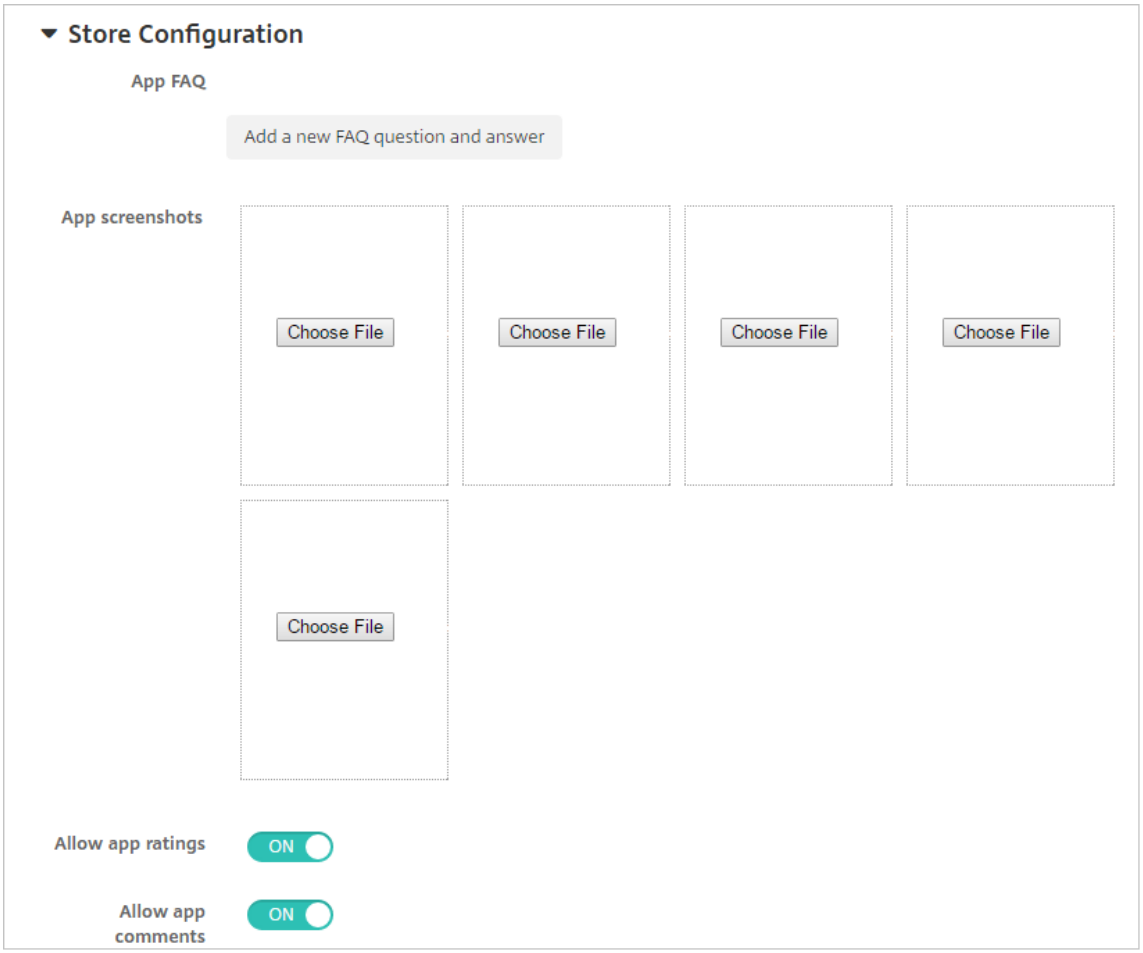


5. 配置以下设置：

   - 设备安全
   - 阻止越狱或获得 **Root** 权限：选择是否阻止已被越狱或获得 Root 权限的设备访问应用程序。默认值为开。
   - 网络要求
   - 需要连接 **WiFi**：选择运行应用程序是否需要使用 Wi-Fi 连接。默认值为关。
   - 需要连接内部网络：选择运行应用程序是否需要使用内部网络。默认值为关。
   - 内部 **WiFi** 网络：如果启用了需要连接 **Wi-Fi**，请键入要使用的内部 Wi-Fi 网络。

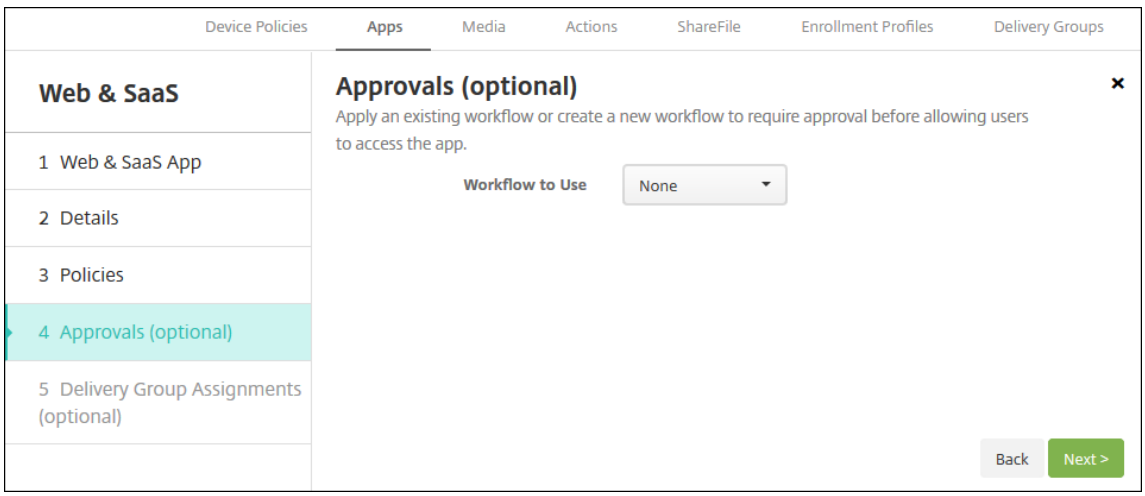
6. 配置部署规则。有关信息，请参阅部署规则。

7. 展开应用商店配置。



- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

8. 单击 **Next**（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。

9. 单击 **Next**（下一步）。此时将显示交付组分配页面。
10. 在选择交付组旁边，键入以查找交付组或者选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。
11. 展开部署计划，然后配置以下设置：

    - 部署：选择是否将应用程序部署到设备。默认值为开。
    - 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
    - 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

    如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则为始终启用的连接部署适用。

    配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

12. 单击保存。

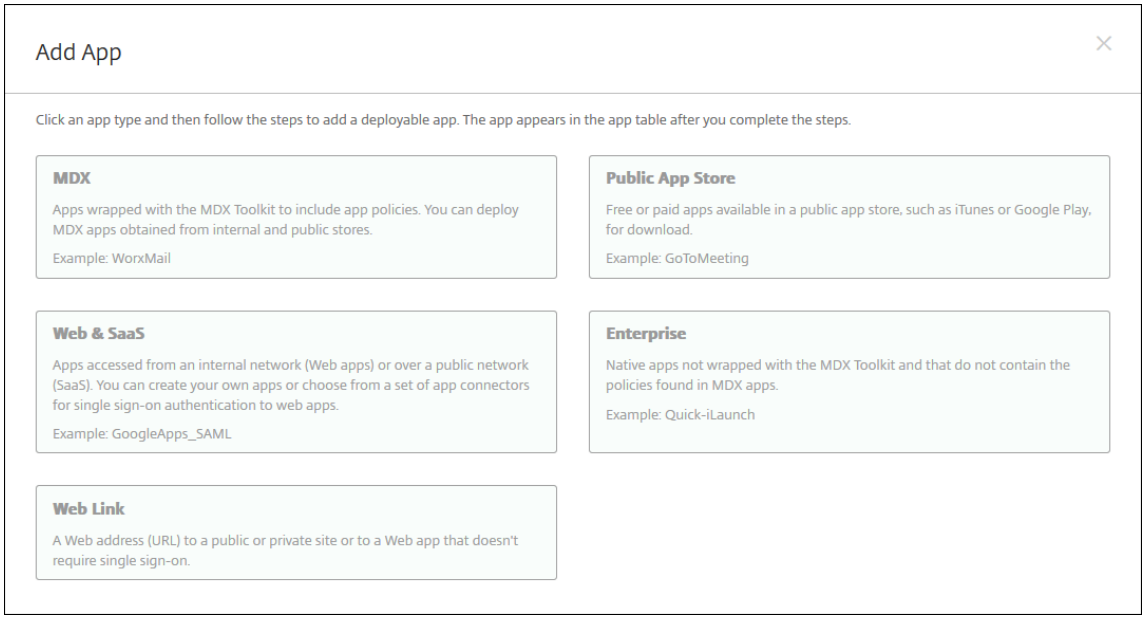
添加企业应用程序

XenMobile 中的企业应用程序表示未使用 MAM SDK 或 MDX Toolkit 准备的本机应用程序。这些应用程序不包含与 MDX 应用程序关联的策略。可以在 XenMobile 控制台中的应用程序选项卡中上载企业应用程序。企业应用程序支持以下平台（和相应的文件类型）：

- iOS（.ipa 文件）
- Android（.apk 文件）
- Samsung Knox（.apk 文件）
- Android Enterprise（.apk 文件）
- 另请参阅：启用了 MDX 的专用应用程序

在企业应用程序不受支持时，添加从 Google Play 应用商店下载的应用程序。将 Google Play 应用商店中的应用程序添加为公共应用商店应用程序。请参阅添加公共应用商店应用程序。

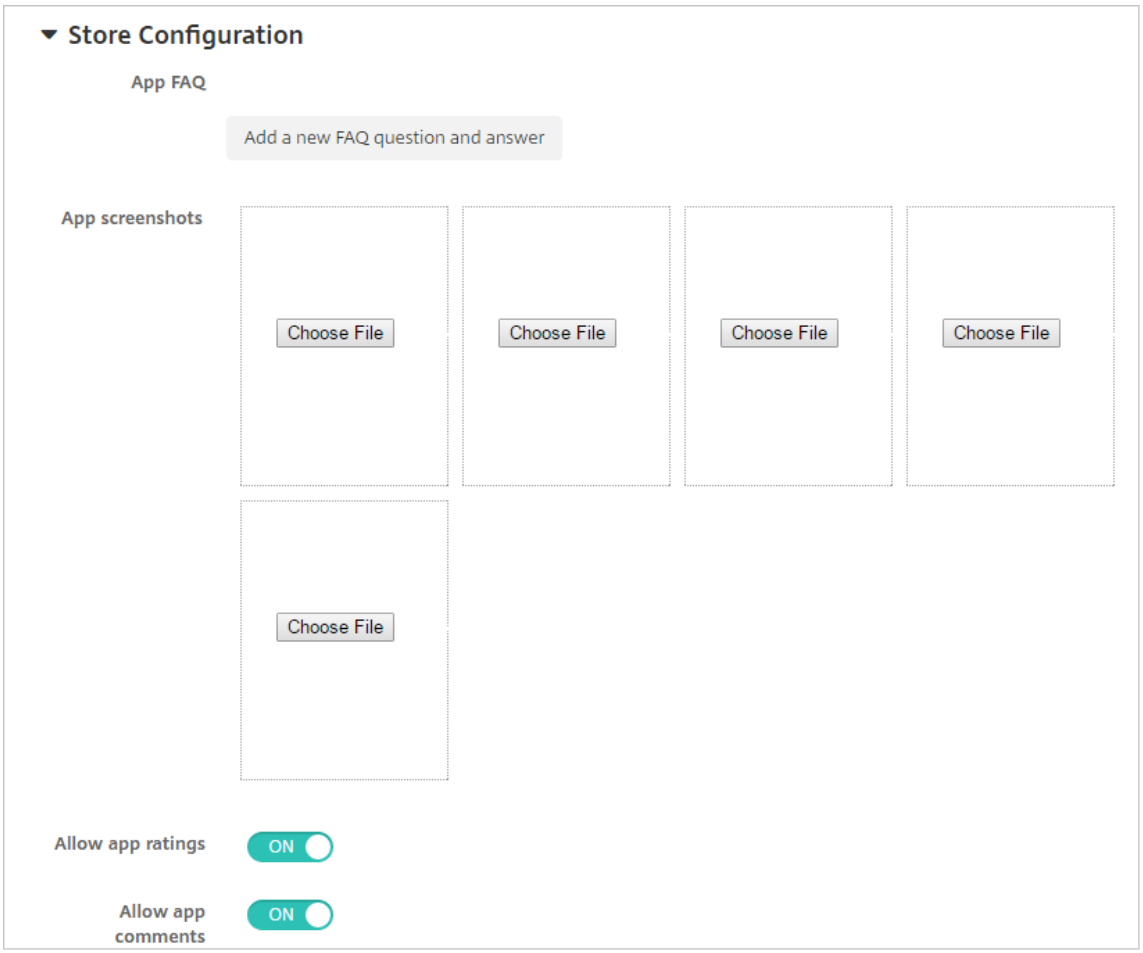
1. 在 XenMobile 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。



2. 单击企业。此时将显示应用程序信息页面。
3. 在应用程序信息窗格中，键入以下信息：
   - 名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   - 说明：键入应用程序的可选说明。
   - 应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 单击 **Next**（下一步）。此时将显示应用程序平台页面。
5. 在平台下，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。
6. 对于所选的每个平台，单击上载并导航到要上载的文件所在位置，选择此文件。
7. 单击 **Next**（下一步）。此时将显示平台的应用程序信息页面。
8. 为平台类型配置设置，例如：
   - 文件名：（可选）键入应用程序的新名称。
   - 应用程序说明：（可选）键入应用程序的新说明。
   - 应用程序版本：无法更改此字段。
   - 最低操作系统版本：（可选）键入为了使用应用程序，设备可以运行的最低操作系统版本。
   - 最高操作系统版本：（可选）键入为了使用应用程序，设备必须运行的最新操作系统版本。
   - 排除的设备：（可选）键入不能运行应用程序的设备的制造商或型号。
   - 软件包 **ID**：应用程序的唯一标识符。
   - 删除 **MDM** 配置文件时也删除应用程序：选择删除 MDM 配置文件时是否从设备中删除应用程序。默认值为开。
   - 阻止备份应用程序数据：选择是否阻止应用程序备份数据。默认值为开。

- 强制管理应用程序：安装非托管应用程序时，如果希望提示未受监督设备上的用户允许管理应用程序，请选择开。如果用户接受提示，将托管应用程序。

9. 配置部署规则。有关信息，请参阅部署规则。
10. 展开应用商店配置。



- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

11. 单击 **Next**（下一步）。此时将显示审批页面。

    要使用工作流在允许用户访问应用程序之前要求批准，请参阅应用工作流。如果您不需要审批工作流程，请继续执行下一步。

12. 单击 **Next**（下一步）。此时将显示交付组分配页面。
13. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。
14. 展开部署计划，然后配置以下设置：

- 部署：选择是否将应用程序部署到设备。默认值为开。
- 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
- 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则为始终启用的连接部署适用。

配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

15. 单击保存。

添加 **Web** 链接

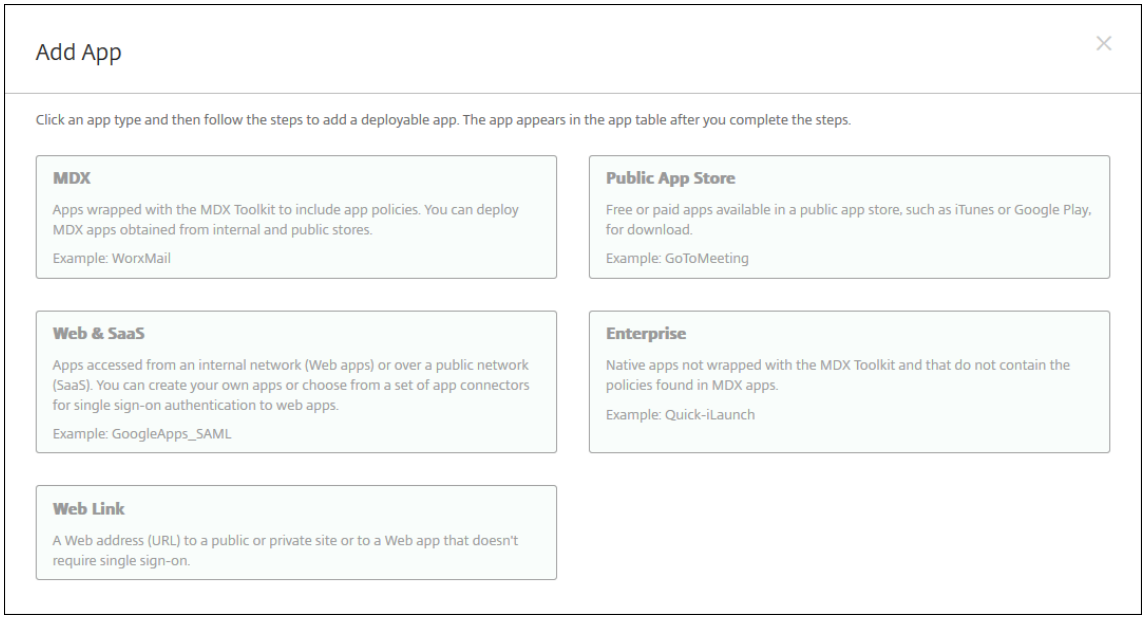
Web 链接是指向 Internet 或 Intranet 站点的 Web 地址。Web 链接还可以指向不需要 SSO 的 Web 应用程序。Web 链接配置完成后，链接将以图标的形式显示在应用商店中。当用户通过 Secure Hub 登录时，将显示该链接以及可用应用程序和桌面的列表。

可以从 XenMobile 控制台中的应用程序选项卡配置 Web 链接。配置完 Web 链接后，该链接将以链接图标的形式显示在应用程序表中的列表中。当用户通过 Secure Hub 登录时，将显示该链接以及可用应用程序和桌面的列表。

要添加链接，请提供以下信息：

- 链接的名称
- 链接的说明
- Web 地址 (URL)
- 类别
- 角色
- .png 格式的图片（可选）

1. 在 XenMobile 控制台中，单击配置 **>** 应用程序 **>** 添加。此时将显示添加应用程序对话框。

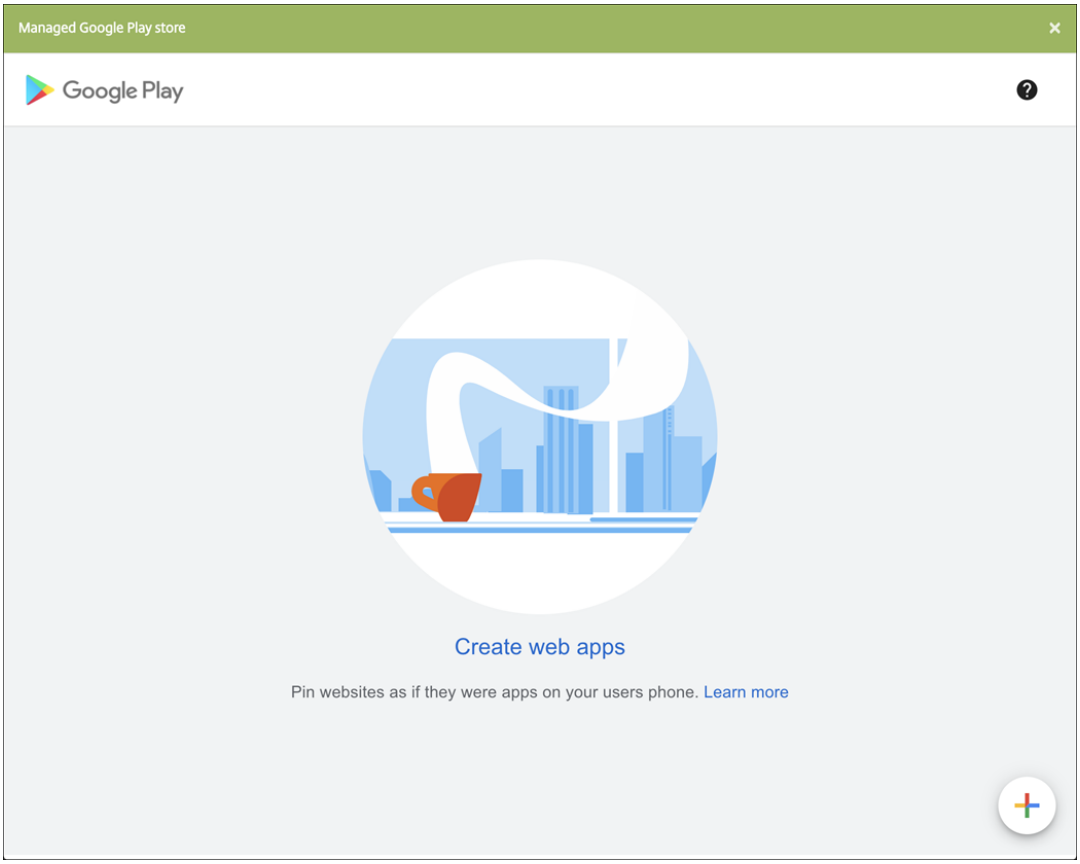


2. 单击 **Web** 链接。此时将显示应用程序信息页面。
3. 在应用程序信息窗格中，键入以下信息：

   名称：键入应用程序的描述性名称。此名称将显示在“应用程序”表中的“应用程序名称”下。
   说明：键入应用程序的可选说明。
   应用程序类别：（可选）在列表中单击要将应用程序添加到的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

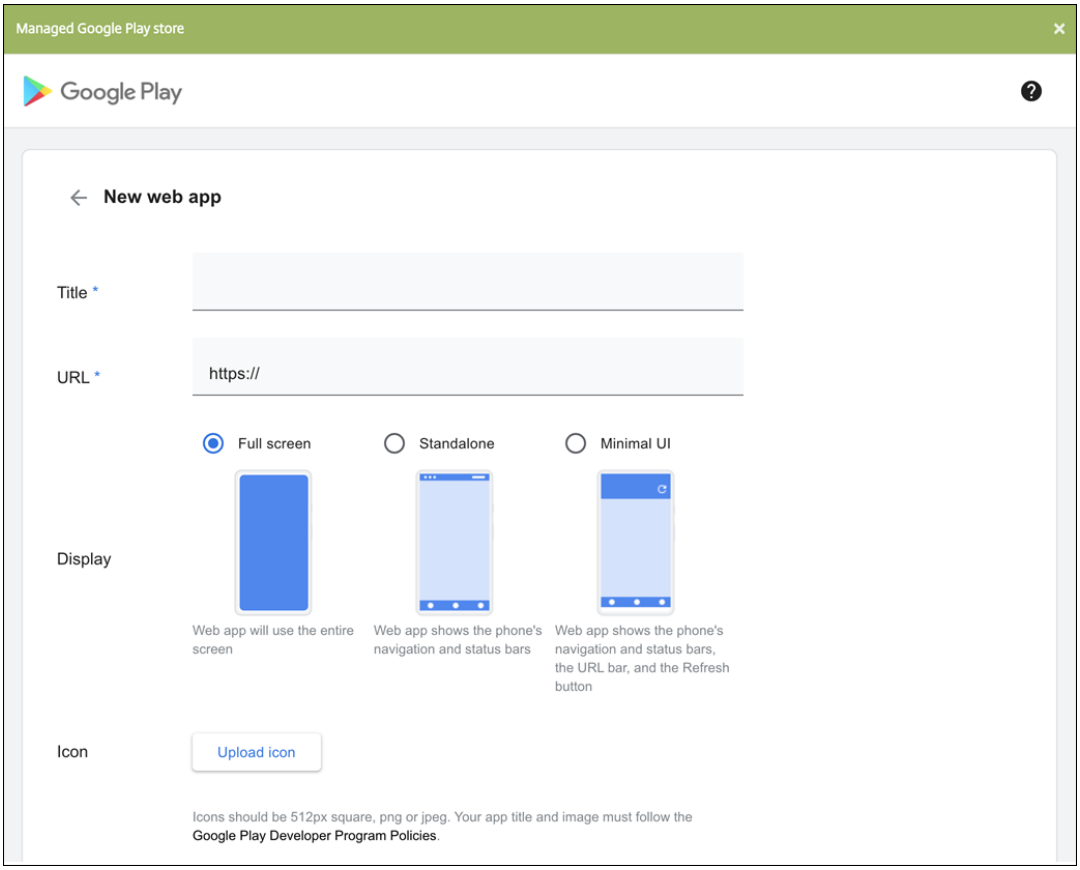
4. 单击 **Next**（下一步）。此时将显示应用程序平台页面。
5. 在平台下，选择其他平台以添加适用于 iOS 和 Android（旧版 DA）的 Web 应用程序，或者选择 **Android Enterprise**。清除不想添加的复选框。

   - 如果选择其他平台，请继续执行下一步以配置设置。
   - 如果选择 **Android Enterprise**，请单击上载按钮打开托管 Google Play 应用商店。您无需注册开发者帐户即可发布 Web 应用程序。单击右下角的加号图标以继续。



配置以下设置：

- 标题：键入 Web 应用程序的名称。
- **URL**：键入应用程序的 Web 地址。
- 显示：选择如何在用户设备上显示 Web 应用程序。可用选项包括全屏、独立和最小 **UI**。
- 图标：上载您自己的图片以表示 Web 应用程序。



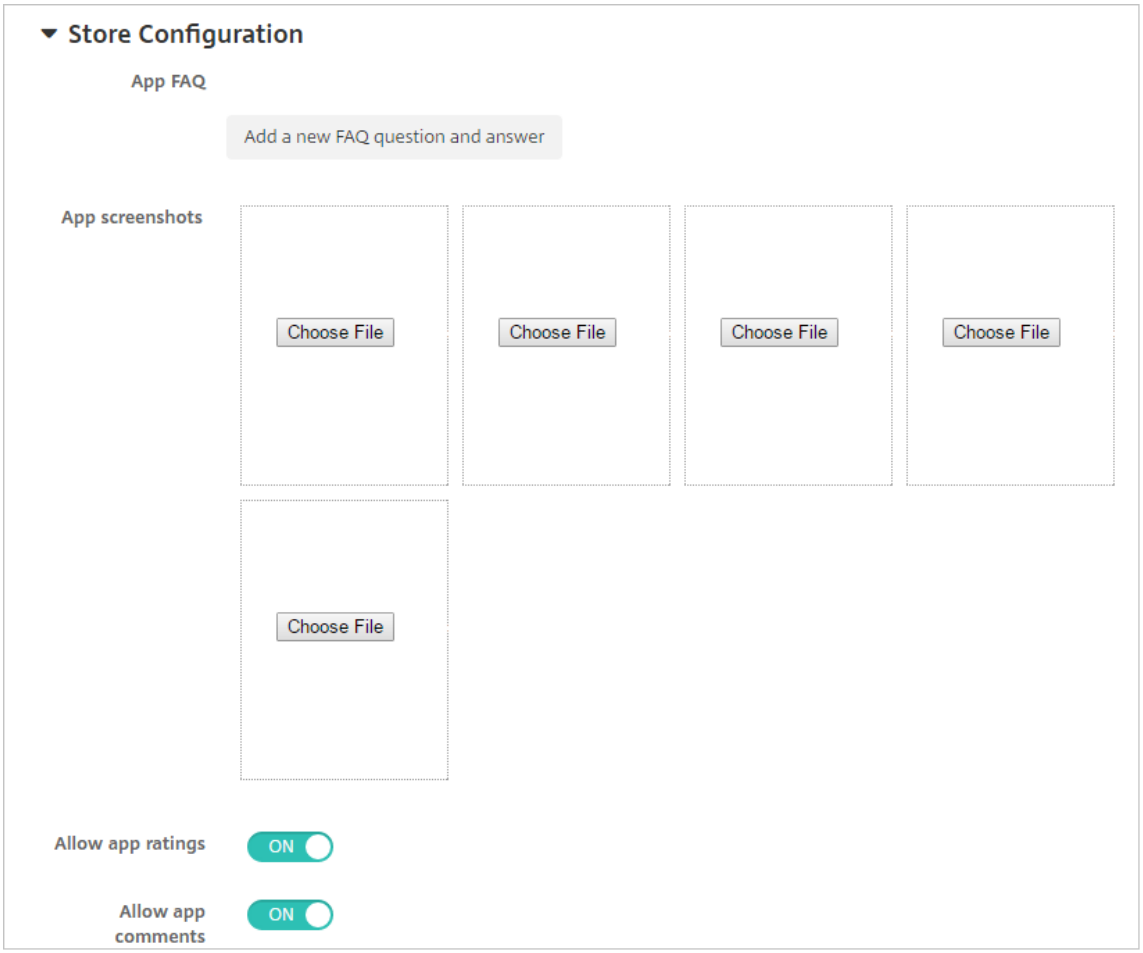
完成后，单击创建。您的 Web 应用程序最多可能需要 10 分钟才能发布。

6. 对于 Android Enterprise 以外的平台，请配置以下设置：

   - 应用程序名称：接受预先填充的名称或键入新名称。
   - 应用程序说明：接受预先填充的说明或键入自己的说明。
   - **URL**：接受预先填充的 URL 或键入应用程序的 Web 地址。根据您选择的连接器，此字段可能包含占位符，您必须替换占位符才能前进到下一个页面。
   - 应用程序托管在内部网络中：选择应用程序是否在内部网络中的服务器上运行。如果用户从远程位置连接到内部应用程序，则必须通过 Citrix Gateway 进行连接。将此选项设置为开将向应用程序添加 VPN 关键字，并允许用户通过 Citrix Gateway 连接。默认值为关。
   - 应用程序类别：在此列表中，单击要应用于应用程序的可选类别。
   - 图片：选择是使用默认 Citrix 图片还是上载您自己的应用程序图片。默认值为 “使用默认值”。
     - 要上载自己的图片，请单击浏览并导航到文件所在位置。该文件必须是.PNG 文件。不能上载 JPEG 或 GIF 文件。如果添加自定义图形，以后将无法进行更改。

7. 配置部署规则。有关信息，请参阅部署规则。

8. 展开应用商店配置。



- 应用程序常见问题解答：单击添加新的常见问题和答案，为应用程序创建常见问题解答。
- 添加手机/平板电脑的屏幕截图：添加应用商店中显示的屏幕截图。
- 允许对应用程序评分：允许用户对应用商店中的应用程序评分。
- 允许评价应用程序：允许用户对应用商店中的应用程序发表评论。

9. 单击 **Next**（下一步）。此时将显示交付组分配页面。
10. 在选择交付组旁边，键入以查找交付组或者在列表中选择一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。
11. 展开部署计划，然后配置以下设置：

    - 部署：选择是否将应用程序部署到设备。默认值为开。
    - 部署计划：选择立即还是以后部署应用程序。如果选择以后，请配置部署应用程序的日期和时间。默认值为立即。
    - 部署条件：选择每次连接时以在设备每次连接时部署应用程序。选择仅当之前的部署失败时以在设备之前未能接收应用程序时部署应用程序。默认值为每次连接时。

    如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则为始终启用的连接部署适用。

    配置的部署计划对所有平台相同。您所做的更改适用于所有平台，但为始终启用的连接部署除外。

12. 单击保存。

启用 **Microsoft 365** 应用程序

可以打开 MDX 容器以允许 Secure Mail、Secure Web 和 Citrix Files 向 Microsoft Office 365 应用程序传输文档和数据。有关详细信息，请参阅允许与 Office 365 应用程序安全交互。

应用工作流

要指定或创建工作流，请配置以下设置：

- 要使用的工作流：在此列表中，单击现有工作流或单击创建新工作流。默认设置为无。

  如果选择创建新工作流，请配置以下设置。

  - 名称：键入工作流的唯一名称。
  - 说明：（可选）键入工作流的说明。
  - 电子邮件审批模板：在列表中，选择要指定的电子邮件审批模板。单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
  - 经理审批级别：在列表中，选择此工作流所需的经理审批级别数。默认值为 1 级。可能的选项包括：
    * 不需要
    * 1 级
    * 2 级
    * 3 级
  - 选择 **Active Directory** 域：在列表中，选择用于工作流的合适 Active Directory 域。
  - 查找所需的其他审批者：在搜索字段中键入其他所需人员的姓名，然后单击搜索。源于 Active Directory 的姓名。
  - 姓名显示在此字段中后，选中姓名旁边的复选框。姓名和电子邮件地址显示在选定的其他所需审批者列表中。

    要从选定的其他所需审批者列表中删除人员，请执行以下操作之一：

    * 单击搜索以查找选定域中的所有人员列表。
    * 在搜索框中键入完整姓名或部分姓名，然后单击搜索以限制搜索结果。
    * 在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。滚动列表，并取消选中要删除的各个姓名旁边的复选框。

应用商店和 **Citrix Secure Hub** 外观方案

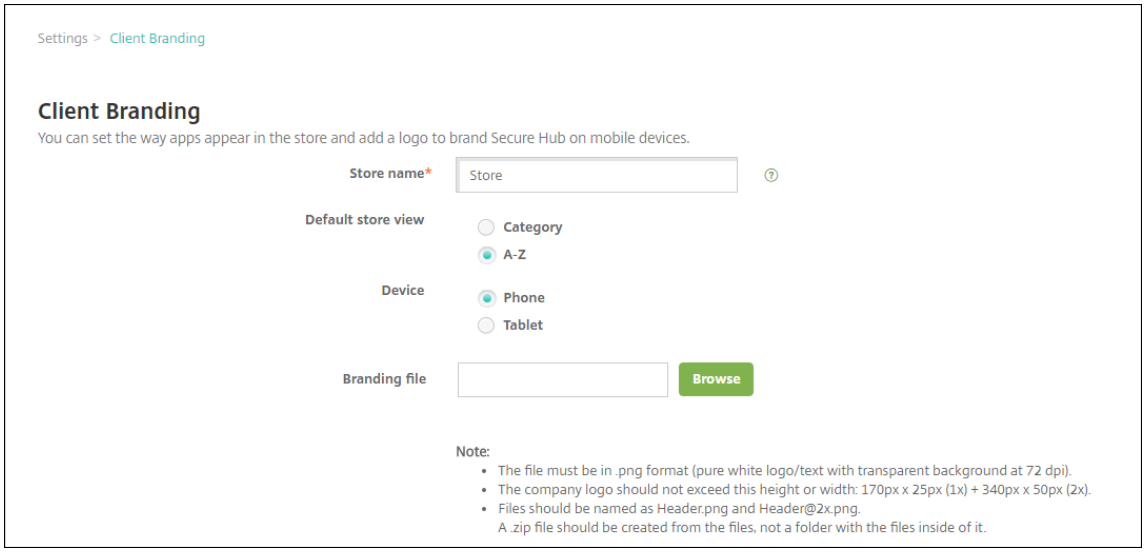
可以设置应用程序在应用商店中的显示方式，并添加用于标记 Secure Hub 和应用商店的徽标。这些标记功能适用于 iOS 和 Android 设备。

开始之前，请确保您的自定义图片已准备就绪并且可供访问。

自定义图片必须满足以下要求：

- 文件必须采用.png 格式
- 使用纯白徽标或文本以及 72 dpi 的透明背景。
- 公司徽标不得超过此高度或宽度：170 px x 25 px (1x) 和 340 px x 50 px (2x)。
- 将文件命名为 Header.png 和 Header@2x.png。
- 从文件而不是文件所在的文件夹创建.zip 文件。

1. 在 XenMobile Server 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在客户端下方，单击客户端外观方案。此时将显示客户端外观方案页面。



配置以下设置：

- 应用商店名称：应用商店名称显示在用户的帐户信息中。更改此名称也会更改用于访问应用商店服务的 URL。通常无需更改默认名称。

  > 重要：
  >
  > 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：选择电话或平板电脑。默认值为电话。
- 外观方案文件：单击浏览并导航到要用于外观方案的图片或图片的.zip 文件所在位置，选择该图片或文件。

3. 单击保存。

应用程序连接器类型

June 28, 2019

下表列出了添加 Web 或 SaaS 应用程序时 XenMobile 中可用的连接器及连接器类型。还可以在添加 Web 或 SaaS 应用程序时向 XenMobile 添加新连接器。

表中指出连接器是否支持用户帐户管理。支持用户帐户管理时，您可以自动或通过工作流创建新帐户。

连接器名称	SSO SAML	支持用户帐户管理
EchoSign_SAML	Y	Y
Globoforce_SAML		注意：使用此连接器时，必须启用用户管理功能以进行预配以确保无缝 SSO 集成。
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y
Office365_SAML	Y	Y
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML	Y	
ShareFile_SAML_SP	Y	
WebEx_SAML_SP	Y	Y

升级 **MDX** 或企业应用程序

January 5, 2022

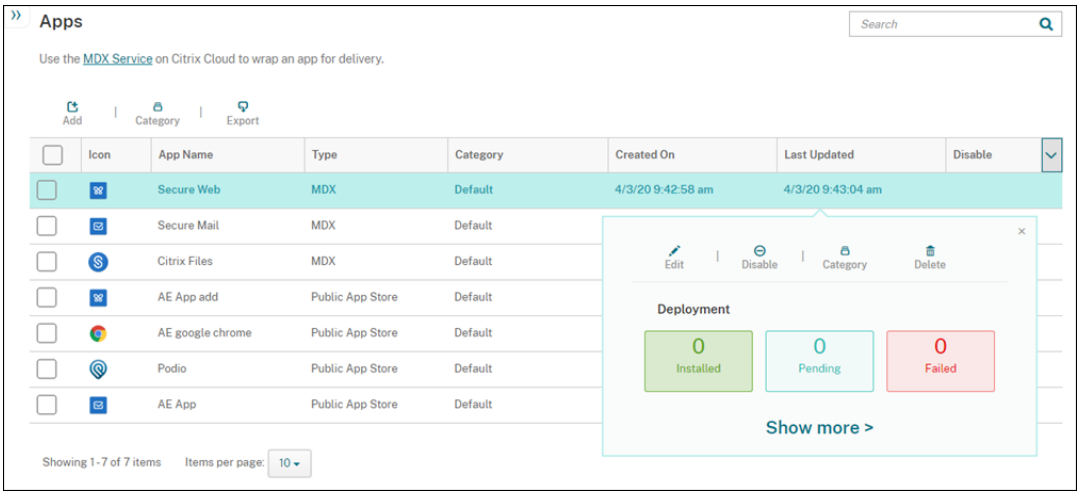
要在 XenMobile 中升级 MDX 或企业应用程序，请在 XenMobile 控制台中禁用该应用程序，然后上载该应用程序的新版本。您无需禁用公共应用商店应用程序，例如 Citrix Secure Mail。

1. 在 XenMobile 控制台中，单击配置 **>** 应用程序。此时将显示应用程序页面。
2. 对于托管设备（在 XenMobile 中注册用于移动设备管理的设备），跳至步骤 3。对于未托管设备（在 XenMobile

中注册仅用于企业版应用程序管理目的的设备），请执行以下操作：

a) 在应用程序表中，选中应用程序旁边的复选框或单击包含要更新的应用程序的行。

b) 在显示的菜单中单击禁用。



c) 在确认对话框中单击禁用。已禁用显示在应用程序的禁用列中。

> 注意：
>
> 禁用应用程序期间，用户无法在注销后重新连接到此应用程序。禁用应用程序是可选的，但我们建议禁用应用程序以避免应用程序功能出现问题。例如，用户在上载新版本的同时请求下载应用程序可能会导致出现问题。

3. 在应用程序表中，单击应用程序旁边的复选框或单击包含要更新的应用程序的行。
4. 在显示的菜单中单击编辑。此时将显示应用程序信息页面，您最初为应用程序选择的平台处于选中状态。
5. 配置以下设置：
   - 名称：（可选）更改应用程序名称。
   - 说明：（可选）更改应用程序说明。
   - 应用程序类别：（可选）更改应用程序类别。
6. 单击 **Next**（下一步）。此时将显示首先选择的平台页面。请为选择的每个平台执行以下操作：

   a) 单击上载并导航到要上载的替换文件所在位置，选择该文件。应用程序即上载到 XenMobile。

   如果您要上载适用于 Android Enterprise 的应用程序，则会出现一个托管 Google Play 窗口。请在此处上载新版本的应用程序。有关更多详细信息，请参阅分发 Android Enterprise 应用程序。

   b) 可选，更改平台的应用程序详细信息和策略设置。

c)（可选）配置部署规则和 XenMobile Store 配置。有关信息，请参阅添加应用程序中的“添加 MDX 应用程序”。

7. 单击保存。此时将显示应用程序页面。
8. 如果在步骤 2 中禁用了该应用程序，请执行以下操作：
   a) 在应用程序表中，通过单击选择已更新的应用程序，然后在显示的菜单中单击启用。
   b) 在显示的确认对话框中，单击启用。用户现在可以访问该应用程序并接收提示用户升级应用程序的通知。

Citrix Launcher

January 5, 2022

Citrix Launcher 替代产品

Citrix 将于 2020 年 8 月从应用商店中删除 Citrix Launcher。要替换 Citrix Launcher，可以使用已提供的功能。

要将设备预配为网亭（专用设备），请执行以下操作：

1. 添加允许 XenMobile 管理员在您的 XenMobile 部署中注册专用设备的 RBAC 角色。请参阅预配专用 Android Enterprise 设备。
2. 创建注册类型为完全托管/工作配置文件的注册配置文件。请参阅创建注册配置文件。
3. 通过启用锁定任务模式设置创建 Kiosk 设备策略，以将应用程序配置为固定到设备屏幕。请参阅 Android Enterprise 设置。

关于 Citrix Launcher

使用 Citrix Launcher 可以自定义由 XenMobile 部署的 Android 设备的用户体验。Citrix Launcher 的 Secure Hub 管理支持的最低 Android 版本为 Android 4.0.3。Citrix Launcher 和 Launcher 配置设备策略与 Android Enterprise 不兼容。

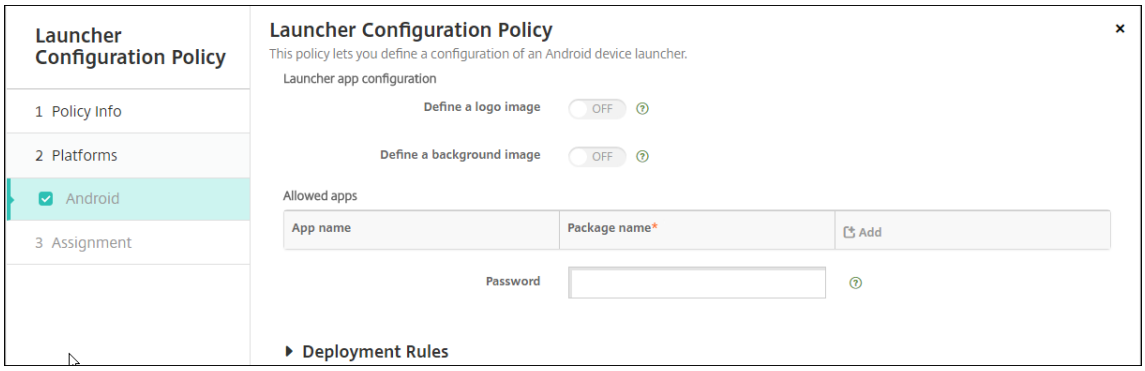
您可以添加 **Launcher** 配置策略来控制以下 Citrix Launcher 功能：

- 管理 Android 设备，确保用户只能访问指定的应用程序。
- （可选）为 Citrix Launcher 图标指定自定义徽标图片以及为 Citrix Launcher 指定自定义背景图片。
- 指定用户在退出启动程序前必须输入的密码。

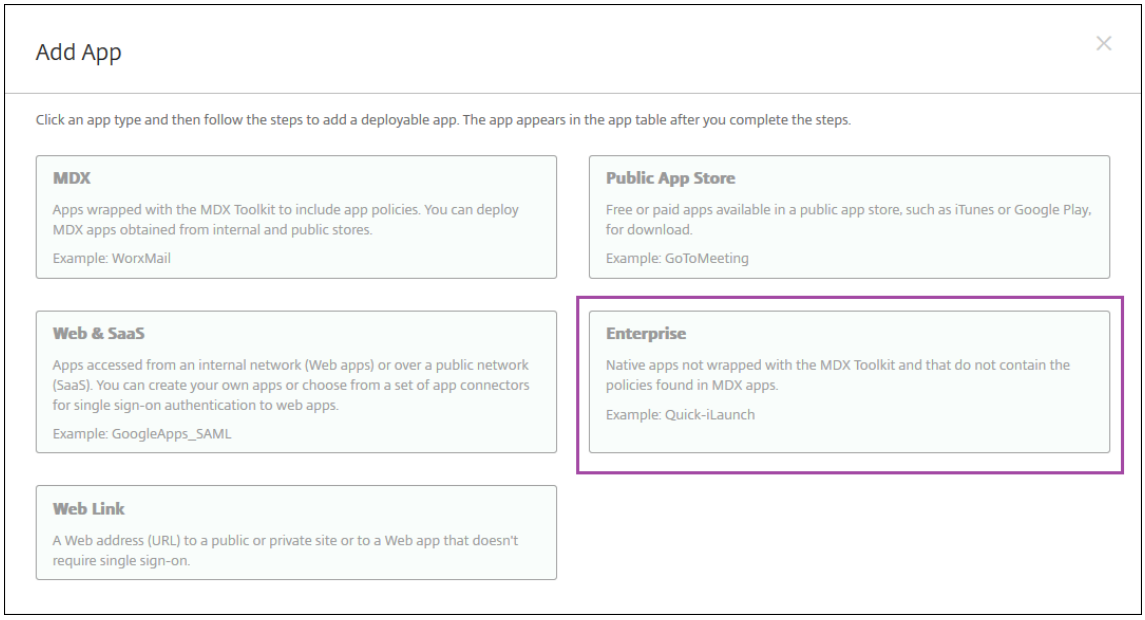
尽管使用 Citrix Launcher 可以应用这些设备级别限制，但 Launcher 也授予用户对 Wi-Fi 设置、蓝牙设置和设备通行码设置等设备设置的内置访问权限。Citrix Launcher 并不是设备平台在已提供的安全层之外额外提供的一个安全层。

要为 Android 设备提供 Citrix Launcher，请执行以下常规步骤。

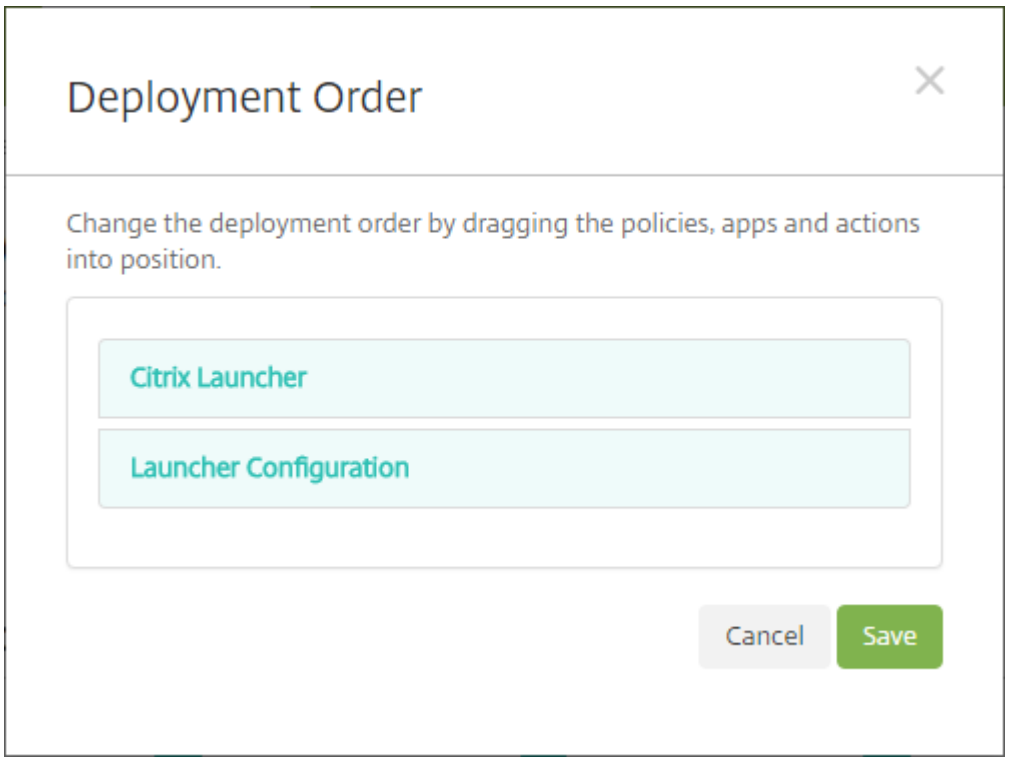
1. 要下载 Citrix Launcher 应用程序，请转到 https://www.citrix.com/downloads。搜索 **Citrix Launcher**。该应用程序的文件名为 CitrixLauncher.apk。该文件可以随时上载到 XenMobile 中，并且不需要打包。
2. 添加设备策略 **Launcher** 配置策略。转至配置 **>** 设备策略，单击添加，然后在添加新策略对话框中，开始键入 **Launcher**。有关详细信息，请参阅 Launcher 配置策略。



3. 将 Citrix Launcher 应用程序作为企业应用程序添加到 XenMobile。在配置 **>** 应用程序中，单击添加，然后单击企业。有关详细信息，请参阅添加企业应用程序。



4. 为 Citrix Launcher 创建交付组，并在配置 **>** 交付组中进行以下配置：
   - 在策略页面上，添加 **Launcher** 配置策略。
   - 在应用程序页面上，将 **Citrix Launcher** 拖动到必需应用程序。
   - 在摘要页面上，单击部署顺序并确保 **Citrix Launcher** 应用程序位于 **Launcher** 配置策略之前。



有关详细信息，请参阅部署资源。

Apple 批量购买

January 5, 2022

可以使用 Apple iOS 批量购买管理 iOS 应用程序许可。批量购买解决方案简化了组织批量查找、购买和分发应用程序及其他数据的过程。

通过批量购买，您可以使用 XenMobile 来分发公共应用商店应用程序。

- MAM 注册不支持批量购买。必须在 MDM 或 MDM+MAM 中注册批量购买设备。
- Citrix 移动生产力应用程序不支持批量购买。
- 虽然您可以通过批量购买分发 XenMobile 公共应用商店应用程序，但该部署不是最佳的。要解决这些限制，需要增强 XenMobile 和 Secure Hub 应用商店的功能。
- 有关通过批量购买分发 XenMobile 公共应用商店应用程序的已知问题的列表，请参阅 Citrix 知识中心中的这篇文章。

通过批量购买，您可以将适用的应用程序直接分发到您的设备。或者，通过使用可兑换代码将内容分配给用户。可以在 XenMobile 中配置 iOS 批量购买特定的设置。

XenMobile 定期重新导入 Apple 提供的批量购买许可证以确保许可证反映所有更改。此类更改包括您何时从批量购买手动删除导入的应用程序。默认情况下，XenMobile 按每 1440 分钟（24 小时）的最小时间间隔为基准刷新批量购买许可证。可以通过服务器属性 `VPP.baseline` 更改批量购买基准时间间隔。请参阅服务器属性。

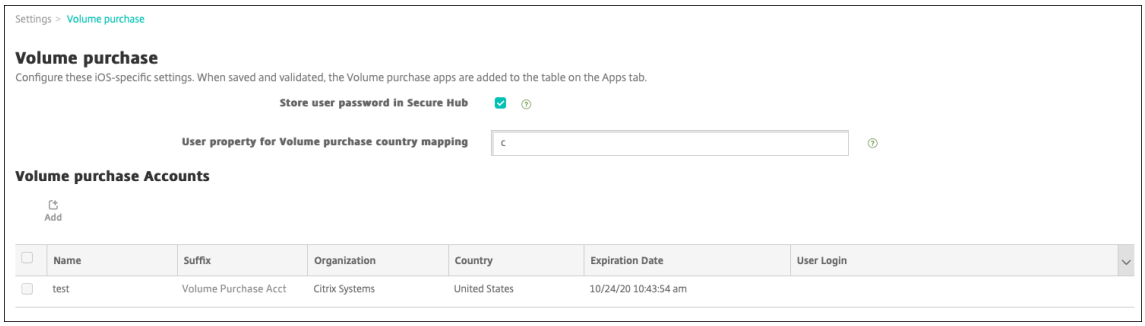
应用程序自动更新设置也依赖 `VPP.baseline` 服务器属性，并且应用程序将按照在该属性中设置的相同计划进行更新。

本文重点介绍通过托管许可证使用批量购买，这样您即可使用 XenMobile 分发应用程序。如果您当前使用兑换代码，并且希望更改为管理式分发，请参阅此 Apple 支持文档：在批量购买中从兑换代码迁移到管理式分发。

有关 iOS 批量购买的信息，请参阅https://volume.itunes.apple.com/us/store。要注册参加批量购买，请转到 https://deploy.apple.com/qforms/open/register/index/avs。要在 iTunes 中访问您的批量购买应用商店，请访问 https://volume.itunes.apple.com/?l=en。

在 XenMobile 中保存这些 iOS 批量购买设置后，购买的应用程序会显示在 XenMobile 控制台中的配置 **>** 应用程序页面上。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击批量购买。此时将显示批量购买配置页面。



3. 配置以下设置：

   - 在 **Secure Hub** 中存储用户密码：选择是否将用户名和密码存储在 Secure Hub 中以用于 XenMobile 身份验证。默认为使用此安全方法存储信息。
   - 批量购买国家/地区映射的用户属性：键入代码以允许用户从国家/地区特定的应用商店下载应用程序。

   XenMobile 使用此映射来选择批量购买的属性池。例如，如果用户属性是美国，若批量购买代码适用于英国，该用户将无法下载应用程序。请联系您的批量购买计划管理员，以了解关于国家/地区映射代码的更多信息。

4. 对于要添加的每个批量购买帐户，请单击添加。此时将显示添加批量购买帐户对话框。
5. 为要添加的每个帐户配置以下设置：

   > 注意：
   >
   > 如果使用 Apple Configurator 1，请上载许可证文件：转至配置 **>** 应用程序，转至平台页面，然后展开批量购买。

   - 名称：键入批量购买帐户名称。
   - 后缀：键入与通过批量购买帐户获取的应用程序名称一起显示的后缀。例如，如果输入 **VP**，Secure Mail 应用程序将在应用程序列表中显示为 **Secure Mail - VP**。
   - 公司令牌：复制并粘贴从 Apple 获取的批量购买服务令牌。要获取令牌，请在 Apple 批量购买门户的 **Account Summary**（帐户摘要）页面中，单击 **Download**（下载）按钮以生成并下载批量购买文件。此文件包含服务令牌和其他信息，如国家/地区代码和过期日期。将此文件保存在安全的位置。

- 用户登录：键入用于导入自定义 B2B 应用程序的可选授权批量购买帐户管理员名称。
- 用户密码：键入批量购买帐户管理员密码。
- 应用程序自动更新：如果设置为开，则当 Apple 应用商店中存在更新时，批量购买应用程序将自动更新。默认值为关。

6. 单击保存以关闭对话框。
7. 单击保存以保存批量购买配置。

   此时将显示一条消息，指出 XenMobile 将应用程序添加到配置 **>** 应用程序页面上的列表中。在该页面上，注意您的批量购买帐户中的应用程序名称包括您在前面的配置中提供的后缀。

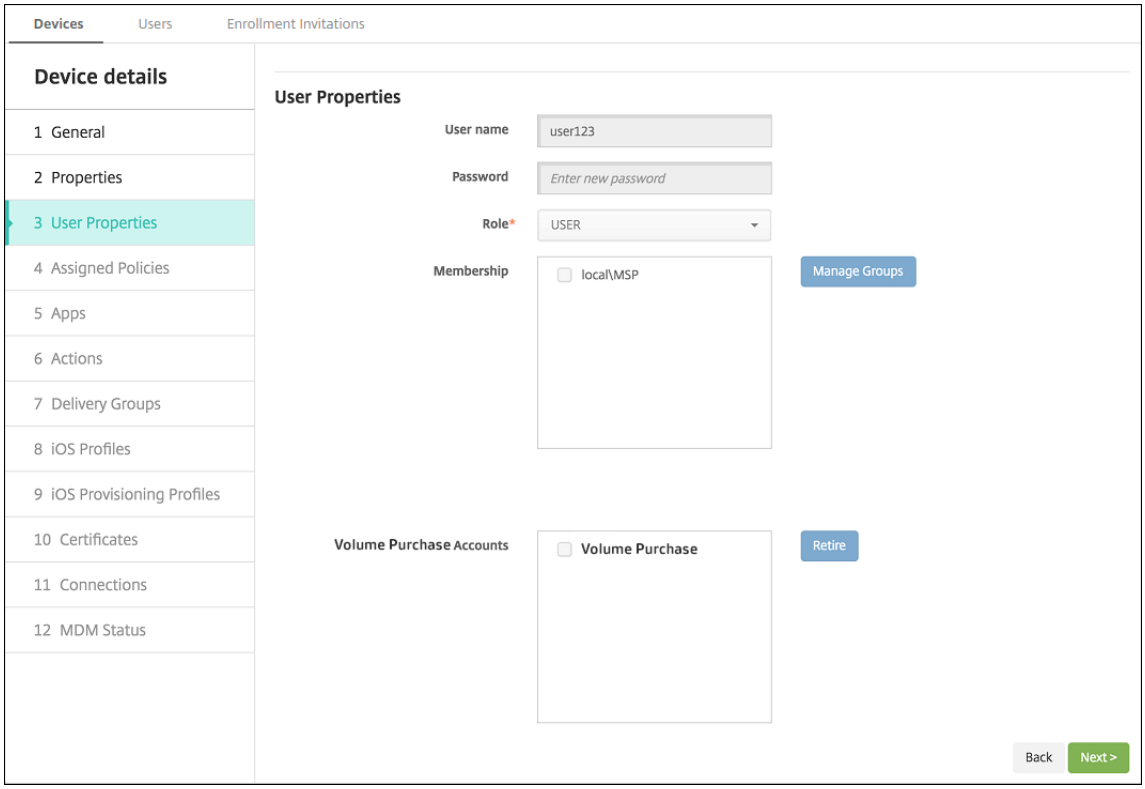
您现在可以配置批量购买应用程序设置，然后优化批量购买应用程序的交付组和设备策略设置。完成这些配置后，用户可以注册其设备。下面的备注提供了这些过程的注意事项。

- 配置批量购买应用程序设置（配置 **>** 应用程序）时，请启用强制与设备建立许可证关联。在受监督设备上使用 Apple 批量购买和部署的一项优势：能够使用 XenMobile 在设备（而非用户）级别分配应用程序。因此，您不必使用 Apple ID 设备。此外，用户不会收到加入 Apple 批量购买的邀请。用户还可以无需登录到其 iTunes 帐户即可下载应用程序。

  要查看该应用程序的批量购买信息，请展开批量购买。请注意，在批量购买许可证密钥表中，许可证与设备相关联。如果用户删除令牌，然后重新导入令牌，由于 Apple 隐私限制，单词隐藏将替代序列号显示。

  要取消关联许可证，请单击许可证对应的行，然后单击取消关联。

  如果将批量购买许可证与用户相关联，XenMobile 会将用户集成到批量购买帐户中，并将其 iTunes ID 与批量购买帐户相关联。用户的 iTunes ID 永远不会对贵公司或 XenMobile Server 可见。Apple 以透明方式创建关联以保留用户隐私。您可以从 Apple 批量购买中停用某个用户，以取消所有许可证与用户帐户的关联。要停用用户，请转至管理 **>** 设备。



- 将某个应用程序分配到交付组时，默认情况下，XenMobile 会将该应用程序标识为可选应用程序。要确保 XenMobile 将某个应用程序部署到设备，请转至配置 **>** 交付组。在应用程序页面上，将该应用程序移到必需应用程序列表。
- 公共应用商店应用程序的更新可用时：批量购买推送该应用程序时，该应用程序将自动在设备上更新。要推送 Secure Hub 的更新（已分配到设备而不是用户时），请执行以下操作。在某个平台页面上的配置 **>** 应用程序中，单击检查更新并应用更新。

  当 Apple 批量购买过期时，XenMobile 会显示许可证到期警告。

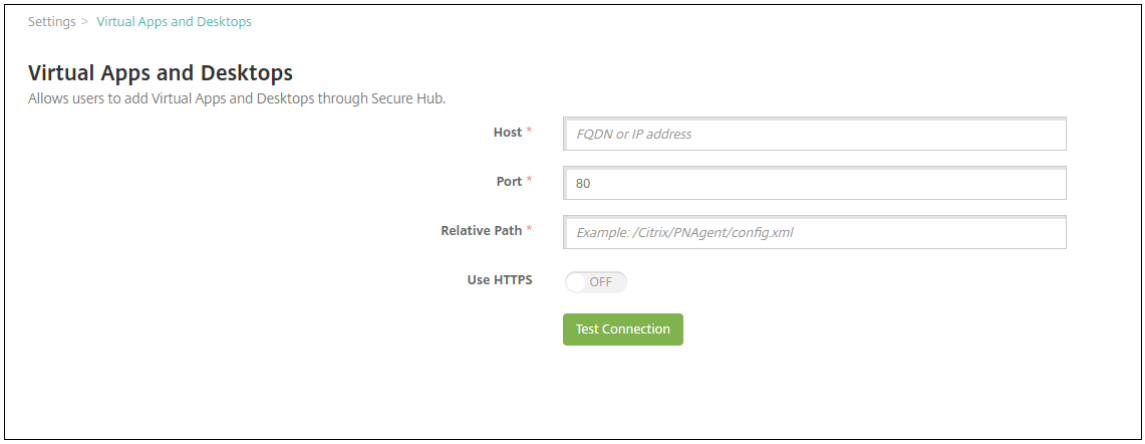
通过 **Citrix Secure Hub** 的 **Virtual Apps and Desktops**

November 12, 2020

XenMobile 可以从 Virtual Apps and Desktops 收集应用程序，使移动设备用户可在 XenMobile Store 中对其进行访问。用户可直接在 XenMobile Store 中订购应用程序，并从 Secure Hub 启动这些应用程序。用户设备上必须安装 Citrix Receiver 才能启动应用程序，但是并不需要对其进行配置。

要配置此设置，需要 Web Interface 站点或 StoreFront 的完全限定域名 (FQDN) 或 IP 地址和端口号。

1. 在 XenMobile Web 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击 **Virtual Apps and Desktops**。此时将显示 **Virtual Apps and Desktops** 页面。



3. 配置以下设置：
   - 主机：键入 Web Interface 站点或 StoreFront 的完全限定域名 (FQDN) 或 IP 地址。
   - 端口：键入 Web Interface 站点或 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 Web Interface 站点或 StoreFront 和客户端设备之间启用安全身份验证。默认值为关。
4. 单击测试连接以确认 XenMobile 是否能够连接到指定的 Virtual Apps and Desktops 服务器。
5. 单击保存。

将 Citrix Content Collaboration 与 XenMobile 结合使用

January 5, 2022

XenMobile 有两个用于与 Citrix Content Collaboration 集成的选项：Citrix Files 和存储区域连接器。与 Citrix Files 或存储区域连接器集成要求使用 XenMobile Enterprise Edition。

Citrix Files

如果您有 XenMobile Enterprise Edition，可以配置 XenMobile 以提供对 Citrix Files 帐户的访问权限。该配置：

- 为移动用户提供对完整 Enterprise 功能集（例如，文件共享、文件同步和存储区域连接器）的访问权限。
- 可以为 Citrix Files 提供 XenMobile Apps 用户的单点登录身份验证以及全面的访问控制策略。
- 通过 XenMobile 控制台提供 Citrix Files 配置、服务级别监视和许可证使用情况监视。

有关针对 Citrix Files 配置 XenMobile 的详细信息，请参阅 SAML 单点登录与 Citrix Files。

存储区域连接器

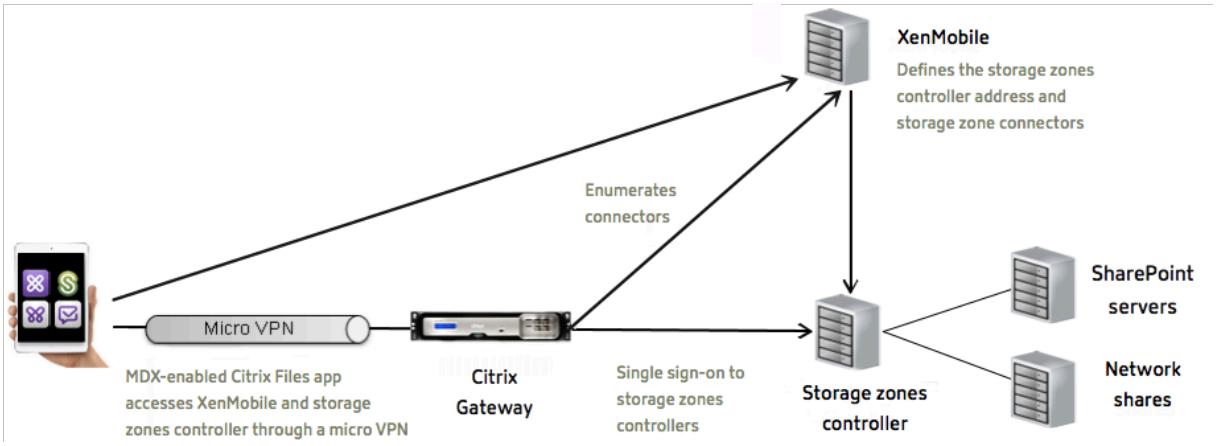
可以配置 XenMobile 以仅提供对通过 XenMobile 控制台创建的存储区域连接器的访问权限。该配置：

- 提供对现有本地存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问。
- 不需要您设置 Citrix Content Collaboration 子域或托管 Citrix Files 数据。
- 为用户提供通过适用于 iOS 和 Android 的 Citrix Files 移动生产力应用程序对数据进行移动访问的权限。用户可以编辑 Microsoft Office 文档。用户还可以从移动设备预览和批注 Adobe PDF 文件。
- 遵守防止在企业网络外部泄漏用户信息的安全限制。
- 可以通过 XenMobile 控制台对存储区域连接器进行简单设置。如果您以后决定在 XenMobile 中使用完整的 Citrix Files 功能，可以在 XenMobile 控制台中更改配置。
- 需要 XenMobile Enterprise Edition。

仅限 XenMobile 与存储区域连接器的集成：

- Citrix Content Collaboration 将单点登录配置用于 Citrix Gateway 以向存储区域控制器进行身份验证。
- 由于不使用 Citrix Files 控制平面，因此 XenMobile 不通过 SAML 进行身份验证。

下图显示了 XenMobile 与存储区域连接器结合使用的高级体系结构。



要求

- 最低组件版本：
  - XenMobile Server 10.5（本地）
  - ShareFile for iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - 存储区域控制器 5.0

    本文包含有关如何配置存储区域控制器 5.0 的说明
- 请确保要运行存储区域控制器的服务器满足系统要求。有关要求，请参阅系统要求。

Citrix Files 数据的存储区域和受限存储区域的要求不适用于 XenMobile 仅与存储区域连接器的集成。

XenMobile 不支持 “文档” 连接器。

- 运行 PowerShell 脚本：
  - 在 32 位 (x86) 版本的 PowerShell 中运行脚本。

安装任务

按显示顺序完成以下任务以安装和设置存储区域控制器。这些步骤专门用于 XenMobile 仅与存储区域连接器的集成。存储区域控制器文档中包含其中一些文章。

1. 为存储区域控制器配置 Citrix ADC

   可以将 Citrix ADC 用作存储区域控制器的 DMZ 代理。

2. 安装 SSL 证书

   托管标准区域的存储区域控制器需要 SSL 证书。托管受限区域的存储区域控制器使用内部地址，不需要 SSL 证书。

3. 准备您的服务器

   需要为存储区域连接器完成 IIS 和 ASP.NET 设置。

4. 安装存储区域控制器
5. 准备存储区域控制器以仅与存储区域连接器结合使用
6. 指定存储区域的代理服务器

   存储区域控制器控制台允许您为存储区域控制器指定代理服务器。还可以使用其他方法指定代理服务器。

7. 配置域控制器以信任存储区域控制器进行委派

   配置域控制器以在网络共享或 SharePoint 站点上支持 NTLM 或 Kerberos 身份验证。

8. 将辅助存储区域控制器加入存储区域

   要配置存储区域以实现高可用性，请至少将两个存储区域控制器连接到该存储区域。

安装存储区域控制器

1. 下载并安装存储区域控制器软件：

   a) 转到 https://www.citrix.com/downloads。搜索 **ShareFile**，然后下载最新的存储区域控制器安装程序。

   b) 安装存储区域控制器会将服务器上的默认 Web 站点更改为控制器的安装路径。在默认 Web 站点上启用匿名身份验证。

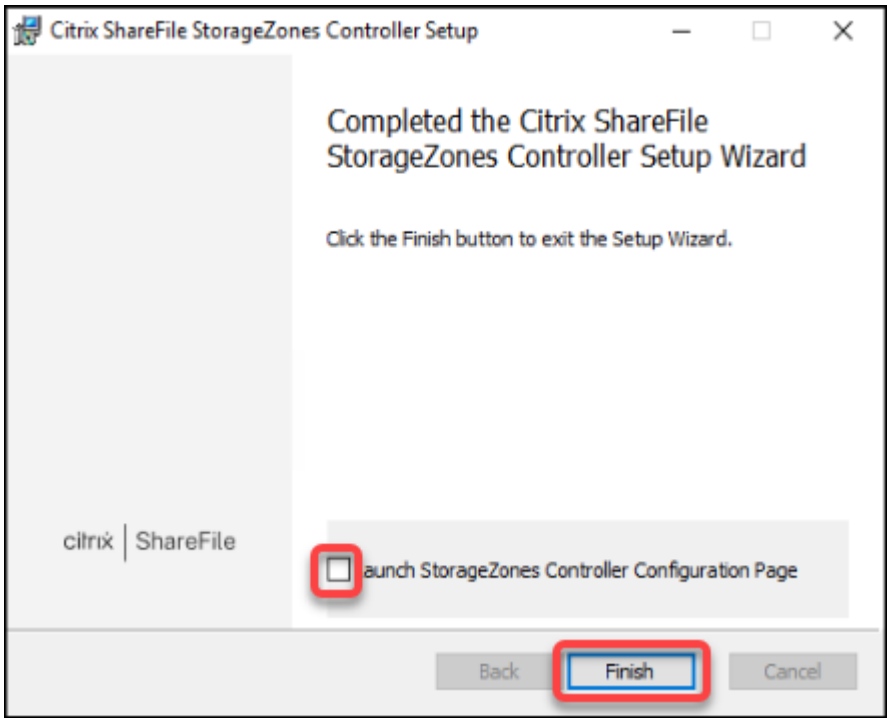
2. 在要安装存储区域控制器的服务器上，运行 StorageCenter.msi。

   存储区域控制器设置向导将会启动。

3. 回复提示：

   - 在目标文件夹页面上，如果 Internet Information Services (IIS) 安装在默认位置中，则保留默认值。如果不是，请浏览到 IIS 安装位置。

- 安装完成后，取消选中 **Launch StorageZones Controller Configuration Page**（启动存储区域控制器配置页面）复选框，然后单击 **Finish**（完成）。



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/`。如果安装成功，会显示 Citrix Files 徽标。

   如果没有显示 Citrix Files 徽标，请清除浏览器缓存，然后重试。

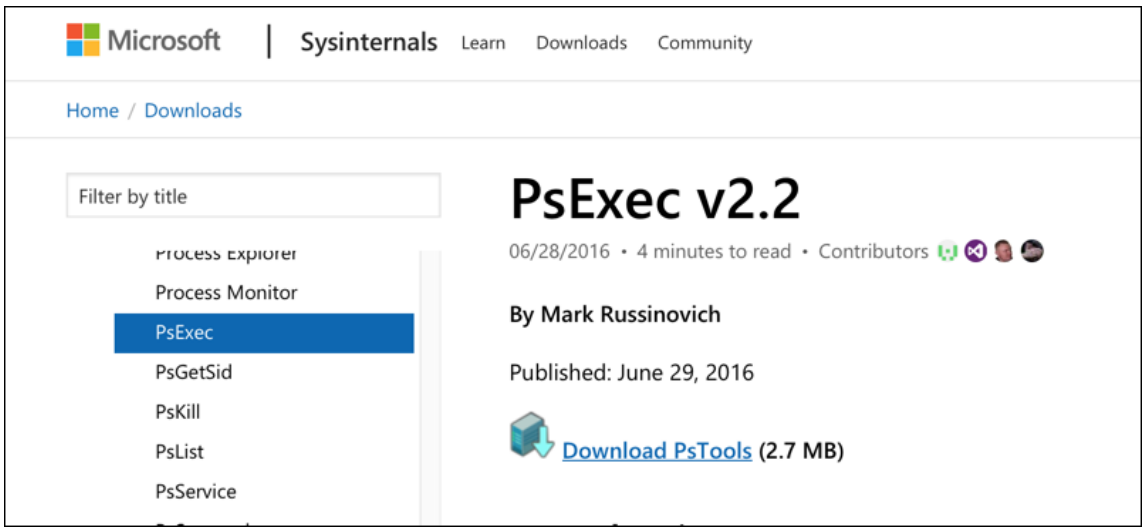
   > 重要：
   >
   > 如果您打算克隆存储区域控制器，请先捕获磁盘映像，然后再继续配置存储区域控制器。

准备存储区域控制器以仅与存储区域连接器结合使用

对于仅与存储区域连接器的集成，不要使用存储区域控制器管理控制台。该接口需要 Citrix Files 管理员帐户，这对此解决方案没有必要。因此，请运行 PowerShell 脚本以在不使用 Citrix Files 控制平面的情况下准备要使用的存储区域控制器。该脚本执行以下操作：

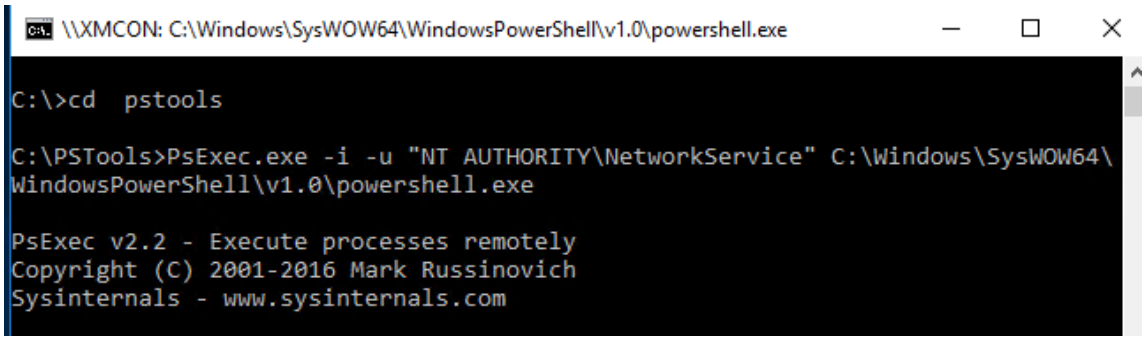
- 将当前存储区域控制器注册为主存储区域控制器。以后可以将辅助存储区域控制器加入主控制器。
- 创建区域并为其设置密码。

1. 在您的存储区域控制器服务器上，下载 PsExec 工具：导航到 Microsoft Windows Sysinternals，然后单击 **Download PsTools**（下载 PsTools）。将工具提取到 C 驱动器的根目录。

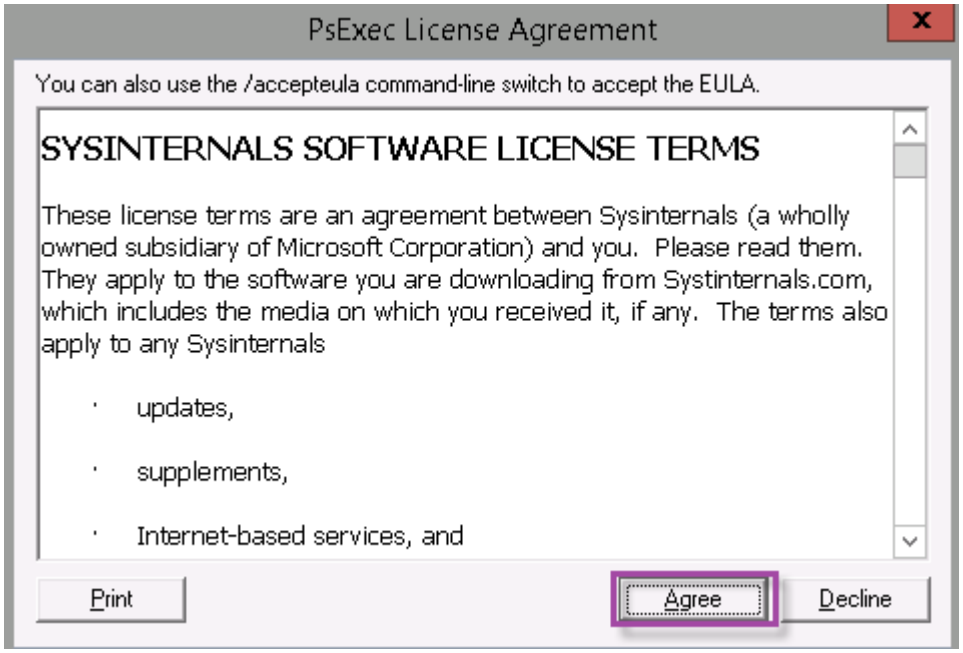


2. 运行 PsExec 工具：以管理员用户身份打开命令提示窗口，然后键入以下命令：

```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy-->
```



3. 出现提示时，单击 **Agree**（同意）以运行 Sysinternals 工具。



此时打开 PowerShell 窗口。

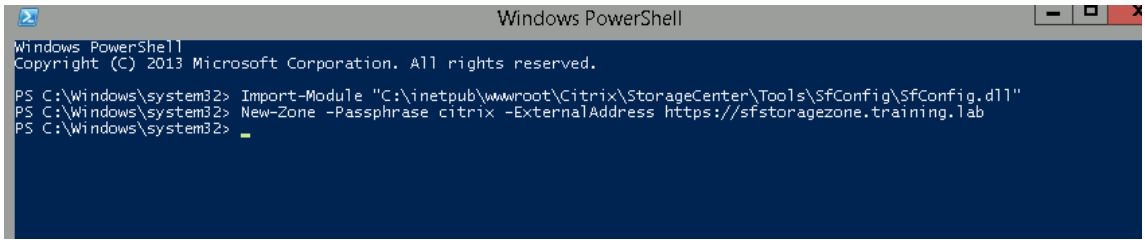
4. 在 PowerShell 窗口中，键入以下命令：

```
1 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
2 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
3 <!--NeedCopy-->
```

其中：

Passphrase（密码）：您要分配给站点的密码。请将其记录下来。无法从控制器恢复密码。如果您丢失了密码，则无法重新安装存储区域控制器。将更多存储区域控制器加入到存储区域，或者在服务器出现故障时恢复存储区域。

ExternalAddress（外部地址）：存储区域控制器服务器的外部完全限定的域名。



您的主存储区域控制器现已就绪。

在登录到 XenMobile 以创建存储区域连接器之前：完成以下配置（如果适用）：

指定存储区域的代理服务器

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 XenMobile 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

要配置存储区域以实现高可用性，请至少将两个存储区域控制器连接到该存储区域。要将辅助存储区域控制器加入区域，请在另一台服务器上安装存储区域控制器。然后将该控制器加入主控制器的区域。

1. 在您要将其加入主服务器的存储区域控制器服务器上打开 PowerShell 窗口。
2. 在 PowerShell 窗口中，键入以下命令：

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

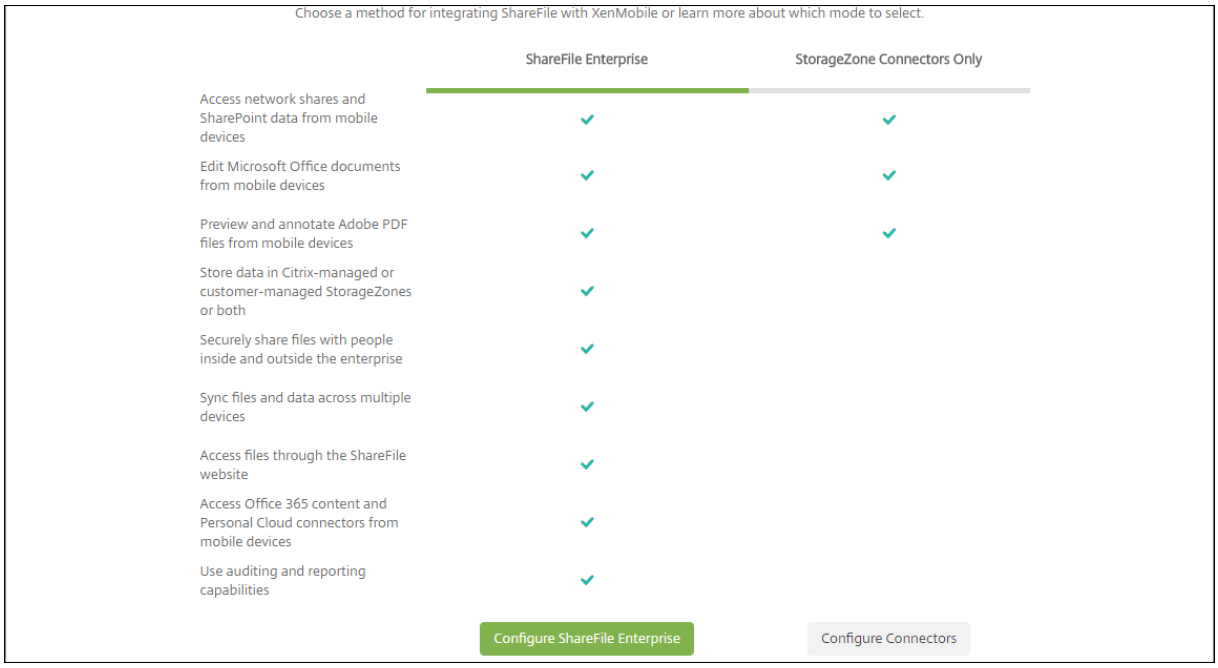
   例如：

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

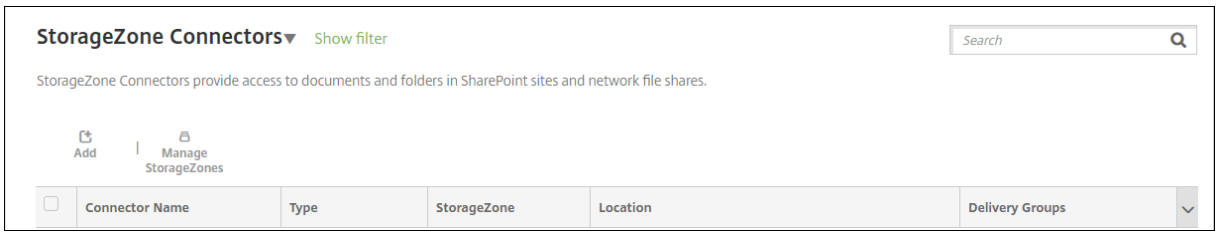
在 **XenMobile** 中定义存储区域控制器连接

在添加存储区域连接器之前，可以为针对存储区域连接器启用的每个存储区域控制器配置连接信息。可以按本节所述定义存储区域控制器，也可以在添加连接器时定义存储区域控制器。

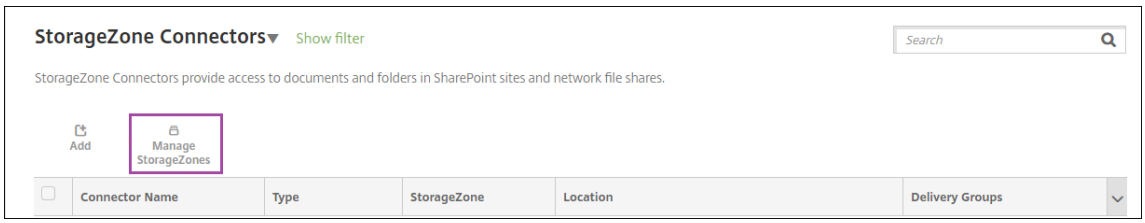
在您第一次访问配置 **> ShareFile** 页面时，页面上会总结适用于企业帐户的 XenMobile 与存储区域连接器结合使用之间差异。



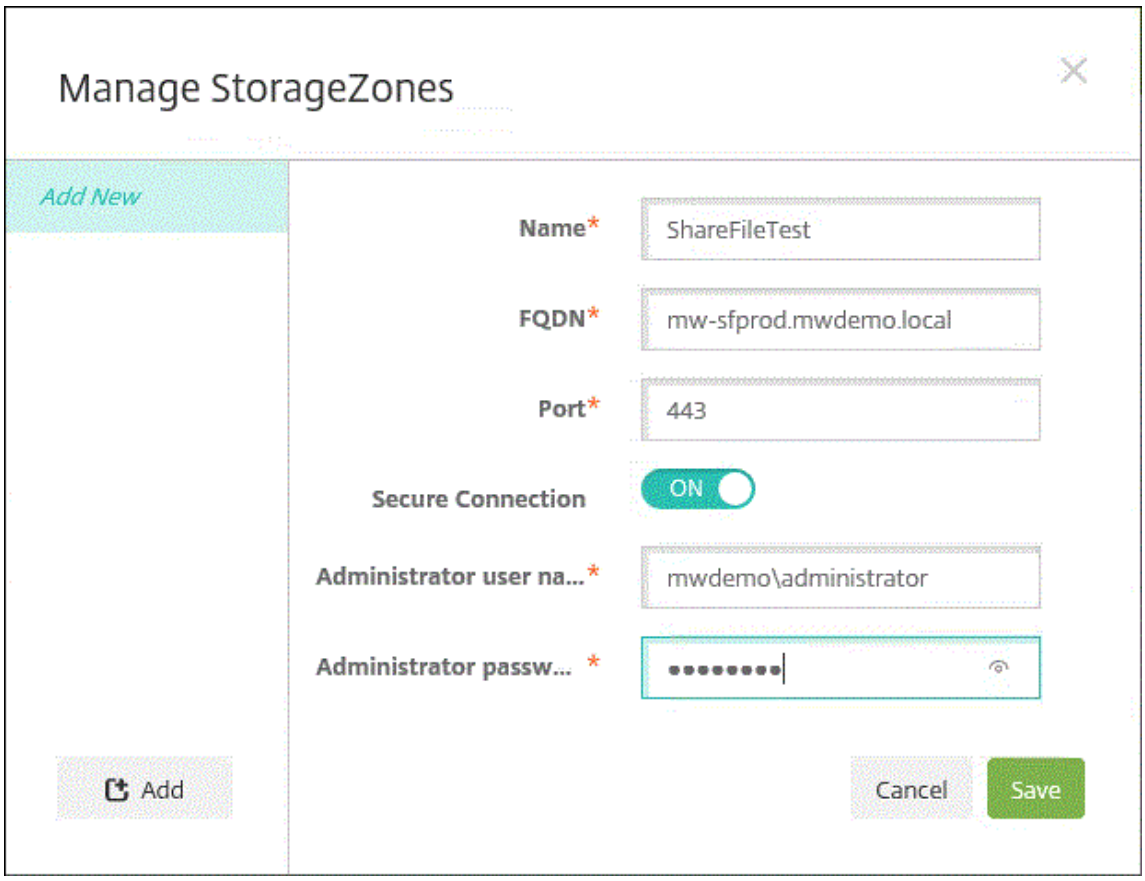
单击配置连接器继续执行本文中的配置步骤。



1. 在配置 **> ShareFile** 中，单击管理 **StorageZone**。



2. 在管理 **StorageZone** 中，添加连接信息。



- 名称： StorageZone 的描述性名称，用于在 XenMobile 中标识 StorageZone。请勿在名称中包含空格或特殊字符。
- **FQDN** 和端口：可从 XenMobile Server 访问的存储区域控制器的完全限定域名和端口号。
- 安全连接：如果对与存储区域控制器的连接使用 SSL，则使用默认设置“开”。如果不对连接使用 SSL，则将此设置更改为关。

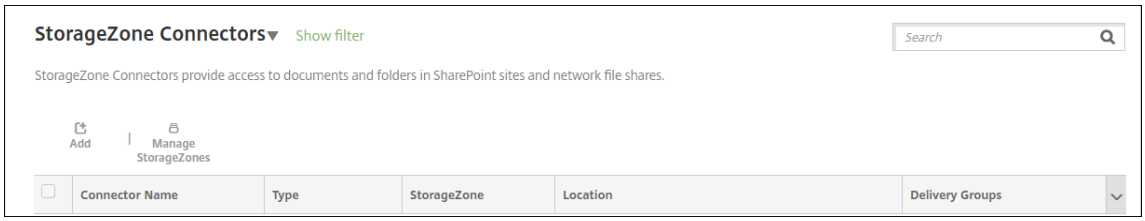
- 管理员用户名和管理员密码：管理员服务帐户用户名称（采用 domain\admin 形式）和密码。或者，对存储区域控制器具有读写权限的用户帐户。

3. 单击保存。
4. 要测试连接，请验证 XenMobile Server 是否可以访问端口 443 上的存储区域控制器的完全限定的域名。
5. 要定义另一个存储区域控制器连接，请在管理 **StorageZone** 中单击添加按钮。

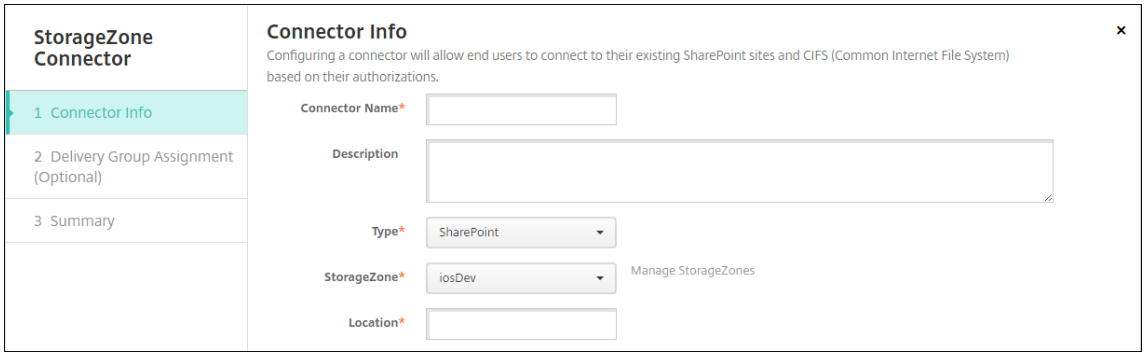
   要编辑或删除存储区域控制器连接的信息，请在管理 **StorageZone** 中选择连接名称。然后单击编辑或删除。

在 **XenMobile** 中添加存储区域连接器

1. 转到配置 **> ShareFile**，然后单击添加。

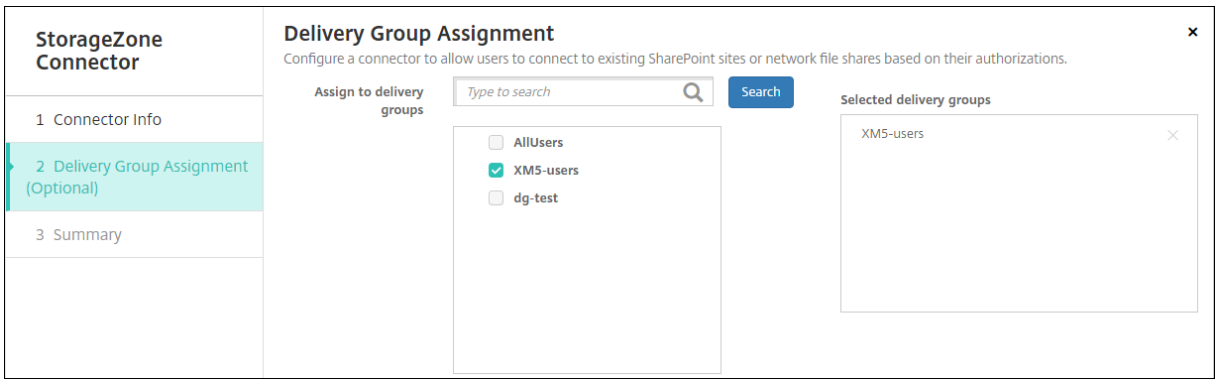


2. 在连接器信息页面上，配置以下设置：



   - 连接器名称：在 XenMobile 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。
   - **StorageZone**：选择与连接器关联的存储区域。如果没有列出存储区域，请单击管理 **StorageZone** 以定义存储区域控制器。
   - 位置：对于 SharePoint，指定 SharePoint 根级别站点、站点集合或文档库的 URL（采用 `https://sharepoint.company.com` 形式）。对于网络共享，指定统一命名约定 (UNC) 路径的完全限定域名（采用 \\server\share 形式）。

3. 在交付组分配页面上，可以选择将连接器分配给交付组。或者，可以通过使用配置 **>** 交付组将连接器关联到交付组。



1. 在摘要页面上，可以查看配置的选项。要调整配置，请单击上一步。
2. 单击保存以保存连接器。
3. 测试连接器：

   a) 打包 Citrix Files 客户端时，请执行以下操作：

   - 将网络访问策略设置为通过通道连接到内部网络。

   在此操作模式下，XenMobile MDX 框架截获来自 Citrix Files 客户端的所有网络流量。通过使用应用程序特定的 Micro VPN，流量经 Citrix Gateway 重定向。

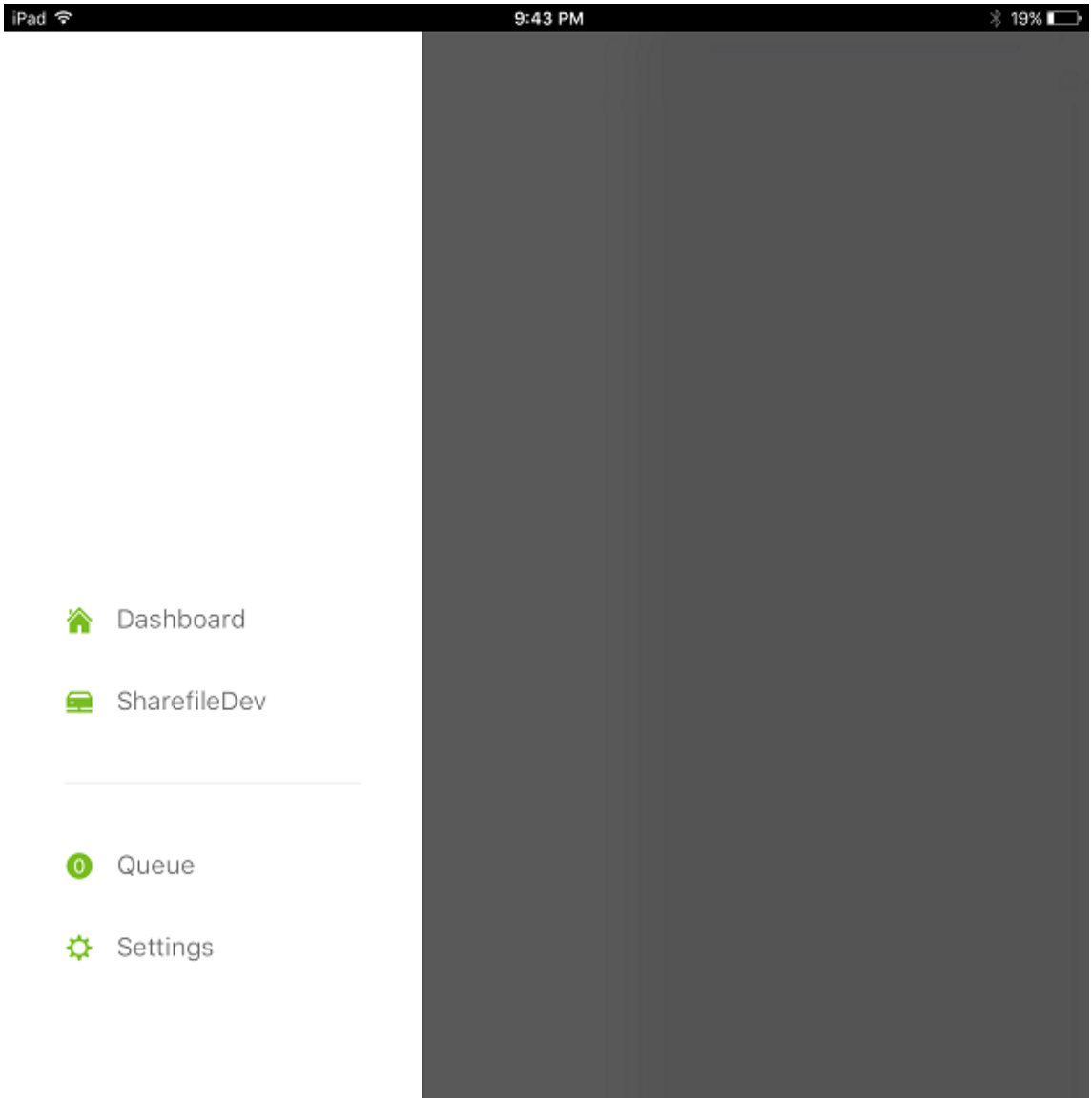
   - 将“首选 VPN 模式”策略设置为通道 **- Web SSO**。

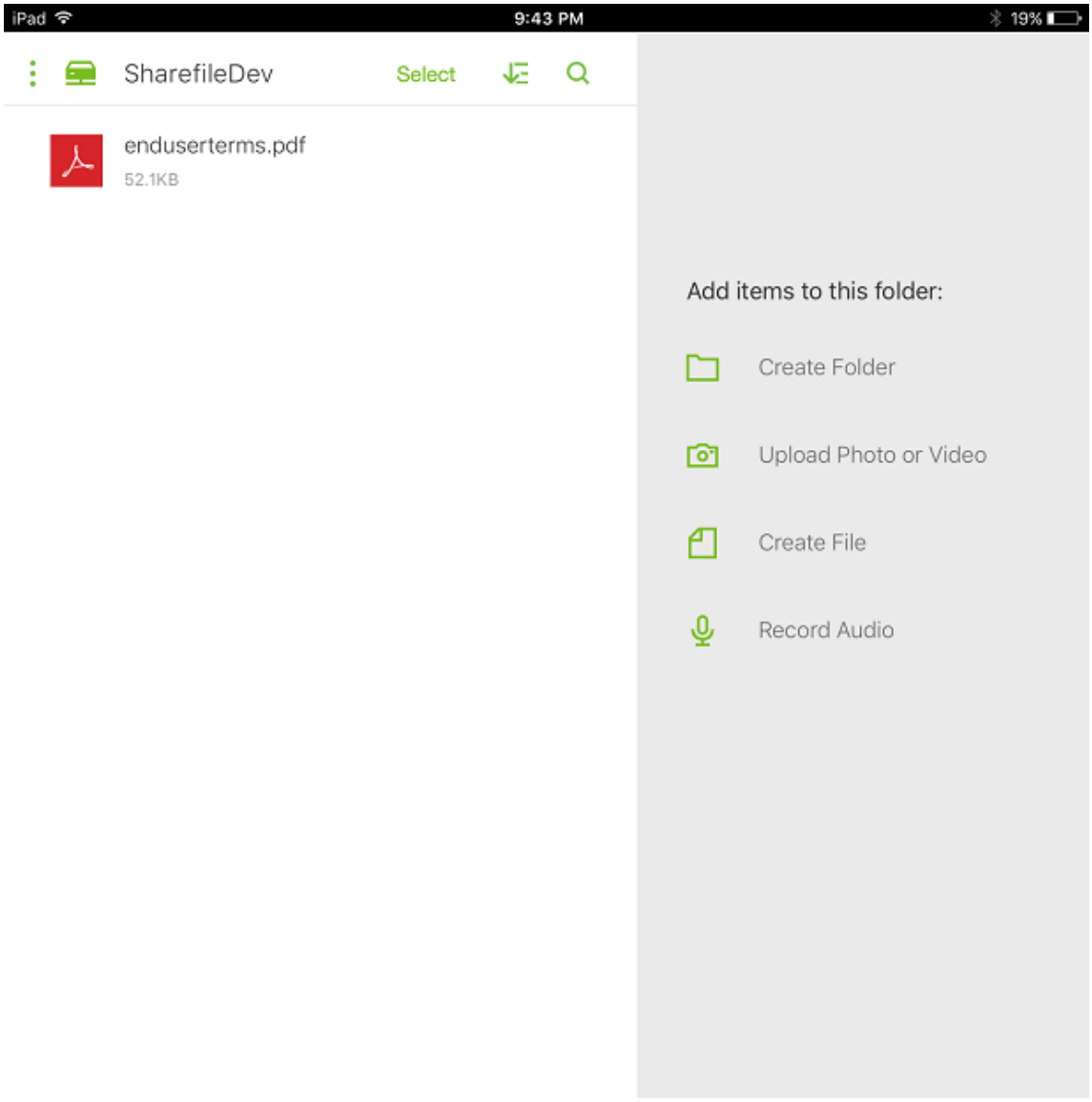
   在此通道模式下，MDX 框架会终止来自 MDX 应用程序的 SSL/HTTP 流量。MDX 随后代表用户启动与内部连接的新连接。此策略设置允许 MDX 框架检测和响应 Web 服务器发出的身份验证质询。

   b) 将 Citrix Files 客户端添加到 XenMobile。有关详细信息，请参阅集成并交付适用于 Endpoint Management 的 Citrix Files 客户端。

   c) 在支持的设备上，验证到 Citrix Files 和连接器的单点登录。

在以下示例中，ShareFileDev 是连接器的名称。

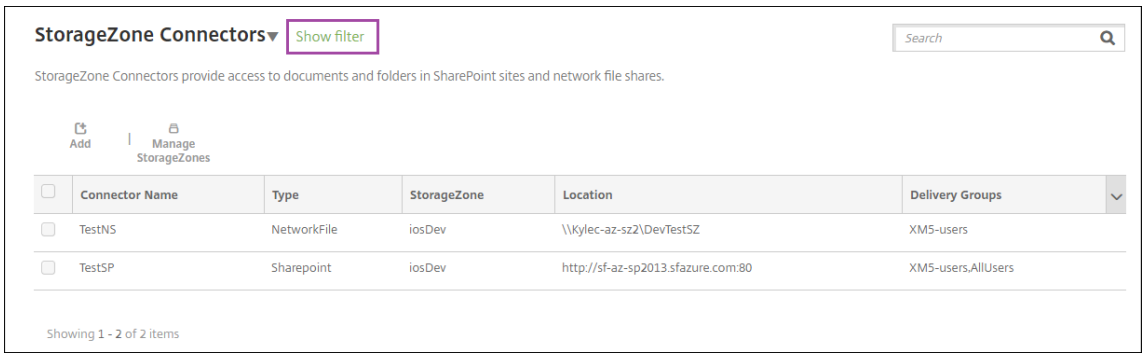




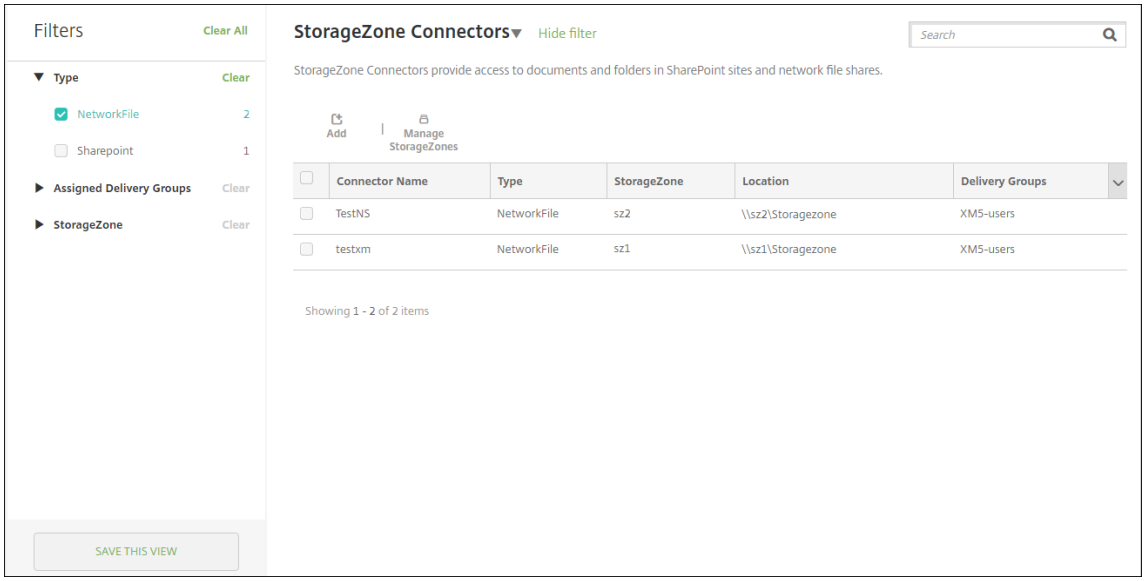
过滤存储区域连接器列表

可以按连接器类型、分配的交付组和存储区域来过滤存储区域连接器列表。

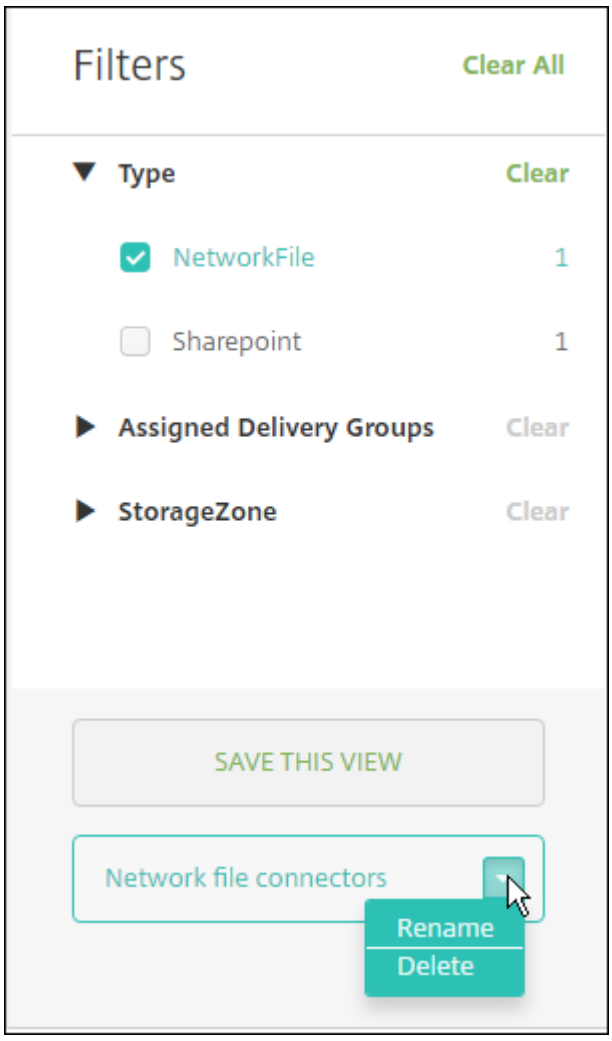
1. 转到配置 **> ShareFile**，然后单击显示过滤器。



2. 展开要进行选择的过滤器标题。要保存过滤器，请单击保存此视图，键入过滤器名称，并单击保存。



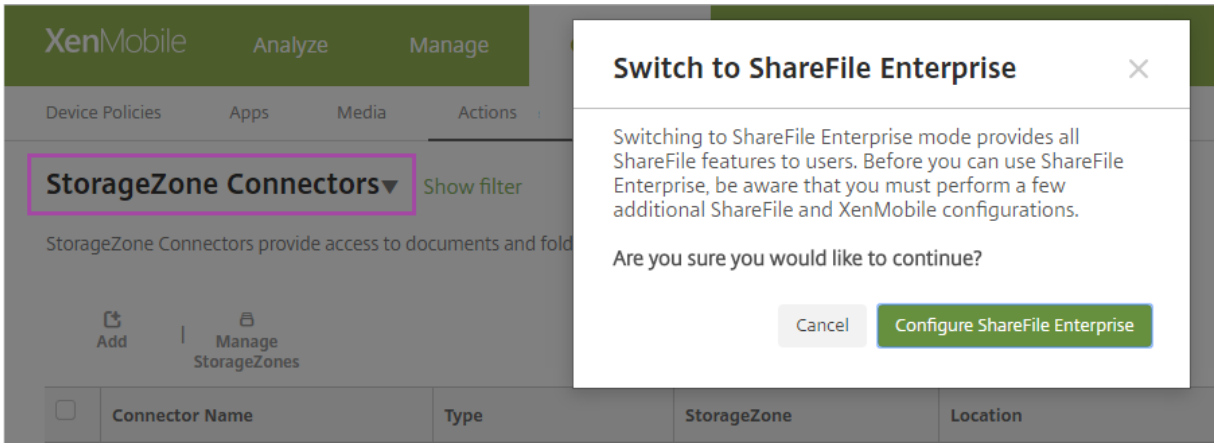
3. 要重命名或删除过滤器，请单击过滤器名称旁边的箭头图标。



切换到 **Citrix Files**

将存储区域连接器与 XenMobile 集成后，可以稍后切换到完整的 Enterprise 功能集。要使用 Citrix Files 功能集，需要使用 XenMobile Enterprise Edition。XenMobile 会保留现有的存储区域连接器集成设置。

转到配置 **> ShareFile**，单击 **StorageZone** 连接器下拉菜单，然后单击配置 **ShareFile Enterprise**。



有关配置 Citrix Files 的信息，请参阅 SAML 单点登录与 Citrix Files。

适用于 **HDX** 应用程序的 **SmartAccess**

January 5, 2022

此功能允许您根据设备属性、设备的用户属性或设备上已安装的应用程序控制对 HDX 应用程序的访问。您可以通过设置自动化操作使用此功能将设备标记为不合规，以拒绝该设备的访问。与此功能结合使用的 HDX 应用程序通过拒绝访问不合规设备的 SmartAccess 策略在 Virtual Apps and Desktops 中配置。XenMobile 使用签名的加密标记向 StoreFront 传达设备的状态。StoreFront 随后根据应用程序的访问控制策略允许或拒绝访问。

要使用此功能，您的部署要求：

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 或 3.8
- 配置为从 StoreFront 服务器聚合 HDX 应用程序的 XenMobile Server
- XenMobile Server 配置有 SAML 证书，用于签名和加密标记。不带私钥的相同证书在 StoreFront 服务器上上载。

要开始使用此功能，请执行以下操作：

- 配置 XenMobile Server 证书并将其上载到 StoreFront 应用商店
- 使用所需的 SmartAccess 策略配置至少一个 Virtual Apps and Desktops 交付组
- 在 XenMobile 中设置自动化操作

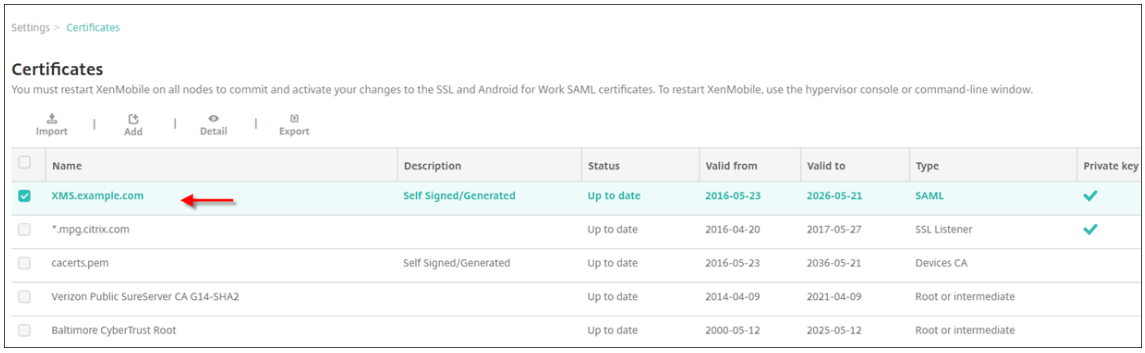
导出并配置 **XenMobile Server** 证书并将其上载到 **StoreFront** 应用商店

SmartAccess 使用签名的加密标记在 XenMobile 与 StoreFront 服务器之间进行通信。要启用该通信，请将 XenMobile Server 证书添加到 StoreFront 应用商店。

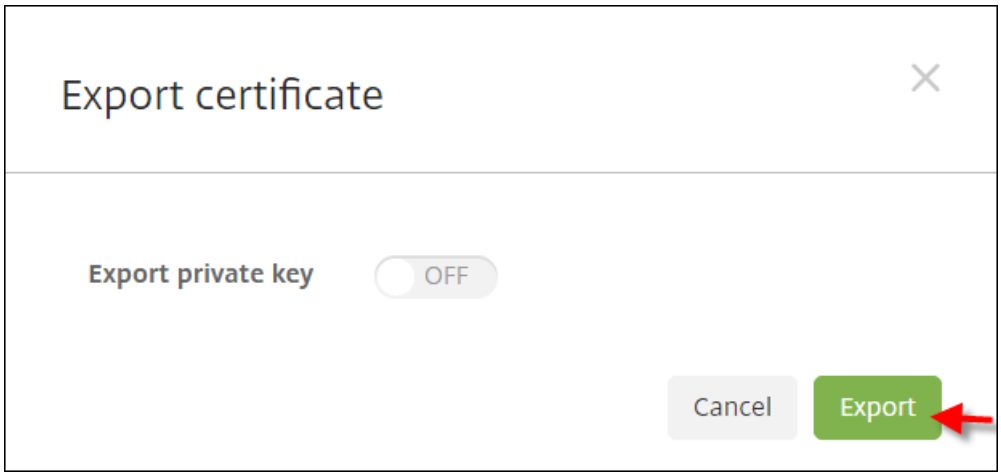
有关在对 XenMobile 启用了域和基于证书的身份验证时将 StoreFront 与 XenMobile 集成的详细信息，请参阅支持知识中心。

从 **XenMobile Server** 中导出 **SAML** 证书

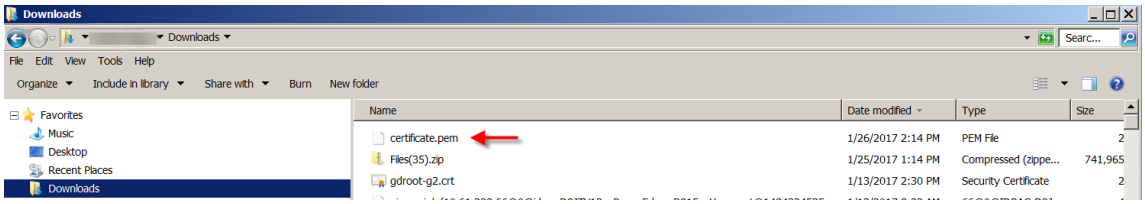
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。单击证书。
2. 找到 XenMobile Server 的 SAML 证书。



3. 确保导出私钥设置为关。单击导出将该证书导出到您的下载目录。

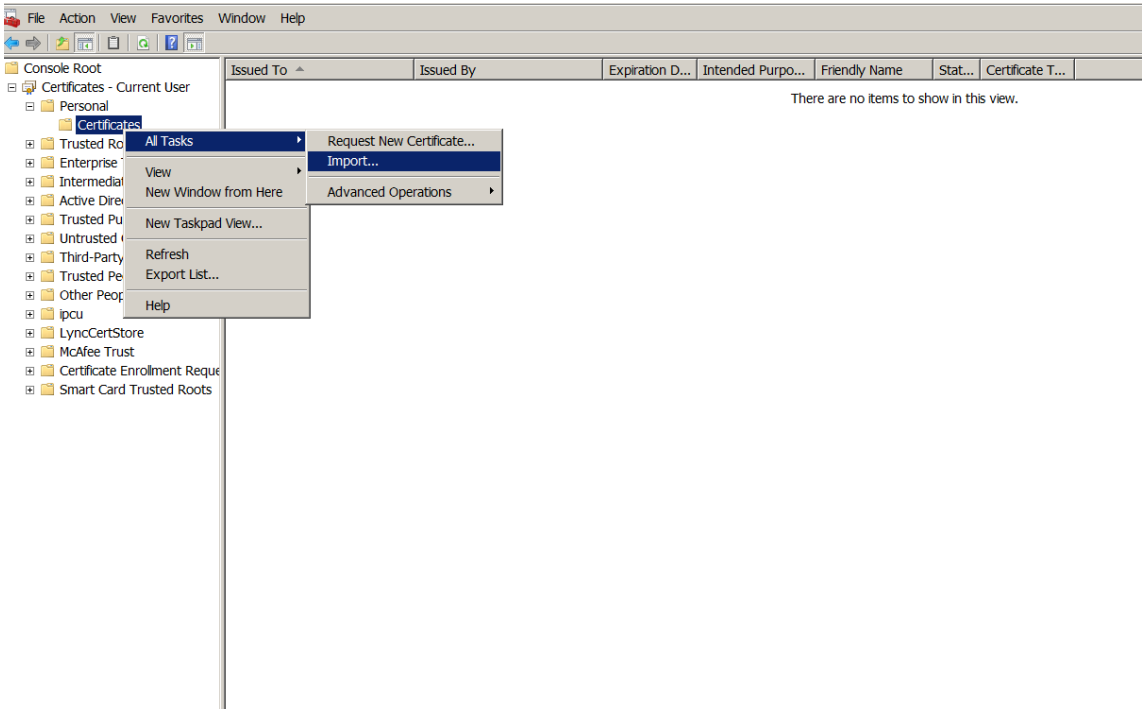


4. 在您的下载目录中找到该证书。证书为 PEM 格式。

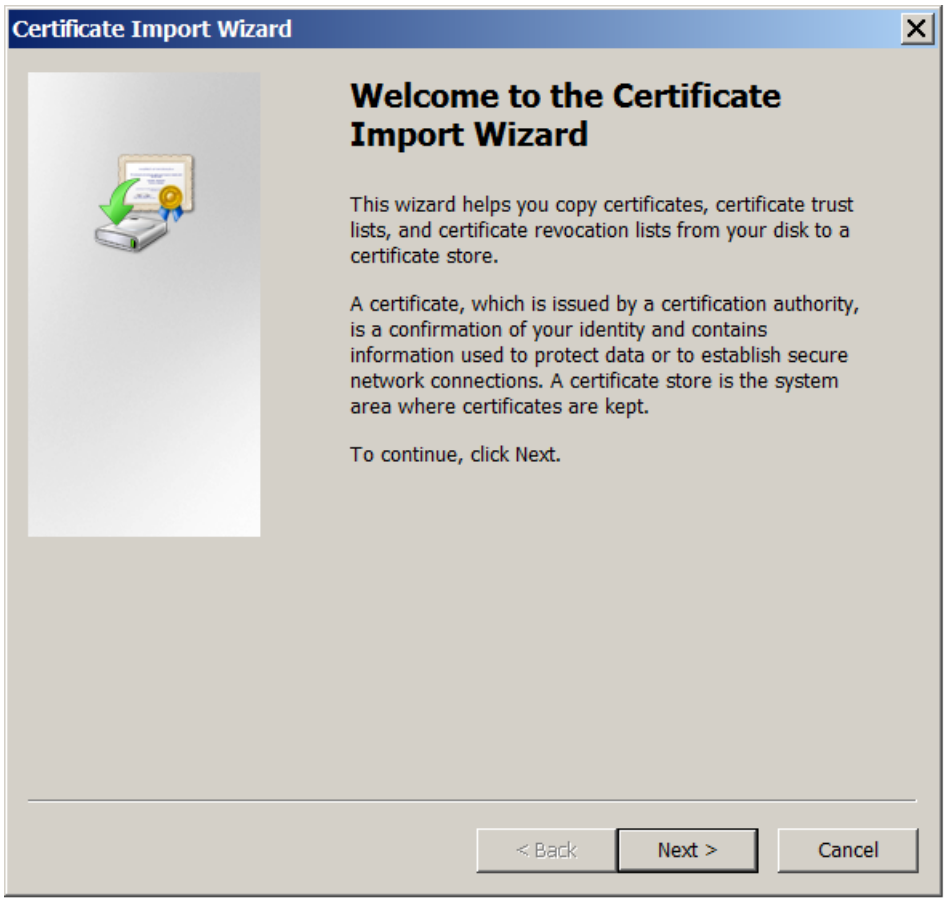


将证书从 **PEM** 转换为 **CER**

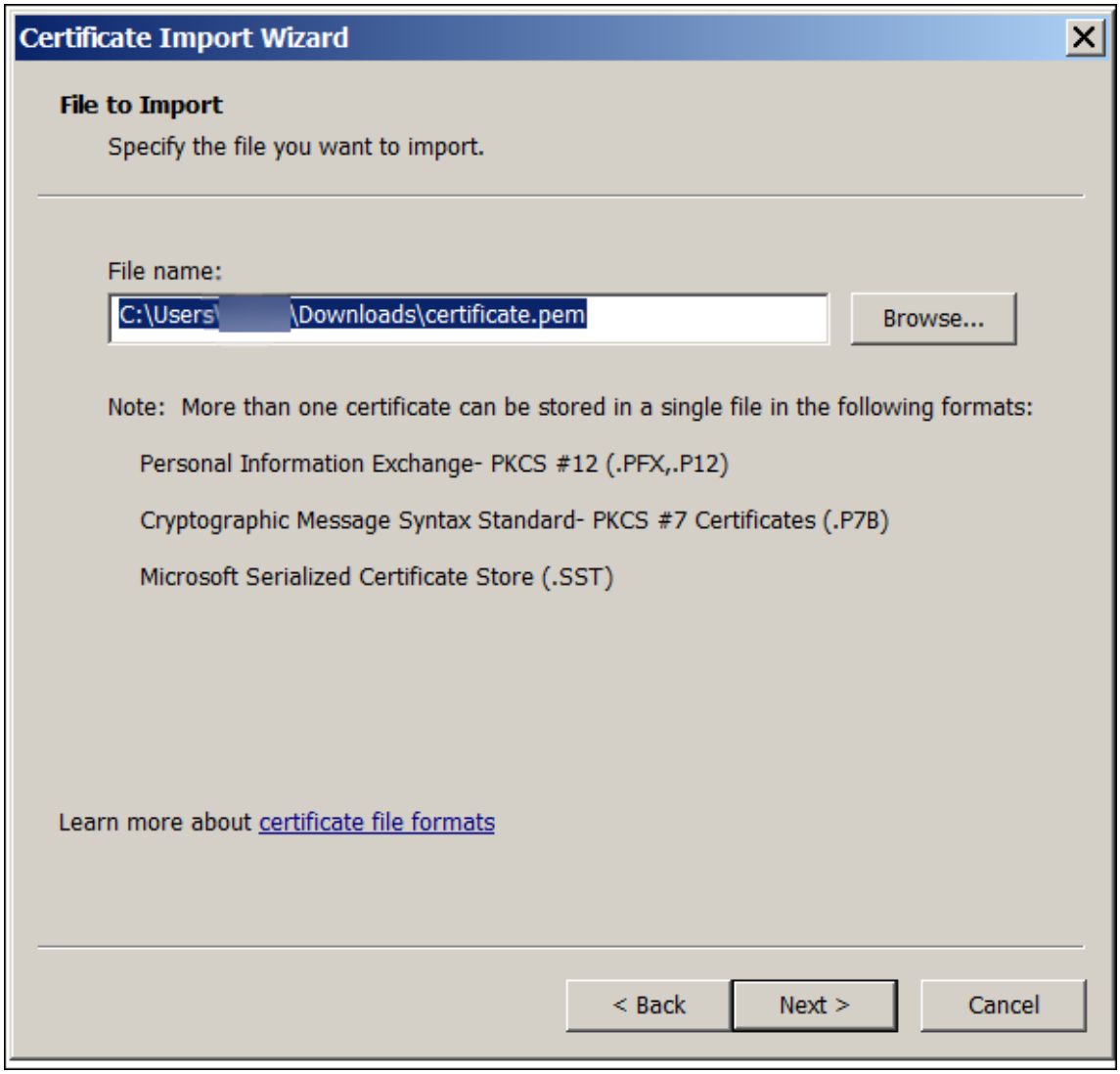
1. 打开 Microsoft 管理控制台 (MMC)，然后右键单击证书 **>** 所有任务 **>** 导入。



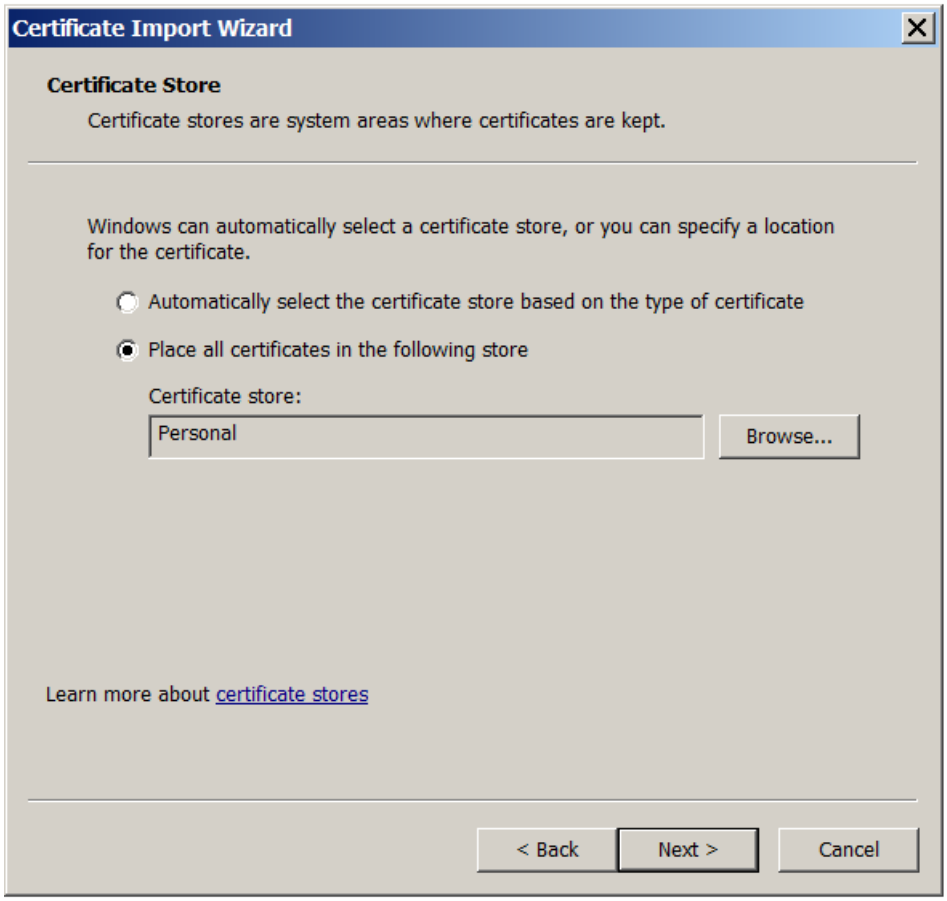
2. 证书导入向导显示时，单击下一步。



3. 浏览到下载目录中的证书。

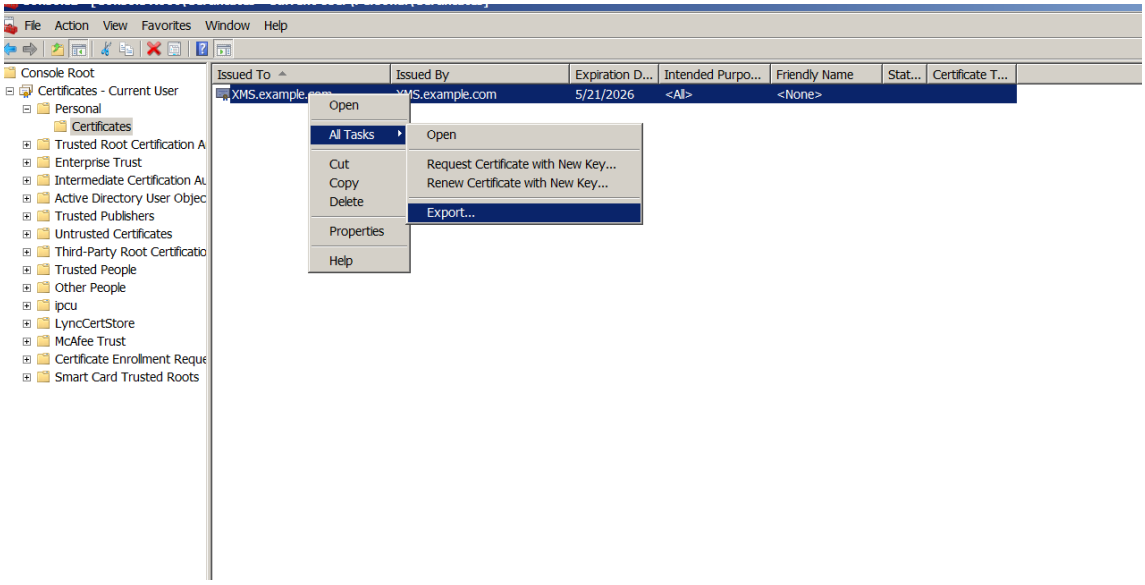


4. 选择将所有的证书都放入下列存储，然后选择个人作为证书存储。单击 **Next**（下一步）。



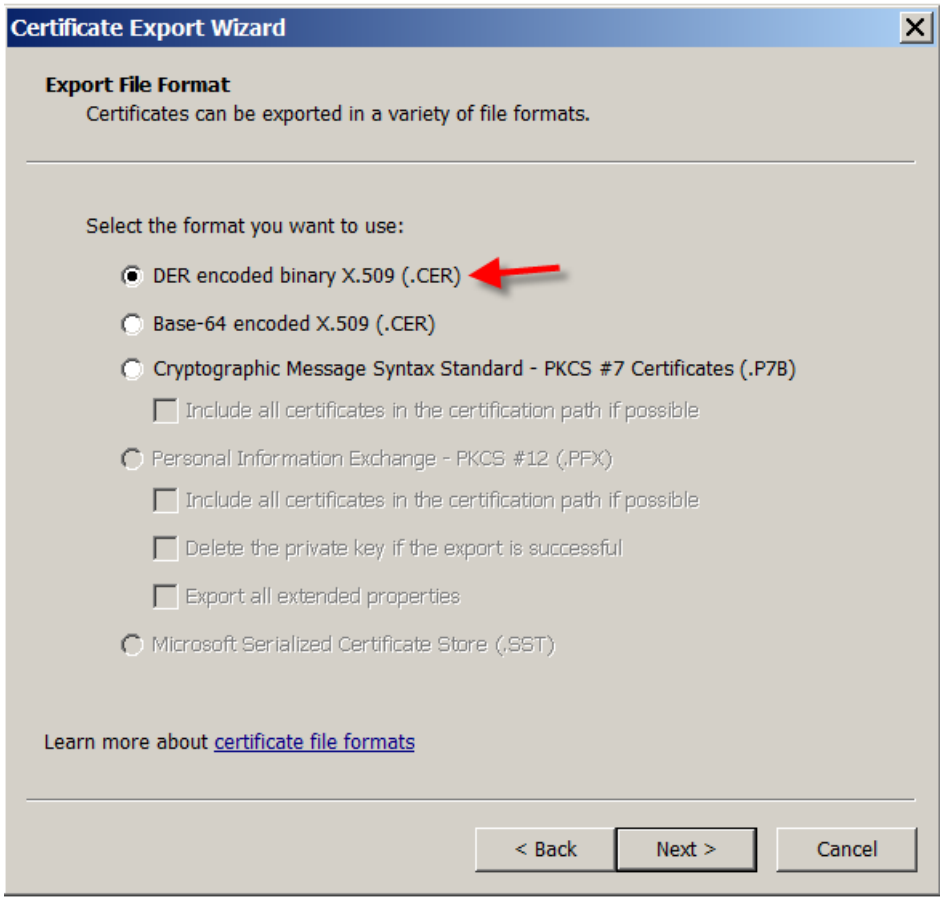
5. 检查您的选择，然后单击完成。单击确定消除确认窗口。

6. 在 MMC 中，右键单击证书，然后选择所有任务 **>** 导出。

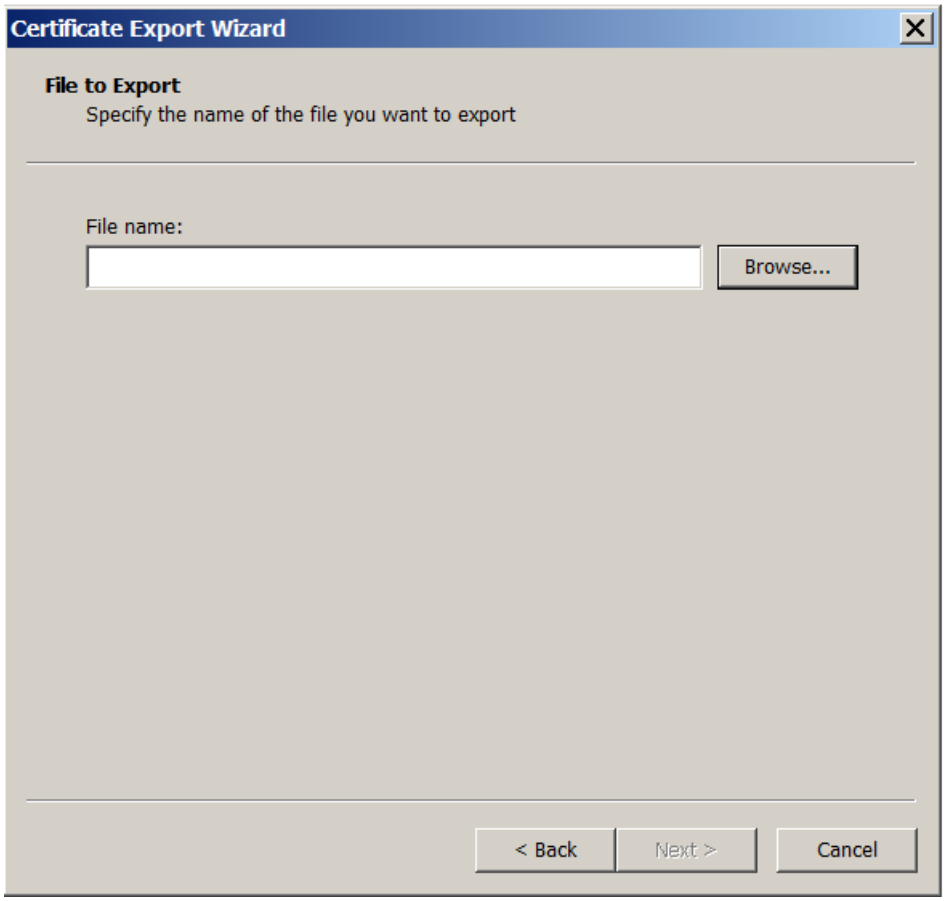


7. 证书导出向导显示时，单击下一步。

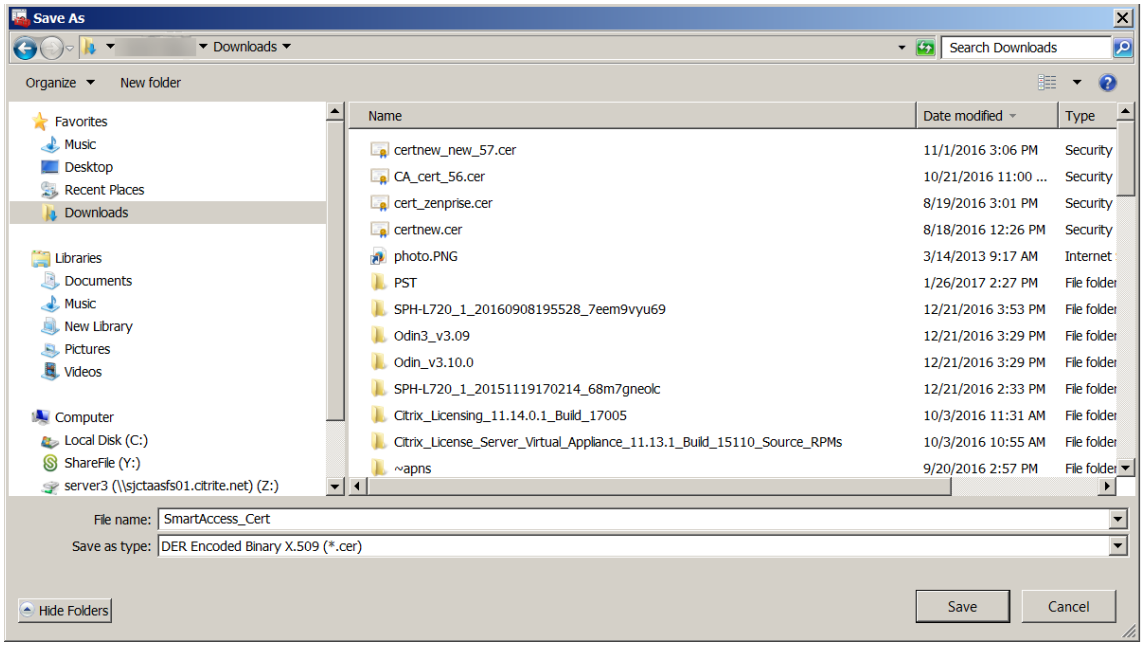
8. 选择格式 **DER** 编码二进制 **X.509 (.CER)**。单击 **Next**（下一步）。



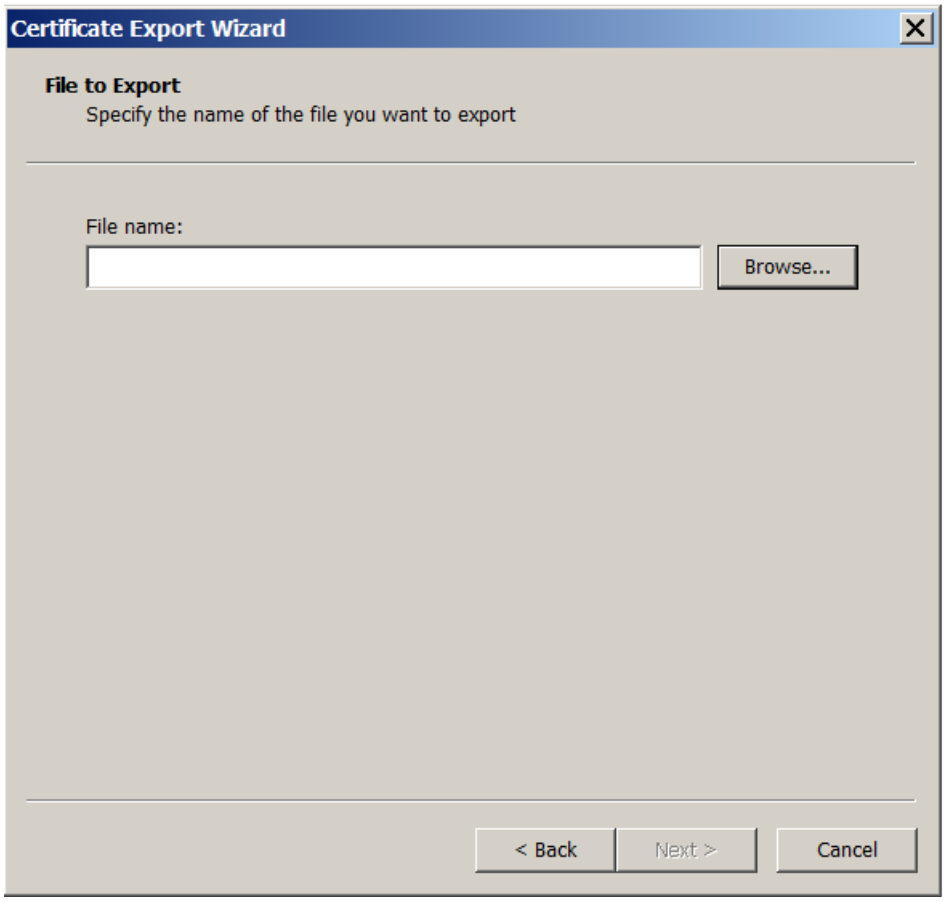
9. 浏览到该证书。键入证书名称，然后单击下一步。



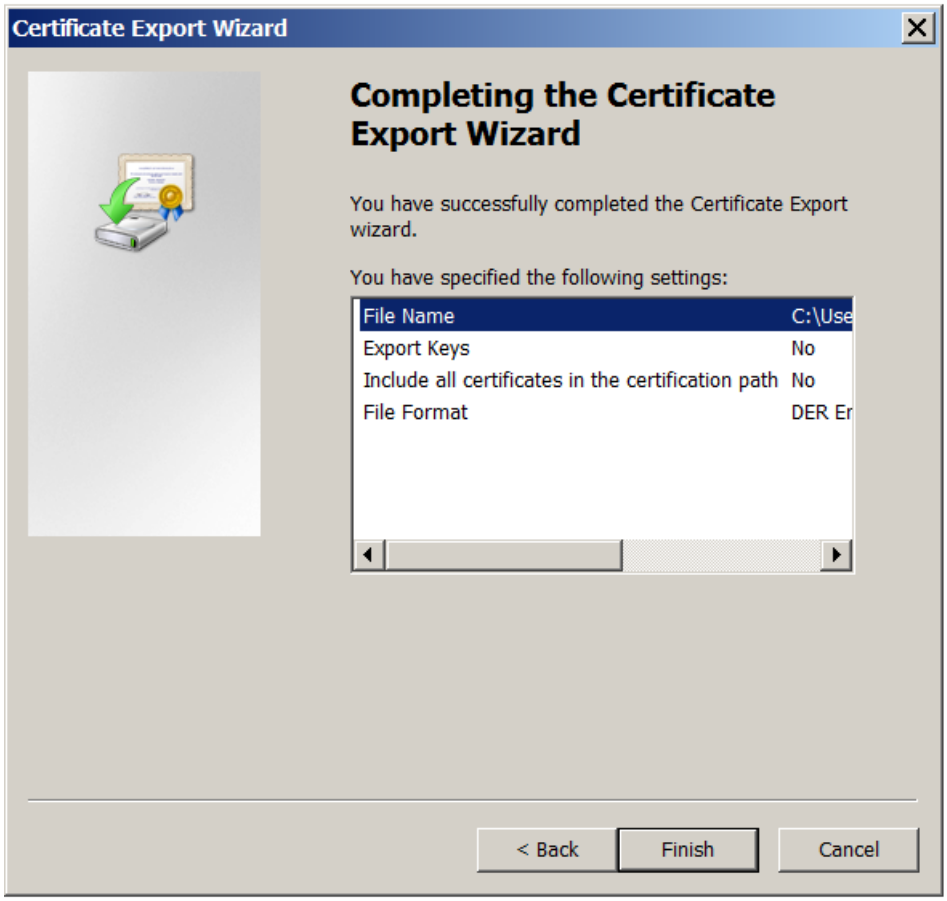
10. 保存该证书。



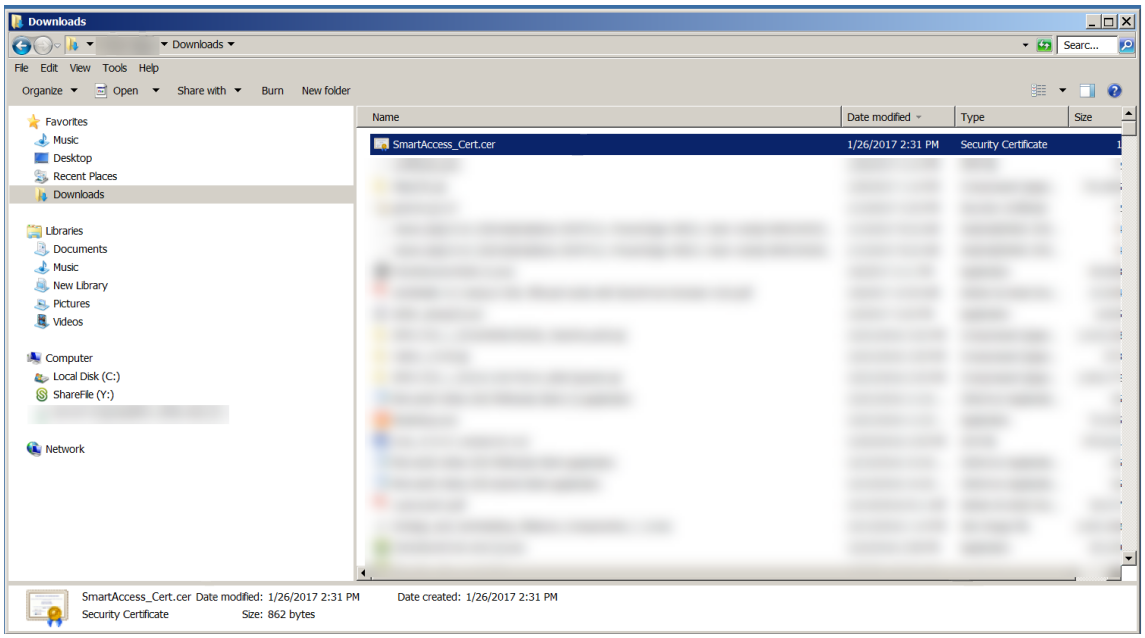
11. 浏览到该证书，然后单击下一步。



12. 检查您的选择，然后单击完成。单击确定消除确认窗口。

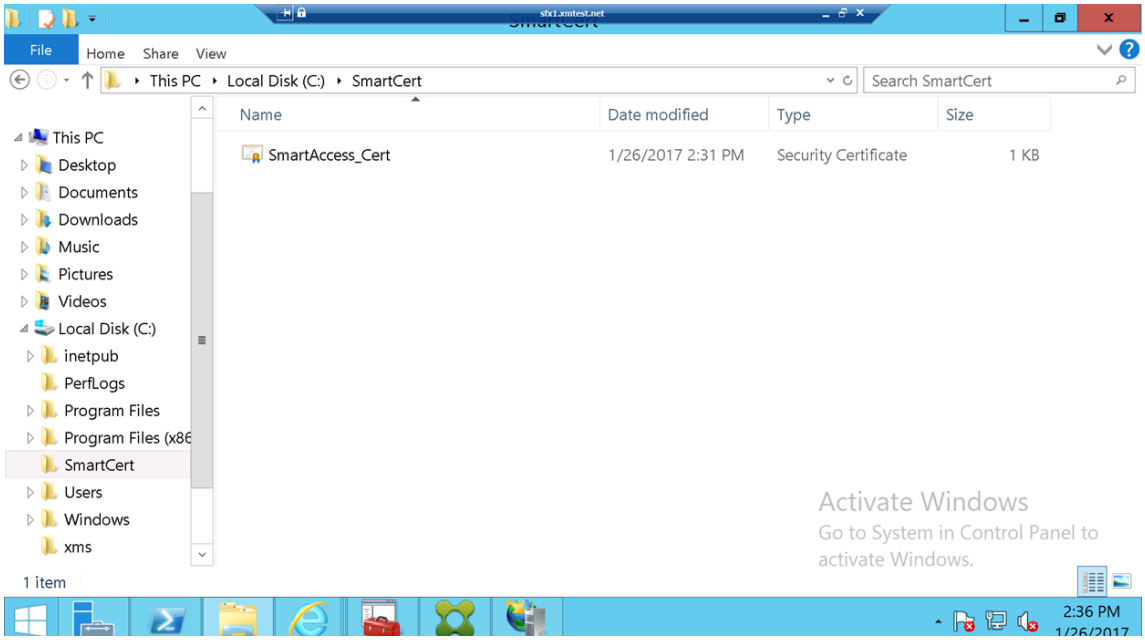


13. 在您的下载目录中找到该证书。请注意，证书为 CER 格式。



将证书复制到 **StoreFront** 服务器

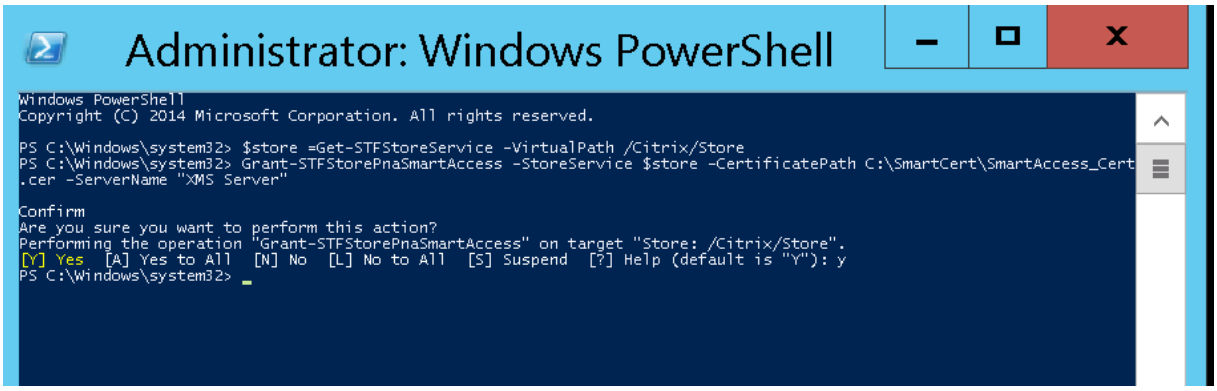
1. 在 StoreFront 服务器上，创建一个名为 **SmartCert** 的文件夹。
2. 将证书复制到 **SmartCert** 文件夹。



在 **StoreFront** 应用商店中配置证书

在 StoreFront 服务器上，运行以下 PowerShell 命令以在该应用商店上配置转换后的 XenMobile Server 证书：

```
1     Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2 <!--NeedCopy-->
```



如果 StoreFront 应用商店上存在任何现有证书，请运行以下 PowerShell 命令以将其吊销：

```
1     Revoke-STFStorePnaSmartAccess -StoreService $store -All
2 <!--NeedCopy-->
```


或者，可以在 StoreFront 服务器上运行以下任意 PowerShell 命令以吊销 StoreFront 应用商店中的现有证书：

- 按名称吊销：

```
1     $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3     Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "
          My XM Server"
4 <!--NeedCopy-->
```

- 按指纹吊销：

```
1     $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3     Revoke-STFStorePnaSmartAccess -StoreService $store -
          CertificateThumbprint "ReplaceWithThumbprint"
4 <!--NeedCopy-->
```

- 按服务器对象吊销：

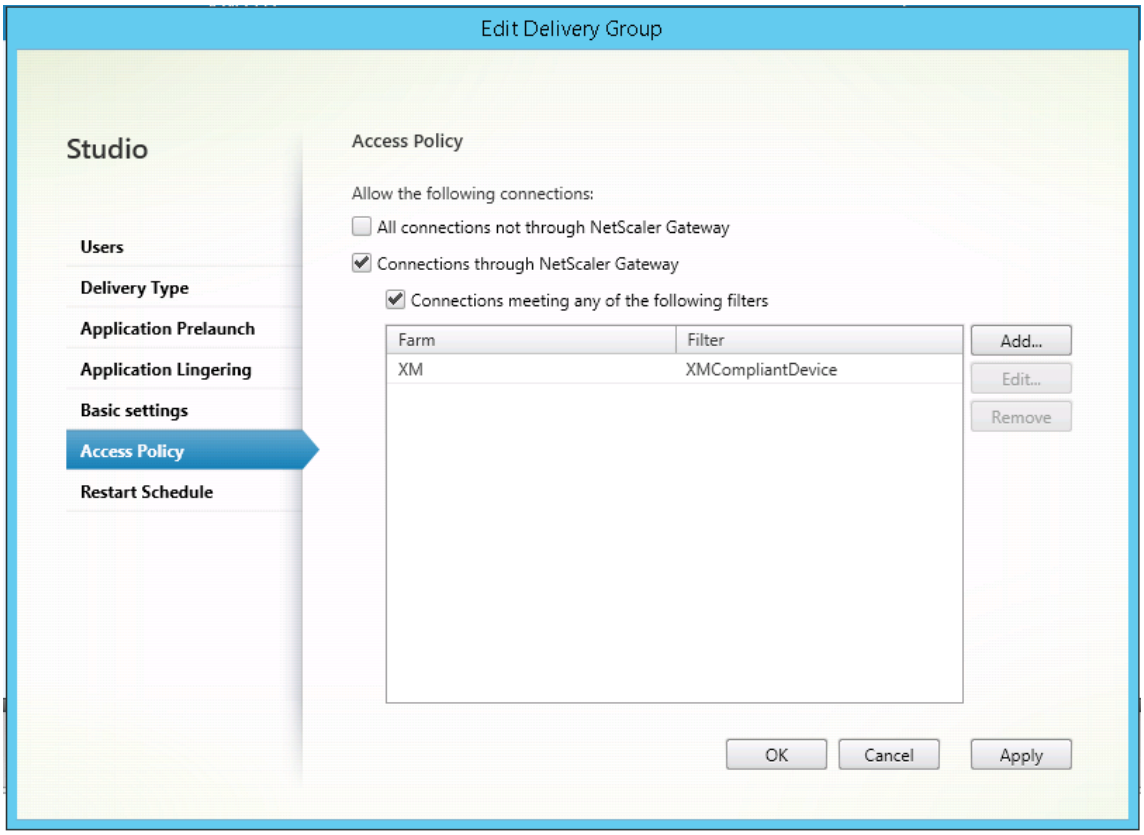
```
1     $store = Get-STFStoreService -VirtualPath /Citrix/Store
2
3     $access = Get-STFStorePnaSmartAccess -StoreService $store
4
5     Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess
          $access.AccessConditionsTrusts[0]
6 <!--NeedCopy-->
```

为 **Virtual Apps and Desktops** 配置 **SmartAccess** 策略

要将所需的 SmartAccess 策略添加到用于提供 HDX 应用程序的交付组中，请执行以下操作：

1. 在 Virtual Apps and Desktops 服务器上，打开 Citrix Studio。
2. 在 Studio 导航窗格中选择交付组。
3. 选择用于提供要控制对其访问的一个或多个应用程序的组。然后在操作窗格中选择编辑交付组。
4. 在访问策略页面上，选择通过 **NetScaler Gateway** 的连接和 **Connection meeting any of the following**（满足以下任一情况的连接）。
5. 单击添加。

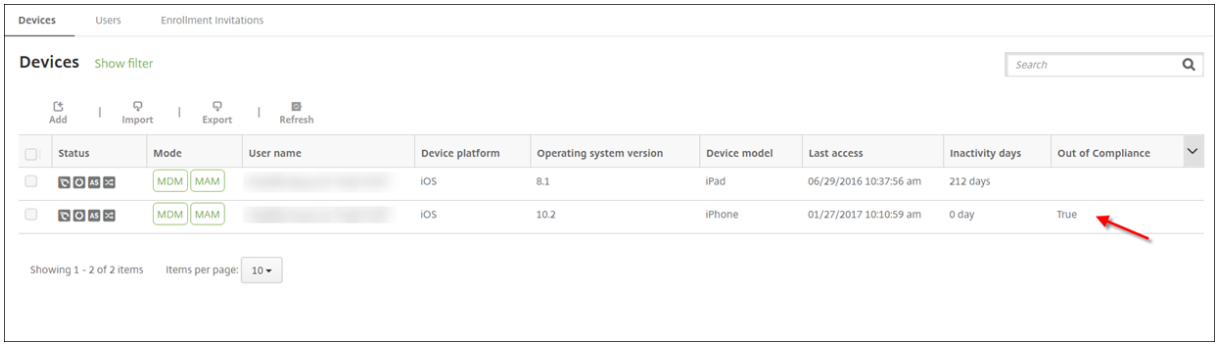
6. 添加场为 **XM** 且过滤器为 **XMCompliantDevice** 的访问策略。



7. 单击应用以应用您所做的任何更改并使窗口保持打开，或单击确定应用更改并关闭窗口。

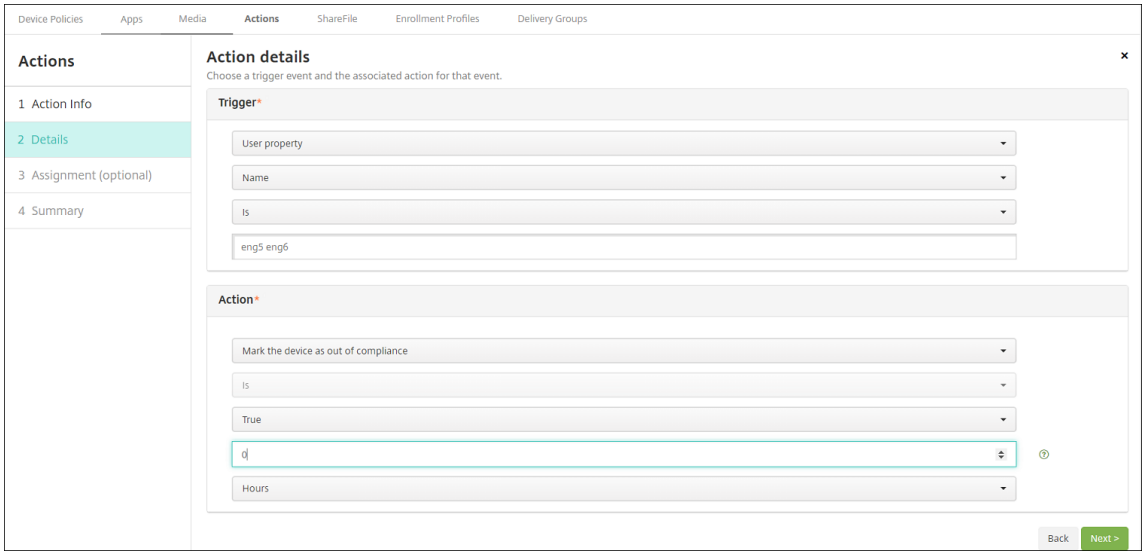
在 **XenMobile** 中设置自动化操作

您在交付组中为 HDX 应用程序设置的 SmartAccess 策略在某个设备不合规时拒绝访问该设备。使用自动化操作将设备标记为不合规。



1. 在 XenMobile 控制台中，单击配置 **>** 操作。此时将显示操作页面。
2. 单击添加以添加操作。此时将显示操作信息页面。
3. 在操作信息页面上，键入操作的名称和说明。

4. 单击 **Next**（下一步）。此时将显示操作详细信息页面。在以下示例中，创建了一个在设备的用户属性名称为 **eng5** 或 **eng6** 时立即将其标记为不合规的触发器。

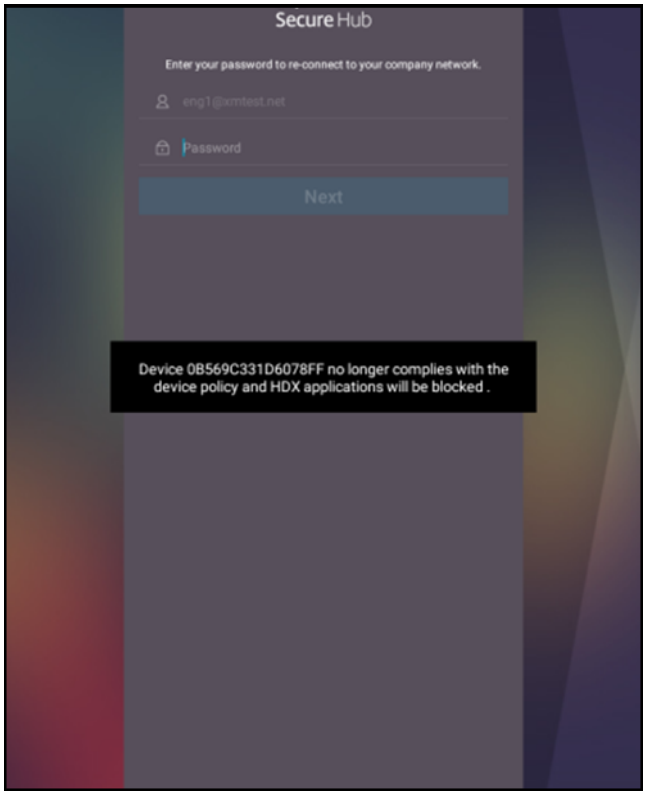


5. 在触发器列表中，选择设备属性、用户属性或已安装应用程序的名称。SmartAccess 不支持事件触发器。
6. 在操作列表中：
   - 选择将设备标记为不合规。
   - 选择是。
   - 选择 **True**。
   - 要将操作设置为满足触发条件时立即将设备标记为不合规，请将时间范围设置为 **0**。
7. 选择要应用此操作的一个或多个 XenMobile 交付组。
8. 检查操作的摘要。
9. 单击下一步，然后单击保存。

当设备被标记为不合规时，HDX 应用程序不会再在 Secure Hub 应用商店中显示。用户将无法再订阅这些应用程序。不会向设备发送任何通知，并且 Secure Hub 应用商店中没有任何迹象指示以前提供过 HDX 应用程序。

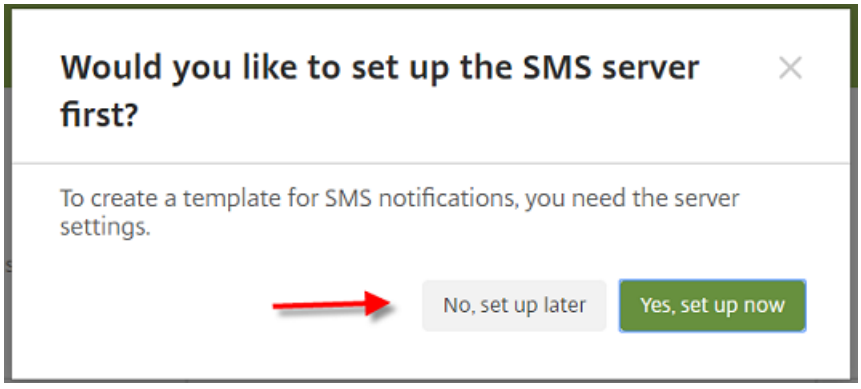
如果希望用户在设备被标记为不合规时接收通知，请创建一个通知，然后创建一项用于发送该通知的自动化操作。

本示例将在设备被标记为不合规时创建并发送以下通知：Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked（设备序列号或电话号码不再符合设备策略，HDX 应用程序将被阻止）。



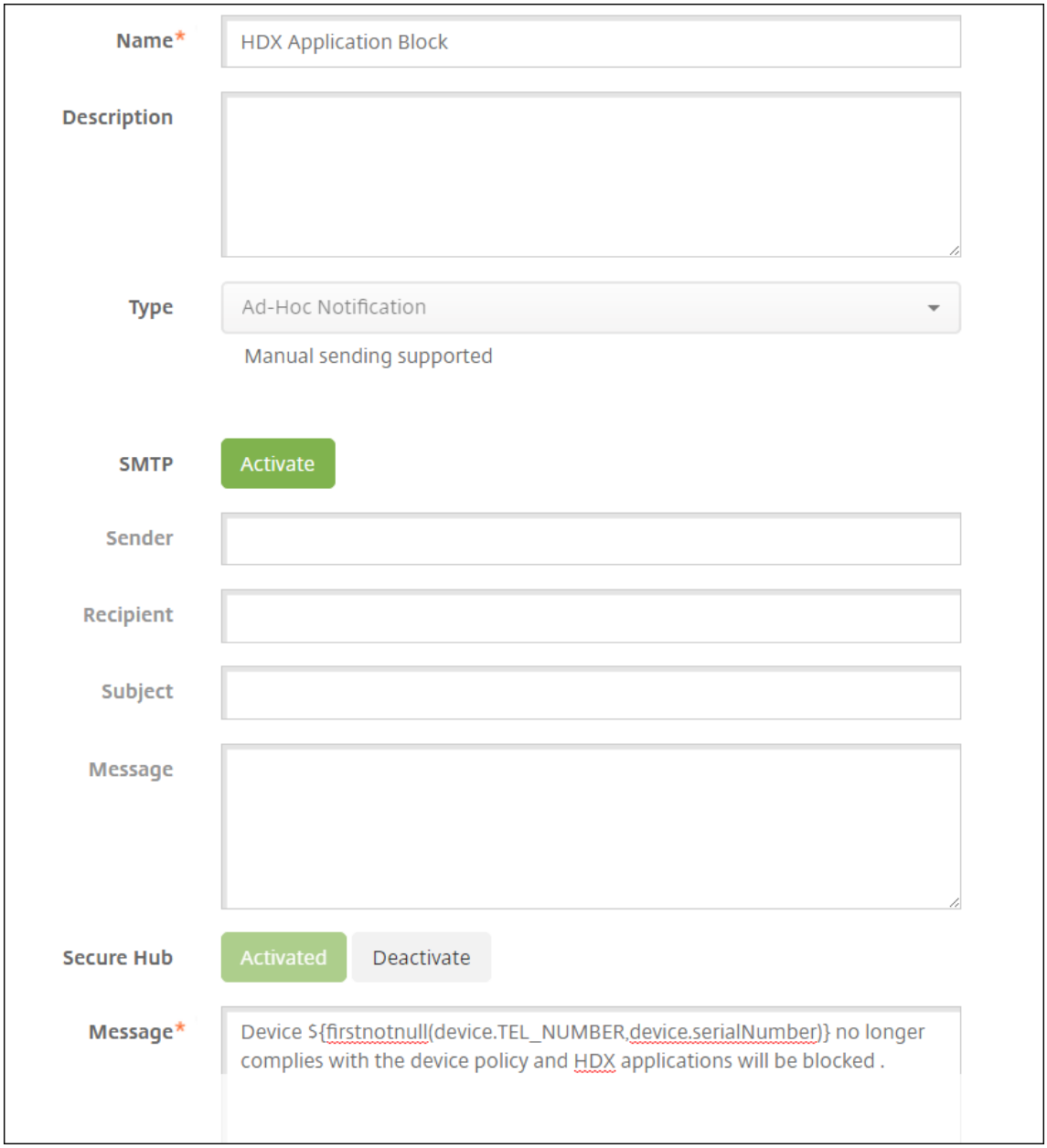
创建当设备被标记为不合规时用户看到的通知

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击通知模板。此时将显示通知模板页面。
3. 单击添加在通知模板页面上进行添加。
4. 当系统提示您先设置 SMS 服务器时，请单击否，稍后设置。



5. 配置以下设置：
   - 名称： HDX 应用程序阻止
   - 说明：设备不合规时的代理通知

- 类型：临时通知
- **Secure Hub**：已激活
- 消息：设备 ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} 不再符合设备策略，HDX 应用程序将被阻止。

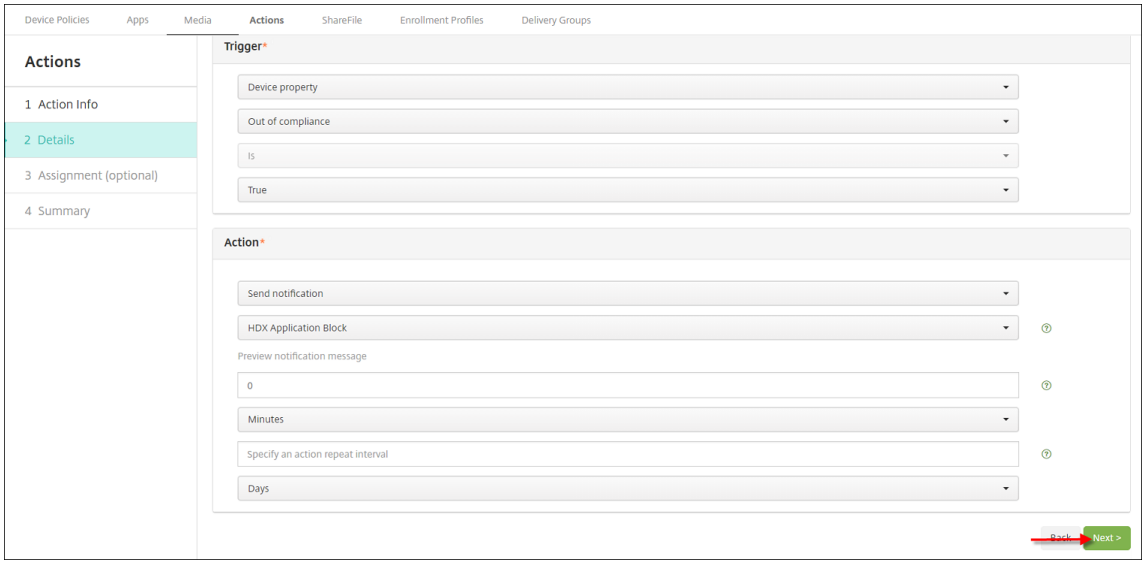


6. 单击保存。

创建当设备标记为不合规时用于发送通知的操作

1. 在 XenMobile 控制台中，单击配置 **>** 操作。此时将显示操作页面。
2. 单击添加以添加操作。此时将显示操作信息页面。

3. 在操作信息页面上，输入操作的名称和说明：
   - 名称： HDX 阻止了通知
   - 说明：由于设备不合规，HDX 阻止了通知
4. 单击 **Next**（下一步）。此时将显示操作详细信息页面。
5. 在触发器列表中：
   - 选择设备属性。
   - 选择不合规。
   - 选择是。
   - 选择 **True**。



6. 在操作列表中，指定满足触发条件时发生的操作：
   - 选择发送通知
   - 选择 **HDX Application Block, the notification you created**（HDX 应用程序阻止，您创建的通知）
   - 选择 **0**。将此值设置为 0 会导致通知在满足触发条件时立即发送。
7. 选择要应用此操作的一个或多个 XenMobile 交付组。在此示例中，请选择 **AllUsers**。
8. 检查操作的摘要。
9. 单击下一步，然后单击保存。

有关设置自动化操作的详细信息，请参阅自动化操作。

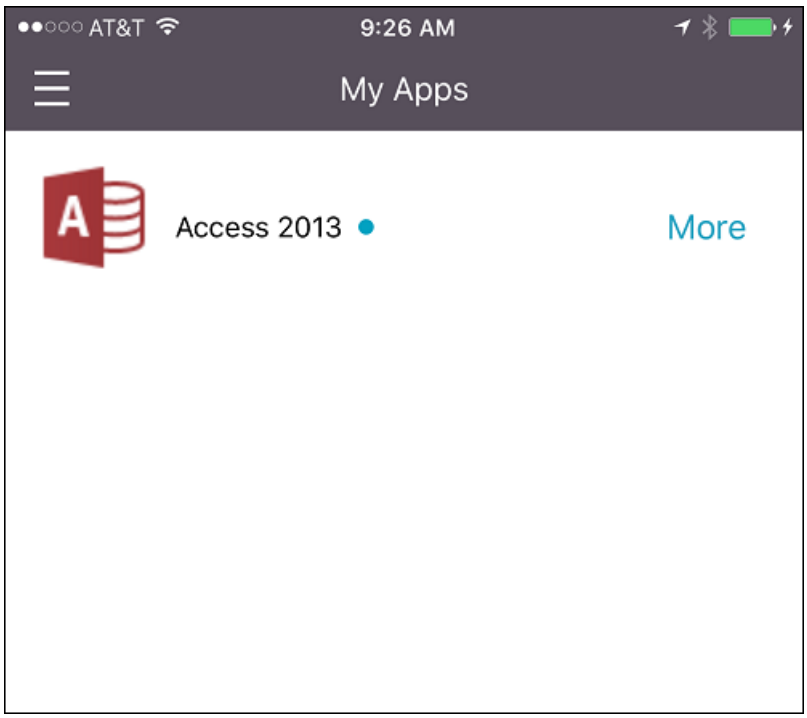
用户如何重新获取对 **HDX** 应用程序的访问权限

用户可以在设备恢复合规后再次获取对 HDX 应用程序的访问权限：

1. 在设备上，转至 Secure Hub 应用商店以刷新应用商店中的应用程序。

2. 转至该应用程序并轻按添加以添加该应用程序。

添加后，该应用程序将在“我的应用程序”中显示，旁边带有一个蓝点，因为这是新安装的应用程序。



添加媒体

December 10, 2020

可以向 XenMobile 中添加媒体，以便您能够向用户设备部署媒体。可以使用 XenMobile 部署您通过 Apple 批量购买获取的 Apple Books。

在 XenMobile 中配置批量购买帐户后，您购买的书籍以及免费书籍将显示在配置 **>** 媒体中。从媒体页面中，可以通过选择交付组并指定部署规则来配置书籍在 iOS 设备中的部署。

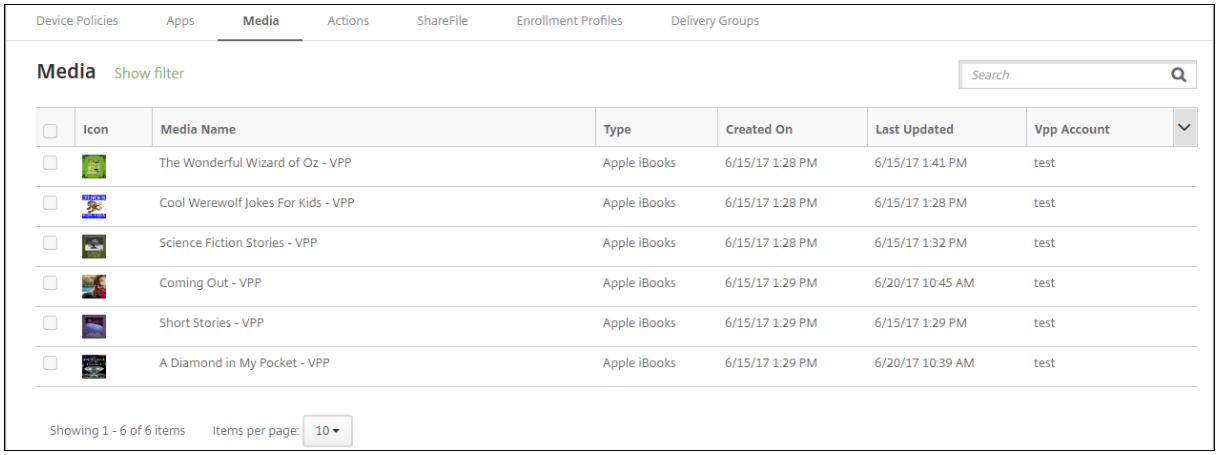
用户首次收到书籍并接受批量购买许可证时，已部署的书籍将在设备上安装。这些书籍将在 Apple 书籍应用程序中显示。不能取消书籍许可证与用户的关联，也不能从设备中删除书籍。XenMobile 安装书籍作为必需媒体。如果用户从其设备中删除了已安装的书籍，该书籍仍保留在 Apple 书籍应用程序中，可随时下载。

必备条件

- iOS 设备
- 在 XenMobile 中配置 Apple 批量购买，如 Apple 批量购买中所述。

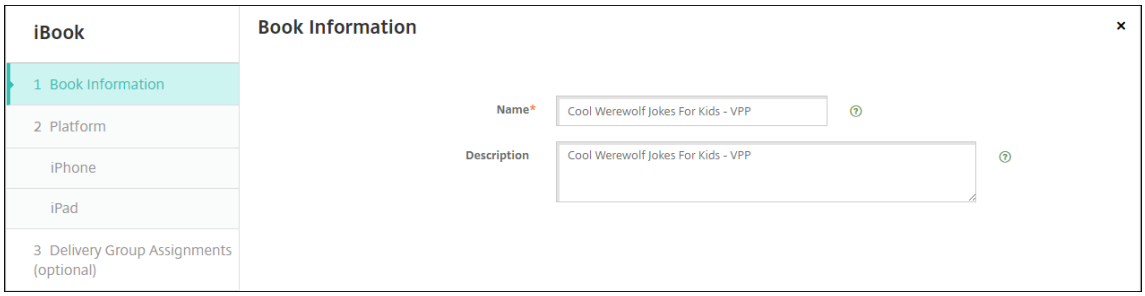
配置书籍

通过批量购买获取的 Apple Books 显示在配置 **>** 媒体页面上。



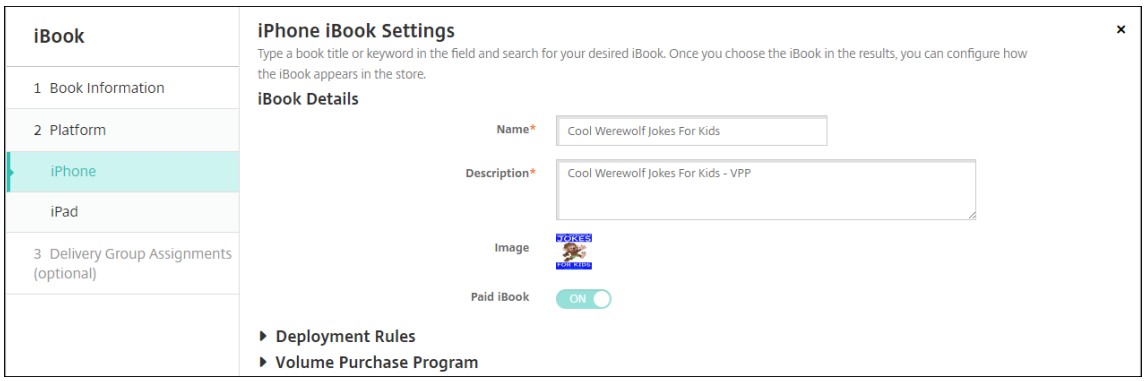
配置要部署的 **Apple** 书籍

1. 在配置 **>** 媒体中，选择一本图书并单击编辑。此时将显示书籍信息页面。

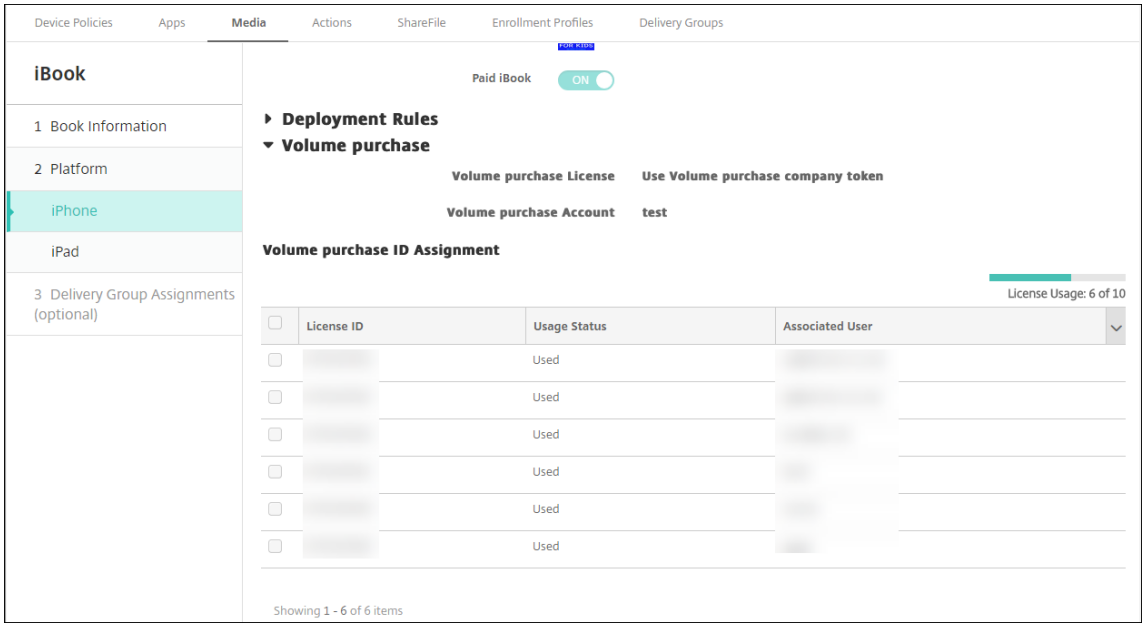


   名称和说明仅显示在 XenMobile 控制台和日志中。

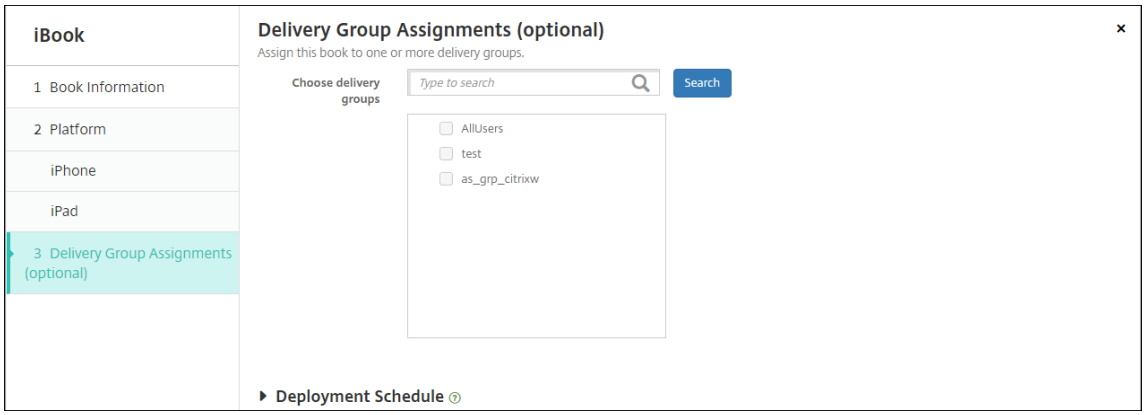
2. 在 **iPhone iBook** 设置和 **iPad iBook** 设置页面中：虽然您可以选择更改书籍名称和说明，但 Citrix 建议您不要更改这些设置。图片仅供参考，不可编辑。**Paid iBook** 指示书籍是通过 Apple 批量购买购买的。



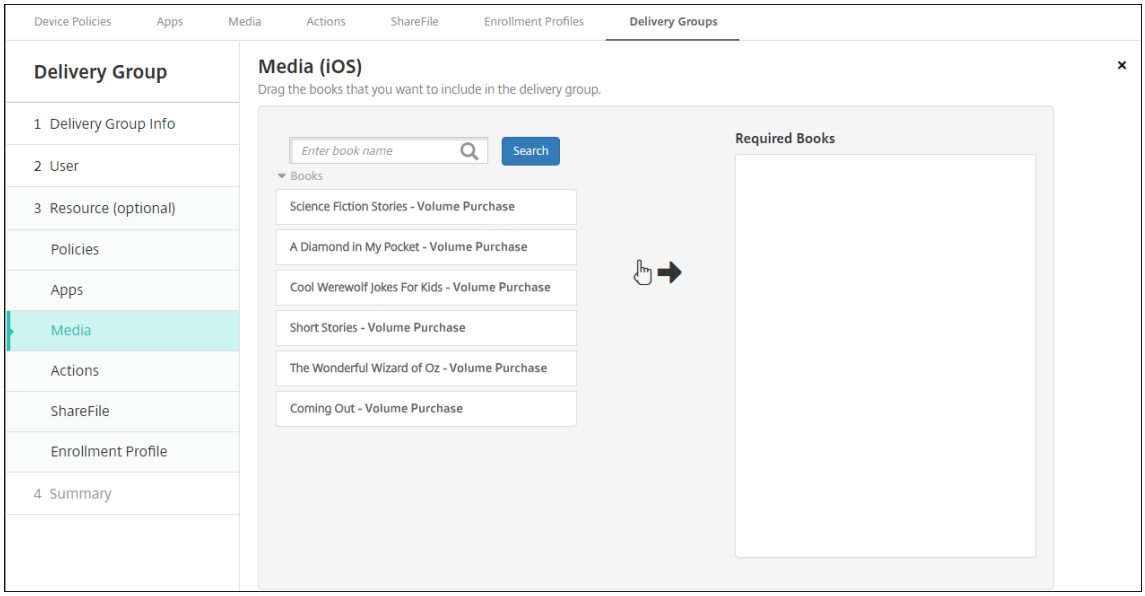
   还可以指定部署规则或查看批量购买信息。



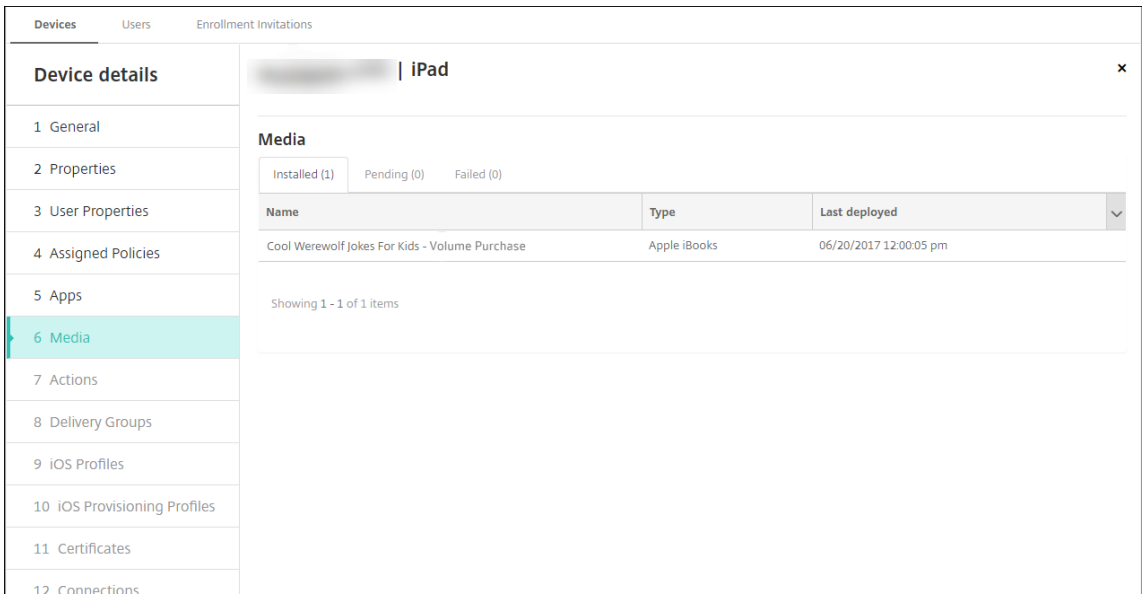
3.（可选）将书籍分配给部署组并设置部署计划。



还可以从配置 **>** 交付组的媒体选项卡将书籍分配给交付组。XenMobile 仅支持所需的书籍部署。

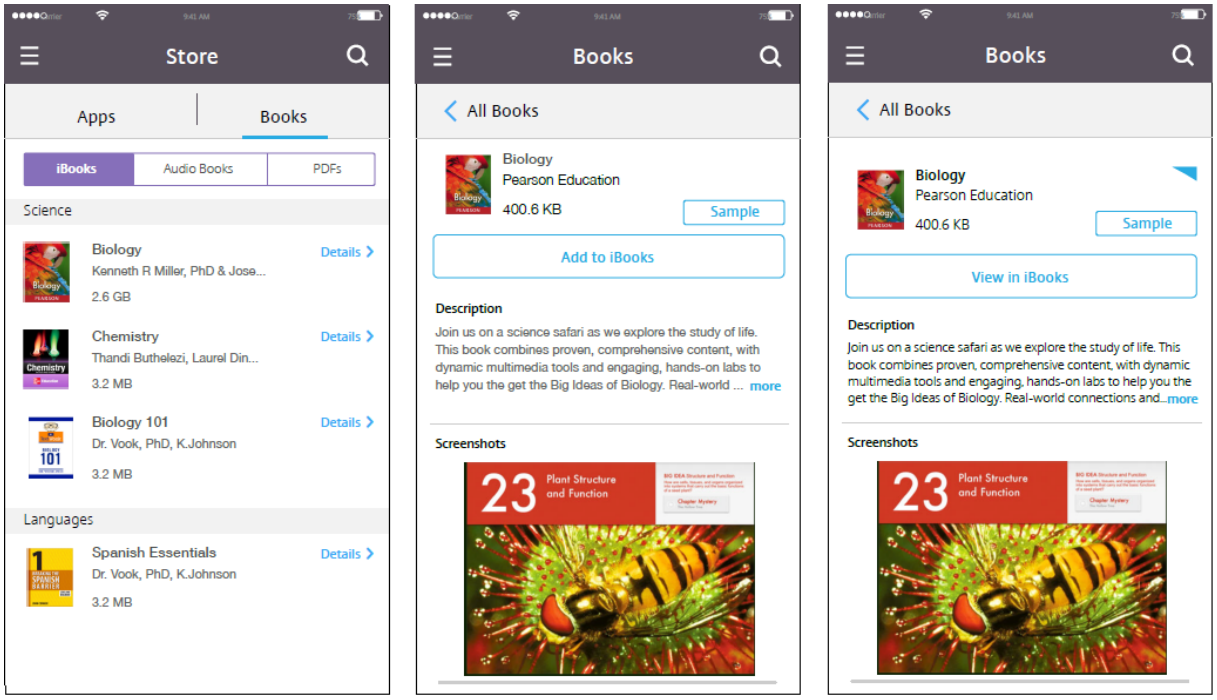


4. 使用管理 > 设备的媒体选项卡可查看部署状态。



> 注意：
>
> 在配置 > 媒体页面上，如果您选择某本书籍并单击删除，XenMobile 将从列表中删除该书籍。但是，XenMobile 下次与 Apple 批量购买同步时，除非已将其从 Apple 批量购买中删除，否则该书籍会在列表中重新出现。从列表中删除某本书籍不会将其从设备中删除。

书籍显示在用户设备上，如以下示例所示。



部署资源

January 5, 2022

在设备配置和管理过程中，通常需在 XenMobile 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。XenMobile 将交付组中的资源和操作推送到设备的顺序称为部署顺序。本文介绍了如何执行以下操作：

- 添加、管理和部署交付组
- 更改交付组中资源的部署顺序和操作。
- XenMobile 决定当用户位于多个具有重复或冲突策略的交付组中时的部署顺序。

交付组指定您向其设备部署策略、应用程序、媒体和操作组合的用户类别。交付组中包含的内容通常取决于用户的特征，例如公司、国家/地区、部门、办公地址和职务。利用交付组可以很好地控制哪些人可以访问哪些资源以及访问时间。可以针对每个人部署交付组，也可以针对严格定义的用户组部署交付组。

部署到某个交付组意味着向使用受支持的 iOS 和 Windows 设备的所有用户发送推送通知。这些用户必须属于该交付组才能重新连接到 XenMobile。您可以重新评估属于某个交付组的设备和部署策略、应用程序、媒体以及操作。

对于使用 Android 设备的用户：如果已连接，用户会立即收到资源。否则，根据其计划策略，用户将在下次连接时收到资源。

安装和配置 XenMobile 时会创建默认的 AllUsers 交付组。它包含所有本地用户和 Active Directory 用户。您无法删除 AllUsers 组，但是，如果您不希望向所有用户推送资源，可以禁用此组。

部署顺序

部署顺序是指 XenMobile 向设备推送资源的顺序。部署顺序仅适用于交付组中具有为设备管理 (MDM) 配置的注册配置文件的设备。

在确定部署顺序时，XenMobile 将对资源应用过滤器和控制标准，例如部署规则和部署计划。资源包括策略、应用程序、操作和交付组。在添加交付组前，请考虑本节信息与您的部署目标的相关性。

下面是有关部署顺序的主要概念的汇总：

- 部署顺序： XenMobile 向设备推送资源（策略、应用程序和媒体）和操作的顺序。某些策略（如条款和条件以及软件清单）的部署顺序对其他资源没有影响。操作的部署顺序对其他资源没有影响，因此，XenMobile 部署资源时会忽略操作的位置。
- 部署规则： XenMobile 使用您为设备属性指定的部署规则来过滤策略、应用程序、媒体、操作和交付组。例如，某个部署规则可能指定当域名与特定值匹配时推送部署软件包。
- 部署计划： XenMobile 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。可以将部署过程指定为立即执行、在特定日期和时间执行或根据部署条件执行。

下表显示了针对各种对象和资源类型的过滤和控制条件。部署规则建立在设备属性的基础之上。

对象/资源	设备平台	部署规则	部署计划	用户/组
设备策略	Y	Y	Y	-
应用程序	Y	Y	Y	-
媒体	Y	Y	Y	-
操作	-	Y	Y	-
交付组	-	Y	-	Y

在典型的环境中，很可能会将多个交付组分配给单个用户，这将产生以下可能结果：

- 交付组中存在重复的对象。
- 在分配给一个用户的多个交付组对某特定策略进行不同的配置。

当发生任一情况时，XenMobile 将为必须交付到设备的所有对象计算部署顺序，或者按顺序进行操作。计算步骤独立于设备平台。

计算步骤

1. 根据用户、组和部署规则的过滤器确定特定用户的所有交付组。
2. 创建选定交付组中所有资源（策略、应用程序、媒体和操作）的有序列表。该列表建立在设备平台、部署规则和部署计划的过滤器的基础之上。排序算法如下所述：

a) 请将交付组中具有用户定义的部署顺序的资源放置在交付组中不具有此类部署顺序的资源之前。此放置方法的理由将在这些步骤后的内容中说明。

b) 作为交付组之间的一个决定项，按交付组名称对交付组中的资源排序。例如，请将交付组 A 中的资源放置在交付组 B 中的资源之前。

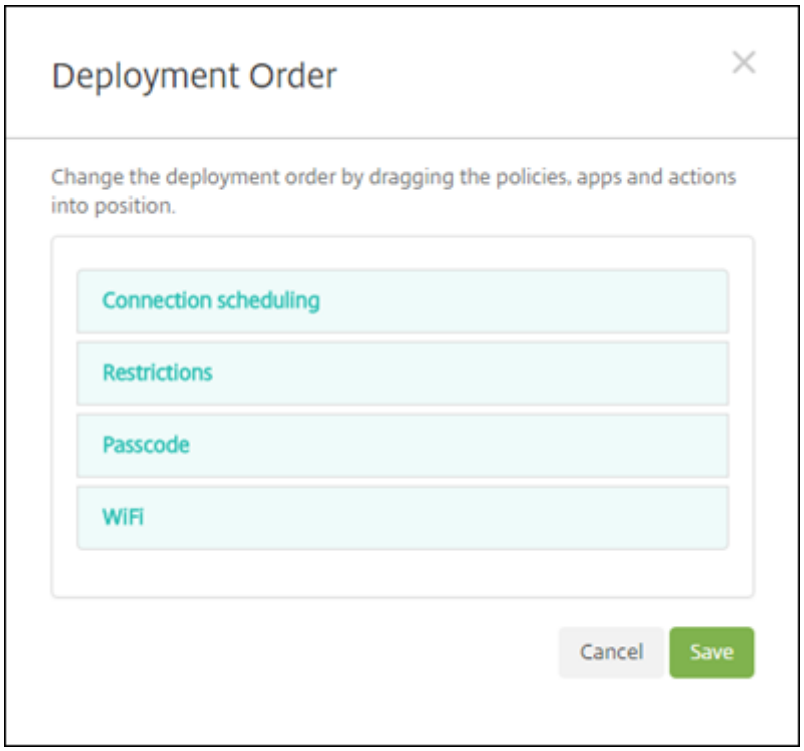
c) 在排序时，如果为交付组的资源指定了用户定义的部署顺序，将保持该顺序。否则，按资源名称对交付组内的资源进行排序。

d) 如果同一个资源出现多次，则删除重复的资源。

已与用户定义的顺序关联的资源将先于不具备此类顺序的资源进行部署。一个资源可位于被分配给用户的多个交付组中。如上述步骤中所述，计算算法会删除冗余的资源，只交付此列表中的第一个资源。删除重复资源后，XenMobile 会实施 XenMobile 管理员定义的顺序。

例如，假设您具有如下两个交付组：

- 交付组 Account Managers 1：资源顺序未指定。包含 **WiFi** 和通行码策略。
- 交付组 Account Managers 2：资源顺序已指定。包含连接计划、限制、通行码和 **WiFi** 策略。在此示例中，您想要在交付 **WiFi** 策略之前先交付通行码策略。



如果计算算法仅按名称对部署组进行排序，XenMobile 将按此顺序执行部署，首先部署交付组 Account Managers 1：**WiFi**、通行码、连接计划和限制。XenMobile 将忽略 Account Managers 2 交付组中的通行码和 **WiFi**，这两者都是重复策略。

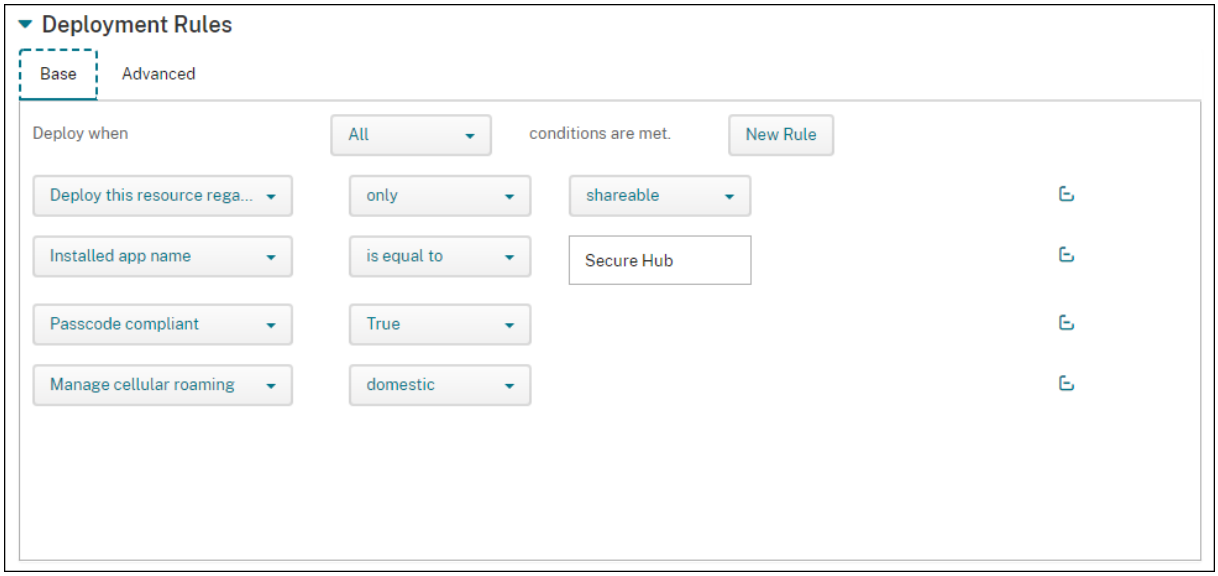
但是，Account Managers 2 组具有用户指定的部署顺序。因此，计算算法会将 Account Managers 2 交付组中的资源放置在列表中其他交付组中的资源之前。因此，XenMobile 按以下顺序部署策略：连接计划、限制、通行码和 **WiFi**

策略。XenMobile 将忽略 Account Managers 1 交付组中的 **WiFi** 和通行码策略，因为它们是重复策略。因此，该算法采用由 XenMobile 管理员指定的顺序。

部署规则

将部署规则配置为仅在存在特定条件时交付资源。可以配置基本部署规则或高级部署规则。

使用基本编辑器添加部署规则时，首先选择何时部署资源。

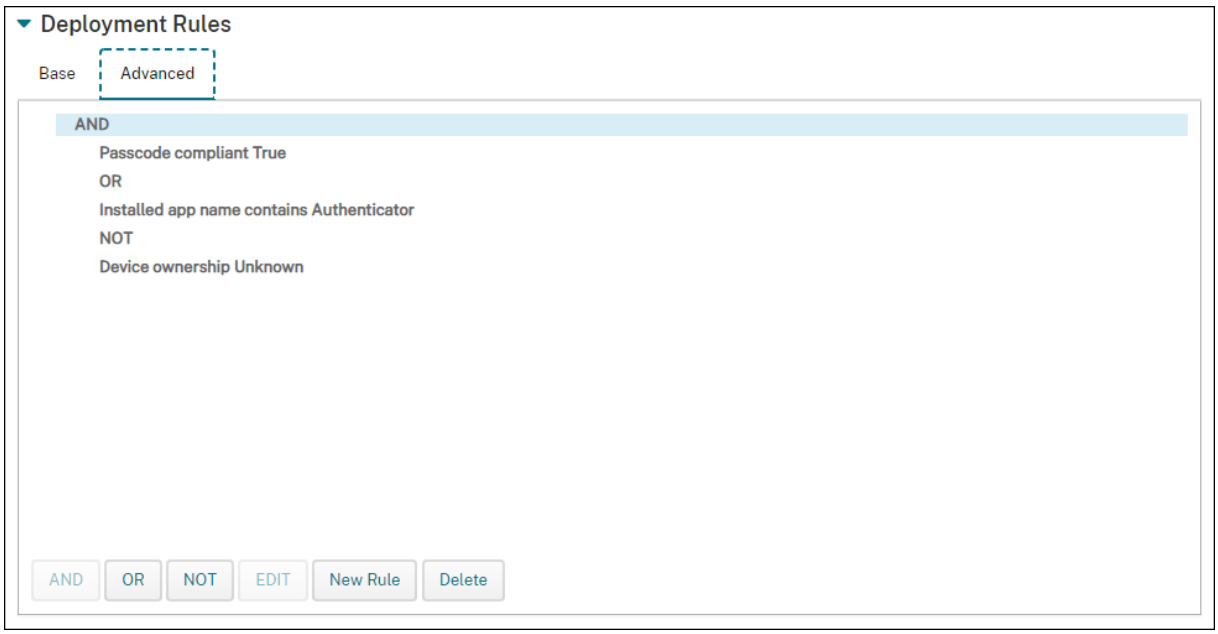


- 全部：当用户或设备满足您配置的所有条件时交付资源。
- 任何：当用户或设备至少满足您配置的一个条件时交付资源。

单击新建规则添加条件。规则因所部署的资源和为其配置资源的平台而异。存在几种类型的规则。可以选择部署资源：

- 仅当选定的属性存在时或选定的属性存在时除外。
- 当属性与您键入的文本完全匹配时，属性将包含您键入的文本，或者属性与您键入的文本不匹配。
- 当设备或用户符合您选择的属性或不符合您选择的属性时。
- 当设备或用户属性与您从预定义列表中选择的条件匹配时。

使用高级编辑器创建更复杂的部署规则。存在更多可供选择的规则，在创建高级规则时，您可以组合不同的布尔逻辑运算符。

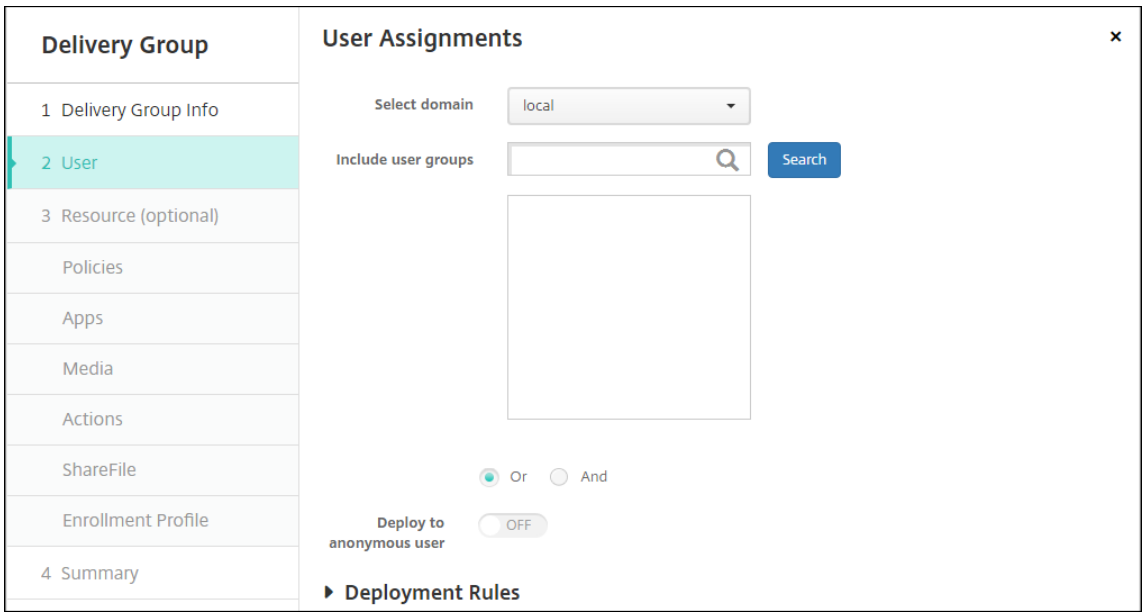


添加交付组

Citrix 建议在创建设备策略和注册配置文件之前创建交付组。

1. 在控制台中，单击配置 **>** 交付组。
2. 在交付组页面上，单击添加。
3. 在交付组信息页面中，键入交付组的名称和说明，然后单击下一步。

   如果用户属于具有不同注册配置文件的多个交付组，该交付组的名称决定使用的注册配置文件。XenMobile 选择按字母顺序排列的交付组列表中最后显示的交付组。有关详细信息，请参阅注册配置文件。
4. 在用户分配页面上，指定如何管理交付组用户分配。



> 重要：
>
> 创建用户组后，不能更改管理用户分配设置。

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

  要从选定用户组列表中删除某个用户组，请执行以下操作之一：

  - 在选定用户组列表中，单击要删除的每个组旁边的 **X**。
  - 单击搜索以查看选定域中所有用户组的列表。滚动列表，并取消选中要删除的各个组旁边的复选框。
  - 在搜索框中键入完整或部分组名称，然后单击搜索以限制用户组列表。滚动列表，并取消选中要删除的各个组旁边的复选框。
- 或/与：选择用户是位于任意组（或）即可，还是必须位于所有组中（与），才能向其部署资源。
- 部署到匿名用户：选择是否部署到交付组中未经身份验证的用户。未经身份验证的用户是指您无法对其进行身份验证、但仍允许其设备与 XenMobile 进行连接的用户。

5. 配置部署规则。
6. 单击 **Next**（下一步）。此时将显示交付组资源页面。您可以在此处选择为交付组添加策略、应用程序或操作。要跳过此步骤，请在交付组下方，单击摘要以查看交付组配置的摘要。

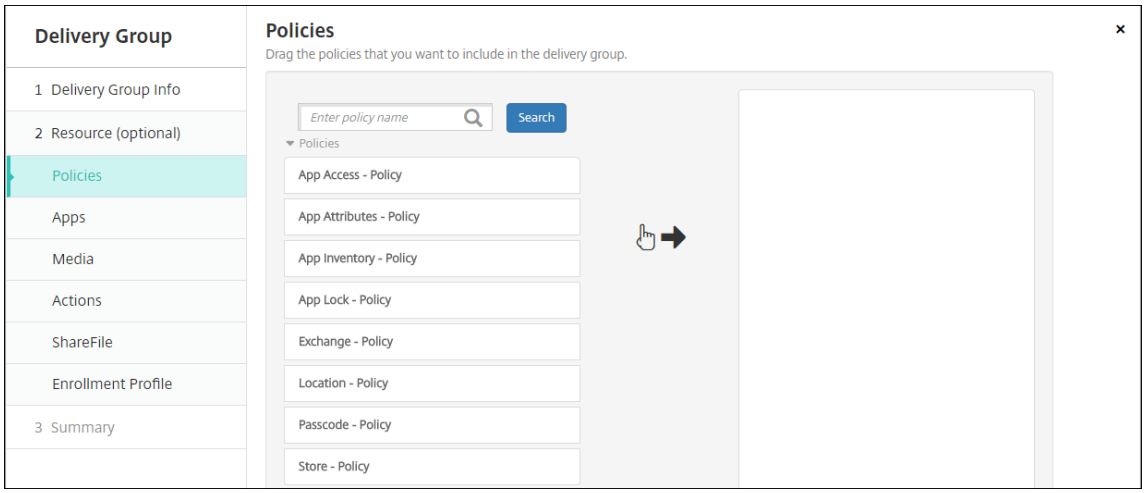
   要跳过某项资源，请在 **Resources (optional)**（资源 (可选)）下方，单击要添加的资源，并按照适用于该资源的步骤操作。

添加策略

1. 对于要添加的每个策略，执行以下操作之一：

   - 滚动可用策略的列表以查找要添加的策略。
   - 或者，要限制策略列表，请在搜索框中键入完整或部分策略名称，然后单击搜索。
   - 单击要添加的策略并将其拖动到右侧的框中。

   要删除策略，请单击右侧框中策略名称旁边的 **X**。



2. 单击 **Next**（下一步）。此时将显示应用程序页面。

添加应用程序

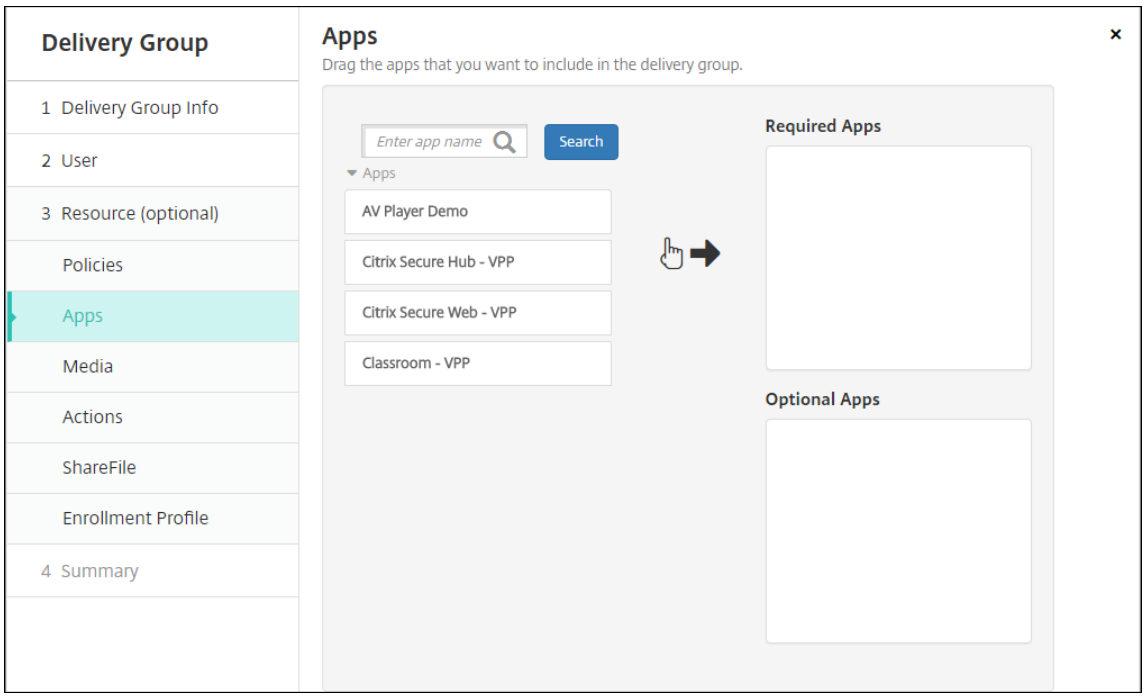
1. 对于要添加的每个应用程序，执行以下操作之一：

   - 滚动可用应用程序的列表以查找要添加的应用程序。
   - 或者，要限制应用程序列表，请在搜索框中键入完整或部分应用程序名称，然后单击搜索。
   - 单击要添加的应用程序，将其拖动到必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，用户在诸如以下情况下能够立即收到更新：

   - 上载新应用程序并根据需要对其进行标记。
   - 根据需要标记现有应用程序。
   - 用户删除所需的应用程序。
   - Secure Hub 更新可用。

   有关必需应用程序的强制部署的信息（包括如何启用该功能），请参阅关于必需应用程序和可选应用程序。

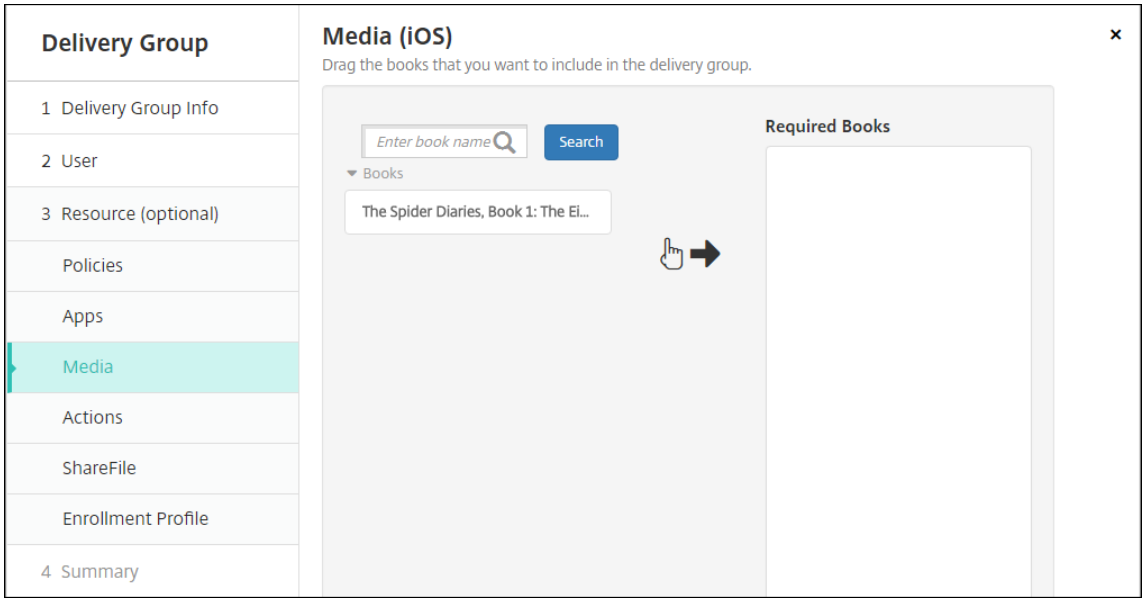


要删除应用程序，请单击右侧框中应用程序名称旁边的 **X**。

2. 单击 **Next**（下一步）。此时将显示媒体页面。

添加媒体

1. 对于要添加的每本书籍，执行以下操作：
   - 滚动浏览可用书籍的列表以查找要添加的书籍。
   - 或者，要限制书籍列表，请在搜索框中键入完整或部分书籍名称，然后单击搜索。
   - 单击要添加的书籍并将其拖动到必选书籍框中。



对于标记为必选的书籍，用户在诸如以下情况下将立即收到更新：

- 上载新书籍并根据需要对其进行标记。
- 根据需要标记现有书籍。
- 用户删除所需的书籍。
- Secure Hub 更新可用。

要删除书籍，请单击右侧框中应用程序名称旁边的 **X**。

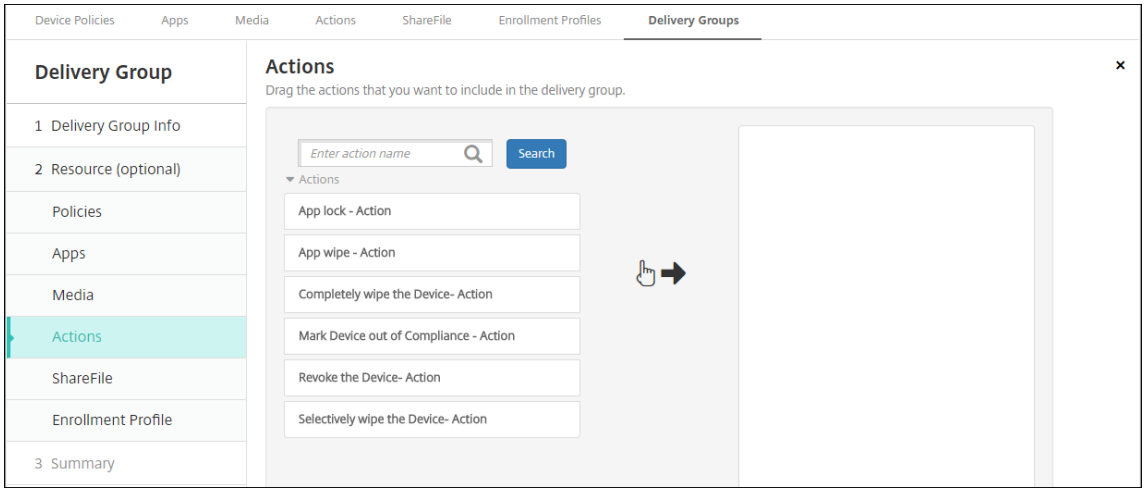
2. 单击 **Next**（下一步）。此时将显示操作页面。

添加操作

1. 对于要添加的每个操作，执行以下操作：

   - 滚动可用操作的列表以查找要添加的操作。
   - 或者，要限制操作列表，请在搜索框中键入完整或部分操作名称，然后单击搜索。
   - 单击要添加的操作并将其拖动到右侧的框中。

   要删除操作，请单击右侧框中操作名称旁边的 **X**。

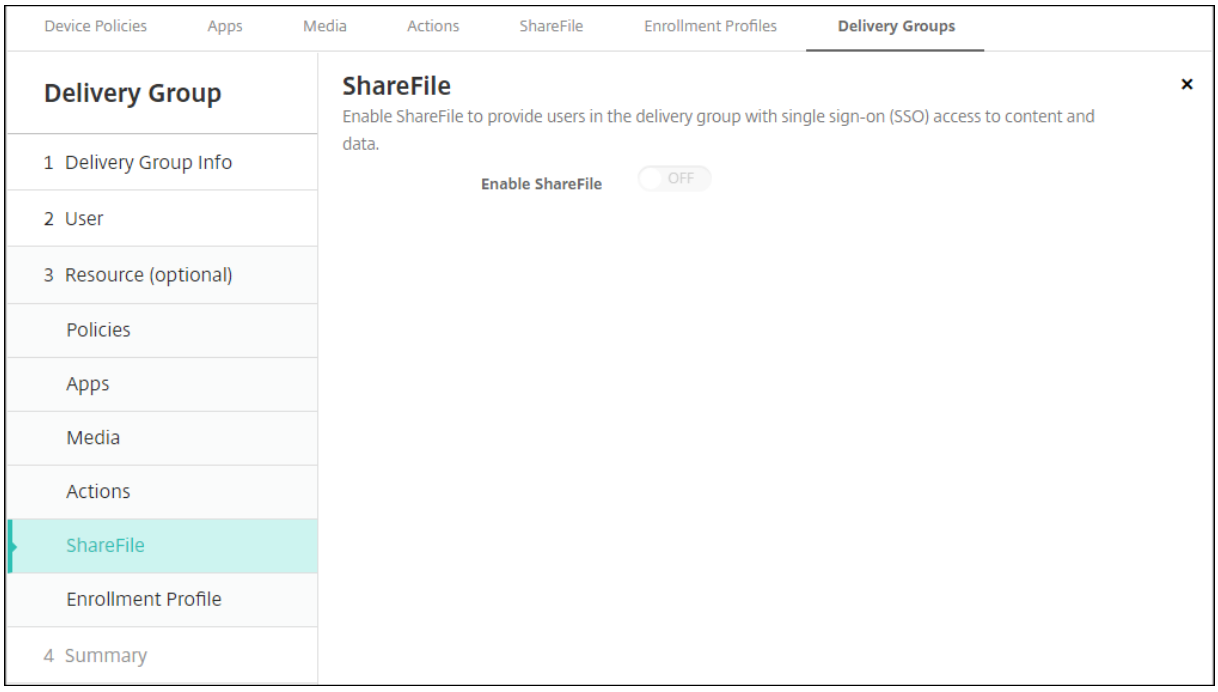


2. 单击 **Next**（下一步）。此时将显示 **ShareFile** 页面。

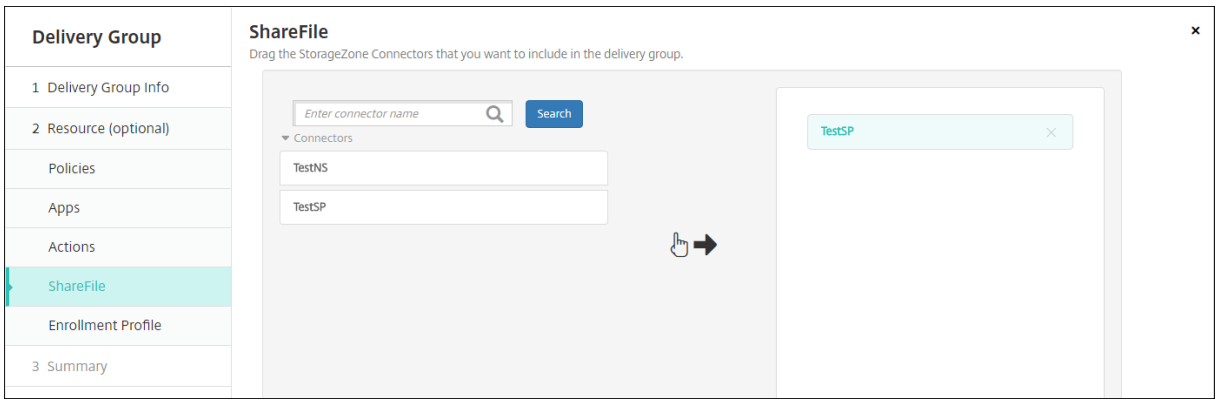
应用 **Content Collaboration** 配置

根据您是否为 Enterprise 帐户或 StorageZone 连接器配置了 XenMobile（配置 **> ShareFile**），Content Collaboration 页面有所差别。

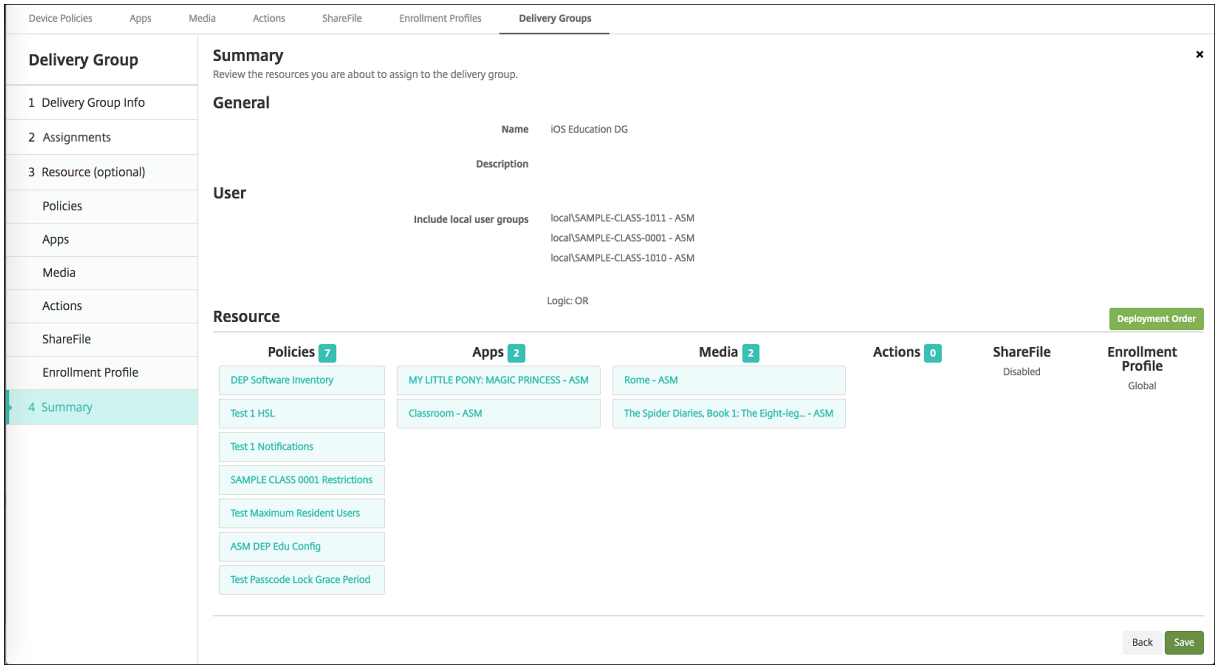
如果您将 Enterprise 帐户配置为与 XenMobile 结合使用：请将启用 **ShareFile** 设置为开以提供对 Content Collaboration 内容和数据的交付组单点登录访问。



如果您将存储区域连接器配置为与 XenMobile 结合使用，请选择要包括在交付组中的存储区域连接器。

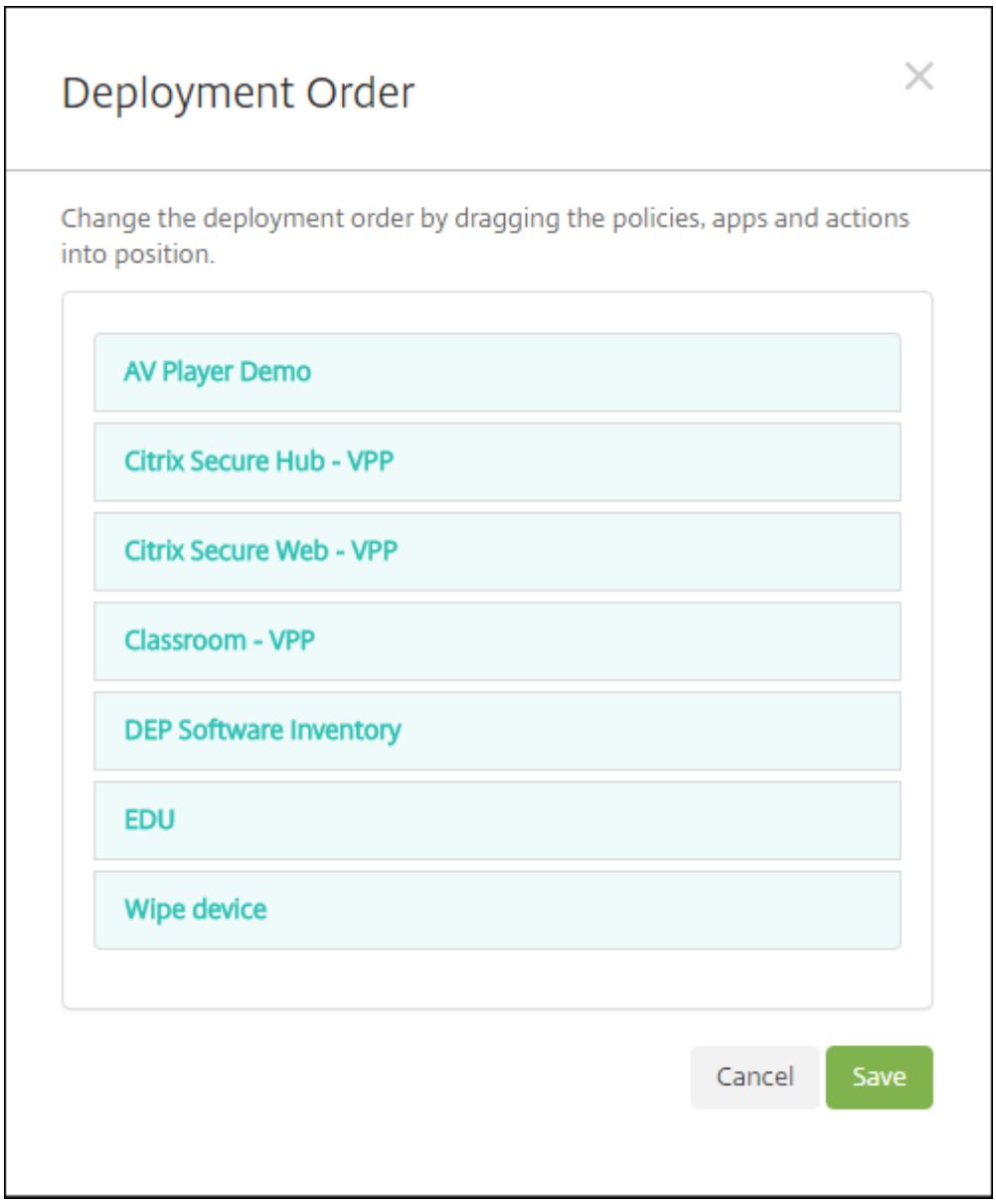


检查已配置的选项并更改部署顺序



在摘要页面上，可以查看为交付组配置的选项以及更改资源的部署顺序。“摘要”页面按类别显示您的资源。“摘要”页面不反映部署顺序。

1. 单击上一步返回到上一个页面，对配置进行必需的调整。
2. 单击部署顺序查看部署顺序或对部署顺序重新排序。此时将显示部署顺序对话框。



3. 单击某个资源并将其拖动到您希望部署此资源的位置。更改部署顺序后，XenMobile 按照从上到下的顺序部署列表中的资源。
4. 单击保存以保存部署顺序。
5. 单击保存以保存交付组。

编辑交付组

不能更改现有交付组的名称。要更新其他设置，请转至配置 **>** 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 是唯一一个您可以启用或禁用的交付组。

在交付组页面上，选中 **AllUsers** 旁边的复选框或单击包含 AllUsers 的行，以选择 “AllUsers” 交付组。然后执行以下操作之一：

- 单击禁用可禁用 AllUsers 交付组。此命令仅在已启用 AllUsers（默认）时才可用。禁用的交付组将显示在交付组表中的已禁用标题下方。
- 单击启用可启用 AllUsers 交付组。此命令仅在禁用了 AllUsers 时才可用。禁用的交付组不再显示在交付组表中的已禁用标题下方。

部署交付组

部署到某个交付组意味着向该使用 iOS、Windows Phone 和 Windows Tablet 设备的用户发送推送通知。这些用户必须属于该交付组才能重新连接到 XenMobile。这样，您就可以重新评估设备以及部署应用程序、策略和操作。

对于使用其他平台设备的用户：如果这些设备已连接到 XenMobile，用户会立即收到资源。否则，根据其计划策略，用户将在下次连接时收到资源。

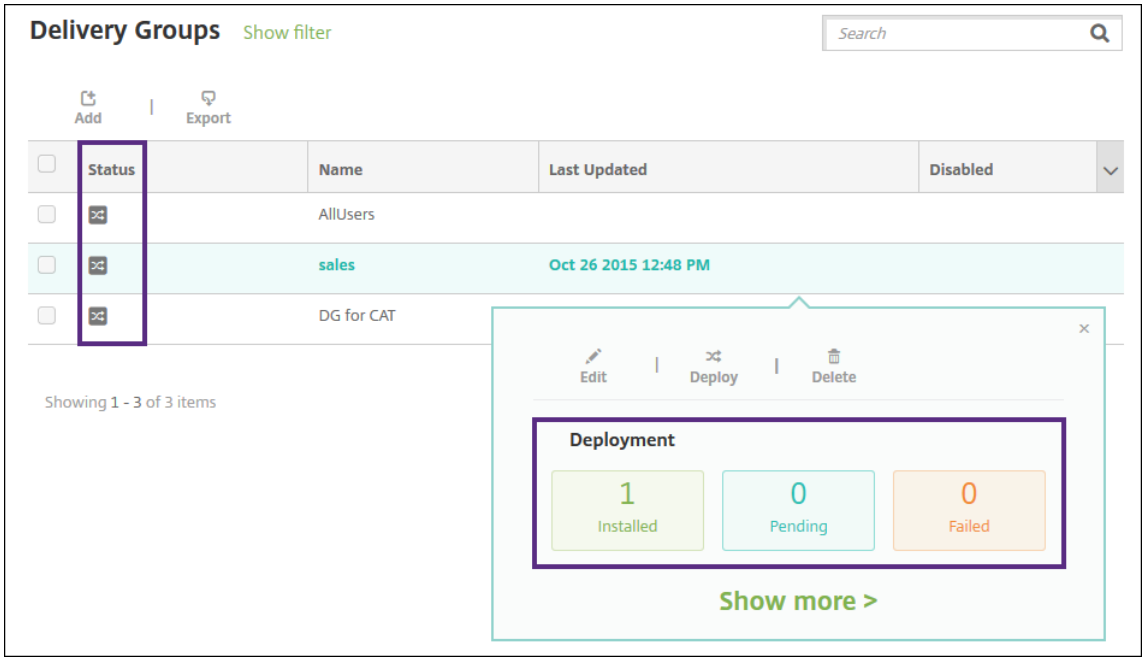
要使更新后的应用程序显示在 Android 设备上 XenMobile Store 中的 “Updated Available”（更新可用）列表中：请先向用户设备部署应用程序清单策略。

1. 在交付组页面上，执行以下操作之一：
   - 要同时部署多个交付组，请选中要部署的组旁边的复选框。
   - 要部署单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。
2. 单击部署。

   根据您选择单个交付组的方式，部署命令将显示在交付组的上方或右侧。

   确认列出了要向其部署应用程序、策略和操作的组，然后单击部署。将根据设备平台和计划策略向选定的组部署应用程序、策略和操作。

   可以通过以下方式之一在交付组页面上检查部署状态。
   - 查看状态标题下方交付组的部署图标，此图标指示任何部署失败状态。
   - 单击包含交付组的行，以显示一个指示已安装、待定和失败部署的叠加项。



删除交付组

您无法删除 AllUsers 交付组，但是，如果您不希望向所有用户推送资源，可以禁用此组。

1. 在交付组页面上，执行以下操作之一：
   - 要同时删除多个交付组，请选中要删除的组旁边的复选框。
   - 要删除单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。
2. 单击删除。此时将显示删除对话框。

   根据您选择单个交付组的方式，删除命令将显示在交付组的上方或右侧。

   > 重要：
   >
   > 您不能撤消删除。
3. 单击删除。

导出交付组表

1. 单击交付组表上方的导出按钮。XenMobile 提取交付组表中的信息，并将其转换为.csv 文件。
2. 按照您的浏览器的常规步骤打开或保存.csv 文件。您也可以取消此操作。

宏

January 5, 2022

XenMobile 阻止将宏作为在以下项目的文本字段中填充用户或设备属性数据的方式：

- 策略
- 通知
- 注册模板
- 自动化操作
- 凭据提供程序证书签名请求

XenMobile 将宏替换为相应的用户或系统值。例如，可以为涵盖数千个用户的单个 Exchange 配置文件中的某个用户预填充邮箱值。

宏语法

宏可以采用以下格式：

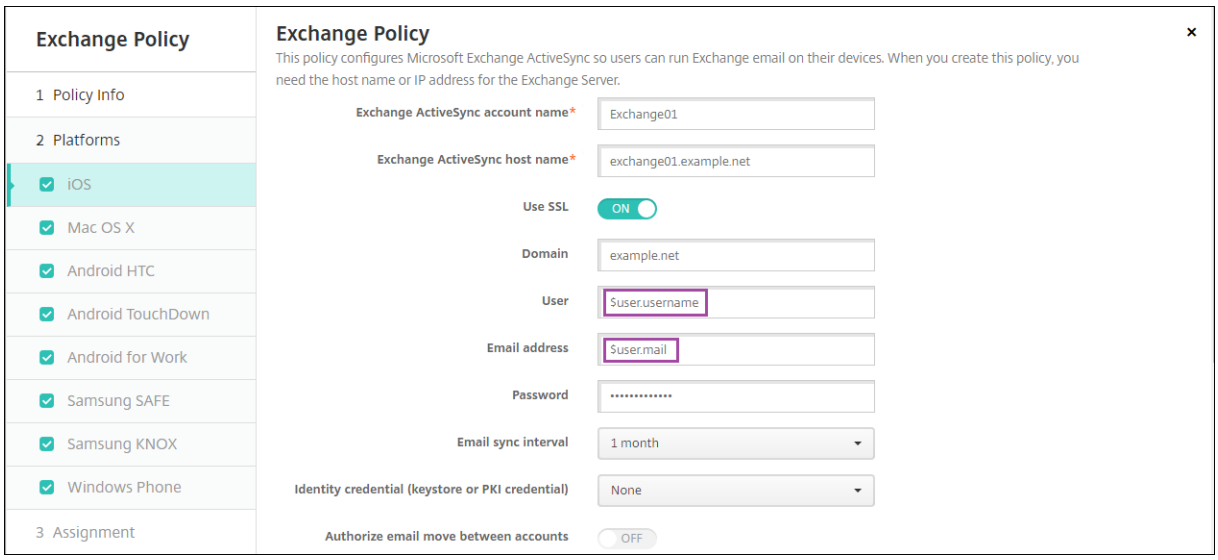
- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

美元符号 ($) 后的所有语法以花括号 ({ }) 括起。

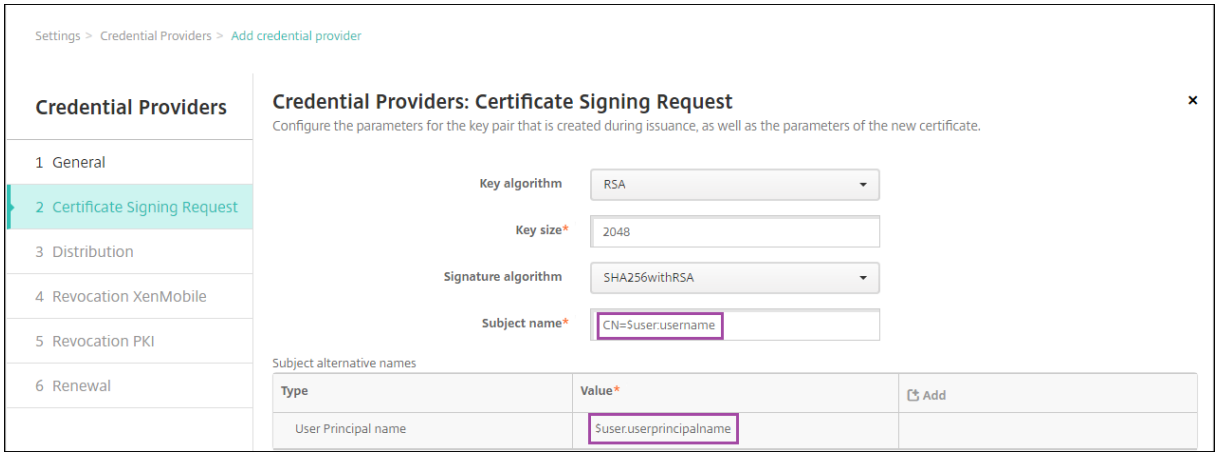
- 限定的属性名称是指用户属性、设备属性或自定义属性。
- 限定的属性名称包括一个前缀，后跟实际属性名称。
- 用户属性的格式为 `${ user.[PROPERTYNAME] (prefix="user.")}`。
- 设备属性的格式为 `${ device.[PROPERTYNAME] (prefix="device.")}`。
- 属性名称区分大小写。
- 函数可以是受限列表，或者指向用于定义函数的第三方引用的链接。以下适用于通知消息的宏包括函数 **firstnotnull**：

  设备 `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 已被阻止...
- 对于自定义宏（您定义的属性），前缀为 `${ custom }`。您可以忽略前缀。

下面是用于在策略的文本字段中填充用户名值的常用宏 `${ user.username }` 的示例。此宏在配置由多个用户使用的 Exchange ActiveSync 配置文件和其他配置文件时非常有用。以下示例显示了如何在 Exchange 策略中使用宏。适用于用户的宏为 **`${ user.username }`**。电子邮件地址的宏为 **`${ user.mail }`**。

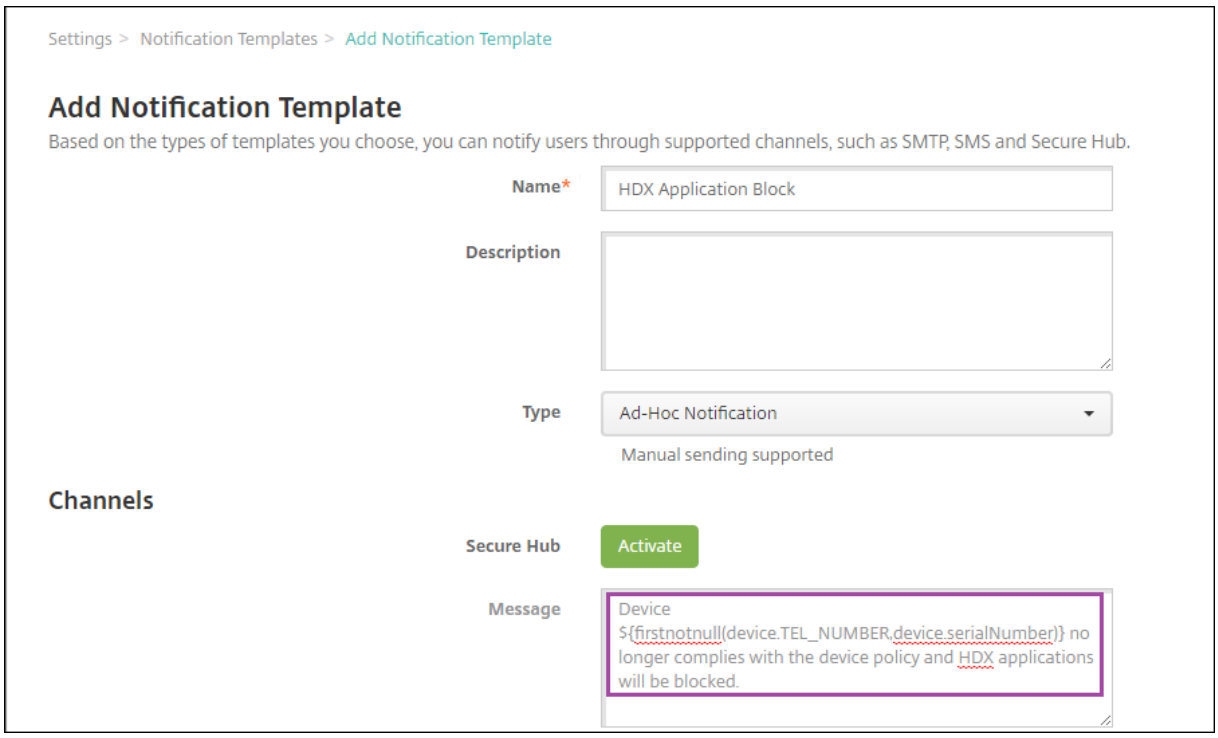


以下示例显示了如何为证书签名请求使用宏。适用于使用者名称的宏为 **CN=$user.username**。适用于使用者备用名称的值的宏为 **$user.userprincipalname**。



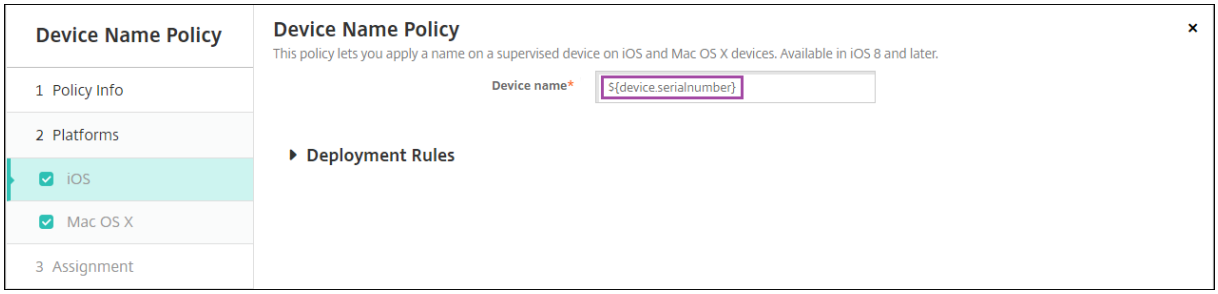
以下示例显示了如何在通知模板中使用宏。示例模板定义阻止 HDX 应用程序时由于不合规设备而向用户发送的消息。适用于消息的宏为：

设备 `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 不再符合设备策略，HDX 应用程序将被阻止。



有关在通知中使用的宏的更多示例，请转至设置 > 通知模板，选择一个预定义的模板，然后单击编辑。

以下示例显示了“设备名称”设备策略中的宏。可以键入宏、宏的组合或宏和文本的组合，为每个设备设置唯一名称。例如，使用 `${ device.serialnumber }` 可将设备名称设置为每个设备的序列号。使用 `${ device.serialnumber } ${ user.username }` 可在设备名称中包含用户名。设备名称设备策略适用于受监督的 iOS 和 macOS 设备。



适用于默认通知模板的宏

可以在默认通知模板中使用以下宏：

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`

- ${ enrollment.pin }
- ${ enrollment.url }
- ${ enrollment.urls }
- ${ enrollment.ios.url }
- ${ enrollment.macos.url }
- ${ enrollment.android.url }
- ${ enrollment.ios.platform }
- ${ enrollment.macos.platform }
- ${ enrollment.android.platform }
- ${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}
- ${ firstnotnull(device.TEL_NUMBER,user.mobile)}
- ${ outofcompliance.reason(smg_block)}
- ${ outofcompliance.reason(whitelist_blacklist_apps_name)}

  > 注意：
  >
  > XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

适用于特定策略的宏

对于设备名称设备策略（适用于 iOS 和 macOS），可以对设备名称使用以下宏：

- ${ device.serialnumber }
- ${ user.username } @example.com
- ${ device.serialnumber }
- ${ device.serialnumber }
- ${ user.username }
- ${ enrollment.pin }
- ${ user.dnsroot }

对于 Web 剪辑设备策略，可以对 **URL** 使用以下宏：

- `${ webeas-url }`

对于 Samsung MDM 许可证密钥设备策略，可以对 **ELM** 许可证密钥使用以下宏：

- `${ elm.license.key }`

用于获取内置设备属性的宏

显示名称	宏
设备 ID	`$device.id`
设备 GUID	`$device.uniqueid`
设备 IMEI	`$device.imei`
操作系统系列	`$device.OSFamily`
序列号	`$device.serialNumber`

适用于所有设备属性的宏

下表列出了显示名称、Web 元素和宏。

帐户已暂停?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED

激活锁绕过码

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE

已启用激活锁

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED

活动 iTunes 帐户

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

MSP 已知的 ActiveSync 设备

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP

ActiveSync ID

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID

已禁用管理员

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED

AIK 是否存在?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT

Amazon MDM API 可用

- AMAZON_MDM
- ${device.AMAZON_MDM

Android Enterprise 设备 ID

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID

启用了 Android Enterprise 的设备?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE

Android Enterprise 安装类型

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE

反间谍软件签名状态

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS

反间谍软件状态

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS

防病毒软件签名状态

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS

防病毒软件状态

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS

ASM DEP 激活锁绕过码

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE

ASM DEP 托管密钥

- DEP_ESCROW_KEY
- ${device.DEP_ESCROW_KEY

资产标签

- ASSET_TAG
- ${device.ASSET_TAG

自动检查软件更新

- AutoCheckEnabled
- ${device.AutoCheckEnabled

自动在后台下载软件更新

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled

自动安装应用程序更新

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled

自动安装操作系统更新

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled

自动安装安全更新

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled

自动更新状态

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS

可用 RAM

- MEMORY_AVAILABLE
- ${device.MEMORY_AVAILABLE

可用的软件更新

- AVAILABLE_OS_UPDATE_HUMAN_READABLE

- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE

可用存储空间

- FREEDISK
- ${device.FREEDISK

备份电池

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT

基带固件版本

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION

电池充电

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS

电池充电

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING

剩余电池电量

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING

电池运行时

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME

电池状态

- BATTERY_STATUS
- ${device.BATTERY_STATUS

MS 已知的 Bes 设备

- BES_DEVICE_KNOWN_BY_ZMSP
- ${device.BES_DEVICE_KNOWN_BY_ZMSP

BES PIN

- BES_PIN
- ${device.BES_PIN

BES 服务器代理 ID

- AGENT_ID
- ${device.AGENT_ID

BES 服务器名称

- BES_SERVER
- ${device.BES_SERVER

BES 服务器版本

- BES_VERSION
- ${device.BES_VERSION

BIOS 信息

- BIOS_INFO
- ${device.BIOS_INFO

BitLocker 状态

- WINDOWS_HAS_BIT_LOCKER_STATUS
- ${device.WINDOWS_HAS_BIT_LOCKER_STATUS

蓝牙 MAC 地址

- BLUETOOTH_MAC
- ${device.BLUETOOTH_MAC

已启用启动调试?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED

启动管理器修订列表版本

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION

运营商代码

- CARRIER_CODE
- ${device.CARRIER_CODE

运营商设置版本

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION

目录 URL

- CatalogURL
- ${device.CatalogURL

手机网络高度

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR

手机网络路线

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR

手机网络水平精度

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

手机网络纬度

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR

手机网络经度

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR

手机网络速度

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR

手机网络技术

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY

手机网络时间戳

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR

手机网络垂直精度

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

下次登录时更改密码?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

客户端设备 ID

- CLIENT_DEVICE_ID

- ${device.CLIENT_DEVICE_ID

已启用云备份

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED

已启用代码完整性?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED

代码完整性修订列表版本

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION

颜色

- COLOR
- ${device.COLOR

CPU 时钟速度

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED

CPU 类型

- CPU_TYPE
- ${device.CPU_TYPE}

创建时间

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME

关键软件更新

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- ${device.AVAILABLE_OS_UPDATE_IS_CRITICAL

当前运营商网络

- CARRIER
- ${device.CARRIER

当前移动设备国家/地区代码

- CURRENT_MCC
- ${device.CURRENT_MCC

当前移动设备网络代码

- CURRENT_MNC
- ${device.CURRENT_MNC

允许数据漫游

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED

最后一次 iCloud 备份日期

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

默认目录

- IsDefaultCatalog
- ${device.IsDefaultCatalog

DEP 帐户名称

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME

DEP 策略

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY

DEP 配置文件分配时间

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME

DEP 配置文件推送时间

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME

DEP 配置文件删除时间

- PROFILE_REMOVE_TIME
- ${device.PROFILE_REMOVE_TIME

DEP 注册者

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY

DEP 注册日期

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE}

说明

- DESCRIPTION
- ${device.DESCRIPTION

设备标识符

- Activesyncid
- ${device.activesyncid

设备型号

- SYSTEM_OEM
- ${device.SYSTEM_OEM

设备名称

- DEVICE_NAME
- ${device.DEVICE_NAME

设备类型

- DEVICE_TYPE
- ${device.DEVICE_TYPE

已激活“请勿打扰”

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB

已加载 ELAM 驱动程序?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED

加密合规性

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- ${device.ENROLLMENT_KEY_GENERATION_DATE

企业 ID

- ENTERPRISEID
- ${device.ENTERPRISEID

外部存储 1：可用空间

- EXTERNAL_STORAGE1_FREE_SPACE

- ${device.EXTERNAL_STORAGE1_FREE_SPACE

外部存储 1：名称

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME

外部存储 1：总空间

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE

外部存储 2：可用空间

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE

外部存储 2：名称

- EXTERNAL_STORAGE2_NAME
- ${device.EXTERNAL_STORAGE2_NAME

外部存储 2：总空间

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE

已加密外部存储

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION

已启用 FileVault

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED

防火墙状态

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS

防火墙状态

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS

固件版本

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION

首次同步

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC

Google Directory 别名

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS

Google Directory 系列名称

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME

Google Directory 名称

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

Google Directory 主电子邮件

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google Directory 用户 ID

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS 海拔

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS

GPS 路线

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS

GPS 水平精度

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS

GPS 纬度

- GPS_LATITUDE_FROM_GPS
- ${device.GPS_LATITUDE_FROM_GPS

GPS 经度

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS

GPS 速度

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS

GPS 时间戳

- GPS_TIMESTAMP_FROM_GPS
- ${device.GPS_TIMESTAMP_FROM_GPS

GPS 垂直精度

- GPS_VERTICAL_ACCURACY_FROM_GPS
- ${device.GPS_VERTICAL_ACCURACY_FROM_GPS

硬件设备 ID

- HW_DEVICE_ID
- ${device.HW_DEVICE_ID

硬件加密功能

- HARDWARE_ENCRYPTION_CAPS
- ${device.HARDWARE_ENCRYPTION_CAPS

HAS_CONTAINER

- HAS_CONTAINER
- ${device.HAS_CONTAINER

当前登录的 iTunes 应用商店帐户的哈希

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH

主运营商网络

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK

主移动设备国家/地区代码

- SIM_MCC
- ${device.SIM_MCC

主移动设备网络代码

- SIM_MNC
- ${device.SIM_MNC

ICCID

- ICCID

- ${device.ICCID

标识

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY

IMEI/MEID 编号

- IMEI
- ${device.IMEI

IMSI

- SIM_ID
- ${device.SIM_ID

已加密内部存储

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION

IP 位置

- IP_LOCATION
- ${device.IP_LOCATION

IPV4 地址

- IP_ADDRESSV4
- ${device.IP_ADDRESSV4

IPV6 地址

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6

颁发时间

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT

已越狱/获得 Root 权限

- ROOT_ACCESS
- ${device.ROOT_ACCESS

已启用内核调试?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED

Kiosk 模式

- IS_KIOSK
- ${device.IS_KIOSK

上次已知 IP 地址

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR

上次策略更新时间

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME

上次扫描日期

- PreviousScanDate
- ${device.PreviousScanDate

上次扫描结果

- PreviousScanResult
- ${device.PreviousScanResult

上次安排的软件更新

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME

上次安排的软件更新失败消息

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG

上次安排的软件更新状态

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS

上次同步

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC

已启用定位器服务

- DEVICE_LOCATOR
- ${device.DEVICE_LOCATOR

MAC 地址

- MAC_ADDRESS
- ${device.MAC_ADDRESS

MAC 地址网络连接

- MAC_NETWORK_CONNECTION
- ${device.MAC_NETWORK_CONNECTION

MAC 地址类型

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE

邮箱设置

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- ${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP

主电池

- MAIN_BATTERY_PERCENT
- ${device.MAIN_BATTERY_PERCENT

已启用 MDM 丢失模式

- IS_MDM_LOST_MODE_ENABLED
- ${device.IS_MDM_LOST_MODE_ENABLED

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- ${device.MDX_SHARED_ENCRYPTION_KEY

MEID

- MEID
- ${device.MEID

移动电话号码

- TEL_NUMBER
- ${device.TEL_NUMBER

型号 ID

- MODEL_ID
- ${device.MODEL_ID}

型号

- MODEL_NUMBER
- ${device.MODEL_NUMBER

网络适配器类型

- NETWORK_ADAPTER_TYPE

- ${device.NETWORK_ADAPTER_TYPE

操作系统内部版本号

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD

操作系统版本

- OS_EDITION
- ${device.OS_EDITION

操作系统语言（区域设置）

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE

操作系统版本

- SYSTEM_OS_VERSION
- ${device.SYSTEM_OS_VERSION

组织地址

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS

组织电子邮件

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL

组织幻数

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC

组织名称

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME

组织电话号码

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE

不合规

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE

所有者

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED

通行码合规性

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT

通行码遵从配置

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG

通行码存在

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0

超出边界

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH

定期检查

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck

已激活个人热点

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED

地理围栏的 PIN 代码

- PIN_CODE_FOR_GEO_FENCE
- ${device.PIN_CODE_FOR_GEO_FENCE

平台

- SYSTEM_PLATFORM
- ${device.SYSTEM_PLATFORM}

平台 API 级别

- API_LEVEL
- ${device.API_LEVEL

策略名称

- POLICY_NAME
- ${device.POLICY_NAME

主电话号码

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER

主 SIM 卡运营商

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR

主 SIM 卡 ICCID

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID

主 SIM IMEI

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI

主 SIM IMSI

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI

主 SIM 漫游

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING

主 SIM 卡漫游合规性

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE

产品名称

- PRODUCT_NAME
- ${device.PRODUCT_NAME

发布者设备 ID

- PUBLISHER_DEVICE_ID
- ${device.PUBLISHER_DEVICE_ID

重置计数

- WINDOWS_HAS_RESET_COUNT

- ${device.WINDOWS_HAS_RESET_COUNT

重新启动计数

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT

已启用安全模式?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE

Samsung KNOX API 可用

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX

Samsung KNOX API 版本

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION

Samsung KNOX 认证

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED

Samsung KNOX 认证更新日期

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME

Samsung SAFE API 可用

- SAMSUNG_MDM
- ${device.SAMSUNG_MDM

Samsung SAFE API 版本

- SAMSUNG_MDM_VERSION
- ${device.SAMSUNG_MDM_VERSION

SBCP 哈希

- WINDOWS_HAS_SBCP_HASH
- ${device.WINDOWS_HAS_SBCP_HASH

屏幕：高度

- SCREEN_HEIGHT
- ${device.SCREEN_HEIGHT

屏幕：颜色数量

- SCREEN_NB_COLORS
- ${device.SCREEN_NB_COLORS

屏幕：大小

- SCREEN_SIZE
- ${device.SCREEN_SIZE

屏幕：宽度

- SCREEN_WIDTH
- ${device.SCREEN_WIDTH

屏幕：X 轴分辨率

- SCREEN_XDPI
- ${device.SCREEN_XDPI

屏幕：Y 轴分辨率

- SCREEN_YDPI
- ${device.SCREEN_YDPI

辅助电话号码

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER

辅助 SIM 卡运营商

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR

辅助 SIM 卡 ICCID

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID

辅助 SIM IMEI

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI

辅助 SIM IMSI

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI

辅助 SIM 漫游

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING

辅助 SIM 卡漫游合规性

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE

已启用安全启动?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED

安全启动状态

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE

已启用 SecureContainer

- DLP_ACTIVE
- ${device.DLP_ACTIVE

安全修补级别

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL

序列号

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER

具有 SMS 功能

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE

受监督

- SUPERVISED
- ${device.SUPERVISED

暂停原因

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON

被篡改状态

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS

条款和条件

- TERMS_AND_CONDITIONS

- ${device.TERMS_AND_CONDITIONS

已接受条款和协议?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS

已启用测试签名?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED

RAM 总量

- MEMORY
- ${device.MEMORY

总存储空间

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE

TPM 版本

- TPM_VERSION
- ${device.TPM_VERSION

UDID

- UDID
- ${device.UDID}

用户帐户控制状态

- UAC_STATUS
- ${device.UAC_STATUS

用户代理

- USER_AGENT
- ${device.USER_AGENT

用户定义的第一个

- USER_DEFINED_1
- ${device.USER_DEFINED_1

用户定义的第二个

- USER_DEFINED_2
- ${device.USER_DEFINED_2

用户定义的第三个

- USER_DEFINED_3
- ${device.USER_DEFINED_3

用户语言（区域设置）

- USER_LANGUAGE
- ${device.USER_LANGUAGE

供应商

- VENDOR
- ${device.VENDOR

语音支持

- IS_VOICE_CAPABLE
- ${device.IS_VOICE_CAPABLE

允许语音漫游

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED

已启用 VSM?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED

WiFi MAC 地址

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY

已启用 WinPE?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE

WNS 通知状态

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS

WNS 通知 URL

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL

WNS 通知 URL 过期日期

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY

XenMobile Agent ID

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID

XenMobile Agent 修订版

- EW_REVISION
- ${device.EW_REVISION

XenMobile Agent 版本

- EW_VERSION
- ${device.EW_VERSION

Zebra API 可用

- ZEBRA_MDM
- ${device.ZEBRA_MDM

Zebra MXMF 版本

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION

Zebra Patch 版本

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

用于获取内置用户属性的宏

显示名称	宏
domainname（域名；默认域）	`${ user.domainname }`
loginname（用户名 + 域名）	`${ user.loginname }`
username（如有，则为登录名去掉域）	`${ user.username }`

适用于所有用户属性的宏

显示名称	**Web** 元素	宏
Active Directory 失败登录尝试次数	badpwdcount	${ user.badpwdcount }
ActiveSync 用户电子邮件	asuseremail	${ user.asuseremail }
ASM 数据源	asmpersonsource	${ user.asmpersonsource }
ASM DEP 帐户名称	asmdepaccount	${ user.asmdepaccount }
ASM 管理式 Apple ID	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
ASM 通行码类型	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ASM 人员 ID	asmpersonid	${ user.asmpersonid }
ASM 人员状态	asmpersonstatus	${ user.asmpersonstatus }
ASM 人员职称	asmpersontitle	${ user.asmpersontitle }
ASM 人员的唯一 ID	asmpersonuniqueid	${ user.asmpersonuniqueid }
ASM 源系统 ID	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
ASM 学生年级	asmpersongrade	${ user.asmpersongrade }
BES 用户电子邮件	besuseremail	${ user.besuseremail }
公司	company	${ user.company }
公司名称	companyname	${ user.companyname }
国家/地区	c	${ user.c }
部门	department	${ user.department }
说明	description	${ user.description }
禁用的用户	disableduser	${ user.disableduser }

显示名称	**Web** 元素	宏
显示名称	displayname	`${ user.displayname }`
标识名	distinguishedname	`${ user.distinguishedname }`
域名	domainname	`${ user.domainname }`
电子邮件	mail	`${ user.mail }`
名字	givenname	`${ user.givenname }`
家庭住址	homestreetaddress	`${ user.homestreetaddress }`
居住城市	homecity	`${ user.homecity }`
居住国家/地区	homecountry	`${ user.homecountry }`
住宅传真	homefax	`${ user.homefax }`
住宅电话	homephone	`${ user.homephone }`
居住州/省/自治区/直辖市/地区	homestate	`${ user.homestate }`
住宅邮政编码	homezip	`${ user.homezip }`
IP 电话	ipphone	`${ user.ipphone }`
中间名首字母	middleinitial	`${ user.middleinitial }`
中间名	middlename	`${ user.middlename }`
移动	mobile	`${ user.mobile }`
名称	cn	`${ user.cn }`
办公室地址	physicaldeliveryofficename	`${ user.physicaldeliveryofficename }`
办公室所在城市	l	`${ user.l }`
办公室传真号码	facsimiletelephonenumber	`${ user.facsimiletelephonenumber }`
办公室所在州/省/自治区/直辖市	st	`${ user.st }`
办公室所在街道地址	officestreetaddress	`${ user.officestreetaddress }`

显示名称	**Web** 元素	宏
办公室电话号码	telephonenumber	`${ user.telephonenumber }`
办公室所在地邮政编码	postalcode	`${ user.postalcode }`
邮箱	postofficebox	`${ user.postofficebox }`
寻呼机	pager	`${ user.pager }`
主组 ID	primarygroupid	`${ user.primarygroupid }`
SAM 帐户	samaccountname	`${ user.samaccountname }`
街道地址	streetaddress	`${ user.streetaddress }`
姓氏	sn	`${ user.sn }`
标题	title	`${ user.title }`
用户登录名	userprincipalname	`${ user.userprincipalname }`

自动化操作

January 5, 2022

在 XenMobile 中创建自动化操作以计划对事件、用户或设备属性或者用户设备上存在应用程序做出反应。创建自动化操作时，针对操作定义的触发器确定在用户设备连接到 XenMobile 时进行的操作。触发事件后，您可以在采取更实质性的操作之前向用户发送通知以更正问题。

设置为自动出现的影响范围如下：

- 完全或选择性地擦除设备。
- 将设备设置为不合规。
- 吊销设备。
- 在采取更严重的操作之前，向用户发送通知以更正问题。

可以为仅 MAM 模式配置应用程序锁定和应用程序擦除操作。

> 注意：
>
> 必须在 XenMobile 设置中为 SMTP 和 SMS 配置通知服务器，以便 XenMobile 能够发送消息，才能通知用户。

> 有关信息，请参阅通知。此外，请在继续操作前设置计划使用的通知模板。有关详细信息，请参阅创建和更新通知模板。

示例操作

下面是使用自动化操作的一些示例：

示例一

- 您要检测先前阻止的应用程序（例如，“Words with Friends”）。可以指定一个触发器，用于在检测到 “Words with Friends” 应用程序时，将用户设备设置为不合规。然后，该操作向用户通知必须删除该应用程序才能使其设备恢复合规状态。您还可以设置等待用户按指示进行操作的时间限制。过了该时间限制后，将发生定义的操作，例如，选择性擦除设备。

示例二

- 您想验证客户是否正在使用最新固件，并在用户需要更新其设备时阻止对资源的访问。您可以指定一个触发器，用于在用户设备未安装最新版本时将用户设备设置为不合规。可以使用自动操作来阻止资源并通知客户。

示例三

- 将用户设备置于不合规状态，用户随后修复该设备。可以配置策略来部署将设备重置为合规状态的软件包。

示例四

- 您希望将在特定时间段内处于不活动状态的用户设备标记为不合规。可以按如下所示为不活动设备创建自动化操作：
    1. 在 XenMobile 控制台中，转到设置 > 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。
    2. 按照添加和管理操作中所述的步骤添加操作。唯一的区别是，您在操作详细信息页面上按如下所示配置设置：
        - 触发器。选择设备属性、不合规性和真。
        - 操作。选择发送通知，然后选择使用设置中的通知模板创建的模板。然后在执行该操作之前设置延迟时间（以天、小时或分钟为单位）。设置用户解决触发问题前重复执行操作的时间间隔。

> 提示：
>
> 要批量删除不活动设备，请使用适用于 REST 的公共 API 服务。首先，您可以手动获取要删除的不活动设备的设备 ID，然后运行删除 API 以将其批量删除。

添加和管理操作

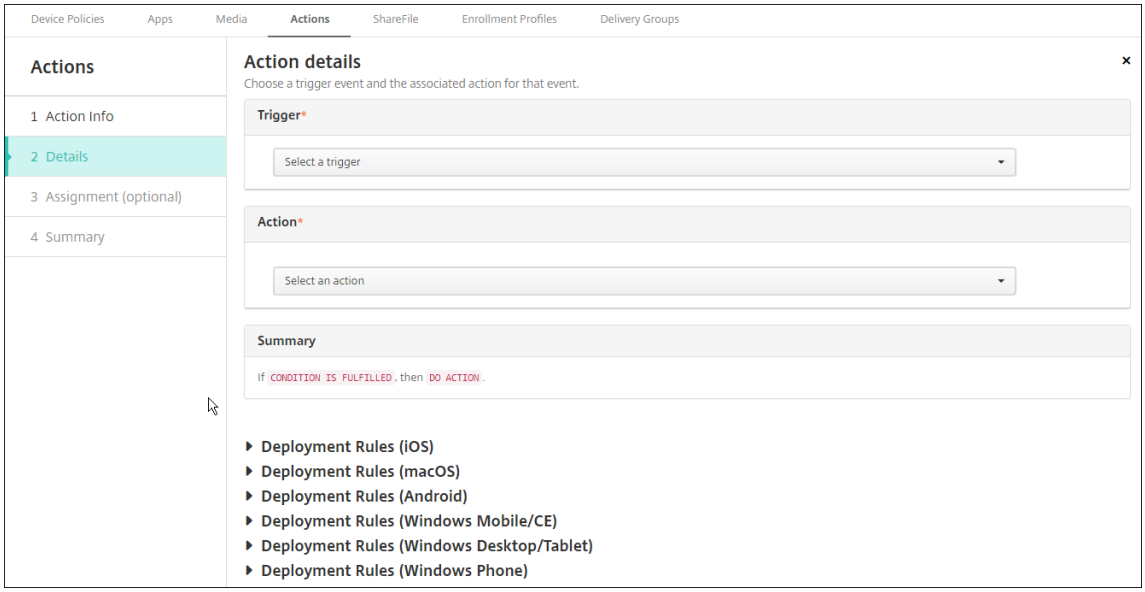
要添加、编辑和过滤自动化操作，请执行以下操作：

1. 在 XenMobile 控制台中，单击配置 > 操作。此时将显示操作页面。
2. 在操作页面上，执行以下操作之一：

- 单击添加以添加操作。
- 选择要编辑或删除的现有操作。单击要使用的选项。

3. 此时将显示操作信息页面。
4. 在操作信息页面上，输入或修改以下信息：
   - 名称：键入名称来标识操作。此字段为必填字段。
   - 说明：描述执行该操作的目的。
5. 单击 **Next**（下一步）。此时将显示操作详细信息页面。

   以下示例显示如何设置事件触发器。如果选择其他触发器，出现的选项将与此处显示的选项有所不同。



6. 在操作详细信息页面上，输入或修改以下信息：

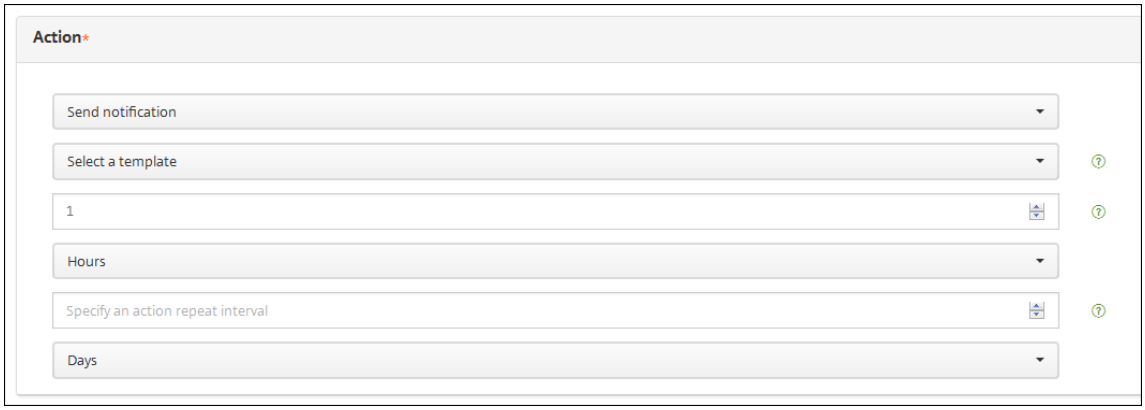
   在触发器列表中，单击适用于此操作的事件触发器类型。每个触发器的含义如下所示：

   - 事件：对预定义的事件做出反应。
   - 设备属性：检查 MDM 管理的设备上的设备属性，然后对其做出反应。有关详细信息，请参阅设备属性名称和值。
   - 用户属性：对用户属性（通常来自 Active Directory）做出反应。
   - 已安装应用程序的名称：对正在安装的应用程序做出反应。不应用于仅 MAM 模式。要求在设备上启用应用程序清单策略。默认情况下，应用程序清单策略在所有平台上均处于启用状态。有关详细信息，请参阅应用程序清单设备策略。
7. 在下一个列表中，单击对触发器的响应。
8. 在操作列表中，单击符合触发器条件时要执行的操作。除发送通知外，请选择一个时间范围，让用户可以解决导致触发的问题。如果在该时间范围内未解决此问题，将执行选定的操作。有关操作的定义，请参阅安全操作。

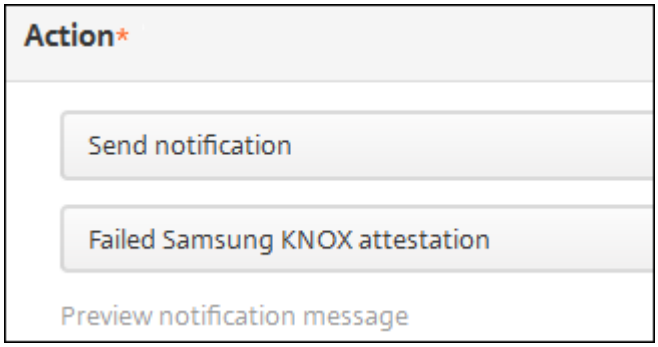
   如果选择发送通知，则按照以下步骤发送通知操作。

9. 在下一个列表中，选择用于通知的模板。与所选事件相关的通知模板将显示，除非还不存在通知类型的模板。在这种情况下，系统会提示您配置模板，并显示消息：此事件类型的模板不存在。请使用设置中的通知模板来创建模板。

   必须在“设置”中为 SMTP 和 SMS 配置通知服务器，以便 XenMobile 可以发送消息，才能通知用户，请参阅通知。此外，请在继续操作前设置计划使用的通知模板。有关设置通知模板的详细信息，请参阅创建或更新通知模板。



   选择模板后，可以单击预览通知消息来预览通知。



10. 在以下字段中，以天、小时或分钟为单位设置执行该操作之前的延迟。设置用户解决触发问题前重复执行操作的时间间隔。

11. 在摘要中，验证您是否已按预期创建自动化操作。

12. 配置操作详细信息后，可以分别为每个平台配置部署规则。为此，针对您选择的每个平台执行步骤 13。
13. 配置部署规则。有关配置部署规则的常规信息，请参阅部署资源。

    对于此示例：

    - 设备所有权必须为 **BYOD**。
    - 设备本地加密必须为 **True**。
    - 设备必须兼容通行码。
    - 设备的移动设备国家/地区代码不能仅为“安道尔”。
14. 针对该操作配置了平台部署规则后，单击下一步。此时将显示操作分配页面，您可以在此将操作分配给一个或多个交付组。此步骤可选。
15. 在选择交付组旁边，键入以查找交付组或者在列表中选择组。选择的组显示在用于接收应用程序分配的交付组列表中。
16. 展开部署计划，然后配置以下设置：

    - 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。如果选择关，则无需其他选项。
    - 在部署计划旁边，单击立即或以后。默认选项为立即。
    - 如果单击以后，请单击日历图标，然后选择部署的日期和时间。
    - 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
    - 在为始终启用的连接部署旁边，单击开或关。默认选项为关。

      如果在设置 **>** 服务器属性中配置了计划后台部署密钥，则适用此选项。始终启用选项不适用于 iOS 设备。

    配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。
17. 单击 **Next**（下一步）。此时将显示摘要页面，您可以在此验证操作配置。
18. 单击保存以保存操作。

面向仅 **MAM** 模式的应用程序锁定和应用程序擦除操作

您可以针对 XenMobile 控制台中列出的全部四种类别触发器（即事件、设备属性、用户属性和已安装应用程序的名称），采取擦除或锁定设备上的应用程序这一响应方式。

配置应用程序擦除或应用程序锁定自动操作

1. 在 XenMobile 控制台中，单击配置 **>** 操作。
2. 在操作页面上，单击添加。
3. 在操作信息页面上，输入操作名称和可选说明。
4. 在操作详细信息页面上，选择所需的触发器。
5. 在操作中，选择一项操作。

   针对此步骤，请记住以下条件：

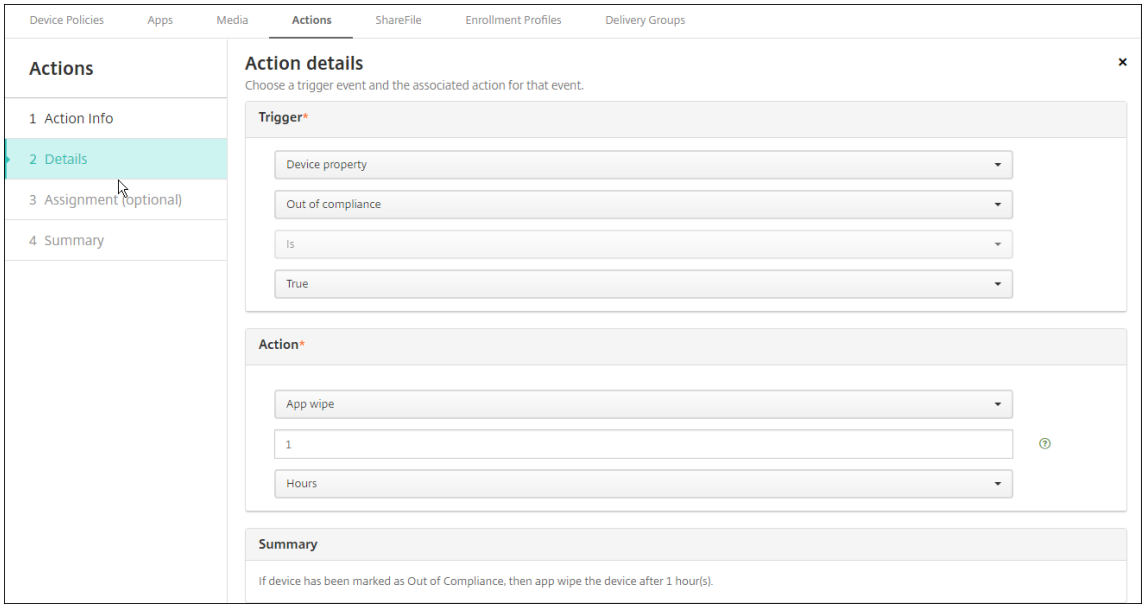
   触发器类型为事件，但值不是 **Active Directory** 已禁用用户时，将不显示应用程序擦除和应用程序锁定操作。

   触发器类型为设备属性，值为已启用 **MDM** 丢失模式时，将不显示以下操作：

   - 选择性擦除设备
   - 完全擦除设备
   - 吊销设备

   每个选项都会自动设置 1 小时延迟，但也可选择以分钟、小时或天为单位的延迟期限。延迟的目的是在执行操作之前让用户有时间解决问题。有关应用程序擦除和应用程序锁定操作的详细信息，请参阅安全操作。

   > 注意：
   >
   > 如果您将触发器设置为事件，重复时间间隔将自动设置为最小值 1 小时。设备必须刷新策略以与服务器同步，才能传入通知。通常情况下，设备将在用户通过 Secure Hub 登录或手动刷新其策略时与服务器同步。
   >
   > 在执行任何操作之前，还可能会再延迟 1 小时左右，以便允许 Active Directory 数据库与 XenMobile 同步。

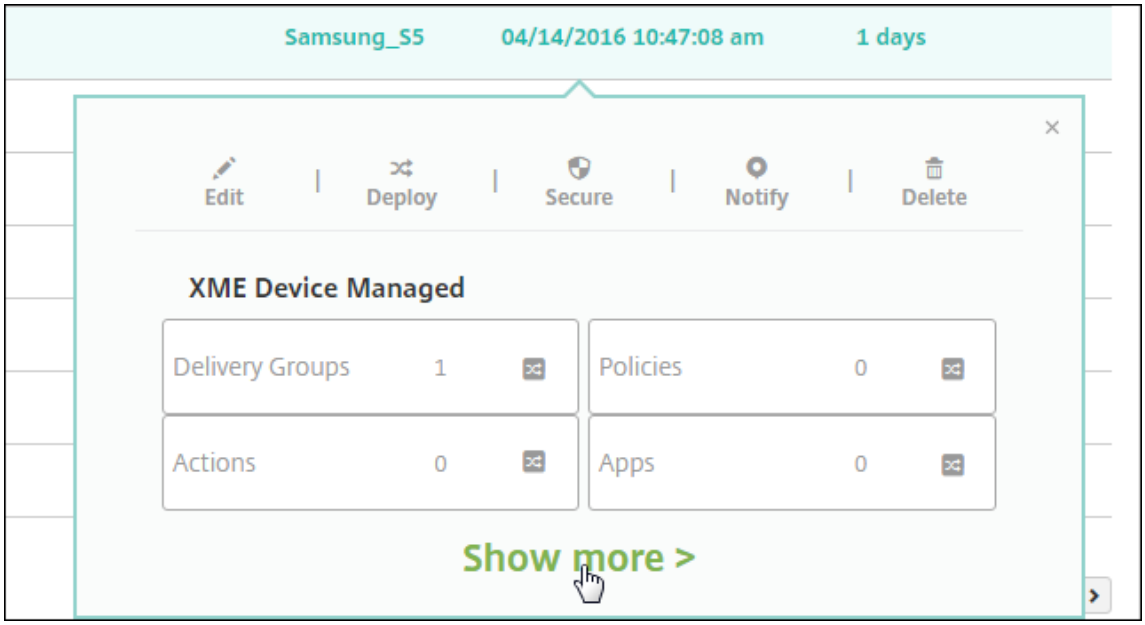


6. 配置部署规则，然后单击下一步。

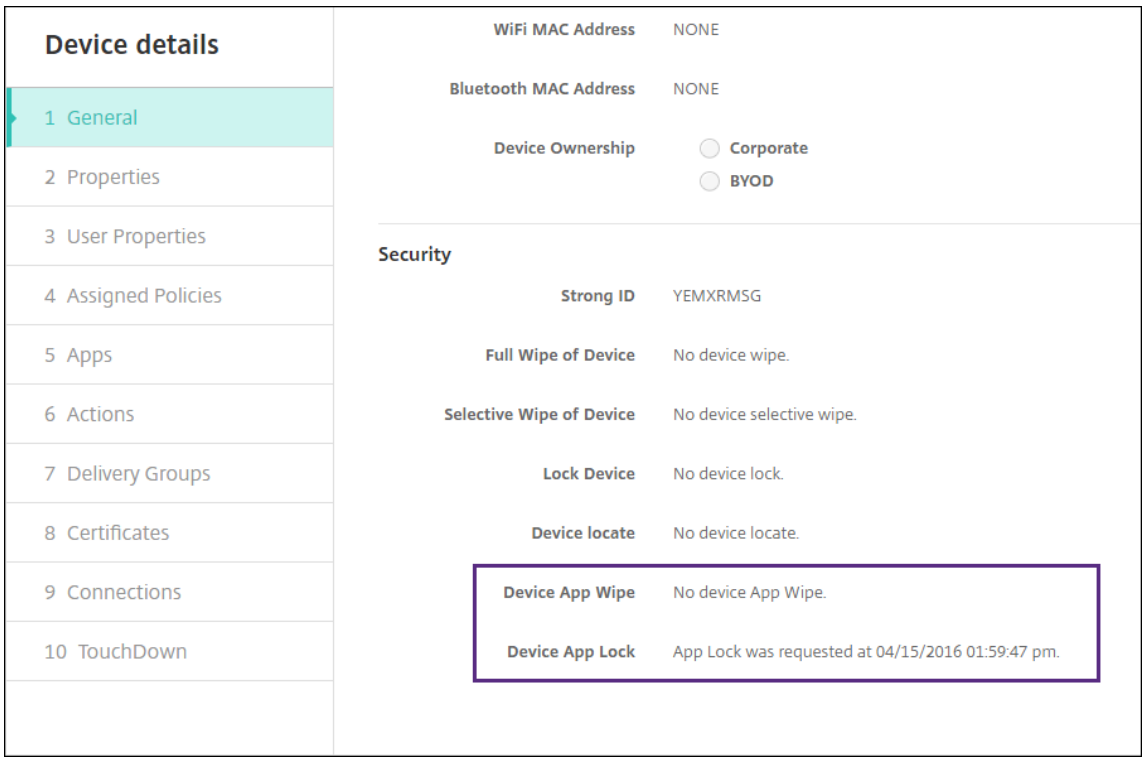
7. 配置交付组分配和部署计划，然后单击下一步。
8. 单击保存。

检查应用程序锁定或应用程序擦除状态

1. 转至管理 **>** 设备，单击某个设备，然后单击显示更多。



2. 滚动到设备应用程序擦除和设备应用程序锁定。



擦除设备后，系统将提示用户输入 PIN 代码。如果用户忘记了该代码，您可以在“设备详细信息”中查找。

监视和支持

January 21, 2021

可以使用 XenMobile 控制板和 XenMobile 的“支持”页面监视 XenMobile Server 以及对其进行故障排除。使用 XenMobile 的“支持”页面可以访问与支持有关的信息和工具。

对于本地 XenMobile Server，还可以从 XenMobile CLI 执行操作。有关详细信息，请参阅命令行接口选项。

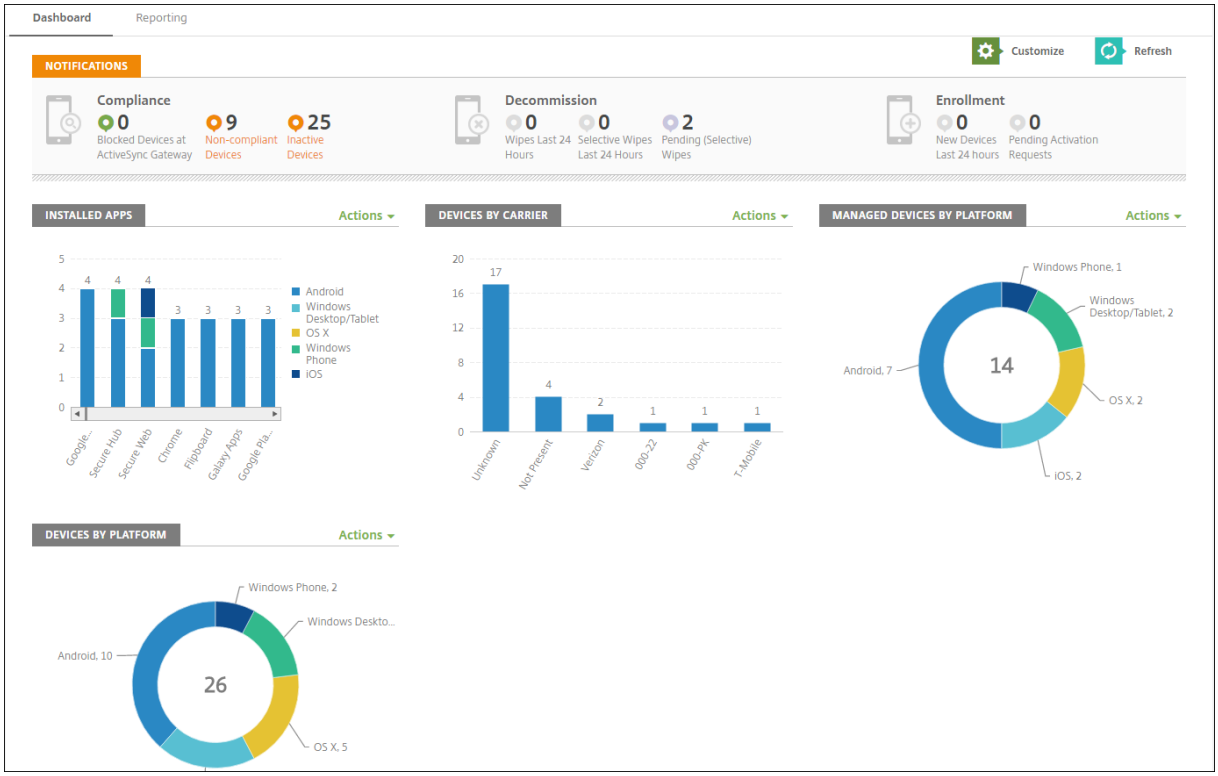
在 XenMobile 控制台中，单击右上角的扳手图标。

此时将显示故障排除和支持页面。

使用 XenMobile 的支持页面可以执行以下操作：

- 访问诊断。
- 创建支持包（仅限本地安装）。
- 访问 Citrix 产品文档和知识中心的链接。
- 访问日志操作。
- 使用高级配置选项。
- 访问工具和实用程序。

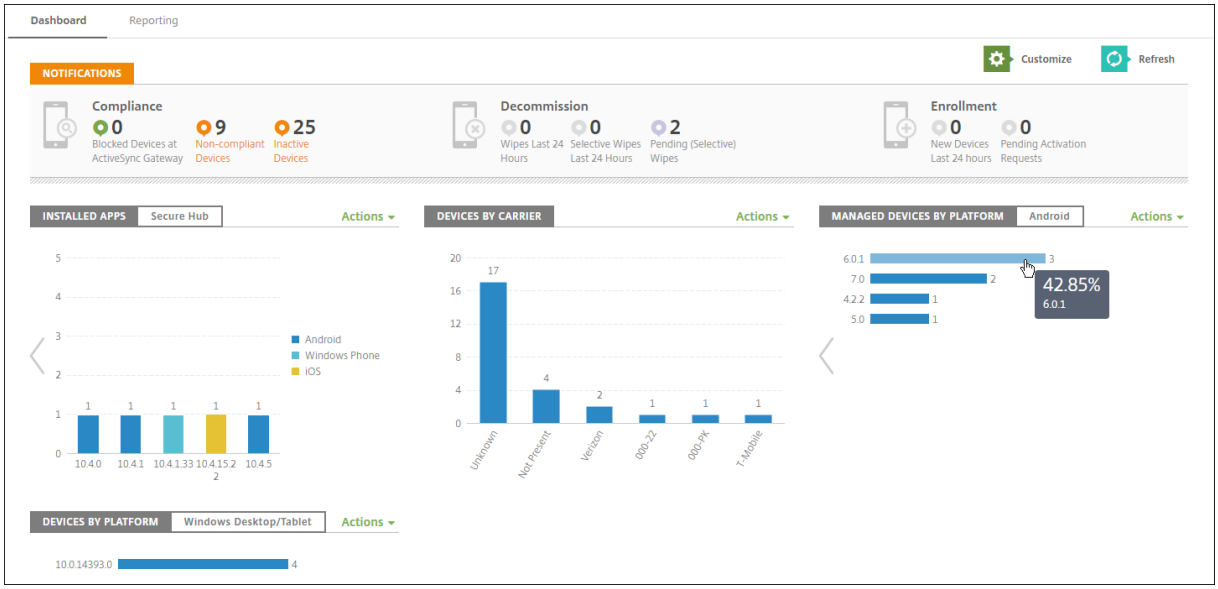
还可以通过访问 XenMobile 控制台控制板概括查看信息。根据这些信息，您可以使用小组件快速查看问题和成功方法。



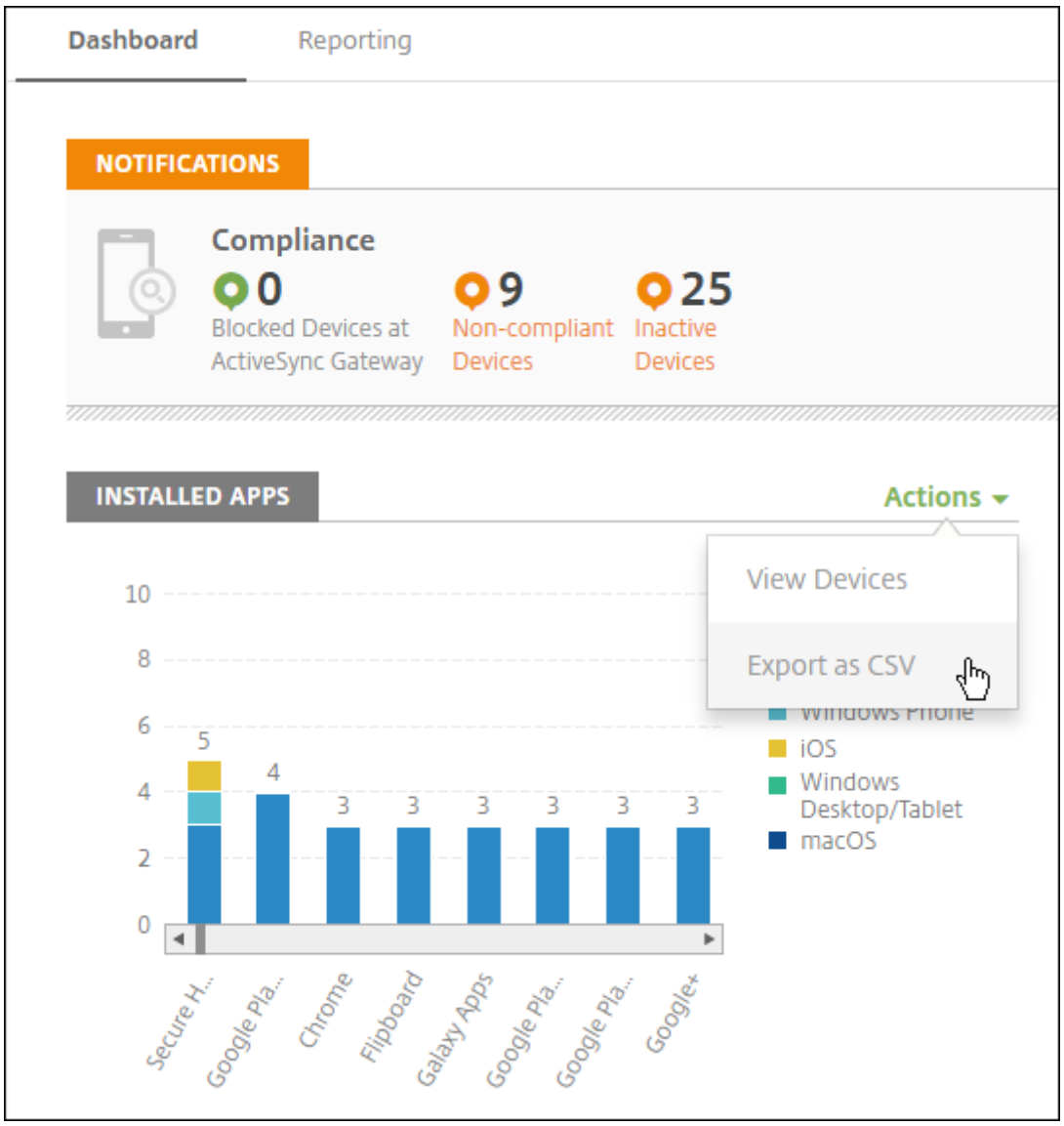
控制板通常是您登录 XenMobile 控制台时首先显示的页面。要从控制台中的其他地方访问控制板，请单击分析。单击控制板中的自定义可编辑页面布局以及编辑显示的小组件。

- 我的控制板：最多可以保存四个控制板。可以单独编辑这些控制板，并通过选择保存的控制板来查看每个控制板。
- 布局样式：在此行中，可以选择在控制板上显示的小组件数以及如何布局小组件。
- 小组件选择：可以选择在控制板上显示的信息。
  - 通知：选中左侧数字上方的复选框可将“通知”栏添加到小组件上方。此栏显示兼容设备、不活动设备以及过去 24 小时擦除或注册的设备数。
  - 设备 (按平台)：按平台显示托管设备和非托管设备数。
  - 设备 (按运营商)：按运营商显示托管设备和非托管设备数。单击每个栏可按平台查看明细。
  - 托管设备 (按平台)：按平台显示托管设备数。
  - 非托管设备 (按平台)：按平台显示非托管设备数。此图表中显示的设备可能安装了代理，但设备的权限已被吊销或设备已被擦除。
  - 设备 (按 **ActiveSync Gateway** 状态)：显示按 ActiveSync Gateway 状态分组的设备数。信息中显示“已阻止”、“已允许”或“未知”状态。可以单击每个栏来按平台细分数据。
  - 设备 (按所有权)：显示按所有权状态分组的设备数。信息中显示“公司拥有”、“员工拥有”或“未知所有权”状态。
  - 失败的交付组部署：按软件包显示失败部署总数。仅显示部署失败的软件包。
  - 设备 (按阻止原因)：显示 ActiveSync 阻止的设备数
  - 已安装的应用程序：键入应用程序信息图的应用程序名称。
  - 批量购买应用程序许可证使用情况：显示 Apple 批量购买应用程序的许可证使用情况统计信息。

通过每个小组件，可以单击各个部分深入查看详细信息。



还可以单击操作下拉列表将信息导出为.csv 文件。

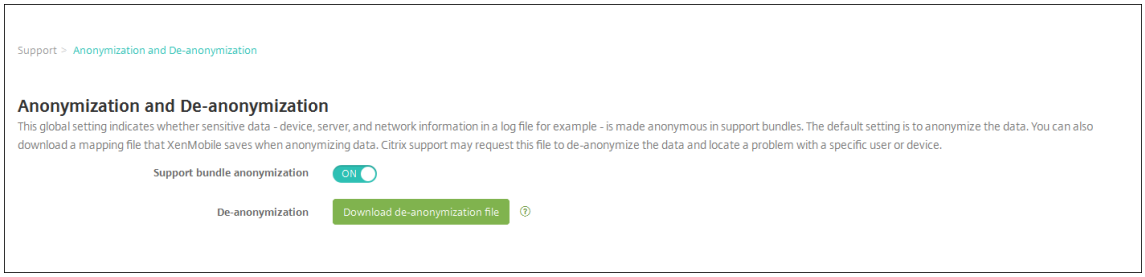


匿名化支持包中的数据

October 10, 2018

在 XenMobile 中创建支持包时，默认情况下会将敏感用户、服务器和网络数据设为匿名。可以在“匿名和取消匿名”页面更改此行为。还可以下载 XenMobile 在匿名化数据时保存的映射文件。Citrix 支持人员可能会要求此文件对数据取消匿名，并查找特定用户和设备的问题。

1. 在 XenMobile 控制台中，单击右上角的扳手图标。此时将显示支持页面。
2. 在支持页面上的高级下方，单击匿名和取消匿名。此时将显示匿名和取消匿名页面。



3. 在支持包匿名中，选择是否对数据进行匿名化处理。默认值为开。
4. 在取消匿名旁边，单击下载取消匿名文件以下载映射文件，在 Citrix 支持需要特定设备或用户信息来诊断问题时，将此文件发送给他们。

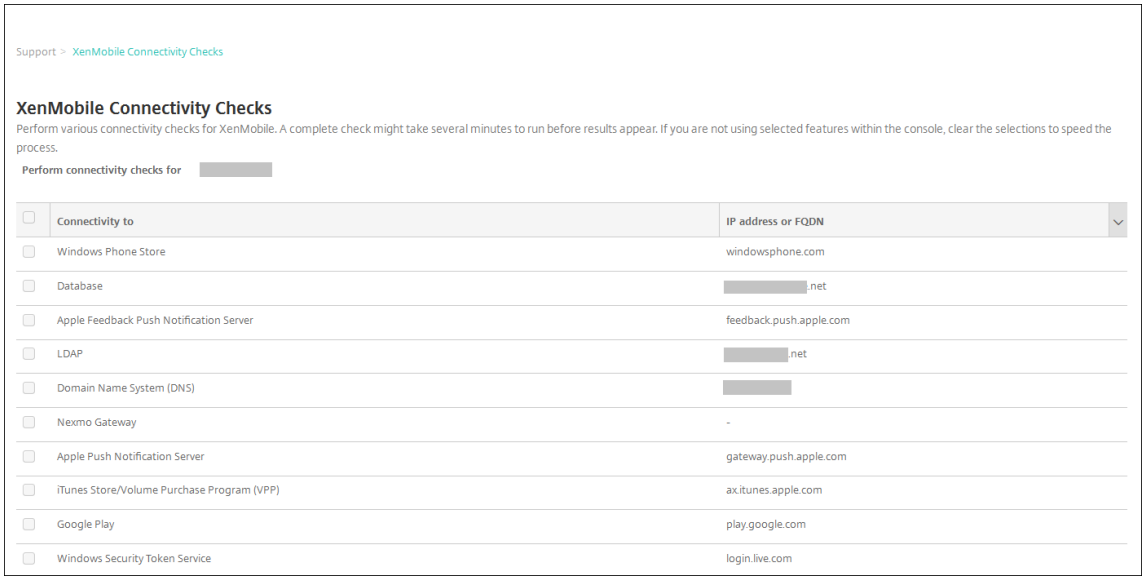
连接检查

November 12, 2020

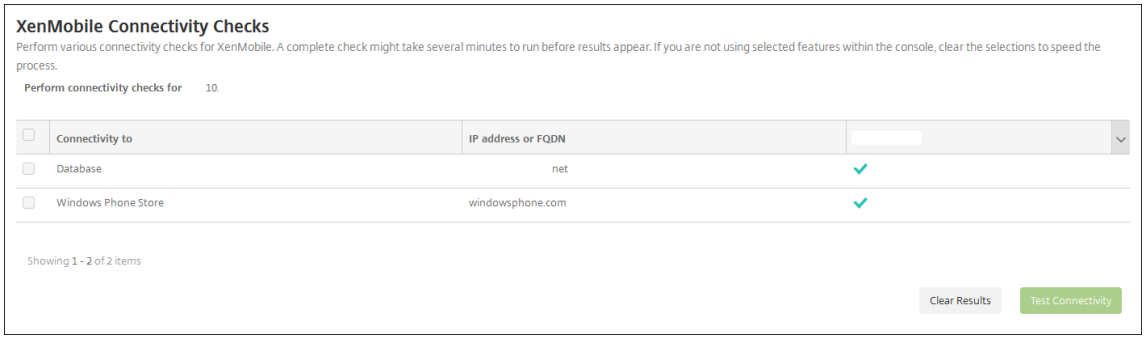
从 XenMobile 的支持页面，可以检查 XenMobile 与 Citrix Gateway 及其他服务器和位置的连接情况。

执行 **XenMobile** 连接检查

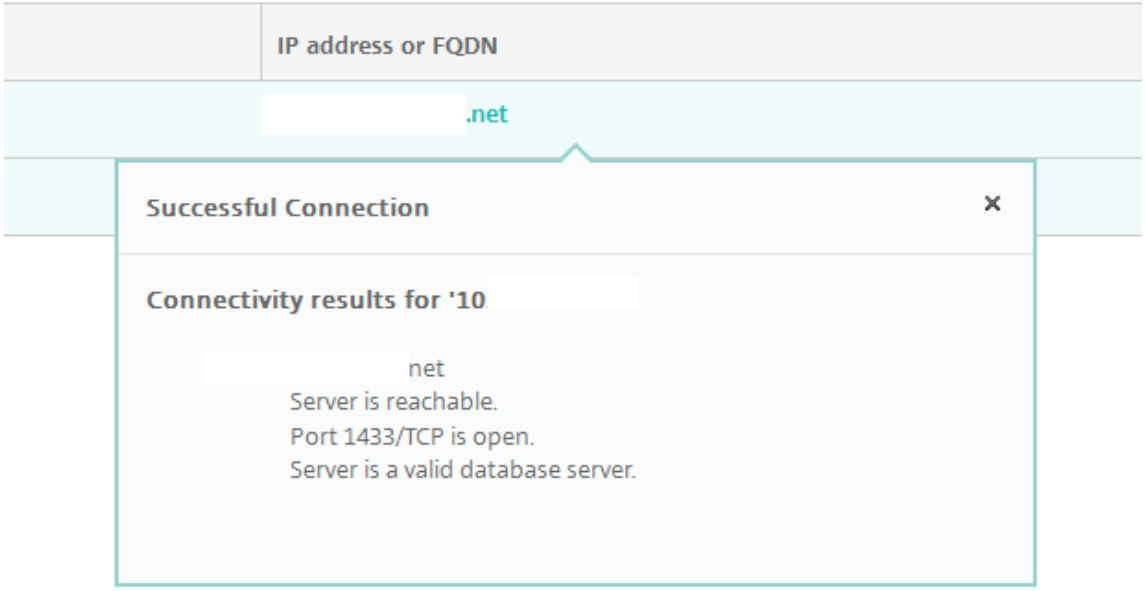
1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。此时将显示支持页面。
2. 在诊断下方，单击 **XenMobile** 连接检查。此时将显示 **XenMobile** 连接检查页面。如果 XenMobile 环境包含加入群集的节点，将显示所有节点。



3. 选择执行连接测试时要包括的服务器，然后单击测试连接。此时将显示测试结果页面。

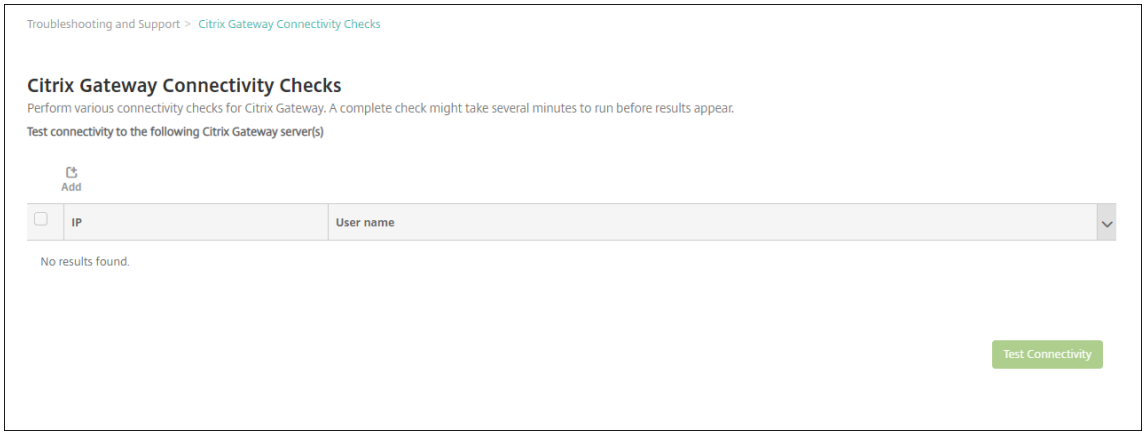


4. 在测试结果表中选择一个服务器以查看该服务器的详细结果。

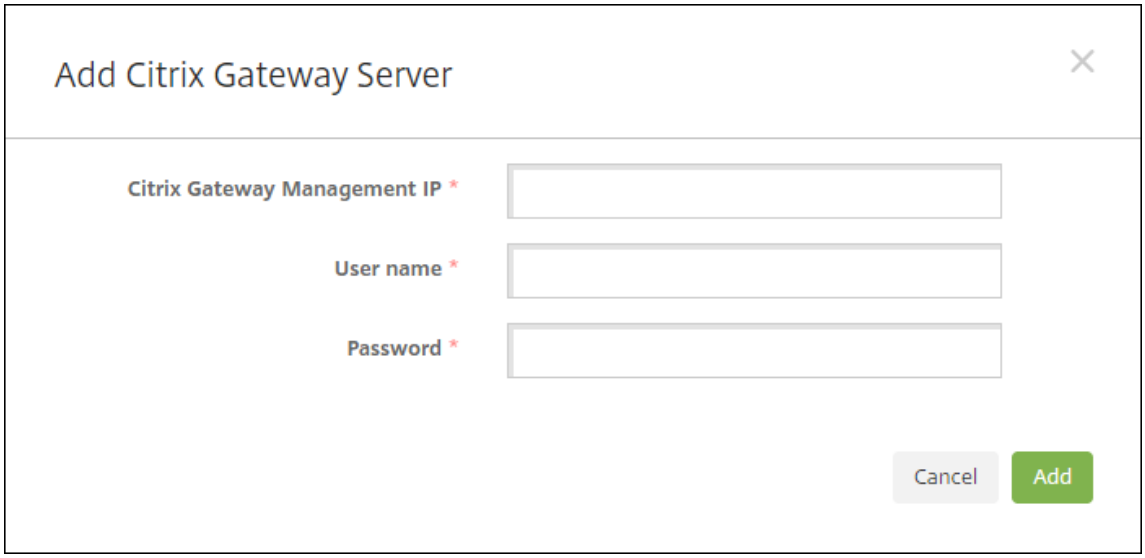


执行 **Citrix Gateway** 连接性检查

1. 在支持页面上的诊断下，单击 **Citrix Gateway** 连接检查。此时将显示 **Citrix Gateway** 连接检查页面。如果尚未添加任何 Citrix Gateway 服务器，此表格为空。



2. 单击添加。此时将显示添加 **Citrix Gateway** 服务器对话框。



3. 在 **Citrix Gateway** 管理 **IP** 中，键入运行要测试的 Citrix Gateway 的服务器的管理 IP 地址。

> 注意：
>
> 如果要对以前已添加的 Citrix Gateway 服务器执行连接检查，系统会提供 IP 地址。

4. 键入关于此 Citrix Gateway 的管理员凭据。

> 注意：
>
> 如果要对以前已添加的 Citrix Gateway 服务器执行连接检查，系统会提供用户名。

5. 单击添加。此 Citrix Gateway 将添加到 **Citrix Gateway** 连接检查页面上的表格中。
6. 选择 Citrix Gateway 服务器，然后单击测试连接。结果将显示在测试结果表格中。
7. 在测试结果表中选择一个服务器以查看该服务器的详细结果。

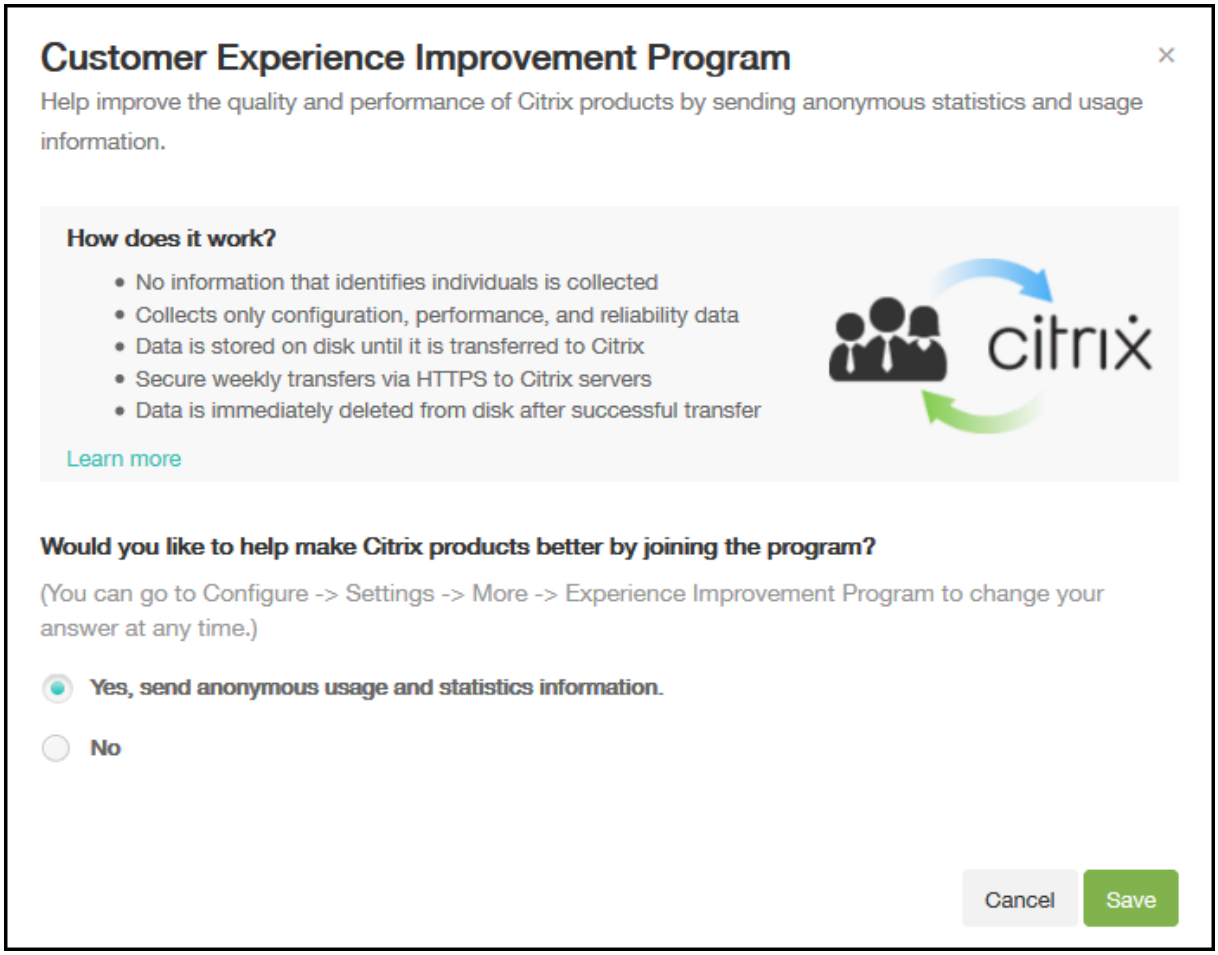
客户体验改善计划

October 31, 2018

Citrix 客户体验改善计划 (CEIP) 从 XenMobile 收集匿名配置和使用数据，并自动将数据发送到 Citrix。此数据可帮助 Citrix 改善 XenMobile 的品质、可靠性和性能。参与 CEIP 完全自愿。首次安装 XenMobile 时或安装更新时，可以选择是否参与 CEIP。选择参与后，通常每周收集一次数据，而性能和使用数据则每小时收集一次。这些数据存储在磁盘上，每周一次通过 HTTPS 安全地传输给 Citrix。您可以在 XenMobile 控制台更改是否参与 CEIP。有关 CEIP 的详细信息，请参阅关于 Citrix 客户体验改善计划 (CEIP)。

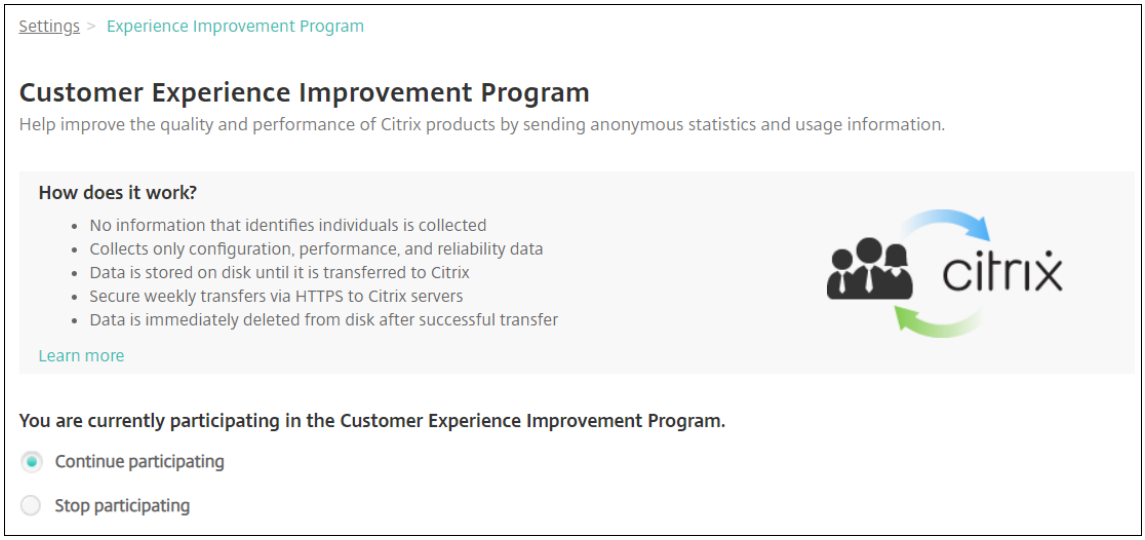
选择参与 **CEIP**

首次安装 XenMobile 或进行更新时，您会看到提示您参与的以下对话框。



更改 **CEIP** 参与设置

1. 要更改 CEIP 参与设置，请在 XenMobile 控制台中，单击控制台右上角的齿轮图标以打开设置页面。
2. 在服务器下方，单击体验改善计划。此时将显示客户体验改善计划页面。所显示的确切页面取决于您当前是否已参与 CEIP。



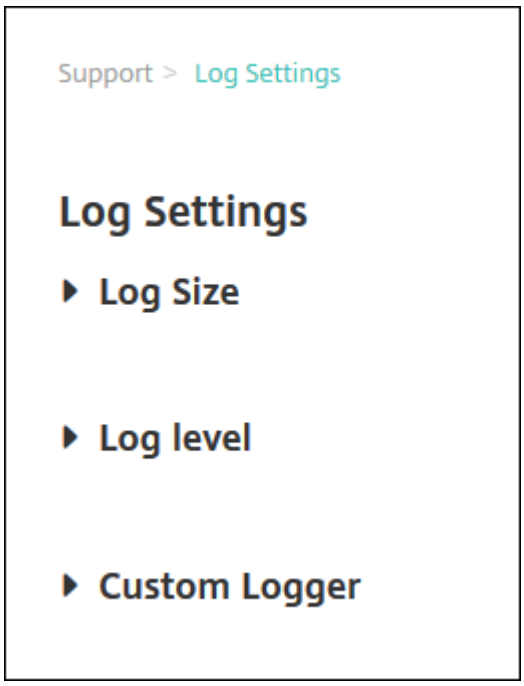
3. 如果当前已参与 CEIP 并希望停止，请单击停止参与。
4. 如果当前未参与 CEIP 并希望开始参与，请单击开始参与。
5. 单击保存。

日志

January 5, 2022

您可以配置日志设置，以自定义 XenMobile 生成的日志的输出。如果您的 XenMobile Server 已加入群集，则在 XenMobile 控制台中配置日志设置时，这些设置将与群集中的所有其他服务器共享。

1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。此时将显示支持页面。
2. 在日志操作下方，单击日志设置。此时将显示日志设置页面。

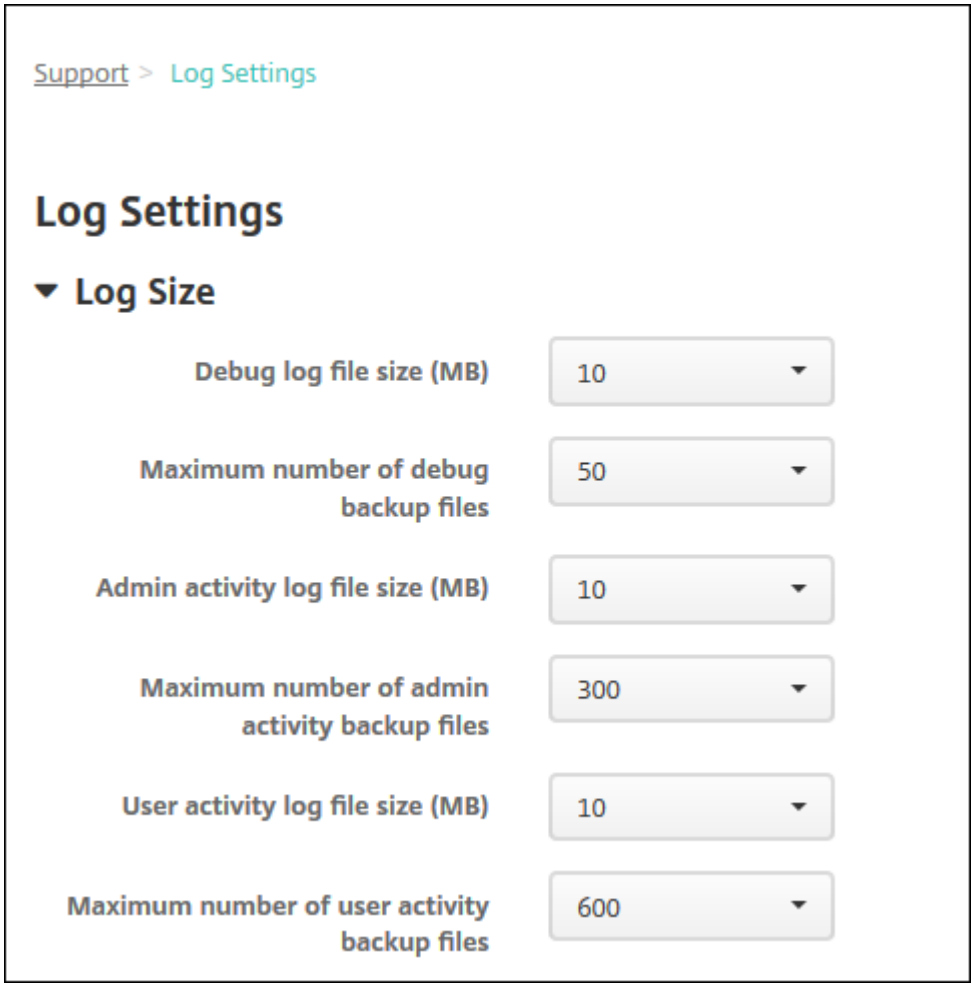


在日志设置页面上，您可以访问以下选项：

- 日志大小。使用此选项可以控制日志文件的大小和保留在数据库中的日志备份文件的最大数量。日志大小适用于 XenMobile 支持的每个日志（调试日志、管理活动日志和用户活动日志）。
- 日志级别。使用此选项可将日志级别更改为静态设置。
- 自定义记录器。使用此选项可以创建自定义的日志记录器；自定义日志需要一个类名称和日志级别。

配置“日志大小”选项

1. 在日志设置页面上，展开日志大小。



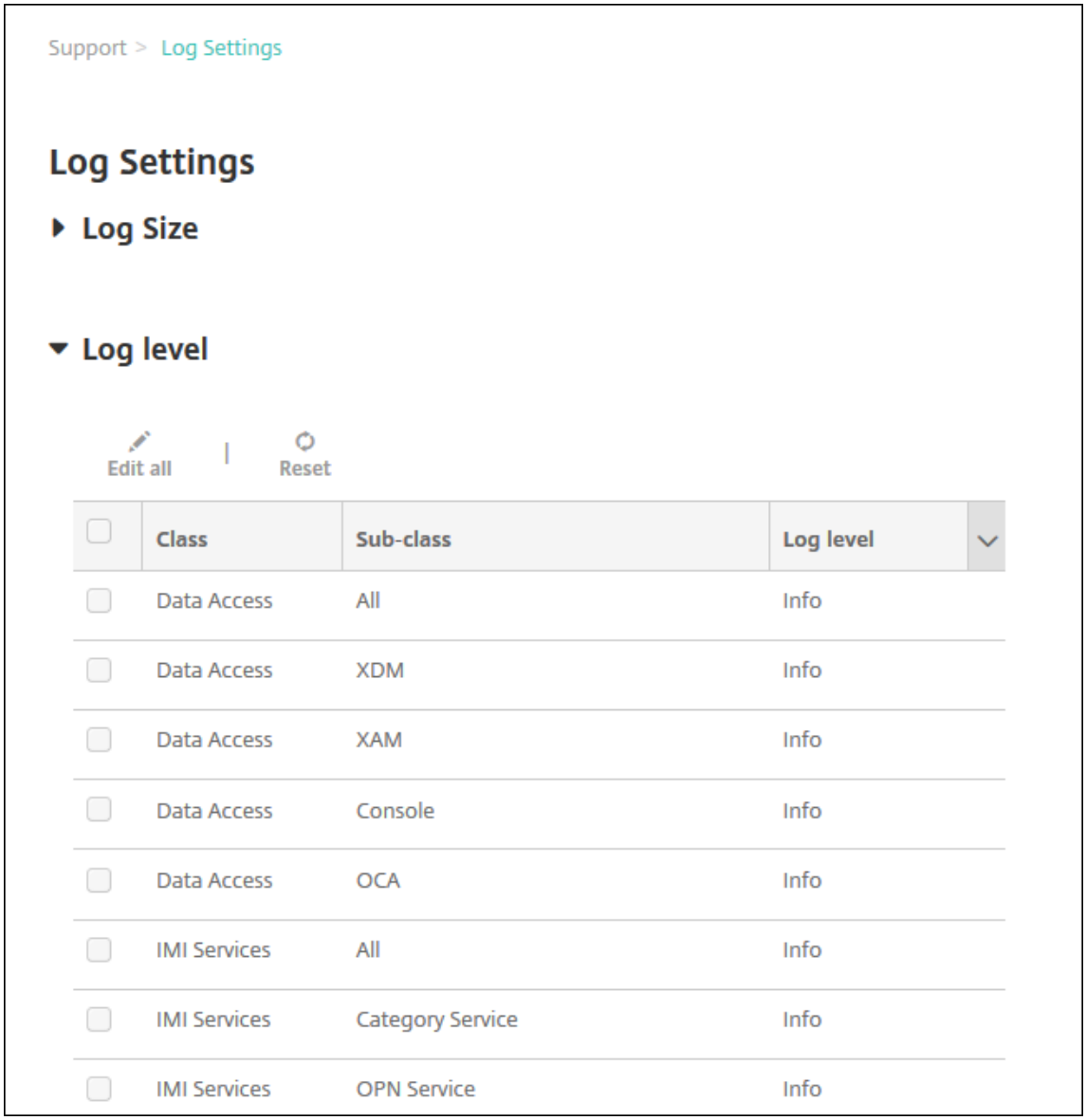
2. 配置以下设置：

- 调试日志文件大小 **(MB)**：在列表中，单击 5 MB 到 20 MB 之间的大小，以更改调试文件的最大大小。默认文件大小为 **10 MB**。
- 调试备份文件数上限：在列表中，单击服务器保留的调试文件数上限。默认情况下，XenMobile 在服务器上保留 50 个备份文件。
- 管理活动日志文件大小 **(MB)**：在列表中，单击 5 MB 到 20 MB 之间的大小，以更改管理活动文件的最大大小。默认文件大小为 **10 MB**。
- 管理活动备份文件数上限：在列表中，单击服务器保留的管理活动文件数上限。默认情况下，XenMobile 在服务器上保留 300 个备份文件。
- 用户活动日志文件大小 **(MB)**：在列表中，单击 5 MB 到 20 MB 之间的大小，以更改用户活动文件的最大大小。默认文件大小为 **10 MB**。
- 用户活动备份文件数上限：在列表中，单击服务器保留的用户活动文件数上限。默认情况下，XenMobile 在服务器上保留 300 个备份文件。

配置“日志级别”选项

通过日志级别，您可以指定 XenMobile 在日志中收集的信息类别。可以为所有类别设置相同的级别，也可以将各个类别设置为特定的级别。

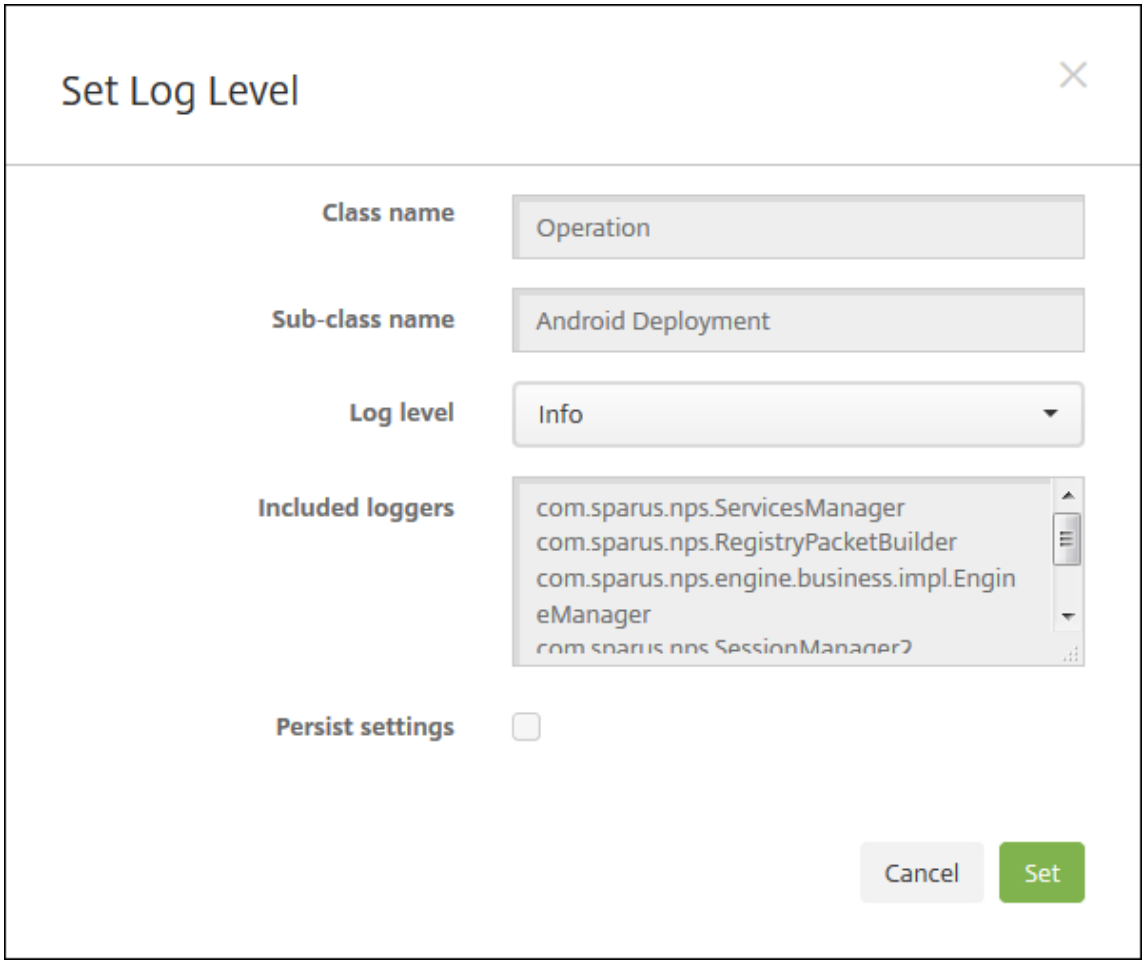
1. 在日志设置页面上，展开日志级别。此时将显示一个包含所有日志类别的表格。



2. 执行以下操作之一：

   - 单击某个类别旁边的复选框，然后单击设置级别以仅更改此类别的日志级别。
   - 单击编辑全部以将日志级别更改应用于表格中的所有类别。

   此时将显示设置日志级别对话框，您可以在此设置日志级别，并选择是否在重新启动 XenMobile Server 时保持日志级别设置不变。

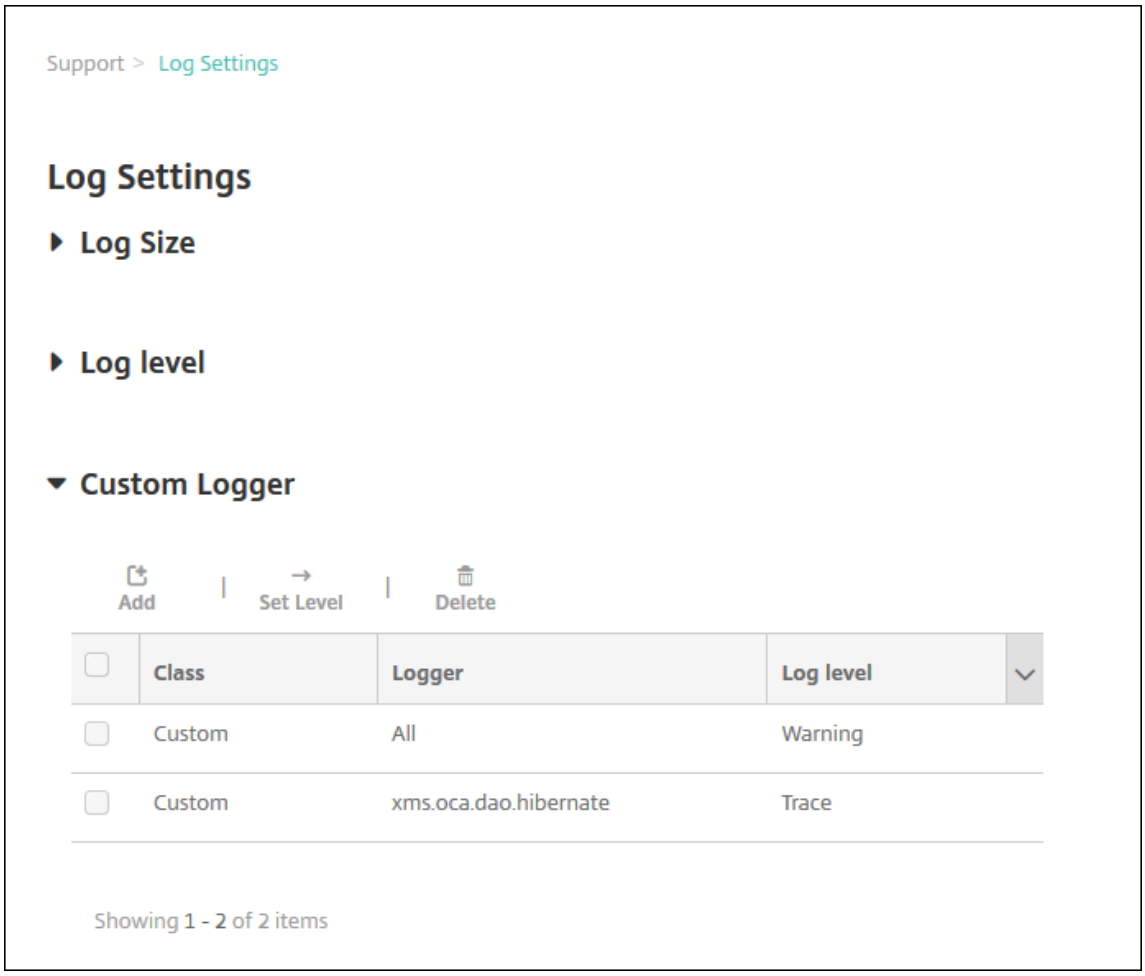


- 类别名称：如果要更改所有类别的日志级别，此字段将显示“全部”，否则将显示单个类别的名称；此字段不可编辑。
- 子类别名称：如果要更改所有类别的日志级别，此字段将显示“全部”，否则将显示单个子类别的名称；此字段不可编辑。
- 日志级别：在列表中，单击日志级别。支持的日志级别包括：
  - 致命
  - 错误
  - 警告
  - 信息
  - 调试
  - 跟踪
  - 关
- 包括记录器：如果要更改所有类别的日志级别，此字段将为空，否则将显示单个类别的当前已配置的记录器；此字段不可编辑。
- 静态设置：如果希望重新启动服务器时日志级别设置保持不变，请选中此复选框。未选中此复选框表示当您重新启动服务器时，日志级别设置将恢复为默认值。

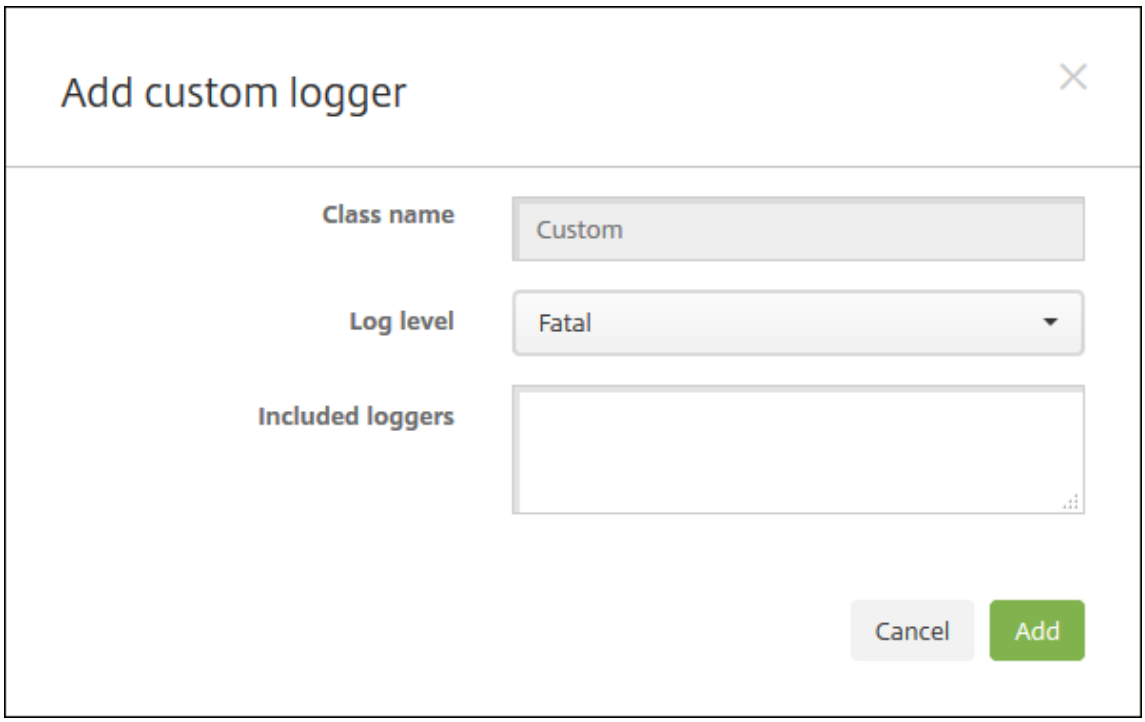
3. 单击设置提交更改。

添加自定义日志记录器

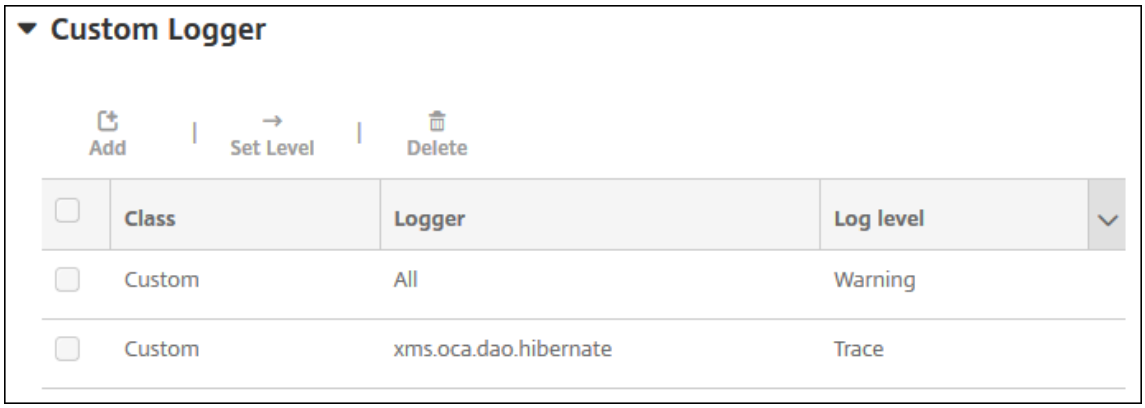
1. 在日志设置页面上，展开自定义记录器。此时将显示自定义记录器表格。如果尚未添加任何自定义记录器，此表格最初为空。



2. 单击添加。此时将显示添加自定义记录器对话框。



3. 配置以下设置：
   - 类别名称：此字段显示自定义；此字段不可编辑。
   - 日志级别：在列表中，单击日志级别。支持的日志级别包括：
     - 致命
     - 错误
     - 警告
     - 信息
     - 调试
     - 跟踪
     - 关
   - 包括记录器：键入要包括在自定义记录器中的特定记录器，或将此字段留空以包括所有记录器。
4. 单击添加。自定义记录器将添加到自定义记录器表格中。



删除自定义日志记录器

1. 在日志设置页面上，展开自定义记录器。
2. 选择要删除的自定义记录器。
3. 单击删除。此时将显示一个对话框，询问您是否要删除该自定义日志记录器。单击确定。

> 重要：
>
> 此操作无法撤消。

移动服务提供商

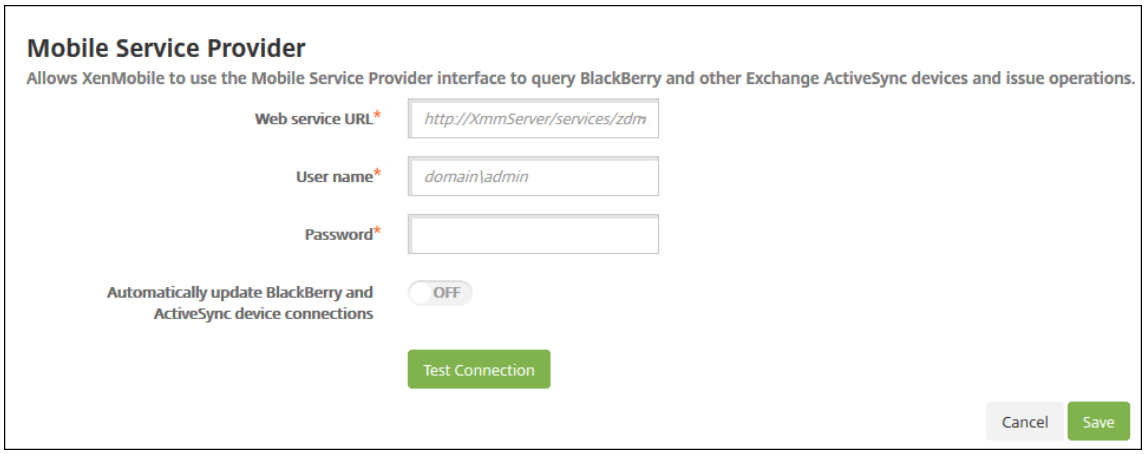
January 5, 2022

可以启用 XenMobile 以使用移动服务提供商界面来查询黑莓和 Exchange ActiveSync 设备并发出操作。

例如，您的组织可能有 1000 个用户，每个用户可能使用一个或多个设备。在您向每个用户传达其必须向 XenMobile 注册其设备以进行管理之后，XenMobile 控制台上将显示用户注册的设备数。通过配置此设置，您可以确定有多少设备连接到 Exchange Server。这样，您可以执行以下操作：

- 确定是否有用户仍需要注册其设备。
- 向连接到 Exchange Server 的用户设备发出命令，例如数据擦除。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击移动服务提供商。此时将显示移动服务提供商页面。



3. 配置以下设置：
   - **Web 服务 URL**：键入 Web 服务的 URL，例如 `https://<XmmServer>/services/xdmservice`
   - 用户名：以 domain\admin 格式键入用户名。
   - 密码：键入密码。

- 自动更新黑莓和 **ActiveSync** 设备连接：选择是否自动更新设备连接。默认值为关。
- 单击测试连接以验证连接性。

4. 单击保存。

报告

August 10, 2020

XenMobile 提供以下预定义报告，您可以利用这些报告分析应用程序和设备部署情况。每个报告都显示为一个表格和一个图表。您可以按列对表格进行排序和过滤。可以从更加详细的信息中选择图表中的元素。

- 总应用程序部署尝试次数：列出用户尝试在其设备上安装的已部署应用程序。
- 应用程序 **(**按平台**)**：按设备平台和版本列出应用程序和应用程序版本。
- 应用程序 **(**按类型**)**：按版本、类型和类别列出应用程序。
- 设备注册：列出所有已注册的设备。
- 设备和应用程序：列出正在运行托管应用程序的设备。
- 不活动设备：在 XenMobile Server 属性 device.inactivity.days.threshold 指定的天数内没有任何活动的设备的列表。
- 已越狱/获得 **Root** 权限的设备：列出已越狱的 iOS 设备和已获得 Root 权限的 Android 设备。
- 条款和条件：列出接受条款和条件协议以及拒绝条款和条件协议的用户。可以选择图表的各个区域以查看更多详细信息。
- 排名前 **10** 的应用程序：部署失败 - 最多列出 10 个部署失败的应用程序。
- 被设备和用户加入黑名单的应用程序：列出用户的用户设备上的阻止的应用程序。

  > 注意：
  >
  > XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们正在将即将发布的版本中的这些术语更改为“阻止列表”和“允许列表”。

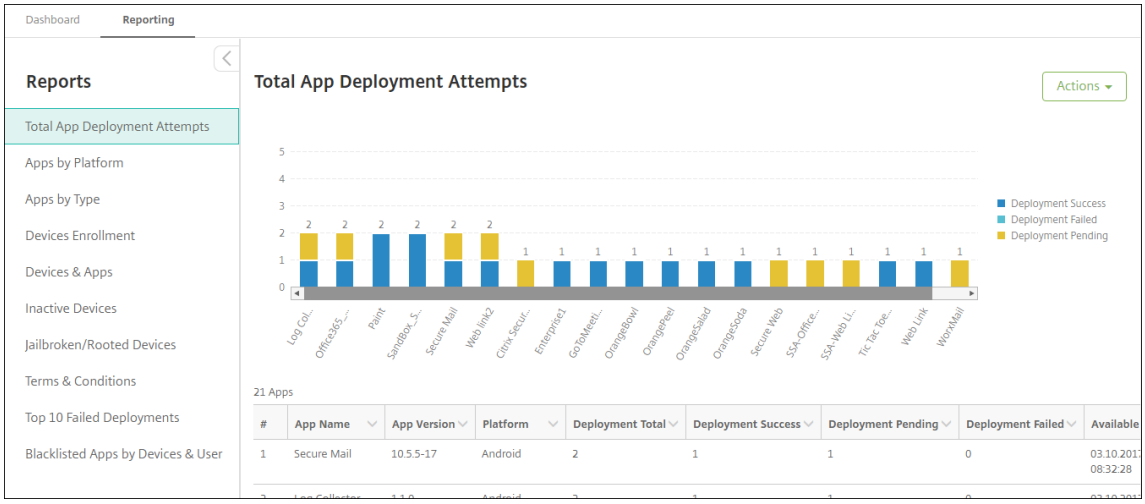
- 不合规设备：列出不符合合规性标准的设备，例如设备是否越狱、运行的操作系统版本以及设备是否具有通行码。

可以使用.csv 格式导出每个表格中的数据，这些数据可以使用 Microsoft Excel 等程序打开。可以使用 PDF 格式导出每个报告的图表。

生成报告

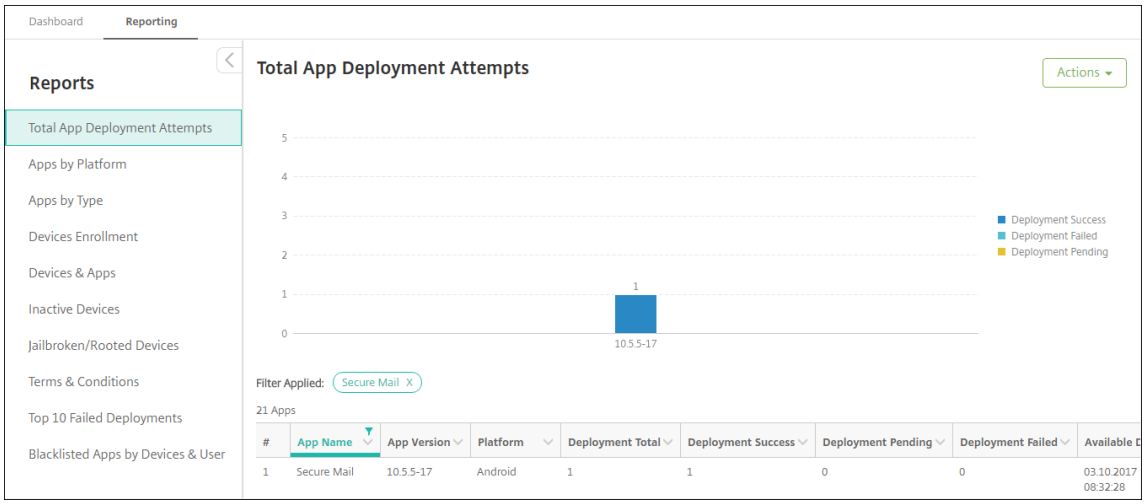
1. 在 XenMobile 控制台中，单击分析 **>** 报告。此时将显示报告页面。

2. 单击要生成的报告。

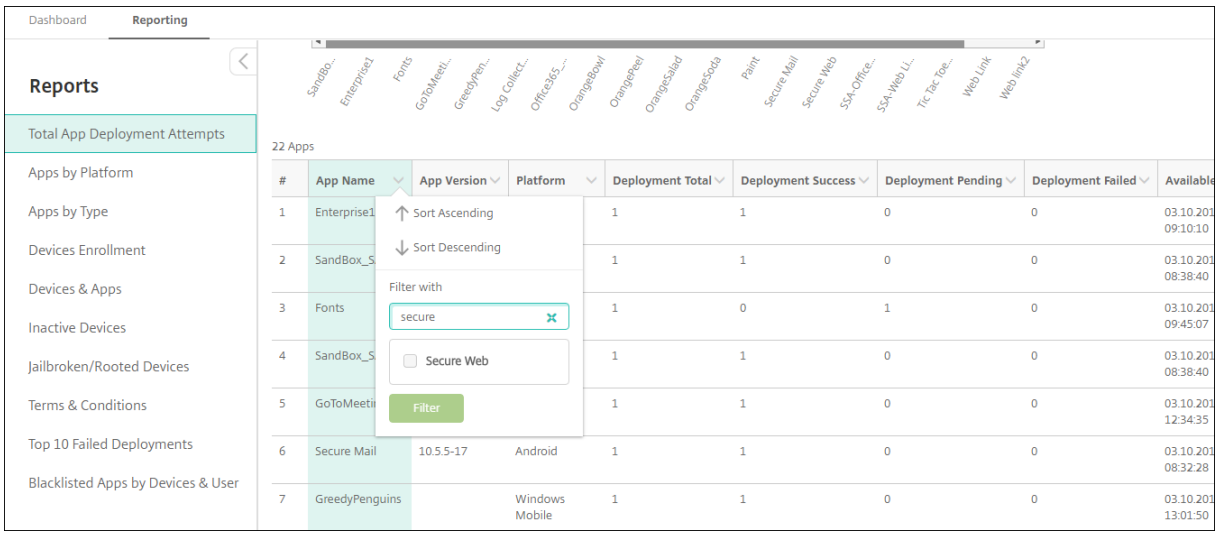


查看报告的更多详细信息

1. 单击图表的各个区域以深入查看更多详细信息。

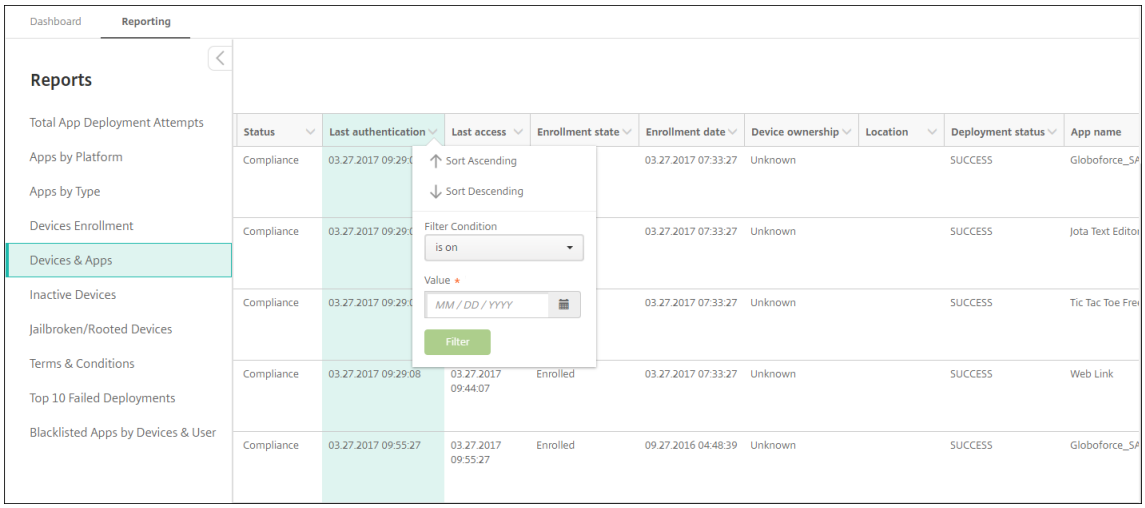


要对表格列进行排序、过滤或搜索，请单击列标题

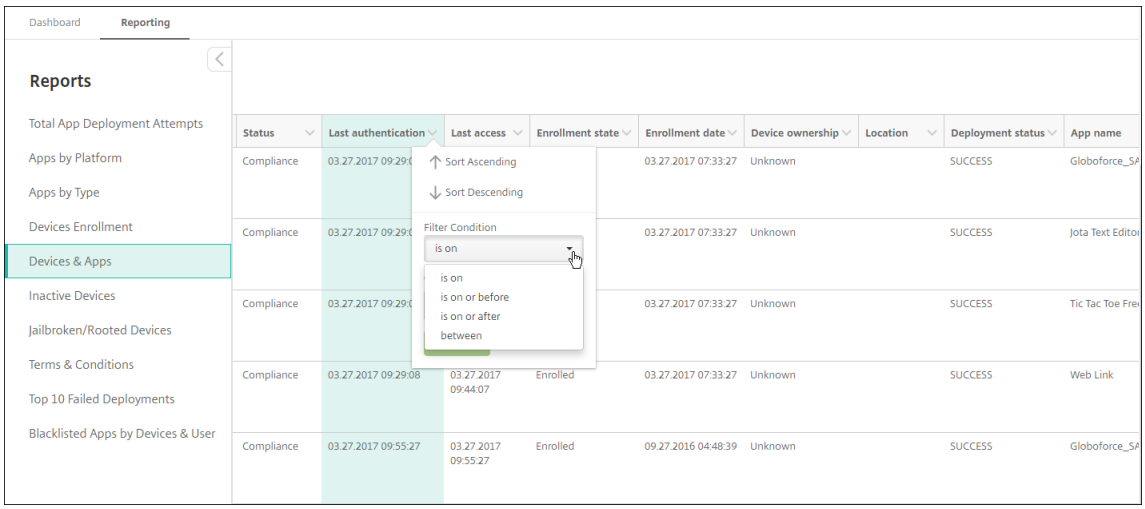


按日期过滤报告

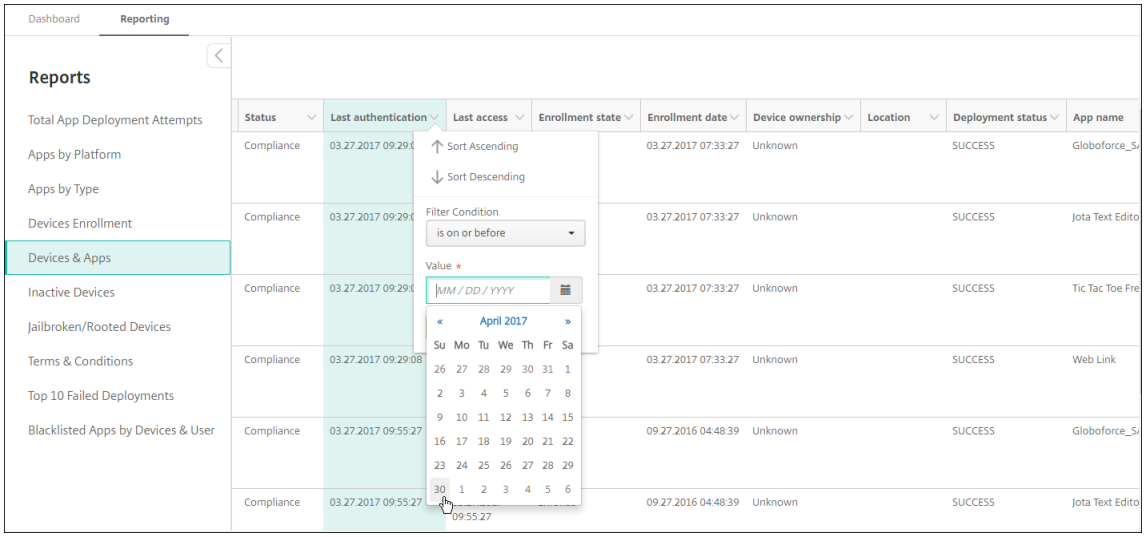
1. 单击列标题以查看过滤设置。



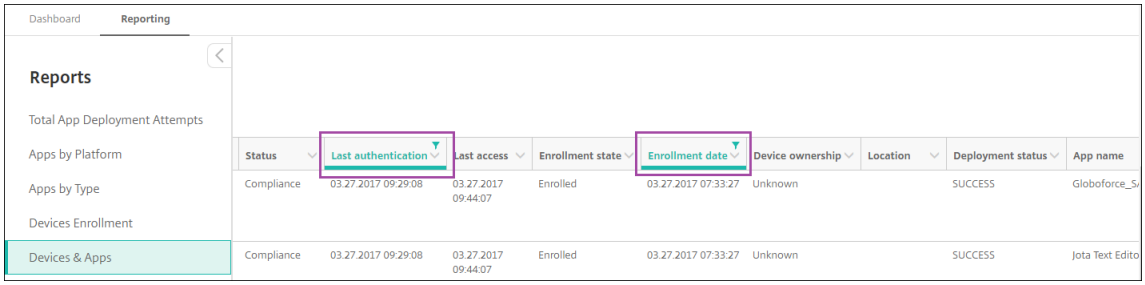
2. 在过滤条件中，选择要限制报告的日期的方式。



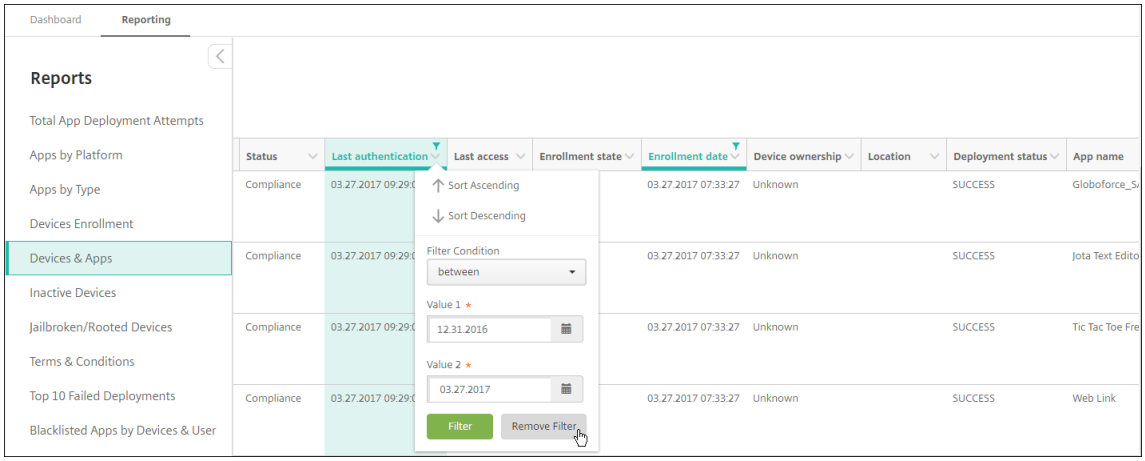
3. 使用日期选择器指定日期。



4. 带日期过滤器的列将按以下示例所示进行显示。

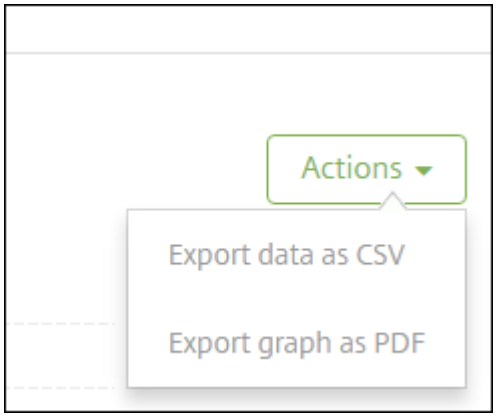


5. 要删除过滤器，请单击列标题，然后单击删除过滤器。



导出图表或表格

- 要导出 PDF 格式的图表，请依次单击操作和将图表导出为 **PDF**。
- 要导出 CSV 格式的表格数据，请依次单击操作和将数据导出为 **CSV**。



> 重要：
>
> 虽然可以使用 SQL Server 来创建自定义报告，但 Citrix 不建议使用此方法。Citrix 不发布架构，但是可以更改架构而不另行通知。如果您决定继续使用此报告方法，请务必使用只读帐户运行 SQL 查询。请注意，需要一段时间才能运行的包含多个 JOIN 的查询在该时间段内将影响 XenMobile Server 的性能。

SNMP 监视

April 14, 2020

可以在 XenMobile Server 中启用 SNMP 监视以允许监视系统，从而查询和获取与您的 XenMobile 节点有关的信息。这些查询使用“处理器负载”、“平均负载”、“内存使用率”和“连接”等参数。有关 SNMP v3 的详细信息（例如，身份验证和加密规范），请参阅 SNMP 的官方文档 RFC 3414。

> 注意：
>
> XenMobile Server 10.8 及更高版本支持 SNMP v3 监视功能。

您可以使用支持 SNMP 监视的各种监视应用程序（例如 SCOM）。有关配置 SCOM 的详细信息，请参阅此 Citrix 支持知识中心文章。

必备条件

配置以下 TCP 端口：

- 端口 **161 (UDP)**：用于使用 UDP 协议的 SNMP 流量。来源为 SNMP 管理器，目标为 XenMobile。
- 端口 **162 (UDP)**：用于从 XenMobile 向 SNMP 管理器发送 SNMP 陷阱警报。来源为 XenMobile，目标为 SNMP 管理器。

有关 XenMobile 端口配置的详细信息，请参阅端口要求。

要查看包括 SNMP 的本地 XenMobile 部署的体系结构图，请参阅面向本地部署的参考体系结构。

设置 SNMP 的常规步骤如下。

1. 添加用户：用户继承接收陷阱和监视 XenMobile Server 的权限。
2. 添加 **SNMP** 管理器以接收陷阱：陷阱是指 XenMobile 在您的 XenMobile 节点超出用户定义的最大阈值时生成的警报。
3. 将 **SNMP** 管理器配置为与 **XenMobile** 交互： XenMobile Server 使用某些管理信息库 (MIB) 执行操作。可从 XenMobile 控制台中的设置 **> SNMP** 配置页面下载 MIB。然后使用 MIB 导入程序将 MIB 导入到 SNMP 管理器中。

   > 注意：
   >
   > 每个 SNMP 管理器都有各自的 MIB 导入程序。

4. 启用陷阱：您在 XenMobile 控制台中启用陷阱并根据您的环境定义时间间隔和阈值。
5. 在第三方 **SNMP** 管理器中查看陷阱：要查看陷阱，请检查 SNMP 管理器。但是，在某些管理器中，您可以配置设置以在管理器外部启用通知。例如，可以将通知配置为在电子邮件中显示。

可以从 XenMobile 中生成以下陷阱。

陷阱名称：处理器负载

- 监视对象 **ID (OID)**： .1.3.6.1.2.1.25.3.3.1.2
- 说明：监视用户定义的时间间隔内系统的 CPU 负载。如果负载超出自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称：一分钟内的平均负载

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.2021.10.1.5.1

- 说明：监视用户定义的时间间隔内 1 分钟时间的系统平均负载。如果平均负载超出自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称：五分钟内的平均负载

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.2021.10.1.5.2
- 说明：监视用户定义的时间间隔内 5 分钟时间的系统平均负载。如果平均负载超出自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称： 15 分钟内的平均负载

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.2021.10.1.5.3
- 说明：监视用户定义的每个时间间隔内 15 分钟时间的系统平均负载。如果平均负载超出自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称：可用内存总量

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.2021.4.11
- 说明：监视用户定义的每个时间间隔内的可用内存。如果可用内存低于自定义阈值，XenMobile 将生成 SNMP 陷阱。注意：可用内存总量包括 RAM 和交换内存（虚拟内存）。要检索交换内存总量，可以使用 SNMP OID .1.3.6.1.4.1.2021.4.3 进行查询。要检索可用的交换内存，可以使用 SNMP OID .1.3.6.1.4.1.2021.4.4 进行查询

陷阱名称：已用磁盘存储总量

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.2021.9.1.9.1
- 说明：监视用户定义的每个时间间隔内的系统磁盘存储。如果磁盘存储超过自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Java 堆内存使用量

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.2.4.0
- 说明：监视用户定义的每个时间间隔内 XenMobile 的 Java 虚拟机 (JVM) 堆内存使用量。如果使用量超过自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Java 元空间使用量

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.2.5.0
- 说明：监视用户定义的每个时间间隔内 XenMobile 的元空间使用量。如果使用量超过阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称： LDAP 连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.1.0
- 说明：监视用户定义的每个时间间隔内 LDAP 服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： DNS 连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.2.0

- 说明：监视用户定义的每个时间间隔内 DNS 服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Google 应用商店服务器连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.3.0
- 说明：监视用户定义的每个时间间隔内 Google 应用商店服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Windows Phone 应用商店连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.4.0
- 说明：监视用户定义的每个时间间隔内 Windows Phone 应用商店服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Windows Tab 应用商店连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.5.0
- 说明：监视用户定义的时间间隔内 Windows Tab 应用商店服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Windows 安全令牌服务器连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.6.0
- 说明：监视用户定义的时间间隔内 Windows 安全令牌服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Windows 通知服务器连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.7.0
- 说明：监视用户定义的时间间隔内 Windows 通知服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Apple 推送通知服务器 (APNs) 连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.8.0
- 说明：监视用户定义的时间间隔内 APNs 与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Apple 反馈服务器连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.9.0
- 说明：监视用户定义的时间间隔内 Apple 反馈服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Apple 应用商店服务器连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.10.0
- 说明：监视用户定义的时间间隔内 Apple 应用商店服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： XenMobile 数据库连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.11.0
- 说明：监视用户定义的时间间隔内 XenMobile 数据库与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Firebase Cloud Messaging 服务器连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.12.0
- 说明：监视用户定义的时间间隔内 Firebase Cloud Messaging 服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Citrix 许可证服务器连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.13.0
- 说明：监视用户定义的时间间隔内 Citrix 许可证服务器与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Citrix Gateway 连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.15.0
- 说明：监视用户定义的时间间隔内 Citrix Gateway 与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： XenMobile 节点间连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.16.0
- 说明：监视用户定义的时间间隔内 XenMobile 群集节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： XenMobile Tomcat 节点服务连接

- 监视对象 **ID (OID)**： .1.3.6.1.4.1.3845.5.1.1.18.17.0
- 说明：监视用户定义的时间间隔内 XenMobile Tomcat 节点服务与 XenMobile 节点之间的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

要在配置 SNMP 阈值时实现最佳服务器性能，请谨记以下几点要素：

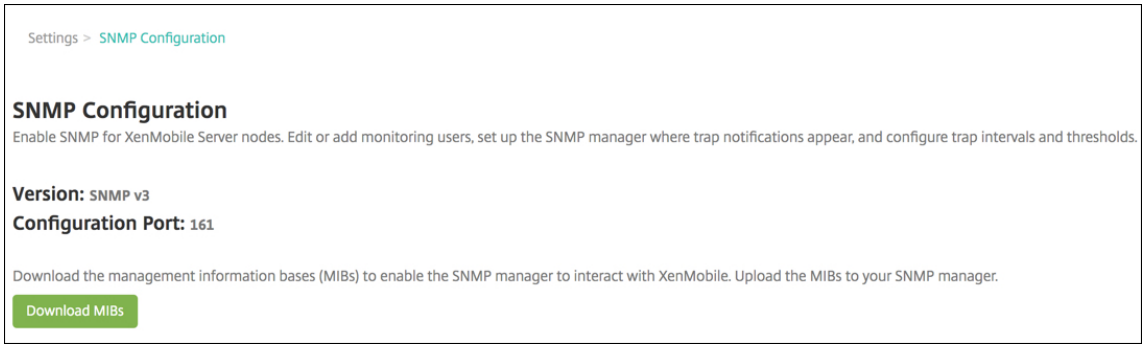
- 调用的频率
- 要收集的陷阱数据和阈值检查次数
- 节点间通信机制
- 连接检查的频率
- 检查过程中任何失败的超时值

添加 **SNMP** 用户

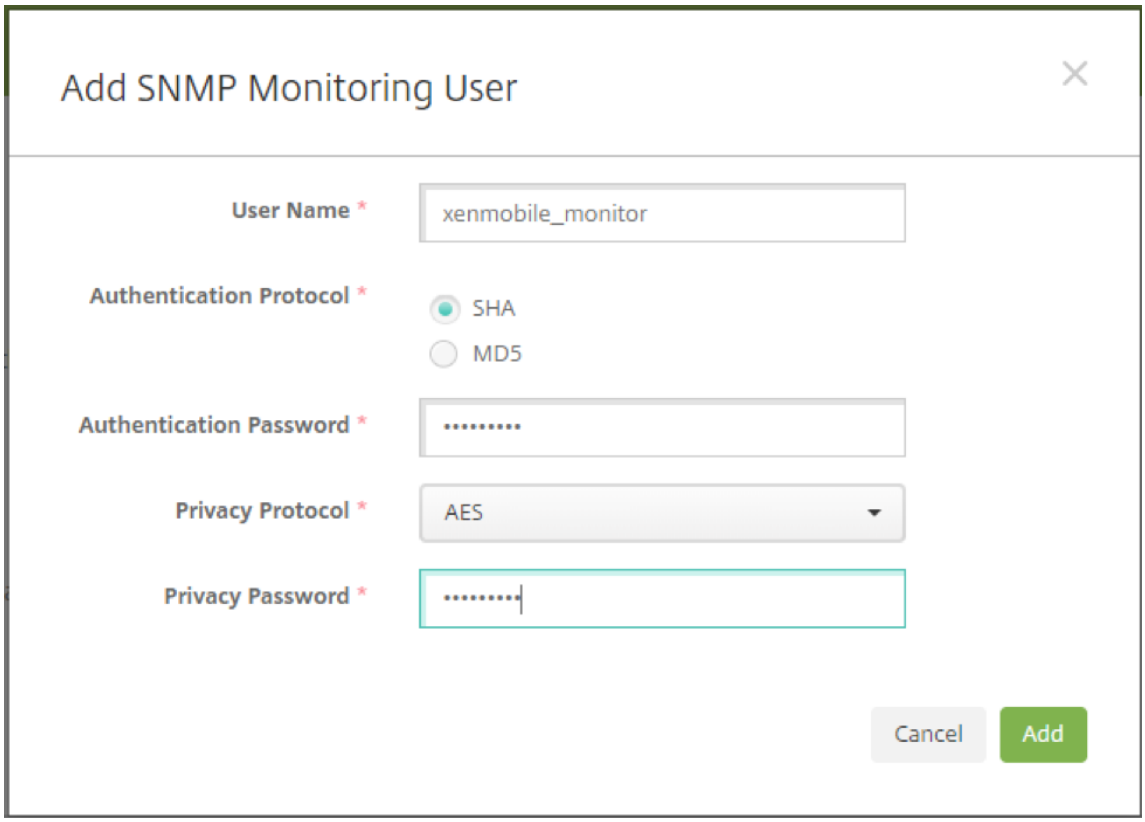
SNMP 用户与 SNMP 管理器交互并接收陷阱。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。

2. 在监视下方，单击 **SNMP** 配置。此时将显示 **SNMP** 配置页面。



3. 在 **SNMP** 监视用户下方，单击添加。
4. 在添加 **SNMP** 监视用户对话框中，配置以下设置：



用户名：用于登录 SNMP 管理器的用户名。虽然可以在用户名中使用字母数字字符、下划线和连字符，但不能使用空格和其他字符。

> 注意：
>
> 不能添加用户名 “xmsmonitor”，因为 XenMobile 保留该名称供内部使用。

身份验证协议：

- **SHA**（推荐）
- **MD5**

身份验证密码：键入 8 到 18 个字符的密码。可以包括字母数字字符和特殊字符。

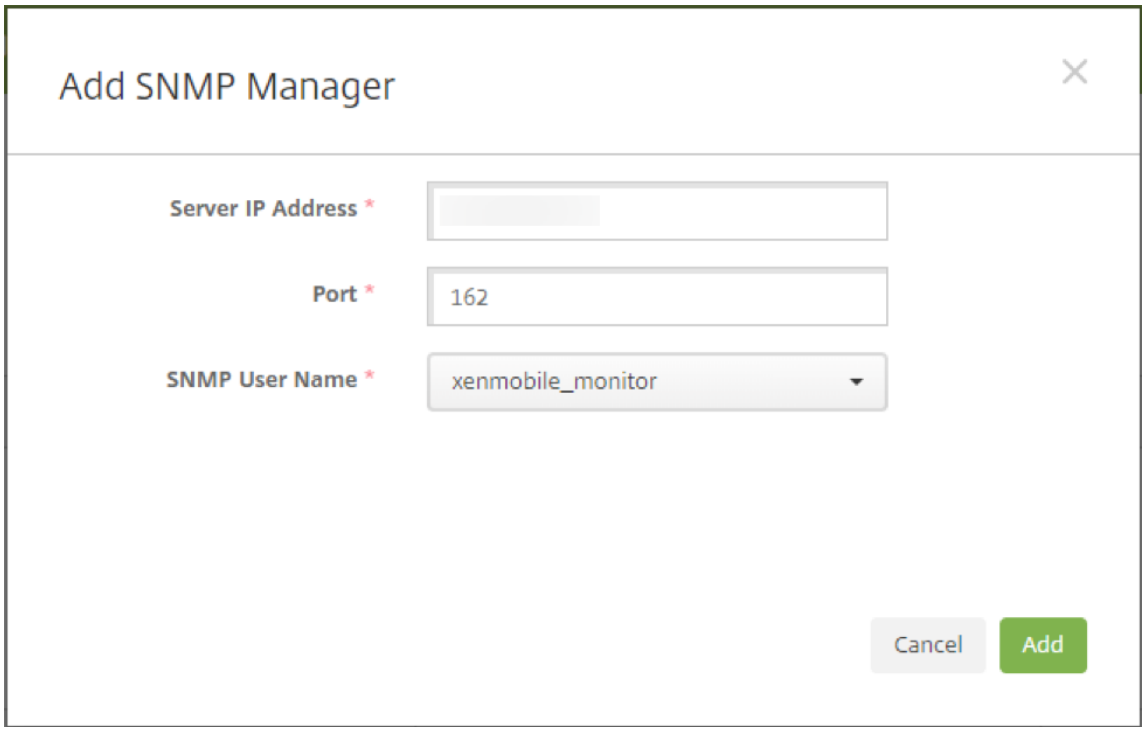
隐私协议：

- **DES**
- **AES 128**（推荐）

隐私密码：键入 8 到 18 个字符的密码。可以包括字母数字字符和特殊字符。

添加 **SNMP** 管理器

1. 在 **SNMP** 管理器下方，单击添加。
2. 在添加 **SNMP** 管理器对话框中，配置以下设置：



服务器 **IP** 地址：键入 SNMP 管理器的 IP 地址。

端口：根据需要更改端口号。默认值为 162。

SNMP 用户名：选择用户访问管理器时使用的名称。

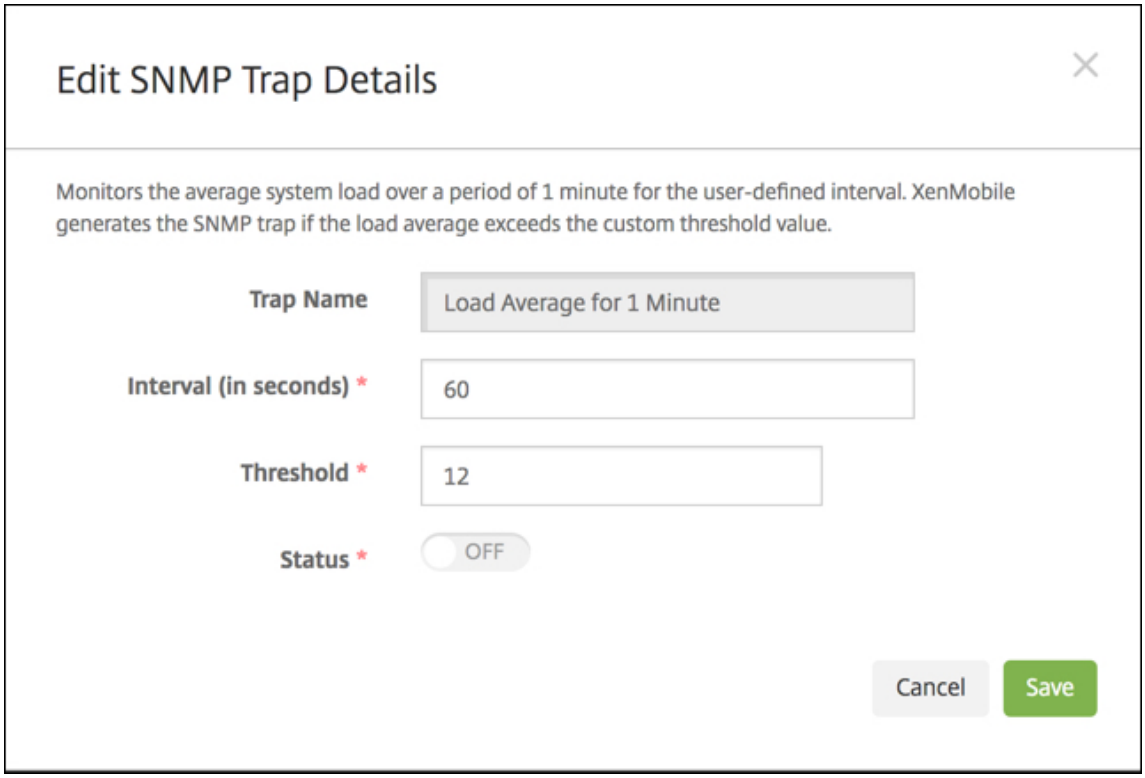
启用和配置 **SNMP** 陷阱

要帮助确定适用于您的环境的合适陷阱设置，请参阅可扩展性和性能。例如，要监视 XenMobile 在 1 分钟内的平均负载，可以启用“1 分钟内的平均负载”并提供阈值。如果 XenMobile Server 的“1 分钟内的平均负载”超出指定阈值，您将在配置的 SNMP 管理器中接收陷阱。

1. 要启用各个陷阱，请执行以下操作之一：

- 选中参数旁边的复选框，然后单击启用。
- 要启用列表中的所有陷阱，请选中顶部的复选框，然后单击启用。

2. 要编辑某个陷阱，请选中该参数，然后单击编辑。
3. 在编辑 **SNMP** 陷阱详细信息对话框中，可以编辑各个陷阱的阈值。



陷阱名称：陷阱的名称。不能编辑此字段。

时间间隔 **(**秒**)**：允许的范围为 60 到 86400（24 小时）。

阈值：只能更改以下陷阱的阈值：

- 处理器负载
- 1 分钟内的平均负载
- 5 分钟内的平均负载
- 15 分钟内的平均负载
- 可用内存总量
- 已用磁盘存储总量
- Java 堆内存使用量
- Java 元空间使用量

状态：选择开可对陷阱启用 SNMP 监视。选择关可禁用监视。

有关使用 SNMP 监视 XenMobile 的详细有用信息，请参阅此博客文章。

支持包

December 21, 2020

要向 Citrix 报告问题或解决问题，请创建一个支持包。然后，将该支持包上载到 Citrix Insight Services (CIS)。

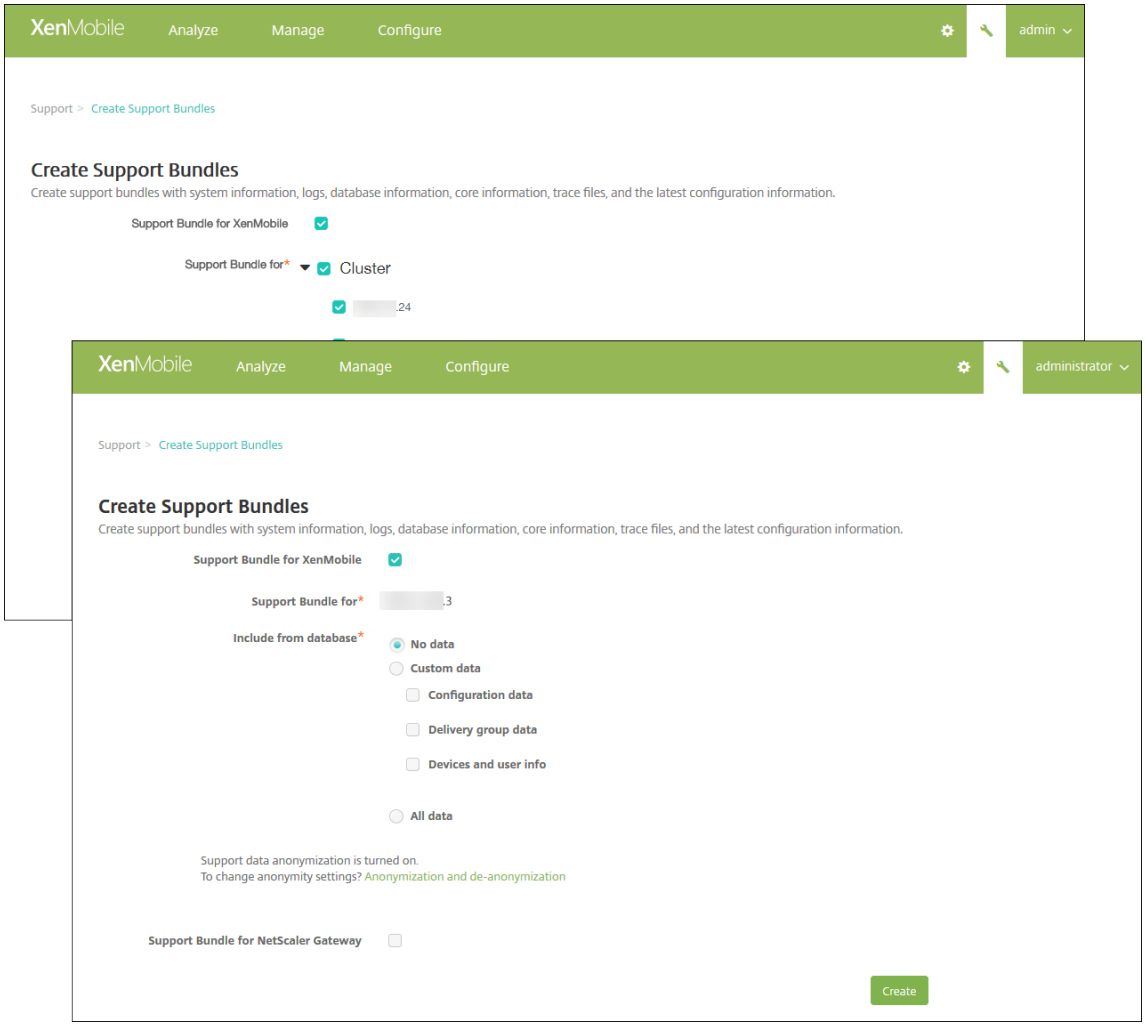
默认情况下，支持包最多包含以下文件的 100 个备份存档。这些文件的默认大小为 10 MB。

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

当支持包包含每种目录的 100 个日志存档时，日志文件将回滚。如果配置的最大日志文件数量较低，XenMobile 将立即删除该节点的无关日志文件。要配置日志文件的数量，请转至故障排除和支持 **>** 日志设置。

要创建支持包，请执行以下操作：

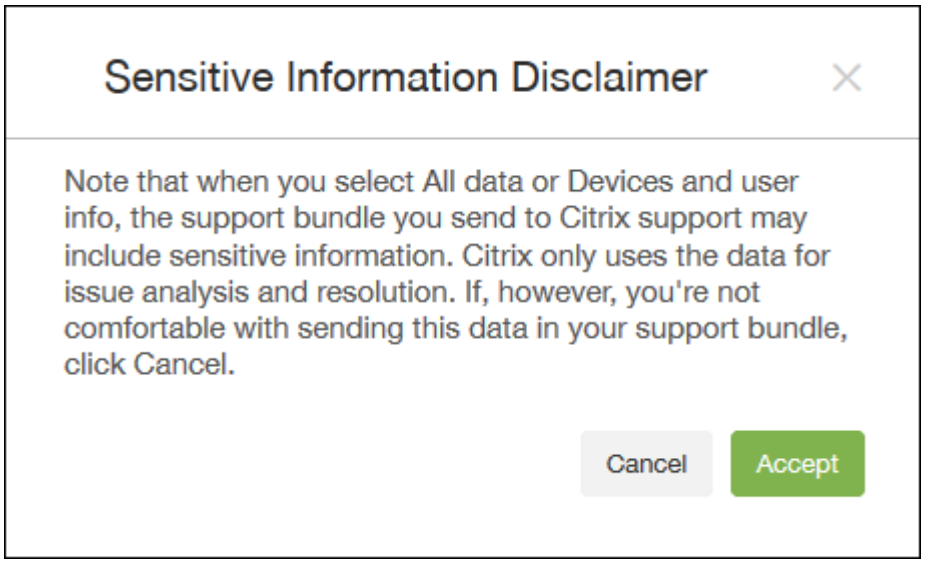
1. 在 XenMobile 控制台中，单击右上角的扳手图标。此时将显示支持页面。
2. 在支持页面上，单击创建支持包。此时将显示创建支持包页面。如果 XenMobile 环境包含加入群集的节点，将显示所有节点。



3. 确保选中适用于 **XenMobile** 的支持包复选框。
4. 如果 XenMobile 环境包含群集节点，在适用于此对象的支持包中，可以选择要从中提取数据的所有节点或任何节点组合。
5. 在包含的数据库内容中，执行以下操作之一：
   - 单击无数据。
   - 单击自定义数据。默认选中所有选项。
     - 配置数据库：包括证书配置和设备管理器策略。
     - 交付组数据：包括应用程序交付组信息，其中包含应用程序类型和应用程序交付策略详细信息。
     - 设备和用户信息：包括设备策略、应用程序、操作和交付组。
   - 单击所有数据。

> 注意：
>
> 如果选择设备和用户信息或所有数据，并且这是您创建的第一个支持包，则会显示敏感信息免责声明对话框。阅读免责声明，然后单击接受或取消。如果单击取消，支持包将无法上载到 Citrix。如果单击接受，则

> 可以将支持包上载到 Citrix，并且下次创建包含设备或用户数据的支持包时不会再出现免责声明。

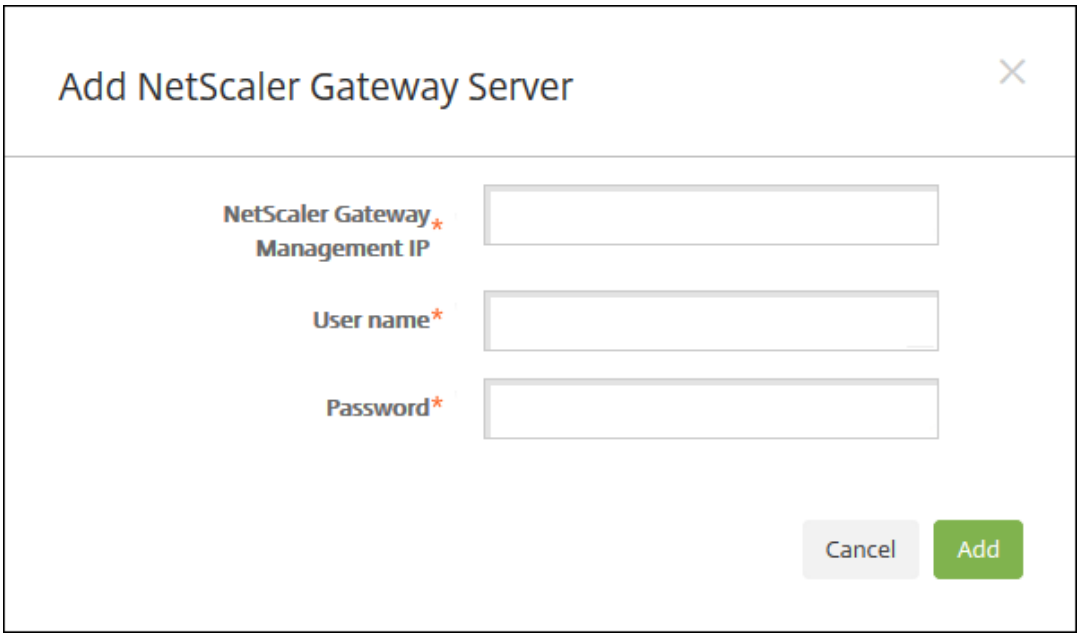


6. 支持数据匿名已打开选项指示默认设置为对数据进行匿名处理。数据匿名表示敏感用户、服务器和网络数据在支持包中设为匿名。

   要更改此设置，请单击匿名和取消匿名。有关数据匿名的详细信息，请参阅匿名化支持包中的数据。

7. 要包含来自 Citrix Gateway 的支持包，请选中适用于 **Citrix Gateway** 的支持包复选框，然后执行以下操作：

   a) 单击添加。此时将显示添加 **Citrix Gateway** 服务器对话框。



   b) 在 **Citrix Gateway** 管理 **IP** 中，键入要从中提取支持包数据的 Citrix Gateway 的 Citrix ADC 管理 IP 地址。

> 注意：
>
> 如果要从已经添加的 Citrix Gateway 服务器创建支持包，系统会提供 IP 地址。

c) 在用户名和密码中，键入访问运行 Citrix Gateway 的服务器所需的用户凭据。

> 注意：
>
> 如果要从已经添加的 Citrix Gateway 服务器创建支持包，系统会提供用户名。

8. 单击添加。新的 Citrix Gateway 支持包将添加到表格中。
9. 重复步骤 7 以添加更多 Citrix Gateway 支持包。
10. 单击创建。将创建支持包，并显示两个新按钮：上载到 **CIS** 和下载到客户端。

将支持包上载到 **Citrix Insight Services**

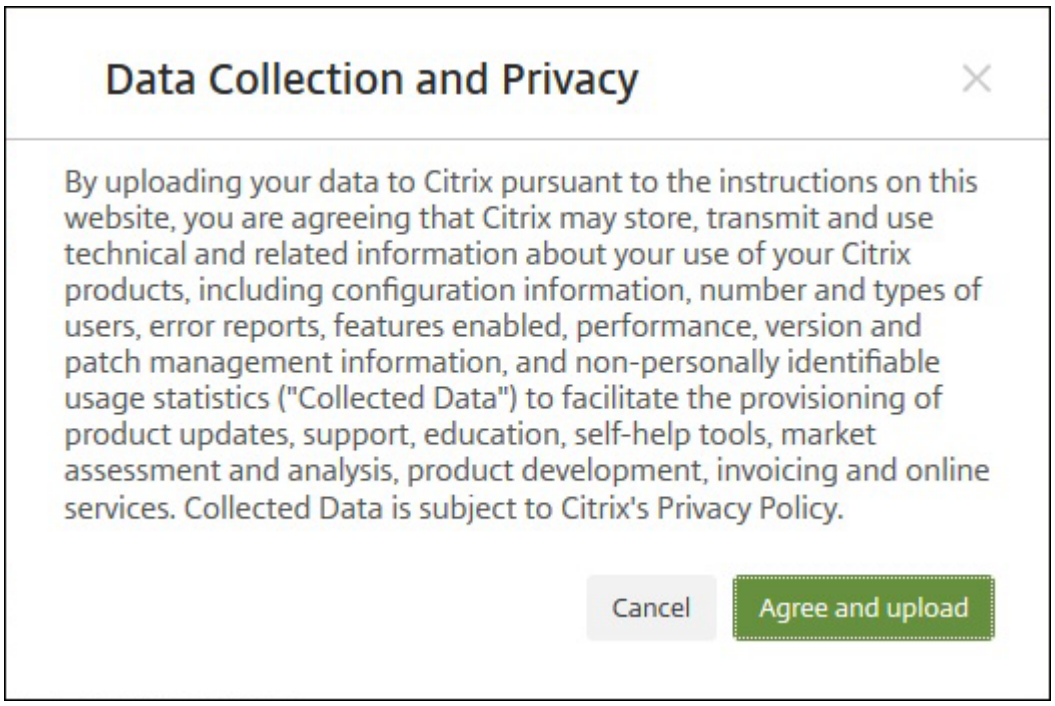
创建支持包后，可以将支持包上载到 Citrix Insight Services (CIS) 或将其下载到您的计算机。

从 XenMobile 上载到 CIS 是通过 SSL 出站连接完成的。打开与 CIS 服务器 IP 地址（52.88.24.76、52.88.118.220、52.11.72.119）进行通信的端口 443。如果您有一个用于 HTTPS 通信的代理，请验证该代理是否能够访问 CIS 服务器 IP 地址。

下面的步骤显示如何将支持包上载到 CIS。上载到 CIS 需要使用 My Citrix ID 和密码。

1. 在创建支持包页面上，单击上载到 **CIS**。此时将显示上载到 **Citrix Insight Services (CIS)** 对话框。
2. 在用户名中，键入 My Citrix ID。
3. 在密码中，键入 My Citrix 密码。
4. 如果要将此支持包与现有服务请求号码关联，请选中与 **SR** 编号关联复选框，并在显示的两个新字段中执行以下操作：
   - 在 **SR** 编号中，键入要与此支持包关联的八位数服务请求号码。
   - 在 **SR** 说明中，键入 SR 的说明。
5. 单击上载。

   如果这是您第一次将支持包上载到 CIS，并且您尚未通过其他产品在 CIS 上创建帐户和接受“数据收集和隐私声明”协议，系统会显示以下对话框；您必须接受此协议才能开始上载操作。如果您已经具有 CIS 帐户并且之前接受过此协议，支持包会立即开始上载。



6. 阅读协议，然后单击同意并上载。将上载支持包。

将支持包下载到您的计算机

创建支持包之后，可以将此包上载到 CIS 或将其下载到您的计算机。如果希望自己进行故障排除，可以将支持包下载到您的计算机。

在创建支持包页面上，单击下载到客户端。支持包将下载到您的计算机。

支持包包含分析值各不相同的文件。请参见下表，获取各文件及其分析值的列表。

文件名	类型	说明	值
DbDump.json	JSON 数据库转储	用户/设备/应用程序信息	高
Garbage.html	HTML 文件	Java 垃圾回收器	低
MemoryInfo.html	HTML 文件	内存使用情况 - java 相关的内存使用情况	高
MultiNodeClusterInfo.html	HTML 文件	群集配置	高
Patches.html	HTML 文件	修补程序信息。Better to xmspatches.txt	高
pg_dump0.sql	PG 转储	默认 Postgress 实例转储	中

文件名	类型	说明	值
rt_db/*	DB 副本（冗余，这是 pg_dump0.sql 的二进制表示形式）		不适用
sas_config/c3p0.properties	属性文件	C3P0 DB Config 属性	中
sas_config/catalina.pol	策略文件	Web 服务器 Catalina 策略 - 文件不更改	低
sas_config/catalina.properties	属性文件	Web 服务器 Catalina 属性 - 文件不更改	低
sas_config/ew-config.properties	属性文件	与 XM 服务器的配置有关的信息	高
sas_config/ew-config-reloadable.properties	属性文件	安全模型信息	高
sas_config/hazelcast.xr	XML 文件	Hazelcast 日志 - 认为用处不大。	低
sas_config/pki.xml	XML 文件	可以用于确定是否正在使用第三方 PKI 服务器。	高
sas_config/push_servic	XML 文件	推送服务 - 文件不更改	低
sas_config/server.xml	XML 文件	此处显示密码套件 - 与安全相关	高
sas_config/sftu_config/	属性文件	AppC 属性 - 文件不更改	低
sas_config/sftu_config/catalina.policy	策略文件	Catalina 策略 - 文件不更改	低
sas_config/sftu_config/	属性文件	Catalina 属性 - 文件不更改	低
sas_config/sftu_config/logging.properties	属性文件	日志记录属性 - 文件不更改	低
sas_config/sftu_config/	XML 文件	此处显示密码套件 - 与安全相关	高
sas_config/sftu_config/server_migration.xml	XML 文件	迁移信息	高
sas_config/sftu_config/	XML 文件	首次使用的用户设置	高
sas_config/sftu_config/tomcat-users.xml	XML 文件	TomCat 用户 - 文件不更改	低
sas_config/sftu_config/	XML 文件	Web - 文件不更改	低

文件名	类型	说明	值
sas_config/sftu.properties	属性文件	SFTU 配置属性	高
sas_config/variables.xml	XML 文件	变量 - 文件不更改	低
sas_config/web.xml	XML 文件	Webserver 相关信息	中
sas_log/AdminAuditLog	Linux 日志文件	任何配置更改	高
sas_log/create_sb_output.sh	Linux 日志文件	支持生成命令输出	低
sas_log/DebugLogFile.l	Linux 日志文件	所有功能日志	高
sas_log/HibernateStats.log	Linux 日志文件	Hibernatestats 日志	低
sas_log/kafka-consumer.log	Linux 日志文件	Kafka 日志	低
sas_log/kafka-server.log	Linux 日志文件	Kafka 日志	低
sas_log/kafka-topics.log	Linux 日志文件	Kafka 日志	低
sas_log/LPE.log	Linux 日志文件	LPE 日志	低
sas_log/migration.log	Linux 日志文件	迁移过程输出	中
sas_log/PlatformAuditLogFile.log	Linux 日志文件	后端审核级别信息	高
sas_log/PlatformDebug	文本文件	后端服务器相关的日志	高
sas_log/postgres.log	Linux 日志文件	PostGres 日志	中
sas_log/SFTU.log	Linux 日志文件	SFTU 日志	中
sas_log/tc1/catalina.log	Linux 日志文件	Catalina 日志	低
sas_log/tc1/console	Linux 日志文件	控制台	低
sas_log/tc1/host-manager.log	Linux 日志文件	主机管理器	低
sas_log/tc1/localhost.l	Linux 日志文件	LocalHost	低
sas_log/updates.log	Linux 日志文件	修补过程输出	中
sas_log/UserAuditLogF	Linux 日志文件	用户操作	高
sas_log/zookeeper.txt	文本文件	Zookeeper 日志	低
snmp/snmpd_etc_nets	属性文件	SNMP 配置属性	低
snmp/snmpd_privileges.conf	属性文件	SNMP 配置属性	低

文件名	类型	说明	值
sys_info/arp_entries.txt	文本文件	XMS 服务器中的 ARP 条目	中
sys_info/chrony.txt	文本文件	Chrony 日志	低
sys_info/diskspace_usa	文本文件	磁盘空间使用情况	高
sys_info/firewall_rules.txt	文本文件	在 XMS 中定义的防火墙规则	中
sys_info/interface_conf	文本文件	系统命令输出	中
sys_info/net_connections.txt	文本文件	系统命令输出	中
sys_info/root_account_	文本文件	系统命令输出	中
sys_info/routing_table.txt	文本文件	“高”值	高
sys_info/running_proce	文本文件	“高”值	高
sys_info/top.txt	文本文件	系统命令输出	中
ThreadDump.html	HTML 文件	不再使用。	低
ThreadDumpV2.html	HTML 文件	线程堆栈跟踪等	中
var_log/auth.log	Linux 日志文件	操作系统级别日志	中
var_log/boot.log	Linux 日志文件	操作系统级别日志	中
var_log/btmp	Linux 日志文件	操作系统级别日志	中
var_log/daemon.log	Linux 日志文件	操作系统级别日志	中
var_log/kern.log	Linux 日志文件	操作系统级别日志	中
var_log/lastlog	Linux 日志文件	操作系统级别日志	中
var_log/mail.log	Linux 日志文件	操作系统级别日志	中
var_log/sys.log	Linux 日志文件	操作系统级别日志	中
var_log/user.log	Linux 日志文件	操作系统级别日志	中
var_log/wtmp	Linux 日志文件	操作系统级别日志	中
version.txt	文本文件	XM 服务器版本	中
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	XML 文件	XMS 服务器上的连接检查结果	中
xmspatches.txt	文本文件	修补程序信息。	高

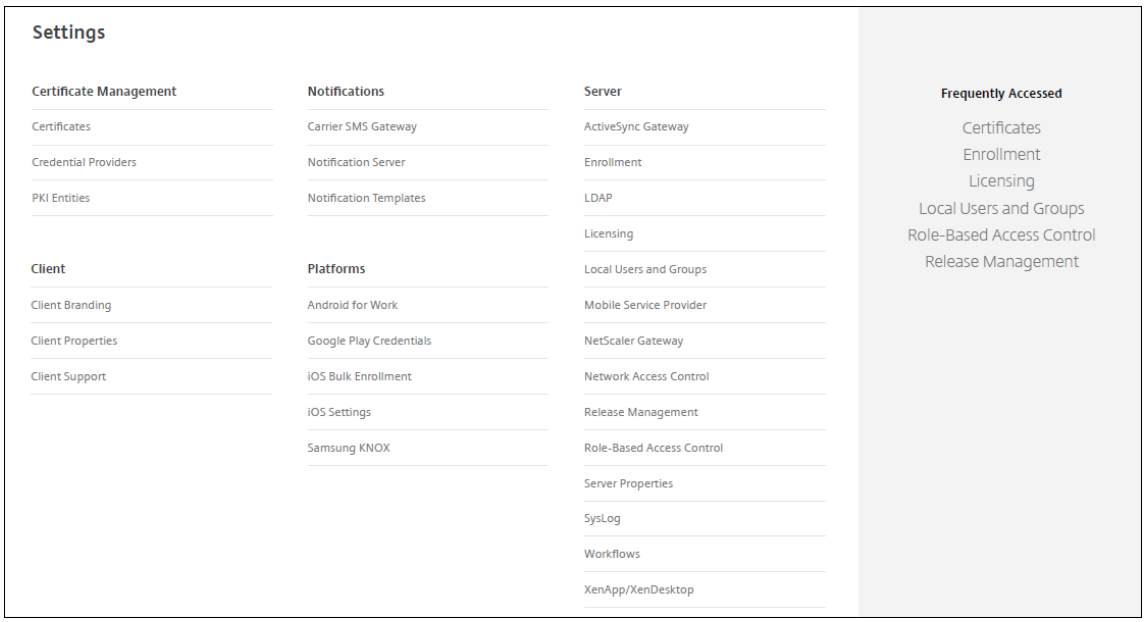
支持选项和远程支持

January 5, 2022

可以提供电子邮件地址，以便用户联系技术支持人员。当用户从其设备请求帮助时，他们会看到该电子邮件地址。

还可以配置用户如何将日志从其设备发送给技术支持人员。可以将日志配置为直接发送或者通过电子邮件发送。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。



2. 在客户端下方，单击客户端支持。此时将显示客户端支持页面。
3. 配置以下设置：
   - 支持电子邮件 **(IT** 技术支持**)**：键入 IT 技术支持联系人的电子邮件地址。
   - 将设备日志发送给 **IT** 技术支持人员：选择直接还是通过电子邮件发送设备日志。默认值为通过电子邮件。
     - 启用直接时，将显示“在 ShareFile（现在称为 Citrix Content Collaboration）上存储日志”对应的设置。如果在 Citrix Content Collaboration 上启用了应用商店日志，日志将直接发送到 Citrix Files。否则，日志将发送至 XenMobile，然后通过电子邮件发送给技术支持人员。此外，还将显示如果直接发送失败，请使用电子邮件选项（默认情况下启用）。如果不希望使用客户端电子邮件发送服务器问题的日志，可以禁用此选项。但是，如果禁用了此选项时出现服务器问题，则不会发送日志。
     - 启用通过电子邮件时，始终使用客户端电子邮件发送日志。
4. 单击保存。

远程支持

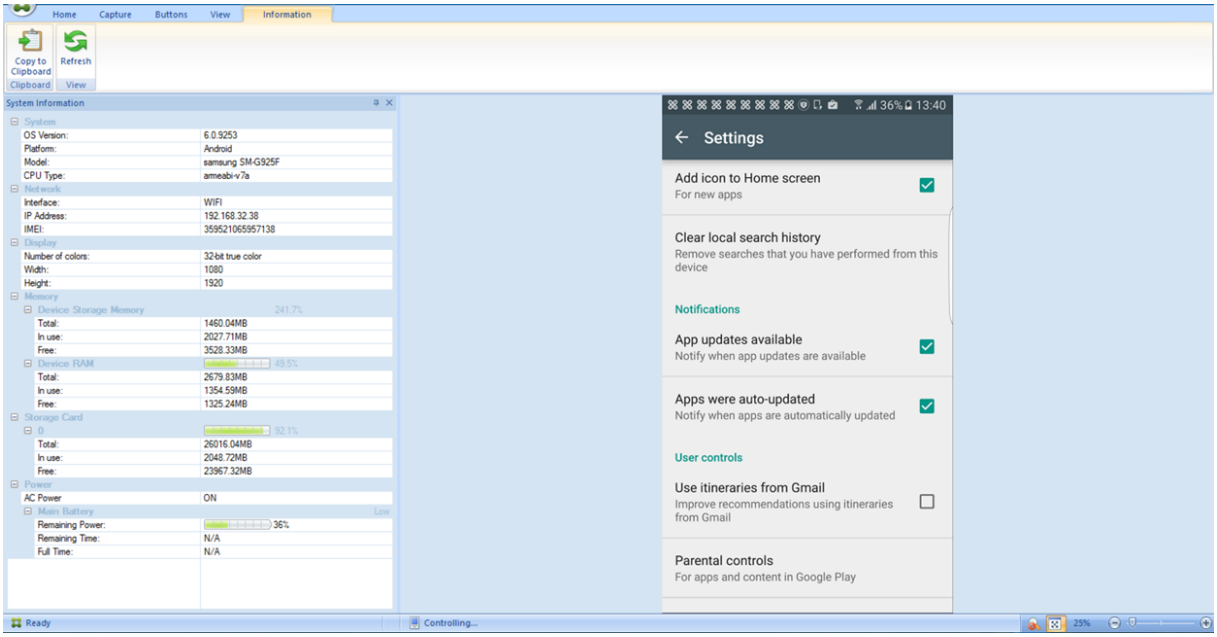
> 注意：
>
> 自 2019 年 1 月 1 日起，远程支持功能不再向新客户提供。现有客户可以继续使用此产品，但 Citrix 将不提供增强功能或修复。

对于本地 XenMobile Server 部署：通过远程支持，您的技术支持代表能够远程控制托管的 Windows CE 和 Android 移动设备。屏幕录像功能仅在 Samsung Knox 设备上受支持。

远程支持不适用于本地群集 XenMobile Server 部署。

在远程控制会话期间：

- 用户会在其移动设备上看到一个图标，指示远程控制会话处于活动状态。
- Remote Support 用户会看到 Remote Support 应用程序窗口以及显示受控设备的远程控制窗口。



使用 Remote Support，可以执行以下操作：

- 远程登录到用户设备并控制屏幕。用户可观看您在屏幕上的操作，这对于培训用户而言也很有帮助。
- 实时导航和修复远程设备。您可以更改配置、对操作系统问题进行故障排除、禁用或停止有问题的应用程序或进程。
- 通过远程禁用网络访问权限、停止恶意进程以及删除应用程序或恶意软件，可以隔立和遏制这些威胁，使其不会传播到其他移动设备。
- 远程启用设备响铃和拨打电话，以帮助用户找到设备。如果用户找不到设备，可以擦除设备以确保敏感数据不会受到损害。

Remote Support 还使技术支持人员能够执行以下操作：

- 显示 XenMobile 的一个或多个实例中所有已连接设备的列表。
- 显示系统信息，包括设备型号、操作系统级别、国际移动设备标识 (IMEI)、序列号、内存和电池状态及连接性。
- 显示 XenMobile 的用户和组。

- 运行设备任务管理器，可在其中显示活动进程、结束活动进程以及重新启动移动设备。
- 运行远程文件传输，包括移动设备与中央文件服务器之间的双向文件传输。
- 成批下载软件程序并安装到一个或多个移动设备上。
- 配置设备上的远程注册表项设置。
- 利用实时设备屏幕远程控制功能优化低带宽移动网络的响应时间。
- 显示大多数移动设备品牌和型号的设备外观。显示用于添加新设备型号和映射物理键的皮肤编辑器。
- 启用设备屏幕捕获、录制和播放，并能够捕获设备上的一系列交互操作以创建视频 AVI 文件。
- 利用共享白板、VoIP 语音通信和移动用户与技术支持人员之间的聊天功能举行实时会议。

远程支持的系统要求

Remote Support 软件可安装在满足以下要求的 Windows 计算机上。有关端口要求的信息，请参阅端口要求。

支持的平台：

- Intel Xeon/Pentium 4 -1 GHz 工作站类（最低要求）
- 最低 512 MB RAM
- 最低 100 MB 可用磁盘空间

支持的操作系统：

- Microsoft Windows 2003 Server Standard Edition 或 Enterprise Edition SP1 或更高版本
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 或更高版本
- Microsoft Windows Vista SP1 或更高版本
- Microsoft Windows 10 或 Windows 11
- Microsoft Windows 8
- Microsoft Windows 7

通过命令行安装 **Remote Support**

运行以下命令：

```
1 \*RemoteSupport\*.exe /S
```

RemoteSupport 为安装程序的名称。例如：

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

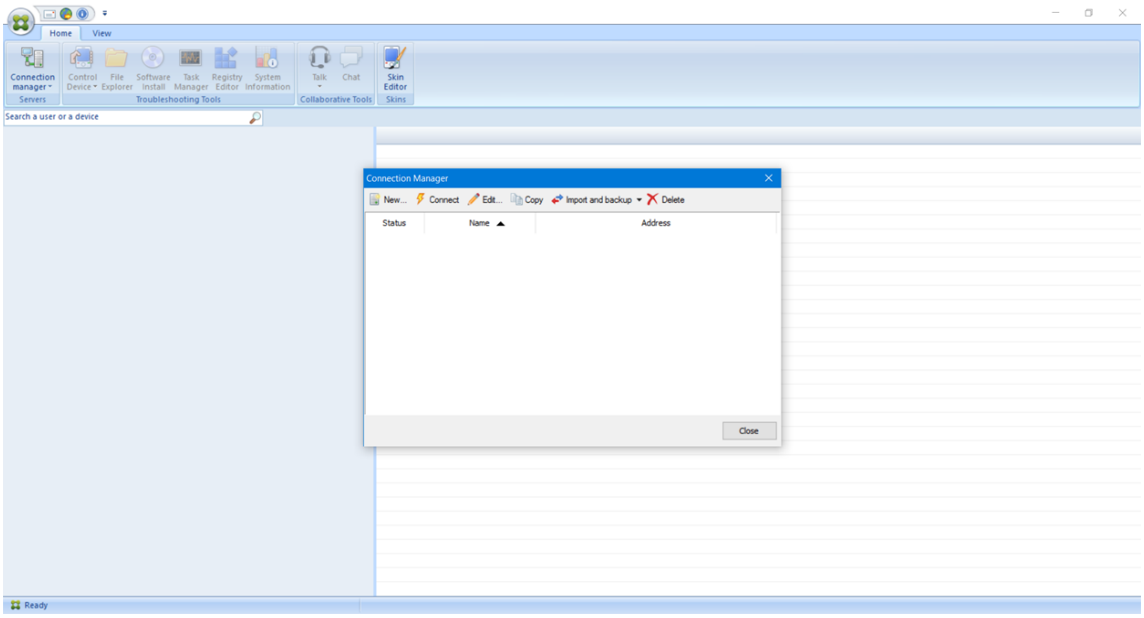
安装 Remote Support 软件时，可以使用以下变量：

- /S：使用默认参数无提示安装 Remote Support 软件。
- /D=dir: 指定自定义安装目录。

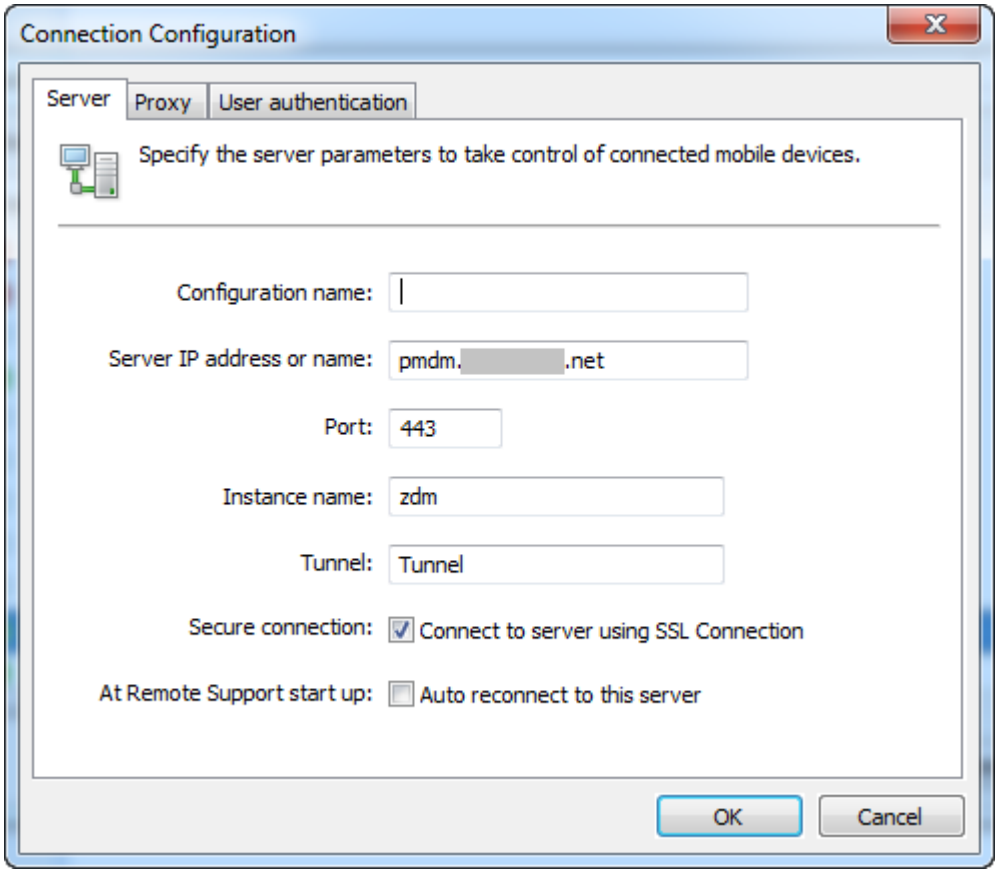
将 **Remote Support** 连接到 **XenMobile**

要建立与托管设备的远程支持连接，必须添加从 Remote Support 到用于管理设备的一台或多台 XenMobile Server 的连接。该连接在通道 MDM 策略（一项适用于 Android 和 Windows Mobile/CE 设备的设备策略）中定义的应用程序通道上运行。应先定义应用程序通道，才能将 Remote Support 连接到 XenMobile。有关详细信息，请参阅应用程序通道设备策略。

1. 启动 Remote Support 软件，并使用您的 XenMobile 凭据登录。
2. 在 **Connection Manager**（连接管理器）中，单击 **New**（新建）。



3. 在 **Connection Configuration**（连接配置）对话框中的 **Server**（服务器）选项卡上，键入以下值：
   a) 在 **Configuration name**（配置名称）中，键入配置条目的名称。
   b) 在 **Server IP address or name**（服务器 IP 地址或名称）中，键入 XenMobile Server 的 IP 地址或 DNS 名称。
   c) 在 **Port**（端口）中，键入在 XenMobile Server 配置中定义的 TCP 端口号。
   d) 如果 XenMobile 属于多租户部署的一部分，请在 **Instance name**（实例名称）中键入实例名称。
   e) 在 **Tunnel**（通道）中，键入通道策略的名称。
   f) 选中 **Connect to server using SSL Connection**（使用 SSL 连接连接到服务器）复选框。
   g) 选中 **Auto reconnect to this server**（自动重新连接此服务器）复选框，在 Remote Support 应用程序每次启动时连接到配置的 XenMobile Server。



4. 在 **Proxy**（代理）选项卡中，选择 **Use an http proxy server**（使用 HTTP 代理服务器），然后键入以下信息：

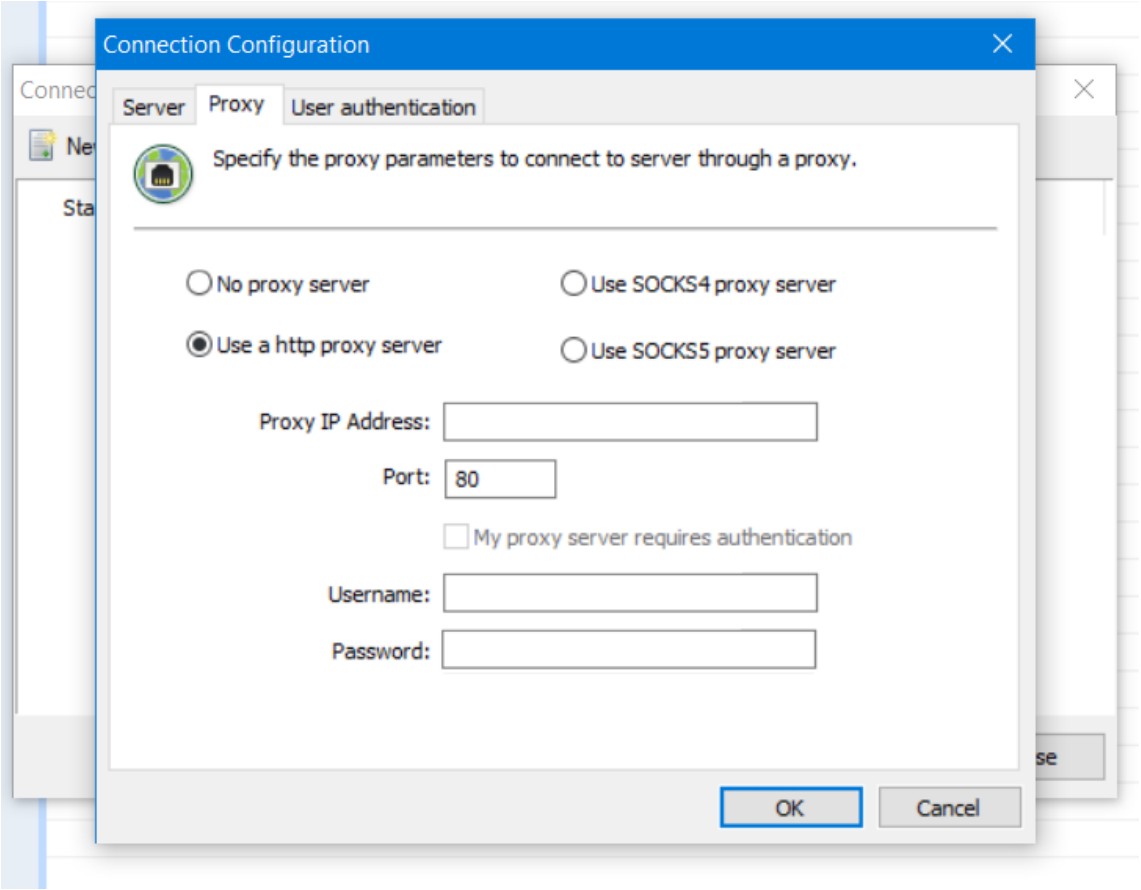
   a) 在 **Proxy IP Address**（代理 IP 地址）中，键入代理服务器的 IP 地址。

   b) 在 **Port**（端口）中，键入代理使用的 TCP 端口号。

   c) 代理服务器要求执行身份验证才能传输流量时，请选中 **My proxy server requires authentication**（我的代理服务器要求执行身份验证）复选框。

   d) 在 **Username**（用户名）中，键入在代理服务器上执行身份验证时使用的用户名。

   e) 在 **Password**（密码）中，键入在代理服务器上进行身份验证时使用的密码。



5. 在 **User Authentication**（用户身份验证）选项卡中，选中 **Remember my login and password**（记住我的登录名和密码）复选框，然后输入凭据。
6. 单击确定。

要连接到 XenMobile，请双击所创建的连接，然后输入为该连接配置的用户名和密码。

为 **Samsung Knox** 设备启用远程支持

可以在 XenMobile 中创建远程支持策略以授予远程访问 Samsung Knox 设备的权限。可以配置两种类型的支持：

- 基本：用于查看有关设备的诊断信息。例如系统信息、正在运行的进程、任务管理器（内存和 CPU 使用率）以及已安装的软件文件夹内容。
- 高级：用于远程控制设备屏幕。例如，控制窗口颜色、在技术支持人员与用户之间建立 VoIP 会话以及在技术支持人员与用户之间建立聊天会话。

  高级支持要求在 XenMobile 控制台中配置 Samsung MDM 许可证密钥设备策略。配置此策略时，只选择 **Samsung KNOX** 平台。对于 Samsung SAFE 平台，在 XenMobile 中注册 Samsung 设备时，ELM 密钥会自动部署在这些设备上。因此，不需要为此策略选择 Samsung SAFE 平台。有关详细信息，请参阅 Samsung MDM 许可证密钥。

有关如何配置远程支持策略的信息，请参阅远程支持设备策略。

使用 **Remote Support** 会话

启动 Remote Support 后，Remote Support 应用程序窗口左侧将显示您在 XenMobile 控制台中定义的 XenMobile 用户组。默认情况下，仅显示包含当前已连接的用户的组。您可以在用户条目旁边看到每个用户的设备。

1. 要查看所有用户，请展开左侧列中的每个组。
   当前已连接到 XenMobile Server 的用户用绿色图标指示。
2. 要显示所有用户（包括当前未连接的用户），请单击 **View**（查看）并选择 **Non-connected devices**（未连接的设备）。
   此时将显示未连接的用户，但不带绿色小图标。

连接到 XenMobile Server 但未分配给用户的设备以匿名模式显示。（列表中将显示字符串匿名。）可以像已登录用户的设备一样控制这些设备。

要控制某个设备，请单击该设备对应的行进行选择，然后单击 **Control Device**（控制设备）。该设备将出现在远程控制窗口中。可通过以下方法与被控制的设备交互：

- 在主窗口或独立的浮动窗口中控制设备的屏幕，包括控制颜色。
- 建立技术支持人员与用户之间的 VoIP 会话。配置 VoIP 设置。
- 与用户建立聊天会话。
- 访问设备的任务管理器以管理项目，例如内存使用率、CPU 使用率和正在运行的应用程序。
- 浏览移动设备的本地目录。传输文件。
- 在 Windows Mobile 设备中编辑设备注册表。
- 显示设备系统信息和所有已安装的软件。
- 更新移动设备与 XenMobile Server 的连接状态。

SysLog

November 12, 2020

可以将 XenMobile Server（仅限本地）配置为向系统日志 (syslog) 服务器发送日志文件。需要服务器主机名称或 IP 地址。

Syslog 是标准日志记录协议，包含两个组件：审核模块（运行在设备上）和服务器（运行在远程系统上）。Syslog 协议使用用户数据报协议 (UDP) 进行数据传输。将记录管理员事件和用户事件。

可以将服务器配置为收集以下类型的信息：

- 包含 XenMobile 操作记录的系统日志。
- 包含按时间排序的 XenMobile 系统活动记录的审核日志。

syslog 服务器从设备收集的日志信息以消息的形式存储在日志文件中。这些消息通常包含以下信息：

- 生成日志消息的设备的 IP 地址

- 时间戳
- 消息类型
- 与事件关联的日志级别（严重、错误、通知、警告、信息、调试、警报或紧急）
- 消息信息

XenMobile 使用 log4j syslog 追加器发送 RFC5424 格式的 syslog 消息。syslog 消息数据是没有任何特定格式的纯文本。

可以使用此信息分析警报来源并在需要时采用纠正措施。

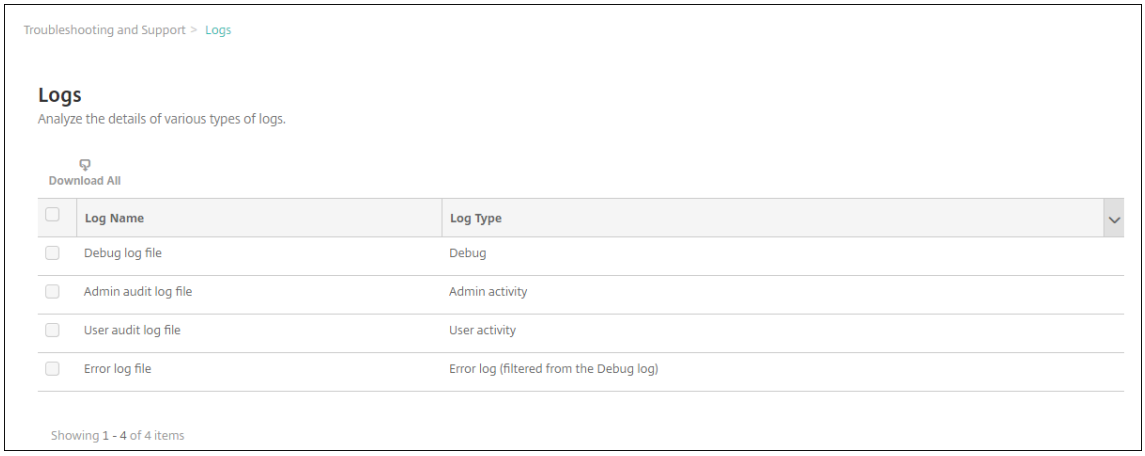
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击 **Syslog**。此时将显示 **Syslog** 页面。
3. 配置以下设置：
   - 服务器：键入 syslog 服务器的 IP 地址或完全限定域名 (FQDN)。
   - 端口：键入端口号。默认情况下，此端口设置为 514。
   - 要记录的信息：选中或取消选中系统日志和审核。
     - 系统日志包含 XenMobile 执行的操作。
     - 审核日志包含 XenMobile 的按时间排序的系统活动记录。
     - XenMobile 的调试日志。
4. 单击保存。

在 **XenMobile** 中查看日志文件

October 13, 2021

查看、操作和下载日志以帮助使用 XenMobile 进行管理。

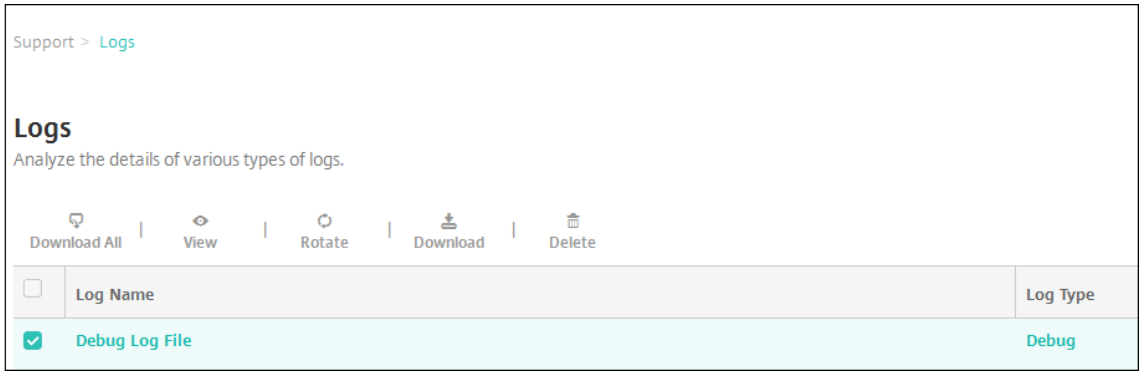
1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。此时将打开支持页面。
2. 在日志操作下方，单击日志。此时将显示日志页面。单独的日志将显示在表格中。



3. 选择要查看的日志：

   - 调试日志文件中包含对 Citrix 技术支持有用的信息，例如错误消息和服务器相关操作。
   - 管理员审核日志文件中包含与 XenMobile 控制台上的活动有关的审核信息。
   - 用户审核日志文件中包含与配置的用户有关的信息。
   - 错误日志文件中仅包含从调试日志中过滤出来的错误消息。

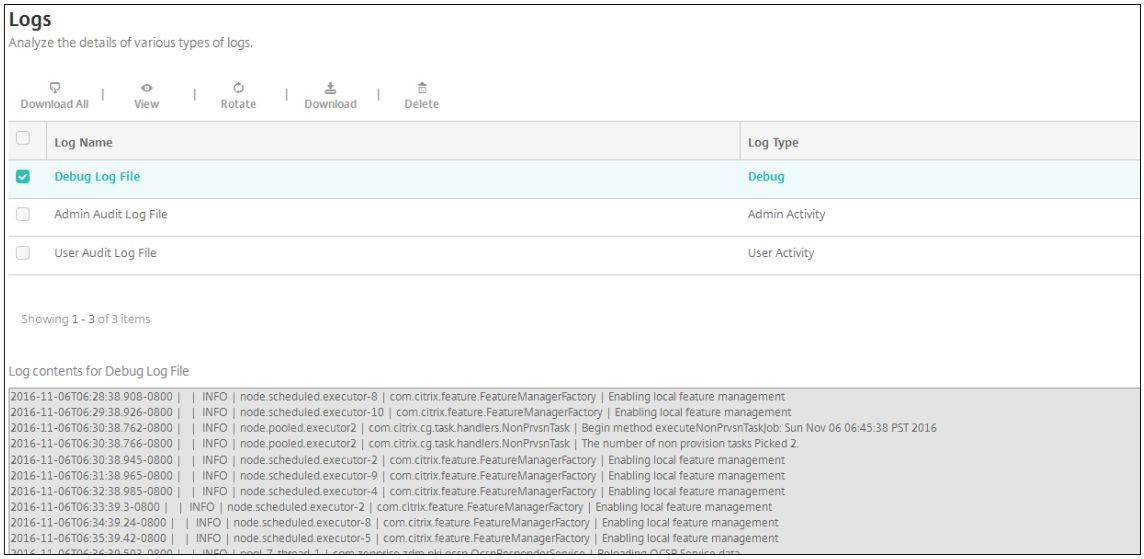
4. 使用表格顶部的操作可下载所有日志，查看、轮转或下载单个日志，或者删除选定的日志。



> 注意：
>
> - 如果选择了多个日志文件，则只有全部下载和轮转可用。
> - 如果您有群集 XenMobile Server，只能查看所连接到的服务器的日志。要查看其他服务器的日志，请使用以下下载选项之一。

5. 执行以下操作之一：

   - 全部下载：控制台下载系统中存在的所有日志（包括调试、管理员审核、用户审核、服务器日志等）。
   - 查看：在表格下方显示所选日志的内容。
   - 轮转：将当前日志文件存档并创建新文件以捕获日志条目。存档日志文件时会显示一个对话框，请单击轮转以继续。
   - 下载：控制台仅下载选定的一种日志文件类型，此外，还下载该类型对应的所有已存档的日志。
   - 删除：永久删除所选日志文件。



XenMobile Analyzer 工具

January 5, 2022

XenMobile Analyzer 是一个基于云的工具，可以使用该工具诊断与 XenMobile 的配置和其他功能有关的问题并进行故障排除。该工具检查您的 XenMobile 环境中是否存在设备或用户注册和身份验证问题。

将该工具配置为指向您的 XenMobile Server，并提供服务器部署类型、移动平台、身份验证类型以及用户凭据等信息。该工具随后将连接到服务器并扫描您的环境，检查是否存在配置问题。如果 XenMobile Analyzer 发现问题，该工具将提供更正问题的建议。

主要功能

- 基于云的安全微服务，可对 XenMobile 相关的所有问题进行故障排除。
- 解决 XenMobile 配置问题的准确建议。
- 减少了支持呼叫数量以及加快了 XenMobile 环境的故障排除速度。
- 为 XenMobile Server 版本提供零天支持。
- 运行状况检查计划每天或每周运行一次。
- Citrix ADC 配置检查。
- 执行 Secure Web 测试，确认能否访问 Intranet 站点。
- Secure Mail 自动发现服务检查。
- Citrix Files 单点登录 (SSO) 检查。

新增功能

- Citrix ADC 配置报告显示指示建议条数的徽章通知。这些建议基于在特定 Citrix Gateway 上执行的基本配置检查。
- “测试环境列表”页面上的全局导航栏内部的图标现已重新排序，以实现更加优异的用户体验。

下面的视频重点介绍了用户界面中的导航变更。

Citrix XenMobile Analyzer：全新的 **“Environment List”**（环境列表）用户界面

这是一个嵌入的视频。单击链接可观看此视频。

> 注意：
>
> 此视频不包含任何音频。最好在全屏模式下查看。

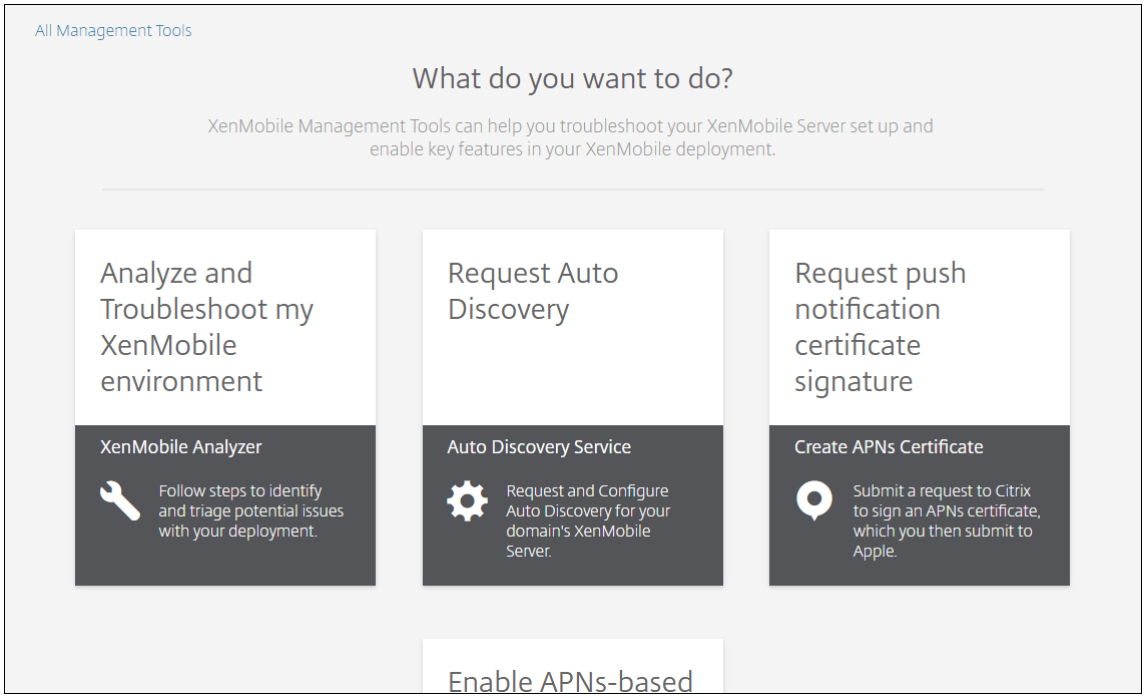
访问和启动 **XenMobile Analyzer**

必备条件

产品	支持的版本
XenMobile Server	10.1.0 及更高版本
Citrix Gateway	10.5 及更高版本
客户端注册模拟	iOS 和 Android

请使用以下方法之一访问 XenMobile Analyzer：

- 在 XenMobile 控制台中，单击右上角的扳手图标以打开故障排除和支持页面。
- 请使用 My Citrix 凭据从 https://tools.xm.cloud.com/ 访问该工具。在显示的 XenMobile“Management Tools”（管理工具）页面上，要启动 XenMobile Analyzer，请单击 **Analyze and Troubleshoot my XenMobile Environment**（分析我的 XenMobile 环境并进行故障排除）。



XenMobile Analyzer 包含五个设计用于引导您完成会审过程以及减少支持票证数量的选项。这些选项可以降低每个人的成本。

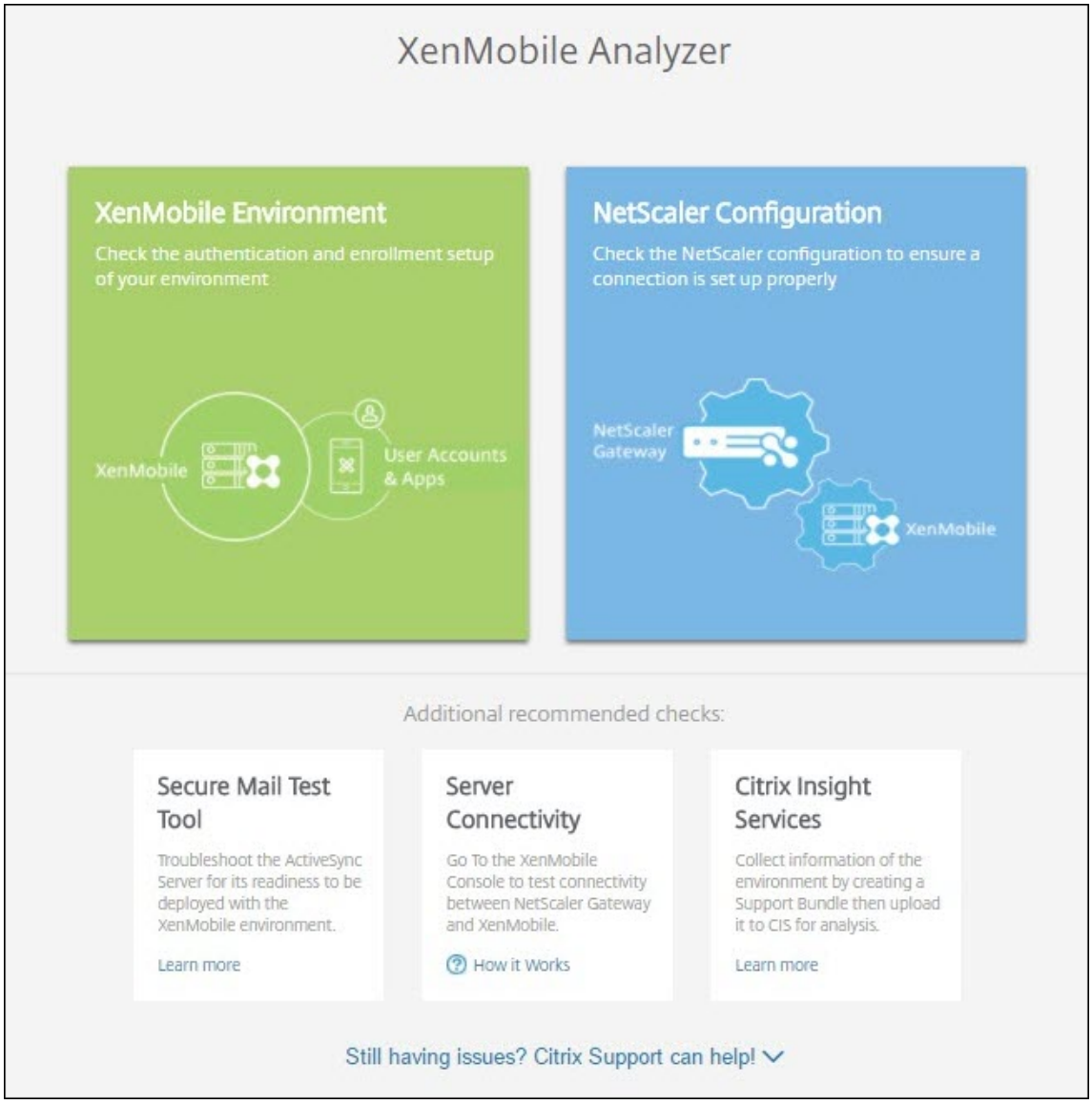
这些选项如下所示：

- **Environment Check**（环境检查）：此步骤指导您设置测试以检查您的设置是否存在问题。此步骤还提供与设备、用户注册和身份验证问题有关的建议和解决方案。
- **Citrix ADC** 检查：此步骤指导您检查您的 Citrix ADC 配置是否符合 XenMobile 部署就绪条件。
- **Advanced Diagnostics**（高级诊断）：此步骤提供与使用 Citrix Insight Services 进一步查找环境检查可能错过的问题有关的信息。
- **Server Connectivity Checks**（服务器连接检查）：此步骤指导您测试服务器的连接。
- **Contact Citrix Support**（联系 **Citrix** 支持）：如果您仍遇到问题，此步骤将链接到您能够在其中创建 Citrix 支持案例的站点。

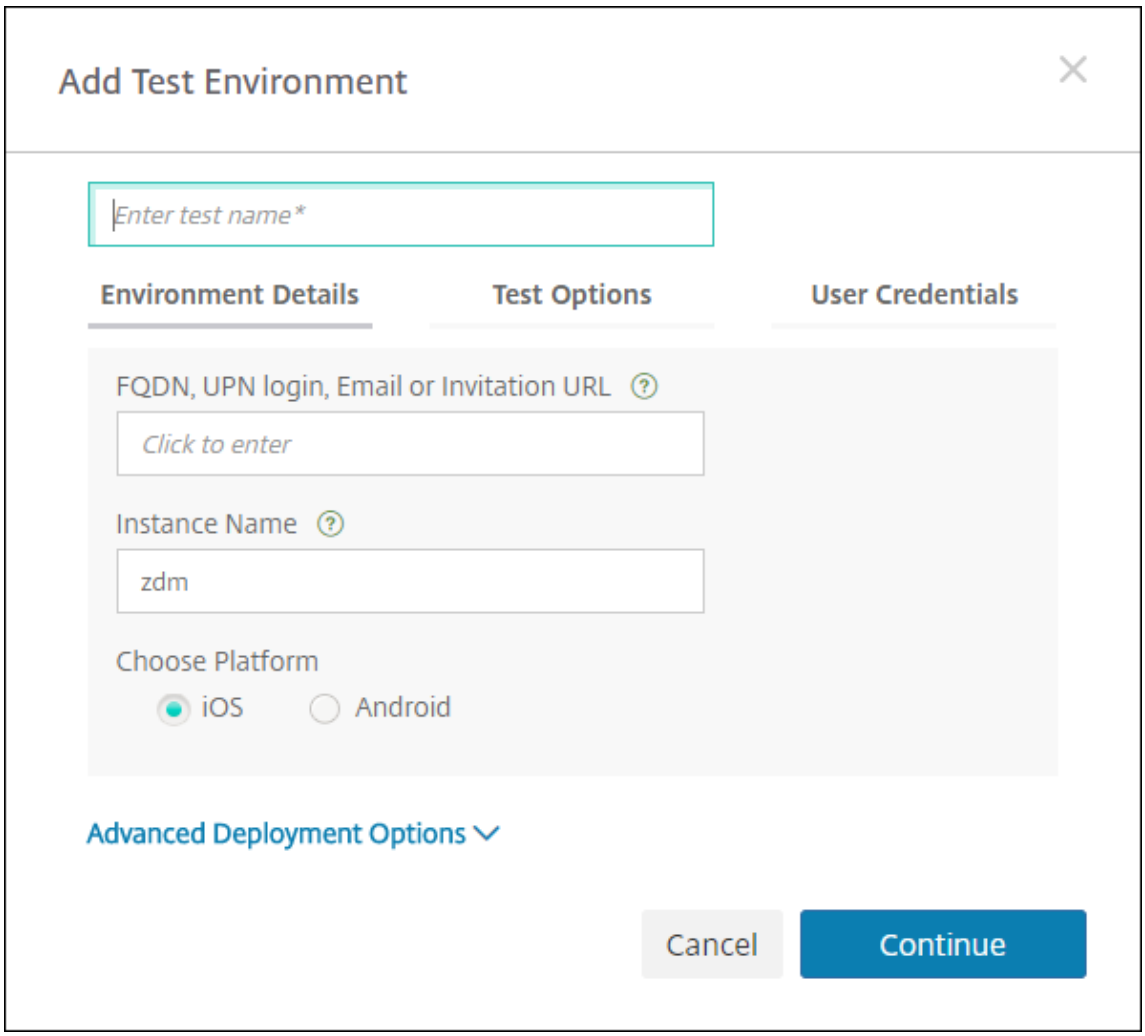
以下各节更加详细地介绍了每个选项。

执行环境检查

1. 登录 XenMobile Analyzer，然后单击 **XenMobile Environment**（XenMobile 环境）。



2. 单击 **Add Test Environment**（添加测试环境）。
3. 在新的 **Add Test Environment**（添加测试环境）对话框中，执行以下操作：



a) 为测试提供一个唯一的名称，以帮助识别将来的测试。

b) 在 **FQDN, UPN login, Email or URL Invitation**（FQDN、UPN 登录、电子邮件或 URL 邀请）中，输入访问服务器时使用的信息。

c) 在 **Instance Name**（实例名称）中，如果使用自定义实例，可以提供该值。

d) 在 **Choose Platform**（选择平台）中，选择 **iOS** 或 **Android** 作为测试平台。

e) 如果展开 **Advanced Deployment Options**（高级部署选项），则可以在 **Deployment Mode**（部署模式）列表中选择您的 XenMobile 部署模式。1. 可用选项为 **Enterprise (MDM + MAM)**（企业 (MDM + MAM)）、**App Management (MAM)**（应用程序管理 (MAM)）或 **Device Management (MDM)**（设备管理 (MDM)）。

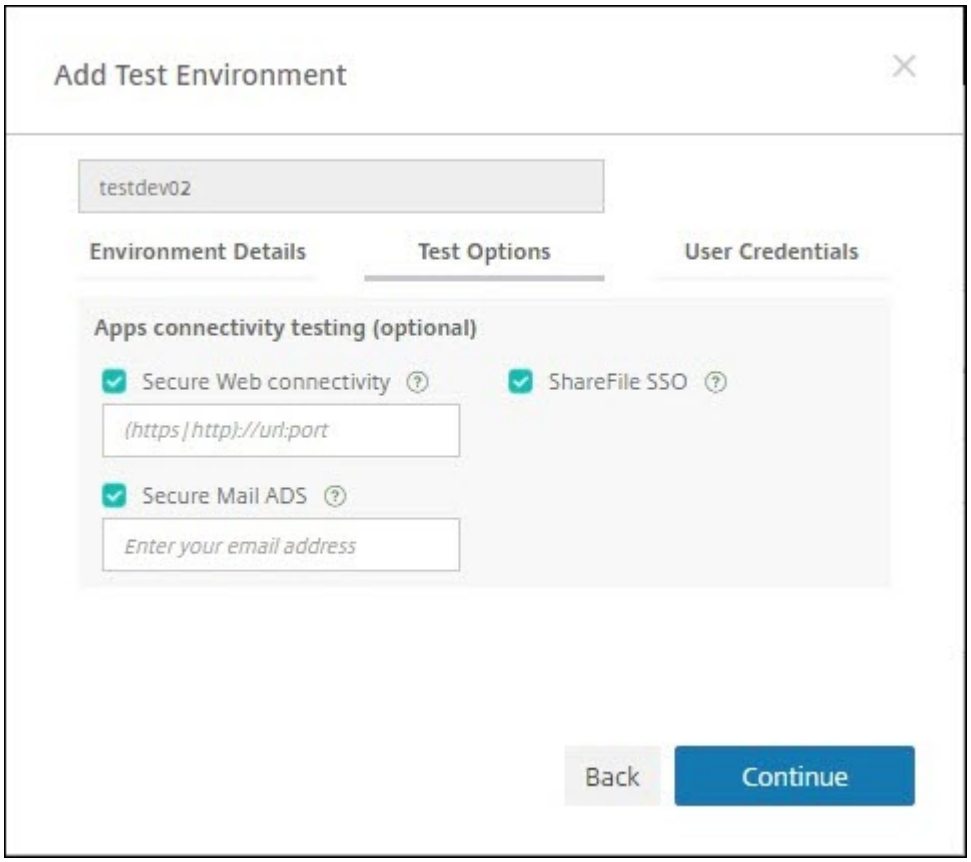
f) 单击继续。

4. 在 **Test Options**（测试选项）选项卡上，选择以下测试中的一个或多个，然后单击 **Continue**（继续）。

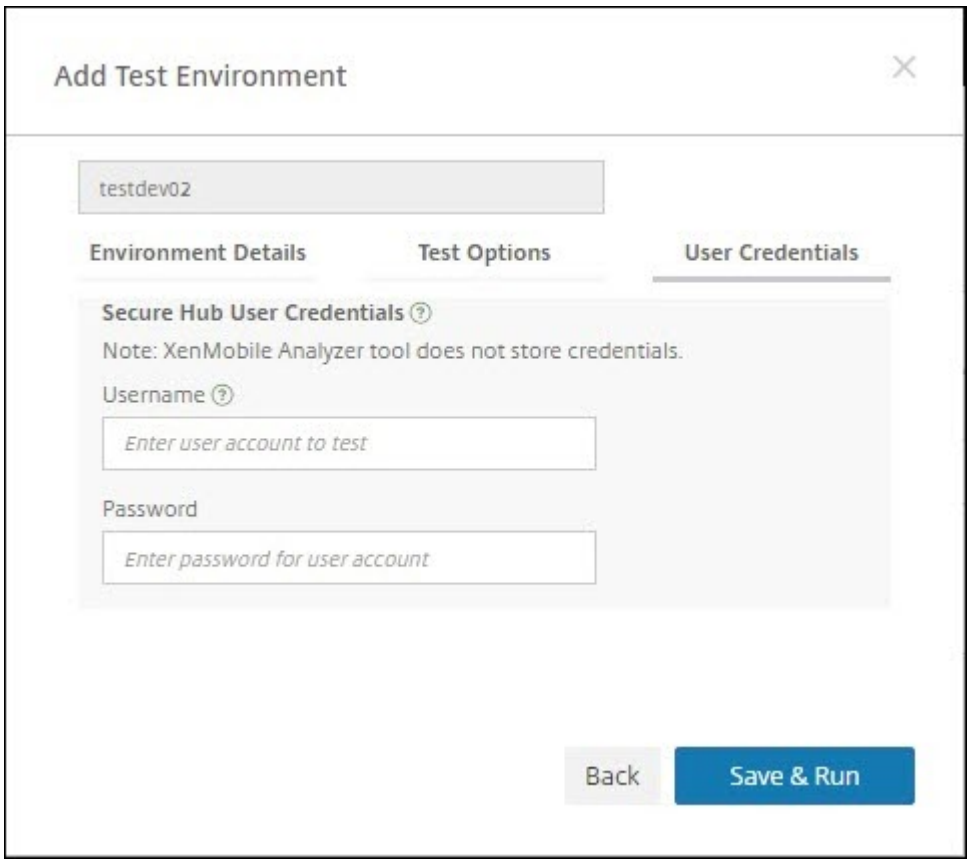
a) **Secure Web** 连接。提供 Intranet URL。该工具测试该 URL 能否访问。在尝试访问 Intranet URL 期间，此测试会检测 Secure Web 应用程序中是否可能发生任何连接问题。

b) **Secure Mail ADS**。提供用户电子邮件 ID。此 ID 用于测试在 XenMobile 环境中自动发现 Microsoft Exchange Server 的情况。它检测是否存在与 Secure Mail 自动发现有关的任何问题。

c) **ShareFile SSO**。如果选择此选项，XenMobile Analyzer 将测试 Citrix Files DNS 解析是否已成功发生。该工具还检查 Citrix Files 单点登录 (SSO) 是否与提供的用户凭据兼容。



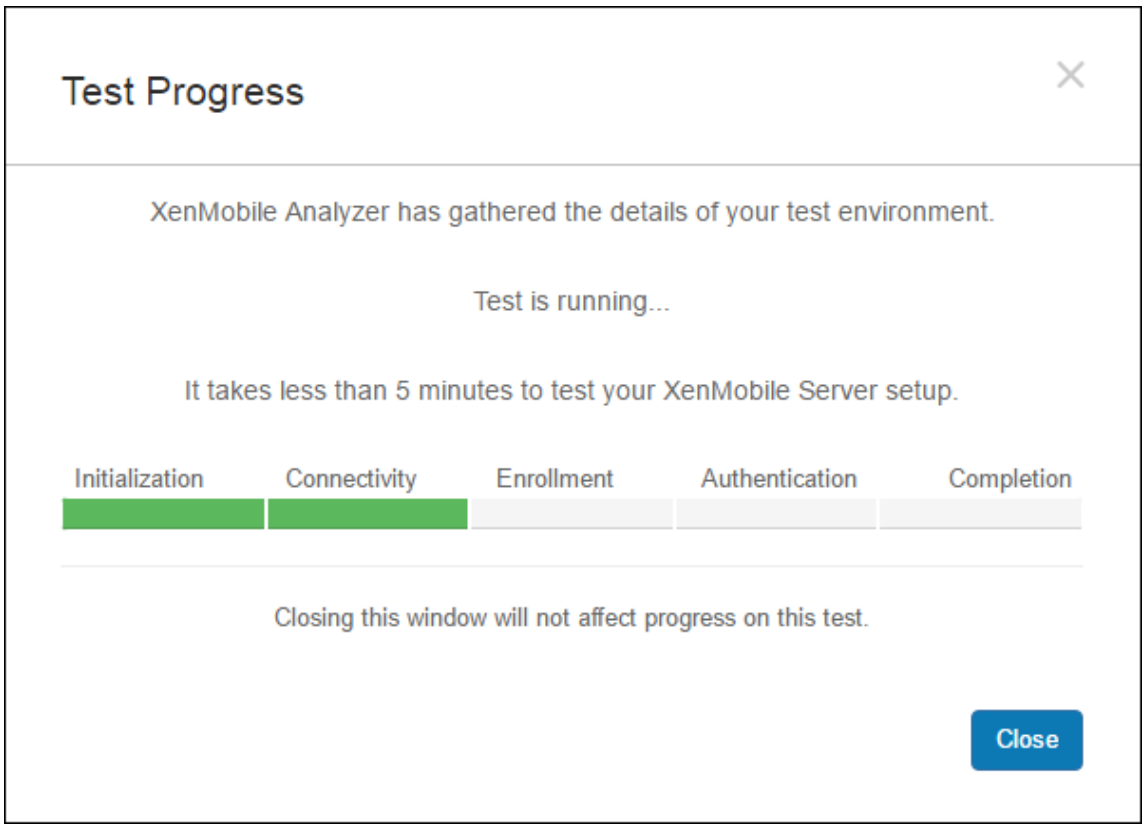
5. 在 **User Credentials**（用户凭据）选项卡上，您可能会看到不同的字段，具体取决于您的服务器设置。可能的字段包括 **Username**（用户名）、**Username and Password**（用户名和密码）或 **Username, Password**（用户名、密码）和 **Enrollment PIN**（注册 PIN）。



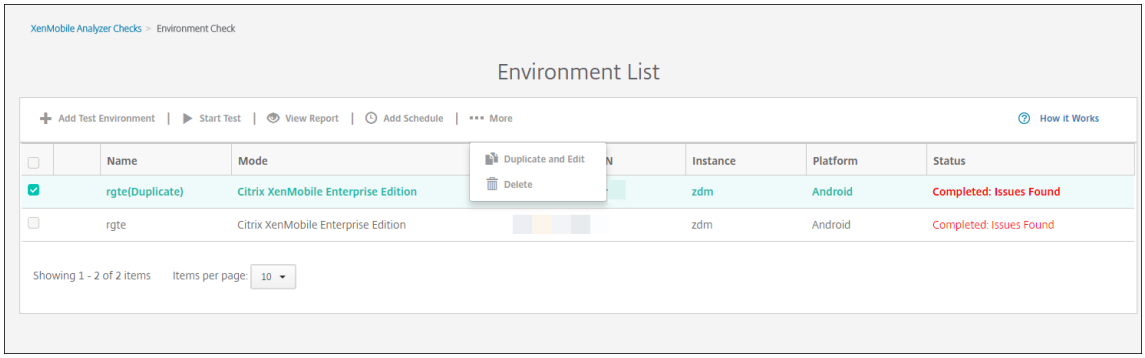
6. 单击 **Save & Run**（保存并运行）开始测试。

   此时将显示进度通知。可以让将进度对话框保留在打开状态，也可以关闭该对话框，测试将继续运行。

   通过的测试将显示为绿色。失败的测试将显示为红色。



在关闭进度对话框后，将返回 **Environments List**（环境列表）页面。



Results（结果）页面显示“Test Details”（测试详细信息）、“Recommendations”（建议）和“Results”（结果）。

7. 单击 **View Report**（查看报告）图标可查看测试结果。

   如果建议有与之关联的 Citrix 知识库文章，相应的文章将在此页面上列出。

8. 单击 **Results**（结果）选项卡显示该工具执行的各个类别和测试及其结果。

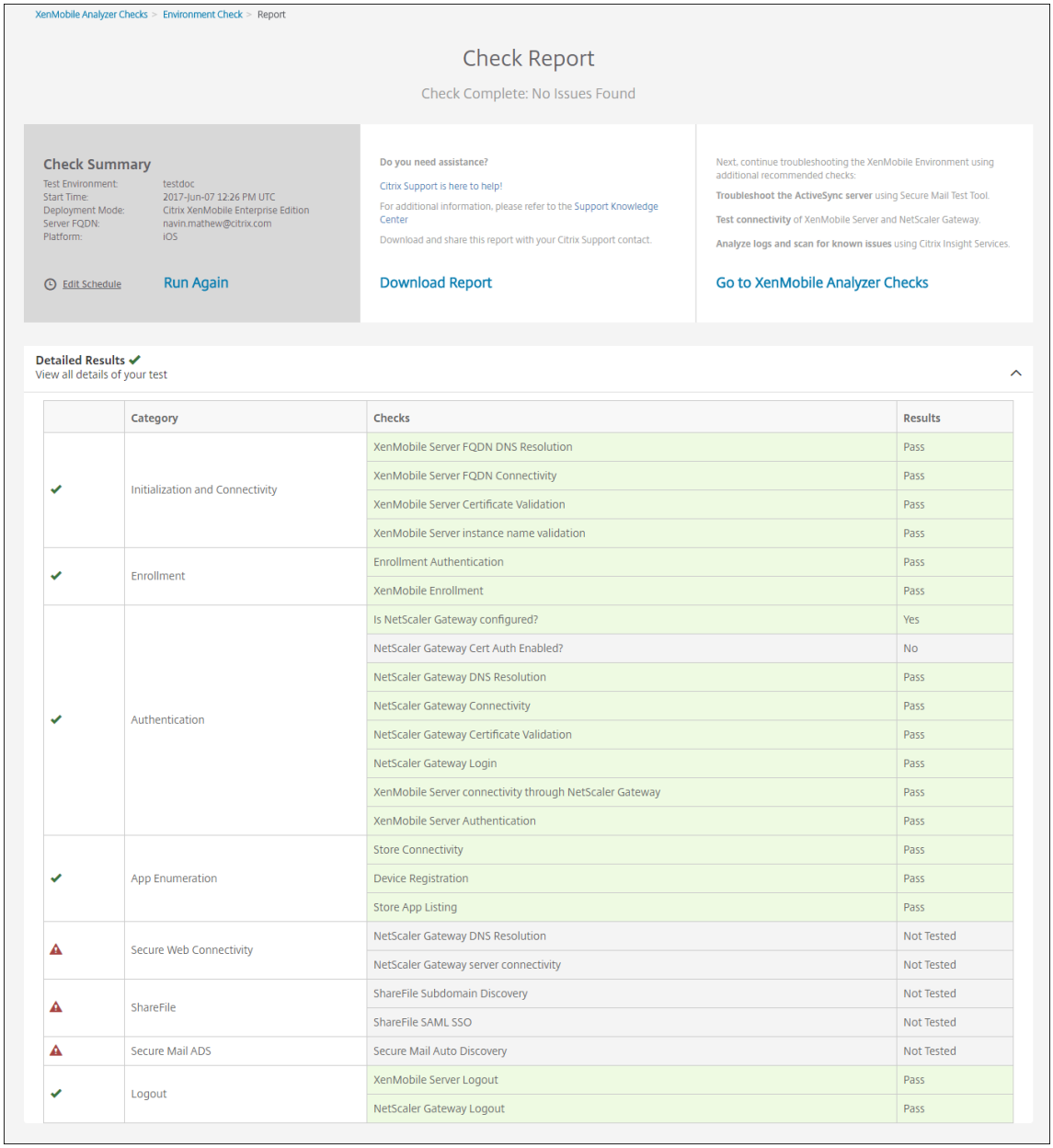
   a) 要下载报告，请单击 **Download Report**（下载报告）。

   b) 要返回测试环境列表，请单击 **Environment Check**（环境检查）。

   c) 要重新运行同一个测试，请单击 **Run Again**（重新运行）。

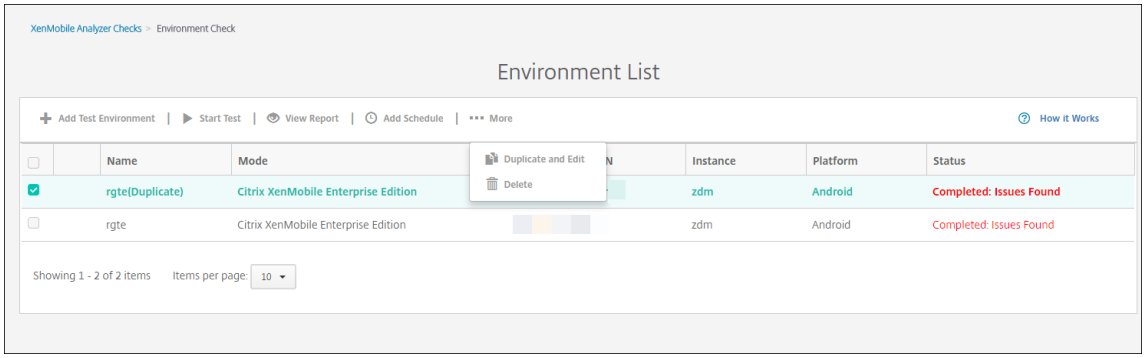
d) 如果要重新运行另一个测试，请返回 **Test Environments**（测试环境），选择测试，然后单击 **Start Test**（开始测试）。

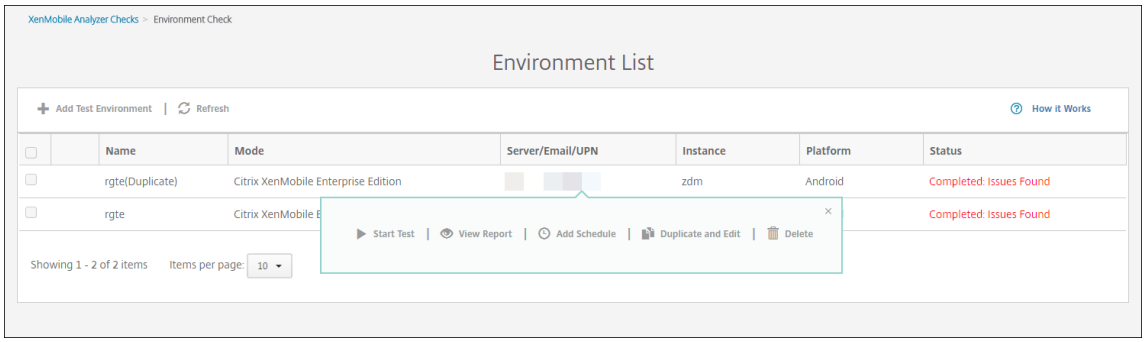
e) 要选择另一个 XenMobile Analyzer 选项，请单击 **Go To XenMobile Analyzer Checks**（转到 XenMobile Analyzer 检查）。

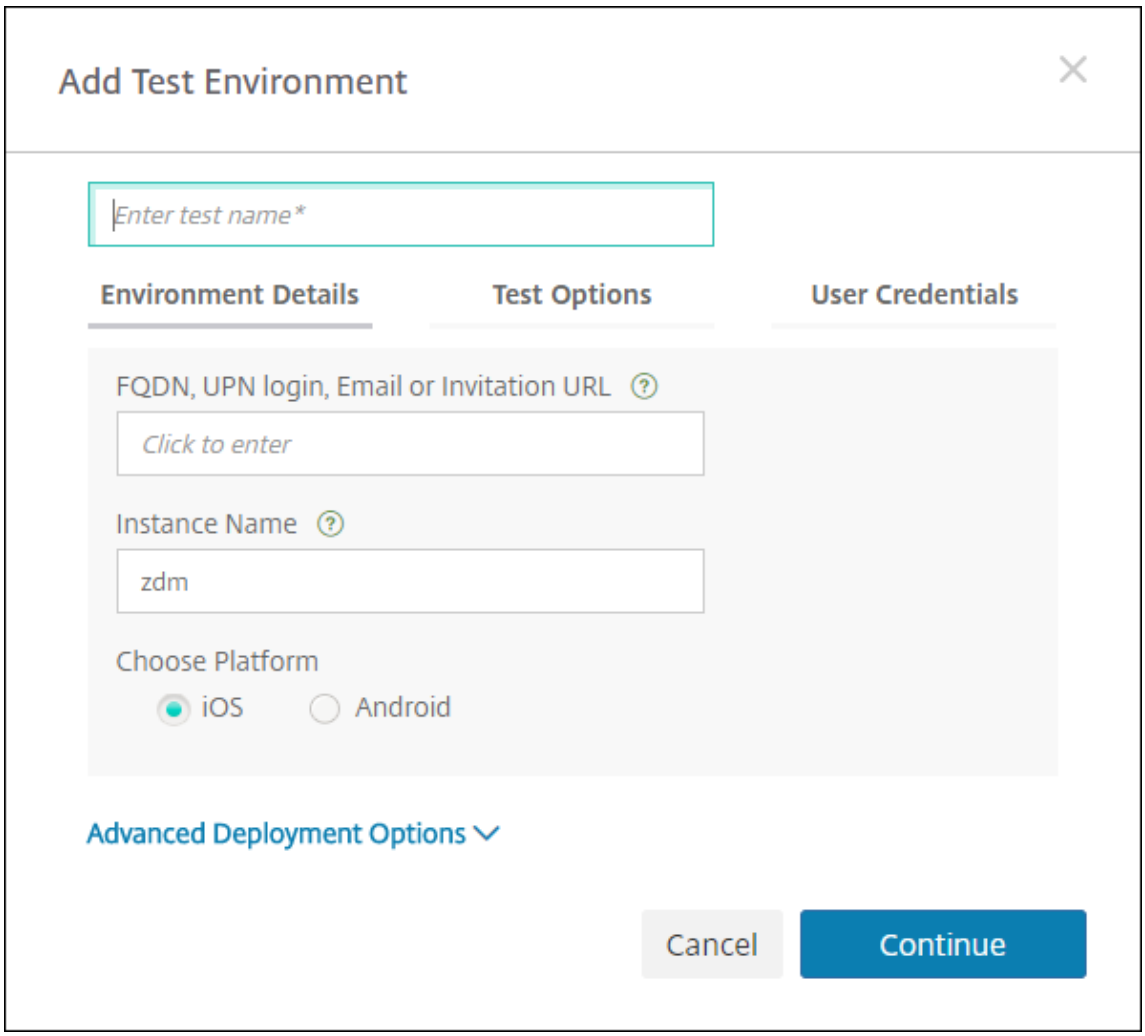


9. 在 “Test Environments”（测试环境）页面上，可以复制并编辑测试。为此，请选择一个测试，然后单击 **More**（更多）并选择 **Duplicate and Edit**（复制并编辑）。

   此时会创建所选测试的副本，并打开 “Add Test Environment”（添加测试环境）对话框，从而允许您修改新测试。



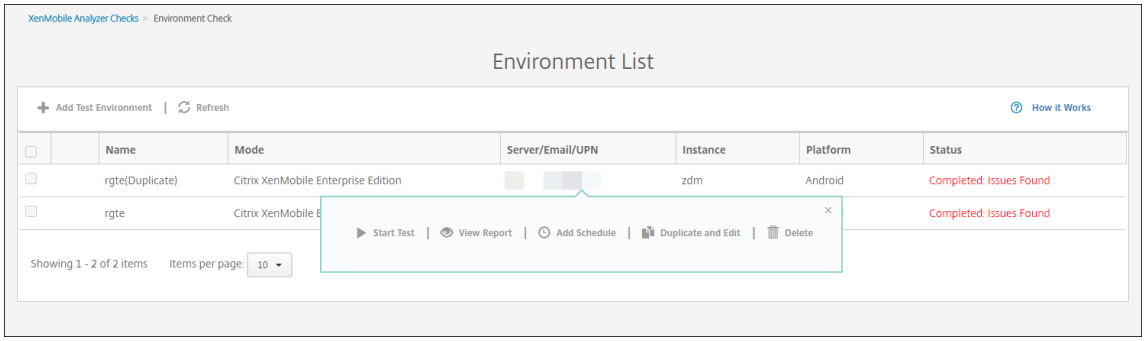




向环境检查添加计划

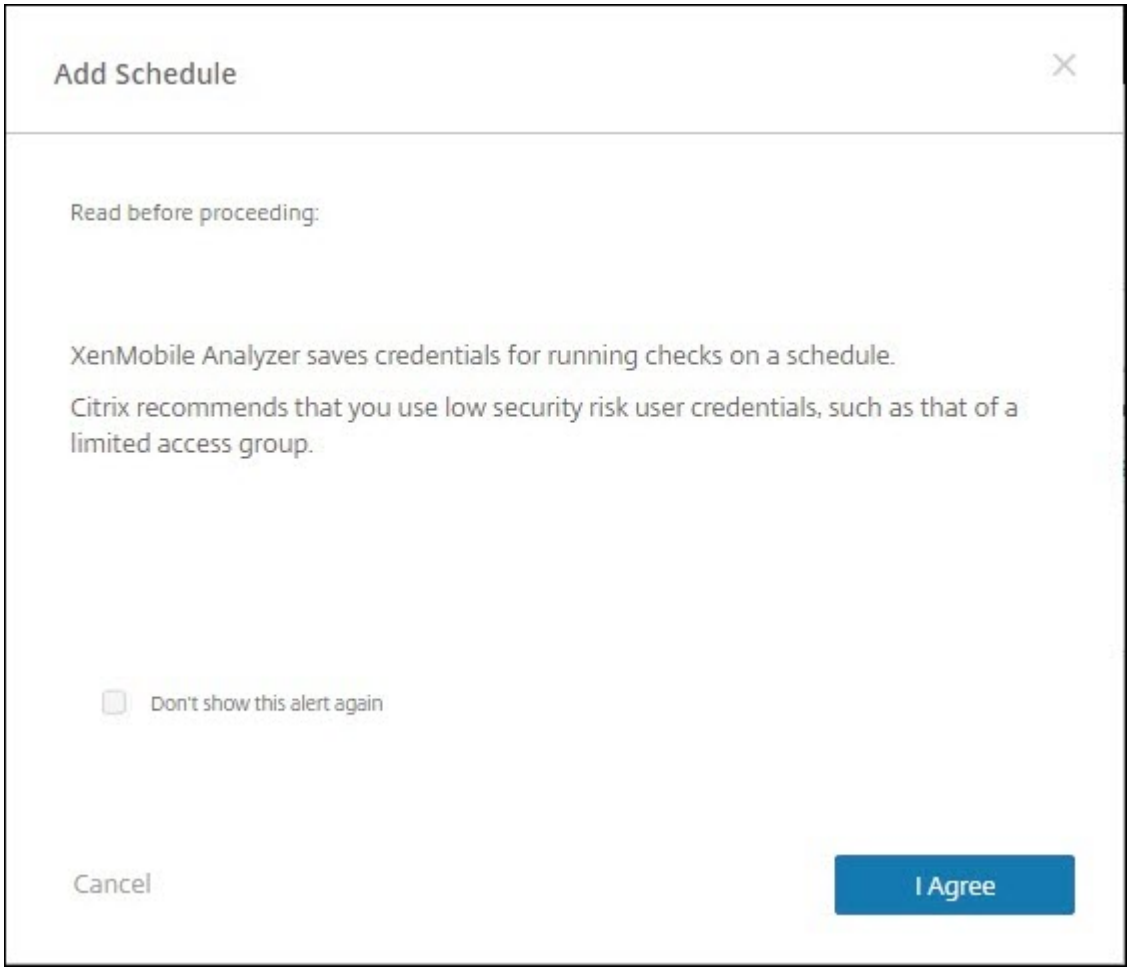
您可以将测试配置为按计划自动执行，且将结果发送给您配置的用户列表。

1. 在 **Environment List**（环境列表）页面上，选择您要为其设置计划的环境，并单击 **Add Schedule**（添加计划）。

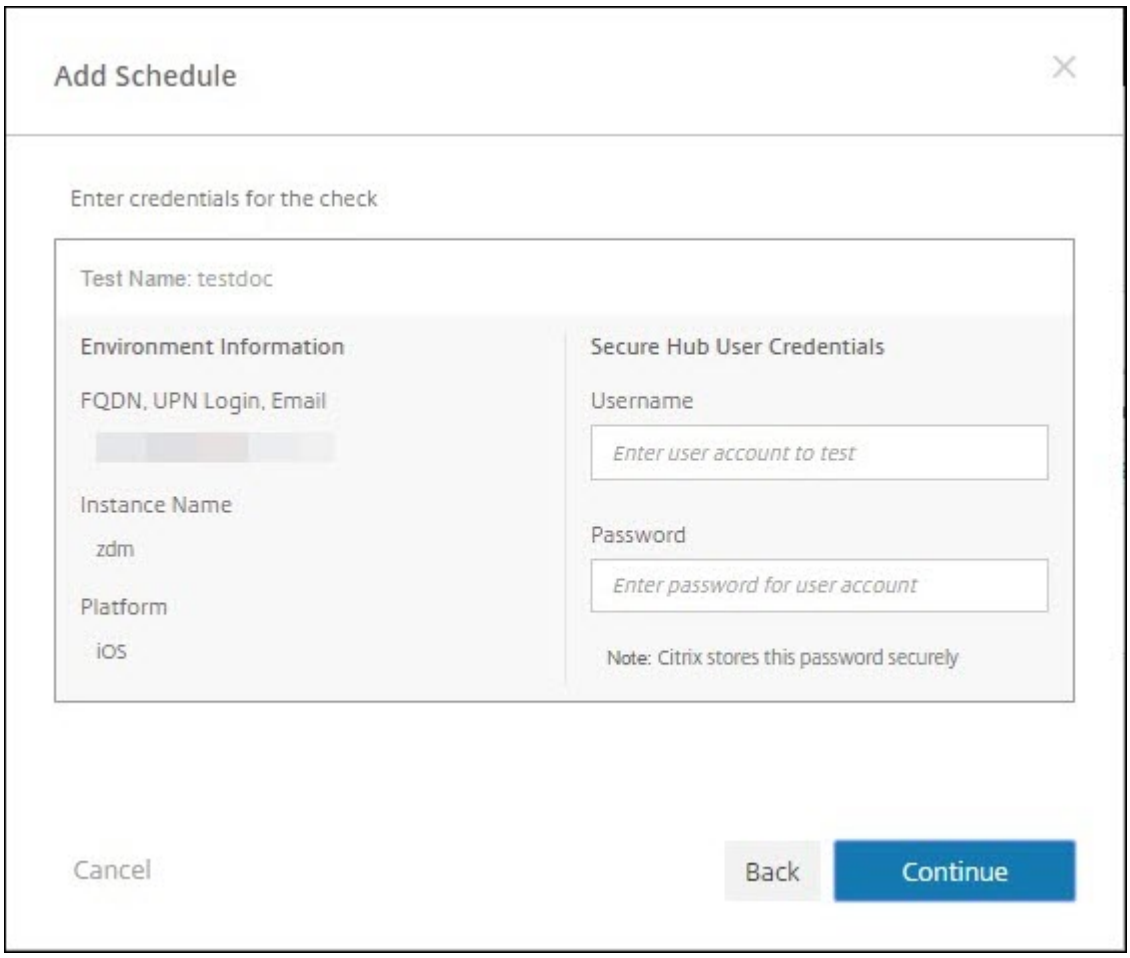


2. **Add Schedule**（添加计划）窗口中将显示一条消息，提醒您 XenMobile Analyzer 将保存凭据以用于按计划

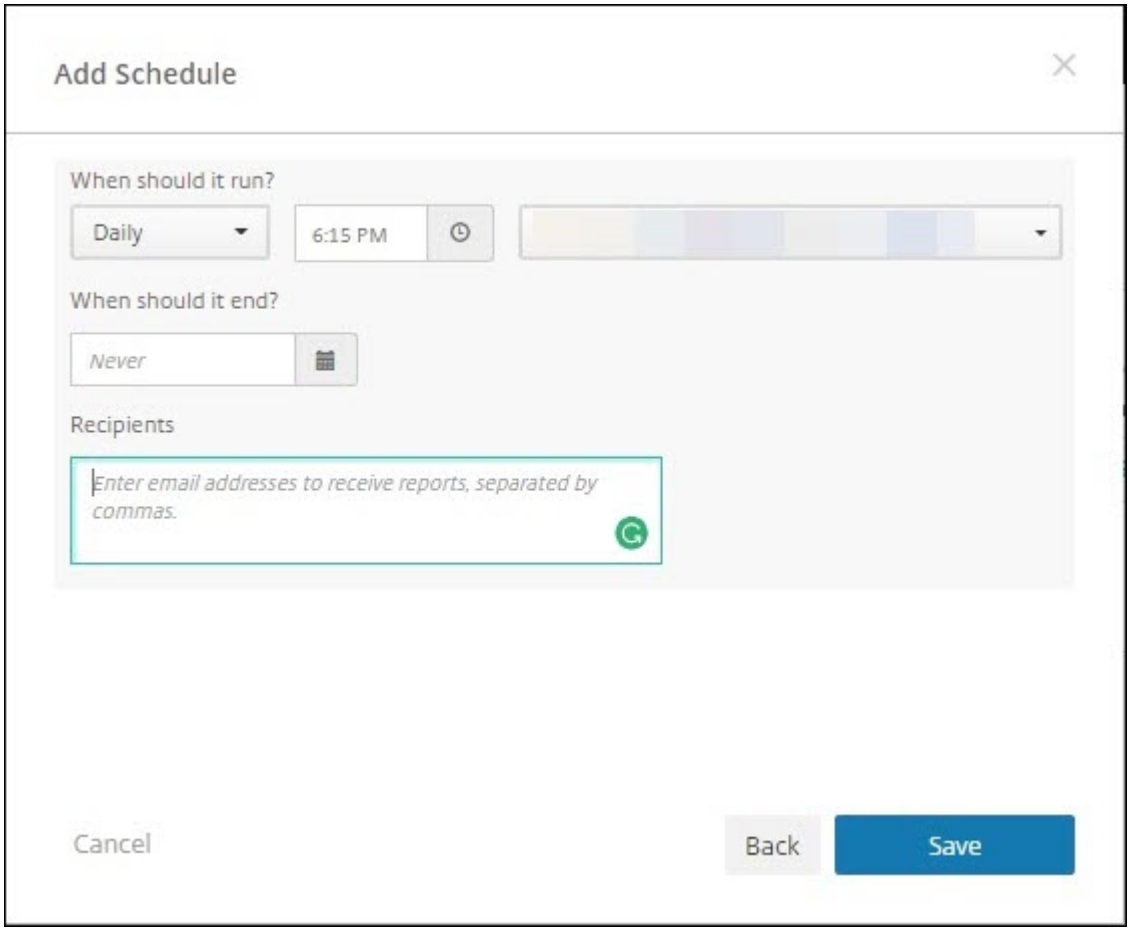
运行测试。Citrix 建议您使用具有有限访问权限的帐户来运行计划的测试。单击 **I Agree**（我同意）继续。



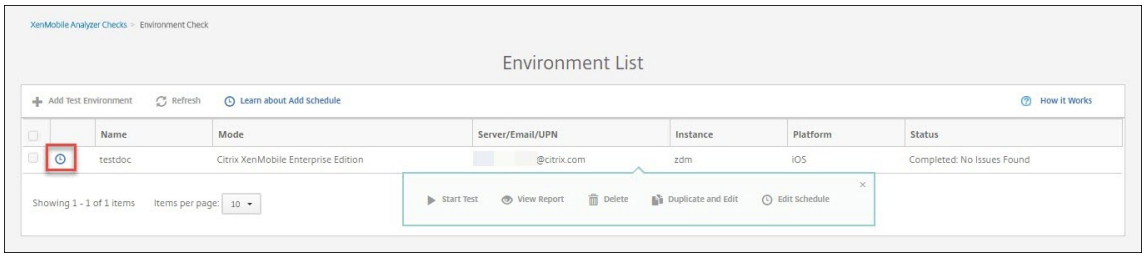
3. 输入用于运行测试的用户名和密码。



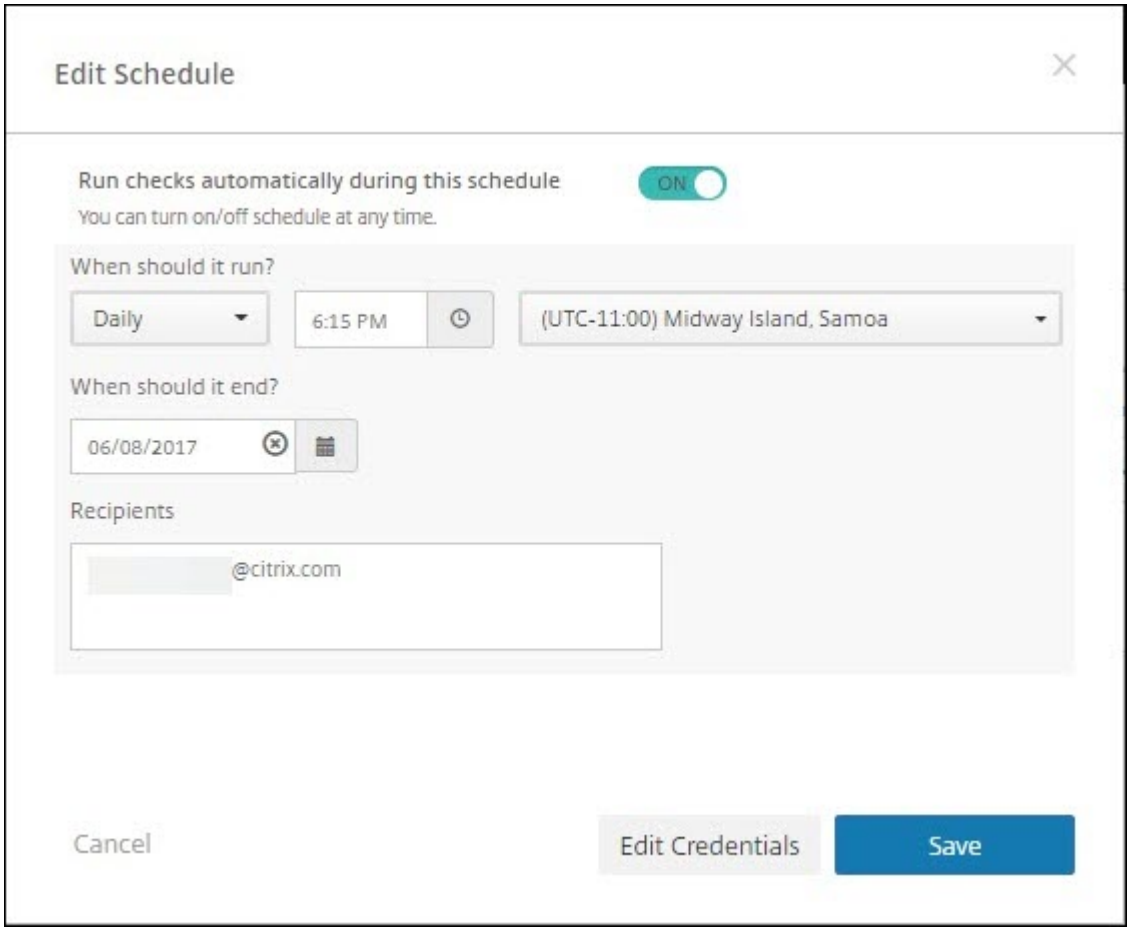
4. 配置测试的运行计划。您可以从下拉框中选择每天或每周。选择测试的运行时间和时区。可使用日期选取器来选择计划的测试停止运行的日期，或留空以让测试无限期地运行。请输入电子邮件地址列表（以逗号分隔）以接收报告。单击保存。



5. 测试左侧的时钟符号表示配置了计划。如果您选择测试，您可以单击 **Edit Schedule**（编辑计划）更改测试运行时间。



6. 在此窗口中，您可以更改测试运行时间。您还可以单击顶部的开关来禁用它。完成时单击 **Save**（保存）。



执行其他信息性检查

您直接与 XenMobile Analyzer 的环境检查步骤交互以执行测试，而其他选项属于信息性的。其中每个选项都会提供与可用于确保正确设置 XenMobile 环境的其他支持工具有关的信息。

- **Advanced Diagnostics**（高级诊断）：指导您收集有关环境的信息，然后将该信息上载到 Citrix Insight Services。该工具分析您的数据并提供包含建议的解决方案在内的个性化报告。
- **Secure Mail Readiness**（**Secure Mail** 就绪）：指导您下载并运行 XenMobile Exchange ActiveSync Test 应用程序。该应用程序将对 ActiveSync 服务器进行故障排除，以确认其是否已准备好在 XenMobile 环境中部署。该应用程序运行后，可以查看报告或将报告与其他人共享。
- **Server Connectivity Checks**（服务器连接检查）：为您提供检查与 XenMobile、身份验证和 Content Collaboration 服务器的连接的说明。
- **Contact Citrix Support**（联系 **Citrix** 支持）：如果所有其他操作都失败，可以通过 Citrix 支持创建一个支持票证。

已知问题

下面是 XenMobile Analyzer 中的已知问题：

- 执行 Secure Web 连接检查时，不支持在文本框中键入多个 URL。
- 不支持使用 Secure Hub 的共享设备身份验证功能。
- Secure Web 测试只检查与输入的 URL 的连接，不检查对相应站点的身份验证。

已修复的问题

XenMobile Analyzer 存在的以下问题已修复：

- 使用注册邀请执行检查时，测试将传递，但不替换注册邀请。

REST API

January 5, 2022

> 注意：
>
> 本文介绍了 XenMobile Server 的 REST API。有关 Endpoint Management 的 REST API，请参阅 REST API。

借助 XenMobile REST API，可以调用通过 XenMobile 控制台展现的服务。可以使用任何 REST 客户端调用 REST 服务。API 不要求您登录 XenMobile 控制台即可调用这些服务。

有关可用 API 的最新完整集合，请下载 Public API for REST Services（适用于 REST 的公共 API 服务）PDF。

访问 **REST API** 所需的权限

访问 REST API 需要具有以下权限：

- 公共 API 访问权限，设置为基于角色的访问配置的一部分。有关信息，请参阅使用 RBAC 配置角色。
- 超级用户权限

调用 **REST API** 服务

可以使用 REST 客户端或 CURL 命令调用 REST API 服务。以下示例使用适用于 Chrome 的高级 REST 客户端。

> 注意：
>
> 在下面的示例中，请更改主机名和端口号以匹配您的环境。

登录

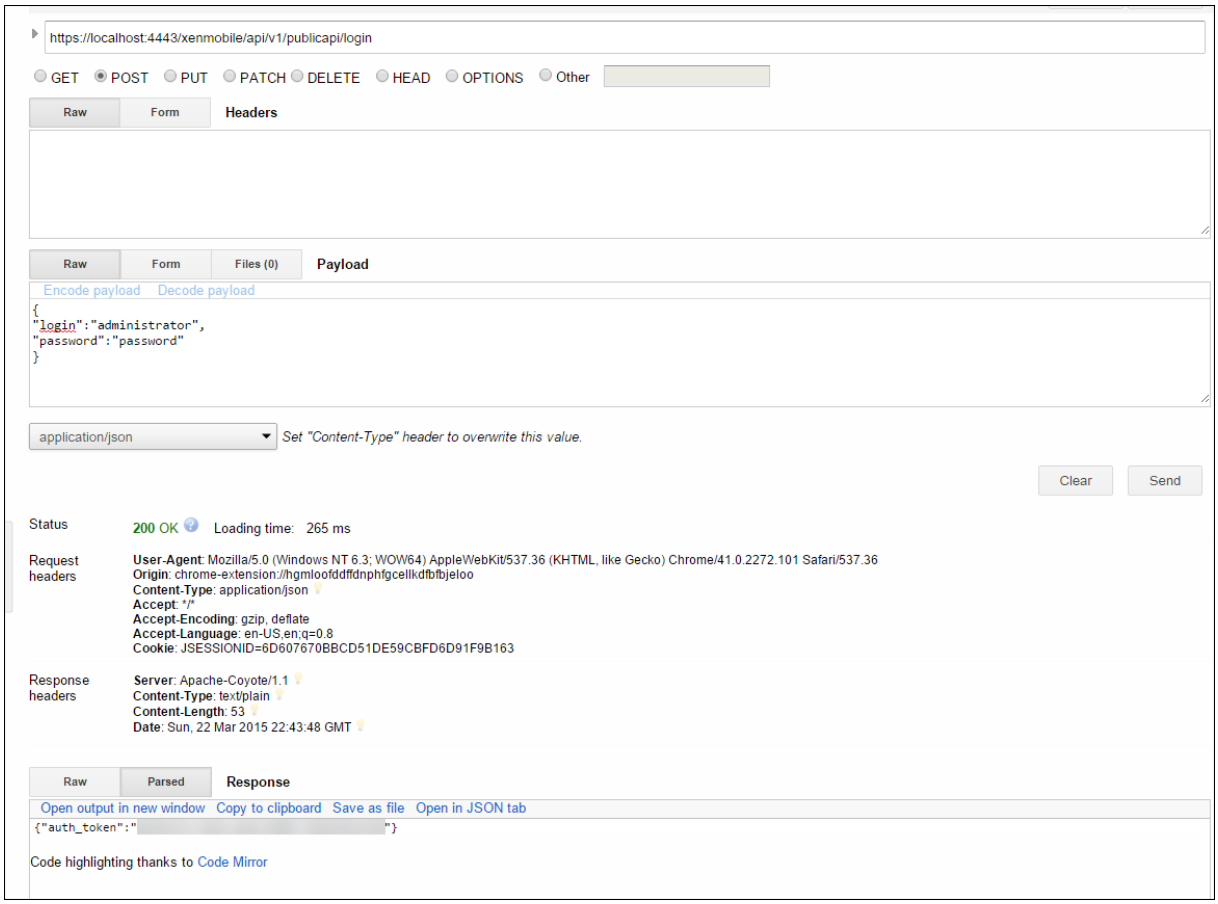
URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

请求：

```
{ "login":"administrator", "password":"password"}
```


方法类型：POST

内容类型：application/json



相关信息

- XenMobile REST API

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

January 5, 2022

XenMobile Mail Manager 现已更名为适用于 Exchange ActiveSync 的 Endpoint Management 连接器。有关 Citrix 统一产品组合的更多详细信息，请参阅 Citrix 产品指南。

连接器通过以下方法扩展 XenMobile 的功能：

- 用于 Exchange ActiveSync (EAS) 设备的动态访问控制。可以自动允许或阻止 EAS 设备访问 Exchange 访问。

- 使 XenMobile 能够访问 Exchange 提供的 EAS 设备合作信息的功能。
- XenMobile 能够根据 EAS 状态擦除移动设备。
- 使 XenMobile 能够访问关于黑莓设备的信息以及执行擦除和重置密码等控制操作的功能。

要根据 EAS 状态擦除设备，请使用 ActiveSync 触发器配置自动操作。请参阅自动化操作。

要下载适用于 Exchange ActiveSync 的 Endpoint Management 连接器，请执行以下操作：

1. 转到 https://www.citrix.com/downloads。
2. 导航到 **Citrix Endpoint Management**（和 **Citrix XenMobile Server**）**> XenMobile Server (**本地**) >** 产品软件 **> XenMobile Server 10 >** 服务器组件。
3. 在 适用于 **Exchange ActiveSync** 的 **Citrix Endpoint Management** 连接器上，单击下载文件。

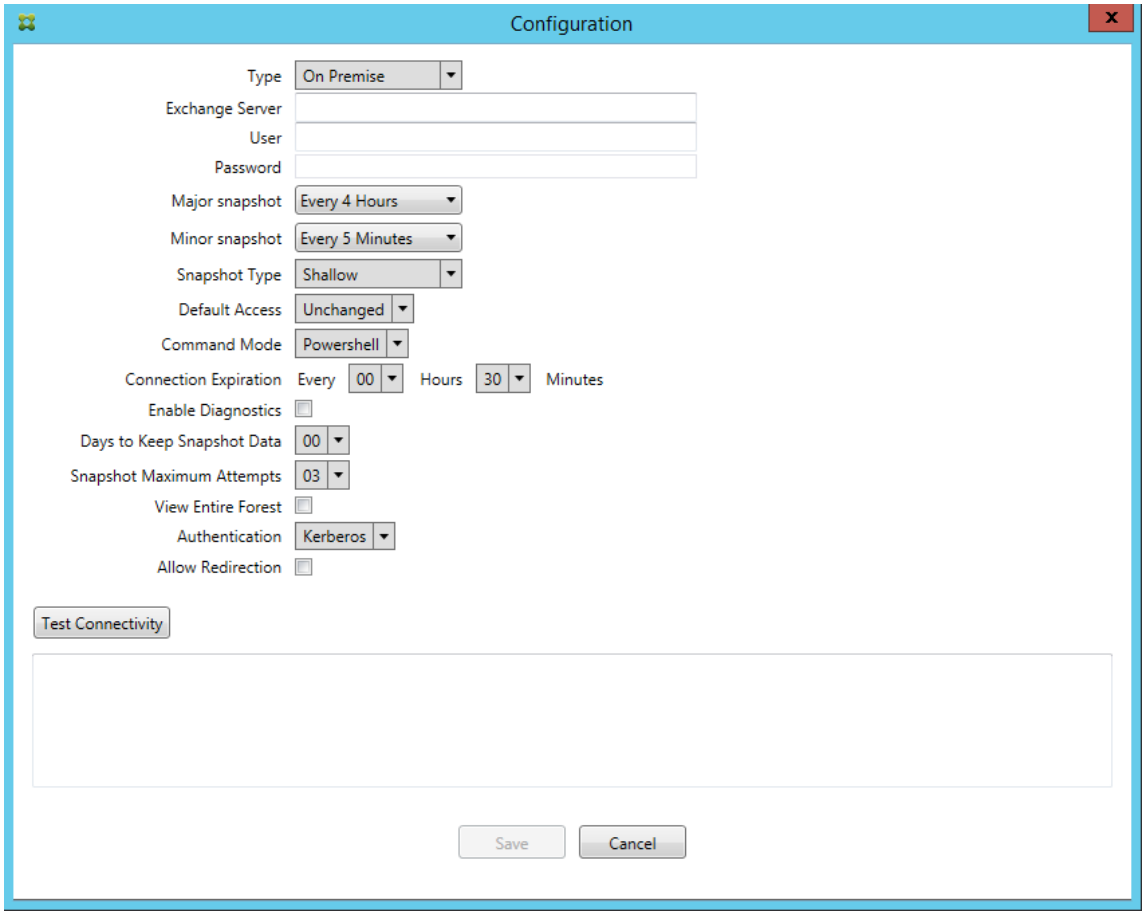
新增功能

以下各部分内容列出了适用于 Exchange ActiveSync 的 Endpoint Management 连接器（以前称为 XenMobile Mail Manager）的新增功能。

版本 **10.1.10** 中的新增功能

10.1.10 版中修复了以下问题：

- 遇到频繁出现的网络问题的客户可能无法在之前提供的三次尝试中完成快照。在本版本中，管理员可以配置最大尝试次数 (1-10)。此修复允许快照在不完全放弃快照过程的情况下在通信中产生多次中断。[CXM-70837]



- 在早期版本中，快照类型未显示在 Exchange 配置列表中。现在，快照类型则显示在该位置。[CXM-70846]
- PowerShell 报告的 PSRemotingTransport 异常表示与 Exchange 的会话不再可行。默认情况下，状态将添加到配置文件中的“严重错误”列表中。这样，当检测到 PSRemotingTransport 异常时，连接被标记为错误以供稍后处理。下一个通信使用有效的连接或创建新连接。[XMHELP-2184，CXM-70836]
- 保存配置更改后，在加载新配置之前，可能并非所有之前配置的内部组件都已正确处理。此问题可能会导致出现不可预测的行为。该行为取决于特定的更改以及该更改是否与之前的配置冲突。在本版本中，所有内部组件都会在加载新配置之前处理。[XMHELP-2259，CXM-71388]

早期版本中的新增功能

下面的部分列出了适用于 Exchange ActiveSync 的 Endpoint Management 连接器的早期版本中的功能和已修复的问题。

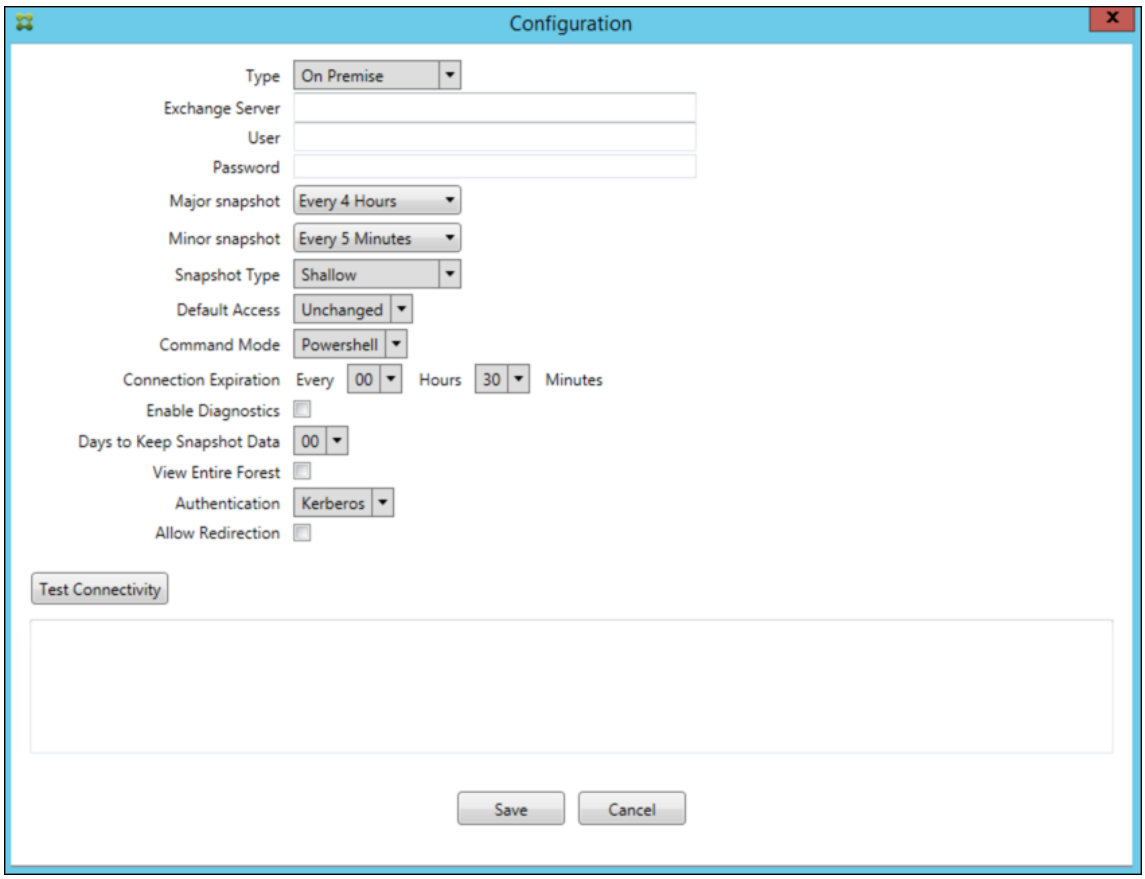
版本 **10.1.9** 中的新增功能

版本 10.1.9 中修复了以下问题：

- 现在，对配置所做的更改将以更加一致的方式进行处理。当服务检测到配置中的更改时，每个内部子系统都将停止运行，这意味着任何活动的或计划的处理过程都会中断。接下来将加载新配置并重新启动子系统，这

意味着将使用新设置重新建立所有计划以及其他内部基础结构。此问题更正了版本 10.1.8 中的一个已知问题。[CXM-47709，CXM-61330]

- 在升级期间，现有数据库配置不合并到新配置文件。现在，数据库配置将合并到升级后的配置文件。[CXM-49326]
- 在快照相关的诊断文件中，列标题缺失。这些标题都将还原。[CXM-62680]
- 从早期版本升级时，配置文件的默认设置部分被正在使用的配置文件中的类似部分覆盖。此问题阻止了服务在升级后加载在默认设置部分中添加或改进的功能。截至本版本，默认设置部分始终反映最新配置。[CXM-62681]
- 执行应用程序时，管理员将无法再通过按 Shift 键访问某些选项。这些选项以前是随 Citrix 权限提供的。现在，某些选项已完全可用（例如“允许重定向”），其他选项（例如，挂起检测和计数更正）已弃用。[CXM-62767]



版本 **10.1.8** 中的新增功能

版本 10.1.8 中修复了以下问题：

- Exchange 有可能会降低适用于 Exchange ActiveSync 服务的 Citrix Endpoint Management 连接器的速度，使其发出命令不会太频繁。这在与 Office 365 的连接中很常见。此限制产生的影响要求该服务先暂停一段指定的时间，然后再发送下一个命令。配置控制台现在显示剩余的暂停时间量。[CXM-48044]
- 修改了配置文件 (config.xml) 的 “Watchdog” 或 “SpecialistsDefaults” 部分时，所做的更改在升级后不反映在配置文件中。在本版本中，修改正确地合并到新配置文件中。[CXM-52523]

- 更多详细信息已添加到发送至 Google Analytics 的分析中，特别是相关的快照。[CXM-56691]
- Exchange 测试连接功能将仅尝试初始化连接一次。由于可以限制 Office 365 的连接，因此，受到限制时，测试连接可能会显示为失败。适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器现在最多尝试初始化连接三次。[CXM-58180]
- 为影响有关 Exchange 的策略，适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器必须将包括每个邮箱的所有相关设备的 **Set-CASMailbox** 命令编译到两个列表中，即允许和阻止列表。如果设备未包含在这两个列表中，Exchange 将回退到其默认访问状态。如果该默认访问状态与设备的所需状态不同，设备将变得不合规。因此，如果 Exchange 默认访问状态为阻止，但实际应为允许，用户可能会丢失对其电子邮件的访问权限。或者，应阻止其访问电子邮件的用户可能会被授予访问权限。适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器现在将确保具有有效所需状态的所有设备都包括在每个 **Set-CasMailbox** 命令中。[CXM-61251]

以下问题在版本 10.1.8 中属于已知问题：

如果管理员在配置应用程序中做出了修改配置数据的更改，而服务正在执行长时间持续进行的操作，例如快照或策略评估，服务可能会进入不确定的状态。可能会出现的症状可能为不处理策略更改，或者不启动快照。必须重新启动服务，才能将服务返回到工作状态。在启动服务之前，您可能需要使用 Windows 服务管理器终止服务。[CXM-61330]

版本 **10.1.7** 中的新增功能

- XenMobile Mail Manager 现已更名为适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
- 我们已弃用 Exchange 配置对话框中的 **Disable Pipelining**（禁用流水线操作）选项。可以在 config.xml 文件中为每个命令配置多个步骤来实现相同功能。[CXM-54593]

版本 10.1.7 中修复了以下问题：

- 在 “Snapshot History”（快照历史记录）窗口中，显示的错误消息可能几乎没有上下文。现在，错误消息的前缀为错误发生位置的上下文。[CXM-49157]
- XmmGoogleAnalytics.dll 没有与版本对应的文件版本。[CXM-52518]
- 为了改进诊断，我们最近更改了用于为邮箱设置 “允许/阻止” 状态的设备 ID 列表的字符串格式。但是，指定的设备太多会超过最大字符串大小。现在，我们使用内部数组数据结构。此结构没有大小限制，并且还会为数据设置合适格式以便用于诊断。[CXM-52610]
- 检测到未与 Exchange 同步的设备策略时，其命令可能包括不属于相关邮箱的设备。适用于 Exchange ActiveSync 的 Endpoint Management 连接器现在可确保针对 Exchange 的命令仅表示属于其各自邮箱的设备。[CXM-54842]
- 在某些环境中，Microsoft 程序集不可用。现在，所需的程序集明确与应用程序一起安装。[CXM-55439]
- 如果设备或邮箱的标识名中属性名称与等号之间有空格，和/或等号后面与值前面有空格，适用于 Exchange ActiveSync 的 Endpoint Management 连接器可能无法正确将设备与其邮箱匹配，反之亦然。这可能会导致在快照协调期间某些设备和/或邮箱被拒绝。[CXM-56088]

> 注意：
>
> 以下各节中在提到适用于 Exchange ActiveSync 的 Endpoint Management 连接器时使用其以前的名称

> XenMobile Mail Manager。名称自版本 10.1.7 起更改。

版本 **10.1.6.20** 中的更新

10.1.6 更新包含版本 10.1.6.20 中的以下修复：

- 检测到未与 Exchange 同步的设备策略时，其命令可能包括不属于相关邮箱的设备。XenMobile Mail Manager 现在可确保针对 Exchange 的命令仅表示属于其各自邮箱的设备。[CXM-54842]

版本 **10.1.6** 中的新增功能

XenMobile Mail Manager 版本 10.1.6 包含以下已修复的问题和增强功能：

- “Snapshot History”（快照历史记录）窗口有时会进入窗口不再更新的状态。改进了窗口刷新机制以更加可靠地更新。[CXM-47983]
- 对分区快照和非分区快照使用两个不同的模式和代码路径。由于非分区快照等同于使用单个 “*” 分区配置的分区快照，因此不需要非分区快照模式。现在，默认快照模式为具有 36 个分区（0-9、A-Z）的分区快照。[CXM-49093]
- 在 “Snapshot History”（快照历史记录）窗口中，错误消息会被状态消息覆盖。现在，XenMobile Mail Manager 提供两个单独的字段，以便用户可以同时查看状态和错误。[CXM-51942]
- 连接到 Exchange Online (Office 365) 时，快照相关查询可能会导致数据集被截断。XenMobile Mail Manager 执行多命令流水线脚本时，可能会出现此问题。上游命令无法足够快速地将数据传递给下游命令，这样下游命令就会提前完成工作，从而导致出现不完整的数据。现在，XenMobile Mail Manager 可以模仿流水线本身，并等到上游命令完成后再调用下游命令。经过此更改，所有数据都将得以处理和捕获。[CXM-52280]
- 如果在针对 Exchange 的策略更新命令中发生无法解决的错误，则会在很长一段时间内重复向工作队列返回相同命令。这种情况会导致多次向 Exchange 发送该命令。在此版本的 XenMobile Mail Manager 中，仅偶尔向工作队列返回导致出现错误的命令。[CXM-52633]
- 如果针对特定邮箱的策略更新涉及允许或阻止所有设备：由于空列表被转换为空字符串而不是 **NULL**，发出的 **Set-CASMailbox** 命令会失败。现在会发送正确的数据。[CXM-53759]
- 处理新设备时，Exchange 可能会在一段时间（通常为 15 分钟）内返回状态 “DeviceDiscovery”。以前，XenMobile Mail Manager 不会专门处理这种状态。现在，XenMobile Mail Manager 会处理这种状态。在 UI 的 “Monitor”（监视）选项卡中，用户可以过滤处于此状态的设备。[CXM-53840]
- 以前，XenMobile Mail Manager 不会检查是否能够向 XenMobile Mail Manager 数据库执行写入操作。因此，如果权限受到限制，可能无法预测行为。现在，XenMobile Mail Manager 会从数据库捕获并验证所需的权限。XenMobile Mail Manager 会在测试连接时（显示的消息）或在主配置窗口底部的数据库指示器（悬停显示消息）中指示降低的权限。[CXM-54219]
- 根据当前工作负载，在被定向时，XenMobile Mail Manager 服务可能无法迅速停止。因此，该服务看上去处于无响应状态。进行了一些改进后，正在进行的任务可以中断，因而可以比较正常地关闭。[CXM-54282]

版本 **10.1.5** 中的新增功能

XenMobile Mail Manager 版本 10.1.5 包含以下已修复的问题：

- Exchange 向 XenMobile Mail Manager 活动应用限制时，系统不会指示（在日志外部）发生了限制。在此版本中，用户可以将鼠标悬停在活动快照上，此时将显示 “限制” 状态。此外，XenMobile Mail Manager 受到限制时，在 Exchange 解除限制禁令之前，会禁止开始创建主要快照。[CXM-49617]
- 如果在创建主要快照期间 XenMobile Mail Manager 受到 Exchange 限制：可能是在下一次尝试创建快照之前，可以使用的时间不够。此问题会导致进一步限制和快照失败。现在，XenMobile Mail Manager 会在两次快照尝试之间等待 Exchange 指定的最小等待时间。[CXM-49618]
- 启用了诊断时，命令文件中显示的 **Set-CasMailbox** 命令中，每个属性名称前面都缺少连字符。仅在设置诊断文件的格式时会发生此问题，发送到 Exchange 的实际命令则不会发生此问题。由于缺少连字符，用户无法剪切命令并直接将其粘贴到 PowerShell 命令提示窗口进行测试或验证。现已添加连字符。[CXM-52520]
- 如果邮箱标识的格式为 “姓氏, 名字”，在从查询返回数据时，Exchange 会在逗号前面添加一个反斜杠。XenMobile Mail Manager 使用该标识查询更多数据时，必须去掉此反斜杠。[CXM-52635]

已知限制

> 注意：
>
> 以下限制在版本 10.1.6 中已解决。

XenMobile Mail Manager 存在一个可能会导致针对 Exchange 的命令失败的已知限制。为了向 Exchange 应用策略更改，XenMobile Mail Manager 会发出 **Set_CASMailbox** 命令。此命令可以接受两个设备列表：一个要允许的列表和一个要阻止的列表。此命令应用于与邮箱关联使用的设备。

这些列表不能超过 256 个字符（按 Microsoft API 划分的每个列表）。如果其中一个列表超过该限制，命令将完全失败，导致无法为与相应邮箱关联的设备设置所有策略。报告的错误（将显示在 XenMobile Mail Manager 日志中）类似如下所示。下面是阻止的列表示例。

“Message:’Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’ to the target. Exception setting “ActiveSyncBlockedDeviceIDs”: “The length of the property is too long. The maximum length is 256 and the length of the value provided is …””（消息: 无法将参数 ActiveSyncBlockedDeviceIDs 绑定到目标。设置 ActiveSyncBlockedDeviceIDs 时发生异常:“属性的长度太长。最大长度为 256，提供的值长度为…”）

设备 ID 长度可能会有所差别，但一条很好的指导原则是，同时允许或阻止大约 10 个或更多设备可能会超过该限制。虽然很少会出现许多设备与某个特定邮箱关联，但仍有可能出现。在 XenMobile Mail Manager 改进为能够处理此情况之前，我们建议您将与一个用户和邮箱关联的设备数限制在 10 以内。[CXM-52633]

版本 **10.1.4** 中的新增功能

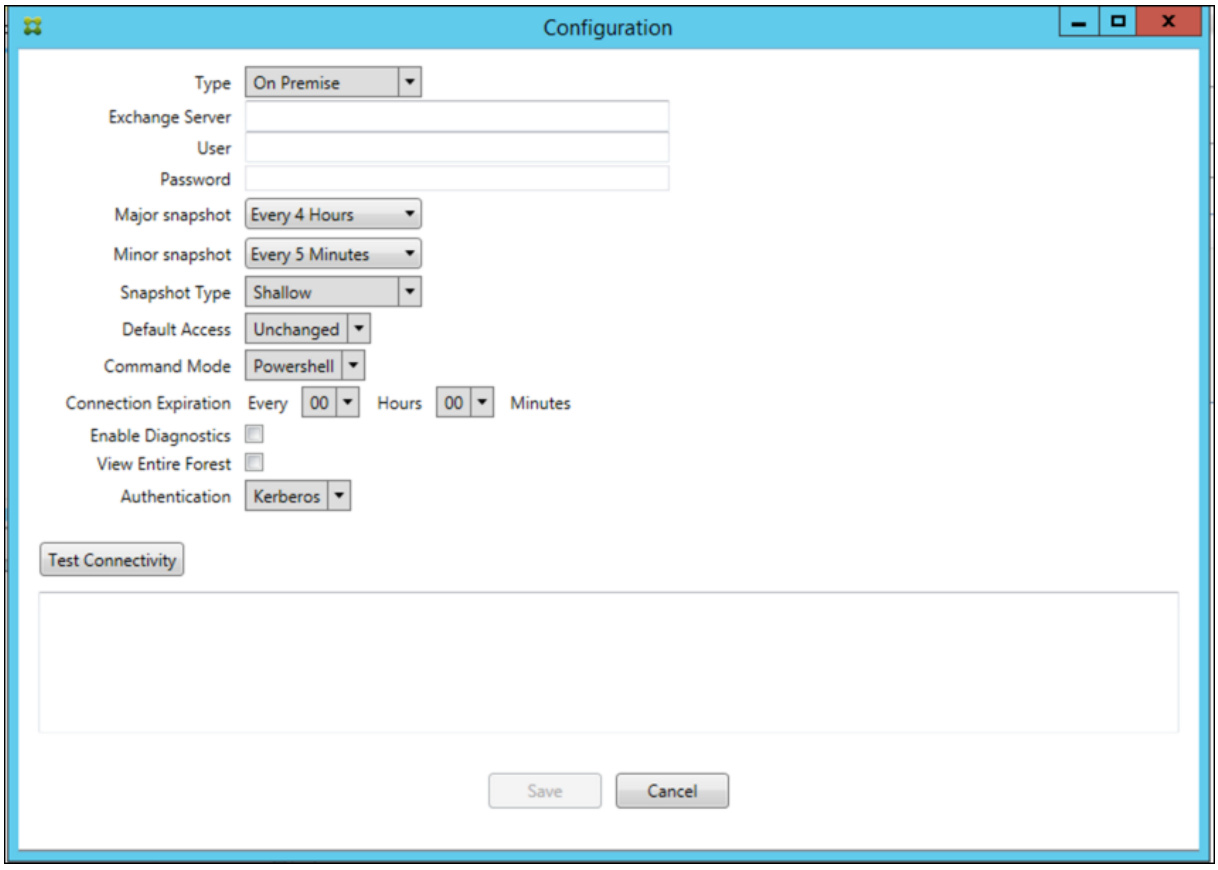
XenMobile Mail Manager 版本 10.1.4 包含以下已修复的问题：

- 由于其日渐削弱的安全性，PCI 委员会正在弃用 TLS 1.0。对 TLS 1.1 和 1.2 的支持已添加到 XenMobile Mail Manager 中。[CXM-38573、CXM-32560]
- XenMobile Mail Manager 包括一个新的诊断文件。在 Exchange 指定内容中选择了 **Enable Diagnostics**（启用诊断）时，将生成新的快照历史记录文件。在每次尝试创建快照时，都会向该文件中添加一行以记录快照结果。[CXM-49631]

- 在命令诊断文件中，**Set-CASMailbox** 命令不显示允许或阻止的设备列表。而是在该文件中的相关参数中显示内部类名称。现在，XenMobile Mail Manager 以逗号分隔的列表显示设备 ID 的列表。[CXM-50693]
- 由于指定内容错误导致尝试获取与 Exchange 的连接失败时：错误消息被不正确的消息覆盖：“All connections in use”（正在使用所有连接）。现在显示更具描述性的消息，例如，“All connections are inoperable”（所有连接均无法使用）、“Connection pool is empty”（连接池为空）、“All connections are throttled”（所有连接都受限制），以及 “No available connections”（没有可用的连接）。[CXM-50783]
- 在某些情况下，允许/阻止/擦除命令会在 XenMobile Mail Manager 内部缓存中排队多次。此问题导致发送到 Exchange 的命令出现延迟。XenMobile Mail Manager 现在仅排队每个命令的一个实例。[CXM-51524]

版本 **10.1.3** 中的新增功能

- **Google Analytics** 支持：我们希望了解您使用 XenMobile Mail Manager 的方式，以便我们可以专注于可以改进产品的方面。
- 用于启用诊断的设置：“Configure”(配置)控制台中的 **Configure**(配置)对话框中显示 **Enable Diagnostics**（启用诊断）复选框。



版本 **10.1.3** 中已修复的问题

- 在 **Snapshot History**（快照历史记录）窗口中，显示快照当前状态的工具提示不反映实际状态。[CXM-5570] 偶尔，XenMobile Mail Manager 无法向命令诊断文件中写入。发生此问题时，完全不记录命令历史记录。

[CXM-49217]

- 某个连接出错时，该连接可能无法标记为“出错”。因此，后续命令可能会尝试使用该连接，并导致出现另一个错误。[CXM-49495]
- 在 Exchange Server 中启用了限制时，可能会在检查运行状况例程中引发异常。因此，可能无法清除出错或已过期的连接。此外，在限制时间到期之前，XenMobile Mail Manager 可能无法创建连接。[CXM-49794]。
- 超过 Exchange 的最大会话计数后，XenMobile Mail Manager 报告“Device Capture Failed”（设备捕获失败）错误，此消息并不准确。相反，该消息应指明正在使用 XenMobile Mail Manager 通常用于 Exchange 通信的两个会话。[CXM-49994]

版本 **10.1.2** 中的新增功能

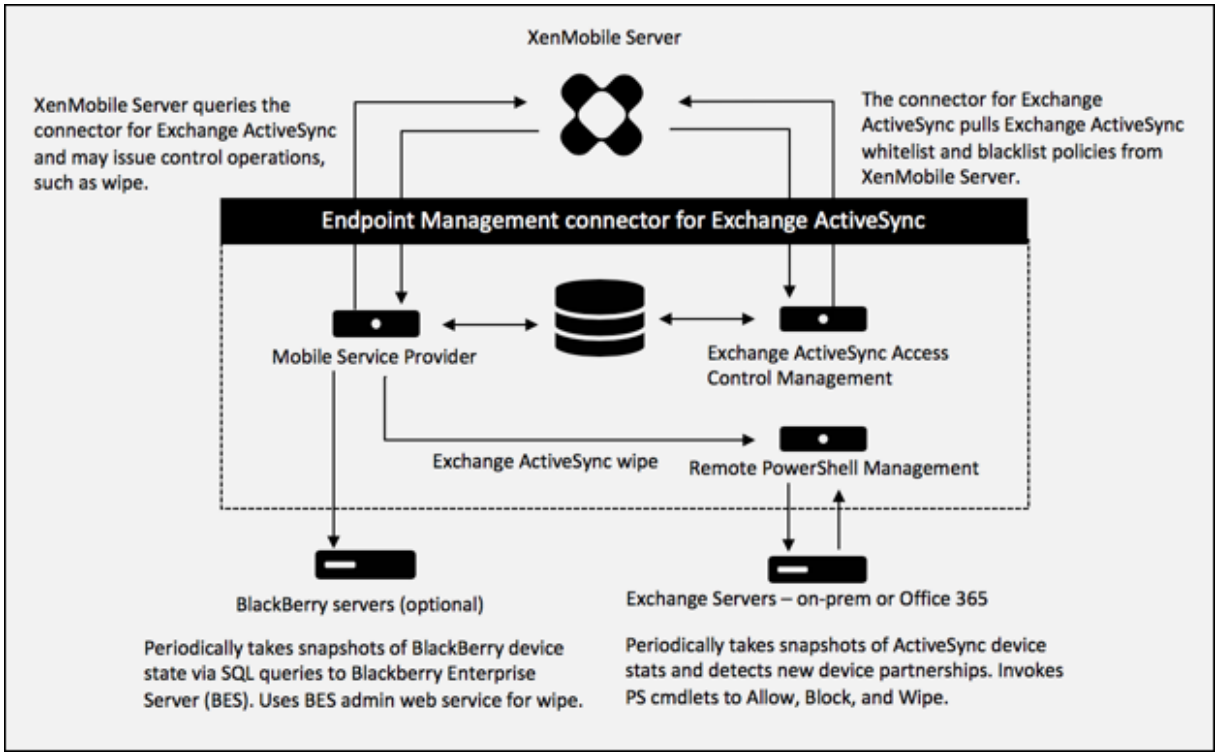
- 改进了与 **Exchange** 的连接：XenMobile Mail Manager 使用 PowerShell 会话与 Exchange 通信。尤其是在用于 Office 365 时，PowerShell 会话在一段时间之后可能会变得不稳定，从而阻止后续命令成功运行。现在可以在 XenMobile Mail Manager 中设置连接的过期期限。当连接达到其到期时间时，XenMobile Mail Manager 将正常关闭 PowerShell 会话，并创建一个会话。这样，PowerShell 会话不太可能变得不稳定，从而大大降低快照失败的可能性。
- 改进了快照工作流：主要快照是耗时的进程密集型操作。如果在创建快照期间发生错误，XenMobile Mail Manager 现在会多次（最多三次）尝试完成快照。后续尝试并不是从头开始。XenMobile Mail Manager 会从其中断的地方继续。此增强功能允许在创建快照期间出现短暂的错误，通常可提高快照的成功率。
- 改进了诊断：现在可以通过（可选）在创建快照期间生成的三个新诊断文件更加方便地进行快照故障排除操作。这些文件有助于确定 PowerShell 命令问题、缺少信息的邮箱以及无法与邮箱相关的设备。管理员可以使用这些文件确定 Exchange 中可能不正确的数据。
- 改进了内存使用率：XenMobile Mail Manager 使用内存的效率现已提高。管理员可以计划 XenMobile Mail Manager 自动重新启动以向系统提供初始状态。
- **Microsoft .NET Framework 4.6** 必备条件：现在，必须使用 Microsoft.NET Framework 版本 4.6。

已修复的问题

- 提示输入凭据错误：Office 365 会话不稳定通常会导致此错误。改进了与 Exchange 的连接增强功能解决了该问题。（XMHELP 293、XMHELP 311、XMHELP 801）
- 邮箱和设备计数不准确：XenMobile Mail Manager 改进了邮箱到设备关联算法。改进的诊断功能有助于确定 XenMobile Mail Manager 认为不在其职责领域的邮箱和设备。(XMHELP-623)
- 无法识别允许/阻止/擦除命令：修复了有时无法识别 XenMobile Mail Manager 允许/阻止/擦除命令的缺陷。(XMHELP-489)
- 内存管理：改进了内存管理和缓解。(XMHELP-419)

体系结构

下图显示了适用于 Exchange ActiveSync 的 Endpoint Management 连接器的主要组件。有关详细的参考体系结构图，请参阅体系结构。



这三个主要组件如下：

- **Exchange ActiveSync** 访问控制管理：与 XenMobile 进行通信以从 XenMobile 中检索 Exchange ActiveSync 策略，并将此策略与所有本地定义的策略合并以确定应被允许或拒绝访问 Exchange 的 Exchange ActiveSync 设备。本地策略允许扩展策略规则，以允许 Active Directory 组、用户、设备类型或设备用户代理（通常为移动平台版本）执行访问控制。
- 远程 **PowerShell** 管理：负责计划和调用远程 PowerShell 命令，以执行 Exchange ActiveSync 访问控制管理编译的策略。此组件定期创建 Exchange ActiveSync 数据库的快照，以检测新的或已更改的 Exchange ActiveSync 设备。
- 移动服务提供商：提供 Web 服务界面，以便 XenMobile 可以查询 Exchange ActiveSync、查询黑莓设备以及对 ActiveSync 和黑莓设备设备发出“擦除”等控制操作。

系统要求和必备条件

使用适用于 Exchange ActiveSync 的 Endpoint Management 连接器需要满足以下最低系统要求：

- Windows Server 2016、Windows Server 2012 R2 或 Windows Server 2008 R2 Service Pack 1。必须是基于英语的服务器。对 Windows Server 2008 R2 Service Pack 1 的支持将于 2020 年 1 月 14 日结束。
- Microsoft SQL Server 2016 Service Pack 2 或 SQL Server 2014 Service Pack 3。
- Microsoft .NET Framework 4.6。
- 黑莓 Enterprise Service 版本 5（可选）。

Microsoft Exchange Server 的最低支持版本：

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3（支持将于 2020 年 1 月 14 日结束）

必备条件

- 必须安装 Windows Management Framework。
  - PowerShell V5、V4 和 V3
- 必须通过 Set-ExecutionPolicy RemoteSigned 将 PowerShell 执行策略设置为 RemoteSigned。
- 必须在运行适用于 Exchange ActiveSync 的 Endpoint Management 连接器的计算机和远程 Exchange Server 之间打开 TCP 端口 80。
- 设备电子邮件客户端：并非所有电子邮件客户端都一致地为设备返回相同的 ActiveSync ID。由于适用于 Exchange ActiveSync 的 Endpoint Management 连接器要求每个设备具有唯一的 ActiveSync ID，因此，仅支持为每个设备一致地生成相同的唯一 ActiveSync ID 的电子邮件客户端。这些电子邮件客户端已通过 Citrix 测试，执行时没有错误：
  - Samsung 本机电子邮件客户端
  - iOS 本机电子邮件客户端
- **Exchange**：运行 Exchange 的本地计算机的要求如下所示：

  在 Exchange 配置用户界面中指定的凭据必须能够连接到 Exchange Server，并且具有执行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：
  - 针对 **Exchange Server 2010 SP2**：
    - Get-CASMailbox
    - Set-CASMailbox
    - Get-Mailbox
    - Get-ActiveSyncDevice
    - Get-ActiveSyncDeviceStatistics
    - Clear-ActiveSyncDevice
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment
  - 对于 **Exchange Server 2013** 和 **Exchange Server 2016**：
    - Get-CASMailbox
    - Set-CASMailbox
    - Get-Mailbox
    - Get-MobileDevice
    - Get-MobileDeviceStatistics

        * Clear-MobileDevice
        * Get-ExchangeServer
        * Get-ManagementRole
        * Get-ManagementRoleAssignment
    - 如果将适用于 Exchange ActiveSync 的 Endpoint Management 连接器配置为查看整个林，则必须授权运行 **Set-AdServerSettings -ViewEntireForest $true**
    - 提供的凭据必须具有通过远程 Shell 连接到 Exchange Server 的权限。默认情况下，安装 Exchange 的用户具有此权限。
    - 要建立远程连接并运行远程命令，凭据必须与远程计算机上的管理员用户相对应。可以使用 Set-PSSessionConfiguration 消除管理要求，但是对该命令的讨论不在本文档的范围内。有关详细信息，请参阅 Microsoft 文章关于会话配置。
    - 此外，Exchange Server 还必须配置为支持通过 HTTP 进行的远程 PowerShell 请求。通常，只需要在 Exchange Server 上运行下列 PowerShell 命令的管理员：WinRM QuickConfig。
    - Exchange 有许多限制策略。其中一个策略控制每个用户允许的并发 PowerShell 连接的数目。在 Exchange 2010 中，一个用户允许的同时连接数默认为 18。达到连接限制时，适用于 Exchange ActiveSync 的 Endpoint Management 连接器无法连接到 Exchange Server。存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。如果有兴趣，可以通过 PowerShell 调查与远程管理相关的 Exchange 限制策略。

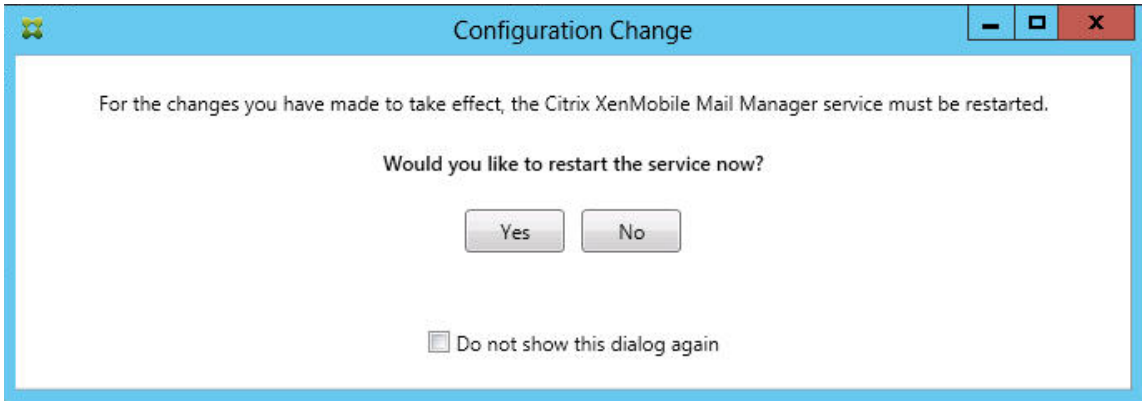
Office 365 Exchange 的要求

- 权限：在 Exchange 配置用户界面中指定的凭据必须能够连接到 Office 365，并且具有执行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：
    - Get-CASMailbox
    - Set-CASMailbox
    - Get-Mailbox
    - Get-MobileDevice
    - Get-MobileDeviceStatistics
    - Clear-MobileDevice
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment
- 特权：提供的凭据必须已获得授权，可以通过远程 Shell 连接到 Office 365 服务器。默认情况下，Office 365 联机管理员具有必备特权。
- 限制策略： Exchange 有许多限制策略。其中一个策略控制每个用户允许的并发 PowerShell 连接的数目。在 Office 365 中，一个用户允许的同时连接数默认为三个。达到连接限制时，适用于 Exchange ActiveSync 的 Endpoint Management 连接器无法连接到 Exchange Server。存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。如果有兴趣，可以通过 PowerShell 调查与远程管理相关的 Exchange 限制策略。

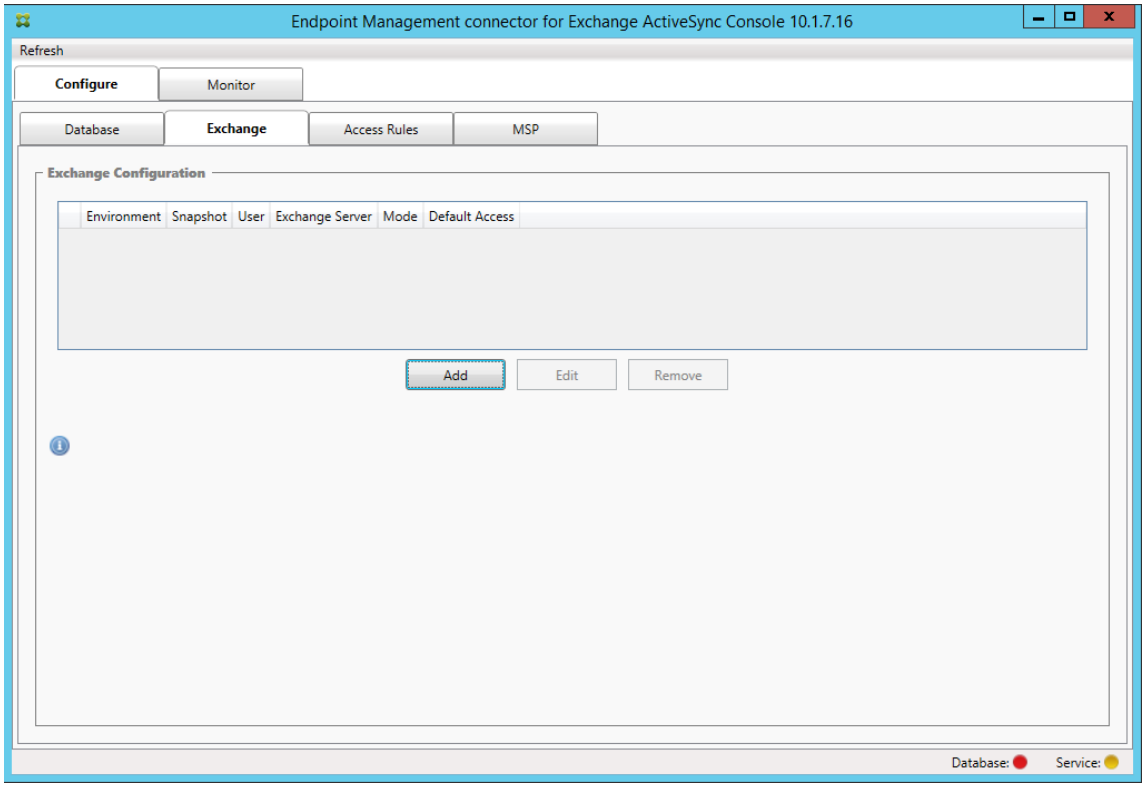
安装和配置

1. 单击 XmmSetup.msi 文件，然后按照安装程序中的提示安装适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
2. 在设置向导的最后一个屏幕中让 **Launch the Configure utility**（启动配置实用程序）保留选中。或者，从开始菜单中，打开适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
3. 配置以下数据库属性：
   - 选择 **Configure**（配置）**> Database**（数据库）选项卡。
   - 输入 SQL Server 的名称（默认值为 localhost）。
   - 将数据库保留为默认 **CitrixXmm**。
4. 选择以下用于 SQL 的身份验证模式之一：
   - **SQL**：输入有效 SQL 用户的用户名和密码。
   - **Windows Integrated**（**Windows** 集成）：如果选择此选项，则必须将适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务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，在适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务条目上单击鼠标右键，然后单击登录选项卡。

   如果还为黑莓数据库连接选择了 “Windows Integrated”（Windows 集成），必须同时为此处指定的 Windows 帐户提供黑莓数据库访问权限。
5. 单击 **Test Connectivity**（测试连接）检查是否可以连接到 SQL Server，然后单击 **Save**（保存）。
6. 此时将显示一条消息，提示您重新启动服务。单击是。



7. 配置一个或多个 Exchange Server：
   - 如果管理单个 Exchange 环境，则仅指定一台服务器。如果管理多个 Exchange 环境，则为每个 Exchange 环境指定一个 Exchange Server。
   - 单击 **Configure**（配置）**> Exchange** 选项卡，然后单击 **Add**（添加）。



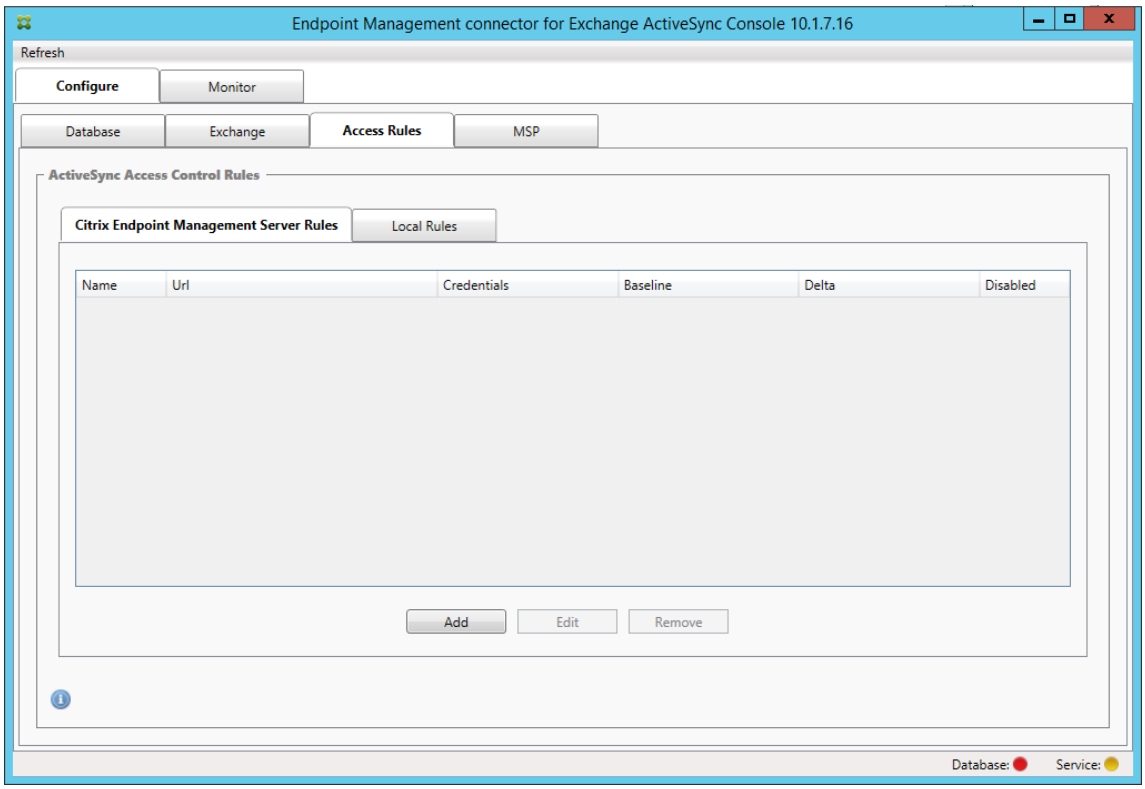
8. 选择 Exchange Server 环境的类型：**On Premise**（本地）或 **Office 365**。

   - 如果选择 **On Premise**（本地），请输入要用于远程 PowerShell 命令的 Exchange Server 名称。
   - 输入在“要求”部分中指定的 Exchange Server 上具有适当权限的 Windows 身份的用户名，然后输入该用户的密码。
   - 选择运行主要快照的计划。主要快照检测每个 Exchange ActiveSync 合作关系。
   - 选择运行次要快照的计划。次要快照检测新创建的 Exchange ActiveSync 合作关系。
   - 选择“Snapshot Type”（快照类型）：**Deep**（深层）或 **Shallow**（浅层）。浅层快照通常更快并且足以执行适用于 Exchange ActiveSync 的 Endpoint Management 连接器的所有 Exchange ActiveSync 访问控制功能。深层快照可能需要花费更长时间，并且仅在为 ActiveSync 启用移动服务提供商后才需要。此选项允许 XenMobile 查询非托管设备。
   - 选择默认访问：**Allow**（允许）、**Block**（阻止）或 **Unchanged**（保持不变）。此设置控制如何处理显式 XenMobile 或本地规则确定的设备以外的所有设备。如果选择 **Allow**（允许），则允许 ActiveSync 访问所有此类设备。如果选择 **Block**（阻止），则拒绝访问。如果选择 **Unchanged**（保持不变），则不进行任何更改。
   - 选择 ActiveSync 命令模式：**PowerShell** 或 **Simulation**（模拟）。
   - 在 **PowerShell** 模式下，适用于 Exchange ActiveSync 的 Endpoint Management 连接器会发出 PowerShell 命令以执行所需的访问控制。在“Simulation”（模拟）模式下，适用于 Exchange ActiveSync 的 Endpoint Management 连接器不发出 PowerShell 命令，但是会将预期命令和预期结果记录到数据库中。在“Simulation”（模拟）模式下，用户随后可使用 **Monitor**（监视）选项卡查看启用 PowerShell 模式时会发生的情况。
   - 在 **Connection Expiration**（连接过期）中，设置连接存在的小时数和分钟数。当连接达到指定的期

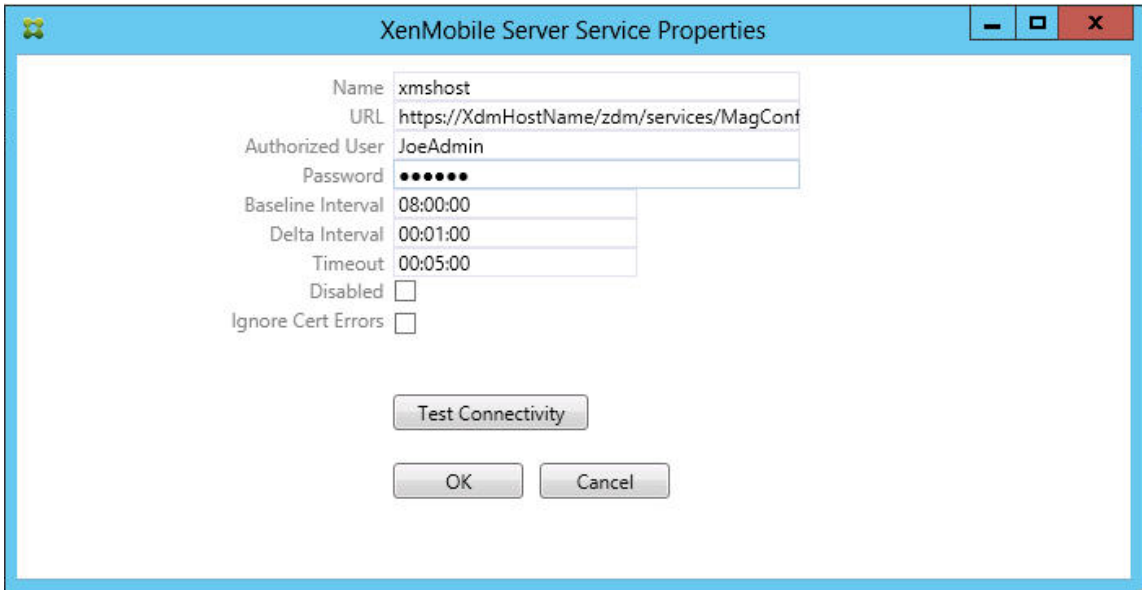
限时，该连接将被标记为已过期，以便绝不会再次使用该连接。当不再使用已过期的连接时，适用于 Exchange ActiveSync 的 Endpoint Management 连接器将正常关闭该连接。再次需要连接时，如果没有连接可用，则会初始化新连接。如果未指定，则将使用默认值 30 分钟。

- 选择 **View Entire Forest**（查看整个林）可将适用于 Exchange ActiveSync 的 Endpoint Management 连接器配置为查看 Exchange 环境中的整个 Active Directory 林。
- 选择身份验证协议：**Kerberos** 或 **Basic**（基本）。适用于 Exchange ActiveSync 的 Endpoint Management 连接器支持本地部署的“Basic”(基本)身份验证。这样，当适用于 Exchange ActiveSync 的 Endpoint Management 连接器不是 Exchange Server 常驻的域的成员时，可以使用适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
- 单击 **Test Connectivity**（测试连接）检查是否可以连接到 Exchange Server，然后单击 **Save**（保存）。
- 此时将显示一条消息，提示您重新启动服务。单击是。

9. 配置访问规则：选择 **Configure**（配置）**> Access Rules**（访问规则）选项卡，单击 **XMS Rules**（XMS 规则）选项卡，然后单击 **Add**（添加）。



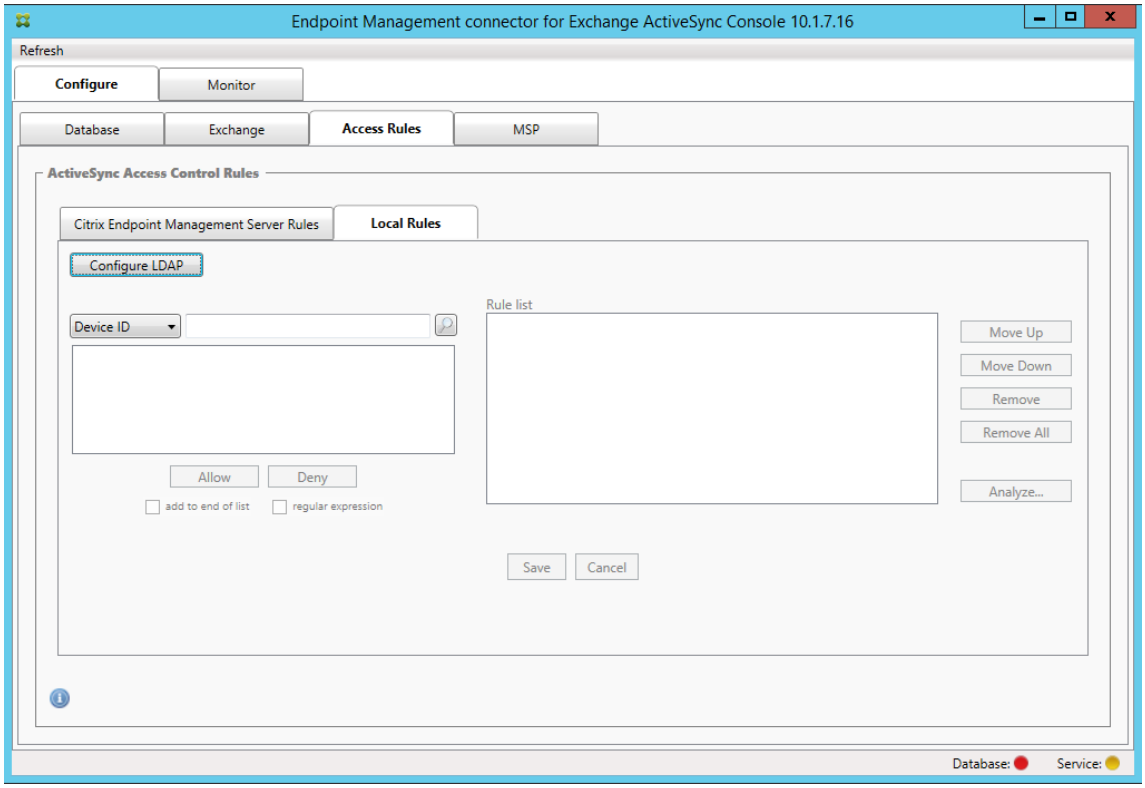
10. 在 **XenMobile server Service Properties**（XenMobile Server 服务属性）页面上，修改 URL 字符串以指向 XenMobile Server。例如，如果实例名称为 **zdm**，则输入 `https://<XdmHostName>/zdm/services/MagConfigService`。在此示例中，将 **XdmHostName** 替换为 XenMobile Server 的 IP 或 DNS 地址。



- 输入服务器的授权用户。
- 输入用户密码。
- 保留 **Baseline Interval**（基准时间间隔）、**Delta Interval**（时间间隔差）和 **Timeout**（超时）值的默认值。
- 单击 **Test Connectivity**（测试连接）检查与服务器的连接，然后单击 **OK**（确定）。

如果选中 **Disabled**（已禁用）复选框，XenMobile Mail Service 将不从 XenMobile 收集策略。

11. 单击 **Local Rules**（本地规则）选项卡。

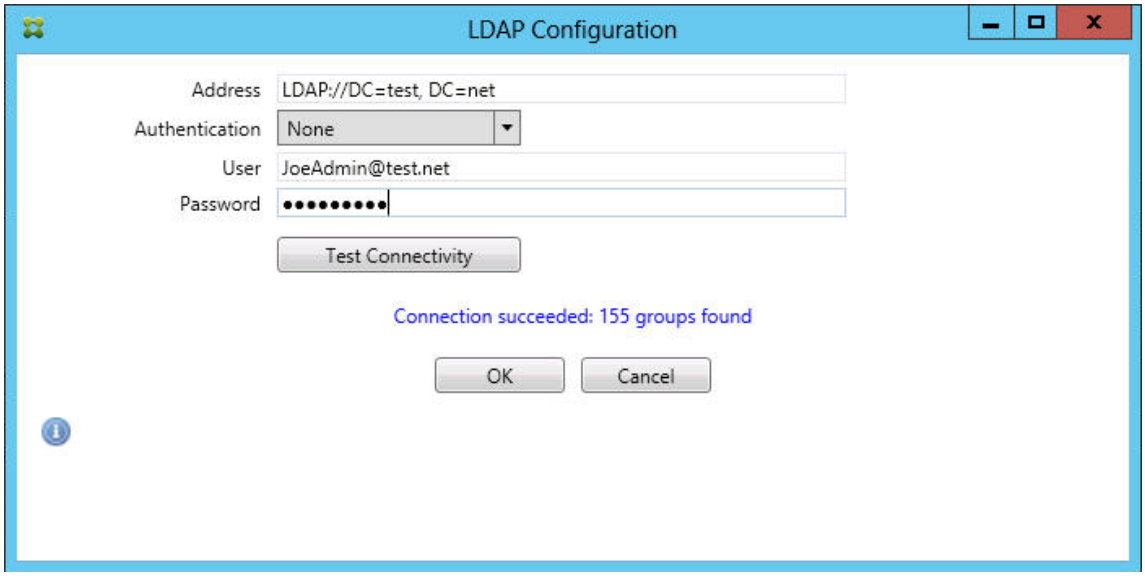


- 您可以根据 ActiveSync 的“Device ID”（设备 ID）、“Device Type”（设备类型）、“AD Group”（AD 组）、“User”（用户）或设备“UserAgent”（用户代理）添加本地规则。在列表中选择适当的类型。
- 在文本框中输入文本或文本片段。也可单击查询按钮，查看与片段匹配的实体。

对于除“Group”（组）以外的所有类型，系统依赖在快照中找到的设备。因此，如果刚刚开始且尚未完成快照，则没有实体可用。

- 选择一个文本值，然后单击 **Allow**（允许）或 **Deny**（拒绝），将其添加到右侧的 **Rule List**（规则列表）窗格。可使用 **Rule List**（规则列表）窗格右侧的按钮更改规则的顺序或移除规则。该顺序很重要，因为对于指定的用户和设备，将按照显示的顺序评估规则，并且一旦与较靠前的规则（离顶部较近）匹配，则后续的规则将失效。例如，如果存在一条允许所有 iPad 设备的规则，而后续的规则阻止用户 Matt，则 Matt 的 iPad 将仍被允许，因为 iPad 规则的有效优先级高于 Matt 规则。
- 要对规则列表中的规则进行分析以找到潜在的覆盖、冲突或补充结构，请单击 **Analyze**（分析），然后单击 **Save**（保存）。

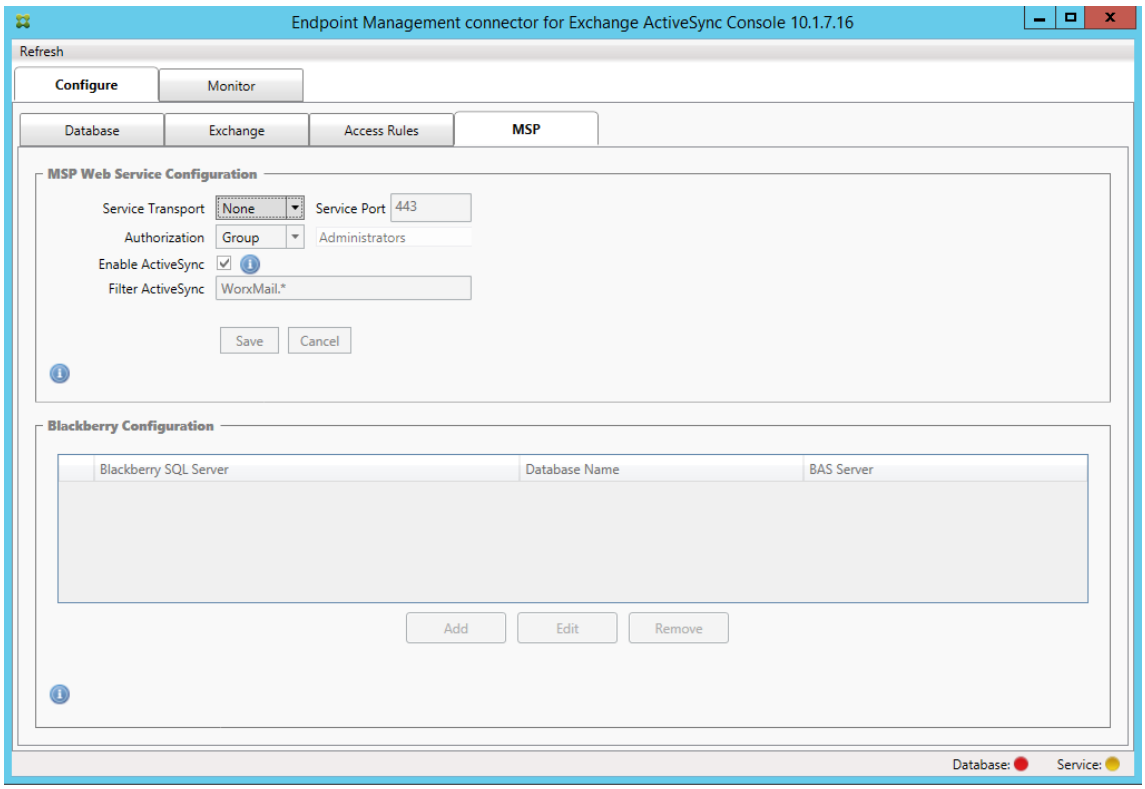
12. 如果要建立应用于 Active Directory 组的本地规则，请单击 **Configure LDAP**（配置 LDAP），然后配置 LDAP 连接属性。



13. 配置移动服务提供商。

移动服务提供商可选。仅当同时将 XenMobile 配置为使用移动服务提供商界面查询非托管设备时需要使用该设置。

- 单击 **Configure**（配置）**> MSP** 选项卡。

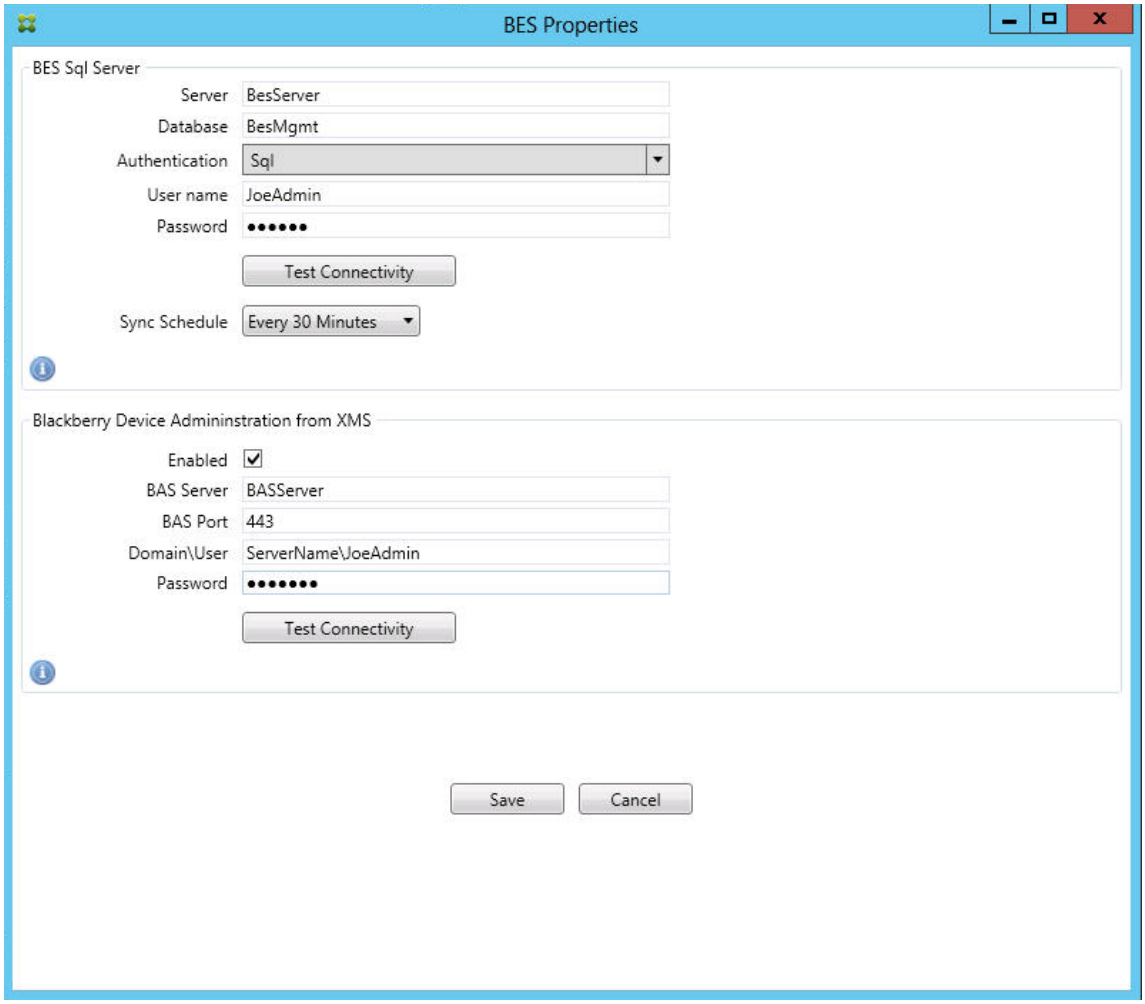


- 为移动服务提供商服务设置“Service Transport”（服务传输）类型：**HTTP** 或 **HTTPS**。
- 为移动服务提供商服务设置 **Service Port**（服务端口）（通常为 80 或 443）。如果使用端口 443，该端

口需要在 IIS 中绑定 SSL 证书。

- 将 “Authorization”（授权）设置为 **Group**（组）或 **User**（用户）。这样可以设定能够从 XenMobile 连接到移动服务提供商服务的用户或用户组。
- 设置是否已启用 ActiveSync 查询。如果为 XenMobile Server 启用了 ActiveSync 查询，则一个或多个 Exchange Server 的快照类型必须设置为 **Deep**（深层）。该设置可能会导致在获取快照时性能显著下降。
- 默认情况下，不会将与正则表达式 WorxMail.* 匹配的 ActiveSync 设备发送到 XenMobile。要更改此行为，请根据需要更改 **Filter ActiveSync**（过滤 ActiveSync）字段。
  空白意味着所有设备都将转发到 XenMobile。
- 单击保存。

14. （可选）配置 BlackBerry Enterprise Server (BES) 的一个或多个实例：单击 **Add**（添加），然后输入 BES SQL Server 的服务器名称



- 输入 BES 管理数据库的数据库名称。
- 选择 **Authentication**（身份验证）模式。如果选择 “Windows Integrated”（Windows 集成）身份验证，则适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务的用户帐户就是用于

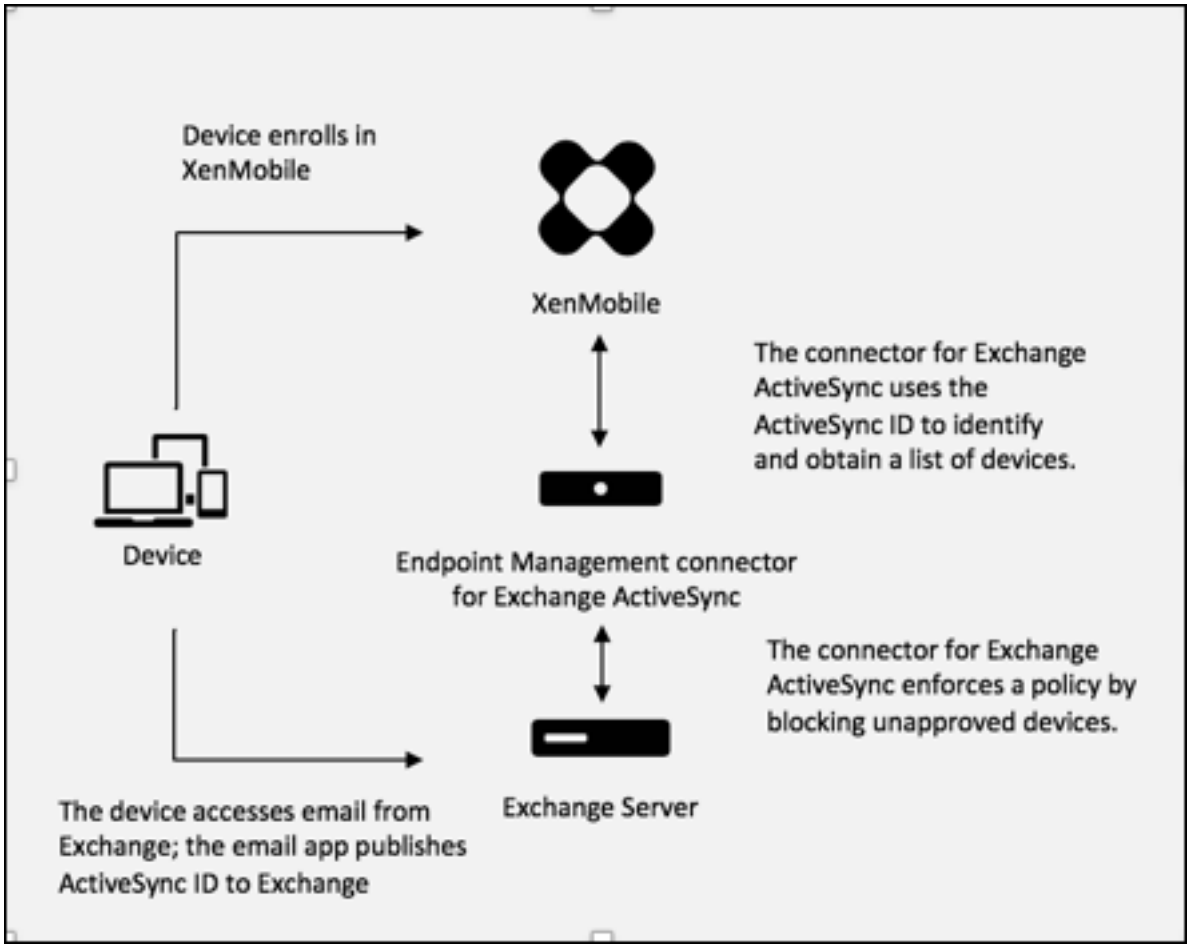
连接 BES SQL Server 的帐户。如果还为适用于 Exchange ActiveSync 的 Endpoint Management 连接器选择了 “Windows Integrated”（Windows 集成），则还必须为在此处指定的 Windows 帐户提供对适用于 Exchange ActiveSync 的 Endpoint Management 连接器数据库的访问权限。

- 如果选择 **SQL authentication**（SQL 身份验证），请输入用户名和密码。
- 设置 **Sync Schedule**（同步计划）。这是用于连接到 BES SQL Server 并检查任何设备更新的计划。
- 单击 **Test Connectivity**（测试连接）检查与 SQL Server 的连接。如果选择 “Windows Integrated”（Windows 集成），则此测试会使用当前登录的用户而非适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务用户，因此无法准确测试 SQL 身份验证。
- 要支持从 XenMobile 对黑莓设备进行远程擦除和重置密码的功能，请选中 **Enabled**（已启用）复选框。
- 输入 BES 完全限定的域名 (FQDN)。
- 输入用于管理 Web 服务的 BES 端口。
- 输入 BES 服务必需的完全限定用户和密码。
- 单击 **Test Connectivity**（测试连接）测试与 BES 的连接。
- 单击保存。

使用 **ActiveSync ID** 强制执行电子邮件策略

您的企业电子邮件策略可以规定不批准特定设备使用企业电子邮件。为与此策略保持一致，您希望确保员工无法通过此类设备访问企业电子邮件。适用于 Exchange ActiveSync 的 Endpoint Management 连接器和 XenMobile 会共同协作以强制实施此类电子邮件策略。XenMobile 会设置用于企业电子邮件访问的策略，当未经批准的设备向 XenMobile 注册时，适用于 Exchange ActiveSync 的 Endpoint Management 连接器会强制实施此策略。

设备上的电子邮件客户端使用设备 ID（也称为 ActiveSync ID，用于标识设备）向 Exchange Server（或 Office 365）广播自己。Secure Hub 获取类似的标识符，并在注册设备时将标识符发送给 XenMobile。通过比较两个设备 ID，适用于 Exchange ActiveSync 的 Endpoint Management 连接器可以确定特定设备是否应该具有企业电子邮件访问权限。下图说明了此概念：



如果 XenMobile 向适用于 Exchange ActiveSync 的 Endpoint Management 连接器发送的 ActiveSync ID 与设备发布到 Exchange 的 ID 不同，则适用于 Exchange ActiveSync 的 Endpoint Management 连接器无法指示 Exchange 应对该设备采取何种操作。

匹配 ActiveSync ID 可以在大多数平台上可靠地执行。但是，Citrix 已发现在某些 Android 实现上，来自设备的 ActiveSync ID 不同于邮件客户端向 Exchange 广播的 ID。为缓解此问题，可以执行以下操作：

- 在 Samsung SAFE 平台上，从 XenMobile 推送设备 ActiveSync 配置。

为保证正确地强制实施企业电子邮件访问策略，可以通过将静态策略默认设置为“拒绝”来采取防御性安全措施，将适用于 Exchange ActiveSync 的 Endpoint Management 连接器配置为阻止电子邮件。这意味着，如果员工在 Android 设备上配置了电子邮件客户端，并且如果 ActiveSync ID 检测不能正常运行，则将拒绝该员工访问企业电子邮件。

访问控制规则

适用于 Exchange ActiveSync 的 Endpoint Management 连接器提供了一种基于规则的方法，为 Exchange ActiveSync 设备动态配置访问控制。适用于 Exchange ActiveSync 的 Endpoint Management 连接器访问控制规则由两部分组成，即一个匹配的表达式和一个所需的访问状态（“允许”或“阻止”）。规则可能会针对给定的 Exchange

ActiveSync 设备进行评估，以确定该规则是否适用于该设备或是否与该设备匹配。有多种匹配的表达式；例如，一条规则可能与给定“设备类型”（或特定 Exchange ActiveSync 设备 ID）的所有设备或者特定用户的所有设备等匹配。

在规则列表中添加、删除和重新排列规则期间，任何时候单击取消按钮都会将规则列表还原回首次打开时的状态。除非单击保存，否则关闭配置工具时将丢失您对此窗口所做的任何更改。

适用于 Exchange ActiveSync 的 Endpoint Management 连接器有三种类型的规则，即本地规则、XenMobile Server 规则（也称为 XDM 规则）和默认访问规则。

本地规则：本地规则的优先级最高：如果设备与本地规则匹配，规则评估将停止。既不查询 XenMobile Server 规则也不查询默认访问规则。本地规则是通过 **Configure**（配置）**> Access Rules**（访问规则）**> Local Rules**（本地规则）选项卡在适用于 Exchange ActiveSync 的 Endpoint Management 连接器中本地配置的。支持匹配基于给定的 Active Directory 组内用户的成员身份。支持匹配基于以下字段的正则表达式：

- ActiveSync Device ID（ActiveSync 设备 ID）
- ActiveSync Device Type（ActiveSync 设备类型）
- User Principal Name (UPN)（用户主体名称 (UPN)）
- ActiveSync User Agent（ActiveSync 用户代理）（通常为设备平台或电子邮件客户端）

只要完成了主要快照并找到设备，您应能够添加常规或正则表达式规则。如果尚未完成主要快照，则只能添加正则表达式规则。

XenMobile Server 规则：XenMobile Server 规则是对提供托管设备相关规则的外部 XenMobile Server 的引用。XenMobile Server 可通过自身的高级规则进行配置，这些规则可标识要基于 XenMobile 已知属性允许或阻止的设备（例如设备是否越狱或设备是否包含禁用的应用程序）。XenMobile 将评估高级规则并生成一组允许或阻止的 ActiveSync 设备 ID，然后将其传递到适用于 Exchange ActiveSync 的 Endpoint Management 连接器。

默认访问规则：默认访问规则是唯一的，它可以潜在匹配每个设备，并且始终是最后一个被评估。此规则是一条笼统的规则，这意味着如果给定的设备与本地规则或 XenMobile Server 规则不匹配，该设备的所需访问状态将由默认访问规则的所需访问状态决定。

- **Default Access - Allow**（默认访问 **-** 允许）：允许与本地规则或 XenMobile Server 规则不匹配的任何设备。
- **Default Access - Block**（默认访问 **-** 阻止）：阻止与本地规则或 XenMobile Server 规则不匹配的任何设备。
- **Default Access - Unchanged**（默认访问 **-** 未更改）：与本地规则或 XenMobile Server 规则不匹配的任何设备将不会由适用于 Exchange ActiveSync 的 Endpoint Management 连接器以任何方式修改其访问状态。如果设备已被 Exchange 置于隔离模式，则不会采取任何措施；例如，从隔离模式删除设备的唯一方法是使用显式本地规则或 XDM 规则覆盖隔离。

关于规则评估

对于 Exchange 向适用于 Exchange ActiveSync 的 Endpoint Management 连接器报告的每个设备，将按照优先级从最高到最低的顺序对这些规则进行评估，如下所示：

- 本地规则
- XenMobile Server 规则

- 默认访问规则

找到匹配项时，评估将停止。例如，如果本地规则与给定设备匹配，则不会根据任何 XenMobile Server 规则或默认访问规则对该设备进行评估。这同样适用于给定的规则类型。例如，如果本地规则列表中有多条规则与某个给定设备匹配，则遇到第一个匹配项时，评估即停止。

当设备属性发生变化、添加或删除设备或者规则本身发生变化时，适用于 Exchange ActiveSync 的 Endpoint Management 连接器会重新评估当前定义的规则集合。主要快照以可配置的时间间隔选取设备属性更改和删除操作。次要快照以可配置的时间间隔选取新设备。

Exchange ActiveSync 还具有控制访问的规则。了解这些规则在适用于 Exchange ActiveSync 的 Endpoint Management 连接器的上下文中的工作方式至关重要。Exchange 可能通过以下三种级别的规则进行配置：个人免除、设备规则以及组织设置。适用于 Exchange ActiveSync 的 Endpoint Management 连接器通过以编程方式发出远程 PowerShell 请求来自动化访问控制，以影响个人免除列表。这些是与给定邮箱关联的允许和阻止的 Exchange ActiveSync 设备 ID 列表。部署后，适用于 Exchange ActiveSync 的 Endpoint Management 连接器有效地接替了 Exchange 中免除列表的管理功能。有关详细信息，请参阅 Microsoft 文章控制设备访问。

在为相同的字段定义了多条规则的情况下，分析特别有用。您可以对规则之间的关系进行故障排除。请从规则字段的角度来执行分析；例如，规则是基于匹配的字段（例如 ActiveSync 设备 ID、ActiveSync 设备类型、用户、用户代理等）按组进行分析的。

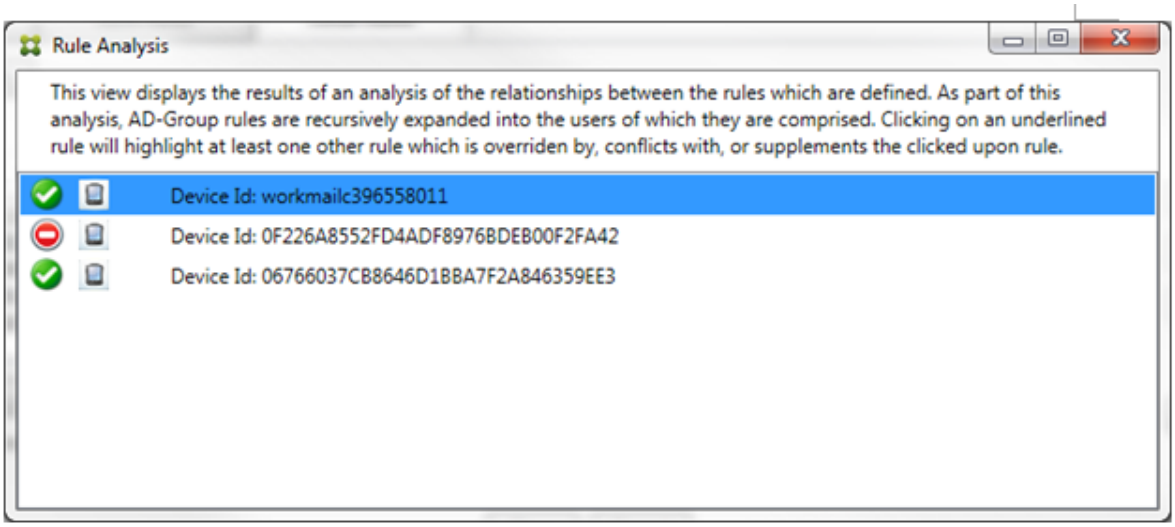
规则术语

- 覆盖规则：当多条规则可以应用于同一设备时会发生覆盖。因为规则是按照列表中的优先级进行评估的，可能会应用的后面的规则实例可能永远不会被评估。
- 冲突规则：当多条规则可以应用于同一设备但访问状态（允许/阻止）不匹配时会发生冲突。如果冲突规则不是正则表达式规则，冲突将始终隐式包含覆盖
- 补充规则：当多条规则是正则表达式规则，因此可能需要确保两个（或多个）正则表达式可以合并到一条正则表达式规则中或者不是重复功能时，会发生补充。补充规则的访问状态（允许/阻止）可能还会发生冲突。
- 主要规则：主要规则是已在对话框内单击的规则。规则通过围绕它的实线框可视化地指示出来。该规则还将具有一个或两个绿色箭头，用来指示向上或向下方向。如果箭头指向上方，该箭头指示辅助规则在主要规则前面。如果箭头指向下方，该箭头指示辅助规则在主要规则后面。只有一个主要规则可以随时处于活动状态。
- 辅助规则：辅助规则以某种方式与主要规则相关（通过覆盖、冲突或补充关系）。规则通过围绕它的虚线框可视化地指示出来。对于每条主要规则，可以一条主要规则对应多条辅助规则。单击任何带有下划线的条目时，始终从主要规则的角度突出显示一条或多条辅助规则。例如，辅助规则被主要规则覆盖，和/或辅助规则的访问状态与主要规则冲突，和/或辅助规则对主要规则进行补充。

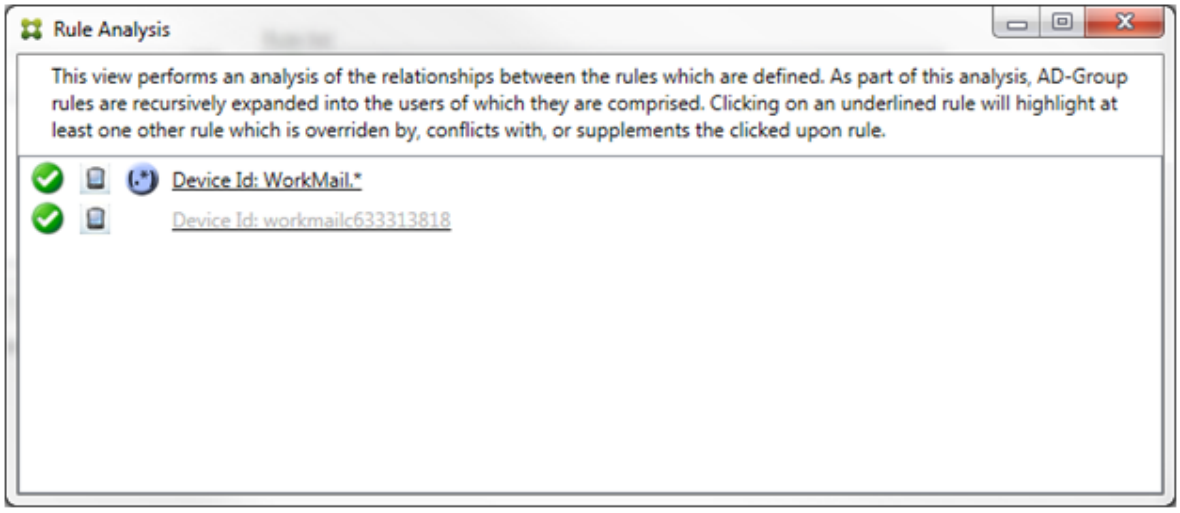
规则类型在 **“Rule Analysis”**（规则分析）对话框中的显示方式

没有冲突、覆盖或补充时，“Rule Analysis”（规则分析）对话框中没有带下划线的条目。单击任何项目都没有效果；例如，出现正常选定项目的视觉效果。

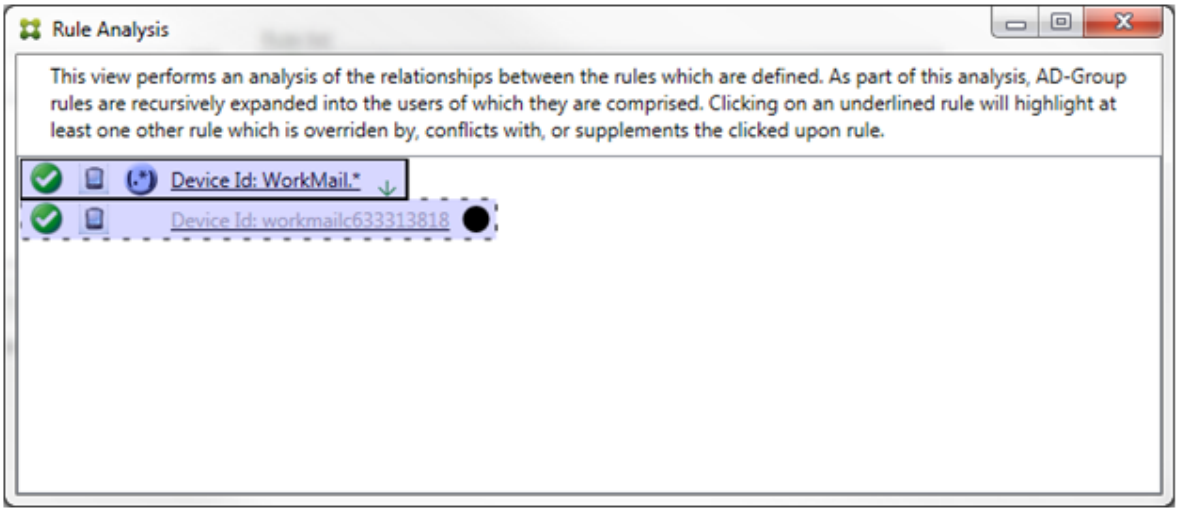
“Rule Analysis”（规则分析）窗口包含一个复选框，选中该复选框时，将仅显示冲突、覆盖、冗余或补充规则。



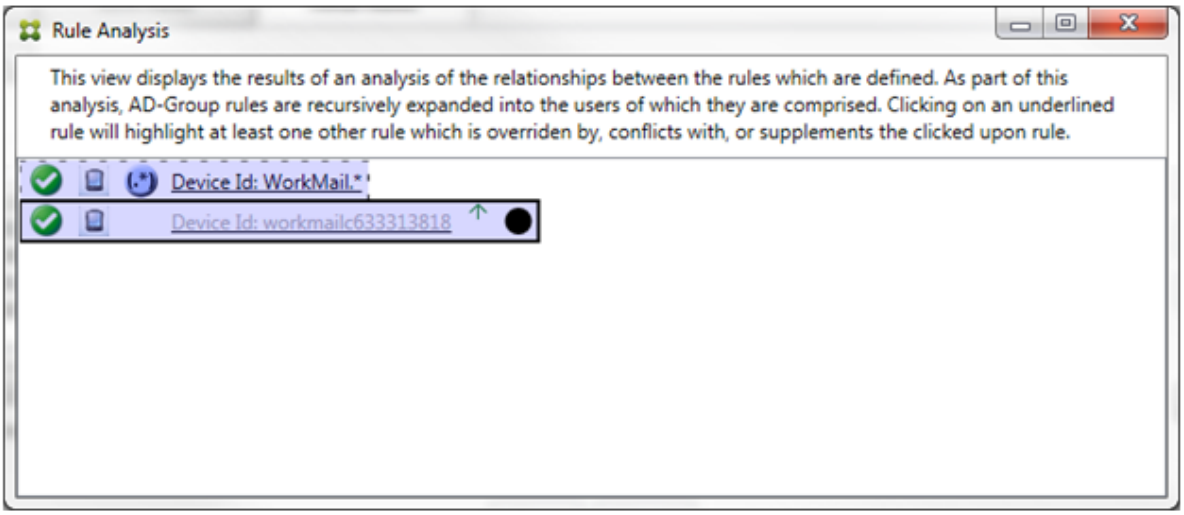
当出现覆盖时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。至少有一条辅助规则以较浅字体显示，指示该规则已被优先级较高的规则覆盖。您可以单击被覆盖的规则以了解覆盖该规则的一条或多条规则。每当被覆盖的规则由于该规则是主要规则或辅助规则而突出显示时，它旁边都会显示一个黑色圆圈，以进一步指示该规则处于不活动状态。例如，在单击该规则之前，对话框显示如下：



单击优先级最高的规则时，对话框显示如下：

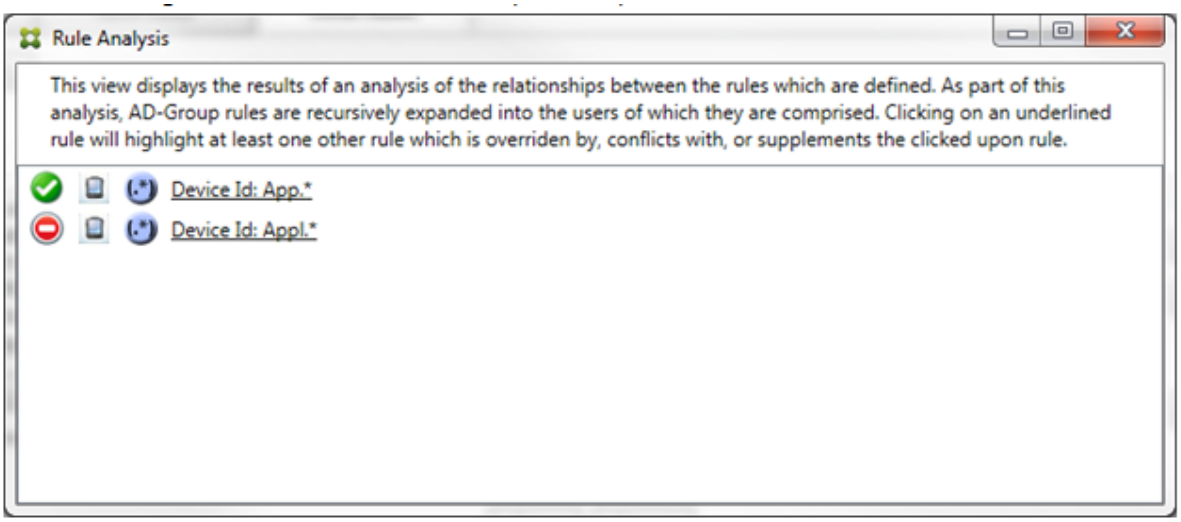


在此示例中，正则表达式规则 `WorkMail.*` 是主要规则（以实线框指示），常规规则 `workmailc633313818` 是辅助规则（以虚线框指示）。辅助规则旁边的黑点是一个视觉提示，可进一步指示由于它的前面有较高优先级的正则表达式而处于不活动状态（永远不会被评估）。单击被覆盖的规则后，对话框显示如下：

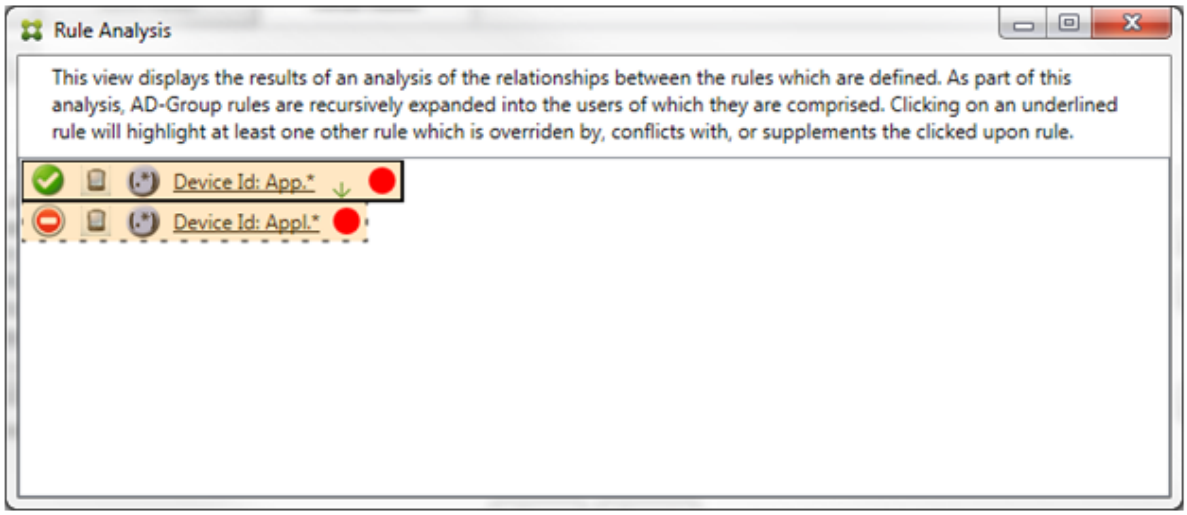


在前面的示例中，正则表达式规则 `WorkMail.*` 是辅助规则（以虚线框指示），常规规则 `workmailc633313818` 是主要规则（以实线框指示）。对于这一简单的示例，没有太大差异。对于更为复杂的示例，请参阅本主题中后面所述的复杂表达式示例。在定义了许多规则的情景中，单击被覆盖的规则将快速识别已覆盖该规则的一条或多条规则。

当出现冲突时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。发生冲突的规则用红点指示。只有相互冲突的规则才可能定义了两条或多条正则表达式规则。在所有其他冲突情景中，不仅将有冲突，而且还会发生覆盖。在简单的示例中单击任一规则之前，对话框显示如下：

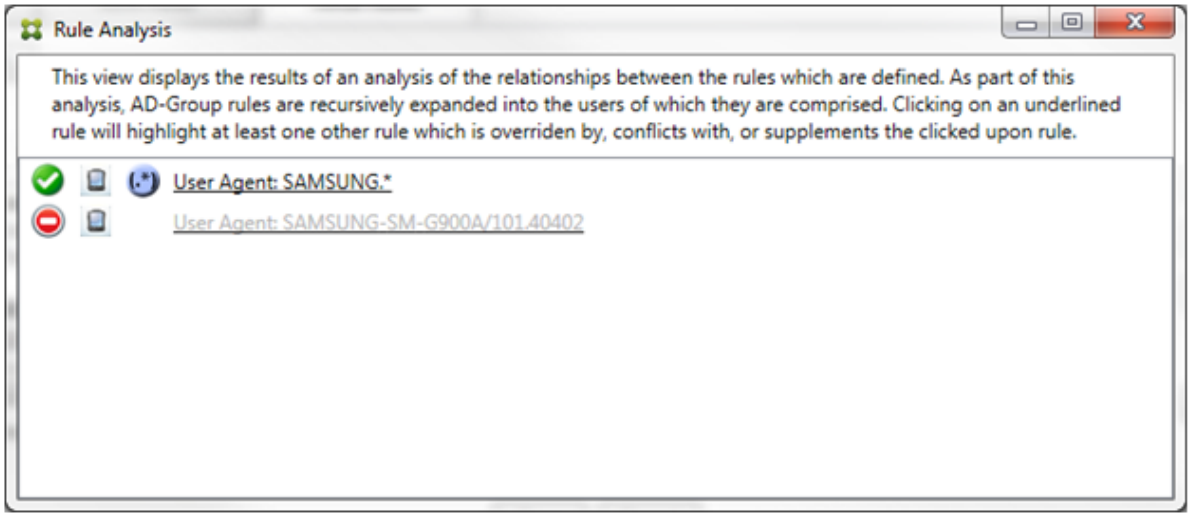


检查这两条正则表达式规则即可明显发现，第一条规则允许设备 ID 包含 “App” 的所有设备，第二条规则拒绝设备 ID 包含 “Appl” 的所有设备。此外，即使第二条规则拒绝了设备 ID 包含 “Appl” 的所有设备，也不会拒绝符合条件的设备，因为允许规则的优先级较高。单击第一条规则后，对话框显示如下：



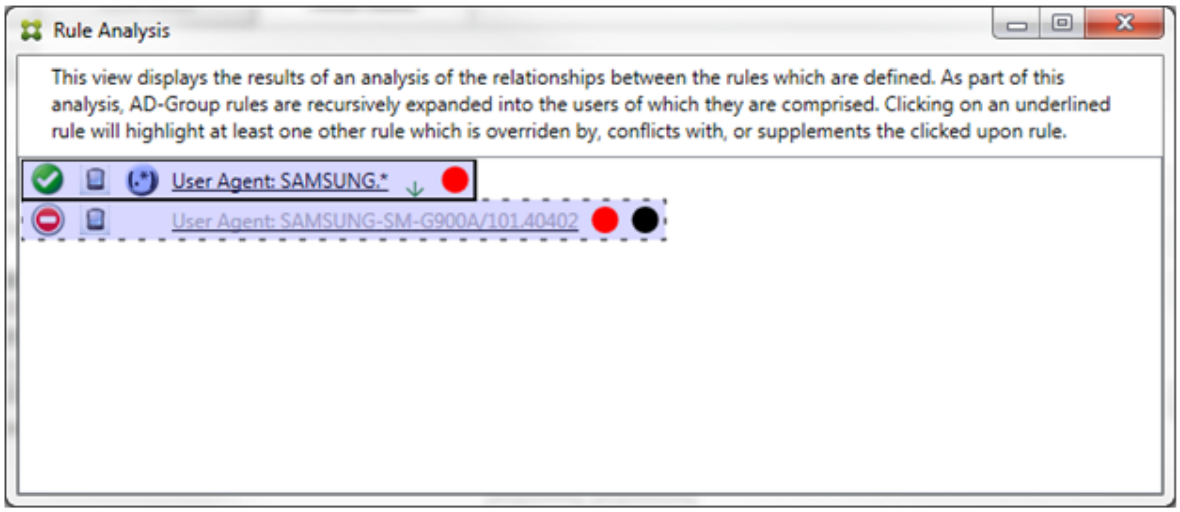
在上述情景中，主要规则（正则表达式规则 `App.*`）和辅助规则（正则表达式规则 `Appl.*`）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

在同时存在冲突和覆盖的情景中，主要规则（正则表达式规则 `App.*`）和辅助规则（正则表达式规则 `Appl.*`）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。



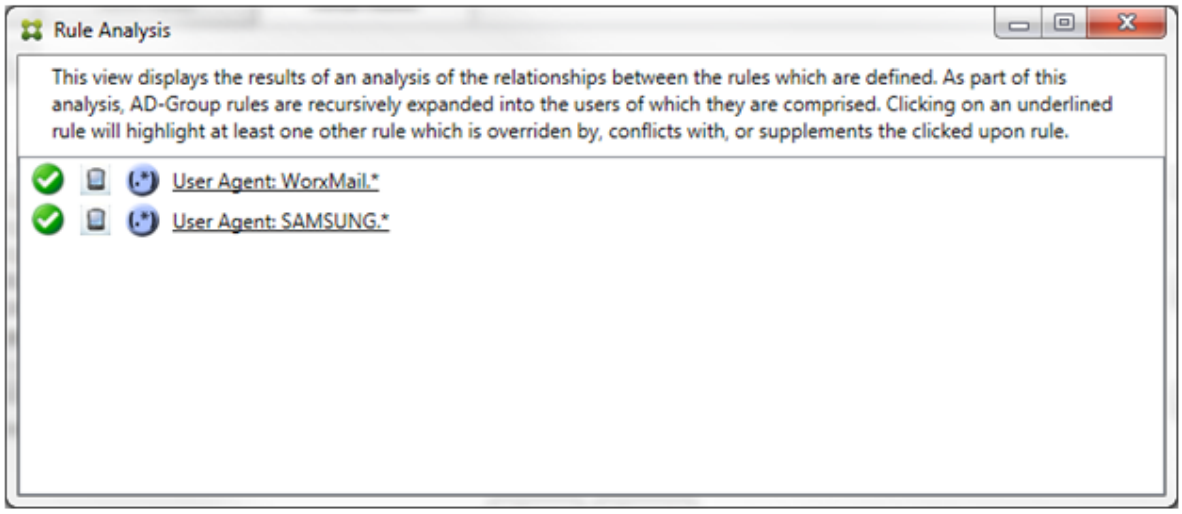
在前面的示例中，显而易见，第一条规则（正则表达式规则 SAMSUNG.*）不仅覆盖下一条规则（常规规则 SAMSUNG-SM-G900A/101.40402），而且这两条规则的访问状态有所不同（主要规则指定“允许”，辅助规则指定“阻止”）。第二条规则（常规规则 SAMSUNG-SM-G900A/101.40402）以较浅文本显示，指示该规则已被覆盖，并因此处于不活动状态。

单击正则表达式规则后，对话框显示如下：

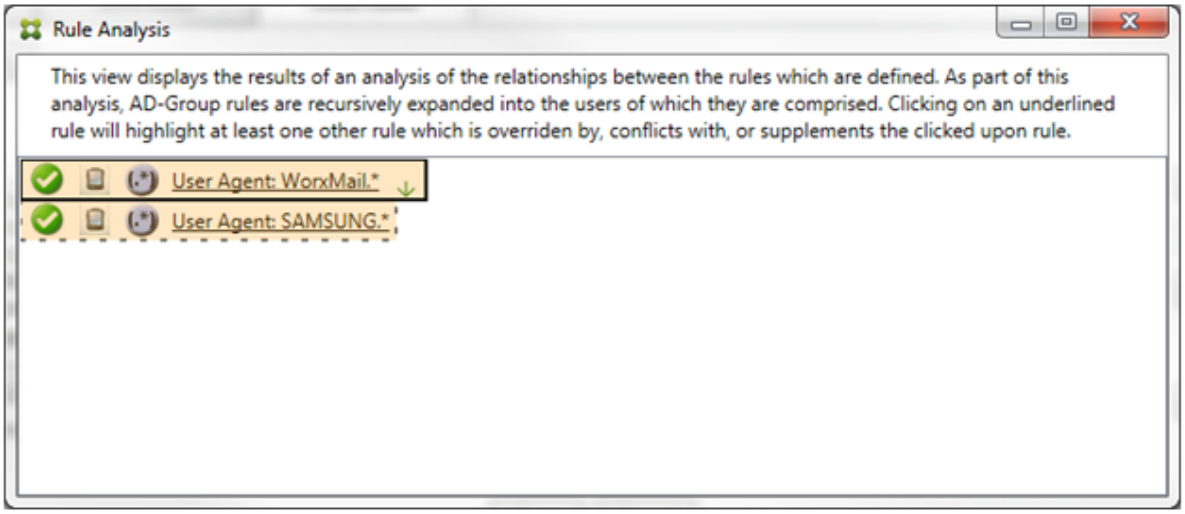


主要规则（正则表达式规则 SAMSUNG.*）后跟一个红点，指示其访问状态与一条或多条辅助规则发生冲突。辅助规则（常规规则 SAMSUNG-SM-G900A/101.40402）后跟一个红点，指示其访问状态与主要规则发生冲突。此外，该规则还后跟黑点，指示其已被覆盖，并因此处于不活动状态。

至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。仅相互补充的规则将只涉及正则表达式规则。当规则相互补充时，将以黄色叠加表示。在简单的示例中单击任一规则之前，对话框显示如下：



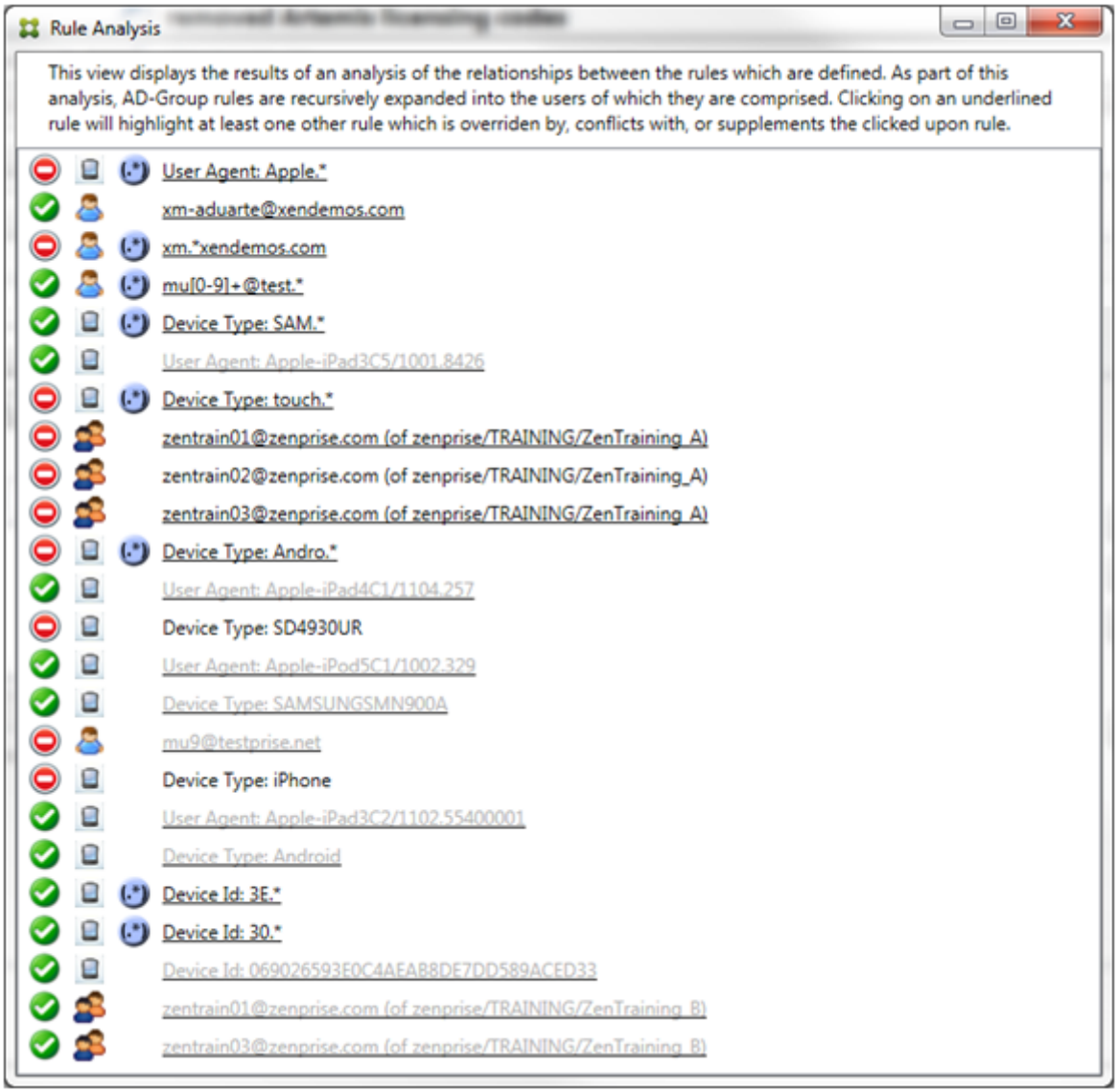
目测会很容易发现这两条规则都是正则表达式规则，都已应用到适用于 Exchange ActiveSync 的 Endpoint Management 连接器中的 ActiveSync 设备 ID 字段。单击第一条规则后，对话框显示如下：



主要规则（正则表达式规则 `WorkMail.*`）以黄色叠加突出显示，指示至少存在另外一个是正则表达式的辅助规则。辅助规则（正则表达式规则 `SAMSUNG.*`）以黄色叠加突出显示，指示辅助规则与主要规则都是要应用于适用于 Exchange ActiveSync 的 Endpoint Management 连接器内同一字段的正则表达式规则。在此示例中，该字段为 ActiveSync 设备 ID。这些正则表达式可能叠加，也可能不叠加。是否正确制作正则表达式由您来决定。

复杂表达式示例

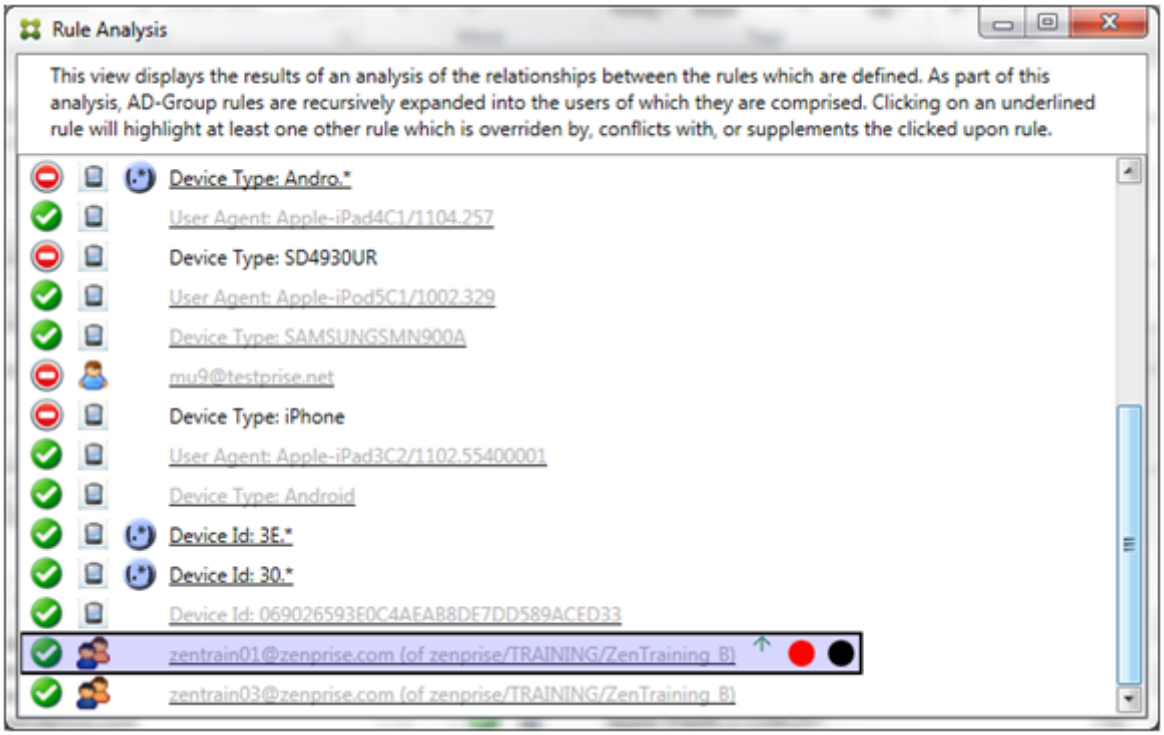
许多潜在的覆盖、冲突或补充都可能会发生，使其不可能举例说明所有可能的情景。以下示例探讨了不会执行的操作，同时还阐明了规则分析视觉构建的强大功能。大多数项目在下图中加了下划线。许多项目以较浅的字体显示，指示存在问题的规则已被优先级较高的规则以某种方式覆盖。多条正则表达式规则也包括在列表中，由  图标指示。



如何分析覆盖

要查看覆盖了特定规则的一条或多条规则，您可以单击该规则。

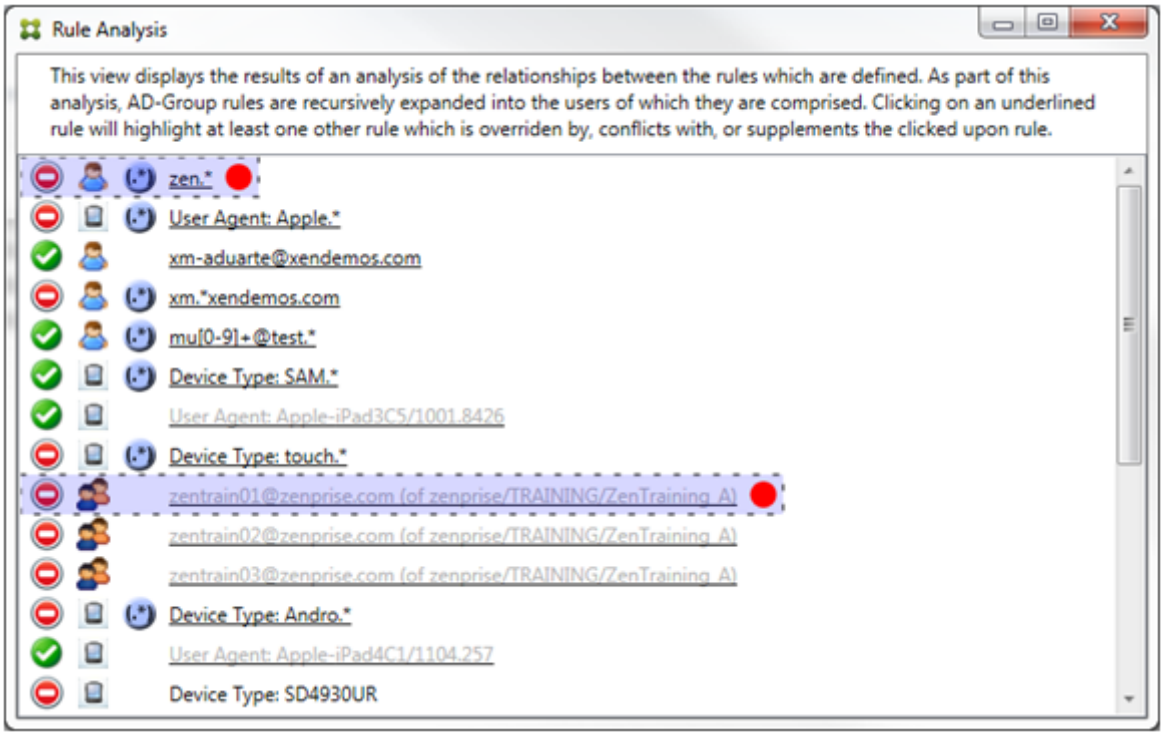
示例 **1**：此示例调查了覆盖 `zentrain01@zenprise.com` 的原因。



主要规则（AD-Group 规则 `zenprise/TRAINING/ZenTraining B`，`zentrain01@zenprise.com` 是其中的一个成员）具有以下特性：

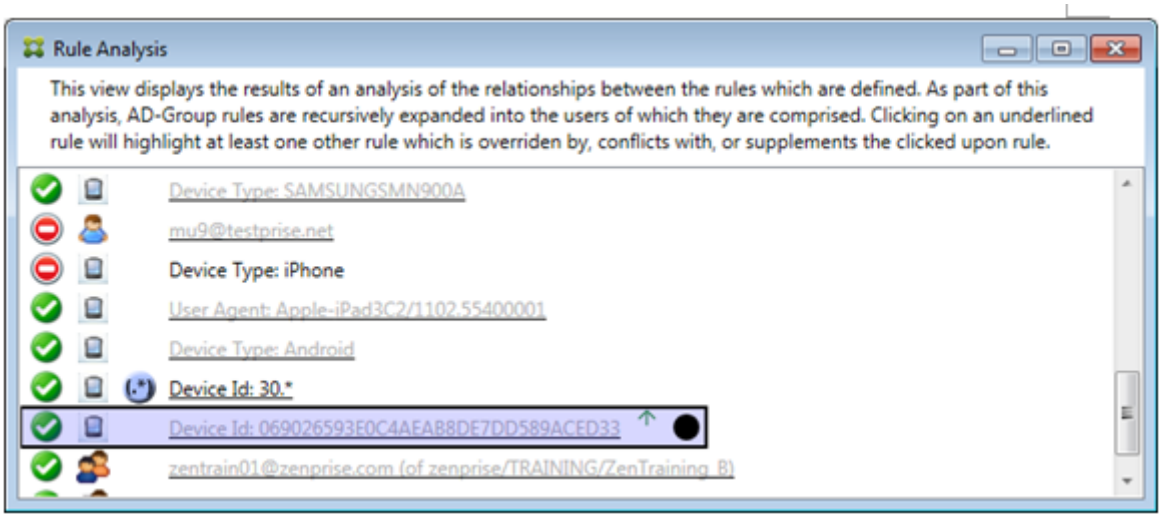
- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示一条或多条辅助规则都能够在该箭头上方找到）。
- 后跟一个红色圆圈和一个黑色圆圈，分别指示一条或多条辅助规则与其访问状态存在冲突，并且主要规则已被覆盖且因此处于不活动状态。

向上滚动时，您会看到以下内容：



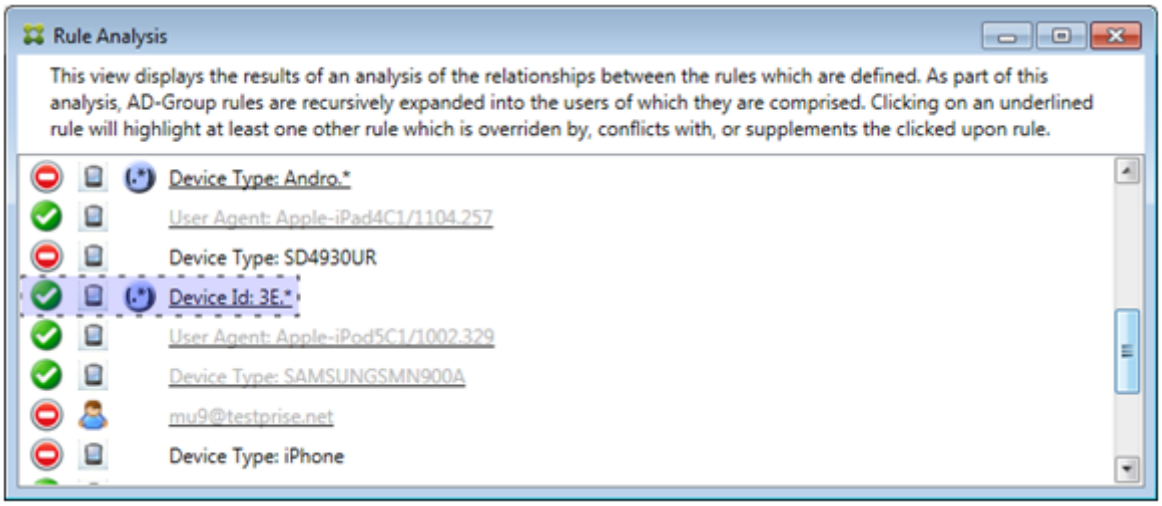
在此示例中，有两条辅助规则覆盖主要规则：正则表达式规则 `zen.*` 和常规规则 `zentrain01@zenprise.com`（属于 `zenprise/TRAINING/ZenTraining A`）。对于后一条辅助规则，出现了以下情况：Active Directory 组规则 `ZenTraining A` 包含用户 `zentrain01@zenprise.com`，Active Directory 组规则 `ZenTraining B` 也包含用户 `zentrain01@zenprise.com`。但是，由于辅助规则的优先级高于主要规则，因此主要规则被覆盖。主要规则的访问状态是“允许”，并且由于这两条辅助规则的访问状态都是“阻止”，因此，后跟一个红色圆圈以进一步指示访问冲突。

示例 **2**：此示例显示了覆盖 ActiveSync 设备 ID 为 `069026593E0C4AEAB8DE7DD589ACED33` 的设备的原因：



主要规则（常规设备 ID 规则 `069026593E0C4AEAB8DE7DD589ACED33`）具有以下特性：

- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示辅助规则能够在该箭头上方找到）。
- 后跟一个黑色圆圈，指示辅助规则已覆盖主要规则，并因此处于非活动状态。

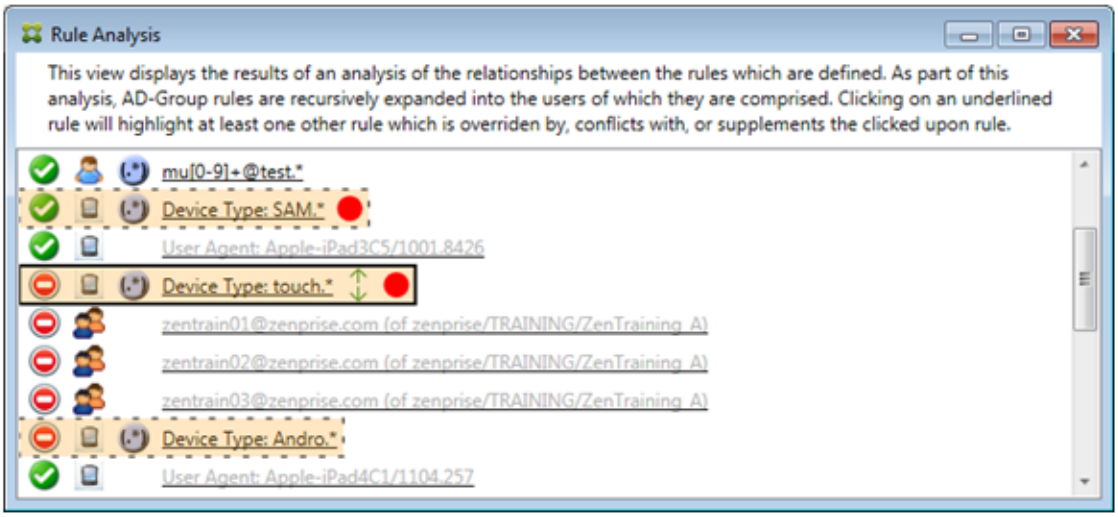


在此示例中，一条辅助规则覆盖主要规则：正则表达式 ActiveSync 设备 ID 规则 `3E.*`。由于正则表达式 `3E.*` 将会与 `069026593E0C4AEAB8DE7DD589ACED33` 匹配，因此，主要规则永远不会被评估。

如何分析补充和冲突

在此示例中，主要规则是正则表达式 ActiveSync 设备类型规则 `touch.*`。特性如下：

- 以实线框指示，并使用黄色叠加作为警告，提示正在针对特定规则字段运行多条正则表达式规则，在这种情况下为 ActiveSync 设备类型。
- 两个箭头分别指向上方和下方，指示至少存在一条具有较高优先级的辅助规则以及至少存在一条具有较低优先级的辅助规则。
- 箭头旁边的红色圆圈指示至少一条辅助规则的访问状态设置为允许，与主要规则的访问状态阻止相冲突
- 存在两条辅助规则，即正则表达式 ActiveSync 设备类型规则 `SAM.*` 和正则表达式 ActiveSync 设备类型规则 `Andro.*`。
- 这两条辅助规则都加了虚线框，指示其属于辅助规则。
- 这两条辅助规则都以黄色叠加，指示其也应用于 ActiveSync 设备类型的规则字段。
- 在此类情景中，您应确保其正则表达式规则不冗余。



如何进一步分析规则

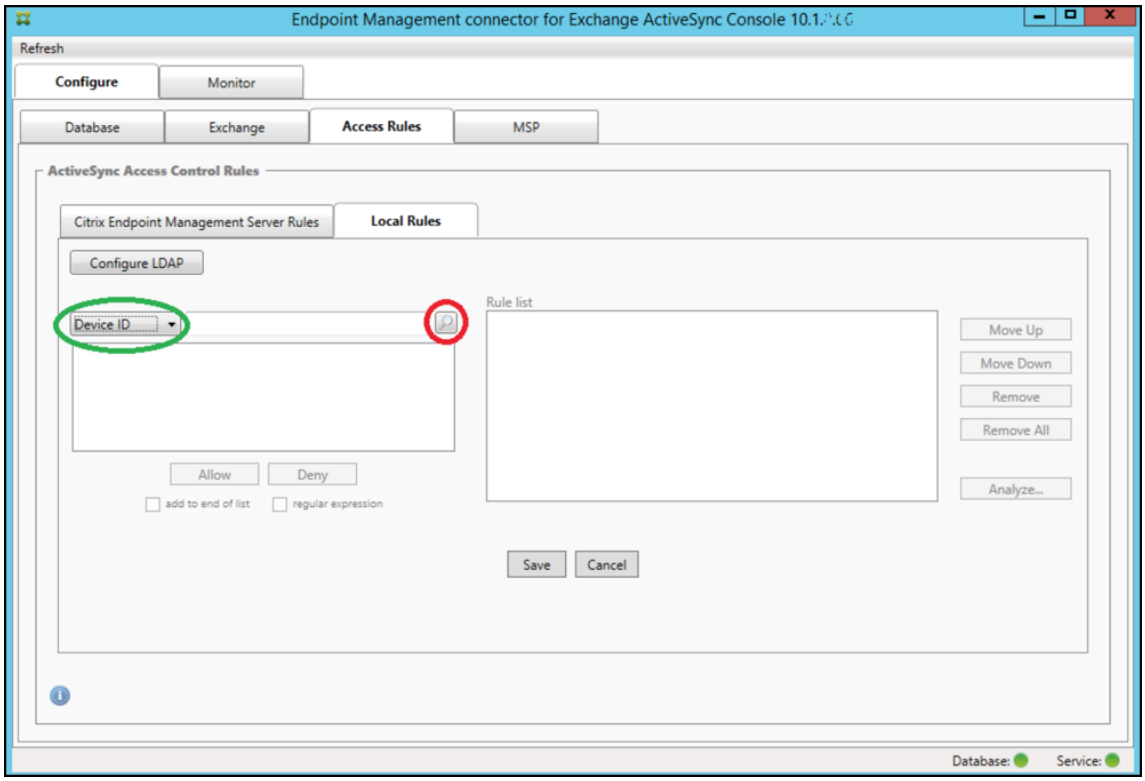
本示例探讨了规则关系如何始终从主要规则的角度建立。前面的示例显示了单击应用于设备类型值为 `touch.*` 的规则字段的正则表达式规则的情况。单击辅助规则 `Andro.*` 将显示一组不同的突出显示的辅助规则。

此示例显示了规则关系中包含的覆盖规则。此规则是常规 ActiveSync 设备类型规则 `Android`，已被覆盖（通过浅色

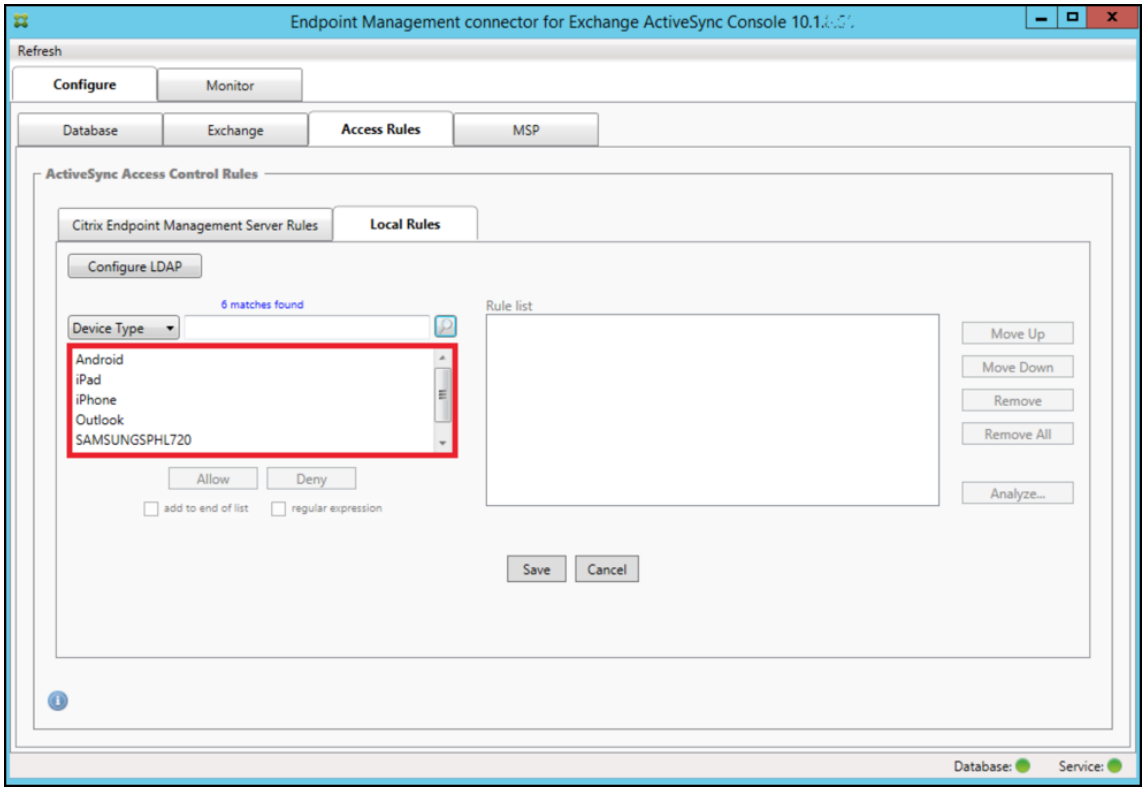
字体和旁边的黑色圆圈指示），并且其访问状态还与主要规则正则表达式 ActiveSync 设备类型规则 `Andro.*` 发生冲突。在单击该规则之前，该规则是辅助规则。在前面的示例中，常规 ActiveSync 设备类型规则 `Android` 未显示为辅助规则，因为从主要规则（正则表达式 ActiveSync 设备类型规则 `touch.*`）的角度来看，该规则与主要规则不相关。

配置常规表达式本地规则

1. 单击 **Access Rules**（访问规则）选项卡。



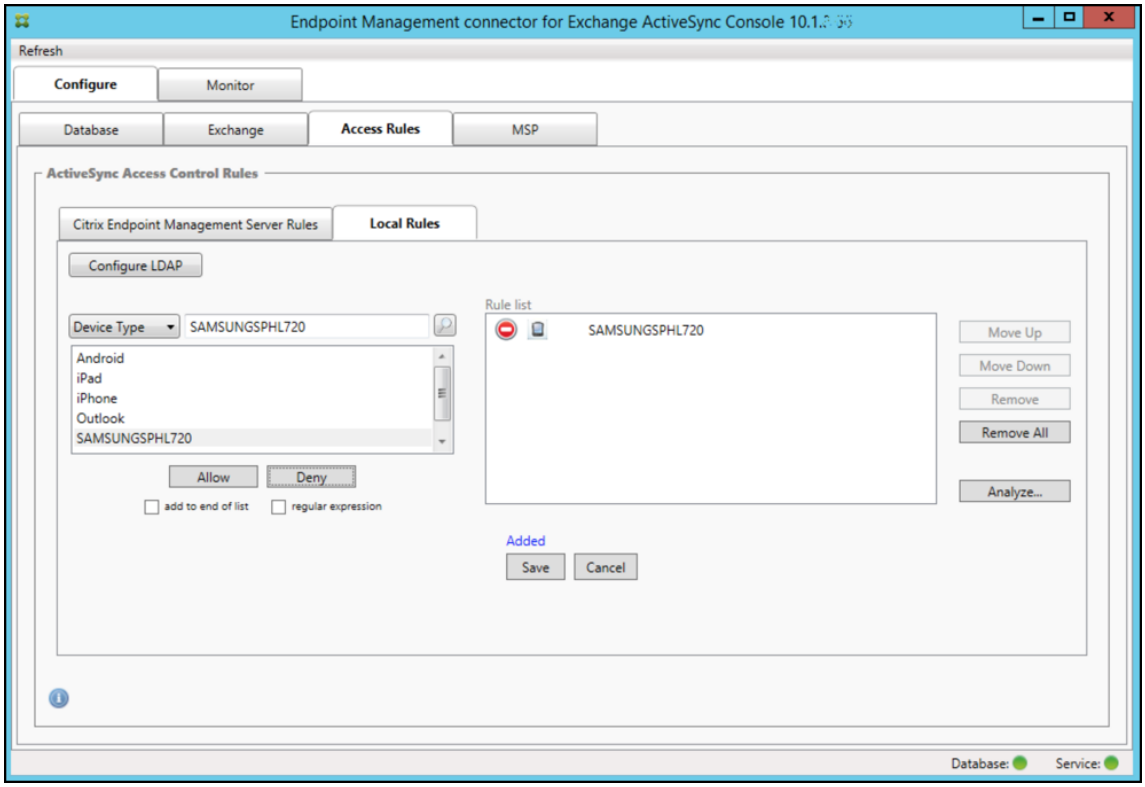
2. 在 **Device ID**（设备 ID）列表中，选择要为其创建本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。在此示例中，已选择 **Device Type**（设备类型）字段，并且选项显示在下面的列表框中。



4. 在结果列表框中单击其中一个项目，然后单击以下选项之一：

   - **Allow**（允许）表示 Exchange 将配置为允许所有匹配设备的 ActiveSync 流量。
   - **Deny**（拒绝）表示 Exchange 将配置为拒绝所有匹配设备的 ActiveSync 流量。

   在此示例中，将拒绝访问设备类型为 SamsungSPhl720 的所有设备。



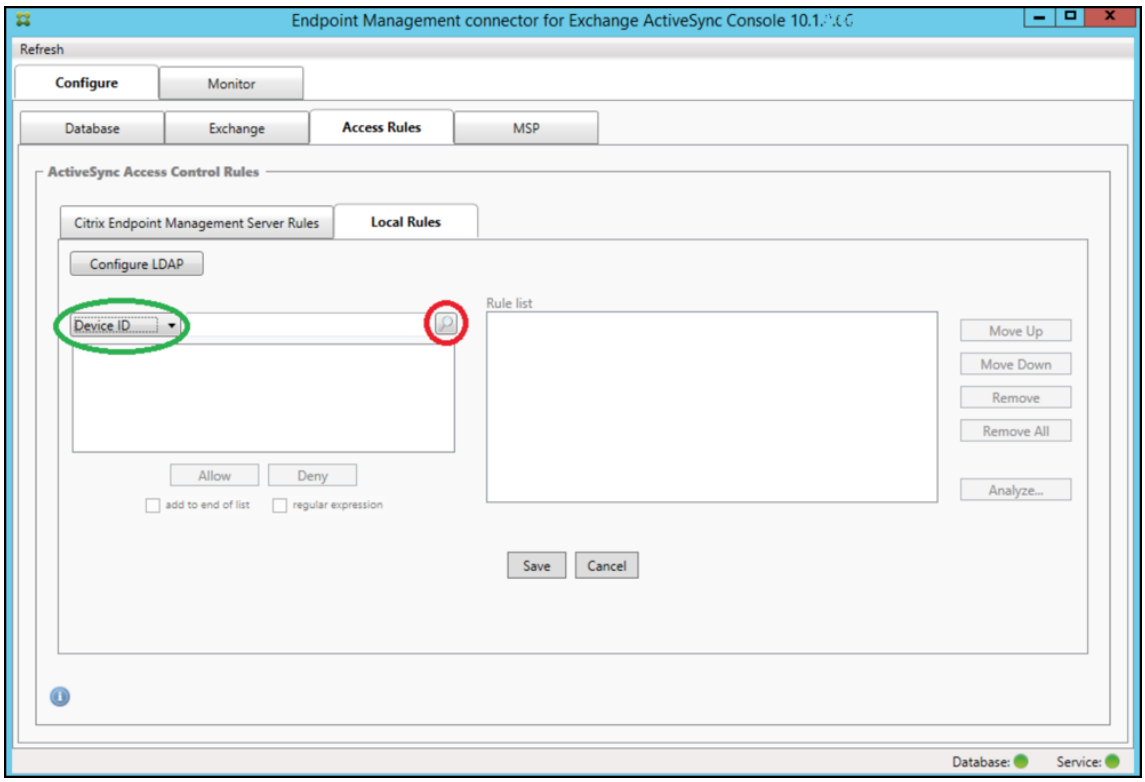
添加正则表达式

正则表达式本地规则可通过其旁边显示的图标进行区分 -  。

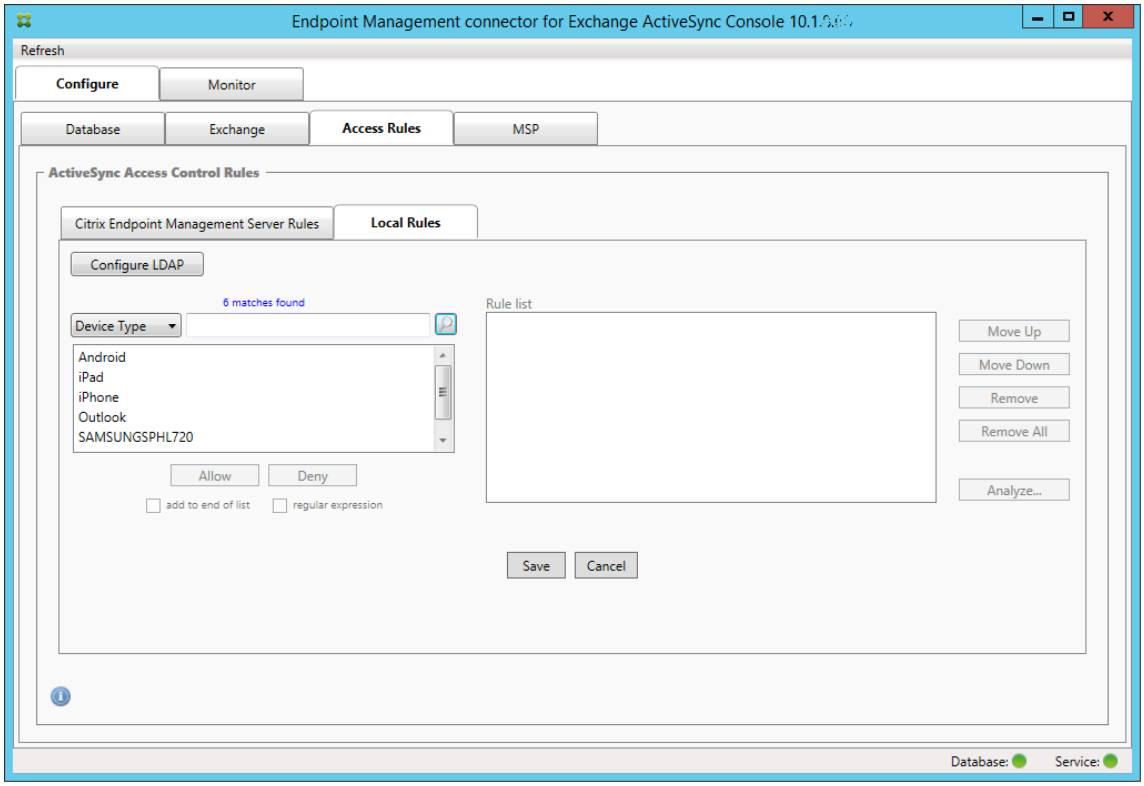
要添加正则表达式规则，您可以通过给定字段的结果列表中的现有值来构建正则表达式规则（只要已完成主要快照），或只需键入您想要的正则表达式。

从现有字段值构建正则表达式

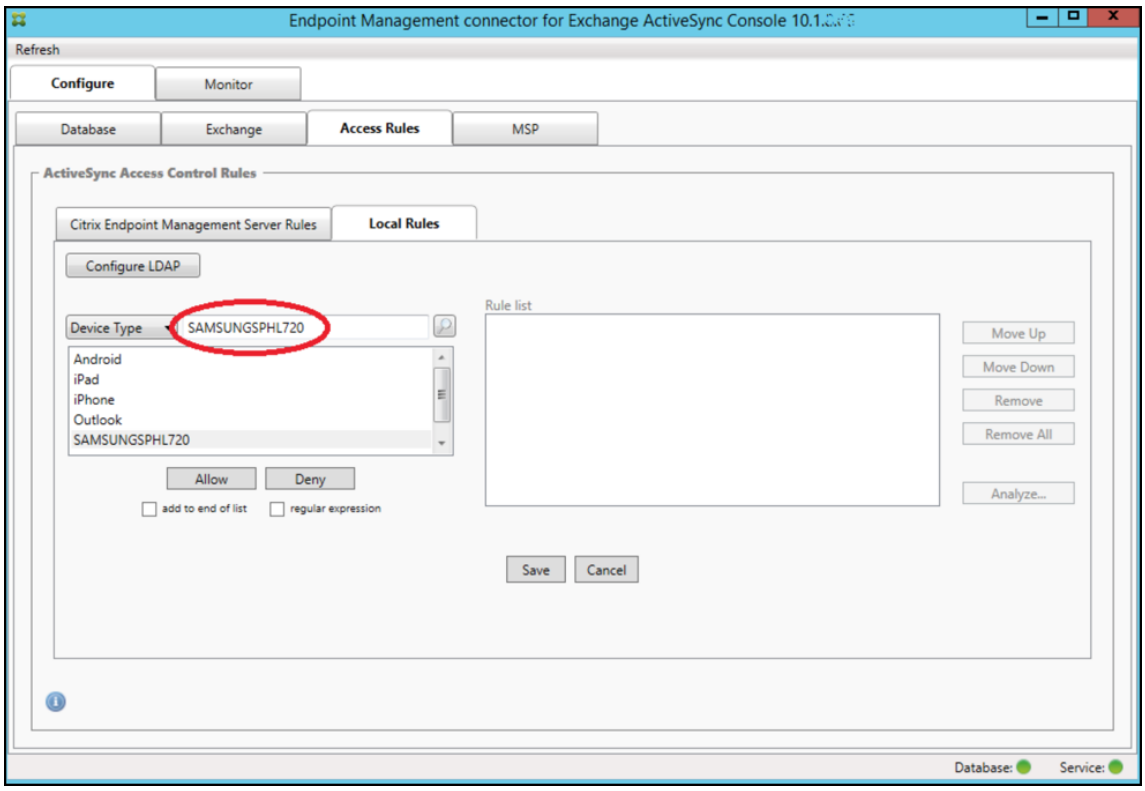
1. 单击 **Access Rules**（访问规则）选项卡。



2. 在 **Device ID**（设备 ID）列表中，选择要为其创建正则表达式本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。在此示例中，已选择 **Device Type**（设备类型）字段，并且选项显示在下面的列表框中。



4. 单击结果列表中的其中一个项目。在此示例中，已选择 **SAMSUNGSPHL720**，并显示在 **Device Type**（设备类型）旁边的文本框中。



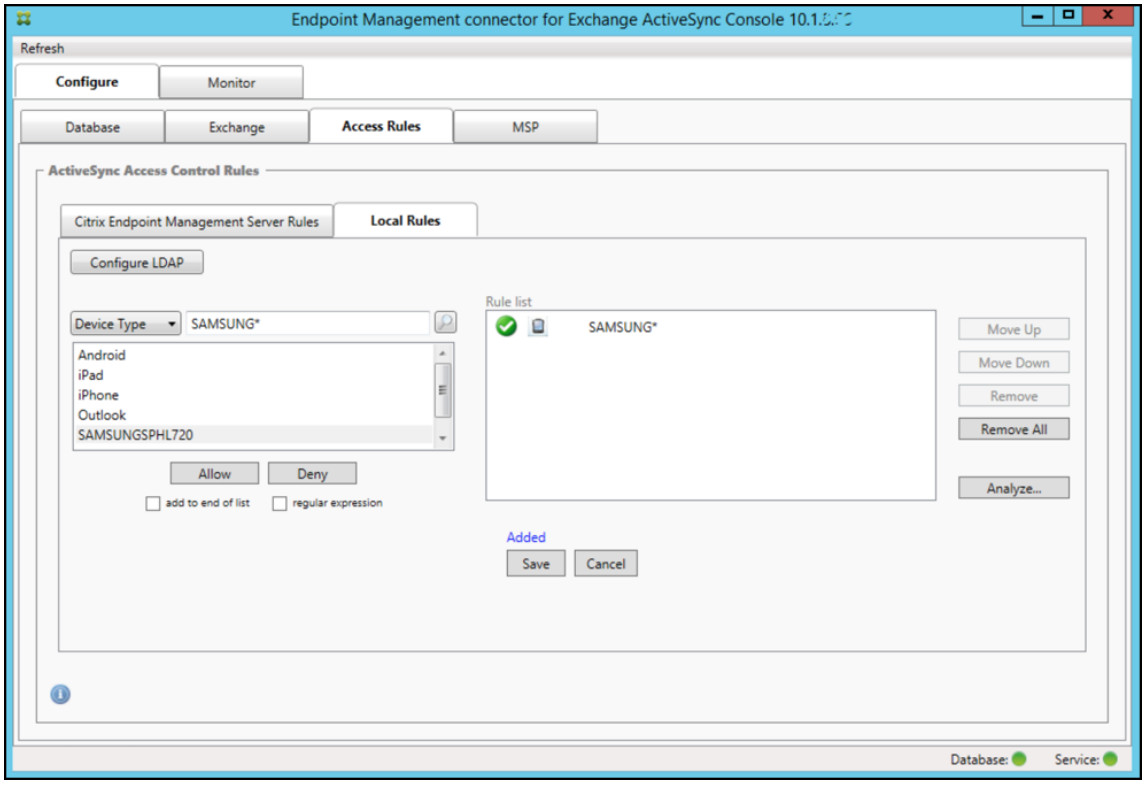
5. 要允许设备类型值中包含 “Samsung” 的所有设备类型，请按照以下步骤添加正则表达式规则：

   a) 在所选项目文本框中单击。

   b) 将文本从 **SAMSUNGSPHL720** 更改为 **SAMSUNG**。*。

   c) 确保选中正则表达式复选框。

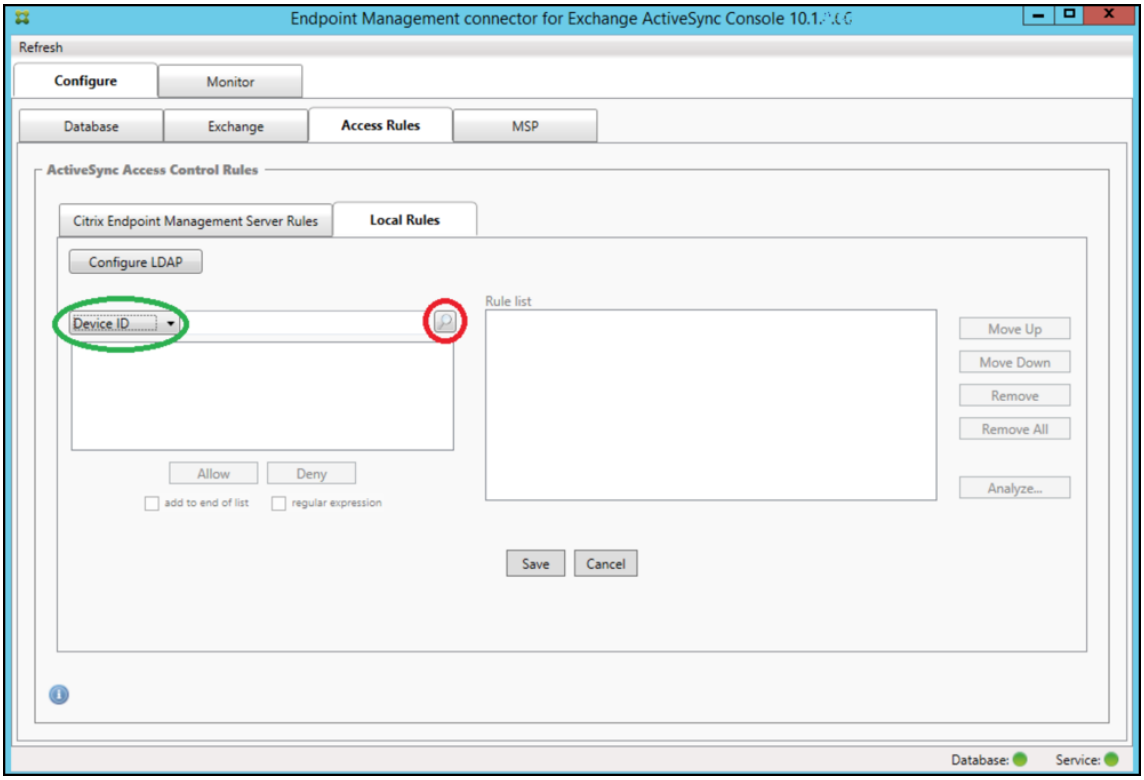
   d) 单击 **Allow**（允许）。



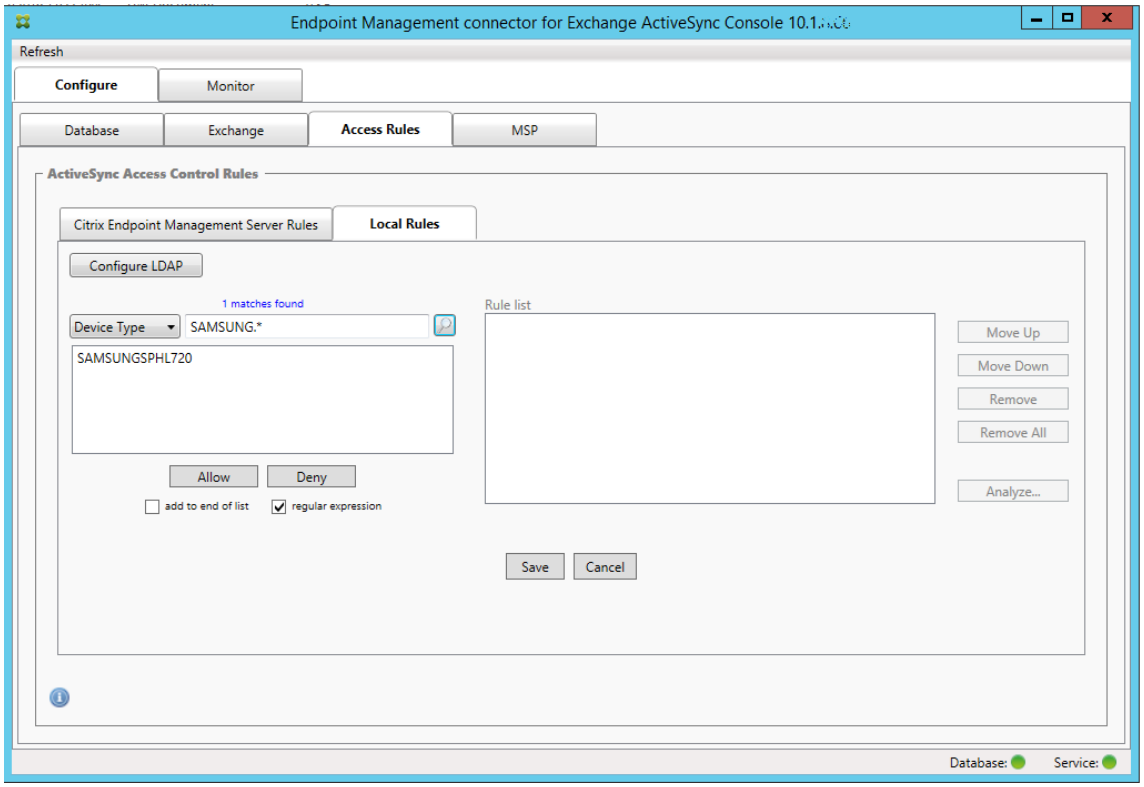
构建访问规则

1. 单击 **Local Rules**（本地规则）选项卡。

2. 要输入正则表达式，需要使用 “Device ID”（设备 ID）列表和所选项目文本框。



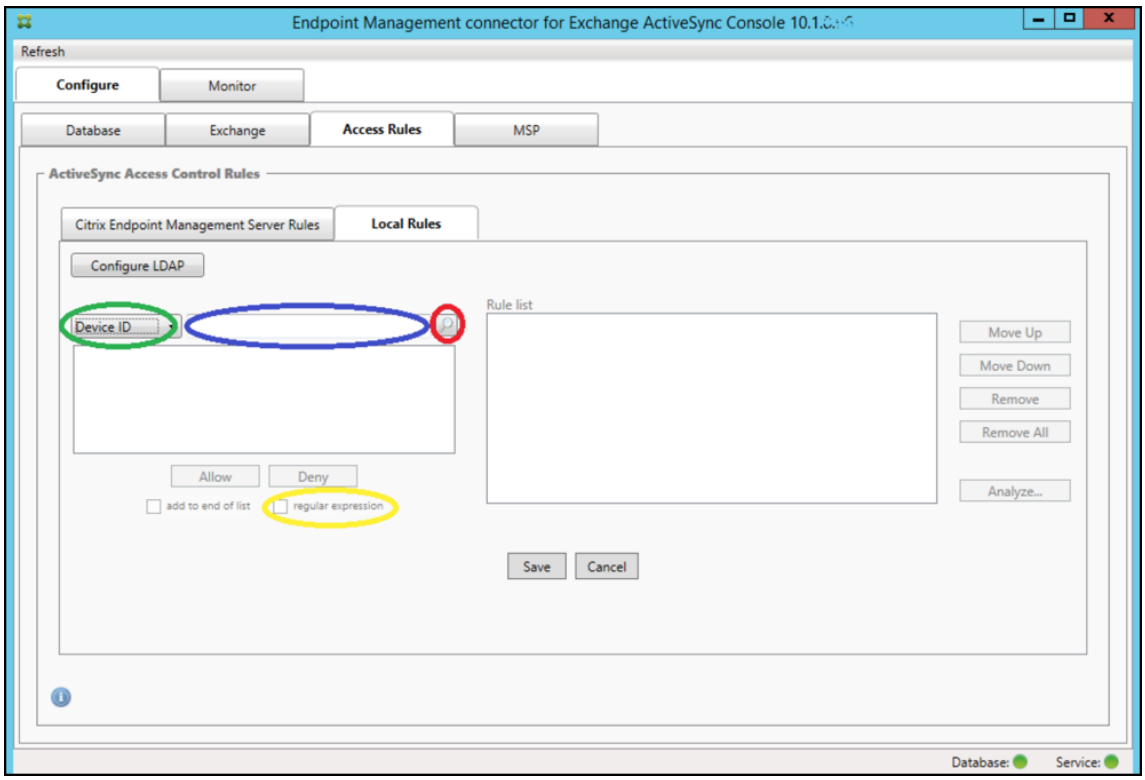
3. 选择要匹配的字段。此示例使用设备类型。
4. 键入正则表达式。此示例使用 `samsung.*`
5. 确保选中 “regular expression”（正则表达式）复选框，然后单击 **Allow**（允许）或 **Deny**（拒绝）。在此示例中，选择的是 **Allow**（允许）。最终结果如下所示：



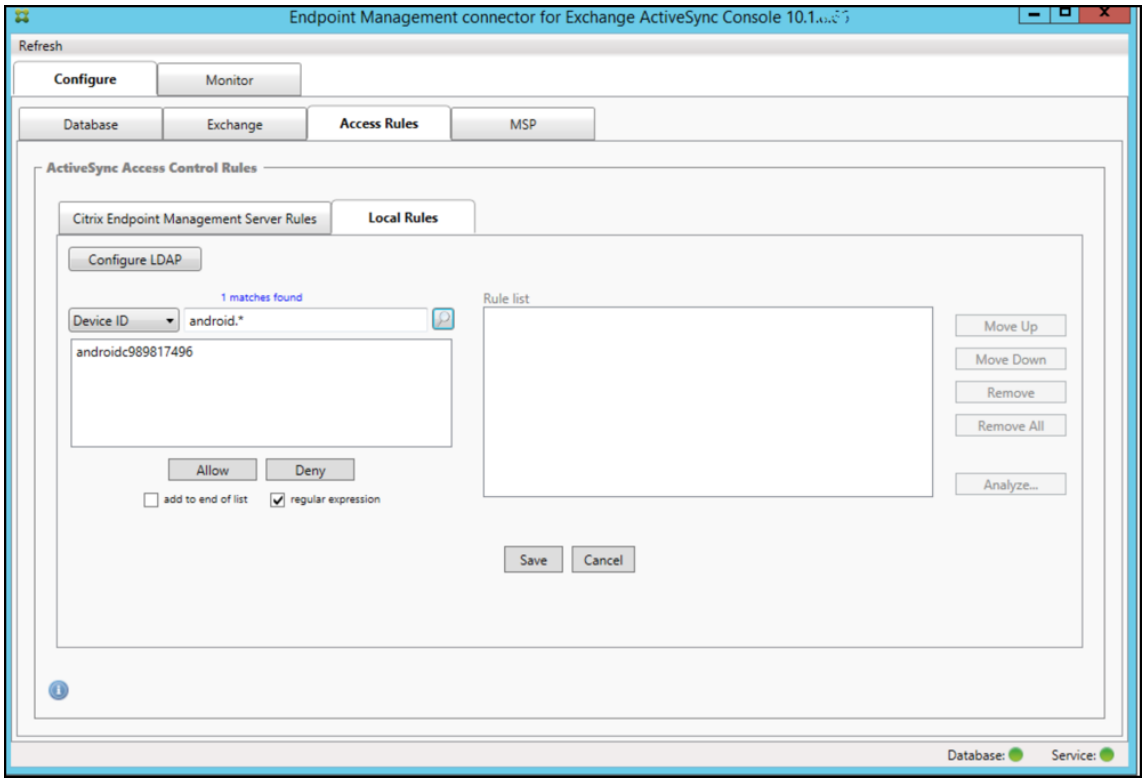
查找设备

通过选中“regular expression”（正则表达式）复选框，可以针对与给定表达式匹配的特定设备运行搜索。此功能仅在成功完成主要快照时可用。即使没有计划使用正则表达式规则，您也可以使用此功能。例如，假定您要查找 ActiveSync 设备 ID 中包含文本“workmail”的所有设备。为此，请执行以下过程。

1. 单击 **Access Rules**（访问规则）选项卡。
2. 确保设备匹配字段选择器设置为“Device ID”（设备 ID）（默认值）。



3. 在所选项目文本框（上图中以蓝色显示的框）内单击，然后键入 `workmail.*`。
4. 确保选中 “regular expression”（正则表达式）复选框，然后单击放大镜图标显示匹配项，如下图所示。

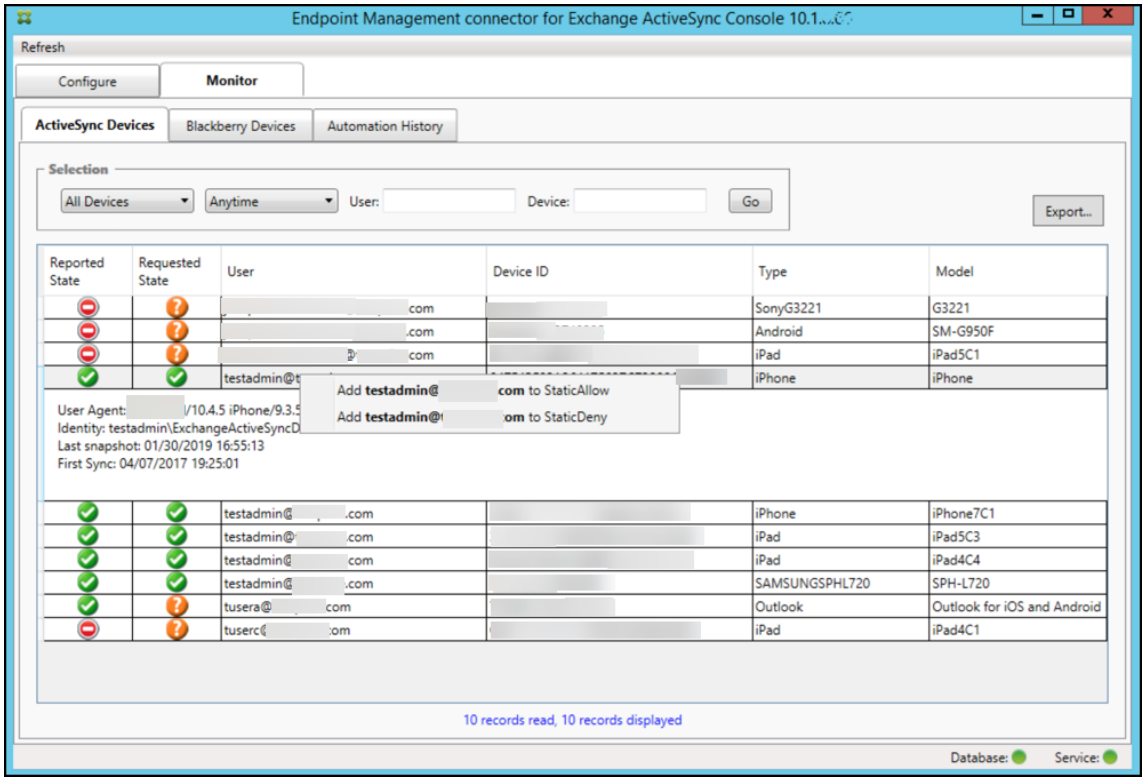


将单个用户、设备或设备类型添加到静态规则

可以基于 ActiveSync 设备选项卡上的用户、设备 ID 或设备类型添加静态规则。

1. 单击 **ActiveSync Devices**（ActiveSync 设备）选项卡。
2. 在列表中，右键单击用户、设备或设备类型，然后选择是允许所选内容还是拒绝所选内容。

   下图显示了选定 user1 时的“允许”/“拒绝”选项。



设备监视

通过适用于 Exchange ActiveSync 的 Endpoint Management 连接器中的监视器选项卡，可以浏览已检测到的 Exchange ActiveSync 和黑莓设备以及已发出的自动化 PowerShell 命令的历史记录。**Monitor**（监视）选项卡有以下三个选项卡：

- **ActiveSync** 设备：
  - 您可以通过单击 **Export**（导出）按钮导出显示的 ActiveSync 设备合作关系。
  - 您可以通过右键单击 **User**（用户）、**Device ID**（设备 ID）或 **Type**（类型）列并选择适当的允许或阻止规则类型来添加本地（静态）规则。
  - 要折叠展开的行，请按住 Ctrl 键并单击该展开的行。
- **Blackberry Devices**（黑莓设备）
- **Automation History**（自动化历史记录）

Configure（配置）选项卡显示所有快照的历史记录。快照历史记录显示快照发生的时间、发生了多久、检测到多少设备以及出现的任何错误。

- 在 **Exchange** 选项卡中，单击所需 Exchange Server 的信息图标。
- 在 **MSP** 选项卡中，单击所需黑莓服务器的信息图标。

故障排除和诊断

适用于 Exchange ActiveSync 的 Endpoint Management 连接器将错误和其他操作信息记录到其日志文件：安装文件夹\log\XmmWindowsService.log。适用于 Exchange ActiveSync 的 Endpoint Management 连接器还会将重要事件记录到 Windows 事件日志中。

更改日志记录级别

适用于 Exchange ActiveSync 的 Endpoint Management 连接器包括以下日志记录级别：错误、信息、警告、调试和跟踪。

> 注意：
>
> 每个连续级别将生成更多详细信息（更多数据）。例如，错误级别提供最少的详细信息，而跟踪级别提供最多的详细信息。

要更改日志记录级别，请执行以下操作：

1. 在 C:\Program Files\Citrix\Citrix Endpoint Management connector 中，打开 nlog.config 文件。
2. 在 <rules> 部分中，更改您更倾向于使用的日志记录级别的 *minilevel* 参数。例如：

```
1      <rules>
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. 保存该文件。

   所做的更改将立即生效。您不需要重新启动适用于 Exchange ActiveSync 的连接器。

常见错误

以下列表包括常见错误：

- 适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务未启动

  检查日志文件和 Windows 事件日志中的错误。包括以下典型原因：

  - 适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务无法访问 SQL Server。以下这些问题可能导致此情况：

    * SQL Server 服务不在运行。
    * 身份验证失败。

    如果已配置 “Windows Integrated”（Windows 集成）身份验证，必须允许适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务的用户帐户进行 SQL 登录。适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务的帐户默认为 “Local System”（本地系统），但是可能会更改为任何具有本地管理员权限的帐户。如果已配置 SQL 身份验证，必须在 SQL 中正确配置 SQL 登录。

  - 为移动服务提供商 (MSP) 配置的端口不可用。必须选择未被系统中其他进程使用的侦听端口。

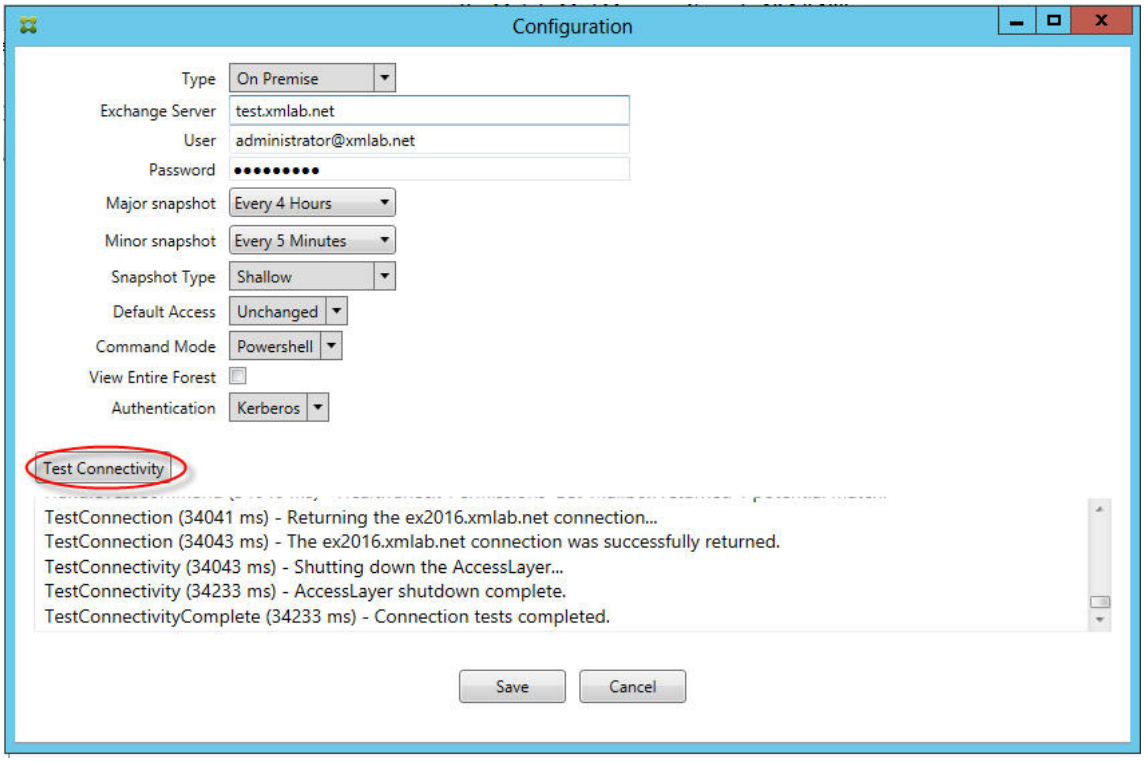
- XenMobile 无法连接到 MSP

  检查是否已在适用于 Exchange ActiveSync 的 Endpoint Management 连接器控制台的配置 **> MSP** 选项卡中正确配置 MSP 服务端口和传输。检查是否已正确设置授权组或用户。

  如果已配置 HTTPS，则必须安装有效的 SSL 服务器证书。如果已安装 IIS，IIS 管理器可以用来安装证书。如果未安装 IIS，请参阅 How to configure a port with an SSL certificate（如何使用 SSL 证书配置端口），了解有关安装证书的详细信息。

  适用于 Exchange ActiveSync 的 Endpoint Management 连接器包含一个用于测试与 MSP 服务的连接的实用程序。运行 安装文件夹\MspTestServiceClient.exe 程序并将 URL 和凭据设置为将在 XenMobile 中配置的 URL 和凭据，然后单击 **Test Connectivity**（测试连接）。这将模拟 XenMobile Server 发出的 Web 服务请求。请注意，如果已配置 HTTPS，您必须指定服务器的实际主机名（在 SSL 证书中指定的名称）。

  使用 **Test Connectivity**（测试连接）时，请确保至少有一条 ActiveSyncDevice 记录，否则测试可能会失败。



故障排除工具

Support\PowerShell 文件夹中提供了一组用于故障排除的 PowerShell 实用程序。

故障排除工具将对用户的邮箱和设备执行深度分析（从而检测错误条件和潜在的故障区域）并对用户执行深度 RBAC 分析。该工具可以将所有 cmdlet 的原始输出保存到一个文本文件。

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

January 5, 2022

XenMobile Citrix ADC Connector 现已更名为适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。有关 Citrix 统一产品组合的更多详细信息，请参阅 Citrix 产品指南。

适用于 Exchange ActiveSync 的连接器向 NetScaler 提供 ActiveSync 客户端的设备级别授权服务，而 Citrix ADC 用作 Exchange ActiveSync 协议的反向代理。授权由在 XenMobile 中定义的策略组合以及适用于 Exchange ActiveSync 的 Citrix Gateway 连接器本地定义的规则控制。

有关详细信息，请参阅 ActiveSync Gateway。

有关详细的参考体系结构图，请参阅体系结构。

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的当前版本为版本 8.5.2。

新增功能

以下各节列出了当前版本和早期版本的适用于 Exchange ActiveSync 的 Citrix Gateway 连接器（以前称为 XenMobile Citrix ADC Connector）的新增功能。

版本 **8.5.3** 中的新增功能

- 本版本增加了对 ActiveSync 协议 16.0 和 16.1 的支持。
- 更多详细信息已添加到发送至 Google Analytics 的分析中，特别是相关的快照。[CXM-52261]

版本 **8.5.2** 中的新增功能

- XenMobile Citrix ADC Connector 现已更名为适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。

此版本中修复了以下问题：

- 如果在定义策略规则时使用多个条件，并且其中一个条件涉及到用户 ID，可能会出现以下问题：如果用户有多个别名，应用该规则时不会检查这些别名。[CXM-55355]

> 注意：
>
> 以下“新增功能”部分在提到适用于 Exchange ActiveSync 的 Citrix Gateway 连接器时使用其以前的名称 XenMobile Citrix ADC Connector。名称自版本 8.5.2 起更改。

版本 **8.5.1.11** 中的新增功能

- 系统要求变更： Citrix ADC Connector 的当前版本需要使用 Microsoft.NET Framework 4.5。
- **Google Analytics** 支持：我们希望了解您使用 XenMobile Citrix ADC Connector 的方式，以便我们可以专注于可以改进产品的方面。
- 支持 **TLS 1.1** 和 **1.2**：由于其日渐削弱的安全性，PCI 委员会正在弃用 TLS 1.0。对 TLS 1.1 和 1.2 的支持已添加到 XenMobile Citrix ADC Connector 中。

监视适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序提供详细的日志记录，可用于查看 Secure Mobile Gateway 允许或阻止的通过 Exchange Server 的所有流量。

使用日志选项卡可查看由 Citrix ADC 转发到适用于 Exchange ActiveSync 的连接器以进行授权的 ActiveSync 请求的历史记录。

此外，为确保适用于 Exchange ActiveSync 的 Citrix Gateway 连接器 Web 服务运行，还可将以下 URL 加载到连接器服务器上的浏览器中：`https://<host:port>/services/ActiveSync/Version`。如果 URL 以字符串形式返回产品版本，则 Web 服务为可响应。

使用适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器模拟 **ActiveSync** 流量

可以使用适用于 Exchange ActiveSync 的 Citrix Gateway 连接器模拟启用了您的策略时 ActiveSync 流量的具体表现。在连接器配置实用程序中，选择 **Simulator**（模拟器）选项卡。结果将根据您已配置的规则显示策略的应用方式。

为适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器选择过滤器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器过滤器的工作方式是针对给定策略违规情况或属性设置分析设备。如果设备满足条件，则将设备放入设备列表中。此设备列表既不是允许列表也不是阻止列表。它是满足定义条件的设备的列表。XenMobile 中的连接器可使用下列过滤器。每个过滤器均有两个选项：允许或拒绝。

- 匿名设备：允许或拒绝在 XenMobile 中已注册但用户的身份未知的设备。例如，可以是以前注册的用户，但用户的 Active Directory 密码已过期，或者是用未知凭据注册的用户。
- **Samsung KNOX** 认证失败： Samsung 设备具有安全和诊断相关功能。此过滤器用于确认已为设备设置 KNOX。有关详细信息，请参阅 Samsung Knox。
- 禁止的应用程序：基于由阻止列表策略定义的设备列表以及是否存在阻止的应用程序来允许或拒绝设备。
- 隐式允许/拒绝：创建不满足其他任何过滤器规则条件的所有设备的设备列表，并根据该列表允许或拒绝。“隐式允许/拒绝”选项可确保“设备”选项卡中的适用于 Exchange ActiveSync 的 Citrix Gateway 连接器状态为已启用，并显示您设备的连接器状态。“隐式允许/拒绝”选项还可以控制所有其他尚未被选定的连接器过滤器。例如，连接器拒绝运行阻止的应用程序，但允许所运行有其他过滤器，因为“隐式允许/拒绝”选项设置为允许。
- 不活动设备：创建在指定时间段内与 XenMobile 没有通信的设备的设备列表。这些设备被视为非活动状态。因此，过滤器会允许或拒绝这些设备。
- 缺少所需的应用程序：用户注册时，将收到必须安装的所需应用程序的列表。“缺少所需的应用程序”过滤器指示一个或多个应用程序不再存在；例如，用户删除了一个或多个应用程序。
- 非推荐应用程序：用户注册时，将收到应安装的应用程序列表。“非推荐应用程序”过滤器会在设备中检查不在该列表中的应用程序。
- 不合规密码：创建设备上没有通行码的所有设备的设备列表。
- 不合规设备：允许您拒绝或允许满足自己内部 IT 合规条件的设备。合规是由名为“不合规”的设备属性定义的任意设置，它是一个可以为真或假的布尔标志。（可以手动创建此属性并设定值，或者也可在设备满足或不满足特定条件时，使用自动操作在设备上创建此属性。）
  - 不合规 **=** 真。如果设备不满足您 IT 部门设定的合规标准和策略定义，则该设备不合规。
  - 不合规 **=** 假。如果设备满足您 IT 部门设定的合规标准和策略定义，则该设备合规。
- 吊销状态：创建所有已吊销设备的设备列表，并根据吊销状态允许或拒绝。
- 已获得 **Root** 权限的 **Android** 设备/已越狱的 **iOS** 设备。创建包括所有标记为获得 root 权限的设备的设备列表，并根据获得 root 权限的状态允许或拒绝。
- 未托管设备。创建包括 XenMobile 数据库中所有设备的设备列表。需要在阻止模式下部署移动应用程序网关。

配置与适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的连接

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器通过安全 Web 服务与 XenMobile 和其他远程配置提供程序进行通信。

1. 在连接器配置实用程序中，单击 **Config Providers**（配置提供程序）选项卡，然后单击 **Add**（添加）。
2. 在 **Config Providers**（配置提供程序）对话框中的 **Name**（名称）中，输入具有管理权限并用于 XenMobile Server 的基本 HTTP 授权的用户名。
3. 在 **URL** 中，输入 XenMobile GCS 的 Web 地址，格式通常为 `https://<FQDN>/<instanceName>/services/<MagConfigService>`。*MagConfigService* 名称区分大小写。
4. 在 **Password**（密码）中，输入将用于 XenMobile Server 的基本 HTTP 授权的密码。
5. 在 **Managing Host**（管理主机）中，输入连接器服务器名称。
6. 在 **Baseline Interval**（基准时间间隔）中，指定从 Device Manager 提取新刷新的动态规则集的时间间隔。
7. 在 **Delta interval**（时间间隔差）中，指定提取动态规则更新的时间间隔。
8. 在 **Request Timeout**（请求超时）中，指定服务器请求超时的时间间隔。
9. 在 **Config Provider**（配置提供程序）中，选择配置提供程序服务器实例是否提供策略配置。
10. 在 **Events Enabled**（事件已启用）中，如果希望连接器在设备被阻止时通知 XenMobile，则启用此选项。如果要在任何 XenMobile 自动化操作中使用连接器规则，则需要使用此选项。
11. 依次单击 **Save**（保存）和 **Test Connectivity**（测试连接），测试网关到配置提供程序的连接。如果连接失败，请检查本地防火墙设置是否允许连接，或与管理员联系。
12. 连接成功后，取消选中 **Disabled**（禁用）复选框，然后单击 **Save**（保存）。

添加新的配置提供程序时，适用于 Exchange ActiveSync 的 Citrix Gateway 连接器会自动创建一个或多个与该提供程序关联的策略。这些策略由模板定义进行定义，模板定义包含在 NewPolicyTemplate 部分的 config\policyTemplates.xml 中。会为在本节中定义的每个策略元素创建一个新策略。

如果满足以下条件，操作员可以添加、删除或修改策略元素：策略元素符合架构定义，并且不修改标准替换字符串（用括号括起）。接下来，为提供程序添加新组并更新策略以将新组包括在内。

从 **XenMobile** 中导入策略

1. 在适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序中，单击 **Config Providers**（配置提供程序）选项卡，然后单击 **Add**（添加）。
2. 在 **Config Providers**（配置提供程序）对话框中的 **Name**（名称）中，输入将用于 XenMobile Server 的基本 HTTP 授权以及具有管理权限的用户名。
3. 在 **URL** 中，输入 XenMobile Gateway Configuration Service (GCS) 的 Web 地址，格式通常为 `https://<xdmHost>/xdm/services/<MagConfigService>`。MagConfigService 名称区分大小写。
4. 在 **Password**（密码）中，输入用于 XenMobile Server 的基本 HTTP 授权的密码。
5. 单击 **Test Connectivity**（测试连接），测试网关到配置提供程序的连接。如果连接失败，请检查本地防火墙设置是否允许连接，或与管理员核查。
6. 连接成功后，取消选中 **Disabled**（禁用）复选框，然后单击 **Save**（保存）。
7. 在 **Managing Host**（管理主机）中，保留本地主机计算机的默认 DNS 名称。在多个 Forefront Threat Management Gateway (TMG) 服务器配置在一个阵列中时，此设置用于协调与 XenMobile 的通信。

   保存设置后，打开 GCS。

配置适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器策略模式

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器可以在以下 6 种模式下运行：

- **Allow All**（全部允许）。此策略模式授权对通过连接器的所有流量进行访问。不使用其他过滤规则。
- **Deny All**（全部拒绝）。此策略模式阻止对通过连接器的所有流量进行访问。不使用其他过滤规则。
- **Static Rules: Block Mode**（静态规则: 阻止模式）。此策略模式执行在结尾具有隐式拒绝或阻止语句的静态规则。连接器会阻止其他过滤规则不允许使用的设备。
- **Static Rules: Permit Mode**（静态规则: 许可模式）。此策略模式执行在结尾具有隐式许可或允许语句的静态规则。允许未被阻止的设备或被其他过滤规则拒绝的设备通过连接器。
- **Static + ZDM Rules: Block Mode**（静态 + ZDM 规则: 阻止模式）。此策略模式首先执行静态规则，然后执行来自 XenMobile 的、在结尾具有隐式拒绝或阻止语句的动态规则。将根据已定义的过滤器和 Device Manager 规则允许或拒绝设备。与定义的过滤器和规则不匹配的任何设备都会被阻止。
- **Static + ZDM Rules: Permit Mode**（静态 + ZDM 规则: 许可模式）。此策略模式首先执行静态规则，然后执行来自 XenMobile 的、在结尾具有隐式许可或允许语句的动态规则。将根据已定义的过滤器和 XenMobile 规则允许或拒绝设备。与定义的过滤器和规则不匹配的任何设备都会被允许。

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器进程根据从 XenMobile 收到的基于 iOS 和 Windows 的移动设备的唯一 ActiveSync ID 允许或阻止动态规则。Android 设备的特性由于制造商不同而有所不同，且有些设备没有准备好公开唯一的 ActiveSync ID。为进行补偿，XenMobile 会发送 Android 设备的用户 ID 信息，以便做出允许或阻止决定。因此，如果用户只有一个 Android 设备，则其允许和阻止功能正常。如果用户具有多个 Android 设备，则所有设备都被允许，因为无法区别 Android 设备。可以将网关配置为通过 ActiveSyncID（如果已知）静态阻止这些设备。还可以将网关配置为根据设备类型或用户代理进行阻止。

要指定策略模式，请在 SMG Controller 配置实用程序中执行以下操作：

1. 单击 **Path Filters**（路径过滤器）选项卡，然后单击 **Add**（添加）。
2. 在 **Path Properties**（路径属性）对话框中，从 **Policy**（策略）列表中选择策略模式，然后单击 **Save**（保存）。

可以在配置实用程序的 **Policies**（策略）选项卡中查看这些规则。这些规则将在适用于 Exchange ActiveSync 的 Citrix Gateway 连接器上自上而下处理。“Allow”（允许）策略显示时带有绿色选中标记。“Deny”（拒绝）策略显示为红色圆圈，中间横穿一条直线。要刷新屏幕并查看最新更新的规则，请单击 **Refresh**（刷新）。也可在 config.xml 文件中修改规则的顺序。

要测试规则，请单击 **Simulator**（模拟器）选项卡。在字段中指定值。这些值也可从日志中获得。将出现指定“允许”或“阻止”的结果消息。

配置静态规则

请输入具有 ActiveSync 连接 HTTP 请求的 ISAPI 过滤功能读取的值的静态规则。静态规则支持适用于 Exchange ActiveSync 的 Citrix Gateway 连接器根据下列准则允许或阻止流量：

- **User**。适用于 Exchange ActiveSync 的 Citrix Gateway 连接器使用在设备注册时捕获的授权用户值和名称结构。其常见形式是“域\用户名”，由运行 XenMobile 的服务器引用，该服务器通过 LDAP 连接到 Active

Directory。连接器配置实用程序中的 **Log**（日志）选项卡将显示通过连接器传递的值。如果需要确定值结构或者值结构不同，则将传递这些值。

- **Deviceid (ActiveSyncID)**。也称为所连接设备的 ActiveSyncID。此值通常可在 XenMobile 控制台的特定设备属性页面中找到。此值也可从连接器配置实用程序的“Log”（日志）选项卡中筛选出来。
- **DeviceType**。连接器可确定设备是 iPhone、iPad 还是其他设备类型，并能根据准则加以允许或阻止。与其他值一样，连接器配置实用程序可显示为 ActiveSync 连接处理的所有已连接设备的类型。
- **UserAgent**。包含有关所使用的 ActiveSync 客户端的信息。在大多数情况下，指定的值对应于移动设备平台的特定操作系统内部版本和版本。

在服务器上运行的连接器配置实用程序始终管理静态规则。

1. 在 SMG Controller 配置实用程序中，单击 **Static Rules**（静态规则）选项卡，然后单击 **Add**（添加）。
2. 在 **Static Rule Properties**（静态规则属性）对话框中，指定要用作条件的值。例如，可通过输入用户名（例如 AllowedUser）然后取消选中 **Disabled**（禁用）复选框，输入允许访问的用户。
3. 单击保存。

   静态规则现在即生效。此外，还可使用正则表达式来定义值，但必须在 config.xml 文件中启用规则处理模式。

配置动态规则

XenMobile 中的设备策略和属性定义动态规则，并且可以触发动态适用于 Exchange ActiveSync 的 Citrix Gateway 连接器过滤器。触发器建立在是否存在策略冲突或属性设置的基础之上。连接器过滤器的工作方式是针对给定策略违规情况或属性设置分析设备。如果设备满足条件，则将设备放入设备列表中。此设备列表既不是允许列表也不是阻止列表。它是满足定义条件的设备的列表。以下配置选项可用于定义是否要使用连接器允许或拒绝“设备列表”中的设备。

> 注意：
>
> 必须使用 XenMobile 控制台配置动态规则。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **ActiveSync Gateway**。此时将显示 ActiveSync Gateway 页面。
3. 在激活以下规则中，选择要激活的一个或多个规则。
4. 在“仅限 Android”下，在将 **Android** 域用户发送到 **ActiveSync Gateway** 中单击是，以确保 XenMobile 将 Android 设备信息发送到 Secure Mobile Gateway。

   启用了此选项时，如果 XenMobile 不具有 Android 设备用户的 ActiveSync 标识符，XenMobile 会将 Android 设备信息发送到适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。

通过编辑适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的 **XML** 文件来配置自定义策略

可以在适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序的策略选项卡上查看默认配置中的基本策略。如果要创建自定义策略，可编辑连接器的 XML 配置文件 (config\config.xml)。

1. 在文件中找到 **PolicyList** 部分，然后添加新的 **Policy** 元素。
2. 如果还需要新组，例如另一个静态组或支持另一个 GCP 的组，请将新 **Group** 元素添加到 **GroupList** 部分。
3. 也可以通过重新排列 **GroupRef** 元素，更改现有策略中组的顺序。

配置适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的 **XML** 文件

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器使用 XML 配置文件表示连接器的各项操作。此外，此文件还指定组文件和过滤器在评估 HTTP 请求时采取的关联操作。默认情况下，此文件命名为 config.xml 且位于以下位置：..\Program Files\Citrix\XenMobile Citrix ADC Connector\config。

GroupRef 节点

GroupRef 节点定义逻辑组名称。默认值为 AllowGroup 和 DenyGroup。

> 注意：
>
> GroupRef 节点在 GroupRefList 节点中出现的顺序非常重要。

GroupRef 节点的 ID 值标识逻辑容器或用于匹配特定用户帐户或设备的成员集合。操作属性指定过滤器处理与集合中的规则匹配的成员的方式。例如，与 AllowGroup 集中的规则匹配的用户帐户或设备将为 “pass”。pass 表示允许其访问 Exchange CAS。与 DenyGroup 集中的规则匹配的用户帐户或设备为 “rejected”。rejected 表示不允许其访问 Exchange CAS。

特定的用户帐户/设备或组合满足两个组中的规则时，会使用优先级约定来引导请求的结果。优先级通过 GroupRef 节点在 config.xml 文件中的自上而下的顺序体现。GroupRef 节点以优先级顺序排序。“允许” 组中针对给定条件的规则将始终优先于 “拒绝” 组中针对相同条件的规则。

组节点

此外，config.xml 还定义组节点。这些节点将逻辑容器 AllowGroup 和 DenyGroup 链接到外部 XML 文件。存储在外部文件中的条目构成过滤器规则的基础。

> 注意：
>
> 在此版本中，仅支持外部 XML 文件。

默认安装会在配置中实施两个 XML 文件：allow.xml 和 deny.xml。

配置适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

可以将适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置为基于以下属性，选择性地阻止或允许 ActiveSync 请求：**Active Sync** 服务 **ID**、设备类型、用户代理（设备操作系统）、授权用户和 **ActiveSync** 命令。

默认配置支持静态和动态组的组合。通过使用 SMG Controller 配置实用程序维护静态组。静态组可由已知类别的设备组成，如使用给定用户代理的所有设备。

名为网关配置提供程序的外部源负责维护动态组。适用于 Exchange ActiveSync 的 Citrix Gateway 连接器会定期连接这些组。XenMobile 可将允许和阻止设备与用户的组导出到连接器。

动态组由称为“网关配置提供程序”的外部源维护，并由适用于 Exchange ActiveSync 的 Citrix Gateway 连接器定期收集。XenMobile 可将允许和阻止设备与用户的组导出到连接器。

策略是组的有序列表，其中每个组都有关联的操作（允许或阻止）和组成员列表。一个策略可以有任何数量的组。策略内组的排序很重要，因为找到匹配项时就会执行组的操作，不会评估后续的组。

成员定义匹配请求中属性的方式。可以匹配单个属性，如设备 ID，或多个属性，如设备类型和用户代理。

为适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器选择安全模型

建立安全模型对于为任何规模的组织成功部署移动设备都至关重要。默认情况下，通常使用受保护或被隔离的网络控制来允许访问用户、计算机或设备。这种做法并非始终属于理想做法。对于确保移动设备的安全性，每个管理 IT 安全的组织的做法会略有不同，或者采用定制的方法。

相同的逻辑适用于移动设备安全性。由于移动设备和类型、每个用户的移动设备以及操作系统平台和应用程序的数量都非常大，因此，使用宽容模型属于较差的选择。在大多数组织中，受限模式将是最合乎逻辑的选择。

Citrix 允许适用于 Exchange ActiveSync 的 Citrix Gateway 连接器与 XenMobile 集成的配置方案如下所示：

宽容模型（许可模式）

宽容安全模型的运行前提是，默认情况下允许或授权任何设备进行访问。只有通过规则和过滤，某些设备才将被阻止并应用限制。宽容安全模型非常适合对移动设备的安全要求相对宽松的组织。该模型仅应用限制性控制来在适当的位置拒绝访问（策略规则失败时）。

限制性模型（阻止模式）

受限安全模型的运行前提是，默认情况下不允许或授权任何设备进行访问。通过安全检查点的任何访问都要进行过滤和检查，并且拒绝访问，除非允许访问的规则获得通过。受限安全模型适合对移动设备具有相对严格的安全标准的组织。该模式仅在所有允许访问的规则都通过时，才授权访问网络服务的使用和功能。

管理适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

可以使用适用于 Exchange ActiveSync 的 Citrix Gateway 连接器构建访问控制规则。这些规则允许或阻止访问来自托管设备的 ActiveSync 连接请求。访问基于设备状态、应用程序允许列表或阻止列表以及其他合规条件。

通过使用适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序，可构建强制实施公司电子邮件策略的动态和静态规则，从而阻止违反合规性标准的用户。也可设置电子邮件附件加密，使通过您的 Exchange Server 到达托管设备的所有附件都被加密，且只有获得授权的用户才能在托管设备上查看。

卸载适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

1. 使用管理员帐户运行 XncInstaller.exe。
2. 按照屏幕说明完成卸载。

安装、升级或卸载适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

1. 使用管理员帐户运行 XncInstaller.exe 以安装连接器，或者升级或删除现有连接器。
2. 按照屏幕说明完成安装、升级或卸载。

安装连接器后，必须手动重新启动 XenMobile 配置服务和通知服务。

安装适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

在其自己的 Windows 服务器上安装适用于 Exchange ActiveSync 的 Citrix Gateway 连接器。

连接器在服务器上放置的 CPU 负载取决于托管的设备数量。对于大量设备（超过 50000 个），如果没有群集环境，可能需要预配多个核心。连接器的内存占用量不足，无法保证更多内存。

适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的系统要求

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器通过 Citrix ADC 设备上配置的 SSL 桥接与 Citrix ADC 进行通信。该桥接允许设备将所有安全流量直接桥接到 XenMobile。连接器要求的最低系统配置如下：

组件	要求
计算机和处理器	733 MHz Pentium III 733 MHz 或更高版本的处理器。2.0 GHz Pentium III 或更高版本的处理器（建议）
Citrix ADC	Citrix ADC 设备，软件版本 10
内存	1 GB
硬盘	具有 150 MB 可用硬盘空间的 NTFS 格式本地分区
操作系统	Windows Server 2016、Windows Server 2012 R2 或 Windows Server 2008 R2 Service Pack 1。必须是基于英语的服务器。对 Windows Server 2008 R2 Service Pack 1 的支持将于 2020 年 1 月 14 日结束。
其他设备	与主机操作系统兼容的网络适配器（用于与内部网络通信）
Microsoft .NET Framework	版本 8.5.1.11 需要使用 Microsoft.NET Framework 4.5。

组件	要求
显示	VGA 或更高分辨率的显示器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的主机计算机要求的最小可用硬盘空间如下：

- 应用程序： 10 - 15 MB（建议 100 MB）
- 日志记录： 1 GB（建议 20 GB）

有关支持适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的平台的信息，请参阅支持的设备操作系统。

设备电子邮件客户端

并非所有电子邮件客户端都一致地为设备返回相同的 ActiveSync ID。由于适用于 Exchange ActiveSync 的 Citrix Gateway 连接器要求每个设备具有唯一的 ActiveSync ID，因此，仅支持为每个设备一致地生成相同的唯一 ActiveSync ID 的电子邮件客户端。Citrix 已测试这些电子邮件客户端，并且这些客户端在执行时没有错误：

- Samsung 本机电子邮件客户端
- iOS 本机电子邮件客户端

部署适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器使您可以使用 Citrix ADC 来代理并平衡 XenMobile Server 与 XenMobile 托管设备之间的通信负载。连接器定期与 XenMobile 通信以同步策略。连接器和 XenMobile 可以共同或单独组成群集，并且可以通过 Citrix ADC 平衡负载。

适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器组件

- 适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器服务：此服务提供一个 REST Web 服务界面，Citrix ADC 可以调用该界面以确定来自设备的 ActiveSync 请求是否获得授权。
- **XenMobile** 配置服务：此服务与 XenMobile 进行通信，以将 XenMobile 策略更改与连接器同步。
- **XenMobile** 通知服务：此服务将未经授权的设备访问通知发送到 XenMobile。这样，XenMobile 可以采取恰当的措施，例如通知用户设备被阻止的原因。
- 适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器配置实用程序：此应用程序允许管理员配置并监视连接器。

设置适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的侦听地址

要使适用于 Exchange ActiveSync 的 Citrix Gateway 连接器接收来自 Citrix ADC 的授权传输 ActiveSync 流量的请求，请执行以下操作。指定连接器在其上侦听 Citrix ADC Web 服务调用的端口。

1. 从开始菜单中，选择适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序。

2. 单击 **Web Service**（Web 服务）选项卡，然后键入连接器 Web 服务的侦听地址。可以选择 **HTTP** 或 **HTTPS**，或者同时选择两者。如果连接器与 XenMobile 的位置相同（安装在同一服务器上），请选择与 XenMobile 不冲突的端口值。
3. 配置值后，单击 **Save**（保存），然后单击 **Start Service**（启动服务），启动 Web 服务。

在适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器中配置设备访问控制策略

要配置将应用于托管设备的访问控制策略，请执行以下操作：

1. 在适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序中，单击 **Path Filters**（路径过滤器）选项卡。
2. 选择第一行 **Microsoft-Server-ActiveSync is for ActiveSync**（Microsoft-Server-ActiveSync 适用于 ActiveSync），然后单击 **Edit**（编辑）。
3. 在 **Policy**（策略）列表中，选择所需策略。对于包含 XenMobile 策略的策略，请选择 **Static + ZDM: Permit Mode**（静态 **+ ZDM:** 许可模式）或 **Static + ZDM: Block Mode**（静态 **+ ZDM:** 阻止模式）。这些策略将本地（或静态）规则与 XenMobile 的规则组合在一起。Permit Mode（许可模式）表示允许未被规则明确识别的所有设备访问 ActiveSync。Block Mode（阻止模式）表示阻止此类设备。
4. 设置策略后，单击 **Save**（保存）。

配置与 **XenMobile** 的通信

指定要与适用于 Exchange ActiveSync 的 Citrix Gateway 连接器和 Citrix ADC 结合使用的 XenMobile Server（又称为配置提供程序）的名称和属性。

> 注意：
>
> 此任务假定您已安装并配置 XenMobile。

1. 在适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置实用程序中，单击 **Config Providers**（配置提供程序）选项卡，然后单击 **Add**（添加）。
2. 输入您在此部署中使用的 XenMobile Server 的名称和 URL。如果您在多租户部署中部署了多个 XenMobile Server，则对每个服务器实例而言，此名称必须唯一。例如，可以在 **Name**（名称）中键入 **XMS**。
3. 在 **URL** 中，输入 XenMobile 全局配置提供程序 (GCP) 的 Web 地址，格式通常为 `https://<FQDN>/<instanceName>/services/<MagConfigService>`。*MagConfigService* 名称区分大小写。
4. 在 **Password**（密码）中，输入将用于 XenMobile Web 服务器的基本 HTTP 授权的密码。
5. 在 **Managing Host**（管理主机）中，输入安装了适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的服务器名称。
6. 在 **Baseline Interval**（基准时间间隔）中，指定从 XenMobile 提取新刷新的动态规则集的时间间隔。
7. 在 **Request Timeout**（请求超时）中，指定服务器请求超时的时间间隔。
8. 在 **Config Provider**（配置提供程序）中，选择配置提供程序服务器实例是否提供策略配置。
9. 在 **Events Enabled**（事件已启用）中，如果希望在设备被阻止时 Secure Mobile Gateway 通知 XenMobile，则启用此选项。如果在任何 Device Manager 自动操作中都使用了 Secure Mobile Gateway 规则，则此选项是必需的。

10. 配置服务器后，单击 **Test Connectivity**（测试连接），测试与 XenMobile 的连接。
11. 建立连接后，单击 **Save**（保存）。

为适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器部署冗余和可扩展性

如果要扩展适用于 Exchange ActiveSync 的 Citrix Gateway 连接器和 XenMobile 部署，可在多个 Windows Server 上安装连接器实例，全都指向同一 XenMobile 实例，然后可使用 Citrix ADC 来平衡服务器的负载。

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器配置有两种模式：

- 在非共享模式下，每个适用于 Exchange ActiveSync 的 Citrix Gateway 连接器实例都与一个 XenMobile Server 进行通信，并且保存所产生策略的自己的私有副本。例如，如果您有一个 XenMobile Server 群集，则可在每个 XenMobile Server 上运行连接器实例，然后连接器将从本地 XenMobile 实例获取策略。
- 在共享模式中，将一个连接器节点指定为主节点，它与 XenMobile 进行通信。产生的配置通过 Windows 网络共享或 Windows（或第三方）复制功能在其他节点中共享。

整个连接器配置在一个文件夹中（由多个 XML 文件组成）。连接器进程将检测对此文件夹中的任何文件所做的更改，并自动重新加载配置。共享模式中的主节点没有故障转移功能。但系统可容许主服务器关闭几分钟（例如，重新启动），因为上次已知的正确配置缓存在连接器进程中。

高级概念

January 5, 2022

> 注意：
>
> 本文介绍了 XenMobile Server 的高级概念。有关 Endpoint Management 的高级信息，请参阅高级概念。

XenMobile 高级概念文章深入介绍了 XenMobile 的相关产品文档。目地是通过专业技巧帮助缩短部署时间。这些文章可能会引用编写了相关内容的技术专家的观点。

有关您的端到端 XenMobile 环境的决策点、建议、常见问题和用例，请参阅《XenMobile 部署手册》中的相应部分。

有关 XenMobile 的社区支持论坛，请参阅 Citrix Discussions。

本地 **XenMobile** 与 **Active Directory** 的交互

January 5, 2022

文档贡献者：Siddartha Vuppala

本文解释 XenMobile Server 与 Active Directory 之间的交互。XenMobile Server 与 Active Directory 可以进行内联交互，也可以在后台交互。以下各节将详细介绍涉及到 Active Directory 交互的内联操作和后台操作。

> 注意：
>
> 本文是对交互的概述，不提供具体细节。有关在 XenMobile 控制台中配置 Active Directory 和 LDAP 的详细信息，请参阅域或域加安全令牌身份验证。

内联交互

XenMobile Server 使用管理员配置的 LDAP 与 Active Directory 通信。这些设置会检索用户和组的有关信息。以下是会导致 XenMobile Server 与 Active Directory 之间发生交互的操作。

1. **LDAP** 配置。配置 Active Directory 本身会导致与 Active Directory 交互。XenMobile Server 会尝试通过使用 Active Directory 进行身份验证来验证信息。服务器通过使用 Internet 协议、端口和提供的服务帐户凭据完成此操作。成功绑定表示已正确配置连接。
2. 基于组的交互。
    a) 在创建基于角色的访问控制 (RBAC) 和交付组定义期间搜索一个或多个组。XenMobile Server 管理员在 XenMobile 控制台中输入搜索文本字符串。XenMobile Server 在选定的域中搜索包含所提供子字符串的所有组。然后，XenMobile Server 检索通过搜索识别出的组的 objectGUID、sAMAccountName 和标识名属性。

    > 注意：
    >
    > 此信息存储在 XenMobile Server 数据库中。

    b) RBAC 和部署组定义添加或更新。XenMobile Server 管理员根据之前的搜索选择感兴趣的 Active Directory 组并将其包含在部署组定义中。XenMobile Server 在 Active Directory 中搜索特定组，每次搜索一个。XenMobile Server 搜索 objectGUID 属性并检索选定的属性，其中包括成员身份信息。组成员身份信息可帮助在检索到的组与 XenMobile Server 数据库的现有用户或组之间确定成员身份。更改组成员身份会导致受影响的用户成员发生 RBAC 和部署组派生，从而导致用户授权。

    > 注意：
    >
    > 更改部署组定义可能会导致受影响用户的应用程序或策略授权发生变化。

    c) 一次性 **PIN (OTP)** 邀请。XenMobile Server 管理员从 XenMobile Server 数据库中的 Active Directory 组列表中选择某个组。对于此组，所有用户（包括直接用户和间接用户）均检索自 Active Directory。OTP 邀请发送给在上述步骤中识别出的用户。

    > 注意：
    >
    > 上述三个交互说明基于组的交互因 XenMobile Server 配置更改而触发。如果配置没有发生更改，则意味着不包含与 Active Directory 的交互。它们也说明后台作业无需定期捕获组的变化。

3. 基于用户的交互。
    a) 用户身份验证。用户身份验证工作流会产生与 Active Directory 的两种交互：
        - 用于使用提供的凭据对用户进行身份验证。

- 将所选用户属性添加或更新到 XenMobile Server 数据库，这些属性包括 objectGUID、标识名、sAMAccountName 和组的直接成员身份。更改组成员身份会导致重新评估应用程序、策略和访问授权。

用户可以从设备或 XenMobile Server 控制台进行身份验证。在这两种情况下，与 Active Directory 的交互都遵循相同的行为。

b) 应用商店访问和刷新。刷新应用商店会导致刷新用户属性，其中包括直接组成员身份。此操作会引起重新评估用户授权。

c) 设备签入。管理员可以在 XenMobile 控制台中定期配置设备签入。每次签入设备时，都会刷新相应的用户属性，其中包括直接组成员身份。这些签入会引起重新评估用户授权。

d) 按组进行 OTP 邀请。XenMobile Server 管理员从 XenMobile Server 数据库中的 Active Directory 组列表中选择某个组。包括直接和间接（缘于嵌套）在内的用户成员均检索自 Active Directory 并保存在 XenMobile Server 数据库中。OTP 邀请会发送给在上述步骤中识别出的用户成员。

e) 按用户进行 OTP 邀请。管理员在 XenMobile 控制台中输入搜索文本字符串。XenMobile Server 查询 Active Directory 并返回与输入的文本字符串匹配的用户记录。然后，管理员选择要向其发送 OTP 邀请的用户。在向用户发送邀请前，XenMobile Server 会从 Active Directory 检索用户的详细信息，并在数据库中更新同样的详细信息。

后台交互

从与 Active Directory 的内联通信可以得出一个结论，即基于组的交互因更改 XenMobile Server 配置而触发。如果配置没有发生更改，则意味着不包含与 Active Directory 的交互。

这种交互需要后台作业：与 Active Directory 定期同步并将相关更改更新到感兴趣的组。

以下是与 Active Directory 交互的后台作业。

1. 组同步作业。此作业的目的是查询 Active Directory，每次针对一个感兴趣的组，以获取标识名或 sAMAccountName 属性的更改情况。对 Active Directory 的搜索查询使用感兴趣组的 objectGUID，以获取标识名和 sAMAccountName 属性的当前值。感兴趣组的标识名或 sAMAccountName 值的变化将更新到数据库中。

   > 注意：
   >
   > 此作业不更新用户相对于组的成员身份信息。

2. 嵌套组同步作业。此作业更新感兴趣组的嵌套层次结构中发生的变化。XenMobile Server 允许感兴趣组的直接成员和间接成员获得授权。用户的直接成员身份在基于用户的内联交互过程中更新。此作业在后台运行，跟踪间接成员身份。如果用户所属的组是感兴趣组的成员，则形成间接成员身份。

   此作业从 XenMobile Server 数据库搜集 Active Directory 组的列表。这些组属于部署组或 RBAC 定义。对于此列表中的每个组，XenMobile Server 会获取该组的成员。组的成员是代表用户和组的标识名列表。XenMobile Server 再查询 Active Directory，以获取感兴趣组的用户成员。这两个列表的差异仅针对感兴趣组的组成员。成员组中的变化将更新到数据库。会针对层次结构中的所有组重复相同的过程。

嵌套更改会导致处理受影响的用户以执行授权更改。

3. 禁用的用户检查。仅当 XenMobile 管理员创建用于检查被禁用用户的操作时才会运行此作业。此作业在组同步作业的范围内运行。此作业查询 Active Directory 以检查感兴趣用户的禁用状态，每次一个用户。

常见问题解答

默认情况下，后台作业运行的频率是多少?

- 组同步作业从本地时间 02:00 开始，每五小时运行一次。
- 嵌套组同步作业每天在本地时间的午夜运行一次。

为什么需要执行组同步作业?

- Active Directory 中用户记录的 memberOf 属性提供用户直接归属的组的列表。如果组从一个 OU 移动到另一个 OU，memberOf 属性将反映标识名的最新值。XenMobile Server 数据库还包含最近刷新的值。组标识名中的任何错误都可能会导致用户失去部署组的访问权限。用户还可能会丢失与该部署组关联的应用程序和策略。
- 后台作业会使 XenMobile Server 数据库中的组标识名属性保持在最新状态，以确保用户拥有其授权的访问权限。
- 将同步作业安排为五小时一次是基于 Active Directory 中发生组更改的情况并不常见这一假设。

是否可以关闭组同步作业?

- 如果您知道感兴趣的组不会从一个 OU 更改为另一个 OU，则可以关闭这些作业。

为什么需要嵌套组处理后台作业?

- 在 Active Directory 中，组嵌套并不是每天都会发生变化。感兴趣组的嵌套层次结构发生变化会导致受影响用户的授权改变。将某个组添加到层次结构中时，其成员用户将被授予相应的角色。当某个组移出嵌套时，该组的成员用户将丢失基于角色的授权的访问权限。
- 用户刷新过程中不会捕获嵌套更改。由于嵌套更改无法按需进行，这些更改通过后台作业捕获。
- 基于嵌套更改并不常见的假设，后台作业每天运行一次，以查找更改。

是否可以关闭嵌套组处理作业?

- 如果您知道感兴趣的组不会发生嵌套变化，则可以关闭这些作业。

XenMobile 部署

November 12, 2020

规划 XenMobile 部署时，需要考虑多种因素：

- 选择哪些设备?
- 如何管理设备?
- 如何确保您的网络在提供出色的用户体验的同时保持安全?

- 您需要哪些硬件以及如何对其进行故障排除?

本部分中的文章旨在帮助回答这些问题。包括的内容为各种用例以及与涵盖您的部署顾虑的主题有关的建议。

请谨记，指导原则或建议可能不适用于所有环境或用例。请务必先设置一个测试环境，然后再在 XenMobile 部署中使用。

本部分中的文章涵盖以下领域：

- 评估：规划您的部署时的常见用例以及需要考虑的问题。
- 设计和配置：设计和配置您的环境的建议
- 运行和监视：确保正在运行的环境平稳运行。

评估

与任何部署一样，评估您的需求是首要任务。您对 XenMobile 的主要需求是什么？您需要管理环境中的每个设备还是只需要管理应用程序？您可能需要同时管理设备和应用程序。您所需的 XenMobile 环境的安全性如何？让我们先了解一下规划您的部署时的常见用例以及需要考虑的问题。

- 管理模式
- 设备要求
- 安全性和用户体验
- 应用程序
- 用户社区
- 电子邮件策略
- XenMobile 集成
- 多站点要求

设计和配置

完成评估您的部署需求后，可以确定您的环境的设计和配置。需要规划以下几点事项：

- 选择您的服务器硬件
- 设置应用程序和设备策略
- 获取注册的用户

本节介绍了其中每种场景的用例和建议等。

- 将 Citrix ADC 与 Citrix Gateway 相集成
- MDX 应用程序的 SSO 和代理注意事项
- 身份验证
- 面向本地部署的参考体系结构
- 服务器属性
- 设备和应用程序策略
- 用户注册选项

- 调整 XenMobile 操作

运行和监视

XenMobile 环境启动并运行后，您将希望对其进行监视以确保平稳运行。监视部分探讨了您可以从何处查找 XenMobile 及其组件生成的各种日志和消息以及如何阅读这些日志。本部分内容还介绍了您可以执行的各种常见故障排除步骤以缩短客户支持反馈时间。

- 应用程序预配和取消预配
- 基于控制板的操作
- 基于角色的访问控制和 XenMobile 支持
- 系统监视
- 灾难恢复
- Citrix 支持过程

管理模式

January 5, 2022

对于每个 XenMobile 实例（单个服务器或节点的群集），您可以选择管理设备、应用程序还是管理两者。XenMobile 对设备和应用程序管理模式使用以下术语：

- 移动设备管理模式（MDM 模式）
- 移动应用程序管理模式（MAM 模式）
- MDM+MAM 模式（企业模式）

移动设备管理（**MDM** 模式）

> 重要：
>
> 如果配置了 MDM 模式，之后更改为 ENT 模式，请务必使用相同的 (Active Directory) 身份验证。XenMobile 不支持在用户注册后更改身份验证模式。有关详细信息，请参阅升级。

在 MDM 模式下，可以配置和支持移动设备以及确保移动设备的安全。MDM 允许您在系统级别保护设备和设备上的数据。可以配置策略、操作和安全功能。例如，如果设备丢失、被盗或不合规，可以选择性擦除设备。虽然应用程序管理功能在 MDM 模式下不可用，但是您可以在此模式下交付移动应用程序，例如公共应用商店应用程序和企业应用程序。下面是 MDM 模式的常见用例：

- MDM 是需要设备级别的管理策略或限制（例如，完全擦除、选择性擦除或地理位置）的公司拥有的设备的考虑因素。
- 客户需要管理实际的设备，但不需要 MDX 策略时，例如，应用程序容器化，控制应用程序数据共享或 Micro VPN。

- 用户仅需要电子邮件传送给其移动设备上的本机电子邮件客户端，并且 Exchange ActiveSync 或客户端访问服务器已可从外部访问时。在此用例中，可以使用 MDM 配置电子邮件传送。
- 部署本机企业应用程序（非 MDX）、公共应用商店应用程序或从公共应用商店交付的 MDX 应用程序时。请注意，MDM 解决方案本身不能防止设备上的应用程序之间的机密数据的数据泄漏。数据泄漏可能会在 Office 365 应用程序中执行复制和剪贴操作或“另存为”操作时发生。

移动应用程序管理（**MAM** 模式）

MAM 保护应用程序并且允许您控制应用程序数据共享。MAM 还允许您独立于个人数据来管理公司数据和资源。在 XenMobile 中配置了 MAM 模式的情况下，可以使用启用了 MDX 的移动应用程序提供每应用程序容器化和控制。术语“MAM 模式”又称为“仅 MAM 模式”。此术语将此模式与旧版 MAM 模式区分开来。

通过利用 MDX 策略，XenMobile 提供通过网络访问（例如 Micro VPN）进行的应用程序级别控制、应用程序和设备交互、数据加密和应用程序访问。

MAM 通常适用于自带 (BYO) 设备，因为即使设备未托管，公司数据仍受保护。MDX 有许多不需要 MDM 控制的仅 MAM 策略。

MAM 还支持移动生产力应用程序。此支持包括向 Citrix Secure Mail 安全地传送电子邮件、在受保护的移动生产力应用程序之间共享数据以及在 Citrix Files 中安全地存储数据。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：

- 您提供在应用程序级别管理的移动应用程序，例如 MDX 应用程序。
- 您不需要在系统级别管理设备。

MDM+MAM（企业模式）

MDM+MAM 属于混合模式，又称为“企业模式”，这将启用 XenMobile 企业移动性管理 (EMM) 解决方案中提供的所有功能集。在 XenMobile 中配置 MDM+MAM 模式将同时启用 MDM 和 MAM 功能。

XenMobile 允许您指定用户是否可以选择退出设备管理或者您是否需要进行设备管理。这种灵活性对包括混合用例的环境非常有用。这些环境可能需要通过 MDM 策略管理设备才能访问您的 MAM 资源。

MDM+MAM 适用于以下示例：

- 您具有同时需要 MDM 和 MAM 的单个用例。需要 MDM 才能访问您的 MAM 资源。
- 有些用例需要 MDM，而有些用例不需要。
- 有些用例需要 MAM，而有些用例不需要。

您通过“服务器模式”属性指定 XenMobile Server 的管理模式。您在 XenMobile 控制台中配置设置。模式可以是 MDM、MAM 或 ENT（适用于 MDM+MAM）。

您具有许可证的 XenMobile 版本决定管理模式和其他可用的功能，如下表中所示。

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
MDM 功能	MDM 功能	MDM 功能
-	MAM 功能	MAM 功能
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	-	ShareConnect
-	-	Citrix Files

管理模式和注册配置文件

管理模式和注册配置文件协同工作。可以使用注册配置文件为 Android 和 iOS 设备配置设备管理和应用程序管理注册选项。对于 Android，可用于 MDM+MAM 服务器模式的注册选项与可用于 MDM 模式的选项不同。有关详细信息，请参阅注册配置文件。

设备管理和 **MDM** 注册

XenMobile Enterprise 环境可以包括混合用例，其中某些用例要求通过 MDM 策略进行设备管理以访问 MAM 资源。为用户部署移动生产力应用程序之前，请完全评估您的用例并决定是否要求 MDM 注册。如果以后决定更改 MDM 注册的要求，用户可能必须重新注册其设备。

> 注意：
>
> 要指定是否要求用户在 MDM 中注册，请使用 XenMobile 控制台中的 XenMobile Server 属性需要注册（设置 > 服务器属性）。该全局服务器属性适用于 XenMobile 实例的所有用户和设备。该属性仅在 XenMobile Server 模式为 ENT 时适用。

下面概述了 XenMobile 企业模式部署中要求 MDM 注册的优势和劣势（以及缓解操作）。

MDM 注册为可选时

优势：

- 用户不需要将其设备置于 MDM 管理模式即可访问 MAM 资源。此选项可以增加用户采用率。

- 能够安全访问 MAM 资源以保护企业数据。
- 应用程序通行码等 MDX 策略可以控制对每个 MDX 应用程序的应用程序访问。
- 配置 Citrix ADC、XenMobile Server 和每应用程序超时以及 Citrix PIN 将提供一层额外的保护。
- 虽然 MDM 操作不适用于设备，但某些 MDX 策略可用于拒绝 MAM 访问。拒绝将取决于系统设置，例如越狱或获得 root 权限的设备。
- 用户可以选择是否在首次使用过程中通过 MDM 注册其设备。

劣势：

- MAM 资源适用于未在 MDM 中注册的设备。
- MDM 策略和操作仅适用于 MDM 注册的设备。

缓解方案：

- 使用户同意在其选择不遵从合规性的情况下追究其责任的公司条款和条件。使管理员监视未托管的设备。
- 使用应用程序计时器管理应用程序访问和安全性。降低的超时值提高了安全性，但可能会影响用户体验。
- 一种方案是使用第二个要求 MDM 注册的 XenMobile 环境。考虑使用此方案时，请谨记管理两种环境的额外开销以及所需的额外资源。

要求 **MDM** 注册时

优势：

- 能够将 MAM 资源的访问仅限制到 MDM 托管的设备。
- 根据需要，MDM 策略和操作可能适用于环境中的所有设备。
- 用户无法选择退出注册其设备。

劣势：

- 要求所有用户通过 MDM 注册。
- 可能会降低反对公司管理其个人设备的用户的采用率。

缓解方案：

- 针对 XenMobile 在其设备上实际管理的对象以及信息管理员可以访问的资源向用户提供教育培训。
- 可以对不需要 MDM 管理的设备使用第二个 XenMobile 环境和服务器模式 MAM（又称为 “仅 MAM 模式”）。考虑使用此方案时，请谨记管理两种环境的额外开销以及所需的额外资源。

关于 **MAM** 和旧版 **MAM** 模式

XenMobile 10.3.5 引入了新的 “仅 MAM” 服务器模式。文档使用这些术语来区分以前的 MAM 模式与新的 MAM 模式。新模式称为 “仅 MAM” 或 “MA”，以前的 MAM 模式称为旧版 MAM 模式。

当 XenMobile 的服务器模式属性为 MAM 时 “仅 MAM” 模式生效。设备在 MAM 模式中注册。

当 XenMobile 的服务器模式属性为 ENT 以及用户选择退出设备管理时，旧 MAM 功能生效。在这种情况下，设备在 MAM 模式下注册。选择退出 MDM 管理的用户将继续接收旧版 MAM 功能。

> 注意：
>
> 以前，将“服务器模式”属性设置为 MAM 与将其设置为 ENT 具有相同的效果：选择退出 MDM 管理的用户收到旧版 MAM 功能。

下表概述了用于特定许可证类型的“服务器模式”设置以及所需的设备模式：

您的许可证适用于此版本	您希望设备在此模式下注册	将 **“服务器模式”** 属性设置为
Enterprise/Advanced/MDM	MDM 模式	MDM
Enterprise/Advanced	MAM 模式（又称为“仅 MAM 模式”）	MAM
Enterprise/Advanced	MDM+MAM 模式	ENT（选择退出设备管理的用户将在旧版 MAM 模式下操作）。

仅 MAM 模式支持以前仅对 ENT 可用的以下功能。这些功能不适用于 Windows Phone。

- 基于证书的身份验证：仅 MAM 模式支持基于证书的身份验证。即使 Active Directory 密码过期时，用户也会遇到继续访问其应用程序的情况。如果对 MAM 设备使用基于证书的身份验证，则必须配置 Citrix Gateway。默认情况下，在 **XenMobile** 设置 **> Citrix Gateway** 中，“向用户提供用于身份验证的证书”设置为关，表示使用用户名和密码身份验证。将该设置更改为开将启用证书身份验证。
- 自助服务门户：允许用户执行各自的应用程序锁定和应用程序擦除操作。这些操作适用于设备上的所有应用程序。您可以在配置 **>** 操作中配置应用程序锁定和应用程序擦除操作。
- 所有注册安全模式：包括“高安全性”、“邀请 URL”和“双重身份验证”，通过管理 **>** 注册邀请进行配置。
- 面向 **Android** 和 **iOS** 设备的设备注册限制：服务器属性每个用户的设备数已移动到配置 **>** 注册配置文件，并且现在适用于所有服务器模式。
- 仅 **MAM API**：对于仅 MAM 设备，可以通过使用任何 REST 客户端和 XenMobile REST API 调用 XenMobile 控制台展现的服务来调用 REST 服务。
- 通过仅 MAM API，可以执行以下操作：
  - 发送邀请 URL 和一次性 PIN。
  - 在设备上发出应用程序锁定和擦除命令。

下表总结了旧版 MAM 和仅 MAM 功能之间的差别。

注册场景及其他功能	旧版 **MAM**（服务器模式为 **ENT**）	仅 **MAM** 模式（服务器模式为 **MAM**）
证书身份验证	不受支持。	支持。对于证书身份验证，需要配置 Citrix Gateway。

部署要求	XenMobile Server 不需要能够直接从设备访问。	XenMobile Server 不需要能够直接从设备访问。
注册选项	使用 Citrix Gateway FQDN，或者使用 MDM FQDN 时，选择退出注册。	使用 XenMobile Server FQDN。
注册方法 *	用户名 + 密码	用户名 + 密码、高安全性、邀请 URL、邀请 URL+PIN、邀请 URL + 密码、双重身份验证、用户名 + PIN
应用程序锁定和擦除	支持。	支持。
用于应用程序锁定和擦除的自助服务门户选项	不受支持。	支持。
应用程序擦除行为	应用程序保留在设备上，但不可使用。XenMobile 仅删除客户端上的帐户。	应用程序保留在设备上，但不可使用。XenMobile 仅删除客户端上的帐户。
面向仅 MAM 用户的自动化操作。	支持事件、设备属性和用户属性操作。不支持基于已安装的应用程序的自动化操作。	支持事件、设备属性、用户属性和某些基于应用程序的操作，包括应用程序擦除和应用程序锁定。
删除了 Active Directory 用户时的内置操作	支持应用程序擦除。	支持应用程序擦除。
注册限制	支持；通过注册配置文件进行配置。	支持；通过注册配置文件进行配置。
软件清单	支持。XenMobile 列出了设备上安装的应用程序	不受支持。

* 关于通知： SMTP 是唯一支持的发送注册邀请的方法。

> 重要：
>
> 对于仅 MAM 模式，以前注册的用户必须重新注册其设备。请务必向用户提供注册所需的 XenMobile Server FQDN。在仅 MAM 模式下，设备使用 XenMobile Server FQDN 进行注册，这一点与 ENT 模式相同。（在旧版 MAM 模式下，设备使用 Citrix Gateway FQDN 进行注册。）

设备要求

January 5, 2022

考虑采用任何部署的重点是您计划推出的设备。在 iOS、Android 和 Windows 平台上，选项非常多。有关 XenMobile 支持的设备列表，请参阅支持的设备平台。

在自带设备 (BYOD) 环境中，可以混合使用支持的平台。但是，通知用户可以注册的设备时，请考虑“支持的设备平台”一文中的限制信息。即使仅允许在您的环境中使用一个或两个设备，XenMobile 在 iOS、Android 和 Windows 设备上运行时也略有差别。在每个平台上提供不同的功能集。

此外，并非所有应用程序设计都同时针对平板电脑和手机的外形规则。做出广泛传播的更改之前，请测试应用程序以确保其适合您要推出的设备屏幕。

可以同时考虑注册因素。Apple 和 Google 提供企业注册计划。通过 Apple 部署计划和 Google Android Enterprise，您可以购买预配置的、可随时供员工使用的设备。

有关注册的详细信息，请参阅用户注册选项。

安全性和用户体验

January 5, 2022

对于任何组织而言，安全性都至关重要，但在提高安全性和改善用户体验方面，您必须在两者之间实现权衡。例如，您的环境可能非常安全，但用户使用起来很困难。或者，您的环境可能具有良好的用户体验，但访问控制却不那么严格。本虚拟手册中的其他部分详细介绍了安全功能。本文的目的是全面概述 XenMobile 中的常见安全问题和可用的安全选项。

下面是针对每种用例需要谨记的一些主要注意事项：

- 您要保护某些应用程序的安全还是整个设备的安全？或者还是同时保护这两者的安全？
- 您希望您的用户如何进行身份验证？您计划使用 LDAP 还是基于证书的身份验证？或者组合使用这两者？
- 您希望如何处理用户会话超时？请谨记，后台服务、Citrix ADC 以及能够在脱机时访问应用程序的超时值不同。
- 您希望用户设置设备级别通行码、应用程序级别通行码还是两者？您希望允许用户可以尝试登录多少次？请谨记，使用 MAM 实现的额外每应用程序身份验证要求可能会影响用户体验。
- 您还希望对用户实施其他哪些限制？您是否希望用户访问 Siri 等云服务？他们可以使用您为其提供的每个应用程序执行哪些操作以及不能执行哪些操作？您是否要部署企业 Wi-Fi 策略，以防止在办公室内部使用手机网络数据流量套餐？

应用程序与设备

首先要考虑的事情之一是是否通过使用移动应用程序管理 (MAM) 来保护某些应用程序。或者，如果您还希望使用移动设备管理 (MDM) 来管理整个设备。通常情况下，如果您不需要设备级别控制，则仅管理移动应用程序，尤其是当贵组织支持自带设备 (BYOD) 时。

使用 XenMobile 不进行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，而不是通过设备级别控制，如选择性擦除或完全擦除。根据您设置的值，策略需要设备定期检查 XenMobile 以确认仍允许运行应用程序。

MDM 允许您保护整个设备的安全，包括对设备上的所有软件执行清单操作的能力。您可以在设备越狱、获得 root 权限或安装了不安全的软件时阻止注册。但是，采用此级别的控制会使用户极不愿意允许对其私人设备拥有太多控制权限，因此可能会降低注册率。

身份验证

身份验证对用户体验有很大的影响。如果贵组织已在运行 Active Directory，则使用 Active Directory 是您的用户访问系统的最简单方法。

身份验证用户体验的另一个重要方面是超时。高安全性环境会要求用户每次访问系统时进行登录，但这种方式对所有组织都不适用。例如，要求用户每次要访问其电子邮件时都输入其凭据会显著影响用户体验。

用户熵

要提高安全性，可以启用一项名为用户熵的功能。Citrix Secure Hub 与其他一些应用程序通常共享通用数据（例如，密码、PIN 和证书）以确保一切正常运行。此信息存储在 Secure Hub 中的一个通用保管库中。如果您通过 **Encrypt Secrets**（加密机密）选项启用用户熵，XenMobile 将创建一个名为 UserEntropy 的新保管库。XenMobile 将信息从通用保管库移动到新保管库中。为使 Secure Hub 或其他应用程序访问这些数据，用户必须输入密码或 PIN。

启用用户熵将会在多个位置添加另一层身份验证。因此，每当应用程序要求访问 UserEntropy 保管库中的共享数据（包括证书）时，用户都必须输入密码或 PIN。

您可以阅读 XenMobile 文档中的关于 MDX Toolkit，了解有关用户熵的详细信息。要启用用户熵，您可以在客户端属性中找到相关设置。

策略

MDX 和 MDM 策略都为组织提供了很大的灵活性，但也可以限制用户。例如，您可能希望阻止对可能会向各种位置发送敏感数据的云应用程序（例如 Siri 或 iCloud）进行访问。您可以设置一个策略来阻止访问这些服务，但请谨记，此类策略会导致发生意外结果。iOS 键盘麦克风也依赖于云访问，因此，您可能也会阻止访问该功能。

应用程序

企业移动性管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 让组织能够保护和控制移动设备，而 MAM 有助于应用程序交付和管理。随着越来越多的人采用自带设备，通常可以实施 MAM 解决方案，以帮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。

通过 XenMobile，您可以配置特定的 MAM 策略和 VPN 设置以防止数据泄漏和其他安全威胁，进一步保护这些应用程序的安全。XenMobile 为组织提供了部署以下任何解决方案的灵活性：

- 仅 MAM 环境
- 仅 MDM 环境
- 在同一平台中同时提供 MDM 和 MAM 功能的统一 XenMobile Enterprise 环境

除了能够将应用程序交付到移动设备外，XenMobile 还通过 MDX 技术提供应用程序容器化。MDX 通过平台提供的独立于设备级别加密的加密来保护应用程序的安全。您可以擦除或锁定该应用程序，并且这些应用程序受到基于策略的精细控制的限制。独立软件供应商 (ISV) 可以使用移动应用程序 SDK 应用这些控制。

在企业环境中，用户使用各种各样的移动应用程序来协助完成自己的工作职责。这些应用程序可能包括公共应用商店中的应用程序、内部开发的应用程序和本机应用程序。XenMobile 按如下所示对这些应用程序进行分类：

公共应用商店：这些应用程序包括公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。组织外的供应商通常在公共应用商店中提供其应用程序。这种方式让其客户可以直接从 Internet 下载应用程序。根据用户的需求，您可以在组织中使用很多公共应用程序。例如，GoToMeeting、Salesforce 和 EpicCare 应用程序属于此类应用程序。

Citrix 不支持直接从公共应用商店下载应用程序二进制文件，然后使用 MDX Toolkit 将其打包以进行企业分发。要通过 MDX 启用第三方应用程序，请与您的应用程序供应商联系以获取应用程序二进制文件。可以使用 MDX Toolkit 封装二进制文件，也可以将 MAM SDK 与二进制文件集成。

内部应用程序：许多组织都有内部开发人员，他们创建提供特定功能并在组织内独立开发和分发的应用程序。在某些情况下，一些组织可能还有 ISV 提供的应用程序。您可以将此类应用程序作为本机应用程序进行部署，也可以通过使用 MAM 解决方案（例如 XenMobile）容器化这些应用程序。例如，某医疗机构会创建一个内部应用程序，以允许医师在移动设备上查看患者信息。然后，组织可以启用 MAM SDK 或通过 MDM 封装应用程序，以保护患者信息的安全并启用对后端患者数据库服务器的 VPN 访问。

Web 和 **SaaS** 应用程序：这些应用程序包括通过内部网络访问的应用程序（Web 应用程序）或通过公用网络访问的应用程序 (SaaS)。XenMobile 还允许您使用一组应用程序连接器创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器便于对现有 Web 应用程序进行单点登录 (SSO)。有关详细信息，请参阅应用程序连接器类型。例如，您可以使用基于安全声明标记语言 (SAML) 的 Google Apps SAML for SSO 登录 Google Apps。

移动生产力应用程序： Citrix 开发且在 XenMobile 许可证中附带的应用程序。有关详细信息，请参阅关于移动生产力应用程序。Citrix 还提供 ISV 使用移动应用程序 SDK 开发的其他业务就绪型应用程序。

HDX 应用程序：您通过 StoreFront 发布且由 Windows 托管的应用程序。如果您有 Citrix Virtual Apps and Desktops 环境，则可以将这些应用程序与 XenMobile 集成以向注册用户提供这些应用程序。

根据您计划通过 XenMobile 部署和管理的移动应用程序的类型，基础配置和体系结构会有所差别。例如，如果具有不同权限级别的多组用户使用某一个应用程序，您可能需要独立的交付组以部署该应用程序的两个版本。此外，您还必须确保用户组成员身份相互排斥，以避免在用户设备上出现策略不匹配。

您还可能希望使用 Apple 批量购买管理 iOS 应用程序许可。此选项将要求您注册加入 Apple 批量购买，并在 XenMobile 控制台中配置 XenMobile 批量购买设置，以便使用批量购买许可证分发应用程序。鉴于各种此类用例，在实施 XenMobile 环境之前务必要评估和规划您的 MAM 策略。规划您的 MAM 策略时，您可以先明确以下各项：

应用程序类型：列出您计划支持的不同类型的应用程序，然后对其进行组织整理。例如：公共应用程序、本机应用程序、移动生产力应用程序、Web 应用程序、内部应用程序、ISV 应用程序等。此外，还按不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。此分类可帮助您调整每种类型的应用程序所需的 XenMobile 设置。例如，某些应用程序可能不符合封装条件，或者可能需要移动应用程序 SDK 来启用特殊 API 才能与其他应用程序进行交互。

网络要求：通过适当的设置为应用程序配置特定的网络访问要求。例如，某些应用程序可能需要通过 VPN 访问您的内部网络。某些应用程序可能需要 Internet 访问权限才能通过 DMZ 对访问进行路由。为了允许此类应用程序连接到所需网络，您必须相应地配置各种设置。明确每个应用程序网络要求有助于在早期做出您的体系结构决策，这将简化整体实施流程。

安全要求：定义适用于单个应用程序或所有应用程序的安全要求非常重要。该规划可确保您在安装 XenMobile Server 时创建正确的配置。尽管 MDX 策略等设置适用于各个应用程序，但会话和身份验证设置应用于所有应用程序。某些应用程序可能具有特定的加密、容器化、封装、加密、身份验证、地理围栏、通行码或数据共享要求，您可以提前指明这些要求，以简化部署。

部署要求：您可能希望使用基于策略的部署以仅允许合规用户下载已发布的应用程序。例如，您可能希望某些应用程序要求满足以下任意要求：

- 基于设备平台的加密已启用
- 设备已托管
- 设备满足最低操作系统版本
- 某些应用程序仅适用于企业用户

您可能还希望某些应用程序仅供企业用户使用。请提前列出此类要求，以便您可以配置适当的部署规则或操作。

许可要求：保留应用程序相关的许可要求的记录。这些笔记有助于您有效地管理许可证使用情况，以及决定是否在 XenMobile 中配置特定功能以便于进行许可。例如，如果部署免费或付费 iOS 应用程序，Apple 会通过要求用户登录其 iTunes 帐户来强制对该应用程序执行许可要求。您可以注册加入 Apple 批量购买以通过 XenMobile 分发和管理这些应用程序。批量购买允许用户无需登录其 iTunes 帐户即可下载应用程序。此外，Samsung SAFE 和 Samsung Knox 等工具有特殊的许可要求，您需要在部署这些功能之前先完成这些要求。

允许列表和阻止列表要求：您可能希望阻止用户安装或使用某些应用程序。创建使设备不合规的应用程序允许列表。然后，设置在设备不合规时触发的策略。另一方面，某个应用程序可能可以使用，但可能会出于某个原因而被列入阻止列表。在这种情况，可以将该应用程序添加到允许列表中，并指出该应用程序是可以使用的但不是必需的。此外，请谨记，预先安装在新设备上的应用程序可能包括一些不属于操作系统的常用应用程序。这些应用程序可能会与您的阻止列表策略相冲突。

应用程序用例

某医疗机构计划部署 XenMobile 以用作其移动应用程序的 MAM 解决方案。移动应用程序将交付给公司和自带设备用户。IT 决定交付和管理以下应用程序：

- 移动生产力应用程序：由 Citrix 提供的 iOS 和 Android 应用程序。
- **Secure Mail**：电子邮件、日历和联系人应用程序。
- **Secure Web**：用于访问 Internet 和 Intranet 站点的 Secure Web 浏览器。
- **Citrix Files**：用于访问共享数据以及共享、同步和编辑文件的应用程序。

公共应用商店

- **Secure Hub**：所有移动设备用来与 XenMobile 通信的客户端。IT 通过 Secure Hub 客户端向移动设备推送安全设置、配置和移动应用程序。Android 和 iOS 设备通过 Secure Hub 在 XenMobile 中注册。
- **Citrix Receiver**：允许用户在移动设备上打开 Virtual Apps and Desktops 托管的应用程序的移动应用程序。
- **GoToMeeting**：在线会议、桌面共享和视频会议客户端，让用户可以通过 Internet 实时与其他计算机用户、客户、客户端或同事联系。
- **Salesforce1**： Salesforce1 允许用户从移动设备访问 Salesforce，并将所有 Chatter、CRM、自定义应用程序和业务流程集中在一起，以使 Salesforce 任何用户拥有统一的体验。
- **RSA SecurID**：用于双重身份验证的基于软件的令牌。
- **EpicCare** 应用程序：这些应用程序让医疗工作人员可以安全便携地访问患者图表、患者列表、计划和消息。
  - **Haiku**：适用于 iPhone 和 Android 手机的移动应用程序。
  - **Canto**：适用于 iPad 的移动应用程序
  - **Rover**：适用于 iPhone 和 iPad 的移动应用程序。

HDX：这些应用程序通过 Citrix Virtual Apps and Desktops 交付。

- **Epic Hyperspace**：用于电子病历管理的 Epic 客户端应用程序。

ISV

- **Vocera**： HIPAA 合规 VoIP 和消息传送移动应用程序，通过 iPhone 和 Android 智能手机随时随地扩展 Vocera 语音技术的优势。

内部应用程序

- **HCMail**：该应用程序用于撰写加密邮件、在内部邮件服务器上搜索通讯簿以及使用电子邮件客户端将加密邮件发送给联系人。

内部 **Web** 应用程序

- **PatientRounding**：该 Web 应用程序用于按不同的部门记录患者健康信息。
- **Outlook Web Access**：允许通过 Web 浏览器访问电子邮件。
- **SharePoint**：用于组织范围的文件和数据共享。

下表列出了 MAM 配置所需的基本信息。

应用程序名称	应用程序类型	**MDX** 打包	**iOS**	**Android**
Secure Mail	XenMobile App	版本 10.4.1 及更高版本不使用	是	是
Secure Web	XenMobile App	版本 10.4.1 及更高版本不使用	是	是

Citrix Files	XenMobile App	版本 10.4.1 及更高版本不使用	是	是
Secure Hub	公共应用程序	不适用	是	是
Citrix Receiver	公共应用程序	不适用	是	是
GoToMeeting	公共应用程序	不适用	是	是
Salesforce1	公共应用程序	不适用	是	是
RSA SecurID	公共应用程序	不适用	是	是
Epic Haiku	公共应用程序	不适用	是	是
Epic Canto	公共应用程序	不适用	是	否
Epic Rover	公共应用程序	不适用	是	否
Epic Hyperspace	HDX 应用程序	不适用	是	是
Vocera	ISV 应用程序	是	是	是
HCMail	内部应用程序	是	是	是
PatientRounding	Web 应用程序	不适用	是	是
Outlook Web Access	Web 应用程序	不适用	是	是
SharePoint	Web 应用程序	不适用	是	是

以下各表列出了您在 XenMobile 中配置 MAM 策略时可以查询的特定要求。

应用程序名称	需要 **VPN**	交互	交互	基于设备平台的加密
		（与容器外部的应用程序）	（从容器外部的应用程序）	
————	—	————————	————————	————
Secure Mail	Y	选择性允许	允许	不需要
Secure Web	Y	允许	允许	不需要
Citrix Files	Y	允许	允许	不需要
Secure Hub	Y	不适用	不适用	不适用
Citrix Receiver	Y	不适用	不适用	不适用
GoToMeeting	N	不适用	不适用	不适用
Salesforce1	N	不适用	不适用	不适用
RSA SecurID	N	不适用	不适用	不适用
Epic Haiku	Y	不适用	不适用	不适用
Epic Canto	Y	不适用	不适用	不适用
Epic Rover	Y	不适用	不适用	不适用

Epic Hyperspace	Y	不适用	不适用	不适用
Vocera	Y	已阻止	已阻止	不需要
HCMail	Y	已阻止	已阻止	必需
PatientRounding	Y	不适用	不适用	必需
Outlook Web Access	Y	不适用	不适用	不需要
SharePoint	Y	不适用	不适用	不需要

应用程序名称	代理过滤	许可	地理围栏	移动应用程序 **SDK**	最低操作系统版本
Secure Mail	必需	不适用	选择性必需	不适用	强制执行
Secure Web	必需	不适用	不需要	不适用	强制执行
Citrix Files	必需	不适用	不需要	不适用	强制执行
Secure Hub	不需要	批量购买	不需要	不适用	不强制执行
Citrix Receiver	不需要	批量购买	不需要	不适用	不强制执行
GoToMeeting	不需要	批量购买	不需要	不适用	不强制执行
Salesforce1	不需要	批量购买	不需要	不适用	不强制执行
RSA SecurID	不需要	批量购买	不需要	不适用	不强制执行
Epic Haiku	不需要	批量购买	不需要	不适用	不强制执行
Epic Canto	不需要	批量购买	不需要	不适用	不强制执行
Epic Rover	不需要	批量购买	不需要	不适用	不强制执行
Epic Hyperspace	不需要	不适用	不需要	不适用	不强制执行
Vocera	必需	不适用	必需	必需	强制执行
HCMail	必需	不适用	必需	必需	强制执行
PatientRound-ing	必需	不适用	不需要	不适用	不强制执行
Outlook Web Access	必需	不适用	不需要	不适用	不强制执行
SharePoint	必需	不适用	不需要	不适用	不强制执行

用户社区

每个组织都由多个以不同的功能角色运作的用户社区组成。这些用户社区使用您通过用户移动设备提供的各种资源执行不同的任务和办公功能。用户可能会使用您提供的移动设备在家中或远程办公室工作。或者，用户可能会使用其私人移动设备，这允许其访问遵从某些安全合规规则的工具。

越来越多的用户设备开始使用移动设备，企业移动性管理 (EMM) 将对防止数据泄漏以及强制执行安全限制至关重要。为了实现高效率以及更加复杂的移动设备管理，您可以对用户社区进行分类。这样可以简化将用户映射到资源的过程，并确保正确的安全策略应用到正确的用户。

以下示例说明了如何对医疗机构的用户社区进行分类以实现 EMM。

用户社区用例

本示例医疗机构提供技术资源以及向多个用户提供访问权限，包括网络和附属机构员工和志愿者。此机构已选择仅向非执行用户推出 EMM 解决方案。

此机构的用户角色和功能可以划分为几个子组，包括：临床、非临床和合同工。选定的一组用户将收到企业移动设备，而其他用户可以从其私人设备访问有限的公司资源。要强制执行正确的安全限制级别以及防止数据泄漏，此机构决定企业 IT 负责管理注册的每个设备（企业发放或 BYOD）。此外，用户只能注册一个设备。

下面的部分概述了每个子组的角色和功能：

临床

- 护士
- 医师（医生、外科医生等）
- 专家（营养学家、麻醉师、放射科医师、心脏病专家、肿瘤学家等）
- 外部医师（从远程办公室工作的非雇员医师和办公室工作人员）
- 家庭医疗服务（执行患者家访的医师服务的办公室和移动工作人员）
- 研究专家（在六家研究机构执行临床研究以寻找医学问题答案的知识型工作者和高级用户）
- 教育和培训（护士、医师以及教育和培训专家）

非临床

- 共享服务（执行以下各种后勤职能的办公室工作人员：HR、工资单、应付账款、供应链服务等）
- 医师服务（执行各种医疗保健管理、管理服务以及针对提供商的业务流程解决方案的办公室工作人员，包括：管理服务、分析和业务智能、业务系统、客户服务、财务、托管式医疗管理、患者访问解决方案、收支周期解决方案等）
- 支持服务（执行各种非临床功能的办公室工作人员，包括：收益管理、临床整合、沟通、薪酬与绩效管理、设施和物业服务、HR 技术系统、信息服务、内部审计和流程改进等。）
- 慈善活动（执行支持慈善活动的各项功能的办公室和移动工作人员）

合同工

- 制造商和供应商合作伙伴（通过站点到站点 VPN 现场连接和远程连接，提供各种非临床支持功能）

根据上述信息，此机构创建了以下实体。有关 XenMobile 中的交付组的详细信息，请参阅部署资源。

Active Directory 组织单位 (OU) 和组

针对 OU = XenMobile 资源：

- OU = 临床；组 =
  - XM-护士
  - XM-医师
  - XM-专家
  - XM-外部医师
  - XM-家庭医疗服务
  - XM-研究专家
  - XM-教育和培训
- OU = 非临床；组 =
  - XM-共享服务
  - XM-医师服务
  - XM-支持服务
  - XM-慈善活动

XenMobile 本地用户和组

针对组 = 合同工，用户 =

- 供应商 1
- 供应商 2
- 供应商 3
- … 供应商 10

XenMobile 交付组

- 临床-护士
- 临床-医师
- 临床-专家
- 临床-外部医师
- 临床-家庭医疗服务
- 临床-研究专家
- 临床-教育和培训
- 非临床-共享服务

- 非临床-医师服务
- 非临床-支持服务
- 非临床-慈善活动

交付组和用户组映射

Active Directory 组	**XenMobile** 交付组
XM-护士	临床-护士
XM-医师	临床-医师
XM-专家	临床-专家
XM-外部医师	临床-外部医师
XM-家庭医疗服务	临床-家庭医疗服务
XM-研究专家	临床-研究专家
XM-教育和培训	临床-教育和培训
XM-共享服务	非临床-共享服务
XM-医师服务	非临床-医师服务
XM-支持服务	非临床-支持服务
XM-慈善活动	非临床-慈善活动

交付组和资源映射

以下各表列出了分配给此用例中每个交付组的资源。第一个表显示了移动应用程序分配。第二个表显示了公共应用程序、HDX 应用程序和设备管理资源。

XenMobile 交付组	**Citrix** 移动应用程序	公共移动应用程序	**HDX** 移动应用程序
临床-护士	X		
临床-医师			
临床-专家			
临床-外部医师	X		
临床-家庭医疗服务	X		
临床-研究专家	X		

临床-教育和培训		X	X
非临床-共享服务		X	X
非临床-医师服务		X	X
非临床-支持服务	X	X	X
非临床-慈善活动	X	X	X
合同工	X	X	X

XenMobile 交付组	公共应用程序：**RSA SecurID**	公共应用程序：**EpicCare Haiku**	**HDX** 应用程序：**Epic Hyperspace**	通行码策略	设备限制	自动化操作	**WiFi** 策略
临床-护士							X
临床-医师					X		
临床-专家							
临床-外部医师							
临床-家庭医疗服务							
临床-研究专家							
临床-教育和培训		X	X				
非临床-共享服务		X	X				
非临床-医师服务		X	X				
非临床-支持服务		X	X				

备注和注意事项

- XenMobile 在初始配置过程中创建名为“所有用户”的默认交付组。如果不禁用此交付组，所有 Active Directory 用户都将具有在 XenMobile 中注册的权限。
- XenMobile 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果某个用户所属的组未在 XenMobile 中映射，该用户将无法注册。同样，如果某个用户属于多个组的成员，XenMobile 将仅对在映射到 XenMobile 的组中的用户进行分类。
- 要强制进行 MDM 注册，必须在 XenMobile 控制台的“服务器属性”中将“需要注册”选项设置为“真”。有关详细信息，请参阅服务器属性。
- 您可以通过删除 SQL Server 数据库中 dbo.userlistgrps 下的条目，将用户组从 XenMobile 交付组中删除。警告：执行此操作之前，请创建 XenMobile 和数据库的备份。

关于 **XenMobile** 中的设备所有权

可以根据用户设备的所有者对用户进行分组。设备所有权包括公司拥有的设备和用户拥有的设备（也称为自带设备 (BYOD)）。您可以在 XenMobile 控制台中的两个位置控制 BYOD 设备连接到您网络的方式：在每种资源的“部署规则”页面上以及通过设置页面上的服务器属性。有关部署规则的详细信息，请参阅 XenMobile 文档中的配置部署规则。有关服务器属性的详细信息，请参阅服务器属性。

可以要求所有 BYOD 用户在接受公司对其设备的管理后才能访问应用程序。或者，也可以在不管理用户设备的情况下直接允许其访问公司应用程序。

将服务器设置 **wsapi.mdm.required.flag** 设为 **true** 时，XenMobile 将托管所有 BYOD 设备，并且任何拒绝注册的用户都将无法访问应用程序。在企业 IT 团队需要高安全性和积极用户体验（在 XenMobile 中注册用户设备时）的环境中，请考虑将 **wsapi.mdm.required.flag** 设置为 **true**。

如果让 **wsapi.mdm.required.flag** 保留 **false**（默认设置），用户可以拒绝注册，但仍可以在其设备上通过 XenMobile Store 访问应用程序。在隐私、法律或规制不需要设备管理而仅需要企业应用程序管理的环境中，请考虑将 **wsapi.mdm.required.flag** 设置为 **false**。

使用 XenMobile 未托管的设备的用户可以通过 XenMobile Store 安装应用程序。您可以通过应用程序策略控制对应用程序的访问，而不是通过设备级别控制，如选择性擦除或完全擦除。根据您设置的值，策略需要设备定期检查 XenMobile Server 以确认仍允许运行应用程序。

安全要求

部署 XenMobile 环境时的安全注意事项数量很快会变得难以应对。有许多连锁件和设置。为了帮助您入门并选择可接受的保护级别，Citrix 提供了高安全性、更高安全性和最高安全性的建议，如下表中所述。

您的部署模式选择不仅涉及安全问题。此外，务必要查看用例的要求，并确定是否可以在选择部署模式之前缓解安全问题。

高：使用这些设置可提供最佳的用户体验，同时保持大多数组织可接受的基本安全级别。

较高：这些设置在安全性和可用性之间建立更加稳健的权衡。

最高：遵循这些建议，安全级别非常高，但可用性和用户采用率会降低。

部署模式安全注意事项

下表列出了实现每种安全级别的部署模式。

高安全性	更高的安全性	最高安全性
MAM 或 MDM	MDM+MAM	MDM+MAM；以及 FIPS

备注：

- 根据用例，仅 MDM 部署或仅 MAM 部署可以满足安全要求，并提供良好的用户体验。
- 如果您不需要应用程序容器化、Micro VPN 或应用程序特定的策略，MDM 就足以管理和保护设备。
- 对单独执行应用程序容器化即可满足所有业务和安全要求的用例（例如 BYOD），Citrix 建议采用仅 MAM 模式。
- 对于高安全性环境（和公司发放的设备），Citrix 建议采用 MDM+MAM 以充分利用可用的所有安全功能。请确保强制执行 MDM 注册。
- FIPS 选项适用于具有最高安全性需求的环境，例如联邦政府。

如果启用 FIPS 模式，则必须配置 SQL Server 以加密 SQL 流量。

Citrix ADC 和 **Citrix Gateway** 安全注意事项

下表列出了针对每种安全级别的 Citrix ADC 和 Citrix Gateway 建议。

高安全性	更高的安全性	最高安全性
推荐使用 Citrix ADC。MAM 和 ENT 需要使用 Citrix Gateway；对于 MDM，建议使用	如果 XenMobile 位于 DMZ 中，则使用带 SSL 桥接的标准 Citrix ADC for XenMobile 向导配置。或者，如果 XenMobile Server 位于内部网络中时，如有必要，则使用 SSL 卸载以满足安全标准。	SSL 卸载与端到端加密

备注：

- 通过 NAT 或现有的第三方代理和负载平衡器将 XenMobile Server 公开给 Internet 可能是 MDM 的一个选项。但是，该设置要求 SSL 流量在 XenMobile Server 上终止，这会带来潜在的安全风险。
- 对于高安全性环境，采用默认 XenMobile 配置的 Citrix ADC 通常可以满足或超过安全要求。
- 对于具有最高安全性需求的 MDM 环境，Citrix ADC 上的 SSL 终止支持在外围执行流量检查，并维护端到端 SSL 加密。

- 用于定义 SSL/TLS 密码的选项。
- 此外，还提供 SSL FIPS Citrix ADC 硬件。
- 有关详细信息，请参阅与 Citrix Gateway 和 Citrix ADC 集成。

注册安全注意事项

下表列出了针对每种安全级别的 Citrix ADC 和 Citrix Gateway 建议。

高安全性	更高的安全性	最高安全性
仅限 Active Directory 组成员身份。禁用“所有用户”交付组。	仅限邀请的注册安全模式。仅限 Active Directory 组成员身份。禁用“所有用户”交付组	注册安全模式关联到设备 ID。仅限 Active Directory 组成员身份。禁用“所有用户”交付组

备注：

- Citrix 通常建议只允许预定义的 Active Directory 组中的用户进行注册。该设置需要禁用内置的“所有用户”交付组。
- 您可以使用注册邀请来限制收到邀请的用户才可以注册。注册邀请不适用于 Windows 设备。
- 您可以使用一次性 PIN (OTP) 注册邀请作为双重身份验证解决方案以及控制用户可以注册的设备数。OTP 邀请不适用于 Windows 设备。

设备通行码安全注意事项

下表列出了针对每种安全级别的设备通行码建议。

高安全性	更高的安全性	最高安全性
推荐。设备级别加密要求高安全性。通过使用 MDM 强制执行。通过使用 MDX 策略“不合规设备行为”，您可以根据需要为仅 MAM 设置高安全性。	通过使用 MDM、MDX 策略或两者强制执行。	通过使用 MDM 和 MDX 策略强制要求。MDM 复杂通行码策略。

备注：

- Citrix 建议使用设备通行码。
- 可以通过 MDM 策略强制要求输入设备通行码。

- 可以通过 MDX 策略要求在使用托管应用程序时输入设备通行码。例如，对于 BYOD 用例。
- Citrix 建议组合使用 MDM 和 MDX 策略选项来提高 MDM+MAM 环境的安全性。
- 对于具有最高安全性要求的环境，可以配置复杂通行码策略，并通过 MDM 强制实施这些策略。您可以配置自动操作，以便在设备不符合通行码策略时通知管理员或执行选择性设备擦除/完全设备擦除。

应用程序

January 5, 2022

企业移动性管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 让组织能够保护和控制移动设备，而 MAM 有助于应用程序交付和管理。为支持 BYOD 采用，您通常可以实施 MAM 解决方案（例如 XenMobile），以帮助执行以下操作：

- 应用程序交付
- 软件授权
- configuration
- 应用程序生命周期管理

可以要求或允许用户同时选择进行 MDM 管理。

通过 XenMobile，您可以配置特定的 MAM 策略和 VPN 设置以防止数据泄漏和其他安全威胁，进一步保护这些应用程序的安全。XenMobile 为组织提供了部署其解决方案的灵活性，作为：

- 仅 MAM 环境
- 仅 MDM 环境
- 同时提供 MDM 和 MAM 功能的统一 XenMobile Enterprise 环境

除了能够将应用程序交付到移动设备外，XenMobile 还通过 MDX 技术提供应用程序容器化。这些应用程序受基于策略的精细控制。独立软件供应商 (ISV) 可以使用移动应用程序 SDK 应用这些控制。

在企业环境中，用户使用各种各样的移动应用程序来协助完成自己的工作职责。这些应用程序可能包括公共应用商店中的应用程序、内部开发的应用程序或本机应用程序。XenMobile 按如下所示对这些应用程序进行分类：

- 公共应用商店：这些应用程序包括公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。组织外的供应商通常在公共应用商店中提供其应用程序。这种方式让其客户可以直接从 Internet 下载应用程序。根据用户的需求，您可以在组织中使用很多公共应用程序。例如，GoToMeeting、Salesforce 和 EpicCare 应用程序属于此类应用程序。
  - 如果使用 **MAM SDK**：请从应用程序供应商处获取应用程序二进制文件。然后，将 MAM SDK 集成到应用程序中。
  - 如果您使用 **MDX Toolkit**：Citrix 不支持直接从公共应用商店下载应用程序二进制文件，然后使用 MDX Toolkit 将其打包以进行企业分发。要打包第三方应用程序，请与您的应用程序供应商合作以获取应用程序二进制文件。然后，您可以使用 MDX Toolkit 打包二进制文件。

- 内部应用程序：许多组织都有内部开发人员，他们创建提供特定功能并在组织内独立开发和分发的应用程序。在某些情况下，一些组织可能还有 ISV 提供的应用程序。您可以将此类应用程序作为本机应用程序进行部署，也可以通过使用 MAM 解决方案（例如 XenMobile）容器化这些应用程序。

  例如，某医疗机构可能会创建一个内部应用程序，以允许医师在移动设备上查看患者信息。然后，组织可以使用以下方法之一来保护患者信息的安全并启用对患者数据库的 VPN 访问：

  - MAM SDK
  - MDX Toolkit

- **Web** 和 **SaaS** 应用程序：这些应用程序包括通过内部网络访问的应用程序（Web 应用程序）或通过公用网络访问的应用程序 (SaaS)。XenMobile 还允许您使用一组应用程序连接器创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器便于对现有 Web 应用程序进行单点登录 (SSO)。有关详细信息，请参阅应用程序连接器类型。例如，您可以使用基于安全声明标记语言 (SAML) 的 Google Apps SAML for SSO 登录 Google Apps。

- 移动生产力应用程序：移动生产力应用程序是 Citrix 开发且在 XenMobile 许可证中附带的应用程序。有关详细信息，请参阅关于移动生产力应用程序。Citrix 还提供 ISV 使用移动应用程序 SDK 开发的其他业务就绪型应用程序。

- **HDX** 应用程序： HDX 应用程序是您通过 StoreFront 发布且由 Windows 托管的应用程序。如果使用 Citrix Virtual Apps and Desktops 以及 Citrix Workspace，HDX 应用程序可供已注册的用户使用。

根据您计划通过 XenMobile 部署和管理的移动应用程序的类型，基础配置可能会有所差别。例如，具有不同权限级别的多组用户可能会使用某一个应用程序。在这种情况下，您可能必须创建独立的交付组以部署同一应用程序的两个独立版本。此外，您还必须确保用户组成员身份相互排斥，以避免在用户设备上发生策略不匹配。

还可以使用 Apple 批量购买管理 iOS 应用程序许可。此选项要求您注册批量购买计划并在 XenMobile 控制台中配置批量购买设置。该配置允许您使用批量购买许可证分发应用程序。鉴于各种用例，在实施 XenMobile 环境之前请务必评估和规划您的 MAM 策略。规划您的 MAM 策略时，您可以先明确以下各项：

- 应用程序类型 - 列出您计划支持的不同应用程序类型，并对其进行分类，例如，公共、本机、Web、内部或 ISV 应用程序。此外，还按不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。此分类将有助于调整每种类型的应用程序所需的各种 XenMobile 设置。例如，一些应用程序可能需要使用移动应用程序 SDK 来启用特殊 API 才能与其他应用程序交互。

- 网络要求：配置具有特定网络访问要求的应用程序的设置。例如，某些应用程序可能需要通过 VPN 访问您的内部网络。某些应用程序可能需要 Internet 访问权限才能通过 DMZ 对访问进行路由。为了允许此类应用程序连接到所需网络，必须相应地配置各种设置。明确每个应用程序网络要求有助于在早期做出您的体系结构决策，这将简化整体实施流程。

- 安全要求：可以定义应用到单个应用程序或所有应用程序的安全要求。

  - MDX 策略等设置适用于单个应用程序
  - 会话和身份验证设置适用于所有应用程序
  - 某些应用程序可能具有特定的容器化、MDX、身份验证、地理围栏、通行码或数据共享要求。

  请提前概述这些要求，以简化部署。有关 Endpoint Management 中的安全性的详细信息，请参阅安全性和用户体验。

- 部署要求 - 您可能希望使用基于策略的部署以仅允许合规用户下载已发布的应用程序。例如，某些应用程序可能会要求设备处于托管状态，或者设备满足最低操作系统版本要求。您可能还希望某些应用程序仅提供给企业用户。请提前列出此类要求，以便您可以配置适当的部署规则或操作。
- 许可要求：保留应用程序相关的许可要求的记录。您的笔记可以帮助您有效地管理许可证使用情况，以及决定是否在 XenMobile 中配置特定功能以便于进行许可。例如，如果部署免费或付费 iOS 应用程序，Apple 会强制执行应用程序的许可要求。因此，用户必须登录其 Apple App Store 帐户。

  但是，您可以注册加入 Apple 批量购买计划，以通过 XenMobile 分发和管理这些应用程序。批量购买允许用户无需登录其 Apple App Store 帐户即可下载应用程序。

  某些平台（例如 Samsung SAFE 和 Samsung Knox）有需要在部署这些功能之前完成的特殊许可要求。
- 允许列表和阻止列表要求：您可以确定不希望用户安装或使用的应用程序。创建阻止列表将定义不合规事件。然后，您可以设置策略，以便在事件发生时触发。另一方面，某个应用程序可能可以使用，但会出于某个原因而被列入阻止列表。在这种情况，可以将该应用程序添加到允许列表中，并指出该应用程序是可以使用的但不是必需的。此外，请谨记，预先安装在新设备上的应用程序可能包括一些不属于操作系统的常用应用程序。此类应用程序可能会与您的阻止列表策略发生冲突。

用例

某医疗机构计划部署 XenMobile 以用作其移动应用程序的 MAM 解决方案。移动应用程序将交付给公司和自带设备用户。IT 决定交付和管理以下应用程序：

移动生产力应用程序：由 Citrix 提供的 iOS 和 Android 应用程序。有关详细信息，请参阅移动生产力应用程序。

Citrix Secure Hub：所有移动设备用来与 XenMobile 通信的客户端。可以使用 Secure Hub 将安全设置、配置和移动应用程序推送到移动设备。Android 和 iOS 设备通过 Secure Hub 在 XenMobile 中注册。

Citrix Receiver：允许移动设备用户打开 Citrix Virtual Apps 托管的应用程序的移动应用程序。

GoToMeeting：在线会议、桌面共享和视频会议客户端，让用户可以通过 Internet 实时与其他计算机用户、客户、客户端或同事联系。

Salesforce1： Salesforce1 允许用户从移动设备访问 Salesforce，并将所有 Chatter、CRM、自定义应用程序和业务流程集中在一起，以使 Salesforce 任何用户拥有统一的体验。

RSA SecurID：用于双重身份验证的基于软件的令牌。

EpicCare 应用程序：这些应用程序让医疗工作人员可以安全便携地访问患者图表、患者列表、计划和消息。

Haiku：适用于 iPhone 和 Android 手机的移动应用程序。

Canto：适用于 iPad 的移动应用程序

Rover：适用于 iPhone 和 iPad 的移动应用程序。

HDX： Citrix Virtual Apps 提供 HDX 应用程序。

- **Epic Hyperspace**：用于电子病历管理的 Epic 客户端应用程序。

ISV:

- **Vocera**： HIPAA 合规 VoIP 和消息传送移动应用程序，通过 iPhone 和 Android 智能手机随时随地扩展 Vocera 语音技术的优势。

内部应用程序：

- **HCMail**：该应用程序用于撰写加密邮件、在内部邮件服务器上搜索通讯簿以及使用电子邮件客户端将加密邮件发送给联系人。

内部 **Web** 应用程序：

- **PatientRounding**：该 Web 应用程序用于按不同的部门记录患者健康信息。
- **Outlook Web Access**：允许通过 Web 浏览器访问电子邮件。
- **SharePoint**：用于组织范围的文件和数据共享。

下表列出了 MAM 配置所需的基本信息。

应用程序名称	应用程序类型	**MAM SDK** 集成或 **MDX** 封装	**iOS**	**Android**
Secure Mail	XenMobile App	版本 10.4.1 及更高版本不使用	是	是
Secure Web	XenMobile App	版本 10.4.1 及更高版本不使用	是	是
Citrix Files	XenMobile App	版本 10.4.1 及更高版本不使用	是	是
Secure Hub	公共应用程序	不适用	是	是
Citrix Receiver	公共应用程序	不适用	是	是
GoToMeeting	公共应用程序	不适用	是	是
Salesforce1	公共应用程序	不适用	是	是
RSA SecurID	公共应用程序	不适用	是	是
Epic Haiku	公共应用程序	不适用	是	是
Epic Canto	公共应用程序	不适用	是	否
Epic Rover	公共应用程序	不适用	是	否
Epic Hyperspace	HDX 应用程序	不适用	是	是
Vocera	ISV 应用程序	是	是	是
HCMail	内部应用程序	是	是	是
PatientRounding	Web 应用程序	不适用	是	是

Outlook Web Access	Web 应用程序	不适用	是	是
SharePoint	Web 应用程序	不适用	是	是

下表列出了您在 XenMobile 中配置 MAM 策略时可以查询的特定要求。

应用程序名称	需要 **VPN**	（与容器外部的应用程序）交互	（从容器外部的应用程序）交互	代理过滤	许可	地理围栏	移动应用程序 **SDK**	最低操作系统版本
Secure Mail	Y	选择性允许	允许	必需	不适用	选择性必需	不适用	强制执行
Secure Web	Y	允许	允许	必需	不适用	不需要	不适用	强制执行
Citrix Files	Y	允许	允许	必需	不适用	不需要	不适用	强制执行
Secure Hub	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Citrix Re-ceiver	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
GoToMeeting	N	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Salesforc	N	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
RSA SecurID	N	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Epic Haiku	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Epic Canto	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行
Epic Rover	Y	不适用	不适用	不需要	批量购买	不需要	不适用	不强制执行

应用程序名称	需要 **VPN**	（与容器外部的应用程序）交互	（从容器外部的应用程序）交互	代理过滤	许可	地理围栏	移动应用程序 **SDK**	最低操作系统版本
Epic Hyper-space	Y	不适用	不适用	不需要	不适用	不需要	不适用	不强制执行
Vocera	Y	已阻止	已阻止	必需	不适用	必需	必需	强制执行
HCMail	Y	已阻止	已阻止	必需	不适用	必需	必需	强制执行
PatientRc ing	Y	不适用	不适用	必需	不适用	不需要	不适用	不强制执行
Outlook Web Access	Y	不适用	不适用	必需	不适用	不需要	不适用	不强制执行
SharePoi	Y	不适用	不适用	必需	不适用	不需要	不适用	不强制执行

用户社区

January 5, 2022

每个组织都由多个以不同的功能角色运作的用户社区组成。这些用户社区使用您通过用户移动设备提供的各种资源执行不同的任务和办公功能。用户可能会使用您提供的移动设备在家中或远程办公室工作。或者，用户可能会使用私人移动设备，这允许其访问遵从某些安全合规规则的工具。

如果存在多个使用移动设备的用户社区，企业移动性管理 (EMM) 将对防止数据泄漏以及强制遵守组织层面的安全限制至关重要。为了实现高效率以及更加复杂的移动设备管理，您可以对用户社区进行分类。这样可以简化将用户映射到资源的过程，并确保正确的安全策略应用到正确的用户。

将用户社区分类可以包括使用以下组件：

- Active Directory 组织单位 (OU) 和组

  添加到特定 Active Directory 安全组的用户可以接收策略以及应用程序等资源。将用户从 Active Directory 安全组中删除将删除对以前允许访问的 XenMobile 资源的访问权限。

- XenMobile 本地用户和组

  对于在 Active Directory 中没有帐户的用户，可以将用户创建为本地 XenMobile 用户。可以通过与 Active Directory 用户相同的方式将本地用户添加到交付组中并为其预配资源。

- XenMobile 交付组

  如果多组具有不同权限级别的用户要占用一个应用程序，您可能需要创建独立的交付组。创建独立的交付组后，可以部署同一应用程序的两个独立版本。

- 交付组和用户组映射

  交付组到 Active Directory 组的映射可以是一对一映射，也可以是一对多映射。将基础策略和应用程序分配给一个一对多交付组映射。将功能特定的策略和应用程序分配给多个一对一交付组映射。

- 应用程序的交付组和资源映射

  将特定的应用程序分配给每个交付组。

- MDM 资源的交付组和资源映射

  将应用程序和特定的设备管理资源分配给每个交付组。例如，为一个交付组配置以下各项的任意组合：应用程序类型（公共应用程序、HDX 应用程序等）、每种应用程序类型的特定应用程序以及设备策略和自动化操作等资源。

以下示例说明了如何对医疗机构的用户社区进行分类以实现 EMM。

用例

本示例医疗机构提供技术资源以及向多个用户提供访问权限，包括网络和附属机构员工和志愿者。此机构已选择仅向非执行用户推出 EMM 解决方案。

您可以将此机构的用户角色和功能划分为几个子组，包括：临床、非临床和合同工。选定的一组用户将收到企业移动设备，而其他用户可以从其私人设备 (BYOD) 访问有限的公司资源。要强制执行恰当的安全限制级别以及防止数据泄漏，此机构决定企业 IT 负责管理注册的每个设备。此外，用户只能注册一个设备。

以下各节概述了每个子组的角色和功能：

临床

- 护士
- 医师（医生、外科医生等）
- 专家（营养学家、验血师、麻醉师、放射科医师、心脏病专家、肿瘤学家等）
- 外部医师（从远程办公室工作的非雇员医师和办公室工作人员）
- 家庭医疗服务（执行患者家访的医师服务的办公室和移动工作人员）
- 研究专家（在六家研究机构执行临床研究以寻找医学问题答案的知识型工作者和高级用户）
- 教育和培训（护士、医师以及教育和培训专家）

非临床

- 共享服务（执行各种后勤功能的办公室工作人员，包括：HR、工资单、应付账款、供应链服务等）

- 医师服务（执行各种医疗保健管理、管理服务以及针对提供商的业务流程解决方案的办公室工作人员，包括：管理服务、分析和业务智能、业务系统、客户服务、财务、托管式医疗管理、患者访问解决方案、收支周期解决方案等）
- 支持服务（执行各种非临床功能的办公室工作人员，包括：收益管理、临床整合、沟通、薪酬与绩效管理、设施和物业服务、HR 技术系统、信息服务、内部审计和流程改进等）
- 慈善活动（执行支持慈善活动的各项功能的办公室和移动工作人员）

合同工

- 制造商和供应商合作伙伴（通过站点到站点 VPN 现场连接和远程连接，提供各种非临床支持功能）

根据上述信息，此机构创建了以下实体。有关 XenMobile 中的交付组的详细信息，请参阅 XenMobile 产品文档中的部署资源。

Active Directory 组织单位 **(OU)** 和组

针对 **OU =** XenMobile 资源

- OU = 临床；组 =
  - XM-护士
  - XM-医师
  - XM-专家
  - XM-外部医师
  - XM-家庭医疗服务
  - XM-研究专家
  - XM-教育和培训
- OU = 非临床；组 =
  - XM-共享服务
  - XM-医师服务
  - XM-支持服务
  - XM-慈善活动

XenMobile 本地用户和组

针对组 = 合同工，用户 =

- 供应商 1
- 供应商 2
- 供应商 3
- … 供应商 10

XenMobile 交付组

- 临床-护士
- 临床-医师
- 临床-专家
- 临床-外部医师
- 临床-家庭医疗服务
- 临床-研究专家
- 临床-教育和培训
- 非临床-共享服务
- 非临床-医师服务
- 非临床-支持服务
- 非临床-慈善活动

交付组和用户组映射

Active Directory 组	**XenMobile** 交付组
XM-护士	临床-护士
XM-医师	临床-医师
XM-专家	临床-专家
XM-外部医师	临床-外部医师
XM-家庭医疗服务	临床-家庭医疗服务
XM-研究专家	临床-研究专家
XM-教育和培训	临床-教育和培训
XM-共享服务	非临床-共享服务
XM-医师服务	非临床-医师服务
XM-支持服务	非临床-支持服务
XM-慈善活动	非临床-慈善活动

应用程序的交付组和资源映射

	Secure Mail	Secure Web	ShareFil	Receiver	Salesfor	RSA Se-curID	EpicCare Haiku	Epic Hyper-space
临床-护士	X	X	X					
临床-医师								
临床-专家								
临床-外部医师	X		X					
临床-家庭医疗服务	X		X					
临床-研究专家	X		X					
临床-教育和培训							X	X
非临床-共享服务							X	X
非临床-医师服务							X	X
非临床-支持服务	X		X				X	X
非临床-慈善活动	X		X				X	X
合同工	X		X	X	X		X	X

MDM 资源的交付组和资源映射

	MDM：通行码策略	**MDM**：设备限制	**MDM**：自动化操作	**MDM**：**WiFi** 策略
临床-护士				X
临床-医师		X		
临床-专家				
临床-外部医师				
临床-家庭医疗服务				
临床-研究专家				
临床-教育和培训				
非临床-共享服务				
非临床-医师服务				
非临床-支持服务				
非临床-慈善活动				
合同工				X

备注和注意事项

- XenMobile 在初始配置过程中创建名为“所有用户”的默认交付组。如果不禁用此交付组，所有 Active Directory 用户都将具有在 XenMobile 中注册的权限。
- XenMobile 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果某个用户所属的组未在 XenMobile 中映射，该用户将无法注册。同样，如果某个用户属于多个组的成员，XenMobile 将仅对在映射到 XenMobile 的组中的用户进行分类。
- 要强制进行 MDM 注册，请在 XenMobile 控制台的服务器属性中将需要注册选项设置为真。有关详细信息，请参阅服务器属性。
- 要从 XenMobile 交付组中删除用户组，请删除 SQL Server 数据库中 dbo.userlistgrps 下的条目。

  > 小心：
  >
  > 执行此操作之前，请创建 XenMobile 和数据库的备份。

关于 **XenMobile** 中的设备所有权

可以根据用户设备的所有者对用户进行分组。设备所有权包括公司拥有的设备和用户拥有的设备（也称为自带设备 (BYOD)）。您可以在 XenMobile 控制台中的两个位置控制 BYOD 设备连接到您网络的方式：在“部署规则”中以及通

过设置页面上的 XenMobile Server 属性。有关部署规则的详细信息，请参阅 XenMobile 文档中的部署资源。有关服务器属性的详细信息，请参阅本手册中的服务器属性。

通过设置服务器属性，您可以要求所有 BYOD 用户在接受公司对其设备的管理后才能访问应用程序。或者，也可以在不管理用户设备的情况下直接允许其访问公司应用程序。

将服务器属性 **wsapi.mdm.required.flag** 设置为 **true** 时，XenMobile 将托管所有 BYOD 设备，并且任何拒绝注册的用户都将无法访问应用程序。在企业 IT 团队在注册过程中需要高安全性和积极用户体验的环境中，请考虑将 **wsapi.mdm.required.flag** 设置为 **true**。

如果 **wsapi.mdm.required.flag** 保留为 **false**（默认设置），用户可以拒绝注册。但是，用户可以通过 XenMobile Store 访问其设备上的应用程序。在隐私、法律或规制不需要设备管理而仅需要企业应用程序管理的环境中，请考虑将 **wsapi.mdm.required.flag** 设置为 **false**。

使用 XenMobile 未托管的设备的用户可以通过 XenMobile Store 安装应用程序。您可以通过应用程序策略控制对应用程序的访问，而不是通过设备级别控制，如选择性擦除或完全擦除。某些策略设置需要设备定期检查 XenMobile Server 以确认仍允许运行应用程序。

电子邮件策略

January 21, 2021

从移动设备安全访问电子邮件是任何组织的移动性管理计划的其中一个主要的驱动因素。确定正确的电子邮件策略是任何 XenMobile 设计的一个关键组成部分。XenMobile 根据安全性、用户体验和集成要求提供多种选项以适应不同的用例。本文介绍了选择正确的解决方案（从选择客户端到邮件通信流）的典型设计决策过程和注意事项。

选择电子邮件客户端

对整体电子邮件策略设计而言，客户端选择通常排在第一位。可以从多个客户端中进行选择：Citrix Secure Mail、特定移动平台操作系统中随附的本机邮件或者通过公共应用商店提供的其他第三方客户端。可以支持使用单个（标准）客户端的用户社区，也可能需要使用客户端的组合，具体取决于您的需求。

下表概述了可用的不同客户端选项的一些设计注意事项：

主题	**Secure Mail**	本机（例如 **iOS Mail**）	第三方邮件
最低 XenMobile 版本	Advanced	MDM	MDM

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：SAFE/KNOX 和 Android Enterprise。所有其他客户端都被视为第三方客户端。	通常需要用户手动配置。
安全性	Secure by Design，提供最高安全性。使用数据加密级别增加的 MDX 策略。Secure Mail 是通过 MDX 策略完全托管的应用程序。增加了通过 Citrix PIN 进行的身份验证层。	取决于供应商/应用程序功能集。提供较高的安全性。使用设备加密设置（不通过 MDX 策略配置安全性）。依靠设备级别的身份验证来访问应用程序。	取决于供应商/应用程序功能集。提供高安全性。
集成	默认情况下，允许与托管 (MDX) 应用程序进行交互。通过 Citrix Secure Web 打开 Web URL。将文件保存到 Citrix Files 以及从 Citrix Files 附加文件。直接加入和拨入 GoToMeeting。	默认情况下，只能与其他未托管（非 MDX）应用程序交互。	默认情况下，只能与其他未托管（非 MDX）应用程序交互。
部署/许可	可以通过 MDM 直接从公共应用商店推送 Secure Mail。随附在 XenMobile Advanced 和 Enterprise 许可中。	平台操作系统中随附的客户端应用程序。无额外的许可要求。	可以通过 MDM 作为企业应用程序推送或者直接从公共应用商店推送。基于应用程序供应商的关联许可模式/成本。
支持	客户端和 EMM 解决方案 (Citrix) 的单供应商支持。Secure Hub/应用程序调试日志记录功能中嵌入了支持联系人信息。可支持一个客户端。	供应商定义的支持 (Apple/Google)。可能需要支持多个客户端，具体取决于设备平台。	供应商定义的支持。可支持一个客户端，前提是第三方客户端在所有托管设备平台上都受支持。

邮件通信流和过滤注意事项

本节探讨与 XenMobile 环境中的邮件 (ActiveSync) 通信流有关的三种主要方案和设计注意事项。

方案 **1**：公开的 **Exchange**

支持外部客户端的环境通常具有面向 Internet 公开的 Exchange ActiveSync 服务。移动 ActiveSync 客户端通过这一面向外部的路径借助反向代理（例如 Citrix ADC）或边缘服务器进行连接。此方案需要使用本机或第三方邮件客户端，使得这些客户端成为此方案的普遍选择。还可以在此方案中使用 Secure Mail 客户端，尽管这并不是常见的做法。这样，您将从使用 MDX 策略和管理应用程序提供的安全功能中获益。

方案 **2**：借助 **Citrix ADC**（**Micro VPN** 和 **STA**）通过通道传输

由于其 Micro VPN 功能，此方案是使用 Secure Mail 客户端时的默认方案。在这种情况下，Secure Mail 客户端将通过 Citrix Gateway 与 ActiveSync 建立安全连接。实际上，可以考虑使用 Secure Mail 作为从内部网络直接连接到 ActiveSync 的客户端。Citrix 客户通常会作为所选的移动 ActiveSync 客户端对 Secure Mail 进行规范。该决策属于避免在公开的 Exchange Server 上面向 Internet 公开 ActiveSync 服务的措施的一部分，如第一种方案中所述。

只有启用了 MAM SDK 或 MDX 封装的应用程序才能使用 Micro VPN 功能。如果您使用 MDX 封装，此方案不适用于本机客户端。即使可以通过 MDX Toolkit 打包第三方客户端，这种做法也不常见。使用设备级别的 VPN 客户端以允许本机或第三方客户端通过通道进行访问已证实非常麻烦，不是可行的解决方案

方案 **3**：云托管的 **Exchange** 服务

云托管的 Exchange 服务（例如 Microsoft Office 365）变得更受欢迎。在 XenMobile 环境中，此方案可能将与第一种方案同等对待，因为 ActiveSync 服务也对 Internet 公开。在这种情况下，云服务提供商要求会规定客户端选项。这些选项通常包括支持大多数 ActiveSync 客户端，例如 Secure Mail 以及其他本机或第三方客户端。

对此方案而言，XenMobile 可以在三个方面增加价值：

- 使用 MDX 策略的客户端以及通过 Secure Mail 进行的应用程序管理
- 在受支持的本机电子邮件客户端上使用 MDM 策略配置客户端
- 使用适用于 Exchange ActiveSync 的 Endpoint Management 连接器时的 ActiveSync 过滤选项

邮件流过滤注意事项

与面向 Internet 公开的大多数服务一样，必须确保路径安全并提供过滤功能以进行授权访问。XenMobile 解决方案包括两个设计为专用于为本机和第三方客户端提供 ActiveSync 过滤功能的组件：适用于 Exchange ActiveSync 的 Citrix Gateway 连机器和适用于 Exchange ActiveSync 的 Endpoint Management 连接器。

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

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器使用 Citrix ADC 作为 ActiveSync 流量的代理，在外围提供 ActiveSync 过滤功能。因此，过滤组件位于邮件通信流的路径中，在邮件进入或离开环境时截获邮件。适用于 Exchange ActiveSync 的 Citrix Gateway 连接器将用作 Citrix ADC 和 XenMobile Server 之间的中介。当某个设备通过 Citrix ADC 上的 ActiveSync 虚拟服务器与 Exchange 通信时，Citrix ADC 将对适用于 Exchange ActiveSync 的连接器服务执行 HTTP 标注。该服务随后将通过 XenMobile 检查设备状态。根据该设备的状态，适用于 Exchange ActiveSync 的连接器会答复 Citrix ADC，指示允许或拒绝连接。您可能还会配置静态规则以根据用户、代理和设备类型或 ID 过滤访问。

此设置允许在增加了安全层的情况下面向 Internet 公开 Exchange ActiveSync 服务，以阻止未经授权的访问。设计注意事项包括以下各项：

- Windows Server：适用于 Exchange ActiveSync 的连接器组件需要 Windows Server。
- 过滤规则集：适用于 Exchange ActiveSync 的连接器旨在根据设备状态和信息而非用户信息进行过滤。尽管您可以将静态规则配置为按用户 ID 进行过滤，但不存在根据（例如）Active Directory 组成员身份进行过滤的选项。如果对 Active Directory 组过滤存在要求，可以改为使用适用于 Exchange ActiveSync 的 Endpoint Management 连接器。
- Citrix ADC 可扩展性：考虑到通过 Citrix ADC 代理 ActiveSync 流量的要求：恰当的 Citrix ADC 实例规模对支持增加的所有 ActiveSync SSL 连接的工作负载至关重要。
- Citrix ADC 集成缓存：Citrix ADC 上的适用于 Exchange ActiveSync 的连接器配置使用集成缓存功能来缓存来自适用于 Exchange ActiveSync 的连接器的响应。该配置的结果是，Citrix ADC 不需要为给定会话中的每个 ActiveSync 事务向适用于 Exchange ActiveSync 的 Citrix Gateway 连接器发出请求。该配置对实现足够的性能和规模而言也非常重要。集成缓存在 Citrix ADC Platinum Edition 中提供，或者可以单独授权 Enterprise Edition 使用该功能。
- 自定义过滤策略：您可能需要创建自定义 Citrix ADC 策略以限制标准本地移动客户端外部的某些 ActiveSync 客户端。此配置要求用户了解 ActiveSync HTTP 请求和 Citrix ADC 响应程序策略创建。
- Secure Mail 客户端：Secure Mail 没有 Micro VPN 功能（使用该功能将不再需要在外围进行过滤）。通过 Citrix Gateway 进行连接时，Secure Mail 客户端通常会被视为内部（可信）ActiveSync 客户端。如果同时支持本机和第三方客户端（通过适用于 Exchange ActiveSync 的连接器）且需要 Secure Mail 客户端，Citrix 建议不要通过用于适用于 Exchange ActiveSync 的连接器的 Citrix ADC 虚拟服务器传输 Secure Mail 流量。可以通过 DNS 实现此通信流，并保持适用于 Exchange ActiveSync 的连接器策略不影响 Secure Mail 客户端。

有关 XenMobile 部署中适用于 Exchange ActiveSync 的 Citrix Gateway 连接器的示意图，请参阅面向本地部署的参考体系结构。

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

适用于 Exchange ActiveSync 的 Endpoint Management 连接器是一个 XenMobile 组件，在 Exchange 服务级别提供 ActiveSync 过滤功能。因此，过滤仅在邮件抵达 Exchange 服务时发生，而不是在其进入 XenMobile 环境时发生。Mail Manager 使用 PowerShell 查询 Exchange ActiveSync 中的设备合作关系信息，并通过设备隔离操作

来控制访问。这些操作可根据适用于 Exchange ActiveSync 的 Endpoint Management 连接器的规则条件隔离和取消隔离设备。与适用于 Exchange ActiveSync 的 Citrix Gateway 连接器类似，适用于 Exchange ActiveSync 的 Endpoint Management 连接器可通过 XenMobile 检查设备状态以基于设备合规性过滤访问权限。您可能还会配置静态规则以根据设备类型或 ID、代理版本和 Active Directory 组成员身份来过滤访问。

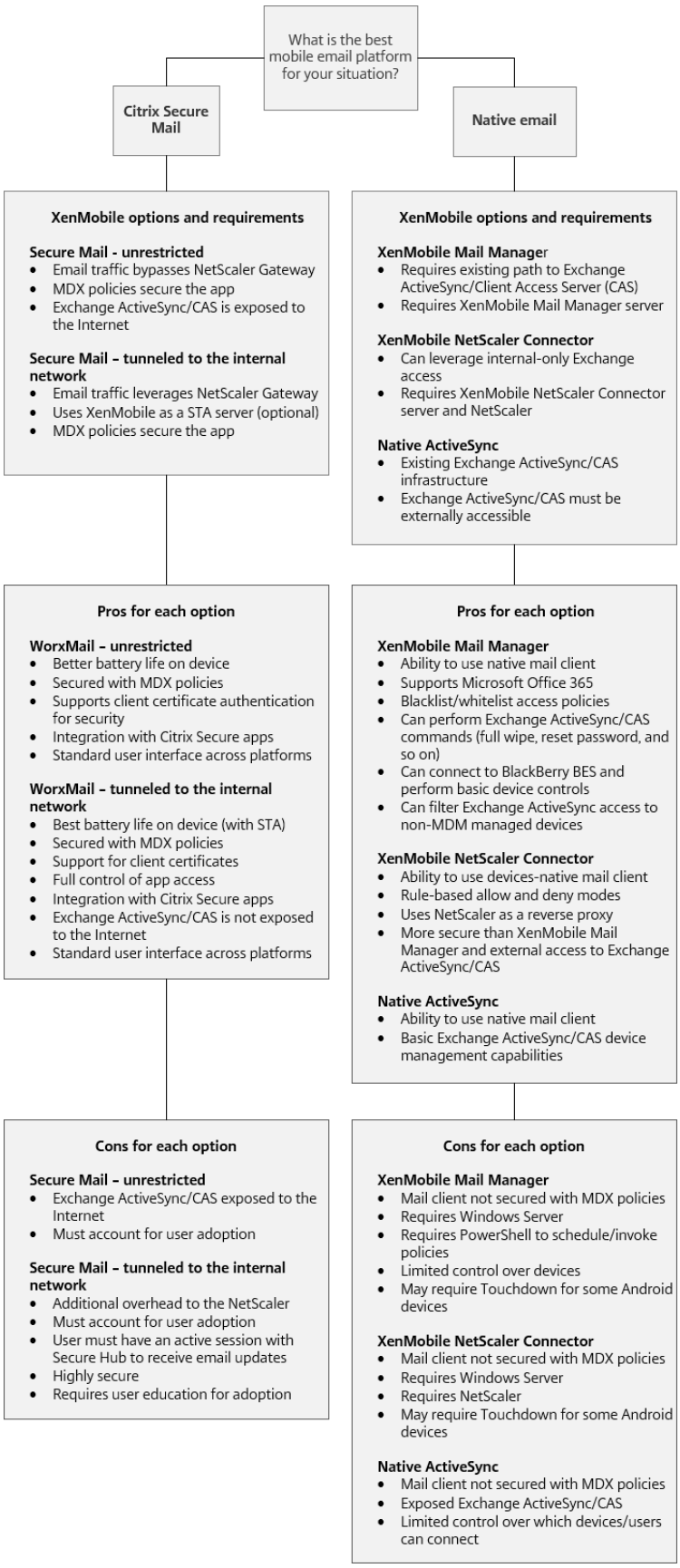
此解决方案不需要使用 Citrix ADC。您无需更改现有 ActiveSync 流量的传输方式，即可部署适用于 Exchange ActiveSync 的 Endpoint Management 连接器。设计注意事项包括：

- Windows Server：适用于 Exchange ActiveSync 的 Endpoint Management 连接器组件需要您部署 Windows Server。
- 过滤规则集：与适用于 Exchange ActiveSync 的 Citrix Gateway 连接器一样，适用于 Exchange ActiveSync 的 Endpoint Management 连接器包含用于评估设备状态的过滤规则。此外，适用于 Exchange ActiveSync 的 Endpoint Management 连接器还支持静态规则以根据 Active Directory 组成员身份进行过滤。
- Exchange 集成：适用于 Exchange ActiveSync 的 Endpoint Management 连接器要求直接访问托管 ActiveSync 角色的 Exchange 客户端访问服务器 (CAS) 以及控制设备隔离操作。此要求可能会提出挑战，具体取决于环境体系结构和安全态势。提前评估此技术要求至关重要。
- 其他 ActiveSync 客户端：由于适用于 Exchange ActiveSync 的 Endpoint Management 连接器在 ActiveSync 服务级别进行过滤，因此，请考虑 XenMobile 环境外部的其他 ActiveSync 客户端。可以配置适用于 Exchange ActiveSync 的 Endpoint Management 连接器静态规则以避免对其他 ActiveSync 客户端产生非预期的影响。
- 扩展的 Exchange 功能：通过与 Exchange ActiveSync 直接集成，适用于 Exchange ActiveSync 的 Endpoint Management 连接器将为 XenMobile 提供在移动设备上执行 Exchange ActiveSync 擦除的功能。适用于 Exchange ActiveSync 的 Endpoint Management 连接器还允许 XenMobile 访问与黑莓设备有关的信息以及执行其他控制操作。

有关 XenMobile 部署中适用于 Exchange ActiveSync 的 Endpoint Management 连接器的示意图，请参阅面向本地部署的参考体系结构。

电子邮件平台决策树

下图将帮助您区分在 XenMobile 部署中使用本机电子邮件或 Secure Mail 解决方案之间的利弊。每种选择都会考虑到关联的 XenMobile 选项以及对启用服务器、网络和数据库访问权限的要求。利弊包括与安全性、策略和用户界面注意事项有关的详细信息。



XenMobile 集成

January 5, 2022

本文介绍了规划 XenMobile 与现有网络和解决方案的集成方式时要考虑的事项。例如，如果您已经将 Citrix ADC 用于 Virtual Apps and Desktops：

- 应该使用现有的 Citrix ADC 实例还是使用新的专用实例?
- 是否要将使用 StoreFront 发布的 HDX 应用程序与 XenMobile 集成?
- 是否计划将 Citrix Files 与 XenMobile 结合使用?
- 是否有要集成到 XenMobile 的网络访问控制解决方案?
- 是否要为您的网络的所有出站流量部署 Web 代理?

Citrix ADC 和 Citrix Gateway

XenMobile ENT 和 MAM 模式强制要求使用 Citrix Gateway。Citrix Gateway 提供用于访问所有公司资源的 Micro VPN 路径，并提供加强的多重身份验证支持。所有 XenMobile Server 设备模式都需要 Citrix ADC 负载平衡：

- 如果您有多个 XenMobile Server
- 或者，如果 XenMobile Server 在您的 DMZ 中或内部网络中（因此，流量从设备依次传输到 Citrix ADC 和 XenMobile）。

您可以使用现有的 Citrix ADC 实例，也可以为 XenMobile 设置新实例。以下各节阐述了使用现有的 Citrix ADC 实例或新的专用 Citrix ADC 实例的优势和劣势。

与为 XenMobile 创建的 Citrix Gateway VIP 共享 Citrix ADC MPX

优势：

- 所有 Citrix 远程连接使用一个公用 Citrix ADC 实例：Citrix Virtual Apps and Desktops、完整 VPN 和无客户端 VPN。
- 对证书身份验证以及服务（例如 DNS、LDAP 和 NTP）访问等使用现有的 Citrix ADC 配置。
- 使用单个 Citrix ADC 平台许可证。

劣势：

- 在同一 Citrix ADC 上处理两个截然不同的用例时，很难规划扩展。
- 有时某个 Citrix Virtual Apps and Desktops 用例需要某个特定的 Citrix ADC 版本。该版本可能存在与 XenMobile 有关的已知问题。或者，XenMobile 可能存在与相应的 Citrix ADC 版本有关的已知问题。
- 如果存在 Citrix Gateway，则不能再次运行适用于 XenMobile 的 Citrix ADC 向导为 XenMobile 创建 Citrix ADC 配置。
- 除了将 Platinum 许可证用于 Citrix Gateway 11.1 或更高版本时外：安装在 Citrix ADC 上及 VPN 连接所需的用户访问许可证汇集在池中。由于这些许可证可用于所有 Citrix ADC 虚拟服务器，因此，XenMobile 以外的服务可能会占用它们。

专用 **Citrix ADC VPX/MPX** 实例

优势：

Citrix 建议使用专用的 Citrix ADC 实例。

- 更易于规划扩展，并可将 XenMobile 流量与资源可能已受限的 Citrix ADC 实例分开。
- 避免在 XenMobile 和 Citrix Virtual Apps and Desktops 需要不同的 Citrix ADC 软件版本出现问题。通常建议在 XenMobile 中使用最新的兼容 Citrix ADC 版本和内部版本。
- 允许通过内置的适用于 XenMobile 的 Citrix ADC 向导对 Citrix ADC 进行 XenMobile 配置。
- 对服务进行虚拟和物理隔离。
- 除了将 Platinum 许可证用于 Citrix Gateway 11.1 或更高版本时外：XenMobile 所需的用户访问许可证仅可用于 Citrix ADC 上的 XenMobile Service。

劣势：

- 需要在 Citrix ADC 上设置额外的服务以支持 XenMobile 配置。
- 需要使用另一个 Citrix ADC 平台许可证。为 Citrix Gateway 许可使用每个 Citrix ADC 实例。

有关在每种 XenMobile Server 模式下集成 Citrix ADC 和 Citrix Gateway 时要考虑的事项的信息，请参阅将 Citrix ADC 与 Citrix Gateway 相集成。

StoreFront

如果您有 Citrix Virtual Apps and Desktops 环境，则可以使用 StoreFront 将 HDX 应用程序与 XenMobile 集成。将 HDX 应用程序与 XenMobile 集成时：

- 在 XenMobile 中注册的用户可获取这些应用程序。
- 这些应用程序与其他移动应用程序一起显示在 XenMobile Store 中。
- 在 StoreFront 上 XenMobile 使用旧版 PNAgent（服务）站点。
- 在设备上安装 Citrix Receiver 后，HDX 应用程序开始使用 Receiver。

StoreFront 存在每个 StoreFront 实例一个服务站点的限制。假设您有多个应用商店，并想要将其与其他生产使用情况分开。在这种情况下，Citrix 通常建议考虑将一个新的 StoreFront 实例和服务站点用于 XenMobile。

注意事项包括：

- StoreFront 是否有任何不同的身份验证要求？StoreFront 服务站点要求使用 Active Directory 凭据进行登录。仅使用基于证书的身份验证的客户不能使用同一 Citrix Gateway 通过 XenMobile 枚举应用程序。
- 使用同一存储还是创建一个新存储？
- 使用同一还是不同的 StoreFront 服务器？

以下各节阐述了对 Receiver 和移动生产力应用程序使用单独的 StoreFront 和组合的 StoreFront 的优势和劣势。

将现有的 **StoreFront** 实例与 **XenMobile Server** 集成

优势：

- 同一应用商店：假定您使用同一 Citrix ADC VIP 访问 HDX，不需要为 XenMobile 对 StoreFront 进行额外配置。假设您选择使用同一应用商店，并想要将 Receiver 访问定向至新的 Citrix ADC VIP。在这种情况下，可将合适的 Citrix Gateway 配置添加到 StoreFront。
- 同一 StoreFront 服务器：使用现有的 StoreFront 安装和配置。

劣势：

- 同一应用商店：如果为了支持 Virtual Apps and Desktops 工作负载而对 StoreFront 进行任何重新配置，也可能会对 XenMobile 产生不利影响。
- 同一 StoreFront 服务器：在大型环境中，要考虑 XenMobile 使用 PNAgent 进行应用程序枚举和启动产生的额外负载。

将新的专用 **StoreFront** 实例用于与 **XenMobile Server** 集成

优势：

- 新应用商店：为 XenMobile 对 StoreFront 应用商店进行任何配置更改应不会影响现有的 Virtual Apps and Desktops 工作负载。
- 新的 StoreFront 服务器：服务器配置更改应不会影响 Virtual Apps and Desktops 工作流。此外，XenMobile 使用 PNAgent 进行应用程序枚举和启动产生的负载应不会影响可扩展性。

劣势：

- 新应用商店：StoreFront 应用商店配置。
- 新的 StoreFront 服务器：需要新的 StoreFront 安装和配置。

有关详细信息，请参阅 XenMobile 文档中的通过 Citrix Secure Hub 使用 Virtual Apps and Desktops。

Citrix Content Collaboration 和 Citrix Files

用户可以通过 Citrix Files 从任何设备访问和同步自己的所有数据。借助 Citrix Files，用户可以与组织内部和外部的人安全地共享数据。如果您将 Citrix Content Collaboration 与 XenMobile Advanced Edition 或 XenMobile Enterprise Edition 集成，则 XenMobile 可为 Citrix Files 提供：

- XenMobile Apps 用户的单点登录身份验证。
- 基于 Active Directory 的用户帐户预配。
- 全面的访问控制策略。

移动设备用户将从完整的 Enterprise 帐户功能集受益。

或者，可以将 XenMobile 配置为只与存储区域连接器集成。通过存储区域连接器，Citrix Files 提供对以下对象的访问：

- 文档和文件夹
- 网络文件共享
- 在 SharePoint 站点中：站点集合和文档库。

连接的文件共享可以包括 Citrix Virtual Apps and Desktops 环境中使用的相同网络主驱动器。可使用 XenMobile 控制台配置与 Citrix Files 或存储区域连接器的集成。有关详细信息，请参阅 Citrix Files 与 XenMobile 结合使用。

以下各节阐述了为 Citrix Files 制定设计决策时提出的问题。

与 **Citrix Files** 集成或仅与存储区域连接器集成

要提问的问题：

- 是否需要在 Citrix 托管的存储区域中存储数据？
- 是否要向用户提供文件共享和同步功能？
- 是否要让用户能够访问 Citrix Files Web 站点上的文件？或者，是否要从移动设备访问 Office 365 内容和个人云连接器？

设计决策：

- 如果对所有这些问题都回答“是”，则与 Citrix Files 集成。
- 仅与存储区域连接器的集成为 iOS 用户提供对现有本地部署存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问权限。在此配置中，您不会设置 Content Collaboration 子域、将用户预配到 Citrix Files 或托管 Citrix Files 数据。将存储区域连接器与 XenMobile 结合使用时遵守防止在企业网络外部泄漏用户信息的安全限制。

存储区域控制器服务器位置

要提问的问题：

- 是否需要本地存储或功能（例如存储区域连接器）？
- 如果使用 Citrix Files 的本地功能，存储区域控制器将位于网络中的什么位置？

设计决策：

- 确定将存储区域控制器服务器置于 Citrix Files 云中、本地单租户存储系统中还是支持的第三方云存储中。
- 存储区域控制器需要某些 Internet 访问权限以与 Citrix Files 控制平面进行通信。可以采用多种方法（包括直接访问、NAT/PAT 配置或代理配置）进行连接。

存储区域连接器

要提问的问题：

- CIFS 共享路径是什么？
- SharePoint URL 是什么？

设计决策：

- 确定访问这些位置是否需要本地存储区域控制器。
- 由于存储区域连接器与内部资源（例如，文件存储库、CIFS 共享和 SharePoint）进行通信：Citrix 建议存储区域控制器位于 DMZ 防火墙后面的内部网络中，且 Citrix ADC 位于前端。

SAML 与 XenMobile Enterprise 的集成

要提问的问题：

- Citrix Files 是否需要 Active Directory 身份验证？
- 首次使用适用于 XenMobile 的 Citrix Files 应用程序是否需要 SSO？
- 当前环境中是否存在标准 IdP？
- 使用 SAML 需要多少个域？
- Active Directory 用户是否有多个电子邮件别名？
- 是否有正在进行或计划不久将进行的任何 Active Directory 域迁移？

设计决策：

XenMobile Enterprise 环境可以选择使用 SAML 作为 Citrix Files 的身份验证机制。身份验证方式包括：

- 使用 XenMobile Server 作为 SAML 的身份提供程序 (IdP)

此方式可以提供卓越的用户体验和自动创建 Citrix Files 帐户的功能，以及支持移动应用程序 SSO 功能。

- 在此过程可增强 XenMobile Server：不需要同步 Active Directory。
- 使用 Citrix Files 用户管理工具进行用户预配。
- 使用受支持的第三方供应商作为 SAML 的 IdP

如果您已有受支持的 IdP，且不需要移动应用程序 SSO 功能，此方式可能最适合您。此方式还需要使用 Citrix Files 用户管理工具进行帐户预配。

使用第三方 IdP 解决方案（例如 ADFS）还可以在 Windows 客户端上提供 SSO 功能。请务必在选择 Citrix Files SAML IdP 之前评估用例。

此外，要满足这两种用例，您可以将 ADFS 和 XenMobile 配置为双 IdP。

移动应用程序

要提问的问题：

- 您计划使用哪种 Citrix Files 移动应用程序（公共、MDM、MDX）？

设计决策：

- 从 Apple App Store 和 Google Play 应用商店分发移动生产力应用程序。采用这种公共应用商店分发，您可以从 Citrix 下载页面获取打包的应用程序。
- 如果安全性较低且您不需要容器化，公共 Citrix Files 应用程序可能不适用。在仅 MDM 环境中，您可以使用处于 MDM 模式的 XenMobile 交付 MDM 版本的 Citrix Files 应用程序。
- 有关详细信息，请参阅应用程序和适用于 XenMobile 的 Citrix Files。

安全性、策略和访问控制

要提问的问题：

- 对桌面、Web 和移动用户有哪些限制要求?
- 对用户要进行哪些标准访问控制设置?
- 计划使用什么文件保留策略?

设计决策:

- Citrix Files 允许您管理员工权限和设备安全性。有关信息，请参阅 Employee Permissions（员工权限）和 Managing Devices and Apps（管理设备和应用程序)。
- 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，XenMobile 策略优先于 Citrix Files 设备安全设置。示例：如果您在 Citrix Files 中禁用外部应用程序，但在 XenMobile 中启用这些应用程序，则在 Citrix Files 中外部应用程序处于禁用状态。您可以配置应用程序，以实现 XenMobile 不要求使用 PIN/通行码，但 Citrix Files 应用程序要求使用 PIN/通行码。

标准存储区域与受限存储区域

要提问的问题:

- 是否需要受限存储区域?

设计决策:

- 标准存储区域专用于存储非敏感数据，员工可以在此区域中与非员工共享数据。此方式支持涉及在域外部共享数据的工作流。
- 受限存储区域保护敏感数据：只有通过身份验证的域用户可以访问此区域中存储的数据。

Web 代理

在以下情况下最有可能通过 HTTP(S)/SOCKS 代理路由 XenMobile 流量：XenMobile Server 所在的子网没有出站 Internet 访问所需 Apple、Google 或 Microsoft IP 地址的权限时。您可以在 XenMobile 中指定代理服务器设置以将所有 Internet 流量路由到代理服务器。有关详细信息，请参阅启用代理服务器。

下表介绍了 XenMobile 中使用的最常见代理的优势和劣势。

选项	优势	劣势
在 XenMobile Server 中使用 HTTP(S)/SOCKS 代理。	如果策略不允许从 XenMobile Server 子网进行出站 Internet 连接：可以配置 HTTP(S) 或 SOCKS 代理以提供 Internet 连接。	如果代理服务器发生故障，APNs (iOS) 或 Firebase Cloud Messaging (Android) 连接将中断。因此，所有 iOS 和 Android 设备将无法发送设备通知。

在 Secure Web 中使用 HTTP(S) 代理。	您可以监视 HTTP/HTTPS 流量以确保 Internet 活动符合贵组织的标准。	此配置要求所有 Secure Web Internet 流量通过通道传回到企业网络，然后再向外发送到 Internet。如果您的 Internet 连接限制浏览：此配置可能会影响 Internet 浏览性能。

用于拆分隧道的 Citrix ADC 会话配置文件配置会影响流量，如下所示。

当 Citrix ADC 拆分隧道设置为关时：

- 如果 MDX 网络访问策略为通过通道连接到内部网络：强制所有流量使用 Micro VPN 或无客户端 VPN (cVPN) 通道传回到 Citrix Gateway。
- 为代理服务器配置 Citrix ADC 流量策略/配置文件，并将其绑定到 Citrix Gateway VIP。

> 重要：
>
> 请务必从代理中排除 Secure Hub cVPN 流量。

- 有关详细信息，请参阅 XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode（在安全浏览模式下通过代理服务器传输 XenMobile Secure Hub 流量）。

当 **Citrix ADC** 拆分隧道设置为开时：

- 如果为应用程序配置的 MDX 网络访问策略设置为通过通道连接到内部网络：应用程序首先尝试直接获取 Web 资源。如果 Web 资源未公开提供，则这些应用程序回退到 Citrix Gateway。
- 为代理服务器配置 Citrix ADC 流量策略和配置文件。然后，将这些策略和配置文件绑定到 Citrix Gateway VIP。

> 重要：
>
> 请务必从代理中排除 Secure Hub cVPN 流量。

有关拆分 **DNS**（在 **Client experience**（客户端体验）下方）的 Citrix ADC 会话配置文件配置作用方式类似于 “拆分隧道”。

在拆分 **DNS** 处于启用状态并设置为两者的情况下：

- 客户端首先尝试在本地解析 FQDN，如果失败，则回退到 Citrix ADC 以进行 DNS 解析。

在拆分 **DNS** 设置为远程的情况下：

- 仅在 Citrix ADC 上进行 DNS 解析。

在拆分 **DNS** 设置为本地的情况下：

- 客户端尝试在本地解析 FQDN。不使用 Citrix ADC 进行 DNS 解析。

访问控制

企业可以管理网络内部和外部的移动设备。企业移动性管理解决方案（例如 XenMobile）非常适合为移动设备提供安全和控制功能，而与位置无关。但是，将其与网络访问控制 (NAC) 解决方案结合使用时，可以为您网络内部的设备增加 QoS 和更加细化的控制。该组合让您可以通过您的 NAC 解决方案延长 XenMobile 设备安全评估。之后您的 NAC 解决方案可以使用 XenMobile 安全评估帮助制定和处理身份验证决策。

可以使用以下任意解决方案来强制实施 NAC 策略：

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix 不保证其他 NAC 解决方案的集成。

NAC 解决方案与 XenMobile 的集成具有以下优势：

- 提高了企业网络上所有端点的安全性和合规性，并增强了对其控制能力。
- NAC 解决方案可以：
  - 在设备尝试连接到网络的同时检测到设备。
  - 在 XenMobile 中查询设备属性。
  - 请使用该设备信息来确定允许、阻止、限制还是重定向这些设备。这些决策取决于您选择强制执行的安全策略。
- NAC 解决方案为 IT 管理员提供非托管设备和不合规设备信息。

有关 XenMobile 支持的 NAC 合规性过滤器的说明和配置概览，请参阅网络访问控制。

多站点要求

January 5, 2022

可以设计包括多个用于实现高可用性和灾难恢复的站点的 XenMobile 部署的架构并配置这些部署。本文概述了 XenMobile 部署中使用的高可用性和灾难恢复模型。

高可用性

- 对于 XenMobile 群集节点，Citrix ADC 负责处理负载平衡。有关详细信息，请参阅配置群集
- XenMobile Server 节点在主动/主动配置中运行。
- 其他 XenMobile Server 节点将添加到高可用性群集，因为需要容量。一个节点最多可以处理大约 8500 台用户设备（有关更多详细信息，请参阅可扩展性和性能）。
- Citrix 建议您配置 “n+1” 个 XenMobile Server：一个服务器用于每 8500 台用户设备，一个额外的服务器用于实现冗余。
- Citrix 建议您在可能允许配置与第二个 Citrix ADC 同步的任意位置为所有 Citrix ADC 实例配置高可用性。

- 标准 Citrix ADC 高可用性对在主动/被动配置中运行。

典型的高可用性 XenMobile 部署通常包括：

- 两个 Citrix ADC 实例（VPX 或 MPX）。如果使用 Citrix ADC SDX 平台，则应考虑高可用性。
- 配置了相同数据库设置的两个或多个 XenMobile Server。

灾难恢复

可以将 XenMobile 配置为跨两个数据中心（一个主动数据中心和一个被动数据中心）进行灾难恢复。Citrix ADC 和全局服务器负载平衡 (GSLB) 用于创建主动/主动数据路径，以便用户体验属于主动/主动设置的用户体验。

对于灾难恢复，XenMobile 部署包括：

- 两个数据中心；其中每个数据中心都包含一个或多个 Citrix ADC 实例、XenMobile Server 和 SQL Server 数据库。
- GSLB 服务器直接将流量传输到数据中心。为负责处理传输到站点的流量的 XenMobile 注册 URL 和 Citrix Gateway URL 同时配置 GSLB 服务器。
- 使用适用于 XenMobile 的 Citrix ADC 向导配置 Citrix Gateway 时，默认情况下，GSLB 未启用，无法解析传输到 XenMobile 注册服务器的流量以及传输到 Citrix Gateway 的流量，这些流量将重新发送到 MAM 负载平衡服务器；因此，需要执行额外的步骤。有关准备和实施这些步骤的详细信息，请参阅灾难恢复。
- AlwaysOn 可用性组的群集化 SQL Server。
- XenMobile Server 与 SQL Server 之间的延迟必须小于 5 毫秒。

> 注意：
>
> 本手册中介绍的灾难恢复方法仅提供针对访问层的自动化灾难恢复。必须在故障转移站点手动启动所有 XenMobile Server 节点和 SQL Server 数据库，才能连接 XenMobile Server。

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

January 5, 2022

与 XenMobile 集成后，Citrix Gateway 为 MAM 设备提供了远程设备访问内部网络时使用的身份验证机制。通过该集成，移动生产力应用程序可以通过 Micro VPN 连接到 Intranet 中的公司服务器。Micro VPN 是在移动设备上的应用程序与 Citrix Gateway 之间创建的。Citrix Gateway 提供用于访问所有公司资源的 Micro VPN 路径，并提供加强的多重身份验证支持。

在以下情况下，所有 XenMobile Server 设备模式都需要 Citrix ADC 负载平衡：

- 如果您有多个 XenMobile Server
- 或者，如果 XenMobile Server 在您的 DMZ 中或内部网络中（因此，流量从设备依次传输到 Citrix ADC 和 XenMobile）

XenMobile Server 模式的集成要求

根据 XenMobile Server 模式（MAM、MDM 和 ENT），Citrix Gateway 和 Citrix ADC 的集成要求有所不同。

MAM

XenMobile Server 处于 MAM 模式时：

- **Citrix Gateway** 是必需的。Citrix Gateway 提供用于访问所有公司资源的 Micro VPN 路径，并提供加强的多重身份验证支持。
- 建议使用 **Citrix ADC** 进行负载平衡。

  Citrix 建议采用高可用性配置部署 XenMobile，这需要 XenMobile 前端有负载平衡器。有关详细信息，请参阅关于 MAM 和旧版 MAM 模式。

MDM

XenMobile Server 处于 MDM 模式时：

- Citrix Gateway 不是必需的。对于 MDM 部署，Citrix 建议对移动设备 VPN 使用 Citrix Gateway。
- 建议使用 Citrix ADC 以提高安全性并进行负载平衡。

  Citrix 建议在 XenMobile Server 前端部署 Citrix ADC 设备，以提高安全性并进行负载平衡。对于 XenMobile 在 DMZ 中的标准部署，Citrix 建议使用适用于 XenMobile 的 Citrix ADC 向导，并采用处于 SSL 桥接模式的 XenMobile Server 负载平衡。还可以考虑对具有以下特点的部署使用 SSL 卸载：

  - XenMobile Server 驻留在内部网络中，而非 DMZ 中
  - 或者您的安全团队要求 SSL 桥配置

  Citrix 建议不要通过 NAT 或现有的第三方代理或负载均衡器将 XenMobile Server 公开到 Internet。即使 SSL 流量在 XenMobile Server（SSL 桥）上终止，这些配置也会造成潜在的安全风险。

  对于高安全性环境，采用默认 XenMobile 配置的 Citrix ADC 满足或超过安全要求。

  对于具有最高安全性需求的 MDM 环境，终止于 Citrix ADC 的 SSL 允许您检查外围流量的功能，同时维持端到端 SSL 加密。有关详细信息，请参阅安全要求。Citrix ADC 提供用于定义 SSL/TLS 密码的选项和 SSL FIPS Citrix ADC 硬件。

ENT (MAM+MDM)

XenMobile Server 处于 ENT 模式时：

- Citrix Gateway 是必需的。Citrix Gateway 提供用于访问所有公司资源的 Micro VPN 路径，并提供加强的多重身份验证支持。

当 XenMobile Server 模式为 ENT 且用户选择退出 MDM 注册时，设备将以旧版 MAM 模式运行。在旧版 MAM 模式下，设备使用 Citrix Gateway FQDN 进行注册。有关详细信息，请参阅关于 MAM 和旧版 MAM 模式。

- 建议使用 Citrix ADC 进行负载平衡。有关详细信息，请参阅本文前面的“MDM”下的 Citrix ADC 点。

> 重要：
>
> 首次注册时，来自用户设备的流量将在 XenMobile Server 上进行身份验证，无论您将负载平衡虚拟服务器配置为 SSL 卸载还是 SSL 桥接。

设计决策

以下各节概述了规划 Citrix Gateway 与 XenMobile 的集成时要考虑的多个设计决策。

许可和版本

决策详细信息：

- 您打算使用什么版本的 Citrix ADC?
- 您是否已将平台许可证应用于 Citrix ADC?
- 如果您需要使用 MAM 功能，您是否已应用 Citrix ADC 通用访问许可证?

设计指导：

请务必将正确的许可证应用于 Citrix Gateway。如果您使用适用于 Exchange ActiveSync 的 Citrix Gateway 连接器，则可能需要集成缓存。因此，您必须确保已安装相应的 Citrix ADC 版。

启用 Citrix ADC 功能的许可证要求如下所示。

- XenMobile MDM 负载平衡至少需要一个 Citrix ADC 标准平台许可证。
- 采用存储区域控制器的 Content Collaboration 负载平衡至少需要一个 Citrix ADC 标准平台许可证。
- XenMobile Enterprise Edition 包含 MAM 所需的 Citrix Gateway 通用许可证。
- Exchange 负载平衡需要一个 Citrix ADC Platinum 平台许可证或 Citrix ADC Enterprise 平台许可证以及集成缓存许可证。

适用于 **XenMobile** 的 **Citrix ADC** 版本

决策详细信息：

- XenMobile 环境中运行的 Citrix ADC 是哪个版本?
- 您是否需要单独的实例?

设计指导：

Citrix 建议 Citrix Gateway 虚拟服务器使用专用的 Citrix ADC 实例。请确保在 XenMobile 环境中使用满足最低要求的 Citrix ADC 版本和内部版本。通常情况下，最好在 XenMobile 中使用最新的兼容 Citrix ADC 版本和内部版本。如果升级 Citrix Gateway 会影响现有环境，可能适合采用第二个专用的 XenMobile 实例。

如果您计划让 XenMobile 和使用 VPN 连接的其他应用程序共用一个 Citrix ADC 实例，请确保您有足够的 VPN 许可证用于两者。请谨记，XenMobile 测试和生产环境不能共用一个 Citrix ADC 实例。

证书

决策详细信息：

- XenMobile 环境中的注册和访问是否需要更高的安全性？
- 是否无法使用 LDAP？

设计指导：

XenMobile 的默认配置是用户名和密码身份验证。要为 XenMobile 环境中的注册和访问再增加一个安全层，请考虑使用基于证书的身份验证。您可以组合使用证书与 LDAP 以实现双重身份验证，从而提高安全性，而无需 RSA 服务器。

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

XenMobile 支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，XenMobile 将使用 Citrix ADC 管理吊销。配置基于客户端证书的身份验证时，请考虑是否需要配置 Citrix ADC 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh**（启用 CRL 自动刷新）。此步骤可确保使用在仅 MAM 模式下注册的设备的用户无法使用设备上的现有证书进行身份验证。XenMobile 将重新颁发新证书，因为吊销一个用户证书后，XenMobile 不限制用户再生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

网络拓扑

决策详细信息：

- 需要什么 Citrix ADC 拓扑？

设计指导：

Citrix 建议 XenMobile 使用一个 Citrix ADC 实例。但是，您可能不希望流量从内部网络传出到 DMZ。在这种情况下，请考虑设置 Citrix ADC 的额外实例。为内部用户使用一个 Citrix ADC 实例，外外部用户使用另一个实例。当用户在内部网络与外部网络之间切换时，DNS 记录缓存可能会导致 Secure Hub 登录提示次数增加。

XenMobile 不支持 Citrix Gateway 双跃点。

专用或共享的 **Citrix Gateway VIP**

决策详细信息：

- 您目前是否为 Virtual Apps and Desktops 使用 Citrix Gateway？
- 您是否计划让 XenMobile 使用与 Virtual Apps and Desktops 相同的 Citrix Gateway？
- 两种通信流的身份验证要求是什么？

设计指导：

如果您的 Citrix 环境包含 XenMobile 以及 Virtual Apps and Desktops，两者可以使用同一 Citrix ADC 实例和 Citrix Gateway 虚拟服务器。由于可能存在版本控制冲突和环境隔离，建议每个 XenMobile 环境使用专用的 Citrix ADC 实例和 Citrix Gateway。但是，如果无法使用专用的 Citrix ADC 实例，Citrix 建议使用专用的 Citrix Gateway 虚拟服务器，以便为 Secure Hub 分离通信流。该配置替代在 XenMobile 与 Virtual Apps and Desktops 之间共享的虚拟服务器。

如果您使用 LDAP 身份验证，Receiver 和 Secure Hub 可以向同一 Citrix Gateway 进行身份验证，不会有任何问题。如果您使用基于证书的身份验证，XenMobile 将推送 MDX 容器中的证书，Secure Hub 将使用该证书向 Citrix Gateway 进行身份验证。Receiver 与 Secure Hub 是分开的，无法与 Secure Hub 使用同一证书向同一 Citrix Gateway 进行身份验证。

您可以考虑以下解决方法，这样，您可以对两个 Citrix Gateway VIP 使用同一 FQDN。

- 创建两个具有相同 IP 地址的 Citrix Gateway VIP。用于 Secure Hub 的 VIP 使用标准 443 端口，用于 Virtual Apps and Desktops（部署 Receiver）的 VIP 使用端口 444。
- 因此，一个 FQDN 解析为相同的 IP 地址。
- 对于此解决方法，您可能会将 StoreFront 配置为返回端口 444 而不是默认端口 443 的 ICA 文件。此解决方法不需要用户输入端口号。

Citrix Gateway 超时

决策详细信息：

- 您要如何配置 XenMobile 流量的 Citrix Gateway 超时?

设计指导：

Citrix Gateway 包括“会话超时”和“强制超时”设置。有关详细信息，请参阅建议的配置。请谨记，后台服务、Citrix ADC 以及脱机时访问应用程序的超时值不同。

用于 **MAM** 的 **XenMobile** 负载平衡器 **IP** 地址

决策详细信息：

- VIP 使用内部 IP 地址还是外部 IP 地址?

设计指导：

在 Citrix Gateway VIP 可以使用公用 IP 地址的环境中，以此方式分配 XenMobile 负载平衡 VIP 和地址会导致注册失败。

在此情况下，请确保负载平衡 VIP 使用内部 IP 以避免注册失败。此虚拟 IP 地址必须遵循有关专用 IP 地址的 RFC 1918 标准。如果您对此虚拟服务器使用非专用 IP 地址，则在身份验证过程中，Citrix ADC 将无法成功联系 XenMobile Server。有关详细信息，请参阅 https://support.citrix.com/article/CTX200430。

MDM 负载平衡机制

决策详细信息：

- Citrix Gateway 如何对 XenMobile Server 进行负载平衡？

设计指导：

如果 XenMobile 在 DMZ 中，请使用 SSL 桥接。当 XenMobile 在内部网络中时，如果为了满足安全标准而需要 SSL 卸载，请使用 SSL 卸载。

- 在 SSL 桥接模式下通过 Citrix ADC VIP 对 XenMobile Server 进行负载平衡时，Internet 流量直接传输到连接终止处的 XenMobile Server。SSL 桥接模式是易于设置和故障排除的最简单模式。
- 在 SSL 卸载模式下通过 Citrix ADC VIP 对 XenMobile Server 进行负载平衡时，Internet 流量直接传输到连接终止处的 Citrix ADC。然后，Citrix ADC 建立从 Citrix ADC 到 XenMobile Server 的新会话。在设置和故障排除过程中，SSL 卸载模式的复杂性将增加。

用于通过 **SSL** 卸载进行 **MDM** 负载平衡的服务端口

决策详细信息：

- 如果您计划使用 SSL 卸载模式进行负载平衡，后端服务将使用哪个端口？

设计指导：

对于 SSL 卸载，按如下所示选择端口 80 或 8443：

- 使用端口 80 返回到 XenMobile Server，以进行实际卸载。
- 不支持端到端加密（即对流量重新加密）。有关详细信息，请参阅 Citrix 支持文章 Supported Architectures Between NetScaler and XenMobile Server（NetScaler 和 XenMobile Server 之间支持的体系结构）。

注册 **FQDN**

决策详细信息：

- 您打算使用什么作为注册和 XenMobile 实例/负载平衡 VIP 的 FQDN？

设计指导：

对群集中的第一个 XenMobile Server 进行初始配置时，您需要提供 XenMobile Server FQDN。该 FQDN 必须匹配您的 MDM VIP URL 和内部 MAM LB VIP URL。（内部 Citrix ADC 地址记录解析 MAM LB VIP）。有关详细信息，请参阅本文后面的 “每种管理模式的注册 FQDN”。

此外，您必须使用与以下证书相同的证书：

- XenMobile SSL 侦听器证书
- 内部 MAM LB VIP 证书
- MDM VIP 证书（如果对 MDM VIP 使用 SSL 卸载）

> 重要：
>
> 配置注册 FQDN 后，无法对其进行更改。新的注册 FQDN 需要重新构建新的 SQL Server 数据库和 XenMobile Server。

Secure Web 流量

决策详细信息：

- 您是否计划限制 Secure Web 仅使用内部 Web 浏览？
- 您是否计划启用 Secure Web 进行内部 Web 浏览和外部 Web 浏览？

设计指导：

如果您计划仅使用 Secure Web 进行内部 Web 浏览，Citrix Gateway 配置将非常简单。默认情况下，Secure Web 必须访问所有内部站点。您可能需要配置防火墙和代理服务器。

如果您计划将 Secure Web 用于外部浏览和内部浏览，则必须启用 SNIP 以便具有出站 Internet 访问权限。IT 通常将注册的设备（使用 MDX 容器）视为企业网络的扩展。因此，IT 通常希望 Secure Web 连接恢复到 Citrix ADC，通过代理服务器，然后转到 Internet。默认情况下，Secure Web 为所有网络访问使用返回到内部网络的每应用程序 VPN 通道。Citrix ADC 使用拆分通道设置。

有关 Secure Web 连接的讨论，请参阅配置用户连接。

Secure Mail 的推送通知

决策详细信息：

- 您是否计划使用推送通知？

适用于 iOS 的设计指导：

您的 Citrix Gateway 配置可能包括 Secure Ticket Authority (STA)，并且关闭了拆分通道。Citrix Gateway 必须允许从 Secure Mail 到（在 Secure Mail for iOS 的“推送通知”中指定的）Citrix 侦听器服务 URL 的流量。

适用于 Android 的设计指导：

请使用 Firebase Cloud Messaging (FCM) 控制 Android 设备需要连接到 XenMobile 的方式和时间。配置了 FCM 后，任何安全操作或部署命令都将触发向 Secure Hub 推送通知，以提示用户重新连接到 XenMobile Server。

HDX STA

决策详细信息：

- 如果您计划集成 HDX 应用程序访问，要使用什么 STA？

设计指导：

HDX STA 必须匹配 StoreFront 中的 STA，并且必须对 Virtual Apps and Desktops 场有效。

Citrix Files 和 Citrix Content Collaboration

决策详细信息：

- 您是否计划在环境中使用存储区域控制器？
- 您计划使用哪些 Citrix Files VIP URL？

设计指导：

如果您将在环境中包含存储区域控制器，请确保正确配置以下对象：

- Citrix Files 交换机 VIP（Citrix Files 控制平面用于与存储区域控制器服务器通信）
- Citrix Files 负载平衡 VIP
- 所有必需的策略和配置文件

有关信息，请参阅存储区域控制器文档。

SAML IdP

决策详细信息：

- 如果 Citrix Files 需要 SAML，您是否要将 XenMobile 用作 SAML IdP？

设计指导：

推荐的最佳做法是，将 Citrix Files 与 XenMobile Advanced Edition 或 XenMobile Enterprise Edition 集成，这样做比配置基于 SAML 的联合身份验证更简单。将 Citrix Files 与这些 XenMobile 版本一起使用时，XenMobile 会为 Citrix Files 提供以下功能：

- 移动生产力应用程序用户的单点登录 (SSO) 身份验证
- 基于 Active Directory 的用户帐户预配
- 全面的访问控制策略

通过 XenMobile 控制台，可以执行 Citrix Files 配置以及监视服务级别和许可证使用情况。

有两种类型的 Citrix Files 客户端：适用于 XenMobile 的 Citrix Files 客户端（也称为打包的 Citrix Files）和 Citrix Files 移动客户端（也称为未打包的 Citrix Files）。要了解差别，请参阅适用于 XenMobile 的 Citrix Files 客户端与 Citrix Files 移动客户端之间的差别。

可以将 XenMobile 和 Citrix Content Collaboration 配置为使用 SAML 提供对以下内容的 SSO 访问：

- Citrix Files 移动应用程序
- 未封装的 Citrix Files 客户端，例如 Web 站点、Outlook 插件或同步客户端

要将 XenMobile 用作 Citrix Files 的 SAML IdP，请确保已实施合适的配置。有关详细信息，请参阅 SAML SSO 与 Citrix Files。

ShareConnect 直接连接

决策详细信息：

- 用户是否必须从运行使用直接连接的 ShareConnect 的计算机或移动设备访问主机计算机?

设计指导:

借助 ShareConnect，用户可以通过 iPad、Android 平板电脑和 Android 手机安全地连接到其计算机，以访问文件和应用程序。对于直接连接，XenMobile 使用 Citrix Gateway 安全地访问对本地网络外部的资源。有关配置详细信息，请参阅 ShareConnect。

每个管理模式的注册 **FQDN**

管理模式	注册 **FQDN**
采用强制 MDM 注册的企业 (MDM+MAM)	XenMobile Server FQDN
采用可选 MDM 注册的企业 (MDM+MAM)	XenMobile Server FQDN 或 Citrix Gateway FQDN
仅 MDM	XenMobile Server FQDN
仅 MAM（旧版）	Citrix Gateway FQDN
仅 MAM	XenMobile Server FQDN

部署摘要

Citrix 建议使用适用于 XenMobile 的 Citrix ADC 向导以确保完成正确配置。只能使用该向导一次。如果您有多个 XenMobile 实例（例如，用于测试、开发和生产环境），必须手动为其他环境配置 Citrix ADC。您有工作环境时，请先记下设置，然后再尝试手动为 XenMobile 配置 Citrix ADC。

使用该向导时要做出的主要决定是对与 XenMobile Server 的通信使用 HTTPS 还是 HTTP。HTTPS 提供安全的后端通信，因为 Citrix ADC 与 XenMobile 之间的流量已加密。重新加密会影响 XenMobile Server 的性能。HTTP 提供了更加出色的 XenMobile Server 性能。Citrix ADC 与 XenMobile 之间的流量不加密。以下各表显示了 Citrix ADC 和 XenMobile Server 的 HTTP 和 HTTPS 端口要求。

HTTPS

Citrix 通常建议对 Citrix ADC MDM 虚拟服务器配置使用 SSL 桥接。如果对 MDM 虚拟服务器使用 Citrix ADC SSL 卸载，XenMobile 仅支持后端服务使用端口 80。

管理模式	**Citrix ADC** 负载平衡方法	**SSL** 重新加密	**XenMobile Server** 端口

MDM	SSL 桥接	不适用	443、8443
MAM	SSL 卸载	已启用	8443
Enterprise	MDM：SSL 桥接	不适用	443、8443
Enterprise	MAM：SSL 卸载	已启用	8443

HTTP

管理模式	**Citrix ADC** 负载平衡方法	**SSL** 重新加密	**XenMobile Server** 端口
MDM	SSL 卸载	不支持	80
MAM	SSL 卸载	已启用	8443
Enterprise	MDM：SSL 卸载	不支持	80
Enterprise	MAM：SSL 卸载	已启用	8443

有关 XenMobile 部署中的 Citrix Gateway 的示意图，请参阅面向本地部署的参考体系结构。

MDX 应用程序的 **SSO** 和代理注意事项

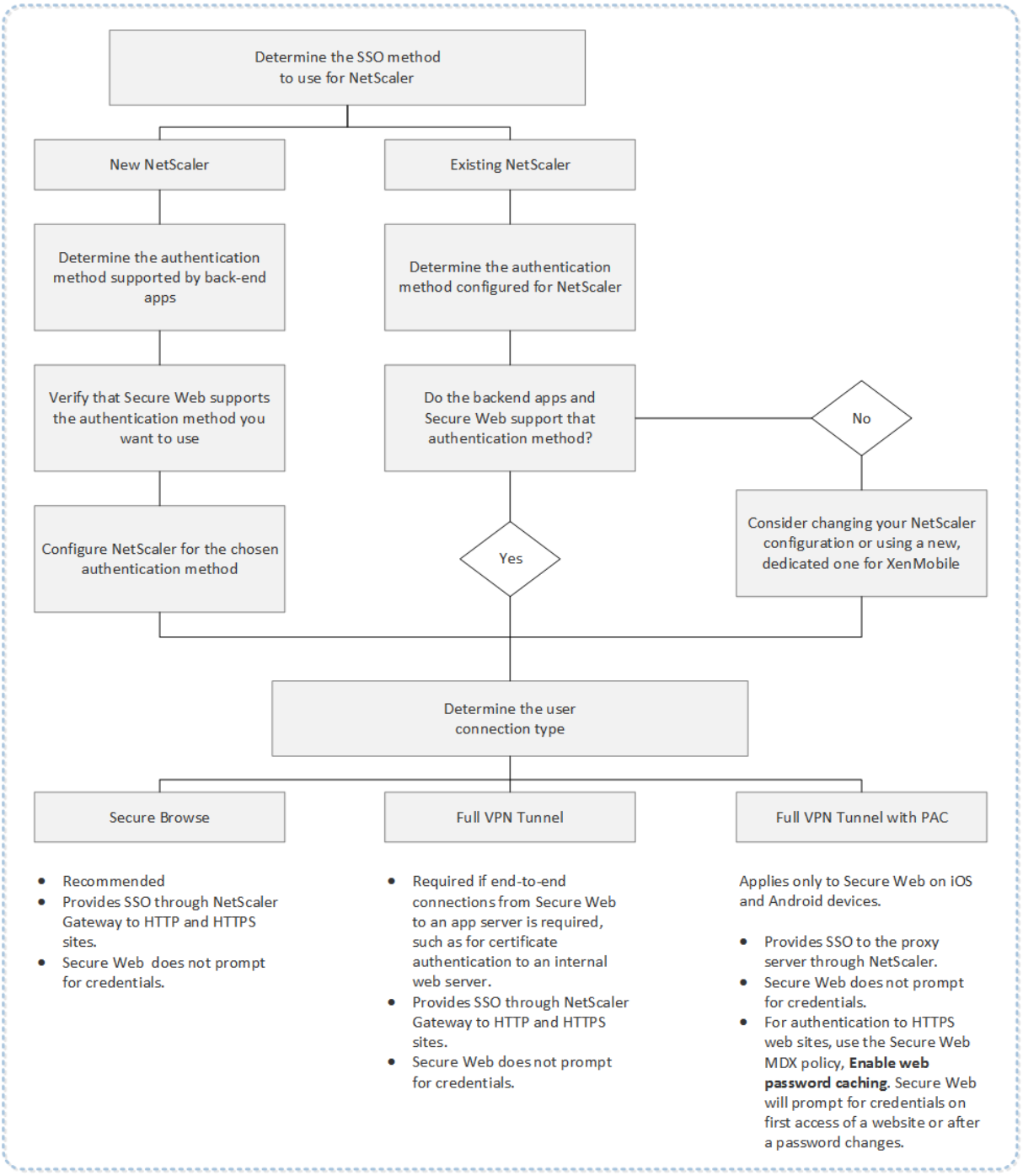
January 5, 2022

通过 XenMobile 与 Citrix ADC 的集成，您可以向用户提供通过单点登录 (SSO) 访问所有后端 HTTP/HTTPS 资源的功能。根据您的 SSO 身份验证要求，可以将 MDX 应用程序的用户连接配置为使用以下任一方式：

- 安全浏览，这是一种无客户端 VPN
- 完整 VPN 通道

如果 Citrix ADC 不是在您的环境中提供 SSO 的最佳方法，则可以为 MDX 应用程序设置基于策略的本地密码缓存。本文探讨了各种 SSO 和代理选项，重点探讨 Secure Web。这些概念适用于其他 MDX 应用程序。

下面的流程图概括了 SSO 和用户连接的决策流程。



Citrix ADC 身份验证方法

本节提供了有关 Citrix ADC 支持的身份验证方法的常规信息。

SAML 身份验证

将 Citrix ADC 配置为使用安全声明标记语言 (SAML) 时，用户可以连接到支持使用 SAML 协议进行单点登录的 Web 应用程序。Citrix Gateway 支持对 SAML Web 应用程序进行身份提供程序 (IdP) 单点登录。

所需的配置：

- 在 Citrix ADC 流量配置文件中配置 SAML SSO。
- 为请求的服务配置 SAML IdP。

NTLM 身份验证

如果在会话配置文件中启用了通过 SSO 登录 Web 应用程序的功能，Citrix ADC 将自动执行 NTLM 身份验证。

所需的配置：

- 在 Citrix ADC 会话或流量配置文件中启用 SSO。

Kerberos 模拟

XenMobile 仅支持对 Secure Web 使用 Kerberos。将 Citrix ADC 配置为进行 Kerberos SSO 时，Citrix ADC 将在用户密码对 Citrix ADC 可用时使用模拟。模拟是指 Citrix ADC 使用用户凭据获得获取对 Secure Web 等服务的访问权限所需的令牌。

所需的配置：

- 配置 Citrix ADC Worx 会话策略以允许其识别来自您的连接的 Kerberos 领域。
- 在 Citrix ADC 上配置 Kerberos 约束委派 (KCD) 帐户。将该帐户配置为无密码，并将其绑定到您的 XenMobile 网关上的流量策略。
- 有关这些配置及其他配置的详细信息，请参阅 Citrix 博客：WorxWeb and Kerberos Impersonation SSO（WorxWeb 和 Kerberos 模拟 SSO）。

Kerberos 约束委派

XenMobile 仅支持对 Secure Web 使用 Kerberos。将 Citrix ADC 配置为进行 Kerberos SSO 时，Citrix ADC 将在用户密码对 Citrix ADC 不可用时使用约束委派。

启用了约束委派时，Citrix ADC 将使用指定的管理员帐户代表用户和服务获取令牌。

所需的配置：

- 在 Active Directory 中为 KCD 帐户配置所需的权限并在 Citrix ADC 上配置一个 KCD 帐户。
- 在 Citrix ADC 流量配置文件中启用 SSO。
- 将后端 Web 站点配置为进行 Kerberos 身份验证。

表单填充身份验证

将 Citrix ADC 配置为进行基于表单的单点登录时，用户登录一次即可访问您的网络中所有受保护的应用程序。此身份验证方法适用于使用安全浏览或完整 VPN 模式的应用程序。

所需的配置：

- 在 Citrix ADC 流量配置文件中配置基于表单的 SSO。

摘要式 **HTTP** 身份验证

如果在会话配置文件中启用通过 SSO 登录 Web 应用程序的功能，Citrix ADC 将自动执行摘要式 HTTP 身份验证。此身份验证方法适用于使用安全浏览或完整 VPN 模式的应用程序。

所需的配置：

- 在 Citrix ADC 会话或流量配置文件中启用 SSO。

基本 **HTTP** 身份验证

如果在会话配置文件中启用通过 SSO 登录 Web 应用程序的功能，Citrix ADC 将自动执行基本 HTTP 身份验证。此身份验证方法适用于使用安全浏览或完整 VPN 模式的应用程序。

所需的配置：

- 在 Citrix ADC 会话或流量配置文件中启用 SSO。

安全浏览、完整 **VPN** 通道或使用 **PAC** 的完整 **VPN** 通道

以下各节介绍了适用于 Secure Web 的用户连接类型。有关详细信息，请参阅 Citrix 文档中的此 Secure Web 文章：配置用户连接。

完整 **VPN** 通道

通过通道连接到内部网络的连接可以使用完整 VPN 通道。可使用 “Secure Web 首选 VPN 模式” 策略配置完整 VPN 通道。Citrix 建议对通过客户端证书或端到端 SSL 与内部网络中的资源建立的连接使用完整 VPN 通道。完整 VPN 通道处理任何 TCP 协议。可以在 Windows、Mac、iOS 和 Android 设备上使用完整 VPN 通道。

在完整 VPN 通道模式下，Citrix ADC 在 HTTPS 会话中不可见。

安全浏览

通过通道连接到内部网络的连接可以使用无客户端 VPN 的变体（称为 “安全浏览”）。安全浏览是为 Secure Web 首选 **VPN** 模式策略指定的默认配置。Citrix 建议对需要单点登录 (SSO) 的连接使用安全浏览。

在安全浏览模式下，Citrix ADC 将 HTTPS 会话分成两个部分：

- 从客户端到 Citrix ADC
- 从 Citrix ADC 到后端资源服务器。

这样，Citrix ADC 将在客户端与服务器之间的所有事务中完全可见，使其能够提供 SSO。

在安全浏览模式下使用时，还可以为 Secure Web 配置代理服务器。有关详细信息，请参阅博客 XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode（在安全浏览模式下通过代理服务器传输 XenMobile WorxWeb 流量）。

使用 **PAC** 的完整 **VPN** 通道

对于 iOS 和 Android 设备上的 Secure Web，可以在完整 VPN 通道部署中使用代理自动配置 (PAC) 文件。XenMobile 支持 Citrix ADC 提供的代理身份验证。PAC 文件中包含的规则用于定义 Web 浏览器如何选择代理以访问指定 URL。PAC 文件规则可以指定对外部和内部站点的处理方式。Secure Web 解析 PAC 文件规则并将代理服务器信息发送到 Citrix Gateway。Citrix Gateway 无法识别 PAC 文件或代理服务器。

对于 HTTPS Web 站点的身份验证：Secure Web MDX 策略启用 **Web** 密码缓存允许 Secure Web 进行身份验证并通过 MDX 提供对代理服务器的 SSO。

Citrix ADC 拆分隧道

规划 SSO 和代理配置时，还必须决定是否要使用 Citrix ADC 拆分通道。如有需要，Citrix 建议您仅使用 Citrix ADC 拆分通道。本节从高层角度提供了拆分通道的工作原理：Citrix ADC 根据其路由表确定流量路径。当 Citrix ADC 拆分通道为“开”时，Secure Hub 将内部（受保护的）网络流量与 Internet 流量区分开。Secure Hub 根据 DNS 后缀和 Intranet 应用程序做出决定。然后，Secure Hub 仅通过 VPN 通道传输内部网络流量。Citrix ADC 拆分通道设置为“关”时，所有流量都将通过 VPN 通道传输。

- 如果出于安全考虑，您更希望监视所有流量，请禁用 Citrix ADC 拆分通道。这样，所有流量都通过 VPN 通道传输。
- 如果要在 PAC 中使用完整 VPN 通道，则必须禁用 Citrix Gateway 拆分通道。如果启用了拆分通道并且您配置了 PAC 文件，PAC 文件规则将覆盖 Citrix ADC 拆分通道规则。在流量策略中配置的代理服务器不会覆盖 Citrix ADC 拆分通道规则。

默认情况下，Secure Web 的网络访问策略设置为通过通道连接到内部网络。采用此配置时，MDX 应用程序使用 Citrix ADC 拆分通道设置。某些其他移动生产力应用程序网络访问策略默认值有所差别。

Citrix Gateway 还具有 Micro VPN 反向拆分通道模式。此配置支持不通过通道连接到 Citrix ADC 的 IP 地址的排除列表。这些地址通过使用设备 Internet 连接发送。有关反向拆分通道的详细信息，请参阅 Citrix Gateway 文档。

XenMobile 包括一个反向拆分通道排除列表。要防止通过 Citrix Gateway 使用通道连接某些 Web 站点：添加将通过 LAN 连接的完全限定域名 (FQDN) 或 DNS 后缀的列表（以逗号分隔）。Citrix Gateway 配置为使用反向拆分通道时，此列表仅适用于安全浏览模式。

身份验证

January 5, 2022

在 XenMobile 部署中，确定如何配置身份验证时，要考虑多个注意事项。本节将通过以下方面来介绍影响身份验证的各种因素：

- 身份验证涉及的主要 MDX 策略、XenMobile 客户端属性和 Citrix Gateway 设置。
- 这些策略、客户端属性和设置的交互方式。
- 每种选择的权衡因素。

本文还提供了三个提高安全等级的建议配置示例。

一般而言，随着安全性的提高，最佳用户体验会降低，因为用户必须更加频繁地进行身份验证。如何平衡这些考虑因素取决于组织的需求和优先级。通过查看三个建议的配置，您应该可以更加清楚地了解您可用的身份验证措施的作用，以及如何以最佳方式部署您自己的 XenMobile 环境。

身份验证模式

联机身份验证：允许用户访问 XenMobile 网络。需要 Internet 连接。

脱机身份验证：在设备上进行。用户解锁安全保管库并脱机访问一些项目，例如，下载的邮件、缓存的 Web 站点和笔记。

身份验证方法

单因素

LDAP：在 XenMobile 中，可以配置到一个或多个与轻型目录访问协议 (LDAP) 兼容的目录（例如 Active Directory）的连接。这是提供以单点登录 (SSO) 方式访问公司环境的常用方法。您可选择将 Citrix PIN 与 Active Directory 密码缓存组合以改进使用 LDAP 时的用户体验，同时在注册、密码过期和帐户锁定方面仍提供复杂密码的安全方式。

有关更多详细信息，请参阅域或域加 STA。

客户端证书： XenMobile 可以与行业标准证书颁发机构集成以将证书用作联机身份验证的唯一方法。XenMobile 在用户注册后提供此证书，这需要一次性密码、邀请 URL 或 LDAP 凭据。将客户端证书用作主要身份验证方法时，在仅客户端证书环境中需要使用 Citrix PIN 来确保设备上证书的安全。

XenMobile 仅支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，XenMobile 将使用 Citrix ADC 管理吊销。配置基于客户端证书的身份验证时，请考虑是否需要配置 Citrix ADC 证书吊销列表 (CRL) 设置 Enable CRL Auto Refresh（启用 CRL 自动刷新）。此步骤可确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证；XenMobile 将重新颁发新证书，因为 XenMobile 在某个证书被吊销的情况下不限制用户生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

有关显示了您计划对用户使用基于证书的身份验证或您需要使用您的企业证书颁发机构 (CA) 颁发设备证书时所需部署的结构图，请参阅面向本地部署的参考体系结构。

双重

LDAP + 客户端证书：在 XenMobile 环境中，此配置是用于实现安全性和用户体验的最佳解决方案，同时，通过 Citrix ADC 进行的双重身份验证还能提供最佳 SSO 选择和安全。同时使用 LDAP 和客户端证书通过用户知晓的内容（其 Active Directory 密码）和用户拥有的内容（设备上的客户端证书）提供安全性。Secure Mail（以及某些其他移动生产力应用程序）在正确配置的 Exchange 客户端访问服务器环境中可以自动配置，并通过客户端证书身份验证提供无缝首次用户体验。要实现最佳可用性，可以将此选项与 Citrix PIN 和 Active Directory 密码缓存组合在一起。

LDAP + 令牌：此配置允许在使用 RADIUS 协议时采用 LDAP 凭据经典配置以及一次性密码。要实现最佳可用性，可以将此选项与 Citrix PIN 和 Active Directory 密码缓存组合在一起。

身份验证中涉及的重要策略、设置和客户端属性

以下三个建议配置中涉及以下策略、设置和客户端属性：

MDX 策略

应用程序通行码：如果设置为开，应用程序在处于不活动状态一段时间后启动或恢复时需要输入 Citrix PIN 或通行码才能解锁。默认值为开。

要为所有应用程序配置不活动计时器，请在 XenMobile 控制台中的设置选项卡上的客户端属性中设置 INACTIVITY_TIMER 值（分钟）。默认值为 15 分钟。要禁用不活动计时器以便 PIN 或通行码提示仅在应用程序启动时出现，请将值设置为 0。

> 注意：
>
> 如果为“加密密钥”策略选择“安全脱机”，则将自动启用此策略。

要求联机会话：如果设置为开，用户必须连接到企业网络并且具有活动会话，才能访问设备上的应用程序。如果设置为关，则访问设备上的应用程序不需要活动会话。默认值为关。

最长脱机期限 **(**小时**)**：定义应用程序可以运行而不需要从 XenMobile 重新确认应用程序授权并刷新策略的最长期限。当您设置“最长脱机期限”时，如果 Secure Hub for iOS 具有有效 Citrix Gateway 令牌，应用程序将从 XenMobile 为 MDX 应用程序检索新策略，而不会导致用户服务发生任何中断。如果 Secure Hub 没有有效 Citrix ADC 令牌，则用户必须通过 Secure Hub 进行身份验证，然后才能更新应用程序策略。Citrix ADC 令牌可能会由于 Citrix Gateway 会话的不活动状态或强制执行的会话超时策略而变得无效。当用户再次登录 Secure Hub 时，他们可以继续运行应用程序。

将在期限过期前 30 分钟、15 分钟和 5 分钟提醒用户登录。超过时间后，将锁定应用程序，直到用户登录。默认值为 **72** 小时（**3** 天）。最长期限为 1 小时。

> 注意：
>
> 请谨记，在用户经常出差并可能使用国际漫游的情况下，默认值 72 小时（3 天）可能太短。

后台服务票据过期日期：后台网络服务票据保持有效的时间段。当 Secure Mail 通过 Citrix Gateway 连接到运行 ActiveSync 的 Exchange Server 时，XenMobile 会发出一个令牌，Secure Mail 将使用该令牌连接到内部

Exchange Server。此属性设置确定 Secure Mail 可以使用该令牌（无需使用新令牌）进行身份验证并连接到 Exchange Server 的持续时间。超过时间限制后，用户必须重新登录以生成新令牌。默认值为 **168** 小时（**7** 天）。超过此超时值后，将停止邮件通知。

要求联机会话宽限期 **(**分钟**)**：确定“要求联机会话”策略阻止用户进一步脱机使用应用程序（直到验证联机会话）之前，用户可以脱机使用应用程序的分钟数，默认值为 0（无宽限期）。

有关身份验证策略的信息，请参阅：

- 如果使用 MAM SDK：MAM SDK 概述
- 如果使用 MDX Toolkit：适用于 iOS 的 MDX 策略和适用于 Android 的 MDX 策略

XenMobile 客户端属性

> 注意：
>
> 客户端属性是应用于连接到 XenMobile 的所有设备的全局设置。

Citrix PIN：要实现简单点登录体验，您可以选择启用 Citrix PIN。使用 PIN 时，用户不需要重复输入其他凭据，例如 Active Directory 用户名和密码。您可以仅将 Citrix PIN 配置为独立脱机身份验证，也可以将 PIN 与 Active Directory 密码缓存组合在一起以简化身份验证，从而实现最佳可用性。可在 XenMobile 控制台中的设置 **>** 客户端 **>** 客户端属性中配置 Citrix PIN。

下面概述了一些重要属性。有关详细信息，请参阅客户端属性。

ENABLE_PASSCODE_AUTH

显示名称：启用 Citrix PIN 身份验证

此键允许您打开 Citrix PIN 功能。启用 Citrix PIN 或通行码后，系统将提示用户定义要使用的 PIN（而非其 Active Directory 密码）。如果启用了 **ENABLE_PASSWORD_CACHING**，或者如果 XenMobile 使用证书身份验证，您应启用此设置。

可能的值： **true** 或 **false**

默认值： **false**

ENABLE_PASSWORD_CACHING

显示名称：启用用户密码缓存

此键允许您在移动设备本地缓存用户的 Active Directory 密码。当您将此键设置为 true 时，系统将提示用户设置 Citrix PIN 或通行码。当您将此键设置为 **true** 时，必须将 ENABLE_PASSCODE_AUTH 键设置为 true。

可能的值： **true** 或 **false**

默认值： **false**

PASSCODE_STRENGTH

显示名称： PIN 强度要求

此键定义 Citrix PIN 或通行码的强度。更改此设置时，系统将在下次提示用户进行身份验证时提示其设置新 Citrix PIN 或通行码。

可能的值：低、中或强

默认值：中

INACTIVITY_TIMER

显示名称：不活动计时器

此键定义用户可以保持其设备处于不活动状态且之后访问应用程序不会提示输入 Citrix PIN 或通行码的时间（分钟）。要为 MDX 应用程序启用此设置，必须将“应用程序通行码”设置设为开。如果“应用程序通行码”设置设为关，用户将被重定向到 Secure Hub 以执行完全身份验证。更改此设置时，该值将在系统下次提示用户进行身份验证时生效。默认值为 15 分钟。

ENABLE_TOUCH_ID_AUTH

显示名称：启用 Touch ID 身份验证

允许在脱机身份验证时使用指纹读取器（仅限 iOS）。联机身份验证仍需要使用主要身份验证方法。

ENCRYPT_SECRETS_USING_PASSCODE

显示名称：使用通行码加密机密

此键允许将敏感数据存储在移动设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串。此配置键允许对密钥进行强加密，但还会添加用户熵（用户生成的只有自己知道的随机 PIN 代码）。

可能的值： **true** 或 **false**

默认值： **false**

Citrix ADC 设置

会话超时：如果启用此设置，则 Citrix ADC 在指定的时间间隔内未检测到任何网络活动时，Citrix Gateway 将断开会话。对于通过 Citrix Gateway 插件、Citrix Receiver、Secure Hub 或通过 Web 浏览器连接的用户，强制执行此设置。默认值为 **1440** 分钟。如果将此值设置为零，则该设置处于禁用状态。

强制超时：如果启用此设置，则超过超时时间间隔后，无论用户正在执行什么操作，Citrix Gateway 都将断开会话。超过超时时间间隔后，用户无法执行任何操作来阻止断开。对于通过 Citrix Gateway 插件、Citrix Receiver、Secure Hub 或通过 Web 浏览器连接的用户，强制执行此设置。如果 Secure Mail 使用 STA（一种特殊 Citrix ADC 模式），则“强制超时”设置不应用于 Secure Mail 会话。默认值为 **1440** 分钟。如果将此值留空，则该设置处于禁用状态。

有关 Citrix Gateway 中的超时设置的详细信息，请参阅 Citrix ADC 文档。

有关提示用户在其设备上输入凭据以在 XenMobile 中执行身份验证的情景的详细信息，请参阅身份验证提示情景。

默认配置设置

这些设置是由以下对象提供的默认设置：

- 适用于 XenMobile 的 NetScaler 向导
- MAM SDK 或 MDX Toolkit
- XenMobile 控制台

设置	设置的查找位置	默认设置
会话超时	Citrix Gateway	1440 分钟
强制超时	Citrix Gateway	1440 分钟
最长脱机期限	MDX 策略	72 小时
后台服务票据过期日期	MDX 策略	168 小时（7 天）
要求联机会话	MDX 策略	关
要求联机会话宽限期	MDX 策略	0
应用程序通行码	MDX 策略	开
使用通行码加密机密	XenMobile 客户端属性	false
启用 Citrix PIN 身份验证	XenMobile 客户端属性	false
PIN 强度要求	XenMobile 客户端属性	中
PIN 类型	XenMobile 客户端属性	数字
启用用户密码缓存	XenMobile 客户端属性	false
不活动计时器	XenMobile 客户端属性	15
启用 Touch ID 身份验证	XenMobile 客户端属性	false

建议的配置

本节提供的三个 XenMobile 配置示例是从最低安全性和最佳用户体验到最高安全性和干扰较多的用户体验。这些示例应该可为您在考虑如何在自己的配置中权衡这些因素时提供有用的参考要点。请注意，如果修改这些设置，可能也需要更改其他设置。例如，最长脱机期限应该始终为小于会话超时。

最高安全性

此配置提供最高安全级别，但可用性显著降低。

设置	设置的查找位置	建议设置	行为影响
会话超时	Citrix Gateway	1440	仅当要求进行联机身份验证时，用户输入其 Secure Hub 凭据 - 每 24 小时一次。
强制超时	Citrix Gateway	1440	严格要求每 24 小时进行一次联机身份验证。活动不会延长会话生存期。
最长脱机期限	MDX 策略	23	要求每天刷新策略。
后台服务票据过期日期	MDX 策略	72 小时	STA 超时，允许在没有 Citrix Gateway 会话令牌的情况下进行长时间会话。对于 Secure Mail，使 STA 超时长于会话超时可避免当用户在会话过期之前没有打开应用程序的情况下，邮件通知停止，但未提示用户。
要求联机会话	MDX 策略	关	确保存在有效的网络连接和 Citrix Gateway 会话以使用应用程序。
要求联机会话宽限期	MDX 策略	0	无宽限期（如果启用了“要求联机会话”）。
应用程序通行码	MDX 策略	开	需要应用程序的通行码。
使用通行码加密机密	XenMobile 客户端属性	true	从用户熵派生的密钥保护保管库。
启用 Citrix PIN 身份验证	XenMobile 客户端属性	true	启用 Citrix PIN 以实现简化的身份验证体验。
PIN 强度要求	XenMobile 客户端属性	强	高密码复杂性要求。
PIN 类型	XenMobile 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	XenMobile 客户端属性	false	不缓存 Active Directory 密码，使用 Citrix PIN 进行脱机身份验证。

不活动计时器	XenMobile 客户端属性	15	如果在此时间段内用户未使用 MDX 应用程序或 Secure Hub，则提示进行脱机身份验证。
启用 Touch ID 身份验证	XenMobile 客户端属性	false	在 iOS 中对脱机身份验证用例禁用 Touch ID。

更高的安全性

比较均衡的方法，此配置要求用户更加频繁地（最多每 3 天一次，而不是 7 天）进行身份验证，安全性较高。身份验证次数增加会增加锁定容器的频率，以确保设备未在使用时的数据安全性。

设置	设置的查找位置	建议设置	行为影响
会话超时	Citrix Gateway	4320	仅当要求进行联机身份验证时，用户输入其 Secure Hub 凭据 - 每 3 天一次。
强制超时	Citrix Gateway	无值	如果存在任何活动，将延长会话。
最长脱机期限	MDX 策略	71	要求每 3 天刷新一次策略。在会话超时之前，允许刷新时间存在小时级差异。
后台服务票据过期日期	MDX 策略	168 小时	STA 超时，允许在没有 Citrix Gateway 会话令牌的情况下进行长时间会话。对于 Secure Mail，使 STA 超时长于会话超时可避免当用户在会话过期之前没有打开应用程序的情况下，邮件通知停止，但未提示用户。
要求联机会话	MDX 策略	关	确保存在有效的网络连接和 Citrix Gateway 会话以使用应用程序。

要求联机会话宽限期	MDX 策略	0	无宽限期（如果启用了“要求联机会话”）。
应用程序通行码	MDX 策略	开	需要应用程序的通行码。
使用通行码加密机密	XenMobile 客户端属性	false	不需要使用用户熵来加密保管库。
启用 Citrix PIN 身份验证	XenMobile 客户端属性	true	启用 Citrix PIN 以实现简化的身份验证体验。
PIN 强度要求	XenMobile 客户端属性	中	强制执行中等密码复杂性规则。
PIN 类型	XenMobile 客户端属性	数字	PIN 是一个数字序列。
启用密码缓存	XenMobile 客户端属性	true	用户 PIN 缓存和保护 Active Directory 密码。
不活动计时器	XenMobile 客户端属性	30	如果在此时间段内用户未使用 MDX 应用程序或 Secure Hub，则提示进行脱机身份验证。
启用 Touch ID 身份验证	XenMobile 客户端属性	true	在 iOS 中对脱机身份验证用例启用 Touch ID。

高安全性

此配置提供基本级别的安全性，对用户来说最方便。

设置	设置的查找位置	建议设置	行为影响
会话超时	Citrix Gateway	10080	仅当要求进行联机身份验证时，用户输入其 Secure Hub 凭据 - 每 7 天一次
强制超时	Citrix Gateway	无值	如果存在任何活动，将延长会话。

最长脱机期限	MDX 策略	167	要求每周（每 7 天）刷新一次策略。在会话超时之前，允许刷新时间存在小时级差异。
后台服务票据过期日期	MDX 策略	240	STA 超时，允许在没有 Citrix Gateway 会话令牌的情况下进行长时间会话。对于 Secure Mail，使 STA 超时长于会话超时可避免当用户在会话过期之前没有打开应用程序的情况下，邮件通知停止，但未提示用户。
要求联机会话	MDX 策略	关	确保存在有效的网络连接和 Citrix Gateway 会话以使用应用程序。
要求联机会话宽限期	MDX 策略	0	无宽限期（如果启用了“要求联机会话”）。
应用程序通行码	MDX 策略	开	需要应用程序的通行码。
使用通行码加密机密	XenMobile 客户端属性	false	不需要使用用户熵来加密保管库。
启用 Citrix PIN 身份验证	XenMobile 客户端属性	true	启用 Citrix PIN 以实现简化的身份验证体验。
PIN 强度要求	XenMobile 客户端属性	低	无密码复杂性要求
PIN 类型	XenMobile 客户端属性	数字	PIN 是一个数字序列。
启用密码缓存	XenMobile 客户端属性	true	用户 PIN 缓存和保护 Active Directory 密码。
不活动计时器	XenMobile 客户端属性	90	如果在此时间段内用户未使用 MDX 应用程序或 Secure Hub，则提示进行脱机身份验证。
启用 Touch ID 身份验证	XenMobile 客户端属性	true	在 iOS 中对脱机身份验证用例启用 Touch ID。

使用递升式身份验证

某些应用程序可能需要增强的身份验证（例如，令牌或主动会话超时等辅助身份验证因素）。您可以通过 MDX 策略控制此身份验证方法。此方法还需要一个单独的虚拟服务器来控制身份验证方法（在相同或不同的 Citrix ADC 设备上）。

设置	设置的查找位置	建议设置	行为影响
备用 Citrix Gateway	MDX 策略	需要辅助 Citrix ADC 设备的 FQDN 和端口。	允许通过辅助 Citrix ADC 设备身份验证和会话策略控制增强的身份验证。

如果登录备用 Citrix Gateway 实例的用户打开某个应用程序，则所有其他应用程序都将使用该 Citrix Gateway 实例与内部网络进行通信。仅当与具有增强安全性的 Citrix Gateway 实例的会话超时后，会话才会切换回安全性较低的 Citrix Gateway 实例。

使用 **“**要求联机会话**”**

对于某些应用程序（例如 Secure Web），您可能希望确保用户仅在具有经过身份验证的会话且设备已连接到网络时运行应用程序。此策略强制执行该方式，并允许有一个宽限期以便用户可以完成其工作。

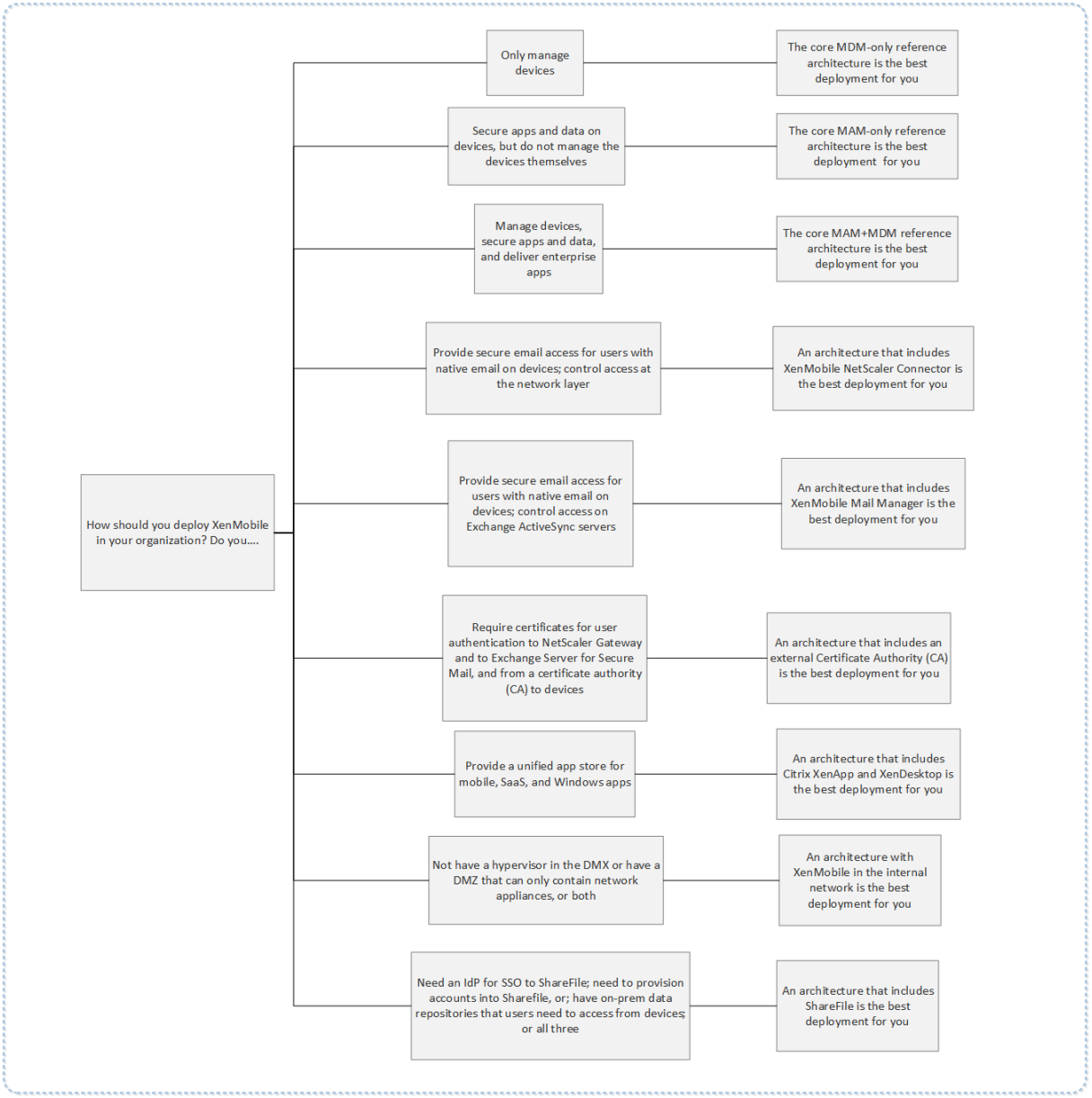
设置	设置的查找位置	建议设置	行为影响
要求联机会话	MDX 策略	开	确保设备处于联机状态，并具有有效的身份验证令牌。
要求联机会话宽限期	MDX 策略	15	允许在用户无法继续使用应用程序之前有 15 分钟的宽限期

面向本地部署的参考体系结构

January 5, 2022

本文中的图表说明了面向本地 XenMobile 部署的参考体系结构。部署场景包括仅 MDM、仅 MAM 和 MDM+MAM 作为核心体系结构，以及包括 SNMP 管理器、适用于 Exchange ActiveSync 的 Citrix Gateway 连接器、适用于 Exchange ActiveSync 的 Endpoint Management 连接器、以及 Virtual Apps and Desktops 等组件的部署场景。这些图表显示了 XenMobile 所需的最小组件。

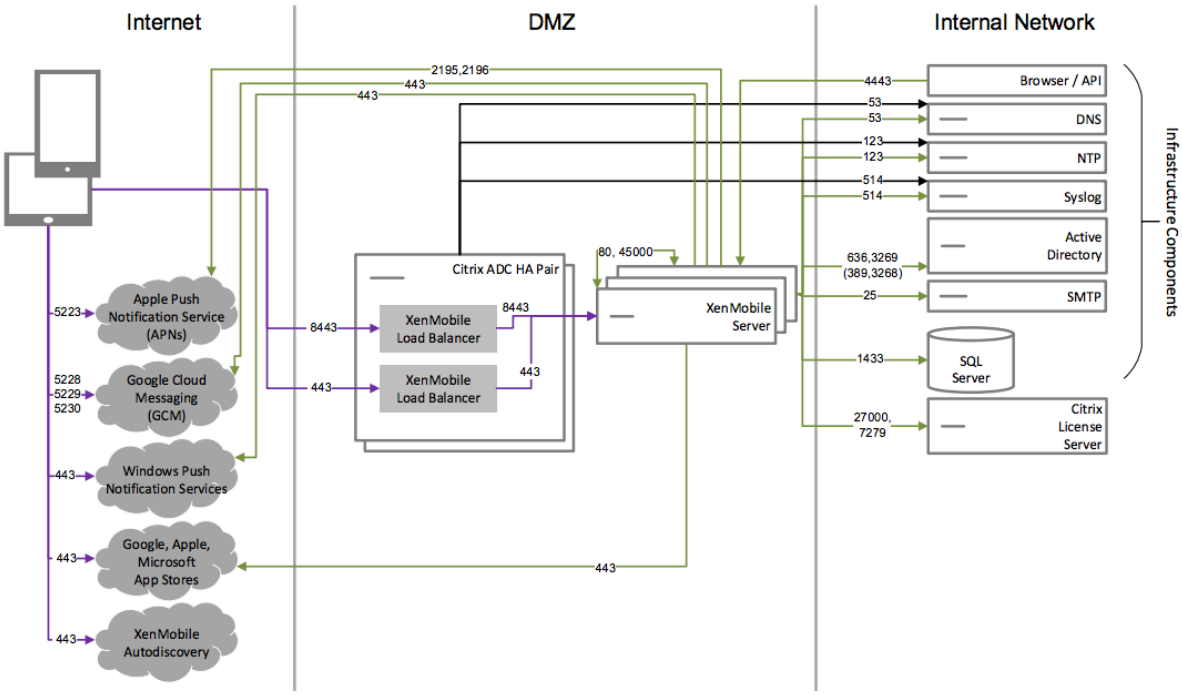
请使用此图表作为您的部署决策的一般性指南。



在这些图表中，连接器上面的数字表示要允许组件之间进行通信必须打开的端口。有关完整的端口列表，请参阅 XenMobile 文档中的端口要求。

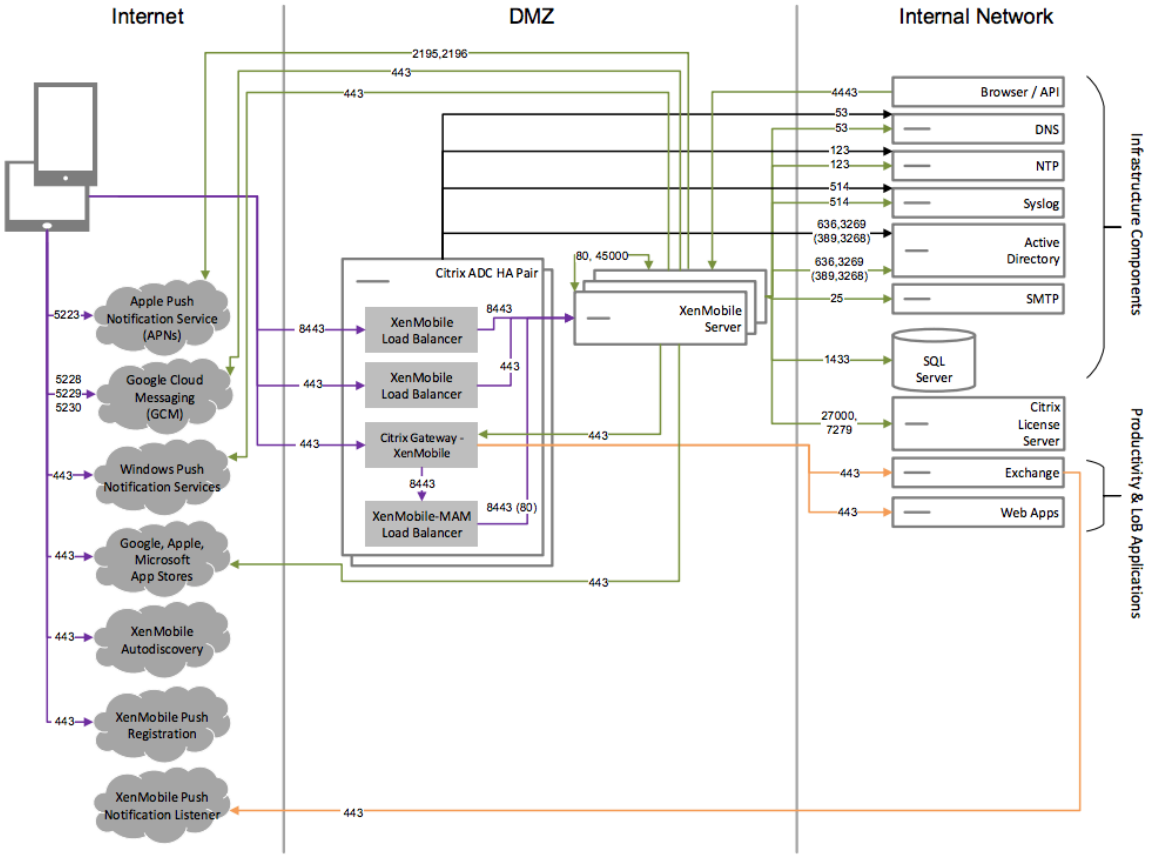
核心仅 **MDM** 参考体系结构

如果您计划只使用 XenMobile 的 MDM 功能，请部署此体系结构。例如，您需要通过 MDM 管理企业所发放的设备以部署设备策略、应用程序，以及检索资产清单，并且能够在设备上进行擦除操作（例如设备擦除）。



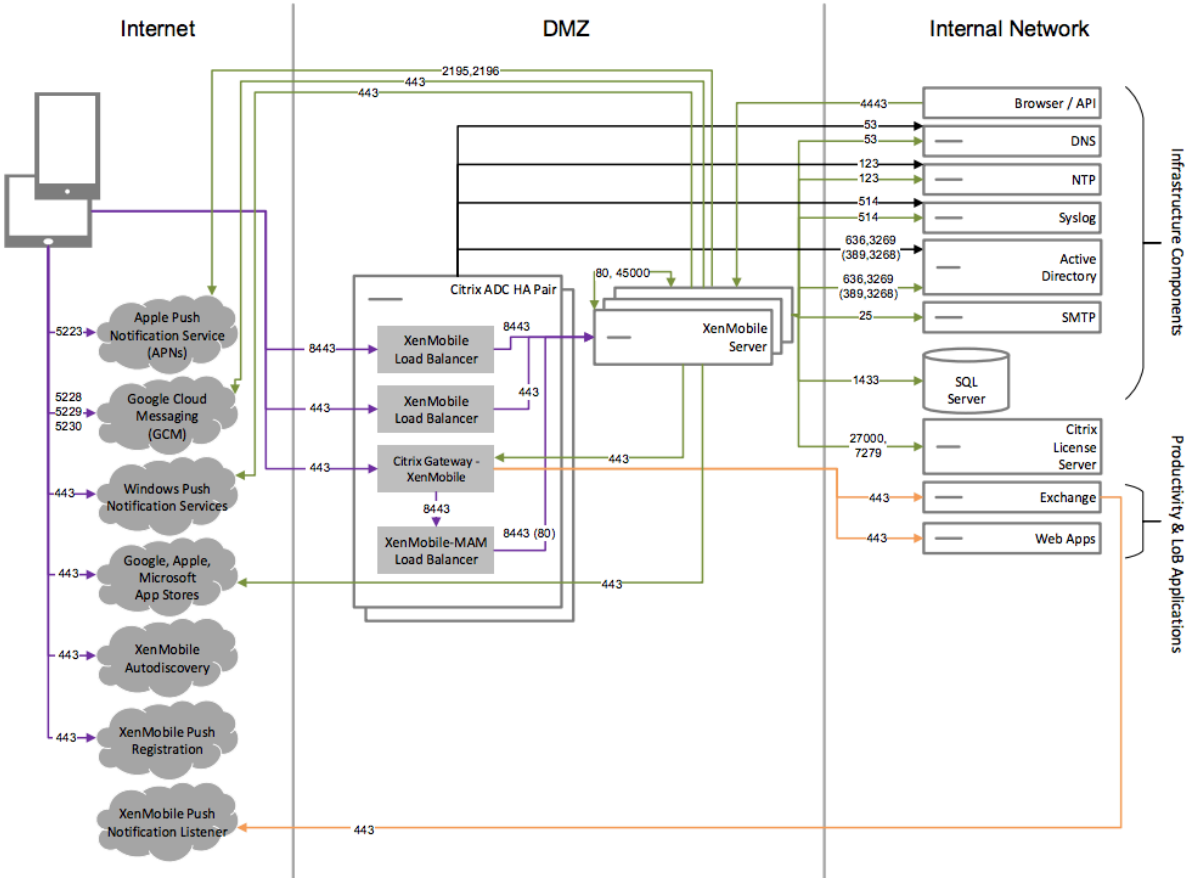
核心仅 **MAM** 参考体系结构

如果您计划只使用 XenMobile 的 MAM 功能而不要求设备进行 MDM 注册，请部署此体系结构。例如，需要在 BYO 移动设备上保护应用程序和数据；需要提供企业移动应用程序并且能够锁定应用程序和擦除其数据。设备不能进行 MDM 注册。



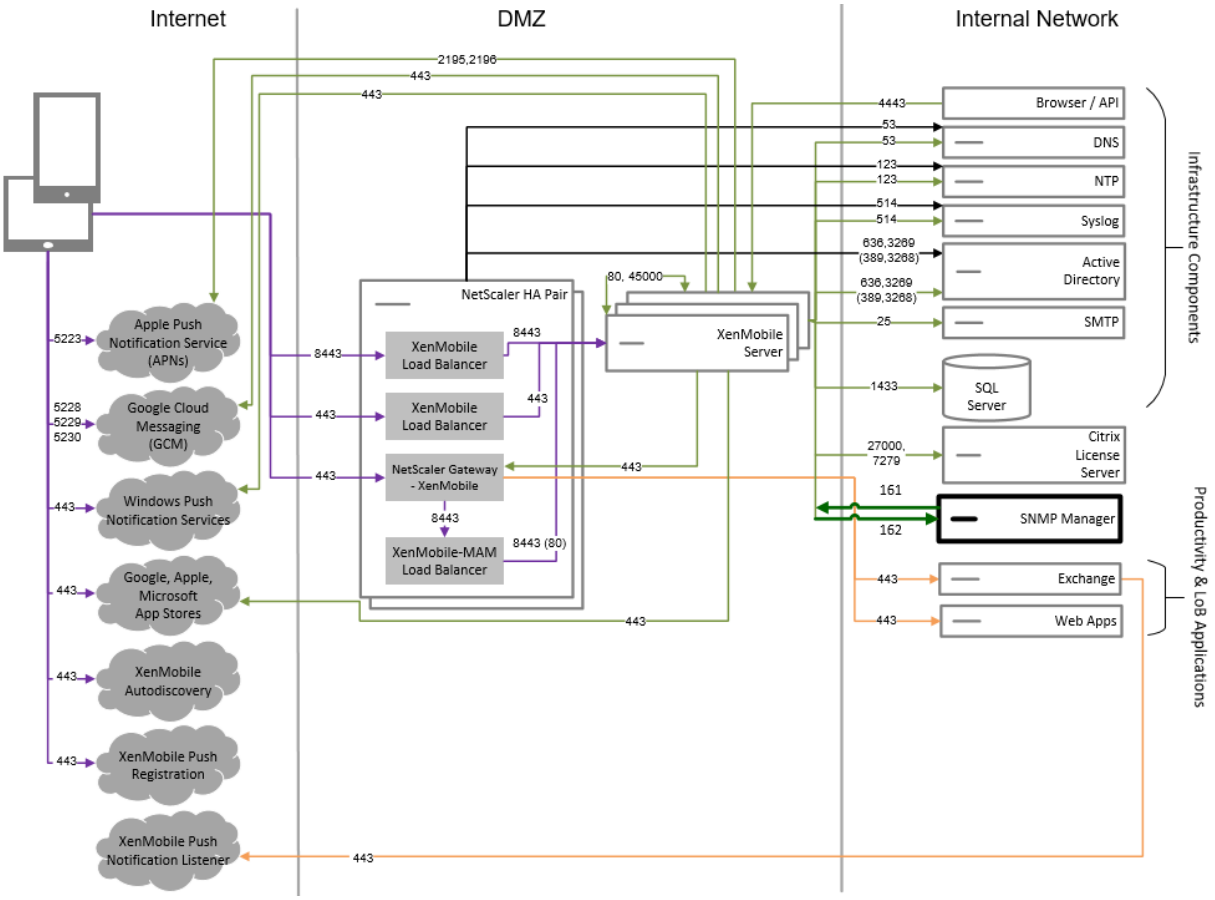
核心 **MAM+MDM** 参考体系结构

如果您计划使用 XenMobile 的 MDM+MAM 功能，请部署此体系结构。例如，希望通过 MDM 管理企业所发放的设备；希望部署设备策略和应用程序以及检索资产清单，并且能够擦除设备。您还需要提供企业移动应用程序并且能够锁定应用程序和擦除设备上的数据。



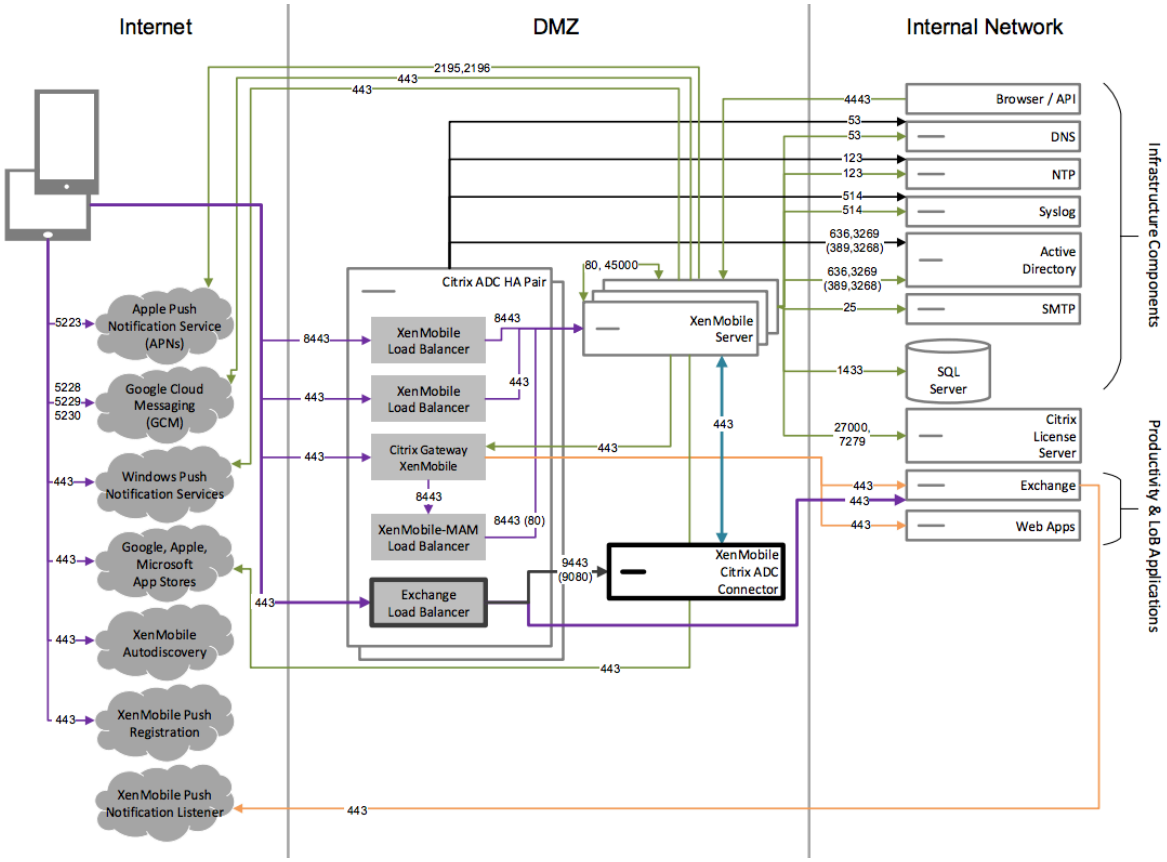
面向 **SNMP** 的参考体系结构

如果要在 XenMobile 中启用 SNMP 监视，请部署此体系结构。例如，如果希望允许监视系统以查询和获取与您的 XenMobile 节点有关的信息。有关详细信息，请参阅 SNMP 监视。



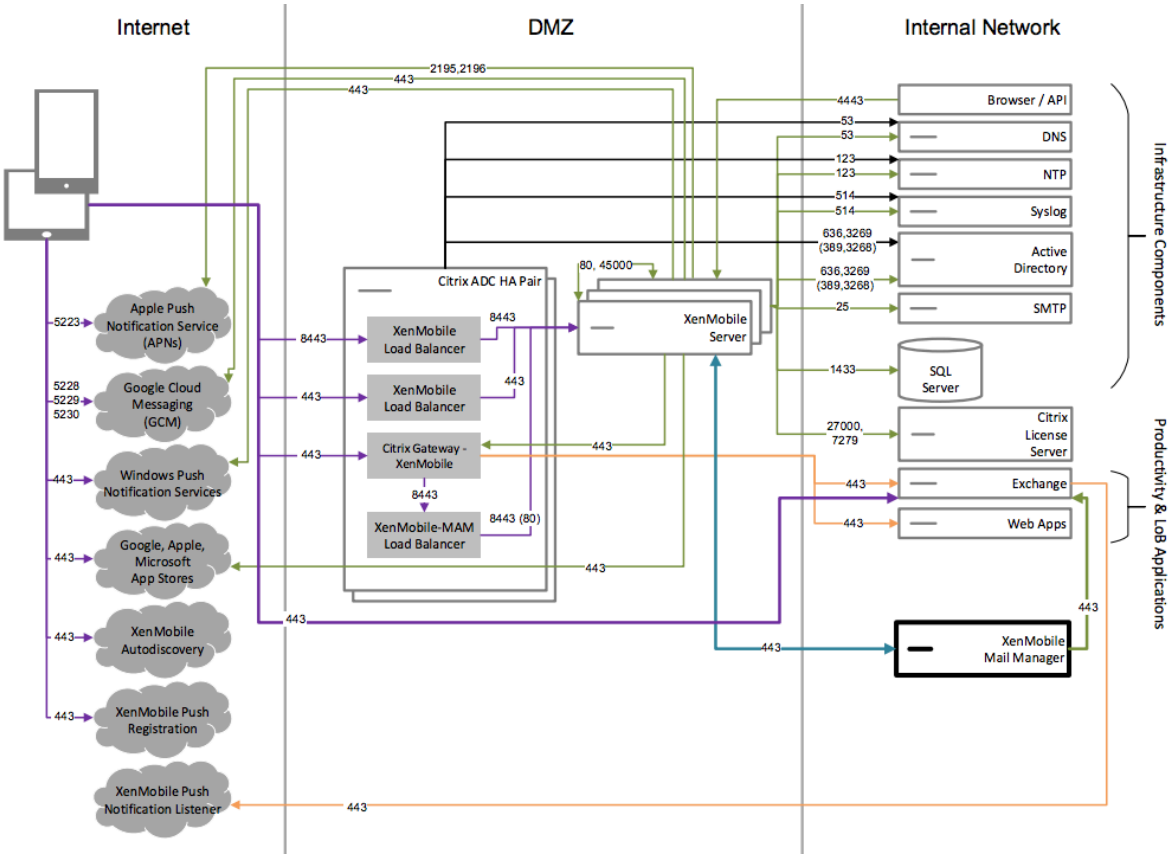
面向适用于 **Exchange ActiveSync** 的 **Citrix Gateway** 连接器的参考体系结构

如果您计划将适用于 Exchange ActiveSync 的 Citrix Gateway 连接器与 XenMobile 结合使用，请部署此体系结构。例如，您需要向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权限。这些用户将继续通过本机应用程序访问电子邮件，或者您可能会逐渐将其过渡到 Citrix Secure Mail。访问控制需要在流量到达 Exchange ActiveSync 服务器之前在网络层发生。即使图表显示了在 MDM 和 MAM 体系结构中部署的适用于 Exchange ActiveSync 的连接器，您也可以通过相同的方式作为仅 MDM 体系结构的一部分部署适用于 Exchange ActiveSync 的连接器。



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

如果您计划将适用于 Exchange ActiveSync 的 Endpoint Management 连接器与 XenMobile 结合使用，请部署此体系结构。例如，您希望向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权限。这些用户将继续通过本机应用程序访问电子邮件，或者您可能会逐渐将用户过渡到 Secure Mail。可以在 Exchange ActiveSync 服务器上实现访问控制。虽然图表显示了在 MDM 和 MAM 体系结构中部署的适用于 Exchange ActiveSync 的 Endpoint Management 连接器，但是您也可以通过相同的方式作为仅 MDM 体系结构的一部分部署适用于 Exchange ActiveSync 的 Endpoint Management 连接器。

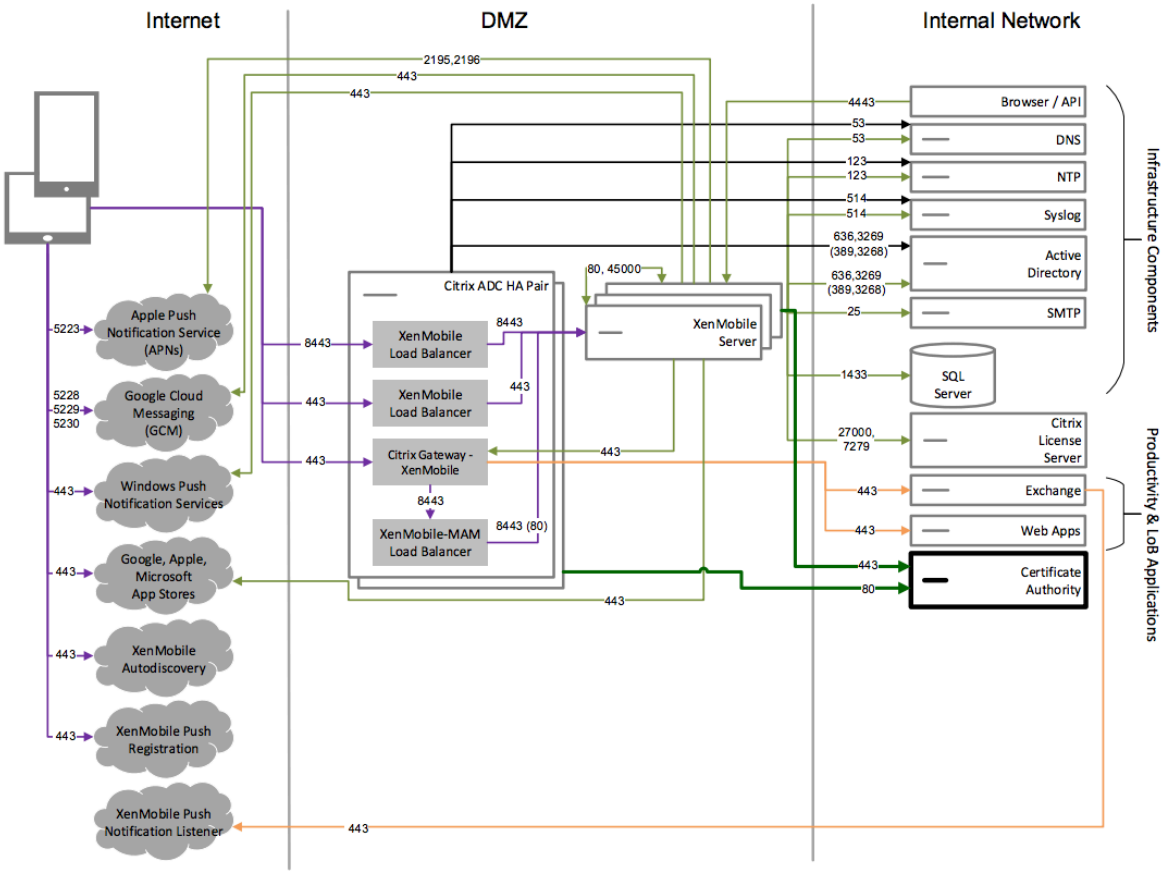


面向外部证书颁发机构的参考体系结构

建议包括外部证书颁发机构的部署满足下面一个或多个要求：

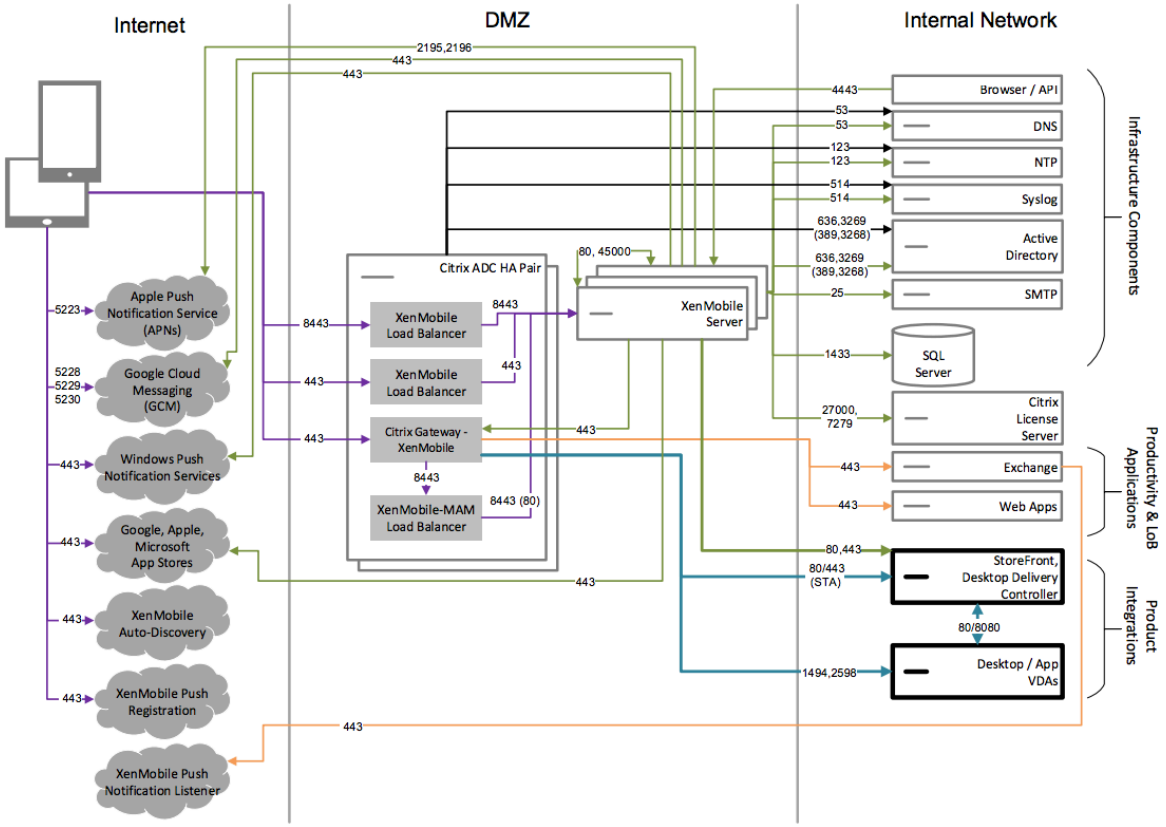
- 您需要使用用户证书进行用户身份验证以登录 Citrix Gateway（适用于 Intranet 访问）。
- 您要求 Secure Mail 用户使用用户证书进行身份验证以登录 Exchange Server。
- 例如，您需要将贵公司的证书颁发机构颁发的证书推送到移动设备以通过 WiFi 进行访问。

虽然图表显示了在 MDM+MAM 体系结构中部署的外部证书颁发机构，但是您也可以以相同的方式作为仅 MDM 或仅 MAM 体系结构的一部分部署外部证书颁发机构。



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

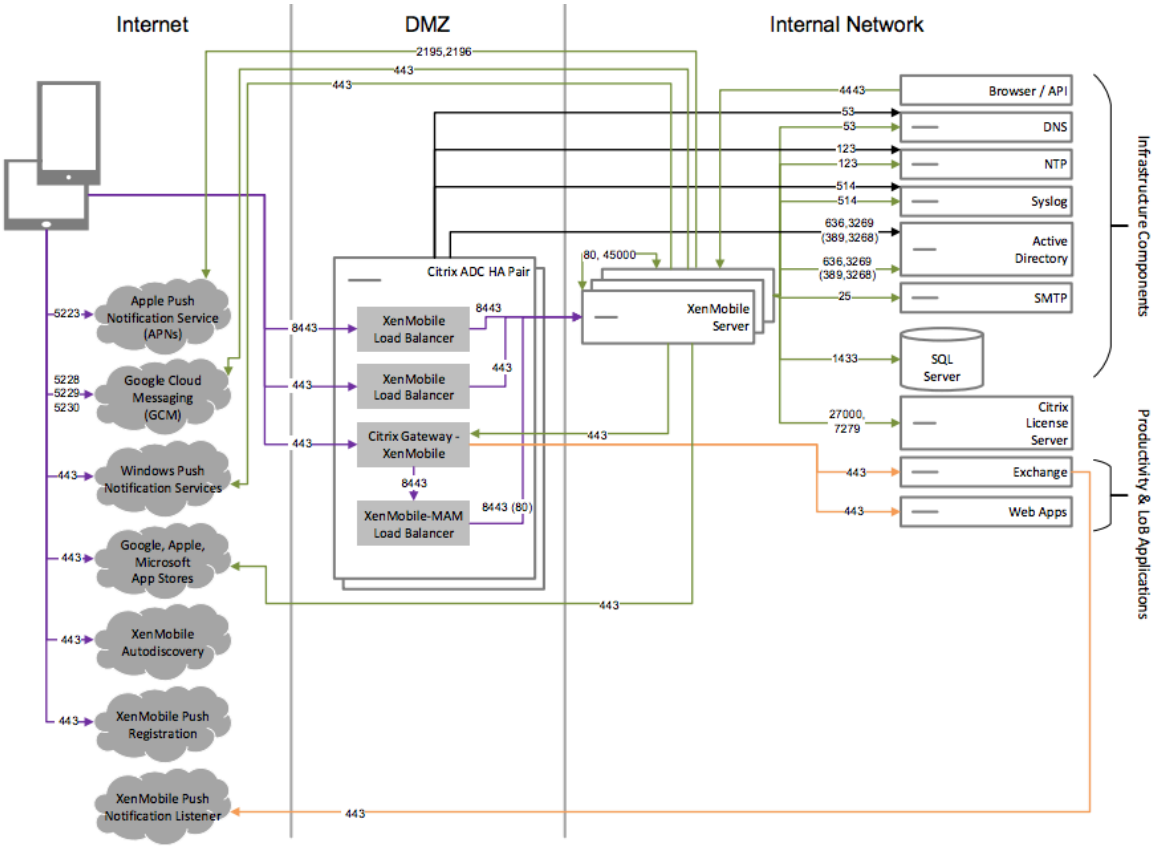
如果计划将 Virtual Apps and Desktops 与 XenMobile 相集成，请部署此体系结构。例如，对于所有类型的应用程序（移动应用程序、SaaS 应用程序和 Windows 应用程序），需要向移动用户提供统一的应用商店。虽然图表显示了在 MDM 和 MAM 体系结构中部署的 Virtual Desktops，但是您也可以以相同的方式作为仅 MAM 体系结构的一部分部署这些桌面。



面向内部网络中的 **XenMobile** 的参考体系结构

可以在内部网络中部署适用于 XenMobile 的体系结构，以满足下面一个或多个要求：

- 您在 DMZ 中未安装或不允许您安装虚拟机管理程序。
- 您的 DMZ 只能包含网络设备。
- 您的安全要求需要使用 SSL 卸载功能。



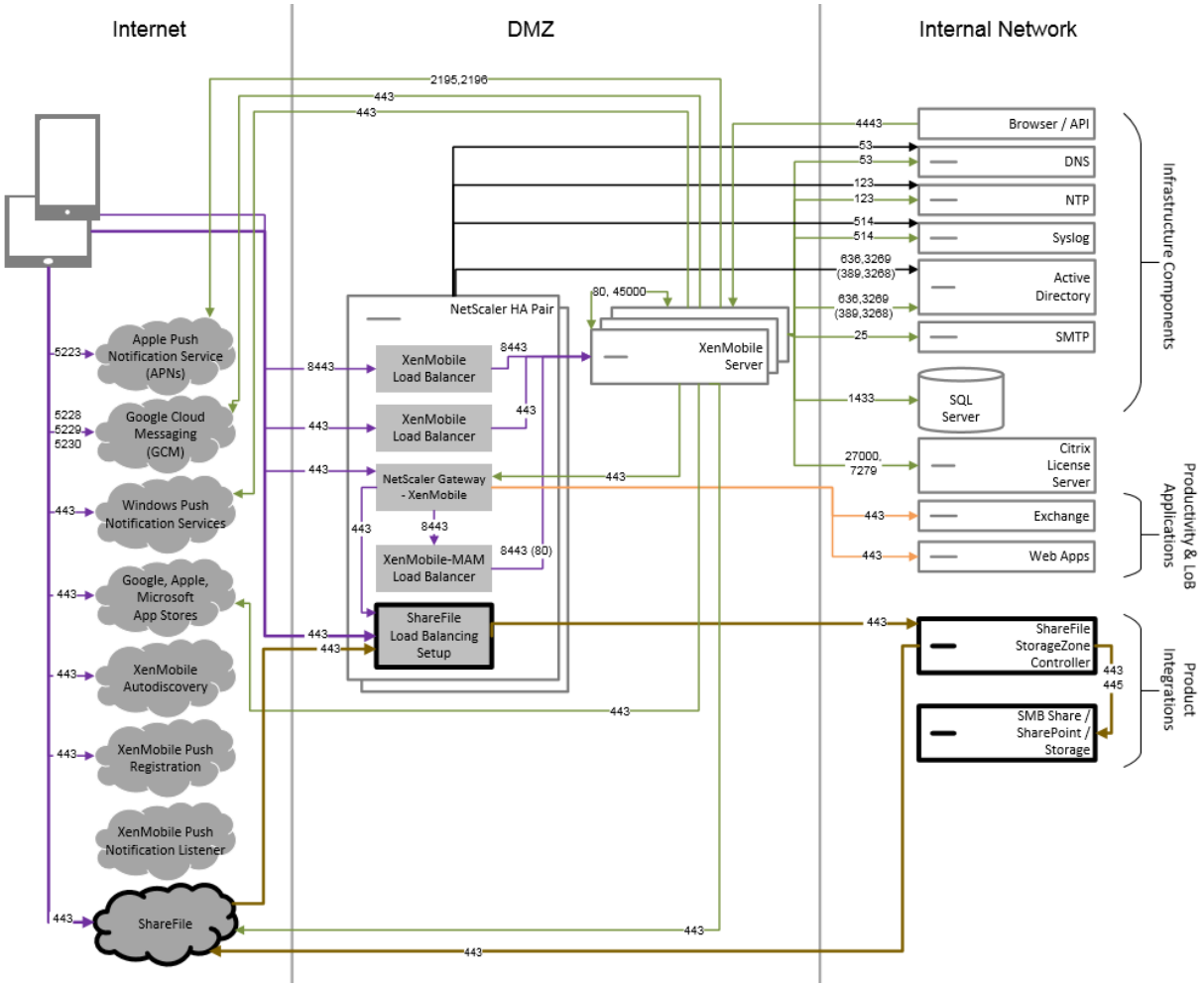
面向 **Citrix Content Collaboration** 的参考体系结构

如果希望集成 Citrix Files 或者仅将存储区域连接器与 XenMobile 相集成，请部署此体系结构。通过 Citrix Files 集成，您可以满足下面一个或多个要求：

- 需要 IDP 以向用户授予单点登录 (SSO) 到 ShareFile.com 的权限。
- 需要在 ShareFile.com 中预配帐户的方法。
- 具有需要从移动设备访问的本地数据存储库。

仅与存储区域连接器的集成向用户提供了对现有本地存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问权限。在此配置中，您不需要设置 Citrix Content Collaboration 子域、将用户预配到 Citrix Files 或托管 Citrix Files 数据。

虽然图表显示了在 MDM+MAM 体系结构中部署的 Citrix Files，但是您也可以以相同的方式作为仅 MAM 体系结构的一部分部署 Citrix Files。



服务器属性

October 13, 2021

服务器属性是适用于跨整个 XenMobile 实例的操作、用户和设备的全局属性。Citrix 建议评估您的环境中设置的本文中介绍的服务器属性。更改其他服务器属性之前，请务必咨询 Citrix。

更改某些服务器属性后需要重新启动每个 XenMobile Server 节点。需要重新启动时，XenMobile 会向您发出通知。

某些服务器属性有助于提高性能和稳定性。有关详细信息，请参阅调整 XenMobile 操作。

将旧版 **Android** 应用程序交付到 **Android Enterprise** 设备：如果将 `afw.allow.legacy.apps` 设置为 **`true`**，则 Android Enterprise 设备会同时接收旧版 Android 应用程序和 Android Enterprise 应用程序。如果为 **`false`**，Android Enterprise 设备将仅接收 Android Enterprise 应用程序。默认值为 **`true`**。

允许文件策略的文件扩展名：通过管理员可以使用“文件设备”策略进行上载的文件类型的逗号分隔列表来配置 `file.extension.whitelist`。无法上载以下文件类型，即使您将其添加到此允许列表中也是如此：

- .cab
- .appx
- .ipa
- .apk
- .xap
- .mdx
- .exe

默认值为 7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,sh,tcl,txt,htm,html,doc,docx,rtf,xap。

访问托管 **Google Play** 应用商店中的所有应用程序。如果设置为 **true**，XenMobile 将使公共 Google Play 应用商店中的所有应用程序可从托管 Google Play 应用商店访问。将此属性设置为 **true** 会将所有 Android Enterprise 用户的公共 Google Play 应用商店应用程序列入允许列表。然后，管理员可以使用限制设备策略来控制对这些应用程序的访问。默认值为 **false**。

Android Enterprise 企业拥有的设备上的工作配置文件注册。将 afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled 设置为 **true** 时，运行 Android 11 或更高版本的设备可以在企业拥有的设备上的工作配置文件 (WPCOD) 模式下注册。XenMobile Server 控制台会反映此注册模式的变化。如果设置为 **false**，则没有可用的 WPCOD 设置。默认值为 **true**。

其他 **Android Enterprise** 限制设置。如果将此属性 afw.restriction.policy.v2 设置为 **true**，则以下限制设置适用于 Android Enterprise 设备：

- 允许卸载应用程序
- 允许蓝牙共享

有关这些设置的详细信息，请参阅限制设备策略。

COPE 设备的 **Android Enterprise** 限制。将 afw.restriction.cope 设置为 **true** 以在限制设备策略中启用适用于具有工作配置文件/企业拥有的设备上的工作配置文件的完全托管设备。默认值为 **true**。有关此设置的详细信息，请参阅限制设备策略。

Allow hostnames for iOS App Store links（允许使用 iOS App Store 链接对应的主机名）：属性 ios.app.store.allowed.hostnames 是使用公共 API 将公共应用商店应用程序上载到服务器时使用的允许的主机名列表。如果您计划使用公共 API 上载公共应用商店应用程序，而非通过服务器上载应用程序，请配置此属性。默认值为 itunes.apple.com,vpp.itunes.apple.com,apps.apple.com。

备用 **APN** 端口。可以使用端口 2197 代替端口 443 来发送和接收来自 api.push.apple.com 的 APN 通知。该端口使用基于 HTTP/2 的 APNs 提供程序 API。将属性 apns.http2.alternate.port.enabled 设置为 **true** 以使用端口 2197。服务器属性 apns.http2.alternate.port.enabled 的默认值为 **false**。

启用密码验证以防止本地用户使用弱密码。如果将 enable.password.strength.validation 设置为 **true**，则无法添加使用弱密码的本地用户。如果设置为 **false**，您可以使用公共 API 创建使用弱密码的本地用户。默认值为 **true**。

阻止注册已获得 **Root** 权限的 **Android** 设备和已越狱的 **iOS** 设备：此属性设置为 **true** 时，XenMobile 将阻止注册已获得 Root 权限的 Android 设备和已越狱的 iOS 设备。默认值为 **true**。对于所有安全级别，建议的设置为 **true**。

需要注册： `wsapi.mdm.required.flag`（仅在 XenMobile Server 模式设置为 ENT 时适用）指定是否要求用户在 MDM 中注册。此属性适用于 XenMobile 实例的所有用户和设备。要求注册可提供更高级别的安全性。但是，该决定取决于您是否需要 MDM。默认情况下，不需要注册。

此属性设置为 **false** 时，用户可以拒绝注册，但是仍然会通过 XenMobile Store 访问其设备上的应用程序。此属性设置为 **true** 时，拒绝注册的任何用户都将被拒绝访问任何应用程序。

如果您在用户注册后更改了此属性，用户必须重新注册。

有关是否要求 MDM 注册的讨论，请参阅设备管理和 MDM 注册。

Remember me（启用多模式注册）：属性 `enable.multimode.xms` 允许您在一个同时控制 Android 和 iOS 设备的设备和应用程序管理的注册设置的 XenMobile Server 上创建注册配置文件。此外，新的增强注册配置文件功能允许注册 Android 的专用设备，以及适用于 Android 和 iOS 设备的仅 MAM 注册。如果此属性为 **false**，则在设置注册配置文件时，这些注册选项将不可用。默认值为 **true**。如果将属性更改为 **false**，在此属性设置为 **true** 时注册的设备仍可使用。

Enable the Self-Help Portal（启用自助服务门户）：如果 `shp.console.enable` 设置为 **false**，则禁止访问自助服务门户。导航到端口 443 上的自助服务门户的用户会收到 404 错误。导航到端口 4443 上的门户的用户会收到“拒绝被访问”消息。如果设置为 **true**，则提供通过端口 443 访问自助服务门户的权限。默认值为 **false**。

Local user account lockout limit（本地用户帐户锁定限制）：使用限制策略，您可以为 Active Directory 用户设置登录尝试限制。使用密钥 `local.user.account.lockout.limit` 对本地用户帐户执行相同的操作。用户尝试按照登录指定的次数后，一段时间之后才能再次尝试。使用 **Local user account lockout time**（本地用户帐户锁定时间）属性配置该时间。默认值为 6。

Local user account lockout time(本地用户帐户锁定时间)：属性 `local.user.account.lockout.time` 允许您设置在锁定的本地用户帐户能够尝试重新登录之前必须经过的分钟数。默认值为 30 分钟。

Maximum size of file upload restriction enabled（启用了文件上载的最大大小限制的最大大小）：启用将上载文件的最大大小限制设置 `max.file.size.upload.restriction` 设置为 **true**。如果启用此限制，请使用 `max.file.size.upload.allowed` 配置最大文件大小。此属性的默认值为 **true**。

Maximum size of file upload allowed（允许的文件上载的最大大小）：使用 `max.file.size.upload.allowed`，您可以指定任何上载的最大文件大小。示例值包括 `500 B`、`1 KB`、`1 MB`、`1 MiB`、`1 G` 或 `1 GiB`。默认值为 `5 MB`。

不活动超时 **(**分钟**)**：XenMobile 注销使用 XenMobile Server 公共 API 访问 XenMobile 控制台或任何第三方应用程序的不活动用户之前等待的分钟数。超时值 `0` 表示不活动的用户保持登录状态。对于访问该 API 的第三方应用程序，通常有必要保持登录状态。默认值为 5。

如有需要，**iOS** 设备管理注册将安装根 **CA**：Apple 的最新注册工作流程要求用户手动安装 MDM 配置文件。该工作流程不适用于在 Apple 商务管理或 Apple 校园教务管理中分配的服务器中的 MDM 注册。但是，在 MDM 中手动注册时，iOS 设备用户在注册过程中将仅收到 MDM 设备证书提示。

要在手动注册过程中提供更加优异的用户体验，Citrix 建议将服务器属性从 `ios.mdm.enrollment.installRootCaIfRequired` 更改为 **`false`**。默认值为 **`true`**。执行该变更后，Safari 窗口将在 MDM 注册过程中打开，以简化用户的配置文件安装过程。

VPP 基准时间间隔：属性 `vpp.baseline` 设置 XenMobile 从 Apple 重新导入批量购买许可证的最小时间间隔。刷新许可证信息可确保 XenMobile 反映所有更改，例如，手动从批量购买中删除导入的应用程序时。默认情况下，XenMobile 按每 `1440` 分钟的最小时间间隔为基准刷新批量购买许可证。

如果您安装了许多批量购买许可证（例如，超过 50000）：Citrix 建议增加基准时间间隔以降低导入许可证的开销。如果您预计 Apple 会频繁更改批量购买许可证，Citrix 建议降低该值以使更改及时更新到 XenMobile 中。两个基准之间的最小时间间隔为 60 分钟。由于 cron 作业每 60 分钟运行一次，如果批量购买基准时间间隔为 60 分钟，则基准之间的时间间隔可能会最长延迟 119 分钟。

XenMobile MDM 自助服务门户控制台的最长不活动时间间隔 **(**分钟**)**：此属性名称反应较旧的 XenMobile 版本。此属性控制 XenMobile 控制台的最大不活动时间间隔。该时间间隔是 XenMobile 从 XenMobile 控制台注销不活动用户之前的分钟数。超时值 0 表示不活动的用户保持登录状态。默认值为 `30`。

设备和应用程序策略

January 5, 2022

通过 XenMobile 设备和应用程序策略，可以在多种因素之间实现最佳平衡，例如：

- 企业安全性
- 公司数据和资产保护
- 用户隐私
- 高效、积极的用户体验

这些因素之间的最佳平衡点可能有所差别。例如，监管比较严格的组织（例如金融组织）要求采取比其他行业（例如教育和零售行业）更严格的安全控制措施，而后者主要考虑的是如何提高用户工作效率。

您可以根据用户的身份、设备、位置和连接类型集中控制和配置策略来限制对公司内容的恶意使用。如果设备丢失或被盗，您可以远程禁用、锁定或擦除业务应用程序和数据。综合上述因素，我们可以开发一种解决方案，不仅可以提高员工满意度和工作效率，同时还能确保安全性和管理控制。

本文主要介绍与安全性有关的多个设备和应用程序策略。

解决安全风险的策略

XenMobile 设备和应用程序策略解决可能会带来安全风险的多种情况，例如：

- 用户尝试从不可信设备和不可预测的位置访问应用程序和数据时。
- 用户在设备之间传递数据时。
- 未经授权的用户尝试访问数据时。

- 已离开公司的用户使用自己的设备 (BYOD) 时。
- 用户错放设备时。
- 用户需要随时安全地访问网络时。
- 用户使自己的设备处于托管状态且您需要将工作数据与个人数据区分开时。
- 设备处于空闲状态并需要再次验证用户凭据时。
- 用户将敏感内容复制并粘贴到不受保护的电子邮件系统时。
- 用户在保存了个人帐户和公司帐户的设备上收到包含敏感数据的电子邮件附件或 Web 链接时。

保护公司数据时，这些情况与两个主要考虑因素相关，即数据所处的状态：

- 静态
- 传输中

XenMobile 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。XenMobile 使用 iOS 和 Android 平台提供的设备加密。XenMobile 使用 Citrix MAM SDK 提供的合规性检查等功能补充基于平台的加密。

通过 XenMobile 中的移动应用程序管理 (MAM) 功能可以对移动生产力应用程序、启用了 MDX 的应用程序及其关联数据进行完整的管理、安全保护和控制。

移动应用程序 SDK 通过使用 Citrix MDX 应用程序容器技术启用 XenMobile 部署的应用程序。容器技术将企业应用程序和数据与个人应用程序和用户设备上的数据分离开来。数据分离允许您通过基于策略的综合控制来保护任何自定义开发的、第三方或 BYO 移动应用程序的安全。

XenMobile 还包括应用程序级加密。XenMobile 单独对任何启用了 MDX 的应用程序中存储的数据加密，而不需要设备通行码，也不需要您管理设备以强制执行策略。

通过策略和移动应用程序 SDK，您可以：

- 使用一个安全的移动容器区分公司和个人应用程序和数据。
- 通过加密和其他移动数据丢失防护 (DLP) 技术保护应用程序的安全。

MDX 策略提供了许多操作控件。您可以在启用了 MAM SDK 的应用程序或 MDX 封装的应用程序之间启用无缝集成，同时还可以控制所有通信。这样，您可以强制执行策略，例如，确保仅启用了 MAM SDK 或 MDX 封装的应用程序可以访问数据。

除了设备和应用程序策略控制，保护静态数据的最佳方法是加密。XenMobile 为启用了 MDX 的应用程序中存储的任何数据添加一层加密，从而让您可以对公用文件加密、私密文件加密和加密排除项等功能进行策略控制。移动应用程序 SDK 使用符合 FIPS 140-2 的 AES 256 位加密，并将密钥存储在受保护的 Citrix Secret Vault 中。

XenMobile 如何保护传输中的数据

在用户的移动设备与您的内部网络之间移动的数据称为传输中的数据。MDX 应用程序容器技术实现了通过 Citrix Gateway 对内部网络进行应用程序特定的 VPN 访问。

假设存在员工希望通过移动设备访问驻留在安全企业网络中的以下资源的情况：

- 公司电子邮件服务器
- 公司 Intranet 上托管的启用了 SSL 的 Web 应用程序
- 存储在文件服务器或 Microsoft SharePoint 上的文档

MDX 支持从移动设备通过应用程序特定的 Micro VPN 访问所有这些企业资源。每个设备都有自己的专用 Micro VPN 通道。

Micro VPN 功能不需要设备范围的 VPN（可能会危及不可信移动设备上的安全）。因此，内部网络不会面临可能影响整个公司系统的恶意软件或攻击。公司移动应用程序和个人移动应用程序能够在一个设备上共存。

为了提高安全级别，您可以为启用了 MDX 的应用程序配置备用 Citrix Gateway 策略（用于身份验证和与应用程序的 Micro VPN 会话）。您可以将备用 Citrix Gateway 与“要求联机会话”策略结合使用，以强制应用程序向特定网关重新进行身份验证。此类网关通常具有不同的（具有更高保障）身份验证要求和流量管理策略。

除了安全功能外，Micro VPN 功能还提供数据优化技术，包括压缩算法。压缩算法可确保：

- 仅传输最少的数据
- 传输在最快的时间内完成。速度改进了用户体验，这是移动设备采用的关键成功因素。

请定期重新评估设备策略，例如在以下情况下：

- 由于发布了设备操作系统更新，新版本的 XenMobile 包括新的或更新的策略时
- 添加设备类型时：

  尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。因此，您可能会发现 iOS、Android 和 Windows 设备之间的差异，甚至不同制造商提供的 Android 设备设备之间的差异。
- 使 XenMobile 操作与企业或行业变化（例如，新公司安全策略或合规性规章）保持同步
- 新版本的 MAM SDK 包括新的或更新的策略时
- 添加或更新应用程序时
- 由于新应用程序或新要求而需要为用户集成新工作流

应用程序策略和用例场景

虽然您可以选择通过 Secure Hub 提供的应用程序，您可能还希望定义这些应用程序与 XenMobile 的交互方式。使用应用程序策略：

- 如果您希望用户在特定时间段过后进行身份验证。
- 如果您希望为用户提供对其信息的脱机访问权限。

以下个部分内容包括一些策略和示例用法。

- 有关您可以使用 MAM SDK 集成到 iOS 和 Android 应用程序中的第三方策略的列表，请参阅 MAM SDK 概述。
- 有关每个平台的所有 MDX 策略的列表，请参阅 MDX 策略概览。

身份验证策略

- 设备通行码

  为什么要使用此策略：启用“设备通行码”策略可强制执行仅当设备上已启用设备通行码时用户才能访问 MDX 应用程序。此功能可确保在设备级别使用 iOS 加密。

  用户示例：启用此策略意味着，用户必须先在其 iOS 设备上设置一个通行码，然后才能访问 MDX 应用程序。

- 应用程序通行码

  为什么要使用此策略：启用“应用程序通行码”策略可让 Secure Hub 提示用户先向托管应用程序进行身份验证，然后才能打开应用程序并访问数据。用户可使用其 Active Directory 密码、Citrix PIN 或 iOS Touch ID 进行身份验证，具体取决于您在 XenMobile Server 设置中的“客户端属性”下配置的内容。您可以在“客户端属性”中设置不活动计时器，以便在持续使用时，Secure Hub 不提示用户向托管应用程序进行身份验证，直到计时器过期。

  应用程序通行码不同于设备通行码，原因在于，设备通行码策略推送到设备后，Secure Hub 将提示用户配置通行码或 PIN，当用户打开设备或不活动计时器过期时，他们必须先解锁，才能访问其设备。有关详细信息，请参阅 XenMobile 中的身份验证。

  用户示例：在设备上打开 Citrix Secure Web 应用程序时，如果不活动期限已过期，用户必须输入其 Citrix PIN，才能浏览 Web 站点。

- 要求联机会话

  为什么要使用此策略：如果某个应用程序要求访问 Web 应用程序（Web 服务）才能运行，则启用此策略以使 XenMobile 提示用户连接到企业网络或具有活动会话才能使用该应用程序。

  用户示例：用户尝试打开已启用“要求联机会话”策略的 MDX 应用程序时，只能在使用手机网络或 Wi-Fi 服务连接到网络后才能使用该应用程序。

- 最长脱机期限

  为什么要使用此策略：将此策略作为额外的安全选项使用，用于确保用户在未重新确认应用程序授权并从 XenMobile 刷新策略的情况下不能长时间脱机运行应用程序。

  用户示例：如果您为某个 MDX 应用程序配置“最长脱机期限”，用户可以打开并脱机使用该应用程序，直到脱机计时器期限过期。此时，如果系统提示，用户必须通过手机网络或 Wi-Fi 服务重新连接网络并重新进行身份验证。

其他访问策略

- 应用程序更新宽限期 (小时)

  为什么要使用此策略：应用程序更新宽限期是指为用户预留的一段时间，到此时间后，用户必须更新 XenMobile Store 中发布的较新版本的应用程序。在过期时，用户必须更新该应用程序才能访问该应用程序中的数据。设置此值时，请谨记您的移动办公人员的需求，尤其是在国际出差时可能很长一段时间脱机的办公人员。

用户示例：加载 XenMobile Store 中的新版本的 Secure Mail，然后将应用程序更新宽限期设置为 6 小时。Secure Mail 的所有用户将都看到一条消息，要求其更新自己的 Secure Mail 应用程序，直到过了 6 小时。过了 6 小时后，Secure Hub 会将用户路由至 XenMobile Store。

- 活动轮询期限 **(**分钟**)**

  为什么要使用此策略：活动轮询期限是指 XenMobile 检查应用程序以确定何时执行安全操作（例如，应用程序锁定和应用程序擦除）的时间间隔。

  用户示例：如果将“活动轮询期限”策略设置为 60 分钟，则从 XenMobile 向设备发送应用程序锁定命令时，将在上次轮询后的 60 分钟内发生锁定。

不合规设备行为策略

当设备低于最低合规性要求时，“不合规设备行为”策略将允许您选择要执行的操作。有关信息，请参阅不合规设备行为。

应用程序交互策略

为什么要使用这些策略：可使用应用程序交互策略来控制文档和数据从 MDX 应用程序传输到设备上其他应用程序的流。例如，您可以阻止用户在容器外部将数据移至其个人应用程序或从容器外部将数据粘贴到容器化应用程序中。

用户示例：您将应用程序交互策略设置为“限制”，这意味着用户可以将文本从 Secure Mail 复制到 Secure Web，但不能将该数据复制到容器外部的其个人 Safari 或 Chrome 浏览器。此外，用户可以在 Citrix Files 或 Quick Edit 中打开 Secure Mail 中的附加文档，但不能在容器外部的自己的个人文件查看应用程序中打开附加文档。

应用程序限制策略

为什么要使用这些策略：可使用应用程序限制策略来控制用户可以从打开的 MDX 应用程序访问的功能。这有助于确保该应用程序运行时不会发生任何恶意活动。在 iOS 和 Android 之间应用程序限制策略略有不同。例如，在 iOS 中，您可以在 MDX 应用程序运行时阻止对 iCloud 的访问。在 Android 中，您可以在 MDX 应用程序运行时停止 NFC 的使用。

用户示例：如果在 iOS 上启用应用程序限制策略以阻止在 MDX 应用程序中使用听写功能，则在 MDX 应用程序运行时，用户无法在 iOS 键盘上使用听写功能。因此，用户听写的数据不会传递到不安全的第三方云听写服务。用户在容器外部打开其个人应用程序时，用户仍可使用听写选项进行自己的个人通信。

应用程序网络访问策略

为什么要使用这些策略：可使用应用程序网络访问策略来提供从设备上容器中的 MDX 应用程序访问企业网络内部数据的权限。对于网络访问策略，设置通过通道连接到内部网络选项可自动启动通过 Citrix ADC 从 MDX 应用程序到后端 Web 服务或数据存储的 Micro VPN。

用户示例：用户打开已启用通道的 MDX 应用程序（例如 Secure Web）时，浏览器将打开并启动 Intranet 站点，而无需用户启动 VPN。Secure Web 应用程序会自动使用 Micro VPN 技术访问内部站点。

应用程序地理定位和地理围栏策略

为什么要使用这些策略：控制应用程序地理定位和地理围栏功能的策略包括中心点经度、中心点纬度和半径。这些策略包含在 MDX 应用程序中访问特定地理区域的数据的权限。这些策略按纬度和经度坐标半径定义地理区域。如果用户尝试在定义的半径外使用应用程序，则应用程序保持锁定状态，用户无法访问应用程序数据。

用户示例：用户在其办公地点时可以访问合并和收购数据。当用户离开办公地点时，不可访问此敏感数据。

Secure Mail 应用程序策略

- 后台网络服务

  为什么要使用此策略： Secure Mail 中的后台网络服务利用 Secure Ticket Authority (STA)，实际上这是用于通过 Citrix Gateway 进行连接的 SOCKS5 代理。STA 支持长时间连接，与 Micro VPN 相比，可延长电池寿命。因此，STA 非常适用于持续连接的邮件。Citrix 建议您为 Secure Mail 配置这些设置。适用于 XenMobile 的 Citrix ADC 向导会自动为 Secure Mail 设置 STA。

  用户示例：未启用 STA 且 Android 用户打开 Secure Mail 时，系统提示用户打开 VPN（在设备上保持打开状态）。启用了 STA 且 Android 用户打开 Secure Mail 时，Secure Mail 将无缝连接，而无需任何 VPN。

- 默认同步时间间隔

  为什么要使用此策略：此设置指定用户首次访问 Secure Mail 时同步到 Secure Mail 的电子邮件默认天数。请注意，同步 2 周的电子邮件所用时间比 3 天长，并会延长用户的设置过程。

  用户示例：如果“默认同步时间间隔”设置为 3 天，则当用户首次设置 Secure Mail 时，他们会在其收件箱中看到从当前到过去 3 天收到的任何电子邮件。如果用户想查看 3 天以前的电子邮件，可以执行搜索。Secure Mail 随即将显示服务器上存储的较早电子邮件。安装 Secure Mail 后，每个用户都可以更改此设置以更好地满足自己的需求。

设备策略和用例行为

设备策略（有时称为 MDM 策略）确定 XenMobile 处理设备的方式。尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。下面列出了其中一些设备策略，并介绍了相应的使用方法。有关所有设备策略的列表，请参阅设备策略下的文章。

- 应用程序清单策略

  为什么要使用此策略：如果您需要查看用户安装的应用程序，可将应用程序清单策略部署到设备。如果您未部署应用程序清单策略，则只能查看用户从 XenMobile Store 安装的应用程序，但看不到任何个人安装的应用程序。如果要阻止某些应用程序在公司设备上运行，必须使用此策略。

  用户示例：使用 MDM 托管的设备的用户不能禁用此功能。用户的个人安装的应用程序对 XenMobile 管理员可见。

- 应用程序锁定策略

为什么要使用此策略：对于 Android，可以通过应用程序锁定策略来阻止或允许运行应用程序。例如，通过允许运行应用程序，可以配置 kiosk 设备。通常情况下，只将应用程序锁定策略部署到公司拥有的设备，因为它会限制用户可以安装的应用程序。您可以设置覆盖密码以允许用户访问被阻止的应用程序。

用户示例：假设您部署的应用程序锁定策略阻止“愤怒的小鸟”应用程序。用户可以从 Google Play 安装“愤怒的小鸟”应用程序，但当其打开该应用程序时，将显示一条消息，告知其管理员已阻止该应用程序。

- 连接计划策略

  为什么要使用此策略：您必须使用连接计划策略，以使 Windows Mobile 设备可以重新连接到 XenMobile Server 以进行 MDM 管理、应用程序推送和策略部署。对于 Android、Android Enterprise 和 Chrome OS 设备，请使用 Google Firebase Cloud Messaging (FCM)（而非此策略）来控制与 XenMobile Server 的连接。计划选项如下所示：

  - 总是：连接永久保持活动状态。Citrix 建议使用此选项以优化安全性。如果选择总是，还要使用连接计时器策略来确保连接不会耗尽电池电量。通过保持连接处于活动状态，您可以根据需要将擦除或锁定等安全命令推送到设备。此外，还必须在部署到设备的每个策略中选择“部署计划”选项为始终启用的连接部署。
  - 从不：手动进行连接。Citrix 建议不要对生产部署使用此选项，因为从不选项会阻止您将安全策略部署到设备，因此，用户从不会收到任何新应用程序或策略。
  - 每隔：按照指定间隔进行连接。如果此选项生效，则当您发送锁定或擦除等安全策略时，XenMobile 将在下次设备连接时在设备上处理该策略。
  - 定义计划：启用后，在网络连接断开后，XenMobile 尝试将用户设备重新连接到 XenMobile Server，并在您定义的时间范围内通过以固定间隔传输控制数据包监视连接。

  用户示例：您希望将通行码策略部署到注册的设备。计划策略可确保设备以固定间隔重新连接到服务器以收集新策略。

- 凭据策略

  为什么要使用此策略：凭据策略常与 WiFi 策略结合使用，您可以通过该策略向需要证书身份验证的内部资源部署用于身份验证的证书。

  用户示例：您在设备上部署用于配置无线网络的 WiFi 策略。WiFi 网络要求使用证书进行身份验证。凭据策略将部署证书，该证书随后存储在操作系统密钥库中。之后，用户在连接到内部资源时可以选择该证书。

- **Exchange** 策略

  为什么要使用此策略：使用 XenMobile 时，您有两种方式传递 Microsoft Exchange ActiveSync 电子邮件。

  - **Secure Mail** 应用程序：使用从公共应用商店或 XenMobile Store 分发的 Secure Mail 应用程序传递电子邮件。
  - 本机电子邮件应用程序：使用 Exchange 策略为设备上的本机电子邮件客户端启用 ActiveSync 电子邮件。对本机电子邮件使用 Exchange 策略时，您可以使用宏提取其 Active Directory 属性中的用户数据进行填充，例如，提取 ${user.username} 中的数据填充用户名，提取 ${user.domain} 中的数据填充用户域。

用户示例：当您推送 Exchange 策略时，将向设备发送 Exchange Server 详细信息。Secure Hub 随后提示用户进行身份验证并且其电子邮件开始同步。

- 定位策略

  为什么要使用此策略：如果已在设备上为 Secure Hub 启用了 GPS，您可以通过定位策略在地图上对设备进行地理定位。部署此策略并随后从 XenMobile Server 发送定位命令后，设备将返回位置坐标。

  用户示例：部署了定位策略且在设备上启用了 GPS 后，如果用户错放了设备，他们可以登录 XenMobile 自助服务门户，然后选择定位选项，可在地图上查看其设备的位置。请注意，用户可进行选择以允许 Secure Hub 使用定位服务。当用户自己注册设备时，您无法强制使用定位服务。使用此策略的另一个注意事项是对电池寿命的影响。

- 通行码策略

  为什么要使用此策略：通行码策略允许您在托管设备上强制执行 PIN 代码或密码。此通行码策略允许您在设备上设置通行码的复杂性和超时。

  用户示例：当您将通行码策略部署到设备后，Secure Hub 将提示用户配置通行码或 PIN，当用户打开设备或不活动计时器过期时，他们必须先解锁，才能访问其设备。

- 配置文件删除策略

  为什么要使用此策略：假设您将某个策略部署到一组用户，以后需要从其中一部分用户删除该策略。您可以创建配置文件删除策略并使用部署规则将该配置文件删除策略仅部署到指定的用户名，以针对选定用户删除策略。

  用户示例：将配置文件删除策略部署到用户设备时，用户可能不会发现所做的更改。例如，如果配置文件删除策略删除了禁用设备摄像头的限制，用户不知道现在允许使用摄像头。当所做的更改影响用户体验时，请考虑让用户了解。

- 限制策略

  为什么要使用此策略：限制策略允许您使用许多选项来锁定和控制托管设备上的特性和功能。您可以对受支持的设备启用数以百计的限制选项，包括禁用设备上的摄像头或麦克风、对第三方服务（例如，应用商店）执行漫游规则和访问等。

  用户示例：如果您将限制部署到 iOS 设备，用户可能无法访问 iCloud 或 Apple App Store。

- 条款和条件策略

  为什么要使用此策略：您可能需要向用户告知托管其设备涉及的法律法规。此外，您可能希望确保用户知道向设备推送公司数据时的安全风险。您可以通过自定义的条款和条件文档在用户注册之前发布规则和声明。

  用户示例：用户将在注册过程中看到条款和条件信息。如果他们拒绝接受所列条件，则注册过程将结束，他们将无法访问公司数据。您可以生成报告以提供给 HR/法律/合规团队，报告中显示接受或拒绝这些条款的用户。

- **VPN** 策略

  为什么要使用此策略：使用 VPN 策略，可通过使用较旧 VPN 网关技术访问后端系统。该策略支持许多 VPN 提供商，包括 Cisco AnyConnect、Juniper 及 Citrix VPN。此外，也可以将此策略链接到 CA 并按需启用 VPN（如果 VPN 网关支持此选项）。

用户示例：启用 VPN 策略后，当用户访问内部域时，用户的设备将打开 VPN 连接。

- **Web** 剪辑策略

  为什么要使用此策略：如果您想要向设备推送可直接打开 Web 站点的图标，可使用 Web 剪辑策略。Web 剪辑包含指向 Web 站点的链接，并可以包括自定义图标。在设备上，Web 剪辑类似应用程序图标。

  用户示例：用户可以单击 Web 剪辑图标打开提供其需要访问的服务的 Internet 站点。与打开浏览器应用程序并键入链接地址的方式相比，使用 Web 链接更加方便。

- **WiFi** 策略

  为什么要使用此策略：通过 WiFi 策略可以将 WiFi 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：在部署 WiFi 策略后，设备将自动连接到 WiFi 网络并对用户进行身份验证，以便用户可访问此网络。

- **Windows** 信息保护策略

  为什么要使用此策略：可使用 Windows 信息保护 (WIP) 策略来避免企业数据可能发生的泄漏。您可以指定在您设置的强制级别需要 Windows 信息保护的应用程序。例如，您可以阻止任何不恰当的数据共享，或者在发生不恰当的数据共享时发出警告，并允许用户覆盖该策略。您可以无提示运行 WIP，同时记录和允许不恰当的数据共享。

  用户示例：假设您配置 WIP 策略以阻止不恰当的数据共享。如果用户将受保护的文件复制或保存到不受保护的位置，将显示类似如下的消息：You can’t place work protected content in this location（您不能将受工作保护的内容放在此位置）。

- **XenMobile Store** 策略

  为什么要使用此策略： XenMobile Store 是一个统一的应用商店，管理员可以在此发布其用户所需的所有公司应用程序和数据资源。管理员可以添加：

  - Web 应用程序、SaaS 应用程序和启用了 MAM SDK 的应用程序或 MDX 封装的应用程序
  - Citrix 移动生产力应用程序
  - 本机移动应用程序，例如.ipa 或.apk 文件
  - Apple App Store 或 Google Play 应用程序
  - Web 链接
  - 使用 Citrix StoreFront 发布的 Citrix Virtual Apps

  用户示例：用户将其设备注册到 XenMobile 后，便可通过 Citrix Secure Hub 应用程序访问 XenMobile Store。之后，用户可以看到可供其使用的所有公司应用程序和服务。用户可以在 XenMobile Store 中单击某个应用程序以进行安装、访问数据、对应用程序进行评分和评论以及下载应用程序更新。

用户注册选项

October 13, 2021

可以通过多种方式让用户在 XenMobile 中注册其设备。在考虑具体情况之前，请决定要在 MDM+MAM、MDM 还是 MAM 中注册哪些设备。有关这些管理模式的详细信息，请参阅管理模式。

在最高级别，有四个注册选项：

- 注册邀请：向用户发送注册邀请或邀请 URL。注册邀请和 URL 不适用于 Windows 设备。
- 自助服务门户：设置一个用户能够访问以下载 Secure Hub 并注册其设备或者向自己发送注册邀请的门户。
- 手动注册：发出电子邮件、手册或其他通信信息，让用户知道系统可以进行注册。用户随后将手动下载 Secure Hub 并注册其设备。
- 企业：另一个用于设备注册的选项是通过 Apple 部署计划和 Google Android Enterprise。您可以通过其中的每个计划来购买预配置并且可随时供用户使用的设备。有关详细信息，请参阅 Apple 支持中的 Apple 部署计划文章以及 Android Enterprise 网站上的 Google Android Enterprise 文档。

注册邀请

可以通过电子邮件向使用 iOS、macOS、Android Enterprise 或旧版 Android 设备的用户发送注册邀请。注册邀请和 URL 不适用于 Windows 设备。

还可以通过 SMTP 或 SMS 向 iOS、macOS、Android 或 Windows 设备的用户发送安装链接。有关详细信息，请参阅注册设备。

如果选择使用注册邀请方法，您可以：

- 选择邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。
- 使用这些模式的任意组合。
- 从设置页面启用或禁用这些模式。

有关每种注册安全模式的信息，请参阅配置注册安全模式。

邀请可实现多种目的。最常见的邀请用法是通知用户系统可用，并且可以进行注册。邀请 URL 是唯一的。用户使用邀请 URL 后，该 URL 将不再可用。可以使用此属性将用户或设备注册限制到您的系统。

配置注册配置文件时，可以根据 Active Directory 组控制特定用户能够注册的设备数。例如，您可能会允许您的财务部门每个用户只使用一台设备。

请注意某些注册选项的附加成本和陷阱。例如，使用 SMS 发送邀请需要额外的基础结构。有关此选项的详细信息，请参阅通知。

此外，要通过电子邮件发送邀请，请确保用户拥有在 Secure Hub 外部访问电子邮件的方法。对于 MDM 注册，可以使用一次性密码 (OTP) 注册安全模式作为 Active Directory 密码的备选方法。

自助服务门户

用户可以通过自助服务门户申请注册邀请。有关设置自助服务门户的信息，请参阅配置注册安全模式。

手动注册

进行手动注册时，用户将通过自动发现或者通过输入服务器信息连接到 XenMobile。使用自动发现时，用户将仅通过其电子邮件地址或用户主体名称格式的 Active Directory 凭据进行登录。不使用自动发现时，用户必须输入其服务器地址和 Active Directory 凭据。有关设置自动发现的详细信息，请参阅 XenMobile AutoDiscovery Service。

可以通过多种方式简化手动注册过程。可以创建一个指南，将其分发给用户，并请用户自行注册。可以请您的 IT 部门在某个时间段内手动注册几组用户。可以使用用户必须输入其凭据、服务器信息或两者的任何类似的方法。

用户加入

设置您的环境后，需要确定如何使用户加入到您的环境中。本文开头的部分探讨了用户注册安全模式的具体信息。本节将探讨您与用户取得联系的方法。

开放式注册与选择性邀请

登录用户时，可以通过两种基本方法允许注册：

- 开放式注册。默认情况下，任何具有 LDAP 凭据和 XenMobile 环境信息的用户都可以注册。
- 有限注册。可以通过仅允许具有邀请的用户进行注册来限制用户数量。还可以通过 Active Directory 组限制开放式注册。

使用此邀请方法时，还可以限制用户能够注册的设备数。在大多数情况下，可接受开放式注册，但有几点事项需要注意：

- 对于 MAM 注册，您可以通过 Active Directory 组成员身份轻松限制开放式注册。
- 对于 MDM 注册，您可以根据 Active Directory 组成员身份限制可以注册的设备数。如果仅允许在您的环境中注册企业设备，该限制通常不是问题。但是，您可能希望考虑在要限制环境中的设备数量的 BYOD 工作区中使用此方法。

通常很少执行选择性邀请，因为与开放式注册相比，此注册方法需要执行更多操作。为使用户在您的环境中注册其设备，必须向每个用户发送一个唯一的邀请。有关如何发送注册邀请的信息，请参阅发送注册邀请。

虽然您可以使用 Active Directory 组来批量创建邀请，但必须分批执行此方法。

首次与用户联系

确定使用开放式注册还是选择性邀请并设置了这些环境之后，您必须使用户知晓其注册选项。

如果使用选择性邀请方法，电子邮件和 SMS 消息将属于此过程的一部分。对于开放式注册，还可以通过 XenMobile 控制台发送电子邮件。有关详细信息，请参阅发送注册邀请。

在任一情况下，都请谨记，如果要发送电子邮件，则需要 SMTP 服务器。如果要发送文本消息，则需要 SMS 服务器。制定决策时，这些服务器可能有需要考虑的附加成本。选择方法之前，请考虑您希望新用户如何访问信息，例如电子邮件。如果希望所有用户都通过 XenMobile 访问其电子邮件，向其发送邀请电子邮件将是一个问题。

还可以通过 XenMobile 以外的其他方式为开放式注册环境发送通信。对于该选项，请务必包含所有相关信息。让用户知道他们可以从哪里获取 Secure Hub 应用程序以及注册时使用的方法。如果您关闭了发现，还要为用户提供 XenMobile Server 地址。要了解有关自动发现的详细信息，请参阅 XenMobile AutoDiscovery Service。

调整 **XenMobile** 操作

May 20, 2021

XenMobile 操作的性能和稳定性涉及 XenMobile 中的多个设置，并取决于您的 Citrix ADC 和 SQL Server 数据库配置。本文重点介绍管理员最常配置且与 XenMobile 的调整和优化相关的设置。Citrix 建议在部署 XenMobile 之前评估本文中的每个设置。

> 重要：
>
> 这些指导原则假定 XenMobile Server 的 CPU 和 RAM 足以满足相应设备数的需要。有关可扩展性的详细信息，请参阅可扩展性和性能。

以下服务器属性全局应用于整个 XenMobile 实例中的操作、用户和设备。更改某些服务器属性后需要重新启动每个 XenMobile Server 节点。需要重新启动时，XenMobile 会向您发出通知。

这些调整指导原则适用于群集环境和非群集环境。

hibernate.c3p0.idle_test_period

此 XenMobile Server 属性（即“自定义键”）确定自动验证连接之前的空闲时间（秒）。按如下所示配置键。默认值为 **30**。

- 键：自定义键
- 键：**hibernate.c3p0. idle_test_period**
- 值：**120**
- 显示名称：**hibernate.c3p0. idle_test_period**
- 说明：休眠空闲测试时间段

hibernate.c3p0.max_size

此自定义键确定 XenMobile 可以打开的与 SQL Server 数据库的最大连接数。XenMobile 使用您为此自定义键指定的值作为上限。仅当需要连接时才会打开连接。设置基于数据库服务器的容量。

请注意群集配置中的以下公式。c3p0 连接乘以节点数等于 XenMobile 可以向 SQL Server 数据库打开的实际最大连接数。

在群集配置和非群集配置中，如果对太小的 SQL Server 设置的值过高，会导致在峰值负载期间 SQL 端出现资源问题。设置的值过低意味着可能无法利用可用的 SQL 资源。

按如下所示配置键。默认值为 **1000**。

- 键：**hibernate.c3p0.max_size**
- 值：**1000**
- 显示名称：**hibernate.c3p0.max_size**
- 说明：DB 与 SQL 的连接数

hibernate.c3p0.min_size

此自定义键确定 XenMobile 打开的与 SQL Server 数据库的最小连接数。按如下所示配置键。默认值为 **100**。

- 键：**hibernate.c3p0.min_size**
- 值：**100**
- 显示名称：**hibernate.c3p0.min_size**
- 说明：DB 与 SQL 的连接数

hibernate.c3p0.timeout

此自定义键确定空闲超时。如果您使用数据库群集故障转移，Citrix 建议您添加此自定义键并对其进行设置以缩短空闲超时。默认值为 **120**。

- 键：自定义键
- 键：**hibernate.c3p0.timeout**
- 值：**120**
- 显示名称：**hibernate.c3p0.timeout**
- 说明：数据库空闲超时

推送服务检测信号时间间隔

此设置决定 iOS 设备检查在相应期间是否未传送 APNs 通知的频率。提高 APNs 检测信号频率可以优化数据库通信。值过大可能会导致增加不必要的负载。此设置仅适用于 iOS。默认值为 **20** 小时。

如果您的环境中有大量 iOS 设备，检测信号时间间隔可能会导致实际负载高于所需负载。选择性擦除、锁定和完全擦除等安全操作不依赖此检测信号。原因是在执行这些操作时系统会向设备发送 APNS 通知。此值管理在 Active Directory 组成员身份发生变化后策略更新的速度。因此，通常适合将此值增加到 12 到 20 小时之间的数以降低负载。

iOS MDM APNS 连接池大小

当您有 100 多台设备时，APNs 连接池太小可能会对 APNs 活动性能产生负面影响。性能问题包括降低向设备部署应用程序和策略的速度以及设备注册速度。默认值为 **1**。我们建议您为大约每 400 个设备将此值增加 1。

auth.ldap.connect.timeout

为了补偿 LDAP 响应慢的情况，Citrix 建议为以下自定义键添加服务器属性。

- 键：自定义键
- 键：**auth.ldap.connect.timeout**
- 值：**60000**
- 显示名称：**auth.ldap.connect.timeout**
- 说明：**LDAP** 连接超时

auth.ldap.read.timeout

为了补偿 LDAP 响应慢的情况，Citrix 建议为以下自定义键添加服务器属性。

- 键：自定义键
- 键：**auth.ldap.read.timeout**
- 值：**60000**
- 显示名称：**auth.ldap.read.timeout**
- 说明：**LDAP** 读取超时

其他服务器优化

服务器属性	默认设置	为什么更改此设置?
后台部署	1440 分钟	后台策略部署的频率（分钟）。仅适用于 Android 设备的始终启用连接。提高策略部署的频率可降低服务器负载。建议的设置为 **1440**（24 小时）。
后台硬件清单	1440 分钟	后台硬件清单的频率（分钟）。仅适用于 Android 设备的始终启用连接。提高硬件清单的频率可降低服务器负载。建议的设置为 **1440**（24 小时）。
检查删除的 **Active Directory** 用户的时间间隔	15 分钟	Active Directory 的标准同步时间为 **15** 分钟。值为 **0** 将阻止 XenMobile 检查删除的 Active Directory 用户。建议的设置为 **15** 分钟。

MaxNumberOfWorker	3	导入许多批量购买许可证时使用的线程数量。默认值为 **3**。如果需要进一步优化，可以增加线程的数量。但请注意，如果使用数量较大的线程，例如 6 个，批量购买导入会导致 CPU 使用率非常高。

如何查看 **SQL** 数据库中的死锁和删除历史数据

当您看到死锁时，请运行以下查询以查看死锁。然后，数据库管理员或 Microsoft SQL 团队可以确认该信息。

SQL 查询

```
SELECT

db.name DB_Service,

tl.request_session_id,

wt.blocking_session_id,

OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,

tl.resource_type,

h1.TEXT AS RequestingText,

h2.TEXT AS BlockingTest,

tl.request_mode

FROM sys.dm_tran_locks AS tl

INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id

INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
    resource_address

INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
    resource_associated_entity_id

```



```
INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
    request_session_id

INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
    blocking_session_id

CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1

CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2

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

清理数据库

> 重要：
>
> 请先备份您的数据库，然后再对表格进行更改。

1. 请运行以下查询以查看历史数据。

```
select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;
select COUNT(\*) as total_record from dbo.EWSESS;
select COUNT(*) as total_record from dbo.EWAUDIT;
<!--NeedCopy-->
```

2. 删除上述三个表中的数据。

> 注意：
>
> 您可能看不到表中的历史数据。如果需要，请跳过为该特定表运行截断查询。

```
truncate TABLE dbo.EWDEPLOY_HISTO;
truncate TABLE dbo.EWSESS;
truncate TABLE dbo.EWAUDIT;
<!--NeedCopy-->
```

3. 解锁因死锁而被阻止的 SELECT 查询。此步骤可处理更多死锁。

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT
    ON WITH ROLLBACK IMMEDIATE
<!--NeedCopy-->
```

4. 默认情况下，对于保留会话保留和审核保留数据的数据库，数据库清理为七天一次，该时间对于许多用户而言较长。请将清理值更改为 1 天或 2 天。在服务器属性中，进行以下更改：


```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
zdm.dbcleanup.auditRetentionTimeInDays=1 day
<!--NeedCopy-->
```

清理 **KEYSTORE** 表中的孤立项

如果 XenMobile 节点性能较差，请检查 KEYSTORE 表是否太大。XenMobile 将注册证书存储在 ENROLLMENT_CERTIFICATE 和 KEYSTORE 表中。当您删除或重新注册设备时，ENROLLMENT_CERTIFICATE 中的证书将被删除。KEYSTORE 表中的条目仍然存在，这可能会导致性能问题。请执行以下过程以清除 KEYSTORE 表中的孤立项。

> 重要：
>
> 请先备份您的数据库，然后再对表格进行更改。

1. 请运行以下查询以查看历史数据。

```
select COUNT(*) from KEYSTORE
<!--NeedCopy-->
```

2. 使用以下查询检查 KEYSTORE 表中的孤立项。

```
WITH cte(KEYSTORE_ID)
AS (SELECT KEYSTORE_ID
    FROM ENROLLMENT_CERTIFICATE
    UNION
    SELECT CA_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT CLIENT_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT KEYSTORE_ID
    FROM SAML_SERVICE_PROVIDER
    UNION
    SELECT KEYSTORE_ID
    FROM SERVER_CERTIFICATE)
SELECT keystore.id
FROM keystore
    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
WHERE KEYSTORE_ID IS NULL;
<!--NeedCopy-->
```


3. 使用以下查询清除孤立项。

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
        UNION
        SELECT KEYSTORE_ID
        FROM SERVER_CERTIFICATE)
    DELETE FROM keystore
    WHERE id IN
    (
        SELECT keystore.id
        FROM keystore
            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
    );
<!--NeedCopy-->
```

4. 向 KEYSTORE 表中添加索引以提高搜索效率。

```
DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
    ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
    DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
<!--NeedCopy-->
```

应用程序预配和取消预配

January 5, 2022

应用程序预配与移动应用程序生命周期管理紧密相关：在 XenMobile 环境中准备、配置、交付和管理移动应用程序。在某些情况下，预配流程可能还包括开发或修改应用程序代码。XenMobile 具有可用于应用程序预配的各种工具和流程。

在阅读有关应用程序预配的这篇文章之前，我们建议您阅读以下文章：

- 应用程序 - 用户社区

最终确定贵组织计划向用户交付的应用程序类型后，可以制定在应用程序的整个生命周期对其进行管理的流程。

在定义应用程序预配流程时，请考虑以下几点：

- 应用程序分析：贵组织可以先开始分析有限数量的应用程序。但是，随着用户采用率的提高和环境的扩大，您管理的应用程序数量会迅速增加。从一开始就定义特定的应用程序配置文件，以便轻松管理应用程序预配。应用程序配置可帮助您从非技术角度将应用程序分类到相应逻辑组。例如，您可以根据以下因素创建应用程序配置文件：
  - 版本：要跟踪的应用程序版本
  - 实例：为具有不同访问级别的多组不同用户部署的多个实例
  - 平台：iOS、Android 或 Windows
  - 目标受众：标准用户、部门、高管
  - 所有权：拥有该应用程序的部门
  - 类型：MDX、公共、Web 和 SaaS 或者 Web 链接
  - 升级周期：应用程序的升级频率
  - 许可：许可要求和所有权
  - MAM SDK 或 MDX 策略：将 MDX 功能应用到您的移动应用程序
  - 网络访问：访问类型，例如，安全浏览或完整 VPN

    > 注意：
    > “通道 Web SSO” 是 MDX 设置中安全浏览的名称。该行为是相同的。

示例：

因数	Secure Mail	邮件	内部	Epic Rover
版本	10.1	10.1	X.x	X.x
实例	VIP	医师	临床	临床
平台	iOS	iOS	iOS	iOS
目标用户	VIP 用户	医师	临床用户	临床用户
所有权	IT	IT	IT	IT
类型	MDX	MDX	本机	公用
升级周期	按季度	按季度	每年	不适用
许可	不适用	不适用	不适用	批量购买
MDX 策略	是	是	是	否
网络访问	VPN	VPN	VPN	公用

- 应用程序版本控制：维护和跟踪应用程序版本是预配流程的关键部分。版本控制对用户是透明的。仅当有新版本

的应用程序可下载时，他们才会收到通知。从您的角度而言，以非生产容量检查和测试每个应用程序版本也是至关重要的，这是为了避免在生产中产生影响。

此外，评估是否需要某个特定升级也很重要。应用程序升级通常有两种类型：一种是次要升级，例如，针对某个特定缺陷的修复。第二种是主要升级，即在应用程序中引入了重大更改和改进。在任一情况下，您都需要仔细查看应用程序的发行说明以评估是否需要进行相应的升级。

- 应用程序开发：将 MAM SDK 集成到您开发的移动应用程序中时，您将 MDX 功能应用到这些应用程序。请参阅 MAM SDK 概述。

  MAM SDK 替代了 MDX Toolkit，后者计划于 2022 年 3 月弃用。有关应用程序封装的信息，请参阅 MDX Toolkit。打包应用程序的应用程序预配流程与标准的未打包应用程序的预配流程有所差别。

- 应用程序安全性：在预配流程中，要定义各个应用程序或应用程序配置文件的安全要求。可以在部署应用程序之前将安全要求映射到特定 MDM 或 MAM 策略。该规划简化并加快了应用程序部署过程。例如：

  - 您可能会以不同的方式部署某些应用程序。
  - 您可能希望对 XenMobile 环境的体系结构进行更改。这些更改取决于应用程序所需的安全合规性类型。例如，您可能需要对设备进行加密以允许使用关键业务智能应用程序。或者某个特定的应用程序可能需要端到端 SSL 加密或地理围栏。

- 应用程序交付： XenMobile 允许您以 MDM 应用程序或 MAM 应用程序方式交付应用程序。MDM 应用程序显示在 XenMobile Store 中。此应用商店允许您方便地向用户交付公共应用程序或本机应用程序。您管理的唯一 MDM 应用程序控件是强制实施设备级别限制。但是，使用 MAM 交付应用程序可以完全控制应用程序交付以及控制应用程序本身。通常情况下，通过 MAM 交付应用程序更合适。

- 应用程序维护：

  - 执行初始审核：跟踪您的生产环境中的应用程序版本以及上一个升级周期。记下需要升级才能实现的特定功能或缺陷修复。
  - 建立基准：维护每个应用程序的最新稳定版本列表。如果升级后出现意外问题，将回退此应用程序版本。同时制定回滚计划。在生产部署之前，在测试环境中测试应用程序升级。如果可能，请先将升级部署到生产用户的子集，然后再部署到整个用户群。
  - 订阅 Citrix 软件更新通知和任何第三方软件供应商通知：始终拥有最新版本的应用程序至关重要。早期访问版本 (EAR) 内部版本可以进行测试。
  - 制定通知用户的策略：定义应用程序升级可用时通知用户的策略。请在部署之前对用户进行培训，使用户做好准备。可以在更新应用程序之前发送多个通知。根据应用程序的情况，最佳的通知方法可能是电子邮件通知或 Web 站点。

应用程序生命周期管理代表应用程序从其初始部署到停用的完整生命周期。应用程序的生命周期有以下阶段：

1. 规范要求：首先提出业务用例和用户要求。
2. 开发：验证应用程序是否满足业务需求。
3. 测试：确定测试用户、问题和缺陷。
4. 部署：将应用程序部署到生产用户。
5. 维护：更新应用程序版本。在生产环境中更新应用程序之前，先在测试环境中部署应用程序。

使用 **Secure Mail** 的应用程序生命周期示例

1. 规范要求：作为安全要求，您需要一款容器化并支持 MDX 安全策略的邮件应用程序。
2. 开发：验证应用程序是否满足业务需求。您必须能够对应用程序应用 MDX 策略控制。
3. 测试：将 Secure Mail 分配给一个测试用户组，并从 XenMobile Server 部署对应的 MDX 文件。测试用户会验证他们是否可以成功发送和接收电子邮件，以及是否可以访问日历和联系人。测试用户还会报告问题并找出缺陷。根据测试用户的反馈，优化 Secure Mail 配置以用于生产。
4. 部署：测试阶段完成后，您可以将 Secure Mail 分配给生产用户，并从 XenMobile 部署对应的 MDX 文件。
5. 维护：Secure Mail 发布新更新时，您可以从 Citrix 下载页面下载新的 MDX 文件并替换 XenMobile Server 上的现有 MDX 文件。指示用户执行更新。注意：Citrix 建议您在测试环境中完成并测试此过程。然后，将应用程序上载到 XenMobile 生产环境，并将应用程序部署给用户。

有关详细信息，请参阅打包 iOS 移动应用程序和打包 Android 移动应用程序。

基于控制板的操作

January 21, 2021

您可以通过访问 XenMobile 控制台控制板概括查看信息。根据这些信息，您可以使用小组件快速查看问题和成功方法。

控制板通常是您首次登录 XenMobile 控制台时显示的屏幕。要从控制台中的其他地方访问控制板，请单击分析。单击控制板中的自定义可编辑页面布局以及编辑显示的小组件。

- 我的控制板：最多可以保存四个控制板。可以单独编辑这些控制板，并通过选择保存的控制板来查看每个控制板。
- 布局样式：在此行中，可以选择在控制板上显示的小组件数以及如何布局小组件。
- 小组件选择：可以选择在控制板上显示的信息。
  - 通知：选中左侧数字上方的复选框可将“通知”栏添加到小组件上方。此栏显示兼容设备、不活动设备以及过去 24 小时擦除或注册的设备数。
  - 设备 **(**按平台**)**：按平台显示托管设备和非托管设备数。
  - 设备 **(**按运营商**)**：按运营商显示托管设备和非托管设备数。单击每个栏可按平台查看明细。
  - 托管设备 **(**按平台**)**：按平台显示托管设备数。
  - 非托管设备 **(**按平台**)**：按平台显示非托管设备数。此图表中显示的设备可能安装了代理，但设备的权限已被吊销或设备已被擦除。
  - 设备 **(**按 **ActiveSync Gateway** 状态**)**：显示按 ActiveSync Gateway 状态分组的设备数。信息中显示“已阻止”、“已允许”或“未知”状态。可以单击每个栏来按平台细分数据。
  - 设备 **(**按所有权**)**：显示按所有权状态分组的设备数。信息中显示“公司拥有”、“员工拥有”或“未知所有权”状态。
  - 失败的交付组部署：按软件包显示失败部署总数。仅显示部署失败的软件包。
  - 设备 **(**按阻止原因**)**：显示 ActiveSync 阻止的设备数
  - 已安装的应用程序：通过使用此小组件，可以键入应用程序名称，将有一个图形显示有关该应用程序的信息。

- 批量购买应用程序许可证使用情况：显示 Apple 批量购买应用程序的许可证使用情况统计信息。

用例

可以通过多种方式使用控制板小组件监视您的环境，其中的部分示例如下。

- 您已部署移动生产力应用程序并且要接收与移动生产力应用程序无法在设备上安装有关的支持票证。使用不合规设备和已安装的应用程序小组件查看未安装移动生产力应用程序的设备。
- 您希望监视不活动的设备，以便能够从环境中删除这些设备并回收许可证。使用不活动设备小组件跟踪此统计信息。
- 您要接收与未正确同步的数据有关的支持票证。您可能希望使用设备 **(**按 **ActiveSync Gateway** 状态**)** 和设备 **(**按阻止原因**)** 小组件来确定问题是否与 ActiveSync 有关。

报告

您的环境完成设置并且用户注册后，可以运行报告以了解您的部署。XenMobile 随附多个内置报告，以帮助您更好地了解环境中运行的设备。有关详细信息，请参阅报告。

> 重要：
>
> 虽然可以使用 SQL Server 来创建自定义报告，但 Citrix 不建议使用此方法。通过这种方式使用 SQL Server 数据库可能会导致您的 XenMobile 部署中出现不可预见的后果。如果您决定继续使用此报告方法，请务必使用只读帐户运行 SQL 查询。

基于角色的访问控制和 **XenMobile** 支持

January 5, 2022

XenMobile 使用基于角色的访问控制 (RBAC) 来限制用户和组对 XenMobile 系统功能的访问权限，例如 XenMobile 控制台、远程支持和公共 API。本文介绍了 XenMobile 中内置的角色，并且介绍了决定使用 RBAC 的 XenMobile 的支持模式的注意事项。

> 注意：
>
> 自 2019 年 1 月 1 日起，远程支持功能不再向新客户提供。现有客户可以继续使用此产品，但 Citrix 将不提供增强功能或修复。

内置角色

可以更改授予以下内置角色的访问权限，并且可以添加角色。要获取与每个角色及其默认设置关联的完整访问和功能权限集，请从 XenMobile 文档中下载 Role-Based Access Control Defaults（基于角色的访问控制的默认设置）。有关每种功能的定义，请参阅 XenMobile 文档中的使用 RBAC 配置角色。

管理角色

授予的默认访问权限：

- 除远程支持外的完全系统访问权限。
- 默认情况下，管理员可以执行某些支持任务，例如检查连接和创建支持包。

注意事项：

- 您的部分或所有管理员是否需要访问远程支持？如果是，则可以编辑管理员角色或添加管理员角色。
- 要进一步限制部分管理员或管理员组的访问权限，请根据管理员模板添加角色并编辑权限。

设备预配

授予的默认访问权限：

- 在 Windows CE 设备上访问 XenMobile 控制台以执行基础管理任务：添加、更改和删除设备；使用“设置”页面。

注意事项：

- 仅适用于 Windows CE 设备。

支持

授予的默认访问权限：

- 对远程支持的访问权限。

注意事项：

- 对于本地 XenMobile Server 部署：通过远程支持，您的技术支持代表能够远程控制托管的 Windows CE 和 Android 移动设备。屏幕录像功能仅在 Samsung KNOX 设备上受支持。
- 远程支持不适用于本地群集 XenMobile Server 部署。

用户

授予的默认访问权限：

- 对 XenMobile 控制台的受限访问权限：设备功能（例如擦除、锁定/解锁设备；锁定/解锁容器；查看位置和设置地理限制；设备响铃；重置容器密码）；添加、删除和发送注册邀请。

注意事项：

- “用户”角色允许您使用户能够自助操作。
- 要支持共享设备，请为共享设备注册创建一个用户角色。

XenMobile 支持模式的注意事项

可以采用的支持模式变化非常大，并且可能涉及负责处理 1 级和 2 级支持的第三方（员工负责处理 3 级和 4 级支持）。无论您如何分发支持负载，都请谨记本部分内容中特定于您的 XenMobile 部署和用户基础的注意事项。

用户使用公司拥有的设备还是 **BYO** 设备?
影响支持的主要问题是在您的 XenMobile 环境中哪些用户拥有用户设备。如果您的用户使用公司拥有的设备，您可能会提供较低级别的支持，作为锁定设备的一种方法。在这种情况下，您可能会提供帮助用户解决设备问题以及教授设备使用方法的技术支持人员。请考虑您可能会通过何种方式使用技术支持人员的 RBAC 设备预配和支持角色，具体取决于需要支持的设备类型。

如果您的用户使用 BYO 设备，贵组织可能会期望用户寻找自己的设备支持来源。在这种情况下，贵组织提供的支持更多的是专注于解决 XenMobile 特定问题的管理角色。

您的桌面的支持模式是什么?
请考虑您的桌面的支持模式是否适用于其他公司拥有的设备。您可以使用相同的支持组织吗？他们需要哪些额外的培训?

您是否希望向用户授予对 **XenMobile** 自助服务门户的访问权限?
使用设置 **>** 注册为注册安全模式启用自助服务门户。通过自助服务门户，用户可以生成注册链接，用户可以使用这些链接注册自己的设备或者向自己发送注册邀请。请参阅配置注册安全模式。

系统监视

January 5, 2022

为了确保应用程序访问和连接实现最佳运行时间，应监视 XenMobile 环境中的以下核心组件。

XenMobile Server

XenMobile Server 可生成日志并将其存储本地存储位置，您还可以将这些日志导出到系统日志 (syslog) 服务器中。您可以配置日志设置以指定大小限制和日志级别，也可以创建自定义记录器来过滤特定事件。您可以随时从 XenMobile 控制台查看 XenMobile Server 日志。您可以通过 syslog 服务器将日志中的信息导出到生产 Splunk 日志记录服务器中。

下面列出了 XenMobile 中可用的不同类型的日志文件：

调试日志文件：包含有关 XenMobile 的核心 Web 服务的调试级别信息，包括错误消息和服务器相关操作。

消息格式：

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <
log message>
```

- 其中 <id> 是唯一标识符，例如会话 ID。
- 其中 <log message> 是应用程序提供的消息。

管理员审核日志文件：包含有关 XenMobile 控制台上的活动的审核信息。

> 注意：
>
> 管理员审核日志和用户审核日志使用相同的格式。

消息格式：

除必需的 Date 值和 Timestamp 值外，所有其他属性都是可选属性。消息中可选字段通过 “ “ 表示。

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

下表列出了可用的管理员审核日志事件：

有关事件的管理员审核日志消息	状态
登录	成功/失败
注销	成功/失败
获取管理员	成功/失败
更新管理员	成功/失败
获取应用程序	成功/失败
添加应用程序	成功/失败
更新应用程序	成功/失败
删除应用程序	成功/失败
绑定应用程序	成功/失败
取消绑定应用程序	成功/失败
禁用应用程序	成功/失败
启用应用程序	成功/失败
获取类别	成功/失败
添加类别	成功/失败
更新类别	成功/失败
删除类别	成功/失败
添加证书	成功/失败
删除证书	成功/失败
活动证书	成功/失败
CSR 证书	成功/失败

有关事件的管理员审核日志消息	状态
导出证书	成功/失败
删除证书链	成功/失败
添加证书链	成功/失败
获取连接器	成功/失败
添加连接器	成功/失败
删除连接器	成功/失败
更新连接器	成功/失败
获取设备	成功/失败
锁定设备	成功/失败
解锁设备	成功/失败
擦除设备	成功/失败
取消擦除设备	成功/失败
删除设备	成功/失败
获取角色	成功/失败
添加角色	成功/失败
更新角色	成功/失败
删除角色	成功/失败
绑定角色	成功/失败
取消绑定角色	成功/失败
更新配置设置	成功/失败
更新工作流电子邮件	成功/失败
添加工作流	成功/失败
删除工作流	成功/失败
添加 Active Directory	成功/失败
更新 Active Directory	成功/失败
添加主用户列表	成功/失败
更新主用户列表	成功/失败
更新 DNS	成功/失败
更新网络	成功/失败

有关事件的管理员审核日志消息	状态
更新日志服务器	成功/失败
从日志服务器传输日志	成功/失败
更新 syslog	成功/失败
更新 Receiver 更新	成功/失败
更新时间服务器	成功/失败
更新信任	成功/失败
添加服务记录	成功/失败
更新服务记录	成功/失败
更新 Receiver 电子邮件	成功/失败
上载修补程序	成功/失败
导入快照	成功/失败
提取应用商店应用程序详细信息	成功/失败
更新 MDM	成功/失败
删除 MDM	成功/失败
添加 HDX	成功/失败
更新 HDX	成功/失败
删除 HDX	成功/失败
添加外观方案	成功/失败
删除外观方案	成功/失败
更新 SSL 卸载	成功/失败
添加帐户属性	成功/失败
删除帐户属性	成功/失败
更新帐户属性	成功/失败
添加信标	成功/失败

用户审核日志文件：包含与注册的设备中的用户活动相关的信息。

> 注意：
>
> 用户审核日志和管理员审核日志使用相同格式。

消息格式：

除必需的 Date 值和 Timestamp 值外，所有其他属性都是可选属性。消息中可选字段通过 “ “ 表示。例如，

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

下表列出了可用的用户审核日志事件：

有关事件的用户审核日志消息	状态
登录	成功/失败
会话超时	成功/失败
订阅	成功/失败
取消订阅	成功/失败
预启动	成功/失败
AGEE SSO	成功/失败
适用于 Citrix Files 的 SAML 令牌	成功/失败
设备注册	成功/失败
设备检查	锁定/擦除
设备更新	成功/失败
令牌刷新	成功/失败
已保存机密信息	成功/失败
已检索机密信息	成功/失败
用户已启动更改密码	成功/失败
移动客户端下载	成功/失败
注销	成功/失败
发现服务	成功/失败
端点服务	成功/失败

MDM 功能	状态
REGHIVE	成功/失败
Cab 清单	成功/失败
Cab	成功/失败
Cab 自动安装	成功/失败

MDM 功能	状态
Cab shell 安装	成功/失败
Cab 创建文件夹	成功/失败
Cab 文件获取	成功/失败
文件创建文件夹	成功/失败
文件获取	成功/失败
文件已发送	成功/失败
脚本创建文件夹	成功/失败
脚本获取	成功/失败
脚本已发送	成功/失败
脚本 shell 执行	成功/失败
脚本自动执行	成功/失败
APK 清单	成功/失败
APK	成功/失败
APK shell 安装	成功/失败
APK 自动安装	成功/失败
APK 创建文件夹	成功/失败
APK 文件获取	成功/失败
APK 应用程序	成功/失败
EXT 应用程序	成功/失败
列表获取	成功/失败
列表已发送	成功/失败
定位设备	成功/失败
CFG	成功/失败
解锁	成功/失败
SharePoint 擦除	成功/失败
SharePoint 配置	成功/失败
删除配置文件	成功/失败
删除应用程序	成功/失败
删除非托管应用程序	成功/失败

MDM 功能	状态
删除非托管配置文件	成功/失败
IPA 应用程序	成功/失败
EXT 应用程序	成功/失败
应用兑换代码	成功/失败
应用设置	成功/失败
启用跟踪设备	成功/失败
应用程序管理策略	成功/失败
SD 卡擦除	成功/失败
加密电子邮件附件	成功/失败
外观方案	成功/失败
Secure Browser	成功/失败
容器浏览器	成功/失败
容器解锁	成功/失败
容器密码重置	成功/失败
AG 客户端身份验证凭据	成功/失败

Citrix ADC 还监视 XenMobile Web 服务状态，该服务配置了智能监视探测以模拟发送到每个 XenMobile Server 群集节点的 HTTP 请求。探测确定服务是否处于联机状态，然后根据收到的响应进行响应。如果某个节点未按预期响应，则 Citrix ADC 将相应的服务器标记为关闭。此外，Citrix ADC 从负载平衡池中获取节点并记录事件以用于通过 Citrix ADC 监视解决方案生成警报。

您还可以使用标准虚拟机管理程序监视工具来监视 XenMobile 虚拟机，并提供有关 CPU、内存和存储利用率指标的相关警报。

SQL Server 和数据库

SQL Server 和数据库性能直接影响 XenMobile Service。XenMobile 实例要求随时可以访问数据库，如果 SQL 基础结构发生中断，则将进入脱机状态（例如，停止响应）。在 SQL Server 发生任何磁盘空间问题后，XenMobile 控制台可能会继续运行一段时间。为了确保在 XenMobile 工作负载中达到最大数据库运行时间和足够的性能，应主动监视您的 SQL Server 的状态。有关监视 SQL Server 的详细信息，请参阅监视和调整性能概述。此外，您还应为 CPU、内存和存储调整资源分配，以在您的 XenMobile 环境持续扩大时保证符合服务级别协议。

Citrix ADC

Citrix ADC 提供将指标记录到内部存储或将日志发送到外部日志记录服务器的功能。您可以配置 syslog 服务器以将 Citrix ADC 日志导出到您的生产 Splunk 日志记录服务器。Citrix ADC 中提供以下日志记录级别：

- 紧急
- 警报
- 严重
- 错误
- 警告
- 信息

日志文件还存储在 Citrix ADC 存储中的 /var/log/ns.log 目录中，且名为 newnslog。Citrix ADC 会滚动这些文件，并使用 GZIP 算法压缩这些文件。日志文件名称为 newnslog.xx.gz，其中 xx 表示运行编号。

此外，Citrix ADC 还支持 SNMP 陷阱和警报作为监视选项。有关 SNMP 陷阱列表，请参阅 SNMP 监视。

灾难恢复

January 5, 2022

可以设计使用主-被故障转移策略的灾难恢复的多个站点的 XenMobile 部署的架构并配置该部署。

本文中探讨的推荐灾难恢复策略由以下几个组件组成：

- 一个 XenMobile 活动站点，位于一个服务于所有全球企业用户的地理位置的数据中心中，称为“主站点”。
- 第二个是 XenMobile 站点，位于第二个地理位置的数据中心中，称为“灾难恢复站点”。如果主站点中出现站点范围内的数据中心故障，此灾难恢复站点将提供主动-被动站点故障转移。主要站点包括 XenMobile、SQL 数据库、Citrix ADC 基础结构以便在与主站点的连接失败时帮助进行故障转移并向用户提供对 XenMobile 的访问权限。

灾难恢复站点中的 XenMobile Server 在常规操作过程中保持脱机状态，并且仅在灾难恢复场景中恢复联机，在该场景中，需要执行从主站点到灾难恢复站点的完整站点故障转移。灾难恢复站点中的 SQL Server 必须处于活动状态并且可随时向连接提供服务，才能在灾难恢复站点启动 XenMobile Server。

此灾难恢复策略依赖 Citrix ADC 访问层的手动故障转移，通过更改用于在中断时将 MDM 和 MAM 连接路由到灾难恢复站点的 DNS 的方式完成。

> 注意：
>
> 要使用此体系结构，必须具备异步备份数据库的过程以及某些确保 SQL 基础结构的高可用性的方式。

灾难恢复故障转移过程

1. 如果要测试您的灾难恢复故障转移过程，请关闭主站点中的 XenMobile Server 以模拟站点故障。

2. 更改 XenMobile Server 的公共 DNS 记录以指向灾难恢复站点的外部 IP 地址。
3. 更改 SQL Server 的内部 DNS 记录以指向灾难恢复站点的 SQL Server IP 地址。
4. 在灾难恢复站点使 XenMobile SQL 数据库恢复联机。确保 SQL Server 和数据库处于活动状态并且可以随时用来向从本地 XenMobile Server 到站点的连接提供服务。
5. 打开灾难恢复站点上的 XenMobile Server。

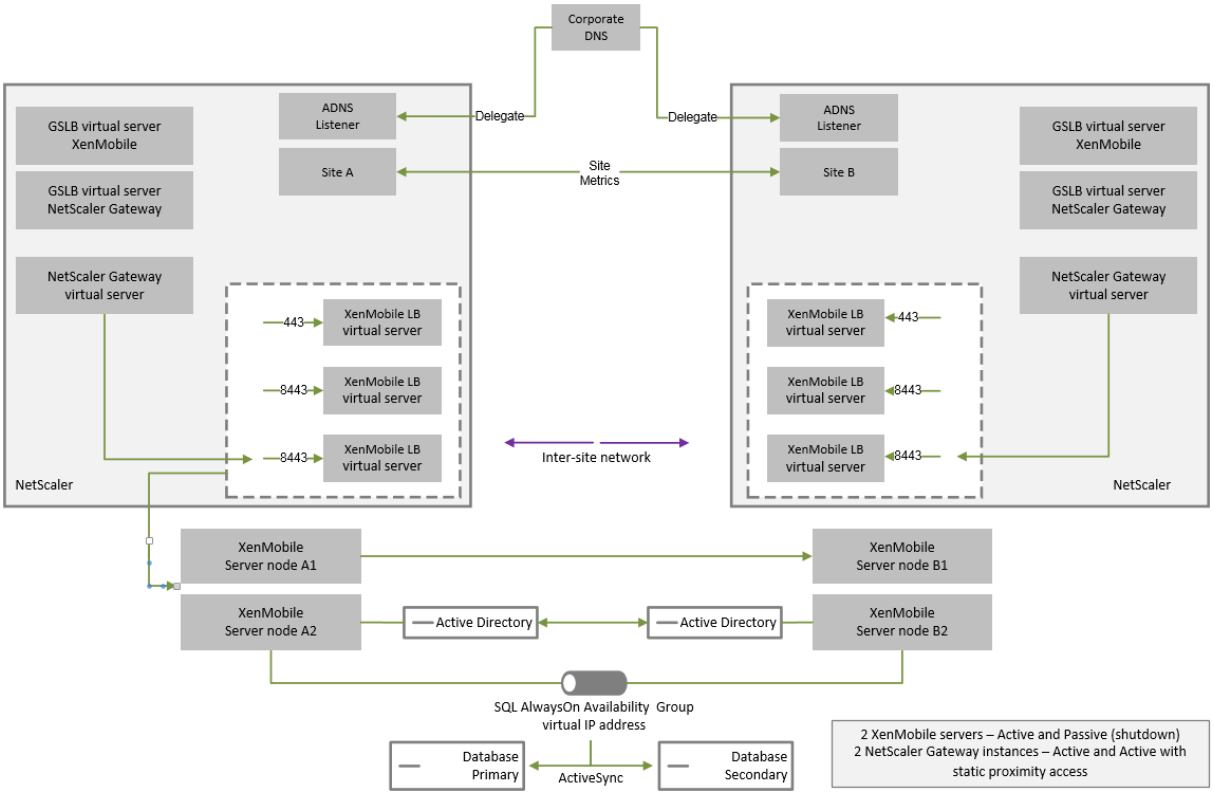
XenMobile Server 更新过程

每次使用修补程序和发行版本更新 XenMobile 时都请按照以下步骤进行操作，以便保持主服务器和灾难恢复服务器的代码相同。

1. 确保主站点中的 XenMobile Server 安装了修补程序或者进行了升级。
2. 确保 SQL Server 的 DNS 记录解析到主站点中的活动 SQL Server 数据库。
3. 使灾难恢复站点的 XenMobile Server 恢复联机。这些服务器仅在升级过程中通过 WAN 连接到主站点的数据库。
4. 对所有灾难恢复站点的 XenMobile Server 应用所需的修补程序和更新。
5. 重新启动 XenMobile Server 并确认修补程序或升级成功完成。

灾难恢复参考体系结构图

下图显示了 XenMobile 的灾难恢复部署的高级体系结构。



使用 **GSLB** 进行灾难恢复

此体系结构的主要元素是使用全局服务器负载平衡 (GSLB) 功能将流量传输到正确的数据中心。

默认情况下，适用于 XenMobile 的 Citrix ADC 向导将通过不允许使用 GSLB 进行灾难恢复的方式来配置 Citrix Gateway。因此，必须执行额外的步骤。

GSLB 的工作原理

GSLB 是 DNS 的核心。参与的 Citrix ADC 设备用作权威 DNS 服务器并将 DNS 记录解析到正确的 IP 地址（通常解析到假定用于接收流量的 VIP）。Citrix ADC 设备先检查系统运行状况，然后再响应将流量传输到该系统的 DNS 查询。

解析记录时，GSLB 在解析流量中所起的作用将完成。客户端将直接与目标虚拟 IP (VIP) 地址进行通信。DNS 客户端行为在控制记录过期的方式和时间方面具有重要作用。这远远超出了 Citrix ADC 系统的界限。因此，GSLB 将遵守与 DNS 名称解析相同的限制。客户端缓存响应；因此，通过这种方式进行的负载平衡并不像传统的负载平衡一样实时进行。

Citrix ADC 上的 GSLB 配置（包括站点、服务和监视器）存在，以便提供正确的 DNS 名称解析。

用于发布服务器的实际配置（在这种情况下，是指适用于 XenMobile 的 Citrix ADC 向导创建的配置）不受 GSLB 影响。GSLB 是 Citrix ADC 上的一项独立服务。

在 **XenMobile** 中使用 **GSLB** 的域委派挑战

适用于 XenMobile 的 Citrix ADC 向导配置适用于 XenMobile 的 Citrix Gateway。此向导将生成三个负载平衡虚拟服务器和一个 Citrix Gateway 虚拟服务器。

其中两个负载平衡虚拟服务器负责在端口 443 和 8443 上处理 MDM 流量。Citrix Gateway 在端口 8443 上接收 MAM 流量并将其转发到第三个服务器，即 MAM 负载平衡虚拟服务器。所有传输到 MAM 负载平衡虚拟服务器的流量都通过 Citrix Gateway 传输。

MAM 负载平衡虚拟服务器所需的 SSL 证书与 XenMobile Server 相同，并且使用的 FQDN 与注册设备时使用的 FQDN 相同。MAM 负载平衡服务器还与其中一个 MDM 负载平衡服务器使用相同的端口 (8443)。为使流量能够被解析，适用于 XenMobile 的 Citrix ADC 向导将在 Citrix Gateway 上创建一条本地 DNS 记录。该 DNS 记录与用于注册设备的 FQDN 一致。

此配置在 XenMobile Server URL 不是 GSLB 域 URL 时有效。如果 GSLB 域 URL 用作 XenMobile Server URL，就像灾难恢复所需的 URL 一样，本地 DNS 记录将阻止 Citrix Gateway 将流量解析到 MDM 负载平衡服务器。

使用 **CNAME** 方法进行 **GSLB** 灾难恢复

为解决适用于 XenMobile 的 Citrix ADC 向导创建的默认配置提出的挑战，可以为父域 (`company.com`) 中的 XenMobile Server FQDN 创建一条 CNAME 记录，并指向 Citrix ADC 对其具有权威的委派子区域 (`gslb.company.com`) 中的记录。这样将允许为解析流量所需的 MAM 负载平衡 VIP 地址创建一条静态 DNS A 记录。

1. 在外部 DNS 上，为指向 Citrix ADC GSLB 上的 GSLB 域 FQDN 的 XenMobile Server FQDN 创建 CNAME。需要两个 GSLB 域：一个用于 MDM 流量，另一个用于 MAM (Citrix Gateway) 流量。

   示例：

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. 在每个站点的 Citrix Gateway 实例中，创建一个使用 CNAME 记录指向的 FQDN 的 GSLB 虚拟服务器。

   示例：

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   使用适用于 XenMobile 的 Citrix ADC 向导部署 Citrix Gateway 时，请在配置 MAM 负载平衡服务器时使用 XenMobile Server URL。这将为 XenMobile Server URL 创建一条静态 DNS A 记录。

3. 使用 XenMobile Server URL (`xms.company.com`) 对在 Secure Hub 中注册的客户端进行测试。

   此示例使用以下 FQDN：

   - `xms.company.com` 是 MDM 流量使用的 URL，并且由设备注册过程使用，在此示例中是使用适用于 XenMobile 的 Citrix ADC 向导配置的。
   - `xms.gslb.company.com` 是 XenMobile Server 的 GSLB 域 FQDN。

Citrix 支持过程

January 5, 2022

可以请 Citrix Technical Support Services 团队帮助解决与 Citrix 产品有关的问题。该团队提供解决方法和解决方案，并且与开发团队紧密合作以提供解决方案。

Citrix Consulting Services 或 Citrix Education Services 提供与产品培训有关的帮助以及与产品使用情况、配置、安装或环境设计和体系结构有关的建议。

Citrix Consulting 协助完成与 Citrix 产品有关的项目，包括概念证明、经济影响评估、基础结构运行状况检查、设计要求分析、体系结构设计验证、集成和操作过程开发。

Citrix Education 提供针对 Citrix 虚拟化、云和网络连接技术的一流 IT 培训和认证。

Citrix 建议您在创建支持案例之前充分利用 Citrix 自助服务资源和建议。例如，您可以从多个位置访问 Citrix 技术专家撰写的文章和公告、查看针对 Citrix 解决方案和技术的产品文档或者阅读来自 Citrix 主管、产品团队和技术专家的坦率谈话。请分别参阅知识中心、产品文档和博客页面。

要获得更多交互式帮助，可以参与讨论论坛，您可以在论坛中提问问题以及获取其他客户提供的现实答案、在用户小组和兴趣小组内部共享想法、意见、技术信息和最佳做法，或者与负责监视 Citrix 支持社交网络站点的 Citrix 支持工程师互动。请分别参阅支持论坛和 Citrix 社区页面。

您还有权访问培训和认证课程以提高自己的技能。请参阅 Citrix Education。

Citrix Insight Services 提供适用于您的 Citrix 环境的简单在线故障排除平台和运行状况检查器。适用于 XenMobile、Citrix Virtual Apps and Desktops、Citrix Hypervisor 和 Citrix Gateway。请参阅分析工具。

要获取技术支持，可以通过电话或网络创建支持案例。对于严重性较低和中等严重性的问题，可以使用网络，对于严重性较高的问题，可以使用电话。有关联系技术支持以帮助解决 XenMobile 问题的信息，请参阅 How to Contact Support（如何联系技术支持）。

如果寻求在交付 Citrix 解决方案方面具有丰富经验的训练有素的单一联系人，Citrix Services 提供技术关系经理。有关 Citrix 服务方案和效益的详细信息，请参阅 Citrix Worldwide Services（Citrix 全球服务）。

在 **XenMobile** 中发送组注册邀请

October 13, 2021

文档贡献者：John Bartel III

可以向 XenMobile Server 中的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。还可以标记设备，以便能够（例如）将公司拥有的设备与员工拥有的设备区分开来。之后，请为用户设备设置身份验证类型。

> 注意：
>
> 如果您打算使用自定义通知模板，必须在配置注册安全模式之前设置模板。有关通知模板的详细信息，请参阅创建和更新通知模板。

有关用户帐户、角色和注册安全模式以及邀请的基础配置的详细信息，请参阅用户帐户、角色和注册。

常规步骤

1. 在 XenMobile 控制台中，导航到管理 **>** 注册邀请。
2. 单击屏幕左上角的添加，然后单击添加邀请。
3. 单击收件人菜单中的组。

   在此步骤中，可以选择一个或多个平台。如果贵公司混合使用不同的操作系统平台，请选择所有平台。仅当确定所有用户都未使用特定的平台时，才能取消选中该平台。
4. 邀请过程中，可以选择标记设备。选择公司或员工。

   通过标记设备，可以轻松分离公司拥有的设备和员工拥有的设备。
5. 在域列表中，选择组所在的域。
6. 在组列表中，选择要向其发送邀请的 Active Directory 组。
7. 注册模式允许您设置更希望用户使用的身份验证安全性类型。

- 用户名 + 密码
- 高安全性
- 邀请 URL
- 邀请 URL + PIN
- 邀请 URL + 密码
- 双重
- 用户名 + PIN

> 注意：
>
> 要发送注册邀请，只能使用邀请 **URL**、邀请 **URL + PIN** 或邀请 **URL +** 密码注册安全模式。对于使用用户名 **+** 密码、双重或用户名 **+ PIN** 注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

8. 对于代理下载、注册 **URL**、注册 **PIN** 和注册确认模板，请选择您以前创建的自定义通知模板。或者，请选择列出的默认模板。

   如果您打算使用自定义通知模板，必须在配置注册安全模式之前设置模板。有关通知模板的详细信息，请参阅通知。

   对于这些通知模板，请使用您在 XenMobile 中配置的 SMTP 服务器设置。请先设置 SMTP 信息，然后再继续操作。

   > 注意：
   >
   > 此时间后过期和最大尝试次数选项根据您选择的注册模式选项而变化。不能更改这些选项。

9. 请为发送邀请选择“开”，然后单击保存并发送以完成该过程。

嵌套组支持

可以使用嵌套组发送邀请。通常情况下，嵌套组在具有相似权限的组相互绑定的大型环境中使用。

导航到设置 **> LDAP**，然后启用支持嵌套组选项。

故障排除和已知限制

问题：即使已将用户从 Active Directory 组中删除，也可以向这些用户发出邀请。

解决方案：最长可能需要 6 个小时才能将更改传播到所有服务器，具体取决于您的 Active Directory 环境的规模。如果最近删除了某个用户或嵌套组，XenMobile 可能仍然会将这些用户视为组的一部分。

因此，最好等待 6 个小时以后再向您的组发出其他组邀请。

配置本地设备运行状况证明服务器

January 5, 2022

文档贡献者：Sanket Mishra

可以通过本地 Windows Server 为 Windows 10 和 Windows 11 移动设备启用设备运行状况证明 (DHA)。要在本地启用 DHA，请先配置一个 DHA 服务器。

配置 DHA 服务器后，请创建 XenMobile Server 策略以启用本地 DHA 服务。有关创建此策略的信息，请参阅设备运行状况证明设备策略。

DHA 服务器的必备项

- 运行使用“桌面体验”安装选项安装的 Windows Server Technical Preview 5 或更高版本的服务器。
- 一个或多个 Windows 10 和 Windows 11 客户端设备。这些设备必须安装运行最新 Windows 版本的 TPM 1.2 或 2.0。
- 以下证书：
  - **DHA SSL** 证书。链接到具有可导出的私钥的企业可信根证书的 x.509 SSL 证书。此证书保护正在传输的 DHA 数据通信，包括服务器到服务器（DHA 服务和 MDM 服务器）和服务器到客户端（DHA 服务和 Windows 10 或 Windows 11 设备）通信。
  - **DHA** 签名证书。链接到具有可导出的私钥的企业可信根证书的 x.509 证书。DHA 服务使用此证书进行数字签名。
  - **DHA** 加密证书。链接到具有可导出的私钥的企业可信根证书的 x.509 证书。DHA 服务还使用此证书进行加密。
- 请选择下面的其中一种证书验证模式：
  - **EKCert**。EKCert 验证模式已针对组织中未连接到 Internet 的设备进行优化。连接到在 EKCert 验证模式下运行的 DHA 服务的设备不能直接访问 Internet。
  - **AIKCert**。AIKCert 验证模式已针对能够直接访问 Internet 的运行环境优化。连接到在 AIKCert 验证模式下运行的 DHA 服务的设备必须能够直接访问 Internet，并且能够从 Microsoft 获取 AIK 证书。

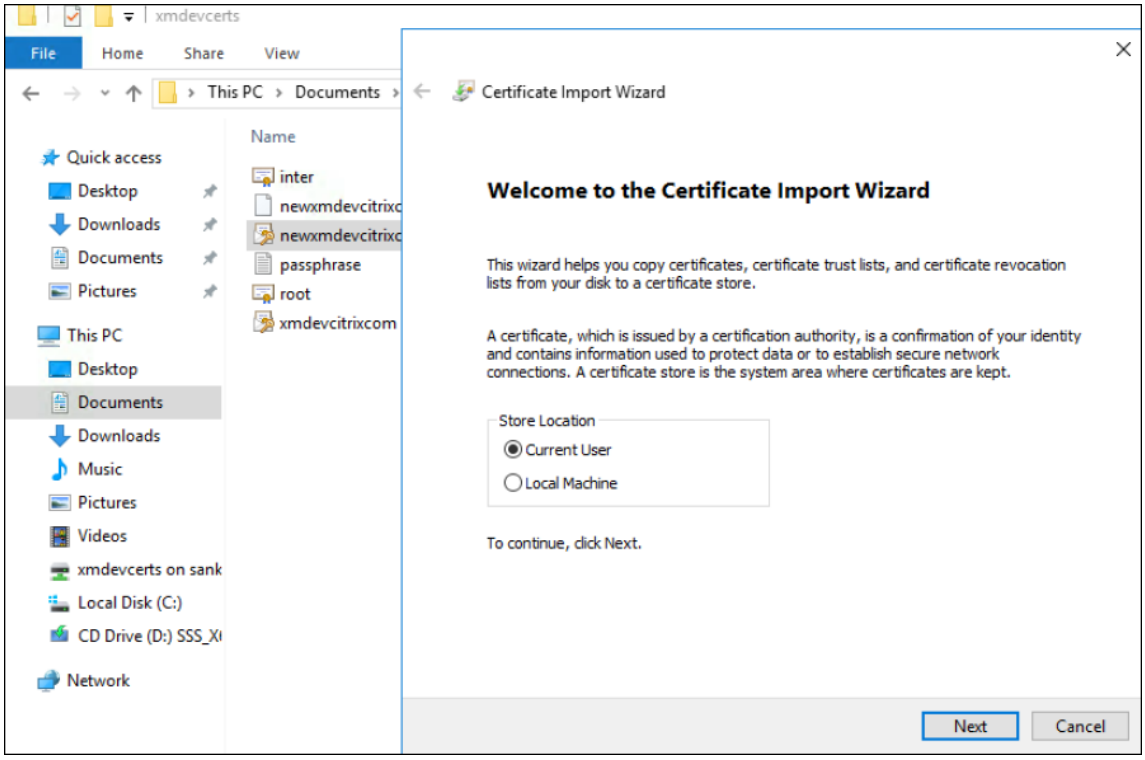
向 Windows Server 中添加 DHA 服务器角色

1. 在 Windows Server 中，如果尚未打开服务器管理器，请单击开始，然后单击服务器管理器。
2. 单击添加角色和功能。
3. 在开始之前页面上，单击下一步。
4. 在选择安装类型页面上，单击基于角色或基于功能的安装，然后单击下一步。
5. 在选择目标服务器页面上，单击从服务器池中选择服务器，选择服务器，然后单击下一步。
6. 在选择服务器角色页面上，选中“设备运行状况证明”复选框。
7. 可选：单击添加功能以添加所需的其他角色服务和功能。
8. 单击 **Next**（下一步）。
9. 在选择功能页面上，单击下一步。
10. 在 **Web** 服务器角色 **(IIS)** 页面上，单击下一步。
11. 在选择角色服务页面上，单击下一步。
12. 在设备运行状况证明服务页面上，单击下一步。

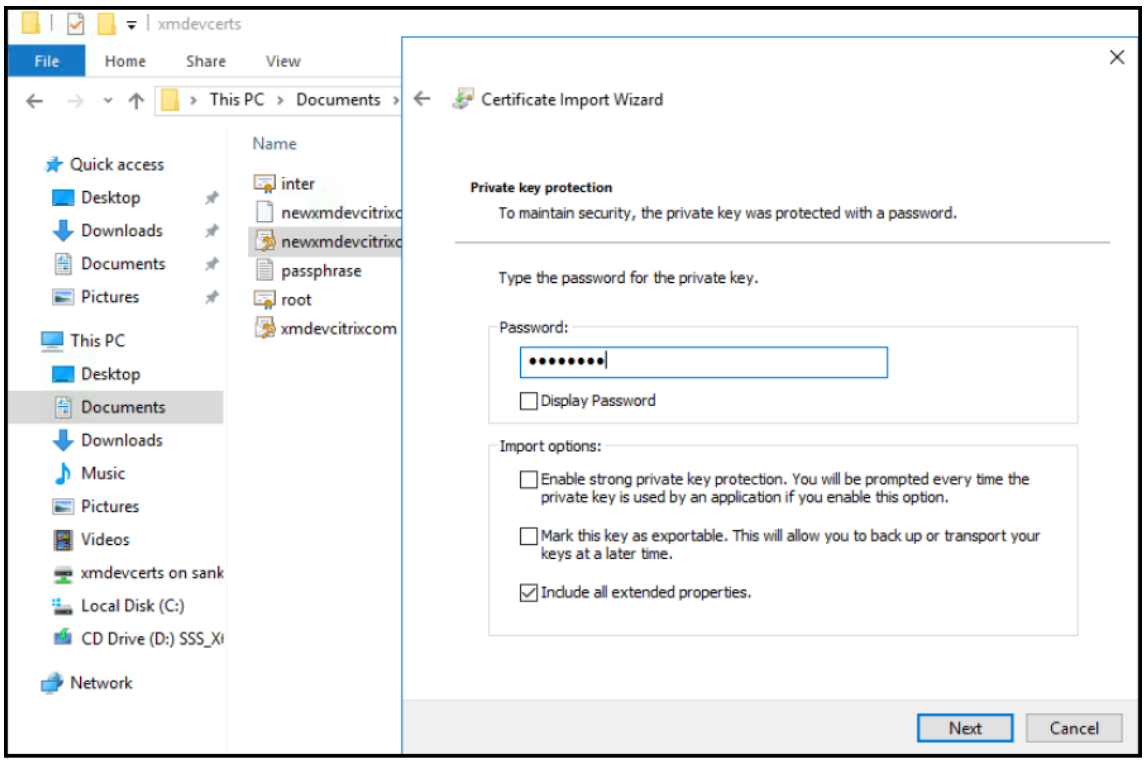
13. 在确认安装选项页面上，单击安装。
14. 安装完成后，单击关闭。

向服务器的证书存储中添加 **SSL** 证书

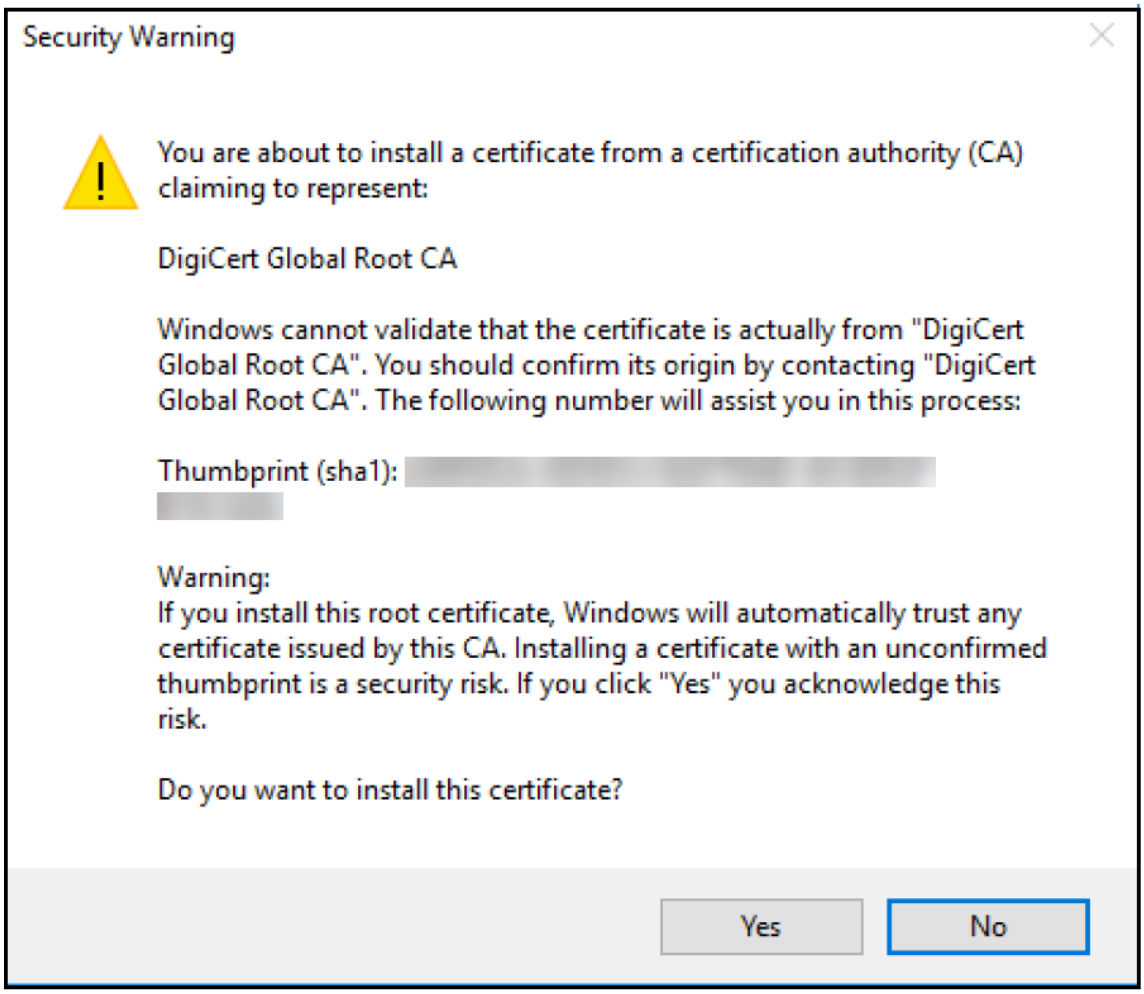
1. 转至 SSL 证书文件并选择该文件。
2. 选择当前用户作为存储位置，然后单击下一步。



3. 键入私钥对应的密码。
4. 确保选中导入选项包括所有扩展属性。单击 **Next**（下一步）。



5. 显示此窗口时，单击是。



6. 确认证书是否已安装：

   a) 打开命令提示窗口。

   b) 键入 **mmc** 并按 Enter 键。您必须是管理员角色，才能查看本地计算机存储中的证书。

   c) 在“文件”菜单中，单击添加/删除管理单元。

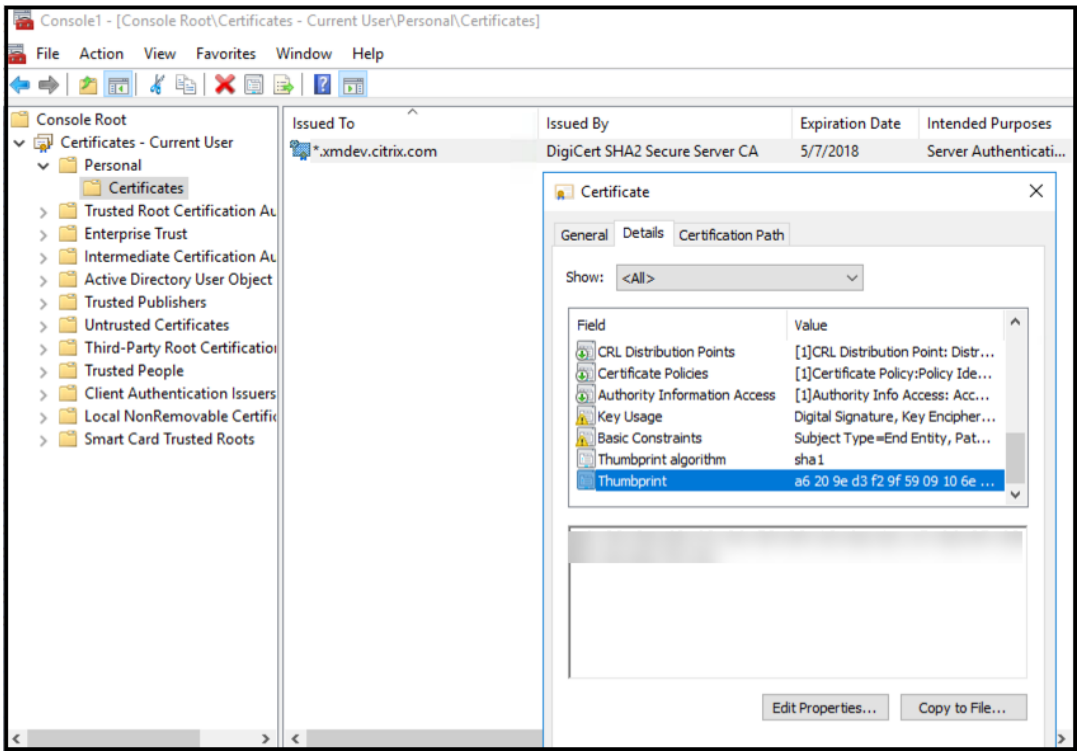
   d) 单击添加。

   e) 在“添加独立管理单元”对话框中，选择证书。

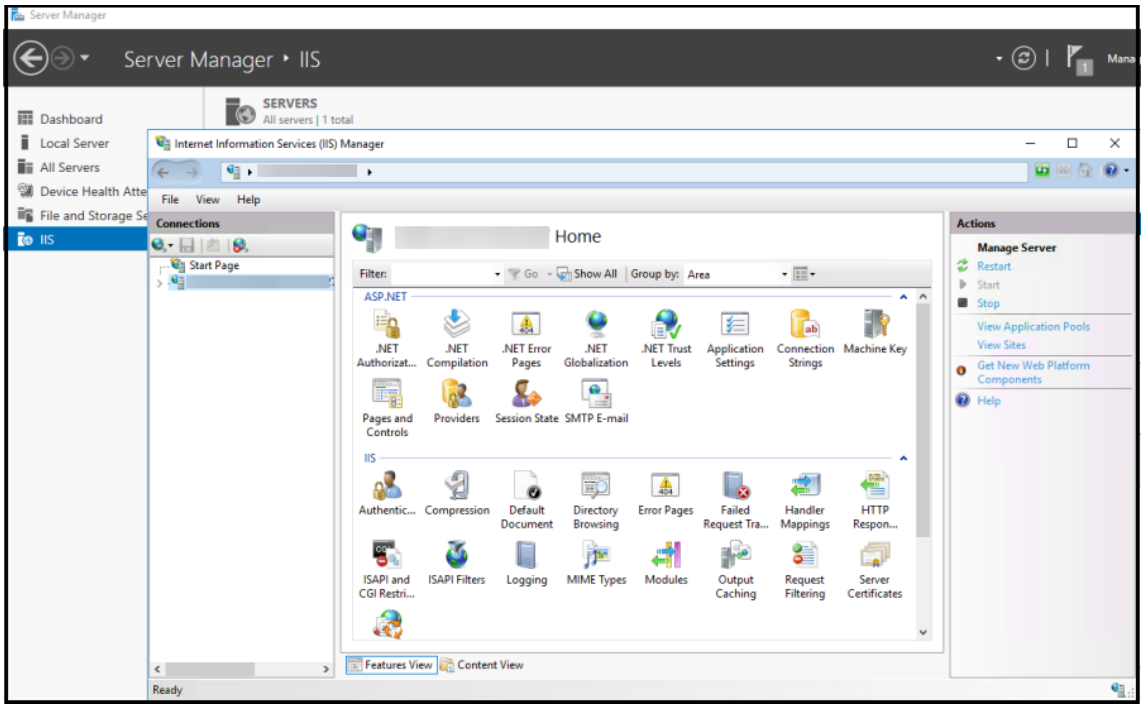
   f) 单击添加。

   g) 在“证书管理单元”对话框中，选择我的用户帐户。（如果您以服务帐户所有者的身份登录，请选择服务帐户。）

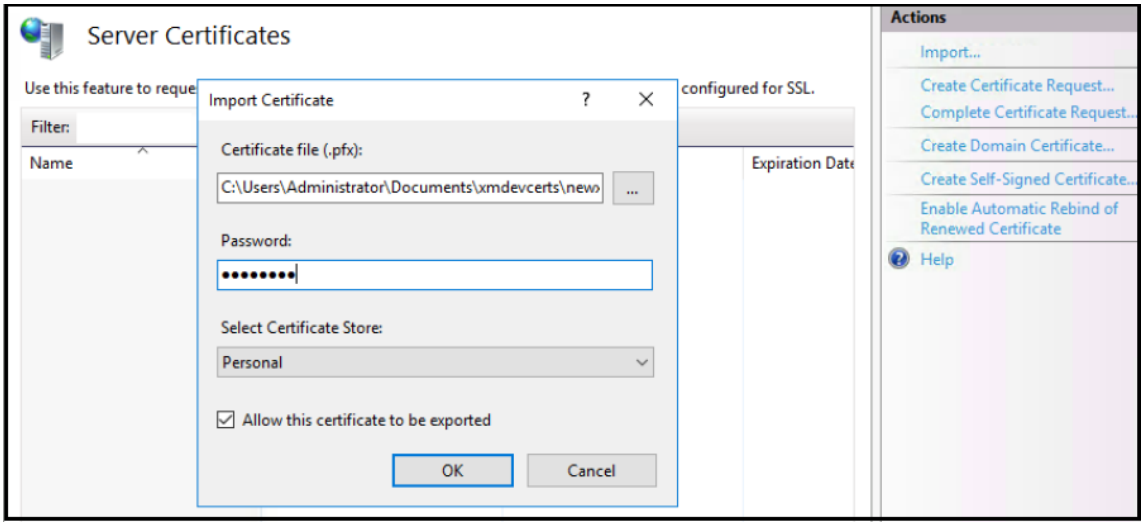
   h) 在“选择计算机”对话框中，单击完成。



7. 转至服务器管理器 **> IIS**，然后从图标列表中选择服务器证书。

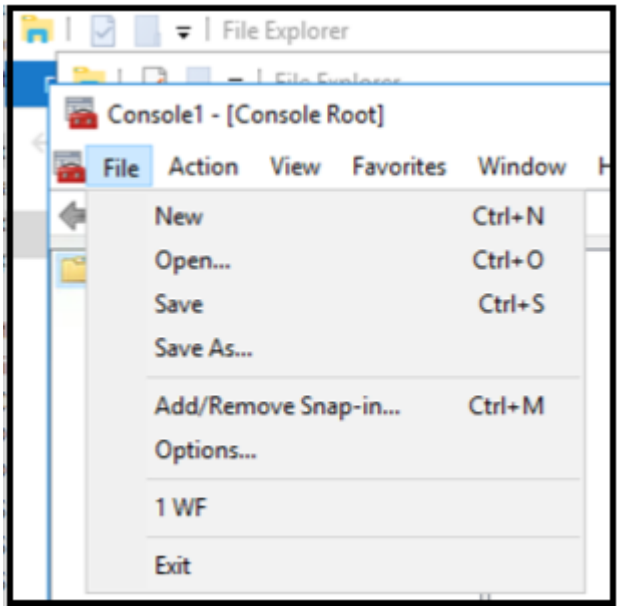


8. 在“操作”菜单中，选择导入**...** 以导入 SSL 证书。

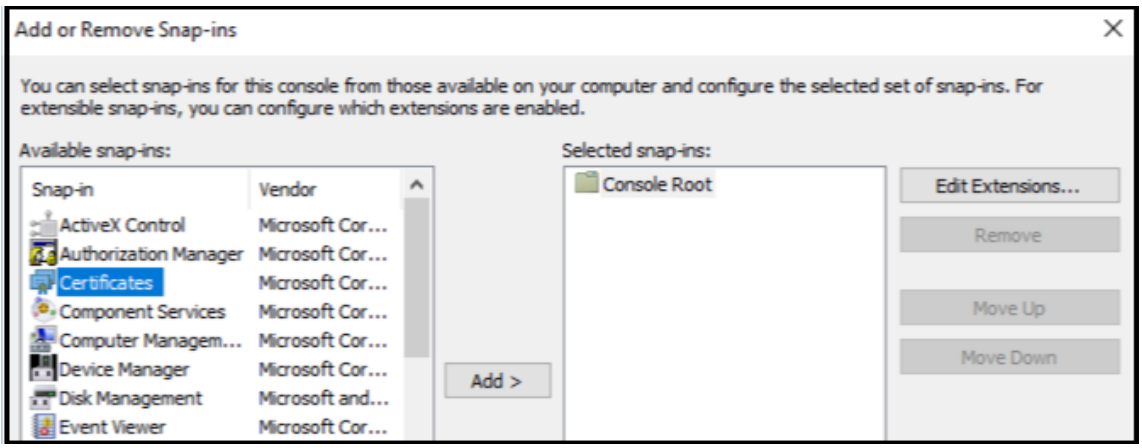


获取并保存证书的指纹

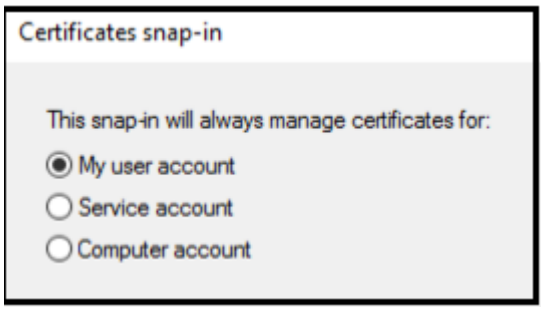
1. 在“文件资源管理器”搜索栏中，键入 **mmc**。
2. 在“控制台根节点”窗口中，单击文件 **>** 添加/删除管理单元**...**。



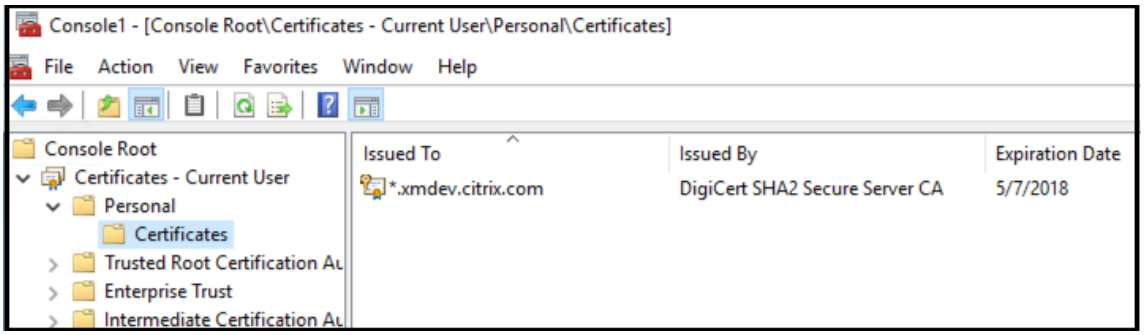
3. 从可用管理单元中选择证书并将其添加到选定的管理单元中。



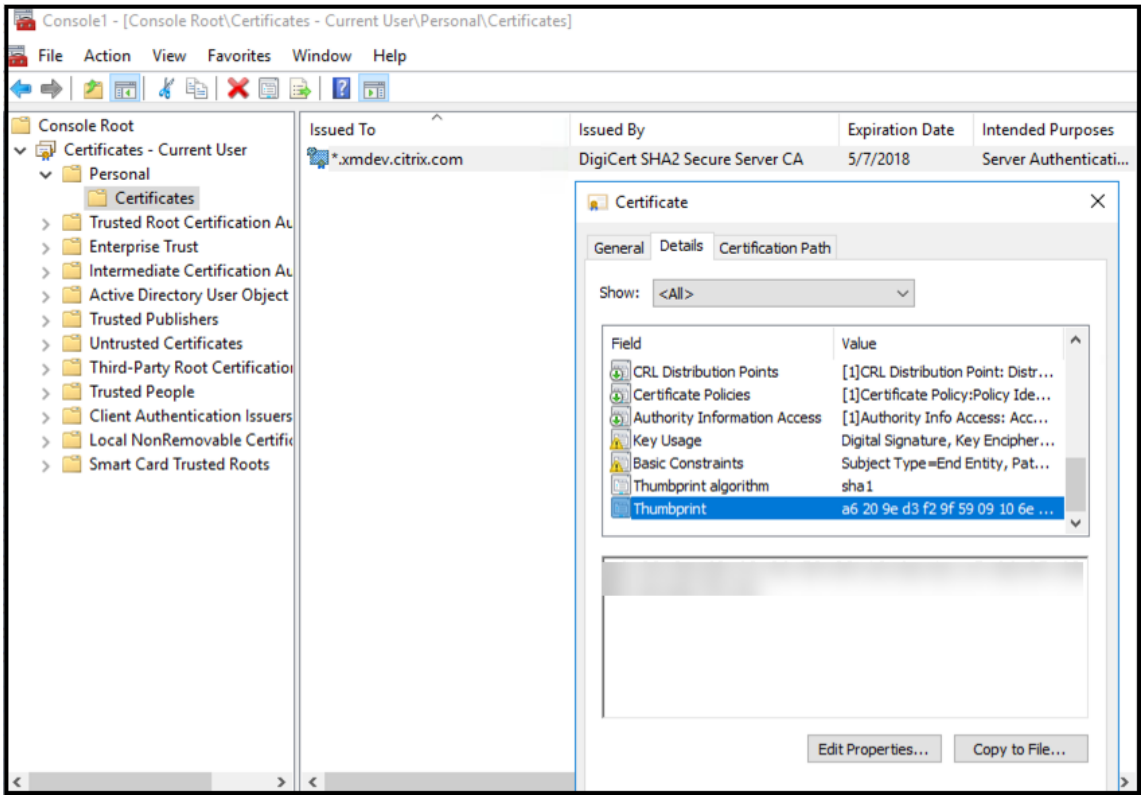
4. 选择我的用户帐户。



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. 将指纹复制到文件中。在 PowerShell 命令中使用指纹时，请删除空格。

安装签名证书和加密证书

在 Windows Server 上运行以下 PowerShell 命令以安装签名证书和加密证书。

替换占位符 ReplaceWithThumbprint 并在两边加双引号，如下所示。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
   $keyname icacls $keypath /grant IIS_IUSRS`:R
<!--NeedCopy-->
```

提取 **TPM** 根证书并安装可信证书包

在 Windows Server 上运行以下命令：

```
mkdir .\TrustedTpm
```



```
2
3 expand -F:* .\TrustedTpm.cab .\TrustedTpm
4
5 cd .\TrustedTpm
6
7 .\setup.cmd
8 <!--NeedCopy-->
```

配置 **DHA** 服务

在 Windows Server 上运行以下命令以配置 DHA 服务。

替换占位符 ReplaceWithThumbprint。

```
1 Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
     ReplaceWithThumbprint
2
3 -SigningCertificateThumbprint ReplaceWithThumbprint
4
5 -SslCertificateStoreName My -SslCertificateThumbprint
     ReplaceWithThumbprint
6
7 -SupportedAuthenticationSchema "AikCertificate"
8 <!--NeedCopy-->
```

在 Windows Server 上运行以下命令以为 DHA 服务设置证书链策略：

```
1 $policy = Get-DHASCertificateChainPolicy
2
3 $policy.RevocationMode = "NoCheck"
4
5 Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
6 <!--NeedCopy-->
```

响应以下提示，如下所示：

```
1   Confirm
2
3     Are you sure you want to perform this action?
4
5     Performing the operation "Install-DeviceHealthAttestation" on
         target "WIN-N27D1FKCEBT".
6
7     [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
         Help (default is "Y"): A
```



```
8
9       Adding SSL binding to website 'Default Web Site'.
10
11      Add SSL binding?
12
13      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15      Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17      Add application pool?
18
19      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21      Adding web application 'DeviceHealthAttestation' to website '
           Default Web Site'.
22
23      Add web application?
24
25      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27      Adding firewall rule 'Device Health Attestation Service' to allow
           inbound connections on port(s) '443'.
28
29      Add firewall rule?
30
31      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33      Setting initial configuration for Device Health Attestation Service
           .
34
35      Set initial configuration?
36
37      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39      Registering User Access Logging.
40
41      Register User Access Logging?
42
43      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
44  <!--NeedCopy-->
```

检查配置

要检查 DHASActiveSigningCertificate 是否处于活动状态，请在服务器上运行以下命令：

`Get-DHASActiveSigningCertificate`

如果证书处于活动状态，则将显示证书类型（签名证书）和指纹。

要检查 DHASActiveSigningCertificate 是否处于活动状态，请在服务器上运行这些命令

替换占位符 ReplaceWithThumbprint 并在两边加双引号，如下所示。

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
    -Force

Get-DHASActiveEncryptionCertificate
<!--NeedCopy-->
```

如果证书处于活动状态，则将显示指纹。

要执行最终检查，请转至以下 URL：

`https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1`

如果 DHA 服务正在运行，则将显示 “Method not allowed”（方法不允许）。

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

January 5, 2022

文档贡献者：Vijay Kumar Kunchakuri

必须将 Exchange Server 配置为进行基于证书的身份验证，以确保 Secure Mail 推送通知能够正常接收。在启用了基于证书的身份验证的 XenMobile 中注册 Secure Hub 时，此要求尤为必要。

您需要在进行基于证书的身份验证的 Exchange Mail Server 上配置 Active Sync 和 Exchange Web 服务 (EWS) 虚拟目录。

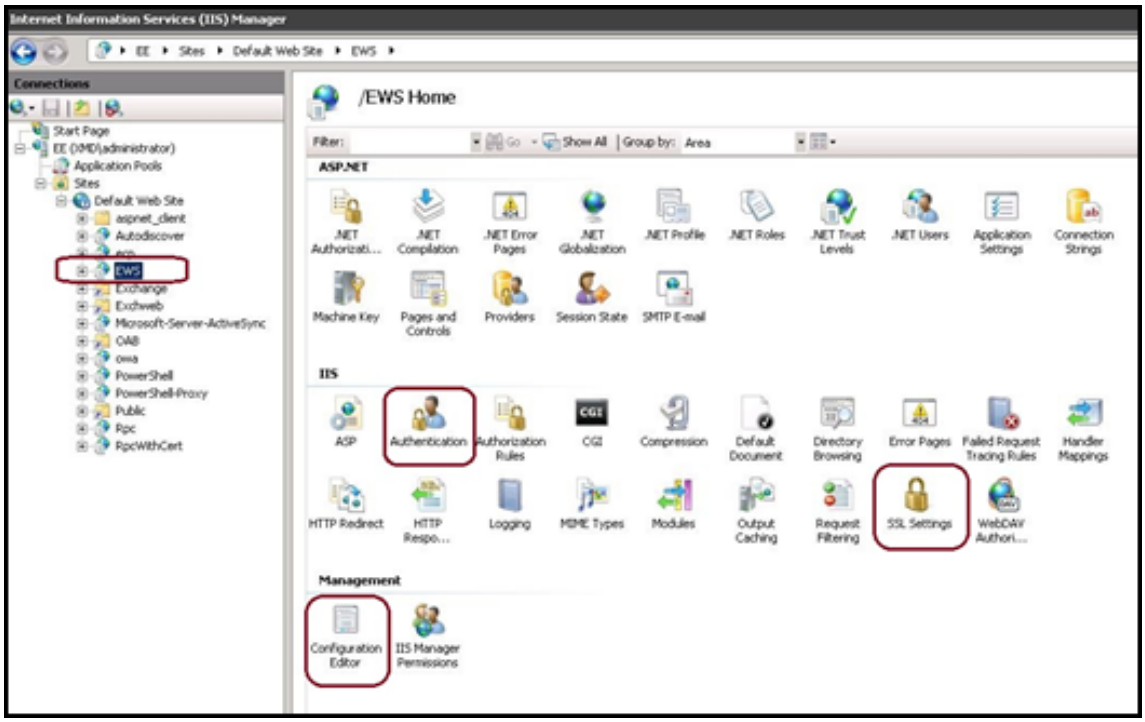
除非完成这些配置，否则对 Secure Mail 推送通知的订阅将失败，并且 Secure Mail 中不会发生任何徽章更新。

本文介绍了配置基于证书的身份验证的步骤。这些配置专门针对 Exchange Server 上的 EWS 虚拟目录。

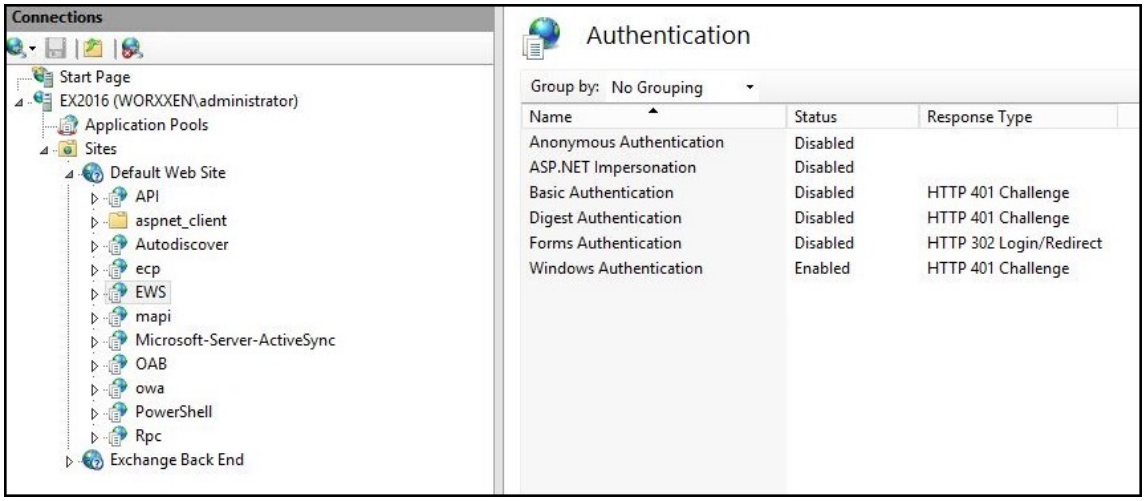
要开始配置，请执行以下操作：

1. 登录安装了 EWS 虚拟目录的一个或多个服务器。
2. 打开 IIS 管理器控制台。
3. 在 **Default Web Site**（默认 Web 站点）下，单击 EWS 虚拟目录。

   “身份验证”、“SSL” 和 “配置编辑器” 管理单元位于 IIS 管理器控制台的右侧。



4. 确保 EWS 的身份验证设置按下图中所示进行配置。

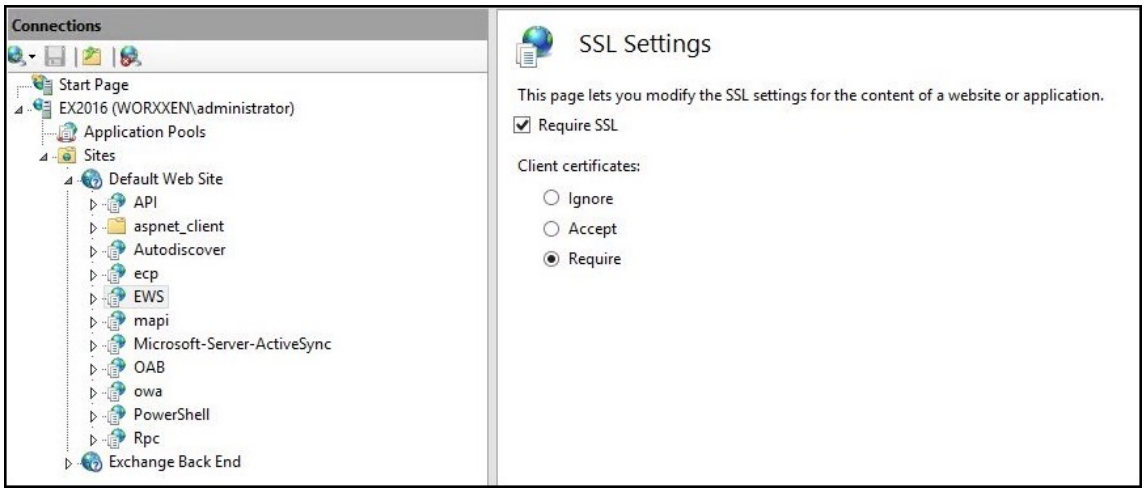


5. 为 EWS 虚拟目录配置 **SSL** 设置。

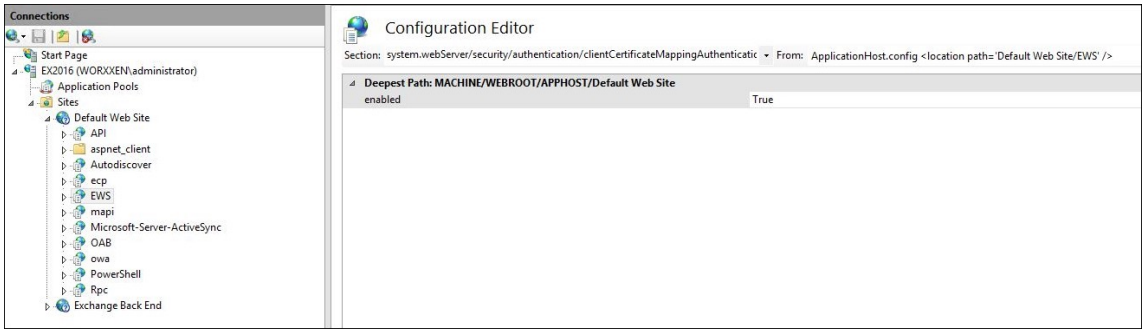
   a) 选中 **Require SSL**（要求 SSL）复选框。

   b) 在 **Client Certificates**（客户端证书）下，单击 **Require**（需要）。如果其他 EWS 邮件客户端使用用

户名和密码作为身份验证凭据进行连接，并且连接到 Exchange Server，可以将此选项设置为 **Accept**（接受）。



6. 单击 **Configuration Editor**（配置编辑器）并在 **Section**（部分）下拉列表中，导航到以下部分：
   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**
7. 将 **enabled** 值设置为 **True**。

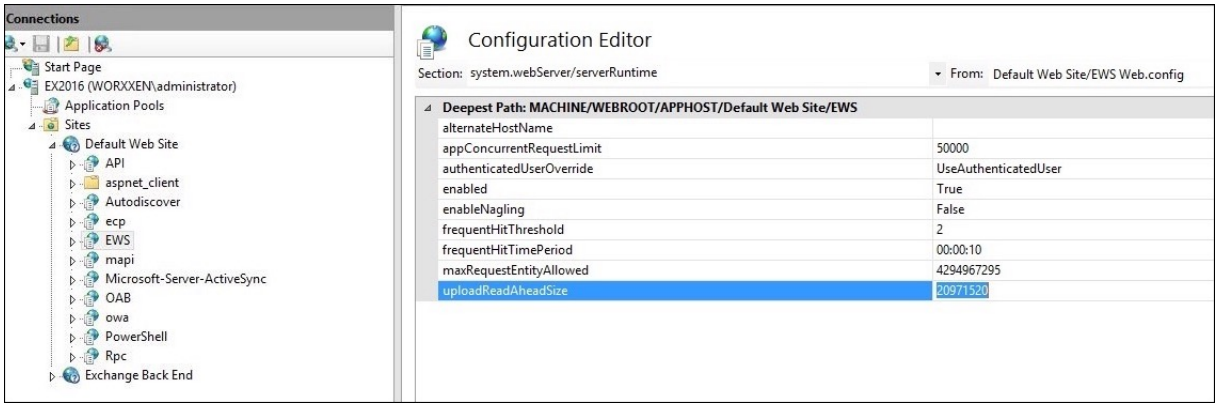


8. 单击 **Configuration Editor**（配置编辑器）并在 **Section**（部分）下拉列表中，导航到以下部分：
   - **system.webServer/serverRuntime**
9. 将 **uploadReadAheadSize** 值设置为 **10485760** (10 MB) 或 **20971520** (20 MB)，或者设置为贵组织需要的值。

   > 重要：
   >
   > 如果未正确设置此值，订阅 EWS 推送通知时基于证书的身份验证可能会失败，并显示错误代码 413。
   >
   > 请勿将此值设置为 **0**。

有关详细信息，请参阅以下第三方资源：

- Microsoft IIS 服务器运行时
- Butsch 客户端管理博客



有关对 Secure Mail 存在的 iOS 推送通知问题进行故障排除的详细信息，请参阅此 Citrix 支持知识中心文章。

相关信息

Secure Mail for iOS 的推送通知

将 XenMobile 移动设备管理 (MDM) 与 Cisco Identity Services Engine (ISE) 集成

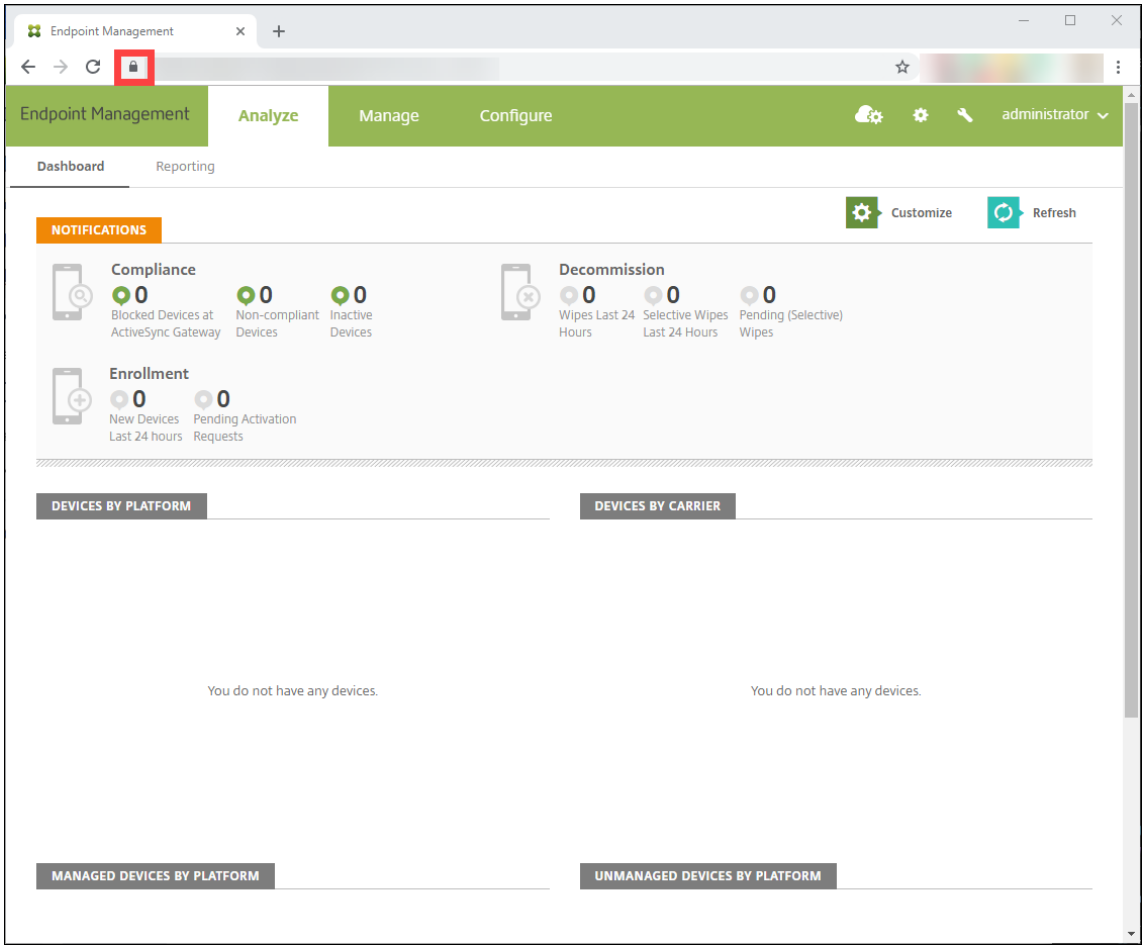
August 10, 2020

文档贡献者：John Bartel III

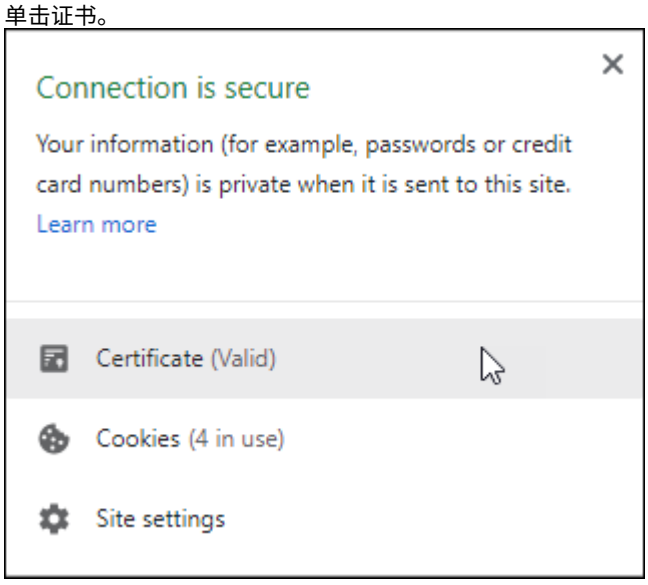
Cisco ISE 用于在工作场所部署、保护、监视、集成和管理移动设备。下载到移动设备的软件控制应用程序和修补程序的分发，以及控制端点上的数据和配置。XenMobile 可以与 Cisco ISE 集成，以管理 Cisco ISE 控制台上的不合规和非托管设备。XenMobile 还允许您有选择地允许、拒绝或隔离对企业服务的访问。

要设置与 XenMobile 的集成，请在 XenMobile Server 上创建一个本地服务帐户，并为其分配管理员 RBAC 角色。此角色允许 Cisco ISE 访问 XenMobile API。ISE 需要信任 XenMobile 证书。要下载此证书，请打开 Web 浏览器并导航到您的服务器 URL 并登录。

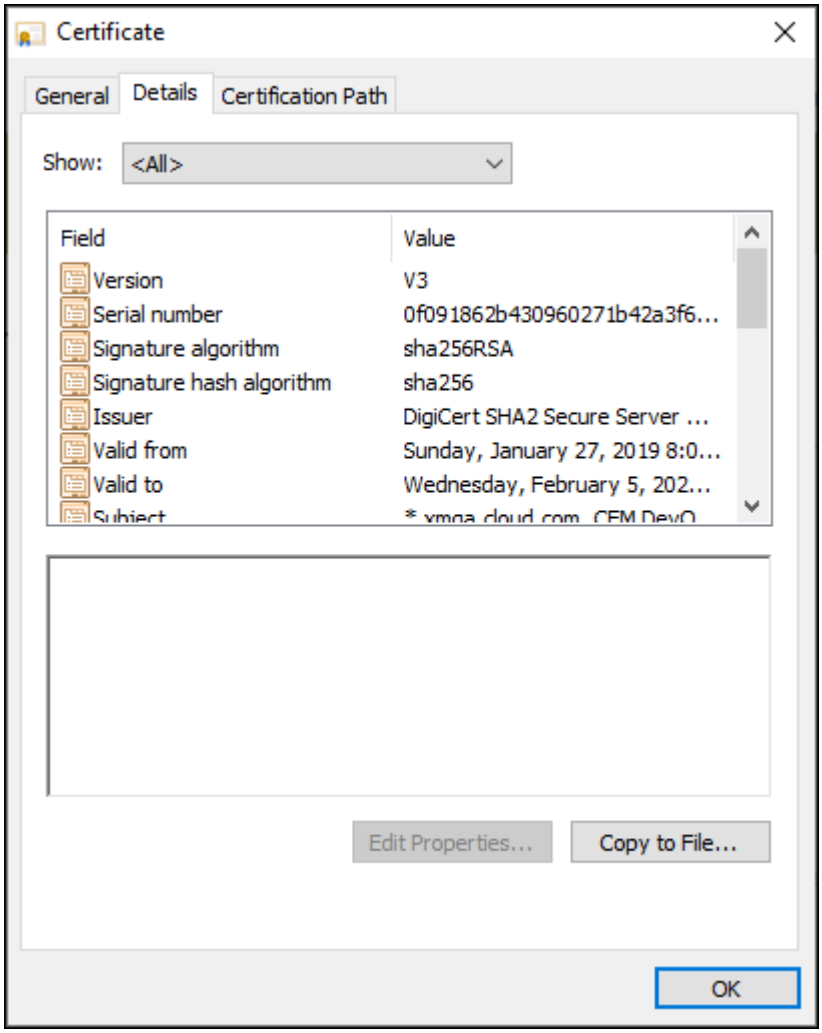
1. 登录后，单击地址栏中 URL 旁边的锁。



2. 单击证书。



3. 选择详细信息选项卡，然后单击复制到文件。



4. 按照向导在本地保存证书。
5. 登录到您的 Cisco ISE 控制台并导入之前下载的 XenMobile 证书。将证书导入 Cisco ISE 的可信证书存储中。需要执行此导入到做，Cisco ISE 才能信任与 XenMobile Server 的通信。
   a) 导航到管理 **>** 系统 **>** 证书 **>** 证书管理 **>** 可信证书。单击导入。
   b) 为证书指定一个名称，然后选中 **Trust for authentication within ISE**（信任 ISE 中的身份验证）和 **Trust for authentication of Cisco Services**（信任 Cisco Services 的身份验证）复选框。
6. 添加 XenMobile 作为 Cisco ISE 内部的外部 MDM。
   a) 导航到管理 **>** 网络资源 **>** 外部 **MDM**。单击添加并填写以下内容：
      - 服务器主机：您的 XenMobile FQDN
      - 端口： 443
      - 实例名称： XenMobile Server 的实例名称。在大多数部署中，实例名称默认为 “zdm”。
      - 用户名：键入您为此任务创建的用户的名称。用户应是原始管理员 RBAC 组中的一个本地管理员帐户。
      - 密码：您刚刚添加的用户的密码。
      - 检查其是否显示为启用。

7. 如果测试成功，请单击提交。

有关 Cisco ISE 的详细信息，请参阅 Cisco 文档。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States