滚动补丁的发行说明

本节包含 XenMobile® Server 最新滚动补丁的发行说明。单击下面的链接可查看已修复和已知问题、功能更改以及所需操作。

最新的滚动补丁包含同一版本之前所有滚动补丁中的所有修复。

当前版本补丁的发行说明	发布日期	支持文章
10.16 滚动修补程序 9	Sep 17, 2026	发行说明
10.16 滚动修补程序 8	Jan 27, 2026	发行说明
10.16 滚动修补程序 7	Nov 13, 2025	发行说明
10.16 滚动修补程序 6	Sep 26, 2025	发行说明
10.16 滚动修补程序 5	Apr 22, 2025	CTX692919
10.16 滚动修补程序 4	Dec 18, 2024	CTX692370
10.16 滚动修补程序 3	Aug 28, 2024	CTX691503
10.16 滚动修补程序 2	Jul 02, 2024	CTX678043
10.16 滚动补丁 1	Jun 17, 2024	CTX677872

先前版本补丁的发行说明	发布日期	支持文章
10.15 滚动补丁 14	Jul 02, 2026	发行说明
10.15 滚动补丁 13	Nov 20, 2025	发行说明
10.15 滚动补丁 12	Oct 23, 2025	发行说明
10.15 滚动补丁 11	May 13, 2025	CTX693257
10.15 滚动补丁 10	Jan 27, 2025	CTX692560

先前版本补丁的发行说明	发布日期	支持文章
10.15 滚动补丁 9	Dec 04, 2024	CTX692268
10.15 滚动补丁 8	Jul 11, 2024	CTX691107
10.15 滚动补丁 7	Jun 06, 2024	CTX677079
10.15 滚动补丁 6	Mar 06, 2024	CTX625010
10.15 滚动补丁 5	Nov 13, 2023	CTX583748
10.15 滚动补丁 4	Sep 18, 2023	CTX579528
10.15 滚动补丁 3	Jul 19, 2023	CTX565649
10.15 滚动补丁 2	Apr 26, 2023	CTX546782
10.15 滚动补丁 1	Feb 23, 2023	CTX478719
10.14 滚动补丁 13	Mar 08, 2024	CTX628921
10.14 滚动补丁 12	Oct 19, 2023	CTX582535
10.14 滚动补丁 11	May 31, 2023	CTX558678
10.14 滚动补丁 10	Mar 23, 2023	CTX491036
10.14 滚动修补程序 9	Dec 20, 2022	CTX477055
10.14 滚动修补程序 8	Sep 22, 2022	CTX464099
10.14 滚动修补程序 7	Aug 18, 2022	CTX463691
10.14 滚动修补程序 6	May 23, 2022	CTX459871
10.14 滚动修补程序 5	Mar 30, 2022	CTX399411
10.14 滚动补丁 4	Jan 26, 2022	CTX339069
10.14 滚动补丁 3	Dec 22, 2021	CTX335897
10.14 滚动补丁 2	Dec 15, 2021	CTX335763

先前版本补丁的发行说明	发布日期	支持文章
10.14 滚动补丁 1	Nov 19, 2021	CTX335342

适用于 XenMobile Server 10.16 滚动修补程序 9 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动修补程序 9 的增强功能、已修复问题和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.16 滚动修补程序 9 软件二进制文件。

新增功能

- **支持在启动器配置设备策略中启用系统信息：**

  已为 Android Enterprise 设备在启动器配置设备策略中添加了一个新设置：**启用系统信息**。此设置允许 Citrix Launcher 在状态栏中显示系统信息。默认值为**关**，需要 Secure Hub 26.8 或更高版本。有关详细信息，请参阅 启动器配置策略。

- **支持在启动器配置设备策略中自动启动应用程序：**

  已为 Android Enterprise 设备在启动器配置设备策略中添加了一个新设置：**自动启动应用程序**。此设置允许管理员选择一个**允许的应用程序**，以便在 Citrix Launcher 启动时自动启动。默认值为**无（不自动启动）**，需要 Citrix Launcher 26.8 或更高版本。有关详细信息，请参阅 启动器配置策略。

  XenMobile Server 具有一个新属性 `afw.launcher.auto_launch`，它使管理员能够为配置了启动器配置策略的 Android Enterprise 设备配置自动启动应用程序。默认值为 **False**。有关详细信息，请参阅 服务器属性。

- **支持设备应用程序的搜索应用程序选项：**

  在 XenMobile Server 控制台中，**设备 > 设备详细信息 > 应用程序**页面现在包含一个新的**搜索应用程序**选项。

- **支持应用程序设置设备策略：**

  在**配置（声明性）**下添加了一个新的设备策略：**应用程序设置**。此策略允许您使用 Apple 的声明性设备管理来配置应用程序允许和拒绝列表。此策略仅支持受监督的 iOS 27 及更高版本设备。有关详细信息，请参阅 应用程序设置设备策略。

  XenMobile Server 具有一个新属性 `ios.mdm.ios27.ddm.support`，它支持应用程序设置设备策略。默认值为 **True**。有关详细信息，请参阅 服务器属性。

- **支持在 iOS 和 macOS 部署规则中使用序列号：**

  XenMobile Server 现在支持适用于 iOS 和 macOS 的新部署规则：**序列号**。您可以在**部署规则 > 高级**中添加此规则。

- **支持 Android 17：**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持运行 Android 17 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。

- **支持 iOS 27：**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在兼容 iOS 27。

- **Secure Hub APNs 证书续订：**

  XenMobile Server 10.16 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 November 9, 2026 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 September 18, 2027。

已修复的问题

- 通过 /api/v1/application/store/{id}/platform/iphone REST API 更新 iOS 应用程序失败，并显示错误 1493。
- 从试用许可证迁移到许可证激活服务 (LAS) 许可证后，许可证类型未正确设置，并且注册配置文件中缺少 iOS 选项。

有关 XenMobile Server 10.16.0 以前的滚动修补程序的信息，请参阅 滚动修补程序的发行说明。

安装 XenMobile Server 更新

> **重要提示：**
>
> 在安装此更新之前，请确保您已升级到 XenMobile Server 版本 10.16.0.48。此外，请对当前设置进行快照并创建数据库备份。
>
> 对于以群集模式配置的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，并将 XenMobile Server 更新 (.bin) 文件下载到适当的位置。
2. 在节点的 XenMobile Server 控制台中，单击 **设置 > 版本管理**。

   版本管理页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级列表。

3. 在版本管理下，单击 **更新**。此时将显示“更新”对话框。
4. 单击 **浏览** 以上传从 Citrix 下载页面 下载的更新 (.bin) 文件。
5. 单击 **更新**，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证修补程序部署

安装此修补程序后，以管理员身份登录到 XenMobile Server 控制台，然后导航到 **设置 > 版本管理 > 更新**。此页面显示有关最新安装的修补程序的详细信息。

适用于 XenMobile Server 10.16 滚动修补程序 9 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动修补程序 9 的增强功能、已修复问题和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.16 滚动修补程序 9 软件二进制文件。

新增功能

- **支持在启动器配置设备策略中启用系统信息：**

  已为 Android Enterprise 设备在启动器配置设备策略中添加了一个新设置：**启用系统信息**。此设置允许 Citrix Launcher 在状态栏中显示系统信息。默认值为**关**，需要 Secure Hub 26.8 或更高版本。有关详细信息，请参阅 启动器配置策略。

- **支持在启动器配置设备策略中自动启动应用程序：**

  已为 Android Enterprise 设备在启动器配置设备策略中添加了一个新设置：**自动启动应用程序**。此设置允许管理员选择一个**允许的应用程序**，以便在 Citrix Launcher 启动时自动启动。默认值为**无（不自动启动）**，需要 Citrix Launcher 26.8 或更高版本。有关详细信息，请参阅 启动器配置策略。

  XenMobile Server 具有一个新属性 `afw.launcher.auto_launch`，它使管理员能够为配置了启动器配置策略的 Android Enterprise 设备配置自动启动应用程序。默认值为 **False**。有关详细信息，请参阅 服务器属性。

- **支持设备应用程序的搜索应用程序选项：**

  在 XenMobile Server 控制台中，**设备 > 设备详细信息 > 应用程序**页面现在包含一个新的**搜索应用程序**选项。

- **支持应用程序设置设备策略：**

  在**配置（声明性）**下添加了一个新的设备策略：**应用程序设置**。此策略允许您使用 Apple 的声明性设备管理来配置应用程序允许和拒绝列表。此策略仅支持受监督的 iOS 27 及更高版本设备。有关详细信息，请参阅 应用程序设置设备策略。

XenMobile Server 具有一个新属性 `ios.mdm.ios27.ddm.support`，它支持应用程序设置设备策略。默认值为 **True**。有关详细信息，请参阅 服务器属性。

- **支持在 iOS 和 macOS 部署规则中使用序列号：**

  XenMobile Server 现在支持适用于 iOS 和 macOS 的新部署规则：**序列号**。您可以在**部署规则 > 高级**中添加此规则。

- **支持 Android 17：**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持运行 Android 17 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。

- **支持 iOS 27：**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在兼容 iOS 27。

- **Secure Hub APNs 证书续订：**

  XenMobile Server 10.16 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 November 9, 2026 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 September 18, 2027。

已修复的问题

- 通过 /api/v1/application/store/{id}/platform/iphone REST API 更新 iOS 应用程序失败，并显示错误 1493。
- 从试用许可证迁移到许可证激活服务 (LAS) 许可证后，许可证类型未正确设置，并且注册配置文件中缺少 iOS 选项。

有关 XenMobile Server 10.16.0 以前的滚动修补程序的信息，请参阅 滚动修补程序的发行说明。

安装 XenMobile Server 更新

> **重要提示：**
>
> 在安装此更新之前，请确保您已升级到 XenMobile Server 版本 10.16.0.48。此外，请对当前设置进行快照并创建数据库备份。
>
> 对于以群集模式配置的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，并将 XenMobile Server 更新 (.bin) 文件下载到适当的位置。

2. 在节点的 XenMobile Server 控制台中，单击 **设置 > 版本管理**。

   版本管理页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级列表。

3. 在版本管理下，单击 **更新**。此时将显示“更新”对话框。
4. 单击 **浏览** 以上传从 Citrix 下载页面 下载的更新 (.bin) 文件。
5. 单击 **更新**，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证修补程序部署

安装此修补程序后，以管理员身份登录到 XenMobile Server 控制台，然后导航到 **设置 > 版本管理 > 更新**。此页面显示有关最新安装的修补程序的详细信息。

XenMobile Server 10.16 滚动修补程序 8 版本的发行说明

这些发行说明描述了 XenMobile Server 10.16 滚动修补程序 8 的增强功能、已修复问题和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.16 滚动修补程序 8 软件二进制文件。

新增功能

- **支持声明式设备管理 (DDM)：**

  XenMobile Server 在 iOS 15 及更高版本中增加了对 Apple 声明式设备管理 (DDM) 的支持。此功能通过使用声明式数据模型，减少对序列化命令和设备轮询的依赖，从而提高性能和可扩展性。有关详细信息，请参阅 利用声明式管理数据模型扩展设备。

  XenMobile Server 具有以下两个新属性：

  `ios.mdm.declarative.management`：启用 iOS 声明式设备管理 (DDM)。

  `ios.mdm.software.update.settings`：启用软件更新强制执行设备策略。

  这两个属性的默认值为 **False**。有关详细信息，请参阅 服务器属性。

  启用 DDM 功能后，支持以下 声明式设备策略：

  - Google 帐户
  - 密码
  - 软件更新强制执行
  - 软件更新设置
  - 状态订阅
  - 用户身份

- **支持检索 iOS 设备的运营商网络相关设备信息：**

  XenMobile Server 现在支持检索 iOS 设备上每个 SIM 卡的额外运营商网络相关设备信息。您可以在 **设备详细信息 > 属性 > 插槽 x SIM 信息** 下查看这些详细信息。新支持的字段包括：

  - 插槽 x — 运营商设置版本
  - 插槽 x — 当前运营商网络
  - 插槽 x — 当前移动国家代码（以前列在“网络信息”下）
  - 插槽 x — 当前移动网络代码（以前列在“网络信息”下）
  - 插槽 x — 是否首选数据
  - 插槽 x — 是否漫游
  - 插槽 x — 是否首选语音
  - 插槽 x — 标签 ID

- **支持 Microsoft Exchange Online 的 OAuth 身份验证：**

  Microsoft 宣布 Exchange Online 将于 2026 年 3 月永久移除对带客户端提交 (SMTP AUTH) 的基本身份验证的支持，并于 April 30, 2026 达到 100% 拒绝。 有关详细信息，请参阅 Exchange Online 将淘汰客户端提交 (SMTP AUTH) 的基本身份验证。

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

- **支持阻止 iOS 设备进行近距离设置：**

  XenMobile Server 为完全设备擦除添加了一个新选项：**下次重新启动时，不允许进行近距离设置，并且将跳过设置助理中的窗格**。此选项可防止 iOS 设备在设备设置期间进行近距离设置。此功能适用于 iOS 11.3 及更高版本。有关详细信息，请参阅安全操作。

- **增强应用程序清单以支持 iOS 26.x 应用程序大小检索：**

  XenMobile Server 支持检索运行 iOS 26.x 的设备的应用程序大小信息。您可以在**设备详细信息 > 应用程序**下找到此信息。

已修复的问题

- 升级到 10.16 滚动修补程序 5 后，XenMobile Server 控制台中管理设备、应用程序和交付组等操作明显变慢，有时会失败。

有关 XenMobile Server 10.16.0 以前的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

安装 XenMobile Server 更新

> **重要提示：**
>
> 在安装此更新之前，请确保您已升级到 XenMobile Server 版本 10.16.0.48。此外，请拍摄当前设置的快照并创建数据库备份。
>
> 对于配置为群集模式的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，并将 XenMobile Server 更新 (.bin) 文件下载到适当的位置。
2. 在节点的 XenMobile Server 控制台中，单击**设置 > 版本管理**。

   版本管理页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级的列表。
3. 在“版本管理”下，单击**更新**。此时将显示“更新”对话框。
4. 单击**浏览**以上传您从Citrix 下载页面下载的更新 (.bin) 文件。
5. 单击 **更新**，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证修补程序部署

安装此修补程序后，以管理员身份登录到 XenMobile Server 控制台，然后导航到 **设置 > 版本管理 > 更新**。此页面显示有关最新安装的修补程序的详细信息。

XenMobile Server 10.16 滚动修补程序 7 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动修补程序 7 的增强功能以及已修复和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.16 滚动修补程序 7 软件二进制文件。

新增功能

- **增强了对 Android Enterprise 设备双 SIM 卡和 eSIM 的支持：**

  XenMobile Server 现在为 Android Enterprise 设备提供全面的双 SIM 卡支持，以确保与 iOS 的功能对等。此增强功能使管理员能够在设备属性中查看所有已安装的 SIM 卡和 eSIM，包括具有两张物理 SIM 卡、一张 SIM 卡加一张 eSIM 或两张 eSIM 的配置。此更新解决了双 SIM 卡 Android Enterprise 设备日益普及的问题，并为客户提供了对其移动设备连接选项的完整可见性，与之前为 iOS 设备提供的 eSIM 功能相匹配。此功能仅支持以下版本：

  - Secure Hub 25.7.0 或更高版本，以及

- Android 13 或更高版本

XenMobile Server 有一个新属性 `ae.esim.support`，它使 XenMobile Server 能够从 Android Enterprise 设备获取 eSIM 信息，并在用户界面上显示 eSIM 相关的设备属性。此属性的默认值为 **True**。有关详细信息，请参阅 服务器属性。

- **许可证激活服务：**

  XenMobile Server 现在支持许可证激活服务 (LAS) 许可机制。LAS 是一种新的基于云的许可解决方案，为 Citrix 产品套件中的传统基于文件的许可提供了一种现代替代方案。将您的 Citrix 许可证服务器注册到 Citrix Cloud，以使用您的许可证激活服务所持有的许可证和权利。有关详细信息，请参阅 许可证激活服务。

> **重要提示：**
>
> 我们正在为 Citrix 平台过渡到行业标准的基于云的许可架构。此举可自动执行权利和激活，带来以下主要客户优势：
>
> - **无需管理许可证文件：** 消除了下载、分配或管理许可证文件的需要，从而简化了您的管理任务。
> - **自动更新权利：** 合同续订后，权利会在后台自动更新，确保服务不中断。
> - **增强了弹性：** 许可证服务器不再是用户会话的单点故障，从而增强了环境的稳定性。
>
> 我们鼓励您利用过渡期，在 April 15, 2026 之前规划并执行向新许可模式的过渡，我们致力于全程为您提供支持。有关更多信息，请参阅 Citrix 现代许可公告。

- **Secure Hub APNs 证书续订：**

  适用于 XenMobile Server 10.16 的 Secure Hub Apple Push Notification service (APNs) 证书将于 January 4, 2026 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 November 9, 2026。

- **支持 iOS 18.x 版本的新 iOS 限制：**

  在 iOS 的限制策略中，已添加以下新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 iOS 18 及更高版本。默认设置为**开**。有关更多信息，请参阅 限制策略。

  - 允许外部智能集成

- 允许登录外部智能集成
- 允许邮件智能回复
- 允许备忘录转录
- 允许 Safari 摘要
- 允许视觉智能摘要
- 允许备忘录转录摘要
- 允许 Apple Intelligence 报告
- 允许修改默认通话应用
- 允许修改默认消息应用
- 允许外部智能工作区 ID
- 默认浏览器修改
- 允许 FaceTime 远程控制

已修复的问题

- 由于 XenMobile 服务器上的 CPU 和内存利用率过高，设备注册失败。

有关 XenMobile Server 10.16.0 以前的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

安装 XenMobile Server 更新

> **重要提示：**
>
> 在安装此更新之前，请确保您已升级到 XenMobile Server 10.16.0.48 版本。同时，请对当前设置进行快照并创建数据库备份。
>
> 对于以群集模式配置的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，并将 XenMobile Server 更新 (.bin) 文件下载到适当的位置。
2. 在节点的 XenMobile Server 控制台中，单击“**设置 > 版本管理**”。

   版本管理页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级列表。
3. 在“版本管理”下，单击“**更新**”。此时将显示“更新”对话框。
4. 单击“**浏览**”以上传您从Citrix 下载页面下载的更新 (.bin) 文件。
5. 点击 **更新**，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证补丁部署

安装此补丁后，以管理员身份登录 XenMobile Server 控制台，然后导航到 **设置 > 版本管理 > 更新**。此页面显示有关最新安装补丁的详细信息。

XenMobile Server 10.16 滚动修补程序 6 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动修补程序 6 的增强功能、已修复问题和已知问题。您可以从 登录下载 下载 XenMobile Server 10.16 滚动修补程序 6 软件二进制文件。

新增功能

- **支持 Android 16**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持运行 Android 16 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。

- **支持 iOS 26**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在与 iOS 26 兼容。

- **支持旧版 MDX 策略升级通知**

  当使用旧版策略的现有 Secure Mail 和 Secure Web MDX 应用程序更新到版本 25.9.0 时，XenMobile Server 现在会显示升级警报。

- **支持基于证书身份验证的新强证书映射**

  引入了一种新的映射方法，以在颁发符合强映射要求的证书时提供更大的灵活性。XenMobile Server 现在将 `URL=tag:microsoft.com`、`2022-09-14:sid:<user's SID>` 附加到证书的主题备用名称 (SAN)。

  - 要为现有用户启用此功能，客户管理员必须添加客户端属性 `MICROSOFT_CERTIFICATE_STRONG_MAPPING`。有关详细信息，请参阅 客户端属性。
  - 强证书映射仅在 **Windows Server 2019 及更高版本**上受支持。有关详细信息，请参阅 Microsoft 强映射。

- **支持 iOS 17.x 版本的新 iOS 限制**

  在 iOS 的限制策略中，已为 iOS 17.2 及更高版本添加了以下新设置。默认值为 **On**。有关详细信息，请参阅 限制策略。

  - 允许实时语音邮件

- **管理配置策略文本框**

当客户将 **Knox Service Plugin** 与 **Managed Configuration policy** 结合使用时，**Separated Apps Policies** 上所有文本框的最大字符长度增加到 8,192 个字符。

- **在 Apple Deployment Programs 页面中支持新的 iOS 设置助理选项**

  Apple 为 Apple Business Management 注册添加了一些新的 iOS 设置助理选项屏幕。以下新选项已添加到 **Settings > Apple Deployment Programs > iOS Setup Assistant Options** 页面中。您可以配置 XenMobile Server 以跳过这些屏幕。有关详细信息，请参阅 iOS 设置助理选项。

  - 操作按钮
  - 锁定模式
  - 智能
  - 相机按钮

- **与 Apple Business Manager 同步以管理设备分配**

  XenMobile® Server (XMS) 现在通过与 Apple Business Manager (ABM) 同步来确保准确的设备分配。此更新验证只有正确分配的设备才会出现在 XMS 中，从而防止出现已从 XMS 中删除并分配给其他供应商管理解决方案的设备记录。例如，如果设备被移动到其他解决方案，则在同步后它们将不再出现在 XMS 中。

  XMS 现在包含一个新属性 `remove.unassigned.abm.devices`，该属性使 XMS 能够删除不再分配给此服务器的设备。默认情况下，此属性设置为 **False**。有关详细信息，请参阅 服务器属性。

已修复的问题

- 即使未上传任何 Legacy MDX 应用程序，Legacy MDX 警报仍会继续显示在 XMS 控制台上。
- 当使用鼠标右键单击并粘贴密码时，XenMobile 门户上的“登录”按钮会变灰。
- 启用“**显示新视图**”功能后，即使已将筛选器应用于设备列表，设备计数也会显示不正确。
- iOS 用户无法启动 Secure Mail/Secure Web 应用程序，并且在从 Secure Mail/Secure Web 重定向到 Secure Hub 时遇到“无法打开”错误。
- 设备注册计划 (DEP) 设备即使在注册配置文件配置为 **MDM-only** 的情况下，也会继续执行 **MDM+MAM** 注册。
- 当 iOS 设备对未安装的应用程序具有应用程序锁定策略时，设备会锁定并显示错误“引导式访问应用程序不可用。请联系您的管理员”，并且触摸屏无响应，即使强制重启后也是如此。
- 使用 XenMobile MDM 解决方案注册 Windows 客户端时，交付组部署失败。因此，需要手动同步操作才能应用推送的策略。作为一种变通方法，需要手动部署到单个设备。

有关 XenMobile Server 10.16.0 以前的滚动修补程序的信息，请参阅 滚动修补程序的发行说明。

安装 XenMobile Server 更新

> **重要提示：**
>
> 在安装此更新之前，请确保已升级到 XenMobile Server 10.16.0.48 版。此外，请对当前设置进行快照并创建数据库备份。
>
> 对于以群集模式配置的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，并将 XenMobile Server 更新 (.bin) 文件下载到适当的位置。
2. 在节点的 XenMobile Server 控制台中，单击“**设置 > 版本管理**”。

   “版本管理”页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级的列表。
3. 在“版本管理”下，单击“**更新**”。“更新”对话框随即显示。
4. 单击“**浏览**”以上传您从 Citrix 下载页面 下载的更新 (.bin) 文件。
5. 点击 **更新**，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证补丁部署

安装此补丁后，以管理员身份登录到 XenMobile Server 控制台，然后导航到 **设置 > 版本管理 > 更新**。此页面显示有关最新安装补丁的详细信息。

XenMobile Server 10.16 滚动补丁 5 版本发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动补丁 5 的增强功能、已修复问题和已知问题。您可以在 登录以下载 处下载 XenMobile Server 10.16 滚动补丁 5 软件二进制文件。

新增功能

- **支持托管配置反馈（技术预览版）**

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

  XenMobile Server 现在包含一个新属性 `afw.app_managed_configurations.feedback`，该属性启用了一项功能，允许管理员从配置了托管配置策略的 Android 设备获取应用程序状态反馈。默认情况下，此属性设置为 **False**。有关详细信息，请参阅 服务器属性。
- **支持设备页面上的持久性筛选器**

在新设备页面中，所有**可筛选**选项现在都支持筛选器。这些筛选器会为登录用户跨会话保存，从而消除了管理员每次访问设备页面时重新应用相同筛选器的需要。如果取消选择相应的列，筛选器将自动删除。

- **支持保留 iPhone 和 iPad 的数据套餐**

  执行完全设备擦除时，可以使用新选项“擦除时保留蜂窝数据套餐”。此选项允许您在擦除过程中保留设备上的蜂窝数据套餐（例如 eSIM）。此功能适用于 iOS 11 及更高版本。有关详细信息，请参阅 安全操作。

- **支持 iOS 的新 iOS 18 设置**

  在 iOS 的限制策略中，已添加以下新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 iOS 18 及更高版本。默认设置为 **On**。有关详细信息，请参阅 限制策略。

  - 通话录音
  - 要隐藏的应用程序
  - 要锁定的应用程序
  - 邮件摘要
  - RCS 消息
  - 默认浏览器修改

- **支持 macOS 的新 macOS 15 设置**

  在 macOS 的限制策略中，已添加以下新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 macOS 15 及更高版本。有关详细信息，请参阅限制策略。

  - 允许媒体共享修改
  - 强制绕过屏幕捕获警报
  - 邮件摘要

已修复的问题

- 如果基于角色的访问控制 (RBAC) 管理员没有“服务器属性”权限，则在“设备”页面上切换“显示新视图（技术预览）”时，他们会意外注销。
- 当应用程序升级到新版本时，批量购买计划 (VPP) 应用程序图标不会更新。
- 当 MDM 证书续订失败时，旧证书会被 XenMobile® Server 标记为已吊销，从而阻止 Secure Hub (SH) 重新连接到服务器。结果，即使旧证书尚未过期，SH 也无法使用它与服务器通信。
- 启用**显示新视图技术预览**功能后，基于角色的访问控制 (RBAC) 管理员会意外看到搜索输入框。

- 为 AE 设备生成了大量负载证书。
- 在重新注册期间，当**部署计划**中的**部署条件**设置为“仅当上次部署失败时”，某些策略未部署到 AE 设备。

有关 XenMobile Server 10.16.0 以前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 10.16 滚动修补程序 4 版本发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动修补程序 4 的增强功能、已修复问题和已知问题。您可以在 登录以下载 处下载 XenMobile Server 10.16 滚动修补程序 4 软件二进制文件。

新增功能

- **Secure Hub APNs 证书续订**

  XenMobile Server 10.16 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 February 9, 2025 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 January 4, 2026。

- **支持 macOS 15**

  XenMobile® Server 和 Citrix Mobile 生产力应用程序现在与 macOS 15 兼容，但目前不支持所有新的 macOS 15 功能。

- **支持 iOS 18**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在与 iOS 18 兼容，但目前不支持所有新的 iOS 18 功能。

- **支持 Android 15**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持 Android Enterprise 设备更新到 Android 15。有关安全和隐私优势的更多信息，请参阅 Android 开发者文档。

- **更新公共 Rest API 文档以包含设备丢失模式 API**

  在 公共 Rest API 文档 中添加了丢失模式 API。

- **修改 API 调用以使用请求正文而不是 URL**

  更新了 API 调用，以便在 公共 Rest API 文档 中将数据包含在请求正文中，而不是 URL 中。

- **支持阻止或限制 iOS 版 Apple Intelligence**

  在 iOS 限制策略中，添加了以下新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 iOS 18 及更高版本。默认设置为 **开**。有关详细信息，请参阅限制策略。

  - 生成式表情符号
  - 图像游乐场
  - 图像魔杖
  - iPhone 镜像
  - 个性化手写结果
  - 书写工具

- **支持阻止或限制 macOS 版 Apple Intelligence**

  在 macOS 限制策略中，添加了以下新设置以阻止访问 Apple Intelligence (AI) 或限制某些新功能。这些设置适用于 macOS 15 及更高版本。默认设置为 **开**。有关详细信息，请参阅限制策略。

  - 图像游乐场
  - iPhone 镜像
  - 书写工具

- **支持立即为 iOS 设备安装操作系统更新**

  在控制操作系统更新设备策略中，iOS 的操作系统更新选项中添加了一个名为 **立即安装** 的新单选按钮。此功能允许您立即为 iOS 设备安装以前下载的操作系统更新。有关详细信息，请参阅适用于 iOS 的控制操作系统更新设备策略。

- **支持在系统擦除设备时保留 eSIM**

  限制策略中新增了一个设置：**擦除时保留 eSIM**。此设置可确保在系统因多次密码尝试失败而擦除设备，或在**设置** > **通用** > **传输或还原 iPhone** 中选择**抹掉所有内容和设置**选项时，保留 eSIM。此功能适用于 iOS 17.2 及更高版本，默认设置为**关闭**。有关详细信息，请参阅限制策略。

- **支持阻止网络分发的第三方应用程序**

  在限制策略中，新增了一个设置**网络分发**应用程序，用于阻止 iOS 设备上网络分发的第三方应用程序。此设置适用于 iOS 17.5 及更高版本。有关详细信息，请参阅限制策略。

- **支持管理复制和粘贴功能**

  在限制策略中，新增了一个设置**要求受管粘贴板**，以允许复制和粘贴功能遵循您应用于**非受管应用程序中的受管应用程序文档**和**受管应用程序中的非受管应用程序文档**的相同限制。默认设置为**关闭**。有关详细信息，请参阅限制策略。

- **支持 Samsung 增强型认证 v3**

Samsung 增强型认证 v3 提高了 Samsung Knox 设备上的 XMS 安全功能。有关详细信息，请参阅Samsung Knox 增强型认证。 XenMobile Server 现在包含一个新属性 `afw.knox.attestation.v3`，该属性可启用可提高 Samsung Knox 设备上 XMS 安全性的功能。默认情况下，此属性设置为**True**。有关详细信息，请参阅服务器属性。

已修复的问题

- XenMobile Server 无法成功注册新的 Android Enterprise 设备，因为 SQL Server 触发警报消息时会出现性能问题。
- 尽管客户已将 FIPS 设置启用为 **true**，但日志仍显示其已禁用。此外，当客户尝试通过 CLI 修改数据库设置时，XenMobile Server 无法建立与数据库的连接，从而阻止应用更新。

有关 XenMobile Server 10.16.0 以前的滚动修补程序的信息，请参阅滚动修补程序发行说明。

XenMobile Server 10.16 滚动修补程序 3 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动修补程序 3 的增强功能、已修复问题和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.16 滚动修补程序 3 软件二进制文件。

新增功能

- **支持 iPhone 和 iPad 的返回服务功能**

  借助返回服务功能，MDM 服务器可以发送擦除命令，该命令包含 Wi-Fi 详细信息和默认 MDM 注册配置文件，并发送到用户设备。然后，设备会自动擦除所有用户数据，连接到指定的 Wi-Fi 网络，并使用提供的注册配置文件重新注册到 MDM 服务器。有关详细信息，请参阅 安全操作。

  XenMobile Server 现在包含一个新属性 `ios.mdm.return.to.service`，该属性可为运行 iOS 17 或更高版本的 iPhone 和 iPad 启用返回服务功能。默认情况下，此属性设置为 **True**。有关详细信息，请参阅 服务器属性。

- **强制执行最低操作系统版本以完成自动注册设置**

  借助 iOS 17，MDM 现在可以强制执行最低操作系统版本，以通过自动设备注册来注册设备。有关详细信息，请参阅 通过 Apple 部署计划部署设备。

  XenMobile Server 现在包含一个新属性 `ios.mdm.minimum_os_version.enrollment`，该属性允许您强制执行最低操作系统版本要求，以在 iOS 17 或更高版本上完成自动注册设置。默认情况下，此属性设置为 **True**。有关详细信息，请参阅 服务器属性。

- **支持从个人资料访问和使用工作资料电子邮件应用程序**

在限制设备策略中，Android Enterprise 设置中添加了一个新设置：**从工作和个人资料访问电子邮件应用程序**。此设置允许您从个人资料访问和使用工作资料电子邮件应用程序。有关详细信息，请参阅 限制设备策略 - Android Enterprise 设置。

XenMobile Server 现在包含一个新属性 `afw.mailapp.crossworkprofile`，该属性可启用在 Android Enterprise 设置中从个人资料访问和使用工作资料电子邮件应用程序的功能。默认情况下，此属性设置为 **True**。有关详细信息，请参阅 服务器属性。

- **支持适用于 iOS 11.x、12.x 和 13.x 版本的新 iOS 限制**

  在适用于 iOS 的限制策略中添加了新设置：

  - 允许共享 iPad 临时会话
  - 允许修改 eSIM
  - 允许网络驱动器连接
  - 允许 USB 设备连接
  - 允许“查找我的设备”
  - 允许“查找我的朋友”
  - 允许 QuickPath 键盘
  - 强制开启 Wi-Fi
  - 强制在自动填充前进行身份验证
  - 修改个人热点设置

  有关详细信息，请参阅限制设备策略 - iOS 设置。

- **Android Enterprise 托管配置策略的增强功能**

  “**托管配置**”策略下“**应用程序管理策略**”页面上所有文本框的最大字符长度已增加到 4096 个字符。

已修复的问题

- 对于启用了 MAM SDK 的新版本应用程序，Secure Hub 商店中不提供“更新”选项。

有关 XenMobile Server 10.16.0 以前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 10.16 滚动补丁 2 版本发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动补丁 2 的增强功能、已修复问题和已知问题。您可以在 登录下载 处下载 XenMobile Server 10.16 滚动补丁 2 软件二进制文件。

已修复问题

- 升级到 XenMobile Server 10.16 版本后，XenMobile Server 已停止向 Syslog 服务器发送日志。
- 配置代理后，使用 HTTP v1 API 的 Firebase Cloud Messaging 无法正常运行。

有关 XenMobile Server 10.16.0 以前的滚动补丁的信息，请参阅 滚动补丁的发行说明。

适用于 XenMobile Server 10.16 滚动修补程序 1 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.16 滚动修补程序 1 的增强功能、已修复问题和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.16 滚动修补程序 1 软件二进制文件。

新增功能

- **支持阻止适用于 iOS 17.4 及更高版本的第三方应用程序：** 在限制策略中，新增了一个设置“**备用应用商店**”，以阻止从 Web 安装备用应用商店应用程序，并阻止任何已安装的备用应用商店应用程序安装其他应用程序。有关详细信息，请参阅 限制设备策略。
- **如果发布了具有旧版 MDX 模式的 MDX 应用程序，则在 XMS 控制台上显示警报：** 如果发布了具有旧版 MDX 模式的 MDX 应用程序，则 XenMobile Server 控制台上会显示警报。有关详细信息，请参阅 服务器属性 中的“**旧版 MDX 弃用警报**”。
- **Firebase Cloud Messaging 支持已迁移到使用新的 http v1 API：** Google 将于 June 21, 2024 弃用适用于 HTTP 的 FCM 旧版 API。为了使 FCM 能够很好地与新 API 配合使用，Firebase Cloud Messaging 页面中新增了一个字段“**服务帐户密钥文件**”，供您上传服务帐户密钥 JSON 文件。有关详细信息，请参阅 Firebase Cloud Messaging。

  XenMobile Server 具有一个新属性 `afw.fcm.httpv1.migration`，它允许您将 Firebase Cloud Messaging 与新的 HTTP v1 API 配合使用。此属性的默认值为 **False**。有关详细信息，请参阅 服务器属性。

  要为 XenMobile Server 10.16 滚动修补程序 1 及更高版本启用 FCM API V1，请参阅知识中心文章 CTX677031。

已修复问题

- 升级到 XenMobile Server 10.16 版本后，可选的 Web 链接会持续重新安装。
- 将 XenMobile Server 升级到 10.16 版本后，当您在“**客户端支持**”设置中选择“**直接**”将“**设备日志发送到 IT 帮助台**”时，Secure Hub 日志无法发送到 IT 帮助台。
- 在 XenMobile® Server 控制台 > “**限制**” > “**Android Enterprise**”中，策略设置“**配置移动网络**”的工具提示说明在德语中不正确。

有关 XenMobile Server 10.16.0 以前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 10.15 滚动修补程序 14 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 14 的增强功能、已修复问题和已知问题。您可以在 登录以下载 下载 XenMobile Server 10.15 滚动修补程序 14 软件二进制文件。

新增功能

- **支持 Android 17：**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持运行 Android 17 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。

- **支持 Microsoft Exchange Online 的 OAuth 身份验证：**

  Microsoft 宣布 Exchange Online 将于 2026 年 3 月永久取消对客户端提交（SMTP AUTH）基本身份验证的支持，并于 April 30, 2026 达到 100% 拒绝。 有关详细信息，请参阅 Exchange Online 将淘汰客户端提交（SMTP AUTH）的基本身份验证。

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

- **增强应用程序清单以支持 iOS 26.x 应用程序大小检索：**

  XenMobile Server 支持检索运行 iOS 26.x 的设备的应用程序大小信息。您可以在 **设备详细信息 > 应用程序** 下找到该信息。

有关 XenMobile Server 10.15.0 以前的滚动修补程序的信息，请参阅 滚动修补程序发行说明。

安装 XenMobile Server 更新

重要提示：

- 在安装此更新之前，请确保您已升级到 XenMobile Server 10.15.0.23 版本。同时，请对当前设置进行快照，并创建数据库备份。
- 如果您从 10.15 RP2 或任何更早的版本（包括 10.15 RTM）升级，请按照 升级群集 XenMobile 部署 中的步骤升级所有群集节点。

对于配置为群集模式的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，然后将 XenMobile Server 更新 (.bin) 文件下载到相应位置。
2. 在节点的 XenMobile Server 控制台中，单击“**设置 > 版本管理**”。

   “版本管理”页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级的列表。
3. 在“版本管理”下，单击“**更新**”。此时将显示“更新”对话框。
4. 单击“**浏览**”以上传从 Citrix 下载页面 下载的更新 (.bin) 文件。
5. 单击“**更新**”，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证修补程序部署

安装此修补程序后，以管理员身份登录 XenMobile Server 控制台，然后导航到“**设置 > 版本管理 > 更新**”。此页面显示有关最新安装的修补程序的详细信息。

XenMobile Server 10.15 滚动修补程序 14 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 14 的增强功能、已修复问题和已知问题。您可以在 登录以下载 下载 XenMobile Server 10.15 滚动修补程序 14 软件二进制文件。

新增功能

- **支持 Android 17：**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持运行 Android 17 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。
- **支持 Microsoft Exchange Online 的 OAuth 身份验证：**

  Microsoft 宣布 Exchange Online 将于 2026 年 3 月永久取消对客户端提交（SMTP AUTH）基本身份验证的支持，并于 April 30, 2026 达到 100% 拒绝。 有关详细信息，请参阅 Exchange Online 将淘汰客户端提交（SMTP AUTH）的基本身份验证。

  XenMobile Server 支持 SMTP 服务器的 OAuth 身份验证。通过选择 **Microsoft Exchange Online OAuth 2.0** 并提供所需的 **租户 ID**、**客户端 ID** 和 **客户端密钥** 来启用此功能。如果您使用 Microsoft Exchange Online，Citrix 建议切换到 OAuth 身份验证。有关配置详细信息，请参阅 通知。
- **增强应用程序清单以支持 iOS 26.x 应用程序大小检索：**

  XenMobile Server 支持检索运行 iOS 26.x 的设备的应用程序大小信息。您可以在 **设备详细信息 > 应用程序** 下找到该信息。

有关 XenMobile Server 10.15.0 以前的滚动修补程序的信息，请参阅 滚动修补程序发行说明。

安装 XenMobile Server 更新

重要提示：

- 在安装此更新之前，请确保您已升级到 XenMobile Server 10.15.0.23 版本。同时，请对当前设置进行快照，并创建数据库备份。
- 如果您从 10.15 RP2 或任何更早的版本（包括 10.15 RTM）升级，请按照 升级群集 XenMobile 部署 中的步骤升级所有群集节点。

对于配置为群集模式的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，然后将 XenMobile Server 更新 (.bin) 文件下载到相应位置。
2. 在节点的 XenMobile Server 控制台中，单击“**设置 > 版本管理**”。

   “版本管理”页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级的列表。
3. 在“版本管理”下，单击“**更新**”。此时将显示“更新”对话框。
4. 单击“**浏览**”以上传从 Citrix 下载页面 下载的更新 (.bin) 文件。
5. 单击“**更新**”，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证修补程序部署

安装此修补程序后，以管理员身份登录 XenMobile Server 控制台，然后导航到“**设置 > 版本管理 > 更新**”。此页面显示有关最新安装的修补程序的详细信息。

适用于 XenMobile Server 10.15 滚动修补程序 13 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 13 的增强功能、已修复问题和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.15 滚动修补程序 13 软件二进制文件。

新增功能

- **许可证激活服务：**

  XenMobile Server 现在支持许可证激活服务 (LAS) 许可机制。LAS 是一种新的基于云的许可解决方案，为 Citrix 产品套件中的传统基于文件的许可提供了一种现代替代方案。将您的 Citrix 许可证服务器注册到 Citrix Cloud，以使用许可证激活服务所持有的许可证和权利。有关详细信息，请参阅 许可证激活服务。

重要：

我们正在将 Citrix 平台过渡到行业标准的基于云的许可架构。此举可自动执行权利和激活，带来以下主要客户优势：

- **无需管理许可证文件：** 无需下载、分配或管理许可证文件，从而简化了您的管理任务。
- **自动更新权利：** 续订合同时，权利会在后台自动更新，从而确保服务不中断。
- **增强的弹性：** 许可证服务器不再是用户会话的单点故障，从而增强了环境的稳定性。

我们鼓励您利用过渡期，计划并执行在 April 15, 2026 之前采用新许可模型的转换，我们将致力于全程为您提供支持。有关详细信息，请参阅 Citrix 现代许可公告。

如果 10.15 滚动修补程序 13 或更高版本的滚动修补程序中启用了许可证激活服务，则直接升级到 10.16.0.48 会重置许可证激活服务配置。请继续应用版本 10.16 滚动修补程序 7 或更高版本的 10.16 滚动修补程序，以便重新配置许可证激活服务。现有设备不受影响。

已修复的问题

- 因为 XenMobile 服务器上的 CPU 和内存利用率过高，设备注册失败。

有关 XenMobile Server 10.15.0 以前的滚动修补程序的信息，请参阅 滚动修补程序的发行说明。

安装 XenMobile Server 更新

重要提示：

- 在安装此更新之前，请确保您已升级到 XenMobile Server 10.15.0.23 版。同时，请拍摄当前设置的快照并创建数据库备份。
- 如果您从 10.15 RP2 或任何更早版本（包括 10.15 RTM）升级，请按照 (/zh-cn/xenmobile/server/upgrade.html#to-upgrade-clustered-xenmobile-deployments) 中的步骤升级所有群集节点。

对于配置为群集模式的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，并将 XenMobile Server 更新 (.bin) 文件下载到适当的位置。

2. 在节点的 XenMobile Server 控制台中，单击 **Settings > Release Management**。

   “版本管理”页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级的列表。

3. 在“版本管理”下，单击 **Update**。“更新”对话框随即出现。
4. 单击 **Browse** 上传从 Citrix 下载页面 下载的更新 (.bin) 文件。
5. 单击 **Update**，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证修补程序部署

安装此修补程序后，以管理员身份登录 XenMobile Server 控制台，然后导航到 **Settings > Release Management > Updates**。此页面显示有关最新安装的修补程序的详细信息。

XenMobile Server 10.15 滚动修补程序 12 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 12 的增强功能以及已修复和已知问题。您可以在 登录以下载 处下载 XenMobile Server 10.15 滚动修补程序 12 软件二进制文件。

新增功能

- **支持基于证书的身份验证的新强证书映射**

  引入了一种新的映射方法，以在颁发符合强映射要求的证书时提供更大的灵活性。XenMobile Server 现在将 `URL=tag:microsoft.com`、`2022-09-14:sid:<user's SID>` 附加到证书的使用者备用名称 (SAN)。

  - 要为现有用户启用此功能，客户管理员必须添加客户端属性 `MICROSOFT_CERTIFICATE_STRONG_MAPPING`。有关详细信息，请参阅 客户端属性。
  - 强证书映射仅在 **Windows Server 2019 及更高版本**上受支持。有关详细信息，请参阅 Microsoft 强映射。

- **支持 iOS 26**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在与 iOS 26 兼容。

- **支持 Android 16**

  XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持运行 Android 16 的 Android Enterprise 设备。有关安全和隐私的详细信息，请参阅 Android 开发者文档。

- **管理配置策略文本框**

  当客户将 **Knox Service Plugin** 与**托管配置策略**结合使用时，**分离应用程序策略**上所有文本框的最大字符长度增加到 8,192 个字符。

- **Secure Hub APNs 证书续订**

  XenMobile Server 10.15 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 January 4, 2026 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 November 9, 2026。

已修复的问题

- 当使用鼠标右键单击并粘贴密码时，XenMobile 门户上的“登录”按钮会变灰。
- 当从 Secure Mail/Secure Web 重定向到 Secure Hub 时，iOS 用户无法启动 Secure Mail/Secure Web 应用程序，并遇到“无法打开”错误。
- 即使注册配置文件配置为 **仅限 MDM**，设备注册计划 (DEP) 设备仍继续执行 **MDM+MAM** 注册。
- 使用 XenMobile MDM 解决方案注册 Windows 客户端时，交付组部署失败。因此，需要手动同步操作才能应用推送的策略。作为一种变通方法，需要手动部署到单个设备。
- 当 iOS 设备对未安装的应用程序具有应用程序锁定策略时，设备会锁定并显示错误“引导式访问应用程序不可用。请联系您的管理员”，即使强制重启后，触摸屏也无响应。

有关 XenMobile Server 10.15.0 以前的滚动修补程序的信息，请参阅滚动修补程序的发行说明。

安装 XenMobile Server 更新

重要提示：

- 在安装此更新之前，请确保您已升级到 XenMobile Server 版本 10.15.0.23。同时，对当前设置进行快照并创建数据库备份。
- 如果您从 10.15 RP2 或任何早期版本（包括 10.15 RTM）升级，请按照升级群集 XenMobile 部署中的步骤操作，以升级所有群集节点。

对于配置为群集模式的系统，请按照以下步骤逐个更新每个节点：

1. 登录 Citrix® 网站上的帐户，并将 XenMobile Server 更新 (.bin) 文件下载到适当的位置。
2. 在节点的 XenMobile Server 控制台中，单击**设置 > 版本管理**。

   版本管理页面显示当前安装的软件版本以及您上传的任何更新、修补程序和升级列表。
3. 在“版本管理”下，单击**更新**。此时将显示“更新”对话框。
4. 单击**浏览**以上载从 Citrix 下载页面 下载的更新 (.bin) 文件。
5. 单击**更新**，然后，如果出现提示，使用命令行重新启动 XenMobile Server 节点。

验证修补程序部署

安装此修补程序后，以管理员身份登录 XenMobile Server 控制台，然后导航到**设置 > 版本管理 > 更新**。此页面将显示有关最新安装的修补程序的详细信息。

XenMobile Server 10.15 滚动补丁 11 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动补丁 11 的增强功能、已修复问题和已知问题。您可以在 登录下载 处下载 XenMobile Server 10.15 滚动补丁 11 软件二进制文件。

已修复问题

- 当部署计划中的部署条件设置为“仅当以前的部署失败时”时，某些策略在重新注册期间不会部署到 AE 设备。
- 为 AE 设备生成了大量负载证书。

有关 XenMobile Server 10.15.0 以前的滚动补丁的信息，请参阅 滚动补丁的发行说明。

XenMobile Server 10.15 滚动修补程序 10 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 10 的增强功能、已修复问题和已知问题。您可以在 登录以下载 处下载 XenMobile Server 10.15 滚动修补程序 10 软件二进制文件。

新增功能

Secure Hub APNs 证书续订：XenMobile Server 10.15 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 February 9, 2025 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，有效期至 January 4, 2026。

有关 XenMobile Server 10.15.0 以前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 10.15 滚动修补程序 9 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 9 的增强功能、已修复问题和已知问题。您可以在 登录下载 处下载 XenMobile Server 10.15 滚动修补程序 9 软件二进制文件。

新增功能

- **支持 Android 15**：XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持 Android Enterprise 设备更新到 Android 15。有关安全和隐私优势的更多信息，请参阅 Android 开发者文档。
- **支持 iOS 18**：XenMobile® Server 和 Citrix Mobile 生产力应用程序现在与 iOS 18 兼容，但目前不支持所有新的 iOS 18 功能。

- **支持 macOS 15**：XenMobile Server 和 Citrix Mobile 生产力应用程序现在与 macOS 15 兼容，但目前不支持所有新的 macOS 15 功能。
- **更新公共 Rest API 文档以包含设备丢失模式 API**：在 公共 Rest API 文档 中添加了丢失模式 API。
- **修改 API 调用以使用请求正文而不是 URL**：更新了 API 调用，以便在 公共 Rest API 文档 中将数据包含在请求正文中而不是 URL 中。
- **管理配置策略文本框**：在“托管配置”策略下的“**应用程序管理策略**”页面上，所有文本框的最大字符长度已增加到 4,096 个字符。

已修复的问题

- 对于启用了 MAM SDK 的新版本应用程序，Secure Hub 商店中不提供“**更新**”选项。
- 由于 SQL Server 触发警报消息时出现的性能问题，XenMobile Server 无法成功注册新的 Android Enterprise 设备。
- 尽管客户已将 FIPS 设置启用为 **true**，但日志仍显示其已禁用。此外，当客户尝试通过 CLI 修改数据库设置时，XenMobile 服务器无法建立与数据库的连接，从而阻止应用更新。

有关 XenMobile Server 10.15.0 以前的滚动修补程序的信息，请参阅 滚动修补程序发行说明。

XenMobile Server 10.15 滚动修补程序 8 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 8 的增强功能、已修复问题和已知问题。您可以在 登录以下载 处下载 XenMobile Server 10.15 滚动修补程序 8 软件二进制文件。

已修复的问题

- 当配置了代理时，使用 HTTP v1 API 的 Firebase Cloud Messaging 无法正常运行。

有关 XenMobile Server 10.15.0 以前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 10.15 滚动补丁 7 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动补丁 7 的增强功能、已修复问题和已知问题。您可以在 登录下载 处下载 XenMobile Server 10.15 滚动补丁 7 软件二进制文件。

新增功能

- **支持阻止 iOS 17.4 及更高版本的第三方应用程序**： 在限制策略中，新增了一个设置 **Alternative App Marketplace**，以防止从 Web 安装替代应用商店应用程序，并防止任何已安装的替代应用商店应用程序安装其他应用程序。有关详细信息，请参阅 限制设备策略。

- **如果发布了具有旧版 MDX 模式的 MDX 应用程序，则在 XMS 控制台上显示警报：** 如果您发布了具有旧版 MDX 模式的 MDX 应用程序，XenMobile Server 控制台上会显示警报。有关详细信息，请参阅 服务器属性 中的 **旧版 MDX 弃用警报**。
- **Firebase Cloud Messaging 支持已迁移以使用新的 http v1 API：** Google 将于 June 21, 2024 弃用用于 HTTP 的 FCM 旧版 API。为了使 FCM 能够很好地与新 API 配合使用，Firebase Cloud Messaging 页面中新增了一个字段 **Service Account Key File**，供您上传服务帐户密钥 JSON 文件。有关详细信息，请参阅 Firebase Cloud Messaging。

  XenMobile Server 有一个新属性 `afw.fcm.httpv1.migration`，它允许您将 Firebase Cloud Messaging 与新的 HTTP v1 API 结合使用。此属性的默认值为 **False**。有关详细信息，请参阅 服务器属性。

  要为 XenMobile Server 10.15 滚动补丁 7 及更高版本启用 FCM API V1，请参阅知识中心文章 CTX677031。

已修复问题

- 对于 Apple Business Manager (ABM) 共享 iPad，如果登录用户在注册前不存在于服务器数据库中，XenMobile® Server 会将其显示为“匿名”。
- 当支持 MacOS 和 iOS 平台的公共 VPP 应用程序同步到 XenMobile 时，仅显示 iOS 平台，而缺少 MacOS 平台。
- XenMobile Server 上的一些 iOS 公共应用程序无法在 Apple Store 中找到。
- 升级到 XenMobile Server 10.15 RP6 后，DEP 设置“等待配置完成设置”不再生效，导致 DEP 设置辅助页面快速出现，而不是等待接收策略。
- 升级后登录 XenMobile Server 控制台时，“管理”选项卡上显示错误消息“**java.util.ConcurrentModificationException**”。
- 升级到 XenMobile Server 10.15 RP6 后，可选的 Web 链接会持续重新安装。
- 在 XenMobile Server 控制台 > **限制** > **Android Enterprise** 中，策略设置 **配置移动网络** 的工具提示描述在德语中不正确。

有关适用于 XenMobile Server 10.15.0 的以前滚动修补程序的信息，请参阅滚动修补程序的发行说明。

适用于 XenMobile Server 10.15 滚动修补程序 6 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 6 的增强功能、已修复问题和已知问题。您可以从 登录以下载 下载 XenMobile Server 10.15 滚动修补程序 6 软件二进制文件。

新增功能

- **Secure Hub APNs 证书续订**

  XenMobile Server 10.15 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 March 12, 2024 到期。此更新会自动续订 Secure Hub APNs 证书，使其成为将于 February 9, 2025 到期的新证书。

- **在 iOS 的 Webclip 策略设置下新增字段“配置文件范围”**

  对于 iOS 设备，Webclip 设备策略的“**策略设置**”下新增了一个名为“**配置文件范围**”的字段。此功能允许您选择策略是应用于用户还是系统。有关详细信息，请参阅 Webclip 设备策略 - iOS 设置。

- **使用 REST API 更新公共应用商店应用程序的部署规则**

  在“**添加新的公共应用商店应用程序**”和“**更新公共应用商店应用程序**”REST API 中新增了一个名为“**规则**”的字段。此功能允许您更新公共应用商店应用程序的部署规则。有关详细信息，请参阅公共 REST API 文档。

- **应用程序属性设备策略支持新的 iOS 应用程序属性**

  您现在可以为安装在 iOS 设备上的应用程序指定以下属性：

  - **可移除应用程序：** 指定当应用程序是托管应用程序时，用户是否可以移除该应用程序。
  - **启用关联域直接下载：** 指定应用程序是否可以直接在域中执行声明的站点关联验证。
  - **关联域：** 指定要添加到应用程序的关联域。

  有关详细信息，请参阅 应用程序属性设备策略。

- **新增了 Knox Platform for Enterprise Key 设备策略**

  新增了一个名为 **Knox Platform for Enterprise Key** 的设备策略。此策略允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息，并使用 KPE 许可证来增强 Samsung 设备的安全性。有关详细信息，请参阅Knox Platform for Enterprise Key 设备策略。

- **支持 Apple Business Manager 共享 iPad**

  从 XenMobile Server 10.15 RP6 开始，共享 iPad 支持与 XenMobile Server 结合使用 Apple Business Manager (ABM)。此功能允许您使用 ABM 帐户登录共享 iPad 并使用它们。有关详细信息，请参阅配置共享 iPad。

> **注意：**

> 目前，此功能存在一个限制，即登录用户在 XenMobile® Server 控制台上可能显示为“匿名”。因此，某些安全操作（例如“删除所有用户”）可能无法在设备上执行，尤其是在用作共享 iPad 的设备上。要解决此问题，建议手动将 DEP 用户（托管 Apple ID）添加到 XenMobile Server 控制台，尤其是在使用 ABM 共享 iPad 的情况下。永久解决方案将包含在即将发布的版本中。

- **新增了名为“删除所有用户”的安全操作，用于共享 iPad**

  从 XenMobile Server 10.15 RP6 开始，XenMobile Server 中为共享 iPad 新增了一个名为 **Delete All users** 的安全操作。此功能允许您删除设备上的所有用户。有关详细信息，请参阅共享 iPad 的安全操作。

- **克隆交付组以用作新交付组的基础**

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

- **支持 iOS 中可选应用程序的自动更新**

  从 XenMobile Server 10.15 RP6 开始，新增了一个名为 `apple.ios.optional_app_update` 的服务器属性。此属性允许您自动更新 iOS 中的可选应用程序。`apple.ios.optional_app_update` 的默认值设置为 `False`。有关详细信息，请参阅服务器属性。

  有关可选批量购买应用程序自动更新的详细信息，请参阅检查应用程序更新。

- **优化数据库升级机制**

  数据库升级过程经过优化，可确保每个群集仅升级一次。这使您可以在 HA 群集中的滚动修补程序更新期间最大限度地减少停机时间。

已修复的问题

- 当您使用 ABM 或 ASM 配置时，无法在 iOS 共享设备上部署 Webclip 设备策略。

有关 XenMobile Server 10.15.0 以前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 10.15 滚动补丁 5 发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动补丁 5 的增强功能、已修复问题和已知问题。您可以从 登录下载 下载 XenMobile Server 10.15 滚动补丁 5 软件二进制文件。

新增功能

- **在 Android Enterprise 的 802.1x 设置中添加了一个新的强制字段“域”**

  在 Android Enterprise 平台网络策略设置页面中，为 **802.1x EAP** 身份验证类型添加了一个新字段 **域**。有关详细信息，请参阅 Android Enterprise 的 802.1x 设置。

  XenMobile Server 具有一个新属性 `afw.network.domain.support`，它在 **Android Enterprise 的 802.1x 设置**中添加了 *域* 字段。此属性的默认值为 **True**。有关详细信息，请参阅服务器属性。

- **在用于 iOS 的控制操作系统更新策略中添加了新选项“操作系统更新版本”**

  在 **iOS** 平台的 **控制操作系统更新** 策略中，在 **操作系统更新频率** 字段之后添加了一个新选项 **操作系统更新版本**。此选项允许您指定用于更新受监管 iOS 设备的操作系统版本。有关详细信息，请参阅 iOS 设置。

- **在用于 iOS 的限制策略和 Exchange 策略中添加了新设置**

  - 在用于 iOS 的 Exchange 策略中添加了新设置 **允许 Mail Drop**。有关详细信息，请参阅 Exchange 设备策略 - iOS 设置。
  - 在用于 iOS 的限制策略中添加了以下新设置：
    - 允许未配对设备启动到恢复模式
    - 安装快速安全响应
    - 删除快速安全响应
    - 允许邮件隐私保护
    - NFC
    - 允许 App Clips
    - 允许 Apple 个性化广告
    - 自动解锁

    有关详细信息，请参阅 限制设备策略 - iOS 设置。

- **操作系统更新**

  - **支持 Android 14：** XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持将 Android Enterprise 设备更新到 Android 14。有关安全和隐私优势的详细信息，请参阅 Android 文档。
  - **支持 iOS 17：** XenMobile® Server 和 Citrix Mobile 生产力应用程序现在与 iOS 17 兼容，但目前不支持任何新的 iOS 17 功能。

- **支持 macOS 14：** XenMobile Server 和 Citrix Mobile 生产力应用程序现在与 macOS 14 兼容，但目前不支持任何新的 macOS 14 功能。

已修复的问题

- 升级到 XenMobile Server 10.15 RP3 或 10.15 RP4 后，在 **Android Enterprise** > **托管 Google Play 商店应用程序** 的 **配置** > **应用程序** 页面上，**组织应用程序** 按钮不可用。
- 升级到 XenMobile Server 10.15 RP3 或 10.15 RP4 后，在为 **Android Enterprise** 平台配置 Wi-Fi 策略时，您无法在 **CA 证书** 下拉菜单中看到任何值。仅显示 **选择证书** 选项。

有关 XenMobile Server 10.15.0 以前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 10.15 滚动修补程序 4 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 4 的增强功能以及已修复和已知问题。您可以在 登录以下载 处下载 XenMobile Server 10.15 滚动修补程序 4 软件二进制文件。

新增功能

- **访问设备和应用程序报告**

  以前，**设备和应用程序**报告页面会显示所有用户的设备和应用程序信息，无论其用户组如何，即使应用了基于角色的访问控制 (RBAC) 也是如此。

  从 XenMobile Server 10.15 滚动修补程序 4 版本开始，**设备和应用程序**报告页面会显示特定于 RBAC 角色有权管理的**特定用户组**配置中定义的用户组的设备和应用程序。有关使用 RBAC 配置角色的详细信息，请参阅 使用 RBAC 配置角色。

- **支持将“控制操作系统更新”设备策略重置为系统默认值**

  从 XenMobile Server 10.15 滚动修补程序 4 版本开始，Android Enterprise 的**控制操作系统更新**页面中的**系统更新策略**下拉列表中添加了一个新值**默认**。此功能允许您将系统更新策略重置为系统默认值。有关详细信息，请参阅 控制操作系统更新设备策略。

- **在 iOS 的 Exchange 设备策略设置中添加了 OAuth 登录 URL 和 OAuth 令牌请求 URL 新字段**

  从 XenMobile Server 10.15 滚动修补程序 4 版本开始，**OAuth 登录 URL** 和 **OAuth 令牌请求 URL** 字段已添加到 **Exchange 策略** > **iOS** > **使用 OAuth** 单选按钮下。有关详细信息，请参阅 Exchange 设备策略。

- **支持同步或覆盖 iOS 的同步 Exchange 服务**

  从 XenMobile Server 10.15 滚动修补程序 4 版本开始，您可以通过启用相关设置来选择是否同步或覆盖 iOS 的以下同步 Exchange 服务。

  - 日历
  - 联系人
  - 邮件
  - 备注
  - 提醒

  有关详细信息，请参阅 Exchange 设备策略。

- **支持 iOS 设备上的 eSIM**

  XenMobile Server 有一个新属性 `ios.esim.support`，该属性使 XenMobile Server 能够从 iOS 设备获取 eSIM 信息，并在用户界面上显示 eSIM 相关的设备属性。此属性的默认值为 **True**。有关详细信息，请参阅 服务器属性。

有关 XenMobile Server 10.15.0 以前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 10.15 滚动补丁 3 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动补丁 3 的增强功能、已修复问题和已知问题。您可以在 登录下载 处下载 XenMobile Server 10.15 滚动补丁 3 软件二进制文件。

新增功能

- **XenMobile Server 支持混合许可证类型。** 此功能允许客户使用 XenMobile Server 或 Citrix Licensing Server 激活混合的 XenMobile 许可证类型和版本。有关详细信息，请参阅 激活其他许可证。
- **支持 macOS 设备上的企业应用程序。** XenMobile Server 具有一个新属性 `mac.app.push`，可用于在运行 macOS 的设备上启用企业应用程序支持。此属性的默认值为 **True**。有关详细信息，请参阅 服务器属性。

已修复问题

- 无法从 **托管 Google Play 帐户** 下载应用程序。
- 在 XenMobile® Server 控制台上，您无法看到快速安全响应 (RSR) 版本。
- 在 Android 设备上，当用户从旧版 MDX Toolkit 切换到 MAM SDK 时，Secure Mail 应用程序会从 Secure Hub Store 中删除。
- 升级到 XenMobile Server 10.15 RP2 后，使用“**受限应用程序使用**”的现有 iOS 限制设备策略无法部署到 iOS 设备上。

适用于 XenMobile Server 10.15 滚动修补程序 2 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动修补程序 2 的增强功能、已修复问题和已知问题。您可以在 登录以下载 下载 XenMobile Server 10.15 滚动修补程序 2 软件二进制文件。

新增功能

XenMobile Analyzer Tool 已弃用。 由于我们发布节奏频繁且稳定，不再需要 XenMobile Analyzer Tool。Citrix 已于 March 31, 2023 起停止此服务。我们建议您使用 Citrix XenMobile 控制台或 Citrix NetScaler Gateway 中提供的连接检查功能。有关详细信息，请参阅 连接检查。

已修复问题

- 您无法在 Android 平台上使用 APK 签名方案 v2 及更高版本算法配置企业应用程序。
- 当 NetScaler 中使用 nFactor 身份验证策略时，您无法在 Android 和 iOS 设备上访问 MAM。
- 当您在 XenMobile Server 10.14 或更高版本上导出 Citrix Gateway 身份验证的配置脚本时，脚本会被截断并且无法正常工作。
- 在 XenMobile Server 上，您无法重新编辑描述包含 **\b** 的已同步 VPP 应用程序。
- 在 XenMobile Server 10.15 及更高版本上，联机证书状态协议 (OCSP) 不响应请求。
- 在 XenMobile® Server 上，您无法注册运行 Windows 11 的设备。

XenMobile Server 10.15 滚动补丁 1 版本发行说明

这些发行说明介绍了 XenMobile Server 10.15 滚动补丁 1 的增强功能、已修复问题和已知问题。您可以在 登录下载 处下载 XenMobile Server 10.15 滚动补丁 1 软件二进制文件。

新增功能

- **网络访问控制。** 使用您的网络访问控制 (NAC) 解决方案扩展适用于 Android 和 Apple 设备的 XenMobile 设备安全评估。您的 NAC 解决方案使用 XenMobile 安全评估来促进和处理身份验证决策。配置 NAC 设备后，您在 XenMobile 中配置的设备策略和 NAC 筛选器将得到强制执行。有关详细信息，请参阅 网络访问控制。
- **Secure Hub APNs 证书续订。** 适用于 XenMobile Server 10.15 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 April 8, 2023 到期。此更新将续订 Secure Hub APNs 证书，该证书将于 March 12, 2024 到期。

已修复问题

- 在 Android Enterprise 设备上编辑或部署托管配置策略时，您会收到错误。
- 在仅限 MAM 模式下注册的 iOS 设备上，您无法从 Secure Hub 商店安装企业或 MDX 应用程序。

- 配置应用程序的跟踪 ID 后，您无法在 XenMobile® Server 控制台上查看应用程序的预期预览版本。相反，您看到的是应用程序的生产版本。
- 在 XenMobile Server 上，当预配配置文件设备策略处于待定状态时，您无法从 Secure Hub 商店安装 MDX 封装的应用程序。
- MDM 配置文件续订后，ABM 共享 iPad 将变为非托管状态。

XenMobile Server 10.14 滚动修补程序 13 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 13 的增强功能、已修复问题和已知问题。

新增功能

Secure Hub APNs 证书续订：

XenMobile Server 10.14 的 Secure Hub Apple Push Notification Service (APNs) 证书将于 March 12, 2024 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，新证书将于 February 9, 2025 到期。

有关 XenMobile Server 10.14.0 以前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 13 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 13 的增强功能、已修复问题和已知问题。

新增功能

Secure Hub APNs 证书续订：

XenMobile Server 10.14 的 Secure Hub Apple Push Notification Service (APNs) 证书将于 March 12, 2024 到期。此更新会自动将 Secure Hub APNs 证书续订为新证书，新证书将于 February 9, 2025 到期。

有关 XenMobile Server 10.14.0 以前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 12 发行版发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 12 的增强功能以及已修复和已知问题。

已修复的问题

- 您无法从 **托管式 Google Play 帐户** 下载应用程序。
- 升级到 XenMobile Server 10.14 RP11 后，现有的 iOS 限制策略无法部署到设备上。
- 当您在 Secure Hub 中注册移动设备时，应用程序不会显示在 Secure Hub 商店和托管式 Google Play 商店中。

有关 XenMobile Server 10.14.0 以前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 11 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 11 的增强功能、已修复问题和已知问题。

已修复的问题

- 无法在 Android 平台上使用 APK 签名方案 v2 及更高版本算法配置企业应用程序。
- 在 XenMobile Server 上，无法重新编辑描述中包含 *\b* 的同步 VPP 应用程序。
- 在 XenMobile Server 10.14 RP9 及更高版本上，联机证书状态协议 (OCSP) 不响应请求。
- 在 XenMobile® Server 上，无法注册运行 Windows 11 的设备。
- 在 XenMobile Server 控制台上，无法查看快速安全响应 (RSR) 版本。

有关 XenMobile Server 10.14.0 以前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 10 版本的发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 10 的增强功能、已修复问题和已知问题。

新增功能

- **Secure Hub APNs 证书续订。** XenMobile Server 10.14 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 April 8, 2023 到期。此更新续订了 Secure Hub APNs 证书，该证书将于 March 12, 2024 到期。
- **XenMobile Analyzer Tool 已弃用。** 由于我们发布节奏频繁且稳定，XenMobile Analyzer Tool 不再需要。Citrix 已决定自 March 31, 2023 起停止此服务。我们建议您使用 Citrix XenMobile 控制台或 Citrix NetScaler Gateway 中提供的连接检查。有关详细信息，请参阅连接检查。

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

已修复问题

- MDM 配置文件续订后，ABM 共享 iPad 会变为非托管状态。
- 在仅限 MAM 模式下注册的 iOS 设备上，您无法从 Secure Hub 商店安装企业或 MDX 应用程序。
- 在 NetScaler 中使用 nFactor 身份验证策略时，您无法在 Android 和 iOS 设备上访问 MAM。
- 当您在 XenMobile Server 10.14 或更高版本上导出 Citrix Gateway 身份验证的配置脚本时，脚本会被截断并且无法工作。

XenMobile Server 10.14 滚动修补程序 9 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 9 的增强功能、已修复问题和已知问题。

新增功能

网络访问控制。 使用您的网络访问控制 (NAC) 解决方案来扩展适用于 Android 和 Apple 设备的 XenMobile 设备安全评估。您的 NAC 解决方案使用 XenMobile 安全评估来促进和处理身份验证决策。配置 NAC 设备后，您在 XenMobile 中配置的设备策略和 NAC 筛选器将强制执行。有关详细信息，请参阅网络访问控制。

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

已修复问题

- 在 XenMobile Server 10.14 版本上，即使许可证到期日期不在通知窗口内，您也会收到许可证到期通知。
- 在某些应用程序上，即使安装的版本是最新版本，您也会在 Secure Hub 应用程序商店中看到“**待处理更新**”状态。
- 在 XenMobile® Server 上，您无法在德语区域设置中创建或编辑“限制”设备策略。
- 在 XenMobile Server 10.14 版本上，非 DEP iOS 设备的“**所有者**”选项卡显示为空白。
- 当“**主题备用名称类型**”不是 *None* 时，SCEP 设备策略会失败。
- 在 Android Enterprise 设备上编辑或部署托管配置策略时，您会收到错误。
- 在以仅 MAM 模式注册的 iOS 设备上，您无法从 Secure Hub 应用程序商店安装企业或 MDX 应用程序。
- 配置应用程序的跟踪 ID 后，您无法在 XenMobile Server 控制台上查看应用程序的预期预览版本。相反，您会看到应用程序的生产版本。

- 在 XenMobile Server 上，当预配配置文件设备策略处于待处理状态时，您无法从 Secure Hub 商店安装 MDX 封装的应用程序。

XenMobile Server 10.14 滚动修补程序 8 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 8 的增强功能、已修复问题和已知问题。

新增功能

弃用对 Windows 信息保护策略的支持。根据 Windows 公告，XenMobile Server 已弃用对 Windows 信息保护 (WIP) 的支持。通过添加名为 **windows.wip.deprecation** 的服务器属性（其值默认为 **True**），已弃用对 WIP 的支持。有关详细信息，请参阅 服务器属性。

有关 XenMobile Server 10.14.0 以前的滚动修补程序的信息，请参阅 滚动修补程序发行说明。

已修复问题

- 在 XenMobile® Server 上，您无法在德语区域设置中创建或编辑“**自动更新托管应用程序**”策略。

XenMobile Server 10.14 滚动修补程序 7 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 7 的增强功能、已修复问题和已知问题。

新增功能

- **操作系统更新**
  - **支持 iOS 16。** XenMobile® Server 和 Citrix Mobile 生产力应用程序与 iOS 16 兼容，但目前不支持任何新的 iOS 16 功能。
  - **支持 Android 13**。XenMobile Server 现在支持将 Android Enterprise 设备更新到 Android 13。有关安全和隐私优势的摘要，请参阅 Android 文档。
- **已弃用功能。** 现已删除对以下功能的支持：
  - RBAC 角色 - 共享和 COSU 设备注册器
  - Android - 索尼和 HTC
  - 高安全性注册模式
  - 派生凭据
  - SEAMS
  - 视窗手机设备，

  - 通用、DigiCert 管理和 Entrust 适配器 PKI 实体。

  有关详细信息，请参阅 弃用。

- **已弃用对移动服务提供商 (MSP) 界面的支持。** 通过添加一个名为 `deprecate.mobile.service.provider` 的新服务器属性，已弃用对 MSP 的支持，该属性将 MSP 界面从控制台中删除，默认设置为 **True**。有关详细信息，请参阅服务器属性。
- **已删除对 Windows 10 设备 *允许自动连接到 WiFi Sense 热点* 限制策略的支持。** 有关详细信息，请参阅Windows 桌面/平板电脑设置。
- **已弃用对 Nexmo SMS 网关的支持。** 通过添加一个名为 `deprecate.carrier.sms.gateway` 的服务器属性，已弃用对 Nexmo SMS 的支持，该属性默认设置为 **True**。Nexmo SMS 在自助服务门户中也已弃用。有关详细信息，请参阅通知。
- **Google 弃用 API。** Google 正在弃用 XenMobile Server 中用于应用程序类别和许可证的多个 API。以下更改已生效：
  - 您现在选择要添加的应用程序，而不是批准。请参阅托管应用商店应用程序。
  - 您现在将应用程序组织到集合中，而不是类别中。请参阅组织应用程序。
  - 您不能再将应用程序许可证与用户解除关联。请参阅添加应用程序。
- **配置优先级以自动更新 Android Enterprise 托管应用程序。** 指定 Android Enterprise 托管应用程序是以低优先级还是高优先级自动更新。您还可以推迟自动更新。有关详细信息，请参阅自动更新托管应用程序设备策略。

有关 XenMobile Server 10.14.0 以前的滚动修补程序的信息，请参阅滚动修补程序发行说明。

已修复的问题

- 在某些运行 Android 的设备上，当某些公共应用程序在 Google Play 上不可用时，您无法访问 Secure Hub。
- 在某些 macOS 设备上，SSL 证书续订后，已安装的配置文件和证书会自动删除。
- 在 XenMobile Server 控制台中，您无法编辑名称中包含 **/** 符号的限制设备策略。
- 已发布的 DEP 设备仍显示在 XenMobile Server 控制台中。
- 您无法访问 Secure Hub Store。您收到以下错误：**您的登录已过期。请重新登录以继续。**

XenMobile Server 10.14 滚动修补程序 6 版本发行说明

这些发行说明描述了 XenMobile Server 10.14 滚动修补程序 6 的增强功能以及已修复和已知问题。

新增功能

新增了限制策略。 在限制策略中添加了**允许从工作配置文件复制和粘贴**和**允许从个人配置文件共享数据**。将这些策略设置为**关闭**以限制从个人配置文件复制、粘贴和导入到工作配置文件。有关详细信息，请参阅限制设备策略。

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

已修复问题

- 在 XenMobile® Server 上，某些 VPP 应用程序的正确版本不会自动更新。
- 在 XenMobile Server 10.14 版本上，您无法删除某些 Active Directory 用户。
- 在运行 iOS 15 的设备新注册时，当连接类型设置为**AlwaysOn IKEv2 双重配置**时，VPN 策略部署失败。

XenMobile Server 10.14 滚动修补程序 5 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 5 的增强功能、已修复问题和已知问题。

新增功能

- **启用 Google Analytics**。要在 XenMobile Server 上启用 Google Analytics，请将服务器属性 **xms.ga.enabled** 的值设置为 **True**。默认值为 **True**。
- **Secure Hub APNs 证书续订。** XenMobile Server 10.14 的 Secure Hub Apple 推送通知服务 (APNs) 证书将于 May 7, 2022 到期。此更新将续订 Secure Hub APNs 证书，该证书将于 April 8, 2023 到期。

有关 XenMobile Server 10.14.0 以前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，设备证书颁发者 CA 在设备上 CA 续订后不会更新。
- 在某些设备上，SQL 数据库中有两个证书条目，这会导致错误。
- 在 XenMobile Server 10.14 版本中，您无法编辑预配配置文件设备策略。
- 在 XenMobile Server 上，当您从 ShareFile Enterprise 更改为连接器时，交付组下的 GUI 不会更新。

XenMobile Server 10.14 滚动修补程序 4 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动修补程序 4 的增强功能、已修复问题和已知问题。

新增功能

启用 WSDL 服务。要在 XenMobile Server 上启用 WSDL 服务，请将服务器属性 `wsdl.service.enabled` 的值设置为 **True**。在使用 ActiveSync 网关连接器时，此项是必需的。默认值为 **False**。

有关 XenMobile Server 10.14.0 以前的滚动修补程序的信息，请参阅滚动修补程序发行说明。

已修复问题

- 在某些 Android Enterprise 设备上，交付组和分配的策略或应用程序会间歇性地无法应用。
- 在 XenMobile Server 10.13 版本上，您无法仅使用存储区域连接器连接和配置存储区域控制器。
- 在仅 MDM 模式下注册的 iOS 设备上，您无法通过 Secure Hub 从 App Store 打开的浏览器添加应用程序。您会收到以下错误：**您的登录已过期。请重新登录以继续。**
- 在 XenMobile Server 10.13 RP1 及更高版本上，SNMP 监控的 XenMobile 节点间连接陷阱不起作用。
- 在 XenMobile® Server 上，W-SU 时区显示的时间不正确。

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

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和已知问题。

此版本包含错误修复。

有关 XenMobile Server 10.14.0 以前的滚动修补程序的信息，请参阅 滚动修补程序发行说明。

XenMobile Server 10.14 滚动补丁 2 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动补丁 2 的增强功能、已修复问题和已知问题。

有关 XenMobile Server 10.14.0 以前的滚动补丁的信息，请参阅 滚动补丁发行说明。

已修复问题

在 XenMobile® Server 上，您会观察到服务器节点在高峰时段 CPU 利用率很高。

XenMobile Server 10.14 滚动补丁 1 版本发行说明

这些发行说明介绍了 XenMobile Server 10.14 滚动补丁 1 的增强功能、已修复问题和已知问题。

新增功能

- **支持 Windows 11 设备。** 您现在可以使用 XenMobile 管理 Windows 11 设备。有关详细信息，请参阅操作系统支持列表。
- **配置 macOS 的连接模式和网络优先级。** 在 Wi-Fi 设备策略中，为 macOS 设备启用**连接模式**设置，以选择用户如何加入网络。设备可以使用系统凭据或在登录窗口输入的凭据来验证用户。如果您有多个网络，请在**优先级**字段中输入一个数字来设置网络连接的优先级。设备将选择数字最小的网络。有关详细信息，请参阅Wi-Fi 设备策略中的 macOS 设置。
- 由于 Google 弃用了对 Android Enterprise 设备上组许可证的支持，XenMobile Server 将无法将组许可证同步到 Google。有关详细信息，请参阅本文。

已知问题

从 macOS 11 或更早版本升级到 macOS 12 的已注册设备，或在 macOS 12 上新注册的设备，可能会在设备的 **“系统偏好设置”>“配置文件”** 下显示为“未验证”。有关详细信息和解决方法，请参阅此支持文章。

已修复问题

- 注册 iOS 15 或 macOS 12 设备后，MDM 配置配置文件显示为**未验证**。
- 在 XenMobile® Server 控制台中，当您修改应用程序设置以清除所有平台并保存时，该应用程序不会列在**配置 > 应用程序**中。
- 您无法退出 Android Enterprise 平台上的 Citrix® 启动器。您会收到以下错误：**密码不正确**。
- 在 XenMobile Server 10.14 版本中，您无法编辑**导入 iOS 和 macOS 配置文件**策略。

XenMobile Server 10.16 中的新增功能

继续支持从 Citrix ADC 弃用的经典策略

Citrix 最近宣布，从 Citrix ADC 12.0 build 56.20 开始，将弃用一些基于经典策略的功能。Citrix ADC 弃用通知对现有 XenMobile Server 与 Citrix Gateway 的集成没有影响。XenMobile Server 将继续支持经典策略，无需采取任何措施。

弃用公告

有关正在逐步淘汰的 Citrix XenMobile 功能的提前通知，请参阅弃用。

升级端点到 iOS 14.5 之前

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

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

升级本地 Citrix ADC 之前

将本地 Citrix ADC 升级到某些版本可能会导致单点登录错误。使用浏览器中的“**公司员工登录**”选项单点登录到 Citrix Files 或 ShareFile 域 URL 会导致错误。用户无法登录。

要解决此问题：如果您尚未在 Citrix Gateway 上从 ADC CLI 运行以下命令，请运行它以启用全局 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) 13.1 Build 33.52

- 受影响的 SSO 配置

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

升级到 XenMobile 10.16（本地部署）之前

某些系统要求已更改。有关详细信息，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 RAM 小于 8 GB，建议将 RAM 增加到至少 8 GB。
2. 在更新到 XenMobile Server 10.16 的最新版本之前，请将您的 Citrix License Server 更新到 11.17.2.0 Build 47000 或更高版本。

   最新版本的 XenMobile 需要 Citrix License Server 11.17（最低版本）。

   > **注意：**
   >
   > XenMobile 10.16 中的客户成功服务日期（以前称为 Subscription Advantage 日期）是 November 15, 2022。您的 Citrix 许可证上的客户成功服务日期必须晚于此日期。
   >
   > 您可以在许可证服务器中许可证旁边查看日期。如果将最新版本的 XenMobile 连接到较旧的许可证服务器环境，则连接性检查将失败，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 Portal 下载最新的许可证文件，然后将文件上传到许可服务器。请参阅客户成功服务。

   许可证激活服务 (LAS) 是用于 Citrix 产品套件中产品激活的下一代技术。如果在 10.15 滚动修补程序 13 或更高版本的滚动修补程序中启用了许可证激活服务，则直接升级到 10.16.0.48 会重置许可证激活服务配置。请继续应用 10.16 滚动修补程序版本 10.16 滚动修补程序 7 或更高版本，其中可以重新配置许可证激活服务。现有设备不受影响。
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 Citrix Gateway 配置为 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
4. 建议：在安装 XenMobile 更新之前，请使用 VM 中的功能为系统创建快照。此外，请备份您的系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。

升级方法

此版本中，XenMobile 支持 VMware ESXi 7.0。请确保在安装或升级 ESXi 7.0 之前，您已升级到 10.14 或更高版本。

您可以从 XenMobile 10.15.x 或 10.14.x 直接升级到 XenMobile 10.16。要执行升级，请下载最新的可用二进制文件：转到思杰下载页面。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击 **Download File**。

要上传升级，请使用 XenMobile 控制台中的 **Release Management** 页面。请参阅(/zh-cn/xenmobile/server/upgrade.html#to-upgrade-using-the-release-management-page)。

升级后

如果涉及出站连接的功能停止工作，并且您没有更改连接配置，请检查 XenMobile Server 日志中是否存在以下错误："Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer"。

- 证书验证错误意味着您必须在 XenMobile Server 上禁用主机名验证。
- 默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。
- 如果主机名验证破坏了您的部署，请将服务器属性 `disable.hostname.verification` 更改为 `true`。此属性的默认值为 `false`。

平台更新

- **支持 Android 14：** XenMobile Server 和 Citrix Mobile 生产力应用程序现在支持将 Android Enterprise 设备更新到 Android 14。有关安全和隐私优势的更多信息，请参阅 Android 文档。
- **支持 iOS 17：** XenMobile Server 和 Citrix Mobile 生产力应用程序现在与 iOS 17 兼容，但目前不支持任何新的 iOS 17 功能。
- **支持 macOS 14：** XenMobile Server 和 Citrix Mobile 生产力应用程序现在与 macOS 14 兼容，但目前不支持任何新的 macOS 14 功能。

访问"设备和应用程序"报告

以前，**设备和应用程序**报告页面会显示所有用户的设备和应用程序信息，无论其用户组如何，即使应用了基于角色的访问控制 (RBAC) 也是如此。

从 XenMobile Server 10.16 版本开始，**设备和应用程序**报告页面会显示特定于 **To specific user groups** 中定义的用户组的设备和应用程序，RBAC 角色有权管理这些用户组。有关使用 RBAC 配置角色的更多信息，请参阅(/zh-cn/xenmobile/server/users/rbac-roles-and-permissions.html)。

在 Android Enterprise 的 802.1x 设置中添加了一个新的必填字段“域”

在 Android Enterprise 平台网络策略设置页面中，为 **802.1x EAP** 身份验证类型添加了一个新字段**域**。有关详细信息，请参阅 Android Enterprise 的 802.1x 设置。

在 iOS 的限制设备策略和 Exchange 设备策略中添加了新设置

- 在 iOS 的 Exchange 设备策略中添加了一个新设置 **允许邮件投送**。有关详细信息，请参阅 Exchange 设备策略 - iOS 设置。
- 在 iOS 的限制设备策略中添加了以下新设置：
  - 允许未配对的设备启动到恢复模式
  - 安装快速安全响应
  - 移除快速安全响应
  - 允许邮件隐私保护
  - NFC
  - 允许 App Clips
  - 允许 Apple 个性化广告
  - 自动解锁

有关详细信息，请参阅 限制设备策略 - iOS 设置。

在 iOS 的 Exchange 设备策略设置中添加了新字段 OAuth 登录 URL 和 OAuth 令牌请求 URL

从 XenMobile Server 10.16 版本开始，在 **Exchange 策略** > **iOS** > **使用 OAuth** 单选按钮下添加了 **OAuth 登录 URL** 和 **OAuth 令牌请求 URL** 字段。有关详细信息，请参阅Exchange 设备策略。

添加了新的 Knox Platform for Enterprise Key 设备策略

已添加名为 **Knox Platform for Enterprise Key** 的新设备策略。此策略允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息，并使用 KPE 许可证来增强 Samsung 设备的安全性。有关详细信息，请参阅Knox Platform for Enterprise Key 设备策略。

克隆交付组以用作新交付组的基础

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

支持 Apple Business Manager 共享 iPad

从 XenMobile Server 10.16 版本开始，共享 iPad 支持将 Apple Business Manager (ABM) 与 XenMobile Server 结合使用。这允许您使用 ABM 帐户登录共享 iPad 并使用它们。有关详细信息，请参阅配置共享 iPad。

为共享 iPad 添加了名为“删除所有用户”的新安全操作

从 XenMobile Server 10.16 版本开始，XenMobile Server 中为共享 iPad 添加了一个名为“**删除所有用户**”的新安全操作。这允许您删除设备上的所有用户。有关详细信息，请参阅共享 iPad 的安全操作。

应用程序属性设备策略支持新的 iOS 应用程序属性

您现在可以为安装在 iOS 设备上的应用程序指定以下属性：

- **可移除应用程序：** 指定当应用程序是托管应用程序时，用户是否可以移除该应用程序。
- **启用关联域直接下载：** 指定应用程序是否可以直接在域上执行声明的站点关联验证。
- **关联域：** 指定要添加到应用程序的关联域。

有关详细信息，请参阅应用程序属性设备策略。

支持同步或覆盖 iOS 的同步 Exchange 服务

从 XenMobile Server 10.16 版本开始，您可以通过启用相关设置来选择同步或覆盖 iOS 的以下同步 Exchange 服务。

- 日历
- 联系人

- 邮件
- 备忘录
- 提醒事项

有关详细信息，请参阅Exchange 设备策略。

支持将“控制操作系统更新”设备策略重置为系统默认值

从 XenMobile Server 10.16 版本开始，Android Enterprise 的“**控制操作系统更新**”下的“**系统更新策略**”下拉列表中新增了一个值“**默认**”。此功能允许您将系统更新策略重置为系统默认值。有关详细信息，请参阅控制操作系统更新设备策略。

在 iOS 的操作系统更新策略中添加了新选项“操作系统更新版本”

在 **iOS** 平台的“**操作系统更新策略**”中，“**操作系统更新频率**”字段后新增了一个选项“**操作系统更新版本**”。此选项允许您指定用于更新受监管 iOS 设备的操作系统版本。有关详细信息，请参阅iOS 设置。

网络访问控制

使用网络访问控制 (NAC) 解决方案扩展 Android 和 Apple 设备的 XenMobile 设备安全评估。NAC 解决方案使用 XenMobile 安全评估来促进和处理身份验证决策。配置 NAC 设备后，您在 XenMobile 中配置的设备策略和 NAC 过滤器将生效。有关详细信息，请参阅网络访问控制。

支持 XenMobile Server 的混合许可证类型

此功能允许您使用 XenMobile Server 或 Citrix Licensing Server 激活 XenMobile 许可证类型和版本的混合。有关详细信息，请参阅 激活不同的许可证。

支持 iOS 设备上的 eSIM

XenMobile Server 具有一个新属性 `ios.esim.support`，该属性使 XenMobile Server 能够从 iOS 设备获取 eSIM 信息，并在用户界面上显示 eSIM 相关的设备属性。此属性的默认值为 **True**。有关详细信息，请参阅 服务器属性。

适用于 Android Enterprise 平台的 VPN 设备策略

以前，您可以通过在 **XenMobile 选项设备策略**中启用**启用始终开启的 VPN** 选项来为运行 Android Enterprise 的设备启用 VPN 服务。

从 XenMobile Server 10.16 开始，您可以通过在 **VPN 设备策略**中启用**启用始终开启的 VPN** 选项来为运行 Android Enterprise 的设备启用始终开启的 VPN 服务。如果您在以前的版本中已在 **XenMobile 选项设备策略**中启用了**启用始终开启的 VPN** 选项，请确保为新注册的设备在 **VPN 设备策略**中再次启用该选项。对于已注册的设备，无需进行任何更改。有关详细信息，请参阅 适用于 Android Enterprise 平台的 VPN 设备策略。

在 iOS 的 Webclip 策略设置下添加了新字段“配置文件范围”

对于 iOS 设备，在 Webclip 设备策略的**策略设置**下添加了一个名为**配置文件范围**的新字段。这允许您选择策略是应用于用户还是系统。有关详细信息，请参阅 Webclip 设备策略 - iOS 设置。

Secure Hub APNs 证书续订

此更新会自动将 XenMobile Server 10.16 的 Secure Hub Apple 推送通知服务 (APNs) 证书续订为将于 February 9, 2025 到期的新证书。

使用 REST API 更新公共应用商店应用的部署规则

在 **Add New Public Store App** 和 **Update Public Store App** REST API 中添加了一个名为 **rules** 的新字段。这允许您更新公共应用商店应用的部署规则。有关详细信息，请参阅 公共 REST API 文档。

支持 iOS 中可选应用的自动更新

从 XenMobile Server 10.16 开始，添加了一个名为 `apple.ios.optional_app_update` 的新服务器属性。此属性允许您在 iOS 中自动更新可选应用。`apple.ios.optional_app_update` 的默认值设置为 **False**。有关详细信息，请参阅 服务器属性。

有关可选批量购买应用的自动更新的详细信息，请参阅 检查应用更新。

macOS 设备上企业应用程序的支持

XenMobile Server 有一个新属性 `mac.app.push`，它支持在运行 macOS 的设备上使用企业应用程序。此属性的默认值为 **True**。有关详细信息，请参阅服务器属性。

“总应用程序部署尝试次数”和“前 100 个已安装应用程序”的设备报告增强功能

在 XenMobile Server 控制台的“分析”->“报告”中，“总应用程序部署尝试次数”中添加了两个新列：“**操作系统版本**”和“**设备型号**”，并添加了新的设备报告“**前 100 个已安装应用程序**”以显示每个平台安装的前 100 个应用程序。有关详细信息，请参阅报告。

XenMobile Server 有一个新属性 `device.report.enhancement.enabled`，它支持上述新的设备报告增强功能。此属性的默认值为 **True**。有关详细信息，请参阅服务器属性。

设备注册中排序和筛选的现代化

XenMobile Server 中的列表视图目前难以导航且用户不友好。通过将筛选和排序选项移动到列标题，用户可以组合这些功能，从而更简单直观地查找所需数据。

弃用和删除

XenMobile Analyzer 工具的弃用： 根据我们频繁且稳定的发布节奏，不再需要 XenMobile Analyzer 工具。Citrix 已于 March 31, 2023 停止此服务。Citrix 建议您使用 Citrix XenMobile 控制台或 Citrix Gateway 中提供的连接检查。有关详细信息，请参阅连接检查。

XenMobile Server 10.15 中的新增功能

XenMobile Server 10.15 (PDF 下载)

继续支持从 Citrix ADC 弃用的经典策略

Citrix 最近宣布，从 Citrix ADC 12.0 版本 56.20 开始，将弃用一些基于经典策略的功能。Citrix ADC 弃用通知对现有 XenMobile Server 与 Citrix Gateway 的集成没有影响。XenMobile Server 将继续支持经典策略，无需采取任何措施。

弃用公告

有关正在逐步淘汰的 Citrix XenMobile 功能的提前通知，请参阅弃用。

将端点升级到 iOS 14.5 之前

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

- 将 Citrix Secure Mail 和 Secure Web 升级到 21.2.X 或更高版本。请参阅升级 MDX 或企业应用程序。

- 如果您使用 MDX Toolkit，请使用 MDX Toolkit 21.3.X 或更高版本封装所有第三方 iOS 应用程序。请查看 MDX Toolkit 下载页面 以获取最新版本。

升级本地 Citrix ADC 之前

将本地 Citrix ADC 升级到某些版本可能会导致单点登录错误。在浏览器中使用**公司员工登录**选项单点登录 Citrix Files 或 ShareFile 域 URL 会导致错误。用户无法登录。

要解决此问题：如果您尚未在 Citrix Gateway 上从 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) 13.1 Build 33.52
- 受影响的 SSO 配置

完成此解决方法后，用户可以使用浏览器中的“公司员工登录”选项通过 SSO 对 Citrix Files 或 ShareFile 域 URL 进行身份验证。

升级到 XenMobile 10.15（本地部署）之前

某些系统要求已更改。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 RAM 小于 8 GB，建议将 RAM 增加到至少 8 GB。
2. 在更新到最新版本的 XenMobile Server 10.15 之前，请将 Citrix License Server 更新到 11.17 或更高版本。

   最新版本的 XenMobile 需要 Citrix License Server 11.17（最低版本）。

   > **注意：**
   >
   > XenMobile 10.15 中的客户成功服务日期（以前称为 Subscription Advantage 日期）是 November 15, 2022。您的 Citrix 许可证上的客户成功服务日期必须晚于此日期。

> 您可以在 License Server 中许可证旁边查看日期。如果将最新版本的 XenMobile 连接到较旧的 License Server 环境，则连接性检查将失败，并且您无法配置 License Server。

> 要续订许可证上的日期，请从 Citrix Portal 下载最新的许可证文件，然后将该文件上传到许可服务器。请参阅客户成功服务。

3. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序有以下要求。如果 Citrix Gateway 配置为 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
4. 建议：在安装 XenMobile 更新之前，请使用 VM 中的功能创建系统快照。此外，请备份系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。

要升级

在此版本中，XenMobile 支持 VMware ESXi 7.0。请确保在安装或升级 ESXi 7.0 之前，先升级到 10.14 或更高版本。

您可以从 XenMobile 10.14.x 或 10.13.x 直接升级到 XenMobile 10.15。要执行升级，请下载最新的可用二进制文件：转至 `<https://www.citrix.com/downloads>`。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击**下载文件**。

要上传升级，请使用 XenMobile 控制台中的**版本管理**页面。请参阅使用版本管理页面进行升级。

升级后

如果涉及出站连接的功能停止工作，并且您没有更改连接配置，请检查 XenMobile Server 日志中是否存在以下错误："无法连接到 VPP 服务器：主机名 '192.0.2.0' 与对等方提供的证书主题不匹配"。

- 证书验证错误意味着您必须在 XenMobile Server 上禁用主机名验证。
- 默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。
- 如果主机名验证导致部署中断，请将服务器属性 `disable.hostname.verification` 更改为 `true`。此属性的默认值为 `false`。

平台更新

支持 iOS 16。 XenMobile Server 和 Citrix Mobile 生产力应用程序与 iOS 16 兼容，但目前不支持任何新的 iOS 16 功能。

支持 Android 13。 XenMobile Server 支持 Android Enterprise 设备更新到 Android 13。有关安全和隐私优势的摘要，请参阅 Android 文档。

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

配置 macOS 的连接模式和网络优先级

在 Wi-Fi 设备策略中，为 macOS 设备启用**连接模式**设置，以选择用户如何加入网络。设备可以使用系统凭据或在登录窗口输入的凭据来验证用户。如果您有多个网络，请在*优先级*字段中键入一个数字来设置网络连接的优先级。设备会选择数字最小的网络。有关详细信息，请参阅 Wi-Fi 设备策略中的 macOS 设置。

配置优先级以自动更新 Android Enterprise 托管应用程序

指定 Android Enterprise 托管应用程序是以低优先级还是高优先级自动更新。您还可以推迟自动更新。有关详细信息，请参阅自动更新托管应用程序设备策略。

在 Citrix Hypervisor 8.2 CU1 及更高版本上使用硬件虚拟化模式 (HVM) 映像

Citrix Hypervisor 8.2 CU1 及更高版本不再支持半虚拟化 (PV) 虚拟机。有关详细信息，请参阅累积更新 1。

从 XenMobile Server 10.15 版开始，支持硬件虚拟化模式 (HVM)。对于新的 XenMobile Server 安装，请从 citrix.com 下载 HVM xva 映像。对于现有 XenMobile Server 环境，请按照步骤从 PV 迁移到 HVM 访客。HVM 访客映像可在 citrix.com 上的 XenMobile Server 10.15 及更高版本中获取。

先决条件

- 确保启用群集，并且数据库是远程的。
- 作为备份，请保留旧的 PV 节点，或保存快照。如果 PV 节点位于 XenMobile Server 10.14 或 10.13 版本上，请同时备份数据库。
- 迁移之前，请从不会传输到新 HVM 节点的旧 PV 节点下载支持包。

迁移步骤

1. 下载 XenMobile Server 10.15 HVM xva 映像。
2. 关闭旧的 PV 访客节点。
3. 在 Citrix Hypervisor 中启动新的 HVM 节点。
4. 配置 XenMobile Server 10.15 节点，使其使用与旧节点相同的数据库设置以及现有群集中的服务器 PKI 密钥库密码。
5. 如有必要，请更新 Citrix Gateway 设置。

> **注意：**
>
> 如果在迁移过程中出现故障，请启动使用相同版本数据库的旧 PV 节点。

> **重要提示：**
>
> 请勿为您的 XenMobile PV 访客运行命令 `/opt/xensource/bin/pv2hvm`。这会导致虚拟机启动失败。

启用 谷歌分析

要在 XenMobile Server 上启用 Google Analytics，请将服务器属性 *xms.ga.enabled* 的值设置为 **True**。默认值为 **True**。

添加了新的限制策略

已将 *Allow copy and paste from work profile* 和 *Allow data sharing from personal profile* 添加到限制策略中。将这些策略设置为 **OFF** 可限制从个人配置文件复制、粘贴和导入到工作配置文件。有关更多详细信息，请参阅限制设备策略。

Secure Hub APNs 证书续订

XenMobile Server 的 Secure Hub Apple 推送通知服务 (APNs) 证书已于 May 7, 2022 到期。此更新续订了 Secure Hub APNs 证书，该证书将于 April 8, 2023 到期。

弃用和删除

- **Google 弃用 API。** Google 正在弃用 XenMobile Server 中用于应用程序类别和许可证的多个 API。以下更改已生效：
  - 您现在选择要添加的应用程序，而不是批准。请参阅托管应用商店应用程序。
  - 您现在将应用程序组织到集合中，而不是类别中。请参阅组织应用程序。
  - 您不能再将应用程序许可证与用户解除关联。请参阅添加应用程序。
- **已弃用对 Windows 信息保护策略的支持。** 根据 Windows 公告，XenMobile Server 已弃用对 Windows 信息保护 (WIP) 的支持。通过添加一个名为 *windows.wip.deprecation* 的服务器属性（其值默认设置为 *True*）来弃用对 WIP 的支持。有关更多信息，请参阅服务器属性。

- **已弃用对移动服务提供商 (MSP) 接口的支持。** 通过添加一个名为 *deprecate.mobile.service.provider* 的新服务器属性来弃用对 MSP 的支持，该属性从控制台中删除了 MSP 接口，其值默认设置为 *True*。有关更多信息，请参阅服务器属性。
- **弃用对 Nexmo SMS 网关的支持。** 通过添加名为 *deprecate.carrier.sms.gateway* 的新服务器属性（默认设置为 *True*），已弃用对 Nexmo SMS 的支持。自助服务门户中也弃用了 Nexmo SMS。有关详细信息，请参阅通知。
- **弃用对 Windows 10 设备 *允许自动连接到 WiFi Sense 热点* 限制策略的支持。** 有关详细信息，请参阅Windows 桌面/平板电脑设置。
- **注册邀请设置。** 弃用使用设备 IMEI、序列号和 UDID 创建注册邀请的支持。创建注册邀请时，请在 XenMobile Server 控制台的 **管理 > 注册邀请** 下配置可用设置。
- **现已删除对以下功能的支持：**
  - Android – 亚马逊
  - Android – 索尼和 HTC
  - Zebra 设备上的自定义 XML
  - 派生凭据
  - 通用、DigiCert 管理和 Entrust 适配器 PKI 实体。
  - 高安全性注册模式
  - RBAC 角色 - 共享和 COSU 设备注册器
  - 三星 SAFE 和 Knox
  - SEAMS
  - Windows 手机设备

  有关详细信息，请参阅弃用。

XenMobile Server 10.14 中的新增功能

XenMobile Server 10.14（PDF 下载）

继续支持从 Citrix ADC 弃用的经典策略

Citrix 最近宣布，从 Citrix ADC 12.0 build 56.20 开始，将弃用一些基于经典策略的功能。Citrix ADC 弃用通知对现有 XenMobile Server 与 Citrix Gateway 的集成没有影响。XenMobile Server 将继续支持经典策略，无需采取任何措施。

弃用公告

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

将端点升级到 iOS 14.5 之前

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

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

升级本地 Citrix ADC 之前

将本地 Citrix ADC 升级到某些版本可能会导致单点登录错误。在浏览器中使用**公司员工登录**选项单点登录到 Citrix Files 或 ShareFile 域 URL 会导致错误。用户无法登录。

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

完成此变通办法后，用户可以使用 SSO 身份验证到 Citrix Files 或 ShareFile 域 URL，在浏览器中使用“公司员工登录”选项。

升级到 XenMobile 10.14（本地部署）之前

某些系统要求已更改。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 RAM 小于 8 GB，我们建议将 RAM 增加到至少 8 GB。
2. 在更新到 XenMobile Server 10.14 的最新版本之前，请将 Citrix License Server 更新到 11.16 或更高版本。

最新版本的 XenMobile 需要 Citrix License Server 11.16（最低版本）。

> **注意：**
>
> XenMobile 10.14 中的客户成功服务日期（以前称为 Subscription Advantage 日期）是 September 15, 2021。您的 Citrix 许可证上的客户成功服务日期必须晚于此日期。
>
> 您可以在 License Server 中查看许可证旁边的日期。如果您将最新版本的 XenMobile 连接到较旧的 License Server 环境，连接性检查将失败，并且您无法配置 License Server。
>
> 要续订许可证上的日期，请从 Citrix Portal 下载最新的许可证文件，然后将文件上传到 Licensing Server。请参阅 客户成功服务。

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 Citrix Gateway 配置为 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
4. 建议：在安装 XenMobile 更新之前，请使用 VM 中的功能为系统创建快照。此外，请备份系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。

要升级

在此版本中，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。

您可以直接从 XenMobile 10.13.x 或 10.12.x 升级到 XenMobile 10.14。要执行升级，请下载最新的可用二进制文件：转至 `<https://www.citrix.com/downloads>`。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击**下载文件**。

要上传升级，请使用 XenMobile 控制台中的**版本管理**页面。请参阅使用版本管理页面进行升级。

升级后

如果涉及出站连接的功能停止工作，并且您没有更改连接配置，请检查 **XenMobile Server 日志**中是否存在以下错误：“无法连接到 VPP 服务器：主机名 '192.0.2.0' 与对等方提供的证书主题不匹配”。

- 证书验证错误意味着您必须在 XenMobile Server 上禁用主机名验证。
- 默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。

- 如果主机名验证导致部署中断，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 Mobile 生产力应用程序与 iOS 15 兼容，但目前不支持任何新的 iOS 15 功能。
- **Android 12：** XenMobile Server 支持 Android 12。有关 Google 设备管理 API 的弃用如何影响运行 Android 10+ 的设备的信息，请参阅从设备管理迁移到 Android Enterprise。另请参阅此 Citrix 博客。

设备策略

- 我们为所有 Android Enterprise 注册模式添加了两个设置，以使其与 Google 设置更紧密地保持一致并简化配置。
  - **允许蓝牙共享：** 如果未选中，用户无法在其设备上建立出站蓝牙共享。
  - **允许卸载应用程序：** 允许用户从托管 Google Play 商店中卸载应用程序。

  此外，我们将**允许无线升级**设置从“限制”策略移至“操作系统更新”策略。

  有关这些更改的更多信息，请参阅限制设备策略和操作系统更新设备策略。
- Android Enterprise 的限制设置已重新组织以提高清晰度。有时，设置名称会进行微小更改。有关重新组织的更多信息，请参阅Android Enterprise 设置。
- 您现在可以自动更新 Android Enterprise 设备上的托管应用程序。有关更多信息，请参阅自动更新托管应用程序设备策略。
- 您可以使用文件设备策略配置可上传的文件类型列表。即使您将以下文件类型添加到此允许列表中，也无法上传它们：
  - .cab 文件
  - .appx 文件
  - .ipa 文件
  - .apk 文件
  - .xap 文件
  - .mdx 文件
  - .exe 文件

  有关更多信息，请参阅服务器属性

设备注册

- 您现在可以为 iOS 和 Android 设备创建不同的注册配置文件。XenMobile Server 支持多种具有不同注册类型的注册配置文件。有关更多信息，请参阅注册配置文件。
- 完全托管的 Android 11+ 设备以公司拥有的设备模式注册工作配置文件。新模式进一步分离了设备上的个人和工作配置文件。此更改使组织能够更好地控制托管配置文件，并为用户提供其个人配置文件的更多隐私。有关更多信息，请参阅Android Enterprise和服务器属性。
- 您现在可以指定更多设置屏幕，以便在用户设置 iOS 或 macOS 设备时跳过。
  - iOS
    - **恢复完成：** 防止用户在设置过程中看到恢复是否完成。适用于 iOS 14.0 及更高版本。
    - **更新完成：** 防止用户在设置过程中看到软件更新是否完成。适用于 iOS 14.0 及更高版本。
  - macOS
    - **辅助功能：** 防止用户自动听到“旁白”。仅当设备连接到以太网时可用。适用于 macOS 11 及更高版本。
    - **生物识别：** 防止用户设置触控 ID 和面容 ID。适用于 macOS 10.12.4 及更高版本。
    - **原彩显示：** 防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：** 防止用户设置 Apple Pay。如果此设置已清除，则用户必须设置触控 ID 和 Apple ID。请确保已清除 **Apple ID** 和 **生物识别** 设置。适用于 macOS 10.12.4 及更高版本。
    - **屏幕使用时间：** 防止用户启用屏幕使用时间。适用于 macOS 10.15 及更高版本。

  有关配置设置选项的详细信息，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。此选项允许您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

在 **故障排除和支持 > 日志** 中查看日志时，您现在可以查看一个日志，其中显示从调试日志中筛选出的错误。有关详细信息，请参阅在 XenMobile 中查看日志文件。

服务器属性

- 您可以通过配置 `afw.allow.legacy.apps` 服务器属性来决定是否将旧版 Android 应用程序交付给 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 的替代方案。您可以使用端口 2197 从 `api.push.apple.com` 发送和接收 APNs 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。当属性 `enable.password.strength.validation` 设置为 `true` 时，您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 服务器名称不包含 `_XM_XenMobileGetway`，则 XenMobile Server 会选择列表中的第一个可用 VPN 虚拟服务器。

对 Citrix Launcher 的支持

XenMobile Server 支持在 Android Enterprise 设备上使用 Citrix Launcher。有关详细信息，请参阅启动器配置设备策略。

XenMobile Server 的颜色更新

XenMobile Server 符合 Citrix 品牌颜色更新。

XenMobile Server 10.13 中的新增功能

XenMobile Server 10.13(/zh-cn/xenmobile/server/downloads/product-documentation-xenmobile-server-10-13.pdf) (PDF 下载)

继续支持从 Citrix ADC 中弃用的经典策略

Citrix 最近宣布，从 Citrix ADC 12.0 build 56.20 开始，将弃用一些基于经典策略的功能。Citrix ADC 弃用通知对现有 XenMobile Server 与 Citrix Gateway 的集成没有影响。XenMobile Server 将继续支持经典策略，无需采取任何措施。

弃用公告

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

将端点升级到 iOS 14.5 之前

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问题：

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

升级本地 Citrix ADC 之前

将本地 Citrix ADC 升级到某些版本可能会导致单点登录错误。在浏览器中使用“**公司员工登录**”选项单点登录到 Citrix Files 或 ShareFile 域 URL 会导致错误。用户无法登录。

要解决此问题：如果您尚未在 Citrix Gateway 上从 ADC CLI 运行以下命令，请运行它以启用全局 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
- 受影响的 SSO 配置

完成变通办法后，用户可以使用 SSO 在浏览器中通过“公司员工登录”选项向 Citrix Files 或 ShareFile 域 URL 进行身份验证。

升级到 XenMobile 10.13（本地部署）之前

某些系统要求已更改。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 RAM 小于 8 GB，建议将 RAM 增加到至少 8 GB。
2. 在更新到最新版本的 XenMobile Server 10.13 之前，请将您的 Citrix License Server 更新到 11.16 或更高版本。

   最新版本的 XenMobile 需要 Citrix License Server 11.16（最低版本）。

   > **注意：**

> XenMobile 10.13 中的客户成功服务日期（以前称为 Subscription Advantage 日期）是 September 29, 2020。您的 Citrix 许可证上的客户成功服务日期必须晚于此日期。

> 您可以在 License Server 中查看许可证旁边的日期。如果将最新版本的 XenMobile 连接到较旧的 License Server 环境，则连接性检查将失败，并且您无法配置 License Server。

> 要续订许可证上的日期，请从 Citrix Portal 下载最新的许可证文件，然后将文件上传到许可服务器。请参阅客户成功服务。

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 Citrix Gateway 配置为 SSL 持久性，则必须在所有 XenMobile Server 节点上打开端口 80。
4. 建议：在安装 XenMobile 更新之前，请使用 VM 中的功能为系统创建快照。此外，请备份您的系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。

要升级

此版本中，XenMobile 支持 VMware ESXi 7.0。请确保在安装或升级 ESXi 7.0 之前升级到 10.13。

您可以直接从 XenMobile 10.12.x 或 10.11.x 升级到 XenMobile 10.13。要执行升级，请下载最新的可用二进制文件：转到 `<https://www.citrix.com/downloads>`。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击 **Download File**。

要上传升级，请使用 XenMobile 控制台中的 **Release Management** 页面。请参阅使用发布管理页面进行升级。

升级后

如果涉及出站连接的功能停止工作，并且您没有更改连接配置，请检查 **XenMobile Server 日志**中是否存在以下错误：“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' 与对等方提供的证书主题不匹配)。

- 证书验证错误意味着您必须在 XenMobile Server 上禁用主机名验证。
- 默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。
- 如果主机名验证导致部署中断，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 Mobile 生产力应用程序与 iOS 14 兼容，但目前不支持任何新的 iOS 14 功能。请使用 MDX Toolkit 20.8.5 或更高版本，或使用 MAM SDK 准备应用程序。
- **Android 11：** XenMobile Server 支持 Android 11。有关 Google 设备管理 API 弃用如何影响运行 Android 10+ 的设备的信息，请参阅从设备管理迁移到 Android Enterprise。另请参阅此Citrix博客。

在单个环境中配置多种设备和应用程序管理模式

您现在可以配置单个 XenMobile 站点以支持多种注册配置。注册配置文件（enrollment profiles）的作用已扩展，以包括设备和应用程序管理的注册设置。

注册配置文件支持单个 XenMobile 控制台中的多种用例和设备迁移路径。用例包括：

- 移动设备管理 (仅 MDM)
- MDM+移动应用程序管理 (MAM)
- 仅限 MAM
- 企业拥有的注册
- 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）

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

如果您不需要注册专用设备，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：

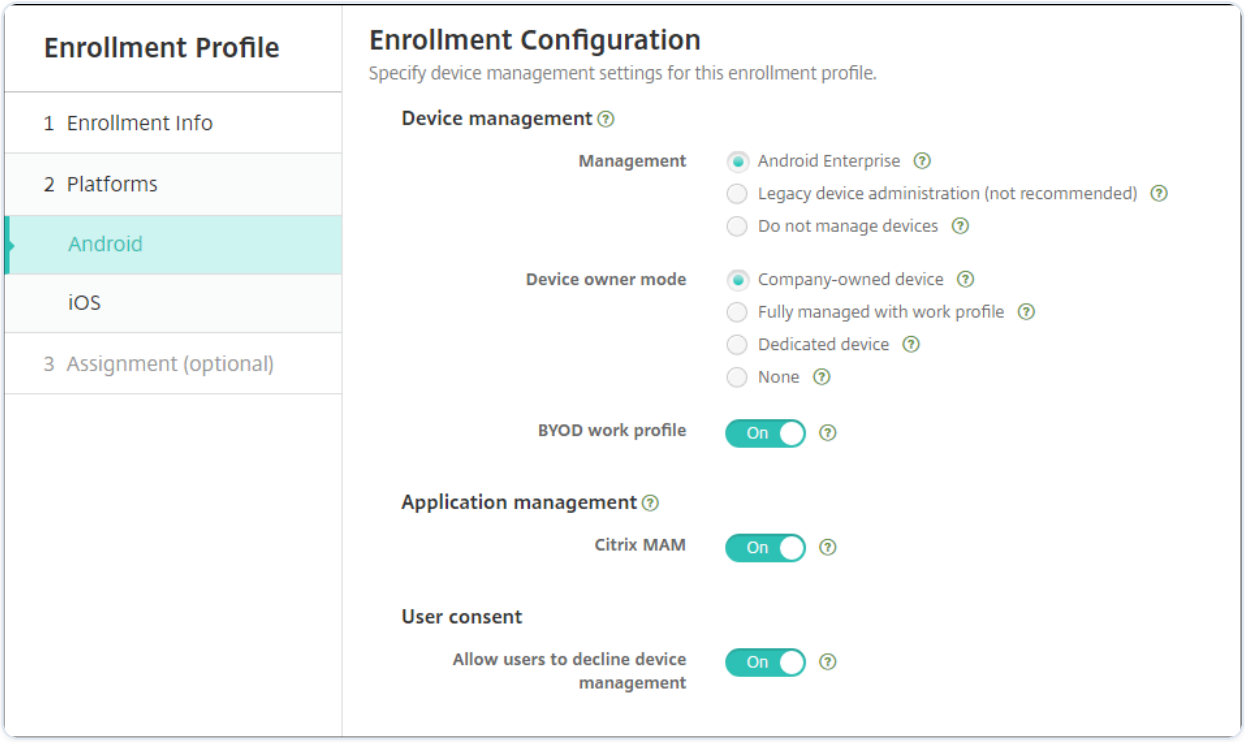
现有服务器属性	新管理模式
ENT 模式 (iOS)	借助 Citrix MAM 进行 Apple 设备注册
ENT 模式 (Android)	借助 Citrix MAM 的旧版设备管理员
企业模式 (Android Enterprise)	完全托管（以前称为 COPE）上的工作配置文件，借助 Citrix MAM

现有服务器属性	新管理模式
MAM 模式 (iOS 和 Android)	思杰移动应用管理
MDM 模式 (iOS)	Apple 设备注册
MDM 模式 (Android)	旧版设备管理员
移动设备管理模式 (安卓企业版)	完全托管设备上的工作资料

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) 模式到 Android Enterprise 的更轻松迁移。** 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资料或专用。请参阅 Android Enterprise。



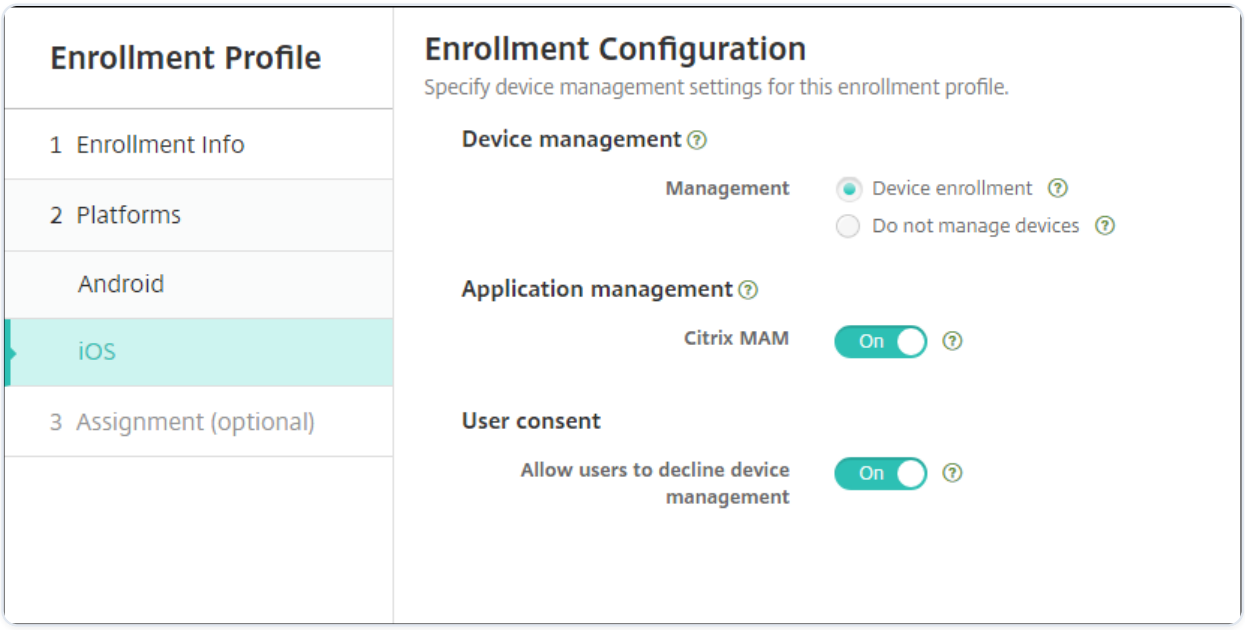
对于此升级，您当前的 XenMobile 服务器模式配置和 **设置 > Android Enterprise** 将映射到新的注册配置文件设置，如下所示。

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

* 如果需要注册，则**允许用户拒绝设备管理**为**关**。

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

- **更简单的 iOS 管理。** 对于 iOS 设备，设置包括选择将设备注册为托管或非托管。



对于此升级，您的先前配置将按如下方式映射到新的注册配置文件设置。

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

如果需要注册，则**允许用户拒绝设备管理**为**关**。

增强型注册配置文件存在以下限制：

- 增强型注册配置文件功能不适用于一次性 PIN 或双因素身份验证注册邀请。

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协议的支持将于 March 31, 2021 结束。Apple 建议您改用基于 HTTP/2 的 APNs 提供程序 API。XenMobile Server 现在支持基于 HTTP/2 的 API。有关详细信息，请参阅 `<https://developer.apple.com/>` 中的新闻更新“Apple 推送通知服务更新”。有关检查 APNs 连接的帮助，请参阅连接性检查。

以下版本的 XenMobile Server 默认启用对基于 HTTP/2 的 API 的支持：

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

如果您使用以下版本的 XenMobile Server，则必须添加服务器属性 **apple.apns.http2** 才能启用此支持：

- 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。

将基于设备证书的 IPsec VPN 与多个 iOS 设备结合使用

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，而是将此过程自动化。

1. 配置连接类型为 **Always on IKEv2** 的 iOS VPN 设备策略。
2. 选择“**基于设备身份的设备证书**”作为设备身份验证方法。

3. 选择要使用的“**设备身份类型**”。
4. 使用 REST API 批量导入设备证书。

有关配置 VPN 设备策略的详细信息，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 批量上传证书。

Apple 批量采购应用的自动更新

添加批量购买帐户（**设置 > iOS 设置**）时，现在可以为所有 iOS 应用程序启用自动更新。请参阅 Apple Volume Purchase 中的 **App 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：** 如果用户连续登录尝试失败次数达到最大值，则本地用户帐户将锁定 30 分钟。系统将拒绝所有后续身份验证尝试，直到锁定时间段到期。要在 XenMobile Server 控制台中解锁帐户，请转至**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

已为 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

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

工作配置文件模式或完全托管模式下 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**用于证书的应用程序**设置。您可以指定应用程序使用此策略中选择的凭据提供程序颁发的用户证书。应用程序在运行时会静默获得证书访问权限。要将证书用于所有应用程序，请将应用程序列表留空。请参阅 凭据设备策略。
- **静默从托管密钥库中删除证书或卸载所有非系统 CA 证书。** 请参阅 凭据设备策略。

- **阻止用户修改存储在托管密钥库中的凭据。** Android Enterprise 的限制设备策略现在包含**允许用户配置用户凭据**设置。默认情况下，该设置为**开**。请参阅 限制设备策略。

在托管配置中更轻松地使用证书别名

在**凭据**设备策略中使用新的**证书别名**设置与**托管配置**设备策略。这样做允许应用程序在 VPN 上进行身份验证，而无需用户操作。您无需在应用程序日志中查找凭据别名，而是创建凭据别名。通过在**托管配置**设备策略的**证书别名**字段中键入别名来创建别名。然后，在**凭据**设备策略的**证书别名**设置中键入相同的证书别名。请参阅托管配置策略和凭据设备策略。

控制 Android Enterprise 设备上的“使用一个锁”设置

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

显示 Android Enterprise 设备上不合规的应用程序和快捷方式

Android Enterprise 的密码设备策略有一个新设置：**在密码不合规时显示应用程序和快捷方式**。启用此设置可使应用程序和快捷方式在设备密码不再合规时保持可见。Citrix 建议您创建自动化操作，以便在密码不合规时将设备标记为不合规。请参阅密码设备策略。

禁用 Android Enterprise 工作配置文件设备或完全托管设备上的打印功能

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。

通过在自助服务终端策略中添加应用程序包名称来允许专用设备上的应用程序

您现在可以输入要在 Android Enterprise 平台上允许的包名称。请参阅Android Enterprise 设置。

管理 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屏。使用键盘锁管理设备策略来控制：

- 工作配置文件设备上的键盘锁管理。您可以指定用户在解锁设备键盘锁和工作挑战键盘锁之前可用的功能。例如，默认情况下，用户可以使用指纹解锁并在锁屏上查看未编辑的通知。您还可以使用键盘锁管理策略禁用运行 Android 9.0 及更高版本的设备的所有生物识别身份验证。
- 完全托管和专用设备上的键盘锁管理。您可以指定在解锁键盘锁屏幕之前可用的功能，例如信任代理和安全摄像头。或者，您可以选择禁用所有键盘锁功能。

请参阅键盘锁管理设备策略。

在 XenMobile 控制台中发布 Android Enterprise 企业应用

添加 Android Enterprise 私有应用时，您不再需要注册 Google Play 开发者帐户。XenMobile 控制台会打开一个托管的 Google Play 商店 UI，供您上传和发布 APK 文件。有关详细信息，请参阅添加企业应用。

在 XenMobile 控制台中发布 Android Enterprise Web 应用

您不再需要前往托管的 Google Play 或 Google 开发者门户来为 XenMobile 发布 Android Enterprise Web 应用。当您在 **Configure > Apps > Web link** 中单击 **Upload** 时，会打开一个托管的 Google Play 商店 UI，供您上传和保存文件。应用审批和发布大约需要 10 分钟。有关详细信息，请参阅添加 Web 链接。

使用 XenMobile Server REST API 批量将证书上传到 iOS 设备

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

1. 配置连接类型为 **Always on IKEv2** 的 iOS VPN 设备策略。
2. 选择 **Device Certificate Based on Device Identity** 作为设备身份验证方法。
3. 选择要使用的 **Device identity type**。
4. 使用 REST API 批量导入设备证书。

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

刷新加密密钥

Refresh encryption keys 选项已添加到 XenMobile CLI 的高级设置中。您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。

支持 ESXi 7.0

此版本中，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

以下服务器属性现已可用：

- **允许 iOS App Store 链接的主机名：** 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，您可以配置允许的主机名列表。
- **本地用户帐户锁定限制：** 配置本地用户在帐户被锁定之前可以尝试登录的次数。
- **本地用户帐户锁定时间：** 配置本地用户在多次登录尝试失败后被锁定的时长。

- **启用文件上传大小限制：** 启用对上传文件最大大小的限制。
- **允许的最大文件上传大小：** 设置上传文件的最大大小。

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

在**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。查看列表后，您可以通过命令行选择删除所有这些文件。有关命令行界面工具的更多信息，请参阅命令行界面选项。

XenMobile Server 10.12 中的新增功能

XenMobile Server 10.12 (PDF 下载)

弃用公告

有关正在逐步淘汰的 Citrix XenMobile 功能的提前通知，请参阅弃用。

为即将到来的更改准备您的 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 设备管理模式的新注册。
  - **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 设备将不再工作。
- MDX 加密：
  - **August 1, 2020:** Citrix 开始强制将 Citrix 移动生产力应用程序和第三方 MDX 应用程序从 MDX 加密迁移到平台加密。
  - **September 1, 2020:** MDX 加密达到生命周期终止。

对于已注册旧版 DA 的设备

- 如果您不使用 MDX 加密，则无需采取任何措施。
- 如果您使用 MDX 加密，请在 July 31, 2020 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。此要求包括仅限 MAM 模式的 Android 设备。请参阅从设备管理迁移到 Android Enterprise。

对于从 7 月 31 日起已注册到 Android Enterprise 的设备

- 如果您使用 Android Enterprise 平台发布了应用程序，则加密已通过 Android Enterprise 处理。无需执行任何操作。
- 如果您使用旧版 Android 平台发布了应用程序，请在 July 31, 2020 之前使用 Android Enterprise 重新发布这些应用程序。

在升级到 XenMobile 10.12（本地部署）之前

某些系统要求已更改。有关信息，请参阅 系统要求和兼容性 和 XenMobile 兼容性。

1. 在更新到 XenMobile Server 10.12 的最新版本之前，请将您的 Citrix License Server 更新到 11.16 或更高版本。

   最新版本的 XenMobile 需要 Citrix License Server 11.16（最低版本）。

   > **注意：**
   >
   > 如果您想在预览版中使用自己的许可证，请注意 XenMobile 10.12 中的客户成功服务日期（以前称为 Subscription Advantage 日期）是 January 20, 2020。您的 Citrix 许可证上的客户成功服务日期必须晚于此日期。
   >
   > 您可以在 License Server 中许可证旁边查看该日期。如果将最新版本的 XenMobile® 连接到较旧的 License Server 环境，则连接性检查将失败，并且您无法配置 License Server。
   >
   > 要续订许可证上的日期，请从 Citrix Portal 下载最新的许可证文件，然后将该文件上传到许可服务器。有关详细信息，请参阅 客户成功服务。

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 Citrix Gateway 配置为 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 RAM 小于 4 GB，请将 RAM 增加到至少 4 GB。请记住，生产环境的建议最低 RAM 为 8 GB。
4. 建议：在安装 XenMobile 更新之前，请使用 VM 中的功能为系统创建快照。此外，请备份您的系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。

要升级

您可以直接从 XenMobile 10.11.x 或 10.10.x 升级到 XenMobile 10.12。要执行升级，请下载最新的可用二进制文件：转至 `<https://www.citrix.com/downloads>`。导航到 **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击 **Download File**。

要上传升级，请使用 XenMobile 控制台中的 **Release Management** 页面。有关详细信息，请参阅使用 Release Management 页面进行升级。

升级后

升级到 XenMobile 10.12（本地部署）后：

如果涉及出站连接的功能停止工作，并且您未更改连接配置，请检查 **XenMobile Server 日志**中是否存在以下错误：“Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer”。

证书验证错误表示您需要在 XenMobile Server 上禁用主机名验证。默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。如果主机名验证导致您的部署中断，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 的额外支持

XenMobile Server 支持升级到 iOS 13 的设备。升级对用户的影响如下：

- 在注册期间，会出现一些新的 iOS 设置助理选项屏幕。Apple 在 iOS 13 中添加了一个新的 iOS 设置助理选项屏幕。新选项包含在此版本的 **Settings > Apple Device Enrollment Program (DEP)** 页面中。您可以配置 XenMobile Server 以跳过这些屏幕。这些页面会显示给 iOS 13 设备上的用户。
- 某些在早期 iOS 版本中适用于受监督或不受监督设备的限制设备策略设置，仅在 iOS 13+ 的受监督设备上可用。当前的 XenMobile Server 控制台工具提示尚未指出这些设置仅适用于 iOS 13+ 的受监督设备。
    - 允许硬件控制：
        - FaceTime
        - 安装应用程序
    - 允许应用程序：
        - iTunes 商店

    - Safari 浏览器
    - Safari > 自动填充
  - 网络 - 允许 iCloud 操作：
    - iCloud 文档和数据
  - 仅限受监督设置 - 允许：
    - Game Center > 添加朋友
    - Game Center > 多人游戏
  - 媒体内容 - 允许：
    - 露骨音乐、播客和 iTunes U 材料

这些限制的适用方式如下：

- 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，则上述限制适用于非受监督和受监督设备。
- 如果非受监督的 iOS 13+ 设备在 XenMobile Server 中注册，则上述限制仅适用于受监督设备。
- 如果受监督的 iOS 13+ 设备在 XenMobile Server 中注册，则上述限制仅适用于受监督设备。

Apple 大宗采购计划迁移到 Apple Business Manager (ABM) 和 Apple School Manager (ASM)

使用 Apple 大宗采购计划 (VPP) 的公司和机构需要在 December 1, 2019 之前迁移到 Apple Business Manager 或 Apple School Manager 中的“应用和图书”。

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

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

要在 XenMobile 上更新您的 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“**批量采购计划**”配置页面。
3. 确保您的 ABM 或 ASM 帐户具有与您之前的 VPP 帐户相同的应用程序配置。
4. 在 ABM 或 ASM 门户中，下载更新的令牌。

5. 在 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采购帐户。

   b. 编辑您的 ABM 或 ASM 凭据。请勿更改后缀。

   c. 单击两次“**保存**”。

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 支持带工作资料的 Android Enterprise 完全托管设备，这些设备以前称为 COPE（公司拥有、个人启用）设备。这些设备是一种 Android Enterprise 完全托管设备，也具有工作资料。您可以对设备和工作资料应用单独的策略设置。对于此版本：

- 您可以使用以下设备策略对设备和工作资料应用单独的设置：凭据、密码和限制。
- 您可以将位置设备策略的位置模式设置应用于 COPE 设备本身，但不能应用于 COPE 设备的工作资料。位置设备策略中的其他设置不适用于 COPE 设备。
- 您可以将“锁定”安全操作分别应用于设备或工作资料。

设备策略

对于带工作资料的 Android Enterprise 完全托管设备（COPE 设备），某些设备策略可以对整个设备和工作资料应用单独的设置。在 XenMobile Server 控制台中，某些设备策略允许您应用单独的设置。您可以使用其他设备策略仅对整个设备或仅对带工作资料的完全托管设备的工作资料应用设置。

安全操作

对于带工作资料的 Android Enterprise 完全托管设备（COPE 设备），您可以应用：

- 将“锁定”安全操作分别应用于设备或工作资料。
- 将所有其他安全操作应用于设备。

注册配置文件控制 Android 设备的注册选项

如果为您的 XenMobile 部署启用了 Android Enterprise，注册配置文件现在将控制 Android 设备的注册方式。注册配置文件确定 Android 设备是以默认的 Android Enterprise 模式（完全托管或工作资料）还是以旧版（设备管理员）模式注册。

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

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

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

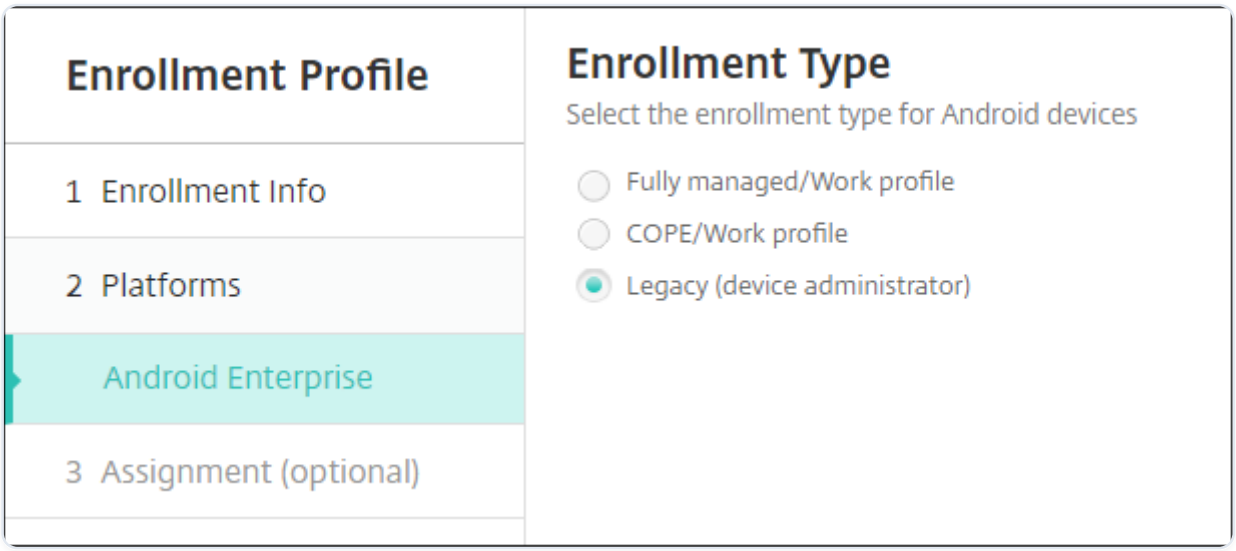
此更改意味着，如果您的 XenMobile 部署启用了 Android Enterprise，则所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。

为应对此更改，XenMobile 现在允许您创建注册配置文件，以控制 Android 设备的注册方式。

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

要为旧版设备创建注册配置文件，请执行以下操作：

1. 在 XenMobile 控制台中，转至**配置 > 注册配置文件**。
2. 要添加注册配置文件，请单击**添加**。在“注册信息”页面中，键入注册配置文件的名称。
3. 单击**下一步**或在**平台**下选择 **Android Enterprise**。“注册配置”页面随即显示。
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）**。“交付组分配”屏幕随即显示。



5. 选择包含注册专用设备的管理员的交付组。然后单击**保存**。

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

有关 Endpoint Management 支持过渡到 Android Enterprise 的更多信息，请参阅博客：Android Enterprise as default for Citrix Endpoint Management service。

简化 Android Enterprise 的应用程序管理

您不再需要前往托管 Google Play 或 Google Developer 门户来批准或发布 XenMobile Server 的应用程序。因此，应用程序的批准和发布只需大约 10 分钟，而不是数小时。

在 XenMobile Server 控制台中批准公共应用商店的 Android Enterprise 应用程序。 您现在无需离开 XenMobile Server 控制台即可批准托管 Google Play 商店应用程序。在搜索字段中输入应用程序名称后，托管 Google Play 商店 UI 将打开，其中包含批准和保存应用程序的说明。然后，您的应用程序将填充到结果中，允许您配置其详细信息。请参阅添加公共应用商店应用程序。

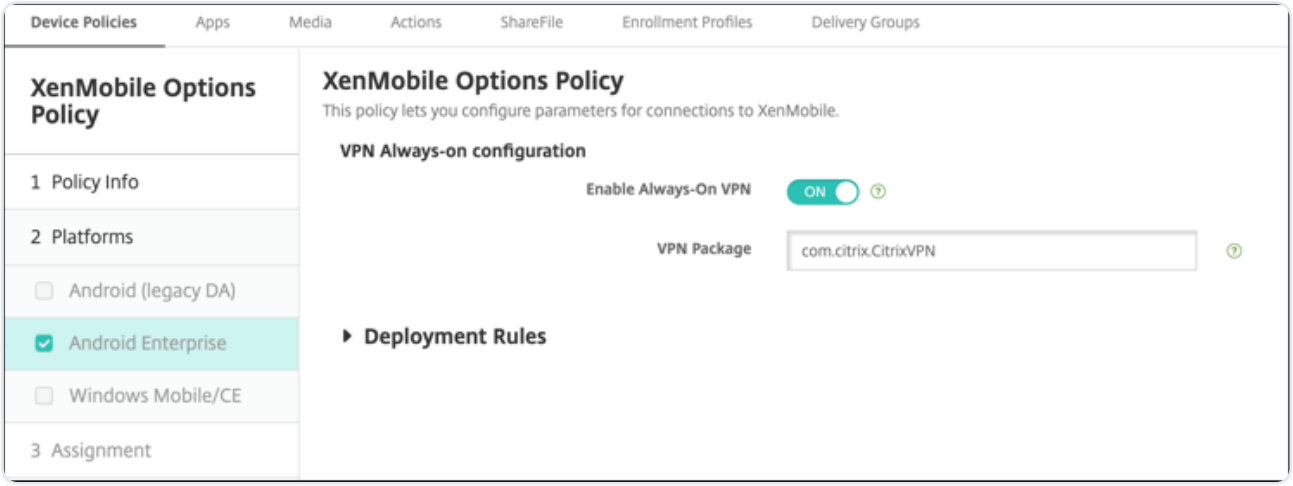
为 Android Enterprise 添加 MDX 应用程序。 XenMobile Server 控制台现在支持 Android Enterprise 作为 MDX 应用程序部署平台。请参阅添加 MDX 应用程序。

在 XenMobile Server 控制台中批准 Android Enterprise 的 MDX 应用程序。 您现在无需离开 XenMobile Server 控制台即可批准 Android Enterprise 的托管 Google Play 商店应用程序。上传 MDX 文件后，托管 Google Play 商店 UI 将打开，其中包含批准和保存应用程序的说明。请参阅添加 MDX 应用程序。

支持 Android Enterprise 的始终开启 VPN

XenMobile Server 选项设备策略现在允许您为 Android Enterprise 启用 Always-On VPN。

为 Android Enterprise 配置 VPN 配置文件时，在**默认 VPN 配置文件**中，键入 VPN 配置文件的名称。当用户在 Citrix SSO 应用程序的用户界面中点击连接开关而不是点击特定配置文件时，XenMobile 将使用此配置文件。如果此字段留空，则主配置文件用于连接。如果只配置了一个配置文件，则将其标记为默认配置文件。对于始终开启的 VPN，此字段必须设置为用于建立始终开启的 VPN 的 VPN 配置文件的名称。



为 Android Enterprise 应用程序配置产品轨道

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

强制 macOS 用户重置密码

当 macOS 设备收到包含密码策略的配置配置文件时，用户必须提供符合策略设置的密码。您现在可以强制用户在下次进行身份验证时重置密码。在 macOS（10.13 及更高版本）的密码设备策略中，启用新设置**强制重置密码**。有关该策略的更多信息，请参阅密码设备策略。

XenMobile Server 10.11 中的新增功能

XenMobile Server 10.11 (PDF 下载)

Apple 批量采购计划迁移到 Apple Business Manager (ABM) 和 Apple School Manager (ASM)

使用 Apple 批量采购计划 (VPP) 的公司和机构必须在 December 1, 2019 之前迁移到 Apple Business Manager 或 Apple School Manager 中的“应用和图书”。

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

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

要在 XenMobile® 上更新您的批量采购（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“**批量采购**”。此时将显示“**批量采购**”配置页面。
3. 确保您的 ABM 或 ASM 帐户具有与您以前的 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. 使用针对该位置的更新令牌信息编辑现有批量采购帐户。
   b. 编辑您的 ABM 或 ASM 凭据。不要更改后缀。
   c. 单击“**保存**”两次。

对 iOS 13 的额外支持

> **重要提示：**

> 为设备升级到 iOS 12+ 做准备：iOS 的 VPN 设备策略中的 Citrix VPN 连接类型不支持 iOS 12+。请删除您的 VPN 设备策略，并创建使用 Citrix SSO 连接类型的 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。您的新 VPN 设备策略配置将在用户注册期间在 XenMobile Server 10.11 中生效。

> XenMobile Server 支持升级到 iOS 13 的设备。此次升级对用户的影响如下：

- 在注册期间，会出现一些新的 iOS 设置助理选项屏幕。Apple 在 iOS 13 中添加了新的 iOS 设置助理选项屏幕。此版本中，新选项未包含在“**设置 > Apple 设备注册计划 (DEP)**”页面中。因此，您无法配置 XenMobile Server 以跳过这些屏幕。这些页面将显示给 iOS 13 设备上的用户。
- 以前 iOS 版本中在受监督或不受监督设备上可用的一些“限制”设备策略设置，现在仅适用于 iOS 13+ 的受监督设备。当前的 XenMobile Server 控制台工具提示尚未指明这些设置仅适用于 iOS 13+ 的受监督设备。
  - 允许硬件控制：
    - FaceTime
    - 安装应用程序
  - 允许应用程序：
    - iTunes 商店

    - 萨法里
    - Safari > 自动填充
  - 网络 - 允许 iCloud 操作：
    - iCloud 文档和数据
  - 仅限受监管设置 - 允许：
    - Game Center > 添加朋友
    - Game Center > 多人游戏
  - 媒体内容 - 允许：
    - 露骨音乐、播客和 iTunes U 材料

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，则上述限制适用于非受监管和受监管设备。
- 如果非受监管的 iOS 13+ 设备在 XenMobile Server 中注册，则上述限制仅适用于受监管设备。
- 如果受监管的 iOS 13+ 设备在 XenMobile Server 中注册，则上述限制仅适用于受监管设备。

iOS 13 和 macOS 15 中受信任证书的要求

Apple 对 TLS 服务器证书有新的要求。请验证所有证书是否符合新的 Apple 要求。请参阅 Apple 发布内容 `<https://support.apple.com/zh-cn/HT210176>`。有关管理证书的帮助，请参阅 在 XenMobile 中上载证书。

从 GCM 升级到 FCM

自 April 10, 2018 起，Google 弃用了 Google Cloud Messaging (GCM)。Google 于 May 29, 2019 移除了 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 建议立即升级到 Firebase Cloud Messaging (FCM)，以开始利用 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>`。

要继续支持向 Android 设备推送通知：如果您将 GCM 与 XenMobile Server 结合使用，请迁移到 FCM。然后，使用 Firebase Cloud Messaging 控制台中提供的新 FCM 密钥更新 XenMobile Server。

以下步骤反映了使用受信任证书时的注册工作流程。

升级步骤：

1. 按照 Google 提供的信息从 GCM 升级到 FCM。
2. 在 Firebase Cloud Messaging 控制台中，复制新的 FCM 密钥。下一步需要用到它。
3. 在 XenMobile Server 控制台中，转到 **Settings > Firebase Cloud Messaging** 并配置您的设置。

设备在下次与 XenMobile Server 签入并执行策略刷新时会切换到 FCM。要强制 Secure Hub 刷新策略：在 Secure Hub 中，转到 **Preferences > Device Information** 并点击 **Refresh Policy**。 有关配置 FCM 的详细信息，请参阅 Firebase Cloud Messaging。

升级到 XenMobile 10.11（本地部署）之前

某些系统要求已更改。有关信息，请参阅 System requirements and compatibility 和 XenMobile compatibility。

1. 在更新到最新版本的 XenMobile Server 10.11 之前，请将您的 Citrix License Server 更新到 11.15 或更高版本。

   最新版本的 XenMobile 需要 Citrix License Server 11.15（最低版本）。

   > **注意：**
   >
   > 如果您想为预览版使用自己的许可证，请注意 XenMobile 10.11 中的客户成功服务日期（以前称为 Subscription Advantage 日期）是 April 9, 2019。您的 Citrix 许可证上的客户成功服务日期必须晚于此日期。

> 您可以在许可证服务器中许可证旁边查看日期。如果将最新版本的 XenMobile 连接到较旧的许可证服务器环境，则连接性检查将失败，并且您无法配置许可证服务器。

> 要更新许可证上的日期，请从 Citrix Portal 下载最新的许可证文件，然后将文件上传到许可服务器。有关详细信息，请参阅客户成功服务。

2. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序有以下要求。如果 Citrix Gateway 配置为 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 RAM 小于 4 GB，请将 RAM 增加到至少 4 GB。请记住，生产环境的建议最小 RAM 为 8 GB。
4. 建议：在安装 XenMobile 更新之前，请使用 VM 中的功能为系统创建快照。此外，请备份系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。

要升级

您可以从 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 (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击**下载文件**。

要上传升级，请使用 XenMobile 控制台中的**版本管理**页面。有关详细信息，请参阅使用版本管理页面升级。

升级后

升级到 XenMobile 10.11（本地部署）后：

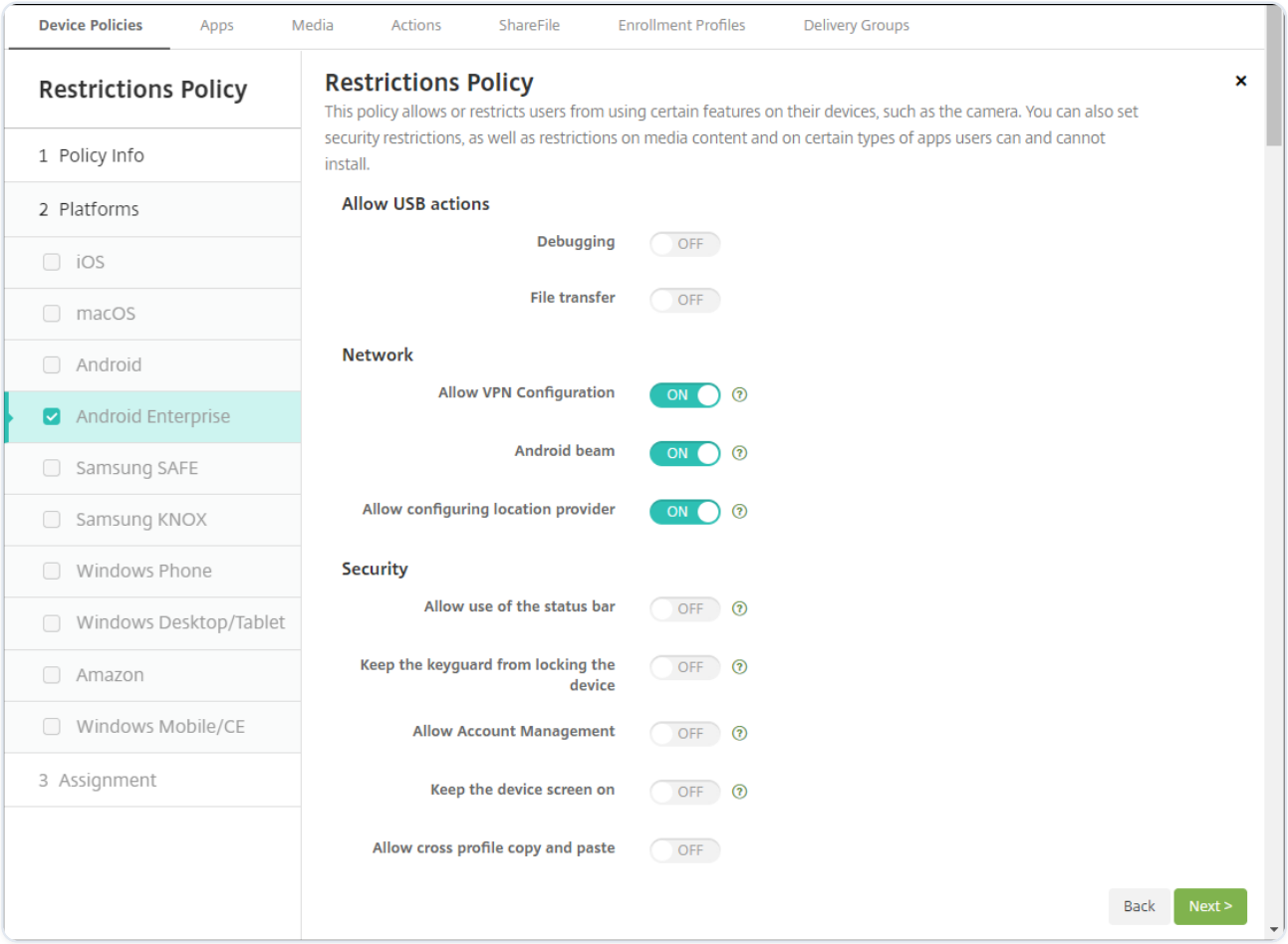
如果涉及出站连接的功能停止工作，并且您没有更改连接配置，请检查 XenMobile Server 日志中是否存在以下错误：“无法连接到 VPP 服务器：主机名 '192.0.2.0' 与对等方提供的证书主题不匹配”。

证书验证错误表示您需要在 XenMobile Server 上禁用主机名验证。默认情况下，除 Microsoft PKI 服务器外，出站连接上都启用了主机名验证。如果主机名验证导致部署中断，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 设备的新增和更新设备策略设置

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 已合并为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：

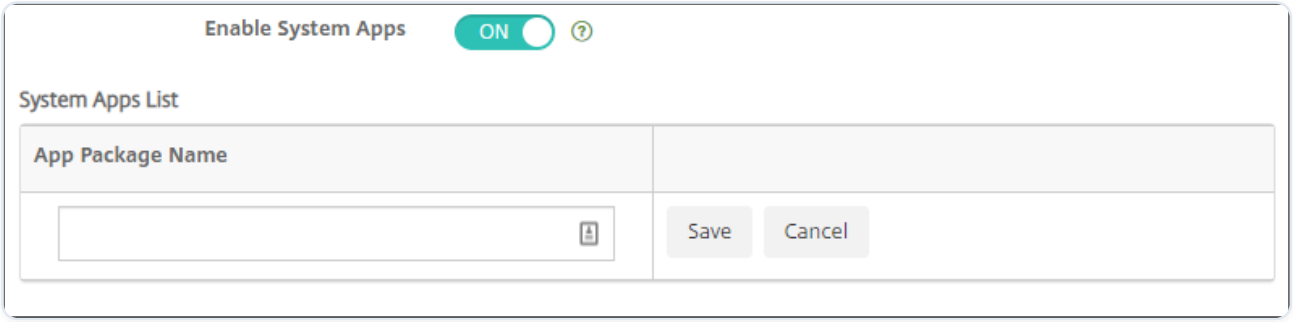
- 操作系统更新设备策略。 包括三星企业 FOTA 更新的设置。
- 密码设备策略。
- **三星 MDM 许可证密钥设备策略。** 配置 Knox 许可证密钥。
- 限制设备策略设置。



适用于 Android Enterprise 的应用程序清单设备策略。 您现在可以收集托管设备上 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 商店中的所有 Google Play 应用程序。 **访问托管 Google Play 商店中的所有应用程序**服务器属性使公共 Google Play 商店中的所有应用程序都可以从托管 Google Play 商店访问。将此属性设置为 **true** 允许所有 Android Enterprise 用户访问公共 Google Play 商店应用程序。管理员随后可以使用 限制设备策略 来控制对这些应用程序的访问。

在 Android Enterprise 设备上启用系统应用程序。 要允许用户在 Android Enterprise 工作配置文件模式或完全托管模式下运行预安装的系统应用程序，请配置 限制设备策略。该配置授予用户访问默认设备应用程序（例如相机、图库等）的权限。要限制对特定应用程序的访问，请使用 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 现在支持专用设备的管理，这些设备以前称为企业自有单用途 (COSU) 设备。

专用 Android Enterprise 设备是完全托管的设备，专门用于满足单一用例。您将这些设备限制为执行此用例所需的一个应用程序或一小组应用程序。您还可以阻止用户启用其他应用程序或在设备上执行其他操作。

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

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

锁定并重置 Android Enterprise 密码

XenMobile 现在支持 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。

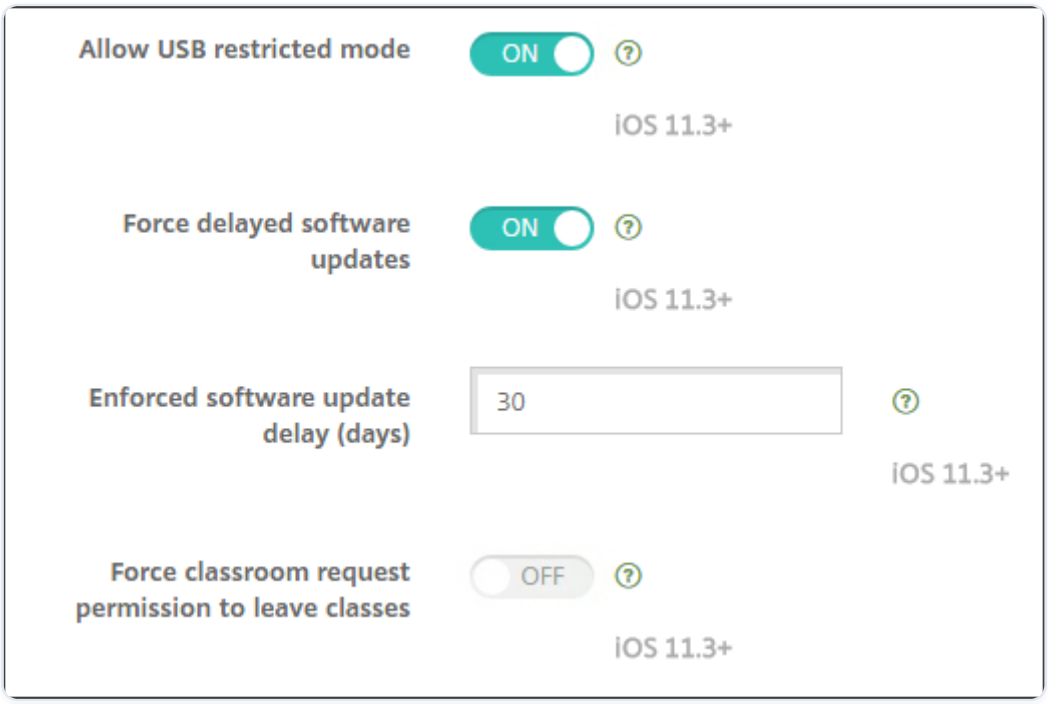
- 发送的密码会锁定工作配置文件。设备不会被锁定。
- 如果未发送密码或发送的密码不符合密码要求：
  - 并且工作配置文件上未设置密码，则设备将被锁定。
  - 并且工作配置文件上已设置密码。工作配置文件被锁定，但设备未被锁定。

有关锁定和重置密码安全操作的详细信息，请参阅安全操作。

适用于 iOS 或 macOS 的新限制设备策略设置

- **非托管应用读取托管联系人：** 可选。仅当**非托管应用中的托管应用文档**被禁用时可用。如果启用此策略，非托管应用可以读取托管帐户联系人中的数据。默认值为**关闭**。从 iOS 12 开始可用。
- **托管应用写入非托管联系人：** 可选。如果启用，允许托管应用将联系人写入非托管帐户的联系人。如果**非托管应用中的托管应用文档**被启用，此限制无效。默认值为**关闭**。从 iOS 12 开始可用。

- **密码自动填充：** 可选。如果禁用，用户无法使用“自动填充密码”或“自动强密码”功能。默认值为**开启**。从 iOS 12 和 macOS 10.14 开始可用。
- **密码邻近请求：** 可选。如果禁用，用户的设备不会从附近的设备请求密码。默认值为**开启**。从 iOS 12 和 macOS 10.14 开始可用。
- **密码共享：** 可选。如果禁用，用户无法使用 AirDrop 密码功能共享其密码。默认值为**开启**。从 iOS 12 和 macOS 10.14 开始可用。
- **强制自动日期和时间：** 受监管。如果启用，用户无法禁用选项**通用 > 日期与时间 > 自动设置**。默认值为**关闭**。从 iOS 12 开始可用。
- **允许 USB 受限模式：** 仅适用于受监管设备。如果设置为“关闭”，设备在锁定时始终可以连接到 USB 配件。默认值为**开启**。从 iOS 11.3 开始可用。
- **强制延迟软件更新：** 仅适用于受监管设备。如果设置为**开启**，则会延迟用户看到软件更新的时间。启用此限制后，用户在软件更新发布日期后的指定天数内将不会看到软件更新。默认值为**关闭**。从 iOS 11.3 和 macOS 10.13.4 开始可用。
- **强制软件更新延迟（天）：** 仅适用于受监管设备。此限制允许管理员设置在设备上延迟软件更新的时间。最大值为 90 天，默认值为**30**。从 iOS 11.3 和 macOS 10.13.4 开始可用。
- **强制课堂请求离开课堂权限：** 仅适用于受监管的设备。如果设置为 **开**，则在 Classroom 中注册了非托管课程的学生在尝试离开课程时必须向老师请求许可。默认设置为 **关**。适用于 iOS 11.3 及更高版本。



请参阅 限制设备策略。

适用于 iOS 或 macOS 的 Exchange 设备策略更新

自 iOS 12 起，增加了 S/MIME Exchange 签名和加密设置。 Exchange 设备策略现在包含用于配置 S/MIME 签名和加密的设置。

对于 S/MIME 签名：

- **签名身份凭据：** 选择要使用的签名凭据。
- **S/MIME 签名用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中打开和关闭 S/MIME 签名。默认设置为 **关**。
- **S/MIME 签名证书 UUID 用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中选择要使用的签名凭据。默认设置为 **关**。

对于 S/MIME 加密：

- **加密身份凭据：** 选择要使用的加密凭据。
- **启用每条消息 S/MIME 开关：** 当设置为 **开** 时，会向用户显示一个选项，用于打开或关闭他们撰写的每条消息的 S/MIME 加密。默认设置为 **关**。
- **S/MIME 默认加密用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中选择 S/MIME 是否默认开启。默认设置为 **关**。
- **S/MIME 加密证书 UUID 用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中打开和关闭 S/MIME 加密身份和加密。默认设置为 **关**。

自 iOS 12 起的 Exchange OAuth 设置。 您现在可以配置与 Exchange 的连接以使用 OAuth 进行身份验证。

macOS 10.14 中的 Exchange OAuth 设置。 您现在可以将 Exchange 连接配置为使用 OAuth 进行身份验证。对于使用 OAuth 的身份验证，您可以为不使用 AutoDiscovery 的设置指定登录 URL。

请参阅 Exchange 设备策略。

iOS 邮件设备策略更新

iOS 12 中更多 S/MIME Exchange 签名和加密设置。 邮件设备策略包含更多用于配置 S/MIME 签名和加密的设置。

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“**开启**”。设置为“**开启**”时，将显示以下字段。

- **S/MIME 签名用户可覆盖：** 如果设置为“**开启**”，用户可以在其设备设置中开启和关闭 S/MIME 签名。默认值为“**关闭**”。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“**开启**”，用户可以在其设备设置中选择要使用的签名凭据。默认值为“**关闭**”。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“**关闭**”。设置为“**开启**”时，将显示以下字段。
  - **启用每条消息 S/MIME 开关：** 如果设置为“**开启**”，则会向用户显示一个选项，用于在他们撰写的每条消息中开启或关闭 S/MIME 加密。默认值为“**关闭**”。
  - **S/MIME 默认加密用户可覆盖：** 如果设置为“**开启**”，用户可以在其设备设置中选择是否默认开启 S/MIME。默认值为“**关闭**”。此选项适用于 iOS 12.0 及更高版本。
  - **S/MIME 加密证书 UUID 用户可覆盖：** 如果设置为“**开启**”，用户可以在其设备设置中开启和关闭 S/MIME 加密身份和加密。默认值为“**关闭**”。此选项适用于 iOS 12.0 及更高版本。

请参阅 邮件设备策略。

iOS 应用程序通知设备策略更新

以下应用程序通知设置从 iOS 12 开始可用。

- **在 CarPlay 中显示**：如果设置为“**开**”，通知将在 Apple CarPlay 中显示。默认设置为“**开**”。
- **启用紧急警报**：如果设置为“**开**”，应用程序可以将通知标记为紧急通知，该通知将忽略“勿扰”和铃声设置。默认设置为“**关**”。

请参阅应用程序通知设备策略

支持与 Apple 教育版配合使用的共享 iPad

XenMobile 与 Apple 教育版功能的集成现在支持共享 iPad。教室中的多名学生可以共享一台 iPad，用于由一名或多名教师教授的不同科目。

您或教师可以注册共享 iPad，然后将设备策略、应用程序和媒体部署到设备。之后，学生提供其托管 Apple ID 凭据以登录共享 iPad。如果您之前已向学生部署了教育配置策略，他们不再以“其他用户”身份登录以共享设备。

共享 iPad 的先决条件：

- 任何 iPad Pro、iPad 第 5 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

- 受监管

有关详细信息，请参阅配置共享 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”现已拆分为两个权限：“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。

第三方通知

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

XenMobile 第三方通知

弃用

本文中的公告旨在提前通知您即将淘汰的 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 会监控客户的使用情况和反馈，以确定何时撤回这些功能。公告可能会在后续版本中发生变化，并且可能不包括所有已弃用的功能或功能。有关产品生命周期支持的详细信息，请参阅产品生命周期支持策略一文。

弃用和移除

以下列表显示了已弃用或已移除的 XenMobile® Server 功能。

*已弃用*的项目不会立即移除。Citrix® 将继续支持已弃用的项目，直到在未来版本中将其移除。

*已移除*的项目要么已被移除，要么在 XenMobile Server 中不再受支持。

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 (/zh-cn/mobile-productivity-apps/eol-deprecated-apps.html) 中的“EOL 和已弃用应用程序”。

项目	描述	弃用公告日期	移除日期	替代方案
基于文件的许可	基于文件的许可在 April 15, 2026 之后将不再起作用。	2025 年 10 月	2026 年 4 月	License Activation Service (LAS) 是用于 Citrix 产品套件中产品激活的下一代技术。使用基于文

项目	描述	弃用公告日期	移除日期	替代方案
				件的许可的客户需要在 April 15, 2026 之前升级到兼容版本并完成此技术过渡。April 15, 2026 之后，LAS 将是激活和许可 Citrix 本地组件的唯一方式。
XenMobile 邮件管理器 (XMM)/ XenMobile NetScaler 连接器 (XNC)	弃用对 XMM 和 XNC 的支持。	2025 年 6 月	2025 年 9 月	无替代方案。
虚拟机管理程序	弃用对 Citrix XenServer 8.2 及更早版本、VMware ESXi 6.x 及更早版本以及 Hyper-V 2016 的支持。	2025 年 3 月	2025 年 5 月	将系统更新到以下受支持版本之一：Citrix Hypervisor 8.2 CU1 及更高版本、VMware (ESXi 7.0、ESXi 8.0) 或 Hyper-V (Windows Server 2019 或 Windows Server 2022)。
与 ShareFile 集成	如果 ShareFile（现为 Progress）停止支持，则将弃用与 ShareFile 的集成。	2025 年 1 月		无替代方案
斑马设备自定义 XML	弃用对斑马设备上自定义 XML 的支持	2022 年 1 月	目标：2022 年 6 月	使用 Android Enterprise 托管配置。

项目	描述	弃用公告日期	移除日期	替代方案
Windows 信息保护 (WIP)	弃用对 Windows 信息保护的支持，具体请参阅 Microsoft 此处的公告。	2022 年 8 月	目标：2022 年 10 月	无替代方案
XenMobile 分析器	弃用对 XenMobile Analyzer 工具的支持。	2022 年 7 月	目标: March 31, 2023	无替代方案
PKI 身份：通用、赛门铁克 PKI、DigiCert 和 Entrust 适配器	弃用对通用、DigiCert 管理和 Entrust 适配器 PKI 实体的支持。	2021 年 6 月	2022 年 1 月	无替代方案
注册邀请设置	弃用对使用设备 IMEI、序列号和 UDID 创建注册邀请的支持。	2022 年 1 月	2022 年 5 月	创建注册邀请时，请在 XenMobile 控制台的 **管理 > 注册邀请** 下配置可用设置。
运营商短信网关	弃用对 Nexmo 短信网关通知的支持	2022 年 1 月	2022 年 4 月	使用 SMTP 服务器通知
移动服务提供商 (MSP)	弃用对 MSP 接口的支持，以查询 Blackberry 和其他 Exchange ActiveSync 设备并执行操作	2022 年 1 月	2022 年 4 月	无替代方案
三星自助服务终端模式	弃用对基于设备管理员 (DA) 模式的旧版三星自	2022 年 1 月	2022 年 3 月	使用 Android Enterprise (AE) 自助服务终端模式。

项目	描述	弃用公告日期	移除日期	替代方案
	助服务终端模式的支持。			
允许自动连接到 Wi-Fi 感知热点限制（适用于 Windows 设备）	删除对适用于 Windows 10 设备的“允许自动连接到 Wi-Fi 感知热点”限制的支持。Windows 10 不再支持此功能。有关信息，请参阅 Microsoft 文档。	2021 年 10 月	2022 年 2 月	无替代方案
三星 SAFE/三星 Knox 平台	弃用对 SAFE 和 Knox 平台的支持。	2022 年 1 月	2022 年 6 月	通过托管应用配置策略使用 Knox 服务插件，以使用 Android Enterprise 设置 Knox 策略。
高安全性注册模式	弃用对使用**高安全性**注册安全模式生成注册邀请的支持。	2021 年 7 月	2022 年 2 月	有关支持的注册安全模式列表，请参阅注册设备。
RBAC 角色 - 共享设备注册器和 COSU 设备注册器	弃用对共享设备注册器和 COSU 设备注册器的预定义基于角色的访问控制设置的支持	2021 年 7 月	2021 年 12 月	通过 支持的注册方法 配置 iOS 设备。通过 注册配置文件 配置 Android COSU（专用）设备。
Knox 移动注册（旧版 DA）	已弃用对所有 Android 版本上旧版设备管理员模式中的 Knox	2021 年 5 月	2021 年 6 月	使用 KME 注册 Android Enterprise 模式。Android 9、10、11 支持

项目	描述	弃用公告日期	移除日期	替代方案
	移动注册 (KME) 的支持。			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	已弃用对 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的 Android 7.x 和 iOS 12.x 版本的支持。	2021 年 4 月	2021 年 6 月	至少使用每个主要操作系统平台的当前版本和以前版本。旧设备仍保持注册状态。但是，Citrix 不会测试或支持旧设备。
派生凭据	已弃用对派生凭据和 Citrix Derived Credentials Manager 应用程序的支持。	2021 年 3 月	2021 年 12 月	请参阅 iOS，了解 iOS 支持的身份验证类型列表。
Internet Explorer 11 浏览器	弃用对将 Internet Explorer 与 XenMobile Server 控制台结合使用的支持。	2021 年 1 月	2021 年 1 月	请使用以下 Web 浏览器的最新版本：Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari
适用于 Android 的 RSA 软令牌支持	弃用对将 RSA 软令牌直接导入 Secure Hub for Android 的支持。	2021 年 1 月	2021 年 2 月	您可以将 RSA 软令牌导入 Google Play 中提供的 RSA Secure ID 应用程序。然后，您可以使用该令牌进行 Citrix

项目	描述	弃用公告日期	移除日期	替代方案
				Gateway 身份验证。
安卓 - 索尼	弃用对 Android Sony 设备和 Sony 特定策略的支持。	2021 年 1 月	2022 年 2 月	使用 Android 企业版
安卓 - HTC	已弃用对 Android HTC 设备和 HTC 特定策略的支持。	2021 年 1 月	2022 年 2 月	使用 安卓企业版
安卓 - 亚马逊	已弃用对 Android Amazon 设备和 Amazon 特定策略的支持。	2021 年 1 月	2022 年 2 月	使用安卓企业版
XenMobile 控制板的第三方组件	我们将弃用用作 XenMobile 控制板一部分的第三方组件。	2020 年 12 月	2021 年 1 月	要继续使用仪表板，请升级到 XenMobile 10.12 或更高版本。
针对 Android Enterprise 设备上的旧版设备管理员模式发布的应用程序	我们不再向注册到 Android Enterprise 的设备交付针对旧版 DA 平台发布的应用程序。	2020 年 10 月	2020 年 11 月	对于 Android Enterprise 设备，请发布适用于 Android Enterprise 平台的应用程序。要继续向处于 DA 模式的设备发布旧版 DA 应用程序，请为这些应用程序创建单独的交付组。
APNs 出站端口	Apple 对 APNs 旧版二进制协议的支持将于 March 31, 2021	2020 年 10 月	2021 年 3 月	请改用端口 443 或 2197。请参阅 打开

项目	描述	弃用公告日期	移除日期	替代方案
	结束。Apple 建议您改用基于 HTTP/2 的 APNs 提供程序 API。作为此更改的一部分，我们将弃用对端口 2195 和 2196 的支持，这些端口用于向 `*.push.apple.com` 发送 APNs 通知。			XenMobile 端口以管理设备。
Samsung SEAMS 容器	弃用了对 Samsung SEAMS 容器的支持。	2020 年 6 月	2020 年 8 月	针对 Android Enterprise 使用 Samsung Knox Service Plug-in (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自签名 SSL 证书的支持。	2020 年 5 月		将现有自签名证书替换为来自知名证书颁发机构 (CA) 的受信任 SSL 证书。
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、	2020 年 5 月	2021 年 6 月	在 XenMobile 控制台中为凭据提供程序创建 CSR 时（**设置 > 凭据提供程序 > 证书签名请求**），请选择更强的密码。

项目	描述	弃用公告日期	移除日期	替代方案
	RIPEMD160withRSA、RIPEMD128withRSA、RIPEMD256withRSA。			
数据库服务器	已弃用对 Microsoft SQL Server 2014 及更早版本的支持。	2021 年 10 月	2022 年 8 月	将系统更新到以下受支持版本之一：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支持的服务器列表。
虚拟机管理程序	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。	2020 年 5 月	2020 年 8 月	将系统更新到以下受支持的版本之一：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)。

项目	描述	弃用公告日期	移除日期	替代方案
Citrix 启动器	弃用对旧版 Citrix Launcher 应用程序的支持。	2020 年 5 月	2020 年 8 月（从应用商店中移除）	将预配设备用作信息亭（专用设备）和适用于 Android Enterprise 的 Citrix Launcher。有关详细信息，请参阅Citrix Launcher 替代方案。
适用于 Android 6.x 和 iOS 11.x 的 Citrix 移动应用程序和 Workspace 应用程序	弃用对 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的 Android 6.x 和 iOS 11.x 版本的支持。	2020 年 4 月	2020 年 6 月	至少使用每个主要操作系统平台的当前版本和先前版本。
MDX 工具包 和 MDX 服务	弃用了对 MDX Toolkit 和 MDX Service 的支持，转而支持移动应用管理 (MAM) SDK。在过渡期内，您可以同时使用 MDX 封装的应用程序和 MAM SDK 开发的应用程序。	2020 年 3 月	目标：2023 年 7 月	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 设备的增强身份验证。	2020 年 3 月	2021 年 9 月	无替代方案

项目	描述	弃用公告日期	移除日期	替代方案
MDX：微型 VPN（全隧道模式）	弃用了适用于 iOS 和 Android 设备的完整虚拟专用网络 (VPN) 隧道。	2020 年 3 月	2021 年 9 月	使用 MAM SDK Web SSO 模式或使用 Citrix SSO 连接类型创建按应用程序 VPN 策略。
MDX：PAC 文件支持	弃用对适用于 iOS 和 Android 设备的完整 VPN 隧道部署的代理自动配置 (PAC) 文件的支持。	2020 年 3 月	2021 年 9 月	使用 Citrix Gateway 通过代理服务器连接以访问内部网络。
MDX 共享设备支持	弃用对 MDX 应用程序的共享设备支持。	2020 年 3 月	2021 年 9 月	对于 Android Enterprise，请使用 MDM 的共享设备支持。对于 iOS，请使用 Apple School Manager 或 GroundControl 。
适用于 Android 10 的新设备管理员注册	弃用对 Android 10 设备上旧版设备管理员模式的新注册或重新注册的支持。已注册的设备将继续工作。	2020 年 2 月	2020 年 9 月	将新的 Android 10+ 设备注册到 Android Enterprise。
适用于 Android 10 设备的旧版设备管理员模式	Google 已弃用部分设备管理员 API。从升级到以 Android API 级别 29 为目标的 Citrix Secure Hub™ 开始，Citrix 不支持已	2020 年 2 月	2020 年 11 月	将 Android 10 设备迁移到 Android Enterprise。

项目	描述	弃用公告日期	移除日期	替代方案
	注册到设备管理员模式的 Android 10 设备。			
MDX 加密	弃用 MDX 加密以及 XenMobile 控制台中的 MDX 加密功能。	2019 年 10 月	2020 年 9 月	使用我们的加密管理功能启用 iOS 或 Android 平台加密，并增加合规性检查。请确保您已在 2020 年 7 月之前测试并计划了从 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 设备仅支持使用字符限制创建的密码。如果您之前将“**所需字符**”设置为“**无限制**”，此更新会将该值更改为“**仅数字**”。	2019 年 2 月	2019 年 4 月	此更改不影响当前用户登录体验。
远程支持	已弃用用于群集本地 XenMobile Server 部署的远程支持客户端。	2019 年 1 月	2020 年 8 月	无替代方案
适用于 iOS 的 Secure Hub 网络扩展	已弃用网络扩展框架，该框架允许您从 Secure Hub 20.3.0 版本开始为 iOS	2018 年 10 月	2020 年 3 月	无替代方案

项目	描述	弃用公告日期	移除日期	替代方案
	设备自定义网络功能。			
TLS 版本 1.0 和 1.1	为提高 XenMobile 的安全性，Citrix 现在阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的任何通信。由于其安全性减弱，PCI 委员会正在弃用 TLS 1.0 和 TLS 1.1。	2018 年 6 月	2019 年 3 月	升级到 TLS 1.2。
视窗移动/CE	弃用了对 Windows Mobile/CE 设备的支持。	2018 年 4 月	2020 年 9 月	使用 Windows 10 桌面版和笔记本电脑。
安卓达阵	DigiCert 停止支持 Android TouchDown。Citrix 将从 Exchange 设备策略中删除 Android TouchDown 平台页面。	2018 年 7 月	2021	建议：使用 Citrix Secure Mail。
完整 VPN 隧道 - Android	弃用了对 Android 完整 VPN 隧道的支持。	2020 年 3 月	2021 年 9 月	MAM SDK Web SSO 模式。
允许 VPN 模式切换 - Android	已弃用对 Android 允许 VPN 模式切换的支持。	2020 年 3 月	2021 年 9 月	无替代方案

项目	描述	弃用公告日期	移除日期	替代方案
入站文档交换 - Android	已弃用对 Android 入站文档交换的支持。	2020 年 3 月	2021 年 9 月	无替代方案

已修复的问题

XenMobile 10.16 包含以下已修复的问题：

- 升级到 XenMobile Server 10.16 版本后，XenMobile Server 已停止向 Syslog 服务器发送日志。
- 配置代理后，使用 HTTP v1 API 的 Firebase Cloud Messaging 无法正常运行。
- 在以 **MAM-only** 模式注册的 iOS 设备上，您无法从 Secure Hub 商店安装企业或 MDX 应用程序。
- 在 Android Enterprise 设备上编辑或部署 **托管配置策略** 时，会显示错误。
- 配置应用程序的跟踪 ID 后，您无法在 XenMobile® Server 控制台上看到预期的应用程序预览版本。相反，您看到的是应用程序的生产版本。
- 在 XenMobile Server 上，当预配配置文件设备策略处于待定状态时，您无法从 Secure Hub 商店安装 MDX 封装的应用程序。
- MDM 配置文件续订后，ABM 共享 iPad 会变为非托管状态。
- 当使用 APK Signature Scheme v2 及更高版本算法时，您无法在 Android 平台上配置企业应用程序。
- 您无法使用 device/filter API 导出设备。
- 如果您使用 NetScaler® 中的 nFactor 身份验证策略同时注册 Android 或 iOS 设备（MAM 和 MDM），则设备将仅注册 MDM。
- 当您在 XenMobile Server 10.14 或更高版本上导出 Citrix Gateway 身份验证的配置脚本时，脚本会被截断且无法工作。
- 在 XenMobile Server 上，您无法重新编辑描述中包含 **\b** 的同步 VPP 应用程序。
- 在 XenMobile Server 10.15 及更高版本上，联机证书状态协议 (OCSP) 不响应请求。
- 在 XenMobile Server 上，您无法注册运行 Windows 11 的设备。
- 在 Android 设备上，当您从旧版 MDX Toolkit 切换到 MAM SDK 时，Secure Mail 应用程序会从 Secure Hub Store 中移除。
- 在 XenMobile Server 控制台中，您无法看到快速安全响应 (RSR) 版本。
- 您无法从 **托管 Google Play 帐户** 下载应用程序。
- 升级到 XenMobile Server 10.16 后，使用“受限应用程序使用”的现有 iOS 限制设备策略无法部署到 iOS 设备上。

- 当您使用 ABM 或 ASM 配置时，无法在 iOS 共享设备上部署 Webclip 设备策略。
- 您无法在 **Android Enterprise** > **托管 Google Play 商店应用程序** 的 **配置** > **应用程序** 页面上看到 **组织应用程序** 按钮。
- 在为 **Android Enterprise** 平台配置 Wi-Fi 策略时，您无法在 **CA 证书** 下拉菜单中看到任何值。仅显示 **选择证书** 选项。
- 有关版本 10.15.0 滚动修补程序版本中的已修复问题，请参阅：
  - XenMobile Server 10.15 滚动修补程序 8 的发行说明
  - XenMobile Server 10.15 滚动修补程序 7 的发行说明
  - XenMobile Server 10.15 滚动修补程序 6 的发行说明
  - XenMobile Server 10.15 滚动修补程序 5 的发行说明
  - XenMobile Server 10.15 滚动修补程序 4 的发行说明
  - XenMobile Server 10.15 滚动修补程序 3 的发行说明

相关信息

XenMobile 支持知识中心

已知问题

XenMobile 10.16 中没有已知问题。

- 有关移动生产力应用程序的已知问题，请参阅 Secure Hub、Secure Mail 和 Secure Web。
- 有关最新版本 10.15.0 滚动修补程序中的已知问题，请参阅 XenMobile Server 10.15 滚动修补程序 7 的发行说明。

相关信息

XenMobile 支持知识中心

体系结构

您的组织对设备和应用程序管理的要求决定了 XenMobile 体系结构中的 XenMobile® 组件。XenMobile 的组件是模块化的，并且相互构建。例如，您的部署包括 Citrix Gateway：

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

部署 XenMobile 组件：您可以通过以下方式部署 XenMobile，以使用户能够连接到内部网络中的资源：

- 连接到内部网络。如果您的用户是远程用户，他们可以通过 Citrix Gateway 使用 VPN 或微型 VPN 连接。该连接提供对内部网络中应用程序和桌面的访问。
- 设备注册。用户可以在 XenMobile 中注册移动设备，以便您可以在 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。用户可以通过 Secure Hub 从 XenMobile 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。用户可以使用 Citrix Receiver™ 或 Web 浏览器连接，以从 StoreFront 或 Web Interface 访问基于 Windows 的应用程序和虚拟桌面。

为了实现本地 XenMobile Server 的任何这些功能，Citrix 建议按以下顺序部署 XenMobile 组件：

- Citrix Gateway。您可以使用快速配置向导在 Citrix Gateway 中配置设置，以启用与 XenMobile、StoreFront™ 或 Web Interface 的通信。在使用 Citrix Gateway 中的快速配置向导之前，您必须安装以下组件之一来设置通信：XenMobile、StoreFront 或 Web Interface。
- XenMobile。安装 XenMobile 后，您可以在 XenMobile 控制台中配置策略和设置，以允许用户注册其移动设备。您还可以配置移动、Web 和 SaaS 应用程序。移动应用程序可以包括来自 Apple App Store 或 Google Play 的应用程序。用户还可以连接到您使用 MDX Toolkit 封装并上传到控制台的移动应用程序。
- MAM SDK 或 MDX Toolkit。MDX 封装技术计划于 2023 年 7 月达到生命周期终止 (EOL)。要继续管理您的企业应用程序，您必须集成 MAM SDK。

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

- StoreFront（可选）。您可以通过与 Receiver 的连接，从 StoreFront 提供对基于 Windows 的应用程序和虚拟桌面的访问。
- Citrix Files（可选）。如果部署 Citrix Files，可以通过 XenMobile 启用企业目录集成，XenMobile 充当安全断言标记语言 (SAML) 身份提供商。有关为 ShareFile 配置身份提供商的更多信息，请参阅 ShareFile 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 部署的参考架构。

在生产环境中，Citrix 建议以群集配置部署 XenMobile 解决方案，以实现可伸缩性和服务器冗余。此外，使用 Citrix ADC SSL 卸载功能可以进一步减轻 XenMobile 服务器的负载并提高吞吐量。有关通过在 Citrix ADC 上配置两个负载平衡虚拟 IP 地址来设置 XenMobile 群集的更多信息，请参阅群集。

有关为灾难恢复部署配置 XenMobile 的更多信息，请参阅部署手册灾难恢复文章。该文章包含一个架构图。

以下各节介绍 XenMobile 部署的不同参考架构。有关参考架构图，请参阅 XenMobile 部署手册文章本地部署的参考架构和架构。有关完整的端口列表，请参阅端口要求（本地）和端口要求（云）。

移动设备管理 (MDM) 模式

> **重要提示：**
>
> 如果配置 MDM 模式，然后更改为 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。有关更多信息，请参阅从 XenMobile MDM 版升级到企业版。

> XenMobile MDM 版提供移动设备管理。有关平台支持，请参阅支持的设备操作系统。如果您计划仅使用 XenMobile 的 MDM 功能，则以 MDM 模式部署 XenMobile。例如，如果您想执行以下操作。

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

在推荐模型中，XenMobile 服务器位于 DMZ 中，前面带有一个可选的 Citrix ADC，这为 XenMobile 提供了更多保护。

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。如果您计划仅使用 XenMobile 的 MAM 功能而无需设备注册 MDM，则以 MAM 模式部署 XenMobile。例如，如果您想执行以下操作。

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

这些设备无法进行 MDM 注册。

在此部署模型中，XenMobile Server 位于 Citrix Gateway 之后，这为 XenMobile 提供了更多保护。

MDM+MAM 模式

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

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

在推荐的部署模型中，XenMobile Server 部署在 DMZ 中，Citrix Gateway 位于其前面，这为 XenMobile 提供了更多保护。

内部网络中的 XenMobile： 另一种部署选项是将本地 XenMobile Server 部署在内部网络中，而不是 DMZ 中。如果您的安全策略要求只有网络设备可以放置在 DMZ 中，则使用此部署。在此部署中，XenMobile Server 不在 DMZ 中。因此，无需在内部防火墙上打开端口以允许从 DMZ 访问 SQL Server 和 PKI 服务器。

系统要求和兼容性

注意：

本文介绍了 XenMobile Server 10.16 的系统要求和兼容性。有关 Endpoint Management 的系统要求，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 10.16，您需要满足以下最低系统要求：

- 以下之一：
  - Citrix Hypervisor 8.2 CU1 和 8.4，有关详细信息，请参阅 XenServer。Citrix Hypervisor 8.2 CU1 及更高版本不再支持半虚拟化 (PV) VM，请在升级 XenServer 之前迁移到硬件虚拟化模式 (HVM)，有关详细信息，请参阅在 Citrix Hypervisor 8.2 CU1 及更高版本上使用 HVM 映像。有关 XenServer 升级的更多信息，请参阅XenServer 升级。
  - VMware（支持的版本：ESXi 6.0、ESXi 6.5.0 Update 3 或 ESXi 6.7 Update 2 patch 10、ESXi 7.0 Update 3g、ESXi 8.0 Update 2）；有关详细信息，请参阅 ESXi 6.7 解决方法 和 VMware
  - Hyper-V (支持版本：Windows Server 2016 和 Windows Server 2019)；有关详细信息，请参阅 Hyper-V

- 适用于 Exchange ActiveSync 10.1.10 的 Endpoint Management 连接器或适用于 Exchange ActiveSync 8.5.3.19 的 Citrix Gateway 连接器
- 双核处理器
- 四个虚拟 CPU
- 生产环境需要 8 GB RAM；概念验证和测试环境需要 4 GB RAM
- 50 GB 磁盘空间
- Citrix 许可证服务器 11.16.

  在升级 XenMobile® Server 之前，请更新您的许可服务器。

ESXi 6.7 变通办法

要使 ESXi 6.7 正常工作，您必须执行以下变通办法。

1. 使用 VMware 提供的 OVF 工具，提取从 citrix.com 下载的 OVA 文件。从 VMware 页面获取 OVF 工具(https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491)。
2. 在提取的三个文件中，将 .vmdk 文件上传到您的数据存储。
3. 创建新的虚拟机。
   a. 命名虚拟机并选择 **ESX/ESXi 4.x 虚拟机** 作为兼容性选项。
   b. 对于客户机操作系统系列，选择 **Linux**。
   c. 对于客户机操作系统版本，选择 **Other 2.6.x Linux (64-bit)**。
   d. 对于数据存储，选择 **Default**。
   e. 在自定义期间，移除默认硬盘、USB 控制器和 CD/DVD 驱动器。
   f. 在“网络”下，将适配器类型选择为 **VMXNET3**。
   g. 在 ESXi 上，如果您的磁盘是本地磁盘，请选择 **SCSI Controller** 和 **LSI Logic Parallel**。如果您使用的是共享磁盘，请选择 **VMware Paravirtual**。
   h. 单击“下一步”完成 VM 创建。
4. 导航到您的数据存储，并复制您之前上传的 .vmdk 文件。将其复制到您为 XenMobile 创建的 VM 目录中。
5. 从 ESXi Web 界面中，选择 VM 并编辑设置。
6. 单击“**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. 启动您的 VM。

Citrix Gateway 系统要求

要在 XenMobile 10.16 中运行 Citrix Gateway，您需要满足以下最低系统要求。

- Citrix Gateway（本地部署）。支持的版本：12.1 或更高版本
- 您还必须能够与 Active Directory 通信，这需要一个服务帐户。您只需要查询和读取访问权限。

XenMobile 10.16 数据库要求

XenMobile 需要以下数据库之一：

- 微软 SQL Server

  XenMobile 支持运行以下受支持版本之一的 Microsoft SQL Server 数据库。有关 Microsoft SQL Server 数据库及其硬件要求的更多信息，请参阅 Microsoft 文档。

  - 微软 SQL Server 2016 SP3
  - 微软 SQL Server 2017 CU 31
  - 微软 SQL Server 2019 CU 25
  - 微软 SQL Server 2022 CU 12

  您的 Microsoft SQL Server 数据库要求还取决于部署规模。有关部署规模的 Microsoft SQL Server 数据库要求的更多信息，请参阅可伸缩性。

  XenMobile 支持 SQL 基本可用性组（Always On 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（仅限测试环境）。XenMobile 包含 PostgreSQL。您可以在测试环境中本地或远程使用它。不支持数据库迁移。您无法将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 的远程 PostgreSQL 9.5.1 和 9.5.11，但存在以下限制：不建议用于生产环境。支持多达 300 台设备。对于超过 300 台设备，请使用本地 SQL Server。不支持群集。

SQL Server 服务帐户要求

确保与 XenMobile 配合使用的 SQL Server 服务帐户具有 `DBcreator` 角色权限。记录您在 XenMobile Server 安装期间指定的 SQL Server 帐户密码。如果在 XenMobile Server 恢复期间需要克隆 XenMobile 数据库，则需要该密码。

使用透明数据加密 (TDE) 保护您的 SQL Server 数据库。不要允许外部访问 SQL Server 端口，如本地部署参考体系结构 中所示。

有关 SQL Server 服务帐户的更多信息，请参阅 Microsoft 文档站点上的以下页面。这些链接指向 SQL Server 2014 的信息。如果您使用的是其他版本，请从“**其他版本**”列表中选择您的服务器版本：

- 配置 Windows 服务帐户和权限
- 服务器级角色

虚拟应用和桌面兼容性

- 虚拟应用和桌面 7.15 LTSR CU3
- 虚拟应用和桌面 7.1811
- 虚拟应用和桌面 7 1906
- 虚拟应用和桌面 7 1909
- 虚拟应用和桌面 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

- 用于 Exchange ActiveSync 的 Endpoint Management 连接器 10.1.10
  - 未测试旧版本
- 用于 Exchange ActiveSync 的 Citrix Gateway 连接器 8.5.3.19

- 未测试旧版本

XenMobile® 兼容性

> **注意：**

> 本文涵盖 XenMobile Server 兼容性。有关使用 Endpoint Management 测试的组件，请参阅 Endpoint Management 兼容性。

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

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

  MDX Toolkit 计划于 2023 年 7 月终止生命周期 (EOL)。要继续管理您的企业应用程序，您必须集成 MAM SDK。

本文总结了您可以集成的受支持 XenMobile 组件的版本。

兼容性和升级路径

Secure Hub、MDX Toolkit 和移动生产力应用程序的最新版本与当前和以前版本的 XenMobile Server 兼容。

移动生产力应用程序的最新版本需要最新版本的 Secure Hub。应用程序的两个以前版本与最新 Secure Hub 兼容。有关详细信息，请参阅 Citrix 产品矩阵。

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

XenMobile Server（本地部署）

- Citrix 支持从 XenMobile Server 的最后两个版本进行升级。
- XenMobile Server 的最新版本：XenMobile Server 10.16
- 升级来源：
  - XenMobile 服务器 10.15.x
  - XenMobile 服务器 10.14.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需要最新版本的 Secure Hub。应用程序的两个先前版本与最新版本的 Secure Hub 兼容。

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

MAM SDK

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

MDX 工具包

MDX 包装技术计划于 2023 年 7 月达到生命周期结束 (EOL)。要继续管理您的企业应用程序，您必须集成 MAM SDK。

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

浏览器支持

XenMobile Server 控制台需要以下受支持的 Web 浏览器之一：

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

支持的设备操作系统

> **注意：**

> 本文介绍了 XenMobile Server 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 并非在所有平台上都支持所有功能。

> **注意：**
>
> XenMobile Server 支持 Windows x86 和 ARM 类型设备的设备管理。
>
> 本文中支持的设备平台信息也适用于 XenMobile connector for Exchange ActiveSync 和 Citrix Gateway connector™ for Exchange ActiveSync。

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

> **注意：**
>
> Citrix® 至少支持每个主要操作系统平台的当前版本和先前版本。Endpoint Management 较新版本并非所有功能都可在较旧的平台版本上运行。
>
> 有关弃用公告，请参阅弃用。

操作系统支持列表

Citrix XenMobile 支持以下操作系统：

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

  对于 Android 10 或更高版本，请参阅Android 注意事项。

- **苹果移动操作系统：**13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  XenMobile 和 Citrix 移动应用程序兼容 iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x 和 iOS 27.x，但目前不支持所有新的 iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x 和 iOS 27.x 功能。要为 iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x 和 iOS 27.x 封装内部企业应用程序，请使用 MDX Toolkit 21.8.5 或更高版本，或者使用 MAM SDK 准备应用程序。

- **iPadOS 平板操作系统：**13.x, 14.x, 15.x, 16.x, 17.x, 18.x,26.x, 27.x

  XenMobile 和 Citrix 移动应用程序兼容 iPadOS 14.x、iPadOS 15.x、iPadOS 16.x、iPadOS 17.x、iPadOS 18.x、iPadOS 26.x 和 iPadOS 27.x，但目前不支持所有新的 iPadOS 14.x、iPadOS 15.x、iPadOS 16.x、iPadOS 17.x、iPadOS 18.x、iPadOS 26.x 和 iPadOS 27.x 功能。

- **macOS 操作系统版本：** 11.x, 12.x, 13.x, 14.x, 15.x

XenMobile 和 Citrix 移动应用程序兼容 macOS 11、macOS 12、macOS 13、macOS 14 和 macOS 15，但目前不支持 macOS 11、macOS 12、macOS 13、macOS 14 和 macOS 15 的所有新功能。

- **Windows 桌面和平板电脑：**（仅限 MDM）。Windows 10 和 Windows 11

Android 注意事项

> **重要提示：**
>
> 不再支持设备管理模式。有关信息，请参阅从设备管理迁移到 Android Enterprise。

- Citrix 建议您避免在旧版设备管理模式下注册 Android 设备。Google 已弃用设备管理 API，这会影响运行 Android 10 或更高版本的设备。在旧版设备管理模式下注册 Android 设备会失败。Citrix 不支持在设备管理模式下注册 Android 11 设备。
- Citrix 建议为 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 更改不影响以仅 MAM 模式注册的设备。

升级前：

- 确保您的服务器基础结构符合安全证书要求，即证书的 subjectAltName (SAN) 扩展中包含匹配的主机名。
- 为了验证主机名，服务器必须提供具有匹配 SAN 的证书。Citrix 仅在证书具有与主机名匹配的 SAN 时才信任它们。

端口要求

为了使设备和应用程序能够与 XenMobile® 通信，您需要在防火墙中打开特定端口。下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

打开以下端口，以允许用户连接从 Citrix Secure Hub™、Citrix Receiver 和 Citrix Gateway 插件经由 Citrix Gateway 到以下组件：

- XenMobile
- StoreFront™

- Citrix 虚拟应用和桌面™
- 用于 Exchange ActiveSync 的 Citrix Gateway 连接器™
- 其他内部网络资源，例如内部网网站

要启用从 Citrix ADC 到 Launch Darkly 的流量，您可以使用此支持知识中心文章中提到的 IP 地址。

有关 Citrix Gateway 的更多信息，请参阅 Citrix Gateway 文档。该文档包含有关 Citrix ADC IP (NSIP)、虚拟服务器 IP (VIP) 和子网 IP (SNIP) 地址的信息。

TCP 端口	描述	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。	思杰网关、思杰移动	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。如果用户使用 Citrix Gateway 插件登录，通常会发生这种情况。	思杰网关	内网网站
80 或 8080；443	用于枚举、票证和身份验证的 XML 和安全票证颁发机构 (STA) 端口。Citrix 建议使用端口 443。	StoreFront 和 Web Interface XML 网络流量；Citrix Gateway STA	虚拟应用或桌面
123 (TCP 和 UDP)	用于网络时间协议 (NTP) 服务。	思杰网关；易安移动	NTP 服务器
389	用于不安全的 LDAP 连接	思杰网关；易安移动	LDAP 身份验证服务器或 Microsoft Active Directory
443	用于 Citrix Receiver™ 或 Receiver for Web 连接到 StoreFront，以访问和管理 Virtual	互联网	Citrix 网关

TCP 端口	描述	源	目标
	Apps and Desktops 中的应用程序。		
443	用于连接 XenMobile 以交付 Web、移动和 SaaS 应用程序。	互联网	思杰网关
443	用于设备与 XenMobile Server 的通用通信。	XenMobile	XenMobile
443	用于移动设备连接到 XenMobile 进行注册。	互联网	XenMobile
443	用于 XenMobile 连接到 Citrix Gateway 连接器以进行 Exchange ActiveSync。	XenMobile	Citrix Gateway 连接器，用于 Exchange ActiveSync
443	用于从 Citrix Gateway connector for Exchange ActiveSync 到 XenMobile 的连接。	Citrix Gateway 用于 Exchange ActiveSync 的连接器	XenMobile
443	用于在没有证书身份验证的部署中回调 URL。	XenMobile	思杰网关
514	用于 XenMobile 与 syslog 服务器之间的连接。	XenMobile	Syslog 服务器
636	用于安全的 LDAP 连接。	思杰网关；XenMobile	LDAP 身份验证服务器或 Active Directory
1494	用于内部网络中基于 Windows 的应用程序的 ICA® 连接。Citrix	思杰网关	虚拟应用或桌面

TCP 端口	描述	源	目标
	建议保持此端口打开。		
1812	用于 RADIUS 连接。	思杰网关	RADIUS 身份验证服务器
2598	用于通过会话可靠性连接到内部网络中基于 Windows 的应用程序。Citrix 建议保持此端口打开。	思杰网关	虚拟应用或桌面
3268	用于 Microsoft 全局编录不安全的 LDAP 连接。	思杰网关；思杰移动	LDAP 身份验证服务器或 Active Directory
3269	用于 Microsoft 全局编录安全 LDAP 连接。	思杰网关；XenMobile	LDAP 身份验证服务器或 Active Directory
9080	用于 Citrix ADC 与 Citrix Gateway connector for Exchange ActiveSync 之间的 HTTP 流量。	思杰 ADC	思杰网关用于 Exchange ActiveSync 的连接器
30001	用于 HTTPS 服务初始暂存的管理 API	内部 LAN	XenMobile 服务器
9443	用于 Citrix ADC 与 Citrix Gateway connector for Exchange ActiveSync 之间的 HTTPS 流量。	思杰 ADC	Citrix Gateway 的 Exchange ActiveSync 连接器
45000; 80	在集群中部署时，用于两个 XenMobile VM 之间的通信。端	XenMobile	XenMobile

TCP 端口	描述	源	目标
	口 80 用于节点间通信和 SSL 卸载。		
8443	用于注册、XenMobile Store 和移动应用管理 (MAM)。	XenMobile; Citrix Gateway; 设备; 互联网	XenMobile
4443	管理员通过浏览器访问 XenMobile 控制台时使用。也用于从一个节点下载所有 XenMobile 集群节点的日志和支持包。	访问点（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 trap 警报。源是 XenMobile，目标是 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 在您的网络中进行通信。

TCP 端口	描述	源	目标
25	XenMobile 通知服务的默认 SMTP 端口。如果您的 SMTP 服务器使用不同的端口，	XenMobile	SMTP 服务器

TCP 端口	描述	源	目标
	请确保您的防火墙未阻止该端口。		
80 和 443	企业应用商店连接到 Apple iTunes App Store 或 Google Play（必须使用 80）。用于 Apple 批量采购。用于从 iOS 或适用于 Android 的 Secure Hub 的应用商店发布应用。	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 和 Nexmo SMS 通知中继之间的出站连接。	XenMobile	Nexmo SMS 中继服务器
389	用于不安全的 LDAP 连接。	XenMobile	LDAP 身份验证服务器或 Active Directory
443	用于 Android 设备的注册和代理设置。	互联网	XenMobile
443	用于 Android 和 Windows 设备的注册和代理设置，以及 MDM 远程支持客户端。	互联网、局域网和 Wi-Fi	XenMobile
1433	默认用于连接远程数据库服务器（可选）。	XenMobile	SQL 服务器
443 或 2197	用于向 `*.push.apple.com` 发送 APNs 通知	XenMobile	Internet（使用公共 IP 地址 17.0.0.0/8 的 APNs 主机

TCP 端口	描述	源	目标
5223	用于从 iOS 设备到 `*.push.apple.com` 的 APNs 出站连接。	iOS 设备	Internet（使用公共 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隧道。默认为 8081。	远程支持客户端	XenMobile
8443	用于 iOS 设备的注册。	互联网；局域网和无线局域网	XenMobile

AutoDiscovery 服务连接的端口要求

此端口配置可确保从适用于 Android 的 Secure Hub 连接的 Android 设备可以从内部网络访问 Citrix AutoDiscovery Service (ADS)。您需要访问 ADS 才能下载通过 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，请允许 ADS 连接绕过代理服务器。

> 如果要启用证书锁定，请执行以下先决条件：

- **收集 XenMobile Server 和 Citrix ADC 证书。** 证书必须为 PEM 格式，并且必须是公共证书，而不是私钥。
- **联系 Citrix 支持部门并提交启用证书锁定的请求。** 在此过程中，系统会要求您提供证书。

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

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

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

有关支持的 IP 地址的信息，请参阅 来自 AWS 的基于云的存储中心。

Android Enterprise 网络要求

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

XenMobile 的端口要求

以下目标主机必须可从网络访问，才能创建 Managed Google Play Enterprise 并访问 Managed Google Play iFrame。Google 向 EMM 开发人员提供了 Managed Play iFrame，以简化应用程序的搜索和批准。要使用 Managed Play iFrame，您用于访问 XenMobile 控制台的浏览器必须能够访问 Google Play。

目标主机	端口	描述
`play.google.com`	TCP/443	用于 Google Play 商店、Play Enterprise 注册
`*.googleapis.com`	TCP/443	用于 谷歌移动管理、谷歌 API 接口、谷歌 Play 商店 API 接口、FCM。
`accounts.youtube.com`, `accounts.google.com`	TCP/443	用于帐户身份验证
`apis.google.com`	TCP/443	用于 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 Fonts 用户生成的内容。例如，商店中的应用程序图标
`cri.pki.goog`, `ocsp.pki.goog`	TCP/443	用于证书验证

可伸缩性和性能

了解 XenMobile® 基础架构的规模对于您决定如何部署和配置 XenMobile 至关重要。本文包含可伸缩性测试数据以及有关确定中小型到大型本地 XenMobile 企业部署的性能和可伸缩性基础架构要求的指导。

此处的可伸缩性定义为已注册到部署的设备同时重新连接到部署的能力。

- *可伸缩性*定义为部署中注册的最大设备数量。
- *登录速率*定义为现有设备重新连接到部署的最大速率。

本文中的数据来源于对规模从 10,000 到 75,000 台设备的部署进行的测试。这些测试包括使用已知工作负载的移动设备。

所有测试均在 XenMobile Advanced Edition（本地）或 Citrix Endpoint Management™（云）上完成。

测试使用 Citrix Gateway 8200 进行。具有相似或更高容量的 Citrix ADC 设备预计会产生相似或更高的可伸缩性和性能。

可伸缩性测试结果摘要如下。

针对多达 75,000 台设备的部署的可伸缩性测试结果摘要

登录速率（现有用户的重新连接速率）— 每小时最多 9,375 台设备

使用的配置：

- Citrix 网关
- MPX 8200
- XenMobile 高级版（本地）或 Citrix Endpoint Management（云）
- XenMobile Server 7 节点群集
- 数据库：Microsoft SQL Server 外部数据库

按设备数量和硬件配置划分的测试结果

设备数量	12,500	30,000	60,000	75,000
每小时现有设备的重新连接速率	1,250	3,750	7,500	9,375

设备数量	12,500	30,000	60,000	75,000
XenMobile Server – 模式	独立	集群	集群	集群
XenMobile 服务器 – 集群	不适用	3	5	7
XenMobile 服务器 – 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
活动目录	内存 = 4 GB RAM；vCPU = 2	内存 = 8 GB RAM; 虚拟 CPU = 4	内存 = 16 GB RAM; 虚拟 CPU = 4	内存 = 16 GB RAM; 虚拟 CPU = 4
Microsoft SQL Server 外部数据库	内存 = 8 GB RAM; 虚拟 CPU = 4	内存 = 16 GB RAM; 虚拟 CPU = 8	内存 = 24 GB RAM; 虚拟 CPU = 16	内存 = 24 GB RAM; 虚拟 CPU = 16

扩展性配置文件

活动目录配置	使用的配置文件
用户	100,000
组	200,000
嵌套级别	5

XENMOBILE SERVER 配置	总计	每用户
策略	20	20
应用程序	270	50
公共应用程序	200	0
MDX	50	30
Web 和 SaaS	20	20

XENMOBILE SERVER 配置	总计	每用户
操作	50	
交付组	20	
每个交付组的 Active Directory 组	10	
SQL		
数据库数量	1	

设备连接和应用程序活动

此可伸缩性测试收集了有关部署中注册设备在 8 小时内重新连接能力的数据。

这些测试模拟了一个重新连接间隔，在此期间，重新连接的设备会获取所有授权的安全策略，使 XenMobile Server 节点承受高于正常水平的负载条件。在随后的重新连接期间，只有更改或新的策略才会推送到 iOS 设备，从而减轻 XenMobile Server 节点的负载。

这些测试使用了 50% 的 iOS 设备和 50% 的 Android 设备。

这些测试假设重新连接的 Android 设备已收到之前的 GCM 通知。

在 8 小时测试间隔期间，发生了以下与应用程序相关的活动：

- Secure Hub 打开一次以枚举授权应用程序
- 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 供 Secure Mail 使用
- 完成了 240 次 STA 票证验证，每次 Secure Mail 通过微型 VPN 重新连接事件进行一次。

参考体系结构

有关这些可伸缩性测试中使用的部署的参考体系结构，请参阅 本地部署的参考体系结构 中的“核心 MAM+MDM 参考体系结构”。

注意事项和限制

在考虑本文中的可伸缩性测试结果时，请注意以下事项：

- 未测试 Windows 平台。

- 策略推送已针对 iOS 和 Android 设备进行测试。
- 每个 XenMobile Server 节点同时支持最多 12,000 台设备。

许可

XenMobile Server 现在支持许可证激活服务 (LAS) 许可机制。LAS 是一种新的基于云的许可解决方案，为 Citrix 产品套件中传统的基于文件的许可提供了一种现代替代方案。将您的 Citrix 许可证服务器注册到 Citrix Cloud，以使用许可证激活服务所持有的许可证和权利。有关详细信息，请参阅 许可证激活服务。

> **重要提示：**
>
> - 请在 April 15, 2026 之前采用新的许可模式。有关详细信息，请参阅 Citrix 现代许可公告。
> - Citrix® 许可证的退回和修改流程自 November 4, 2020 起已更改。有关详细信息，请参阅以下文章：
> - 如何使用我的帐户退回许可证
> - 如何重新分配许可证文件

> XenMobile® 使用 Citrix Licensing 来管理许可证。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 Citrix 许可系统。

购买 XenMobile Server 后，您会收到一封订单确认电子邮件，其中包含激活许可证的说明。新客户必须在下订单前注册许可计划。有关 XenMobile 许可模型和计划的详细信息，请参阅 XenMobile 许可。

要求

- 在更新到最新版本的 XenMobile Server 之前，请将您的 Citrix 许可证服务器更新到 11.16.x 或更高版本。旧版许可证服务器不支持最新版本的 XenMobile。
- 在下载 XenMobile 许可证之前，您必须安装 Citrix Licensing。生成许可证文件需要安装 Citrix Licensing 的服务器名称。默认情况下，安装 XenMobile 时会在服务器上安装 Citrix Licensing。或者，您可以使用现有的 Citrix Licensing 部署来管理您的 XenMobile 许可证。有关安装、部署和管理 Citrix Licensing 的详细信息，请参阅 许可您的产品。

- 如果您打算对 XenMobile 的节点或实例进行群集，则必须在远程服务器上使用 Citrix Licensing。
- Citrix 建议您保留所有收到的许可证文件的本地副本。当您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，如果您在未首先备份配置文件的情况下重新安装 XenMobile，则需要原始许可证文件。

XenMobile 许可注意事项

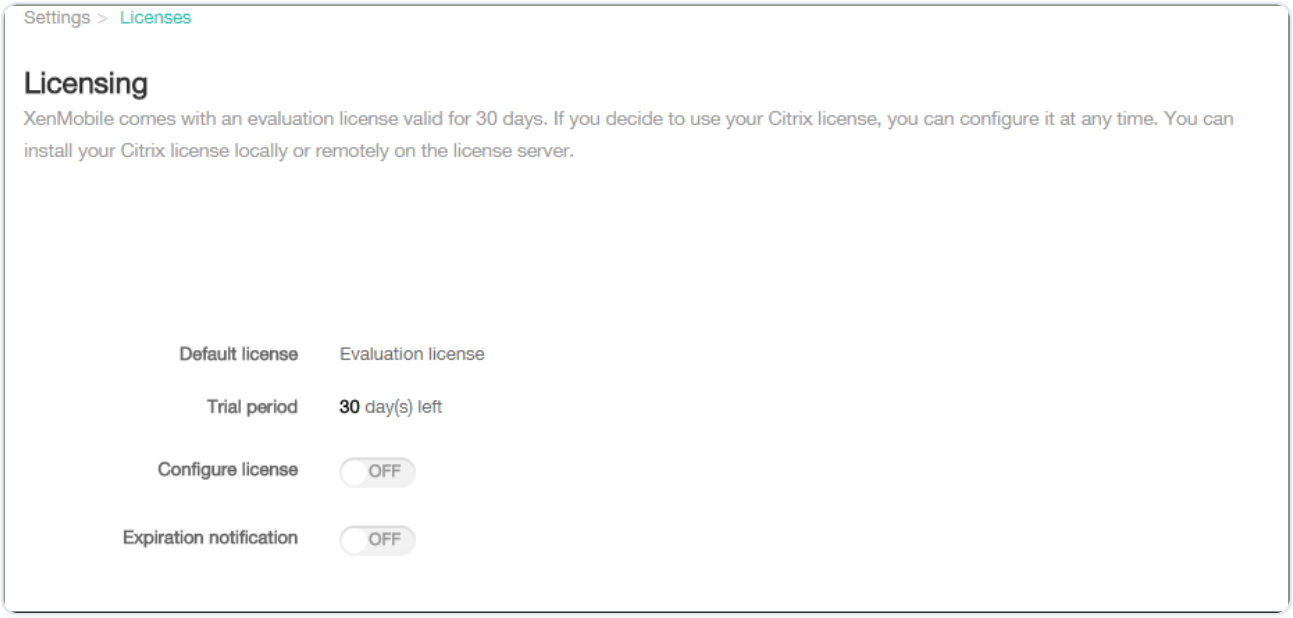
如果没有许可证，XenMobile 将在试用模式下以完整功能运行，宽限期为 30 天。此试用模式只能使用一次，30 天的期限从您安装 XenMobile 时开始计算。无论 XenMobile 许可证是否有效，对 XenMobile Web 控制台的访问都不会被阻止。在 XenMobile 控制台中，您可以查看试用期还剩多少天。

尽管 XenMobile 允许您上传多个许可证，但一次只能激活一个许可证。

当 XenMobile 许可证过期时，您将无法再执行任何设备管理功能。例如，无法注册新用户或设备，也无法更新部署到已注册设备的应用和配置。有关 XenMobile 许可模型和程序的详细信息，请参阅 XenMobile 许可。

在 XenMobile 控制台上查找“许可”页面

在您安装 XenMobile 后首次出现“**许可**”页面时，许可证将设置为默认的 30 天试用模式，并且尚未配置。您可以在此页面上添加和配置许可证。



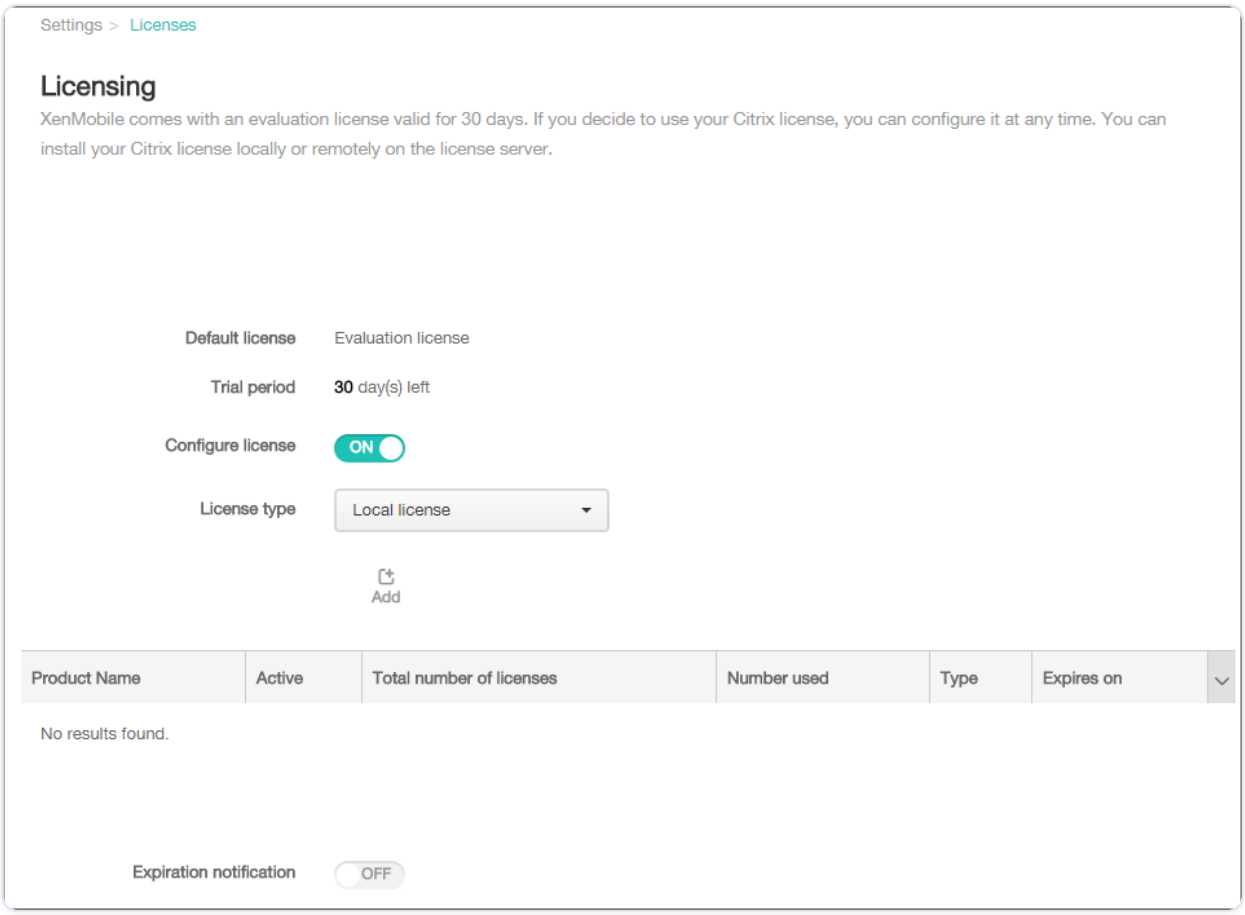
1. 在 XenMobile 控制台上，单击右上角的齿轮图标。此时将显示“**设置**”页面。
2. 单击“**许可**”。此时将显示“**许可**”页面。

添加本地许可证

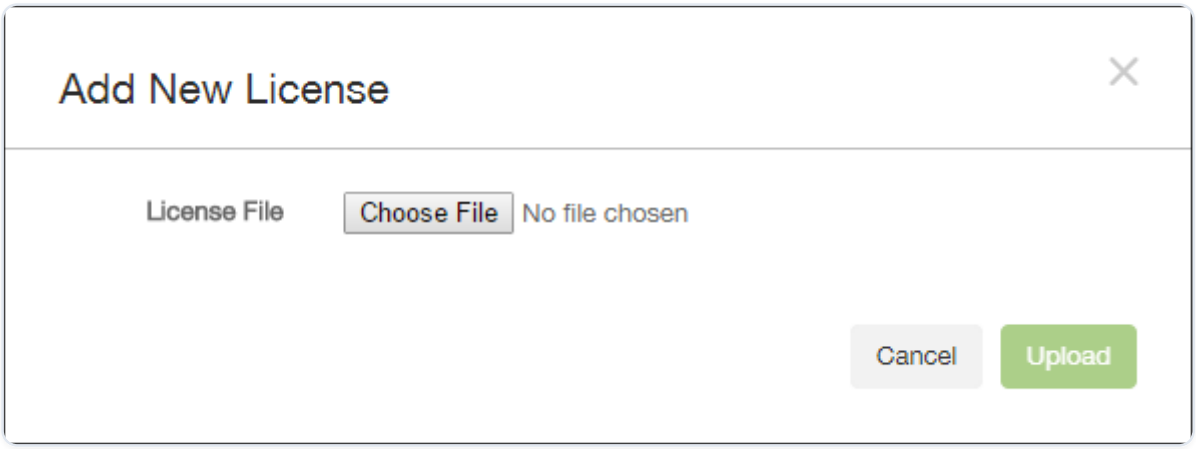
添加新许可证时，它们会显示在表中。添加的第一个许可证会自动激活。如果您添加多个相同类别（例如企业版和类型）的许可证，这些许可证将显示在表中的一行中。在这些情况下，“**许可证总数**”和“**已用数量**”反映了通用许可证的总和。“**过期日期**”显示了通用许可证中的最新过期日期。

您通过 XenMobile 控制台管理所有本地许可证。

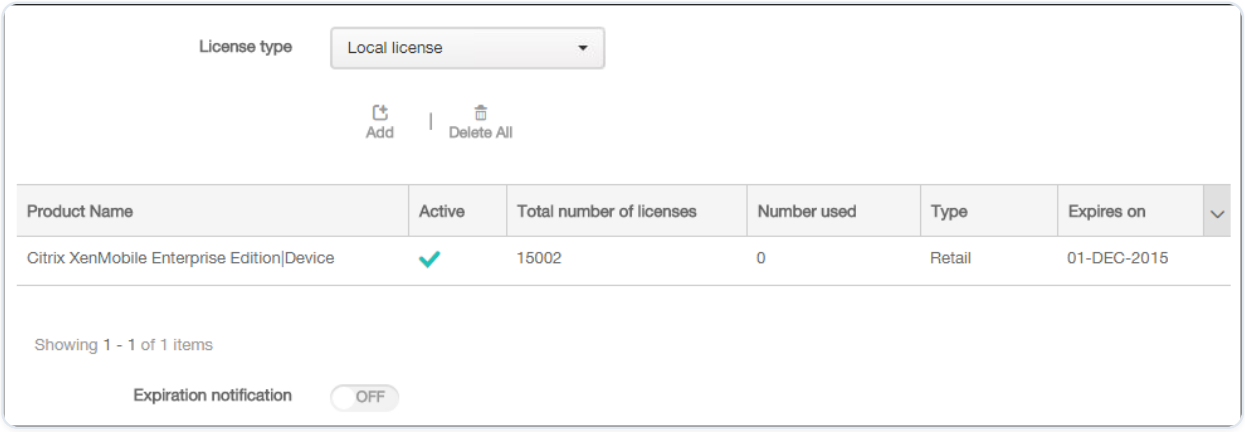
1. 从 Simple License Service、通过 License Administration Console 或直接从 Citrix.com 上的帐户获取许可证文件。有关详细信息，请参阅 Citrix 许可文档。
2. 在 XenMobile 控制台上，单击右上角的齿轮图标。此时将显示“**设置**”页面。
3. 单击“**许可**”。此时将显示“**许可**”页面。
4. 将“**配置许可证**”设置为“**开**”。“**许可证类型**”列表、“**添加**”按钮和“**许可**”表随即显示。“**许可**”表包含您已与 XenMobile 配合使用的许可证。如果您尚未添加 Citrix 许可证，则该表为空。



5. 确保“**许可证类型**”设置为“**本地许可证**”，然后单击“**添加**”。“**添加新许可证**”对话框随即显示。



6. 在“**添加新许可证**”对话框中，单击“**选择文件**”，然后浏览到您的许可证文件位置。
7. 单击“**上载**”。许可证将上载到本地并显示在表中。



8. 当许可证显示在“**许可**”页面上的表中时，将其激活。如果许可证在表中排在首位，则会自动激活。

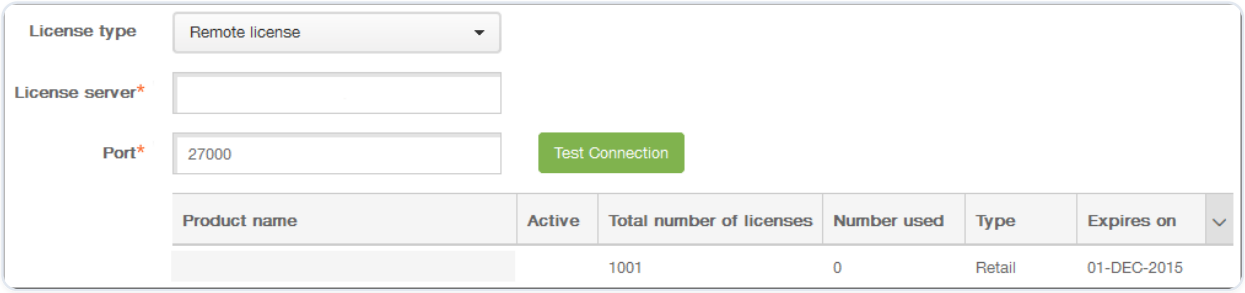
添加远程许可证

如果您使用的是远程 Citrix 许可服务器，您可以使用 Citrix 许可服务器管理*所有*许可活动。有关详细信息，请参阅许可您的产品。

1. 将许可证服务器证书导入 XenMobile Server (**Settings > Certificates**)。
2. 默认情况下，除 Microsoft PKI 服务器外，传出连接上均启用主机名验证。如果主机名验证中断您的部署，请将服务器属性 **disable.hostname.verification** 更改为 **true**。此属性的默认值为 **false**。

   当主机名验证失败时，服务器日志中会包含以下错误：“无法连接到批量购买服务器: 主机名 '192.0.2.0' 与对等方提供的证书主题不匹配”
3. 在“**许可**”页面上，将“**配置许可证**”设置为“**开**”。“**许可证类型**”列表、“**添加**”按钮和“**许可**”表随即显示。“**许可**”表包含您已与 XenMobile 配合使用的许可证。如果您尚未添加 Citrix 许可证，则该表为空。

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：

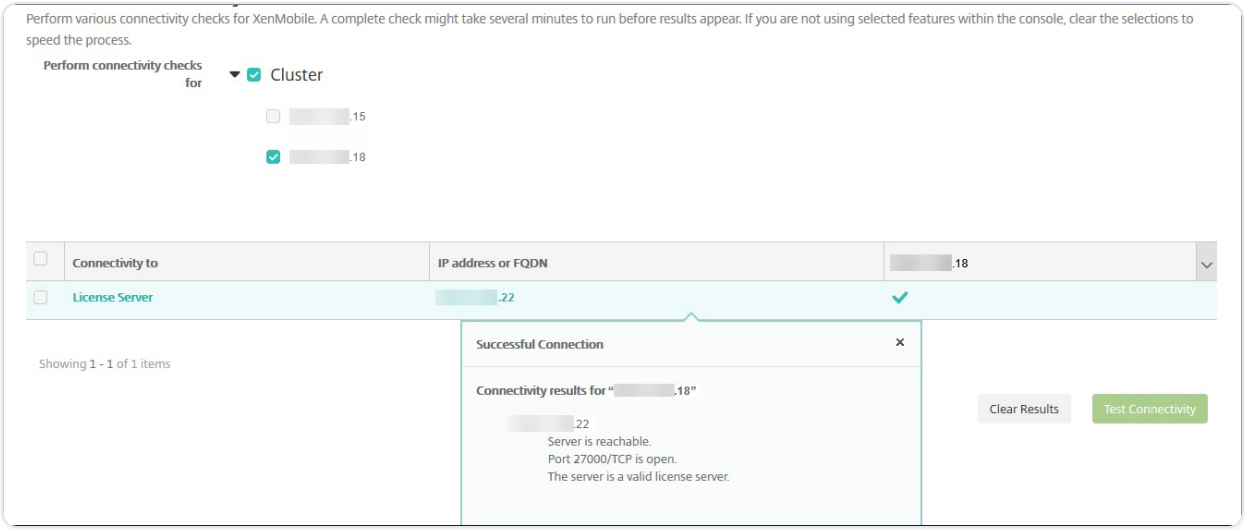
   - **许可证服务器：**键入远程许可服务器的 IP 地址或完全限定域名 (FQDN)。
   - **端口：**接受默认端口或键入用于与许可服务器通信的端口号。

6. 单击**测试连接**。如果连接成功，XenMobile 将连接到许可服务器，并且许可表将填充可用许可证。如果只有一个许可证，它将自动激活。

   当您单击**测试连接**时，XenMobile 会确认以下内容：

   - 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。

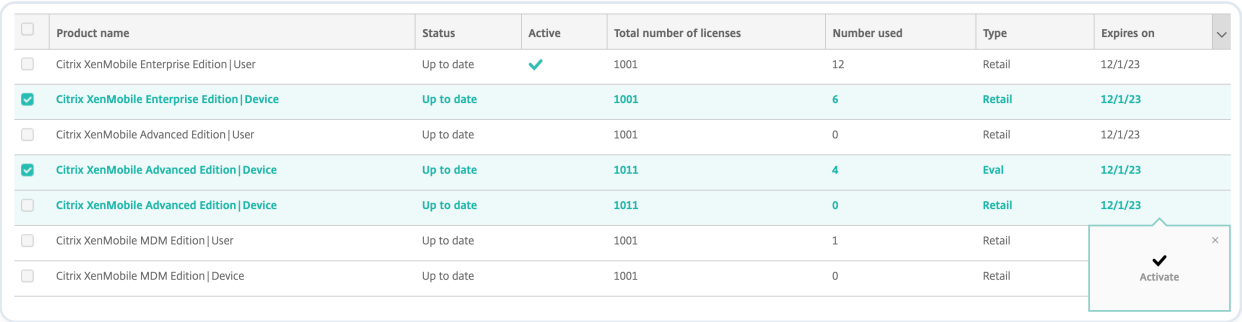
   如果连接不成功，请查看显示的错误消息，进行必要的更正，然后单击**测试连接**。



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。

1. 在**许可**页面上的**许可表**中，选择要激活的许可证。单击列表中的任意行，将显示**激活**对话框。



Product name	Status	Active	Total number of licenses	Number used	Type	Expires on
Citrix XenMobile Enterprise Edition | User	Up to date	✔	1001	12	Retail	12/1/23
Citrix XenMobile Enterprise Edition | Device	Up to date		1001	6	Retail	12/1/23
Citrix XenMobile Advanced Edition | User	Up to date		1001	0	Retail	12/1/23
Citrix XenMobile Advanced Edition | Device	Up to date		1011	4	Eval	12/1/23
Citrix XenMobile Advanced Edition | Device	Up to date		1011	0	Retail	12/1/23
Citrix XenMobile MDM Edition | User	Up to date		1001	1	Retail	
Citrix XenMobile MDM Edition | Device	Up to date		1001	0	Retail	

2. 点击 **激活**。
3. 当您在许可证的“**活动**”行中看到复选标记时，点击“**保存**”。

> **重要提示：**
>
> - 每**用户**许可证和每**设备**许可证是互斥的，不能同时激活。
> - 只有 ADV Edition 和 ENT Edition 许可证可以混合使用。MDM Edition 许可证不能与 ADV Edition 或 ENT Edition 许可证混合使用。
> - 确保同一版本的许可证文件具有相同的状态。例如，如果一个 ADV 版本文件被激活，则其余的 ADV 文件将自动激活。
> - 对于 XenMobile Server 10.15 Rolling Patch 3 之前的版本，一次只能激活一个许可证。当您激活所选许可证时，当前活动的许可证将被停用。

自动发送过期通知

激活远程或本地许可证后，您可以配置 XenMobile 以在许可证到期日期临近时通知您或指定人员。

1. 在“**许可**”页面上，将“**过期通知**”设置为“**开**”。将出现新的通知相关字段。

   许可配置屏幕的图像(/en-us/xenmobile/server/media/notification-setup.png)

2. 配置以下设置：

   - **通知频率：** 类型：
   - 发送通知的频率，例如每 **7** 天。
   - 何时开始发送通知，例如在许可证到期前 60 天。
   - **收件人：** 输入您的电子邮件地址或负责许可证的人员的电子邮件地址。
   - **内容：** 输入收件人将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**中输入的收件人发送电子邮件，其中包含您在**内容**中输入的文本。通知将按照您设置的频率发送。

许可证激活服务

重要提示：

我们正在向 Citrix 平台采用行业标准的云端许可架构。此举可实现授权和激活自动化，为客户带来以下主要优势：

- **无需管理许可证文件：** 无需下载、分配或管理许可证文件，从而简化您的管理任务。
- **自动更新授权：** 合同续订后，授权会在后台自动更新，确保服务不中断。
- **增强的弹性：** 许可证服务器不再是用户会话的单点故障，从而增强了环境的稳定性。

我们鼓励您利用在切换之前的时间来规划并执行您的过渡，以便在 April 15, 2026 之前采用新的许可模式，我们致力于在每一步为您提供支持。有关更多信息，请参阅 Citrix 现代许可公告。

许可证激活服务 (LAS) 是一种新的云端许可解决方案，可替代传统的 Citrix 旧版许可。LAS 引入了新的激活模块，确保了无缝且现代的许可证管理方法。

LAS 简化了 Citrix 许可体验。不再需要在许可证服务器上生成、下载或安装许可证访问代码或文件。您只需升级许可证服务器并向 Citrix Cloud 注册。一旦兼容产品指向许可证服务器，它们就可以自动激活。

激活后，许可证服务器会定期与许可证激活服务通信，以保持其激活状态最新。LAS 采用云技术构建，可提高性能并确保无停机时间。如果由于任何原因许可证服务器或 LAS 无法访问，系统将进入许可证缓存模式，该模式旨在保护系统免于未授权状态并避免中断。有关更多信息，请参阅 许可证缓存模式。

对于无法连接到云的许可证服务器，LAS 还提供离线激活选项，确保了各种网络环境的灵活性。此服务引入了一种无缝且现代的方法来管理您的 Citrix 产品许可证。

有关 LAS 的更多详细信息，请参阅许可文档 许可证激活服务。

LAS 兼容性

与 LAS 兼容的最低 XenMobile Server 版本为：

- 10.16 滚动修补程序 7
- 10.15 滚动补丁 13

> **注意：**
>
> On April 15, 2026, 旧版基于文件的许可将停止运行。使用旧版基于文件的许可机制的部署将对最终用户产生影响。

先决条件

- 安装或更新许可证服务器到版本 11.17.2 build 51000 或更高版本。
- 一个 Citrix Cloud 帐户，其 OrgID 与您的 XenMobile Server 权利相关联。
- 配置许可证服务器以进行在线激活。

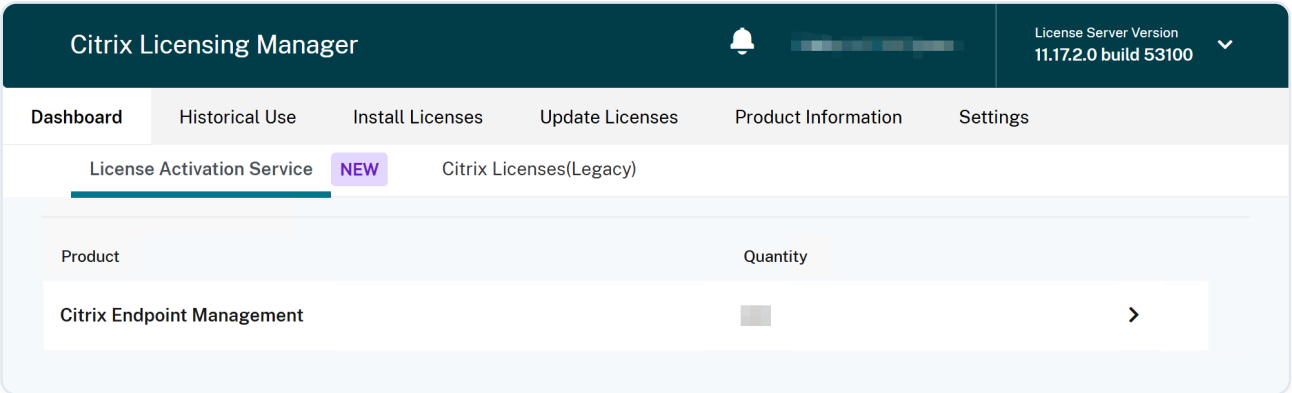
配置许可证激活服务

步骤 1：安装或升级许可证服务器

将许可证服务器安装或升级到版本 11.17.2 build 51000 或更高版本。您可以从 Citrix 许可下载页面下载适用于 Windows 的 Citrix 许可证服务器。

步骤 2：配置 LAS

按照 如何配置许可证服务器以进行许可证激活服务 中所述的说明配置 LAS，确保 XenMobile Server 权利包含在用于载入许可证服务器的 Citrix Cloud 客户帐户中。



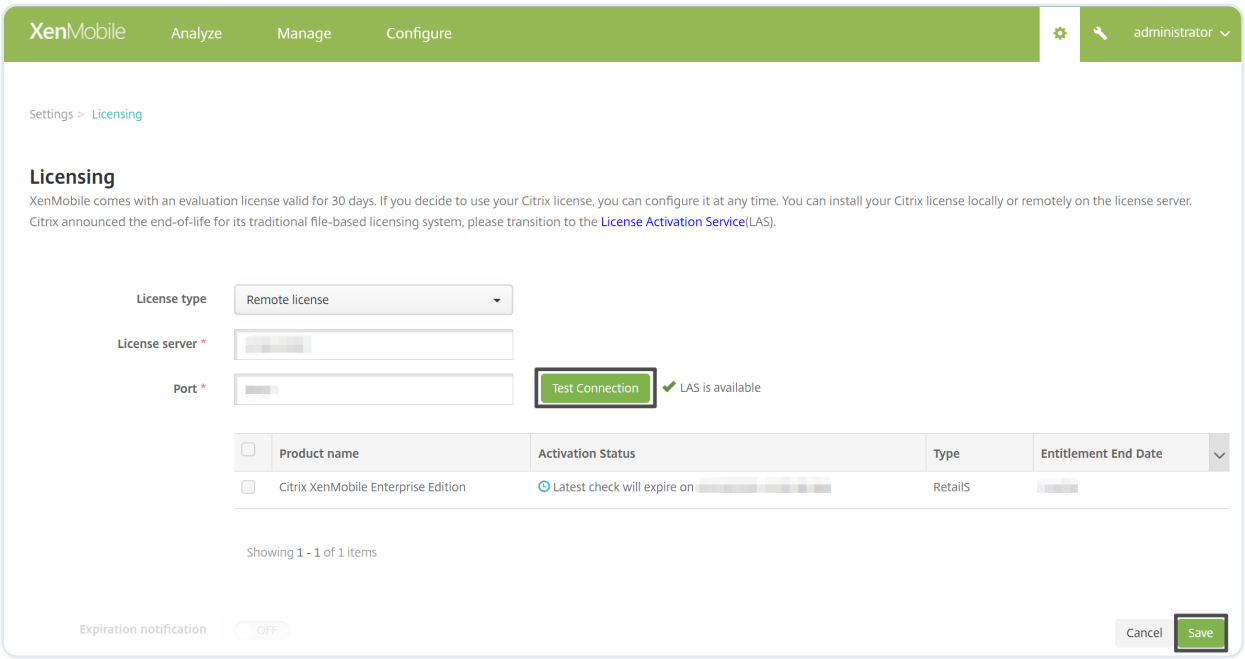
步骤 3：升级 XenMobile Server

将 XenMobile Server 升级到与 LAS 兼容的版本。所需的最低 XenMobile Server 版本为：

- 10.16 滚动修补程序 7
- 10.15 滚动修补程序 13

步骤 4：配置 XenMobile Server 以使用 LAS

1. 登录 XenMobile Server 控制台，然后导航到**设置 > 许可**。
2. 将**许可证类型**设置为**远程许可证**。
3. 配置**许可证服务器**和**端口**：
   - **许可证服务器：** 键入远程许可服务器的 IP 地址或完全限定域名 (FQDN)。
   - **端口：** 接受默认端口（LAS 为 8083）或键入用于与 LAS 许可服务器通信的自定义端口号。
4. 单击**测试连接**。如果连接成功，则表示 LAS 可用，并且“许可”表已填充可用许可证，请确保“激活状态”正常，没有任何错误。



5. 单击**保存**。配置已保存，并且 XenMobile Server 将切换为使用许可证激活服务。

故障排除

如果许可证服务器状态不是绿色，请按照以下步骤操作以查看激活详细信息并排查任何问题。

要在 Citrix Cloud 中验证 XenMobile Server 激活详细信息，请执行以下步骤：

1. 导航到**许可** > **已许可的部署** > **许可证服务器**。
2. 找到 XenMobile Server 使用的许可证服务器，然后点击 **查看详细信息**。
3. 在许可证服务器详细信息页面中，展开 **Citrix Endpoint Management** 以查看激活列表。

每个激活显示的 **ID** 是 XenMobile Server 主机名。

CEM 成功连接的图像(/en-us/xenmobile/server/media/cem-successful-connection.png)

4. 点击 **查看详细信息** 以查看所需的激活。

   详细信息页面显示以下信息：

   - **XMS 主机名：** XenMobile Server 主机名。
   - **XMS IP：** XenMobile Server IP 地址。
   - **主机名：** XenMobile Server 主机名。

   LAS 视图详细信息图像(/en-us/xenmobile/server/media/xms-view-details.png)

FIPS 140-2 合规性

联邦信息处理标准 (FIPS) 由美国国家标准与技术研究院 (NIST) 发布。FIPS 规定了安全系统中使用的加密模块的安全要求。FIPS 140-2 是该标准的第二个版本。有关 NIST 验证的 FIPS 140 模块的更多信息，请参阅 NIST 计算机安全资源中心。

> **重要提示：**
>
> - 仅在初始安装期间才能启用 XenMobile® FIPS 模式。
> - 如果不使用 HDX™ 应用程序，则 XenMobile 仅移动设备管理、XenMobile 仅移动应用程序管理以及 XenMobile MDM+MAM 都符合 FIPS 标准。

> iOS 上所有静态数据和传输中数据的加密操作均使用 Citrix® 和 Apple 提供的经 FIPS 验证的加密模块。在 Android 上，所有静态数据的加密操作均使用设备制造商提供的平台加密模块提供的经 FIPS 验证的加密模块。有关设备制造商模块的更多信息，请联系您的 Citrix 代表。

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的加密操作均使用经 FIPS 验证的加密模块。

XenMobile MDM 的所有静态数据和传输中数据的加密操作均使用经 FIPS 验证的加密模块。MDM 流的所有静态数据和传输中数据均端到端使用符合 FIPS 标准的加密模块。该安全性包括前面描述的移动设备的加密操作，以及移动设备与 Citrix Gateway 之间的加密操作。

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

语言支持

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

本文列出了 XenMobile 最新版本中支持的语言。

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 表示该应用程序采用该特定语言可用。

iOS 和 Android 平台

语言	安全中心	安全邮件	安全浏览器	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

语言	安全中心	安全邮件	安全浏览器	QUICKEDIT
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 操作系统

语言	安全中心	安全邮件	安全 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

从右到左语言支持

下表总结了每款应用对中东语言文本的支持。X 表示该功能适用于该平台。Windows 设备不支持从右到左语言。

应用	IOS	安卓
安全中心	X	X
安全邮件	X	X
安全 Web	X	X
QuickEdit	X	X

安装和配置

开始之前

您可以使用以下预安装清单来记录在本地安装 XenMobile® 的先决条件和设置。每个任务或备注都包含一列，指示该要求适用的组件或功能。

规划 XenMobile 部署涉及许多注意事项。有关完整 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。

预安装清单

基本网络连接

以下是 XenMobile 解决方案所需的网络设置。

先决条件或设置	组件或功能	记录设置	
记录远程用户连接的完全限定域名 (FQDN)。	XenMobile 和 Citrix 网关		
记录公共和本地 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 网关		
记下子网掩码。	思杰 XenMobile 和 思杰网关		
记下 DNS IP 地址。	思杰 XenMobile 和 思杰网关		

先决条件或设置	组件或功能	记录设置	
记下 WINS 服务器 IP 地址（如果适用）。	Citrix 网关		
识别并记下 Citrix Gateway 主机名。	Citrix 网关	此项不是 FQDN。FQDN 包含在绑定到虚拟服务器并供用户连接的签名服务器证书中。您可以使用 Citrix Gateway 中的安装向导配置主机名。	思杰网关
记下 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，请记下所需的所有 IP 地址。	XenMobile		
在 Citrix Gateway 上配置的一个公共 IP 地址	思杰网关		
Citrix Gateway 的一个外部 DNS 条目	思杰网关		
记下 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了代理	思杰网关	配置 Web 代理的用户名时，可以使用 sAMAccountName 或用户主体名称 (UPN)。	XenMobile 和思杰网关

先决条件或设置	组件或功能	记录设置		
服务器（如果适用），则这些设置是可选的。				
记下默认网关 IP 地址。	XenMobile 和思杰网关			
记下系统 IP (NSIP) 地址和子网掩码。	思杰网关			
记下子网 IP (SNIP) 地址和子网掩码。	思杰网关			
记下证书中的 Citrix Gateway 虚拟服务器 IP 地址和 FQDN。要配置多个虚拟服务器，请记下证书中的所有虚拟 IP 地址和 FQDN。	思杰网关			
记下用户可以通过 Citrix Gateway 访问的内部网络。示例：10.10.0.0/24。在以下情况下，输入用户需要访问的所有内部网络和网络段：当用户使用 Secure Hub 或 Citrix Gateway 插件连接且拆分隧道设置为“开”时。	Citrix 网关			

先决条件或设置	组件或功能	记录设置	
确保 XenMobile Server、Citrix Gateway、外部 Microsoft SQL Server 和 DNS 服务器之间的网络连接可达。	XenMobile 和 Citrix 网关		

许可

XenMobile 要求您购买 Citrix Gateway 和 XenMobile 的许可选项。有关 Citrix 许可的详细信息，请参阅Citrix 许可系统。

必备条件	组件	记下位置
从 Citrix 网站获取通用许可证。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 需要证书才能启用与其他 Citrix 产品和应用程序以及用户设备的连接。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。	思杰移动和思杰网关	

端口

打开端口以允许与 XenMobile 组件通信。

先决条件	组件	备注
为 XenMobile 打开端口	思杰移动和思杰网关	

数据库

XenMobile 需要数据库连接配置。XenMobile 存储库需要运行在 系统要求和兼容性 中所述的受支持版本之一的 Microsoft SQL Server 数据库。Citrix 建议远程使用 Microsoft SQL。XenMobile 包含 PostgreSQL。*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。要在本地部署的 XenMobile Server 中使用 Microsoft JDBC 驱动程序，请参阅 SQL Server 驱动程序。

先决条件	组件	备注
Microsoft SQL Server IP 地址和端口。确保要在 XenMobile 上使用的 SQL Server 服务帐户具有 DBcreator 角色权限。	XenMobile	

活动目录设置

先决条件	组件	备注
记下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”选项更改为“是”。	XenMobile 和 思杰网关	
记下 Active Directory 域名。	XenMobile 和 思杰网关	
记下 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 用于查询 Active Directory 的帐户。	XenMobile 和 思杰网关	
记下用户基本 DN，即用户所在的目录级别。例如：`cn=users,dc=ace,dc=com`。Citrix Gateway 和 XenMobile 使用用户基本 DN 查询 Active Directory。	XenMobile 和 思杰网关	

先决条件	组件	备注
记下组基本 DN，这是组所在的目录级别。Citrix Gateway 和 XenMobile 使用此 DN 查询 Active Directory。	XenMobile 和 思杰网关	

XenMobile 与 Citrix Gateway 之间的连接

必备条件	组件	记下设置
记下 XenMobile 主机名。	XenMobile	
记下 XenMobile 的 FQDN 或 IP 地址。	XenMobile	
确定用户可以访问的应用程序。	Citrix 网关	
记下回调 URL。	XenMobile	

用户连接：访问 Citrix 虚拟应用和桌面™ 和 Citrix 安全中心

Citrix 建议您使用 Citrix ADC 中的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。您可以创建第二个虚拟服务器，以启用来自 Citrix Receiver™ 和 Web 浏览器的用户连接。这些连接用于 Virtual Apps and Desktops 中的基于 Windows 的应用程序和虚拟桌面。Citrix 建议您也使用 Citrix ADC 中的快速配置向导来配置这些设置。

前提条件	组件	记下设置
记下 Citrix Gateway 主机名和外部 URL。外部 URL 是用户连接所用的 Web 地址。	XenMobile	
记下 Citrix Gateway 回调 URL。	XenMobile	
记下虚拟服务器的 IP 地址和子网掩码。	思杰网关	

前提条件	组件	记下设置
记下 Program Neighborhood Agent 或 虚拟应用和桌面 站点的路径。	思杰网关和 XenMobile	
记下运行安全票证颁发机构 (STA) 的 Citrix Virtual Apps™ and Desktops 服务器的 FQDN 或 IP 地址（仅适用于 ICA 连接）。	思杰网关	
记下 XenMobile 的公共 FQDN。	思杰网关	
请注意 Secure Hub 的公共 FQDN。	思杰网关	

XenMobile 部署流程图

您可以使用此流程图来指导您完成部署 XenMobile 的主要步骤。每个步骤的主题链接位于图后。

1: 系统要求和兼容性

2: 安装和配置

3 和 4: 预安装清单（本文）

5: 在命令提示符窗口中配置 XenMobile（本文）

6: 在 Web 浏览器中配置 XenMobile（本文）

7: 配置您的 XenMobile 环境的设置

8: 端口要求

安装 XenMobile

XenMobile 虚拟机 (VM) 运行在 Citrix XenServer、VMware ESXi 或 Microsoft Hyper-V 上。您可以使用 XenCenter® 或 vSphere 管理控制台来安装 XenMobile。

注意：

> 确保管理程序配置了正确的时间（使用 NTP 服务器或手动配置），因为 XenMobile 会使用该时间。如果在将 XenMobile 时间与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 (/zh-cn/xenmobile/server/install-configure/command-line-interface.html) 中所述。

> **XenServer 或 VMware ESXi 先决条件**。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，请参阅您的 XenServer 或 VMware 文档。

- 在具有足够硬件资源的计算机上安装 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到 XenServer 或 VMware ESXi 主机。

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

- 在具有足够系统资源的计算机上安装已启用 Hyper-V 角色功能的 Windows Server 2016 或 Windows Server 2019。安装 Hyper-V 角色时，请务必指定服务器上 Hyper-V 用于创建虚拟网络的 NIC。您可以为主机保留一些 NIC。
- 删除文件 Virtual Machines/<*build-specific UUID*>.xml
- 将文件 Legacy/<*build-specific UUID*>.exp 移动到 Virtual Machines 中

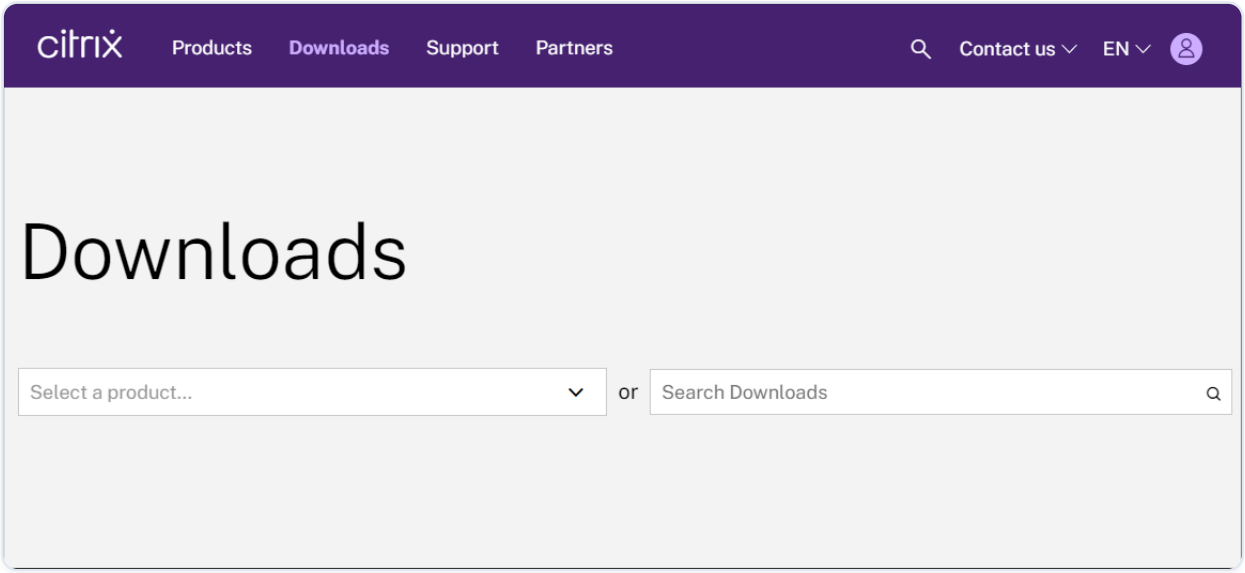
FIPS 140-2 模式。要在 FIPS 模式下安装 XenMobile Server，请完成一个先决条件组，如 (/zh-cn/xenmobile/server/install-configure/fips.html) 中所述。

下载 XenMobile 产品软件

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

下载 XenMobile 软件

1. 转到 Citrix 网站。
2. 在“搜索”框旁边，单击“**登录**”并登录您的帐户。
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) 页面自动显示。



5. 展开 **XenMobile Server（本地部署）**。
6. 展开 **产品软件**。
7. 单击 **XenMobile Server 10**。
8. 单击“**跳转到下载**”菜单，然后选择用于安装 XenMobile 的相应虚拟映像。或者，向下滚动页面以找到要安装的映像的“**下载文件**”按钮。
9. 按照屏幕上的说明下载软件。

下载 Citrix Gateway 软件

您可以使用此过程下载 Citrix Gateway 虚拟设备或将软件升级到您现有的 Citrix Gateway 设备。

1. 转到 Citrix 网站。
2. 如果您尚未登录 Citrix 网站，请在搜索框旁边，单击“**登录**”并登录您的帐户。
3. 单击“**下载**”选项卡。
4. 在“下载”页面上，从产品选择列表中，单击 **Citrix Gateway**。
5. 单击“**转到**”。Citrix Gateway 页面显示。
6. 在 Citrix Gateway 页面上，展开您正在运行的 Citrix Gateway 版本。
7. 在 **固件** 下，单击您要下载的设备软件版本。

> **注意：**
>
> 您也可以单击 **虚拟设备** 下载 Citrix ADC VPX。选择此选项时，您会收到每个虚拟机管理程序的虚拟机软件列表。

8. 单击您要下载的设备软件版本。
9. 在您要下载的版本的设备软件页面上，单击相应虚拟设备的 **下载**。
10. 按照屏幕上的说明下载软件。

首次使用 XenMobile 的配置

1. 要配置 XenMobile 的 IP 地址和子网掩码、默认网关、DNS 服务器及其他设置：请使用 XenCenter 或 vSphere 命令行控制台。

   > **注意：**
   >
   > 使用 vSphere Web 客户端时：我们建议您在 **自定义模板** 页面上部署 OVF 模板时不要配置网络属性。在高可用性配置中这样做：可以避免在克隆并重新启动第二个 XenMobile 虚拟机时出现的 IP 地址问题。

2. 仅通过 XenMobile Server 完全限定域名或节点的 IP 地址访问 XenMobile 管理控制台。
3. 登录，然后按照初始登录屏幕中的步骤操作。

在命令提示符窗口中配置 XenMobile

1. 将 XenMobile 虚拟机导入 Citrix XenServer、Microsoft Hyper-V 或 VMware ESXi。有关详细信息，请参阅 XenServer、Hyper-V 或 VMware 文档。
2. 在您的虚拟机管理程序中，选择导入的 XenMobile 虚拟机并启动命令提示符视图。有关详细信息，请参阅您的虚拟机管理程序文档。
3. 从虚拟机管理程序控制台页面，通过键入管理员用户名和密码，在命令提示符窗口中为 XenMobile 创建管理员帐户。

   当您为命令提示符管理员帐户、公钥基础结构 (PKI) 服务器证书和 FIPS 创建或更改密码时：XenMobile 对所有用户强制执行以下规则，但密码在 XenMobile 外部管理的 Active Directory 用户除外。

   - 密码长度必须至少为八个字符。
   - 密码必须满足以下至少三个复杂性条件：
     - 大写字母（A 到 Z）
     - 小写字母（a 到 z）
     - 数字（0 到 9）

- 特殊字符（例如 `! # $ %`）

```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
  Username: admin
  New password:
```

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 服务器的 IP 地址

   b. 子网掩码

   c. 默认网关，即 DMZ 中默认网关的 IP 地址

   d. 主 DNS 服务器，即 DNS 服务器的 IP 地址

   e. 辅助 DNS 服务器（可选）

```
Network settings:
  IP address: 192.0.2.0
  Netmask: 225.225.225.128
  Default gateway: 203.0.113.3
  Primary DNS server: 192.0.2.4
  Secondary DNS server [optional]: 192.0.2.5

  Commit settings [y/n]: y
```

> **注意：**
>
> 此图和后续图中显示的地址不可用，仅供参考。

5. 键入 **y** 以通过生成随机加密密码短语来提高安全性，或键入 **n** 以提供您自己的密码短语。Citrix 建议键入 **y** 以生成随机密码短语。

   密码短语用于保护用于保护敏感数据的加密密钥。存储在服务器文件系统中的密码短语哈希用于在数据加密和解密期间检索密钥。密码短语无法查看。

> **注意：**

如果您打算扩展环境并配置更多服务器，请提供您自己的密码短语。如果您选择随机密码短语，则无法查看它。

```
Encryption passphrase:
  Generate a random passphrase to secure the server data? [y/n]: y
```

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，请务必完成先决条件组，如 使用 XenMobile 配置 FIPS 中所述。

```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

7. 提供以下信息以配置数据库连接。

```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server:        .10
  Port: 5432
  Username: postgres
  Password:
```

- 您的数据库可以是本地的或远程的。键入 **l** 表示本地，键入 **r** 表示远程。
- 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。XenMobile 包含 PostgreSQL。仅在测试环境中*本地或远程*使用 PostgreSQL。
  - 不支持数据库迁移。在测试环境中创建的数据库无法移动到生产环境。

- （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域名 (FQDN)。此单主机服务器提供设备管理和应用程序管理服务。
- 如果数据库端口号与默认端口号不同，请键入您的数据库端口号。Microsoft SQL 的默认端口是 1433，PostgreSQL 的默认端口是 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** 以提交数据库设置。

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

> **重要：**
>
> 如果启用 XenMobile 群集，在系统配置完成后，打开端口 80 以启用群集成员之间的实时通信。在所有群集节点上完成该设置。

9. 键入 XenMobile Server 的完全限定域名 (FQDN)。

```
XenMobile hostname:
  Hostname: justan.example.com
```

10. 按 **Enter** 键以提交设置。
11. 识别通信端口。有关端口及其用途的详细信息，请参阅 Port Requirements。

> **注意：**
>
> 通过按 **Enter** 键（在 Mac 上为 Return 键）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. 跳过关于从以前的 XenMobile 版本升级的下一个问题，因为您是首次安装 XenMobile。
13. 如果您想为每个公钥基础设施 (PKI) 证书使用相同的密码，请键入 **y**。有关 XenMobile PKI 功能的详细信息，请参阅 Uploading Certificates。

```
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:
```

> **重要提示：**
>
> 如果您打算将 XenMobile 的节点或实例进行群集，请为后续节点提供相同的密码。

14. 键入新密码，然后再次输入新密码以确认。

    键入新密码时，不会显示任何字符，例如星号。

15. 按 **Enter** 键以提交设置。
16. 创建一个管理员帐户，用于通过 Web 浏览器登录 XenMobile 控制台。请务必记录这些凭据以备后用。

```
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：**
>
> 输入新密码时，不会显示任何字符（例如星号）。

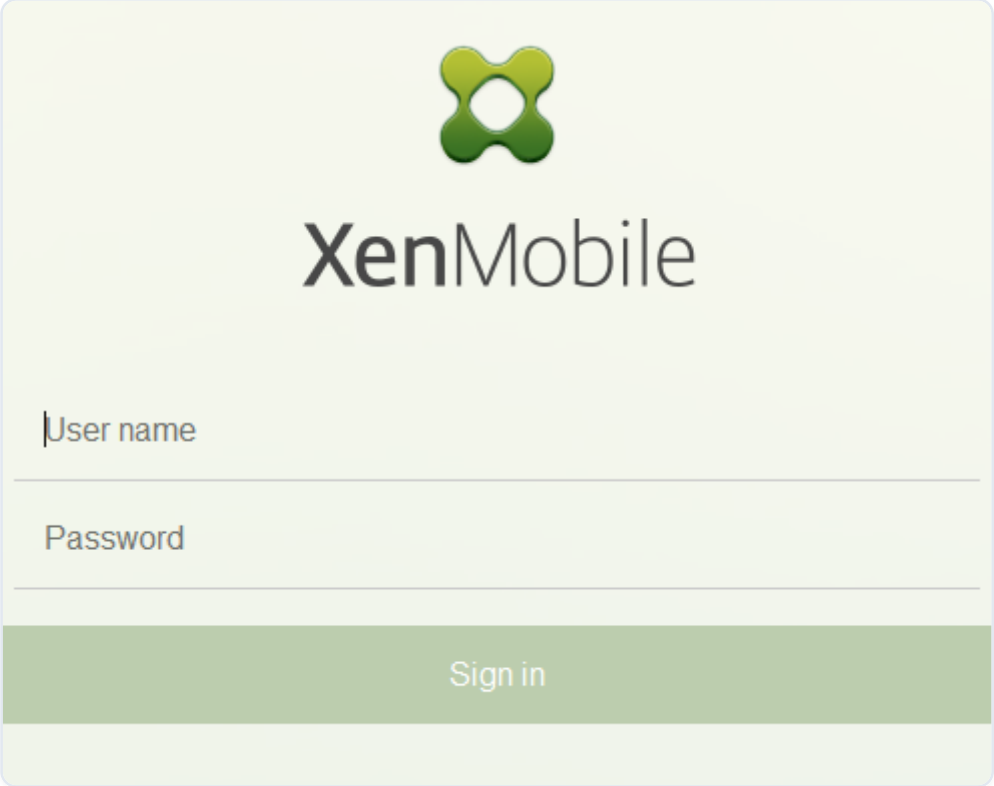
17. 按 **Enter** 键提交设置。初始系统配置已保存。
18. 当询问您是否正在升级时，键入 **n**，因为这是新安装。
19. 复制屏幕上显示的完整 URL，然后在 Web 浏览器中继续此初始 XenMobile 配置。

```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
  Upgrade from previous release (y/n) [n]:

Stopping configuration app...                                    [ OK ]
Starting configuration app...
  application started successfully                               [ OK ]
Stopping main app...                                             [ OK ]
Starting main app...
  this may take a few minutes.....................................................
.................................
  application started successfully                               [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://203.0.113.8:4443/

Starting monitoring...                                           [ OK ]
```

在 Web 浏览器中配置 XenMobile

在管理程序命令提示符窗口中完成 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，导航到命令提示符窗口配置结束时提供的位置。
2. 键入您在命令提示符窗口中创建的 XenMobile 控制台管理员帐户用户名和密码。



3. 在“入门”页面上，单击 **Start**（开始）。将显示“**许可**”页面。

4. 配置许可证。如果您不上传许可证，则会使用有效期为 30 天的评估许可证。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。

> **重要提示：**
>
> 如果您打算通过添加 XenMobile 群集节点或实例来使用 XenMobile 群集，则必须在远程服务器上使用 Citrix 许可。

5. 在“**证书**”页面上，单击“**导入**”。此时将显示“导入”对话框。
6. 导入 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. 如果适合环境，请配置 Citrix Gateway。有关配置 Citrix Gateway 的详细信息，请参阅Citrix Gateway 和 XenMobile和配置 XenMobile 环境的设置。

> **注意：**
>
> - 您可以在内部网络（或内网）的边界部署 Citrix Gateway。该部署提供对内部网络中服务器、应用程序和其他网络资源的安全单点访问。在此部署中，所有远程用户都必须先连接到 Citrix Gateway，然后才能访问内部网络中的任何资源。
> - 尽管 Citrix Gateway 是一个可选设置：在页面上输入数据后，您必须清除或完成必填字段才能离开页面。

8. 完成 LDAP 配置以从 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. 配置通知服务器以能够向用户发送消息。有关通知服务器配置的详细信息，请参阅通知。

先决条件。重新启动 XenMobile Server 以激活您的证书。

使用 XenMobile® 配置 FIPS

XenMobile 中的联邦信息处理标准 (FIPS) 模式通过仅使用 FIPS 140-2 认证的库进行所有加密操作，支持美国联邦政府客户。以 FIPS 模式安装 XenMobile Server 可确保 XenMobile 客户端和服务器的所有数据完全符合 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，请完成以下先决条件。

- 为 XenMobile 数据库使用外部 SQL Server 2014。SQL Server 还必须配置为安全的 SSL 通信。有关配置与 SQL Server 的安全 SSL 通信的说明，请参阅 启用与数据库引擎的加密连接（SQL Server 配置管理器）。
- 安全 SSL 通信要求您在 SQL Server 上安装来自知名证书颁发机构 (CA) 的受信任 SSL 证书。SQL Server 2014 不接受通配符证书。Citrix® 建议您申请一个带有 SQL Server FQDN 的 SSL 证书。

配置 FIPS 模式

只能在 XenMobile Server 的初始设置期间启用 FIPS 模式。安装完成后无法启用 FIPS。因此，如果您计划使用 FIPS 模式，则必须从一开始就以 FIPS 模式安装 XenMobile Server。对于 XenMobile 群集，所有群集节点都必须启用 FIPS。同一群集中不能混合使用 FIPS 和非 FIPS XenMobile Server。

XenMobile 命令行界面中有一个**切换 FIPS 模式**选项，该选项不适用于生产环境。此选项旨在用于非生产环境的诊断用途，并且在生产 XenMobile Server 上不受支持。

1. 在初始设置期间，启用**FIPS 模式**。
2. 上传 SQL Server 的根 CA 证书。
3. 指定 SQL Server 的服务器名称和端口、登录 SQL Server 的凭据以及为 XenMobile 创建的数据库名称。

   > **注意：**
   >
   > 您可以使用 SQL 登录或 Active Directory 帐户访问 SQL Server，但您使用的登录必须具有 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，继续进行 XenMobile 初始设置。

要确认 FIPS 模式配置成功，请登录 XenMobile 命令行界面。登录横幅中会显示短语 **In FIPS Compliant Mode**。

导入证书

以下过程介绍了如何通过导入证书在 XenMobile 上配置 FIPS。

SQL 先决条件

1. 从 XenMobile 到 SQL 实例的连接必须是安全的，并且必须是 SQL Server 2012 或 SQL Server 2014 版本。要保护连接，请参阅 如何使用 Microsoft 管理控制台为 SQL Server 实例启用 SSL 加密。
2. 如果服务未正确重新启动，请检查以下各项：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. 转到 **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。在向导的两个页面中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**，然后找到导入的 SSL 证书。
   f. 右键单击导入的证书（在 SQL Server 配置管理器中选择），然后单击 **所有任务 > 管理私钥**。
   g. 在 **组或用户名** 下，单击 **添加**。
   h. 输入您在前面步骤中复制的 SQL 服务帐户名称。
   i. 清除 **允许完全控制** 选项。默认情况下，服务帐户同时具有完全控制和读取权限，但它必须只能读取私钥。
   j. 关闭 **MMC** 并启动 SQL 服务。
3. 确保 SQL 服务已正确启动。

Internet 信息服务 (IIS) 先决条件

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 未被阻止。
7. 从本地服务器上的 Web 浏览器中浏览到 .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，请确保 IIS 服务器上已启用 ASP，如下所示。
   a. 打开服务器管理器。
   b. 导航到“**管理 > 添加角色和功能**”中的向导。
   c. 在服务器角色中，展开“**Web 服务器 (IIS)**”，展开“**Web 服务器**”，展开“**应用程序开发**”，然后选择“**ASP**”。
   d. 单击“**下一步**”，直到安装完成。
9. 浏览到 `https://localhost/cert.cer`。

   有关详细信息，请参阅 Web Server (IIS)。

> **注意：**
>
> 您可以使用 CA 的 IIS 实例执行此过程。

在初始 FIPS 配置期间导入根证书

首次在命令行控制台中完成 XenMobile 配置步骤时，必须完成这些设置才能导入根证书。有关安装步骤的详细信息，请参阅 Installing XenMobile。

- 启用 FIPS：是
- 上传根证书：是
- 复制(c) 或导入(i)：i
- 输入要导入的 HTTP URL：`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，移动设备上的 FIPS 模式是禁用的。要启用 FIPS 模式，请转到**设置 > 客户端属性**，编辑**启用 FIPS 模式**属性，并将其值设置为 **true**。有关详细信息，请参阅客户端属性。

配置集群

要配置集群，请在 Citrix ADC 上配置以下两个负载平衡虚拟 IP 地址。

- **移动设备管理 (MDM) 负载平衡虚拟 IP 地址：** 需要 MDM 负载平衡虚拟 IP 地址才能与集群中配置的 XenMobile® 节点通信。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 需要 MAM 负载平衡虚拟 IP 地址才能与集群中配置的 XenMobile 节点通信。在 XenMobile 中，默认情况下，来自 Citrix Gateway 的所有流量都路由到端口 8443 上的负载平衡虚拟 IP 地址。

本节中的过程说明了如何创建 XenMobile 虚拟机 (VM) 并将新 VM 加入到现有 VM。这些步骤将创建一个集群设置。

先决条件

- 您已完全配置所需的 XenMobile 节点。
- 在所有集群节点和 XenMobile 数据库上配置 NTP。为了使集群正常工作，所有这些服务器的时间必须相同。
- 一个用于 MDM 负载平衡器的公共 IP 地址和一个用于 MAM 的私有 IP 地址。
- 服务器证书。
- 一个用于 Citrix Gateway 虚拟 IP 地址的空闲 IP。
- 如果 XenMobile 部署在集群设置中且处于仅 MDM 模式或企业模式 (MDM+MAM)：修改您的 Citrix ADC 负载平衡器配置，以便对所有 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**源 IP 持久性**。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>`。
- 要在 iOS 11 设备上从 XenMobile Store 安装应用程序，您必须在 XenMobile Server 上启用端口 80。

有关集群配置中 XenMobile 10.x 的参考体系结构图，请参阅体系结构。

安装 XenMobile 集群节点

根据所需的节点数量，创建 XenMobile VM。将新的 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，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。

```
Network settings:
  IP address []: 10.147.75.51
  Netmask []: 255.255.255.0
  Default gateway []: 10.147.75.1
  Primary DNS server []: 10.147.75.240
  Secondary DNS server (optional) []:

  Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps
```

3. 如果要使用数据保护的默认密码，请键入 **y**；否则，请键入 **n** 并输入新密码。

```
Encryption passphrase:
  Generate a random passphrase to secure the server data (y/n) [y]:
```

4. 如果要使用 FIPS，请键入 **y**；否则，请键入 **n**。

```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

5. 配置数据库，使其指向与之前完全配置的 VM 所指向的相同数据库。您将看到消息：`Database already exists`。

```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

  Server []: sql2012.wg.lab
  Port [1433]:
  Username [sa]:
  Password:
  Database name [DB_service]: DB_51

  Commit settings (y/n) [y]:

  Checking database status...
  Database already exists.
 To enable realtime communication between cluster members please open port 80 us
ing Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..
```

6. 输入与为第一个 VM 提供的证书相同的密码。

```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

  Server []: sql2012.wg.lab
  Port [1433]:
  Username [sa]:
  Password:
  Database name [DB_service]: DB_51

  Commit settings (y/n) [y]:

  Checking database status...
  Database already exists.
 To enable realtime communication between cluster members please open port 80 us
ing Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key In
frastructure (PKI) in first node
  Do you want to use the same password for all the certificates of the PKI [y]:
```

输入密码后，第二个节点上的初始配置将完成。

```
Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key In
frastructure (PKI) in first node
  Do you want to use the same password for all the certificates of the PKI [y]:
y
  New password:
  Re-enter new password:
Saving server and client certs password...

Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app...                                          [ OK ]
Starting configuration app...
  this may take a few seconds.................................
  application started                                                  [ OK ]
Stopping main app...                                                   [ OK ]
Starting main app...
  this may take a few minutes.......
```

7. 配置完成后，服务器将重新启动并显示登录对话框。

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

Initial system configuration complete!
Stopping configuration app...                                          [ OK ]
Starting configuration app...
  this may take a few seconds.......
  application started                                                  [ OK ]
Stopping main app...                                                   [ OK ]
Starting main app...
  this may take a few minutes.........................^[.....................
....................................
  application started                                                  [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://10.147.75.59:4443/

Starting monitoring...                                                 [ OK ]

xms51.wg.lab login:
```

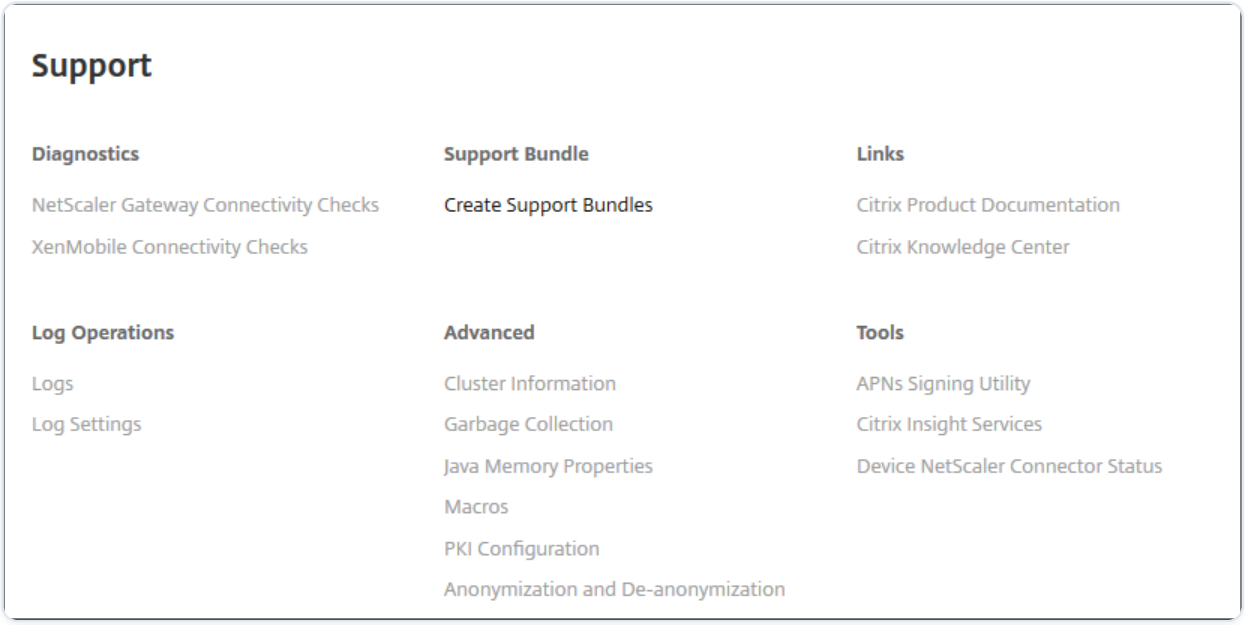
注意：

登录对话框与第一个 VM 的登录对话框类似。此匹配是您确认两个 VM 正在使用同一数据库服务器的一种方式。

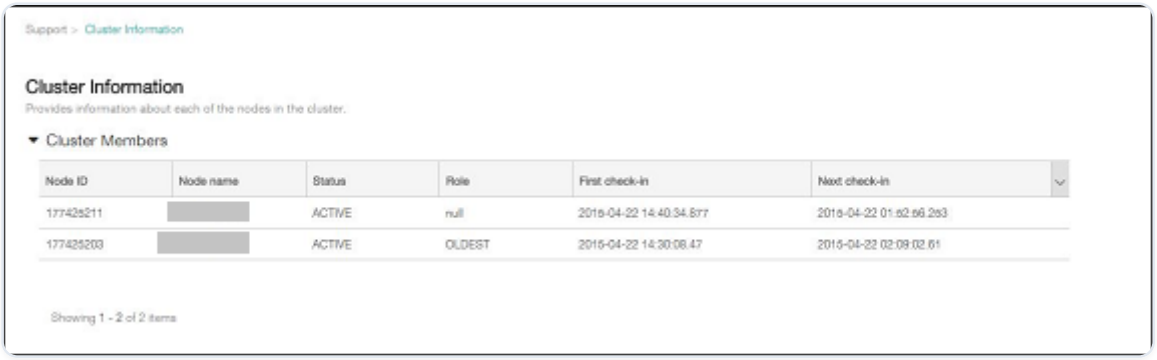
8. 使用 XenMobile 的完全限定域名 (FQDN) 在 Web 浏览器中打开 XenMobile 控制台。
9. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。

支持页面打开。

10. 在**高级**下，单击**群集信息**。



将显示有关群集的所有信息，包括群集成员、设备连接信息、任务等。新节点现在是群集的成员。

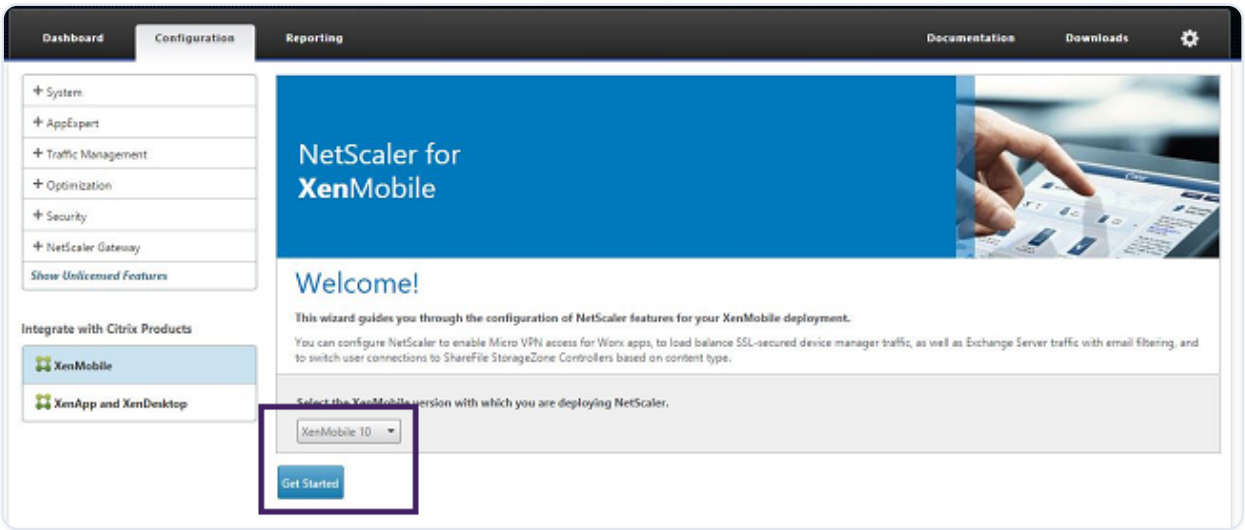


您可以按照相同的步骤添加其他节点。添加到群集的第一个节点的角色为 **OLDEST**。之后添加的节点显示的角色为 **NONE** 或 **null**。

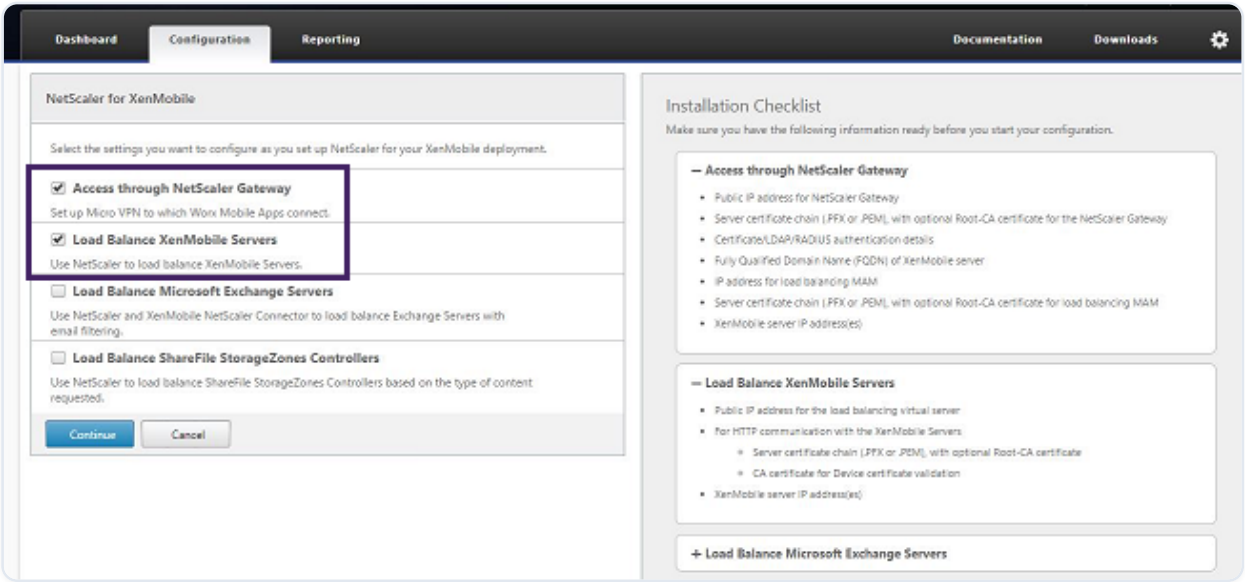
在 Citrix ADC 中为 XenMobile 群集配置负载平衡

将所需节点添加为 XenMobile 群集成员后，对这些节点进行负载平衡，以便您可以访问群集。负载平衡通过运行 Citrix ADC 中提供的 XenMobile 向导来完成。以下步骤介绍了如何通过运行向导对 XenMobile 进行负载平衡。

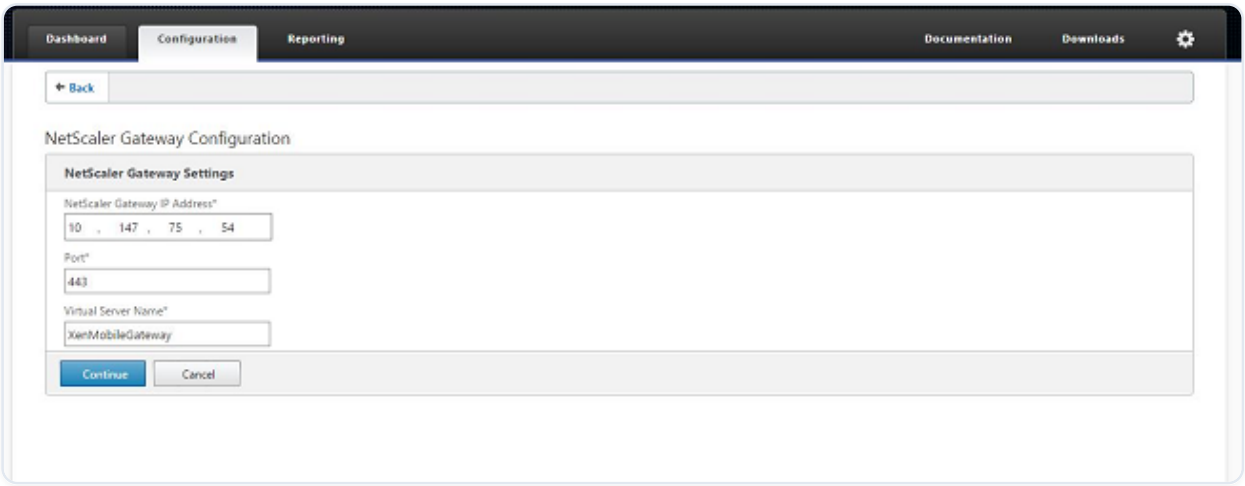
1. 登录到 Citrix ADC。
2. 在“配置”选项卡上，单击 **XenMobile**，然后单击 **Get Started**。



3. 选中 **Access through Citrix Gateway** 复选框和 **Load Balance XenMobile Servers** 复选框，然后单击 **Continue**。



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



5. 通过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**。

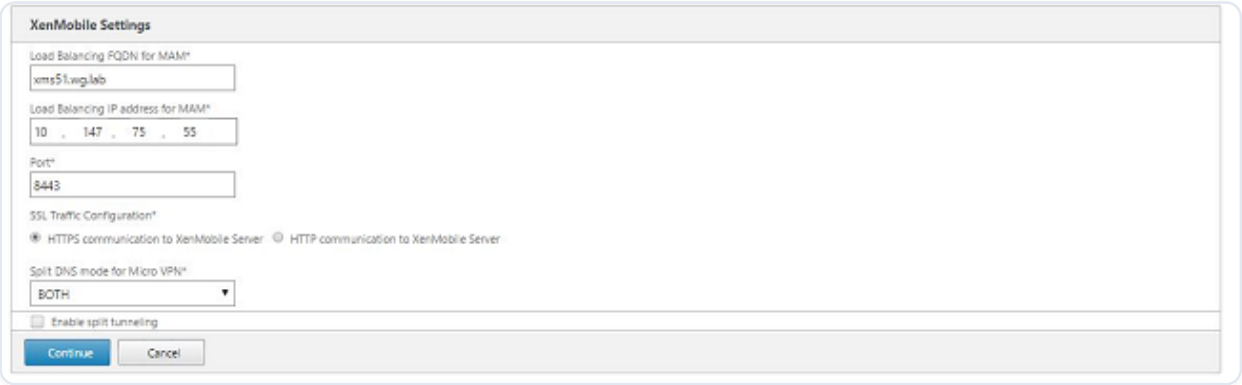
- 在 **Use existing certificate** 中，从列表中选择服务器证书。
- 单击 **Install Certificate** 选项卡以上载新的服务器证书。

6. 输入身份验证服务器详细信息，然后单击 **Continue**。

注意：

确保“服务器登录名属性”与您在 XenMobile LDAP 配置中提供的相同。

7. 在 XenMobile 设置下，输入 MAM 的负载平衡 FQDN，然后单击**继续**。

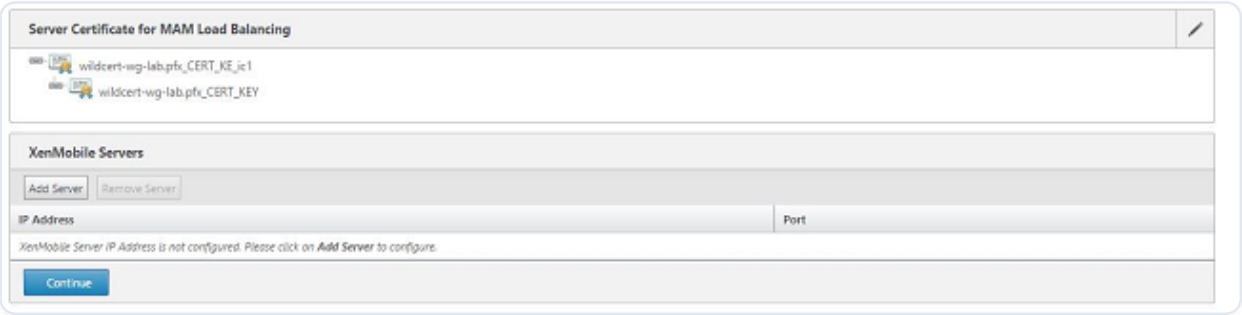


注意：

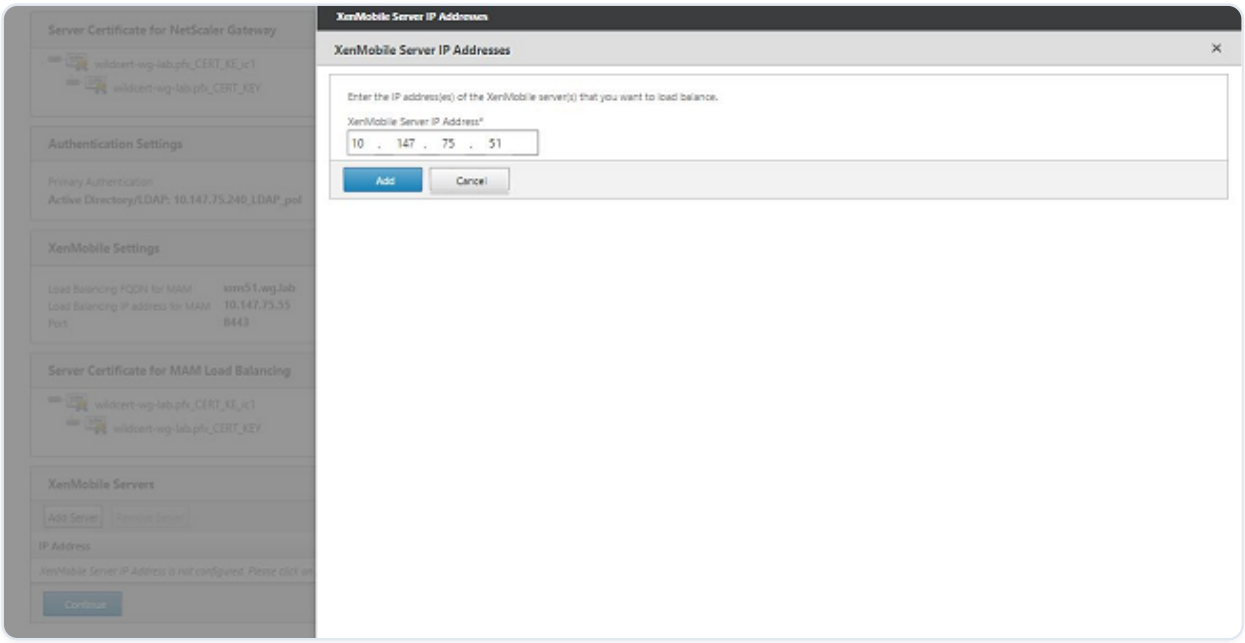
确保 MAM 负载平衡虚拟 IP 地址的 FQDN 与 XenMobile 的 FQDN 相同。

8. 如果要使用 SSL 桥接模式 (HTTPS)，请选择**与 XenMobile Server 的 HTTPS 通信**。但是，如果要使用 SSL 卸载，请选择**与 XenMobile Server 的 HTTP 通信**，如上图所示。就本文而言，选择的是 SSL 桥接模式 (HTTPS)。
9. 绑定 MAM 负载平衡虚拟 IP 地址的服务器证书，然后单击“继续”。

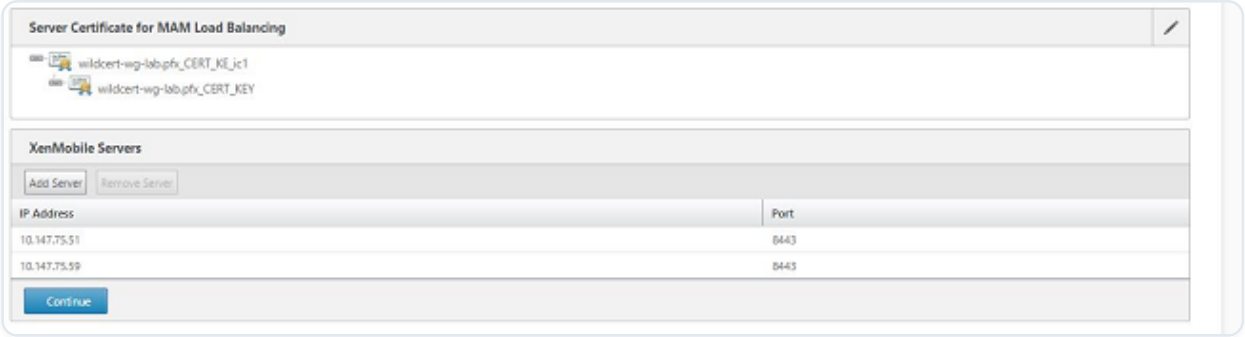
10. 在 XenMobile 服务器下，单击**添加服务器**以添加 XenMobile 节点。



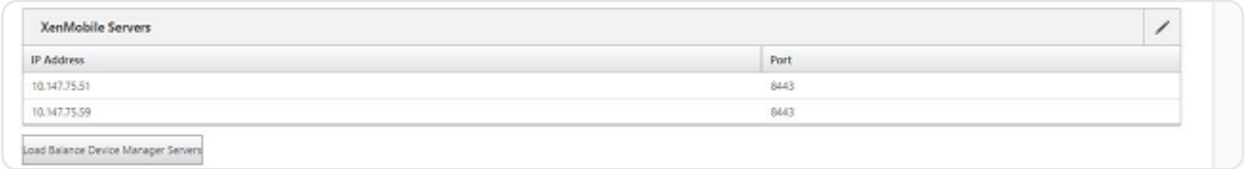
11. 输入 XenMobile 节点的 IP 地址，然后单击“添加”。



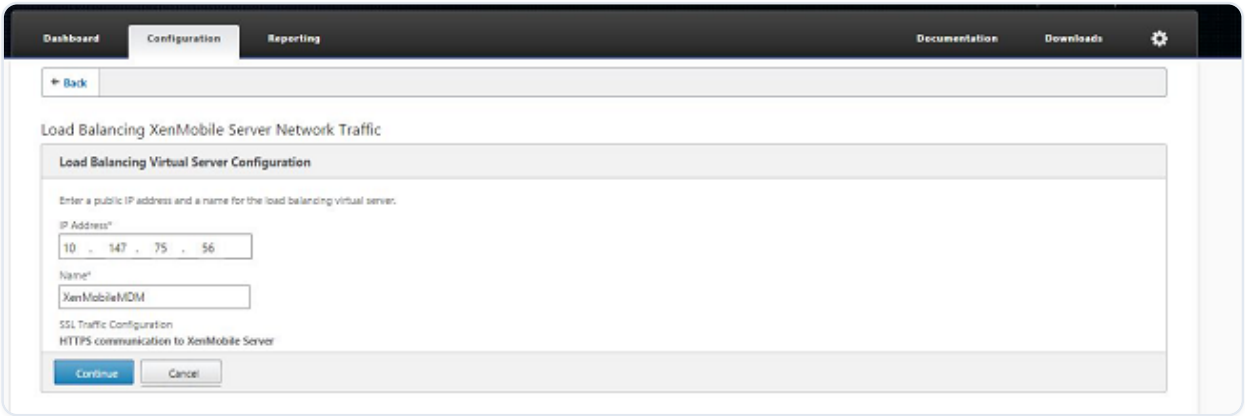
12. 重复步骤 10 和 11 以添加属于 XenMobile 群集的更多 XenMobile 节点。您将看到所有已添加的 XenMobile 节点。单击“继续”。



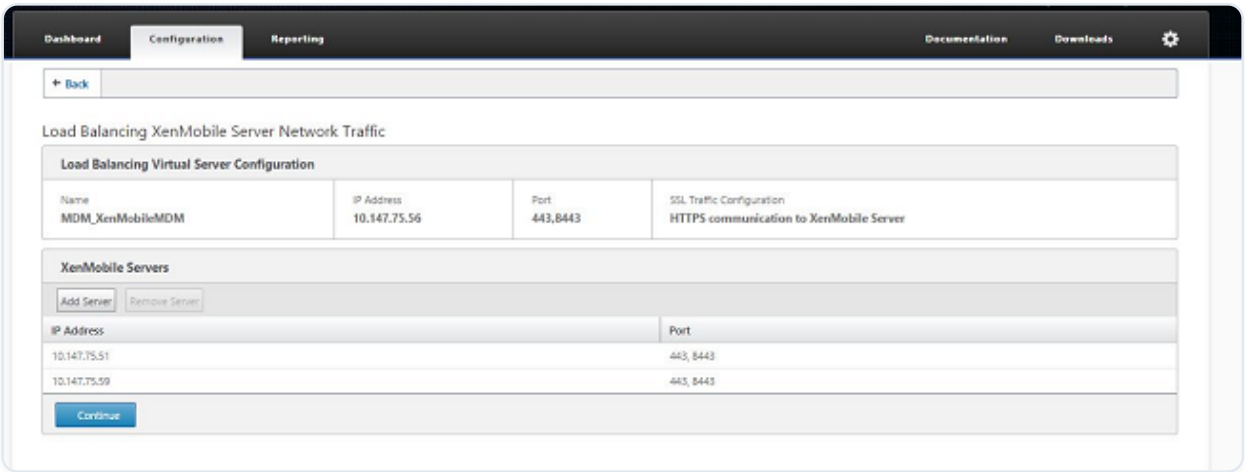
13. 单击**负载平衡设备管理器服务器**以继续 MDM 负载平衡配置。



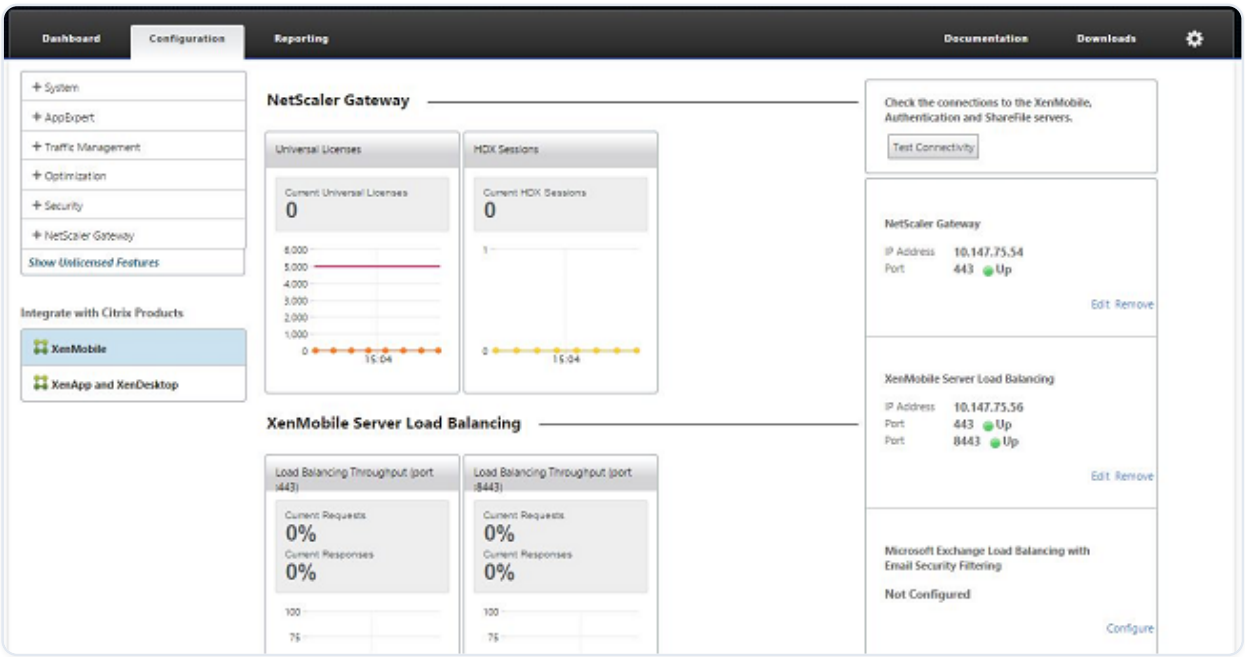
14. 输入用于 MDM 负载平衡 IP 地址的 IP 地址，然后单击**继续**。



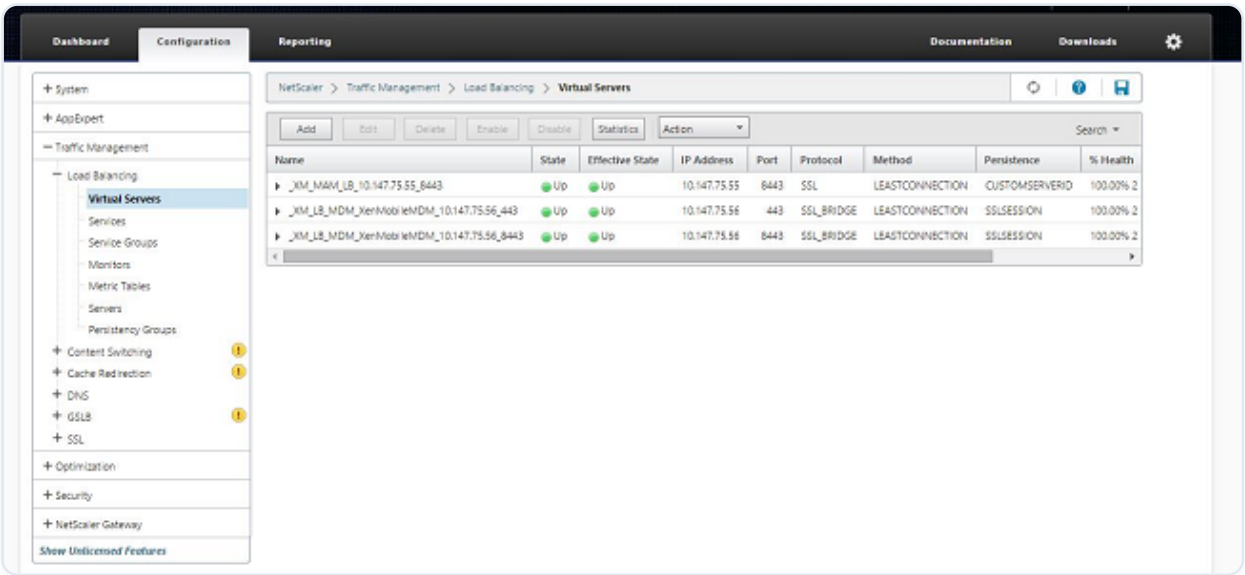
15. 在列表中看到 XenMobile 节点后，单击 **Continue**，然后单击 Done 完成此过程。



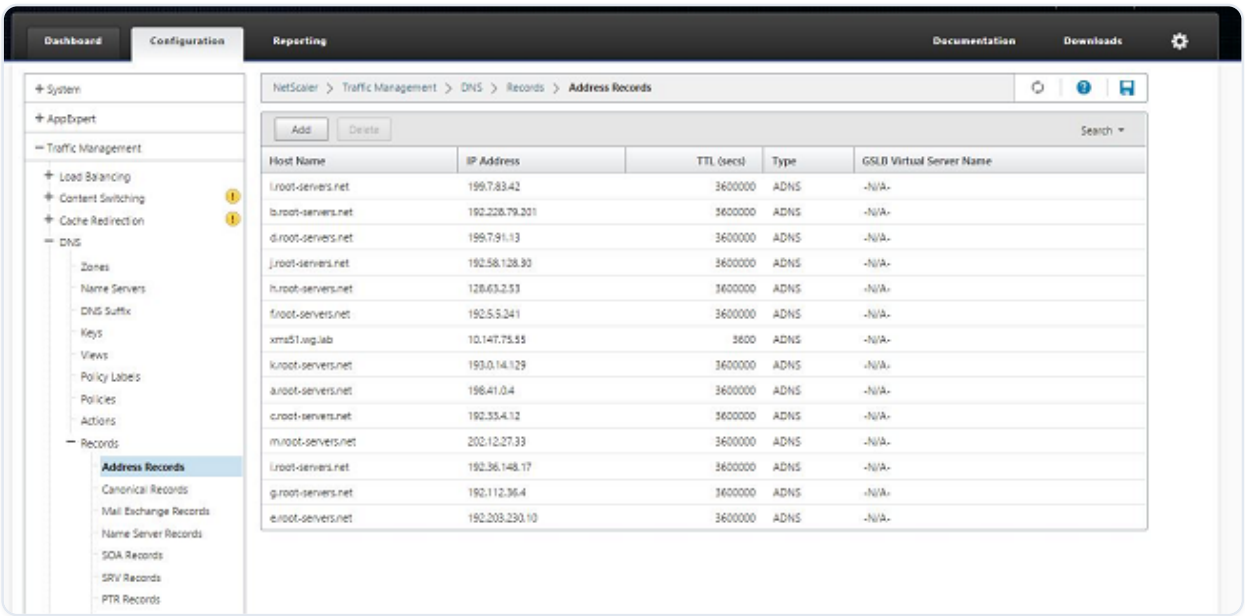
您会看到虚拟 IP 地址状态显示在 XenMobile 页面上。



16. 要确认虚拟 IP 地址是否已启动并正在运行，请单击“Configuration”（配置）选项卡，然后导航到 **Traffic Management > Load Balancing > Virtual Servers**。



您还会看到 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

您可以架构和配置包含多个站点的 XenMobile 部署，以使用主动-被动故障转移策略进行灾难恢复。有关详细信息，请参阅 XenMobile 部署手册中的 灾难恢复 文章。

启用代理服务器

为了控制出站互联网流量，您可以在 XenMobile® 中设置代理服务器来承载该流量。您可以通过命令行界面 (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“系统”菜单。
2. 在“系统”菜单中，键入 **6** 以选择“代理服务器”菜单。

```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----------------------------------
Choice: [0 - 5] 2

-----------------------------------
System Menu
-----------------------------------
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] Admin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----------------------------------
```

3. 在“代理配置”菜单中，键入 **1** 以选择 SOCKS。

   在保存此设置之前，您还必须配置 HTTPS。仅当您在同一配置中保存 SOCKS 和 HTTPS 设置时，代理才起作用。

```
-----------------------------------
Choice: [0 - 10] 6

-----------------------------------
Proxy Configuration Menu
-----------------------------------
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----------------------------------
```

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

带身份验证的 HTTP	Web、PKI
带身份验证的 HTTPS	Web、PKI

代理服务器设置图(/en-us/xenmobile/server/media/proxy-server-setup-3.png)

5. 键入 **n**，然后键入 **2** 以选择 HTTPS。
6. 键入代理服务器 IP 地址、端口号和目标。
7. 如果您选择为代理服务器上的身份验证配置用户名和密码，请键入 **y**，然后键入用户名和密码。

   代理服务器设置图(/en-us/xenmobile/server/media/proxy-server-setup-4.png)
8. 键入 **y** 以保存设置。

配置 SQL Server

对于从本地 XenMobile® Server 到 SQL Server 的连接，可以使用以下任一驱动程序：

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

在以下情况下，jTDS 驱动程序是默认驱动程序：

- 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 都支持 SQL Server 身份验证或 Windows 身份验证。对于这些身份验证和驱动程序的组合，SSL 可以开启或关闭。

当您将 Windows 身份验证与 Microsoft JDBC 驱动程序结合使用时，该驱动程序将使用 Kerberos 进行集成身份验证。XenMobile 会联系 Kerberos 以获取 Kerberos 密钥分发中心 (KDC) 详细信息。如果所需的详细信息不可用，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 连接到所有 XenMobile Server 节点，并使用 XenMobile CLI 进行配置。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 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**。
3. 输入 **12** 以选择高级设置。
4. 输入 **7** 以选择切换 JDBC 驱动程序，然后输入 **m** 表示 Microsoft。

   选择 JDBC 驱动程序的图像(/en-us/xenmobile/server/media/cli-choose-jdbc-driver.png)
5. 出现提示时，输入 **y** 以选择 SQL 身份验证，然后输入 SQL Server 用户名和密码。
6. 对每个 XenMobile Server 节点重复这些步骤。
7. 重新启动每个 XenMobile Server 节点。

切换到 Microsoft JDBC（SSL 已关闭；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，输入 **2** 以选择**系统菜单**。
3. 输入 **12** 以选择高级设置。
4. 输入 **7** 以选择切换 JDBC 驱动程序，然后输入 **m**。
5. 当提示是否使用 SQL Server 身份验证时，输入 **n**。
6. 出现提示时，输入为 SQL Server 配置的 Active Directory 用户名和密码。
7. 如果 XenMobile 未自动发现 Kerberos KDC 领域，它会提示输入 KDC 详细信息，包括 SQL Server FQDN。
8. 当提示是否使用 SSL 时，键入 **n**。XenMobile 会保存配置。如果 XenMobile 因错误而无法保存配置，它会显示错误消息和您输入的详细信息。
9. 对每个 XenMobile Server 节点重复这些步骤。
10. 重新启动每个 XenMobile Server 节点。

更改 XenMobile 数据库密码

请遵循此指南更改 XenMobile 数据库密码，例如当 Citrix 支持部门指示您更改密码时。

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，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。之后，您可以按如下方式在 XenMobile 中更改密码。

> **重要提示：**

- 计划一个预定的维护时段，用于在 XenMobile 中更改数据库密码。密码更改必须在系统停机期间进行。
- 更改密码时，请确保所有 XenMobile 节点都已连接到网络。更改密码后，重新启动 XenMobile。

  如果在更改密码后不重新启动 XenMobile，XenMobile 将进入恢复模式。在这种情况下，请在 SQL Server 中恢复为旧密码，重新启动 XenMobile，然后再次更改密码。

1. 验证所有 XenMobile Server 节点是否正在运行。对于群集环境，请启动所有节点。
2. 通过禁用虚拟服务器，在 Citrix ADC 负载平衡器上阻止传入 XenMobile 的设备流量。
3. 要在 SQL Server 中更改数据库密码：登录到 XenMobile CLI，导航到 **Configuration > Database**，并在出现提示时输入更改后的密码：

   ```
   Server []: <ipAddress>

   Port [1433]: 1433

   Username [sa]: <userName>

   Password: <****>
   ```

4. 选择 **Y** 以重新启动服务器。
5. 对群集中的所有其他节点重复步骤 3 和 4。
6. 通过在 Citrix ADC 负载均衡器上启用虚拟服务器，解除对传入设备流量的阻止。

服务器属性

XenMobile® 具有许多适用于服务器范围操作的属性。本文介绍了许多服务器属性，并详细说明了如何添加、编辑或删除服务器属性。

某些属性是自定义密钥。要添加自定义密钥，请单击**添加**，然后从**密钥**中选择**自定义密钥**。

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

- 如果为 **true**，XenMobile 会将设备添加到 XenMobile 控制台，即使注册失败，以便您可以看到哪些设备尝试注册。默认为 **false**。

AG 客户端证书颁发限制间隔

- 生成证书之间的宽限期。此间隔可防止 XenMobile 在短时间内为设备生成多个证书。Citrix® 建议您不要更改此值。默认为 **30** 分钟。

审核日志清理执行时间

- 开始审核日志清理的时间，格式为 HH:MM AM/PM。示例：04:00 AM。默认为 **02:00 AM**。

审核日志清理间隔（天）

- XenMobile 保留审核日志的天数。默认为 **1**。

审核记录器

- 如果为 **False**，则不记录用户界面 (UI) 事件。默认为 **False**。

审计日志保留（天）

- XenMobile 保留审计日志的天数。默认为 **7**。

auth.ldap.connect.timeout 和 auth.ldap.read.timeout

- 为弥补 LDAP 响应缓慢的问题，Citrix 建议您为以下自定义密钥添加服务器属性。
    - 密钥：**自定义密钥**
    - 密钥：**auth.ldap.connect.timeout**
    - 值：**60000**
    - 显示名称：**auth.ldap.connect.timeout**
    - 描述：**LDAP 连接超时**
    - 密钥：**自定义密钥**
    - 密钥：**auth.ldap.read.timeout**
    - 值：**60000**
    - 显示名称：**auth.ldap.read.timeout**
    - 描述：**LDAP 读取超时**

证书续订（秒）

- 证书过期前 XenMobile 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 日至 12 月 30 日之间连接，XenMobile 会尝试续订证书。默认为 **2592000** 秒（30 天）。

连接超时

- 会话不活动超时（以分钟为单位），在此时间后 XenMobile 会关闭与设备的 TCP 连接。会话保持打开状态。适用于 Android 设备和远程支持。默认为 **5** 分钟。

连接到 Microsoft 证书服务器超时

- XenMobile 等待证书服务器响应的秒数。如果证书服务器速度慢且流量大，请将此值增加到 60 秒或更长时间。如果证书服务器在 120 秒后仍无响应，则需要维护。默认为 **15000** 毫秒（15 秒）。

默认部署通道

- 确定 XenMobile 如何将资源部署到设备：用户级别 (**DEFAULT_TO_USER**) 或设备级别。默认为 **DEFAULT_TO_DEVICE**。

部署日志清理（天）

- XenMobile 保留部署日志的天数。默认为 **7**。

禁用主机名验证

- 默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。当主机名验证失败时，服务器日志会包含以下错误：“无法连接到批量购买服务器：主机名 '192.0.2.0' 与对等方提供的证书主题不匹配”。如果主机名验证导致部署中断，请将此属性更改为 **true**。默认为 **false**。

禁用 SSL 服务器验证

- 如果为 **True**，则在满足以下所有条件时禁用 SSL 服务器证书验证：
  - 您已在 XenMobile Server 上启用基于证书的身份验证。
  - Microsoft CA 服务器是证书颁发者。
  - 内部 CA（其根 XenMobile Server 不信任）签署了您的证书。

默认为 **True**。

启用控制台

- 如果为 **true**，则允许用户访问自助服务门户控制台。默认为 **true**。

启用崩溃报告

- 如果为 **true**，Citrix 会收集崩溃报告和诊断信息，以帮助排查适用于 iOS 和 Android 的 Secure Hub 的问题。如果为 **false**，则不收集任何数据。默认值为 **true**。

启用/禁用 Hibernate 统计信息日志记录用于诊断

- 如果为 **True**，则启用 Hibernate 统计信息日志记录，以帮助排查应用程序性能问题。Hibernate 是用于 XenMobile 连接到 Microsoft SQL Server 的组件。默认情况下，日志记录处于禁用状态，因为它会影响应用程序性能。仅在短时间内启用日志记录，以避免创建巨大的日志文件。XenMobile 将日志写入 /opt/sas/logs/hibernate_stats.log。默认为 **False**。

启用 macOS OTAE

- 如果为 **false**，则阻止将注册链接用于 macOS 设备，这意味着 macOS 用户只能通过注册邀请进行注册。默认为 **true**。

启用通知触发器

- 启用或禁用 Secure Hub 客户端通知。值 **true** 启用通知。默认为 **true**。

force.server.push.required.apps

- 启用在 Android 和 iOS 设备上强制部署所需应用程序，例如在以下情况下：
  - 您上传了一个新应用程序并将其标记为必需。
  - 您将现有应用标记为必需。
  - 用户删除必需应用时。
  - Secure Hub 更新可用。

默认情况下，必需应用的强制部署为 **false**。创建自定义密钥并将 **Value** 设置为 **true** 以启用强制部署。在强制部署期间，启用 MDX 的必需应用（包括企业应用和公共应用商店应用）会立即升级。即使您为应用更新宽限期配置了 MDX 策略，并且用户选择稍后升级应用，也会发生升级。

- 密钥：**自定义密钥**
- 密钥：**force.server.push.required.apps**
- 值：**false**
- 显示名称：**force.server.push.required.apps**

- 描述：**强制部署必需应用**

完全拉取 ActiveSync 允许和拒绝的用户

- XenMobile 拉取 ActiveSync 允许和拒绝用户的完整列表（基线）的间隔（以秒为单位）。默认为 **28800** 秒。

hibernate.c3p0.idle_test_period

- 此 XenMobile Server 属性（自定义密钥）确定连接自动验证前的空闲时间（以秒为单位）。按如下方式配置密钥。默认值为 **30**。
- 密钥：**自定义密钥**
- 密钥：**hibernate.c3p0. idle_test_period**
- 值: **30**
- 显示名称: **hibernate.c3p0. idle_test_period =*nnn***
- 描述: **Hibernate 空闲测试周期**

hibernate.c3p0.max_size

- 此自定义密钥确定 XenMobile 可以打开到 SQL Server 数据库的最大连接数。XenMobile 将为此自定义密钥指定的值用作上限。仅在需要时才打开连接。根据数据库服务器的容量设置。有关详细信息，请参阅调整 XenMobile 操作。按如下方式配置密钥。默认值为 **1000**。
- 密钥: **hibernate.c3p0.max_size**
- 值: **1000**
- 显示名称: **hibernate.c3p0.max_size**
- 描述: **到 SQL 的数据库连接**

hibernate.c3p0.min_size

- 此自定义密钥确定 XenMobile 打开到 SQL Server 数据库的最小连接数。按如下方式配置密钥。默认值为 **100**。
- 密钥: **hibernate.c3p0.min_size**
- 值: **100**
- 显示名称: **hibernate.c3p0.min_size**
- 描述: **到 SQL 的数据库连接**

hibernate.c3p0.timeout

- 此自定义密钥确定空闲超时（以秒为单位）。默认值为 **120**。
- 密钥：**自定义密钥**
- 密钥：**hibernate.c3p0.timeout**
- 值：**120**
- 显示名称：**hibernate.c3p0.timeout**
- 描述：**数据库空闲超时**

标识是否启用遥测

- 标识是否启用遥测（客户体验改善计划，即 CEIP）。您可以在安装或升级 XenMobile 时选择加入 CEIP。如果 XenMobile 连续 15 次上传失败，它将禁用遥测。默认为 **false**。

不活动超时（分钟）

- 如果 **WebServices timeout type** 服务器属性为 **INACTIVITY_TIMEOUT**：此属性定义 XenMobile 在以下情况下注销不活动管理员的分钟数：
  - 使用 XenMobile 公共 API for REST Services 访问 XenMobile 控制台
  - 使用 XenMobile 公共 API for REST Services 访问任何第三方应用程序。超时设置为 **0** 表示不活动用户仍处于登录状态。

默认为 **5**。

启用 iOS 设备管理注册自动安装

- 如果为 true，此属性会减少设备注册期间所需的用户交互量。用户必须单击“**根 CA 安装**”（如果需要）和“**MDM 配置文件安装**”。

iOS 设备管理注册第一步延迟

- 用户在设备注册期间输入其凭据后，此值指定在提示根 CA 之前等待的时间。Citrix 建议您仅在出现网络延迟或速度问题时编辑此属性。在这种情况下，请勿将值设置为超过 5000 毫秒（5 秒）。默认为 **1000** 毫秒（1 秒）。

iOS 设备管理注册最后一步延迟

- 在设备注册期间，此属性值指定在安装 MDM 配置文件和在设备上启动代理之间等待的时间。Citrix 建议您仅在出现网络延迟或速度问题时编辑此属性。在这种情况下，请勿将值设置为超过 5000 毫秒（5 秒）。默认为 **1000** 毫秒（1 秒）。

iOS 设备管理身份交付模式

- 指定 XenMobile 是使用 **SCEP**（出于安全原因推荐）还是 **PKCS12** 将 MDM 证书分发到设备。在 PKCS12 模式下，密钥对在服务器上生成，不进行协商。默认为 **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 代理身份的私钥大小。默认为 **1024**。

iOS 设备管理身份续订天数

- 指定在证书过期前 XenMobile 开始续订证书的天数。例如：如果证书在 10 天内过期，并且此属性为 **10** 天，则当设备在过期前 9 天连接时，XenMobile 会颁发新证书。默认为 **30** 天。

iOS MDM APNS 私钥密码

- 此属性包含 APNs 密码，XenMobile 需要此密码才能将通知推送到 Apple 服务器。

设备断开连接前的非活动时长

- 指定设备在 XenMobile 断开连接之前可以保持非活动状态（包括上次身份验证）的时长。默认为 **7** 天。

MAM 专用设备最大数量

- 此自定义密钥限制了每个用户可以注册的仅限 MAM 设备的数量。按如下方式配置密钥。**值**为 **0** 允许无限数量的设备注册。
- 密钥 = **number.of.mam.devices.per.user**
- 值 = **5**
- 显示名称 = **MAM Only Device Max**
- 描述 = **限制每个用户可以注册的 MAM 设备数量。**

最大工作线程数

- 导入大量批量购买许可证时使用的线程数。默认为 **3**。如果需要进一步优化，可以增加线程数。但是，如果线程数较大（例如 6 个），批量购买导入会导致 CPU 使用率过高。

Citrix ADC 单点登录

- 如果为 **False**，则在从 Citrix ADC 到 XenMobile 的单点登录期间禁用 XenMobile 回调功能。如果 Citrix Gateway 配置包含回调 URL，XenMobile 将使用回调功能验证 Citrix Gateway 会话 ID。默认为 **False**。

连续失败上传次数

- 显示客户体验改善计划 (CEIP) 上传期间连续失败的次数。上传失败时，XenMobile 会增加此值。15 次上传失败后，XenMobile 将禁用 CEIP（也称为遥测）。有关详细信息，请参阅服务器属性 **Identifies if telemetry is enabled or not**。上传成功时，XenMobile 会将此值重置为 **0**。

每设备用户数

- 可以在 MDM 中注册同一设备的最大用户数。值 **0** 表示无限数量的用户可以注册同一设备。默认为 **0**。

允许和拒绝用户的增量更改拉取

- XenMobile 在运行 PowerShell 命令以获取 ActiveSync 设备的增量时，等待域响应的秒数。默认为 **60** 秒。

读取 Microsoft 证书服务器超时

- XenMobile 在执行读取操作时，等待证书服务器响应的秒数。如果证书服务器速度慢且流量大，您可以将此值增加到 60 秒或更长时间。如果证书服务器在 120 秒后仍无响应，则需要维护。默认为 **15000** 毫秒（15 秒）。

REST Web 服务

- 启用 REST Web 服务。默认为 **true**。

按指定大小分块检索设备信息

- 此值在设备导出期间用于内部多线程处理。如果值较高，则单个线程解析更多设备。如果值较低，则更多线程获取设备。减小此值可能会提高导出和设备列表获取的性能，但可能会减少可用内存。默认为 **1000**。

会话日志清理（天）

- XenMobile 保留会话日志的天数。默认为 **7**。

服务器模式

- 确定 XenMobile 是在 MAM、MDM 还是 ENT（企业）模式下运行，分别对应应用程序管理、设备管理或应用程序和设备管理。根据您希望设备注册的方式设置服务器模式属性，如下表所示。无论许可证类型如何，服务器模式默认为 **ENT**。

如果您拥有 XenMobile MDM Edition 许可证，则无论您在 **服务器属性** 中如何设置服务器模式，有效的服务器模式始终为 MDM。如果您拥有 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。

您的许可证版本	您希望设备以这种模式注册	将服务器模式属性设置为
企业版 / 高级版	MDM 模式	MDM
企业版 / 高级版	MDM+MAM 模式	ENT
MDM	MDM 模式	MDM

有效的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，无论服务器模式设置如何，有效的服务器模式始终为 MDM。对于企业版和高级版许可证，如果服务器模式为 **ENT** 或 **MDM**，则有效的服务器模式与服务器模式匹配。如果服务器模式为 **MAM**，则有效的服务器模式为 ENT。

XenMobile 会将服务器模式添加到以下每个活动的服务器日志中：激活许可证、删除许可证以及在 **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。

ShareFile 配置类型

- 指定 Citrix Files 存储类型。**ENTERPRISE** 启用 Citrix Files 企业模式。**CONNECTORS** 仅提供对通过 XenMobile 控制台创建的存储区域连接器的访问权限。默认为 **NONE**，这将显示 **配置 > ShareFile** 屏幕的初始视图，您可以在其中选择 Citrix Files Enterprise 和连接器。默认为 **NONE**。

静态超时（分钟）

- 如果 **WebServices 超时类型** 服务器属性为 **STATIC_TIMEOUT**：此属性定义了 XenMobile 在使用以下内容后将管理员注销的分钟数：
  - XenMobile 公共 API，用于 REST 服务访问 XenMobile 控制台。
  - XenMobile 公共 API，用于 REST 服务访问任何第三方应用程序。

默认为 **60**。

触发代理消息抑制

- 启用或禁用 Secure Hub 客户端消息传送。值 **false** 启用消息传送。默认为 **true**。

触发代理声音抑制

- 启用或禁用 Secure Hub 客户端声音。值 **false** 启用声音。默认为 **true**。

Android 设备的未经验证应用程序下载

- 如果为 **True**，则可以将自托管应用程序下载到运行 Android Enterprise 的 Android 设备。如果启用了 Android Enterprise 选项以在 Google Play 商店中静态提供下载 URL，则 XenMobile 需要此属性。在这种情况下，下载 URL 不能包含具有身份验证令牌的一次性票证（由 **XAM One-Time Ticket server** 属性定义）。默认为 **False**。

Windows 设备的未经验证应用程序下载

- 仅用于不验证一次性票证的旧版 Secure Hub。如果为 **False**，则可以从 XenMobile 下载未经验证的应用程序到 Windows 设备。默认为 **False**。

使用 ActiveSync ID 执行 ActiveSync 设备擦除

- 如果为 **true**，则用于 Exchange ActiveSync 的 Endpoint Management 连接器将 ActiveSync 标识符用作 asWipeDevice 方法的参数。默认为 **false**。

仅来自 Exchange 的用户

- 如果为 **true**，则禁用 ActiveSync Exchange 用户的用户身份验证。默认为 **false**。

VP 基线间隔

- XenMobile 从 Apple 重新导入批量采购许可证的最小间隔。刷新许可证信息可确保 XenMobile 反映所有更改，例如当您手动从批量采购中删除导入的应用程序时。默认情况下，XenMobile 至少每 **720** 分钟刷新一次批量采购许可证基线。

如果您安装了大量批量采购许可证（例如，超过 50,000 个）：Citrix 建议您增加基线间隔，以减少导入许可证的频率和开销。

如果您预计 Apple 会频繁更改批量采购许可证：Citrix 建议您降低该值，以使 XenMobile 及时更新这些更改。两个基线之间的最小间隔为 60 分钟。此外，XenMobile 每 60 分钟执行一次增量导入，以捕获自上次导入以来的更改。因此，如果批量采购基线间隔为 60 分钟，则基线之间的间隔可能会延迟长达 119 分钟。

Web 服务超时类型

- 指定如何使从公共 API 检索到的身份验证令牌过期。如果为 **STATIC_TIMEOUT**，则 XenMobile 会在服务器属性 **Static Timeout in Minutes** 中指定的值之后将身份验证令牌视为已过期。

如果为 **INACTIVITY_TIMEOUT**，则 XenMobile 会在令牌不活动达到服务器属性 **Inactivity Timeout in Minutes** 中指定的值之后将身份验证令牌视为已过期。默认为 **STATIC_TIMEOUT**。

Windows WNS 通道 - 续订前天数

- ChannelURI 的续订频率。默认为 **10** 天。

Windows WNS 心跳间隔

- XenMobile 在每三分钟连接设备五次后，再次连接设备之前等待的时间。默认为 **6** 小时。

XAM 一次性票证

- 一次性身份验证令牌 (OTT) 在下载应用程序时有效的毫秒数。此属性与属性 **Unauthenticated App download for Android** 和 **Unauthenticated App download for Windows** 协同工作。这些属性指定是否允许未经身份验证的应用程序下载。默认为 **3600000**。

XenMobile MDM 自助服务门户控制台最大不活动间隔（分钟）

- XenMobile 在指定分钟数后将不活动用户从 XenMobile 自助服务门户注销。超时设置为 **0** 表示不活动用户保持登录状态。默认为 **30**。

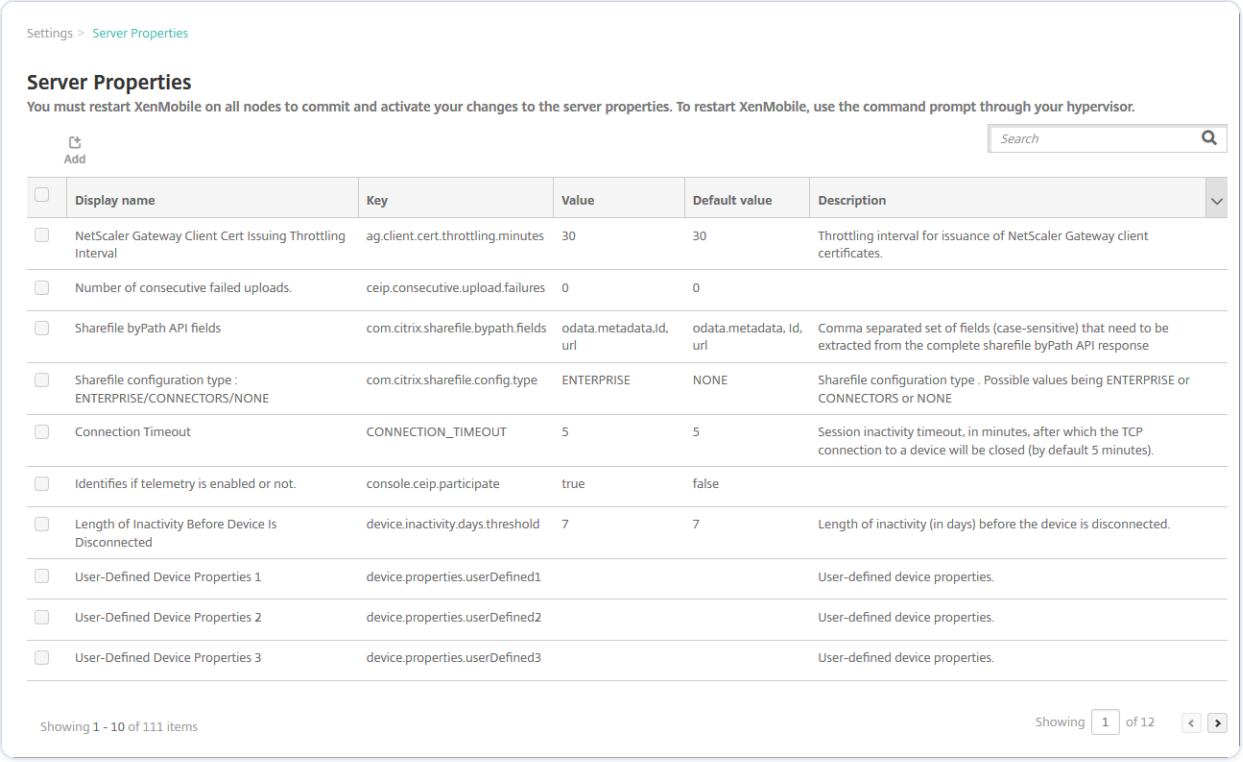
添加、编辑或删除服务器属性

在 XenMobile 中，您可以将属性应用于服务器。进行更改后，请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，请通过您的虚拟机管理程序使用命令提示符。

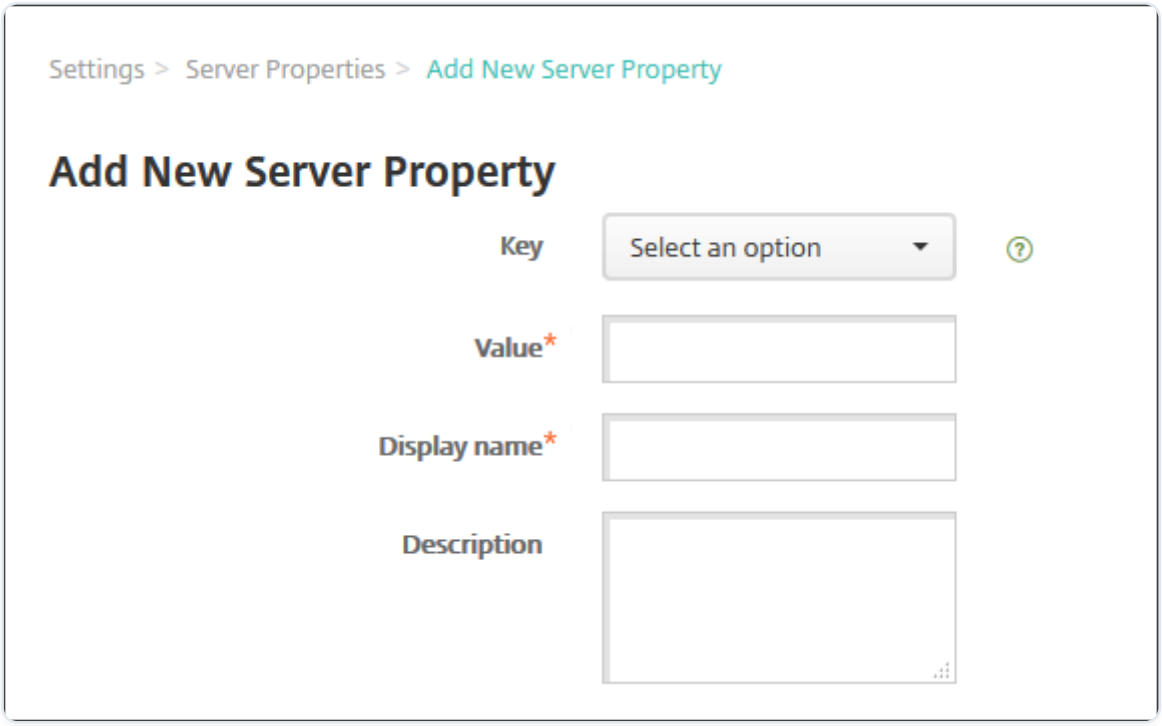
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示“**设置**”页面。
2. 在“**服务器**”下，单击“**服务器属性**”。此时将显示“**服务器属性**”页面。您可以从此页面添加、编辑或删除服务器属性。



Display name	Key	Value	Default value	Description
NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata,Id, url	odata.metadata, Id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE
Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

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，选择相应的密钥。密钥区分大小写。在编辑属性值或请求特殊密钥之前，请联系 Citrix 支持。
   - 值：根据您选择的密钥输入一个值。

- 显示名称：为显示在“**服务器属性**”表中的新属性值输入一个名称。
- 描述：可选，为新的服务器属性键入描述。

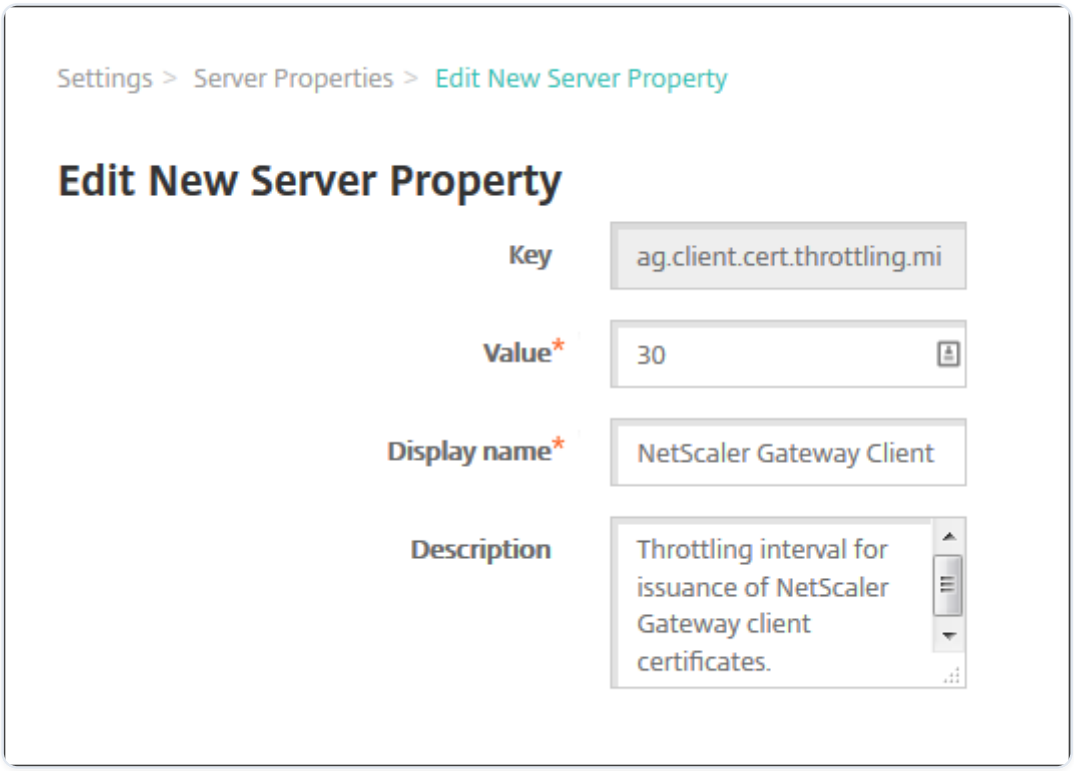
3. 点击**保存**。

编辑服务器属性

1. 在**服务器属性**表中，选择要编辑的服务器属性。

   当您选择服务器属性旁边的复选框时，选项菜单会显示在服务器属性列表上方。在列表中的其他任意位置单击，以打开列表右侧的选项菜单。

2. 点击**编辑**。此时将显示**编辑新服务器属性**页面。



3. 根据需要更改以下信息：

   - 键：您无法更改此字段。
   - 值：属性值。
   - 显示名称：属性名称。
   - 描述：属性描述。

4. 点击**保存**以保存更改，或点击**取消**以使属性保持不变。

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。

您可以通过选择每个属性旁边的复选框来选择多个要删除的属性。

2. 点击 **删除**。出现确认对话框。再次点击 **删除**。

命令行界面选项

对于 XenMobile® Server 的本地部署安装，您可以通过以下方式访问 CLI 选项：

- **从安装了 XenMobile 的管理程序中：** 在您的管理程序中，选择导入的 XenMobile 虚拟机，启动命令提示符视图，然后登录到您的 XenMobile 管理员帐户。有关详细信息，请参阅您的管理程序文档。
- **如果您的防火墙中启用了 SSH，则通过 SSH：** 登录到您的 XenMobile 管理员帐户。

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

```
-----------------------------------
Main Menu
-----------------------------------
[0] Configuration
[1] Clustering
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----------------------------------
```

配置选项

以下是**配置菜单**的示例以及每个选项显示的设置。

```
-----------------------------------
Configuration Menu
-----------------------------------
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----------------------------------
```

网络

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  IP address [10.207.87.75]:10.200.87.75
  Netmask [255.255.254.0]:255.255.254.0
  Default gateway [10.207.86.1]:10.200.86.1
  Primary DNS server [10.207.86.50]:10.200.86.50
  Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]:
```

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...
```

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]:
```

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

以下是**群集菜单**的示例以及每个选项显示的设置。

```
-----------------------------------
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
-----------------------------------
```

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
```

启用/禁用群集

当您选择启用群集时，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.`.

当您选择禁用群集时，将显示以下消息：

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

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:
```

启用或禁用 SSL 卸载

当您选择启用或禁用 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.`.

显示 Hazelcast 群集

当您选择显示 Hazelcast 群集时，将显示以下选项：

Hazelcast 群集成员：

> **注意：**
>
> 如果配置的节点不属于群集，请重新启动该节点。

系统选项

在“**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“**高级设置**”。

```
-----------------------------------
System Menu
-----------------------------------
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----------------------------------
```

“设置 NTP 服务器”使您能够指定 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。更改此选项后，请重新启动所有群集服务器。

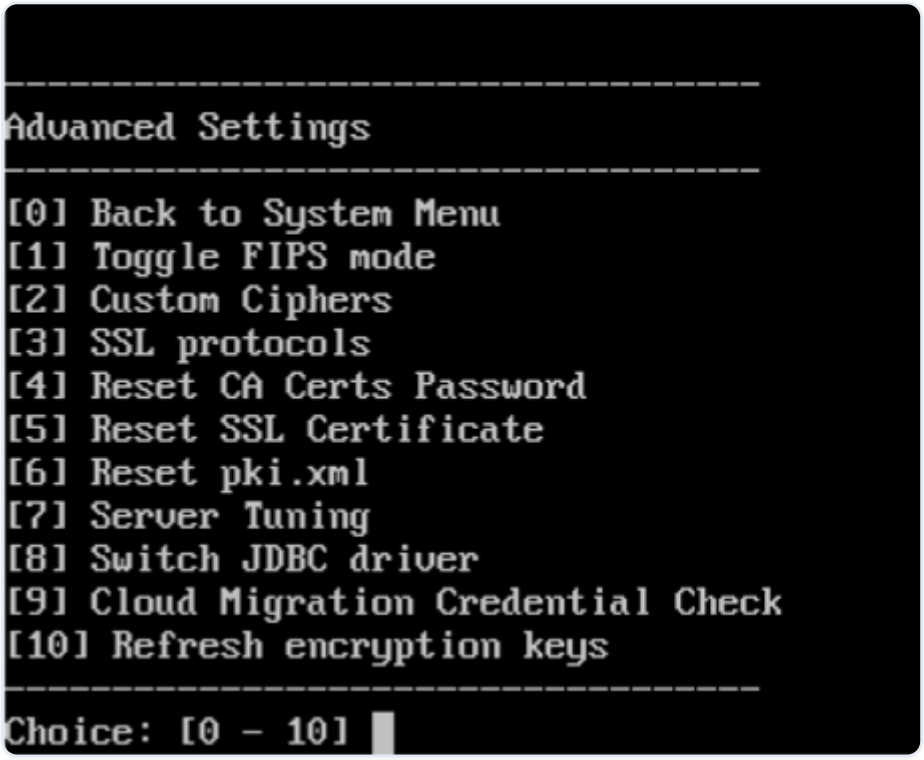
您还可以通过查看“ **显示系统磁盘使用情况**”菜单项来检查磁盘空间。

关于关闭服务器节点

当您关闭群集中的单个服务器节点时，如果其他节点满足 可扩展性和性能 中记录的要求，它们通常可以处理工作负载。影响可能因同时关闭的节点数量、用户总数以及节点关闭时间长短而异。

- 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，用户仍然可以访问和启动已部署的托管应用程序。连接可能会变慢，导致设备签入速度变慢。
- 除非所有节点都已关闭，否则设备策略将继续运行。根据资源和设备数量，策略部署可能会变慢。

高级设置



SSL 协议选项默认为所有允许的协议。在提示**要启用的新 SSL 协议**后，键入要启用的协议。XenMobile 将禁用您未在响应中包含的任何协议。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。

服务器优化选项包括服务器连接超时、最大连接数（按端口）和最大线程数（按端口）。

切换 JDBC 驱动程序选项包括 **jTDS** 和 **Microsoft** JDBC。默认驱动程序是 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

以下是**故障排除菜单**的示例以及每个选项显示的设置。

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

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
-----------------------------------
```

日志

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

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
-----------------------------------
```

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
```

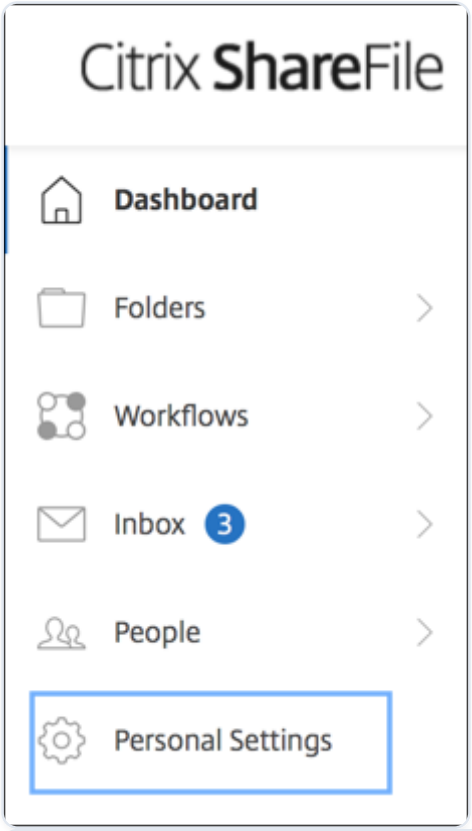
使用 Citrix Files 作为 FTP 站点上传支持包

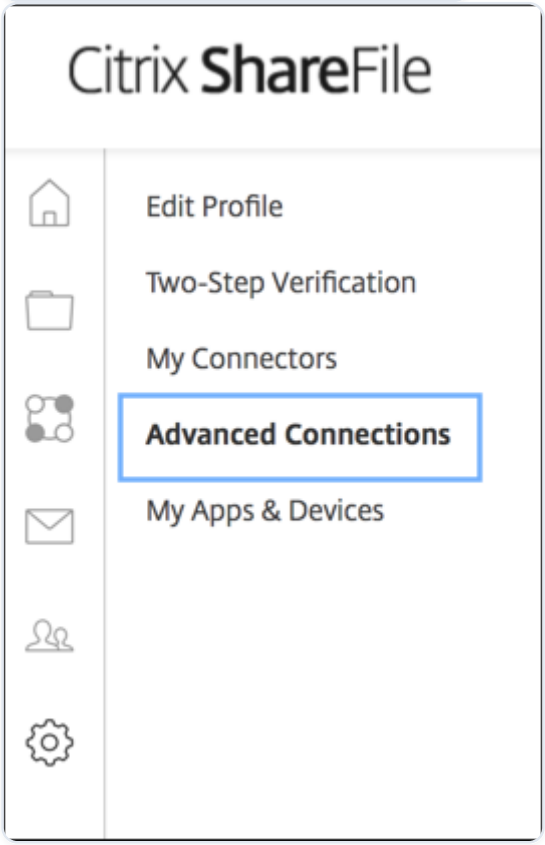
在开始上传支持包之前，请在 Citrix Files 上配置以下先决条件：

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”，验证是否显示字母数字用户 ID 以及默认的子域/用户名详细信息。

You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the **/** and **@** characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

Detailed Set-up Instructions

FTP Server Information

Security:	Standard (Port 21) or Implicit SSL/TLS (Port 990)
FTP Server:	citrite.sharefileftp.com
User name:	.com *or*
Password:	*(your ShareFile password)*

Both secure and standard FTP are enabled for your account.

注意：

- 您从 XenMobile 上传的文件是基于 Linux CLI 的 FTP 客户端。因此，您不能输入反斜杠 (\) 和 @ 符号字符作为用户名的一部分。
- 如果您没有看到字母数字用户 ID，可以向您的 ShareFile 管理员或 ShareFile 支持请求此用户 ID。

2. 验证 Citrix Files 服务器是否已启用 FTP 通信以及 FTPS。理想情况下，ShareFile 管理员允许用户帐户开放 FTP 通信。但是，有时只允许 FTPS 通信。

   具有管理员权限的用户可以通过单击 **Settings** > **Admin Settings** > **Advanced Preferences** > **Enable ShareFile Tools** 来验证并启用此设置。在 **External Apps** > **FTP Access** 中，验证是否已选中 **Enable** 复选框。

   Citrix Files 启用复选框(/en-us/xenmobile/server/media/sharefile-externaltools-ftp.png)

3. 为 FTP 客户端创建一个共享文件夹，用作文件上传目录。单击 **Home**，单击 **Folders**，然后单击 **Personal Folders**。

4. 在最右侧，单击加号 (+) 图标，单击 **Create Folder**，然后输入文件夹名称。

   Citrix Files 共享文件夹对话框(/en-us/xenmobile/server/media/sharefile-create-sharedfolder.png)

5. 在 XenMobile Server CLI 中，在**主菜单**上，选择**故障排除 > 支持包**。然后，在**支持包菜单**上，选择**生成支持包**。

   命令行选项(/en-us/xenmobile/server/media/sharefile-ftp-cli-options.png)

> **注意：**
>
> 如果支持包已存在，在出现提示时，键入 **y** 以覆盖该包。

6. 将支持包上传到 FTP 服务器：

   a. 选择**使用 FTP 上传支持包**。

   b. **输入远程主机：** 出现提示时，键入您的 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：** 出现提示时，键入字母数字用户 ID。

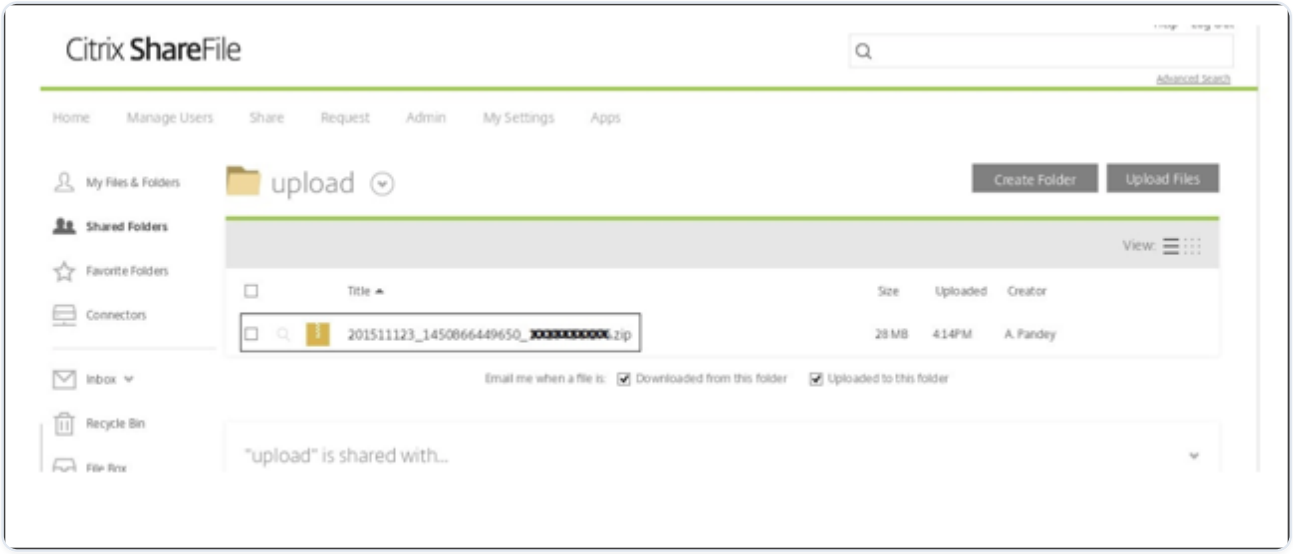
   d. **输入远程用户密码：** 出现提示时，输入您的密码。

   e. **输入远程目录：** 出现提示时，输入您在 Citrix Files 中创建的共享文件夹名称，然后按 **Enter**。

```
-----------------------------------
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
-----------------------------------
Choice: [0 - 3] 3

Current support bundle: 201511123_1450866449650_[redacted]zip

Enter remote host: [redacted].sharefileftp.com
Enter remote user name: [redacted]
Enter remote user password:
Enter remote directory
(Note: Do not use ftp://, http:// or host name. Path should be relative to ftp r
oot location.):/upload
```

```
Connected to ec[redacted]eu-west-1.compute.[redacted].com.
Remote system type is UNIX.
230-Connection established from (unknown) [[redacted]
230-You are connected as [redacted] ([redacted]itrix
.com).
230 Welcome to the [redacted] Test Account FTP site.
250 "/upload" is the current directory.
125 Data connection open; transfer starting.
226-Received 29050517 bytes.
226 Transfer Complete.
29050517 bytes sent in 16.3 seconds (1779137 bytes/s)
221-Sent: 550 bytes   Rcvd: 29,050,639 bytes   Billable: 1 operations   Time: 27
s
```

您可以在 Citrix Files 中创建的共享文件夹中查看上传的支持包。



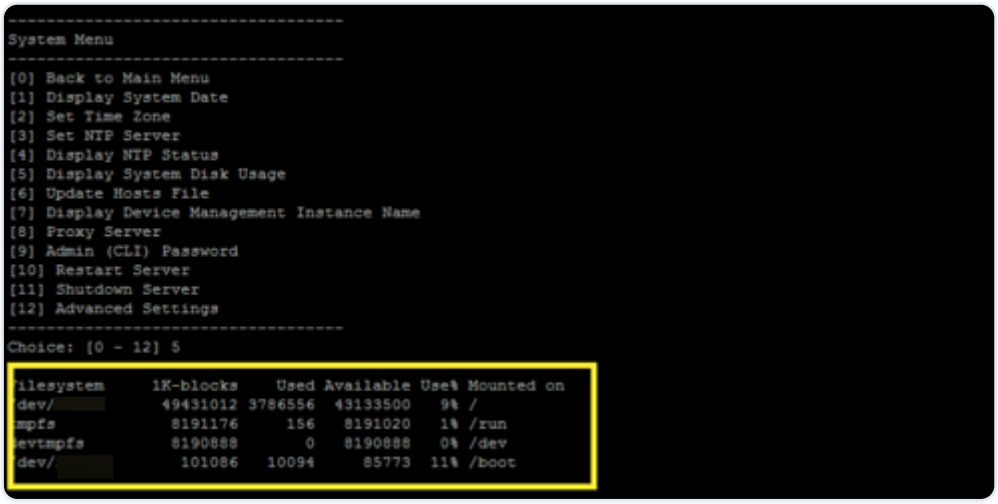
有关 Citrix Files FTP 的更多信息，请参阅此 Citrix 支持知识中心文章。

检查磁盘空间

您可以在 CLI 中按如下方式检查系统磁盘空间：

1. 在主菜单上，选择 **System** 菜单。
2. 在 **System** 菜单中，选择 **Display System Disk Usage** 选项。

   文件系统信息随即显示。



执行自助磁盘清理

您可以在 CLI 中按如下方式清理磁盘：

1. 在 **Troubleshooting** 菜单上，选择 **Disk Usage**。**Disk Usage** 列表包含以下选项：

```
-----------------------------------
Disk Usage Menu (Core dump and Support Bundle)
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Display Disk Usage
[2] Clean
-----------------------------------
Choice: [0 - 2] 1

No core dump and support bundle found.
```

2. 输入 1 以列出核心转储文件和支持包文件类型。如果没有文件存在，您会收到以下消息：**未找到核心转储和支持包。**
3. 输入 2 以清理扫描的核心转储文件和支持包文件。

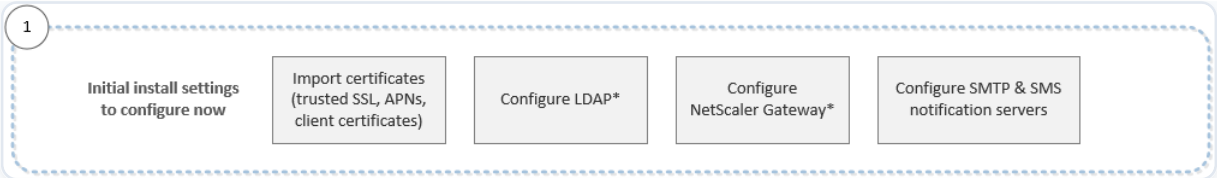
XenMobile® 控制台入门工作流程

XenMobile 控制台是 XenMobile 中的统一管理工具。本文假设您已安装 XenMobile 并准备好在控制台中工作。如果您尚未安装 XenMobile，请参阅 安装 XenMobile。有关 XenMobile 控制台浏览器支持的详细信息，请参阅 XenMobile 兼容性文章。

初始设置工作流程

在命令行控制台和 XenMobile 控制台中完成 XenMobile 的配置后，将打开仪表板。您无法返回到初始配置屏幕。如果您跳过了一些安装配置，则可以在控制台中配置以下设置。在开始添加用户、应用程序和设备之前，请考虑完成这些安装设置。要开始，请单击控制台右上角的齿轮图标。

> **注意：**
>
> 带星号的项目是可选的。



有关每个设置的更多信息以及分步过程，请参阅以下 Citrix 产品文档文章和部分：

- 身份验证
- 思杰网关 和 XenMobile

- 通知

为了支持 Android、iOS 和 Windows 平台，您必须进行以下帐户相关设置。

安卓

- 创建 Google Play 凭据。有关详细信息，请参阅 Google Play 启动。
- 创建 Android Enterprise 管理员帐户。有关详细信息，请参阅 Android Enterprise。
- 使用 Google 验证您的域名。有关详细信息，请参阅 Verify your domain for Google Workspace 。
- 为 Android Enterprise 启用 API 并创建服务帐户。有关详细信息，请参阅 Android Enterprise Help。

iOS

- 创建 Apple ID 和开发者帐户。有关详细信息，请参阅 Apple Developer Program 网站。
- 创建 Apple 推送通知服务 (APNs) 证书。如果您计划使用 XenMobile Server 部署管理 iOS 设备，则需要 Apple APNs 证书。如果您将推送通知用于 Secure Mail 部署，则还需要 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 的更多信息，请参阅 APNs certificates 和 Push Notifications for Secure Mail for iOS。
- 创建批量购买公司令牌。有关详细信息，请参阅 Apple Volume Purchasing Program。

视窗

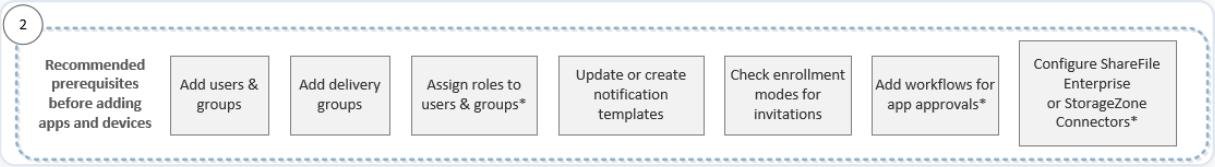
- 创建 Microsoft Windows 应用商店开发者帐户。有关详细信息，请参阅 Account types, locations, and fees。
- 获取 Microsoft Windows 应用商店发布者 ID。有关详细信息，请参阅 Manage account settings and profile info。
- 如果您计划将 XenMobile AutoDiscovery 用于 Windows 设备注册，请确保您拥有可用的公共 SSL 证书。有关详细信息，请参阅 XenMobile AutoDiscovery Service。

控制台必备条件工作流

此工作流显示了在添加应用程序和设备之前需要配置的必备条件。

> **注意：**

> 带星号的项目是可选的。



有关每个设置的更多信息以及分步过程，请参阅以下 Citrix 产品文档文章和部分：

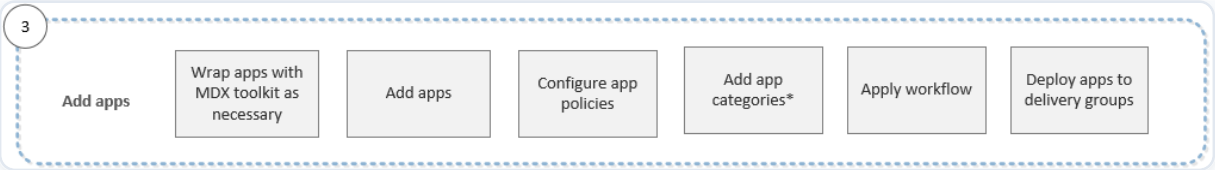
- 用户帐户、角色和注册
- 部署资源
- 使用 RBAC 配置角色
- 通知
- 应用工作流
- 将 ShareFile 与 XenMobile 结合使用

添加应用程序工作流

此工作流显示了向 XenMobile 添加应用程序时建议遵循的顺序。

注意：

带星号的项目是可选的。



有关每个设置的更多信息以及分步过程，请参阅以下 Citrix 产品文档文章和部分：

- 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

此工作流显示了在 XenMobile 中添加和注册设备时建议遵循的顺序。

注意：

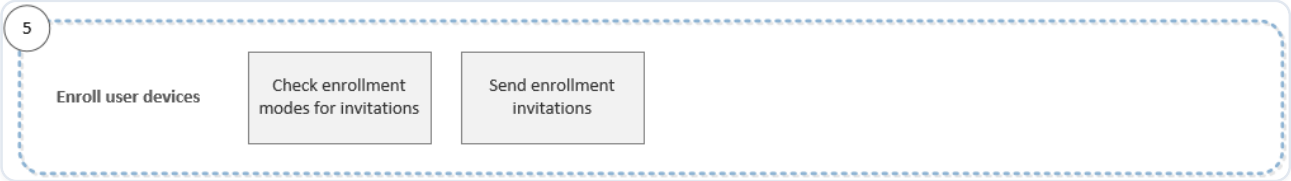
带星号的项目是可选的。

有关每个设置的更多信息以及分步过程，请参阅以下 Citrix 产品文档文章和部分：

- 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

此工作流程显示了在 XenMobile 中注册用户设备时建议遵循的顺序。



有关每个设置的更多信息以及分步过程，请参阅以下 Citrix 产品文档文章：

- 用户帐户、角色和注册
- 通知

持续的应用程序和设备管理工作流程

此工作流程显示了您可以在控制台中执行的应用程序和设备管理活动。

注意：

带星号的项目是可选的。

有关单击控制台右上角的扳手图标时找到的支持选项的更多信息，请参阅监视和支持。

证书和身份验证

在 XenMobile® 操作期间，有多个组件在身份验证中发挥作用：

- **XenMobile Server：** XenMobile Server 是定义注册安全性和注册体验的位置。用户入门选项包括：
  - 注册是向所有人开放还是仅限邀请。
  - 是否需要双因素身份验证或三因素身份验证。通过 XenMobile 中的客户端属性，您可以启用 Citrix PIN 身份验证并配置 PIN 的复杂性和过期时间。
- **Citrix ADC：** Citrix ADC 为微 VPN SSL 会话提供终止。Citrix ADC 还提供网络传输中安全性，并允许您定义用户每次访问应用程序时使用的身份验证体验。
- **Secure Hub：** Secure Hub 和 XenMobile Server 在注册操作中协同工作。Secure Hub 是设备上与 Citrix ADC 通信的实体：当会话过期时，Secure Hub 从 Citrix ADC 获取身份验证票证，并将票证传递给 MDX 应用程序。Citrix 建议使用证书锁定，这可以防止中间人攻击。有关详细信息，请参阅 Secure Hub 文章中的此部分：证书锁定。

  Secure Hub 还支持 MDX 安全容器：Secure Hub 推送策略，在应用程序超时时与 Citrix ADC 创建会话，并定义 MDX 超时和身份验证体验。Secure Hub 还负责越狱检测、地理位置检查以及您应用的任何策略。
- **MDX 策略：** MDX 策略在设备上创建数据保管库。MDX 策略将微 VPN 连接定向回 Citrix ADC，强制执行离线模式限制，并强制执行客户端策略，例如超时。

有关配置身份验证的更多信息，包括单因素和双因素身份验证方法的概述，请参阅部署手册文章 身份验证。

您在 XenMobile 中使用证书来创建安全连接和验证用户。本文的其余部分讨论证书。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

- 用于 Citrix Files 单点登录的 SAML
- 微软 Azure Active Directory 服务器设置
- 要将证书发送到设备以向 Wi-Fi 服务器进行身份验证：Wi-Fi 设备策略
- 要推送不用于身份验证的唯一证书（例如内部根证书颁发机构 (CA) 证书或特定策略）：凭据设备策略

证书

XenMobile 在安装过程中生成自签名安全套接字层 (SSL) 证书，以保护到服务器的通信流。您必须将此 SSL 证书替换为来自知名 CA 的受信任 SSL 证书。

XenMobile 还使用其自己的公钥基础结构 (PKI) 服务或从 CA 获取客户端证书。所有 Citrix 产品都支持通配符证书和主题备用名称 (SAN) 证书。对于大多数部署，您只需要两个通配符或 SAN 证书。

客户端证书身份验证为移动应用程序提供了额外的安全层，并允许用户无缝访问 HDX™ 应用程序。配置客户端证书身份验证后，用户输入其 Citrix PIN 即可单点登录 (SSO) 访问启用 XenMobile 的应用程序。Citrix PIN 还简化了用户身份验证体验。Citrix PIN 用于保护客户端证书或在设备本地保存 Active Directory 凭据。

要使用 XenMobile 注册和管理 iOS 设备，请设置并创建 Apple 推送通知服务 (APNs) 证书。有关步骤，请参阅APNs 证书。

下表显示了每个 XenMobile 组件的证书格式和类型：

XENMOBILE 组件	证书格式	所需证书类型
思杰网关	PEM (BASE64), PFX (PKCS #12)	SSL, Root（Citrix Gateway 会自动将 PFX 转换为 PEM。）
XenMobile 服务器	.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整的 PKI。）重要提示：XenMobile Server 不支持 .pem 扩展名的证书。要使用 .pem 证书，请将 .pem 文件拆分为证书和密钥，然后将每个文件导入 XenMobile Server。
StoreFront™	PFX (PKCS #12)	SSL, 根

XenMobile 支持位长为 4096、2048 和 1024 的 SSL 侦听器证书和客户端证书。1024 位证书很容易受到攻击。

对于 Citrix Gateway 和 XenMobile Server，Citrix 建议从公共 CA（例如 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，将其提交给 CA 进行签名。当 CA 返回签名证书时，您可以将证书安装在 Citrix Gateway 或 XenMobile 上。

> **重要提示：iOS、iPadOS 和 macOS 中受信任证书的要求**

> Apple 对 TLS 服务器证书提出了新要求。请验证所有证书是否符合 Apple 的新要求。请参阅 Apple 出版物 `<https://support.apple.com/zh-cn/HT210176>`。

> Apple 正在缩短 TLS 服务器证书的最大允许有效期。此更改仅影响 2020 年 9 月之后颁发的服务器证书。请参阅 Apple 出版物 `<https://support.apple.com/zh-cn/HT211025>`。

在 XenMobile 中上传证书

您上传的每个证书都在“证书”表中有一个条目，其中包括其内容的摘要。当您配置需要证书的 PKI 集成组件时，您需要选择一个满足上下文相关条件的服务器证书。例如，您可能希望配置 XenMobile 以与您的 Microsoft 证书颁发机构 (CA) 集成。与 Microsoft CA 的连接必须使用客户端证书进行身份验证。

本节提供了上传证书的通用过程。有关创建、上传和配置客户端证书的详细信息，请参阅客户端证书或证书加域身份验证。

私钥要求

XenMobile 可能拥有或不拥有给定证书的私钥。同样，XenMobile 可能需要或不需要上传证书的私钥。

上传证书

您有两种上传证书的选项：

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

将证书上传到控制台时，您有两个主要选项：

- 单击以导入密钥库。然后，您需要识别要安装的密钥库存储库中的条目，除非您正在上传 PKCS #12 格式。
- 单击以导入证书。

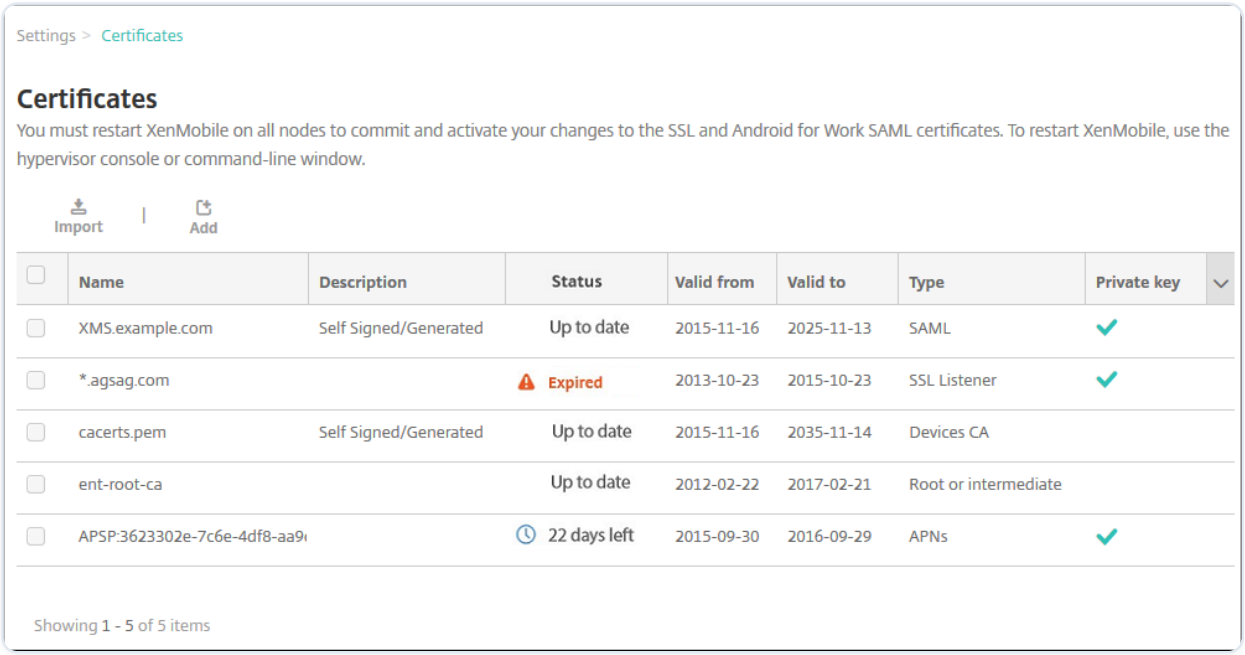
您可以上传 CA 用于签署请求的 CA 证书（不带私钥）。您还可以上传 SSL 客户端证书（带私钥）用于客户端身份验证。

配置 Microsoft CA 实体时，您需要指定 CA 证书。您可以从所有作为 CA 证书的服务器证书列表中选择 CA 证书。同样，配置客户端身份验证时，您可以从 XenMobile 拥有私钥的所有服务器证书列表中进行选择。

导入密钥库

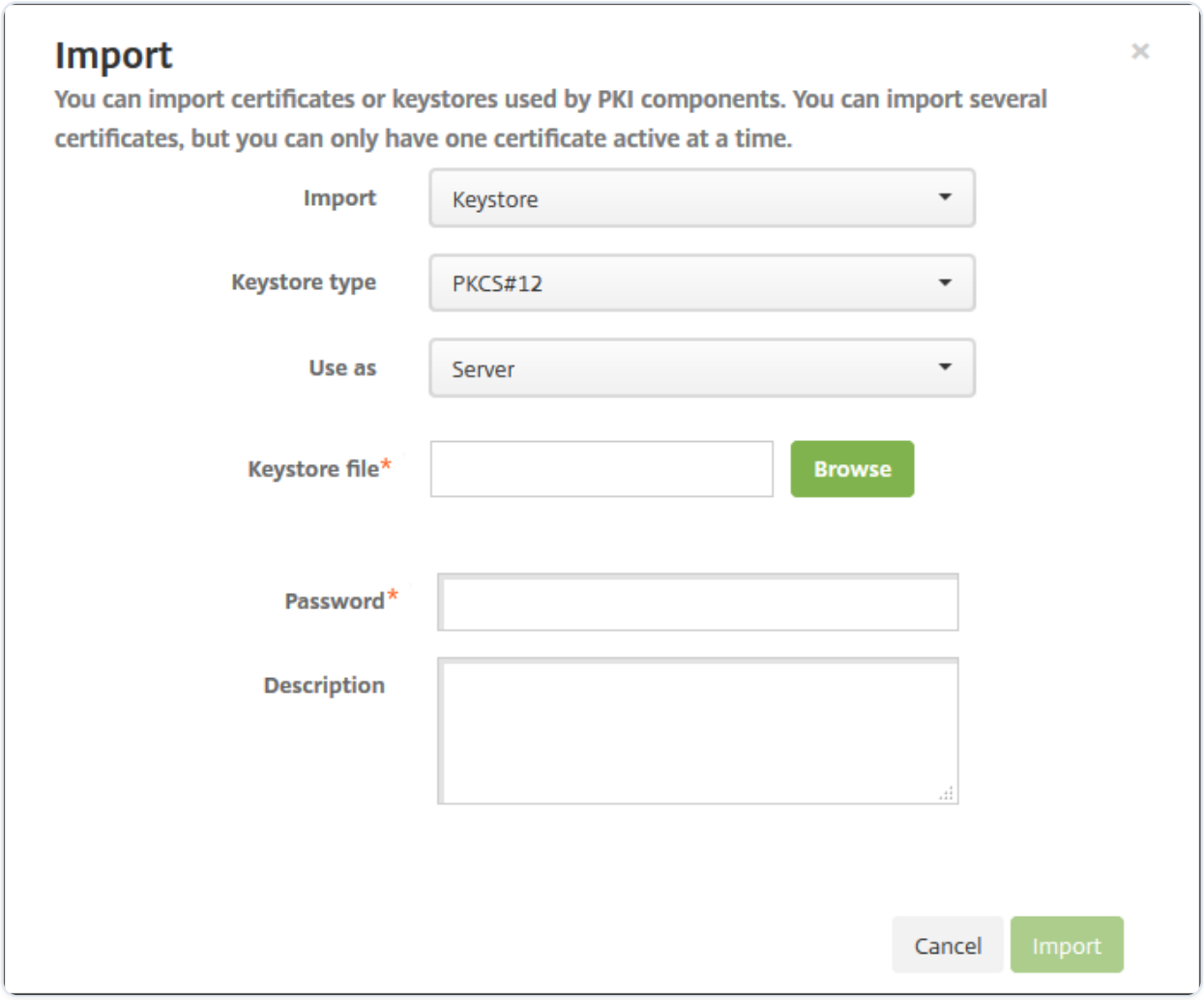
根据设计，作为安全证书存储库的密钥库可以包含多个条目。因此，从密钥库加载时，系统会提示您指定标识要加载的条目的别名。如果您未指定别名，则会加载存储中的第一个条目。由于 PKCS #12 文件通常只包含一个条目，因此当您选择 PKCS #12 作为密钥库类型时，别名字段不会出现。

1. 在 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. 点击**证书**。**证书**页面随即出现。



3. 点击**导入**。**导入**对话框随即出现。
4. 配置以下设置：

   - **导入**：在列表中，点击**密钥库**。**导入**对话框将随之更改，以反映可用的密钥库选项。



- **密钥库类型**：在列表中，点击 **PKCS #12**。
- **用途**：在列表中，点击您计划如何使用证书。可用选项包括：
  - **服务器**。服务器证书是 XenMobile Server 功能性使用的证书，这些证书已上传到 XenMobile Web 控制台。它们包括 CA 证书、RA 证书以及用于客户端身份验证的证书，可与您的基础结构的其他组件配合使用。此外，您可以使用服务器证书作为要部署到设备的证书的存储。此用途尤其适用于用于在设备上建立信任的 CA。
  - **SAML**。安全断言标记语言 (SAML) 认证允许您为服务器、网站和应用程序提供 SSO 访问。
  - **APNs**。来自 Apple 的 APNs 证书通过 Apple 推送网络实现移动设备管理。
  - **SSL 侦听器**。安全套接字层 (SSL) 侦听器通知 XenMobile SSL 加密活动。
- **密钥库文件**：浏览以查找要导入的 .p12 文件类型（或基于 Windows 的计算机上的 .pfx）的密钥库。
- **密码**：键入分配给证书的密码。
- **描述**：可选，键入密钥库的描述，以帮助您将其与其他密钥库区分开来。

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 会尝试从输入构建证书链。XenMobile 会导入该链中的所有证书，为每个证书创建一个服务器证书条目。此操作仅在文件或密钥库条目中的证书确实构成链时才有效。例如，如果链中每个后续证书都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。说明仅附加到链中的第一个证书。您可以稍后更新其余证书的说明。

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**”对话框中，在“**导入**”下，如果尚未选择，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**”下，选择您计划如何使用密钥库。可用选项包括：
   - **服务器**。服务器证书是 XenMobile Server 功能性使用的证书，这些证书已上传到 XenMobile Web 控制台。它们包括 CA 证书、RA 证书以及用于客户端与基础结构的其他组件进行身份验证的证书。此外，您可以使用服务器证书作为要部署到设备的证书的存储。此选项尤其适用于用于在设备上建立信任的 CA。
   - **SAML**。安全断言标记语言 (SAML) 认证允许您为服务器、网站和应用程序提供单点登录 (SSO) 访问。
   - **SSL 侦听器**。安全套接字层 (SSL) 侦听器会通知 XenMobile SSL 加密活动。
5. 浏览以查找要导入的 .p12 文件类型（或基于 Windows 的计算机上的 .pfx）的密钥库。
6. 浏览以查找证书的可选私钥文件。私钥与证书一起用于加密和解密。
7. （可选）键入证书的说明，以帮助您将其与其他证书区分开来。
8. 单击“**导入**”。证书将添加到“证书”表中。

使用 REST API 批量将证书上传到 iOS 设备

如果逐个上传证书不切实际，您可以使用 REST API 将它们批量上传到 iOS 设备。此方法支持 .p12 格式的证书。有关 REST API 的更多信息，请参阅 REST API。

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

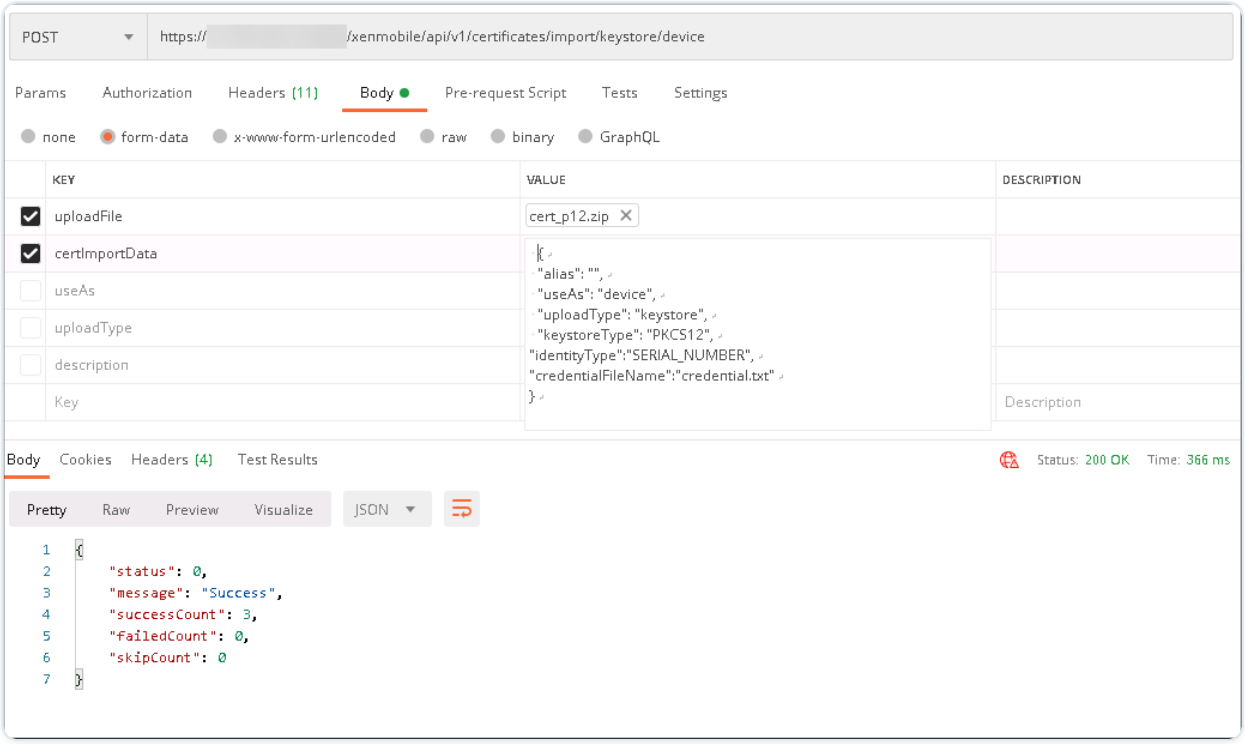
   例如，您选择使用序列号作为识别方法。如果一个设备的序列号是 `A12BC3D4EFGH`，则将您希望安装在该设备上的证书文件命名为 `A12BC3D4EFGH.p12`。

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

```
A12BC3D4EFGH.p12=password1!

A12BC3D4EFIJ.p12=password2@

A12BC3D4EFKL.p12=password3#
```

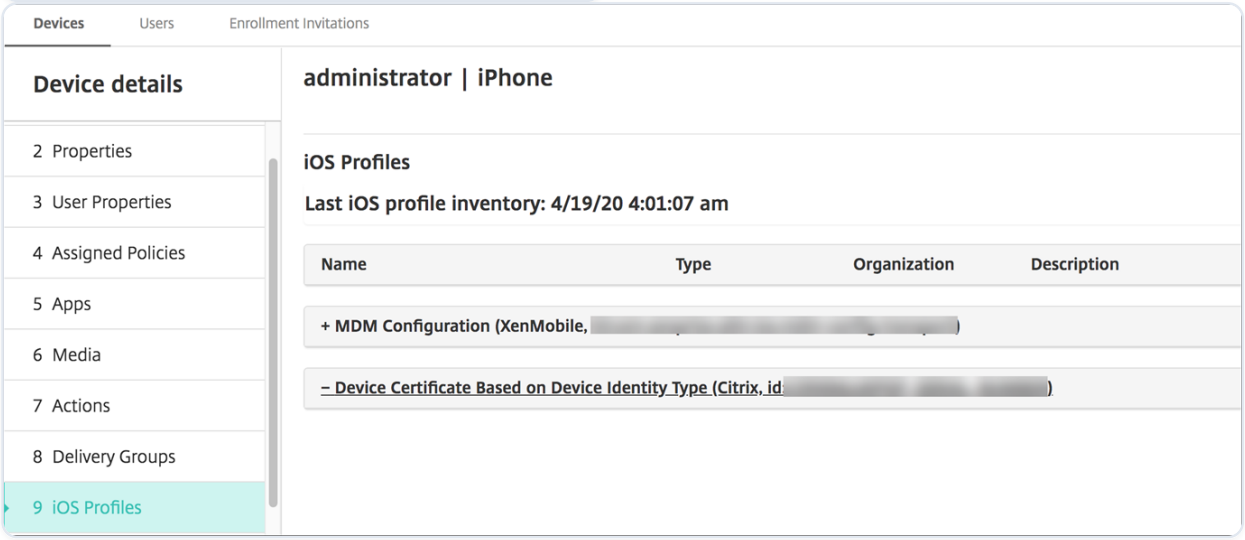
3. 将所有证书和您创建的文本文件打包到一个 .zip 文件中。
4. 启动您的 REST API 客户端，登录 XenMobile，并获取身份验证令牌。
5. 导入您的证书，确保在消息正文中包含以下内容：

```
{

    "alias": "",

    "useAs": "device",

    "uploadType": "keystore",

    "keystoreType": "PKCS12",

    "identityType":"SERIAL_NUMBER",        # identity type can be
"SERIAL_NUMBER","IMEI","MEID"

    "credentialFileName":"credential.txt"   # The credential file name
in .zip

}
```



6. 创建 VPN 策略，凭据类型为 **Always on IKEv2**，设备身份验证方法为 **基于设备身份的设备证书**。选择您在证书文件名中使用的 **设备身份类型**。请参阅 VPN 设备策略。
7. 注册 iOS 设备并等待 VPN 策略部署。通过检查设备上的 MDM 配置来确认证书安装。您还可以在 XenMobile 控制台中检查设备详细信息。

12:08
Profile
MDM Configuration
MOBILE DEVICE MANAGEMENT
DEVICE IDENTITY CERTIFICATE
XenMobile MDM
Issued by: Devices Certificate Authority
Expires: April 17, 2022
CERTIFICATES (4)
Root Certificate Authority
Issued by: Root Certificate Authority
Expires: February 18, 2038
DigiCert SHA2 Secure Server CA
Issued by: DigiCert Global Root CA
Expires: March 8, 2023
DigiCert Global Root CA
Issued by: DigiCert Global Root CA
Expires: November 10, 2031
cem user02
Issued by:
Expires: February 25, 2021
SIGNING CERTIFICATE


Devices
Users
Enrollment Invitations
Device details
administrator | iPhone
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Media
7 Actions
8 Delivery Groups
9 iOS Profiles
iOS Profiles
Last iOS profile inventory: 4/19/20 4:01:07 am
Name
Type
Organization
Description
+ MDM Configuration (XenMobile,
– Device Certificate Based on Device Identity Type (Citrix, id

您还可以通过创建一个文本文件来批量删除证书，该文件中列出了要删除的每个证书的 `device_identity_value`。在 REST API 中，调用删除 API 并使用以下请求，将 `device_identity_value` 替换为相应的标识符：

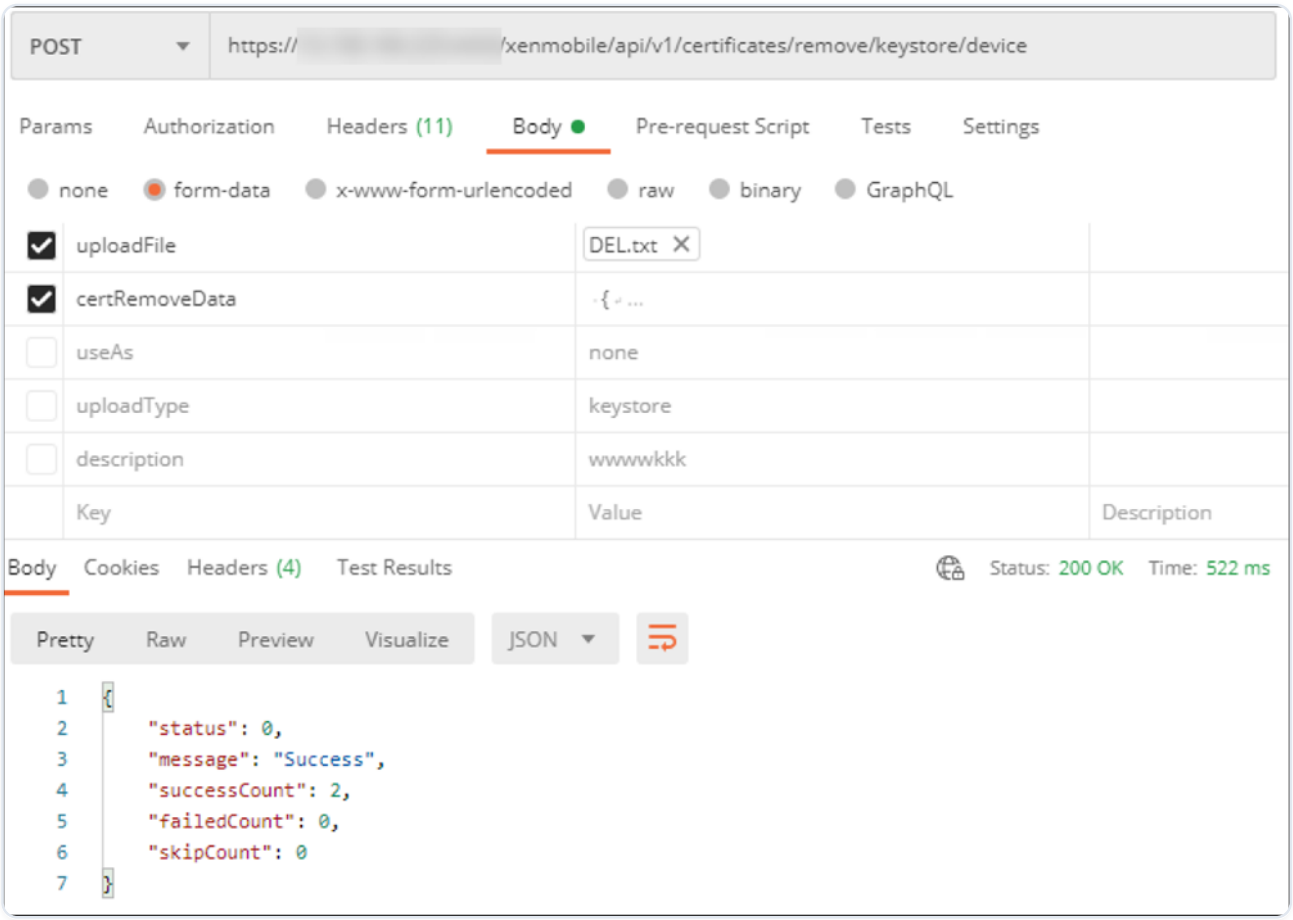
```
```

{

    "identityType"="device_identity_value"

}

```
```



更新证书

XenMobile 系统中一次只允许每个公钥存在一个证书。如果您尝试为与已导入证书相同的密钥对导入证书，则可以选择替换现有条目或删除该条目。

要在 XenMobile 控制台中最有效地更新证书，请执行以下操作。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。

更新服务器证书时，使用先前证书的组件会自动切换为使用新证书。同样，如果您已在设备上部署服务器证书，则该证书会在下次部署时自动更新。

续订证书

XenMobile Server 内部使用以下证书颁发机构 (CA) 进行 PKI：根 CA、设备 CA 和服务器 CA。这些 CA 被归类为一个逻辑组并提供一个组名。预配新的 XenMobile Server 实例时，会生成这三个 CA 并为其指定组名“default”。

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

以下 API 可用于续订或重新生成 XenMobile Server 中的内部 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 并停用旧 CA。
- 续订配置设备列表上的设备证书。已注册的设备将继续正常工作，不受中断。设备连接回服务器时会颁发设备证书。
- 返回仍在使用旧 CA 的设备列表。
- 在所有设备都具有新 CA 后删除旧 CA。

有关信息，请参阅 Public API for REST Services PDF 中的以下部分：

- 第 3.16.58 节，续订设备证书
- 第 3.23 节，内部 PKI CA 组

管理设备控制台包含安全操作**证书续订**，用于续订设备上的注册证书。

先决条件

- 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**。

> **重要提示：**
>
> 如果您的 Citrix ADC 设置为 SSL 卸载，当您生成新证书时，请确保使用新的 cacert.perm 更新您的负载均衡器。有关 Citrix Gateway 设置的更多信息，请参阅使用 SSL 卸载模式处理 NetScaler VIP。

用于重置群集节点服务器 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，使用 XenMobile CLI 重置其他群集节点上的证书密码。在 CLI 主菜单中，选择 **System > Advanced Settings > Reset CA certs password**。如果在没有新 CA 证书的情况下重置密码，XenMobile 不会重置密码。

```
-----------------------------------
Advanced Settings
-----------------------------------
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset CA Certs Password
[5] Reset SSL Certificate
[6] Reset pki.xml
[7] Server Tuning
[8] Switch JDBC driver
[9] Cloud Migration Credential Check
[10] Refresh encryption keys
-----------------------------------
Choice: [0 - 10]
```

XenMobile 证书管理

我们建议您列出在 XenMobile 部署中使用的证书，特别是它们的到期日期和相关密码。本节旨在帮助您更轻松地进行 XenMobile 证书管理。

您的环境可能包含以下部分或全部证书：

- XenMobile 服务器
  - MDM FQDN 的 SSL 证书
  - SAML 证书（适用于 Citrix Files）
  - 用于上述证书和任何其他内部资源（StoreFront/代理等）的根和中间 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 工具包

  - Apple 开发者证书
  - Apple 配置文件（每个应用程序）
  - Apple APNs 证书（与 Citrix Secure Mail™ 结合使用）
  - Android 密钥库文件

  MAM SDK 不封装应用程序，因此不需要证书。

- 思杰 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 负载平衡的 SSL 证书（卸载配置）
  - StoreFront 负载平衡的 SSL 证书
  - 前述证书的根证书和中间 CA 证书

XenMobile 证书过期策略

如果您允许证书过期，则该证书将变为无效。您将无法在您的环境中运行安全事务，也无法访问 XenMobile 资源。

> **注意：**

> 证书颁发机构 (CA) 会在 SSL 证书过期前提示您续订。

Citrix Secure Mail 所需的 APNs 证书

Apple 推送通知服务 (APNs) 证书每年都会过期。请务必在证书过期前创建 APNs SSL 证书并在 Citrix 门户中更新。如果证书过期，用户将遇到 Secure Mail 推送通知不一致的问题。此外，您将无法再为您的应用程序发送推送通知。

用于 iOS 设备管理的 APNs 证书

要使用 XenMobile 注册和管理 iOS 设备，请设置并创建 Apple 的 APNs 证书。如果证书过期，用户将无法注册 XenMobile，并且您无法管理其 iOS 设备。有关详细信息，请参阅APNs 证书。

您可以通过登录 Apple 推送证书门户查看 APNs 证书状态和过期日期。请务必以创建该证书的同一用户身份登录。

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

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



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



Thank You,



Apple Push Notification Service
```

MDX Toolkit（iOS 分发证书）

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

- 使用预配配置文件对应用程序进行签名。
- 使用相应的分发证书对应用进行签名。

要验证您是否拥有有效的 iOS 分发证书，请执行以下操作：

1. 在 Apple Enterprise Developer 门户中，为您计划使用 MDX Toolkit 封装的每个应用创建一个显式 App ID。可接受的 App ID 示例如下：`com.CompanyName.ProductName`。
2. 在 Apple Enterprise Developer 门户中，转至 **Provisioning Profiles > Distribution** 并创建内部预配配置文件。对上一步中创建的每个 App 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 证书均有效，请执行以下操作：

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

Android 密钥库

密钥库是一个文件，其中包含用于签署 Android 应用程序的证书。当您的密钥有效期到期时，用户将无法无缝升级到应用程序的新版本。

思杰 ADC

有关如何处理 Citrix ADC 证书过期问题的详细信息，请参阅 Citrix 支持知识中心中的 如何处理 NetScaler 上的证书过期。

过期的 Citrix ADC 证书会阻止用户注册和访问 Store。过期的证书还会阻止用户在使用 Secure Mail 时连接到 Exchange Server。此外，用户无法枚举和打开 HDX 应用程序（具体取决于哪个证书已过期）。

Expiry Monitor 和 Command Center 可以帮助您跟踪 Citrix ADC 证书。当证书过期时，Command Center 会通知您。这些工具可帮助监控以下 Citrix ADC 证书：

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

Citrix 网关和 XenMobile®

当您使用 XenMobile 配置 Citrix Gateway 时，您将建立远程设备访问内部网络的身份验证机制。此功能使移动设备上的应用程序能够访问内网中的公司服务器。XenMobile 会在设备上的应用程序与 Citrix Gateway 之间创建微型 VPN。

您可以通过从 XenMobile 导出脚本并在 Citrix Gateway 上运行，来配置 Citrix Gateway 以与 XenMobile 结合使用。

使用 Citrix Gateway 配置脚本的先决条件

Citrix ADC 要求：

- Citrix ADC（最低版本 11.0，内部版本 70.12）。
- Citrix ADC IP 地址已配置并与 LDAP 服务器具有连接性，除非 LDAP 已进行负载平衡。

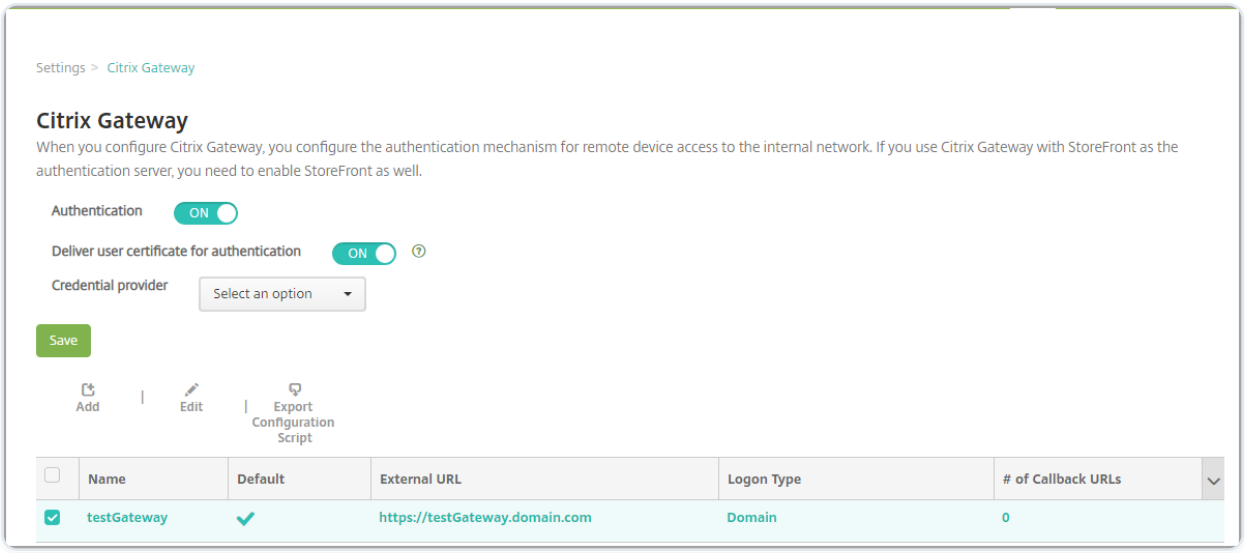
- Citrix ADC 子网 (SNIP) IP 地址已配置，与必要的后端服务器具有连接性，并可通过端口 8443/TCP 访问公共网络。
- DNS 可以解析公共域。
- Citrix ADC 已获得平台/通用或试用许可证。有关详细信息，请参阅 `<https://support.citrix.com/article/CTX126049>`。
- Citrix Gateway SSL 证书已上传并安装在 Citrix ADC 上。有关详细信息，请参阅 `<https://support.citrix.com/article/CTX136023>`。

XenMobile 要求：

- XenMobile Server（最低版本 10.6）。
- LDAP 服务器已配置。

配置身份验证以使远程设备访问内部网络

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。将显示“**设置**”页面。
2. 在“**服务器**”下，单击“**Citrix Gateway**”。将显示“**Citrix Gateway**”页面。在以下示例中，已存在一个 Citrix Gateway 实例。



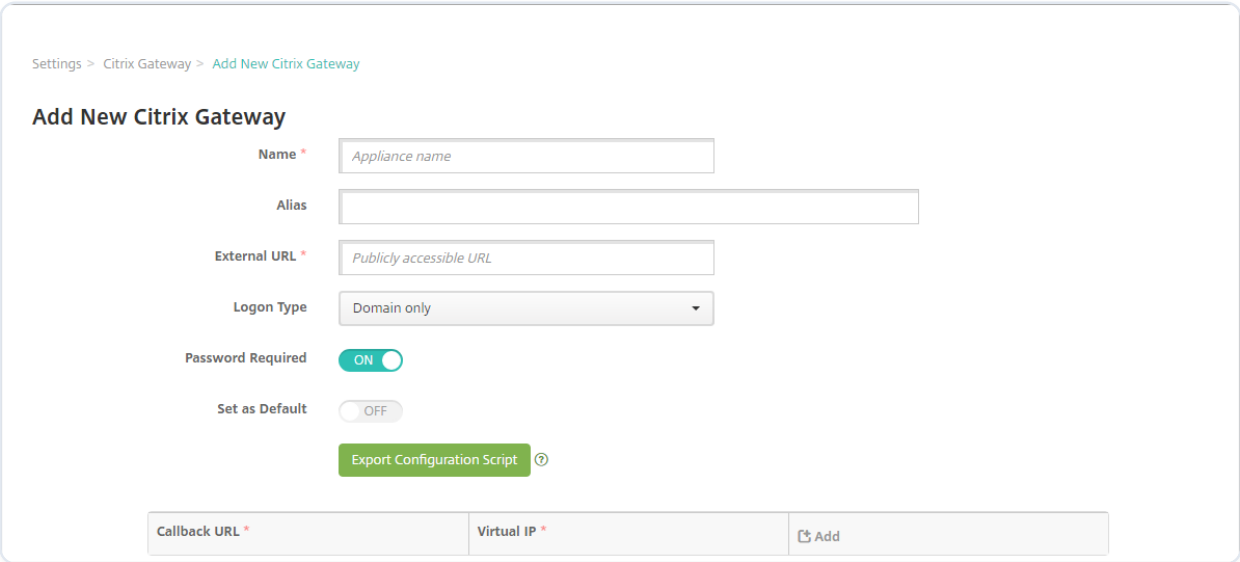
3. 配置以下设置：
   - **身份验证：** 选择是否启用身份验证。默认值为“**开**”。
   - **交付用户证书以进行身份验证：** 选择是否希望 XenMobile 与 Secure Hub 共享身份验证证书，以使 Citrix Gateway 能够处理客户端证书身份验证。默认值为“**关**”。
   - **凭据提供程序：** 在列表中，单击要使用的凭据提供程序。有关详细信息，请参阅凭据提供程序。

4. 单击“**保存**”。

添加 Citrix Gateway 实例

保存身份验证设置后，将 Citrix Gateway 实例添加到 XenMobile。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。将打开“**设置**”页面。
2. 在“**服务器**”下，单击“**Citrix Gateway**”。将显示“**Citrix Gateway**”页面。
3. 单击“**添加**”。将显示“**添加新 Citrix Gateway**”页面。



4. 配置以下设置：

   - **名称：** 输入 Citrix Gateway 实例的名称。
   - **别名：** 可选地为 Citrix Gateway 包含一个别名。
   - **外部 URL：** 输入 Citrix Gateway 的公共可访问 URL。例如，`https://receiver.com`。
   - **登录类型：** 选择一个登录类型。类型包括**仅域**、**仅安全令牌**、**域和安全令牌**、**证书**、**证书和域**以及**证书和安全令牌**。**需要密码**字段的默认设置会根据您选择的**登录类型**而变化。默认值为**仅域**。

   如果您有多个域，请使用**证书和域**。有关使用 XenMobile 和 Citrix Gateway 配置多域身份验证的详细信息，请参阅配置多域身份验证。

   如果您使用**证书和安全令牌**，则需要在 Citrix Gateway 上进行一些额外配置以支持 Secure Hub。有关信息，请参阅为证书和安全令牌身份验证配置 XenMobile。

   有关详细信息，请参阅部署手册中的身份验证。

   - **需要密码：** 选择是否需要密码身份验证。默认值因所选的**登录类型**而异。

- **设为默认值：** 选择是否将此 Citrix Gateway 用作默认值。默认值为**关闭。**
- **导出配置脚本：** 单击此按钮可导出配置包，您可以将其上传到 Citrix Gateway 以使用 XenMobile 设置对其进行配置。有关信息，请参阅这些步骤之后的“配置本地 Citrix Gateway 以与 XenMobile Server 结合使用”。
- **回调 URL** 和**虚拟 IP：** 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**。

   新的 Citrix Gateway 已添加并显示在表中。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 结合使用

要配置本地 Citrix Gateway 以与 XenMobile 结合使用，请执行本文中详述的以下常规步骤：

1. 从 XenMobile Server 下载脚本和相关文件。有关最新详细说明，请参阅脚本随附的自述文件。
2. 验证您的环境是否满足先决条件。
3. 更新脚本以适应您的环境。
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 所需的 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。 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

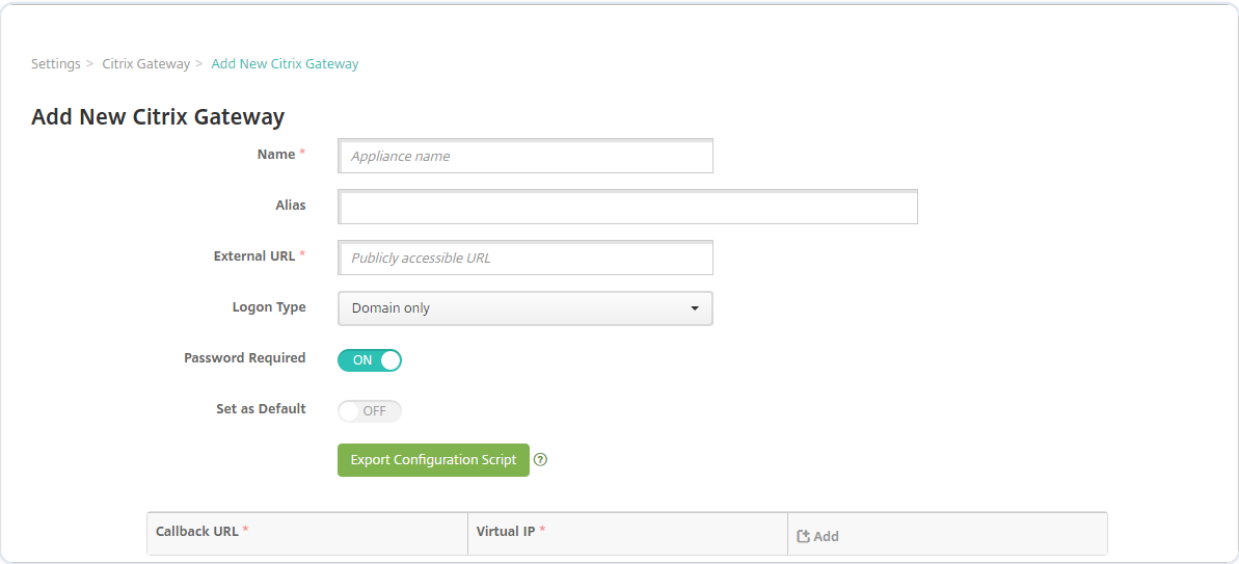
该脚本不处理以下配置：

- Exchange 负载平衡
- Citrix Files 负载平衡
- ICA® 代理配置

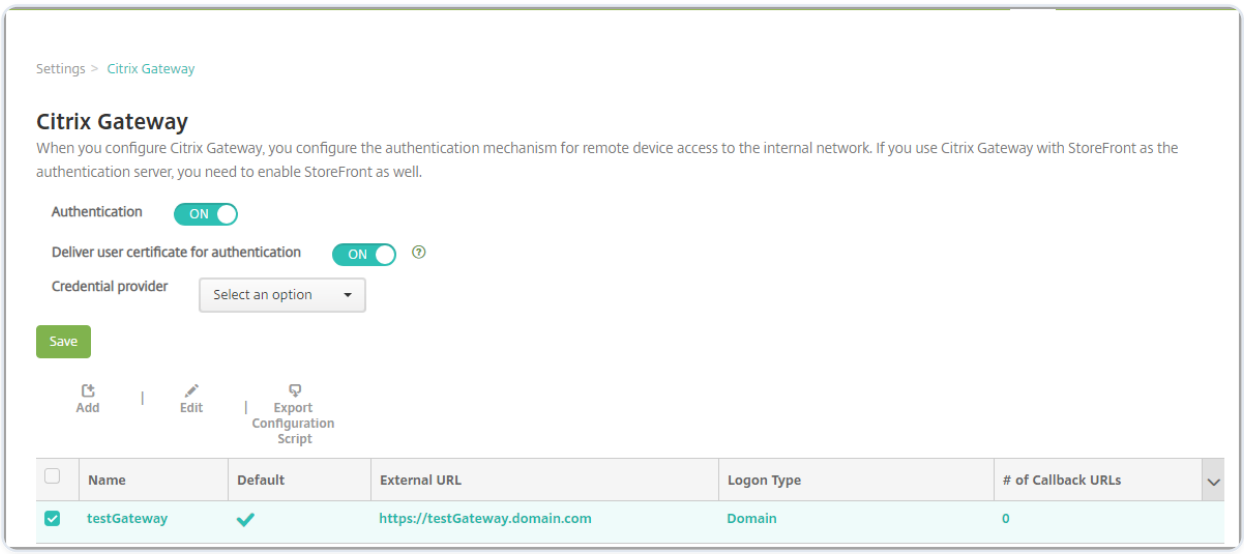
- SSL 卸载

下载、更新和运行脚本

1. 如果您要添加 Citrix Gateway，请在**添加新 Citrix Gateway** 页面上单击**导出配置脚本**。



或者，如果您在导出脚本之前添加了 Citrix Gateway 实例并单击了**保存**：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。该脚本包包括：

- 包含详细说明的自述文件
- 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 的公共根 CA 证书和中间 CA 证书（这些用于 SSL 卸载的证书在当前版本中不需要）
- 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)，将所有占位符替换为您的环境中的详细信息。

```
# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <NSG_ROOT_CA_CERT_TAG> -- NetScaler ROOT CA Tag.
# <RADIUS_KEY> -- Radius Key.
# <XMS_CERT_TAG> -- XenMobile Certificate Tag.
# <MAM_LB_IP> -- Virtual IP Address to be assigned for MAM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <MDM_LB_IP> -- Virtual IP Address to be assigned for MDM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <NSG_VIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reacha
ble from your devices either directly or via a NAT.
```

3. 在 Citrix ADC bash shell 中运行您编辑的脚本，按照脚本包中包含的 readme 文件中的说明进行操作。例如：

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

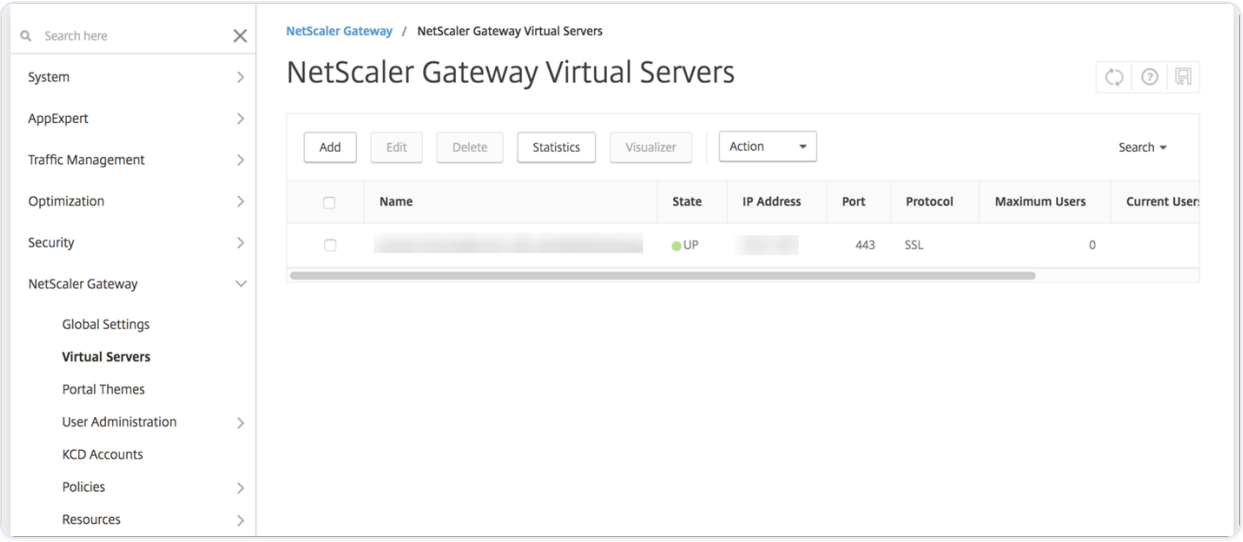
```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only          #
#         Disconnect IMMEDIATELY if you 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。

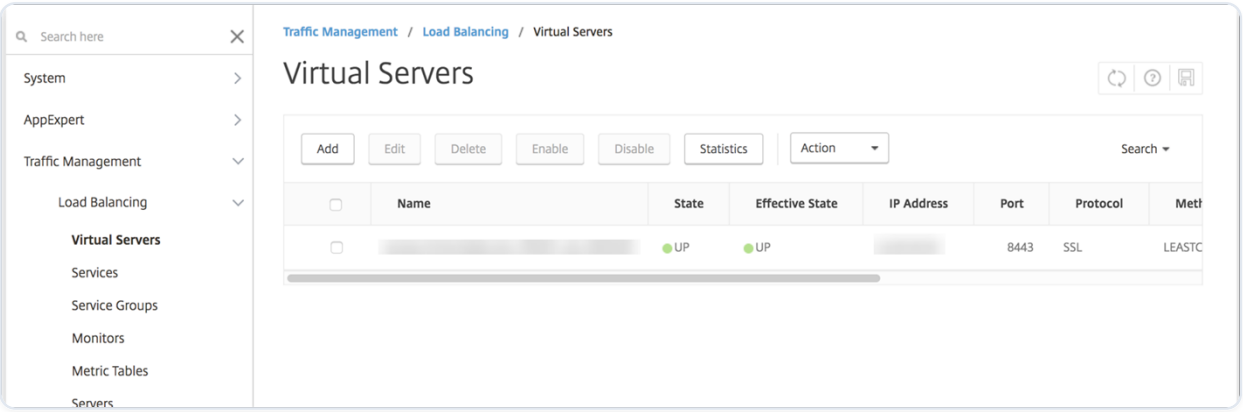
```
exec: save ns config
 Done
 Done
root@ns#
```

测试配置

1. 验证 Citrix Gateway 虚拟服务器显示状态为 **UP**。



2. 验证代理负载平衡虚拟服务器显示状态为 **UP**。



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，将显示此消息：HTTP Status 404 - Not Found
4. 注册设备并确保它同时获得 MDM 和 MAM 注册。

添加回调 URL 和 Citrix Gateway VPN 虚拟 IP

添加 Citrix Gateway 实例后，您可以添加回调 URL 并指定 Citrix Gateway 虚拟 IP 地址。这些设置是可选的，但可以配置以增强安全性，尤其是在 XenMobile Server 位于 DMZ 中时。

1. 在 **设置 > Citrix Gateway** 中，选择 Citrix Gateway，然后点击**编辑**。
2. 在表中，点击**添加**。
3. 对于**回调 URL**，键入完全限定域名 (FQDN)。回调 URL 验证请求是否源自 Citrix Gateway。

   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 或其他 URL。
4. 键入 Citrix Gateway **虚拟 IP** 地址，然后点击**保存**。

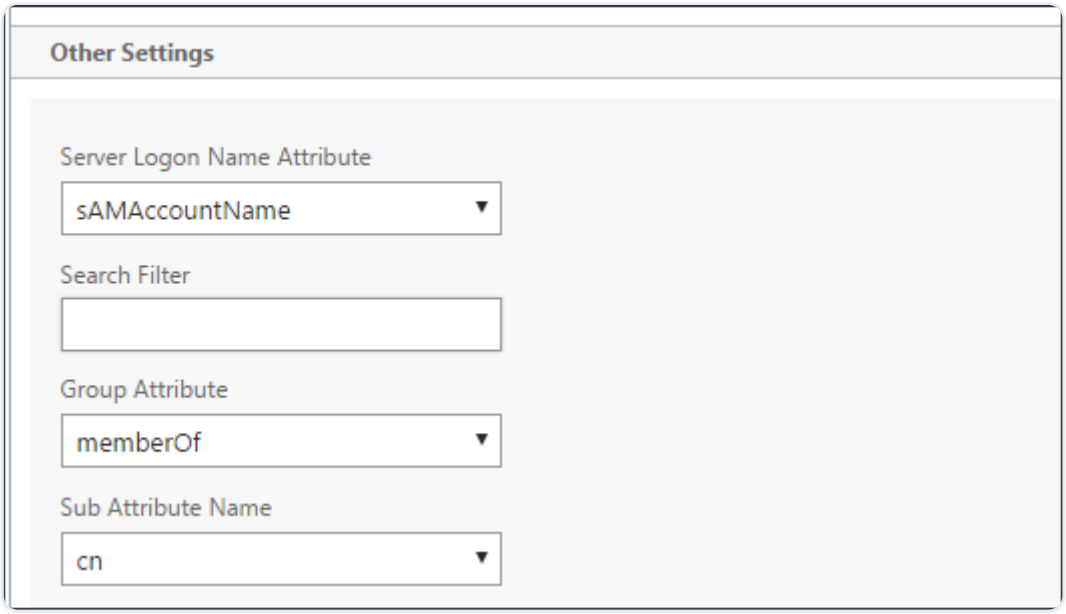
配置多个域的身份验证

如果您有多个 XenMobile Server 实例（例如用于测试、开发和生产环境），则需要手动为其他环境配置 Citrix Gateway。（您只能使用一次 Citrix ADC for XenMobile 向导。）

思杰网关配置

要为多域环境配置 Citrix Gateway 身份验证策略和会话策略：

1. 在 Citrix Gateway 配置实用程序中，在**配置**选项卡上，展开 **Citrix Gateway > 策略 > 身份验证**。
2. 在导航窗格中，点击**LDAP**。
3. 点击以编辑 LDAP 配置文件。将**服务器登录名属性**更改为 **userPrincipalName** 或您要用于搜索的属性。记下您指定的属性，以便在 XenMobile 控制台中配置 LDAP 设置时使用。

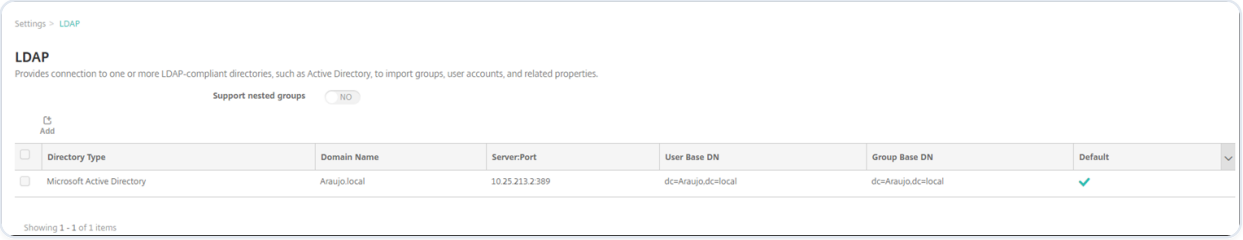


4. 对每个 LDAP 策略重复这些步骤。每个域都需要一个单独的 LDAP 策略。
5. 在绑定到 Citrix Gateway 虚拟服务器的会话策略中，导航到 **编辑会话配置文件 > 已发布的应用程序**。确保**单点登录域**为空。

XenMobile Server 配置

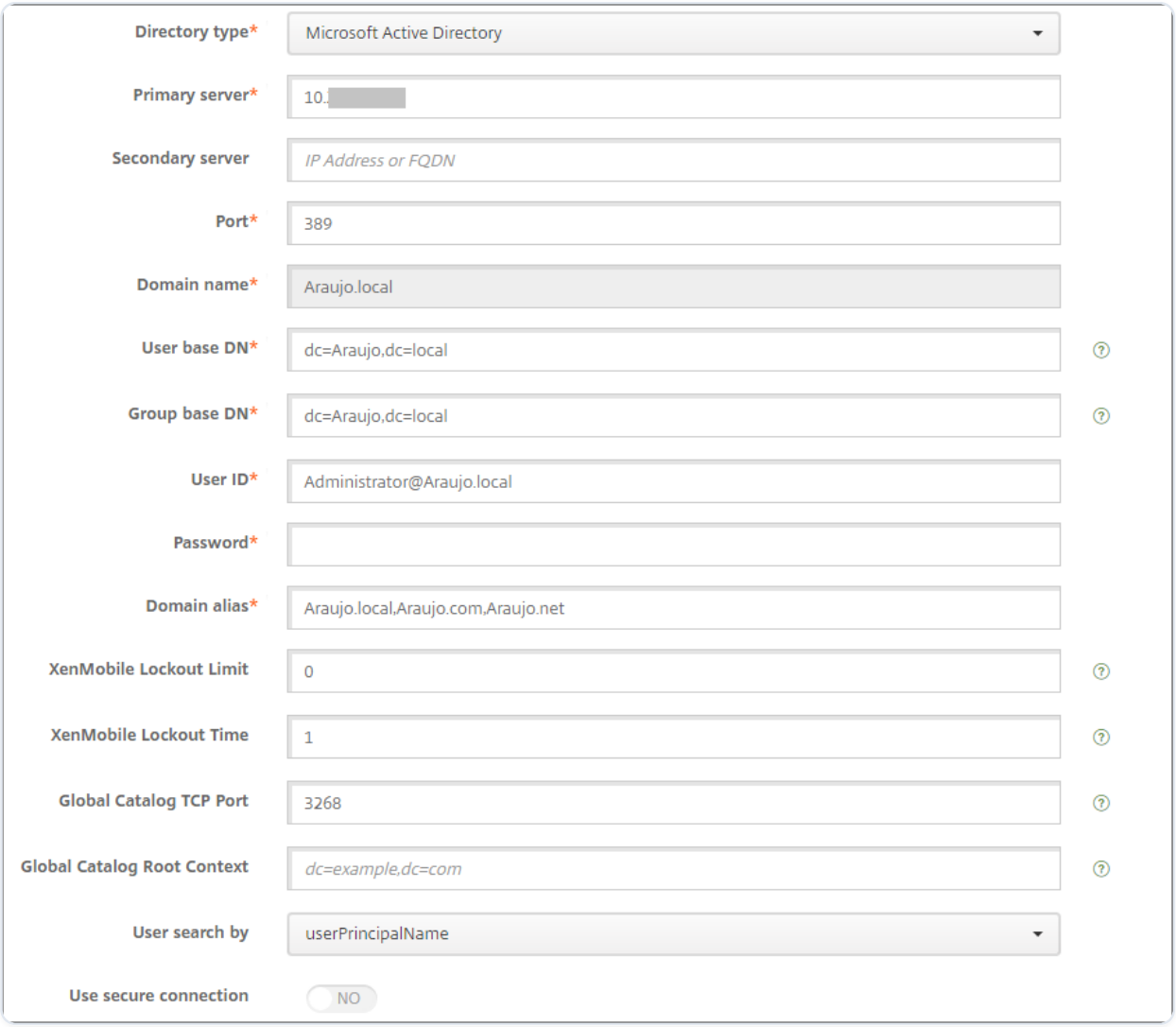
要为多域 XenMobile 环境配置 LDAP，请执行以下操作：

1. 在 XenMobile 控制台中，转到 **设置 > LDAP** 并添加或编辑目录。



2. 提供信息。

- 在 **域别名** 中，指定用于用户身份验证的每个域。使用逗号分隔域，并且域之间不要使用空格。例如：`domain1.com,domain2.com,domain3.com`
- 确保 **用户搜索依据** 字段与 Citrix Gateway LDAP 策略中指定的 **服务器登录名属性** 匹配。



删除到特定 URL 的入站连接请求

如果您的环境中配置了用于 SSL 卸载的 Citrix Gateway，您可能希望网关删除到特定 URL 的入站连接请求。

如果您需要额外的安全性，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）。使用以下信息作为设置模板。

> **重要提示：**
>
> 以下更新仅适用于配置了 SSL 卸载的 Citrix Gateway。

1. 创建名称为 `XMS_DropURLs` 的模式集。

```
add policy patset XMS_DropURLs
```

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


bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5


bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4


bind policy patset XMS_DropURLs /zdm/log.jsp -index 3


bind policy patset XMS_DropURLs /zdm/login.jsp -index 2


bind policy patset XMS_DropURLs /zdm/console -index 1
```

3. 创建一个策略，以丢弃所有发往这些 URL 的流量，除非连接请求源自指定的子网。

```
add responder policy XMS_DROP_pol
“CLIENT.IP.SRC.IN_SUBNET(192.168.0.0/24).NOT &&

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"
```

4. 将新策略绑定到两个 MDM 负载均衡器虚拟服务器（端口 443 和 8443）。

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST



bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST
```

5. 通过浏览器阻止 MAM URL 访问

直接通过浏览器访问 MAM URL 会提示用户输入其 Active Directory 凭据。虽然它可作为用户验证其凭据的工具，但某些用户可能会将其视为安全漏洞。以下部分将帮助您使用 NetScaler 上的响应程序策略功能限制浏览器访问 MAM URL (NetScaler® Gateway VIP)。

创建以下响应程序策略之一并将其绑定到您的 NetScaler Gateway 虚拟服务器：

- `add responder policy Resp_Brow_Pol "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"Mozilla\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`
- `add responder policy Resp_Brow_Pol_CR "!HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`
- `add responder policy Resp_Brow_Pol_CR "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`

使用 `bind vpn vserver _XM_XenMobileGateway -policy Resp_Brow_Pol_CR -priority 100 -gotoPriorityExpression END -type REQUEST` 绑定到 NetScaler Gateway 虚拟服务器

> **注意：**
>
> `_XM_XenMobileGateway` 是 NetScaler Gateway 虚拟服务器的示例名称。

域或域加安全令牌身份验证

XenMobile® 支持针对一个或多个符合轻量级目录访问协议 (LDAP) 的目录进行基于域的身份验证。您可以在 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 是一种开源、供应商中立的应用程序协议，用于通过 Internet 协议 (IP) 网络访问和维护分布式目录信息服务。目录信息服务用于共享有关网络中可用的用户、系统、网络、服务和应用程序的信息。

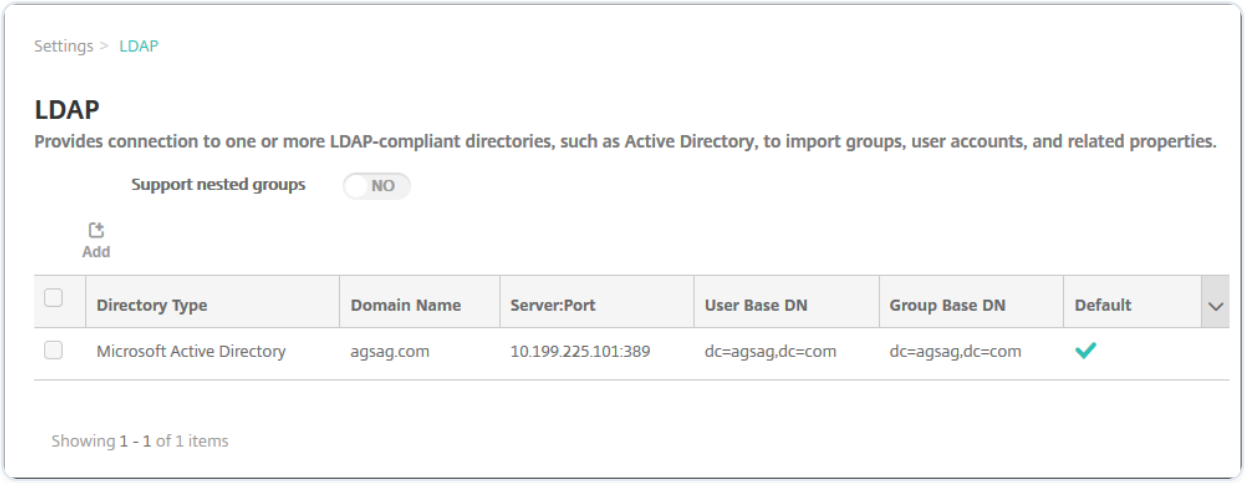
LDAP 的常见用途是为用户提供单点登录 (SSO)，其中单个密码（每个用户）在多个服务之间共享。单点登录使用户能够一次登录公司网站，以进行对公司内网的身份验证访问。

客户端通过连接到 LDAP 服务器来启动 LDAP 会话，该服务器称为目录系统代理 (DSA)。然后客户端向服务器发送操作请求，服务器使用相应的身份验证进行响应。

> **重要：**
>
> 在用户将设备注册到 XenMobile 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。

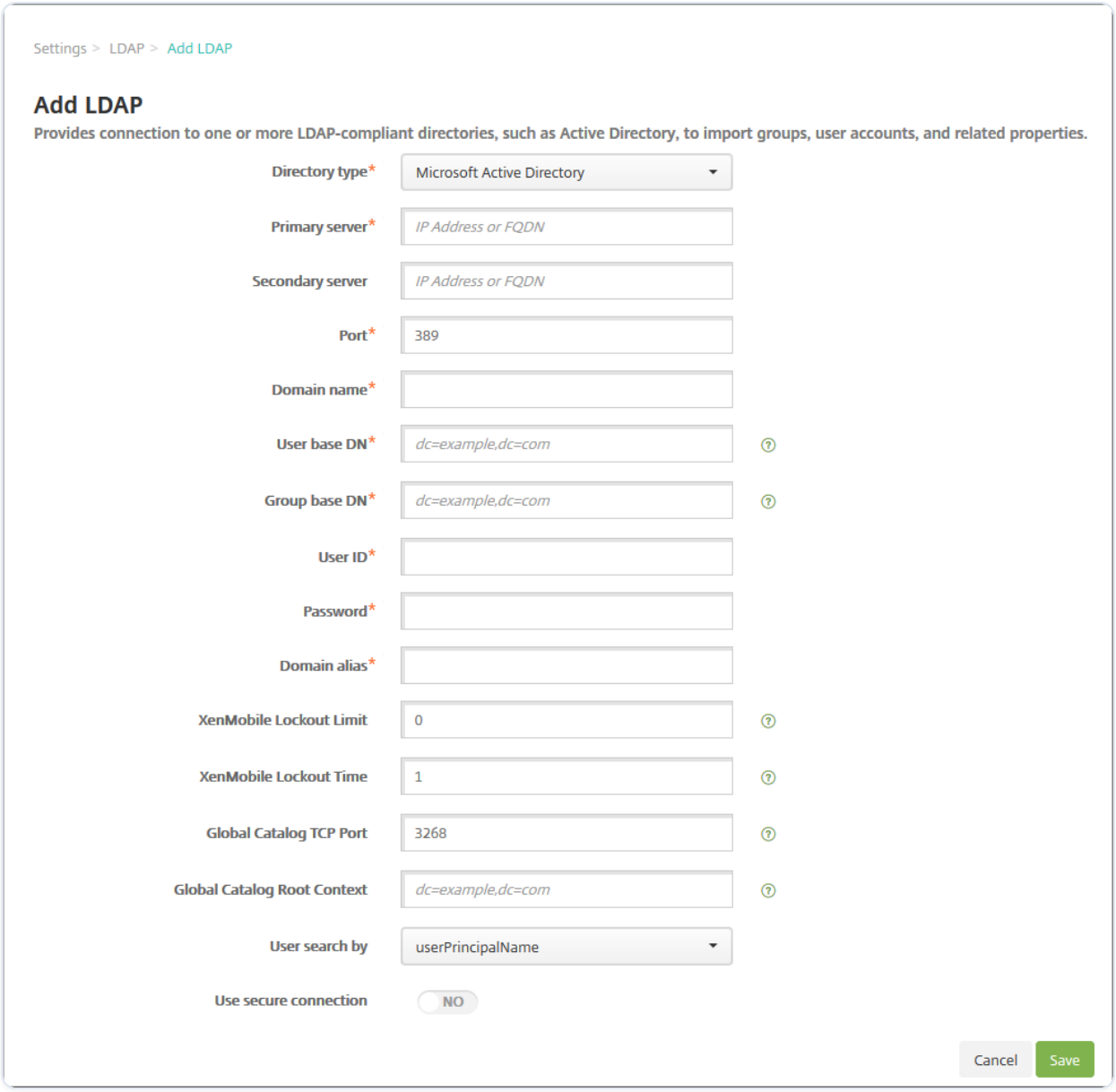
在 XenMobile 中添加 LDAP 连接

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。**设置**页面随即显示。
2. 在**服务器**下，单击**LDAP**。**LDAP**页面随即显示。您可以添加、编辑或删除符合 LDAP 的目录，如本文所述。



添加符合 LDAP 的目录

1. 在**LDAP**页面上，单击**添加**。**添加 LDAP**页面随即显示。



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 地址或完全限定域名 (FQDN)。
- **辅助服务器：** （可选）如果已配置辅助服务器，请输入辅助服务器的 IP 地址或 FQDN。此服务器是主服务器无法访问时使用的故障转移服务器。
- **端口：** 键入 LDAP 服务器使用的端口号。默认情况下，未加密 LDAP 连接的端口号设置为 **389**。安全 LDAP 连接使用端口号 **636**，Microsoft 未加密 LDAP 连接使用 **3268**，Microsoft 安全 LDAP 连接使用 **3269**。
- **域名：** 键入域名。
- **用户基本 DN：** 通过唯一标识符键入 Active Directory 中用户的位置。语法示例包括：`ou=users`、`dc=example` 或 `dc=com`。
- **组基本 DN：** 键入 Active Directory 中组的位置。例如，`cn=users, dc=domain, dc=net`，其中 `cn=users` 表示组的容器名称，`dc` 表示 Active Directory 的域组件。
- **用户 ID：** 键入与 Active Directory 帐户关联的用户 ID。
- **密码：** 键入与用户关联的密码。
- **域别名：** 键入域名的别名。如果在注册后更改了**域别名**设置，用户必须重新注册。
- **XenMobile 锁定限制：** 键入一个介于 **0** 到 **999** 之间的数字，表示失败登录尝试的次数。值为 **0** 表示 XenMobile 永远不会根据失败的登录尝试锁定用户。
- **XenMobile 锁定时间：** 键入一个介于 **0** 到 **99999** 之间的数字，表示用户在超出锁定限制后必须等待的分钟数。值为 **0** 表示用户在锁定后无需强制等待。
- **全局编录 TCP 端口：** 键入全局编录服务器的 TCP 端口号。默认情况下，TCP 端口号设置为 **3268**；对于 SSL 连接，请使用端口号 **3269**。
- **全局编录根上下文：** （可选）键入用于在 Active Directory 中启用全局编录搜索的全局根上下文值。此搜索是对标准 LDAP 搜索的补充，可在任何域中进行，而无需指定实际域名。
- **用户搜索依据：** 在列表中，单击 **userPrincipalName** 或 **sAMAccountName**。默认值为 **userPrincipalName**。如果在注册后更改了**用户搜索依据**设置，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**。

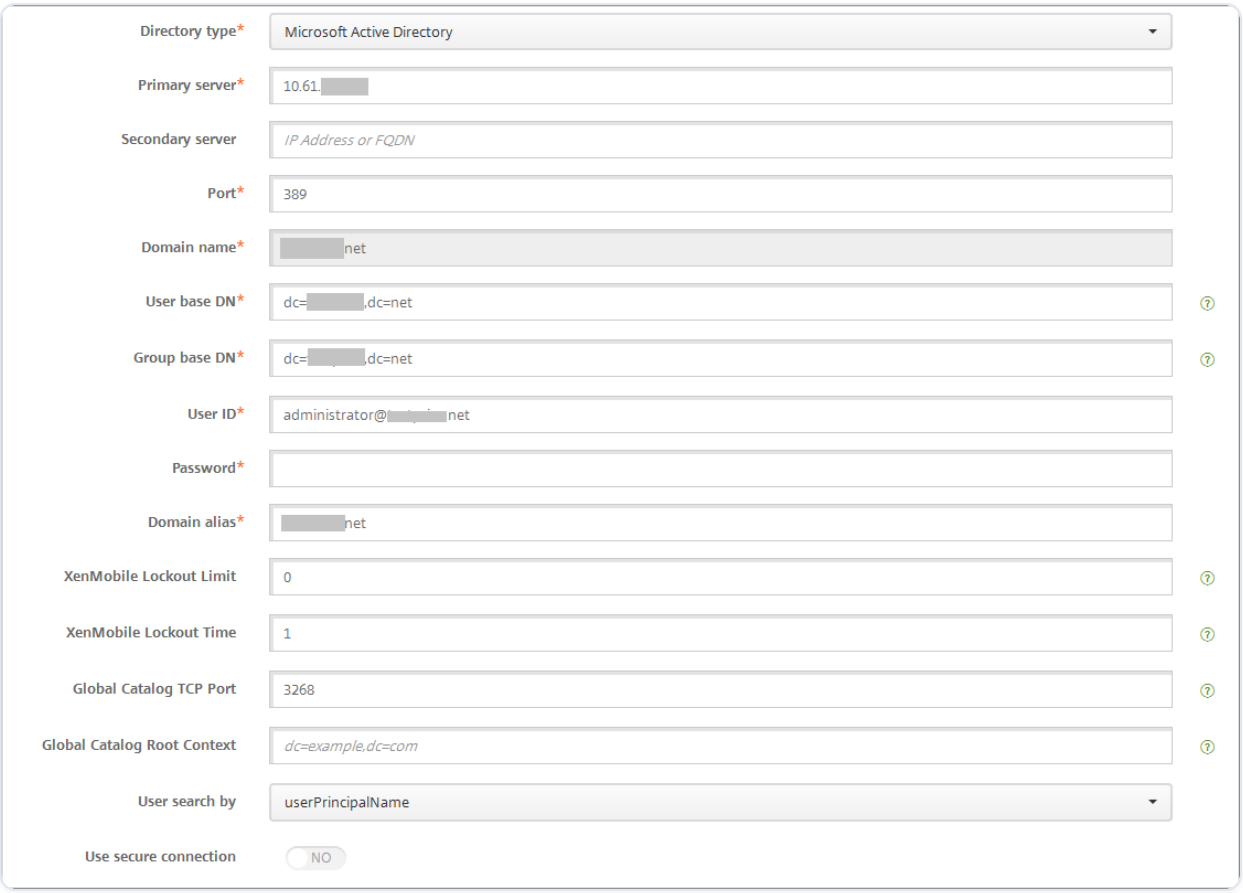
3. 单击**保存**。

编辑符合 LDAP 标准的目录

1. 在 **LDAP** 表中，选择要编辑的目录。

选中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的右侧。

2. 单击**编辑**。此时将显示**编辑 LDAP** 页面。



3. 根据需要更改以下信息：

- **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（如果已配置）。
- **端口：** 键入 LDAP 服务器使用的端口号。默认情况下，未加密 LDAP 连接的端口号设置为 **389**。安全 LDAP 连接使用端口号 **636**，Microsoft 未加密 LDAP 连接使用 **3268**，Microsoft 安全 LDAP 连接使用 **3269**。
- **域名：** 您无法更改此字段。
- **用户基本 DN：** 通过唯一标识符键入 Active Directory 中用户的位置。语法示例包括：`ou=users`、`dc=example` 或 `dc=com`。
- **组基本 DN：** 键入指定为 `cn=groupname` 的组基本 DN 组名称。例如，`cn=users, dc=servername, dc=net`，其中 `cn=users` 是组名称。`DN` 和 `servername` 表示运行 Active Directory 的服务器名称。

- **用户 ID：** 输入与 Active Directory 帐户关联的用户 ID。
- **密码：** 输入与用户关联的密码。
- **域别名：** 输入域名的别名。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：** 输入一个介于 **0** 到 **999** 之间的数字，表示失败登录尝试的次数。值为 **0** 表示 XenMobile 永远不会根据失败的登录尝试锁定用户。
- **XenMobile 锁定时间：** 输入一个介于 **0** 到 **99999** 之间的数字，表示用户在超出锁定限制后必须等待的分钟数。值为 **0** 表示用户在锁定后无需强制等待。
- **全局编录 TCP 端口：** 输入全局编录服务器的 TCP 端口号。默认情况下，TCP 端口号设置为 **3268**；对于 SSL 连接，请使用端口号 **3269**。
- **全局编录根上下文：** （可选）输入用于在 Active Directory 中启用全局编录搜索的全局根上下文值。此搜索是对标准 LDAP 搜索的补充，可在任何域中进行，无需指定实际域名。
- **用户搜索依据：** 在列表中，单击 **userPrincipalName** 或 **sAMAccountName**。如果在注册后更改**用户搜索依据**设置，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**以保存更改，或单击**取消**以使属性保持不变。

删除符合 LDAP 的目录

1. 在 **LDAP** 表中，选择要删除的目录。

   您可以通过选中每个属性旁边的复选框来选择多个要删除的属性。

2. 单击**删除**。将显示确认对话框。再次单击**删除**。

配置多个域的身份验证

要配置 XenMobile Server 在 LDAP 配置中使用多个域后缀，请参阅 Citrix Endpoint Management 文档中的过程，配置多个域的身份验证。这些步骤在 XenMobile Server 的本地版本和 Endpoint Management 云版本中是相同的。

配置域加安全令牌身份验证

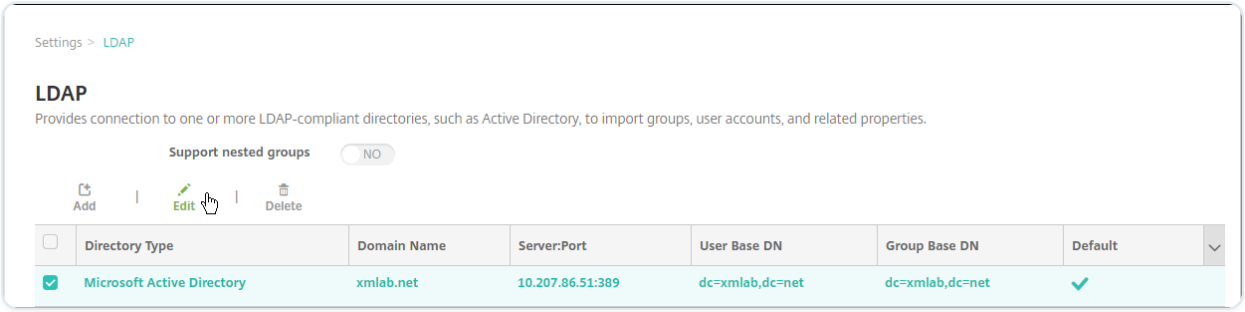
您可以将 XenMobile 配置为要求用户使用其 LDAP 凭据加上一次性密码（通过 RADIUS 协议）进行身份验证。

为了获得最佳可用性，您可以将此配置与 Citrix PIN 和 Active Directory 密码缓存结合使用。通过该配置，用户无需重复输入其 LDAP 用户名和密码。用户在注册、密码过期和帐户锁定期间输入用户名和密码。

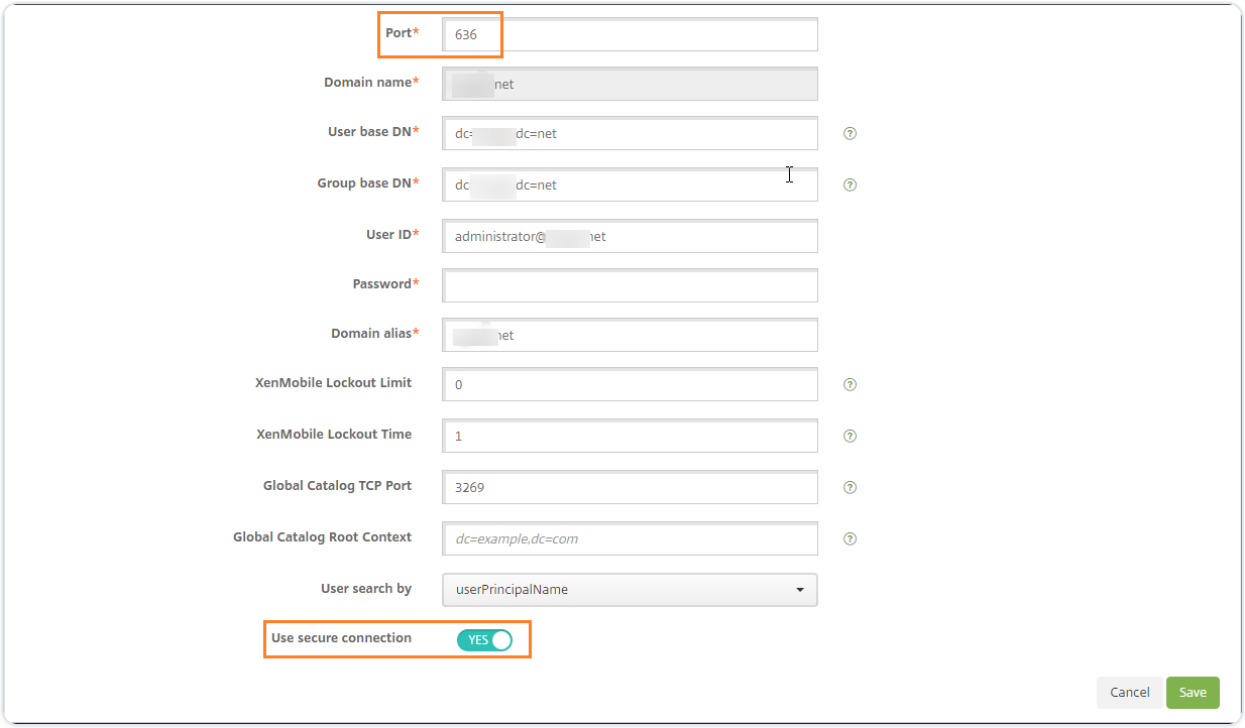
配置 LDAP 设置

使用 LDAP 进行身份验证要求您在 XenMobile 上安装来自证书颁发机构的 SSL 证书。有关信息，请参阅在 XenMobile 中上传证书。

1. 在 **Settings**（设置）中，单击 **LDAP**。
2. 选择 **Microsoft Active Directory**，然后单击 **Edit**（编辑）。



3. 验证端口是否为 **636**（用于安全 LDAP 连接）或 **3269**（用于 Microsoft 安全 LDAP 连接）。
4. 将 **Use secure connection**（使用安全连接）更改为 **Yes**（是）。

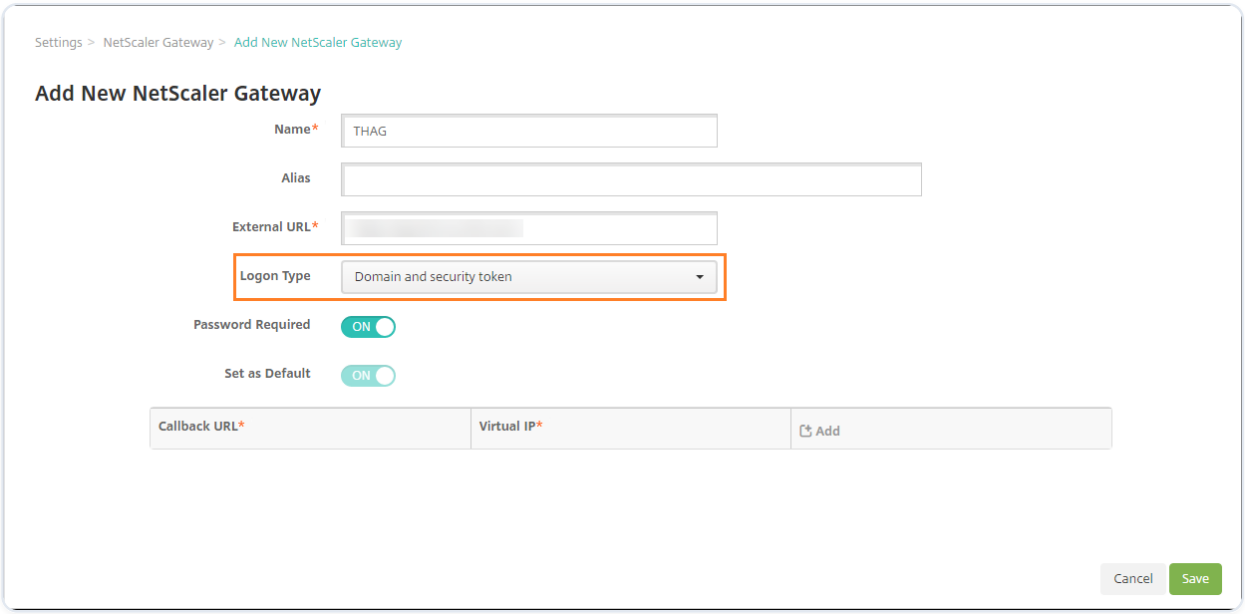


配置 Citrix Gateway 设置

以下步骤假定您已将 Citrix Gateway 实例添加到 XenMobile。要添加 Citrix Gateway 实例，请参阅添加 Citrix Gateway 实例。

1. 在 **Settings**（设置）中，单击 **Citrix Gateway**。
2. 选择 **“Citrix Gateway”**，然后单击 **“编辑”**。

3. 从 **“登录类型”** 中，选择 **“域和安全令牌”**。



启用 Citrix PIN 和用户密码缓存

要启用 Citrix PIN 和用户密码缓存，请转至 **“设置”>“客户端属性”**，然后选择以下复选框：**“启用 Citrix PIN 身份验证”** 和 **“启用用户密码缓存”**。有关详细信息，请参阅客户端属性。

配置 Citrix Gateway 以用于域和安全令牌身份验证

为与 XenMobile 结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

XenMobile® 的默认配置是用户名和密码身份验证。要为注册和访问 XenMobile 环境增加一层安全性，请考虑使用基于证书的身份验证。在 XenMobile 环境中，此配置是安全性与用户体验的最佳组合。证书加域身份验证具有最佳的 SSO 可能性，并结合了 Citrix ADC 提供的双因素身份验证安全性。

为了获得最佳可用性，您可以将证书加域身份验证与 Citrix PIN 和 Active Directory 密码缓存结合使用。因此，用户无需重复输入其 LDAP 用户名和密码。用户在注册、密码过期和帐户锁定期间输入用户名和密码。

> **重要提示：**
>
> 在用户将设备注册到 XenMobile 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。

> 如果您不允许 LDAP 并使用智能卡或类似方法，则配置证书可让您将智能卡表示给 XenMobile。然后，用户使用 XenMobile 为其生成的唯一 PIN 进行注册。用户获得访问权限后，XenMobile 会创建并部署用于向 XenMobile 环境进行身份验证的证书。

您可以使用 Citrix ADC for XenMobile 向导在 Citrix ADC 仅证书身份验证或证书加域身份验证时执行 XenMobile 所需的配置。Citrix ADC for XenMobile 向导只能运行一次。

在高度安全的环中，在公共或不安全网络中，在组织外部使用 LDAP 凭据被认为是组织的主要安全威胁。对于高度安全的环，使用客户端证书和安全令牌的双因素身份验证是一种选择。有关信息，请参阅 Configuring XenMobile for Certificate and Security Token Authentication。

客户端证书身份验证适用于 XenMobile MAM 模式（仅限 MAM）和 ENT 模式（当用户注册到 MDM 时）。客户端证书身份验证不适用于用户注册到旧版 MAM 模式时的 XenMobile ENT 模式。要将客户端证书身份验证用于 XenMobile ENT 和 MAM 模式，您必须配置 Microsoft 服务器、XenMobile 服务器，然后配置 Citrix Gateway。请按照本文中介绍的这些常规步骤操作。

在 Microsoft 服务器上：

1. 将证书管理单元添加到 Microsoft 管理控制台。
2. 将模板添加到证书颁发机构 (CA)。
3. 从 CA 服务器创建 PFX 证书。

在 XenMobile 服务器上：

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. 配置 Citrix Gateway 以交付用户证书进行身份验证。

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

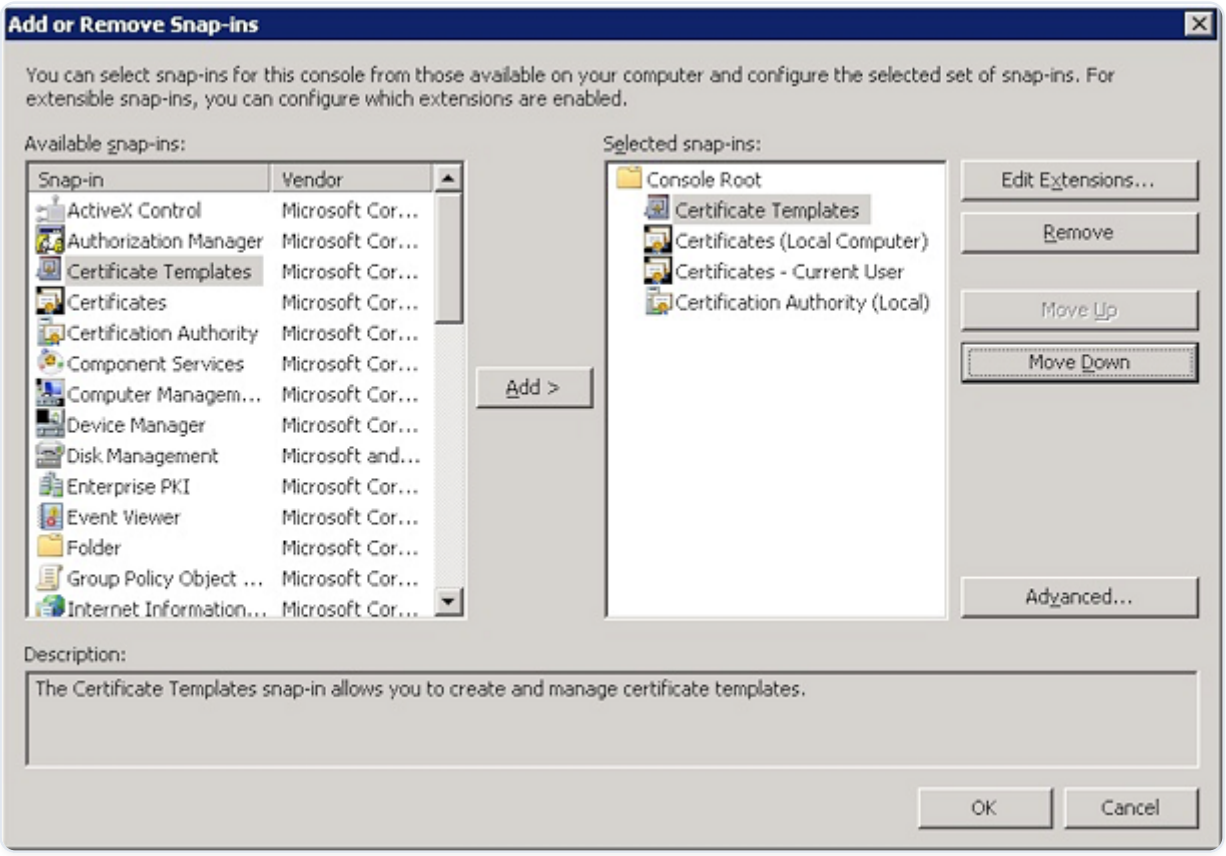
先决条件

- 创建 Microsoft 证书服务实体模板时，请通过排除特殊字符来避免已注册设备可能出现的身份验证问题。例如，请勿在模板名称中使用以下字符：`: ! $ () # % + * ~ ? | {} []`

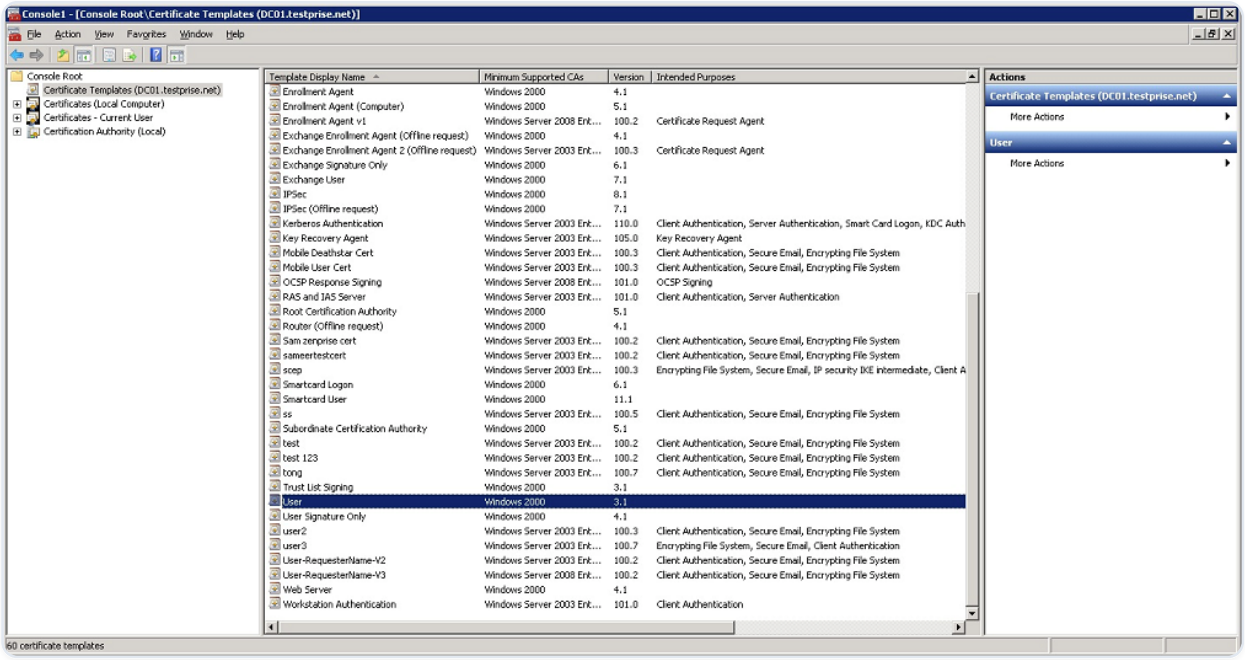
- 要为 Exchange ActiveSync 配置基于证书的身份验证，请参阅此Microsoft 博客。将 Exchange ActiveSync 的证书颁发机构 (CA) 服务器站点配置为要求客户端证书。
- 如果您使用私有服务器证书来保护 ActiveSync 到 Exchange Server 的流量，请确保移动设备具有所有必需的根/中间证书。否则，在 Secure Mail 中设置邮箱期间，基于证书的身份验证将失败。在 Exchange IIS 控制台中，您必须：
  - 添加一个用于 XenMobile 与 Exchange 结合使用的网站，并绑定 Web 服务器证书。
  - 使用端口 9443。
  - 对于该网站，您必须添加两个应用程序，一个用于“Microsoft-Server-ActiveSync”，另一个用于“EWS”。对于这两个应用程序，在**SSL 设置**下，选择**要求 SSL**。

将证书管理单元添加到 Microsoft 管理控制台

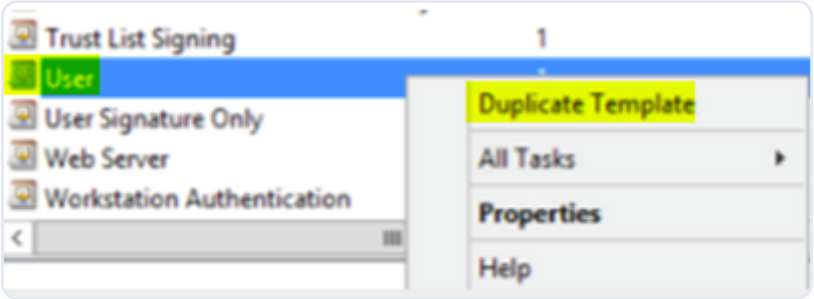
1. 打开控制台，然后单击**添加/删除管理单元**。
2. 添加以下管理单元：
   - 证书模板
   - 证书（本地计算机）
   - 证书 - 当前用户
   - 证书颁发机构（本地）



3. 展开**证书模板**。



4. 选择**用户**模板，然后**复制模板**。



5. 提供模板显示名称。

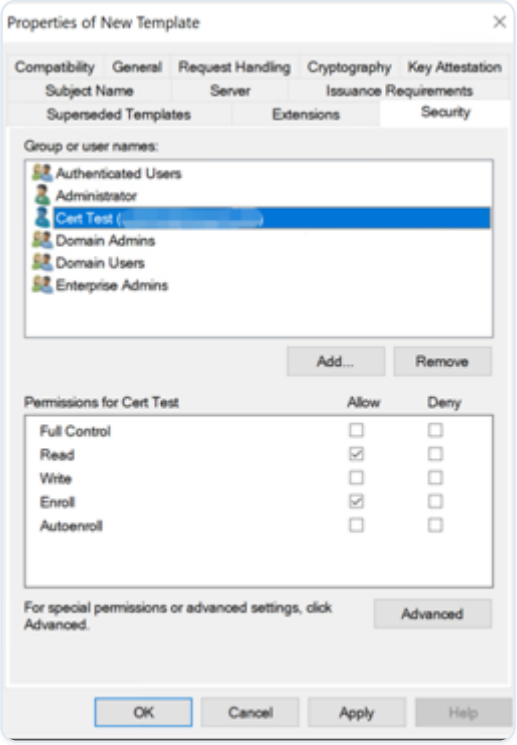
> **重要提示：**
>
> 不建议选择**在 Active Directory 中发布证书**选项。如果选择此选项，它会为 Active Directory 中的所有用户创建客户端证书，这可能会使您的 Active Directory 数据库变得混乱。

6. 为模板类型选择 **Windows 2003 Server**。在 Windows 2012 R2 服务器中，在**兼容性**下，选择**证书颁发机构**并将收件人设置为 **Windows 2003**。
7. 在“**安全性**”下，配置以下内容：
   a. 单击“**添加**”，然后选择 XenMobile Server 用于生成证书的 AD 用户帐户。

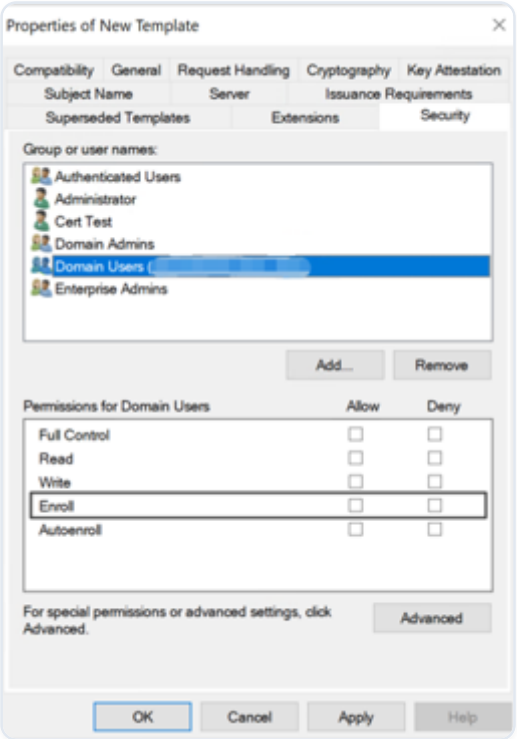
> **重要提示：**

> 此处仅添加服务帐户用户。仅将“**注册**”权限添加到此 AD 用户帐户。

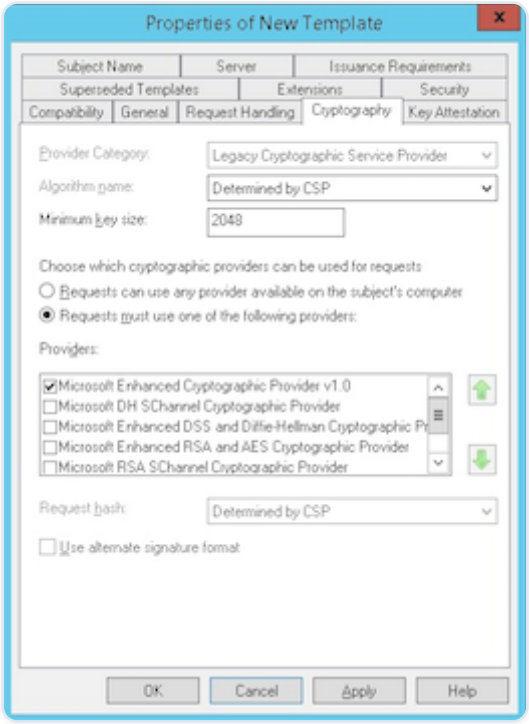
> 如本文后面所述，您将使用服务帐户创建用户 .pfx 证书。有关信息，请参阅从 CA 服务器创建 PFX 证书。



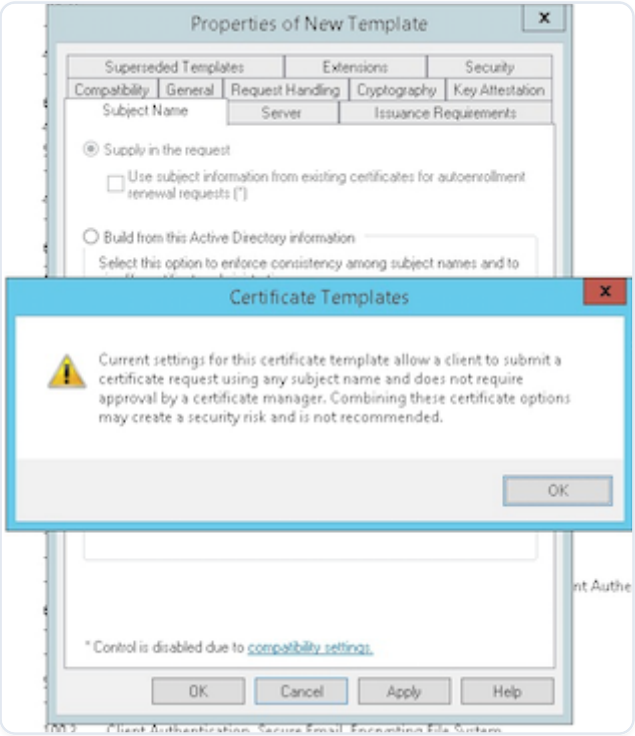
b. 从“**域用户**”中撤销“**注册**”权限。



8. 在“**加密**”下，确保提供密钥大小。稍后在配置 XenMobile 时输入密钥大小。

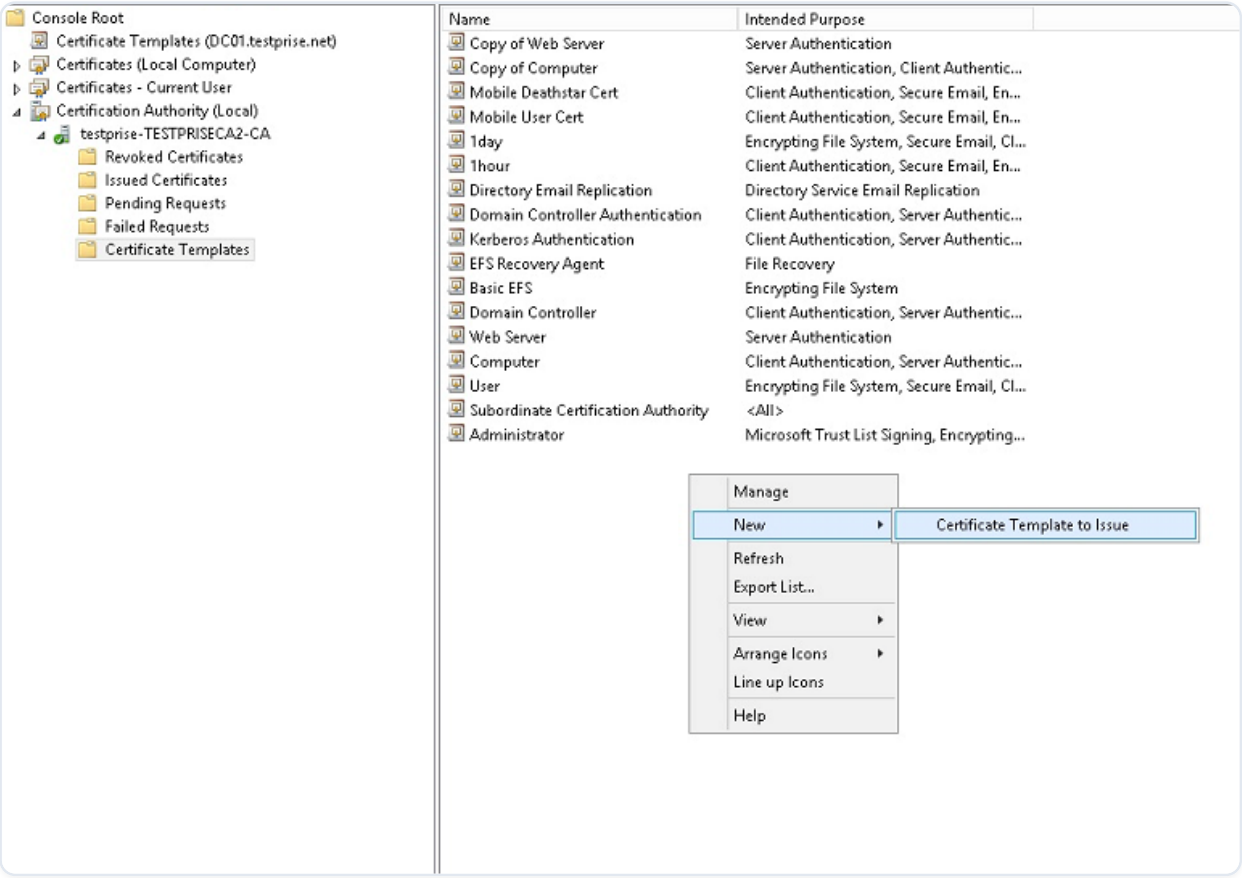


9. 在“**使用者名称**”下，选择“**在请求中提供**”。应用更改，然后保存。

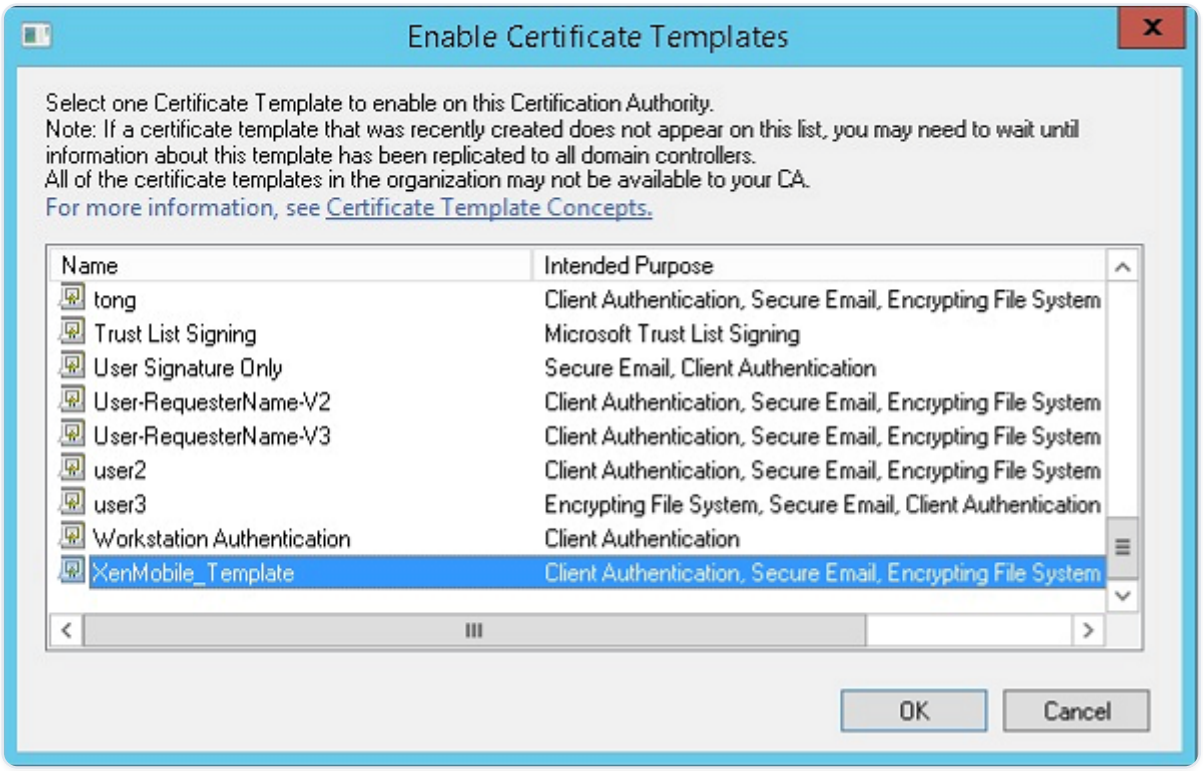


将模板添加到证书颁发机构

1. 转到“**证书颁发机构**”，然后选择“**证书模板**”。
2. 右键单击右侧窗格，然后选择“**新建 > 要颁发的证书模板**”。

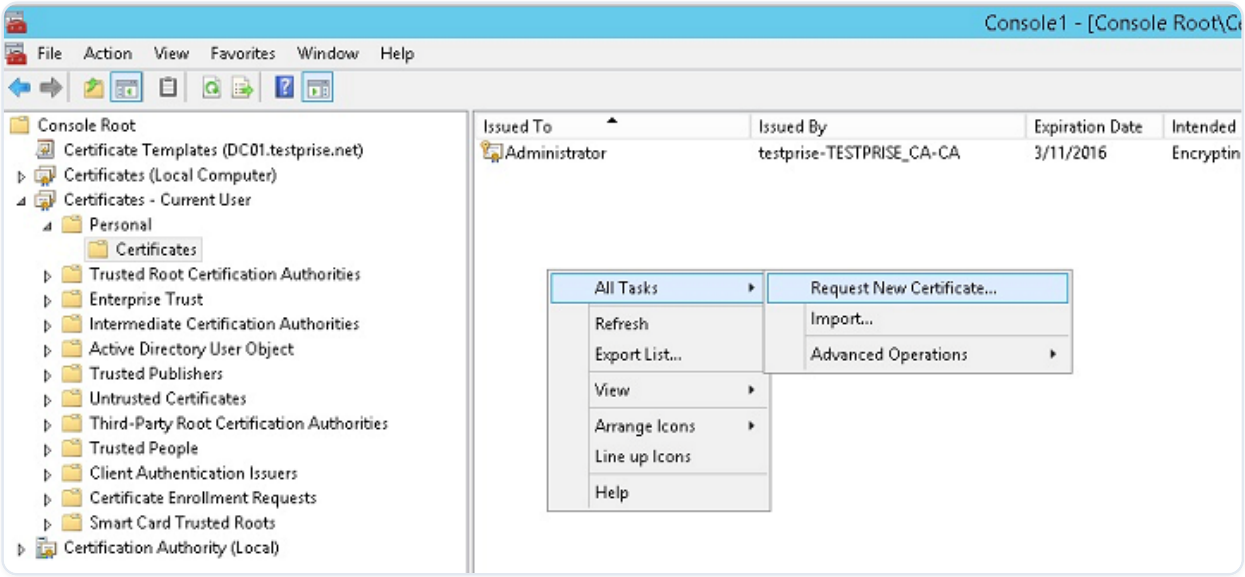


3. 选择您在上一步中创建的模板，然后单击“**确定**”以将其添加到“**证书颁发机构**”中。

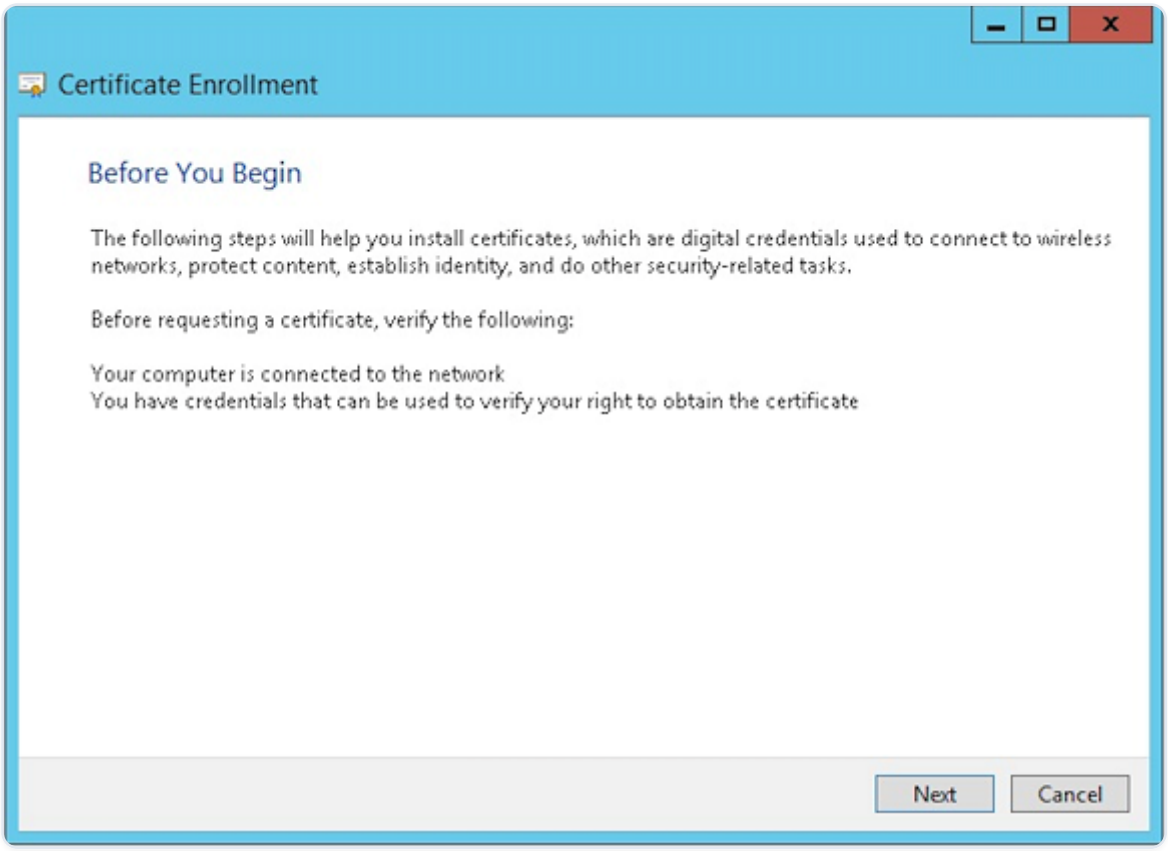


从 CA 服务器创建 PFX 证书

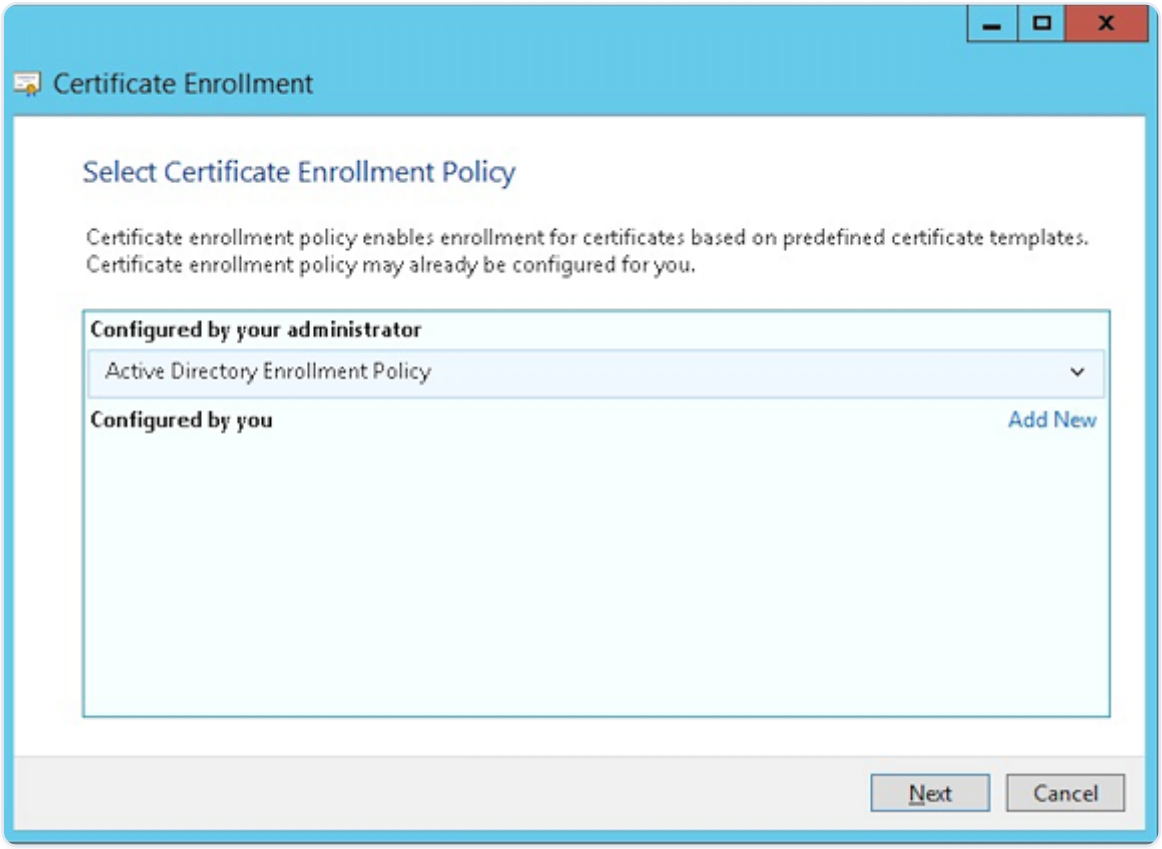
1. 使用您登录时所用的服务帐户创建用户 .pfx 证书。此 .pfx 文件将上传到 XenMobile，XenMobile 随后会代表注册其设备的用户请求用户证书。
2. 在“**当前用户**”下，展开“**证书**”。
3. 在右侧窗格中右键单击，然后单击“**请求新证书**”。



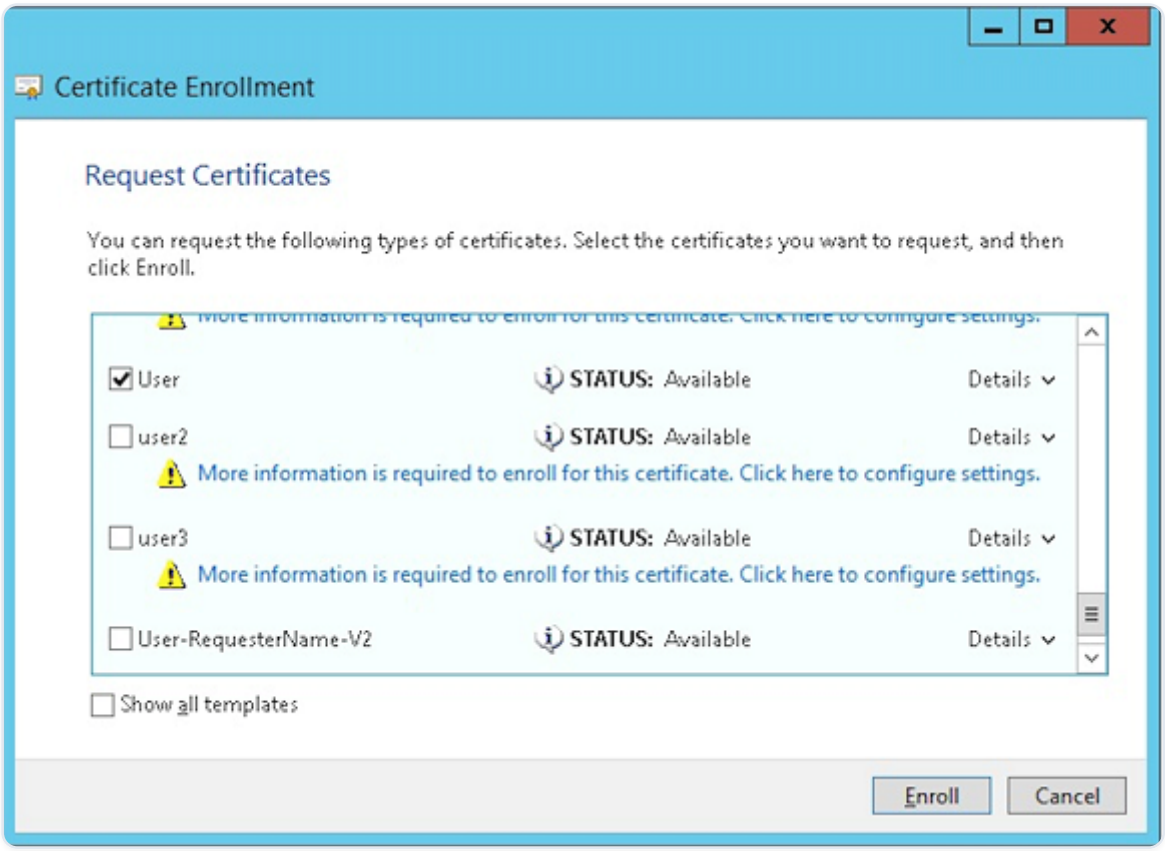
4. 此时将显示“**证书注册**”屏幕。单击“**下一步**”。



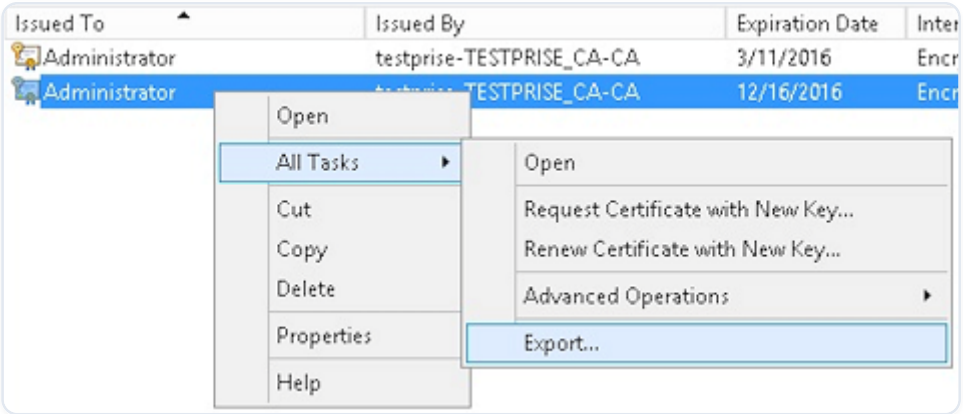
5. 选择“**Active Directory 注册策略**”，然后单击“**下一步**”。



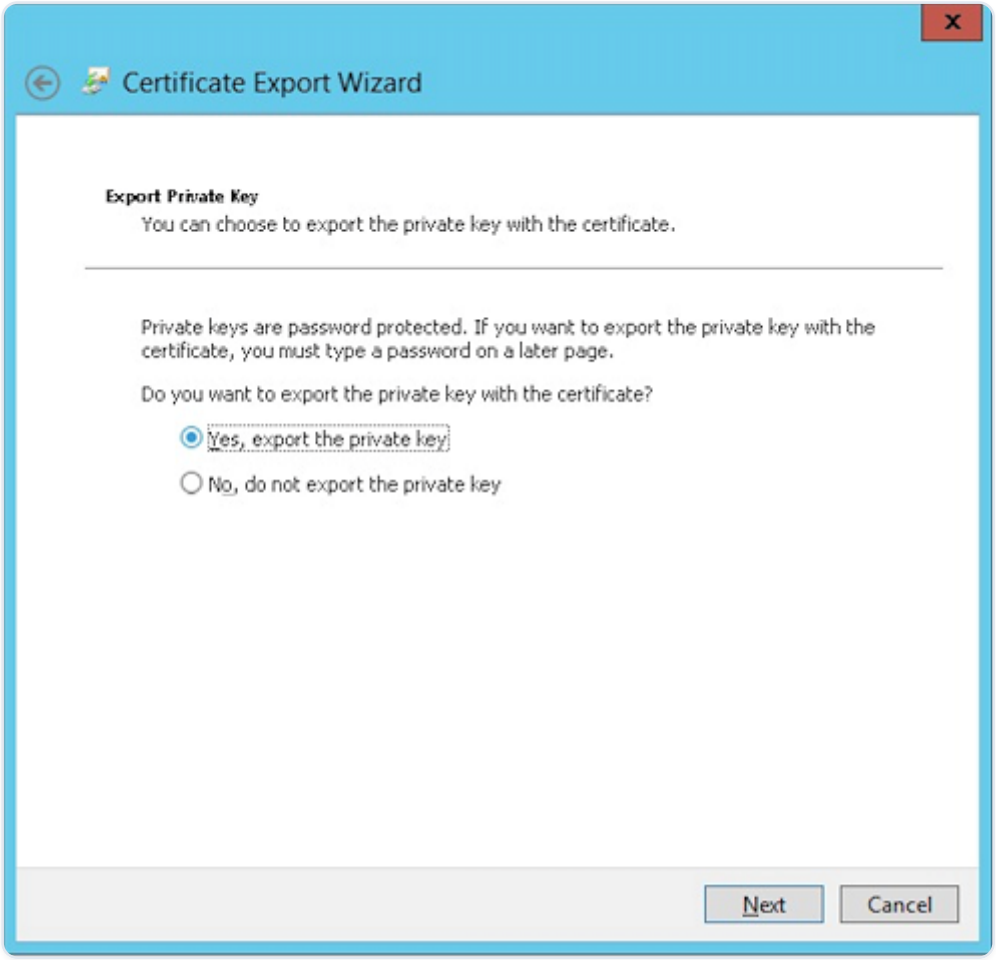
6. 选择“**用户**”模板，然后单击“**注册**”。



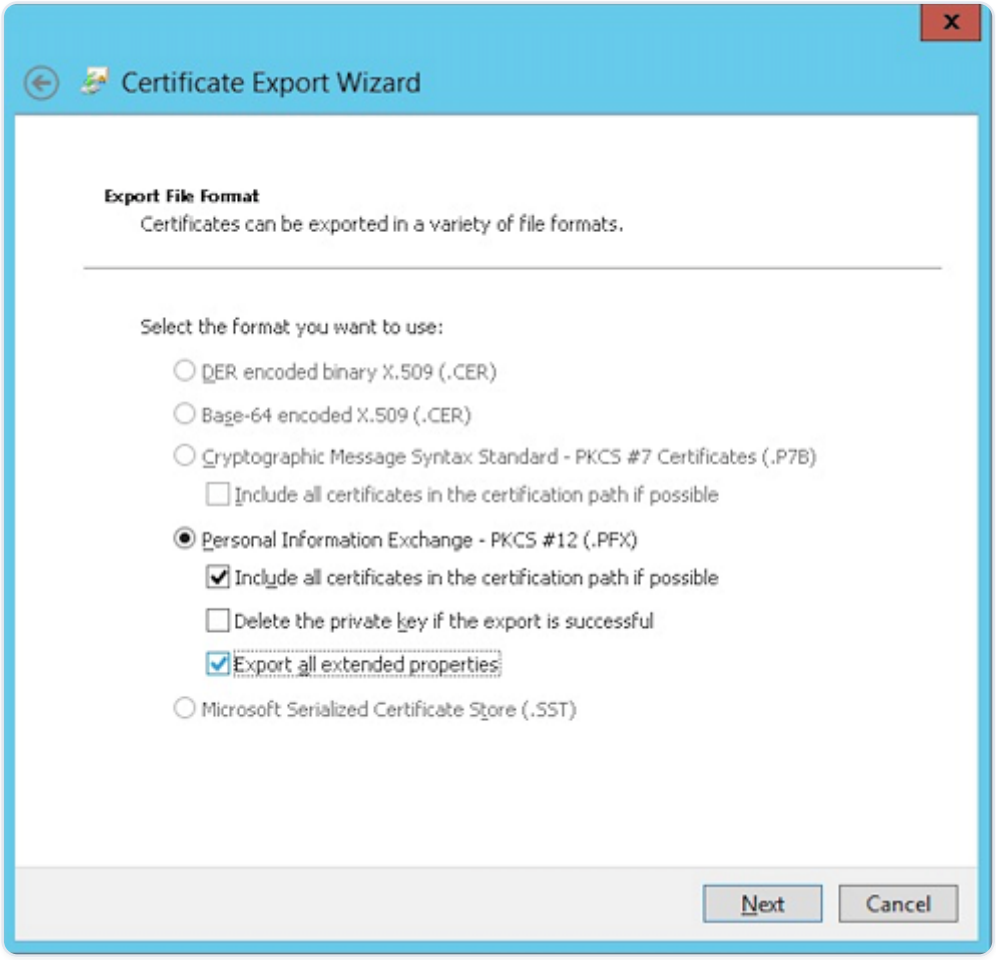
7. 导出您在上一步中创建的 .pfx 文件。



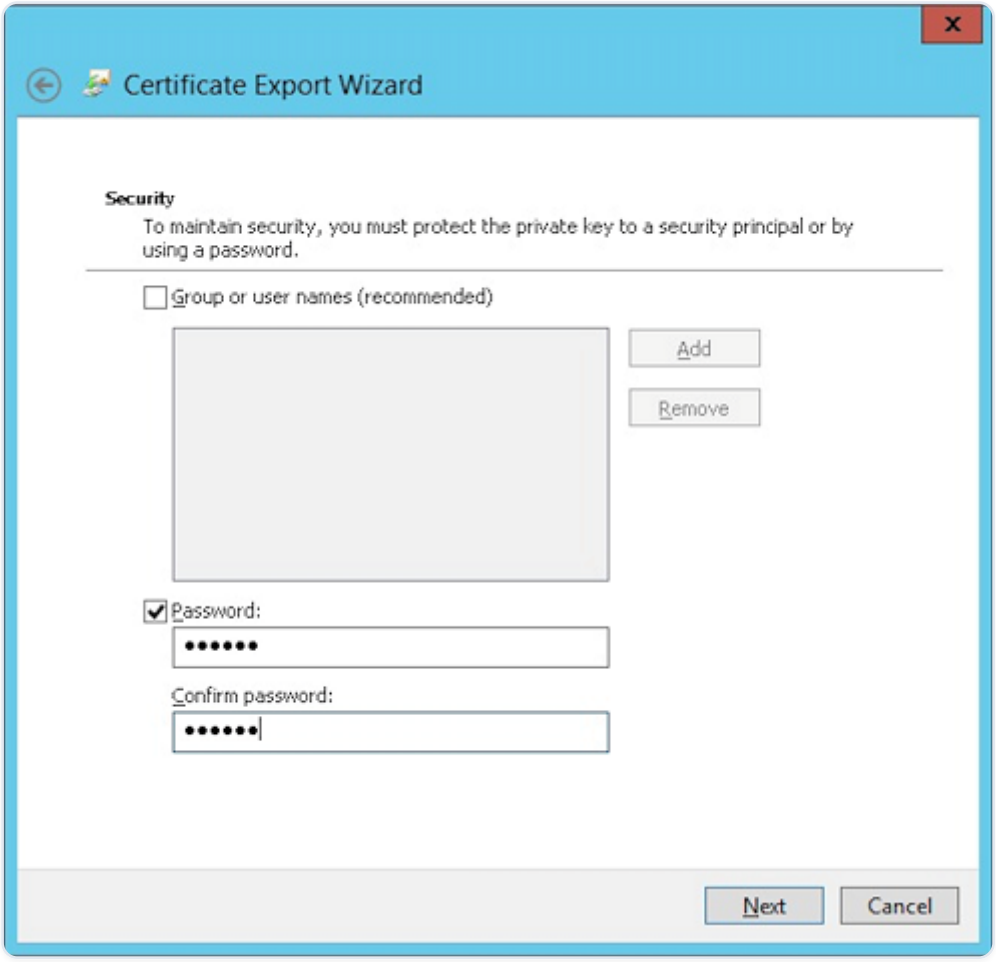
8. 单击**是，导出私钥**。



9. 选择**如果可能，包括证书路径中的所有证书**，然后选中**导出所有扩展属性**复选框。



10. 设置在将此证书上载到 XenMobile 时使用的密码。

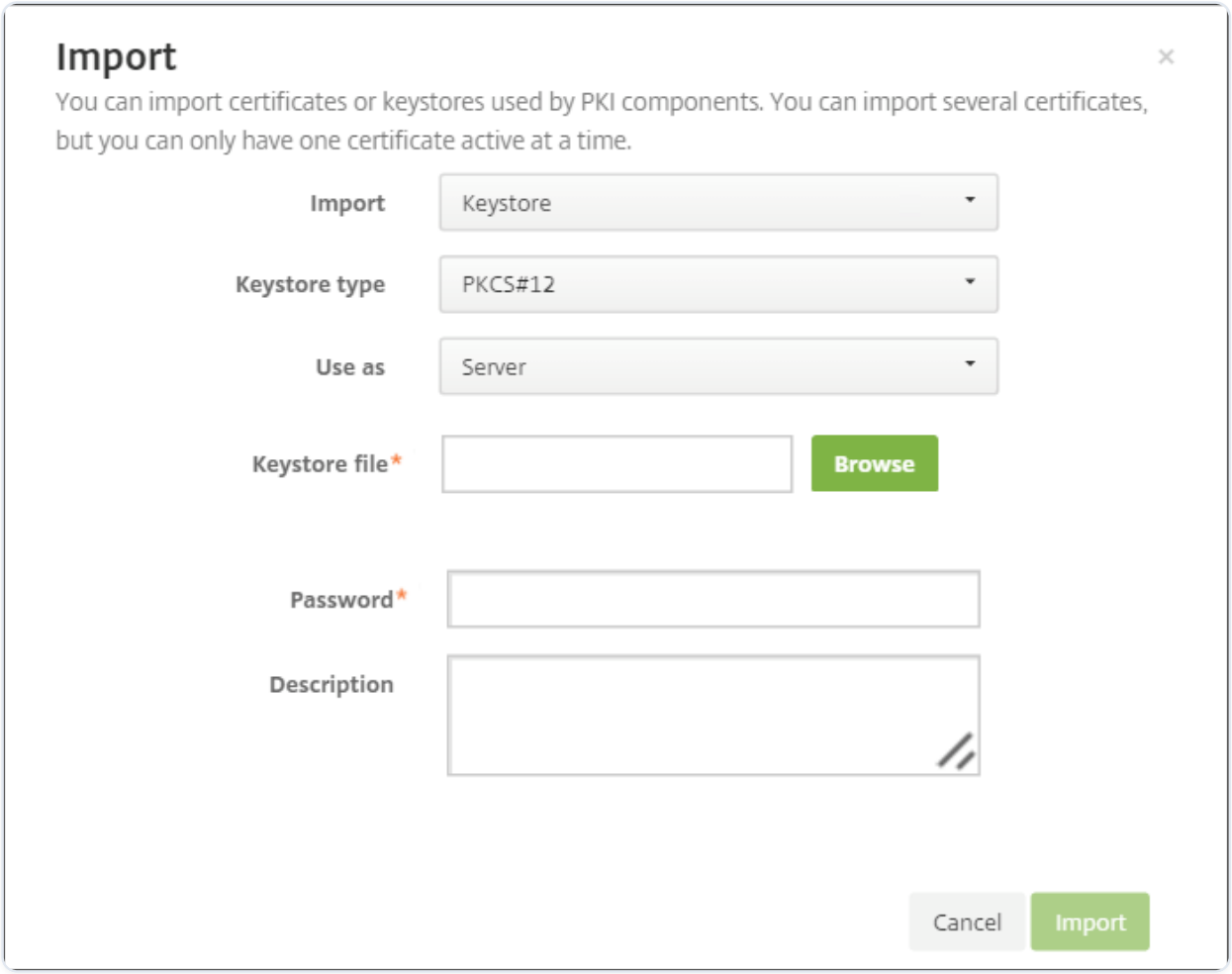


11. 将证书保存到硬盘驱动器。

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. 单击**证书**，然后单击**导入**。
3. 输入以下参数：

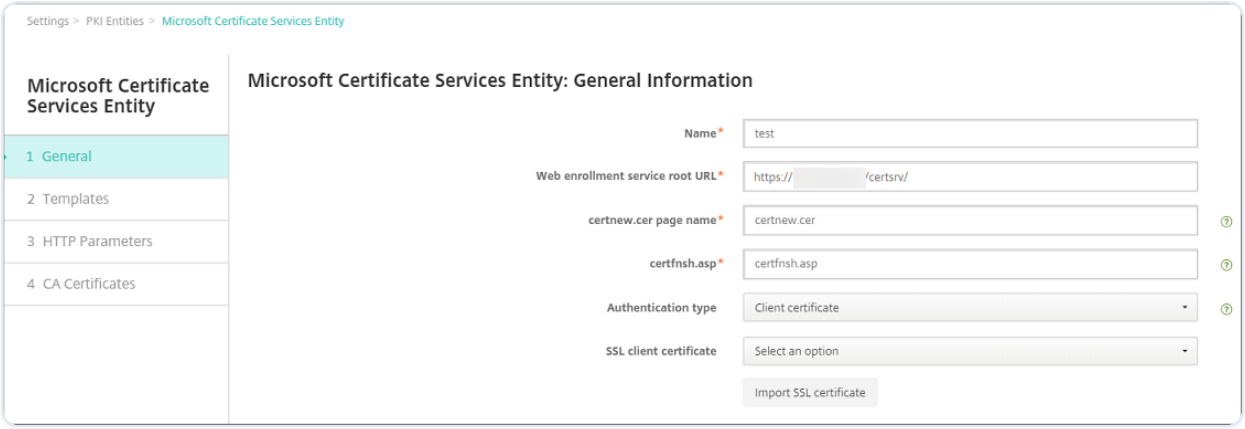
   - **导入：** 密钥库
   - **密钥库类型：** PKCS #12
   - **用作：** 服务器
   - **密钥库文件**：单击“**浏览**”以选择您创建的 `.pfx` 证书。
   - **密码**：输入您为此证书创建的密码。



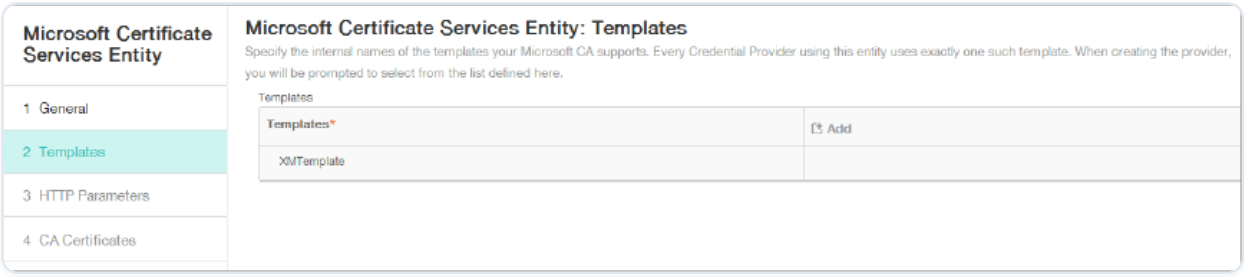
4. 单击“**导入**”。
5. 验证证书是否已正确安装。正确安装的证书将显示为用户证书。

创建用于基于证书的身份验证的 PKI 实体

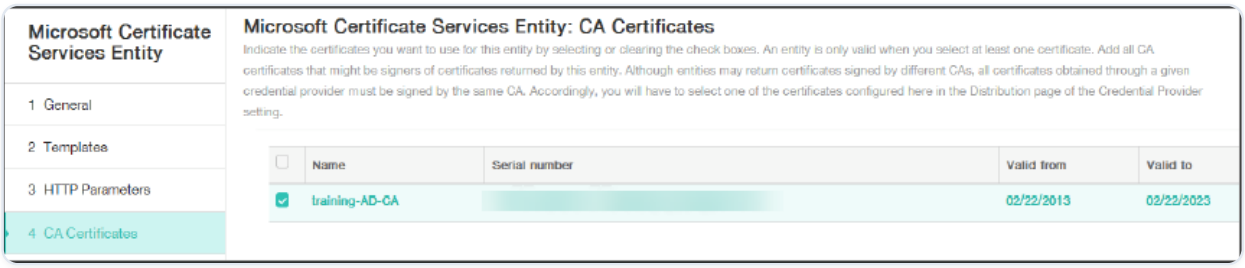
1. 在“**设置**”中，转至“**更多 > 证书管理 > PKI 实体**”。
2. 单击“**添加**”，然后单击“**Microsoft 证书服务实体**”。此时将显示“**Microsoft 证书服务实体: 常规信息**”屏幕。
3. 输入以下参数：
   - **名称**：键入任何名称
   - **Web 注册服务根 URL**：`https://RootCA-URL/certsrv/`（请务必在 URL 路径中添加最后一个斜杠 /。）
   - **certnew.cer 页面名称**：certnew.cer（默认值）
   - **certfnsh.asp**：certfnsh.asp（默认值）
   - **身份验证类型**：客户端证书
   - **SSL 客户端证书**：选择用于颁发 XenMobile 客户端证书的用户证书。



4. 在**模板**下，添加您在配置 Microsoft 证书时创建的模板。请勿添加空格。



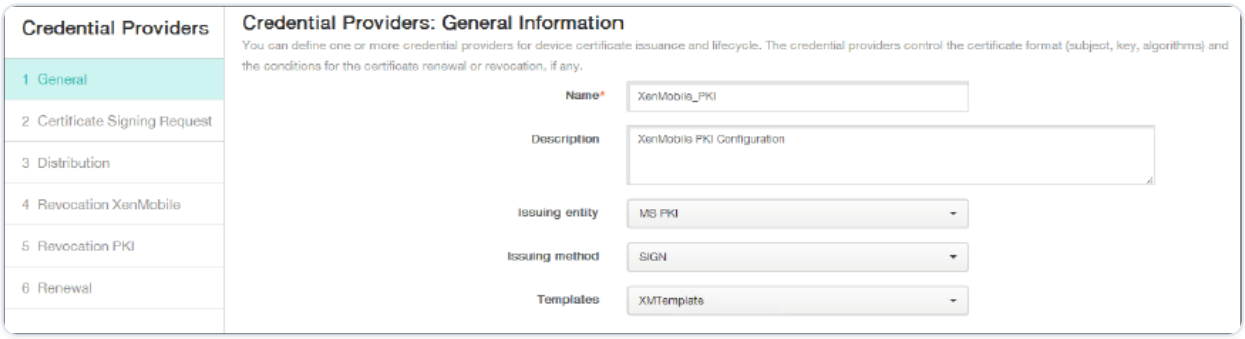
5. 跳过 HTTP 参数，然后单击**CA 证书**。
6. 选择与您的环境对应的根 CA 名称。此根 CA 是从 XenMobile 客户端证书导入的链的一部分。



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，输入以下参数：
   - **名称：** 键入任何名称。
   - **描述：** 键入任何描述。
   - **颁发实体：** 选择之前创建的 PKI 实体。
   - **颁发方法：** SIGN
   - **模板**：选择在 PKI 实体下添加的模板。

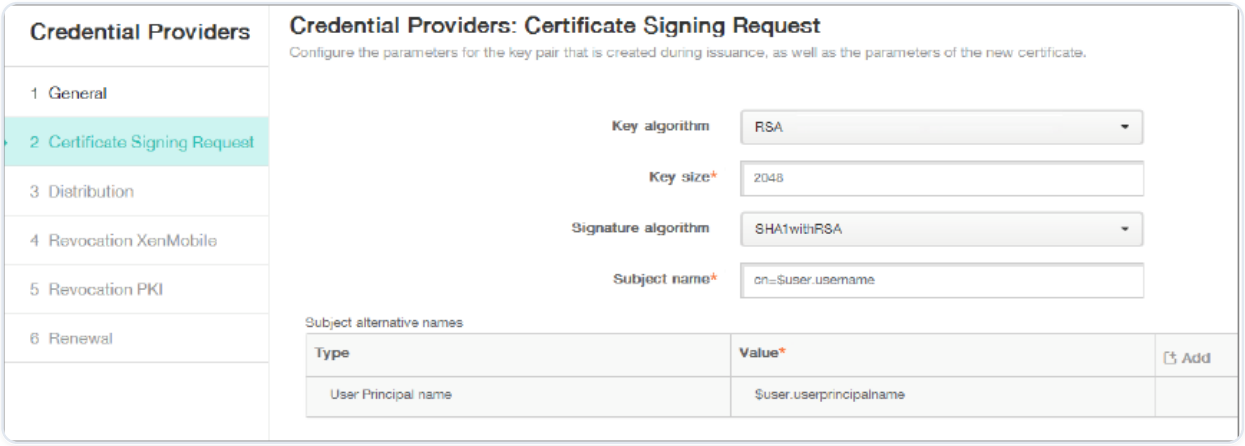


4. 单击“**证书签名请求**”，然后输入以下参数：

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

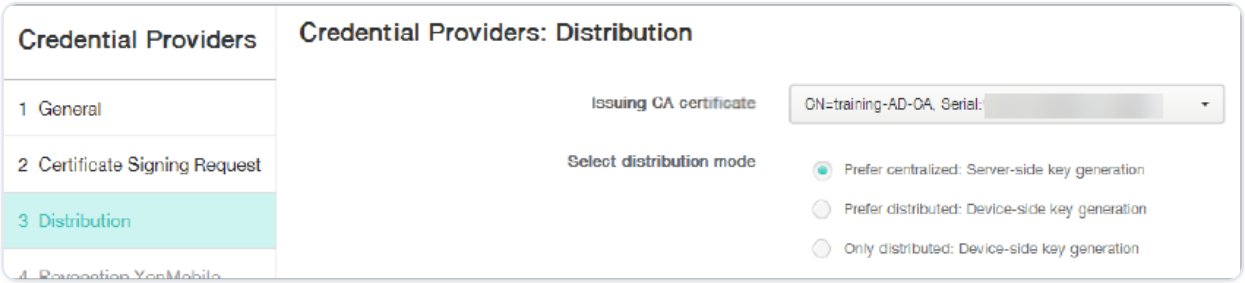
   对于“**使用者备用名称**”，单击“**添加**”，然后输入以下参数：

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

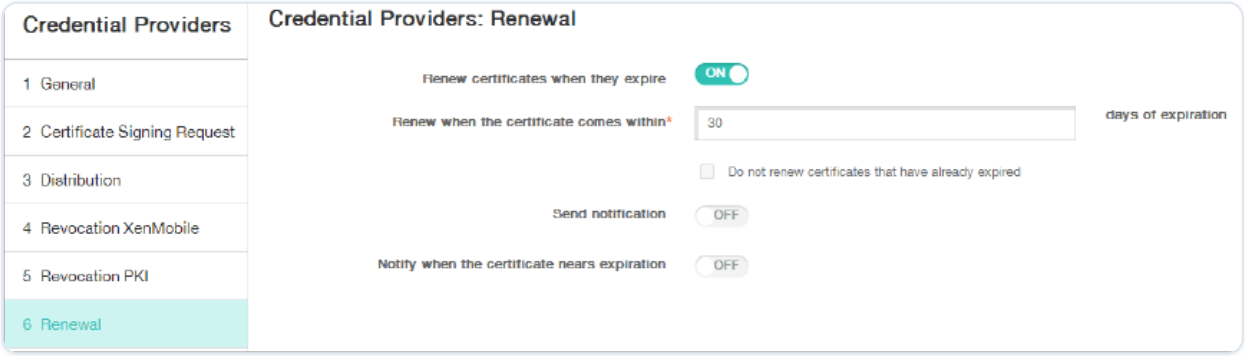


5. 单击“**分发**”，然后输入以下参数：

   - **颁发 CA 证书**：选择为 XenMobile 客户端证书签名的颁发 CA。
   - **选择分发模式**：选择“**首选集中式：服务器端密钥生成**”。



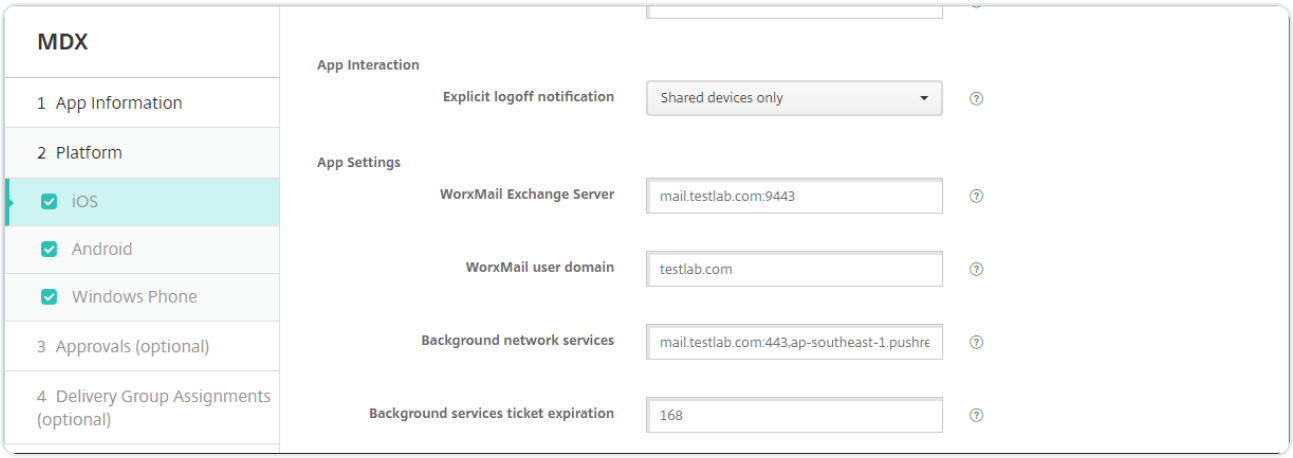
6. 对于接下来的两个部分，**吊销 XenMobile** 和 **吊销 PKI**，请根据需要设置参数。在此示例中，这两个选项都已跳过。
7. 单击 **续订**。
8. 对于 **证书过期时续订**，选择 **开**。
9. 将所有其他设置保留为默认值或根据需要进行更改。



10. 单击 **保存**。

配置 Secure Mail 以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** 下配置 Exchange 设置。

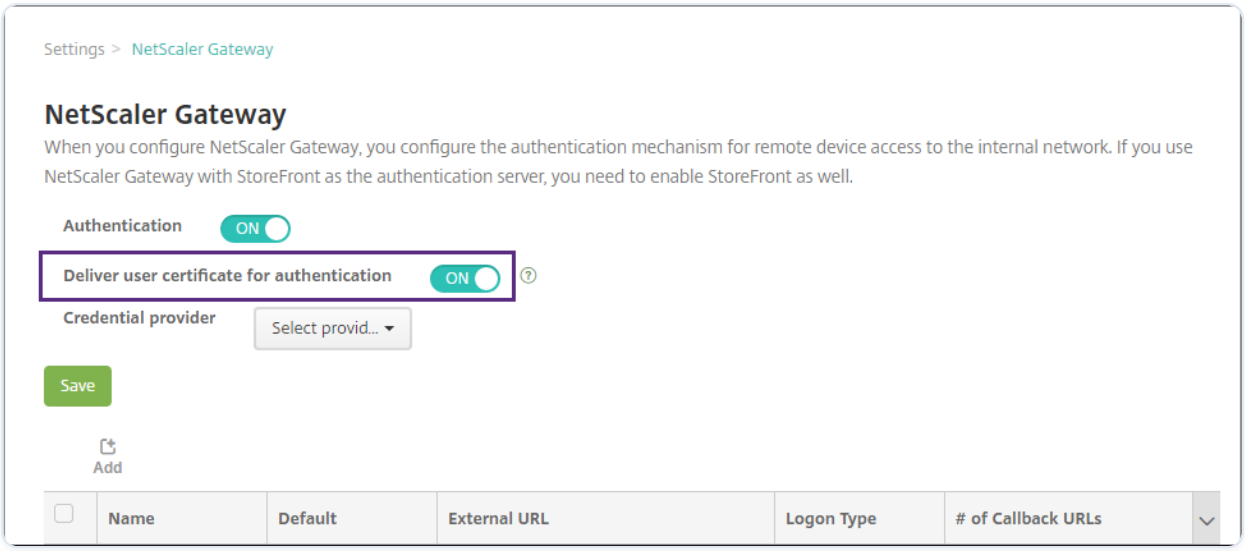


在 XenMobile 中配置 Citrix ADC 证书交付

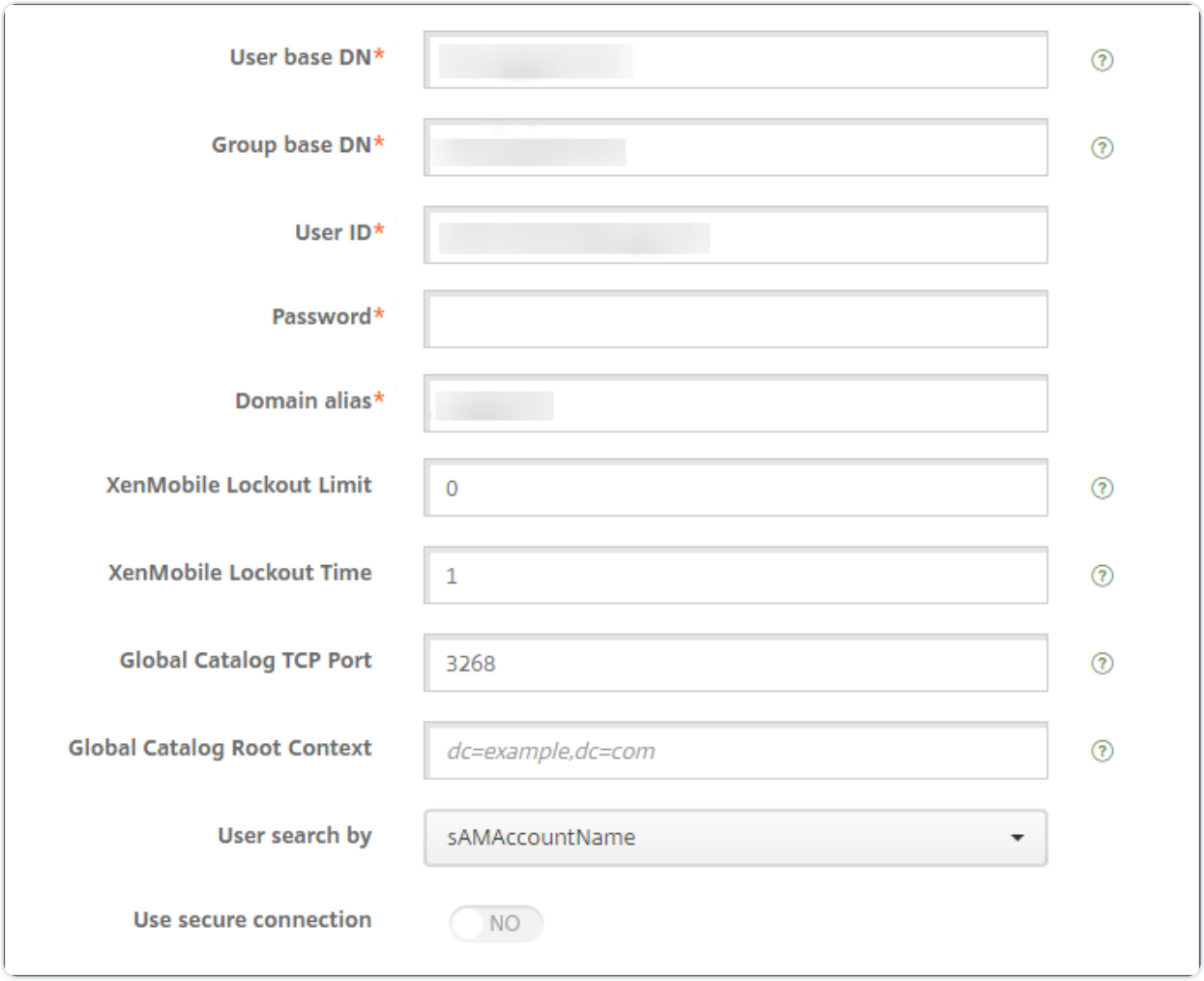
1. 登录到 XenMobile 控制台，然后单击右上角的齿轮图标。此时将显示 **设置** 屏幕。
2. 在 **服务器** 下，单击 **Citrix Gateway**。
3. 如果尚未添加 Citrix Gateway，请单击 **添加** 并指定设置：
   - **外部 URL：** `https://YourCitrixGatewayURL`
   - **登录类型：** 证书和域
   - **需要密码：** 关

- **设为默认值：** 开

4. 对于**传递用户证书以进行身份验证**，选择**开**。



5. 对于**凭据提供程序**，选择一个提供程序，然后单击**保存**。
6. 要使用用户证书中的 sAMAccount 属性作为用户主体名称 (UPN) 的替代方法，请在 XenMobile 中按如下方式配置 LDAP 连接器：转到**设置 > LDAP**，选择目录并单击**编辑**，然后在**用户搜索依据**中选择 **sAMAccountName**。



启用 Citrix PIN 和用户密码缓存

要启用 Citrix PIN 和用户密码缓存，请转到**设置 > 客户端属性**并选择以下复选框：**启用 Citrix PIN 身份验证**和**启用用户密码缓存**。有关详细信息，请参阅客户端属性。

排查您的客户端证书配置

成功配置上述设置以及 Citrix Gateway 配置后，用户工作流程如下：

1. 用户注册其移动设备。
2. XenMobile 提示用户创建 Citrix PIN。
3. 用户随后被重定向到 XenMobile 应用商店。
4. 当用户启动 Secure Mail 时，XenMobile 不会提示他们输入用户凭据以进行邮箱配置。相反，Secure Mail 会从 Secure Hub 请求客户端证书，并将其提交给 Microsoft Exchange Server 进行身份验证。如果用户启动 Secure Mail 时 XenMobile 提示输入凭据，请检查您的配置。

如果用户可以下载并安装 Secure Mail，但在邮箱配置过程中 Secure Mail 未能完成配置：

1. 如果 Microsoft Exchange Server ActiveSync 使用私有 SSL 服务器证书来保护流量，请验证根/中间证书是否已安装在移动设备上。
2. 验证为 ActiveSync 选择的身份验证类型是否为 **要求客户端证书**。

   Microsoft ActiveSync 属性屏幕(/en-us/xenmobile/server/media/activesync-require-client-certs.png)
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。该选项位于 **配置编辑器 > 安全 > 身份验证** 下。

   Microsoft ActiveSync 配置屏幕(/en-us/xenmobile/server/media/activesync-enable-cert-mapping.png)

   选择 **True** 后，请务必单击 **应用** 以使更改生效。
4. 检查 XenMobile 控制台中的 Citrix Gateway 设置：确保 **交付用户证书以进行身份验证** 为 **ON**，并且 **凭据提供程序** 已选择正确的配置文件。

确定客户端证书是否已交付到移动设备

1. 在 XenMobile 控制台中，转到 **管理 > 设备** 并选择设备。
2. 单击 **编辑** 或 **显示更多**。
3. 转到 **交付组** 部分，并搜索此条目：

   Citrix Gateway 凭据：请求的凭据，CertId=

验证是否已启用客户端证书协商

1. 运行此 `netsh` 命令以显示绑定到 IIS 网站的 SSL 证书配置：

   `netsh http show sslcert`
2. 如果 **协商客户端证书** 的值为 **禁用**，请运行以下命令以启用它：

   `netsh http delete sslcert ipport=0.0.0.0:443`

   `netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable`

   例如：

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid={4dc3e181-e14b-4a21-
b022-59fc669b0914} certstorename=ExampleCertStoreName
verifyclientcertrevocation=Enable
VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable
clientcertnegotiation=Enable
```

PKI 实体

XenMobile® 公钥基础设施 (PKI) 实体配置表示执行实际 PKI 操作（颁发、吊销和状态信息）的组件。这些组件可以是 XenMobile 内部的，也可以是外部的。内部组件称为自由裁量组件。外部组件是您企业基础架构的一部分。

XenMobile 支持以下类型的 PKI 实体：

- Microsoft 证书服务
- 自由裁量证书颁发机构 (CA)

XenMobile 支持以下 CA 服务器：

- Windows 服务器 2019
- Windows 服务器 2016

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

常见 PKI 概念

无论类型如何，每个 PKI 实体都具有以下功能的子集：

- **签名：** 根据证书签名请求 (CSR) 颁发新证书。
- **获取：** 恢复现有证书和密钥对。
- **吊销：** 吊销客户端证书。

关于 CA 证书

配置 PKI 实体时，请指示 XenMobile 哪个 CA 证书是该实体颁发（或恢复）的证书的签名者。该 PKI 实体可以返回由任意数量的不同 CA 签名的（已获取或新签名的）证书。

在 PKI 实体配置中提供每个这些 CA 的证书。为此，请将证书上传到 XenMobile，然后在 PKI 实体中引用它们。对于自由裁量的 CA，证书隐式为签名 CA 证书。对于外部实体，您必须手动指定证书。

重要提示：

创建 Microsoft 证书服务实体模板时，请避免已注册设备的潜在身份验证问题：不要在模板名称中使用特殊字符。例如，不要使用：`! : $ ( ) # % + * ~ ? | { } [ ]`

Microsoft 证书服务

XenMobile 通过其 Web 注册界面与 Microsoft 证书服务进行接口。XenMobile 仅支持通过该界面颁发新证书。如果 Microsoft CA 生成 Citrix Gateway 用户证书，Citrix Gateway 支持这些证书的续订和吊销。

要在 XenMobile 中创建 Microsoft CA PKI 实体，您必须指定证书服务 Web 界面的基本 URL。如果您选择，请使用 SSL 客户端身份验证来保护 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**”。

   将显示 PKI 实体类型菜单。
3. 单击“**Microsoft 证书服务实体**”。

   将显示“**Microsoft 证书服务实体: 常规信息**”页面。
4. 在“**Microsoft 证书服务实体: 常规信息**”页面上，配置以下设置：

   - **名称：**键入新实体的名称，您以后将使用该名称引用该实体。实体名称必须是唯一的。
   - **Web 注册服务根 URL：**键入 Microsoft CA Web 注册服务的基 URL；例如，`https://192.0.2.13/certsrv/`。该 URL 可以使用纯 HTTP 或 HTTP-over-SSL。
   - **certnew.cer 页面名称：**certnew.cer 页面的名称。除非您因某种原因重命名了它，否则请使用默认名称。

- **certfnsh.asp：**certfnsh.asp 页面的名称。除非您因某种原因重命名了它，否则请使用默认名称。
- **身份验证类型：**选择要使用的身份验证方法。
  - **无**
  - **HTTP 基本：**键入连接所需的用户名和密码。
  - **客户端证书：**选择正确的 SSL 客户端证书。

5. 单击**测试连接**以确保服务器可访问。如果不可访问，将显示一条消息，指出连接失败。请检查您的配置设置。
6. 单击**下一步**。

   将显示**Microsoft 证书服务实体：模板**页面。在此页面上，您可以指定 Microsoft CA 支持的模板的内部名称。创建凭据提供程序时，您可以从此处定义的列表中选择一个模板。使用此实体的每个凭据提供程序都只使用一个此类模板。

   有关 Microsoft 证书服务模板要求，请参阅您的 Microsoft Server 版本的 Microsoft 文档。除了证书 中注明的证书格式外，XenMobile 对其分发的证书没有其他要求。
7. 在**Microsoft 证书服务实体：模板**页面上，单击**添加**，键入模板名称，然后单击**保存**。对要添加的每个模板重复此步骤。
8. 单击**下一步**。

   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 XenMobile 要添加到 Microsoft Web 注册界面的 HTTP 请求中的自定义参数。自定义参数仅对在 CA 上运行的自定义脚本有用。
9. 在“**Microsoft 证书服务实体: HTTP 参数**”页面上，单击“**添加**”，键入要添加的 HTTP 参数的名称和值，然后单击“**下一步**”。

   此时将显示“**Microsoft 证书服务实体: CA 证书**”页面。在此页面上，您必须告知 XenMobile 系统通过此实体获取的证书的签名者。当您的 CA 证书续订时，请在 XenMobile 中更新它。XenMobile 会透明地将更改应用于实体。
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**”。

    该实体将显示在 PKI 实体表中。

Citrix ADC 证书吊销列表 (CRL)

XenMobile 仅支持第三方证书颁发机构的证书吊销列表 (CRL)。如果已配置 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“**启用 CRL 自动刷新**”。此步骤可确保处于仅 MAM 模式的设备用户无法使用设备上的现有证书进行身份验证。

XenMobile 会重新颁发新证书，因为它不限制用户在证书被吊销后生成用户证书。当 CRL 检查过期的 PKI 实体时，此设置可提高 PKI 实体的安全性。

自由裁量 CA

当您向 XenMobile 提供 CA 证书和关联的私钥时，将创建自由裁量 CA。XenMobile 根据您指定的参数在内部处理证书颁发、吊销和状态信息。

配置自由裁量 CA 时，可以为该 CA 激活联机证书状态协议 (OCSP) 支持。当且仅当您启用 OCSP 支持时，CA 才会将扩展 `id-pe-authorityInfoAccess` 添加到 CA 颁发的证书中。该扩展指向以下位置的 XenMobile 内部 OCSP 响应程序：

`https://<server>/<instance>/ocsp`

配置 OCSP 服务时，请为相关自由裁量实体指定 OCSP 签名证书。您可以使用 CA 证书本身作为签名者。为避免不必要地暴露您的 CA 私钥（建议）：创建由 CA 证书签名的委托 OCSP 签名证书，并包含此扩展：`id-kp-OCSPSigning extendedKeyUsage`。

XenMobile OCSP 响应程序服务支持基本 OCSP 响应和请求中的以下哈希算法：

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

响应使用 SHA-256 和签名证书密钥算法（DSA、RSA 或 ECDSA）进行签名。

添加自由裁量 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**。

将显示 PKI 实体类型菜单。

3. 单击**自由裁量 CA**。

   将显示**自由裁量 CA: 常规信息**页面。

4. 在**自由裁量 CA: 常规信息**页面上，执行以下操作：

   - **名称：**键入自由裁量 CA 的描述性名称。
   - **用于签署证书请求的 CA 证书：**单击一个证书，供自由裁量 CA 用于签署证书请求。

     此证书列表生成自您在 XenMobile 的 **配置 > 设置 > 证书** 中上传的包含私钥的 CA 证书。

5. 单击 **下一步**。

   显示 **自由裁量 CA: 参数** 页面。

6. 在 **自由裁量 CA: 参数** 页面上，执行以下操作：

   - **序列号生成器：** 自由裁量 CA 为其颁发的证书生成序列号。在此列表中，单击 **顺序** 或 **非顺序** 以确定如何生成这些数字。
   - **下一个序列号：** 键入一个值以确定下一个颁发的数字。
   - **证书有效期：** 键入证书的有效天数。
   - **密钥用法：** 通过将相应的密钥设置为 **开** 来确定自由裁量 CA 颁发的证书的用途。设置后，CA 只能为这些用途颁发证书。
   - **扩展密钥用法：** 要添加更多参数，请单击 **添加**，键入密钥名称，然后单击 **保存**。

7. 单击 **下一步**。

   显示 **自由裁量 CA: 分发** 页面。

8. 在 **自由裁量 CA: 分发** 页面上，选择分发模式：

   - **集中式：服务器端密钥生成**。Citrix 建议使用集中式选项。私钥在服务器上生成并存储，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，需要一个具有 `keyUsage keyEncryption` 扩展的 RA 加密证书和一个具有 `keyUsage digitalSignature` 扩展的 RA 签名证书。同一个证书可用于加密和签名。

9. 单击 **下一步**。

   显示 **自由裁量 CA：在线证书状态协议 (OCSP)** 页面。

   在 **自由裁量 CA：在线证书状态协议 (OCSP)** 页面上，执行以下操作：

- 如果要将 `AuthorityInfoAccess` (RFC2459) 扩展添加到此 CA 签名的证书中，请将**为此 CA 启用 OCSP 支持**设置为**开**。此扩展指向位于 `https://<server>/<instance>/ocsp` 的 CA OCSP 响应程序。
- 如果启用了 OCSP 支持，请选择一个 OSCP 签名 CA 证书。此证书列表是根据您上传到 XenMobile 的 CA 证书生成的。

10. 单击**保存**。

    自由裁量 CA 将显示在 PKI 实体表中。

凭据提供程序

凭据提供程序是您在 XenMobile® 系统的各个部分中使用的实际证书配置。凭据提供程序定义了证书的来源、参数和生命周期。无论证书是设备配置的一部分，还是独立的（即按原样推送到设备），这些操作都会发生。

设备注册限制了证书的生命周期。也就是说，XenMobile 不会在注册之前颁发证书，尽管 XenMobile 可能会在注册过程中颁发一些证书。此外，在一次注册的上下文中从内部 PKI 颁发的证书，在注册被撤销时也会被撤销。管理关系终止后，将不再有有效的证书。

您可以在多个地方使用一个凭据提供程序配置，这意味着一个配置可以同时管理任意数量的证书。统一性体现在部署资源和部署上。例如，如果凭据提供程序 P 作为配置 C 的一部分部署到设备 D：P 的颁发设置决定了部署到 D 的证书。同样，当 C 更新时，D 的续订设置适用。并且，当 C 被删除或 D 被撤销时，D 的撤销设置也适用。

根据这些规则，XenMobile 中的凭据提供程序配置决定了以下内容：

- 证书的来源。
- 获取证书的方法：签署新证书或获取（恢复）现有证书和密钥对。
- 颁发或恢复的参数。例如，证书签名请求 (CSR) 参数，如密钥大小、密钥算法和证书扩展。
- 证书交付到设备的方式。
- 撤销条件。尽管当管理关系断开时，XenMobile 中的所有证书都会被撤销，但配置可以指定更早的撤销。例如，配置可以指定在关联的设备配置被删除时撤销证书。此外，在某些条件下，XenMobile 中关联证书的撤销可能会发送到后端公钥基础设施 (PKI)。也就是说，XenMobile 中的证书撤销可能导致 PKI 上的证书撤销。
- 续订设置。通过给定凭据提供程序获取的证书在临近过期时可以自动续订。或者，与此情况分开，当过期临近时可以发出通知。

配置选项的可用性主要取决于您为凭据提供程序选择的 PKI 实体类型和颁发方法。

证书颁发方法

您可以通过签名方式获取证书，这被称为颁发方法。

使用此方法，颁发过程包括创建新的私钥、创建 CSR，并将 CSR 提交给证书颁发机构 (CA) 进行签名。XenMobile 支持 MS 证书服务实体和自由裁量 CA 实体的签名方法。

凭据提供程序使用签发方法。

证书交付

XenMobile 中有两种证书交付模式：集中式和分布式。分布式模式使用简单证书注册协议 (SCEP)，并且仅在客户端支持该协议（仅限 iOS）的情况下可用。在某些情况下，分布式模式是强制性的。

要使凭据提供程序支持分布式（SCEP 辅助）交付，需要一个特殊的配置步骤：设置注册机构 (RA) 证书。RA 证书是必需的，因为如果您使用 SCEP 协议，XenMobile 会充当实际证书颁发机构的委托（注册商）。XenMobile 必须向客户端证明它有权执行此操作。该权限是通过将前面提到的证书上传到 XenMobile 来建立的。

需要两种不同的证书角色（尽管单个证书可以满足这两个要求）：RA 签名和 RA 加密。这些角色的限制如下：

- RA 签名证书必须具有 X.509 密钥用法数字签名。
- RA 加密证书必须具有 X.509 密钥用法密钥加密。

要配置凭据提供程序 RA 证书，请将证书上传到 XenMobile，然后在凭据提供程序中链接到它们。

仅当凭据提供程序配置了证书角色的证书时，才认为该提供程序支持分布式交付。您可以将每个凭据提供程序配置为优先使用集中模式、优先使用分布式模式或要求使用分布式模式。实际结果取决于上下文：如果上下文不支持分布式模式，但凭据提供程序需要此模式，则部署失败。同样，如果上下文需要分布式模式，但凭据提供程序不支持分布式模式，则部署失败。在所有其他情况下，将遵循首选设置。

下表显示了 XenMobile 中的 SCEP 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 配置配置文件	是	否

上下文	支持 SCEP	需要 SCEP
SHTP 注册	否	否
SHTP 配置	否	否
Windows 平板电脑注册	否	否
Windows 平板电脑配置	否，但 Wi-Fi 设备策略除外，该策略支持 Windows 10 和 Windows 11	否

证书吊销

吊销分为三种类型。

- **内部吊销：** 内部吊销会影响 XenMobile 维护的证书状态。XenMobile 在评估所提供的证书或提供证书的 OCSP 状态信息时会考虑此状态。凭据提供程序配置决定了此状态在各种条件下的受影响方式。例如，凭据提供程序可能会指定在从设备中删除证书时将证书标记为已吊销。
- **外部传播吊销：** 也称为 XenMobile 吊销，此类吊销适用于从外部 PKI 获取的证书。当 XenMobile 在凭据提供程序配置定义的条件下内部吊销证书时，证书会在 PKI 上被吊销。
- **外部诱导吊销：** 也称为 PKI 吊销，此类吊销也仅适用于从外部 PKI 获取的证书。每当 XenMobile 评估给定证书状态时，XenMobile 都会向 PKI 查询该状态。如果证书被吊销，XenMobile 会内部吊销该证书。此机制使用 OCSP 协议。

这三种类型并非相互排斥，而是共同适用。外部吊销或独立发现可能导致内部吊销。内部吊销可能会影响外部吊销。

证书续订

证书续订是现有证书的吊销与另一证书的颁发相结合的过程。

XenMobile 首先尝试获取新证书，然后再吊销旧证书，以避免在颁发失败时服务中断。对于分布式（支持 SCEP）交付，吊销也仅在证书成功安装到设备上之后发生。否则，吊销会在新证书发送到设备之前发生。该吊销与证书安装的成功或失败无关。

吊销配置要求您指定一个特定持续时间（以天为单位）。当设备连接时，服务器会验证证书 `NotAfter` 日期是否晚于当前日期减去指定持续时间。如果证书符合该条件，XenMobile 会尝试续订证书。

创建凭据提供程序

配置凭据提供程序主要取决于您为凭据提供程序选择的颁发实体和颁发方法。您可以区分使用内部实体或外部实体的凭据提供程序：

- 自由裁量实体是 XenMobile 内部的实体，属于内部实体。自由裁量实体的颁发方法始终是签名。签名意味着在每次颁发操作中，XenMobile 都会使用为该实体选择的 CA 证书对新的密钥对进行签名。密钥对是在设备上还是在服务器上生成，取决于您选择的分发方法。
- 外部实体是公司基础结构的一部分，包括 Microsoft CA。

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：** 键入新提供程序配置的唯一名称。此名称稍后用于在 XenMobile 控制台的其他部分中标识此配置。
   - **说明：** 描述凭据提供程序。尽管此字段是可选的，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：** 单击证书颁发实体。
   - **颁发方法：** 单击**签名**或**提取**，作为系统从配置的实体获取证书的方法。对于客户端证书身份验证，请使用**签名**。
   - 如果**模板**列表可用，请选择在凭据提供程序的 PKI 实体下添加的模板。

     在**设置 > PKI 实体**中添加 Microsoft 证书服务实体后，这些模板将可用。
4. 单击**下一步**。

   此时将显示**凭据提供程序: 证书签名请求**页面。
5. 在**凭据提供程序: 证书签名请求**页面上，根据您的证书配置进行以下配置：

   - **密钥算法：** 为新的密钥对选择密钥算法。可用值为 **RSA**、**DSA** 和 **ECDSA**。
   - **密钥大小：** 输入密钥对的大小（以位为单位）。此字段为必填项。

     允许的值取决于密钥类型。例如，DSA 密钥的最大大小为 1024 位。为避免假阴性（这取决于底层硬件和软件），XenMobile 不强制执行密钥大小。在生产环境中激活凭据提供程序配置之前，请务必在测试环境中对其进行测试。
   - **签名算法：** 为新证书单击一个值。值取决于密钥算法。

- **主题名称：** 必填。输入新证书主题的专有名称 (DN)。例如：`CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation`

  例如，对于客户端证书身份验证，请使用以下设置：

  - **密钥算法：** RSA
  - **密钥大小：** 2048
  - **签名算法：** SHA256withRSA
  - **主题名称：** `cn=$user.username`

- 要向**主题备用名称**表中添加条目，请单击**添加**。选择备用名称的类型，然后在第二列中键入一个值。

  对于客户端证书身份验证，请指定：

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

    与主题名称一样，您可以在值字段中使用 XenMobile 宏。

6. 单击**下一步**。

   出现**凭据提供程序: 分发**页面。

7. 在**凭据提供程序: 分发**页面上，执行以下操作：

   - 在**颁发 CA 证书**列表中，单击提供的 CA 证书。由于凭据提供程序使用自由裁量的 CA 实体，因此凭据提供程序的 CA 证书始终是实体本身上配置的 CA 证书。此处显示 CA 证书是为了与使用外部实体的配置保持一致。
   - 在**选择分发模式**中，单击以下生成和分发密钥的方式之一：

     - **首选集中式: 服务器端密钥生成：** Citrix 建议使用此集中式选项。它支持 XenMobile 支持的所有平台，并且在使用 Citrix Gateway 身份验证时是必需的。私钥在服务器上生成和存储，并分发到用户设备。
     - **首选分布式: 设备端密钥生成：** 私钥在用户设备上生成和存储。此分布式模式使用 SCEP，并且需要一个具有 keyUsage keyEncryption 的 RA 加密证书和一个具有 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可用于加密和签名。
     - **仅分布式: 设备端密钥生成：** 此选项的工作方式与“首选分布式: 设备端密钥生成”相同，不同之处在于，由于它是“仅”，而不是“首选”，因此如果设备端密钥生成失败或不可用，则没有可用选项。

如果您选择了**首选分布式: 设备端密钥生成**或**仅分布式: 设备端密钥生成**，请单击 RA 签名证书和 RA 加密证书。同一个证书可用于两者。这些证书将显示新字段。

8. 单击**下一步**。

   出现**凭据提供程序: 吊销 XenMobile**页面。在此页面上，您可以配置 XenMobile 在何种条件下将通过此提供程序配置颁发的证书内部标记为已吊销。

9. 在**凭据提供程序: 吊销 XenMobile**页面上，执行以下操作：

   - 在**吊销已颁发证书**中，选择指示何时吊销证书的选项之一。
   - 要指示 XenMobile 在证书被吊销时发送通知：将**发送通知**的值设置为**开**，然后选择一个通知模板。
   - 当证书从 XenMobile 撤销时，在 PKI 上撤销证书：将 **Revoke certificate on PKI** 设置为 **On**，然后在 **Entity list** 中，单击一个模板。实体列表显示所有具有撤销功能的可用实体。当证书从 XenMobile 撤销时，撤销调用将发送到从实体列表中选择的 PKI。

10. 单击 **Next**。

    此时将显示 **Credential Providers: Revocation PKI** 页面。在此页面上，您可以确定如果证书被撤销，应在 PKI 上执行哪些操作。您还可以选择创建通知消息。

11. 在 **Credential Providers: Revocation PKI** 页面上，如果要从 PKI 撤销证书，请执行以下操作：

    - 将 **Enable external revocation checks** 的设置更改为 **On**。将显示更多与撤销 PKI 相关的字段。
    - 在 **OCSP responder CA certificate** 列表中，单击证书主题的专有名称 (DN)。

      您可以将 XenMobile 宏用于 DN 字段值。例如：`CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`

    - 在 **When certificate is revoked** 列表中，单击以下操作之一，以在证书被撤销时对 PKI 实体执行操作：

      - 不执行任何操作。
      - 续订证书。
      - 撤销并擦除设备。

    - 要指示 XenMobile 在证书被撤销时发送通知：将 **Send notification** 的值设置为 **On**。

      您可以选择两种通知选项：

- 如果选择 **Select notification template**，则可以选择一个预先编写的通知消息，然后对其进行自定义。这些模板位于通知模板列表中。
- 如果选择 **Enter notification details**，则可以编写自己的通知消息。除了提供收件人的电子邮件地址和消息外，您还可以设置通知的发送频率。

12. 单击 **下一步**。

    凭据提供程序: 续订 页面出现。在此页面上，您可以配置 XenMobile 以执行以下操作：

    - 续订证书。您可以选择在续订时发送通知，并可选择从操作中排除已过期的证书。
    - 针对即将过期的证书发出通知（续订前的通知）。

13. 在 **凭据提供程序: 续订** 页面上，如果要续订过期证书，请执行以下操作：

    将 **证书过期时续订** 设置为 **开**。将显示更多字段。

    - 在 **证书在以下天数内到期时续订** 字段中，键入证书到期前多少天续订证书。
    - （可选）选择 **不续订已过期的证书**。在这种情况下，“已过期”表示 `NotAfter` 日期已过，而不是已吊销。XenMobile 不会在证书内部吊销后续订它们。

    要指示 XenMobile 在证书续订时发送通知：将 **发送通知** 设置为 **开**。要指示 XenMobile 在证书即将到期时发送通知：将 **证书即将到期时通知** 设置为 **开**。 对于上述任一选择，您可以选择以下两种通知选项：

    - **选择通知模板：** 选择一个预先编写的通知消息，然后您可以对其进行自定义。这些模板位于通知模板列表中。
    - **输入通知详细信息：** 编写您自己的通知消息。提供收件人的电子邮件地址、消息以及发送通知的频率。

    在 **证书在以下天数内到期时通知** 字段中，键入证书到期前多少天发送通知。

14. 单击 **保存**。

    凭据提供程序显示在凭据提供程序表中。

APNs 证书

> **重要提示：**

> Apple 对 APNs 旧版二进制协议的支持将于 March 31, 2021 结束。Apple 建议您改用基于 HTTP/2 的 APNs 提供程序 API。自 10.13.0 版本起，XenMobile Server 支持基于 HTTP/2 的

> API。有关详细信息，请参阅 `<https://developer.apple.com/>` 中的新闻更新“Apple 推送通知服务更新”。有关检查 APNs 连接的帮助，请参阅连接检查。

> 要在 XenMobile® 中注册和管理 iOS 和 macOS 设备，您需要设置 Apple 的 Apple 推送通知服务 (APNs) 证书。

工作流摘要：

- **步骤 1：** 创建证书签名请求 (CSR) 通过以下任一方法：
  - 通过 macOS 上的“钥匙串访问”创建 CSR（Citrix® 推荐）
  - 通过 Microsoft IIS 创建 CSR
  - 通过 OpenSSL 创建 CSR
- **步骤 2：** 在 XenMobile Tools 中签署 CSR
- **步骤 3：** 将已签名的 CSR 提交给 Apple 以获取 APNs 证书
- **步骤 4：** 使用用于步骤 1 的同一台计算机，完成 CSR 并导出 PKCS #12 文件：
  - 通过 macOS 上的“钥匙串访问”创建 PKCS #12 文件
  - 通过 Microsoft IIS 创建 PKCS #12 文件
  - 通过 OpenSSL 创建 PKCS #12 文件
- **步骤 5：** 将 APNs 证书导入 XenMobile
- **步骤 6：** 续订 APNs 证书

创建证书签名请求

建议您使用 macOS 上的“钥匙串访问”创建 CSR。您也可以使用 Microsoft IIS 或 OpenSSL 创建 CSR。

> **重要提示：**

> - 对于用于创建证书的 Apple ID：
> - Apple ID 必须是公司 ID，而不是个人 ID。
> - 记录您用于创建证书的 Apple ID。

- 要续订证书，请使用相同的组织名称和 Apple ID。使用不同的 Apple ID 续订证书需要重新注册设备。

- 如果您意外或有意撤销证书，您将失去管理设备的能力。
- 如果您使用 iOS Developer Enterprise Program 创建了移动设备管理器推送证书：请务必在 Apple 推送证书门户中处理已迁移证书的任何操作。

使用 macOS 上的“钥匙串访问”创建 CSR

1. 在运行 macOS 的计算机上，在“**应用程序 > 实用工具**”下，启动“钥匙串访问”应用。
2. 打开“**钥匙串访问**”菜单，然后单击“**证书助理 > 从证书颁发机构请求证书**”。
3. 证书助理会提示您输入以下信息：
   - **电子邮件地址：** 负责管理证书的个人或角色帐户的电子邮件地址。
   - **通用名称：** 负责管理证书的个人或角色帐户的通用名称。
   - **CA 电子邮件地址：** 证书颁发机构的电子邮件地址。
4. 选择“**保存到磁盘**”和“**让我指定密钥对信息**”选项，然后单击“**继续**”。
5. 输入 CSR 文件的名称，将文件保存到计算机上，然后单击“**保存**”。
6. 指定密钥对信息：选择 2048 位的“**密钥大小**”和“**RSA 算法**”，然后单击“**继续**”。CSR 文件已准备就绪，可作为 APNs 证书过程的一部分进行上传。
7. 证书助手完成 CSR 过程后，单击“**完成**”。
8. 要继续，请签署 CSR。

使用 Microsoft IIS 创建 CSR

生成 APNs 证书请求的第一步是创建证书签名请求 (CSR)。对于 Windows，请使用 Microsoft IIS 生成 CSR。

1. 打开 Microsoft IIS。
2. 双击 IIS 的“服务器证书”图标。
3. 在“**服务器证书**”窗口中，单击“**创建证书请求**”。
4. 键入相应的专有名称 (DN) 信息，然后单击“**下一步**”。
5. 为加密服务提供程序选择“**Microsoft RSA SChannel Cryptographic Provider**”，为位长度选择“**2048**”，然后单击“**下一步**”。
6. 输入文件名并指定保存 CSR 的位置，然后单击“**完成**”。

7. 要继续，请(#sign-the-csr)。

使用 OpenSSL 创建 CSR

如果无法使用 macOS 设备或 Microsoft IIS 生成 CSR，请使用 OpenSSL。您可以从 OpenSSL 网站下载并安装 OpenSSL。

1. 在安装 OpenSSL 的计算机上，从命令提示符或 shell 运行以下命令。

   `openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048`

2. 出现以下证书命名信息消息。按要求输入信息。

```
You are about to be asked to enter information that will be
incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a
DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:RWC

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

Organizational Unit Name (eg, section) [:Marketing

Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com
```

3. 在下一条消息中，输入 CSR 私钥的密码。

```
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:
```

4. 要继续，请按照下一节中的说明签署 CSR。

签署 CSR

要将证书与 XenMobile 配合使用，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签署 CSR，并以 `.plist` 格式返回已签名的文件。

1. 在浏览器中，转到 端点管理工具 网站，然后单击“**请求推送通知证书签名**”。

   (/en-us/xenmobile/server/media/tools-cloud-push-notification-certificate-signature.png)

2. 在“**创建新证书页面**”上，单击“**上传 CSR**”。

   (/en-us/xenmobile/server/media/tools-cloud-push-notification-upload-csr.png)

3. 浏览并选择证书。

   证书必须是 .pem/txt 格式。

4. 在“**Endpoint Management APNs CSR 签名**”页面上，单击“**签名**”。CSR 将被签名并自动保存到您配置的下载文件夹中。
5. 若要继续，请按照下一节中的说明提交已签名的 CSR。

将已签名的 CSR 提交给 Apple 以获取 APNs 证书

从 Citrix 收到已签名的证书签名请求 (CSR) 后，将 CSR 提交给 Apple 以获取导入 XenMobile 所需的 APNs 证书。

> **注意：**

> 一些用户报告登录 Apple 推送门户时遇到问题。作为替代方案，请登录 Apple Developer Portal，然后按照以下步骤操作：

1. 在浏览器中，转到 Apple Push Certificates Portal。

2. 单击“**创建证书**”。
3. 首次使用 Apple 创建证书时：选中“**我已阅读并同意这些条款和条件**”复选框，然后单击“**接受**”。
4. 单击“**选择文件**”，浏览到计算机上已签名的 CSR，然后单击“**上传**”。确认消息指示上传成功。
5. 单击“**下载**”以检索 .pem 证书。
6. 若要继续，请按照下一节中的说明完成 CSR 并导出 PKCS #12 文件。

完成 CSR 并导出 PKCS #12 文件

收到 Apple 的 APNs 证书后，返回到钥匙串访问、Microsoft IIS 或 OpenSSL，将证书导出为 PCKS #12 文件。

PKCS #12 文件包含 APNS 证书文件和您的私钥。PFX 文件通常具有 .pfx 或 .p12 扩展名。您可以互换使用 .pfx 和 .p12 文件。

> **重要提示：**

> Citrix 建议您从本地系统保存或导出个人密钥和公钥。您需要这些密钥才能访问 APNs 证书以供重复使用。如果没有相同的密钥，您的证书将无效，并且您必须重复整个 CSR 和 APNs 过程。

在 macOS 上使用钥匙串访问创建 PKCS #12 文件

> **重要提示：**

> 对于此任务，请使用您用于生成 CSR 的同一 macOS 设备。

1. 在设备上，找到从 Apple 收到的生产身份 (.pem) 证书。
2. 启动“钥匙串访问”应用程序，然后导航到“**登录 > 我的证书**”选项卡。将产品身份证书拖放到打开的窗口中。
3. 单击证书并展开左箭头以验证证书是否包含关联的私钥。
4. 要开始将证书导出为 PCKS #12 (.pfx) 证书，请选择证书和私钥，右键单击，然后选择“**导出 2 项**”。
5. 为证书文件指定一个用于 XenMobile 的唯一名称。名称中不要包含空格字符。然后，为保存的证书选择一个文件夹位置，选择 .pfx 文件格式，然后单击“**保存**”。

6. 输入用于导出证书的密码。Citrix 建议您使用唯一且强度高的密码。此外，请务必妥善保管证书和密码，以备将来使用和参考。
7. “钥匙串访问”应用会提示您输入登录密码或选定的钥匙串。键入密码，然后单击“**确定**”。现在，保存的证书已可用于 XenMobile Server。
8. 要继续，请参阅将 APNs 证书导入 XenMobile。

使用 Microsoft IIS 创建 PKCS #12 文件

> **重要：**
>
> 对于此任务，请使用生成 CSR 时所用的同一 IIS 服务器。

1. 打开 Microsoft IIS。
2. 单击“**服务器证书**”图标。
3. 在“**服务器证书**”窗口中，单击“**完成证书请求**”。
4. 浏览到 Apple 提供的 Certificate.pem 文件。然后，键入一个友好名称或证书名称，并单击“**确定**”。名称中不要包含空格字符。
5. 选择在步骤 4 中确定的证书，然后单击“**导出**”。
6. 为 .pfx 证书指定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 证书复制到您计划安装 XenMobile 的服务器。
8. 要继续，请参阅将 APNs 证书导入 XenMobile。

使用 OpenSSL 创建 PKCS #12 文件

如果您使用 OpenSSL 创建 CSR，也可以使用 OpenSSL 创建 .pfx APNs 证书。

1. 在命令提示符或 shell 中，运行以下命令。`Customer.privatekey.pem` 是您的 CSR 中的私钥。`APNs_Certificate.pem` 是您刚从 Apple 收到的证书。

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
   ```
2. 为 .pfx 证书文件输入密码。请记住此密码，因为在将证书上传到 XenMobile 时会再次使用它。
3. 记下 .pfx 证书文件的位置。然后，将文件复制到 XenMobile Server，以便您可以使用控制台上传该文件。

4. 要继续，请按照下一节中的说明将 APNs 证书导入 XenMobile。

将 APNs 证书导入 XenMobile

收到新的 APNs 证书后：将 APNs 证书导入 XenMobile，以首次添加证书或替换现有证书。

1. 在 XenMobile 控制台中，转到 **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 中证书的详细信息，请参阅 证书和身份验证。

续订 APNs 证书

> **重要提示：**
>
> 如果续订过程中使用了不同的 Apple ID，则必须重新注册用户设备。
>
> 要续订 APNs 证书，请执行创建证书的步骤，然后转到 Apple 推送证书门户。使用该门户上传新证书。登录后，您现有的证书或从您之前的 Apple 开发者帐户导入的证书将显示。

在证书门户中，续订证书时唯一的区别是您单击**续订**。您必须拥有证书门户的开发者帐户才能访问该站点。要续订证书，请使用相同的组织名称和 Apple ID。

要在 XenMobile 控制台中确定 APNs 证书何时到期，请转到**设置 > 证书**。如果证书到期，请勿吊销它。

1. 使用 Microsoft IIS、钥匙串访问 (macOS) 或 OpenSSL 生成 CSR。有关生成 CSR 的更多信息，请参阅创建证书签名请求。
2. 在浏览器中，转到Endpoint Management Tools。然后，单击**请求推送通知证书签名**。
3. 单击**+ 上传 CSR**。
4. 在对话框中，导航到 CSR，单击**打开**，然后单击**签名**。
5. 收到 `.plist` 文件后，请保存它。
6. 在步骤 3 标题中，单击**Apple 推送证书门户**并登录。
7. 选择要续订的证书，然后单击**续订**。

8. 上传 `.plist` 文件。您将收到一个 .pem 文件作为输出。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 的方法）。
10. 将证书导出为 .pfx 文件。

在 XenMobile 控制台中，导入 .pfx 文件并按如下方式完成配置：

1. 转到**设置 > 证书 > 导入**。
2. 从“**导入菜单**”中，选择“**密钥库**”。
3. 从“**密钥库类型**”菜单中，选择“**PKCS #12**”。
4. 在“**用途**”中，选择“**APNs**”。

   导入证书对话框(/en-us/xenmobile/server/media/import-apns-certificate.png)
5. 对于“**密钥库文件**”，单击“**浏览**”并导航到该文件。
6. 在“**密码**”中，键入证书密码。
7. 键入可选的“**描述**”。
8. 单击“**导入**”。

XenMobile 会将您重定向回“**证书**”页面。“**名称**”、“**状态**”、“**有效期从**”和“**有效期至**”字段会更新。

Citrix Files 的 SAML 单点登录

> **免责声明：**

> 如果 ShareFile（现为 Progress）停止支持，此功能将被弃用。

> 您可以配置 XenMobile® 和 ShareFile 以使用安全断言标记语言 (SAML) 为 Citrix Files 移动应用程序提供单点登录 (SSO) 访问。此功能包括：

- 已启用 MAM SDK 或使用 MDX Toolkit 封装的 Citrix Files 应用程序
- 未封装的 Citrix Files 客户端，例如网站、Outlook 插件或同步客户端
- **对于封装的 Citrix Files 应用程序**。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 以进行用户身份验证并获取 SAML 令牌。成功进行身份验证后，Citrix Files 移动应用程序会将 SAML 令牌发送到 ShareFile。首次登录后，用户可以通过 SSO 访问 Citrix Files 移动应用程序。他们还可以将 ShareFile 中的文档附加到 Secure Mail 邮件，而无需每次都登录。

- **对于未封装的 Citrix Files 客户端**。使用 Web 浏览器或其他 Citrix Files 客户端登录 Citrix Files 的用户将被重定向到 XenMobile。XenMobile 会对用户进行身份验证，然后用户获取一个 SAML 令牌，该令牌会发送到 ShareFile。首次登录后，用户可以通过 SSO 访问 Citrix Files 客户端，而无需每次都登录。

要将 XenMobile 用作 ShareFile 的 SAML 身份提供程序 (IdP)，您必须按照本文所述配置 XenMobile 以与企业帐户配合使用。或者，您可以将 XenMobile 配置为仅与存储区域连接器配合使用。有关详细信息，请参阅 将 ShareFile 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。

先决条件

在配置 XenMobile 和 Citrix Files 应用程序的 SSO 之前，请完成以下先决条件：

- MAM SDK 或兼容版本的 MDX Toolkit（适用于 Citrix Files 移动应用程序）。

  有关详细信息，请参阅 XenMobile 兼容性。
- 兼容版本的 Citrix Files 移动应用程序和 Secure Hub。
- ShareFile 管理员帐户。
- XenMobile 与 ShareFile 之间的连接已验证。

配置 ShareFile 访问

在为 ShareFile 设置 SAML 之前，请按如下方式提供 ShareFile 访问信息：

1. 在 XenMobile Web 控制台中，单击 **Configure > ShareFile**。将显示 **ShareFile** 配置页面。

   ShareFile 配置设置(/en-us/xenmobile/server/media/configure-content-collaboration-saml-for-non-mdx-apps.png)
2. 配置以下设置：

   - **域：** 键入您的 ShareFile 子域名。例如：`example.sharefile.com`。
   - **分配到交付组：** 选择或搜索您希望能够将 SSO 与 ShareFile 结合使用的交付组。
   - **ShareFile 管理员帐户登录**
   - **用户名：** 键入 ShareFile 管理员用户名。此用户必须具有管理员权限。
   - **密码：** 键入 ShareFile 管理员密码。
   - **用户帐户预配：** 将此设置保持禁用状态。使用 ShareFile 用户管理工具进行用户预配。请参阅预配用户帐户和通讯组。

3. 单击 **Test Connection** 以验证 ShareFile 管理员帐户的用户名和密码是否已对指定的 ShareFile 帐户进行身份验证。
4. 单击 **Save**。
   - XenMobile 与 ShareFile 同步并更新 ShareFile 设置 **ShareFile Issuer/Entity ID** 和 **Login URL**。
   - "**Configure > ShareFile**"页面显示"**App internal name**"。您需要该名称才能完成 Modify the Citrix Files.com SSO settings 中稍后描述的步骤。

为封装的 Citrix Files MDX 应用程序设置 SAML

对于封装的 Citrix Files MDX 应用程序，您无需使用 Citrix Gateway 进行单点登录配置。要为非封装的 Citrix Files 客户端（例如网站、Outlook 插件或同步客户端）配置访问权限，请参阅 Configure the Citrix Gateway for Other Citrix Files Clients。

以下步骤适用于 iOS 和 Android 应用程序及设备。要为封装的 Citrix Files MDX 应用程序配置 SAML：

1. 使用 MDX Toolkit 封装 Citrix Files 移动应用程序。有关使用 MDX Toolkit 封装应用程序的更多信息，请参阅 Wrapping Apps with the MDX Toolkit。
2. 在 XenMobile 控制台中，上传封装的 Citrix Files 移动应用程序。有关上传 MDX 应用程序的信息，请参阅 To add an MDX app to XenMobile。
3. 验证 SAML 设置：使用您之前配置的管理员用户名和密码登录 ShareFile。
4. 验证 ShareFile 和 XenMobile 是否配置为相同的时区。确保 XenMobile 显示配置时区的正确时间。否则，SSO 可能会失败。

验证 Citrix Files 移动应用程序

1. 在用户设备上，安装并配置 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 将直接启动，无需提示输入用户名或密码。

使用 Secure Mail 进行验证

1. 在用户设备上，如果尚未完成，请安装并配置 Secure Hub。
2. 从 XenMobile Store 下载、安装并设置 Secure Mail。
3. 打开新的电子邮件表单，然后点击"**从 Citrix Files 附加**"。可附加到电子邮件的文件将显示，无需请求用户名或密码。

为其他 Citrix Files 客户端配置 Citrix Gateway

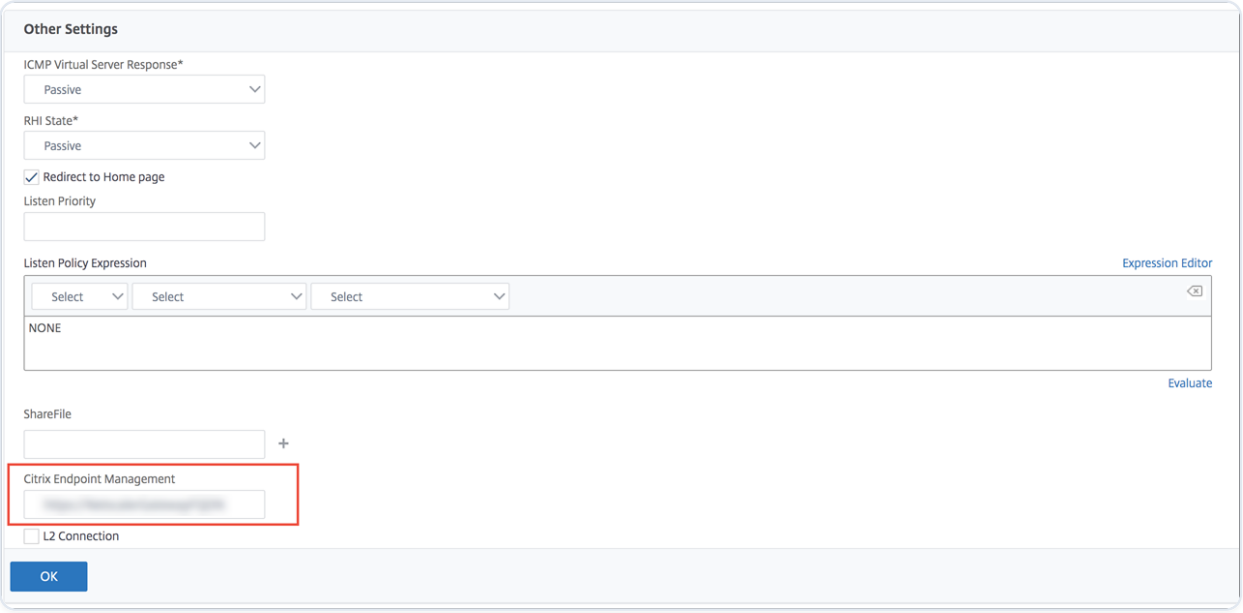
要为非封装的 Citrix Files 客户端（例如网站、Outlook 插件或同步客户端）配置访问权限，请按以下步骤配置 Citrix Gateway 以支持使用 XenMobile 作为 SAML 身份提供程序。

- 禁用主页重定向。
- 创建 Citrix Files 会话策略和配置文件。
- 在 Citrix Gateway 虚拟服务器上配置策略。

禁用主页重定向

禁用通过 /cginfra 路径发出的请求的默认行为。此操作使用户能够看到原始请求的内部 URL，而不是配置的主页。

1. 编辑用于 XenMobile 登录的 Citrix Gateway 虚拟服务器的设置。在 Citrix ADC 中，转到“**其他设置**”，然后清除标有“**重定向到主页**”的复选框。



2. 在“**ShareFile**”（现在称为 ShareFile）下，键入您的 XenMobile 内部服务器名称和端口号。
3. 在“**Citrix Endpoint Management™**”下，键入您的 XenMobile URL。您的 Citrix Gateway 版本可能引用旧产品名称“**AppController**”。

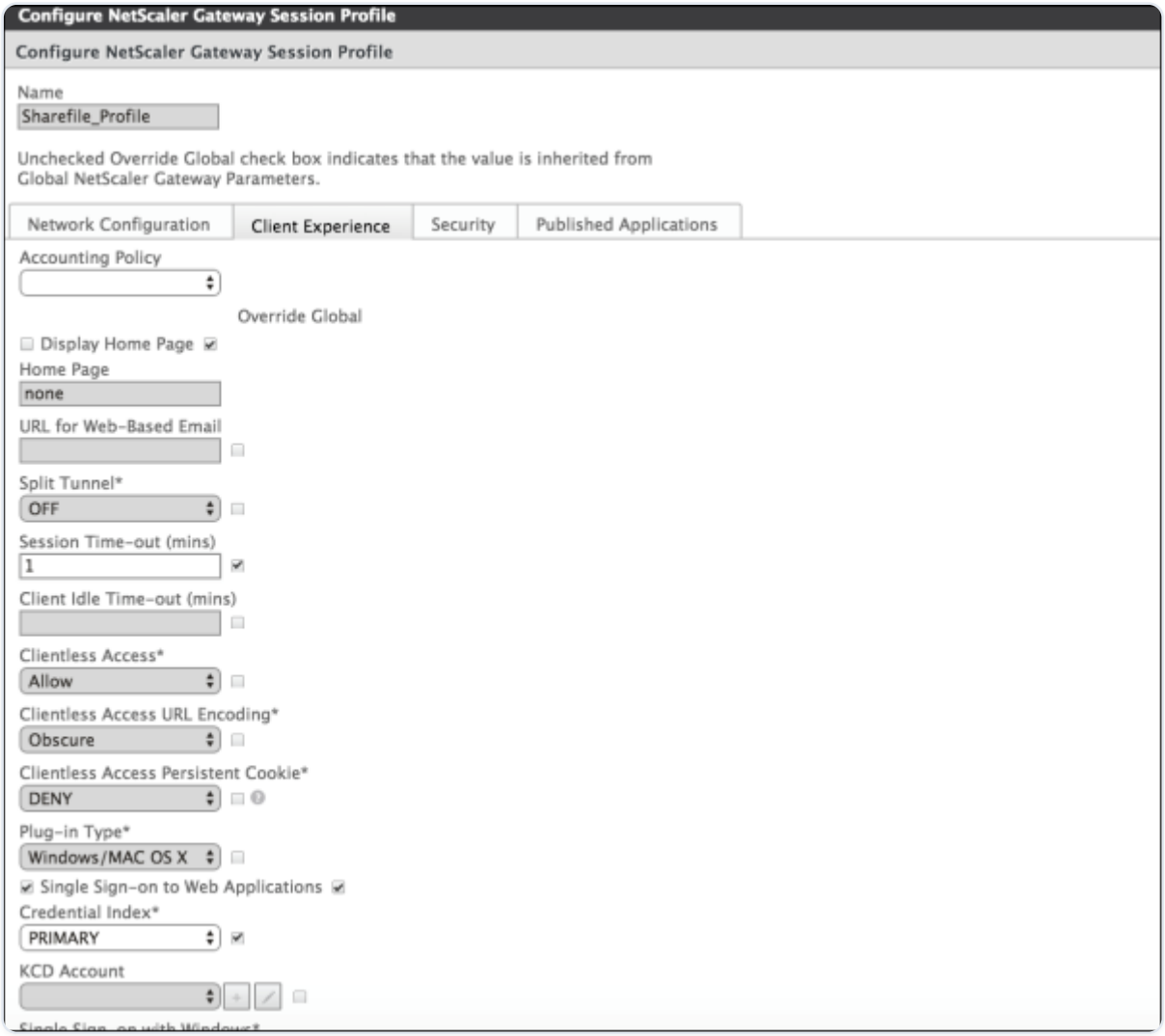
   此配置授权通过 /cginfra 路径访问您输入的 URL 的请求。

创建 Citrix Files 会话策略和请求配置文件

配置这些设置以创建 Citrix Files 会话策略和请求配置文件：

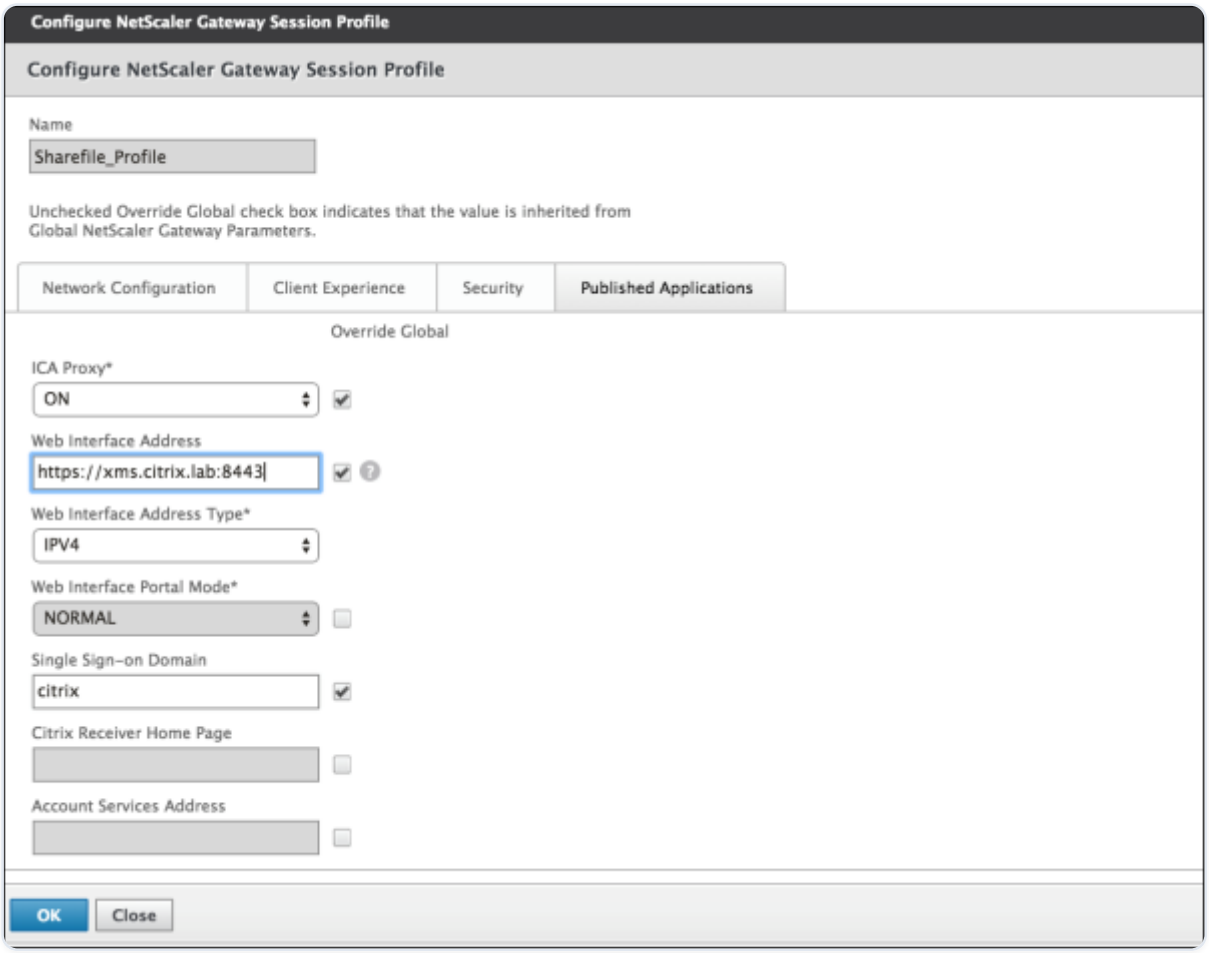
1. 在 Citrix Gateway 配置实用程序中，在左侧导航窗格中，单击 **Citrix Gateway > Policies > Session**。

2. 创建会话策略。在“**策略**”选项卡上，单击“**添加**”。
3. 在“**名称**”字段中，键入 **ShareFile_Policy**。
4. 单击“**+**”按钮创建操作。“**创建会话配置文件**”页面随即显示。



配置以下设置：

- **名称：** 键入 **ShareFile_Profile**。
- 单击“**客户端体验**”选项卡，然后配置以下设置：
  - **主页：** 键入 **none**。
  - **会话超时（分钟）：** 键入 **1**。
  - **Web 应用程序的单点登录：** 选择此设置。
  - **凭据索引：** 单击 **PRIMARY**。
- 单击“**已发布的应用程序**”选项卡。

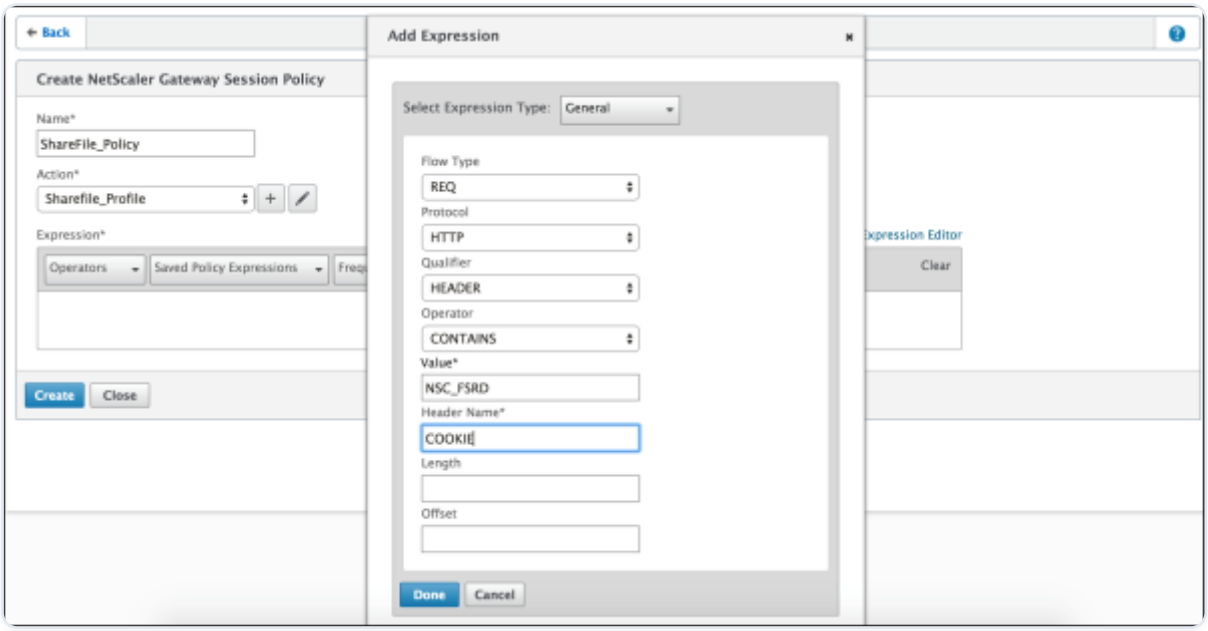


配置以下设置：

- **ICA® 代理：** 单击“**开**”。
- **Web 界面地址：** 键入您的 XenMobile Server URL。
- **单点登录域：** 键入您的 Active Directory 域名。

  配置 Citrix Gateway 会话配置文件时，**单点登录域**的域后缀必须与 LDAP 中定义的 XenMobile 域别名匹配。

5. 单击“**创建**”以定义会话配置文件。
6. 单击“**表达式编辑器**”。



配置以下设置：

- **值：** 键入 **NSC_FSRD**。
- **标头名称：** 键入 **COOKIE**。

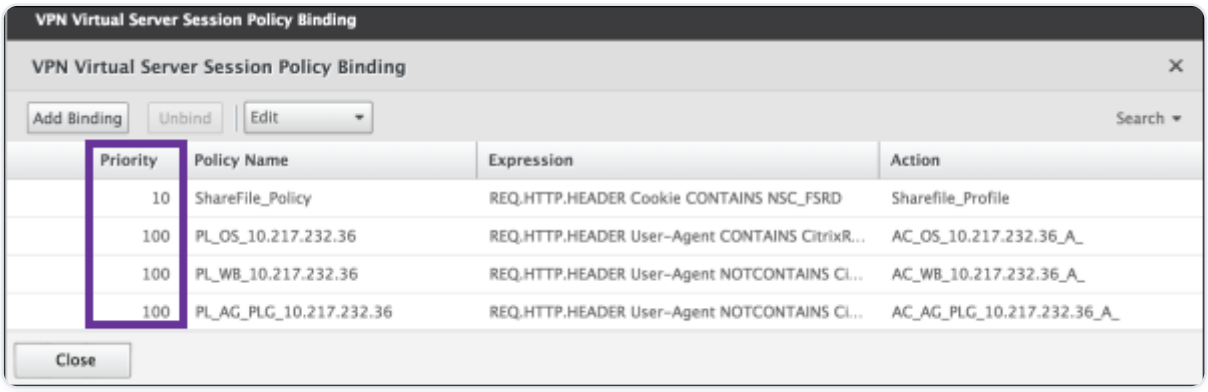
7. 单击“**创建**”，然后单击“**关闭**”。

在 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 配置实用程序中，在左侧导航窗格中，单击 **Citrix Gateway > 虚拟服务器**。
2. 在**详细信息**窗格中，单击您的 Citrix Gateway 虚拟服务器。
3. 单击**编辑**。
4. 单击**已配置策略 > 会话策略**，然后单击**添加绑定**。
5. 选择 **ShareFile_Policy**。

6. 编辑所选策略的自动生成**优先级**编号，使其相对于列出的任何其他策略具有最高优先级（最小的数字）。例如：



7. 单击**完成**，然后保存正在运行的 Citrix ADC 配置。

修改 Citrix Files.com SSO 设置

对 MDX 和非 MDX Citrix Files 应用程序进行以下更改。

重要提示：

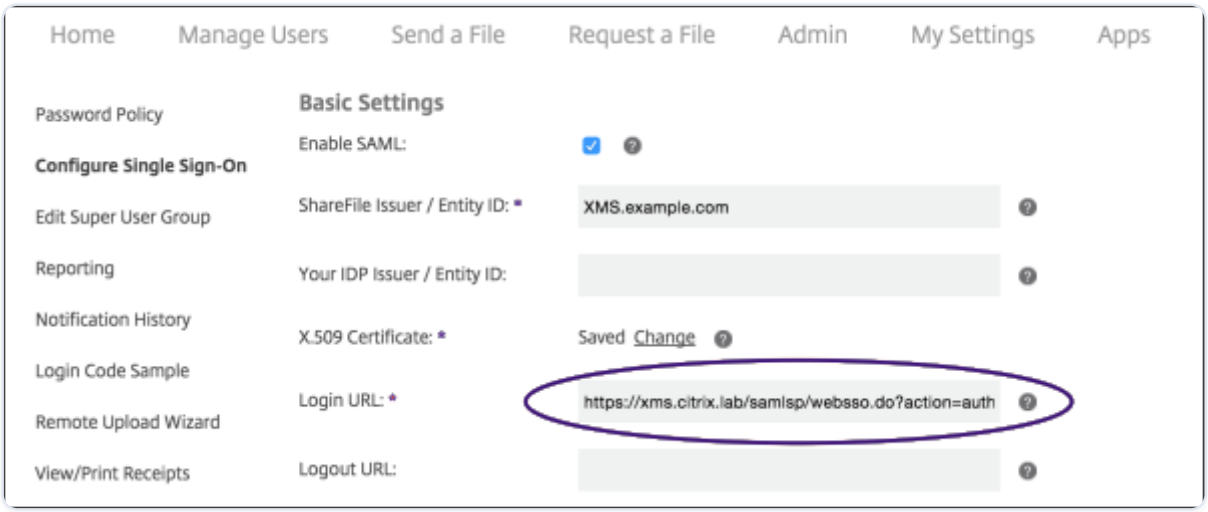
内部应用程序名称后会附加一个新数字：

- 每次编辑或重新创建 Citrix Files 应用程序时
- 每次更改 XenMobile 中的 ShareFile 设置时

因此，您还必须更新 Citrix Files 网站中的登录 URL，以反映更新后的应用程序名称。

1. 以 ShareFile 管理员身份登录您的 ShareFile 帐户 (`https://<subdomain>.sharefile.com`)。
2. 在 ShareFile Web 界面中，单击 **Admin**，然后选择 **Configure Single Sign-on**。
3. 按如下方式编辑 **Login URL**：

   以下是编辑前的 **Login URL** 示例：`https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`。



- 在 XenMobile Server FQDN 前面插入 Citrix Gateway 虚拟服务器外部 FQDN 和 `/cginfra/https/`，然后在 XenMobile FQDN 后面添加 **8443**。

  以下是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

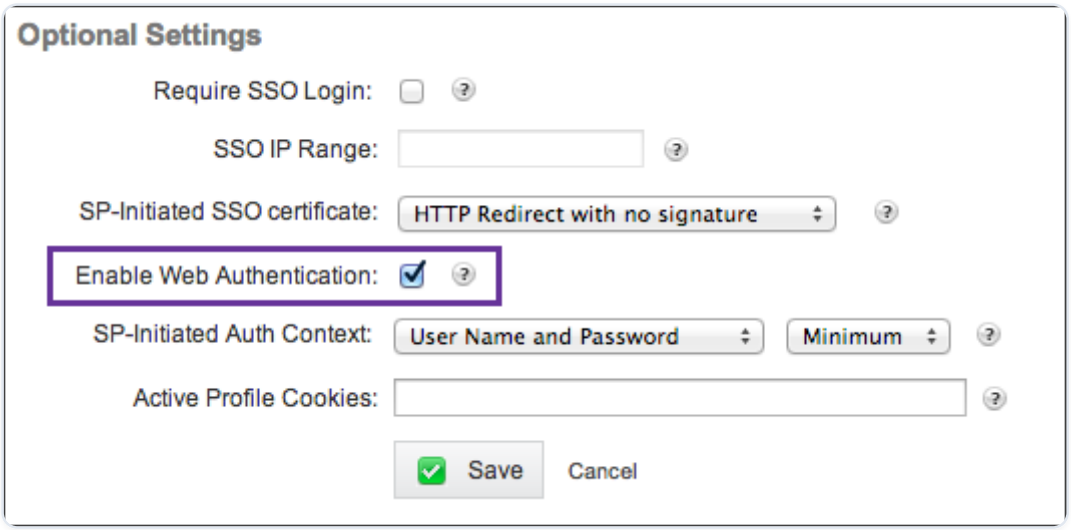
- 将参数 `&app=ShareFile_SAML_SP` 更改为内部 Citrix Files 应用程序名称。默认情况下，内部名称为 `ShareFile_SAML`。但是，每次更改配置时，内部名称后面都会附加一个数字（例如 `ShareFile_SAML_2`、`ShareFile_SAML_3` 等）。您可以在 **Configure > ShareFile** 页面上查找 **App internal name**。

  以下是编辑后的 URL 示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- 将 `&nssso=true` 添加到 URL 的末尾。

  以下是最终 URL 的示例：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`。

4. 在 **Optional Settings** 下，选中 **Enable Web Authentication** 复选框。



验证配置

执行以下操作以验证配置。

1. 将浏览器指向 `https://<subdomain>sharefile.com/saml/login`。

   您将被重定向到 Citrix Gateway 登录表单。如果您未被重定向，请验证之前的配置设置。

2. 输入您配置的 Citrix Gateway 和 XenMobile 环境的用户名和密码。

   您在 `<subdomain>.sharefile.com` 的 Citrix Files 文件夹将显示。如果您没有看到 Citrix Files 文件夹，请确保您输入了正确的登录凭据。

将 Azure 活动目录 用作 IdP

将 Azure Active Directory (AAD) 配置为身份提供程序 (IdP) 允许用户使用其 Azure 凭据注册 XenMobile®。

支持 iOS、Android 以及 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 注册 MDM 的用户。注册 MAM 的设备无法使用 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 and XenMobile。

您可以在 **设置 > 身份验证 > IDP** 下将 Azure 配置为您的 IdP。**IDP** 页面是 XenMobile 此版本中新增的。在 XenMobile 的早期版本中，您可以在 **设置 > Microsoft Azure** 下配置 Azure。

要求

- 版本和许可证
  - 要注册 iOS 或 Android 设备，您需要 Secure Hub 10.5.5。

  - 要注册 Windows 10 和 Windows 11 设备，您需要 Microsoft Azure Premium 许可证。

- 目录服务和身份验证
  - XenMobile Server 必须配置为基于证书的身份验证。
  - 如果您使用 Citrix ADC 进行身份验证，Citrix ADC 必须配置为基于证书的身份验证。
  - Secure Hub 身份验证使用 Azure AD 并遵循在 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

当设备通过 Secure Hub 注册且 XenMobile 配置为使用 Azure 作为其 IdP 时：

1. 用户在其设备上，在 Secure Hub 中显示的 Azure AD 登录屏幕中输入其 Azure Active Directory 用户名和密码。
2. Azure AD 验证用户并发送 ID 令牌。
3. Secure Hub 与 XenMobile Server 共享 ID 令牌。
4. XenMobile 验证 ID 令牌以及 ID 令牌中存在的用户信息。XenMobile 返回会话 ID。

Azure 帐户设置

要将 Azure AD 用作 IdP，请首先登录到您的 Azure 帐户并进行以下更改：

1. 注册您的自定义域并验证该域。有关详细信息，请参阅 将自定义域名添加到 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 帐户进行以下更改：

1. 将 MDM 设为 Azure AD 的可靠方。为此，请单击 **Azure Active Directory > Applications**，然后单击 **Add**。
2. 从库中选择 **Add an application**。转至 **MOBILE DEVICE MANAGEMENT**，然后选择 **on-premises MDM application**。保存设置。

   即使您已注册 Citrix XenMobile 云，也要选择本地应用程序。在 Microsoft 术语中，任何非多租户应用程序都是本地 MDM 应用程序。
3. 在应用程序中，配置 XenMobile Server 发现、使用条款终结点和 APP 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。启用选项 **管理这些用户的设备** 以便为所有用户或任何特定用户组启用 MDM 管理。

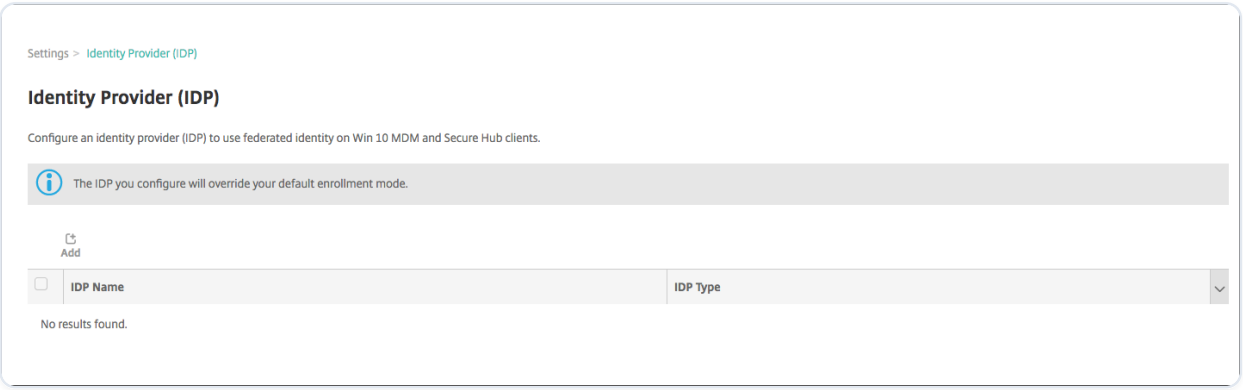
   有关将 Azure AD 与 Windows 10 和 Windows 11 设备结合使用的详细信息，请参阅 Microsoft 文章 Azure Active Directory 与 MDM 集成。

将 Azure AD 配置为您的 IdP

1. 查找或记下您 Azure 帐户中所需的信息：

   - Azure 应用程序设置页面中的租户 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：** Azure 应用程序设置页面中的密钥。

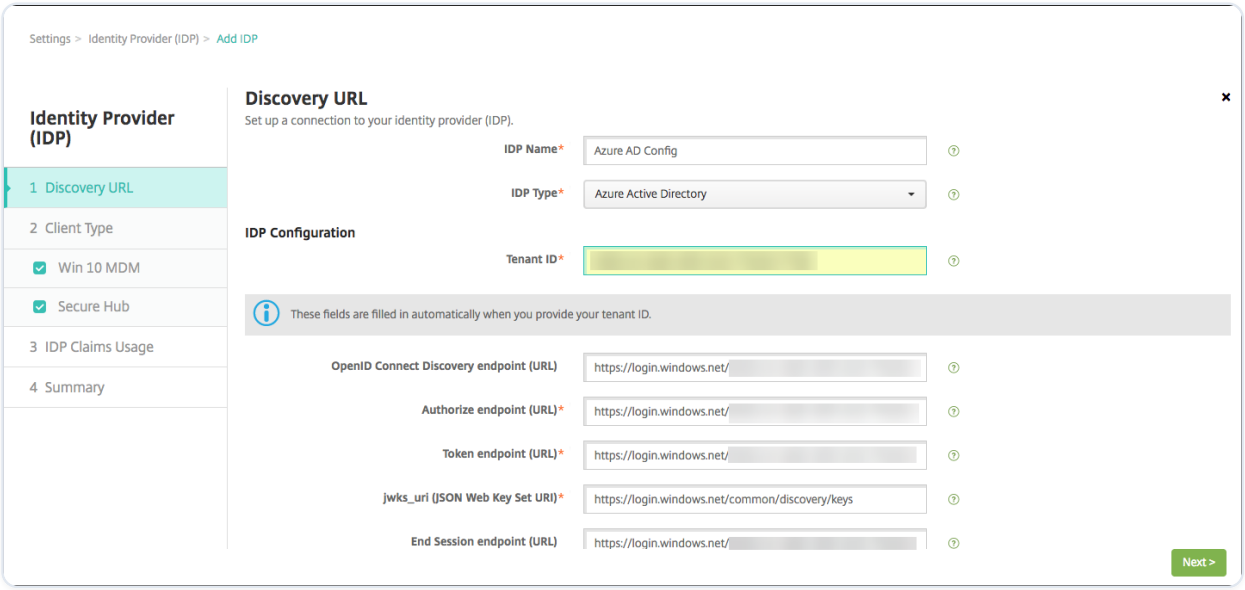
2. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示 **设置** 页面。
3. 在 **身份验证** 下，单击 **身份提供程序 (IDP)**。此时将显示 **身份提供程序** 页面。



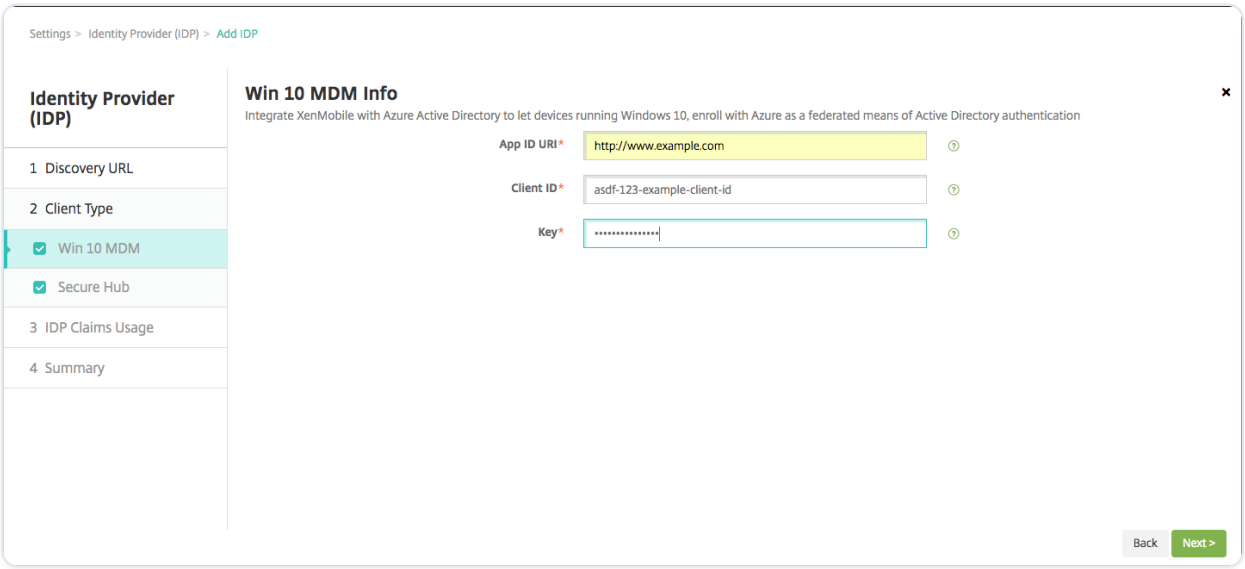
4. 单击 **添加**。此时将显示 **IDP 配置** 页面。
5. 配置有关您的 IdP 的以下信息：

   - **IDP 名称：** 键入您正在创建的 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段。

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` 。



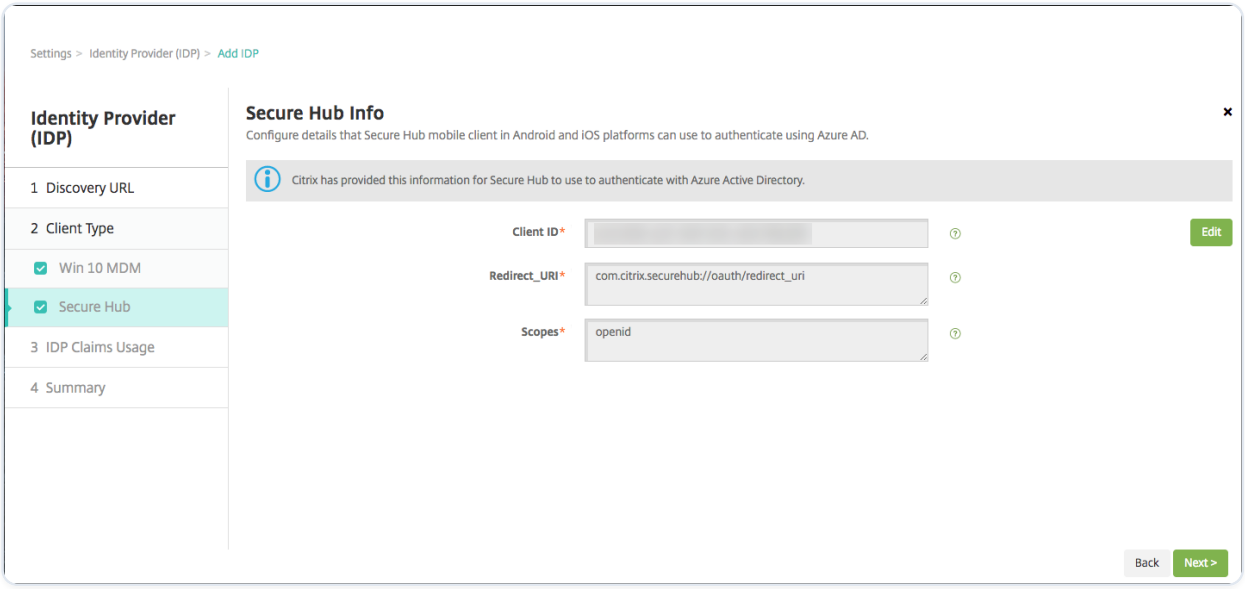
6. 其余字段将自动填充。填充完毕后，单击**下一步**。
7. 要配置 XenMobile 以使用 Azure AD 进行 MDM 注册来注册 Windows 10 和 Windows 11 设备，请配置以下设置。要跳过此可选步骤，请清除**Windows MDM**。
   - **应用程序 ID URI：** 键入您在配置 Azure 设置时输入的 XenMobile Server 的 URL。
   - **客户端 ID：** 从 Azure 配置页面复制并粘贴此值。客户端 ID 是您的应用程序的唯一标识符。
   - **密钥：** 从 Azure 应用程序设置页面复制此值。在密钥下，从列表中选择一个持续时间，然后保存设置。然后您可以复制该密钥并将其粘贴到此字段中。当应用程序在 Microsoft Azure AD 中读取或写入数据时，需要密钥。



8. 单击**下一步**。

Citrix 已将 Secure Hub 注册到 Microsoft Azure 并维护相关信息。此屏幕显示 Secure Hub 用于与 Azure Active Directory 通信的详细信息。如果将来需要更改任何信息，将使用此页面。仅当 Citrix 建议您这样做时才编辑此页面。

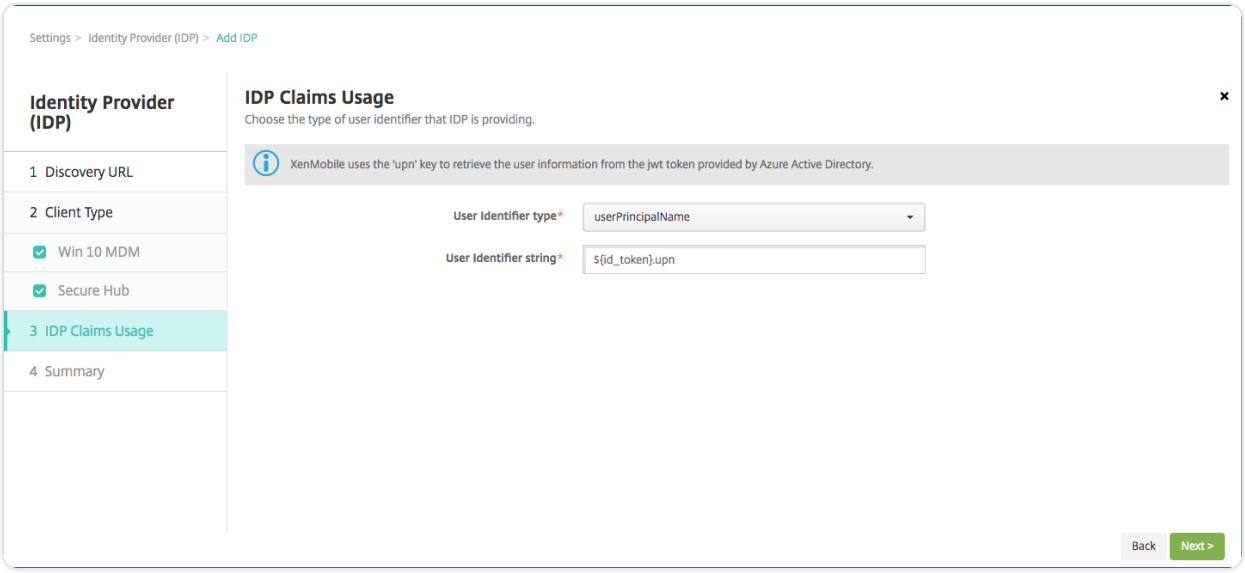
9. 单击**下一步**。



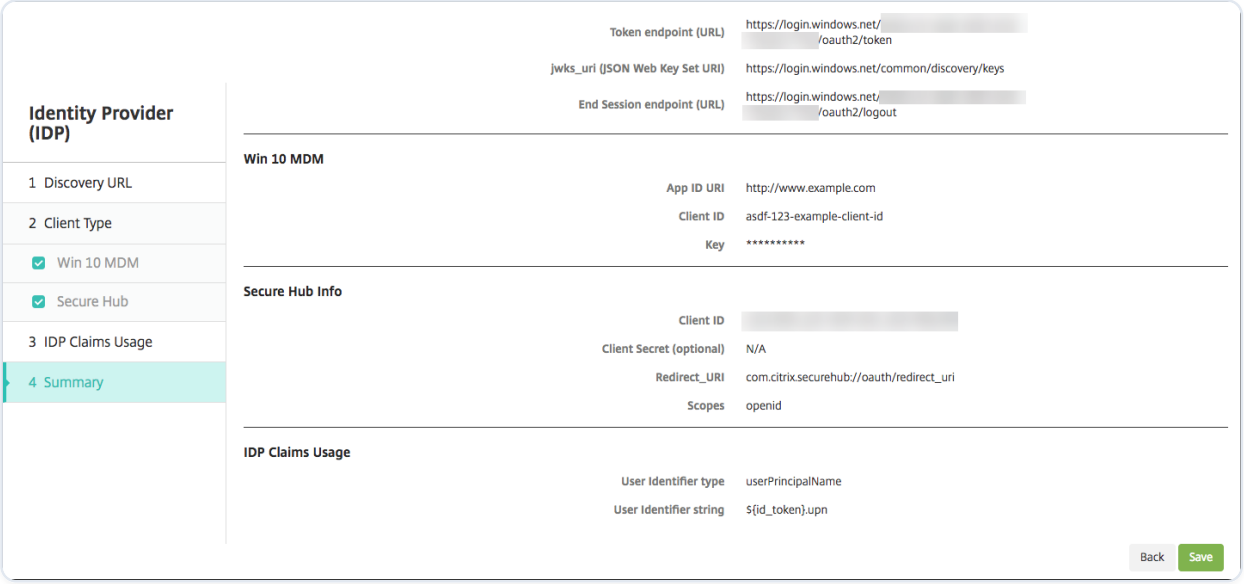
10. 配置您的 IdP 提供的用户标识符类型：

    - **用户标识符类型：** 从列表中选择 **userPrincipalName**。
    - **用户标识符字符串：** 此字段将自动填充。

11. 单击**下一步**。

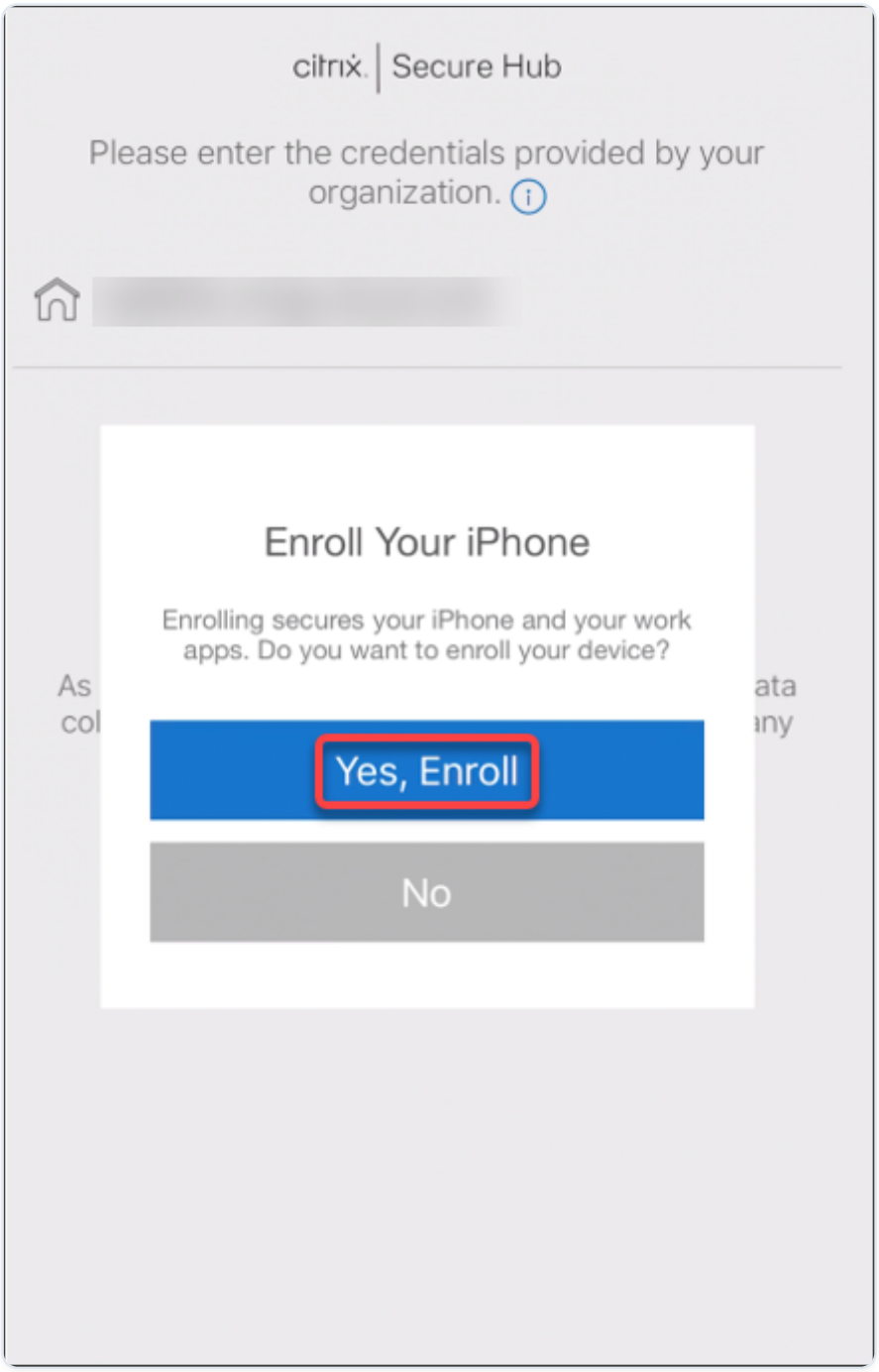


12. 查看**摘要**页面，然后单击**保存**。

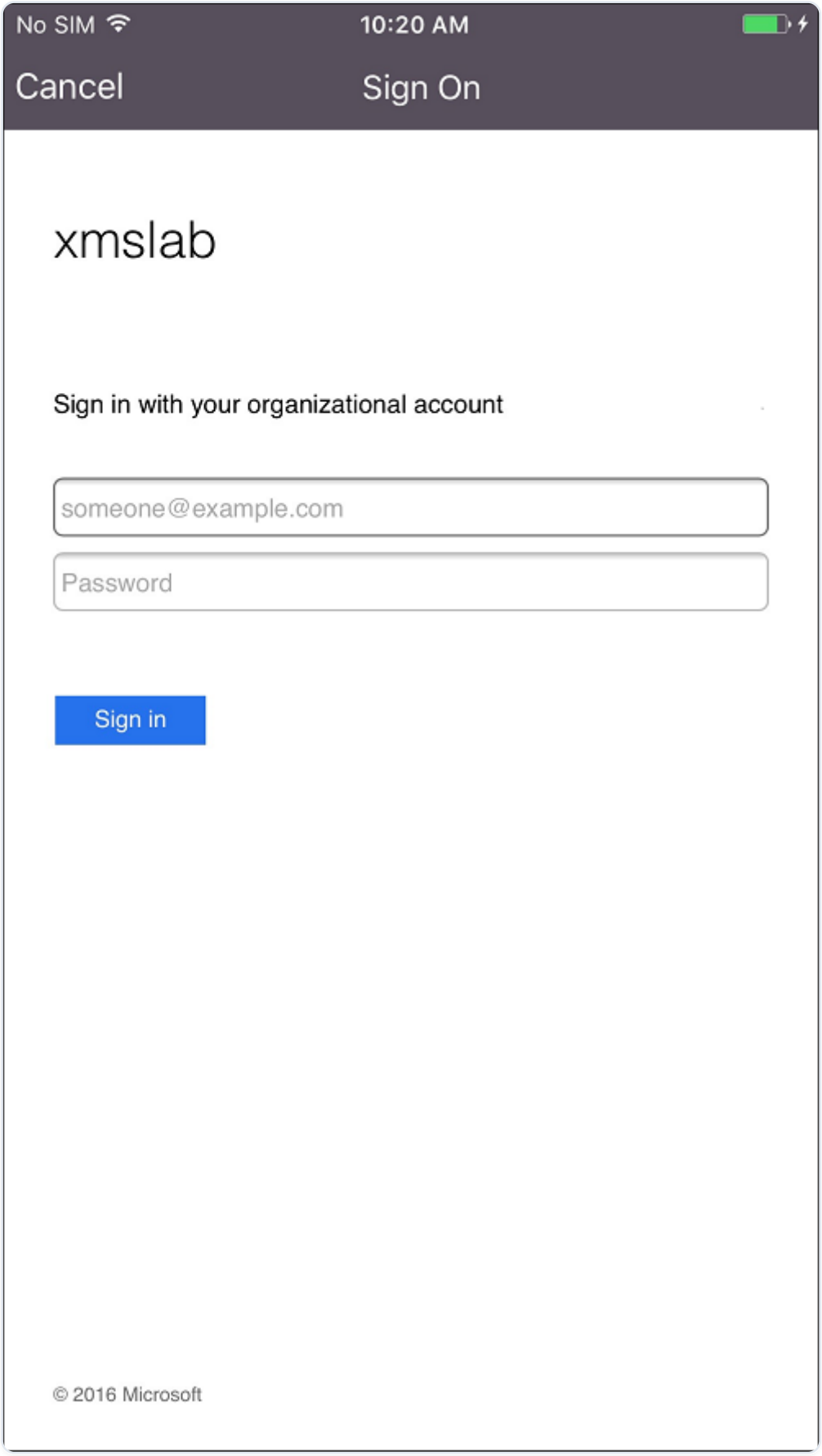


用户体验

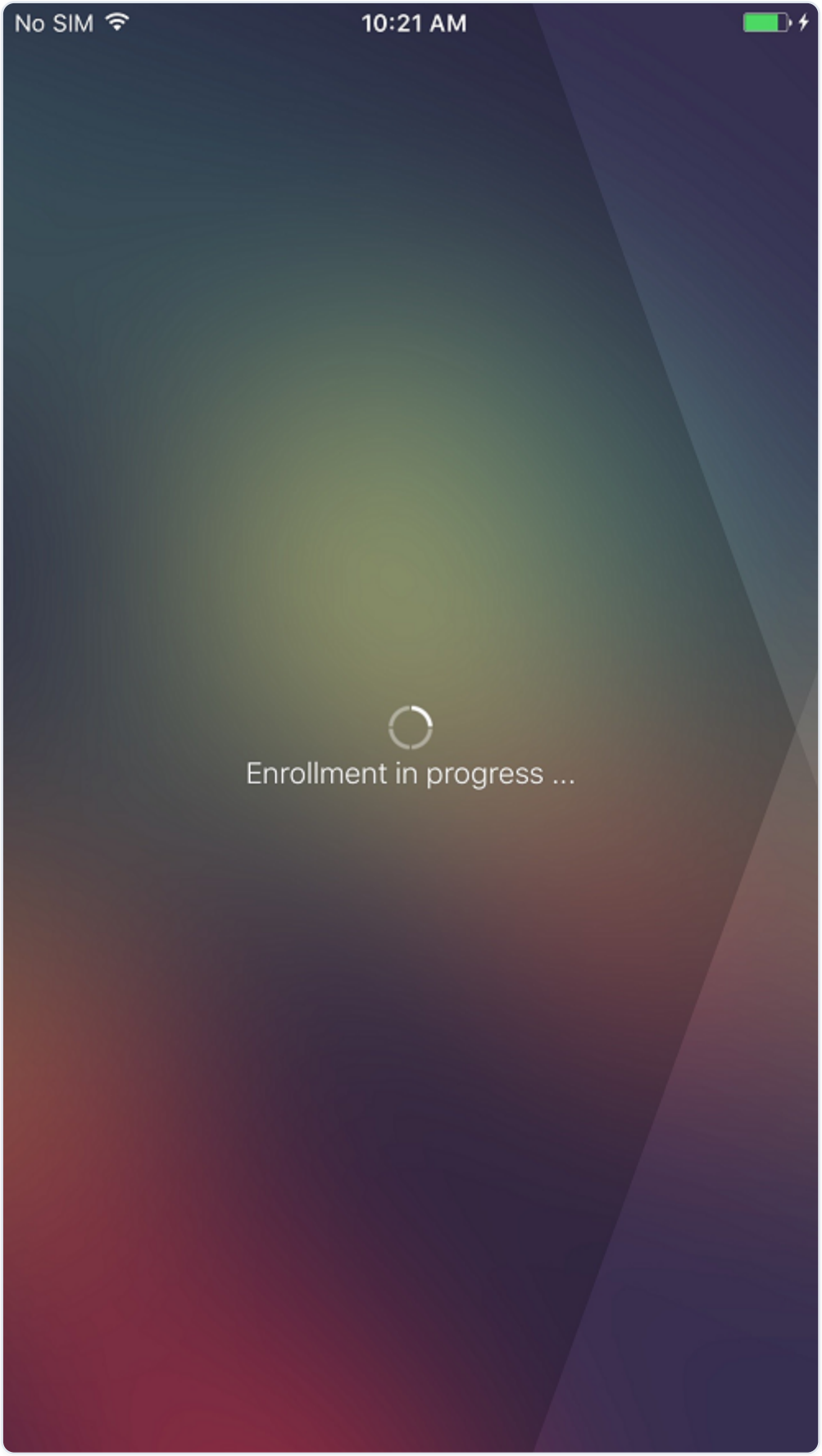
1. 用户启动 Secure Hub。然后，用户输入 XenMobile Server 完全限定域名 (FQDN)、用户主体名称 (UPN) 或电子邮件地址。

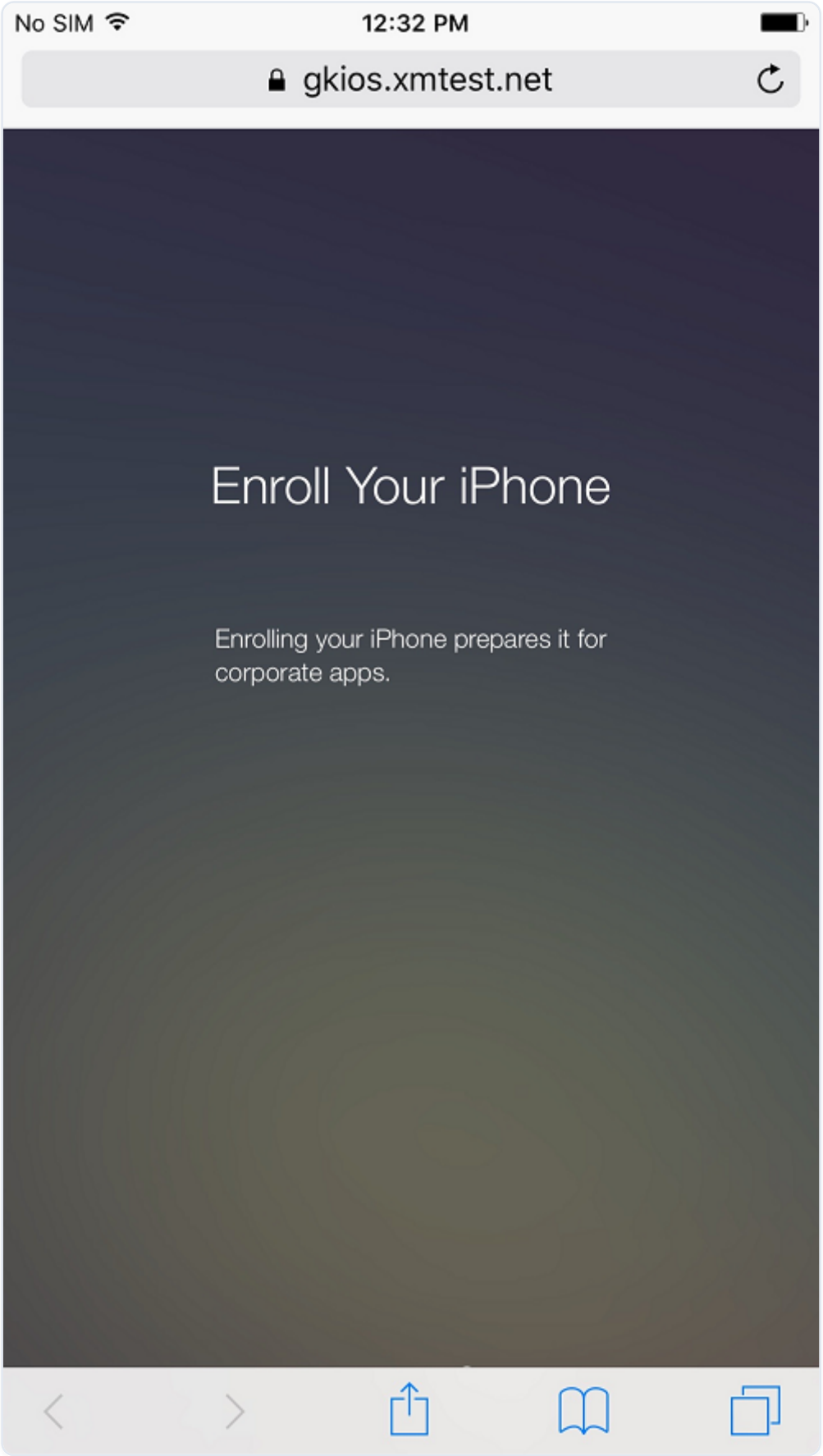

citrix. | Secure Hub
Please enter the credentials provided by your organization.
Enroll Your iPhone
Enrolling secures your iPhone and your work apps. Do you want to enroll your device?
Yes, Enroll
No

2. 然后，用户单击**是，注册**。



3. 用户使用其 Azure AD 凭据登录。


No SIM
10:21 AM
Enrollment in progress ...



Secure Hub 屏幕截图(/en-us/xenmobile/server/media/secure-hub-ios-idp-enroll5.png)

4. 用户通过 Secure Hub 完成注册步骤的方式与进行其他注册的方式相同。

注意：

XenMobile 不支持通过 Azure AD 对注册邀请进行身份验证。如果您向用户发送包含注册 URL 的注册邀请，用户将通过 LDAP 而非 Azure AD 进行身份验证。

升级

升级到 XenMobile 10.16 之前

1. 在更新到最新版本的 XenMobile Server 10.16 之前，请将您的 Citrix License Server 更新到 11.17.2.0 Build 47000 或更高版本。

   最新版本的 XenMobile 需要 Citrix License Server 11.17（最低版本）。

   XenMobile 10.16 中的客户成功服务日期（以前称为订阅权益日期）是 November 15, 2022。您的 Citrix 许可证上的客户成功服务日期必须晚于此日期。您可以在许可证服务器中许可证旁边查看该日期。如果您将最新版本的 XenMobile 连接到较旧的许可证服务器环境，则连接检查将失败，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，然后将该文件上传到许可服务器。有关详细信息，请参阅客户成功服务。
2. 对于群集环境：向运行 iOS 11 及更高版本的设备部署 iOS 策略和应用程序有以下要求。如果 Citrix Gateway 配置为 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 RAM 小于 8 GB，建议您将 RAM 增加到至少 8 GB。
4. 建议：在安装 XenMobile 更新之前，请使用 VM 中的功能为系统创建快照。此外，请备份您的系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。

升级

您可以直接从 XenMobile 10.15.x 或 10.14.x 升级到 XenMobile 10.16。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 > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击**下载文件**。要上传升级，请使用 XenMobile 控制台中的**版本管理**页面。

使用版本管理页面进行升级

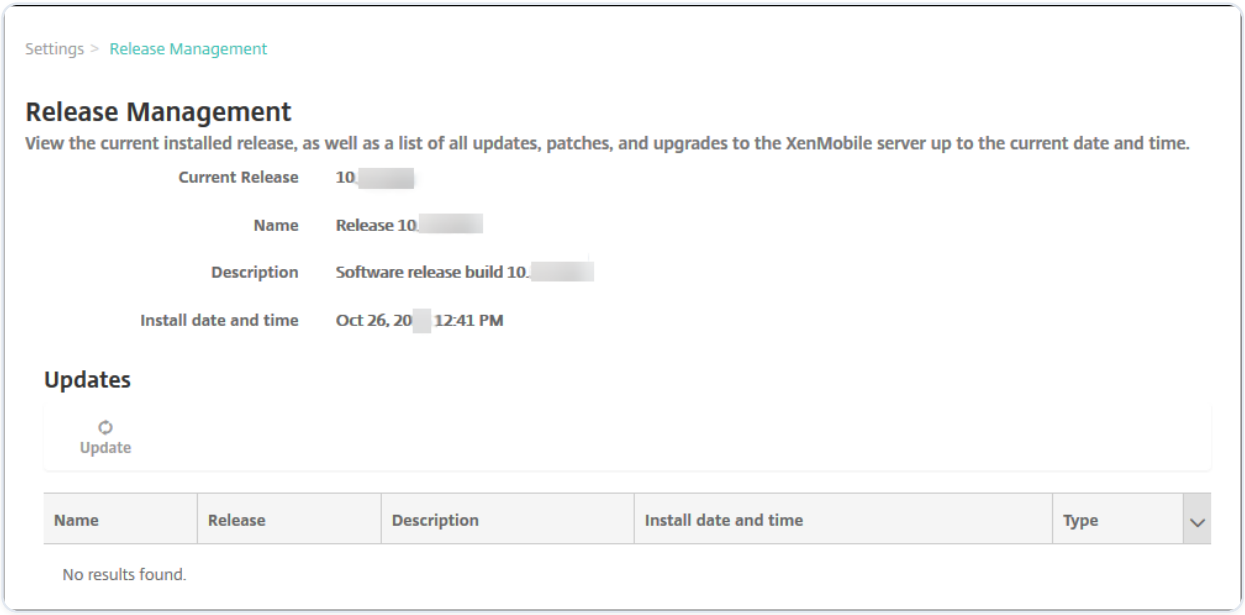
使用**版本管理**页面升级到最新版本的 XenMobile Server。

必备条件：

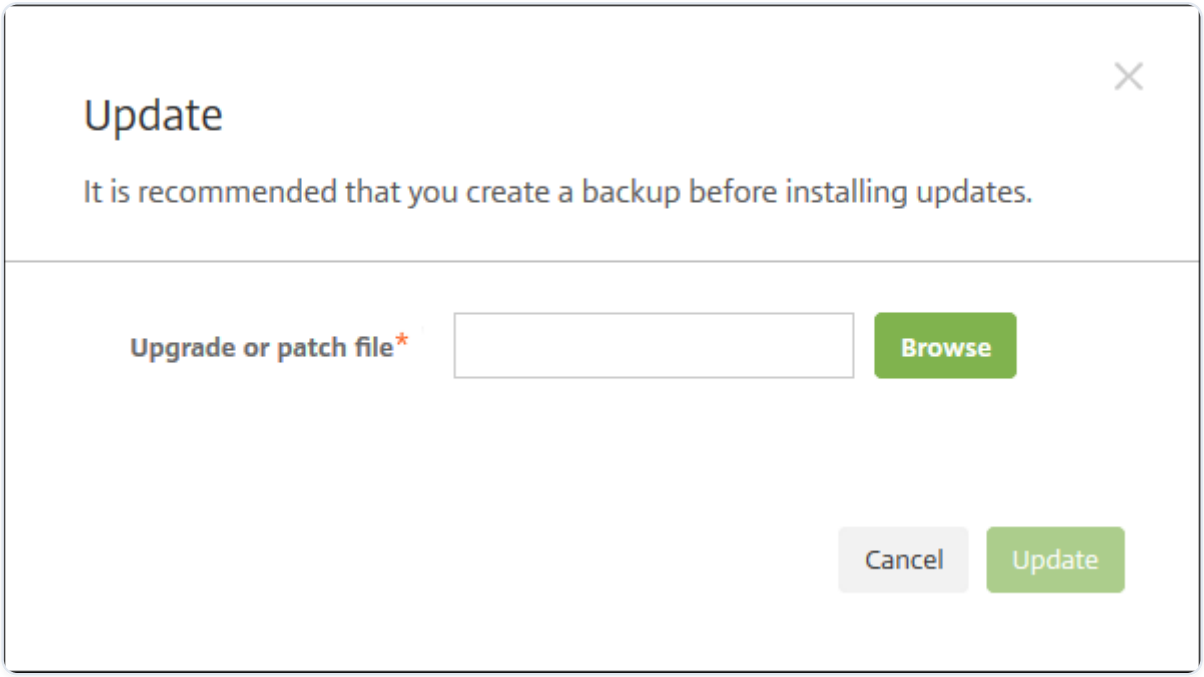
- 查看系统要求。

如果您有集群部署，请参阅本文末尾的说明。

1. 下载最新的可用二进制文件：转到 `<https://www.citrix.com/downloads>`。导航到 **Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**。在适用于您的虚拟机管理程序的 XenMobile Server 软件磁贴上，单击 **Download File**。
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“**版本管理**”。此时将显示“**版本管理**”页面。



4. 在“**更新**”下，单击“**更新**”。此时将显示“**更新**”对话框。



5. 通过单击“**浏览**”并导航到文件位置，选择从 Citrix.com 下载的 XenMobile 升级文件。
6. 单击“**更新**”，如果出现提示，请重新启动 XenMobile。

   如果由于某种原因无法成功完成更新，则会显示一条错误消息以指示问题。系统将恢复到更新尝试之前的状态。

升级后

升级后，XenMobile 需要重新启动。使用 XenMobile CLI 重新启动 XenMobile Server。系统重新启动后，务必清除浏览器缓存。

如果涉及出站连接的功能停止工作，并且您没有更改连接配置，请检查 **XenMobile Server 日志**中是否存在以下错误：“无法连接到 VPP 服务器：主机名 '192.0.2.0' 与对等方提供的证书主题不匹配”

证书验证错误表明您需要在 XenMobile Server 上禁用主机名验证。默认情况下，除 Microsoft PKI 服务器外，出站连接上均启用主机名验证。如果主机名验证导致您的部署中断，请将服务器属性 **disable.hostname.verification** 更改为 **true**。此属性的默认值为 **false**。

Citrix 会将 XenMobile 的新版本或重要更新发布到 Citrix.com。同时，会向每位客户的备案联系人发送通知。

升级群集 XenMobile 部署

> **重要提示：**
>
> 在安装 XenMobile 更新之前，请使用虚拟机 (VM) 中的功能对系统进行快照。此外，请备份系统配置数据库。如果在升级过程中遇到问题，完整的备份可帮助您恢复。
>
> 如果您的系统配置为群集模式，请按照以下步骤从 XenMobile 10 版本更新每个节点：

1. 从**设置 > 版本管理**将 .bin 文件上传到所有节点。
2. 从 CLI 中的**系统菜单**关闭所有节点。
3. 从 CLI 中的**系统菜单**启动一个节点，并检查服务是否正在运行。
4. 逐个启动其他节点。

   如果 XenMobile 无法成功完成更新，将显示错误消息以指示问题。然后，XenMobile 会将系统恢复到更新尝试之前的状态。

从 XenMobile MDM 版本升级到企业版

您可以将 XenMobile MDM Edition 升级到适用于 iOS 和 Android 设备的 XenMobile Advanced Edition（本地）或 Citrix Endpoint Management™（云）。

先决条件

- 正确的 Enterprise 许可证。
- Citrix Gateway 已配置。

升级

1. 转到 **设置 > 许可** 并验证是否已上传正确的企业版许可证类型。
2. 转到 **设置 > 服务器属性** 并将 **服务器模式** 属性从 **MDM** 更改为 **ENT**。
3. 转到 **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 版本相同，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：转到 **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才能将设备切换到企业模式。

iOS 用户

1. 关闭 Secure Hub：快速轻按设备主屏幕按钮两次，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. 转到 **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 会提示用户创建 PIN。用户创建 PIN 后，XenMobile 会将设备配置为企业模式。在 XenMobile 控制台中，**管理 > 设备** 页面会显示设备的 MDM 和 MAM 均处于活动状态。

用户帐户、角色和注册

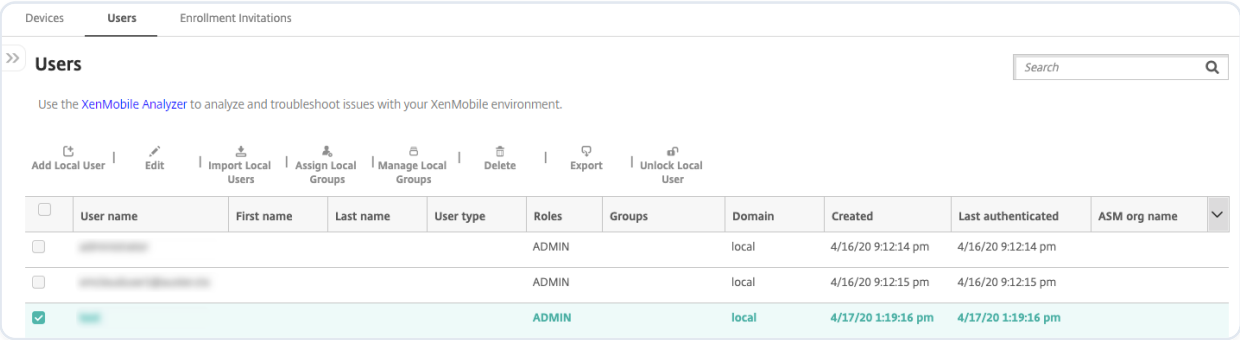
您可以在 XenMobile® 控制台的“**管理**”选项卡和“**设置**”页面中配置用户帐户、角色和注册。除非另有说明，否则本文中提供了以下任务的步骤。

- 用户帐户和组：
  - 在“**管理 > 用户**”中，手动添加用户帐户，或使用 .csv 预配文件导入帐户并管理本地组。
  - 在“**设置 > 工作流**”中，使用工作流管理用户帐户的创建和删除。
- 用户帐户和组的角色
  - 在“**设置 > 基于角色的访问控制**”中，将预定义角色或权限集分配给用户和组。这些权限控制用户对系统功能的访问级别。有关详细信息，请参阅使用 RBAC 配置角色。
  - 在“**设置 > 通知模板**”中，创建或更新要在自动化操作、注册以及发送给用户的标准通知消息中使用的通知模板。您可以配置通知模板以通过三种不同的渠道发送消息：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
  - 在“**设置 > 注册**”中，配置最多七种注册安全模式并发送注册邀请。每种注册安全模式都有自己的安全级别以及用户注册其设备必须执行的步骤。
  - 在 XenMobile 中为用户注册启用 AutoDiscovery

添加、编辑、解锁或删除本地用户帐户

您可以手动将本地用户帐户添加到 XenMobile，也可以使用预配文件导入帐户。有关从预配文件导入用户帐户的步骤，请参阅导入用户帐户。

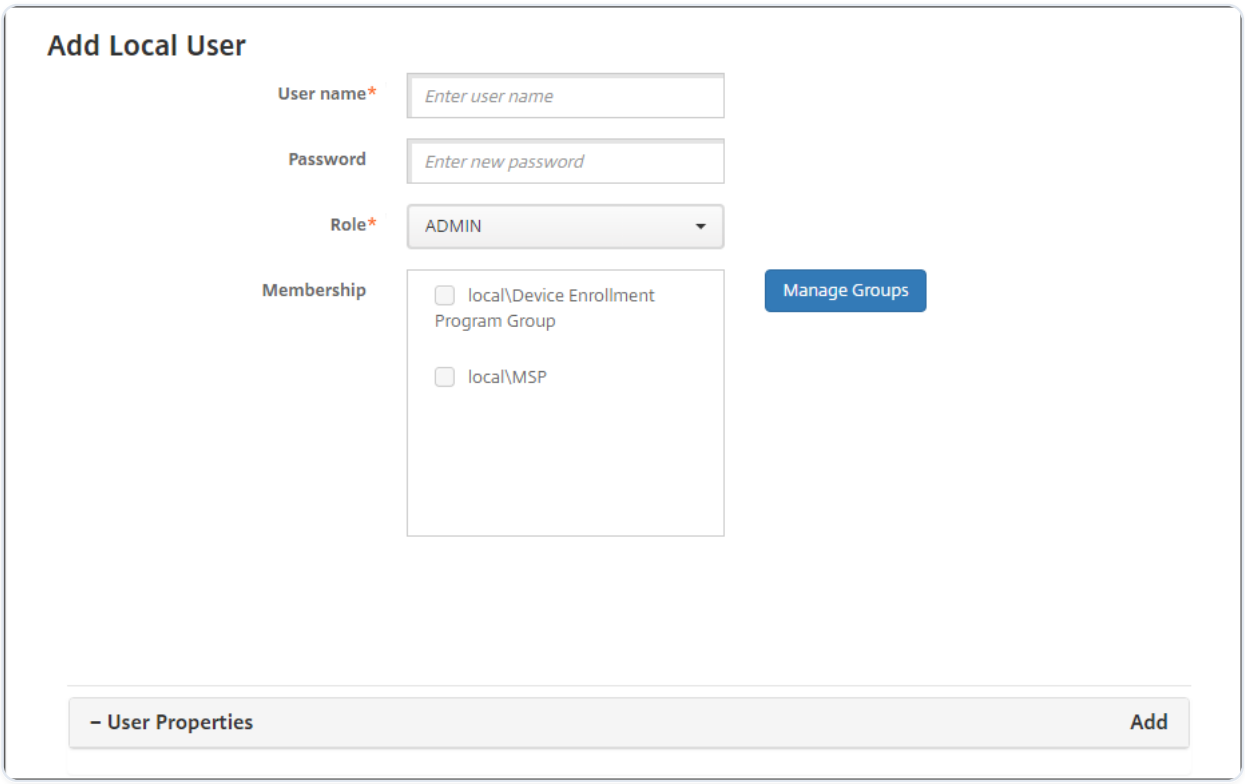
1. 在 XenMobile 控制台中，单击“**管理 > 用户**”。此时将显示“**用户**”页面。



2. 点击**显示筛选器**以筛选列表。

添加本地用户帐户

1. 在**用户**页面上，单击**添加本地用户**。此时将显示**添加本地用户**页面。



2. 配置以下设置：

- **用户名：** 键入名称，这是一个必填字段。名称中可以包含空格以及大小写字母。
- **密码：** 键入可选的用户密码。密码必须至少包含 14 个字符，并满足以下所有条件：
  - 包含至少两个数字
  - 包含至少一个大写字母和一个小写字母
  - 包含至少一个特殊字符
  - 不包含字典词或受限词，例如您的 Citrix® 用户名或电子邮件地址

  - 不包含三个以上连续重复的字符或键盘模式，例如 1111、1234 或 asdf

- **角色：** 在列表中，单击用户角色。有关角色的更多信息，请参阅使用 RBAC 配置角色。可能的选项包括：
  - ADMIN
  - DEVICE_PROVISIONING
  - 支持
  - 用户
- **成员资格：** 在列表中，单击要添加用户的组。
- **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**并执行以下操作：
  - **用户属性：** 在列表中，单击一个属性，然后在属性旁边的字段中键入用户属性值。
  - 单击**完成**以保存用户属性，或单击**取消**。

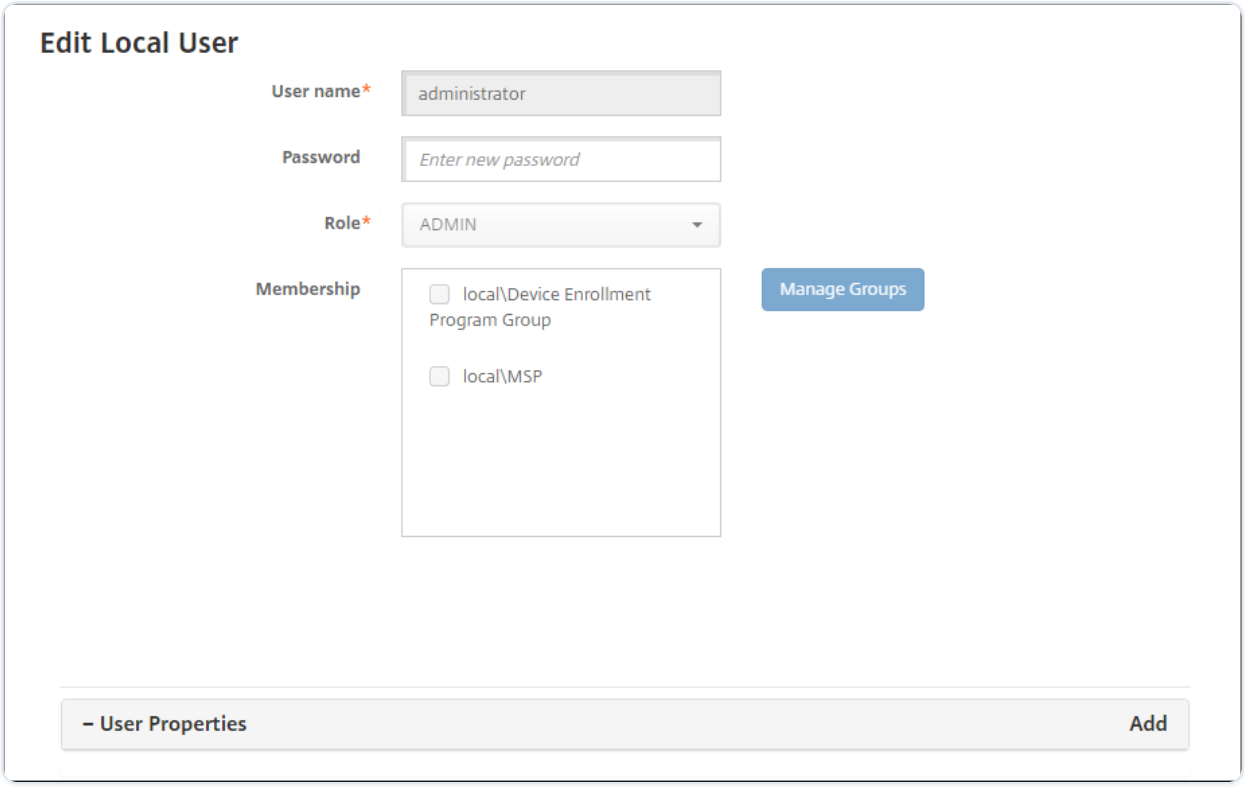
要删除现有用户属性，请将鼠标悬停在包含该属性的行上，然后单击右侧的 X。该属性将立即删除。

要编辑现有用户属性，请单击该属性并进行更改。单击**完成**以保存更改的列表，或单击**取消**以保持列表不变。

3. 单击**保存**。

编辑本地用户帐户

1. 在**用户**页面上，在用户列表中，单击以选择一个用户，然后单击**编辑**。此时将显示**编辑本地用户**页面。



2. 根据需要更改以下信息：

- **用户名：** 您无法更改用户名。
- **密码：** 更改或添加用户密码。
- **角色：** 在列表中，单击用户角色。
- **成员资格：** 在列表中，单击要添加或编辑用户帐户的组。要从组中删除用户帐户，请清除组名称旁边的复选框。
- **用户属性：** 执行以下操作之一：
  - 对于要更改的每个用户属性，单击该属性并进行更改。单击“**完成**”以保存更改的列表，或单击“**取消**”以使列表保持不变。
  - 对于要添加的每个用户属性，单击“**添加**”并执行以下操作：
    - **用户属性：** 在列表中，单击一个属性，然后在该属性旁边的字段中键入用户属性值。
    - 单击“**完成**”以保存用户属性，或单击“**取消**”。
  - 对于要删除的每个现有用户属性，将鼠标悬停在包含该属性的行上，然后单击右侧的“**X**”。该属性将立即删除。

3. 单击“**保存**”以保存更改，或单击“**取消**”以使用户保持不变。

解锁本地用户帐户

1. 在“**用户**”页面上的用户帐户列表中，单击以选择一个用户帐户。
2. 单击“**解锁本地用户**”。此时将显示一个确认对话框。
3. 单击“**解锁**”以解锁用户帐户，或单击“**取消**”以使用户保持不变。

删除本地用户帐户

1. 在“**用户**”页面上的用户帐户列表中，单击以选择一个用户帐户。

您可以通过选中每个用户帐户旁边的复选框来选择多个要删除的用户帐户。

1. 单击**删除**。将出现一个确认对话框。
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**。

如果您删除的用户已注册设备，并且您希望重新注册这些设备，请在重新注册之前删除这些设备。要删除设备，请转到**管理 > 设备**，选择设备，然后单击**删除**。

导入用户帐户

您可以从名为预配文件的 .csv 文件导入本地用户帐户和属性，该文件可以手动创建。有关预配文件格式的更多信息，请参阅预配文件格式。

注意：

- 对于本地用户，请在导入文件中使用域名和用户名。例如，指定 username@domain。如果您创建或导入的本地用户用于 XenMobile 中的托管域，则该用户无法使用相应的 LDAP 凭据进行注册。
- 如果要将用户帐户导入 XenMobile 内部用户目录，请禁用默认域以加快导入过程。请记住，禁用域会影响注册，因此在内部用户导入完成后重新启用默认域。
- 本地用户可以是用户主体名称 (UPN) 格式。但是，Citrix 建议您不要使用托管域。例如，如果 example.com 是托管域，请勿创建具有此 UPN 格式的本地用户：user@example.com。

> 准备好预配文件后，请按照以下步骤将文件导入 XenMobile。

1. 在 XenMobile 控制台中，单击**管理 > 用户**。将显示**用户**页面。
2. 单击**导入本地用户**。将显示**导入预配文件**对话框。

   用户管理图像(/en-us/xenmobile/server/media/local-users-and-groups-import-provisioning-file.png)

3. 对于要导入的预配文件的格式，请选择“**用户**”或“**属性**”。
4. 单击“**浏览**”，然后导航到文件位置，选择要使用的预配文件。
5. 单击“**导入**”。

预配文件格式

您可以手动创建预配文件，以将用户帐户和属性导入到 XenMobile。有效格式如下：

- **用户预配文件字段：** `user;password;role;group1;group2`
- **用户属性预配文件字段：** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> **注意：**
>
> - 使用分号 (;) 分隔预配文件中的字段。如果字段的一部分包含分号，请使用反斜杠字符 (\\) 对其进行转义。例如，在预配文件中将属性 `propertyV;test;1;2` 键入为 `propertyV\\;test\\;1\\;2`。
> - **角色**的有效值为预定义角色 USER、ADMIN、SUPPORT 和 DEVICE_PROVISIONING，以及您定义的任何其他角色。
> - 使用句点字符 (.) 作为分隔符来创建组层次结构。请勿在组名称中使用句点。
> - 在属性预配文件中，属性特性请使用小写。数据库区分大小写。

用户预配内容示例

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`

再举一个例子，`AUser0;1.password;USER;ActiveDirectory.test.net` 表示：

- **用户：** `AUser0`
- **密码：** `1.password`
- **角色：** `USER`
- **组：** `ActiveDirectory.test.net`

用户属性预配内容的示例

条目 `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` 表示：

- **用户：** `user01`
- **属性 1**
  - **名称：** `propertyN`
  - **值：** `propertyV;test;1;2`
- **属性 2：**
  - **名称：** `prop 2`
  - **值：** `prop2 value`

配置注册安全模式

您可以配置设备注册安全模式，以指定 XenMobile 中设备注册的安全级别和通知模板。

XenMobile 提供七种注册安全模式，每种模式都有自己的安全级别以及用户注册其设备必须采取的步骤。您可以在 XenMobile Server 控制台中从“**设置 > 注册**”页面配置注册安全模式。

您可以使某些模式在自助服务门户上可用。用户可以从门户生成注册链接，以便注册其设备。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。Windows 设备不提供注册邀请。

您可以从“**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：**
>
> 如果您计划使用自定义通知模板，则必须在配置注册安全模式之前设置这些模板。有关通知模板的详细信息，请参阅创建或更新通知模板。

1. 在 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，所有注册安全模式都处于启用状态。
3. 选择列表中的任何注册安全模式进行编辑。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：**
   >
   > 当您选择注册安全模式旁边的复选框时，选项菜单会出现在注册安全模式列表上方。当您单击列表中的其他任何位置时，选项菜单会出现在列表的右侧。
   >
   > 注册设置图像(/en-us/xenmobile/server/media/settings-enrollment.png)

   从以下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
   - 双因素身份验证
   - 用户名 + PIN

   您可以使用注册邀请来限制只有收到邀请的用户才能注册。要发送注册邀请，您只能使用**邀请 URL**、**邀请 URL + PIN**或**邀请 URL + 密码**注册安全模式。对于使用**用户名 + 密码**、**双因素身份验证**或**用户名 + PIN**注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

   您可以将一次性 PIN (OTP) 注册邀请用作双因素身份验证解决方案。OTP 注册邀请可控制用户可以注册的设备数量。OTP 邀请不适用于 Windows 设备。

编辑注册安全模式

1. 在 **注册** 列表中，选择一个注册安全模式，然后单击 **编辑**。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。

   注册安全模式编辑(/en-us/xenmobile/server/media/settings-enrollment-edit.png)

2. 根据需要更改以下信息：

   - **过期时间：** 键入一个过期截止日期，在此日期之后用户无法注册其设备。此值显示在用户和组注册邀请配置页面中。

     键入 **0** 可防止邀请过期。
   - **天数：** 在列表中，单击 **天数** 或 **小时** 以与您在 **过期时间** 中输入的过期截止日期相对应。
   - **最大尝试次数：** 键入用户在被锁定在注册过程之外之前可以尝试注册的次数。此值显示在用户和组注册邀请配置页面中。

     键入 **0** 以允许无限次尝试。
   - **PIN 长度：** 键入一个数字以设置生成的 PIN 的长度。
   - **数字：** 在列表中，单击 **数字** 或 **字母数字** 作为 PIN 类型。
   - **通知模板：**
     - **注册 URL 模板：** 在列表中，单击一个模板以用于注册 URL。例如，注册邀请模板会向用户发送电子邮件或短信。该方法取决于您如何配置允许用户在 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，单击一个模板以用于注册 PIN。
     - **注册确认模板：** 在列表中，单击一个模板以用于通知用户他们已成功注册。

3. 单击 **保存**。

将注册安全模式设置为默认模式

当您将注册安全模式设置为默认模式时，除非您选择不同的注册安全模式，否则该模式将用于所有设备注册请求。如果没有注册安全模式设置为默认模式，则必须为每个设备注册创建一个注册请求。

> **注意：**
>
> 您可以设置为默认模式的注册安全模式只有“**仅用户名 + 密码**”、“**双因素**”或“**用户名 + PIN**”。

1. 选择默认注册安全模式，可以是“**用户名 + 密码**”、“**双因素**”或“**用户名 + PIN**”。

   要将模式用作默认模式，请首先启用它。

2. 单击“**默认**”。所选模式现在是默认模式。如果之前有其他注册安全模式设置为默认模式，则该模式将不再是默认模式。

禁用注册安全模式

禁用注册安全模式会使其无法用于组注册邀请和自助服务门户。您可以通过禁用一个注册安全模式并启用另一个来更改用户注册设备的方式。

1. 选择注册安全模式。

   您无法禁用默认注册安全模式。如果要禁用默认注册安全模式，必须首先取消其默认状态。

2. 单击“**禁用**”。注册安全模式不再启用。

在自助服务门户上启用注册安全模式

在自助服务门户上启用注册安全模式允许用户在 XenMobile 中单独注册其设备。

> **注意：**
>
> - 注册安全模式必须启用并绑定到通知模板，才能在自助服务门户上提供。
> - 您一次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**。您选择的注册安全模式现在可供自助服务门户上的用户使用。自助服务门户上已启用的任何模式将不再可供用户使用。

添加或删除组

您可以在 XenMobile 控制台的 **用户**、**添加本地用户** 或 **编辑本地用户** 页面中的 **管理组** 对话框中管理组。没有组编辑命令。

如果您删除一个组，请记住删除组对用户帐户没有影响。删除组只是删除用户与该组的关联。用户还将失去对与该组关联的交付组提供的应用程序或配置文件的访问权限；但是，任何其他组关联保持不变。如果用户未与任何其他本地组关联，则他们将与顶层关联。

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**。

   用户组管理图像(/en-us/xenmobile/server/media/local-users-and-groups-page-menu.png)

   - 在 **添加本地用户** 页面或 **编辑本地用户** 页面上，单击 **管理组**。

   用户组管理图像(/en-us/xenmobile/server/media/local-users-and-groups-manage-group.png)

   管理组 对话框随即显示。

   用户组管理图像(/en-us/xenmobile/server/media/local-users-and-groups-manage-group-add.png)

2. 在组列表下方，键入新组名称，然后单击加号 (**+**)。用户组将添加到列表中。
3. 单击“**关闭**”。

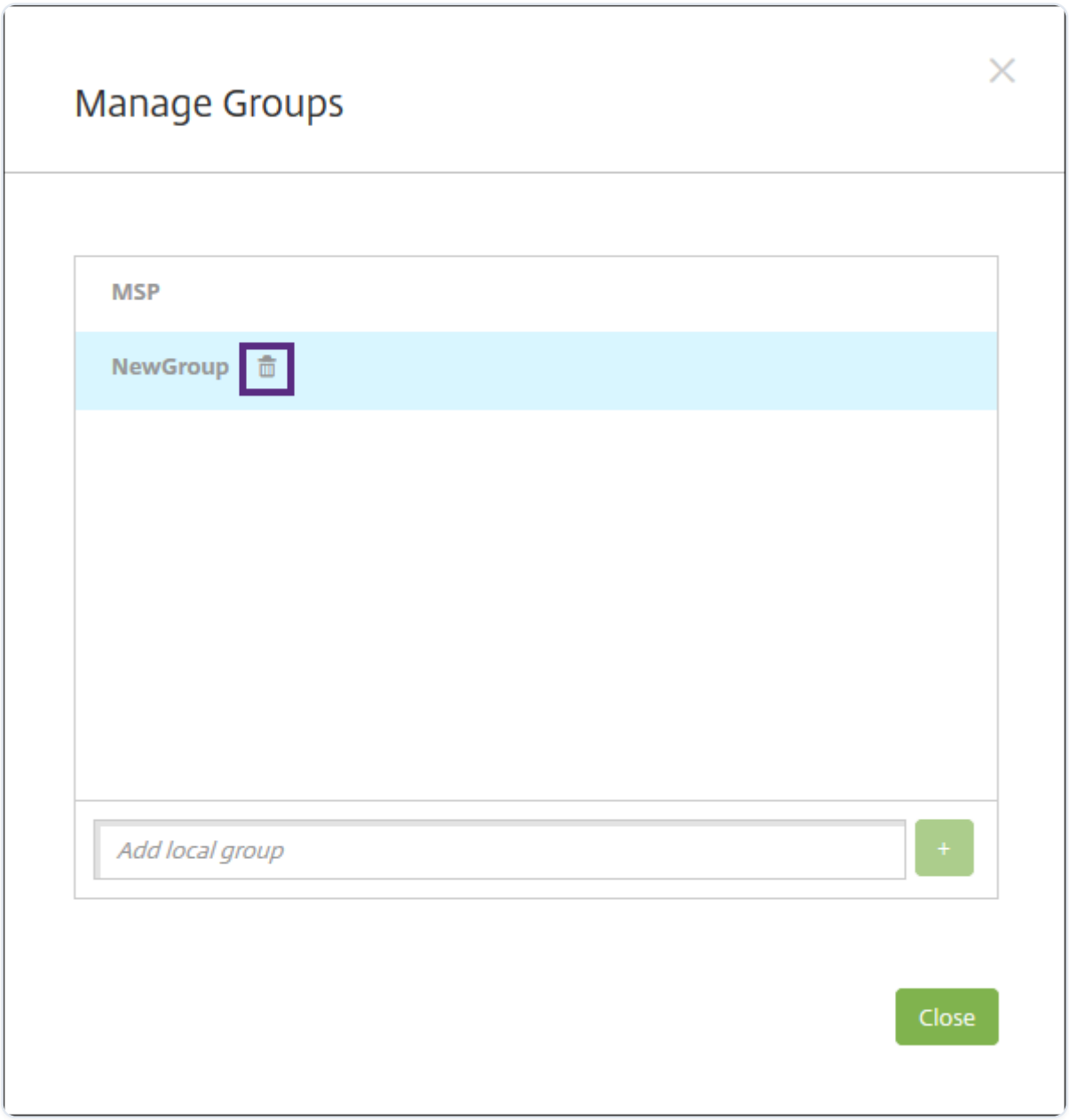
删除组

删除组对用户帐户没有影响。删除组只是删除用户与该组的关联。用户还将失去对与该组关联的交付组提供的应用程序或配置文件的访问权限。但是，任何其他组关联保持不变。如果用户未与任何其他本地组关联，则他们将与顶级关联。

1. 执行以下操作之一：

   - 在“**用户**”页面上，单击“**管理本地组**”。
   - 在“**添加本地用户**”页面或“**编辑本地用户**”页面上，单击“**管理组**”。

   此时将显示“**管理组**”对话框。



2. 在“**管理组**”对话框中，单击要删除的组。
3. 单击组名称右侧的垃圾桶图标。此时将显示确认对话框。
4. 单击“**删除**”以确认操作并删除组。

> **重要提示：**
>
> 无法撤消此操作。

5. 在“**管理组**”对话框中，单击“**关闭**”。

创建和管理工作流

您可以使用工作流来管理用户帐户的创建和删除。在使用工作流之前，请确定组织中哪些人员有权批准用户帐户请求。然后，您可以使用工作流模板来创建和批准用户帐户请求。

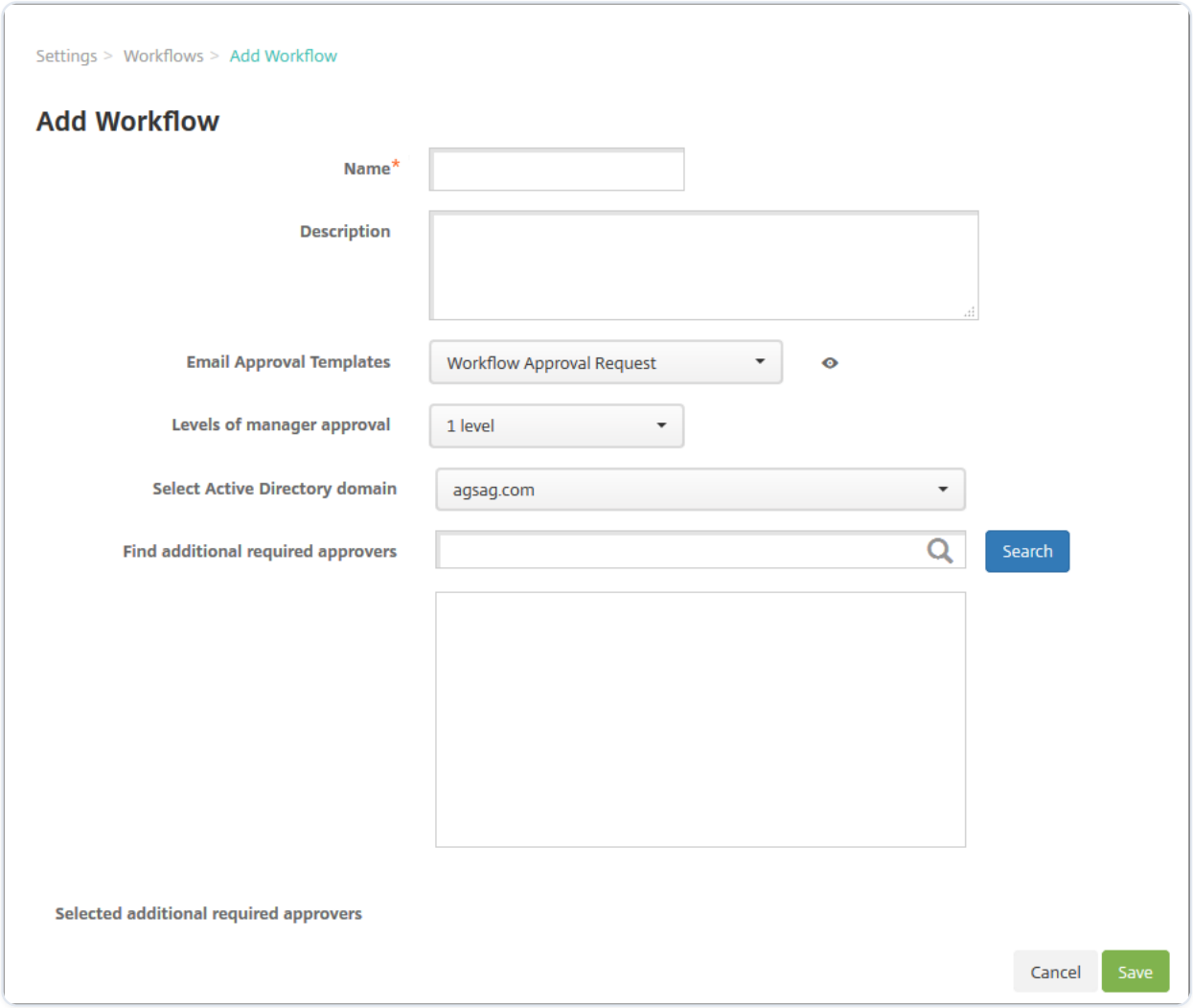
首次设置 XenMobile 时，您需要配置工作流电子邮件设置，这些设置必须在您使用工作流之前完成。您可以随时更改工作流电子邮件设置。这些设置包括电子邮件服务器、端口、电子邮件地址以及创建用户帐户的请求是否需要批准。

您可以在 XenMobile 中的两个位置配置工作流：

- 在 XenMobile 控制台的**工作流**页面中。在**工作流**页面上，您可以配置多个工作流以用于应用程序配置。在工作流页面上配置工作流时，您可以在配置应用程序时选择该工作流。
- 在应用程序中配置应用程序连接器时，您需要提供工作流名称，然后配置可以批准用户帐户请求的人员。请参阅将应用程序添加到 XenMobile。

您可以为用户帐户的经理审批分配最多三个级别。如果您需要其他人批准用户帐户，您可以使用其姓名或电子邮件地址进行搜索和选择。当 XenMobile 找到该人员时，您可以将其添加到工作流中。工作流中的所有人员都会收到批准或拒绝新用户帐户的电子邮件。

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，选择要分配的电子邮件审批模板。您可以在 XenMobile 控制台的设置**下的**通知模板**部分中创建电子邮件模板。当您单击此字段右侧的眼睛图标时，您会看到正在配置的模板的预览。
- **经理审批级别：**在列表中，选择此工作流所需的经理审批级别数。默认值为 **1 级**。可选选项包括：
  - 不需要
  - 1 级
  - 2 级
  - 3 级
- **选择 Active Directory 域：**在列表中，选择要用于此工作流的相应 Active Directory 域。

- **查找其他必需的审批者：** 在搜索字段中键入名称，然后单击“**搜索**”。名称源自 Active Directory。
- 当名称出现在字段中时，选中名称旁边的复选框。名称和电子邮件地址将显示在“**选定的其他必需审批者**”列表中。
  - 要从列表中删除名称，请执行以下操作之一：
    - 单击“**搜索**”以查看所选域中所有人员的列表。
    - 在搜索框中键入完整或部分名称，然后单击“**搜索**”以限制搜索结果。
    - “**选定的其他必需审批者**”列表中的人员在搜索结果列表中其名称旁边带有复选标记。滚动列表并清除要删除的每个名称旁边的复选框。

5. 单击“**保存**”。创建的工作流将显示在“**工作流**”页面上。

创建工作流后，您可以查看工作流详细信息、查看与工作流关联的应用程序或删除工作流。创建工作流后，无法编辑工作流。如果需要具有不同审批级别或审批者的工作流，请创建另一个工作流。

查看详细信息和删除工作流

1. 在“**工作流**”页面上，在现有工作流列表中，选择一个特定的工作流。为此，请单击表中的行或选择工作流旁边的复选框。
2. 要删除工作流，请单击“**删除**”。将出现一个确认对话框。再次单击“**删除**”。

> **重要提示：**
>
> 您无法撤消此操作。

注册配置文件

注册配置文件指定以下内容：

- 适用于 Android 和 iOS 设备的设备管理注册选项。对于 Android，MDM+MAM (ENT) 服务器模式可用的注册选项与 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，错误消息会告知用户他们已超出设备注册限制。

- 是否允许用户拒绝设备管理。

您可以使用注册配置文件在单个 XenMobile® Server 控制台中组合多个用例和设备迁移路径。一些用例包括：

- 移动设备管理 (仅 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、工作资料、专用设备）

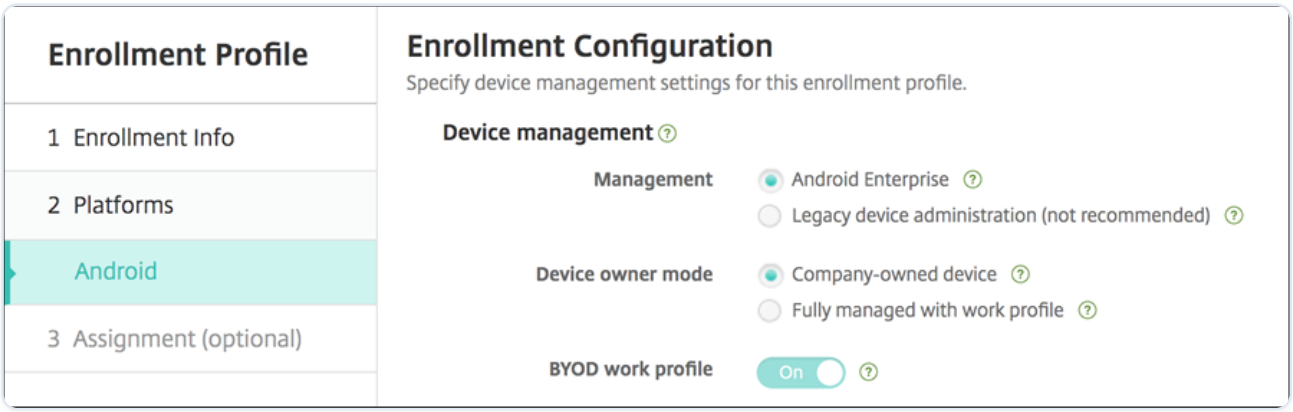
创建交付组时，可以使用名为“全局”的默认注册配置文件，也可以指定其他注册配置文件。

按平台划分的注册配置文件功能包括：

- **对于 Android 设备：** 您可以指定设备所有者模式。例如：完全托管、带工作资料的完全托管以及 BYOD 工作资料。**专用设备**选项仅在您拥有 XenMobile 的企业版或高级版许可证时显示。新设备默认注册到 Android Enterprise 和应用程序管理。注册安全模式“**用户名 + PIN**”、“**邀请 URL**”、“**邀请 URL + PIN**”和“**邀请 URL + 密码**”不适用于 Android Enterprise。
- **对于 iOS 设备：** 您可以指定设备注册类型：设备注册或不管理设备。iOS 设置仅在您拥有 XenMobile 的企业版或高级版许可证时显示。新设备默认注册到 Apple 设备管理和应用程序管理。

如果您不需要为 Android 设备注册专用设备，或者不需要为 Android 或 iOS 设备进行仅 MAM 注册，则可以禁用服务器属性 `enable.multimode.xms`。但是，保持此属性启用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` 后，只有此屏幕截图中的设置可用：

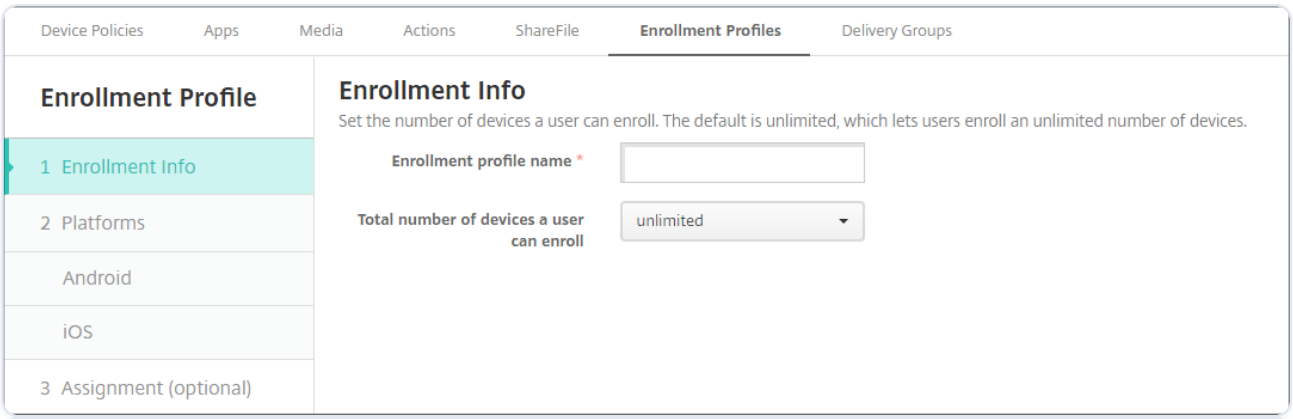


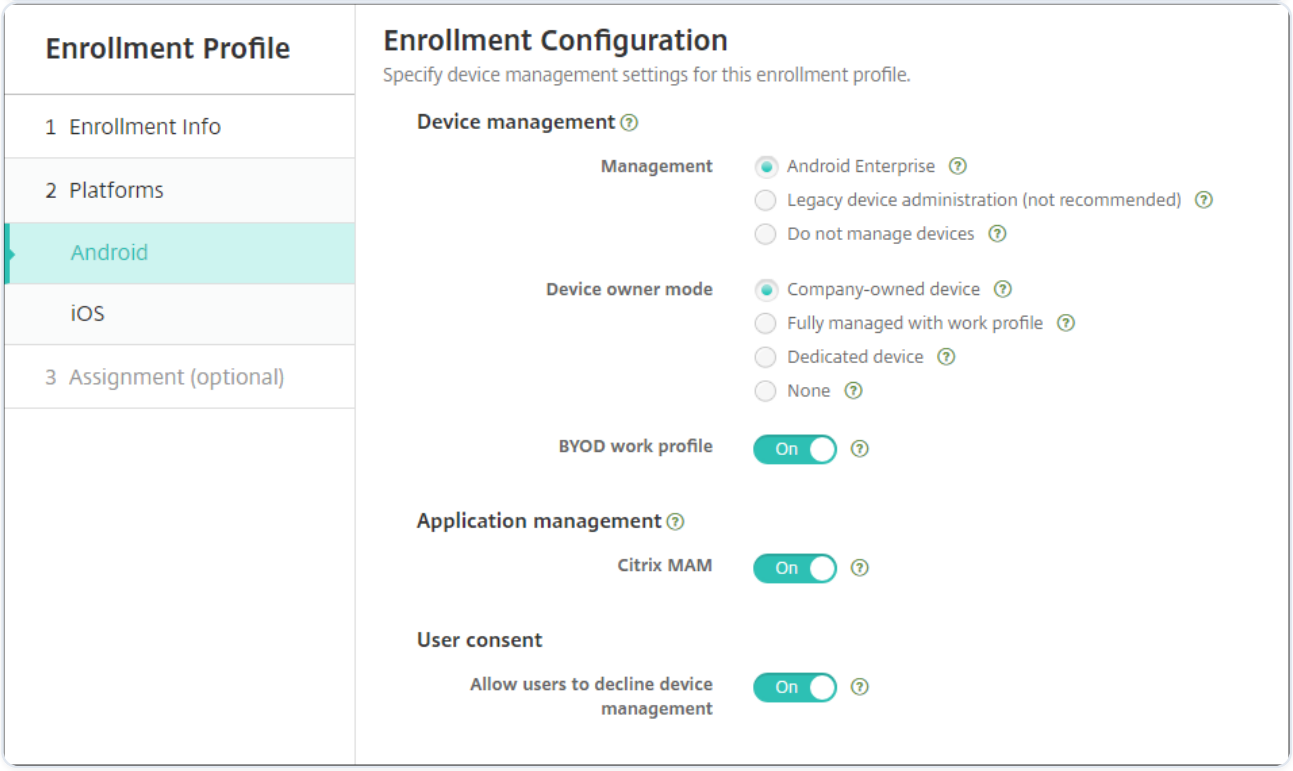
有关这些设置的更多详细信息，请参阅 Android Enterprise。

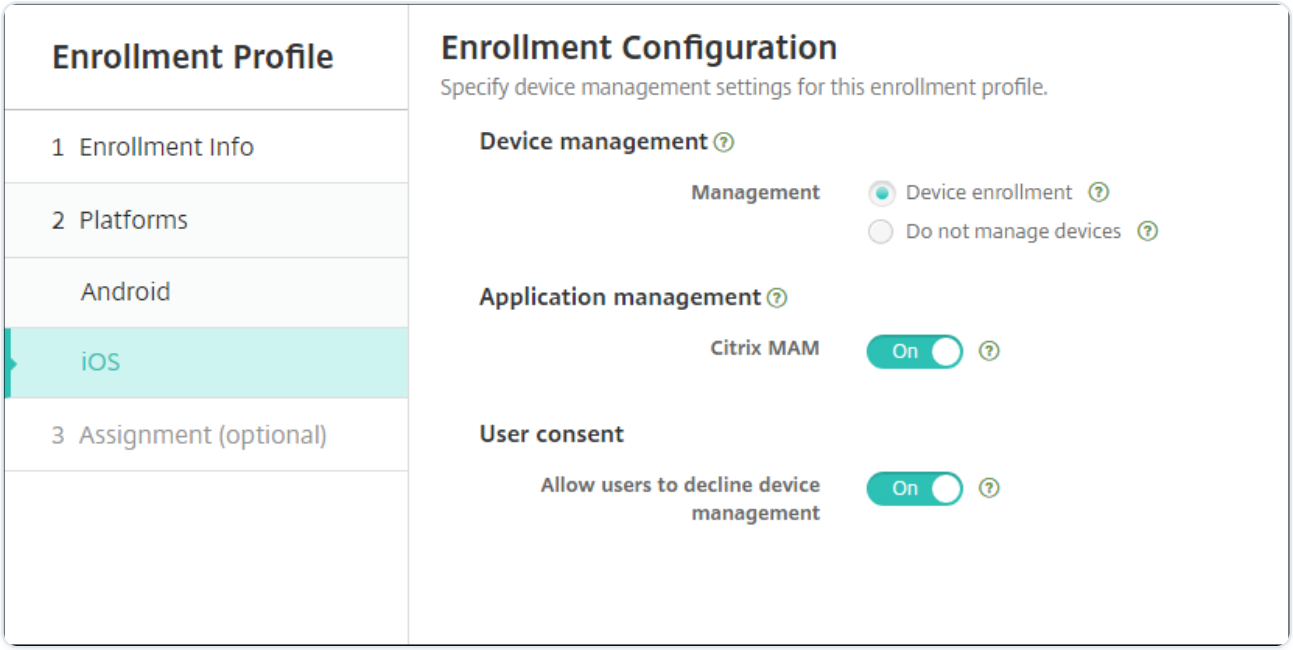
全局注册配置文件

默认注册配置文件名为“全局”。在您有机会创建注册配置文件之前，“全局”配置文件对于测试很有用。

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的交互方式如下：

- 您可以将注册配置文件附加到一个或多个交付组。
- 如果用户属于具有不同注册配置文件的多个交付组，则交付组的名称决定了所使用的注册配置文件。XenMobile Server 会选择按字母顺序排列的交付组列表中最后一个出现的交付组。例如，假设您有以下内容：
  - 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”关联。
  - “DG2”与“EP2”关联。

  如果注册用户同时属于“DG1”和“DG2”交付组，XenMobile Server 将使用“EP2”注册配置文件来确定用户的注册类型。
- 部署顺序仅适用于配置了 MDM（设备管理）注册配置文件的交付组中的设备。
- 设备注册后，对注册配置文件的一些更改需要重新注册：
  - 将 MAM 添加到为 MDM 配置的注册配置文件中。
  - 将已注册 MDM 的设备移动到为 MDM+MAM 配置的交付组。此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中。

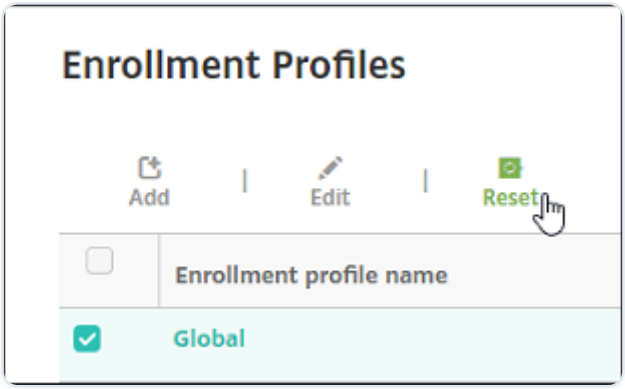
- 切换到不同的注册配置文件不会影响现有已注册设备。但是，用户必须取消注册然后重新注册这些设备，更改才能生效。

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，为配置文件键入一个描述性名称。默认情况下，用户可以注册无限数量的设备。选择一个值以限制每个用户的设备数量。此限制适用于用户注册的 MAM 或 MDM 管理的 Android 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：
   - 安卓企业版
   - 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，交付组的名称决定了所使用的注册配置文件。XenMobile 会选择按字母顺序排列的交付组列表中最后一个出现的交付组。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值，请选择全局配置文件所在行，然后单击 **重置**。您无法删除全局配置文件。



使用 RBAC 配置角色

每个预定义的基于角色的访问控制 (RBAC) 角色都具有某些关联的访问和功能权限。本文介绍了每个权限的作用。有关每个内置角色的默认权限的完整列表，请下载 基于角色的访问控制默认值。

当您*应用权限*时，您正在定义 RBAC 角色有权管理的用户组。默认管理员无法更改已应用的权限设置。默认情况下，已应用的权限适用于所有用户组。

当您进行*分配*时，您正在将 RBAC 角色分配给一个组，以便该用户组拥有 RBAC 管理员权限。

重要提示：

在“设置”权限下，RBAC 权限授予管理员用户完全访问权限，包括分配其自身权限的能力。仅将此访问权限授予您打算授予其操作 Endpoint Management 系统中所有内容的权限的用户。

本文包含以下部分：

- 管理员角色
- 支持角色
- 用户角色
- 使用 RBAC 配置角色

管理员角色

具有预定义管理员角色的用户可以访问或无法访问 XenMobile 中的以下功能。默认情况下，**授权访问**（自助服务门户除外）、**控制台功能**和**应用权限**已启用。

授权访问

管理员控制台访问	管理员可以访问 XenMobile 控制台上的所有功能。
自助服务门户访问权限	管理员没有自助服务门户访问权限。
共享设备注册员	管理员没有共享设备注册员访问权限。此功能适用于需要注册共享设备的用户。
远程支持访问权限	管理员拥有远程支持访问权限。*
公共 API 访问权限	管理员可以访问公共 API，以编程方式执行 XenMobile 控制台上可用的操作。这些操作包括管理证书、应用程序、设备、交付组和本地用户。
COSU 设备注册员	如果未通过注册配置文件配置此功能，则为管理员提供了一种注册专用 Android Enterprise 设备（也称为 COSU 设备）的方法。

* 远程支持使您的帮助台代表能够远程控制托管的 Android 移动设备。屏幕投射仅在 Samsung Knox 设备上受支持。远程支持不适用于群集本地 XenMobile Server 部署。自 January 1, 2019 起，新客户不再提供远程支持。现有客户可以继续使用该产品，但 Citrix 不提供增强功能或修复。

控制台功能

管理员对 XenMobile 控制台拥有不受限制的访问权限。

控制板	在登录 XenMobile 控制台后，**控制板**是管理员看到的第一个页面。**控制板**显示有关通知和设备的基本信息。	
报告	**分析 > 报告**页面提供预定义报告，可用于分析您的应用程序和设备部署。	
设备	**管理 > 设备**页面是用于管理用户设备的位置。您可以在此页面上添加单个设备，或导入设备预配文件以一次添加多个设备。	
本地用户和组	**管理 > 用户**页面是用于添加、编辑或删除本地用户和本地用户组的位置。	
注册	**管理 > 注册邀请**页面是用于管理如何邀请用户将其设备注册到 XenMobile 的位置。	
策略	**配置 > 设备策略**页面是用于管理设备策略（例如 VPN 和 Wi-Fi）的位置。	
应用程序	**配置 > 应用程序**页面是用于管理用户可以在其设备上安装的各种应用程序的位置。	
媒体	**配置 > 媒体**页面是用于管理用户可以在其设备上安装的各种媒体的位置。	

操作	**配置 > 操作**页面用于管理对触发事件的响应。	
注册配置文件	**配置 > 注册配置文件**页面用于配置注册配置文件（模式），以允许用户注册其设备。	
交付组	**配置 > 交付组**页面用于管理交付组及其关联的资源。	
设置	**设置**页面用于管理系统设置，例如客户端和服务器属性、证书和凭据提供程序。**重要提示：**这些设置包括 RBAC 权限。RBAC 权限授予管理员完全访问权限，包括分配其自身权限的能力。仅向您打算授予操作 Endpoint Management 系统中所有内容的权限的用户授予此访问权限。	
支持	**故障排除和支持**页面用于执行故障排除活动，例如运行诊断和生成日志。	

设备

管理员通过设置设备限制、设置和向设备发送通知、管理设备上的应用程序等方式，在整个控制台中访问设备功能。

完全擦除设备	擦除设备上的所有数据和应用程序，包括设备中的存储卡（如果有）。
清除限制	移除一个或多个设备限制。
选择性擦除设备	擦除设备中的所有企业数据和应用程序，同时保留个人数据和应用程序。
查看位置	查看设备位置并对设备设置地理限制。包括：定位设备、查看设备位置、跟踪设备、跟踪设备随时间变化的位置。

锁定设备	远程锁定设备，以便用户无法使用该设备。
解锁设备	远程解锁设备，以便用户可以使用该设备。
锁定容器	远程锁定设备上的企业容器。
解锁容器	远程解锁设备上的企业容器。
重置容器密码	重置企业容器密码。
启用 ASM DEP/绕过激活锁	当激活锁启用时，在受监管的 iOS 设备上存储绕过代码。如果您需要擦除设备，请使用此代码自动清除激活锁。
使设备响铃	远程使 Windows 设备以最大音量持续响铃 5 分钟。
重启设备	从 XenMobile 控制台重启 Windows 设备。
部署到设备	将应用程序、通知、限制等发送到设备。
编辑设备	更改设备上的设置。
向设备发送通知	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	将一组设备从文件导入到 XenMobile。
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 上，用户可以登录，但无法访问应用程序。
应用程序擦除	在 Android 上，此操作会删除用户的 XenMobile 帐户。在 iOS 上，此操作会删除用户访问 XenMobile 功能所需的加密密钥。
查看软件清单	查看设备上安装了哪些软件。

请求 AirPlay 镜像	请求开始 AirPlay 流式传输。
停止 AirPlay 镜像	停止 AirPlay 流式传输。
启用丢失模式	在 **管理 > 设备** 中，您可以将受监管设备置于丢失模式，以在锁定屏幕上阻止受监管设备。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** 中，您可以为已设置为丢失模式的设备禁用丢失模式。
操作系统更新设备	您可以将控制操作系统更新设备策略部署到设备。
关闭设备	从 XenMobile 控制台关闭 iOS 设备。
重启设备	从 XenMobile 控制台重启 iOS 设备。

本地用户和组

管理员在 XenMobile 的 **管理 > 用户** 页面上管理本地用户和本地用户组。

添加本地用户
删除本地用户
编辑本地用户
导入本地用户
导出本地用户
本地用户组
获取本地用户锁定 ID
删除本地用户锁定

注册

管理员可以添加和删除注册邀请、向用户发送通知，并将注册表导出为 .csv 文件。

添加/删除注册	添加或删除用户或用户组的注册邀请。
通知用户	向用户或用户组发送注册邀请。
导出注册邀请表	从“注册”页面收集注册信息并将其导出为 .csv 文件。

策略

添加/删除策略	添加或删除设备或应用程序策略。
编辑策略	更改设备或应用程序策略。
上传策略	上传设备或应用程序策略。
克隆策略	复制设备或应用程序策略。
禁用策略	禁用现有应用程序策略。
导出策略	从“设备策略”页面收集设备策略信息并将其导出到 .csv 文件。
分配策略	将设备策略分配给一个或多个交付组。

应用程序

管理员在 XenMobile 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	添加或删除公共应用商店应用或企业应用（非 MDX 启用）。
编辑应用商店或企业应用	更改公共应用商店应用或企业应用（非 MDX 启用）。
添加/删除 MDX、Web 和 SaaS 应用	向 XenMobile 添加或删除 MDX 启用应用、内部网络应用（Web 应用）或公共网络应用 (SaaS)。
编辑 MDX、Web 和 SaaS 应用	更改 XenMobile 中的 MDX 启用应用、内部网络应用（Web 应用）或公共网络应用 (SaaS)。

添加/删除类别	添加或删除应用可在 XenMobile Store 中显示的类别。
将公共/企业应用分配到交付组	将公共应用商店应用或 MDX 启用应用分配到交付组以进行部署。
将 MDX/WebLink/SaaS 应用分配到交付组	将 MDX 启用、无需单点登录 (WebLink) 或来自公共网络 (SaaS) 的应用分配到交付组。
导出应用表	从“应用程序”页面收集应用程序信息并将其导出到 .csv 文件。

注意：

当您选择 **控制台功能 > 应用程序** 时，API 终结点 `GET <https://XMS_IP:4443/controlpoint/rest/ad>` 会按设计返回 LDAP 信息。

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图书
将公共/企业图书分配给交付组
编辑应用商店或企业图书

操作

添加/删除操作	添加或删除由触发器（事件、设备或用户属性或已安装的应用程序名称）和关联响应定义的操作。
编辑操作	更改由触发器（事件、设备或用户属性或已安装的应用程序名称）和关联响应定义的操作。
将操作分配给交付组	将操作分配给交付组，以便部署到用户设备。

导出操作	从“操作”页面收集操作信息并将其导出到 .csv 文件。

交付组

管理员从**配置 > 交付组**页面管理交付组。

添加/删除交付组	创建或删除交付组，此操作会添加指定的用户以及可选的策略、应用程序和操作。
编辑交付组	更改现有交付组，此操作会修改用户以及可选的策略、应用程序和操作。
部署交付组	使交付组可供使用。
导出交付组	从“交付组”页面收集交付组信息并将其导出到 .csv 文件。

注册配置文件

管理注册配置文件。

添加/删除注册配置文件
编辑注册配置文件
将注册配置文件分配给交付组

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。**重要提示：**此权限授予管理员完全访问权限，包括分配其自身权限的能力。仅将此访问权限授予您打算授予其操作 Endpoint Management 系统中所有内容的权限的用户。

LDAP	管理一个或多个符合 LDAP 的目录（例如 Active Directory），以导入组、用户帐户和相关属性。
许可证	适用于本地 XenMobile Server。管理您的 Citrix® 许可证。
注册	为用户和自助服务门户启用注册安全模式。
版本管理	查看当前安装的版本。包括：版本管理更新
证书	编辑 APNS 证书、证书 SSL 侦听器
通知模板	创建通知模板，用于自动化操作、注册以及向用户发送标准通知消息。
工作流	管理用户帐户的创建、审批和删除，以用于应用程序配置。
凭据提供程序	添加一个或多个有权颁发设备证书的凭据提供程序。凭据提供程序控制证书格式以及续订或吊销证书的条件。
PKI 实体	管理公钥基础结构实体（通用、Microsoft 证书服务或自由裁量 CA）。
测试 PKI 连接	使用“**设置 > PKI 实体**”页面上的“**测试连接**”按钮，确保服务器可访问。
客户端属性	管理用户设备上的各种属性，例如密码类型、强度或过期时间。
客户端支持	设置用户联系支持服务的方式（电子邮件、电话或支持票证电子邮件）。
客户端品牌	为 XenMobile Store 创建自定义商店名称和默认商店视图。添加一个自定义徽标，该徽标将显示在 XenMobile Store 或 Secure Hub 中。
运营商短信网关	设置运营商短信网关，以配置 XenMobile 通过运营商短信网关发送的通知。

通知服务器	设置 SMTP 网关服务器以向用户发送电子邮件。
ActiveSync 网关	通过规则和属性管理用户对用户和设备的访问。
Apple 部署计划	将 Apple 部署计划帐户添加到 XenMobile。
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 和其他 Exchange ActiveSync 设备并执行操作。
思杰网关	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	设置确定设备不合规并因此拒绝访问网络的条件。
三星 Knox	启用或禁用 XenMobile 查询 Samsung Knox 证明服务器 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。
系统日志	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 添加虚拟应用程序和桌面。
思杰文件	将 XenMobile 与企业帐户结合使用时：配置设置以连接到 ShareFile 帐户和管理员服务帐户以管理用户帐户。需要现有的 Citrix Files 域和管理员凭据。将 XenMobile 与存储区域连接器结

	合使用时：配置 XenMobile 以指向存储区域连接器中定义的网络共享和 SharePoint 位置。
体验改进计划	适用于本地 XenMobile Server。选择加入或退出向 Citrix 发送匿名统计信息和使用情况信息。
微软 Azure	适用于本地 XenMobile Server。将 XenMobile 与 Microsoft Azure 集成。
Android 企业版	配置 Android Enterprise 服务器设置。
身份提供程序 (IdP)	配置身份提供程序。
XenMobile 工具	访问 XenMobile 工具页面。
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，并配置陷阱间隔和阈值。

支持

管理员可以执行各种支持任务。

Citrix Gateway 连接检查	对 Citrix Gateway 按 IP 地址执行各种连接检查。需要用户名和密码。
XenMobile 连接检查	对选定的 XenMobile 功能（例如数据库、DNS 或 Google Plan）执行连接检查。
创建支持包	适用于本地 XenMobile Server。创建一个文件发送给 Citrix 支持以进行故障排除。包含系统信息、日志、数据库信息、核心信息、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、管理员审计和用户审计的日志文件详细信息。

群集信息	适用于本地 XenMobile Server。访问有关群集环境中每个节点的信息。
垃圾回收	适用于本地 XenMobile Server。访问有关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中填充用户或设备属性数据。配置单个策略，将其部署到大量用户，并为每个目标用户显示用户特定的值。
PKI 配置	导入和导出 PKI 配置信息。
APNS 签名实用程序	提交 Apple 推送网络签名 (APNs) 证书请求，或上传适用于 iOS 的 Secure Mail APNs 证书。
Citrix 洞察服务	将日志上传到 Citrix Insight Services (CIS) 以获取各种问题的帮助。
适用于 Exchange ActiveSync 状态的设备 Citrix Gateway connector™	根据设备的 ActiveSync ID，查询 XenMobile 以获取发送到适用于 Exchange ActiveSync 的 Citrix Gateway connector 的设备状态。
匿名化和去匿名化	适用于本地 XenMobile Server。在 XenMobile 中创建支持包时，敏感的用户、服务器和网络数据默认匿名化。您可以在**高级**下的**支持 > 匿名化和去匿名化**中更改此行为。
日志设置	自定义日志级别或添加自定义日志记录器。

限制组访问

管理员用户可以将权限应用于所有用户组。

支持角色

具有支持角色的用户可以访问远程支持。他们的权限默认适用于所有用户，并且他们无法编辑此设置。

用户角色

具有用户角色的用户对 XenMobile 具有以下受限访问权限。

授权访问

自助服务门户	用户只能访问 XenMobile 中的自助服务门户。

控制台功能

用户对 XenMobile 控制台具有以下受限访问权限。

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（如果设备有）。
选择性擦除设备	擦除设备上的所有企业数据和应用程序，保留个人数据和应用程序。
查看位置	查看设备位置并设置地理限制。包括：定位设备、查看设备位置、跟踪设备、跟踪设备位置随时间变化
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	在启用激活锁时，在受监管的 iOS 设备上存储旁路代码。如果需要擦除设备，请使用此代码自动清除激活锁。
响铃设备	远程以最大音量使 Windows 设备响铃 5 分钟。
重启设备	重启 Windows 设备。
查看软件清单	查看设备上安装了哪些软件。

注册

添加/删除注册	为用户或用户组添加或删除注册邀请。
通知用户	向用户或用户组发送注册邀请。

限制组访问

对于所有四个默认角色，此权限默认设置，可应用于所有用户组。您无法编辑此角色。

使用 RBAC 配置角色

XenMobile 中的基于角色的访问控制 (RBAC) 功能允许您将预定义角色或权限集分配给用户和组。这些权限控制用户对系统功能的访问级别。

XenMobile 实现了四种默认用户角色，以逻辑方式分离对系统功能的访问：

- **管理员：** 授予完整的系统访问权限。
- **支持：** 授予远程支持访问权限。
- **用户：** 供可以注册设备和访问自助服务门户的用户使用。

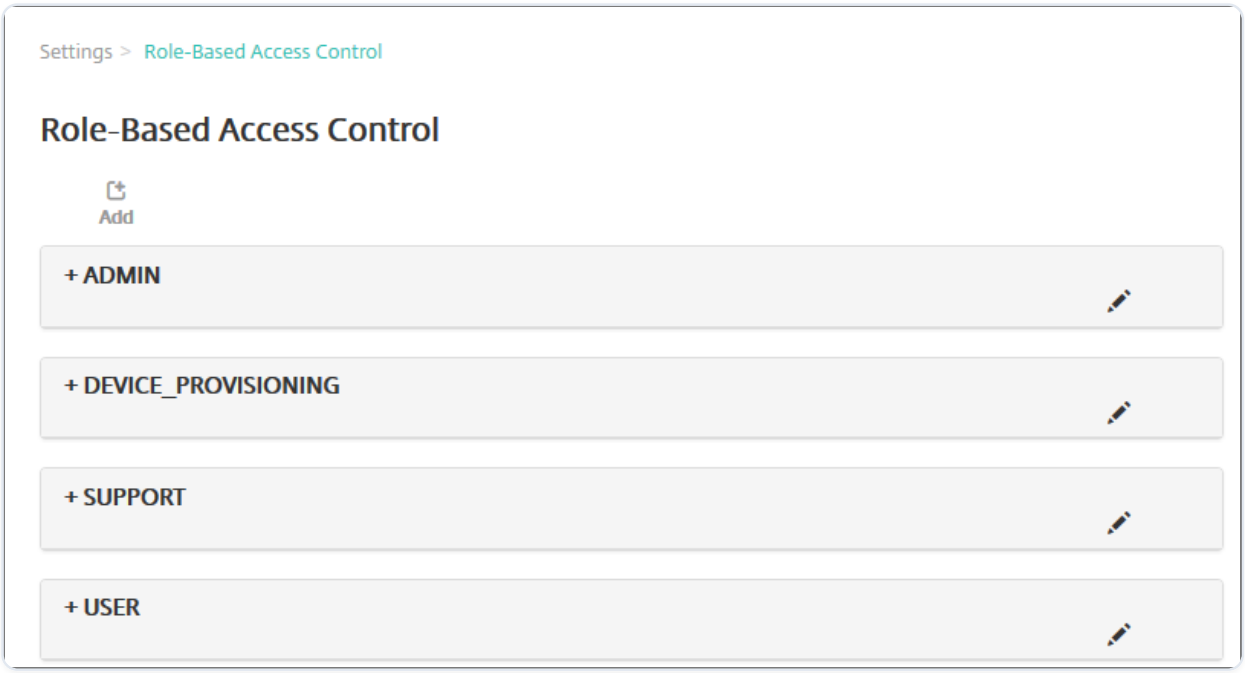
您还可以使用默认角色作为模板，自定义这些模板以创建用户角色。您可以为角色分配权限，以访问超出默认角色定义的功能的特定系统功能。

角色可以分配给本地用户（在用户级别）或 Active Directory 组（该组中的所有用户都具有相同的权限）。如果用户属于多个 Active Directory 组，则所有权限将合并以定义该用户的权限。例如，假设 ADGroupA 用户可以定位经理设备，ADGroupB 用户可以擦除员工设备。在这种情况下，属于这两个组的用户可以定位和擦除经理和员工的设备。

> **注意：**
>
> 本地用户可能只分配有一个角色。
>
> 您可以使用 XenMobile 中的 RBAC 功能执行以下操作：

- 创建角色。
- 将组添加到角色。
- 将本地用户与角色关联。

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，其中显示了四个默认用户角色以及您之前添加的任何角色。



如果您单击角色旁边的加号 (+)，该角色将展开以显示该角色的所有权限，如下图所示。

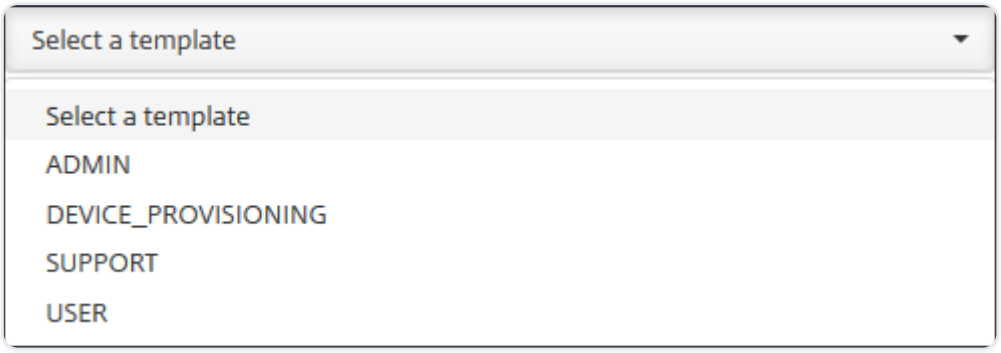
2. 单击 **添加** 以添加新的用户角色。要编辑角色，请单击现有角色右侧的铅笔图标。要删除角色，请单击角色右侧的垃圾桶图标。您不能删除默认用户角色。

   - 当您单击 **添加** 或铅笔图标时，将显示 **添加角色** 或 **编辑角色** 页面。
   - 当您单击垃圾桶图标时，将出现一个确认对话框。单击 **删除** 以删除选定的角色。

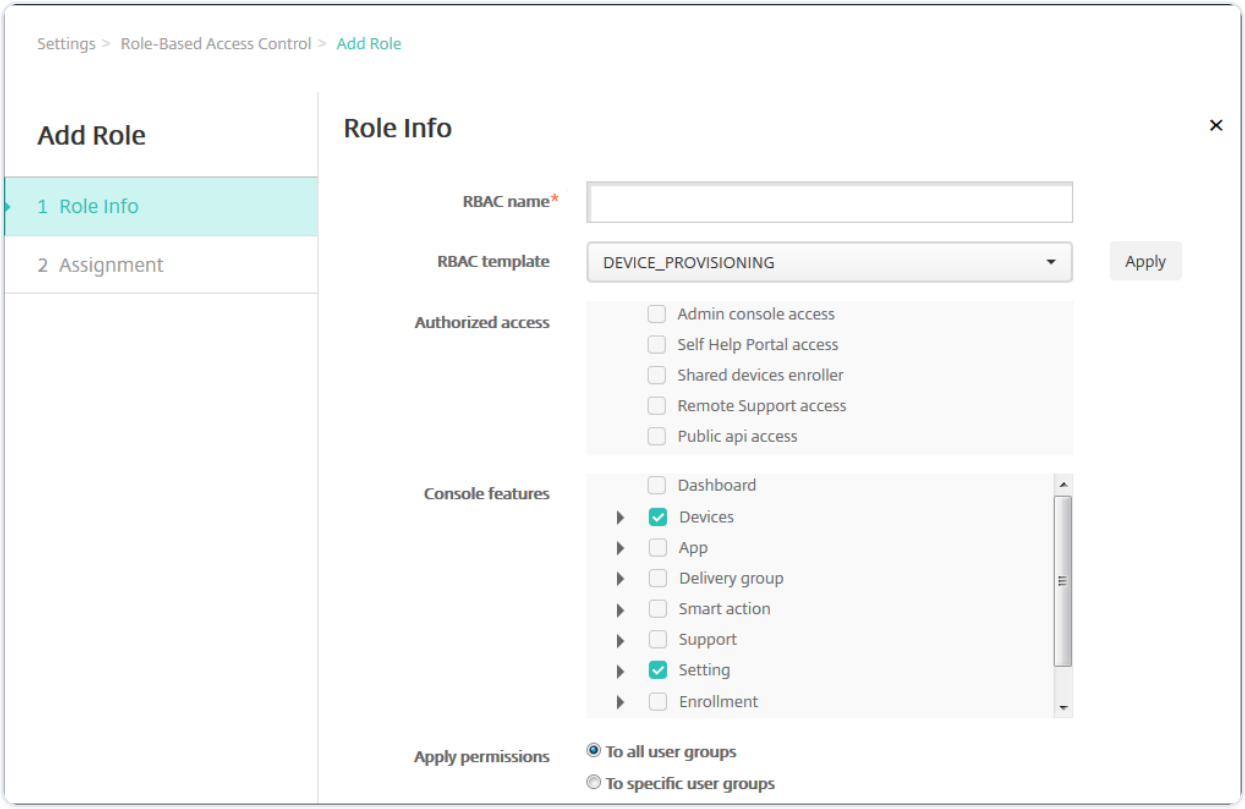
3. 输入以下信息以创建或编辑用户角色：

   - **RBAC 名称：** 为新用户角色输入一个描述性名称。您不能更改现有角色的名称。
   - **RBAC 模板：** （可选）单击一个模板作为新角色的起点。如果您正在编辑现有角色，则无法选择模板。

RBAC 模板是默认用户角色。它们定义了与该角色关联的用户对系统功能的访问权限。选择 RBAC 模板后，您可以在 **授权访问** 和 **控制台功能** 字段中看到与该角色关联的所有权限。使用模板是可选的。您可以直接在 **授权访问** 和 **控制台功能** 字段中选择要分配给角色的选项。

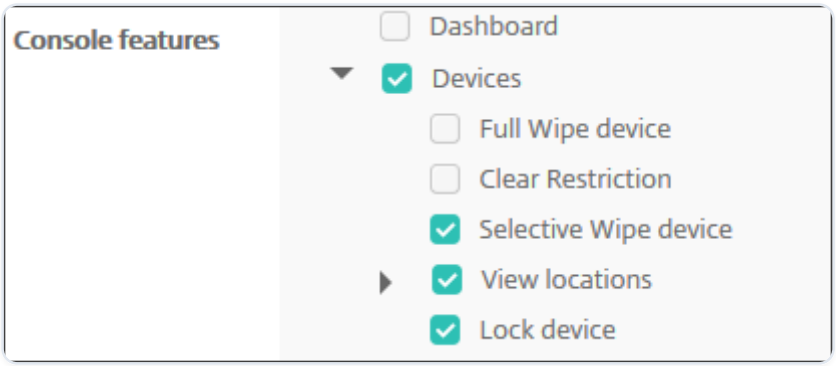


4. 单击选定 **RBAC 模板** 字段旁边的 **应用** 以使用预定义的访问和功能权限填充 **授权访问** 和 **控制台功能**。



5. 在 **授权访问** 和 **控制台功能** 中选择和清除复选框以自定义角色。

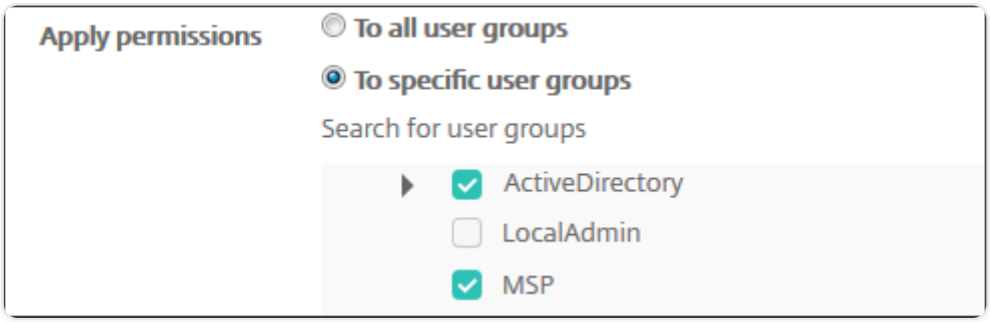
如果您单击控制台功能旁边的三角形，将显示该功能特有的权限，您可以选择和清除这些权限。单击顶级复选框将禁止访问该控制台区域。选择顶级以下的单个选项以启用这些选项。例如，在下图中，分配给该角色的用户不会显示 **完全擦除设备** 和 **清除限制** 选项。选中的选项会显示。



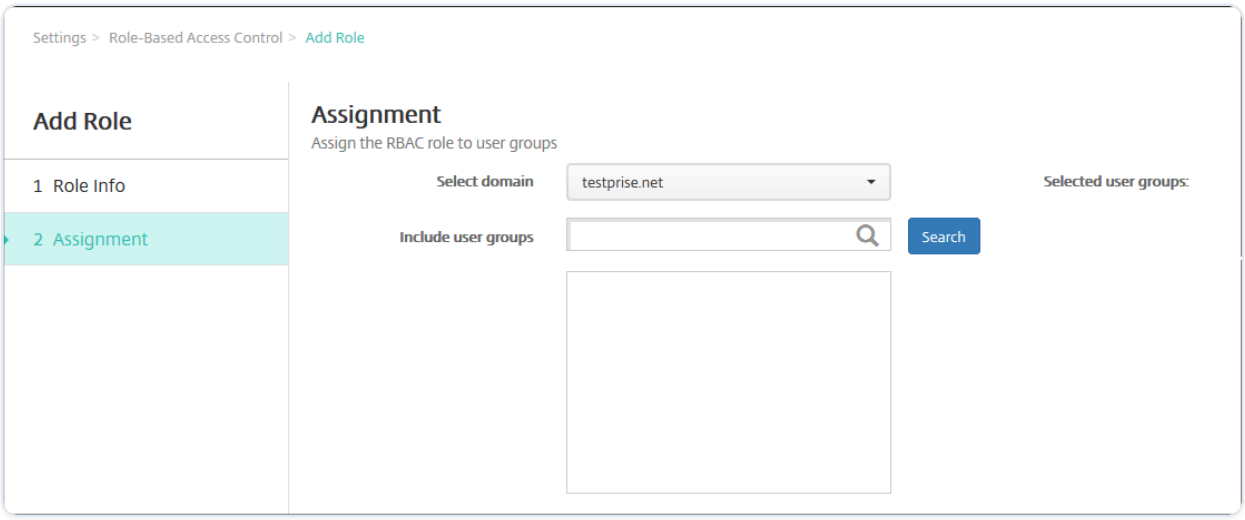
6. **应用权限：** 选择一个或多个用户组，以限制管理员可以管理的组。如果单击**到特定用户组**，将显示一个组列表，您可以从中选择一个或多个组。

   例如，如果 RBAC 管理员对 ActiveDirectory 和 MSP 用户组具有权限：

   - 管理员只能访问 ActiveDirectory 组、MSP 组或这两个组中的用户的相关信息。
   - 管理员无法查看任何其他本地用户或 AD 用户。管理员可以查看属于这些组的子组成员的用户。
   - 管理员可以向以下对象发送邀请：
     - 权限组及其子组
     - 属于权限组及其子组的成员的用户

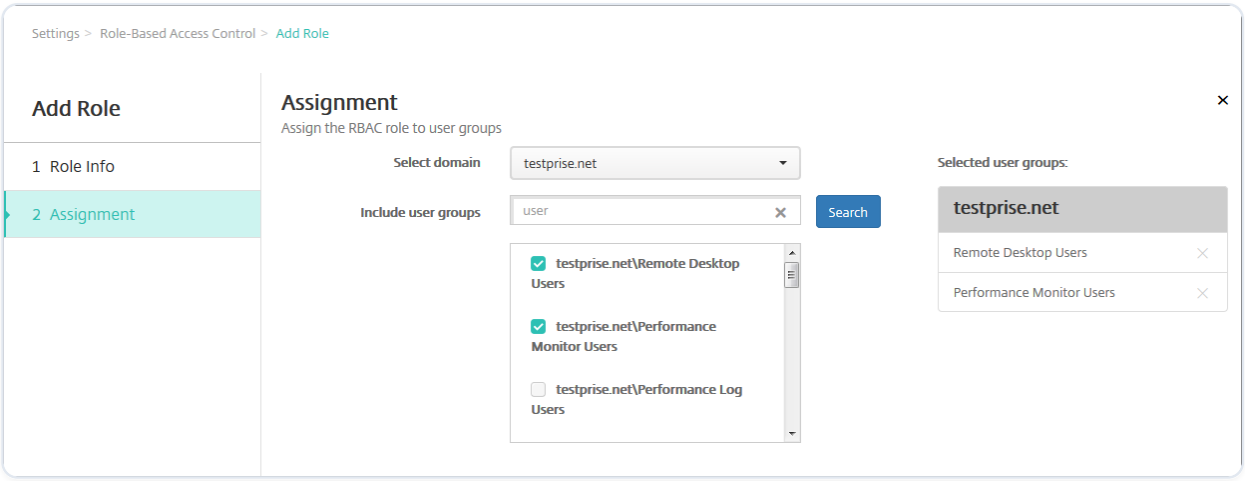


7. 单击**下一步**。此时将显示**分配**页面。



8. 输入以下信息以将角色分配给用户组。

   - **选择域：** 在下拉列表中单击一个域。
   - **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包含该名称的组。
   - 在显示的列表中，选择要为其分配角色的用户组。选择用户组后，该组将显示在**选定的用户组**列表中。



> **注意：**
>
> 要从**选定的用户组**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

您可以在 XenMobile® 中使用通知来实现以下目的：

- 与特定用户组就多项系统相关功能进行通信。您还可以将这些通知定向到特定用户。例如，所有使用 iOS 设备的用户、设备不合规的用户、拥有员工自有设备的用户等。
- 注册用户及其设备。
- 在满足特定条件时自动通知用户（使用自动化操作）。例如：
  - 当用户设备因合规性问题即将被公司域阻止时。
  - 当设备已被越狱或 Root 时

有关自动化操作的详细信息，请参阅自动化操作。

要使用 XenMobile 发送通知，您必须配置网关和通知服务器。您可以在 XenMobile 中设置通知服务器，以配置简单邮件传输协议 (SMTP) 和短消息服务 (SMS) 网关服务器，从而向用户发送电子邮件和文本 (SMS) 通知。您可以使用通知通过两种不同的通道发送消息：SMTP 或 SMS。

- SMTP 是一种面向连接的、基于文本的协议，邮件发送方通过发出命令字符串并提供必要数据（通常通过传输控制协议 (TCP) 连接）与邮件接收方进行通信。SMTP 会话由 SMTP 客户端（发送消息的人）发出的命令和 SMTP 服务器的相应响应组成。
- SMS 是电话、Web 或移动通信系统中的文本消息服务组件。SMS 使用标准化通信协议，使固定电话或移动电话设备能够交换短文本消息。

您还可以在 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 网关向电信网络发送或从电信网络接收 SMS 传输。这些基于文本的消息使用标准化通信协议，允许固定电话或移动电话设备交换短文本消息。

先决条件

- 在配置 SMS 网关之前，请咨询您的系统管理员以确定服务器信息。了解 SMS 服务器是托管在内部公司服务器上，还是作为托管电子邮件服务的一部分，这一点很重要。如果是后者，您需要从服务提供商的网站获取信息。
- 配置 SMTP 通知服务器以向用户发送消息。如果服务器托管在内部服务器上，请联系您的系统管理员获取配置信息。如果服务器是托管电子邮件服务，请在服务提供商的网站上查找相应的配置信息。
- 您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。这两个通信通道都只允许一个活动配置。
- 从位于网络 DMZ 中的 XenMobile 打开端口 25，使其指向内部网络上的 SMTP 服务器。这使 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，单击“**通知服务器**”。此时将显示“**通知服务器**”页面。

   通知服务器页面图像(/en-us/xenmobile/server/media/notification-server.png)
3. 单击“**添加**”。此时将显示一个菜单，其中包含用于配置 SMTP 服务器或 SMS 网关的选项。

   通知服务器添加(/en-us/xenmobile/server/media/settings-notifications-notification-server-add.png)

- 要添加 SMTP 服务器，请单击“**SMTP 服务器**”，然后参阅添加 SMTP 服务器以了解配置此设置的步骤。
- 要添加 SMS 网关，请单击“**SMS 网关**”，然后参阅添加 SMS 网关以了解配置此设置的步骤。

添加 SMTP 服务器

通知服务器添加 SMTP(/en-us/xenmobile/server/media/settings-notifications-notification-server-add-smtp.png)

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。主机名必须是完全限定域名 (FQDN) 或 IP 地址。
- **安全通道协议：** 在下拉列表中单击 **SSL**、**TLS** 或 **None**，以选择服务器使用的安全通道协议（如果服务器配置为使用安全身份验证）。默认值为 **None**。
- **SMTP 服务器端口：** 键入 SMTP 服务器使用的端口。默认情况下，端口设置为 25。如果 SMTP 连接使用 SSL 安全通道协议，则端口设置为 465。
- **身份验证：** 选择 **ON** 或 **OFF**。默认值为 **OFF**。
- 如果启用**身份验证**，请配置以下设置：
  - **用户名：** 键入用于身份验证的用户名
  - **密码：** 键入身份验证用户的密码。

> **重要提示：**
>
> 要将 OAuth 与 Microsoft Exchange Online 结合使用，您必须首先 在 Microsoft Entra ID 中注册您的应用程序。注册后，启用**身份验证**和 **Microsoft Exchange Online OAuth 2.0**。

- 如果启用**身份验证**和 **Microsoft Exchange Online OAuth 2.0**，请配置以下设置：
  - **用户名：** 键入用于身份验证的用户名。
  - **租户 ID：** 键入 Microsoft Entra ID 目录的租户 ID。
  - **客户端 ID：** 键入已注册应用程序的客户端（应用程序）ID。您可以在 Azure 门户 > 您的已注册应用程序 > **应用程序（客户端）ID** 中找到它。

  - **客户端密码：** 键入已注册应用程序的客户端密码。您可以在 Azure 门户 > 您的已注册应用程序 > **证书和密码** 中找到它。

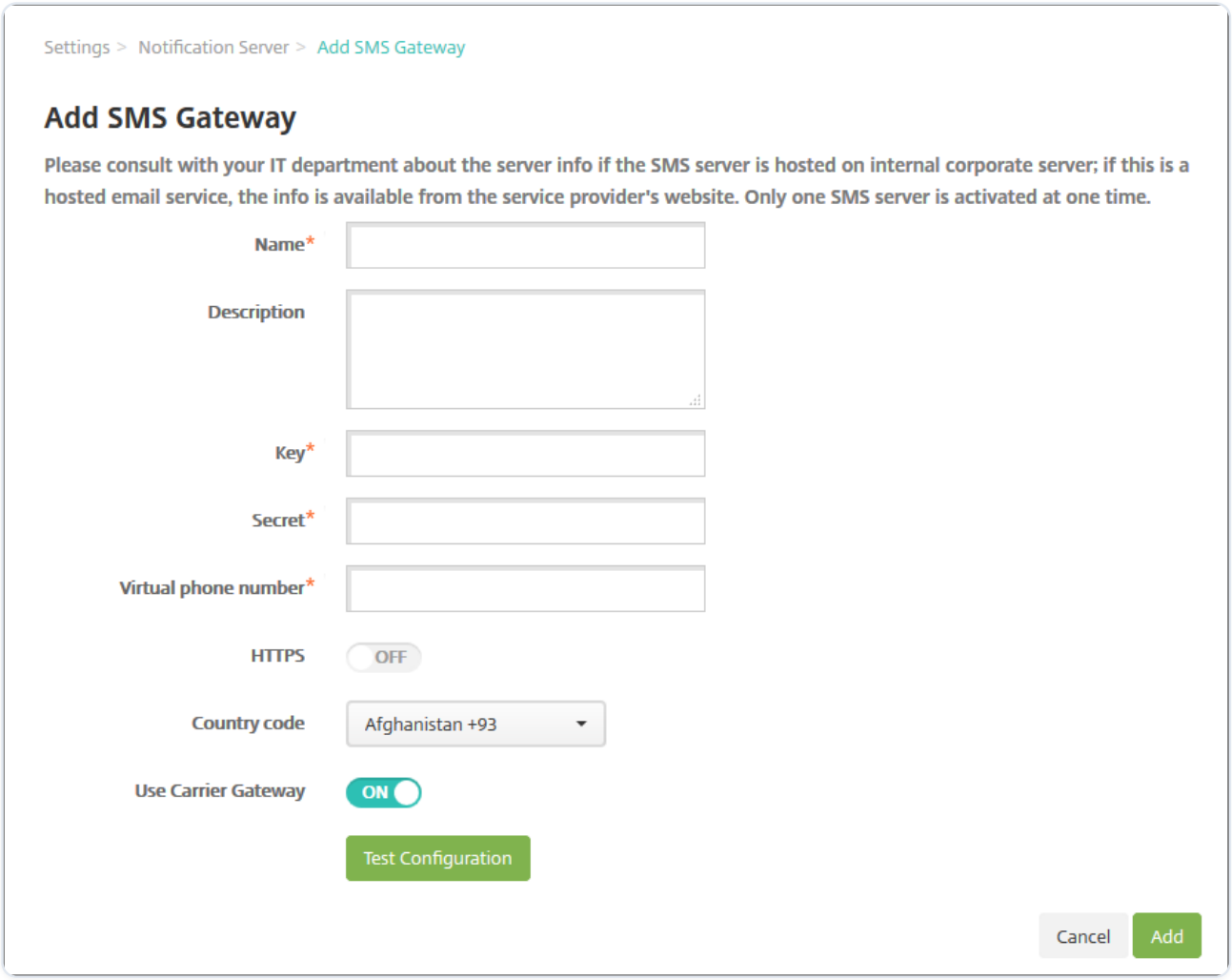
- **Microsoft 安全密码身份验证 (SPA)：** 如果 SMTP 服务器正在使用 SPA，请单击 **ON**。默认值为 **OFF**。
- **发件人姓名**：键入客户端从此服务器收到通知电子邮件时在“**发件人**”框中显示的名称。例如，公司 IT。
- **发件人电子邮件**：键入当电子邮件收件人回复 SMTP 服务器发送的通知时使用的电子邮件地址。

2. 单击“**测试配置**”以发送测试电子邮件通知。
3. 展开“**高级设置**”，然后配置以下设置：

   - **SMTP 重试次数**：键入从 SMTP 服务器发送失败邮件的重试次数。默认值为 5。
   - **SMTP 超时**：键入发送 SMTP 请求时等待的持续时间（以秒为单位）。如果邮件发送因超时而持续失败，请增加此值。减少此值时请谨慎；这可能会增加超时和未送达邮件的数量。默认值为 30 秒。
   - **SMTP 收件人最大数量**：键入 SMTP 服务器发送的每封电子邮件的最大收件人数。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。如果您还没有用于 Nexmo 消息传递的帐户，请访问其网站创建一个。

1. 配置以下设置：

   - **名称**：键入 SMS 网关配置的名称。此字段为必填项。
   - **描述**：（可选）键入配置的描述。
   - **密钥**：输入系统管理员在激活帐户时提供的数字标识符。此字段为必填项。
   - **密钥**：输入系统管理员提供的密钥，该密钥用于在密码丢失或被盗时访问您的帐户。此字段为必填项。

- **虚拟电话号码：** 此字段用于向北美电话号码（带有 +1 前缀）发送消息时。您必须输入 Nexmo 虚拟电话号码，并且此字段中只能使用数字。您可以在 Nexmo 网站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。默认设置为 **OFF**。

> **重要提示：**
>
> 将 HTTPS 保持设置为 **ON**，除非您收到 Citrix 支持的指导将其设置为 **OFF**。

- **国家/地区代码：** 单击下拉列表中的默认 SMS 国家/地区代码前缀，以用于您组织中的收件人。此字段始终以 + 符号开头。默认设置为 **Afghanistan +93**。

2. 单击 **测试配置** 以使用当前配置发送测试消息。连接错误（例如身份验证或虚拟电话号码错误）会立即检测到并显示。消息的接收时间与手机之间发送消息的时间相同。
3. 单击 **添加**。

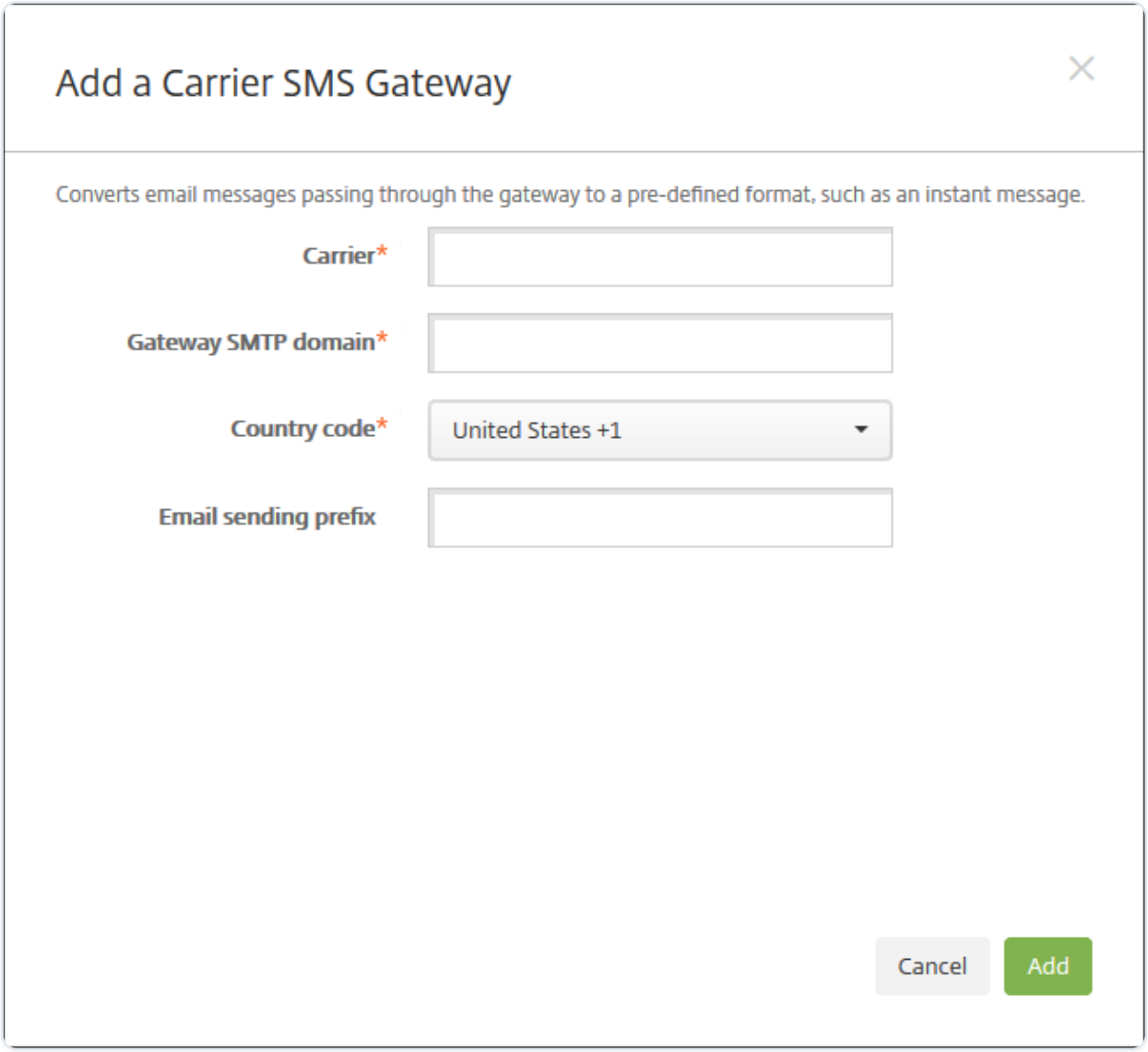
添加运营商 SMS 网关

您可以在 XenMobile 中设置运营商 SMS 网关，以配置通过运营商 SMS 网关发送的通知。运营商使用短消息服务 (SMS) 网关向电信网络发送或从电信网络接收 SMS 传输。这些基于文本的消息使用标准化通信协议，允许固定电话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。**设置** 页面随即显示。
2. 在 **通知** 下，单击 **运营商 SMS 网关**。**运营商 SMS 网关** 页面随即打开。

   通知服务器添加 SMS 网关(/en-us/xenmobile/server/media/settings-notifications-carrier-sms-gateway.png)
3. 执行以下操作之一：

   - 点击“**检测**”以自动发现网关。将出现一个对话框，指示未检测到新运营商，或列出在已注册设备中检测到的新运营商。
   - 点击“**添加**”。将出现“**添加运营商短信网关**”对话框。



注意：

XenMobile 仅支持 Nexmo 短信。如果您还没有用于 Nexmo 短信的帐户，请访问其网站创建一个。

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：** 在下拉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. 点击“**添加**”以添加新运营商，或点击“**取消**”以不添加新运营商。

创建和更新通知模板

您可以在 XenMobile 中创建或更新通知模板，以用于自动化操作、注册以及发送给用户的标准通知消息。您可以配置通知模板，以通过三种不同的渠道发送消息：Secure Hub、SMTP 或 SMS。

XenMobile 包含许多预定义的通知模板，这些模板反映了 XenMobile 自动响应系统中每个设备的各种不同事件类型。

> **注意：**
>
> 如果您计划使用 SMTP 或 SMS 通道向用户发送通知，则必须先设置这些通道，然后才能激活它们。如果尚未设置通道，XenMobile 会在您添加通知模板时提示您设置通道。

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。

   通知模板配置页面图像(/en-us/xenmobile/server/media/settings-notification-templates.png)

添加通知模板

1. 单击“**添加**”。如果尚未设置 SMS 网关或 SMTP 服务器，则会显示有关使用 SMS 和 SMTP 通知消息。您可以选择现在设置 SMTP 服务器或 SMS 网关，也可以稍后设置。

   如果您选择现在设置 SMS 或 SMTP 服务器设置，则会重定向到“**设置**”页面上的“**通知服务器**”页面。设置完要使用的通道后，您可以返回“**通知模板**”页面以继续添加或修改通知模板。

   > **重要提示：**
   >
   > 如果您选择稍后设置 SMS 或 SMTP 服务器设置，则在添加或编辑通知模板时将无法激活这些通道，这意味着这些通道将无法用于发送用户通知。

2. 配置以下设置：

   - **名称：**键入模板的描述性名称。
   - **描述：**键入模板的描述。
   - **类型：**在下拉列表中单击通知类型。仅显示所选类型支持的通道。只允许一个 APNS 证书过期模板，这是一个预定义模板。这意味着您无法添加此类型的新模板。

> **注意：**
>
> 对于某些模板类型，类型下方会显示“支持手动发送”字样。这意味着该模板在“**控制板**”和“**设备**”页面上的“**通知**”列表中可用，可让您手动向用户发送通知。在任何通道的“主题”或“消息”字段中使用以下宏的任何模板中，均不支持手动发送：
>
> - ${outofcompliance.reason(allowlist_blocklist_apps_name)}
> - ${outofcompliance.reason(smg_block)}

3. 在 **通道** 下，配置将用于此通知的每个通道的信息。您可以选择任何或所有通道。您选择的通道取决于您希望如何发送通知：

   - 如果您选择 **Secure Hub**，则只有 iOS 和 Android 设备会收到通知，通知会显示在设备的通知托盘中。
   - 如果您选择 **SMTP**，大多数用户会收到消息，因为他们已使用其电子邮件地址注册。
   - 如果您选择 **SMS**，则只有使用带 SIM 卡的设备的用户才会收到通知。

   安全中心：

   - **激活：** 单击以启用通知通道。
   - **消息：** 键入要发送给用户的消息。如果您正在使用 Secure Hub，则此字段为必填项。有关在消息中使用宏的信息，请参阅宏。
   - **声音文件：** 在下拉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。

     只有在设置 SMTP 服务器后，才能激活 SMTP 通知。
   - **发件人：** 键入通知的可选发件人，可以是姓名、电子邮件地址或两者兼有。
   - **收件人：** 此字段包含一个预构建的宏，适用于除 Ad Hoc 通知之外的所有通知，以确保通知发送到正确的 SMTP 收件人地址。Citrix 建议您不要修改模板中的宏。除了用户之外，您还可以通过添加以分号 (;) 分隔的地址来添加收件人（例如，公司管理员）。要发送 Ad Hoc 通知，您可以在此页面上输入特定的收件人，或者您可以从 **管理 > 设备** 页面选择设备并从那里发送通知。有关详细信息，请参阅设备。
   - **主题：** 为通知键入描述性主题。此字段为必填项。
   - **消息：** 键入要发送给用户的消息。有关在消息中使用宏的信息，请参阅宏。

短信：

- **激活：** 单击以启用通知通道。

  只有在设置 SMTP 服务器后，才能激活 SMTP 通知。

- **收件人：** 此字段包含一个预构建宏，适用于除即席通知之外的所有通知，以确保通知发送到正确的短信收件人地址。Citrix 建议您不要修改模板中的宏。要发送即席通知，您可以输入特定的收件人，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。此字段为必填项。有关在消息中使用宏的信息，请参阅宏。

4. 单击“**添加**”。正确配置所有通道后，它们将按此顺序显示在“**通知模板**”页面上：SMTP、短信和 Secure Hub。任何未正确配置的通道将显示在已正确配置的通道之后。

编辑通知模板

1. 选择一个通知模板。将显示该模板的编辑页面，您可以在其中更改除“**类型**”字段之外的所有内容，并激活或停用通道。
2. 单击“**保存**”。

删除通知模板

您只能删除您添加的通知模板。您无法删除预定义的通知模板。

1. 选择现有通知模板。
2. 单击“**删除**”。将显示确认对话框。
3. 点击 **删除** 以删除通知模板，或点击 **取消** 以取消删除通知模板。

设备

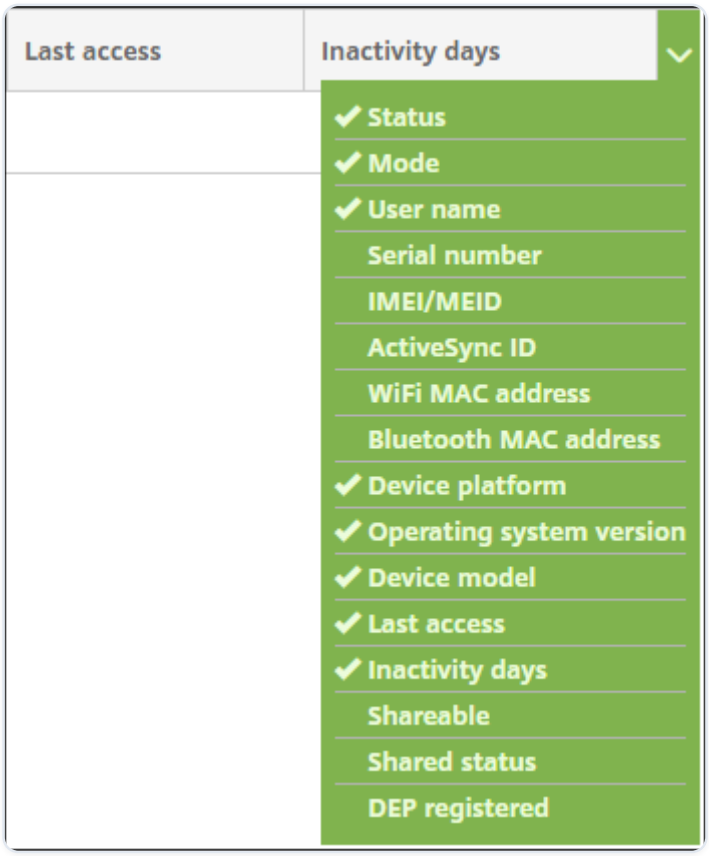
Citrix XenMobile® 可以在单个管理控制台中调配、管理、保护和清点各种设备类型。

XenMobile Server 数据库存储移动设备列表。唯一的序列号或国际移动设备识别码 (IMEI)/移动设备标识符 (MEID) 可唯一标识每台移动设备。要使用您的设备填充 XenMobile 控制台，您可以手动添加设备或从文件中导入设备列表。有关设备调配文件格式的详细信息，请参阅本文后面的 设备调配文件格式。

XenMobile 控制台中的“**设备**”页面列出了每台设备和以下信息：

- **状态：** 图标指示设备是否已越狱、是否受管理、Active Sync Gateway 是否可用以及部署状态。
- **模式：** 设备模式是 MDM、MAM 还是两者兼有。
- 有关设备的其他信息，例如“**用户名**”、“**设备平台**”、“**操作系统版本**”、“**设备型号**”、“**上次访问**”和“**非活动天数**”。这些标题是默认显示的。

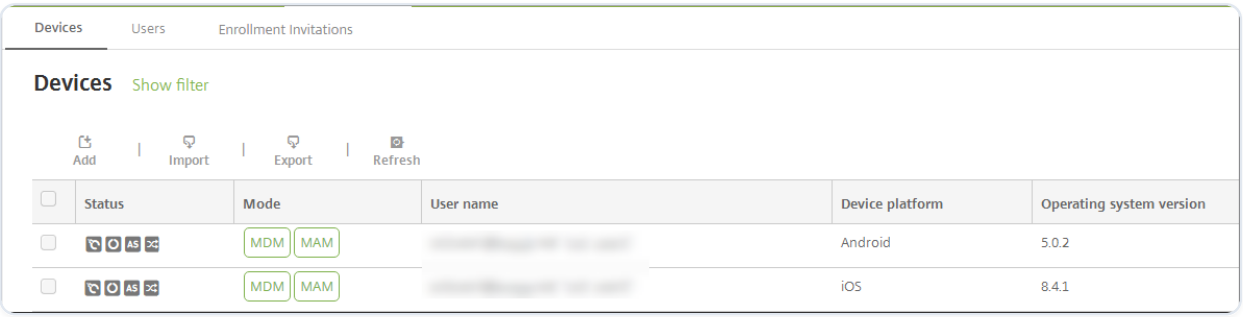
要自定义“**设备**”表，请单击最后一个标题上的向下箭头。然后，选择要在表中看到的其他标题或清除要删除的任何标题。



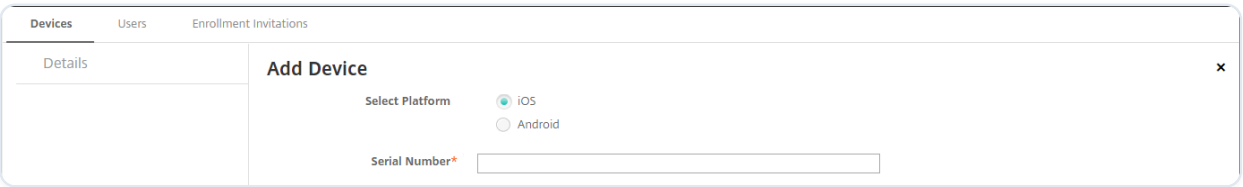
您可以手动添加设备、从设备调配文件导入设备、编辑设备详细信息、执行安全操作以及向设备发送通知。您还可以将所有设备表数据导出到 .csv 文件以创建自定义报告。服务器会导出所有设备属性。如果应用筛选器，XenMobile 会在创建 .csv 文件时使用这些筛选器。

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. 配置这些设置：

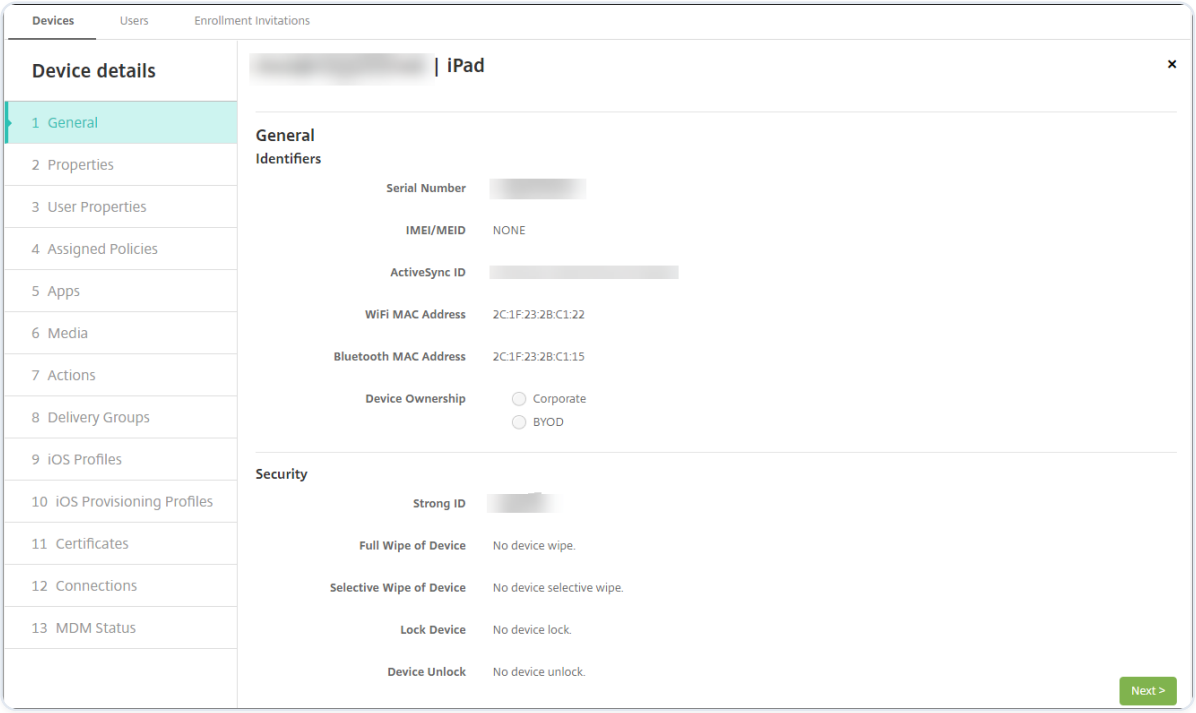
   - **选择平台：**单击 **iOS** 或 **Android**。
   - **序列号：**键入设备序列号。
   - **IMEI/MEID：**（可选）仅适用于 Android 设备，键入设备的 IMEI/MEID 信息。

4. 单击 **Add**。“**设备**”表显示，设备已添加到列表底部。选择您添加的设备，然后在出现的菜单中单击 **Edit** 以查看并确认设备详细信息。

> **注意：**
>
> 当您选中设备旁边的复选框时，选项菜单将显示在设备列表上方。当您单击列表中的其他任何位置时，选项菜单将显示在列表的右侧。

   - 以企业 (XME) 或 MDM 模式配置的 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。
  - 将本地用户分配到本地组。
  - 交付组与本地组关联。
- 如果使用 Active Directory：
  - 交付组与 Active Directory 组关联。



5. “**常规**”页面列出了设备**标识符**，例如序列号、ActiveSync ID 和平台类型的其他信息。对于“**设备所有权**”，请选择“**公司**”或“**BYOD**”。

   “**常规**”页面还列出了设备**安全**属性，例如强 ID、锁定设备、激活锁绕过以及平台类型的其他信息。“**完全擦除设备**”字段包含用户 PIN 码。设备擦除后，用户必须输入该代码。如果用户忘记了该代码，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个属性。有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

   添加属性时，它最初会显示在您添加它的类别下。单击“**下一步**”并返回“**属性**”页面后，该属性将显示在相应的列表中。

   要删除属性，请将鼠标悬停在列表项上，然后单击右侧的“**X**”。XenMobile 会立即删除该项目。

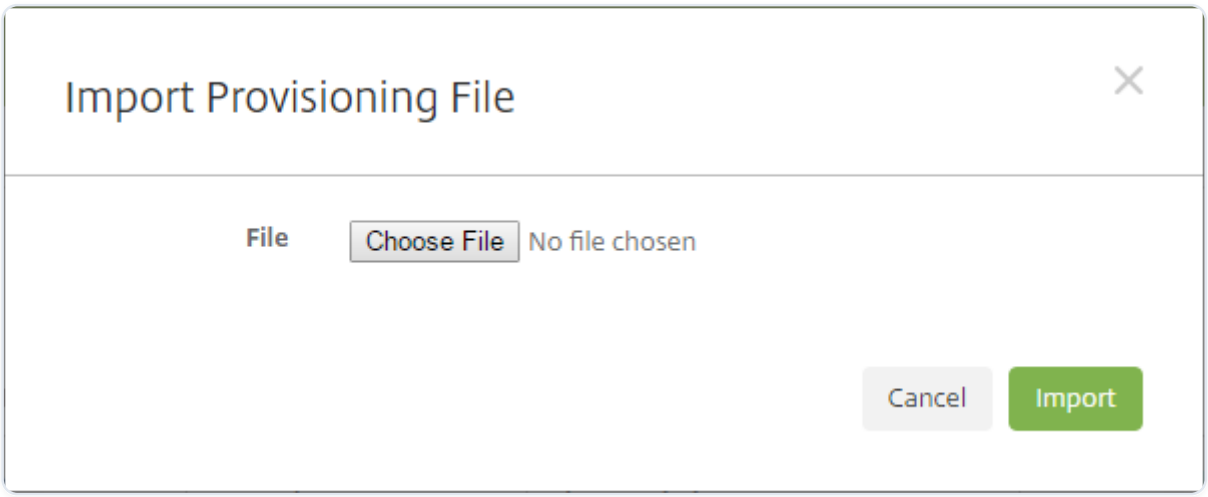
7. 其余的“**设备详细信息**”部分包含设备的摘要信息。

- **用户属性：** 显示 RBAC 角色、组成员身份、批量采购帐户以及用户的属性。您可以从此页面停用批量采购帐户。
- **已分配策略：** 显示已分配策略的数量，包括已部署、待处理和失败策略的数量。提供每个策略的策略名称、类型和上次部署信息。
- **应用程序：** 显示上次清单中已安装、待处理和失败的应用程序部署数量。提供应用程序名称、标识符、类型和其他信息。
- **媒体：** 显示上次清单中已部署、待处理和失败的媒体部署数量。
- **操作：** 显示已部署、待处理和失败操作的数量。提供操作名称和上次部署时间。
- **交付组：** 显示成功、待处理和失败交付组的数量。对于每个部署，提供交付组名称和部署时间。选择一个交付组以查看更详细的信息，包括状态、操作以及渠道或用户。
- **iOS 配置文件：** 显示上次 iOS 配置文件清单，包括名称、类型、组织和描述。
- **iOS 预配配置文件：** 显示企业分发预配配置文件信息，例如 UUID、到期日期以及是否受管理。
- **证书：** 显示有效、已过期或已吊销证书的信息，例如类型、提供商、颁发者、序列号以及到期前的剩余天数。
- **连接：** 显示首次连接状态和上次连接状态。为每个连接提供用户名、倒数第二次（上次之前）身份验证时间和上次身份验证时间。
- **MDM 状态：** 显示 MDM 状态、上次推送时间以及上次设备回复时间等信息。

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提供的文件，也可以创建自己的设备预配文件。有关详细信息，请参阅本文后面的设备预配文件格式。

1. 转到**管理 > 设备**，然后单击**导入**。将显示**导入预配文件**对话框。

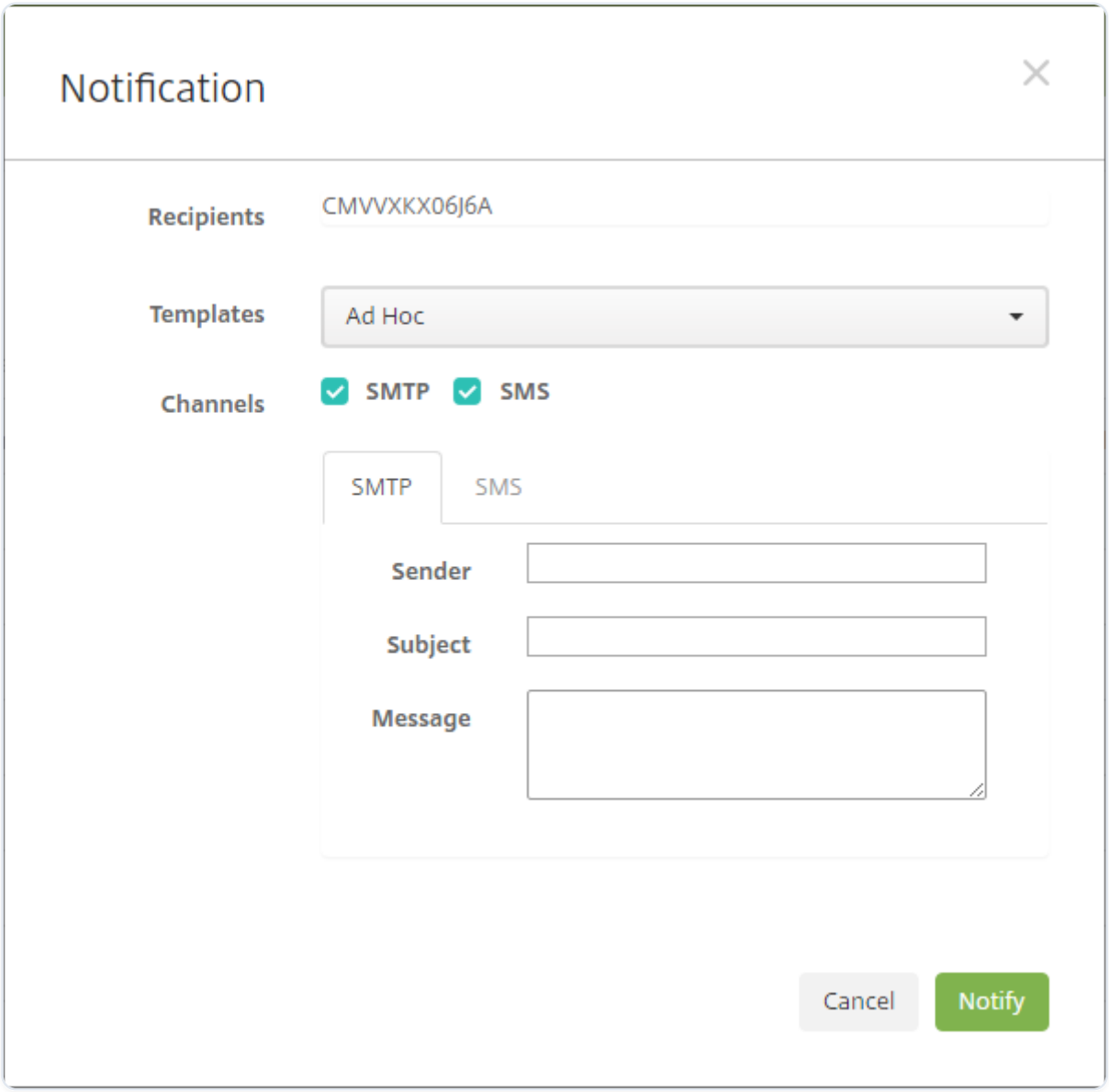


2. 单击**选择文件**，然后导航到要导入的文件。
3. 单击**导入**。**设备**表将列出导入的文件。
4. 要编辑设备信息，请选择该设备，然后单击**编辑**。有关**设备详细信息**页面的信息，请参阅手动添加设备。

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**字段列出了所有将接收通知的设备。



3. 配置以下设置：

- **模板：** 在列表中，单击要发送的通知类型。除了**Ad Hoc**模板外，其他每个模板的**主题**和**消息**字段都会显示您所选模板的配置文本。
- **通道：** 选择发送消息的方式。默认值为 **SMTP** 和 **SMS**。单击选项卡可查看每个通道的消息格式。
- **发件人：** 输入可选的发件人。
- **主题：** 为 **Ad Hoc** 消息输入主题。
- **消息：** 为 **Ad Hoc** 消息输入消息。

4. 单击**通知**。

导出设备表

1. 根据您希望在导出文件中显示的内容筛选**设备**表。
2. 单击**设备**表上方的**导出**按钮。XenMobile 会提取筛选后的**设备**表中的信息并将其转换为 .csv 文件。
3. 出现提示时，打开或保存 .csv 文件。

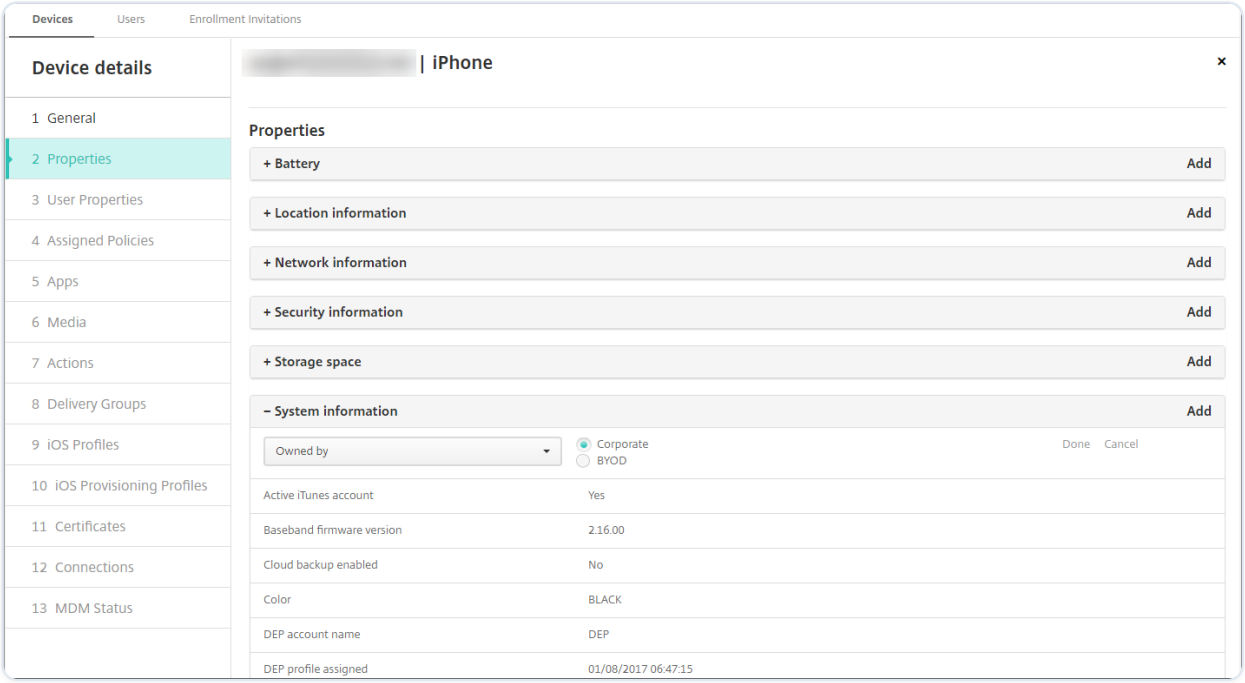
手动标记用户设备

您可以通过以下方式在 XenMobile 中手动标记设备：

- 在基于邀请的注册过程中。
- 在自助服务门户注册过程中。
- 通过将设备所有权添加为设备属性

您可以选择将设备标记为公司所有或员工所有。使用自助服务门户自行注册设备时，您可以将设备标记为公司所有或员工所有。您还可以手动标记设备，如下所示。

1. 从 XenMobile 控制台的“**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**”（员工所有）。



设备预配文件格式

许多移动运营商或设备制造商提供授权移动设备列表。您可以使用这些列表，避免手动输入冗长的移动设备列表。XenMobile 支持一种导入文件格式，该格式适用于所有三种受支持的设备类型：Android、iOS 和 Windows。

您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：

SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

请记住以下事项：

- 有关每个属性的有效值，请参阅 PDF 设备属性名称和值。
- 使用 UTF-8 字符集。
- 使用分号 (;) 分隔预配文件中的字段。如果字段的一部分包含分号，请使用反斜杠字符 (\\) 对其进行转义。

  例如，对于此属性：

  `propertyV;test;1;2`

  按如下方式转义它：

  `propertyV\;test\;1\;2`
- iOS 设备需要序列号，因为序列号是 iOS 设备标识符。

- 对于其他设备平台，您必须包含序列号或 IMEI。
- **OperatingSystemFamily** 的有效值为 **WINDOWS**、**ANDROID** 或 **iOS**。

设备预配文件示例：

```
`1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;prop
ertyV\;test\;1\;2;prop 2

2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;prope
rtyV$*&&éééétest

3050BF3F517301081610065510590393;35244201625379903;iOS;test;

4050BF3F517301081610065510590393;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;`
```

文件中的每一行描述一个设备。上述示例中的第一个条目表示以下内容：

- 序列号: `1050BF3F517301081610065510590391`
- IMEI: `15244201625379901`
- 操作系统系列: `WINDOWS`
- 属性名称: `propertyN`
- 属性值: `propertyV\;test\;1\;2;prop 2`

ActiveSync 网关

ActiveSync 是 Microsoft 开发的一种移动数据同步协议。ActiveSync 可将数据与手持设备以及台式机（或笔记本电脑）同步。

您可以在 XenMobile 中配置 ActiveSync 网关规则。根据这些规则，您可以允许或拒绝设备访问 ActiveSync 数据。例如，如果您激活“缺少所需应用程序”规则，XenMobile 将检查应用程序访问策略中所需的应用程序，如果缺少所需的应用程序，则拒绝访问 ActiveSync 数据。对于每条规则，您可以选择**允许**或**拒绝**。默认设置为**允许**。

有关应用程序访问设备策略的详细信息，请参阅应用程序访问设备策略。

XenMobile 支持以下规则：

匿名设备： 检查设备是否处于匿名模式。如果设备尝试重新连接时 XenMobile 无法重新验证用户身份，则此检查可用。

Samsung KNOX 证明失败： 检查设备是否未能查询 Samsung KNOX 证明服务器。

禁用应用程序： 检查设备是否具有禁用应用程序，如应用程序访问策略中所定义。

隐式允许和拒绝： 此操作是 ActiveSync 网关的默认操作。网关会创建不符合任何其他筛选规则条件的所有设备的设备列表，并根据该列表允许或拒绝连接。如果没有规则匹配，则默认设置为隐式允许。

非活动设备： 检查设备是否处于非活动状态，如**服务器属性**中的**设备非活动天数阈值**设置所定义。

缺少所需应用程序： 检查设备是否缺少所需应用程序，如应用程序访问策略中所定义。

非建议应用程序： 检查设备是否具有非建议应用程序，如应用程序访问策略中所定义。

不合规密码： 检查用户密码是否合规。在 iOS 和 Android 设备上，XenMobile 可以确定设备上当前的密码是否符合发送到设备的密码策略。例如，在 iOS 上，如果 XenMobile 向设备发送密码策略，用户有 60 分钟的时间来设置密码。在用户设置密码之前，密码可能不合规。

不合规设备： 根据不合规设备属性检查设备是否不合规。该属性通常由自动化操作或利用 XenMobile API 的第三方更改。

已吊销状态： 检查设备证书是否已吊销。已吊销的设备在再次获得授权之前无法重新注册。

已 Root 的 Android 和已越狱的 iOS 设备： 检查 Android 或 iOS 设备是否已越狱。

未受管设备： 检查设备是否仍处于受 XenMobile 控制的受管状态。例如，已注册 MAM 的设备或未注册的设备不受管理。

将 Android 域用户发送到 ActiveSync Gateway： 单击 **YES** 以确保 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 **Settings**（设置）页面。
2. 在 **Server**（服务器）下，单击 **ActiveSync Gateway**。此时将显示 **ActiveSync Gateway** 页面。

ActiveSync Gateway 图像(/en-us/xenmobile/server/media/settings-server-activesync-gateway.png)

1. 在 **Activate the following rules**（激活以下规则）中，选择要激活的一个或多个规则。

2. 在 **Android-only**（仅限 Android）中，在 **Send Android domain users to ActiveSync Gateway**（将 Android 域用户发送到 ActiveSync Gateway）中，单击 **YES** 以确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。
3. 单击 **Save**（保存）。

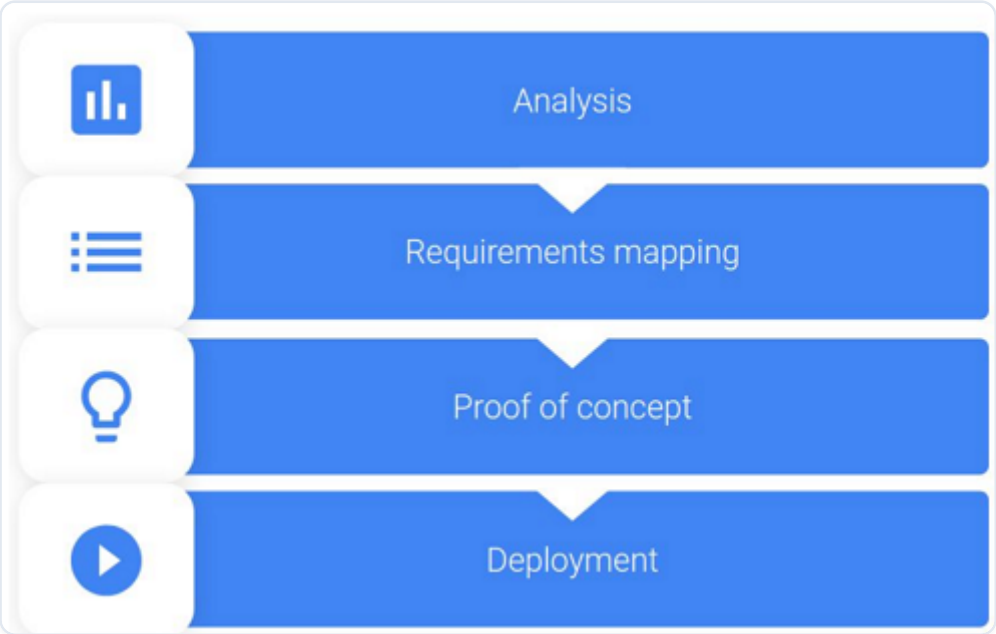
从设备管理迁移到 Android Enterprise

本文讨论了从旧版 Android 设备管理迁移到 Android Enterprise 的注意事项和建议。Google 正在弃用 Android 设备管理 API。该 API 支持 Android 设备上的企业应用。Android Enterprise 是 Google 和 Citrix 推荐的现代化管理解决方案。

XenMobile® 正在将 Android Enterprise 更改为 Android 设备的默认注册方法。Google 弃用这些 API 后，Android Q 设备在设备管理模式下的注册将失败。

Android Enterprise 支持完全托管和工作资料设备模式。Google 出版的《Android Enterprise 迁移蓝皮书》(http://static.googleusercontent.com/media/android.com/en/enterprise/static/2016/pdfs/enterprise/Android-Enterprise-Migration-Bluebook_2019.pdf) 详细解释了旧版设备管理和 Android Enterprise 之间的区别。我们建议您阅读 Google 提供的迁移信息。

该出版物还描述了设备管理迁移的四个阶段，并包含以下图表。本文包含针对 XenMobile 的迁移阶段的特定建议。



> 来自《Android Enterprise 迁移 蓝皮书》(http://static.googleusercontent.com/media/android.com/en/enterprise/static/2016/pdfs/enterprise/Android-Enterprise-Migration-Bluebook_2019.pdf) 的图表。 经 Google 许可重新发布。

设备管理弃用的影响

Google 弃用以下设备管理 API。将 Secure Hub 升级到 Android Q API 级别后，这些 API 将无法在运行 Android Q 的设备上运行：

- 禁用摄像头：控制对设备摄像头的访问。
- 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 对在 Citrix 仅 MAM 模式下注册的设备没有影响。

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	建议操作
现有设备已注册到设备管理模式，并且可升级到 Android Q。	在将设备升级到 Android Q 之前，请从设备管理模式迁移到 Android Enterprise。
现有设备已注册到设备管理模式。该设备无法升级到 Android Q。	设备可以保留在设备管理模式。但是，请计划在设备刷新时将设备迁移到 Android Enterprise。
现有设备已注册到设备管理模式，并且已升级到 Android Q。	在 Google 弃用 API 之前，请从设备管理模式迁移到 Android Enterprise。这些设备的警告消息将显示在 XenMobile 控制台中。
随附 Android Q 并注册到设备管理模式的新设备。	在 Google 弃用 API 之前，请从设备管理模式迁移到 Android Enterprise。这些设备的警告消息将显示在 XenMobile 控制台中。
随附 Android Q 或可升级到 Android Q 的新设备。该设备未注册。	对所有新设备使用 Android Enterprise。
在 Google 弃用 API 后，Android Q 上的新设备或现有设备将注册到设备管理模式。	为避免弃用的 Google API 造成影响，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。
注册到 Citrix 仅 MAM 模式的新设备或现有设备	无需采取任何操作。已弃用的 Google API 对仅限 MAM 模式下的设备没有影响。

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，以便将旧版功能映射到 Android Enterprise 功能

建议的分析

1. 评估 XenMobile 上的 Android Enterprise：完全托管、带工作资料的完全托管、专用设备、工作资料 (BYOD)。
2. 根据 Android Enterprise 分析您当前的设备管理功能。
3. 记录您的设备管理用例。

要记录您的设备管理用例，请执行以下操作：

1. 创建电子表格并列出 XenMobile 控制台中的当前策略组。
2. 根据现有策略组创建单独的用例。
3. 对于每个用例，请记录以下内容：
    - 名称
    - 业务负责人
    - 用户身份模型
    - 设备要求
        - 安全性
        - 管理
        - 可用性
    - 设备清单
        - 品牌和型号
        - 操作系统版本
    - 应用程序
4. 对于每个应用程序，列出：
    - 应用程序名称
    - 包名称

- 托管方法
- 应用程序是公共的还是私有的
- 应用程序是否强制（是/否）

要求映射

根据已完成的分析，确定您的 Android Enterprise 功能要求。

推荐的要求映射

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。无需恢复出厂设置。
   - 完全托管：需要恢复出厂设置。通过使用二维码、近场通信 (NFC) 碰撞、设备策略控制器 (DPC) 标识符、零接触来注册设备。
2. 创建应用程序迁移策略。
3. 将用例要求映射到 Android Enterprise 功能。为每个设备要求记录最符合该要求及其相应 Android 版本的特性。
4. 根据功能要求确定最低 Android 操作系统版本（7.0、8.0、9.0）。
5. 选择身份模型：
   - 推荐：托管式 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：如果设备支持并可以更新到受支持的操作系统
   - 替换：如果设备无法更新到支持的操作系统级别

推荐的应用程序迁移策略

完成要求映射后，将应用程序从 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。

- 公共商店应用程序
  a. 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，并选择 **Android Enterprise** 作为平台。

b. 选择交付组。如果应用程序是强制性的，请将应用程序移动到交付组中的**所需应用程序**列表。

保存应用程序后，它会显示在 Google Play 商店中。如果您有工作配置文件，应用程序会显示在工作配置文件中的 Google Play 商店中。

- 私有（企业）应用程序

  私有应用程序由内部或第三方开发人员开发。我们建议您使用 Google Play 发布私有应用程序。

  a. 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。
  b. 上传 APK 文件，然后配置应用程序设置。
  c. 将应用程序发布到所需的交付组。

- MDX 应用程序

  a. 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。
  b. 上传 MDX 文件。完成应用程序审批流程。
  c. 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 模式封装的应用程序：

  - 选项 1：在 Google Play 中托管 APK，并使用私下分配给您组织的开发者帐户。在 XenMobile 中发布 MDX 文件。
  - 选项 2：将应用程序从 XenMobile 发布为企业应用程序。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：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工作配置文件模式或完全托管模式下的设备。

概念验证

将应用程序迁移到 Android Enterprise 后，您可以设置迁移测试以验证功能是否按预期工作。

推荐的概念验证设置

1. 设置部署基础结构：

- 为您的 Android Enterprise 测试创建交付组。
- 在 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. 测试并确认功能。
6. 为每个用例完成设备设置演练。
7. 记录用户设置步骤。

部署

您现在可以部署 Android Enterprise 设置并为用户迁移做好准备。

推荐的部署策略

Citrix 推荐的部署策略是测试所有生产系统以支持 Android Enterprise，然后稍后完成设备迁移。

- 在此场景中，用户继续使用具有当前配置的旧设备。您为 Android Enterprise 管理设置新设备。
- 仅在需要升级或更换时才迁移现有设备。
- 在现有设备达到其常规生命周期结束时将其迁移到 Android Enterprise 管理。或者，当设备因丢失或损坏需要更换时迁移它们。

Android 企业版

Android Enterprise 是 Google 提供的一套工具和服务，作为 Android 设备的企业管理解决方案。借助 Android Enterprise：

- 您可以使用 XenMobile® 管理公司拥有的 Android 设备和自带设备 (BYOD) Android 设备。
- 您可以管理整个设备或设备上的独立配置文件。独立配置文件将业务帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。
- 您还可以管理专用于单一用途的设备，例如库存管理。有关 Google Android Enterprise 功能的概述，请参阅 Android Enterprise 管理。

资源：

- 有关 Android Enterprise 相关术语和定义的列表，请参阅 Google Android Enterprise 开发者指南中的 Android Enterprise 术语。Google 会频繁更新这些术语。
- 有关 XenMobile 支持的 Android 操作系统，请参阅 支持的设备操作系统。

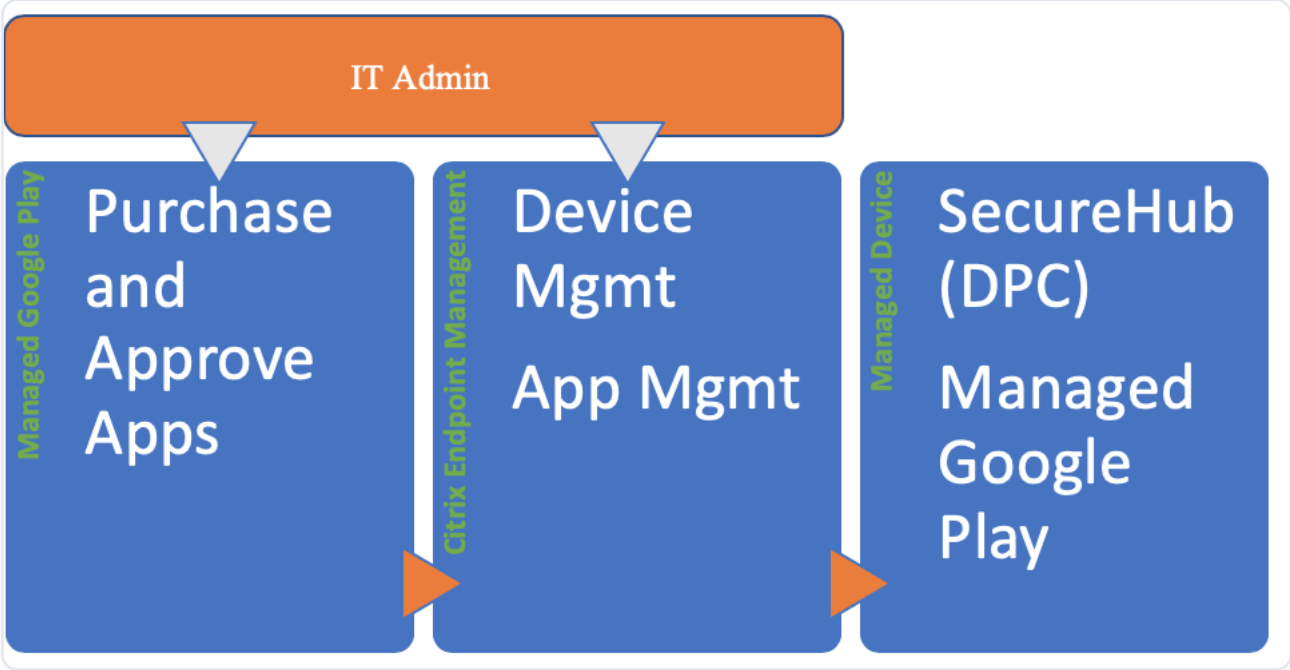
- 有关为 Android Enterprise 设置网络环境时要考虑的出站连接信息，请参阅 Google 支持文章 Android Enterprise 网络要求。

当您将 XenMobile 与托管 Google Play 集成以使用 Android Enterprise 时，您将创建一个企业。Google 将企业定义为组织与您的企业移动管理 (EMM) 解决方案之间的绑定。组织通过您的解决方案管理的所有用户和设备都属于其企业。

Android Enterprise 的企业包含三个组件：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 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 管理员提供了管理其组织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。

此图说明了管理员如何与这些组件交互以及这些组件如何相互交互：



将托管式 Google Play 与 XenMobile 结合使用

> **注意：**

> 您可以使用托管式 Google Play 或 Google Workspace 将 Citrix 注册为您的 EMM 提供程序。本文讨论将 Android Enterprise 与托管式 Google Play 结合使用。如果您的组织使用 Google Workspace 提供对应用程序的访问，则可以将其与 Android Enterprise 结合使用。请参阅 适用于 Google Workspace（以前称为 G-Suite）客户的旧版 Android Enterprise。

> 当您使用托管式 Google Play 时，您为设备和最终用户预配托管式 Google Play 帐户。托管式 Google Play 帐户提供对托管式 Google Play 的访问权限，允许用户安装和使用您提供的应用程序。如果您的组织使用第三方身份服务，您可以将托管式 Google Play 帐户与现有身份帐户关联。

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

对于 XenMobile 管理员而言，托管式 Google Play 将 Google Play 的用户体验和应用商店功能与一套专为企业设计的管理功能相结合。您可以使用托管式 Google Play 添加、购买和批准应用程序，以部署到设备上的 Android Enterprise 工作区。您可以使用 Google Play 部署公共应用程序、私人应用程序和第三方应用程序。

对于托管设备的用户而言，托管式 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并安装它们。与公共版 Google Play 不同，用户只能从您为他们提供的托管式 Google Play 中安装应用程序。

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 如何管理和强制执行设备上的策略。

工作配置文件将业务帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。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 什么是工作配置文件。

> **重要：**

> 当 Android Enterprise 设备更新到 Android 11 时，Google 会将作为“完全托管且带有工作配置文件”管理的设备迁移到新的安全增强型工作配置文件体验。有关详细信息，请参阅 Android Enterprise 完全托管且带有工作配置文件的未来变化。

设备管理	用例	工作配置文件	个人配置文件	备注
公司拥有的设备（完全托管）	仅用于工作的公司拥有的设备	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、配置全局设置以及执行出厂重置。	仅适用于新设备或已恢复出厂设置的设备。
通过工作配置文件完全托管	用于工作和个人用途的公司拥有的设备	是	是。这些设备上运行着两个 DPC 副本：一个以设备所有者模式管理设备，另一个以配置文件所有者模式管理工作配置文件。您可以对设备和工作配置文件应用单独的策略。	以前称为公司拥有的个人启用 (COPE) 设备。
专用设备*	配置用于单一用例的公司拥有的设备，例如数字标牌或票据打印	否	是。您只提供所需的应用程序，并阻止用户添加其他应用程序。	以前称为企业自有单用途 (COSU) 设备。
BYOD 工作配置文件**	以工作配置文件模式（也称为配置文件所有者模式）注册的个人设备	是	是。DPC 仅管理工作配置文件，而不管理整个设备。	这些设备无需是新设备或恢复出厂设置的设备。

* 用户可以共享专用设备。当用户登录专用设备上的应用程序时，其工作状态与应用程序相关，而非设备本身。

** XenMobile 不支持 BYOD 工作配置文件模式下的 Zebra 设备。XenMobile 支持将 Zebra 设备作为完全托管设备和设备旧版模式（也称为设备管理员模式）使用。

有关从旧版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

注册配置文件决定 Android 设备是注册到 MAM、MDM 还是 MDM+MAM，并允许用户选择退出 MDM。

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 MDM+MAM 中注册的 Android 设备的以下身份验证方法。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 活动目录
  - Citrix 身份提供程序

另一种不常用的身份验证方法是客户端证书加安全令牌。有关信息，请参阅 `<https://support.citrix.com/article/CTX215200>`。

要求

开始使用 Android Enterprise 之前，您需要：

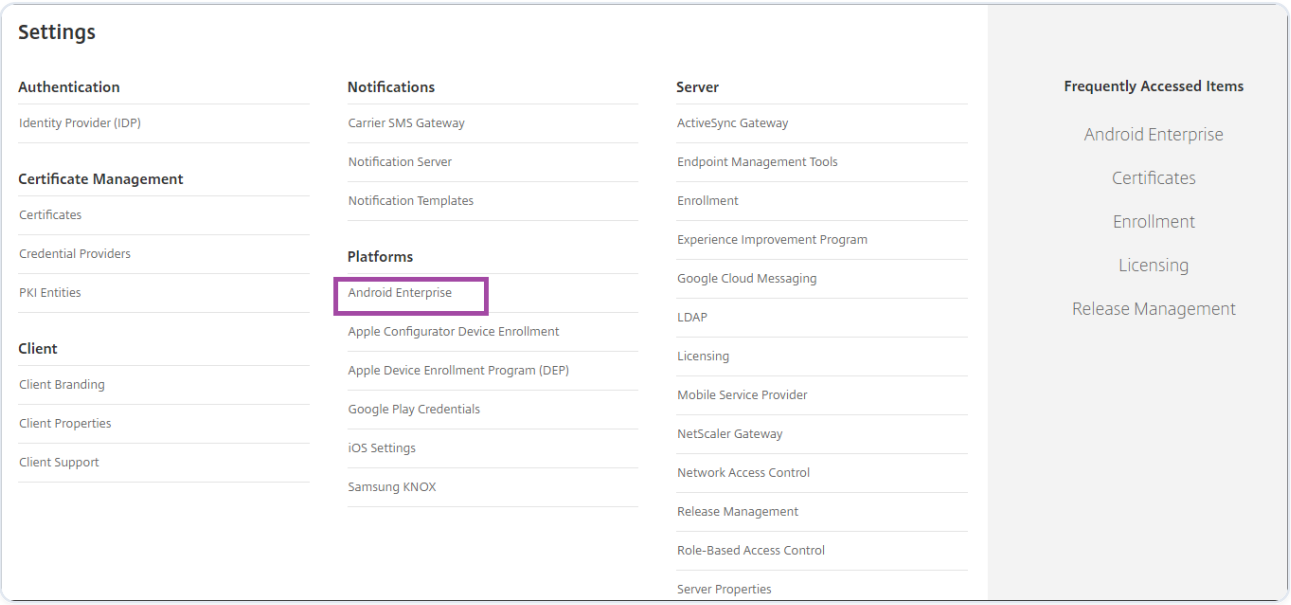
- 帐户和凭据:
  - 要使用托管 Google Play 设置 Android Enterprise，需要一个企业 Google 帐户
  - 要下载最新的 MDX 文件，需要一个 Citrix 客户帐户
  - 要部署私有应用程序（可选），需要一个 Google 开发者帐户
- 为 XenMobile 配置的 Firebase Cloud Messaging (FCM)。有关说明，请参阅 Firebase Cloud Messaging。
- 对于 Samsung Knox Mobile Enrollment（可选），Knox 高级许可证。

将 XenMobile 连接到 Google Play

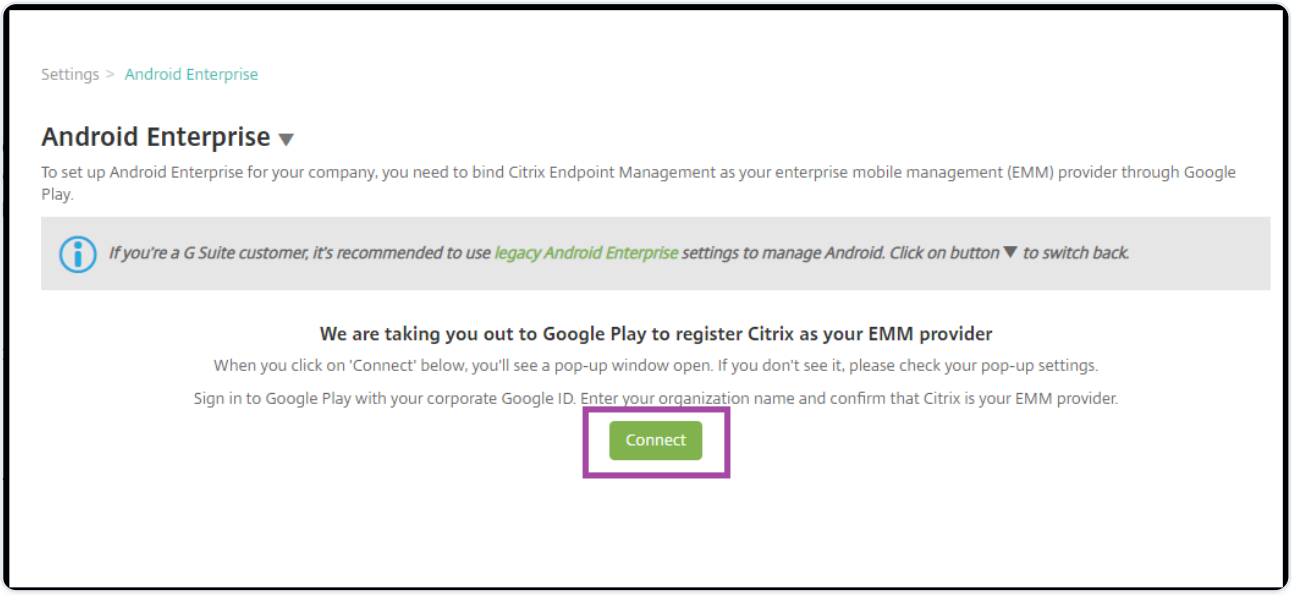
要为您的组织设置 Android Enterprise，请通过托管 Google Play 将 Citrix 注册为您的 EMM 提供商。此设置会将托管 Google Play 连接到 XenMobile，并在 XenMobile 中为 Android Enterprise 创建一个企业。

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**。

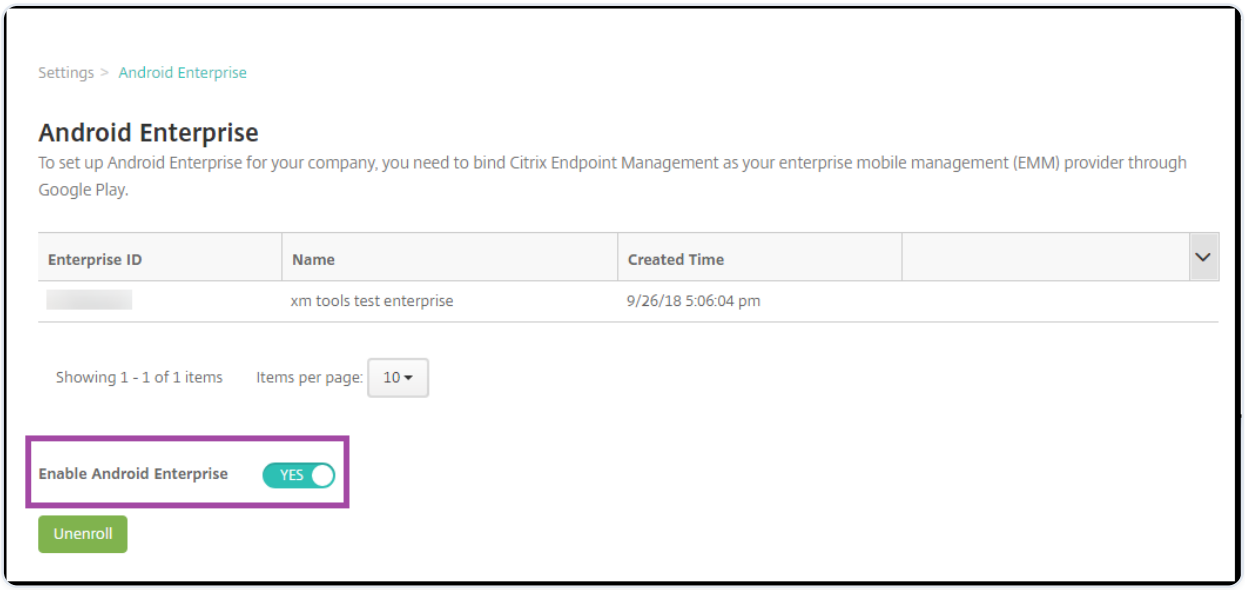


1. 单击**连接**。Google Play 将打开。

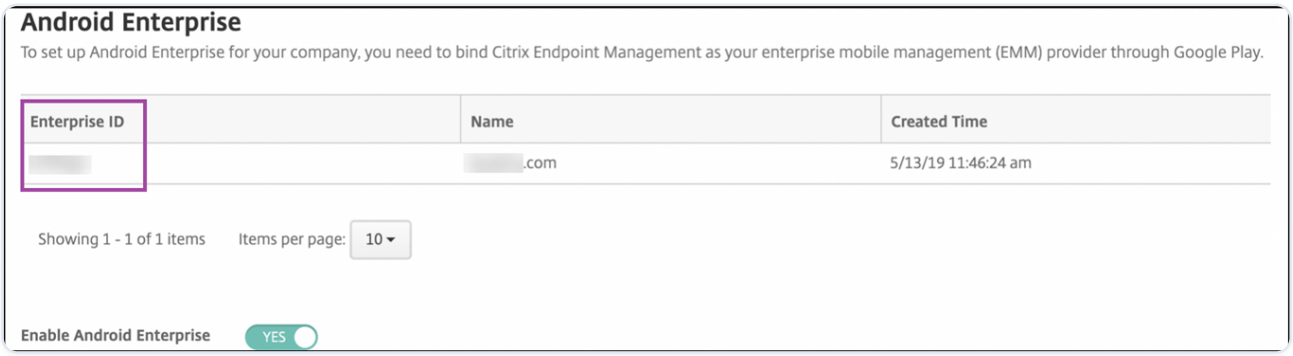


1. 使用您的企业 Google 帐户凭据登录 Google Play。输入您的组织名称并确认 Citrix 是您的 EMM 提供商。

2. 将为 Android Enterprise 添加一个企业 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，并已准备好管理设备。您现在可以为用户提供应用程序了。

XenMobile 可用于向用户提供 Citrix 移动生产力应用程序、MDX 应用程序、公共应用商店应用程序、Web 和 SaaS 应用程序、企业应用程序以及 Web 链接。有关这些类型的应用程序以及如何向用户提供这些应用程序的更多信息，请参阅添加应用程序。

以下部分介绍了如何提供移动生产力应用程序。

向 Android Enterprise 用户提供 Citrix 移动生产力应用程序

为 Android Enterprise 用户提供 Citrix 移动生产力应用程序需要以下步骤。

1. 将应用程序发布为 MDX 应用程序。请参阅将应用程序配置为 MDX 应用程序。
2. 配置用户用于访问其设备上工作配置文件的安全质询规则。请参阅配置安全质询策略。

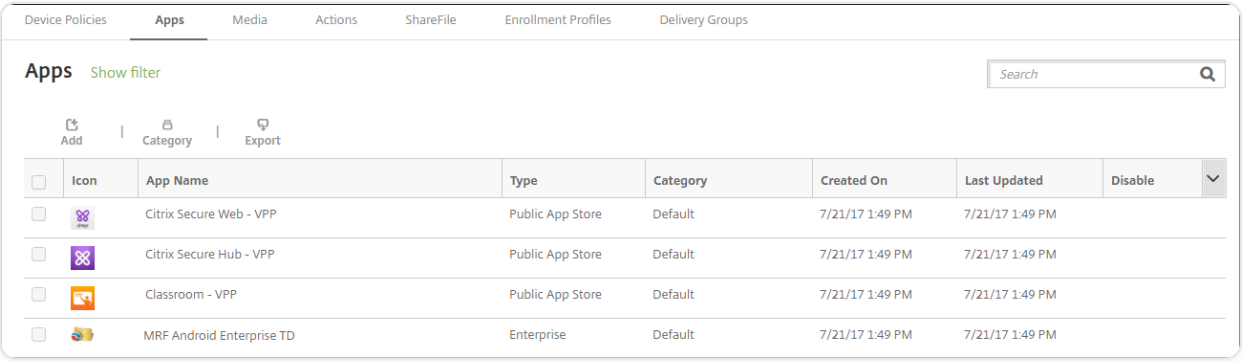
您发布的应用程序可供已注册到您的 Android Enterprise 企业的设备使用。

> **注意：**
>
> 当您向 Android 用户部署 Android Enterprise 公共应用商店应用程序时，该用户将自动注册到 Android Enterprise。

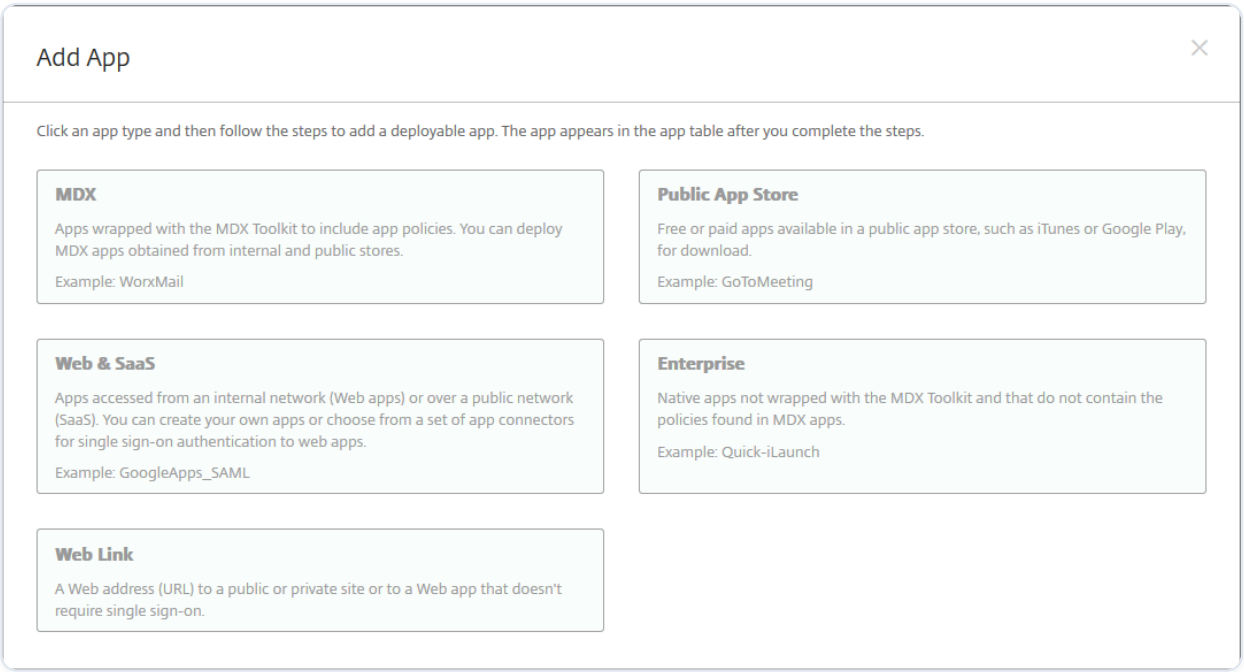
将应用程序配置为 MDX 应用程序

要将 Citrix 生产力应用程序配置为 Android Enterprise 的 MDX 应用程序，请执行以下操作：

1. 在 XenMobile 控制台中，单击**配置 > 应用程序**。此时将显示**应用程序**页面。



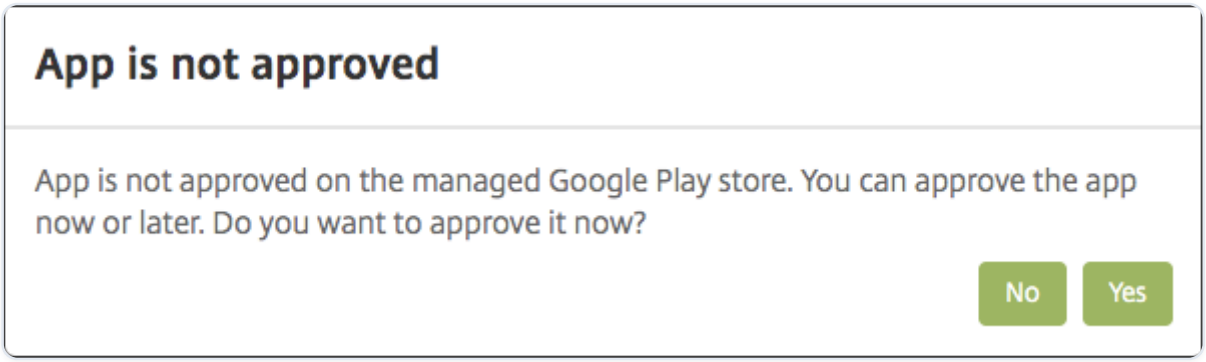
2. 单击**添加**。此时将显示**添加应用程序**对话框。



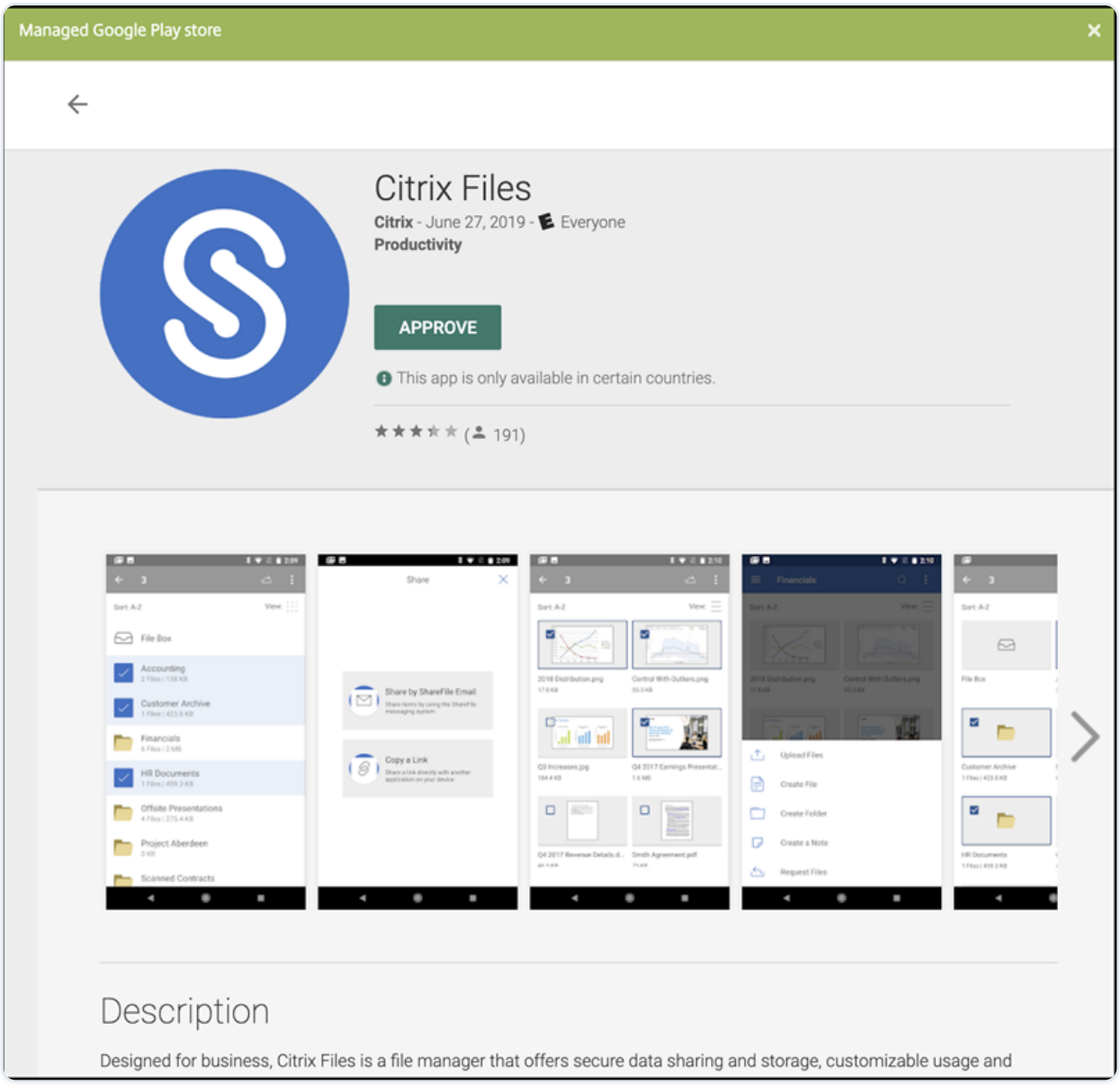
3. 点击 **MDX**。将显示“**应用程序信息**”页面。
4. 在页面的左侧，选择 **Android Enterprise** 作为平台。
5. 在“**应用程序信息**”页面上，键入以下信息：
   - **名称：** 键入应用程序的描述性名称。此名称将显示在“**应用程序**”表中的“**应用程序名称**”下。

- **说明：** 键入应用程序的可选说明。
- **应用程序类别：** （可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

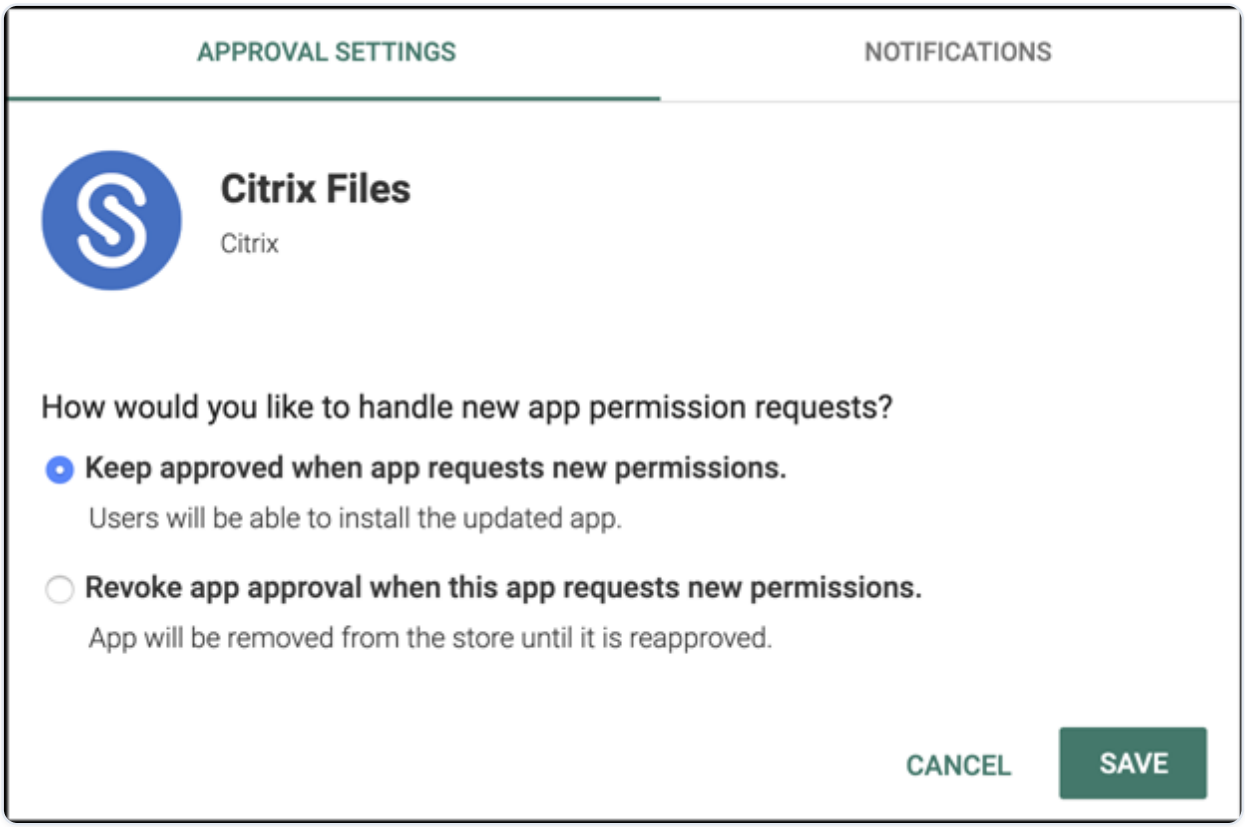
6. 点击“**下一步**”。将显示“**Android Enterprise MDX 应用程序**”页面。
7. 点击“**上载**”，然后导航到应用程序 .mdx 文件的文件位置。选择文件，然后点击“**打开**”。
8. 如果附加的应用程序需要托管 Google Play 商店的批准，UI 会通知您。要在不离开 XenMobile 控制台的情况下批准应用程序，请点击“**是**”。



9. 托管 Google Play 商店页面打开后，点击“**批准**”。



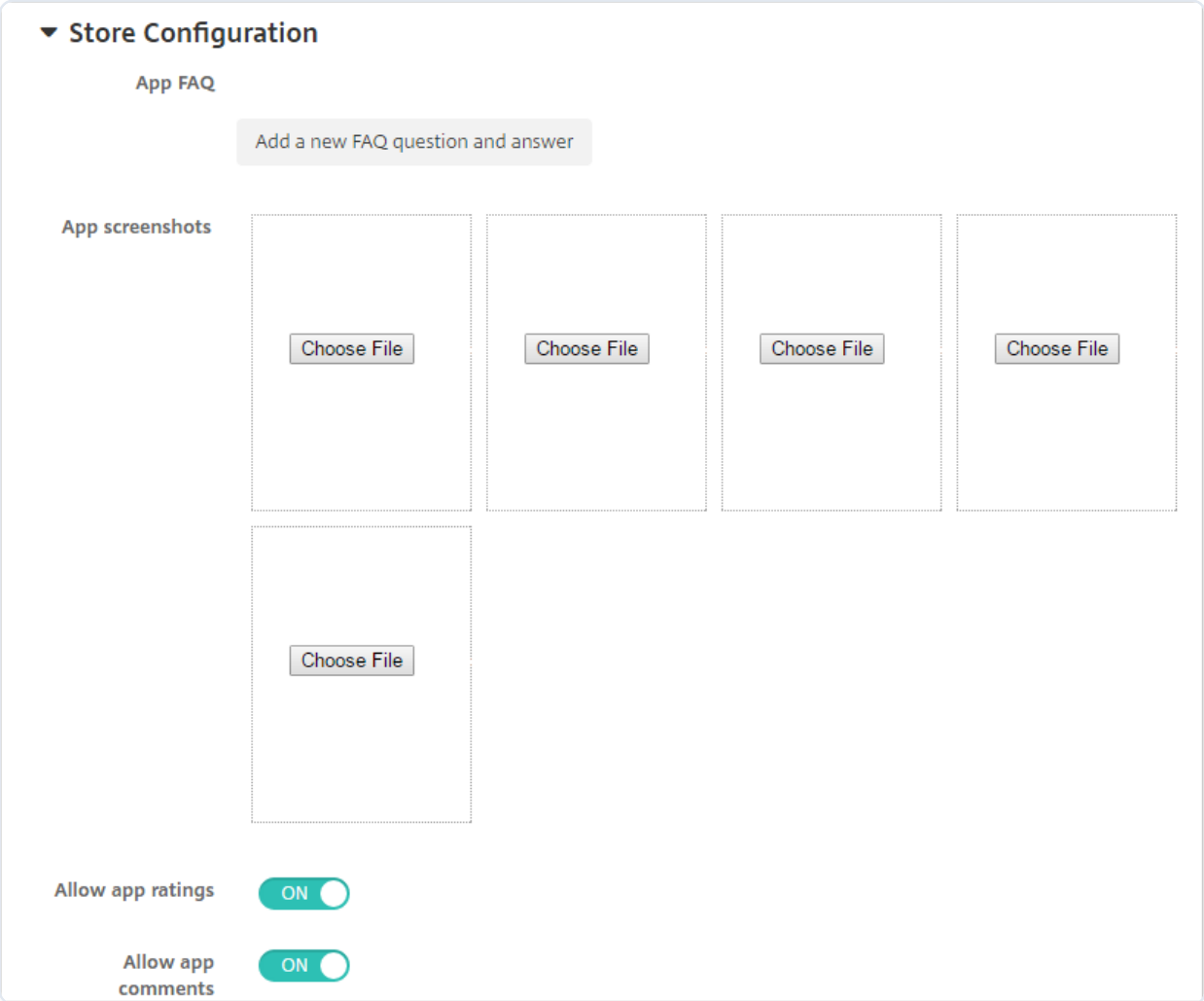
10. 再次点击“**批准**”。
11. 选择“**当应用程序请求新权限时保持批准**”。点击“**保存**”。



12. 当应用获得批准并保存后，页面上会显示更多设置。配置这些设置：

    - **文件名：** 输入与应用关联的文件名。
    - **应用描述：** 输入应用描述。
    - **产品轨道：** 指定要推送到用户设备的产品轨道。如果您有专为测试设计的轨道，可以选择并将其分配给用户。默认值为“生产”。
    - **应用版本：** （可选）输入应用版本号。
    - **包 ID：** 应用在 Google Play 商店中的 URL。
    - **最低操作系统版本：** （可选）输入设备运行该应用所需的最低操作系统版本。
    - **最高操作系统版本：** （可选）输入设备运行该应用所需的最新操作系统版本。
    - **排除的设备：** （可选）输入无法运行该应用的设备制造商或型号。

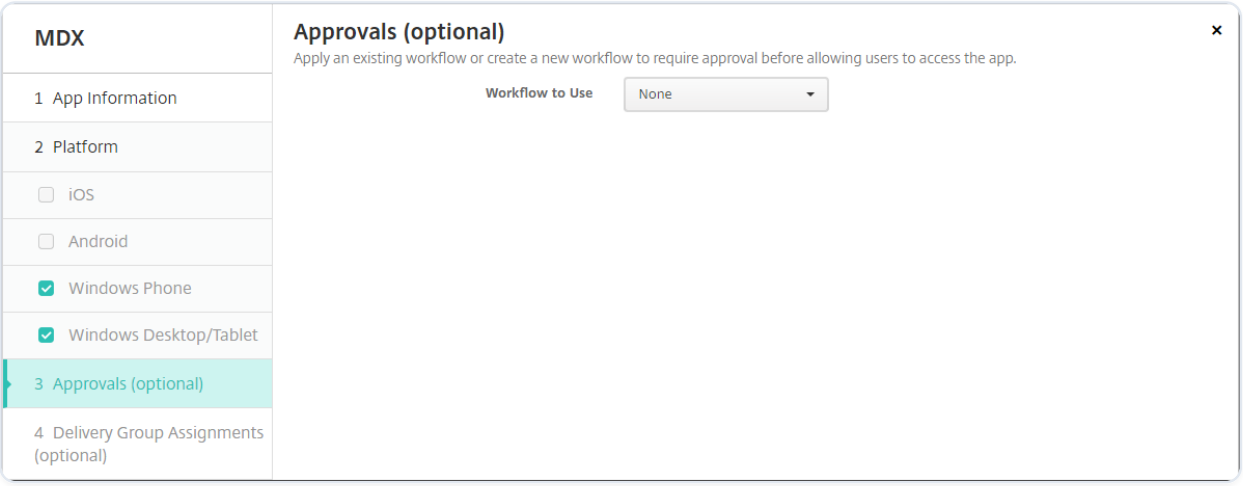
13. 配置 **MDX 策略**。有关 MDX 应用的应用策略的更多信息，请参阅 MDX 策略一览 和 MAM SDK 概述。
14. 配置部署规则。有关信息，请参阅 部署资源。
15. 展开 **商店配置**。此设置不适用于 Android Enterprise 应用，这些应用仅显示在托管的 Google Play 中。



（可选）您可以为应用添加常见问题解答或在应用商店中显示的屏幕截图。您还可以设置用户是否可以对应用进行评分或评论。

- 配置这些设置：
  - **应用常见问题：** 添加应用的常见问题和答案。
  - **应用屏幕截图：** 添加屏幕截图以帮助在应用商店中对应用进行分类。您上传的图形必须是 PNG 格式。您不能上传 GIF 或 JPEG 图像。
  - **允许应用评分：** 选择是否允许用户对应用进行评分。默认值为 **ON**。 **允许应用评论：** 选择是否允许用户评论所选应用。默认值为 **ON**。

16. 单击“**下一步**”。此时将显示“**审批**”页面。



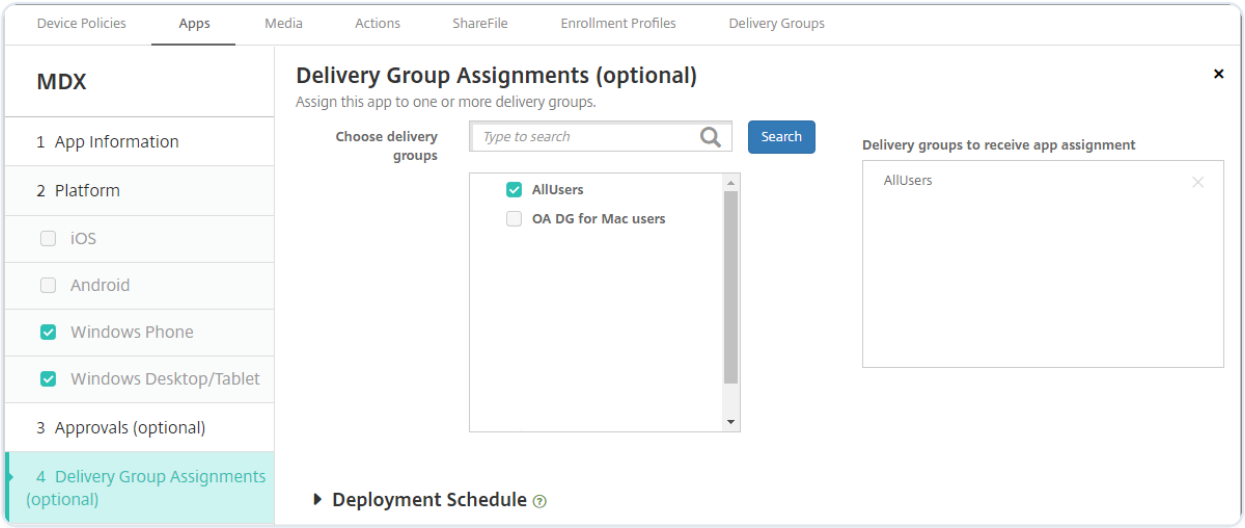
在创建用户帐户时需要审批，此时您可以使用工作流。如果您不想设置审批工作流，可以跳到步骤 15。

配置以下设置以分配或创建工作流：

- **要使用的工作流：** 在列表中，单击现有工作流或单击“**创建新工作流**”。默认值为“**无**”。
- 如果选择“**创建新工作流**”，请配置以下设置。有关详细信息，请参阅应用工作流。
- **名称：** 键入工作流的唯一名称。
- **描述：** （可选）键入工作流的描述。
- **电子邮件审批模板：** 在列表中，选择要分配的电子邮件审批模板。当您单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在其中预览模板。
- **经理审批级别：** 在列表中，选择此工作流所需的经理审批级别数。默认值为 1 级。可能的选项包括：
  - 不需要
  - 1 级
  - 2 个级别
  - 3 个级别
- **选择 Active Directory 域：** 在列表中，选择要用于工作流的相应 Active Directory 域。
- **查找其他必需的审批者：** 在搜索字段中键入其他必需人员的姓名，然后单击“**搜索**”。姓名源自 Active Directory。
- 当姓名出现在字段中时，选中姓名旁边的复选框。姓名和电子邮件地址将显示在“**已选定的其他必需审批者**”列表中。
  - 要从“**已选定的其他必需审批者**”列表中删除人员，请执行以下操作之一：
    - 单击“**搜索**”以查看所选域中所有人员的列表。

- 在搜索框中键入完整或部分姓名，然后单击“**搜索**”以限制搜索结果。
- “**已选定的其他必需审批者**”列表中的人员在搜索结果列表中其姓名旁边带有复选标记。滚动列表并清除要删除的每个姓名旁边的复选框。

17. 单击“**下一步**”。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在列表中选择一个或多个组。您选择的组将显示在“**接收应用程序分配的交付组**”列表中。
19. 展开“**部署计划**”，然后配置以下设置：

    - 在“**部署**”旁边，单击“**开**”以安排部署，或单击“**关**”以阻止部署。默认选项设置为“**开**”。
    - 在“部署计划”旁边，单击“**立即**”或“**稍后**”。默认选项设置为“**立即**”。
    - 如果您点击**稍后**，请点击日历图标，然后选择部署的日期和时间。
    - 在**部署条件**旁边，点击**每次连接时**或点击**仅当上次部署失败时**。默认选项设置为**每次连接时**。
    - 在**部署用于始终在线连接**旁边，确保选择**关闭**。默认选项设置为**关闭**。如果您从 XenMobile 10.18.19 或更高版本开始使用，则 Android Enterprise 不支持始终在线连接。我们不建议在 XenMobile 10.18.19 之前开始使用的客户使用此连接。

      当您在**设置 > 服务器属性**中配置了计划后台部署密钥时，此选项适用。

      您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但**部署用于始终在线连接**除外。

20. 点击**保存**。

重复这些步骤，为每个移动生产力应用程序配置一个 MDX 应用程序。

配置安全质询策略

XenMobile 密码设备策略配置了一组规则，用于用户访问其设备或设备上的 Android Enterprise 工作配置文件时的安全质询。安全质询可以是密码或生物识别。有关密码策略的更多信息，请参阅密码设备策略。

- 如果您的 Android Enterprise 部署包含 BYOD 设备，请为工作配置文件配置密码策略。
- 如果您的部署包含公司拥有的完全托管设备，请为设备本身配置密码策略。
- 如果您的部署包含这两种类型的设备，请配置这两种类型的密码策略。

要配置密码策略：

1. 在 XenMobile 控制台中，转至**配置 > 设备策略**。
2. 点击**添加**。
3. 点击“**显示筛选器**”以显示“**策略平台**”窗格。在“**策略平台**”窗格中，选择“**Android Enterprise**”。
4. 在右侧窗格中，点击“**密码**”。

密码安全选项(/en-us/xenmobile/server/media/password-security-policy.png)

1. 输入“**策略名称**”。点击“**下一步**”。

   密码安全名称(/en-us/xenmobile/server/media/password-security-name.png)
2. 配置密码策略设置。
   - 将“**设备密码要求**”设置为“**开**”，以查看设备本身的安全质询可用设置。
   - 将“**工作配置文件安全质询**”设置为“**开**”，以查看工作配置文件安全质询的可用设置。
3. 点击“**下一步**”。
4. 将策略分配给一个或多个交付组。
5. 点击“**保存**”。

创建注册配置文件

如果为 XenMobile 部署启用了 Android Enterprise，注册配置文件将控制 Android 设备的注册方式。创建注册配置文件以注册 Android Enterprise 设备时，您可以将注册配置文件配置为注册新设备和恢复出厂设置的设备，具体如下：

- 完全托管设备
- 专用设备（COSU 设备）
- 具有工作资料的完全托管设备 (COPE 设备)

您还可以将每个 Android Enterprise 注册配置文件配置为将 BYOD Android 设备注册为工作资料设备。

如果您的 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 设备注册为工作资料设备。

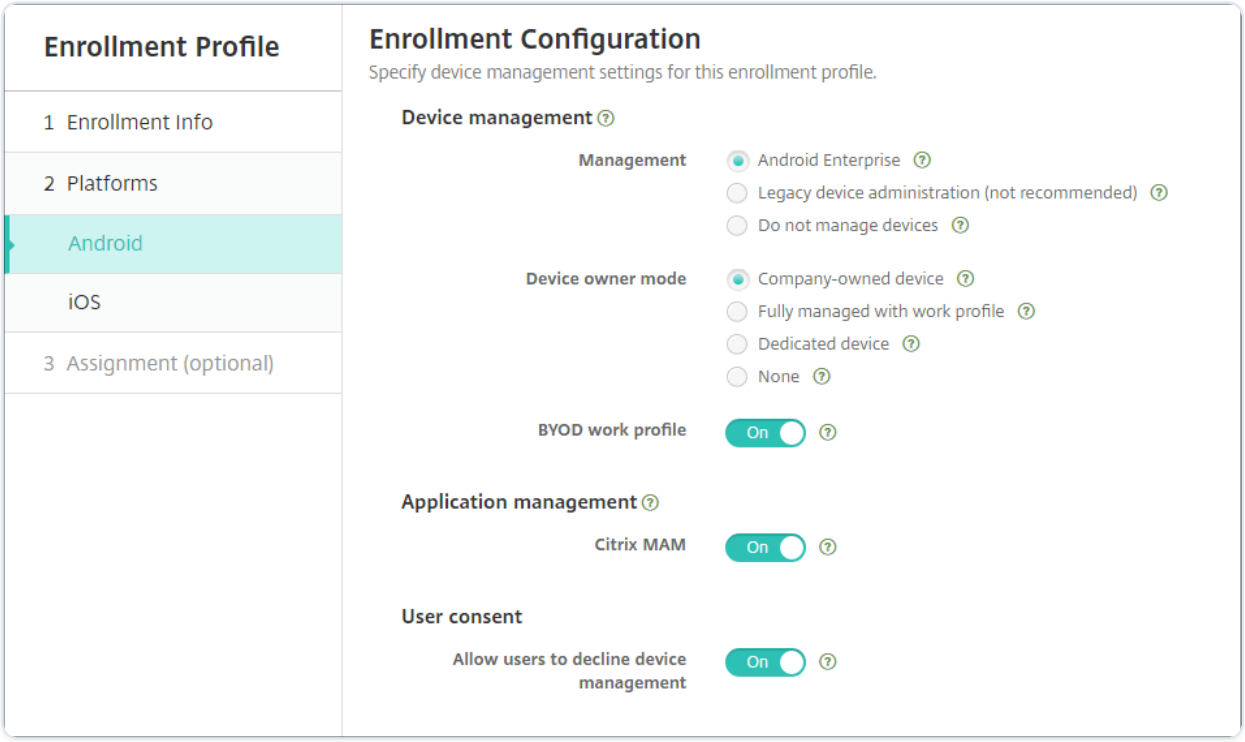
创建注册配置文件时，需要为其分配交付组。如果用户属于具有不同注册配置文件的多个交付组，则交付组的名称决定了所使用的注册配置文件。XenMobile 会选择按字母顺序排列的交付组列表中最后出现的交付组。有关详细信息，请参阅注册配置文件。

您可以使用注册配置文件来组合多种用例，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**中可用的设置。

添加完全托管设备的注册配置文件

默认情况下，全局注册配置文件会注册完全托管设备，但您可以创建更多注册配置文件来注册完全托管设备。

1. 在 XenMobile 控制台中，转至**配置 > 注册配置文件**。
2. 要添加注册配置文件，请单击**添加**。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置具有此配置文件的成员可以注册的设备数量。
4. 在**平台**下选择 **Android** 或单击**下一步**。“注册配置”页面随即显示。
5. 将**管理**设置为 **Android Enterprise**。
6. 将**设备所有者模式**设置为**公司拥有的设备**。



7. **BYOD 工作资料**允许您配置注册配置文件，以将 BYOD 设备注册为工作资料设备。新的和恢复出厂设置的设备将注册为完全托管设备。

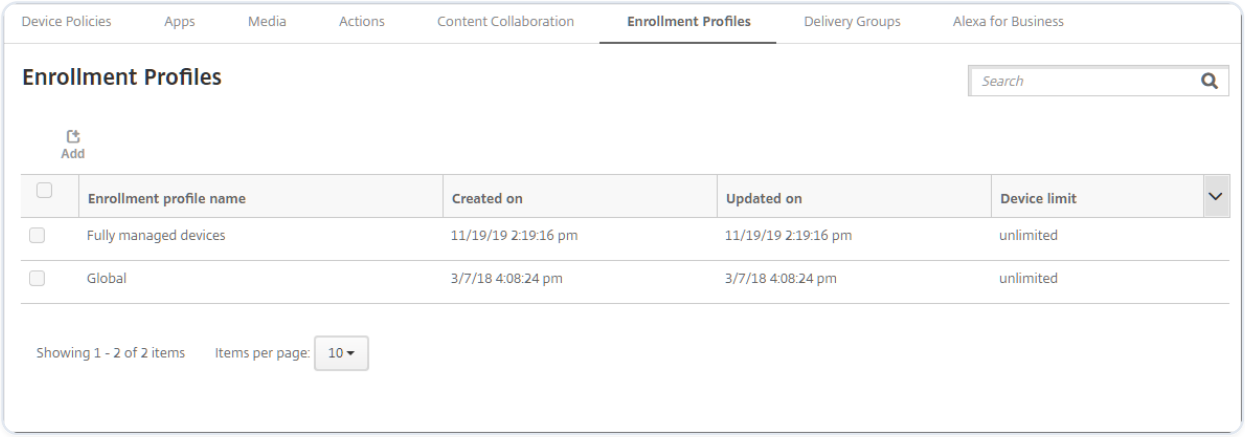
   - 将 **BYOD 工作配置文件** 设置为 **开** 以允许将 BYOD 设备注册为工作配置文件设备。默认值为 **开**。
   - 将 **BYOD 工作配置文件** 设置为 **关** 以限制注册到完全托管设备。

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。要允许 BYOD 工作配置文件设备的用户在注册设备时拒绝设备管理，请将 **允许用户拒绝设备管理** 设置为 **开**。

   如果 **BYOD 工作配置文件** 设置为 **开**，则 **允许用户拒绝设备管理** 的默认值为 **开**。如果 **BYOD 工作配置文件** 设置为 **关**，则 **允许用户拒绝设备管理** 将被禁用。

10. 选择 **分配（选项）**。将显示“交付组分配”屏幕。
11. 选择包含注册完全托管设备的管理员的交付组或交付组。然后单击 **保存**。

    将显示“注册配置文件”页面，其中包含您添加的配置文件。



添加专用设备注册配置文件

当您的 XenMobile 部署包含专用设备时，单个 XenMobile 管理员或一小部分管理员会注册许多专用设备。为确保这些管理员可以注册所有必需的设备，请为他们创建一个注册配置文件，其中每个用户允许的设备数量不受限制。

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。确保将具有此配置文件的成员可以注册的设备数量设置为无限制。
3. 在 **平台** 下选择 **Android** 或单击 **下一步**。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**。

   注册配置文件页面(/en-us/xenmobile/server/media/enrollment-profile-android-dedicated.png)

6. **BYOD 工作配置文件**允许您配置注册配置文件，以将 BYOD 设备注册为工作配置文件设备。新设备和恢复出厂设置的设备将注册为专用设备。将**BYOD 工作配置文件**设置为**开**以允许将 BYOD 设备注册为工作配置文件设备。将**BYOD 工作配置文件**设置为**关**以限制注册到公司拥有的设备。默认值为**开**。
7. 选择是否在 Citrix MAM 中注册设备。
8. 如果您将**BYOD 工作配置文件**设置为**开**，请配置用户同意。要允许 BYOD 工作配置文件设备的用户在注册设备时拒绝设备管理，请将**允许用户拒绝设备管理**设置为**开**。

   如果**BYOD 工作配置文件**设置为**开**，则**允许用户拒绝设备管理**的默认值为**开**。如果**BYOD 工作配置文件**设置为**关**，则**允许用户拒绝设备管理**将被禁用。

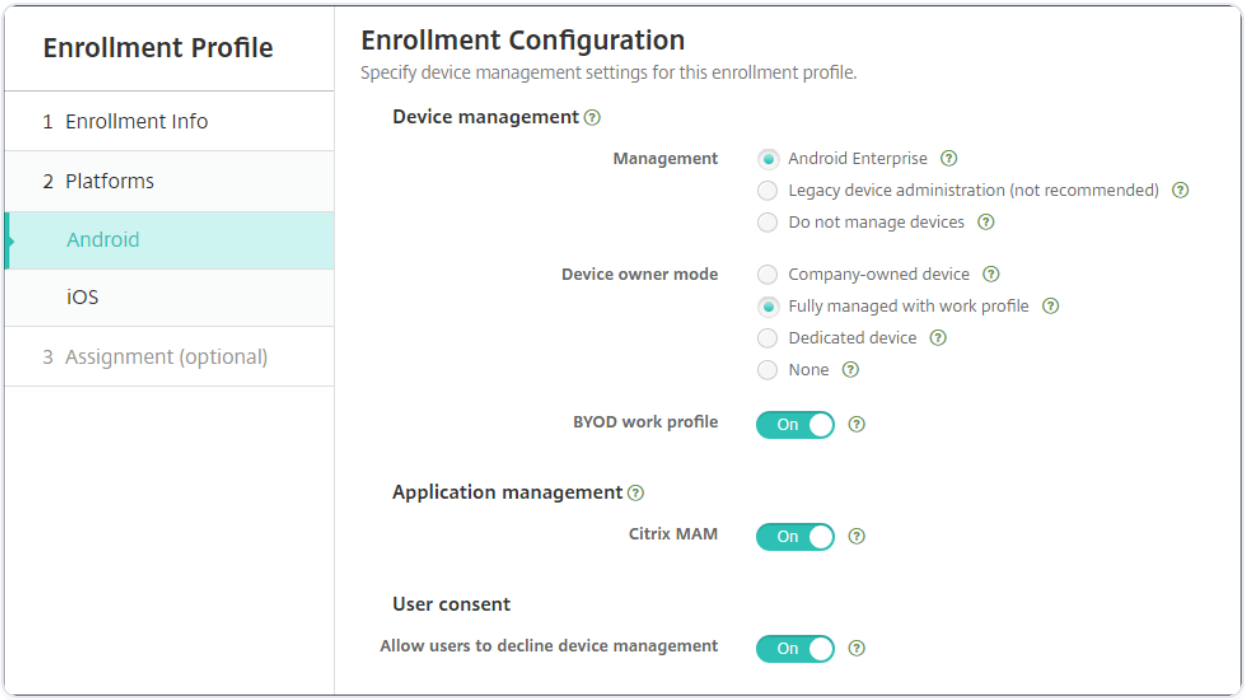
9. 选择**分配（选项）**。此时将显示“交付组分配”屏幕。
10. 选择包含注册专用设备的管理员的交付组或多个交付组。然后单击**保存**。

    此时将显示“注册配置文件”页面，其中包含您添加的配置文件。

注册配置文件配置屏幕(/en-us/xenmobile/server/media/android-enterprise-enrollment-profile-cosu-done.png)

为具有工作配置文件的完全托管设备添加注册配置文件

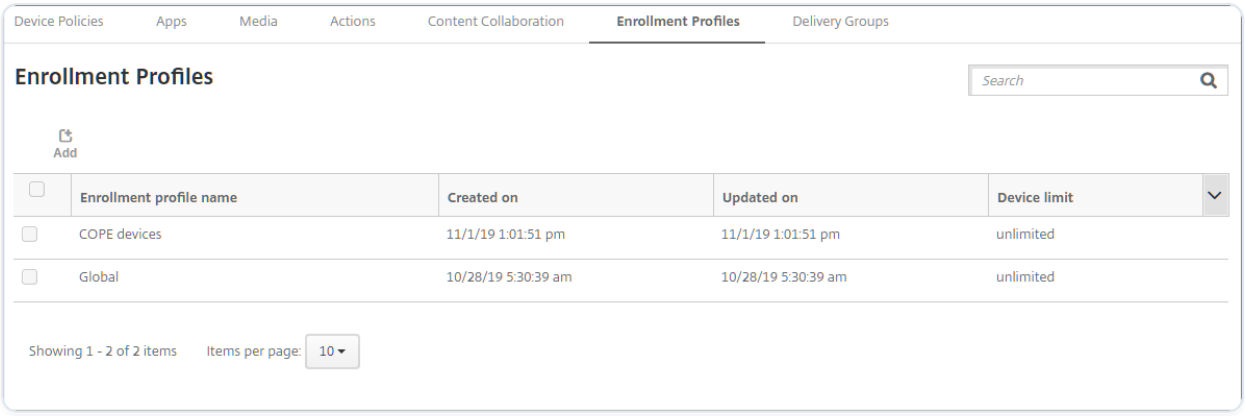
1. 在 XenMobile 控制台中，转至**配置 > 注册配置文件**。
2. 要添加注册配置文件，请单击**添加**。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置具有此配置文件的成员可以注册的设备数量。
4. 在**平台**下选择 **Android** 或单击**下一步**。此时将显示“注册配置”页面。
5. 将**管理**设置为**Android Enterprise**。将**设备所有者模式**设置为**完全托管（含工作配置文件）**。



6. **BYOD 工作配置文件**允许您配置注册配置文件，以将 BYOD 设备注册为工作配置文件设备。新设备和恢复出厂设置的设备将注册为带工作配置文件的完全托管设备。将**BYOD 工作配置文件**设置为**开**以允许将 BYOD 设备注册为工作配置文件设备。将**BYOD 工作配置文件**设置为**关**以将注册限制为专用设备。默认值为**关**。
7. 选择是否在 Citrix MAM 中注册设备。
8. 如果将**BYOD 工作配置文件**设置为**开**，请配置用户同意。要允许 BYOD 工作配置文件设备的用户在注册设备时拒绝设备管理，请将**允许用户拒绝设备管理**设置为**开**。

   如果**BYOD 工作配置文件**设置为**开**，则**允许用户拒绝设备管理**的默认值为**开**。如果**BYOD 工作配置文件**设置为**关**，则**允许用户拒绝设备管理**将被禁用。
9. 选择**分配（选项）**。将显示“交付组分配”屏幕。
10. 选择包含注册带工作配置文件的完全托管设备的管理员的交付组或多个交付组。然后单击**保存**。

将显示“注册配置文件”页面，其中包含您添加的配置文件。



添加旧设备的注册配置文件

Google 正在弃用设备管理的设备管理员模式。Google 鼓励客户以设备所有者模式或配置文件所有者模式管理所有 Android 设备。（请参阅 Google Android Enterprise 开发者指南中的设备管理员弃用。）

为支持此更改：

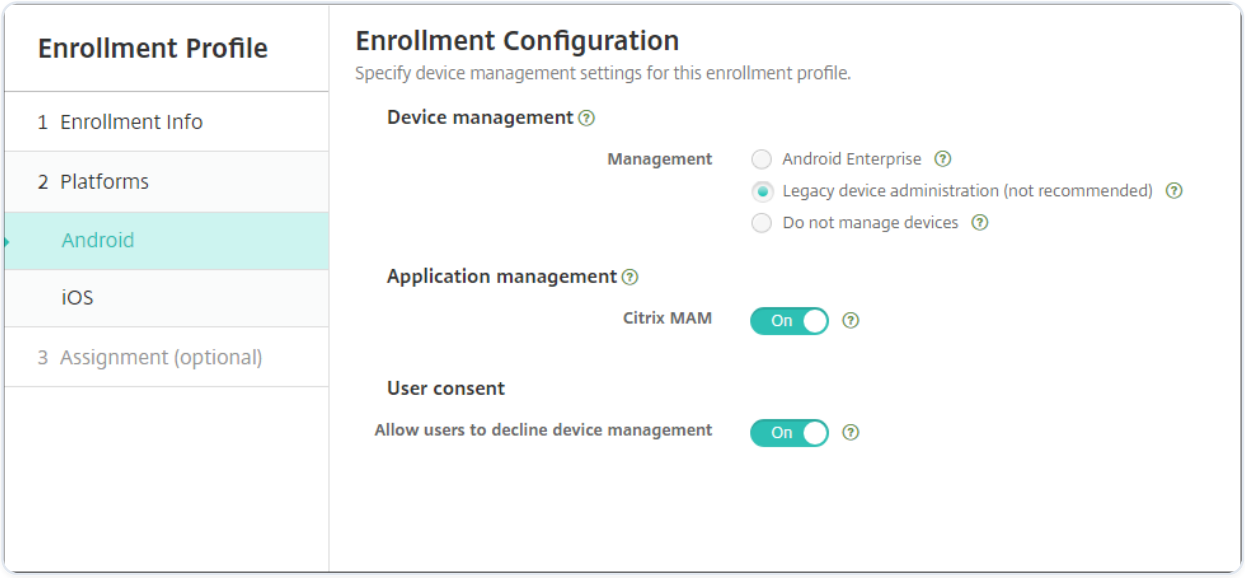
- Citrix 将 Android Enterprise 设为 Android 设备的默认注册选项。
- 如果为您的 XenMobile 部署启用了 Android Enterprise，所有新注册或重新注册的 Android 设备都将注册为 Android Enterprise 设备。

您的组织可能尚未准备好使用 Android Enterprise 开始管理旧版 Android 设备。在这种情况下，您可以继续在设备管理员模式下管理它们。对于已在设备管理员模式下注册的设备，XenMobile 将继续在设备管理员模式下管理它们。

为旧版设备创建注册配置文件，以允许新的 Android 设备注册使用设备管理员模式。

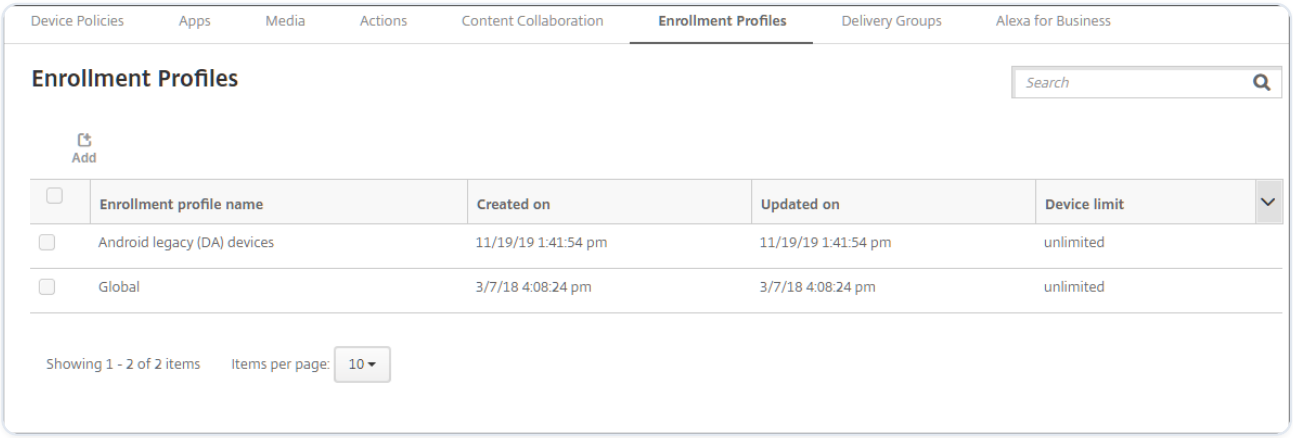
要为旧版设备创建注册配置文件：

1. 在 XenMobile 控制台中，转至 **Configure > Enrollment Profiles**。
2. 要添加注册配置文件，请单击 **Add**。在“注册信息”页面中，键入注册配置文件的名称。
3. 设置具有此配置文件的成员可以注册的设备数量。
4. 在 **Platforms** 下选择 **Android** 或单击 **Next**。“注册配置”页面随即显示。
5. 将 **管理** 设置为 **旧版设备管理（不推荐）**。单击 **下一步**。



6. 选择是否在 Citrix MAM 中注册设备。
7. 要允许用户在注册设备时拒绝设备管理，请将 **Allow users to decline device management** 设置为 **On**。默认值为 **On**。
8. 选择 **Assignment (options)**。“交付组分配”屏幕随即显示。
9. 选择包含注册专用设备的管理员的交付组。然后单击 **Save**。

“注册配置文件”页面随即显示您添加的配置文件。



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

预配 Android Enterprise 工作配置文件设备

Android Enterprise 工作配置文件设备以配置文件所有者模式注册。这些设备无需是新设备或恢复出厂设置的设备。BYOD 设备注册为工作配置文件设备。注册体验类似于 XenMobile 中的 Android 注册。用户从 Google Play 下载 Secure Hub 并注册其设备。

默认情况下，当设备作为工作配置文件设备注册到 Android Enterprise 时，设备上的**USB 调试和未知来源**设置处于禁用状态。

将设备作为工作配置文件设备注册到 Android Enterprise 时，请始终转到 Google Play。从那里，启用 Secure Hub 以显示在用户的个人资料中。

预配 Android Enterprise 全面管理设备

您可以将全面管理设备注册到您在前面部分中设置的部署中。全面管理设备是公司拥有的设备，以设备所有者模式注册。只有新设备或恢复出厂设置的设备才能以设备所有者模式注册。

您可以使用以下任何注册方法以设备所有者模式注册设备：

- **DPC 标识符令牌：** 使用此注册方法，用户在设置设备时输入字符 `afw#xenmobile`。`afw#xenmobile` 是 Citrix DPC 标识符令牌。此令牌将设备标识为由 XenMobile 管理，并从 Google Play 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 碰撞注册方法通过近场通信在两台设备之间传输数据。在新设备或恢复出厂设置的设备上，蓝牙、Wi-Fi 和其他通信模式均已禁用。NFC 是设备在此状态下可以使用的唯一通信协议。请参阅使用 NFC 碰撞注册设备。
- **QR 码：** QR 码注册可用于注册不支持 NFC 的分布式设备群，例如平板电脑。QR 码注册方法通过从设置向导扫描 QR 码来设置和配置设备配置文件模式。请参阅使用 QR 码注册设备。
- **零接触：** 零接触注册允许您配置设备在首次开机时自动注册。零接触注册在某些运行 Android 9.0 或更高版本的 Android 设备上受支持。请参阅零接触注册。
- **Google 帐户：** 用户输入其 Google 帐户凭据以开始预配过程。此选项适用于使用 Google Workspace 的企业。

使用 Citrix DPC 标识符令牌注册设备

用户在首次设置时打开新设备或恢复出厂设置的设备后，在提示输入 Google 帐户时输入 `afw#xenmobile`。此操作会下载并安装 Secure Hub。然后，用户按照 Secure Hub 设置提示完成注册。

这种注册方法推荐给大多数客户，因为最新版本的 Secure Hub 是从 Google Play 商店下载的。与其他注册方法不同，您无需从 XenMobile Server 提供 Secure Hub 供下载。

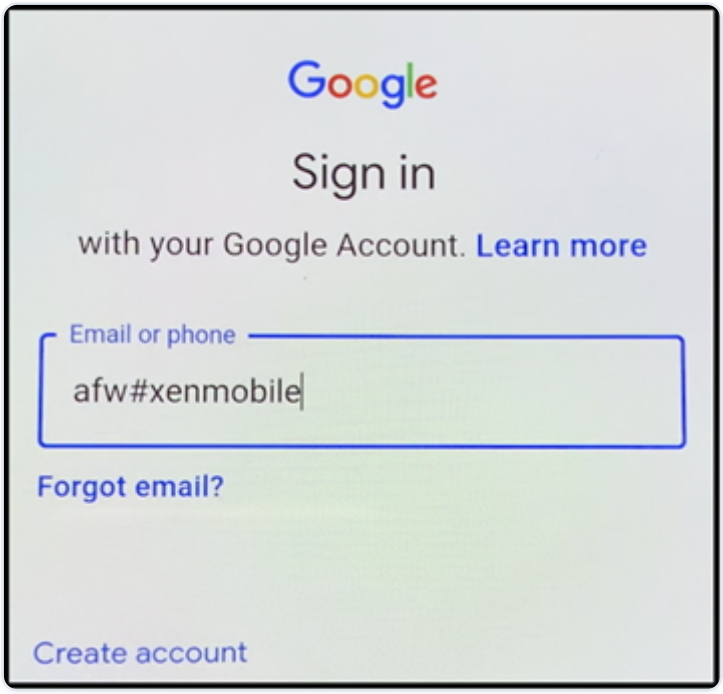
系统要求

- 支持所有运行 Android 操作系统的 Android 设备。

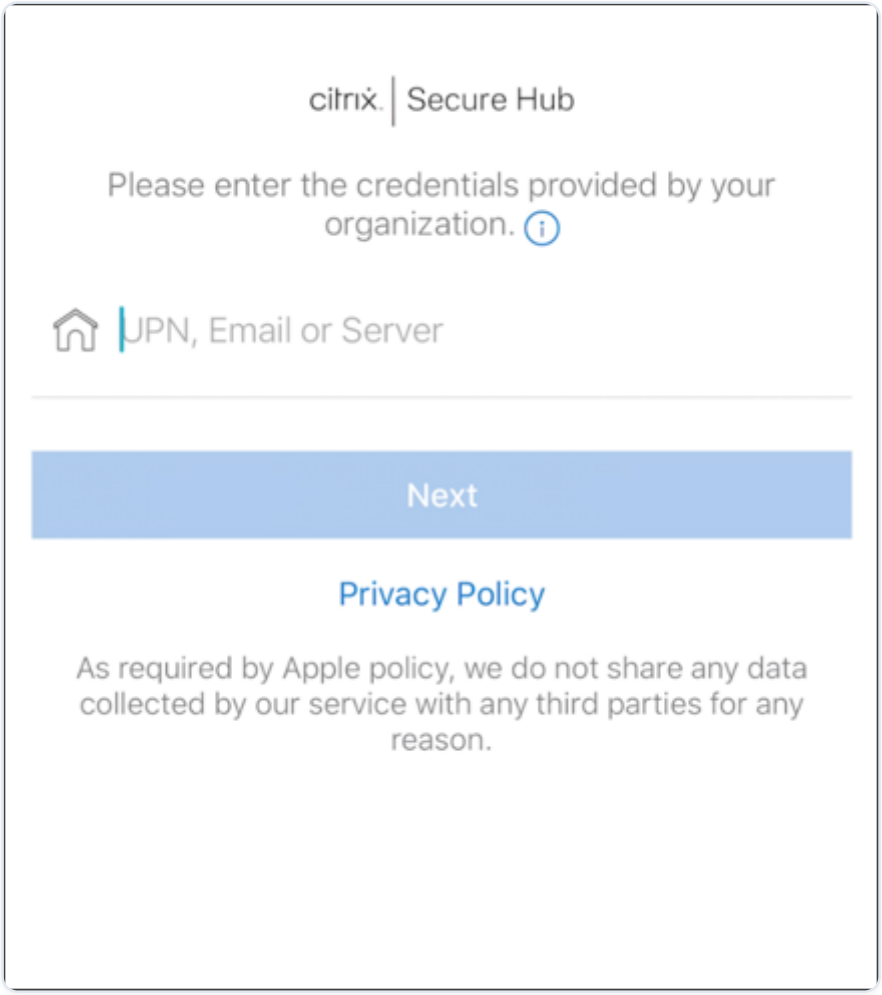
注册设备

1. 启动新设备或已恢复出厂设置的设备。
2. 初始设备设置加载并提示输入 Google 帐户。如果设备加载了设备主屏幕，请检查通知栏中是否有“**完成设置**”通知。

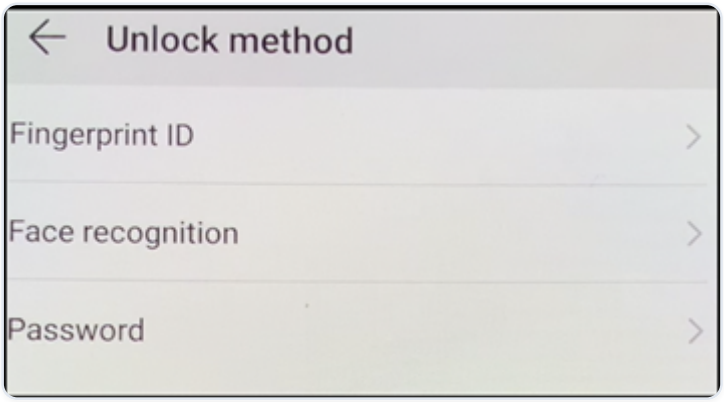
3. 在“**电子邮件或电话**”字段中输入 `afw#xenmobile`。



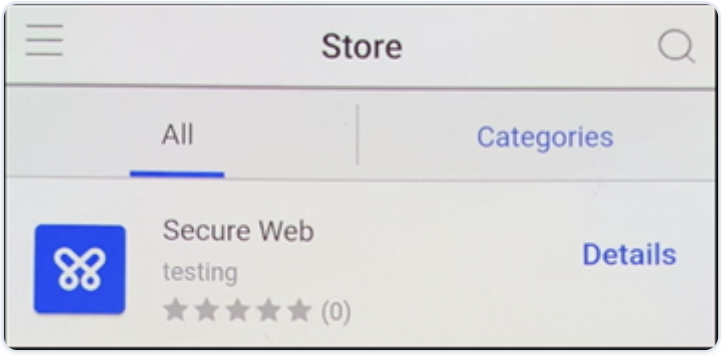
4. 在提示安装 Secure Hub 的 Android Enterprise 屏幕上，点击“**安装**”。
5. 在 Secure Hub 安装程序屏幕上，点击“**安装**”。
6. 对于所有应用权限请求，点击“**允许**”。
7. 点击“**接受并继续**”以安装 Secure Hub 并允许其管理设备。
8. Secure Hub 现已安装并显示在默认注册屏幕上。在此示例中，未设置 AutoDiscovery。如果已设置，用户可以输入其用户名/电子邮件，系统将为其找到服务器。否则，请输入环境的注册 URL，然后点击“**下一步**”。



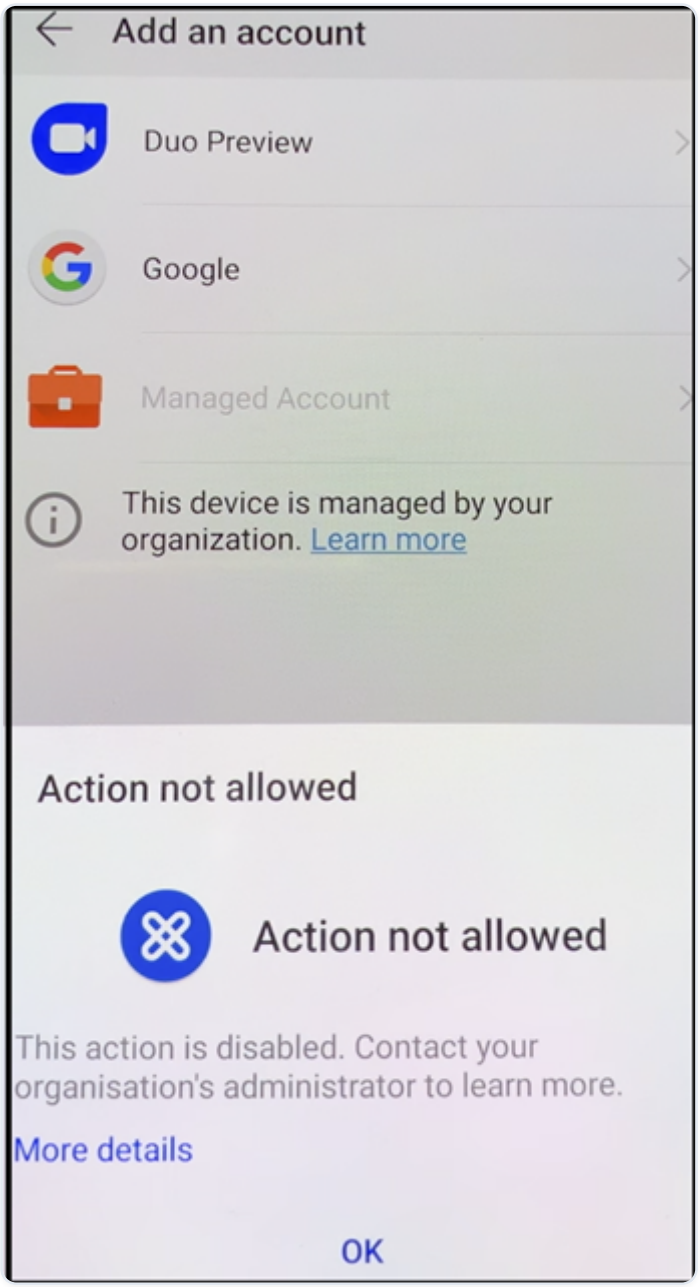
9. XenMobile 的默认配置允许用户选择是使用 MAM 还是 MDM+MAM。如果出现此提示，请点击“**是，注册**”以选择 MDM+MAM。
10. 输入用户名和密码，然后点击 **下一步**。
11. 系统提示用户配置设备密码。点击 **设置** 并输入密码。
12. 系统提示用户配置工作资料解锁方法。在此示例中，点击 **密码**，点击 **PIN**，然后输入 PIN。



13. 设备现在位于 Secure Hub 的 **我的应用程序** 登录屏幕。点击 **从商店添加应用程序**。
14. 要添加 Secure Web，请点击 **Secure Web**。



15. 点击 **添加**。
16. Secure Hub 会将用户定向到 Google Play 商店以安装 Secure Web。点击 **安装**。
17. 安装 Secure Web 后，点击 **打开**。在地址栏中输入内部站点的 URL，并验证页面是否加载。
18. 在设备上转到 **设置 > 帐户**。观察到 **托管帐户** 无法修改。共享屏幕或远程调试的开发人员选项也被阻止。



使用 NFC 碰撞注册设备

要使用 NFC 碰撞将设备注册为完全托管设备，需要两台设备：一台已重置为出厂设置，另一台运行 XenMobile Provisioning Tool。

系统要求和先决条件

- 支持的 Android 设备。
- 配置为 Android Enterprise 完全托管设备的新设备或恢复出厂设置的设备。您可以在本文后面找到完成此先决条件的步骤。
- 另一台具有 NFC 功能的设备，运行已配置的预配工具。预配工具可在 Secure Hub 中或 Citrix 下载页面 上获取。

每台设备只能有一个 Android Enterprise 配置文件，由 Secure Hub 管理。每台设备只允许一个配置文件。尝试添加第二个 DPC 应用程序会删除已安装的 Secure Hub。

通过 NFC 碰撞传输的数据

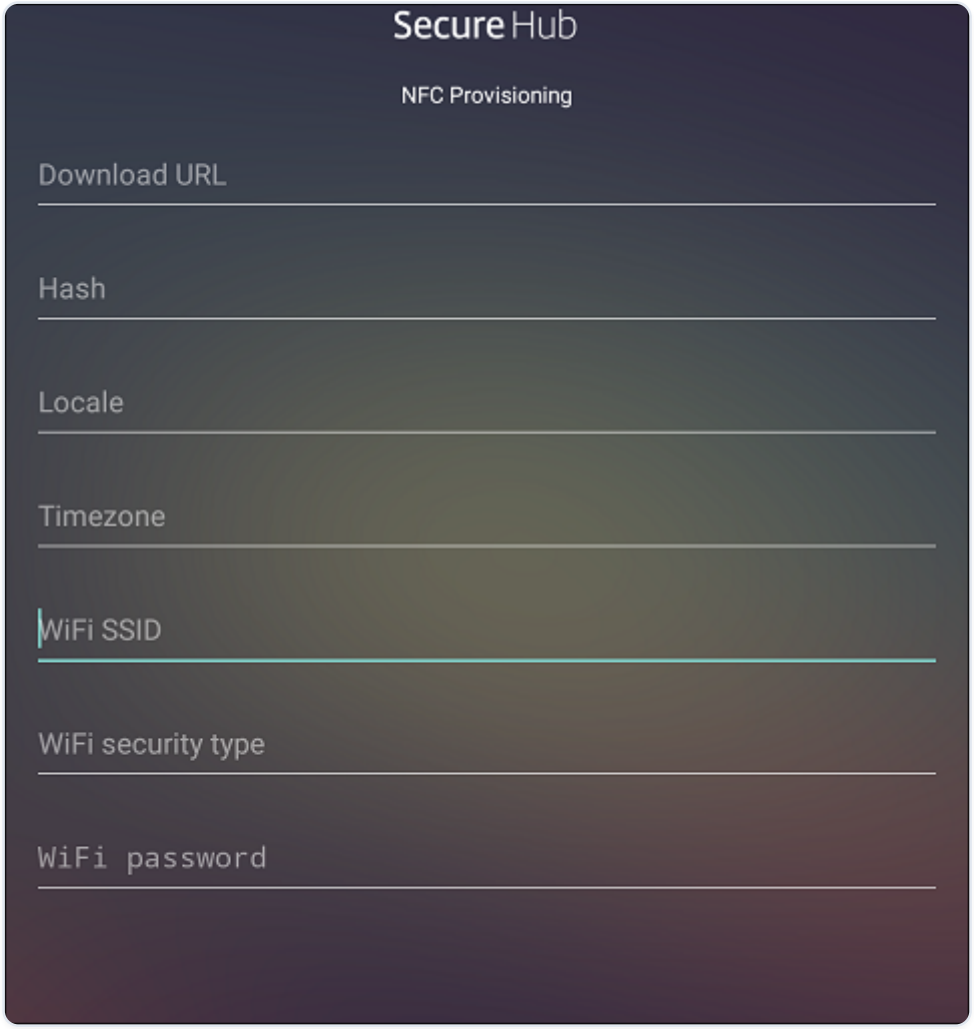
预配恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以初始化 Android Enterprise：

- 作为设备所有者的 DPC 应用程序的包名称（在本例中为 Secure Hub）。
- 设备可从中下载 DPC 应用程序的内网/互联网位置。
- DPC 应用程序的 SHA1 哈希值，以验证下载是否成功。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备可以连接并下载 DPC 应用程序。注意：Android 现在不支持此步骤的 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

当两台设备碰撞时，预配工具中的数据将发送到恢复出厂设置的设备。然后，该数据用于下载具有管理员设置的 Secure Hub。如果您不输入时区和位置值，Android 会自动在新设备上配置这些值。

配置 XenMobile 预配工具

在进行 NFC 碰撞之前，您必须配置预配工具。此配置随后在 NFC 碰撞期间传输到恢复出厂设置的设备。



您可以在必填字段中输入数据，也可以使用文本文件填充它们。下一个步骤描述了如何配置文本文件，并包含每个字段的描述。应用在您输入信息后不会保存，因此您可能需要创建一个文本文件来保存信息以备将来使用。

使用文本文件配置配置工具

将文件命名为 nfcprovisioning.txt，并将其放置在设备的 SD 卡上的 `/sdcard/` 文件夹中。应用随后可以读取该文本文件并填充值。

文本文件必须包含以下数据：

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

此行是 EMM 提供商应用的内网/互联网位置。在恢复出厂设置的设备通过 NFC 碰撞连接到 Wi-Fi 后，设备必须能够访问此位置才能进行下载。此 URL 是一个常规 URL，无需特殊格式。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>`

此行是 EMM 提供商应用的校验和。此校验和用于验证下载是否成功。获取校验和的步骤将在本文后面讨论。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

此行是运行配置工具的设备上已连接的 Wi-Fi SSID。

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

支持的值为 WEP 和 WPA2。如果 Wi-Fi 未受保护，此字段必须为空。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

如果 Wi-Fi 未受保护，此字段必须为空。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

输入语言和国家/地区代码。语言代码是 ISO 639-1 定义的两位小写 ISO 语言代码（例如 en）。国家/地区代码是 ISO 3166-1 定义的两位大写 ISO 国家/地区代码（例如 US）。例如，输入 en_US 表示在美国使用的英语。如果不输入任何代码，国家/地区和语言将自动填充。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

设备运行所在的时区。键入 Olson 区域/位置形式的名称。例如，America/Los_Angeles 表示太平洋时间。如果不输入名称，时区将自动填充。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

此数据不是必需的，因为该值已作为 Secure Hub 硬编码到应用程序中。此处提及仅为完整性考虑。

如果存在受 WPA2 保护的 Wi-Fi，则完成的 nfcprovisioning.txt 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://
www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

如果存在未受保护的 Wi-Fi，则完成的 nfcprovisioning.txt 文件可能如下所示：

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

获取 Citrix Secure Hub 的校验和

Secure Hub 的校验和是一个常量值：`qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。要下载 Secure Hub 的 APK 文件，请使用以下 Google Play 商店链接：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

获取应用程序校验和

先决条件：

- 来自 Android SDK Build Tools 的 **apksigner** 工具
- OpenSSL 命令行

要获取任何应用程序的校验和，请按照以下步骤操作：

1. 从 Google Play 商店下载应用程序的 APK 文件。
2. 在 OpenSSL 命令行中，导航到 **apksigner** 工具：`android-sdk/build-tools/<version>/apksigner` 并键入以下内容：

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   ```

   该命令返回一个有效的校验和。
3. 要生成二维码，请在 `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM` 字段中输入校验和。例如：

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
```

```
"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"

   }

}
```

使用的库

预配工具在其源代码中使用了以下库：

- Google 在 Apache 2.0 许可证下提供的 v7 `appcompat` 库、设计支持库和 v7 Palette 库

  有关信息，请参阅支持库功能指南。
- Jake Wharton 在 Apache 2.0 许可证下提供的 Butter Knife

使用二维码注册设备

要使用二维码注册完全托管设备，您可以通过创建 JSON 并将其转换为二维码来生成二维码。设备摄像头会扫描二维码以注册设备。

系统要求

- 支持所有运行 Android 9.0 及更高版本的 Android 设备。

从 JSON 创建二维码

创建一个包含以下字段的 JSON。

这些字段是必需的：

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

值：com.zenprise/com.zenprise.configuration.AdminFunction

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

值： qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

值：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

以下字段是可选的：

- **android.app.extra.PROVISIONING_LOCALE：** 输入语言和国家/地区代码。

  语言代码是 ISO 639-1 定义的两位小写 ISO 语言代码（例如 en）。国家/地区代码是 ISO 3166-1 定义的两位大写 ISO 国家/地区代码（例如 US）。例如，输入 en_US 表示在美国使用的英语。

- **android.app.extra.PROVISIONING_TIME_ZONE：** 设备运行所在的时区。

  键入 Olson 格式的区域/位置名称。例如，America/Los_Angeles 表示太平洋时间。如果不输入，时区将自动填充。

- **android.app.extra.PROVISIONING_LOCAL_TIME：** 自 Epoch 以来的毫秒数。

  Unix 纪元（或 Unix 时间、POSIX 时间或 Unix 时间戳）是自 January 1, 1970（UTC/GMT 午夜）以来经过的秒数。该时间不包括闰秒（在 ISO 8601 中：1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION：** 设置为 **true** 可在配置文件创建期间跳过加密。设置为 **false** 可在配置文件创建期间强制加密。

典型的 JSON 如下所示：

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "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
}
```

使用任何 JSON 验证工具（例如 https://jsonlint.com）验证创建的 JSON。使用任何在线 QR 码生成器（例如 https://www.qr-code-generator.com）将该 JSON 字符串转换为 QR 码。

此二维码由恢复出厂设置的设备扫描，以将设备注册为完全托管设备。

注册设备

启动新设备或恢复出厂设置的设备后：

1. 在欢迎屏幕上轻触屏幕六次，以启动二维码注册流程。
2. 出现提示时，连接到 Wi-Fi。二维码中（编码在 JSON 中）Secure Hub 的下载位置可通过此 Wi-Fi 网络访问。

设备成功连接到 Wi-Fi 后，它会从 Google 下载一个二维码阅读器并启动摄像头。

3. 将摄像头对准二维码以扫描代码。

   Android 从二维码中的下载位置下载 Secure Hub，验证签名证书签名，安装 Secure Hub 并将其设置为设备所有者。

有关详细信息，请参阅此适用于 Android EMM 开发人员的 Google 指南：`<https://developers.google.com/android/work/prov-devices#qr_code_method>`。

零接触注册

零接触注册允许您在设备首次开机时将其设置为完全托管设备。

您的设备经销商会在 Android 零接触门户（一个允许您将配置应用于设备的在线工具）上为您创建一个帐户。使用 Android 零接触门户，您可以创建一个或多个零接触注册配置，并将这些配置应用于分配给您帐户的设备。当您的用户启动这些设备时，设备会自动注册到 XenMobile。分配给设备的配置定义了其自动注册过程。

系统要求

- 零接触注册支持从 Android 9.0 开始。

来自经销商的设备和帐户信息

- 符合零接触注册条件的设备是从企业经销商或 Google 合作伙伴处购买的。有关 Android Enterprise 零接触合作伙伴列表，请参阅 Android 网站。
- 由您的经销商创建的 Android Enterprise 零接触门户帐户。
- 由您的经销商提供的 Android Enterprise 零接触门户帐户登录信息。

创建零接触配置

创建零接触配置时，请包含自定义 JSON 以指定配置的详细信息。

使用此 JSON 配置设备以在您指定的 XenMobile Server 上注册。在此示例中，将“URL”替换为您的服务器 URL。

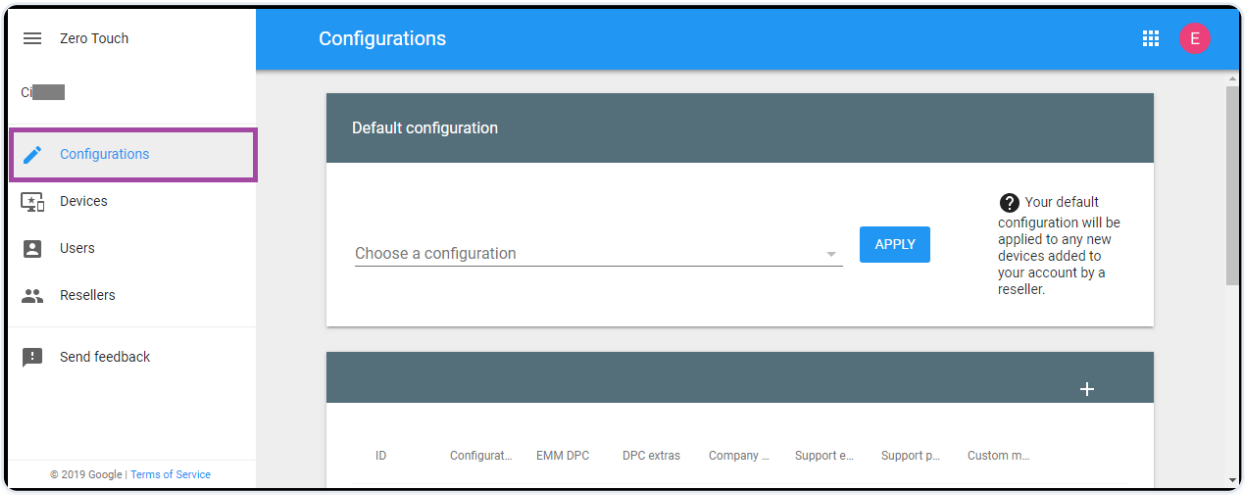
```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

  {

        "serverURL":"URL",
```

```
    }

}
```

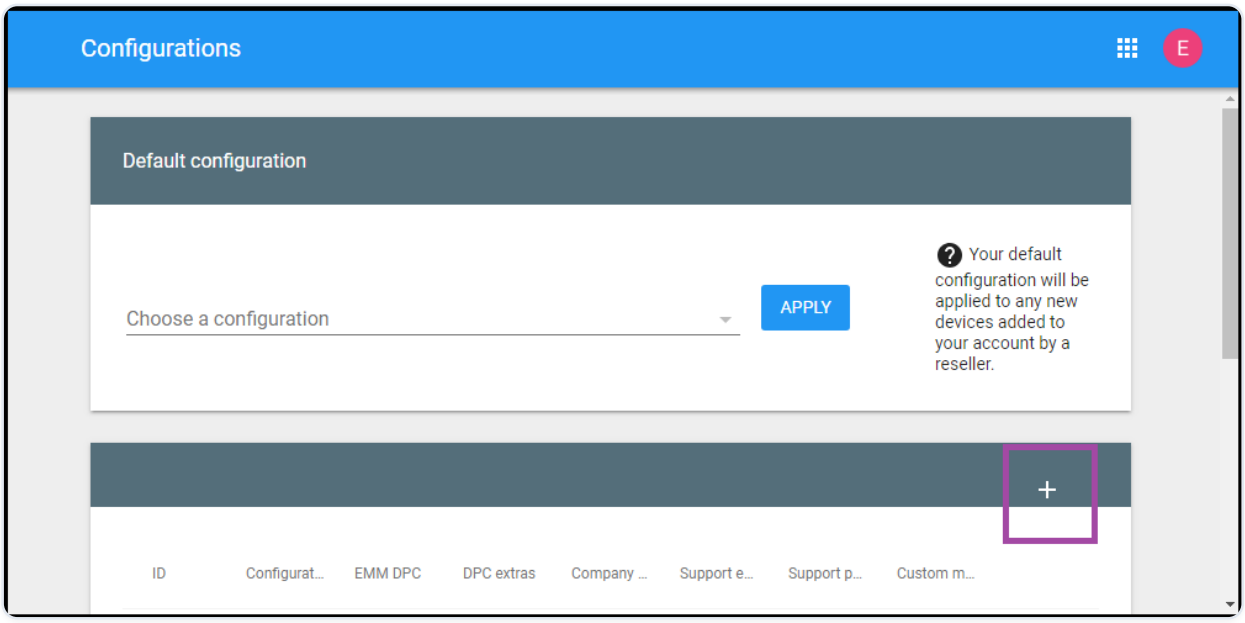
您可以使用包含更多参数的可选 JSON 来进一步自定义配置。此示例指定了 XenMobile Server 以及使用此配置的设备用于登录服务器的用户名和密码。

```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

     {

         "serverURL":"URL",

         "xm_username":"username",

         "xm_password":"password"

     }

       }
```

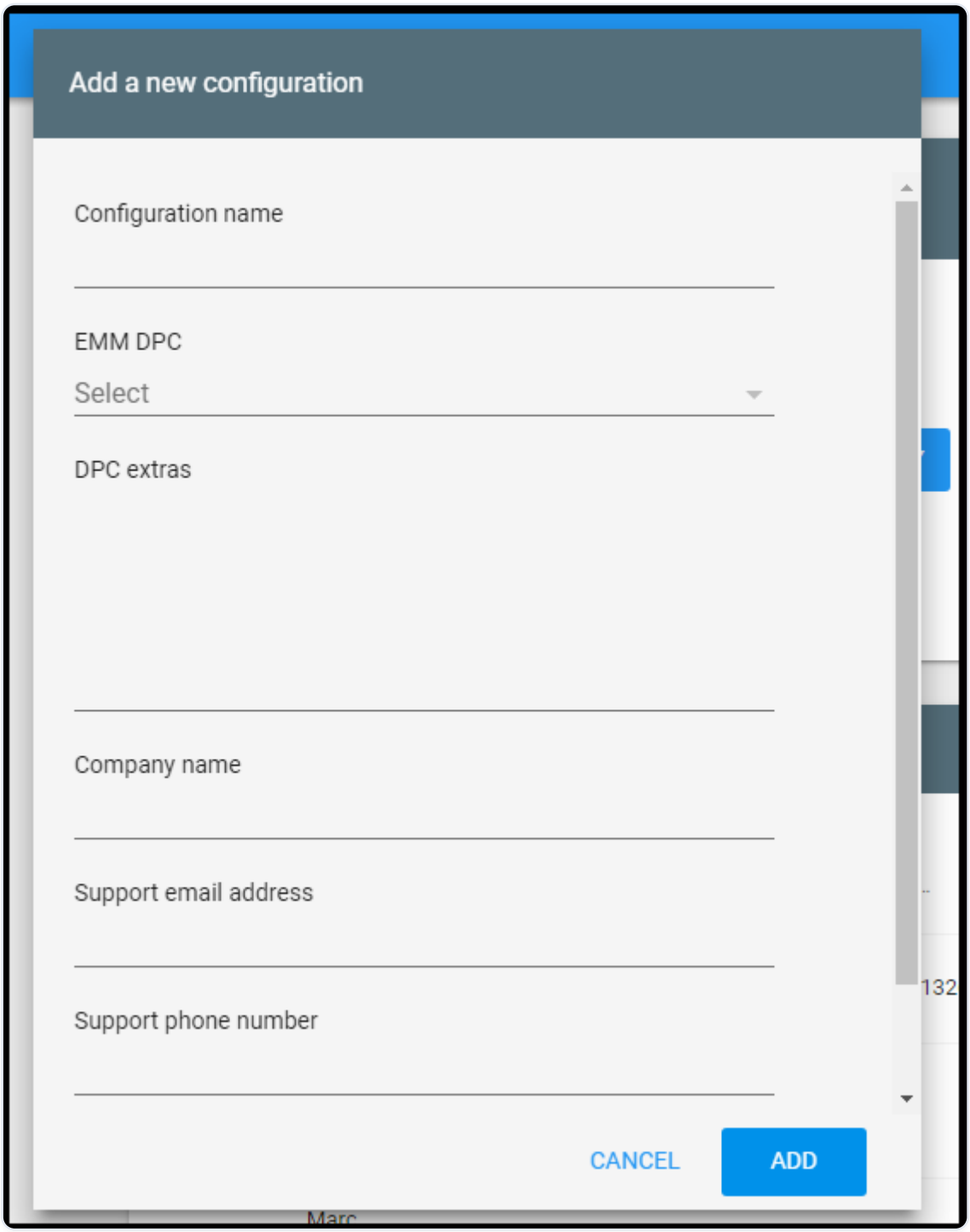
1. 访问 Android 零接触门户 https://partner.android.com/zerotouch。使用您的零接触设备经销商提供的帐户信息登录。
2. 单击 **Configuration**。



3. 单击配置表上方的 +。


Configurations
E
Default configuration
Choose a configuration
APPLY
Your default configuration will be applied to any new devices added to your account by a reseller.
+
ID
Configurat...
EMM DPC
DPC extras
Company ...
Support e...
Support p...
Custom m...

4. 在出现的配置窗口中输入您的配置信息。



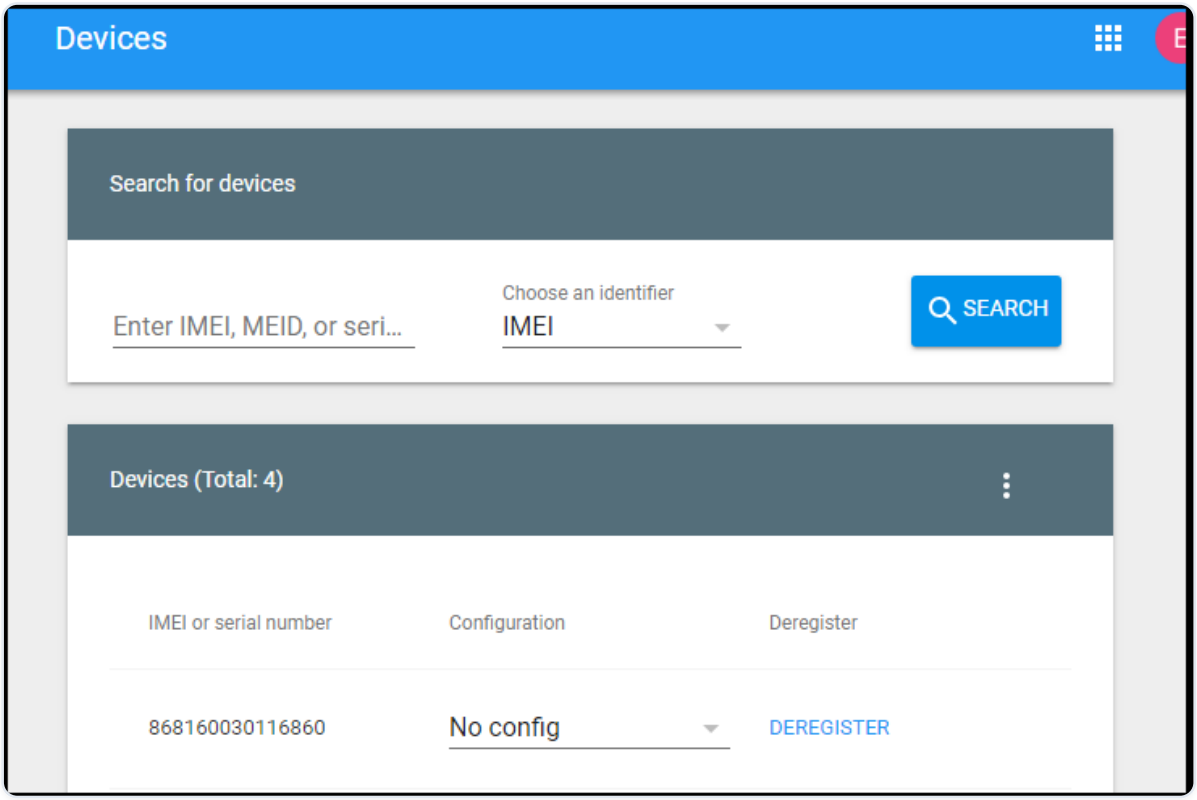
- **配置名称：** 输入您为此配置选择的名称。
- **EMM 设备策略控制器**：选择 **Citrix Secure Hub**。
- **DPC 额外项：** 将您的自定义 JSON 文本粘贴到此字段中。
- **公司名称：** 输入您希望在设备预配期间显示在 Android Enterprise 零接触设备上的名称。
- **支持电子邮件地址：** 键入用户可以联系以获取帮助的电子邮件地址。此地址在设备预配之前显示在您的 Android Enterprise 零接触设备上。

- **支持电话号码：** 键入用户可以联系以获取帮助的电话号码。此电话号码在设备预配之前显示在您的 Android Enterprise 零接触设备上。
- **自定义消息：** （可选）添加一两句话，以帮助用户与您联系，或向他们提供有关其设备情况的更多详细信息。此自定义消息在设备预配之前显示在您的 Android Enterprise 零接触设备上。

5. 单击**添加**。
6. 要创建更多配置，请重复步骤 2 到 4。
7. 要将配置应用于设备：

   a. 在 Android 零接触门户中，单击**设备**。

   b. 在设备列表中找到该设备，然后选择要分配给它的配置。



   c. 单击**更新**。

您可以使用 CSV 文件将配置应用于许多设备。

有关如何将配置应用于许多设备的信息，请参阅 Android Enterprise 帮助主题 适用于 IT 管理员的零接触注册。此 Android Enterprise 帮助主题包含有关如何管理配置并将其应用于设备的更多信息。

预配专用 Android Enterprise 设备

专用 Android Enterprise 设备是完全托管的设备，专门用于实现单个用例。专用设备也称为企业自有单用途 (COSU) 设备。您将这些设备限制为执行此用例所需的一个应用程序或一小组应用程序。您还可以阻止用户启用其他应用程序或在设备上执行其他操作。

使用用于其他完全托管设备的任何注册方法注册专用设备，如 预配 Android Enterprise 完全托管设备 中所述。预配专用设备在注册前需要更多设置。

要预配专用设备：

- 为允许将专用设备注册到 XenMobile 部署的 XenMobile 管理员添加注册配置文件。请参阅创建注册配置文件。
- 允许专用设备访问您希望其访问的应用程序。
- （可选）将允许的应用程序设置为允许锁定任务模式。当应用程序处于锁定任务模式时，用户打开应用程序时，该应用程序会固定到设备屏幕。不显示主页按钮，并且禁用返回按钮。用户通过应用程序中编程的操作（例如注销）退出应用程序。
- 在您添加的注册配置文件中注册每个设备。

系统要求

- 对专用设备注册的支持始于 Android 6.0。

允许应用程序并设置锁定任务模式

Kiosk 设备策略允许您允许应用程序并设置锁定任务模式。默认情况下，Secure Hub 和 Google Play 服务是允许的。

要添加 Kiosk 策略：

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**Kiosk**。此时将显示**Kiosk 策略**页面。
4. 在“平台”下，选择**Android Enterprise**。清除其他平台。
5. 在“策略信息”窗格中，键入**策略名称**和可选的**描述**。
6. 单击**下一步**，然后单击**添加**。
7. 要允许应用并允许或拒绝该应用的锁定任务模式：

   从列表中选择要允许的应用。

选择“**允许**”以在用户启动应用时将应用固定到设备屏幕。选择“**拒绝**”以不固定应用。默认值为“**允许**”。

设备策略配置屏幕(/en-us/xenmobile/server/media/configure-device-policies-kiosk-android-enterprise.png)

8. 单击“**保存**”。
9. 要允许另一个应用并允许或拒绝该应用的锁定任务模式，请单击“**添加**”。
10. 配置部署规则并选择交付组。有关详细信息，请参阅设备策略。

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**”。

   注册配置文件配置屏幕(/en-us/xenmobile/server/media/android-enterprise-enrollment-profile-do-multimode.png)

4. 选择“**分配（选项）**”。此时将显示“交付组分配”屏幕。
5. 选择包含注册专用设备的管理员的交付组。然后单击“**保存**”。

如果您在注册配置文件中启用了“**BYOD 工作配置文件**”，则非全新或未恢复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。

配置带工作资料的 Android Enterprise 全面管理设备 (COPE 设备)

带工作资料的全面管理设备（以前称为 COPE 设备）是公司拥有的设备，用于工作和个人目的。您的组织管理整个设备。您可以对设备应用一组策略，并对工作资料应用另一组单独的策略。

在 XenMobile 控制台中，带工作资料的全面管理设备显示以下术语：

- 设备所有权为“公司”.
- 设备 Android Enterprise 安装类型为“企业所有者个人启用”.

系统要求

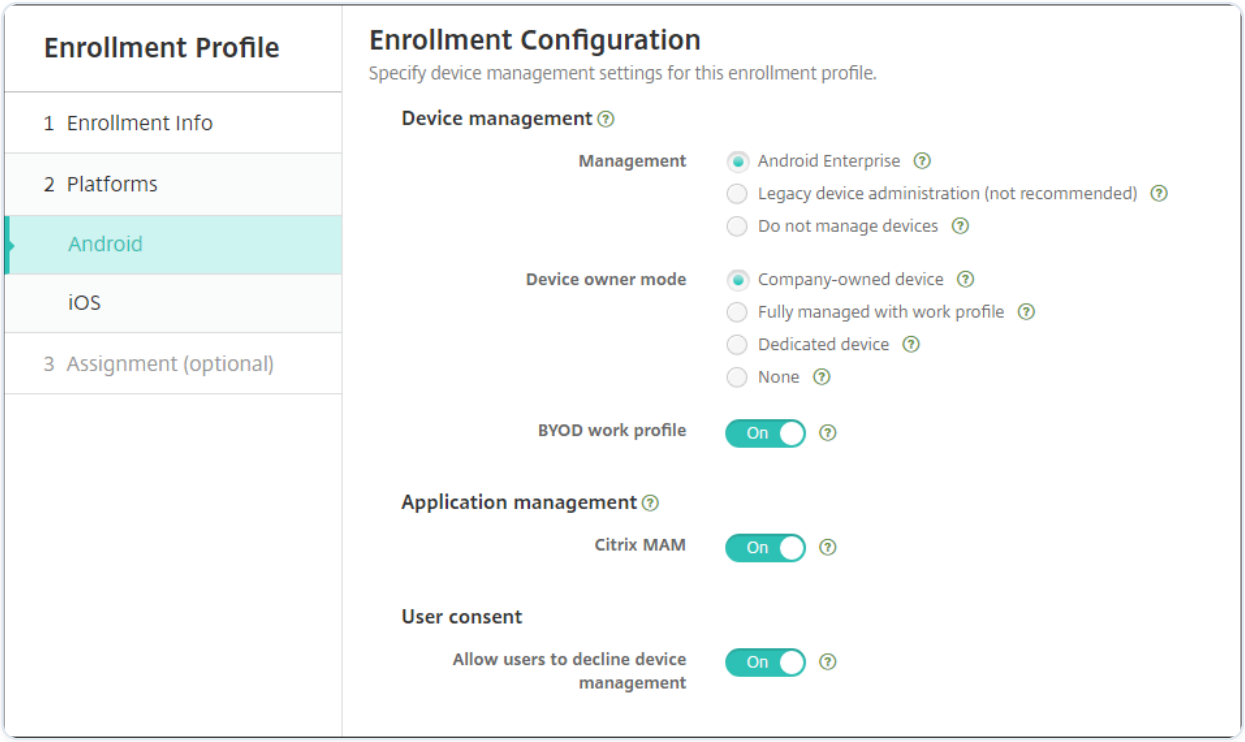
- 对注册带工作资料的全面管理设备的支持始于 Android 9.0 到 Android 10.x。

为带工作资料的全面管理设备添加注册配置文件

创建用于注册带工作资料的全面管理设备的注册配置文件。分配给此注册配置文件的交付组中的管理员可以注册带工作资料的全面管理设备。为确保这些管理员可以注册所有必需的设备，请为他们

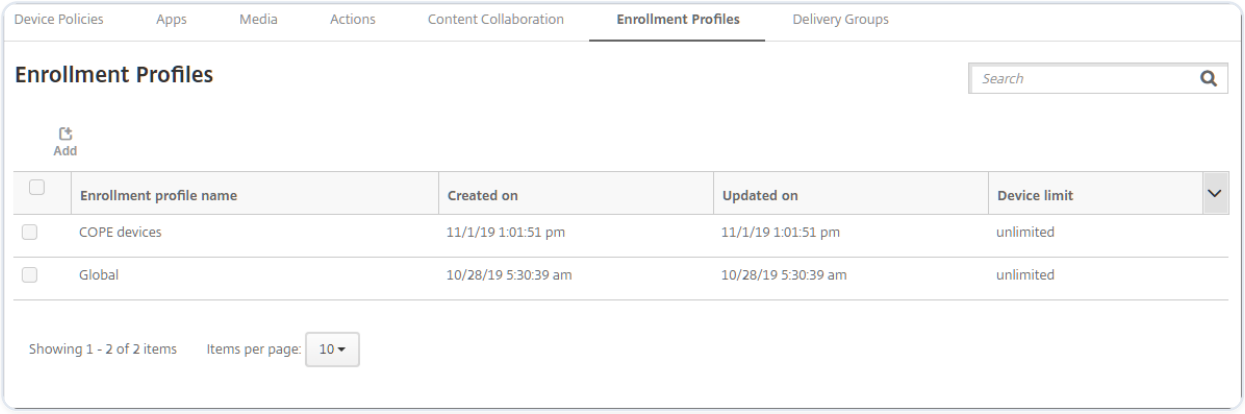
创建一个注册配置文件，其中允许每个用户拥有无限数量的设备。将此配置文件分配给包含注册带工作资料的全面管理设备的管理员的交付组。

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。确保将具有此配置文件的成员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**。“注册配置”页面随即显示。
4. 将 **注册类型** 设置为以下选项之一：
   - **全面管理/工作资料：** 新设备或恢复出厂设置的设备将注册为全面管理。BYOD 设备仅注册由您管理的工作资料。
   - **COPE/工作资料：** 新设备或恢复出厂设置的设备将注册为带工作资料的全面管理。BYOD 设备仅注册由您管理的工作资料。



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. 选择包含注册专用设备的管理员的交付组或多个交付组。然后单击“**保存**”。

   此时将显示“注册配置文件”页面，其中包含您添加的配置文件。



如果用户属于具有不同注册配置文件的多个交付组，则交付组的名称将决定所使用的注册配置文件。XenMobile 会选择按字母顺序排列的交付组列表中最后一个出现的交付组。

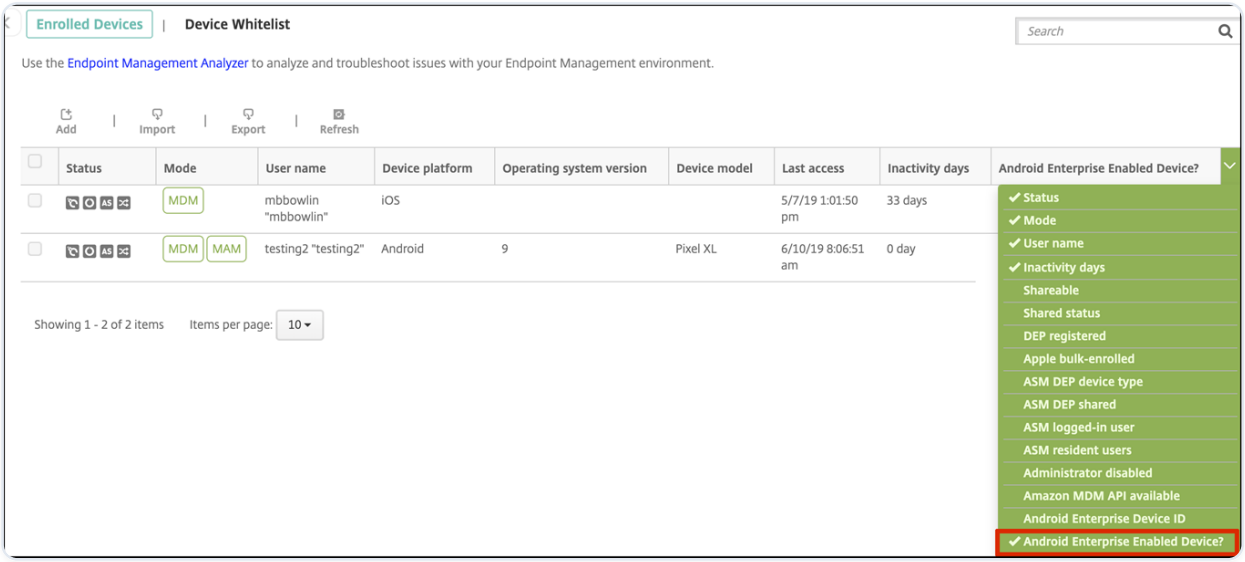
注册设备

全新设备和恢复出厂设置的设备将作为具有工作资料的完全托管设备进行注册，可使用 DPC 标识符令牌、近场通信 (NFC) 碰撞或二维码方法。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 码注册设备。

未全新或恢复出厂设置的设备将注册为工作资料设备，如预配 Android Enterprise 工作资料设备中所述。

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. 通过单击此页面上表格右侧的菜单，添加“**Android Enterprise 已启用设备?**”列。



3. 要查看可用的安全操作，请选择一个完全托管的设备，然后单击“**保护**”。当设备完全托管时，“**完全擦除**”操作可用，但“**选择性擦除**”不可用。此差异是因为设备仅允许来自托管 Google Play 商店的应用程序。用户无法从公共商店安装应用程序。您的组织管理设备上的所有内容。

配置 Android Enterprise 设备和应用程序策略

有关设备和应用程序级别控制的策略概述，请参阅 适用于 Android Enterprise 的受支持设备策略和 MDX 策略。

有关策略的注意事项：

- **数据丢失防护：** XenMobile MAM 容器技术通过加密和其他移动数据丢失防护 (DLP) 技术保护应用程序。使用 Citrix MAM SDK 或 MDX Toolkit 启用应用程序的 MDX 功能。
- **设备限制：** 数十种设备限制允许您控制以下功能：
  - 设备摄像头的使用
  - 在工作配置文件和个人配置文件之间复制和粘贴的使用
- **每应用 VPN：** 使用“托管配置”设备策略为 Android Enterprise 配置 VPN 配置文件。
- **电子邮件策略：** 我们建议使用“托管配置”设备策略来配置应用程序。

此表列出了适用于 Android Enterprise 设备的所有设备策略。

> **重要：**
>
> 对于注册 Android Enterprise 并使用 MDX 应用程序的设备：您可以通过 MDX 和 Android Enterprise 控制某些设置。对 MDX 使用限制最少的策略设置，并通过 Android Enterprise 控制策略。

Android Enterprise 应用程序权限	托管配置	应用程序清单
应用程序卸载	自动更新托管应用	控制操作系统更新
凭据	自定义 XML	Exchange 邮件
文件	锁屏管理	自助服务终端
位置	密码	限制
Samsung MDM 许可证密钥	计划	Wi-Fi 网络
XenMobile 选项		

具有工作资料的完全托管设备（COPE 设备）的设备策略

对于具有工作资料的完全托管设备（COPE 设备），某些设备策略可用于对整个设备和工作资料应用单独的设置。您可以使用其他设备策略仅对整个设备或仅对具有工作资料的完全托管设备的工作资料应用设置。

策略	适用于
Android Enterprise 应用程序权限	工作资料
托管配置	工作资料
应用程序清单	工作资料
应用程序卸载	工作资料
自动更新托管应用程序	工作资料
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
邮件交换	不适用

策略	适用于
文件	工作配置文件
锁屏管理	设备和工作配置文件
自助服务终端	不适用
位置	设备（仅限位置模式）
密码	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
无线网络	设备
XenMobile 选项	工作配置文件

另请参阅，适用于 Android Enterprise 的受支持设备策略和 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
定位	是	是
锁定	是	是
锁定并重置密码	否	是
通知（响铃）	是	是
吊销	是	是

安全操作	工作配置文件	完全托管
选择性擦除	是	否

安全操作说明

- 定位安全操作会失败，除非位置设备策略将设备的定位模式设置为**高精度**或**省电**。请参阅位置设备策略。
- 在运行早于 Android 9.0 版本的 Android 系统的工作配置文件设备上：
  - 锁定和重置密码操作不受支持。
- 在 Android 9.0 或更高版本的工作配置文件设备上：
  - 发送的密码会锁定工作配置文件。设备本身不会被锁定。
  - 如果工作配置文件上未设置密码：
    - 如果未发送密码，或者发送的密码不符合密码要求：设备将被锁定。
  - 如果工作配置文件上设置了密码：
    - 如果未发送密码，或者发送的密码不符合密码要求：工作配置文件将被锁定，但设备本身不会被锁定。
- 在具有工作配置文件的完全托管设备（COPE 设备）上：
  - 您可以将“锁定”安全操作分别应用于设备或工作配置文件

取消注册 Android Enterprise 企业

如果您不再希望使用您的 Android Enterprise 企业，可以取消注册该企业。

> **警告：**

> 取消注册企业后，已通过该企业注册的设备上的 Android Enterprise 应用程序将重置为默认状态。Google 不再管理这些设备。如果您注册新的 Android Enterprise 企业，则必须从托管 Google Play 批准新组织的应用程序。然后，您可以从 XenMobile 控制台更新应用程序。

> Android Enterprise 企业取消注册后：

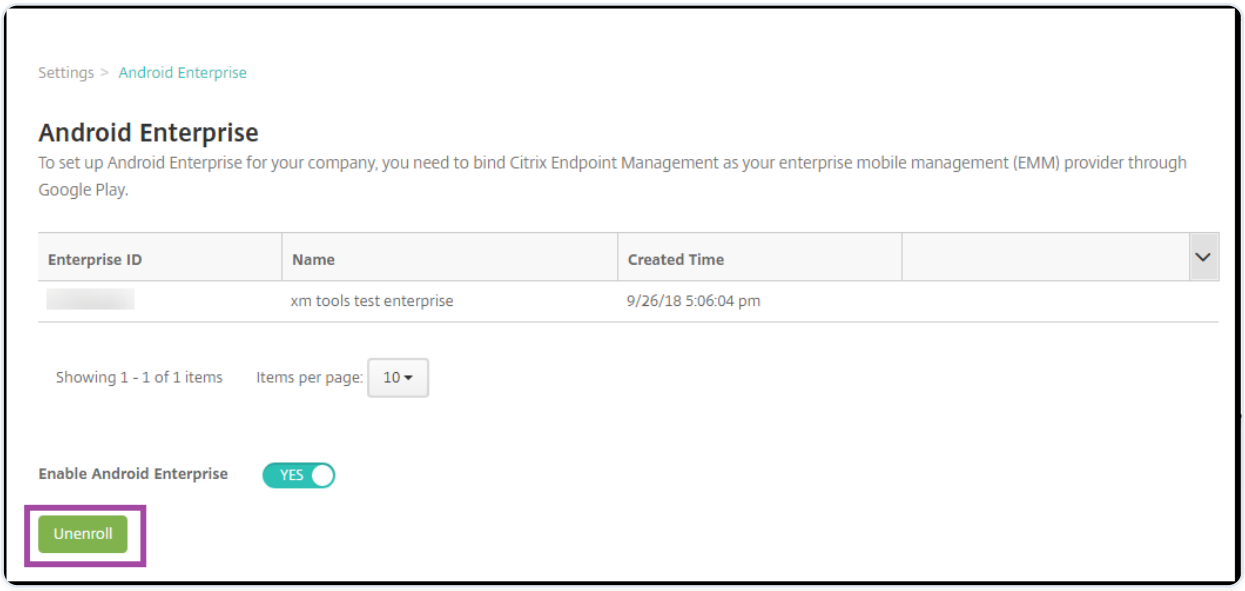
- 通过企业注册的设备和用户，其 Android Enterprise 应用程序将重置为默认状态。以前应用的托管配置策略不再影响操作。
- XenMobile 管理通过企业注册的设备。从 Google 的角度来看，这些设备是未受管理的。您无法添加新的 Android Enterprise 应用程序。您无法应用托管配置策略。您可以将其他策略（例如计划、密码和限制）应用于这些设备。
- 如果您尝试在 Android Enterprise 中注册设备，它们将注册为 Android 设备，而不是 Android Enterprise 设备。

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 会为 XenMobile Tools 打开一个弹出窗口。在开始之前，请确保 XenMobile 具有在您使用的浏览器中打开弹出窗口的权限。某些浏览器（例如 Google Chrome）要求您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：

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。“设置”页面随即显示。
2. 在“设置”页面上，单击 **Android Enterprise**。
3. 单击 **取消注册**。



分发 Android Enterprise 应用程序

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 Android Enterprise 应用程序。

- **托管应用商店应用程序：** 这些应用程序包括托管 Google Play 商店中提供的免费应用程序。例如，GoToMeeting。

- **MDX：** 使用 MAM SDK 准备或使用 MDX Toolkit 封装的应用程序。这些应用程序包含 MDX 策略。您可以从内部源和公共商店获取 MDX 应用程序。将 Citrix® 移动生产力应用程序部署为 MDX 应用程序。
- **企业：** 您开发或从其他来源获取的私有应用程序。您通过托管 Google Play 商店向用户提供这些应用程序。托管 Google Play 商店是 Google 企业应用商店。
- **启用 MDX 的私有应用程序：** 使用 MAM SDK 准备或使用 MDX Toolkit 封装的企业应用程序。

您可以通过两种不同的方式添加企业应用程序和启用 MDX 的私有应用程序。

- 将应用程序作为企业应用程序添加到 XenMobile 控制台，如本文中的 企业应用程序 和 启用 MDX 的私有应用程序 部分所述。
- 使用您的 Google 开发者帐户将应用程序直接发布到托管 Google Play 商店。然后将应用程序作为托管应用商店应用程序添加到 XenMobile 控制台。请参阅 托管应用商店应用程序。

如果您使用 Google 开发者帐户发布应用程序，然后切换到使用 XenMobile 控制台，则应用程序的所有权会有所不同。在这种情况下，请在这两个位置管理您的应用程序。Citrix 建议您使用其中一种方法添加应用程序。

如果您需要从托管 Google Play 商店中删除自行管理的应用程序，请向 Google 提交工单。开发者可以禁用但不能删除托管 Google Play 商店中的应用程序。

以下部分提供了有关 Android Enterprise 应用程序配置的更深入信息。有关分发应用程序的信息，请参阅 添加应用程序。该文章包括：

- 添加 Web 和 SaaS 应用程序或 Web 链接的常规工作流程
- 企业和公共商店应用程序所需的应用程序工作流程
- 如何从 Citrix 企业应用程序内容分发网络 (CDN) 交付企业应用程序

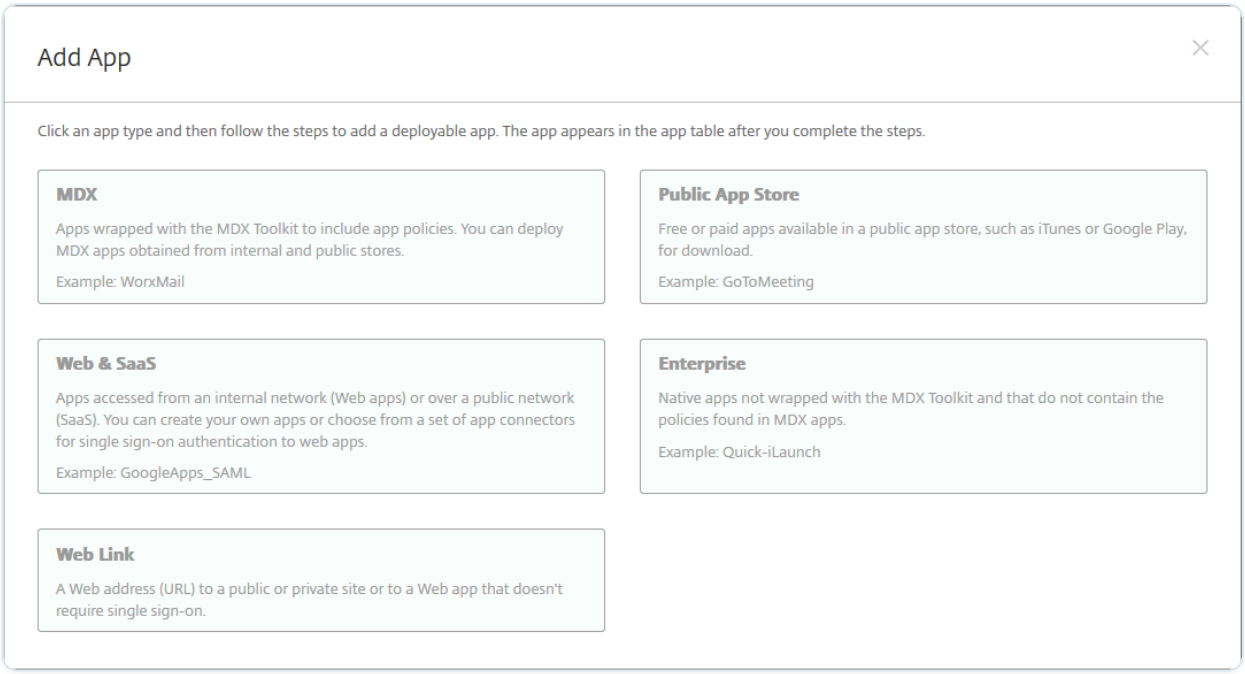
托管应用商店应用

您可以将托管 Google Play 商店中提供的免费应用添加到 XenMobile。

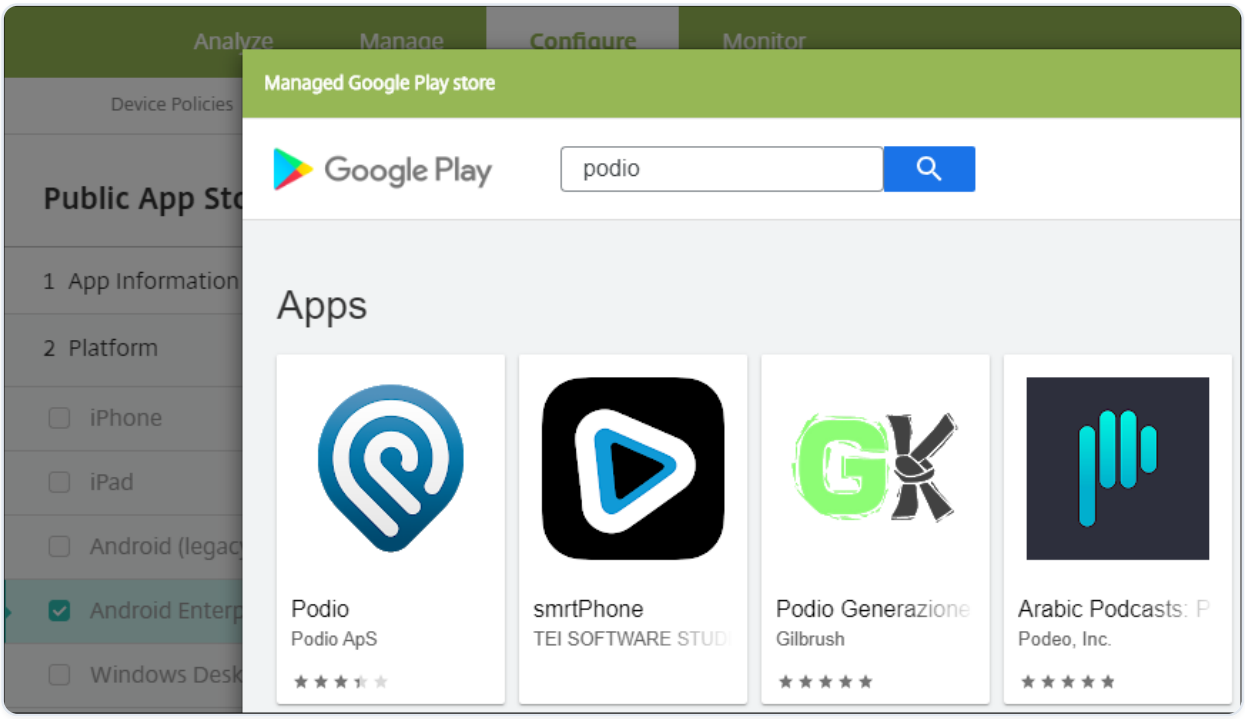
> **注意：**
>
> 要使 Google Play 商店中的所有应用都可以从托管 Google Play 访问，请使用 **Access all apps in the managed Google Play store** 服务器属性。请参阅服务器属性。将此属性设置为 **true** 允许所有 Android Enterprise 用户访问公共 Google Play 商店应用。然后，您可以使用限制设备策略 来控制对这些应用的访问。

步骤 1：添加和配置应用

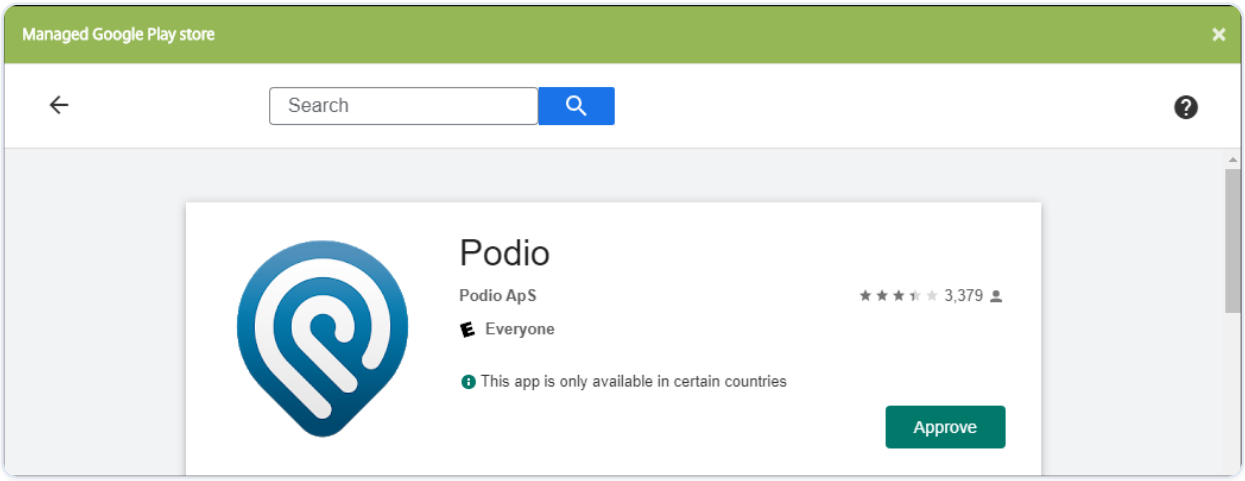
1. 在 XenMobile 控制台中，导航到 **Configure > Apps**。单击**添加**。
2. 单击 **公共应用商店**。



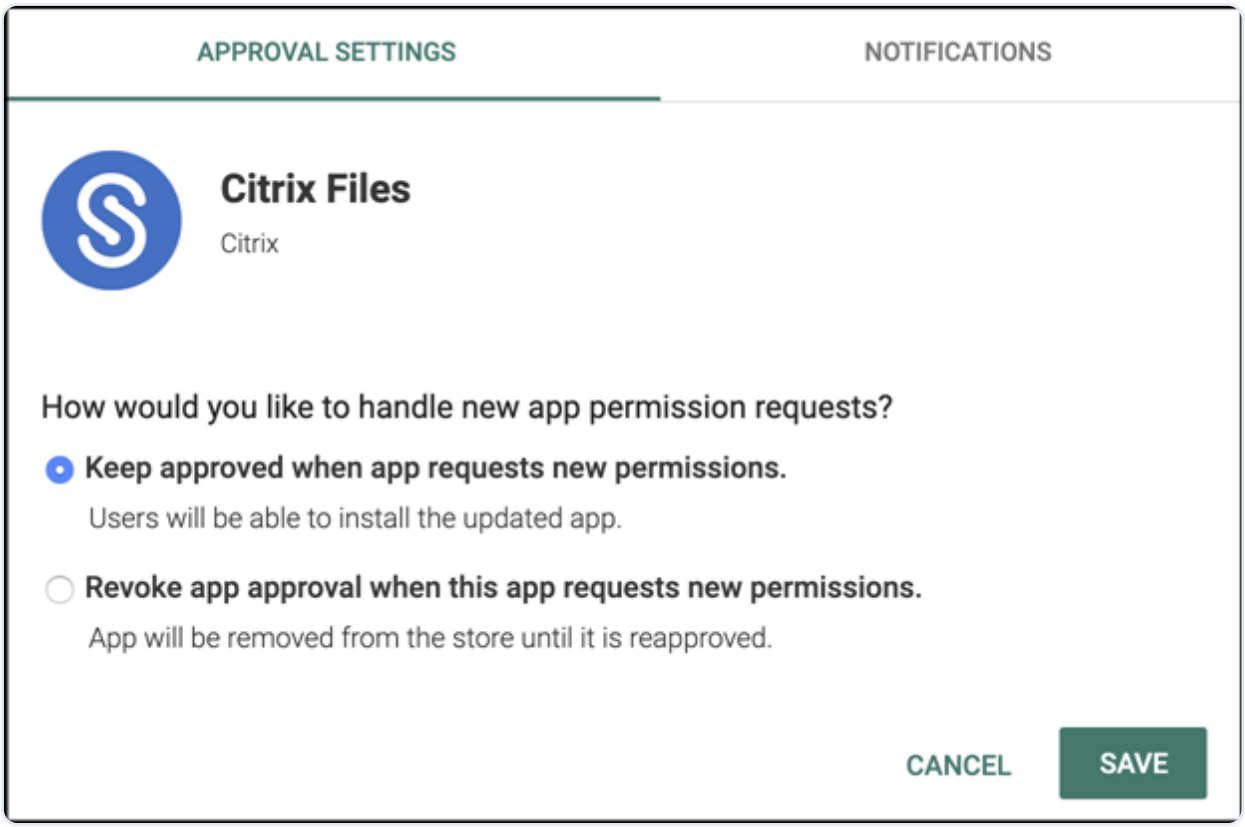
3. 在 **App Information** 窗格中，键入以下信息：
   - **名称：** 键入应用的描述性名称。该名称显示在 **Apps** 表的 **App Name** 下。
   - **说明：** 键入应用的可选说明。
   - **应用类别：** （可选）在列表中，单击要添加应用的类别。有关应用类别的详细信息，请参阅关于应用类别。
4. 选择 **Android Enterprise** 作为平台。
5. 在搜索框中键入应用名称或程序包 ID，然后单击**搜索**。您可以在 Google Play 商店中找到程序包 ID。该 ID 位于应用的 URL 中。例如，`com.Slack` 是 `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US` 中的程序包 ID。



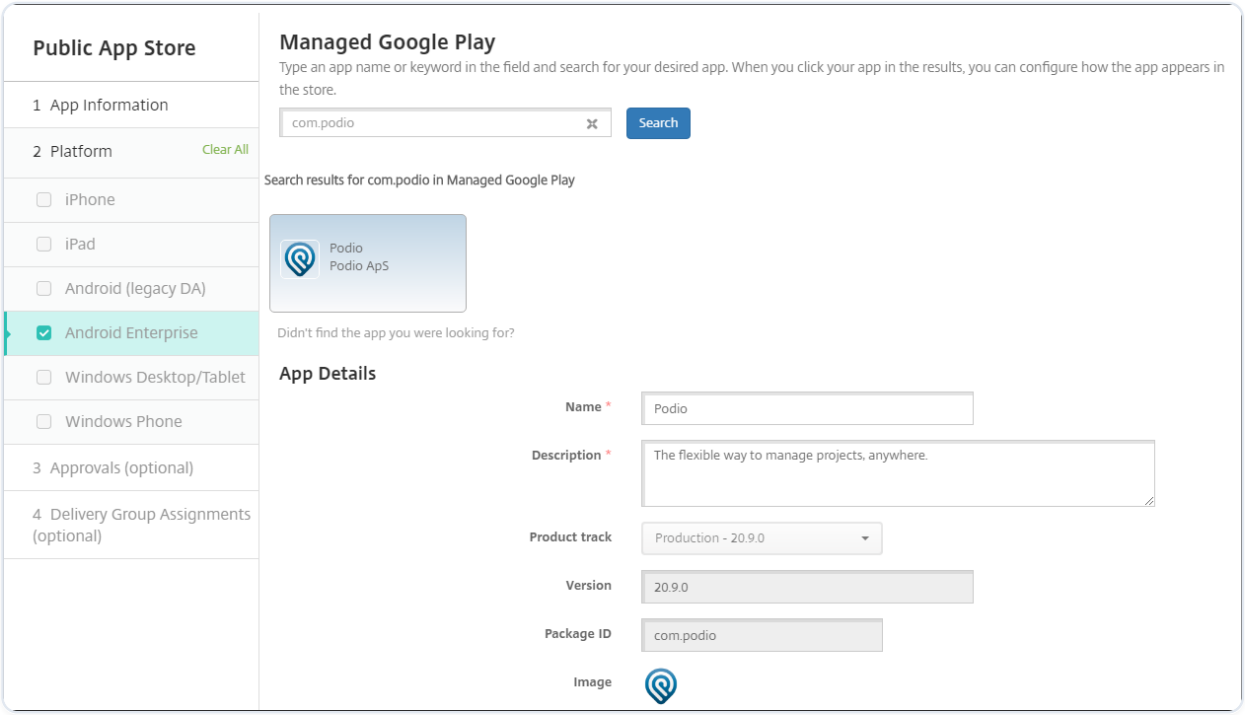
6. 与搜索条件匹配的应用程序将显示。单击所需的应用程序，然后单击**批准**。



7. 再次单击**批准**。
8. 选择**当应用程序请求新权限时保持批准**。单击**保存**。



9. 单击应用程序图标并配置应用程序的**名称**和**描述**。

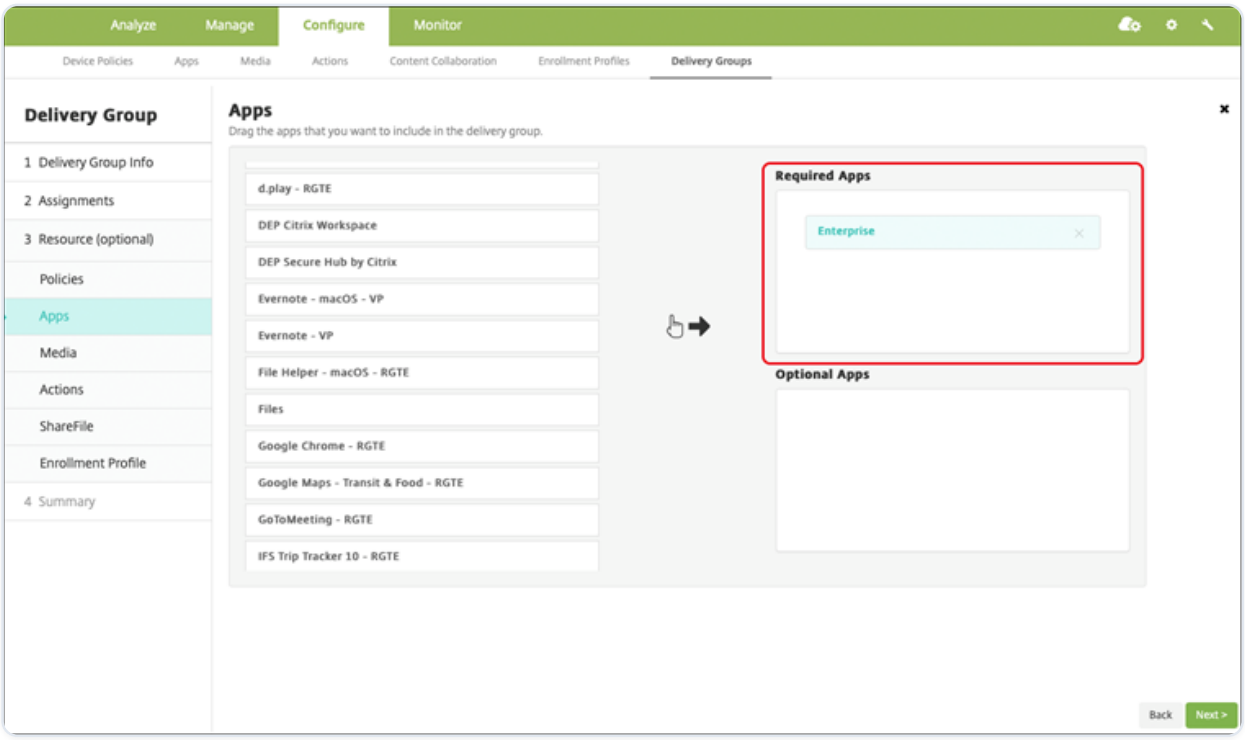


10. 将任何交付组分配给应用程序，然后单击**保存**。有关信息，请参阅部署资源。

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**部分中，将所需的应用程序拖动到**所需应用程序**框中。



3. 在**摘要**页面上，单击**保存**。
4. 在**交付组**页面上，选择交付组，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。有关适用于每种设备平台类型的应用程序策略的信息，请参阅：

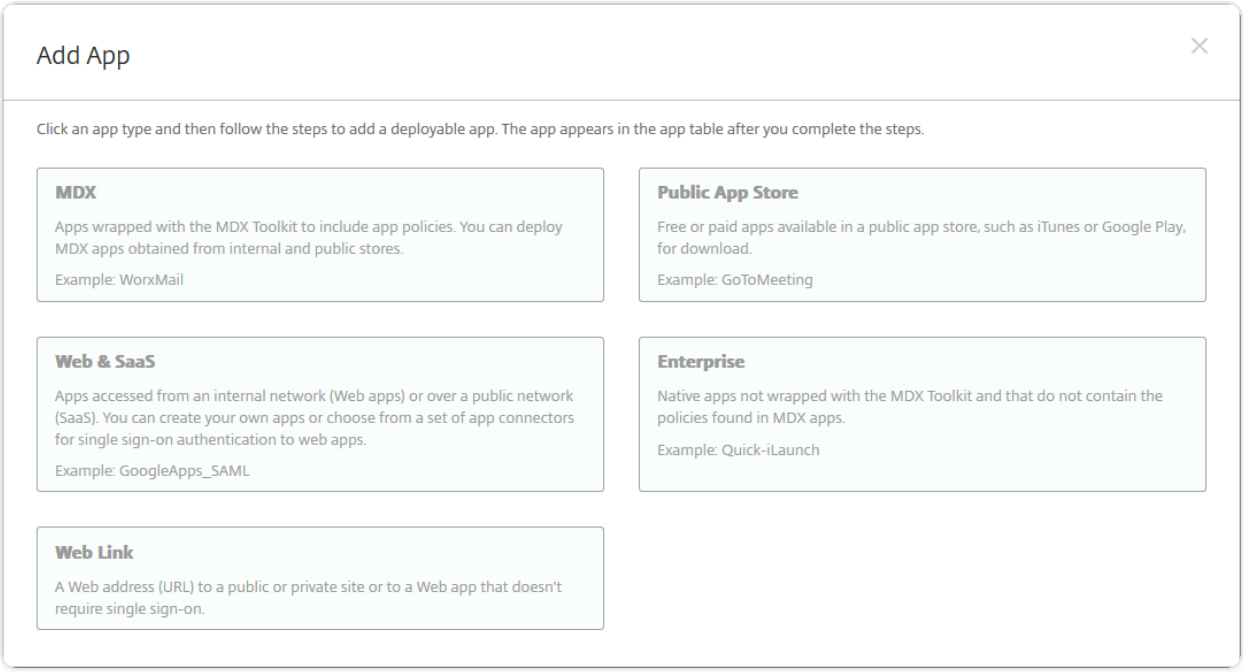
- MAM SDK 概述
- MDX 策略一览

步骤 1：添加和配置应用程序

1. 对于 Citrix 移动生产力应用程序，请下载公共商店 MDX 文件：转至 `<https://www.citrix.com/downloads>`。导航到 **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**。

   对于其他类型的 MDX 应用程序，请获取 MDX 文件。

2. 在 XenMobile 控制台中，单击**配置 > 应用程序**。单击**添加**。将显示**添加应用程序**对话框。

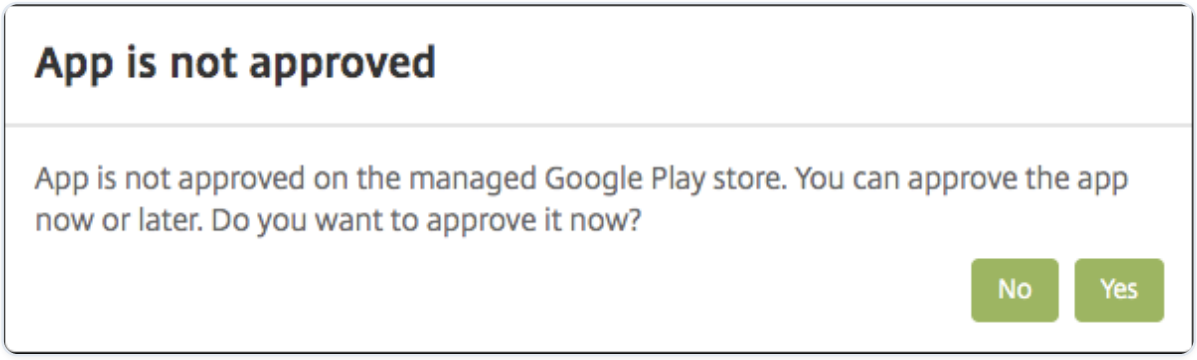


3. 单击 **MDX**。将显示 **MDX 应用程序信息**页面。在**应用程序信息**窗格中，键入以下信息：

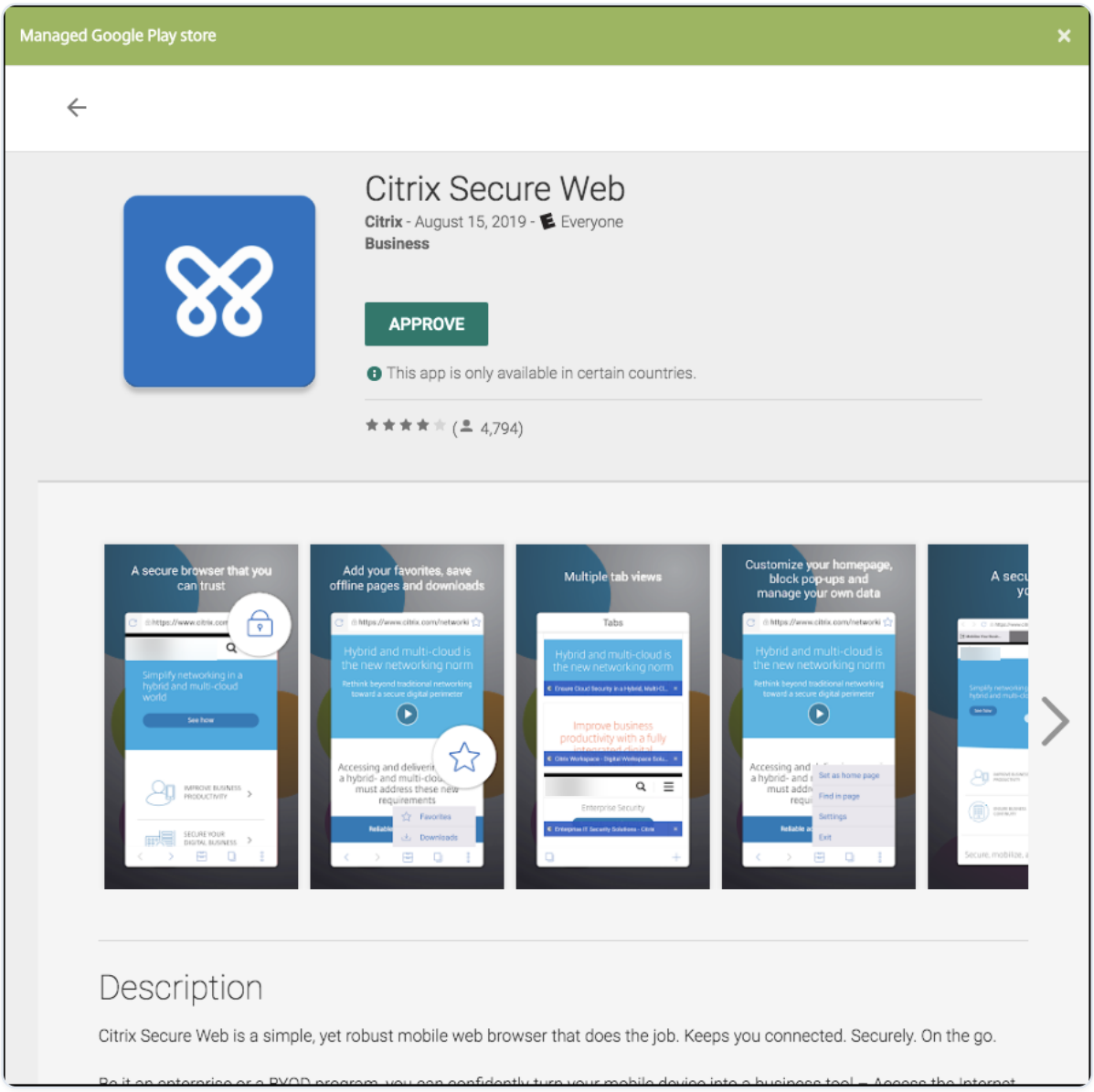
   - **名称：键入应用程序的描述性名称。该名称将显示在应用程序**表中的**应用程序名称**下。
   - **说明：**键入应用程序的可选说明。
   - **应用程序类别：**（可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

4. 选择 **Android Enterprise** 作为平台。
5. 单击**上载**并导航到 MDX 文件。Android Enterprise 仅支持使用 MAM SDK 或 MDX Toolkit 准备的应用程序。

   - 如果附加的应用程序需要托管 Google Play 商店的批准，UI 会通知您。要在不离开 XenMobile 控制台的情况下批准应用程序，请单击**是**。



   在托管的 Google Play 商店打开后，按照说明批准并保存应用程序。



成功添加应用程序后，将显示“**应用程序详细信息**”页面。

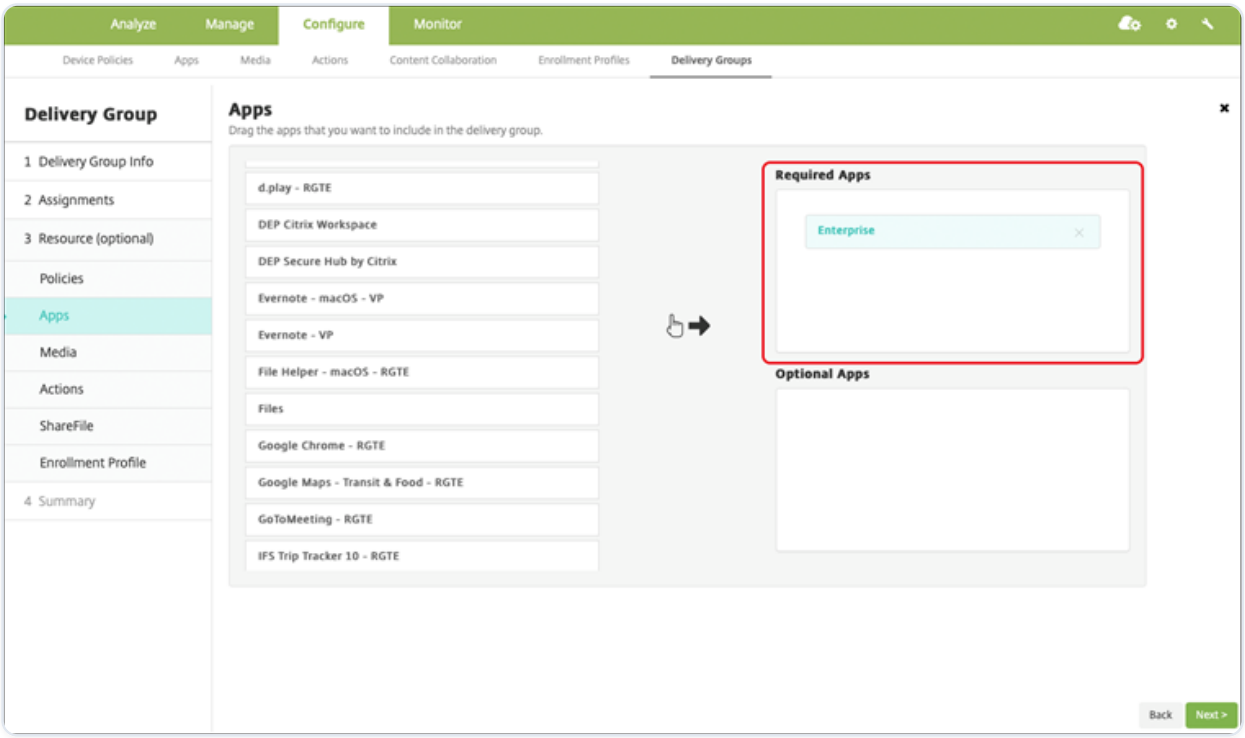
6. 配置以下设置：

- **文件名：** 键入与应用程序关联的文件名。
- **应用程序描述：** 键入应用程序的描述。
- **应用程序版本：** （可选）键入应用程序版本号。
- **程序包 ID：** 键入从托管的 Google Play 商店获取的应用程序程序包 ID。
- **最低操作系统版本：** （可选）键入设备可运行以使用应用程序的最旧操作系统版本。
- **最高操作系统版本：** （可选）键入设备必须运行以使用应用程序的最新操作系统版本。
- **排除的设备：** （可选）键入无法运行此应用程序的设备制造商或型号。

7. 配置 **MDX 策略**。MDX 策略因平台而异，包括身份验证、设备安全性以及应用程序限制等策略区域的选项。在控制台中，每个策略都有一个描述该策略的工具提示。有关适用于每种设备平台类型的应用程序策略的信息，请参阅：
   - MAM SDK 概述
   - MDX 策略一览
8. 配置部署规则和商店配置。
9. 将任何交付组分配给应用程序，然后单击“**保存**”。有关信息，请参阅部署资源。

步骤 2：配置应用程序部署

1. 导航到“**配置 > 交付组**”，然后选择您配置的交付组。单击“**编辑**”。
2. 在“**应用程序**”部分中，将所需的应用程序拖动到“**所需应用程序**”框中。



3. 在“**摘要**”页面上，单击“**保存**”。
4. 在“**交付组**”页面上，选择交付组，然后单击“**部署**”。

企业应用程序

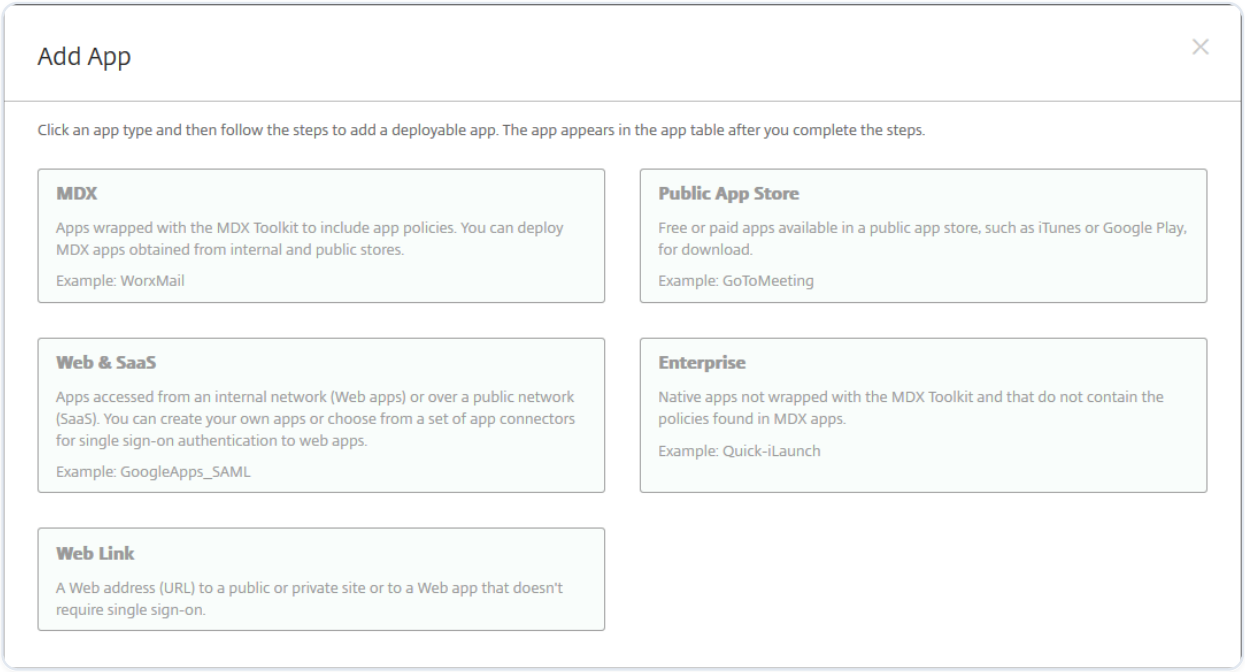
企业应用程序表示未使用 MAM SDK 或 MDX Toolkit 准备的专用应用程序。您可以自行开发这些应用程序，也可以直接从其他来源获取。要添加企业应用程序，您需要与该应用程序关联的 APK 文件。请确保遵循 Google 的专用应用程序最佳实践。

步骤 1：添加和配置应用程序

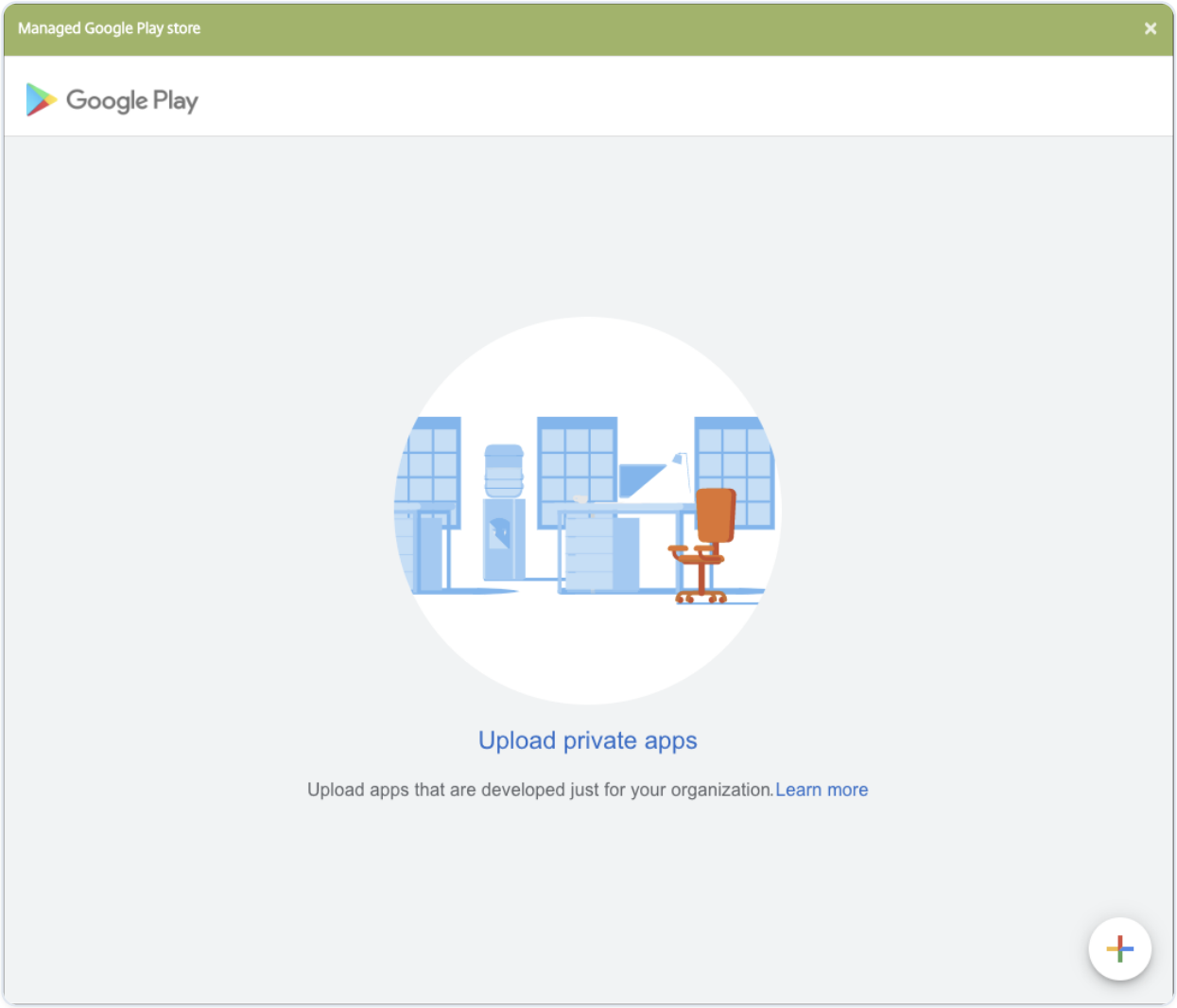
通过以下两种方式之一添加应用程序：

- 将应用程序直接发布到托管的 Google Play 商店，并将其作为托管 Play 商店应用程序添加到 XenMobile 控制台。请按照 Google 文档中有关如何发布专用应用程序的说明进行操作，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。执行以下步骤：

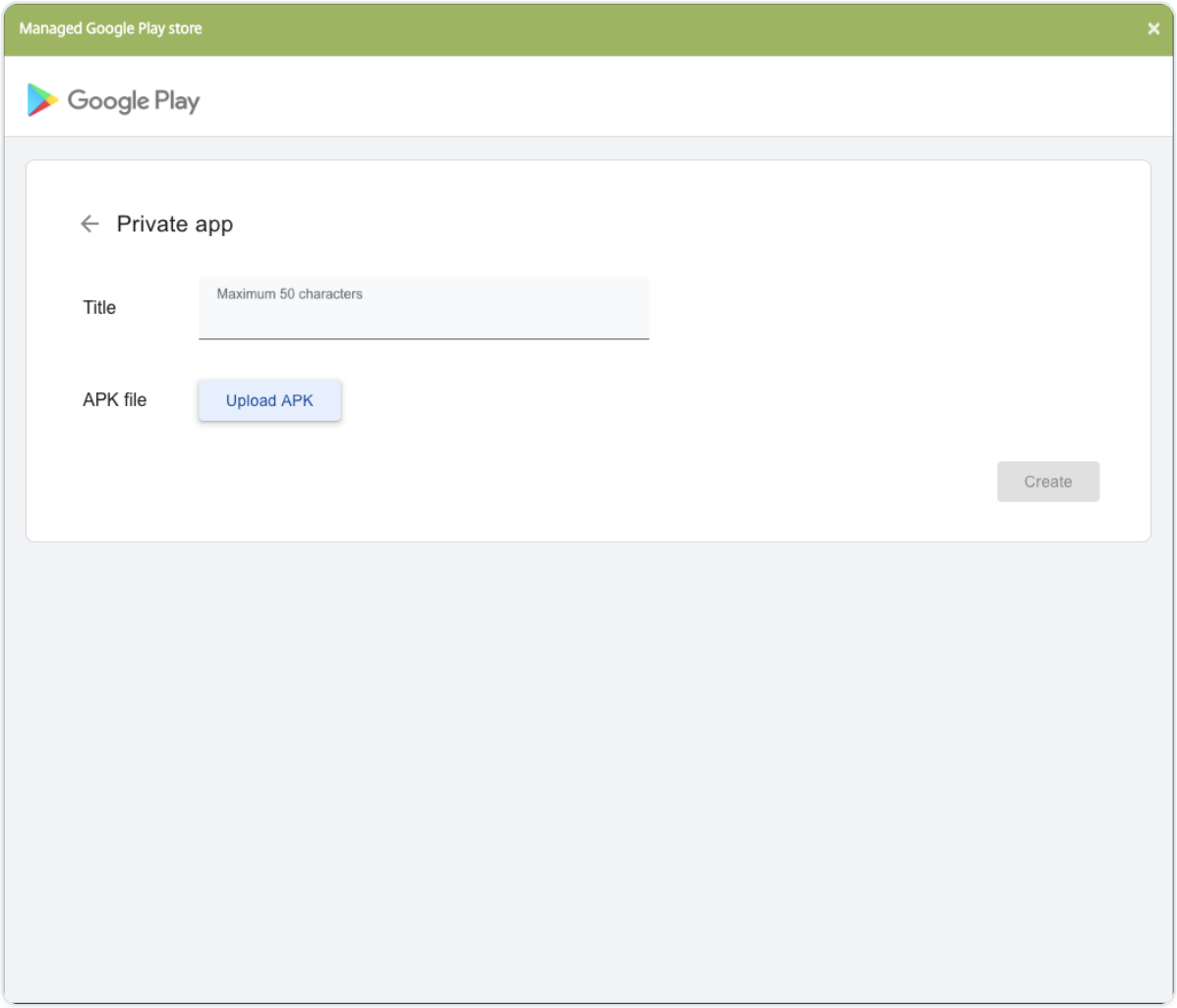
1. 在 XenMobile 控制台中，单击“**配置 > 应用程序**”。单击“**添加**”。此时将显示“**添加应用程序**”对话框。



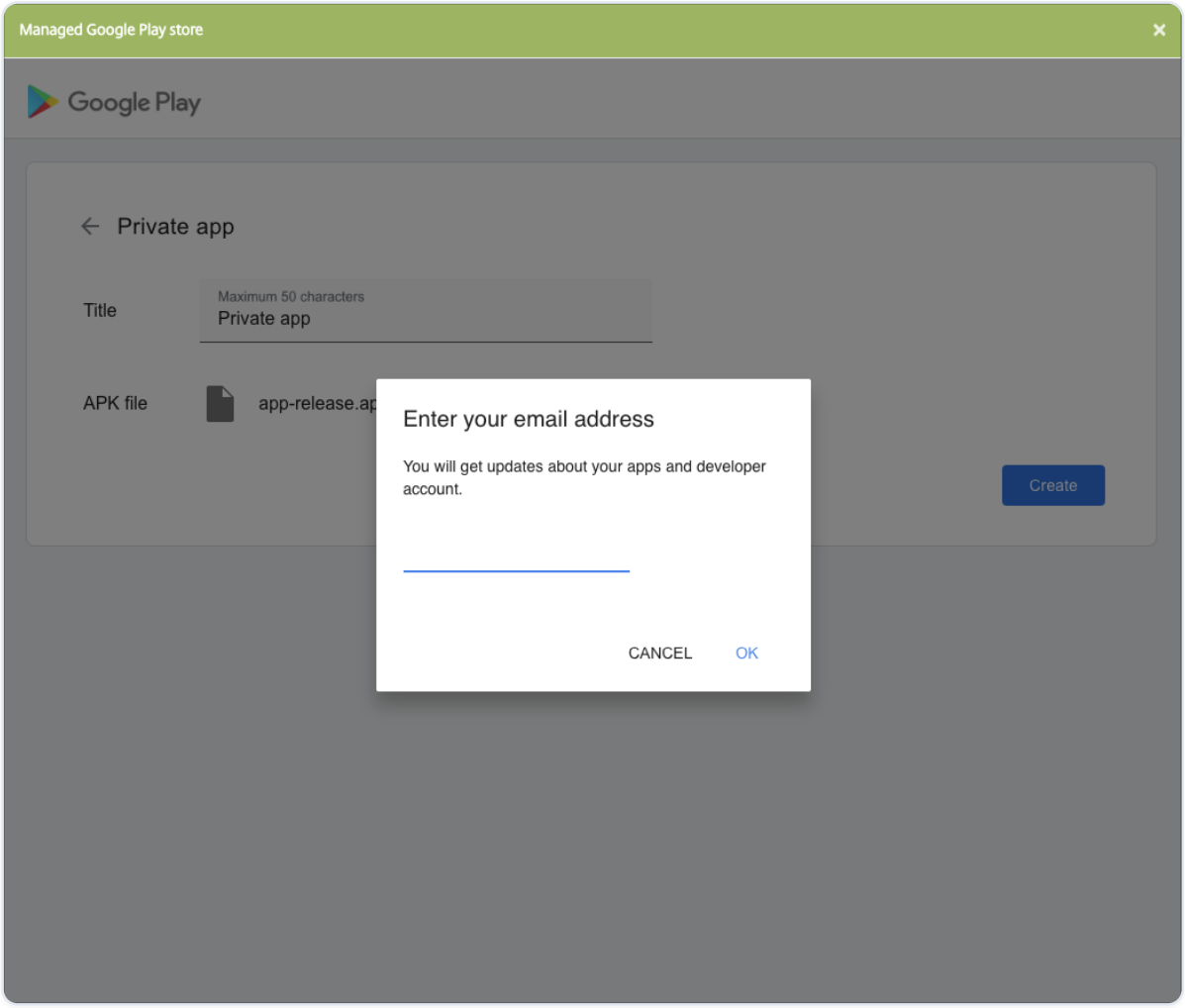
2. 点击“**企业**”。在“**应用程序信息**”窗格中，键入以下信息：
   - “**名称：**”键入应用程序的描述性名称。此名称在“应用程序”表中的“应用程序名称”下显示。
   - “**描述：**”键入应用程序的可选描述。
   - “**应用程序类别：**”（可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
3. 选择“**Android Enterprise**”作为平台。
4. “**上载**”按钮将打开托管的 Google Play 商店。您无需注册开发者帐户即可发布专用应用程序。单击右下角的“**加号**”图标以继续。



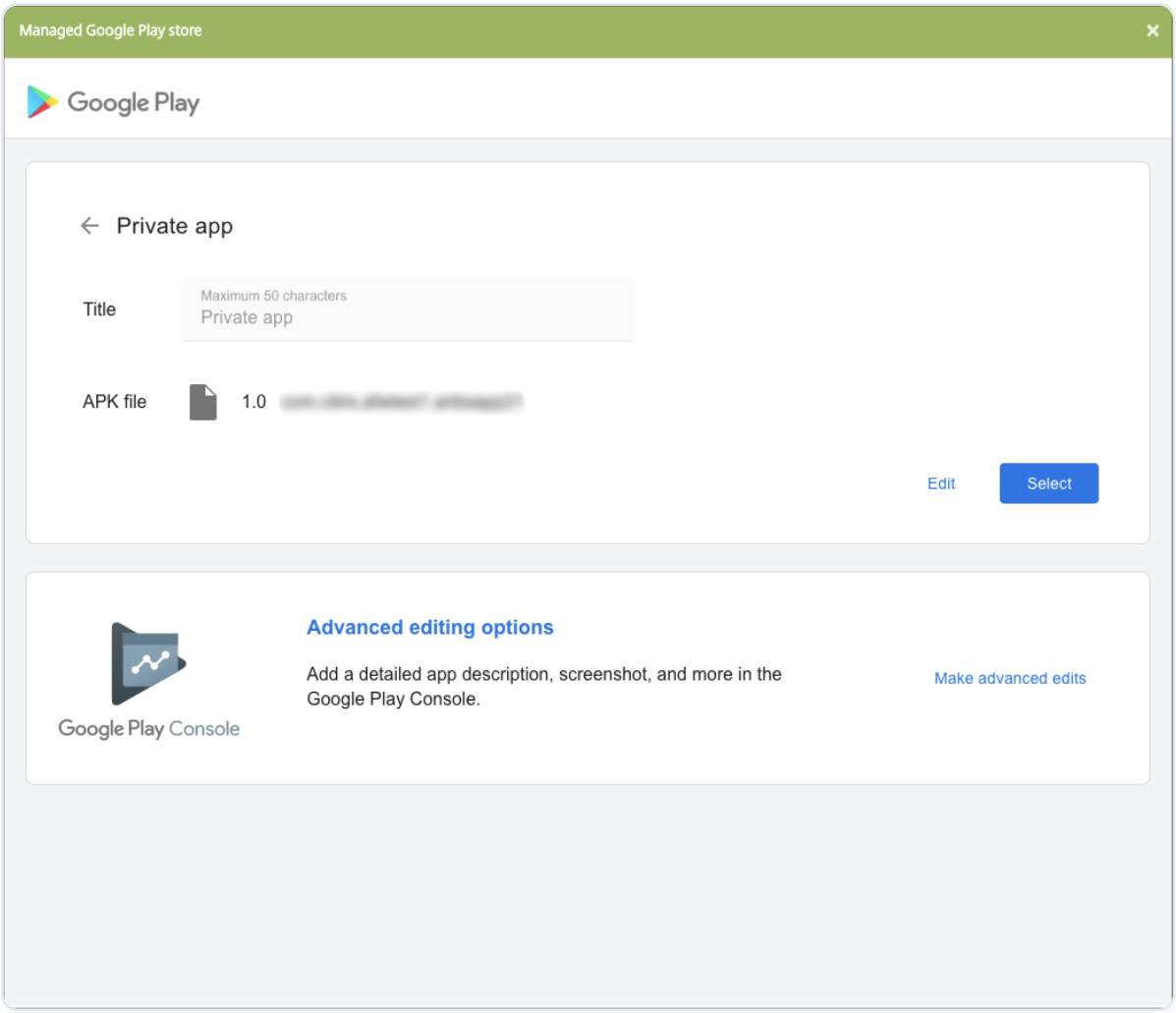
a. 键入应用程序的名称并上载 .apk 文件。完成后，单击“**创建**”。您的专用应用程序可能需要长达 10 分钟才能发布。



b. 输入电子邮件地址以获取有关应用程序的更新。



c. 应用程序发布后，单击专用应用程序的图标。如果要添加应用程序描述、更改应用程序图标以及执行其他操作，请单击“**进行高级编辑**”。否则，单击“**选择**”以打开应用程序信息页面。

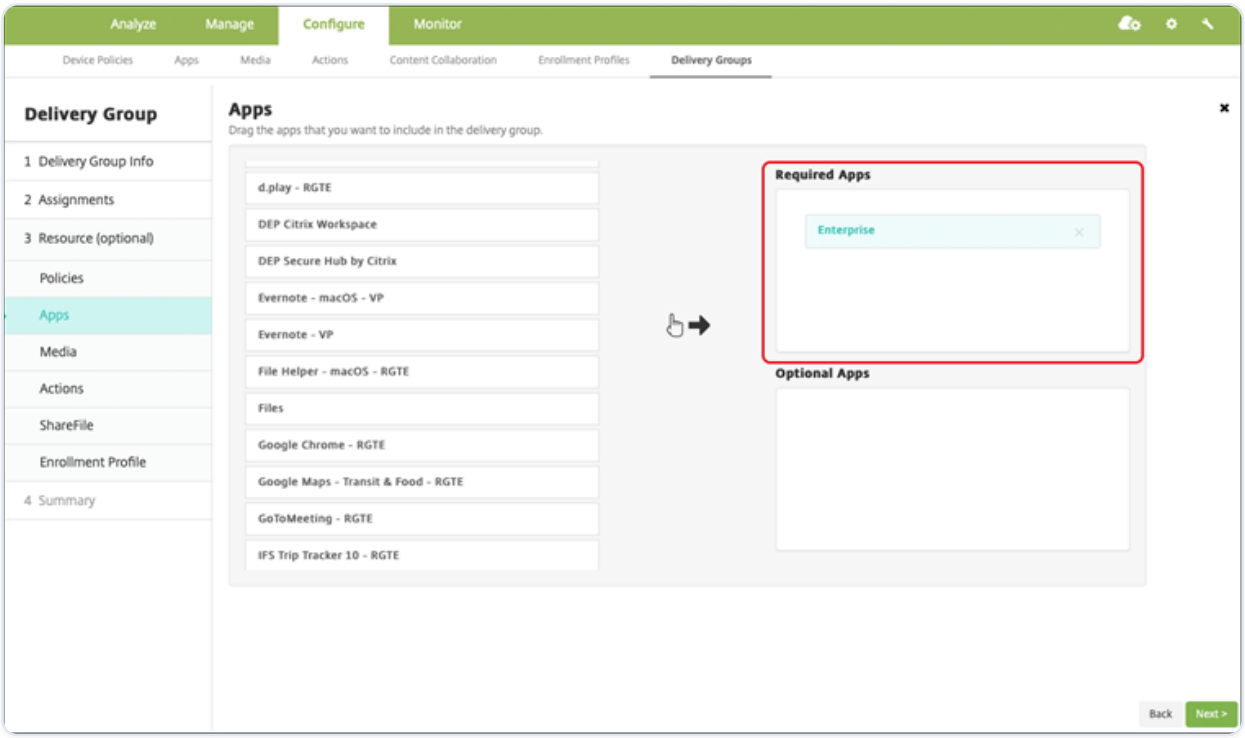


5. 单击“**下一步**”。将显示该平台的应用程序信息页面。
6. 配置平台类型的设置，例如：
   - **文件名：** 可选，为应用程序键入一个新名称。
   - **应用程序描述：** 可选，为应用程序键入一个新描述。
   - **应用程序版本：** 您无法更改此字段。
   - **包 ID：** 您的应用程序的唯一标识符。
   - **最低操作系统版本：** 可选，键入设备可运行以使用此应用程序的最旧操作系统版本。
   - **最高操作系统版本：** 可选，键入设备必须运行以使用此应用程序的最新操作系统版本。
   - **排除的设备：** 可选，键入无法运行此应用程序的设备制造商或型号。
7. 配置部署规则和商店配置。
8. 将任何交付组分配给应用程序，然后单击**保存**。有关信息，请参阅部署资源。

步骤 2：配置应用程序部署

1. 导航到**配置 > 交付组**，然后选择您配置的交付组。单击**编辑**。

2. 在**应用程序**部分中，将所需的应用程序拖动到**所需应用程序**框中。



3. 在**摘要**页面上，单击**保存**。
4. 在**交付组**页面上，选择交付组，然后单击**部署**。

MDX 启用的私有应用

要将 Android Enterprise 应用添加为 MDX 启用的企业应用，请执行以下操作：

1. 创建私有 Android Enterprise 应用并启用该应用的 MDX。
2. 将应用添加到 XenMobile 控制台。
   - 在托管的 Google Play 商店中托管和发布应用。
   - 将应用作为企业应用添加到 XenMobile 控制台。
3. 将 MDX 文件添加到 XenMobile。

如果您决定通过 Google Play 商店托管和发布应用，请不要选择 Google 证书签名。使用用于启用应用 MDX 的同一证书对应用进行签名。有关发布应用的详细信息，请参阅 Google 文档中的发布您的应用和签署您的应用。MAM SDK 不会打包应用，因此除了用于开发应用的证书外，不需要其他证书。

有关通过 Google Play 管理中心发布私有应用的详细信息，请参阅 Google 文档中有关如何从 Play 管理中心发布私有应用的内容。

要通过 XenMobile 发布应用，请参阅以下各节。

准备私有 Android Enterprise 应用

创建私有 Android Enterprise 应用时，请确保遵循 Google 的私有应用最佳实践。

创建私有 Android Enterprise 应用后，将 MAM SDK 与应用集成，或使用 MDX Toolkit 打包应用。然后，将生成的文件添加到 XenMobile。

您可以通过上传更新的 .apk 文件来更新应用。以下步骤介绍了使用 MDX Toolkit 进行应用打包。

1. 创建您的私有 Android Enterprise 应用并生成签名的 .apk 文件。
2. 以下示例文件包含所有已知策略，其中一些可能不适用于您的环境。任何不可用的设置都将被忽略。使用以下参数创建 XML 文件：

```
<?xml version="1.0" encoding="UTF-8"?>

<MobileAppPolicies>

    <PolicySchemaVersion>

        1.0

    </PolicySchemaVersion>

    <Policies>

        <DevicePasscode>false</DevicePasscode>

        <AppPasscode>false</AppPasscode>

        <MaxOfflinePeriod>72</MaxOfflinePeriod>

        <StepupAuthAddress/>

        <RequireUserEntropy>false</RequireUserEntropy>

        <BlockRootedDevices>true</BlockRootedDevices>

        <BlockDebuggerAccess>false</BlockDebuggerAccess>

        <RequireDeviceLock>false</RequireDeviceLock>

        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
NonCompliantDeviceBehavior>
```

```
<WifiOnly>false</WifiOnly>

<RequireInternalNetwork>false</RequireInternalNetwork>

<InternalWifiNetworks/>

<AllowedWifiNetworks/>

<UpgradeGracePeriod>168</UpgradeGracePeriod>

<WipeDataOnAppLock>false</WipeDataOnAppLock>

<ActivePollPeriod>60</ActivePollPeriod>

<PublicFileAccessLimitsList/>

<CutAndCopy>Unrestricted</CutAndCopy>

<Paste>Unrestricted</Paste>

<DocumentExchange>Unrestricted</DocumentExchange>

<OpenInExclusionList/>

<InboundDocumentExchange>Unrestricted</InboundDocumentExchange>

<InboundDocumentExchangeWhitelist/>

<connectionSecurityLevel>TLS</connectionSecurityLevel>

<DisableCamera>false</DisableCamera>

<DisableGallery>false</DisableGallery>

<DisableMicrophone>false</DisableMicrophone>

<DisableLocation>false</DisableLocation>

<DisableSms>false</DisableSms>

<DisableScreenCapture>false</DisableScreenCapture>

<DisableSensor>false</DisableSensor>
```

```
        <DisableNFC>false</DisableNFC>

        <BlockLogs>false</BlockLogs>

        <DisablePrinting>false</DisablePrinting>

        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
MvpnNetworkAccess>

        <MvpnSessionRequired>False</MvpnSessionRequired>

        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>

        <DisableLocalhostConnections>false</
DisableLocalhostConnections>

        <CertificateLabel/>

        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>

        <DefaultLoggerLevel>15</DefaultLoggerLevel>

        <MaxLogFiles>2</MaxLogFiles>

        <MaxLogFileSize>2</MaxLogFileSize>

        <RedirectSystemLogs>false</RedirectSystemLogs>

        <EncryptLogs>false</EncryptLogs>

        <GeofenceLongitude>0</GeofenceLongitude>

        <GeofenceLatitude>0</GeofenceLatitude>

        <GeofenceRadius>0</GeofenceRadius>

        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>

        <Authentication>OfflineAccessOnly</Authentication>

        <ReauthenticationPeriod>480</ReauthenticationPeriod>

        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
```

```
    </Policies>

</MobileAppPolicies>
```

3. 使用 MDX Toolkit 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**。在接下来描述的命令中使用上一步中的 XML 文件。

   如果您知道应用程序的商店 URL，请将 **storeURL** 参数设置为该商店 URL。发布应用程序后，用户将从商店 URL 下载该应用程序。

   以下是用于封装名为 SampleAEapp 的应用程序的 MDX Toolkit 命令示例：

```
 ```

 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en
-Duser.variant

 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap

 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk

 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx

 -MinPlatform 5.0

 -keystore /MyKeystore

 -storepass mystorepwd123

 -keyalias key0

 -keypass mykeypwd123

 -storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"

 -appType Premium

 -premiumMdxPolicies <Path to Premium policy XML>
```
```

```
```

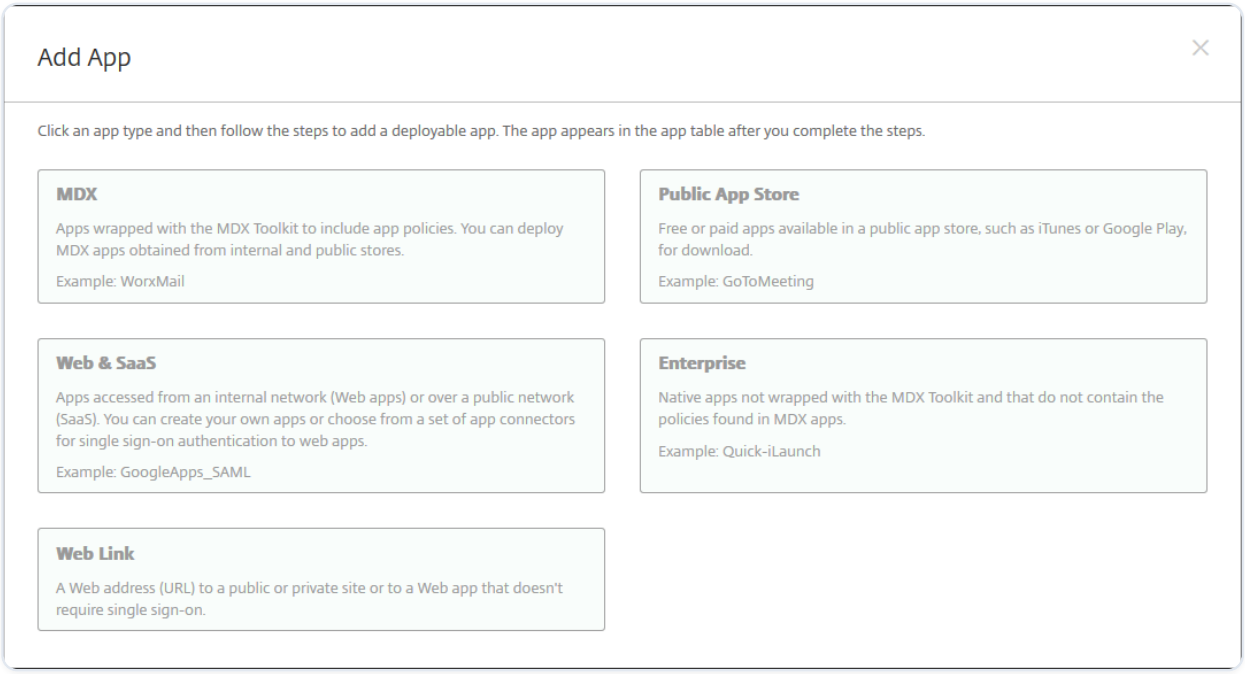
封装应用程序会生成一个封装的 .apk 文件和一个 .mdx 文件。

添加封装的 .apk 文件

通过以下两种方式之一添加应用程序：

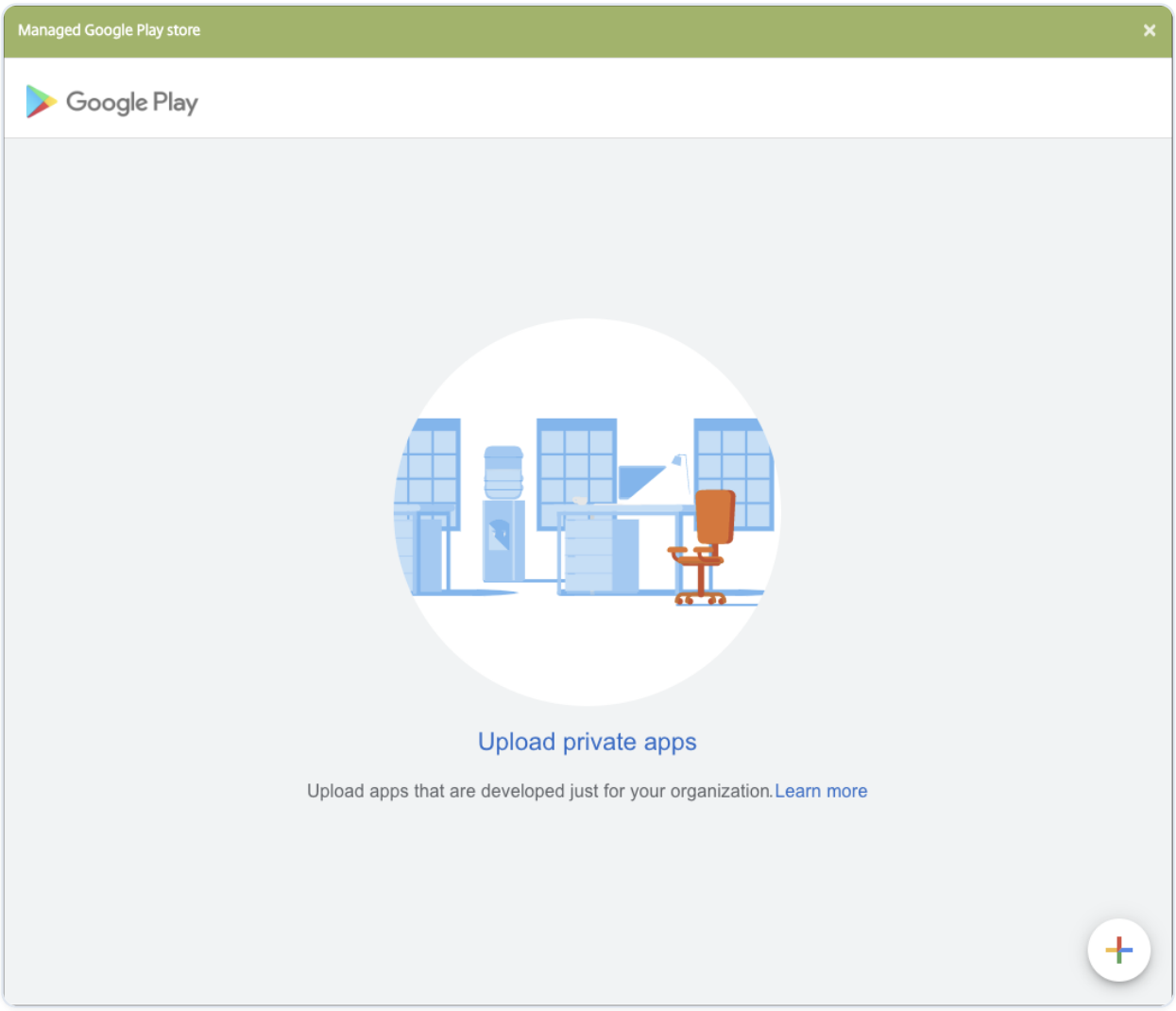
- 将应用程序直接发布到托管 Google Play 商店，并将其作为托管应用商店应用程序添加到 XenMobile 控制台。按照 Google 文档中关于发布私有应用程序 的说明进行操作，然后按照托管应用商店应用程序 部分中的步骤进行操作。
- 将应用程序作为企业应用程序添加到 XenMobile 控制台。执行以下步骤：

1. 在 XenMobile 控制台中，单击 **Configure > Apps**。**Apps** 页面随即打开。
2. 单击 **Add**。**Add App** 对话框随即出现。

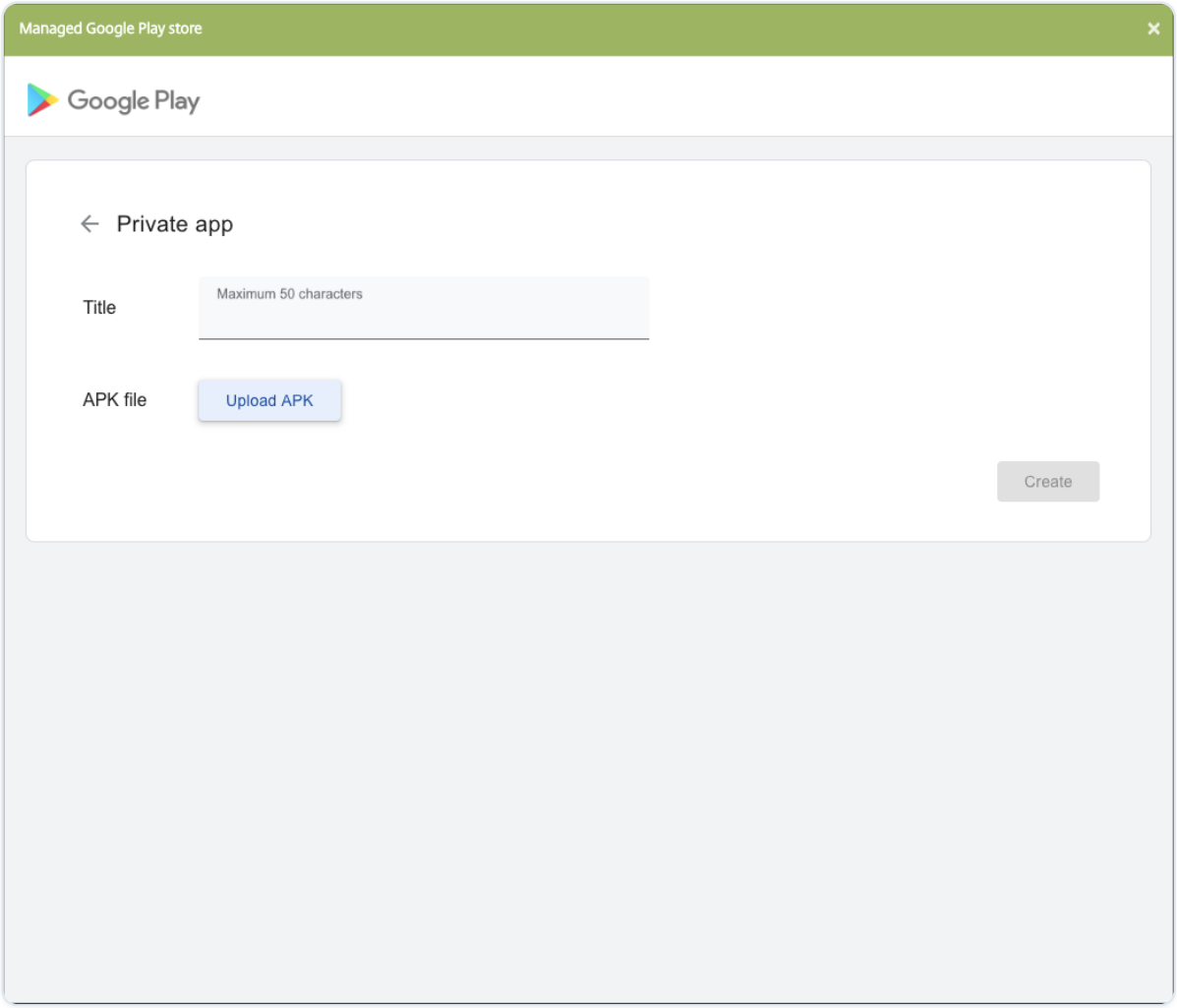


3. 单击 **Enterprise**。在 **App Information** 窗格中，键入以下信息：
   - **名称：** 键入应用程序的描述性名称。此名称将列在“应用程序”表中的“应用程序名称”下。
   - **描述：** 键入应用程序的可选描述。
   - **应用程序类别：** （可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 选择 **Android Enterprise** 作为平台。

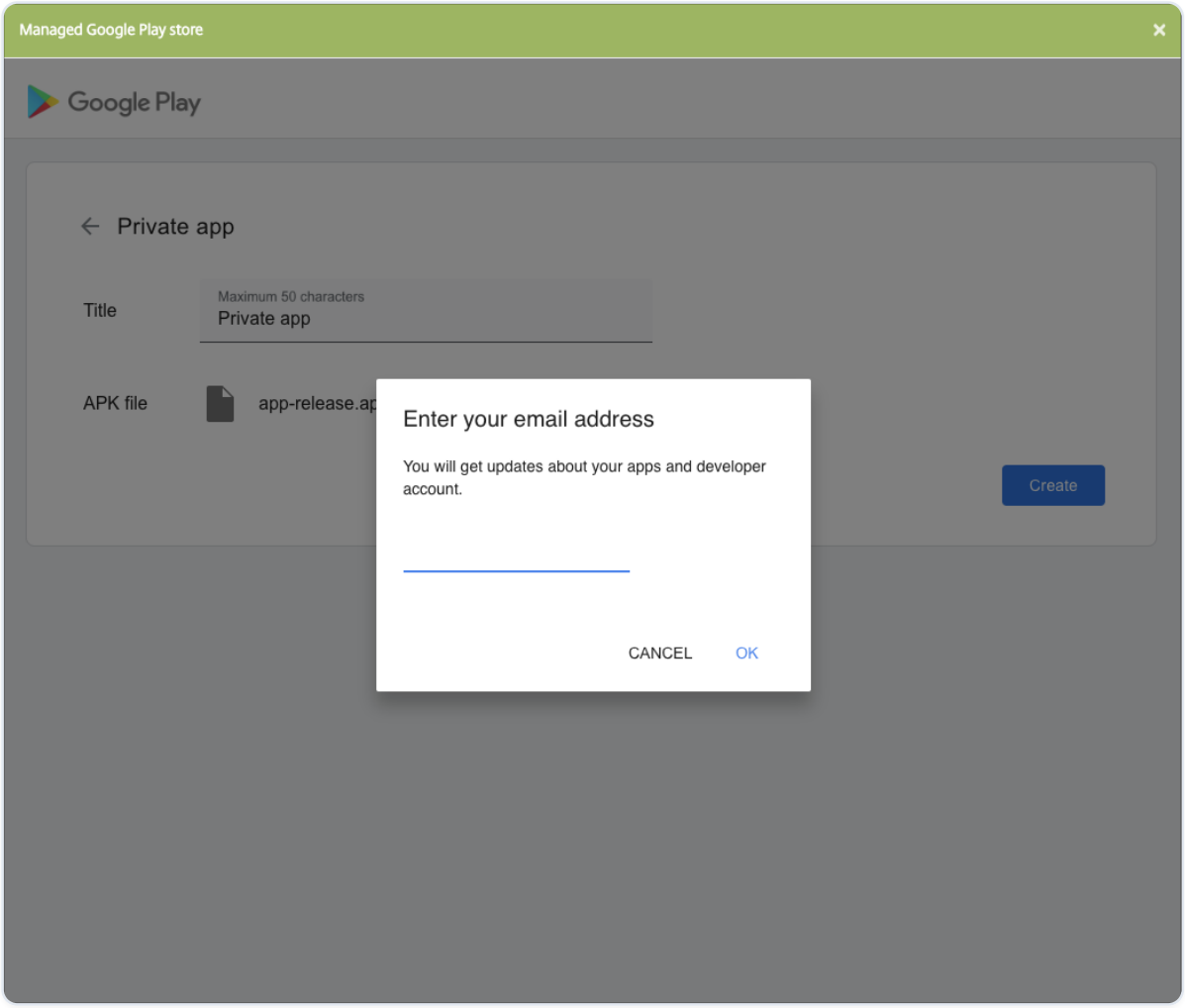
5. “**上载**”按钮将打开托管的 Google Play 商店。您无需注册开发人员帐户即可发布专用应用程序。单击右下角的“**加号**”图标以继续。



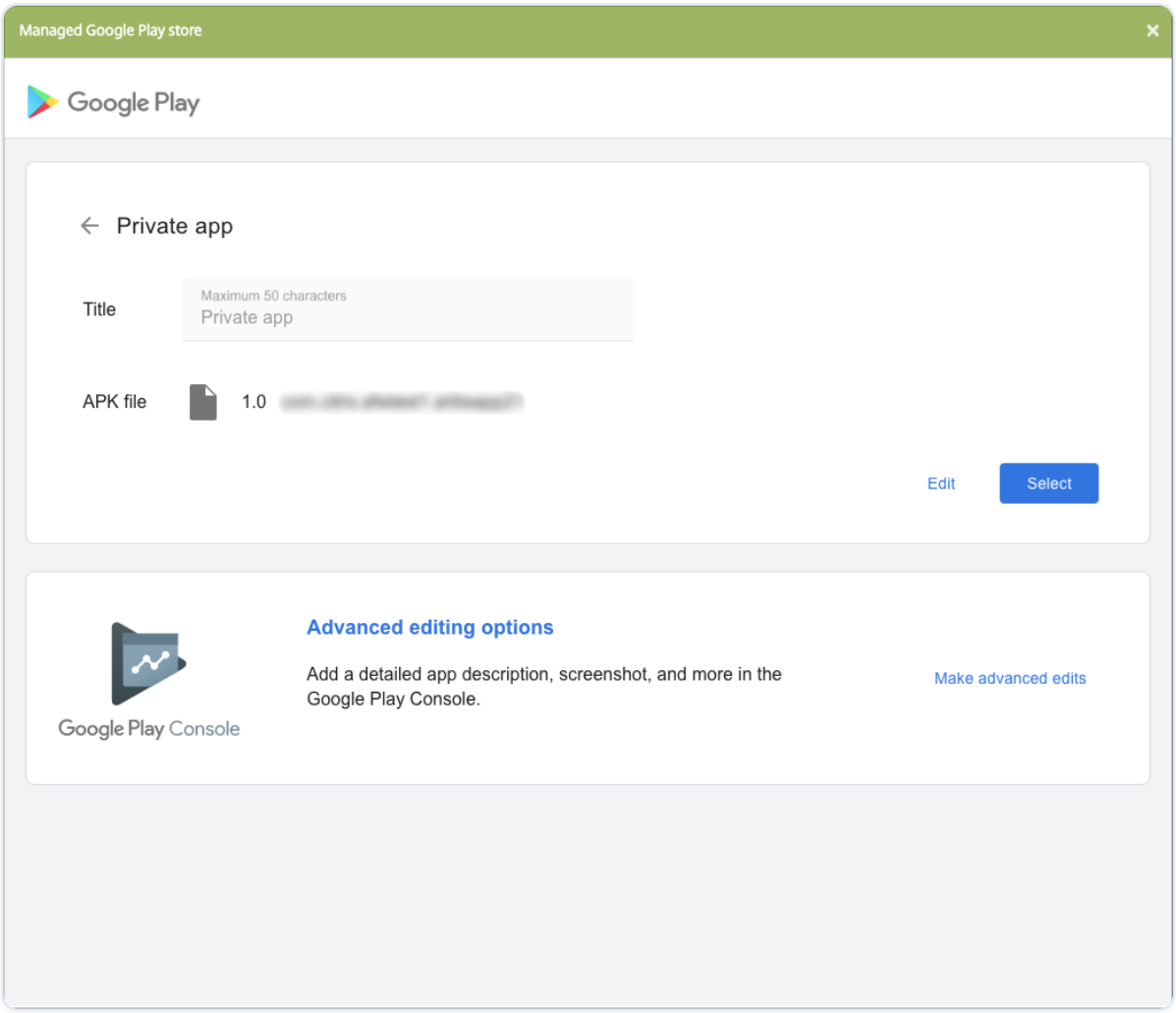
   a. 键入应用程序的名称并上载 .apk 文件。完成后，单击“**创建**”。您的专用应用程序可能需要长达 10 分钟才能发布。



b. 输入电子邮件地址以获取有关应用程序的更新。



c. 应用程序发布后，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“**下一步**”。此时将显示该平台的应用程序信息页面。
7. 配置平台类型的设置，例如：
   - **文件名：** （可选）为应用程序键入新名称。
   - **应用程序描述：** （可选）为应用程序键入新描述。
   - **应用程序版本：** 您无法更改此字段。
   - **程序包 ID：** 您的应用程序的唯一标识符。
   - **最低操作系统版本：** （可选）键入设备可运行的、用于使用此应用程序的最旧操作系统版本。
   - **最高操作系统版本：** （可选）键入设备必须运行的、用于使用此应用程序的最新操作系统版本。
   - **排除的设备：** （可选）键入无法运行此应用程序的设备的制造商或型号。
8. 配置部署规则和应用商店配置。
9. 在 **Android Enterprise Enterprise App** 页面中，单击 **Next**（下一步）。此时将显示 **Approvals**（批准）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。如果您不需要批准工作流，可以跳到步骤 13。

10. 单击 **Next**（下一步）。
11. 此时将显示 **Delivery Group Assignment**（交付组分配）页面。此页面上不需要执行任何操作。添加 .mdx 文件时，您将配置此应用程序的交付组和部署计划。单击 **Save**（保存）。

可选：添加或更改应用商店 URL

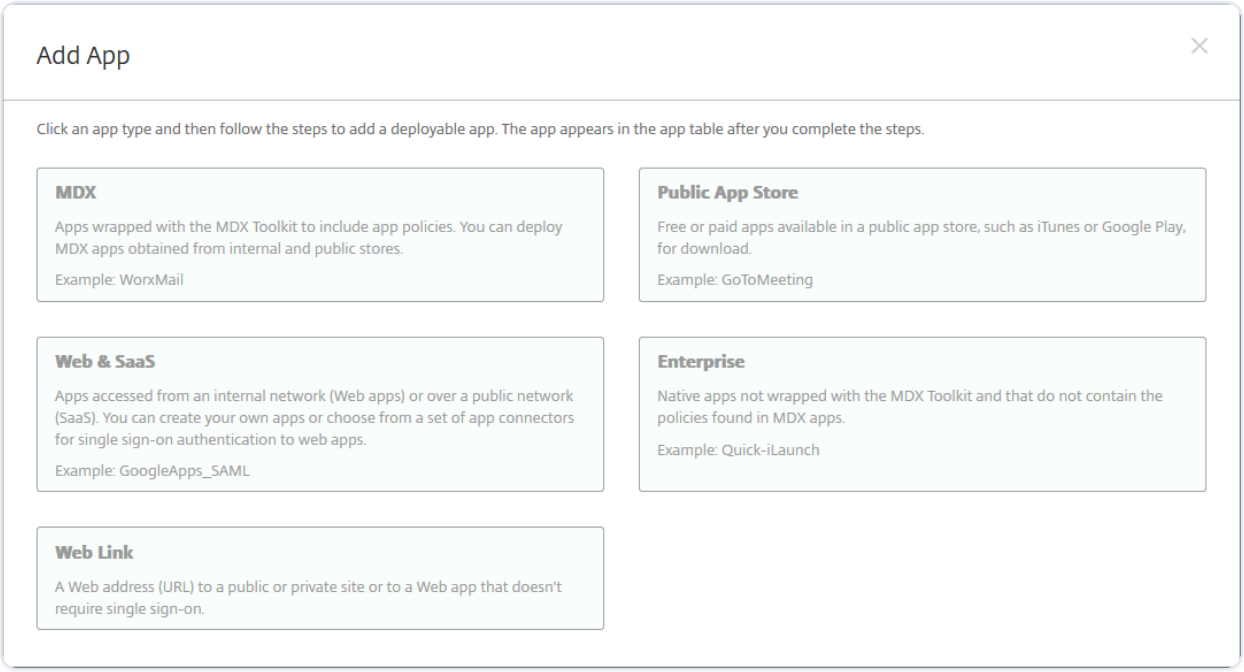
如果您在打包应用程序时不知道应用商店 URL，请立即添加应用商店 URL。

1. 在托管的 Google Play 商店中查看应用程序。选择应用程序时，应用商店 URL 将显示在浏览器的地址栏中。从 URL 形式复制应用程序的程序包名称。例如：`https://play.google.com/store/apps/details?id=SampleAEappPackage`。您复制的 URL 可能以 `https://play.google.com/work/` 开头。请确保将 `work` 更改为 `store`。
2. 使用 MDX Toolkit 将应用商店 URL 添加到 .mdx 文件中：

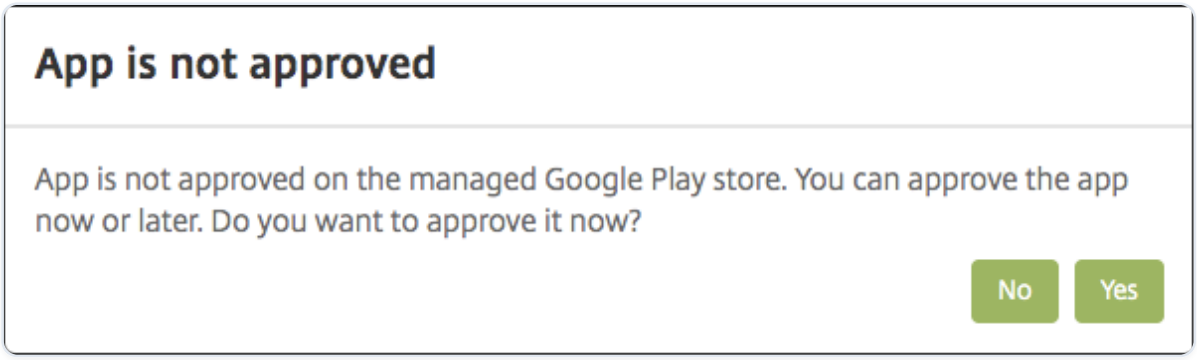
```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \

setinfo \

-in ~/Desktop/SampleApps/Sample.mdx \

-out ~/Desktop/SampleApps/wrapped/Sample.mdx \

-storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"
```

添加 .mdx 文件

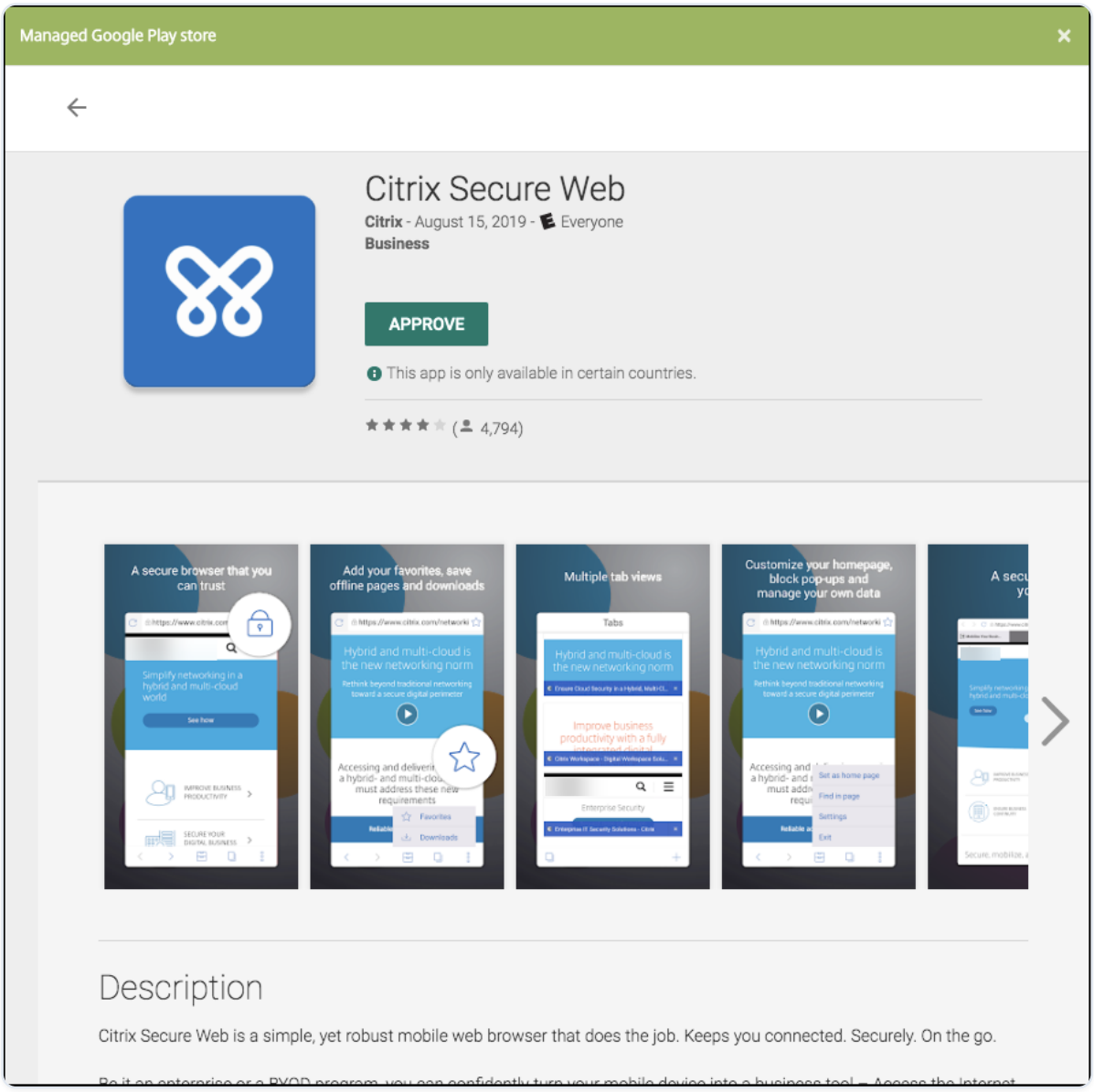
1. 在 XenMobile 控制台中，单击“**配置 > 应用程序**”。单击“**添加**”。此时将显示“**添加应用程序**”对话框。



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，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
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。
   - 如果附加的应用程序需要托管 Google Play 商店的批准，UI 会通知您。要在不离开 XenMobile 控制台的情况下批准应用程序，请单击“**是**”。



托管 Google Play 商店打开后，按照说明批准并保存应用程序。



成功添加应用程序后，将显示“**应用程序详细信息**”页面。

5. 配置以下设置：

- **文件名：** 键入与应用程序关联的文件名。
- **应用程序描述：** 键入应用程序的描述。
- **应用程序版本：** （可选）键入应用程序版本号。
- **程序包 ID：** 键入从托管 Google Play 商店获取的应用程序的程序包 ID。
- **最低操作系统版本：** （可选）键入设备可运行的用于使用此应用程序的最早操作系统版本。
- **最高操作系统版本：** （可选）键入设备必须运行的用于使用此应用程序的最新操作系统。
- **排除的设备：** （可选）键入无法运行此应用程序的设备的制造商或型号。

6. 配置 **MDX 策略**。MDX 策略因平台而异，包括身份验证、设备安全和应用程序限制等策略区域的选项。在控制台中，每个策略都有一个描述该策略的工具提示。有关适用于每种设备平台类型的应用程序策略的信息，请参阅：

   - MAM SDK 概述
   - MDX 第三方应用程序策略一览

7. 配置部署规则和应用商店配置。

   部署以实现始终在线连接 在 **设置 > 服务器属性** 中配置计划后台部署密钥时适用。

   始终在线选项：

   - 不适用于从版本 10.18.19 或更高版本开始使用 Endpoint Management 的 Android Enterprise 客户
   - 不建议从版本 10.18.19 之前开始使用 Endpoint Management 的 Android Enterprise 客户使用

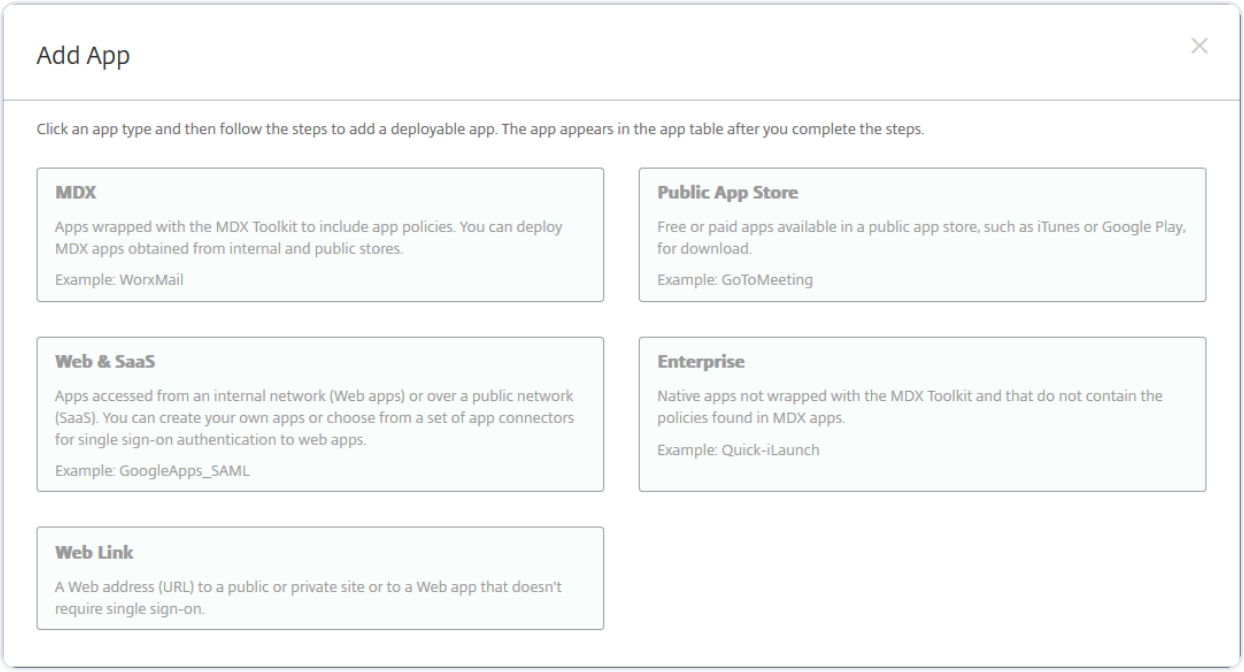
   您配置的部署计划适用于所有平台。您所做的任何更改都适用于所有平台，但 **部署以实现始终在线连接** 除外。

8. 将任何交付组分配给应用程序，然后单击**保存**。有关详细信息，请参阅部署资源。

更新应用程序

要更新 Android Enterprise 应用程序，请打包并上载更新的 .apk 文件：

1. 使用 MAM SDK 或 MDX Toolkit 打包更新应用程序的 .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。此名称将列在“应用程序”表中的“应用程序名称”下。
   - **说明：**键入应用程序的可选说明。
   - **应用程序类别：**（可选）在列表中，单击要向其中添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
5. 选择 **Android Enterprise** 作为平台。
6. 单击**下一步**。此时将显示 **Android Enterprise 企业应用程序**页面。
7. 单击**上载**。
8. 在托管的 Google Play 商店页面中，选择要更新的应用程序。
9. 在应用信息页面中，单击 .apk 文件名旁边的**编辑**。

   编辑应用(/en-us/xenmobile/server/media/publish-enterprise-app.png)
10. 导航到新的 .apk 文件并上传它。
11. 在托管 Google Play 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

Google Workspace（以前称为 G Suite）客户必须使用旧版 Android Enterprise 设置来配置旧版 Android Enterprise。

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运行 Android 5.0+ Lollipop 的设备
- 已安装 Google Play 的 Google 帐户
- 设备上已设置工作配置文件

要开始配置旧版 Android Enterprise，请在 XenMobile® 设置的 **Android Enterprise** 页面中单击 **legacy Android Enterprise**。

旧版 Android Enterprise 选项的图像(/en-us/xenmobile/server/media/android-for-work-legacy-1.png)

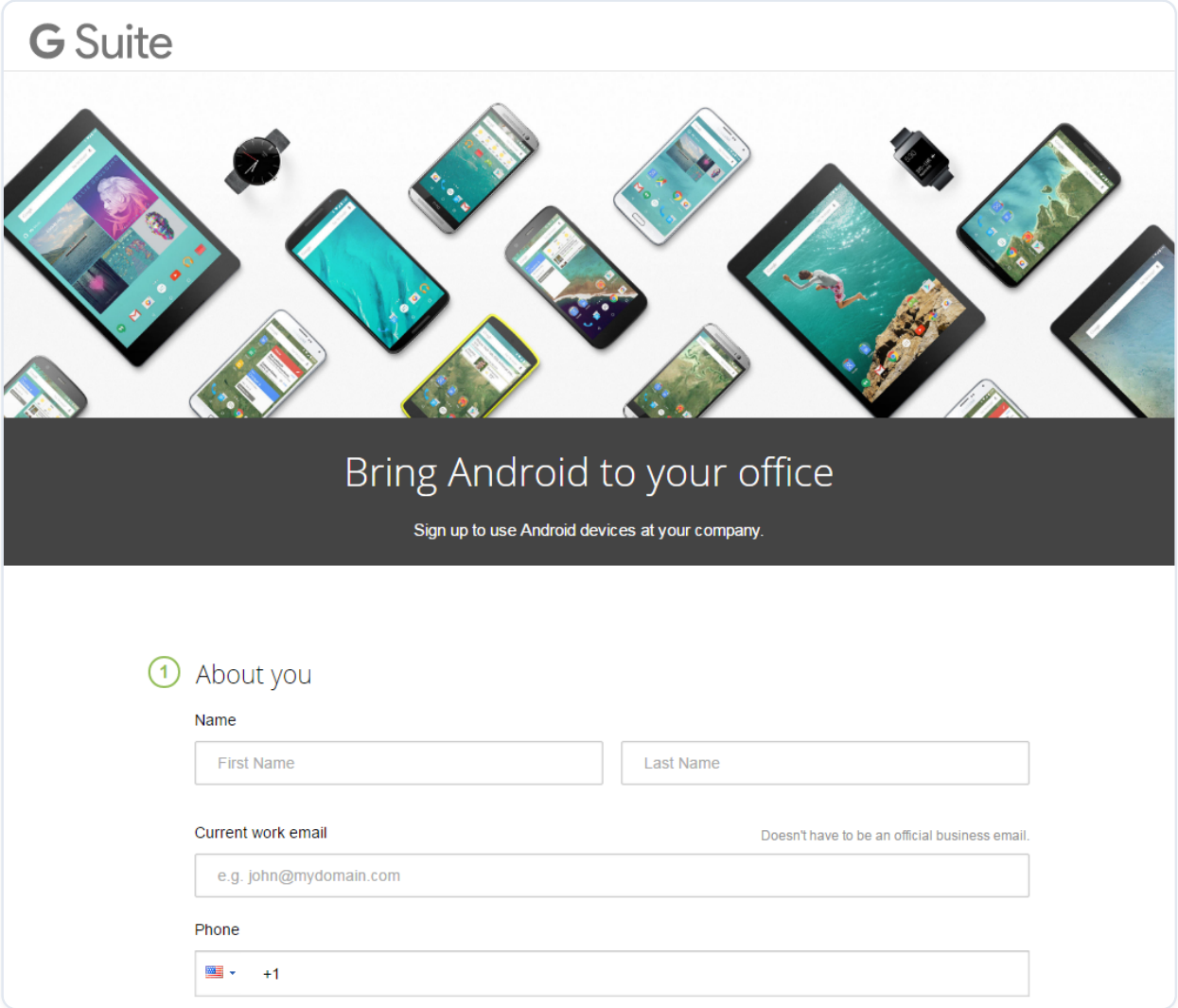
创建 Android Enterprise 帐户

在设置 Android Enterprise 帐户之前，您必须向 Google 验证您的域名。

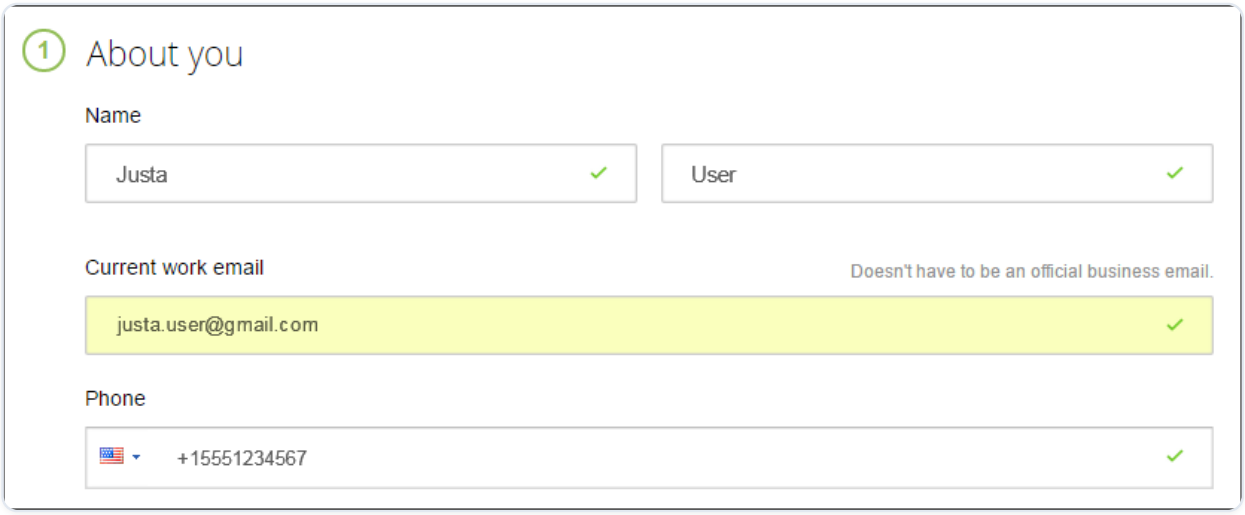
如果您已向 Google 验证您的域名，则可以跳到此步骤：设置 Android Enterprise 服务帐户并下载 Android Enterprise 证书。

1. 导航到 `<https://gsuite.google.com/signup/basic/welcome>`。

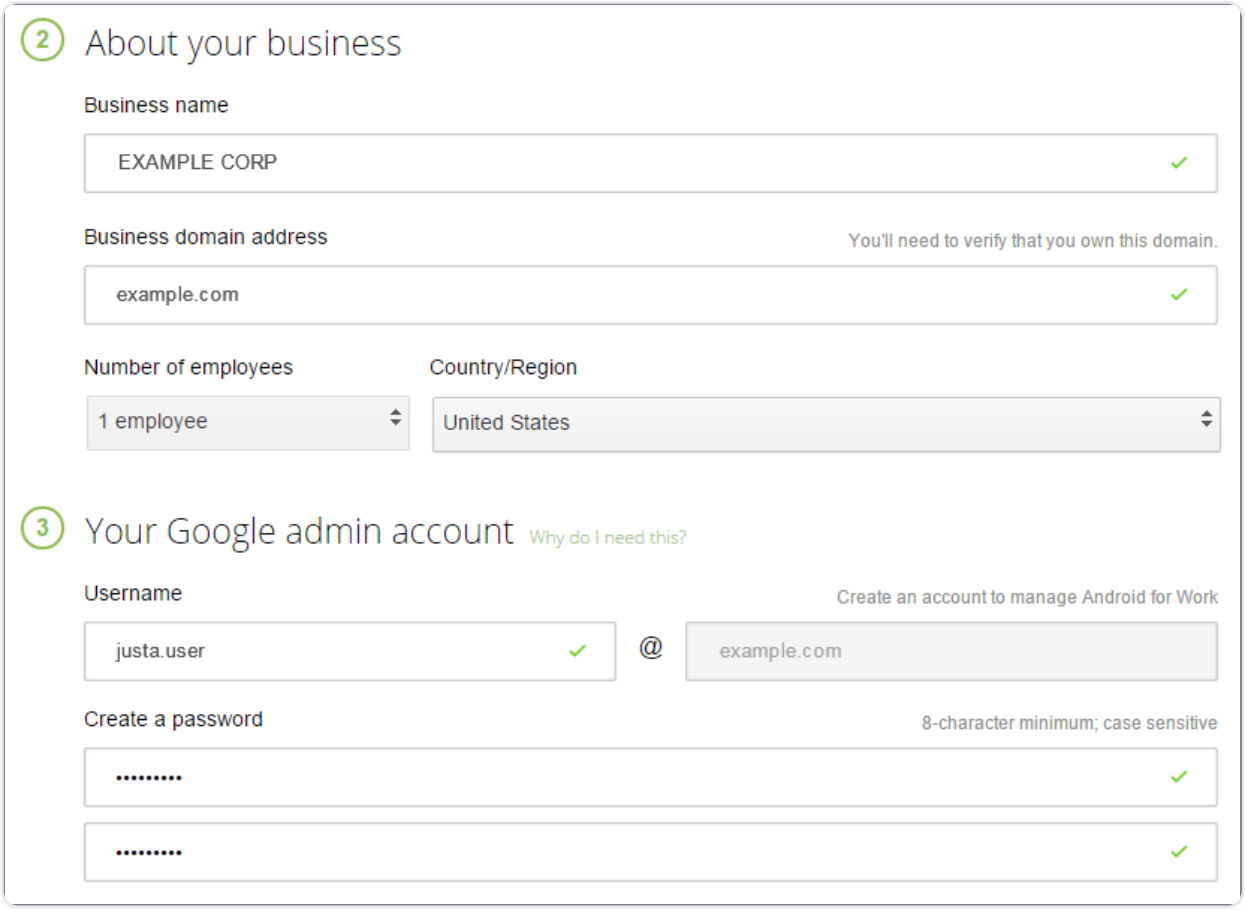
   以下页面显示您输入管理员和公司信息的位置。



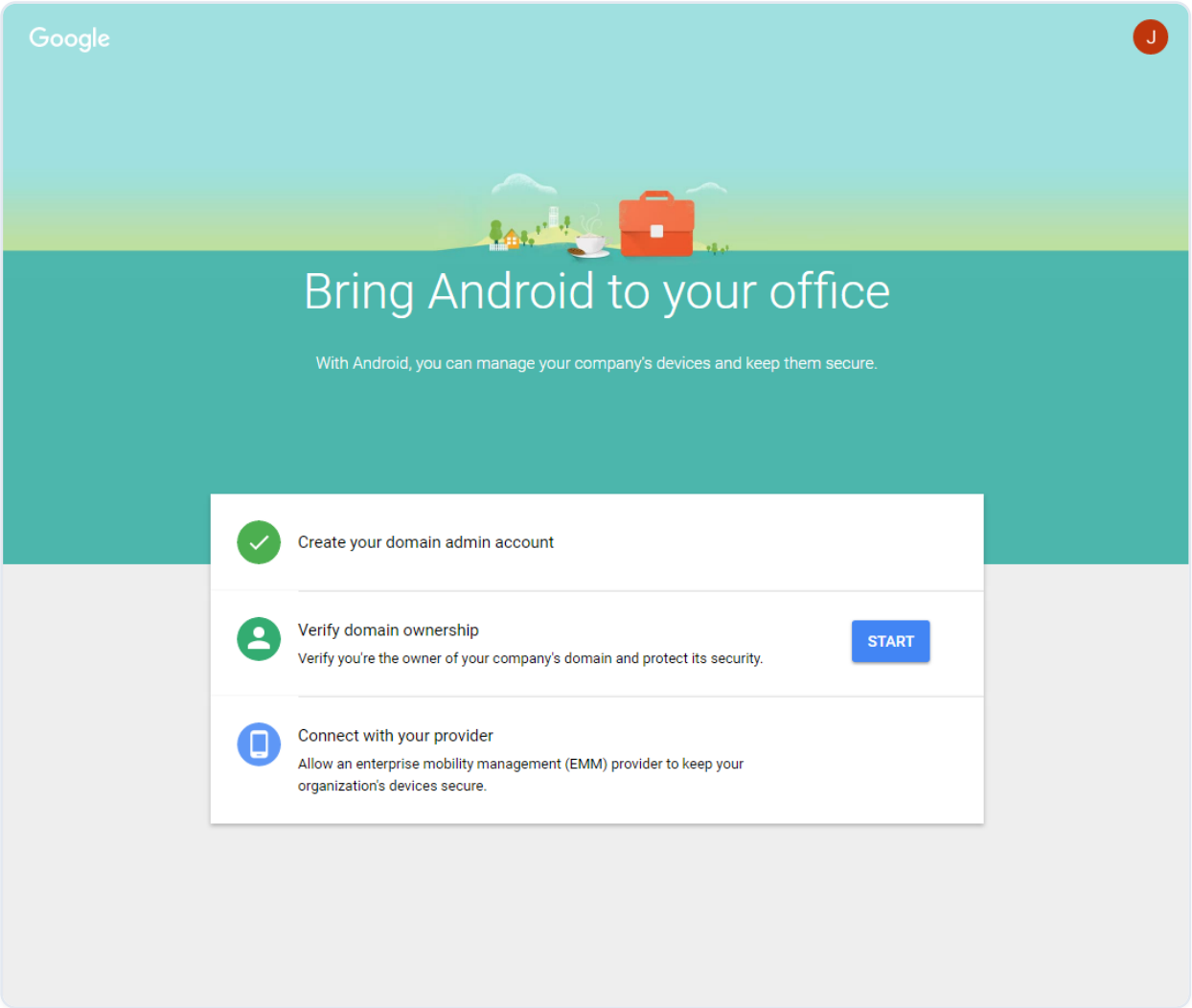
2. 输入您的管理员用户信息。



3. 除了管理员账户信息之外，还要输入您的公司信息。



此过程的第一步已完成，您将看到以下页面。



验证域所有权

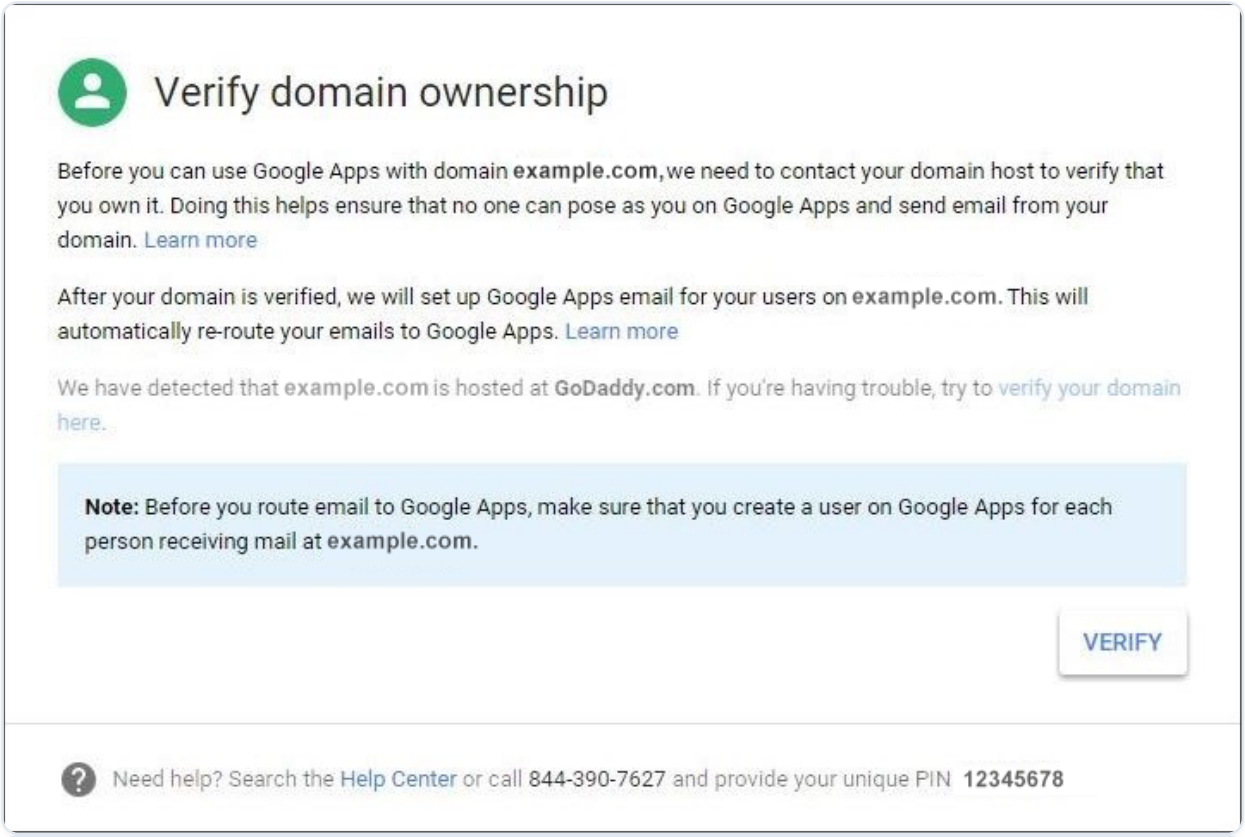
允许 Google 通过以下任一方式验证您的域：

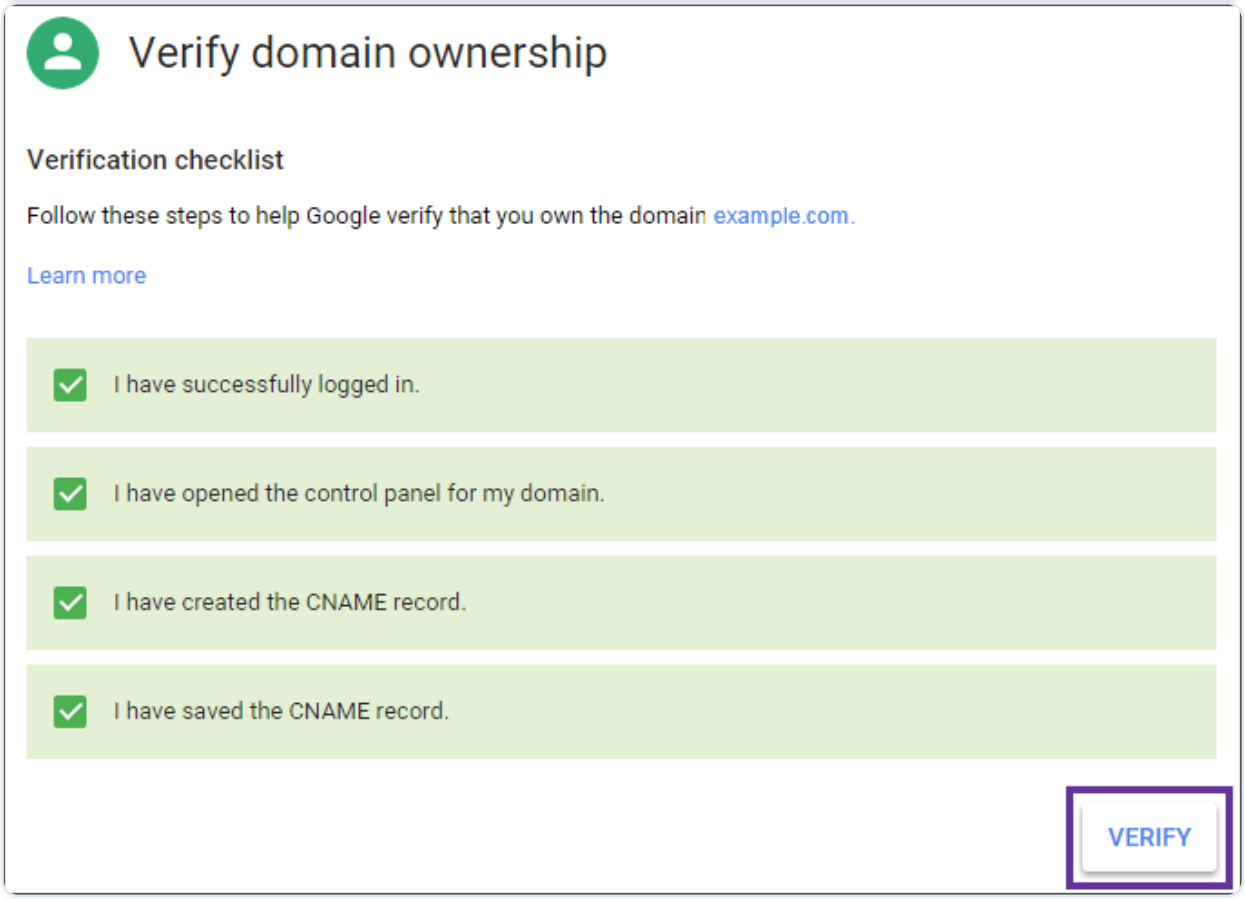
- 将 TXT 或 CNAME 记录添加到您的域主机网站。
- 将 HTML 文件上传到您的域的 Web 服务器。
- 将 `<meta>` 标记添加到您的主页。Google 建议使用第一种方法。本文不介绍验证域所有权的步骤，但您可以在此处找到所需信息：https://support.google.com/a/answer/6248925。

1. 单击“**开始**”以开始验证您的域。

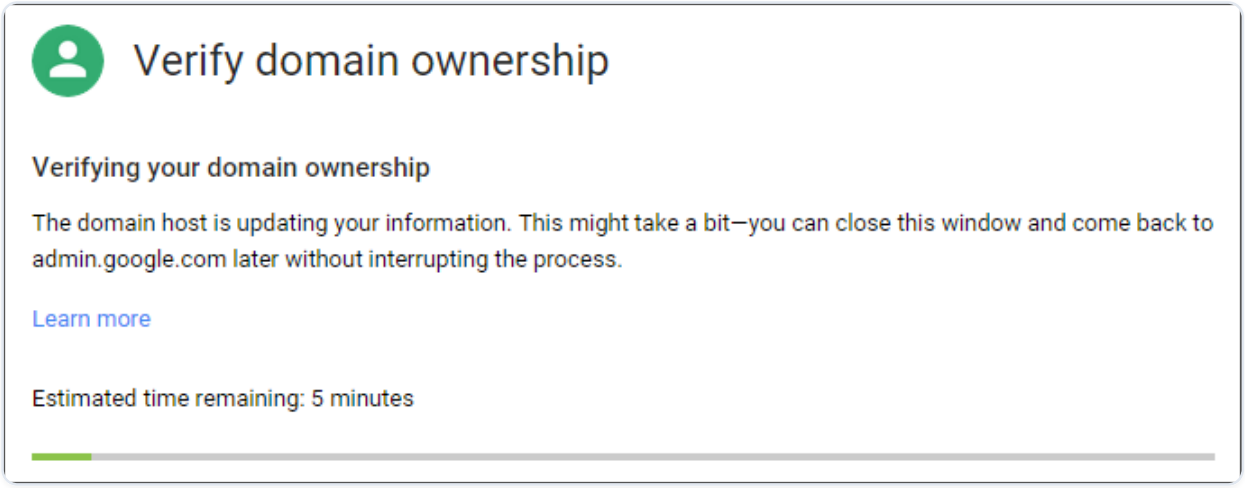
   将显示“**验证域所有权**”页面。按照页面上的说明验证您的域。

2. 单击“**验证**”。

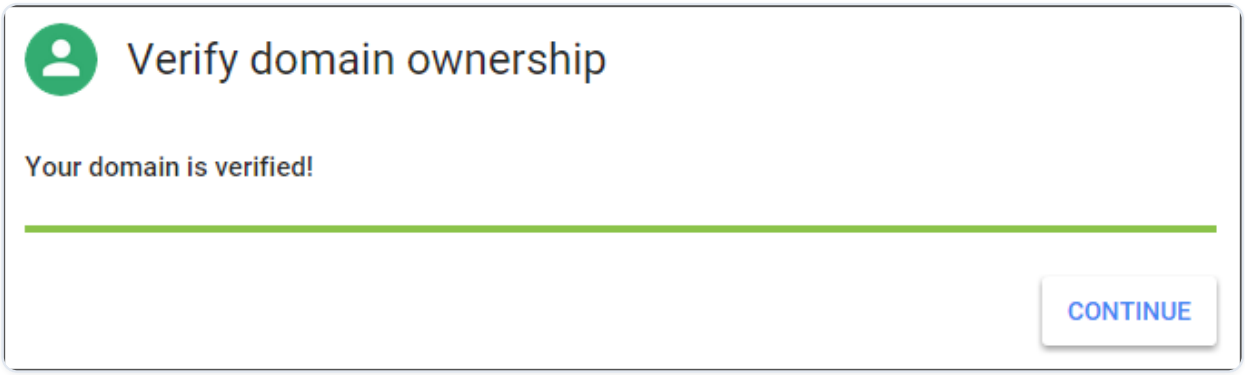




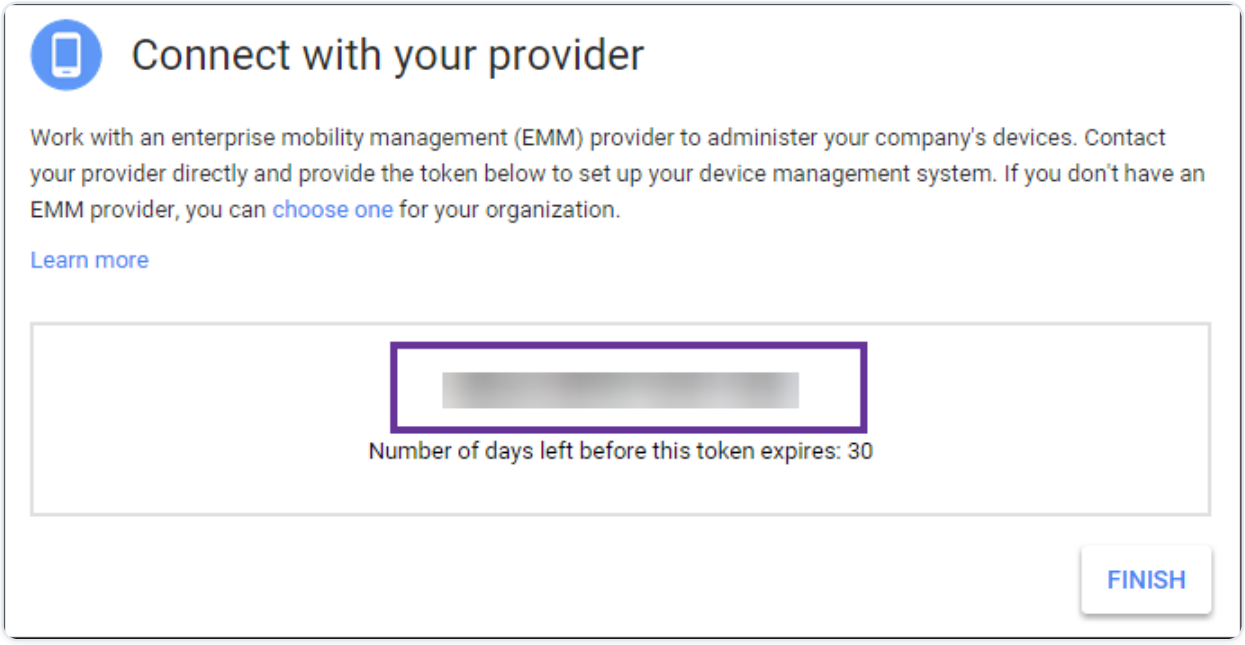
3. Google 验证您的域所有权。



4. 成功验证后，将显示以下页面。单击**继续**。



5. Google 会创建一个 EMM 绑定令牌，您需要将其提供给 Citrix® 并在配置 Android Enterprise 设置时使用。 复制并保存该令牌；在后续设置过程中需要用到它。



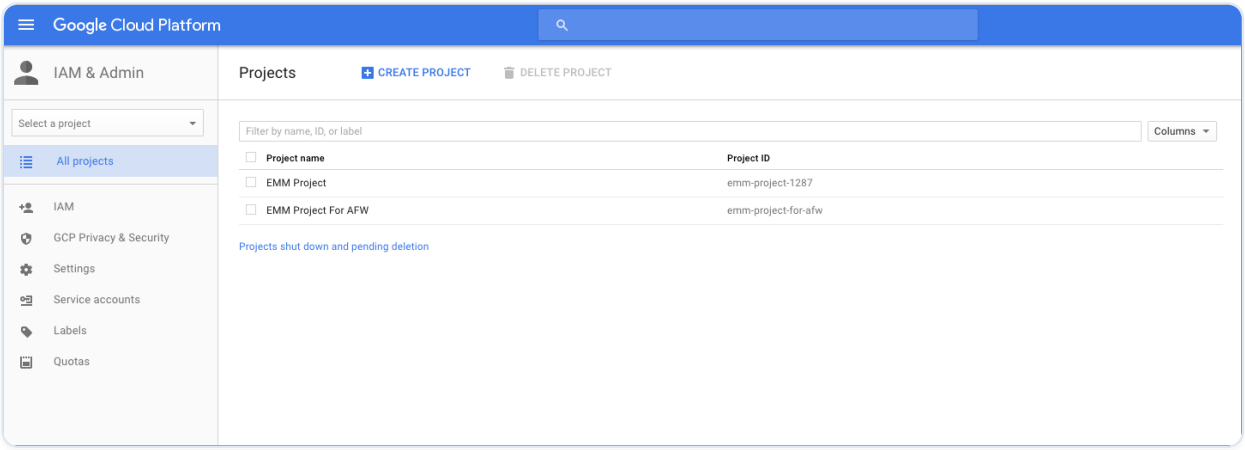
6. 单击**完成**以完成 Android Enterprise 的设置。此时将显示一个页面，指示您已成功验证域。

创建 Android Enterprise 服务帐户后，您可以登录 Google 管理控制台来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 和目录服务，您必须使用面向开发人员的 Google Project 门户创建服务帐户。此服务帐户用于 XenMobile 与 Google Android 服务之间的服务器到服务器通信。有关所用身份验证协议的详细信息，请访问 `<https://developers.google.com/identity/protocols/OAuth2ServiceAccount>`。

1. 在 Web 浏览器中，转至 `<https://console.cloud.google.com/project>` 并使用您的 Google 管理员凭据登录
2. 在**项目**列表中，单击**创建项目**。



3. 在 **项目名称** 中，键入项目名称。

   项目名称选项的图像(/en-us/xenmobile/server/media/google-config-api-2.png)

4. 在仪表板上，单击 **使用 Google API**。

   使用 Google API 选项的图像(/en-us/xenmobile/server/media/google-config-api-6.png)

5. 单击 **库**，在 **搜索** 中，键入 **EMM**，然后单击搜索结果。

   EMM 搜索选项的图像(/en-us/xenmobile/server/media/afw-emm-search.png)

6. 在 **概览** 页面上，单击 **启用**。

   启用选项的图像(/en-us/xenmobile/server/media/afw-emm-enable.png)

7. 在 **Google Play EMM API** 旁边，单击 **转到凭据**。

   转到凭据选项的图像(/en-us/xenmobile/server/media/google-config-api-13.png)

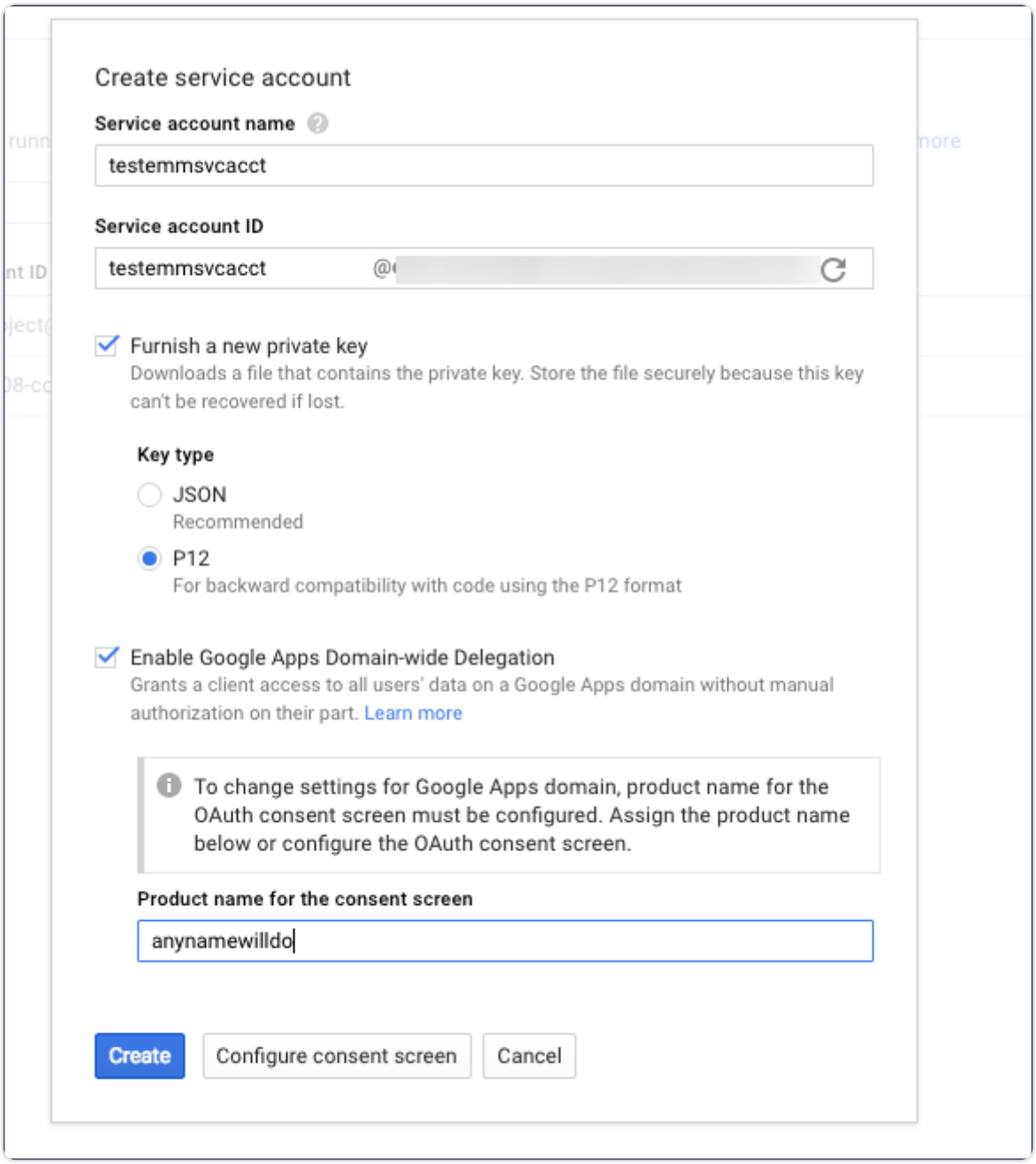
8. 在 **将凭据添加到我们的项目** 列表中，在步骤 1 中，单击 **服务帐户**。

   服务帐户选项的图像(/en-us/xenmobile/server/media/google-config-api-1b.png)

9. 在 **服务帐户** 页面上，单击 **创建服务帐户**。

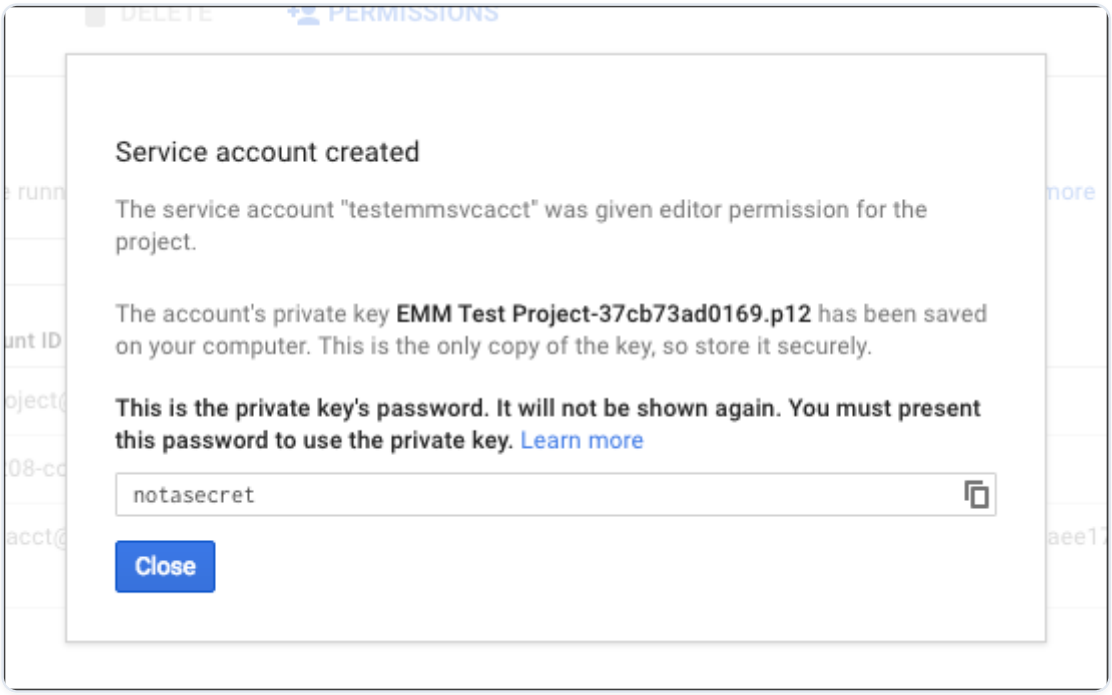
创建服务帐户选项的图像(/en-us/xenmobile/server/media/google-config-api-1e.png)

10. 在 **创建服务帐户** 中，命名帐户，并选中 **提供新私钥** 复选框。单击 **P12**，选中 **启用 Google Apps 域范围委派** 复选框，然后单击 **创建**。

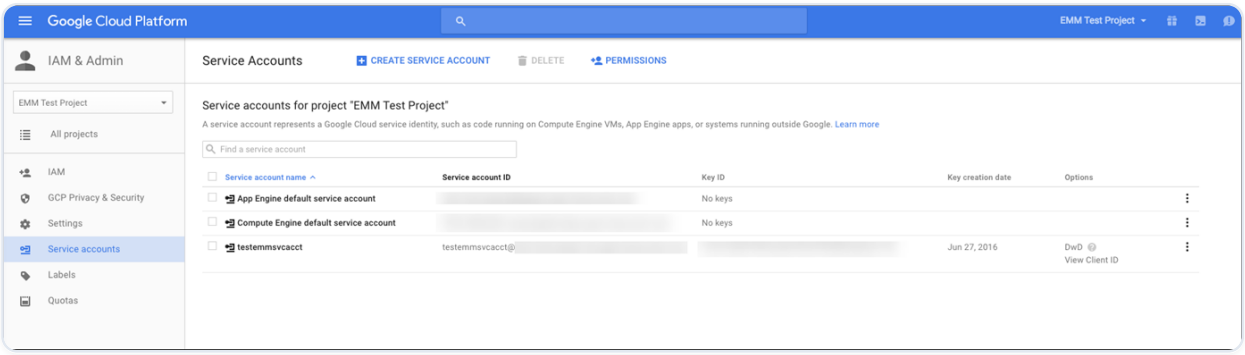


证书（P12 文件）已下载到您的计算机。请务必将证书保存在安全位置。

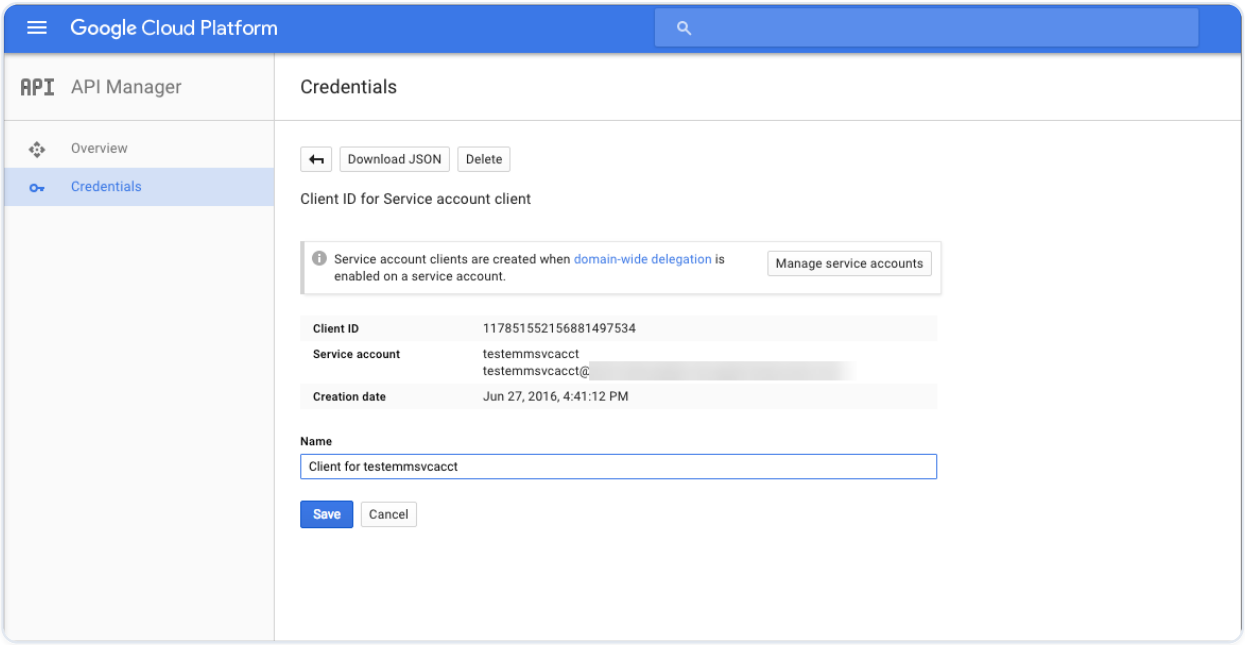
11. 在“**服务帐户已创建**”确认页面上，单击“**关闭**”。



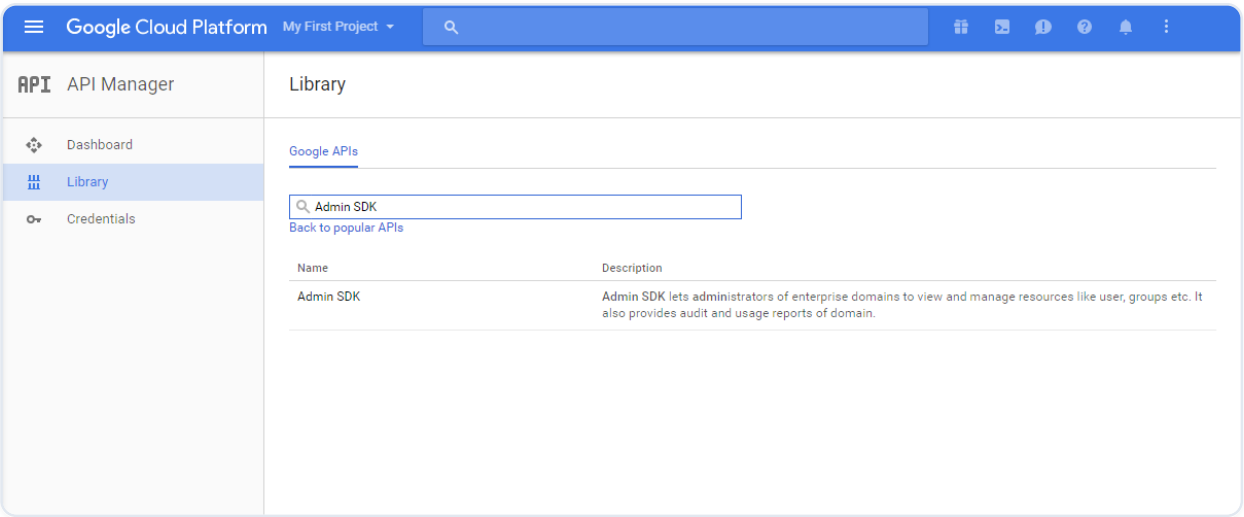
12. 在“**权限**”中，单击“**服务帐户**”，然后在您的服务帐户的“**选项**”下，单击“**查看客户端 ID**”。



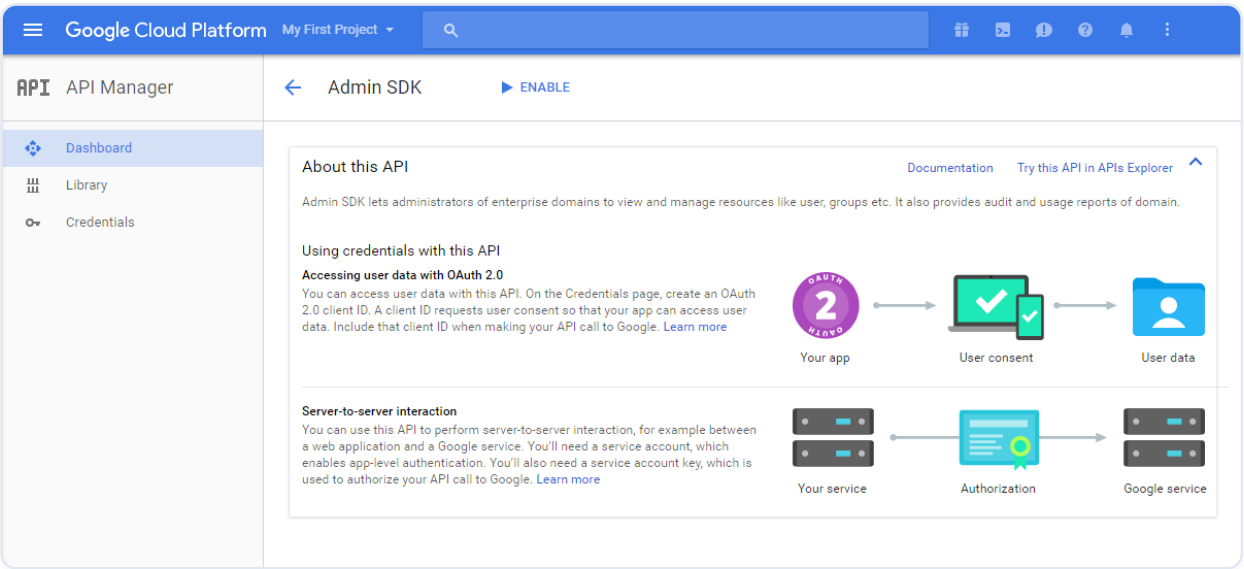
13. Google 管理控制台上帐户授权所需的详细信息将显示。将“**客户端 ID**”和“**服务帐户 ID**”复制到以后可以检索信息的位置。您需要此信息以及域名，以便发送给 Citrix 支持以进行允许。



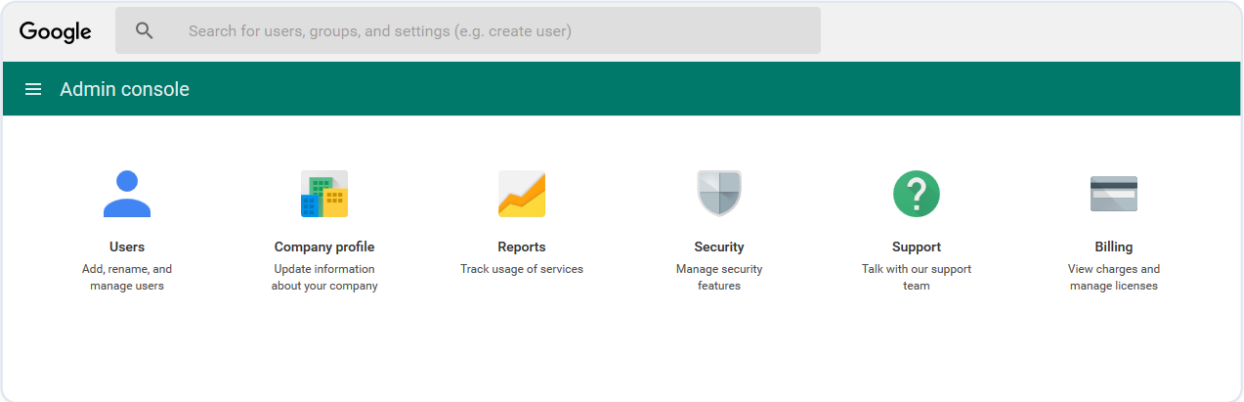
14. 在“**库**”页面上，搜索“**Admin SDK**”，然后单击搜索结果。



15. 在“**概览**”页面上，单击“**启用**”。



16. 打开您的域的 Google 管理控制台，然后单击“**安全性**”。



17. 在“**设置**”页面上，单击“**显示更多**”，然后单击“**高级设置**”。

高级设置的图像(/en-us/xenmobile/server/media/afw-admin-console-security-2.png)

高级设置的图像(/en-us/xenmobile/server/media/afw-admin-console-security-3.png)

18. 单击“**管理 API 客户端访问**”。

    管理 API 客户端访问选项的图像(/en-us/xenmobile/server/media/afw-admin-console-security-4.png)

19. 在“**客户端名称**”中，键入您之前保存的客户端 ID，在“**一个或多个 API 范围**”中，键入 `https://www.googleapis.com/auth/admin.directory.user`，然后单击“**授权**”。

    客户端名称选项的图像(/en-us/xenmobile/server/media/google-config-API-1l.png)

绑定到 EMM

在使用 XenMobile 管理 Android 设备之前，您必须联系 Citrix 技术支持并提供您的域名、服务帐户和绑定令牌。Citrix 会将令牌绑定到 XenMobile，作为您的企业移动性管理 (EMM) 提供商。有关 Citrix 技术支持的联系信息，请参阅 Citrix 技术支持。

1. 要确认绑定，请登录 Google 管理门户，然后单击“**安全性**”。
2. 单击“**管理 Android 的 EMM 提供商**”。

   您会看到您的 Google Android Enterprise 帐户已绑定到 Citrix，作为您的 EMM 提供商。

   确认令牌绑定后，即可开始使用 XenMobile 控制台管理 Android 设备。导入您在步骤 14 中生成的 P12 证书。设置 Android Enterprise 服务器设置，启用基于 SAML 的单点登录 (SSO)，并定义至少一个 Android Enterprise 设备策略。

   管理 Android 的 EMM 提供商选项的图像(/en-us/xenmobile/server/media/afw-verify-emm-binding.png)

导入 P12 证书

请按照以下步骤导入您的 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**”。“**证书**”页面随即显示。

   证书页面图像(/en-us/xenmobile/server/media/afw-certificates-page.png)

3. 单击“**导入**”。“**导入**”对话框随即显示。

   导入对话框图像(/en-us/xenmobile/server/media/afw-import-certificate-detail.png)

   配置以下设置：

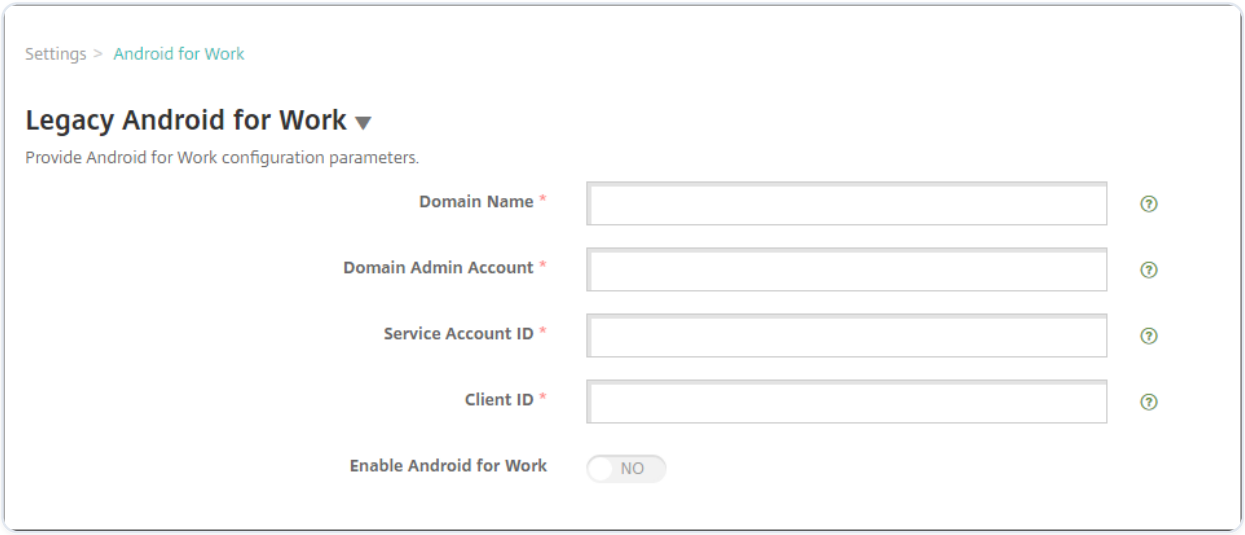
   - **导入：** 在列表中，单击“**密钥库**”。

- **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**”并导航到 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。“**设置**”页面随即显示。
2. 在 **服务器** 下，单击 **Android Enterprise**。**Android Enterprise** 页面随即显示。



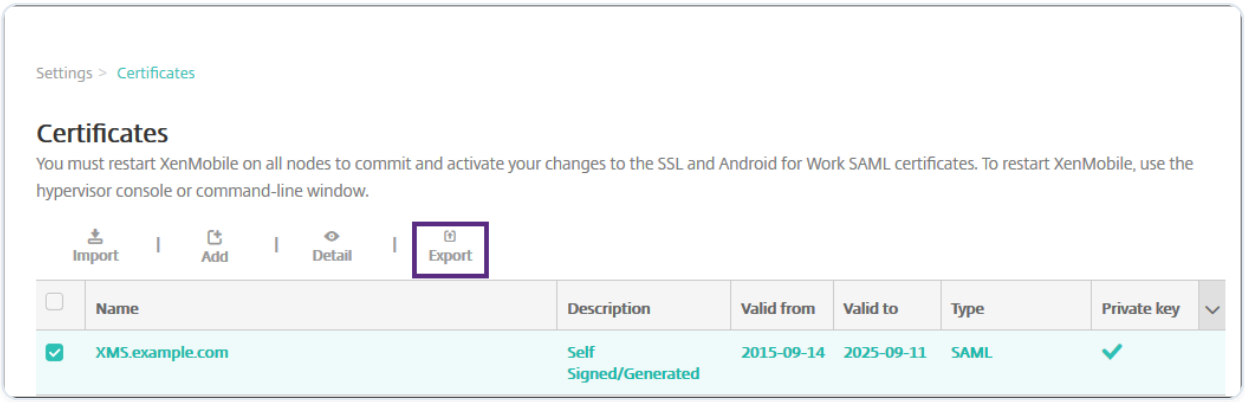
配置以下设置，然后单击 **保存**。

- **域名：** 键入您的 Android Enterprise 域名；例如，domain.com。
- **域管理员帐户：** 键入您的域管理员用户名；例如，用于 Google Developer Portal 的电子邮件帐户。
- **服务帐户 ID：** 键入您的服务帐户 ID；例如，Google 服务帐户中关联的电子邮件（`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`）。
- **客户端 ID：** 键入您的 Google 服务帐户的数字客户端 ID。
- **启用 Android Enterprise：** 选择以启用或禁用 Android Enterprise。

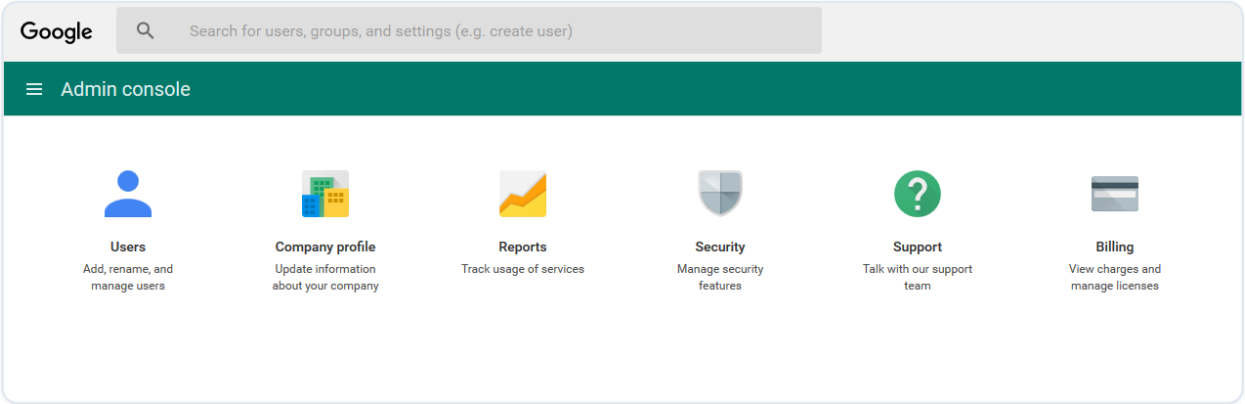
启用基于 SAML 的单点登录

1. 登录到 XenMobile 控制台。
2. 单击控制台右上角的齿轮图标。**设置** 页面随即显示。

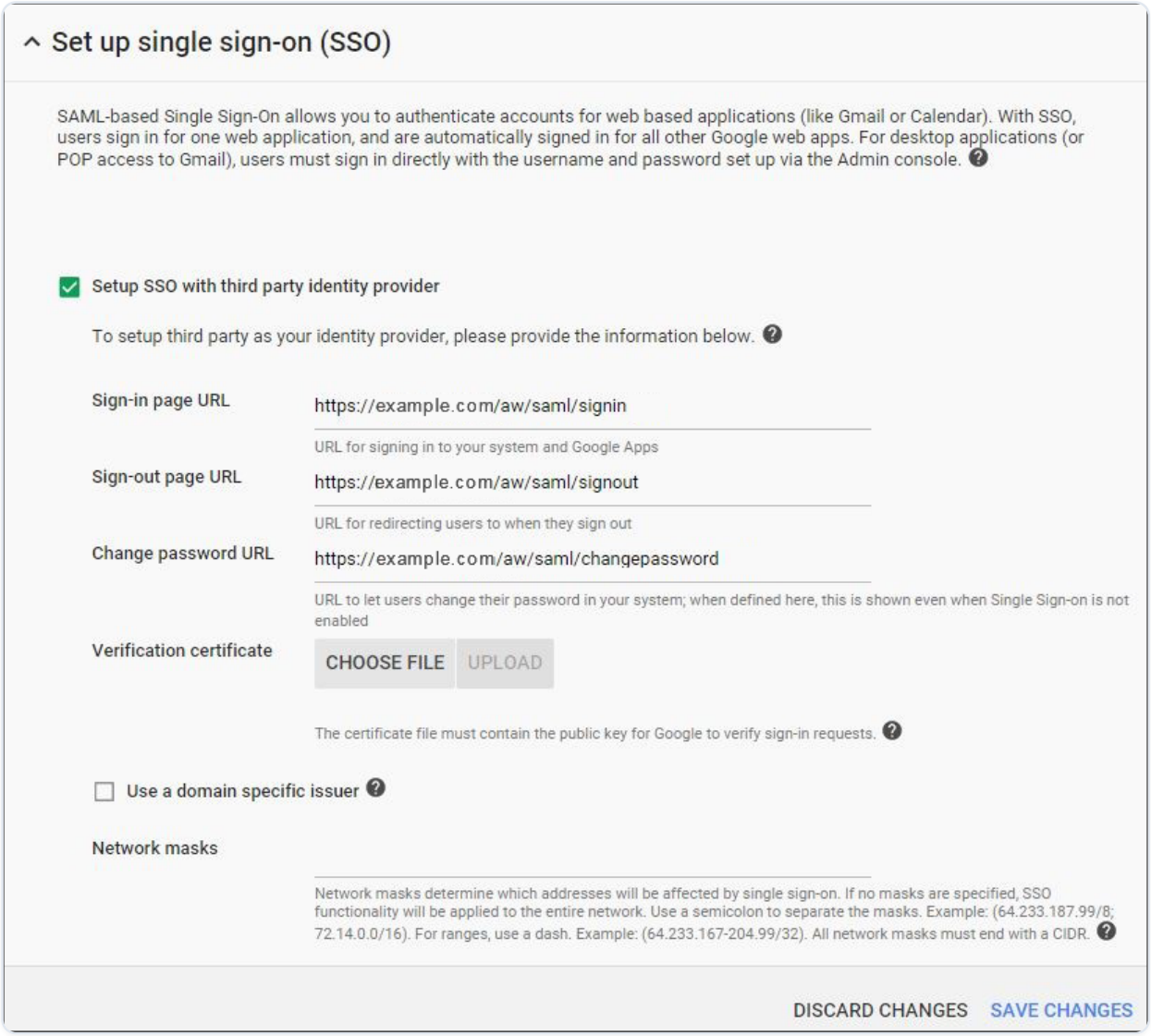
3. 单击 **证书**。**证书** 页面随即显示。



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。要访问该门户，请参阅 Google 管理门户。
7. 单击“**安全性**”。



8. 在“**安全性**”下，单击“**设置单点登录 (SSO)**”，然后配置以下设置。

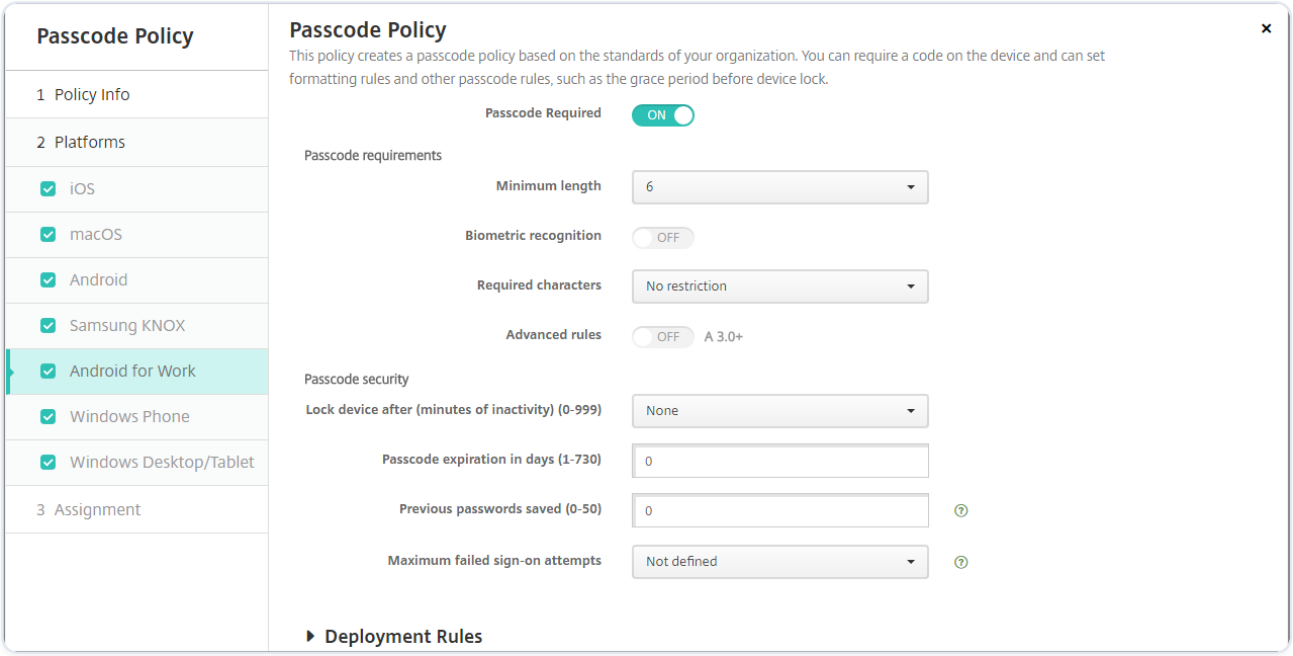


- **登录页面 URL：** 键入用户登录您的系统和 Google Apps 的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/signin`。
- **注销页面 URL：** 键入用户注销时重定向到的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/signout`。
- **更改密码 URL：** 键入允许用户在您的系统中更改密码的 URL。例如：`https://<Xenmobile-FQDN>/aw/saml/changepassword`。如果定义了此字段，即使 SSO 不可用，用户也会看到此提示。
- **验证证书：** 单击“**选择文件**”，然后导航到从 XenMobile 导出的 SAML 证书。

9. 单击“**保存更改**”。

设置 Android Enterprise 设备策略

设置密码策略，以便用户在首次注册时必须在其设备上建立密码。



设置任何设备策略的基本步骤如下。

1. 登录 XenMobile 控制台。
2. 点击“**配置**”，然后点击“**设备策略**”。
3. 点击“**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，您点击“**密码**”。
4. 完成“**策略信息**”页面。
5. 点击“**Android Enterprise**”，然后配置该策略的设置。
6. 将策略分配给交付组。

配置 Android Enterprise 帐户设置

在开始管理设备上的 Android 应用程序和策略之前，您必须在 XenMobile 中设置 Android Enterprise 域和帐户信息。首先，在 Google 上完成 Android Enterprise 设置任务，以设置域管理员并获取服务帐户 ID 和绑定令牌。

1. 在 XenMobile Web 控制台中，点击右上角的齿轮图标。此时将显示“**设置**”页面。
2. 在“**服务器**”下，点击“**Android Enterprise**”。此时将显示“**Android Enterprise**”配置页面。

Android Enterprise 配置页面的图像(/en-us/xenmobile/server/media/settings-server-legacy-android-for-work-1.png)

1. 在“**Android Enterprise**”页面上，配置以下设置：
   - **域名：** 键入您的域名。
   - **域管理员帐户：** 键入您的域管理员用户名。
   - **服务帐户 ID：** 键入您的 Google 服务帐户 ID。

- **客户端 ID::** 键入您的 Google 服务帐户的客户端 ID。
- **启用 Android Enterprise：** 选择是否启用 Android Enterprise。

2. 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 和您的 Google Workspace 域之间进行通信。例如，XenMobile 需要 API 来实现管理 Chrome 功能（如无痕模式和访客模式）的设备策略。

要启用合作伙伴 API，请在 XenMobile 控制台中设置您的 Google Workspace 域，然后配置您的 Google Workspace 帐户。

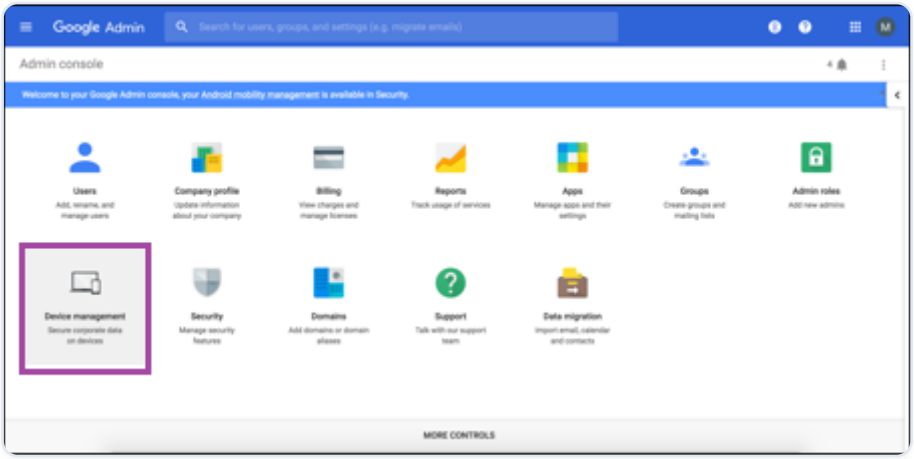
在 XenMobile 中设置您的 Google Workspace（以前称为 G Suite）域

要使 XenMobile 能够与您的 Google Workspace 域中的 API 进行通信，请转到“**设置 > Google Chrome 配置**”并配置设置。

- **G Suite 域：** 托管 XenMobile 所需 API 的 Google Workspace 域。
- **G Suite 管理员帐户：** 您的 G Suite 域的管理员帐户。
- **G Suite 客户端 ID：** Citrix 的客户端 ID。使用此值配置您的 Google Workspace 域的合作伙伴访问权限。
- **G Suite 企业 ID：** 您的帐户的企业 ID，从您的 Google 企业帐户中填写。

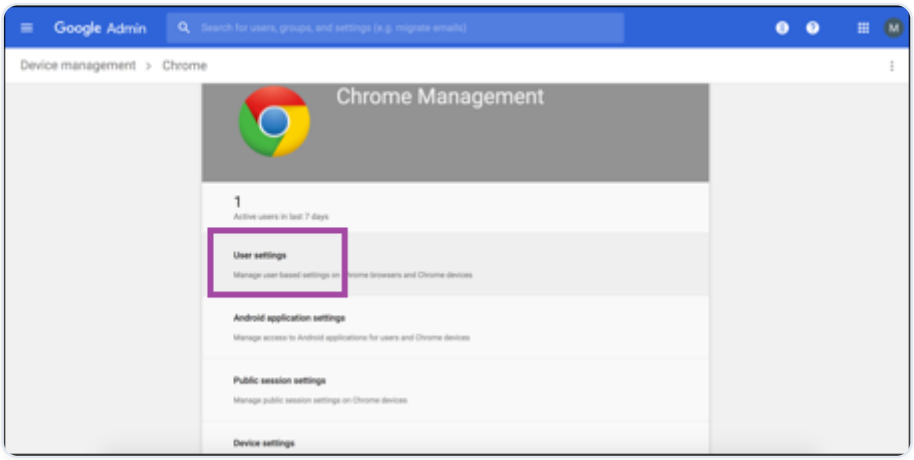
为 Google Workspace 域中的设备和用户启用合作伙伴访问权限

1. 登录 Google 管理控制台：`<https://admin.google.com>`
2. 单击“**设备管理**”。



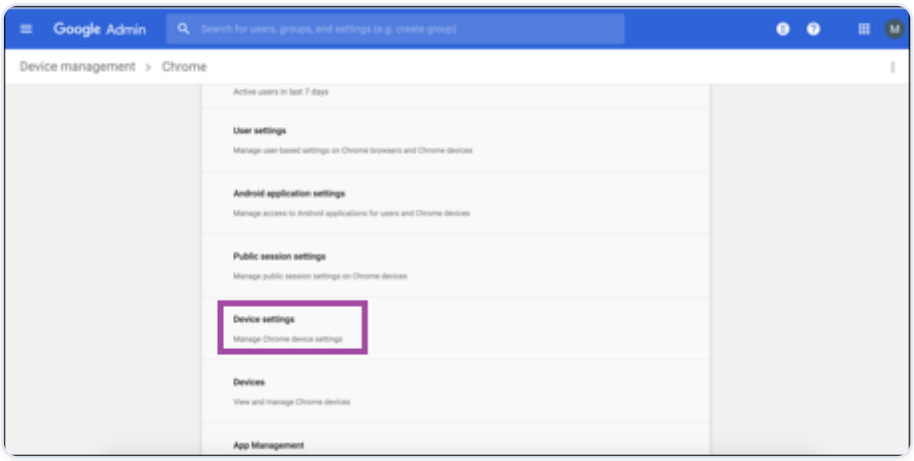
3. 点击 **Chrome 管理**。

4. 点击 **用户设置**。



5. 搜索 **Chrome 管理 - 合作伙伴访问**。

6. 选中“**启用 Chrome 管理 - 合作伙伴访问**”复选框。
7. 同意您理解并希望启用合作伙伴访问。点击 **保存**。
8. 在 Chrome 管理页面中，点击 **设备设置**。



9. 搜索 **Chrome 管理 - 合作伙伴访问**。

10. 选中“**启用 Chrome 管理 - 合作伙伴访问**”复选框。
11. 同意您理解并希望启用合作伙伴访问。点击 **保存**。
12. 转到“**安全**”页面，然后点击 **高级设置**。

    Google 管理员控制台的图像(/en-us/xenmobile/server/media/google-admin-partner-access7.png)

13. 单击 **管理 API 客户端访问**。
14. 在 XenMobile 控制台中，转到 **设置 > Google Chrome 配置** 并复制 Google Workspace 客户端 ID 的值。然后，返回到 **管理 API 客户端访问** 页面并将复制的值粘贴到 **客户端名称** 字段。
15. 在 **一个或多个 API 范围** 中，添加 URL：`https://www.googleapis.com/auth/chromedevicemanagementapi`

    Google 管理员控制台的图像(/en-us/xenmobile/server/media/google-admin-partner-access8.png)

16. 单击 **授权**。

    消息“您的设置已保存”出现。

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/restrictions-device-policy-ios113.png)

注册 Android Enterprise 设备

如果您的设备注册过程要求用户输入用户名或用户 ID，则接受的格式取决于 XenMobile Server 配置为通过用户主体名称 (UPN) 或 SAM 帐户名称搜索用户的方式。

如果 XenMobile Server 配置为通过 UPN 搜索用户，用户必须按以下格式输入 UPN：

- *用户名@域名*

如果 XenMobile Server 配置为通过 SAM 搜索用户，用户必须按以下任一格式输入 SAM：

- *用户名@域名*
- *domain\username*

要确定您的 XenMobile Server 配置为哪种类型的用户名：

1. 在 XenMobile Server 控制台中，单击右上角的齿轮图标。将显示“**设置**”页面。
2. 单击“**LDAP**”以查看 LDAP 连接的配置。
3. 在页面底部，查看“**用户搜索依据**”字段：
    - 如果设置为 **userPrincipalName**，则 XenMobile Server 已设置为 UPN。
    - 如果设置为 **sAMAccountName**，则 XenMobile Server 已设置为 SAM。

取消注册 Android Enterprise 企业

您可以使用 XenMobile Server 控制台和 XenMobile Tools 取消注册 Android Enterprise 企业。

执行此任务时，XenMobile Server 会为 XenMobile Tools 打开一个弹出窗口。开始之前，请确保 XenMobile Server 具有在您使用的浏览器中打开弹出窗口的权限。某些浏览器（例如 Google Chrome）要求您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。

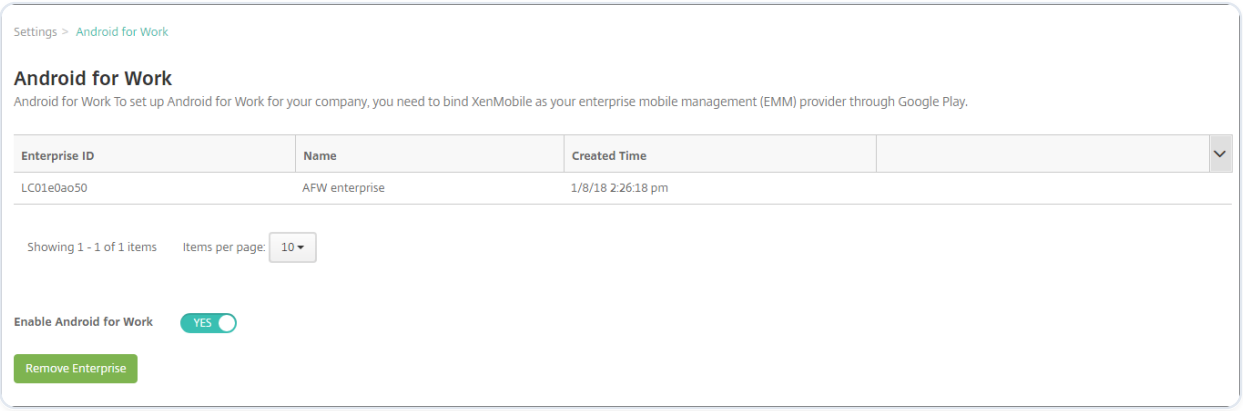
> **警告：**
>
> 企业取消注册后，已通过该企业注册的设备上的 Android Enterprise 应用程序将重置为其默认状态。这些设备将不再由 Google 管理。在 Android Enterprise 企业中重新注册它们可能无法在不进行进一步配置的情况下恢复以前的功能。

> Android Enterprise 企业取消注册后：

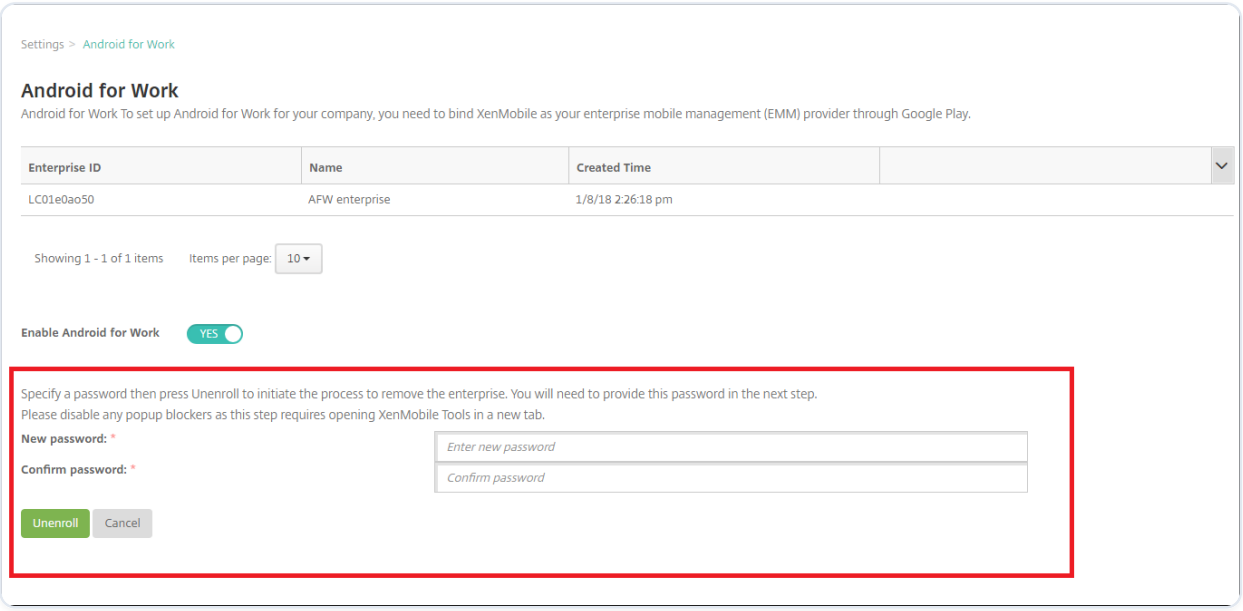
- 通过企业注册的设备和用户，其 Android Enterprise 应用程序将重置为默认状态。以前应用的 Android Enterprise 应用程序权限和 Android Enterprise 应用程序限制策略不再生效。
- 通过企业注册的设备由 XenMobile 管理，但从 Google 的角度来看是未受管理的。无法添加新的 Android Enterprise 应用程序。无法应用 Android Enterprise 应用程序权限或 Android Enterprise 应用程序限制策略。其他策略（例如计划、密码和限制）仍可应用于这些设备。
- 如果您尝试在 Android Enterprise 中注册设备，它们将注册为 Android 设备，而不是 Android Enterprise 设备。

要取消注册 Android Enterprise 企业：

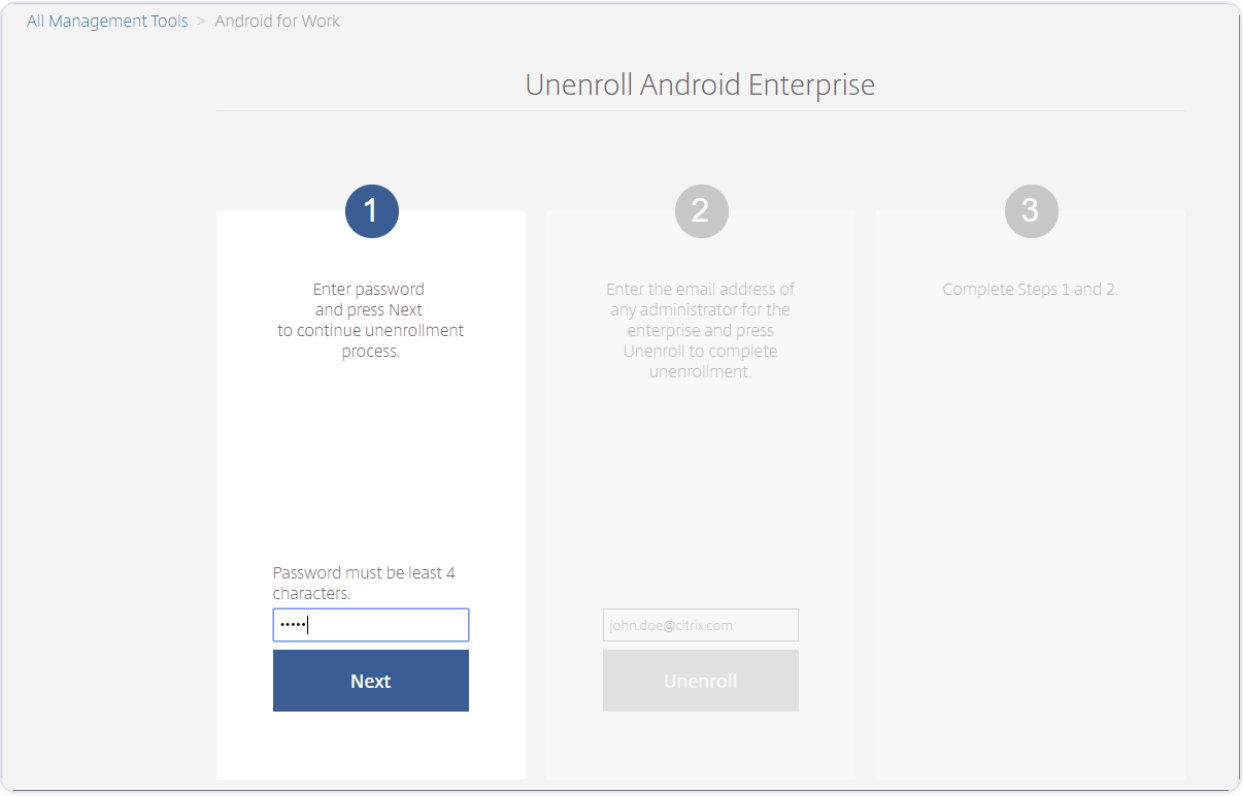
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示“设置”页面。
2. 在“设置”页面上，单击 **Android Enterprise**。
3. 单击 **移除企业**。



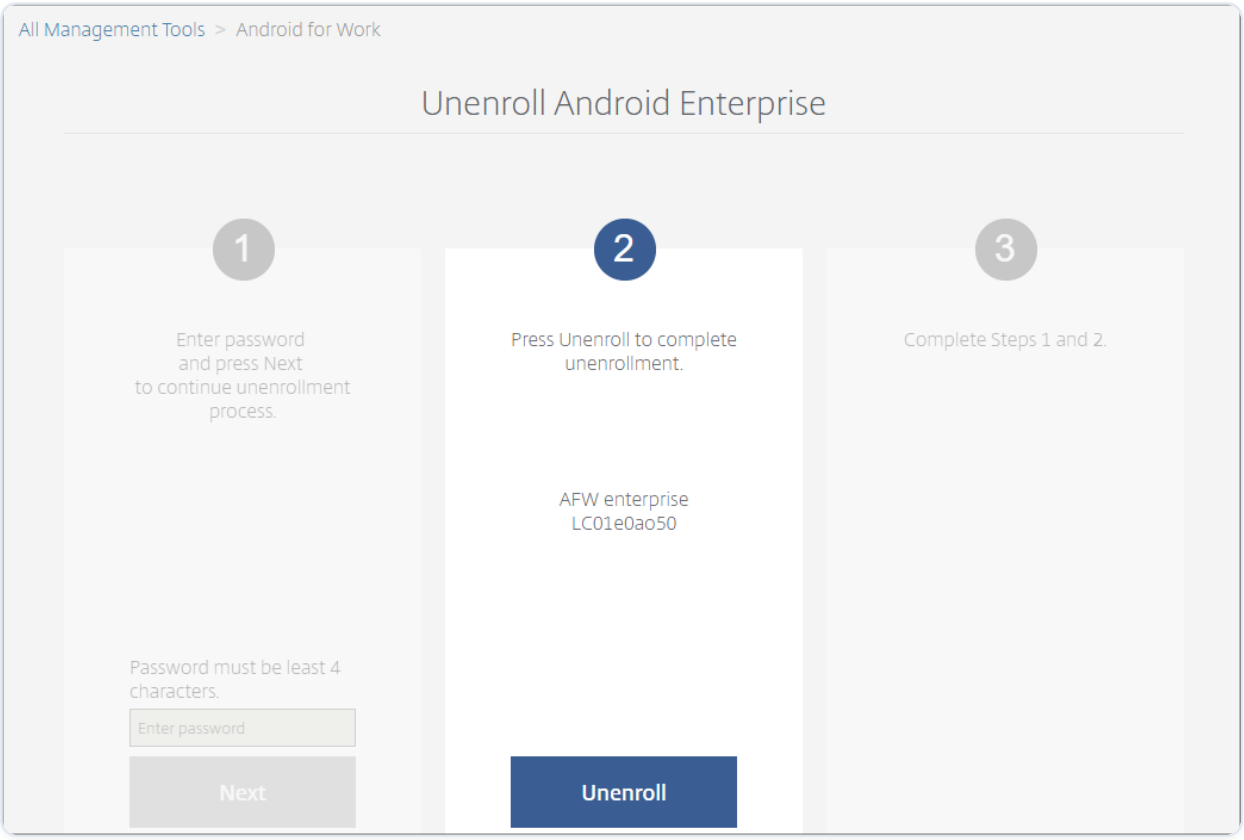
4. 指定密码。下一步需要此密码才能完成取消注册。然后单击 **Unenroll**。



5. 当 XenMobile Tools 页面打开时，输入您在上一步中创建的密码。



6. 单击 **Unenroll**。



在 Android Enterprise 中预配完全托管设备

只有公司拥有的设备才能成为 Android Enterprise 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 支持以下完全托管设备的注册方法：

- **afw#xenmobile：** 使用此注册方法，用户在设置设备时输入字符“afw#xenmobile”。此令牌将设备标识为由 XenMobile 管理并下载 Secure Hub。
- **二维码：** 二维码预配是一种简单的方法，可用于预配不支持 NFC 的分布式设备群（例如平板电脑）。二维码注册方法可用于已恢复出厂设置的设备群。二维码注册方法通过从设置向导扫描二维码来设置和配置完全托管设备。
- **近场通信 (NFC) 碰撞：** NFC 碰撞注册方法可用于已恢复出厂设置的设备群。NFC 碰撞通过近场通信在两台设备之间传输数据。在已恢复出厂设置的设备上，蓝牙、Wi-Fi 和其他通信模式已禁用。NFC 是设备在此状态下可以使用的唯一通信协议。

安卓企业版#XenMobile

此注册方法用于在新设备或恢复出厂设置的设备开机后进行初始设置。当系统提示用户输入 Google 帐户时，用户输入“afw#xenmobile”。此操作会下载并安装 Secure Hub。然后，用户按照 Secure Hub 设置提示完成注册。

此注册方法推荐用于大多数客户，因为最新版本的 Secure Hub 是从 Google Play 商店下载的。与其他注册方法不同，您无需提供 Secure Hub 以便从 XenMobile Server 下载。

先决条件：

- 支持所有运行 Android 5.0 及更高版本的 Android 设备。

二维码

要使用二维码在设备模式下注册设备，您可以通过创建 JSON 并将 JSON 转换为二维码来生成二维码。设备摄像头扫描二维码以注册设备。

先决条件：

- 支持所有运行 Android 7.0 及更高版本的 Android 设备。

从 JSON 创建二维码

使用以下字段创建 JSON。

这些字段是必需的：

键：android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

值: com.zenprise/com.zenprise.configuration.AdminFunction

键: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

值: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

键: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

值: `https://path/to/securehub.apk`

> **注意：**

> 如果 Secure Hub 作为企业应用程序上传到 Citrix XenMobile Server，则可以从 `https://<fqdn>:4443/*instanceName*/worxhome.apk` 下载。Secure Hub APK 的路径必须可通过设备在预配期间连接的 Wi-Fi 连接进行访问。

> 这些字段是可选的：

- **android.app.extra.PROVISIONING_LOCALE:** 输入语言和国家/地区代码。

  语言代码是 ISO 639-1 定义的两位小写 ISO 语言代码（例如 en）。国家/地区代码是 ISO 3166-1 定义的两位大写 ISO 国家/地区代码（例如 US）。例如，输入 en_US 表示在美国使用的英语。

- **android.app.extra.PROVISIONING_TIME_ZONE:** 设备运行所在的时区。

  输入 Olson 区域/位置形式的名称。例如，America/Los_Angeles 表示太平洋时间。如果不输入，时区将自动填充。

- **android.app.extra.PROVISIONING_LOCAL_TIME:** 自纪元以来的毫秒数。

  Unix 纪元（或 Unix 时间、POSIX 时间或 Unix 时间戳）是自 January 1, 1970（UTC/GMT 午夜）以来经过的秒数。该时间不包括闰秒（在 ISO 8601 中：1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** 设置为 **true** 可在配置文件创建期间跳过加密。设置为 **false** 可在配置文件创建期间强制加密。

典型的 JSON 如下所示：

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "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
}
```

使用任何 JSON 验证工具（例如 https://jsonlint.com）验证创建的 JSON。使用任何在线 QR 码生成器（例如 https://goqr.me）将该 JSON 字符串转换为 QR 码。

此 QR 码由恢复出厂设置的设备扫描，以将设备注册到工作管理设备模式。

注册设备

要将设备注册为完全托管设备，设备必须处于恢复出厂设置状态。

1. 在欢迎屏幕上点击屏幕六次以启动 QR 码注册流程。
2. 出现提示时，连接到 Wi-Fi。QR 码中（编码在 JSON 中）Secure Hub 的下载位置可通过此 Wi-Fi 网络访问。

   设备成功连接到 Wi-Fi 后，它会从 Google 下载 QR 码阅读器并启动相机。
3. 将相机对准 QR 码以扫描代码。

   Android 从 QR 码中的下载位置下载 Secure Hub，验证签名证书签名，安装 Secure Hub 并将其设置为设备所有者。

有关详细信息，请参阅此适用于 Android EMM 开发人员的 Google 指南：`<https://developers.google.com/android/work/prov-devices#qr_code_method>`。

NFC 碰触

要使用 NFC 碰触将设备注册为完全托管设备，需要两台设备：一台已恢复出厂设置，另一台运行 XenMobile Provisioning Tool。

先决条件：

- 支持所有运行 Android 5.0、Android 5.1、Android 6.0 及更高版本的 Android 设备。
- 已启用 Android Enterprise 的 XenMobile Server 10.4 版。
- 已配置为 Android Enterprise 全面管理设备的新设备或恢复出厂设置的设备。您可以在本文后面找到完成此先决条件的步骤。
- 另一台具有 NFC 功能的设备，运行已配置的预配工具。预配工具可在 Secure Hub 10.4 中或在 Citrix 下载页面 上获取。

每台设备只能有一个 Android Enterprise 配置文件，由企业移动性管理 (EMM) 应用程序管理。在 XenMobile 中，Secure Hub 是 EMM 应用程序。每台设备只允许一个配置文件。尝试添加第二个 EMM 应用程序会删除第一个 EMM 应用程序。

通过 NFC 碰撞传输的数据

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：

- 作为设备所有者的 EMM 提供程序应用程序的包名称（在本例中为 Secure Hub）。
- 设备可以从中下载 EMM 提供程序应用程序的内网/互联网位置。

- EMM 提供程序应用程序的 SHA1 哈希值，用于验证下载是否成功。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备可以连接并下载 EMM 提供程序应用程序。注意：Android 现在不支持此步骤的 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

当两台设备碰撞时，预配工具中的数据将发送到恢复出厂设置的设备。然后，该数据用于下载带有管理员设置的 Secure Hub。如果您不输入时区和位置值，Android 会自动在新设备上配置这些值。

配置 XENMOBILE 预配工具

在进行 NFC 碰触之前，您必须配置预配工具。此配置随后会在 NFC 碰触期间传输到恢复出厂设置的设备。

预配工具配置的图像(/en-us/xenmobile/server/media/nfc-provisioning-secure-hub.png)

您可以将数据键入到必填字段中，或者通过文本文件填充这些字段。下一个过程中的步骤介绍了如何配置文本文件，并包含每个字段的说明。键入信息后，应用程序不会保存信息，因此您可能需要创建一个文本文件以保留信息供将来使用。
使用文本文件配置预配工具
将文件命名为 nfcprovisioning.txt，并将其放置在设备 SD 卡上的 /sdcard/ 文件夹中。然后，应用程序可以读取文本文件并填充值。

文本文件必须包含以下数据：

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

此行是 EMM 提供程序应用程序的内网/互联网位置。在 NFC 碰触后，恢复出厂设置的设备连接到 Wi-Fi 后，设备必须能够访问此位置才能进行下载。URL 是一个常规 URL，无需特殊格式。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<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。获取校验和的步骤将在本文后面讨论。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

此行是运行预配工具的设备的已连接 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，则此字段必须为空。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

如果 Wi-Fi 未受保护，此字段必须为空。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

输入语言和国家/地区代码。语言代码是 ISO 639-1 定义的两位小写 ISO 语言代码（例如 en）。国家/地区代码是 ISO 3166-1 定义的两位大写 ISO 国家/地区代码（例如 US）。例如，键入 en_US 表示在美国使用的英语。如果您不键入任何代码，国家/地区和语言将自动填充。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

设备运行所在的时区。键入 Olson 格式的区域/位置名称。例如，America/Los_Angeles 表示太平洋时间。如果您不输入名称，时区将自动填充。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

此数据不是必需的，因为该值已作为 Secure Hub 硬编码到应用程序中。此处提及仅为完整性考虑。

如果 Wi-Fi 受 WPA2 保护，则已完成的 nfcprovisioning.txt 文件可能如下所示：

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name`

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2`

`android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

如果存在未受保护的 Wi-Fi，则已完成的 nfcprovisioning.txt 文件可能如下所示：

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name`

`android.app.extra.PROVISIONING_LOCALE=en_US`

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

获取 SECURE HUB 校验和

要获取任何应用程序的校验和，请将该应用程序添加为企业应用程序。

1. 在 XenMobile 控制台中，转至 **Configure > Apps**，然后单击 **Add**。

   此时将显示 **Add Apps** 窗口。

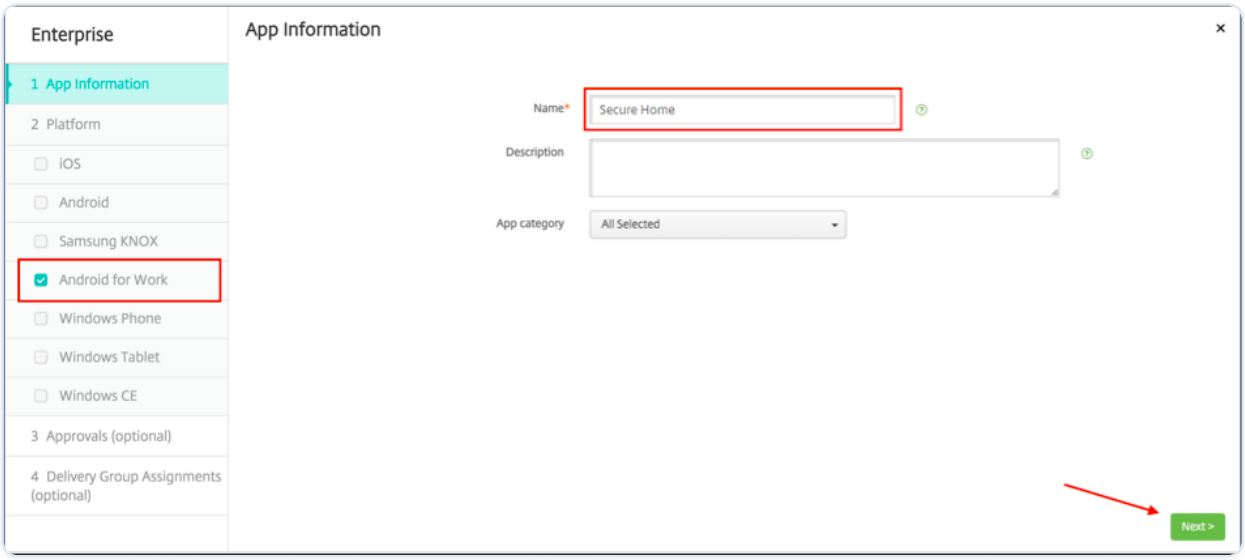
2. 单击 **Enterprise**。

   此时将显示 **App information** 页面。

   应用程序信息页面图像(/en-us/xenmobile/server/media/nfc-provisioning-add-app-enterprise.png)

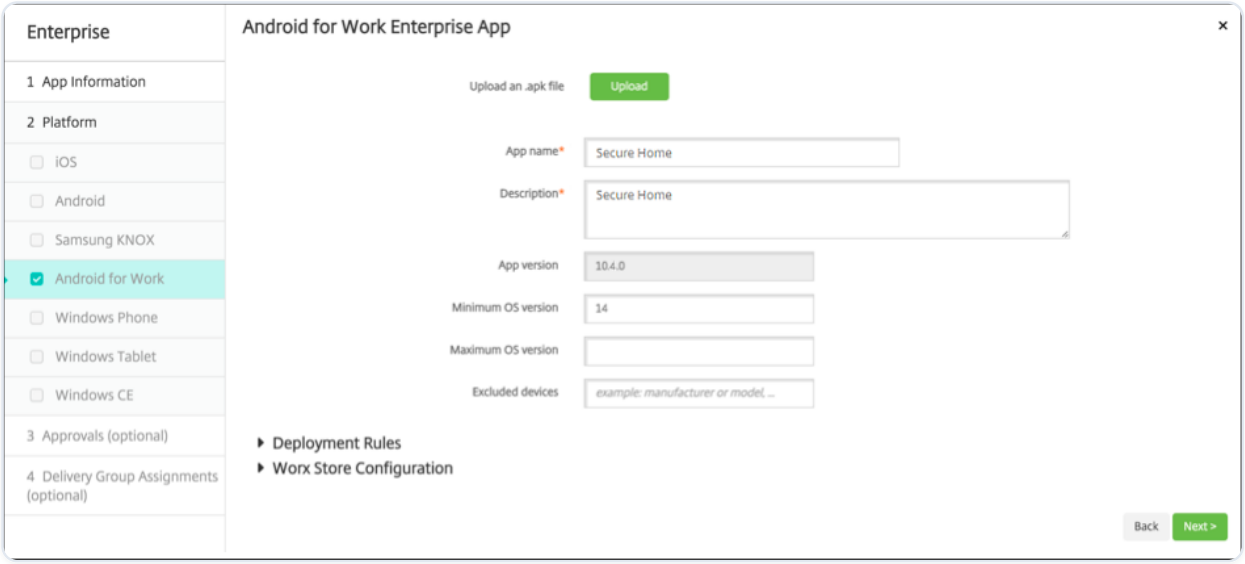
3. 选择以下配置，然后单击 **Next**。

   此时将显示 **Android Enterprise Enterprise App** 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，将显示上载包的详细信息。



5. 单击“**下一步**”以打开下载 JSON 文件的页面，然后您可以使用该文件上载到 Google Play。对于 Secure Hub，不需要上载到 Google Play，但您需要 JSON 文件才能从中读取 SHA1 值。

   典型的 JSON 文件如下所示：

6. 复制 **file_sha1_base64 值**，并在预配工具的“**哈希**”字段中使用它。

   > **注意：**
   >
   > 哈希必须是 URL 安全的。

   - 将所有 **+** 符号转换为 **-**
   - 将所有 **/** 符号转换为 _
   - 将尾随的 **\\u003d** 替换为 **=**

   如果将哈希存储在设备 SD 卡上的 nfcprovisioning.txt 文件中，应用程序会执行安全转换。但是，如果选择手动键入哈希，您有责任确保其 URL 安全性。

使用的库

配置工具在其源代码中使用了以下库：

- Google 在 Apache 2.0 许可下提供的 v7 appcompat 库、设计支持库和 v7 Palette 库

  有关信息，请参阅 支持库功能指南。

- Jake Wharton 在 Apache 2.0 许可下提供的 Butter Knife

在 Android Enterprise 中配置工作配置文件设备

在 Android Enterprise 的工作配置文件设备上，您可以安全地将设备上的公司区域和个人区域分开。例如，BYOD 设备可以是工作配置文件设备。工作配置文件设备的注册体验与 XenMobile 中的 Android 注册类似。用户从 Google Play 下载 Secure Hub 并注册其设备。

默认情况下，当设备作为工作配置文件设备注册到 Android Enterprise 时，其 USB 调试和未知来源设置处于禁用状态。

> **提示：**
>
> 将设备作为工作配置文件设备注册到 Android Enterprise 时，请始终前往 Google Play。在那里，启用 Secure Hub 以显示在用户的个人资料中。

支持托管配置反馈（技术预览版）

> **注意：**
>
> 技术预览版中的功能可在非生产或有限生产环境中使用，并为客户提供分享反馈的机会。Citrix® 不接受技术预览版功能的任何支持案例，但欢迎提供反馈以改进这些功能。您可以通过点击 **向我们发送您的反馈** 来提供对此功能的反馈。Citrix 可能会根据反馈的严重性、关键性和重要性采取行动。

> 托管配置反馈功能允许管理员从配置了托管配置策略的 Android 设备获取有关应用程序状态的反馈。此反馈可用于监控这些策略的有效性和状态。

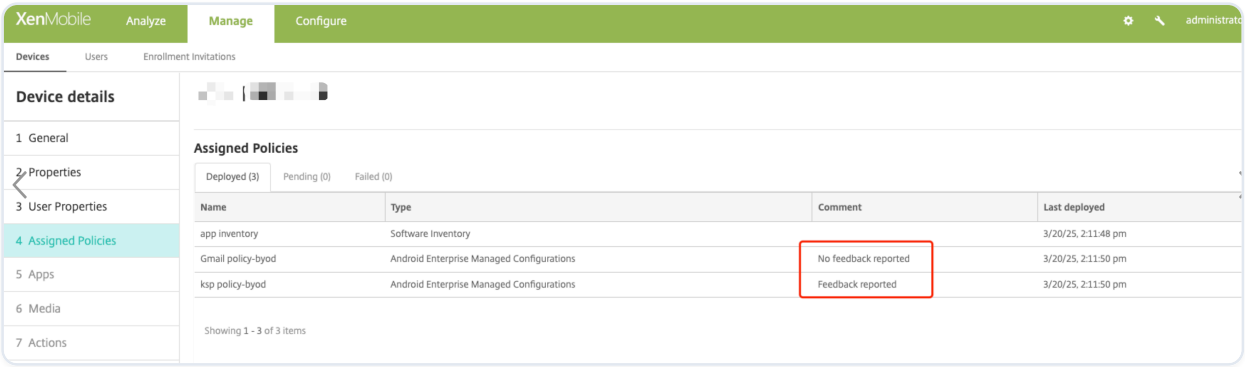
先决条件

1. `App Support`：应用程序必须支持托管配置策略。
2. `Keyed App States`：应用程序还必须支持带键的应用程序状态。有关应用程序反馈如何运作的详细信息，请参阅 将应用程序反馈发送到 EMM。

管理和利用配置反馈的步骤

1. 为指定的 XenMobile Server 启用服务器属性 `afw.app_managed_configurations.feedback`。
2. 验证托管配置策略。

- 确认 Android 设备已注册且托管配置策略已成功应用。
- 导航到 **设备详细信息** 并点击 **已分配策略**。将显示与托管配置策略相关的注释。
  - **已报告反馈**：表示此策略相关应用程序有可用反馈。
  - **未报告反馈**：表示此策略相关应用程序未报告任何反馈。



- 导航到“**设备详细信息**”并点击“**应用程序**”。详细反馈显示在“**托管配置反馈**”表下，其中包含所有应用程序数据。

  管理配置反馈(/en-us/xenmobile/server/media/manage-config-feedback.png)

- 对于单个托管配置策略，您可以查看所有已分配设备的反馈详细信息：
  - “**信息**”：所有报告的反馈数据不包含错误的设备。
  - “**错误**”：所有报告的反馈数据包含错误的设备。
  - “**空**”：所有未报告反馈数据的设备。

  反馈详细信息(/en-us/xenmobile/server/media/feedback-details.png)

- 要手动获取反馈，请点击“**管理**”并选择复选框以查找相应的设备。例如，您可以选择相应的复选框并点击“**应用程序反馈**”。

  应用程序反馈(/en-us/xenmobile/server/media/app-feedback.png)

- 点击“**获取反馈**”以从选定的设备获取托管配置反馈。

  获取反馈(/en-us/xenmobile/server/media/get-feedback.png)

- 在托管配置反馈报告中，选择“**分析**”并点击“**报告**”以获取总体反馈。您可以查看所有设备的报告、管理配置策略以及相关的配置失败。

  管理配置反馈报告(/en-us/xenmobile/server/media/manage-config-feedback-report.png)

3. 已引入两个服务器属性以调整反馈计划。使用服务器属性修改控制台中的值，并控制反馈数据何时保存到数据库。

a. 更新 Android Enterprise 托管配置反馈数据库的批处理大小：

- 键: `android.managed.configuration.feedback.db.update.batch.size`
- 您可以定义存储到数据库的报告批处理大小，只有存储在数据库中的数据才能在用户界面中显示。默认值为 100，最大值为 1000。

b. Android Enterprise 托管配置反馈数据库更新时间间隔:

- 键: `android.managed.configuration.feedback.db.update.time.interval`
- 您可以指定报告在数据库中存储的时长，即使大小未达到批处理限制。默认值为六小时。

故障排除

默认情况下，反馈报告会在每次设备签入时检索（当 Secure Hub 连接到服务器时）。但是，您可以使用“应用程序反馈”按钮手动获取特定设备的报告。

iOS

要在 XenMobile Server 中管理 iOS 设备，您需要从 Apple 设置 Apple Push Notification service (APNs) 证书。有关信息，请参阅APNs 证书。

注册配置文件决定 iOS 设备是否注册 MDM+MAM，用户可以选择退出 MDM。XenMobile Server 支持 MDM+MAM 中 iOS 设备的以下身份验证类型。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 中受信任证书的要求：**

> Apple 对 TLS 服务器证书有新的要求。请验证所有证书是否符合 Apple 的新要求。请参阅 Apple 的出版物 `<https://support.apple.com/zh-cn/HT210176>`。有关管理证书的帮助，请参阅在 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。

对于受监管的 iOS 设备，您可以将软件升级延迟最多 90 天。在 iOS 的“限制”设备策略中，使用以下设置：

- **强制延迟软件更新**
- **强制软件更新延迟**

请参阅 iOS 设置。这些设置不适用于用户注册模式或非监督（完全 MDM）模式下的设备。

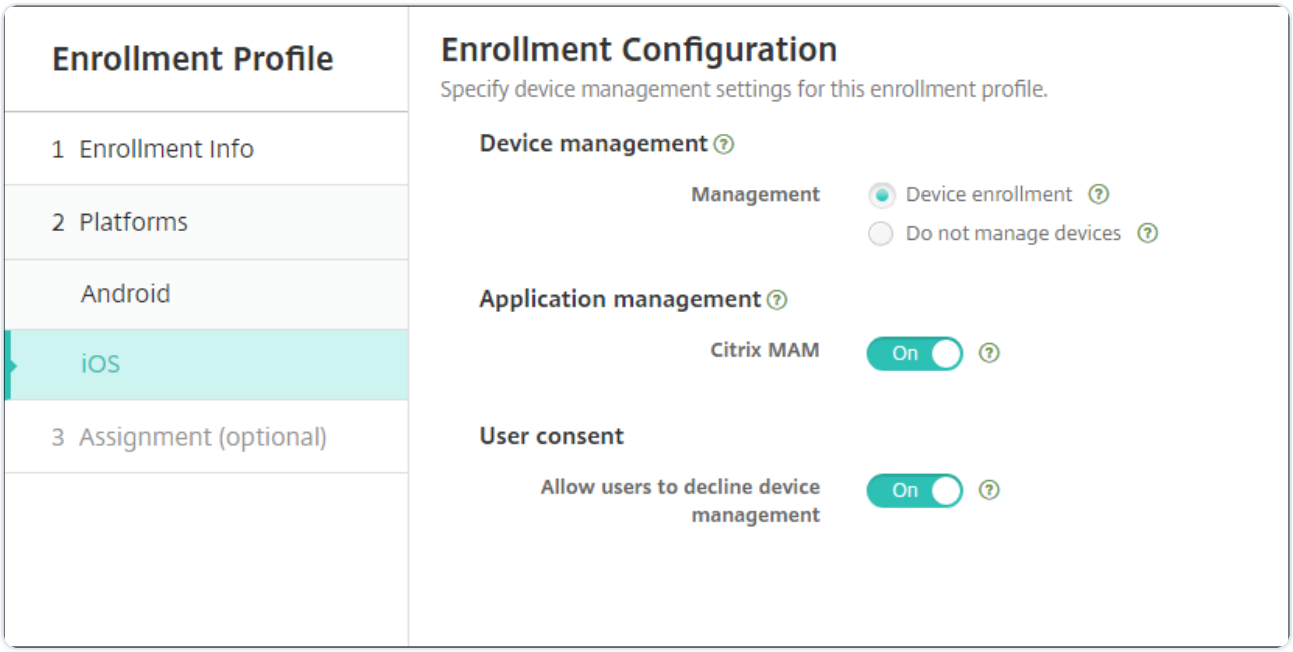
必须保持开放的 Apple 主机名

某些 Apple 主机名必须保持开放，以确保 iOS、macOS 和 Apple App Store 的正常运行。阻止这些主机名可能会影响以下各项的安装、更新和正常运行：iOS、iOS 应用程序、MDM 操作以及设备和应用程序注册。有关详细信息，请参阅 `<https://support.apple.com/zh-cn/HT201999>`。

支持的注册方法

您可以在注册配置文件中指定如何管理 iOS 设备。您可以选择设备注册或不进行 MDM 注册。

要配置 iOS 设备的注册设置，请转至 **Configure > Enrollment Profiles > iOS**。



下表列出了 XenMobile Server 支持的 iOS 设备注册方法：

方法	支持
Apple 部署计划	是

方法	支持
Apple 校园教务管理	是
Apple 配置器	是
手动注册	是
注册邀请	是

Apple 为企业和教育帐户提供了设备注册计划。对于企业帐户，您可以注册 Apple 部署计划，以便在 XenMobile Server 中使用 Apple 部署计划进行设备注册和管理。该计划适用于 iOS 和 macOS 设备。请参阅 通过 Apple 部署计划部署设备。

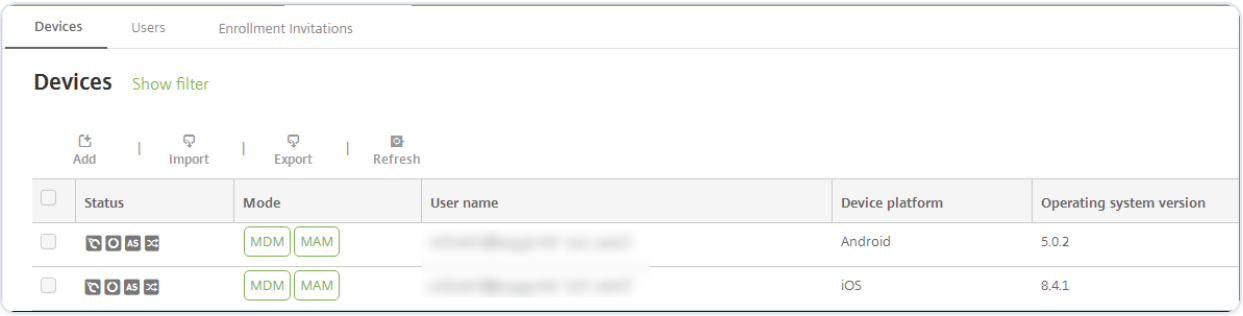
对于教育帐户，您可以创建 Apple 校园教务管理帐户。Apple 校园教务管理整合了部署计划和大宗采购。Apple 校园教务管理是一种教育 Apple 部署计划。请参阅 与 Apple 教育功能集成。

您可以使用 Apple 部署计划批量注册 iOS 和 macOS 设备。您可以直接从 Apple、参与的 Apple 授权经销商或运营商处购买这些设备。无论您是否直接从 Apple 购买 iOS 设备，都可以使用 Apple Configurator 注册这些设备。请参阅 批量注册 Apple 设备。

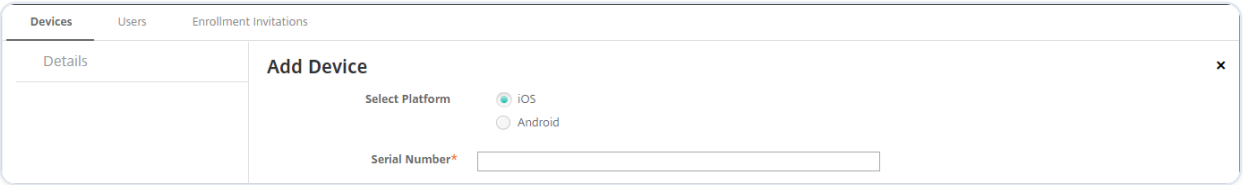
手动添加 iOS 设备

如果要手动添加 iOS 设备（例如用于测试目的），请按照以下步骤操作。

1. 在 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：

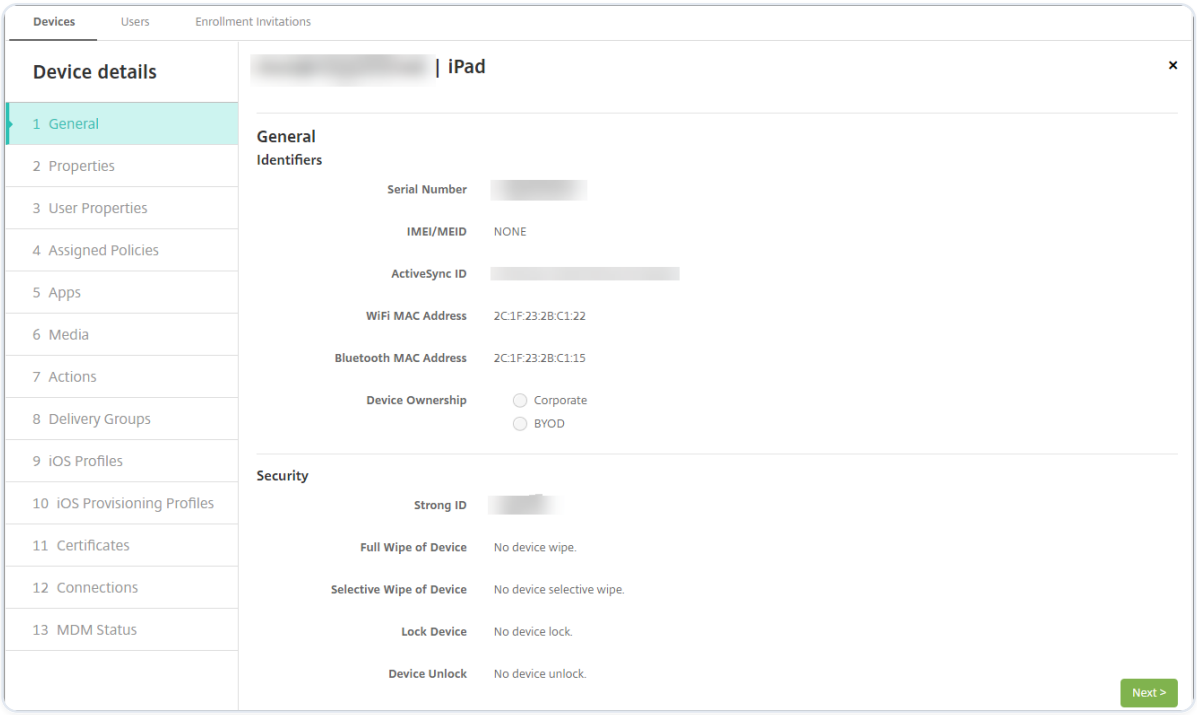
   - **选择平台：** 点击 **iOS**。

- **序列号：** 输入设备序列号。

4. 点击 **添加**。**设备** 表格出现，设备已添加到列表底部。要查看并确认设备详细信息：选择您添加的设备，然后在出现的菜单中，点击 **编辑**。

> **注意：**
>
> 当您选择设备旁边的复选框时，选项菜单会出现在设备列表上方。当您点击列表中的其他任何位置时，选项菜单会出现在列表的右侧。

- LDAP 已配置
- 如果使用本地组和本地用户：
  - 一个或多个本地组。
  - 分配给本地组的本地用户。
  - 交付组与本地组关联。
- 如果使用 Active Directory：
  - 交付组与 Active Directory 组关联。



5. **常规** 页面列出了设备**标识符**，例如序列号和平台类型的其他信息。对于**设备所有权**，选择**公司**或**BYOD**。

常规 页面还列出了设备**安全**属性，例如强 ID、锁定设备、激活锁绕过以及平台类型的其他信息。**完全擦除设备** 字段包含用户 PIN 码。设备擦除后，用户必须输入该代码。如果用户忘记了代码，您可以在此处查找。

6. “**属性**”页面列出了 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个属性。有关每个属性的有效值，请参阅 PDF 设备属性名称和值。

   添加属性时，它最初会显示在您添加它的类别下。单击“**下一步**”并返回“**属性**”页面后，该属性将显示在相应的列表中。

   要删除属性，请将鼠标悬停在列表项上，然后单击右侧的“**X**”。XenMobile Server 会立即删除该项目。

7. 其余的“**设备详细信息**”部分包含设备的摘要信息。

   - **用户属性：** 显示用户的 RBAC 角色、组成员身份、批量购买帐户和属性。您可以从此页面停用批量购买帐户。
   - **已分配策略：** 显示已分配策略的数量，包括已部署、待处理和失败策略的数量。提供每个策略的策略名称、类型和上次部署信息。
   - **应用程序：** 显示上次盘点中已安装、待处理和失败的应用程序部署数量。提供应用程序名称、标识符、类型和其他信息。有关 iOS 和 macOS 盘点密钥（例如 **HasUpdateAvailable**）的说明，请参阅 移动设备管理 (MDM) 协议。
   - **媒体：** 显示上次盘点中已部署、待处理和失败的媒体部署数量。
   - **操作：** 显示已部署、待处理和失败操作的数量。提供操作名称和上次部署时间。
   - **交付组：** 显示成功、待处理和失败的交付组数量。对于每个部署，提供交付组名称和部署时间。选择一个交付组以查看更详细的信息，包括状态、操作以及渠道或用户。
   - **iOS 配置文件：** 显示上次 iOS 配置文件盘点，包括名称、类型、组织和描述。
   - **iOS 预配配置文件：** 显示企业分发预配配置文件信息，例如 UUID、过期日期和托管状态。
   - **证书：** 显示有效、已过期或已吊销证书的信息，例如类型、提供商、颁发者、序列号以及过期前的剩余天数。
   - **连接：** 显示首次连接状态和上次连接状态。提供每个连接的用户名、倒数第二次身份验证时间和上次身份验证时间。
   - **MDM 状态：** 显示 MDM 状态、上次推送时间和上次设备回复时间等信息。

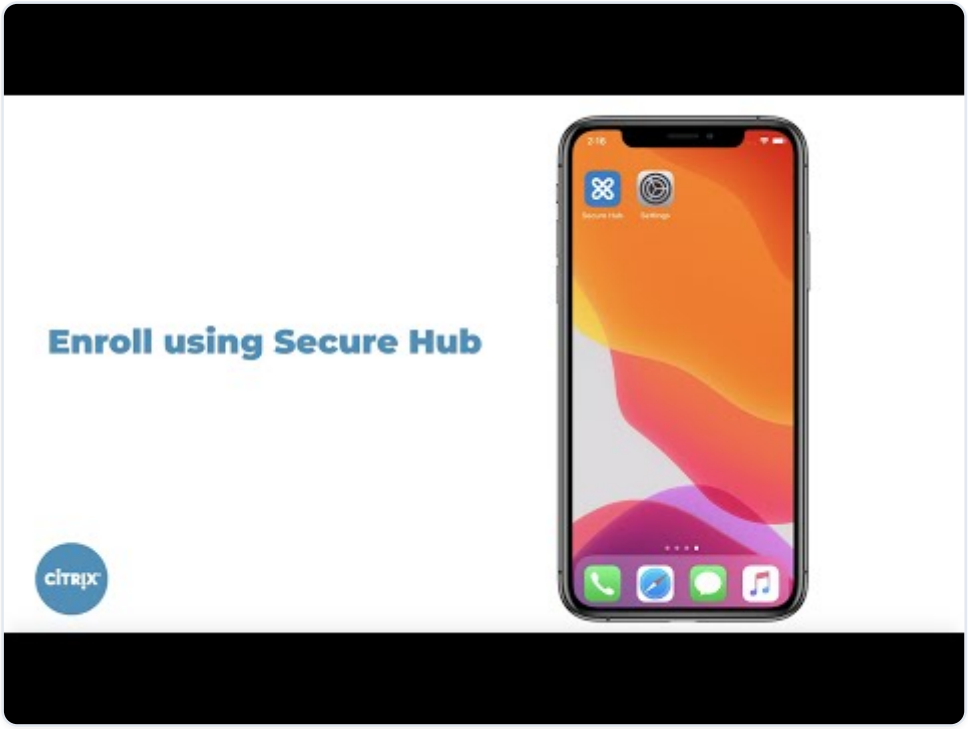
配置 iOS 设备策略

使用这些策略配置 XenMobile Server 如何与运行 iOS 的设备交互。此表列出了适用于 iOS 设备的所有设备策略。

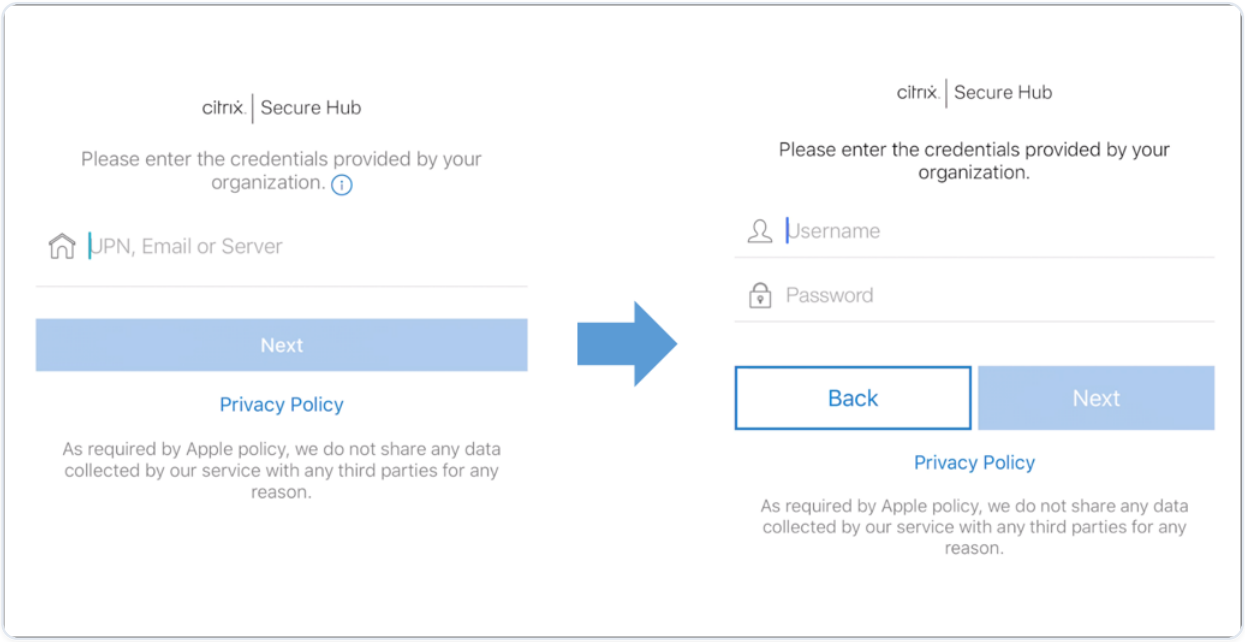
AirPlay 镜像	AirPrint	APN
应用访问	应用属性	应用配置
应用清单	应用锁定	应用网络使用情况
应用卸载	应用通知	日历 (CalDAV)
蜂窝网络	联系人 (CardDAV)	控制操作系统更新
凭据	设备名称	教育配置
交换	字体	主屏幕布局
导入 iOS 和 macOS 配置文件	LDAP	位置
邮件	托管域	MDM 选项
组织信息	密码	个人热点
配置文件删除	预配配置文件	预配配置文件删除
代理	限制	漫游
SCEP	共享 iPad - 最大驻留用户数	共享 iPad - 密码锁定宽限期
SSO 帐户	商店	订阅的日历
条款和条件	VPN	壁纸
Web 内容筛选器	网页剪辑	无线局域网

注册 iOS 设备

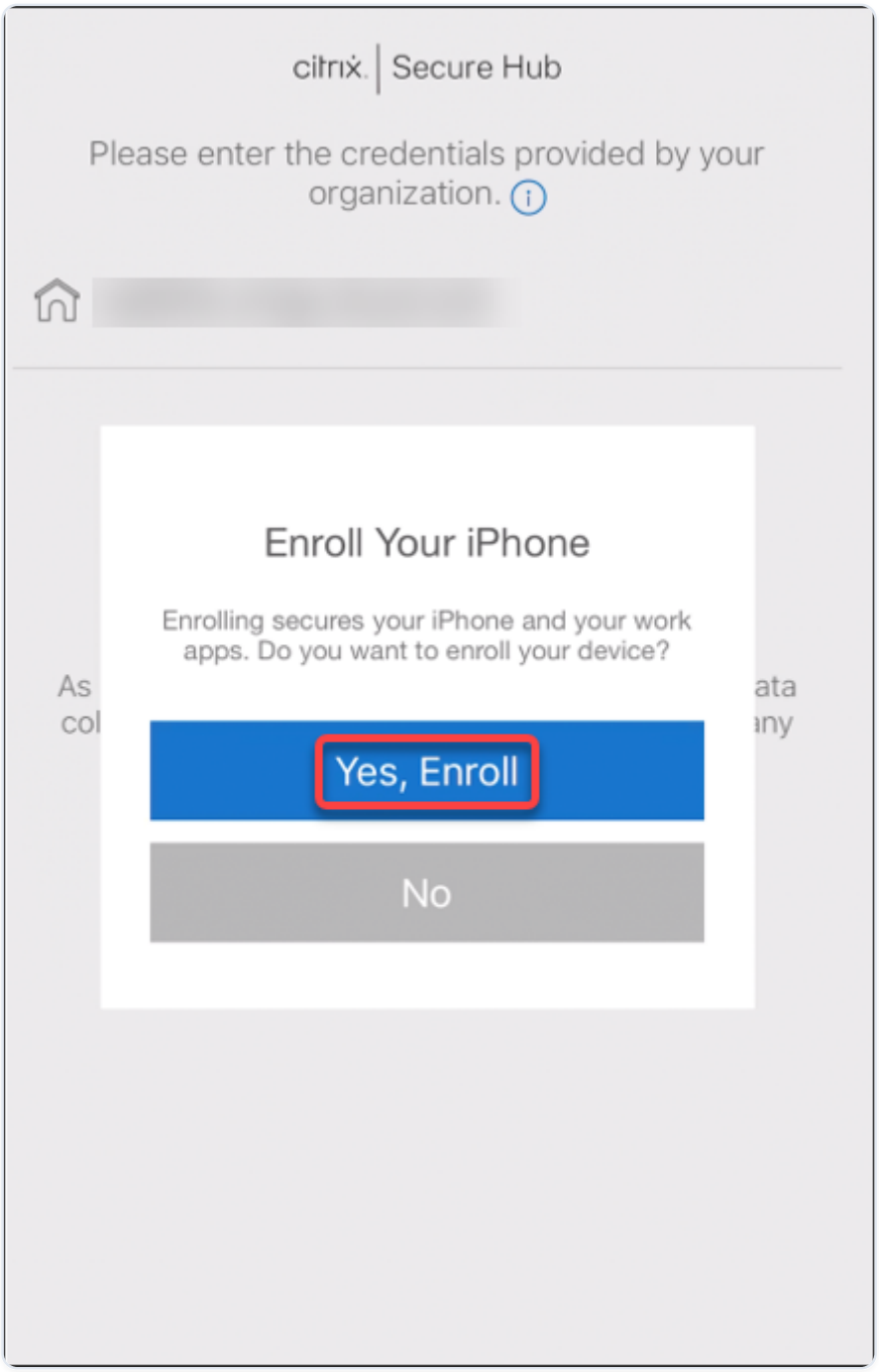
本节介绍用户如何将 iOS 设备（12.2 或更高版本）注册到 XenMobile Server。有关 iOS 注册的更多信息，请观看以下视频：



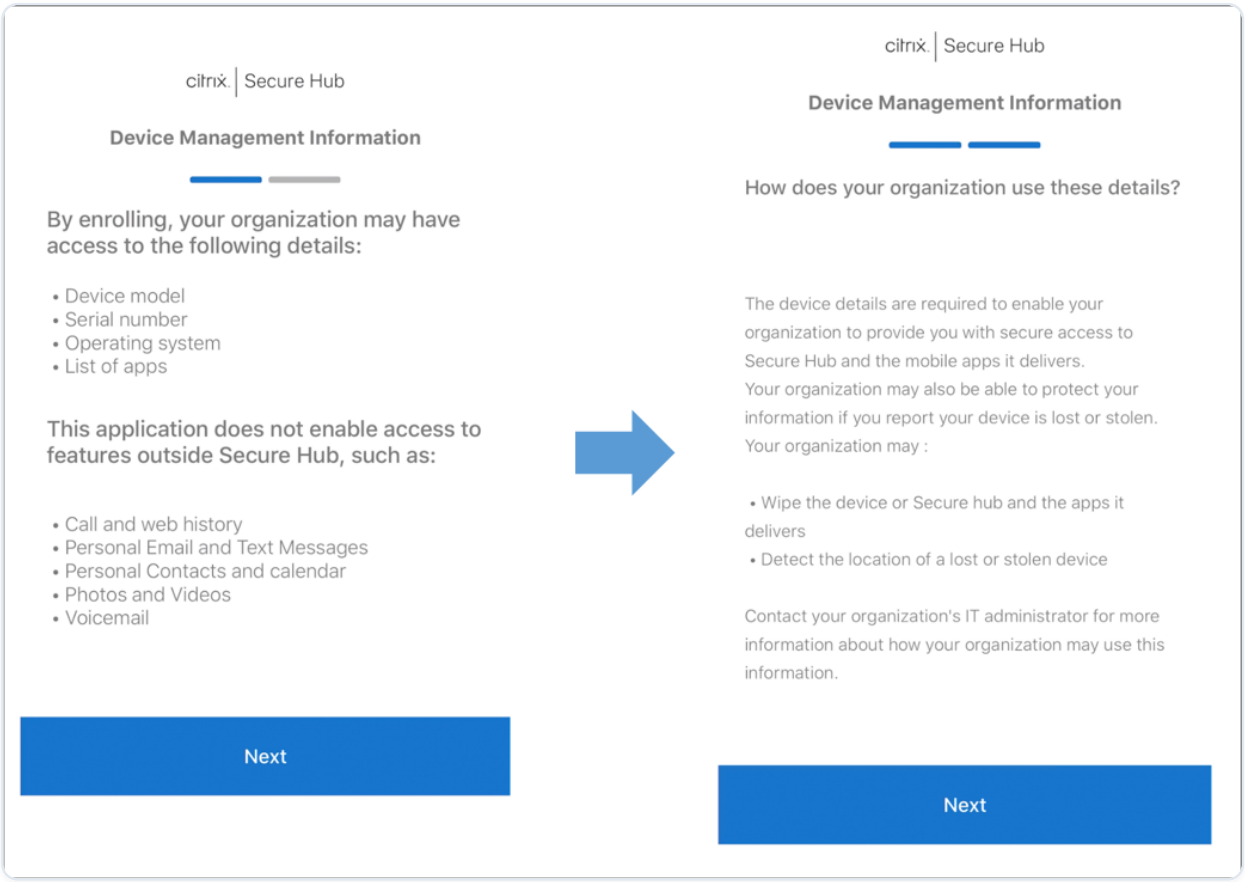
1. 在 iOS 设备上前往 Apple Store，下载 Citrix Secure Hub™ 应用，然后点击该应用。
2. 当提示安装应用时，点击“**下一步**”，然后点击“**安装**”。
3. Secure Hub 安装完成后，点击“**打开**”。
4. 输入您的公司凭据，例如 XenMobile Server 服务器名称、用户主体名称 (UPN) 或电子邮件地址。然后，点击“**下一步**”。



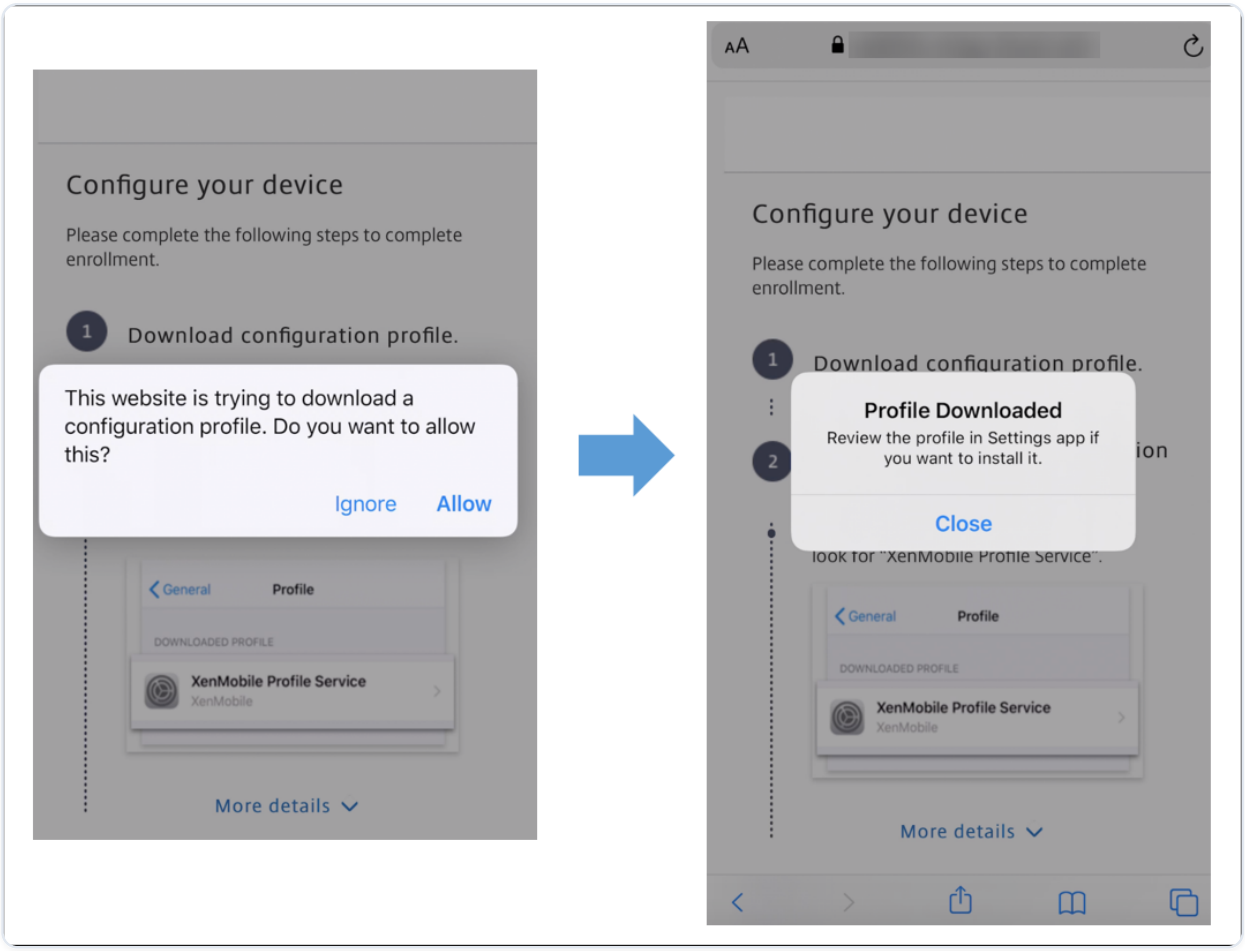
5. 点击“**是，注册**”以注册您的 iOS 设备。



6. 将显示 XenMobile Server 收集的数据列表。点击“**下一步**”。将显示组织如何使用这些数据的说明。点击“**下一步**”。



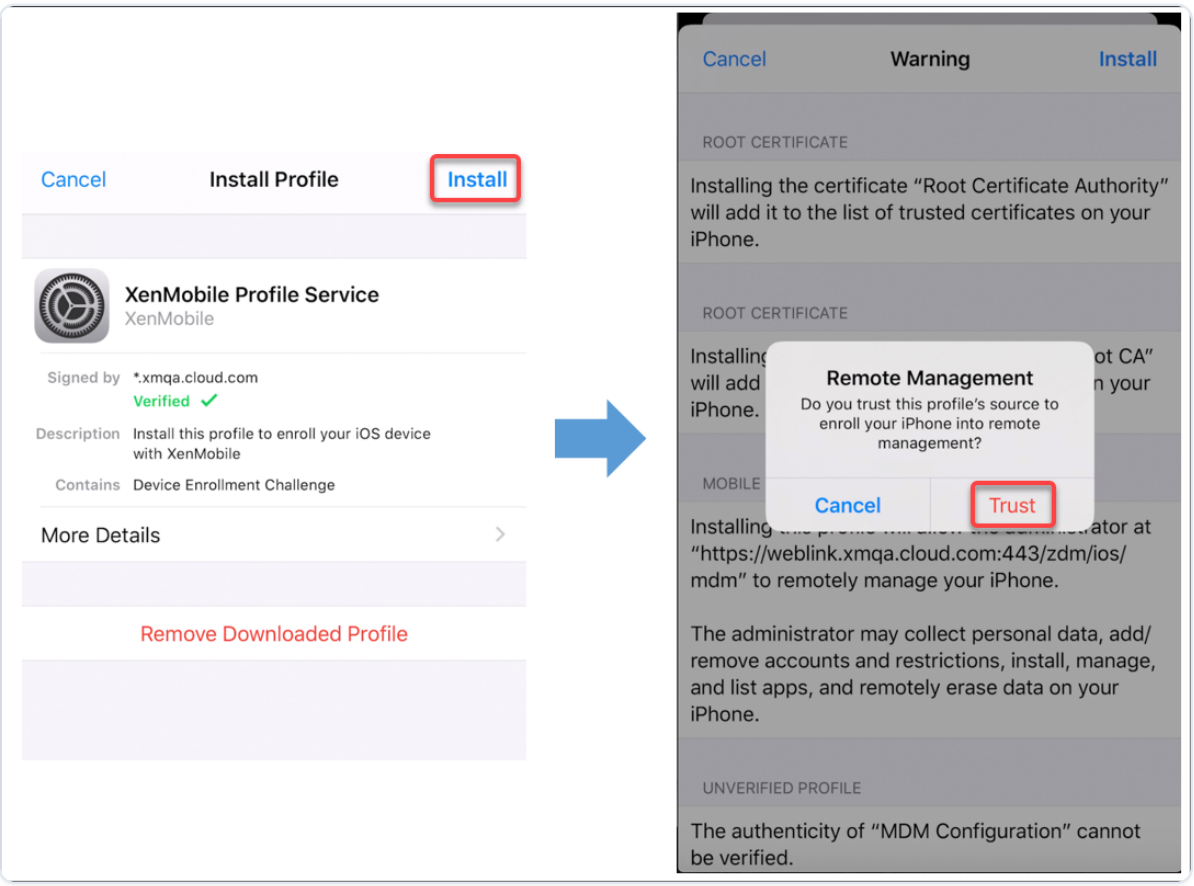
7. 输入凭据后，在出现提示时点击“**允许**”以下载配置配置文件。下载配置配置文件后，点击“**关闭**”。



8. 在您的设备设置中，安装 iOS 证书并将设备添加到受信任列表。

   - 转到 **设置 > 通用 > 描述文件 > XenMobile 描述文件服务**，然后点击 **安装** 以添加描述文件。

- 在通知窗口中，点击 **信任** 以将您的设备注册到远程管理。



9. 注册成功后，打开 Secure Hub。如果您正在注册 MDM+MAM：凭据验证后，在提示时创建并确认您的 Citrix PIN。
10. 工作流完成后，设备即已注册。然后您可以访问应用商店，查看可在 iOS 设备上安装的应用。

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。

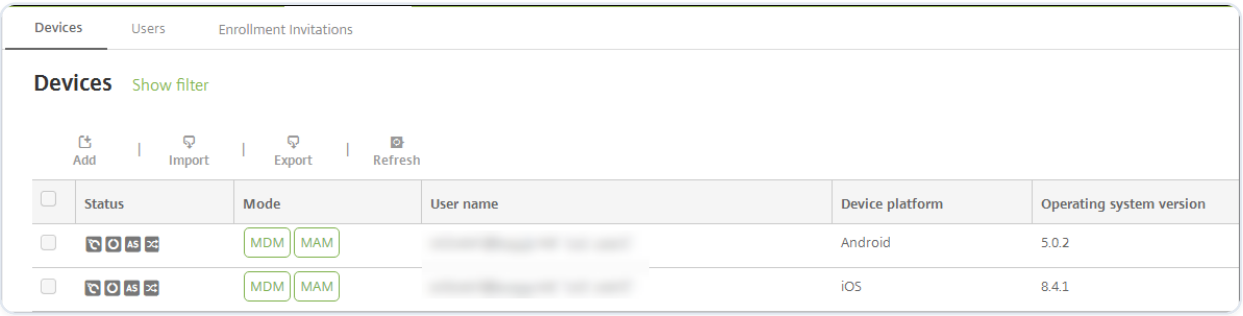
激活锁绕过	应用锁定	应用擦除
ASM 激活锁	证书续订	清除限制
启用/禁用丢失模式	启用/禁用跟踪	完全擦除
定位	锁定	响铃
请求/停止 AirPlay 镜像	重新启动/关机	吊销/授权
选择性擦除	解锁	

锁定 iOS 设备

您可以锁定丢失的 iOS 设备，并在设备锁定屏幕上显示一条消息和电话号码。

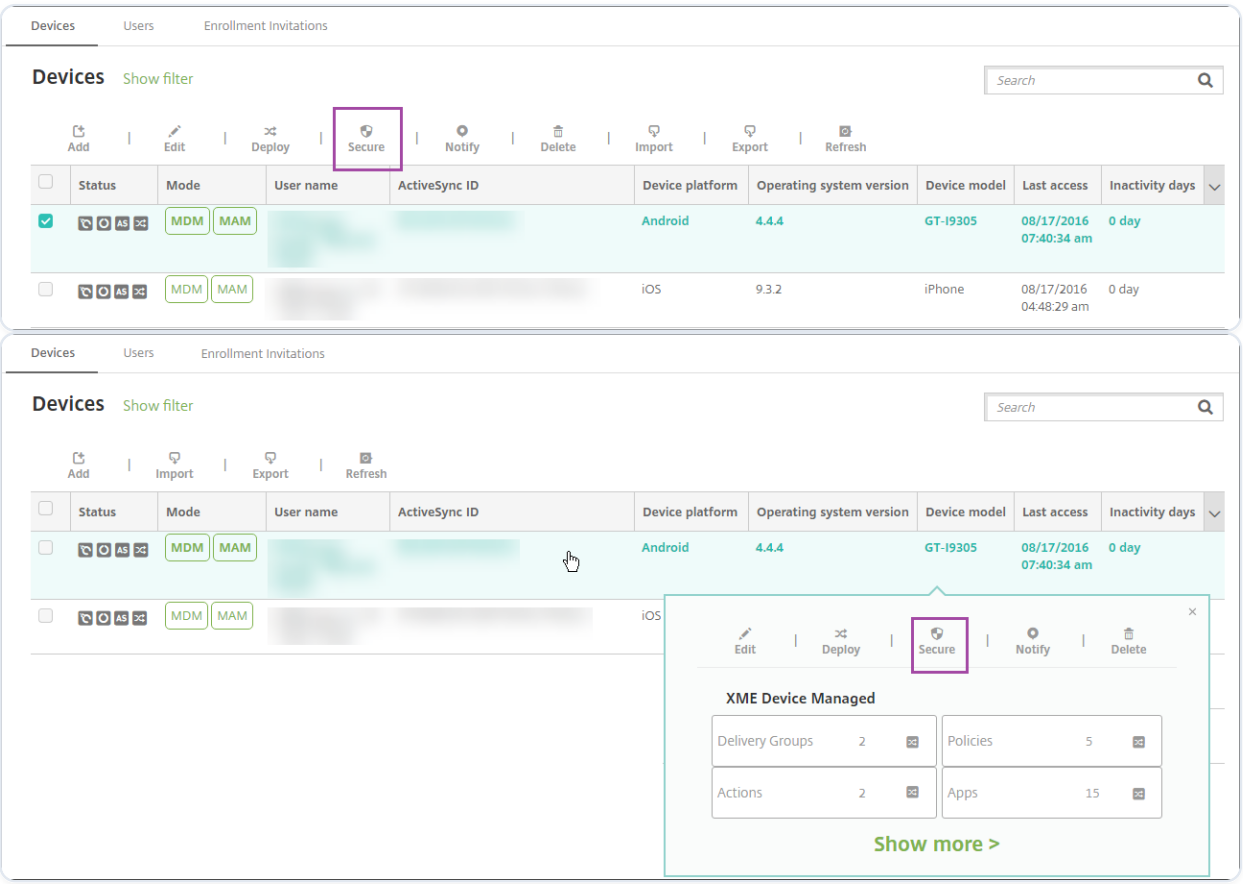
要在锁定的设备上显示消息和电话号码，请在 XenMobile Server 控制台中将 Passcode 策略设置为 **true**。或者，用户可以手动在设备上启用密码。

1. 单击 **管理 > 设备**。将显示“**设备**”页面。

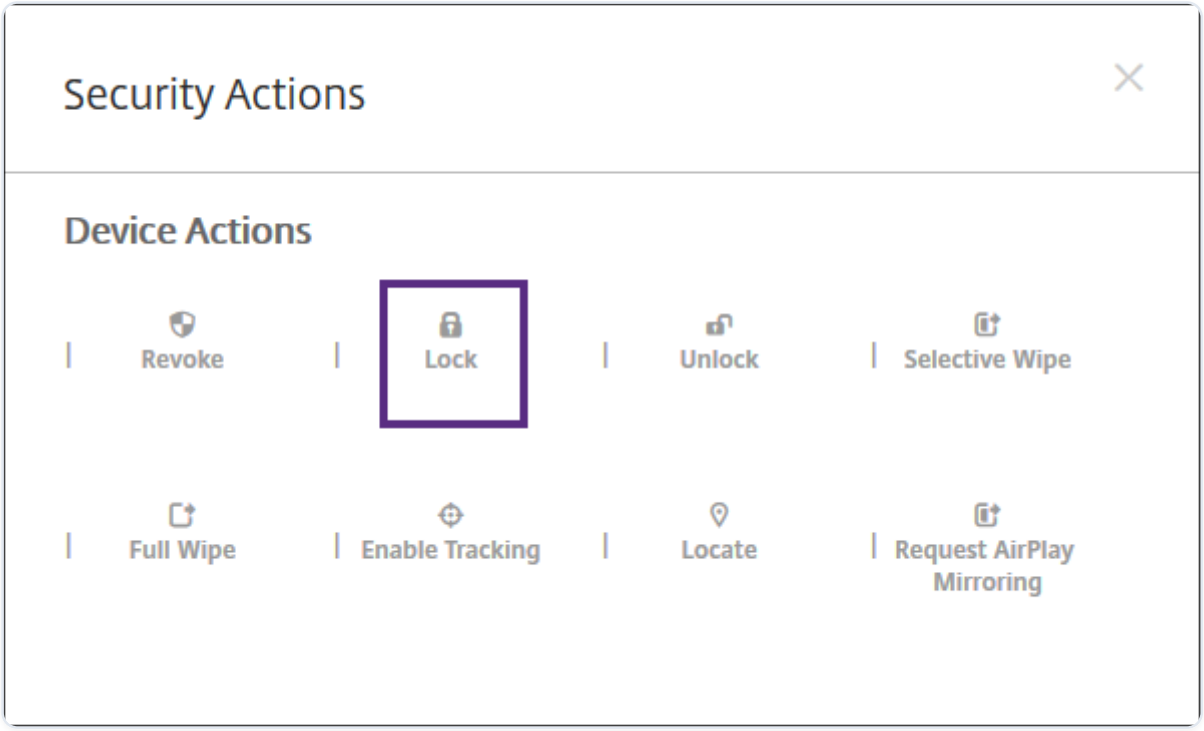


2. 选择要锁定的 iOS 设备。

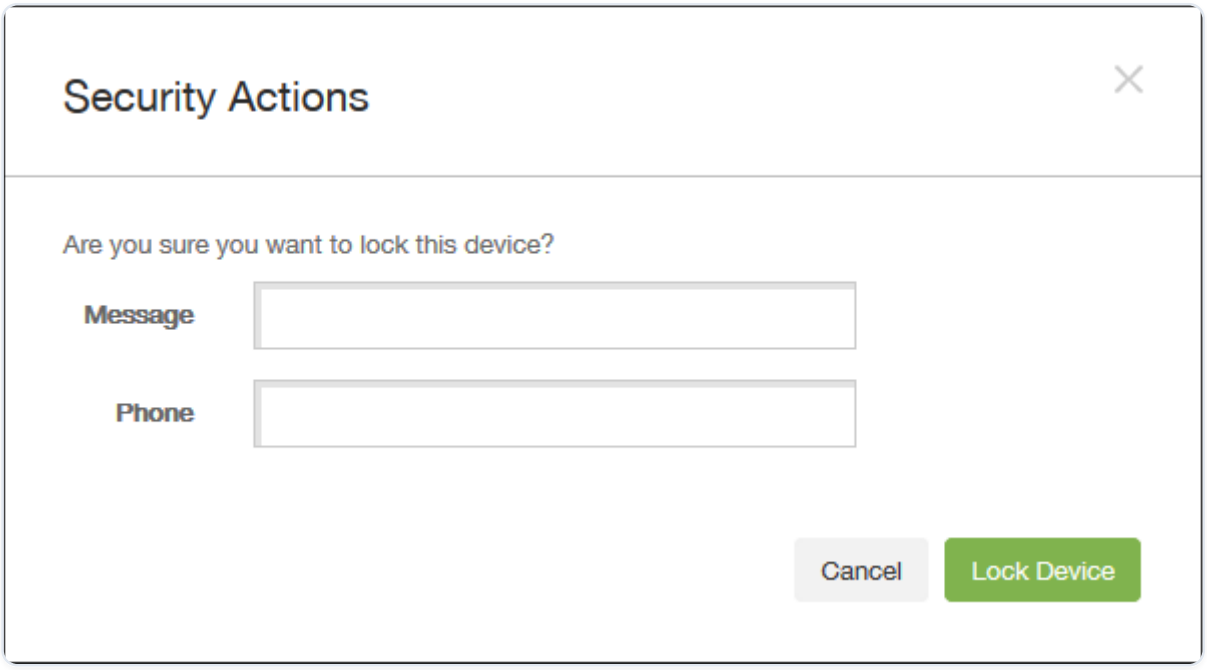
   选择设备旁边的复选框以显示设备列表上方的选项菜单。单击列表中的其他任意位置以在列表右侧显示选项菜单。



3. 在选项菜单中，单击“**安全**”。此时将显示“**安全操作**”对话框。



4. 单击“**锁定**”。此时将显示“**安全操作**”确认对话框。



5. （可选）键入将在设备锁定屏幕上显示的消息和电话号码。

   iOS 会将“Lost iPad”字样附加到您在“**消息**”字段中键入的内容之后。

   如果将“**消息**”字段留空并提供电话号码，Apple 会在设备锁定屏幕上显示消息“Call owner”。

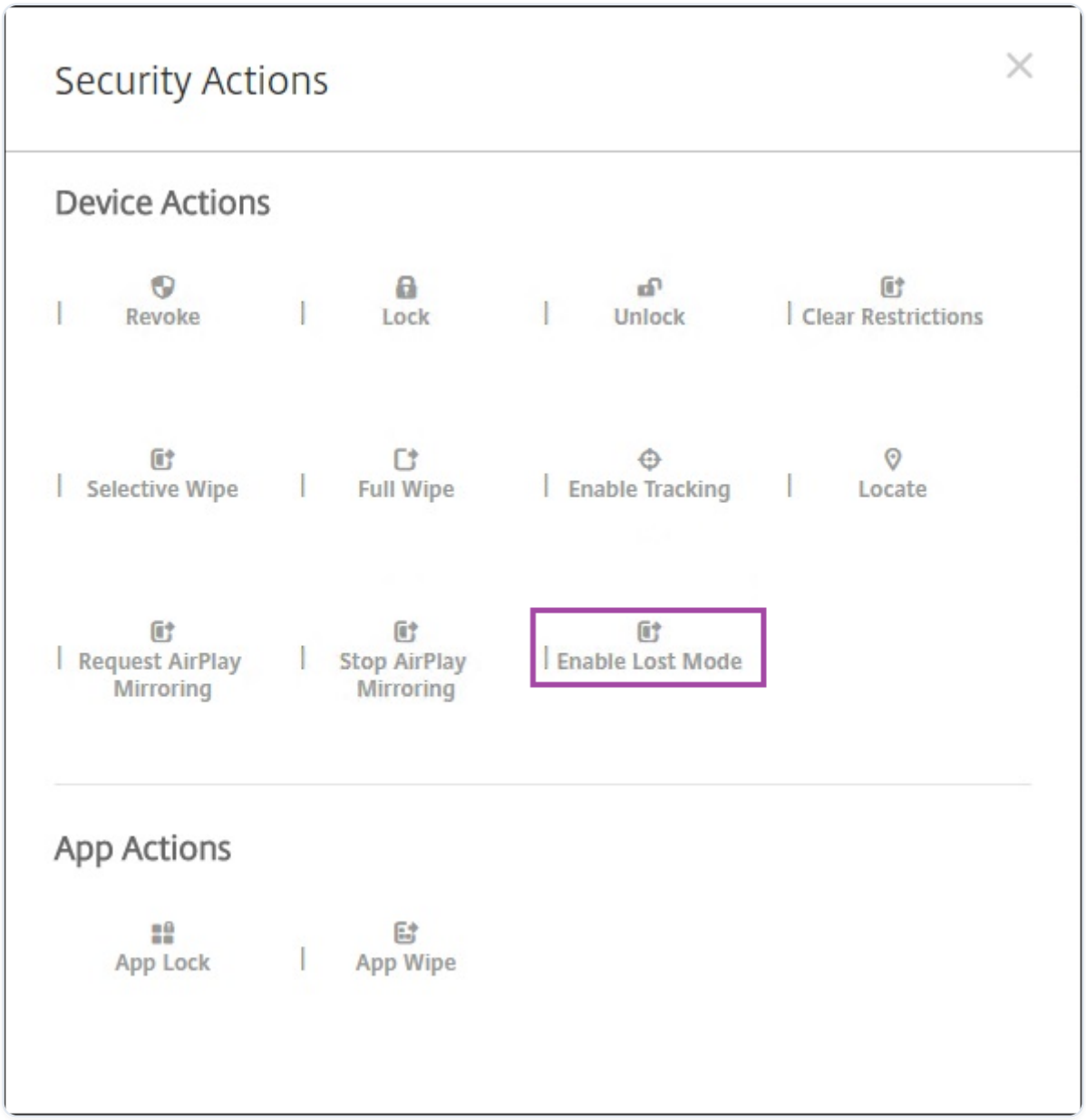
6. 单击“**锁定设备**”。

将 iOS 设备置于丢失模式

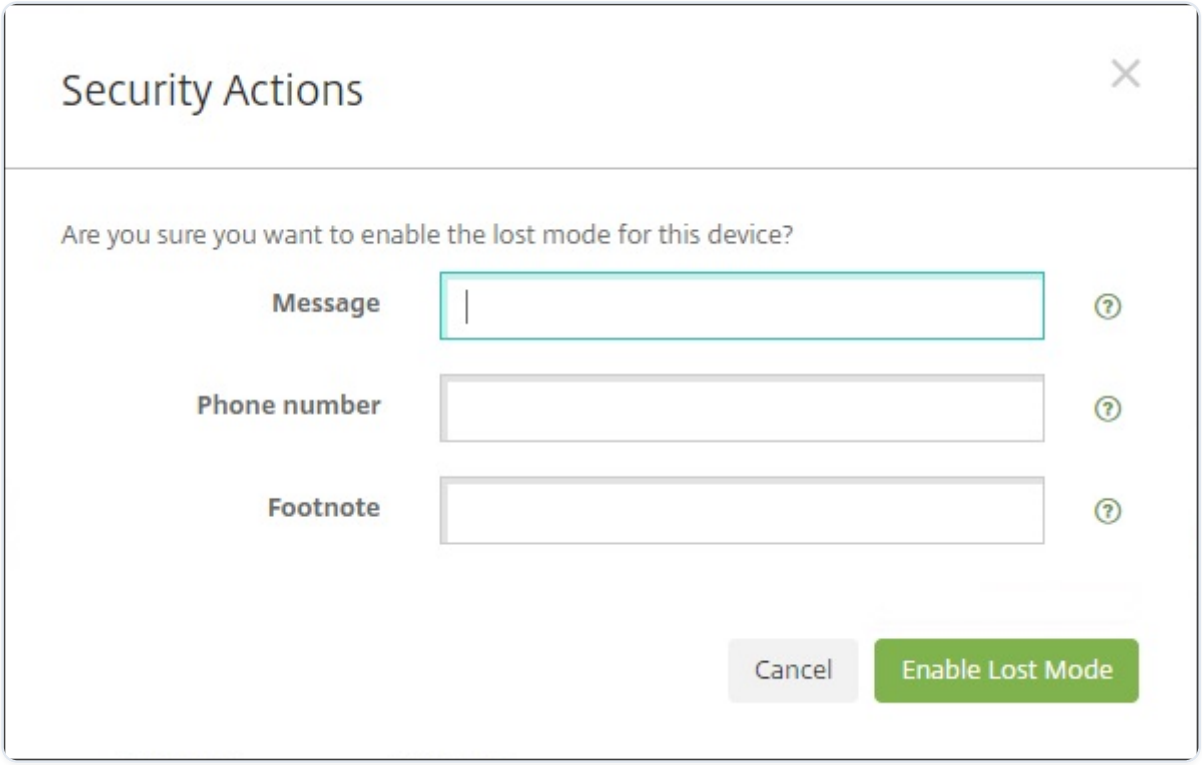
XenMobile Server 丢失模式设备属性会将 iOS 设备置于丢失模式。与 Apple 托管的丢失模式不同，XenMobile Server 丢失模式不要求用户执行以下任一操作来启用设备定位：配置“**查找我的 iPhone/iPad**”设置或为 Citrix Secure Hub 启用定位服务。

在 XenMobile Server 丢失模式下，只有 XenMobile Server 可以解锁设备。（相比之下，如果您使用 XenMobile Server 设备锁定功能，用户可以使用您提供的 PIN 码直接解锁设备。

要启用或禁用丢失模式：转至“**管理 > 设备**”，选择受监管的 iOS 设备，然后单击“**安全**”。然后，单击“**启用丢失模式**”或“**禁用丢失模式**”。

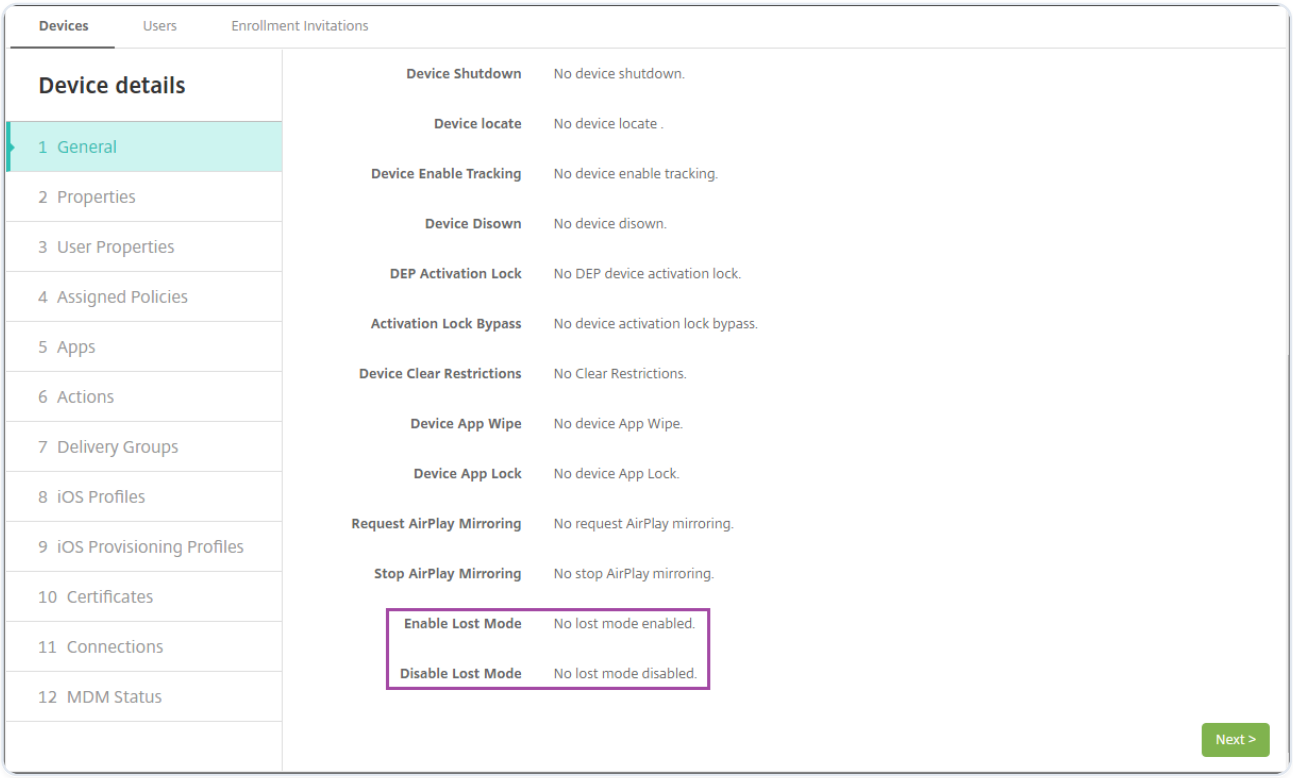


如果您单击“**启用丢失模式**”，请键入设备处于丢失模式时要显示的信息。

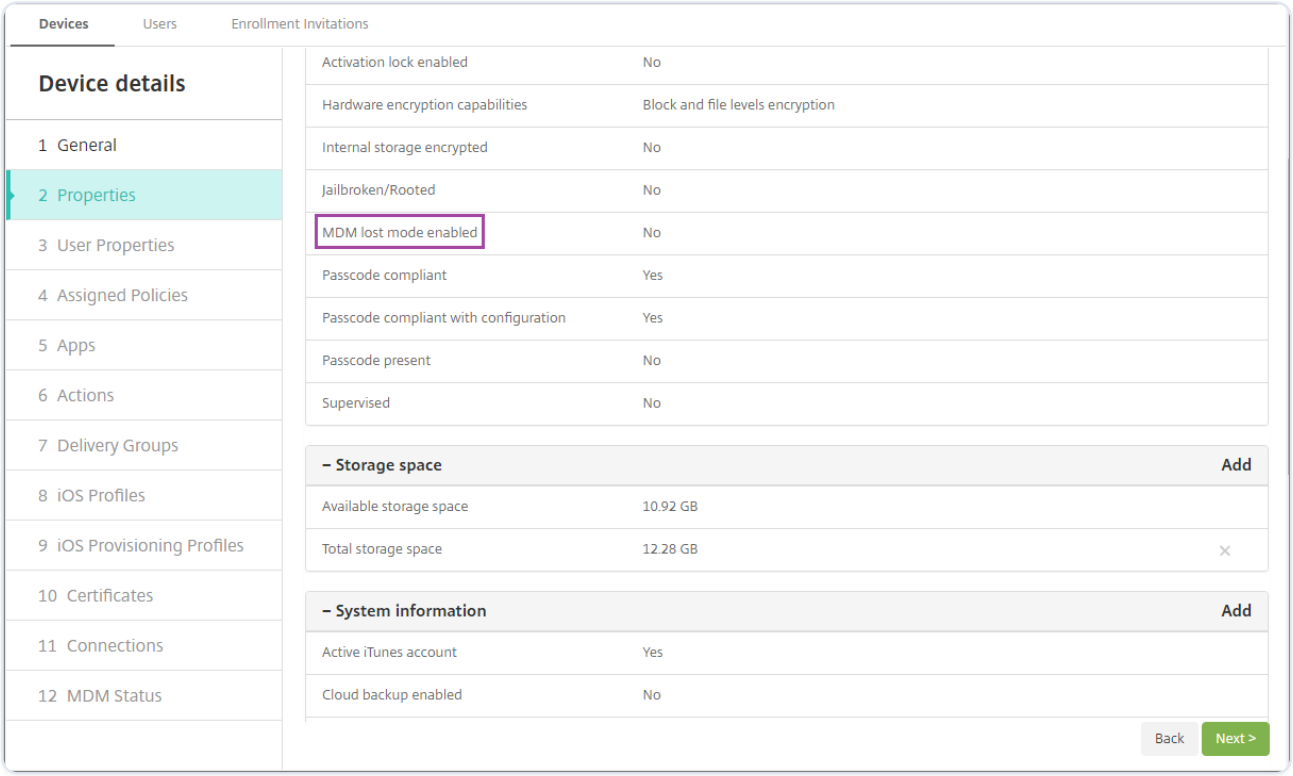


使用以下任一方法检查丢失模式状态：

- 在“**安全操作**”窗口中，验证按钮是否设置为“**禁用丢失模式**”。
- 在“**管理 > 设备**”中，在“**安全**”下的“**常规**”选项卡上，查看上次的“启用丢失模式”或“禁用丢失模式”操作。



- 在“**管理 > 设备**”中，在“**属性**”选项卡上，验证“**MDM 丢失模式已启用**”设置的值是否正确。



如果您在 iOS 设备上启用 XenMobile Server 丢失模式，XenMobile Server 控制台也会发生以下更改：

- 在“**配置 > 操作**”中，“**操作**”列表不包括以下自动化操作：“**吊销设备**”、“**选择性擦除设备**”和“**完全擦除设备**”。
- 在“**管理 > 设备**”中，“**安全操作**”列表不再包括“**吊销**”和“**选择性擦除**”设备操作。您仍然可以根据需要使用安全操作执行“**完全擦除**”操作。

iOS 会将“Lost iPad”字样附加到您在“**安全操作**”屏幕的“**消息**”中键入的内容。

如果您将“**消息**”留空并提供电话号码，Apple 会在设备锁定屏幕上显示“Call owner”消息。

绕过 iOS 激活锁

激活锁是“查找我的 iPhone/iPad”的一项功能，可防止重新激活丢失或被盗的受监管设备。激活锁要求用户提供 Apple ID 和密码，然后才能执行以下操作：关闭“查找我的 iPhone/iPad”、抹掉设备或重新激活设备。对于贵组织拥有的设备，绕过激活锁是必要的，例如，用于重置或重新分配设备。

要启用激活锁，请配置并部署 XenMobile Server MDM 选项设备策略。然后，您可以从 XenMobile Server 控制台管理设备，而无需用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 XenMobile Server 控制台发出“激活锁绕过”安全操作。

例如，如果用户归还丢失的手机，或者在完全擦除之前或之后设置设备：当手机提示输入 Apple App Store 帐户凭据时，您可以通过从 XenMobile Server 控制台发出“激活锁绕过”安全操作来绕过该步骤。

激活锁绕过的设备要求

- 通过 Apple Configurator 或 Apple Deployment Program 进行监管
- 配置了 iCloud 帐户
- 查找我的 iPhone/iPad 已启用
- 已注册到 XenMobile Server
- MDM 选项设备策略（且已启用激活锁）已部署到设备

在对设备执行完全擦除之前绕过激活锁：

1. 转到 **管理 > 设备**，选择设备，单击**安全**，然后单击**激活锁绕过**。
2. 擦除设备。激活锁屏幕不会在设备设置期间出现。

在对设备执行完全擦除之后绕过激活锁：

1. 重置或擦除设备。激活锁屏幕会在设备设置期间出现。
2. 转到 **管理 > 设备**，选择设备，单击**安全**，然后单击**激活锁绕过**。
3. 在设备上轻触“返回”按钮。主屏幕随即出现。

请记住以下几点：

- 建议您的用户不要关闭“查找我的 iPhone/iPad”。不要从设备执行完全擦除。在上述任何一种情况下，系统都会提示用户输入 iCloud 帐户密码。帐户验证后，用户在擦除所有内容和设置后将不会看到“激活 iPhone/iPad”屏幕。
- 对于已生成激活锁绕过代码且已启用激活锁的设备：如果您在完全擦除后无法绕过“激活 iPhone/iPad”页面，则无需从 XenMobile Server 中删除该设备。您或用户可以直接联系 Apple 支持以解除设备锁定。
- 在硬件清单盘点期间，XenMobile Server 会查询设备以获取激活锁绕过代码。如果绕过代码可用，设备会将其发送到 XenMobile Server。然后，要从设备中删除绕过代码，请从 XenMobile Server 控制台发送“激活锁绕过”安全操作。此时，XenMobile Server 和 Apple 都拥有解除设备锁定所需的绕过代码。
- 激活锁绕过安全操作依赖于 Apple 服务的可用性。如果该操作不起作用，您可以按如下方式解除设备锁定。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代码。要查找绕过代码，请转至“**管理 > 设备**”，选择设备，单击“**编辑**”，然后单击“**属性**”。“**激活锁绕过代码**”位于“**安全信息**”下。

macOS

要在 XenMobile 中管理 macOS 设备，您需要从 Apple 设置 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 支持以下适用于 MDM 中 macOS 设备的注册身份验证类型。

- 域
- 域加一次性密码
- 邀请 URL 加一次性密码

macOS 15 中受信任证书的要求：

Apple 对 TLS 服务器证书有新的要求。请验证所有证书是否符合 Apple 的新要求。请参阅 Apple 发布的内容，`<https://support.apple.com/zh-cn/HT210176>`。有关管理证书的帮助，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。

必须保持开放的 Apple 主机名

某些 Apple 主机名必须保持开放，以确保 iOS、macOS 和 Apple App Store 的正常运行。阻止这些主机名可能会影响以下各项的安装、更新和正常运行：iOS、iOS 应用程序、MDM 操作以及设备和应用程序注册。有关详细信息，请参阅 `<https://support.apple.com/zh-cn/HT201999>`。

支持的注册方法

下表列出了 XenMobile 支持的 macOS 设备注册方法：

方法	支持
Apple 部署计划	是

方法	支持
Apple 校园教务管理	是
Apple 配置器	否
手动注册	是
注册邀请	是

Apple 为企业和教育帐户提供了设备注册计划。对于企业帐户，您可以通过注册 Apple 部署计划，在 XenMobile 中使用 Apple 部署计划进行设备注册和管理。该计划适用于 iOS 和 macOS 设备。请参阅 通过 Apple 部署计划部署设备。

对于教育账户，您可以创建一个 Apple School Manager 账户。Apple School Manager 统一了部署计划和批量采购。Apple School Manager 是一种教育版 Apple 部署计划。请参阅 与 Apple 教育功能集成。

您可以使用 Apple 部署计划批量注册 iOS 和 macOS 设备。您可以直接从 Apple、参与的 Apple 授权经销商或运营商处购买这些设备。

配置 macOS 设备策略

使用这些策略配置 XenMobile 如何与运行 macOS 的设备交互。此表列出了适用于 macOS 设备的所有设备策略。

AirPlay 镜像	应用清单	日历 (CalDAV)
联系人 (CardDAV)	控制操作系统更新	凭据

防火墙	字体	导入 iOS 和 macOS 配置文件
LDAP	邮件	密码
配置文件删除	限制	SCEP
VPN	Web 剪辑	无线局域网

注册 macOS 设备

XenMobile 提供了两种注册运行 macOS 的设备的方法。这两种方法都允许 macOS 用户通过无线方式直接从其设备注册。

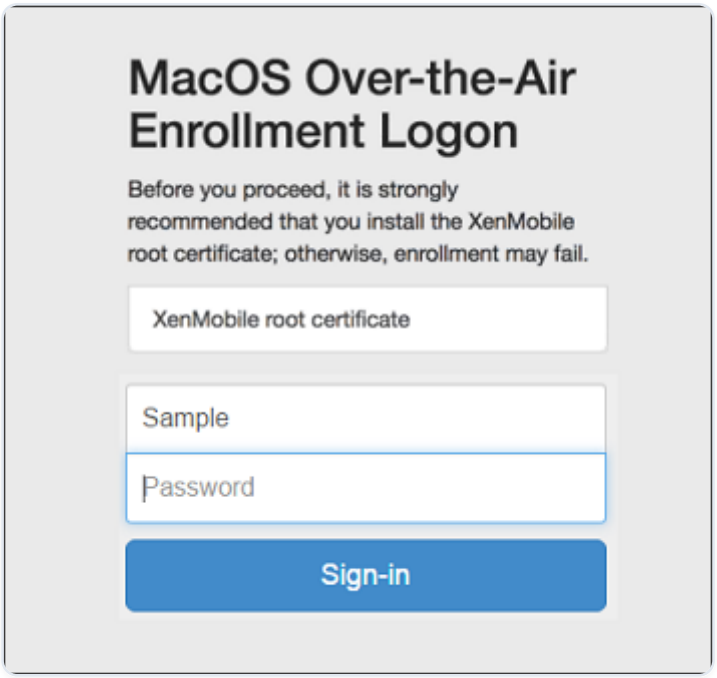
- **向用户发送注册邀请：**此注册方法允许您为 macOS 设备设置以下任何注册安全模式：
  - 用户名 + 密码
  - 用户名 + PIN
  - 双因素身份验证

  当用户按照注册邀请中的说明操作时，将出现一个已填写用户名的登录屏幕。
- **向用户发送注册链接：** 这种适用于 macOS 设备的注册方法会向用户发送一个注册链接，用户可以在 Safari 或 Chrome 浏览器中打开该链接。然后，用户通过提供其用户名和密码进行注册。

  要阻止将注册链接用于 macOS 设备，请将服务器属性 **Enable macOS OTAE** 设置为 **false**。因此，macOS 用户只能通过使用注册邀请进行注册。

向 macOS 用户发送注册邀请

1. 添加 macOS 用户注册邀请。请参阅 创建注册邀请。
2. 用户收到邀请并点击链接后，Safari 浏览器中将出现以下屏幕。XenMobile 会填写用户名。如果您为注册安全模式选择了 **Two Factor**，则会出现另一个字段。



3. 用户根据需要安装证书。用户是否看到安装证书的提示取决于您是否为 macOS 配置了以下内容：公共信任的 SSL 证书和公共信任的数字签名证书。有关证书的信息，请参阅 证书和身份验证。

4. 用户提供请求的凭据。

   Mac 设备策略已安装。您现在可以像管理移动设备一样，开始使用 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** 是默认的安全端口。如果您配置了不同的端口，请使用该端口而不是 8443。
   - **instanceName**（通常显示为 `zdm`）是服务器安装期间指定的名称。

   有关发送安装链接的详细信息，请参阅发送注册邀请。

2. 用户根据需要安装证书。如果为 iOS 和 macOS 配置了公共信任的 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。

   Mac 设备策略已安装。您现在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

您可以远程锁定丢失的 macOS 设备。XenMobile 会锁定设备。然后，它会生成一个 PIN 码并将其设置到设备中。要访问设备，用户需要键入 PIN 码。使用**取消锁定**可从 XenMobile 控制台移除锁定。

您可以使用密码设备策略配置与 PIN 码关联的更多设置。有关详细信息，请参阅macOS 设置。

1. 点击 **管理 > 设备**。将显示 **设备** 页面。

   设备页面 (/en-us/xenmobile/server/media/manage-devices-macos.png)

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。您也可以单击列表项中的其他任意位置以显示列表右侧的选项菜单。

选项菜单 (/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos.png)

选项菜单 (/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos-2.png)

3. 在选项菜单中，单击 **保护**。将显示 **安全操作** 对话框。

   安全操作对话框 (/en-us/xenmobile/server/media/manage-devices-secure-lock-macos.png)

4. 单击 **锁定**。将显示 **安全操作** 确认对话框。

   安全操作确认 (/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm-macos.png)

5. 单击 **锁定设备**。

> **重要提示：**
>
> 您也可以指定一个密码，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，则锁定操作将失败。

批量注册 Apple 设备

您可以通过两种方式在 XenMobile® 中注册大量 iOS、iPadOS 和 macOS 设备。

- 使用 Apple 部署计划注册您直接从 Apple、参与的 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 支持用于 Apple Business Manager (ABM) 和 Apple School Manager (ASM) 教育的 Apple 部署计划。本文介绍了如何将多个设备与您的 ABM 帐户集成。有关注册 ABM 以及将您的 ABM 帐户与 XenMobile 连接的信息，请参阅通过 Apple 部署计划部署设备。有关 Apple School Manager 帐户的信息，请参阅与 Apple 教育功能集成。

  对于 macOS 设备的注册，XenMobile 要求设备运行 macOS 10.10 或更高版本。

- 您还可以使用 Apple Configurator 2 注册 iOS 设备，无论您是否直接从 Apple 购买。

使用 ABM：

- 您无需接触或准备设备。相反，您通过 ABM 提交设备序列号或采购订单号来配置和注册设备。

- XenMobile 注册设备后，您可以将其提供给用户，用户可以立即开始使用。使用 ABM 设置设备时，您可以省去用户首次启动设备时可能需要完成的一些设置助理步骤。
- 有关设置 ABM 的更多信息，请参阅Apple Business Manager 提供的文档。

使用 苹果配置器 2：

- 您将 iOS 设备连接到运行 macOS 10.7.2 或更高版本以及 Apple Configurator 2 应用程序的 Apple 电脑。您通过 Apple Configurator 2 准备 iOS 设备并配置策略。
- 在您使用所需策略配置设备后，设备首次连接到 XenMobile 时，将从 XenMobile 接收策略。然后，您可以开始管理这些设备。
- 有关使用 Apple Configurator 2 的更多信息，请参阅Apple Configurator Help。

先决条件

打开 XenMobile 与 Apple 之间连接所需的端口。有关更多信息，请参阅端口要求。

将您的 Apple Business Manager 帐户与 XenMobile 集成

如果您尚未在 XenMobile 中设置 ABM 帐户，请在 通过 Apple 部署计划部署设备 中完成以下步骤。

- 注册到 Apple Business Manager 中。
- 将您的 Apple Business Manager 帐户与 XenMobile 连接。
- 订购已启用部署计划的设备。
- 管理已启用部署计划的设备。

为批量注册设置默认服务器

要将大量 iOS、iPadOS 和 macOS 设备分配给 MDM 服务器，您可以将 XenMobile 设置为默认服务器。

1. 使用管理员或设备注册管理器帐户登录 Apple Business Manager。
2. 在侧边栏中，单击 **设置 > 设备管理设置**。
3. 选择一个现有 MDM 服务器。在 **默认设备分配** 下，单击 **更改**。为每种设备类型选择默认的 XenMobile 服务器。单击 **完成**。

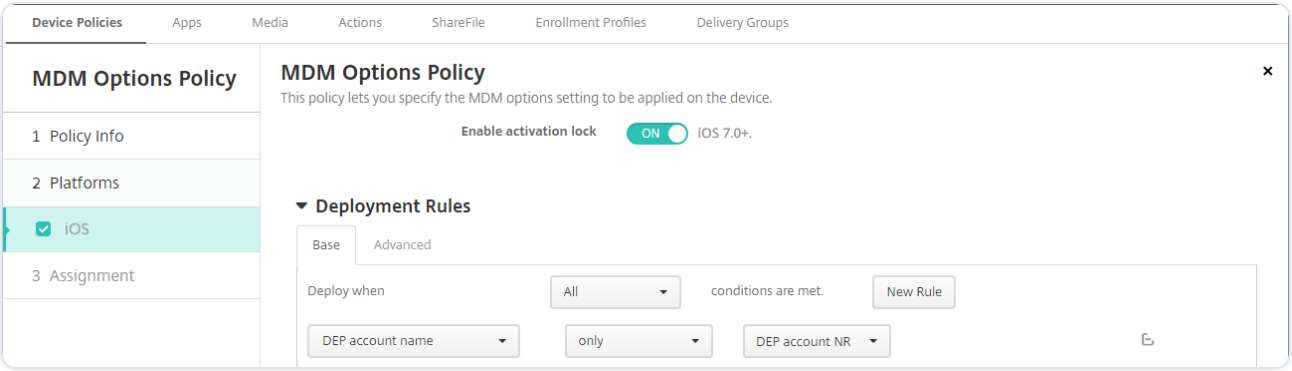
为 ABM 帐户配置设备策略和应用程序的部署规则

您可以使用 **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。您可以指定策略或应用程序：

- 仅部署到特定 ABM 帐户。
- 部署到除所选帐户之外的所有 ABM 帐户。

ABM 帐户列表仅包含状态为“已启用”或“已禁用”的帐户。如果 ABM 帐户已禁用，则 ABM 设备不属于此帐户。因此，XenMobile 不会将应用程序或策略部署到设备。

在以下示例中，设备策略仅部署到 ABM 帐户名称为“ABM Account NR”的设备。

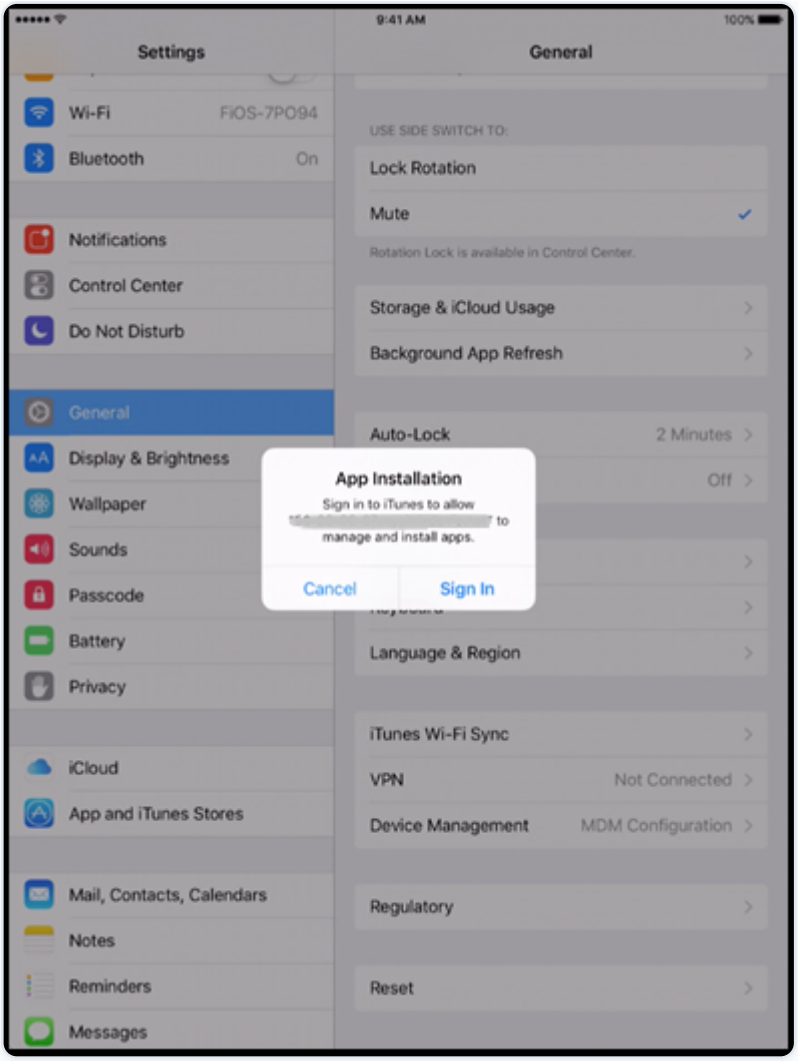


注册已启用 Apple 部署计划的设备时的用户体验

用户注册已启用 Apple 部署计划的设备时，其体验如下。

1. 用户启动其已启用 Apple 部署计划的设备。
2. XenMobile 将您在 XenMobile 控制台中配置的 Apple 部署计划配置交付到已启用 Apple 部署计划的设备。
3. 用户在其设备上配置初始设置。
4. 设备自动启动 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，则此步骤是可选的。在这种情况下，您无需创建 Apple App Store 帐户或使用现有帐户。



7. 用户打开 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。

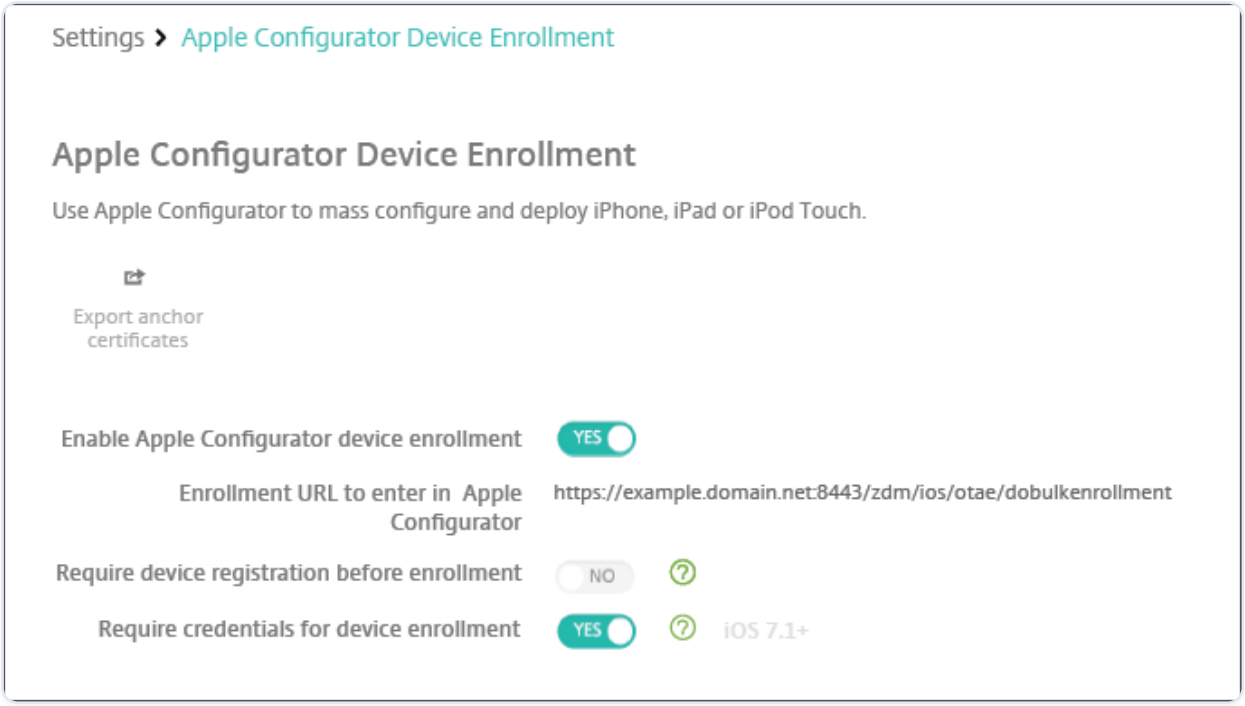
   XenMobile 将所有剩余的所需应用程序部署到设备。

配置 Apple Configurator 2 设置

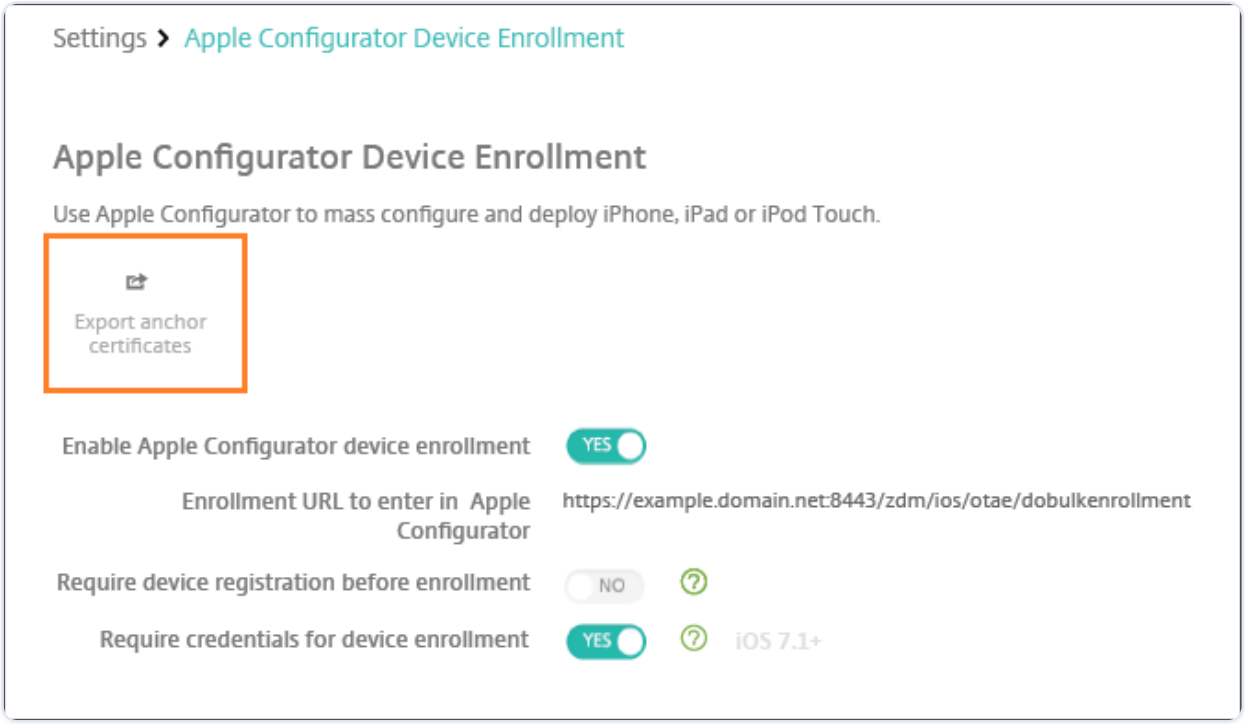
您可以使用 Apple Configurator 2 而不是 Apple Business Manager 批量配置和部署 iPhone 和 iPad 设备。

步骤 1：在 XenMobile 中配置设置

1. 在 XenMobile 控制台中，转到 **Settings > Apple Configurator Device Enrollment**（设置 > Apple Configurator 设备注册）。



2. 将 **Enable Apple Configurator device enrollment**（启用 Apple Configurator 设备注册）设置为 **Yes**（是）。
3. **Enrollment URL to enter in Apple Configurator**（要在 Apple Configurator 中输入的注册 URL）是一个只读字段。此设置提供与 Apple 通信的 XenMobile Server 的 URL。在 Apple Configurator 2 中配置设置时，复制并粘贴此 URL。注册 URL 是 XenMobile Server 完全限定域名 (FQDN)，例如 `mdm.server.url.com`，或 IP 地址。
4. 要防止未知设备注册，请将 **Require device registration before enrollment**（注册前需要设备注册）设置为 **Yes**（是）。注意：如果此设置为 **Yes**（是），则必须在注册前手动或通过 CSV 文件将配置的设备添加到 XenMobile 中的 **Manage > Devices**（管理 > 设备）。
5. 要要求 iOS 设备用户在注册时输入其凭据，请将 **Require credentials for device enrollment**（设备注册需要凭据）设置为 **Yes**（是）。默认情况下，注册不需要凭据。
6. 注意：如果 XenMobile Server 使用受信任的 SSL 证书，请跳过此步骤。单击 **Export anchor certs**（导出锚点证书）并将 certchain.pem 文件保存到 macOS 钥匙串（登录或系统）。



步骤 2：在 Apple Configurator 2 中配置设置

1. 从 应用商店 安装 Apple Configurator 2。
2. 使用 Dock Connector 转 USB 连接线将设备连接到运行 Apple Configurator 2 的 Mac。您可以同时配置多达 30 台连接的设备。如果没有 Dock Connector，请使用一个或多个有源 USB 2.0 高速集线器连接设备。
3. 启动 Apple Configurator 2。配置器会显示您可以准备进行监管的任何设备。
4. 要准备设备进行监管：
   - 如果您打算通过定期重新应用配置来保持对设备的控制，请选择 **Supervise devices**。单击 **Next**。

     > **重要提示：**
     >
     > 将设备置于监管模式会在设备上安装所选版本的 iOS，并完全清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** 以获取要安装的最新版本 iOS。
5. 在 **Enroll in MDM Server** 中，选择一个 MDM 服务器。要添加新服务器，请单击 **Next**
6. 在 **Define an MDM server** 中，为服务器提供一个名称，并从 XenMobile 控制台粘贴 MDM 服务器 URL。

7. 在 **Assign to organization** 中，选择一个组织来监管设备。

   有关使用 Apple Configurator 2 准备设备的更多信息，请参阅 Apple Configurator 帮助页面 准备设备。

8. 准备好每台设备后，将其打开以启动 iOS 设置助理，该助理会为设备首次使用做好准备。

将设备从 Apple Configurator 2 分配到 Apple Business Manager

您可以将 Apple Configurator 2 中的 iPhone 和 iPad 设备与您的 Apple Business Manager 帐户关联。添加设备后，它们会显示在 **Devices** 部分。这些设备不再包含通过 Apple Configurator 2 分配的注册设置。有关更多信息，请参阅 将从 Apple Configurator 2 添加的设备分配到 Apple Business Manager。

使用 Apple 部署计划时续订或更新证书

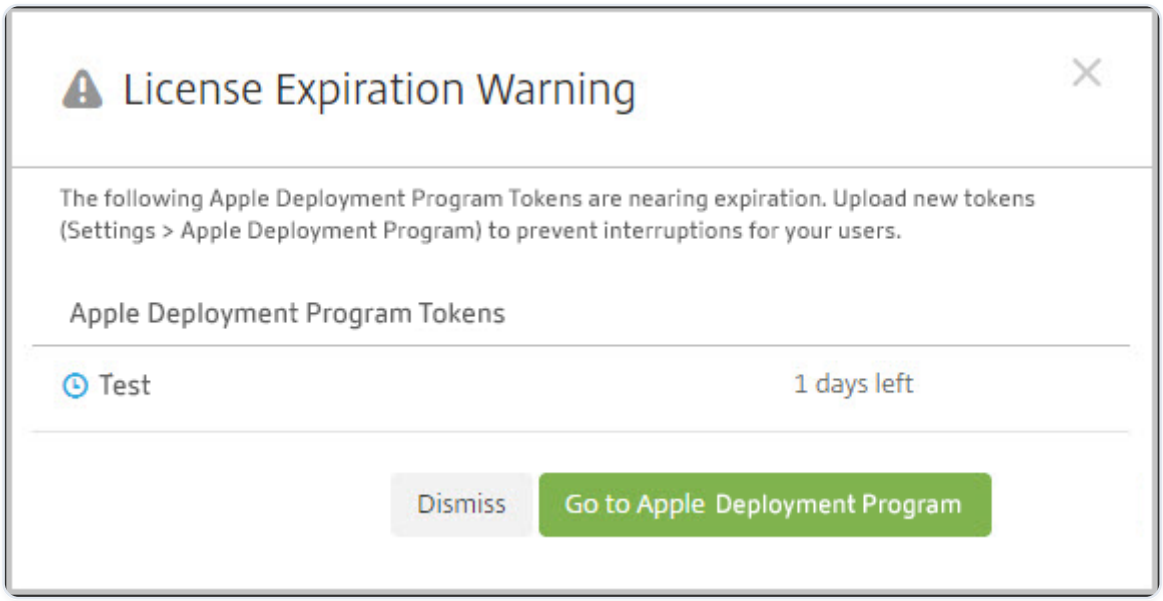
当 XenMobile 安全套接字层 (SSL) 证书续订时，您可以在 XenMobile 控制台的 **Settings > Certificates** 中上传新证书。在 **Import** 对话框中，在 **Use as** 中，单击 **SSL Listener**，以便将证书用于 SSL。重新启动服务器后，XenMobile 将使用新的 SSL 证书。有关 XenMobile 中证书的更多信息，请参阅 在 XenMobile 中上传证书。

在续订或更新 SSL 证书时，无需重新建立 Apple Deployment Program 与 XenMobile 之间的信任关系。但是，您可以随时按照本文中的前面步骤重新配置您的 **Apple Deployment Program** 设置。

有关 Apple Deployment Program 的详细信息，请参阅Apple 文档。

续订 Apple Deployment Program 与 XenMobile 之间的连接

当您的自动化设备注册服务器令牌过期时，XenMobile 会显示“许可证过期警告”。



替换来自 Apple School Manager/Apple Business Manager 的令牌。

步骤 1：从 XenMobile Server 下载公钥

1. 在 XenMobile 控制台中，转到**设置 > Apple Deployment Program**以下载新的公钥。

步骤 2：从您的 Apple 帐户创建并下载服务器令牌文件

1. 登录 Apple Business Manager 以下载令牌。
2. 打开**设置**，然后选择需要令牌的服务器。单击**编辑**。
3. 在 **MDM 服务器设置**下，上传从 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 中上传服务器令牌文件

1. 在 Citrix XenMobile 中，转到**设置 > Apple Deployment Program**。
2. 选择部署计划帐户，单击**编辑**，并上传您的服务器令牌文件。
3. 单击**下一步**并保存更改。

客户端属性

客户端属性包含直接提供给用户设备上的 Secure Hub 的信息。您可以使用这些属性来配置高级设置，例如 Citrix PIN。您可以从 Citrix 支持获取客户端属性。

客户端属性会随着 Secure Hub 的每个版本以及偶尔的客户端应用程序而变化。有关更常用客户端属性的详细信息，请参阅本文后面的客户端属性参考。

1. 在 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，单击“**客户端属性**”。此时将显示“**客户端属性**”页面。您可以从此页面添加、编辑和删除客户端属性。

Settings > Client Properties

Client Properties

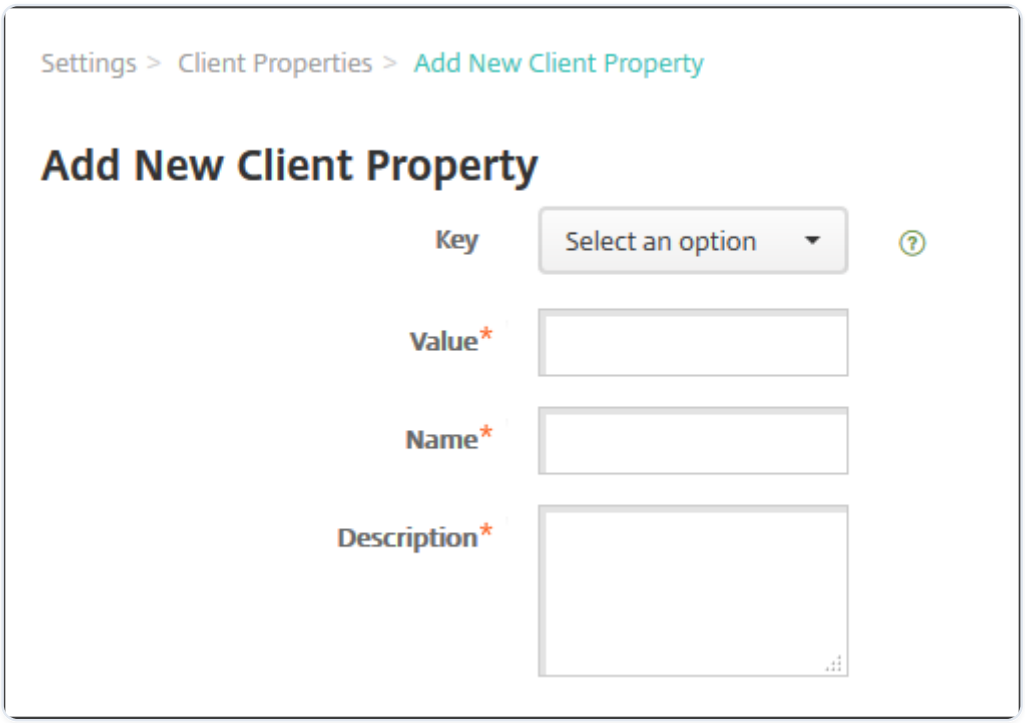
To change a property, select the property and then click Edit.

Add

Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

添加客户端属性

1. 单击“**添加**”。此时将显示“**添加新客户端属性**”页面。



2. 配置以下设置：

   - **密钥：** 在列表中，单击要添加的属性密钥。重要提示：在更新设置之前，请联系 Citrix 支持。您可以请求一个特殊密钥。
   - **值：** 所选属性的值。
   - **名称：** 属性的名称。
   - **描述：** 属性的描述。

3. 单击“**保存**”。

编辑客户端属性

1. 在“**客户端属性**”表中，选择要编辑的客户端属性。

   选中客户端属性旁边的复选框时，选项菜单会显示在客户端属性列表上方。当您单击列表中的其他任何位置时，选项菜单会显示在列表的右侧。

2. 单击“**编辑**”。“**编辑客户端属性**”页面随即显示。

   客户端属性屏幕的图像(/en-us/xenmobile/server/media/client-properties-edit.png)

3. 根据需要更改以下信息：

   - **密钥：** 您无法更改此字段。
   - **值：** 属性值。
   - **名称：** 属性名称。
   - **描述：** 属性描述。

4. 单击“**保存**”以保存更改，或单击“**取消**”以使属性保持不变。

删除客户端属性

1. 在“**客户端属性**”表中，选择要删除的客户端属性。

   您可以通过选中每个属性旁边的复选框来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 预定义客户端属性及其默认设置如下：

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 显示名称：MDX 容器自毁周期
  - 自毁功能可在指定天数不活动后阻止访问 Secure Hub 和托管应用程序。超过时间限制后，应用程序将无法使用。擦除数据包括清除每个已安装应用程序的应用程序数据，包括应用程序缓存和用户数据。

    不活动时间是指服务器在特定时间长度内未收到验证用户的身份验证请求。例如，如果此属性设置为 30 天，并且用户超过 30 天未使用该应用程序，则此策略将生效。

    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，请转到 **设置 > 客户端属性** 并添加自定义密钥 **CONTAINER_SELF_DESTRUCT_PERIOD**。
  - 值：天数

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - 显示名称：将设备日志发送到 IT 帮助台
  - 此属性启用或禁用向 IT 帮助台发送日志的功能。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**

- **DISABLE_LOGGING**
  - 显示名称: 禁用日志记录
  - 使用此属性可防止用户从其设备收集和上传日志。此属性会禁用 Secure Hub 和所有已安装 MDX 应用程序的日志记录。用户无法从“支持”页面发送任何应用程序的日志。即使出现邮件撰写对话框，也不会附加日志。此时会显示一条消息，指示日志记录已禁用。此设置还会阻止您在 XenMobile 控制台中更新 Secure Hub 和 MDX 应用程序的日志设置。

    当此属性设置为 **true** 时，Secure Hub 会将 **阻止应用程序日志** 设置为 **true**。因此，当应用新策略时，MDX 应用程序将停止日志记录。
  - 可能的值: **true** 或 **false**
  - 默认值: **false** (日志记录未禁用)

- **ENABLE_CRASH_REPORTING**
  - 显示名称: 启用崩溃报告
  - 如果为 **true**，Citrix 将收集崩溃报告和诊断信息，以帮助排查 Secure Hub for iOS 和 Android 的问题。如果为 **false**，则不收集任何数据。
  - 可能的值: **true** 或 **false**
  - 默认值: **true**

- **ENABLE_CREDENTIAL_STORE**
  - 显示名称: 启用凭据存储
  - 启用凭据存储意味着 Android 或 iOS 用户在访问移动生产力应用程序时只需输入一次密码。无论是否启用 Citrix PIN，您都可以使用凭据存储。如果不启用 Citrix PIN，用户将输入其 Active Directory 密码。XenMobile 仅支持 Secure Hub 和公共应用商店应用程序将 Active

Directory 密码与凭据存储结合使用。如果将 Active Directory 密码与凭据存储结合使用，XenMobile 不支持 PKI 身份验证。

- 在 Secure Mail 中自动注册要求您将此属性设置为 **true**。
- 要配置此自定义客户端策略，请转至 **设置 > 客户端属性**，添加自定义密钥 **ENABLE_CREDENTIAL_STORE**，并将 **值** 设置为 **true**。

- **ENABLE_FIPS_MODE**
  - 显示名称: 启用 FIPS 模式
  - 此属性用于在移动设备上启用或禁用 FIPS 模式。更改此值后，Secure Hub 会在执行下一次在线身份验证时将新值传递给设备。
  - 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
  - 此属性允许您启用 Citrix PIN 功能。使用 Citrix PIN 或密码时，系统会提示用户定义一个 PIN，以替代其 Active Directory 密码。当 ENABLE_PASSWORD_CACHING 启用或 XenMobile 使用证书身份验证时，此设置会自动启用。

    对于离线身份验证，Citrix PIN 在本地进行验证，用户可以访问其请求的应用程序或内容。对于在线身份验证，Citrix PIN 或密码会解锁 Active Directory 密码或证书，然后将其发送以使用 XenMobile 进行身份验证。

    如果 ENABLE_PASSCODE_AUTH 为 true 且 ENABLE_PASSWORD_CACHING 为 false，在线身份验证将始终提示输入密码，因为 Secure Hub 不会保存它。
  - 可能的值: **true** 或 **false**
  - 默认值: **false**

- **ENABLE_PASSWORD_CACHING**
  - 显示名称: 启用用户密码缓存
  - 此属性允许 Active Directory 密码在移动设备上本地缓存。将此属性设置为 **true** 时，还必须将 **ENABLE_PASSCODE_AUTH** 属性设置为 **true**。启用用户密码缓存后，XenMobile 会提示用户设置 Citrix PIN 或密码。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**

- **ENABLE_TOUCH_ID_AUTH**
  - 显示名称：启用触控 ID 身份验证
  - 对于支持触控 ID 身份验证的设备，此属性可启用或禁用设备上的触控 ID 身份验证。要求：

    用户设备必须启用 Citrix PIN 或 LDAP。如果 LDAP 身份验证已关闭（例如，因为仅使用基于证书的身份验证），用户必须设置 Citrix PIN。在这种情况下，即使客户端属性 **ENABLE_PASSCODE_AUTH** 为 **false**，XenMobile 也需要 Citrix PIN。

    将 **ENABLE_PASSCODE_AUTH** 设置为 **false**，以便当用户启动应用程序时，他们必须响应使用触控 ID 的提示。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **ENABLE_WORXHOME_CEIP**
  - 显示名称：启用 Worx Home CEIP
  - 此属性将启用客户体验改善计划。该功能会定期向 Citrix 发送匿名配置和使用情况数据。这些数据有助于 Citrix 提高 XenMobile 的质量、可靠性和性能。
  - 值：**true** 或 **false**
  - 默认值：**false**
- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 显示名称：使用密码加密机密
  - 此属性将敏感数据存储在设备上的秘密保管库中，而不是存储在基于平台的本机存储（例如 iOS 钥匙串）中。此属性可对关键工件进行强加密并增加用户熵。用户熵是用户生成的随机 PIN 码，只有用户知道。

    Citrix 建议您启用此属性，以帮助提高用户设备上的安全性。因此，用户会收到更多 Citrix PIN 身份验证提示。
  - 可能的值：**true** 或 **false**
  - 默认值：**false**
- **INACTIVITY_TIMER**
  - 显示名称：不活动计时器
  - 此属性定义了用户可以将设备置于不活动状态多长时间，然后无需提示 Citrix PIN 或密码即可访问应用程序。要为 MDX 应用程序启用此设置，请将“应用程序密码”设置设为“开”。如

果“应用程序密码”设置设为“关”，用户将被重定向到 Secure Hub 以进行完全身份验证。更改此设置后，该值将在用户下次收到身份验证提示时生效。

在 iOS 上，“不活动计时器”还控制 MDX 和非 MDX 应用程序对 Secure Hub 的访问。

- 可能的值：任何正整数
- 默认值：**15**（分钟）

- **ON_FAILURE_USE_EMAIL**
  - 显示名称：失败时使用电子邮件将设备日志发送到 IT 帮助台
  - 此属性启用或禁用使用电子邮件将设备日志发送到 IT 的功能。
  - 可能的值：**true** 或 **false**
  - 默认值：**true**

- **PASSCODE_EXPIRY**
  - 显示名称：PIN 更改要求
  - 此属性定义 Citrix PIN 或密码的有效期，此后，用户必须更改其 Citrix PIN 或密码。更改此设置后，新值仅在当前 Citrix PIN 或密码过期时生效。
  - 可能的值：建议为 **1** 到 **99**。若要避免 PIN 重置，请将值设置为一个较大的数字（例如，100,000,000,000）。如果您最初将有效期设置为 1 到 99 天之间，然后在此期间更改为较大的数字：PIN 仍会在初始期限结束时过期，但此后不会再过期。
  - 默认值：**90**（天）

- **PASSCODE_HISTORY**
  - 显示名称：PIN 历史记录
  - 此属性定义用户在更改 Citrix PIN 或密码时不能重复使用的先前 Citrix PIN 或密码的数量。更改此设置后，新值将在用户下次重置其 Citrix PIN 或密码时生效。
  - 可能的值：**1** 到 **99**
  - 默认值：**5**

- **PASSCODE_MAX_ATTEMPTS**
  - 显示名称：PIN 尝试次数
  - 此属性定义用户在系统提示进行完全身份验证之前可以尝试输入错误 Citrix PIN 或密码的次数。用户成功完成完全身份验证后，系统会提示他们创建 Citrix PIN 或密码。
  - 可能的值：任何正整数

  - 默认值: **15**

- **PASSCODE_MIN_LENGTH**
  - 显示名称: PIN 码长度要求
  - 此属性定义 Citrix PIN 码的最小长度。
  - 可能的值: **4** 到 **10**
  - 默认值: **6**

- **PASSCODE_STRENGTH**
  - 显示名称: PIN 码强度要求
  - 此属性定义 Citrix PIN 码或通行码的强度。更改此设置后，用户下次在系统提示进行身份验证时，将需要创建 Citrix PIN 码或通行码。
  - 可能的值: **低**、**中**、**高**或**强**
  - 默认值: **中**
  - 基于 PASSCODE_TYPE 设置的每个强度设置的密码规则如下：

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，允许任意序列	444444, 123456, 654321	
中（默认设置）	所有数字不能相同或连续。	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
高	相邻数字不能相同。	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
强	不要使用相同的数字超过两次。不要使用三个或更多连续的数字。不要使用三个或更多反向连续的数字。	102983, 085085, 824673, 132312	132132, 131313, 902030

字母数字密码的规则：

密码强度	字母数字密码类型的规则	允许	不允许
低	必须包含至少一个数字和一个字母	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
中（默认设置）	除了低密码强度的规则外，字母和所有数字不能相同。字母不能连续，数字也不能连续。	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, 或 aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, 或 cba123
高	至少包含一个大写字母和一个小写字母。	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
强	至少包含一个数字、一个特殊符号、一个大写字母和一个小写字母。	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **PASSCODE_TYPE**
  - 显示名称：PIN 类型
  - 此属性定义用户是可定义数字 Citrix PIN 还是字母数字密码。当您选择**数字**时，用户只能使用数字 (Citrix PIN)。当您选择**字母数字**时，用户可以使用字母和数字的组合（密码）。

    如果您更改此设置，用户在下次系统提示其进行身份验证时必须设置新的 Citrix PIN 或密码。
  - 可能的值：**数字**或**字母数字**
  - 默认值：**数字**
- **REFRESHINTERVAL**
  - 显示名称: REFRESHINTERVAL
  - 默认情况下，XenMobile 每 3 天 ping 一次自动发现服务器 (ADS) 以获取固定证书。要更改刷新间隔，请转到**设置 > 客户端属性**，添加自定义密钥 **REFRESHINTERVAL**，并将**值**设置为小时数。
  - 默认值: **72** 小时（3 天）
- **SEND_LDAP_ATTRIBUTES**

- 对于 Android、iOS 或 macOS 设备的仅 MAM 部署：您可以配置 XenMobile，以便使用电子邮件凭据注册 Secure Hub 的用户自动注册 Secure Mail。因此，用户无需提供额外信息或采取额外步骤即可注册 Secure Mail。
- 要配置此全局客户端策略，请转到**设置 > 客户端属性**，添加自定义密钥 **SEND_LDAP_ATTRIBUTES**，并按如下方式设置**值**。
- 值: `userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}`
- 属性值指定为宏，类似于 MDM 策略。
- 以下是此属性的示例帐户服务响应：

  ```
  <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,em
  name="SEND_LDAP_ATTRIBUTES"/>
  ```

- 对于此属性，XenMobile 将逗号字符视为字符串终止符。因此，如果属性值包含逗号，请在其前面加上反斜杠。反斜杠可防止客户端将嵌入的逗号解释为属性值的结尾。使用 `"\\"` 表示反斜杠字符。

- **HIDE_THREE_FINGER_TAP_MENU**
  - 当此属性未设置或设置为 **false** 时，用户可以通过在其设备上执行三指轻触来访问隐藏功能菜单。隐藏功能菜单允许用户重置应用程序数据。将此属性设置为 **true** 会禁用用户对隐藏功能菜单的访问。
  - 要配置此全局客户端策略，请转到**设置 > 客户端属性**，添加自定义密钥 **HIDE_THREE_FINGER_TAP_MENU**，并设置**值**。
- **TUNNEL_EXCLUDE_DOMAINS**
  - 显示名称：隧道排除域
  - 默认情况下，MDX 会从微 VPN 隧道中排除 XenMobile SDK 和应用程序用于各种功能的某些服务终结点。例如，这些终结点包括不需要通过企业网络路由的服务，例如 Google Analytics、Citrix Cloud™ 服务和 Active Directory 服务。使用此客户端属性可覆盖默认的排除域列表。
  - 要配置此全局客户端策略，请转至“**设置 > 客户端属性**”，添加自定义密钥 **TUNNEL_EXCLUDE_DOMAINS**，然后设置“**值**”。
  - 值：要将默认列表替换为您要从隧道中排除的域，请键入一个逗号分隔的域后缀列表。要将所有域都包含在隧道中，请键入 **none**。默认值为：

`app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.launchdarkly.com hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

XenMobile Server 的自定义客户端属性如下：

- **ENABLE_MAM_NFACTOR_SSO**
  - 此属性允许您在使用 NetScaler® Gateway 中的高级身份验证策略时，在 Secure Hub 的 MAM 注册或登录期间启用或禁用 MAM nFactor SSO。如果值设置为 **true**，则在 Secure Hub 的 MAM 注册或登录期间启用 MAM nFactor SSO。
  - 要配置此属性，请转至“**设置 > 客户端属性**”，然后单击“**添加**”。在“**密钥**”下拉菜单中选择“**自定义密钥**”，并根据需要更新以下信息：
    - 密钥 - ENABLE_MAM_NFACTOR_SSO
    - 值 - true 或 false
    - 名称 - ENABLE_MAM_NFACTOR_SSO
    - 描述 - 添加相关描述
- **MICROSOFT_CERTIFICATE_STRONG_MAPPING**
  - 此属性控制在使用 Secure Mail 和 Microsoft 公钥基础结构 (PKI) 时，是否通过将安全标识符 (SID) 附加到主题备用名称 (SAN) 来续订现有客户端证书以支持证书强映射功能。如果值设置为 **true**，则将续订现有客户端证书以包含 SAN SID。
  - 此属性仅适用于 Microsoft PKI。
  - 要配置此属性，请转到“**设置 > 客户端属性**”，然后单击“**添加**”。在“**密钥**”下拉菜单中选择“**自定义密钥**”，并根据需要更新以下信息：
    - 密钥 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
    - 值 - true 或 false
    - 名称 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
    - 描述 - 续订客户端证书以包含 SAN SID

通过 Apple Deployment Program 部署设备

Apple 为企业和教育帐户提供了设备注册计划。对于企业帐户，您需要注册 Apple Deployment Program，以便在 XenMobile 中使用 Apple Business Manager (ABM) 或 Apple School Manager (ASM) 进行设备注册和管理。该计划适用于 iOS、iPadOS 和 macOS 设备。

Apple Deployment Program 适用于组织而非个人。您必须提供大量的公司详细信息和资料才能创建 Apple Deployment Program 帐户。因此，请求和获得帐户批准可能需要一些时间。

对于教育帐户，您需要创建一个 Apple School Manager 帐户。ASM 整合了 Apple Deployment Program 和 Apple 批量采购。要创建 Apple School Manager 帐户，请访问 Apple 学校网站。

注册 Apple 部署计划

要注册 Apple Business Manager，请访问 business.apple.com。单击“**立即注册**”以申请新帐户。最佳做法是使用您组织的电子邮件地址，例如 `deployment@company.com`。注册过程可能需要几天时间。收到登录凭据后，请按照 Apple Business Manager 中提供的步骤创建帐户。

> **注意：**

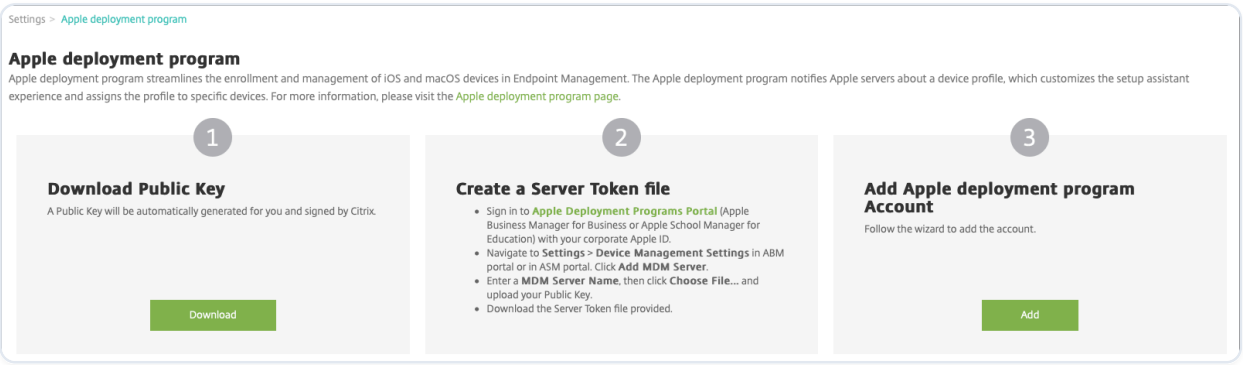
> 对于教育帐户，请参阅 与 Apple 教育功能集成。

将您的 Apple Business Manager 帐户与 XenMobile 连接

要将您的 Apple Business Manager 帐户与 XenMobile 部署连接，请在 XenMobile 控制台和 Apple Business Manager 中输入信息。请按照以下步骤操作：

步骤 1：从 XenMobile Server 下载公钥

1. 在 XenMobile 控制台中，转到“**设置 > Apple Deployment Program**”。



2. 在“**下载公钥**”下，单击“**下载**”。

步骤 2：从您的 Apple 帐户创建并下载服务器令牌文件

1. 使用管理员或设备注册管理器帐户登录 Apple 商务管理。
2. 在侧栏底部，单击“**设置**”，然后单击“**设备管理设置 > 添加 MDM 服务器**”。

   Apple Deployment Program 设置屏幕(/en-us/xenmobile/server/media/asm-add-mdm-server.png)
3. 在“**MDM 服务器名称**”设置中，键入 XenMobile 服务器的名称。您键入的服务器名称仅供参考。它不是服务器 URL 或名称。
4. 在“**上传公钥**”下，单击“**选择文件**”。上传从 XenMobile 下载的公钥，然后保存更改。
5. 单击“**下载令牌**”将服务器令牌文件下载到您的计算机。

   将 ABM 帐户添加到 XenMobile 时，必须上传服务器令牌文件。导入令牌文件后，您的 ABM 令牌信息将显示在 XenMobile 控制台中。
6. 在“**默认设备分配**”下，单击“**更改**”。选择您要如何分配设备，然后提供所请求的信息。有关详细信息，请参阅 ABM 用户指南。

步骤 3：将 ABM 帐户添加到 XenMobile

您可以将多个 ABM 帐户添加到 XenMobile。此功能使您能够按国家/地区、部门等使用不同的注册设置和设置助理选项。然后，您可以将 ABM 帐户与不同的设备策略相关联。

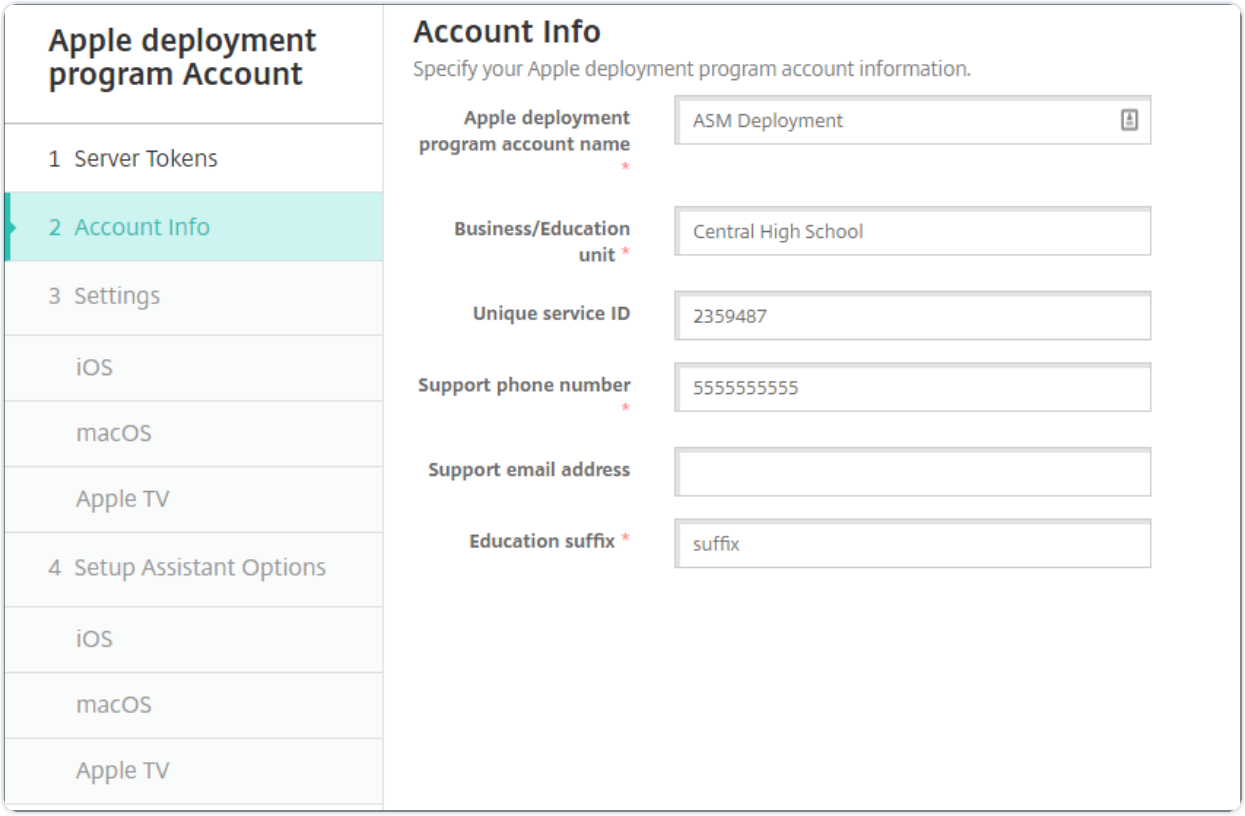
例如，您可以在同一 XenMobile 服务器上集中管理来自不同国家/地区的所有 ABM 帐户，以导入和监督所有 ABM 设备。通过按部门、组织层次结构或其他结构自定义注册设置和设置助理选项，策略可在整个组织中提供适当的功能，并且用户会获得适当的帮助。

1. 在 XenMobile 控制台中，转到“**设置 > Apple Deployment Program**”，然后在“**添加 Apple Deployment Program 帐户**”下，单击“**添加**”。

   Apple Deployment Program 设置屏幕(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-1.png)
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“**上传**”。

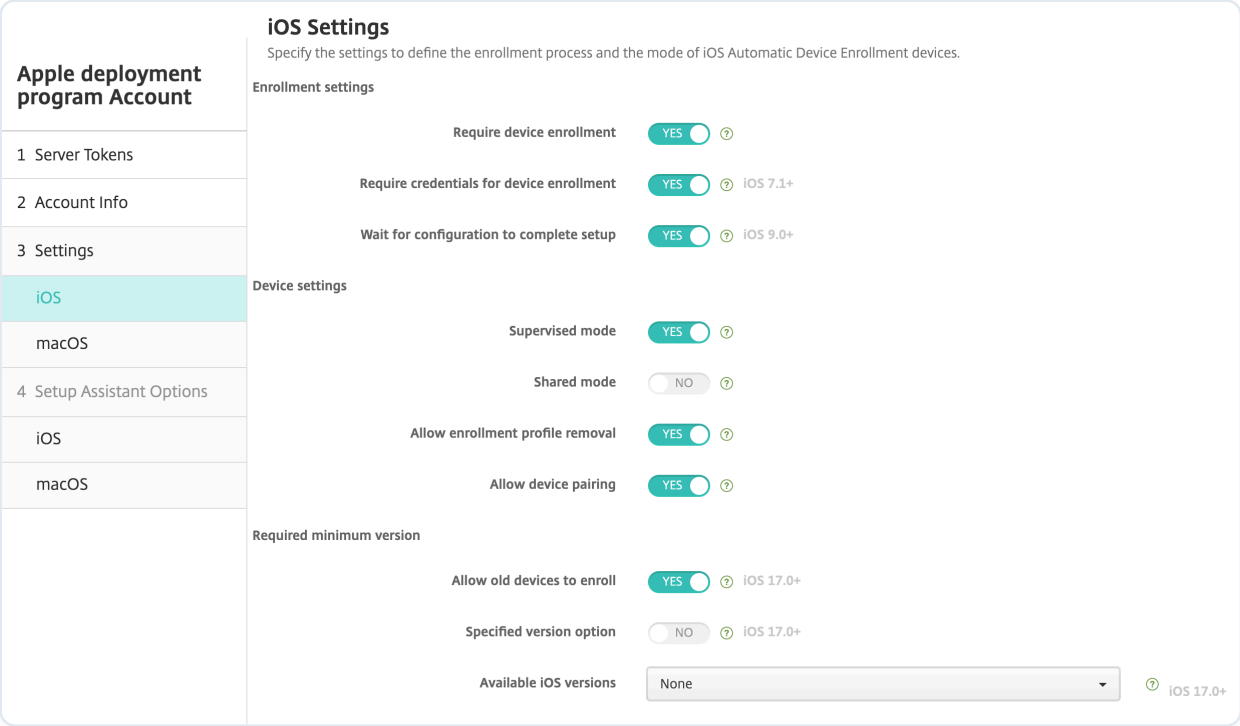
   Apple Deployment Program 设置屏幕(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-2.png)

   您的服务器令牌信息将显示。
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。使用能够反映您如何组织 Apple 部署计划帐户的名称，例如按国家/地区或组织层次结构。
- **业务/教育单位：** 设备分配到的业务单位或部门。此字段为必填项。
- **唯一服务 ID：** 一个可选的唯一 ID，可帮助您进一步识别帐户。
- **支持电话号码：** 用户在设置过程中寻求帮助时拨打的支持电话号码。此字段为必填项。
- **支持电子邮件地址：** 可供最终用户使用的可选支持电子邮件地址。
- **教育后缀**：适用于 ASM 帐户。键入通过此帐户注册的设备所分配的后缀。

4. 在 **iOS 设置**中，指定以下设置：



注册设置

- **要求设备注册：** 是否要求用户注册其设备。默认值为**是**。
- **要求设备注册凭据：** 是否要求用户在 ABM 设置期间输入其凭据。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 且未选择此选项，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。如果您确实选择了此选项，XenMobile 将不会创建这些组件。因此，如果您以后清除此选项，则尚未输入凭据的用户将无法注册 ABM，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 ABM 帐户并重新启用它。
- **等待配置完成设置：** 是否要求用户设备保持在“设置助理”模式，直到所有 MDM 资源部署到设备。此设置适用于受监管模式下的设备。默认值为“**否**”。
- Apple 文档指出，当设备处于“设置助理”模式时，以下命令可能无法工作：
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

设备设置

- **受监管模式：** 如果您使用 Apple Configurator 管理 ABM 注册设备，或者启用了“**等待配置完成设置**”时，必须设置为“**是**”。默认值为“**是**”。有关将 iOS 设备置于受监管模式的详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监管模式。
- **允许删除注册配置文件：** 是否允许设备使用可远程删除的配置文件。默认值为“**否**”。
- **允许设备配对：** 对于通过 ABM 注册的设备，是否可以通过 Apple Music 和 Apple Configurator 管理它们。默认值为“**否**”。

所需的最低版本

- **允许旧设备注册**：如果启用，即使设备无法升级到当前所需的最低版本，也可以注册。默认值为“开”。此选项仅适用于 iOS 17.0 及更高版本。
- **指定版本选项**：是否允许管理员手动输入指定版本。默认值为“**关**”。此选项仅适用于 iOS 17.0 及更高版本。
- **可用 iOS 版本**：您可以从列表中选择可用的 iOS 版本。如果设备的 iOS 版本低于当前版本，它将在设备上启动更新过程。如果版本将来过期，则使用可用版本列表中的最低版本。默认值为 **无**，设置为 **无** 时不会生效。此选项仅适用于 iOS 17.0 及更高版本。
- **指定版本**：如果设备的 iOS 版本低于当前版本，它将在设备上启动更新过程。如果版本将来过期，则使用可用版本列表中的最低版本。请确保输入正确的版本号，以防止出现任何意外错误。

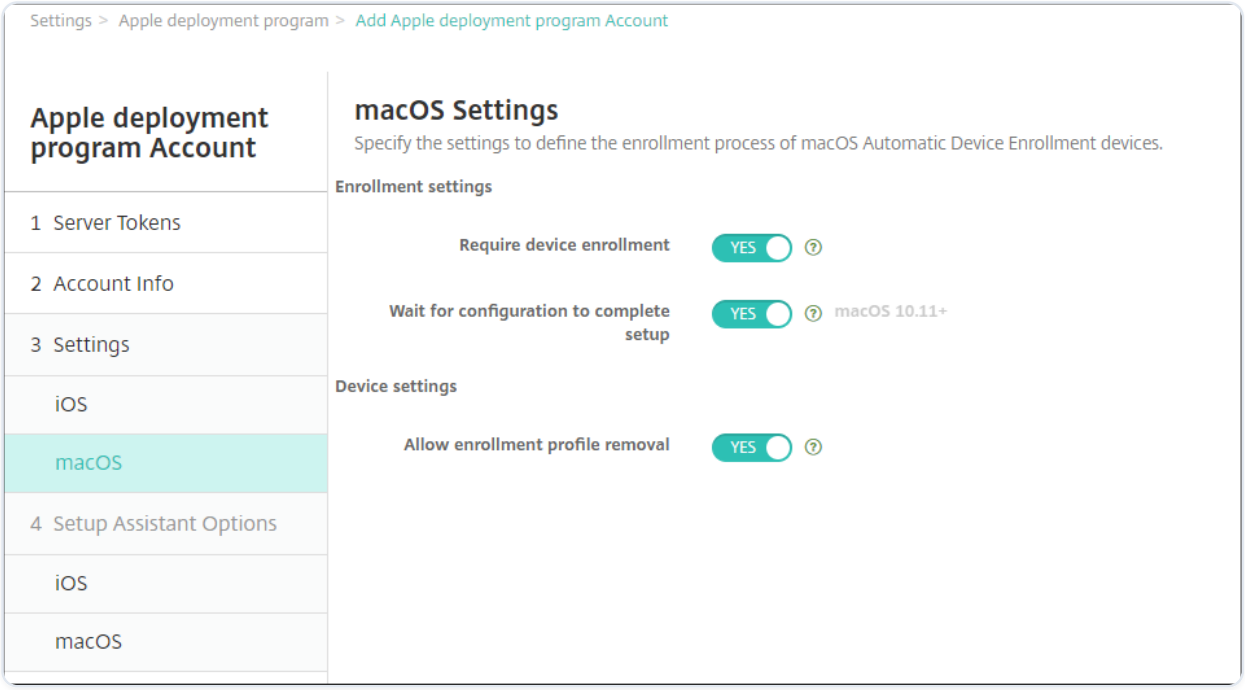
监管身份

如果您使用 GroundControl 工具，可以添加证书以执行以下操作：

- 覆盖配对限制，以避免出现“信任此主机”提示。
- 通过 USB 提升受管设备操作，以执行配置文件安装等活动，无需用户交互。这样做允许 GroundControl 启用单一应用模式和设备锁定以进行结账。
- 将备份还原到 ABM 设备。

有关 GroundControl 的更多信息，请参阅 GroundControl 网站。

5. 在 **macOS 设置** 中，指定以下设置：



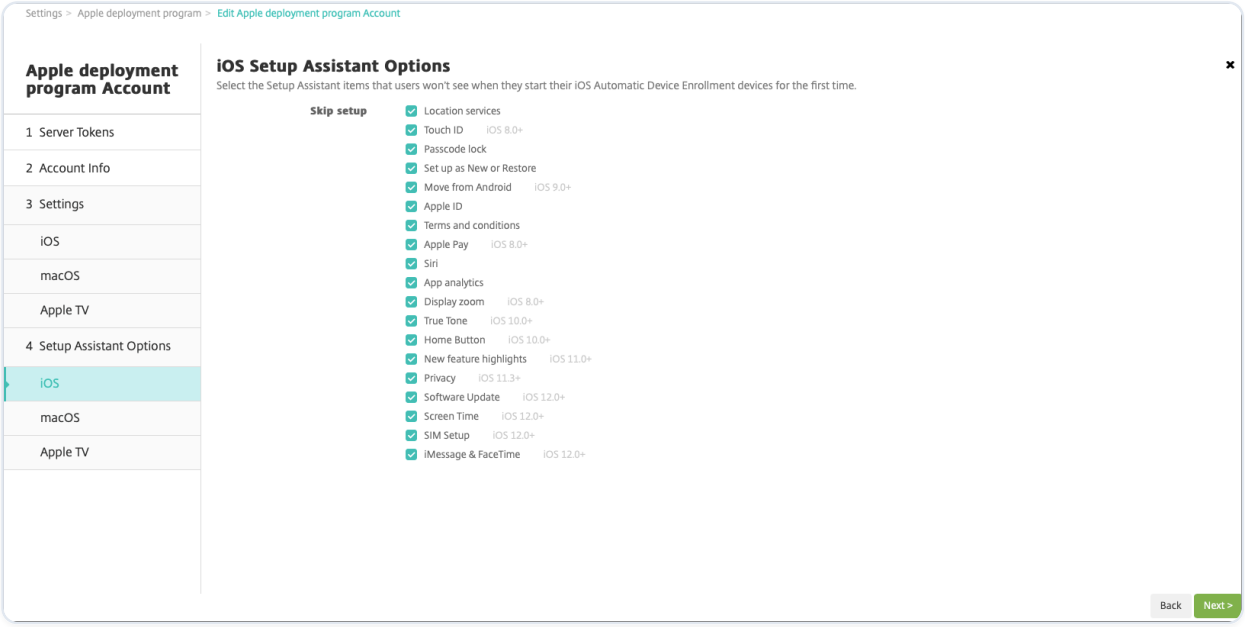
注册设置

- **要求设备注册**：是否要求用户注册其设备。默认值为 **是**。
- **等待配置完成设置**：如果为 **是**，macOS 设备将不会在设置助手中继续，直到 MDM 资源密码部署到设备。该部署发生在本地帐户创建之前。此设置适用于 macOS 10.11 及更高版本的设备。默认值为 **否**。

设备设置

- **允许移除注册配置文件**：是否允许设备使用可远程移除的配置文件。默认值为 **否**。

6. 在 **iOS 设置助理选项**中，选择用户首次启动设备时 iOS 设置助理跳过的步骤。跳过某个屏幕时，相关功能将使用默认设置。除非您完全限制对这些功能的访问，否则用户可以在设置完成后配置跳过的功能。有关限制对功能访问的详细信息，请参阅限制设备策略。所有项目的默认设置均未选中。以下说明解释了选中某个设置时会发生什么。

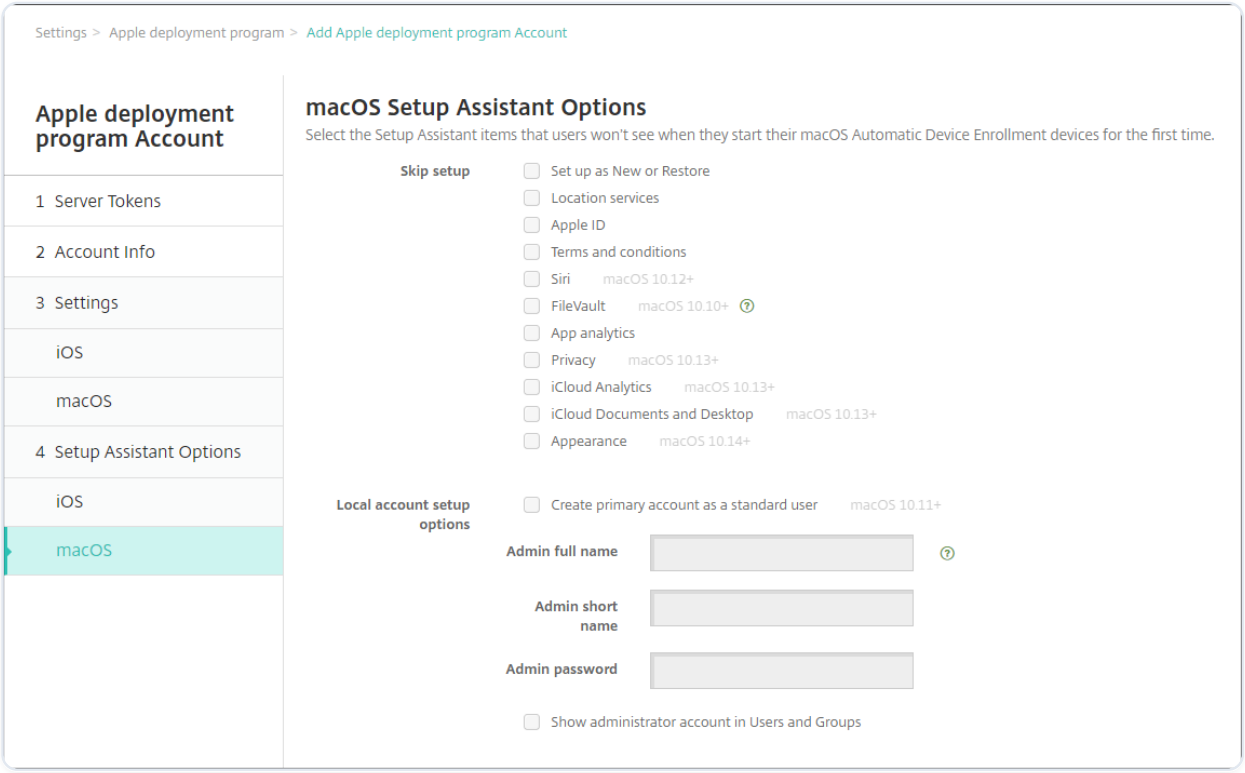


- **定位服务：** 阻止用户在设备上设置定位服务。
- **触控 ID：** 阻止用户在 iOS 设备上设置触控 ID 或面容 ID。在 iOS 15 中已弃用。
- **密码锁定：** 阻止用户为设备设置密码。如果不存在密码，用户将无法使用触控 ID 或 Apple Pay。
- **设置为新设备或恢复：** 阻止用户将设备设置为新设备或从 iCloud 或 Apple App Store 备份恢复。
- **从 Android 迁移：** 阻止用户将数据从 Android 设备传输到 iOS 设备。此选项仅在选中**设置为新设备或恢复**时可用（即，跳过此步骤）。
- **Apple ID：** 阻止用户为设备设置受管 Apple ID 帐户。
- **条款和条件：** 阻止用户阅读和接受设备使用条款和条件。
- **Apple Pay：** 阻止用户设置 Apple Pay。如果此设置未选中，用户必须设置触控 ID 和 Apple ID。请确保这些设置已清除。
- **Siri：** 阻止用户配置 Siri。
- **应用分析：** 阻止用户设置是否与 Apple 共享崩溃数据和使用统计信息。
- **显示缩放：** 阻止用户在 iOS 设备上设置显示分辨率（标准或缩放）。在 iOS 17 中已弃用。
- **原彩显示：** 阻止用户设置四通道传感器以动态调整显示屏的白平衡。
- **主屏幕按钮：** 阻止用户设置主屏幕按钮的反馈样式。在 iOS 15 中已弃用。
- **新功能亮点：** 阻止用户看到显示 Apple 软件新功能信息的屏幕。
- **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。
- **屏幕使用时间：** 阻止用户启用屏幕使用时间。适用于 iOS 12.0 及更高版本。

- **SIM 卡设置：** 阻止用户设置蜂窝网络套餐。适用于 iOS 12.0 及更高版本。
- **iMessage 与 FaceTime：** 阻止用户启用 iMessage 和 FaceTime。适用于 iOS 12.0 及更高版本。
- **外观：** 阻止用户选择外观模式。适用于 iOS 13.0 及更高版本。
- **欢迎：** 阻止用户看到“**开始使用**”屏幕。适用于 iOS 13.0 及更高版本。
- **恢复完成：** 阻止用户在设置过程中看到恢复是否完成。适用于 iOS 14.0 及更高版本。
- **更新完成：** 阻止用户在设置过程中看到软件更新是否完成。适用于 iOS 14.0 及更高版本。
- **操作按钮：** 阻止用户看到操作按钮配置窗格。适用于 iOS 17.0 及更高版本。
- **锁定模式：** 如果已设置 Apple 帐户，则阻止用户看到锁定模式窗格。适用于 iOS 17.1 及更高版本。
- **智能：** 阻止用户看到智能窗格。适用于 iOS 18.0 及更高版本。
- **相机按钮：** 阻止用户看到相机按钮窗格。适用于 iOS 18.0 及更高版本。

ABM 帐户显示在“**设置 > Apple 部署计划**”中。

7. 在 **macOS 设置助理选项**中，选择用户首次启动设备时 macOS 设置助理跳过的步骤。跳过某个屏幕时，相关功能将使用默认设置。除非您完全限制对这些功能的访问，否则用户可以在设置完成后配置跳过的功能。有关限制对功能的访问的更多信息，请参阅限制设备策略。所有项目的默认设置均已清除。以下说明解释了选择某个设置时会发生什么。



- **设置为新设备或恢复：** 阻止用户将设备设置为新设备，或从时间机器备份恢复，或执行系统迁移。
- **定位服务：** 阻止用户在设备上设置定位服务。适用于 macOS 10.11 及更高版本。
- **Apple ID：** 阻止用户为设备设置托管式 Apple ID 帐户。
- **条款和条件：** 阻止用户阅读和接受设备使用条款和条件。
- **Siri：** 阻止用户配置 Siri。适用于 macOS 10.12 及更高版本。
- **FileVault：** 使用 FileVault 加密启动磁盘。XenMobile 仅在系统具有单个本地用户帐户且该帐户已登录 iCloud 时才应用 FileVault 设置。

  您可以使用 macOS FileVault 磁盘加密功能通过加密其内容来保护系统卷 (https://support.apple.com/zh-cn/HT204837)。如果您在未启用 FileVault 的新型便携式 Mac 上运行设置助理，系统可能会提示您启用此功能。此提示会出现在新系统和升级到 OS X 10.10 或 10.11 的系统上，但仅当系统具有单个本地管理员帐户且该帐户已登录 iCloud 时才会出现。
- **应用分析：** 阻止用户设置是否与 Apple 共享崩溃数据和使用统计信息。
- **隐私：** 阻止用户查看“数据与隐私”窗格。适用于 macOS 10.13 及更高版本。
- **iCloud 分析：** 阻止用户选择是否将诊断 iCloud 数据发送给 Apple。适用于 macOS 10.13 及更高版本。
- **iCloud 文稿和桌面：** 阻止用户设置 iCloud 桌面和文稿。适用于 macOS 10.13 及更高版本。
- **外观：** 阻止用户选择外观模式。适用于 macOS 10.14 及更高版本。
- **辅助功能：** 阻止用户自动听到旁白。仅当设备连接到以太网时可用。适用于 macOS 11 及更高版本。
- **生物识别：** 阻止用户设置触控 ID 和面容 ID。适用于 macOS 10.12.4 及更高版本。
- **原彩显示：** 阻止用户设置四通道传感器以动态调整显示器的白平衡。适用于 macOS 10.13.6 及更高版本。
- **Apple Pay：** 阻止用户设置 Apple Pay。如果此设置被清除，用户必须设置触控 ID 和 Apple ID。请确保“**Apple ID**”和“**生物识别**”设置已清除。适用于 macOS 10.12.4 及更高版本。
- **屏幕使用时间：** 阻止用户启用屏幕使用时间。适用于 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 使用指定的信息创建帐户。
  - **将主帐户创建为标准用户：** XenMobile 不会授予此用户设备上的管理员权限，而是使用标准权限创建用户。由于 macOS 需要管理员帐户，XenMobile 会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和 shell 中显示的名称。
- **管理员密码：** 为管理员帐户键入一个安全密码。
- **在“用户与群组”中显示管理员帐户：** 如果清除此选项，管理员帐户将不会显示在 macOS 设置的“**用户与群组**”中。如果您将主帐户创建为标准用户，请启用此设置以隐藏 XenMobile 首先创建的管理员帐户。

订购已启用部署计划的设备

您可以直接从 Apple 或已启用部署计划的授权经销商或运营商处订购已启用部署计划的设备。要从 Apple 订购，请在 Apple 部署计划门户中提供您的 Apple 客户 ID。您的客户 ID 使 Apple 能够将您购买的设备与您的 Apple 部署计划帐户关联起来。

要从您的经销商或运营商处订购，请联系您的 Apple 经销商或运营商，以检查他们是否参与 Apple 部署计划。购买设备时，请索取经销商的 Apple 部署计划 ID。当您将 Apple 部署计划经销商添加到您的 Apple 部署计划帐户时，Apple 需要此信息。添加经销商的 Apple 部署计划 ID 后，您将收到一个部署计划客户 ID。将部署计划客户 ID 提供给经销商，经销商将使用该 ID 向 Apple 提交有关您设备购买的信息。有关更多信息，请参阅此Apple 使用设备注册网站。

管理已启用部署计划的设备

订单发货后，您可以将 iOS、iPadOS 和 macOS 设备与您的 XenMobile Server 关联。

1. 使用管理员或设备注册经理帐户登录Apple Business Manager。
2. 在侧边栏中，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 分配到 Apple Business Manager，请参阅 Apple Business Manager 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**。您有两个选项：

   - 要将设备分配给 MDM 服务器，请在 **分配到服务器** 下选择您的 XenMobile Server 名称。单击 **继续**。

     要将新设备批量分配到 Apple Business Manager，请设置一个默认的 XenMobile Server 用于部署。有关详细信息，请参阅 (/zh-cn/xenmobile/server/provision-devices/ios-bulk-enrollment.html#set-a-default-server-for-bulk-enrollment)。
   - 要从 XenMobile Server 取消分配设备，请选择 **取消分配**。

您的 Apple Deployment Program 设备现已与选定的 XenMobile Server 关联。

如果您将 iOS、iPadOS 或 macOS 设备送修，则需要从 Apple Business Manager 中移除该设备。当您收到维修好的设备后，必须将该设备重新分配给 XenMobile Server。更换设备时，您可以使用订单号将新设备分配给 XenMobile Server。

要查看已分配设备的历史记录：

1. 使用管理员或设备注册经理帐户登录 Apple 商务管理。
2. 在侧边栏中，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** 以下载包含所有已分配和未分配设备序列号的 CSV 文件。

如果设备已售出、被盗或无法修复，您可以从 Apple Business Manager 中移除 iOS、iPadOS 和 macOS 设备。

1. 使用管理员或设备注册经理帐户登录 Apple商务管理。
2. 在侧边栏中，单击 **设备** 并搜索设备。
3. 选择设备，然后点击**释放设备**。在对话框中，确认您的更改以将设备从程序中移除。要重新添加 iOS 和 iPadOS 设备，请使用 Apple Configurator 2。您无法使用 Apple Configurator 2 重新添加 macOS 设备。

注册设备

为了远程安全地管理用户设备，您需要在 XenMobile 中注册用户设备。XenMobile 客户端软件将安装在用户设备上，并对用户身份进行身份验证。然后，将安装 XenMobile 和用户配置文件。接下来，在 XenMobile 控制台中，您可以执行设备管理任务。您可以应用策略、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 以及 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 Azure Active Directory 作为 IdP 的集成。

> **注意：**
>
> 在注册 iOS 设备用户之前，您必须请求 APNs 证书。有关详细信息，请参阅 证书和身份验证。
>
> 要更新用户和设备的配置选项，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. 在您的 Android 设备上前往 Google Play 商店，下载 Citrix Secure Hub™ 应用程序，然后点击该应用程序。
2. 当系统提示安装应用程序时，单击“**下一步**”，然后单击“**安装**”。
3. Secure Hub 安装完成后，点击“**打开**”。
4. 输入您的公司凭据，例如您的 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“**激活设备管理员**”屏幕中，点击“**激活**”。
6. 输入您的公司密码，然后点击“**登录**”。
7. 根据 XenMobile 的配置方式，系统可能会要求您创建 Citrix PIN。您可以使用此 PIN 登录 Secure Hub 和其他启用 XenMobile 的应用程序，例如 Secure Mail 和 Citrix Files。您需要输入两次 Citrix PIN。在“**创建 Citrix PIN**”屏幕上，输入一个 PIN。
8. 重新输入 PIN。Secure Hub 将打开。然后，您可以访问 XenMobile 应用商店，查看可在 Android 设备上安装的应用程序。
9. 如果您已将 XenMobile 配置为在注册后自动将应用程序推送到设备，系统会提示用户安装应用程序。此外，您在 XenMobile 中配置的策略将部署到设备。点击“**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 中取消注册。当用户使用以下过程取消注册时，设备仍会显示在 XenMobile 控制台的设备清单中。但是，您无法对设备执行操作。您无法跟踪设备，也无法监控设备合规性。

1. 点击以打开 Secure Hub 应用程序。
2. 根据您使用的是手机还是平板电脑，执行以下操作：

   在手机上：

   - 从屏幕左侧滑动以打开设置窗格。
   - 点击“**首选项**”，点击“**帐户**”，然后点击“**删除帐户**”。

   在平板电脑上：

- 点击右上角您的电子邮件地址旁边的箭头。
- 点击“**首选项**”，点击“**帐户**”，然后点击“**删除帐户**”。

3. 点击“**重新注册**”。此时将显示一条消息，确认您是否要重新注册设备。
4. 点击“**确定**”。

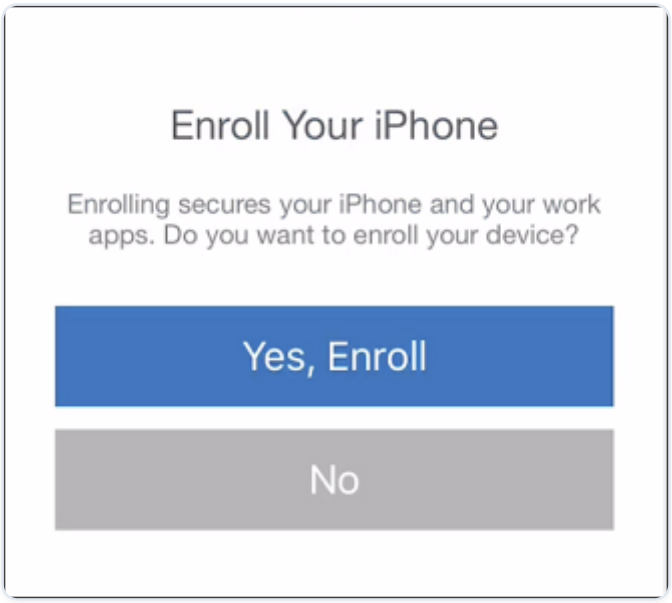
   您的设备已取消注册。

5. 按照屏幕上的说明重新注册您的设备。

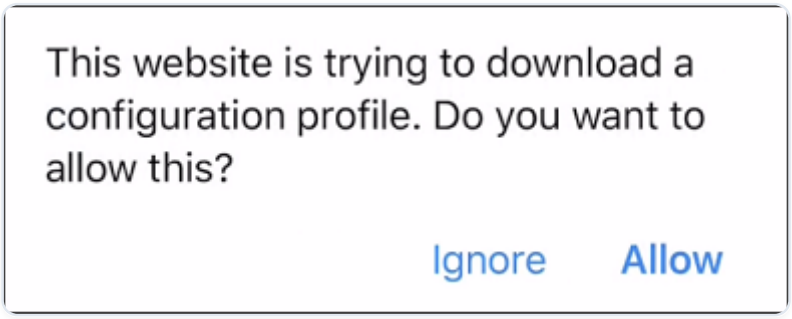
注册 iOS 设备

本节介绍用户如何将 iOS 设备（12.2 或更高版本）注册到 XenMobile Server。有关 iOS 注册的更多信息，请打开以下视频：

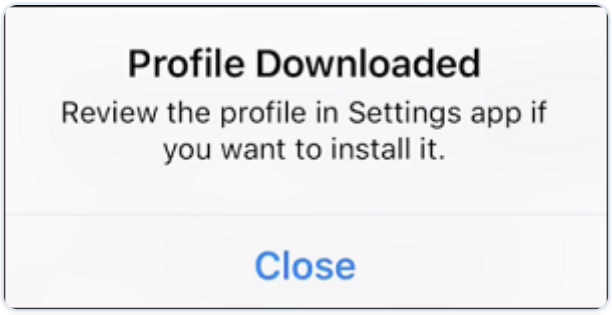
1. 在您的 iOS 设备上前往 Apple Store，下载 Citrix Secure Hub 应用程序，然后点击该应用程序。
2. 当提示安装应用程序时，点击 **Next**，然后点击 **Install**。
3. Secure Hub 安装完成后，点击 **Open**。
4. 输入您的企业凭据，例如您的 XenMobile Server 名称、用户主体名称 (UPN) 或电子邮件地址。然后，点击 **Next**。
5. 点击 **Yes, Enroll** 以注册您的 iOS 设备。



6. 输入凭据后，当提示时点击 **Allow**，以下载配置配置文件。

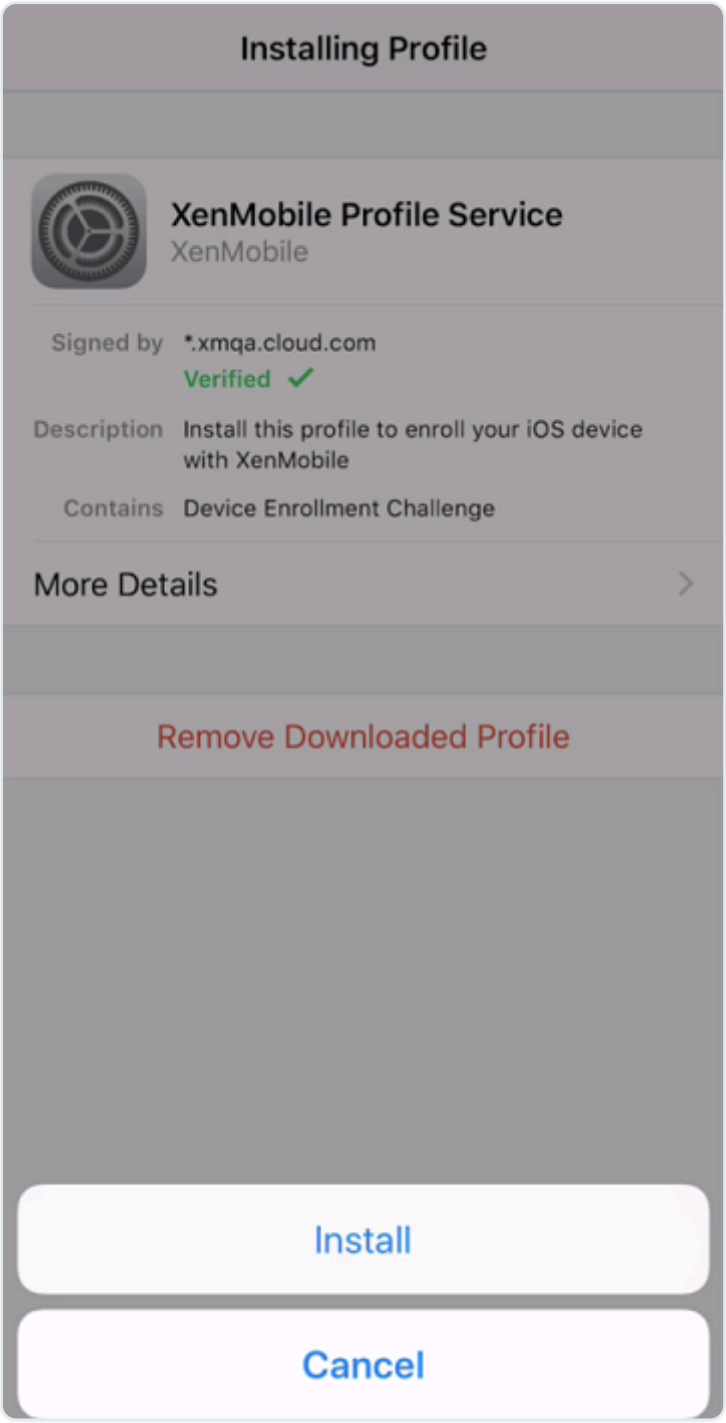


7. 下载配置配置文件后，点击 **Close**。

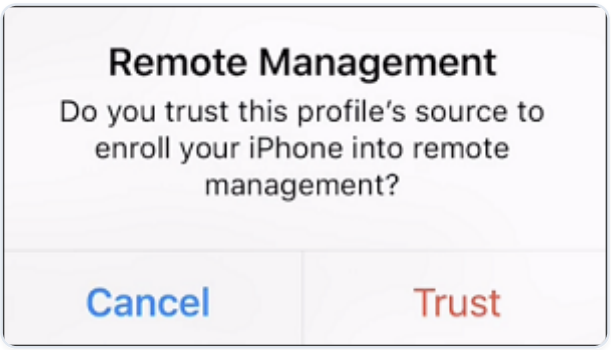


8. 在您的设备设置中，安装 iOS 证书并将设备添加到受信任列表。

   - 转到 **设置 > 通用 > 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** 以将您的设备注册到远程管理。



9. 登录 Secure Hub。如果您正在注册 MDM+MAM：凭据验证后，在出现提示时创建并确认您的 Citrix PIN。
10. 工作流完成后，设备即已注册。然后，您可以访问应用商店以查看可在 iOS 设备上安装的应用。

iOS 设备

1. 从设备上的 Apple iTunes App Store 下载 Secure Hub 应用程序，然后将该应用程序安装到设备上。
2. 在 iOS 设备主屏幕上，轻按 Secure Hub 应用程序。
3. Secure Hub 应用程序打开后，输入您的技术支持部门提供的服务器地址。

   显示的屏幕可能与这些示例不同，具体取决于 XenMobile 的配置方式。
4. 出现提示时，输入您的用户名和密码或 PIN。单击 **下一步**。
5. 出现注册提示时，单击 **是，注册**，然后在出现提示时输入您的凭据。
6. 轻按 **安装** 以安装 Citrix Profile Services。

   Citrix Profile Services 屏幕图像(/en-us/xenmobile/server/media/worxhome-enroll-5.png)
7. 轻按“**信任**”。

   远程管理信任屏幕图像(/en-us/xenmobile/server/media/worxhome-enroll-8.png)
8. 轻按“**打开**”，然后输入您的凭据。

macOS 设备

XenMobile 提供了两种注册运行 macOS 的设备的方法。这两种方法都允许 macOS 用户直接从其设备通过无线方式注册。

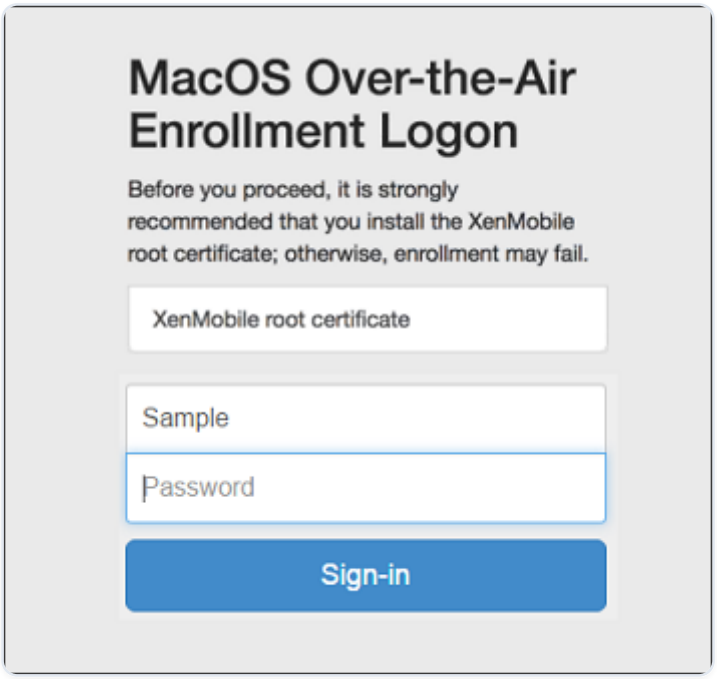
- **向用户发送注册邀请：**此注册方法允许您为 macOS 设备设置以下任何注册安全模式：
  - 用户名 + 密码
  - 用户名 + PIN
  - 双因素

  当用户按照注册邀请中的说明操作时，将显示一个已填写用户名的登录屏幕。
- **向用户发送安装链接：**此 macOS 设备注册方法会向用户发送一个注册链接，他们可以在 Safari 或 Chrome 浏览器中打开该链接。然后，用户通过输入其用户名和密码进行注册。

要阻止将注册链接用于 macOS 设备，请将服务器属性 **Enable macOS OTAE** 设置为 **false**。因此，macOS 用户只能通过注册邀请进行注册。

向用户发送注册邀请

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. 为 macOS 用户注册添加邀请。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，Safari 浏览器中将显示以下屏幕。XenMobile 会填写用户名。如果您为注册安全模式选择了**双因素**，则会出现另一个字段。



4. 用户根据需要安装证书。用户是否看到安装证书的提示取决于您是否为 macOS 配置了以下内容：公共信任的 SSL 证书和公共信任的数字签名证书。有关证书的详细信息，请参阅证书和身份验证。
5. 用户提供请求的凭据。

   Mac 设备策略已安装。您现在可以像管理移动设备一样使用 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** 是默认安全端口。如果您配置了不同的端口，请使用该端口而不是 8443。
- **instanceName**（通常显示为 zdm）是服务器安装期间指定的名称。

有关发送安装链接的详细信息，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 配置了公共信任的 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。

   Mac 设备策略已安装。您现在可以使用 XenMobile 管理 Mac，就像管理移动设备一样。

Windows 设备

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。您可以通过以下任一方式将 Windows 10 和 Windows 11 设备加入 Microsoft Azure AD：

- 在设备首次开机时，作为 Azure AD Join 的一部分，开箱即用地注册到 MDM。
- 设备配置后，从 Windows 设置页面作为 Azure AD Join 的一部分注册到 MDM。

您可以在 XenMobile 中注册运行以下 Windows 操作系统的设备：

- 视窗 10
- 视窗 11

用户可以直接通过其设备注册。

> **注意：**

> 对于 Windows 10 RS2 手机和平板电脑，在重新注册期间，系统不会提示用户输入服务器 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，点击“**正在连接到服务**”旁边的 X，以转到服务器 URL 页面。这是一个第三方问题。

> 您必须配置 AutoDiscovery 和 Windows 发现服务以进行用户注册，才能启用对受支持的 Windows 设备的管理。

在 Windows 设备用户可以使用 Azure 注册之前，您必须在 XenMobile 中配置 Microsoft Azure 服务器设置。有关详细信息，请参阅Microsoft Azure Active Directory 服务器设置。

使用自发现注册 Windows 设备

要启用 Windows 设备的管理，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，检查并安装所有可用的 Windows 更新。
2. 在超级按钮菜单中，点击**设置**，然后点击**帐户 > 访问工作或学校 > 连接到工作或学校**。
3. 对于 Windows 10 和 Windows 11：输入您的公司电子邮件地址，然后点击**继续**。对于 Windows 8.1：点击**打开设备管理**。要以本地用户身份注册，请输入一个不存在但具有正确域名的电子邮件地址（例如，`foo@mydomain.com`）。这使您可以绕过一个已知的 Microsoft 限制，即注册由 Windows 内置的设备管理完成；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。设备会自动找到 XenMobile Server 并开始注册过程。
4. 输入您的密码。使用与 XenMobile 中用户组帐户关联的密码。
5. 对于 Windows 10 和 Windows 11：在**使用条款**对话框中，表明您同意管理您的设备，然后点击**接受**。对于 Windows 8.1：在**允许 IT 管理员的应用和服务**对话框中，表明您同意管理您的设备，然后点击**打开**。

在不使用自动发现的情况下注册 Windows 设备

可以在不使用 AutoDiscovery 的情况下注册 Windows 设备。但是，Citrix 建议您配置 AutoDiscovery。不使用 AutoDiscovery 进行注册会导致在连接到所需 URL 之前调用端口 80，因此不被视为生产部署的最佳实践。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，检查并安装所有可用的 Windows 更新。
2. 对于 Windows 10 和 Windows 11：在超级按钮菜单中，点击**设置**，然后点击**帐户 > 访问工作或学校 > 连接到工作或学校**。对于 Windows 8.1：点击**电脑设置 > 网络 > 工作场所**。
3. 输入您的公司电子邮件地址。
4. 对于 Windows 10 和 Windows 11：如果未配置 AutoDiscovery，则会出现一个选项，您可以在其中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**，请点击以将该选项设置为**关**。
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的 SSL 连接的端口不是 8443，请在此地址中使用该端口号替换 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的 SSL 连接的端口不是 8443，请在此地址中使用该端口号替换 8443。

6. 输入您的密码。
7. 对于 Windows 10 和 Windows 11：在“**使用条款**”对话框中，指示您同意管理您的设备，然后点击“**接受**”。对于 Windows 8.1：在“**允许 IT 管理员的应用程序和服务**”对话框中，指示您同意管理您的设备，然后点击“**打开**”。

发送注册邀请

在 XenMobile 控制台中，您可以向使用 iOS、macOS、Android Enterprise 和旧版 Android 设备的用户发送注册邀请。您还可以向使用 iOS、Android Enterprise 或旧版 Android 设备的用户发送安装链接。

注册邀请的发送方式如下：

- 如果注册邀请是针对一个本地用户或 Active Directory 用户：用户将通过短信在您指定的电话号码和运营商名称处收到邀请。
- 如果注册邀请是针对一个组：用户将通过短信收到邀请。如果 Active Directory 用户在 Active Directory 中有电子邮件地址和手机号码，他们将收到邀请。本地用户将在用户属性中指定的电子邮件和电话号码处收到邀请。

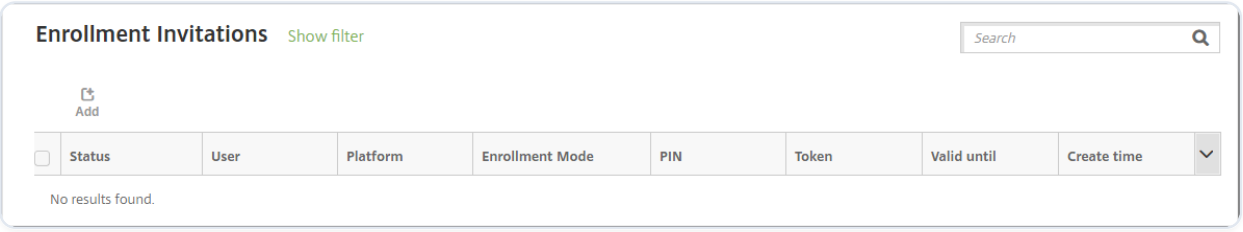
用户注册后，他们的设备将在“**管理 > 设备**”下显示为已管理。邀请 URL 的状态显示为“**已兑换**”。

先决条件

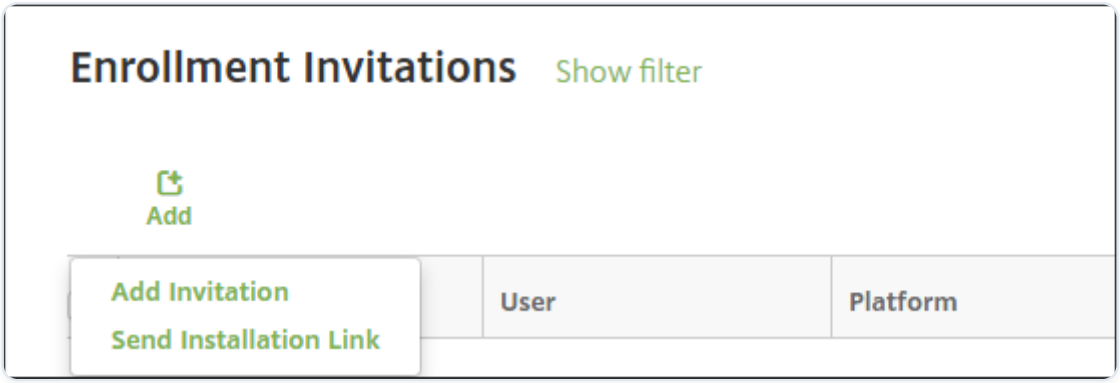
- 在企业 (XME) 或 MDM 模式下配置的 XenMobile Server
- 已配置 LDAP
- 如果使用本地组和本地用户：
  - 一个或多个本地组。
  - 分配给本地组的本地用户。
  - 交付组与本地组关联。
- 如果使用 Active Directory：
  - 交付组与 Active Directory 组关联。

创建注册邀请

1. 在 XenMobile 控制台中，单击**管理 > 注册邀请**。**注册邀请**页面显示。



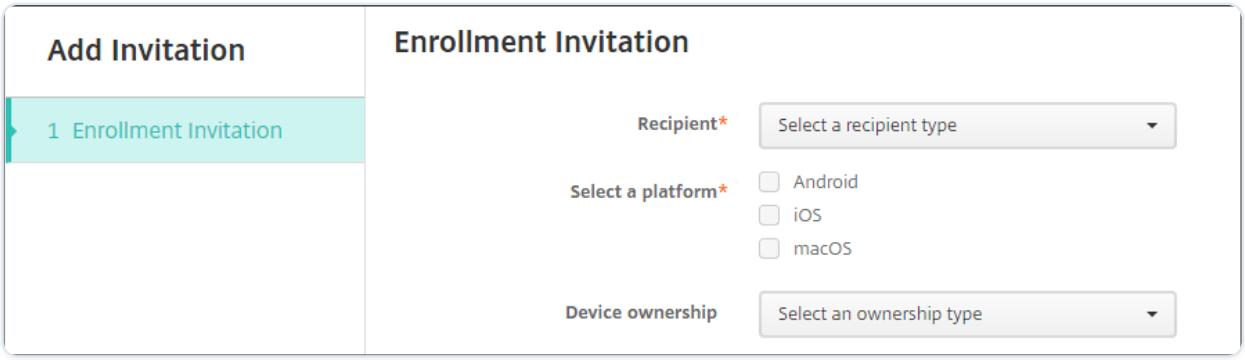
2. 单击**添加**。注册选项菜单显示。



- 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**。

发送注册邀请和安装链接将在这些步骤之后进行说明。

3. 单击**添加邀请**。**注册邀请**屏幕显示。



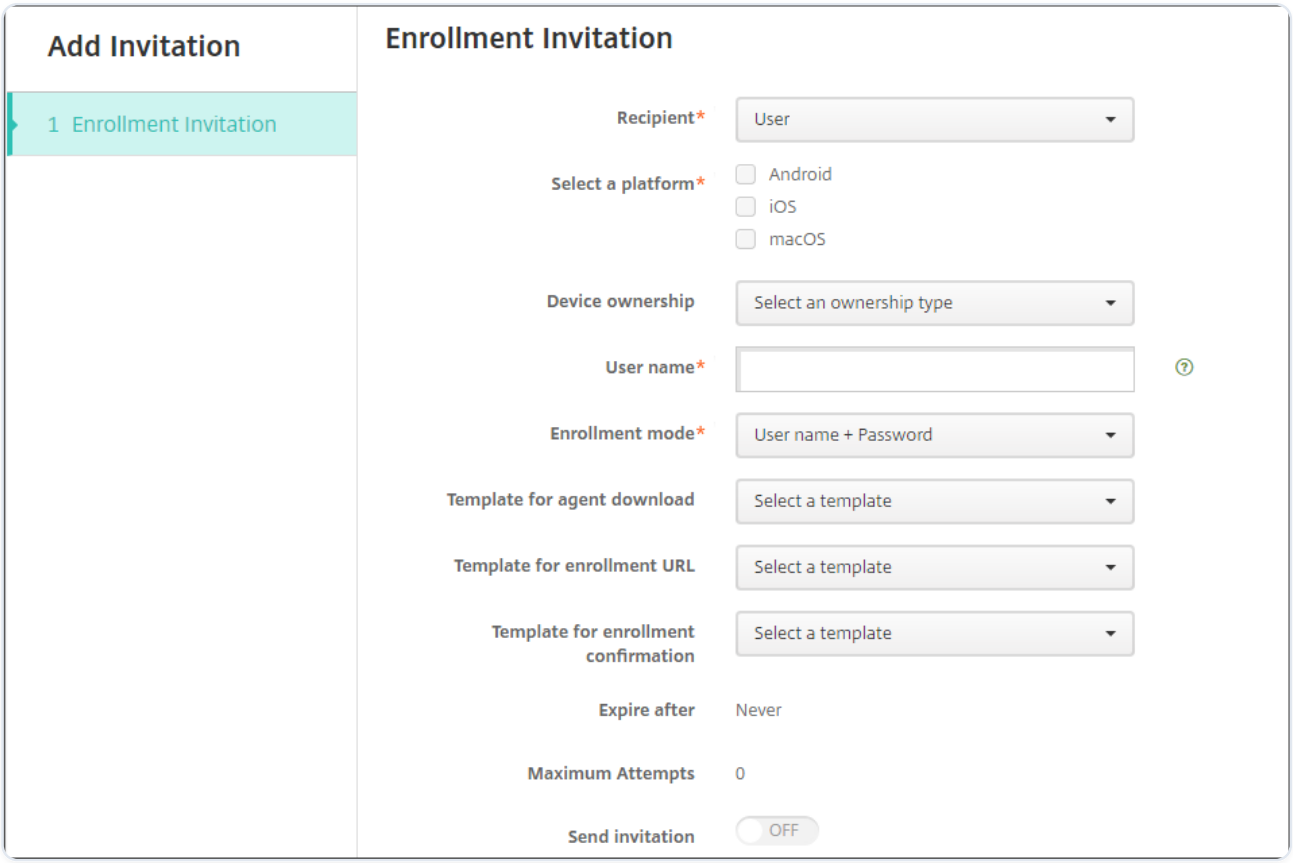
4. 配置以下设置：

- **收件人：选择组**或**用户**。
- **选择平台：如果收件人**是**组**，则选择所有平台。您可以更改平台选择。如果**收件人**是**用户**，则未选择任何平台。选择一个平台。

  要为 Android Enterprise 设备创建注册邀请，请选择 **Android > Android Enterprise**。
- **设备所有权：** 选择 **公司** 或 **员工**。

用户或组的设置将显示，如以下部分所述。

向用户发送注册邀请



1. 配置这些**用户**设置：

   - **用户名：** 键入用户名。该用户必须作为本地用户或 Active Directory 中的用户存在于 XenMobile Server 中。如果用户是本地用户，请确保已设置用户的电子邮件属性，以便您可以向该用户发送通知。如果用户在 Active Directory 中，请确保已配置 LDAP。
   - **设备信息：** 如果您选择多个平台或仅选择 macOS，则此设置不会显示。选择**序列号**、**UDID** 或 **IMEI**。选择一个选项后，将出现一个字段，您可以在其中键入设备的相应值。
   - **电话号码：** 如果您选择多个平台或仅选择 macOS，则此设置不会显示。可选地，键入用户的电话号码。
   - **运营商：** 如果您选择多个平台或仅选择 macOS，则此设置不会显示。选择一个运营商以与用户的电话号码关联。
   - **注册模式：** 为用户选择注册安全模式。默认值为**用户名 + 密码**。以下某些选项并非适用于所有平台：
     - 用户名 + 密码
     - 高安全性
     - 邀请 URL
     - 邀请 URL + PIN

- 邀请 URL + 密码
- 双因素
- 用户名 + PIN

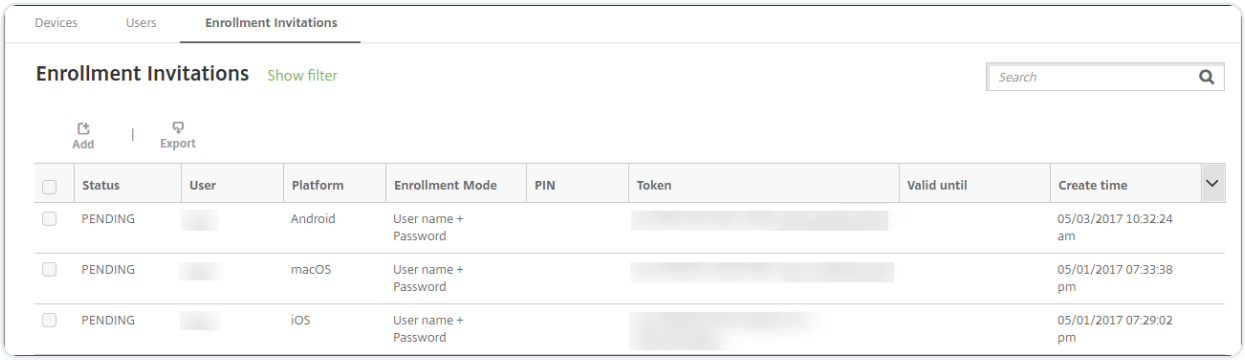
要发送注册邀请，您只能使用**邀请 URL**、**邀请 URL + PIN** 或**邀请 URL + 密码**注册安全模式。对于使用**用户名 + 密码**、**双因素**或**用户名 + PIN**注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

注册 PIN 也称为一次性 PIN。此类 PIN 仅在用户注册时有效。

> **注意：**
>
> 当您选择任何包含 PIN 的注册安全模式时，**注册 PIN 模板**字段将显示，您可以在其中单击**注册 PIN**。

- **代理下载模板：选择名为下载链接**的下载链接模板。该模板适用于所有受支持的平台。
- **注册 URL 模板：选择注册邀请**。
- **注册确认模板：选择注册确认**。
- **过期时间：**此字段在您配置注册模式时设置，并指示注册何时过期。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- **最大尝试次数：此字段在您配置注册模式**时设置，并指示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**可立即发送邀请。选择**关**可将邀请添加到**注册邀请**页面上的表中，但不发送。

2. 如果您启用了**发送邀请**，请单击**保存并发送**。否则，单击**保存**。邀请将显示在**注册邀请**页面上的表中。



向组发送注册邀请

下图显示了为组配置注册邀请的设置。

注册邀请到组页面的图像(/en-us/xenmobile/server/media/manage-enrollment-invitation-group.png)

1. 配置以下设置：

   - **域：**选择接收邀请的组的域。
   - **组：**选择接收邀请的组。
   - **注册模式：选择组中用户注册的方式。默认值为用户名 + 密码**。以下某些选项并非适用于所有平台：
     - 用户名 + 密码
     - 高安全性
     - 邀请 URL
     - 邀请 URL + PIN
     - 邀请 URL + 密码
     - 双因素
     - 用户名 + PIN

   要发送注册邀请，您只能使用**邀请 URL**、**邀请 URL + PIN**或**邀请 URL + 密码**注册安全模式。对于使用**用户名 + 密码**、**双因素**或**用户名 + PIN**注册的设备，用户必须在 Secure Hub 中手动输入其凭据。

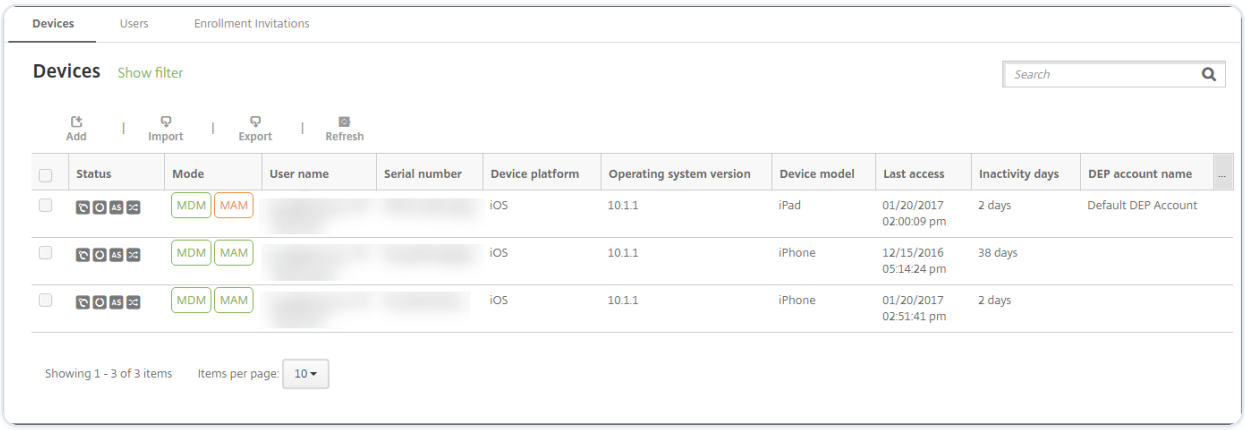
   仅显示对每个选定平台有效的注册安全模式。

   > **注意：**
   >
   > 当您选择任何包含 PIN 的注册安全模式时，将显示“**注册 PIN 模板**”字段，您可以在其中单击“**注册 PIN**”。

   - **代理下载模板：** 选择名为“**下载链接：**”的下载链接模板。该模板适用于所有受支持的平台。
   - **注册 URL 模板：** 选择“**注册邀请**”。
   - **注册确认模板：** 选择“**注册确认**”。
   - **过期时间：** 此字段在配置注册模式时设置，指示注册何时过期。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。

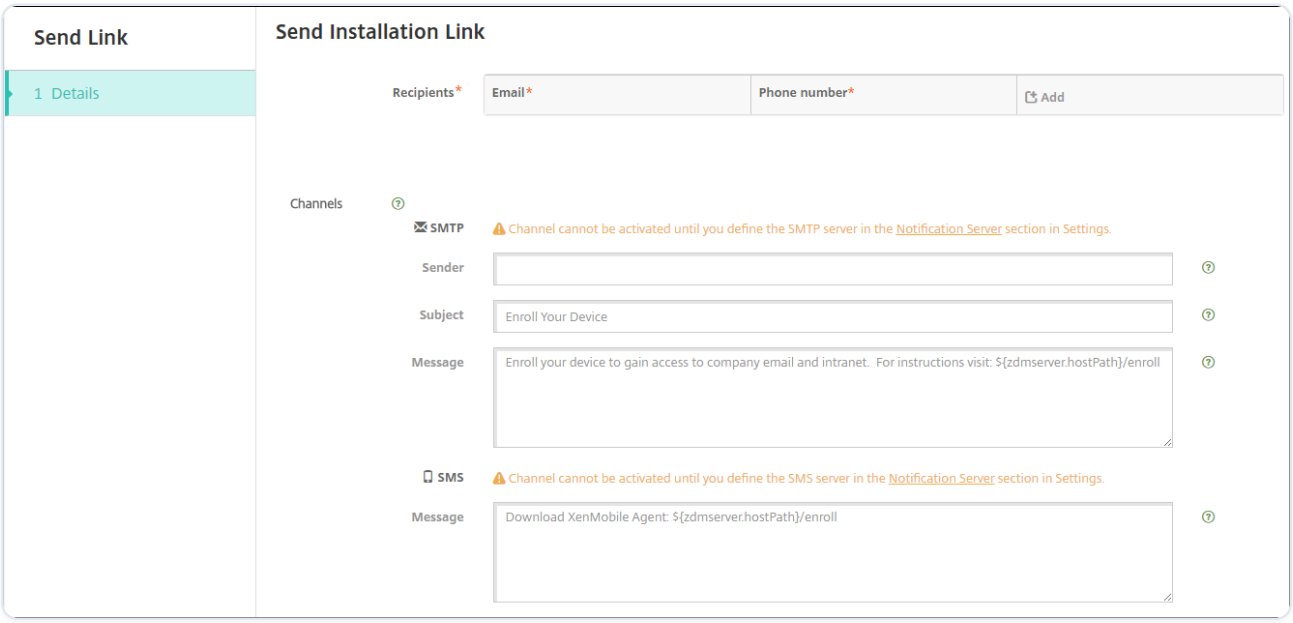
- **最大尝试次数：** 此字段在配置注册模式时设置，指示注册过程发生的最大次数。有关配置注册安全模式的详细信息，请参阅配置注册安全模式。
- **发送邀请：** 选择“**ON**”可立即发送邀请。选择“**OFF**”可将邀请添加到“**注册邀请**”页面上的表格中，但不发送。

2. 如果您启用了“**发送邀请**”，请单击“**保存并发送**”。否则，单击“**保存**”。邀请将显示在“**注册邀请**”页面上的表格中。



发送安装链接

在发送注册安装链接之前，您必须从“**设置**”页面在通知服务器上配置通道（SMTP 或 SMS）。有关详细信息，请参阅通知。



1. 配置这些设置，然后单击“**保存**”。

- **收件人：对于您要添加的每个收件人，单击添加**，然后执行以下操作：
  - **电子邮件：**键入收件人的电子邮件地址。此字段为必填项。

- **电话号码：**键入收件人的电话号码。此字段为必填项。

> **注意：**
>
> 要删除现有收件人，请将鼠标悬停在包含该条目的行上，然后单击右侧的垃圾桶图标。此时将显示确认对话框。单击**删除**以删除该条目，或单击**取消**以保留该条目。
>
> 要编辑现有收件人，请将鼠标悬停在包含该条目的行上，然后单击右侧的笔形图标。更新该条目，然后单击**保存**以保存更改的条目，或单击**取消**以保持该条目不变。

- **渠道：选择用于发送注册安装链接的渠道。您可以通过 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之前，无法激活这些渠道。有关详细信息，请参阅通知。
- **SMTP：**配置这些可选设置。如果您未在这些字段中键入任何内容，则将使用为所选平台配置的通知模板中指定的默认值：
  - **发件人：**键入可选发件人。
  - **主题：**键入邮件的可选主题。例如，“注册您的设备。”
  - **消息：**键入要发送给收件人的可选消息。例如，“注册您的设备以访问组织应用程序和电子邮件。”
- **SMS：**配置此设置。如果您未在此字段中键入任何内容，则将使用为所选平台配置的通知模板中指定的默认值：
  - **消息：**键入要发送给收件人的消息。此字段是基于 SMS 的通知所必需的。

> **注意：**在北美，超过 160 个字符的 SMS 消息将分多条消息发送。

2. 单击**发送**。

> **注意：**
>
> 如果您的环境使用 sAMAccountName：用户收到邀请并点击链接后，必须编辑用户名才能完成身份验证。用户名以 `sAMAccountName@domainname.com` 的形式显示。用户必须删除 @domainname.com 部分。

按平台划分的注册安全模式

下表显示了可用于注册用户设备的安全模式。在表中，**是** 表示哪些设备平台支持具有不同注册配置文件的特定注册和管理模式。

MDM 注册安全模式	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）	安卓企业版	IOS（用户注册模式）	IOS	MAC OS	视窗
通过 Citrix Cloud™ 的 Azure AD 和 Okta 作为身份提供程序	客户端证书	MDM+MAM 或 MDM	是	是	是	是	是	否	否
用户名 + 密码	LDAP、LDAP + 客户端证书和仅客户端证书	MDM+MAM、MDM 或 MAM（仅 MAM 模式不支持 Citrix Gateway	是	是	是	是	是	是	是

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）	安卓企业版	IOS（用户注册模式）	IOS	MAC OS	视窗
		上的客户端证书）							
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
双因素身份验证（用户名 + 密	LDAP、LDAP + 客户端证书以	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）	安卓企业版	IOS（用户注册模式）	IOS	MAC OS	视窗
码 + PIN）	及仅客户端证书								
用户名 + PIN	客户端证书	MDM +MAM 或 MDM	是	是	是	否	是	是	否

下文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）
  - 向用户发送包含注册 URL 的单个通知。当用户单击该 URL 时，Secure Hub 将打开。然后，用户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。当用户单击该 URL 时，Secure Hub 将打开。XenMobile Server 名称和**是，注册**按钮将显示。用户点击**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：
    - 一封包含注册 URL 的电子邮件，用户可以通过该 URL 经由 Secure Hub 在 XenMobile 中注册设备。
    - 一封包含一次性 PIN 的电子邮件，用户在注册设备时必须输入该 PIN 以及用户的 Active Directory（或本地）密码。

  - 在此模式下，用户只能通过通知中的注册 URL 进行注册。如果用户丢失了通知邀请，则无法注册。但是，您可以发送另一个邀请。

- **邀请 URL + 密码**
  - 向用户发送一个包含注册 URL 的通知。当用户单击该 URL 时，Secure Hub 将打开。XenMobile Server 名称将显示，并带有一个允许用户输入密码的字段。

- **双因素**
  - 向用户发送一个包含注册 URL 和一次性 PIN 的通知。当用户单击该 URL 时，Secure Hub 将打开。XenMobile Server 名称将显示，并带有两个允许用户输入密码和 PIN 码的字段。

- **用户名 + PIN**
  - 向用户发送以下电子邮件：
    - 一封包含注册 URL 的电子邮件，用户可以通过该 URL 下载并安装 Secure Hub。Secure Hub 打开后，系统会提示用户输入用户名和密码以在 XenMobile 中注册设备。
    - 一封包含一次性 PIN 的电子邮件，用户在注册设备时必须输入该 PIN 以及用户的 Active Directory（或本地）密码。
  - 如果用户丢失了通知邀请，则无法注册。但是，您可以发送另一个邀请。

以下描述了注册安全模式在 macOS 设备上的行为方式：

- **用户名 + 密码**
  - 向用户发送包含注册 URL 的单个通知。当用户点击该 URL 时，Safari 浏览器会打开。此时会显示一个登录页面，提示用户输入用户名和密码以将设备注册到 XenMobile。

- **双因素**
  - 向用户发送包含注册 URL 和一次性 PIN 的单个通知。当用户点击该 URL 时，Safari 浏览器会打开。此时会显示一个登录页面，其中包含两个字段，供用户输入密码和 PIN 码。

- **用户名 + PIN**
  - 向用户发送以下电子邮件：
    - 一封包含注册 URL 的电子邮件。当用户点击该 URL 时，Safari 浏览器会打开。此时会显示一个登录页面，提示用户输入用户名和密码以将设备注册到 XenMobile。
    - 一封包含一次性 PIN 的电子邮件，用户在注册设备时必须输入该 PIN，以及用户的 Active Directory（或本地）密码。

- 如果用户丢失了通知邀请，则无法注册。但是，您可以发送另一个邀请。

您无法向 Windows 设备发送注册邀请。Windows 用户直接通过其设备进行注册。

Firebase 云消息传递

> **注意：**

> Firebase Cloud Messaging (FCM) 以前称为 Google Cloud Messaging (GCM)。某些 XenMobile® 控制台标签和消息使用 GCM 术语。

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

完成本文中的配置步骤并且设备签入后，设备会在 XenMobile Server 中向 FCM 服务注册。该连接通过使用 FCM 实现了从 XenMobile Service 到设备的近实时通信。FCM 注册适用于新设备注册和以前注册的设备。

当 XenMobile 需要启动与设备的连接时，它会连接到 FCM 服务。然后，FCM 服务会通知设备进行连接。这种连接类型类似于 Apple 用于其推送通知服务的方式。

必备条件

- 最新 Secure Hub 客户端
- Google 开发者帐户凭据
- 在已启用 FCM 的 Android 设备上安装 Google Play 服务

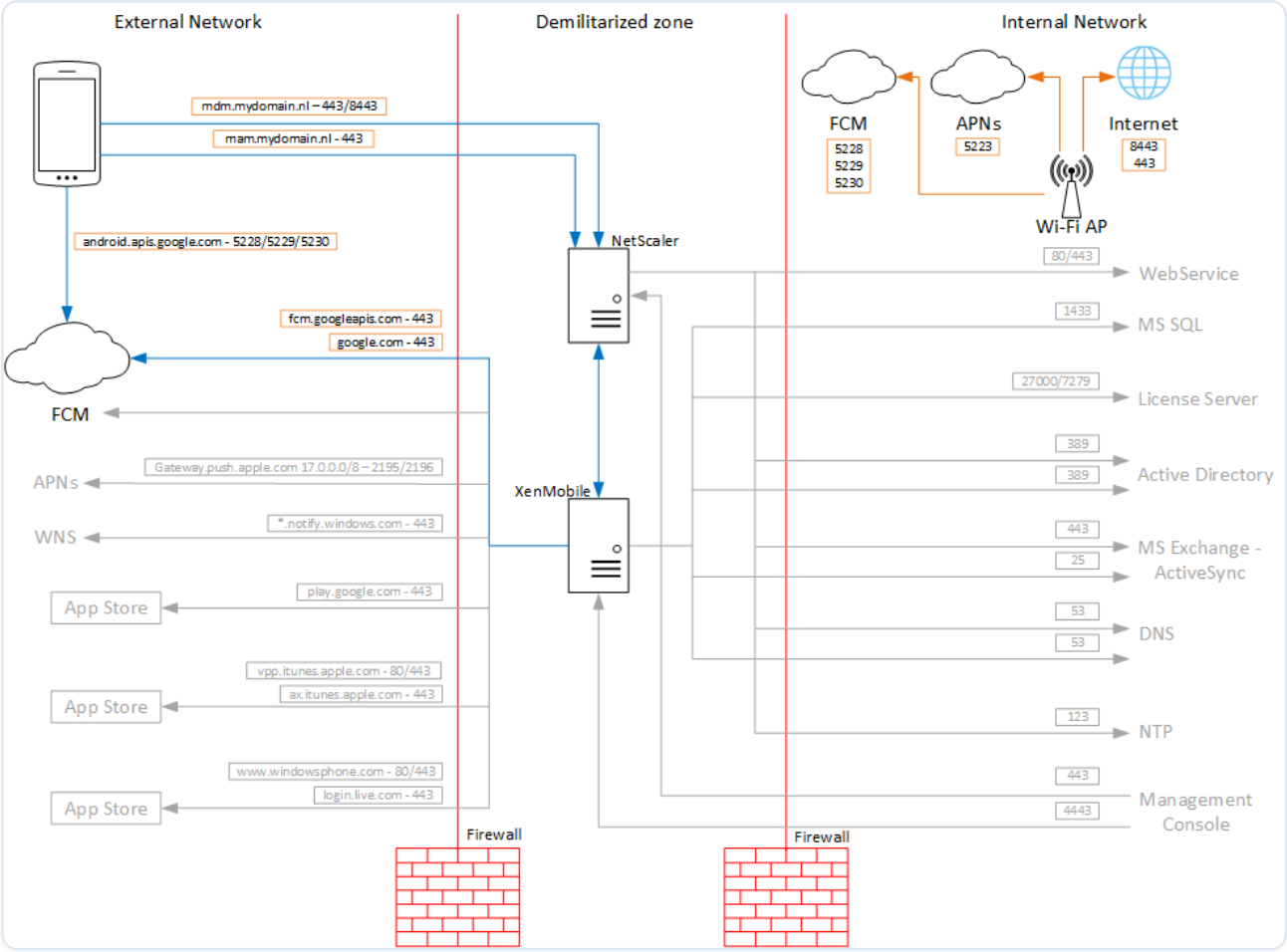
防火墙端口

- 在 XenMobile 上打开端口 443 以连接到 `fcm.googleapis.com` 和 `Google.com`。
- 为设备 Wi-Fi 打开端口 5228、5229 和 5230 上的出站 Internet 通信。
- 为了允许出站连接，FCM 建议允许端口 5228 到 5230，且不带 IP 限制。但是，如果需要 IP 限制，FCM 建议允许 IPv4 和 IPv6 块中的所有 IP 地址。这些块列在 Google ASN of 15169 中。每月更新该列表。有关 FCM 端口的更多信息，请参阅 Google 文档中的 FCM 端口。

有关详细信息，请参阅 端口要求。

架构

此图显示了 FCM 在外部和内部网络中的通信流。

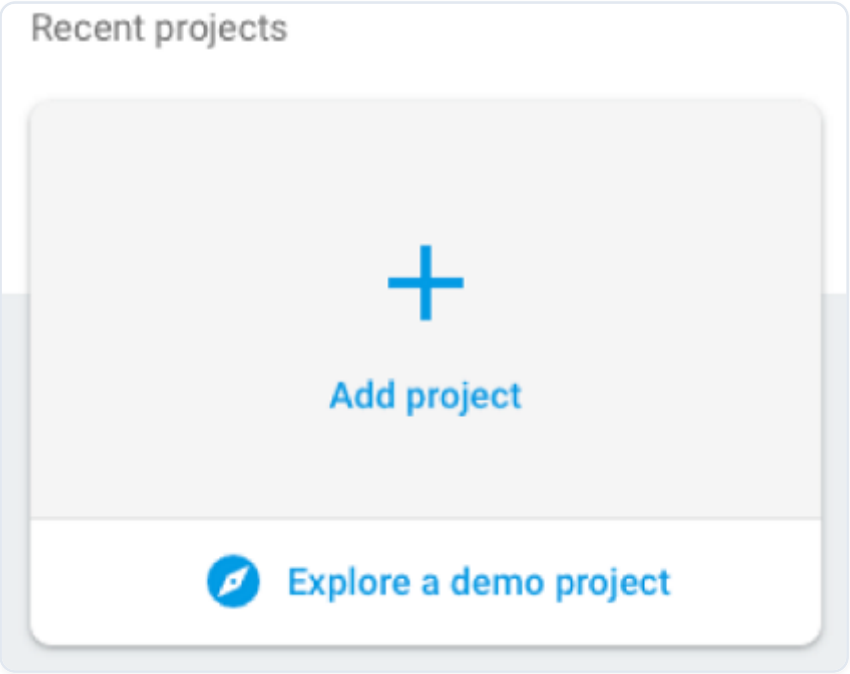


为 FCM 配置您的 Google 帐户

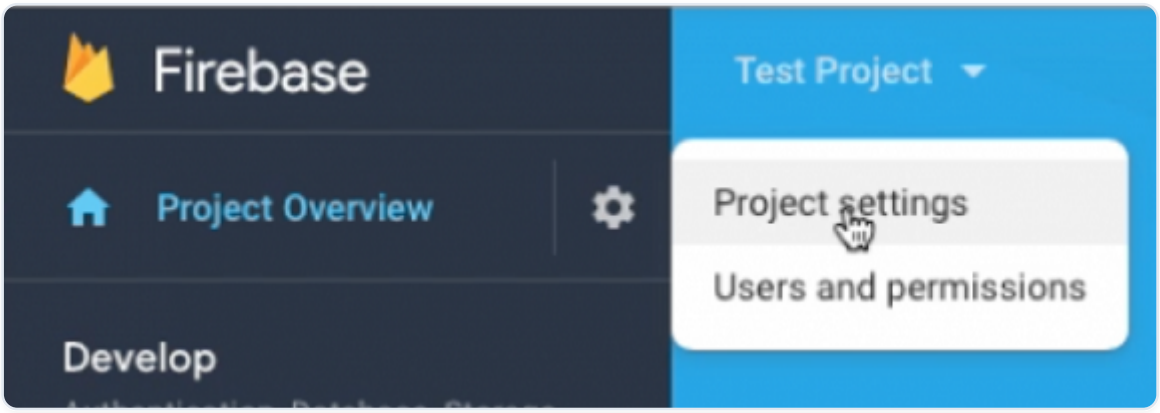
1. 使用您的 Google 开发者帐户凭据登录以下 URL：

   `<https://console.firebase.google.com/>`

2. 单击“**添加项目**”。



3. 创建项目后，单击“**项目设置**”。

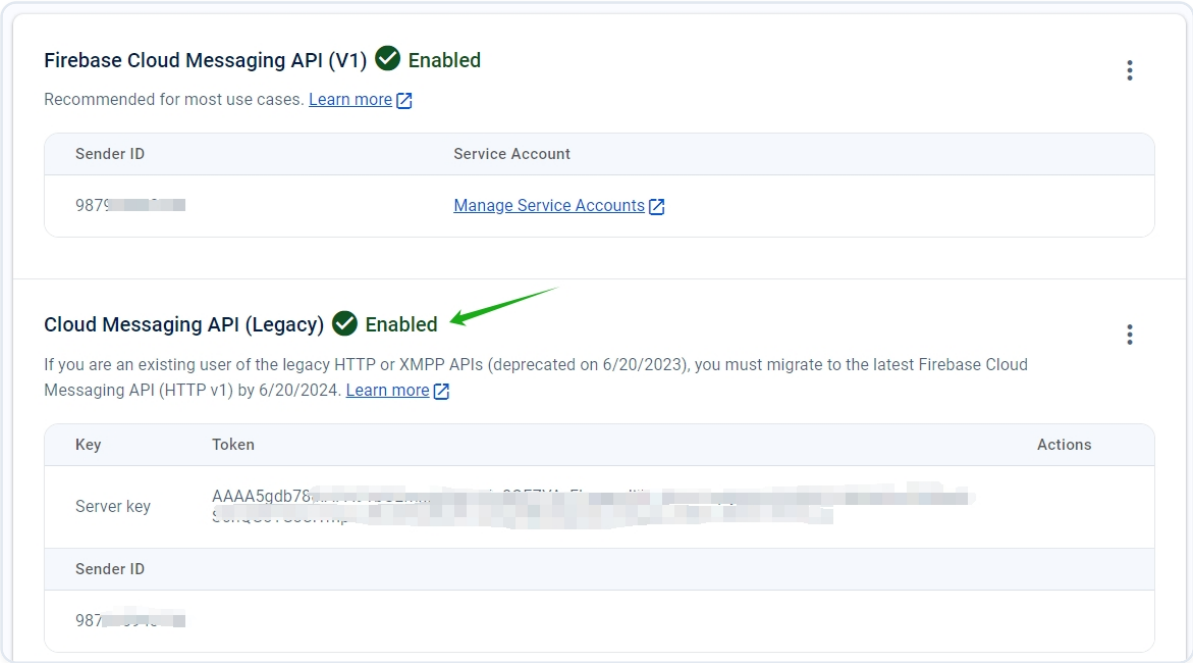


注意：

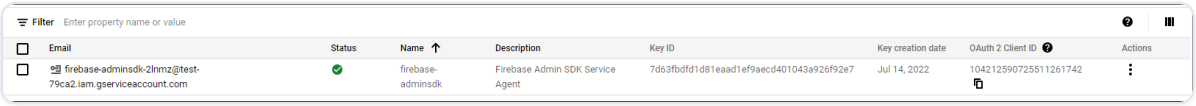
Google 将弃用用于 HTTP 的 FCM 旧版 API，该 API 目前在我们的 FCM 实现中使用。迁移截止日期为 June 21, 2024。我们需要将 FCM 从旧版 FCM API 迁移到 HTTP v1 API。有关详细信息，请参阅从旧版 FCM API 迁移到 HTTP v1。

4. 单击“**云消息传递**”选项卡。验证 Firebase Cloud Messaging API 已启用，然后单击“**管理服务帐户**”。

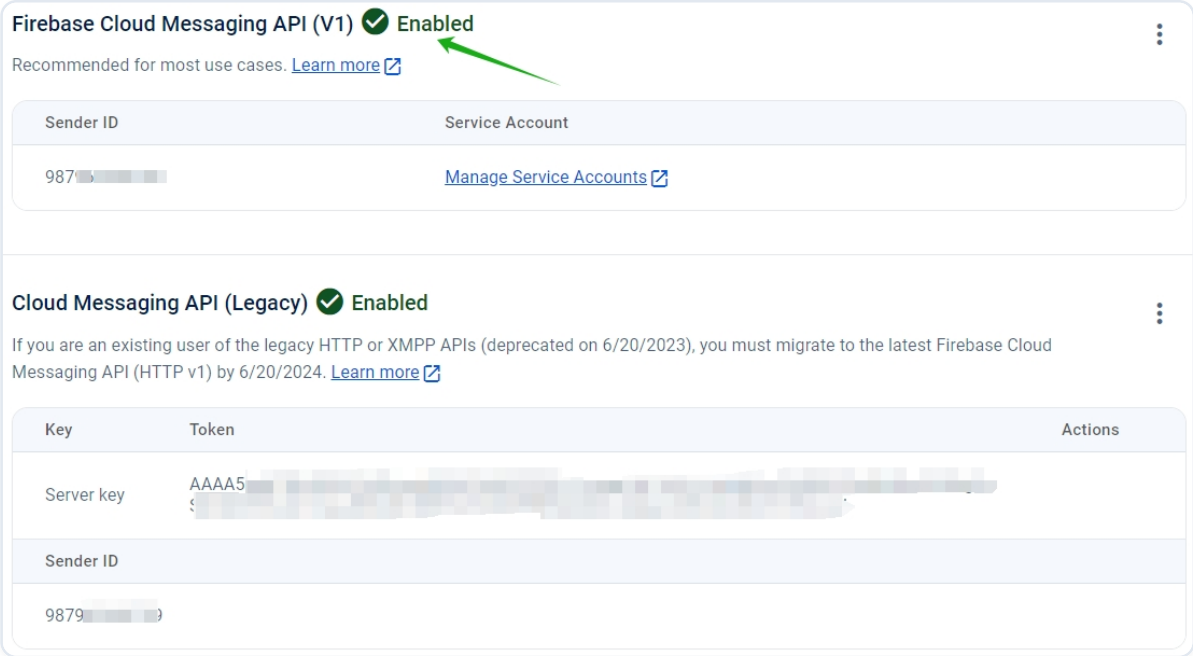
   a. 迁移之前，您可以使用旧版 API，确保已启用 Cloud Messaging API（旧版）。复制“**密钥**”和“**发件人 ID**”字段中的值。



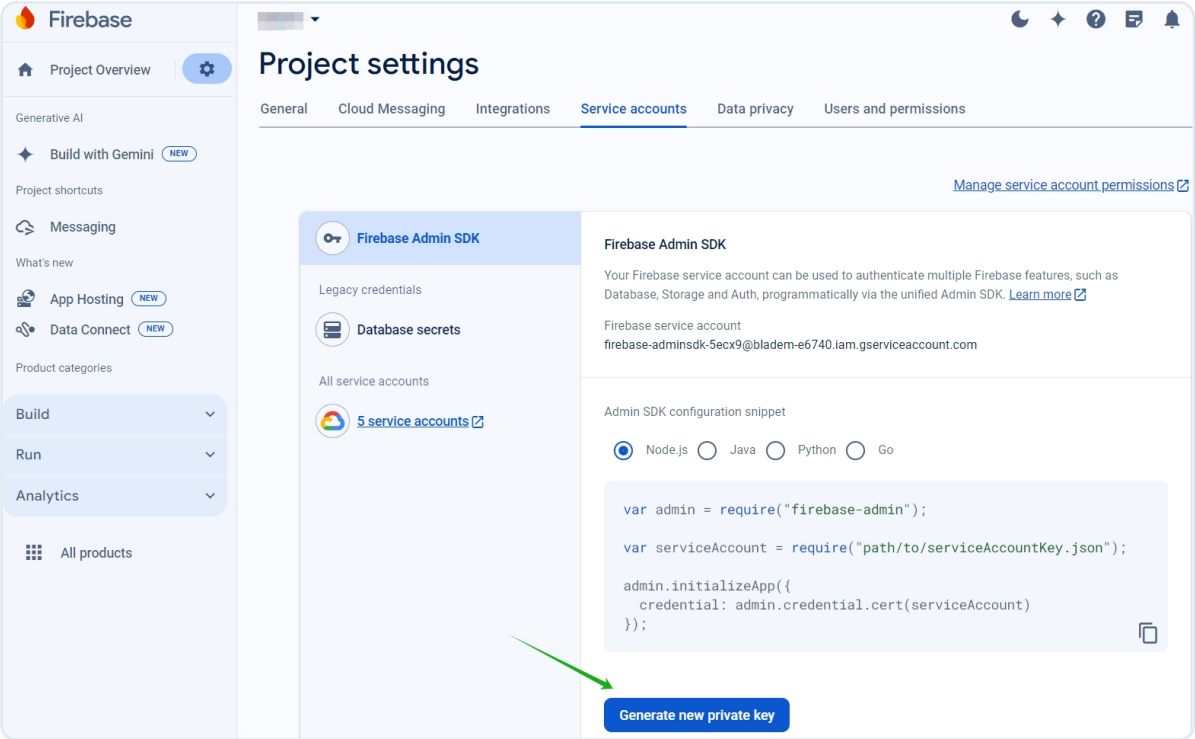
如果您没有列出的密钥，请点击**操作**下的省略号以添加密钥。



b. 迁移后，旧版 API 已从 Google 弃用。您必须启用 Firebase Cloud Messaging API(V1)。有关更多信息，请参阅从旧版 FCM API 迁移到 HTTP v1。



从**项目设置**下的**服务帐户**下载服务帐户 JSON 文件。请参阅手动提供凭据部分，为您的服务帐户生成私钥文件。点击**生成新私钥**以下载服务帐户密钥 JSON 文件。



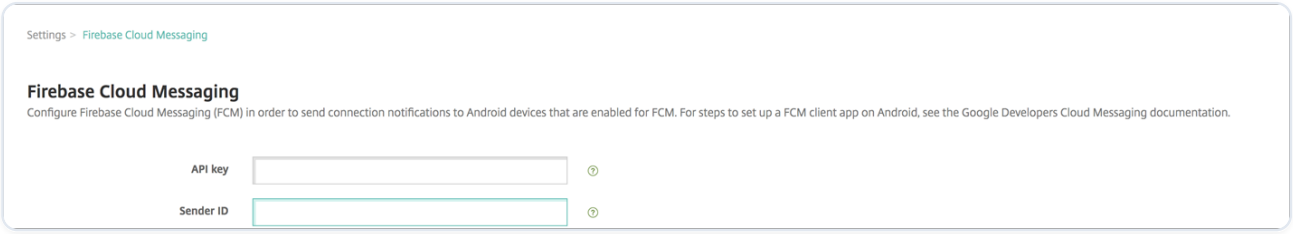
有关在 Android 上设置 FCM 客户端应用程序的步骤，请参阅此 Google Developers Cloud Messaging 文章：`<https://firebase.google.com/docs/cloud-messaging/android/client>`。

配置 XenMobile 以使用 FCM

在 XenMobile 控制台中，转到**设置 > Firebase Cloud Messaging**。

对于 Cloud Messaging API（旧版）

1. 在**API 密钥**字段中输入 Firebase Cloud Messaging 配置最后一步中的 Firebase Cloud Messaging **密钥**。
2. 输入上一步骤中的**发件人 ID** 值。

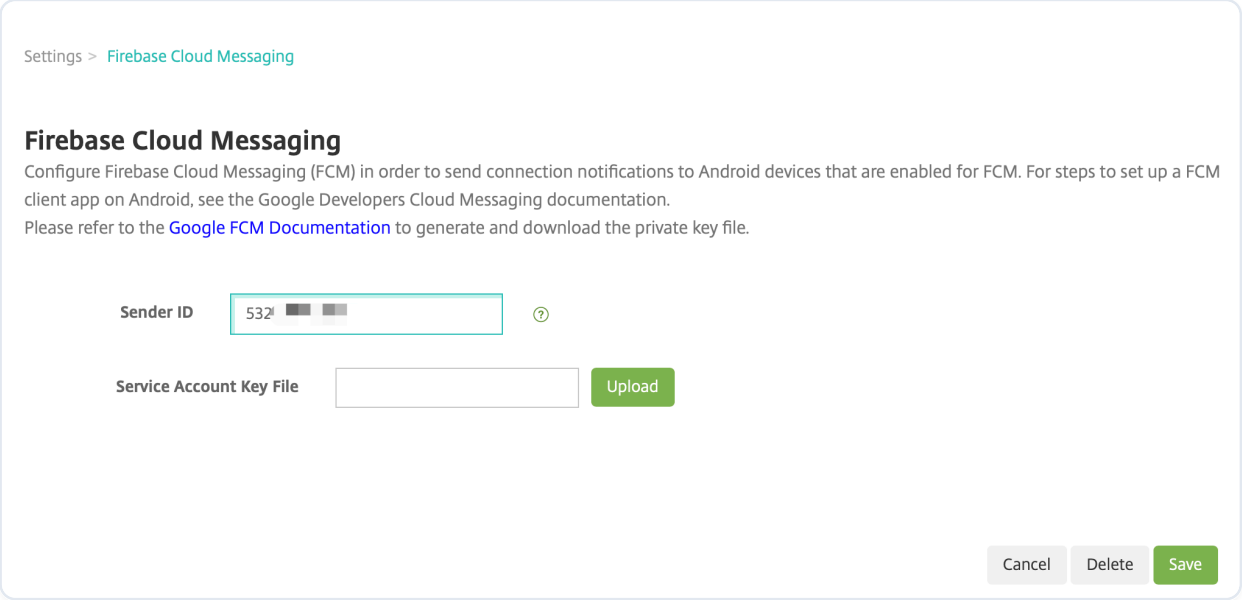


对于 Firebase 云消息传递 API (V1)

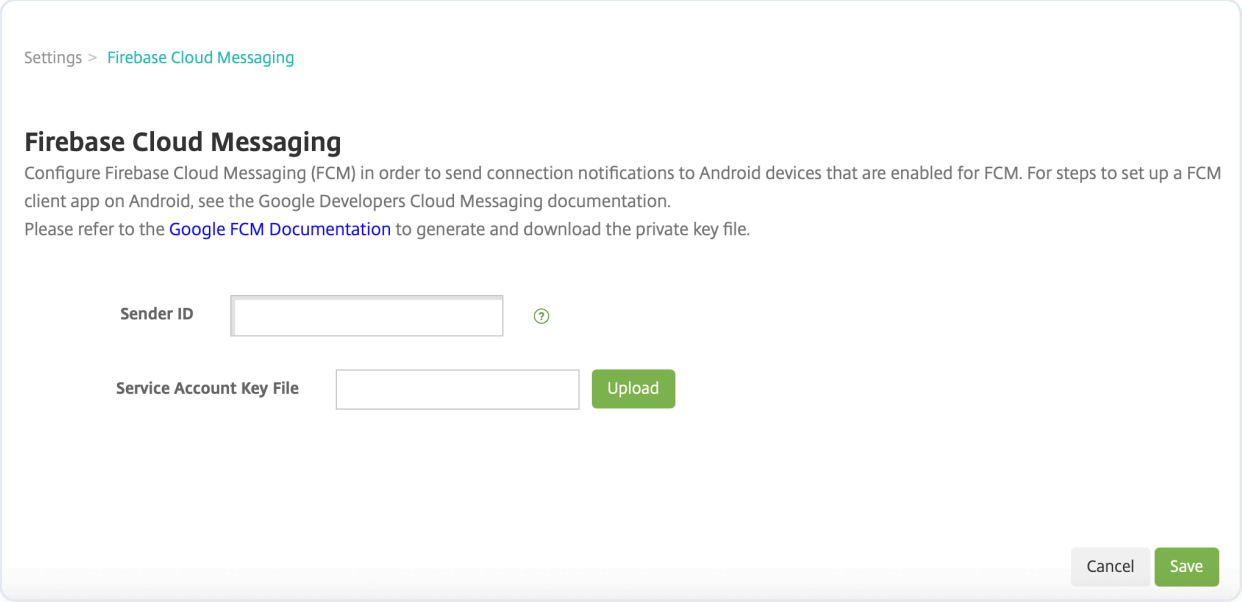
> **注意：**

- 要为 XenMobile Server 10.15 滚动修补程序 7 及更高版本启用 FCM API V1，请参阅知识中心文章 CTX677031。
- 如果您是新的 FCM 用户，请跳过步骤 1，从步骤 2 开始。

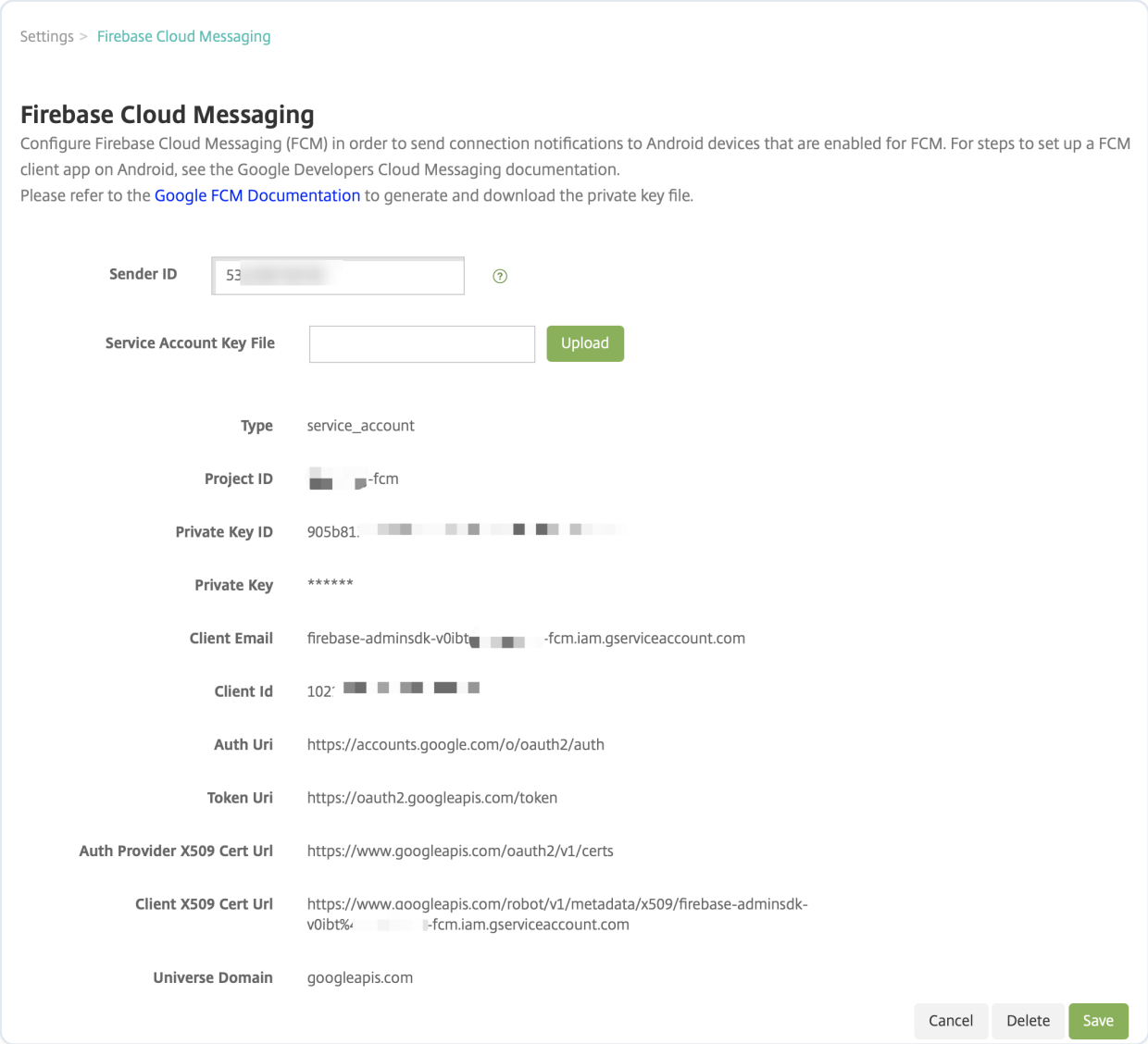
1. 如果您已在使用 FCM，您会注意到“发件人 ID”已自动填充您当前的 FCM 项目，并且新增了一个用于上传“**服务帐户密钥文件**”的选项。



2. 如果您是新的 FCM 用户，请输入“**发件人 ID**”并上传上一个步骤中的“**服务帐户密钥文件**”。



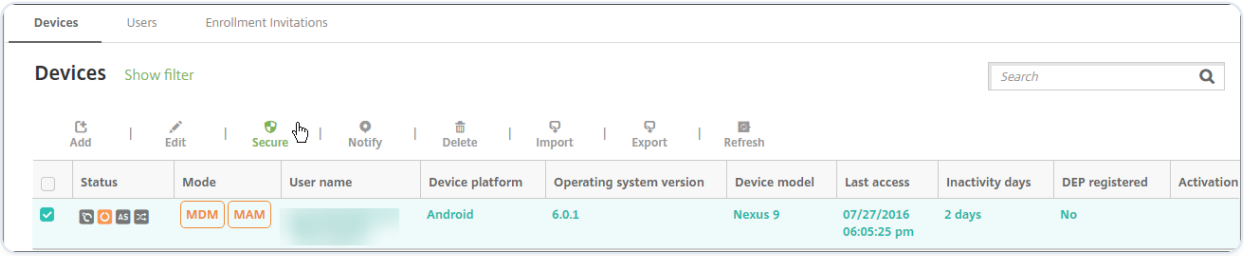
3. 上传的文件将被解析，并且相应的字段将自动生成。



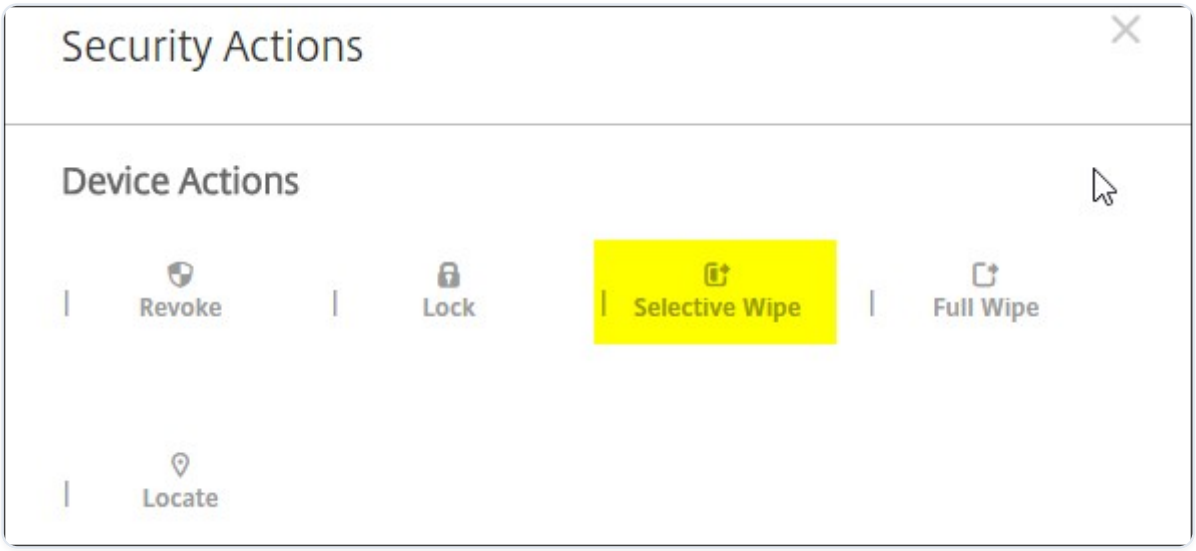
4. 验证信息，然后单击“**保存**”。

测试您的配置

1. 注册 Android 设备。
2. 让设备闲置一段时间，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“**保护**”。



4. 在“**设备操作**”下，单击“**选择性擦除**”。



如果配置成功，将在设备上执行选择性擦除。

与 Apple 教育功能集成

您可以使用 XenMobile® 作为您的移动设备管理 (MDM) 解决方案，在采用 Apple 教育的环境中。XenMobile 支持包括 Apple School Manager (ASM) 和适用于 iPad 的课堂应用。XenMobile 教育配置设备策略配置教师和学生设备以与 Apple 教育配合使用。

您向教师和学生提供预配置和受监管的 iPad。该配置包括 XenMobile 中的 ASM 注册、使用新密码配置的 Managed Apple ID 帐户以及所需的批量购买应用和 iBooks。

以下是 XenMobile 对 Apple 教育功能的支持亮点。

Apple 校园教务管理

ASM 是一项服务，可让您设置、部署和管理教育机构中使用的 iOS (iPadOS) 设备和 macOS 笔记本电脑。ASM 包括一个基于 Web 的门户，IT 管理员可以通过该门户执行以下操作：

- 将 Apple 部署计划设备分配到不同的 MDM 服务器。
- 购买用于应用和 iBooks 的批量许可证
- 批量创建 **Managed Apple ID**。这些自定义的 Apple ID 提供对 Apple 服务的访问权限，例如在 iCloud Drive 中存储文档以及注册 Apple App Store 课程。

您可以向 XenMobile 添加多个 ASM 帐户。例如，此功能使您能够按教育单位或部门使用不同的注册设置和设置助理选项。然后，您将 ASM 帐户与不同的设备策略关联。

将 ASM 帐户添加到 XenMobile 控制台后，XenMobile 会检索班级和名册信息。在设备设置期间，XenMobile 会执行以下操作：

- 注册设备。

- 安装您配置用于部署的资源，例如设备策略（教育配置、主屏幕布局等）。
- 还会安装通过批量购买的应用和 iBooks。

然后，您将预配置的设备提供给教师和学生。如果设备丢失或被盗，您可以使用 MDM 丢失模式功能锁定并定位设备。

适用于 iPad 的课堂应用

适用于 iPad 的课堂应用使教师能够连接和管理学生设备。您可以查看设备屏幕、在 iPad 上打开应用以及共享和打开网页链接。

课堂应用在 App Store 中免费提供。您可以将该应用上传到 XenMobile 控制台。然后，您可以使用教育配置设备策略来配置课堂应用，并将其部署到教师设备。

有关 Apple 教育功能的更多信息，请参阅 Apple 教育 网站以及同一网站上的 Apple 教育部署指南。

先决条件

- 思杰网关
- 为 MDM+MAM 配置的注册配置文件。
- Apple iPad 第三代（最低版本）或 iPad Mini，运行 iOS 9.3（最低版本）

> **注意：**

> XenMobile 不会根据 LDAP 或 Active Directory 验证 ASM 用户帐户。但是，您可以将 XenMobile 连接到 LDAP 或 Active Directory，以管理与 ASM 教师或学生无关的用户和设备。例如，您可以使用 Active Directory 向其他 ASM 成员（例如 IT 管理员和经理）提供 Secure Mail 和 Secure Web。

> 由于 ASM 教师和学生是本地用户，因此无需将 Citrix Secure Hub™ 部署到他们的设备。

> 包含 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所需的批量购买应用和 iBooks。

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：请遵循本节中的工作流程来设置您的 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。

请按照以下说明操作，为以一对一模式（每个学生一个 iPad）使用的任何 iPad 或教师 iPad（非共享）配置集成。要配置共享 iPad，请参阅 配置共享 iPad。

步骤 1: 创建您的 Apple School Manager 帐户并完成设置助理

如果您计划从 Apple Deployment Program 升级，请参阅 Apple 支持文章 将您的机构升级到 ASM。要创建您的 ASM 帐户，请访问 `<https://school.apple.com/>` 并按照说明进行注册。首次登录 ASM 时，设置助理将打开。

- 有关 ASM 先决条件、设置助理和管理任务的信息，请参阅 Apple School Manager 用户指南。
- 设置 ASM 时，请使用与 Active Directory 域名不同的域名。例如，为 ASM 域名添加类似 `appleid` 的前缀。
- 将 ASM 连接到您的名册数据时，ASM 会为教师和学生创建托管式 Apple ID。您的名册数据包括教师、学生和班级。有关将名册数据添加到 ASM 的信息，请参阅前面提到的 ASM 用户指南。
- 您可以为您的机构自定义托管式 Apple ID 格式，如前面提到的 ASM 用户指南中所述。

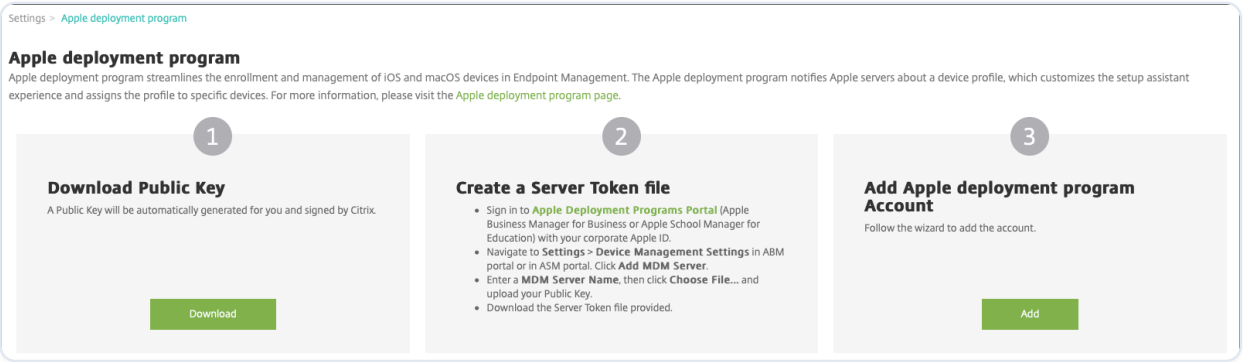
> **重要提示：**
>
> 导入 ASM 信息到 XenMobile 后，请勿更改托管式 Apple ID。

- 如果您通过经销商或运营商购买了设备，请将这些设备链接到 ASM。有关信息，请参阅前面提到的 ASM 用户指南。

步骤 2: 将 XenMobile 配置为 Apple School Manager 的 MDM 服务器并配置设备分配

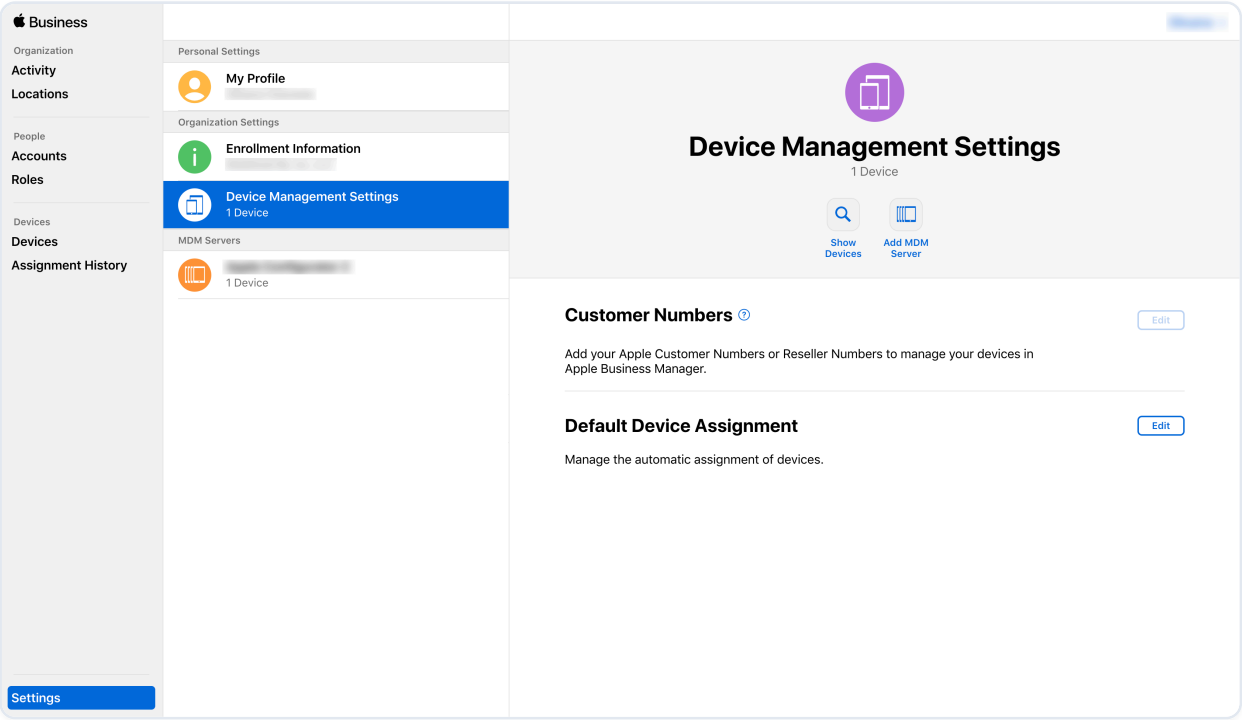
ASM 门户包含一个“**MDM 服务器**”选项卡。您需要 XenMobile 中的公钥文件才能完成该设置。

1. 将 XenMobile 的公钥下载到本地计算机：在 XenMobile 控制台中，转到“**设置 > Apple Deployment Program**”。

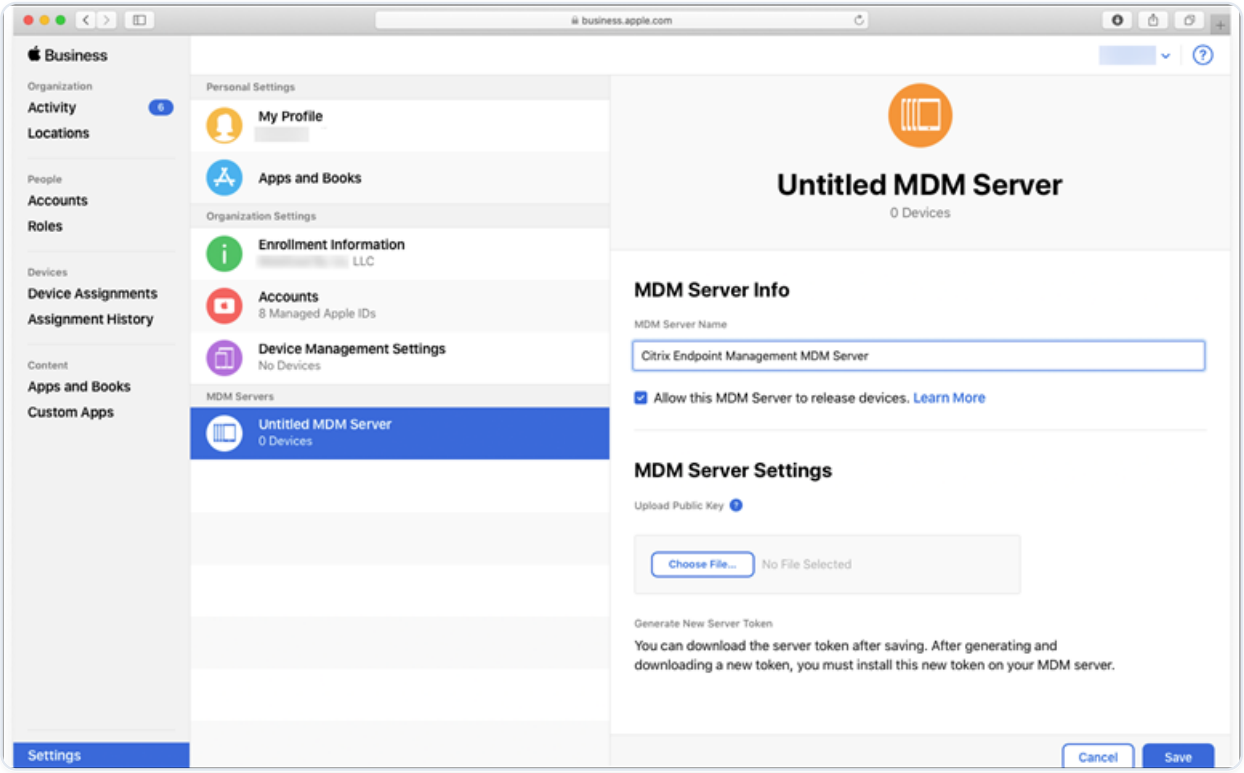


2. 在“**下载公钥**”下，单击“**下载**”，然后保存 PEM 文件。

3. 在 **Apple School Manager** 门户中，单击“**设置**”，然后单击“**设备管理设置**”。单击“**添加 MDM 服务器**”。

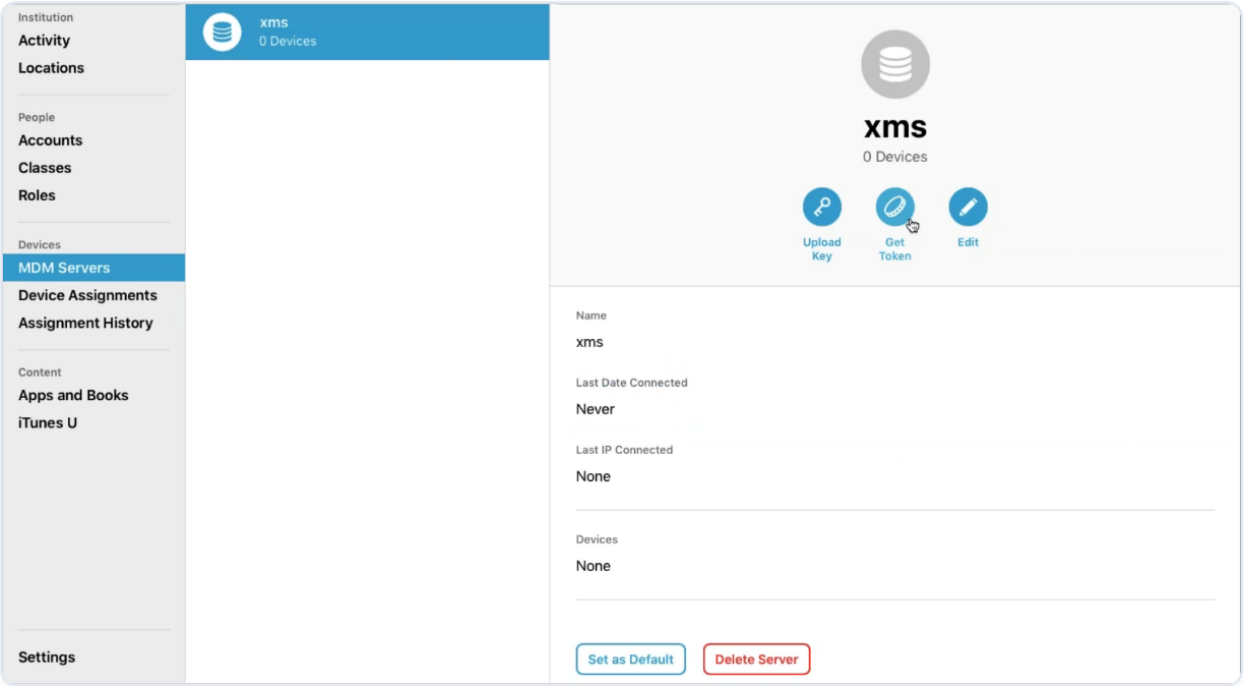


4. 为 XenMobile 键入一个名称。您键入的服务器名称仅供参考，并非服务器 URL 或名称。在“**上传公钥**”下，单击“**选择文件**”。



5. 上传从 XenMobile 下载的公钥，然后单击“**保存**”。

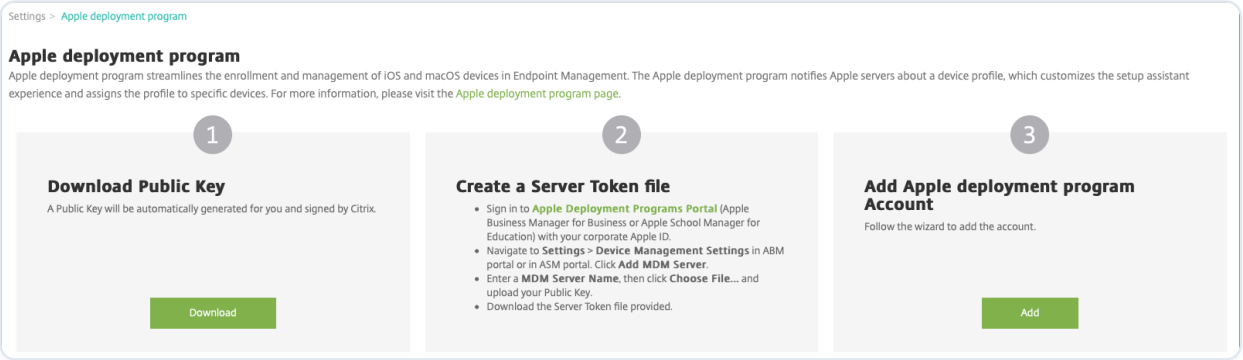
6. 生成服务器令牌：单击“**下载令牌**”将服务器令牌文件下载到您的计算机。



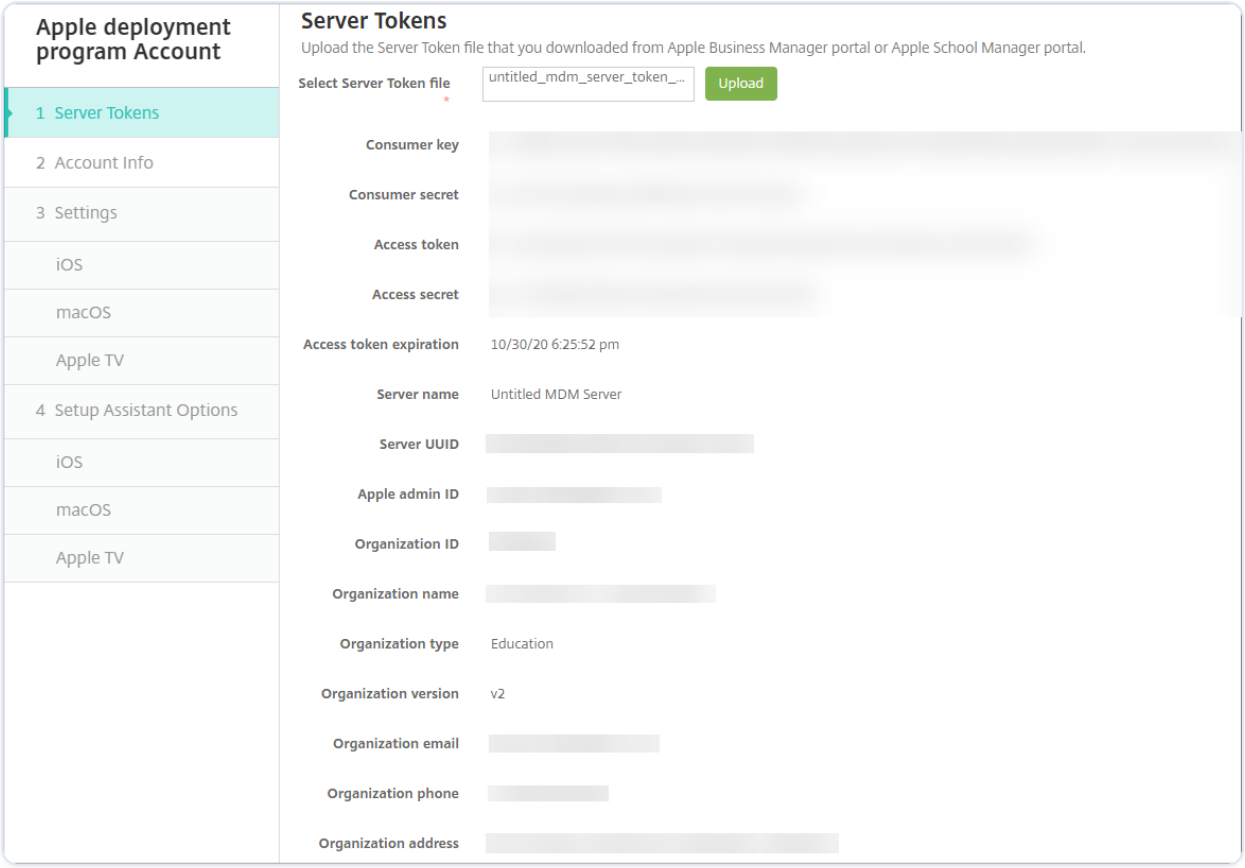
7. 在“**默认设备分配**”下，单击“**更改**”。选择您希望如何分配设备，然后提供所请求的信息。有关信息，请参阅 ASM 用户指南。

步骤 3：将 Apple School Manager 帐户添加到 XenMobile

1. 在 XenMobile 控制台中，转至“**设置 > Apple 部署计划**”并在“**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“**上传**”并选择从 ASM 门户下载的服务器令牌（P7M 文件）。令牌信息随即显示。



备注：

- **组织 ID** 是您在 Apple 部署计划中的客户 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 Deployment Program 设置屏幕(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-3.png)

- **Apple Deployment Program 帐户名称：** 此 Apple Deployment Program 帐户的唯一名称。使用能够反映您组织 Apple Deployment Program 帐户的方式的名称，例如按国家/地区或组织层次结构。
- **业务/教育单位：** 用于设备分配的教育单位或部门。此字段为必填项。
- **唯一服务 ID：** 一个可选的唯一 ID，可帮助您进一步识别帐户。
- **支持电话号码：** 用户在设置期间可以致电寻求帮助的支持电话号码。此字段为必填项。
- **支持电子邮件地址：** 供最终用户使用的可选支持电子邮件地址。
- **教育后缀：** 标记给定 ASM Deployment Program 帐户的类别。（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 ASM Deployment Program 和 ASM 批量购买这两个帐户使用相同的后缀。

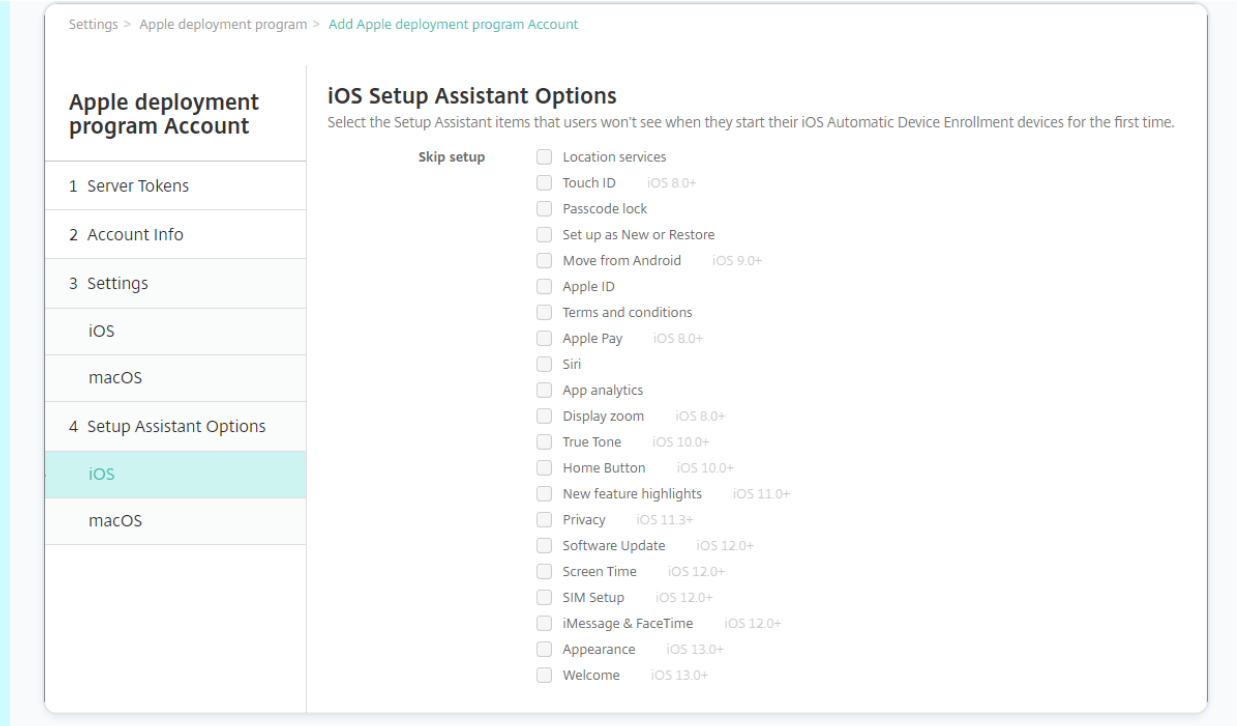
4. 单击“**下一步**”。在“**iOS 设置**”中，指定以下设置。

   Apple 设置屏幕(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-4.png)

   - **注册设置**
     - **要求设备注册：** 要求用户注册其设备。将此设置更改为“**否**”。
     - **要求设备注册凭据：** 要求用户在 Apple Deployment Program 设置期间输入其凭据。对于 ASM 与 XenMobile 的集成，此设置默认为“**是**”，且无法更改。Apple Deployment Program 要求设备注册凭据。
     - **等待配置完成设置：** 是否要求用户设备保持在“设置助理”模式，直到所有 MDM 资源部署到设备。对于 ASM 与 XenMobile 的集成，此设置默认为“**否**”。根据 Apple 文档，在设备处于“设置助理”模式时，以下命令可能不起作用：
       - InviteToProgram
       - 安装应用程序
       - 安装媒体
       - 应用兑换码
   - **设备设置**
     - **监管模式：** 将 iOS 设备置于监管模式。不要更改默认的“**是**”。有关将 iOS 设备置于监管模式的详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于监管模式。
     - **共享模式：** 在 iPad 上启用共享模式。不符合最低要求的设备无法共享。
     - **允许移除注册配置文件：** 对于 ASM 集成，允许用户从设备中移除注册配置文件。将此设置更改为“**是**”。
     - **允许设备配对：** 对于 ASM 集成，允许设备配对，以便您可以通过 Apple App Store 和 Apple Configurator 管理它们。将此设置更改为“**是**”。

5. 在“**iOS 设置助理选项**”中，选择用户首次启动设备时要跳过的 iOS 设置助理步骤。默认情况下，设置助理包含所有步骤。请注意，从设置助理中移除步骤可以简化用户体验。

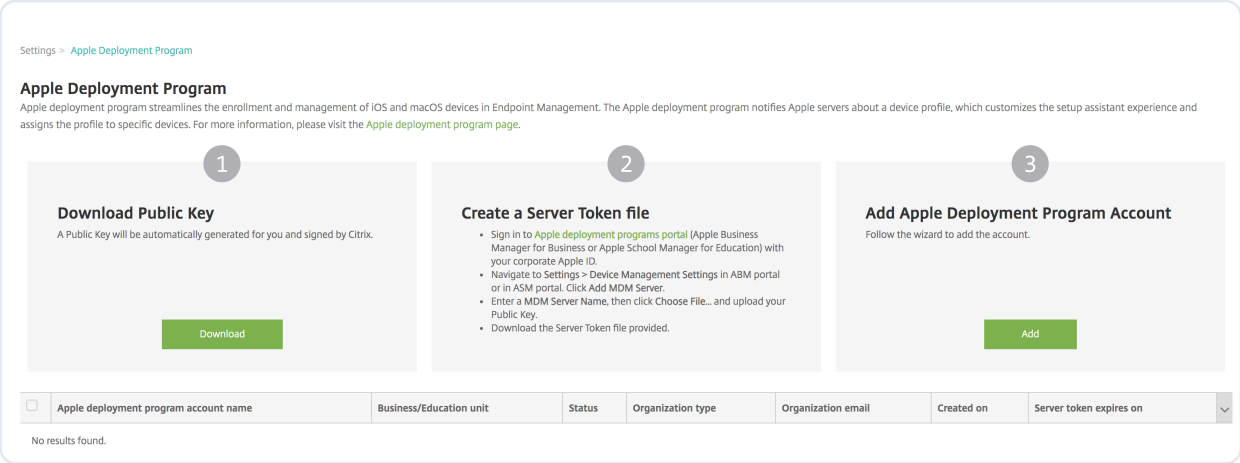
   > **重要提示：**
   >
   > Citrix 强烈建议您包含“**Apple ID**”和“**条款与条件**”步骤。这些步骤使教师和学生能够提供他们新的托管 Apple ID 密码并接受所需的条款和条件。



- **定位服务：** 在设备上设置定位服务。
- **触控 ID：** 在 iOS 设备上设置触控 ID。
- **密码锁定：** 为设备创建密码。
- **设置为新设备或恢复：** 将设备设置为新设备，或从 iCloud 或 Apple App Store 备份恢复。
- **从 Android 迁移：** 启用将数据从 Android 设备传输到 iOS 设备。此选项仅在选择“**设置为新设备或恢复**”时可用（即跳过此步骤）。
- **Apple ID：** 为设备设置 Apple ID 帐户。Citrix 建议您选中此复选框以包含此步骤。
- **条款和条件：** 要求用户接受设备使用条款和条件。Citrix 建议您选中此复选框以包含此步骤。
- **Apple Pay：** 在 iOS 设备上设置 Apple Pay。
- **Siri：** 在设备上使用或不使用 Siri。
- **应用分析：** 设置是否与 Apple 共享崩溃数据和使用统计信息。
- **显示缩放：** 在 iOS 设备上设置显示分辨率（标准或缩放）。
- **原彩显示：** 在 iOS 设备上设置原彩显示。
- **主屏幕按钮：** 设置主屏幕按钮的屏幕灵敏度。
- **新功能亮点：** 在 iOS 11.0 设备（最低版本）上设置引导信息屏幕、从任意位置访问 Dock 以及在最近使用的应用之间切换。
- **隐私：** 在设置 Apple 部署计划设备期间，阻止用户看到数据和隐私面板。适用于 iOS 11.3 及更高版本。

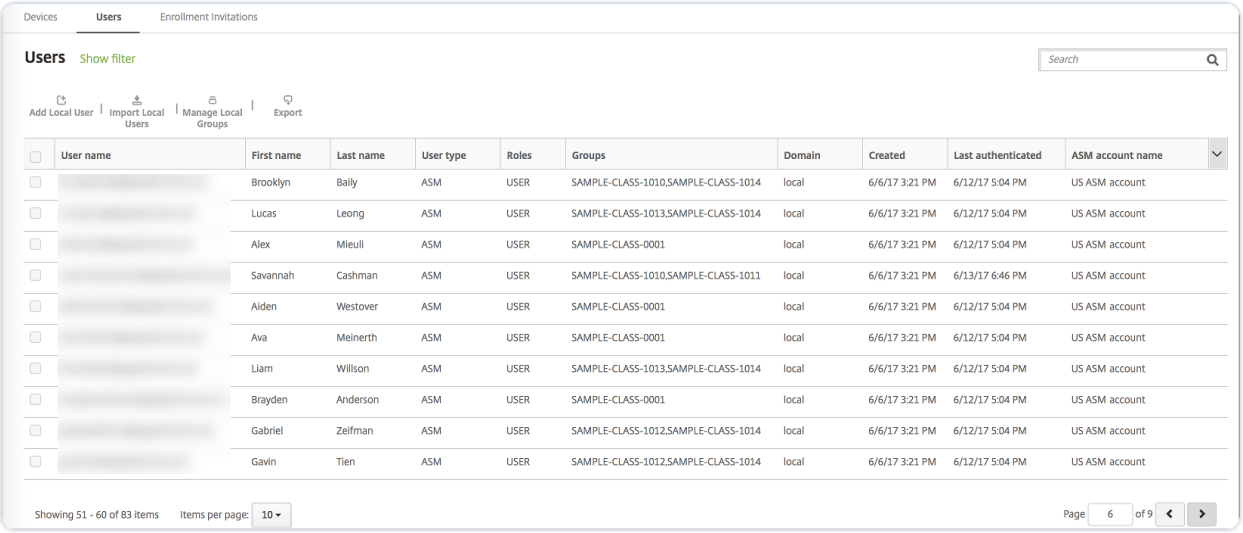
- **软件更新：** 在设置 Apple 部署计划设备期间，阻止用户看到强制软件更新屏幕。适用于 iOS 12.0 及更高版本。
- **屏幕使用时间：** 在设置 Apple 部署计划设备期间，阻止用户看到屏幕使用时间屏幕。适用于 iOS 12.0 及更高版本。
- **SIM 卡设置：** 在设置 Apple 部署计划设备期间，阻止用户看到添加蜂窝号码屏幕。适用于 iOS 12.0 及更高版本。
- **iMessage & FaceTime：** 阻止用户在设置 Apple Deployment Program 设备时看到 iMessage 和 FaceTime 屏幕。适用于 iOS 12.0 及更高版本。

6. 该帐户显示在“**设置 > Apple Deployment Program**”中。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**”。



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 会根据每个用户导入的托管 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`。

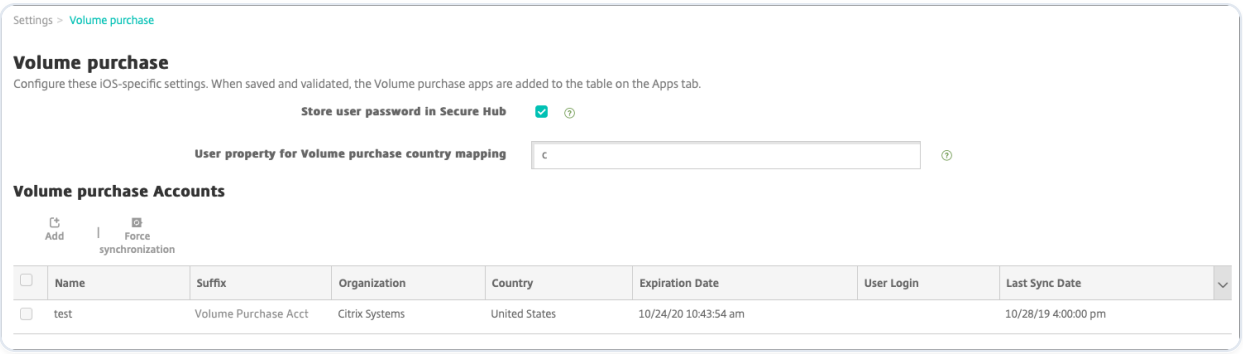


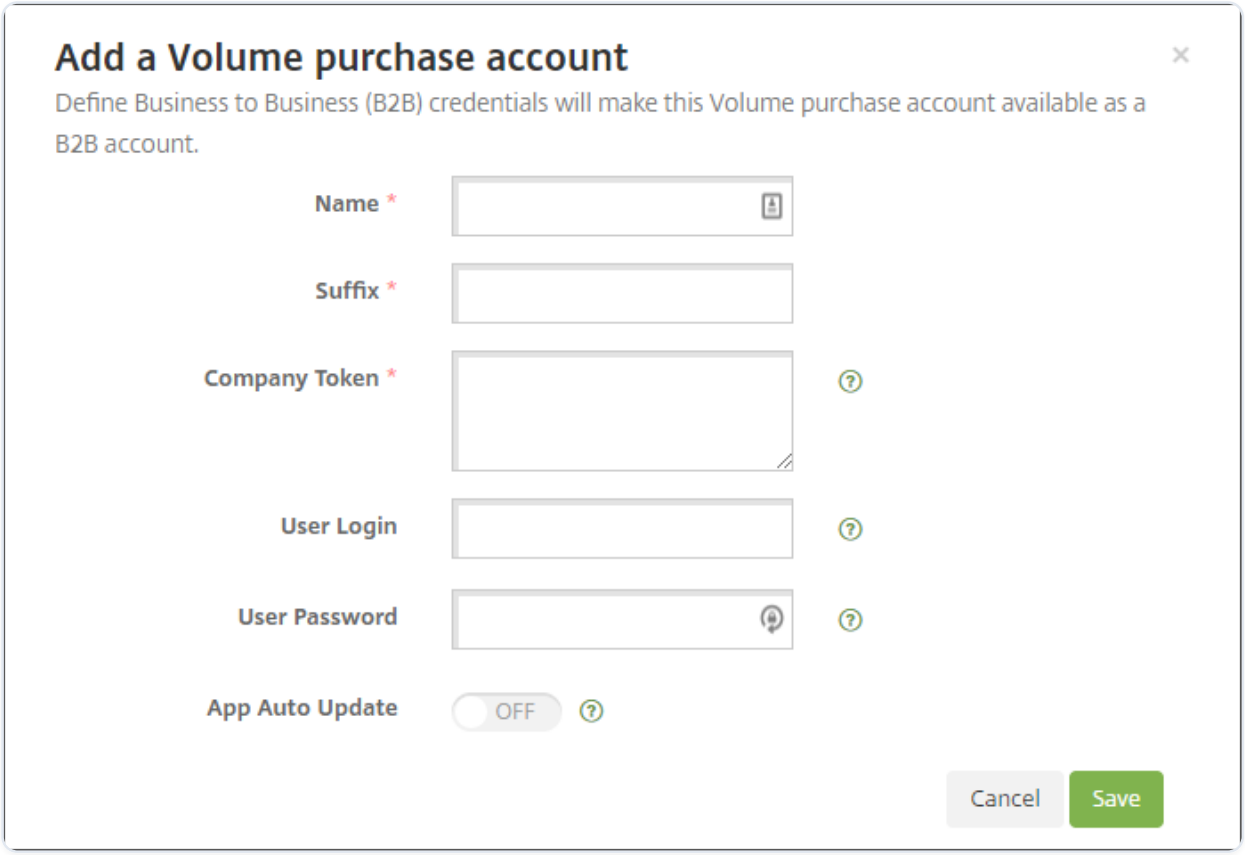
要查找给定 ASM 帐户的所有用户，请在用户搜索筛选器中键入帐户名称。

步骤 4：为 Apple School Manager 配置教育批量采购帐户

在本节中，您将 XenMobile 指向用于购买应用程序和 iBooks 批量采购许可证的批量采购帐户。

1. 要为 ASM 配置教育批量采购帐户，请按照 Apple 批量采购 中的说明进行操作。“添加批量采购帐户”屏幕要求您提供公司令牌。直接从您的教育批量采购帐户下载令牌，并将其粘贴到“**添加批量采购帐户**”屏幕中。





2. 请等待几分钟，以便将批量采购许可证导入 XenMobile。

步骤 5：为 Apple School Manager 用户添加密码

添加 ASM 帐户后，XenMobile 会从 ASM 导入班级和用户。XenMobile 将班级视为本地组，并在控制台中使用“组”一词。如果班级在 ASM 中有组名，XenMobile 会将该组名分配给该班级。否则，XenMobile 会使用源系统 ID 作为组名。XenMobile 不会使用课程名称作为班级名称，因为 ASM 中的课程名称不是唯一的。

XenMobile 使用管理式 Apple ID 创建用户类型为 **ASM** 的本地用户。这些用户是本地用户，因为 ASM 独立于所有外部数据源创建凭据。因此，XenMobile 不会使用目录服务器来验证这些新用户。

ASM 不会将临时用户密码发送到 XenMobile。您可以从 CSV 文件导入它们，也可以手动添加。要导入临时用户密码：

1. 获取在创建管理式 Apple ID 临时密码时由 ASM 生成的 CSV 文件。
2. 编辑 CSV 文件，将临时密码替换为用户提供以注册到 XenMobile 的新密码。为此，对密码类型没有限制。

   CSV 文件中条目的格式如下：

   `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`!

   其中：

用户：`user@appleid.citrix.com`

名字：`Firstname`

中间名：`Middle`

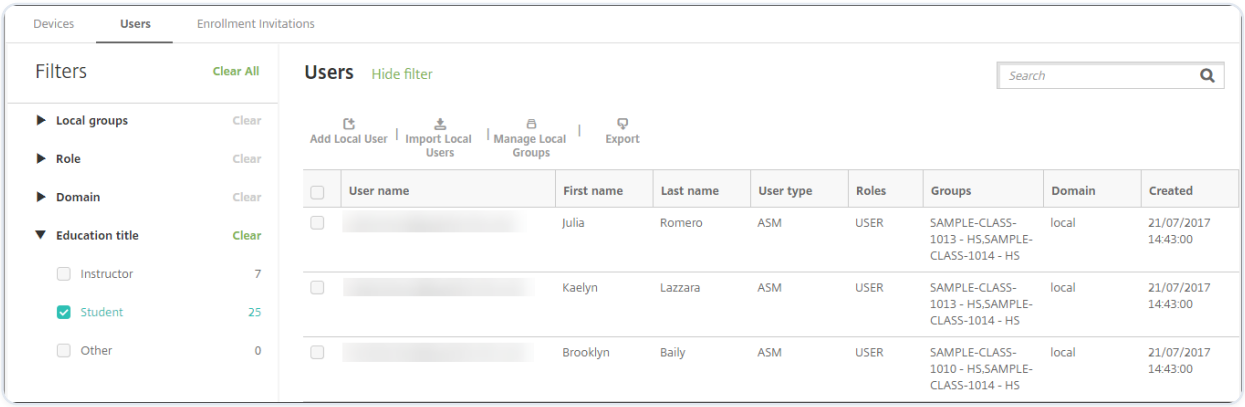
姓氏：`Lastname`

密码：`Password123!`!

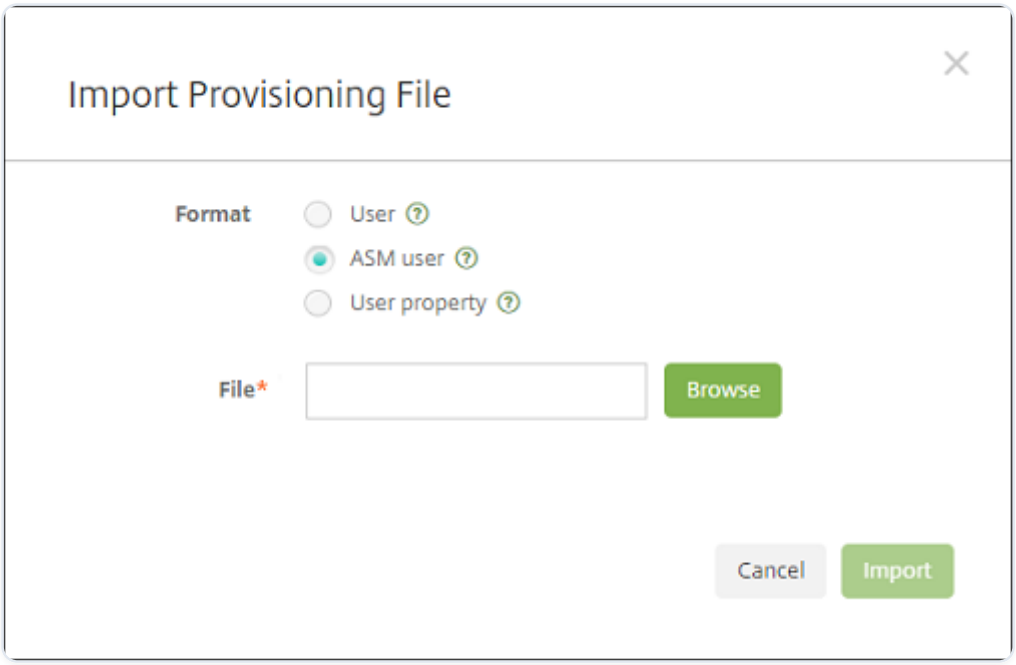
3. 在 XenMobile 控制台中，单击 **管理 > 用户**。此时将显示“**用户**”页面。

   以下“**管理 > 用户**”屏幕示例显示了从 ASM 导入的用户列表。在“**用户**”列表中：

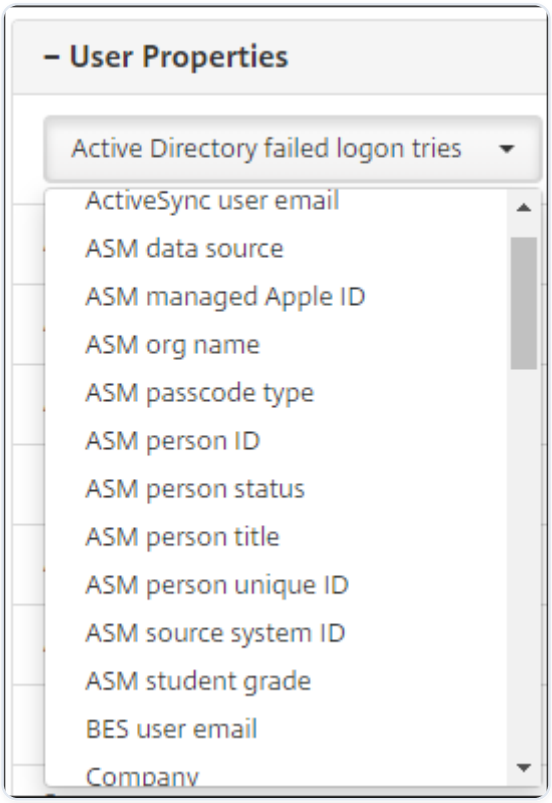
   - “**用户名**”显示管理式 Apple ID。
   - 用户类型为 **ASM**，表示该帐户源自 ASM。
   - **组**显示班级。



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”，选择 **ASM 用户**，导航到您在步骤 2 中准备的 CSV 文件，然后单击**导入**。



6. 要查看本地用户的属性，请选择该用户，然后单击**编辑**。



除了名称属性之外，还提供以下 ASM 属性：

- **ASM 数据源：** 班级的数据源，例如 **CSV** 或 **SFTP**。
- **ASM 托管式 Apple ID：** 托管式 Apple ID 可能包含您的机构名称和 `appleid`。例如，该 ID 可能类似于 `johnappleseed@appleid.myschool.edu`。XenMobile 需要托管式 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 密码类型：** 此人的密码策略：**复杂**（八个或更多数字和字母组成的非学生密码）、**四位**（数字）或**六位**（数字）。
- **ASM 个人唯一 ID：** 用户的标识符。
- **ASM 个人状态：** 指定托管式 Apple ID 是**活动**还是**非活动**。此状态在用户为其托管式 Apple ID 帐户提供新密码后变为活动状态。
- **ASM 人员职称：** 教师、学生或其他。
- **ASM 人员唯一 ID：** 用户的唯一标识符。
- **ASM 源系统 ID：** 系统源的标识符。
- **ASM 学生年级：** 学生年级信息（教师不使用）。

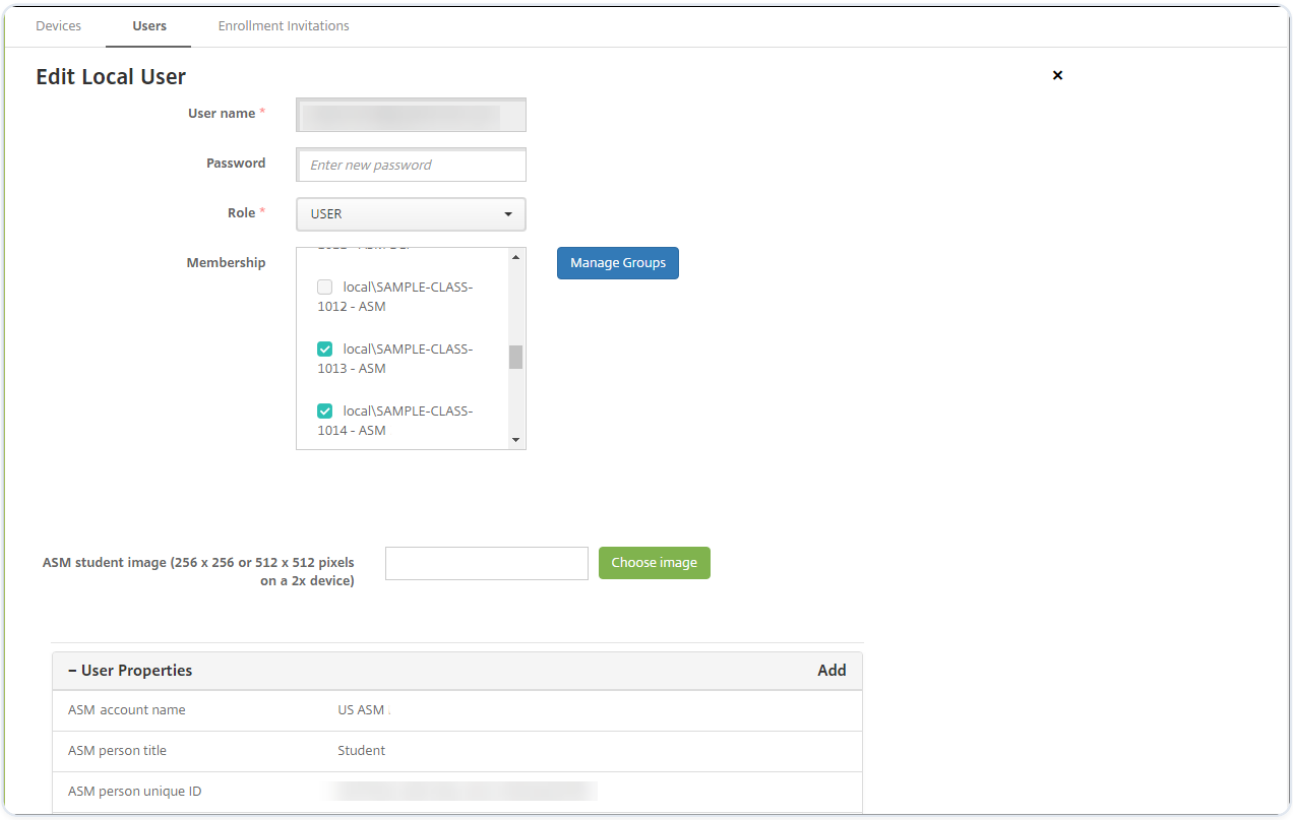
步骤 6：可选地添加学生照片

您可以为每位学生添加照片。如果教师使用 Apple Classroom 应用，照片将显示在该应用中。

照片建议：

- 分辨率：256 x 256 像素（在 2 倍设备上为 512 x 512 像素）
- 格式：JPEG、PNG 或 TIFF

要添加照片，请转至**管理 > 用户**，选择一个用户，单击**编辑**，然后单击**选择图像**。



步骤 7：规划并将资源和交付组添加到 XenMobile

交付组指定要部署到用户类别的资源。例如，您可以为教师和学生创建一个交付组。或者，您可以创建多个交付组，以便自定义发送给不同教师或学生的应用程序、媒体和策略。您可以为每个班级创建一个或多个交付组。您还可以为管理员（您教育机构中的其他员工）创建一个或多个交付组。

您部署到用户设备的资源包括设备策略、批量购买应用程序和 iBooks。

- 设备策略：

  如果教师使用课堂应用，则需要教育配置设备策略。请务必查看其他设备策略，以确定如何配置和限制教师和学生的 iPad。

- 批量购买应用：

  XenMobile 要求您将批量购买应用部署为教育用户的必需应用。XenMobile 不支持将此类批量购买应用部署为可选应用。

  如果您使用 Apple 课堂应用，请仅将其部署到教师设备。

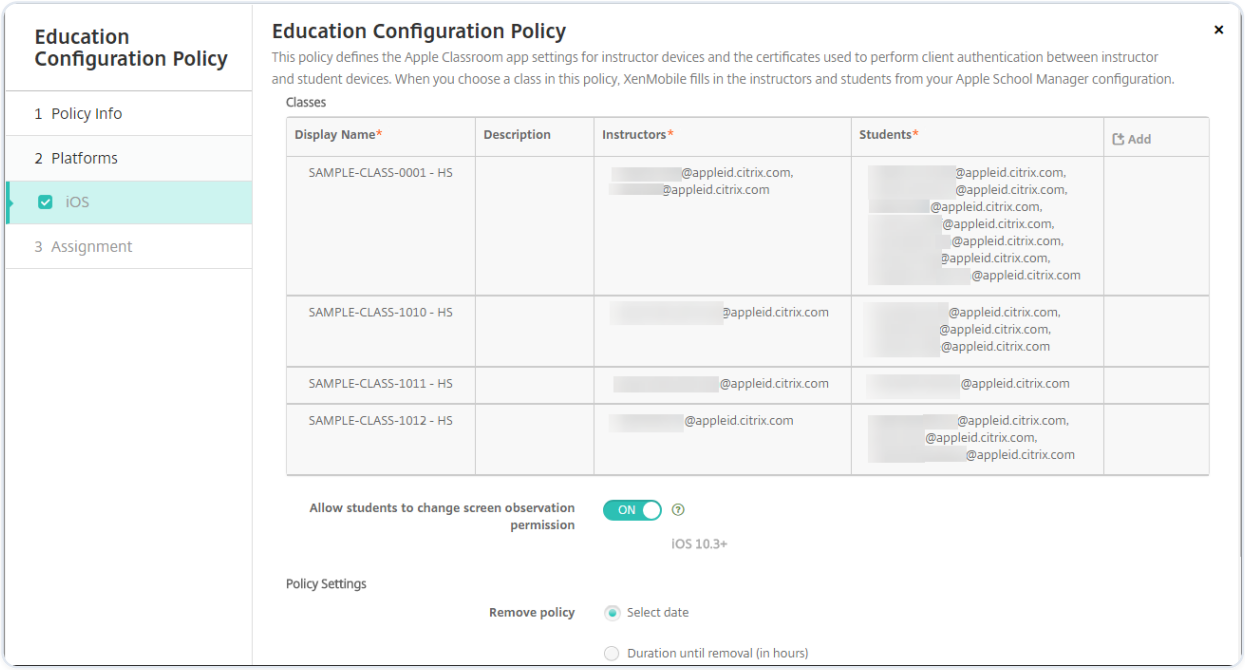
  部署您希望提供给教师或学生的任何其他应用。此解决方案不使用 Citrix Secure Hub 应用，因此无需将其部署给教师或学生。

- 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 可用于添加到交付组。XenMobile 仅支持将 iBooks 添加为必需媒体。

在您为教师和学生规划好资源和交付组后，您可以在 XenMobile 控制台中创建这些项目。

1. 创建您希望部署到教师或学生设备的任何设备策略。有关教育配置设备策略的信息，请参阅教育配置设备策略。

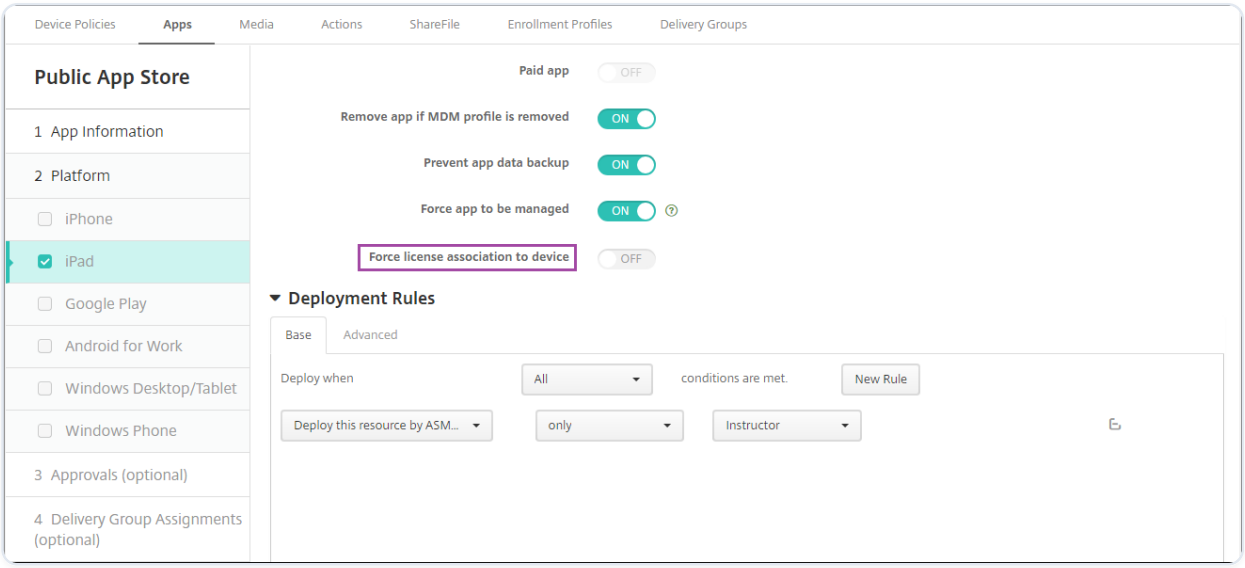


有关设备策略的信息，请参阅设备策略和各个策略文章。

2. 配置应用 (**配置 > 应用**) 和 iBooks (**配置 > 媒体**)：

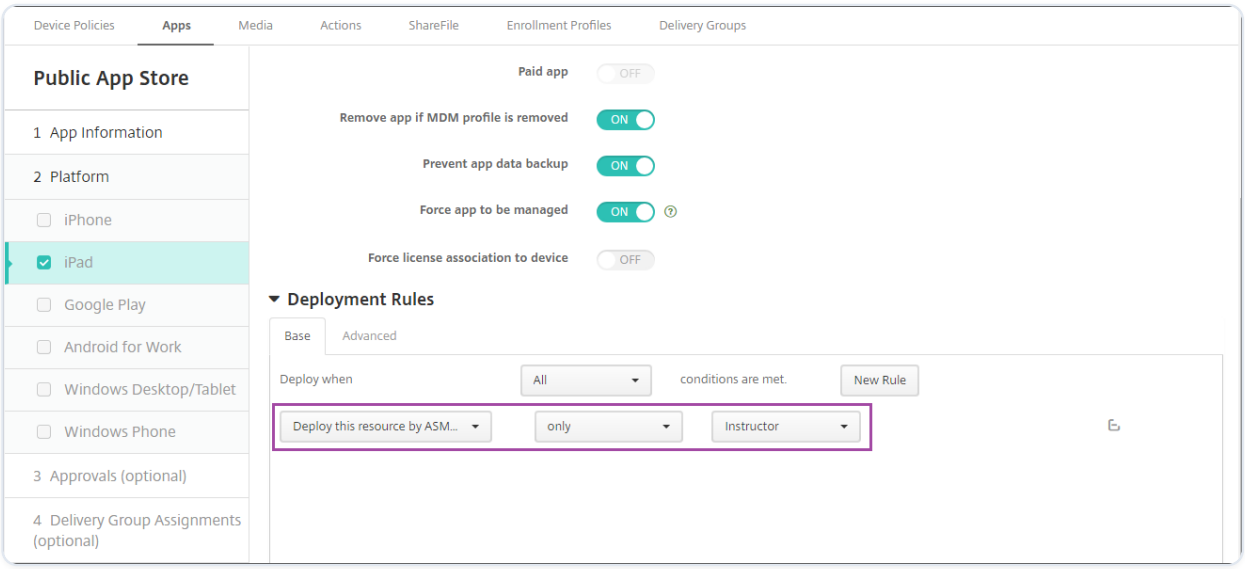
   - 默认情况下，XenMobile 在用户级别分配应用和 iBooks。首次部署期间，教师和学生会收到注册 ASM 的提示。接受邀请后，用户将在下次部署（六小时内）时收到其 ASM 应用和 iBooks。Citrix 建议您强制将应用和 iBooks 部署到新的 ASM 用户。为此，请选择交付组并单击**部署**。

     您可以选择在设备级别分配应用（但不能分配 iBooks）。为此，请将设置**强制许可证关联到设备**更改为**开**。当您在设备级别分配应用时，用户不会收到加入 Apple 批量购买的邀请。



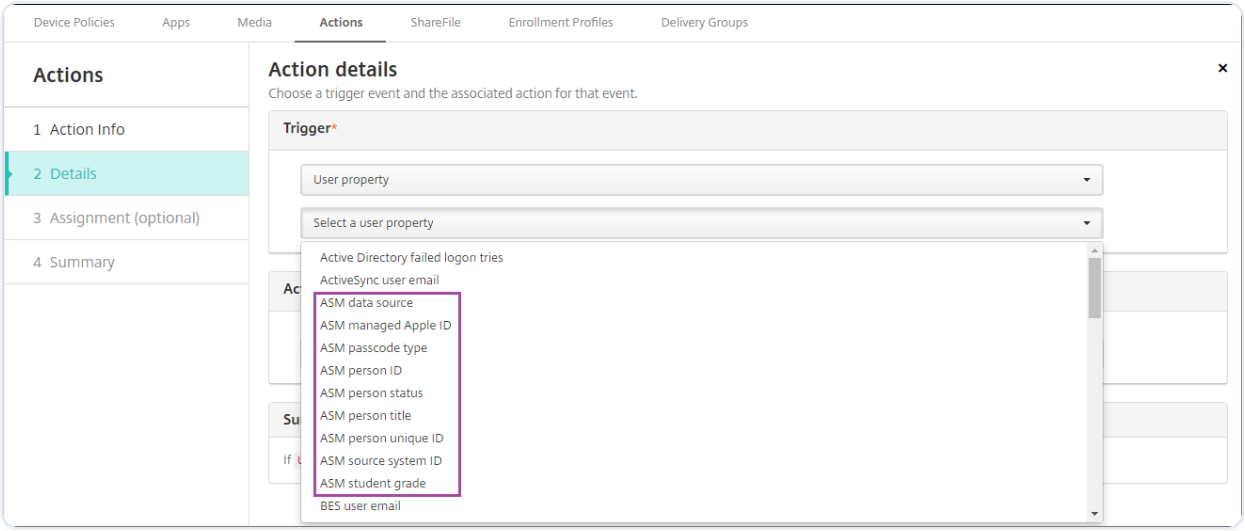
   - 要仅向教师部署应用程序，请选择仅包含教师的交付组或使用以下部署规则：

```
Deploy this resource by ASM device type

only

Instructor
```



- 有关添加批量购买应用程序的帮助，请参阅添加公共应用商店应用程序。

3. 可选。根据 ASM 用户属性创建操作。例如，您可以创建一个操作，在新应用程序安装时向学生设备发送通知。或者，您可以创建一个由用户属性触发的操作，如以下示例所示。

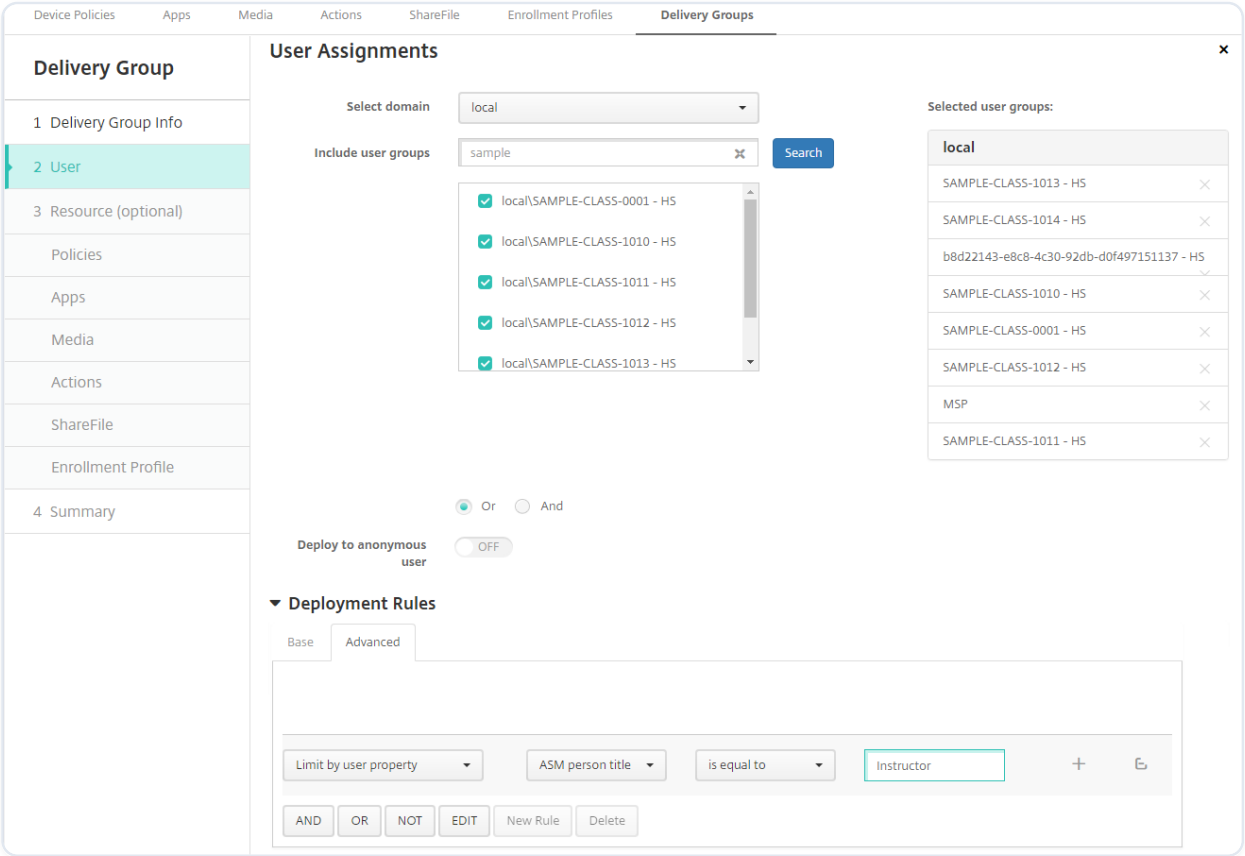


要创建操作，请转到**配置 > 操作**。有关配置操作的信息，请参阅自动化操作。

4. 在**配置 > 交付组**中，为教师和学生创建交付组。选择从 ASM 导入的班级。此外，为教师和学生创建部署规则。

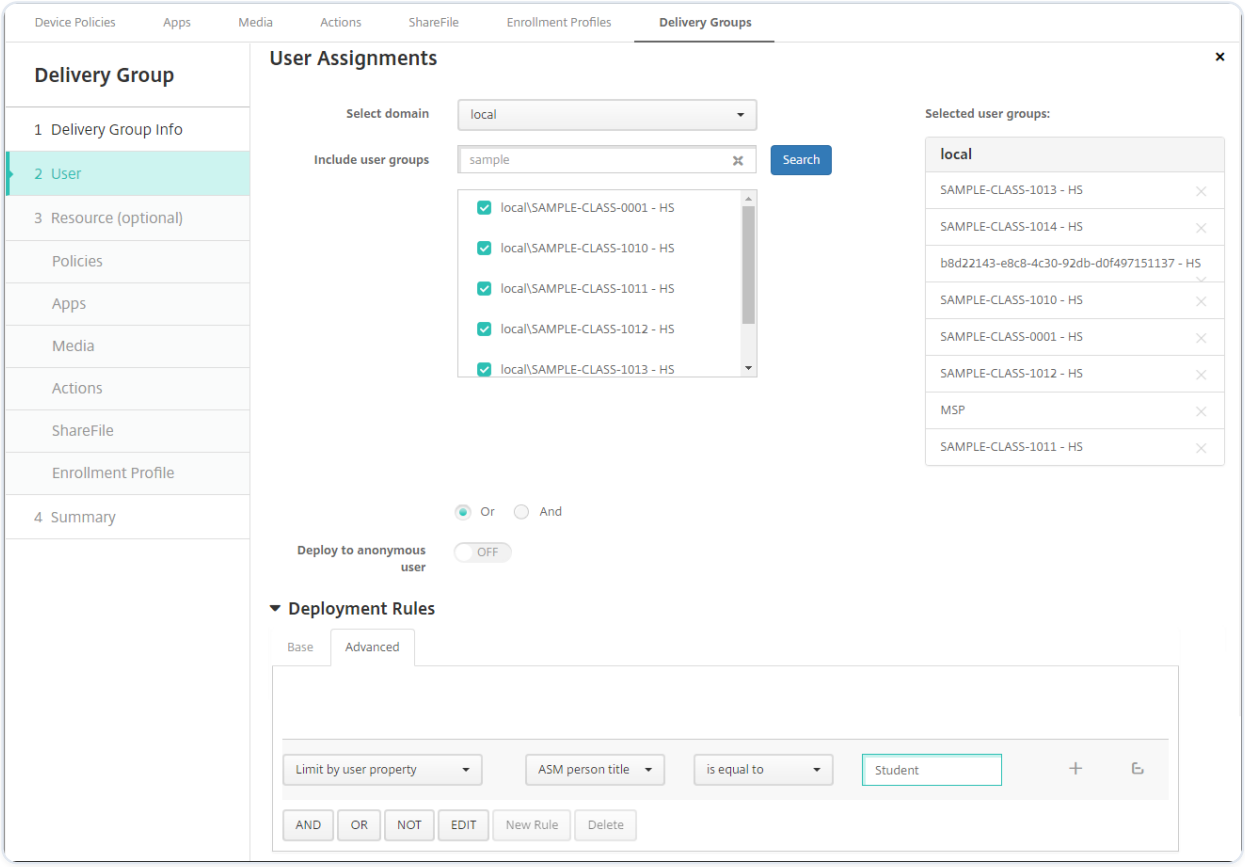
   例如，以下用户分配适用于教师。部署规则为：

```
Limit by user property

ASM person title

is equal to

Instructor
```

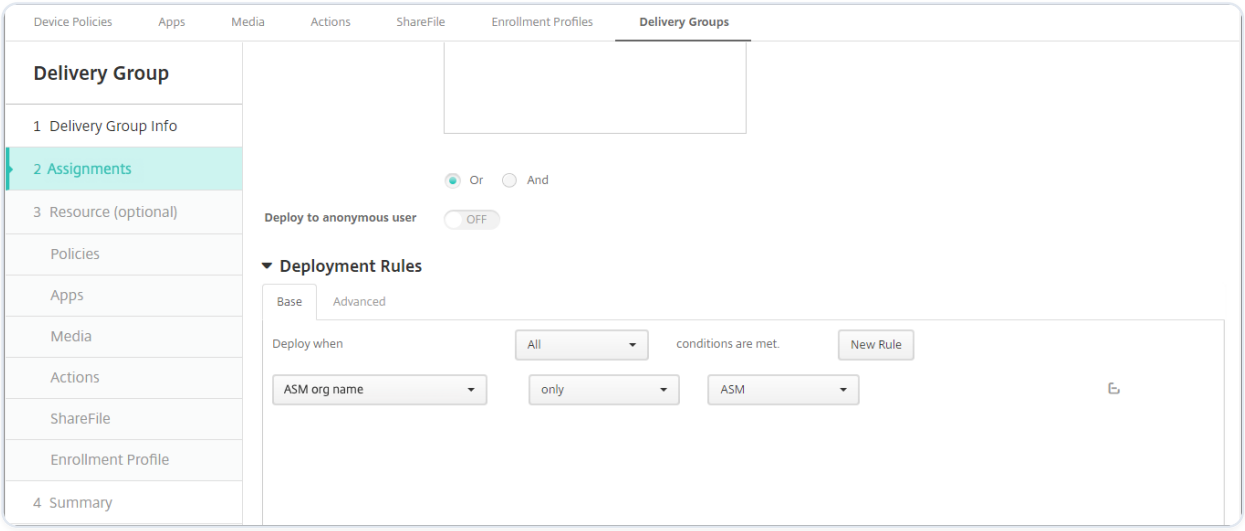


以下用户分配适用于学生。部署规则为：

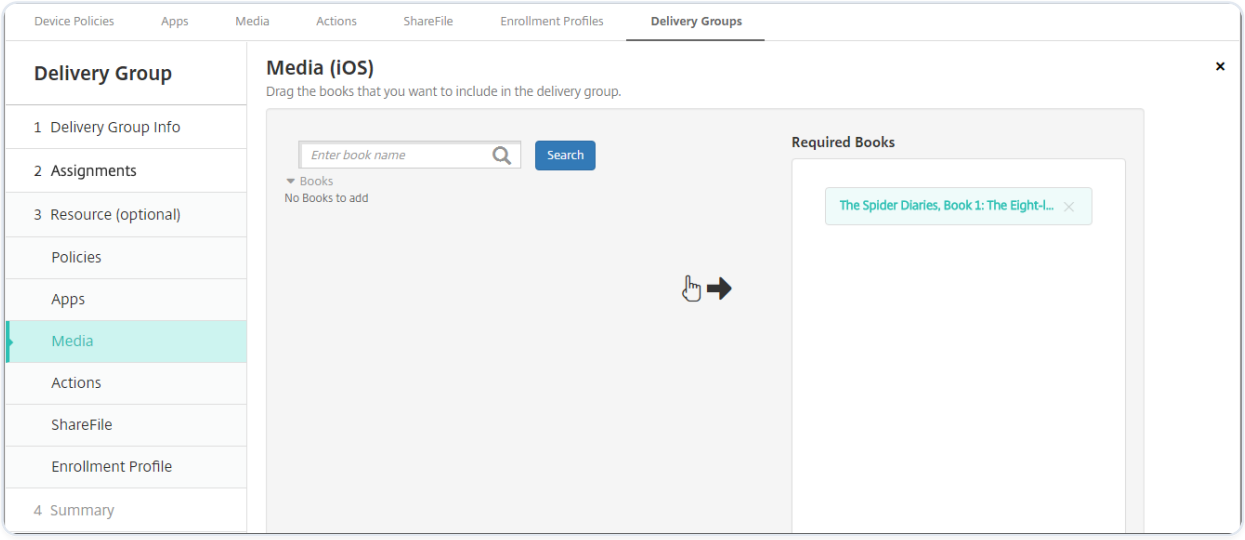
```
Limit by user property

ASM person title

is equal to

Student
```



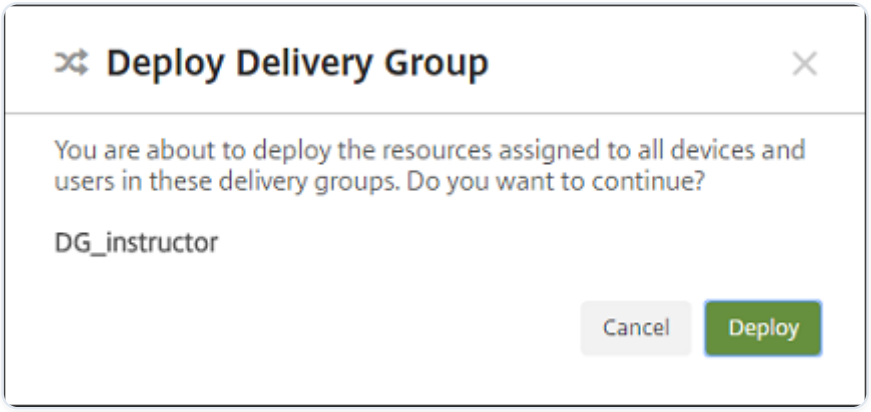
您还可以使用基于 ASM 组织名称的部署规则来筛选交付组。



5. 将资源分配给交付组。以下示例显示了交付组中包含的 iBook。



以下示例显示了选择交付组并单击“**部署**”时出现的确认对话框。



有关详细信息，请参阅 部署资源 中的“编辑交付组”和“部署到交付组”。

步骤 8：测试教师和学生设备注册

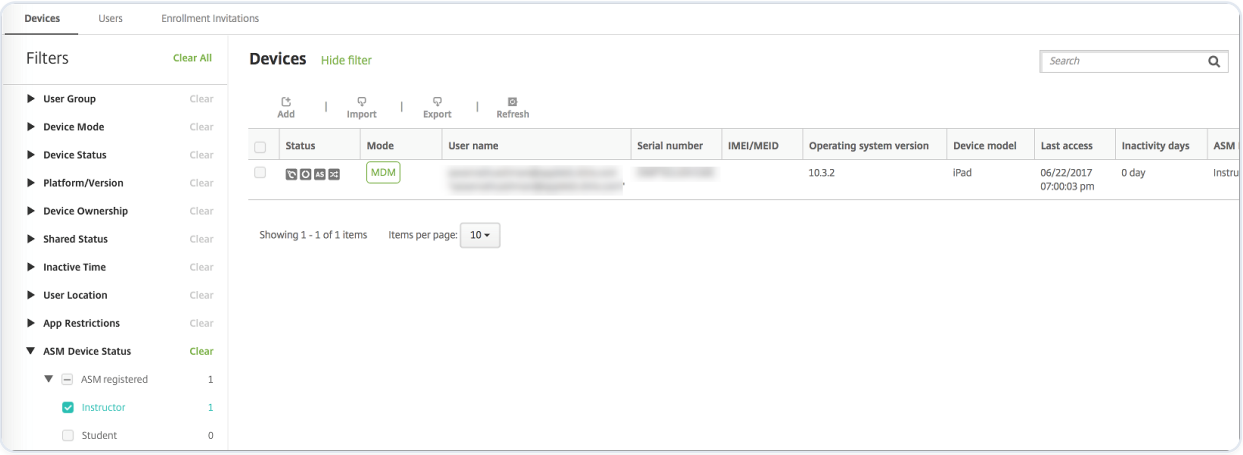
您可以通过以下任一方法注册设备：

- 学校管理员可以使用您在 XenMobile 控制台中设置的用户密码注册教师和学生设备。因此，您可以为用户提供已设置好应用程序和媒体的设备。
- 当用户收到设备时，他们使用您提供给他们的用户密码进行注册。注册完成后，XenMobile 会将设备策略、应用程序和媒体发送到设备。

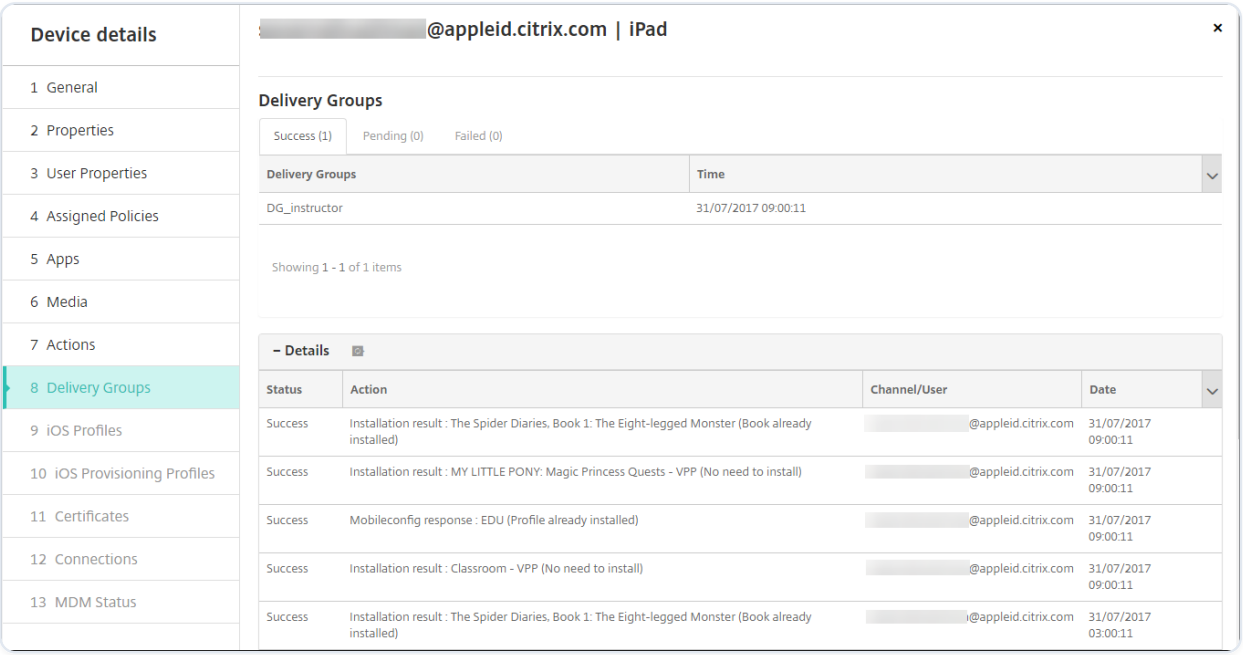
要测试注册，请使用链接到 ASM 的 Apple Deployment Program 设备。

1. 如果设备未链接到 ASM，请通过硬重置擦除设备内容和设置。
2. 为教师注册一个 ASM 设备。然后，为学生注册一个 ASM 设备。
3. 在“**管理 > 设备**”页面中，检查两个 ASM 设备是否都仅注册到 MDM。

   您可以按 ASM 设备状态筛选“**设备**”页面：**ASM 已注册**、**ASM 共享**、**教师**和**学生**。



4. 要验证 MDM 资源是否已为每个设备正确部署：选择设备，单击“**编辑**”，然后检查各个页面。



步骤 9: 分发设备

Apple 建议您举办一个活动，以便将设备分发给教师和学生。

如果您不分发预注册设备，请同时向这些用户提供以下信息：

- 用于注册的 XenMobile 密码
- 用于托管式 Apple ID 的 ASM 临时密码。

首次用户体验如下。

1. 用户在硬重置后首次启动设备时，XenMobile 会在注册屏幕中提示他们注册设备。
2. 用户提供其托管式 Apple ID 和用于向 XenMobile 进行身份验证的 XenMobile 密码。
3. 在 Apple ID 设置步骤中，设备会提示用户提供其托管式 Apple ID 和 ASM 临时密码。这些信息用于向 Apple 服务验证用户身份。

4. 设备会提示用户为其托管式 Apple ID 创建密码，该密码用于保护其在 iCloud 中的数据。
5. 在设置助理结束时，XenMobile 开始将策略、应用程序和媒体安装到设备。对于在用户级别分配的应用程序和 iBooks，助理会提示教师和学生注册批量采购。接受邀请后，用户将在下次部署（六小时内）时收到其批量采购的应用程序和 iBooks。

管理教师、学生和班级数据

管理教师、学生和班级数据时，请注意以下事项：

- 将 ASM 信息导入 XenMobile 后，请勿更改托管式 Apple ID。XenMobile 还使用 ASM 用户标识符来识别用户。
- 如果您在创建一项或多项教育配置设备策略后在 ASM 中添加或更改班级数据：请编辑策略，然后重新部署它们。
- 如果部署教育配置设备策略后，班级教师发生更改：请检查该策略以确保其在 XenMobile 控制台中更新，然后重新部署该策略。
- 如果您在 ASM 门户中更新用户属性，XenMobile 也会在控制台中更新这些属性。但是，XenMobile 接收 ASM 人员职称属性（教师、学生或其他）的方式与其他属性不同。因此，如果您在 ASM 中更改 ASM 人员职称，请完成以下步骤以在 XenMobile 中反映该更改。

要管理数据：

1. 在 ASM 门户中，更新学生年级并清除教师年级。
2. 如果您将学生帐户更改为教师帐户，请从班级学生列表中删除该用户。然后，将该用户添加到同一班级或另一个班级的教师列表中。

   如果您将教师帐户更改为学生帐户，请从班级中删除该用户。然后，将该用户添加到同一班级或另一个班级的学生列表中。您的更新将在下次同步（默认每五分钟一次）或获取（默认每 24 小时一次）期间显示在 XenMobile 控制台中。
3. 编辑教育配置设备策略以应用更改并重新部署它。

   - 如果您从 ASM 门户中删除用户，XenMobile 也会在获取后从 XenMobile 控制台中删除该用户。

     您可以通过更改此服务器属性值来缩短两个基线之间的时间间隔：**bulk.enrollment.fetchRosterInfoDelay**（默认值为 **1440** 分钟）。
   - 部署资源后：如果学生加入班级，请仅包含该学生创建一个交付组，并将资源部署给该学生。
   - 如果学生或教师丢失了临时密码，请让他们联系 ASM 管理员。管理员可以提供临时密码或生成新密码。

管理已注册 Apple School Manager Apple 部署计划的丢失或被盗设备

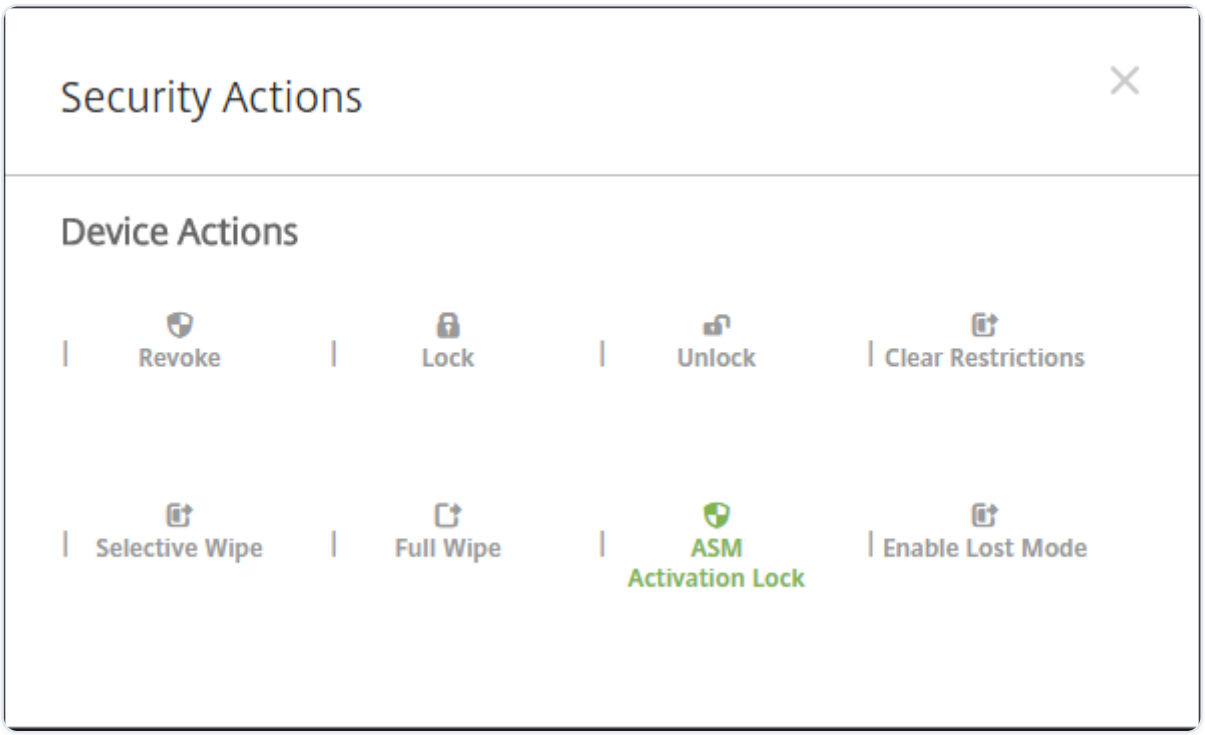
Apple 的“查找我的 iPhone/iPad”服务包含激活锁功能。激活锁可防止未经授权的用户使用或转售已注册 Apple 部署计划的丢失或被盗设备。

XenMobile 包含一个 **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。

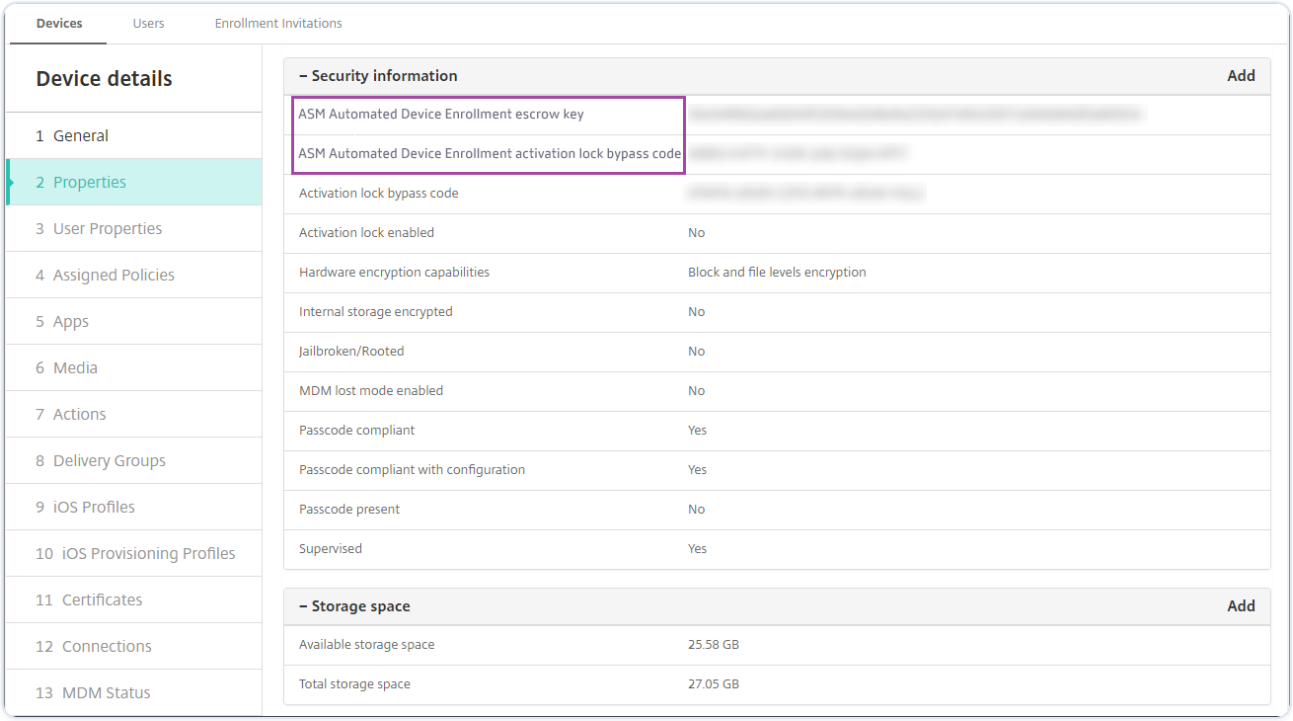
当您使用 **ASM 激活锁**安全操作时，XenMobile 可以定位设备，而无需用户启用“查找我的 iPhone/iPad”服务。当 ASM 设备被硬重置或完全擦除时，用户需要提供其管理式 Apple ID 和密码才能解锁设备。

要从控制台解除锁定，请单击安全操作 **激活锁绕过**。有关绕过激活锁的信息，请参阅 绕过 iOS 激活锁。用户还可以将登录名留空，并将 **ASM 激活锁绕过代码** 作为密码输入。该信息可在 **设备详细信息** 的 **属性** 选项卡中找到。

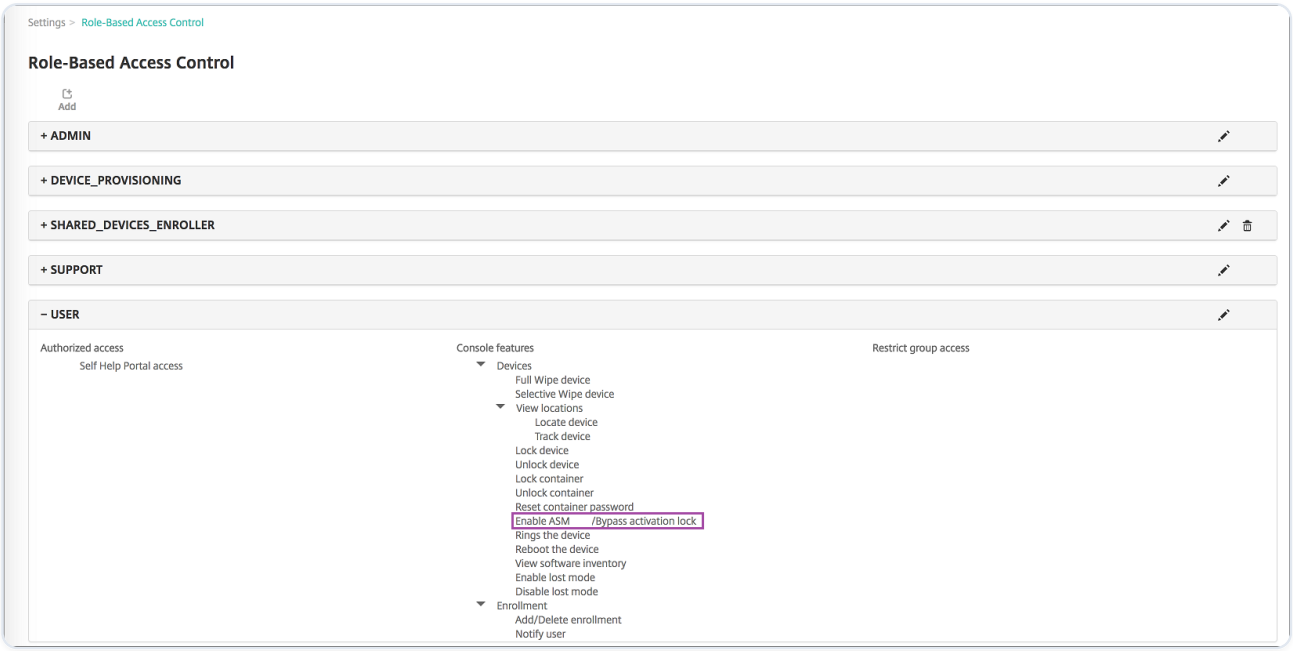
要设置激活锁，请转到 **管理 > 设备**，选择设备，单击 **安全**，然后单击 **ASM 激活锁**。



属性 **ASM 托管密钥** 和 **ASM 激活锁绕过代码** 显示在 **设备详细信息** 中。



ASM 激活锁的 RBAC 权限为 **设备 > 启用 ASM 绕过激活锁**。



共享 iPad

共享 iPad 功能允许多个用户使用一台 iPad。即使设备是共享的，用户体验也可以个性化。您可以将共享 iPad 用于教育或商业用途。Apple School Manager (ASM) 除了支持 Apple Business Manager (ABM) 支持的角色外，还支持教师和学生角色。

先决条件

- Apple 校园教务管理 或 Apple 商务管理

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

配置共享 iPad

教室中的多名学生可以共享一台 iPad，用于一位或多位教师教授的不同科目。

您或教师注册共享 iPad，然后将设备策略、应用程序和媒体部署到设备。之后，学生提供其托管 Apple ID 凭据以登录共享 iPad。如果您之前已向学生部署了教育配置策略，他们将不再以“其他用户”身份登录共享设备。

XenMobile 为共享 iPad 使用两个通信通道：用于设备所有者（教师）的系统通道和用于当前驻留用户（学生）的用户通道。XenMobile 使用这些通道发送 Apple 支持的资源的相应 MDM 命令。

通过系统通道部署的资源包括：

- 设备策略：教育配置、最大驻留用户数 和 密码锁定宽限期
- 基于设备的批量购买应用程序

  Apple 不支持在共享 iPad 上使用企业应用或基于用户的批量采购应用。安装在共享 iPad 上的应用是设备全局的，而非按用户分配。
- 基于用户的批量采购 iBooks

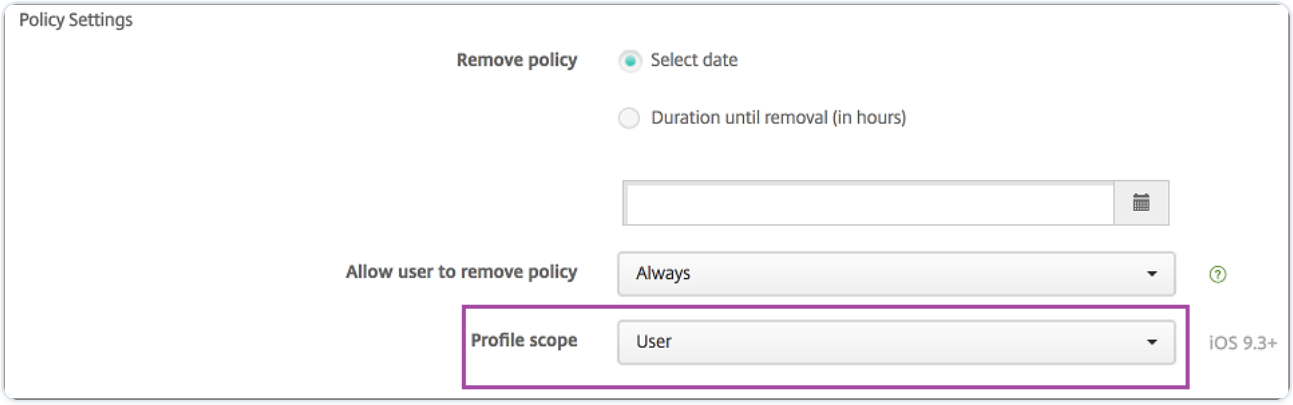
  Apple 支持在共享 iPad 上分配基于用户的批量采购 iBooks。

通过用户通道部署的资源如下：

- 设备策略：应用通知、主屏幕布局、限制和 Webclip

  XenMobile 仅支持通过用户通道部署的这些设备策略。

配置设备策略时，您可以在策略设置 **配置文件范围** 中指定部署通道。



要删除通过用户通道部署的设备策略，请确保为配置文件删除策略选择**部署范围**为**用户**。

一般工作流程

通常，您会向教师提供预配置和受监管的共享 iPad。教师随后将设备分发给学生。如果您不向教师分发预注册的共享 iPad：请确保向教师提供其 XenMobile Server 密码，以便他们可以注册其设备。

配置和注册共享 iPad 的一般工作流程如下：

1. 使用 XenMobile Server 控制台添加 ASM 或 ABM 帐户（**设置** > **Apple 部署计划**），并启用**共享模式**。有关详细信息，请参阅管理共享 iPad 的 ASM 或 ABM 帐户。
2. 如本节所述，将所需的设备策略、应用和媒体添加到 XenMobile。将这些资源分配给交付组。
3. 让教师对共享 iPad 执行硬重置。此时将显示用于注册的远程管理屏幕。
4. 教师注册共享 iPad。

   XenMobile 部署配置的资源到每个已注册的共享 iPad。自动重启后，教师可以将设备与学生共享。iPad 上会出现一个登录页面。
5. 学生选择班级，然后输入其管理的 Apple ID 以及临时的 ASM 或 ABM 密码。

   共享 iPad 使用 ASM 或 ABM 进行身份验证，并提示学生创建 ASM 或 ABM 密码。下次登录共享 iPad 时，学生必须输入新密码。
6. 共享 iPad 的另一名学生可以通过重复上一步来登录。

管理用于共享 iPad 的 Apple School Manager 或 Apple Business Manager 帐户

如果您已将 XenMobile 与 Apple Education 结合使用：您在 XenMobile 中配置了现有的 ASM 或 ABM 帐户，用于非共享设备，例如教师使用的设备。您可以将相同的 ASM 或 ABM 以及相同的 XenMobile Server 用于共享设备和非共享设备。

XenMobile 支持以下部署方案：

- 每个班级一组共享 iPad

  在此方案中，您将共享 iPad 分配给一个班级的学生。iPad 留在教室中。在该班级教授不同科目的教师使用同一组 iPad。

- 每个教师一组共享 iPad

  在此方案中，您将共享 iPad 分配给一名教师，该教师将这些 iPad 用于其教授的各种课程。

将共享 iPad 组织成设备组

ASM 或 ABM 允许您通过创建多个 MDM 服务器将设备组织成组。当您将共享 iPad 分配给 MDM 服务器时，请为每组共享 iPad（按班级或按教师划分）创建一个设备组：

- 共享 iPad 组 1 > 设备组 1 MDM 服务器
- 共享 iPad 组 2 > 设备组 2 MDM 服务器
- 共享 iPad 组 N > 设备组 N MDM 服务器

为每个设备组添加 ASM 或 ABM 帐户

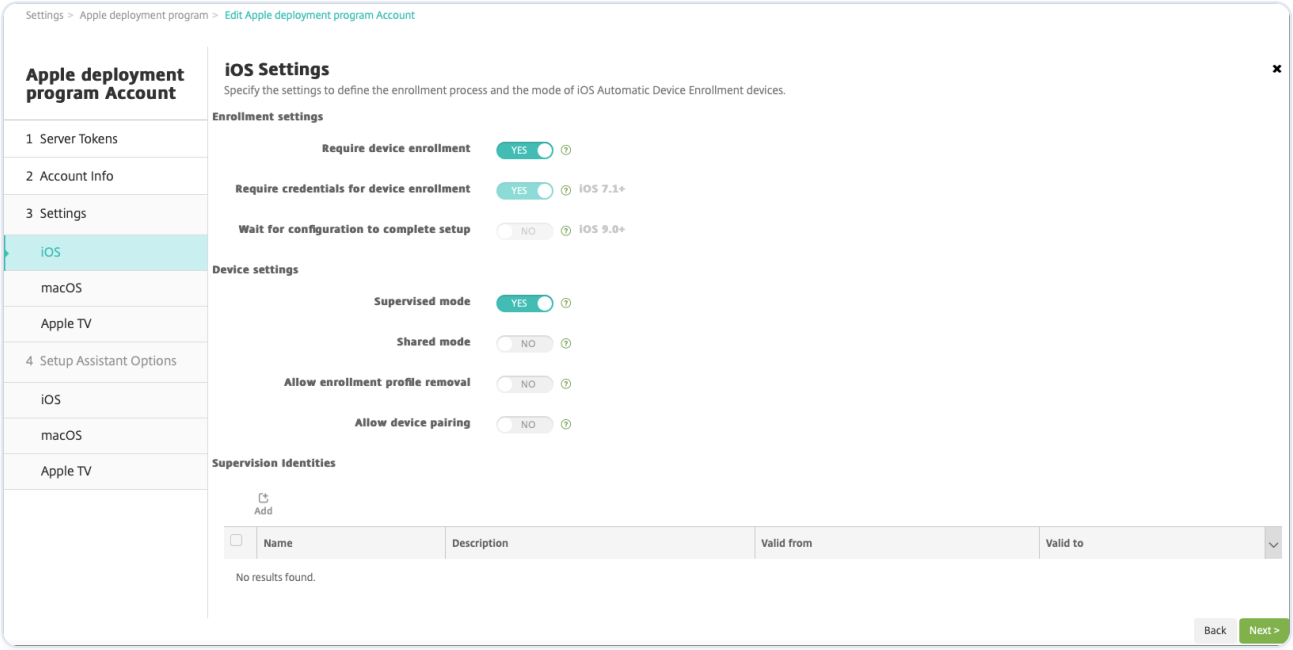
当您从 XenMobile Server 控制台创建多个 ASM 或 ABM 帐户时，您会自动导入共享 iPad 组（每个班级或教师一个）：

- 设备组 1 MDM 服务器 > 设备组 1 帐户
- 设备组 2 MDM 服务器 > 设备组 2 帐户
- 设备组 N MDM 服务器 > 设备组 N 帐户

共享 iPad 的特定要求如下：

- 每个设备组一个 ASM 或 ABM 帐户，并启用以下设置：
  - **要求设备注册**
  - **监管模式**
  - **共享模式**
- 对于给定的教育机构，请确保对所有 ASM 或 ABM 帐户使用相同的**教育后缀**。

要添加帐户，请转到**设置** > **Apple 部署计划**。

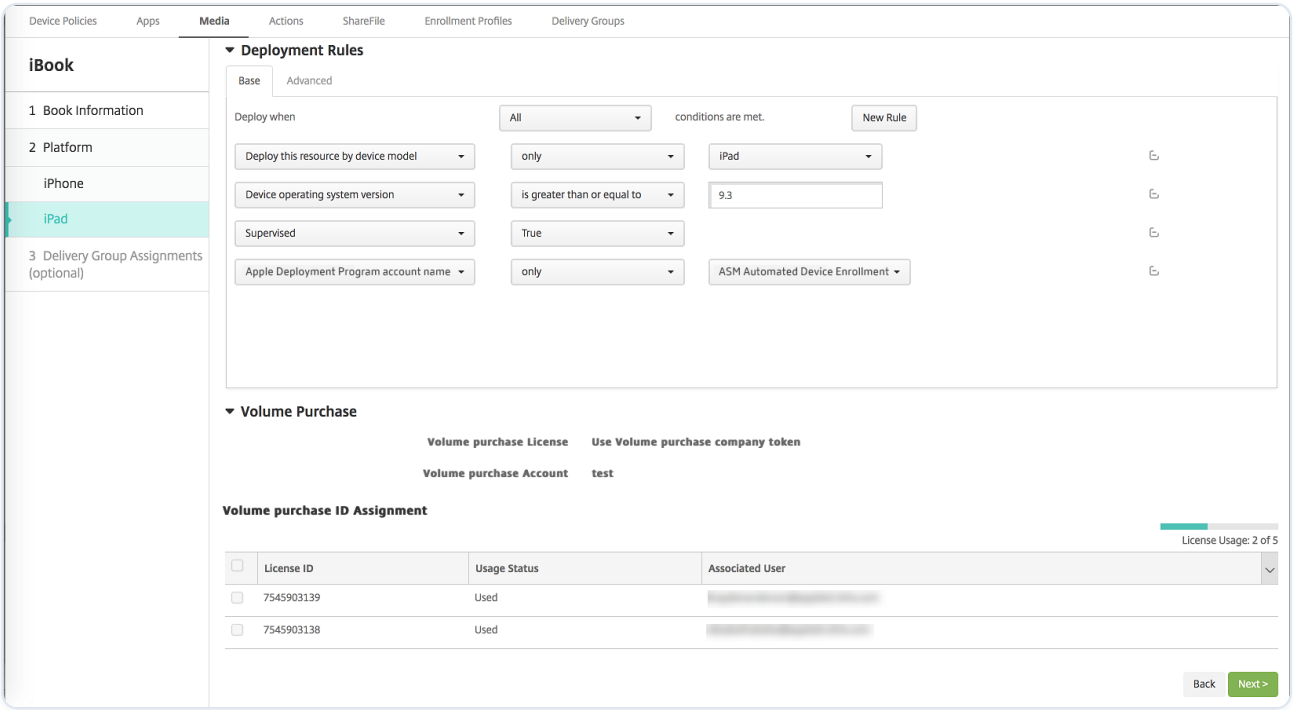


适用于共享 iPad 的应用程序

共享 iPad 支持分配基于设备的批量购买应用程序。在共享 iPad 上部署应用程序之前，XenMobile 会向 Apple 批量购买服务器发送请求，以将批量购买许可证分配给设备。要检查批量购买分配，请转至“**配置**”>“**应用程序**”>“**iPad**”，然后展开“**批量购买**”。

适用于共享 iPad 的媒体

共享 iPad 支持分配基于用户的批量购买 iBooks。在共享 iPad 上部署 iBooks 之前，XenMobile 会向 Apple 批量购买服务器发送请求，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**”，然后展开“**批量购买**”。



适用于共享 iPad 的部署规则

对于共享 iPad 部署，交付组级别的规则不适用，因为它们与用户属性相关。要筛选每个设备组的策略、应用程序和媒体：根据帐户名称为资源添加部署规则。例如：

- 对于设备组 1 帐户，设置此部署规则：

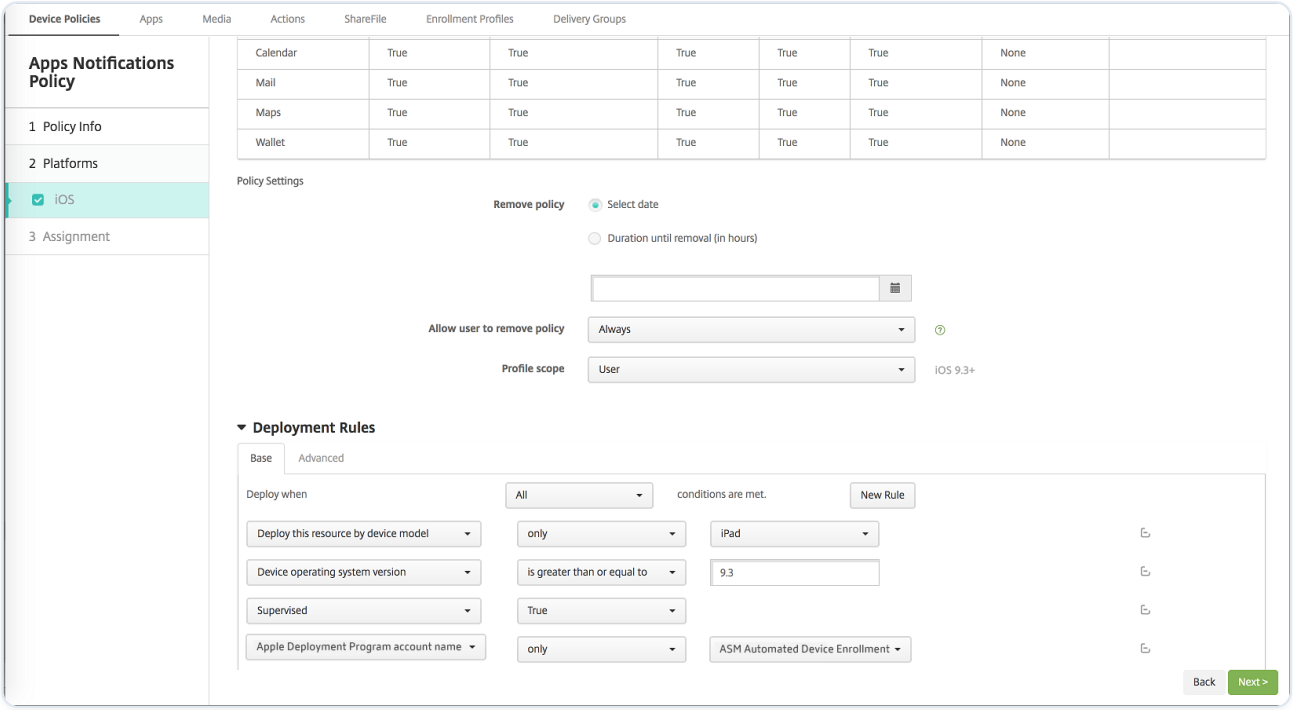
```
Apple Deployment Program account name

Only

Device Group 1 account
```

- 对于设备组 2 帐户，设置此部署规则：

```
Apple Deployment Program account name

Only

Device Group 2 account
```

- 对于设备组 N 帐户，设置此部署规则：

```
Apple Deployment Program account name

Only

Device Group N account
```

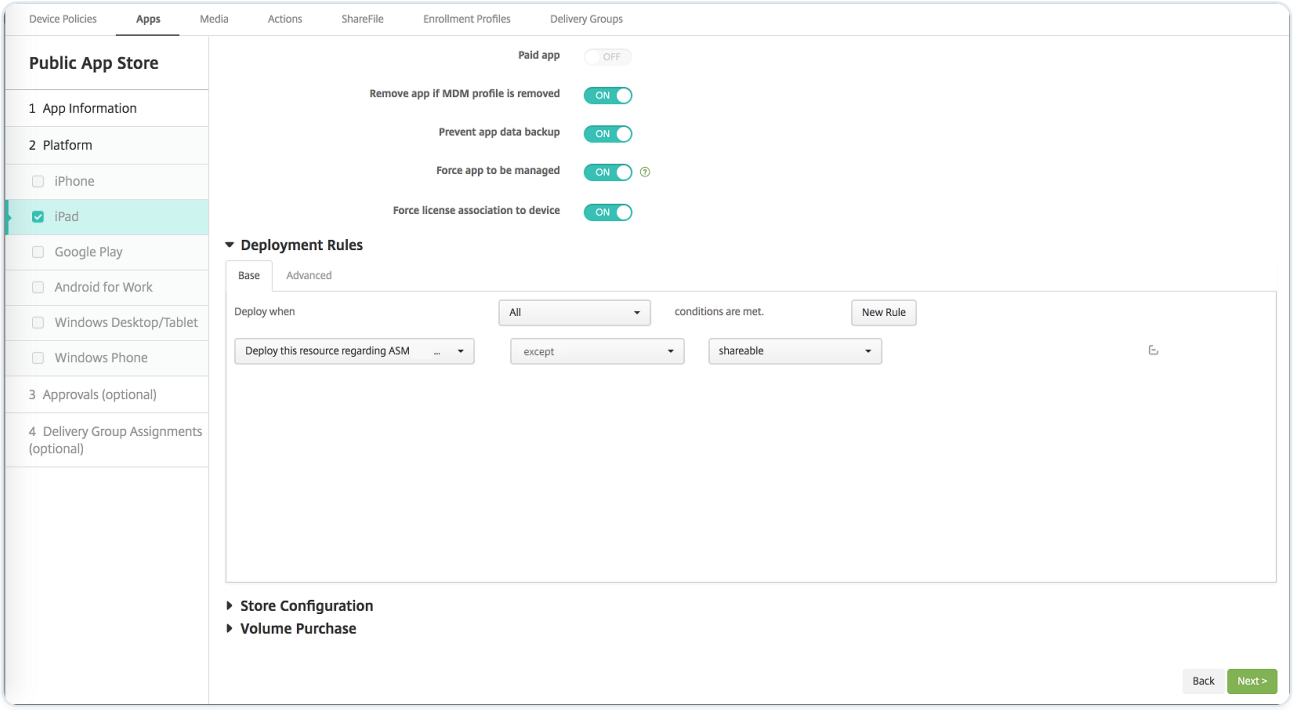


要仅向教师（使用非共享 iPad）部署 Apple Classroom 应用程序，请使用以下部署规则按 ASM 或 ABM 共享状态筛选资源：

```
Deploy this resource regarding ASM or ABM shared mode

only

unshared
```

或：

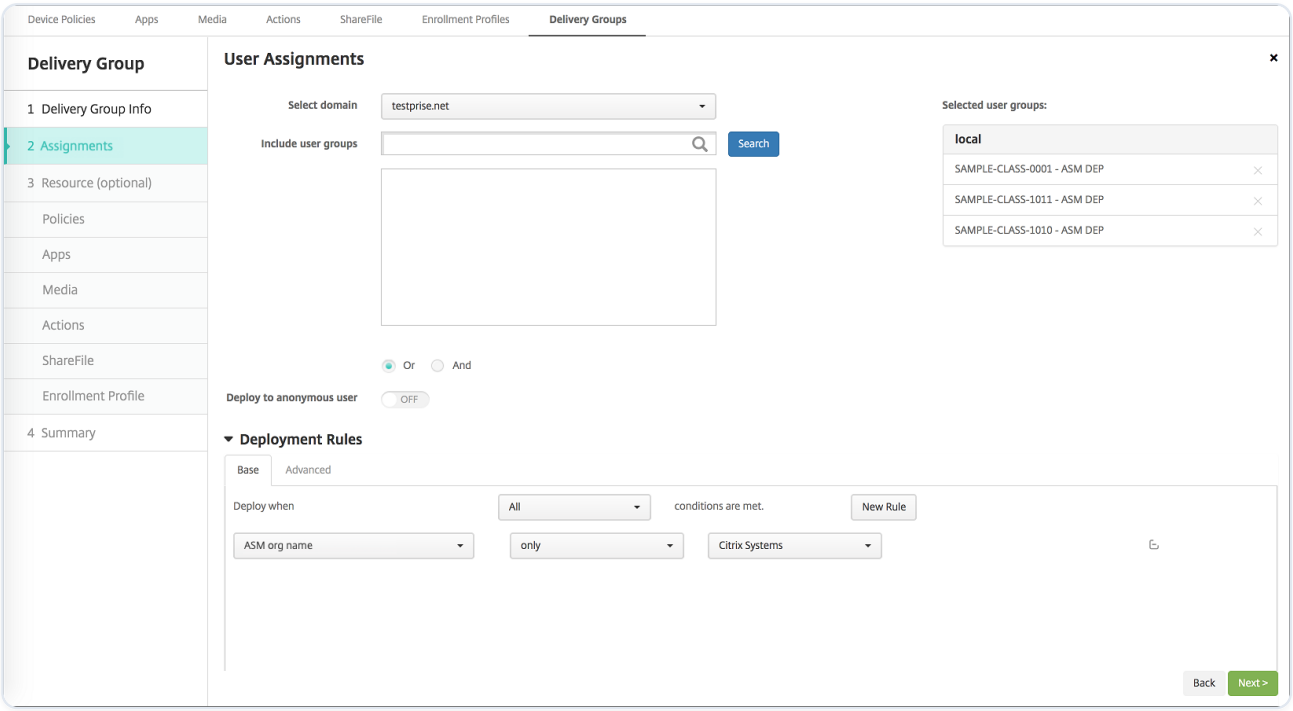
```
Deploy this resource regarding ASM or ABM shared mode

except

shareable
```



适用于共享 iPad 的交付组

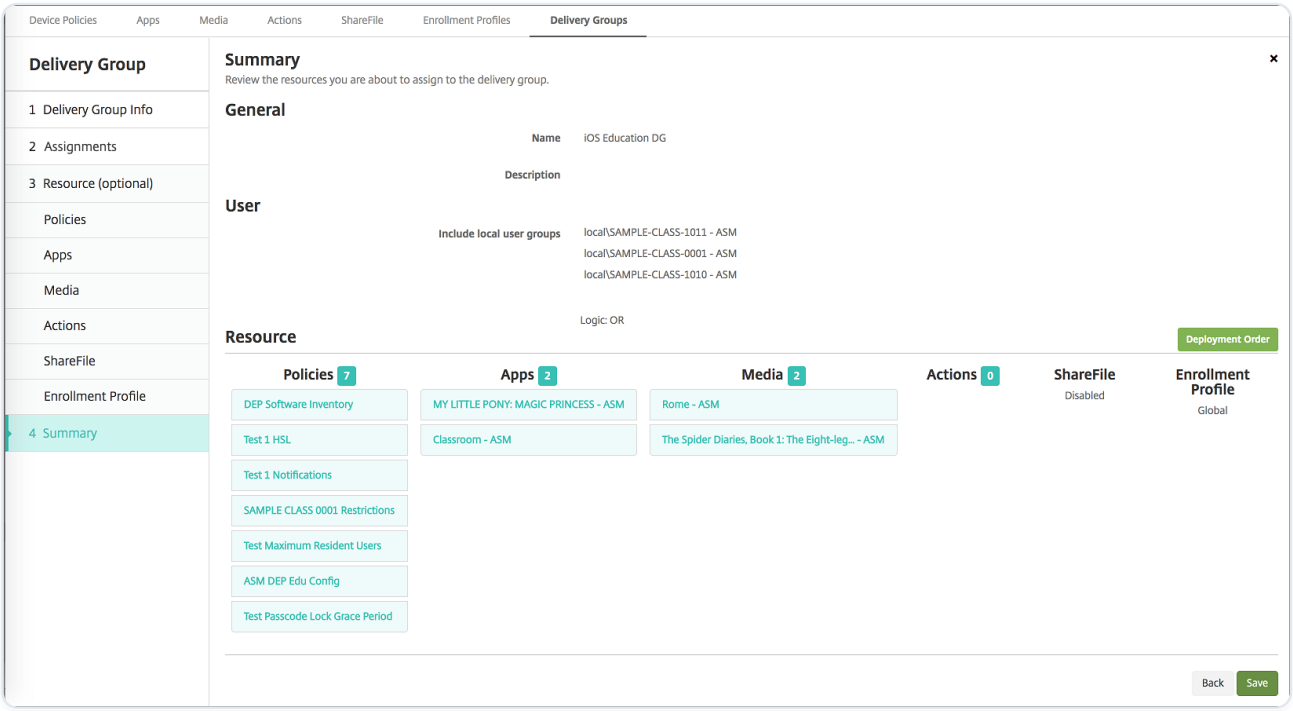
对于每位教师的设备组：

- 配置一个交付组。对于教师，分配“教育配置”策略定义的所有班级。



- 该交付组必须包含以下 MDM 资源：
  - 设备策略：
    - 教育配置

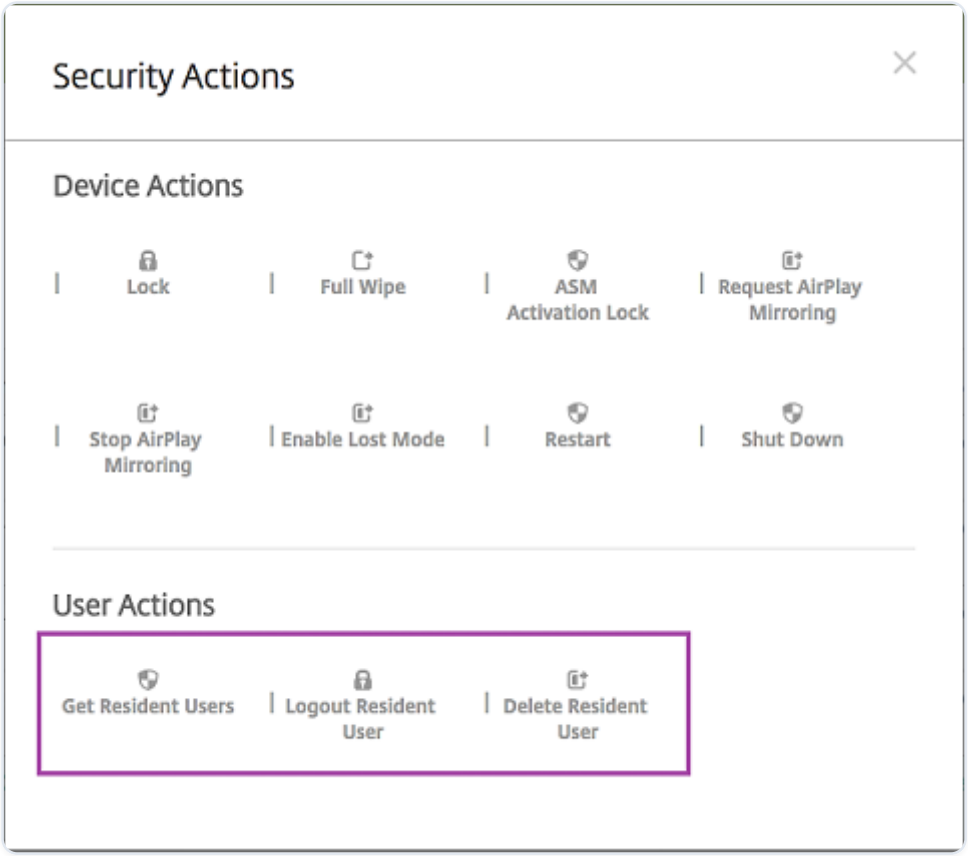
    - 应用程序通知
    - 主屏幕布局
    - 限制
    - 最大常驻用户数
    - 密码锁定宽限期
  - 必需的批量购买应用程序
  - 必需的批量购买 iBooks



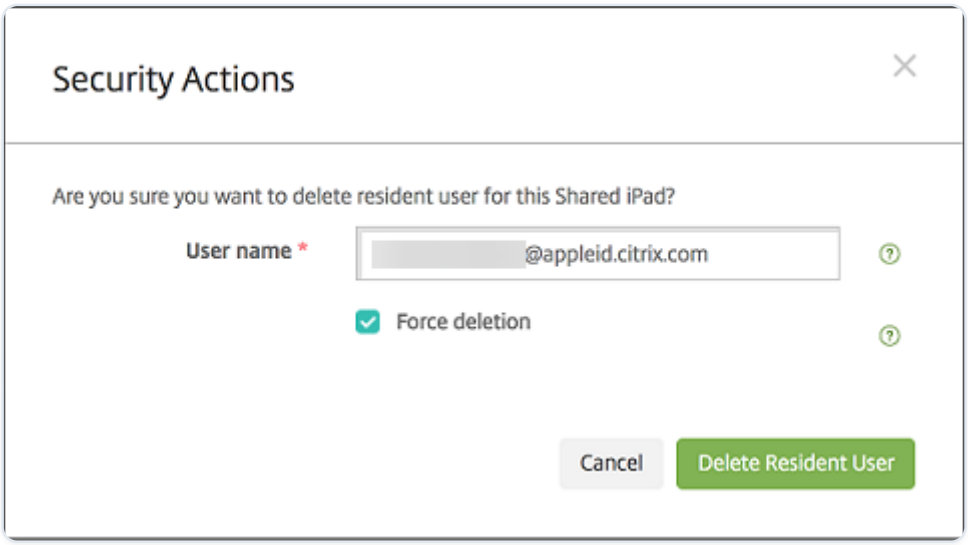
共享 iPad 的安全操作

除了现有安全操作之外，您还可以对共享 iPad 使用以下安全操作：

- **获取常驻用户：**列出当前设备上拥有活动帐户的用户。此操作会强制设备与 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。用户可以再次登录。
- **删除所有用户：**删除设备上的所有用户。



单击**删除常驻用户**后，您可以指定用户名。



安全操作的结果显示在**管理** > **设备** > **常规**和**管理** > **设备** > **交付组**页面上。

获取有关共享 iPad 的信息

在**管理** > **设备**页面上查找有关共享 iPad 的特定信息：

- 查找：
  - 设备是否共享（**ASM 或 ABM 共享**）
  - 谁登录到共享设备（**ASM 或 ABM 登录用户**）

  - 分配给共享设备的所有用户（**ASM 或 ABM 常驻用户**）

设备配置屏幕(/en-us/xenmobile/server/media/manage-devices-shared-ipad-columns.png)

- 按设备的 **ASM 或 ABM 设备状态**筛选设备列表：

设备配置屏幕(/en-us/xenmobile/server/media/manage-devices-shared-ipad-filtered.png)

- 在 **管理** > **设备** > **已登录用户属性** 页面上，查看已登录共享 iPad 的用户的详细信息。

设备配置屏幕(/en-us/xenmobile/server/media/manage-devices-logged-in-user-properties.png)

设备配置屏幕(/en-us/xenmobile/server/media/manage-devices-logged-in-user-properties-details.png)

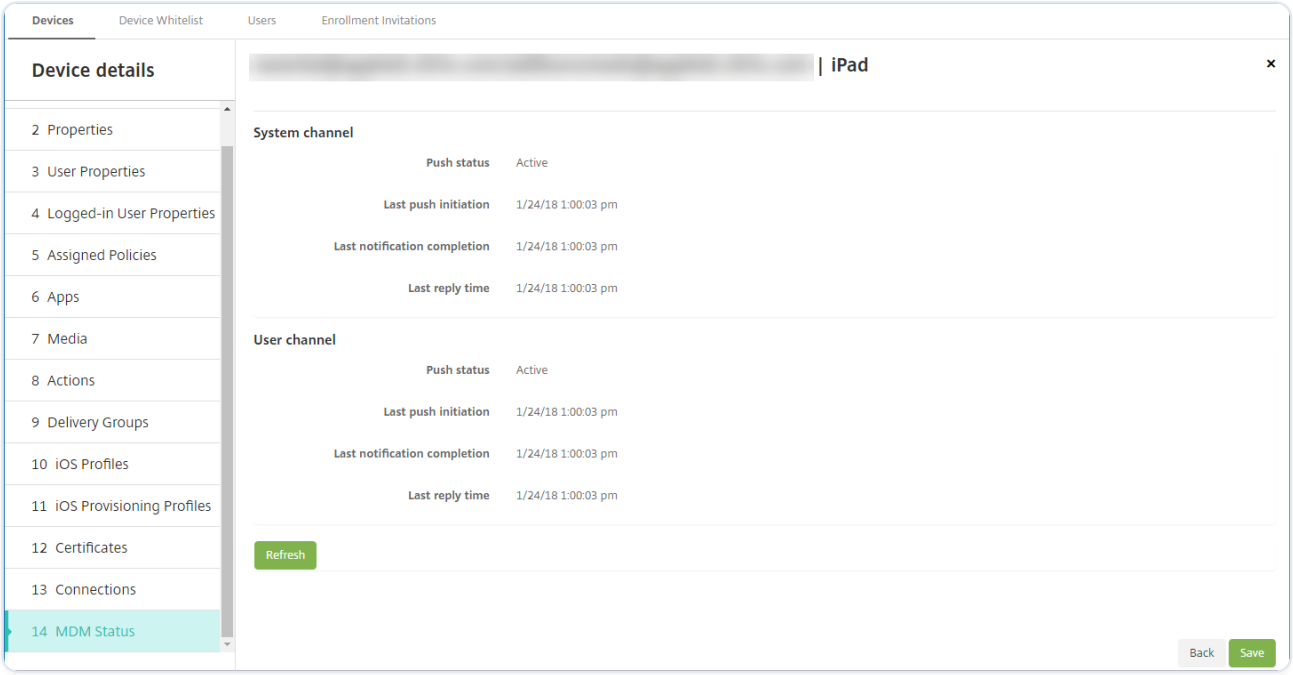
- 在 **管理** > **设备** > **交付组** 页面上，查看用于向交付组中的教师和用户部署资源的通道。**通道/用户** 列显示类型（**系统** 或 **用户**）和接收者（教师或学生）。

设备配置屏幕(/en-us/xenmobile/server/media/manage-devices-delivery-groups-details.png)

- 获取常驻用户的信息：
  - **有要同步的数据：** 用户是否有要同步到云的数据。
  - **数据配额：** 为用户设置的以字节为单位的数据配额。如果用户配额暂时关闭或未对用户强制执行，则可能不会显示配额。
  - **已用数据：** 用户已用数据的字节数。如果系统收集信息时发生错误，则可能不会显示值。
  - **已登录：** 用户是否已登录设备。

设备配置屏幕(/en-us/xenmobile/server/media/manage-devices-connections.png)

- 查看两个通道的推送状态。



分发 Apple 应用程序

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）**：这些应用程序包括在公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。例如，GoToMeeting。
- **企业（iOS/iPadOS/macOS）**：未启用 MDX 且不具有与 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 准备或使用 MDX Toolkit 封装的应用程序。这些应用程序包含 MDX 策略。您可以从内部源和公共商店获取 MDX 应用程序。
- **批量采购（iOS/iPadOS/macOS）**：通过 Apple 批量采购计划管理许可证的应用程序。
- **iOS 自定义应用程序（仅限 iOS/iPadOS）**：内部开发或由第三方开发的专有企业对企业应用程序。

有关不同类型应用程序的更多信息，请参阅添加应用程序。

某些部署需要 Apple Business Management (ABM) 或 Apple School Management (ASM) 帐户。有关详细信息，请参阅以下部分。

对于每种应用程序类型和分发方法，Citrix 都建议一套配置实践。有关分发其他平台应用程序的信息，请参阅添加应用程序。以下部分提供了有关 iOS 应用程序配置的更深入信息。

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
(#public-app-store-apps)，包括 Citrix® 移动应用程序	不适用	**在 XenMobile® 中：配置 > 应用程序**，添加适用于 iPhone 或 iPad 的**公共应用商店**应用程序。配置应用程序并将其分配给交付组。	**在 XenMobile 中：**使用交付组配置和部署应用程序。
(#public-app-store-apps-delivered-with-apple-volume-purchase)，包括 Citrix 移动应用程序	注册 Apple 部署计划。**在 XenMobile 中：** 转到**设置 > 批量购买**以添加您的批量购买帐户。	**在 ABM 或 ASM 中：** 从“应用程序和图书”购买并添加应用程序。**在 XenMobile 中：** 转到**配置 > 应用程序**，配置应用程序并将其分配给交付组。	**在 XenMobile 中：**使用交付组配置和部署应用程序。
(#enterprise-apps)	不适用	**在 XenMobile 中：**转到**配置 > 应用程序**。单击**添加**，然后单击**企业**。上传 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。
(#mdx-apps)	不适用	**在 XenMobile 中：**转到**配置 > 应用程序**。单击**添加**，然后单击 **MDX**。确保为平台选择 **iPad/iPhone**。上传 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 批量采购分发的 MDX 应用程序	注册 Apple 部署计划。**在 XenMobile 中：** 转到**设置 > 批量采购**以添加您的批量采购帐户。	**在 ABM 中：** 从“应用和图书”购买并添加 MDX 应用程序。将应用程序链接到您的 ABM 帐户。**在 XenMobile 中：** 转	**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
		到**配置 > 应用程序**，配置应用程序，并将其分配给交付组。	
自定义应用程序	注册 Apple 部署计划。**在 XenMobile 中：** 转到**设置 > 批量采购**以添加您的批量采购帐户。	**在 ABM 中：** 将您的应用程序作为私有应用程序添加到 App Store。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，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。
启用 MDX 的自定义应用程序	注册 Apple 部署计划。**在 XenMobile 中：** 转到**设置 > 批量采购**以添加您的批量采购帐户。	**在 ABM 中：** 将您的应用程序作为私有应用程序添加到应用商店。将应用程序链接到您的 ABM 帐户。**在 XenMobile 中：** 转到**配置 > 应用程序**并上传 MDX 文件。配置应用程序并将其分配给交付组。	**在 XenMobile 中：** 使用交付组配置和部署应用程序。

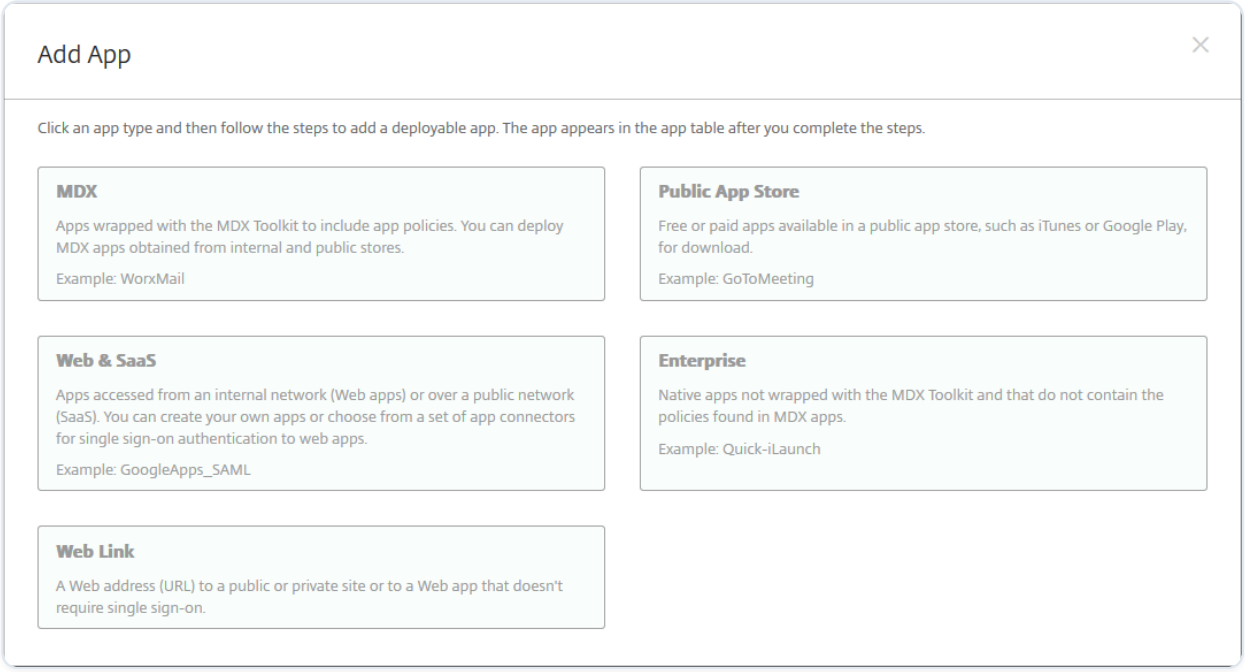
公共应用商店应用程序

您可以将 App Store 上提供的免费和付费应用程序添加到 XenMobile。

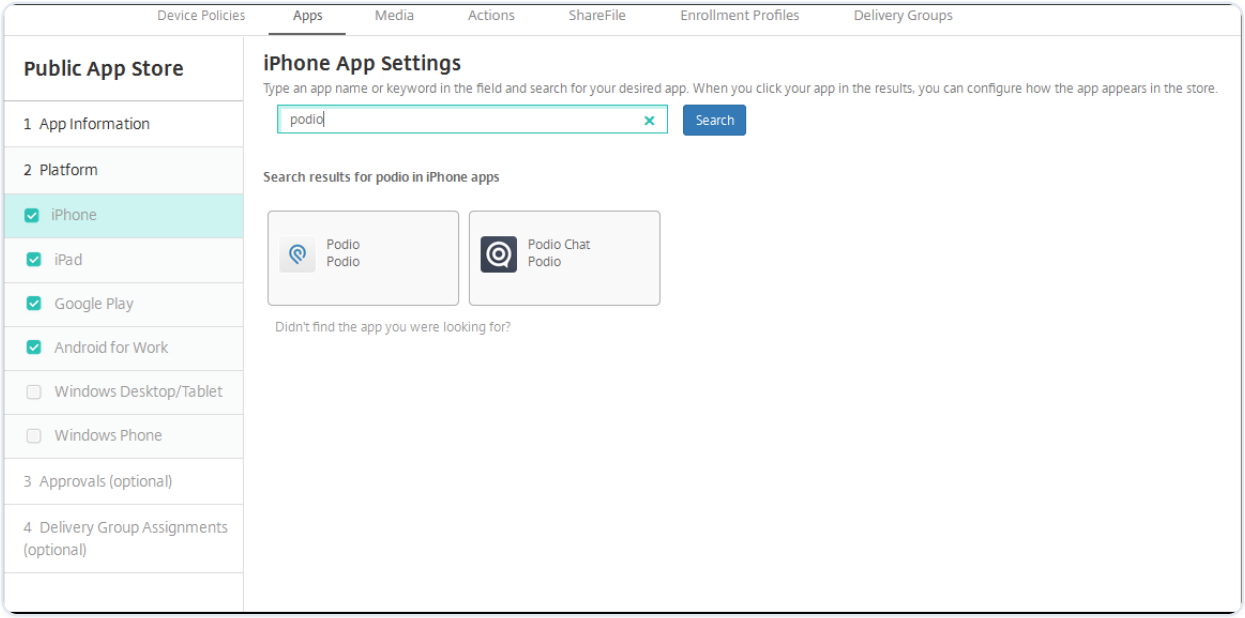
功能可用性	
需要设备监管	否
适用于用户注册模式	否
可用于	iOS/iPadOS

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**。

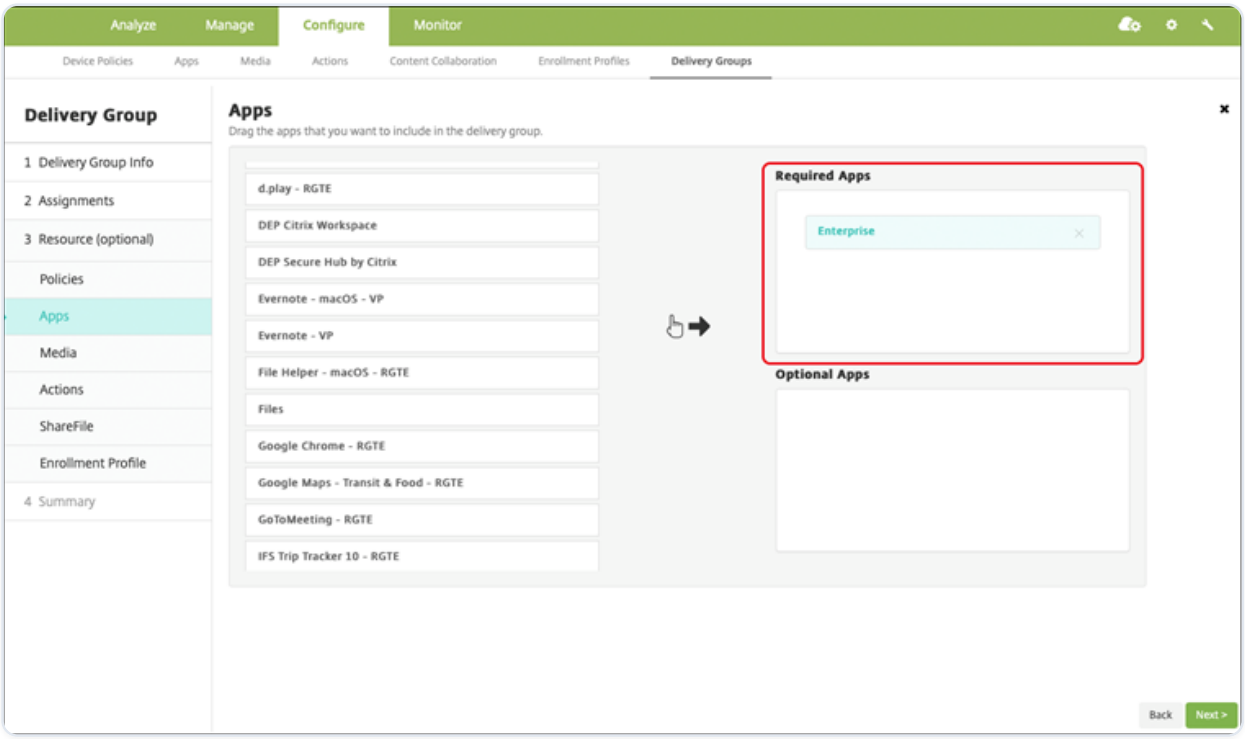


5. 出现与搜索条件匹配的应用程序。单击所需的应用程序。
6. 将交付组分配给应用程序，然后单击 **保存**。

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 **强制应用程序受管** 功能。
4. 分配任何交付组，然后单击 **保存**。
5. 导航到 **配置 > 交付组 > 应用程序**。
6. 将所需的应用程序标记为 **必需**。



7. 导航回 **配置 > 交付组**。
8. 选择交付组，然后单击 **部署**。

9. 用户会收到安装应用程序的请求，接受后应用程序会在后台安装。

通过 Apple 批量采购交付的公共应用商店应用程序

您可以通过 Apple 批量采购计划管理 iOS/iPadOS 应用程序许可证。请按照以下步骤将批量采购应用程序添加到 XenMobile。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
适用于	iOS/iPadOS/macOS

步骤 1：链接帐户

1. 设置并注册 Apple Business Manager (ABM) 或 Apple School Manager (ASM)。有关这些程序的更多信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 XenMobile 链接。有关链接批量购买帐户的更多信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，请启用 **App 自动更新**。此设置可确保当 Apple Store 中出现更新时，用户设备上的应用程序会自动更新。

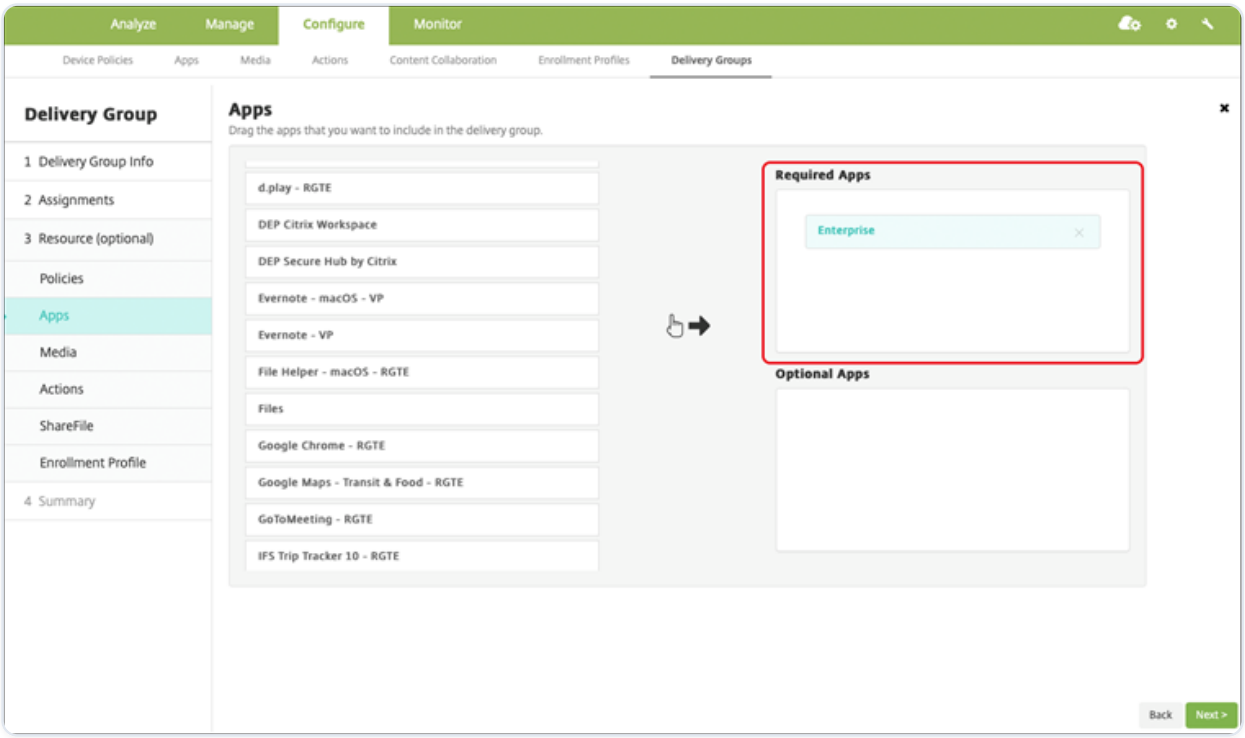
步骤 2：从 Apple 获取应用程序和许可证

在您的 ABM/ASM 帐户中添加应用程序。您可以从 Apple App Store 或 Apple Books（仅限 iOS/iPadOS）添加购买项。请记住，您必须购买所有应用程序，即使它们是免费的。

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 **Configure > Apps**。
2. 选择要配置的批量购买应用程序，然后单击 **Edit**。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. Citrix 建议启用**强制应用程序受管**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，然后单击**部署**。

10. 用户收到安装应用程序的请求，并在他们接受后在后台安装应用程序。

企业应用程序

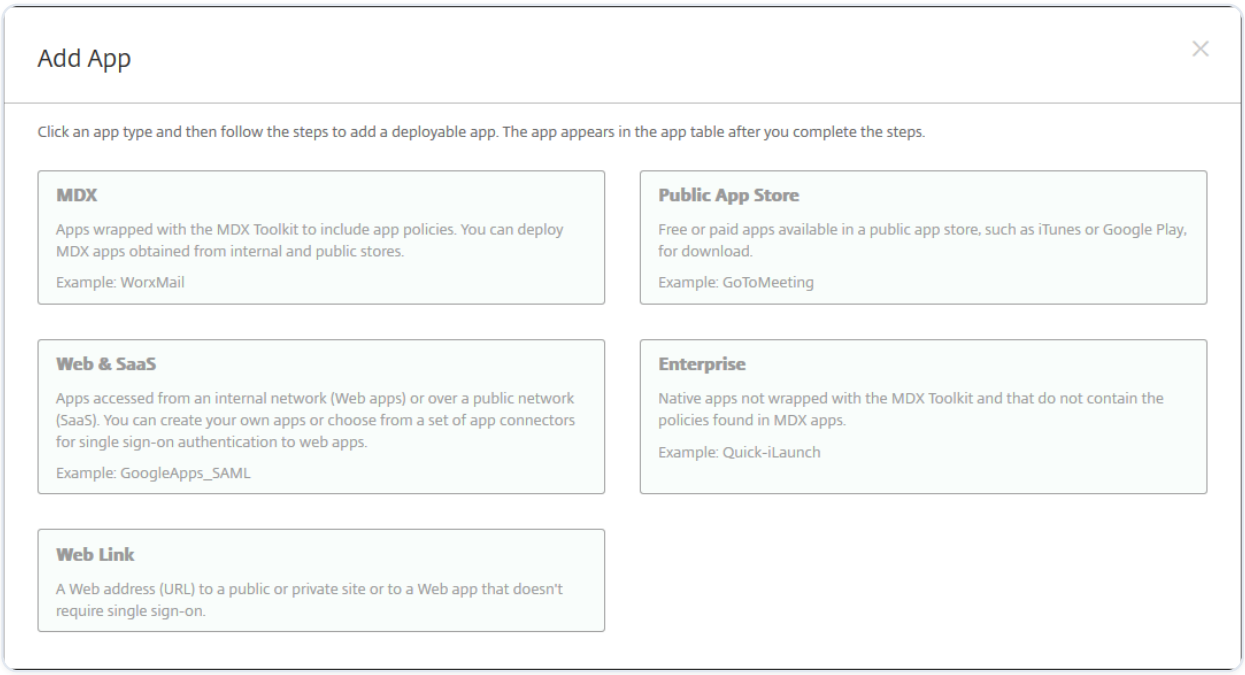
您还可以添加未关联任何 MDX 策略的本机应用程序。请按照以下步骤添加 App Store 中不存在的应用程序。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
操作系统	iOS/iPadOS/macOS

步骤 1：添加和配置应用程序

1. 在 XenMobile 控制台中，导航到 **Configure > Apps**。单击 **Add**。

2. 单击 **Enterprise**。



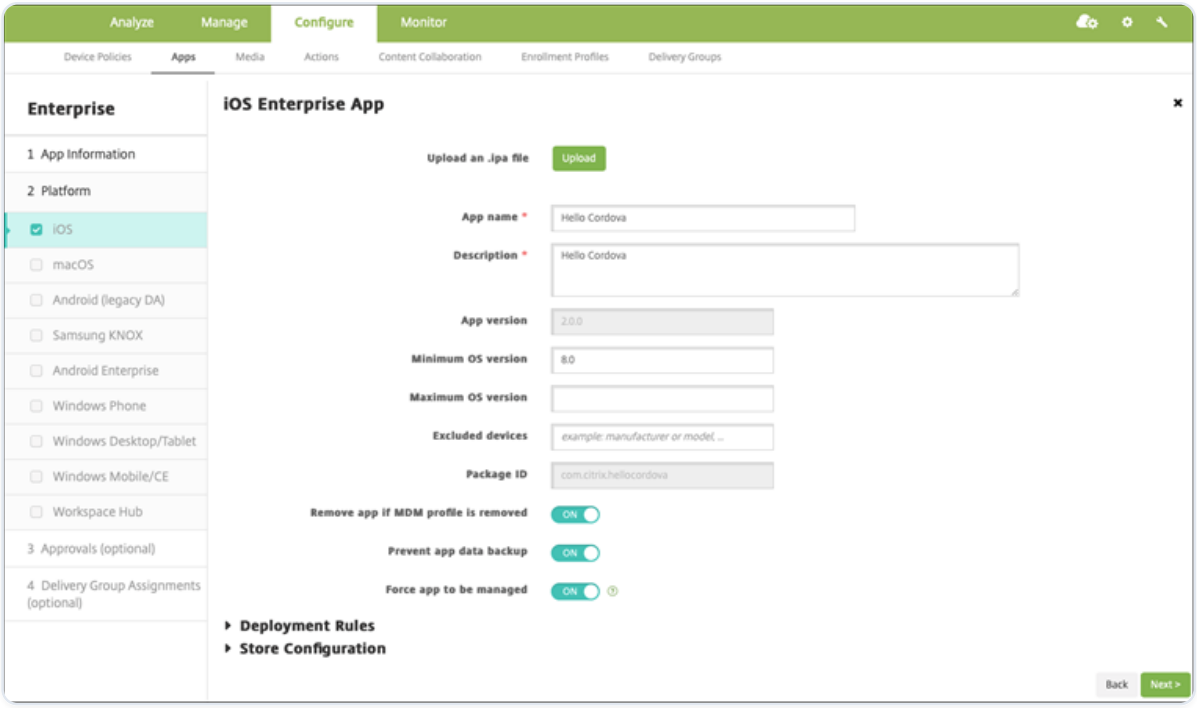
3. 在 **App information** 页面上，配置以下内容：

   - **Name:** 键入应用程序的描述性名称。该名称将显示在“Apps”表中的“App Name”下。
   - **Description:** 键入应用程序的可选描述。
   - **App category:** （可选）在列表中，单击要添加应用程序的类别。

4. 单击 **Next**。将显示 **App Platforms** 页面。
5. 选择平台：**iPhone**、**iPad** 或 **macOS**。
6. 上传 IPA 文件 (iOS/iPadOS) 或上传 PKG 文件 (macOS)
7. 单击 **Next**。将显示 **App details** 页面。
8. 配置以下设置：

   - **File name:** （可选）键入应用程序的新名称。
   - **App description:** （可选）键入应用程序的新描述。
   - **App version:** 您无法更改此字段。
   - **最低操作系统版本：** （可选）键入设备可运行以使用此应用的最旧操作系统版本。
   - **最高操作系统版本：** （可选）键入设备必须运行以使用此应用的最新操作系统版本。
   - **排除的设备：** （可选）键入无法运行此应用的设备的制造商或型号。
   - **如果 MDM 配置文件已删除，则删除应用：** 选择当 MDM 配置文件被删除时是否从设备中删除此应用。默认设置为“开”。（仅限 iOS/iPadOS）

- **阻止应用数据备份：** 选择是否阻止此应用备份数据。默认设置为“开”。（仅限 iOS/iPadOS）
- **强制应用受管：** 如果您安装了非受管应用，如果您希望非受管设备上的用户看到允许管理应用的提示，请选择“**开**”。如果他们接受提示，则该应用将受管。（仅限 iOS/iPadOS）

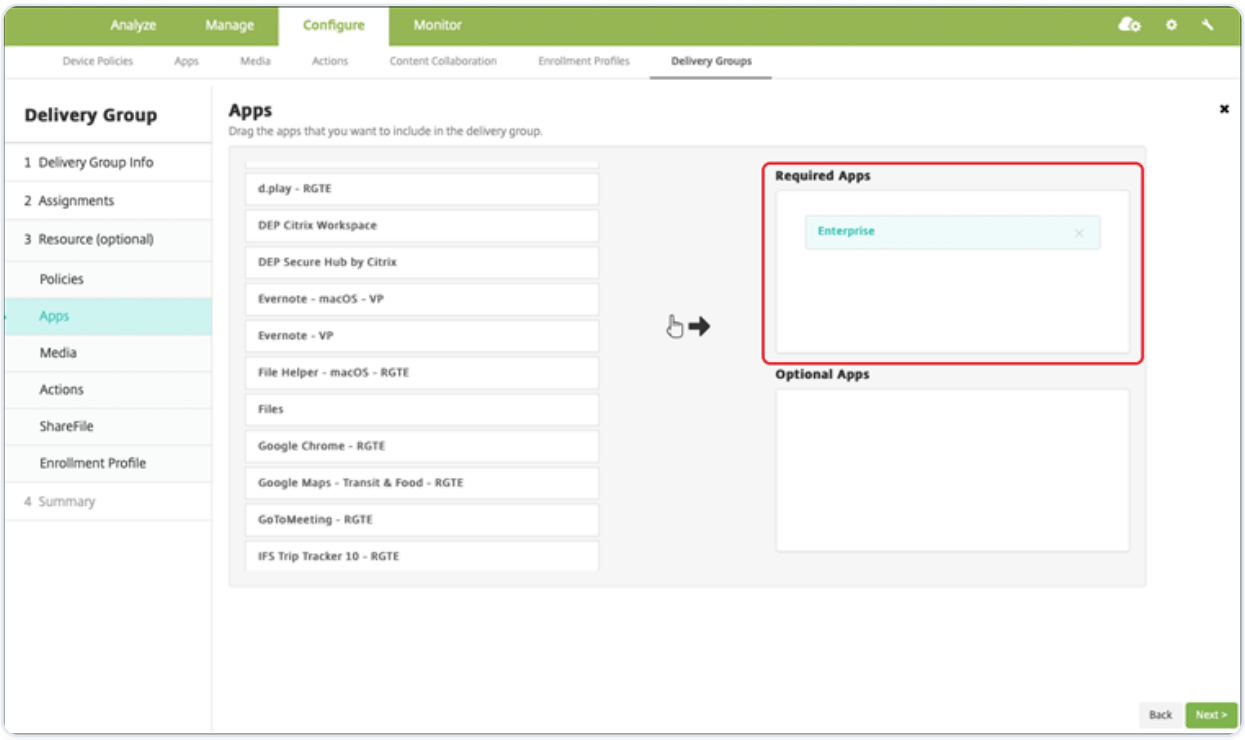


9. 将交付组分配给此应用，然后单击“**保存**”。

步骤 2：配置应用部署

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**”页面。

2. 将所需应用标记为“**必需**”。



3. 导航到“**配置 > 交付组**”。

4. 选择交付组，然后单击“**部署**”。

5. 用户会收到安装应用的请求，接受后应用会在后台安装。

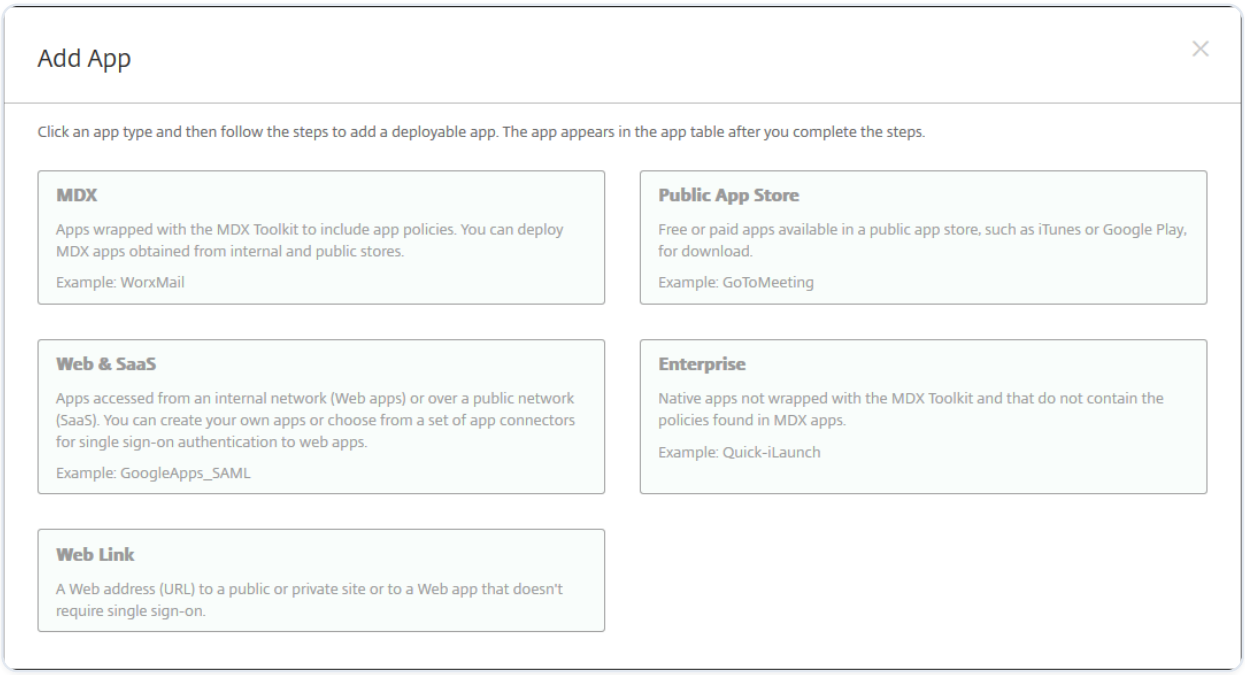
MDX 应用

要使用 MDX 策略和安全功能，请添加已启用 MAM SDK 或已进行 MDX 包装的应用。您可以使用批量购买或不使用批量购买来部署 MDX 应用。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
可用平台	iOS/iPadOS

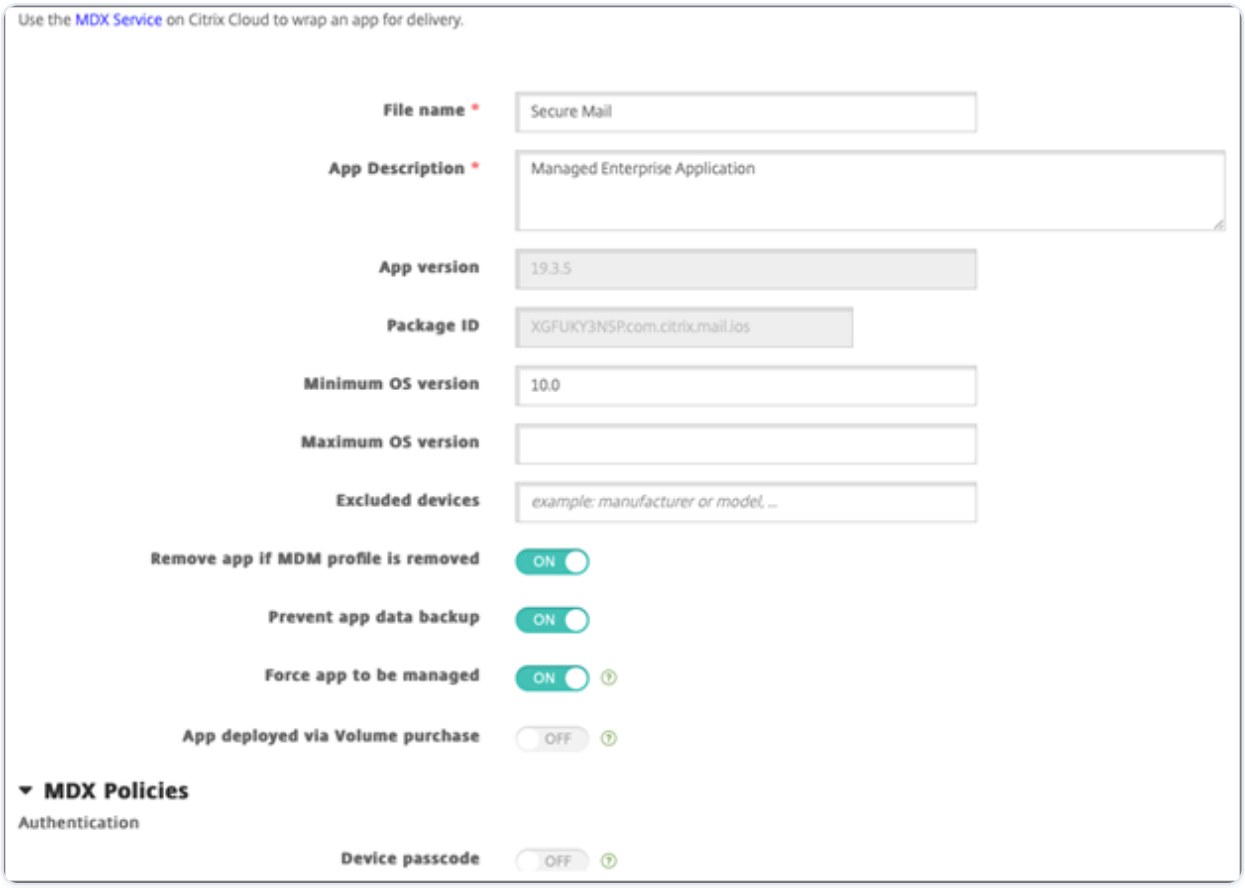
步骤 1：添加和配置应用程序

1. 在 XenMobile 控制台中，导航到 **Configure > Apps**。单击 **Add**。
2. 单击 **MDX**。

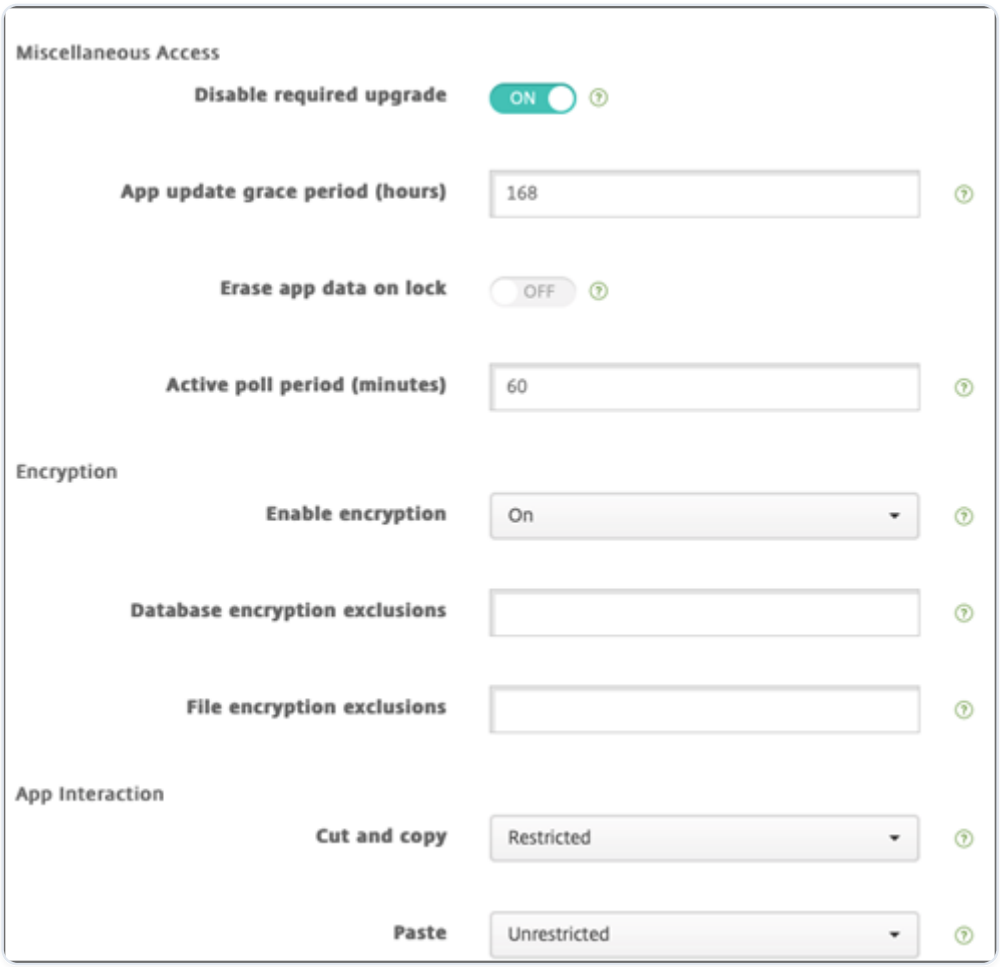


3. 为平台选择 **iPhone** 或 **iPad**。
4. 上传 MDX 文件。

5. 配置应用程序详细信息。将 **App deployed via Volume purchase** 设置为 **Off**。Citrix 还建议启用 **Force app to be managed** 功能。



6. 配置 MDX 策略。将 **Disable required upgrade** 设置为 **On**。

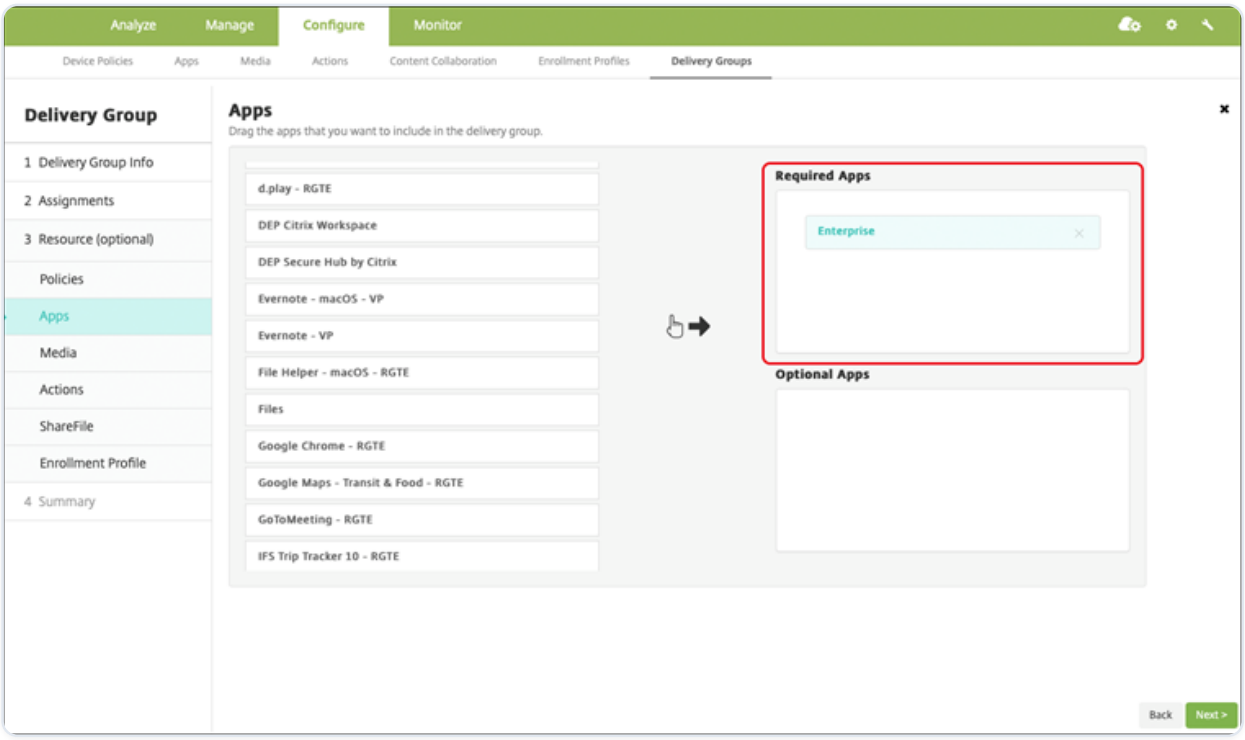


7. 将交付组分配给应用程序，然后单击 **Save**。

步骤 2: 配置应用程序部署

1. 在 XenMobile 控制台中，导航到 **Configure > Delivery Groups > Apps**。

2. 将所需应用程序标记为 **Required**。



3. 导航到 **配置 > 交付组**。

4. 选择交付组并单击 **Deploy**。

5. 用户会收到安装应用程序的请求，接受后，应用程序会在后台安装。

使用 Apple 批量采购分发的 MDX 应用程序

要使用 MDX 策略和安全功能，请添加已启用 MAM SDK 或已进行 MDX 包装的应用程序。要使用批量采购部署应用程序，应用程序必须存在于应用商店中。

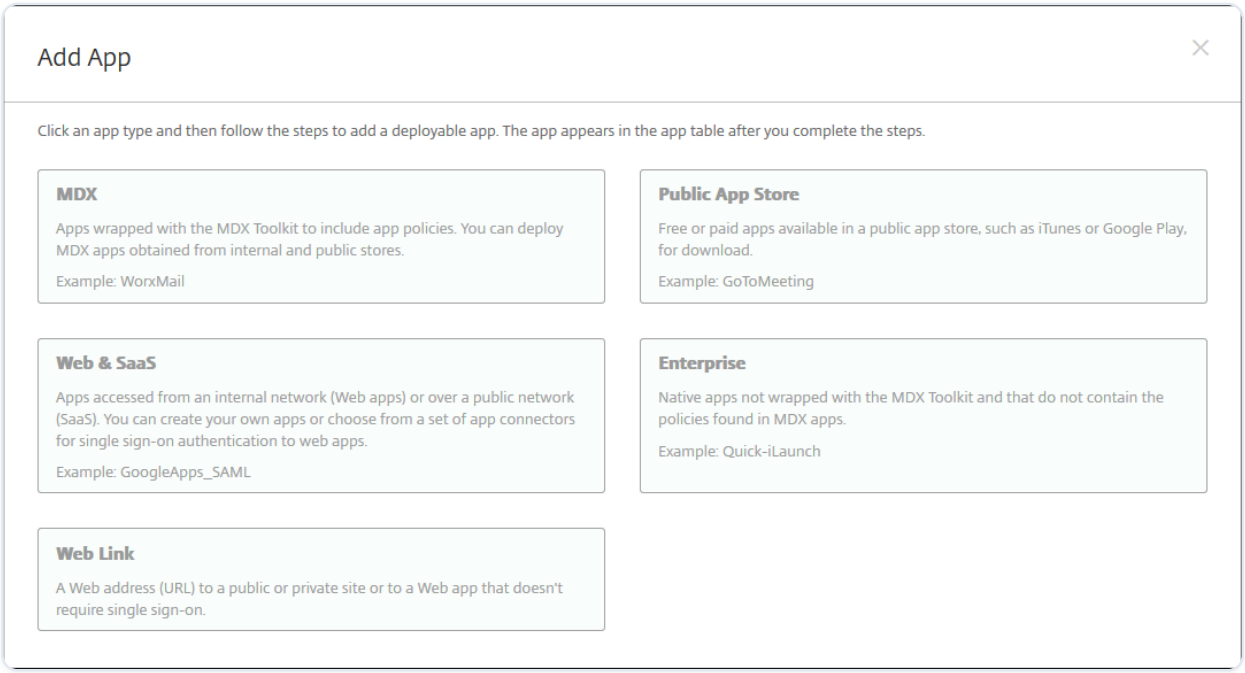
功能可用性	
需要设备监管	否
适用于用户注册模式	是
适用于	iOS/iPadOS

步骤 1：链接帐户

1. 设置并注册 Apple Business Manager (ABM) 或 Apple School Manager (ASM)。有关这些程序的更多信息，请参阅 Apple 文档。
2. 将您的 ABM/ASM 帐户与 XenMobile 链接。有关链接批量购买帐户的更多信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，启用**应用程序自动更新**。此设置可确保当 Apple Store 中出现更新时，用户设备上的应用程序会自动更新。

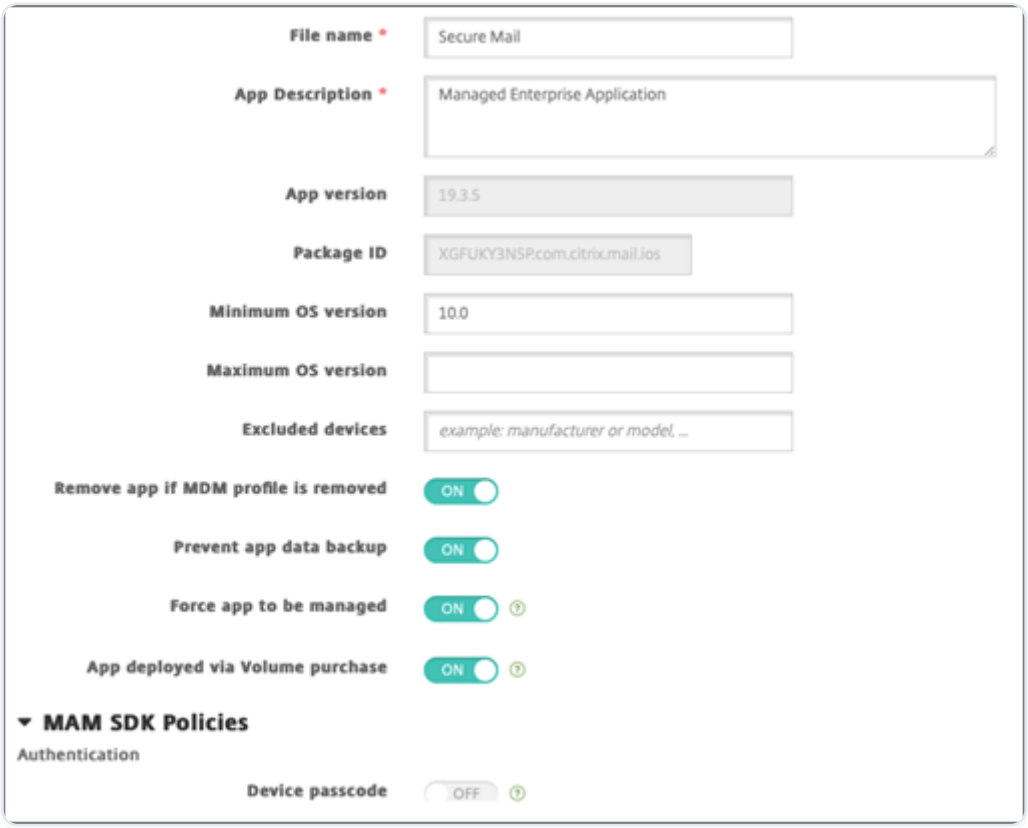
步骤 2：添加和配置应用程序

1. 在 XenMobile 控制台中，导航到**配置 > 应用程序**。单击**添加**。
2. 单击 **MDX**。

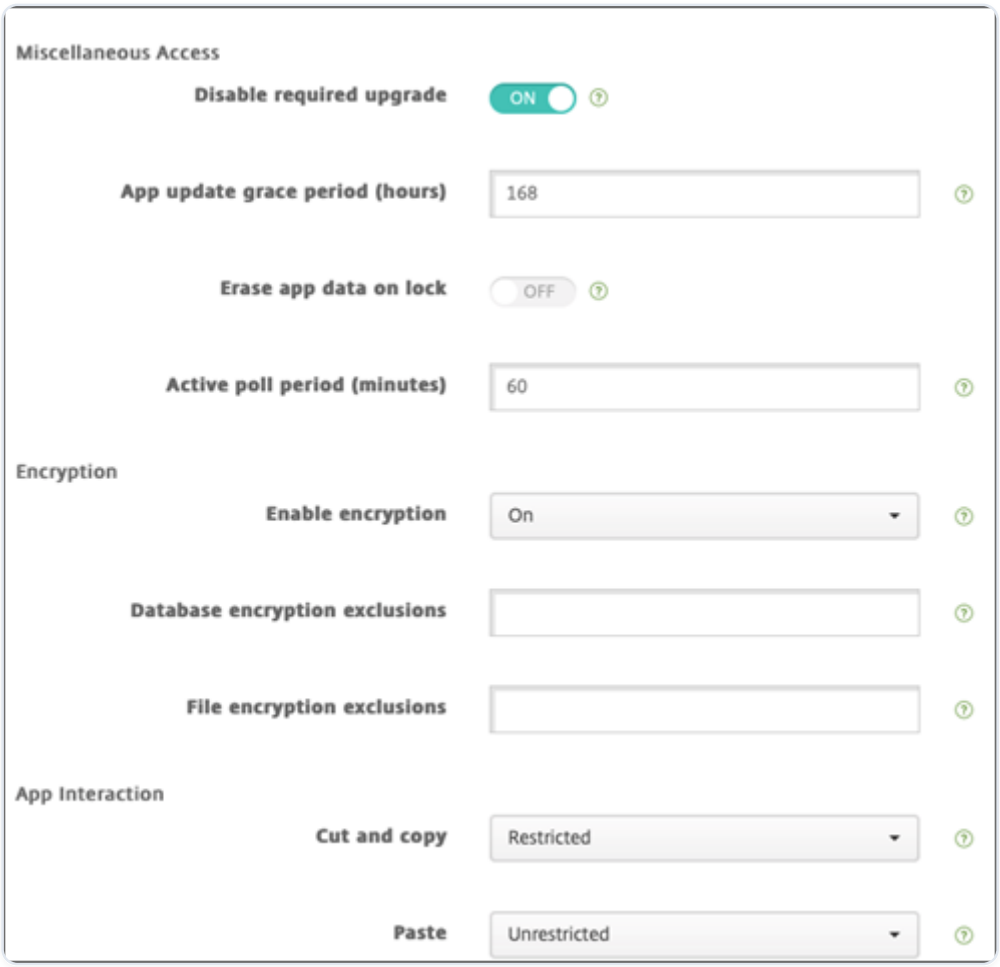


3. 为平台选择 **iPhone** 或 **iPad**。

4. 上传 MDX 文件。
5. 配置应用程序详细信息。将**通过批量购买部署的应用程序**设置为**开**。Citrix 还建议启用**强制管理应用程序**功能。



6. 配置 MDX 策略。将**禁用强制升级**设置为**开**。



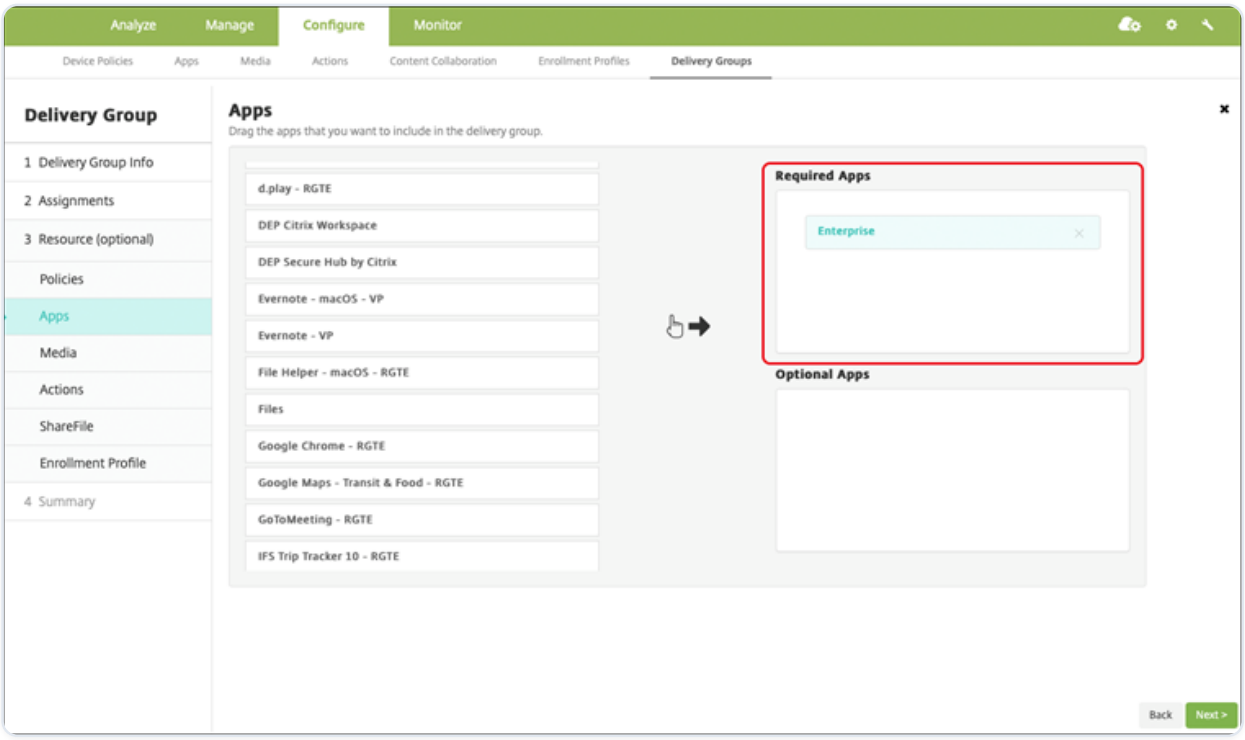
7. 为每个平台将交付组分配给应用程序，然后单击**保存**。

此配置会导致此应用程序在应用程序列表中列出两个条目。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标记为“**必需**”。



3. 导航到“**配置 > 交付组**”。
4. 选择交付组，然后单击“**部署**”。
5. 用户会收到安装应用的请求，接受后应用会在后台安装。

自定义应用

自定义应用是专有的企业对企业应用。您可以使用 XenMobile 和 Apple 批量购买来私密且安全地分发专有应用。您可以将应用分发给特定合作伙伴、客户、特许经营商和内部员工。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
适用于	iOS/iPadOS

自定义应用的要求

- Apple 商务管理或 Apple 教育管理帐户
- Apple 批量采购账户（要求设备运行 iOS 7 或更高版本）
- 使用以下某个 Apple 注册模式，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

要使用批量采购部署自定义应用程序，请将您的批量采购帐户链接到 XenMobile。

1. 设置并注册 Apple Business Manager (ABM)。有关这些程序的更多信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 XenMobile 链接。有关链接批量采购帐户的更多信息，请参阅 Apple 批量采购。
3. 添加批量采购帐户时，请启用 **App Auto Update**。此设置可确保当 Apple Store 中出现更新时，用户设备上的应用程序会自动更新。

步骤 2：在 ABM 上配置应用程序

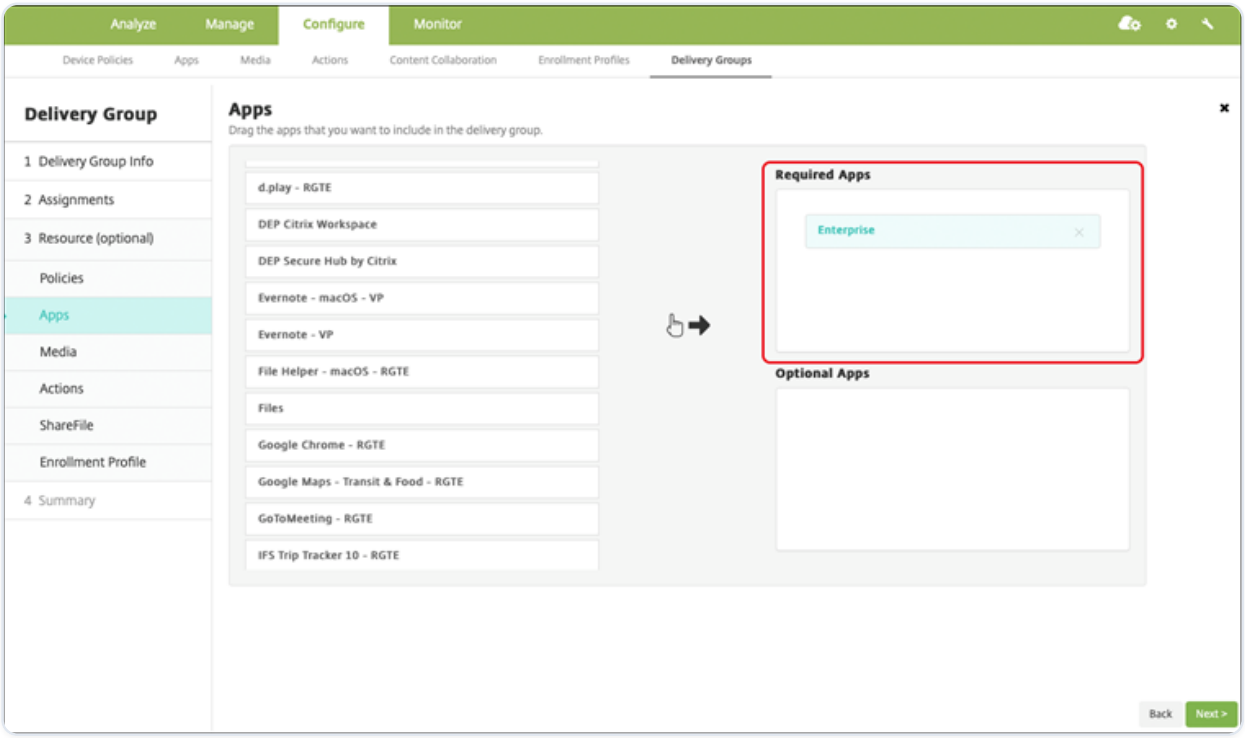
在您的 ABM 帐户上添加应用程序。您可以上传和分发自己的自定义应用程序，或从其他组织购买自定义应用程序的许可证。有关在 ABM 上添加和启用自定义应用程序的更多信息，请参阅 Apple 文档。

步骤 3：在 XenMobile 中添加和配置应用程序

1. 在 XenMobile 控制台中，导航到 **Configure > Apps**。批量采购应用程序将显示在应用程序列表中。
2. 选择要配置的应用程序。单击 **Edit**。
3. 选择平台：**iPhone**、**iPad** 或 **macOS**。
4. 选择要分发应用程序的交付组。单击**保存**。

步骤 4：配置应用程序部署

1. 在 XenMobile 控制台中，导航到 **Configure > Delivery Groups > Apps**。
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. 用户收到部署应用程序的请求。用户接受后，应用程序将在后台安装。

启用 MDX 的自定义应用程序

要使用 MDX 策略和安全功能，请添加已启用 MAM SDK 或已进行 MDX 包装的自定义应用程序。

功能可用性	
需要设备监管	否
适用于用户注册模式	是
适用于	iOS/iPadOS

步骤 1：关联帐户

要使用批量购买部署自定义应用程序，请将您的批量购买帐户关联到 XenMobile。

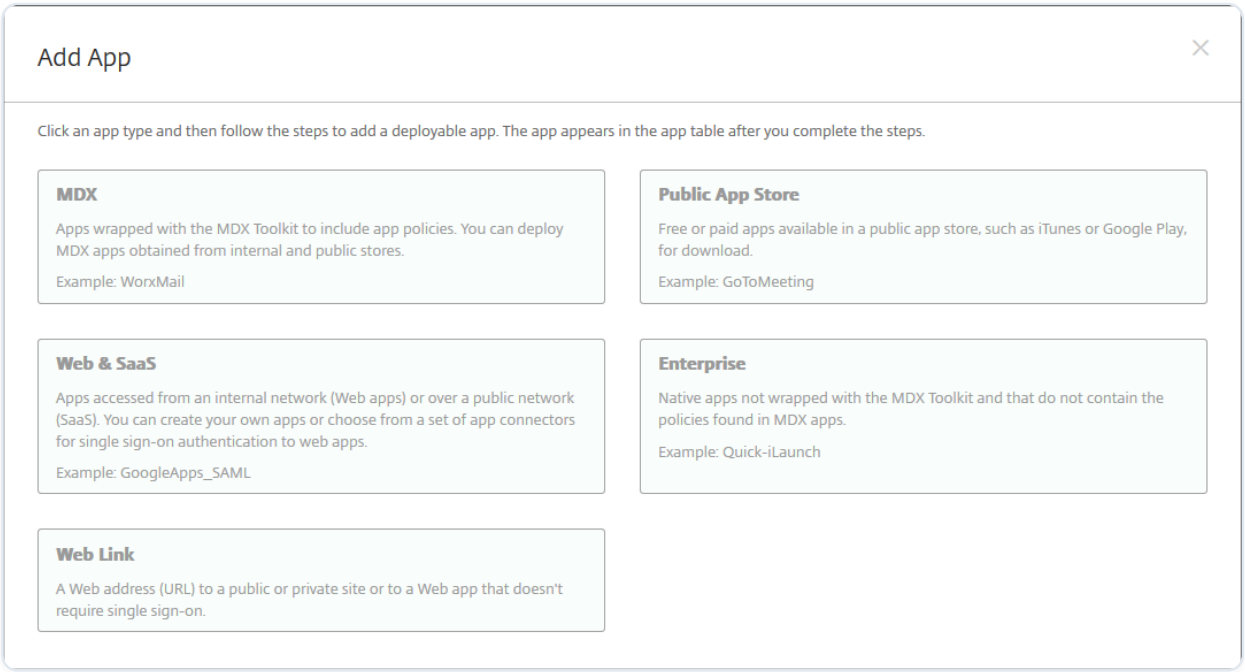
1. 设置并注册 Apple Business Manager (ABM)。有关这些程序的更多信息，请参阅 Apple 文档。
2. 将您的 ABM 帐户与 XenMobile 关联。有关关联批量购买帐户的更多信息，请参阅 Apple 批量购买。
3. 添加批量购买帐户时，请启用 **App Auto Update**（应用程序自动更新）。此设置可确保当 Apple Store 中出现更新时，用户设备上的应用程序会自动更新。

步骤 2：在 ABM 上配置应用程序

在您的 ABM 帐户上添加应用程序。您可以上传和分发自己的自定义应用程序，或从其他组织购买自定义应用程序的许可证。有关在 ABM 上添加和启用自定义应用程序的更多信息，请参阅 Apple 文档。

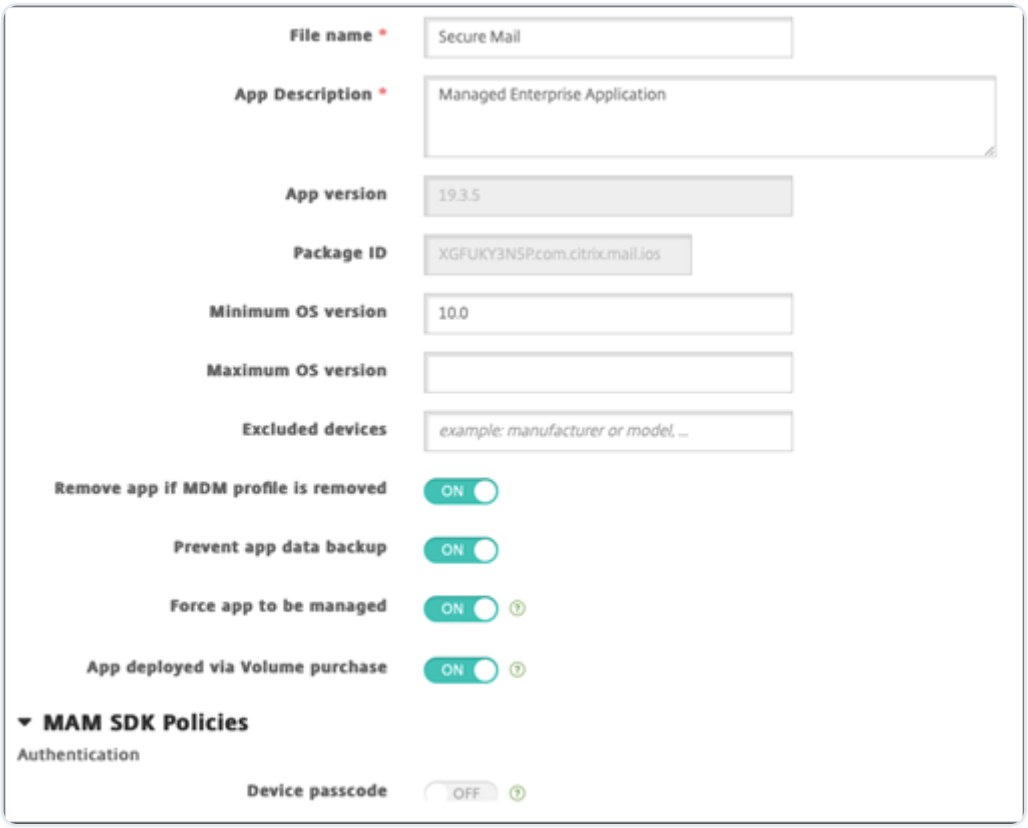
步骤 3：在 XenMobile 中添加和配置应用程序

1. 在 XenMobile 控制台中，导航到 **Configure > Apps**（配置 > 应用程序）。单击 **Add**（添加）。
2. 单击 **MDX**。

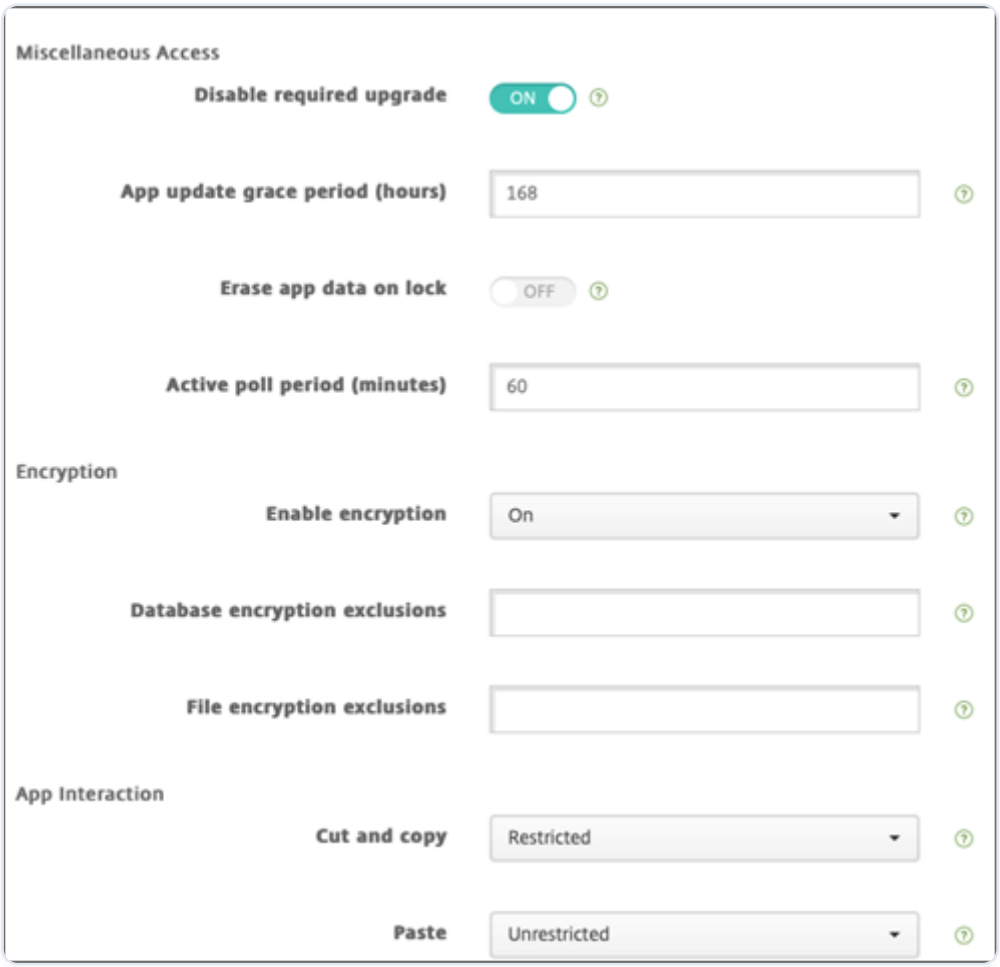


3. 选择 **iPhone** 或 **iPad** 平台。
4. 上传要添加的应用程序的 MDX 文件。

5. 配置应用程序详细信息。将 **App deployed via Volume purchase**（通过批量购买部署的应用程序）设置为 **On**（开）。Citrix 还建议启用 **Force app to be managed**（强制管理应用程序）功能。



6. 配置 MDX 策略。将 **禁用强制升级** 设置为 **开**。



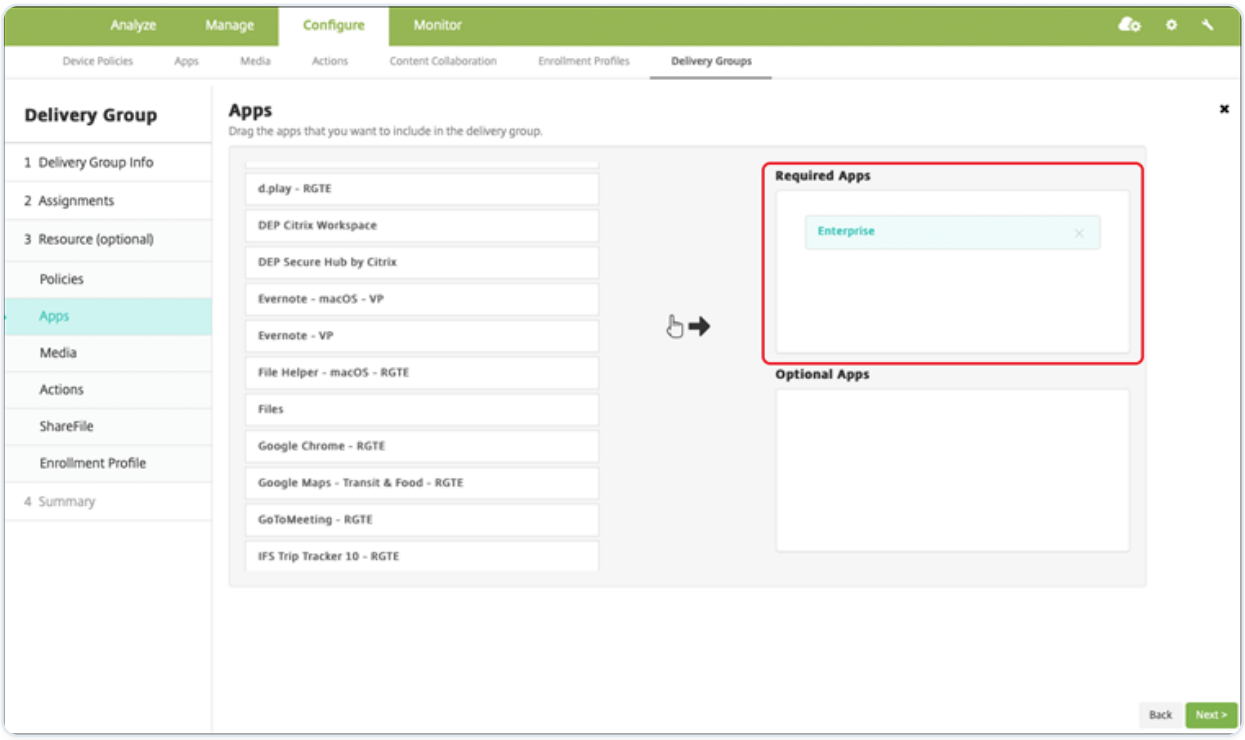
7. 将交付组分配给应用程序，然后单击 **保存**。

此配置会导致此应用程序在应用程序列表中显示两个条目。配置应用程序时，请选择 **类型** 为 **MDX** 的应用程序。

步骤 4：配置应用程序部署

1. 在 XenMobile 控制台中，导航到 **配置 > 应用程序**。批量购买的应用程序将显示在应用程序列表中。
2. 选择要配置的应用程序。单击 **编辑**。
3. 选择要在每个平台上分发应用程序的交付组。单击 **保存**。
4. 导航回 **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**。

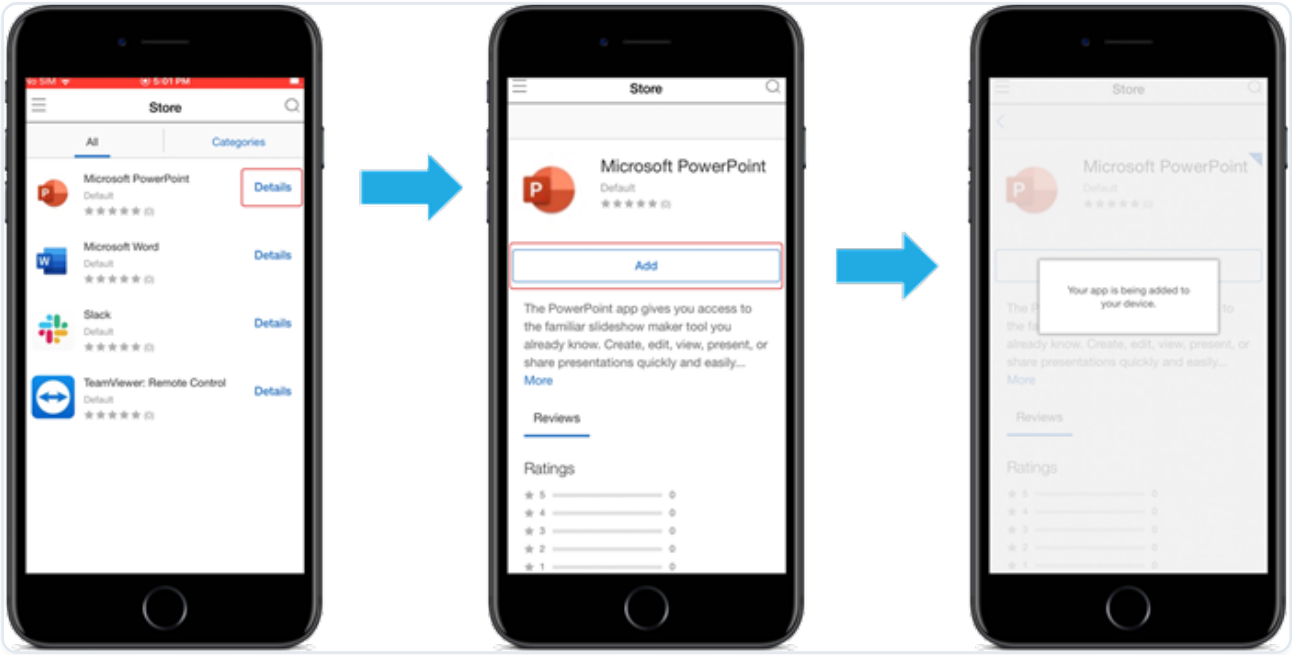
8. 用户会收到部署应用程序的请求。用户接受后，应用程序将在后台安装。

可选应用程序（仅限 iOS/iPadOS）

Citrix 建议将应用程序部署为 **必需**。必需应用程序会在用户设备上静默安装，从而最大程度地减少交互。启用此功能还允许应用程序自动更新。

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，用户必须启动 Secure Hub，转到“**应用商店**”，选择所需应用的“**详细信息**”，然后单击“**添加**”。



网络访问控制

您可以使用网络访问控制 (NAC) 解决方案来扩展适用于 Android 和 Apple 设备的 XenMobile® 设备安全评估。NAC 解决方案使用 XenMobile 安全评估来促进和处理身份验证决策。配置 NAC 设备后，您在 XenMobile 中配置的设备策略和 NAC 筛选器将得到强制执行。

将 XenMobile 与 NAC 解决方案结合使用可为网络内部的设备添加 QoS 和更精细的控制。有关将 NAC 与 XenMobile 集成的优势摘要，请参阅 访问控制。

Citrix® 支持以下解决方案与 XenMobile 集成：

- Citrix 网关
- 思科身份服务引擎 (ISE)
- ForeScout

Citrix 不保证与其他 NAC 解决方案的集成。

在您的网络中使用 NAC 设备时：

- XenMobile 支持 NAC 作为 iOS、Android Enterprise 和 Android 设备的端点安全功能。
- 您可以在 XenMobile 中启用筛选器，根据规则或属性将设备设置为符合或不符合 NAC 规定。例如：
  - 如果 XenMobile 中的托管设备不符合指定条件，XenMobile 会将该设备标记为不合规。NAC 设备会阻止网络上的不合规设备。
  - 如果 XenMobile 中的托管设备安装了不合规应用程序，NAC 筛选器可以阻止 VPN 连接。因此，不合规的用户设备无法通过 VPN 访问应用程序或网站。
  - 如果您将 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 合规性筛选器

XenMobile Server 支持以下 NAC 合规性筛选器：

匿名设备： 检查设备是否处于匿名模式。如果 XenMobile 在设备尝试重新连接时无法重新验证用户身份，则此检查可用。

Samsung Knox 证明失败： 检查设备是否未能查询 Samsung Knox 证明服务器。

禁用应用： 检查设备是否具有禁用应用，如应用访问设备策略中所定义。有关该策略的信息，请参阅应用访问设备策略。

非活动设备： 检查设备是否处于非活动状态，如**服务器属性**中的**设备非活动天数阈值**设置所定义。有关详细信息，请参阅服务器属性。

缺少所需应用： 检查设备是否缺少任何所需应用，如应用访问策略中所定义。

非建议应用： 检查设备是否具有非建议应用，如应用访问策略中所定义。

不合规密码： 检查用户密码是否合规。在 iOS 和 Android 设备上，XenMobile 可以确定设备上当前密码是否符合发送到设备的密码策略。例如，在 iOS 上，如果 XenMobile 向设备发送密码策略，用户有 60 分钟的时间来设置密码。在用户设置密码之前，密码可能不合规。

不合规设备： 根据不合规设备属性检查设备是否不合规。通常，自动化操作或使用 XenMobile API 的第三方会更改该设备属性。

已吊销状态： 检查设备证书是否已吊销。已吊销的设备在再次获得授权之前无法重新注册。

已 Root 的 Android 和已越狱的 iOS 设备： 检查 Android 或 iOS 设备是否已越狱。

未管理设备： 检查设备是否仍处于 XenMobile 控制下的受管理状态。例如，已注册 MAM 的设备或未注册的设备不受管理。

> **注意：**
>
> 隐式合规/不合规筛选器仅在 XenMobile 管理的设备上设置默认值。例如，任何安装了被阻止应用或未注册的设备都会被标记为“不合规”。NAC 设备会阻止这些设备访问您的网络。

配置概述

我们建议您按照列出的顺序配置 NAC 组件。

1. 配置设备策略以支持 NAC：

   对于 iOS 设备： 请参阅 配置 VPN 设备策略以支持 NAC。

   对于 Android Enterprise 设备： 请参阅 为 Citrix SSO 创建 Android Enterprise 托管配置。

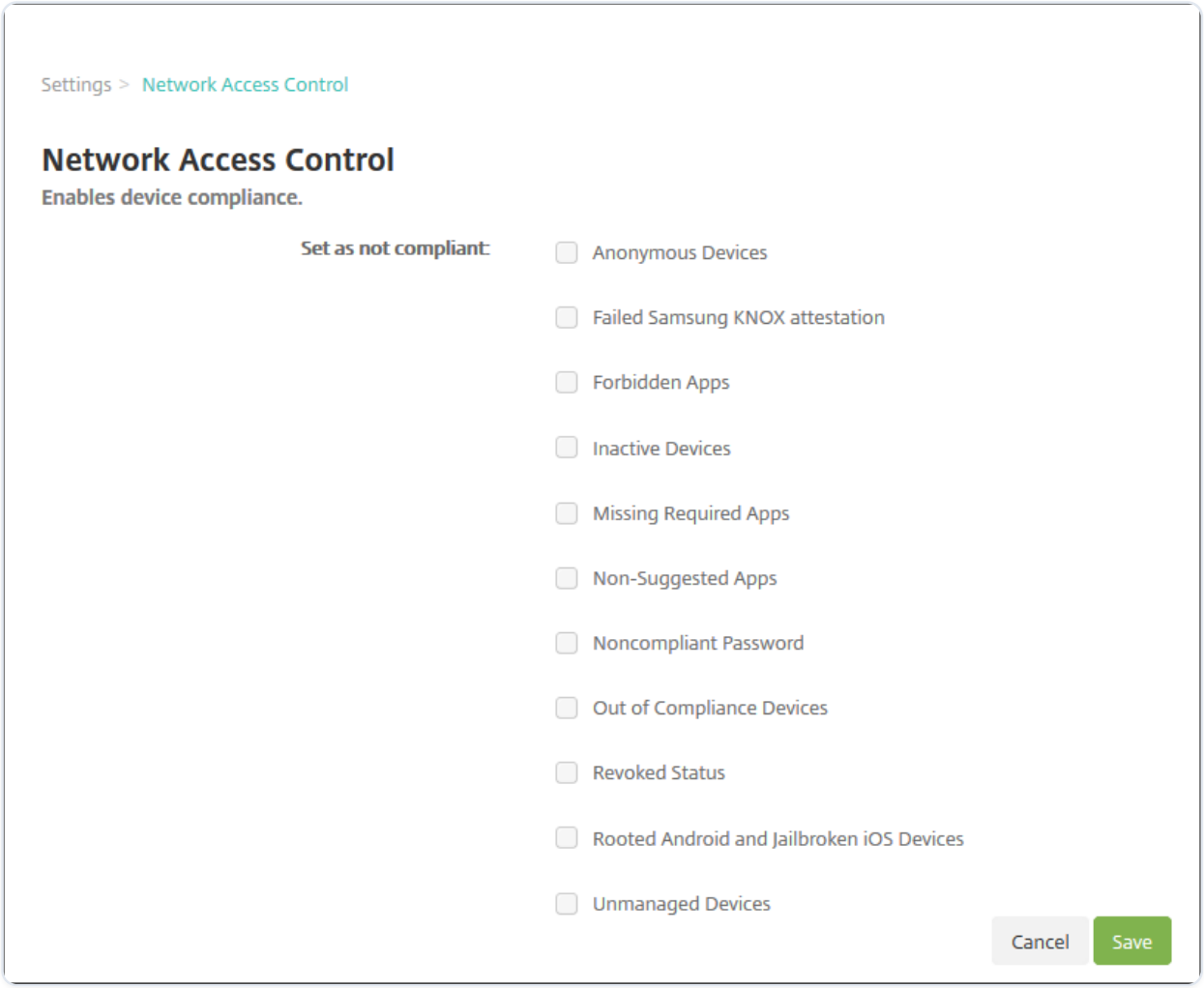
   对于 Android 设备： 请参阅 配置适用于 Android 的 Citrix SSO 协议。
2. 在 XenMobile 中启用 NAC 筛选器。
3. 配置 NAC 解决方案：

   - Citrix Gateway，详细信息请参阅 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 筛选器

1. 在 XenMobile 控制台中，转到 **设置 > 网络访问控制**。



2. 选中要启用的 **设置为不合规** 筛选器的复选框。
3. 点击 **保存**。

更新 Citrix Gateway 策略以支持 NAC

您必须在 VPN 虚拟服务器上配置高级（而非经典）身份验证和 VPN 会话策略。

以下步骤更新具有以下任一特征的 Citrix Gateway：

- 与 XenMobile Server 环境集成。
- 或者，已设置为 VPN，不属于 XenMobile Server 环境，并且可以访问 XenMobile。

在您的虚拟 VPN 服务器上，从控制台窗口执行以下操作。命令和示例中的 IP 地址是虚构的。

1. 如果您正在 VPN 虚拟服务器上使用经典策略，请删除并解除绑定所有经典策略。要检查，请键入:

   ```
   show vpn vserver <VPN_VServer>
   ```

删除任何包含单词 **Classic** 的结果。例如: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

要删除策略，请键入:

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. 通过键入以下内容创建相应的 S高级会话策略。

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

例如: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. 通过键入以下内容，将策略绑定到您的 VPN 虚拟服务器。

```
bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
```

4. 通过键入以下内容，创建身份验证虚拟服务器。

```
add authentication vserver <authentication vserver name> <service type> <ip address>
```

例如：`add authentication vserver authvs SSL 0.0.0.0` 在此示例中，`0.0.0.0` 表示身份验证虚拟服务器不面向公众。

5. 通过键入以下内容，将 SSL 证书与虚拟服务器绑定。

```
bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>
```

例如：`bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. 将身份验证配置文件从 VPN 虚拟服务器关联到身份验证虚拟服务器。首先，通过键入以下内容创建身份验证配置文件。

```
add authentication authnProfile <profile name> -authnVsName <authentication vserver name>
```

例如：

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. 通过键入以下内容，将身份验证配置文件与 VPN 虚拟服务器关联。

```
set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
```

例如：

`set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof`

8. 通过键入以下内容，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，此查询通过获取环境中注册的第一个设备 (`deviceid_1`) 的合规性状态来验证连接：

   `curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"`

   成功的结果类似于以下示例。

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. 如果上一步成功，请创建到 XenMobile 的 Web 身份验证操作。首先，创建一个策略表达式以从 iOS VPN 插件中提取设备 ID。键入以下内容。

   `add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\', \'&\').VALUE(\"deviceidvalue\")"`

10. 通过键入以下内容将请求发送到 XenMobile。在此示例中，XenMobile 服务器 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. 通过键入以下内容，创建用于关联操作的身份验证策略。

`add authentication Policy <policy name> -rule <rule> -action <web authentication action>`

例如：`add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")" -action xm_nac`

12. 通过键入以下内容，将现有 LDAP 策略转换为高级策略。

    `add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>`

    例如：`add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 通过键入以下内容，添加一个策略标签以关联 LDAP 策略。

    `add authentication policylabel <policy_label_name>`

    例如：`add authentication policylabel ldap_pol_label`

14. 通过键入以下内容，将 LDAP 策略与策略标签关联。

    `bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT`

15. 连接合规设备以执行 NAC 测试，确认 LDAP 身份验证成功。键入以下内容。

    `bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END`

16. 添加要与身份验证虚拟服务器关联的 UI。键入以下命令以检索设备 ID。

    `add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid`

17. 通过键入以下内容，绑定身份验证虚拟服务器。

    `bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END`

18. 创建 LDAP 高级身份验证策略以启用 Secure Hub 连接。键入以下内容。

    `add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\").NOT" -action 10.200.80.60_LDAP`

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority 110
-gotoPriorityExpression NEXT
```

三星 Knox

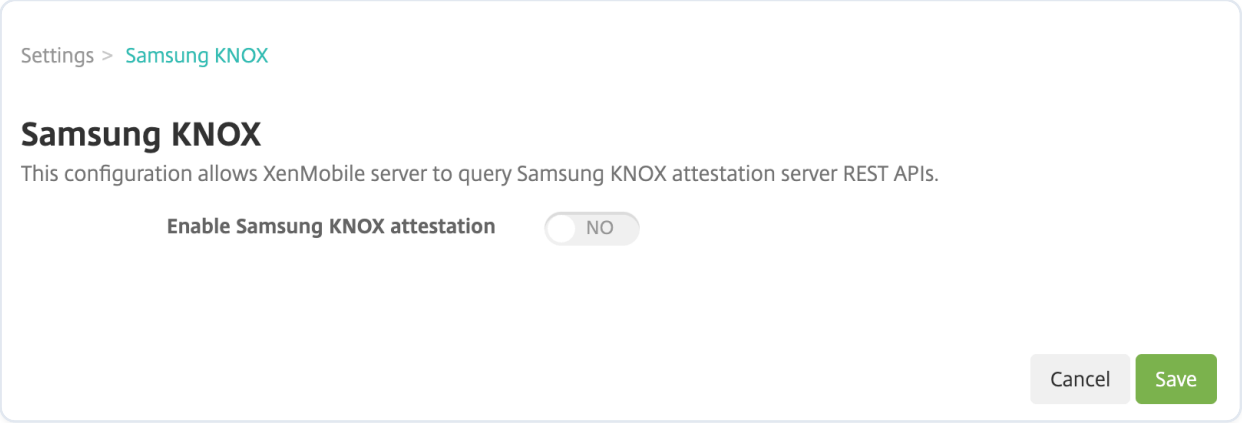
Samsung 提供了多种与 XenMobile® Server 兼容的解决方案。

- XenMobile 支持并扩展了在兼容的 Samsung 设备上的 Samsung Knox 策略。
- Knox 服务插件 (KSP) 是一款支持 Knox Platform for Enterprise (KPE) 部分功能的应用程序。有关 Samsung KPE 的信息，请参阅配置 Knox Platform for Enterprise 和概述。

您可以将 XenMobile 配置为查询 Samsung Knox 证明服务器 REST API。

Samsung Knox 利用硬件安全功能，为操作系统和应用程序提供多层保护。其中一个安全级别是通过证明在平台层面实现的。证明服务器提供对移动设备核心系统软件（例如，引导加载程序和内核）的验证。验证在运行时根据可信启动期间收集的数据进行。

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，单击“**Samsung KNOX**”。此时将显示“**Samsung KNOX**”页面。



3. 在“**启用 Samsung KNOX 证明**”中，选择是否启用 Samsung Knox 证明。默认值为“**否**”。
4. 单击“**保存**”。

注意：

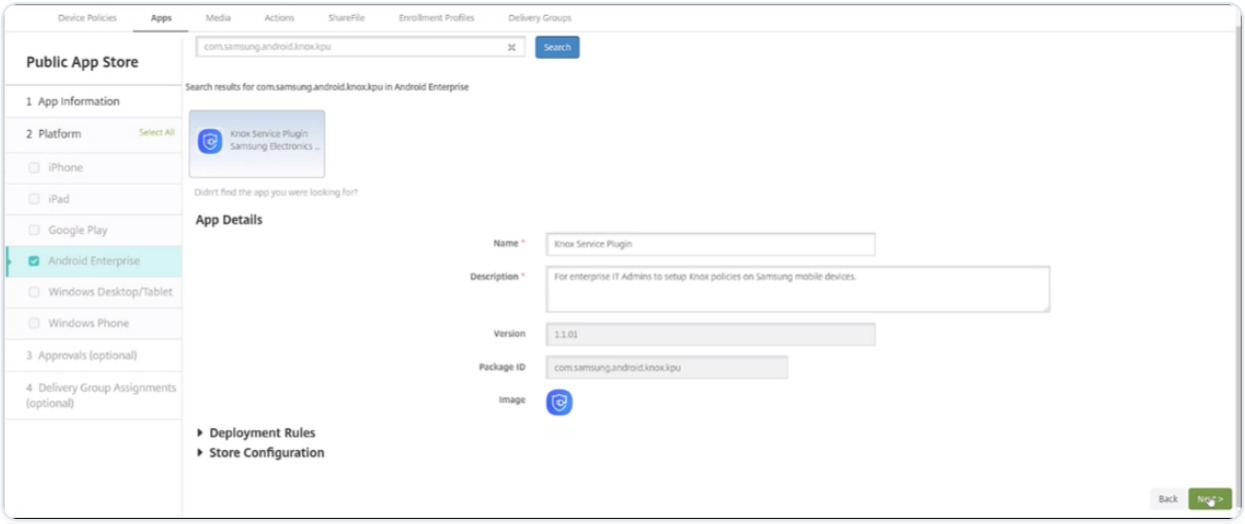
您可以使用 Samsung Knox Mobile Enrollment 将多个 Samsung Knox 设备注册到 XenMobile（或任何移动设备管理器）中，而无需手动配置每个设备。有关信息，请参阅Samsung Knox 批量注册。

添加 Knox 服务插件应用程序

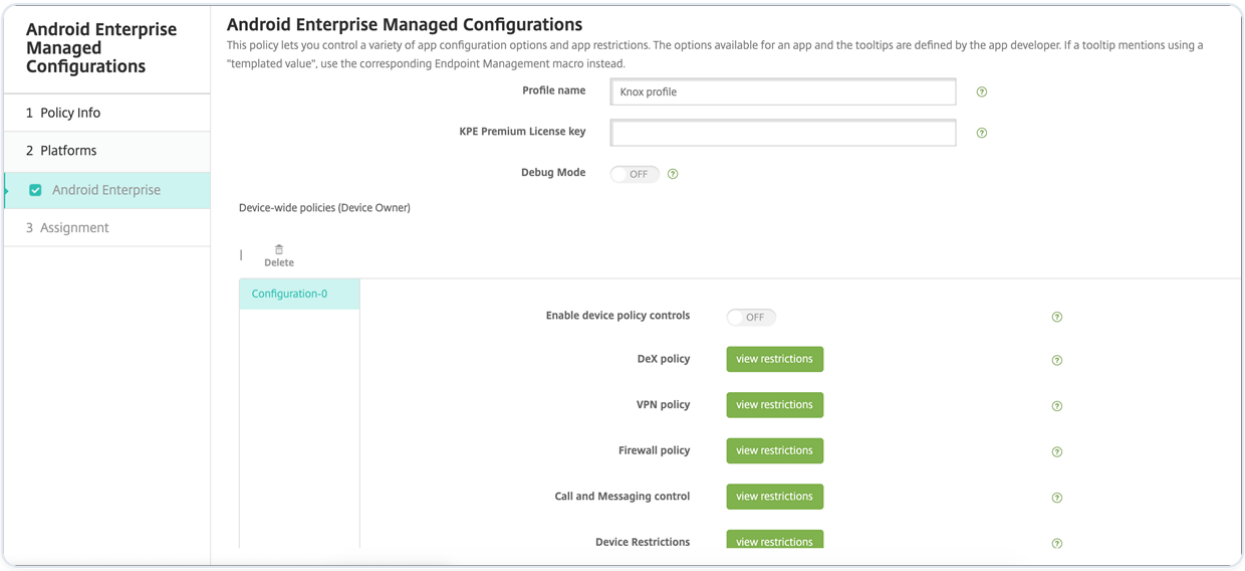
如果您计划将 Android Enterprise 与 Knox 结合使用，请将 Knox 服务插件 (KSP) 添加到 XenMobile。KSP 应用程序使用 AndroidOEMConfig 支持安全策略、灵活的 VPN 配置和生物识别身份验证控制等功能。AndroidOEMConfig 使 OEM 和端点移动性管理器 (EMM) 能够支持自定义 OEM API。这些 API 涵盖了 Android Enterprise 不支持的用例。

有关 KSP 的更多信息，请参阅 Knox Service Plugin Guide。

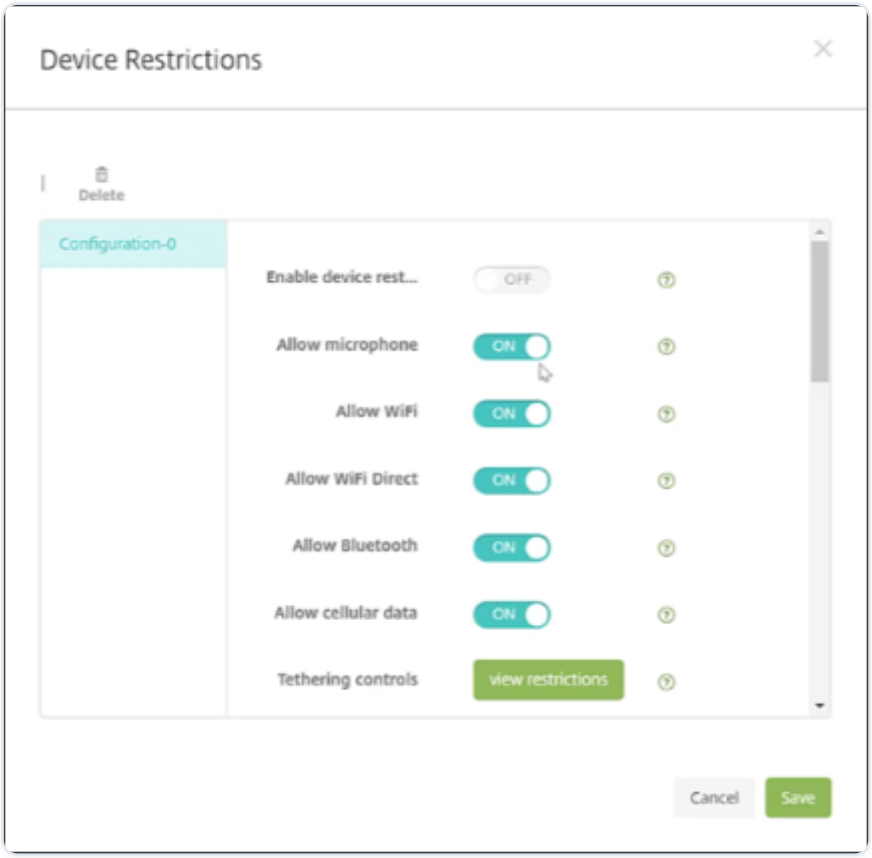
1. 登录您的 Google 帐户并导航到 `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`。批准 Knox Service Plug-in 应用程序。
2. 登录您的 XenMobile 控制台，并将 Knox 服务插件添加为公共应用商店应用程序。有关添加公共应用商店应用程序的更多信息，请参阅 Add a public app store app。



3. 在您的 XenMobile 控制台中，导航到 **Configure > Device policies**。单击 **Add**。
4. 单击 **Managed Configurations**。在弹出的对话框中，从菜单中选择 **Knox Service Plugin**。有关托管配置策略的更多信息，请参阅 Managed configurations policy。
5. 为策略键入名称，然后继续到平台页面。



6. 在平台页面上，为您的 Knox 配置文件键入**配置文件名称**，并输入 Samsung 提供的 **KPE Premium License key**。这些字段下方显示的策略来自您的 Knox 部署。有关 Knox 策略的更多信息，请参阅本节前面引用的《Knox 服务管理员插件指南》。



7. 单击 **Next** 并配置策略的部署规则。
8. 单击 **Save**。

Samsung Knox 批量注册

要将多个 Samsung Knox 设备注册到 XenMobile®（或任何移动设备管理器）而无需手动配置每台设备，请使用 Knox Mobile Enrollment。注册在首次使用或恢复出厂设置后进行。管理员还可以将用户名和密码直接传递给设备，因此用户在注册时无需输入任何信息。

> **注意：**
>
> Knox Mobile Enrollment 的设置与 XenMobile Knox 容器无关。有关 Knox Mobile Enrollment 的更多信息，请参阅 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）并正在运行。

- Secure Hub APK 文件。在设置 Knox Mobile Enrollment 时，您需要上传此文件。
- 有关 KME 要求的列表，请参阅 Knox Mobile Enrollment 简介。
- Samsung Knox Platform for Enterprise (PKE) 许可证，应用设备策略所需。在 XenMobile 设备策略“Knox Platform for Enterprise”中提供许可证密钥。

下载 Secure Hub APK 文件

转到 Google Play 商店下载适用于 Android 的 Citrix Secure Hub™ 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。其中一些防火墙例外适用于所有设备，另一些则特定于设备的地理区域。

设备区域	URL	端口	目标
所有	`https://gslb.secb2b.com`	443	用于启动 Knox Mobile Enrollment 的全局负载均衡器
所有	`https://gslb.secb2b.com`	80	用于在某些有限的旧设备上启动 Knox Mobile Enrollment 的全局负载均衡器
所有	`umc-cdn.secb2b.com`	443	三星代理更新服务器
所有	`bulkenrollment.s3.amazonaws.com`	80	Knox Mobile Enrollment 客户最终用户许可协议
所有	`eula.secb2b.com`	443	Knox Mobile Enrollment 客户最终用户许可协议
所有	`us-be-api-mssl.samsungknox.com`	443	用于 IMEI 验证的三星服务器
美国	`https://us-segd-api.secb2b.com`	443	用于美国地区的三星企业网关

设备区域	URL	端口	目标
欧洲	`https://eu-segd-api.secb2b.com`	443	适用于欧洲地区的 Samsung Enterprise Gateway
中国	`https://china-segd-api.secb2b.com`	443	适用于中国地区的 Samsung Enterprise Gateway

注意：

您可以在 Knox Mobile Enrollment 管理指南 中找到防火墙例外项的完整列表。

获取 Knox Mobile Enrollment 访问权限

请按照 Samsung 文档中的说明，在 KME 入门 中获取 Knox Mobile Enrollment 访问权限。

设置诺克斯移动注册

获取 Knox Mobile Enrollment 访问权限后，登录到 Knox 门户。

注册过程遵循以下一般步骤。

1. 使用您的 MDM 控制台信息和设置创建 MDM 配置文件。

   MDM 配置文件指示您的设备如何连接到您的 MDM。

2. 将设备添加到您的 MDM 配置文件。

   您可以上传包含设备信息的 CSV 文件，也可以从 Google Play 安装并使用 Knox 部署应用程序。

3. 当设备所有权得到验证时，三星会提醒您。
4. 向用户提供 MDM 凭据。指示他们使用 Wi-Fi 连接到互联网，并接受提示以注册其设备。

创建 MDM 配置文件

按照三星文档中关于 配置文件配置 的步骤进行操作。

当您遇到以下字段或步骤时，请按所述进行配置：

- **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 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 文件可以保留在设备在注册期间可以访问的任何服务器上。在注册期间，设备将：

  - 从 APK 下载 URL 下载 Secure Hub
  - 安装 Secure Hub
  - 然后使用接下来描述的自定义 JSON 数据打开 Secure Hub。

  .apk 文件名的大小写必须与您输入的 URL 匹配。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：** 不要指定 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 地址以及用于注册的用户名和密码。您可以在 JSON 中提供这些数据，这样 Secure Hub 就不会提示用户输入。Secure Hub 仅在 JSON 中缺少服务器地址、用户名或密码字段时才会提示用户输入。

  自定义 JSON 数据的格式为：

  `{"serverURL": "URL", "xm_username":"Username", "xm_password":"Password"}`

  在此示例中（批量注册的典型情况），Secure Hub 在注册期间不会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（基于自助服务终端设备的典型情况），Secure Hub 会提示用户输入其凭据：

  `{"serverURL":"https://example.com/zdm"}`

  您还可以输入适用于 Android Enterprise 的零接触注册的自定义 JSON。

  ```
  {

      "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

      {

  "serverURL":"URL","xm_username":"username","xm_password":"password"
  ```

```
    }

}
```

当设备开始注册时，设备会从给定 URL 下载 Secure Hub，安装 Secure Hub，然后打开 Secure Hub。

进一步配置

有关配置的更多信息，请参阅以下 Samsung 文档页面：

- 设备配置：批量添加设备。
- Samsung Knox Deployment App：通过蓝牙、NFC 或 Wi-Fi Direct 注册设备。
- Knox Mobile Enrollment：探索三星文档以获取有关 Samsung Knox 的更多信息。

注册运行早于 2.4 版本的 Knox API 的设备

在 Knox API 版本早于 2.4 的设备上，批量注册不会在初始设备设置期间启动。相反，用户必须启动注册。为此，用户需要访问三星网站下载新的移动注册客户端并开始注册。

下载的注册客户端使用在 Knox 批量注册门户中为 Knox 2.4/2.4.1 设备配置的相同 MDM 配置文件和 APK。

用户通常遵循以下步骤：

1. 打开设备并连接到 Wi-Fi。如果移动注册未启动或 Wi-Fi 不可用，请执行以下操作：
   a. 转到 Samsung Knox 移动设备注册。
   b. 点击“**下一步**”按钮以使用移动数据注册设备。
2. 当出现提示“**使用 Knox 注册**”时，点击“**继续**”。
3. 阅读 EULA（如果可用）。点击“**下一步**”。
4. 如果出现提示，请输入 IT 管理员提供的“**用户 ID**”和“**密码**”。

此时，用户凭据将得到验证，其设备将注册到您组织的企业 IT 环境中。

为三星设备启用和禁用生物识别身份验证

XenMobile 支持指纹和虹膜扫描身份验证，也称为生物识别身份验证。您可以为三星设备启用和禁用生物识别身份验证，而无需用户执行任何操作。如果您在 XenMobile 中禁用生物识别身份验证，则用户和第三方应用程序无法启用此功能。

1. 在 XenMobile 控制台中，点击“**配置**”>“**设备策略**”。此时将显示“**设备策略**”页面。
2. 点击 **添加**。出现 **添加新策略** 页面。
3. 点击 **密码**。出现 **密码策略信息** 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。
   - **描述：** （可选）键入策略的描述。
5. 点击 **下一步**。出现 **平台** 页面。
6. 在 **平台** 下，选择 **Android** 或 **Samsung Knox**。
7. 将 **配置生物识别身份验证** 设置为 **开**。
8. 如果您选择了 **Android**，在 **Samsung SAFE** 下，选择 **允许指纹**、**允许虹膜** 或两者。

   配置生物识别身份验证选项(/en-us/xenmobile/server/media/samsung-knox-biometric-auth.png)

安全操作

您可以在**管理** > **设备**页面执行设备和应用程序安全操作。设备操作包括吊销、锁定、解锁和擦除。应用程序安全操作包括应用程序锁定和应用程序擦除。

- **激活锁绕过：** 在设备激活之前，从受监管的 iOS 设备中移除激活锁。此命令不需要用户的个人 Apple ID 或密码。
- **应用程序锁定：** 拒绝访问设备上的所有应用程序。在 Android 上，应用程序锁定后，用户无法登录 XenMobile。在 iOS 上，用户可以登录，但无法访问任何应用程序。
- **应用程序擦除：** 从 Secure Hub 中移除用户帐户并取消设备注册。在您执行**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：** 为已注册 Apple School Manager DEP 的 iOS 设备创建激活锁绕过代码。
- **清除限制：** 在受监管的 iOS 设备上，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：** 将受监管的 iOS 设备置于丢失模式，并向设备发送要显示的消息、电话号码和脚注。第二次发送此命令会将设备带出丢失模式。
- **启用跟踪：** 在 Android 或 iOS 设备上，此命令允许 XenMobile 以您定义的频率轮询特定设备的位置。要查看设备坐标和地图上的位置，请转到**管理 > 设备**，选择一个设备，然后单击**编辑**。设备信息位于**安全**下的**常规**选项卡中。使用**启用跟踪**持续跟踪设备。当设备运行时，Secure Hub 会定期报告位置。

- **完全擦除：** 立即从设备中擦除所有数据和应用程序，包括任何存储卡中的数据和应用程序。
  - 对于 Android 设备，此请求还可以包括擦除存储卡的选项。
  - 对于具有工作配置文件（COPE 设备）的 Android Enterprise 完全托管设备，您可以在选择性擦除移除工作配置文件后执行完全擦除。
  - 对于 iOS 和 macOS 设备，即使设备已锁定，擦除也会立即发生。
    - 对于 iOS 11 设备（最低版本）：当您确认完全擦除时，可以选择保留设备上的蜂窝数据套餐。
    - 对于 iOS 11.3 设备（最低版本）：当您确认完全擦除时，可以阻止 iOS 设备进行近距离设置。设置新的 iOS 设备时，用户通常可以使用已配置的 iOS 设备来设置自己的设备。您可以阻止 XenMobile Server 管理且已擦除的设备进行近距离设置。
    - 对于 iOS 17 设备（最低版本）：当您确认完全擦除时，设备会自动擦除所有用户数据，连接到指定的 Wi-Fi 网络，并使用提供的注册配置文件重新注册到 MDM 服务器。
  - 如果设备用户在内存卡内容删除之前关闭设备，用户可能仍然可以访问设备数据。
  - 您可以在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“**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**”可在执行操作时显示设备的当前位置。要持续跟踪设备一段时间，请使用“**启用跟踪**”。
  - 将此操作应用于 Android（Android Enterprise 除外）设备或 Android Enterprise（公司拥有或 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位置权限。如果用户在注册期间未授予权限，XenMobile 会在发送“**定位**”命令时再次请求位置权限。
  - 将此功能应用于 iOS 或 Android Enterprise 设备时，请注意以下限制：
    - 对于 Android Enterprise 设备，除非 位置设备策略 已将设备的位置模式设置为“**高精度**”或“**省电**”，否则此请求将失败。
    - 对于 iOS 设备，此命令仅在设备处于 MDM 丢失模式时才成功。
- **锁定：** 远程锁定设备。当您丢失设备且不确定设备是否被盗时，此操作非常有用。XenMobile 会生成一个 PIN 码并将其设置到设备中。要访问设备，用户需要输入 PIN 码。使用“**取消锁定**”可从 XenMobile 控制台移除锁定。
- **锁定并重置密码：** 远程锁定设备并重置密码。

  - 对于在工作配置文件模式下注册到 Android Enterprise 且运行 Android 8.0 之前版本的设备，不支持此功能。
  - 在工作配置文件模式下注册到 Android Enterprise 且运行 Android 8.0 或更高版本的设备上：
    - 发送的密码会锁定工作配置文件。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，并且工作配置文件上未设置密码：设备将被锁定。
    - 如果未发送密码，或发送的密码不符合密码要求，但工作配置文件上已设置密码：工作配置文件已锁定，但设备未锁定。

- **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 平板电脑和 PC，将显示消息“系统即将重新启动”，然后五分钟后重新启动。
- **请求/停止 AirPlay 镜像：** 在受监督的 iOS 设备上启动和停止 AirPlay 镜像。
- **重新启动/关机：** 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。
- **吊销/授权 (iOS, macOS)：** 执行与选择性擦除相同的操作。吊销后，您可以重新授权设备以重新注册。
- **响铃：** 如果设备处于丢失模式，响铃会在受监督的 iOS 设备上播放声音。声音会一直播放，直到您将设备从丢失模式中移除或用户禁用声音。
- **选择性擦除：** 从设备中擦除所有公司数据和应用程序，同时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设备管理器和公司网络的连接。为防止设备访问设备管理器，您还必须吊销设备证书。
  - 选择性擦除 Android 设备也会吊销该设备。您只能在重新授权设备或从控制台删除设备后才能重新注册。
  - 对于具有工作配置文件（COPE 设备）的 Android Enterprise 完全托管设备，在选择性擦除移除工作配置文件后，您可以执行完全擦除。或者，您可以使用相同的用户名重新注册设备。重新注册设备会重新创建工作配置文件。
  - 如果启用了 Samsung Knox API，选择性擦除设备也会移除 Samsung Knox 容器。
  - 对于 iOS 和 macOS 设备，此命令会移除通过 MDM 安装的任何配置文件。
  - 对 Windows 设备执行选择性擦除还会移除任何当前登录用户的配置文件文件夹内容。选择性擦除不会移除您通过配置交付给用户的任何 Web 剪辑。要移除 Web 剪辑，用户需要手动取消注册其设备。您无法重新注册已选择性擦除的设备。

- **解锁：** 清除设备锁定时发送到设备的密码。此命令不会解锁设备。

在 **管理 > 设备** 中，“**设备详细信息**”页面还列出了设备安全属性。这些属性包括强 ID、锁定设备、激活锁绕过以及平台类型的其他信息。“**完全擦除设备**”字段包含用户 PIN 码。设备擦除后，用户必须输入该代码。如果用户忘记了代码，您可以在此处查找。

适用于 Android 设备的安全操作

安全操作	ANDROID（安卓企业版设备除外）	安卓企业版 (自带设备)	ANDROID ENTERPRISE（公司所有）
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
定位	是：对于运行 Android 6.0+ 的设备，定位功能要求用户在注册期间授予位置权限。用户可以选择不授予位置权限。如果用户在注册期间未授予该权限，XenMobile 会在发送定位命令时再次请求位置权限。	是：对于运行 Android 6.0+ 的设备，定位功能要求用户在注册期间授予位置权限。用户可以选择不授予位置权限。如果用户在注册期间未授予该权限，XenMobile 会在发送定位命令时再次请求位置权限。	是：对于运行 Android 6.0+ 的设备，定位功能要求用户在注册期间授予位置权限。用户可以选择不授予位置权限。如果用户在注册期间未授予该权限，XenMobile 会在发送定位命令时再次请求位置权限。
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

适用于 iOS 和 macOS 设备的安全性操作

安全性操作	IOS	MACOS
激活锁绕过	是	否
应用锁定	是	否
应用擦除	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
定位	是	否
锁定	是	是
响铃	是	是
请求/停止 AirPlay 镜像	是	否
重新启动/关机	是	否
撤销/授权	是	是
选择性擦除	是	是
解锁	是	否

Windows 设备的安全性操作

安全性操作	WINDOWS 平板电脑 10
定位	是
锁定	是

安全性操作	WINDOWS 平板电脑 10
锁定并重置密码	否
重新启动	是
吊销	是
响铃	否
选择性擦除	是
擦除	是

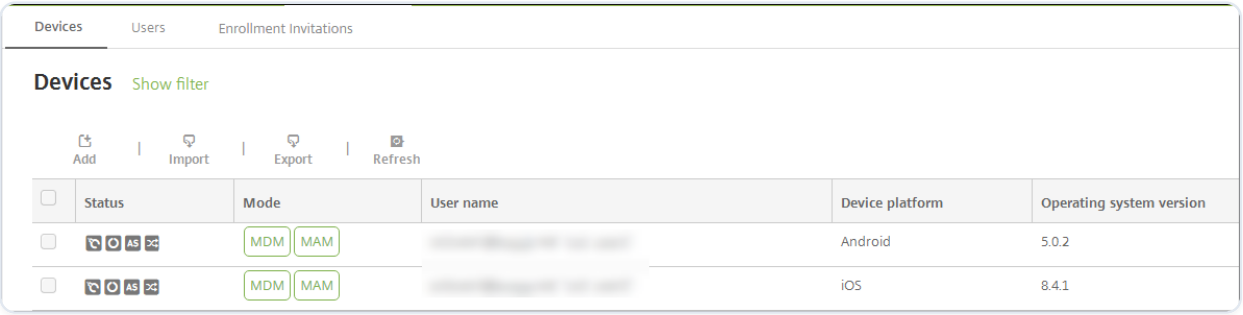
本文的其余部分提供了执行各种安全操作的步骤。您还可以自动执行某些操作。有关详细信息，请参阅自动化操作。

锁定 iOS 设备

您可以锁定丢失的 iOS 设备，并在设备锁定屏幕上显示一条消息和电话号码。此功能支持运行 iOS 7 及更高版本的设备。

要在锁定的设备上显示消息和电话号码，请在 XenMobile 控制台中将密码策略设置为 **true**。或者，用户可以手动在设备上启用密码。

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。

   当您选择设备旁边的复选框时，选项菜单会显示在设备列表上方。当您单击列表中的其他任何位置时，选项菜单会显示在列表的右侧。

   选项菜单的图像(/en-us/xenmobile/server/media/manage-devices-with-commands-secure.png)

   选项菜单的图像(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-2.png)

3. 在选项菜单中，单击“**安全**”。此时将显示“**安全操作**”对话框。

   “安全操作”对话框的图像(/en-us/xenmobile/server/media/manage-devices-secure-lock.png)

4. 单击“**锁定**”。此时将显示“**安全操作**”确认对话框。

   “安全操作”确认的图像(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm.png)

5. （可选）键入要在设备锁定屏幕上显示的消息和电话号码。

   对于运行 iOS 7 及更高版本的 iPad：iOS 会在您在“**消息**”字段中键入的内容后附加“丢失的 iPad”字样。

   对于运行 iOS 7 及更高版本的 iPhone：如果您将“**消息**”字段留空并提供电话号码，Apple 会在设备锁定屏幕上显示“呼叫所有者”消息。

6. 单击“**锁定设备**”。

从 XenMobile 控制台中删除设备

> **重要提示：**

> 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”。

> 要从 XenMobile 控制台删除设备，请转到 **管理 > 设备**，选择一个受管设备，然后单击 **删除**。

删除选项的图像(/en-us/xenmobile/server/media/manage-devices-delete.png)

选择性擦除设备

1. 转到 **管理 > 设备**，选择一个受管设备，然后单击 **保护**。
2. 在 **安全操作** 中，单击 **选择性擦除**。
3. 仅适用于 Android 设备，将设备从公司网络断开连接：设备擦除后，在 **安全操作** 中，单击 **撤销**。

   要在擦除发生之前撤回选择性擦除请求，请在 **安全操作** 中，单击 **取消选择性擦除**。

删除设备

此过程将从设备中删除受管应用程序和数据，并从 XenMobile 控制台的“设备”列表中删除该设备。您可以使用 Endpoint Management 公共 REST API 批量删除设备。

1. 转到 **管理 > 设备**，选择一个受管设备，然后单击 **保护**。
2. 单击 **选择性擦除**。出现提示时，单击 **执行选择性擦除**。
3. 要验证擦除命令是否成功，请刷新 **管理 > 设备**。在 **模式** 列中，MDM 和 MAM 的琥珀色表示擦除命令已成功。

   成功擦除命令的图像(/en-us/xenmobile/server/media/manage-devices-check-wipe-status.png)
4. 在 **管理 > 设备** 上，选择设备，然后单击 **删除**。出现提示时，再次单击 **删除**。

锁定、解锁、擦除或取消擦除应用程序

1. 转到 **管理 > 设备**，选择一个托管设备，然后单击 **安全**。
2. 在 **安全操作** 中，单击应用程序操作。

   您还可以使用 **安全操作** 框来检查其帐户已禁用或从 Active Directory 中删除的用户的设备状态。App Unlock 或 App Unwipe 操作的存在表示应用程序已锁定或已擦除。

应用程序擦除和取消擦除

1. 转到 **管理 > 设备**。选择一个设备。
2. 应用程序擦除
   - 单击 **安全 > 应用程序擦除**。将出现一个对话框，其中包含以下消息：**您确定要擦除此设备上的应用程序吗？** 单击 **应用程序擦除**。
3. 应用程序取消擦除
   - 单击 **安全 > 应用程序取消擦除**。将出现一个对话框，其中包含以下消息：**您确定要取消擦除此设备上的应用程序吗？** 单击 **设备应用程序取消擦除**。
4. 在设备上打开 Secure Hub，然后单击 **商店**。
5. 启动 Secure Hub。

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 丢失模式不需要用户执行以下任何操作即可启用设备定位：配置 **查找我的 iPhone/iPad** 设置或为 Citrix Secure Hub 启用定位服务。

在 XenMobile 丢失模式下，只有才能解锁设备。（相比之下，如果您使用 XenMobile 设备锁定功能，用户可以通过您提供的 PIN 码直接解锁设备。

要启用或禁用丢失模式：转到 **管理 > 设备**，选择一个受监管的 iOS 设备，然后单击 **安全**。然后，单击 **启用丢失模式** 或 **禁用丢失模式**。

丢失模式选项的图像(/en-us/xenmobile/server/media/manage-devices-enable-lost-mode-button.png)

如果单击**启用丢失模式**，请键入设备处于丢失模式时要显示的信息。

设备上显示的信息图像(/en-us/xenmobile/server/media/enable-lost-mode-dialog.png)

使用以下任一方法检查丢失模式状态：

- 在**安全操作**窗口中，验证按钮是否为**禁用丢失模式**。
- 从**管理 > 设备**，在**安全**下的**常规**选项卡上，查看上次的“启用丢失模式”或“禁用丢失模式”操作。

常规选项卡的图像(/en-us/xenmobile/server/media/manage-devices-ios-lost-mode.png)

- 从**管理 > 设备**，在**属性**选项卡上，验证**MDM 丢失模式已启用**设置的值是否正确。

MDM 丢失模式已启用设置的图像(/en-us/xenmobile/server/media/manage-devices-details-properties.png)

如果在 iOS 设备上启用 XenMobile 丢失模式，XenMobile 控制台也会发生以下更改：

- 在**配置 > 操作**中，**操作**列表不包括以下自动化操作：**吊销设备**、**选择性擦除设备**和**完全擦除设备**。
- 在**管理 > 设备**中，**安全操作**列表不再包括**吊销**和**选择性擦除**设备操作。您仍然可以根据需要使用安全操作执行**完全擦除**操作。

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**中键入的内容。

对于运行 iOS 7 及更高版本的 iPhone：如果将**消息**留空并提供电话号码，Apple 会在设备锁定屏幕上显示“呼叫所有者”消息。

绕过 iOS 激活锁

激活锁是“查找我的 iPhone/iPad”的一项功能，可防止重新激活丢失或被盗的受监管设备。激活锁要求用户提供 Apple ID 和密码，然后才能禁用“查找我的 iPhone/iPad”、擦除设备或重新激活设备。对于您的组织拥有的设备，绕过激活锁是必要的，例如，用于重置或重新分配设备。

要启用激活锁，请配置并部署 XenMobile MDM 选项设备策略。然后，您可以从 XenMobile 控制台管理设备，而无需用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 XenMobile 控制台发出“激活锁绕过”安全操作。

例如，如果用户归还丢失的手机，或者在完全擦除之前或之后设置设备：当手机提示输入 iTunes 帐户凭据时，您可以通过从 XenMobile 控制台发出“激活锁绕过”安全操作来绕过该步骤。

激活锁绕过的设备要求

- iOS 7.1（最低版本）
- 通过 Apple Configurator 或 Apple DEP 进行监管
- 配置了 iCloud 帐户
- “查找我的 iPhone/iPad”已启用
- 已注册到 XenMobile
- MDM 选项设备策略（已启用激活锁）已部署到设备

要在执行设备完全擦除之前绕过激活锁，请执行以下操作：

1. 转到“**管理 > 设备**”，选择设备，单击“**安全**”，然后单击“**激活锁绕过**”。
2. 擦除设备。在设备设置期间，激活锁屏幕不会出现。

要在执行设备完全擦除之后绕过激活锁，请执行以下操作：

1. 重置或擦除设备。在设备设置期间，激活锁屏幕会出现。
2. 转到**管理 > 设备**，选择设备，单击**安全**，然后单击**激活锁绕过**。
3. 轻触设备上的“返回”按钮。主屏幕随即显示。

请记住以下事项：

- 建议用户不要禁用“查找我的 iPhone/iPad”。不要从设备执行完全擦除。在这两种情况下，系统都会提示用户输入 iCloud 帐户密码。帐户验证后，用户在擦除所有内容和设置后将不会看到“激活 iPhone/iPad”屏幕。
- 对于已生成激活锁绕过代码且已启用激活锁的设备：如果在完全擦除后无法绕过“激活 iPhone/iPad”页面，则无需从 XenMobile 中删除设备。您或用户可以直接联系 Apple 支持以解除设备锁定。
- 在硬件清点期间，XenMobile 会查询设备以获取激活锁绕过代码。如果绕过代码可用，设备会将其发送到 XenMobile。然后，要从设备中删除绕过代码，请从 XenMobile 控制台发送“激活锁绕过”安全操作。届时，以及 Apple 拥有解除设备锁定所需的绕过代码。

- “激活锁绕过”安全操作依赖于 Apple 服务的可用性。如果此操作不起作用，您可以按如下方式解除设备锁定。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代码。要查找绕过代码，请转到**管理 > 设备**，选择设备，单击**编辑**，然后单击**属性**。**激活锁绕过代码**位于**安全信息**下。

XenMobile® 自动发现服务

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

借助 AutoDiscovery 服务，用户可以：

- 使用其公司网络凭据注册设备。
- 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`。

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

要访问 AutoDiscovery 服务，请导航到 `<https://adsui.cloud.com>`（商业版）或 `<https://adsui.cem.cloud.us>`（政府版）。

先决条件

- Citrix Cloud 中的新 AutoDiscovery 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

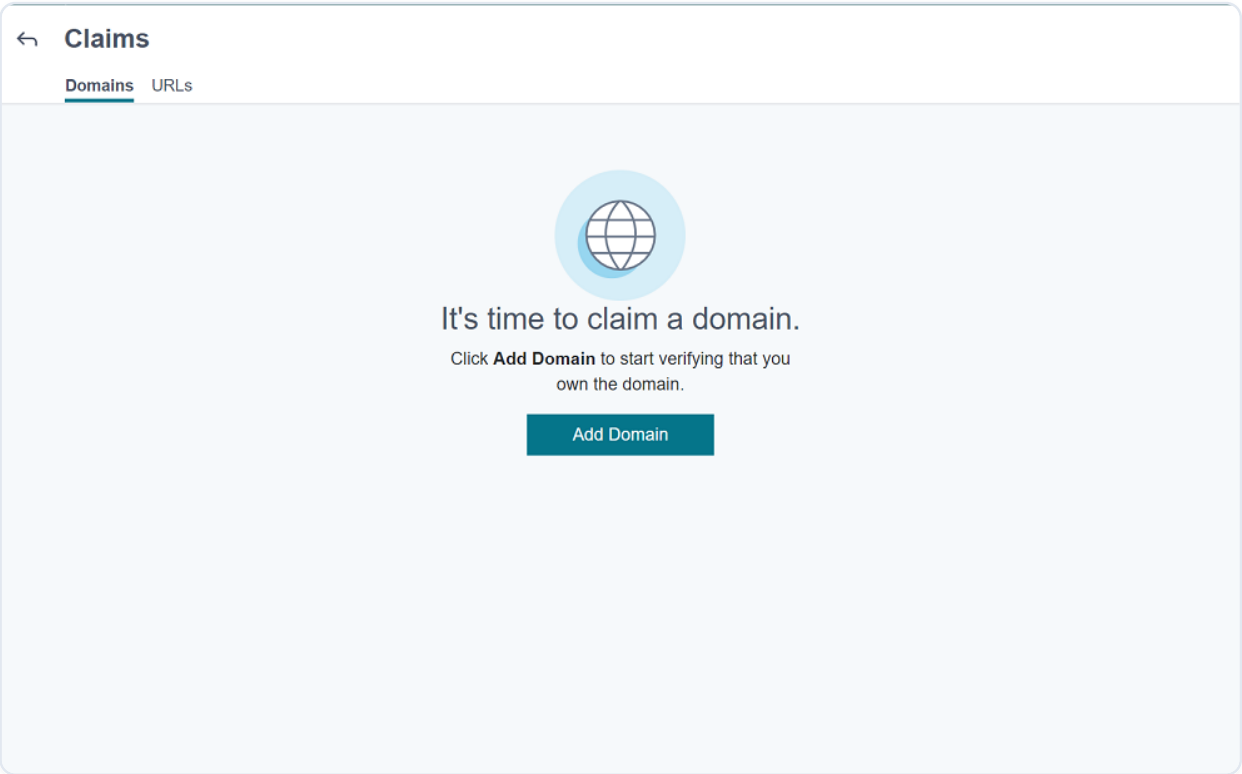
  运行早期版本 Secure Hub 的设备可能会遇到服务中断。
- 要访问新的 AutoDiscovery 服务，您必须拥有具有完全访问权限的 Citrix Cloud 管理员帐户。AutoDiscovery 服务不支持具有自定义访问权限的管理员帐户。如果您没有帐户，请参阅注册 Citrix Cloud。

  Citrix 已将所有现有 AutoDiscovery 记录迁移到 Citrix Cloud，服务未中断。迁移的记录不会自动显示在新控制台中。您必须在新 AutoDiscovery 服务中收回域以证明所有权。有关详细信息，请参阅 CTX312339。

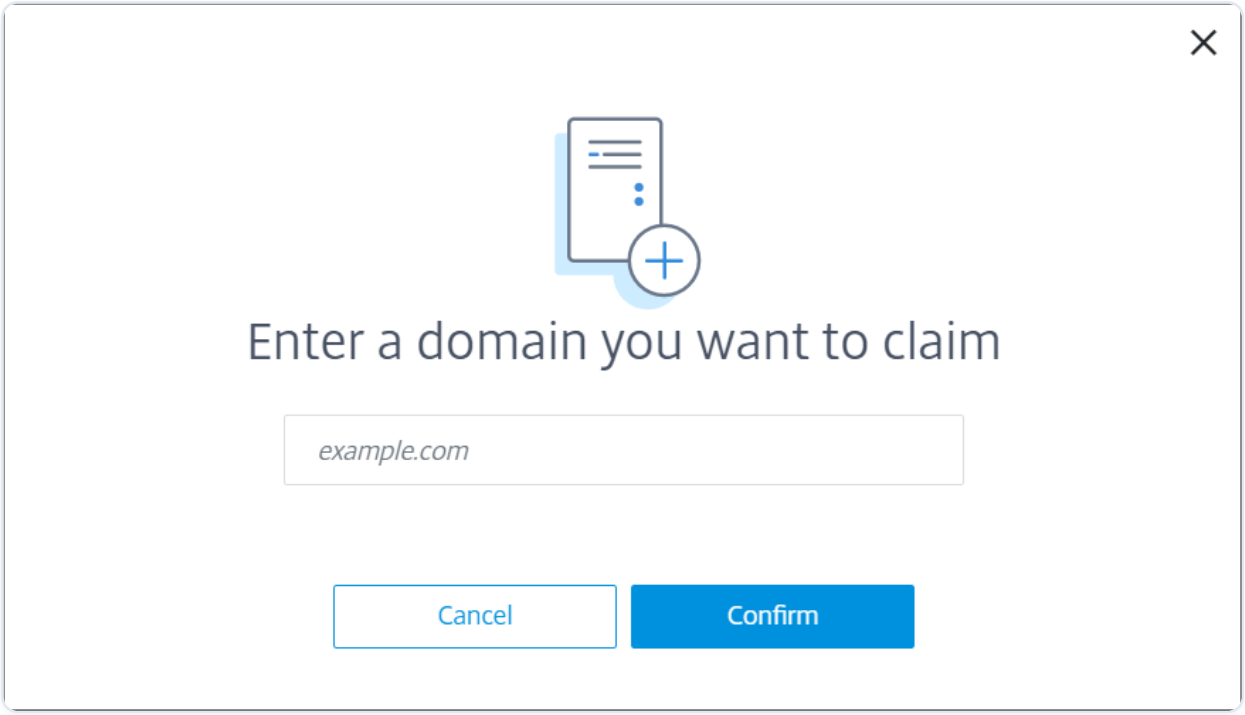
- 在使用适用于您的 Endpoint Management 部署的 AutoDiscovery 服务之前，请验证并声明您的域。您最多可以声明 10 个域。声明会将已验证的域与 AutoDiscovery 服务关联起来。要声明 10 个以上的域，请提交 SRE 工单或联系 Citrix 技术支持。
- 使用 MAM 端口设置而不是 Citrix Gateway FQDN 将 MAM 流量定向到您的数据中心。如果您输入完全限定域名以及 Citrix Gateway 的端口，客户端设备将使用 **MAM Port** 设置中的配置。
- 如果广告拦截器阻止网站打开，请确保为整个网站禁用广告拦截器。

声明域

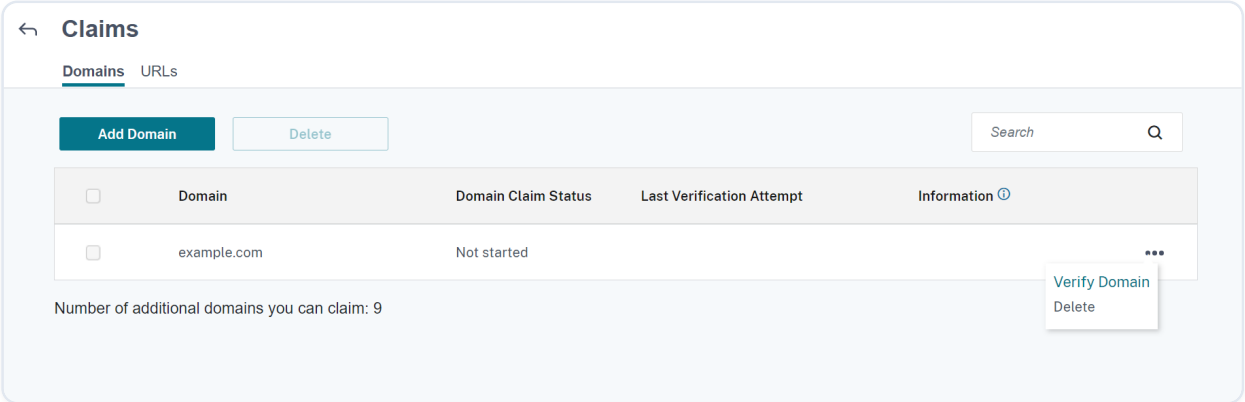
1. 在 **Claims > Domains** 选项卡上，单击 **Add Domain**。



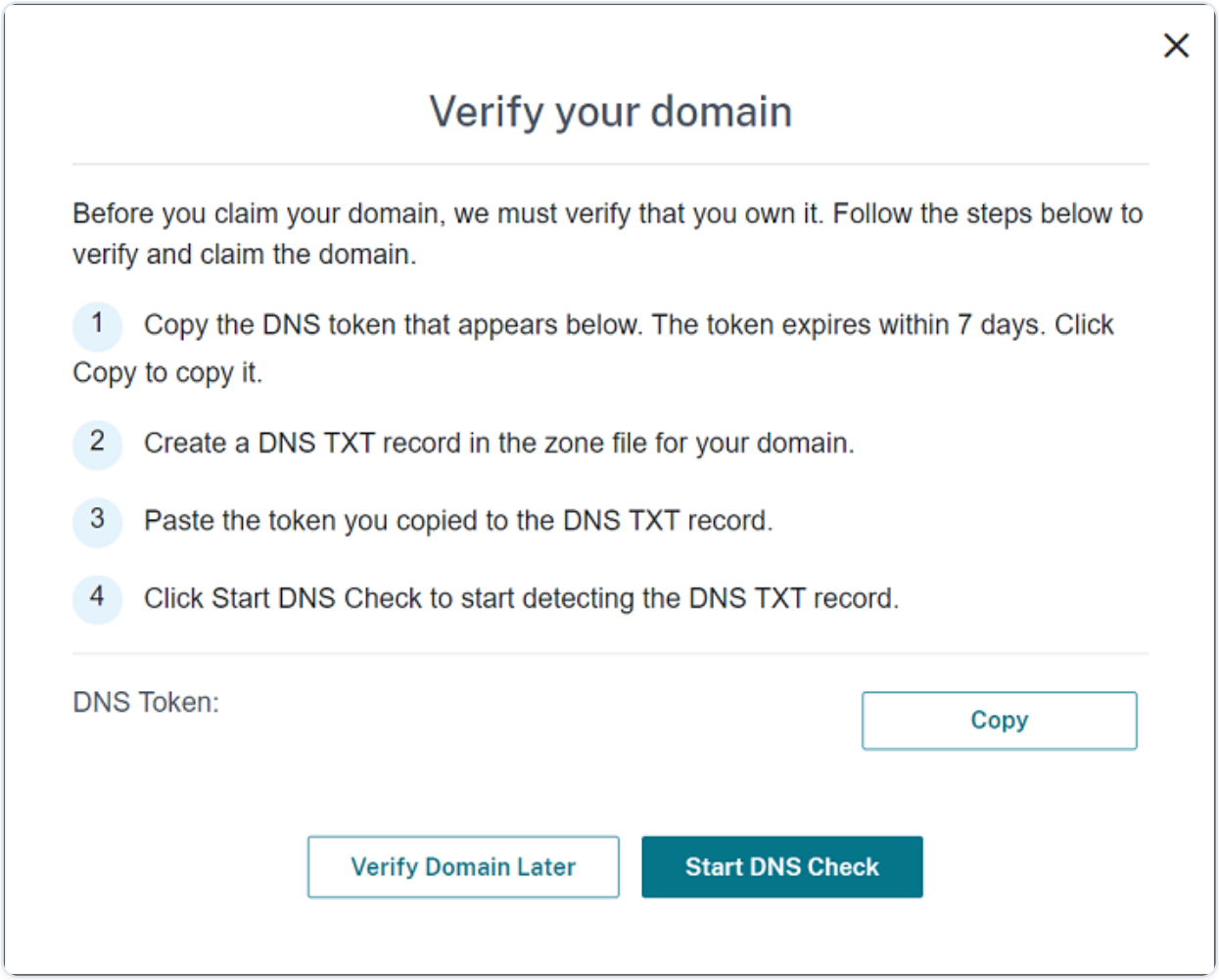
2. 在出现的对话框中，输入 XenMobile 环境的域名，然后单击 **Confirm**。您的域将显示在 **Claims > Domains** 中。



3. 在您添加的域上，单击省略号菜单并选择 **Verify Domain** 以启动验证过程。将显示 **Verify your domain** 页面。



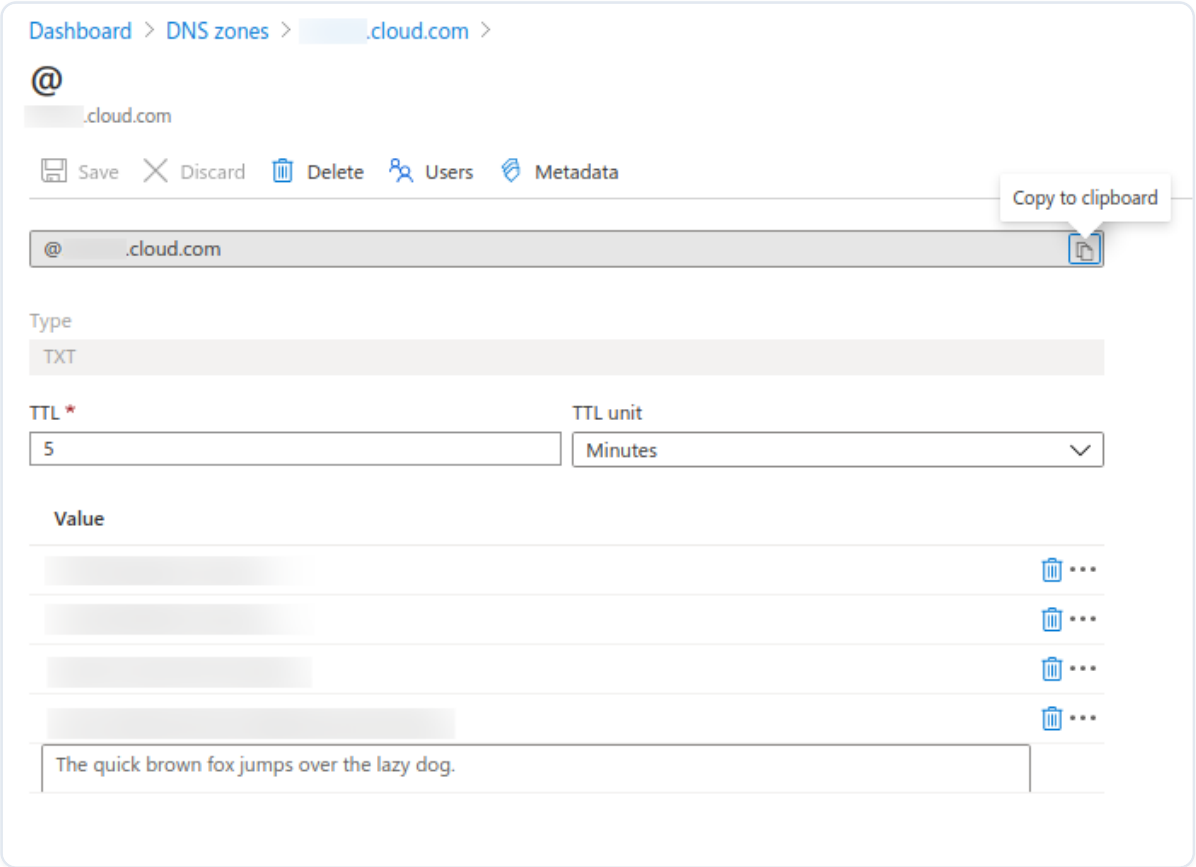
4. 在 **Verify your domain** 页面上，按照说明验证您拥有该域。



a. 单击 **Copy** 将 DNS 令牌复制到剪贴板。

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

   以下屏幕截图显示了域托管服务提供商门户。您的门户可能有所不同。



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

验证过程通常需要大约一小时。但是，可能需要长达两天才能返回响应。在状态检查期间，您可以注销并再次登录。

配置完成后，您的域状态将从“**待处理**”更改为“**已验证**”。

5. 声明您的域后，提供有关自动发现服务的信息。单击您添加的域上的省略号菜单，然后单击“**添加 Endpoint Management 信息**”。此时将显示“**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 MDM 部署，请将此字段留空。

> **注意：**

> Citrix 建议您使用“**MAM 端口**”设置而不是“**Citrix Gateway FQDN**”来控制 MAM 流量。如果您输入完全限定域名以及 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：** 输入您之前配置的 XenMobile Server 的实例名称。如果您不确定实例名称，请保留默认值“**zdm**”。
- **MDM 端口：** 输入用于 MDM 控制流量和 MDM 注册的端口。对于基于云的服务，默认值为 443。
- **MAM 端口：** 输入用于 MAM 控制流量、MAM 注册、iOS 注册和应用程序枚举的端口。对于基于云的服务，默认值为 8443。

请求 Windows 设备的自动发现

如果您计划注册 Windows 设备，请执行以下操作：

1. 联系 Citrix 支持并创建支持请求以启用 Windows AutoDiscovery。
2. 获取一个公开签名、非通配符的 SSL 证书，用于 `enterpriseenrollment.mycompany.com`。`mycompany.com` 部分是包含用户用于注册的帐户的域。将 .pfx 格式的 SSL 证书及其密码附加到上一步创建的支持请求中。

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

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

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

   - 提供您的 XenMobile Server 的详细信息。
   - 指示设备从 XenMobile 请求有效证书。

此时，您可以注册所有受支持的设备。转到下一节，准备向设备交付资源。

设备策略

您可以通过创建策略来配置 XenMobile® 与设备交互的方式。尽管许多策略对所有设备都通用，但每台设备都有一组特定于其操作系统的策略。因此，您可能会发现不同平台之间，甚至不同 Android 设备制造商之间存在差异。

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，请牢记以下规则。如果一个或多个已注册设备上的策略发生冲突，则与 GPO 对齐的策略优先。

> 要查看 Android Enterprise 容器支持哪些策略，请参阅 Android Enterprise。

先决条件

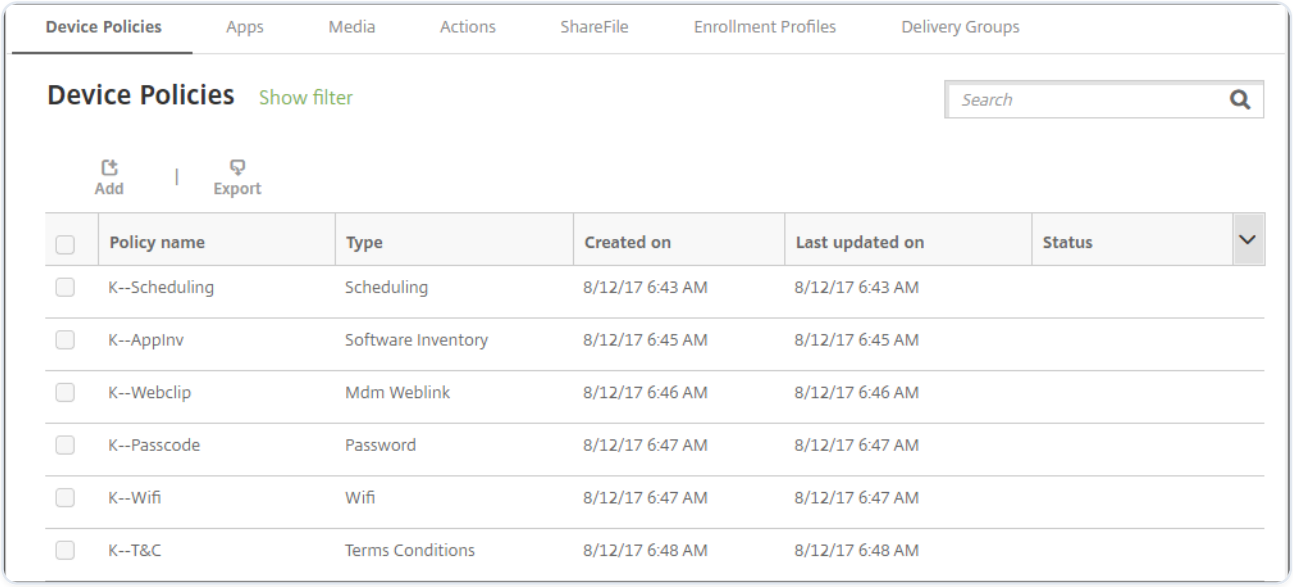
- 创建您计划使用的任何交付组。
- 安装任何必要的 CA 证书。

添加设备策略

创建设备策略的基本步骤如下：

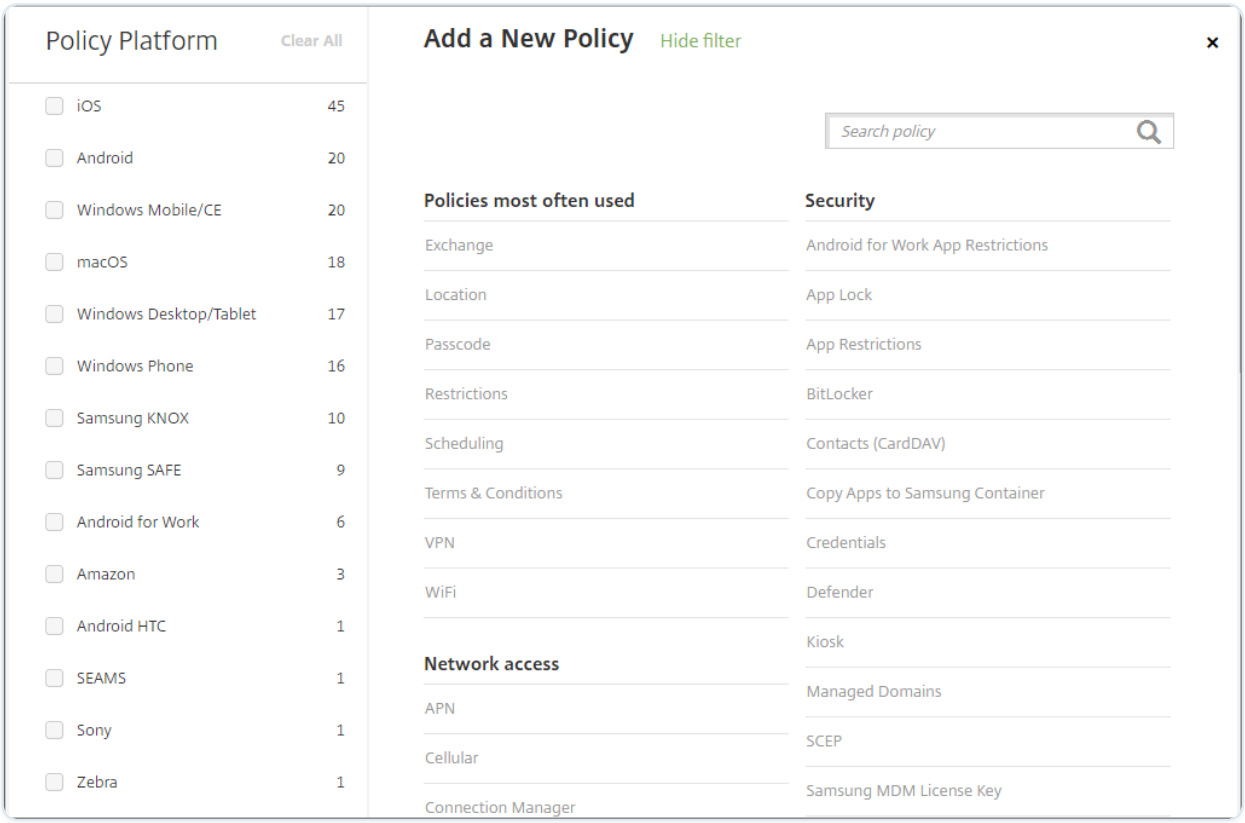
1. 命名并描述策略。
2. 为一个或多个平台配置策略。
3. 创建部署规则（可选）。
4. 将策略分配给交付组。
5. 配置部署计划（可选）。

要创建和管理设备策略，请转到 **配置 > 设备策略**。

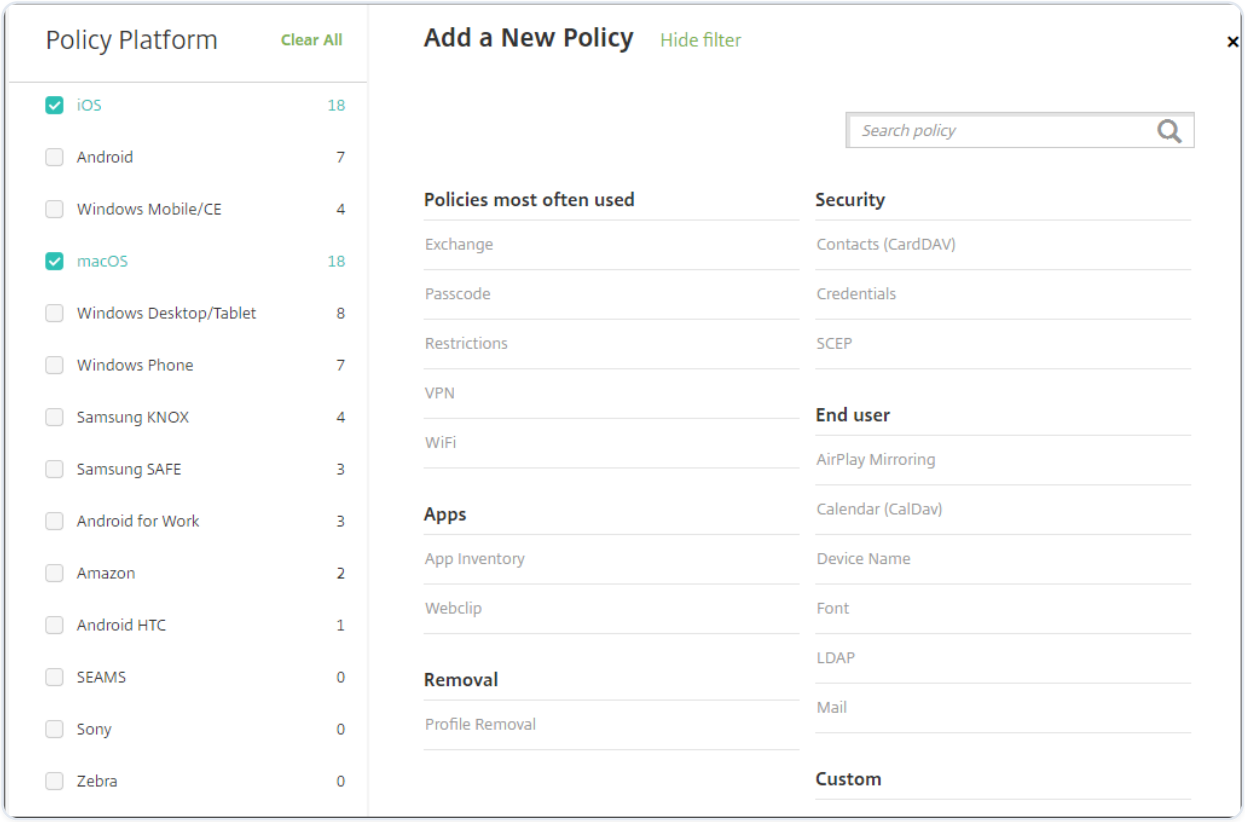


要添加策略：

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以查看所选平台的设备策略列表。单击策略名称以继续添加策略。



您也可以在搜索框中键入策略名称。键入时，将显示潜在匹配项。如果您的策略在列表中，请单击它。结果中将只保留您选择的策略。单击它以打开该策略的 **策略信息** 页面。

3. 选择要包含在策略中的平台。所选平台的配置页面将显示在步骤 5 中。
4. 完成 **策略信息** 页面，然后单击 **下一步**。**策略信息** 页面收集策略名称等信息，以帮助您识别和跟踪策略。此页面对于所有策略都类似。
5. 完成平台页面。您在步骤 3 中选择的每个平台都会显示平台页面。这些页面对于每个策略都不同。策略在不同平台之间可能有所不同。并非所有策略都适用于所有平台。

   某些页面包含项目表。要删除现有项目，请将鼠标悬停在包含列表的行上，然后单击右侧的垃圾桶图标。在确认对话框中，单击 **删除**。

   要编辑现有项目，请将鼠标悬停在包含列表的行上，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。默认情况下显示**基本**选项卡。

   - 在列表中，单击选项以确定何时部署策略。您可以选择在满足所有条件时或在满足任何条件时部署策略。默认选项设置为**所有**。
   - 单击**新建规则**以定义条件。
   - 在列表中，单击条件，例如**设备所有权**和**BYOD**。

- 如果要添加更多条件，请再次单击**新建规则**。您可以根据需要添加任意数量的条件。

2. 单击**高级**选项卡以使用布尔选项组合规则。您在**基本**选项卡上选择的条件将显示。
3. 您可以使用更高级的布尔逻辑来组合、编辑或添加规则。

   - 单击**AND**、**OR**或**NOT**。
   - 在列表中，选择要添加到规则的条件。然后，单击右侧的加号 (**+**) 将条件添加到规则中。

     您可以随时单击以选择条件，然后单击**编辑**以更改条件或**删除**以删除条件。
   - 单击**新建规则**以添加另一个条件。

4. 单击**下一步**以转到下一个平台页面，或者在所有平台页面完成后，转到**分配**页面。
5. 在**分配**页面上，选择要应用策略的交付组。如果单击某个交付组，该组将显示在**接收应用程序分配的交付组**框中。

   接收应用分配的交付组在您选择交付组之前不会出现。

   设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policies-assignment.png)
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**以安排部署，或单击**关**以阻止部署。默认选项设置为**开**。
   - 在**部署计划**旁边，单击**立即**或**稍后**。默认选项设置为**立即**。
   - 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
   - 在**部署条件**旁边，单击**每次连接时**或单击**仅当上次部署失败时**。默认选项设置为**每次连接时**。
   - 在**部署用于始终在线连接**旁边，单击**开**或**关**。默认选项设置为**关**。

     > **注意：**
     >
     > 此选项在您已在**设置 > 服务器属性**中配置计划后台部署密钥时适用。始终在线选项不适用于 iOS 设备。
     >
     > 您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但**部署用于始终在线连接**除外，该选项不适用于 iOS。

   设备策略配置屏幕的图像(/en-us/xenmobile/server/media/deployment-schedule.png)
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。

- 安卓

  要从 Android 设备中删除设备策略，请使用 XenMobile 卸载设备策略。有关详细信息，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，所有策略都是 MDM 配置文件的一部分。因此，您可以为要删除的策略创建配置文件删除设备策略。其余策略和配置文件将保留在设备上。有关信息，请参阅配置文件删除设备策略。

- Windows 10 操作系统和 Windows 11 操作系统

  您无法直接从 Windows 桌面或平板电脑设备中删除设备策略。但是，您可以使用以下任一方法：

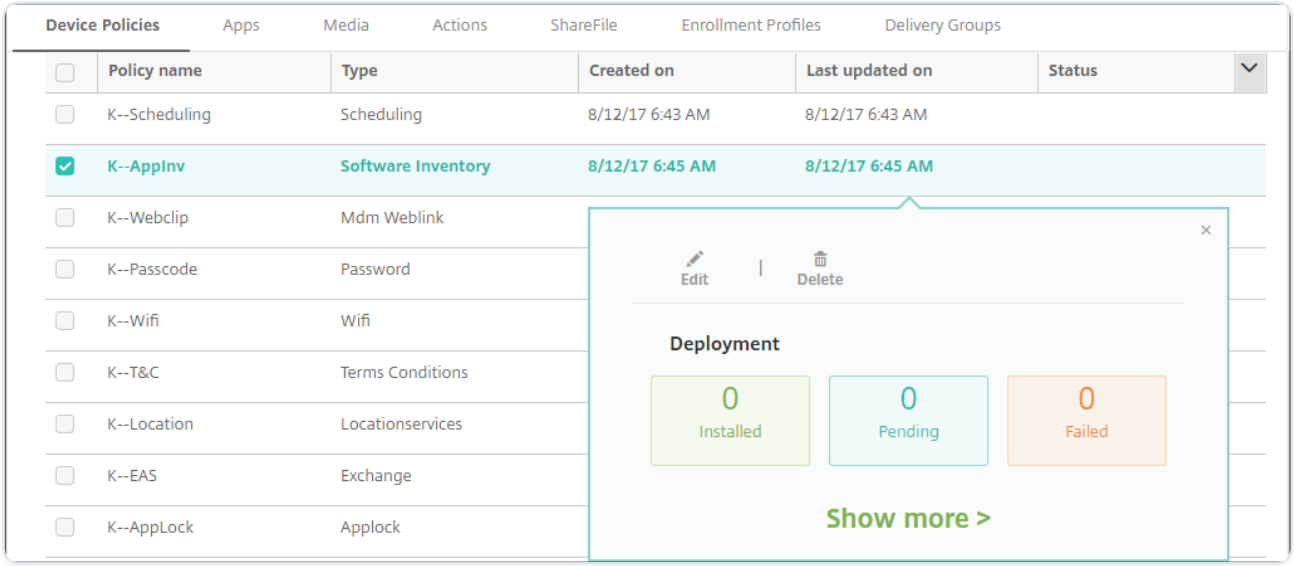
  - 取消注册设备，然后将一组新策略推送到设备。然后用户重新注册以继续。
  - 推送安全操作以选择性擦除特定设备。该操作会从设备中删除所有企业应用和数据。然后，从仅包含该设备的交付组中删除设备策略，并将该交付组推送到设备。然后用户重新注册以继续。

- Chrome 操作系统

  要从 Chrome OS 设备中删除设备策略，您可以从仅包含该设备的交付组中删除设备策略。然后将该交付组推送到设备。

编辑设备策略

要编辑策略，请选中策略旁边的复选框以显示策略列表上方的选项菜单。或者，单击列表中的策略以显示列表右侧的选项菜单。



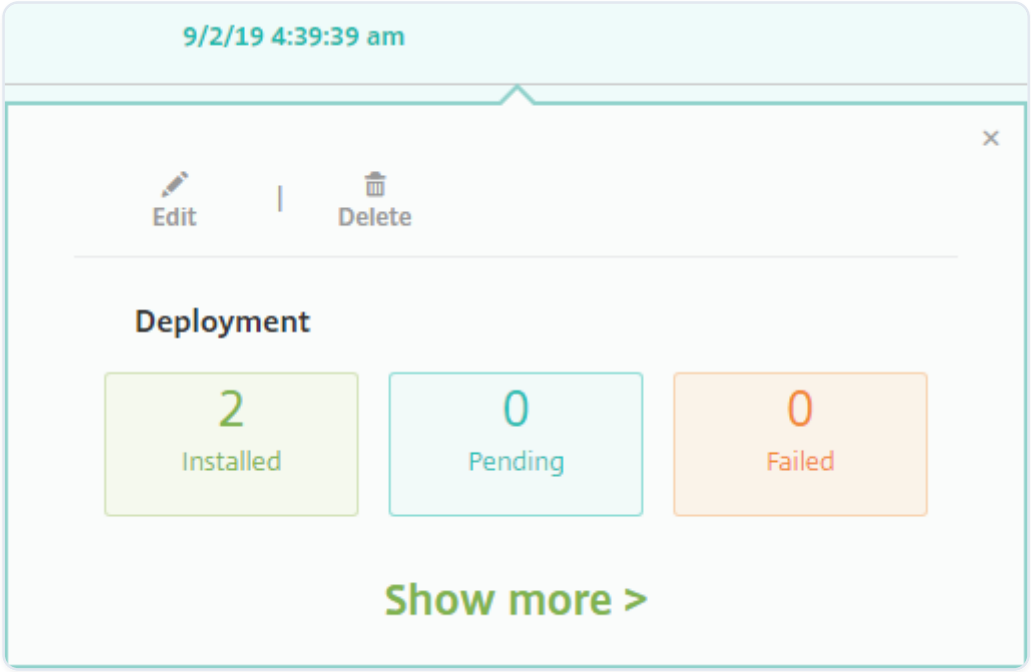
要查看策略详细信息，请单击**显示更多**。

要编辑设备策略的所有设置，请单击 **编辑**。

如果单击 **删除**，将显示确认对话框。再次单击 **删除** 以删除策略。

检查策略部署状态

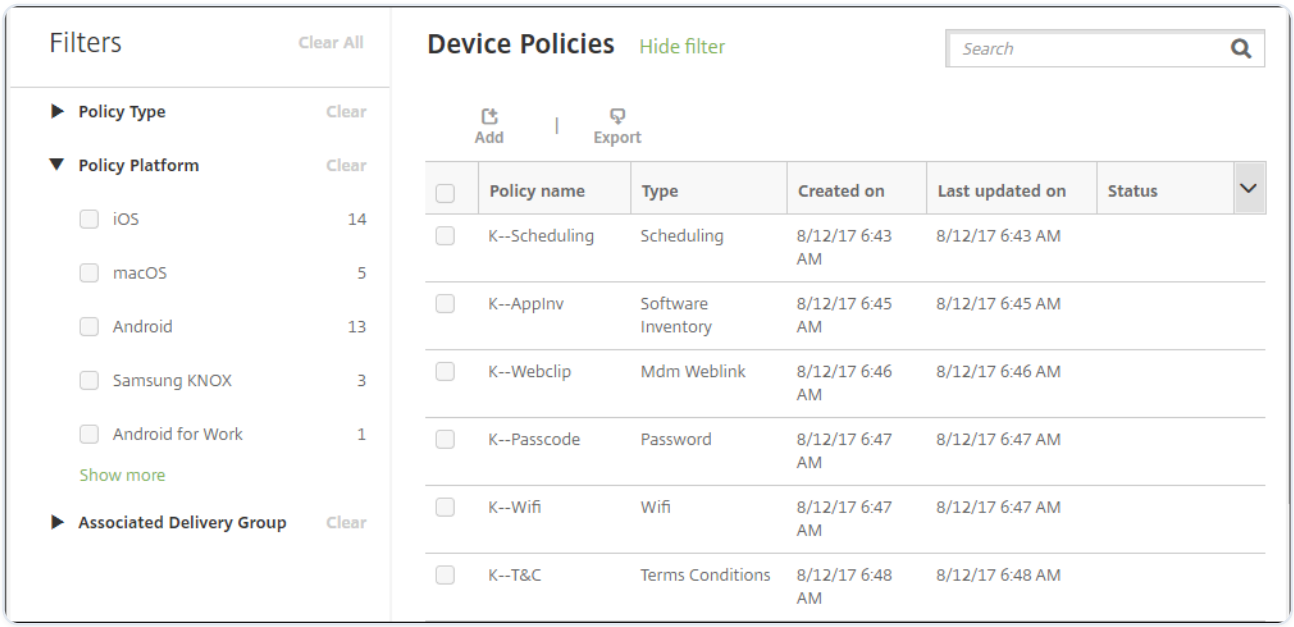
在 **配置 > 设备策略** 页面上单击策略行以检查其部署状态。



当策略部署处于待定状态时，用户可以通过点击 **首选项 > 设备信息 > 刷新策略** 从 Secure Hub 刷新策略。

筛选已添加的设备策略列表

您可以按策略类型、平台和关联的交付组筛选已添加的策略列表。在 **配置 > 设备策略** 页面上，单击 **显示筛选器**。在列表中，选择要查看的项目的复选框。



单击 **保存此视图** 以保存筛选器。筛选器的名称将显示在 **保存此视图** 按钮下方的按钮中。

设备策略摘要

设备策略名称	设备策略描述
AirPlay 镜像	将特定的 AirPlay 设备（例如另一台 Mac 计算机）添加到 iOS 设备。您还可以选择将设备添加到受监督设备的允许列表中。该选项将用户限制为仅允许列表中的 AirPlay 设备。
隔空打印	将隔空打印机添加到 iOS 设备上的隔空打印机列表。此策略使得在打印机和设备位于不同子网的环境中提供支持变得更加容易。
Android Enterprise 应用权限	配置工作配置文件中对 Android Enterprise 应用的请求如何处理 Google 所谓的“危险”权限。
Android Enterprise 应用限制	更新与 Android 应用相关的限制。
APN	确定用于将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 的设置。此设置已在大多数新手机中定义。如果您的组织不使用消费

设备策略名称	设备策略描述
	者 APN 从移动设备连接到互联网，请使用此策略。
应用访问	定义设备上必需、可选或禁止的应用列表。然后，您可以创建自动化操作以响应设备与该应用列表的合规性。
应用属性	为 iOS 设备指定属性，例如托管应用捆绑包 ID 或每应用 VPN 标识符。
应用配置	远程配置支持托管配置的各种应用的设置和行为。为此，您可以将 XML 配置文件（称为属性列表或 plist）部署到 iOS 设备。或者，您可以将键/值对部署到 Windows 10 手机，或运行 Windows 10 或 Windows 11 的桌面或平板设备。
应用清单	收集受管设备上的应用程序清单。XenMobile 随后会将该清单与部署到这些设备的任何应用程序访问策略进行比较。通过这种方式，您可以检测到位于应用程序访问允许列表或阻止列表上的应用程序，然后采取正确的措施。
应用程序锁定	定义用户可以在 iOS 或某些 Android 设备上运行或无法运行的应用程序列表。
应用程序网络使用情况	设置网络使用规则，以指定受管应用程序如何在 iOS 设备上使用网络（例如蜂窝数据网络）。这些规则仅适用于受管应用程序。受管应用程序是通过 XenMobile 部署到用户设备的应用程序。
应用程序卸载	从用户设备中删除应用程序。
应用程序通知	控制 iOS 用户如何接收来自指定应用程序的通知。
自动更新受管应用程序	控制已安装的受管应用程序如何在 Android Enterprise 设备上更新。
BitLocker	配置 Windows 10 和 Windows 11 设备上 BitLocker 界面中可用的设置。

设备策略名称	设备策略描述
日历 (CalDAV)	将日历 (CalDAV) 帐户添加到 iOS 或 macOS 设备。CalDAV 帐户使用户能够将日程数据与任何支持 CalDAV 的服务器同步。
蜂窝网络	配置蜂窝网络设置。
连接管理器	指定自动连接到互联网和专用网络的应用程序的连接设置。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。CardDAV 帐户使用户能够将联系人数据与任何支持 CardDAV 的服务器同步。
控制操作系统更新	将最新的操作系统更新部署到受支持的受监管设备。
凭据	在 XenMobile 中启用与您的 PKI 配置的集成身份验证。例如，使用 PKI 实体、密钥库、凭据提供程序或服务器证书。
自定义 XML	自定义设备预配、设备功能启用、设备配置和故障管理等功能。
防御者	配置 Windows 10 和 Windows 11 台式机和平板电脑的 Windows Defender 设置。
设备运行状况证明	要求 Windows 10 和 Windows 11 设备报告其运行状况。为此，它们会将特定数据和运行时信息发送到健康证明服务 (HAS) 进行分析。HAS 会创建并返回一个健康证明证书，然后设备会将其发送到 XenMobile。当 XenMobile 收到健康证明证书时，它会根据该证书的内容部署您配置的自动操作。
设备名称	设置 iOS 和 macOS 设备上的名称，以便您可以识别这些设备。您可以使用宏、文本或两者的组合来定义设备名称。

设备策略名称	设备策略描述
教育配置	配置教师和学生设备以与 Apple Education 配合使用。如果教师使用课堂应用，则需要教育配置设备策略。
交换	为设备上的本机电子邮件客户端启用 ActiveSync 电子邮件。
文件	将脚本文件添加到 XenMobile，这些文件为用户执行特定功能。或者，您可以添加文档文件，以便 Android 设备用户可以在其设备上访问。添加文件时，您还可以指定希望文件存储在设备上的目录。
FileVault	此策略允许您在已注册的 macOS 设备上启用 FileVault 设备加密。您还可以控制用户在登录期间可以跳过 FileVault 设置的次数。适用于 macOS 10.7 或更高版本。
字体	将字体添加到 iOS 和 macOS 设备。字体必须是 TrueType (.TTF) 或 OpenType (.OFT) 字体。XenMobile 不支持字体集合 (.TTC 或 .OTC)。
主屏幕布局	指定 iOS 9.3 及更高版本受监管设备上 iOS 主屏幕的应用和文件夹布局。
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 XenMobile。该文件包含您使用 Apple Configurator 准备的设备安全策略和限制。
键盘锁管理	控制用户在解锁设备键盘锁和工作挑战键盘锁之前可用的功能。您还可以控制完全托管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，如指纹解锁、信任代理和通知。
信息亭	限制 Samsung SAFE 设备上的应用程序使用。您可以将可用应用程序限制为特定应用程序。此策略适用于仅用于运行特定类型或类别应用程序的企业设备。此策略还允许您为信息亭模式选择设备主屏幕和锁屏壁纸的自定义图像。

设备策略名称	设备策略描述
Knox 企业平台密钥	允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息。
启动器配置	指定 Android 设备上 Citrix Launcher 的设置，例如允许的应用程序和启动器图标的自定义徽标图像。
LDAP	提供用于 iOS 设备的 LDAP 服务器信息，包括任何必要的帐户信息，例如 LDAP 服务器主机名。此策略还提供一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。
位置	允许您在地图上对设备进行地理定位，前提是设备已为 Secure Hub 启用 GPS。将此策略部署到设备后，您可以从 XenMobile Server 发送定位命令。然后设备会响应其位置坐标。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。
受管域	定义适用于电子邮件和 Safari 浏览器的受管域。受管域通过控制哪些应用程序可以打开使用 Safari 从域下载的文档来帮助您保护公司数据。对于 iOS 8 及更高版本的受监督设备，您可以指定 URL 或子域来控制用户如何从浏览器打开文档、附件和下载。
MDM 选项	管理受监督的 iOS 7.0 及更高版本手机设备上的“查找我的手机”和 iPad 激活锁。
组织信息	指定 XenMobile 部署到 iOS 设备的警报消息的组织信息。
密码	在受管设备上强制执行 PIN 码或密码。您可以设置设备上密码的复杂性和超时。
个人热点	允许用户在不在 Wi-Fi 网络范围内时连接到互联网。用户通过其 iOS 设备上的蜂窝数据连接，使用个人热点功能进行连接。

设备策略名称	设备策略描述
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。当您开发和代码签名 iOS 企业应用程序时，通常会包含一个预配配置文件。Apple 要求应用程序在 iOS 设备上运行需要此配置文件。如果预配配置文件丢失或已过期，则当用户点击打开应用程序时，应用程序会崩溃。
预配配置文件移除	移除 iOS 预配配置文件。
代理	指定运行 iOS 的设备的全局 HTTP 代理设置。每个设备只能部署一个全局 HTTP 代理策略。
限制	提供数百种选项来锁定和控制托管设备上的功能。限制选项示例包括：禁用摄像头或麦克风、强制执行漫游规则以及强制访问第三方服务（例如应用商店）。
漫游	配置是否允许 iOS 设备上的语音和数据漫游。如果禁用语音漫游，则数据漫游会自动禁用。
计划	Android 设备连接回 XenMobile Server 以进行 MDM 管理、应用推送和策略部署所需。如果您未将此策略发送到设备且未启用 Google FCM，则设备无法连接回服务器。
SCEP	配置 iOS 和 macOS 设备以从外部 SCEP 服务器检索证书。您还可以使用 SCEP 从连接到 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，以便用户只需登录一次即可访问 XenMobile 和您的内部公司资源。用户无需在设备上存储任何凭据。XenMobile 将企业用户凭据用于跨应用程序（包括来自 App Store 的应用程序）的 SSO 帐户。此策略与 Kerberos 身份验证兼容。适用于 iOS。

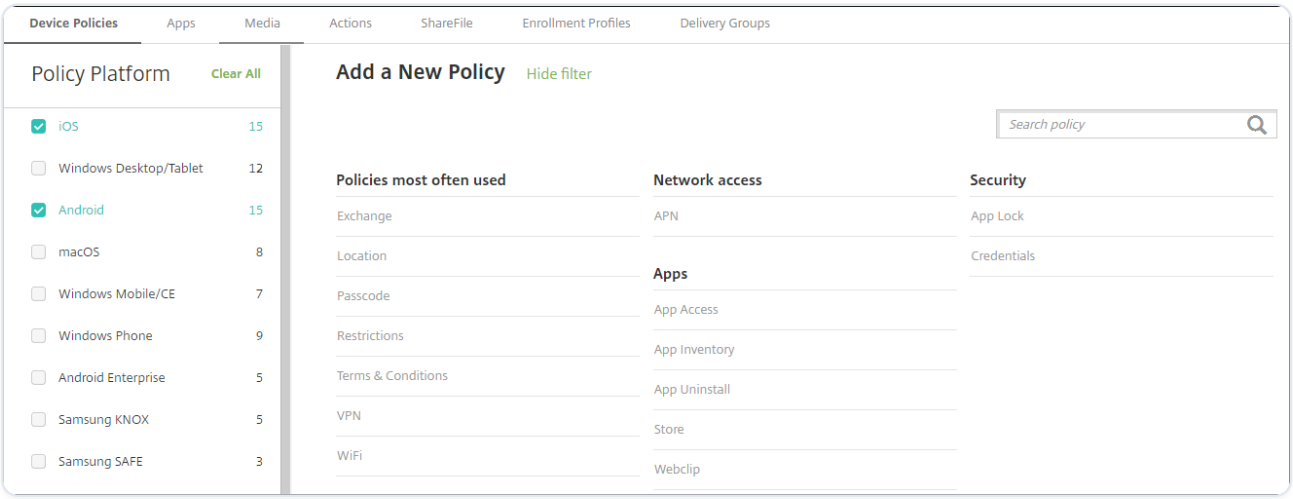
设备策略名称	设备策略描述
订阅的日历	在 iOS 设备上的日历列表中添加订阅日历。请确保在将日历添加到用户设备上的订阅日历列表之前，您已订阅该日历。
条款和条件	要求用户接受公司管理企业网络连接的特定策略。当用户使用 XenMobile 注册其设备时，他们必须接受条款和条件才能注册其设备。拒绝条款和条件将取消注册过程。
隧道	仅用于远程支持。远程支持使您的技术支持代表能够远程控制受管的 Windows CE 和 Android 移动设备。远程支持不适用于群集部署的本地 XenMobile Server。自 January 1, 2019 起，新客户不再提供远程支持。现有客户可以继续使用该产品，但 Citrix 不会提供增强功能或修复。
VPN	提供对使用旧版 VPN 网关技术的后端系统的访问。此策略提供可部署到设备的 VPN 网关连接详细信息。XenMobile 支持多种 VPN 提供商，包括 Cisco AnyConnect、Juniper 和 Citrix VPN。如果您的 VPN 网关支持此选项，您可以将此策略链接到 CA 并启用按需 VPN。
壁纸	添加 .png 或 .jpg 文件以在 iOS 设备的锁定屏幕、主屏幕或两者上设置壁纸。要在 iPad 和 iPhone 上使用不同的壁纸，请创建不同的壁纸策略并将其部署给相应的用户。
Web 内容筛选器	筛选 iOS 设备上的 Web 内容。XenMobile 使用 Apple 自动筛选功能以及您添加到允许列表和阻止列表的站点。仅适用于 iOS 监管设备。
网页快捷方式	将网站快捷方式或 Web 剪辑放置在用户设备上，使其与应用程序一起显示。您可以为 iOS、macOS 和 Android 设备指定自己的图标来表示 Web 剪辑。Windows 平板电脑仅需要标签和 URL。

设备策略名称	设备策略描述
无线局域网	允许管理员将 Wi-Fi 路由器详细信息部署到受管设备。路由器详细信息包括 SSID、身份验证数据和配置数据。
Windows 信息保护	指定需要 Windows 信息保护的应用程序，达到您为策略设置的强制级别。该策略适用于 Windows 10 和 Windows 11 受监管设备。
XenMobile 商店	指定 XenMobile Store Web 剪辑是否显示在用户设备的主屏幕上。
XenMobile 选项	配置从 Android 设备连接到 XenMobile 时的 Secure Hub 行为。
XenMobile 卸载	从 Android 和 Window Mobile/CE 设备卸载 XenMobile。部署后，此策略会从部署组中的所有设备中删除 XenMobile。

按平台划分的设备策略

要查看每个平台可用的策略，请执行以下操作：

1. 在 XenMobile® 控制台中，转到“**配置 > 设备策略**”。
2. 单击“**添加**”。
3. 每个设备平台都显示在“**策略平台**”窗格的列表中。如果该窗格未打开，请单击“**显示筛选器**”。
4. 要查看某个平台可用的所有策略列表，请选择该平台。要查看多个平台可用的策略列表，请选择每个平台。策略仅在适用于所选的每个平台时才显示在列表中。



最新版本的 XenMobile 支持以下平台的设备策略：

- 亚马逊
- 安卓
- 安卓企业版
- 安卓 Zebra
- iOS
- macOS
- 三星 SAFE
- 三星 Knox
- 视窗 10 和 视窗 11 桌面/平板电脑

有关 XenMobile 最新版本中支持的设备的详细信息，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)：
>
> 在为 Windows 10 和 Windows 11 配置 XenMobile 设备策略时，请牢记以下规则。如果一个或多个已注册设备上的策略发生冲突，则与 GPO 一致的策略优先。

AirPlay 镜像设备策略

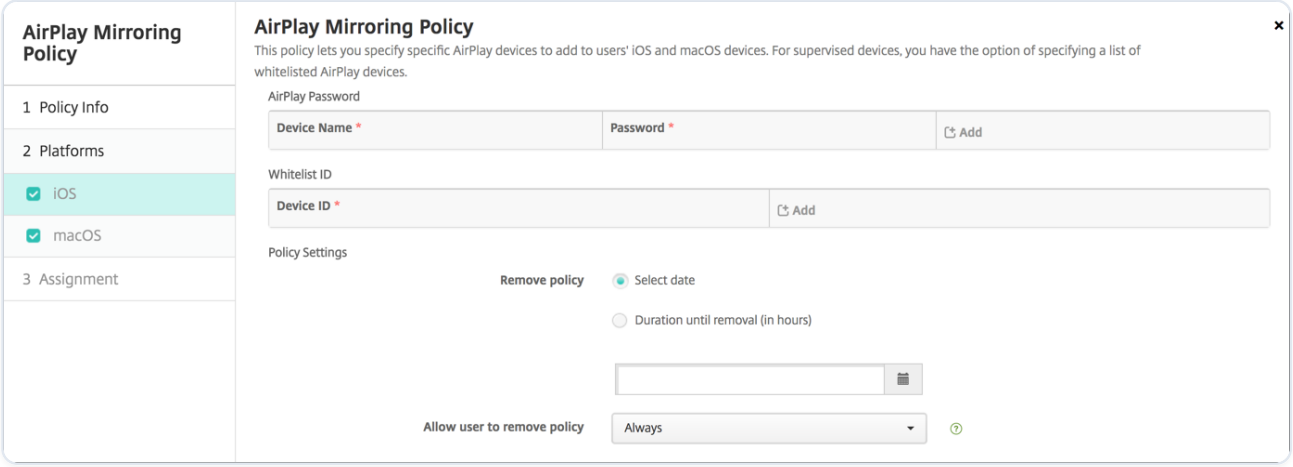
Apple AirPlay 功能允许用户将设备显示屏上的内容精确镜像到另一台 Mac 电脑。

您可以在 XenMobile 中添加设备策略，以将特定的 AirPlay 设备（例如另一台 Mac 电脑）添加到 iOS 设备。您还可以选择将设备添加到受监管设备的允许列表中，这会将用户限制为仅使用允许列表中的 AirPlay 设备。有关将设备置于受监管模式的信息，请参阅 使用 Apple Configurator 将 iOS 设备置于受监管模式。

> **注意：**
>
> 在继续之前，请确保拥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：** 此列表对于非受监管设备将被忽略。此列表中的设备 ID 是用户设备唯一可用的 AirPlay 设备。对于要添加到列表中的每个 AirPlay 设备，单击“**添加**”，然后执行以下操作：

  > **注意：**
  >
  > XenMobile® Server 控制台包含术语“黑名单”和“白名单”。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

  - **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：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。

macOS 设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/airplay-mirroring-policy-macos.png)

- **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：** 对于不受监管的设备，此列表将被忽略。此列表中的设备 ID 是用户设备可用的唯一 AirPlay 设备。对于要添加到列表中的每个 AirPlay 设备，单击“**添加**”，然后执行以下操作：
  - **设备 ID：** 以 xx:xx:xx:xx:xx:xx 格式键入设备 ID。此字段不区分大小写。
  - 单击“**添加**”以添加设备，或单击“**取消**”以取消添加设备。
- **策略设置**
  - **移除策略：** 选择一种计划策略移除的方法。可用选项为**选择日期**和**移除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略移除发生。
  - **允许用户移除策略：** 您可以选择用户何时可以从其设备中移除策略。从菜单中选择**始终**、**需要密码**或**从不**。如果选择**需要密码**，请在**移除密码**字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**用户**。此选项仅在 macOS 10.7 及更高版本上可用。

AirPrint 设备策略

您可以在 XenMobile® 中添加设备策略，以将 AirPrint 打印机添加到 iOS 设备上的 AirPrint 打印机列表。此策略有助于支持打印机和设备位于不同子网中的环境。

此策略适用于 iOS 7.0 及更高版本。

> **注意：**

> 请务必获取每台打印机的 IP 地址和资源路径。

> 要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

- **AirPrint 目标：** 对于要添加的每个 AirPrint 目标，请单击**添加**，然后执行以下操作：
  - **IP 地址：** 输入 AirPrint 打印机 IP 地址。
  - **资源路径：** 输入与打印机关联的资源路径。此值对应于 _ipps.tcp Bonjour 记录的参数。例如，printers/Canon_MG5300_series 或 printers/Xerox_Phaser_7600。
  - 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：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：** 输入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。

Android Enterprise 应用权限

您可以配置工作配置文件中 Android Enterprise 应用的请求如何处理 Google 所谓的“危险”权限。您可以控制是否提示用户授予或拒绝来自应用的权限请求。此功能适用于运行 Android 7.0 及更高版本的设备。

Google 将危险权限定义为允许应用访问涉及用户私人信息的数据或资源，或者可能影响用户存储数据或其他应用操作的权限。例如，读取用户联系人的能力就是一种危险权限。

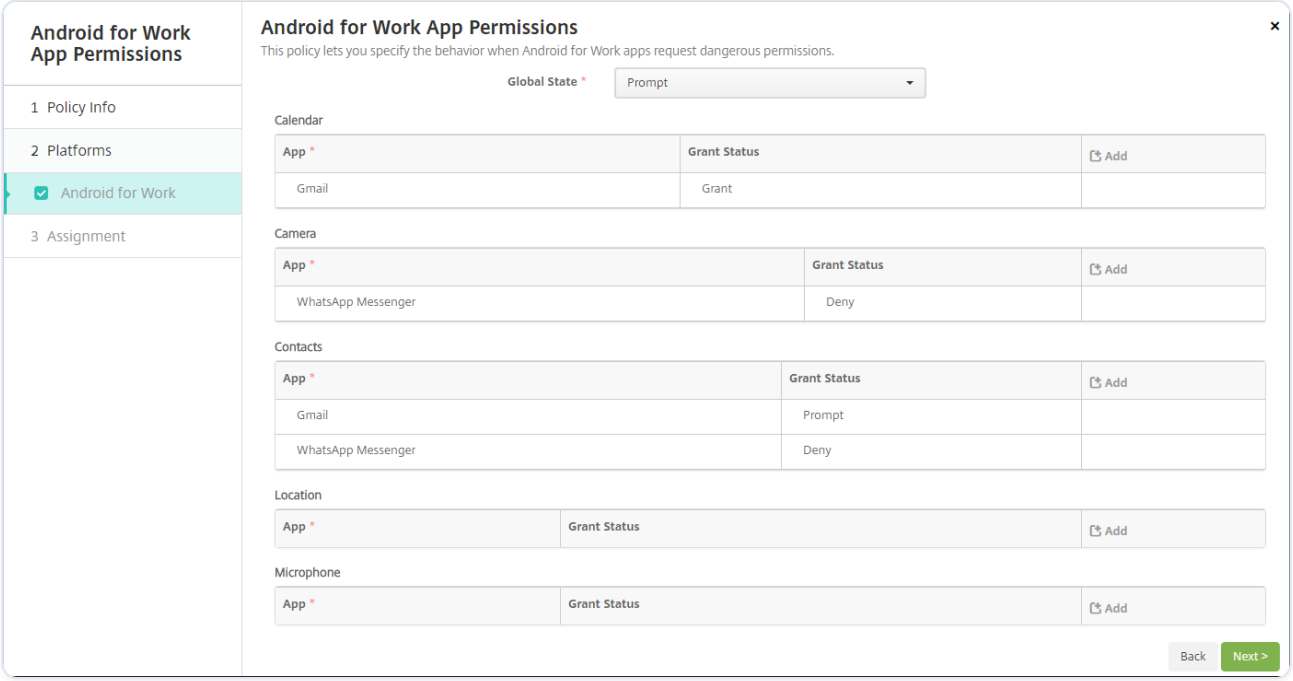
您可以配置一个全局状态，用于控制工作配置文件中所有 Android Enterprise 应用的危险权限请求行为。您还可以针对每个应用，控制 Google 定义的各个权限组的危险权限请求行为。这些单独的设置会覆盖全局状态。

有关 Google 如何定义权限组的信息，请参阅此Android 开发者指南中的“权限组”。

默认情况下，系统会提示用户授予或拒绝危险权限请求。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

Android 企业版设置



- **全局状态：** 控制所有危险权限请求的行为。在列表中，单击**提示**、**授予**或**拒绝**。
  - **提示：** 系统会提示用户授予或拒绝危险权限请求。
  - **授予：** 所有危险权限请求都将获得授予。系统不会提示用户。
  - **拒绝：** 所有危险权限请求都将被拒绝。系统不会提示用户。

  默认值为**提示**。
- 为每个应用中的每个权限组设置单独的行为。要配置权限组的行为：单击**添加**。在**应用**下，从列表中选择一个应用。如果配置 Android Enterprise 系统应用，请单击**添加新项**并输入您在“限制”设备策略中启用的应用程序包名称。在“授予状态”下，选择**提示**、**授予**或**拒绝**。此授予状态将覆盖全局状态。
  - **提示：** 系统会提示用户授予或拒绝此应用从此权限组发出的危险权限请求。
  - **授予：** 此应用从此权限组发出的危险权限请求将获得授予。系统不会提示用户。

    > **注意：**
    >
    > 对于以 **配置文件所有者** 模式注册的设备，如果设备运行的是 Android 12 或更高版本，则 **授予** 权限不适用于摄像头、位置、麦克风和传感器。

  - **拒绝：** 此应用从此权限组发出的危险权限请求将被拒绝。系统不会提示用户。

默认值为 **提示**。

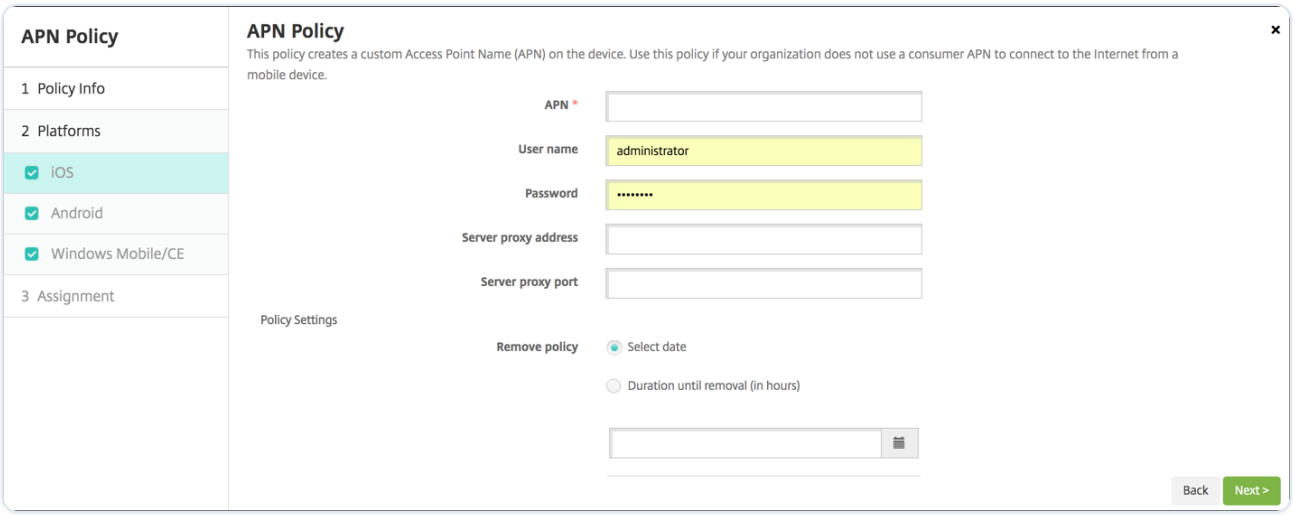
- 单击应用和授予状态旁边的 **保存**。
- 要为此权限组添加更多应用，请再次单击 **添加** 并重复这些步骤。
- 完成所有所需权限组的授予状态设置后，单击 **下一步**。

APN 设备策略

您可以为 iOS 和 Android 设备添加自定义的接入点名称 (APN) 设备策略。如果您的组织不使用消费者 APN 从移动设备连接到 Internet，则可以使用此策略。APN 策略确定用于将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 的设置。此设置已在大多数新型手机中定义。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置



- **APN：** 键入接入点的名称。此 APN 名称必须与接受的 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。如果缺少用户名，设备将在配置文件安装期间提示输入该字符串。
- **密码：** 此 APN 用户的密码。出于混淆目的，密码已编码。如果有效负载中缺少密码，设备将在配置文件安装期间提示输入密码。
- **服务器代理地址：** APN 代理的 IP 地址或 URL。
- **服务器代理端口：** APN 代理的端口号。如果输入了服务器代理地址，则需要此服务器代理端口号。
- 在**策略设置**下，在**删除策略**旁边，单击**选择日期**或**删除前持续时间（小时）**。
  - 如果单击**选择日期**，单击日历以选择要删除的具体日期。
  - 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**删除密码**旁边，键入必要的密码。

- **策略设置**
  - **移除策略：** 选择策略移除的计划方法。可用选项包括**选择日期**和**移除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略移除。仅适用于 iOS 6.0 及更高版本。

Android 设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/devicepolicy-apn-android.png)

- **APN：** 键入接入点的名称。此 APN 名称必须与接受的 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。如果缺少用户名，设备将在配置文件安装期间提示输入该字符串。
- **密码：** 此 APN 用户的密码。为混淆目的，密码已编码。如果负载中缺少密码，设备将在配置文件安装期间提示输入密码。
- **服务器：** 此设置早于智能手机，通常为空。它引用了无线应用协议 (WAP) 网关服务器，适用于可能无法访问标准网站的手机。
- **APN 类型：** 此设置必须与运营商对接入点的预期用途匹配。它是一个逗号分隔的 APN 服务指定符字符串，必须与无线运营商发布的定义匹配。示例包括：
  - *: 所有流量都通过此接入点。
  - mms: 多媒体流量通过此接入点。
  - default: 所有流量（包括多媒体）都通过此接入点。
  - supl: 安全用户平面定位与辅助 GPS 相关联。
  - dun: 拨号网络已过时，很少使用。
  - hipri" 高优先级网络。
  - fota: 固件空中下载用于接收固件更新。
- **身份验证类型：** 在下拉列表中单击要使用的身份验证类型。默认为“无”。
- **服务器代理地址：** 运营商 APN HTTP 代理的 IP 地址或 URL。
- **服务器代理端口：** APN 代理的端口号。如果输入了服务器代理地址，则需要此服务器代理端口号。
- **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：** 这是用于 MMS 流量的多媒体消息服务服务器。MMS 成功取代 SMS，用于发送包含图片或视频等多媒体内容的较大消息。这些服务器需要特定的协议（例如 MM1，... MM11）。
- **MMS 端口：** 用于 MMS 代理的端口。

应用访问设备策略

XenMobile® 中的应用访问设备策略允许您定义以下内容：

- 需要在设备上安装的应用列表。
- 可以在设备上安装的应用列表。
- 不得在设备上安装的应用列表。

然后，您可以创建自动化操作以响应设备与应用列表的合规性。您可以为 iOS 和 Android 设备创建应用访问策略。

您一次只能配置一种访问策略。您可以为所需应用列表、建议应用列表或不允许的应用列表添加策略，但不能在同一个应用访问策略中混合使用。如果您为每种类型的列表创建策略，建议您仔细命名每个策略。仔细命名每个策略可让您了解 XenMobile 中的哪个策略适用于哪个应用列表。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅设备策略。

平台设置

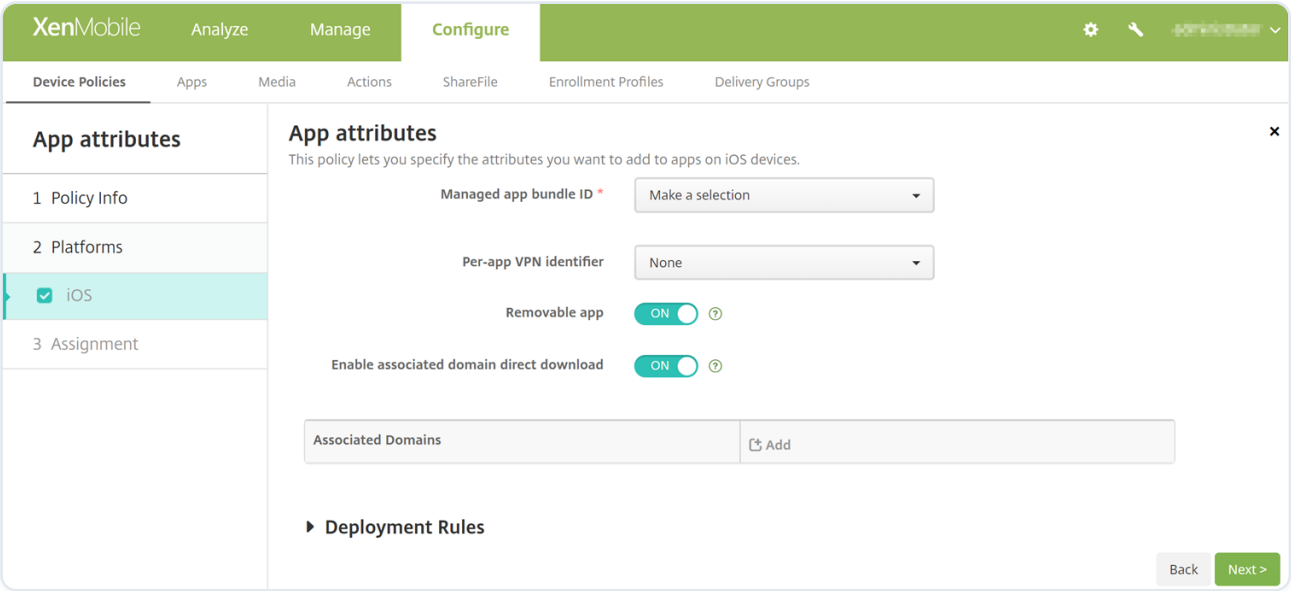
- **访问策略：** 单击**必需**、**建议**或**禁止**。默认值为**必需**。
- 要向列表中添加一个或多个应用，请单击**添加**，然后执行以下操作：
  - **应用名称：** 输入应用名称。
  - **应用标识符：** 输入可选的应用标识符。
  - 单击**保存**或**取消**。
  - 对要添加的每个应用重复这些步骤。

应用程序属性设备策略

应用程序属性设备策略允许您为 iOS 设备指定属性，例如托管应用程序捆绑包 ID 或按应用程序 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：**通过以下方式指定应用程序：
  - 选择应用程序捆绑包 ID。只有在启用“**应用程序清单**”设备策略（该策略收集托管设备上的应用程序清单）后，选项才可用。
  - 选择“**添加新项**”，然后键入应用程序捆绑包 ID。 要查找应用程序捆绑包 ID，请参阅在 App Store 中查找应用程序的捆绑包 ID。
- **按应用程序 VPN 标识符：**（可选）为此应用程序选择一个按应用程序 VPN。选项包括您在**设备策略** > **VPN 策略**页面上配置的按应用程序 VPN 连接。有关详细信息，请参阅配置按应用程序 VPN。
- **可移除应用程序：**（可选）指定当应用程序为托管应用程序时，用户是否可以移除该应用程序。要阻止用户卸载应用程序，请将此选项设置为“**关**”。默认值设置为“**开**”。适用于 iOS 14 及更高版本。
- **启用关联域直接下载：**（可选）指定应用程序是否可以直接在域而不是 Apple 服务器上执行声明的站点关联验证。仅对于无法访问 Internet 的域，才将此选项设置为“**开**”。默认值设置为“**开**”。适用于 iOS 14 及更高版本。
- **关联域：**（可选）要为此应用程序添加关联域，请单击“**添加**”，然后键入其完全限定域名 (FQDN)。适用于 iOS 13 及更高版本。

在 App Store 中查找应用程序的捆绑包 ID

1. 在 App Store 中找到该应用程序并复制 URL 末尾的数字。例如，363501921 是 Citrix Workspace 应用程序的应用程序 ID。
2. 转到 `https://itunes.apple.com/lookup?id=` 并在该 URL 后粘贴该数字。TXT 文件将自动下载到您的计算机。

3. 在 TXT 文件中，搜索 `bundleId` 并获取应用程序的捆绑包 ID。例如，Citrix Workspace 应用程序的捆绑包 ID 为 `com.citrix.ReceiveriPad`。

应用程序配置设备策略

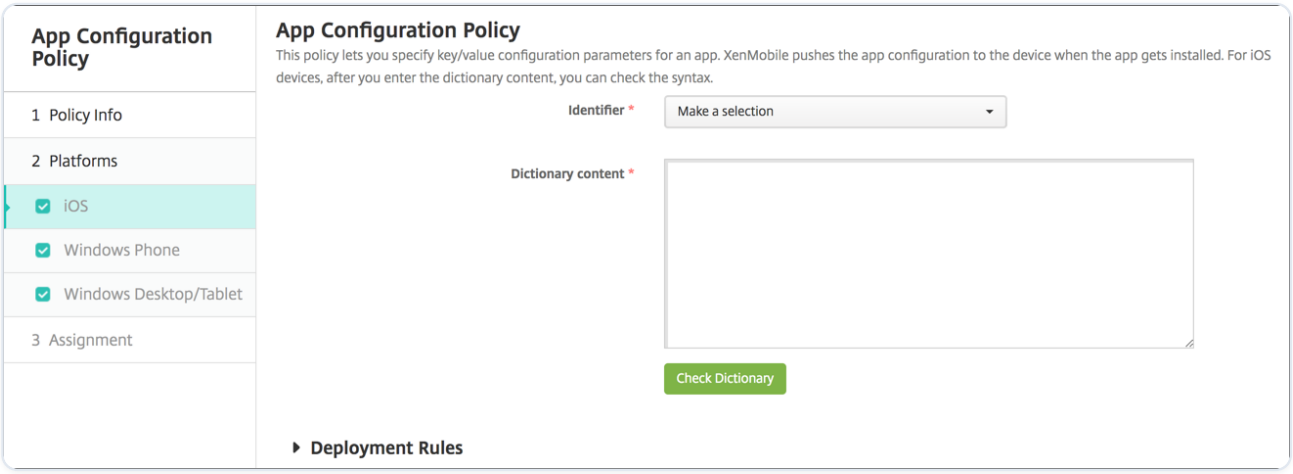
您可以通过部署以下方式远程配置支持托管配置的应用程序：

- XML 配置文件（称为属性列表或 plist）到 iOS 设备
- 或者，用于运行 Windows 10 或 Windows 11 的 Windows 10 手机、平板电脑或桌面设备的键/值对。

此配置指定应用程序中的各种设置和行为。XenMobile® 会在用户安装应用程序时将配置推送到设备。您可以配置的实际设置和行为取决于应用程序，并且超出了本文的范围。

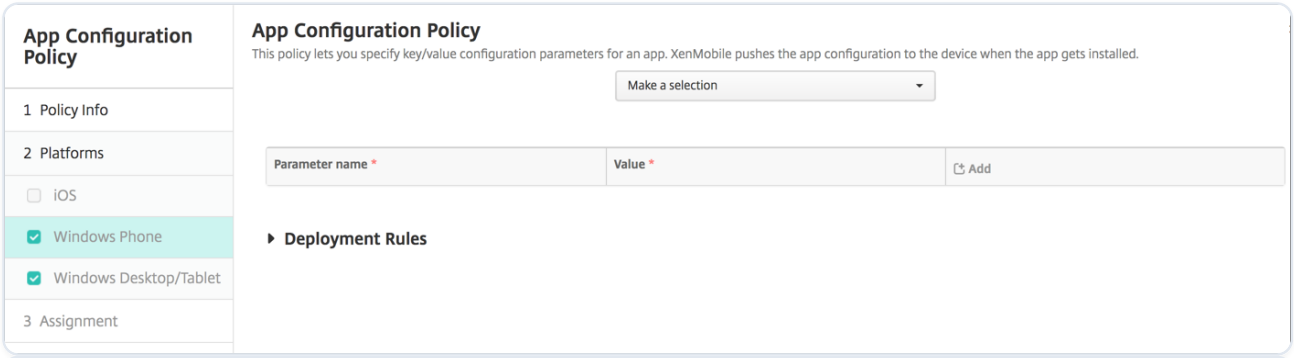
要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅设备策略。

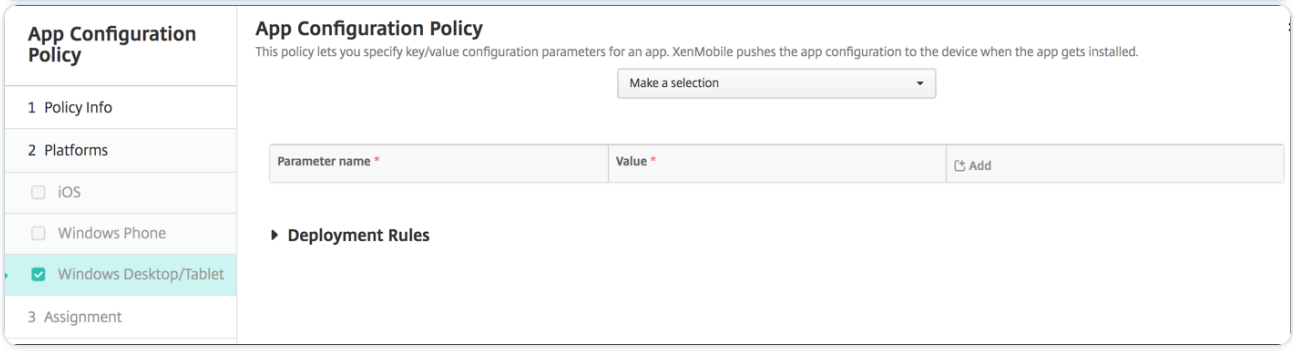
iOS 设置



- **标识符：** 在下拉列表中单击要配置的应用程序，或单击 **Add new** 将应用程序添加到列表中。
  - 如果单击 **Add new**，请在出现的字段中键入应用程序标识符。
- **字典内容：** 键入或复制并粘贴 XML 属性列表 (plist) 配置信息。
- 单击 **Check Dictionary**。XenMobile 将验证 XML。如果没有错误，您将在内容框下方看到 **Valid XML**。如果内容框下方出现任何语法错误，您必须先更正它们才能继续。

Windows 桌面和平板电脑设置





- 在“**进行选择**”列表中，单击要配置的应用程序，或单击“**添加新项**”将应用程序添加到列表中。
  - 如果单击“**添加新项**”，请在出现的字段中键入包系列名称。
- 对于要添加的每个配置参数，请单击“**添加**”，然后执行以下操作：
  - **参数名称：** 输入 Windows 设备的应用程序设置的密钥名称。有关 Windows 应用程序设置的信息，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。

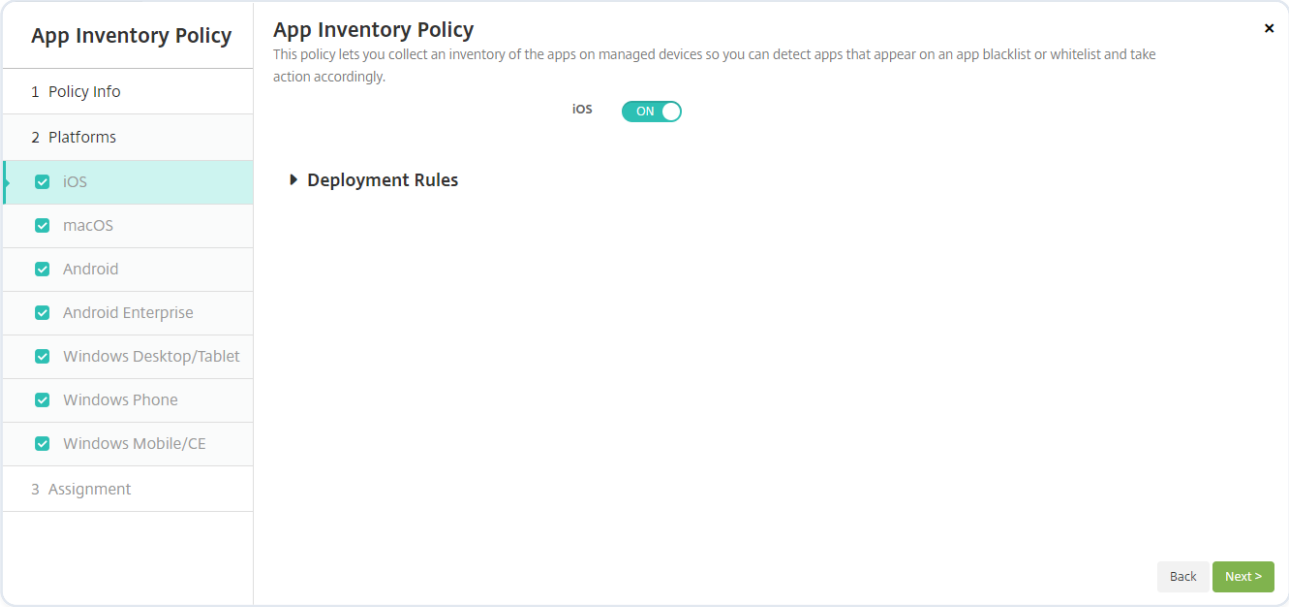
应用清单设备策略

应用清单策略允许您收集受管设备上的应用清单。然后，XenMobile® 可以将此清单与部署到这些设备的任何应用访问策略进行比较。通过这种方式，您可以检测出现在应用允许列表或阻止列表中的应用，并采取正确措施。

您可以创建适用于 iOS、macOS、Android、Android Enterprise 或 Windows 桌面/平板电脑设备的应用程序访问策略。

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



- 对于您选择的每个平台，保留默认设置或将设置更改为**关**。默认设置为**开**。

应用锁定设备策略

应用锁定设备策略定义了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。您可以为 iOS 和 Android 设备配置此策略，但策略的具体工作方式因平台而异。例如，您无法在 iOS 设备上阻止多个应用程序。

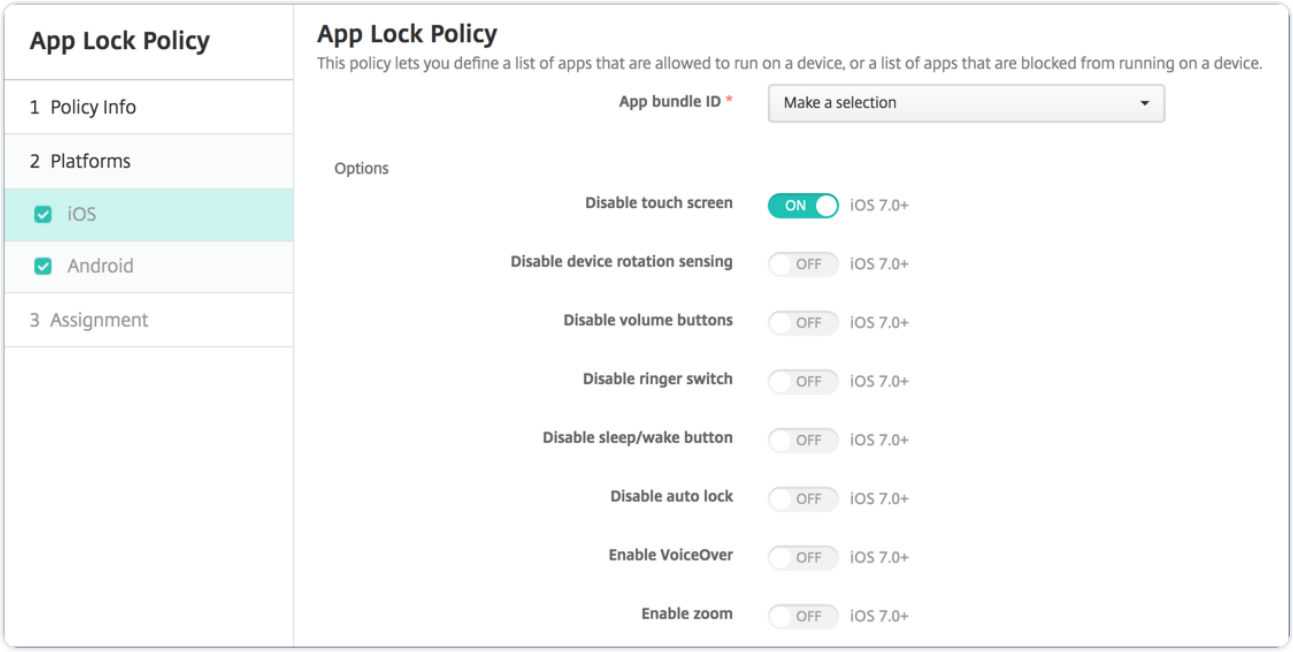
同样，对于 iOS 设备，每个策略只能选择一个 iOS 应用程序。这意味着用户只能使用其设备运行单个应用程序。除了在实施应用锁定策略时您明确允许的选项外，他们无法在设备上执行任何其他活动。

此外，iOS 设备必须处于受监管状态才能推送应用锁定策略。

尽管设备策略适用于大多数 Android L 和 M 设备，但应用锁定在 Android N 或更高版本的设备上不起作用，因为 Google 已弃用所需的 API。

要添加或配置此策略，请转到**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置



- **应用捆绑包 ID：** 单击下拉列表中此策略适用的应用程序，或单击**添加新项**将应用程序添加到列表中。如果选择**添加新项**，请在出现的字段中键入应用程序名称。
- **选项：** 以下每个选项仅适用于 iOS 7.0 或更高版本。对于每个选项，默认值为**关**，但“禁用触摸屏”除外，其默认值为**开**。
  - 禁用触摸屏
  - 禁用设备旋转感应
  - 禁用音量按钮
  - 禁用响铃开关

    当“禁用响铃开关”为**开**时，响铃行为取决于首次禁用时开关所处的位置。
  - 禁用睡眠/唤醒按钮
  - 禁用自动锁定
  - 禁用旁白
  - 启用缩放
  - 启用反转颜色
  - 启用辅助触控
  - 启用朗读所选内容
  - 启用单声道音频
- **用户启用选项：以下每个选项仅适用于 iOS 7.0 或更高版本。对于每个选项，默认值为关闭。**

  - 允许调整旁白
  - 允许调整缩放
  - 允许调整反转颜色
  - 允许调整辅助触控

- **策略设置**
  - **删除策略：选择一种计划策略删除的方法。可用选项为选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略被移除。仅适用于 iOS 6.0 及更高版本。

Android 设置

> **注意：**

> 您无法通过使用应用程序锁定设备策略来阻止 Android 设置应用程序。

> 设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-applock-android.png)

- **应用程序锁定参数**
  - **锁定消息：** 键入用户尝试打开锁定的应用程序时看到的消息。
  - **解锁密码：** 键入用于解锁应用程序的密码。
  - **阻止卸载：** 选择是否允许用户卸载应用程序。默认值为“**关**”。
  - **锁定屏幕：** 通过单击“浏览”并导航到文件位置，选择设备锁定屏幕上显示的图像。
  - **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列表，或单击“**白名单**”以创建允许在设备上运行的应用程序列表。

    > **注意：**

    > XenMobile® Server 控制台包含术语“黑名单”和“白名单”。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

- **应用程序：** 单击“**添加**”，然后执行以下操作：

- **应用程序名称：** 单击下拉列表中的应用程序名称以添加到允许列表或阻止列表，或单击“**添加新项**”以将应用程序添加到可用应用程序列表。
- 如果选择“**添加新项**”，请在出现的字段中键入应用程序名称。
- 单击“**保存**”或“**取消**”。
- 对要添加到允许列表或阻止列表的每个应用程序重复这些步骤。

应用程序网络使用设备策略

您可以设置网络使用规则，以指定托管应用程序如何使用网络，例如 iOS 设备上的蜂窝数据网络。这些规则仅适用于托管应用程序。托管应用程序是指您通过 XenMobile 部署到用户设备上的应用程序。它们不包括用户在未通过 XenMobile 部署的情况下直接下载到其设备上的应用程序，也不包括设备在注册到 XenMobile 时已安装在设备上的应用程序。

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

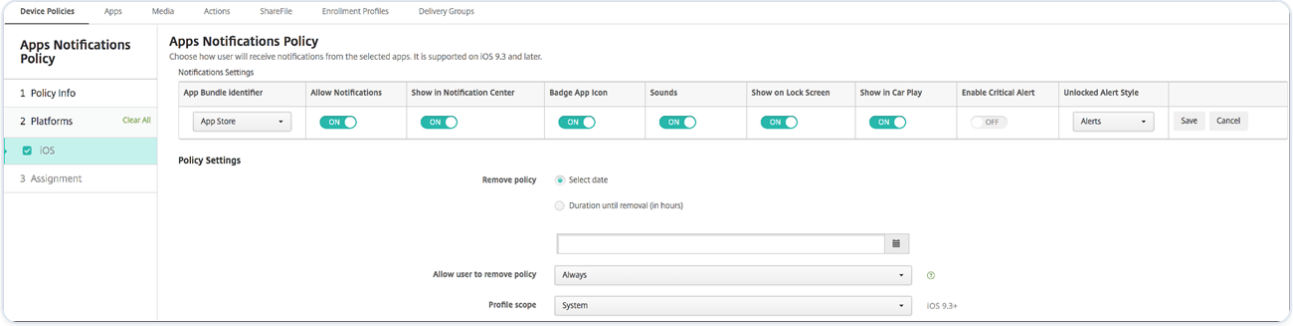
- **允许漫游蜂窝数据：** 选择指定的应用程序在漫游时是否可以使用蜂窝数据连接。默认值为 **关闭**。
- **允许蜂窝数据：** 选择指定的应用程序是否可以使用蜂窝数据连接。默认值为 **关闭**。
- **应用程序标识符匹配：** 对于要添加到列表中的每个应用程序，单击 **添加**，然后执行以下操作：
  - **应用程序标识符：** 输入应用程序标识符。
  - 单击 **保存** 将应用程序保存到列表，或单击 **取消** 不将应用程序保存到列表。

应用通知设备策略

应用通知策略允许您控制 iOS 用户如何接收来自指定应用的通知。此策略支持运行 iOS 9.3 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** 以允许通知。
- **在通知中心显示：** 选择 **开** 以在用户设备的通知中心显示通知。
- **标记应用图标：** 选择 **开** 以显示带有通知的标记应用图标。
- **声音：** 选择 **开** 以在通知中包含声音。
- **在锁定屏幕上显示：** 选择 **开** 以在用户设备的锁定屏幕上显示通知。
- **在 CarPlay 中显示：** 如果为 **开**，则通知将显示在 Apple CarPlay 中。适用于 iOS 12 及更高版本。默认值为 **开**。
- **启用紧急警报：** 如果为 **开**，则应用程序可以将通知标记为紧急通知，该通知将忽略“勿扰”和铃声设置。适用于 iOS 12 及更高版本。默认值为 **关**。
- **解锁警报样式：** 在列表中，选择 **无**、**横幅** 或 **警报** 以配置解锁警报的显示方式。
- **策略设置**
  - **移除策略：** 选择策略移除的计划方法。可用选项包括**选择日期**和**移除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略移除发生。仅适用于 iOS 6.0 及更高版本。
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**系统**。此选项仅适用于 iOS 9.3 及更高版本。

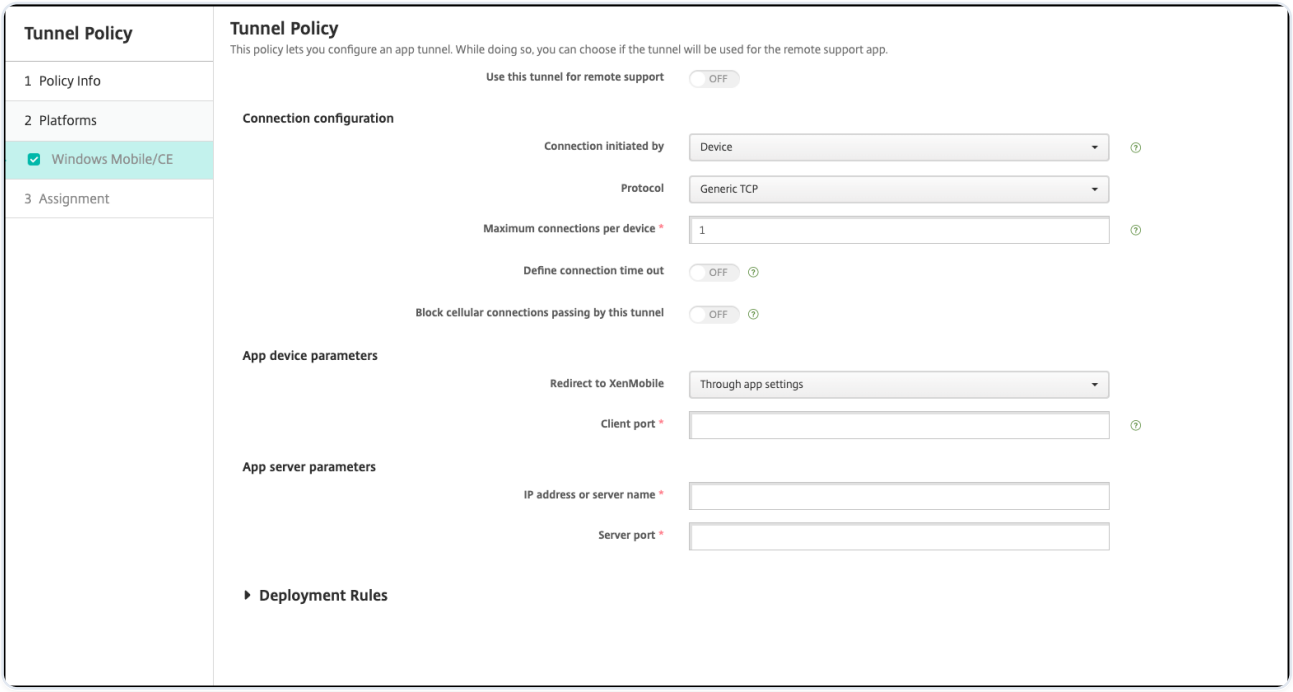
隧道设备策略

应用程序隧道（应用隧道）旨在提高移动应用程序的服务连续性和数据传输可靠性。应用隧道定义了任何移动设备应用程序的客户端组件与应用程序服务器组件之间的代理参数。您可以为 Android 设备配置隧道策略。

通过此策略中定义的隧道发送的任何应用流量都将先通过 XenMobile®，然后才重定向到运行该应用的服务器。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

Android 设置



- **连接发起方：** 单击**设备**或**服务器**以指定启动连接的源。
- **每个设备的最大连接数：** 键入一个数字以指定应用可以建立的并发 TCP 连接数。此字段仅适用于设备发起的连接。
- **定义连接超时：** 选择是否设置应用在隧道关闭前可以保持空闲的时间长度。
  - **连接超时：** 如果将**定义连接超时**设置为**开**，请键入应用在隧道关闭前可以保持空闲的时间长度（以秒为单位）。
- **阻止通过此隧道的蜂窝连接：** 选择漫游时是否阻止此隧道。Wi-Fi 和 USB 连接不会被阻止。
- **重定向到 XenMobile：** 选择**通过应用设置**。
- **客户端端口：** 键入客户端端口号。通常，此值与服务器端口相同。
- **IP 地址或服务器名称：** 键入应用服务器的 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。

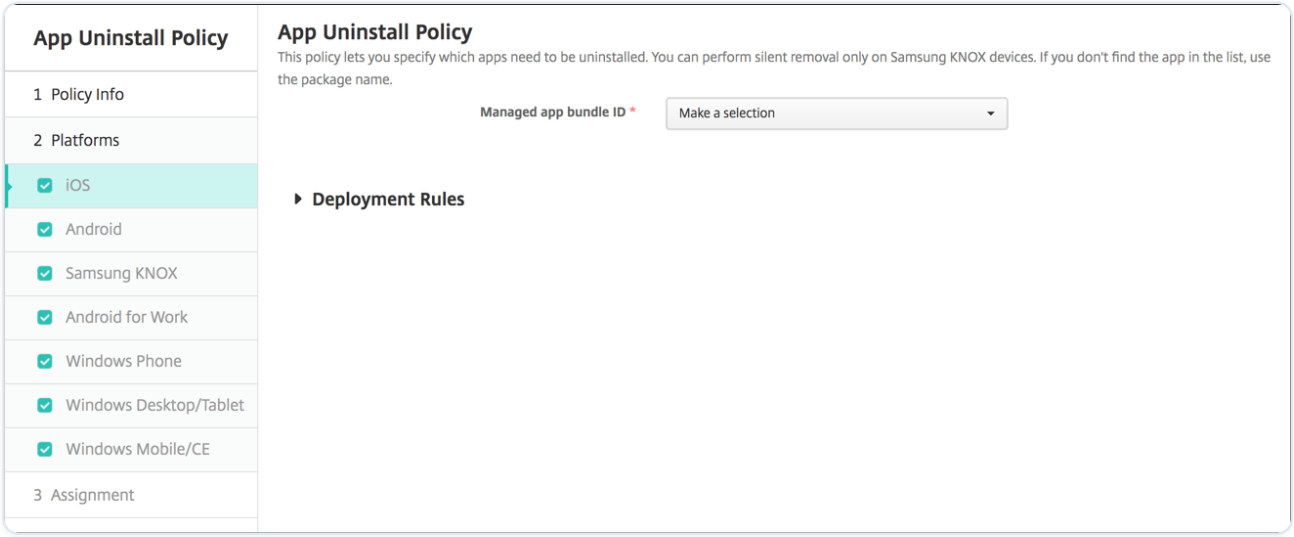
应用卸载设备策略

您可以为 iOS、Android、Samsung Knox、Android Enterprise 和 Windows Desktop/Tablet 平台创建应用卸载策略。应用卸载策略允许您出于多种原因从用户设备中删除应用。例如，您可能不再希望支持某些应用，您的公司可能希望用不同供应商的类似应用替换现有应用等。

将此策略部署到用户设备后，应用将被删除。除 Samsung Knox 设备外，用户会收到卸载应用的提示。Samsung Knox 设备用户不会收到卸载应用的提示。

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



- **托管应用捆绑包 ID：单击下拉列表中的现有应用或单击添加新应用**。如果此平台未配置任何应用，则列表将为空，您必须添加一个应用。
  - 单击**添加**时，将出现一个字段，您可以在其中键入应用名称。

所有其他平台设置

- **要卸载的应用：对于要添加的每个应用，请单击添加**，然后执行以下操作：
  - **应用名称：单击下拉列表中的现有应用或单击添加新应用**以输入新的应用名称。如果此平台未配置任何应用，则列表将为空，您必须添加新应用。
  - 单击**添加**以添加应用，或单击**取消**以取消添加应用。

在相应的公共应用商店应用安装后自动卸载企业应用

您可以将 XenMobile® 配置为在安装公共应用商店版本后删除 Citrix® 应用的企业版本。此功能可防止用户设备在安装公共应用商店版本后出现两个相同的应用图标。

应用卸载设备策略的部署条件会触发 XenMobile 在安装新版本后从用户设备中删除旧应用。此功能仅适用于以企业模式 (XME) 连接到 XenMobile Server 的托管 iOS 设备。

要配置具有“已安装应用程序名称”条件的部署规则：

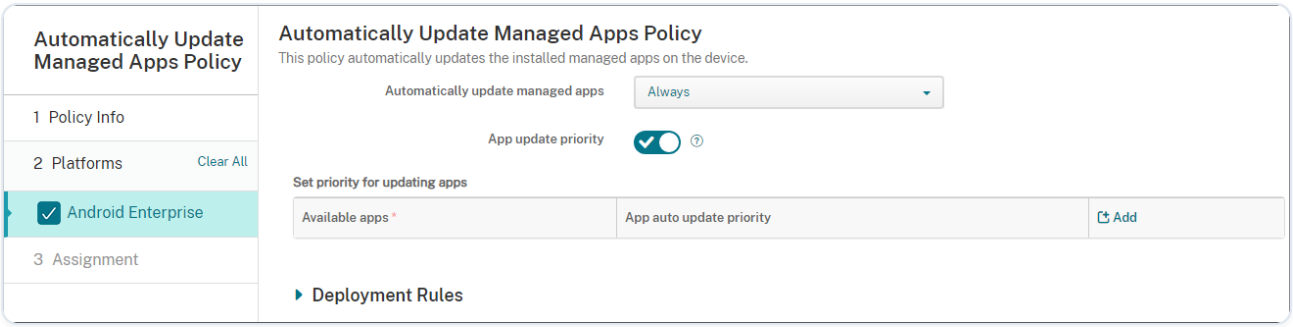
- 指定企业应用程序的**托管应用程序捆绑包 ID**。
- 添加规则：单击**新建规则**，然后，如示例所示，选择**已安装应用程序名称**和**等于**。键入公共应用商店应用程序的应用程序捆绑包 ID。

在此示例中，当公共应用商店应用程序 (com.citrix.mail.ios) 安装在指定交付组中的设备上时，XenMobile 将删除企业版 (com.citrix.mail)。

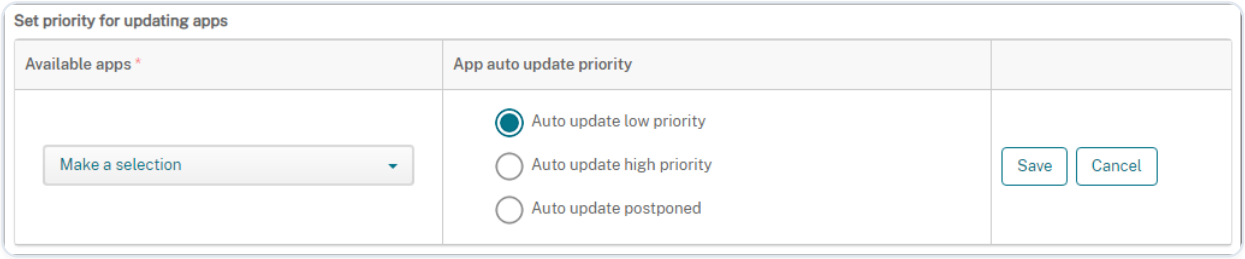
自动更新托管应用程序设备策略

此策略控制 Android Enterprise 设备上已安装的托管应用程序的更新方式。您可以限制用户在其设备上允许应用程序自动更新的功能。如果您允许用户控制其设备上应用程序的自动更新，他们将在托管的 Google Play 商店中设置自动应用程序更新策略。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅设备策略。



- **自动更新托管应用程序**
  - **始终：** 启用自动应用程序更新。**始终**是默认设置。
  - **允许用户配置策略：** 允许用户在托管的 Google Play 商店中为设备配置自动应用程序更新策略。
  - **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 时才允许自动应用程序更新。
- **应用程序更新优先级：** 如果为**开**，则可以为每个托管应用程序配置更新优先级级别。
- **设置应用程序更新优先级：** 单击**添加**以配置应用程序的更新优先级。



- **可用应用程序：** 从菜单中选择一个应用程序以配置更新优先级。
- **应用程序自动更新优先级：** 从以下选项中选择一个更新优先级：
  - **自动更新低优先级：** 当设备正在充电、未被主动使用且连接到非计量网络时，应用程序会更新。
  - **高优先级自动更新：** 应用程序会尽快更新，不受限制。
  - **推迟自动更新：** 在新版本可用后，应用程序最长 90 天内不会自动更新。90 天后，应用程序将以低优先级自动更新。应用程序更新后，在接下来的 90 天内不会再次自动更新。用户可以随时手动更新应用程序。
- 完成后，单击 **保存**。您可以通过单击铅笔图标来编辑配置。通过单击垃圾桶图标删除配置。

BitLocker 设备策略

Windows 10 和 Windows 11 包含一个名为 BitLocker 的磁盘加密功能，该功能可提供额外的文件和系统保护，防止丢失或被盗的 Windows 设备遭到未经授权的访问。为了获得更多保护，您可以将 BitLocker 与受信任的平台模块 (TPM) 芯片（版本 1.2 或更高版本）结合使用。TPM 芯片负责处理加密操作，并生成、存储和限制加密密钥的使用。

从 Windows 10 版本 1703 开始，MDM 策略可以控制 BitLocker。您可以使用 XenMobile® 中的 BitLocker 设备策略来配置 Windows 10 和 Windows 11 设备上 BitLocker 向导中可用的设置。例如，在启用了 BitLocker 的设备上，BitLocker 可以提示用户如何在启动时解锁其驱动器、如何备份其恢复密钥以及如何解锁固定驱动器。BitLocker 设备策略设置还配置是否执行以下操作：

- 在没有 TPM 芯片的设备上启用 BitLocker。
- 在 BitLocker 界面中显示恢复选项。
- 在未启用 BitLocker 时，拒绝写入固定或可移动驱动器。

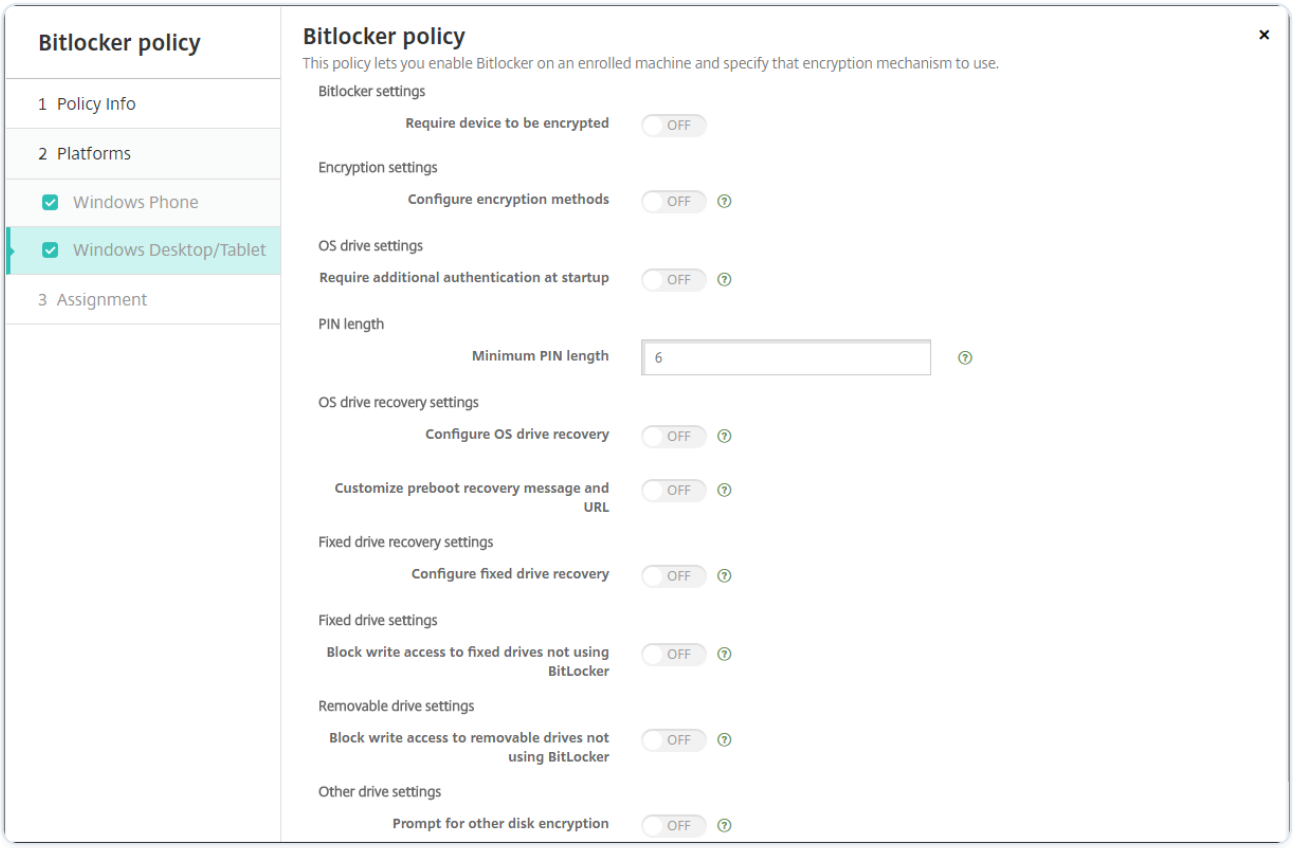
> **注意：**
>
> 设备上的 BitLocker 加密启动后，您无法通过部署更新的 BitLocker 设备策略来更改设备上的 BitLocker 设置。

> 要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

要求

- BitLocker 设备策略需要 Windows 10 或 Windows 11 企业版。
- 在部署 BitLocker 设备策略之前，请为 BitLocker 的使用准备好您的环境。有关 Microsoft 提供的详细信息，包括 BitLocker 系统要求和设置，请参阅 BitLocker 以及该节点下的文章。

Windows 桌面和平板电脑设置



- **要求设备加密：** 确定是否提示用户在 Windows 桌面或平板电脑上启用 BitLocker 加密。如果设置为**开**，设备在注册完成后会显示一条消息，指示企业要求设备加密。如果设置为**关**，则不会提示用户，并且 BitLocker 将使用策略设置。默认为**关**。
- **配置加密方法**：确定用于特定驱动器类型的加密方法。如果设置为**关**，BitLocker 向导会提示用户选择用于驱动器类型的加密方法。所有驱动器的加密方法默认为 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 将使用策略中指定的加密方法。如果设置为**开**，将显示以下额外设置：**操作系统驱动器**、**固定驱动器**和**可移动驱动器**。选择每种驱动器类型的默认加密方法。默认为**关**。
- **启动时需要额外身份验证**：指定设备启动期间所需的额外身份验证。还指定是否允许在没有 TPM 芯片的设备上使用 BitLocker。如果设置为**关**，没有 TPM 的设备无法使用 BitLocker 加

密。有关 TPM 的信息，请参阅 Microsoft 文章 受信任的平台模块技术概述。如果设置为**开**，将显示以下额外设置。默认为**关**。

- **阻止在没有 TPM 芯片的设备上使用 BitLocker**：在没有 TPM 芯片的设备上，BitLocker 要求用户创建解锁密码或启动密钥。启动密钥存储在 USB 驱动器中，用户必须在启动前将其连接到设备。解锁密码至少为八个字符。默认为**关**。
- **TPM 启动**：在具有 TPM 的设备上，有四种解锁模式：仅限 TPM、TPM + PIN、TPM + 密钥和 TPM + PIN + 密钥。TPM 启动适用于仅限 TPM 模式，其中加密密钥存储在 TPM 芯片中。此模式不需要用户提供更多解锁数据。用户设备在重新启动期间会自动解锁，使用 TPM 芯片中的加密密钥。默认为**允许 TPM**。
- **TPM 启动 PIN**：此设置为 TPM + PIN 解锁模式。PIN 最多可包含 20 位数字。使用**最小 PIN 长度**设置指定最小 PIN 长度。用户在 BitLocker 设置期间配置 PIN，并在设备启动期间提供 PIN。
- **TPM 启动密钥**：此设置为 TPM + 密钥解锁模式。启动密钥存储在 USB 或其他可移动驱动器中，用户必须在启动前将其连接到设备。
- **TPM 启动密钥和 PIN**：此设置为 TPM + PIN + 密钥解锁模式。

  如果解锁成功，操作系统将开始加载。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。默认为**6**。
- **配置操作系统驱动器恢复**：如果解锁步骤失败，BitLocker 会提示用户输入配置的恢复密钥。此设置配置了在用户没有解锁密码或 USB 启动密钥时可用的操作系统驱动器恢复选项。默认为**关**。
  - **允许基于证书的数据恢复代理**：指定是否允许基于证书的数据恢复代理。从“公钥策略”添加数据恢复代理，该策略位于“组策略管理控制台 (GPMC)”或“本地组策略编辑器”中。有关数据恢复代理的更多信息，请参阅 Microsoft 文章 BitLocker 组策略设置。默认为**关**。
  - **为操作系统驱动器恢复创建 48 位恢复密码**：指定是允许还是要求用户使用恢复密码。BitLocker 生成密码并将其存储在文件或 Microsoft 云帐户中。默认为**允许 48 位密码**。
  - **创建 256 位恢复密钥**：指定是允许还是要求用户使用恢复密钥。恢复密钥是一个 BEK 文件，存储在 USB 驱动器上。默认为**允许 256 位恢复密钥**。
  - **隐藏操作系统驱动器恢复选项**：指定是在 BitLocker 界面中显示还是隐藏恢复选项。如果设置为**开**，BitLocker 界面中不会显示任何恢复选项。在这种情况下，请将设备注册到 Active Directory，将恢复选项保存到 Active Directory，并将**将恢复信息保存到 AD DS**设置为**开**。默认为**关**。
  - **将恢复信息保存到 AD DS**：指定是否将恢复选项保存到 Active Directory 域服务。默认为**关**。

  - **配置存储在 AD DS 中的恢复信息：** 指定是将 BitLocker 恢复密码，还是将恢复密码和密钥包存储在 Active Directory 域服务中。存储密钥包支持从物理损坏的驱动器中恢复数据。默认值为“**备份恢复密码**”。
  - **在 AD DS 中存储恢复信息后启用 BitLocker：** 指定是否阻止用户启用 BitLocker，除非设备已连接到域且 BitLocker 恢复信息已成功备份到 Active Directory。如果设置为“**开**”，则设备必须在启动 BitLocker 之前加入域。默认值为“**关**”。

- **自定义预启动恢复消息和 URL：** 指定 BitLocker 是否在恢复屏幕上显示自定义消息和 URL。如果设置为“**开**”，则会出现以下额外设置：“**使用默认恢复消息和 URL**”、“**使用空恢复消息和 URL**”、“**使用自定义恢复消息**”和“**使用自定义恢复 URL**”。如果设置为“**关**”，则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 BitLocker 加密的固定驱动器的恢复选项。BitLocker 不会向用户显示有关固定驱动器加密的消息。要在启动期间解锁驱动器，用户需要提供密码或智能卡。启动的解锁设置（不在此策略中）会在用户在固定驱动器上启用 BitLocker 加密时显示在 BitLocker 界面中。有关相关设置的信息，请参阅此列表前面部分的“**配置操作系统驱动器恢复**”。默认值为“**关**”。
- **阻止对未使用 BitLocker 的固定驱动器进行写入访问：** 如果设置为“**开**”，则用户只能在固定驱动器使用 BitLocker 加密时才能对其进行写入。默认值为“**关**”。
- **阻止对未使用 BitLocker 的可移动驱动器进行写入访问：** 如果设置为“**开**”，则用户只能在可移动驱动器使用 BitLocker 加密时才能对其进行写入。根据您的组织是否允许对其他组织的可移动驱动器进行写入访问来配置此设置。默认值为“**关**”。
- **提示其他磁盘加密：** 允许您禁用设备上其他磁盘加密的警告提示。默认值为“**关**”。

日历 (CalDav) 设备策略

您可以在 XenMobile® 中添加设备策略，以将日历 (CalDAV) 帐户添加到用户的 iOS 或 macOS 设备，从而使他们能够与任何支持 CalDAV 的服务器同步日程数据。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

- **帐户描述：**键入帐户描述。此字段为必填项。
- **主机名：**键入 CalDAV 服务器的地址。此字段为必填项。
- **端口：**键入用于连接到 CalDAV 服务器的端口。此字段为必填项。默认值为 **8443**。
- **主体 URL：**键入用户日历的基本 URL。
- **用户名：**键入用户的登录名。此字段为必填项。

- **密码：**键入可选的用户密码。
- **使用 SSL：选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为开。**
- **策略设置**
  - **删除策略：选择策略删除的计划方法。可用选项包括选择日期和删除前持续时间（小时）**
    - **选择日期：**单击日历以选择要删除的特定日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），表示策略删除前的持续时间。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- **帐户描述：** 键入帐户描述。此字段为必填项。
- **主机名：** 键入 CalDAV 服务器的地址。此字段为必填项。
- **端口：** 键入用于连接 CalDAV 服务器的端口。此字段为必填项。默认值为 **8443**。
- **主体 URL：** 键入用户日历的基本 URL。
- **用户名：** 键入用户的登录名。此字段为必填项。
- **密码：** 键入可选的用户密码。
- **使用 SSL：** 选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为“**开**”。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略删除发生前的持续时间。
  - **允许用户删除策略：** 您可以选择用户何时可以从其设备中删除策略。从菜单中选择“**始终**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于“**用户**”还是整个“**系统**”。默认值为“**用户**”。此选项仅在 macOS 10.7 及更高版本上可用。

蜂窝设备策略

此策略允许您在 iOS 设备上配置蜂窝网络设置。

要添加或配置此策略，请转到“**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：**在下拉列表中单击“质询握手身份验证协议”(**CHAP**) 或“密码身份验证协议”(**PAP**)。默认值为 **PAP**。
  - **用户名**和**密码：**用于身份验证的用户名和密码。
- **APN**
  - **名称：**接入点名称 (APN) 配置的名称。
  - **身份验证类型：**在下拉列表中单击“**CHAP**”或“**PAP**”。默认值为 **PAP**。
  - **用户名**和**密码：**用于身份验证的用户名和密码。
  - **代理服务器：**代理服务器网络地址。
  - **代理服务器端口：**代理服务器端口。
- **策略设置**
  - **移除策略：** 选择一种策略移除的计划方法。可用选项包括**选择日期**和**移除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略移除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。

连接计划设备策略

> **重要提示：**

> Citrix 建议您使用 Firebase 云消息传递 (FCM) 来控制 Android、Android Enterprise 和 Chrome 操作系统设备与 XenMobile Server 的连接。有关使用 FCM 的信息，请参阅 Firebase 云消息传递。

> 如果您选择不使用 FCM，则可以创建连接计划策略来控制用户设备连接到 XenMobile® Server 的方式和时间。

您可以指定用户手动连接其设备，或者设备在定义的时间范围内连接。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅 设备策略。

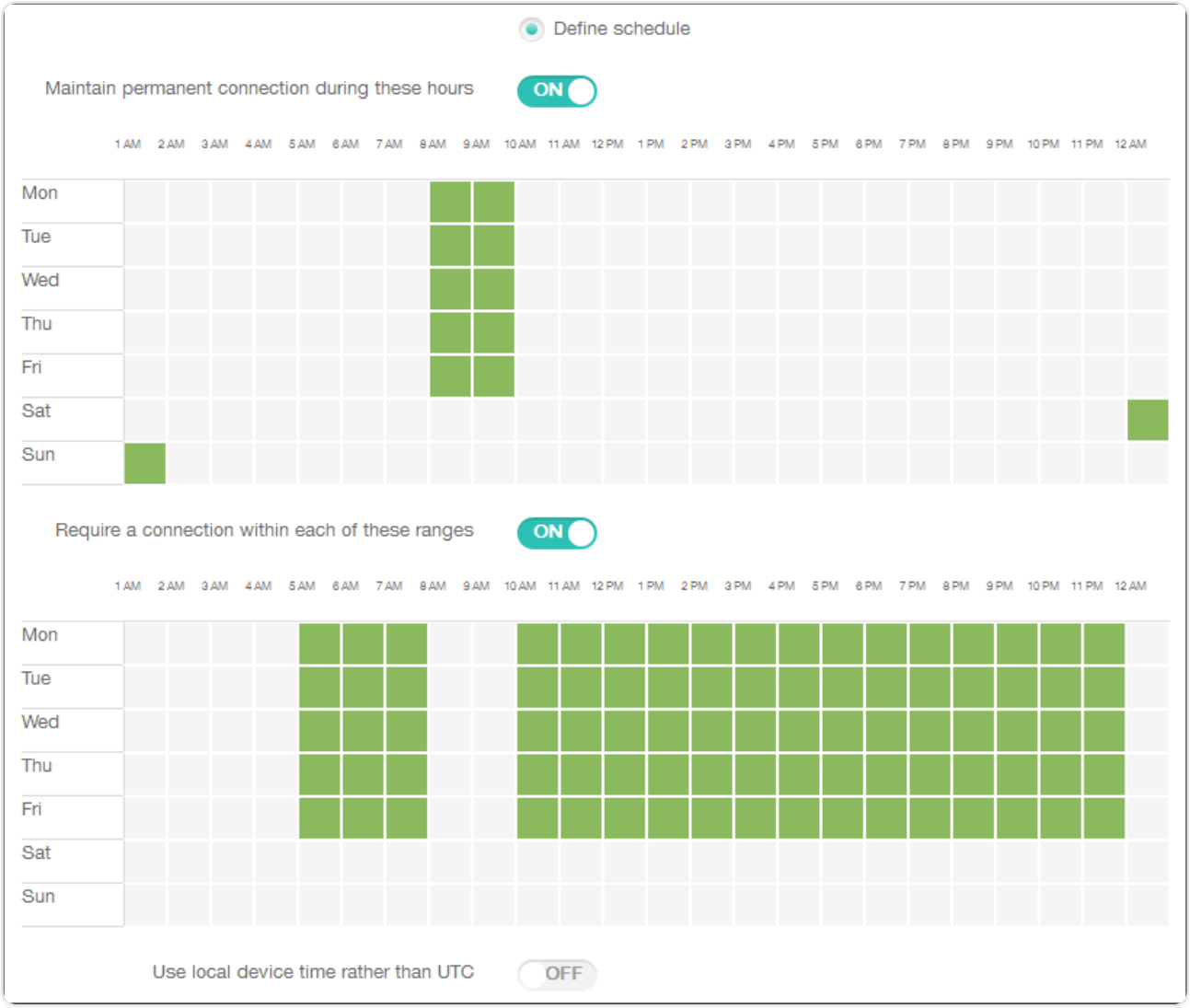
平台设置

- **要求设备连接：**单击要为此计划设置的选项。
  - **始终：永久保持连接。用户设备上的 XenMobile 在网络连接丢失后会尝试重新连接到 XenMobile Server，并通过定期传输控制数据包来监视连接。Citrix® 建议使用此选项以优化安全性。当您选择始终**时，还应为设备**隧道策略**使用**定义连接超时**设置，以确保连接不会耗尽电池电量。通过保持连接活动，您可以按需向设备推送擦除或锁定等安全命令。您还必须在部署到设备的每个策略中选择**部署计划**选项**部署用于始终在线连接**。
  - **从不：**手动连接。用户必须从其设备上的 XenMobile 启动连接。Citrix 不建议将此选项用于生产部署，因为它会阻止您向设备部署安全策略，因此用户永远不会收到任何新应用程序或策略。
  - **每隔：按指定间隔连接。当此选项生效并且您发送锁定或擦除等安全策略时，XenMobile 会在设备下次连接时处理设备上的操作。当您选择此选项时，将显示每 N 分钟连接一次**字段，您必须在其中输入设备必须重新连接的分钟数。默认值为 **20**。
  - **定义计划：**启用后，用户设备上的 XenMobile 在网络连接丢失后会尝试重新连接到 XenMobile Server，并通过在您定义的时间范围内定期传输控制数据包来监视连接。有关如何定义连接时间范围的信息，请参阅下一节“定义连接时间范围”。
    - **在这些时间内保持永久连接：**用户的设备必须在定义的时间范围内保持连接。
    - **在每个这些范围内要求连接：**用户的设备必须在任何定义的时间范围内至少连接一次。
    - **使用本地设备时间而非 UTC：**将定义的时间范围同步到本地设备时间而非协调世界时 (UTC)。

定义连接时间范围

启用以下选项时，将显示一个时间轴，您可以在其中定义所需的时间范围。您可以启用其中一个或两个选项，以在特定时间要求永久连接，或在特定时间范围内要求连接。时间轴中的每个方块代表 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 之间建立连接，则需要单击时间轴上每个工作日上午 8 点到上午 9 点之间的两个方块。

例如，下图中的两个时间轴要求在每个工作日的上午 8:00 到上午 9:00 之间建立永久连接，在星期六上午 12:00 到星期日上午 1:00 之间建立永久连接，以及在每个工作日的上午 5:00 到上午 8:00 之间或上午 10:00 到晚上 11:00 之间至少建立一个连接。



联系人 (CardDAV) 设备策略

您可以在 XenMobile® 中添加设备策略，以将 iOS 联系人 (CardDAV) 帐户添加到用户的 iOS 或 macOS 设备，从而使他们能够与支持 CardDAV 的任何服务器同步联系人数据。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

- **帐户描述：**键入帐户描述。此字段为必填项。
- **主机名：**键入 CardDAV 服务器的地址。此字段为必填项。
- **端口：**键入用于连接到 CardDAV 服务器的端口。此字段为必填项。默认值为 **8443**。
- **主体 URL：**键入用户日历的基本 URL。
- **用户名：**键入用户的登录名。此字段为必填项。
- **密码：**键入可选的用户密码。

- **使用 SSL：选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为开。**
- **策略设置**
  - **删除策略：选择一种计划策略删除的方法。可用选项包括选择日期和删除前持续时间（小时）**
    - **选择日期：**单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），表示策略删除前的时间。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- **帐户描述：** 键入帐户描述。此字段为必填项。
- **主机名：** 键入 CardDAV 服务器的地址。此字段为必填项。
- **端口：** 键入用于连接到 CardDAV 服务器的端口。此字段为必填项。默认值为 **8443**。
- **主体 URL：** 键入用户日历的基本 URL。
- **用户名：** 键入用户的登录名。此字段为必填项。
- **密码：** 键入可选的用户密码。
- **使用 SSL：** 选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为 **开**。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项为“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您可以选择用户何时可以从其设备中删除策略。从菜单中选择“**始终**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于“**用户**”还是整个“**系统**”。默认值为“**用户**”。此选项仅在 macOS 10.7 及更高版本上可用。

控制操作系统更新设备策略

控制操作系统更新设备策略允许您部署：

- 最新的操作系统更新到受监管的 iOS 设备。

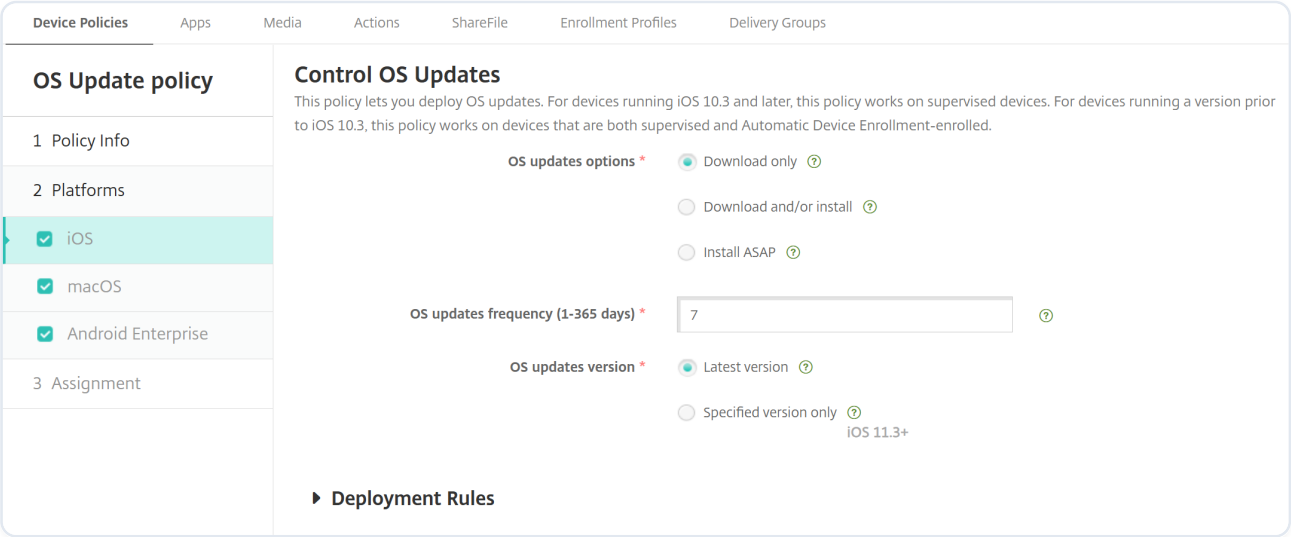
  操作系统更新设备策略仅适用于已注册 Apple 部署计划的受监管设备。

- 最新的操作系统和应用程序更新到运行 macOS 10.11.5 及更高版本的 DEP 注册 macOS 设备。
- 最新的操作系统更新到 Android Enterprise 工作托管设备。

  对于 Android Enterprise 工作托管设备，XenMobile® 会将控制操作系统更新策略发送到 Secure Hub，然后 Secure Hub 会将该策略应用到设备。**管理** > **设备**页面显示 XenMobile Server 何时发送策略以及设备何时接收策略。

要添加或配置此策略，请转到**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置



- **操作系统更新选项：**
  - **仅下载：** 根据操作系统更新频率将最新的操作系统更新下载到受监管设备，而不进行安装。
  - **下载和/或安装：** 根据操作系统更新频率将最新的操作系统更新下载到受监管设备。设备会提示您安装更新。解锁设备后，提示可见。
  - **尽快安装：** 允许您立即安装以前下载的操作系统更新。
- **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。
- **操作系统更新版本：** 指定用于更新受监管 iOS 设备的操作系统版本。默认值为“**最新版本**”。
  - **最新版本：** 选择更新到最新的操作系统版本。
  - **仅限特定版本：** 选择更新到特定操作系统版本，然后键入版本号。此选项适用于 iOS 11.3 或更高版本。

macOS 设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/control-os-update-macos-platform.png)

- **操作系统更新选项：** 这两个选项都根据“**操作系统更新频率**”下载最新的 macOS 更新。您可以选择安装更新，或通过 App Store 通知用户有可用更新。
- **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

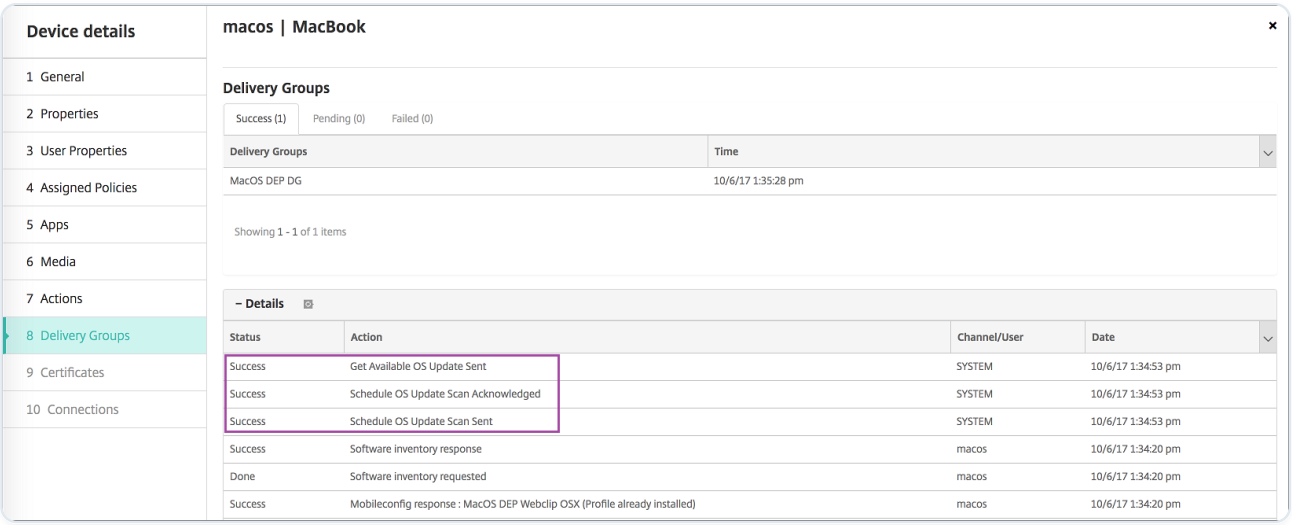
对于 iOS 和 macOS，XenMobile 不会将“控制操作系统更新”策略部署到设备。相反，XenMobile 使用该策略向设备发送以下 MDM 命令：

- 计划操作系统更新扫描：请求设备执行后台操作系统更新扫描。（iOS 可选）
- 可用操作系统更新：查询设备以获取可用操作系统更新列表。
- 计划操作系统更新：请求设备执行 macOS 更新、应用程序更新或两者。因此，设备操作系统决定何时下载或安装操作系统和应用程序更新。

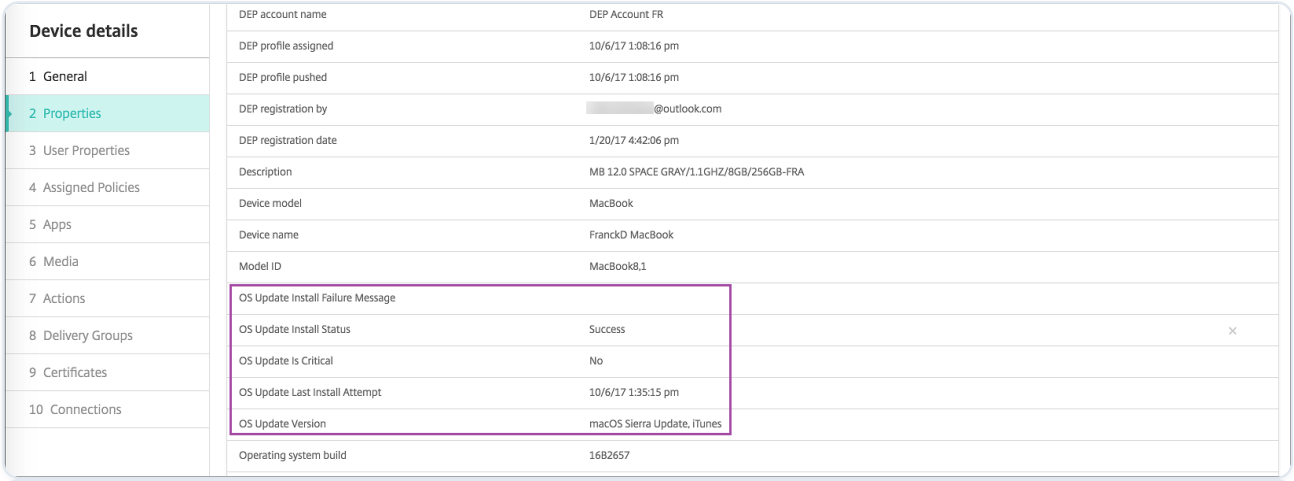
“**管理 > 设备 > 设备详细信息（常规）**”页面显示计划和可用操作系统更新扫描以及计划的 macOS 和应用程序更新的状态。

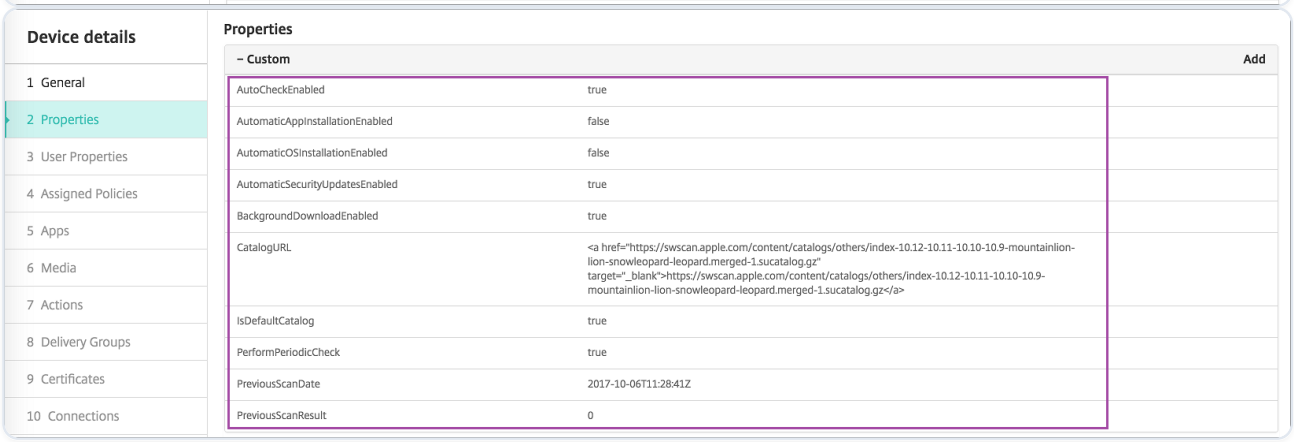
设备详细信息屏幕的图像(/en-us/xenmobile/server/media/control-os-update-general.png)

有关更新操作状态的更多详细信息，请转到“**管理 > 设备 > 设备详细信息（交付组）**”页面。

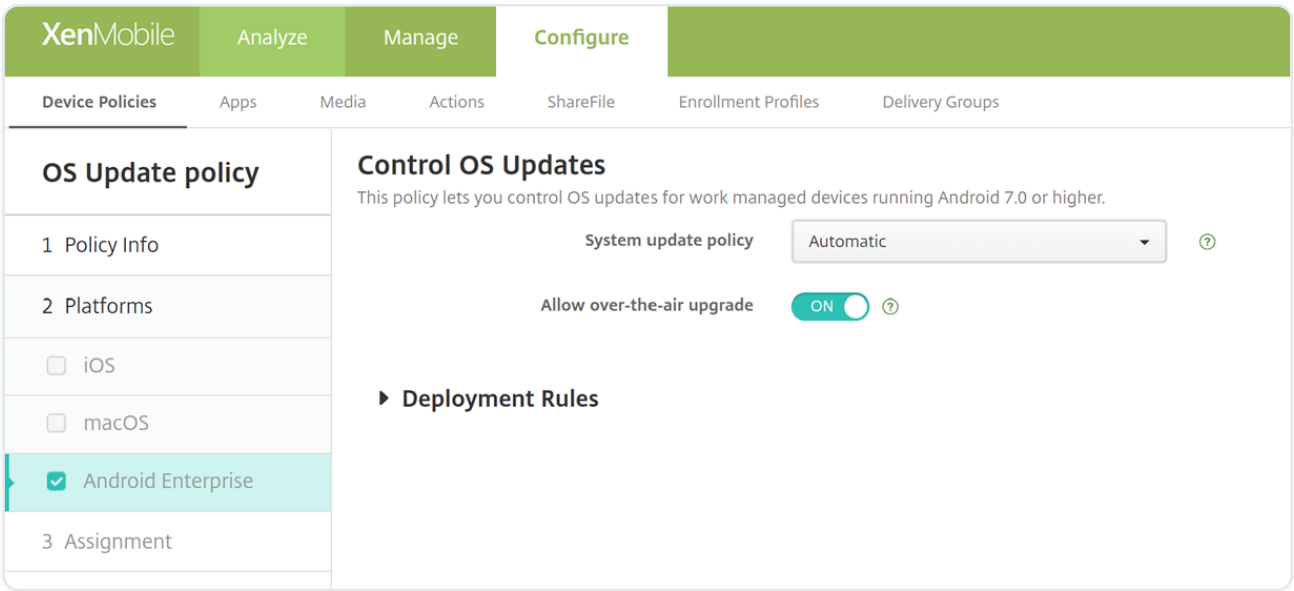


有关可用操作系统更新和上次安装尝试等详细信息，请转到“**管理 > 设备 > 设备详细信息（属性）**”页面。





安卓企业版设置



- **系统更新策略：** 确定系统更新发生的时间。如果启用“**控制企业 FOTA**”设置，则无论此设置的配置如何，更新都会自动发生。
  - **自动：** 在更新可用时安装更新。
  - **窗口化：** 在“**开始时间**”和“**结束时间**”中指定的每日维护窗口内自动安装更新。

  - **开始时间：** 维护窗口的开始时间，以设备本地时间从午夜开始的分钟数（**0 - 1440**）衡量。默认值为 **0**。
  - **结束时间：** 维护窗口的结束时间，以设备本地时间从午夜开始的分钟数（**0 - 1440**）衡量。默认值为 **120**。
- **推迟：** 允许用户将更新推迟最多 30 天。
- **默认：** 将更新策略设置为系统默认值。

- **允许无线升级：** 如果禁用，用户设备将无法无线接收软件更新。默认值为“**开**”。

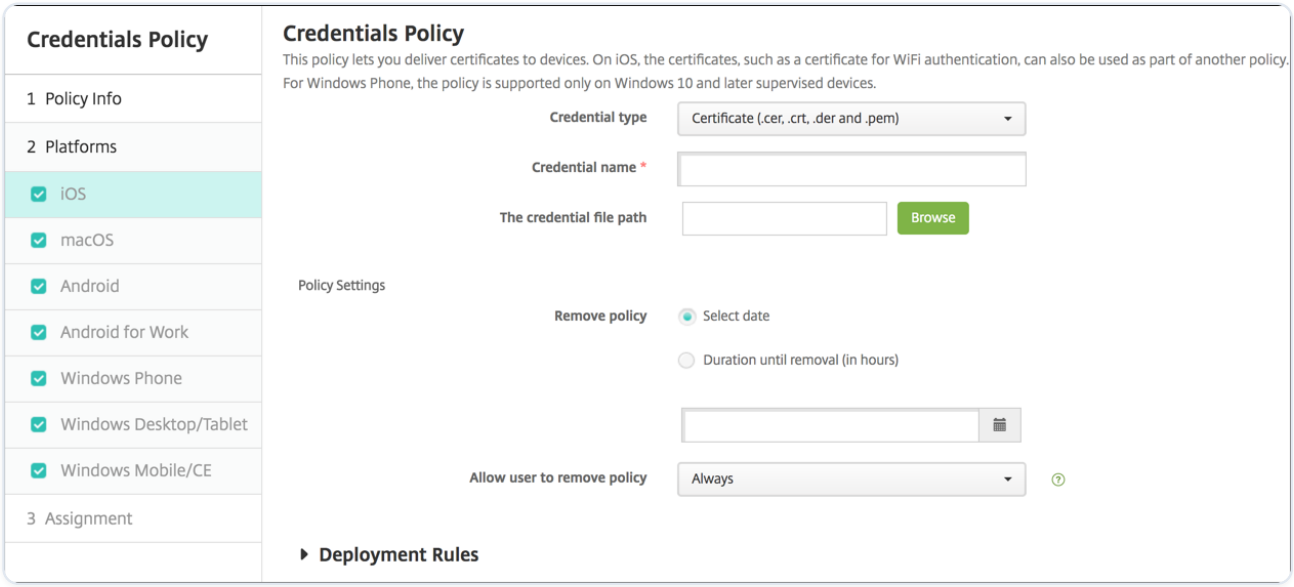
凭据设备策略

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，本文对此进行了介绍。

> **注意：**
>
> 在创建此策略之前，您需要计划用于每个平台的凭据信息，以及任何证书和密码。
>
> 要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

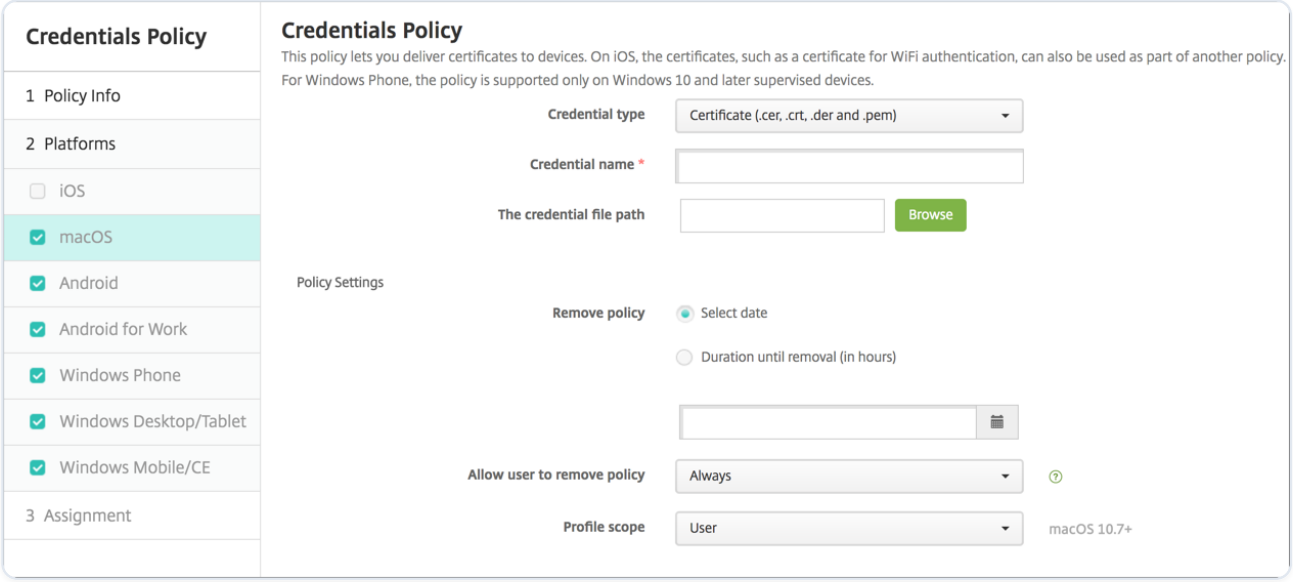
iOS 设置



配置以下设置：

- **凭据类型：** 在下拉列表中单击要与此策略一起使用的凭据类型，然后输入所选凭据的以下信息：
  - **证书**
    - **凭据名称：** 输入凭据的唯一名称。
    - **凭据文件路径：** 通过单击“浏览”并导航到文件位置来选择凭据文件。
  - **密钥库**
    - **凭据名称：** 输入凭据的唯一名称。
    - **凭据文件路径：** 通过单击“浏览”并导航到文件位置来选择凭据文件。
    - **密码：** 输入凭据的密钥库密码。
  - **服务器证书**
    - **服务器证书：** 单击下拉列表中要使用的证书。
  - **凭据提供程序**
    - **凭据提供程序：** 单击下拉列表中的凭据提供程序名称。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

macOS 设置

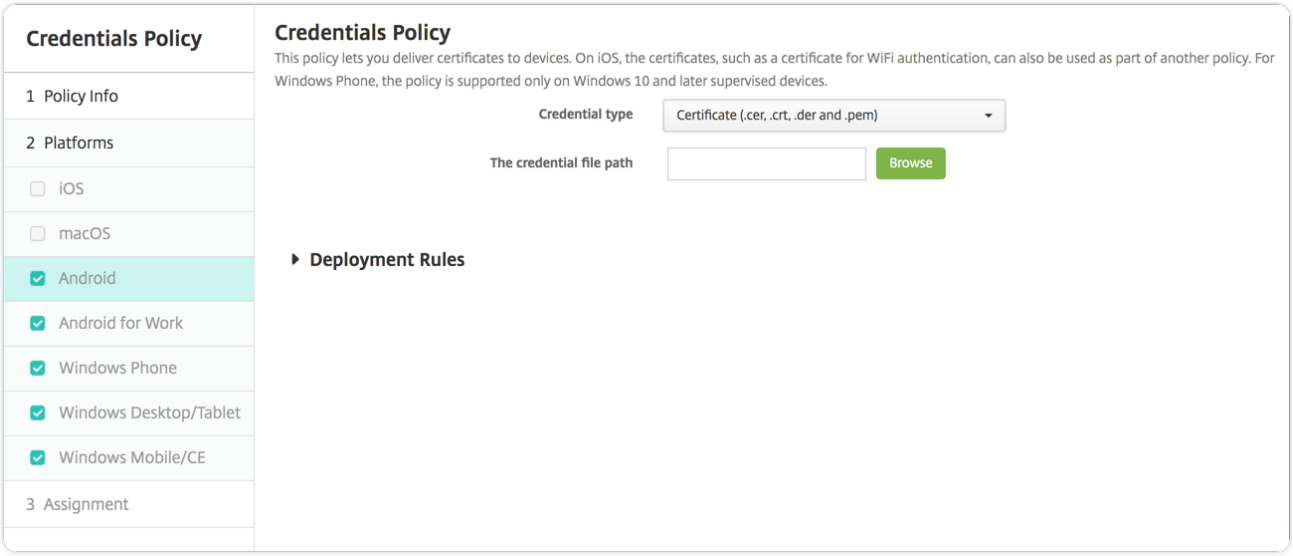


配置以下设置：

- **凭据类型：** 单击下拉列表中要与此策略一起使用的凭据类型，然后输入所选凭据的以下信息：
  - **证书**
    - **凭据名称：**输入凭据的唯一名称。
    - **凭据文件路径：**通过单击“**浏览**”并导航到文件位置来选择凭据文件。
  - **密钥库**
    - **凭据名称：**输入凭据的唯一名称。
    - **凭据文件路径：**通过单击“**浏览**”并导航到文件位置来选择凭据文件。
    - **密码：**输入凭据的密钥库密码。
  - **服务器证书**
    - **服务器证书：**单击下拉列表中要使用的证书。
  - **凭据提供程序**
    - **凭据提供程序：**单击下拉列表中凭据提供程序的名称。
- **策略设置**
  - **删除策略：**选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：**单击日历以选择要删除的具体日期。

    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：**您可以选择用户何时可以从其设备中删除策略。从菜单中选择“**始终**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**用户**。此选项仅适用于 macOS 10.7 及更高版本。

Android 设置

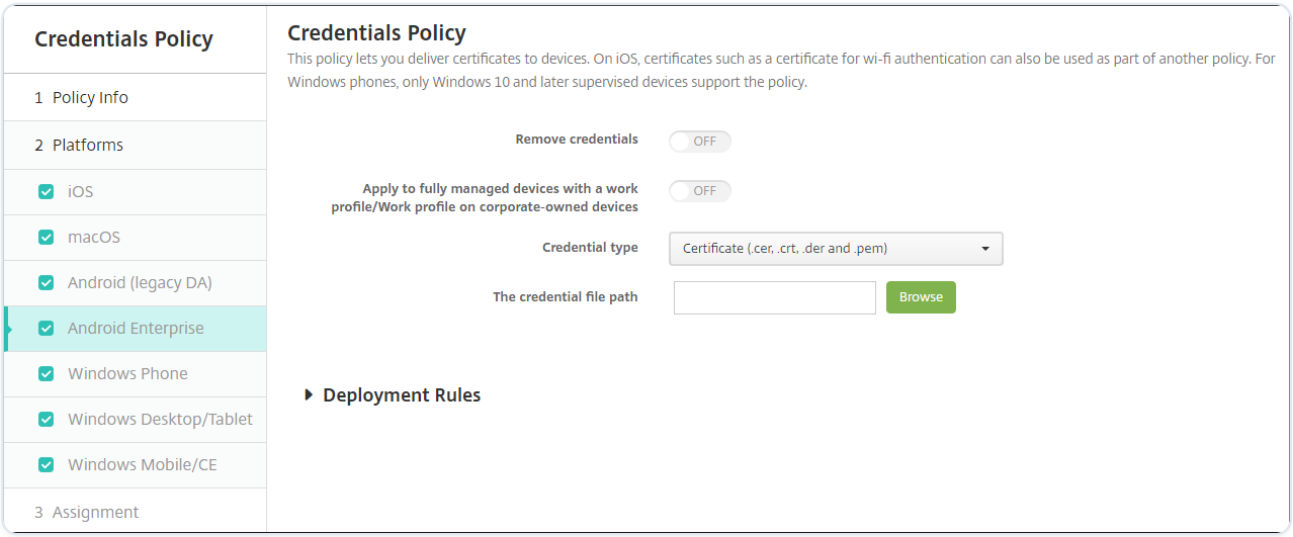


配置以下设置：

- **凭据类型：** 单击下拉列表中的凭据类型，以选择要与此策略一起使用的凭据，然后为所选凭据输入以下信息：
  - **证书**
    - **凭据名称：** 键入凭据的唯一名称。
    - **凭据文件路径：** 通过单击“浏览”选择凭据文件，然后导航到文件位置。
  - **密钥库**
    - **凭据名称：** 键入凭据的唯一名称。
    - **凭据文件路径：** 通过单击“**浏览**”选择凭据文件，然后导航到文件位置。
    - **密码：** 键入凭据的密钥库密码。
  - **服务器证书**
    - **服务器证书：** 单击下拉列表中要使用的证书。
  - **凭据提供程序**

- **凭据提供程序：**在下拉列表中单击凭据提供程序的名称。

安卓企业版设置



配置这些设置以确定 XenMobile® 如何应用凭据设置：

- **移除凭据：设置为开**以配置以下设置。默认值为**关**。
  - **移除用户凭据：从托管密钥库中移除证书。默认值为关。**
  - **移除受信任的根证书：卸载所有非系统 CA 证书。默认值为关。**
- **应用于具有工作资料的完全托管设备/公司拥有的设备上的工作资料：允许您为具有工作资料的完全托管设备配置凭据策略设置。当此设置为开**时，您配置的凭据设置仅应用于工作资料。当此设置为**关**时，您配置的凭据设置仅应用于设备。默认值为**关**。

配置凭据设置：

- **凭据类型：**在下拉列表中单击要与此策略一起使用的凭据类型，然后为所选凭据输入以下信息：
  - **证书**
    - **凭据文件路径：通过单击浏览**选择凭据文件，然后导航到文件位置。
  - **密钥库**
    - **凭据文件路径：通过单击浏览**选择凭据文件，然后导航到文件位置。
    - **证书别名：证书别名使应用程序更容易访问证书。在托管配置设备策略中配置证书别名。然后，在凭据设备策略的证书别名**字段中键入该别名。应用程序将检索证书并验证 VPN，而无需用户执行任何操作。
    - **密码：**键入凭据的密钥库密码。

- **服务器证书**
  - **服务器证书：**单击下拉列表中要使用的证书。
- **凭据提供程序**
  - **证书别名：证书别名使应用程序更容易访问证书。在托管配置设备策略中配置证书别名。然后，在凭据设备策略的证书别名**字段中键入该别名。应用程序将检索证书并验证 VPN，而无需用户执行任何操作。
  - **凭据提供程序：**单击下拉列表中凭据提供程序的名称。
  - **使用证书的应用程序：要指定可静默访问此提供程序凭据的应用程序：单击添加**，选择一个应用程序，然后单击**保存**。

视窗桌面/平板电脑设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/credentials-policy-windesktop.png)

- **证书类型：**在下拉列表中单击 **ROOT** 或 **CLIENT**。
- 如果单击 **ROOT**，请配置以下设置：
  - **存储设备：**在下拉列表中单击 **root**、**My** 或 **CA**，以指定凭据证书存储的位置。**My** 将证书存储在用户的证书存储中。
  - **位置：**对于 Windows 10 和 Windows 11 平板电脑，**系统**是唯一的位置。
  - **凭据类型：**对于 Windows 10 和 Windows 11 平板电脑，**证书**是唯一的凭据类型。
  - **凭据文件路径：通过单击浏览**并导航到文件位置来选择证书文件。
- 如果单击“**客户端**”，请配置以下设置：
- **位置：** 对于 Windows 10 和 Windows 11 平板电脑，**系统**是唯一的位置。
- **凭据类型：** 对于 Windows 10 和 Windows 11 平板电脑，**密钥库**是唯一凭据类型。
- **凭据名称：** 键入凭据的名称。此字段为必填项。
- **凭据文件路径：** 单击“**浏览**”并导航到文件位置，选择证书文件。
- **密码：** 键入与凭据关联的密码。此字段为必填项。

自定义 XML 设备策略

您可以在 XenMobile® 中创建自定义 XML 策略，以在受支持的 Windows 设备上自定义以下功能：

- 预配，包括配置设备以及启用或禁用功能

- 设备配置，包括允许用户更改设置和设备参数
- 软件升级，包括提供要加载到设备上的新软件或错误修复，包括应用程序和系统软件
- 故障管理，包括接收来自设备的错误和状态报告

注意：

创建 XML 内容时，请谨慎使用 \% 字符。\% 字符是 XML 保留字符，仅用于转义 XML 特殊字符。要在名称中使用 \%，请将其编码为 \%25。

对于 Windows 设备：您可以通过使用 Windows 中的开放移动联盟设备管理 (OMA DM) API 来创建自定义 XML 配置。使用 OMA DM API 创建自定义 XML 超出了本主题的范围。有关使用 OMA DM API 的更多信息，请参阅 Microsoft 开发人员网络站点上的 OMA 设备管理。

注意：

对于 Windows 10 RS2 手机：在禁用 Internet Explorer 的自定义 XML 策略或限制策略部署到手机后，浏览器仍保持启用状态。要解决此问题，请重新启动手机。此问题是第三方问题。

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 桌面/平板电脑设置

- **XML 内容：** 键入或剪切并粘贴要添加到策略的自定义 XML 代码。

  单击 **下一步** 后，XenMobile 将检查 XML 内容语法。任何语法错误都会显示在内容框下方。在继续之前，请修复所有错误。

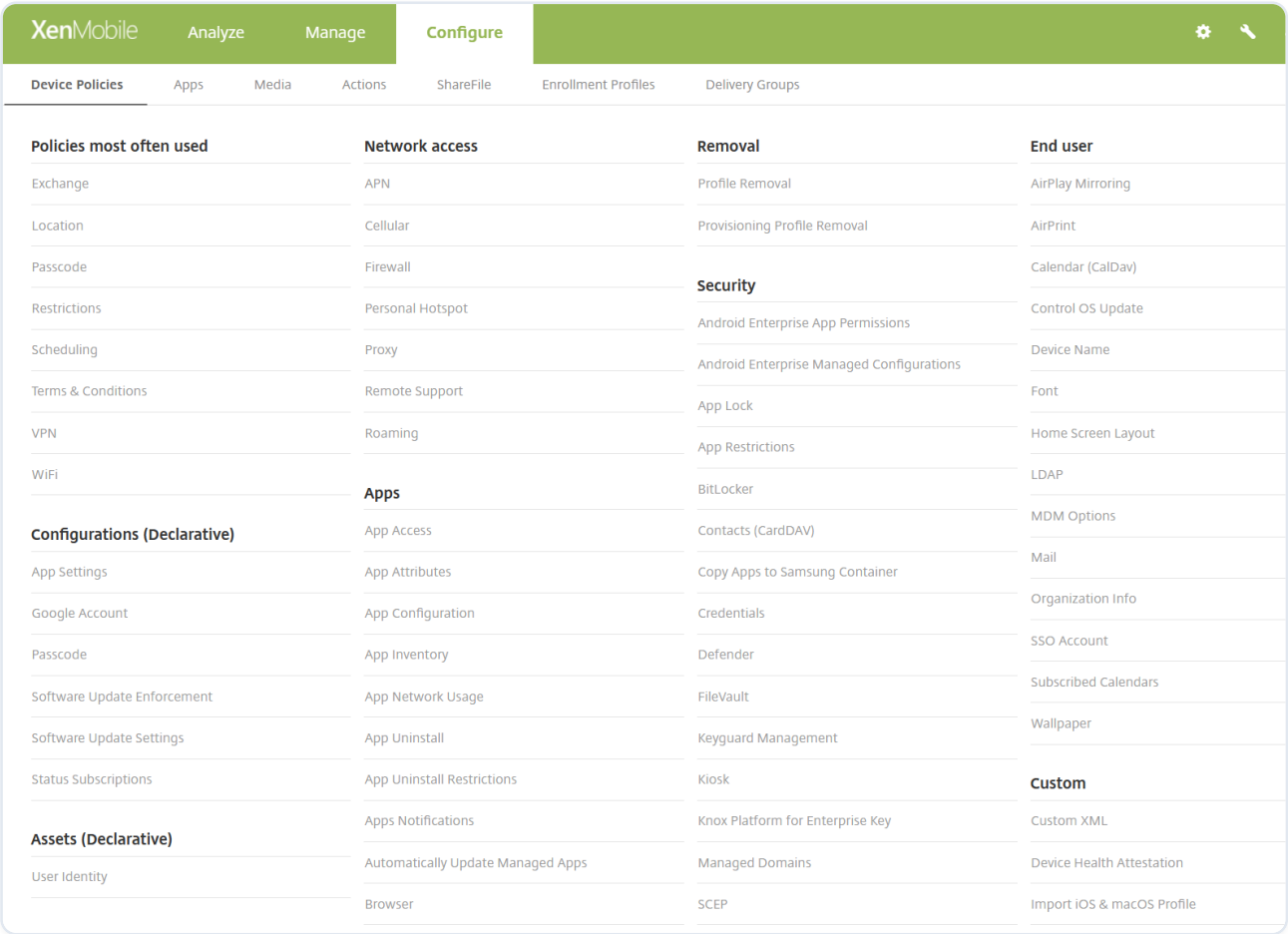
  如果没有语法错误，则会出现**自定义 XML 策略**分配页面。

声明式设备管理策略

Apple 已在 iOS 15 中宣布推出声明式设备管理 (DDM)，采用声明式数据模型范例。此范例允许服务器避免通常与通过 MDM 序列化命令和轮询设备相关的常见性能和可伸缩性问题。有关详细信息，请参阅利用声明式管理数据模型扩展设备。

启用 DDM 功能后，支持以下声明式设备策略：

- 应用程序设置
- Google 帐户
- 密码
- 软件更新强制执行
- 软件更新设置
- 状态订阅
- 用户身份



应用设置设备策略

应用设置设备策略允许您使用 Apple 的声明式设备管理配置应用程序允许和拒绝列表。它取代了已弃用的 `allowListedAppBundleIDs` 和 `blockedAppBundleIDs` 限制密钥。此策略仅支持受监管的设备。

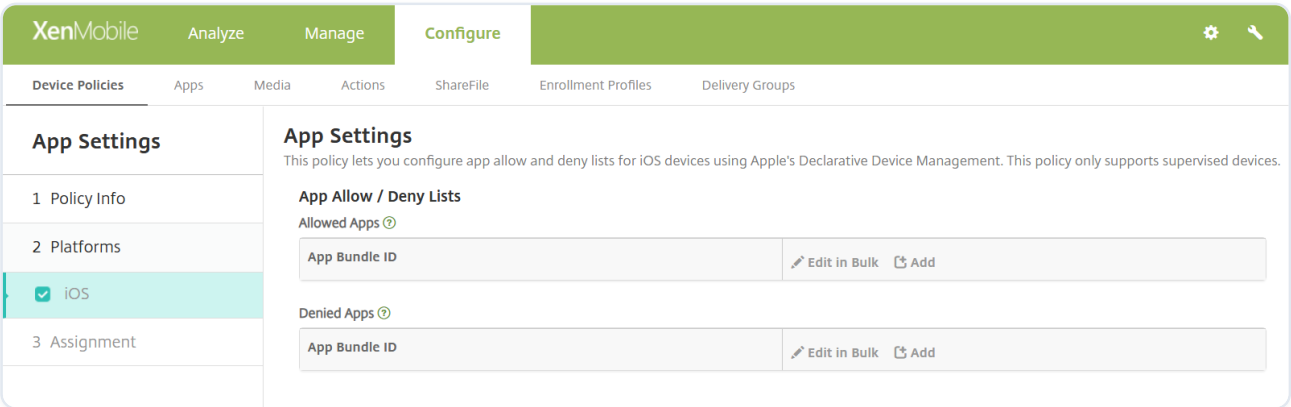
要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- XenMobile Server 10.16 滚动修补程序 9 或更高版本。

- 服务器属性 `ios.mdm.ios27.ddm.support` 设置为 **True**。
- 适用于 iOS 27 或更高版本以及 iPadOS 27 或更高版本。仅支持受监管的设备。

iOS 设置



- **应用程序允许/拒绝列表：**
  - **允许的应用程序：** 如果存在，设备将仅显示或启动列表中包含捆绑 ID 的应用程序。包含值 `com.apple.webapp` 以允许所有 Web 剪辑。这适用于 App Store 应用程序、市场应用程序和本地安装的应用程序（使用 Configurator、Xcode 等）。
    - **应用程序捆绑 ID：** 要添加应用程序捆绑 ID，请单击 **添加**，键入应用程序捆绑 ID，然后单击 **保存**。对要添加的每个应用程序捆绑 ID 重复此过程。您还可以单击 **批量编辑**，输入或粘贴应用程序捆绑 ID（每行一个或用逗号分隔），然后单击 **保存**。
  - **拒绝的应用程序：** 如果存在，设备将阻止显示或启动列表中包含捆绑 ID 的应用程序。包含值 `com.apple.webapp` 以限制所有 Web 剪辑。这适用于 App Store 应用程序、市场应用程序和本地安装的应用程序（使用 Configurator、Xcode 等）。

> **注意：**
>
> - 拒绝系统应用程序可能会禁用其他功能。例如，拒绝 App Store 应用程序可能会阻止用户接受基于用户的批量采购计划 (VPP) 的条款和条件。
> - 我们建议您配置应用允许列表或应用拒绝列表，但不要同时配置两者。

Google 帐户设备策略

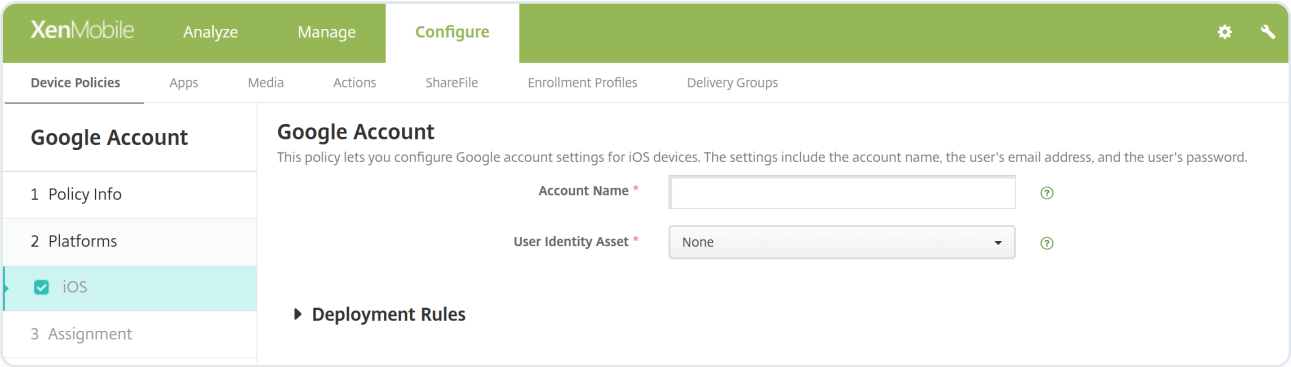
Google 帐户设备策略允许您配置适用于 iOS 设备的 Google 帐户设置。这些设置包括帐户名称和用户身份资产，用于配置电子邮件地址和用户的全名。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- XenMobile Server 10.16 滚动修补程序 8 或更高版本。
- 服务器属性 `ios.mdm.declarative.management` 设置为 **True**。
- 用户身份策略已配置。请参阅 用户身份设备策略。

iOS 设置



- **帐户名称：** 键入 Google 帐户的名称。
- **用户身份资产：** 在列表中，选择由用户身份策略创建的用户身份资产，其中包含用户的电子邮件地址和全名。默认值为 **无**。

密码设备策略

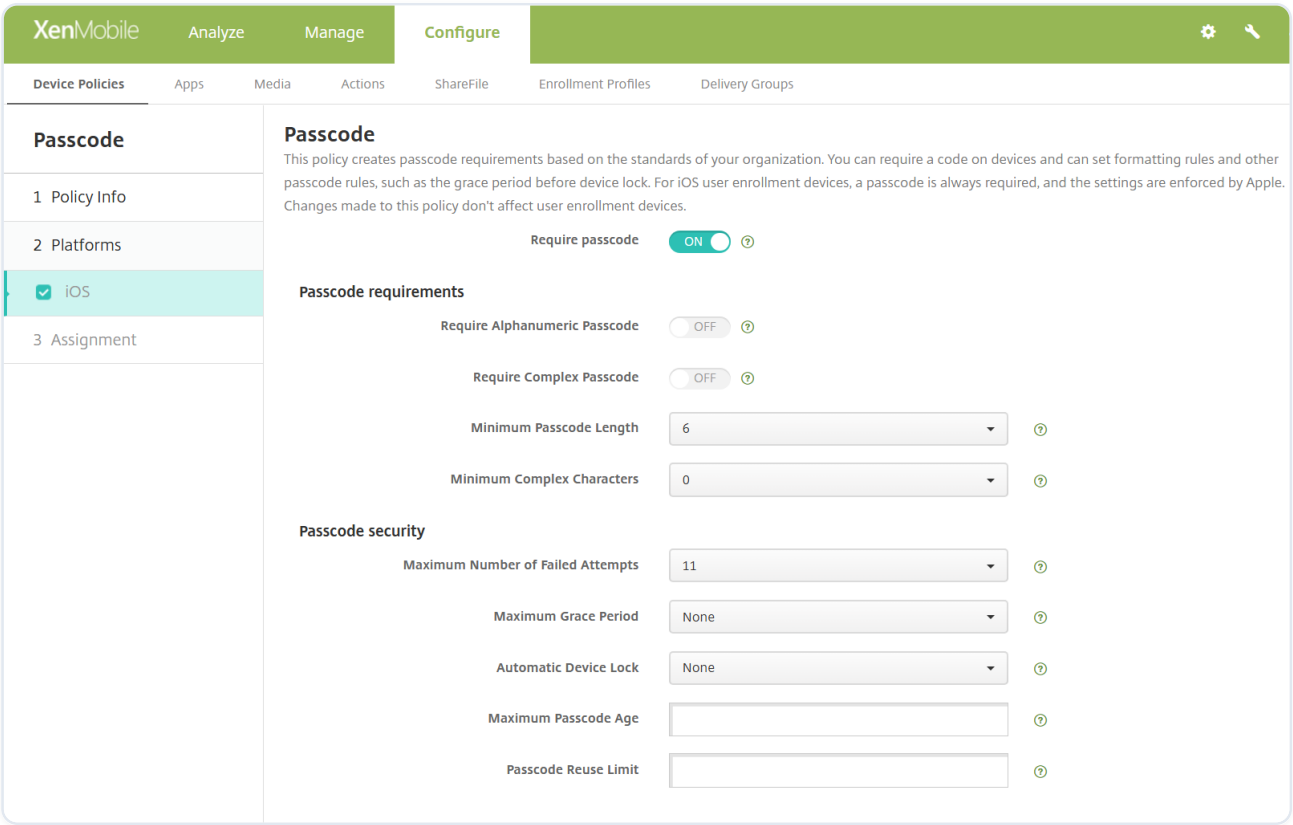
密码设备策略根据您组织的标准创建密码要求。您可以要求设备上使用密码，并可以设置格式规则和其他密码规则，例如设备锁定前的宽限期。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅 设备策略。

先决条件

- XenMobile Server 10.16 Rolling Patch 8 或更高版本。
- 服务器属性 `ios.mdm.declarative.management` 设置为 **True**。

iOS 设置



- **要求密码：** 选择此选项可要求使用密码并显示 iOS 密码设备策略的配置选项。如果设置为**开**，则要求用户设置密码，而对密码的长度或质量没有任何要求，并且页面会展开，允许您配置密码要求和密码安全设置。默认值为**开**。
- **密码要求**
  - **要求字母数字密码：** 选择是否要求密码至少包含一个字母字符和一个数字。默认值为**关**。
  - **要求复杂密码：** 选择是否要求使用复杂密码。复杂密码是指不包含重复字符或递增或递减字符（例如 123 或 CBA），并且必须至少包含一个非数字和非字母字符的密码。默认值为**关**。
  - **最小密码长度：** 选择密码可包含的最小字符数。默认值为**6**。
  - **最小复杂字符数：** 选择密码中复杂字符的最小数量。复杂字符是指除数字或字母以外的字符，例如 &、%、$ 和 #。默认值为**0**。
- **密码安全**
  - **最大失败尝试次数：** 选择系统允许用户在 iOS 擦除设备之前失败的密码尝试次数。如果您不更改此设置，在六次失败尝试后，设备会强制延迟一段时间，然后用户才能再次输入密码。每次失败尝试都会增加时间延迟。在最后一次失败尝试后，系统会安全地擦除 iOS 设备上的所有数据和设置。密码时间延迟从第六次尝试后开始，因此如果此值为六或更低，系统将没有时间延迟，并在用户超出限制后立即触发擦除或锁定。默认值为 **11**。

- **最长宽限期：** 选择用户无需密码即可解锁设备的最长时期。选择**立即**表示没有宽限期，设备会立即要求输入密码。默认值为**无**，这意味着用户可以选择任何时期。
- **自动设备锁定：** 选择设备在系统自动锁定之前可以闲置的最长时期。当设备达到此限制时，设备会锁定，用户必须输入密码才能解锁。默认值为**无**，这意味着用户可以选择任何时期。
- **最长密码有效期：** 选择密码可以保持不变的最长天数。在此天数之后，系统会强制用户在解锁设备之前更改密码。有效值为 0–730。值为 **0** 会强制立即更改密码。默认值为空，表示没有密码有效期限制。
- **密码重用限制：** 选择系统在验证新密码时检查的历史密码条目数。如果新密码与指定密码历史范围内的先前使用过的密码匹配，设备将拒绝该新密码。有效值为 1–50。默认值为空，表示系统不执行历史检查。

注意：

如果将相同的设置作为 MDM 配置文件和声明性配置发送到设备，则适用与通过多个配置文件传递设置相同的规则。例如，如果密码策略通过配置文件（通过密码策略）和配置（通过声明性密码策略）进行配置，则这些策略将合并，并强制执行最严格的设置。

软件更新强制执行设备策略

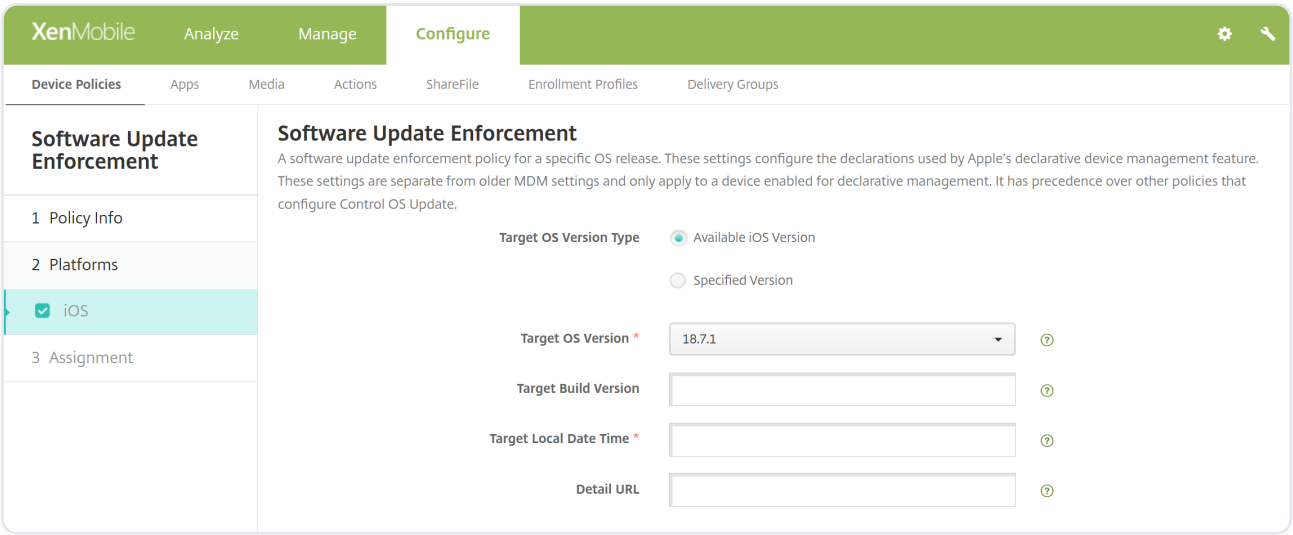
针对特定操作系统版本的软件更新强制执行设备策略使 IT 管理员能够管理 iOS 设备更新，允许他们控制应用哪些更新并设置完成所有更新的截止日期。这些设置配置了 Apple 声明式设备管理功能所使用的声明。这些设置与旧的 MDM 设置是分开的，并且仅适用于已启用声明式管理的设备。对于相同的设置，它优先于“控制操作系统更新”策略。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- XenMobile Server 10.16 滚动修补程序 8 或更高版本。
- 服务器属性 `ios.mdm.declarative.management` 设置为 **True**。
- 适用于 **iOS 17.0** 或更高版本以及 **iPadOS 17.0** 或更高版本。

iOS 设置



- **目标操作系统版本类型：** 指定如何配置目标操作系统版本。默认值为 **可用 iOS 版本**。
  - **可用 iOS 版本：** 如果为 **开**，请在 **目标操作系统版本** 中列出可用的目标操作系统版本。
  - **指定版本：** 如果为 **开**，请手动输入建议格式的操作系统版本。
- **目标操作系统版本：（必需）** 选择或键入要在适当时间将设备更新到的目标操作系统版本。这是操作系统版本号，例如 17.7。它还可以包含补充版本标识符，例如 17.7.2。
- **目标内部版本号：** 键入要在适当时间将设备更新到的目标内部版本号，例如 20A242。系统在种子测试期间使用内部版本号进行测试。内部版本号可以包含补充版本标识符，例如 20A242a。如果内部版本号与 TargetOSVersion 键中指定的目标操作系统版本不一致，则目标操作系统版本优先。
- **目标本地日期时间：（必需）** 键入本地日期时间值，指定何时强制安装软件更新。使用格式 yyyy-mm-ddThh:mm:ss，该格式源自 RFC3339，但不包含时区偏移。如果用户在此时间之前未触发软件更新，设备将强制安装它。
- **详细信息 URL：** 键入一个网页的 URL，该网页显示组织提供的有关强制更新的详细信息。

注意：

软件更新强制策略和控制操作系统更新策略都可以管理设备上的操作系统更新。但是，软件更新强制策略优先于控制操作系统更新策略。如果两个策略都以相同的设置部署，则控制操作系统更新策略中的配置将被覆盖且不会生效。有关详细信息，请参阅过渡到声明式设备管理。

此外，软件更新强制策略和控制操作系统更新策略之间存在一些差异。

策略类型	软件更新强制	控制操作系统更新
设备类型	受监督或不受监督的设备	受监督的设备
强制更新截止日期	✓	✗
输入帮助 URL	✓	✗
指定内部版本号	✓	✗
自动部署最新更新	✗	✓
最低支持版本	iOS 17.0	iOS 10.3 (受监管)

软件更新设置设备策略

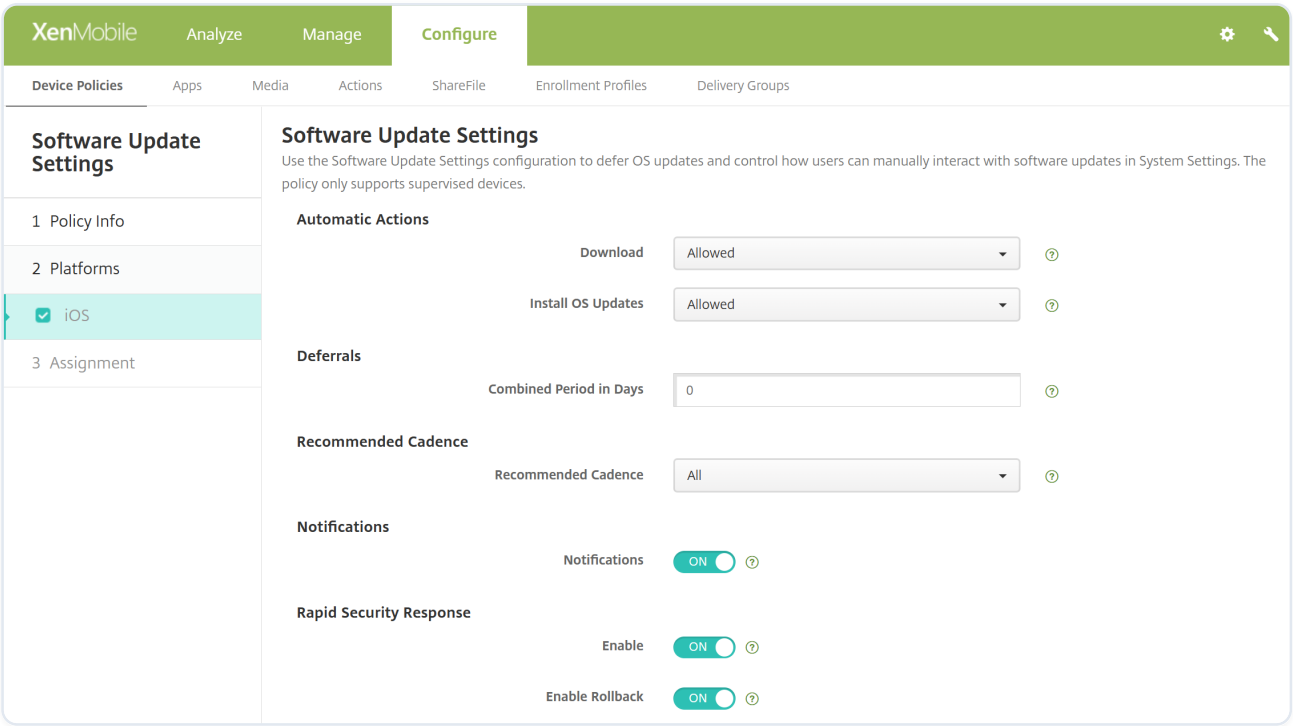
软件更新设置设备策略可用于推迟操作系统更新，并控制用户如何在“系统设置”中手动与软件更新交互。此策略仅支持受监督的设备。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- XenMobile Server 10.16 滚动修补程序 8 或更高版本。
- 服务器属性 `ios.mdm.declarative.management` 和 `ios.mdm.software.update.settings` 设置为 **True**。
- 适用于 **iOS 18.0** 或更高版本以及 **iPadOS 18.0** 或更高版本，仅支持受监督的设备。

iOS 设置



- **自动操作**
  - **下载：** 指定用户是否可以控制可用更新的自动下载。默认值为 **允许**。
    - **允许** - 用户可以启用或禁用自动下载。
    - **始终开启** - 自动下载始终启用。
    - **始终关闭** - 自动下载始终禁用。
  - **安装操作系统更新：** 指定用户是否可以控制可用更新的自动安装。默认值为 **允许**。
    - **允许** - 用户可以启用或禁用自动安装。
    - **始终开启** - 自动安装始终启用。
    - **始终关闭** - 自动安装始终禁用。
- **延迟**
  - **合并延迟天数：** 指定在设备上延迟主要或次要操作系统软件更新的天数。设置后，软件更新只会在软件更新发布后经过指定延迟时间才会显示。适用于 iOS 18 及更高版本。有效值为 0–90。默认值为 **0**，表示不延迟。
- **推荐节奏**
  - **推荐节奏：** 指定设备如何向用户显示软件更新。当有多个更新可用时，设备行为如下。默认值为 **所有**。

  - **所有** - 显示所有软件更新版本。
  - **最旧** - 仅显示最旧（编号最小）的软件更新版本。
  - **最新** - 仅显示最新（编号最大）的软件更新版本。

- **通知**
  - **通知：** 如果设置为“**开**”，设备将显示所有软件更新强制通知。如果设置为“**关**”，设备将仅显示在强制执行截止日期前一小时触发的通知以及重新启动倒计时通知。默认值为“**开**”。

- **快速安全响应**
  - **启用：** 如果设置为“**关**”，则不向用户提供快速安全响应以供安装。系统仍可通过 `com.apple.configuration.softwareupdate.enforcement.specific` 配置安装快速安全响应。如果设置为“**开**”，系统会向用户提供快速安全响应。默认值为“**开**”。
  - **启用回滚：** 如果设置为“**关**”，系统不会向用户提供快速安全响应回滚。如果设置为“**开**”，系统会向用户提供快速安全响应回滚。默认值为“**开**”。

状态订阅设备策略

状态订阅设备策略允许您为设备配置状态订阅，包括操作系统版本/内部版本、电池健康状况、软件更新状态等属性。

要添加或配置此策略，请转到**配置 > 设备策略**。有关详细信息，请参阅 设备策略。

先决条件

- XenMobile Server 10.16 滚动修补程序 8 或更高版本。
- 服务器属性 `ios.mdm.declarative.management` 设置为 **True**。

iOS 设置

](/en-us/xenmobile/server/media/status-subscriptions-ios-settings1.png)

- **设备属性**
  - **系统版本：** 如果为 **开**，设备将报告操作系统的版本（例如 18.0），该版本将显示在设备属性的“系统信息”部分。这很有用，因为当版本升级时，设备会自动报告。默认值为 **开**。适用于 iOS 15 及更高版本。
  - **系统内部版本：** 如果为 **开**，设备将报告操作系统的内部版本（例如 18F132），该版本将显示在设备属性的“系统信息”部分。这很有用，因为当版本升级时，设备会自动报告。默认值为 **开**。适用于 iOS 15 及更高版本。

- **电池健康状况：** 如果为 **开**，则会在设备属性中添加一个新设置 **电池健康状况**。此设置允许管理员通过导航到**管理 > 设备 > 属性 > 电池 > 电池健康状况**来查看已注册 iOS 设备的电池健康状况。默认值为 **开**。适用于 iOS 17 及更高版本。

- **软件更新**
  - **失败原因：** 如果为 **开**，设备将报告操作系统更新失败的原因，该原因将显示在设备属性的“软件更新信息”部分。默认值为 **关**。适用于 iOS 17 及更高版本。

用户身份设备策略

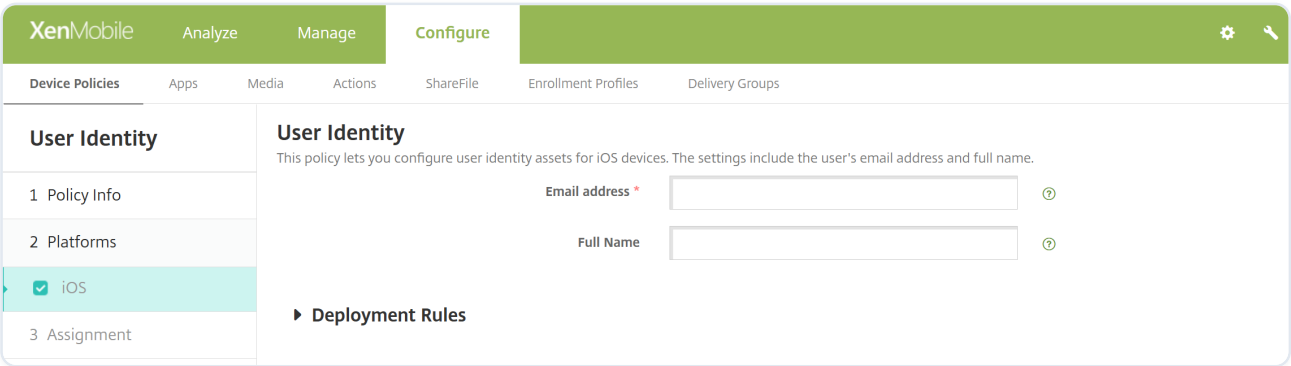
用户身份设备策略允许您为 iOS 设备配置用户身份资产。设置包括用户的电子邮件地址和全名。

要添加或配置此策略，请转至 **Configure > Device Policies**（配置 > 设备策略）。有关详细信息，请参阅 设备策略。

必备条件

- XenMobile Server 10.16 滚动修补程序 8 或更高版本。
- 服务器属性 `ios.mdm.declarative.management` 设置为 **True**。

iOS 设置



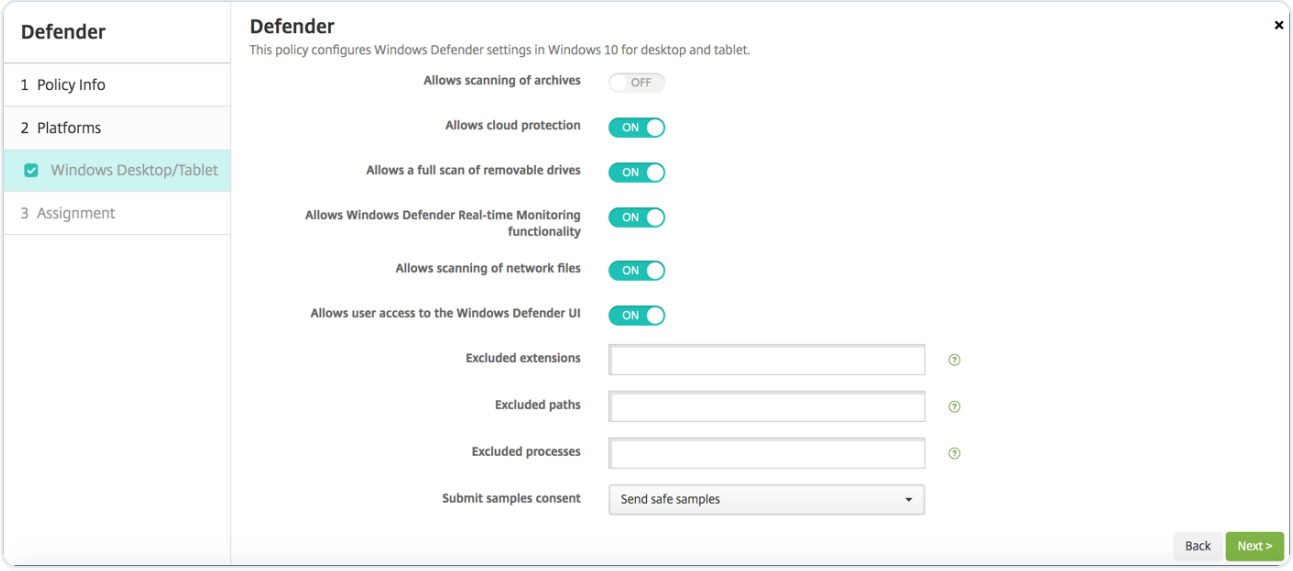
- **电子邮件地址：** 键入用户的电子邮件地址。此字段为必填项。
- **全名：** 键入用户的全名。

Defender 设备策略

Windows Defender 是 Windows 10 和 Windows 11 中包含的恶意软件防护功能。您可以使用 XenMobile® 设备策略 Defender 来配置适用于 Windows 10 和 Windows 11 桌面版和平板电脑版的 Microsoft Defender 策略。

要添加或配置此策略，请转至“**配置 > 设备策略**”。有关详细信息，请参阅设备策略。

Windows 桌面版和平板电脑设置



- **允许扫描存档：** 允许或禁止 Defender 扫描存档文件。默认为“**关**”。
- **允许云保护：** 允许或禁止 Defender 向 Microsoft 发送有关恶意软件活动的信息。默认为“**开**”。
- **允许对可移动驱动器进行完全扫描：** 允许或禁止 Defender 扫描可移动驱动器，例如 USB 闪存盘。默认为“**开**”。
- **允许 Windows Defender 实时监控功能：** 默认为“**开**”。
- **允许扫描网络文件：** 允许或禁止 Defender 扫描网络文件。默认为“**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。此设置在用户设备下次启动时生效。如果此设置为“**关**”，则用户不会收到任何 Windows Defender 通知。默认为“**开**”。
- **排除的扩展名：** 要从实时或计划扫描中排除的扩展名。要分隔扩展名，请使用“**\|**”字符。例如，“lib\|obj”。
- **排除的路径：** 要从实时或计划扫描中排除的路径。要分隔路径，请使用“**\|**”字符。例如，“C:\\Example\|C:\\Example1”。
- **排除的进程：** 要从实时或计划扫描中排除的进程。要分隔进程，请使用“**\|**”字符。例如，“C:\\Example.exe\|C:\\Example1.exe”。
- **提交样本同意：** 控制是否将可能需要进一步分析以确定其是否恶意的文件发送给 Microsoft。选项包括：“**始终提示**”、“**发送安全样本**”、“**从不发送**”、“**发送所有样本**”。默认为“**发送安全样本**”。

设备健康证明设备策略

在 XenMobile® 中，您可以要求 Windows 10 和 Windows 11 设备报告其健康状况，方法是让这些设备将特定数据和运行时信息发送到健康证明服务 (HAS) 进行分析。HAS 会创建并返回一个健康证

明证书，然后设备会将其发送到 XenMobile。当 XenMobile 收到健康证明证书时，它会根据健康证明证书的内容，部署您之前设置的自动操作。

HAS 验证的数据包括：

- AIK 存在
- BitLocker 状态
- 启动调试已启用
- 启动管理器修订列表版本
- 代码完整性已启用
- 代码完整性修订列表版本
- Apple 部署计划策略
- ELAM 驱动程序已加载
- 颁发时间
- 内核调试已启用
- PCR
- 重置计数
- 重启计数
- 安全模式已启用
- SBCP 哈希
- 安全启动已启用
- 测试签名已启用
- VSM 已启用
- WinPE 已启用

有关详细信息，请参阅 Microsoft 设备运行状况证明 CSP 页面。

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 Cloud 配置 DHA

添加设备运行状况证明策略，并为所选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 **关闭**。

使用本地 Windows DHA 服务器配置 DHA

要在本地启用 DHA，您首先需要配置 DHA 服务器。然后，创建 XenMobile Server 策略以启用本地 DHA 服务。

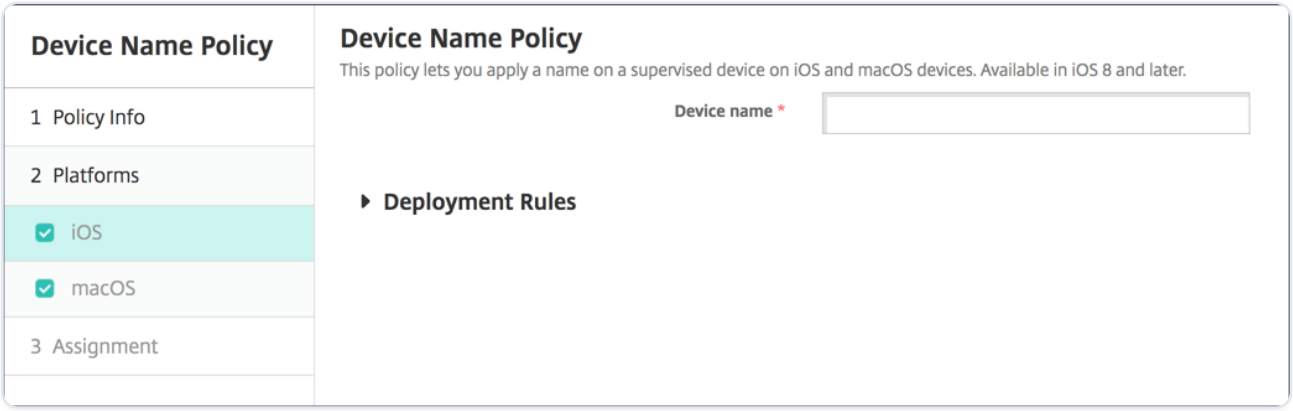
1. 要配置 DHA 服务器，请在运行 Windows Server 2016 Technical Preview 5 或更高版本的计算机上安装 DHA 服务器角色。有关说明，请参阅 配置本地设备运行状况证明服务器。
2. 添加设备健康证明策略并配置以下设置：
   - **启用设备健康证明：** 设置为 **开**。
   - **配置本地健康证明服务：** 设置为 **开**。
   - **本地 DHA 服务 FQDN：** 键入您设置的 DHA 服务器的完全限定域名。
   - **本地 DHA API 版本：** 选择安装在 DHA 服务器上的 DHA 服务的版本。

设备名称设备策略

您可以在受监管的 iOS 和 macOS 设备上设置名称，以便轻松识别这些设备。您可以使用宏、文本或两者的组合来定义设备名称。例如，要将设备名称设置为设备的序列号，您必须使用 ${device.serialnumber}。要将设备名称设置为用户名和域的组合，您必须使用 ${user.username}@example.com。有关宏的更多信息，请参阅 XenMobile 中的宏。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅 设备策略。

iOS 和 macOS 设置



- **设备名称：** 键入宏、宏组合或宏与文本的组合，以唯一命名每个设备。例如，使用 ${device.serialnumber} 将设备名称设置为每个设备的序列号，或者使用 ${device.serialnumber} ${ user.username } 在设备名称中包含用户名。

教育配置设备策略

教育配置设备策略定义了：

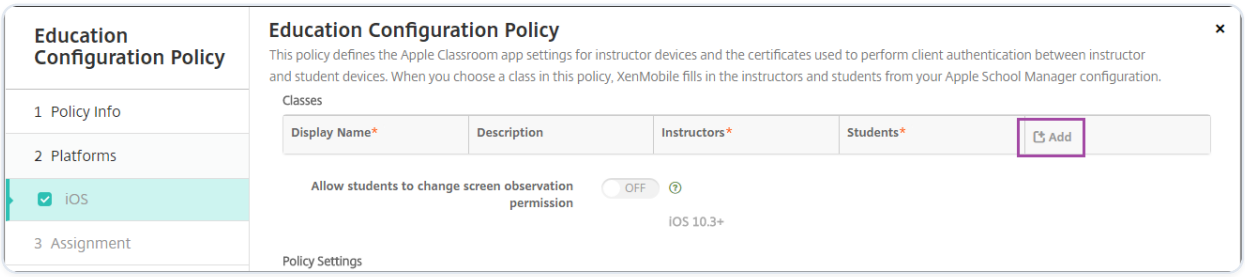
- 教师设备的 Apple Classroom 应用设置。
- 用于在教师设备和学生设备之间执行客户端身份验证的证书。

当您在此策略中选择一个班级时，XenMobile® 控制台会从您的 Apple School Manager 配置中填充教师和学生信息。如果此策略中的 Apple Classroom 应用设置对所有班级都相同，则创建一个策略。

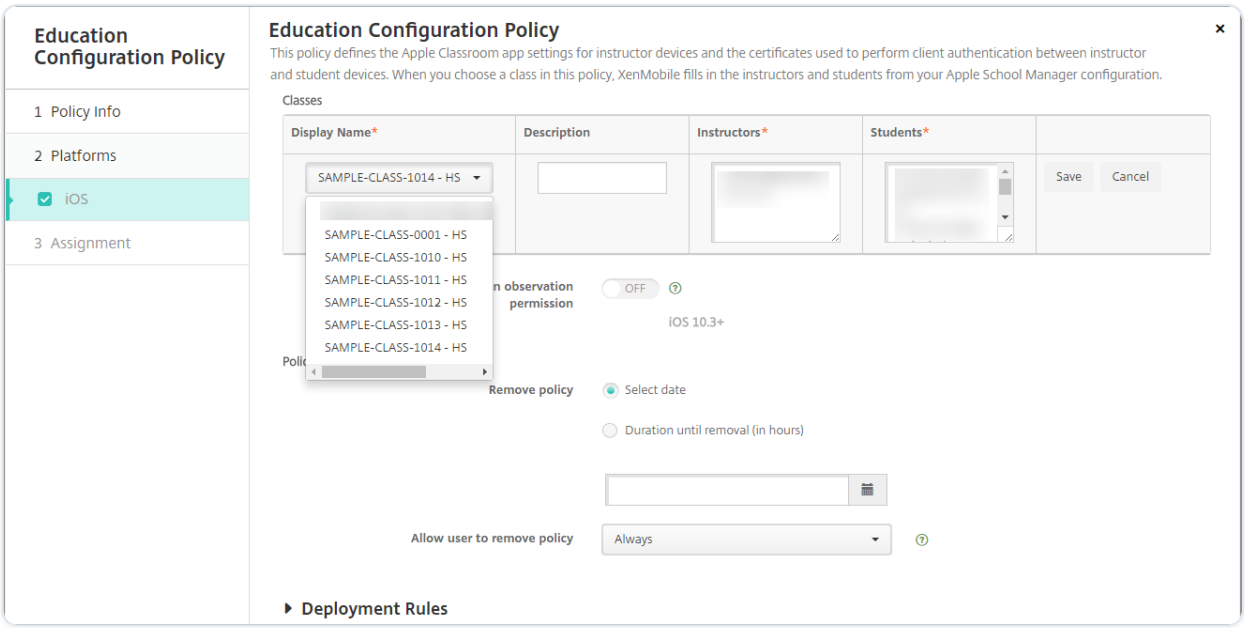
要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅设备策略。

iOS 设置

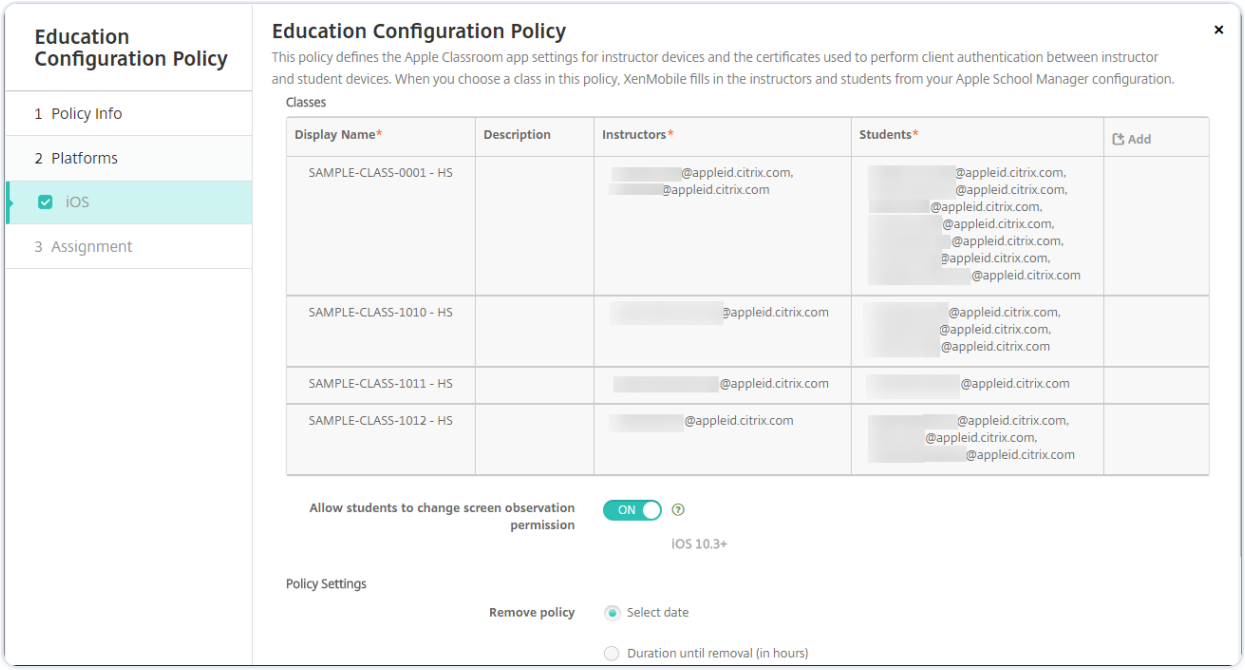
- **班级：** 要添加班级，请单击 **Add**。



然后，单击 **Display Name** 列表。将显示从您连接的 Apple School Manager 帐户获取的班级列表。



当您从 **Display Name** 中选择一个班级时，XenMobile 会填充教师和学生信息。继续添加班级。

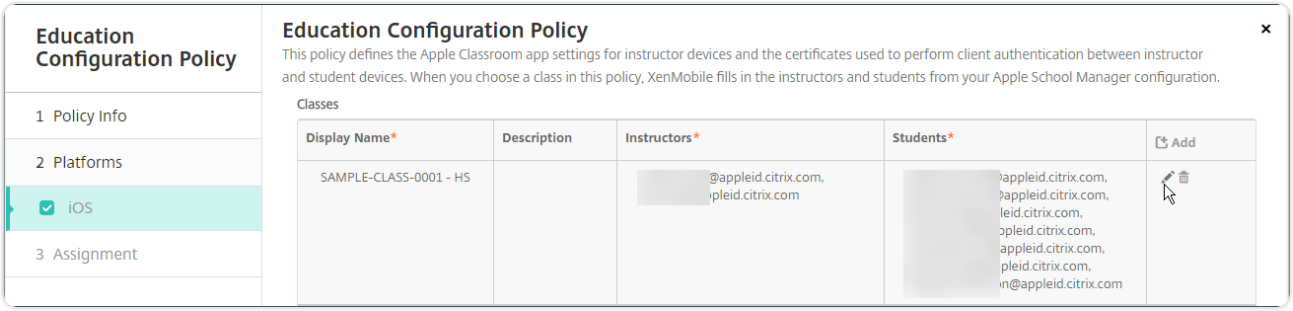


- **允许学生更改屏幕观察权限：** 如果为 **On**，则注册到受管班级的学生可以选择是否允许其教师观察其设备屏幕。默认值为 **Off**。
- **策略设置**
  - **删除策略：** 选择一种策略删除的计划方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”。
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略删除发生前的持续时间。

编辑策略中的班级信息

您可以为班级添加说明（在 Classroom 应用中为“显示名称”）。您还可以添加或删除教师和学生。XenMobile 不会将此类更改保存到您的 Apple School Manager 帐户。有关详细信息，请参阅 (/zh-cn/xenmobile/server/provision-devices/integrate-with-apple-education.html) 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。

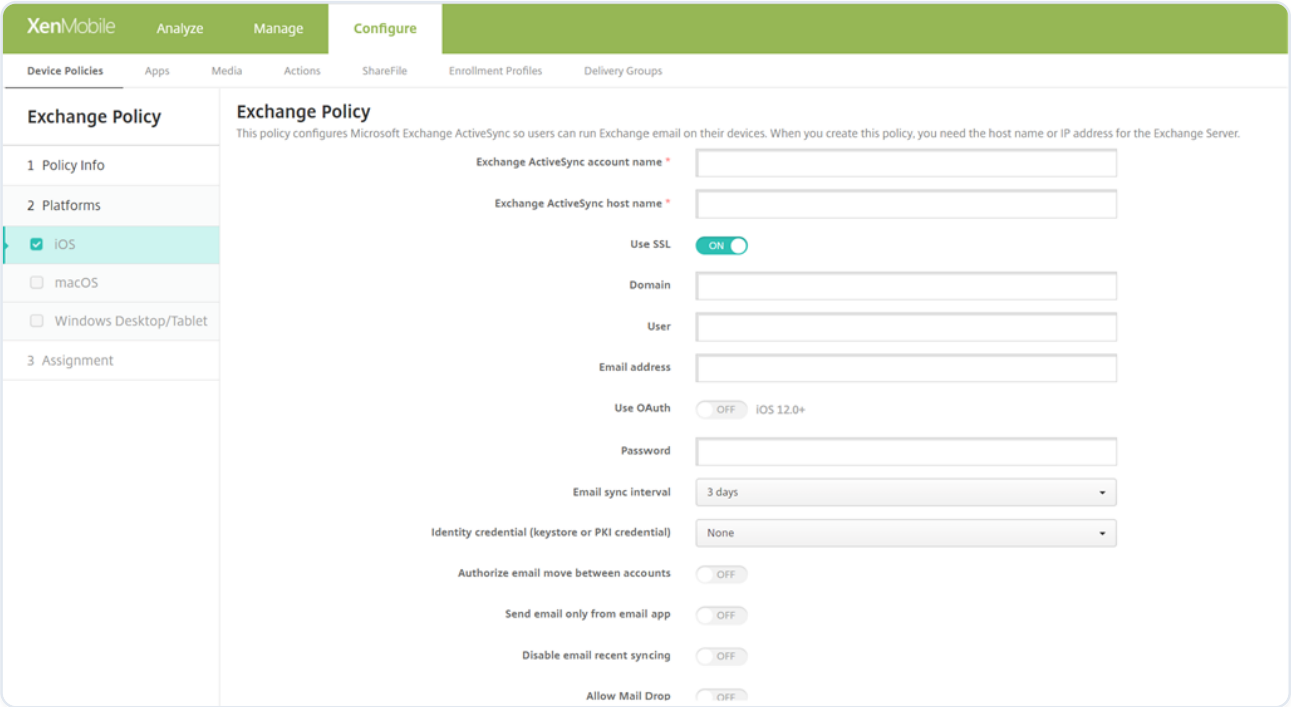
Exchange 设备策略

您可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以便他们访问托管在 Exchange 上的公司电子邮件。您可以为 iOS、macOS、Android Enterprise、Samsung SAFE、Samsung Knox 和 Windows 平板电脑创建策略。每个平台都需要一组不同的值，这些值将在以下部分中详细描述。

要创建此策略，您需要 Exchange Server 的主机名或 IP 地址。有关 ActiveSync 设置的信息，请参阅 Microsoft 文章 ActiveSync CSP。

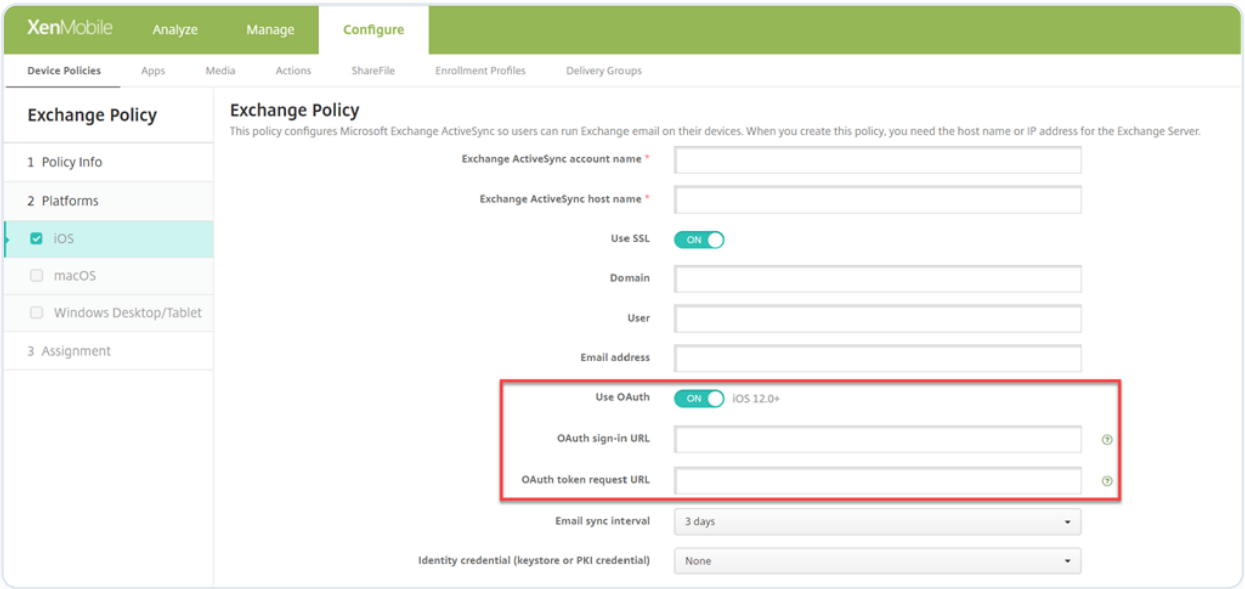
要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

iOS 设置



- **Exchange ActiveSync 帐户名称：** 键入在用户设备上显示的电子邮件帐户的描述。
- **Exchange ActiveSync 主机名：** 键入电子邮件服务器的地址。
- **使用 SSL：** 选择是否保护用户设备与 Exchange Server 之间的连接。默认值为 **开**。
- **域：** 输入 Exchange Server 所在的域。您可以在此字段中使用系统宏 $user.domainname 自动查找用户域名。
- **用户：** 指定 Exchange 用户帐户的用户名。您可以在此字段中使用系统宏 $user.username 自动查找用户名。

- **电子邮件地址：** 指定完整的电子邮件地址。您可以在此字段中使用系统宏 $user.mail 自动查找用户电子邮件帐户。
- **使用 OAuth：** 如果设置为 **开**，则连接使用 OAuth 进行身份验证。默认值为 **关**。此选项适用于 iOS 12.0 及更高版本。
  - **OAuth 登录 URL**：指定在不使用自动发现服务时，加载到 webview 中以使用 OAuth 进行身份验证的 URL。此字段仅在 **使用 OAuth** 设置为 **开** 时显示。
  - **OAuth 令牌请求 URL**：指定帐户可用于 OAuth 令牌请求的 URL。此字段仅在 **使用 OAuth** 设置为 **开** 时显示。

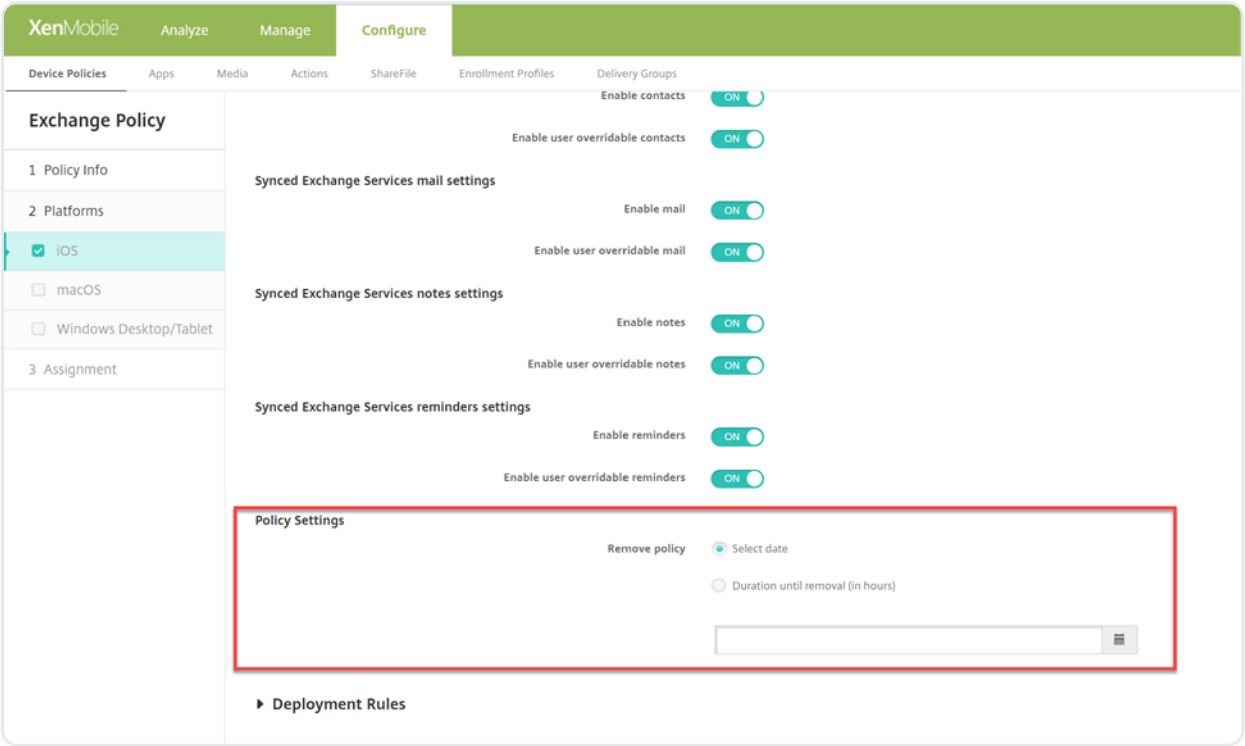


- **密码：输入 Exchange 用户帐户的可选密码。当使用 OAuth设置为开时，此设置不会显示。**
- **电子邮件同步间隔：在列表中，选择电子邮件与 Exchange Server 同步的频率。默认值为3 天**
  。
- **身份凭据（密钥库或 PKI）：如果您已为 XenMobile 配置身份提供程序，请在下拉列表中单击可选的身份凭据。仅当 Exchange 需要客户端证书身份验证时，才需要此字段。默认值为无。**
- **授权帐户间电子邮件移动：选择是否允许用户将电子邮件从此帐户移至其他帐户，以及从其他帐户转发和回复电子邮件。默认值为关。**
- **仅从电子邮件应用发送电子邮件：选择是否限制用户只能使用 iOS 邮件应用发送电子邮件。默认值为关。**
- **禁用电子邮件最近同步：选择是否阻止用户同步最近的地址。默认值为关。**此选项仅适用于 iOS 6.0 及更高版本。
- **允许 Mail Drop：选择是否允许帐户使用 Mail Drop。默认值为关。**
- **启用 S/MIME 签名：选择此帐户是否支持 S/MIME 签名。默认值为开。**设置为开时，将显示以下字段。

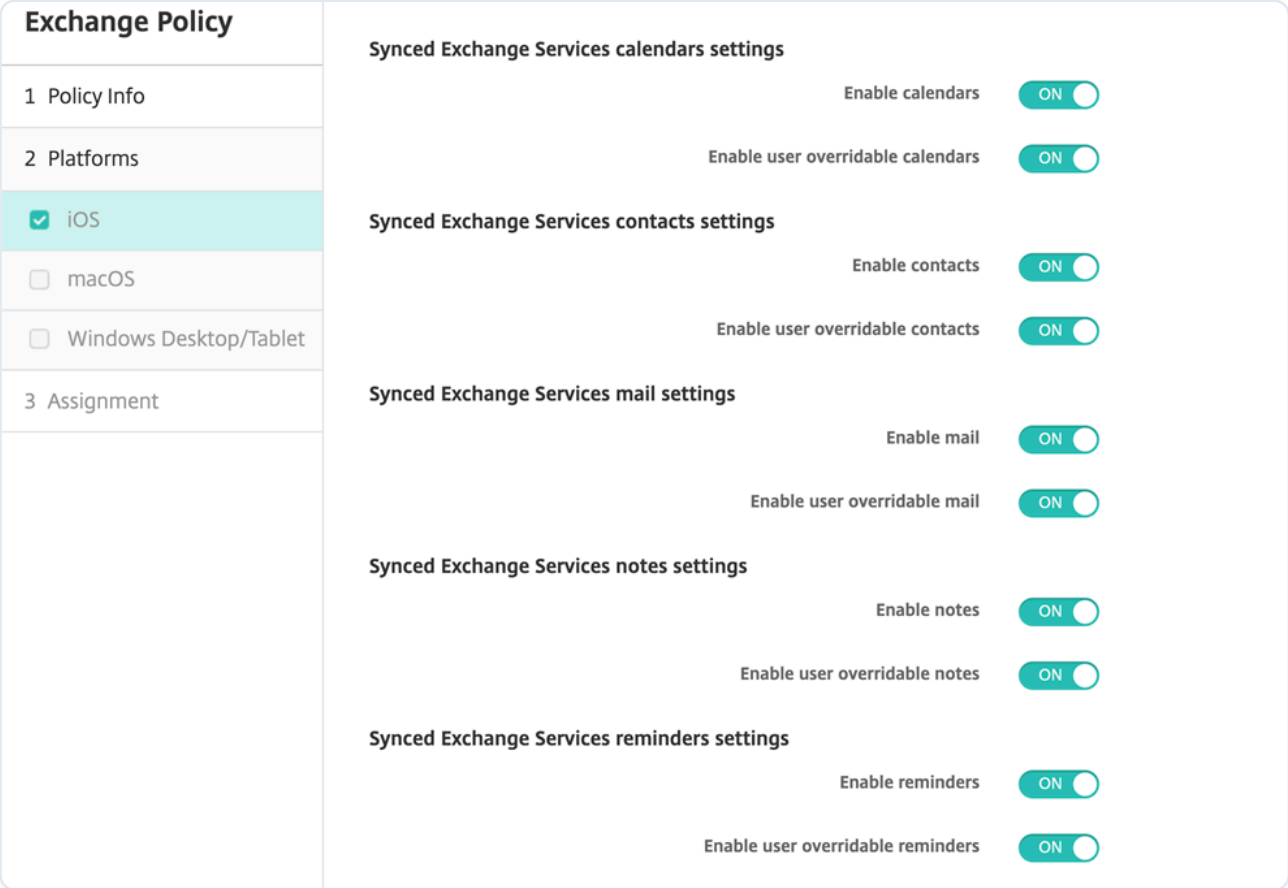
- **签名身份凭据：**选择要使用的签名凭据。
- **S/MIME 签名用户可覆盖：如果设置为开**，用户可以在其设备设置中打开和关闭 S/MIME 签名。默认值为**关**。此选项适用于 iOS 12.0 及更高版本。
- **S/MIME 签名证书 UUID 用户可覆盖：如果设置为开**，用户可以在其设备设置中选择要使用的签名凭据。默认值为**关**。此选项适用于 iOS 12.0 及更高版本。

- **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，将显示以下字段。
  - **加密身份凭据：**选择要使用的加密凭据。
  - **启用每条消息 S/MIME 开关：设置为开**时，会向用户显示一个选项，用于在他们撰写的每条消息中打开或关闭 S/MIME 加密。默认值为**关**。
  - **S/MIME 默认加密用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中选择 S/MIME 是否默认开启。默认值为 **关**。此选项适用于 iOS 12.0 及更高版本。
  - **S/MIME 加密证书 UUID 用户可覆盖：** 如果设置为 **开**，用户可以在其设备设置中开启和关闭 S/MIME 加密身份和加密功能。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：** 选择策略删除的计划方法。可用选项包括 **选择日期** 和 **距离删除的持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **距离删除的持续时间（小时）：** 键入一个数字（以小时为单位），表示距离策略删除的时间。仅适用于 iOS 6.0 及更高版本。



同步的 Exchange 服务



- 同步的 Exchange 服务日历设置

- **启用日历**：允许您为帐户启用或禁用 *日历* 服务。默认值为 **开**。 如果设置为 **关**，则该帐户的 *日历* 服务将被禁用。只有当 **启用用户可覆盖日历** 按钮设置为 **开** 时，才能在设置中再次启用 *日历* 服务。
- **启用用户可覆盖日历**：允许您在设置中更改帐户的 *日历* 服务状态。默认值为 **开**。 如果设置为 **关**，则无法更改 *日历* 服务的状态。

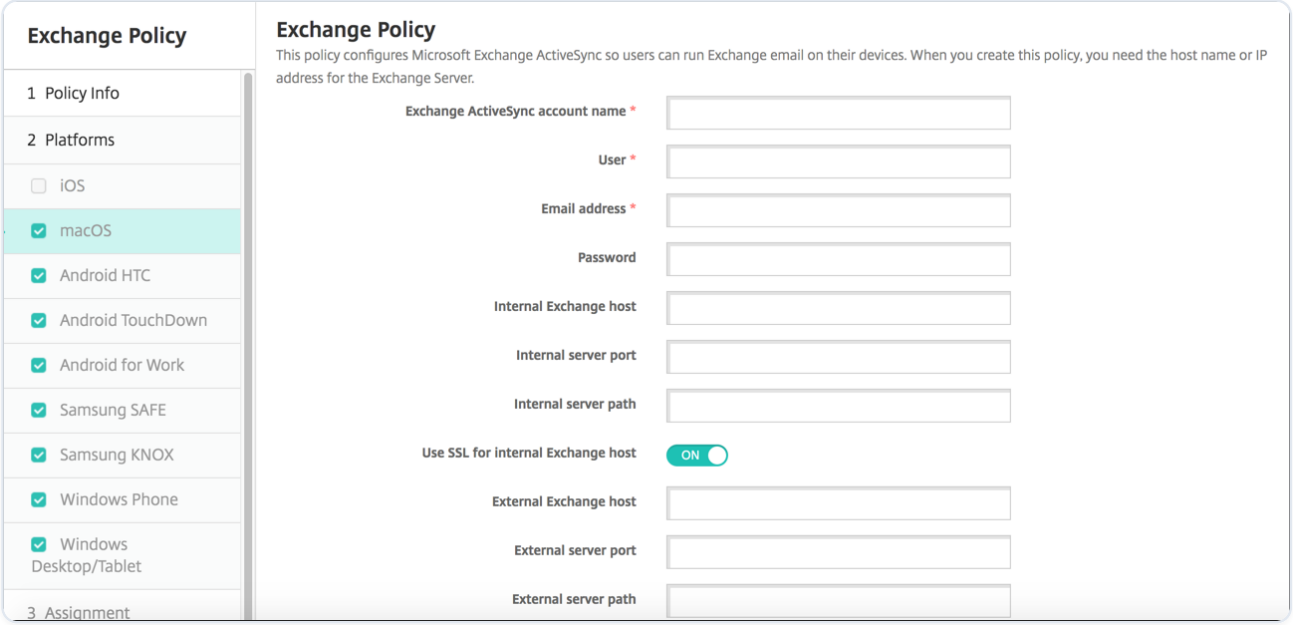
- **同步的 Exchange 服务联系人设置**
  - **启用联系人**：允许您为帐户启用或禁用 *联系人* 服务。默认值为 **开**。 如果设置为 **关**，则该帐户的 *联系人* 服务将被禁用。只有当 **启用用户可覆盖联系人** 按钮设置为 **开** 时，才能在设置中再次启用 *联系人* 服务。
  - **启用用户可覆盖联系人**：允许您在设置中更改帐户的 *联系人* 服务状态。默认值为 **开**。 如果设置为 **关**，则无法更改 *日历* 服务的状态。

- **同步的 Exchange 服务邮件设置**
  - **启用邮件**：允许您为帐户启用或禁用*邮件*服务。默认值为**ON**。 如果设置为**OFF**，则该帐户的*邮件*服务将被禁用。只有当**启用用户可覆盖邮件**按钮设置为**ON**时，才能在设置中再次启用*邮件*服务。
  - **启用用户可覆盖邮件**：允许您在设置中更改帐户的*邮件*服务状态。默认值为**ON**。 如果设置为**OFF**，则无法更改*邮件*服务的状态。

- **同步的 Exchange 服务便笺设置**
  - **启用便笺**：允许您为帐户启用或禁用*便笺*服务。默认值为**ON**。 如果设置为**OFF**，则该帐户的*便笺*服务将被禁用。只有当**启用用户可覆盖便笺**按钮设置为**ON**时，才能在设置中再次启用*便笺*服务。
  - **启用用户可覆盖便笺**：允许您在设置中更改帐户的*便笺*服务状态。默认值为**ON**。 如果设置为**OFF**，则无法更改*便笺*服务的状态。

- **同步的 Exchange 服务提醒设置**
  - **启用提醒**：允许您为帐户启用或禁用*提醒*服务。默认值为**ON**。 如果设置为**OFF**，则该帐户的*提醒*服务将被禁用。只有当**启用用户可覆盖提醒**按钮设置为**ON**时，才能在设置中再次启用*提醒*服务。
  - **启用用户可覆盖提醒**：允许您在设置中更改帐户的*提醒*服务状态。默认值为**ON**。 如果设置为**OFF**，则无法更改*提醒*服务的状态。

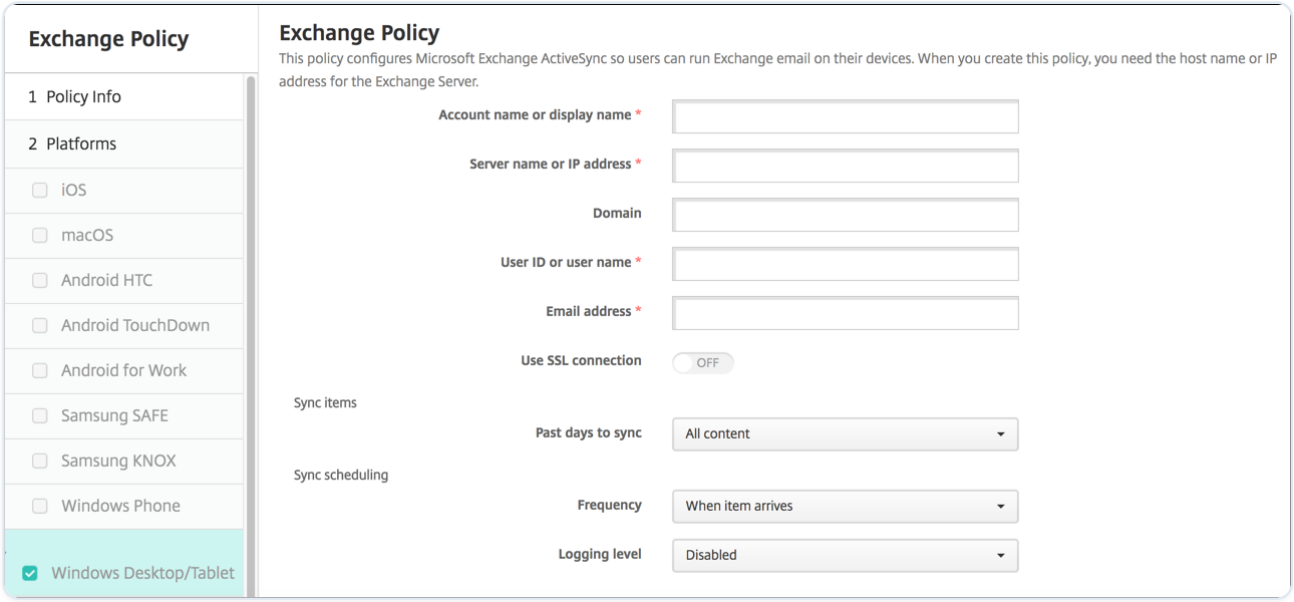
macOS 设置



- **Exchange ActiveSync 帐户名称：** 键入在用户设备上显示的电子邮件帐户的描述。
- **用户：** 指定 Exchange 用户帐户的用户名。您可以在此字段中使用系统宏 $user.username 自动查找用户名。
- **电子邮件地址：** 指定完整的电子邮件地址。您可以在此字段中使用系统宏 $user.mail 自动查找用户电子邮件帐户。
- **使用 OAuth：** 如果设置为 **On**，则连接使用 OAuth 进行身份验证。默认值为 **Off**。此选项适用于 macOS 10.14 及更高版本。
- **OAuth 登录 URL：** 指定当未使用自动发现服务时，加载到 Web 视图中以使用 OAuth 进行身份验证的 URL。当**使用 OAuth** 设置为**开**时，此字段显示。
- **密码：** 输入 Exchange 用户帐户的可选密码。当**使用 OAuth** 为**开**时，此设置不显示。
- **内部 Exchange 主机：** 如果您希望内部和外部 Exchange 主机名不同，请键入可选的内部 Exchange 主机名。
- **内部服务器端口：** 如果您希望内部和外部 Exchange 服务器端口不同，请键入可选的内部 Exchange 服务器端口号。
- **内部服务器路径：** 如果您希望内部和外部 Exchange 服务器路径不同，请键入可选的内部 Exchange 服务器路径。
- **对内部 Exchange 主机使用 SSL：** 选择是否保护用户设备与内部 Exchange 主机之间的连接。默认值为**开**。
- **外部 Exchange 主机：** 如果您希望内部和外部 Exchange 主机名不同，请键入可选的外部 Exchange 主机名。

- **外部服务器端口：** 如果您希望内部和外部 Exchange 服务器端口不同，请键入可选的外部 Exchange 服务器端口号。
- **外部服务器路径：** 如果您希望内部和外部 Exchange 服务器路径不同，请键入可选的外部 Exchange 服务器路径。
- **对外部 Exchange 主机使用 SSL：** 选择是否保护用户设备与内部 Exchange 主机之间的连接。默认值为**开**。
- **允许邮件投送：** 选择是否允许用户在两台 Mac 之间无线共享文件，而无需连接到现有网络。默认值为**关**。
- **策略设置**
  - **删除策略：** 选择策略删除的计划方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您可以选择用户何时可以从其设备中删除策略。从菜单中选择**始终**、**需要密码**或**从不**。如果选择**需要密码**，请在**删除密码**字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**用户**。此选项仅适用于 macOS 10.7 及更高版本。

Windows 桌面/平板电脑设置



注意：

此策略不允许您设置用户密码。用户必须在您推送策略后从其设备设置该参数。

- **帐户名称或显示名称：** 键入 Exchange ActiveSync 帐户名称。
- **服务器名称或 IP 地址：** 键入 Exchange Server 主机名或 IP 地址。
- **域：** 输入 Exchange Server 所在的域。您可以在此字段中使用系统宏 $user.domainname 自动查找用户域名。
- **用户 ID 或用户名：** 指定 Exchange 用户帐户的用户名。您可以在此字段中使用系统宏 $user.username 自动查找用户名。
- **电子邮件地址：** 指定完整的电子邮件地址。您可以在此字段中使用系统宏 $user.mail 自动查找用户电子邮件帐户。
- **使用 SSL 连接：** 选择是否保护用户设备与 Exchange Server 之间的连接。默认值为**关**。
- **过去同步天数：** 在列表中，单击要将设备上的所有内容与 Exchange Server 同步到过去的多少天。默认值为**所有内容**。
- **频率：** 在列表中，单击从 Exchange Server 发送到设备的数据同步时使用的计划。默认值为**到达时**。
- **日志记录级别：** 在下拉列表中单击**禁用**、**基本**或**高级**，以指定记录 Exchange 活动时的详细程度。**默认值为禁用**。

文件设备策略

您可以添加和部署文件，供用户在其 Android 和 Android Enterprise 设备上访问。您可以指定要在设备上存储文件的目录。例如，您希望用户接收公司文档或 .pdf 文件。将文件部署到设备并告知用户文件所在的位置。

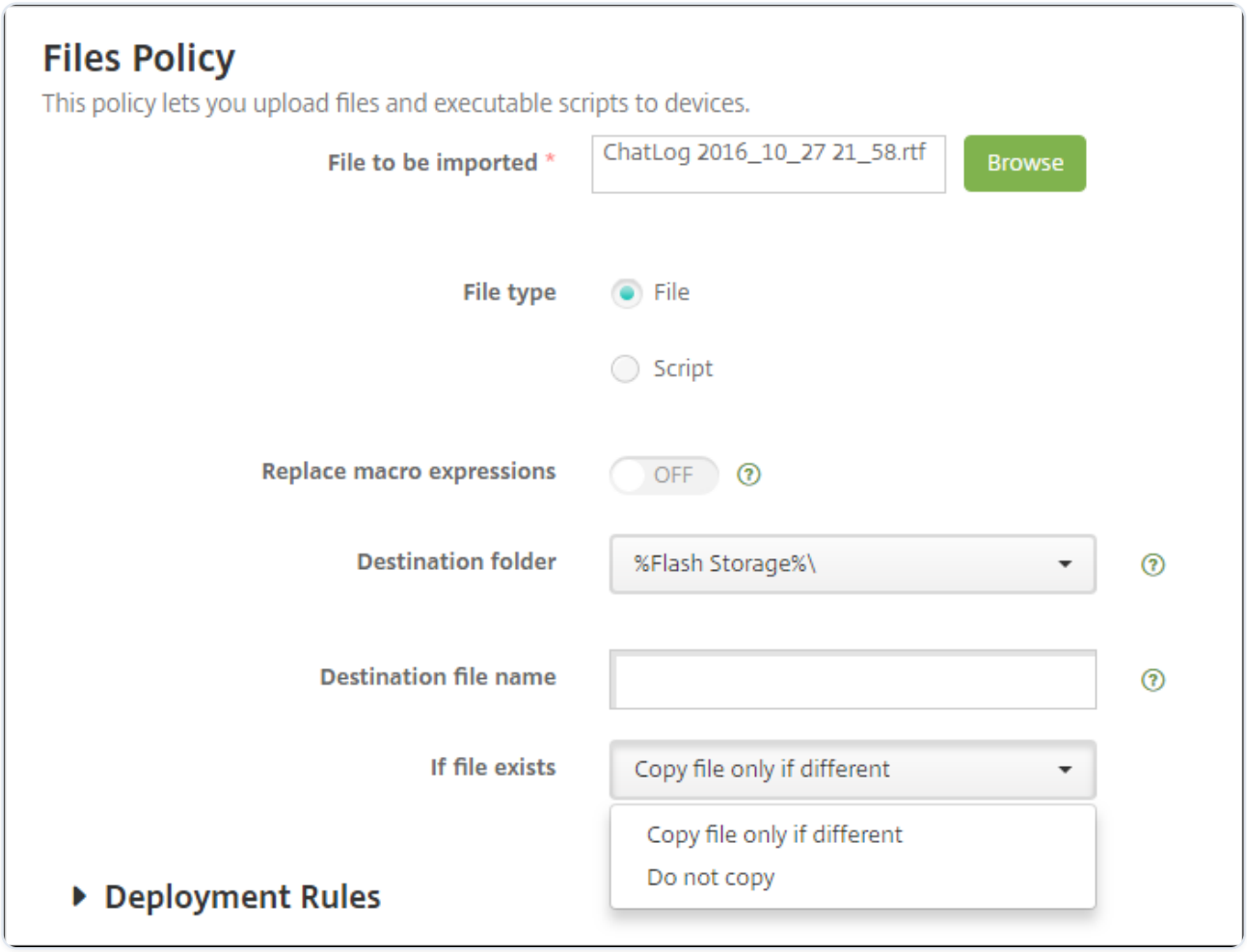
Android 设备不支持本机运行脚本。用户需要第三方软件才能运行脚本。

您可以使用此策略添加以下文件类型：

- 基于文本的文件（.xml、.html、.py 等）
- 其他文件，例如文档、图片、电子表格或演示文稿

要添加或配置此策略，请转到**配置 > 设备策略**。有关详细信息，请参阅设备策略。

Android Enterprise 相关设置



- **要导入的文件：要选择要导入的文件，请单击浏览**并导航到文件位置。
- **文件类型：选择文件。**
- **目标文件夹：在列表中，选择存储上载文件的位置，或单击添加新项**以选择未列出的文件位置。您可以使用宏 %XenMobile Folder%\ 或 %Flash Storage%\ 作为任何路径标识符的开头。
- **目标文件名：**可选。如果必须在将文件部署到设备之前更改文件名，请键入文件名。
- **如果文件存在：在列表中，选择是否复制现有文件。默认值为仅当文件不同时复制文件。**

Android 设置

- **要导入的文件**：通过单击“**浏览**”并导航到文件位置来选择要导入的文件。
- **文件类型**：选择“**文件**”。
- **目标文件夹**：在列表中，选择存储上传文件的位置，或单击“**添加新项**”以选择未列出的文件位置。此外，您可以使用宏 %XenMobile Folder%\\ 或 %Flash Storage%\\ 作为路径标识符的开头。
- **目标文件名**：（可选）如果文件在部署到设备之前必须更改，请键入不同的文件名。

- **仅当文件不同时才复制**：在列表中，选择是否在文件与现有文件不同时复制该文件。默认设置是仅当文件不同时才复制。

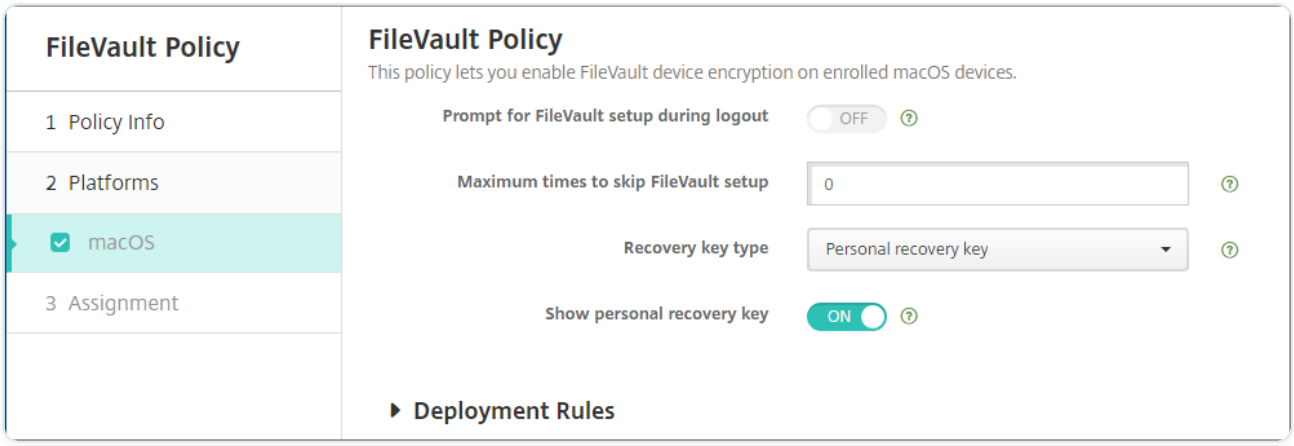
FileVault 设备策略

macOS FileVault 磁盘加密功能通过加密其内容来保护系统卷。在 macOS 设备上启用 FileVault 后，用户每次启动设备时都使用其帐户密码登录。如果用户丢失密码，恢复密钥可让他们解锁磁盘并重置密码。

XenMobile 设备策略 FileVault 启用 FileVault 用户设置屏幕并配置恢复密钥等设置。有关 FileVault 的更多信息，请参阅 Apple 支持网站，`<https://support.apple.com>`。

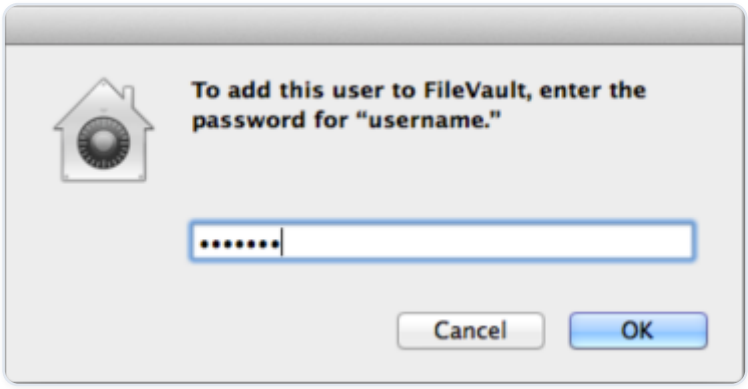
要添加 FileVault 策略，请转至 **配置 > 设备策略**。

macOS 设置

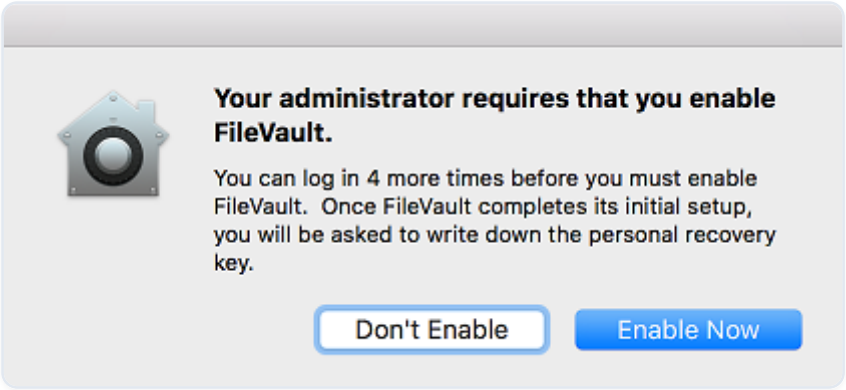


- **注销时提示设置 FileVault**： 如果设置为“**开**”，则在接下来的 N 次注销期间提示用户启用 FileVault，其中 N 由选项“**跳过 FileVault 设置的最大次数**”指定。如果设置为“**关**”，则不会出现 FileVault 密码提示。

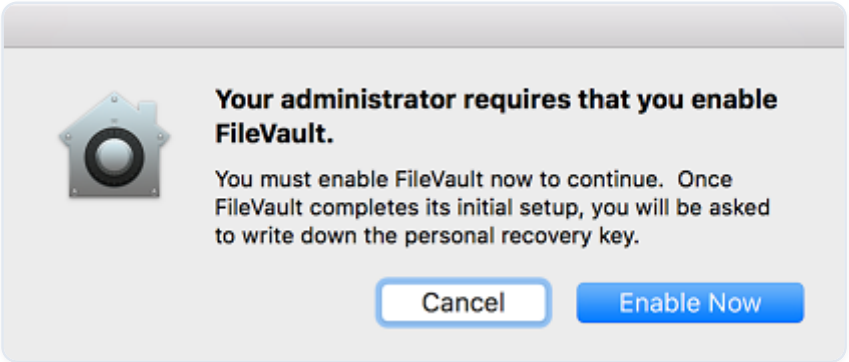
部署启用此设置的 FileVault 策略后，当用户注销设备时，将显示以下屏幕。该屏幕为用户提供了在注销前启用 FileVault 的选项。

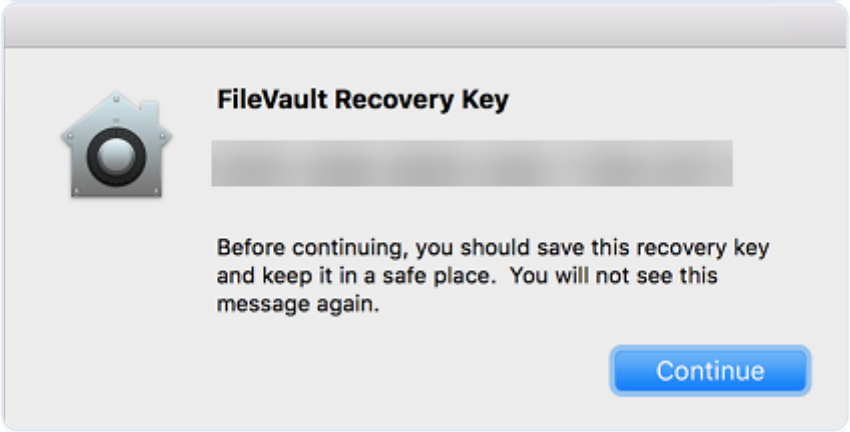


如果“**跳过 FileVault 设置的最大次数**”值不为 0：在部署禁用此设置的 FileVault 策略后，当用户登录时，将显示以下屏幕。



如果“**跳过 FileVault 设置的最大次数**”值为 0 或者用户已跳过设置达到最大次数，将显示以下屏幕。





字体设备策略

您可以在 XenMobile® 中添加设备策略，以向 iOS 和 macOS 设备添加更多字体。字体必须是 TrueType (`.ttf`) 或 OpenType (`.oft`) 字体。不支持字体集 (`.ttc` 或 `.otc`)。

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 **Configure > Device Policies**。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**，然后导航到文件位置，选择要添加到用户设备的字体文件。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- **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**，然后导航到文件位置，选择要添加到用户设备的字体文件。
- **策略设置**
  - **移除策略：** 选择一种安排策略移除的方法。可用选项为“**选择日期**”和“**移除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略移除。
  - **允许用户移除策略：** 您可以选择用户何时可以从其设备中移除策略。从菜单中选择“**始终**”、“**需要密码**”或“**从不**”。如果您选择“**需要密码**”，请在“**移除密码**”字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**用户**。此选项仅适用于 macOS 10.7 及更高版本。

主屏幕布局设备策略

您可以指定 iOS 主屏幕上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 及更高版本的受监管设备。

> **重要提示：**

> 将多个主屏幕布局策略部署到设备会导致设备上出现 iOS 错误。此限制适用于通过此 XenMobile® 策略或通过 Apple Configurator 定义主屏幕的情况。

> 要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-homescreen.png)

- 对于要配置的每个屏幕区域（例如**Dock**或**Page 1**），单击**添加**。
- **类型：** 选择**应用程序**、**文件夹**或**Web 剪辑**。

  限制设备策略中的**受限应用程序使用 > 仅允许某些应用程序**设置可能会阻止 Web 剪辑在主屏幕上正常显示。要使 Web 剪辑正常显示，请执行以下任一操作：

  - 将**受限应用程序使用**设置为**允许所有应用程序**或**不允许某些应用程序**。
  - 在**受限应用程序使用**设置为**仅允许某些应用程序**的情况下，添加捆绑包 ID 为 `com.apple.webapp` 的应用程序以允许 Web 剪辑。

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/homescreen-policy-application.png)

- **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，键入捆绑包标识符。对于文件夹，键入以逗号分隔的捆绑包标识符列表。对于 Web 剪辑，键入捆绑包 ID `com.apple.webClip.managed` 并在 Web 剪辑策略中配置 Web 剪辑的 URL。如果存在多个具有相同 URL 的 Web 剪辑值，则在 iOS 11.3 及更高版本的设备上行为未定义。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 输入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。
  - **配置文件范围：** 选择此策略是应用于“**用户**”还是整个“**系统**”。默认值为“**用户**”。此选项仅适用于 iOS 9.3 及更高版本。

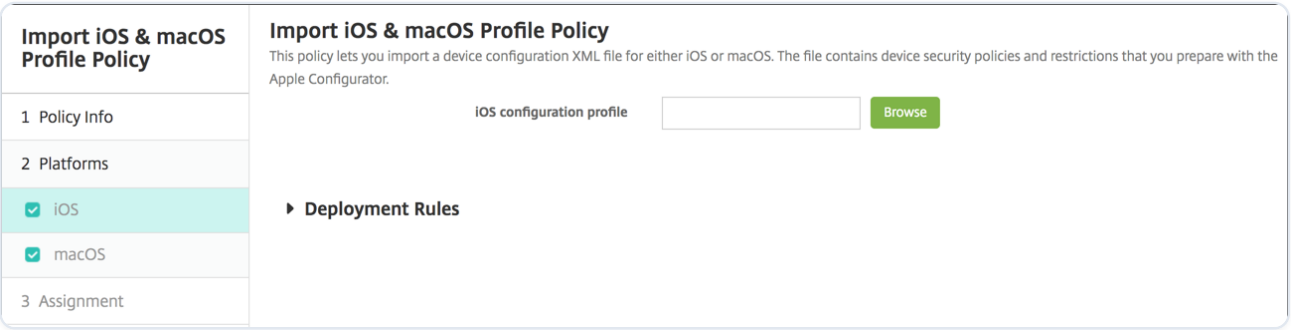
导入 iOS 和 macOS 配置文件设备策略

您可以将用于 iOS 和 macOS 设备的设备配置 XML 文件导入到 XenMobile 中。该文件包含您使用 Apple Configurator 准备的设备安全策略和限制。

您可以使用 Apple Configurator 将 iOS 设备置于监督模式，如本文稍后所述。有关使用 Apple Configurator 创建配置文件的更多信息，请参阅 Apple Configurator 支持。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅 设备策略。

iOS 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**并导航到文件位置。

使用 Apple Configurator 将 iOS 设备置于监督模式

要使用 Apple Configurator，您需要一台运行 macOS 10.7.2 或更高版本的 Apple 电脑。

> **重要提示：**
>
> 将设备置于监督模式会在设备上安装所选版本的 iOS，从而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 设备连接到您的 Apple 电脑。
3. 启动 Apple Configurator。Configurator 会显示您有一台设备需要准备进行监督。
4. 要准备设备进行监督：
   a. 将**监管**控制设置为**开**。Citrix® 建议您选择此设置，如果您打算通过定期重新应用配置来持续控制设备。
   b. （可选）为设备提供一个名称。
   c. 在 iOS 中，单击**最新**以获取您要安装的最新 iOS 版本。
5. 当您准备好将设备用于监管时，单击**准备**。

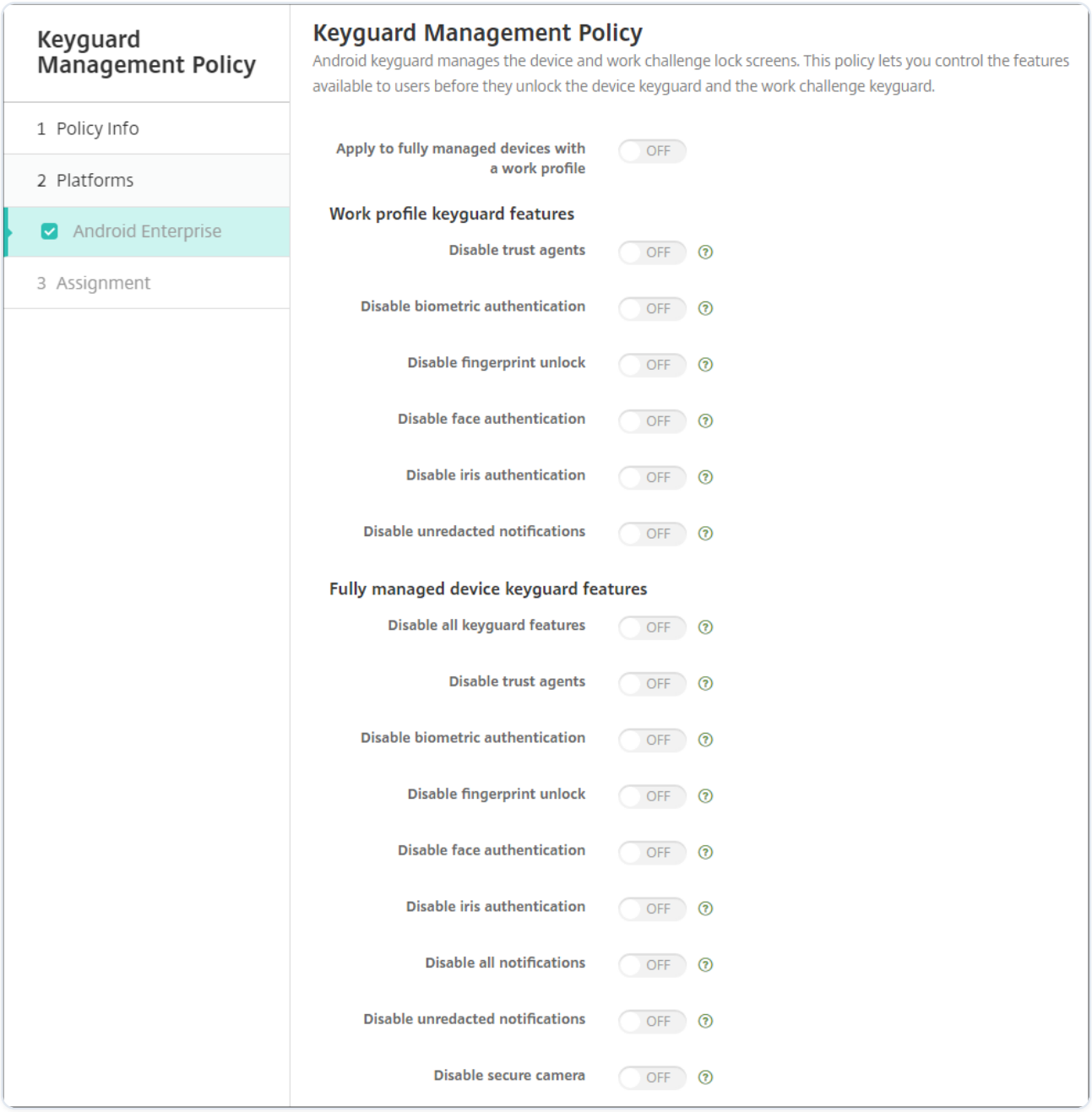
屏幕锁定管理设备策略

Android 屏幕锁定管理设备和工作挑战锁屏。此策略允许您管理 Android Enterprise 工作资料屏幕锁定和高级设备屏幕锁定的功能。您可以控制：

- 工作资料设备上的屏幕锁定管理。您可以指定用户在解锁设备屏幕锁定和工作挑战屏幕锁定之前可用的功能。例如，默认情况下，用户可以使用指纹解锁并在锁屏上查看未编辑的通知。
- 完全托管设备和专用设备上的屏幕锁定管理。您可以指定在解锁屏幕锁定之前可用的功能，例如信任代理和安全摄像头。或者，您可以选择禁用所有屏幕锁定功能。
- 具有工作资料的完全托管设备上的屏幕锁定管理。您可以使用一个屏幕锁定管理策略来对设备和工作资料应用单独的设置。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

Android 企业版设置



- **应用于具有工作资料的完全托管设备：** 允许您为具有工作资料的完全托管设备配置屏幕锁定管理设备策略设置。

  当此设置设为“**开**”时，您可以对具有工作资料的完全托管设备上的设备和工作资料应用单独的设置。

  当此设置设为“**关**”时，您可以将设置应用于工作资料设备或完全托管设备。您为工作资料配置的设置仅适用于工作资料设备。您为完全托管设备配置的设置仅适用于完全托管设备。

  默认值为“**关**”。

- **工作资料屏幕锁定功能：** 控制用户在解锁工作资料屏幕锁定（锁屏）之前是否可以使用以下功能。
  - **禁用信任代理：** 如果设为“**关**”，则当工作资料上设置了挑战时，信任代理可以在安全屏幕锁定屏幕上运行。设为“**开**”可禁用工作资料上的所有信任代理。默认值为“**关**”。
  - **禁用生物识别身份验证：** 如果设为“**关**”，则当工作资料上设置了挑战时，生物识别身份验证可在安全屏幕锁定屏幕上使用。设为“**开**”可禁用工作资料上的生物识别身份验证。此设置禁用指纹解锁、面部身份验证和虹膜身份验证。默认值为“**关**”。适用于 Android 9.0 及更高版本。
  - **禁用指纹解锁：** 如果设置为“**开**”，则在工作资料上设置质询时，安全锁屏界面上无法使用指纹解锁。设置为“**关**”以在工作资料上启用指纹解锁。默认值为“**关**”。
  - **禁用面部认证：** 如果设置为“**关**”，则在工作资料上设置质询时，安全锁屏界面上可以使用面部认证。设置为“**开**”以在工作资料上禁用面部认证。默认值为“**关**”。适用于 Android 9.0 及更高版本。
  - **禁用虹膜认证：** 如果设置为“**关**”，则在工作资料上设置质询时，安全锁屏界面上可以使用虹膜认证。设置为“**开**”以在工作资料上禁用虹膜认证。默认值为“**关**”。适用于 Android 9.0 及更高版本。
  - **禁用未编辑的通知：** 如果设置为“**关**”，则安全锁屏界面上会显示已编辑和未编辑的通知。设置为“**开**”以禁用未编辑的通知，并仅显示已编辑的通知。默认值为“**关**”。
- **完全托管设备锁屏功能：** 控制用户解锁设备锁屏（锁定屏幕）之前是否可以使用以下功能。这些功能适用于完全托管或专用设备。
  - **禁用所有锁屏功能：** 如果设置为“**关**”，则安全锁屏界面上可以使用所有当前和未来的锁屏自定义设置。设置为“**开**”以禁用所有锁屏自定义设置。默认值为“**关**”。
  - **禁用信任代理：** 如果设置为“**关**”，则信任代理可以在安全锁屏界面上运行。设置为“**开**”以禁用信任代理。默认值为“**关**”。
  - **禁用生物识别认证：** 如果设置为“**关**”，则在设备上设置质询时，安全锁屏界面上可以使用生物识别认证。设置为“**开**”以在设备上禁用生物识别认证。这将禁用指纹解锁、面部认证和虹膜认证。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**”，则在设备上设置质询时，安全锁屏界面上可以使用指纹解锁。设置为“**开**”以在设备上禁用指纹解锁。默认值为“**关**”。
  - **禁用面部认证：** 如果设置为“**关**”，则在设备上设置质询时，安全锁屏界面上可以使用面部认证。设置为“**开**”以在设备上禁用面部认证。默认值为“**关**”。适用于 Android 9.0 及更高版本。
  - **禁用虹膜认证：** 如果设置为“**关**”，则在设备上设置质询时，安全锁屏界面上可以使用虹膜认证。设置为“**开**”以在设备上禁用虹膜认证。默认值为“**关**”。适用于 Android 9.0 及更高版本。

- **禁用所有通知：** 如果设置为“**关**”，则所有通知都会显示在安全锁屏界面上。设置为“**开**”以显示所有通知。默认值为“**关**”。
- **禁用未编辑的通知：** 如果设置为“**关**”，则安全锁屏界面上会显示已编辑和未编辑的通知。设置为“**开**”以禁用未编辑的通知，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**”，则安全锁屏界面上可以使用安全摄像头。设置为“**开**”以禁用安全摄像头。默认值为“**关**”。

自助服务终端设备策略

自助服务终端策略允许您通过限制可运行的应用程序，将设备限制为自助服务终端模式。XenMobile® 不控制设备在自助服务终端模式下锁定的部分。部署策略后，设备会管理**自助服务终端模式**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。

添加自助服务终端设备策略

为自助服务终端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 移动设备管理 (MDM) API 4.0 及更高版本。

安卓企业设置

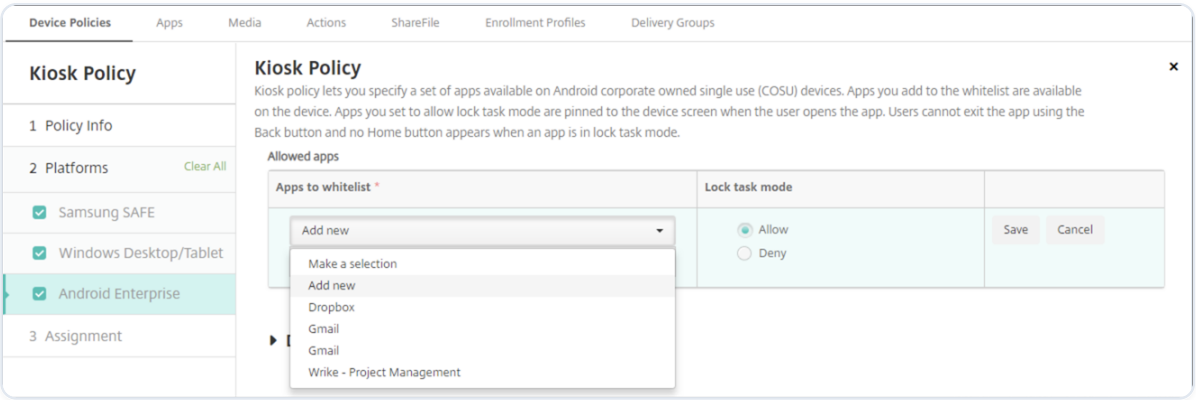
您可以允许应用程序并为专用 Android Enterprise 设备设置锁定任务模式，这些设备也称为企业自有单用途 (COSU) 设备。默认情况下，Secure Hub 和 Google Play 服务位于允许列表中。

要允许某个应用程序，请单击**添加**。您可以允许多个应用程序。有关详细信息，请参阅Android Enterprise。

> **注意：**
>
> XenMobile Server 控制台包含“黑名单”和“白名单”术语。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

- **要列入白名单的应用程序：** 输入要列入白名单的应用程序的包名称，或从列表中选择该应用程序。
  - 单击**添加新项**以输入经批准可在列表中显示的应用程序的包名称。

- 从列表中选择现有应用程序。该列表显示已上传到 XenMobile Server 的应用程序。默认情况下，Secure Hub 和 Google Play 服务已列入白名单。



- **锁定任务模式：** 选择**允许**可将应用程序固定到设备屏幕，以便用户启动该应用程序。选择**拒绝**可将应用程序设置为不固定。默认情况下，Secure Hub 和 Google Play 服务是允许的。默认值为**允许**。

当应用处于锁定任务模式时，用户打开应用时，应用会固定在设备屏幕上。不显示主页按钮，并且“**返回**”按钮被禁用。用户通过应用中编程的操作（例如注销）退出应用。

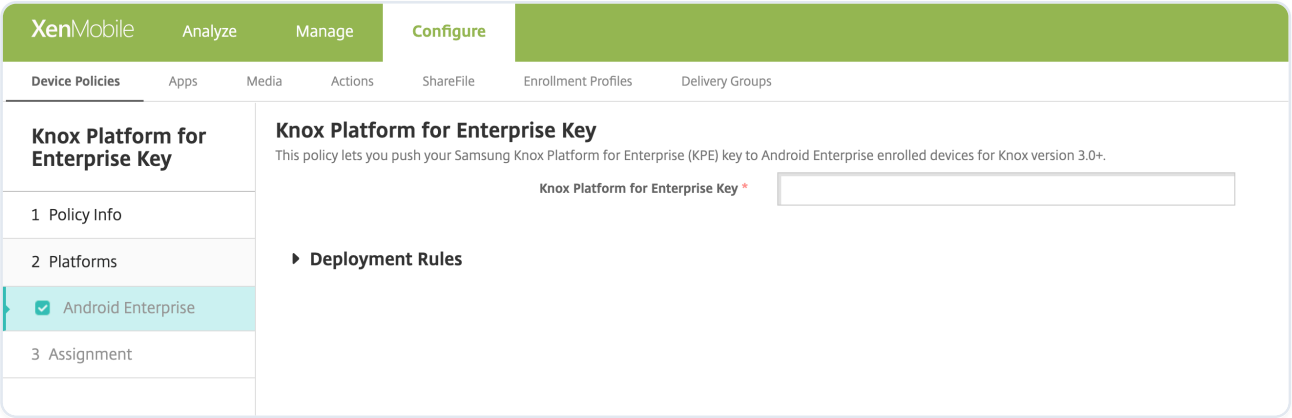
Knox Platform for Enterprise 密钥设备策略

此策略允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息。

要添加或配置此策略，请转至 **配置** > **设备策略**。有关详细信息，请参阅设备策略。

安卓企业版设置

此策略允许您将 Samsung Knox Platform for Enterprise (KPE) 许可证密钥推送到已注册到 Android Enterprise 平台且适用于 Samsung Knox 3.0 或更高版本的设备。



Knox Platform for Enterprise 密钥： 输入要推送到 Android Enterprise 设备的 Samsung Knox Platform for Enterprise (KPE) 密钥。在Samsung Knox Platform for Enterprise (KPE) 密钥处申请 KPE 许可证密钥。

启动器配置设备策略

Citrix Launcher 允许您自定义 XenMobile 部署的 Android 设备的用户体验。Citrix Launcher 和启动器配置设备策略与 Android Enterprise 不兼容。

您可以添加启动器配置策略来控制以下 Citrix Launcher 功能：

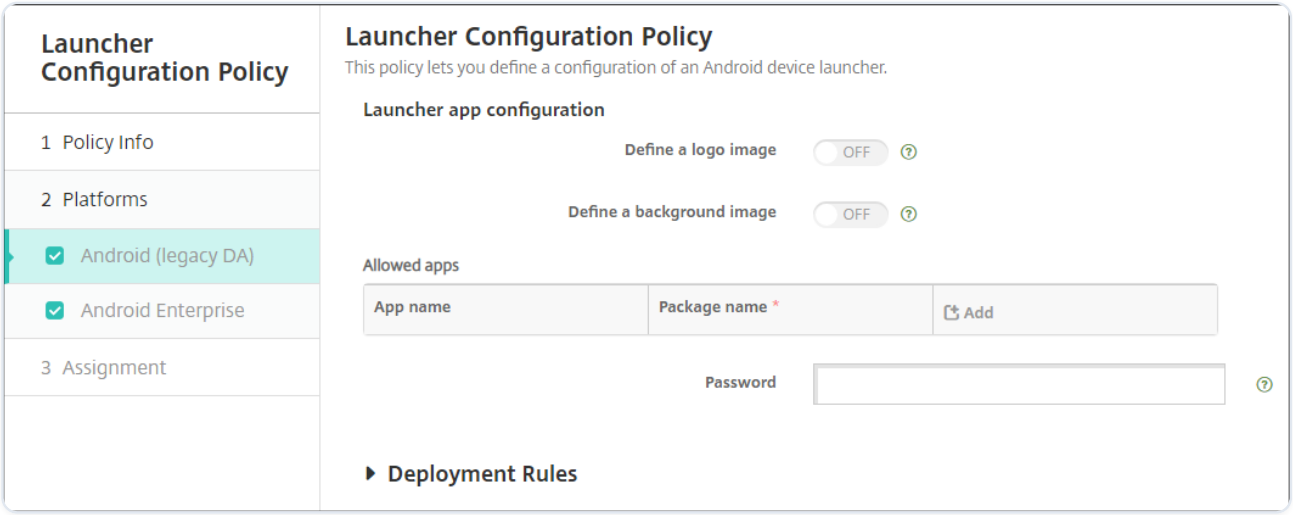
- 管理 Android 设备，以便用户只能访问您指定的应用程序。
- （可选）为 Citrix Launcher 图标指定自定义徽标图像，并为 Citrix Launcher 指定自定义背景图像。
- 指定用户必须输入才能退出启动器的密码。

虽然 Citrix Launcher 使您能够应用这些设备级限制，但该启动器通过内置访问设备设置（例如 Wi-Fi 设置、蓝牙设置和设备密码设置）为用户提供了所需的操作灵活性。Citrix Launcher 并非旨在提供设备平台已提供的额外安全层。

部署 Citrix Launcher 后，XenMobile 将安装它，替换默认的 Android 启动器。

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



- **定义徽标图像：** 选择是否为 Citrix Launcher 图标使用自定义徽标图像。默认值为 **关**。
- **徽标图像：** 启用**定义徽标图像**后，通过单击**浏览**并导航到文件位置来选择图像文件。支持的文件类型为 PNG、JPG、JPEG 和 GIF。
- **定义背景图像：** 选择是否为 Citrix Launcher 背景使用自定义图像。默认值为 **关**。
- **背景图像：** 启用**定义背景图像**后，通过单击**浏览**并导航到文件位置来选择图像文件。支持的文件类型为 PNG、JPG、JPEG 和 GIF。

- **允许的应用程序：** 对于要在 Citrix Launcher 中允许的每个应用程序，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，Android 日历应用程序的 com.android.calendar。
  - 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：** 用户必须输入才能退出 Citrix Launcher 的密码。

安卓企业设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-launcherconfig-android-enterprise.png)

- **启用系统信息：** 选择是否在 Citrix Launcher 状态栏中显示系统信息。默认值为“**关闭**”。需要 Secure Hub 26.8 或更高版本。
- **定义徽标图像：** 选择是否为 Citrix Launcher 图标使用自定义徽标图像。默认值为“**关闭**”。
- **徽标图像：** 启用“**定义徽标图像**”后，通过单击“**浏览**”并导航到文件位置来选择图像文件。支持的文件类型为 PNG、JPG、JPEG 和 GIF。
- **定义背景图像：** 选择是否为 Citrix Launcher 背景使用自定义图像。默认值为“**关闭**”。
- **背景图像：** 启用“**定义背景图像**”后，通过单击“**浏览**”并导航到文件位置来选择图像文件。支持的文件类型为 PNG、JPG、JPEG 和 GIF。
- **允许的应用程序：** 对于要在 Citrix Launcher 中允许的每个应用程序，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，Android 日历应用程序的 com.android.calendar。
  - 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。
- **自动启动应用程序：** 选择一个“**允许的应用程序**”，以便在 Citrix Launcher 启动时自动启动。默认值为“**无**”（不自动启动）。需要 Citrix Launcher 26.8 或更高版本。
- **密码：** 用户退出 Citrix Launcher 时必须输入的密码。

LDAP 设备策略

您可以在 XenMobile® 中为 iOS 设备创建 LDAP 策略，以提供有关要使用的 LDAP 服务器的信息，包括任何必要的帐户信息。该策略还提供了一组在查询 LDAP 服务器时要使用的 LDAP 搜索策略。

在配置此策略之前，您需要 LDAP 主机名。

要添加或配置此策略，请转到**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

- **帐户描述：** 输入可选的帐户描述。
- **帐户用户名：** 输入可选的用户名。
- **帐户密码：** 输入可选密码。仅将此字段用于加密配置文件。
- **LDAP 主机名：** 输入 LDAP 服务器主机名。此字段为必填项。
- **使用 SSL：** 选择是否使用安全套接字层连接到 LDAP 服务器。默认值为**开**。
- **搜索设置：** 添加在查询 LDAP 服务器时要使用的搜索设置。您可以输入任意数量的搜索设置，但必须至少添加一个搜索设置才能使帐户有用。单击**添加**，然后执行以下操作：
  - **描述：** 输入搜索设置的描述。此字段为必填项。
  - **范围：** 选择**基本**、**一级**或**子树**以定义在 LDAP 树中搜索的深度。默认值为**基本**。
    - **基本**搜索“搜索基准”指向的节点。
    - **一级**搜索基本节点及其下一级。
    - **子树**搜索基本节点及其所有子节点，无论深度如何。
  - **搜索基准：**输入开始搜索的节点的路径。例如，ou=people 或 0=example corp。此字段为必填项。
  - 单击“**保存**”以添加搜索设置，或单击“**取消**”以取消添加搜索设置。
  - 对要添加的每个搜索设置重复这些步骤。
- **策略设置**
  - **删除策略：**选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：**单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

macOS 设置

- **帐户描述：**输入可选的帐户描述。
- **帐户用户名：**输入可选的用户名。
- **帐户密码：**输入可选密码。仅将此字段用于加密配置文件。

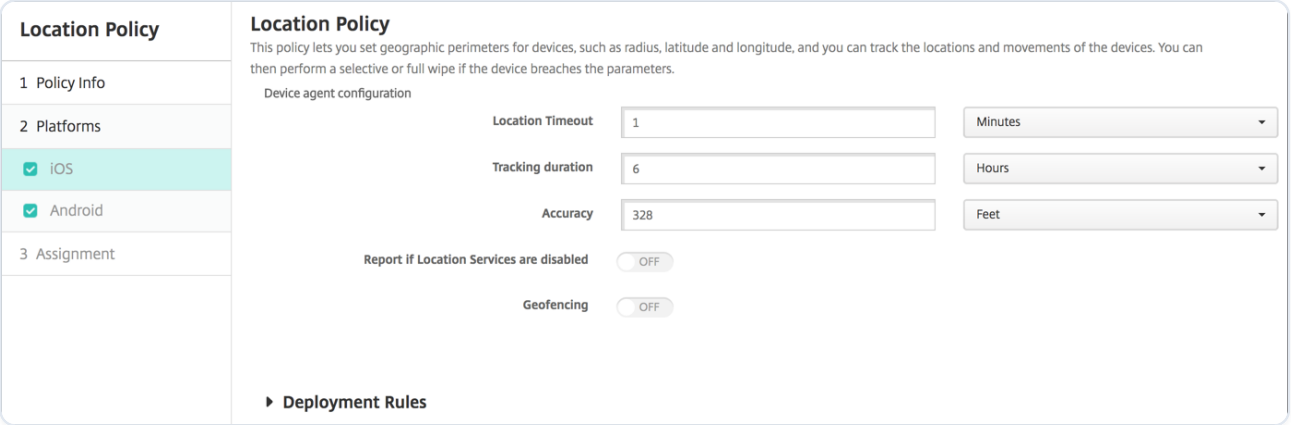
- **LDAP 主机名：**输入 LDAP 服务器主机名。此字段为必填项。
- **使用 SSL：**选择是否使用安全套接字层连接到 LDAP 服务器。默认值为“**开**”。
- **搜索设置：**添加在查询 LDAP 服务器时要使用的搜索设置。您可以根据需要输入任意数量的搜索设置，但必须至少添加一个搜索设置才能使帐户有用。单击“**添加**”，然后执行以下操作：
  - **描述：** 输入搜索设置的描述。此字段为必填项。
  - **范围：** 选择“**基本**”、“**一级**”或“**子树**”以定义在 LDAP 树中搜索的深度。默认值为“**基本**”。
    - **基本**”搜索“搜索基本”指向的节点。
    - **一级**”搜索基本节点及其下一级。
    - **子树**”搜索基本节点及其所有子节点，无论深度如何。
  - **搜索基本：** 输入开始搜索的节点路径。例如，ou=people 或 0=example corp。此字段为必填项。
  - 单击“**保存**”以添加搜索设置，或单击“**取消**”以取消添加搜索设置。
  - 对要添加的每个搜索设置重复这些步骤。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您可以选择用户何时可以从其设备中删除策略。从菜单中选择“**始终**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于“**用户**”还是整个“**系统**”。默认值为“**用户**”。此选项仅在 macOS 10.7 及更高版本上可用。

位置设备策略

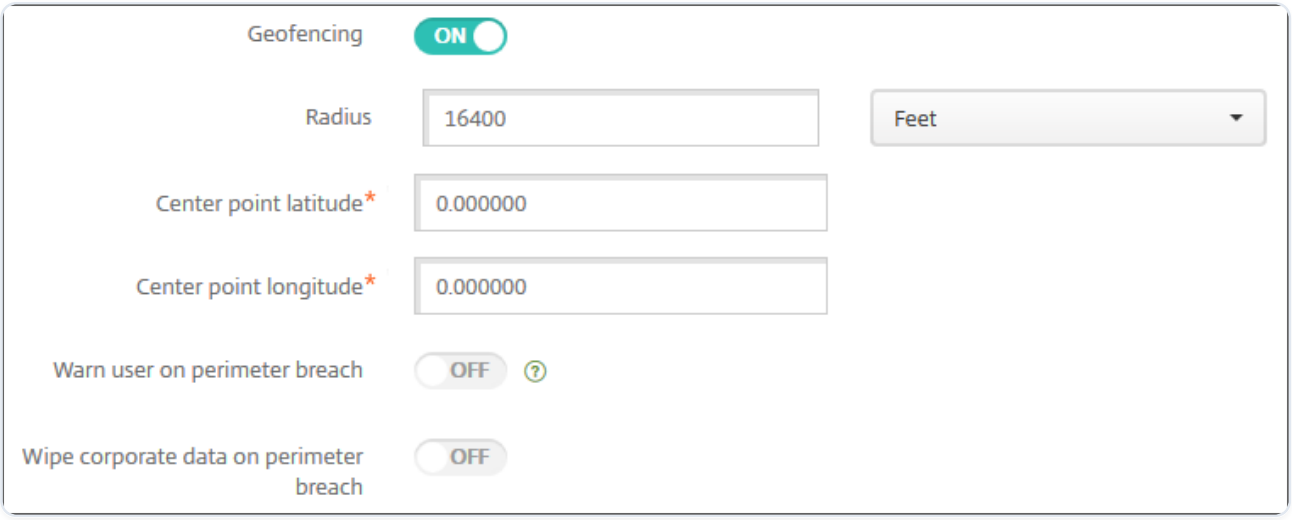
您可以在 XenMobile 中创建位置设备策略以强制执行地理边界。当用户超出定义的边界（也称为*地理围栏*）时，XenMobile 可以执行某些操作。例如，您可以将策略配置为在用户超出定义的范围时向其发出警告消息。您还可以将策略配置为在用户超出范围时立即或延迟擦除其企业数据。有关安全操作（例如启用跟踪和定位设备）的信息，请参阅安全操作。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置



- **位置超时：** 键入一个数字，然后从列表中单击**秒**或**分钟**以设置 XenMobile® 尝试确定设备位置的频率。有效值为 60–900 秒或 1–15 分钟。默认值为 1 分钟。
- **跟踪持续时间：** 键入一个数字，然后从列表中单击**小时**或**分钟**以设置 XenMobile 跟踪设备的时长。有效值为 1–6 小时或 10–360 分钟。默认值为 6 小时。
- **精确度：** 键入一个数字，然后从列表中单击**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 30–15000 英尺。默认值为 328 英尺。
- **如果位置服务已禁用则报告：** 选择当 GPS 禁用时设备是否向 XenMobile 发送报告。默认值为**关**。
- **地理围栏**



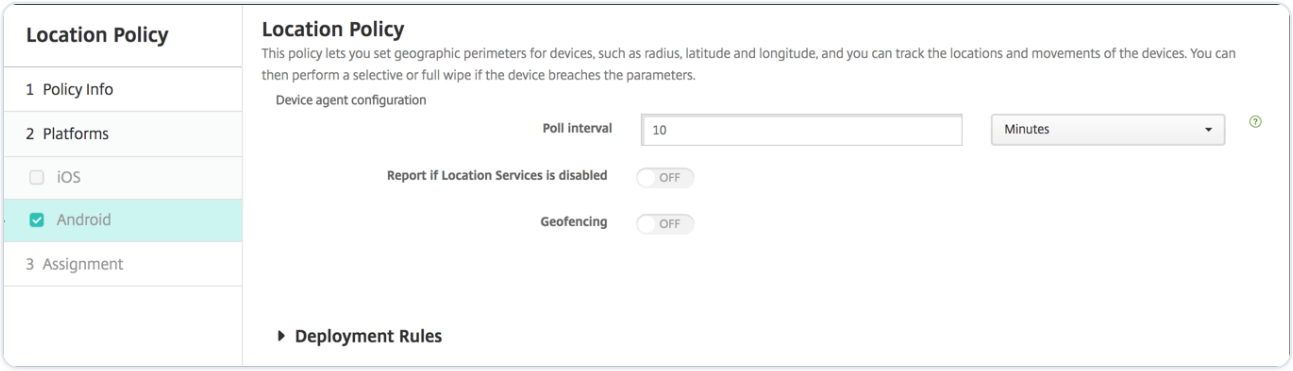
启用地理围栏后，配置以下设置：

- **半径：** 键入一个数字，然后从列表中单击用于测量半径的单位。默认值为 16,400 英尺。半径的有效值为：
  - 164–164000 英尺
  - 50–50000 米

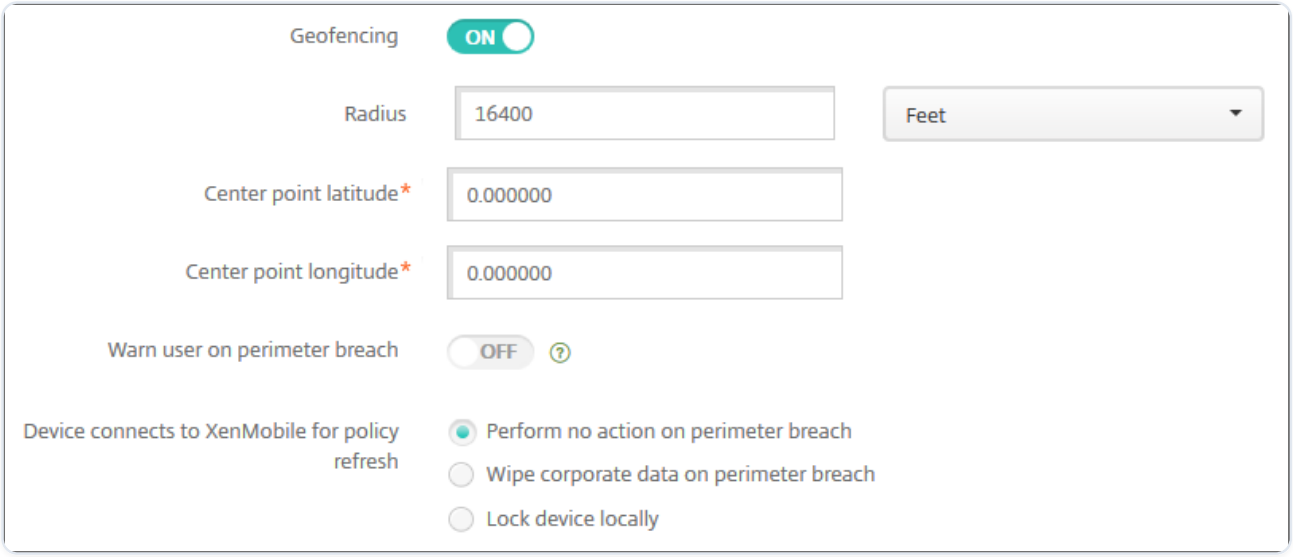
- 54–54680 码
- 1–31 英里

- **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。
- **在突破边界时警告用户：** 选择当用户突破定义的边界时是否发出警告消息。默认设置为“**关**”。显示警告消息不需要连接到 XenMobile。
- **在突破边界时擦除公司数据：** 选择当用户突破边界时是否擦除其设备。默认设置为“**关**”。启用此选项后，将显示“**本地擦除延迟**”字段。
  - 键入一个数字，然后在列表中单击“**秒**”或“**分钟**”，以设置在从用户设备擦除公司数据之前延迟的时间长度。此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：** 键入一个数字，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。
- **如果位置服务已禁用则报告：** 选择当 GPS 禁用时设备是否向 XenMobile 发送报告。默认设置为“**关**”。
- **地理围栏**



启用地理围栏后，请配置以下设置：

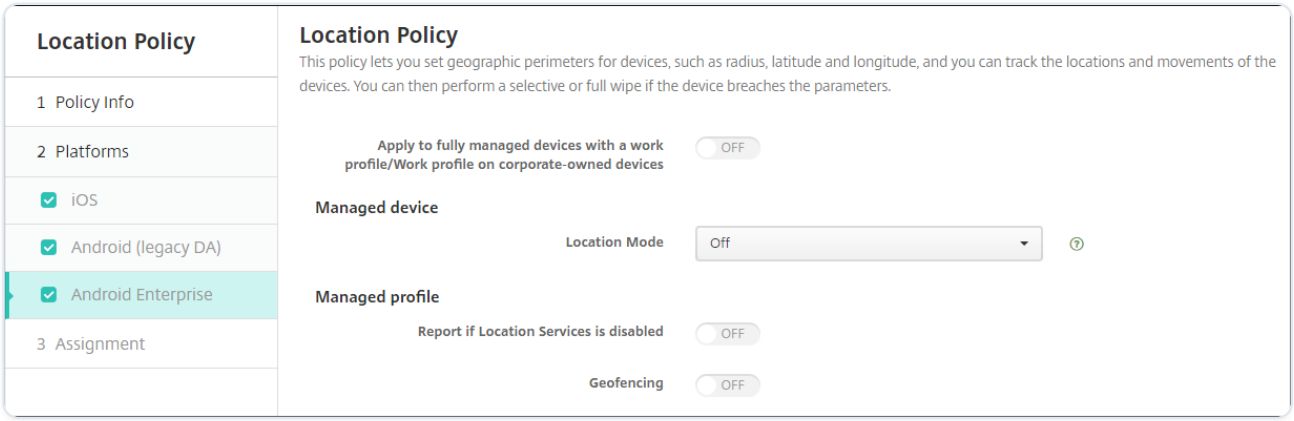
- **半径：** 键入一个数字，然后在列表中单击用于测量半径的单位。默认值为 16,400 英尺。半径的有效值包括：
  - 164–164000 英尺
  - 1–50 公里
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- **中心点纬度：** 输入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- **中心点经度：** 输入经度（例如 122.402952）以定义地理围栏中心点的经度。
- **在突破边界时警告用户：** 选择当用户突破定义的边界时是否发出警告消息。默认设置为**关闭**。显示警告消息不需要连接到 XenMobile。
- **设备连接到 XenMobile 以刷新策略：** 当用户突破边界时，选择以下选项之一：
  - **在突破边界时执行无操作：** 不执行任何操作。此设置为默认值。
  - **在突破边界时擦除公司数据：** 在指定时间长度后擦除公司数据。启用此选项时，将显示**本地擦除延迟**字段。
    - 键入一个数字，然后从列表中单击“秒”或“分钟”，以设置在从用户设备擦除公司数据之前延迟的时间长度。此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：** 在指定时间长度后锁定用户设备。启用此选项时，将显示**锁定延迟字段**。

- 键入一个数字，然后从列表中单击“秒”或“分钟”，以设置在锁定用户设备之前延迟的时间长度。此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。

安卓企业设置

为了使 Android 位置跟踪正常工作，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“**允许位置共享**”设置
- 连接调度（建议使用 Firebase Cloud Messaging）



应用于具有工作资料的完全托管设备

对于具有工作资料的完全托管设备，仅位置模式设置可用。

- **应用于具有工作资料的完全托管设备/公司拥有的设备上的工作资料：** 允许您为具有工作资料的完全托管设备配置位置模式。启用此设置后，请为工作资料配置位置模式设置：
  - **如果位置服务已禁用则报告：** 选择当用户关闭 GPS 时设备是否向 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“**应用于具有工作资料的完全托管设备/公司拥有的设备上的工作资料**”关闭时，设置将应用于托管设备和工作资料，如以下部分所示。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“省电”时，才能使用“**定位**”安全操作。默认值为“高精度”。
  - **高精度：** 启用所有位置检测方法，包括 GPS、网络和其他传感器。

  - **仅传感器：** 仅启用 GPS 和其他传感器。
  - **省电模式：** 仅启用网络位置提供程序。
  - **关闭：** 禁用位置检测。

- **地理围栏：**

地理围栏 Android Enterprise 图像(/en-us/xenmobile/server/media/device-policy-location-android-enterprise-geofencing.png)

启用**地理围栏**时，请配置以下设置：

- **轮询间隔：** 输入一个数字，然后单击**分钟**、**小时**或**天**，以设置 XenMobile Server 尝试确定设备位置的频率。有效值为 1–1440 分钟、1–24 小时或任意天数。默认值为**10 分钟**。将此值设置为小于 10 分钟可能会对设备的电池续航时间产生不利影响。
- **半径：** 输入一个数字，然后单击用于测量半径的单位。默认值为**16400 英尺**（**5000 米**）。半径的有效值包括：
  - 164–164000 英尺
  - 1–50 公里
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- **中心点纬度：** 输入纬度（例如 37.787454）以定义地理围栏中心点的纬度。要查找该值，请转到**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 会在设备**详细信息 > 常规**页面的**安全**下报告设备位置。
- **中心点经度：** 输入经度（例如 122.402952）以定义地理围栏中心点的经度。
- **在突破边界时警告用户：** 选择当用户突破定义的边界时是否发出警告消息。默认值为**关闭**。显示警告消息无需连接到 XenMobile Server。
- **设备连接到 XenMobile Server 以刷新策略：** 选择以下选项之一，用于用户突破边界时：
  - **突破边界时不执行任何操作：** 不执行任何操作。此设置为默认值。
  - **突破边界时擦除公司数据：** 在指定时间长度后擦除公司数据。启用此选项时，将显示**本地擦除延迟**字段。
    - 键入一个数字，然后单击**秒**或**分钟**以设置在从用户设备擦除公司数据之前延迟的时间长度。此延迟使用户有机会返回到允许的位置，然后 XenMobile Server 才会选择性地擦除其设备。默认值为**0 秒**。

- **本地锁定设备：** 在指定时间长度后锁定用户设备。启用此选项时，将显示**锁定延迟**字段。
  - 键入一个数字，然后单击**秒**或**分钟**以设置在锁定用户设备之前延迟的时间长度。此延迟使用户有机会返回到允许的位置，然后 XenMobile Server 才会锁定其设备。默认值为**0 秒**。

托管配置文件

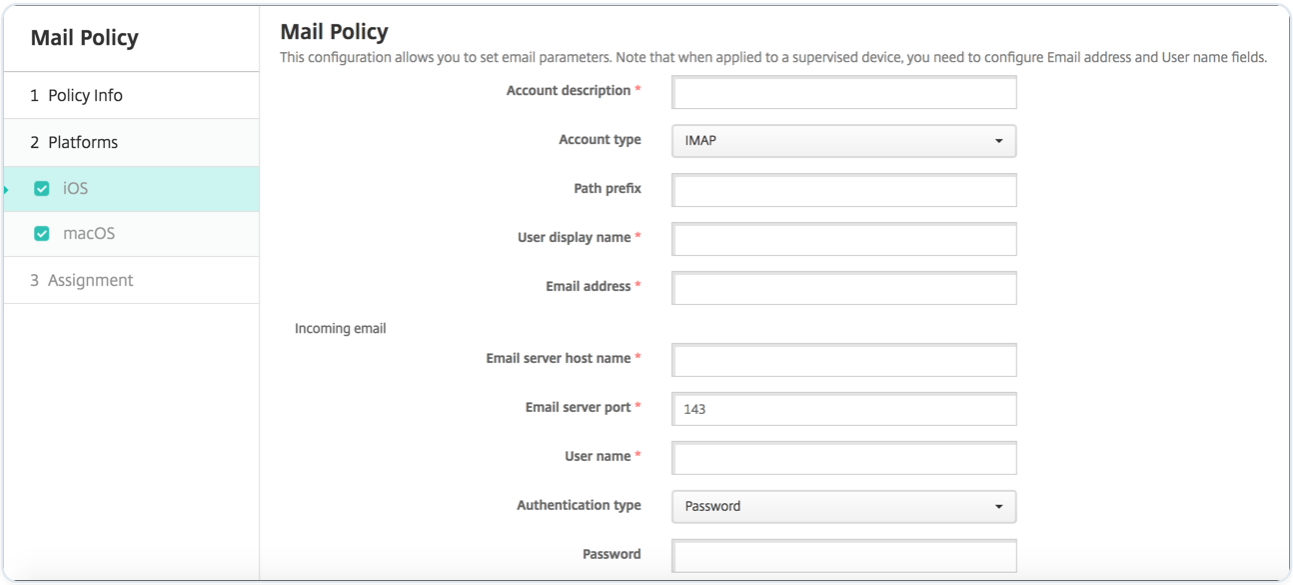
- **报告位置服务是否已禁用：** 选择当用户关闭 GPS 时设备是否向 XenMobile Server 发送报告。默认值为**关闭**。
- **地理围栏：** 请参阅本文中 托管设备 下的设置。

邮件设备策略

您可以在 XenMobile® 中添加邮件设备策略，以在 iOS 或 macOS 设备上配置电子邮件帐户。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 和 macOS 设置



- **帐户描述：** 键入在“邮件”和“设置”应用中显示的帐户描述。此字段为必填项。
- **帐户类型：** 选择 **IMAP** 或 **POP** 以选择用于用户帐户的协议。默认值为 **IMAP**。当您选择 **POP** 时，以下 **路径** 前缀选项将消失。
- **路径前缀：** 键入 **INBOX** 或您的 IMAP 邮件帐户路径前缀。此字段为必填项。
- **用户显示名称：** 键入用于邮件和其他用途的完整用户名称。此字段为必填项。
- **电子邮件地址：** 键入帐户的完整电子邮件地址。此字段为必填项。
- **传入电子邮件设置**

- **电子邮件服务器主机名：** 键入传入邮件服务器主机名或 IP 地址。此字段为必填项。
- **电子邮件服务器端口：** 键入传入邮件服务器端口号。默认值为 **143**。此字段为必填项。
- **用户名：** 键入电子邮件帐户的用户名。此名称通常与 @ 字符之前的电子邮件地址相同。此字段为必填项。
- **身份验证类型：** 选择要使用的身份验证类型。默认值为 **密码**。当选择 **无** 时，以下 **密码** 字段将消失。
- **密码：** 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：** 键入传出邮件服务器主机名或 IP 地址。此字段为必填项。
  - **电子邮件服务器端口：** 键入传出邮件服务器端口号。如果未输入端口号，则使用给定协议的默认端口。
  - **用户名：** 键入电子邮件帐户的用户名。此名称通常与 @ 字符之前的电子邮件地址相同。此字段为必填项。
  - **身份验证类型：** 选择要使用的身份验证类型。默认值为“**密码**”。
  - **密码：** 键入传出邮件服务器的可选密码。
  - **传出密码与传入密码相同：** 选择传入和传出密码是否相同。默认值为“**关**”，表示密码不同。
  - **使用 SSL：** 选择传出邮件服务器是否使用安全套接字层身份验证。默认值为“**关**”。

- **策略**
  - **授权在帐户之间移动电子邮件：** 选择是否允许用户将电子邮件从此帐户移动到另一个帐户，以及从其他帐户转发和回复。默认值为“**关**”。
  - **仅从邮件应用发送电子邮件：** 选择是否将用户限制为仅使用 iOS 邮件应用发送电子邮件。
  - **禁用邮件最近同步：** 选择是否阻止用户同步最近的地址。默认值为“**关**”。此选项仅适用于 iOS 6.0 及更高版本。
  - **允许 Mail Drop：** 选择是否允许运行 iOS 9.2 及更高版本的设备使用 Apple Mail Drop。默认值为“**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，将显示以下字段。
    - **签名身份凭据：** 选择要使用的签名凭据。

    - **S/MIME 签名用户可覆盖：** 如果设置为“**开**”，用户可以在其设备设置中打开和关闭 S/MIME 签名。默认值为“**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，将显示以下字段。
    - **加密身份凭据：** 选择要使用的加密凭据。
    - **启用每条消息 S/MIME 开关：** 设置为“**开**”时，会向用户显示一个选项，用于在他们撰写的每条消息中打开或关闭 S/MIME 加密。默认值为“**关**”。
    - **S/MIME 默认加密用户可覆盖：** 如果设置为“**开**”，用户可以在其设备设置中选择 S/MIME 是否默认开启。默认值为“**关**”。此选项适用于 iOS 12.0 及更高版本。
    - **S/MIME 加密证书 UUID 用户可覆盖：** 如果设置为“**开**”，用户可以在其设备设置中打开和关闭 S/MIME 加密身份和加密。默认值为“**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，您可以将此设置配置为在“**选定日期**”或“**直到删除的持续时间（小时）**”删除策略。
  - **允许用户删除策略：** 允许用户“**始终**”删除邮件策略，仅在“**需要密码**”时删除，或“**从不**”删除。
  - **配置文件范围：** 仅适用于 macOS，选择策略是应用于每个“**用户**”级别还是应用于整个“**系统**”。

托管配置策略

托管配置设备策略控制各种应用程序配置选项和应用程序限制。应用程序开发人员定义了应用程序可用的选项和工具提示。如果工具提示提到使用“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 开发者网站上）和 宏。

应用程序配置设置可以包括以下各项：

- 应用程序电子邮件设置
- 允许或阻止 Web 浏览器的 URL
- 通过蜂窝连接或仅通过 Wi-Fi 连接控制应用程序内容同步的选项

有关应用程序显示设置的信息，请联系应用程序开发人员。

必备条件

- 完成 Google 上的 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 将应用程序添加到 XenMobile。

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅 设备策略。

每应用 VPN 的要求

要为 AE 创建每应用 VPN，除了配置托管配置策略之外，还需要执行额外的步骤。此外，您必须验证是否满足以下先决条件：

- 本地 Citrix 网关
- 设备上安装了以下应用程序：
  - Citrix 单点登录
  - Citrix 安全中心™

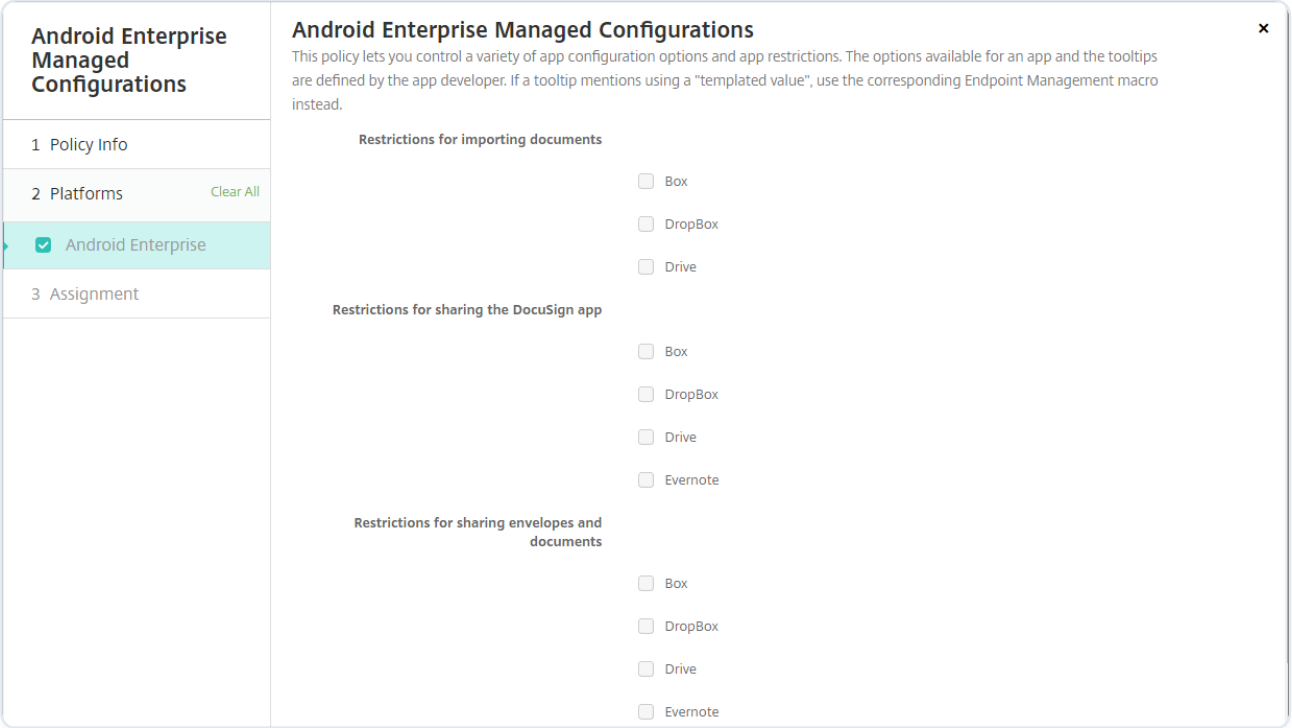
配置AE设备的每应用VPN的通用工作流程如下：

1. 按照本文所述配置VPN配置文件。
2. 配置Citrix ADC以接受来自每应用VPN的流量。有关详细信息，请参阅Citrix Gateway上的完整VPN设置。

安卓企业设置

选择添加托管配置设备策略后，将出现选择应用程序的提示。如果XenMobile®中没有添加Android Enterprise应用程序，则无法继续。

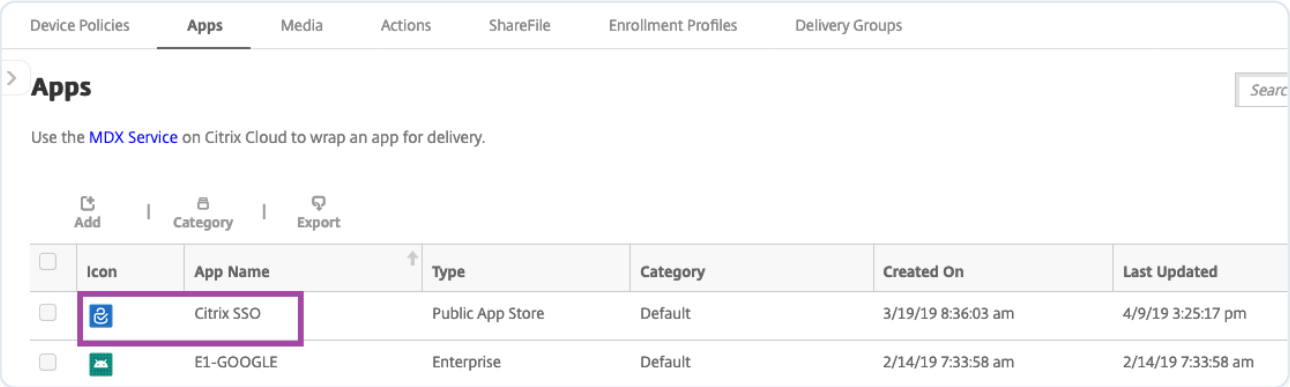
选择应用程序后，配置策略设置。这些设置特定于每个应用程序。



为Android Enterprise配置VPN配置文件

使用Citrix SSO应用程序和托管配置设备策略，使VPN配置文件可用于Android Enterprise设备。

首先，将Citrix SSO作为Google Play商店应用程序添加到XenMobile控制台。请参阅添加公共应用商店应用程序。



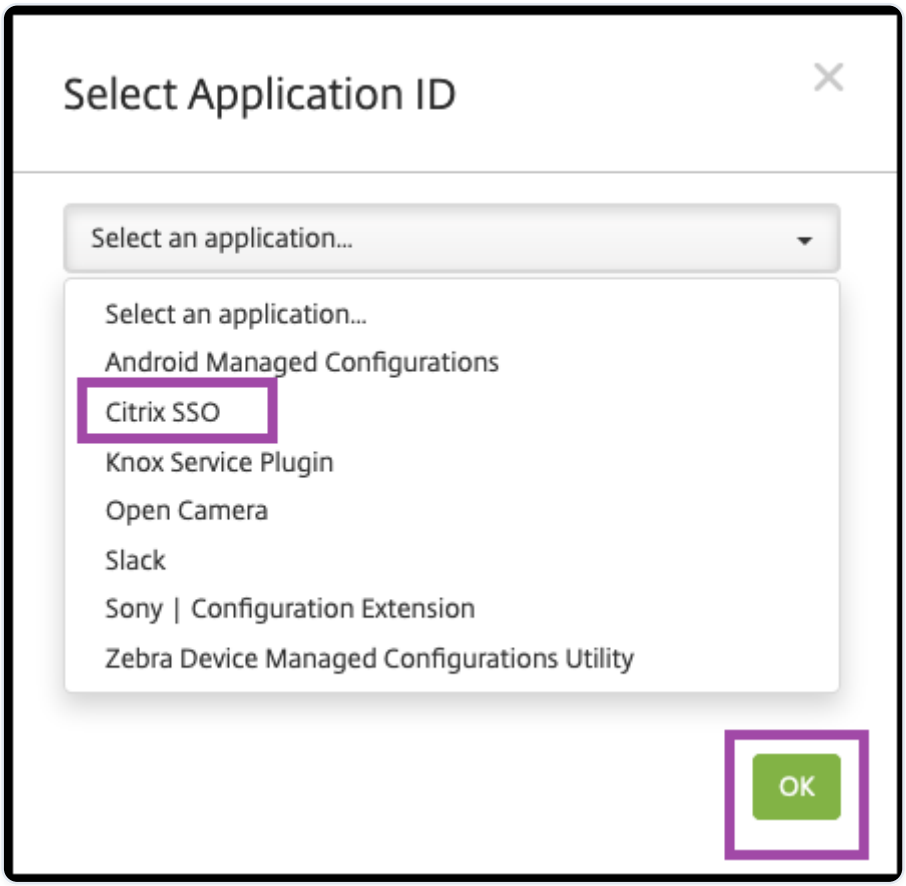
为Citrix SSO创建Android Enterprise托管配置

配置Citrix SSO的托管配置设备策略以创建VPN配置文件。已安装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。

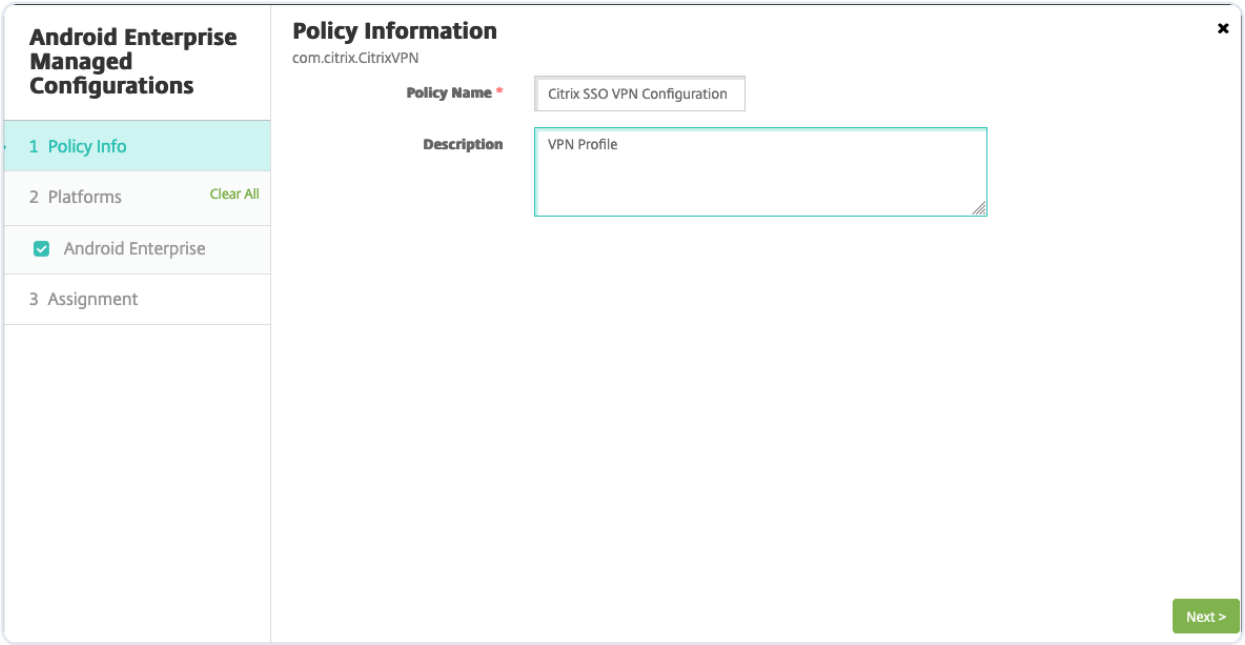
您需要您的 Citrix Gateway FQDN 和端口。

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 **托管配置**。

3. 当出现 **选择应用程序 ID** 窗口时，从列表中选择 **Citrix SSO**，然后单击 **确定**。

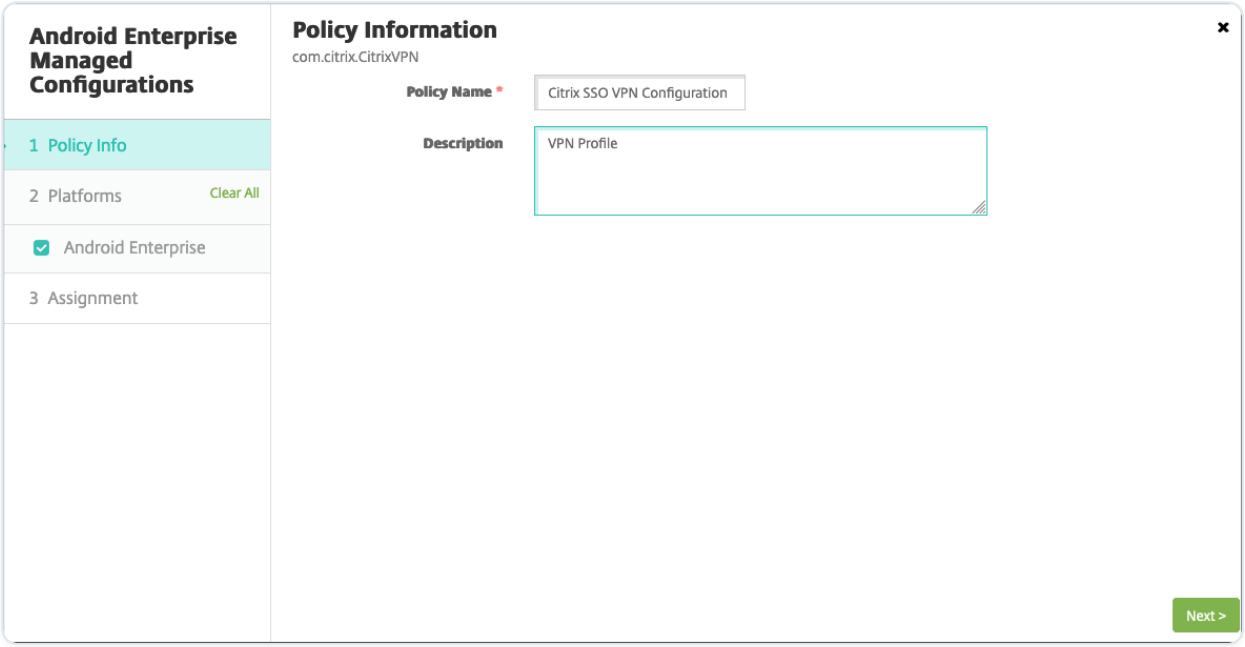


4. 为您的 Citrix SSO VPN 配置键入名称和描述。单击 **下一步**。

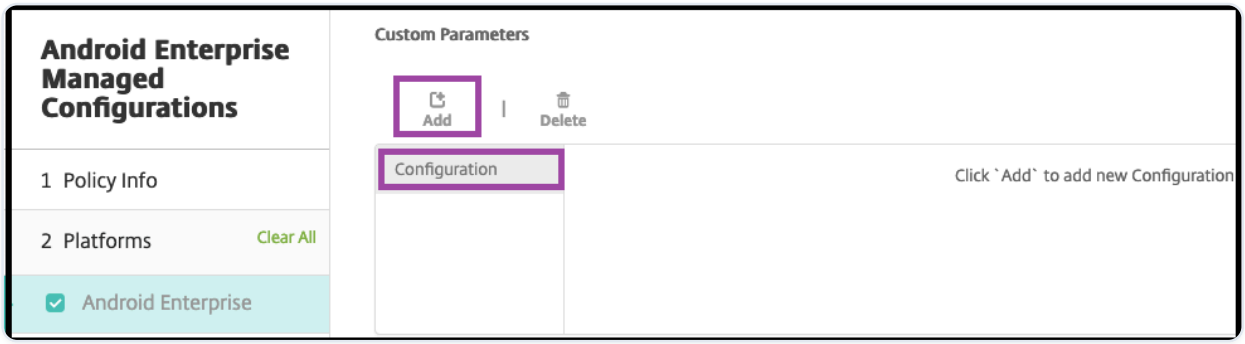


5. 配置 VPN 配置文件参数。

- **VPN 配置文件名称。** 为 VPN 配置文件键入名称。如果您要创建多个 VPN 配置文件，请为每个配置文件使用唯一的名称。如果您未提供名称，则 **服务器地址** 字段中输入的地址将用作 VPN 配置文件名称。
- **服务器地址(*)。** 键入您的 Citrix Gateway FQDN。如果您的 Citrix Gateway 端口不是 443，请同时键入您的端口。使用 URL 格式。例如，`https://gateway.mycompany.com:8443`。
- **用户名（可选）。** 提供最终用户用于向 Citrix Gateway 进行身份验证的用户名。您可以在此字段中使用 XenMobile 宏 {user.username}。（请参阅 宏。）如果您未提供用户名，则用户在连接到 Citrix Gateway 时会收到提供用户名的提示。
- **密码（可选）。** 提供最终用户用于向 Citrix Gateway 进行身份验证的密码。如果您未提供密码，则用户在连接到 Citrix Gateway 时会收到提供密码的提示。
- **证书别名（可选）。** 键入证书别名。证书别名使应用程序更容易访问证书。当相同的证书别名与凭据设备策略一起使用时，应用程序会检索证书并对 VPN 进行身份验证，而无需用户执行任何操作。
- **每应用 VPN 类型（可选）。** 如果您正在使用每应用 VPN 来限制哪些应用程序使用此 VPN，则可以配置此设置。如果选择 **允许**，则 **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将路由到 VPN 外部。如果选择 **不允许**，则 **PerAppVPN 应用程序列表** 中列出的应用程序包名称的网络流量将路由到 VPN 外部。所有其他应用程序的网络流量将通过 VPN 路由。默认值为 **允许**。
- **PerAppVPN 应用程序列表。** 一个应用程序列表，其流量在 VPN 上被允许或阻止，具体取决于 **每应用 VPN 类型** 的值。列出用逗号或分号分隔的应用程序包名称。应用程序包名称区分大小写，并且必须与它们在 Google Play 商店中显示的名称完全一致。此列表是可选的。将此列表留空以配置设备范围的 VPN。
- **默认 VPN 配置文件。** 键入当用户在 Citrix SSO 应用程序的用户界面中点击连接开关而不是点击特定配置文件时要使用的 VPN 配置文件的名称。如果此字段留空，则使用主配置文件进行连接。如果只配置了一个配置文件，则将其标记为默认配置文件。对于始终开启的 VPN，此字段必须设置为用于建立始终开启的 VPN 的 VPN 配置文件的名称。
- **禁用用户配置文件。** 如果此设置为“开”，用户无法在其设备上创建自己的 VPN。如果此设置为“关”，用户可以在其设备上创建自己的 VPN。默认值为“关”。
- **阻止不受信任的服务器。** 当为 Citrix Gateway 使用自签名证书时，或者当颁发 Citrix Gateway 证书的 CA 的根证书不在系统 CA 列表中时，此设置为“关”。如果此设置为“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”。

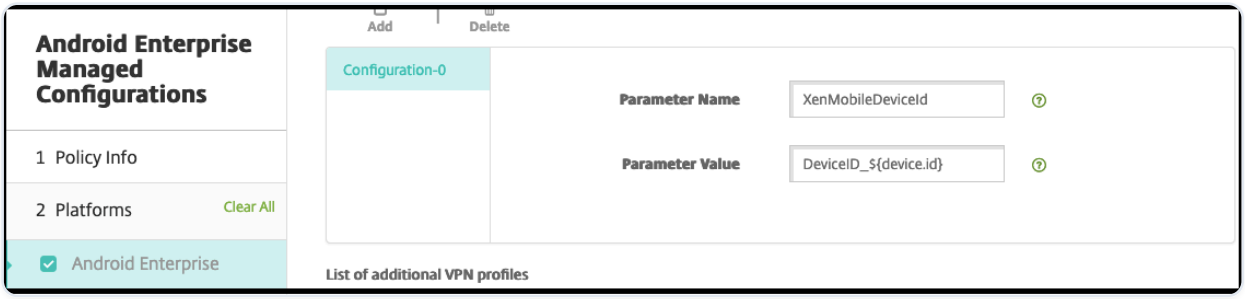


6. （可选）创建自定义参数。支持自定义参数 **XenMobileDeviceId** 和 **UserAgent**。选择当前的 VPN 配置，然后单击“**添加**”。



a. 创建自定义参数：

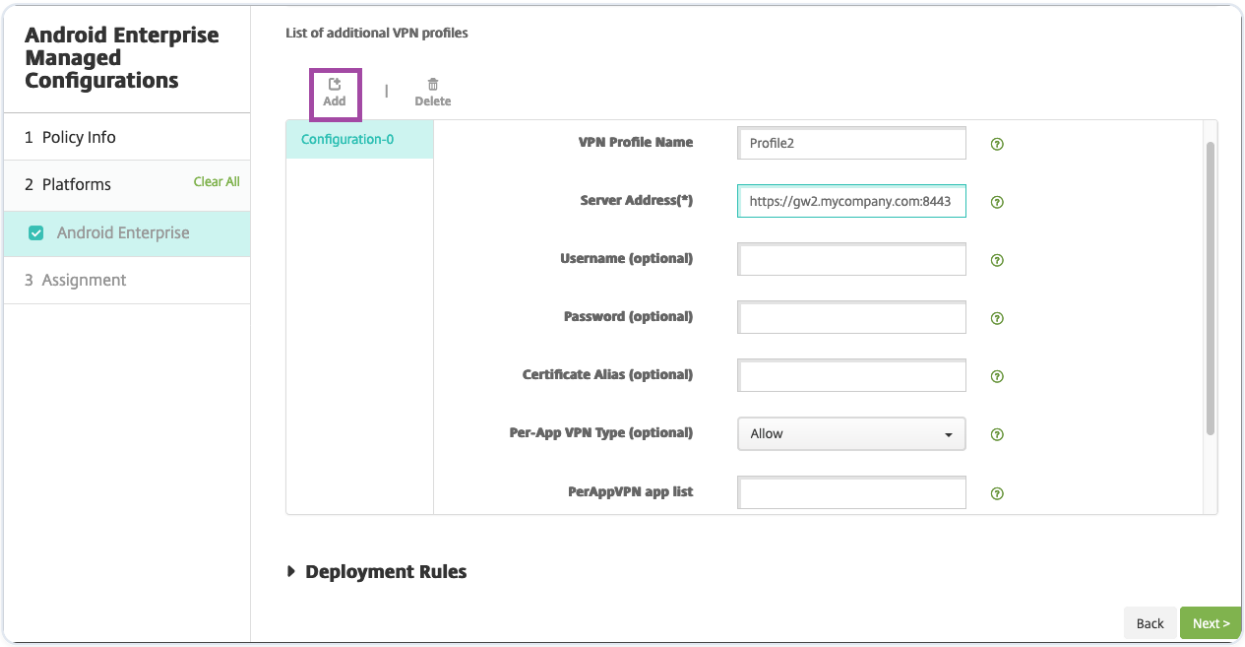
- **参数名称。** 键入 **XenMobileDeviceId**。此字段是用于基于 XenMobile 中的设备注册进行网络访问检查的设备 ID。如果 XenMobile 注册并管理设备，则允许 VPN 连接。否则，在建立 VPN 时将拒绝身份验证。
- **参数值** 为了让 XenMobile 确定设备的注册和管理状态，XenMobileDeviceID 的值设置为 `DeviceID_${device.id}`。



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**。此文本将附加到 User-Agent HTTP 标头，用于对 Citrix Gateway 进行额外检查。此文本的值在 Citrix SSO 应用程序与 Citrix Gateway 通信时附加到 User-Agent HTTP 标头。
- **参数值。** 键入要附加到 User-Agent HTTP 标头的文本。此文本必须符合 HTTP User-Agent 规范。

7. （可选）创建更多 VPN 配置文件配置。在配置列表下单击“**添加**”。新配置将出现在列表中。选择新配置并重复步骤 5，（可选）重复步骤 6。



8. 创建完所有所需的 VPN 配置文件后，单击**下一步**。
9. 为 Citrix SSO 配置此托管配置的部署规则。
10. 单击**保存**。

此 Citrix SSO 托管配置现在显示在您配置的设备策略列表中。

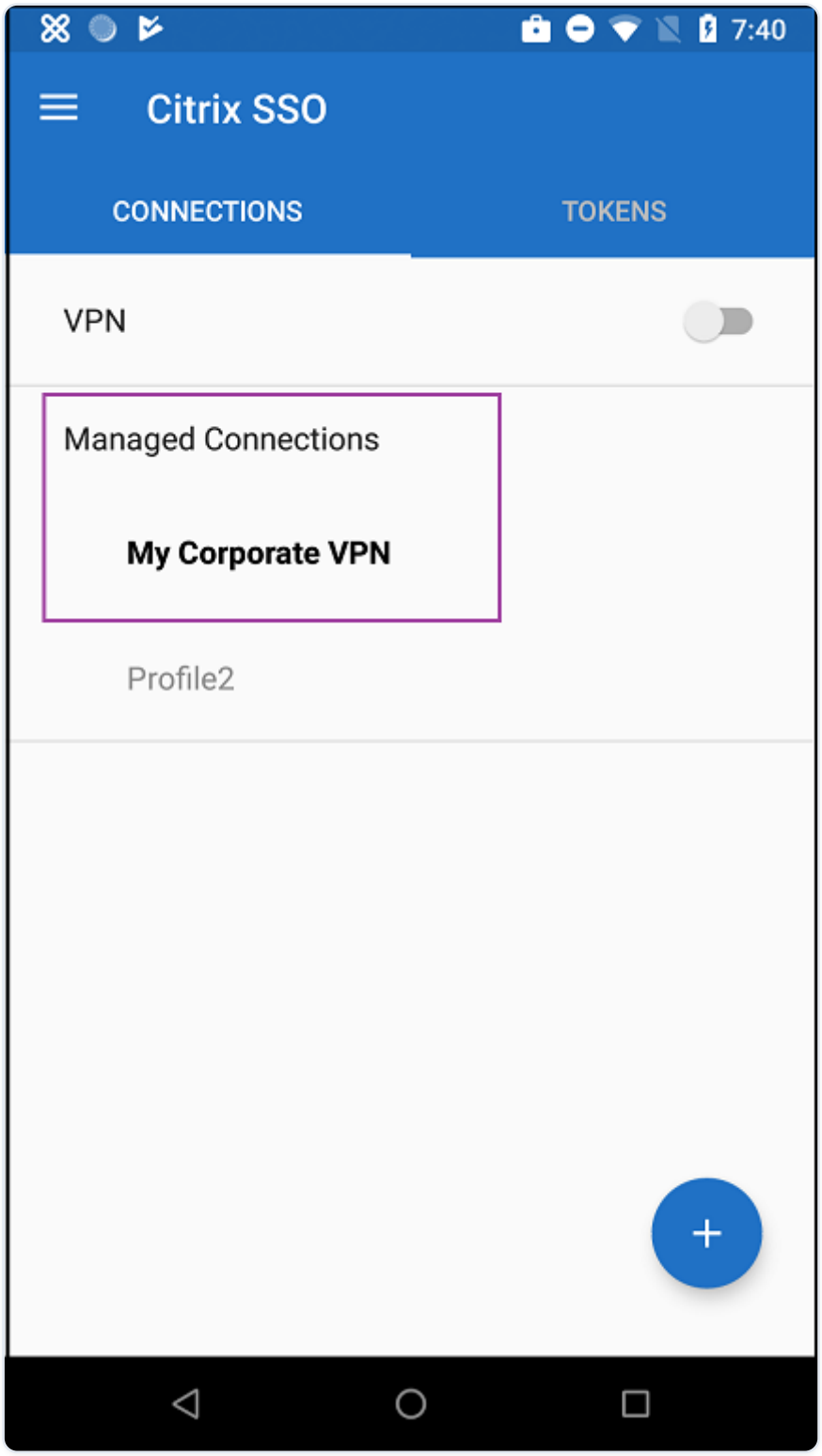
要为配置的 VPN 配置文件启用始终开启，请设置 XenMobile 选项设备策略。

> **注意：** Android Enterprise 的始终开启 VPN 需要 Citrix Secure Hub 19.5.5 或更高版本。

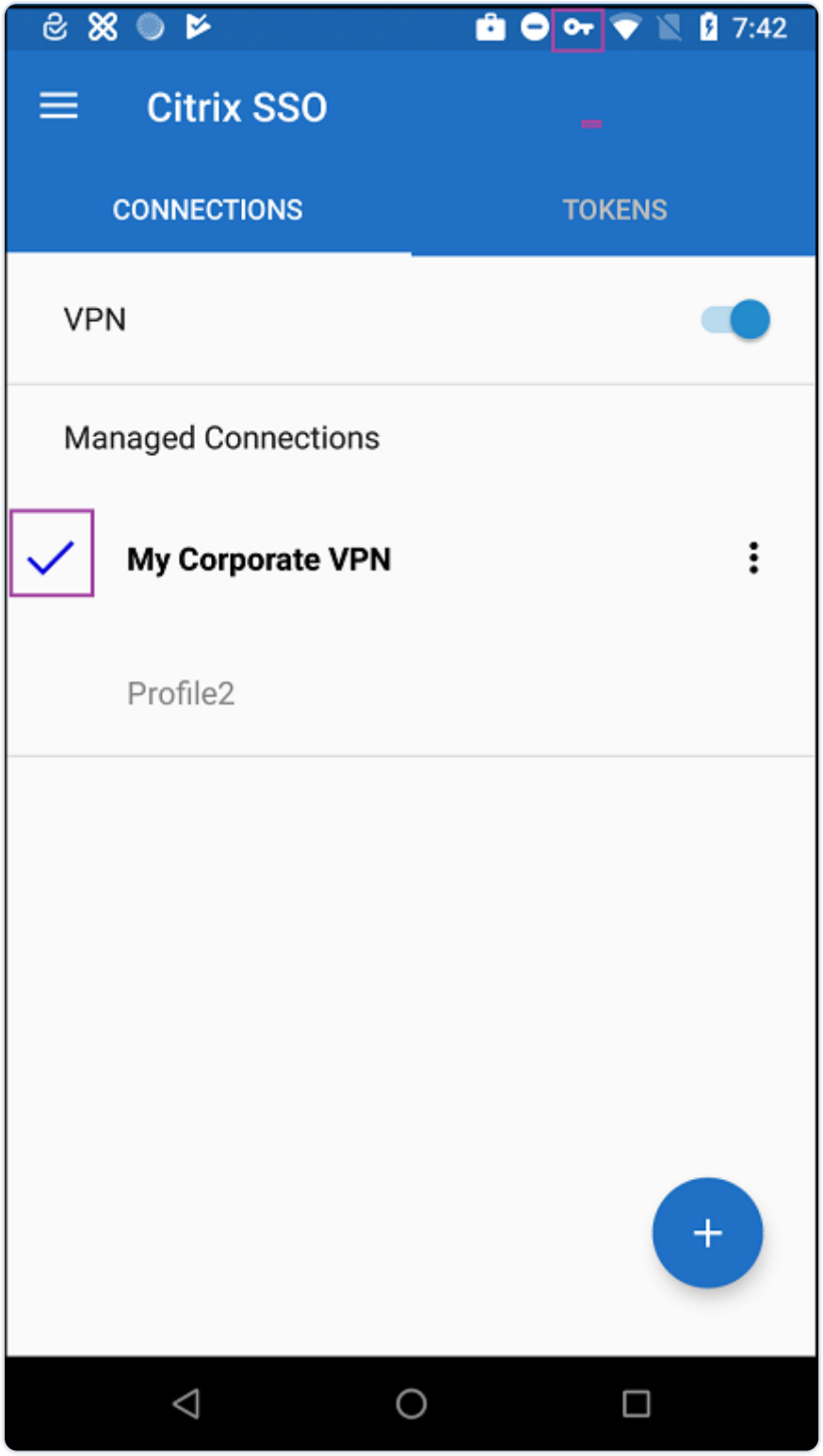
从设备访问 VPN 配置文件

要访问您创建的 VPN 配置文件，Android Enterprise 用户需从 Google Play 商店安装 Citrix SSO。

您配置的 VPN 配置文件显示在应用程序的**托管连接**区域中。用户点击 VPN 配置文件以使用该 VPN 配置文件进行连接。



用户完成身份验证并连接后，VPN 配置文件旁边会出现一个复选标记。钥匙图标表示 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 网站。

XenMobile 支持 Zebra OEMConfig 9.2 及更高版本。有关在设备上安装 Zebra OEMConfig 的系统要求信息，请参阅 Zebra Technologies 网站上的 OEMConfig 设置。

首先，将 Zebra OEMConfig 应用程序作为 Google Play 商店应用程序添加到 XenMobile 控制台。请参阅 添加公共应用商店应用程序。

为 Zebra OEMConfig 应用程序创建 Android Enterprise 托管配置

为 Zebra OEMConfig 应用程序配置托管配置设备策略。该策略适用于已安装 Zebra OEMConfig 应用程序并已部署该策略的 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 **托管配置**。
3. 当出现 **选择应用程序 ID** 窗口时，从列表中选择 **ZebraOEMConfig powered by MX**，然后单击 **确定**。
4. 为您的 Zebra OEMConfig 配置键入名称和描述。单击 **下一步**。
5. 为 Zebra OEMConfig 配置键入名称。
6. 配置可用参数。例如：
   - 要禁用设备前置摄像头，请选择 **摄像头配置** 并将 **前置摄像头使用** 设置为 **关闭**。
   - 要更改设备时间格式，请选择 **时钟配置** 并将 **时间格式** 设置为 **12**（表示 12 小时制）或 **24**（表示 24 小时制）。

有关所有可用配置的列表和说明，请参阅 Zebra Technologies 网站上的 Zebra 托管配置。

1. （可选）创建更多 Zebra OEMConfig 配置。在配置列表下单击 **添加**。新配置将出现在列表中。选择新配置并配置参数。
2. 当您创建了所有所需的 Zebra OEMConfig 配置后，单击**下一步**。
3. 配置此 Zebra OEMConfig 托管配置的部署规则。
4. 单击**保存**。

托管域设备策略

您可以定义适用于电子邮件和 Safari 浏览器的托管域。托管域通过控制哪些应用程序可以打开使用 Safari 从域下载的文档来帮助您保护企业数据。

对于 iOS 8 及更高版本的受监督设备，您可以指定 URL 或子域来控制用户如何从浏览器打开文档、附件和下载内容。对于 iOS 9.3 及更高版本的受监督设备，您可以指定用户可以在 Safari 中保存密码的 URL。

有关将 iOS 设备设置为监督模式的步骤，请参阅 使用 Apple Configurator 将 iOS 设备置于监督模式。

当用户向其域不在托管电子邮件域列表中的收件人发送电子邮件时，邮件会在用户的设备上被标记，以警告他们正在向企业域之外的人发送邮件。

对于文档、附件或下载等项目：当用户使用 Safari 从托管 Web 域列表中的 Web 域打开项目时，相应的企业应用程序会打开该项目。如果项目不是来自托管 Web 域列表中的 Web 域，则用户无法使用企业应用程序打开该项目。他们必须使用个人、非托管应用程序。

对于受监督设备，即使您未指定 Safari 密码自动填充域：如果设备配置为临时多用户，则用户无法保存密码。但是，如果设备未配置为临时多用户，则用户可以保存所有密码。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

iOS 设置

要指定域：

格式	说明
`example.com`	将 `example.com` 下的任何路径视为托管，但 `site.example.com/` 除外。
`foo.example.com`	将 `foo.example.com` 下的任何路径视为托管，但 `example.com/` 或 `bar.example.com/` 除外。
`*.example.com`	将 `foo.example.com` 或 `bar.example.com` 下的任何路径视为托管，但 `example.com/` 除外。
`example.com/sub`	将 `example.com/sub` 及其下的任何路径视为托管，但 `example.com/` 除外。
`foo.example.com/sub`	将 `foo.example.com/sub` 下的任何路径视为托管，但 `example.com`、`example.com/sub`、`foo.example.com/` 或 `bar.example.com/sub` 除外。
`*.example.com/sub`	将 `foo.example.com/sub` 或 `bar.example.com/sub` 下的任何路径视为托

格式	说明
	管，但 `example.com` 或 `foo.example.com/` 除外。

规则：

- 比较域时，URL 中开头的“www.”和末尾的斜杠将被忽略。
- 如果条目包含端口号，则只有指定该端口号的地址才被视为托管。否则，只有标准端口被视为托管（http 为端口 80，https 为端口 443）。例如，模式 `*.example.com:8080` 匹配 `https://site.example.com:8080/page.html`，但不匹配 `https://site.example.com/page.html`；而模式 `*.example.com` 匹配 `https://site.example.com/page.html` 和 `https://site.example.com/page.html`，但不匹配 `https://site.example.com:8080/page.html`。
- 托管的 Safari Web 域定义是累积的。所有托管的 Safari Web 域负载定义的模式都用于匹配 URL 请求。

设置：

- **托管域**
  - **未标记的电子邮件域**：对于要包含在列表中的每个电子邮件域，单击“**添加**”，然后执行以下操作：
    - **托管电子邮件域**：键入电子邮件域。
    - 单击“**保存**”以保存电子邮件域，或单击“**取消**”以不保存电子邮件域。
  - **托管 Safari Web 域**：对于要包含在列表中的每个 Web 域，单击“**添加**”，然后执行以下操作：
    - **托管 Web 域**：键入 Web 域。
    - 单击“**保存**”以保存 Web 域，或单击“**取消**”以不保存 Web 域。
  - **Safari 密码自动填充域**：对于要包含在列表中的每个自动填充域，单击“**添加**”，然后执行以下操作：
    - **Safari 密码自动填充域**：键入自动填充域。
    - 单击“**保存**”以保存自动填充域，或单击“**取消**”以不保存自动填充域。
- **策略设置**

- **删除策略**：选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**直到删除的持续时间（小时）**”
  - **选择日期**：单击日历以选择要删除的具体日期。
  - **直到删除的持续时间（小时）**：键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

最大常驻用户设备策略

最大常驻用户设备策略适用于运行 iOS (iPadOS) 的共享设备。有关共享 iPad 的更多信息，请参阅与 Apple Education 功能集成。

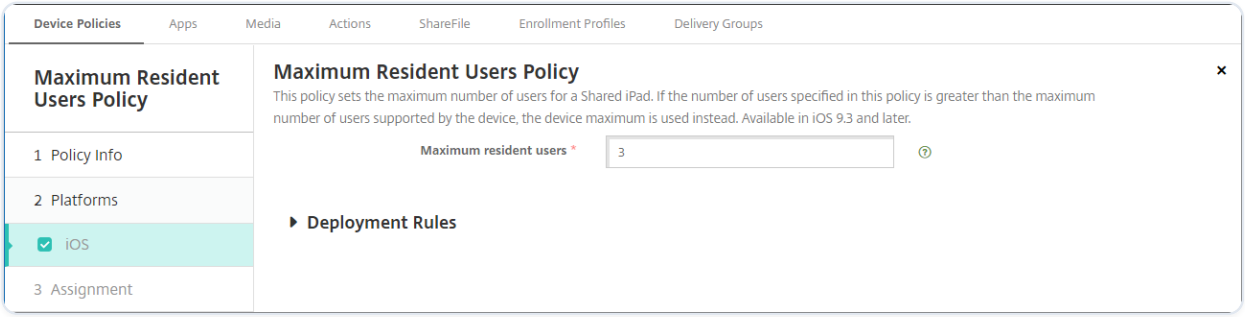
此策略必须在 iPad 在设置助理期间处于“等待配置”阶段时部署。Apple 不允许在共享 iPad 注册后部署此策略。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

iOS 设置

- **最大常驻用户数**： 共享 iPad 的最大用户数。如果此策略中指定的用户数大于设备支持的最大用户数，Citrix Endpoint Management 将使用设备的最大值。默认值为 **5** 个用户。

  Apple 建议您将最大常驻用户数的值保持在尽可能低的水平。较低的值可以最大程度地为每个用户提供 iPad 存储空间。此外，较低的值可以最大程度地减少与 iCloud 的通信，并提供更快的登录体验。有关 Apple 如何处理 iPad 上的共享存储的信息，请参阅 `<https://developer.apple.com/education/shared-ipad/>`。



MDM 选项设备策略

您可以在 XenMobile 中创建设备策略，以管理受监督的 iOS 7.0 及更高版本手机设备上的“查找我的手机/iPad 激活锁”。有关将 iOS 设备设置为监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于监督模式。

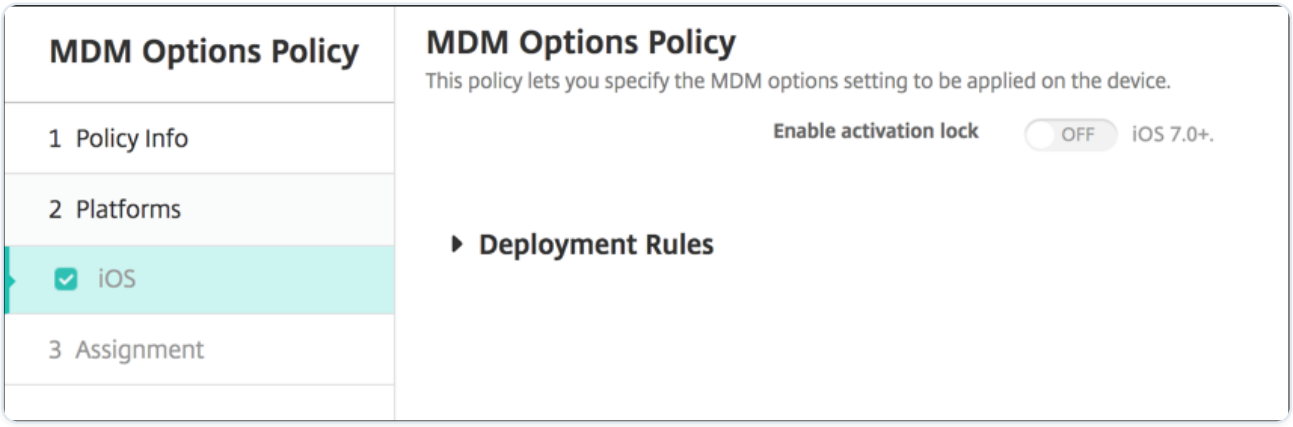
激活锁是“查找我的 iPhone/iPad”的一项功能，可防止丢失或被盗的受监督设备重新激活。激活锁要求用户提供 Apple ID 和密码，然后才能关闭“查找我的 iPhone/iPad”、抹掉设备或重新激活设备。对于贵组织拥有的设备，绕过激活锁是必要的，例如，用于重置或重新分配设备。

要启用激活锁，请配置并部署 XenMobile® MDM 选项设备策略。然后，您可以从 XenMobile 控制台管理设备，而无需用户的 Apple 凭据。要绕过激活锁的 Apple 凭据要求，请从 XenMobile 控制台发出“激活锁绕过”安全操作。

例如，如果用户归还了丢失的手机，或者在完全擦除之前或之后设置设备：当手机提示输入 iTunes 帐户凭据时，您可以通过从 XenMobile 控制台发出“激活锁绕过”安全操作来绕过该步骤。

要添加或配置此策略，请转至**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：** 选择是否在您部署此策略的设备上启用激活锁。默认值为**关闭**。

在通过部署 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**。激活锁绕过允许您在设备激活之前从受监督的设备中移除激活锁，而无需知道设备用户的 Apple ID 和密码。您可以在完全擦除之前或之后向设备发送激活锁绕过。有关详细信息，请参阅安全操作文章中的绕过 iOS 激活锁。

组织信息设备策略

您可以在 XenMobile® 中添加设备策略，以指定您组织的详细信息，用于从 XenMobile 推送到 iOS 设备的警报消息。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。

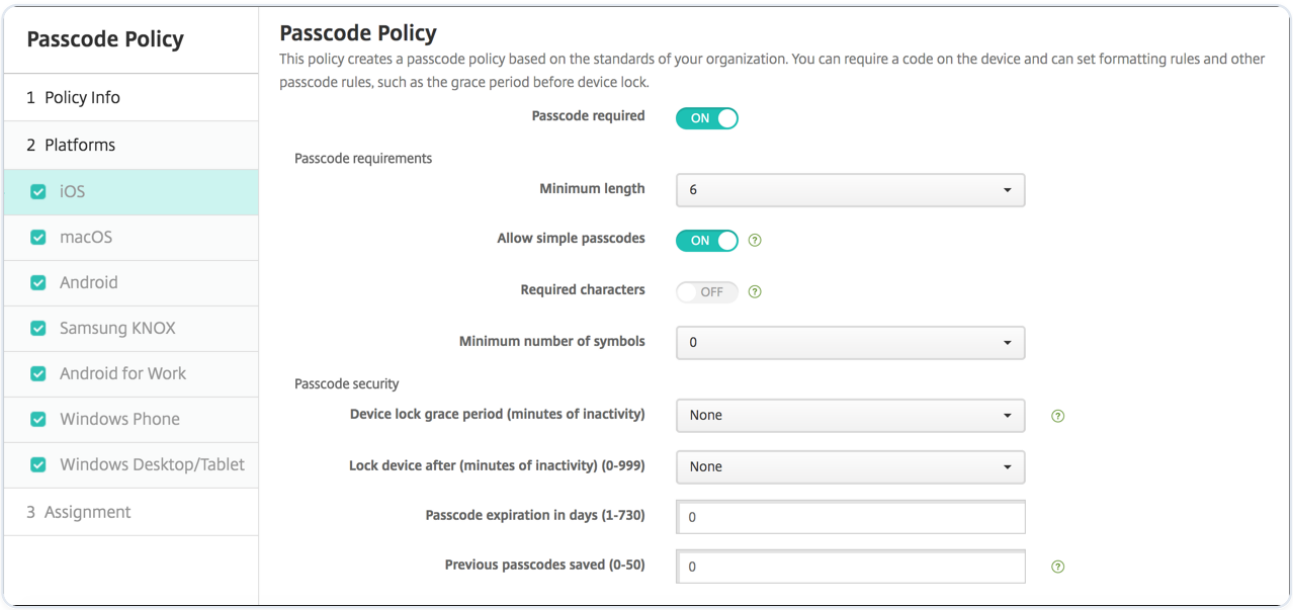
- **电话：** 键入组织的支持电话号码。
- **电子邮件：** 键入支持电子邮件地址。
- **魔术：** 键入描述组织所管理服务的词语或短语。

密码设备策略

您可以在 XenMobile 中根据组织的标准创建密码策略。您可以要求用户设备使用密码，并可以设置各种格式和密码规则。您可以为 iOS、macOS、Android、Samsung Knox、Android Enterprise 和 Windows 桌面/平板电脑创建策略。每个平台都需要一组不同的值，本文将对此进行介绍。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

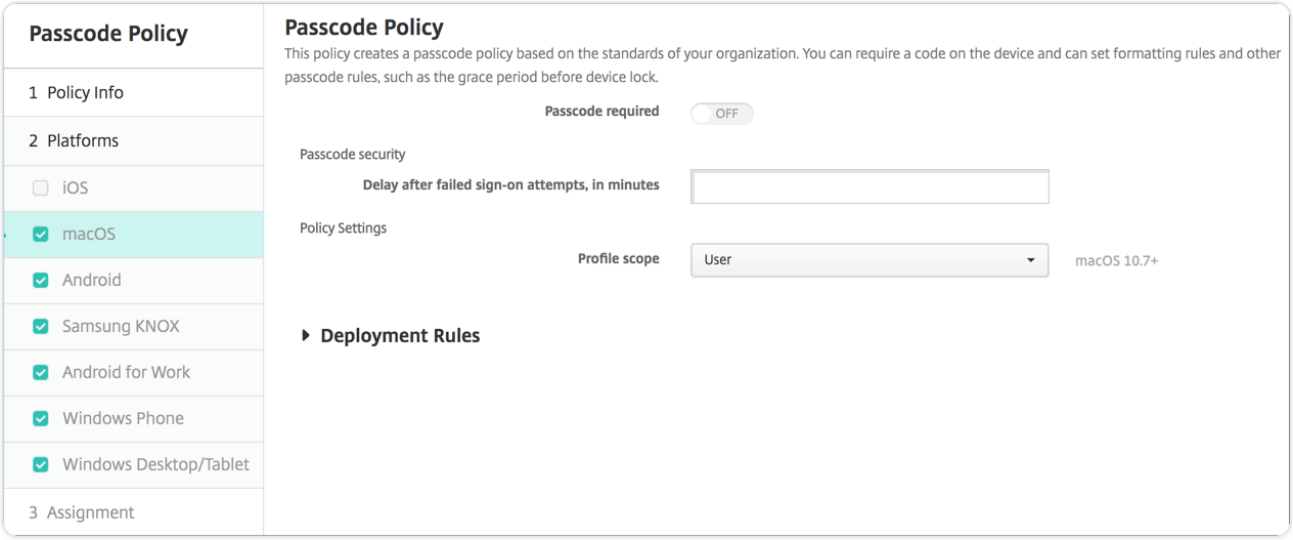
iOS 设置



- **需要密码：** 选择此选项可要求使用密码并显示 iOS 密码设备策略的配置选项。页面将展开，允许您配置密码要求、密码安全和策略设置。
- **密码要求**
  - **最小长度：** 在下拉列表中单击最小密码长度。默认值为 **6**。
  - **允许简单密码：** 选择是否允许简单密码。简单密码是重复或连续的字符集。默认值为 **开**。
  - **所需字符：** 选择是否要求密码至少包含一个字母。默认值为 **关**。
  - **最小符号数：** 在列表中，单击密码必须包含的符号数。默认值为 **0**。
- **密码安全**

- **设备锁定宽限期（不活动分钟数）：** 在列表中，单击用户必须输入密码才能解锁锁定设备之前的时间长度。默认值为 **无**。
- **在此时间后锁定设备（不活动分钟数）：** 在列表中，单击设备在锁定前可以不活动的时间长度。默认值为无。
- **密码过期天数 (1-730)：** 键入密码过期后的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
- **已保存的旧密码 (0-50)：** 键入要保存的已用密码数。用户无法使用此列表中存在的任何密码。有效值为 0–50。默认值为 **0**，这意味着用户可以重复使用密码。
- **最大登录失败尝试次数：** 在列表中，单击用户可以失败的登录尝试次数，超过此次数后设备将被完全擦除。默认值为 **未定义**。

macOS 设置

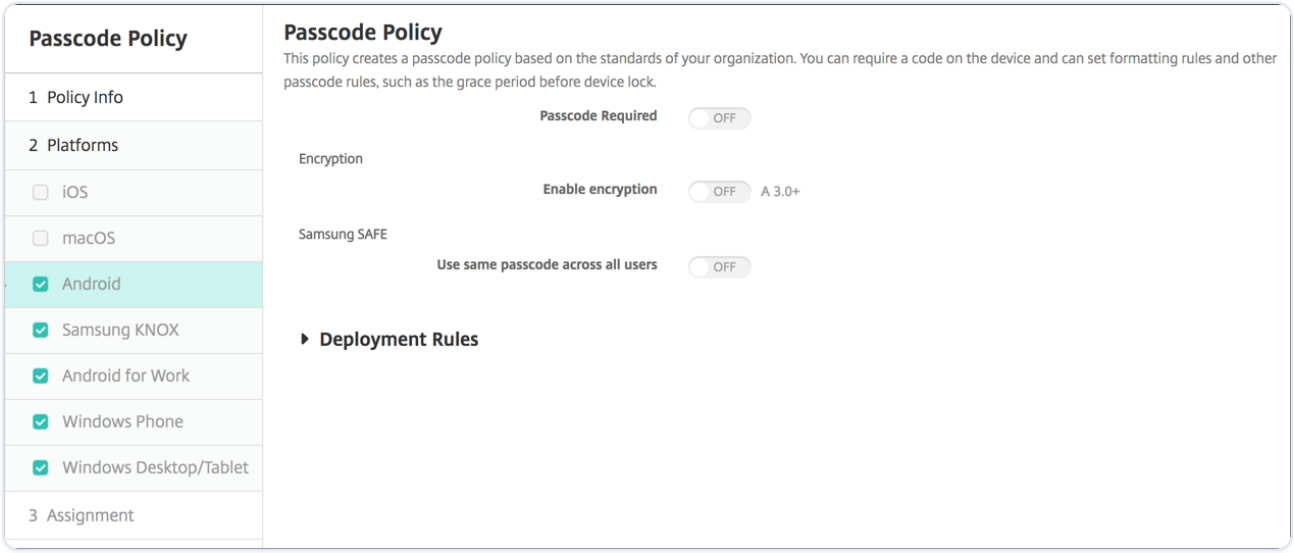


- **需要密码：** 选择此选项以要求密码并显示 iOS 密码设备策略的配置选项。页面将展开，允许您配置密码要求、密码安全和策略设置。
- 如果您未启用 **需要密码**，请在 **登录失败尝试后的延迟（分钟）** 旁边，键入在允许用户重新输入密码之前延迟的分钟数。
- 如果您启用 **需要密码**，请配置以下设置：
- **密码要求**
  - **最小长度：** 在列表中，单击最小密码长度。默认值为 **6**。
  - **允许简单密码：** 选择是否允许简单密码。简单密码是重复或连续的字符集。默认值为 **开**。
  - **所需字符：** 选择是否要求密码至少包含一个字母。默认值为 **关**。
  - **最小符号数：** 在列表中，单击密码必须包含的符号数。默认值为 **0**。
- **密码安全**

- **设备锁定宽限期（不活动分钟数）：** 在列表中，单击用户必须输入密码才能解锁锁定设备之前的时间长度。默认值为 **无**。
- **在（不活动分钟数）后锁定设备：** 在列表中，单击设备在锁定之前可以不活动的时间长度。默认值为 **无**。
- **密码有效期（天，1-730）：** 键入密码的有效期天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
- **已保存的旧密码（0-50）：** 键入要保存的已用密码数。用户无法使用此列表中的任何密码。有效值为 0–50。默认值为 **0**，表示用户可以重复使用密码。
- **最大登录失败尝试次数：** 在列表中，单击用户可以失败登录的次数，超过此次数后设备将被锁定。默认值为 **未定义**。
- **登录失败尝试后的延迟（分钟）：** 键入在允许用户重新输入密码之前延迟的分钟数。
- **强制重置密码：** 用户下次进行身份验证时，必须重置其密码。

- **策略设置**
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**用户**。此选项仅在 macOS 10.7 及更高版本上可用。

Android 设置



> **注意：**

> Android 的默认设置为**关闭**。

- **需要密码：** 选择此选项以要求密码并显示 Android 密码设备策略的配置选项。页面将展开，允许您配置密码要求、密码安全性、加密和 Samsung SAFE 的设置。
- **密码要求**
  - **最小长度：** 在下拉列表中选择最小密码长度。默认值为 6。
  - **生物识别：** 选择是否启用生物识别。如果启用此选项，则“所需字符”字段将被隐藏。默认值为**关闭**。
  - **所需字符：** 在下拉列表中选择**无限制**、**数字和字母**、**仅数字**或**仅字母**，以配置密码的组成方式。默认值为无限制。
  - **高级规则：** 选择是否应用高级密码规则。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**后，从以下每个列表中，单击密码必须包含的每种字符类型的最小数量：
    - **符号：** 符号的最小数量。
    - **字母：** 字母的最小数量。
    - **小写字母：** 小写字母的最小数量。
    - **大写字母：** 大写字母的最小数量。
    - **数字或符号：** 数字或符号的最小数量。
    - **数字：** 数字的最小数量。
- **密码安全性**
  - **设备锁定时间（不活动分钟数）：** 在列表中，单击设备在锁定前可以不活动的时间长度。默认值为**无**
  - **密码过期天数 (1-730)：** 键入密码过期后的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
  - **已保存的以前密码 (0-50)：** 键入要保存的已用密码数量。用户无法使用此列表中找到的任何密码。有效值为 0–50。默认值为 **0**，表示用户可以重复使用密码。
  - **最大登录失败尝试次数：** 在列表中，单击用户可以失败登录的次数，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“**需要密码**”设置如何，此选项都可用。

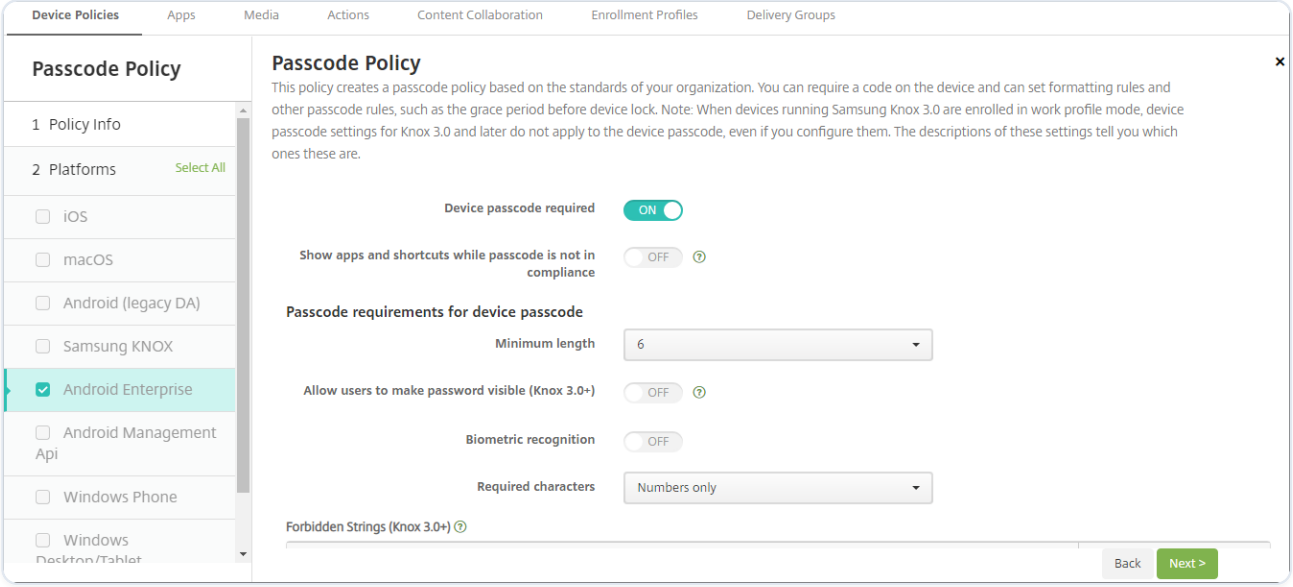
要加密设备，用户必须从电池充满电开始，并在加密所需的一个或多个小时内保持设备连接电源。如果他们中断加密过程，可能会丢失设备上的部分或全部数据。设备加密后，除了通过恢复出厂设置（这将擦除设备上的所有数据）之外，无法逆转此过程。

- **三星SAFE**

> **注意：**
>
> 作为在 Samsung SAFE 设备上禁用面部或虹膜识别的变通方法：为 Samsung SAFE 创建一个限制设备策略。在限制策略中，启用“**禁用应用程序**”并向表中添加 `com.samsung.android.bio.face.service` 或 `com.samsung.android.server.iris`。然后，部署限制策略。

  - **对所有用户使用相同的密码：** 选择是否对所有用户使用相同的密码。默认值为“**关**”。此设置仅适用于 Samsung SAFE 设备，并且无论“**需要密码**”设置如何都可用。
  - 启用“**对所有用户使用相同的密码**”时，请在“**密码**”字段中键入所有用户要使用的密码。
  - 启用“**需要密码**”时，请配置以下 Samsung SAFE 设置：
    - **更改的字符：** 键入用户必须从其上一个密码中更改的字符数。默认值为“**0**”。
    - **字符可出现的次数：** 键入字符在密码中可出现的最大次数。默认值为“**0**”。
    - **字母序列长度：** 键入密码中字母序列的最大长度。默认值为“**0**”。
    - **数字序列长度：** 键入密码中数字序列的最大长度。默认值为“**0**”。
    - **允许用户显示密码：** 选择用户是否可以显示其密码。默认值为“**开**”。
    - **配置生物识别身份验证**。选择是否启用生物识别身份验证。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**。选择以允许用户使用指纹进行身份验证。
      - **允许虹膜**。选择此项以允许用户使用虹膜进行身份验证。
    - **禁用字符串**：您创建禁用字符串以防止用户使用不安全的、易于猜测的字符串，例如“password”、“pwd”、“welcome”、“123456”、“111111”。对于您要拒绝的每个字符串，单击“**添加**”，然后执行以下操作：
      - **禁用字符串**：键入用户可能不会使用的字符串。
      - 单击“**保存**”以添加字符串，或单击“**取消**”以取消添加字符串。

安卓企业设置



对于 Android Enterprise 设备，您可以要求设备使用密码，或要求 Android Enterprise 工作资料使用安全质询，或两者都要求。

对于运行 Android 9.0 或更高版本以及 Samsung Knox 3.0 或更高版本的设备，请在“**Android Enterprise**”页面上配置 Samsung Knox 的设置。对于运行早期版本 Android 或 Samsung Knox 的设备，请使用“**Samsung Knox**”页面。

> **注意：**
>
> 当运行 Samsung Knox 3.0 的设备注册为工作资料设备时，即使您配置了 Knox 3.0 及更高版本的设备密码设置，这些设置也不适用于设备密码。

- **需要设备密码**：要求设备上设置密码。当此设置为“**开**”时，请配置“**设备密码要求**”和“**设备密码安全性**”下的设置。默认值为“**关**”。
- **在密码不合规时显示应用程序和快捷方式**：当此设置为“**开**”时，即使密码不合规，设备上的应用程序和快捷方式也不会隐藏。当此设置为“**关**”时，如果密码不合规，则应用程序和快捷方式将被隐藏。如果启用此设置，Citrix® 建议您创建自动化操作，以便在密码不合规时将设备标记为不合规。默认值为“**关**”。
- **设备密码要求**：
  - **最小长度**：指定最小密码长度。默认值为 6。
  - **允许用户显示密码**：适用于运行 Samsung Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。仅适用于完全托管的设备。此设置不适用于注册为工作资料的设备。允许用户显示密码。默认值为“**关**”。

- **生物识别：** 启用生物识别。如果此设置为“**开**”，则“**所需字符**”字段将被隐藏。默认值为“**关**”。
- **所需字符：** 指定密码所需的字符类型。在列表中，选择“**无限制**”、“**数字和字母**”、“**仅数字**”或“**仅字母**”。仅适用于运行 Android 7.0 的设备使用“**无限制**”。Android 7.1 及更高版本不支持“**无限制**”设置。默认值为“**数字和字母**”。
- **禁用字符串：** 适用于运行 Samsung Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作资料设备的设备。指定用户不能用作密码的字符串。您可以创建禁用字符串，以防止用户使用不安全的、易于猜测的字符串，例如“password”、“pwd”、“welcome”、“123456”、“111111”。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：** 应用密码中可出现的字符类型的高级规则。当此设置为“**开**”时，配置“**最少数量**”和“**最多数量**”下的设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为“**关**”。
- **最少数量：**
  - **符号：** 指定符号的最小数量。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**。
  - **已更改字符：** 适用于运行 Samsung Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作资料设备的设备。指定用户必须从其上一个密码中更改的字符数。默认值为 **0**。
- **最多数量：** 适用于运行 Samsung Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。仅适用于完全托管设备。此设置不适用于注册为工作资料设备的设备。
  - **字符可出现的次数：** 指定一个字符在密码中可出现的最大次数。默认值为 **0**，表示没有最大限制。
  - **字母序列长度：** 指定密码中字母序列的最大长度。默认值为 **0**，表示没有最大限制。
  - **数字序列长度：** 指定密码中数字序列的最大长度。默认值为 **0**，表示没有最大限制。

- **设备密码的密码安全性：**

  - **在（登录尝试失败）后擦除设备：** 指定用户可以登录失败的次数，超过该次数后设备将被完全擦除。默认值为 **未定义**。
  - **在（不活动分钟数）后锁定设备 (0-999)：** 指定设备在锁定前可以不活动的分钟数。默认值为 **无**。
  - **密码过期天数 (1-730)：** 指定密码过期前的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
  - **已保存的旧密码 (0-50)：** 指定要保存的已使用密码的数量。用户无法使用此列表中找到的任何密码。有效值为 0–50。默认值为 **0**，表示用户可以重复使用密码。
  - **在（登录尝试失败）后锁定设备** 对于运行 Samsung Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。仅适用于完全托管的设备。此设置不适用于注册为工作配置文件设备的设备。指定用户可以登录失败的次数，超过该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在 Android Enterprise 工作配置文件中运行的应用程序。适用于运行 Android 7.0 及更高版本的设备。当此设置为 **开** 时，请配置“**工作配置文件安全质询的密码要求**”和“**工作配置文件安全质询的密码安全性**”下的设置。默认值为 **关**。
- **工作配置文件安全质询的密码要求：**
  - **最小长度：** 指定最小密码长度。默认值为 6。
  - **允许用户显示密码：** 适用于运行 Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。允许用户显示密码。默认值为 **关**。
  - **生物识别：** 启用生物识别。如果此设置为 **开**，则“**所需字符**”字段将被隐藏。默认值为 **关**。
  - **所需字符：** 指定密码所需的字符类型。在列表中，选择“**无限制**”、“**数字和字母**”、“**仅数字**”或“**仅字母**”。仅适用于运行 Android 7.0 的设备使用“**无限制**”。Android 7.1 及更高版本不支持“**无限制**”设置。默认值为“**数字和字母**”。
  - **禁用字符串：** 适用于运行 Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。指定用户不能用作密码的字符串。您可以创建禁用字符串，以防止用户使用容易猜测的不安全字符串，例如“password”、“pwd”、“welcome”、“123456”、“111111”。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：** 应用关于密码中可出现字符类型的高级规则。当此设置为 **开** 时，请配置“**最少数量**”和“**最多数量**”下的设置。此设置不适用于 Android 5.0 之前的 Android 设备。默认值为 **关**。
  - **最小数量：**
    - **符号：** 指定符号的最小数量。默认值为 **0**。

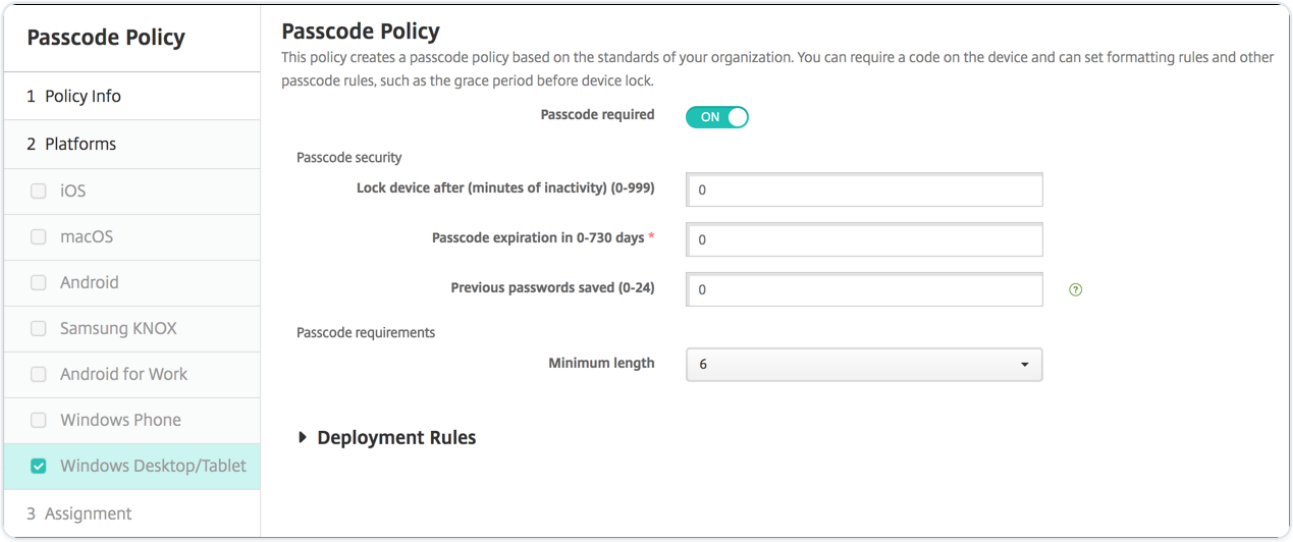
  - **字母：** 指定字母的最小数量。默认值为 **0**。
  - **小写字母：** 指定小写字母的最小数量。默认值为 **0**。
  - **大写字母：** 指定大写字母的最小数量。默认值为 **0**。
  - **数字或符号：** 指定数字或符号的最小数量。默认值为 **0**。
  - **数字：** 指定数字的最小数量。默认值为 **0**。
  - **已更改字符：** 适用于运行 Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。指定用户必须从其以前的密码中更改的字符数。默认值为 **0**。
- **最大数量：** 适用于运行 Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。
  - **字符可出现次数：** 指定字符在密码中可出现的最大次数。默认值为 **0**，表示没有最大限制。
  - **字母序列长度：** 指定密码中字母序列的最大长度。默认值为 **0**，表示没有最大限制。
  - **数字序列长度：** 指定密码中数字序列的最大长度。默认值为 **0**，表示没有最大限制。
- **启用统一密码：** 如果为 **开**，用户将为其设备和工作配置文件使用一个密码。如果为 **关**：
  - 用户必须为其设备和工作配置文件使用不同的密码。
  - 设备上的“**使用一个锁**”设置（用户在希望为其设备和工作配置文件使用一个密码时进行设置）已禁用。用户无法启用它。
  - 如果工作配置文件安全质询的密码要求比设备密码更复杂：启用了“**使用一个锁定**”设置的用户会收到更改其工作配置文件密码的提示。

  默认值为“**关**”。适用于 Android 9.0 及更高版本。

- **工作配置文件安全质询的密码安全性**
  - **在以下次数的登录尝试失败后擦除容器：** 指定用户可以登录失败的次数，达到此次数后，工作配置文件及其数据将从设备中擦除。擦除后，用户必须重新初始化工作配置文件。默认值为“**未定义**”。
  - **在以下不活动分钟数后锁定容器：** 指定设备在工作配置文件锁定前可以不活动的分钟数。默认值为“**无**”。
  - **密码有效期（天，1-730）：** 指定密码过期前的天数。有效值为 1–730。默认值为 **0**，表示密码永不过期。
  - **已保存的旧密码（0-50）：** 指定要保存的已用密码数量。用户无法使用此列表中的任何密码。有效值为 0–50。默认值为 **0**，表示用户可以重复使用密码。

- **在以下次数的登录尝试失败后锁定容器：** 适用于运行 Knox 3.0 及更高版本且已配置有效 Knox 许可证密钥的设备。指定用户可以登录失败的次数，达到此次数后，设备将被锁定。默认值为“**未定义**”。

视窗桌面/平板电脑设置



- **禁止便捷登录：** 选择是否允许用户使用图片密码或生物识别登录来访问其设备。默认值为“**关**”。
- **最小密码长度：** 在下拉列表中选择最小密码长度。默认值为 **6**。
- **擦除前的最大密码尝试次数：** 在列表中，单击用户可以登录失败的次数，达到此次数后，公司数据将从设备中擦除。默认值为 **4**。
- **密码有效期（天，0-730）：** 键入密码过期前的天数。有效值为 0–730。默认值为 **0**，表示密码永不过期。
- **密码历史记录：（1-24）：** 键入要保存的已用密码数量。用户无法使用此列表中的任何密码。有效值为 1–24。您必须在此字段中输入一个介于 1 到 24 之间的数字。默认值为 **0**。
- **设备锁定前的最长不活动时间（分钟，1-999）：** 键入设备在锁定前可以不活动的最长时间（分钟）。有效值为 1–999。您必须在此字段中输入一个介于 1 到 999 之间的数字。默认值为 **0**。

个人热点设备策略

您可以允许用户通过其 iOS 设备的个人热点功能，在没有 Wi-Fi 网络覆盖的区域使用蜂窝数据连接来连接互联网。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

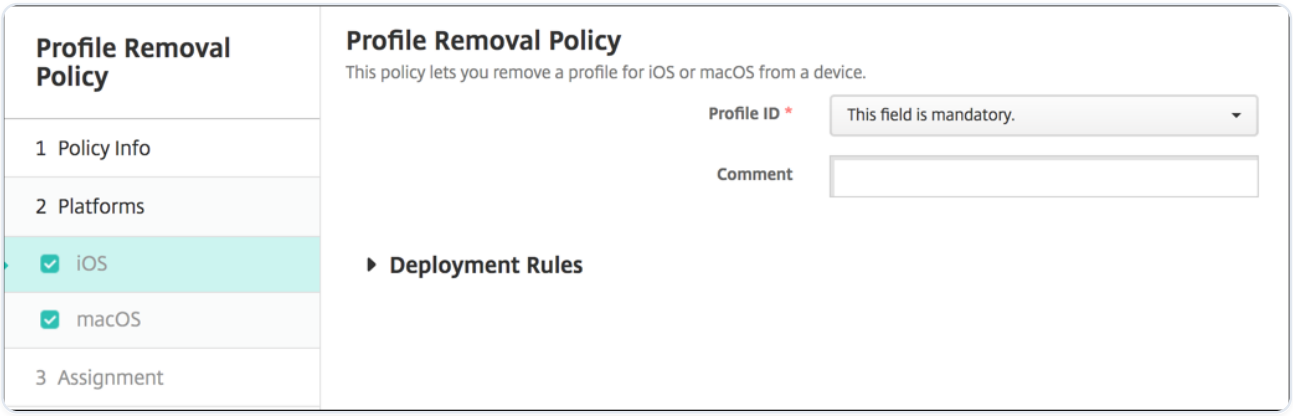
禁用个人热点： 选择是否在用户设备上禁用个人热点功能。默认设置为**关**，这会关闭用户设备上的个人热点。此策略不会禁用该功能。用户仍可在其设备上使用个人热点。但当策略部署后，个人热点将关闭，以避免默认保持开启状态。

配置文件删除设备策略

您可以在 XenMobile 中创建应用程序配置文件删除设备策略。部署后，此策略会从用户的 iOS 或 macOS 设备中删除应用程序配置文件。

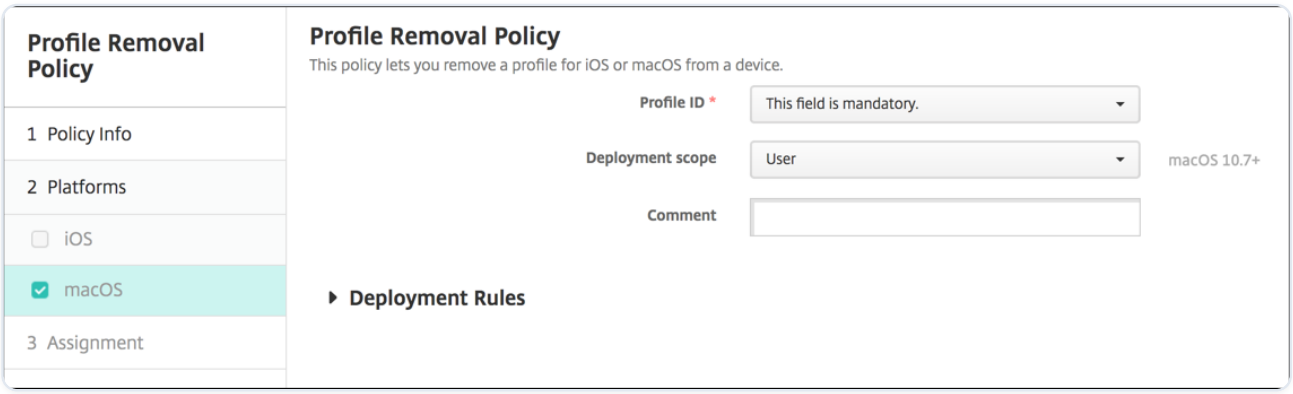
要添加或配置此策略，请转至“**配置 > 设备策略**”。有关详细信息，请参阅设备策略。

iOS 设置



- **配置文件 ID：** 在下拉列表中选择应用程序配置文件 ID。此字段为必填项。
- **注释：** 键入可选注释。

macOS 设置



- **配置文件 ID：** 在下拉列表中选择应用程序配置文件 ID。此字段为必填项。
- **部署范围：** 在下拉列表中选择“**用户**”或“**系统**”。默认值为“**用户**”。此选项仅适用于 macOS 10.7 及更高版本。

- **注释：** 键入可选注释。

预置配置文件设备策略

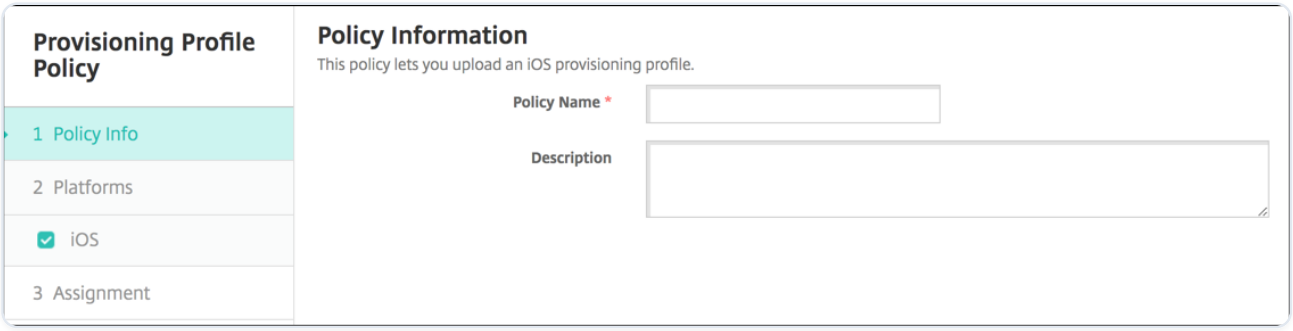
当您开发并对 iOS 企业应用进行代码签名时，您通常会包含一个企业分发预置配置文件，这是 Apple 要求应用在 iOS 设备上运行所必需的。如果预置配置文件缺失或已过期，用户点击打开应用时，应用会崩溃。

预置配置文件的主要问题是，它们在 Apple Developer Portal 上生成一年后就会过期，您必须跟踪用户注册的所有 iOS 设备上所有预置配置文件的过期日期。跟踪过期日期不仅涉及跟踪实际过期日期，还涉及哪些用户正在使用哪个版本的应用。两种解决方案是将预置配置文件通过电子邮件发送给用户，或者将其放在门户网站上供下载和安装。这些解决方案可行，但容易出错，因为它们要求用户根据电子邮件中的说明进行操作，或者访问门户网站下载正确的配置文件并进行安装。

为了使用户能够透明地完成此过程，在 XenMobile® 中，您可以使用设备策略安装和删除预置配置文件。缺失或过期的配置文件会根据需要删除，并将最新的配置文件安装到用户的设备上，这样，点击应用即可直接打开使用。

在创建预置配置文件策略之前，您必须创建一个预置配置文件。有关详细信息，请参阅 Apple 关于如何在 Apple Developer 网站 上创建开发预置配置文件的文章。

iOS 设置



- **iOS 预置配置文件：** 选择要导入的预置配置文件，方法是单击“**浏览**”，然后导航到文件位置。

配置文件移除设备策略

您可以使用设备策略移除 iOS 配置文件。有关配置文件的更多信息，请参阅配置文件设备策略。

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 配置文件：** 单击下拉列表中要移除的配置文件。

- **注释：** （可选）添加注释。

代理设备策略

您可以在 XenMobile 中添加设备策略，为运行 iOS 6.0 或更高版本的设备指定全局 HTTP 代理设置。每台设备只能部署一个全局 HTTP 代理策略。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

先决条件

在部署此策略之前，请务必将所有要设置全局 HTTP 代理的 iOS 设备设置为监管模式。有关详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于监管模式 或通过 Apple 部署计划部署设备。

在将代理策略发送到设备之前，设置部署规则以注册设备。

iOS 设置

- **代理配置：** 单击**手动**或**自动**，以确定如何在用户设备上配置代理。
  - 如果单击**手动**，请配置以下设置：
    - **代理服务器的主机名或 IP 地址：** 键入代理服务器的主机名或 IP 地址。此字段为必填项。
    - **代理服务器端口：** 键入代理服务器端口号。此字段为必填项。
    - **用户名：** 键入可选用户名以向代理服务器进行身份验证。
    - **密码：** 键入可选密码以向代理服务器进行身份验证。
  - 如果单击**自动**，请配置以下设置：
    - **代理 PAC URL：** 键入定义代理配置的 PAC 文件的 URL。
    - **如果 PAC 不可达则允许直接连接：** 选择当 PAC 文件不可达时，是否允许用户直接连接到目标。默认值为 **开**。此选项仅适用于 iOS 7.0 及更高版本。
- **允许绕过代理访问强制网络：** 选择是否允许绕过代理访问强制网络。默认值为 **关**。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。

- **删除前持续时间（小时）：** 输入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。

限制设备策略

限制设备策略允许或限制用户设备上的某些功能或特性，例如摄像头。除了对媒体内容的限制以及对用户可以和不可以安装的应用程序类型的限制之外，您还可以设置安全限制。大多数限制设置默认为 **开**，即 *允许*。主要例外是 iOS 安全 - 强制功能和所有 Windows 平板电脑功能，它们默认为 **关**，即 *限制*。

对于 Windows 10 RS2 手机：在禁用 Internet Explorer 的自定义 XML 策略或限制策略部署到手机后，浏览器仍然启用。要解决此问题，请重启手机。此问题是第三方问题。

提示：

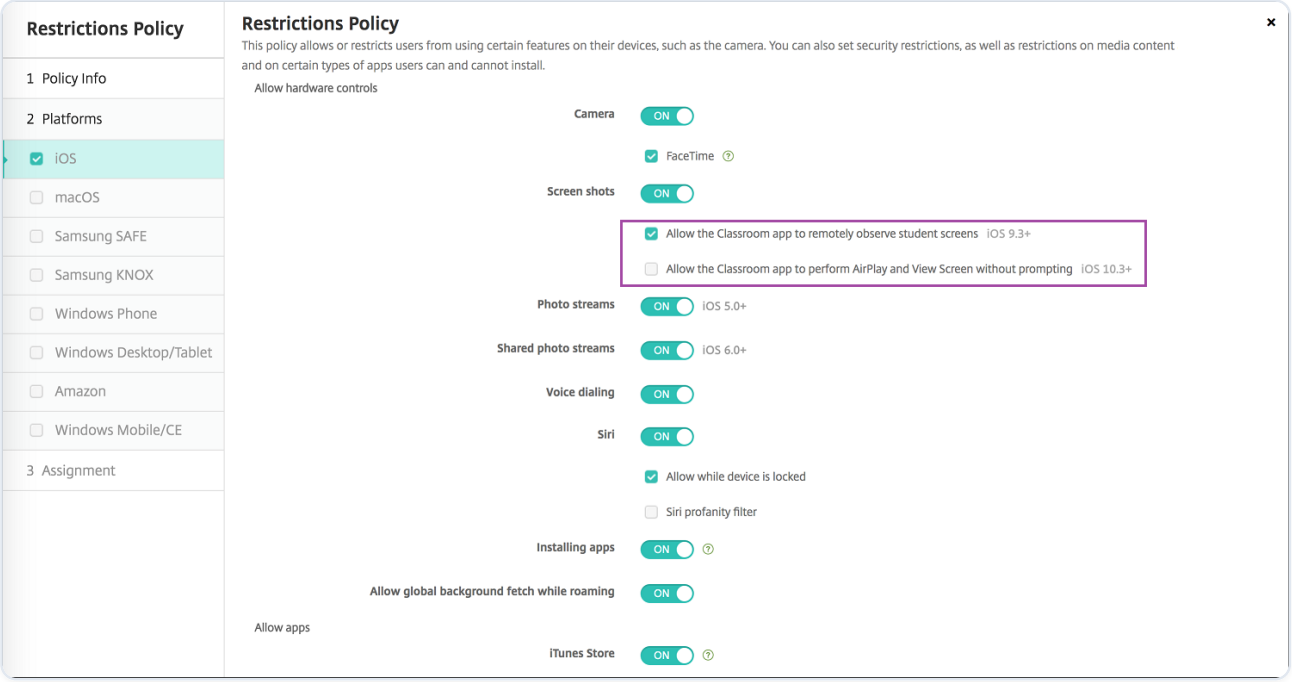
任何您选择 **开** 的选项都意味着用户可以执行该操作或使用该功能。例如：

摄像头。如果为 **开**，用户可以在其设备上使用摄像头。如果为 **关**，用户无法在其设备上使用摄像头。

屏幕截图。如果为 **开**，用户可以在其设备上进行屏幕截图。如果为 **关**，用户无法在其设备上进行屏幕截图。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

iOS 设置



某些 iOS 限制策略设置仅适用于特定版本的 iOS，如本文和 XenMobile® 控制台限制策略页面中所述。

当设备注册到用户注册模式、非监督（完全 MDM）模式或监督模式时，iOS 限制策略设置可以应用。下表显示了适用于 iOS 13 及更高版本中每个限制策略设置的注册模式。

如表中所示，某些以前在非监督模式和监督模式下可用的设置从 iOS 13 开始仅在监督模式下可用。适用以下规则：

- 如果受监督的 iOS 13+ 设备注册到 XenMobile，这些设置将应用于该设备。
- 如果非监督的 iOS 13+ 设备注册到 XenMobile，这些设置不适用于该设备。
- 如果已注册到 XenMobile 的 iOS 12（或更低版本）设备升级到 iOS 13，则不会有任何更改。设置将像升级前一样应用于设备。

有关将 iOS 设备设置为受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

设置	用户注册	非受监督	受监督
允许硬件控制			
摄像头	否	是	是
FaceTime	否	否（iOS 13 新增）	是

设置	用户注册	非受监督	受监督
允许 FaceTime 远程控制	否	否	是
屏幕截图	是	否	是
允许课堂应用远程观察学生屏幕	否	否	是
允许课堂应用在不提示的情况下执行 AirPlay 和查看屏幕	否	否	是
照片流	否	是	是
共享照片流	否	是	是
允许共享 iPad 临时会话	否	是	是
语音拨号	否	是	是
语音助手	是	是	是
设备锁定时允许	是	是	是
Siri 脏话过滤器	否	否	是
安装应用	否	否（iOS 13 新增）	是
备用应用市场	否	否	是
Web 分发应用	否	否	是
漫游时允许全局后台获取	否	是	是
允许应用			
iTunes 商店	否	否 (iOS 13 新增)	是
应用内购买	否	是	是

设置	用户注册	非受监督	受监督
购买时需要 iTunes 密码	否	是	是
萨法里	否	否 (iOS 13 新增)	是
自动填充	否	否 (iOS 13 新增)	是
强制欺诈警告	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 iCloud 操作			
iCloud 文档和数据	否	否（iOS 13 新增）	是
iCloud 备份	否	是	是
iCloud 照片钥匙串	否	是	是
iCloud 照片图库	否	是	是
安全性 - 强制			
加密备份	是	是	是
限制广告跟踪	否	是	是
首次 AirPlay 配对时需要密码	是	是	是
配对的 Apple Watch 使用手腕检测	是	是	是
使用 AirDrop 共享托管文档	是	是	是
安全性 - 允许			

设置	用户注册	非受监督	受监督
接受不受信任的 SSL 证书	否	是	是
自动更新证书信任设置	否	是	是
要求受管剪贴板	是	是	是
受管应用程序中的文档在非受管应用程序中	是	是	是
非托管应用读取托管联系人	否	否	是
托管应用写入非托管联系人	否	否	是
托管应用中的非托管应用文档	是	是	是
向 Apple 提交诊断信息	是	是	是
使用触控 ID 解锁设备	否	是	是
自动解锁	否	是	是
锁定时的 Passbook 通知	否	是	是
接力	否	是	是
受管应用的 iCloud 同步	是	是	是
企业图书备份	是	是	是
企业图书的笔记和高亮同步	是	是	是

设置	用户注册	非受监督	受监督
Spotlight 中的互联网结果	否	是	是
企业应用信任	否	是	是
允许 Apple 个性化广告	否	是	是
仅限受监督的设置 - 允许			
允许 eSIM 修改	否	否	是
擦除时保留 eSIM	否	否	是
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
指纹修改	否	否	是
从设备安装应用程序	否	否	是
键盘快捷键	否	否	是
配对的 Apple Watch	否	否	是
密码修改	否	否	是
设备名称修改	否	否	是
壁纸修改	否	否	是
自动下载应用程序	否	否	是
隔空投送	否	否	是
iMessage	否	否	是

设置	用户注册	非受监督	受监督
Siri 用户生成内容	否	否	是
iBooks	否	否	是
移除应用	否	是	是
游戏中心	否	否 (iOS 13 新增)	是
添加朋友	否	否	是
多人游戏	否	否 (iOS 13 新增)	是
修改帐户设置	否	否	是
修改应用蜂窝数据设置	否	否	是
允许网络驱动器连接	否	否	是
允许 USB 设备连接	否	否	是
允许查找我的设备	否	否	是
允许查找我的朋友	否	否	是
修改查找我的朋友设置	否	否	是
与非 Configurator 主机配对	否	否	是
预测键盘	否	否	是
键盘自动更正	否	否	是
键盘拼写检查	否	否	是
允许 QuickPath 键盘	否	否	是
定义查找	否	否	是
单个应用捆绑包 ID	否	否	是

设置	用户注册	非受监督	受监督
新闻	否	否	是
Apple Music 服务	否	否	是
iTunes 广播	否	否	是
通知修改	否	否	是
受限应用使用	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
强制开启 Wi-Fi	否	否	是
仅加入由 Wi-Fi 策略安装的 Wi-Fi 网络	否	否	是
允许课堂应用在不提示的情况下执行隔空播放和查看屏幕	否	否	是
允许课堂应用在不提示的情况下锁定到某个应用并锁定设备	否	否	是
允许课堂应用在不提示的情况下自动加入课程	否	否	是
允许隔空打印	否	否	是
允许在钥匙串中存储隔空打印凭据	否	否	是
允许使用 iBeacon 发现隔空打印机	否	否	是

设置	用户注册	非受监督	受监督
仅允许隔空打印到具有受信任证书的目标	否	否	是
添加 VPN 配置	否	否	是
修改蜂窝数据套餐设置	否	否	是
移除系统应用	否	否	是
设置新的附近设备	否	否	是
允许 USB 受限模式	否	否	是
强制延迟软件更新	否	否	是
强制软件更新延迟	否	否	是
强制课堂请求离开班级的权限	否	否	是
在自动填充前强制进行身份验证	否	否	是
强制自动设置日期和时间	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
修改个人热点设置	否	否	是
允许未配对设备启动到恢复模式	否	否	是
安装快速安全响应	否	否	是
移除快速安全响应	否	否	是

设置	用户注册	非受监督	受监督
允许邮件隐私保护	否	否	是
NFC	否	否	是
允许 App Clips	否	否	是
生成式表情符号	否	否	是
图像游乐场	否	否	是
图像魔杖	否	否	是
iPhone 镜像	否	否	是
个性化手写结果	否	否	是
书写工具	否	否	是
通话录音	否	否	是
要隐藏的应用程序	否	否	是
要锁定的应用程序	否	否	是
邮件摘要	否	否	是
RCS 消息	否	否	是
允许外部智能集成	否	否	是
允许登录到外部智能集成	否	否	是
允许邮件智能回复	否	否	是
允许备忘录转录	否	否	是
允许 Safari 摘要	否	否	是
允许视觉智能摘要	否	否	是
允许备忘录转录摘要	否	否	是

设置	用户注册	非受监督	受监督
允许 Apple 智能报告	否	否	是
允许修改默认通话应用	否	否	是
允许修改默认消息应用	否	否	是
允许外部智能工作区 ID	否	否	是
默认浏览器修改	否	否	是
允许实时语音邮件	否	否	是
安全性 - 在锁定屏幕中显示			
控制中心	是	是	是
通知	是	是	是
今天视图	是	是	是
媒体内容 - 允许			
露骨音乐、播客和 iTunes U 材料	否	否（iOS 13 新增）	是
iBooks 中的露骨色情内容	否	是	是
评级区域	否	是	是
电影	否	是	是
电视节目	否	是	是
应用	否	是	是

- **允许硬件控制**

- **摄像头：** 允许用户在其设备上使用摄像头。
  - **FaceTime：** 允许用户在其设备上使用 FaceTime。适用于受监管的 iOS 设备。
  - **允许 FaceTime 远程控制：** 允许远程 FaceTime 会话请求控制设备。适用于受监管的 iOS 设备。适用于 iOS 18.4 及更高版本。
- **屏幕截图：** 允许用户在其设备上截取屏幕截图。
  - **允许课堂应用远程观察学生屏幕：** 如果未选择此限制，教师将无法使用课堂应用远程观察学生屏幕。默认设置为已选择，教师可以使用课堂应用观察学生屏幕。**允许课堂应用在不提示的情况下执行 AirPlay 和查看屏幕**的设置决定了学生是否会收到提示以授予教师权限。适用于受监管的 iOS 设备。
  - **允许课堂应用在不提示的情况下执行 AirPlay 和查看屏幕：** 如果选择了此限制，教师可以在学生设备上执行 AirPlay 和查看屏幕，而无需提示权限。默认设置为未选择。适用于受监管的 iOS 设备。
- **照片流：** 允许用户使用“我的照片流”通过 iCloud 将照片共享到其所有 iOS 设备。
- **共享照片流：** 允许用户使用 iCloud 照片共享与同事、朋友和家人共享照片。
- **允许共享 iPad 临时会话：** 当设置为“**关闭**”时，阻止访问共享 iPad 上的临时会话。默认设置为“**打开**”。
- **语音拨号：** 在用户设备上启用语音拨号功能。
- **Siri：** 允许用户使用 Siri。
  - **设备锁定时允许使用：** 允许用户在设备锁定时使用 Siri。
  - **Siri 脏话过滤器：** 启用 Siri 脏话过滤器。默认情况下，此功能受到限制，这意味着不执行脏话过滤。

    有关 Siri 和安全性的更多信息，请参阅 Siri 和听写策略。
- **安装应用：** 允许用户安装应用。适用于受监督的 iOS 设备。
- **替代应用市场：** 阻止从网络安装替代应用市场应用，并阻止任何已安装的替代应用市场应用安装其他应用。此功能适用于 iOS 17.4 及更高版本。默认设置为 **开**。适用于受监督的 iOS 设备。
- **Web 分发应用：** 允许客户管理员阻止 iOS 设备上通过 Web 分发的第三方应用。这适用于 iOS 17.5 及更高版本。有关详细信息，请参阅 限制。
- **漫游时允许全局后台获取：** 允许设备在漫游时自动将邮件帐户同步到 iCloud。当设置为 **关** 时，会在 iOS 手机漫游时禁用全局后台获取活动。默认设置为 **开**。

- **允许应用**
  - **iTunes Store：** 允许用户访问 iTunes Store。适用于受监督的 iOS 设备。
  - **应用内购买：** 允许用户进行应用内购买。
    - **购买时需要 iTunes 密码：** 要求应用内购买时输入密码。默认情况下，此功能受到限制，这意味着应用内购买不需要密码。
  - **Safari：** 允许用户访问 Safari。适用于受监督的 iOS 设备。
    - **自动填充：** 允许用户在 Safari 上设置用户名和密码的自动填充功能。
    - **强制欺诈警告：** 如果启用此设置，并且用户访问可疑的钓鱼网站，Safari 会向用户发出警报。默认情况下，此功能受到限制，这意味着不会发出任何警告。
    - **启用 JavaScript：** 允许 JavaScript 在 Safari 上运行。
    - **阻止弹出窗口：** 在浏览网站时阻止弹出窗口。默认情况下，此功能受到限制，这意味着不会阻止弹出窗口。
  - **接受 Cookie：** 设置 Cookie 的接受程度。在列表中，选择一个选项以允许或限制 Cookie。默认选项是**始终**，它允许所有网站在 Safari 中保存 Cookie。其他选项包括**仅限当前网站**、**从不**和**仅限访问过的网站**。
- **网络 - 允许 iCloud 操作**
  - **iCloud 文档和数据：** 允许用户将文档和数据同步到 iCloud。适用于受监管的 iOS 设备。
  - **iCloud 备份：** 允许用户将其设备备份到 iCloud。
  - **iCloud 钥匙串：** 允许用户将密码、Wi-Fi 网络、信用卡和其他信息存储在 iCloud 钥匙串中。
  - **云照片图库：** 允许用户访问其 iCloud 照片图库。
- **安全 - 强制**

  默认情况下，以下功能受到限制，这意味着未启用任何安全功能。
  - **加密备份：** 强制将备份到 iCloud 的数据进行加密。
  - **限制广告跟踪：** 阻止定向广告跟踪。
  - **首次 AirPlay 配对时需要密码：** 要求 AirPlay 设备在使用 AirPlay 之前通过一次性屏幕代码进行验证。
  - **配对的 Apple Watch 使用手腕检测：** 要求配对的 Apple Watch 使用**手腕检测**。
  - **使用 AirDrop 共享托管文档：**将此选项设置为“**开**”会使 AirDrop 显示为非托管投放目标。

- **安全性 - 允许**
  - **接受不受信任的 SSL 证书：**允许用户接受网站不受信任的 SSL 证书。
  - **自动更新证书信任设置：**允许自动更新受信任的证书。
  - **要求托管粘贴板：**如果设置为“开”，则允许复制和粘贴功能遵循您应用于“**非托管应用中的托管应用文档**”和“**托管应用中的非托管应用文档**”的相同限制。默认值为“**关**”。 例如，您可以配置以下内容：
    - **要求托管粘贴板**：开
    - **非托管应用中的托管应用文档**：关
    - **托管应用中的非托管应用文档**：开

> **注意：**
>
> 将策略部署到 iOS 设备后，用户无法将数据从托管应用复制并粘贴到非托管应用，但可以将数据从非托管应用复制并粘贴到托管应用。

  - **非托管应用中的托管应用文档：**允许用户将数据从托管（公司）应用移动到非托管（个人）应用。
  - **托管应用中的非托管应用文档：**允许用户将数据从非托管（个人）应用移动到托管（公司）应用。
  - **向 Apple 提交诊断信息：**允许将有关用户设备的匿名诊断数据发送给 Apple。
  - **使用触控 ID 解锁设备：**允许用户使用指纹解锁设备。
  - **自动解锁：**如果设置为“**关**”，则用户无法使用 Apple Watch 解锁配对的 iPhone。默认值为“**开**”。适用于 iOS 14.5 或更高版本。
  - **锁定时显示 Passbook 通知：** 允许 Passbook 通知显示在锁定屏幕上。
  - **Handoff：** 允许用户将活动从一台 iOS 设备传输到另一台附近的 iOS 设备。
  - **受管应用的 iCloud 同步：** 允许用户将受管应用同步到 iCloud。
  - **企业图书备份：** 允许将企业图书备份到 iCloud。
  - **企业图书的笔记和高亮同步：** 允许用户添加到企业图书的笔记和高亮同步到 iCloud。
  - **企业应用信任：** 允许信任企业应用程序。企业应用是为您的组织定制的任何应用。这些应用可以由内部制作，也可以由外部供应商开发和购买。有关其他信息，请参阅在 iOS 上安装自定义企业应用。

- **Spotlight 中的互联网结果：** 允许 Spotlight 除了设备上的搜索结果外，还显示来自互联网的搜索结果。
- **非受管应用读取受管联系人：** 可选。仅当**非受管应用中的受管应用文档**被禁用时可用。如果启用此策略，非受管应用可以读取受管帐户联系人中的数据。默认值为**关**。从 iOS 12 开始可用。
- **受管应用写入非受管联系人：** 可选。如果启用，允许受管应用将联系人写入非受管帐户的联系人。如果**非受管应用中的受管应用文档**已启用，则此限制无效。默认值为**关**。从 iOS 12 开始可用。
- **允许 Apple 个性化广告：** 如果设置为**关**，则 Apple 广告平台不会使用用户数据来投放个性化广告。默认值为**开**。适用于 iOS 14.0 或更高版本。

- **仅限受监管设备设置 - 允许**

这些设置仅适用于受监管设备。有关将 iOS 设备设置为受监管模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监管模式。

- **允许修改 eSIM：** 允许用户更改其设备上的 eSIM 设置。
- **擦除时保留 eSIM：** 如果设置为**开**，当系统因密码尝试失败次数过多或在**设置** > **通用** > **重置**中选择“抹掉所有内容和设置”选项而擦除设备时，系统会保留 eSIM。默认值为**关**。

> **注意：**
>
> 如果 **查找我的** 启动擦除设备，系统不会保留 eSIM。

- **抹掉所有内容和设置：** 允许用户抹掉其设备上的所有内容和设置。
- **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。
- **安装配置描述文件：** 允许用户安装您部署的配置描述文件以外的其他描述文件。
- **指纹修改：** 允许用户更改或删除其触控 ID 指纹。
- **从设备安装应用：** 允许用户安装应用。禁用此设置可阻止最终用户安装新应用。App Store 将被禁用，其图标将从主屏幕中移除。
- **键盘快捷键：** 允许用户为其经常使用的词语或短语创建自定义键盘快捷键。
- **配对 Apple Watch：** 允许用户将 Apple Watch 与受监督的设备配对。
- **密码修改：** 允许用户更改受监督设备上的密码。

- **设备名称修改：** 允许用户更改其设备的名称。
- **墙纸修改：** 允许用户更改其设备上的墙纸。
- **自动下载应用：** 允许应用下载。
- **隔空投送：** 允许用户与附近的 iOS 设备共享照片、视频、网站、位置等。
- **iMessage：** 允许用户通过 Wi-Fi 使用 iMessage 发送短信。
- **Siri 用户生成内容：** 允许 Siri 查询网络上的用户生成内容。消费者而非传统记者生成用户生成内容。例如，Twitter 或 Facebook 上的内容就是用户生成的。
- **iBooks：** 允许用户使用 iBooks 应用程序。
- **移除应用程序：** 允许用户从其设备中移除应用程序。
- **Game Center：** 允许用户通过其设备上的 Game Center 玩在线游戏。
  - **添加好友：** 允许用户向好友发送玩游戏的通知。
  - **多人游戏：** 允许用户在其设备上开始多人游戏。
- **修改帐户设置：** 允许用户修改其设备帐户设置。
- **修改应用程序蜂窝数据设置：** 允许用户修改应用程序使用蜂窝数据的方式。
- **允许网络驱动器连接：** 当设置为“**关闭**”时，阻止在“文件”应用程序中连接到网络驱动器。默认设置为“**打开**”。
- **允许 USB 设备连接：** 当设置为“**关闭**”时，阻止在“文件”应用程序中连接到任何已连接的 USB 设备。默认设置为“**打开**”。
- **允许查找我的设备：** 当设置为“**关闭**”时，禁用“查找”应用程序中的“**查找我的设备**”选项。默认设置为“**打开**”。
- **允许查找我的朋友：** 当设置为“**关闭**”时，禁用“查找”应用程序中的“**查找我的朋友**”选项。默认设置为“**打开**”。
- **修改查找我的朋友设置：** 允许用户更改其“查找我的朋友”设置。
- **与非 Configurator 主机配对：** 允许管理员控制用户设备可以与哪些设备配对。禁用此设置可阻止配对，除非是与运行 Apple Configurator 的监督主机配对。如果未配置监督主机证书，则所有配对都将被禁用。
- **预测键盘：** 允许用户设备使用预测键盘在键入时提供单词建议。在管理标准化测试等情况下禁用此选项，因为您不希望用户访问建议的单词。
- **键盘自动更正：** 允许用户设备使用键盘自动更正功能。在管理标准化测试等情况下禁用此选项，因为您不希望用户访问自动更正功能。

- **键盘拼写检查：** 允许用户设备在键入时使用拼写检查功能。在管理标准化测试等情况下禁用此选项，因为您不希望用户访问拼写检查器。
- **允许 QuickPath 键盘：** 当设置为 **Off** 时，禁用 QuickPath 键盘。默认值为 **On**。
- **定义查找：** 允许用户设备在键入时使用定义查找功能。在管理标准化测试等情况下禁用此选项，因为您不希望用户在键入时查找定义。
- **单个应用程序捆绑包 ID：** 创建允许保留设备控制权并阻止与其他应用程序或功能交互的应用程序列表。 要添加应用程序，请单击 **Add**，键入 **App name**，然后单击 **Save**。对要添加的每个应用程序重复此过程。
- **新闻：** 允许用户使用新闻应用程序。
- **Apple Music 服务：** 允许用户使用 Apple Music 服务。如果您不允许 Apple Music 服务，则音乐应用程序将以经典模式运行。
- **iTunes 广播：** 允许用户使用 iTunes 广播。
- **通知修改：** 允许用户修改通知设置。
- **受限应用程序使用：** 根据您提供的捆绑包 ID，允许用户使用所有应用程序，或使用/不使用某些应用程序。仅适用于受监管的设备。如果您选择 **Only allow some apps**，请添加捆绑包 ID 为 `com.apple.webapp` 的应用程序以允许 Web 剪辑。

  > **注意：**
  >
  > 从 iOS 11 开始，Apple 对可用于应用程序限制的策略进行了更改。Apple 不再允许您通过限制相应的 iOS 应用程序捆绑包来移除对“设置”应用程序和“电话”应用程序的访问权限。
  >
  > 在您配置“限制”设备策略以阻止某些应用程序并部署该策略后：如果您以后想允许其中部分或所有应用程序，更改和部署“限制”设备策略不会更改限制。在这种情况下，iOS 不会将更改应用于 iOS 配置文件。要继续，请使用“配置文件删除”策略删除 iOS 配置文件，然后部署更新的“限制”设备策略。

  如果您将此设置更改为 **Only allow some apps**：在部署此策略之前，请建议使用 Apple 部署计划注册的设备用户从“设置助理”登录其 Apple 帐户。否则，用户可能必须在其设备上禁用双重身份验证才能登录其 Apple 帐户并访问允许的应用程序。
- **诊断提交修改：** 允许用户在 **Settings > Diagnostics & Usage** 窗格中修改诊断提交和应用程序分析设置。
- **蓝牙修改：**允许用户修改蓝牙设置。

- **允许听写：**仅限受监管设备。如果此限制设置为“**关闭**”，则不允许听写输入，包括语音转文本。默认设置为“**开启**”。
- **强制开启 Wi-Fi：**阻止在“设置”或“控制中心”中开启或关闭 Wi-Fi。激活飞行模式对此限制没有影响，此限制不会阻止您选择要连接的 Wi-Fi 网络。默认设置为“**关闭**”。
- **仅加入由 Wi-Fi 策略安装的 Wi-Fi 网络：**可选。仅限受监管设备。如果此限制设置为“**开启**”，则设备只能加入通过配置配置文件设置的 Wi-Fi 网络。默认设置为“**关闭**”。
- **允许课堂应用在不提示的情况下执行 AirPlay 和查看屏幕：**如果选中此限制，教师可以在学生设备上执行 AirPlay 和查看屏幕，而无需提示权限。默认设置为未选中。适用于受监管的 iOS 设备。
- **允许课堂应用在不提示的情况下锁定到某个应用并锁定设备：**如果此限制设置为“**开启**”，课堂应用会自动将用户设备锁定到某个应用并锁定设备，而无需提示用户。默认设置为“**关闭**”。适用于运行 iOS 11（最低版本）的受监管设备。
- **自动加入课堂应用课程，无需提示：**如果此限制设置为“**开启**”，课堂应用会自动将用户加入课程，而无需提示用户。默认设置为“**关闭**”。适用于运行 iOS 11（最低版本）的受监管设备。
- **允许 AirPrint：**如果此限制设置为“**关闭**”，用户将无法使用 AirPrint 进行打印。默认设置为“**开启**”。当此限制设置为“**开启**”时，将显示这些额外限制。适用于运行 iOS 11（最低版本）的受监管设备。
  - **允许在钥匙串中存储 AirPrint 凭据：**如果未选中此限制，AirPrint 用户名和密码将不会存储在钥匙串中。默认设置为选中。适用于运行 iOS 11（最低版本）的受监管设备。
  - **允许使用 iBeacon 发现 AirPrint 打印机：**如果未选中此限制，则会禁用 iBeacon 发现 AirPrint 打印机。这可以防止虚假的 AirPrint 蓝牙信标进行网络流量钓鱼。默认设置为选中。适用于运行 iOS 11（最低版本）的受监管设备。
  - **仅允许 AirPrint 到具有受信任证书的目标：**如果选中此限制，用户只能使用 AirPrint 打印到具有受信任证书的目标。默认设置为未选中。适用于运行 iOS 11（最低版本）的受监管设备。
- **添加 VPN 配置：**如果此限制设置为“**关闭**”，用户将无法创建 VPN 配置。默认设置为“**开启**”。适用于运行 iOS 11（最低版本）的受监管设备。
- **修改蜂窝数据套餐设置：**如果此限制设置为“**关闭**”，用户将无法修改蜂窝数据套餐设置。默认设置为“**开启**”。适用于运行 iOS 11（最低版本）的受监管设备。
- **移除系统应用：**如果此限制设置为“**关闭**”，用户将无法从其设备中移除系统应用。默认设置为“**开启**”。适用于运行 iOS 11（最低版本）的受监管设备。

- **设置新的附近设备：**如果此限制设置为“关闭”，用户将无法设置新的附近设备。默认设置为“开启”。适用于运行 iOS 11（最低版本）的受监管设备。
- **允许 USB 受限模式：** 如果设置为“**关**”，设备在锁定状态下始终可以连接 USB 配件。默认设置为“**开**”。仅适用于受监管的 iOS 11.3 及更高版本设备。
- **强制延迟软件更新：** 如果设置为“**开**”，则会延迟用户看到软件更新的时间。启用此限制后，用户在软件更新发布日期后的指定天数内不会看到软件更新。默认设置为“**关**”。仅适用于受监管的 iOS 11.3 及更高版本设备。
- **强制软件更新延迟（天）：** 允许您指定设备上软件更新的延迟天数。最大延迟为 **90** 天。默认延迟为 **30** 天。仅适用于受监管的 iOS 11.3 及更高版本设备。
- **强制课堂请求离开课程的权限：** 如果设置为“**开**”，则在 Classroom 中注册了非托管课程的学生在尝试离开课程时必须向老师请求权限。默认设置为“**关**”。仅适用于受监管的 iOS 11.3 及更高版本设备。
- **强制自动填充前进行身份验证：** 如果设置为“**开**”，则用户需要先进行身份验证，系统才能在 Safari 和应用程序中自动填充密码或信用卡信息。仅支持配备面容 ID 或触控 ID 的设备。默认设置为“**关**”。
- **强制自动日期和时间：** 允许您在受监管设备上自动设置日期和时间。如果设置为“**开**”，设备用户将无法在“**通用 > 日期与时间**”下关闭“**自动设置**”。设备上的时区仅在设备能够确定其位置时更新。也就是说，当设备具有蜂窝网络连接或启用了定位服务的 Wi-Fi 连接时。默认设置为“**关**”。仅适用于受监管的 iOS 12 及更高版本设备。
- **密码自动填充：** 可选。如果禁用，用户将无法使用“自动填充密码”或“自动强密码”功能。默认设置为“**开**”。适用于 iOS 12 及更高版本。
- **密码邻近请求：** 可选。如果禁用，用户的设备不会从附近的设备请求密码。默认设置为“**开**”。适用于 iOS 12 及更高版本。
- **密码共享：** 可选。如果禁用，用户将无法使用“隔空投送密码”功能共享其密码。默认设置为“**开**”。适用于 iOS 12 及更高版本。
- **修改个人热点设置：** 当个人热点设置为“**关**”时，禁用对其的修改。默认设置为“**开**”。
- **允许未配对设备启动到恢复模式：** 如果设置为“**开**”，则允许未配对设备将设备启动到恢复模式。默认设置为“**关**”。适用于 iOS 14.5 或更高版本。
- **安装快速安全响应：** 如果设置为“**关**”，则禁止安装快速安全响应。默认设置为“**开**”。
- **移除快速安全响应：** 如果设置为“**关**”，则禁止移除快速安全响应。默认设置为“**开**”。
- **允许邮件隐私保护：** 如果设置为“**关**”，则禁用设备上的邮件隐私保护。默认设置为“**开**”。适用于 iOS 15.2 或更高版本。
- **NFC：** 如果设置为“**关**”，则禁用 NFC。默认设置为“**开**”。适用于 iOS 14.2 或更高版本。

- **允许 App Clips**：如果设置为“**关闭**”，则阻止用户添加任何 App Clips 并移除设备上所有现有的 App Clips。默认设置为“**开启**”。适用于 iOS 14.0 或更高版本。
- **Genmoji**： 如果设置为“**关闭**”，则禁止创建新的 Genmoji。适用于 iOS 18 或更高版本。
- **图像游乐场**： 如果设置为“**关闭**”，则禁止使用图像生成功能。适用于 iOS 18 或更高版本。
- **图像魔杖**： 如果设置为“**关闭**”，则禁止使用图像魔杖。适用于 iOS 18 或更高版本。
- **iPhone 镜像**： 如果设置为“**关闭**”，则禁止使用 iPhone 镜像功能。在 iOS 上使用时，这会阻止 iPhone 镜像到任何 Mac。适用于 iOS 18 或更高版本。
- **个性化手写结果**： 如果设置为“**关闭**”，则阻止系统生成用户手写文本。适用于 iOS 18 或更高版本。
- **书写工具**： 如果设置为“**关闭**”，则禁用 Apple Intelligence 书写工具。适用于 iOS 18 或更高版本。
- **通话录音**： 如果设置为“**关闭**”，则禁用通话录音。需要受监管的设备。适用于 iOS 18.1 或更高版本。
- **要隐藏的应用程序**： 如果设置为“**关闭**”，则禁止用户隐藏应用程序。在 iOS 上使用时，这会阻止用户隐藏应用程序，但仍允许他们将应用程序留在 App 资源库中，同时将其从主屏幕移除。需要受监管的设备。适用于 iOS 18 或更高版本。
- **要锁定的应用程序**： 如果设置为“**关闭**”，则禁止用户锁定应用程序。在 iOS 上使用时，这会阻止用户锁定应用程序，因此也阻止隐藏应用程序。需要受监管的设备。适用于 iOS 18 或更高版本。
- **邮件摘要**： 如果设置为“**关闭**”，则禁止手动创建电子邮件摘要。在 iOS 上使用时，这不会影响自动摘要生成。需要受监管的设备。适用于 iOS 18.1 或更高版本。
- **RCS 消息**： 如果设置为“**关闭**”，则阻止使用 RCS 消息。需要受监管的设备。适用于 iOS 18.1 或更高版本。
- **允许外部智能集成**： 如果设置为“**关闭**”，则禁用 Siri 与外部基于云的智能服务的使用。默认设置为“**开启**”。适用于 iOS 18.2 及更高版本。
- **允许登录外部智能集成**： 如果设置为“**关闭**”，则强制外部智能提供商进入匿名模式。如果用户已登录外部智能提供商，则应用此限制将在下次尝试请求时导致其退出登录。默认设置为“**开启**”。适用于 iOS 18.2 及更高版本。
- **允许邮件智能回复**： 如果设置为“**关闭**”，则禁用邮件中的智能回复。默认设置为“**开启**”。适用于 iOS 18.2 及更高版本。
- **允许备忘录转录**： 如果设置为“**关**”，则禁用备忘录中的转录功能。默认设置为“**开**”。适用于 iOS 18.2 及更高版本。

- **允许 Safari 摘要：** 如果设置为“**关**”，系统将禁用 Safari 中内容摘要功能。默认设置为“**开**”。适用于 iOS 18.4 及更高版本。
- **允许视觉智能摘要：** 如果设置为“**关**”，系统将禁用视觉智能摘要功能。默认设置为“**开**”。适用于 iOS 18.3 及更高版本。
- **允许备忘录转录摘要：** 如果设置为“**关**”，则禁用备忘录中的转录摘要功能。默认设置为“**开**”。适用于 iOS 18.3 及更高版本。
- **允许 Apple 智能报告：** 如果设置为“**关**”，系统将禁用 Apple 智能报告。默认设置为“**开**”。适用于 iOS 18.4 及更高版本。
- **允许修改默认通话应用：** 如果设置为“**关**”，则禁用默认通话应用偏好设置的修改。应用此设置后，用于设置默认通话应用偏好设置的 MDM 设置命令仍然有效。默认设置为“**开**”。适用于 iOS 18.4 及更高版本。
- **允许修改默认消息应用：** 如果设置为“**关**”，则禁用默认消息应用偏好设置的修改。应用此设置后，用于设置默认消息应用偏好设置的 MDM 设置命令仍然有效。默认设置为“**开**”。适用于 iOS 18.4 及更高版本。
- **允许外部智能工作区 ID：** 一个字符串数组，但目前仅限于单个元素。如果存在，Apple 智能仅允许使用给定的外部集成工作区 ID，并且需要登录才能发出请求；用户将被要求登录支持登录的集成。多个负载使用交集操作进行组合。这意味着如果在多个负载中指定了冲突值，则允许的工作区 ID 集可能成为空集。适用于 iOS 18.3 及更高版本。
  - **外部智能工作区 ID：** 要添加外部智能工作区 ID，请单击“**添加**”，键入“**外部智能工作区 ID**”，然后单击“**保存**”。对要添加的每个工作区 ID 重复此过程。
- **默认浏览器修改：** 如果设置为“**关**”，则禁止修改默认浏览器偏好设置。在 iOS 上使用时，这仍然允许 MDM 设置命令设置默认浏览器偏好设置。需要受监督的设备。适用于 iOS 18.2 或更高版本。
- **允许实时语音邮件：** 如果设置为“**关**”，系统将禁用设备上的实时语音邮件。默认设置为“**开**”。适用于 iOS 17.2 及更高版本。

- **安全性 - 在锁定屏幕上显示**
  - **控制中心：** 允许在锁定屏幕上访问控制中心。控制中心允许用户轻松修改飞行模式、Wi-Fi、蓝牙、勿扰模式和锁定旋转设置。
  - **通知：** 允许在锁定屏幕上显示通知。
  - **今天视图：** 允许在锁定屏幕上显示“今天视图”，该视图聚合了天气和当天日历项等信息。
- **媒体内容 - 允许**
  - **露骨的音乐、播客和 iTunes U 材料：** 允许用户设备上出现露骨材料。

  - **iBooks 中的露骨色情内容：** 允许从 iBooks 下载露骨材料。
  - **评级区域：** 设置获取家长控制评级的区域。在列表中，单击一个国家/地区以设置评级区域。默认值为 **美国**。
  - **电影：** 设置是否允许用户设备上播放电影。如果允许播放电影，则可选择设置电影的评级级别。在列表中，单击一个选项以允许或限制设备上的电影。默认值为“允许所有电影”。
  - **电视节目：** 设置是否允许用户设备上播放电视节目。如果允许播放电视节目，则可选择设置电视节目的评级级别。在列表中，单击一个选项以允许或限制设备上的电视节目。默认值为“允许所有电视节目”。
  - **应用程序：** 设置是否允许用户设备上使用应用程序。如果允许使用应用程序，则可选择设置应用程序的评级级别。在列表中，单击一个选项以允许或限制设备上的应用程序。默认值为“允许所有应用程序”。

- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括 **选择日期** 和 **距离删除的持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **距离删除的持续时间（小时）：** 输入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。
  - **配置文件范围：** 选择此策略是应用于 **用户** 还是整个 **系统**。默认值为 **用户**。此选项仅适用于 iOS 9.3 及更高版本。

macOS 设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-restrictions-macos.png)

- **首选项**
  - **限制系统偏好设置中的项目：** 允许或限制用户访问系统偏好设置。默认值为**关闭**，允许用户完全访问系统偏好设置。如果启用，请配置以下设置。
    - **系统偏好设置面板：** 选择您选择的设置是启用还是禁用。默认是启用所有设置，这些设置默认处于**开启**状态。
      - 用户与群组
      - 通用
      - 辅助功能
      - 应用商店

- 软件更新
- 蓝牙
- CD 与 DVD
- 日期与时间
- 桌面与屏幕保护程序
- 显示器
- 程序坞
- 节能
- 扩展
- 光纤通道
- iCloud
- 墨水
- 互联网帐户
- 键盘
- 语言与文本
- 调度中心
- 鼠标
- 网络
- 通知
- 家长控制
- 打印机与扫描仪
- 描述文件
- 安全与隐私
- 共享
- 声音
- 发音与语音
- 聚焦
- 启动磁盘
- 时间机器
- 触控板

    - 艾克斯安

- **应用**
    - **允许使用 Game Center：** 允许用户通过 Game Center 玩在线游戏。默认设置为“**开**”。
    - **允许添加 Game Center 好友：** 允许用户向好友发送通知以玩游戏。默认设置为“**开**”。
    - **允许多人游戏：** 允许用户开始多人游戏。默认设置为“**开**”。
    - **允许修改 Game Center 帐户：** 允许用户修改其 Game Center 帐户设置。默认设置为“**开**”。
    - **允许 App Store 采用：** 允许或限制 App Store 采用 OS X 中已有的应用程序。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网站上的字段。默认设置为“**开**”。
    - **安装或更新应用需要管理员密码：** 安装或更新应用需要管理员密码。默认设置为“**关**”，这意味着不需要管理员密码。
    - **将 App Store 限制为仅软件更新：** 将 App Store 限制为仅更新，这将禁用 App Store 中的所有选项卡，除了“更新”。默认值为“**关**”，允许完全访问 App Store。
    - **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”，允许使用所有应用程序。如果启用，请配置以下设置：
        - **允许的应用程序：** 单击“**添加**”，输入允许启动的应用程序的名称和捆绑 ID，然后单击“**保存**”。对每个允许启动的应用程序重复此步骤。
        - **不允许的文件夹：** 单击“**添加**”，键入要限制用户访问的文件夹的文件路径（例如，/Applications/Utilities），然后单击“**保存**”。对所有不希望用户访问的文件夹重复此步骤。
        - **允许的文件夹：** 单击“**添加**”，键入要授予用户访问权限的文件夹的文件路径，然后单击“**保存**”。对所有希望用户访问的文件夹重复此步骤。

- **小组件**
    - **仅允许以下仪表板小组件运行：** 允许或限制用户可以运行的仪表板小组件，例如世界时钟或计算器。默认值为“**关**”，允许用户运行所有小组件。如果启用，请配置以下设置：
        - **允许的小组件：** 单击“**添加**”，键入允许运行的小组件的名称和 ID，然后单击“**保存**”。对要在仪表板上运行的每个小组件重复此步骤。

- **媒体**
    - **允许隔空投送：** 允许用户与附近的 iOS 设备共享照片、视频、网站、位置等。

- **共享**

- **自动启用新的共享服务：** 选择是否自动启用共享服务。
- **邮件：** 选择是否允许共享邮箱。
- **Facebook：** 选择是否允许共享 Facebook 帐户。
- **视频服务 - Flickr、Vimeo、土豆和优酷：** 选择是否允许共享视频服务。
- **添加到 Aperture：** 选择是否允许共享添加到 Aperture 的功能。
- **新浪微博：** 选择是否允许共享新浪微博帐户。
- **Twitter：** 选择是否允许共享 Twitter 帐户。
- **消息：** 选择是否允许共享访问消息。
- **添加到 iPhoto：** 选择是否允许共享添加到 iPhoto 的功能。
- **添加到阅读列表：** 选择是否允许共享添加到阅读列表的功能。
- **隔空投送 (AirDrop)：** 选择是否允许共享隔空投送帐户。

- **功能**
  - **锁定桌面图片：** 选择用户是否可以更改桌面图片。默认值为“**关**”，表示用户可以更改桌面图片。
  - **允许使用摄像头：** 选择用户是否可以在其 Mac 上使用摄像头。默认值为“**关**”，表示用户无法使用摄像头。
  - **允许 Apple Music：** 允许用户使用 Apple Music 服务（macOS 10.12 及更高版本）。如果不允许 Apple Music 服务，则“音乐”应用将以经典模式运行。仅适用于受监管的设备。默认值为“**开**”。
  - **允许 Spotlight 建议：** 选择用户是否可以使用 Spotlight 建议来搜索其 Mac，以及是否可以从互联网、iTunes 和 App Store 获取 Spotlight 建议。默认值为“**关**”，这会阻止用户使用 Spotlight 建议。
  - **允许查询：** 选择用户是否可以使用上下文菜单或 Spotlight 搜索菜单来查找单词定义。默认设置为“关闭”，这会阻止用户在其 Mac 上使用查询功能。
  - **允许本地帐户使用 iCloud 密码：** 选择用户是否可以使用其 Apple ID 和 iCloud 密码登录其 Mac。启用此策略意味着用户在其 Mac 上的*所有*登录屏幕都只使用一个 ID 和密码。默认值为“**开**”，这允许用户使用其 Apple ID 和 iCloud 密码访问其 Mac。
  - **允许 iCloud 文档和数据：** 选择是否允许用户在其 Mac 上访问存储在 iCloud 中的文档和数据。默认值为“**关**”，这会阻止用户在其 Mac 上使用 iCloud 文档和数据。
    - **允许 iCloud 桌面和文稿：** (macOS 10.12.4 及更高版本)。默认已选中。

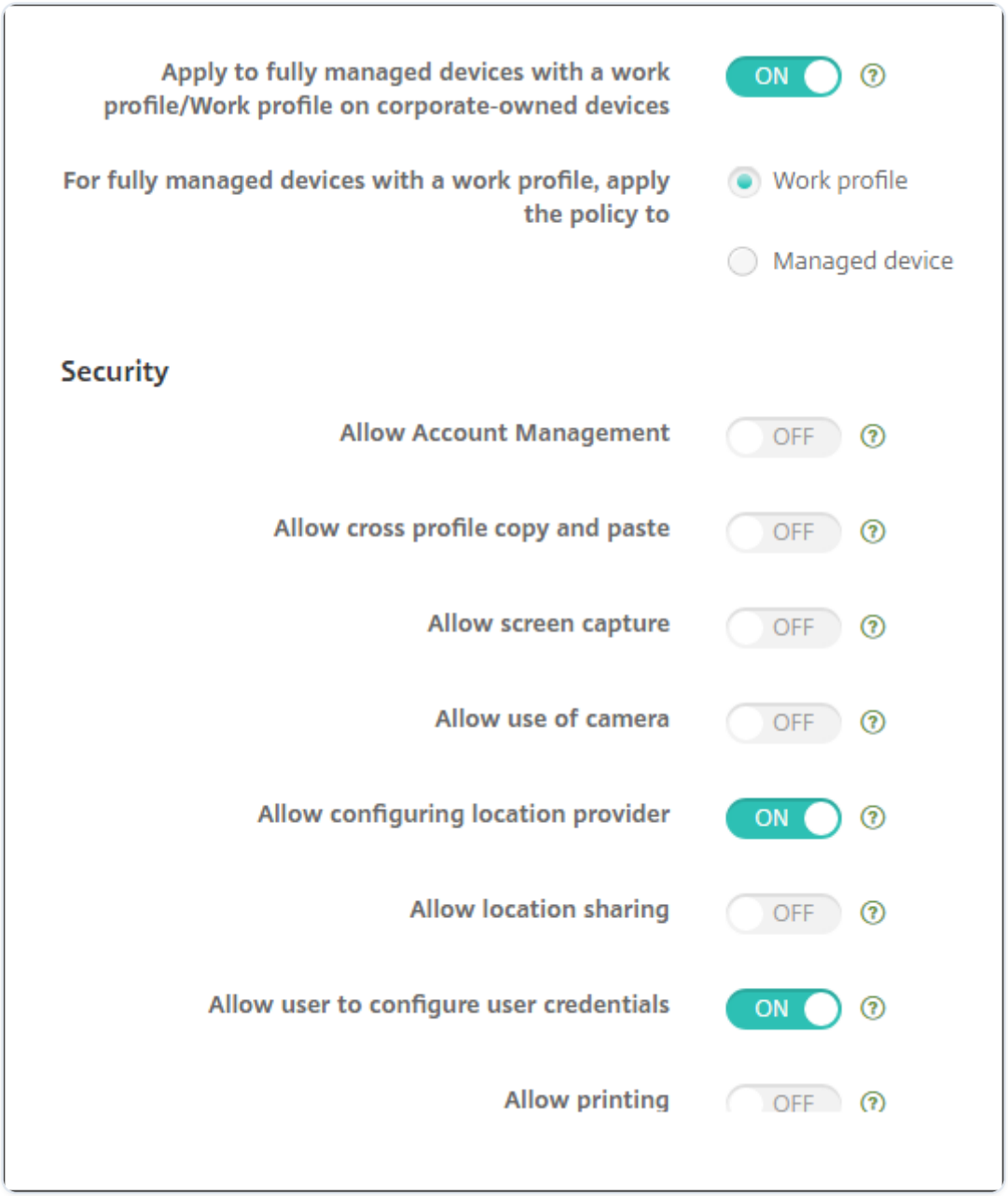
- **允许 iCloud 钥匙串同步：** 允许 iCloud 钥匙串同步 (macOS 10.12 及更高版本)。默认设置为 **开**。
- **允许 iCloud 邮件：** 允许用户使用 iCloud 邮件 (macOS 10.12 及更高版本)。默认设置为 **开**。
- **允许 iCloud 通讯录：** 允许用户使用 iCloud 通讯录 (macOS 10.12 及更高版本)。默认设置为 **开**。
- **允许 iCloud 日历：** 允许用户使用 iCloud 日历 (macOS 10.12 及更高版本)。默认设置为 **开**。
- **允许 iCloud 提醒事项：** 允许用户使用 iCloud 提醒事项 (macOS 10.12 及更高版本)。默认设置为 **开**。
- **允许 iCloud 书签：** 允许用户与 iCloud 书签同步 (macOS 10.12 及更高版本)。默认设置为 **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)。默认设置为 **开**。
- **允许 iCloud 照片：** 如果将此设置更改为 **关**，则任何未从 iCloud 照片图库完全下载的照片都将从本地设备存储中删除 (macOS 10.12 及更高版本)。默认设置为 **开**。
- **允许自动解锁：** 有关此选项和 Apple Watch 的信息，请参阅 https://www.imore.com/auto-unlock (macOS 10.12 及更高版本)。默认设置为 **开**。
- **允许使用触控 ID 解锁 Mac：** (macOS 10.12.4 及更高版本)。默认设置为 **开**。
- **强制延迟软件更新：** 如果设置为 **开**，此设置将延迟用户看到软件更新的时间。用户在软件更新发布日期后的指定天数内不会看到软件更新。默认设置为 **关**。仅适用于运行 macOS 10.13.4 及更高版本的受监管设备。
- **强制软件更新延迟（天）：** 指定在设备上延迟软件更新的天数。最大值为 90 天。默认值为 **30**。仅适用于运行 macOS 10.13.4 及更高版本的受监管设备。
- **密码自动填充：** 可选。如果禁用，用户将无法使用“自动填充密码”或“自动强密码”功能。默认设置为 **开**。适用于 macOS 10.14 及更高版本。
- **密码邻近请求：** 可选。如果禁用，用户的设备将不会从附近的设备请求密码。默认设置为 **开**。适用于 macOS 10.14 及更高版本。
- **密码共享：** 可选。如果禁用，用户无法使用隔空投送密码功能共享其密码。默认值为“**开**”。适用于 macOS 10.14 及更高版本。
- **图像游乐场：** 如果“**关**”，则禁止使用图像生成功能。默认值为“**开**”。仅适用于运行 macOS 15 及更高版本的受监督设备。

- **iPhone 镜像：** 如果“**关**”，则禁止使用 iPhone 镜像功能。在 macOS 上使用时，这会阻止 Mac 镜像任何 iPhone。默认值为“**开**”。仅适用于运行 macOS 15 及更高版本的受监督设备。
- **写作工具：** 如果“**关**”，则禁用 Apple Intelligence 写作工具。默认值为“**开**”。仅适用于运行 macOS 15 及更高版本的受监督设备。
- **允许媒体共享修改：** 如果“**关**”，则阻止修改媒体共享设置。默认值为“**开**”。适用于 macOS 15.1 及更高版本。
- **强制绕过屏幕捕获警报：** 如果“**开**”，则绕过屏幕捕获警报的显示。默认值为“**关**”。适用于 macOS 15.1 及更高版本。
- **邮件摘要：** 如果“**关**”，则禁用手动创建电子邮件摘要的功能。这不影响自动摘要生成。默认值为“**开**”。适用于 macOS 15.1 或更高版本。

Android 设置

- **摄像头：** 允许用户在其设备上使用摄像头。如果“**关**”，则摄像头被禁用。默认值为“**开**”。

安卓企业版设置



当新的或恢复出厂设置的 Android 设备注册到工作配置文件模式时，运行 Android 9.0-10.x 的设备将注册为带有工作配置文件的完全托管设备。运行 Android 11+ 的设备将注册为公司拥有设备上的工作配置文件。限制策略可以应用于设备上的工作配置文件或托管设备。

在注册到公司拥有设备上的工作配置文件模式的设备上，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
- 防止键盘锁锁定设备
- 允许使用状态栏
- 保持设备屏幕常亮

- 允许用户控制应用程序设置
- 允许用户配置用户凭据
- 允许 VPN 配置
- 允许 USB 大容量存储
- 允许恢复出厂设置
- 允许应用卸载
- 从工作和个人配置文件访问电子邮件应用
- 允许非 Google Play 应用
- 允许跨配置文件复制和粘贴
- 启用应用验证
- 允许帐户管理
- 允许打印
- 允许 NFC
- 允许添加用户

默认情况下，当设备以工作配置文件模式注册到 Android Enterprise 时，设备上的 **USB 调试和未知来源**设置会被禁用。

对于运行 Android 9.0-10.x 和 Samsung Knox 3.0 及更高版本的设备，请在**Android Enterprise**页面上配置 Samsung Knox 和 Samsung SAFE 的设置。对于运行早期版本 Android 或 Samsung Knox 的设备，请使用**Samsung Knox**和**Samsung SAFE**页面。

Samsung 限制不适用于以公司拥有设备上的工作配置文件模式注册的设备。使用 Knox Service Plugin (KSP) 将 Samsung 限制应用于这些设备。有关详细信息，请参阅Samsung 文档。

建议您使用 Samsung Knox 3.4 或更高版本以获取最新的 Samsung Knox 管理功能。

- **应用于具有工作配置文件的完全托管设备/公司拥有设备上的工作配置文件：** 允许为具有工作配置文件的完全托管设备配置限制策略设置。当此设置为**开**时，请选择以下设置之一：
  - **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。

  当此设置为**关**时，您配置的凭据设置将应用于设备，但明确应用于工作配置文件的设置除外。默认值为**关**。

当**应用于具有工作配置文件的完全托管设备/公司拥有设备上的工作配置文件**为关时，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添加帐户。默认值为**关**。
  - **允许跨配置文件复制和粘贴：** 如果设置为**开**，用户可以在 Android Enterprise 配置文件中的应用和个人区域中的应用之间复制和粘贴。默认值为**关**。
  - **允许屏幕捕获：** 允许用户录制或捕获设备屏幕。默认值为**关**。
  - **允许使用摄像头：** 允许用户使用设备摄像头拍照和录制视频。默认设置为**关闭**。
  - **允许 VPN 配置：** 允许用户创建 VPN 配置。适用于运行 Android 6 及更高版本的工作配置文件设备和完全托管设备。默认设置为**开启**。
  - **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。默认设置为**开启**。
  - **允许 NFC：** 允许用户使用近场通信 (NFC) 将网页、照片、视频或其他内容从其设备发送到另一台设备。适用于 MDM 4.0 及更高版本。默认设置为**开启**。
  - **允许配置位置提供程序：** 允许用户在其设备上开启 GPS。适用于 Android API 28 及更高版本。默认设置为**开启**。
  - **允许位置共享：** 对于托管配置文件，设备所有者可以覆盖此设置。默认设置为**关闭**。

    > **提示：**
    >
    > 您可以在 XenMobile 中创建位置设备策略以强制执行地理边界。请参阅位置设备策略。

  - **允许用户配置用户凭据：** 指定用户是否可以在托管密钥库中配置凭据。默认设置为**开启**。
  - **允许打印：** 如果设置为**开启**，则允许用户打印到用户设备可访问的任何打印机。默认设置为**关闭**。适用于：Android 9 及更高版本。
  - **允许 USB 调试：** 默认设置为**关闭**。
- **应用程序**
  - **启用系统应用程序：** 允许用户运行预安装的设备应用程序。默认设置为**关闭**。要启用特定应用程序，请在**系统应用程序列表**表中单击**添加**。
    - **系统应用程序列表：** 您要在设备上启用的系统应用程序列表。将**启用系统应用程序**设置为**开启**并添加应用程序包名称。要查找系统应用程序的包名称，您可以使用 Android 调

试桥 (`adb`) 调用 Android 包管理器 (`pm`) 命令。例如， `adb shell "pm list packages -f name"` ，其中“name”是包名称的一部分。有关详细信息，请参阅 `<https://developer.android.com/studio/command-line/adb>` 。对于 Android Enterprise 设备，您可以使用Android Enterprise 应用程序权限策略限制应用程序权限。

- **禁用应用程序：** 阻止指定列表中的应用程序在设备上运行。默认设置为**关闭**。要禁用已安装的应用程序，请将设置更改为**开启**，然后在**应用程序列表**表中单击**添加**。
  - **应用程序列表**：您要阻止的应用程序列表。将**禁用应用程序**设置为**开**，然后添加应用程序。键入应用程序包名称。更改和部署应用程序列表会覆盖先前的应用程序列表。例如：如果您禁用 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，XenMobile 将启用 com.example.2。
- **启用应用验证**：使操作系统能够扫描应用以检测恶意行为。默认值为**开**。
- **启用 Google 应用**：允许用户从 Google 移动服务下载应用到设备。默认值为**开**。
- **允许非 Google Play 应用**：允许安装来自 Google Play 以外商店的应用。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、禁用应用、清除缓存和数据、强制停止任何应用以及清除默认设置。用户通过“设置”应用执行这些操作。默认值为**关**。
- **允许应用卸载**：允许用户从托管的 Google Play 商店中卸载应用。默认值为**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。
- **从工作和个人配置文件访问电子邮件应用**：当此设置为**开**时，允许用户从个人配置文件访问和使用工作配置文件电子邮件应用。默认值为**关**。

- **BYOD 工作配置文件**
  - **允许工作配置文件应用小组件显示在主屏幕上**：如果此设置为**开**，用户可以将工作配置文件应用小组件放置在设备主屏幕上。如果此设置为**关**，用户无法将工作配置文件应用小组件放置在设备主屏幕上。默认值为**关**。
    - **允许小组件的应用**：您要允许在主屏幕上显示的应用列表。将**允许工作配置文件应用小组件显示在主屏幕上**设置为**开**，然后添加应用。单击**添加**，然后从列表中选择要在主屏幕上允许其小组件的应用。单击**保存**。重复此过程以允许更多应用小组件。
  - **允许设备联系人中显示工作配置文件联系人**：在父配置文件中显示来自托管 Android Enterprise 配置文件的联系人，用于来电（Android 7.0 及更高版本）。默认值为**关**。
- **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蜂窝数据。默认值为“关”，这将禁用用户设备上的漫游。默认值为**关**。
- **允许短信**：允许用户发送和接收短信。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（也称为 COSU 设备）上启用状态栏。此设置会禁用通知、快速设置以及其他允许从全屏模式退出的屏幕叠加层。用户可以转到系统设置并查看通知。适用于 Android 6.0 及更高版本。默认值为“**关**”。
- **允许蓝牙：** 允许用户使用蓝牙。默认值为“**开**”。
  - **允许蓝牙共享：** 如果未选中，用户无法在其设备上建立传出蓝牙共享。默认值为选中。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的更多信息，请参阅服务器属性。
- **允许配置日期和时间：** 允许用户更改其设备上的日期和时间。默认值为“**开**”。
- **允许恢复出厂设置：** 允许用户对其设备执行恢复出厂设置。默认值为“**开**”。
- **保持设备屏幕常亮：** 如果此设置为“**开**”，则当设备插入电源时，设备屏幕将保持常亮。默认值为“**关**”。
- **允许 USB 大容量存储：** 允许通过 USB 连接在用户设备和计算机之间传输大型数据文件。默认值为“**开**”。
- **允许麦克风：** 允许用户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共享数据。默认值为“**关**”。
- **防止按键锁定设备：** 如果为“**开**”，此设置将在托管设备和专用设备（也称为 COSU 设备）的锁定屏幕上禁用按键锁定。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 传输文件。默认值为“**关**”。

- **三星**
  - **启用 TIMA 密钥库：** TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书将路由到默认密钥库提供程序进行存储。默认值为“**关**”。
  - **允许共享列表：** 允许用户在“通过以下方式共享”列表中在应用程序之间共享内容。默认值为“**开**”。
  - **启用审计日志：** 启用事件审计日志的创建，用于设备的取证分析。默认设置为“**关闭**”。
- **三星：仅限完全托管设备**

- **启用 ODE 可信启动验证：** 使用 ODE 可信启动验证，从引导加载程序到系统映像建立信任链。默认设置为“**开启**”。
- **仅允许紧急呼叫：** 允许用户在其设备上启用“仅限紧急呼叫”模式。默认设置为“**关闭**”。
- **允许固件恢复：** 允许用户在其设备上恢复固件。默认设置为“**开启**”。
- **允许快速加密：** 仅允许加密已使用的内存空间。这种加密与完全磁盘加密不同，后者会加密所有数据。这些数据包括设置、应用程序数据、下载的文件和应用程序、媒体以及其他文件。默认设置为“**开启**”。
- **启用通用标准模式：** 将设备置于通用标准模式。通用标准配置强制执行严格的安全流程。默认设置为“**开启**”。
- **启用重启横幅：** 在用户设备重启时显示经 DoD 批准的系统使用通知消息或横幅。默认设置为“**关闭**”。
- **允许更改设置：** 允许用户在其完全托管设备上更改设置。默认设置为“**开启**”。
- **启用后台数据使用：** 允许应用程序在后台同步数据。适用于完全托管设备。默认设置为“**开启**”。
- **允许剪贴板：** 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计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。
- **允许主页键：** 允许用户在其完全托管设备上使用“**主页**”键。默认设置为“**开启**”。
- **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。默认设置为“**关闭**”。
- **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）。默认设置为“**开启**”。
- **允许关机：** 允许用户关闭其完全托管的设备 (MDM 3.0 及更高版本)。默认值为“**开**”。
- **允许 Wi-Fi 直连：** 允许用户通过其 Wi-Fi 连接直接连接到另一台设备。默认值为“**开**”。如果为“**开**”，则必须启用“**允许 Wi-Fi 更改**”设置。
- **允许 SD 卡：** 允许用户在其设备上使用 SD 卡（如果可用）。默认值为“**开**”。
- **允许 USB 主机存储：** 允许用户的设备在 USB 设备连接到其设备时充当 USB 主机。用户的设备随后向 USB 设备供电。默认值为“**开**”。
- **允许语音拨号器：** 允许用户在其设备上使用语音拨号器 (MDM 4.0 及更高版本)。默认值为“**开**”。
- **允许 S Beam：** 允许用户使用 NFC 和 Wi-Fi Direct 与他人共享内容 (MDM 4.0 及更高版本)。默认值为“**开**”。

- **允许 S Voice：** 允许用户在其设备上使用智能个人助理和知识导航器 (MDM 4.0 及更高版本)。默认值为“**开**”。
- **允许 USB 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：** 如果未选中，用户无法在其设备上建立出站蓝牙共享。默认值为选中。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的更多信息，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**”。
- **允许接收彩信：** 允许用户接收彩信。默认值为“**关**”。如果为“**开**”，则必须打开“**允许短信**”设置。
- **允许发送彩信：** 允许用户发送彩信。默认值为“**关**”。如果为“**开**”，则必须打开“**允许短信**”设置。
- **允许接收短信：** 允许用户接收短信。默认值为“**关**”。如果为“**开**”，则必须打开“**允许短信**”设置。
- **允许发送短信：** 允许用户发送短信。默认值为“**关**”。如果为“**开**”，则必须打开“**允许短信**”设置。
- **配置移动网络：** 允许用户使用其蜂窝数据连接。默认设置为**关闭**。
- **每日限制 (MB)：** 输入用户每天可使用的移动数据量（以 MB 为单位）。默认值为 0，这将禁用此功能（MDM 4.0 及更高版本）。
- **每周限制 (MB)：** 输入用户每周可使用的移动数据量（以 MB 为单位）。默认值为 0，这将禁用此功能（MDM 4.0 及更高版本）。
- **每月限制 (MB)：** 输入用户每月可使用的移动数据量（以 MB 为单位）。默认值为 0，这将禁用此功能（MDM 4.0 及更高版本）。
- **仅允许安全的 VPN 连接：** 允许用户仅使用安全连接（MDM 4.0 及更高版本）。默认设置为**开启**。
- **允许录音：** 允许用户使用其设备录制音频（MDM 4.0 及更高版本）。默认设置为**开启**。如果设置为**开启**，则必须开启**允许麦克风**设置。
- **允许录像：** 允许用户使用其设备录制视频（MDM 4.0 及更高版本）。默认设置为**关闭**。如果设置为**开启**，则必须开启**允许使用摄像头**设置。

  - **漫游时允许推送消息：** 允许用户在漫游时使用蜂窝数据进行推送。默认设置为**关闭**。如果设置为**开启**，则必须启用**允许数据漫游**设置。
  - **漫游时允许自动同步：** 允许用户在漫游时使用蜂窝数据进行同步。默认设置为**关闭**。如果设置为**开启**，则必须启用**允许数据漫游**设置。
  - **漫游时允许语音通话：** 允许用户在漫游时使用蜂窝数据进行语音通话。默认设置为**关闭**。如果设置为**开启**，则必须启用**允许数据漫游**设置。
- **三星: 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。默认设置为**关闭**。
- **Samsung：仅限 Knox 容器**
  - **将应用程序移动到容器：** 允许用户在其设备上的 Knox 容器和个人区域之间移动应用程序。默认设置为**开启**。
  - **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（例如密码或 PIN）才能打开其设备。默认设置为**开启**。
  - **强制容器身份验证：** 使用与解锁设备不同的身份验证方法来打开 KNOX 容器。默认值为 **开**。
  - **启用安全键盘：** 强制用户在 Knox 容器内使用安全键盘。默认值为 **开**。
- **三星：DeX**
  - **启用 Samsung DeX：** 使受支持的启用 Knox 的设备能够在 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 Developers 文档。
    - **仅在 DeX 模式下允许以太网：** 启用在 Samsung DeX 模式下使用以太网。蜂窝数据、Wi-Fi 和网络共享（Wi-Fi、蓝牙和 USB）在 DeX 模式下受到限制。默认值为未选中。
    - **上传 DeX 徽标图像：** 选择此设置以指定一个 .png 图像作为 Samsung DeX 的图标。
    - **DeX 屏幕超时（秒）：** 指定 DeX 屏幕关闭前的空闲时间（以秒为单位）。要禁用超时，请键入 **0**。默认值为 **1200** 秒（20 分钟）。
    - **在 Samsung DeX 中添加应用快捷方式：** 指定一个应用包名称，以便为该应用添加 DeX 快捷方式。要查找应用包名称，请转到 Google Play 并选择该应用。URL 包含包名称：`https://play.google.com/store/apps/details?id=<package.name>`。
    - **在 Samsung DeX 中移除应用快捷方式：** 指定一个应用包名称，以便从 DeX 中移除快捷方式。转到 Google Play 查找应用包名称。

- **要在 Samsung DeX 中禁用的应用包：** 指定一个逗号分隔的应用包列表，您希望在 Samsung DeX 模式下阻止这些应用包。例如：`"com.android.chrome", "com.google.android.gm"`。

当 **应用于具有工作资料的完全托管设备** 处于开启状态且 **对于具有工作资料的完全托管设备，将策略应用于** 设置为 **工作资料** 时，请配置以下设置：

- **安全性**
  - **允许帐户管理：** 允许在工作资料和托管设备中添加帐户。默认值为 **关**。
  - **允许跨资料复制和粘贴：** 如果设置为 **开**，用户可以在 Android Enterprise 资料中的应用和个人区域中的应用之间复制和粘贴。默认值为 **关**。
  - **允许屏幕捕获：** 允许用户录制或截取设备屏幕。默认值为 **关**。
  - **允许使用摄像头：** 允许用户使用设备摄像头拍照和录制视频。默认设置为“**关闭**”。
  - **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。默认设置为“**开启**”。
  - **允许位置共享：** 对于托管配置文件，设备所有者可以覆盖此设置。默认设置为“**关闭**”。

    > **提示：**
    >
    > 您可以在 XenMobile 中创建位置设备策略以强制执行地理边界。请参阅位置设备策略。

  - **允许用户配置用户凭据：** 指定用户是否可以在托管密钥库中配置凭据。默认设置为“**开启**”。
  - **允许打印：** 如果设置为“**开启**”，则此设置允许用户打印到可从用户设备访问的任何打印机。默认设置为“**关闭**”。适用于：Android 9 及更高版本。
- **应用程序**
  - **启用系统应用程序：** 允许用户运行预安装的设备应用程序。默认设置为“**关闭**”。要启用特定应用程序，请在“**系统应用程序列表**”表中单击“**添加**”。
    - **系统应用程序列表：** 您要在设备上启用的系统应用程序列表。将“**启用系统应用程序**”设置为“**开启**”，然后添加应用程序包名称。要查找系统应用程序的包名称，可以使用 Android 调试桥 (`adb`) 调用 Android 包管理器 (`pm`) 命令。例如，`adb shell "pm list packages -f name"`，其中“name”是包名称的一部分。有关详细信息，请参阅

`<https://developer.android.com/studio/command-line/adb>`。对于 Android Enterprise 设备，您可以使用Android Enterprise 应用程序权限 策略限制应用程序权限。

- **禁用应用程序：** 阻止指定列表中的应用程序在设备上运行。默认设置为“**关闭**”。要禁用已安装的应用程序，请将设置更改为“**开启**”，然后在“**应用程序列表**”表中单击“**添加**”。
  - **应用程序列表：** 您要阻止的应用程序列表。将“**禁用应用程序**”设置为“**开启**”，然后添加应用程序。键入应用程序包名称。更改和部署应用程序列表会覆盖先前的应用程序列表。例如：如果您禁用 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，则 XenMobile 会启用 com.example.2。
- **启用应用程序验证：** 使操作系统能够扫描应用程序以检测恶意行为。默认设置为“**开启**”。
- **启用 Google 应用程序：** 允许用户从 Google 移动服务下载应用程序到设备。默认设置为“**开启**”。
- **允许非 Google Play 应用程序：** 允许安装来自 Google Play 以外商店的应用程序。默认设置为“**关闭**”。
- **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。用户可以通过“设置”应用程序执行这些操作。默认设置为 **关**。
- **允许卸载应用程序：** 允许用户从托管的 Google Play 商店中卸载应用程序。默认设置为 **关**。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的更多信息，请参阅服务器属性。
- **从工作和个人配置文件访问电子邮件应用程序：** 当设置为 **开** 时，允许用户从其个人配置文件访问和使用工作配置文件电子邮件应用程序。默认设置为 **关**。

- **BYOD 工作配置文件**
  - **允许工作配置文件应用程序小组件在主屏幕上显示：** 如果此设置为 **开**，用户可以将工作配置文件应用程序小组件放置在设备主屏幕上。如果此设置为 **关**，用户无法将工作配置文件应用程序小组件放置在设备主屏幕上。默认设置为 **关**。
    - **允许使用小组件的应用程序：** 您希望在主屏幕上允许的应用程序列表。将 **允许工作配置文件应用程序小组件在主屏幕上显示** 设置为 **开** 并添加应用程序。单击 **添加**，然后从列表中选择一个您希望其小组件在主屏幕上显示的应用程序。单击 **保存**。重复此过程以允许更多应用程序小组件。
  - **允许设备联系人中包含工作配置文件联系人：** 在父配置文件中显示来自托管 Android Enterprise 配置文件的联系人，用于来电（Android 7.0 及更高版本）。默认设置为 **关**。
- **三星**

  - **启用 TIMA 密钥库：** TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书将路由到默认密钥库提供程序进行存储。默认设置为 **关**。
  - **允许共享列表：** 允许用户在“共享方式”列表中在应用程序之间共享内容。默认设置为 **开**。
  - **启用审计日志：** 启用事件审计日志的创建，用于设备的取证分析。默认设置为 **关**。
- **三星：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。默认设置为 **关**。
- **三星：仅限 Knox 容器**
  - **将应用程序移动到容器：** 允许用户在其设备上的 Knox 容器和个人区域之间移动应用程序。默认设置为 **开**。
  - **强制多因素身份验证：** 用户必须使用指纹和另一种身份验证方法（例如密码或PIN）来打开其设备。默认设置为**开**。
  - **强制容器身份验证：** 使用与解锁设备不同的身份验证方法来打开KNOX容器。默认设置为**开**。
  - **启用安全键盘：** 强制用户在Knox容器内使用安全键盘。默认设置为**开**。

当**应用于具有工作资料的完全托管设备**为“开”且**对于具有工作资料的完全托管设备，将策略应用于**设置为**托管设备**时，请配置以下设置：

- **安全性**
  - **允许帐户管理：** 允许在工作资料和托管设备中添加帐户。默认设置为**关**。
  - **允许跨配置文件复制和粘贴：** 如果设置为**开**，用户可以在Android Enterprise配置文件中的应用程序和个人区域中的应用程序之间复制和粘贴。默认设置为**关**。
  - **允许屏幕截图：** 允许用户录制或截取设备屏幕。默认设置为**关**。
  - **允许使用摄像头：** 允许用户使用设备摄像头拍照和录制视频。默认设置为**关**。
  - **允许VPN配置：** 允许用户创建VPN配置。适用于运行Android 6及更高版本的工作资料设备和完全托管设备。默认设置为**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。默认设置为**开**。
  - **允许NFC：** 允许用户使用近场通信(NFC)将其设备上的网页、照片、视频或其他内容发送到另一台设备。适用于MDM 4.0及更高版本。默认设置为**开**。
  - **允许配置位置提供程序：** 允许用户在其设备上开启GPS。适用于Android API 28及更高版本。默认设置为**开**。
  - **允许位置共享：** 对于托管配置文件，设备所有者可以覆盖此设置。默认设置为**关**。

> **提示：**
>
> 您可以在 XenMobile 中创建位置设备策略以强制执行地理边界。请参阅位置设备策略。

- **允许用户配置用户凭据：** 指定用户是否可以在托管密钥库中配置凭据。默认值为“**开**”。
- **允许打印：** 如果设置为“**开**”，则此设置允许用户打印到可从用户设备访问的任何打印机。默认值为“**关**”。适用于：Android 9 及更高版本。
- **允许 USB 调试：** 默认值为“**关**”。

- **应用程序**
  - **启用系统应用程序：** 允许用户运行预安装的设备应用程序。默认值为“**关**”。要启用特定应用程序，请在“**系统应用程序列表**”表中单击“**添加**”。
    - **系统应用程序列表：** 设备上要启用的系统应用程序列表。将“**启用系统应用程序**”设置为“**开**”并添加应用程序包名称。要查找系统应用程序的包名称，可以使用 Android 调试桥 (`adb`) 调用 Android 包管理器 (`pm`) 命令。例如，`adb shell "pm list packages -f name"`，其中“name”是包名称的一部分。有关详细信息，请参阅 `<https://developer.android.com/studio/command-line/adb>`。对于 Android Enterprise 设备，您可以使用 Android Enterprise 应用程序权限 策略限制应用程序权限。
  - **禁用应用程序：** 阻止指定列表中的应用程序在设备上运行。默认值为“**关**”。要禁用已安装的应用程序，请将设置更改为“**开**”，然后在“**应用程序列表**”表中单击“**添加**”。
    - **应用程序列表：** 要阻止的应用程序列表。将“**禁用应用程序**”设置为“**开**”并添加应用程序。键入应用程序包名称。更改和部署应用程序列表会覆盖先前的应用程序列表。例如：如果您禁用 com.example1 和 com.example2，然后将列表更改为 com.example1 和 com.example3，则 XenMobile 会启用 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：** 允许用户从 Google 移动服务下载应用程序到设备。默认值为“**开**”。
  - **允许非 Google Play 应用程序：** 允许安装来自 Google Play 以外商店的应用程序。默认值为“**关**”。

- **允许用户控制应用程序设置：** 允许用户卸载应用程序、禁用应用程序、清除缓存和数据、强制停止任何应用程序以及清除默认设置。用户通过“设置”应用程序执行这些操作。默认值为“**关**”。
- **允许应用程序卸载：** 允许用户从托管 Google Play 商店中卸载应用程序。默认值为“**关**”。要显示此设置，请启用服务器属性 `afw.restriction.policy.v2`。有关服务器属性的更多信息，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蜂窝数据。默认值为“关”，这会禁用用户设备上的漫游。默认值为“**关**”。
  - **允许短信：** 允许用户发送和接收短信。默认值为“**关**”。
  - **允许使用状态栏：** 如果设置为“**开**”，此设置将在托管设备和专用设备（也称为 COSU 设备）上启用状态栏。此设置会禁用通知、快速设置以及其他允许从全屏模式退出的屏幕叠加层。用户可以转到系统设置并查看通知。适用于 Android 6.0 及更高版本。默认值为“**关**”。
  - **允许蓝牙：** 允许用户使用蓝牙。默认值为“**开**”。
    - **允许蓝牙共享：** 如果未选中，用户无法在其设备上建立出站蓝牙共享。默认值为选中。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：** 允许用户更改其设备上的日期和时间。默认值为“**开**”。
  - **允许恢复出厂设置：** 允许用户对其设备执行恢复出厂设置。默认值为“**开**”。
  - **保持设备屏幕常亮：** 如果此设置设置为“**开**”，则设备插入电源时屏幕将保持常亮。默认值为“**关**”。
  - **允许 USB 大容量存储：** 允许通过 USB 连接在用户设备和计算机之间传输大型数据文件。默认值为“**开**”。
  - **允许麦克风：** 允许用户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共享数据。默认值为“**关**”。当此设置开启时，以下设置适用于三星设备：
  - **防止键盘锁锁定设备：** 如果设置为“**开**”，此设置将禁用托管设备和专用设备（也称为 COSU 设备）锁屏上的键盘锁。默认值为“**关**”。
  - **允许更改 Wi-Fi：** 如果设置为“**开**”，用户可以打开或关闭 Wi-Fi 并连接到 Wi-Fi 网络。默认值为“**开**”。
  - **允许文件传输：** 允许通过 USB 传输文件。默认值为“**关**”。

- **三星**
  - **启用 TIMA 密钥库：** TIMA 密钥库为对称密钥提供基于 TrustZone 的安全密钥存储。RSA 密钥对和证书将路由到默认密钥存储提供程序进行存储。默认值为“**关**”。
  - **允许共享列表：** 允许用户在“通过共享”列表中在应用程序之间共享内容。默认值为“**开**”。
  - **启用审核日志：** 启用事件审核日志的创建，以便对设备进行取证分析。默认值为“**关**”。
- **三星：仅限完全托管设备**
  - **启用 ODE 可信启动验证：** 使用 ODE 可信启动验证建立从引导加载程序到系统映像的信任链。默认值为“**开**”。
  - **仅允许紧急呼叫：** 允许用户在其设备上启用“仅紧急呼叫”模式。默认值为“**关**”。
  - **允许固件恢复：** 允许用户恢复其设备上的固件。默认值为“**开**”。
  - **允许快速加密：** 仅允许加密已使用的内存空间。此加密与完全磁盘加密不同，后者会加密所有数据。这些数据包括设置、应用程序数据、下载的文件和应用程序、媒体以及其他文件。默认值为“**开**”。
  - **启用通用标准模式：** 将设备置于通用标准模式。通用标准配置强制执行严格的安全流程。默认值为“**开**”。
  - **启用重新启动横幅：** 在用户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**”。
  - **允许剪贴板：** 允许用户将数据复制到其设备上的剪贴板。默认值为“**开**”。
    - **允许剪贴板共享：** 允许用户在其设备和计算机之间共享剪贴板内容（MDM 4.0 及更高版本）。
  - **允许主页键：** 允许用户在其完全托管的设备上使用**主页**键。默认值为**开**。
  - **允许模拟位置：** 允许用户伪造其 GPS 位置。适用于完全托管的设备。默认值为**关**。
  - **NFC：** 允许用户在其完全托管的设备上使用 NFC (MDM 3.0 及更高版本)。默认值为**开**。
  - **允许关机：** 允许用户关闭其完全托管的设备 (MDM 3.0 及更高版本)。默认值为**开**。
  - **允许 Wi-Fi 直连：** 允许用户通过其 Wi-Fi 连接直接连接到另一台设备。默认值为**开**。如果为**开**，则必须启用**允许 Wi-Fi 更改**设置。
  - **允许 SD 卡：** 允许用户在其设备上使用 SD 卡（如果可用）。默认值为**开**。

- **允许 USB 主机存储：** 允许用户的设备在 USB 设备连接到其设备时充当 USB 主机。用户的设备随后向 USB 设备供电。默认值为**开**。
- **允许语音拨号器：** 允许用户在其设备上使用语音拨号器 (MDM 4.0 及更高版本)。默认值为**开**。
- **允许 S Beam：** 允许用户使用 NFC 和 Wi-Fi Direct 与他人共享内容 (MDM 4.0 及更高版本)。默认值为**开**。
- **允许 S Voice：** 允许用户在其设备上使用智能个人助理和知识导航器 (MDM 4.0 及更高版本)。默认值为**开**。
- **允许 USB 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**。
- **允许接收彩信：** 允许用户接收彩信。默认值为**关**。如果为**开**，则必须启用**允许短信**设置。
- **允许发送彩信：** 允许用户发送彩信。默认值为**关**。如果为**开**，则必须启用**允许短信**设置。
- **允许接收短信：** 允许用户接收短信。默认值为“**关**”。如果为“**开**”，则必须启用“**允许短信**”设置。
- **允许发送短信：** 允许用户发送短信。默认值为“**关**”。如果为“**开**”，则必须启用“**允许短信**”设置。
- **配置移动网络：** 允许用户使用其蜂窝数据连接。默认值为“**关**”。
- **每日限制 (MB)：** 输入用户每天可使用的移动数据量（以 MB 为单位）。默认值为 0，这将禁用此功能（MDM 4.0 及更高版本）。
- **每周限制 (MB)：** 输入用户每周可使用的移动数据量（以 MB 为单位）。默认值为 0，这将禁用此功能（MDM 4.0 及更高版本）。
- **每月限制 (MB)：** 输入用户每月可使用的移动数据量（以 MB 为单位）。默认值为 0，这将禁用此功能（MDM 4.0 及更高版本）。
- **仅允许安全的 VPN 连接：** 允许用户仅使用安全连接（MDM 4.0 及更高版本）。默认值为“**开**”。
- **允许录音：** 允许用户使用其设备录制音频（MDM 4.0 及更高版本）。默认值为“**开**”。如果为“**开**”，则必须启用“**允许麦克风**”设置。
- **允许录像：** 允许用户使用其设备录制视频（MDM 4.0 及更高版本）。默认值为“**关**”。如果为“**开**”，则必须启用“**允许使用摄像头**”设置。

- **漫游时允许推送消息：** 允许用户使用蜂窝数据进行推送。默认值为“**关**”。如果为“**开**”，则必须启用“**允许数据漫游**”设置。
- **漫游时允许自动同步：** 允许用户使用蜂窝数据进行同步。默认值为“**关**”。如果为“**开**”，则必须启用“**允许数据漫游**”设置。
- **漫游时允许语音通话：** 允许用户使用蜂窝数据进行语音通话。默认值为“**关**”。如果为“**开**”，则必须启用“**允许数据漫游**”设置。

- **三星：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**
  - **将应用移动到容器：** 允许用户在其设备上的 Knox 容器和个人区域之间移动应用。默认设置为“**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（例如密码或 PIN）来打开其设备。默认设置为“**开**”。
  - **强制执行容器身份验证：** 使用与解锁设备所用方法不同的身份验证方法来打开 KNOX 容器。默认设置为“**开**”。
  - **启用安全键盘：** 强制用户在 Knox 容器内使用安全键盘。默认设置为“**开**”。

Windows 桌面/平板电脑设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-restrictions-winphone.png)

- **Wi-Fi 设置**
  - **允许 Internet 共享：** 允许设备通过将其转换为 Wi-Fi 热点来与其他设备共享其 Internet 连接。
- **连接**
  - **允许通过蜂窝网络使用 VPN：** 允许设备通过 VPN 连接到蜂窝网络。
  - **允许在漫游时通过蜂窝网络使用 VPN：** 允许设备在蜂窝网络漫游时通过 VPN 连接。
  - **允许蜂窝数据漫游：** 允许用户在漫游时使用蜂窝数据。
- **帐户**
  - **允许 Microsoft 帐户连接：** 允许设备使用 Microsoft 帐户进行非电子邮件相关的连接身份验证和服务。
  - **允许非 Microsoft 电子邮件：** 允许用户添加非 Microsoft 电子邮件帐户。

- **系统**
  - **允许存储卡：** 允许设备使用存储卡。
  - **遥测：** 在下拉列表中选择一个选项，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，但次要数据请求除外**”。
  - **允许定位服务：** 允许定位服务。
  - **允许预览内部版本：** 允许用户预览 Microsoft 内部版本。
- **摄像头：**
  - **允许使用摄像头：** 允许用户使用其设备摄像头。
- **蓝牙：**
  - **允许可发现模式：** 允许蓝牙设备发现本地设备。
  - **本地设备名称：** 本地设备的名称。
- **体验：**
  - **允许 Cortana：** 允许用户访问 Cortana，即智能个人助理和知识导航器。
  - **允许设备发现：** 允许网络发现设备。
  - **允许手动取消 MDM 注册：** 允许用户手动将其设备从 XenMobile MDM 取消注册。
  - **允许同步设备设置：** 允许用户在漫游时在 Windows 10 和 Windows 11 设备之间同步设置。
- **锁屏上方：**
  - **允许浮动通知：** 允许在锁屏界面显示浮动通知。
- **应用程序**
  - **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。
- **隐私：**
  - **允许输入个性化：** 允许运行输入个性化服务，以根据用户输入的内容改进预测性输入（例如笔和触摸键盘）。
- **设置：**
  - **允许自动播放：** 允许用户更改自动播放设置。
  - **允许数据感知：** 允许用户更改数据感知设置。
  - **允许日期时间：** 允许用户更改日期和时间设置。

- **允许语言：** 允许用户更改语言设置。
- **允许电源和睡眠：** 允许用户更改电源和睡眠设置。
- **允许区域：** 允许用户更改区域设置。
- **允许登录选项：** 允许用户更改登录设置。
- **允许工作区：** 允许用户更改工作区设置。
- **允许您的账户：** 允许用户更改账户设置。

漫游设备策略

您可以在 XenMobile 中添加设备策略，以配置是否允许用户 iOS 设备上的语音和数据漫游。当语音漫游被禁用时，数据漫游会自动禁用。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

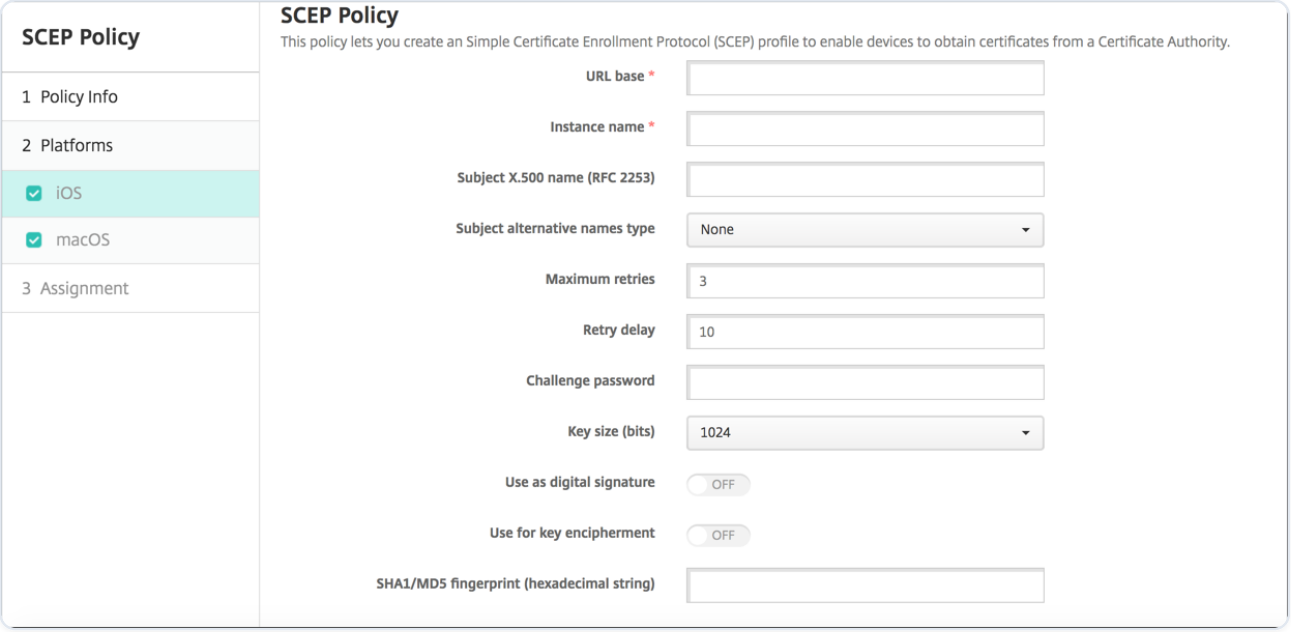
- **禁用语音漫游：** 选择是否禁用语音漫游。启用此选项时，数据漫游会自动禁用。默认值为 **关闭**，表示允许语音漫游。
- **禁用数据漫游：** 选择是否禁用数据漫游。此选项仅在语音漫游启用时可用。默认值为 **关闭**，表示允许数据漫游。

SCEP 设备策略

此策略允许您配置 iOS 和 macOS 设备，以使用简单证书注册协议 (SCEP) 从外部 SCEP 服务器检索证书。如果您希望使用连接到 XenMobile 的 PKI 通过 SCEP 向设备分发证书，则必须以分布式模式创建 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。

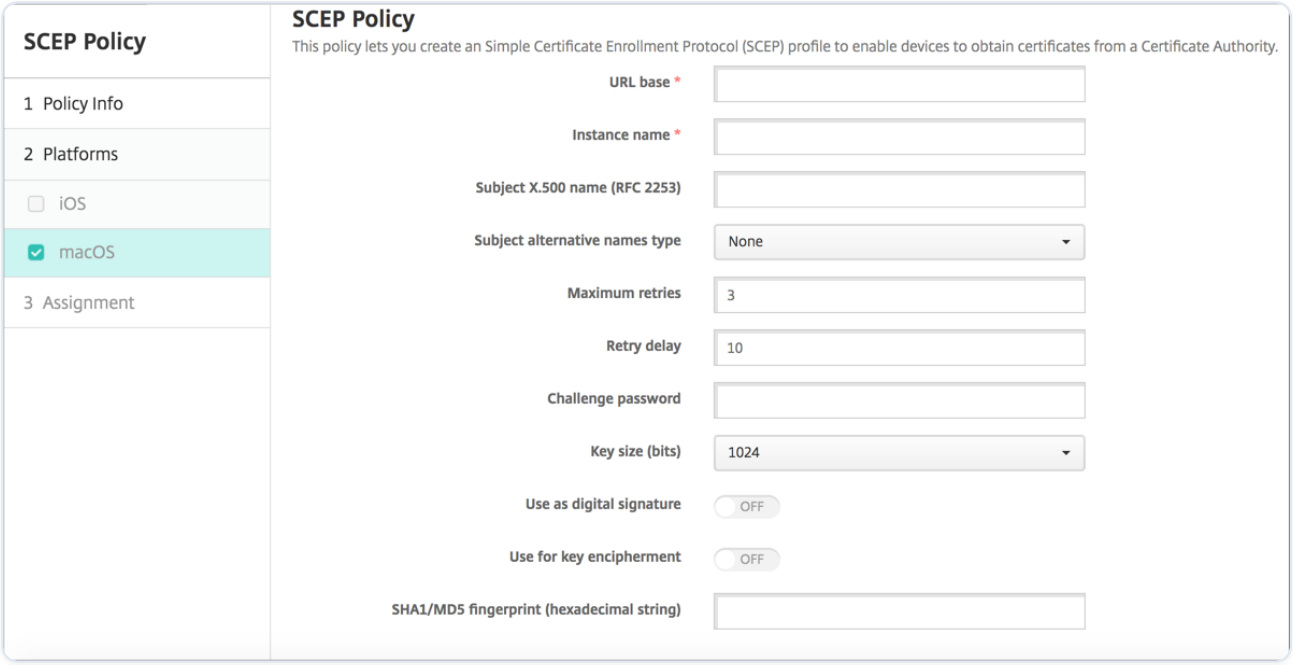
iOS 设置



- **URL 基址：** 键入 SCEP 服务器的地址，以定义 SCEP 请求通过 HTTP 或 HTTPS 发送的位置。私钥不会随证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能是安全的。但是，如果允许重复使用一次性密码，则必须使用 HTTPS 来保护密码。此步骤是必需的。
- **实例名称：** 键入 SCEP 服务器可识别的任何字符串。例如，它可以是 example.org 等域名。如果 CA 具有多个 CA 证书，则可以使用此字段来区分所需的域。此步骤是必需的。
- **主题 X.500 名称 (RFC 2253)：** 键入表示为对象标识符 (OID) 和值数组的 X.500 名称。例如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar，这可能转换为：\[\[\["C", "US"\] \], \[\["O", "Apple Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \]。您可以将 OID 表示为带有点的数字，并使用国家/地区 (C)、地区 (L)、省/市/自治区 (ST)、组织 (O)、组织单位 (OU) 和通用名称 (CN) 的快捷方式。
- **主题备用名称类型：** 在下拉列表中单击备用名称类型。SCEP 策略可以指定一个可选的备用名称类型，该类型提供 CA 颁发证书所需的值。您可以指定**无**、**RFC 822 名称**、**DNS 名称**或 **URI**。
- **最大重试次数：** 键入当 SCEP 服务器发送 PENDING 响应时设备可以重试的次数。默认值为 **3**。
- **重试延迟：** 键入两次后续重试之间等待的秒数。第一次重试不延迟。默认值为 **10**。
- **质询密码：** 输入预共享密钥。
- **密钥大小（位）：** 选择 **2048** 或更高作为密钥大小（以位为单位）。
- **用作数字签名：** 指定是否希望将证书用作数字签名。如果有人使用证书来验证数字签名（例如验证证书是否由 CA 颁发），SCEP 服务器将在使用公钥解密哈希之前验证证书是否可以以这种方式使用。

- **用于密钥加密：** 指定是否希望将证书用于密钥加密。如果服务器使用客户端提供的证书中的公钥来验证数据是否使用私钥加密，则服务器将首先检查证书是否可以用于密钥加密。如果不能，则操作失败。
- **SHA1/MD5 指纹（十六进制字符串）：** 如果您的 CA 使用 HTTP，请使用此字段提供 CA 证书的指纹，设备在注册期间使用此指纹确认 CA 响应的真实性。您可以输入 SHA1 或 MD5 指纹，也可以选择证书以导入其签名。
- **策略设置**
  - **删除策略：** 选择一种方法来安排策略删除。可用选项为“**选择日期**”和“**距离删除时长（小时）**”
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **距离删除时长（小时）：** 输入一个数字（以小时为单位），表示策略删除发生前的时长。仅适用于 iOS 6.0 及更高版本。

macOS 设置



- **URL 基址：** 键入 SCEP 服务器的地址，以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。私钥不会随证书签名请求 (CSR) 一起发送，因此可以安全地发送未加密的请求。但是，如果允许重复使用一次性密码，则必须使用 HTTPS 来保护密码。此步骤是必需的。
- **实例名称：** 键入 SCEP 服务器可识别的任何字符串。例如，它可以是 example.org 这样的域名。如果 CA 具有多个 CA 证书，则可以使用此字段来区分所需的域。此步骤是必需的。
- **主题 X.500 名称 (RFC 2253)：** 键入表示为对象标识符 (OID) 和值数组的 X.500 名称。例如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar，这将转换为：\[\[\["C", "US"\] \], \[\["O", "Apple

Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \]。您可以将 OID 表示为带有点的数字，并使用国家/地区 (C)、地区 (L)、省/市/自治区 (ST)、组织 (O)、组织单位 (OU) 和通用名称 (CN) 的快捷方式。

- **主题备用名称类型：** 在下拉列表中单击备用名称类型。SCEP 策略可以指定一个可选的备用名称类型，该类型提供 CA 颁发证书所需的值。您可以指定“**无**”、“**RFC 822 名称**”、“**DNS 名称**”或“**URI**”。
- **最大重试次数：** 键入当 SCEP 服务器发送 PENDING 响应时设备可以重试的次数。默认值为“**3**”。
- **重试延迟：** 键入后续重试之间等待的秒数。第一次重试不延迟。默认值为“**10**”。
- **质询密码：** 键入预共享密钥。
- **密钥大小（位）：** 选择 **2048** 或更高作为密钥大小（以位为单位）。
- **用作数字签名：** 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，例如验证证书是否由 CA 颁发，则 SCEP 服务器将验证证书是否可以以这种方式使用，然后才使用公钥解密哈希。
- **用于密钥加密：** 指定是否要将证书用于密钥加密。如果服务器使用客户端提供的证书中的公钥来验证数据是否已使用私钥加密，则服务器将首先检查证书是否可用于密钥加密。如果不能，则操作失败。
- **SHA1/MD5 指纹（十六进制字符串）：** 如果您的 CA 使用 HTTP，请使用此字段提供 CA 证书的指纹，设备在注册期间使用该指纹确认 CA 响应的真实性。您可以输入 SHA1 或 MD5 指纹，也可以选择证书以导入其签名。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 输入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您可以选择用户何时可以从其设备中删除策略。从菜单中选择**始终**、**需要密码**或**从不**。如果选择**需要密码**，请在**删除密码**字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**用户**。此选项仅适用于 macOS 10.7 及更高版本。

Siri 和听写策略

当用户在受管 iOS 设备上向 Siri 提问或听写文本时，Apple 会收集语音数据以改进 Siri。语音数据通过 Apple 的云服务，因此存在于安全的 XenMobile® 容器之外。但是，听写产生的文本仍保留在容器内。

XenMobile 允许您根据安全需求阻止 Siri 和听写服务。

在 MAM 部署中，每个应用的“**阻止听写**”策略默认设置为“**开**”，这会禁用设备的麦克风。如果要允许听写，请将其设置为“**关**”。您可以在 XenMobile 控制台的“**配置 > 应用程序**”中找到此策略。选择应用程序，单击“**编辑**”，然后单击“**iOS**”。

应用程序配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-siri-dictation-off.png)

在 MDM 部署中，您还可以通过“**配置 > 设备策略**”中的 Siri 策略禁用 Siri。默认情况下允许使用 Siri。

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-siri-restrictions-on.png)

在决定是否允许 Siri 和听写时，请记住以下几点：

- 根据 Apple 公开的信息，Apple 会将 Siri 和听写语音片段数据保留长达两年。数据会分配一个随机数来代表用户，语音文件与此随机数关联。有关详细信息，请参阅这篇 Wired 文章：Apple 揭示 Siri 保留您的数据多长时间。
- 您可以通过在任何 iOS 设备上转到“**设置 > 通用 > 键盘**”，然后点击“**启用听写**”下的链接来查看 Apple 隐私政策。

SSO 帐户设备策略

您在 XenMobile® 中创建单点登录 (SSO) 帐户，以允许用户一次登录即可从各种应用访问 XenMobile 和您的内部公司资源。用户无需在设备上存储任何凭据。SSO 帐户企业用户凭据可用于所有应用，包括 App Store 中的应用。此策略旨在与 Kerberos 身份验证后端配合使用。

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。此字段为必填项。
- **Kerberos 主体名称：**输入 Kerberos 主体名称。此字段为必填项。

- **身份凭据（密钥库或 PKI 凭据）：**单击下拉列表中的可选身份凭据，该凭据可用于在无需用户交互的情况下续订 Kerberos 凭据。
- **Kerberos 领域：**输入此策略的 Kerberos 领域。此设置值通常是您的大写域名（例如，EXAMPLE.COM）。此字段为必填项。
- **允许的 URL：**对于要要求 SSO 的每个 URL，请单击“**添加**”，然后执行以下操作：
  - **允许的 URL：**输入当用户从 iOS 设备访问该 URL 时要要求 SSO 的 URL。

    例如，当用户尝试浏览某个站点且该网站启动 Kerberos 质询时：如果该站点不在 URL 列表中，则 iOS 设备不会通过提供 Kerberos 可能从以前的 Kerberos 登录在设备上缓存的 Kerberos 令牌来尝试 SSO。匹配必须与 URL 的主机部分完全一致。例如，`https://shopping.apple.com` 有效，但 `https://*.apple.com` 无效。

    此外，如果 Kerberos 未基于主机匹配激活，则 URL 仍会回退到标准 HTTP 调用。这可能意味着任何事情，包括标准密码质询或 HTTP 错误（如果 URL 仅配置为使用 Kerberos 进行 SSO）。
  - 单击“**添加**”以添加 URL，或单击“**取消**”以取消添加 URL。
- **应用标识符：**对于允许使用此登录的每个应用，请单击“**添加**”，然后执行以下操作：
  - **应用标识符：** 输入允许使用此登录的应用程序的应用标识符。如果您不添加任何应用标识符，此登录将匹配**所有**应用标识符。
  - 单击**添加**以添加应用标识符，或单击**取消**以取消添加应用标识符。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项包括**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

应用商店设备策略

您可以在 XenMobile® 中创建策略，以指定 iOS、Android 或 Windows 平板设备是否在其主屏幕上显示 XenMobile 应用商店 Web Clip。

要添加或配置此策略，请转到**配置 > 设备策略**。有关详细信息，请参阅设备策略。

平台设置

对于您配置的每个平台，请选择是否在用户设备上显示 XenMobile 应用商店 Web Clip。默认设置为**开**。

已订阅日历设备策略

您可以在 XenMobile 中添加设备策略，以将已订阅日历添加到 iOS 设备上的日历列表。您可以订阅的公共日历列表可在以下位置获取：www.apple.com/downloads/macosx/calendars。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

先决条件

您必须已订阅日历，然后才能将其添加到用户设备上的已订阅日历列表。

iOS 设置

- **说明：**输入日历的说明。此字段为必填项。
- **URL：**输入日历 URL。您可以输入 `webcal://` URL 或指向 iCalendar 文件 (.ics) 的 `https://` 链接。此字段为必填项。
- **用户名：**输入用户的登录名。此字段为必填项。
- **密码：**输入可选的用户密码。
- **使用 SSL：选择是否使用安全套接字层连接到日历。默认值为关。**
- **策略设置**
  - **删除策略：选择策略删除的计划方法。可用选项包括选择日期和删除前持续时间（小时）**
    - **选择日期：**单击日历以选择要删除的具体日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），表示策略删除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。

条款和条件设备策略

当您希望用户接受公司关于连接到公司网络的特定策略时，可以在 XenMobile® 中创建条款和条件设备策略。当用户使用 XenMobile 注册其设备时，系统会向他们显示条款和条件，他们必须接受这些条款和条件才能注册其设备。拒绝条款和条件将取消注册过程。

如果您的公司有国际用户，并且您希望他们以其母语接受条款和条件，则可以为不同语言的条款和条件创建不同的策略。您必须为计划部署的每个平台和语言组合提供一个文件。对于 Android 和

iOS 设备，您必须提供 PDF 文件。对于 Windows 设备，您必须提供文本 (.txt) 文件和随附的图像文件。

要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 和 Android 设置

- **要导入的文件：** 单击**浏览**，然后导航到文件位置，选择要导入的条款和条件文件。
- **默认条款和条件：** 选择此文件是否为属于具有不同条款和条件的多个组的用户的默认文档。默认设置为**关**。

Windows 平板电脑设置

- **要导入的文件：** 单击**浏览**，然后导航到文件位置，选择要导入的条款和条件文件。
- **图像：** 单击**浏览**，然后导航到文件位置，选择要导入的图像文件。
- **默认条款和条件：** 选择此文件是否为属于具有不同条款和条件的多个组的用户的默认文档。默认设置为**关**。

VPN 设备策略

VPN 设备策略配置虚拟专用网络 (VPN) 设置，使用户设备能够安全地连接到公司资源。您可以为以下平台配置 VPN 设备策略。每个平台都需要一组不同的值，本文将详细介绍这些值。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

每应用 VPN 的要求

您可以通过 VPN 策略为以下平台配置每应用 VPN 功能：

- iOS
- macOS
- Android（旧版 DA）
- 三星 SAFE
- 三星 Knox

要为 Android Enterprise 设备配置 VPN，请为 Citrix SSO 应用程序创建托管配置设备策略。请参阅为 Android Enterprise 配置 VPN 配置文件。

每应用 VPN 选项适用于某些连接类型。下表指出了每应用 VPN 选项何时可用。

平台	连接类型	备注
iOS	思科 Legacy AnyConnect、瞻博网络 SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、思杰 SSO 或自定义 SSL。	
macOS	思科 AnyConnect、瞻博网络 SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA 或自定义 SSL。	
Android (旧版设备管理员)	思杰 SSO	
三星 SAFE	IPSEC、SSL	VPN 类型设置为 **通用**
三星 Knox	IPSEC、SSL	VPN 类型设置为 **通用**

要使用 Citrix SSO 应用程序为 iOS 和 Android（旧版设备管理员）设备创建每应用 VPN，除了 VPN 策略配置之外，您还需要执行额外步骤。此外，您必须验证是否满足以下先决条件：

- 本地 思杰 Gateway
- 设备上安装了以下应用程序：
  - 思杰 SSO
  - 思杰 Secure Hub™

使用 Citrix SSO 应用程序为 iOS 和 Android 设备配置每应用 VPN 的通用工作流程如下：

1. 配置本文所述的 VPN 设备策略。
   - 对于 *iOS*，请参阅 配置适用于 iOS 的 Citrix SSO 协议。通过 VPN 设备策略配置适用于 iOS 的 Citrix SSO 协议后，您还必须创建应用程序属性策略以将应用程序与每应用 VPN 策略关联。有关详细信息，请参阅 配置每应用 VPN。
     - 对于“**连接的身份验证类型**”字段，如果您选择“**证书**”，则必须首先为 Endpoint Management 配置基于证书的身份验证。请参阅 客户端证书或证书加域身份验证。
   - 对于 *Android（旧版 DA）*，请参阅 配置适用于 Android 的 Citrix SSO 协议。

- 对于“**连接的身份验证类型**”字段，如果您选择“**证书**”或“**密码和证书**”，则必须首先为 Endpoint Management 配置基于证书的身份验证。请参阅 客户端证书或证书加域身份验证。

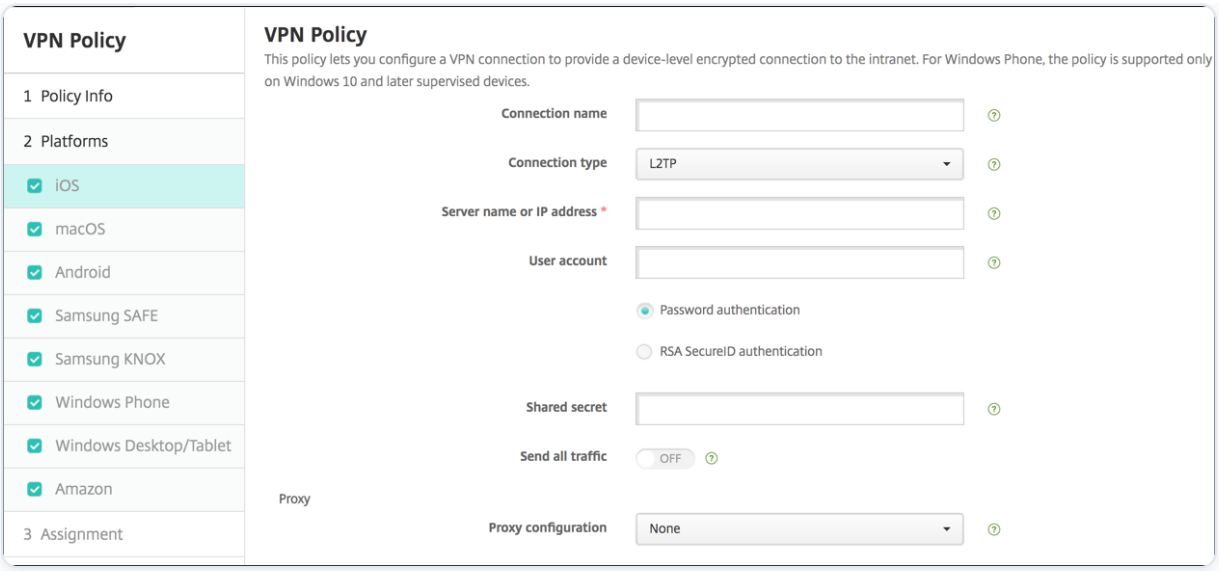
2. 配置 Citrix ADC 以接受来自每应用 VPN 的流量。有关详细信息，请参阅 在 Citrix Gateway 上进行完整 VPN 设置。

iOS 设置

为设备升级到 iOS 12 做准备：

适用于 iOS 的 VPN 设备策略中的 Citrix VPN 连接类型不支持 iOS 12。请执行以下步骤删除现有 VPN 设备策略并创建具有 Citrix SSO 连接类型的 VPN 设备策略：

1. 删除适用于 iOS 的 VPN 设备策略。
2. 添加适用于 iOS 的 VPN 设备策略。重要设置：
   - **连接类型** = **Citrix SSO**
   - **启用每应用 VPN** = **开**
   - **提供程序类型** = **数据包隧道**
3. 为 iOS 添加一个应用程序属性设备策略。对于**每应用 VPN 标识符**，选择 **iOS_VPN**。



- **连接名称：** 键入连接的名称。
- **连接类型：** 在列表中，选择此连接要使用的协议。默认值为 **L2TP**。

- **L2TP：** 具有预共享密钥身份验证的第 2 层隧道协议。
- **PPTP：** 点对点隧道协议。
- **IPSec：** 您的企业 VPN 连接。
- **Cisco Legacy AnyConnect：** 此连接类型要求用户设备上安装 Cisco Legacy AnyConnect VPN 客户端。Cisco 正在逐步淘汰基于现已弃用的 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**自定义 SSL** 的**连接类型**。有关所需设置，请参阅本节中的“配置自定义 SSL 协议”。
- **瞻博 SSL：** 瞻博网络 SSL VPN 客户端。
- **F5 SSL：** F5 Networks SSL VPN 客户端。
- **SonicWALL Mobile Connect：** 适用于 iOS 的 Dell 统一 VPN 客户端。
- **Ariba VIA：** Ariba Networks 虚拟 Internet 访问客户端。
- **IKEv2（仅限 iOS）：** 仅限 iOS 的 Internet 密钥交换版本 2。
- **AlwaysOn IKEv2：** 使用 IKEv2 的始终开启访问。
- **AlwaysOn IKEv2 双配置：** 使用 IKEv2 双配置的始终开启访问。
- **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。此连接类型是具有捆绑 ID **com.cisco.anyconnect** 的 Cisco AnyConnect 客户端所必需的。指定**连接名称**为 **Cisco AnyConnect**。您还可以部署 VPN 策略并为 iOS 设备启用网络访问控制 (NAC) 筛选器。该筛选器会阻止安装了不合规应用程序的设备的 VPN 连接。此配置需要 iOS VPN 策略的特定设置，如以下 iOS 部分所述。有关启用 NAC 筛选器所需的其他设置的更多信息，请参阅网络访问控制。

以下各节列出了上述每种连接类型的配置选项。

配置适用于 iOS 的 L2TP 协议

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选用户帐户。
- 选择**密码身份验证**或 **RSA SecurID 身份验证**。
- **共享密钥：** 键入 IPsec 共享密钥。
- **发送所有流量：** 选择是否通过 VPN 发送所有流量。默认值为**关闭**。

配置适用于 iOS 的 PPTP 协议

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选用户帐户。
- 选择**密码身份验证**或**RSA SecurID 身份验证**。
- **加密级别：** 在列表中，选择一个加密级别。默认值为**无**。
  - **无：** 不使用加密。
  - **自动：** 使用服务器支持的最强加密级别。
  - **最大值 (128 位)：** 始终使用 128 位加密。
- **发送所有流量：** 选择是否通过 VPN 发送所有流量。默认值为**关**。

配置适用于 iOS 的 IPsec 协议

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入一个可选的用户帐户。
- **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择**共享密钥**或**证书**。默认值为**共享密钥**。
- 如果启用**共享密钥**，请配置以下设置：
  - **组名称：** 键入一个可选的组名称。
  - **共享密钥：** 键入一个可选的共享密钥。
  - **使用混合身份验证：** 选择是否使用混合身份验证。使用混合身份验证时，服务器首先向客户端进行身份验证，然后客户端向服务器进行身份验证。默认值为**关**。
  - **提示输入密码：** 选择是否在用户连接到网络时提示他们输入密码。默认值为**关**。
- 如果启用**证书**，请配置以下设置：
  - **身份凭据**：在列表中，选择要使用的身份凭据。默认值为**无**。
  - **连接时提示输入 PIN**：选择是否要求用户在连接到网络时输入其 PIN。默认值为**关**。
  - **启用按需 VPN**：选择是否在用户连接到网络时触发 VPN 连接。默认值为**关**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置 iOS 的按需 VPN 设置。
- **启用按应用 VPN**：选择是否启用按应用 VPN。默认值为**关**。
- **按需匹配应用已启用**：选择当链接到按应用 VPN 服务的应用开始网络通信时，按应用 VPN 连接是否自动触发。默认值为**关**。
- **Safari 域**：单击**添加**以添加 Safari 域名。

配置适用于 iOS 的 Cisco 旧版 AnyConnect 协议

要从 Cisco 旧版 AnyConnect 客户端过渡到新的 Cisco AnyConnect 客户端，请使用自定义 SSL 协议。

- **提供程序捆绑包标识符**：对于旧版 AnyConnect 客户端，捆绑包 ID 为 com.cisco.anyconnect.gui。
- **服务器名称或 IP 地址**：键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户**：键入可选的用户帐户。
- **组**：键入可选的组名称。
- **连接的身份验证类型**：在列表中，选择**密码**或**证书**作为此连接的身份验证类型。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
  - 如果启用**证书**，请配置以下设置：
    - **身份凭据**：在列表中，选择要使用的身份凭据。默认值为**无**。
    - **连接时提示输入 PIN**：选择用户连接到网络时是否提示输入 PIN。默认值为**关闭**。
    - **按需启用 VPN**：选择用户连接到网络时是否启用触发 VPN 连接。默认值为**关闭**。有关**按需启用 VPN**为**开**时配置设置的信息，请参阅配置 iOS 的按需启用 VPN 设置。
- **启用每应用 VPN**：选择是否启用每应用 VPN。默认值为**关闭**。如果启用此选项，请配置以下设置：
  - **按需匹配应用已启用**：选择当链接到每应用 VPN 服务的应用开始网络通信时，每应用 VPN 连接是否自动触发。默认值为**关闭**。
  - **提供程序类型**：选择每应用 VPN 是作为**应用代理**还是作为**数据包隧道**提供。默认值为**应用代理**。
  - **Safari 域**：对于要包含的每个可触发每应用 VPN 连接的 Safari 域，请单击**添加**并执行以下操作：
    - **域**：键入要添加的域。
    - 单击**保存**以保存域，或单击**取消**以不保存域。

配置 iOS 的 Juniper SSL 协议

- **提供程序捆绑包标识符**：如果您的每应用 VPN 配置文件具有具有多个相同类型 VPN 提供程序的应用的捆绑包标识符，请在此处指定要使用的提供程序。
- **服务器名称或 IP 地址**：键入 VPN 服务器的服务器名称或 IP 地址。

- **用户帐户**：键入可选的用户帐户。
- **领域**：键入可选的领域名称。
- **角色**：键入可选的角色名称。
- **连接的身份验证类型**：在列表中，为该连接的身份验证类型选择“**密码**”或“**证书**”。默认值为“**密码**”。
  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 如果启用“**证书**”，请配置以下设置：
    - **身份凭据**：在列表中，选择要使用的身份凭据。默认值为“**无**”。
    - **连接时提示输入 PIN**：选择在用户连接到网络时是否提示其输入 PIN。默认值为“**关**”。
    - **启用按需 VPN**：选择是否在用户连接到网络时触发 VPN 连接。默认值为“**关**”。有关在“**启用按需 VPN**”设置为“**开**”时配置设置的信息，请参阅配置 iOS 的按需 VPN 设置。
- **启用每应用 VPN**：选择是否启用每应用 VPN。默认值为“**关**”。如果启用此选项，请配置以下设置：
  - **启用按需匹配应用**：选择当链接到每应用 VPN 服务的应用启动网络通信时，每应用 VPN 连接是否自动触发。默认值为“**关**”。
  - **提供程序类型**：选择每应用 VPN 是作为“**应用代理**”还是“**数据包隧道**”提供。默认值为“**应用代理**”。
  - **Safari 域**：对于要包括的每个可触发每应用 VPN 连接的 Safari 域，单击“**添加**”并执行以下操作：
    - **域**：键入要添加的域。
    - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。

配置 iOS 的 F5 SSL 协议

- **提供程序捆绑包标识符**：如果您的每应用 VPN 配置文件具有具有多个相同类型 VPN 提供程序的应用的捆绑包标识符，请在此处指定要使用的提供程序。
- **服务器名称或 IP 地址**： 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户**： 键入可选的用户帐户。
- **连接的身份验证类型**： 在列表中，选择此连接的身份验证类型为**密码**或**证书**。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
  - 如果启用**证书**，请配置以下设置：

    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为**无**。
    - **连接时提示输入 PIN：** 选择用户连接到网络时是否提示输入 PIN。默认值为**关**。
    - **启用按需 VPN：** 选择用户连接到网络时是否启用触发 VPN 连接。默认值为**关**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置 iOS 的按需 VPN 设置。

- **启用按应用 VPN：** 选择是否启用按应用 VPN。默认值为**关**。如果启用此选项，请配置以下设置：
    - **启用按需匹配应用：** 选择当链接到按应用 VPN 服务的应用启动网络通信时，按应用 VPN 连接是否自动触发。
    - **提供程序类型：** 选择按应用 VPN 是作为**应用代理**还是作为**数据包隧道**提供。默认值为**应用代理**。
    - **Safari 域：** 对于要包含的每个可触发按应用 VPN 连接的 Safari 域，请单击**添加**并执行以下操作：
        - **域：** 键入要添加的域。
        - 单击**保存**以保存域，或单击**取消**以不保存域。

配置 iOS 的 SonicWALL 协议

- **提供商捆绑包标识符：** 如果您的按应用 VPN 配置文件具有包含多个相同类型 VPN 提供商的应用的捆绑包标识符，请在此处指定要使用的提供商。
- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选的用户帐户。
- **登录组或域：** 键入可选的登录组或域。
- **连接的身份验证类型：** 在列表中，为该连接的身份验证类型选择**密码**或**证书**。默认值为**密码**。
    - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
    - 如果启用**证书**，请配置以下设置：
        - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为**无**。
        - **连接时提示输入 PIN：** 选择是否在用户连接到网络时提示他们输入 PIN。默认值为**关闭**。
        - **启用按需 VPN：** 选择是否在用户连接到网络时启用触发 VPN 连接。默认值为**关闭**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置 iOS 的按需 VPN 启用设置。

- **启用按应用 VPN：** 选择是否启用按应用 VPN。默认值为**关闭**。如果将此选项设置为“开”，请配置以下设置：

- **按需匹配应用已启用：** 选择当链接到按应用 VPN 服务的应用发起网络通信时，按应用 VPN 连接是否自动触发。
- **提供商类型：** 选择按应用 VPN 是作为**应用代理**还是作为**数据包隧道**提供。默认值为**应用代理**。
- **Safari 域：** 对于要包含的每个可触发按应用 VPN 连接的 Safari 域，单击**添加**并执行以下操作：
  - **域：** 键入要添加的域。
  - 点击“**保存**”以保存域，或点击“**取消**”以不保存域。

配置适用于 iOS 的 Ariba VIA 协议

- “**提供程序捆绑包标识符：**”如果您的每应用 VPN 配置文件具有一个应用程序的捆绑包标识符，该应用程序具有多个相同类型的 VPN 提供程序，请在此处指定要使用的提供程序。
- “**服务器名称或 IP 地址：**”键入 VPN 服务器的服务器名称或 IP 地址。
- “**用户帐户：**”键入可选的用户帐户。
- “**连接的身份验证类型：**”在列表中，选择“**密码**”或“**证书**”作为此连接的身份验证类型。默认值为“**密码**”。
  - 如果您启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 如果您启用“**证书**”，请配置以下设置：
    - “**身份凭据：**”在列表中，选择要使用的身份凭据。默认值为“**无**”。
    - “**连接时提示输入 PIN：**”选择是否在用户连接到网络时提示他们输入 PIN。默认值为“**关**”。
    - “**启用按需 VPN：**”选择是否在用户连接到网络时启用触发 VPN 连接。默认值为“**关**”。有关在“**启用按需 VPN**”为“**开**”时配置设置的信息，请参阅 配置适用于 iOS 的按需 VPN 设置。
- “**启用每应用 VPN：**”选择是否启用每应用 VPN。默认值为“**关**”。如果您启用此选项，请配置以下设置：
  - “**按需匹配应用程序已启用：**”选择当链接到每应用 VPN 服务的应用程序发起网络通信时，每应用 VPN 连接是否自动触发。
  - “**Safari 域：**”对于要包含的每个可触发每应用 VPN 连接的 Safari 域，请点击“**添加**”并执行以下操作：
    - “**域：**”键入要添加的域。

- 点击“**保存**”以保存域，或点击“**取消**”以不保存域。

配置适用于 iOS 的 IKEv2 协议

本节包含用于 IKEv2、AlwaysOn IKEv2 和 AlwaysOn IKEv2 双配置协议的设置。对于 AlwaysOn IKEv2 双配置协议，请为蜂窝网络和 Wi-Fi 网络配置所有这些设置。

- **允许用户禁用自动连接：** 适用于 AlwaysOn 协议。选择是否允许用户在其设备上关闭与网络的自动连接。默认值为“**关闭**”。
- **服务器主机名或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **本地标识符：** IKEv2 客户端的 FQDN 或 IP 地址。此字段为必填项。
- **远程标识符：** VPN 服务器的 FQDN 或 IP 地址。此字段为必填项。
- **设备身份验证：** 为此连接的身份验证类型选择“**共享密钥**”、“**证书**”或“**基于设备标识符的设备证书**”。默认值为“**共享密钥**”。
  - 如果选择“**共享密钥**”，请键入可选的共享密钥。
  - 如果选择“**证书**”，请选择要使用的“**身份凭据**”。默认值为“**无**”。
  - 如果选择“**基于设备标识符的设备证书**”，请选择要使用的“**设备身份类型**”。默认值为“**IMEI**”。要使用此选项，请使用 REST API 批量导入证书。请参阅 使用 REST API 批量上传证书到 iOS 设备。仅当选择“**Always On IKEv2**”时可用。
- **启用扩展身份验证：** 选择是否启用扩展身份验证协议 (EAP)。如果选择“**开**”，请键入“**用户帐户**”和“**身份验证密码**”。
- **死对等体检测间隔：** 选择联系对等设备的频率，以确保对等设备保持可达。默认值为“**无**”。选项包括：
  - **无：** 禁用死对等体检测。
  - **低：** 每 30 分钟联系对等体。
  - **中等：**每 10 分钟联系一次对等设备。
  - **高：**每 1 分钟联系一次对等设备。
- **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。
- **设备休眠时启用 NAT 保持活动状态：**适用于 AlwaysOn 协议。保持活动数据包可维护 IKEv2 连接的 NAT 映射。设备唤醒时，芯片会定期发送这些数据包。如果此设置处于打开状态，即使

设备处于休眠状态，芯片也会发送保持活动数据包。默认间隔为 Wi-Fi 20 秒，蜂窝网络 110 秒。您可以通过使用 NAT 保持活动间隔参数来更改间隔。

- **NAT 保持活动间隔（秒）：**默认为 20 秒。
- **启用完全前向保密：**选择是否启用此功能。
- **DNS 服务器 IP 地址：**可选。DNS 服务器 IP 地址字符串列表。这些 IP 地址可以包含 IPv4 和 IPv6 地址的混合。单击“**添加**”以键入地址。
- **域名：**可选。隧道的主域。
- **搜索域：**可选。用于完全限定单标签主机名的域字符串列表。
- **将补充匹配域附加到解析器列表：**可选。确定是否将补充匹配域列表添加到解析器的搜索域列表。默认为“**开**”。
- **补充匹配域：**可选。用于确定哪些 DNS 查询将使用 DNS 服务器地址中的 DNS 解析器设置的域字符串列表。此密钥创建了一个拆分 DNS 配置，其中只有特定域中的主机通过使用隧道的 DNS 解析器进行解析。不在此列表中的任何域中的主机将通过使用系统的默认解析器进行解析。

如果此参数具有空字符串，则该字符串是默认域。这是拆分隧道配置在主 DNS 服务器之前将所有 DNS 查询定向到 VPN DNS 服务器的方式。如果 VPN 隧道是网络的默认路由，则列出的 DNS 服务器将成为默认解析器。在这种情况下，将忽略补充匹配域列表。

- **IKE SA 参数**和**子 SA 参数**。为每个安全关联 (SA) 参数选项配置这些设置：
  - **加密算法：** 在列表中，选择要使用的 IKE 加密算法。默认值为 **3DES**。
  - **完整性算法：** 在列表中，选择要使用的完整性算法。默认值为 **SHA1-96**。
  - **Diffie Hellman 组：** 在列表中，选择 Diffie Hellman 组号。默认值为 **2**。
  - **IKE 生命周期（分钟）：** 键入一个介于 10 到 1440 之间的整数，表示 SA 生命周期（重新密钥间隔）。默认值为 **1440** 分钟。
- **服务例外：** 适用于 AlwaysOn 协议。服务例外是指不受 AlwaysOn VPN 限制的系统服务。配置以下服务例外设置：
  - **语音邮件：** 在列表中，选择如何处理语音邮件例外。默认值为 **允许流量通过隧道**。
  - **隔空打印：** 在列表中，选择如何处理隔空打印例外。默认值为 **允许流量通过隧道**。
  - **允许来自 VPN 隧道外部的强制网络门户流量：** 选择是否允许用户连接到 VPN 隧道外部的公共热点。默认值为 **关闭**。
  - **允许来自 VPN 隧道外部的所有强制网络应用程序流量：** 选择是否允许所有热点网络应用程序在 VPN 隧道外部运行。默认值为 **关闭**。

  - **强制网络应用程序捆绑包标识符：** 对于用户允许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**以保存应用程序捆绑包标识符。

- **按应用程序 VPN**。为 IKEv2 连接类型配置以下设置。
  - **启用按应用程序 VPN：** 选择是否启用按应用程序 VPN。默认值为 **关闭**。
  - **启用按需匹配应用程序：** 选择当链接到按应用程序 VPN 服务的应用程序启动网络通信时，按应用程序 VPN 连接是否自动触发。默认值为 **关闭**。
  - **Safari 域：** 单击**添加**以添加 Safari 域名。
- **代理配置：** 选择 VPN 连接如何通过代理服务器路由。默认值为 **无**。

配置适用于 iOS 的 Citrix SSO 协议

Citrix SSO 客户端可在 Apple Store `<https://apps.apple.com/us/app/citrix-sso/id1333396910>` 中获取。

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选的用户帐户。
- **连接的身份验证类型：** 在列表中，选择此连接的身份验证类型为**密码**或**证书**。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
  - 如果启用**证书**，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为**无**。
    - **连接时提示输入 PIN：** 选择用户连接到网络时是否提示他们输入 PIN。默认值为**关**。
    - **启用按需 VPN：** 选择当用户连接到网络时是否启用触发 VPN 连接。默认值为**关**。有关在**启用按需 VPN** 为**开**时配置设置的信息，请参阅配置适用于 iOS 的按需 VPN 设置。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为**关**。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：** 选择当与每应用 VPN 服务关联的应用程序启动网络通信时，每应用 VPN 连接是否自动触发。
  - **提供程序类型：** 选择每应用 VPN 是作为**应用程序代理**还是作为**数据包隧道**提供。默认值为**应用程序代理**。
  - **提供程序类型：** 设置为**数据包隧道**。

  - **Safari 域：** 对于要包含的每个可以触发每应用 VPN 连接的 Safari 域，单击**添加**并执行以下操作：
    - **域：** 键入要添加的域。
    - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。
- **自定义 XML：** 对于要添加的每个自定义 XML 参数，单击“**添加**”并指定键/值对。可用参数为：
  - **disableL3：** 禁用系统级 VPN。仅允许按应用程序 VPN。不需要**值**。
  - **useragent：** 将此设备策略与面向 VPN 插件客户端的任何 Citrix Gateway 策略关联。对于由插件启动的请求，此键的**值**会自动添加到 VPN 插件中。

为 iOS 配置自定义 SSL 协议

要从 Cisco Legacy AnyConnect 客户端过渡到 Cisco AnyConnect 客户端：

1. 使用自定义 SSL 协议配置 VPN 设备策略。将策略部署到 iOS 设备。
2. 从 `<https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>` 上载 Cisco AnyConnect 客户端，将应用程序添加到 XenMobile，然后将应用程序部署到 iOS 设备。
3. 从 iOS 设备中删除旧的 VPN 设备策略。

设置：

- **自定义 SSL 标识符（反向 DNS 格式）：** 设置为捆绑包标识符。对于 Cisco AnyConnect 客户端，请使用 **com.cisco.anyconnect**。
- **提供程序捆绑包标识符：** 如果“**自定义 SSL 标识符**”中指定的应用程序具有多个相同类型（应用程序代理或数据包隧道）的 VPN 提供程序，则指定此捆绑包标识符。对于 Cisco AnyConnect 客户端，请使用 **com.cisco.anyconnect**。
- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选用户帐户。
- **连接的身份验证类型：** 在列表中，选择“**密码**”或“**证书**”作为此连接的身份验证类型。默认值为“**密码**”。
  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 如果启用“**证书**”，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为“**无**”。
    - **连接时提示输入 PIN：** 选择是否在用户连接到网络时提示他们输入 PIN。默认值为“**关闭**”。

    - **启用按需 VPN：** 选择是否在用户连接到网络时触发 VPN 连接。默认值为“**关闭**”。有关在“**启用按需 VPN**”设置为“**开**”时配置设置的信息，请参阅配置 iOS 的按需 VPN 设置。

- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为“**关闭**”。如果将此选项设置为“开”，请配置以下设置：
    - **启用按需匹配应用：** 选择当链接到每应用 VPN 服务的应用发起网络通信时，每应用 VPN 连接是否自动触发。
    - **提供程序类型：** 提供程序类型指示提供程序是 VPN 服务还是代理服务。对于 VPN 服务，请选择“**数据包隧道**”。对于代理服务，请选择“**应用代理**”。对于 Cisco AnyConnect 客户端，请选择“**数据包隧道**”。
    - **Safari 域：** 对于要包含的每个可触发每应用 VPN 连接的 Safari 域，单击“**添加**”并执行以下操作：
        - **域：** 键入要添加的域。
        - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。
- **自定义 XML：** 对于要添加的每个自定义 XML 参数，单击“**添加**”并执行以下操作：
    - **参数名称：** 键入要添加的参数的名称。
    - **值：** 键入与“**参数名称**”关联的值。
    - 单击 **保存** 以保存参数，或单击 **取消** 以不保存参数。

配置 VPN 设备策略以支持 NAC

1. **连接类型** 为 **自定义 SSL** 是配置 NAC 筛选器所必需的。
2. 指定 **连接名称** 为 **VPN**。
3. 对于 **自定义 SSL 标识符**，键入 **com.citrix.NetScalerGateway.ios.app**
4. 对于 **提供程序捆绑包标识符**，键入 **com.citrix.NetScalerGateway.ios.app.vpnplugin**

步骤 3 和 4 中的值来自 NAC 筛选所需的 Citrix SSO 安装。您无需配置身份验证密码。有关使用 NAC 功能的更多信息，请参阅 网络访问控制。

配置启用按需 VPN 选项（适用于 iOS）

- **按需域：** 对于用户连接时要采取的每个域和关联操作，单击 **添加** 并执行以下操作：
- **域：** 键入要添加的域。
- **操作：** 从列表中选择以下可能的操作之一：
    - **始终建立：** 该域始终触发 VPN 连接。

- **从不建立：** 该域从不触发 VPN 连接。
- **必要时建立：** 如果域名解析失败，该域会触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，就会发生故障。
- 单击 **保存** 以保存域，或单击 **取消** 以不保存域。

- **按需规则**
  - **操作**：在列表中，选择要执行的操作。默认值为 **EvaluateConnection**。可能的操作包括：
    - **允许**：允许按需 VPN 在触发时连接。
    - **连接**：无条件启动 VPN 连接。
    - **断开连接**：删除 VPN 连接，并且只要规则匹配，就不要按需重新连接。
    - **EvaluateConnection**：评估每个连接的 ActionParameters 数组。
    - **忽略**：保持任何现有 VPN 连接处于活动状态，但只要规则匹配，就不要按需重新连接。
  - **DNSDomainMatch**：对于要添加的、设备搜索域列表可以匹配的每个域，单击“**添加**”并执行以下操作：
    - **DNS 域**：键入域名。您可以使用通配符“*”前缀来匹配多个域。例如，*.example.com 匹配 mydomain.example.com、yourdomain.example.com 和 herdomain.example.com。
    - 单击“**保存**”以保存域或单击“**取消**”以不保存域。
  - **DNSServerAddressMatch**：对于要添加的、网络中任何指定的 DNS 服务器可以匹配的每个 IP 地址，单击“**添加**”并执行以下操作：
    - **DNS 服务器地址**：键入要添加的 DNS 服务器地址。您可以使用通配符“*”后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的任何 DNS 服务器。
    - 单击“**保存**”以保存 DNS 服务器地址或单击“**取消**”以不保存 DNS 服务器地址。
  - **InterfaceTypeMatch**：在列表中，选择正在使用的主要网络接口硬件类型。默认值为 **Unspecified**。可能的值包括：
    - **Unspecified**：匹配任何网络接口硬件。此选项为默认值。
    - **以太网：**仅匹配以太网网络接口硬件。
    - **Wi-Fi：**仅匹配 Wi-Fi 网络接口硬件。
    - **蜂窝：**仅匹配蜂窝网络接口硬件。
  - **SSIDMatch：对于要添加的、与当前网络匹配的每个 SSID，单击添加**并执行以下操作。

    - **SSID：**键入要添加的 SSID。如果网络不是 Wi-Fi 网络，或者 SSID 未出现，则匹配失败。将此列表留空以匹配任何 SSID。
    - 单击**保存**以保存 SSID，或单击**取消**以不保存 SSID。
  - **URLStringProbe：**键入要获取的 URL。如果此 URL 在没有重定向的情况下成功获取，则此规则匹配。
  - **ActionParameters : Domains：对于要添加的、EvaluateConnection 检查的每个域，单击添加**并执行以下操作：
    - **域：**键入要添加的域。
    - 单击**保存**以保存域，或单击**取消**以不保存域。
  - **ActionParameters : DomainAction：**在列表中，为指定的 **ActionParameters : Domains** 域选择 **VPN 行为**。默认值为 **ConnectIfNeeded**。可能的操作包括：
    - **ConnectIfNeeded：**如果域名解析失败，该域将触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，就会发生故障。
    - **NeverConnect：**该域从不触发 VPN 连接。
  - **Action Parameters: RequiredDNSServers：对于用于解析指定域的每个 DNS 服务器 IP 地址，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。此服务器无需是设备当前网络配置的一部分。如果 DNS 服务器不可达，则会建立 VPN 连接作为响应。此 DNS 服务器必须是内部 DNS 服务器或受信任的外部 DNS 服务器。
    - 单击 **保存** 以保存 DNS 服务器，或单击 **取消** 以不保存 DNS 服务器。
  - **ActionParameters : RequiredURLStringProbe:** （可选）键入要探测的 HTTP 或 HTTPS（首选）URL，使用 GET 请求。如果 URL 的主机名无法解析、服务器不可达或服务器没有响应，则会建立 VPN 连接。仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。
  - **OnDemandRules : XML content:** 键入或复制粘贴按需 XML 配置规则。
    - 单击 **检查字典** 以验证 XML 代码。如果 XML 有效，您将在 **XML content** 文本框下方的绿色文本中看到“Valid XML”。如果无效，您将在橙色文本中看到描述错误的错误消息。
- **代理**
  - **代理配置：** 在列表中，选择 VPN 连接如何通过代理服务器路由。默认值为 **无**。

- 如果启用 **手动**，请配置以下设置：
  - **代理服务器的主机名或 IP 地址：** 键入代理服务器的主机名或 IP 地址。此字段为必填项。
  - **代理服务器端口：** 键入代理服务器端口号。此字段为必填项。
  - **用户名：** 键入可选的代理服务器用户名。
  - **密码：** 键入可选的代理服务器密码。
- 如果配置 **自动**，请配置以下设置：
  - **代理服务器 URL：** 键入代理服务器的 URL。此字段为必填项。

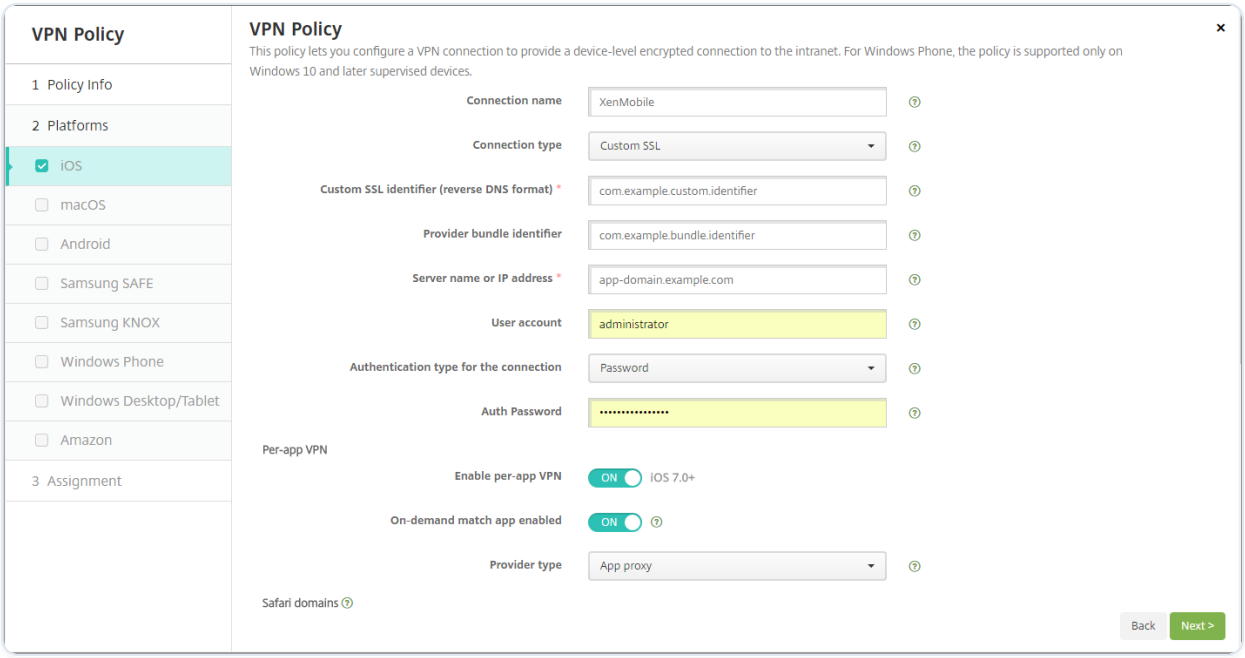
- **策略设置**
  - 在 **策略设置** 下，在 **删除策略** 旁边，选择 **选择日期** 或 **直到删除的持续时间（小时）**。
  - 如果您选择“**选择日期**”，请单击日历以选择具体的删除日期。
  - 在“**允许用户删除策略**”列表中，选择“**始终**”、“**需要密码**”或“**从不**”。
  - 如果您选择“**需要密码**”，请在“**删除密码**”旁边键入必要的密码。

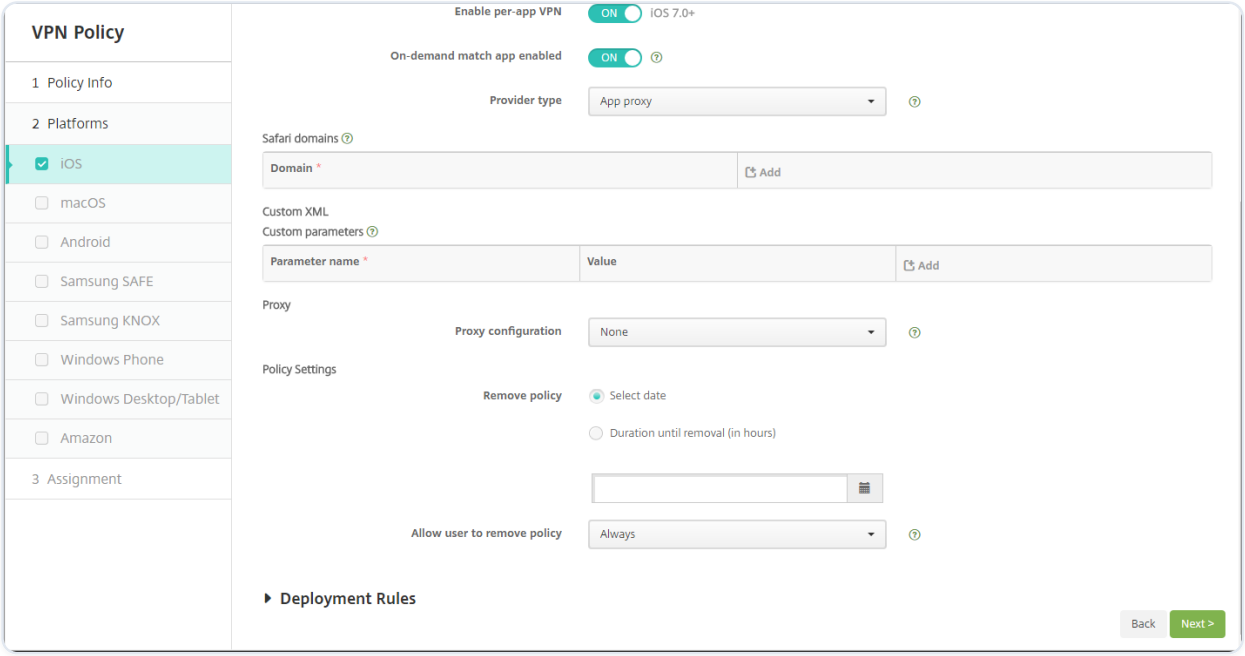
配置每应用 VPN

iOS 的每应用 VPN 选项适用于以下连接类型：Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix VPN、Citrix SSO 和 Custom SSL。

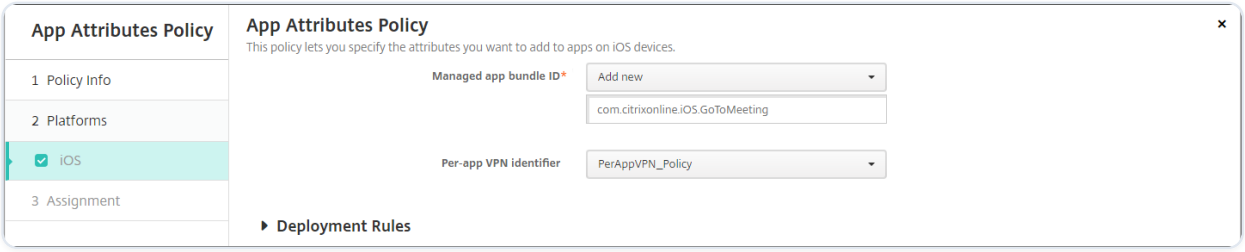
要配置每应用 VPN：

1. 在“**配置 > 设备策略**”中，创建一个 VPN 策略。例如：



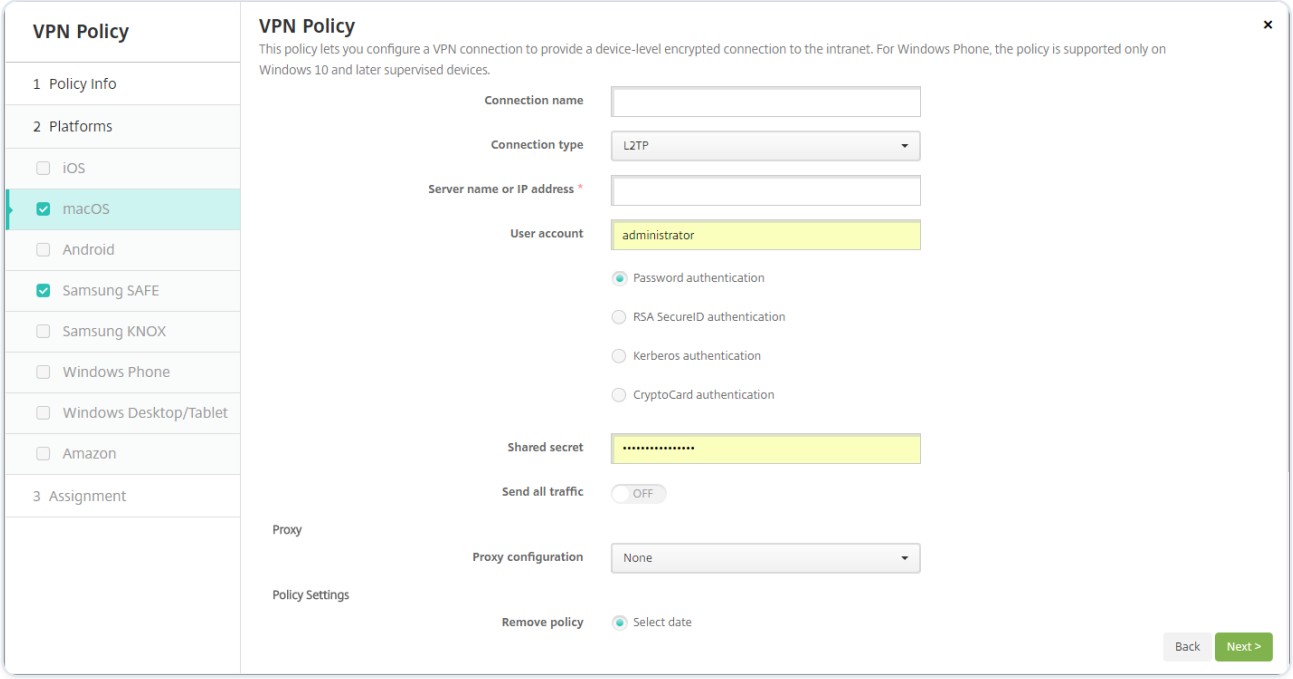


2. 在“**配置 > 设备策略**”中，创建一个应用程序属性策略，以将应用程序与每应用 VPN 策略关联。对于“**每应用 VPN 标识符**”，选择在步骤 1 中创建的 VPN 策略的名称。对于“**托管应用程序捆绑包 ID**”，从应用程序列表中选择或键入应用程序捆绑包 ID。（如果您部署了 iOS 应用程序清单策略，则应用程序列表中将包含应用程序。）



- **策略设置**
  - **删除策略：**选择一种计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：**单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：**键入一个数字（以小时为单位），直到策略删除发生。仅适用于 iOS 6.0 及更高版本。

macOS 设置



- **连接名称：** 键入连接的名称。
- **连接类型：** 在列表中，选择此连接要使用的协议。默认值为 L2TP。
  - **L2TP：** 带有预共享密钥身份验证的第 2 层隧道协议。
  - **PPTP：** 点对点隧道。
  - **IPSec：** 您的企业 VPN 连接。
  - **Cisco AnyConnect：** Cisco AnyConnect VPN 客户端。
  - **Juniper SSL：** 瞻博网络 SSL VPN 客户端。
  - **F5 SSL：** F5 Networks SSL VPN 客户端。
  - **SonicWALL Mobile Connect：** 适用于 iOS 的 Dell 统一 VPN 客户端。
  - **Ariba VIA：** Ariba Networks 虚拟 Internet 访问客户端。
  - **Citrix VPN：** Citrix VPN 客户端。
  - **Custom SSL：** 自定义安全套接字层。

以下各节列出了上述每种连接类型的配置选项。

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：** 键入可选的用户帐户。

- 选择**密码身份验证**、**RSA SecurID 身份验证**、**Kerberos 身份验证**或**CryptoCard 身份验证**。默认值为**密码身份验证**。
- **共享密钥：** 键入 IPsec 共享密钥。
- **发送所有流量：** 选择是否通过 VPN 发送所有流量。默认值为**关**。

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：** 键入可选的用户帐户。
- 选择**密码身份验证**、**RSA SecurID 身份验证**、**Kerberos 身份验证**或**CryptoCard 身份验证**。默认值为**密码身份验证**。
- **加密级别：** 选择所需的加密级别。默认值为**无**。
  - **无：** 不使用加密。
  - **自动：** 使用服务器支持的最强加密级别。
  - **最大**（128 位）：始终使用 128 位加密。
- **发送所有流量：** 选择是否通过 VPN 发送所有流量。默认值为**关**。

配置适用于 macOS 的 IPsec 协议

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选的用户帐户。
- **连接的身份验证类型：** 在列表中，选择此连接的身份验证类型为**共享密钥**或**证书**。默认值为**共享密钥**。
  - 如果启用**共享密钥**身份验证，请配置以下设置：
    - **组名称：** 键入可选的组名称。
    - **共享密钥：** 键入可选的共享密钥。
    - **使用混合身份验证：** 选择是否使用混合身份验证。使用混合身份验证时，服务器首先向客户端进行身份验证，然后客户端向服务器进行身份验证。默认值为**关闭**。
    - **提示输入密码：** 选择在用户连接到网络时是否提示他们输入密码。默认值为**关闭**。
  - 如果启用**证书**身份验证，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为**无**。

- **连接时提示输入 PIN：** 选择在用户连接到网络时是否要求他们输入 PIN。默认值为**关闭**。
- **启用按需 VPN：** 选择在用户连接到网络时是否启用触发 VPN 连接。默认值为**关闭**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置按需 VPN 选项。

配置适用于 macOS 的 Cisco AnyConnect 协议

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选的用户帐户。
- **组：** 键入可选的组名。
- **连接的身份验证类型：** 在列表中，选择 **密码** 或 **证书** 作为此连接的身份验证类型。默认值为 **密码**。
  - 如果启用 **密码**，请在 **身份验证密码** 字段中键入可选的身份验证密码。
  - 如果启用 **证书**，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为 **无**。
    - **连接时提示输入 PIN：** 选择用户连接到网络时是否提示其输入 PIN。默认值为 **关**。
    - **启用按需 VPN：** 选择用户连接到网络时是否启用触发 VPN 连接。默认值为 **关**。有关在 **启用按需 VPN** 为 **开** 时配置设置的信息，请参阅配置按需 VPN 选项。
  - **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为 **关**。如果启用此选项，请配置以下设置：
    - **启用按需匹配应用：** 选择当链接到每应用 VPN 服务的应用开始网络通信时，每应用 VPN 连接是否自动触发。默认值为 **关**。
    - **Safari 域：** 对于要包含的每个可触发每应用 VPN 连接的 Safari 域，单击 **添加** 并执行以下操作：
      - **域：** 键入要添加的域。
      - 单击 **保存** 以保存域，或单击 **取消** 以不保存域。

配置适用于 macOS 的 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：**键入可选的用户帐户。
- **领域：**键入可选的领域名称。
- **角色：**键入可选的角色名称。

- **连接的身份验证类型：在列表中，选择密码**或**证书**作为此连接的身份验证类型。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
  - 如果启用**证书**，请配置以下设置：
    - **身份凭据：在列表中，选择要使用的身份凭据。默认值为无。**
    - **连接时提示输入 PIN：选择在用户连接到网络时是否提示他们输入 PIN。默认值为关。**
    - **启用按需 VPN：选择是否在用户连接到网络时启用触发 VPN 连接。默认值为关**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置按需 VPN 设置。
- **启用每应用 VPN：选择是否启用每应用 VPN。默认值为关**。如果启用此选项，请配置以下设置：
  - **启用按需匹配应用：选择当链接到每应用 VPN 服务的应用发起网络通信时，每应用 VPN 连接是否自动触发。默认值为关。**
  - **Safari 域：对于要包含的每个可以触发每应用 VPN 连接的 Safari 域，单击添加**并执行以下操作：
    - **域：**键入要添加的域。
    - 单击**保存**以保存域，或单击**取消**以不保存域。

配置适用于 macOS 的 F5 SSL 协议

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选的用户帐户。
- **连接的身份验证类型：** 在列表中，选择“**密码**”或“**证书**”作为此连接的身份验证类型。默认值为“**密码**”。
  - 如果启用“**密码**”，请在“**身份验证密码**”字段中键入可选的身份验证密码。
  - 如果启用“**证书**”，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为“**无**”。
    - **连接时提示输入 PIN：** 选择在用户连接到网络时是否提示他们输入 PIN。默认值为“**关**”。
    - **按需启用 VPN：** 选择是否在用户连接到网络时触发 VPN 连接。默认值为“**关**”。有关在“**按需启用 VPN**”为“**开**”时配置设置的信息，请参阅配置按需启用 VPN 设置。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为“**关**”。如果启用此选项，请配置以下设置：

- **按需匹配应用已启用：** 选择当链接到每应用 VPN 服务的应用开始网络通信时，每应用 VPN 连接是否自动触发。默认值为“**关**”。
- **Safari 域：** 对于要包含的每个可以触发每应用 VPN 连接的 Safari 域，单击“**添加**”并执行以下操作：
  - **域：** 键入要添加的域。
  - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。

为 macOS 配置 SonicWALL Mobile Connect 协议

- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。
- **用户帐户：** 键入可选的用户帐户。
- **登录组或域：** 键入可选的登录组或域。
- **连接的身份验证类型：** 在列表中，选择 **密码** 或 **证书** 作为此连接的身份验证类型。默认值为 **密码**。
  - 如果启用 **密码**，请在 **身份验证密码** 字段中键入可选的身份验证密码。
  - 如果启用 **证书**，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为 **无**。
    - **连接时提示输入 PIN：** 选择是否在用户连接到网络时提示他们输入 PIN。默认值为 **关**。
    - **启用按需 VPN：** 选择是否在用户连接到网络时触发 VPN 连接。默认值为 **关**。有关在 **启用按需 VPN** 为 **开** 时配置设置的信息，请参阅 配置按需 VPN 设置。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。默认值为 **关**。如果启用此选项，请配置以下设置：
  - **按需匹配应用已启用：** 选择当与每应用 VPN 服务关联的应用发起网络通信时，每应用 VPN 连接是否自动触发。默认值为 **关**。
  - **Safari 域：** 对于要包含的每个可触发每应用 VPN 连接的 Safari 域，请单击 **添加** 并执行以下操作：
    - **域：** 键入要添加的域。
    - 单击 **保存** 以保存域，或单击 **取消** 以不保存域。

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：** 键入可选的用户帐户。

- **连接的身份验证类型：** 在列表中，选择**密码**或**证书**作为此连接的身份验证类型。默认值为**密码**。
  - 如果启用**密码**，请在**身份验证密码**字段中键入可选的身份验证密码。
  - 如果启用**证书**，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为**无**。
    - **连接时提示输入 PIN：** 选择用户连接到网络时是否提示他们输入 PIN。默认值为**关**。
    - **启用按需 VPN：** 选择用户连接到网络时是否启用触发 VPN 连接。默认值为**关**。有关在**启用按需 VPN**为**开**时配置设置的信息，请参阅配置按需 VPN 设置。
- **启用按应用 VPN：** 选择是否启用按应用 VPN。默认值为**关**。如果启用此选项，请配置以下设置：
  - **按需匹配应用已启用：** 选择当链接到按应用 VPN 服务的应用发起网络通信时，按应用 VPN 连接是否自动触发。默认值为**关**。
  - **Safari 域：** 对于要包含的每个可触发按应用 VPN 连接的 Safari 域，单击**添加**并执行以下操作：
    - **域：** 键入要添加的域。
    - 单击**保存**以保存域，或单击**取消**以不保存域。

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。此字段为必填项。
- **服务器名称或 IP 地址：** 键入 VPN 服务器的服务器名称或 IP 地址。此字段为必填项。
- **用户帐户：** 键入可选的用户帐户。
  - **连接的身份验证类型：** 在列表中，选择 **密码** 或 **证书** 作为此连接的身份验证类型。默认值为**密码**。
  - 如果启用 **密码**，请在 **身份验证密码** 字段中键入可选的身份验证密码。
  - 如果启用 **证书**，请配置以下设置：
    - **身份凭据：** 在列表中，选择要使用的身份凭据。默认值为 **无**。
    - **连接时提示输入 PIN：** 选择是否在用户连接到网络时提示他们输入 PIN。默认值为 **关闭**。

    - **启用按需 VPN：** 选择是否在用户连接到网络时启用触发 VPN 连接。默认值为 **关闭**。有关在 **启用按需 VPN** 为 **开启** 时配置设置的信息，请参阅 配置按需 VPN 设置。

  - **每应用 VPN：** 选择是否启用每应用 VPN。默认值为 **关闭**。如果启用此选项，请配置以下设置：

    - **按需匹配应用已启用：** 选择当链接到每应用 VPN 服务的应用发起网络通信时，每应用 VPN 连接是否自动触发。
    - **Safari 域：** 对于要包含的每个可以触发每应用 VPN 连接的 Safari 域，单击 **添加** 并执行以下操作：

      - **域：** 键入要添加的域。
      - 单击 **保存** 以保存域，或单击 **取消** 以不保存域。

- **自定义 XML：** 对于要添加的每个自定义 XML 参数，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。
  - 点击“**保存**”以保存域，或点击“**取消**”以不保存域。

配置启用按需 VPN 选项

- **按需域：** 对于要添加的每个域以及用户连接到这些域时要执行的相关操作，请单击“**添加**”并执行以下操作：

  - **域：** 键入要添加的域。
  - **操作：** 在列表中选择一个可能的操作：

    - **始终建立：** 该域始终触发 VPN 连接。
    - **从不建立：** 该域从不触发 VPN 连接。
    - **必要时建立：** 如果域名解析失败，该域会触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，就会发生失败。

  - 点击“**保存**”以保存域，或点击“**取消**”以不保存域。

- **按需规则**

  - **操作：** 在列表中，选择要执行的操作。默认值为 **EvaluateConnection**。可能的操作包括：

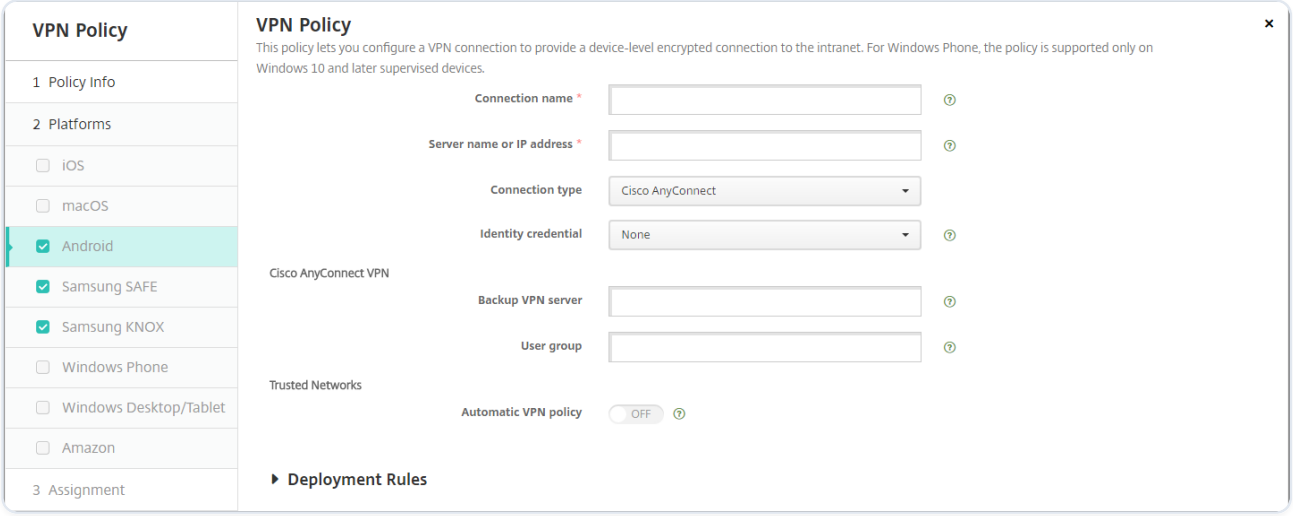
    - **允许：** 允许按需 VPN 在触发时连接。
    - **连接：** 无条件启动 VPN 连接。

    - **断开连接：** 删除 VPN 连接，并且只要规则匹配，就不要按需重新连接。
    - **EvaluateConnection：** 评估每个连接的 **ActionParameters** 数组。
    - **忽略**：保持任何现有 VPN 连接处于活动状态，但只要规则匹配，就不要按需重新连接。
- **DNS 域匹配**：对于要添加的、用户设备的搜索域列表可以匹配的每个域，单击“**添加**”并执行以下操作：
    - **DNS 域**：键入域名。您可以使用通配符“*”前缀来匹配多个域。例如，*.example.com 匹配 mydomain.example.com、yourdomain.example.com 和 herdomain.example.com。
    - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。
- **DNS 服务器地址匹配**：对于要添加的、网络中任何指定 DNS 服务器可以匹配的每个 IP 地址，单击“**添加**”并执行以下操作：
    - **DNS 服务器地址**：键入要添加的 DNS 服务器地址。您可以使用通配符“*”后缀来匹配 DNS 服务器。例如，17.* 匹配 A 类子网中的任何 DNS 服务器。
    - 单击“**保存**”以保存 DNS 服务器地址，或单击“**取消**”以不保存 DNS 服务器地址。
- **接口类型匹配**：在列表中，单击正在使用的主要网络接口硬件类型。默认值为“**未指定**”。可能的值包括：
    - **未指定**：匹配任何网络接口硬件。此选项为默认值。
    - **以太网**：仅匹配以太网网络接口硬件。
    - **Wi-Fi**：仅匹配 Wi-Fi 网络接口硬件。
    - **蜂窝**：仅匹配蜂窝网络接口硬件。
- **SSID 匹配**：对于要添加的、与当前网络匹配的每个 SSID，单击“**添加**”并执行以下操作。
    - **SSID**：键入要添加的 SSID。如果网络不是 Wi-Fi 网络，或者 SSID 未出现，则匹配失败。将此列表留空以匹配任何 SSID。
    - 单击“**保存**”以保存 SSID，或单击“**取消**”以不保存 SSID。
- **URLStringProbe：** 键入要获取的 URL。如果此 URL 在没有重定向的情况下成功获取，则此规则匹配。
- **ActionParameters : Domains：** 对于 EvaluateConnection 检查的每个要添加的域，单击“**添加**”并执行以下操作：
    - **Domain：** 键入要添加的域。
    - 单击“**保存**”以保存域，或单击“**取消**”以不保存域。

- **ActionParameters : DomainAction：** 在列表中，为指定的 **ActionParameters : Domains** 域选择 **VPN 行为**。默认值为 **ConnectIfNeeded**。可能的操作包括：
  - **ConnectIfNeeded：** 如果域名解析失败，该域将触发 VPN 连接尝试。当 DNS 服务器无法解析域、重定向到其他服务器或超时时，会发生故障。
  - **NeverConnect：** 该域从不触发 VPN 连接。
- **Action Parameters: RequiredDNSServers：** 对于用于解析指定域的每个 DNS 服务器 IP 地址，单击“**添加**”并执行以下操作：
  - **DNS Server：** 仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。键入要添加的 DNS 服务器。此服务器无需是设备当前网络配置的一部分。如果 DNS 服务器不可达，则会建立 VPN 连接作为响应。此 DNS 服务器必须是内部 DNS 服务器或受信任的外部 DNS 服务器。
  - 单击“**保存**”以保存 DNS 服务器，或单击“**取消**”以不保存 DNS 服务器。
- **ActionParameters : RequiredURLStringProbe：** （可选）键入要探测的 HTTP 或 HTTPS（首选）URL，使用 GET 请求。如果 URL 的主机名无法解析、服务器不可达或服务器没有响应，则会建立 VPN 连接。仅当 **ActionParameters** : **DomainAction** = **ConnectIfNeeded** 时有效。
- **OnDemandRules : XML content：** 键入或复制粘贴 XML 按需配置规则。
  - 单击“**检查字典**”以验证 XML 代码。如果 XML 有效，您将在“**XML content**”文本框下方的绿色文本中看到“Valid XML”。如果无效，您将在橙色文本中看到描述错误的错误消息。

- **代理**
  - **代理配置：** 在列表中，选择 VPN 连接如何通过代理服务器路由。默认值为 **None**。
    - 如果您启用**手动**，请配置以下设置：
      - **代理服务器的主机名或 IP 地址：** 键入代理服务器的主机名或 IP 地址。此字段为必填项。
      - **代理服务器端口：** 键入代理服务器端口号。此字段为必填项。
      - **用户名：** 键入可选的代理服务器用户名。
      - **密码：** 键入可选的代理服务器密码。
    - 如果您配置**自动**，请配置以下设置：
      - **代理服务器 URL：** 键入代理服务器的 URL。此字段为必填项。

Android 设置



配置适用于 Android 的 Cisco AnyConnect VPN 协议

- **连接名称：** 键入 Cisco AnyConnect VPN 连接的名称。此字段为必填项。
- **服务器名称或 IP 地址：** 键入 VPN 服务器的名称或 IP 地址。此字段为必填项。
- **身份凭据：** 在列表中，选择一个身份凭据。
- **备份 VPN 服务器：** 键入备份 VPN 服务器信息。
- **用户组：** 键入用户组信息。
- **信任网络**
  - **自动 VPN 策略：** 启用或禁用此选项，以设置 VPN 对信任和非信任网络的反应方式。如果启用，请配置以下设置：
    - **信任网络策略：** 在列表中，选择所需的策略。默认值为 **断开连接**。可能的选项包括：
      - **断开连接：** 客户端在信任网络中终止 VPN 连接。此设置为默认值。
      - **连接：** 客户端在信任网络中启动 VPN 连接。
      - **不执行任何操作：** 客户端不执行任何操作。
      - **暂停：** 当用户在信任网络外部建立 VPN 会话，然后进入配置为信任的网络时，VPN 会话将暂停。当用户再次离开信任网络时，会话将恢复。此设置消除了在离开信任网络后重新建立 VPN 会话的需要。
    - **非信任网络策略：** 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：** 客户端在非信任网络中启动 VPN 连接。
      - **不执行任何操作：** 客户端在非信任网络中启动 VPN 连接。此选项会禁用始终开启的 VPN。

- **信任域：** 对于客户端位于信任网络中时网络接口拥有的每个域后缀，单击 **添加** 以执行以下操作：
  - **域：** 键入要添加的域。
  - 单击 **保存** 以保存域，或单击 **取消** 以不保存域。
- **信任服务器：** 对于客户端位于信任网络中时网络接口拥有的每个服务器地址，单击 **添加** 并执行以下操作：
  - **服务器：** 键入要添加的服务器。
  - 点击“**保存**”以保存服务器，或点击“**取消**”以不保存服务器。

配置适用于 Android 的 Citrix SSO 协议

- **连接名称：** 键入 VPN 连接的名称。此字段为必填项。
- **服务器名称或 IP 地址：** 键入 Citrix Gateway 的 FQDN 或 IP 地址。
- **连接的身份验证类型：** 选择一种身份验证类型，并填写该类型出现的任何字段：
  - **用户名**和**密码：** 为“**密码**”或“**密码和证书**”的**身份验证类型**键入您的 VPN 凭据。可选。如果您不提供 VPN 凭据，Citrix VPN 应用程序将提示输入用户名和密码。
  - **身份凭据：** 适用于“**证书**”或“**密码和证书**”的**身份验证类型**。在列表中，选择一个身份凭据。
- **启用每应用 VPN：** 选择是否启用每应用 VPN。如果不启用每应用 VPN，所有流量都将通过 Citrix VPN 隧道。如果启用每应用 VPN，请指定以下设置。默认值为“**关**”。
  - **白名单**或**黑名单：** 如果是“**白名单**”，则所有允许的应用程序都通过此 VPN 隧道传输。如果是“**黑名单**”，则除阻止列表上的应用程序外，所有应用程序都通过此 VPN 隧道传输。

    > **注意：**
    >
    > XenMobile® Server 控制台包含“黑名单”和“白名单”术语。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

  - **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包名称列表。
- **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：

- **DisableUserProfiles：** 可选。要启用此参数，请为“**值**”键入“**是**”。如果启用，XenMobile 不会显示用户添加的 VPN 连接，并且用户无法添加连接。此设置为全局限制，适用于所有 VPN 配置文件。
- **userAgent：** 字符串值。您可以指定自定义用户代理字符串以在每个 HTTP 请求中发送。指定的用户代理字符串将附加到现有 Citrix VPN 用户代理。

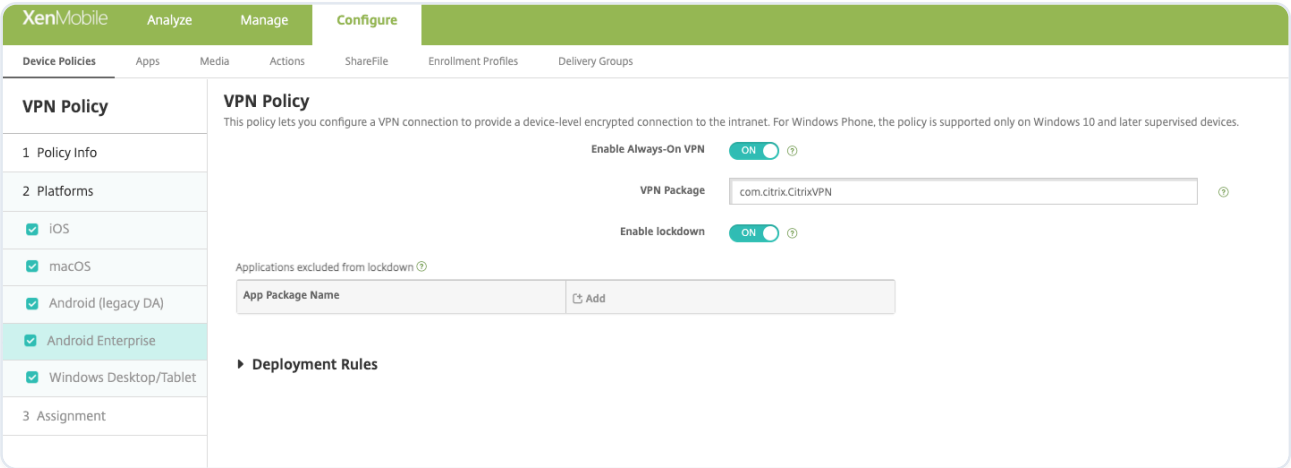
配置 VPN 以支持 NAC

1. 使用 **连接类型 自定义 SSL** 来配置 NAC 过滤器。
2. 指定 **连接名称** 为 **VPN**。
3. 对于 **自定义 XML**，单击 **添加** 并执行以下操作：
   - **参数名称：** 键入 **XenMobileDeviceId**。此字段是用于根据 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 VPN 连接。否则，在建立 VPN 时将拒绝身份验证。
   - **值：** 键入 **DeviceID_${device.id}**，这是参数 **XenMobileDeviceId** 的值。
   - 单击 **保存** 以保存参数。

为 Android Enterprise 配置 VPN

要为 Android Enterprise 设备配置 VPN，请为 Citrix SSO 应用程序创建托管配置设备策略。请参阅为 Android Enterprise 配置 VPN 配置文件。

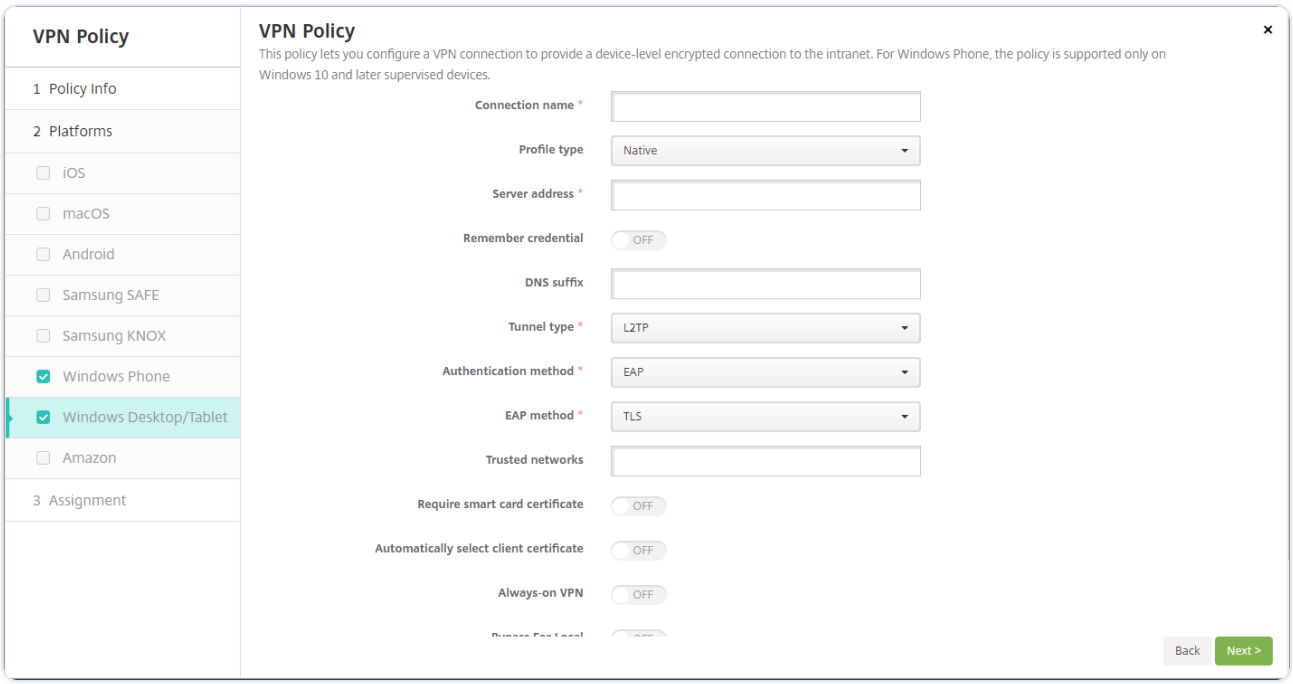
安卓企业设置



- **启用始终开启的 VPN：** 选择 VPN 是否始终开启。默认值为 **关闭**。启用后，VPN 连接将保持开启状态，直到用户手动断开连接。
- **VPN 包：** 键入设备使用的 VPN 应用程序的包名称。

- **启用锁定：** 如果禁用，则在 VPN 连接不存在时，任何应用程序都无法访问网络。如果启用，则在以下设置中配置的应用程序可以访问网络，即使 VPN 连接不存在。适用于 Android 10 及更高版本的设备。
- **从锁定中排除的应用程序：** 单击 **添加** 以键入要绕过锁定设置的应用程序的包名称。

视窗桌面／平板电脑设置



- **连接名称：** 输入连接的名称。此字段为必填项。
- **配置文件类型：** 在列表中，选择**本机**或**插件**。默认值为**本机**。
- **配置本机配置文件类型：** 这些设置适用于用户 Windows 设备中内置的 VPN。
  - **服务器地址：** 键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填项。
  - **记住凭据：** 选择是否缓存凭据。默认值为**关闭**。启用后，凭据将尽可能缓存。
  - **DNS 后缀：** 键入 DNS 后缀。
  - **隧道类型：** 在列表中，选择要使用的 VPN 隧道类型。默认值为**L2TP**。可能的选项包括：
    - **L2TP：** 带有预共享密钥身份验证的第 2 层隧道协议。
    - **PPTP：** 点对点隧道协议。
    - **IKEv2：** Internet 密钥交换版本 2。
  - **身份验证方法：** 在列表中，选择要使用的身份验证方法。默认值为**EAP**。可能的选项包括：
    - **EAP：** 可扩展身份验证协议。

    - **MSChapV2：** 使用 Microsoft 的质询握手身份验证进行相互身份验证。当您为隧道类型选择 **IKEv2** 时，此选项不可用。

  - **EAP 方法：** 在列表中，选择要使用的 EAP 方法。默认值为 **TLS**。启用 MSChapV2 身份验证时，此字段不可用。可用选项包括：

    - **TLS：** 传输层安全性
    - **PEAP：** 受保护的可扩展身份验证协议

  - **受信任的网络：** 键入一个用逗号分隔的网络列表，这些网络不需要 VPN 连接即可访问。例如，当用户位于公司无线网络上时，他们可以直接访问受保护的资源。
  - **需要智能卡证书：** 选择是否需要智能卡证书。默认值为 **关**。
  - **自动选择客户端证书：** 选择是否自动选择用于身份验证的客户端证书。默认值为 **关**。启用“**需要智能卡证书**”时，此选项不可用。
  - **始终开启 VPN：** 选择 VPN 是否始终开启。默认值为 **关**。启用后，VPN 连接将保持开启状态，直到用户手动断开连接。
  - **本地绕过：** 键入地址和端口号，以允许本地资源绕过代理服务器。

- **配置插件配置文件类型：** 这些设置适用于从 Windows 应用商店获取并安装在用户设备上的 VPN 插件。

  - **服务器地址：** 键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填项。
  - **记住凭据：** 选择是否缓存凭据。默认值为 **关**。启用后，凭据将尽可能缓存。
  - **DNS 后缀：** 键入 DNS 后缀。
  - **客户端应用 ID：** 键入 VPN 插件的包系列名称。
  - **插件配置文件 XML：** 通过单击“**浏览**”并导航到文件位置，选择要使用的自定义 VPN 插件配置文件。有关格式和详细信息，请联系插件提供商。
  - **受信任的网络：** 键入一个用逗号分隔的网络列表，这些网络不需要 VPN 连接即可访问。例如，当用户位于公司无线网络上时，他们可以直接访问受保护的资源。
  - **始终开启 VPN：** 选择 VPN 是否始终开启。默认值为**关闭**。启用后，VPN 连接将保持开启状态，直到用户手动断开连接。
  - **本地旁路：** 键入地址和端口号，以允许本地资源绕过代理服务器。

壁纸设备策略

您可以添加 .png 或 .jpg 文件，以在 iOS 设备的锁定屏幕、主屏幕或两者上设置壁纸。此功能仅适用于 iOS 7.1.2 及更高版本中的受监管设备。要在 iPad 和 iPhone 上使用不同的壁纸，您需要创建不同的壁纸策略并将其部署给相应的用户。

下表列出了 Apple 推荐的 iOS 设备图像尺寸。

iPhone

设备	图像尺寸（像素）
苹果 iPhone 12 Pro Max	2778 x 1284
iPhone 12 和 iPhone 12 Pro	2532 x 1170
苹果 iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
苹果 XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 第二代	1334 x 750
苹果 7 PLus, 8 PLus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 加	1334 x 750
iPhone 8	1334 x 750

iPad

设备	图像尺寸（像素）
iPad Pro（第 1、2 和 3 代 12.9 英寸）	2732 x 2048
iPad Pro 10.5 英寸	2224 x 1668
iPad Pro（9.7 英寸）	1536 x 2048
iPad Air 2	2048 x 1536

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

- **应用到：** 在列表中，选择 **锁定屏幕**、**主屏幕（图标列表）** 或 **锁定和主屏幕** 以设置壁纸显示位置。
- **壁纸文件：** 通过单击 **浏览** 并导航到文件位置来选择壁纸文件。

网页内容筛选器设备策略

您可以在 XenMobile 中添加设备策略，通过使用 Apple 的自动筛选功能以及您添加到允许列表和阻止列表中的特定站点，在 iOS 设备上筛选网页内容。此策略仅适用于处于监督模式的 iOS 7.0 及更高版本设备。有关将 iOS 设备置于监督模式的信息，请参阅 使用 Apple Configurator 将 iOS 设备置于监督模式。

> **注意：**
>
> - Android 设备不支持网页内容筛选。
> - 从 iOS 16.5 及更高版本开始，网页内容筛选器设备策略停止识别允许列表中的 `https://localhost`。此问题会导致某些应用程序无响应。此外，在允许列表中添加 URL 的派生形式（例如 `http://localhost:`、`http://localhost:*` 等）也无法解决此问题。

> 要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

iOS 设置

- **筛选器类型：** 在下拉列表中单击**内置**或**插件**，然后按照所选选项的步骤操作。默认值为**内置**。

内置筛选器类型

- **网页内容筛选器**
  - **启用自动筛选：** 是否使用 Apple 自动筛选功能分析网站是否存在不当内容。默认值为**关**。
  - **允许的 URL：** 当**启用自动筛选**设置为**关**时，此列表将被忽略。当**启用自动筛选**设置为**开**时，无论自动筛选器是否允许访问，此列表中的项目始终可访问。对于要添加到允许列表的每个 URL，请单击**添加**并执行以下操作：
    - 键入允许的网站的 URL。您必须在网址前添加 `http://` 或 `https://`。
    - 单击**保存**将网站保存到允许列表，或单击**取消**不保存。
  - **阻止的 URL：** 此列表中的项目始终被阻止。对于要添加到阻止列表的每个 URL，请单击**添加**并执行以下操作：
    - 输入要阻止的网站 URL。您必须在网址前添加 `http://` 或 `https://`。
    - 单击“**保存**”将网站保存到阻止列表，或单击“**取消**”不保存。

> **注意：**
>
> XenMobile® Server 控制台包含术语“黑名单”和“白名单”。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

- **书签白名单**
  - **书签白名单：** 指定用户可以访问的站点。要启用对网站的访问，请添加其 URL。
    - **URL：** 用户可以访问的每个网站的 URL。例如，要启用对 Secure Hub 商店的访问，请将 XenMobile Server URL 添加到“**URL**”列表。您必须在网址前添加 `http://` 或 `https://`。此字段为必填项。
    - **书签文件夹：** 输入可选的书签文件夹名称。如果此字段留空，则书签将添加到默认书签目录。
    - **标题：** 输入网站的描述性标题。例如，对于 URL `https://google.com`，键入“Google”。
    - 单击“**保存**”将网站保存到允许列表，或单击“**取消**”不保存。

插件筛选器类型

- **筛选器名称：** 输入筛选器的唯一名称。
- **标识符：** 输入提供筛选服务的插件的捆绑包 ID。
- **服务地址：** 输入可选的服务器地址。有效格式为 IP 地址、主机名或 URL。
- **用户名：** 输入服务的可选用户名。
- **密码：** 输入服务的可选密码。
- **证书：** 在下拉列表中单击一个可选的身份证书，该证书将用于向服务验证用户身份。默认值为“**无**”。
- **筛选 WebKit 流量：** 选择是否筛选 WebKit 流量。
- **筛选套接字流量：** 选择是否筛选套接字流量。
- **自定义数据：** 对于要添加到 Web 筛选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。
- **策略设置**
  - **删除策略：** 选择计划策略删除的方法。可用选项包括“**选择日期**”和“**删除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除。仅适用于 iOS 6.0 及更高版本。

Web 剪辑设备策略

您可以将网站的快捷方式（或 Web 剪辑）放置在用户设备上，使其与应用程序一同显示。您可以为 iOS、iPadOS、macOS 和 Android 设备指定自己的图标来表示 Web 剪辑。Windows 平板电脑仅需要标签和 URL。对于 iOS 和 iPadOS 设备，请配置主屏幕布局设备策略以组织您创建的 Web 剪辑。如果您限制 iOS 上的应用程序访问，请确保配置限制设备策略以允许 Web 剪辑。有关配置这些策略的信息，请参阅主屏幕布局设备策略和限制设备策略。

要添加或配置此策略，请转至 **配置 > 设备策略**。有关详细信息，请参阅设备策略。

iOS 设置

- **标签：** 键入将与 Web 剪辑一同显示的标签。
- **URL：** 键入与 Web 剪辑关联的 URL。URL 必须以协议开头，例如 `https://server`。
- **可移除：** 选择用户是否可以移除 Web 剪辑。默认值为“**关**”。共享 iPad 不支持此选项。
- **要更新的图标：** 通过单击“**浏览**”并导航到文件位置来选择要用于 Web 剪辑的图标。
- **预合成图标：** 选择是否对图标应用效果（圆角、阴影和反射光泽）。默认值为“**关**”，这会添加效果。
- **全屏：** 选择链接的网页是否以全屏模式打开。默认值为“**关**”。
- **策略设置**
  - **移除策略：** 选择一种计划策略移除的方法。可用选项包括“**选择日期**”和“**移除前持续时间（小时）**”
    - **选择日期：** 单击日历以选择具体的移除日期。
    - **移除前持续时间（小时）：** 键入一个数字（以小时为单位），表示策略移除发生前的持续时间。仅适用于 iOS 6.0 及更高版本。
  - **配置文件范围：** 选择策略是应用于用户还是整个系统。默认值为“**系统**”。仅适用于 iOS 9.3 及更高版本。

macOS 设置

- **标签：** 键入将与 Web 剪辑一起显示的标签。
- **URL：** 键入与 Web 剪辑关联的 URL。URL 必须以协议开头，例如 `https://server`。
- **要更新的图标：** 单击“浏览”并导航到文件位置，选择要用于 Web 剪辑的图标。

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：** 键入将与 Web 剪辑一起显示的标签。
- **URL：** 键入与 Web 剪辑关联的 URL。
- **定义图标：** 选择是否使用图标文件。默认值为“**关**”。
- **图标文件：** 如果“**定义图标**”为“**开**”，请单击“**浏览**”并导航到文件位置，选择要使用的图标文件。
- **策略设置**
  - **删除策略：** 选择一种方法来安排策略删除。可用选项为“**选择日期**”和“**直到删除的持续时间（小时）**”

    - **选择日期：** 单击日历以选择具体的删除日期。
    - **直到删除的持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。
  - **允许用户删除策略：** 您可以选择用户何时可以从其设备中删除策略。从菜单中选择“**始终**”、“**需要密码**”或“**从不**”。如果选择“**需要密码**”，请在“**删除密码**”字段中键入密码。
  - **配置文件范围：** 选择此策略是应用于**用户**还是整个**系统**。默认值为**用户**。此选项仅适用于 macOS 10.7 及更高版本。

视窗桌面/平板电脑设置

- **名称：** 键入将与 Web Clip 一起显示的标签。
- **URL：** 键入与 Web Clip 关联的 URL。

Wi-Fi 设备策略

您可以使用 **Configure > Device Policies** 页面在 XenMobile® 中创建新的或编辑现有的 Wi-Fi 设备策略。Wi-Fi 策略允许您通过定义以下各项来管理用户如何将其设备连接到 Wi-Fi 网络：

- 网络名称和类型
- 身份验证和安全策略
- 代理服务器的使用
- 其他 Wi-Fi 相关详细信息

要添加或配置此策略，请转至 **Configure > Device Policies**。有关详细信息，请参阅 设备策略。

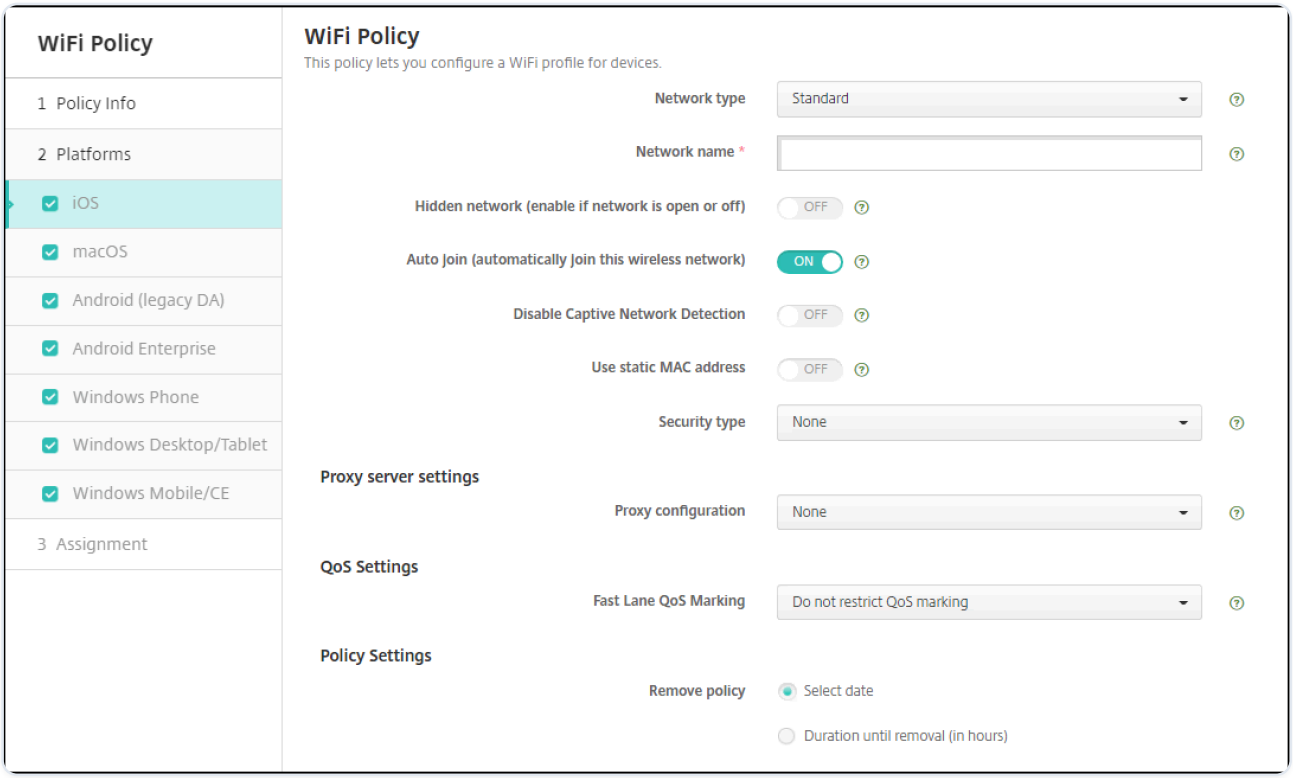
先决条件

在创建策略之前，请务必完成以下步骤：

- 创建您计划使用的任何交付组。
- 了解网络名称和类型。
- 了解您计划使用的任何身份验证或安全类型。
- 了解您可能需要的任何代理服务器信息。
- 安装任何必要的 CA 证书。
- 拥有任何必要的共享密钥。
- 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，请参阅身份验证及其子文章。

iOS 设置



- **网络类型：** 在列表中，选择**标准**、**旧版热点**或**热点 2.0**以设置您计划使用的网络类型。
- **网络名称：** 键入设备可用网络列表中显示的 SSID。不适用于**热点 2.0**。
- **隐藏网络（如果网络开放或关闭，则启用）：** 选择网络是否隐藏。
- **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。用户必须先断开与上一个网络的连接，设备才能自动连接。默认设置为**开**。
- **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。为了增强隐私性，iOS 和 iPadOS 设备每次连接到网络时都可以使用不同的 MAC 地址。如果设置为**开**，设备在连接到此网络时始终使用相同的 MAC 地址。如果设置为**关**，设备每次连接到此网络时都会使用不同的 MAC 地址。默认设置为**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**热点 2.0**。
  - 无 - 无需进一步配置。
  - WEP
  - WPA/WPA2 个人
  - 任意（个人）
  - WEP 企业版

- WPA/WPA2 企业版：使用 WPA-2 企业版需要配置简单证书注册协议 (SCEP)。XenMobile 随后可以将证书发送到设备以向 Wi-Fi 服务器进行身份验证。要配置 SCEP，请转到**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。
- 任意 (企业版)

以下各节列出了为上述每种连接类型配置的选项。

适用于 iOS 的 WPA、WPA 个人版、任意 (个人版) 设置

密码： 键入可选密码。如果将此字段留空，用户登录时可能会收到输入密码的提示。

适用于 iOS 的 WEP 企业版、WPA 企业版、WPA2 企业版、任意 (企业版) 设置

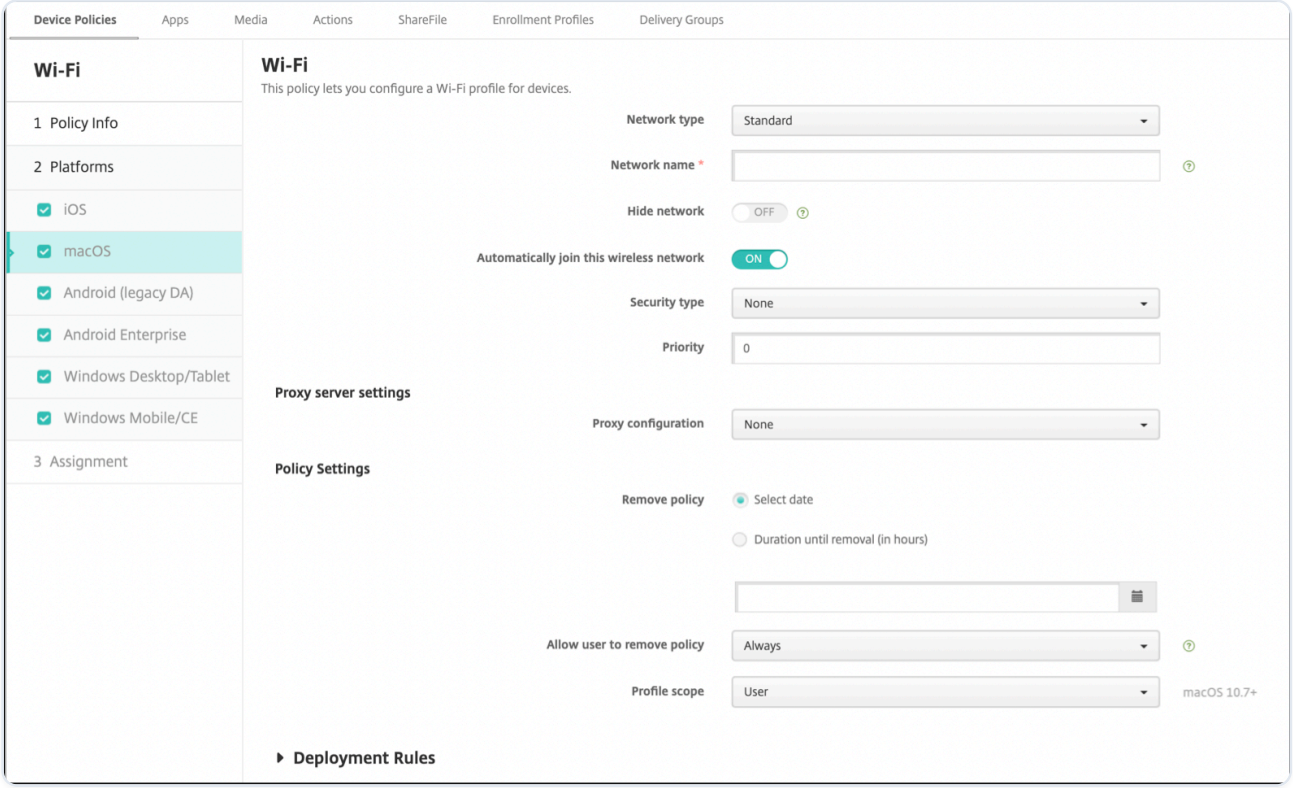
选择其中任何一个设置时，其设置将列在**代理服务器设置**之后。

- **协议，接受的 EAP 类型：** 启用要支持的 EAP 类型，然后配置相关设置。对于每个可用的 EAP 类型，默认值为**关闭**。
- **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**，选择是否使用预配 PAC。
    - 如果选择**预配 PAC**，选择是否允许最终用户客户端与 XenMobile 之间进行匿名 TLS 握手。
      - **匿名预配 PAC**
- **身份验证：**
  - **用户名：** 键入用户名。
  - **每次连接密码：** 选择是否要求用户每次登录时都输入密码。
  - **密码：** 键入可选密码。如果将此字段留空，用户登录时可能会被提示输入密码。
  - **身份凭据（密钥库或 PKI 凭据）：** 在列表中，选择身份凭据的类型。默认值为 **无**。
  - **外部身份：** *仅在启用* **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“匿名”等通用术语来提高安全性，从而使用户名不可见。
  - **需要 TLS 证书：** 选择是否需要 TLS 证书。
- **信任**

- **受信任的证书：** 要添加受信任的证书，请单击 **添加**，然后对要添加的每个证书执行以下操作：
  - **应用程序：** 在列表中，选择要添加的应用程序。
  - 单击 **保存** 以保存证书，或单击 **取消**。
- **受信任的服务器证书名称：** 要添加受信任的服务器证书通用名称，请单击 **添加**，然后对要添加的每个名称执行以下操作：
  - **证书：** 键入服务器证书的名称。您可以使用通配符指定名称，例如 wpa.*.example.com。
  - 单击 **保存** 以保存证书名称，或单击 **取消**。

- **允许信任例外：** 选择当证书不受信任时，是否在用户设备上显示证书信任对话框。默认值为 **开**。
- **代理服务器设置**
  - **代理配置：** 在列表中，选择**无**、**手动**或**自动**以设置VPN连接如何通过代理服务器路由，然后配置任何其他选项。默认值为**无**，无需进一步配置。
  - 如果选择**手动**，请配置以下设置：
    - **主机名/IP地址：** 键入代理服务器的主机名或IP地址。
    - **端口：** 键入代理服务器端口号。
    - **用户名：** 键入可选的用户名以向代理服务器进行身份验证。
    - **密码：** 键入可选密码以向代理服务器进行身份验证。
  - 如果选择**自动**，请配置以下设置：
    - **服务器URL：** 键入定义代理配置的PAC文件的URL。
    - **如果PAC不可达，则允许直接连接：** 选择当PAC文件不可达时是否允许用户直接连接到目标。默认值为**开**。此选项仅适用于iOS 7.0及更高版本。
- **策略设置**
  - **删除策略：** 选择一种计划策略删除的方法。可用选项为**选择日期**和**删除前持续时间（小时）**
    - **选择日期：** 单击日历以选择具体的删除日期。
    - **删除前持续时间（小时）：** 键入一个数字（以小时为单位），直到策略删除发生。仅适用于iOS 6.0及更高版本。

macOS 设置



- **网络类型：** 在列表中，选择**标准**、**旧版热点**或**热点 2.0**以设置您计划使用的网络类型。
- **网络名称：** 键入设备可用网络列表中显示的 SSID。不适用于**热点 2.0**。
- **隐藏网络：** 选择是否要隐藏网络。
- **自动加入此无线网络：** 选择是否自动加入网络。如果设备已连接到另一个网络，则不会加入此网络。用户必须先断开与上一个网络的连接，设备才会自动连接。默认设置为**开**。
- **安全类型：** 在列表中，选择您计划使用的安全类型。不适用于**热点 2.0**。
  - 无 - 无需进一步配置。
  - WEP
  - WPA/WPA2 个人
  - 任意（个人）
  - WEP 企业
  - WPA/WPA2 企业
  - 任意（企业）
- **优先级：** 如果有多个网络，请在**优先级**字段中键入一个数字以设置网络连接的优先级。设备将选择数字最小的网络。

以下各节列出了为上述每种连接类型配置的选项。

macOS 的 WPA、WPA 个人、WPA 2 个人、任意（个人）设置

- **密码：** 输入一个可选密码。如果您将此字段留空，用户在登录时可能会被要求输入密码。

WEP 企业版、WPA 企业版、WPA2 企业版、任意（企业版）macOS 设置

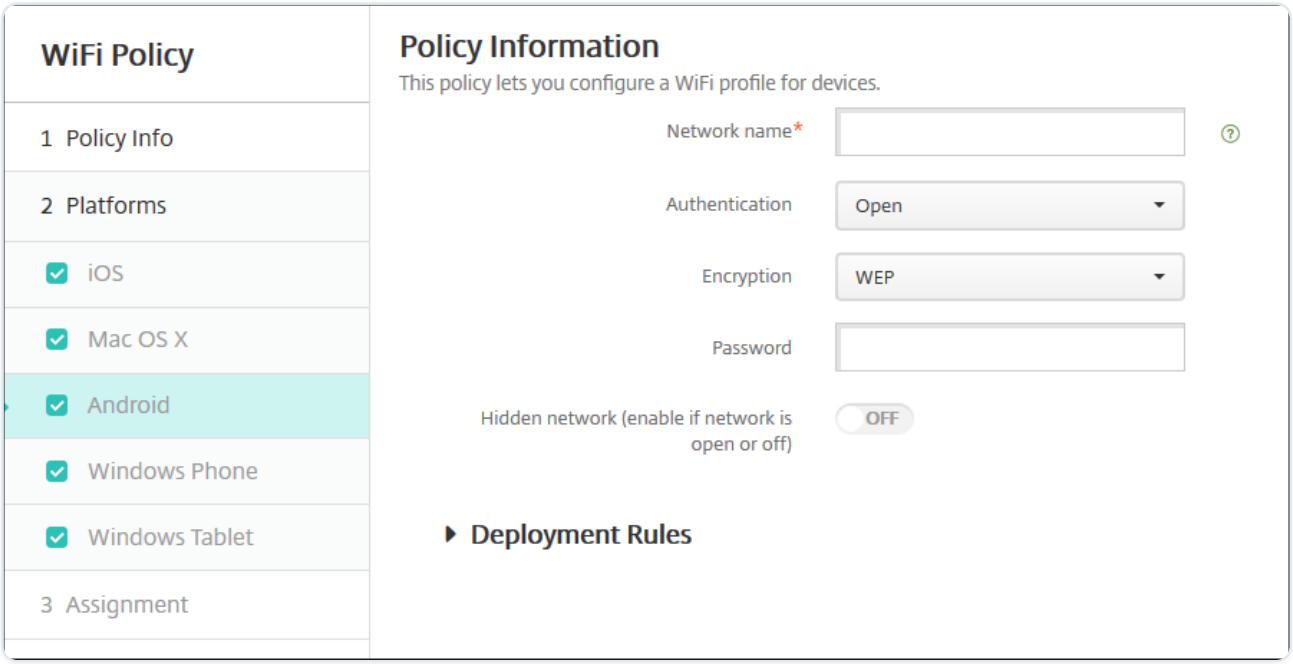
当您选择这些设置中的任何一个时，它们的设置将列在**代理服务器设置**之后。

- **协议，接受的 EAP 类型：** 启用您想要支持的 EAP 类型，然后配置相关设置。对于每个可用的 EAP 类型，默认值为**关闭**。
- **内部身份验证 (TTLS)：** *仅当您启用 TTLS 时才需要*。在列表中，选择要使用的内部身份验证方法。选项包括：**PAP**、**CHAP**、**MSCHAP** 或 **MSCHAPv2**。默认值为 **MSCHAPv2**。
- **协议，EAP-FAST：** 选择是否使用受保护的访问凭据 (PAC)。
  - 如果您选择**使用 PAC**，请选择是否使用预配 PAC。
    - 如果您选择**预配 PAC**，请选择是否允许最终用户客户端和 XenMobile 之间进行匿名 TLS 握手。
      - **匿名预配 PAC**
- **身份验证：**
  - **用户名：** 输入用户名。
  - **每次连接密码：** 选择是否要求用户每次登录时都输入密码。
  - **密码：** 输入一个可选密码。如果您将此字段留空，用户在登录时可能会被要求输入密码。
  - **身份凭据（密钥库或 PKI 凭据）：** 在列表中，选择身份凭据的类型。默认值为**无**。
  - **外部身份：** *仅当您启用* **PEAP**、**TTLS** *或* **EAP-FAST** 时才需要。输入外部可见的用户名。您可以通过输入“匿名”之类的通用术语来提高安全性，从而使用户名不可见。
  - **要求 TLS 证书：** 选择是否要求 TLS 证书。
- **信任**
  - **受信任证书：** 要添加受信任证书，请单击**添加**，然后对要添加的每个证书执行以下操作：
    - **应用程序：** 在列表中，选择要添加的应用程序。
    - 单击**保存**以保存证书，或单击**取消**。
  - **受信任服务器证书名称：** 要添加受信任服务器证书的通用名称，请单击**添加**，然后对要添加的每个名称执行以下操作：

  - **证书：** 键入要添加的服务器证书的名称。您可以使用通配符指定名称，例如 wpa.*.example.com。
  - 单击**保存**以保存证书名称，或单击**取消**。

- **允许信任例外：** 选择当证书不受信任时，是否在用户设备上显示证书信任对话框。默认值为**开**。
- **用作登录窗口配置：** 选择是否使用在登录窗口输入的相同凭据来验证用户。
- **代理服务器设置**
  - **代理配置：** 在列表中，选择**无**、**手动**或**自动**以设置 VPN 连接如何通过代理服务器路由，然后配置任何其他选项。默认值为**无**，无需进一步配置。
  - 如果选择**手动**，请配置以下设置：
    - **主机名/IP 地址：** 键入代理服务器的主机名或 IP 地址。
    - **端口：** 键入代理服务器的端口号。
    - **用户名：** 键入可选的用户名，以向代理服务器进行身份验证。
    - **密码：** 键入可选的密码，以向代理服务器进行身份验证。
  - 如果选择**自动**，请配置以下设置：
    - **服务器 URL：** 键入定义代理配置的 PAC 文件的 URL。
    - **如果 PAC 不可访问，则允许直接连接：** 选择如果 PAC 文件不可访问，是否允许用户直接连接到目标。默认值为**开**。此选项仅适用于 iOS 7.0 及更高版本。

Android 设置



- **网络名称：** 键入用户设备上可用网络列表中的 SSID。
- **身份验证：** 在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - 共享
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下部分列出了您可以为上述每种连接类型配置的选项。

Android 的开放、共享设置

- **加密：** 在列表中，选择**禁用**或**WEP**。默认值为**WEP**。
- **密码：** 键入可选密码。

WPA、WPA-PSK、WPA2、WPA2-PSK 的 Android 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。

802.1x 的 Android 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：** 键入可选的外部可见用户名。您可以通过键入“匿名”之类的通用术语来提高安全性，这样用户名就不会显示。
- **CA 证书：** 在列表中，选择要使用的证书。
- **身份凭据**：在列表中，选择要使用的身份凭据。默认值为“**无**”。
- **隐藏网络（如果网络是开放的或关闭的，则启用）**：选择网络是否隐藏。

安卓企业版设置

Wi-Fi 策略 Android Enterprise 的图像(/en-us/xenmobile/server/media/device-policy-wifi-android-enterprise.png)

- **网络名称**：键入用户设备上可用网络列表中的 SSID。
- **身份验证**：在列表中，选择用于 Wi-Fi 连接的安全类型。
  - 开放
  - 共享
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下各节列出了为上述每种连接类型配置的选项。

Android Enterprise 的开放、共享设置

- **加密**：在列表中，选择**禁用**或**WEP**。默认值为**WEP**。
- **密码**：键入可选密码。

适用于 Android Enterprise 的 WPA、WPA-PSK、WPA2、WPA2-PSK 设置

- **加密**：在列表中，选择 TKIP 或 AES。默认值为 TKIP。
- **密码**：键入可选密码。

适用于 Android Enterprise 的 802.1x 设置

- **EAP 类型**：在列表中，选择 **PEAP**、**TLS** 或 **TTLS**。默认值为 **PEAP**。
- **密码**：键入可选密码。
- **身份验证阶段 2**：在列表中，选择**无**、**PAP**、**MSCHAP**、**MSCHAPPv2** 或 **GTC**。默认值为 **PAP**。
- **身份**：键入可选的用户名和域。
- **匿名**：键入可选的外部可见用户名。您可以通过键入“anonymous”之类的通用术语来提高安全性，这样用户名就不会可见。
- **CA 证书**：在列表中，选择要使用的证书。
- **域**：键入所需的域名。有关详细信息，请参阅域。

> **注意**：
>
> 在运行 Android 13 或更高版本的设备上配置 Wi-Fi 策略时，必须强制更新**CA 证书**和**域**字段。如果未更新，则配置将失败。

- **身份凭据**：在列表中，选择要使用的身份凭据。默认值为**无**。
- **隐藏网络（如果网络是开放或关闭的，则启用）**：选择网络是否隐藏。

Windows 10 和 Windows 11 设置

设备策略配置屏幕的图像(/en-us/xenmobile/server/media/device-policy-wifi-windesktop.png)

- **身份验证**：单击下拉列表中要用于 Wi-Fi 连接的安全类型。
  - 开放
  - WPA 个人
  - WPA-2 个人
  - WPA 企业

- WPA-2 Enterprise：使用 WPA-2 Enterprise 需要配置 SCEP。SCEP 配置使 XenMobile 能够将证书发送到设备以向 Wi-Fi 服务器进行身份验证。要配置 SCEP，请转到**设置 > 凭据提供程序**的**分发**页面。有关详细信息，请参阅凭据提供程序。

以下各节列出了为上述每种连接类型配置的选项。

Windows 10 和 Windows 11 的开放设置

- **隐藏网络（如果网络是开放或关闭的，则启用）**：选择网络是否隐藏。
- **自动连接**：选择是否自动连接到网络。

Windows 10 和 Windows 11 的 WPA 个人、WPA-2 个人设置

- **加密**：在列表中，选择 **AES** 或 **TKIP** 以设置加密类型。默认值为 **AES**。
- **隐藏网络（如果网络是开放或关闭的，则启用）**：选择网络是否隐藏。
- **自动连接**：选择是否自动连接到网络。

适用于 Windows 10 和 Windows 11 的 WPA-2 企业版设置

- **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**。
- **如果隐藏则连接**：选择网络是否隐藏。
- **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 凭据提供程序**：在列表中，选择 SCEP 凭据提供程序。默认值为 **None**。

Windows 信息保护设备策略

Windows 信息保护 (WIP)，以前称为企业数据保护 (EDP)，是一种 Windows 技术，可防止企业数据潜在泄露。数据泄露可能通过将企业数据共享给非企业保护的应用程序、应用程序之间或组织网络外部而发生。有关详细信息，请参阅 使用 Windows 信息保护 (WIP) 保护您的企业数据。

您可以在 XenMobile® 中创建设备策略，以指定需要 Windows 信息保护的应用程序，并设置其强制级别。Windows 信息保护策略适用于运行 Windows 10 或 Windows 11 的受监督平板电脑和桌面设备。

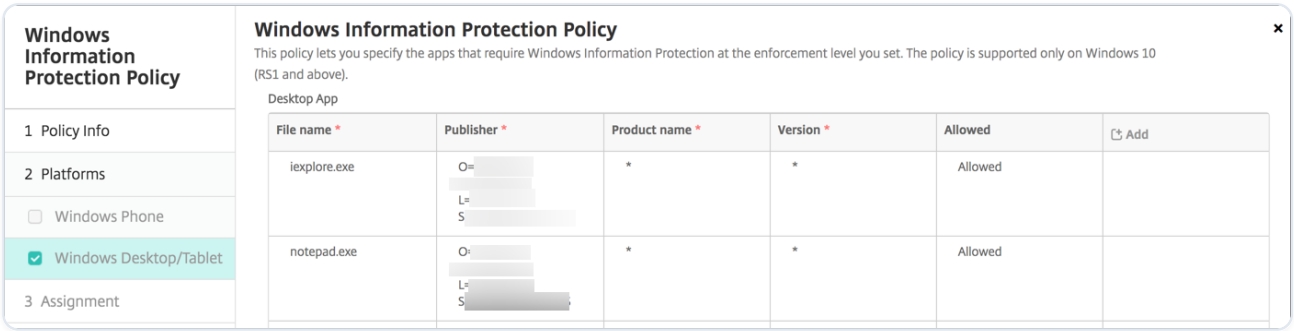
XenMobile 包含一些常用应用程序，您也可以添加其他应用程序。您可以为策略指定一个影响用户体验的强制级别。例如，您可以：

- 阻止任何不适当的数据共享。
- 警告不适当的数据共享，并允许用户覆盖策略。
- 在记录并允许不适当数据共享的同时，静默运行 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 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。

Windows 10 和 Windows 11 设置



- **桌面应用程序** (Windows 10 或 Windows 11 桌面)、**应用商店应用程序** (Windows 10 或 Windows 11 平板电脑)：XenMobile 包含一些常用应用程序，如前面的示例所示。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：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。**拒绝的**应用程序无法访问企业数据。**豁免的**应用程序可以读取企业数据，但无法创建或修改数据。

  - **AppLocker XML：** Microsoft 提供了一份与 WIP 存在已知兼容性问题的 Microsoft 应用程序列表。要将这些应用程序从 WIP 中排除，请单击**浏览**以上传该列表。XenMobile 会将上传的 AppLocker XML 以及策略中配置的桌面和应用商店应用程序结合起来发送到设备。有关详细信息，请参阅 Windows 信息保护的推荐阻止列表。
  - **强制级别：** 选择一个选项以指定您希望 Windows 信息保护如何保护和管理数据共享。默认为“**关闭**”。
    - **0-关闭：** WIP 已关闭，不保护或审计您的数据。
    - **1-静默：** WIP 静默运行，记录不适当的数据共享，并且不阻止任何操作。您可以通过 Reporting CSP 访问日志。
    - **2-覆盖：** WIP 会警告用户可能不安全的数据共享。用户可以覆盖警告并共享数据。此模式会将操作（包括用户覆盖）记录到您的审计日志中。

  - **3-阻止：** WIP 阻止用户完成可能不安全的数据共享。

- **受保护的域名：** 您的企业用于其用户身份的域。此托管身份域列表以及主域构成了您的管理企业的身份。列表中的第一个域是 Windows UI 中使用的主要公司身份。使用“|”分隔列表项。例如：`domain1.com | domain2.com`
- **数据恢复证书：** 单击“**浏览**”，然后选择一个恢复证书，用于加密文件的数据恢复。此证书与加密文件系统 (EFS) 的数据恢复代理 (DRA) 证书相同，只是通过 MDM 而非组策略交付。如果恢复证书不可用，请创建它。有关信息，请参阅本节中的“创建数据恢复证书”。
- **网络域名：** 构成企业边界的域列表。WIP 保护流向此列表中完全限定域的所有流量。此设置与“**IP 范围**”设置一起，用于检测专用网络上的网络终结点是企业还是个人。使用逗号分隔列表项。例如：corp.example.com,region.example.com
- **IP 范围：** 定义企业网络中计算机的企业 IPv4 和 IPv6 范围列表。WIP 将这些位置视为企业数据共享的安全目标。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 范围列表是权威的：** 为防止 Windows 自动检测 IP 范围，请将此设置更改为“**开**”。默认为“**关**”。
- **代理服务器：** 企业可用于公司资源的代理服务器列表。如果您的网络中使用代理，则需要此设置。如果没有代理服务器，当客户端位于代理后面时，企业资源可能不可用。例如，酒店和餐厅的某些 Wi-Fi 热点可能无法提供资源。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：** 您的设备用于访问云资源的代理服务器列表。使用此服务器类型表示您正在连接的云资源是企业资源。请勿在此列表中包含“**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。使用逗号分隔列表项。例如：

  `example.internalproxy1.com;10.147.80.50`
- **云资源：** 受 WIP 保护的云资源列表。对于每个云资源，您还可以选择在“**代理服务器**”列表中指定一个代理服务器，以路由此云资源的流量。所有通过“**代理服务器**”路由的流量都将被视为企业流量。使用逗号分隔列表项。例如：

  `domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.domain2.com`
- **取消注册时吊销 WIP 证书：** 指定当用户设备从 Windows 信息保护取消注册时，是否吊销其本地加密密钥。加密密钥被吊销后，用户将无法访问加密的企业数据。如果设置为“**关**”，则密钥不会被吊销，用户在取消注册后仍可继续访问受保护的文件。默认为“**开**”。
- **显示叠加图标：** 指定是否在资源管理器中的企业文件和“开始”菜单中的仅限企业应用磁贴上包含 Windows 信息保护图标叠加。默认为“**关**”。

创建数据恢复证书

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，打开命令提示符并导航到要创建证书的文件夹（Windows\\System32 除外）。
2. 运行此命令：

   `cipher /r:ESFDRA`

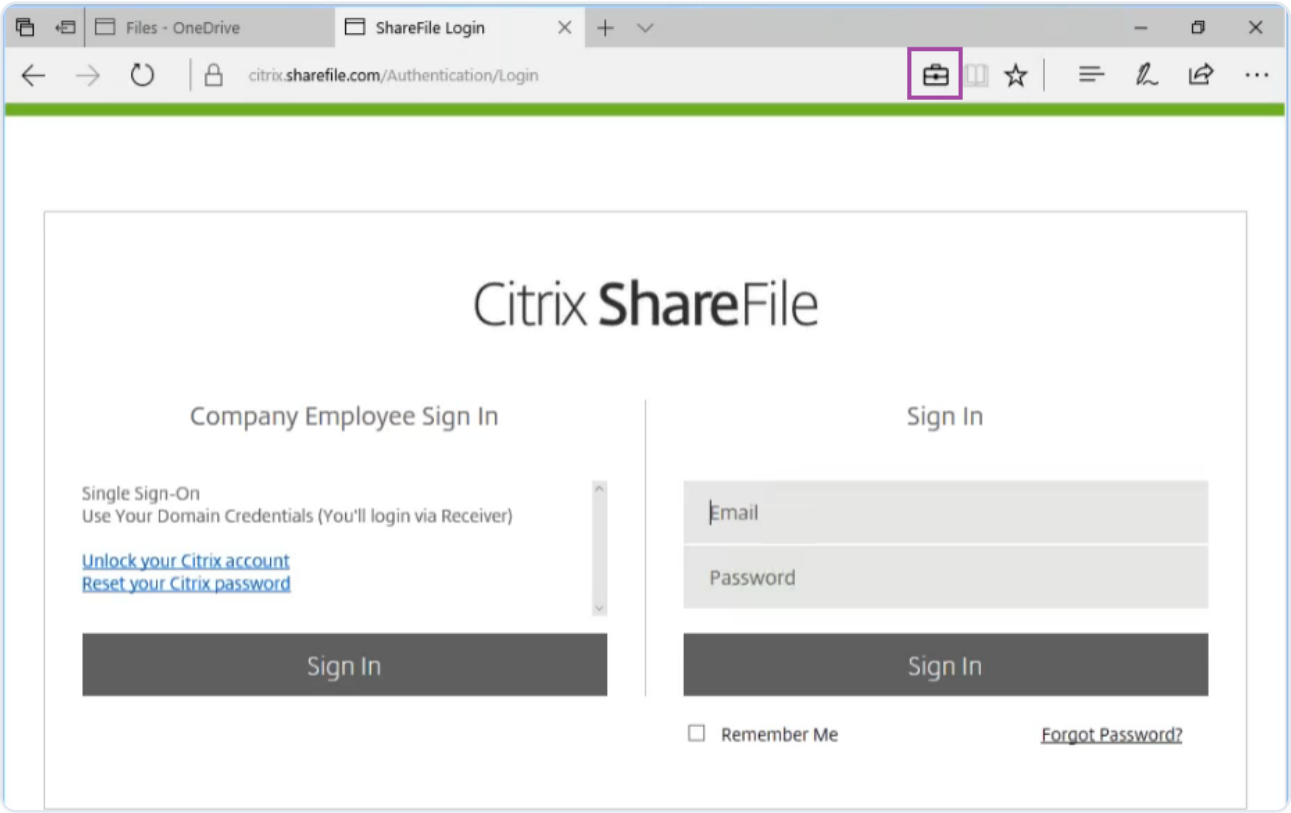
3. 出现提示时，输入密码以保护私钥文件。

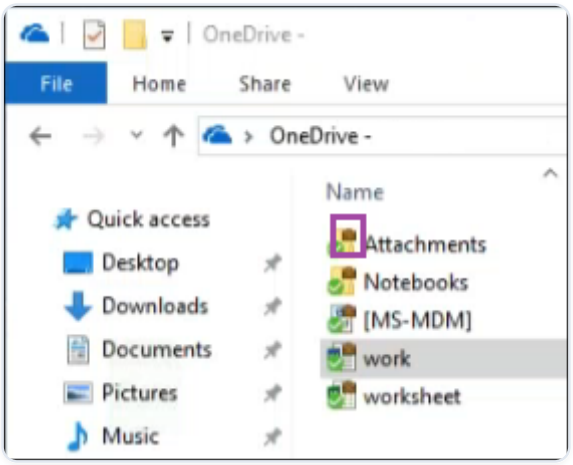
   cipher 命令会创建 .cer 和 .pfx 文件。

4. 在 XenMobile 控制台中，转到“**设置 > 证书**”并导入 .cer 文件，该文件适用于 Windows 10 和 Windows 11 平板电脑。

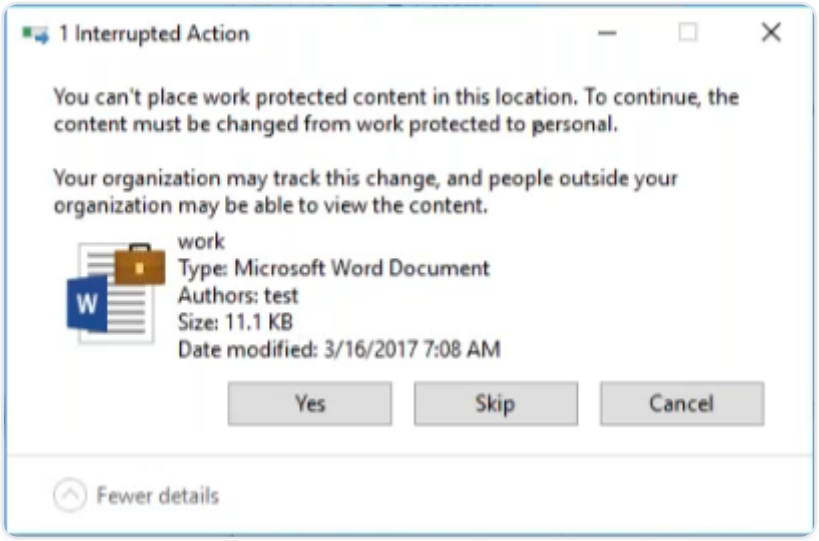
用户体验

当 Windows 信息保护生效时，应用程序和文件会包含一个图标：





如果用户将受保护的文件复制或保存到非受保护的位置，则会出现以下通知，具体取决于配置的强制级别。

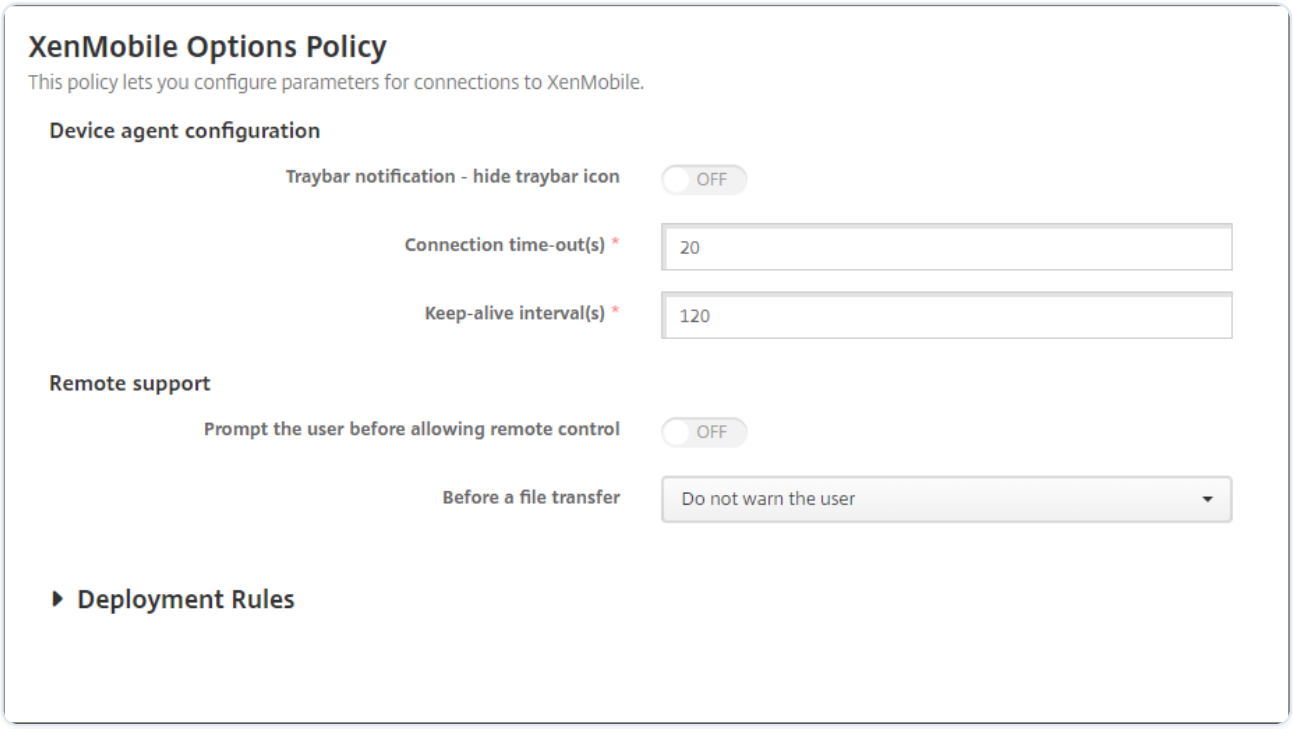


XenMobile® 选项设备策略

您添加 XenMobile 选项策略以配置从 Android 设备连接到 XenMobile 时 Secure Hub 的行为。

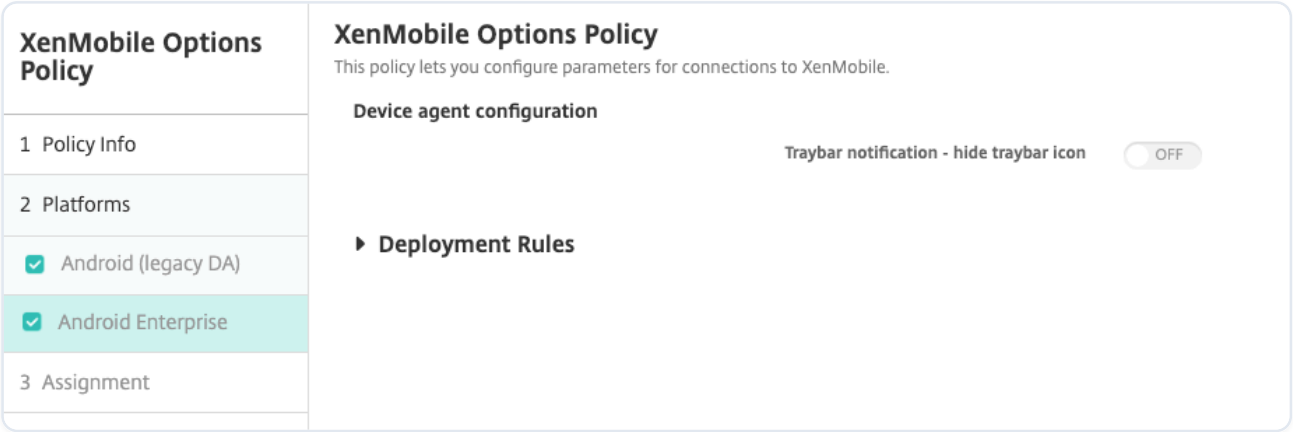
要添加或配置此策略，请转至**配置 > 设备策略**。有关详细信息，请参阅设备策略。

Android 设置



- **托盘栏通知 - 隐藏托盘栏图标：选择托盘栏图标是隐藏还是可见。默认值为关。**
- **连接：超时(秒)：**键入连接在超时前可以保持空闲状态的秒数。默认值为 20 秒。
- **保持活动间隔(秒)：**键入保持连接打开的秒数。默认值为 120 秒。

安卓企业版设置



从 Android 7 版开始支持。

托盘栏通知 - 隐藏托盘栏图标：选择托盘栏图标是隐藏还是可见。默认值为关。

> **注意：**

> 如果您想为运行 Android Enterprise 的设备启用 VPN 服务，则可以在**VPN 设备策略**中启用**启用始终开启的 VPN** 选项。如果您在以前的版本中已在 **XenMobile 选项设备策略**中启用了**启用始终开启的 VPN** 选项，请确保在**VPN 设备策略**中再次启用该选项。有关 VPN 设备策略的详细信息，请参阅VPN 设备策略 - Android Enterprise 设置。

XenMobile® 卸载设备策略

您可以在 XenMobile 中添加设备策略，以从 Android 设备卸载 XenMobile。部署后，此策略会从部署组中的所有设备中删除 XenMobile。

要添加或配置此策略，请转到 **配置 > 设备策略**。有关详细信息，请参阅 设备策略。

配置 Android 设置

- **从设备卸载 XenMobile：** 选择是否从您部署此策略的每台设备中卸载 XenMobile。默认值为 **关**。

添加应用程序

将应用程序添加到 XenMobile® 可提供移动应用程序管理 (MAM) 功能。XenMobile 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。

对应用程序启用 MDX 是为分发到用户设备准备大多数类型应用程序的重要组成部分。有关 MDX 的介绍，请参阅 关于 MDX Toolkit 和 MAM SDK 概述。

- Citrix 建议使用 MAM SDK 对应用程序启用 MDX。或者，您可以继续对应用程序进行 MDX 封装，直到 MDX Toolkit 弃用为止。请参阅 弃用。
- 您不能使用 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）将应用程序分类，以便在 Secure Hub 中进行组织
- （可选）定义工作流，以要求在允许用户访问应用程序之前进行审批
- 向用户部署应用程序

本文介绍了添加应用程序的通用工作流。有关特定于平台的信息，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

下表总结了您可以使用 XenMobile 部署的应用程序类型。

应用类型	来源	备注	请参阅
MDX	您为用户开发的 iOS 和 Android 应用程序。Citrix 移动生产力应用程序。	使用 MAM SDK 开发 iOS 或 Android 应用程序，或使用 MDX Toolkit 封装它们。对于移动生产力应用程序，请从 Citrix 下载	添加 MDX 应用程序

应用类型	来源	备注	请参阅
		中下载公共应用商店 MDX 文件。然后，将应用程序添加到 XenMobile。	
公共应用商店	来自公共应用商店（例如 Google Play 或 Apple App Store）的免费或付费应用程序。	上传应用程序，启用 MDX，然后将应用程序添加到 XenMobile。	添加公共应用商店应用程序
Web 和 SaaS	您的内部网络（Web 应用程序）或公共网络 (SaaS)。	Citrix Workspace™ 为注册了 MDM 的 iOS 和 Android 设备提供对本机 SaaS 应用程序的移动单点登录。或者，使用安全断言标记语言 (SAML) 应用程序连接器	添加 Web 或 SaaS 应用程序
企业	未启用 MDX 的私有应用程序，包括 Win 32 应用程序。已启用 MDX 的私有 Android Enterprise 应用程序。企业应用程序位于内容分发网络位置或 XenMobile 服务器中。	将应用程序添加到 XenMobile。	添加企业应用程序
Web 链接	Internet Web 地址、Intranet Web 地址或不需要单点登录的 Web 应用程序。	在 XenMobile 中配置 Web 链接。	添加 Web 链接

规划应用程序分发时，请考虑以下功能：

- 关于静默安装
- 关于必需和可选应用程序

- 关于应用程序类别
- 启用 Microsoft 365 应用程序
- 应用工作流
- 应用商店和 Citrix Secure Hub™ 品牌(#app-store-and-citrix-secure-hub-branding)

关于静默安装

Citrix 支持 iOS、Android Enterprise 和 Samsung 应用程序的静默安装和升级。静默安装意味着用户不会收到安装部署到设备的应用程序的提示。应用程序会在后台自动安装。

实施静默安装的先决条件：

- 对于 iOS，请将受管 iOS 设备置于受监督模式。有关详细信息，请参阅导入 iOS 和 macOS 配置文件设备策略。
- 对于 Android Enterprise，应用程序会安装在设备上的 Android 工作配置文件中。有关详细信息，请参阅Android Enterprise。
- 对于 Samsung 设备，请在设备上启用 Samsung Knox。

  为此，您需要设置 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

将应用程序添加到交付组时，您可以选择它们是可选的还是必需的。Citrix 建议将应用程序部署为**必需**。

- 必需应用程序会在用户设备上静默安装，从而最大限度地减少交互。启用此功能还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，用户可以在以下情况下及时收到更新：

- 您上传了一个新应用程序并将其标记为必需。
- 您将现有应用程序标记为必需。
- 用户删除一个必需的应用程序。
- Secure Hub 更新可用。

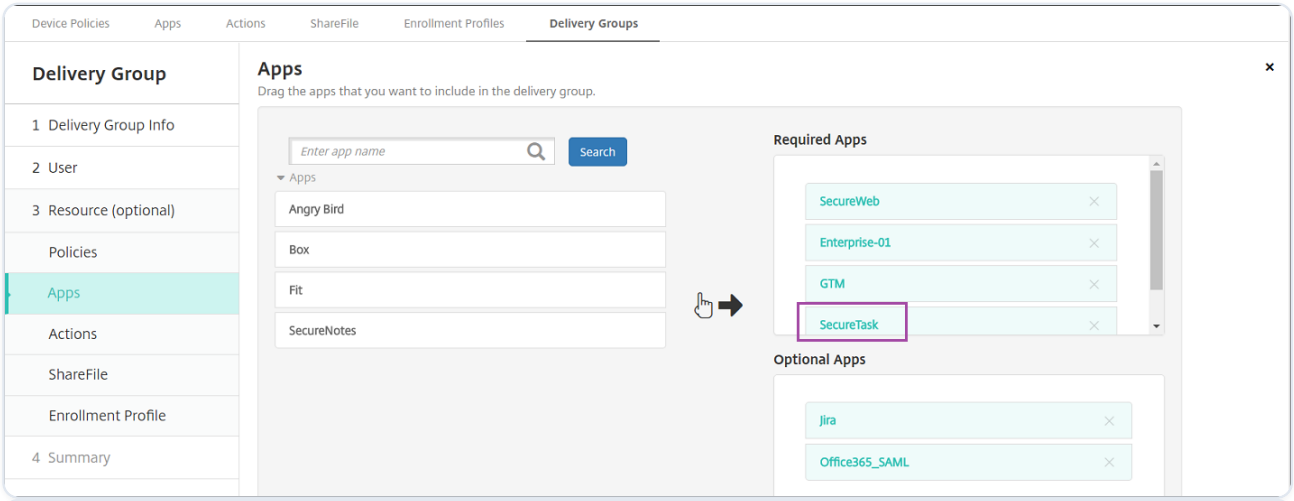
强制部署必需应用程序的要求

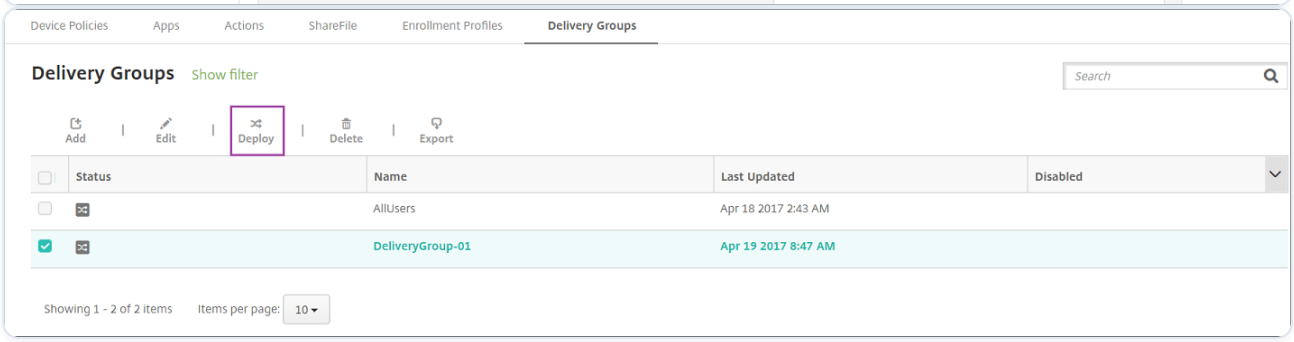
- XenMobile Server 10.6（最低版本）
- 适用于 iOS 的 Secure Hub 10.5.15 和适用于 Android 的 Secure Hub 10.5.20（最低版本）
- MAM SDK 或 MDX Toolkit 10.6（最低版本）
- 自定义服务器属性 force.server.push.required.apps

  必需应用程序的强制部署默认处于禁用状态。要启用此功能，请创建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**，并将**值**设置为 **true**。
- 升级 XenMobile Server 和 Secure Hub 后：已注册设备的用户必须注销 Secure Hub，然后登录一次，才能获取所需的应用程序部署更新。

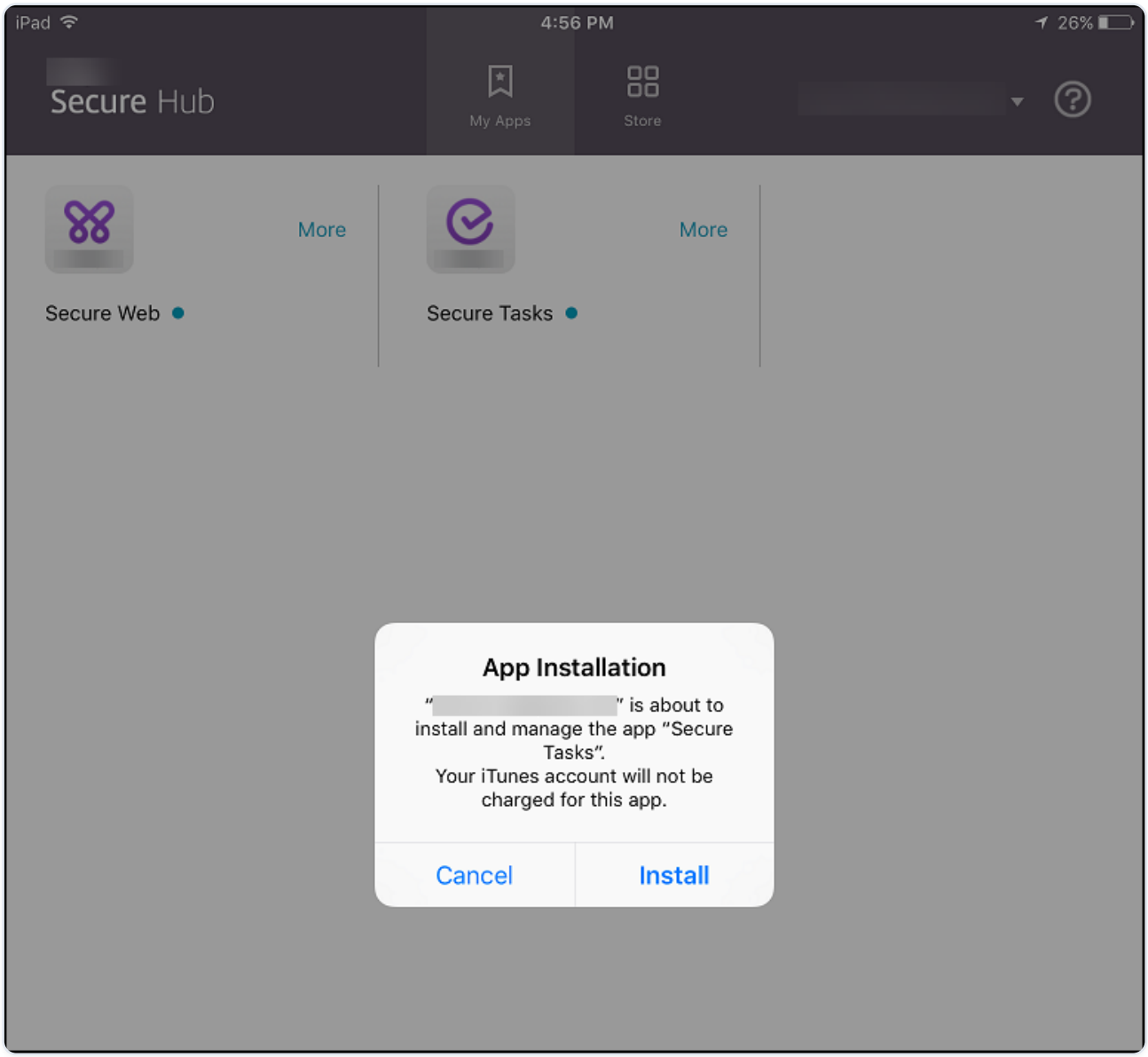
示例

以下示例显示了将名为 Citrix Secure Tasks 的应用程序添加到交付组，然后部署该交付组的顺序。





示例应用程序 Citrix Secure Tasks 部署到用户设备后，Secure Hub 会提示用户安装该应用程序。



Secure Hub 屏幕(/en-us/xenmobile/server/media/secure-hub-app-installed.png)

重要提示：

启用 MDX 的必需应用程序（包括企业应用程序和公共应用商店应用程序）会立即升级。即使您为应用程序更新宽限期配置了 MDX 策略，并且用户选择稍后升级应用程序，也会发生升级。

适用于企业和公共应用商店应用程序的 iOS 必需应用程序工作流

1. 在初始注册期间部署 XenMobile 应用程序。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已更新。对于公共应用商店应用程序，升级会自动开始。不会提示用户更新。
5. 用户从主屏幕打开应用程序。即使您设置了应用程序更新宽限期，并且用户点击稍后升级应用程序，应用程序也会立即升级。

适用于企业应用程序的 Android 必需应用程序工作流

1. 在初始注册期间部署 XenMobile 应用程序。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 设备会提示安装更新，但三星设备会静默安装。）
4. 用户从主屏幕打开应用程序。即使您设置了应用程序更新宽限期，并且用户点击稍后升级应用程序，应用程序也会立即升级。（三星设备会静默安装。）

适用于公共应用商店应用程序的 Android 必需应用程序工作流

1. 在首次注册期间部署 XenMobile 应用程序。所需的应用程序将安装在设备上。
2. 在 XenMobile 控制台上更新应用程序。
3. 使用 XenMobile 控制台部署所需的应用程序。或者，在设备上打开 Secure Hub 商店。更新图标将显示在商店中。
4. 应用程序升级自动开始。（Nexus 设备会提示用户安装更新。）
5. 在主屏幕上打开应用程序。应用程序已升级。系统不会提示用户宽限期。（三星设备会静默安装。）

当应用程序配置为必需时卸载应用程序

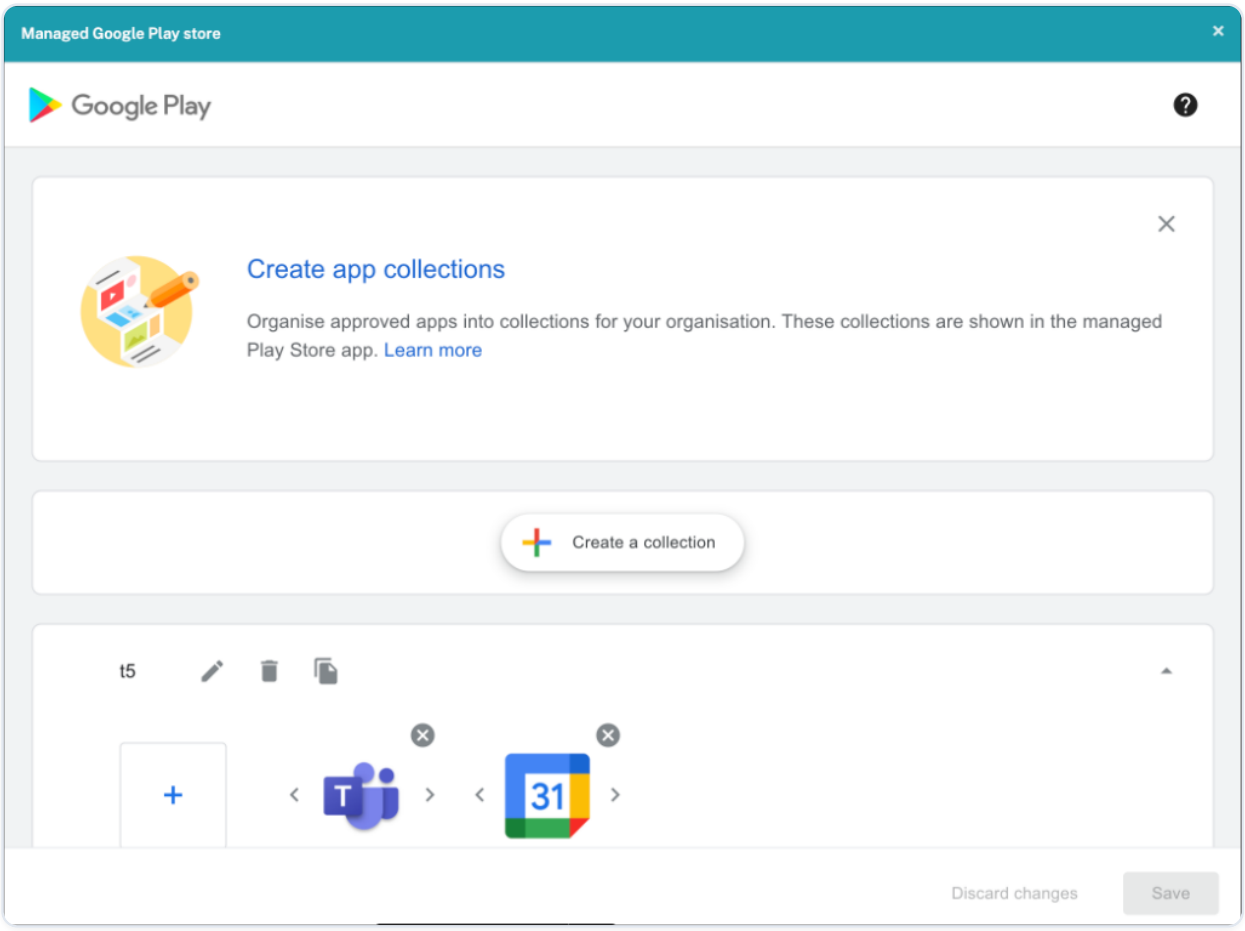
您可以允许用户卸载配置为必需的应用程序。转到 **Configure > Delivery Groups**，然后将应用程序从 **Required Apps** 移动到 **Optional Apps**。

建议： 使用特殊的交付组将应用程序暂时更改为可选，以便特定用户可以卸载该应用程序。然后，您可以将现有必需应用程序更改为可选，将应用程序部署到该交付组，然后从这些设备卸载应用程序。之后，如果您希望该交付组的未来注册需要该应用程序，您可以将应用程序重新设置为必需。

组织应用程序 (Android Enterprise)

当用户登录 Secure Hub 时，他们会收到您在 XenMobile Server 中设置的应用程序、Web 链接和商店列表。在 Android Enterprise 中，您可以将这些应用程序组织到集合中，以允许用户仅访问某些应用程序、商店或 Web 链接。例如，您可以创建一个财务集合，然后将仅与财务相关的应用程序添加到该集合中。或者，您可以配置一个销售集合，并将销售应用程序分配给它。

1. 在 XenMobile Server 控制台上，单击 **Configure > Apps > Organize Apps**。将显示 **Managed Google Play store** 窗口。



2. 单击 **Create** 集合并选择要添加到该集合的应用程序。
3. 完成添加集合后，单击 **Save**。

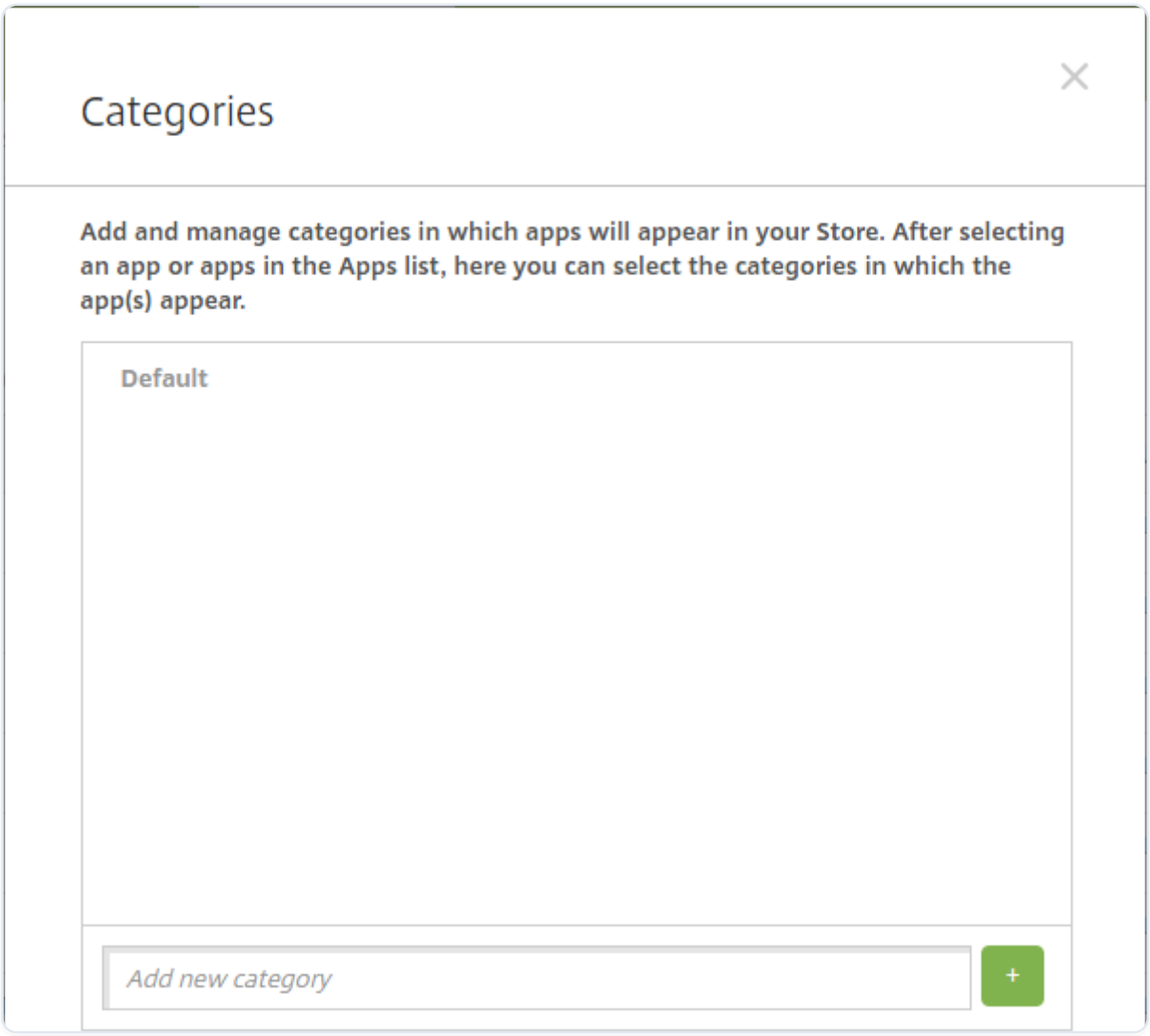
> **注意：**
>
> IT 管理员需要先批准应用，然后才能将其添加到托管 Google Play 窗口上的集合中。IT 管理员可以通过转到 `<https://play.google.com/work>` 批准应用。在未来的版本中，您无需在将应用添加到集合之前批准它。

关于应用类别

当用户登录 Secure Hub 时，他们会收到您在 XenMobile 中设置的应用、Web 链接和商店列表。您可以使用应用类别让用户仅访问某些应用、商店或 Web 链接。例如，您可以创建一个“财务”类别，然后将仅与财务相关的应用添加到该类别中。或者，您可以配置一个“销售”类别，并将销售应用分配给它。

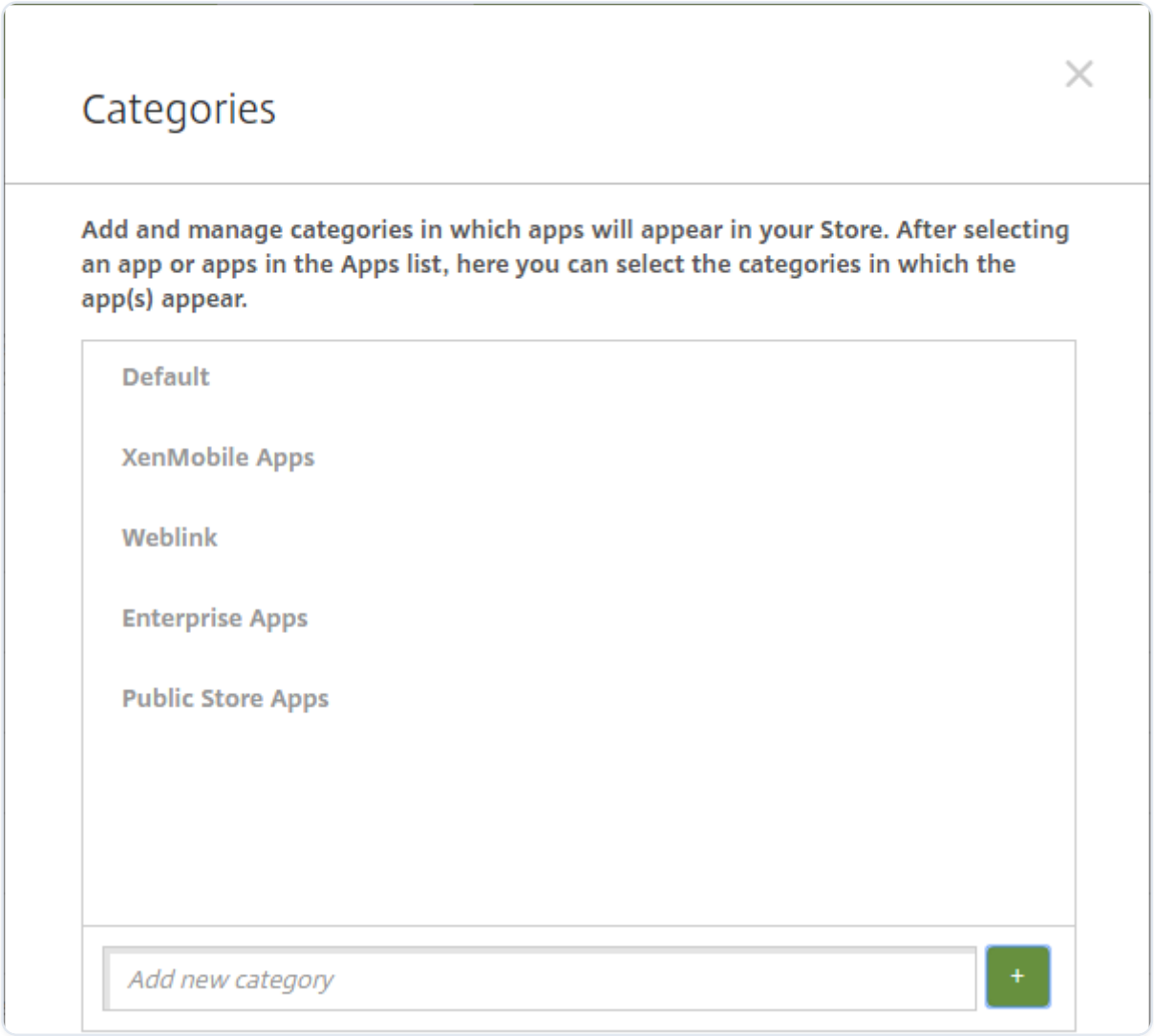
当您添加或编辑应用、Web 链接或商店时，您可以将应用添加到一个或多个已配置的类别中。

1. 在 XenMobile 控制台中，单击 **Configure > Apps > Category**。此时将显示**类别**对话框。



2. 对于要添加的每个类别，请执行以下操作：

   - 在对话框底部的**添加新类别**字段中键入要添加的类别名称。例如，您可以键入“企业应用”以创建企业应用类别。
   - 单击加号 (+) 以添加类别。新创建的类别随即添加并显示在**类别**对话框中。



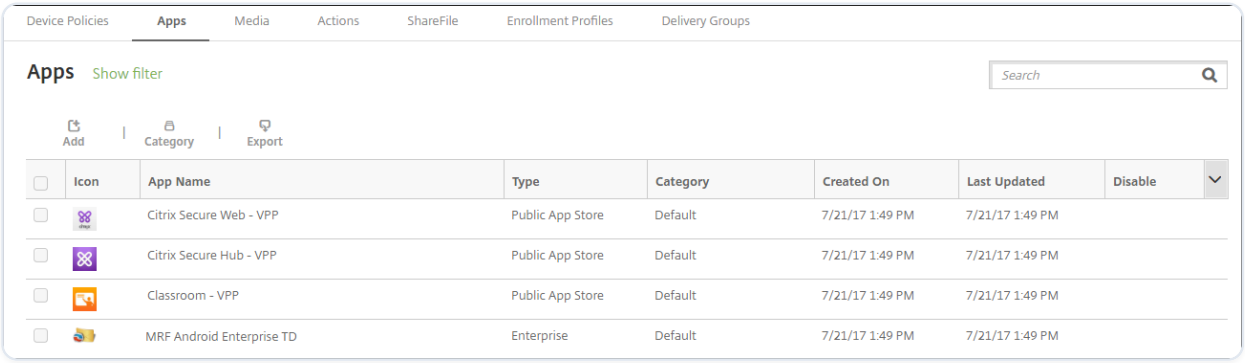
3. 添加完类别后，关闭**类别**对话框。
4. 在**应用**页面上，您可以将现有应用放入新类别中。
   - 选择要分类的应用。
   - 单击**编辑**。此时将显示**应用信息**页面。
   - 在**应用类别**列表中，通过选择类别复选框来应用新类别。清除不希望应用于应用的任何现有类别的复选框。
   - 点击**交付组分配**选项卡，或在以下每个页面上点击**下一步**，以逐步完成剩余的应用程序设置页面。
   - 在**交付组分配**页面上点击**保存**以应用新类别。新类别将应用于应用程序并显示在**应用程序**表中。

添加 MDX 应用程序

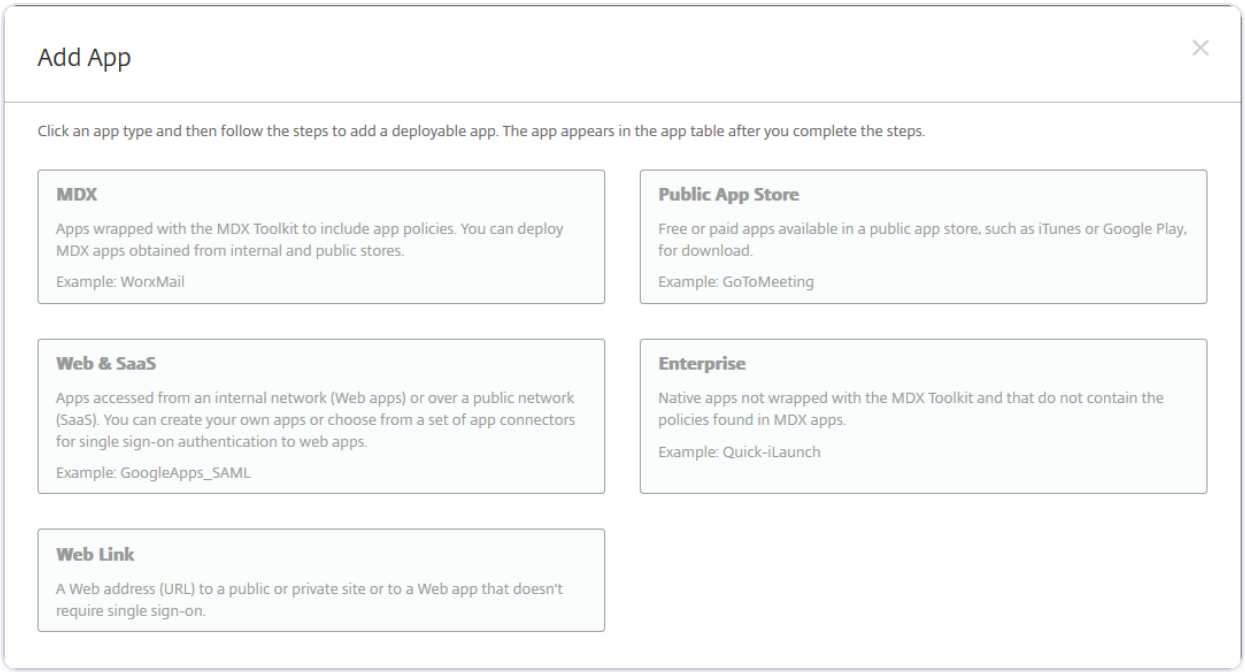
当您收到适用于 iOS 或 Android 应用程序的 MDX 文件时，您可以将该应用程序上传到 XenMobile。上传应用程序后，您可以配置应用程序详细信息和策略设置。有关适用于每种设备平台类型的应用程序策略的更多信息，请参阅：

- MAM SDK 概述
- MDX 策略一览

1. 在 XenMobile 控制台中，点击**配置 > 应用程序**。**应用程序**页面随即显示。



2. 点击**添加**。**添加应用程序**对话框随即显示。



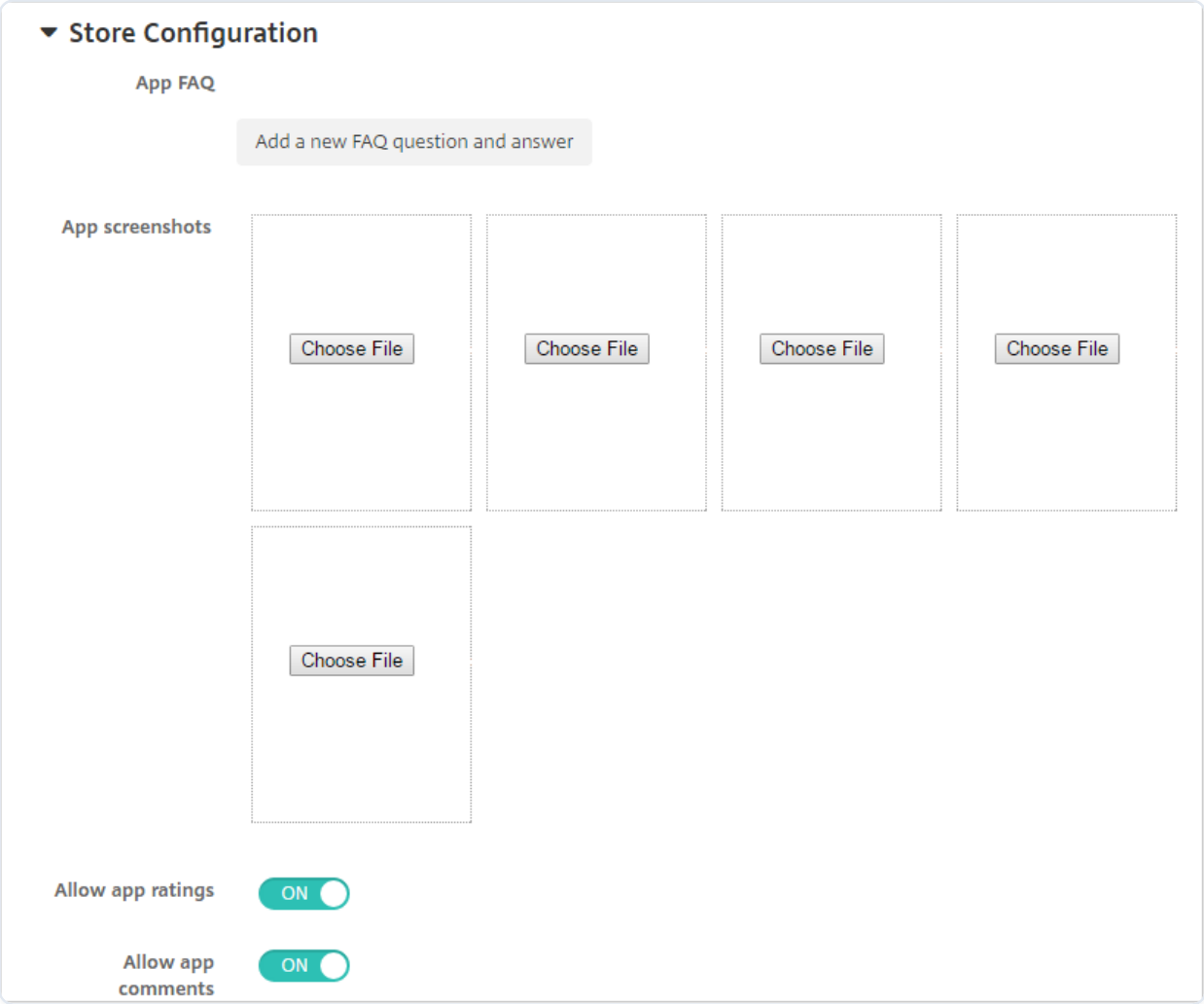
3. 点击 **MDX**。**MDX 应用程序信息**页面随即显示。
4. 在**应用程序信息**窗格中，键入以下信息：
   - **名称：键入应用程序的描述性名称。该名称将显示在应用程序**表中的**应用程序名称**下。
   - **说明：**键入应用程序的可选说明。

- **应用程序类别：**（可选）在列表中，点击要添加应用程序的类别。有关应用程序类别的更多信息，请参阅关于应用程序类别。

5. 单击**下一步**。**应用程序平台**页面随即出现。
6. 在**平台**下，选择要添加的平台。如果只为一个平台进行配置，请清除其他平台。
7. 要选择要上载的 MDX 文件，请单击**上载**并导航到文件位置。
8. 在**应用程序详细信息**页面中，配置以下设置：

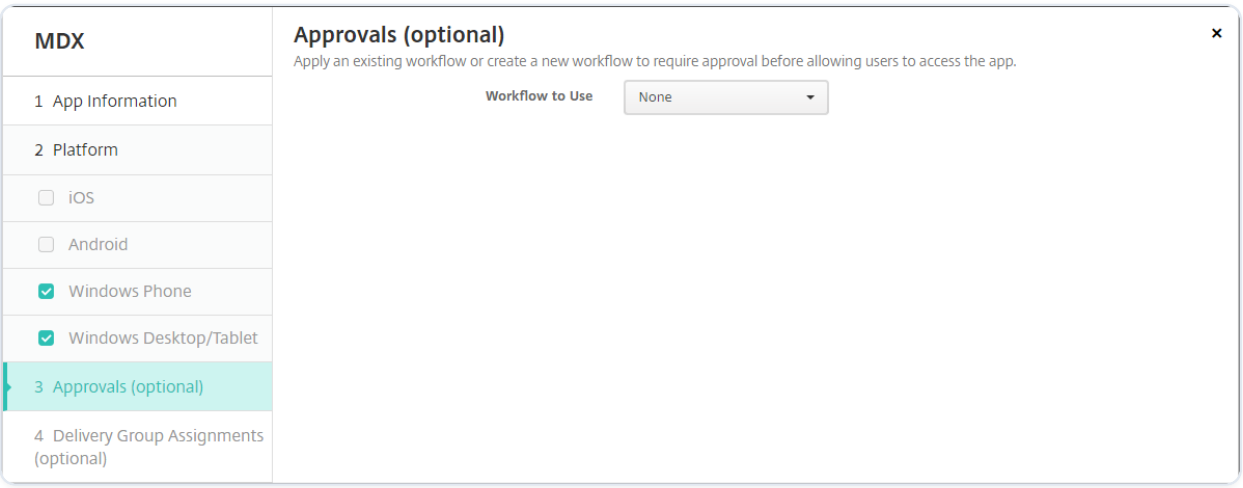
- **文件名：**键入与应用程序关联的文件名。
- **应用程序描述：**键入应用程序的描述。
- **应用程序版本：**（可选）键入应用程序版本号。
- **程序包 ID：**键入应用程序的程序包 ID，该 ID 从托管的 Google Play 商店获取。
- **最低操作系统版本：**（可选）键入设备可运行的、用于使用此应用程序的最旧操作系统版本。
- **最高操作系统版本：**（可选）键入设备必须运行的、用于使用此应用程序的最新操作系统版本。
- **排除的设备：**（可选）键入无法运行此应用程序的设备的制造商或型号。
- **如果 MDM 配置文件已删除，则删除应用程序：选择当 MDM 配置文件从 iOS 设备中删除时是否删除应用程序。默认值为开。**
- **阻止应用程序数据备份：选择是否阻止用户在 iOS 设备上备份应用程序数据。默认值为开。**
- **产品跟踪：指定要推送到 iOS 设备的产品跟踪。如果您有专为测试设计的跟踪，则可以将其选中并分配给用户。默认值为生产。**
- **强制应用程序受管理：对于作为非托管应用程序安装的应用程序，选择是否提示用户允许在非受监管的 iOS 设备上管理该应用程序。默认值为开。**
- **通过批量采购部署的应用：** 选择是否使用 Apple 批量采购部署应用。如果为 **开**，并且您部署了 MDX 版本的应用并使用批量采购部署该应用，Secure Hub 将仅显示批量采购实例。默认值为 **关**。

9. 配置 **MDX 策略**。MDX 策略因平台而异，包括身份验证、设备安全和应用限制等策略区域的选项。在控制台中，每个策略都有一个描述该策略的工具提示。
10. 配置部署规则。有关信息，请参阅部署规则。
11. 展开 **商店配置**。



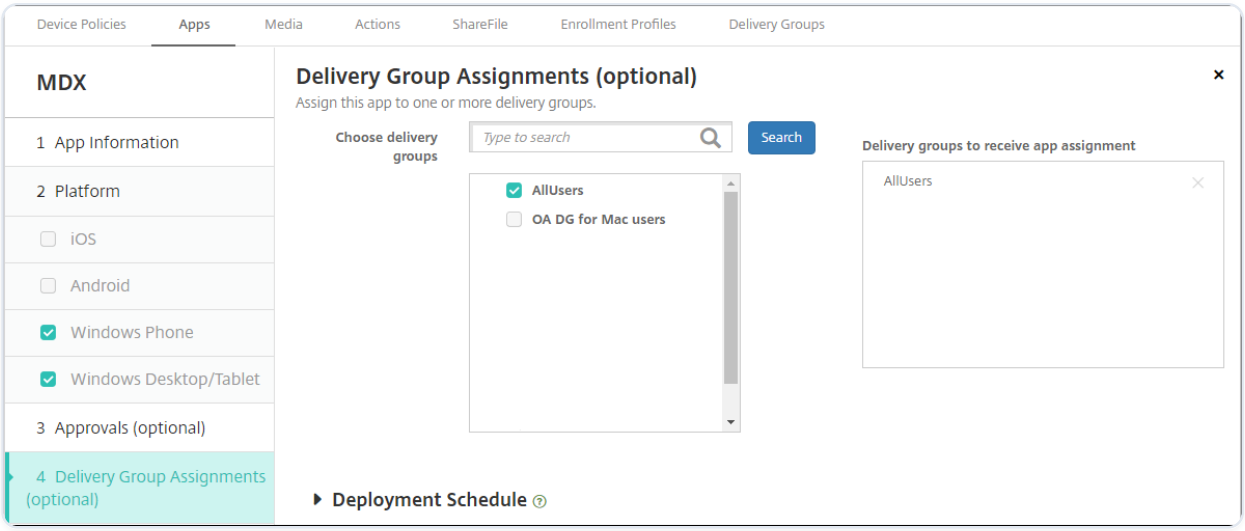
- **应用常见问题解答：** 单击 **添加新的常见问题解答** 为应用创建常见问题解答。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用评分：** 允许用户在应用商店中对应用进行评分。
- **允许应用评论：** 允许用户在应用商店中对应用发表评论。

12. 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之前要求审批，请参阅应用工作流。如果您不想设置审批工作流，请继续执行下一步。

13. 单击 **下一步**。此时将显示 **交付组分配** 页面。



14. 在 **选择交付组** 旁边，键入以查找交付组或在列表中选择一个或多个组。您选择的组将显示在 **接收应用分配的交付组** 列表中。

15. 展开 **部署计划**，然后配置以下设置：

    - **部署：** 选择是否将应用部署到设备。默认值为 **开**。
    - **部署计划：** 选择是 **立即** 还是 **稍后** 部署应用。如果选择 **稍后**，请配置部署应用的日期和时间。默认值为 **立即**。
    - **部署条件：** 选择 **每次连接时** 以在设备每次连接时部署应用。选择 **仅当上次部署失败时** 以在设备之前未能接收应用时部署应用。默认值为 **每次连接时**。

    当您在 **设置 > 服务器属性** 中配置了计划后台部署密钥时，**部署用于始终在线连接** 选项适用。

    您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但 **部署用于始终在线连接** 除外。

16. 单击 **保存**。

添加公共应用商店应用

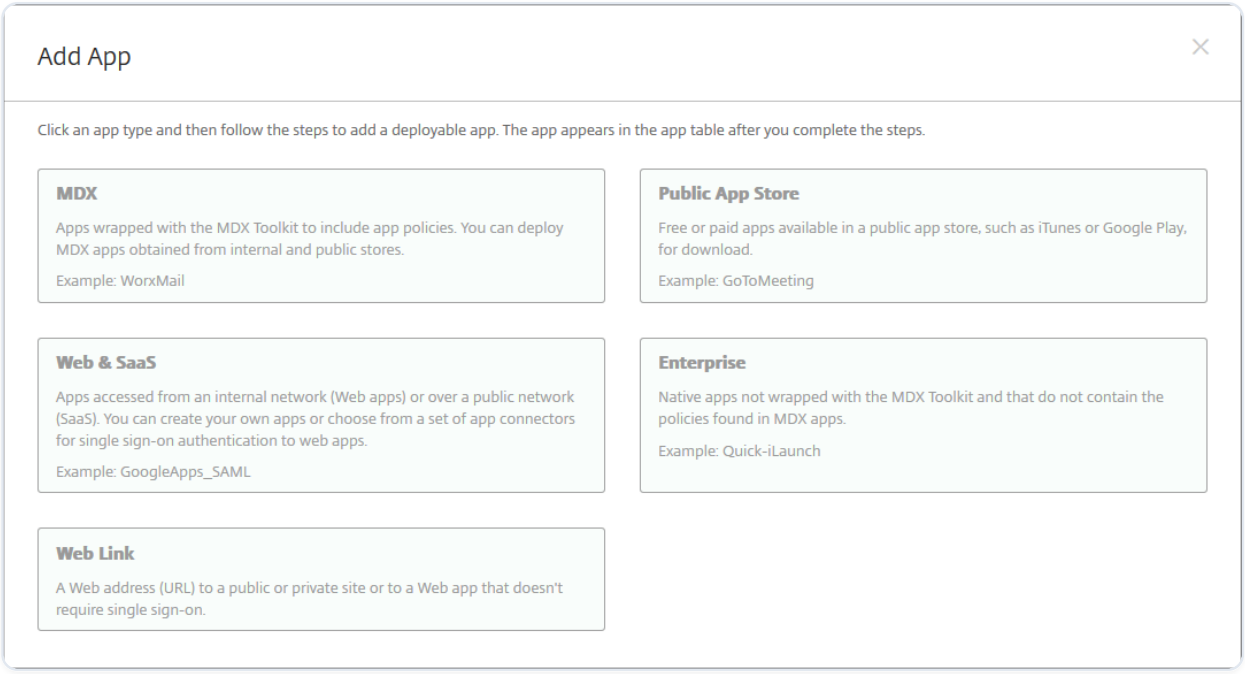
您可以将公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用添加到 XenMobile。

您可以配置设置以从 Apple App Store 检索应用名称和说明。当您从商店检索应用信息时，XenMobile 会覆盖现有的名称和说明。请手动配置 Google Play 商店应用信息。

当您为 Android Enterprise 添加付费公共应用商店应用时，可以查看批量购买许可状态。该状态包括可用许可证总数、当前正在使用的数量以及每个使用许可证的用户的电子邮件地址。Android Enterprise 的批量购买计划简化了为组织批量查找、购买和分发应用及其他数据的过程。

配置应用信息并选择要向其交付应用的平台：

1. 在 XenMobile 控制台中，单击 **配置 > 应用 > 添加**。“**添加应用**”对话框随即显示。



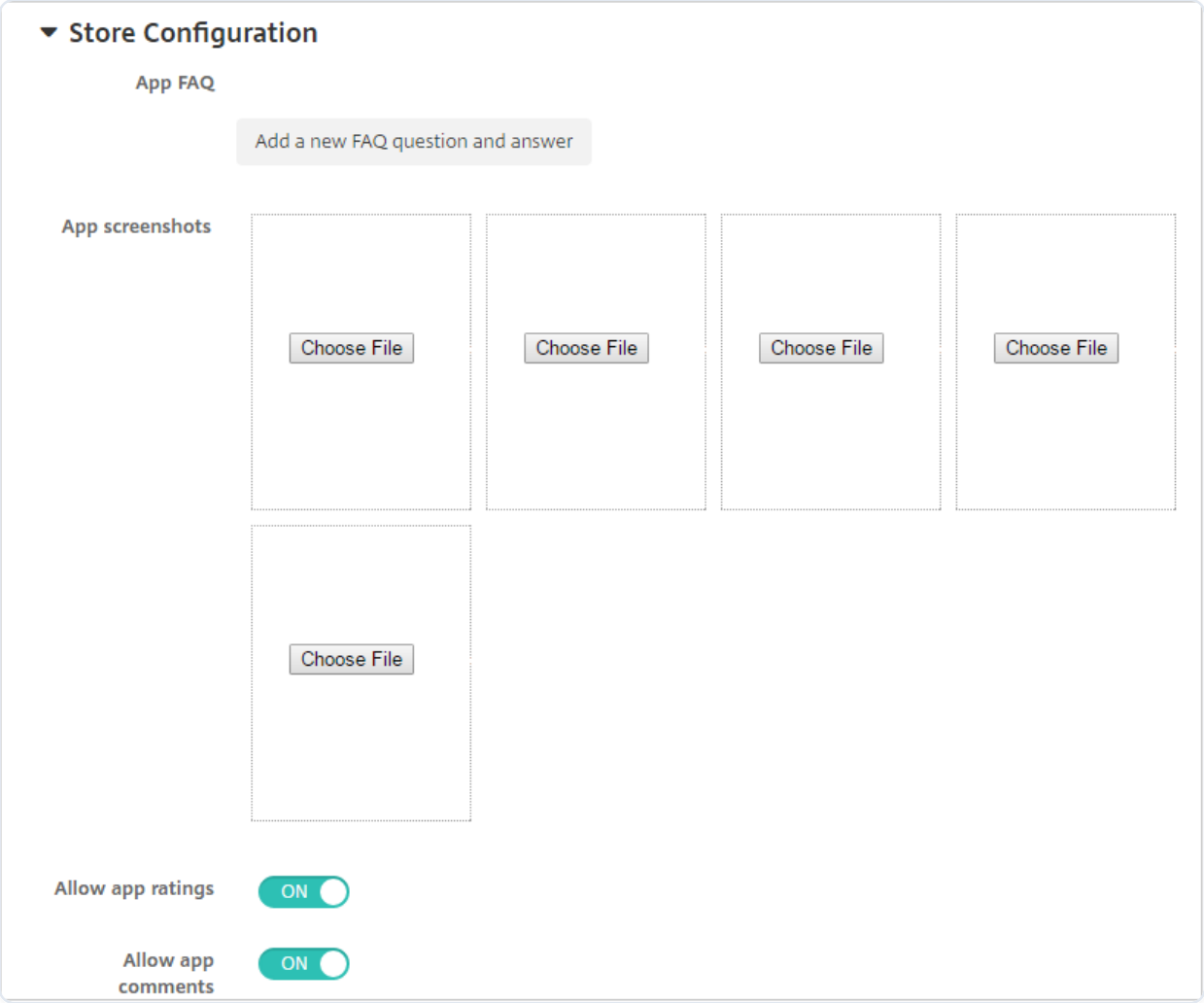
2. 单击 **公共应用商店**。“**应用信息**”页面随即显示。
3. 在“**应用信息**”窗格中，键入以下信息：
   - **名称：**键入应用的描述性名称。此名称显示在“**应用**”表中的“**应用名称**”下。
   - **说明：**键入应用的可选说明。
   - **应用类别：**（可选）在列表中，单击要添加应用的类别。有关应用类别的详细信息，请参阅关于应用类别。
4. 单击“**下一步**”。此时将显示“**应用平台**”页面。
5. 在“**平台**”下，选择要添加的平台。如果仅为一个平台进行配置，请清除其他平台。

接下来，为每个平台配置应用设置。请参阅：

- 配置 Google Play 应用的应用设置
- 托管应用商店应用
- 配置 iOS 应用的应用设置

完成平台设置配置后，设置平台部署规则和应用商店配置。

1. 配置部署规则。有关信息，请参阅部署规则。
2. 展开“**商店配置**”。



- **应用常见问题解答：**单击“**添加新的常见问题解答**”为应用创建常见问题解答。
- **添加手机/平板电脑屏幕截图：**添加显示在应用商店中的屏幕截图。
- **允许应用评分：**允许用户在应用商店中对应用进行评分。
- **允许应用评论：**允许用户在应用商店中对应用发表评论。

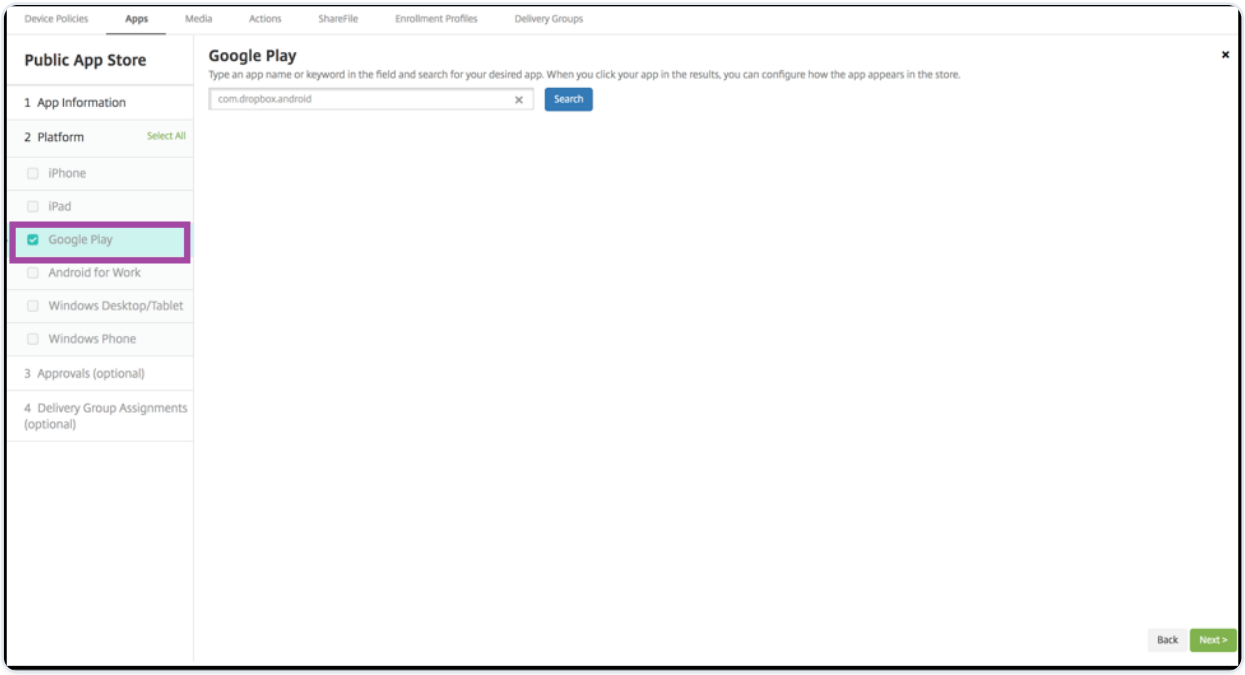
配置 Google Play 应用的应用设置

> **注意：**

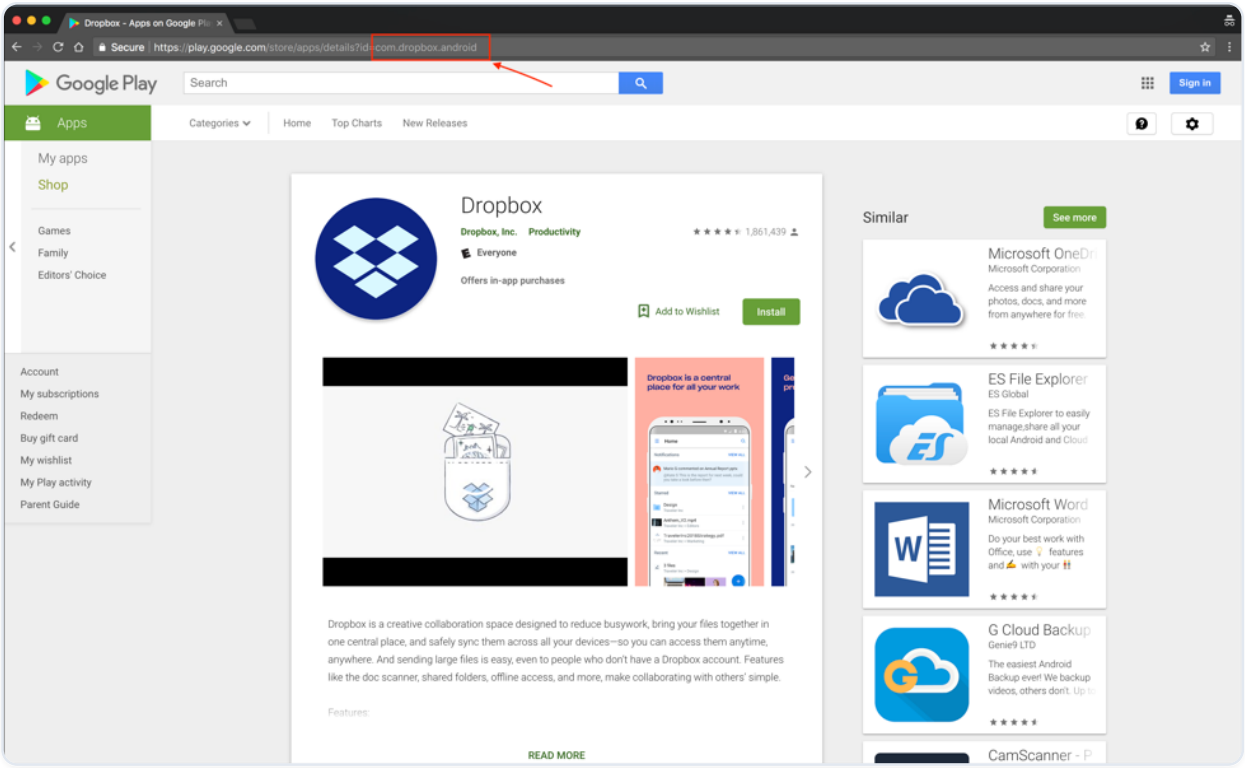
> 要使 Google Play 商店中的所有应用都可以从托管 Google Play 访问，请使用 XenMobile Server 属性 **Access all apps in the managed Google Play store**。请参阅 服务器属性。将此属性设置为 **true** 允许所有 Android Enterprise 用户使用公共 Google Play 商店应用。然后，您可以使用 限制设备策略 来控制对这些应用的访问。

> 配置 Google Play 商店应用设置所需的步骤与配置其他平台的应用不同。您必须手动配置 Google Play 商店应用信息。

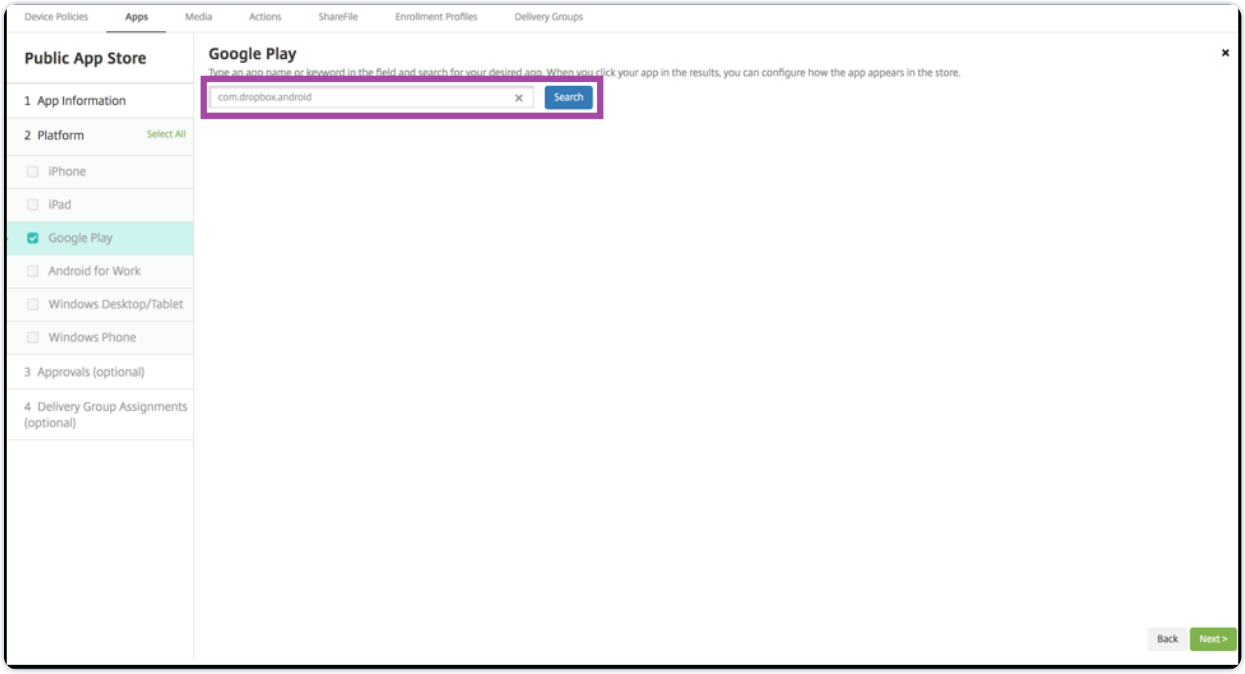
1. 确保在**平台**下选中 **Google Play**。



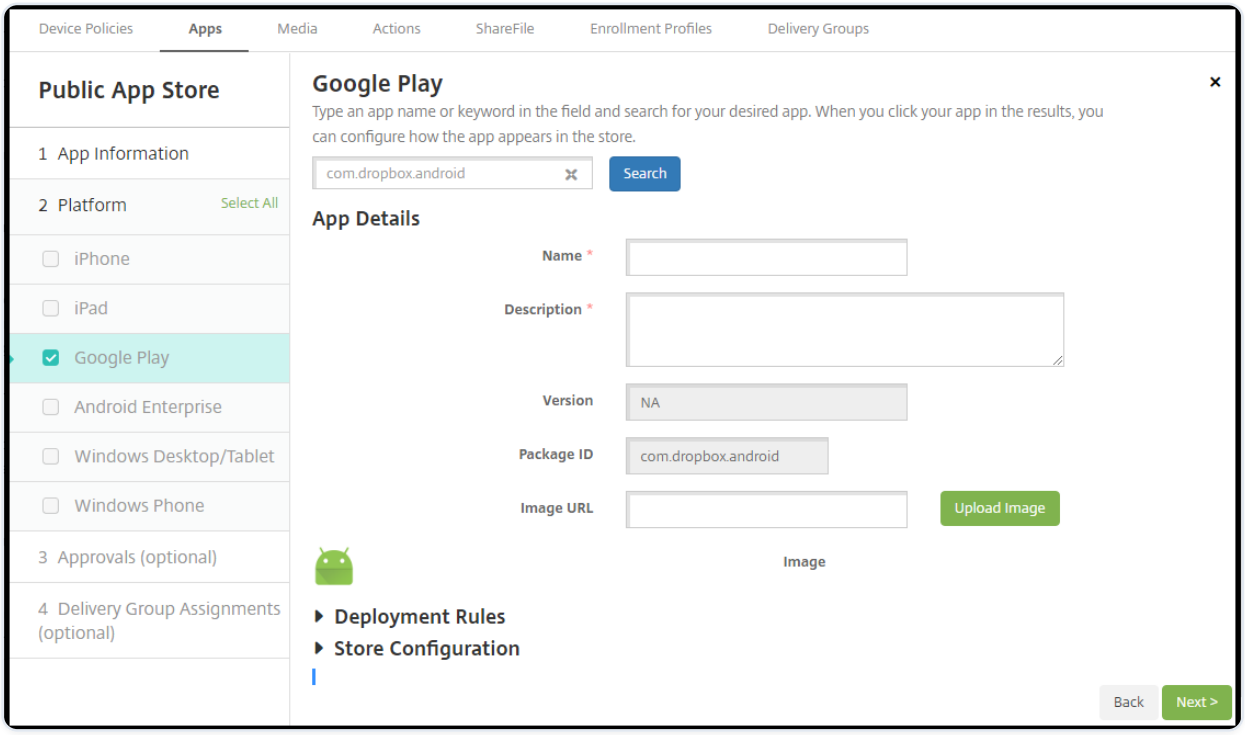
2. 转到 Google Play 商店。从 Google Play 商店复制程序包 ID。该 ID 可以在应用的 URL 中找到。



3. 在 XenMobile Server 控制台中添加公共商店应用时，将程序包 ID 粘贴到搜索栏中。单击**搜索**。



4. 如果程序包 ID 有效，将出现一个 UI，允许您输入应用详细信息。



5. 您可以配置图像的 URL，使其与应用一起显示在商店中。要使用 Google Play 商店中的图像：

   a. 转到 Google Play 商店。右键单击应用图像并复制图像地址。

   b. 将图像地址粘贴到“**图像 URL**”字段中。

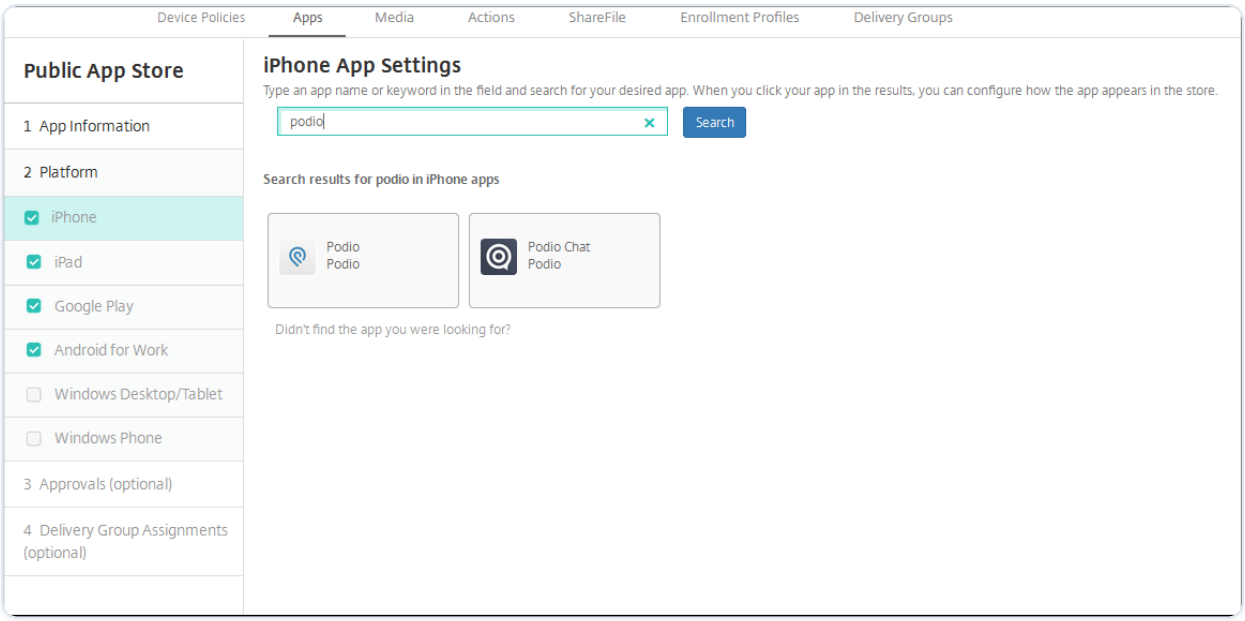
   c. 单击“**上传图像**”。图像将显示在“**图像**”旁边。

如果您未配置图像，则通用 Android 图像将与应用一起显示。

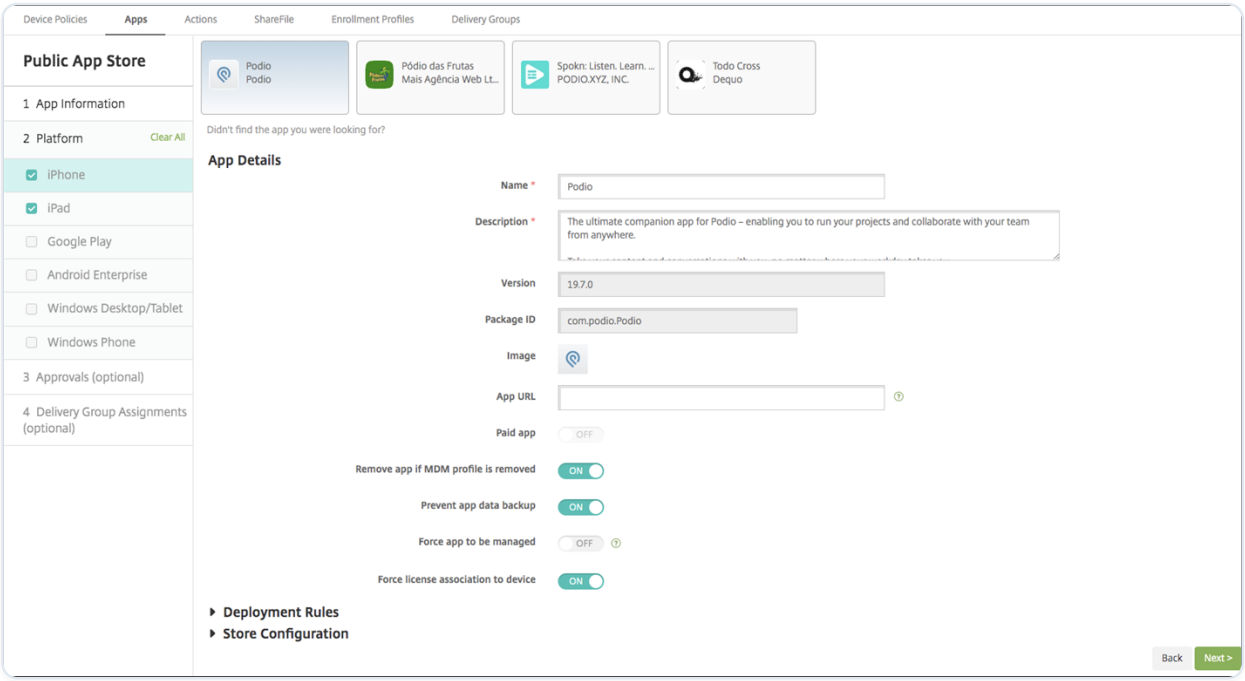
配置 iOS 应用的应用设置

1. 在搜索框中键入应用名称，然后单击“**搜索**”。将显示与搜索条件匹配的应用。将显示与搜索条件匹配的应用。

   下图显示了在 iPhone 应用中搜索 **podio** 的结果。



2. 单击要添加的应用。
3. “**应用详细信息**”字段将预填充所选应用的相关信息（包括名称、说明、版本号和关联图像）。

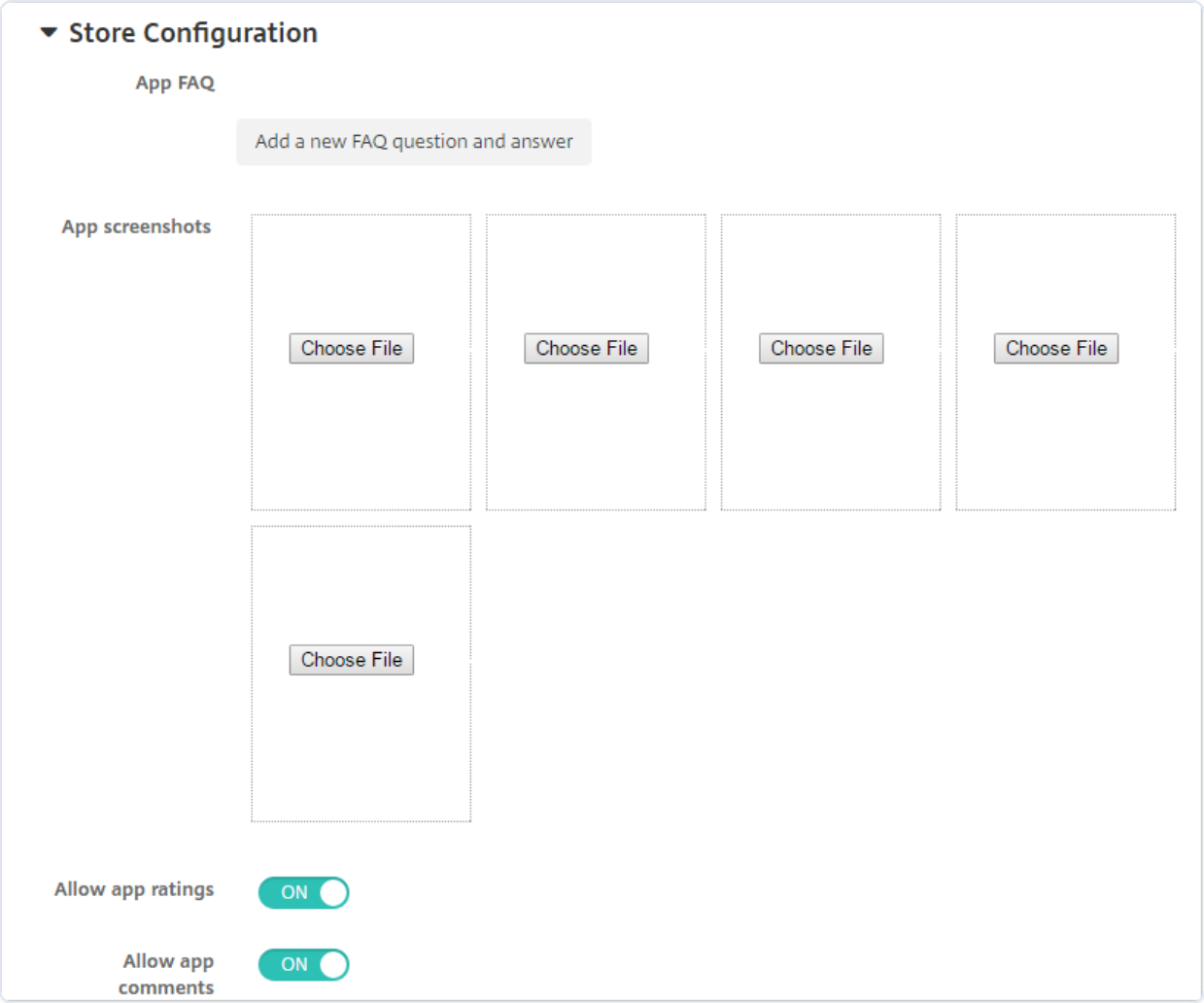


4. 配置设置：

   - 如有必要，更改应用的名称和说明。
   - “**付费应用**”：此字段已预配置，无法更改。

- **如果 MDM 配置文件被移除，则移除应用程序：** 选择是否在 MDM 配置文件被移除时移除应用程序。默认值为 **ON**。
- **阻止应用程序数据备份：** 选择是否阻止应用程序备份数据。默认值为 **ON**。
- **产品跟踪：** 指定要推送到用户设备的产品跟踪。如果您有专为测试设计的跟踪，则可以选择并将其分配给您的用户。默认值为 **Production**。
- **强制应用程序受管理：** 选择当应用程序以非受管理方式安装时，是否提示用户允许在非受监管设备上管理该应用程序。默认值为 **OFF**。适用于 iOS 9.0 及更高版本。
- **强制许可证与设备关联：** 选择是否将已启用设备关联开发的应用程序关联到设备而不是用户。适用于 iOS 9 及更高版本。如果您选择的应用程序不支持分配给设备，则此字段无法更改。

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：** 单击 **添加新的常见问题和答案** 为应用程序创建常见问题。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。

- **允许应用程序评分：** 允许用户在应用商店中对应用程序进行评分。
- **允许应用程序评论：** 允许用户在应用商店中对应用程序发表评论。

7. 对于 iPhone 或 iPad，展开 **批量购买**。

   a. 要使 XenMobile 能够为应用程序应用批量购买许可证：在 **批量购买许可证** 列表中，单击 **上传批量购买许可证**。

   b. 在出现的对话框中，导入许可证。

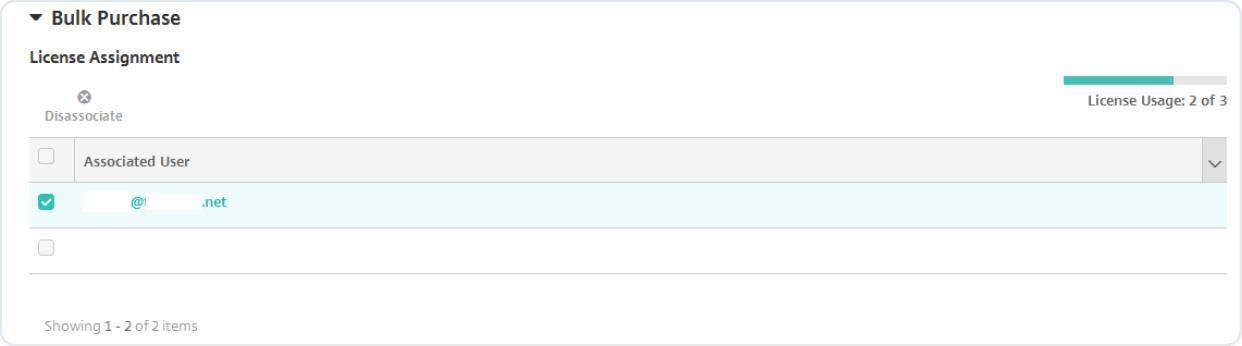
      许可证分配表显示了该应用已使用的许可证数量，以及可用的许可证总数。

      您可以取消关联单个用户的批量购买许可证。这样做会终止许可证分配并释放许可证。

8. 对于 Android Enterprise，展开**批量购买**部分。

   许可证分配表显示了该应用已使用的许可证数量，以及可用的许可证总数。

   您可以选择一个用户，然后单击**取消关联**以终止其许可证分配并为其他用户释放许可证。但是，如果用户不属于包含特定应用的交付组，则只能取消关联该许可证。



9. 完成**批量购买**或**批量采购**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之前要求审批，请参阅应用工作流。如果您不需要审批工作流，请继续执行下一步。

10. 单击**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在列表中选择一个或多个组。您选择的组将显示在**接收应用分配的交付组**列表中。

12. 展开**部署计划**，然后配置以下设置：

    - **部署：选择是否将应用部署到设备。默认值为开。**
    - **部署计划：选择是立即**部署应用还是**稍后**部署。如果选择**稍后**，请配置部署应用的日期和时间。默认值为**立即**。

- **部署条件：选择每次连接时**以在设备每次连接时部署应用。选择**仅当以前的部署失败时**以在设备之前未能接收应用时部署应用。默认值为**每次连接时**。

当您在**设置 > 服务器属性**中配置了计划后台部署密钥时，**为始终在线连接部署**适用。

您配置的部署计划适用于所有平台。您所做的任何更改都将应用于所有平台，但 **Deploy for always-on connection** 除外。

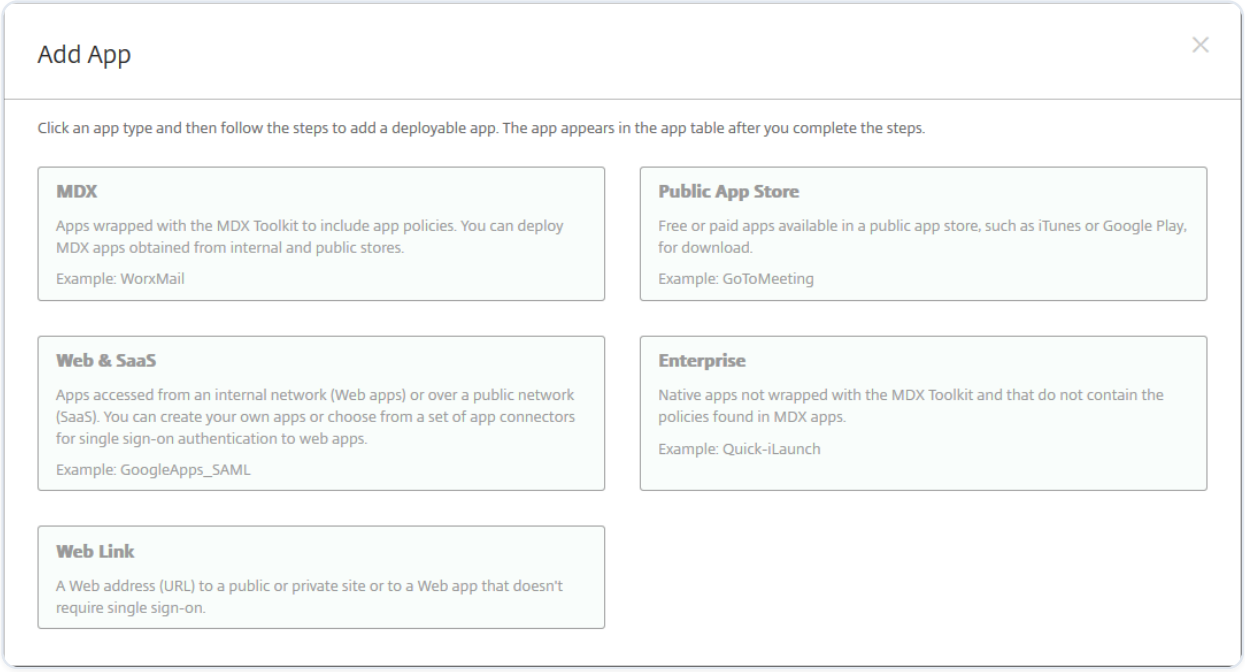
13. 单击 **保存**。

添加 Web 或 SaaS 应用程序

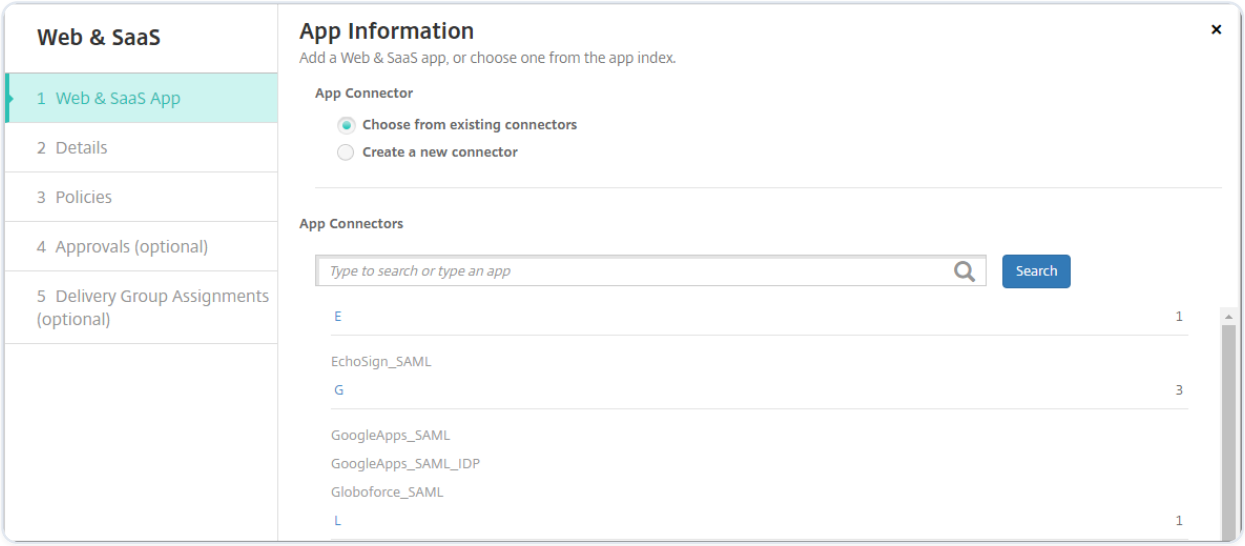
使用 XenMobile 控制台，您可以为用户提供对移动、企业、Web 和 SaaS 应用程序的单点登录 (SSO) 授权。您可以使用应用程序连接器模板为应用程序启用 SSO。有关 XenMobile 中可用的连接器类型列表，请参阅 应用程序连接器类型。在 XenMobile 中添加 Web 或 SaaS 应用程序时，您还可以构建自己的连接器。

如果应用程序仅适用于 SSO：保存设置后，该应用程序将显示在 XenMobile 控制台的 **应用程序** 选项卡上。

1. 在 XenMobile 控制台中，单击 **配置 > 应用程序 > 添加**。将显示 **添加应用程序** 对话框。



2. 单击 **Web 和 SaaS**。将显示 **应用程序信息** 页面。



3. 按如下所示配置现有或新的应用程序连接器。

配置现有应用程序连接器

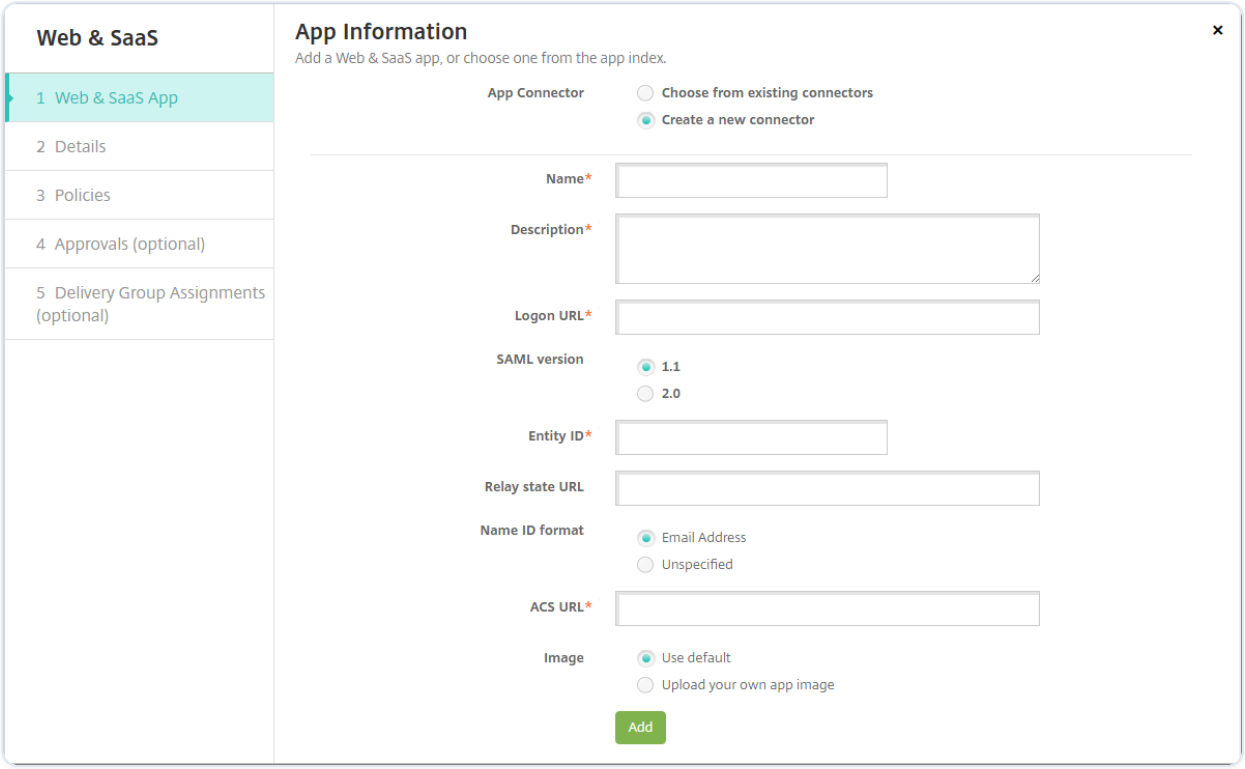
1. 在 **应用程序信息** 页面上，**从现有连接器中选择** 已被选中，如前所示。在 **应用程序连接器** 列表中单击要使用的连接器。将显示应用程序连接器信息。
2. 配置以下设置：
   - **应用程序名称：** 接受预填充的名称或键入新名称。
   - **应用程序描述：** 接受预填充的描述或键入您自己的描述。
   - **URL：** 接受预填充的 URL 或键入应用程序的网址。根据您选择的连接器，此字段可能包含一个占位符，您必须先替换它才能转到下一页。
   - **域名：** 如果适用，键入应用程序的域名。此字段为必填项。
   - **应用程序托管在内部网络中：** 选择应用程序是否在您的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，他们必须通过 Citrix Gateway 连接。将此选项设置为 **ON** 会将 VPN 关键字添加到应用程序，并允许用户通过 Citrix Gateway 连接。默认值为 **OFF**。
   - **应用程序类别：** 在列表中，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。如果您使用 Globoforce_SAML 连接器，则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。此字段为必填项。
       - **密码：** 键入应用程序管理员密码。此字段为必填项。

- **用户帐户**
  - **用户授权结束时：** 在列表中，单击当用户不再被允许访问应用程序时要执行的操作。默认值为 **Disable account**。
- **用户名规则**
  - 对于要添加的每个用户名规则，请执行以下操作：
    - **用户属性：** 在列表中，单击要添加到规则的用户属性。
    - **长度（字符）：** 在列表中，单击要用于用户名规则的用户属性中的字符数。默认值为 **All**。
    - **规则：** 您添加的每个用户属性都会自动附加到用户名规则中。

- **密码要求**
  - **长度：** 键入最小用户密码长度。默认值为 **8**。
- **密码过期**
  - **有效期（天）：** 键入密码的有效天数。有效值为 **0–90**。默认值为 90。
  - **密码过期后自动重置：** 选择是否在密码过期时自动重置密码。默认值为 **OFF**。如果未启用此字段，则用户在密码过期后无法打开应用程序。

配置新的应用程序连接器

1. 在**应用程序信息**页面上，选择**创建新连接器**。应用程序连接器字段随即显示。

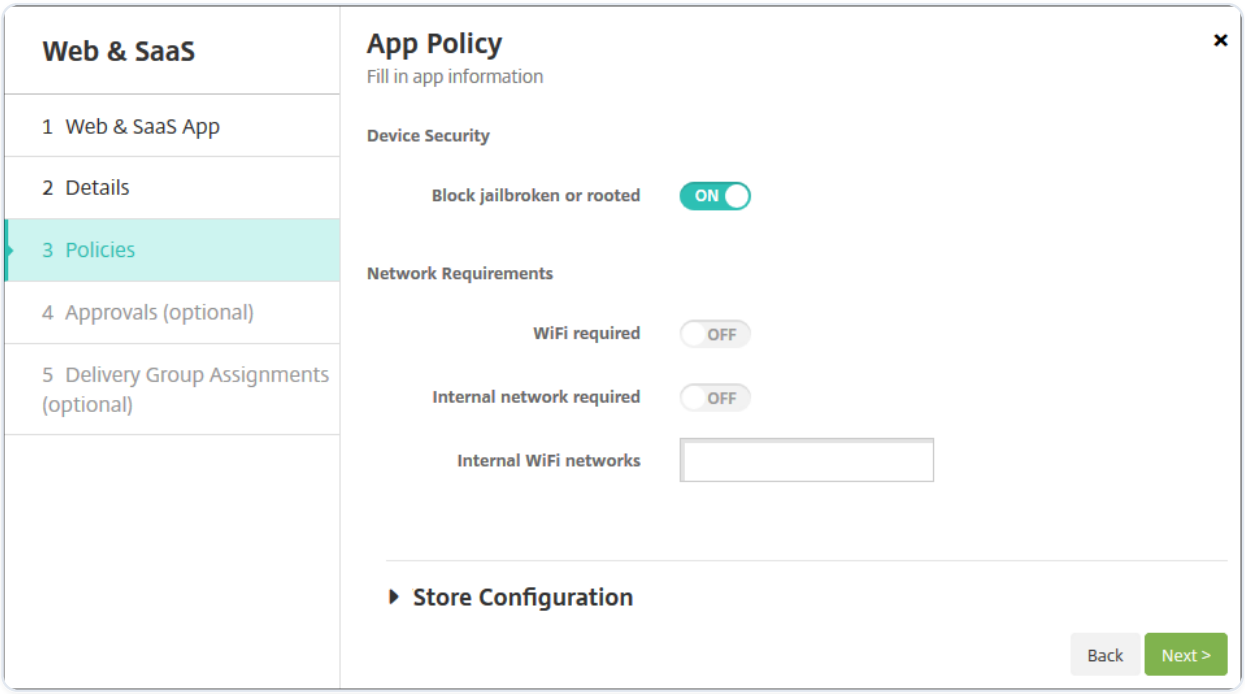


2. 配置以下设置：

- **名称：** 键入连接器的名称。此字段为必填项。
- **描述：** 键入连接器的描述。此字段为必填项。
- **登录 URL：** 键入或复制并粘贴用户登录站点的 URL。例如，如果您要添加的应用程序具有登录页面，请打开 Web 浏览器并转到该应用程序的登录页面。例如，它可能是 `https://www.example.com/logon`。此字段为必填项。
- **SAML 版本：** 选择 **1.1** 或 **2.0**。默认值为 **1.1**。
- **实体 ID：** 键入 SAML 应用程序的标识。
- **中继状态 URL：** 键入 SAML 应用程序的网址。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程序的断言消费者服务 URL。ACS URL 为用户提供 SSO 功能。
- **图像：** 选择是使用默认 Citrix 图像还是上传您自己的应用程序图像。默认值为“使用默认值”。
    - 要上传您自己的图像，请单击“**浏览**”并导航到文件位置。文件必须是 .PNG 文件。您不能上传 JPEG 或 GIF 文件。添加自定义图形后，以后无法更改。

3. 完成后，单击“**添加**”。此时将显示“**详细信息**”页面。

4. 单击“**下一步**”。此时将显示“**应用程序策略**”页面。

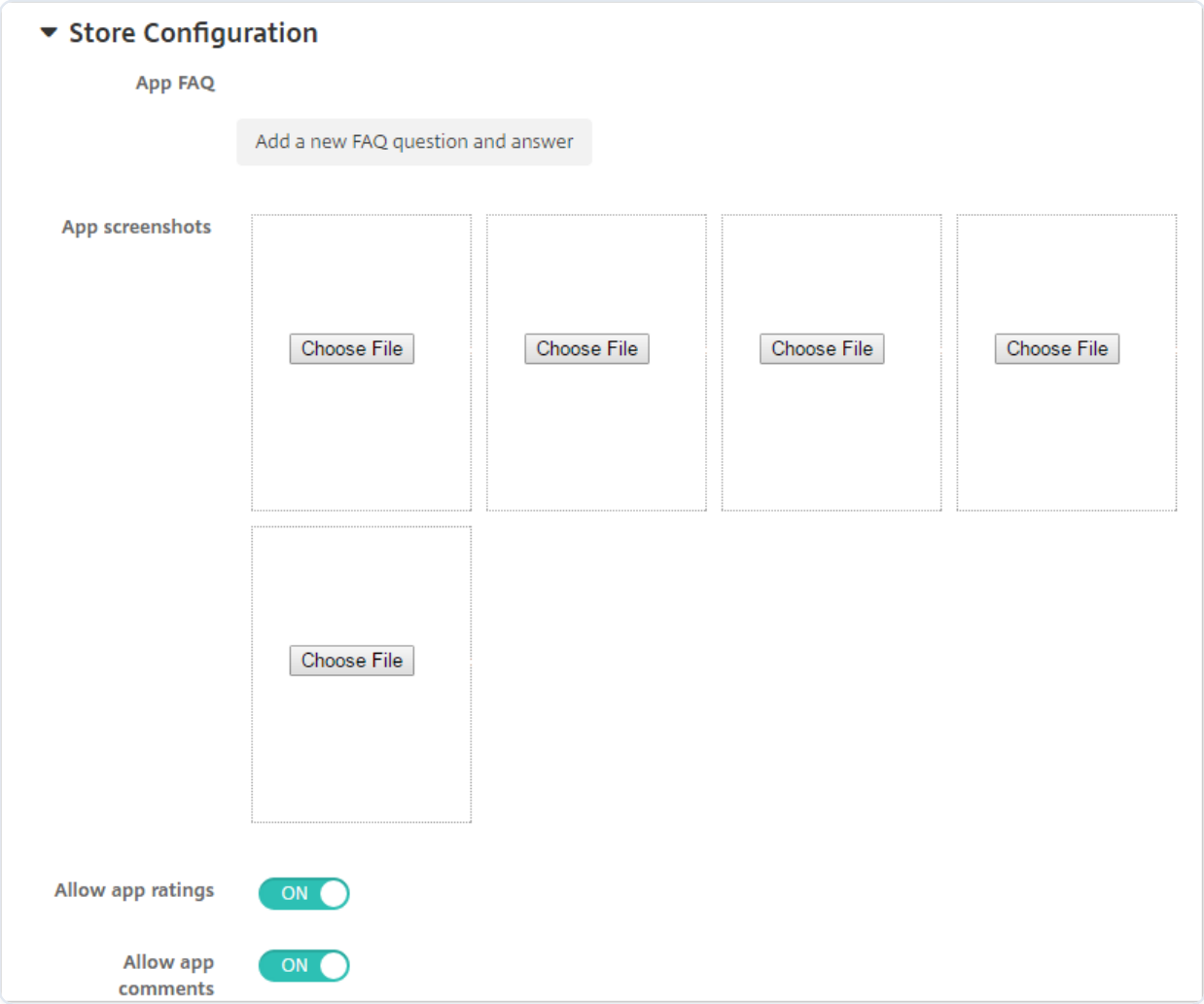


5. 配置以下设置：

   - **设备安全性**
   - **阻止越狱或已获得 root 权限的设备：** 选择是否阻止越狱或已获得 root 权限的设备访问应用程序。默认值为“**开**”。
   - **网络要求**
   - **需要 WiFi：** 选择运行应用程序是否需要 Wi-Fi 连接。默认值为“**关**”。
   - **需要内部网络：** 选择运行应用程序是否需要内部网络。默认值为“**关**”。
   - **内部 WiFi 网络：** 如果启用了“**需要 Wi-Fi**”，请键入要使用的内部 Wi-Fi 网络。

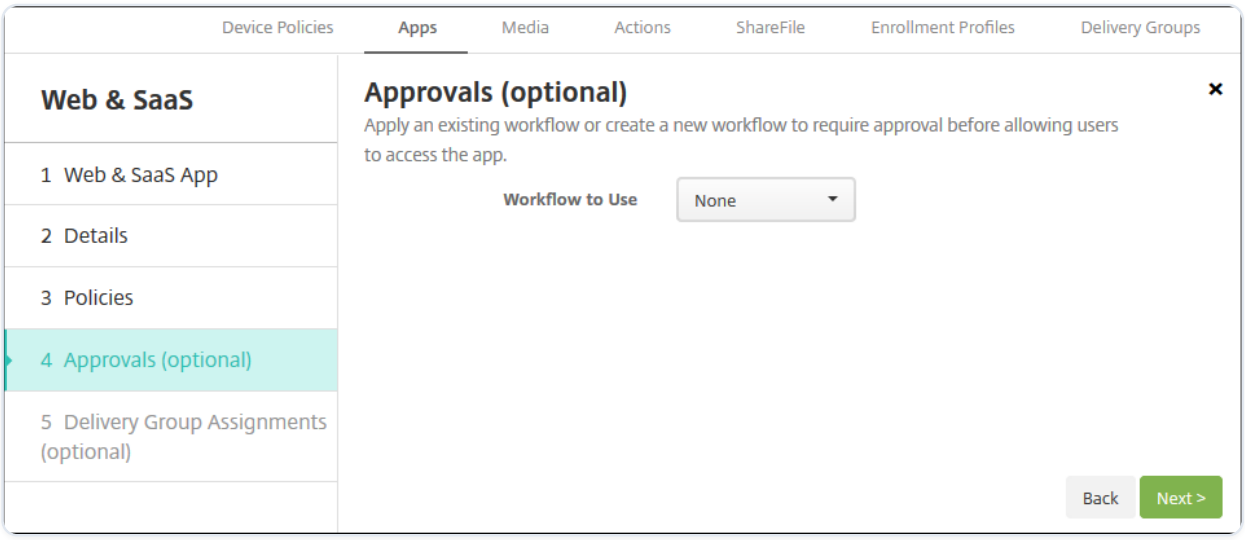
6. 配置部署规则。有关信息，请参阅部署规则。

7. 展开**应用商店配置**。



- **应用程序常见问题解答：** 单击**添加新的常见问题解答**为应用程序创建常见问题解答。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用程序评分：** 允许用户在应用商店中对应用程序进行评分。
- **允许应用程序评论：** 允许用户在应用商店中对应用程序发表评论。

8. 单击**下一步**。将显示**审批**页面。



要使用工作流在允许用户访问应用程序之前要求审批，请参阅应用工作流。

9. 单击**下一步**。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选择一个或多个组。您选择的组将显示在**接收应用程序分配的交付组**列表中。
11. 展开**部署计划**，然后配置以下设置：

    - **部署：** 选择是否将应用程序部署到设备。默认值为**开**。
    - **部署计划：** 选择是**立即**部署应用程序还是**稍后**部署。如果选择**稍后**，请配置部署应用程序的日期和时间。默认值为**立即**。
    - **部署条件：** 选择“**每次连接时**”可在设备每次连接时部署应用。选择“**仅当上次部署失败时**”可在设备之前未能接收应用时部署应用。默认值为“**每次连接时**”。

    当您在“**设置 > 服务器属性**”中配置了计划后台部署密钥时，“**部署用于始终在线连接**”适用。

    您配置的部署计划适用于所有平台。您所做的任何更改都适用于所有平台，但“**部署用于始终在线连接**”除外。
12. 单击“**保存**”。

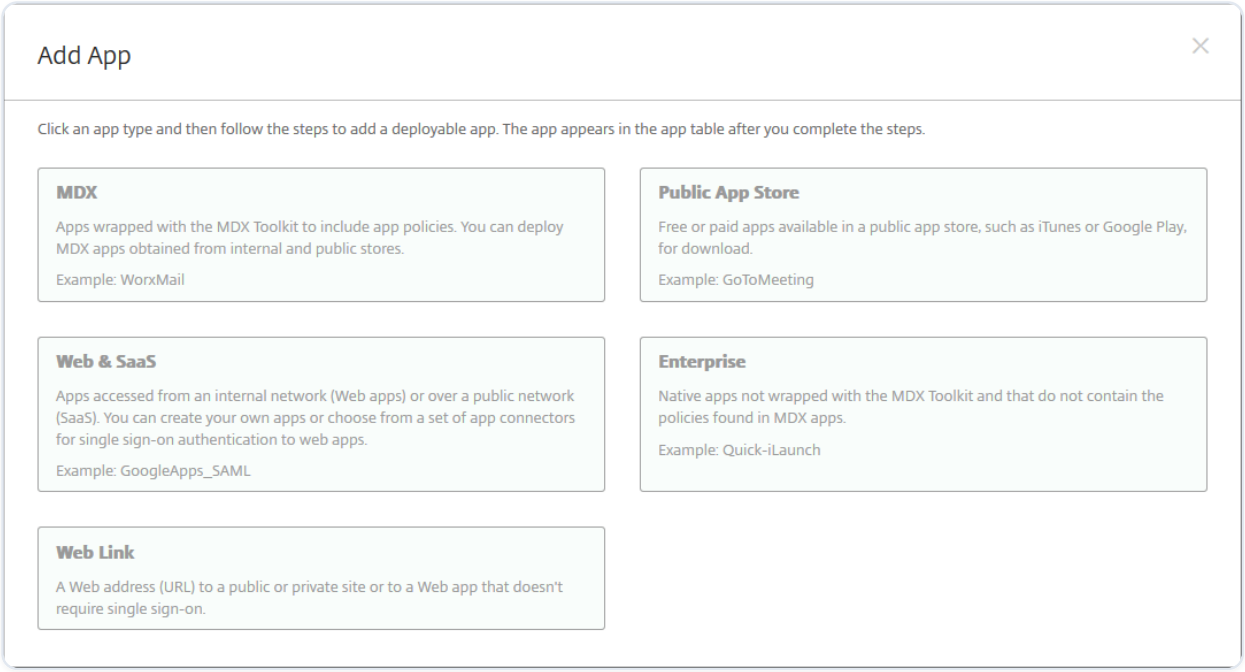
添加企业应用

XenMobile 中的企业应用表示未使用 MAM SDK 或 MDX Toolkit 进行准备的本机应用。这些应用不包含与 MDX 应用关联的策略。您可以在 XenMobile 控制台的“**应用**”选项卡上上传企业应用。企业应用支持以下平台（和相应的文件类型）：

- iOS（.ipa 文件）
- Android（.apk 文件）
- 三星 Knox（.apk 文件）
- 安卓企业版（.apk 文件）
- 另请参阅：启用 MDX 的私有应用

不支持将从 Google Play 商店下载的应用添加为企业应用。请改为将 Google Play 商店中的应用添加为公共应用商店应用。请参阅添加公共应用商店应用。

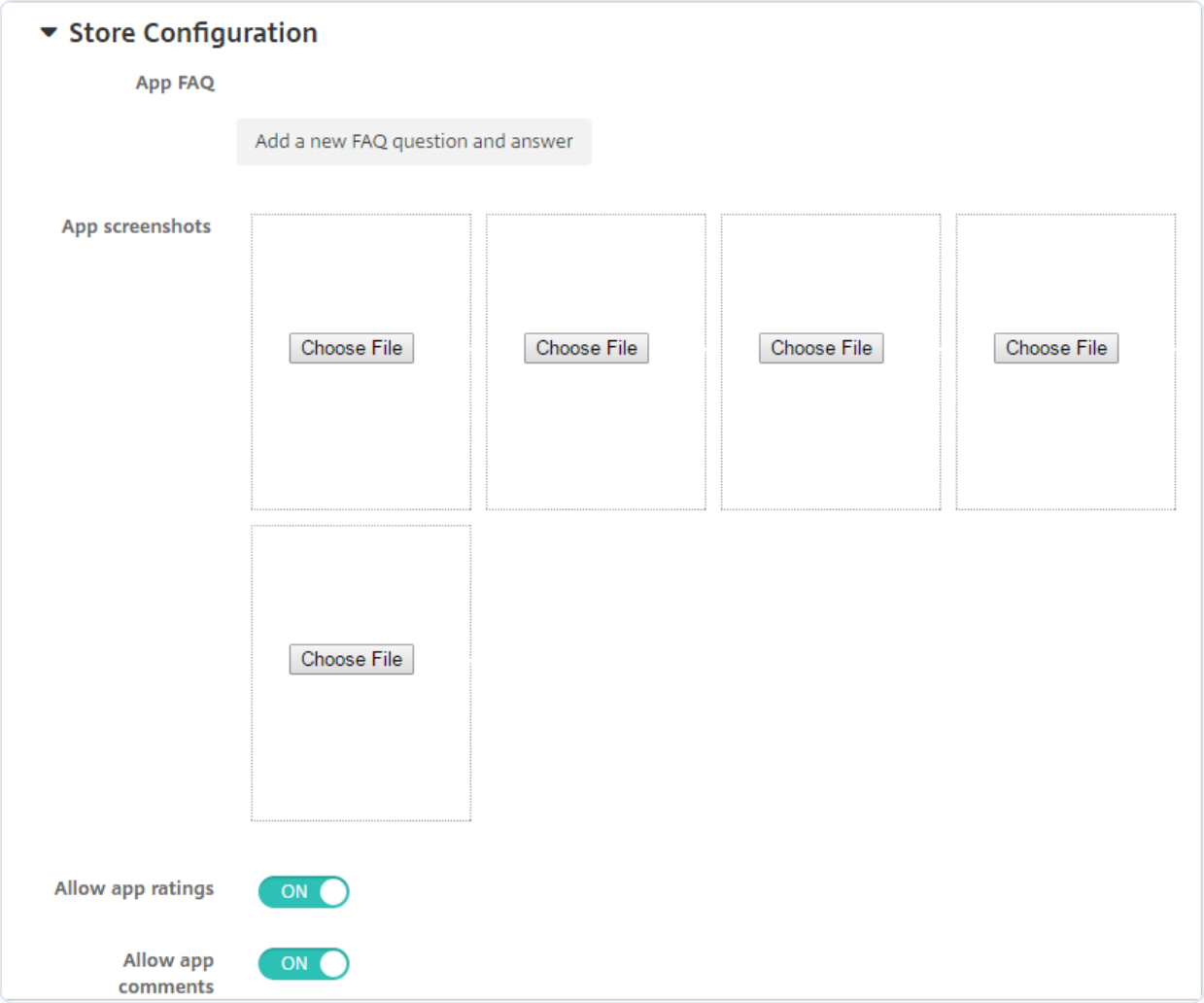
1. 在 XenMobile 控制台中，单击“**配置 > 应用 > 添加**”。此时将显示“**添加应用**”对话框。



2. 单击“**企业**”。此时将显示“**应用信息**”页面。
3. 在**应用程序信息**窗格中，键入以下信息:
   - **名称：** 键入应用程序的描述性名称。此名称在“应用程序”表中的“应用程序名称”下显示。
   - **描述：** 键入应用程序的可选描述。
   - **应用程序类别：** （可选）在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。
4. 单击**下一步**。此时将显示**应用程序平台**页面。
5. 在**平台**下，选择要添加的平台。如果仅为一个平台配置，请清除其他平台。
6. 对于您选择的每个平台，通过单击**上载**并导航到文件位置来选择要上载的文件。
7. 单击**下一步**。此时将显示该平台的应用程序信息页面。
8. 配置平台类型的设置，例如:
   - **文件名：** （可选）键入应用程序的新名称。
   - **应用程序描述：** （可选）键入应用程序的新描述。
   - **应用程序版本：** 无法更改此字段。
   - **最低操作系统版本：** （可选）键入设备可运行的用于使用应用程序的最旧操作系统版本。
   - **最高操作系统版本：** （可选）键入设备必须运行的用于使用应用程序的最新操作系统。
   - **排除的设备：** （可选）键入无法运行此应用程序的设备的制造商或型号。
   - **包 ID：** 您的应用的唯一标识符。

- **如果 MDM 配置文件被移除，则移除应用：** 选择当 MDM 配置文件被移除时是否从设备中移除应用。默认值为“**开**”。
- **阻止应用数据备份：** 选择是否阻止应用备份数据。默认值为“**开**”。
- **强制应用受管理：** 如果您正在安装一个非托管应用，如果您希望非受监管设备上的用户被提示允许管理该应用，请选择“**开**”。如果他们接受提示，则该应用将受管理。

9. 配置部署规则。有关信息，请参阅部署规则。
10. 展开**商店配置**。



- **应用常见问题：** 单击“**添加新的常见问题和答案**”为应用创建常见问题。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用评分：** 允许用户在应用商店中对应用进行评分。
- **允许应用评论：** 允许用户在应用商店中对应用发表评论。

11. 单击“**下一步**”。将显示“**审批**”页面。

要使用工作流在允许用户访问应用之前要求审批，请参阅应用工作流。如果您不需要审批工作流，请继续执行下一步。

12. 单击“**下一步**”。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在列表中选择一个或多个组。您选择的组将显示在“**接收应用分配的交付组**”列表中。
14. 展开**部署计划**，然后配置以下设置：

    - **部署：** 选择是否将应用程序部署到设备。默认值为**开**。
    - **部署计划：** 选择是**立即**还是**稍后**部署应用程序。如果选择**稍后**，请配置部署应用程序的日期和时间。默认值为**立即**。
    - **部署条件：** 选择**每次连接时**以在设备每次连接时部署应用程序。选择**仅当以前的部署失败时**以在设备以前未能接收应用程序时部署应用程序。默认值为**每次连接时**。

    始终在线连接部署在您已在**设置 > 服务器属性**中配置计划后台部署密钥时适用。

    您配置的部署计划适用于所有平台。您所做的任何更改都适用于所有平台，但**始终在线连接部署**除外。
15. 单击**保存**。

添加 Web 链接

Web 链接是 Internet 或 Intranet 站点的 Web 地址。Web 链接还可以指向不需要 SSO 的 Web 应用程序。完成配置 Web 链接后，该链接将作为图标显示在应用商店中。当用户使用 Secure Hub 登录时，该链接将与可用应用程序和桌面列表一起显示。

您可以从 XenMobile 控制台的**应用程序**选项卡配置 Web 链接。完成配置 Web 链接后，该链接将作为链接图标显示在**应用程序**表中的列表中。当用户使用 Secure Hub 登录时，该链接将与可用应用程序和桌面列表一起显示。

要添加链接，请提供以下信息：

- 链接名称
- 链接说明
- Web 地址 (URL)
- 类别
- 角色
- .png 格式的图像（可选）

1. 在 XenMobile 控制台中，单击“**配置 > 应用程序 > 添加**”。将显示“**添加应用程序**”对话框。

   应用程序配置屏幕(/en-us/xenmobile/server/media/configure-apps-add.png)

2. 单击“**Web 链接**”。将显示“**应用程序信息**”页面。
3. 在“**应用程序信息**”窗格中，键入以下信息：

   名称：键入应用程序的描述性名称。此名称将列在“应用程序”表中的“应用程序名称”下。 **说明**：键入应用程序的可选说明。 **应用程序类别**：可选。在列表中，单击要添加应用程序的类别。有关应用程序类别的详细信息，请参阅关于应用程序类别。

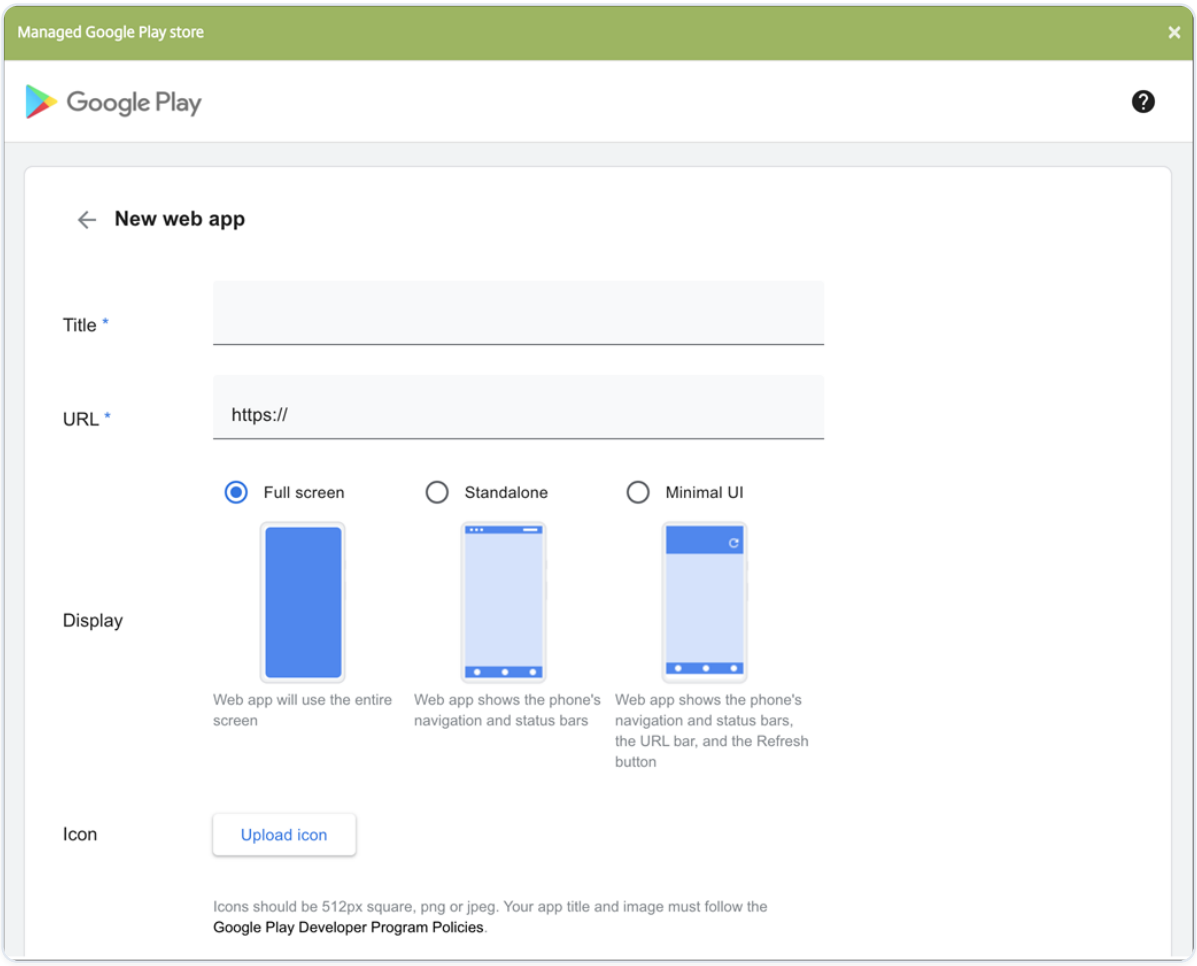
4. 单击“**下一步**”。将显示“**应用程序平台**”页面。
5. 在“**平台**”下，选择“**其他平台**”以添加适用于 iOS 和 Android（旧版 DA）的 Web 应用程序，或选择“**Android Enterprise**”。清除您不想添加的复选框。

   - 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**”按钮以打开托管的 Google Play 商店。您无需注册开发人员帐户即可发布 Web 应用程序。单击右下角的“**加号**”图标以继续。

     创建 Web 应用程序(/en-us/xenmobile/server/media/create-web-apps.png)

     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**最小化 UI**。
     - **图标**： 上传您自己的图像以表示 Web 应用程序。



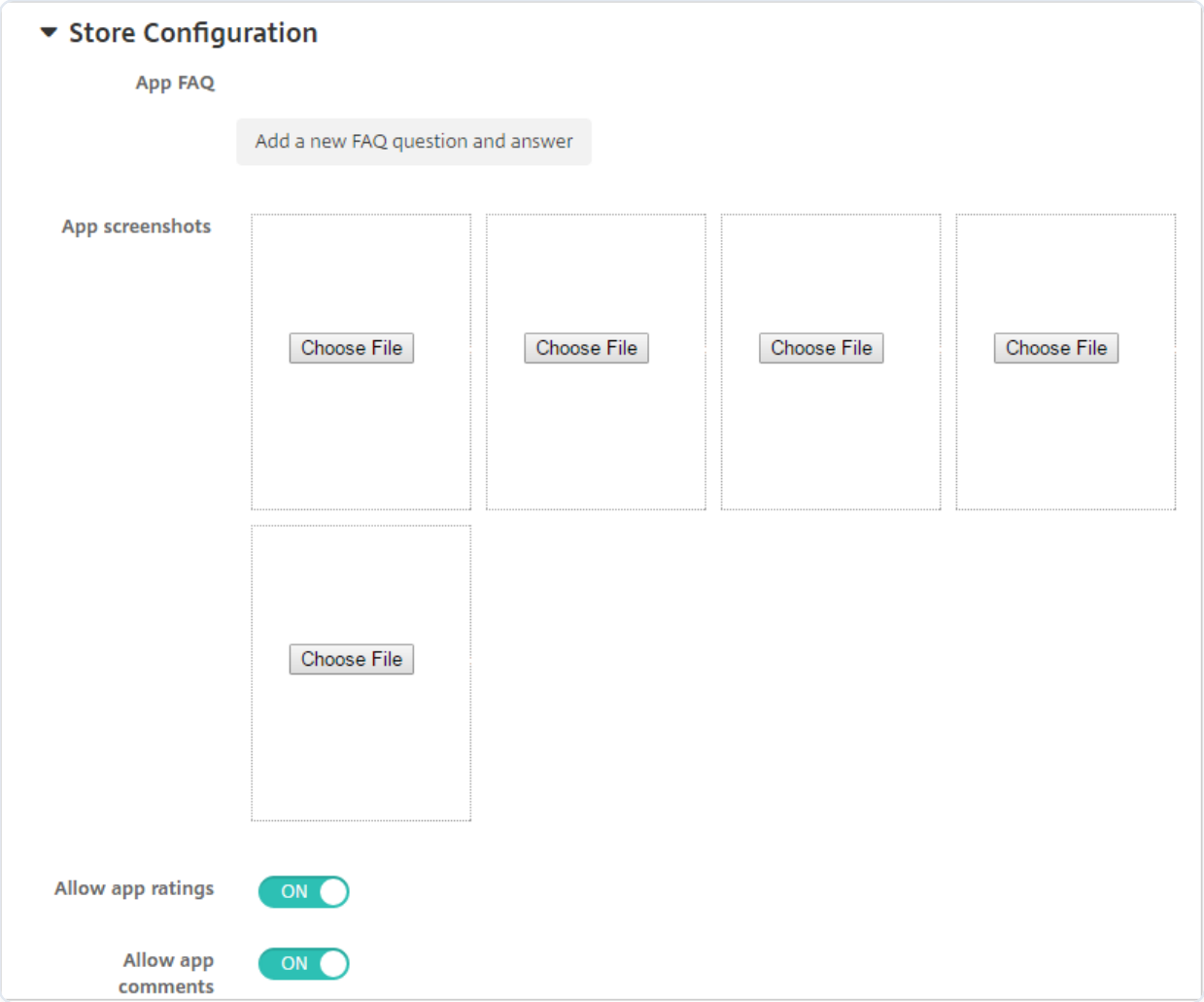
完成后，单击**创建**。您的 Web 应用程序发布可能需要长达 10 分钟。

6. 对于 Android Enterprise 以外的平台，请配置以下设置：

   - **应用程序名称：** 接受预填充的名称或键入新名称。
   - **应用程序描述：** 接受预填充的描述或键入您自己的描述。
   - **URL：** 接受预填充的 URL 或键入应用程序的 Web 地址。根据您选择的连接器，此字段可能包含一个占位符，您必须先替换它才能转到下一页。
   - **应用程序托管在内部网络中：** 选择应用程序是否在您的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，他们必须通过 Citrix Gateway 连接。将此选项设置为**开**会将 VPN 关键字添加到应用程序，并允许用户通过 Citrix Gateway 连接。默认值为**关**。
   - **应用程序类别：** 在列表中，单击要应用于应用程序的可选类别。
   - **图像：** 选择是使用默认的 Citrix 图像还是上传您自己的应用程序图像。默认值为“使用默认值”。
     - 要上传您自己的图像，请单击**浏览**并导航到文件位置。文件必须是 .PNG 文件。您不能上传 JPEG 或 GIF 文件。添加自定义图形后，您无法更改它。

7. 配置部署规则。有关信息，请参阅部署规则。

8. 展开**商店配置**。



- **应用常见问题：** 单击**添加新的常见问题解答**可为应用创建常见问题。
- **添加手机/平板电脑屏幕截图：** 添加显示在应用商店中的屏幕截图。
- **允许应用评分：** 允许用户在应用商店中对应用进行评分。
- **允许应用评论：** 允许用户在应用商店中对应用发表评论。

9. 单击**下一步**。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从列表中选择一个或多个组。您选择的组将显示在**接收应用分配的交付组**列表中。
11. 展开**部署计划**，然后配置以下设置：

- **部署：** 选择是否将应用部署到设备。默认值为**开**。
- **部署计划：** 选择是**立即**部署应用还是**稍后**部署。如果选择**稍后**，请配置部署应用的日期和时间。默认值为**立即**。

- **部署条件：** 选择**每次连接时**以在设备每次连接时部署应用。选择**仅当以前的部署失败时**以在设备以前未能接收到应用时部署应用。默认值为**每次连接时**。

当您在**设置 > 服务器属性**中配置了计划后台部署密钥时，**为始终连接部署**适用。

您配置的部署计划适用于所有平台。您所做的任何更改都将应用于所有平台，但**为始终连接部署**除外。

12. 单击**保存**。

启用 Microsoft 365 应用

您可以打开 MDX 容器，以允许 Secure Mail、Secure Web 和 Citrix Files 将文档和数据传输到 Microsoft Office 365 应用。有关详细信息，请参阅允许与 Office 365 应用安全交互。

应用工作流

配置以下设置以分配或创建工作流：

- **要使用的工作流：** 在列表中，单击现有工作流或单击**创建新工作流**。默认值为**无**。

  如果选择**创建新工作流**，请配置以下设置。

  - **名称：** 键入工作流的唯一名称。
  - **描述：** （可选）键入工作流的描述。
  - **电子邮件审批模板：** 在列表中，选择要分配的电子邮件审批模板。单击此字段右侧的眼睛图标时，将出现一个对话框，您可以在其中预览模板。
  - **经理审批级别：** 在列表中，选择此工作流所需的经理审批级别数。默认值为 1 级。可能的选项包括：
    - 不需要
    - 1 级
    - 2 级
    - 3 级
  - **选择 Active Directory 域：** 在列表中，选择要用于工作流的相应 Active Directory 域。
  - **查找其他必需的审批者：** 在搜索字段中键入其他必需人员的姓名，然后单击**搜索**。姓名源自 Active Directory。
  - 当姓名出现在字段中时，选中姓名旁边的复选框。姓名和电子邮件地址将显示在**选定的其他必需审批者**列表中。

要从**选定的其他必需审批者**列表中删除人员，请执行以下操作之一：

- 单击**搜索**以查看所选域中所有人员的列表。
- 在搜索框中键入完整或部分名称，然后单击**搜索**以限制搜索结果。
- **选定的其他必需审批者**列表中的人员在搜索结果列表中其姓名旁边有复选标记。滚动列表并清除要删除的每个姓名旁边的复选框。

应用商店和 Citrix Secure Hub 品牌

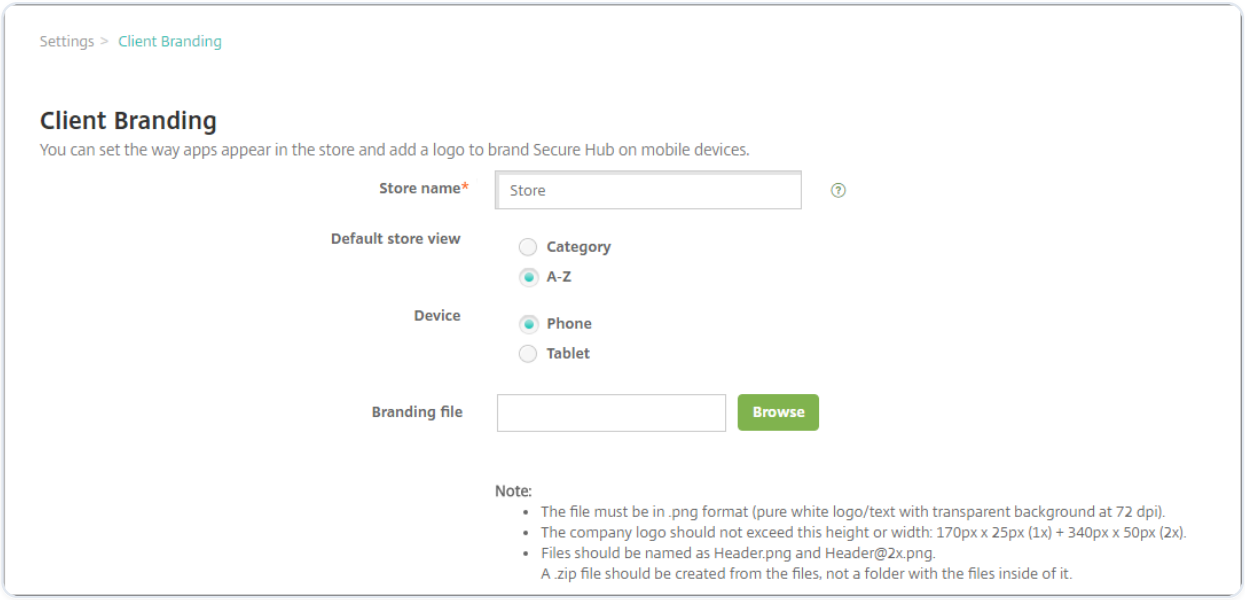
您可以设置应用在商店中的显示方式，并添加徽标以对 Secure Hub 和应用商店进行品牌化。这些品牌功能适用于 iOS 和 Android 设备。

开始之前，请确保您的自定义图像已准备就绪且可访问。

自定义图像必须满足以下要求：

- 文件必须是 .png 格式
- 使用纯白色徽标或文本，背景透明，分辨率为 72 dpi。
- 公司徽标的高度或宽度不应超过：170 像素 x 25 像素 (1x) 和 340 像素 x 50 像素 (2x)。
- 将文件命名为 Header.png 和 `Header@2x.png`。
- 从文件创建 .zip 文件，而不是包含这些文件的文件夹。

1. 在 XenMobile Server 控制台中，单击右上角的齿轮图标。将显示**设置**页面。
2. 在**客户端**下，单击**客户端品牌**。将显示**客户端品牌**页面。



配置以下设置：

- **商店名称：** 商店名称显示在用户的帐户信息中。更改名称也会更改用于访问商店服务的 URL。通常，您无需更改默认名称。

> **重要提示：**
>
> 商店名称只能包含字母数字字符。

- **默认商店视图：** 选择**类别**或**A-Z**。默认值为**A-Z**
- **设备选项：** 选择**手机**或**平板电脑**。默认值为**手机**。
- **品牌文件：** 通过单击**浏览**并导航到文件位置，选择用于品牌推广的图像或图像 .zip 文件。

3. 单击**保存**。

应用连接器类型

下表列出了在 XenMobile® 中添加 Web 或 SaaS 应用程序时可用的连接器及其类型。您还可以在添加 Web 或 SaaS 应用程序时向 XenMobile 添加新的连接器。

该表指明了连接器是否支持用户帐户管理，通过该功能，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	是	是
Globoforce_SAML		**注意：**使用此连接器时，您必须为预配启用用户管理，以实现无缝 SSO 集成。
GoogleApps_SAML	是	是
GoogleApps_SAML_IDP	是	是
Lynda_SAML	是	是
Office365_SAML	是	是
Salesforce_SAML	是	是
Salesforce_SAML_SP	是	是

连接器名称	SSO SAML	支持用户帐户管理
SandBox_SAML	是	
SuccessFactors_SAML	是	
ShareFile_SAML	是	
ShareFile_SAML_SP	是	
WebEx_SAML_SP	是	是

升级 MDX 或企业应用

要在 XenMobile 中升级 MDX 或企业应用，请在 XenMobile 控制台中禁用该应用，然后上传新版本的应用。您无需禁用公共应用商店应用，例如 Citrix Secure Mail。

1. 在 XenMobile® 控制台中，单击“**配置 > 应用**”。此时将显示“**应用**”页面。
2. 对于托管设备（已在 XenMobile 中注册以进行移动设备管理的设备），请跳至步骤 3。对于非托管设备（仅为企业应用管理目的而在 XenMobile 中注册的设备），请执行以下操作：

   a. 在“**应用**”表中，选中应用旁边的复选框，或单击包含要更新的应用的行。

   b. 在出现的菜单中单击“**禁用**”。

   应用菜单(/en-us/xenmobile/server/media/configure-apps-disable-app.png)

   c. 在确认对话框中单击“**禁用**”。应用的“**禁用**”列中将显示“*已禁用*”。

   已禁用的应用(/en-us/xenmobile/server/media/configure-apps-disable-app-disabled.png)

   > **注意：**
   >
   > 应用禁用后，用户注销后无法重新连接到该应用。禁用应用是可选的，但我们建议禁用应用以避免应用功能出现问题。例如，用户在您上传新版本的同时请求下载应用可能会导致问题。

3. 在“**应用**”表中，单击应用旁边的复选框，或单击包含要更新的应用的行。
4. 在出现的菜单中单击“**编辑**”。此时将显示“**应用信息**”页面，其中已选择您最初为该应用选择的平台。

5. 配置以下设置：
   - **名称：**可选，更改应用名称。
   - **说明：**（可选）更改应用程序说明。
   - **应用程序类别：**（可选）更改应用程序类别。
6. 单击**下一步**。将显示第一个选定平台页面。对每个选定平台执行以下操作：
   a. 通过单击**上载**并导航到文件位置来选择要上载的替换文件。应用程序将上载到 XenMobile。

      如果您要上载 Android Enterprise 应用程序，将显示一个托管 Google Play 窗口。在此处上载新版本的应用程序。有关详细信息，请参阅分发 Android Enterprise 应用程序。

   b. （可选）更改该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**。将显示**应用程序**页面。
8. 如果您在步骤 2 中禁用了应用程序，请执行以下操作：
   a. 在**应用程序**表中，单击以选择您更新的应用程序，然后在显示的菜单中单击**启用**。
   b. 在显示的确认对话框中，单击**启用**。用户现在可以访问该应用程序并收到提示他们升级应用程序的通知。

Citrix 启动器

Citrix Launcher 替代方案

Citrix 于 2020 年 8 月从应用商店中移除了 Citrix Launcher。要替代 Citrix Launcher，您可以使用已有的功能。

要将设备预配为自助服务终端（专用设备）：

1. 添加一个 RBAC 角色，允许 XenMobile 管理员将专用设备注册到您的 XenMobile 部署中。请参阅 预配专用 Android Enterprise 设备。
2. 创建注册配置文件，并将**注册类型**设置为**完全托管/工作配置文件**。请参阅 创建注册配置文件。
3. 通过启用**锁定任务模式**设置，创建自助服务终端设备策略以配置要固定到设备屏幕的应用程序。请参阅 Android Enterprise 设置。

关于 Citrix 启动器

Citrix Launcher 允许您自定义 XenMobile 部署的 Android 设备的用户体验。Secure Hub 管理 Citrix Launcher 支持的最低 Android 版本为 Android 4.0.3。Citrix Launcher 和启动器配置设备策略与 Android Enterprise 不兼容。

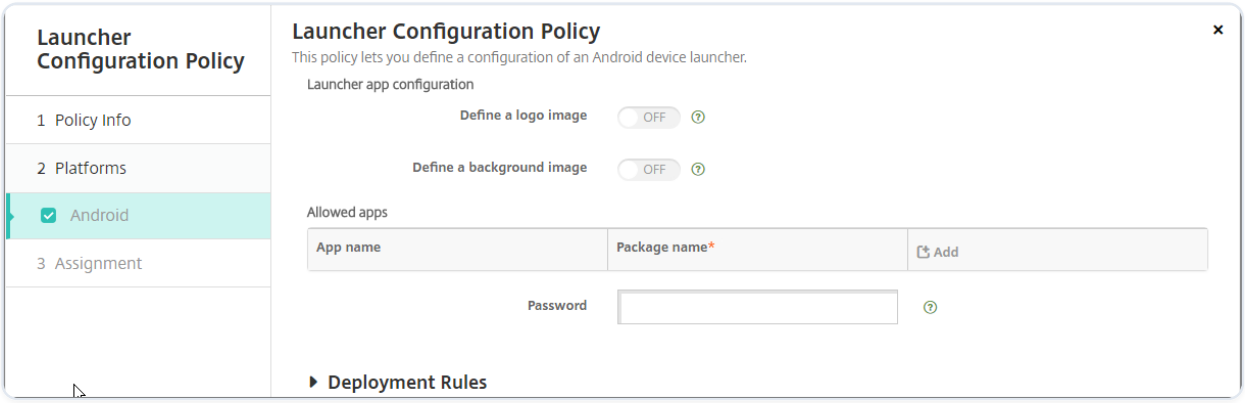
您可以添加**启动器配置策略**来控制以下 Citrix Launcher 功能：

- 管理 Android 设备，以便用户只能访问您指定的应用程序。
- 可选地为 Citrix Launcher 图标指定自定义徽标图像，并为 Citrix Launcher 指定自定义背景图像。
- 指定用户必须输入才能退出启动器的密码。

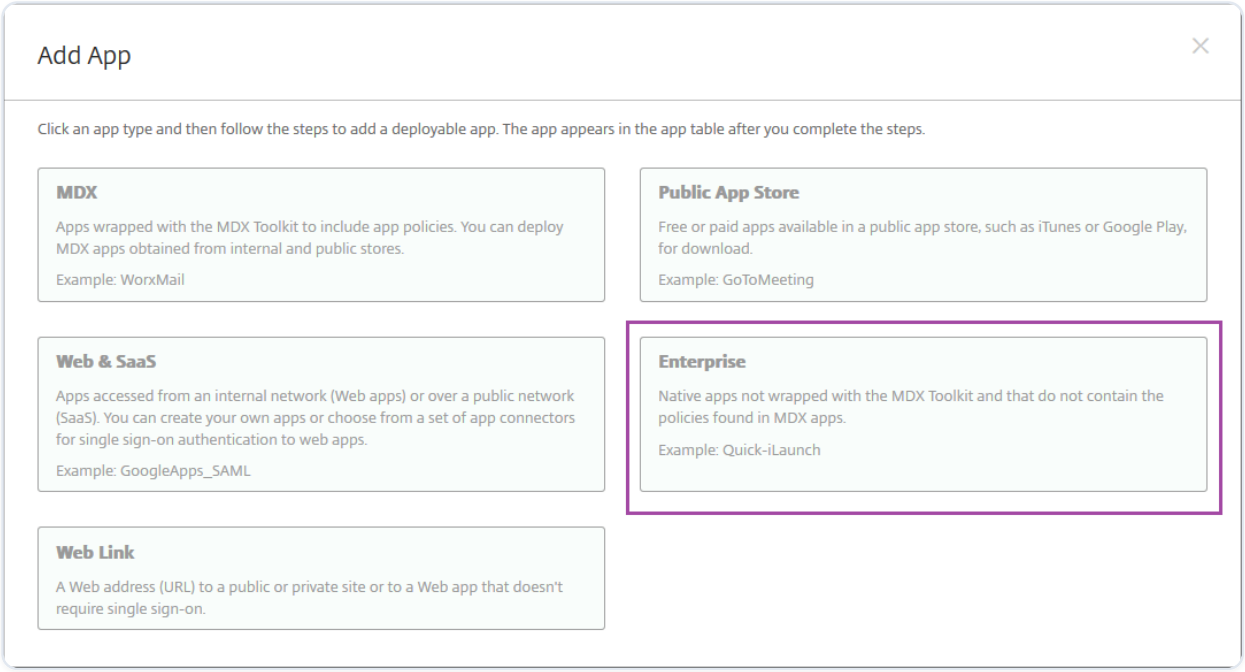
虽然 Citrix Launcher 允许您应用这些设备级限制，但启动器授予用户对设备设置（例如 Wi-Fi 设置、蓝牙设置和设备密码设置）的内置访问权限。Citrix Launcher 并非旨在作为设备平台已提供安全性的额外层。

要为 Android 设备提供 Citrix Launcher，请遵循以下常规步骤。

1. 要下载 Citrix Launcher 应用程序：转到 `<https://www.citrix.com/downloads>`。搜索 **Citrix Launcher**。文件名为 CitrixLauncher.apk。该文件已准备好上传到 XenMobile，无需打包。
2. 添加设备策略 **Launcher Configuration Policy**。转到 **Configure > Device Policies**，单击 **Add**，然后在 **Add a New Policy** 对话框中，开始键入 **Launcher**。有关详细信息，请参阅 Launcher Configuration Policy。

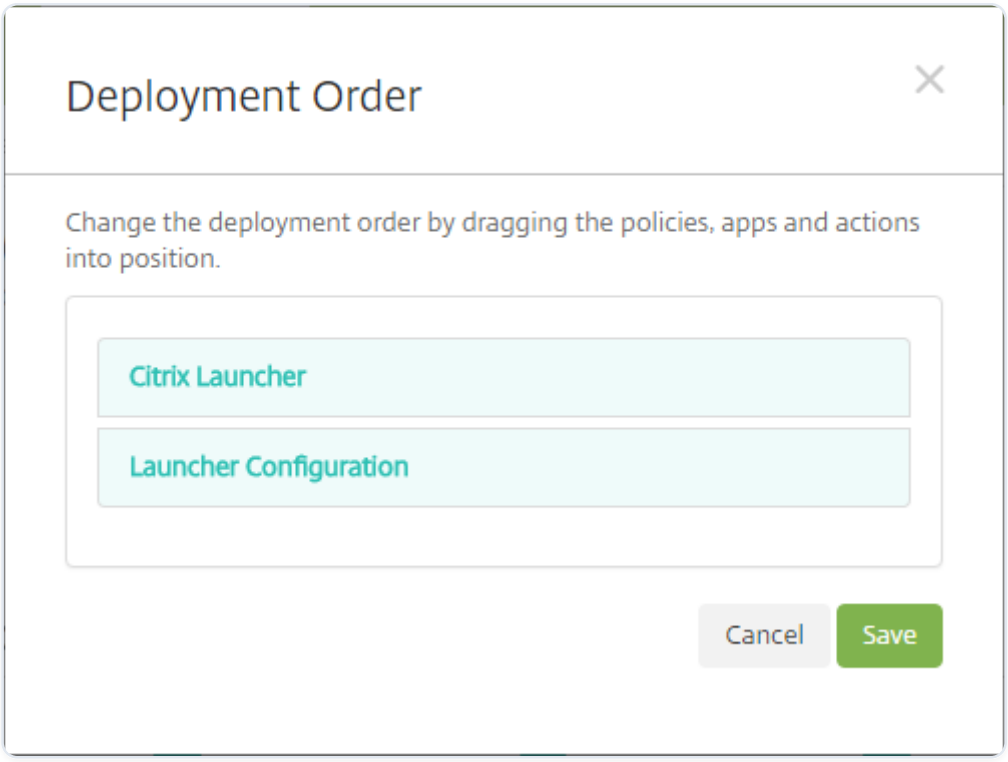


3. 将 Citrix Launcher 应用程序作为企业应用程序添加到 XenMobile。在 **Configure > Apps** 中，单击 **Add**，然后单击 **Enterprise**。有关详细信息，请参阅 Add an enterprise app。



4. 在 **Configure > Delivery groups** 中，为 Citrix Launcher 创建一个具有以下配置的交付组。

   - 在“**策略**”页面上，添加“**启动器配置策略**”。
   - 在 **Apps** 页面上，将 **Citrix Launcher** 拖动到 **Required Apps**。
   - 在 **Summary** 页面上，单击 **Deployment Order**，并确保 **Citrix Launcher** 应用程序在 **Launcher Configuration** 策略之前。



有关详细信息，请参阅 Deploy resources。

Apple 批量采购

您可以使用 Apple iOS 批量采购来管理 iOS 应用程序许可。批量采购解决方案简化了为组织批量查找、购买和分发应用程序及其他数据的过程。

通过批量采购，您可以使用 XenMobile® 分发公共应用商店应用程序。

- MAM 注册不支持批量采购。您必须在 MDM 或 MDM+MAM 中注册批量采购设备。
- 批量采购不支持 Citrix® 移动生产力应用程序。
- 尽管您可以通过批量采购分发 XenMobile 公共商店应用程序，但部署效果不佳。需要对 XenMobile 和 Secure Hub 商店进行增强以解决这些限制。
- 有关通过批量采购分发 XenMobile 公共商店应用程序的已知问题列表，请参阅 Citrix 知识中心中的 CTX222633。

通过批量采购，您可以将适用的应用程序直接分发到您的设备。或者，您可以通过兑换码将内容分配给用户。您可以在 XenMobile 中配置 iOS 批量采购的特定设置。

XenMobile 会定期从 Apple 重新导入批量采购许可证，以确保许可证反映所有更改。此类更改包括您从批量采购中手动删除导入的应用程序时。默认情况下，XenMobile 至少每 1440 分钟（24 小时）刷新一次批量采购许可证基线。您可以通过服务器属性 `VPP.baseline` 更改批量采购基线间隔。请参阅 服务器属性。

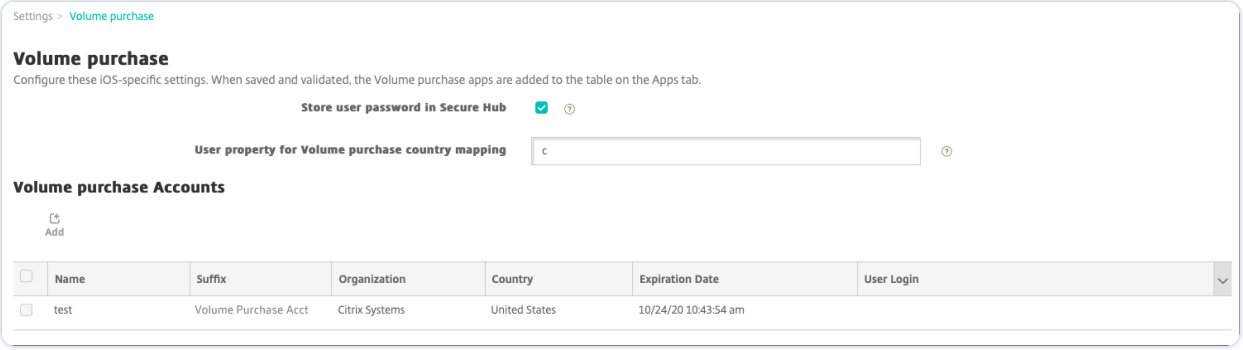
“**应用程序自动更新**”设置也依赖于 `VPP.baseline` 服务器属性，并且应用程序会按照该属性中设置的相同计划进行更新。

本文重点介绍将批量采购与托管许可证结合使用，这使您能够使用 XenMobile 分发应用程序。如果您当前使用兑换码并希望更改为托管分发，请参阅此 Apple 支持文档 从兑换码迁移到批量采购的托管分发。

有关 iOS 批量采购的信息，请参阅 `<https://volume.itunes.apple.com/us/store>`。要注册批量采购，请访问 `<https://deploy.apple.com/qforms/open/register/index/avs>`。要在 iTunes 中访问您的批量采购商店，请访问 `<https://volume.itunes.apple.com/?l=en>`。

在 XenMobile 中保存这些 iOS 批量采购设置后，购买的应用程序将显示在 XenMobile 控制台的“**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。将显示“**设置**”页面。
2. 单击“**批量采购**”。将显示“**批量采购**”配置页面。



3. 配置以下设置：

   - **在 Secure Hub 中存储用户密码：** 选择是否在 Secure Hub 中存储用户名和密码以进行 XenMobile 身份验证。默认情况下，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：** 键入一个代码，以允许用户从特定国家/地区的应用程序商店下载应用程序。

   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，则如果批量购买代码适用于英国，该用户将无法下载应用程序。有关国家/地区映射代码的更多信息，请联系您的批量购买计划管理员。

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. 为添加的每个帐户配置以下设置：

   > **注意：**
   >
   > 如果您使用 Apple Configurator 1，请上传许可证文件：转到“**配置 > 应用程序**”，转到平台页面，然后展开“**批量购买**”。

   - **名称：** 键入批量购买帐户名称。
   - **后缀：** 键入将与通过批量购买帐户获得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：在 Apple 批量购买门户的“**帐户摘要**”页面中，单击“**下载**”按钮以生成并下载批量购买文件。该文件包含服务令牌和其他信息，例如国家/地区代码和有效期。将文件保存在安全位置。
   - **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。

- **应用自动更新**：如果为**开**，批量购买的应用会在 Apple Store 中存在更新时自动更新。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。

   将显示一条消息，指出 XenMobile 将应用添加到**配置 > 应用**页面上的列表中。在该页面上，请注意，批量购买帐户中的应用名称包含您在上述配置中提供的后缀。

现在，您可以配置批量购买应用设置，然后调整批量购买应用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。以下说明提供了这些过程的注意事项。

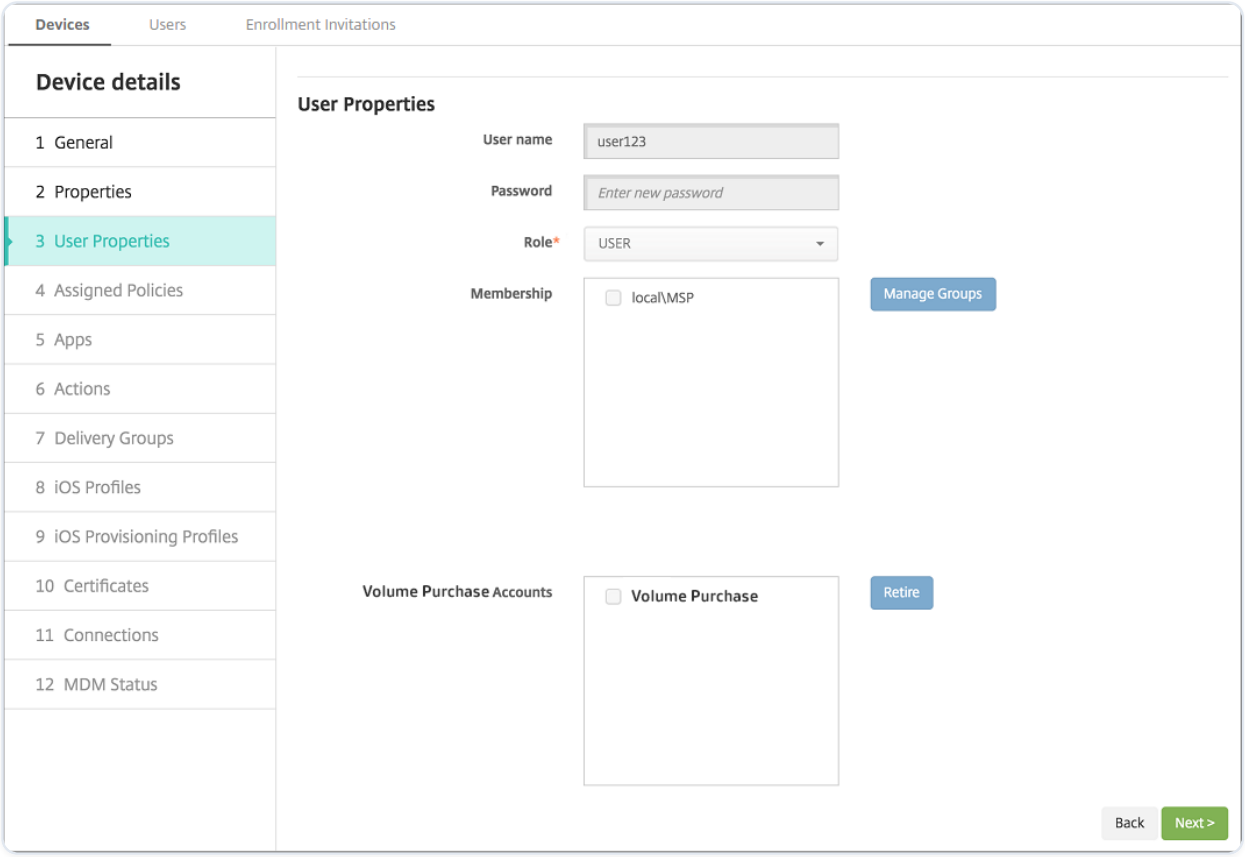
- 配置批量购买应用设置（**配置 > 应用**）时，启用**强制许可证与设备关联**。

  将 Apple 批量购买和部署计划与受监管设备结合使用的优势：能够使用 XenMobile 在设备（而非用户）级别分配应用。因此，您无需使用 Apple ID 设备。此外，用户不会收到加入 Apple 批量购买的邀请。用户还可以下载应用，而无需登录其 iTunes 帐户。

  - 要查看该应用的批量购买信息，请展开**批量购买**。请注意，在**批量购买许可证密钥**表中，许可证与设备关联。如果用户删除令牌然后再次导入，则由于 Apple 隐私限制，将显示**隐藏**而不是序列号。

  - 要取消关联许可证，请单击许可证所在行，然后单击**取消关联**。

  - 如果您将批量购买许可证与用户关联，XenMobile 会将用户集成到您的批量购买帐户中。此外，还会将其 iTunes ID 与批量购买帐户关联。用户的 iTunes ID 对您的公司或 XenMobile Server 始终不可见。Apple 透明地创建关联以保留用户隐私。您可以从 Apple 批量购买中停用用户，以取消关联用户帐户中的所有许可证。要停用用户，请转至**管理 > 设备**。



- 将应用分配给交付组时，XenMobile 默认将该应用标识为可选应用。要确保 XenMobile 将应用部署到设备，请转至**配置** > **交付组**。在**应用**页面上，将应用移动到**所需应用**列表。
- 当应用程序有可用更新时，批量采购会将更新推送到应用程序，并自动更新设备上的应用程序。有关详细信息，请参阅检查应用程序更新。

  当 Apple 批量采购过期时，XenMobile 会显示许可证过期警告。

检查应用程序更新

如果您在添加批量采购帐户时开启了**应用程序自动更新**设置，XenMobile Server 会定期检查批量采购的应用程序（必需应用程序）和从 Citrix Secure Hub 商店订阅的可选应用程序的新版本并进行更新。一旦 XenMobile Server 收到必需应用程序的新版本，它会自动将新版本推送到设备进行安装，而无需提示您手动更新。但是，要自动更新可选应用程序，属性 `apple.ios.optional_app_update` 必须设置为 **True**。否则，您必须手动更新可选应用程序。有关详细信息，请参阅服务器属性。

要手动检查任何应用程序的新版本并进行更新，请执行以下步骤：

1. 单击**配置** > **应用程序**。

此时将显示**应用程序**页面。

2. 选择一个应用程序，然后单击**编辑**。
3. 转到**平台**页面，然后单击**版本**旁边的**检查更新**按钮。
4. 在**更新**对话框中，如果有新版本可用，请应用更新。

通过 Citrix Secure Hub™ 提供的虚拟应用和桌面

XenMobile 可以从虚拟应用和桌面收集应用程序，并将其提供给 XenMobile Store 中的移动设备用户。用户可以直接在 XenMobile Store 中订阅应用程序，并从 Secure Hub 启动它们。用户设备上必须安装 Citrix Receiver™ 才能启动应用程序，但无需对其进行配置。

要配置此设置，您需要 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。**设置**页面随即显示。
2. 单击**虚拟应用和桌面**。**虚拟应用和桌面**页面随即显示。

   虚拟应用和桌面设置屏幕(/en-us/xenmobile/server/media/configure-virtual-apps-and-desktops-with-test-connection-button.png)

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 与客户端设备之间启用安全身份验证。默认值为关闭。**
4. 单击**测试连接**以验证 XenMobile 是否可以连接到指定的虚拟应用和桌面服务器。
5. 单击**保存**。

将 ShareFile 与 XenMobile® 结合使用

> **免责声明：**

> 如果 ShareFile（现为 Progress）停止支持，此功能将被弃用。

> XenMobile 有两种与 ShareFile 集成的方式：Citrix Files 和存储区域连接器。与 Citrix Files 或存储区域连接器集成需要 XenMobile Advanced Edition（本地）或 Citrix Endpoint Management™（云）。

Citrix 文件

如果您拥有 XenMobile Advanced Edition（本地）或 Citrix Endpoint Management（云），您可以配置 XenMobile 以提供对您的 Citrix Files 帐户的访问。该配置：

- 为移动用户提供对完整企业功能集的访问，例如文件共享、文件同步和存储区域连接器。
- 可以为 Citrix Files 提供 XenMobile App 用户的单点登录身份验证和全面的访问控制策略。
- 通过 XenMobile 控制台提供 Citrix Files 配置、服务级别监控和许可证使用情况监控。

有关为 Citrix Files 配置 XenMobile 的更多信息，请参阅 SAML for single sign-on with Citrix Files。

存储区域连接器

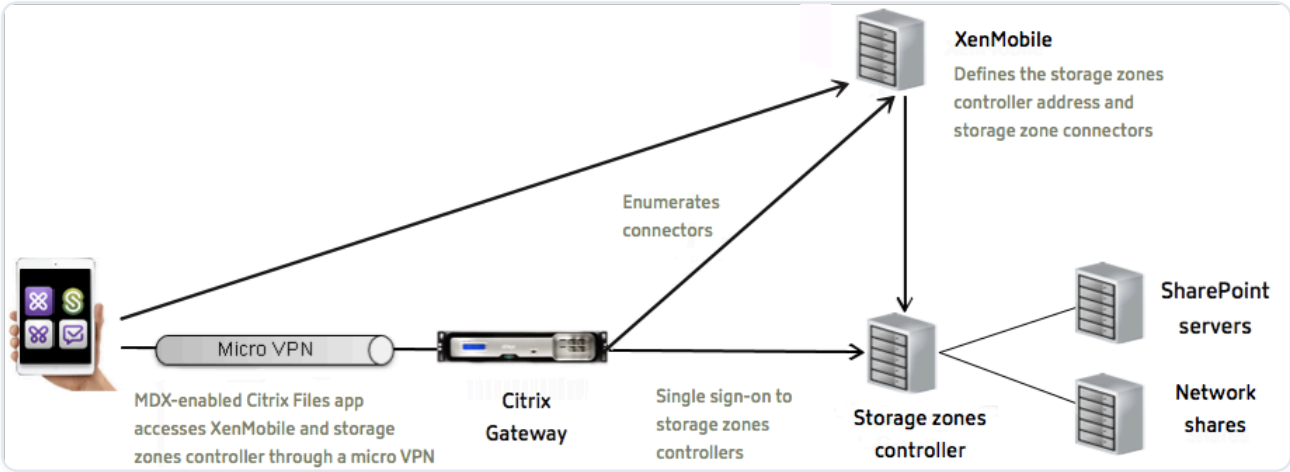
您可以配置 XenMobile，使其仅提供对通过 XenMobile 控制台创建的存储区域连接器的访问。该配置：

- 提供对现有本地存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问。
- 不需要您设置 ShareFile 子域或托管 Citrix Files 数据。
- 通过适用于 iOS 和 Android 的 Citrix Files 移动生产力应用程序，为您提供对数据的移动访问。您可以编辑 Microsoft Office 文档。此外，您还可以从移动设备预览和批注 Adobe PDF 文件。
- 遵守安全限制，防止用户信息泄露到公司网络之外。
- 通过 XenMobile 控制台提供存储区域连接器的简单设置。如果以后决定将完整的 Citrix Files 功能与 XenMobile 结合使用，可以在 XenMobile 控制台中更改配置。
- 需要 XenMobile 高级版（本地）或 Citrix 端点管理（云）。

仅适用于 XenMobile 与存储区域连接器的集成：

- ShareFile 使用您的单点登录配置到 Citrix Gateway，以通过存储区域控制器进行身份验证。
- XenMobile 不通过 SAML 进行身份验证，因为未使用 Citrix Files 控制平面。

下图显示了 XenMobile 与存储区域连接器配合使用的高级架构。



要求

- 最低组件版本：
  - XenMobile Server 10.5（本地）
  - 适用于 iOS 的 ShareFile (MDX) 5.3
  - 适用于 Android 的 ShareFile (MDX) 5.3
  - 存储区域控制器 5.0

    本文提供了有关如何配置存储区域控制器 5.0 的说明。
- 确保运行存储区域控制器的服务器满足系统要求。有关要求，请参阅系统要求。

Citrix Files Data 存储区域和受限存储区域的要求不适用于仅与存储区域连接器集成的 XenMobile。

XenMobile 不支持 Documentum 连接器。

- 要运行 PowerShell 脚本：
  - 在 32 位 (x86) 版本的 PowerShell 中运行脚本。

安装任务

按照所示顺序完成以下任务，以安装和设置存储区域控制器。这些步骤仅适用于 XenMobile 与存储区域连接器的集成。其中一些文章位于存储区域控制器文档中。

1. 为存储区域控制器配置 Citrix ADC

   您可以将 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。托管受限区域并使用内部地址的存储区域控制器不需要 SSL 证书。

3. 准备服务器

   存储区域连接器需要 IIS 和 ASP.NET 设置。

4. 安装存储区域控制器
5. 准备存储区域控制器以仅与存储区域连接器配合使用
6. 为存储区域指定代理服务器(/zh-cn/storagezones-controller/5-0/install/specify-proxy.html)

   存储区域控制器控制台允许您为存储区域控制器指定代理服务器。您也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(/zh-cn/storagezones-controller/5-0/install/configure-domain-controller.html)

   配置域控制器以支持网络共享或 SharePoint 站点上的 NTLM 或 Kerberos 身份验证。

8. 将辅助存储区域控制器加入存储区域(#join-a-secondary-storage-zones-controller-to-a-storage-zone)

   要为高可用性配置存储区域，请至少连接两个存储区域控制器。

安装存储区域控制器

1. 下载并安装存储区域控制器软件：

   a. 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。

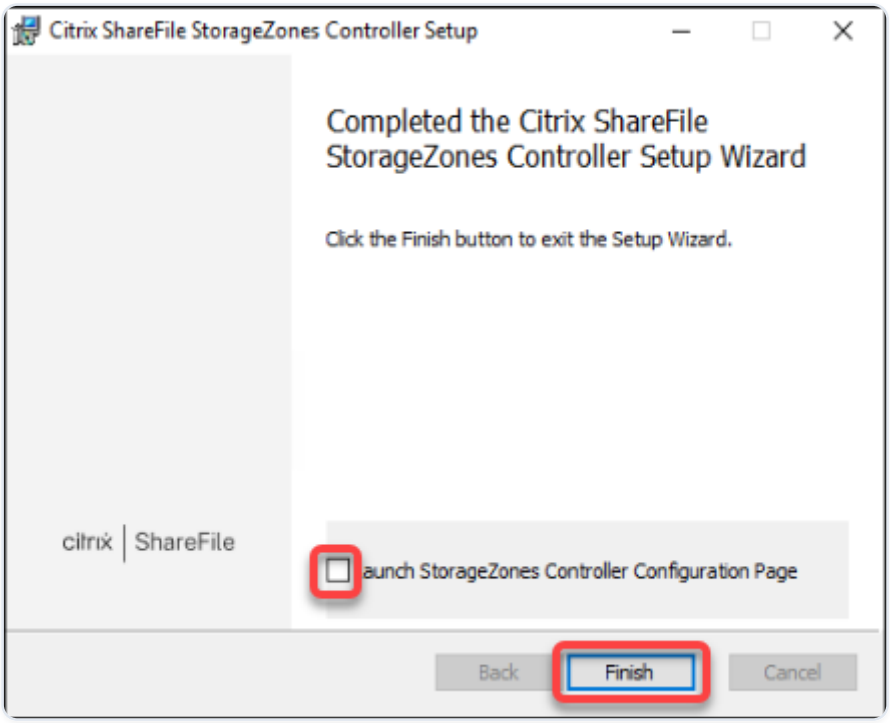
   b. 安装存储区域控制器会将服务器上的默认网站更改为控制器的安装路径。在默认网站上启用**匿名身份验证**。

2. 在要安装存储区域控制器的服务器上，运行 StorageCenter.msi。

   存储区域控制器安装向导启动。

3. 响应提示：

   - 在**目标文件夹**页面中，如果 Internet Information Services (IIS) 安装在默认位置，请保留默认设置。否则，请浏览到 IIS 安装位置。
   - 安装完成后，清除**启动存储区域控制器配置页面**的复选框，然后单击**完成**。



4. 出现提示时，重新启动存储区域控制器。
5. 要测试安装是否成功，请导航到 `https://localhost/`。如果安装成功，将显示 Citrix Files 徽标。

   如果未显示 Citrix Files 徽标，请清除浏览器缓存然后重试。

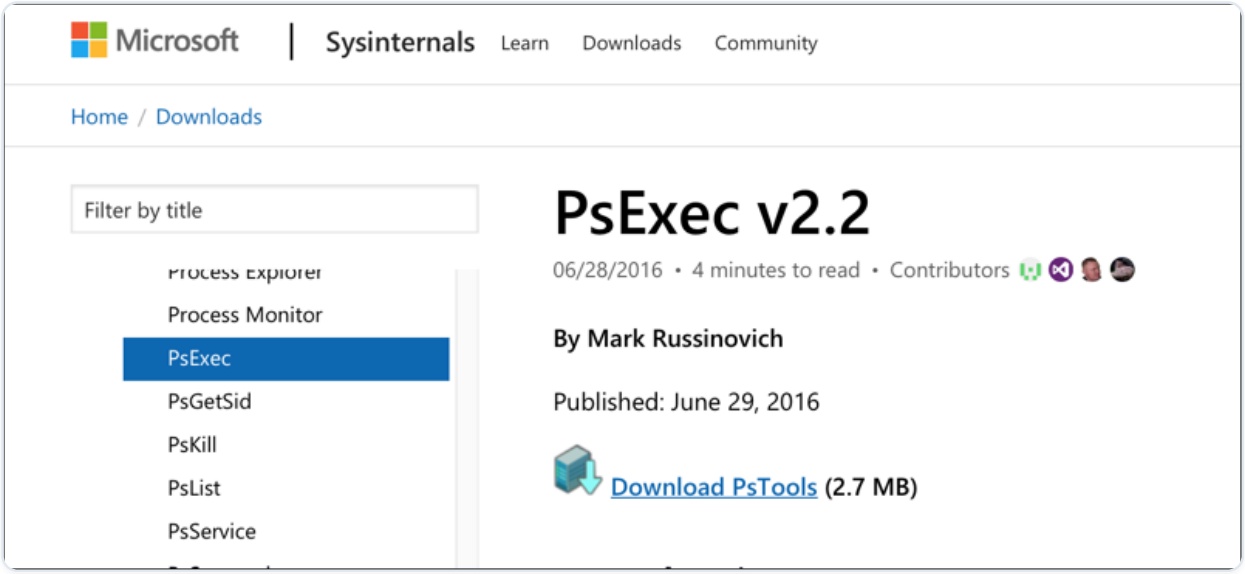
> **重要提示：**
>
> 如果您计划克隆存储区域控制器，请在继续配置存储区域控制器之前捕获磁盘映像。

准备存储区域控制器以仅用于存储区域连接器

对于仅与存储区域连接器集成的部署，您无需使用存储区域控制器管理控制台。该界面需要 Citrix Files 管理员帐户，这对于此解决方案而言并非必需。因此，您需要运行 PowerShell 脚本以准备存储区域控制器，使其在没有 Citrix Files 控制平面的情况下使用。该脚本执行以下操作：

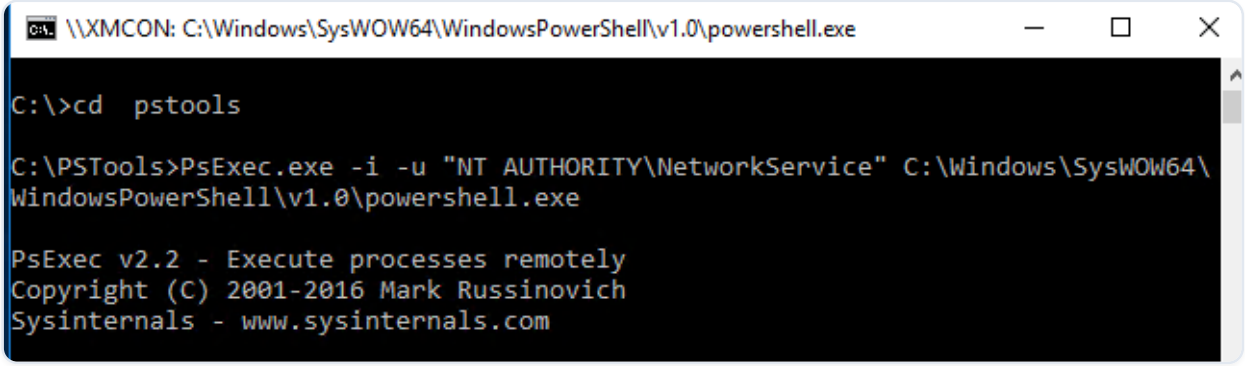
- 将当前存储区域控制器注册为主存储区域控制器。您以后可以将辅助存储区域控制器加入到主控制器。
- 创建区域并为其设置密码。

1. 从您的存储区域控制器服务器，下载 PsExec 工具：导航到 Microsoft Windows Sysinternals，然后单击 **Download PsTools**。将该工具解压到 C 盘根目录。

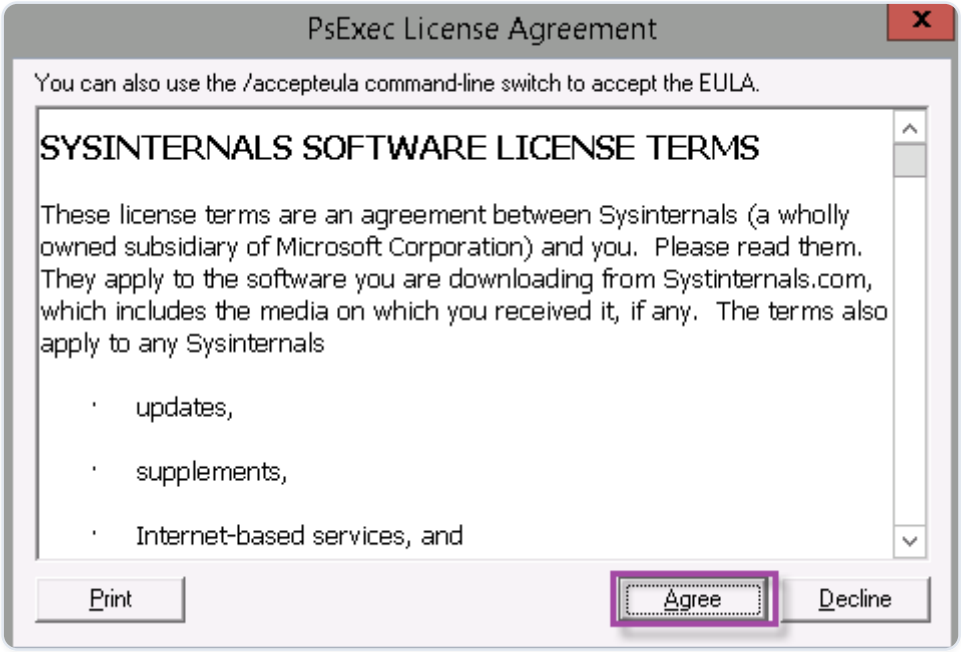


2. 运行 PsExec 工具：以管理员用户身份打开命令提示符，然后键入以下内容：

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. 出现提示时，单击 **Agree** 以运行 Sysinternals 工具。



一个 PowerShell 窗口打开。

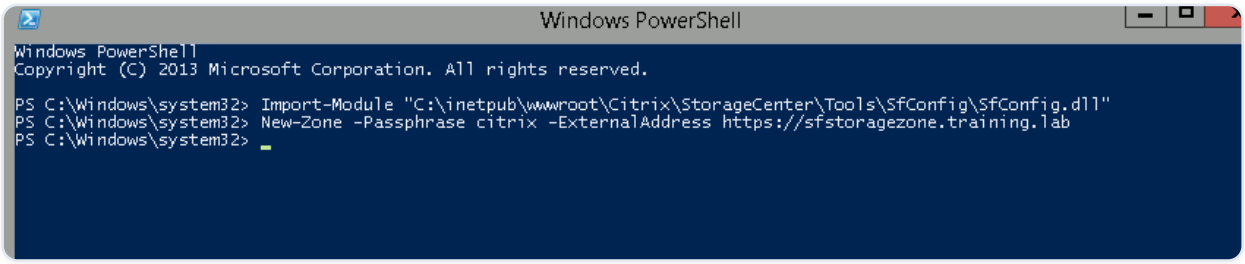
4. 在 PowerShell 窗口中，键入以下内容：

```
Import-Module "C:
\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

其中：

密码短语： 是要分配给站点的密码短语。请记下它，因为无法从控制器恢复密码短语。如果丢失密码短语，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存储区域，或者在服务器发生故障时恢复存储区域。

外部地址： 是存储区域控制器服务器的外部完全限定域名。



您的主存储区域控制器现已准备就绪。

在登录 XenMobile 创建存储区域连接器之前：如果适用，请完成以下配置：

为存储区域指定代理服务器

配置域控制器以信任存储区域控制器进行委派

将辅助存储区域控制器加入存储区域

要创建存储区域连接器，请参阅 在 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

要配置高可用性存储区域，请至少连接两个存储区域控制器。要将辅助存储区域控制器加入某个区域，请在第二台服务器上安装存储区域控制器。然后将该控制器加入主控制器的区域。

1. 在要加入主服务器的存储区域控制器服务器上打开 PowerShell 窗口。
2. 在 PowerShell 窗口中，键入以下内容：

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

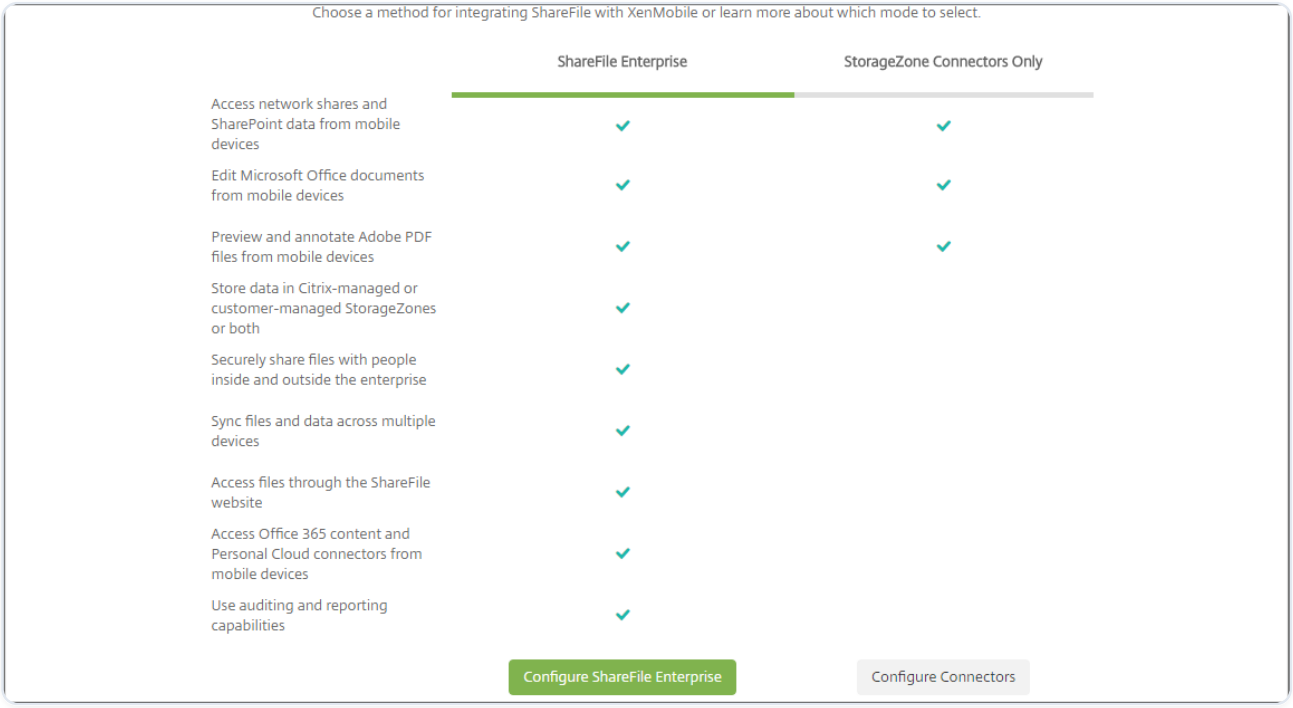
   例如：

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

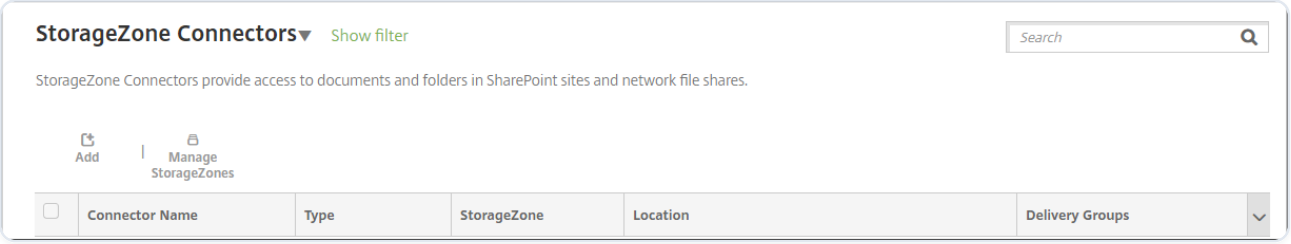
在 XenMobile 中定义存储区域控制器连接

在添加存储区域连接器之前，请为每个已启用存储区域连接器的存储区域控制器配置连接信息。您可以按照本节所述或在添加连接器时定义存储区域控制器。

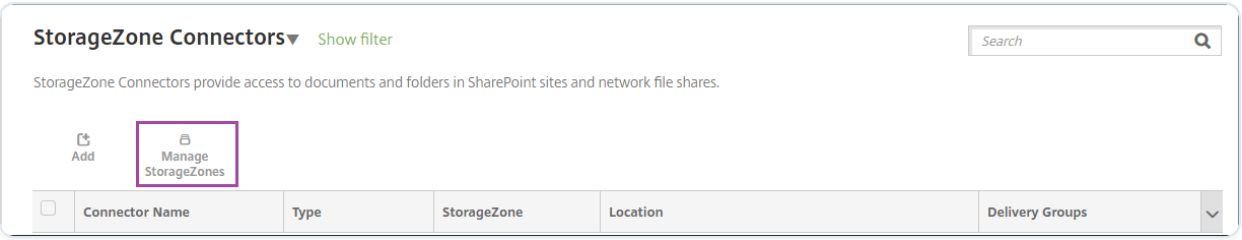
首次访问“**配置 > ShareFile**”页面时，该页面会总结将 XenMobile 用于企业帐户和存储区域连接器之间的差异。



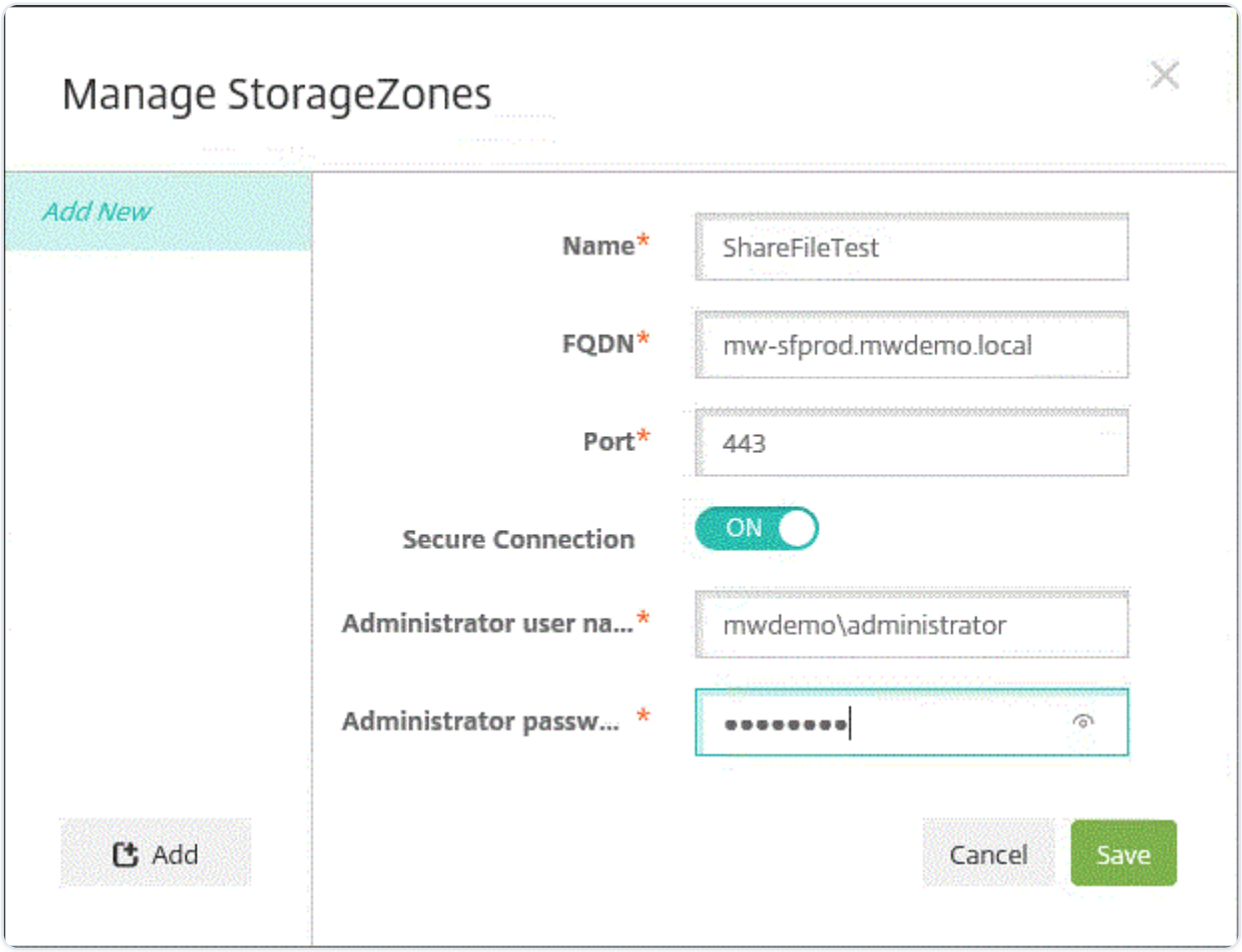
单击“**配置连接器**”以继续本文中的配置步骤。



1. 在“**配置 > ShareFile**”中，单击“**管理存储区域**”。



2. 在“**管理存储区域**”中，添加连接信息。



- **名称：** StorageZone 的描述性名称，用于在 XenMobile 中标识 StorageZone。名称中不要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：** 如果您使用 SSL 连接到存储区域控制器，请使用默认设置“开”。如果您不使用 SSL 连接，请将此设置更改为“关”。

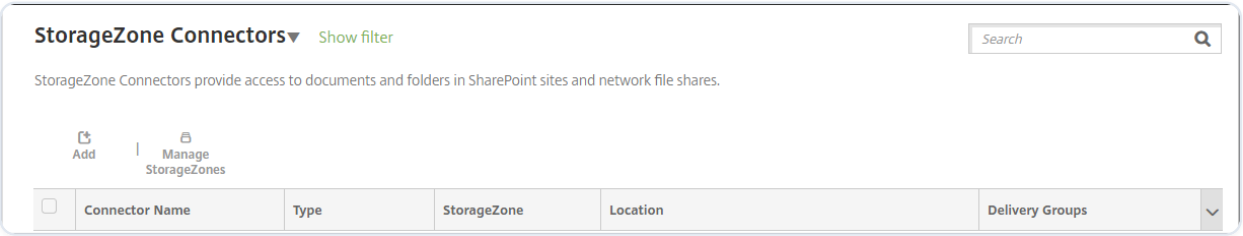
- **管理员用户名** 和 **管理员密码：** 管理员服务帐户用户名（格式为 domain\\admin）和密码。或者，具有存储区域控制器读写权限的用户帐户。

3. 单击 **保存**。
4. 要测试连接，请验证 XenMobile Server 是否可以通过端口 443 访问存储区域控制器的完全限定域名。
5. 要定义另一个存储区域控制器连接，请单击“**管理存储区域**”中的“**添加**”按钮。

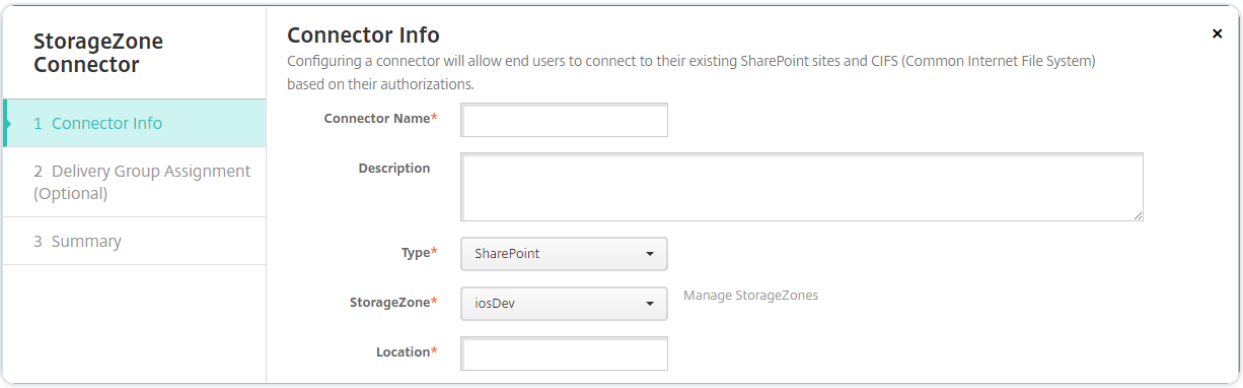
   要编辑或删除存储区域控制器连接的信息，请在“**管理存储区域**”中选择连接名称。然后，单击“**编辑**”或“**删除**”。

在 XenMobile 中添加存储区域连接器

1. 转到 **配置 > ShareFile**，然后单击 **添加**。

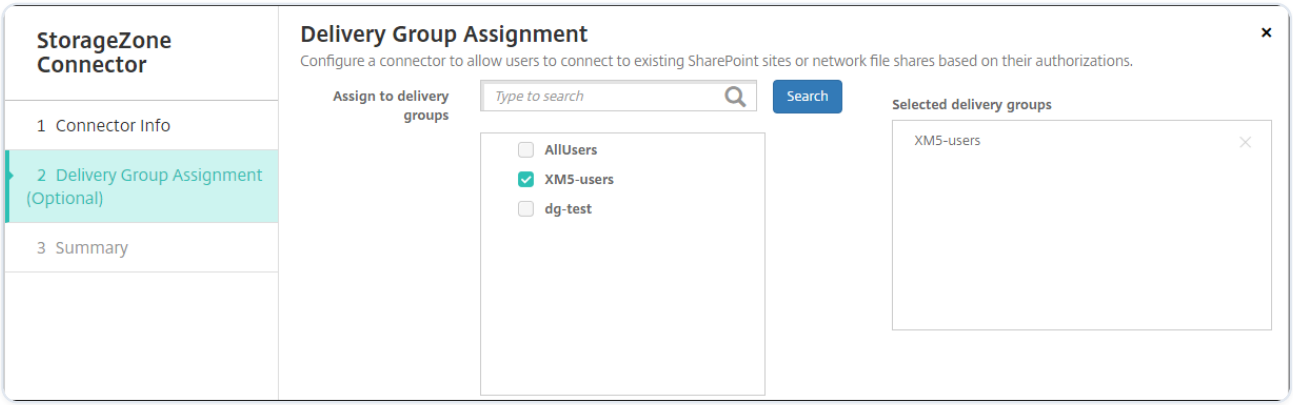


2. 在“**连接器信息**”页面上，配置以下设置：



- **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**。
- **存储区域**：选择与连接器关联的存储区域。如果未列出存储区域，请单击 **管理存储区域** 以定义存储区域控制器。
- **位置**：对于 SharePoint，请指定 SharePoint 根级别站点、站点集或文档库的 URL，格式为 `https://sharepoint.company.com`。对于网络共享，请指定统一命名约定 (UNC) 路径的完全限定域名，格式为 \\\\server\\share。

3. 在 **交付组分配** 页面上，可选地将连接器分配给交付组。或者，您可以使用 **配置 > 交付组** 将连接器与交付组关联。



1. 在 **摘要** 页面上，您可以查看您配置的选项。要调整配置，请单击 **返回**。
2. 单击 **保存** 以保存连接器。
3. 测试连接器：

   a. 封装 Citrix Files 客户端时，请执行以下操作：

      - 将网络访问策略设置为 **隧道连接到内部网络**。

      在此操作模式下，XenMobile MDX 框架会拦截来自 Citrix Files 客户端的所有网络流量。流量通过使用特定于应用程序的微型 VPN 经由 Citrix Gateway 重定向。

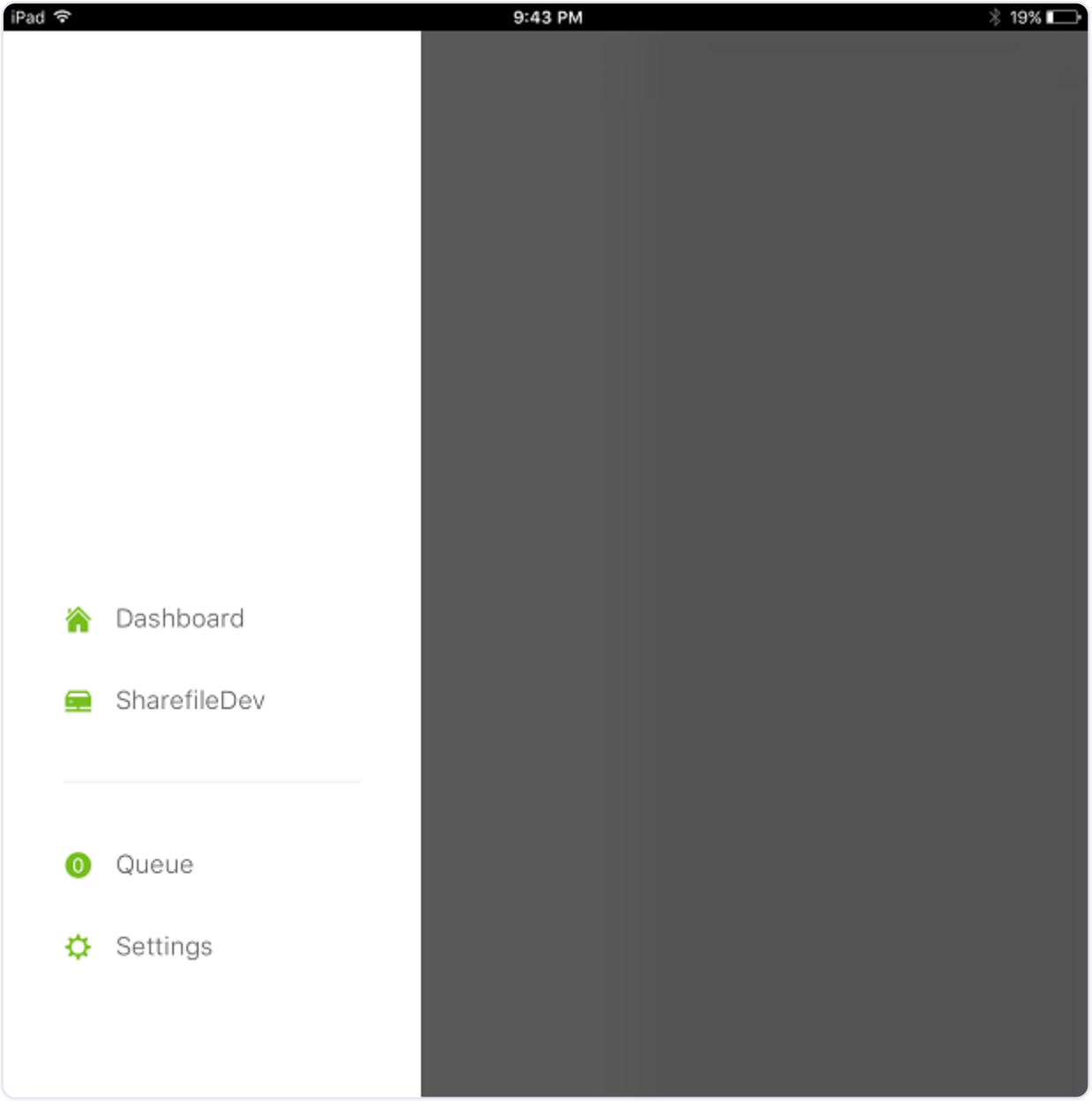
      - 将首选 VPN 模式策略设置为 **隧道连接 - Web SSO**。

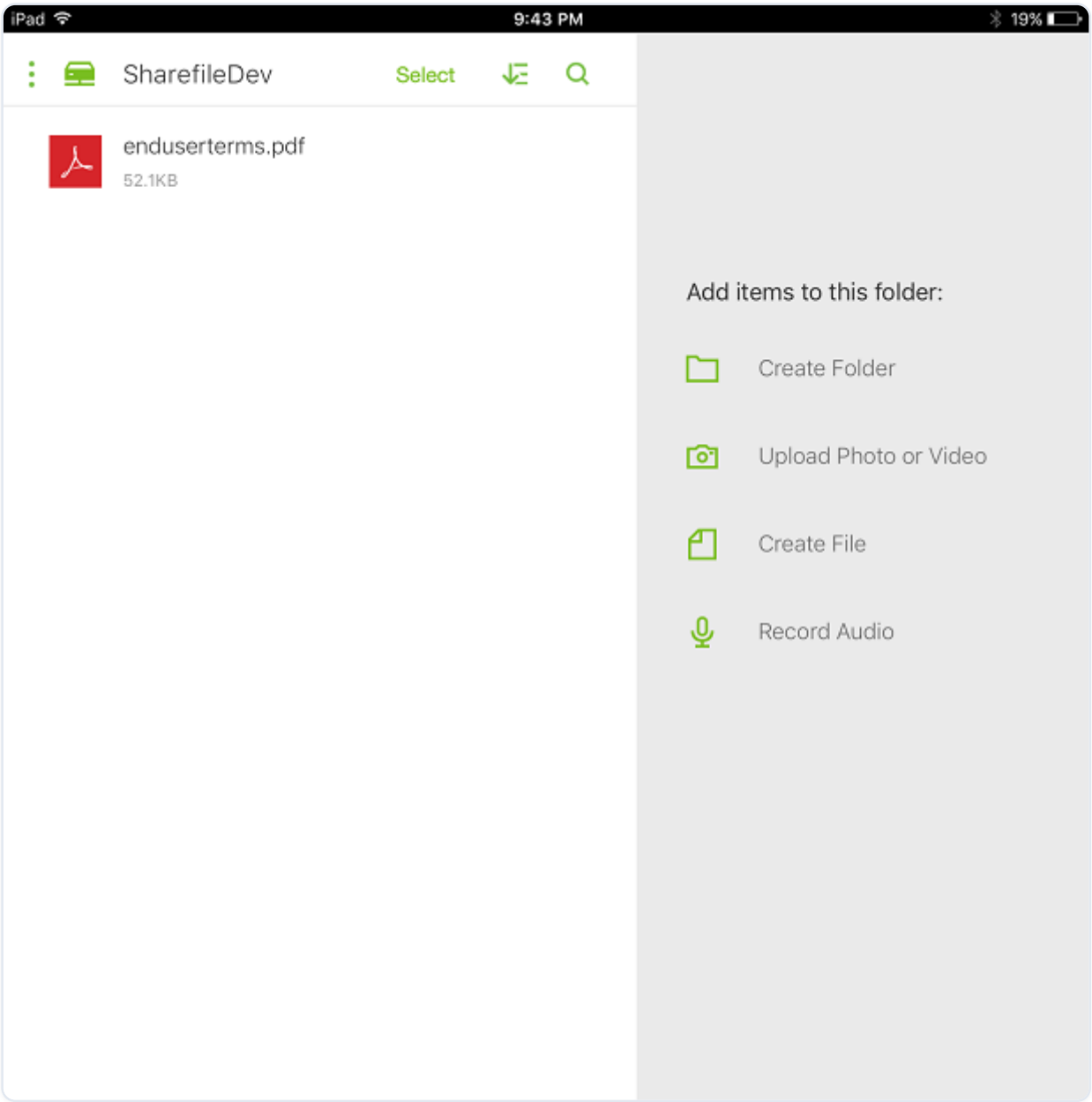
      在此隧道连接模式下，MDX 框架会终止来自 MDX 应用程序的 SSL/HTTP 流量。然后，MDX 代表用户启动到内部连接的新连接。此策略设置使 MDX 框架能够检测并响应 Web 服务器发出的身份验证质询。

   b. 将 Citrix Files 客户端添加到 XenMobile。有关详细信息，请参阅 集成和交付适用于 Endpoint Management 客户端的 Citrix Files。

   c. 从受支持的设备，验证 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。

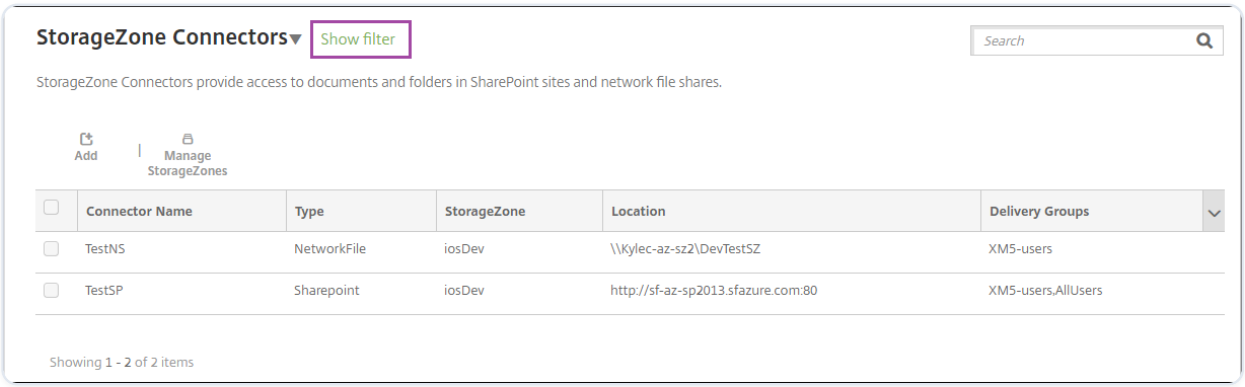

iPad
9:43 PM
19%
Dashboard
SharefileDev
Queue
Settings



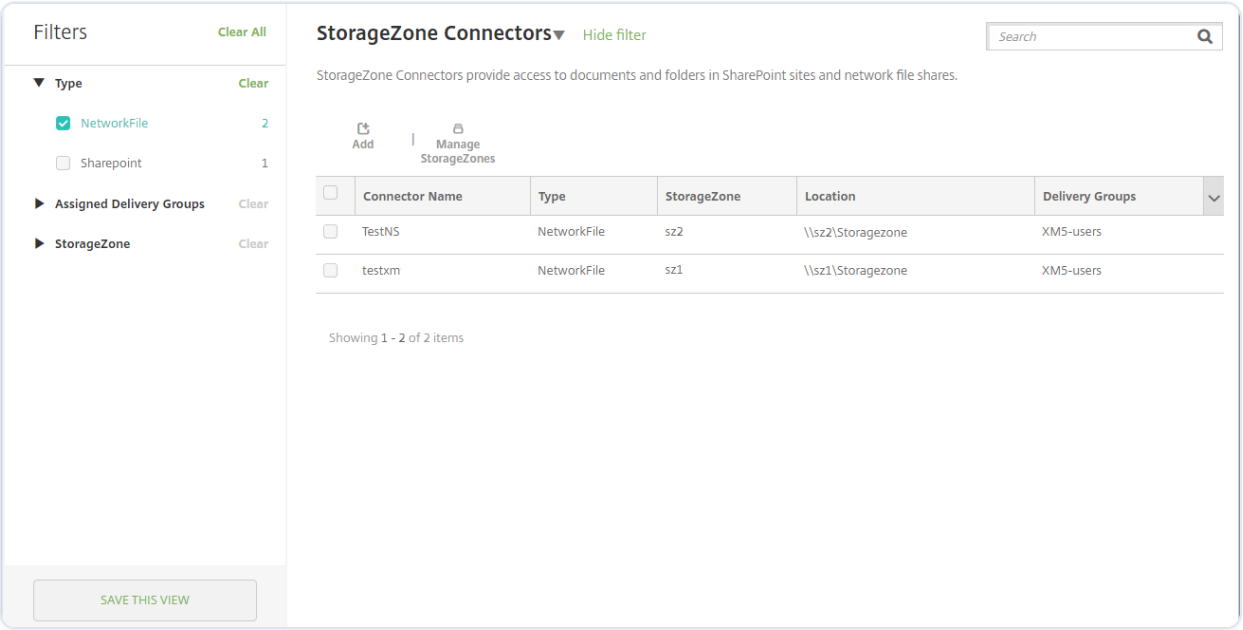
筛选存储区域连接器列表

您可以按连接器类型、分配的交付组和存储区域筛选存储区域连接器列表。

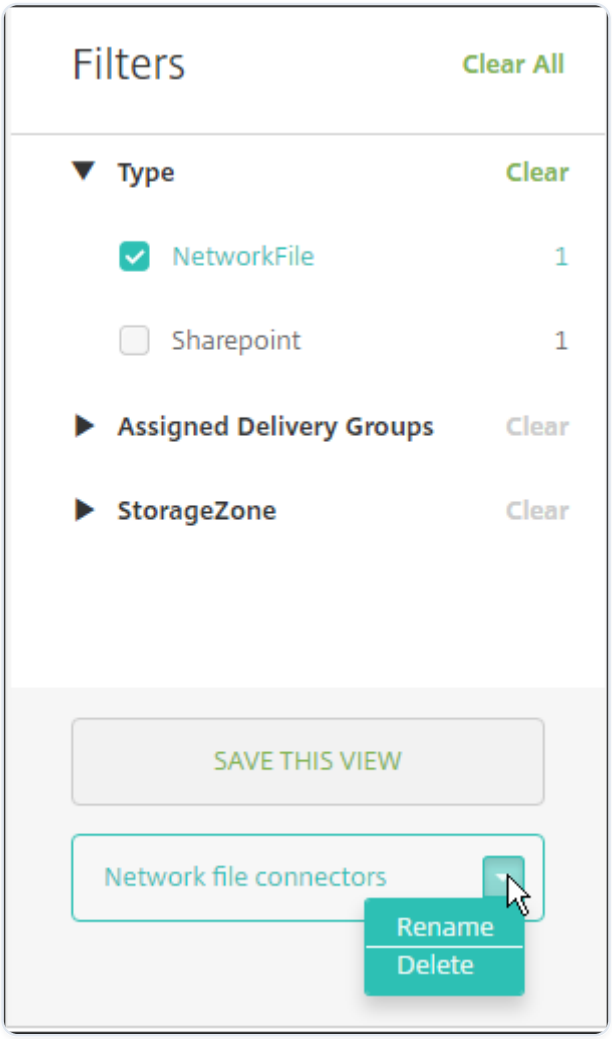
1. 转到 **Configure > ShareFile**，然后单击 **Show filter**。



2. 展开筛选器标题以进行选择。要保存筛选器，请单击 **Save This View**，键入筛选器名称，然后单击 **Save**。



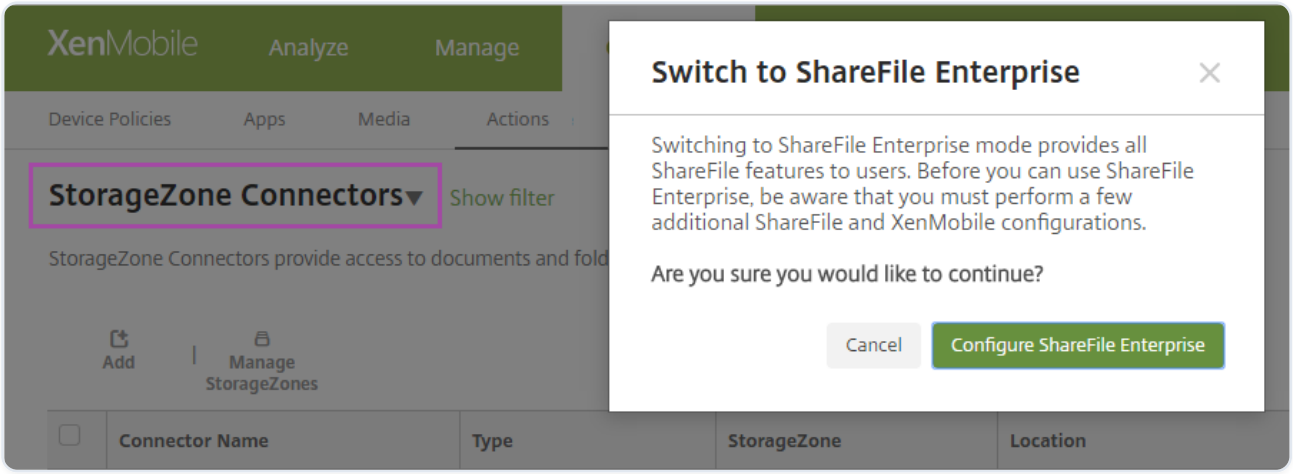
3. 要重命名或删除筛选器，请单击筛选器名称旁边的箭头图标。



切换到 Citrix Files

将存储区域连接器与 XenMobile 集成后，您可以稍后切换到完整的 Enterprise 功能集。使用 Citrix Files 功能集需要 XenMobile Advanced Edition（本地）或 Citrix Endpoint Management（云）。XenMobile 会保留您现有的存储区域连接器集成设置。

转到 **Configure > ShareFile**，单击 **StorageZone Connectors** 下拉菜单，然后单击 **Configure ShareFile Enterprise**。



有关配置 Citrix Files 的信息，请参阅使用 Citrix Files 进行单点登录的 SAML。

适用于 HDX™ 应用程序的 SmartAccess

此功能允许您根据设备属性、设备的用户属性或设备上安装的应用程序来控制对 HDX 应用程序的访问。您可以通过设置自动化操作来使用此功能，将设备标记为不合规，从而拒绝该设备访问。与此功能一起使用的 HDX 应用程序在 Virtual Apps and Desktops 中配置，方法是使用 SmartAccess 策略拒绝不合规设备的访问。XenMobile 使用签名加密标签将设备状态传达给 StoreFront™。StoreFront 然后根据应用程序的访问控制策略允许或拒绝访问。

要使用此功能，您的部署需要：

- 虚拟应用和桌面 7.6
- StoreFront 3.7 或 3.8
- 配置为聚合来自 StoreFront 服务器的 HDX 应用程序的 XenMobile® Server
- 配置了 SAML 证书的 XenMobile Server，用于签名和加密标签。不带私钥的相同证书将上传到 StoreFront 服务器。

要开始使用此功能：

- 将 XenMobile Server 证书配置到 StoreFront 存储
- 配置至少一个具有所需 SmartAccess 策略的 Virtual Apps and Desktops 交付组

- 在 XenMobile 中设置自动化操作

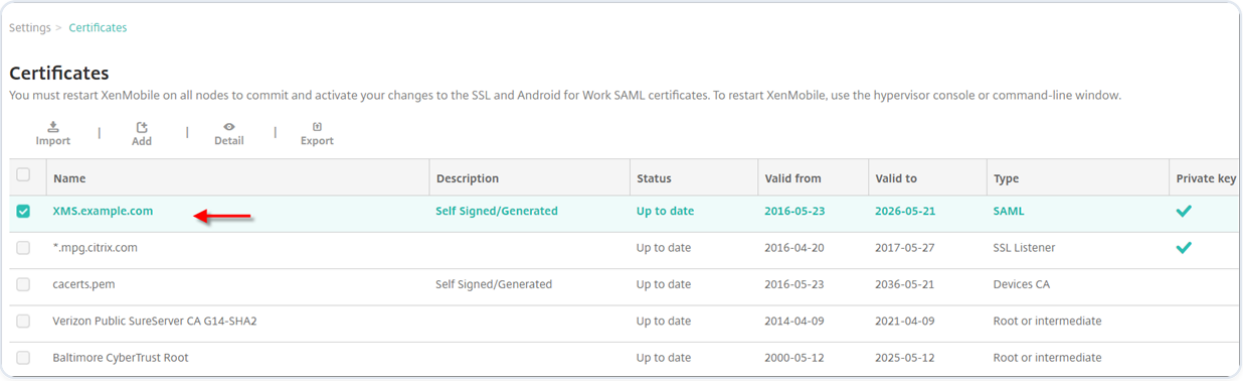
导出并配置 XenMobile Server 证书，并将其上传到 StoreFront 存储

SmartAccess 使用签名和加密标签在 XenMobile 和 StoreFront 服务器之间进行通信。为启用该通信，您需要将 XenMobile Server 证书添加到 StoreFront 存储。

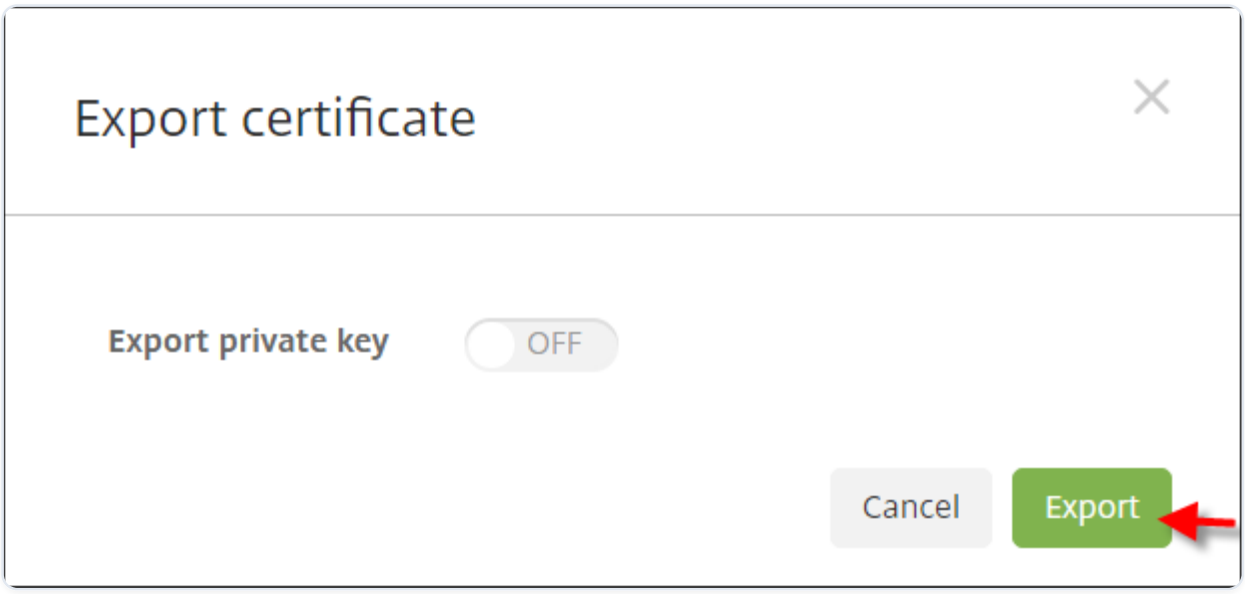
有关在 XenMobile 启用域和基于证书的身份验证时集成 StoreFront 和 XenMobile 的更多信息，请参阅 支持知识中心。

从 XenMobile Server 导出 SAML 证书

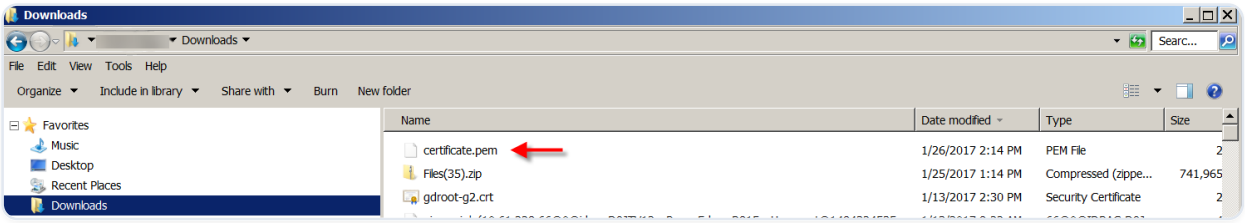
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示“**设置**”页面。单击“**证书**”。
2. 找到 XenMobile Server 的 SAML 证书。



3. 确保“**导出私钥**”设置为“**关**”。单击“**导出**”将证书导出到下载目录。

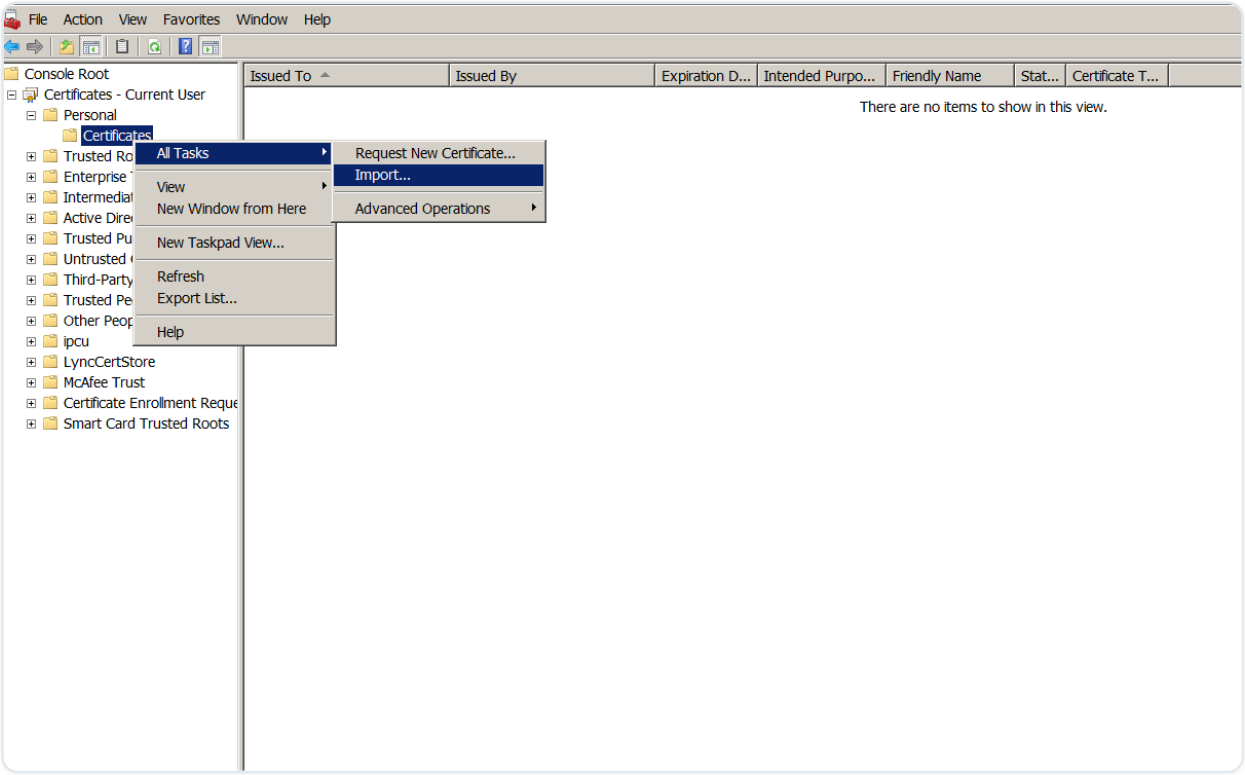


4. 在下载目录中找到该证书。该证书采用 PEM 格式。



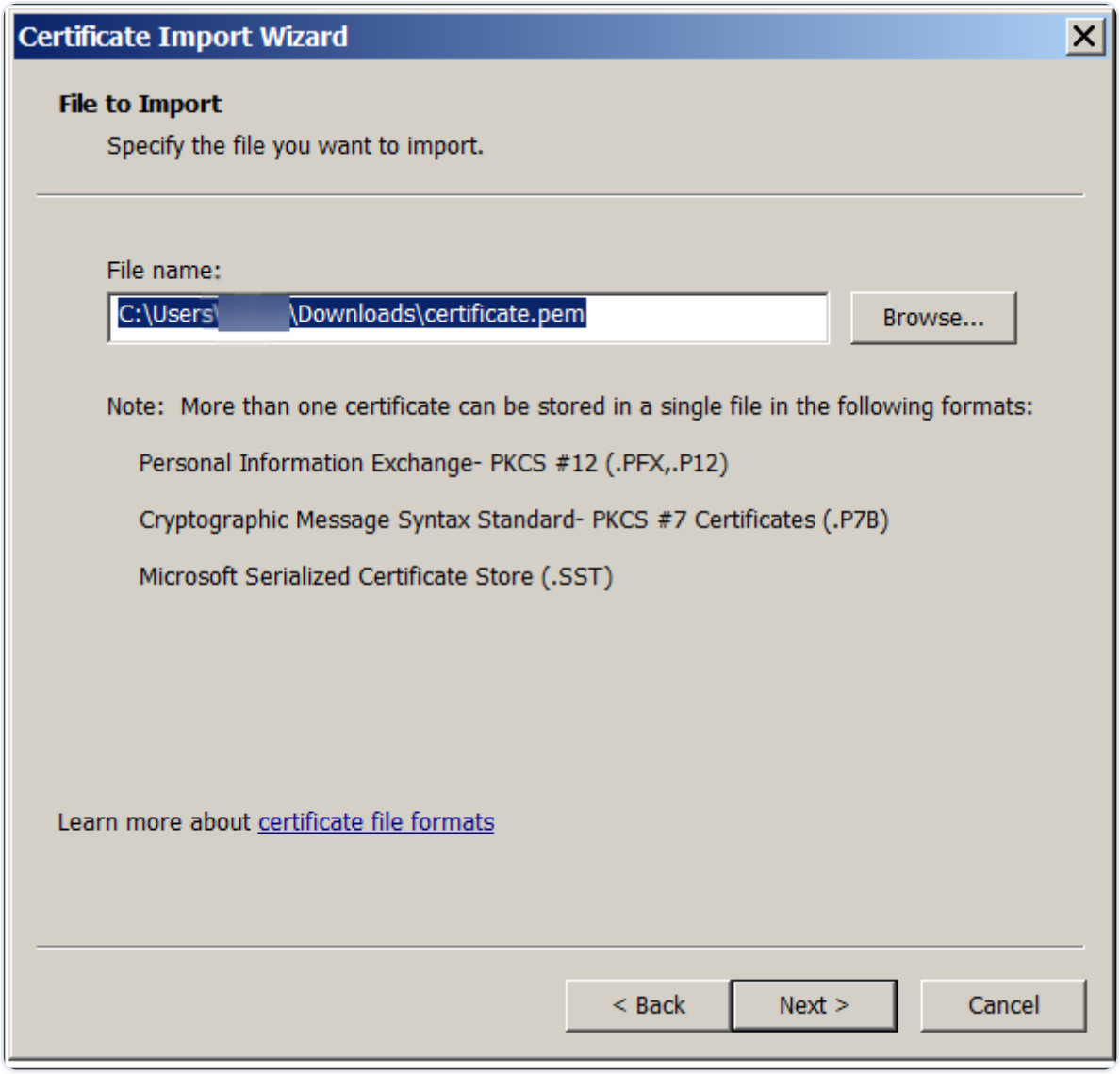
将证书从 PEM 格式转换为 CER 格式

1. 打开 Microsoft 管理控制台 (MMC) 并右键单击“**证书 > 所有任务 > 导入**”。

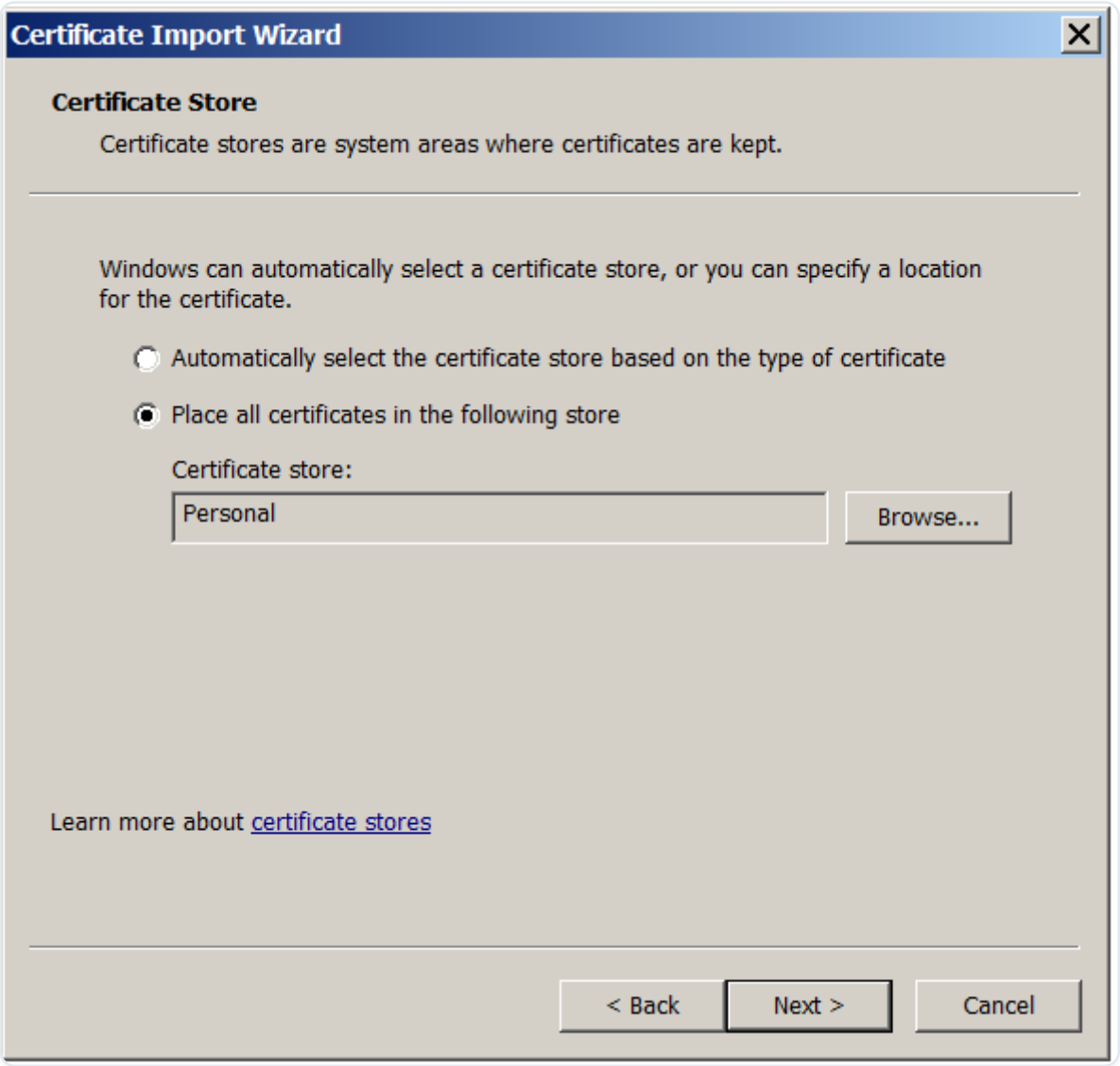


2. 证书导入向导出现后，单击“**下一步**”。

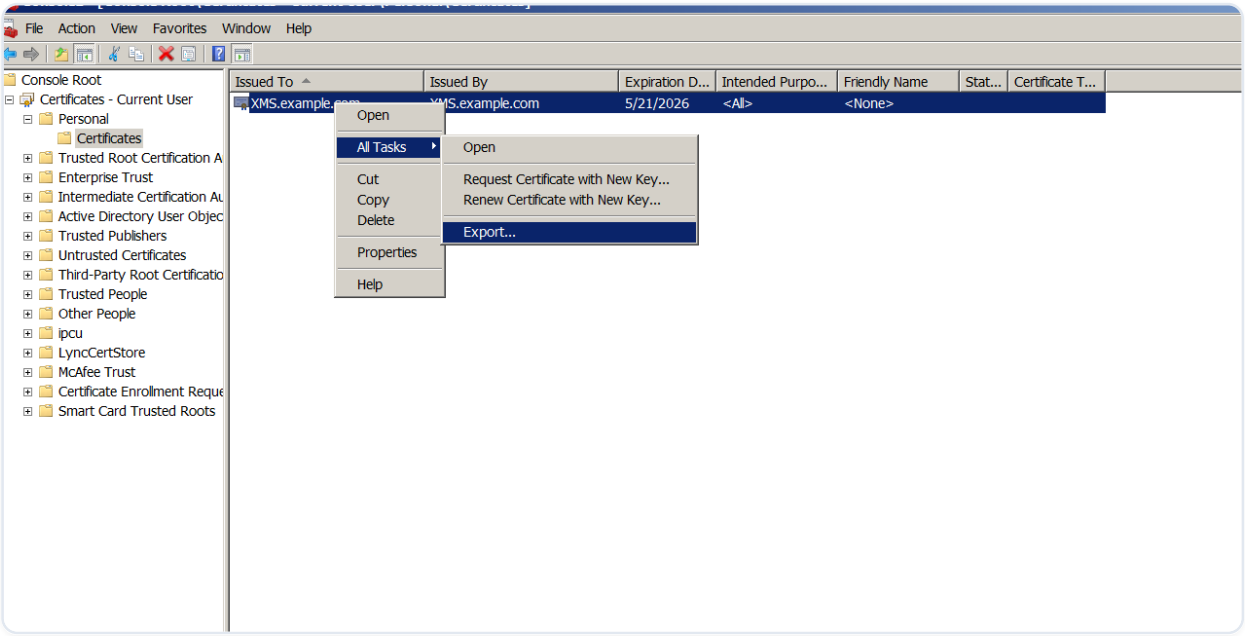
3. 浏览到下载目录中的证书。



4. 选择“**将所有证书放入以下存储**”并选择“**个人**”作为证书存储。单击“**下一步**”。

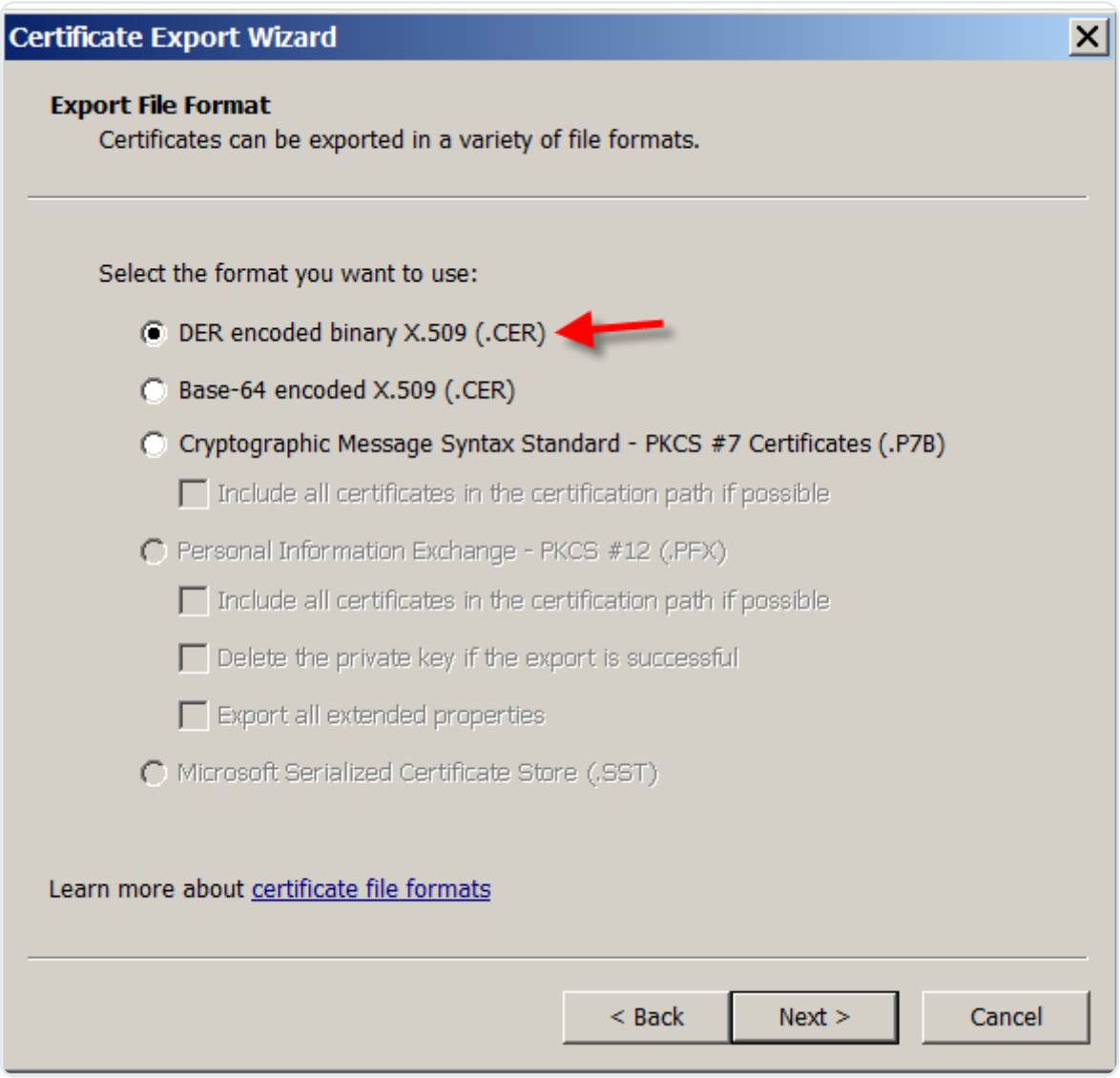


5. 查看您的选择，然后单击“**完成**”。单击“**确定**”关闭确认窗口。
6. 在 MMC 中，右键单击证书，然后选择“**所有任务 > 导出**”。

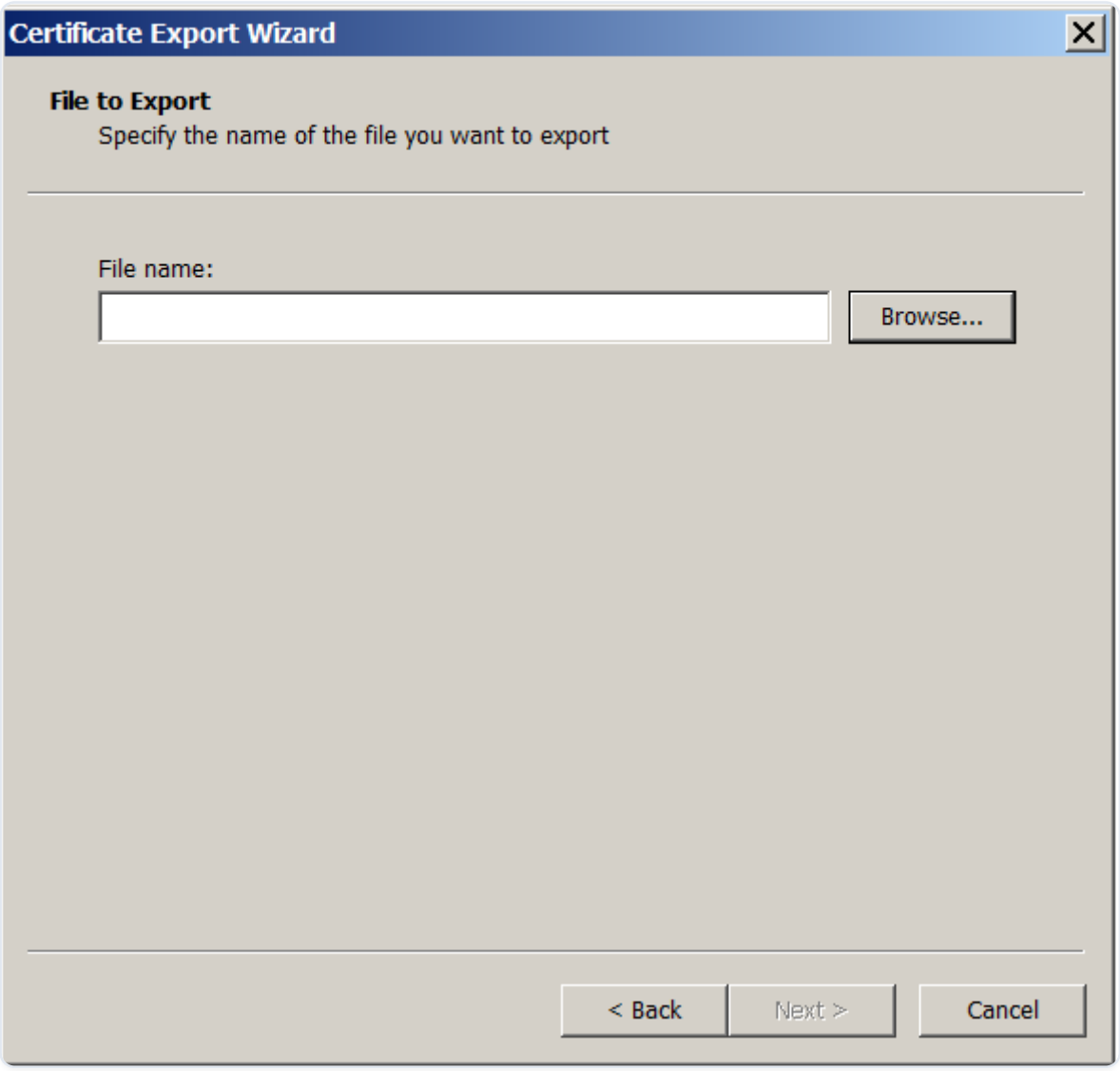


7. 当证书导出向导出现时，单击“**下一步**”。

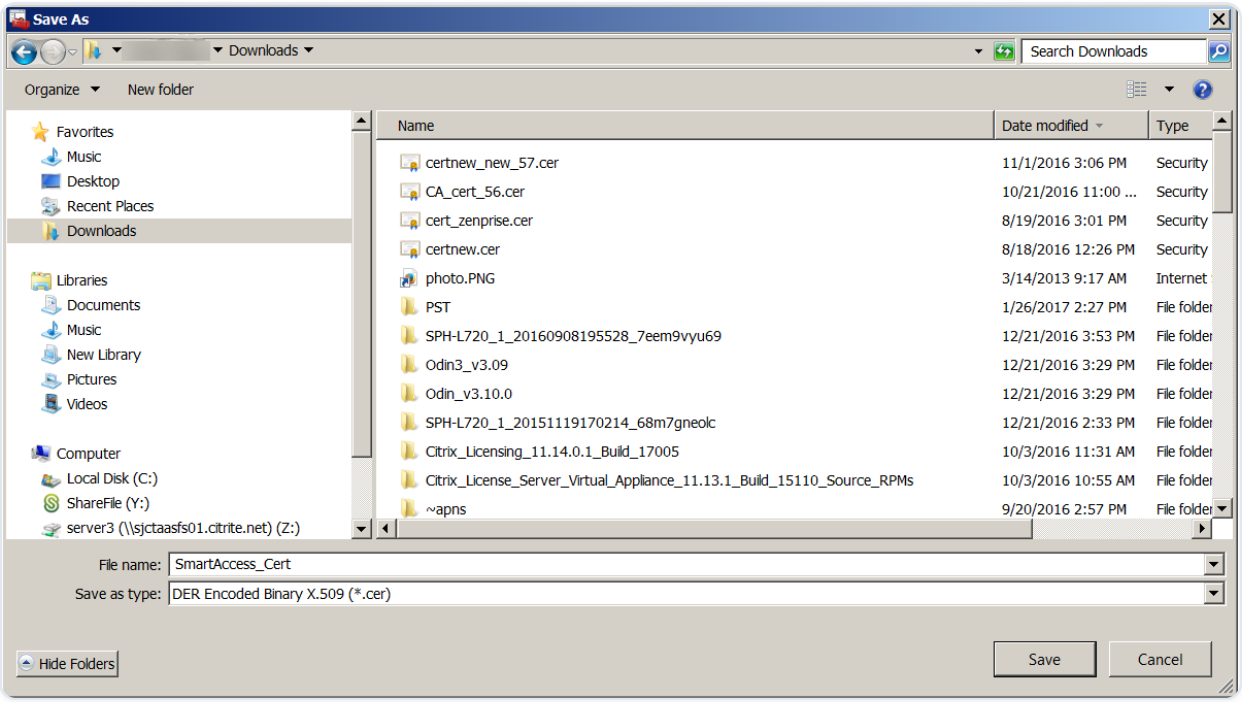
8. 选择格式“**DER 编码二进制 X.509 (.CER)**”。单击“**下一步**”。



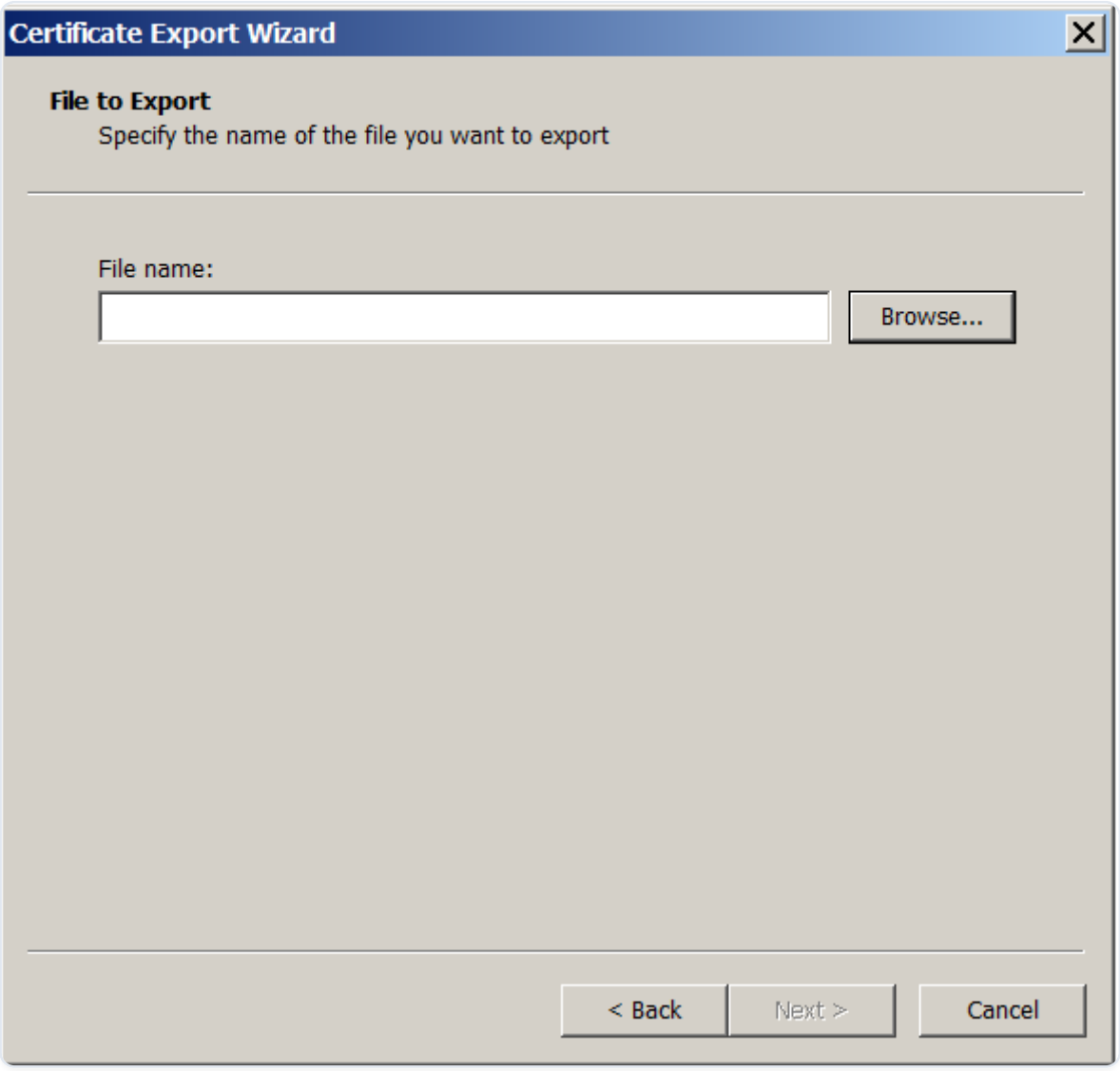
9. 浏览到证书。键入证书名称，然后单击“**下一步**”。


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
< Back
Next >
Cancel

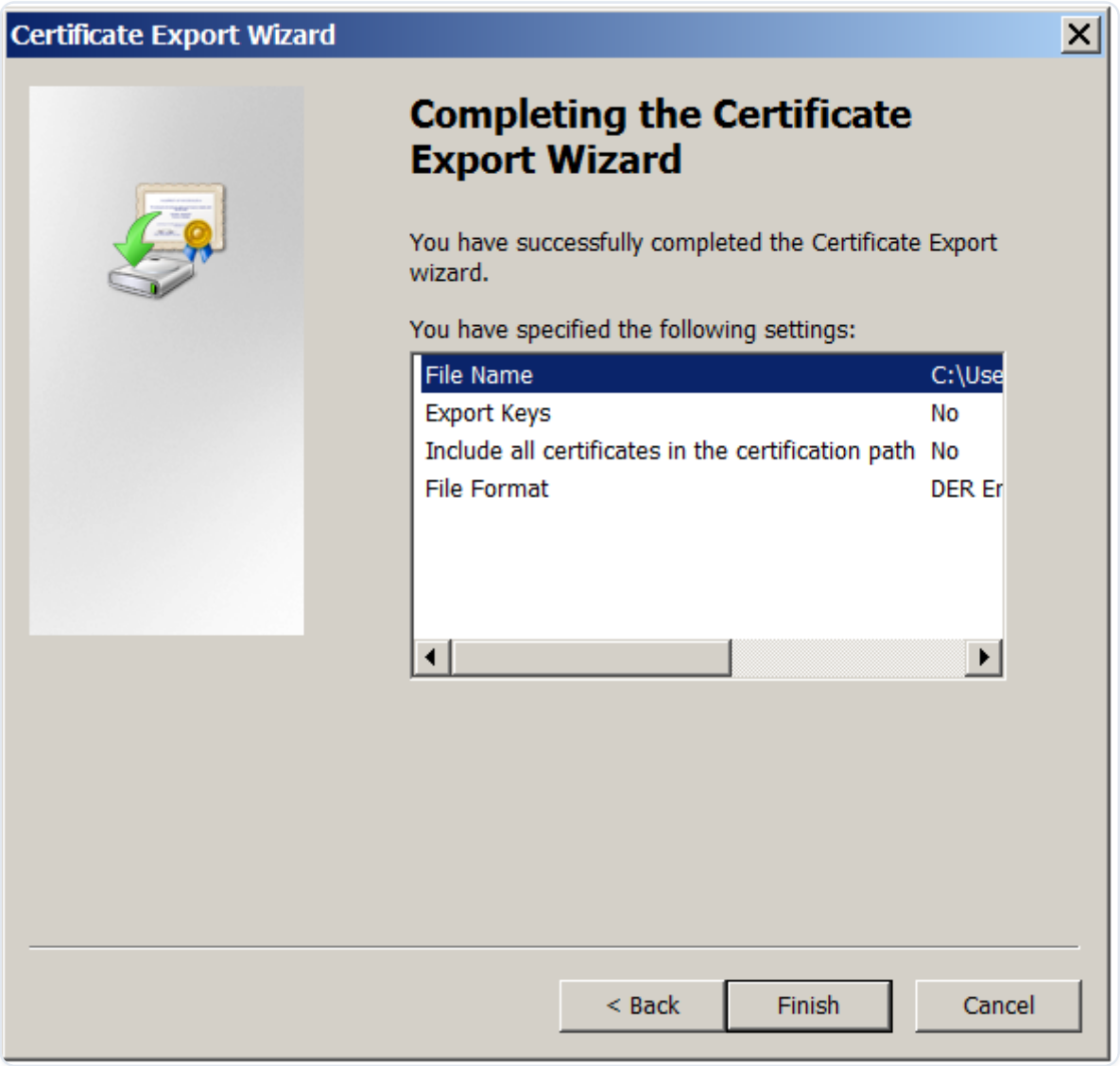
10. 保存证书。


Save As
Downloads
Search Downloads
Organize
New folder
Favorites
Music
Desktop
Recent Places
Downloads
Libraries
Documents
Music
New Library
Pictures
Videos
Computer
Local Disk (C:)
ShareFile (Y:)
server3 (\\sjctaasfs01.citrite.net) (Z:)
Name
Date modified
Type
certnew_new_57.cer
CA_cert_56.cer
cert_zenprise.cer
certnew.cer
photo.PNG
PST
SPH-L720_1_20160908195528_7eem9vyu69
Odin3_v3.09
Odin_v3.10.0
SPH-L720_1_20151119170214_68m7gneolc
Citrix_Licensing_11.14.0.1_Build_17005
Citrix_License_Server_Virtual_Appliance_11.13.1_Build_15110_Source_RPMs
~apns
File name:
SmartAccess_Cert
Save as type:
DER Encoded Binary X.509 (*.cer)
Hide Folders
Save
Cancel

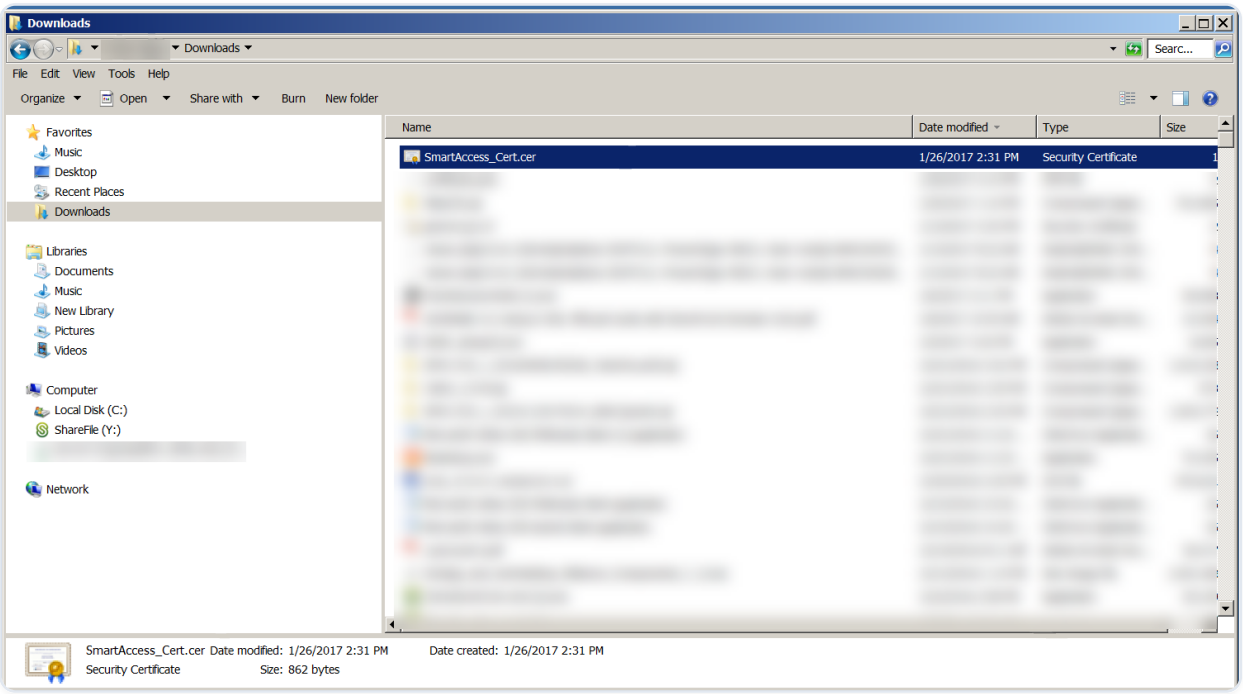
11. 浏览到证书，然后单击“**下一步**”。



12. 查看您的选择，然后单击“**完成**”。单击“**确定**”关闭确认窗口。

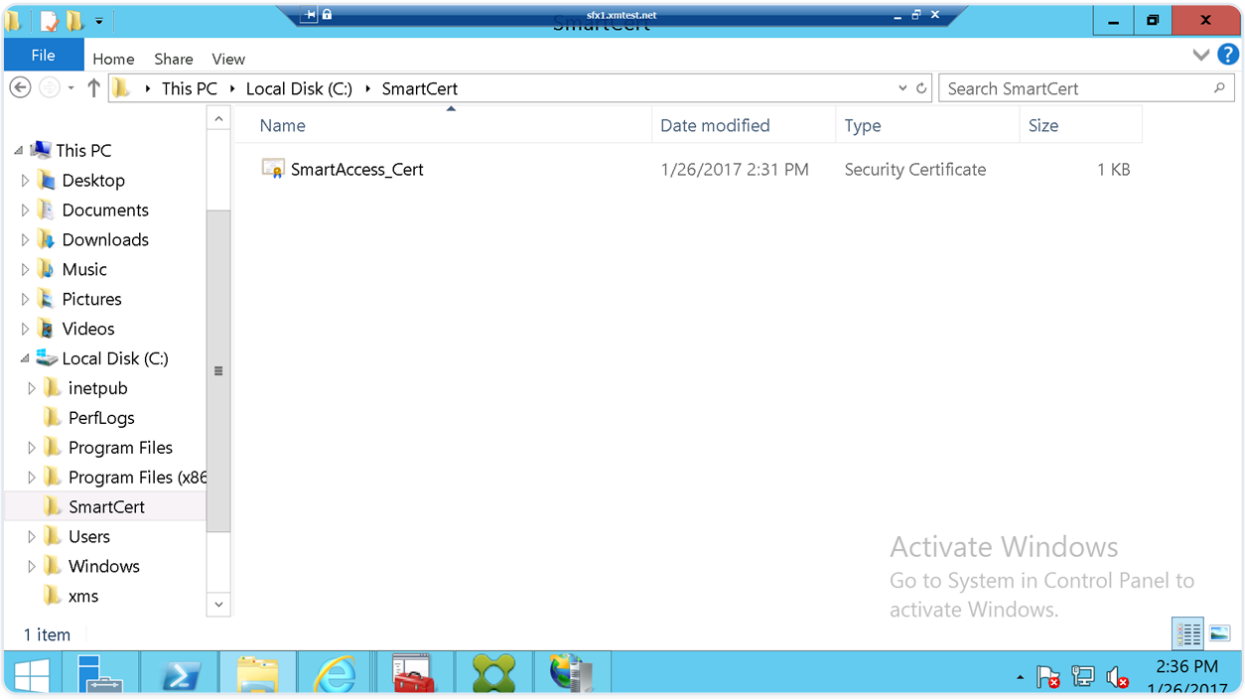


13. 在下载目录中找到证书。该证书采用 CER 格式。



将证书复制到 StoreFront 服务器

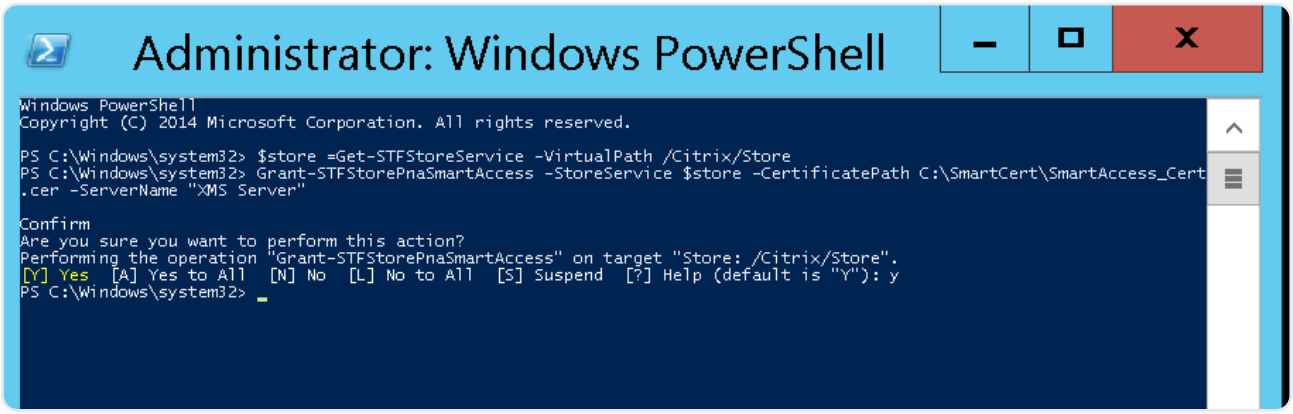
1. 在 StoreFront 服务器上，创建一个名为 **SmartCert** 的文件夹。
2. 将证书复制到 **SmartCert** 文件夹。



在 StoreFront 存储上配置证书

在 StoreFront 服务器上，运行此 PowerShell 命令以在存储上配置转换后的 XenMobile Server 证书：

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath  “C:\xms\xms.cer” –ServerName “XMS server”
```



如果 StoreFront 存储上存在任何现有证书，请运行此 PowerShell 命令将其吊销：

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```

或者，您可以在 StoreFront 服务器上运行以下任何 PowerShell 命令来吊销 StoreFront 存储上的现有证书：

- 按名称吊销：

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store



Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server"
```

- 按指纹吊销：

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store



Revoke-STFStorePnaSmartAccess –StoreService $store –CertificateThumbprint “ReplaceWithThumbprint”
```

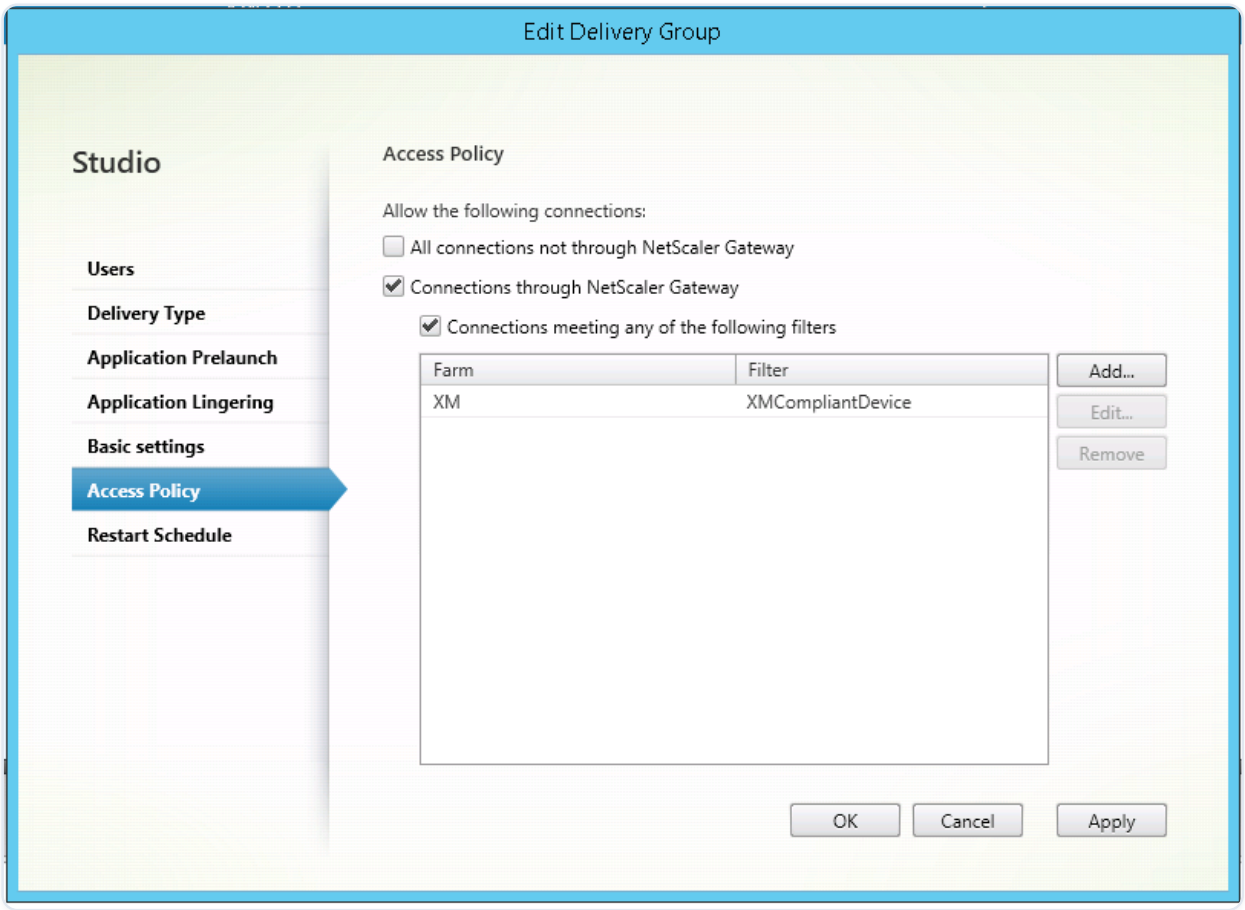
- 按服务器对象吊销：

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store



$access = Get-STFStorePnaSmartAccess –StoreService $store



Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess $access.AccessConditionsTrusts[0]
```

为 Virtual Apps and Desktops 配置 SmartAccess 策略

要将所需的 SmartAccess 策略添加到交付 HDX 应用程序的交付组，请执行以下操作：

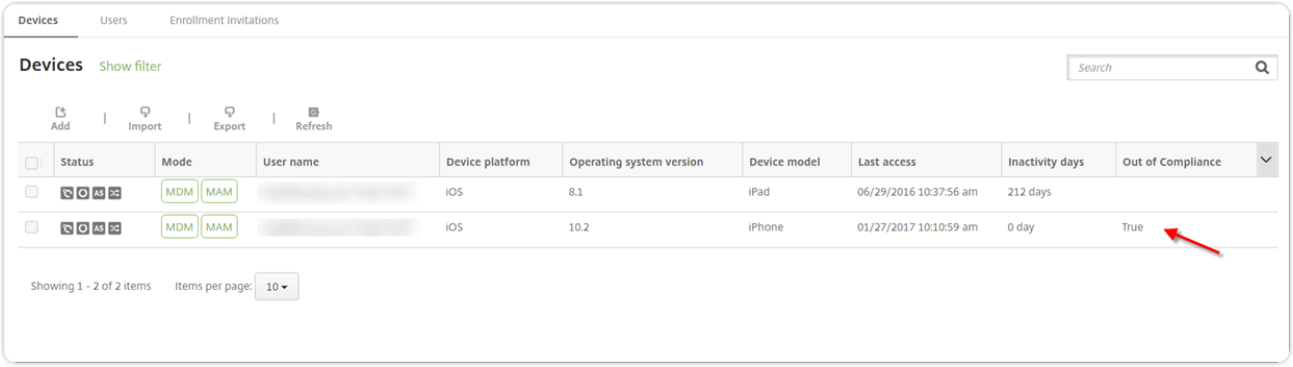
1. 在 Virtual Apps and Desktops 服务器上，打开 Citrix Studio。
2. 在 Studio 导航窗格中选择 **交付组**。
3. 选择一个交付您要控制访问的应用程序的组。然后在**操作**窗格中选择**编辑交付组**。
4. 在**访问策略**页面上，选择**通过 NetScaler® Gateway 的连接**和**满足以下任一条件的连接**。
5. 单击**添加**。
6. 添加访问策略，其中 **Farm** 为 **XM**，**Filter** 为 **XMCompliantDevice**。



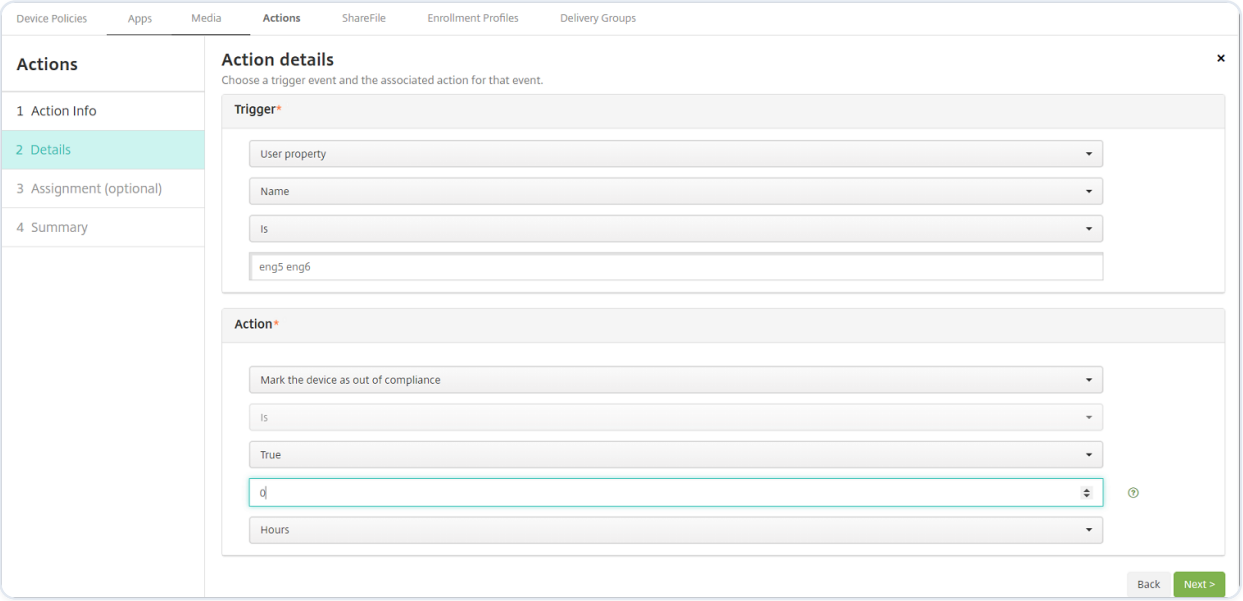
7. 单击**应用**以应用所做的任何更改并保持窗口打开，或者单击**确定**以应用更改并关闭窗口。

在 XenMobile 中设置自动化操作

当设备不合规时，您为 HDX 应用程序在交付组中设置的 SmartAccess 策略会拒绝设备访问。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. 点击“**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. 点击“**下一步**”。此时将显示“**操作详细信息**”页面。在以下示例中，如果设备具有用户属性名称 **eng5** 或 **eng6**，则会创建一个触发器，该触发器会立即将设备标记为不合规。



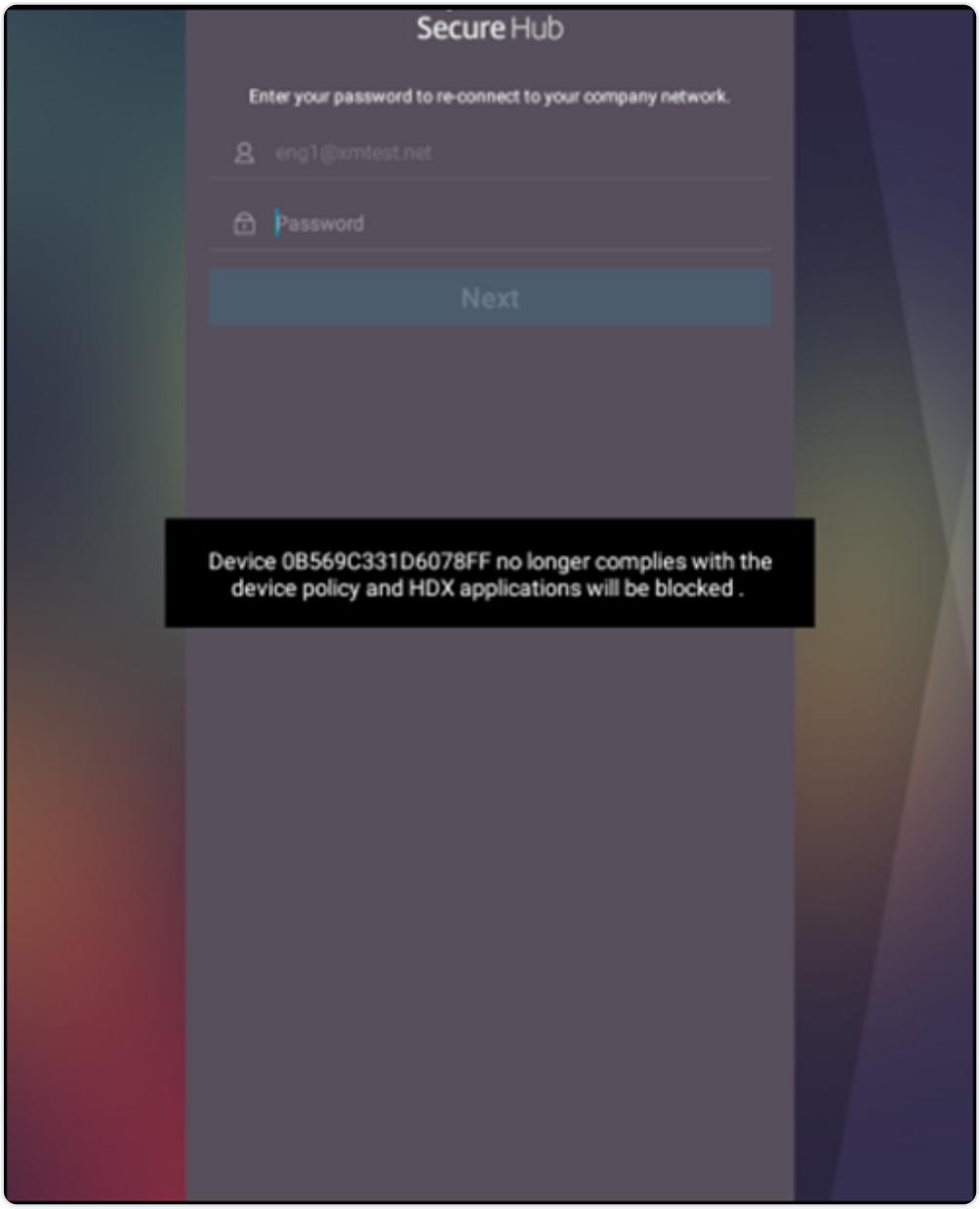
5. 在“**触发器**”列表中，选择“**设备属性**”、“**用户属性**”或“**已安装的应用程序名称**”。SmartAccess 不支持事件触发器。
6. 在“**操作**”列表中：
   - 选择“**将设备标记为不合规。**”.
   - 选择“**是**”。
   - 选择“**真**”。
   - 要将操作设置为在满足触发器条件时立即将设备标记为不合规，请将时间范围设置为 **0**。
7. 选择要应用此操作的 XenMobile 交付组。
8. 查看操作摘要。

9. 点击“**下一步**”，然后点击“**保存**”。

当设备被标记为不合规时，HDX 应用程序将不再显示在 Secure Hub 商店中。用户将不再订阅该应用程序。设备不会收到通知，Secure Hub 商店中也没有任何内容表明 HDX 应用程序以前可用。

如果您希望在设备被标记为不合规时通知用户，请创建通知，然后创建自动化操作以发送该通知。

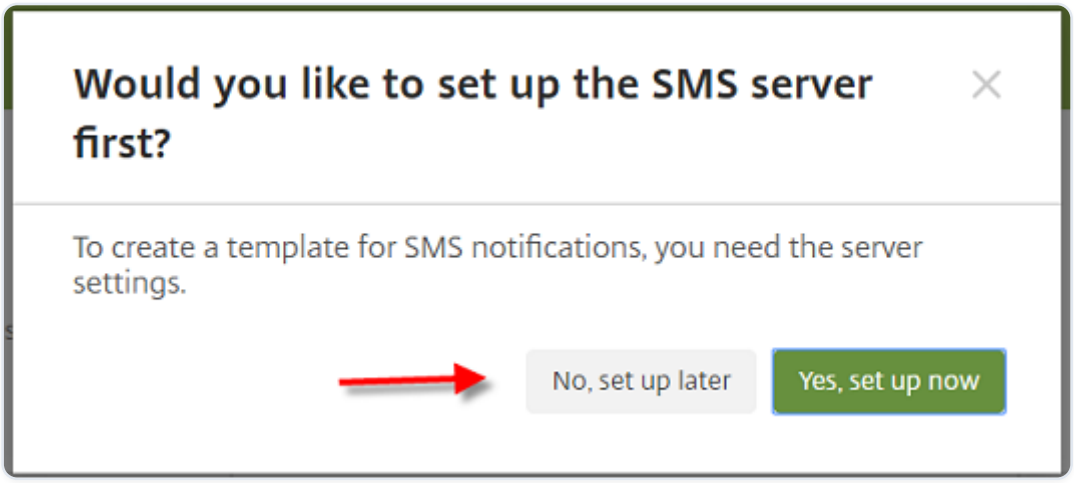
此示例在设备被标记为不合规时创建并发送此通知：“设备序列号或电话号码不再符合设备策略，并且 HDX 应用程序已被阻止。”



创建设备被标记为不合规时用户看到的通知

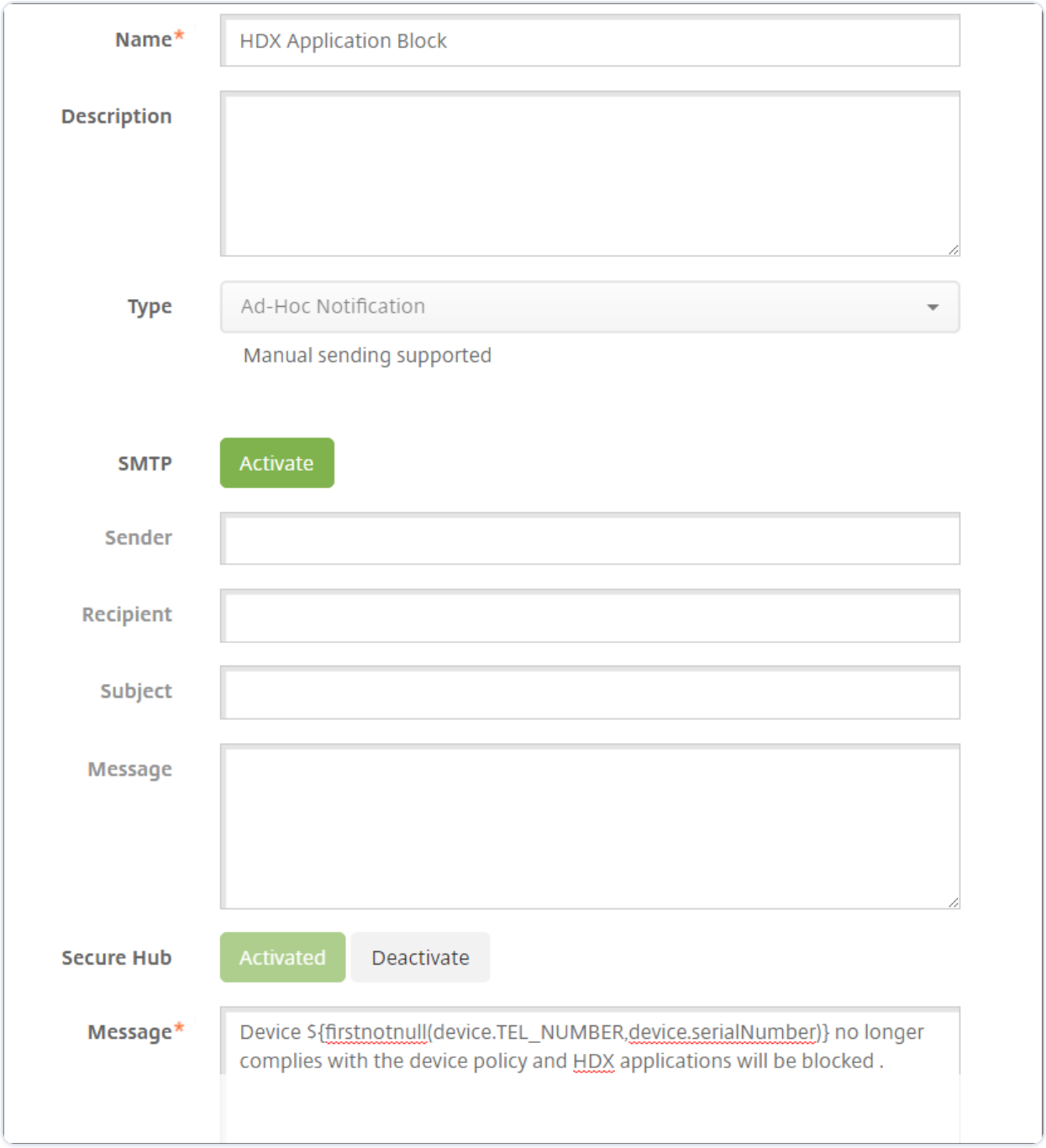
1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示**设置**页面。
2. 单击**通知模板**。此时将显示**通知模板**页面。

3. 在**通知模板**页面上，单击**添加**。
4. 当系统提示您首先设置 SMS 服务器时，单击**否，稍后设置**。



5. 配置以下设置：

- **名称：**HDX 应用程序阻止
- **描述：**设备不合规时的代理通知
- **类型：**即席通知
- **Secure Hub：**已激活
- **消息：**设备 ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} 不再符合设备策略，并且 HDX 应用程序已被阻止。

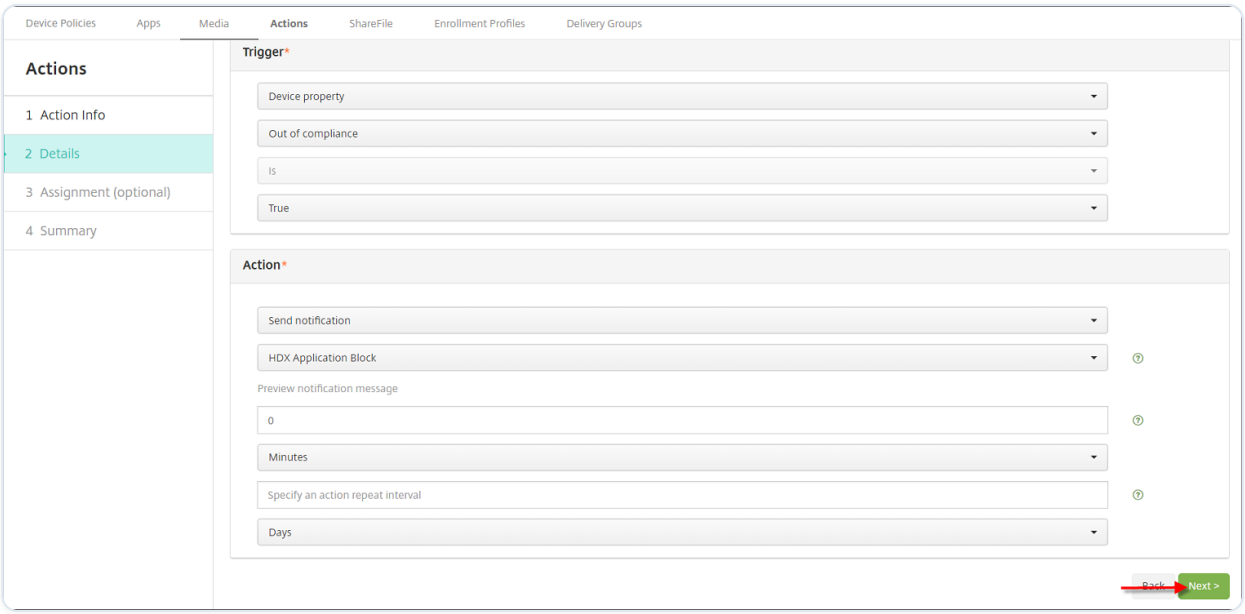


6. 单击**保存**。

创建在设备被标记为不合规时发送通知的操作

1. 在 XenMobile 控制台中，单击**配置 > 操作**。**操作**页面随即显示。
2. 单击**添加**以添加操作。**操作信息**页面随即显示。
3. 在**操作信息**页面上，输入操作的名称和说明：
   - **名称：**HDX 阻止通知
   - **说明：**HDX 阻止通知，因为设备不合规

4. 单击**下一步**。**操作详细信息**页面随即显示。
5. 在**触发器**列表中：
   - 选择**设备属性**。
   - 选择**不合规**。
   - 选择**是**。
   - 选择**真**。



6. 在**操作**列表中，指定满足触发器时执行的操作：
   - 选择 **发送通知**
   - 选择 **HDX 应用程序阻止，您创建的通知**。
   - 选择 **0**。将此值设置为 0 会导致在满足触发条件时发送通知。
7. 选择要应用此操作的 XenMobile 交付组。在此示例中，选择 **AllUsers**。
8. 查看操作摘要。
9. 单击 **下一步**，然后单击 **保存**。

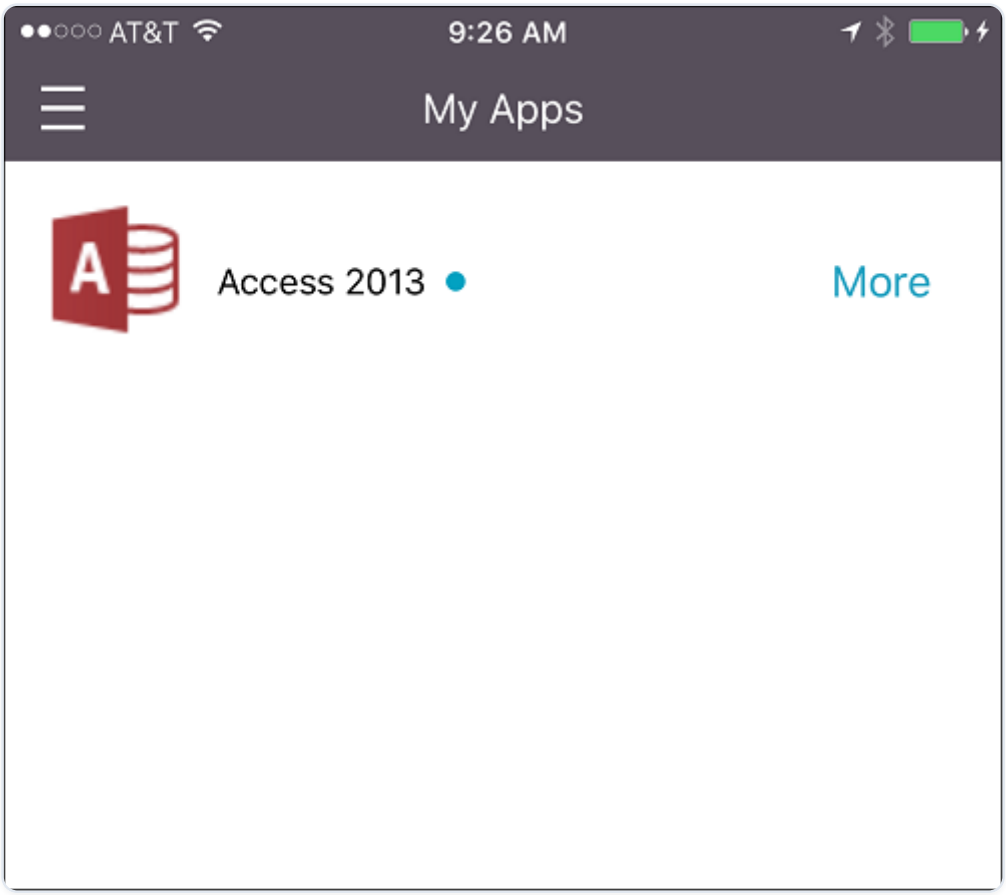
有关设置自动化操作的详细信息，请参阅 自动化操作。

用户如何重新获得对 HDX 应用程序的访问权限

设备恢复合规性后，用户可以再次访问 HDX 应用程序：

1. 在设备上，转到 Secure Hub 商店以刷新商店中的应用程序。
2. 转到应用程序并轻按 **添加** 到应用程序。

添加应用程序后，它会出现在“我的应用程序”中，旁边有一个蓝点，因为它是一个新安装的应用程序。



添加媒体

您将媒体添加到 XenMobile®，以便可以将媒体部署到用户设备。您可以使用 XenMobile 部署通过 Apple 批量采购获得的 Apple Books。

在 XenMobile 中配置批量采购帐户后，您购买的和免费的图书将显示在 **Configure > Media** 中。在 **Media** 页面中，通过选择交付组并指定部署规则来配置要部署到 iOS 设备的图书。

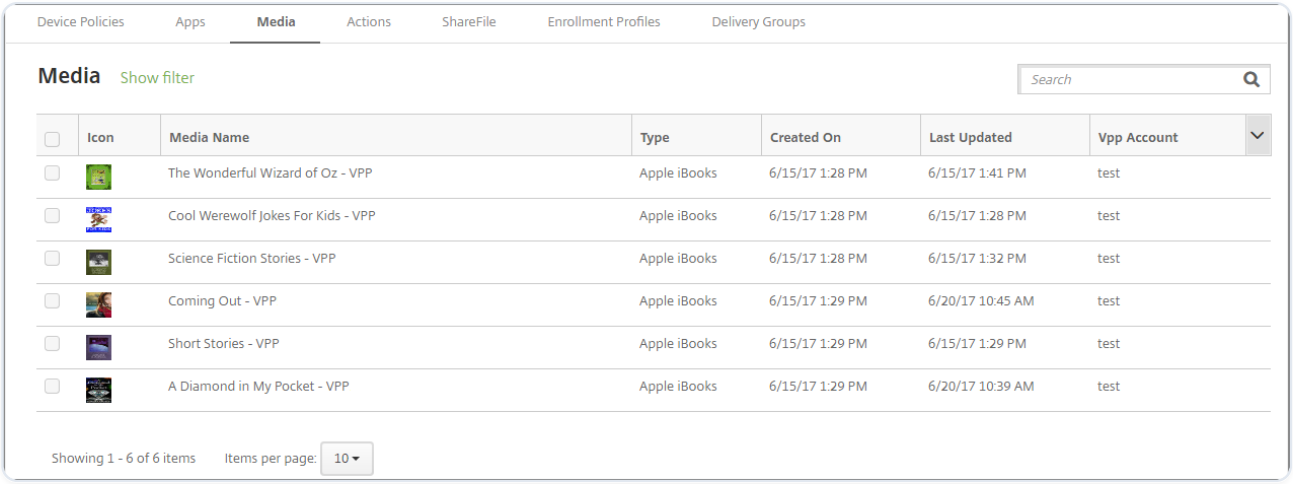
用户首次收到图书并接受批量采购许可证后，部署的图书将安装到设备上。这些图书会显示在 Apple Book 应用中。您无法将图书许可证与用户解除关联，也无法从设备中删除图书。XenMobile 将图书安装为必需媒体。如果用户从其设备中删除已安装的图书，该图书仍会保留在 Apple Book 应用中，可供下载。

必备条件

- iOS 设备
- 在 XenMobile 中配置 Apple 批量采购，如 Apple Volume Purchase 中所述。

配置图书

通过批量采购获得的 Apple Books 将显示在 **Configure > Media** 页面上。

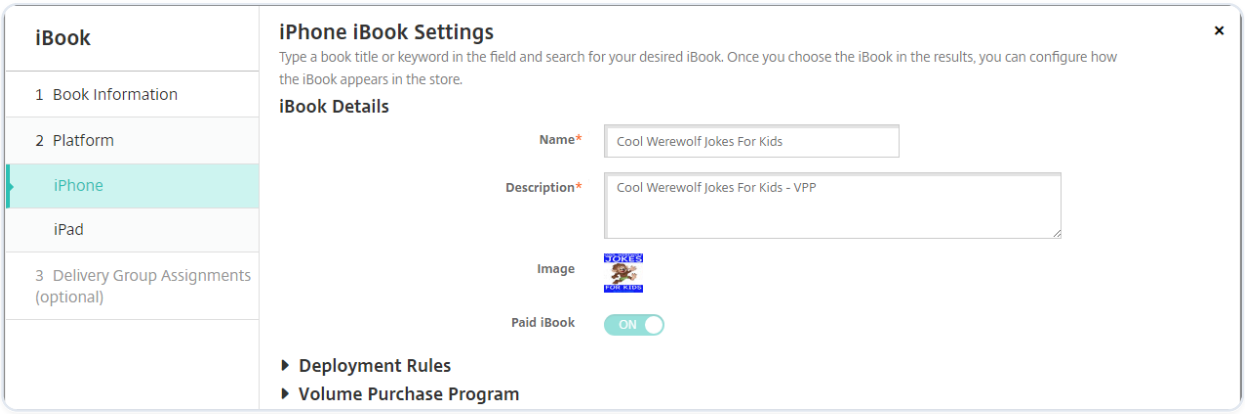


配置要部署的 Apple Book

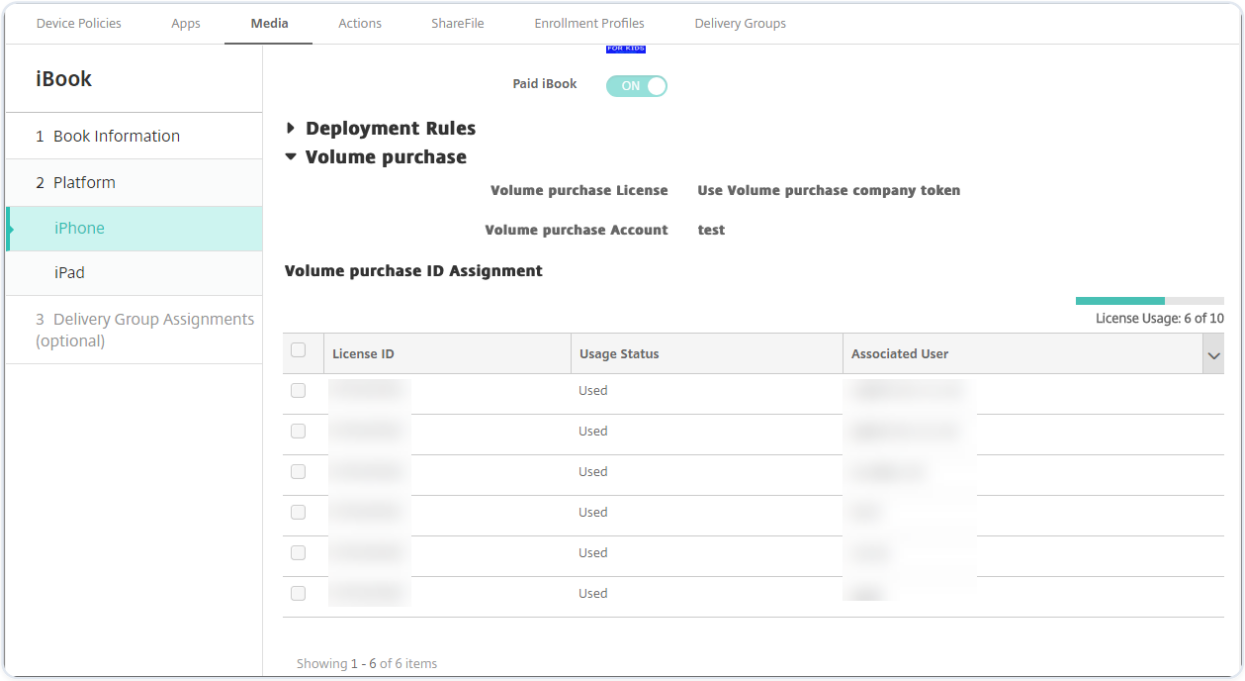
1. 在 **Configure > Media** 中，选择一本图书，然后单击 **Edit**。此时将显示 **Book Information** 页面。

Name 和 **Description** 仅显示在 XenMobile 控制台和日志中。

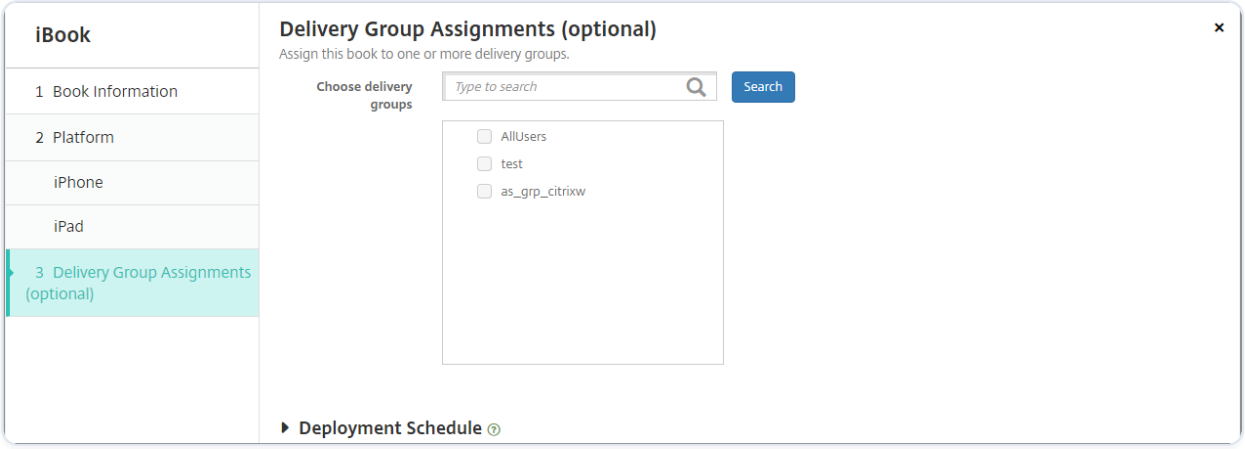
2. 在 **iPhone iBook Settings** 和 **iPad iBook Settings** 页面中：虽然您可以选择更改图书名称和说明，但 Citrix® 建议您不要更改这些设置。该图像仅供参考，不可编辑。**Paid iBook** 表示图书是通过 Apple 批量采购购买的。



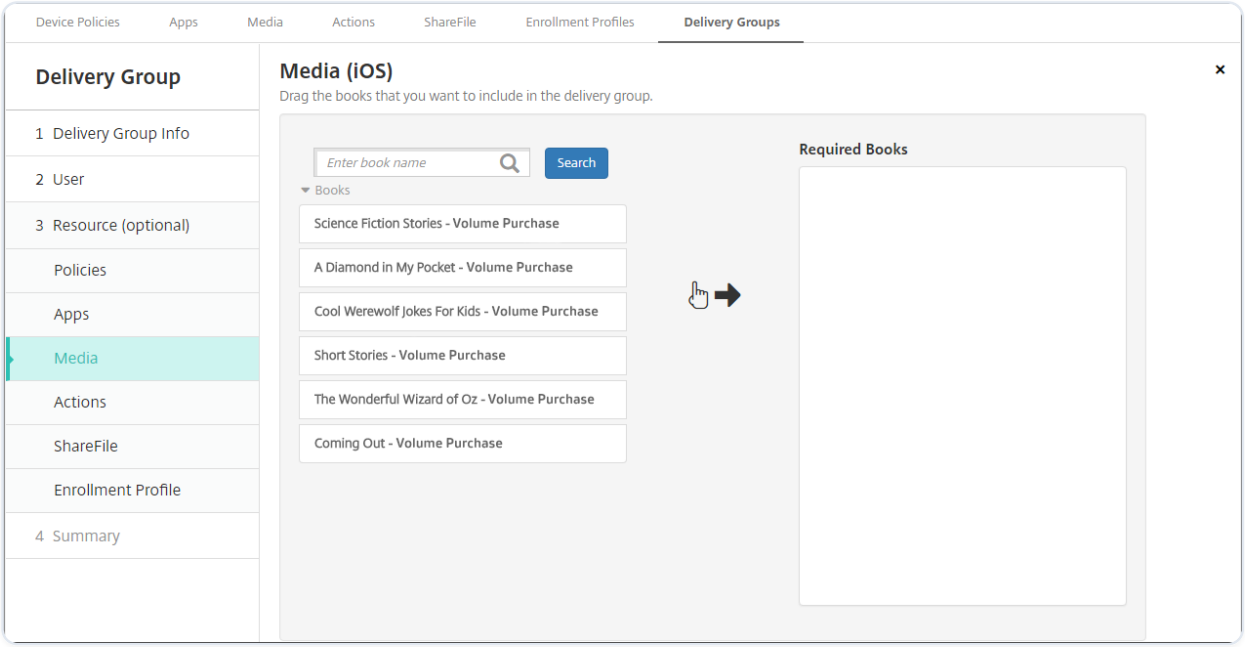
您还可以指定部署规则或查看批量购买信息。



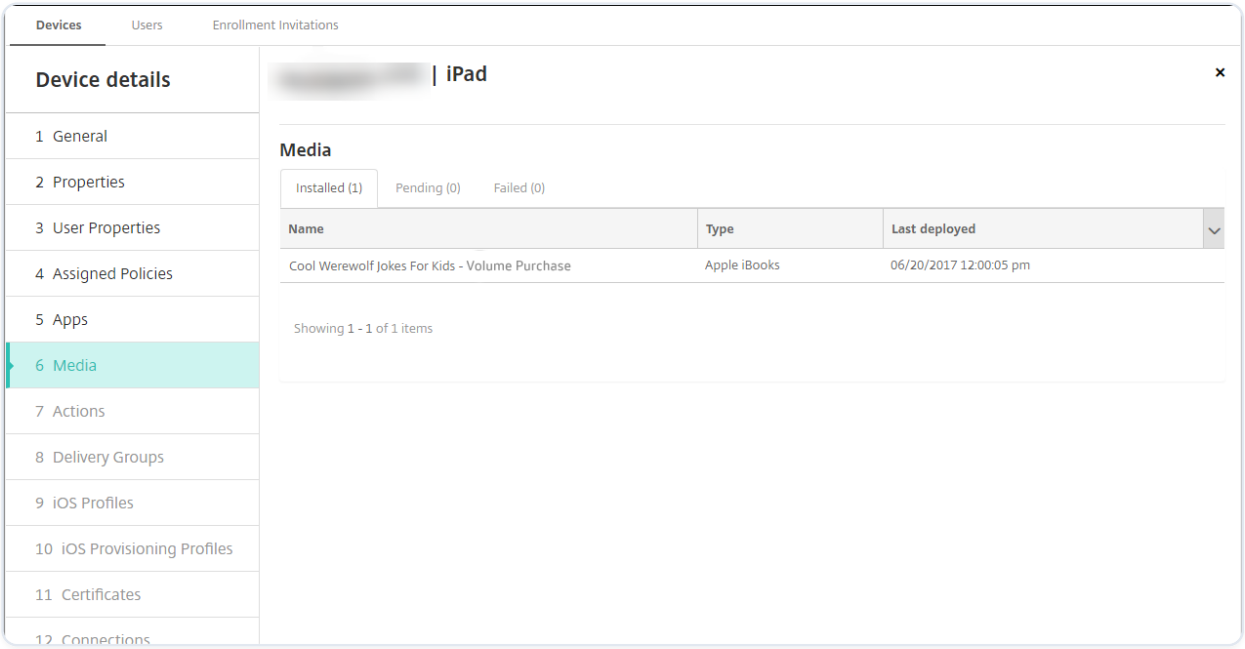
3. （可选）将图书分配给交付组并设置部署计划。



您还可以从**配置 > 交付组**的**媒体**选项卡中将图书分配给交付组。XenMobile 仅支持强制图书部署。



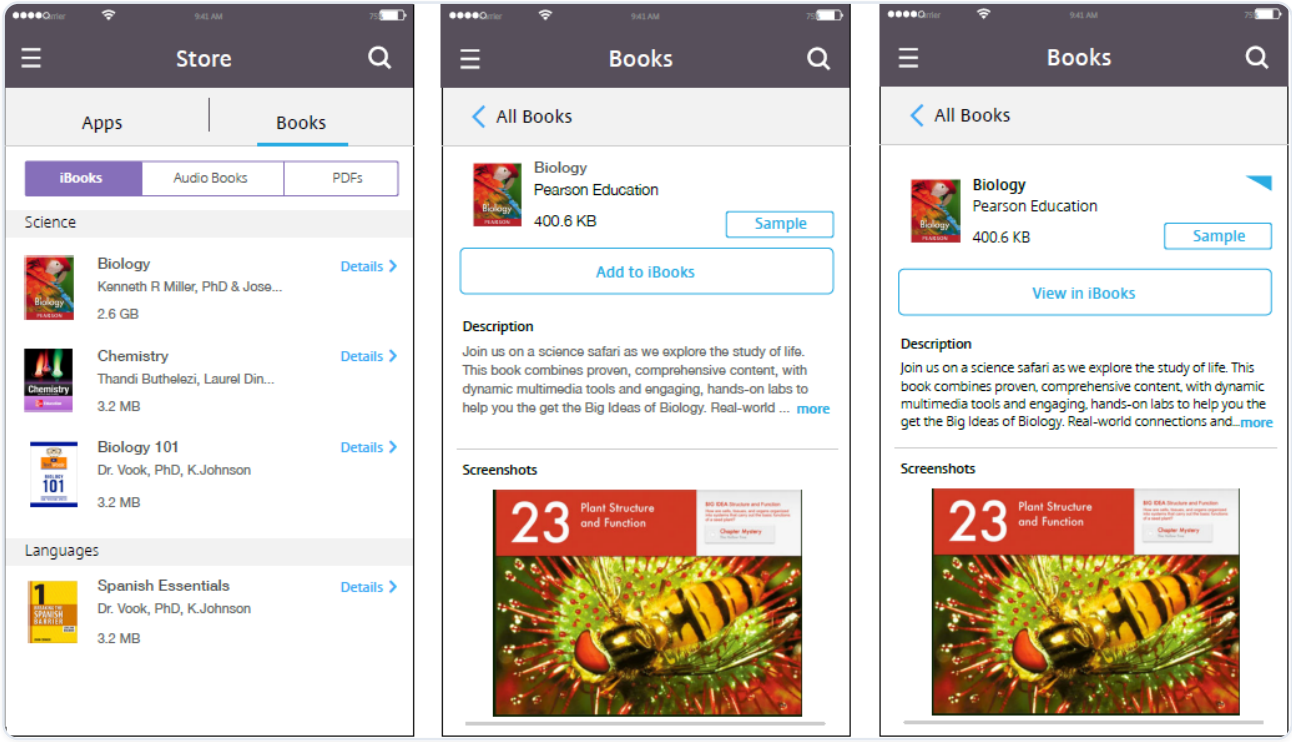
4. 使用**管理 > 设备**的**媒体**选项卡查看部署状态。



注意：

在**配置 > 媒体**页面上，如果您选择一本图书并单击**删除**，XenMobile 会将该图书从列表中删除。但是，下次 XenMobile 与 Apple 批量购买同步时，除非该图书已从 Apple 批量购买中删除，否则它会重新出现在列表中。从列表中删除图书不会从设备中删除图书。

图书在用户设备上显示，如以下示例所示。


Store
Apps
Books
iBooks
Audio Books
PDFs
Science
Biology
Kenneth R Miller, PhD & Jose...
2.6 GB
Details
Chemistry
Thandi Buthelezi, Laurel Din...
3.2 MB
Details
Biology 101
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Languages
Spanish Essentials
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
Add to iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world ... more
Screenshots
23
Plant Structure and Function
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
View in iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world connections and...more
Screenshots
23
Plant Structure and Function

部署资源

设备配置和管理通常涉及在 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。本文介绍如何：

- 添加、管理和部署交付组
- 更改交付组中资源和操作的部署顺序
- 当用户位于具有重复或冲突策略的多个交付组中时，XenMobile 如何确定部署顺序。

交付组指定用户类别，您将策略、应用程序、媒体和操作的组合部署到这些用户的设备。包含在交付组中通常基于用户特征，例如公司、国家/地区、部门、办公地址和职称。交付组让您可以更好地控制谁获得哪些资源以及何时获得这些资源。您可以将交付组部署给所有人，或部署给更精确定义的用户组。

部署到交付组意味着向所有使用受支持的 iOS 和 Windows 设备的用户发送推送通知。这些用户必须属于交付组才能重新连接到 XenMobile。您可以重新评估设备并部署作为交付组一部分的策略、应用程序、媒体和操作。

对于 Android 设备用户：如果他们已连接，则会立即收到资源。否则，根据其调度策略，他们将在下次连接时收到资源。

默认的 AllUsers 交付组在您安装和配置 XenMobile 时创建。它包含所有本地用户和 Active Directory 用户。您不能删除 AllUsers 组，但当您不想将资源推送到所有用户时，可以禁用该组。

部署顺序

部署顺序是 XenMobile 将资源推送到设备的顺序。部署顺序仅适用于配置了设备管理 (MDM) 注册配置文件的交付组中的设备。

在确定部署顺序时，XenMobile 会对资源应用筛选器和控制条件，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。在添加交付组之前，请考虑本节中的信息与您的部署目标之间的关系。

以下是与部署顺序相关的主要概念的摘要：

- **部署顺序：** XenMobile 将资源（策略、应用程序和媒体）和操作推送到设备的顺序。某些策略（例如“条款和条件”和“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，当 XenMobile 部署资源时，会忽略它们的位置。
- **部署规则：** XenMobile 使用您为设备属性指定的部署规则来筛选策略、应用程序、媒体、操作和交付组。例如，部署规则可能指定当域名与特定值匹配时推送部署包。
- **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。您可以指定部署立即发生、在特定日期和时间发生，或根据部署条件发生。

下表显示了各种对象和资源类型的筛选和控制条件。部署规则基于设备属性。

对象/资源	设备平台	部署规则	部署计划	用户/组
设备策略	是	是	是	-
应用程序	是	是	是	-
媒体	是	是	是	-
操作	-	是	是	-
交付组	-	是	-	Y

在典型环境中，很可能将多个交付组分配给单个用户，这可能会导致以下结果：

- 交付组中存在重复对象。
- 分配给用户的多个交付组中，某个特定策略的配置不同。

当出现上述任一情况时，XenMobile 会计算必须交付到设备或对其执行操作的所有对象的部署顺序。计算步骤与设备平台无关。

计算步骤

1. 根据用户、组和部署规则的筛选器，确定特定用户的所有交付组。
2. 在选定的交付组中创建所有资源（策略、应用程序、媒体和操作）的有序列表。该列表基于设备平台、部署规则和部署计划的筛选器。排序算法如下：

    a. 将具有用户定义的部署顺序的交付组中的资源置于没有用户定义的部署顺序的交付组中的资源之前。此放置的原理将在这些步骤之后进行说明。

    b. 作为交付组之间的决胜因素，按交付组名称对交付组中的资源进行排序。例如，将交付组 A 中的资源置于交付组 B 中的资源之前。

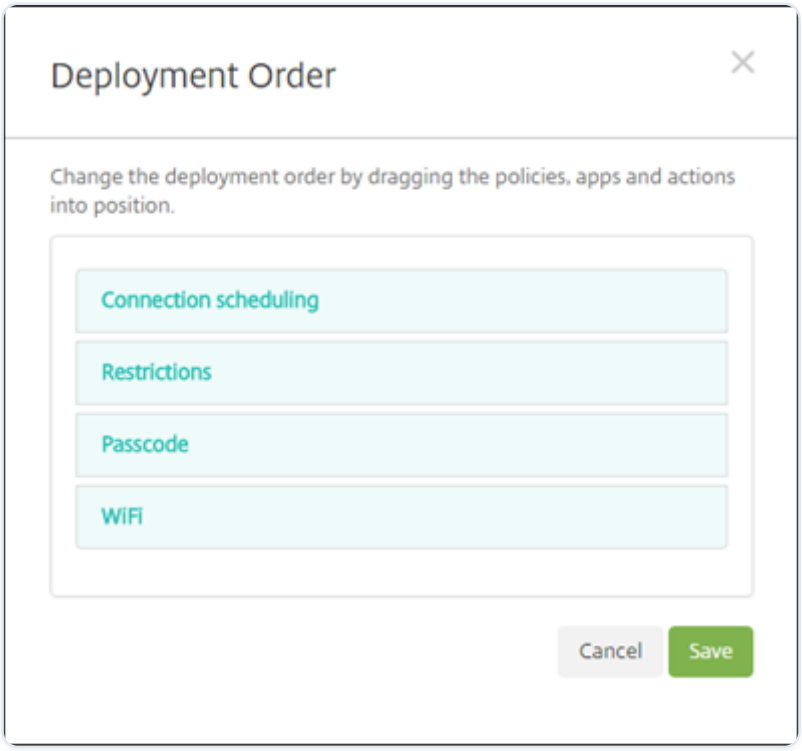
c. 排序时，如果为交付组的资源指定了用户定义的部署顺序，则保持该顺序。否则，按资源名称对该交付组中的资源进行排序。

d. 如果同一资源出现多次，则删除重复资源。

具有用户定义顺序的资源在没有用户定义顺序的资源之前部署。一个资源可以存在于分配给用户的多个交付组中。如上述步骤所示，计算算法会删除冗余资源，并且只交付此列表中的第一个资源。通过这种方式删除重复资源，XenMobile 会强制执行 XenMobile 管理员定义的顺序。

例如，假设您有两个交付组，如下所示：

- 交付组，客户经理 1：资源顺序**未指定**。包含策略 **WiFi** 和 **Passcode**。
- 交付组，客户经理 2：资源顺序**已指定**。包含策略 **连接计划**、**限制**、**Passcode** 和 **WiFi**。在此情况下，您希望在 **WiFi** 策略之前交付 **Passcode** 策略。



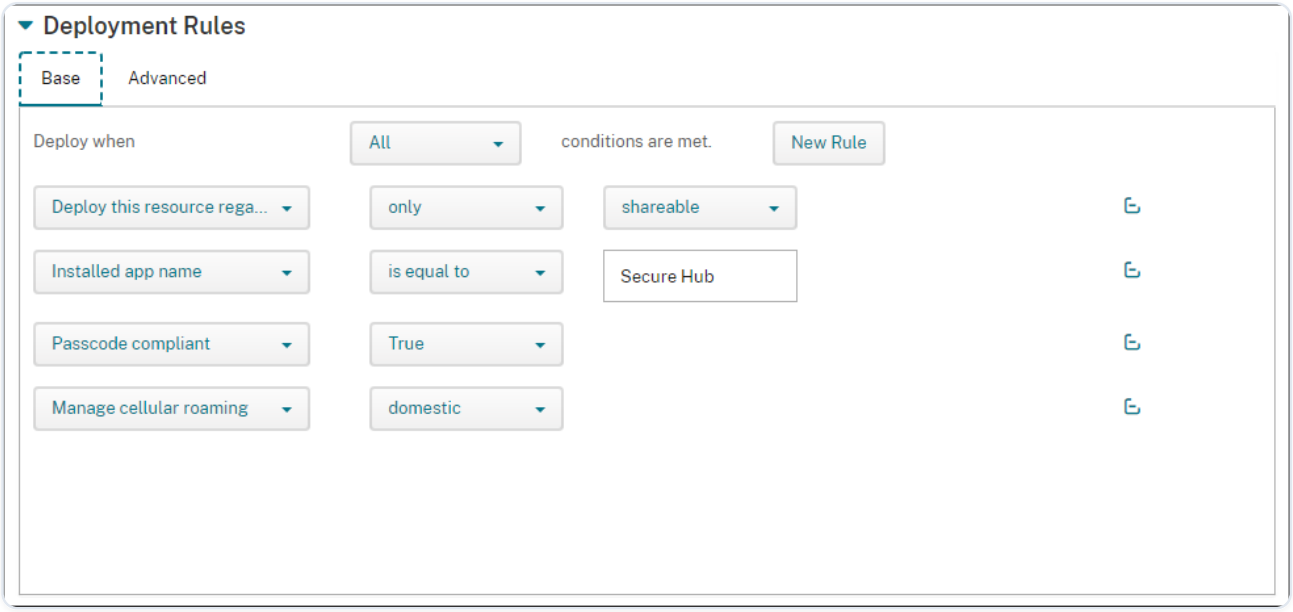
如果计算算法仅按名称对部署组进行排序，XenMobile 将按此顺序执行部署，从交付组客户经理 1 开始：**WiFi**、**Passcode**、**连接计划**和**限制**。XenMobile 将忽略客户经理 2 交付组中的 **Passcode** 和 **WiFi**（两者均为重复项）。

但是，客户经理 2 组具有管理员指定的部署顺序。因此，计算算法将客户经理 2 交付组中的资源置于列表中的较高位置，高于其他交付组中的资源。结果，XenMobile 按此顺序部署策略：**连接计划**、**限制**、**Passcode** 和 **WiFi**。XenMobile 忽略客户经理 1 交付组中的 **WiFi** 和 **Passcode** 策略，因为它们是重复项。因此，该算法遵循 XenMobile 管理员指定的顺序。

部署规则

配置部署规则，以便仅在特定条件存在时交付资源。您可以配置基本或高级部署规则。

使用基本编辑器添加部署规则时，首先选择何时部署资源。

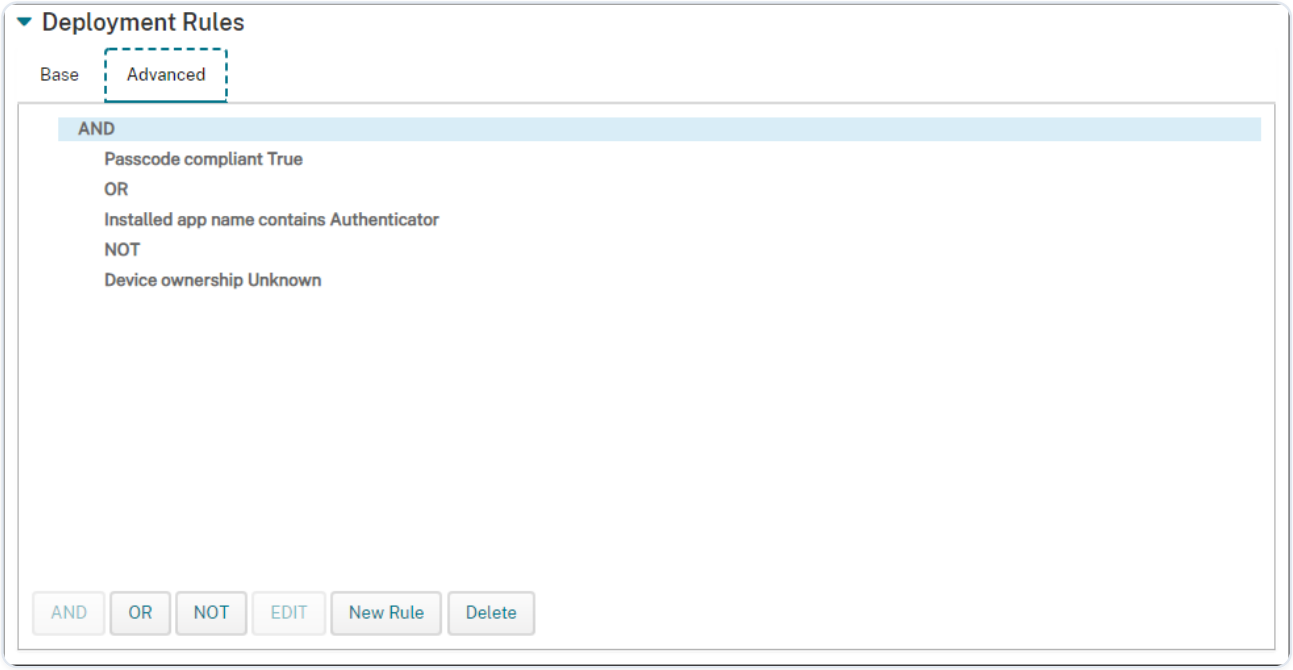


- **全部：**当用户或设备满足您配置的所有条件时交付资源。
- **任意：**当用户或设备满足您配置的至少一个条件时交付资源。

单击**新建规则**以添加条件。规则因所部署的资源以及您配置资源的平台而异。存在多种类型的规则。您可以选择部署资源：

- 仅当选定属性存在时或选定属性不存在时。
- 当属性与您键入的文本完全匹配时、属性包含您键入的文本时，或属性与您键入的文本不匹配时。
- 当设备或用户符合您选择的属性时或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。有更多规则可供选择，并且在创建高级规则时可以组合不同的布尔逻辑运算符。



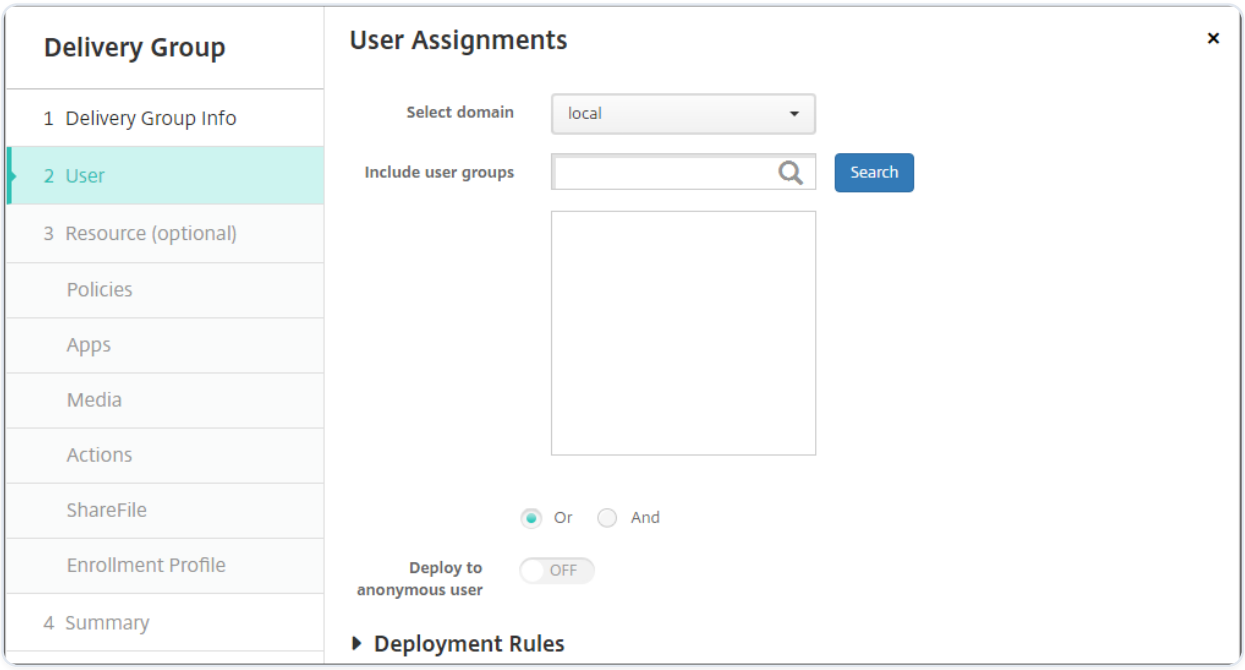
添加交付组

Citrix® 建议您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** 页面上，键入交付组的名称和描述，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，则交付组的名称决定了所使用的注册配置文件。XenMobile 会选择按字母顺序排列的交付组列表中最后出现的交付组。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。



重要提示：

用户组创建后，您无法更改 **管理用户分配** 设置。

- **选择域：** 从列表中，选择要从中选择用户的域。
- **包括用户组：** 执行以下操作之一：
  - 在用户组列表中，单击要添加的组。所选组将显示在“**选定用户组**”列表中。
  - 单击“**搜索**”以查看所选域中的所有用户组列表。
  - 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**”以查看所选域中的所有用户组列表。滚动列表并清除要删除的每个组的复选框。
  - 在搜索框中键入完整或部分组名称，然后单击“**搜索**”以限制用户组列表。滚动列表并清除要删除的每个组的复选框。
- **或/和：** 选择用户是否可以属于任何组（或），或者他们是否必须属于所有组（和）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的未经身份验证的用户。未经身份验证的用户是您无法对其进行身份验证，但仍允许其设备连接到 XenMobile 的用户。

5. 配置部署规则。
6. 单击“**下一步**”。此时将显示“**交付组资源**”页面。您可以在此处选择性地为交付组添加策略、应用程序或操作。要跳过此步骤，请在“**交付组**”下单击“**摘要**”以查看交付组配置的摘要。

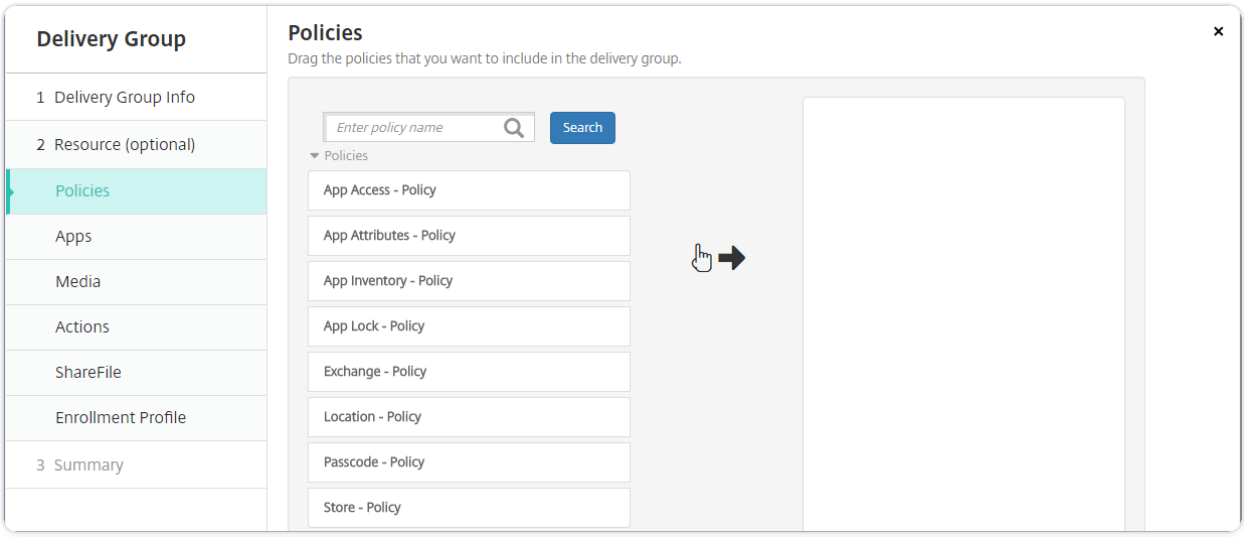
   要跳过资源，请在“**资源（可选）**”下，单击要添加的资源并按照该资源的步骤操作。

添加策略

1. 对于要添加的每个策略，请执行以下操作：

   - 滚动可用策略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**下一步**。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，请执行以下操作：

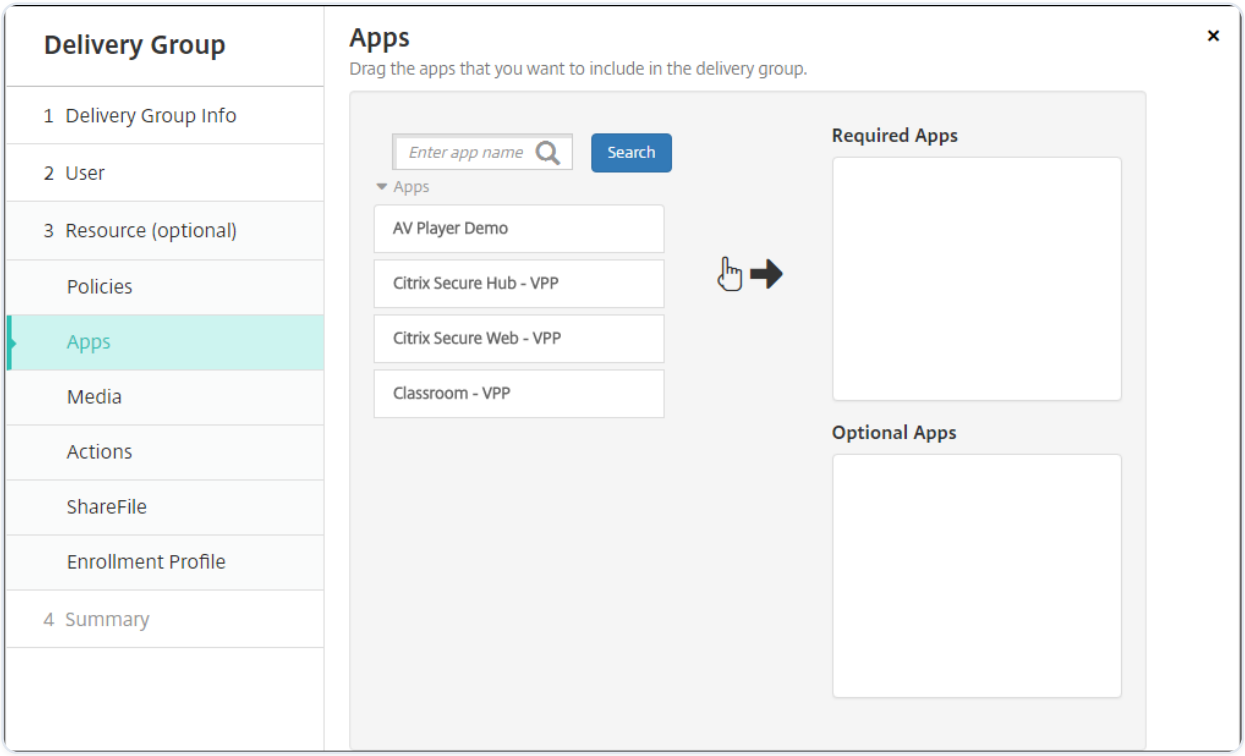
   - 滚动可用应用程序列表以查找要添加的应用程序。
   - 或者，要限制应用程序列表，请在搜索框中键入完整或部分应用程序名称，然后单击**搜索**。
   - 单击要添加的应用程序，并将其拖动到**所需应用程序**框或**可选应用程序**框中。

   对于标记为必需的应用程序，用户可以在以下情况下及时接收更新：

   - 您上传了一个新应用程序并将其标记为必需。

- 您将现有应用程序标记为必需。
- 当用户删除必需应用程序时。
- Secure Hub 更新可用。

有关强制部署所需应用程序的信息，包括如何启用该功能，请参阅关于所需和可选应用程序。



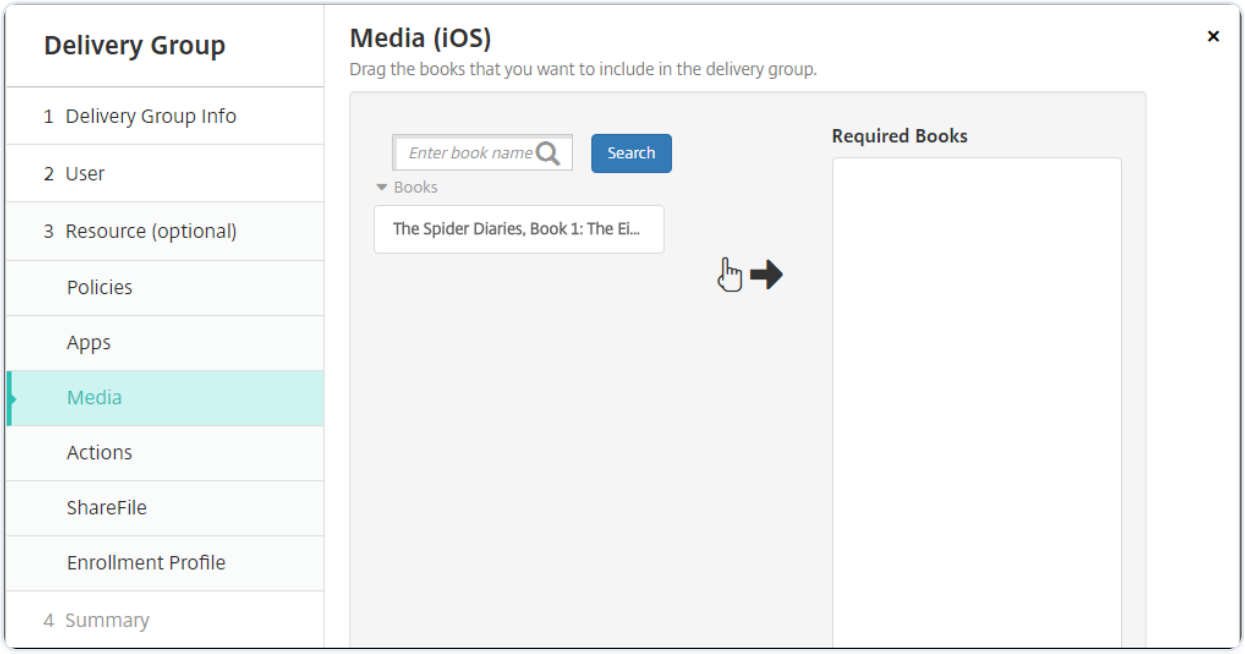
要删除应用程序，请单击右侧框中应用程序名称旁边的 **X**。

2. 单击“**下一步**”。将显示“**媒体**”页面。

添加媒体

1. 对于要添加的每本书，请执行以下操作：

   - 滚动可用书籍列表，找到要添加的书籍。
   - 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“**所需书籍**”框中。



对于标记为必需的书籍，用户会在以下情况下及时收到更新：

- 您上传了一本新书并将其标记为必需。
- 您将现有书籍标记为必需。
- 当用户删除必需书籍时。
- Secure Hub 更新可用。

要删除一本书，请单击右侧框中书名旁边的 **X**。

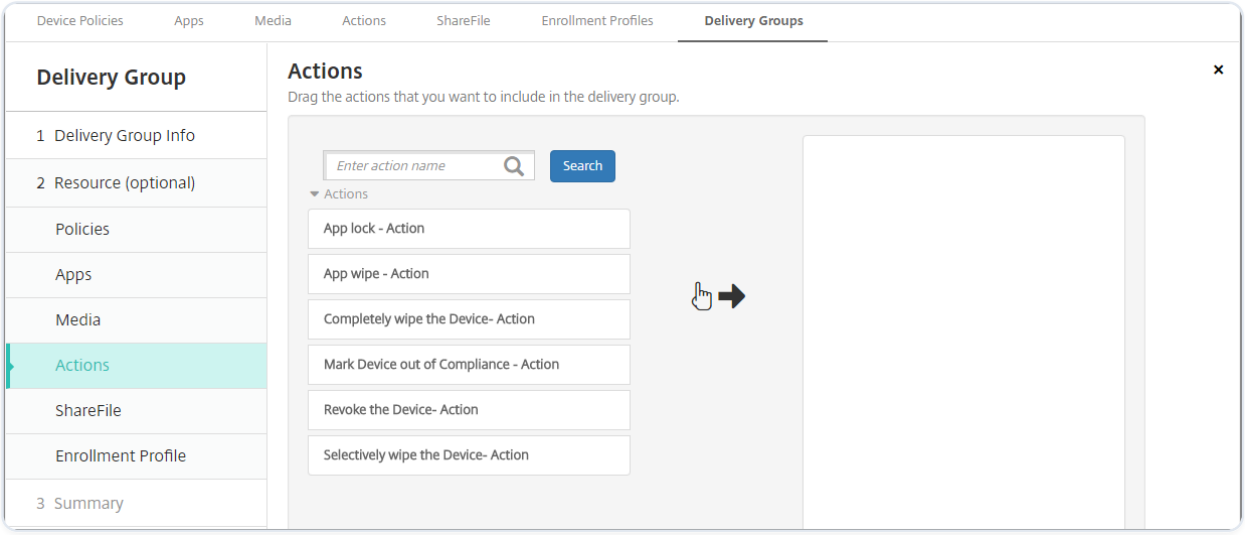
2. 单击“**下一步**”。此时将显示“**操作**”页面。

添加操作

1. 对于要添加的每个操作，请执行以下操作：

   - 滚动可用操作列表以查找要添加的操作。
   - 或者，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**。

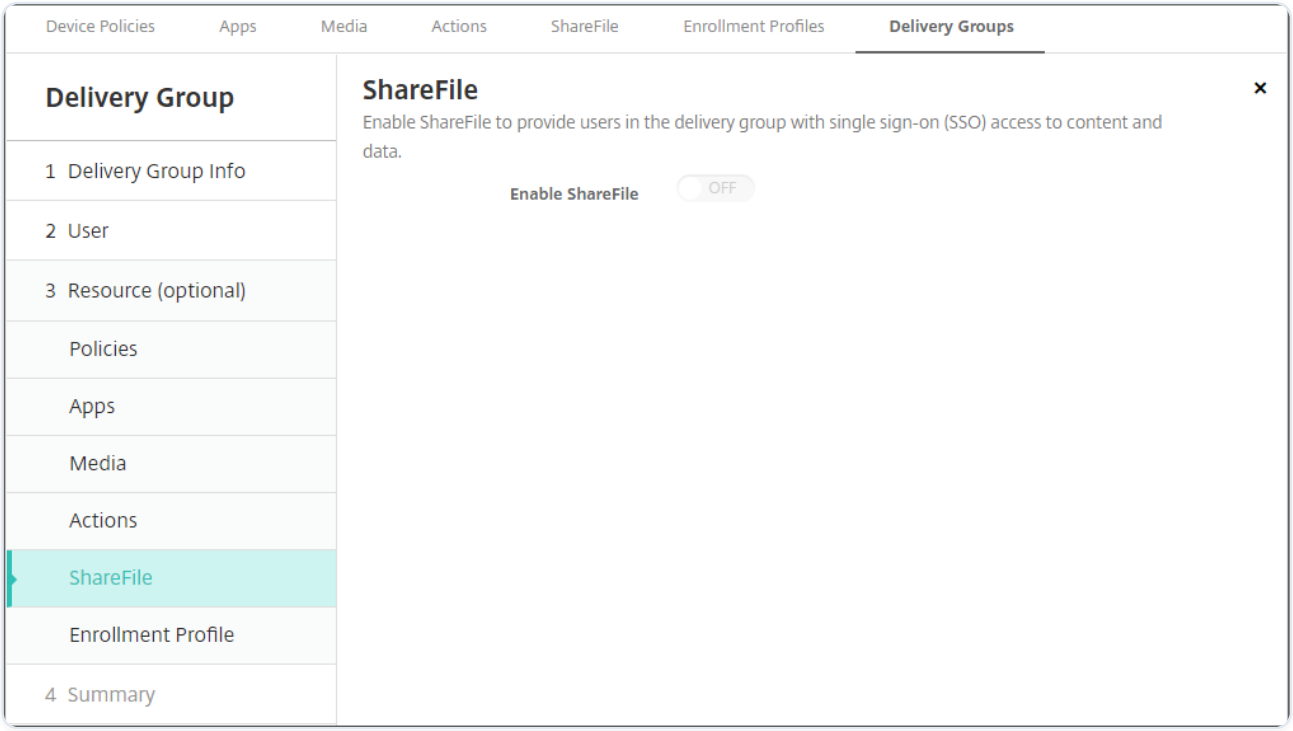


2. 单击“**下一步**”。此时将显示“**ShareFile**”页面。

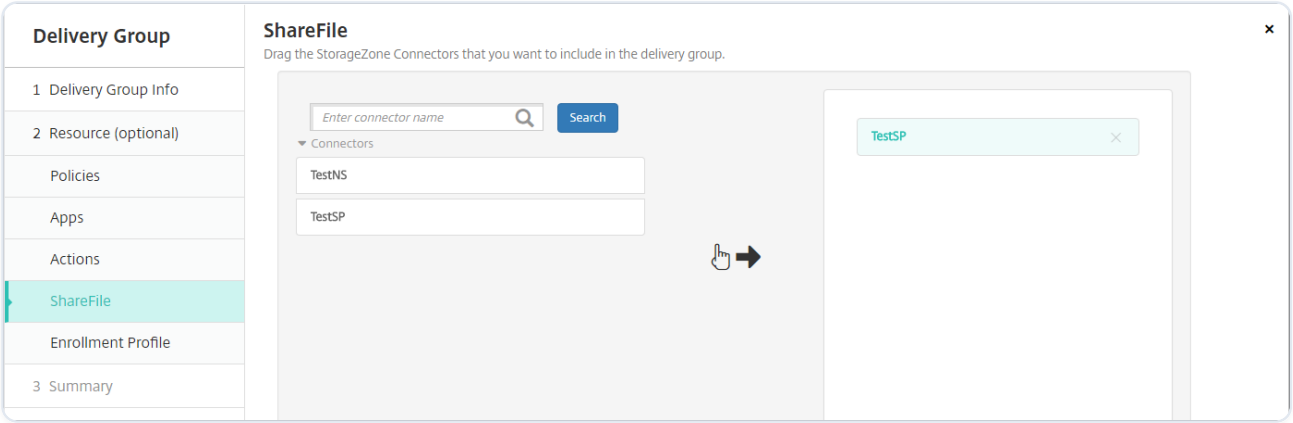
应用 ShareFile 配置

ShareFile 页面因您是为企业帐户还是为存储区域连接器配置了 XenMobile（**配置 > ShareFile**）而异。

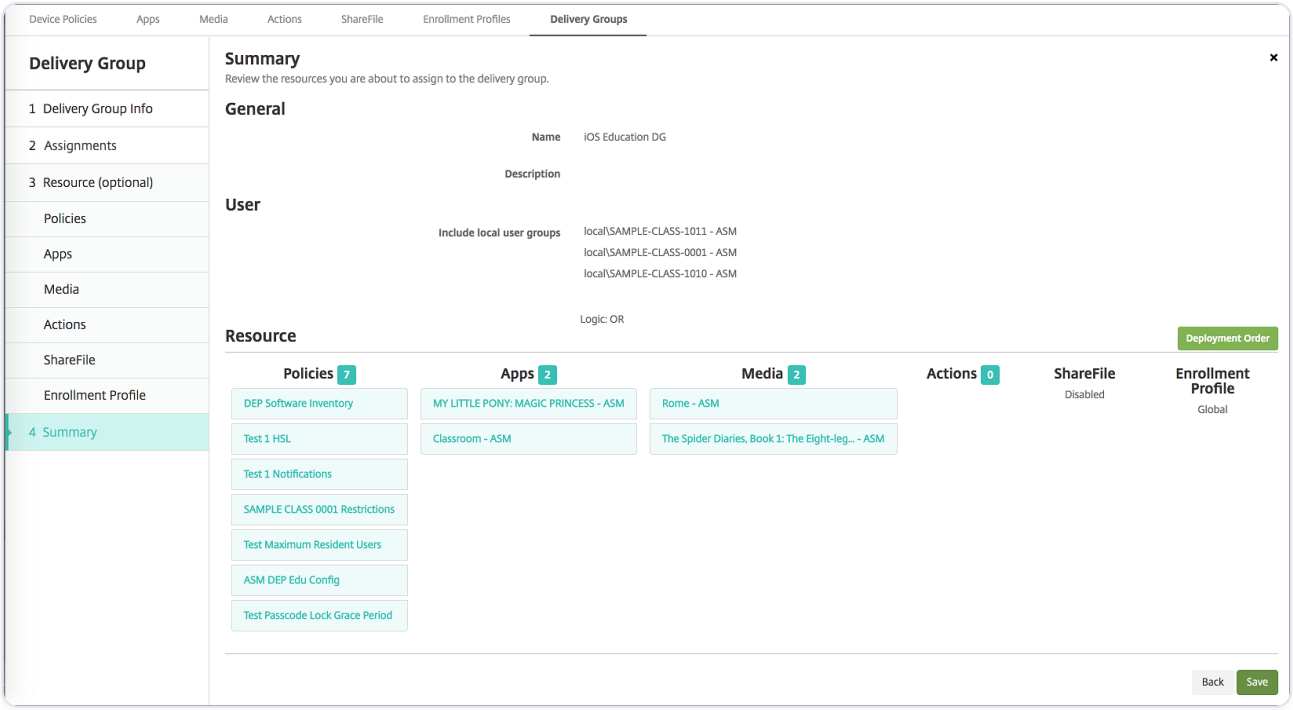
如果您配置了用于 XenMobile 的企业帐户：将“**启用 ShareFile**”设置为“**开**”，以为交付组提供对 ShareFile 内容和数据的单点登录访问权限。



如果您配置了用于 XenMobile 的存储区域连接器，请选择要包含在交付组中的存储区域连接器。

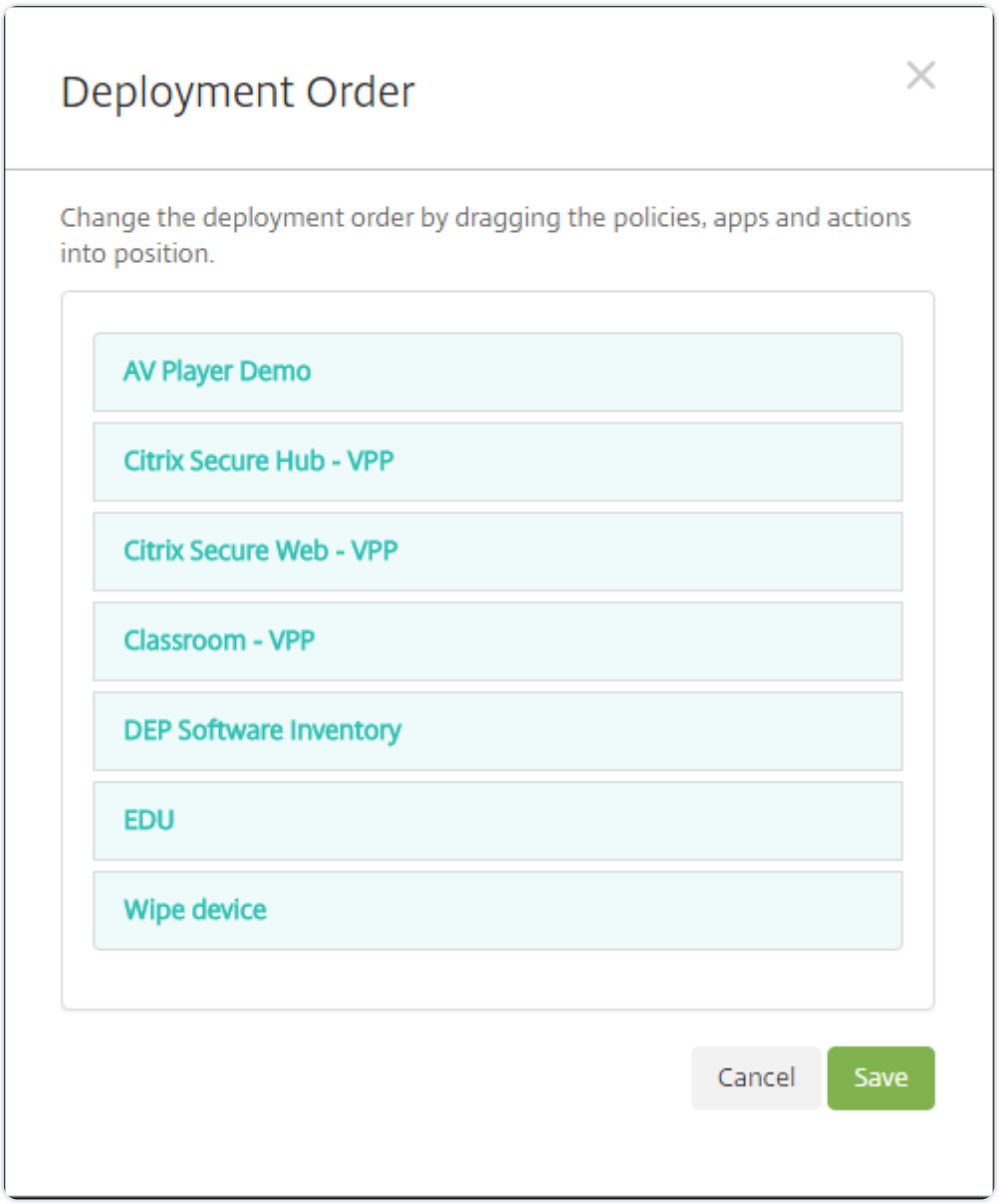


查看已配置选项并更改部署顺序



在**摘要**页面上，您可以查看为交付组配置的选项并更改资源的部署顺序。摘要页面按类别显示您的资源。摘要页面不反映部署顺序。

1. 单击**返回**以返回到上一页，对配置进行任何必要的调整。
2. 单击**部署顺序**以查看部署顺序或重新排序部署顺序。将显示**部署顺序**对话框。



3. 单击一个资源并将其拖动到您希望部署的位置。更改部署顺序后，XenMobile 将按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

您无法更改现有交付组的名称。要更新其他设置：转到**配置 > 交付组**，选择要编辑的组，然后单击**编辑**。

启用和禁用 AllUsers 交付组

AllUsers 是唯一可以启用或禁用的交付组。

在**交付组**页面上，通过选中 **AllUsers** 旁边的复选框或单击包含 AllUsers 的行来选择 AllUsers 交付组。然后执行以下操作之一：

- 点击“**禁用**”以禁用 AllUsers 交付组。此命令仅在 AllUsers 启用（默认）时可用。“**已禁用**”将显示在交付组表中的“**已禁用**”标题下。
- 点击“**启用**”以启用 AllUsers 交付组。此命令仅在 AllUsers 禁用时可用。“**已禁用**”将从交付组表中的“**已禁用**”标题下消失。

部署到交付组

部署到交付组意味着向所有使用 iOS 和 Windows 平板电脑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，您可以重新评估设备并部署应用程序、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，它们会立即收到资源。否则，根据其调度策略，它们会在下次连接时收到资源。Android Enterprise 平台上的用户会从 Firebase Cloud Messaging 通知系统接收通知，然后连接到 XenMobile Server 以检索资源。

要使更新的应用程序显示在 Android 设备上 XenMobile Store 中的“可用更新”列表中：首先向用户设备部署应用程序清单策略。

1. 在“**交付组**”页面上，执行以下操作之一：

   - 要一次部署到多个交付组，请选中要部署的组旁边的复选框。
   - 要部署到单个交付组，请选中其名称旁边的复选框，或单击包含其名称的行。

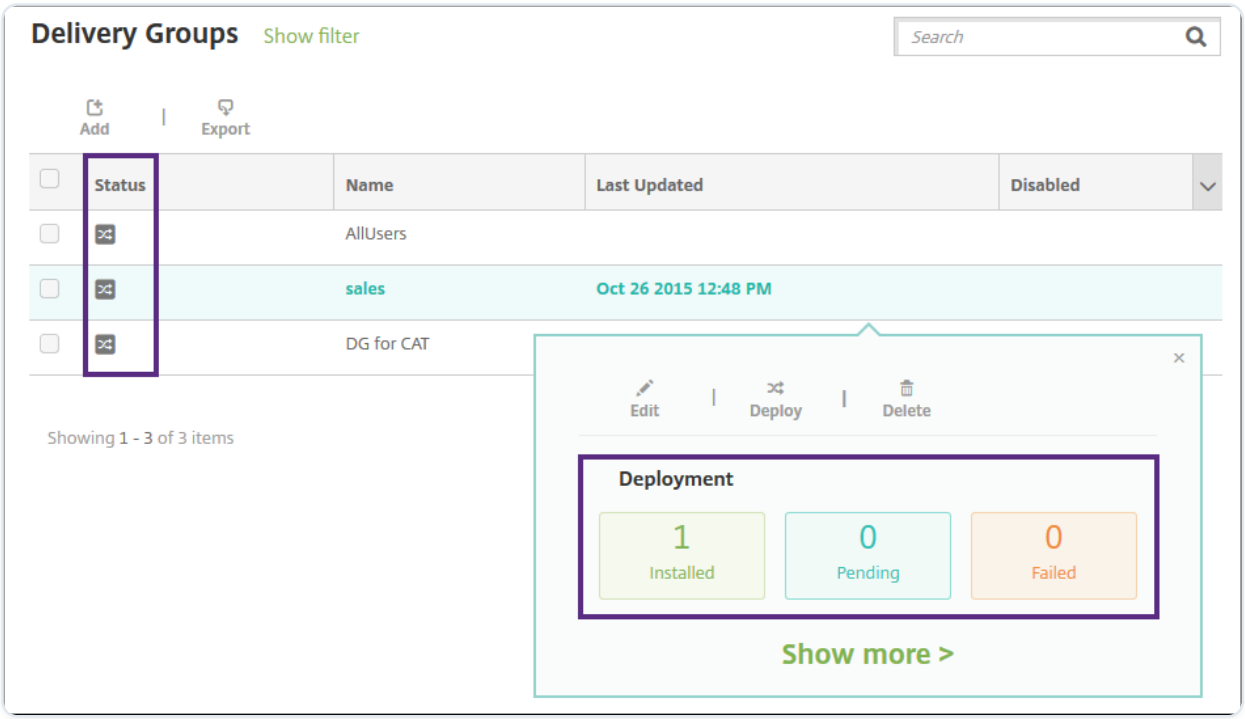
2. 点击“**部署**”。

   根据您选择单个交付组的方式，“**部署**”命令会显示在交付组上方或右侧。

   验证要部署应用程序、策略和操作的组是否已列出，然后点击“**部署**”。应用程序、策略和操作将根据设备平台和调度策略部署到所选组。

   您可以通过以下方式之一在“**交付组**”页面上检查部署状态：

   - 查看交付组“**状态**”标题下的部署图标，该图标指示任何部署失败。
   - 点击包含交付组的行以显示一个叠加层，其中指示“**已安装**”、“**待处理**”和“**失败**”的部署。



克隆交付组

当您想要创建与现有交付组类似的交付组时，请克隆一个交付组。将克隆的交付组用作新交付组的起点。然后对克隆的交付组进行更改，例如添加注册配置文件或新的 AD 用户集。

1. 在 XenMobile Server 控制台中，单击“**配置**”，然后选择“**交付组**”选项卡。
2. 从交付组列表中，选择要用作新组基础的交付组。
3. 选择“**克隆**”。
4. 在“**克隆交付组**”对话框中，输入新组的名称和说明（可选）。
5. 选择“**克隆**”。

删除交付组

您无法删除 AllUsers 交付组，但当您不想向所有用户推送资源时，可以禁用该组。

1. 在“**交付组**”页面上，执行以下操作之一：
   - 要一次删除多个交付组，请选中要删除的组旁边的复选框。
   - 要删除单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。
2. 单击“**删除**”。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**”命令会显示在交付组上方或右侧。

> **重要提示：**
>
> 您无法撤消删除操作。

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 将提取**交付组**表中的信息并将其转换为 .csv 文件。
2. 按照浏览器的常规步骤打开或保存 .csv 文件。您也可以取消该操作。

宏

XenMobile® 提供宏，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一种方式：

- 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，您可以在单个 Exchange 配置文件中为数千名用户预填充用户的邮箱值。

宏语法

宏可以采用以下形式：

- `${type.PROPERTYNAME}`
- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]}`

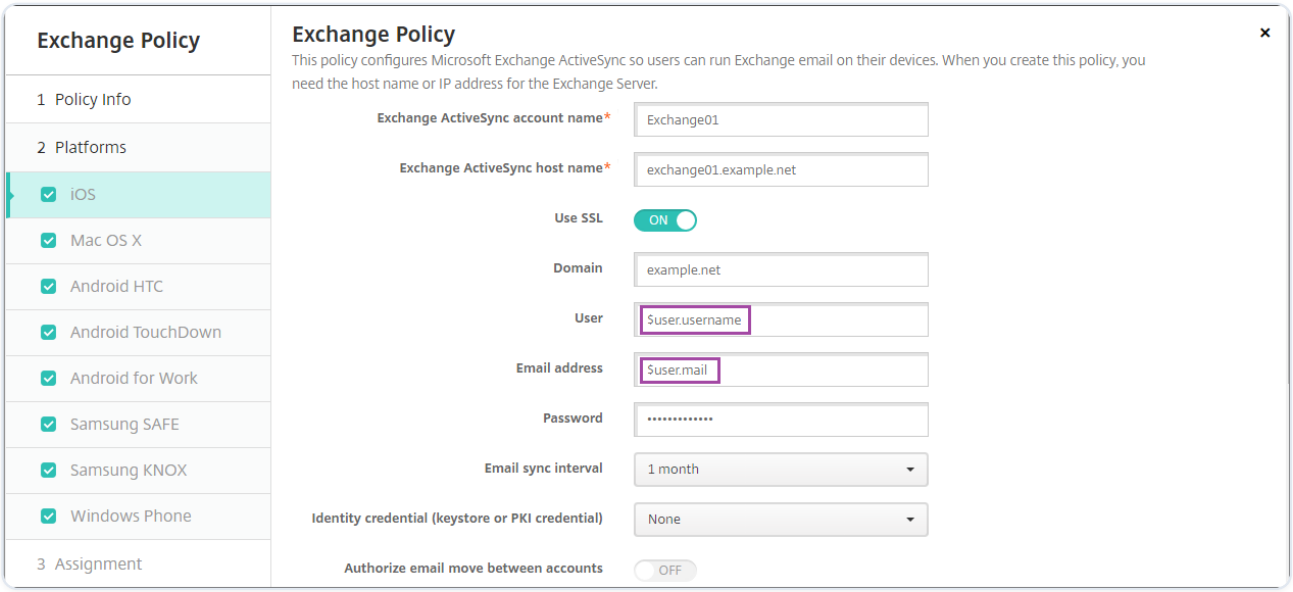
将美元符号 ($) 后面的所有语法用大括号 ({ }) 括起来。

- 限定属性名称引用用户属性、设备属性或自定义属性。
- 限定属性名称由前缀和实际属性名称组成。
- 用户属性采用以下形式 `${user.[PROPERTYNAME] (prefix="user.")}`。
- 设备属性采用以下形式 `${device.[PROPERTYNAME] (prefix="device.")}`。

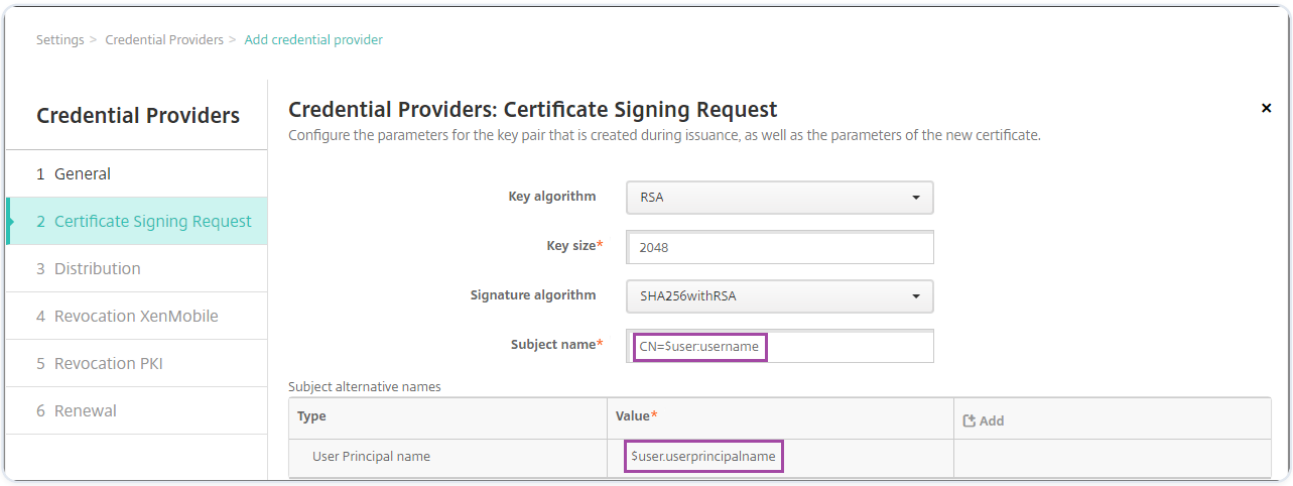
- 属性名称区分大小写。
- 函数可以是有限列表，也可以是定义函数的第三方参考链接。以下用于通知消息的宏包含 **firstnotnull** 函数。

  设备 `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 已被阻止...
- 对于自定义宏（您定义的属性），前缀为 `${custom}`。您可以省略此前缀。

以下是一个常用宏的示例 `${user.username}`，它在策略的文本字段中填充用户名值。此宏对于配置 Exchange ActiveSync 配置文件以及许多用户使用的其他配置文件非常有用。以下示例说明了如何在 Exchange 策略中使用宏。**用户**的宏为 **`${user.username}`**。**电子邮件地址**的宏为 **`${user.mail}`**。

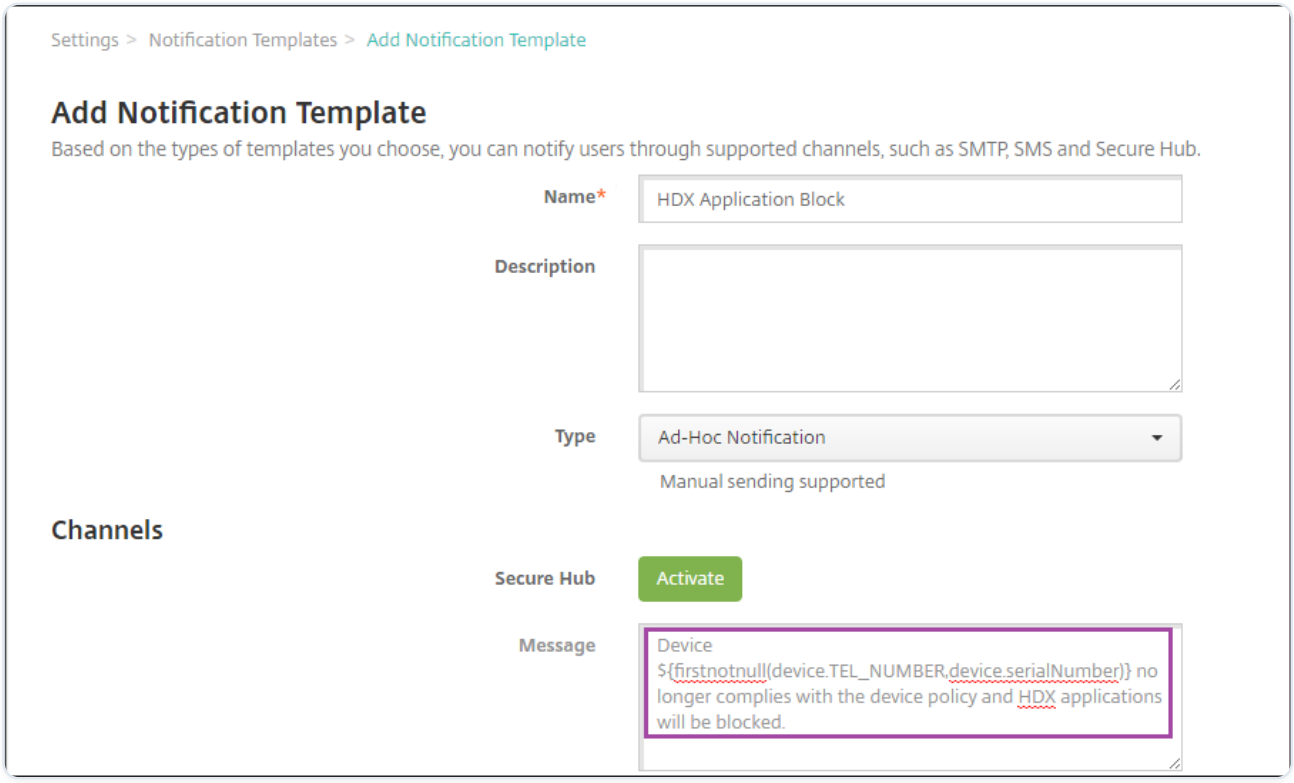


以下示例说明了如何将宏用于证书签名请求。**主题名称**的宏为 **`CN=$user.username`**。**主题备用名称的值**的宏为 **`$user.userprincipalname`**。



以下示例说明了如何在通知模板中使用宏。该示例模板定义了当 HDX™ 应用程序因设备不合规而被阻止时发送给用户的消息。**消息**的宏为：

设备 `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` 不再遵循设备策略，HDX 应用程序将被阻止。



有关通知中使用的宏的更多示例，请转至**设置 > 通知模板**，选择预定义模板，然后单击**编辑**。

以下示例显示了设备名称设备策略中的宏。您可以键入宏、宏组合或宏与文本的组合来唯一命名每个设备。例如，使用 `${device.serialnumber}` 将设备名称设置为每个设备的序列号。使用 `${device.serialnumber} ${ user.username }` 在设备名称中包含用户名。设备名称设备策略适用于受监管的 iOS 和 macOS 设备。

设备策略配置屏幕中的宏图像(/en-us/xenmobile/server/media/macro-example-device-name-policy.png)

默认通知模板的宏

您可以在默认通知模板中使用以下宏：

- `${account.SUPPORT_EMAIL}`
- `${applicationName}`
- `${enrollment.andriod.agent.download.url}`
- `${enrollment.ios.agent.download.url}`
- `${enrollment.pin}`
- `${enrollment.url}`

- `${enrollment.urls}`
- `${enrollment.ios.url}`
- `${enrollment.macos.url}`
- `${enrollment.android.url}`
- `${enrollment.ios.platform}`
- `${enrollment.macos.platform}`
- `${enrollment.android.platform}`
- `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${outofcompliance.reason(smg_block)}`
- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`

> **注意：**
>
> XenMobile Server 控制台包含术语“黑名单”和“白名单”。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

- `${vpp.account}`
- `${vpp.appname}`
- `${vpp.url}`
- `${zdmserver.hostPath}/enroll`

特定策略的宏

对于设备名称设备策略（适用于 iOS 和 macOS），您可以使用以下宏作为**设备名称**：

- `${device.serialnumber}`
- `${user.username}@example.com`
- `${device.serialnumber}`
- `${device.serialnumber}`
- `${user.username}`
- `${enrollment.pin}`

- `${user.dnsroot}`

对于 Webclip 设备策略，您可以将此宏用于 **URL**：

- `${webeas-url}`

对于 Samsung MDM 许可证密钥设备策略，您可以将此宏用于 **ELM 许可证密钥**：

- `${elm.license.key}`

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`

所有设备属性的宏

以下列表提供了显示名称、Web 元素和宏。

帐户已暂停？

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED}

激活锁绕过代码

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE}

激活锁已启用

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED}

活跃的 iTunes 账户

- 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}

管理员已禁用

- 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}

安卓企业版设备 ID

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID}

Android Enterprise 已启用设备？

- 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}

防病毒签名状态

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS}

防病毒状态

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS}

ASM DEP 激活锁绕过代码

- 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}

在后台自动下载软件更新

- 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}

备用电池

- 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}

电池剩余电量

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING}

电池运行时间

- 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}

启动调试已启用？

- 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}

蜂窝网络海拔

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR}

蜂窝网络航向

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR}

蜂窝网络水平精度

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}

蜂窝网络纬度

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR}

蜂窝网络经度

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR}

蜂窝网络速度

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR}

蜂窝网络技术

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY}

蜂窝网络时间戳

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR}

蜂窝网络垂直精度

- 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}

云备份已启用

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED}

代码完整性已启用？

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}

代码完整性吊销列表版本

- 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}

当前移动国家代码

- CURRENT_MCC
- ${device.CURRENT_MCC}

当前移动网络代码

- CURRENT_MNC
- ${device.CURRENT_MNC}

允许数据漫游

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED}

上次 iCloud 备份日期

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

默认目录

- IsDefaultCatalog

- ${device.IsDefaultCatalog}

DEP 账户名称

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}

DEP 策略

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY}

DEP 配置文件已分配

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME}

DEP 配置文件已推送

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME}

DEP 配置文件已移除

- 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}

描述

- DESCRIPTION
- ${device.DESCRIPTION}

设备标识符

- 活动同步标识符
- ${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}

勿扰模式已激活

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB}

ELAM 驱动程序已加载？

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED}

加密合规性

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE}

注册密钥生成日期

- 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}

外部存储已加密

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION}

FileVault 已启用

- 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 目录别名

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}

Google 目录姓氏

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}

Google 目录名称

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

Google 目录主要电子邮件

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google 目录用户 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 航向

- 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 商店帐户的哈希值

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH}

归属运营商网络

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK}

归属移动国家代码

- SIM_MCC
- ${device.SIM_MCC}

归属移动网络代码

- SIM_MNC
- ${device.SIM_MNC}

ICCID

- ICCID
- ${device.ICCID}

身份

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY}

IMEI/MEID 号码

- IMEI

- ${device.IMEI}

IMSI

- SIM_ID
- ${device.SIM_ID}

内部存储已加密

- 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}

颁发于

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT}

越狱/Rooted

- ROOT_ACCESS
- ${device.ROOT_ACCESS}

内核调试已启用？

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}

信息亭模式

- 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}

上次计划的软件更新

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}

上次计划的软件更新失败消息

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}

上次计划的软件更新状态

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}

上次同步

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC}

定位服务已启用

- 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}

MDM 丢失模式已启用

- 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}

手机号码

- 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}

操作系统构建版本

- 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}

组织魔术

- 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}

密码合规

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT}

密码符合配置

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG}

密码存在

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT}

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0}

边界违规

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH}

定期检查

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck}

个人热点已激活

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED}

地理围栏的 PIN 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 运营商

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}

主 SIM ICCID

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID}

主 SIM IMEI

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI}

主 SIM IMSI

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI}

主 SIM 卡漫游

- 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}

重启次数

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT}

安全模式已启用？

- 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 证明更新日期

- 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：尺寸

- 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 卡 IMEI

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI}

辅助 SIM 卡 IMSI

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI}

副 SIM 卡漫游

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING}

副 SIM 卡漫游合规性

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE}

安全启动已启用？

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}

安全启动状态

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE}

安全容器已启用

- DLP_ACTIVE
- ${device.DLP_ACTIVE}

安全补丁级别

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL}

序列号

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER}

支持短信

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE}

受监管

- SUPERVISED
- ${device.SUPERVISED}

暂停原因

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON}

篡改状态

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS}

条款和条件

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS}

条款和协议已接受？

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}

测试签名已启用？

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}

总 RAM

- 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}

用户账户控制状态

- UAC_STATUS
- ${device.UAC_STATUS}

用户代理

- USER_AGENT
- ${device.USER_AGENT}

用户定义 #1

- USER_DEFINED_1
- ${device.USER_DEFINED_1}

用户定义 #2

- USER_DEFINED_2

- ${device.USER_DEFINED_2}

用户定义 #3

- 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}

语音功能

- IS_VOICE_CAPABLE
- ${device.IS_VOICE_CAPABLE}

允许语音漫游

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED}

VSM 已启用？

- 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}

是否启用 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 代理 ID

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID}

XenMobile 代理修订版

- EW_REVISION
- ${device.EW_REVISION}

XenMobile 代理版本

- 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 修补程序版本

- 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）	`${user.domainname}`
loginname（用户名加域名）	`${user.loginname}`
username（登录名减去域，如果有）	`${user.username}`

所有用户属性的宏

显示名称	WEB 元素	宏
Active Directory 登录失败尝试次数	错误密码计数	`${user.badpwdcount}`
ActiveSync 用户电子邮件	作为用户电子邮件	`${user.asuseremail}`
ASM 数据源	作为管理人员来源	`${user.asmpersonsource}`
ASM DEP 账户名称	作为管理部门帐户	`${user.asmdepaccount}`
ASM 托管 Apple ID	作为管理人员受管Apple ID	`${user.asmpersonmanagedappleid}`
ASM 密码类型	作为管理人员密码类型	`${user.asmpersonpasscodetype}`
ASM 人员 ID	ASM人员ID	`${user.asmpersonid}`
ASM 人员状态	ASM人员状态	`${user.asmpersonstatus}`
ASM 人员职称	ASM人员职称	`${user.asmpersontitle}`

显示名称	WEB 元素	宏
ASM 人员唯一 ID	ASM人员唯一ID	`${user.asmpersonuniqueid}`
ASM 源系统 ID	ASM人员源系统ID	`${user.asmpersonsourcesystemid}`
ASM 学生年级	人员等级	`${user.asmpersongrade}`
BES 用户电子邮件	BES用户电子邮件	`${user.besuseremail}`
公司	公司	`${user.company}`
公司名称	公司名称	`${user.companyname}`
国家/地区	c	`${user.c}`
部门	部门	`${user.department}`
描述	描述	`${user.description}`
已禁用用户	禁用用户	`${user.disableduser}`
显示名称	显示名称	`${user.displayname}`
可分辨名称	专有名称	`${user.distinguishedname}`
域名	域名	`${user.domainname}`
电子邮件	邮件	`${user.mail}`
名字	名字	`${user.givenname}`
家庭住址	家庭街道地址	`${user.homestreetaddress}`
家庭城市	家庭城市	`${user.homecity}`
家庭国家/地区	家庭国家/地区	`${user.homecountry}`

显示名称	WEB 元素	宏
家庭传真	家庭传真	`${user.homefax}`
家庭电话	家庭电话	`${user.homephone}`
家庭省/地区	家庭州/省	`${user.homestate}`
家庭邮政编码	家庭邮编	`${user.homezip}`
IP 电话	IP电话	`${user.ipphone}`
中间名首字母	中间名首字母	`${user.middleinitial}`
中间名	中间名	`${user.middlename}`
手机	移动电话	`${user.mobile}`
姓名	cn	`${user.cn}`
办公地址	物理交付办公室名称	`${user.physicaldeliveryofficename}`
办公城市	l	`${user.l}`
办公传真号码	传真电话号码	`${user.facsimiletelephonenumber}`
办公省/州	st	`${user.st}`
办公街道地址	办公室街道地址	`${user.officestreetaddress}`
办公电话号码	电话号码	`${user.telephonenumber}`
办公邮政编码	邮政编码	`${user.postalcode}`
邮政信箱	邮政信箱	`${user.postofficebox}`
寻呼机	寻呼机	`${user.pager}`

显示名称	WEB 元素	宏
主组 ID	主组ID	`${user.primarygroupid}`
SAM 帐户	SAM 账户名	`${user.samaccountname}`
街道地址	街道地址	`${user.streetaddress}`
姓氏	sn	`${user.sn}`
职务	职务	`${user.title}`
用户登录名	用户主体名称	`${user.userprincipalname}`

自动化操作

您可以在 XenMobile® 中创建自动化操作，以编程方式响应事件、用户或设备属性，或用户设备上应用程序的存在。创建自动化操作时，为该操作定义的触发器将确定用户设备连接到 XenMobile 时会发生什么。触发事件时，您可以向用户发送通知以纠正问题，然后再采取更严重的措施。

您可以设置自动执行的效果，包括以下内容：

- 完全或选择性擦除设备。
- 将设备设置为不合规。
- 吊销设备。
- 向用户发送通知以纠正问题，然后再采取更严重的措施。

您可以为仅限 MAM 模式配置应用程序锁定和应用程序擦除操作。

> **注意：**
>
> 在通知用户之前，您必须在 XenMobile 设置中为 SMTP 和 SMS 配置通知服务器，以便 XenMobile 可以发送消息。有关信息，请参阅通知。此外，在继续操作之前，请设置您计划使用的任何通知模板。有关详细信息，请参阅创建和更新通知模板。

操作示例

以下是使用自动化操作的一些示例：

示例一

- 您想要检测以前阻止的应用程序（例如，“Words with Friends”）。您可以指定一个触发器，在检测到“Words with Friends”应用程序后将用户设备设置为不合规。然后，该操作会通知用户他们必须删除该应用程序才能使设备恢复合规。您还可以设置一个时间限制，以确定等待用户合规的时间。超过该时间限制后，将执行定义的动作，例如选择性擦除设备。

示例二

- 您希望验证客户是否正在使用最新固件，并且如果用户必须更新其设备，则阻止其访问资源。您可以指定一个触发器，当用户设备没有最新版本时，将用户设备设置为不合规。您可以使用自动化操作来阻止资源并通知客户。

示例三

- 用户设备处于不合规状态，用户随后修复了设备。您可以配置策略以部署将设备重置为合规状态的软件包。

示例四

- 您希望将特定时间段内不活跃的用户设备标记为不合规。您可以为不活跃设备创建自动化操作，如下所示：

  a. 在 XenMobile 控制台中，转到“**设置 > 网络访问控制**”，然后选择“**不活跃设备**”。有关“**不活跃设备**”设置的详细信息，请参阅网络访问控制。

  b. 按照添加和管理操作中概述的步骤添加操作。唯一的区别是，您在“**操作详细信息**”页面上按如下方式配置设置：

     - **触发器**。选择“**设备属性**”、“**不合规**”和“**True**”。
     - **操作**。选择“**发送通知**”，然后选择在“**设置**”中使用“**通知模板**”创建的模板。然后设置执行操作前的延迟（天、小时或分钟）。设置操作重复的间隔，直到用户解决触发问题。

> **提示：**
>
> 要批量删除不活跃设备，请使用REST 服务的公共 API。您首先手动获取要删除的不活跃设备的设备 ID，然后运行删除 API 以批量删除它们。

添加和管理操作

要添加、编辑和筛选自动化操作：

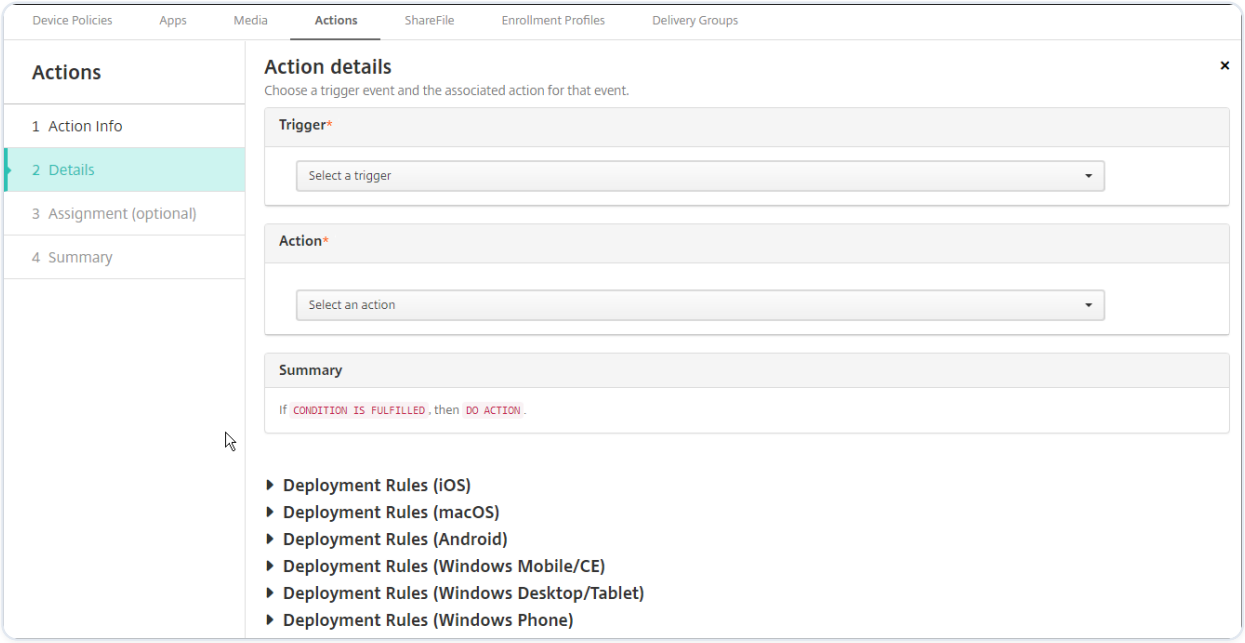
1. 在 XenMobile 控制台中，单击“**配置 > 操作**”。此时将显示“**操作**”页面。
2. 在“**操作**”页面上，执行以下操作之一：
   - 点击“**添加**”以添加操作。
   - 选择现有操作以编辑或删除。单击要使用的选项。
3. 出现“**操作信息**”页面。

4. 在“**操作信息**”页面上，输入或修改以下信息：

   - **名称：**键入用于标识操作的名称。此字段为必填项。
   - **说明：**描述此操作的用途。

5. 单击“**下一步**”。出现“**操作详细信息**”页面。

   以下示例显示了如何设置“**事件**”触发器。如果选择不同的触发器，则生成的选项将与此处显示的选项不同。



6. 在“**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，单击此操作的事件触发器类型。每个触发器的含义如下：

   - **事件：**对预定义事件做出反应。
   - **设备属性：**检查 MDM 管理设备上的设备属性，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。
   - **已安装的应用程序名称：**对正在安装的应用程序做出反应。不适用于仅 MAM 模式。要求在设备上启用应用程序清单策略。应用程序清单策略默认在所有平台上启用。有关详细信息，请参阅应用程序清单设备策略。

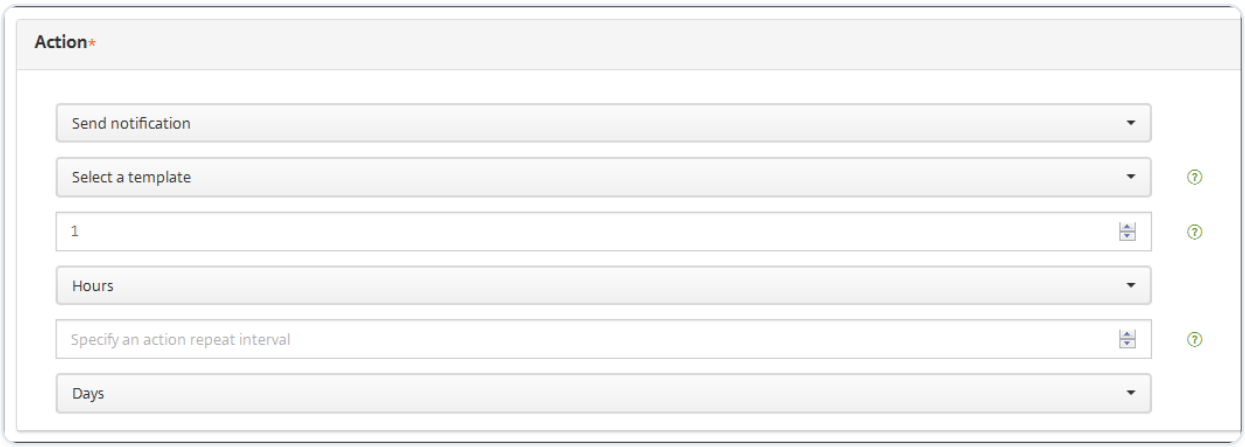
7. 在下一个列表中，单击触发器的响应。

8. 在**操作**列表中，单击满足触发器条件时要执行的操作。除了**发送通知**，您可以选择一个时间范围，在此时间范围内用户可以解决导致触发器的问题。如果问题未在该时间范围内解决，则会执行所选操作。有关操作的定义，请参阅安全操作。

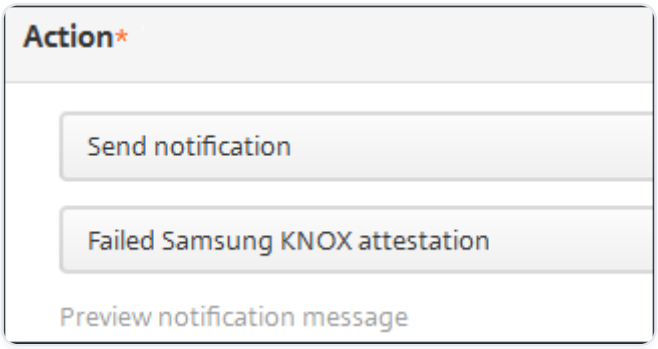
如果您选择**发送通知**，请按照以下步骤发送通知操作。

9. 在下一个列表中，选择用于通知的模板。将显示与所选事件相关的通知模板，除非该通知类型尚不存在模板。在这种情况下，系统会提示您配置一个模板，并显示消息：此事件类型没有模板。请使用**设置**中的**通知模板**创建模板。

   在通知用户之前，您必须在SMTP和SMS的设置中配置通知服务器，以便XenMobile可以发送消息，请参阅通知。此外，在继续之前，请设置您计划使用的任何通知模板。有关设置通知模板的详细信息，请参阅创建和更新通知模板。



   选择模板后，您可以通过单击**预览通知消息**来预览通知。



10. 在以下字段中，设置执行操作前的延迟（以天、小时或分钟为单位）。设置操作重复的间隔，直到用户解决触发问题。

11. 在**摘要**中，验证您是否按预期创建了自动化操作。

Summary

If The installed app name is " `APP` ", then notify `USING TEMPLATE` after 1 hour(s).

12. 配置操作详细信息后，您可以单独配置每个平台的部署规则。为此，请为您选择的每个平台完成步骤13。
13. 配置部署规则。有关配置部署规则的常规信息，请参阅部署资源。

    例如：

    - 设备所有权必须为 **BYOD**。
    - 设备本地加密必须为 **True**。
    - 设备必须符合密码策略。
    - 设备移动国家代码不能仅为安道尔。

14. 完成为操作配置平台部署规则后，单击**下一步**。此时将显示**操作分配**页面，您可以在其中将操作分配给一个或多个交付组。此步骤是可选的。
15. 在**选择交付组**旁边，键入以查找交付组或从列表中选择组。您选择的组将显示在**接收应用程序分配的交付组**列表中。
16. 展开“部署计划”，然后配置以下设置：

    - 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。默认选项设置为**开**。如果选择**关**，则无需其他选项。
    - 在**部署计划**旁边，单击**立即**或**稍后**。默认选项设置为**立即**。
    - 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
    - 在**部署条件**旁边，单击**每次连接时**或单击**仅当上次部署失败时**。默认选项设置为**每次连接时**。
    - 在**为始终在线连接部署**旁边，单击**开**或**关**。默认选项设置为**关**。

      当您在**设置 > 服务器属性**中配置了计划后台部署密钥时，此选项适用。始终在线选项不适用于 iOS 设备。

    您配置的部署计划对所有平台都相同。您所做的任何更改都适用于所有平台，但**为始终在线连接部署**除外，此选项不适用于 iOS。

17. 单击**下一步**。此时将显示**摘要**页面，您可以在其中验证操作配置。
18. 单击**保存**以保存操作。

应用程序锁定和应用程序擦除操作（仅限 MAM 模式）

您可以擦除或锁定设备上的应用程序，以响应 XenMobile 控制台中列出的所有四类触发器：事件、设备属性、用户属性和已安装的应用程序名称。

配置自动应用程序擦除或应用程序锁定

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，输入操作的名称以及可选的描述。
4. 在**操作详细信息**页面上，选择所需的触发器。
5. 在**操作**中，选择一个操作。

   对于此步骤，请记住以下条件：

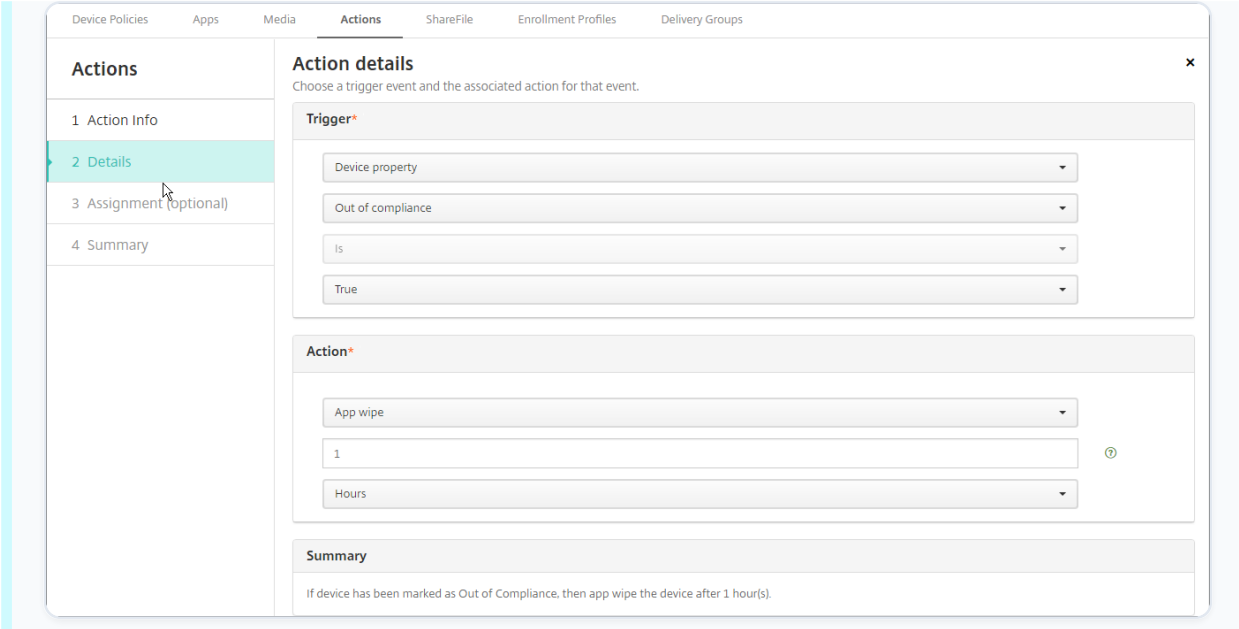
   当触发器类型设置为**事件**并且值不是**Active Directory 禁用用户**时，则不会显示**应用程序擦除**和**应用程序锁定**操作。

   当触发器类型设置为**设备属性**并且值为**MDM 丢失模式已启用**时，则不会显示以下操作：

   - 选择性擦除设备
   - 完全擦除设备
   - 吊销设备

   对于每个选项，系统会自动设置 1 小时延迟，但您可以选择以分钟、小时或天为单位的延迟时间。延迟的目的是让用户在操作发生之前有时间解决问题。有关应用程序擦除和应用程序锁定操作的更多信息，请参阅安全操作。

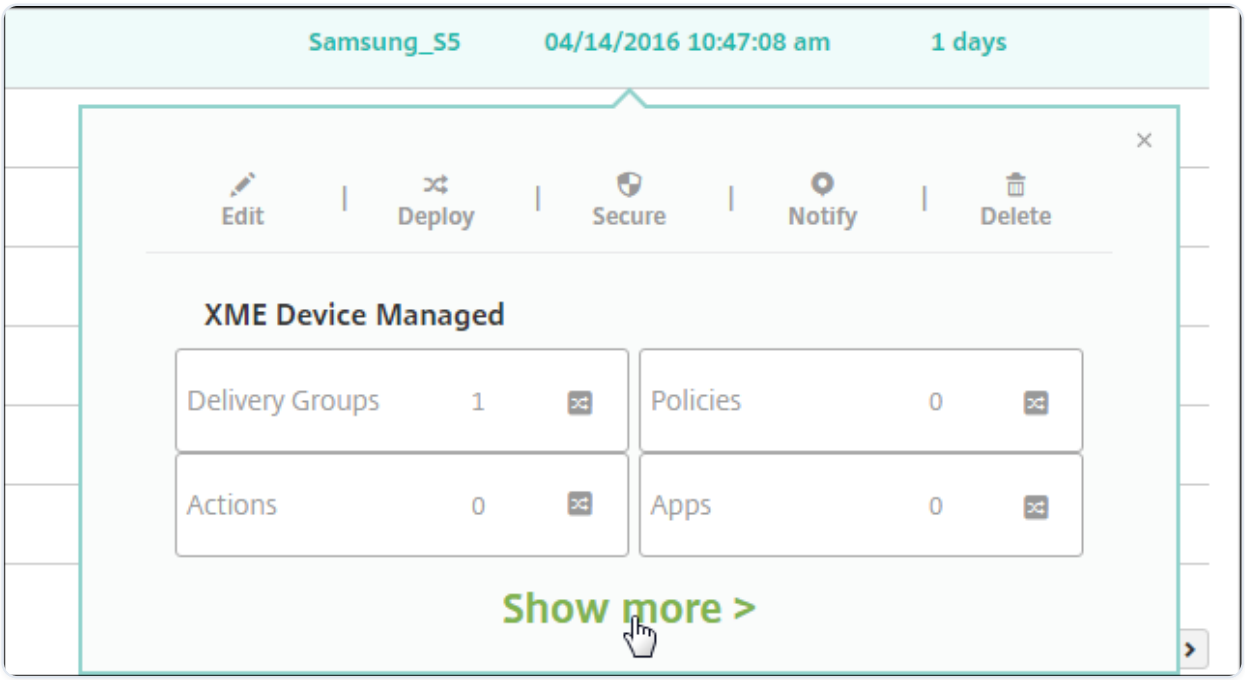
   > **注意：**
   >
   > 如果将触发器设置为**事件**，则重复间隔将自动设置为最短 1 小时。设备必须刷新策略才能与服务器同步以接收通知。通常，设备会在用户登录或通过 Secure Hub 手动刷新其策略时与服务器同步。
   >
   > 在执行任何操作之前，可能会出现大约 1 小时的额外延迟，以允许 Active Directory 数据库与 XenMobile 同步。



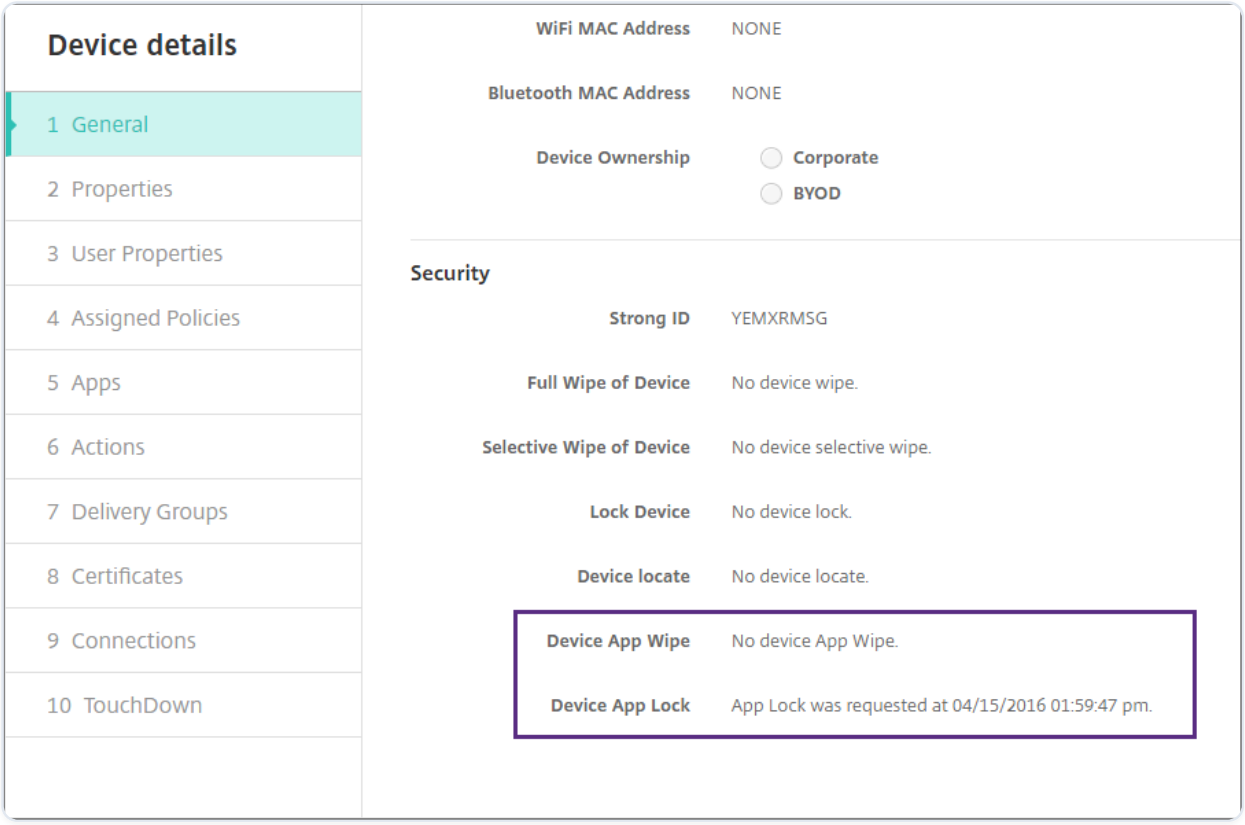
6. 配置部署规则，然后单击**下一步**。
7. 配置交付组分配和部署计划，然后单击**下一步**。
8. 单击**保存**。

检查应用程序锁定或应用程序擦除状态

1. 转到**管理 > 设备**，单击设备，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**。



设备擦除后，系统会提示用户输入 PIN 码。如果用户忘记了代码，您可以在“设备详细信息”中查找。

监视和支持

您可以使用 XenMobile® 仪表板和 XenMobile 支持页面来监视和故障排除 XenMobile Server。使用 XenMobile 支持页面可访问支持相关信息和工具。

对于本地 XenMobile Server，您还可以从 XenMobile CLI 执行操作。有关详细信息，请参阅命令行界面选项。

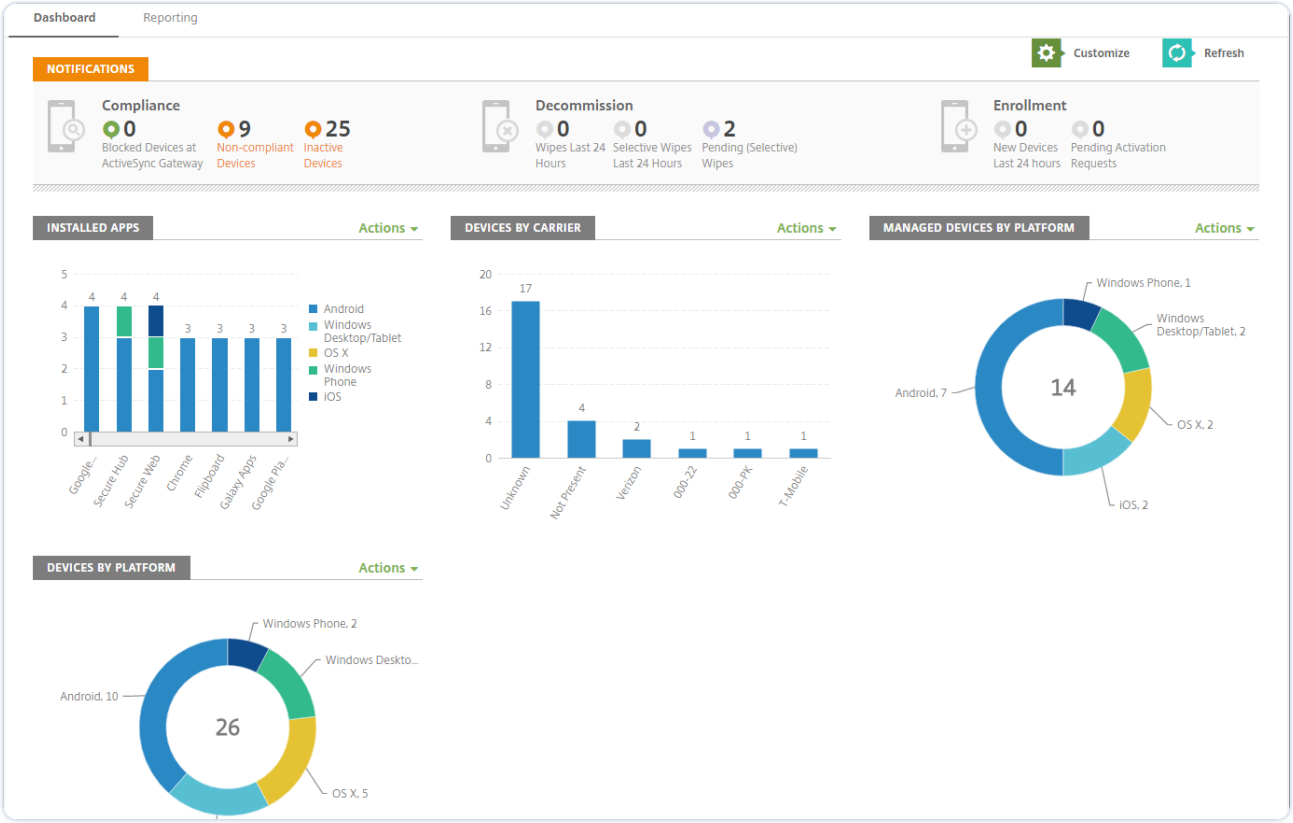
在 XenMobile 控制台中，单击右上角的扳手图标。

此时将显示“故障排除和支持”页面。

使用 XenMobile **支持**页面可执行以下操作：

- 访问诊断。
- 创建支持包（仅限本地安装）。
- 访问指向 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。
- 访问一组工具和实用程序。

您还可以通过访问 XenMobile 控制台仪表板快速查看信息。借助此信息，您可以通过使用小组件快速查看问题和成功之处。



仪表板通常是您登录 XenMobile 控制台时首先出现的页面。要从控制台的其他位置访问仪表板，请单击“**分析**”。在仪表板上单击“**自定义**”以编辑页面布局和显示的微件。

- **我的仪表板：** 最多可以保存四个仪表板。您可以单独编辑这些仪表板，并通过选择已保存的仪表板来查看每个仪表板。
- **布局样式：** 在此行中，您可以选择仪表板上显示的微件数量以及微件的布局方式。
- **微件选择：** 您可以选择要在仪表板上显示的信息。
  - **通知：** 选中左侧数字上方的复选框，可在微件上方添加一个通知栏。此栏显示合规设备、非活动设备以及在过去 24 小时内已擦除或注册的设备数量。
  - **按平台划分的设备：** 按平台显示托管设备和非托管设备的数量。
  - **按运营商划分的设备：** 按运营商显示托管设备和非托管设备的数量。单击每个条形图可按平台查看详细信息。
  - **按平台划分的托管设备：** 按平台显示托管设备的数量。
  - **按平台划分的非托管设备：** 按平台显示非托管设备的数量。此图表中显示的设备可能已安装代理，但其权限已被撤销或已被擦除。
  - **按 ActiveSync 网关状态划分的设备：** 显示按 ActiveSync 网关状态分组的设备数量。信息显示“已阻止”、“已允许”或“未知”状态。您可以单击每个条形图按平台细分数据。
  - **按所有权划分的设备：** 显示按所有权状态分组的设备数量。信息显示“公司所有”、“员工所有”或“未知”所有权状态。

- **失败的交付组部署：** 显示每个软件包的失败部署总数。仅显示部署失败的软件包。
- **按阻止原因划分的设备：** 显示 ActiveSync 阻止的设备数量
- **已安装的应用程序：** 键入应用程序名称以获取应用程序信息图表。
- **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。

对于每个小组件，您可以单击各个部分以深入了解更多信息。

分析仪表板深入探查的图像(/en-us/xenmobile/server/media/analyze-dashboard-drill-down.png)

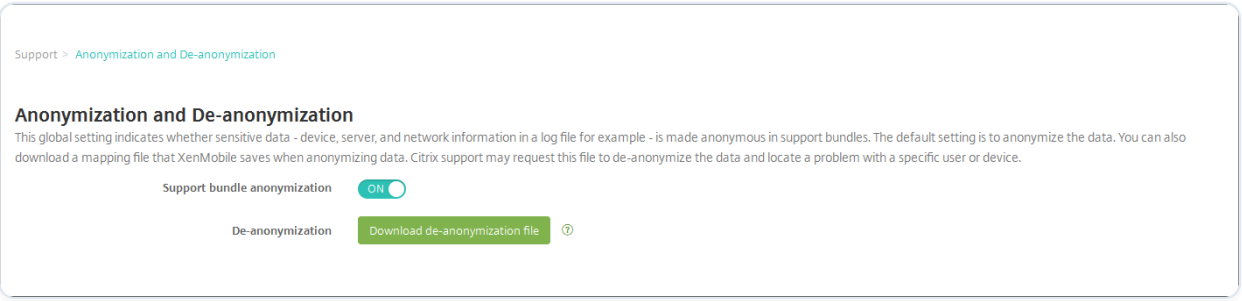
您还可以通过单击“**操作**”菜单将信息导出为 .csv 文件。

分析仪表板菜单的图像(/en-us/xenmobile/server/media/analyze-dashboard-actions-menu.png)

匿名化支持包中的数据

在 XenMobile® 中创建支持包时，敏感的用户、服务器和网络数据默认会被匿名化。您可以在“匿名化和去匿名化”页面上更改此行为。您还可以下载 XenMobile 在匿名化数据时保存的映射文件。Citrix® 支持人员可以请求此文件以去匿名化数据，并查找特定用户或设备的问题。

1. 在 XenMobile 控制台中，单击右上角的扳手图标。将显示“**支持**”页面。
2. 在“**支持**”页面上，在“**高级**”下，单击“**匿名化和去匿名化**”。将显示“**匿名化和去匿名化**”页面。



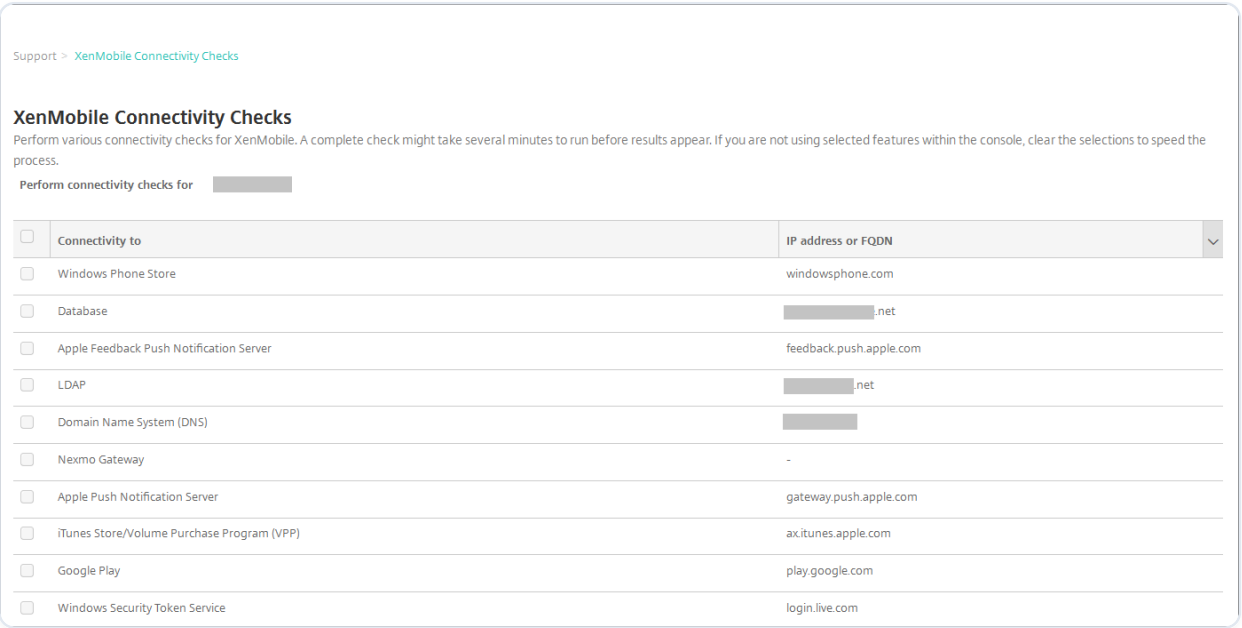
3. 在“**支持包匿名化**”中，选择数据是否匿名化。默认设置为“**开**”。
4. 在“**去匿名化**”旁边，单击“**下载去匿名化文件**”以下载映射文件，以便在 Citrix 支持人员需要特定设备或用户信息来诊断问题时发送给他们。

连接性检查

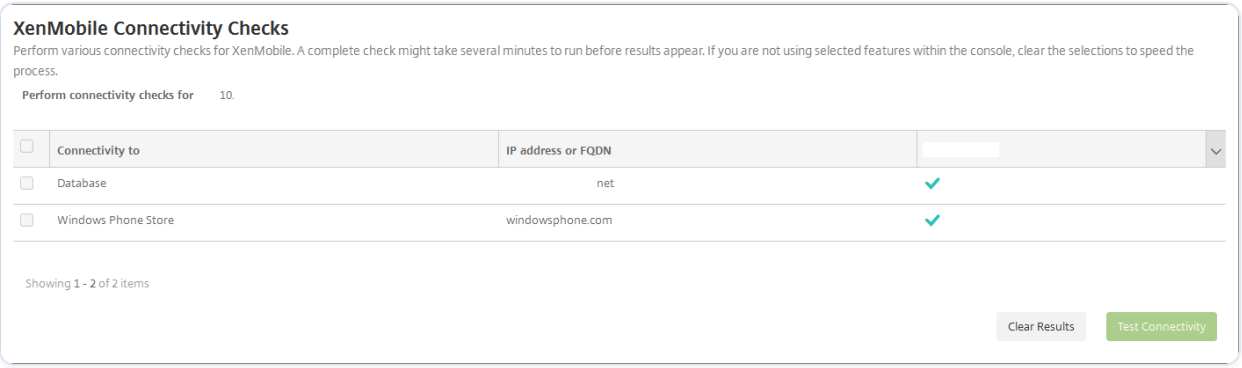
在 XenMobile® 的“**支持**”页面上，您可以检查 XenMobile 与 Citrix Gateway 以及其他服务器和位置的连接。

执行 XenMobile 连接性检查

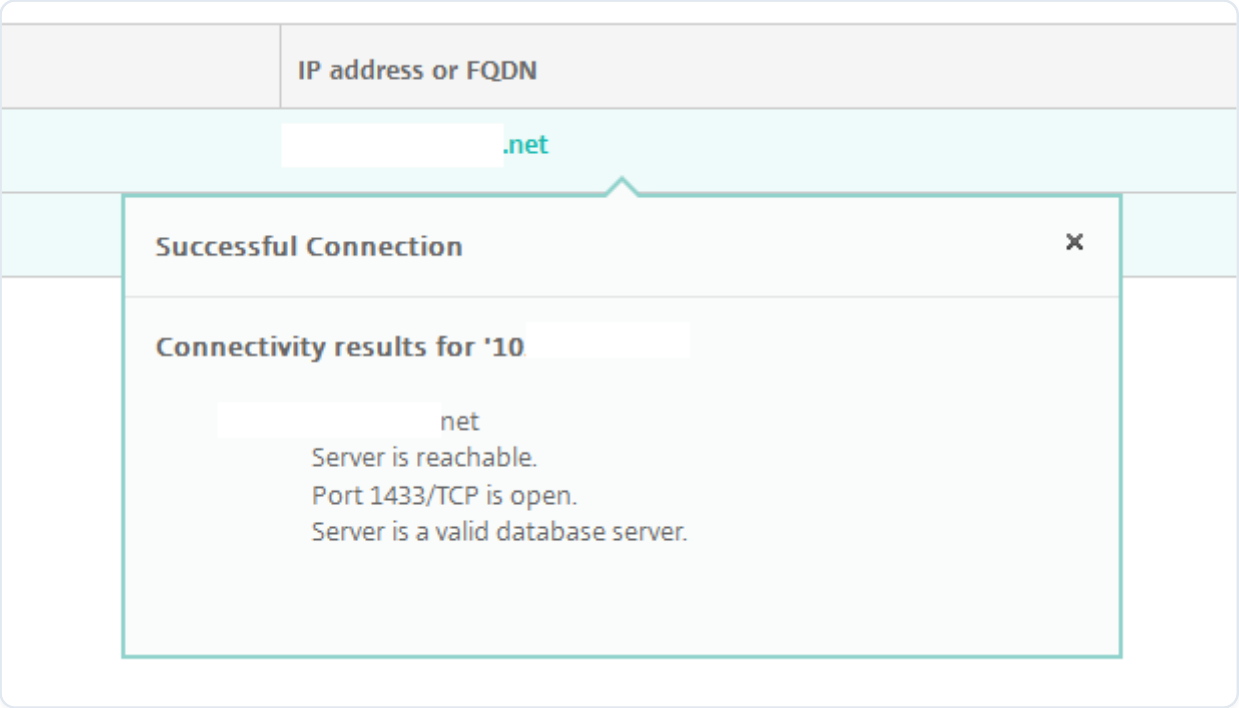
1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。此时将显示“**支持**”页面。
2. 在“**诊断**”下，单击“**XenMobile 连接性检查**”。此时将显示“**XenMobile 连接性检查**”页面。如果您的 XenMobile 环境具有群集节点，则会显示所有节点。



3. 选择要包含在连接性测试中的服务器，然后单击“**测试连接**”。此时将显示测试结果页面。

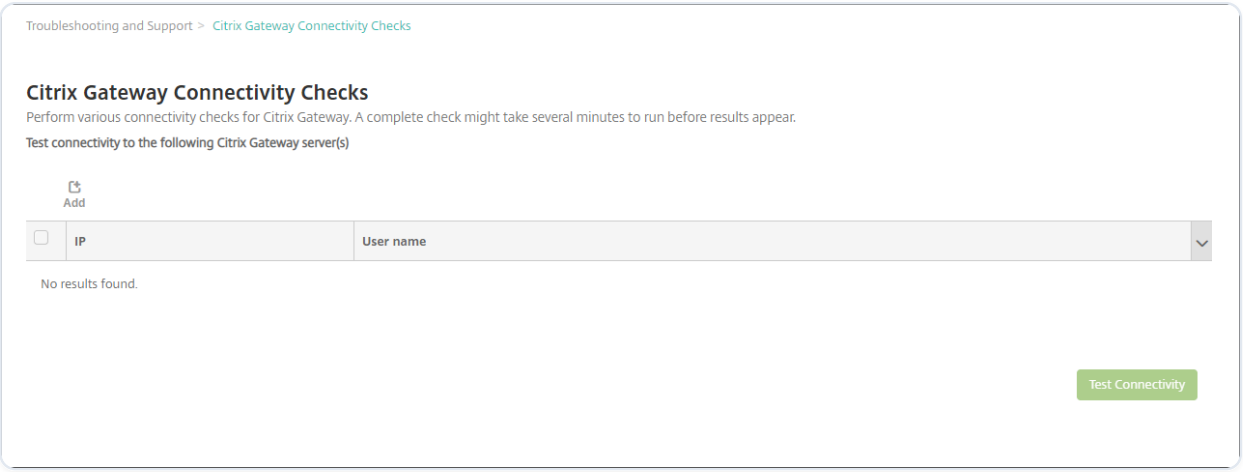


4. 在测试结果表中选择一个服务器以查看该服务器的详细结果。

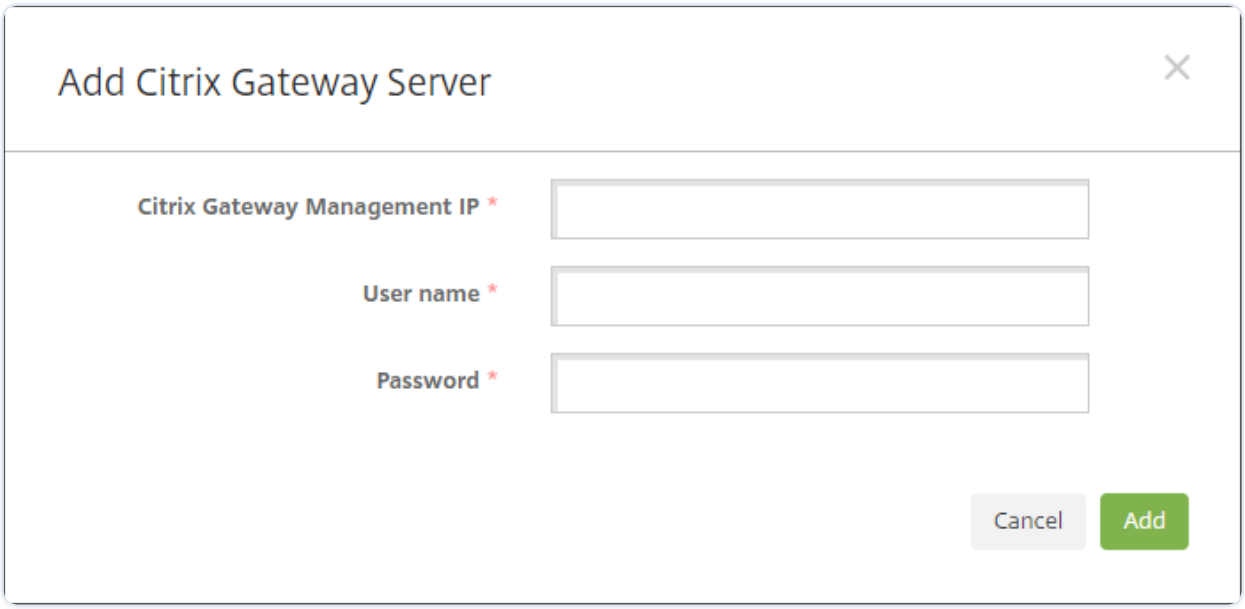


执行 Citrix Gateway 连接性检查

1. 在“**支持**”页面上的“**诊断**”下，单击“**Citrix Gateway 连接性检查**”。此时将显示“**Citrix Gateway 连接性检查**”页面。如果您尚未添加任何 Citrix Gateway 服务器，则该表为空。



2. 单击“**添加**”。此时将显示“**添加 Citrix Gateway 服务器**”对话框。



3. 在 **Citrix Gateway 管理 IP** 中，键入您要测试的运行 Citrix Gateway 的服务器的管理 IP 地址。

> **注意：**
>
> 如果您正在对之前已添加的 Citrix Gateway 服务器执行连接性检查，则会提供 IP 地址。

4. 键入此 Citrix Gateway 的管理员凭据。

> **注意：**
>
> 如果您正在对之前已添加的 Citrix Gateway 服务器执行连接性检查，则会提供用户名。

5. 单击 **添加**。Citrix Gateway 将添加到 **Citrix Gateway 连接性检查** 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。

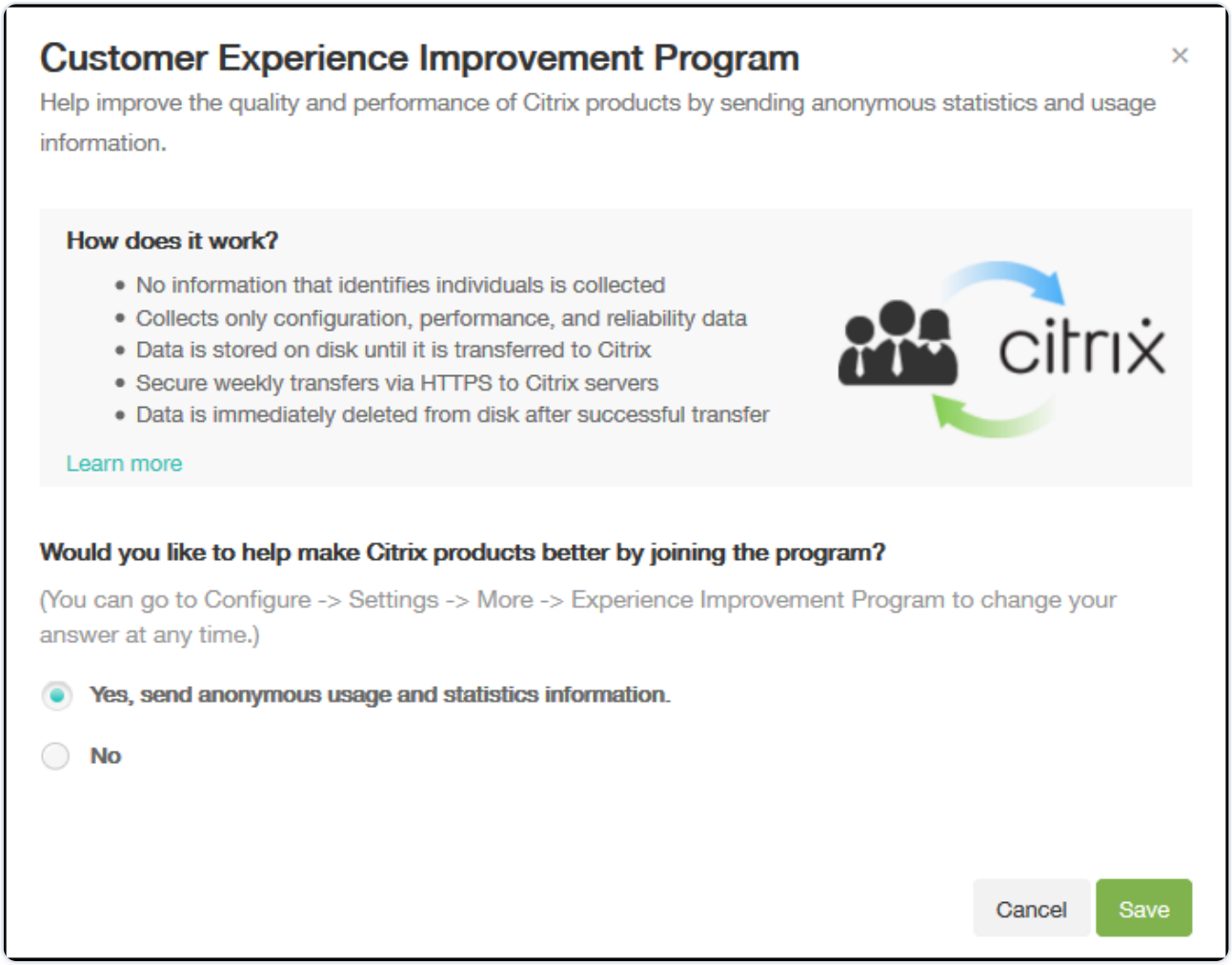
客户体验改善计划

Citrix 客户体验改善计划 (CEIP) 收集 XenMobile 的匿名配置和使用数据，并自动将数据发送给 Citrix。此数据有助于 Citrix 提高 XenMobile 的质量、可靠性和性能。参与 CEIP 是自愿的。首次安装 XenMobile 或安装更新时，您可以选择参与 CEIP。当您选择加入时，数据通常每周收集一次，性能和使用数据每小时收集一次。数据存储在磁盘上，并通过 HTTPS 每周安全地传输到 Citrix。您

可以在 XenMobile 控制台中更改是否参与 CEIP。有关 CEIP 的更多信息，请参阅关于 Citrix 客户体验改善计划 (CEIP)。

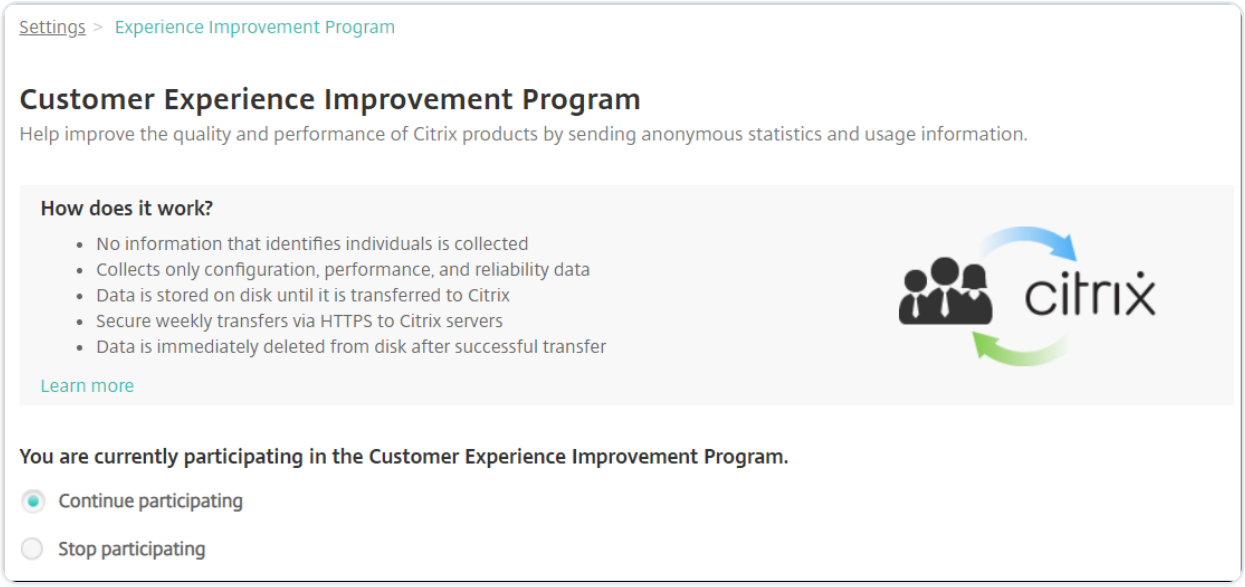
选择参与 CEIP

首次安装 XenMobile® 或执行更新时，您会看到以下对话框，提示您参与。



更改 CEIP 参与设置

1. 要在 XenMobile 控制台中更改 CEIP 参与设置，请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，单击“**体验改善计划**”。“**客户体验改善计划**”页面随即显示。您看到的具体页面取决于您当前是否参与 CEIP。

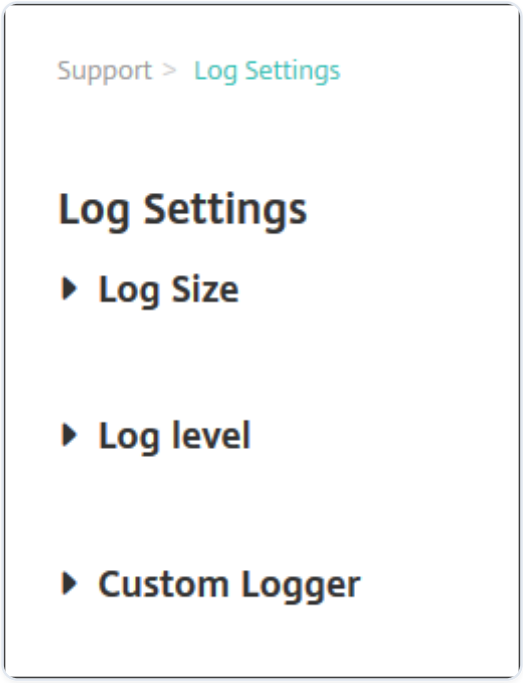


3. 如果您当前正在参与 CEIP 并希望停止，请单击“**停止参与**”。
4. 如果您当前未参与 CEIP 并希望开始，请单击“**开始参与**”。
5. 单击“**保存**”。

日志

您可以配置日志设置，以自定义 XenMobile® 生成的日志输出。如果您有群集 XenMobile 服务器，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。**支持**页面随即显示。
2. 在**日志操作**下，单击**日志设置**。**日志设置**页面随即显示。

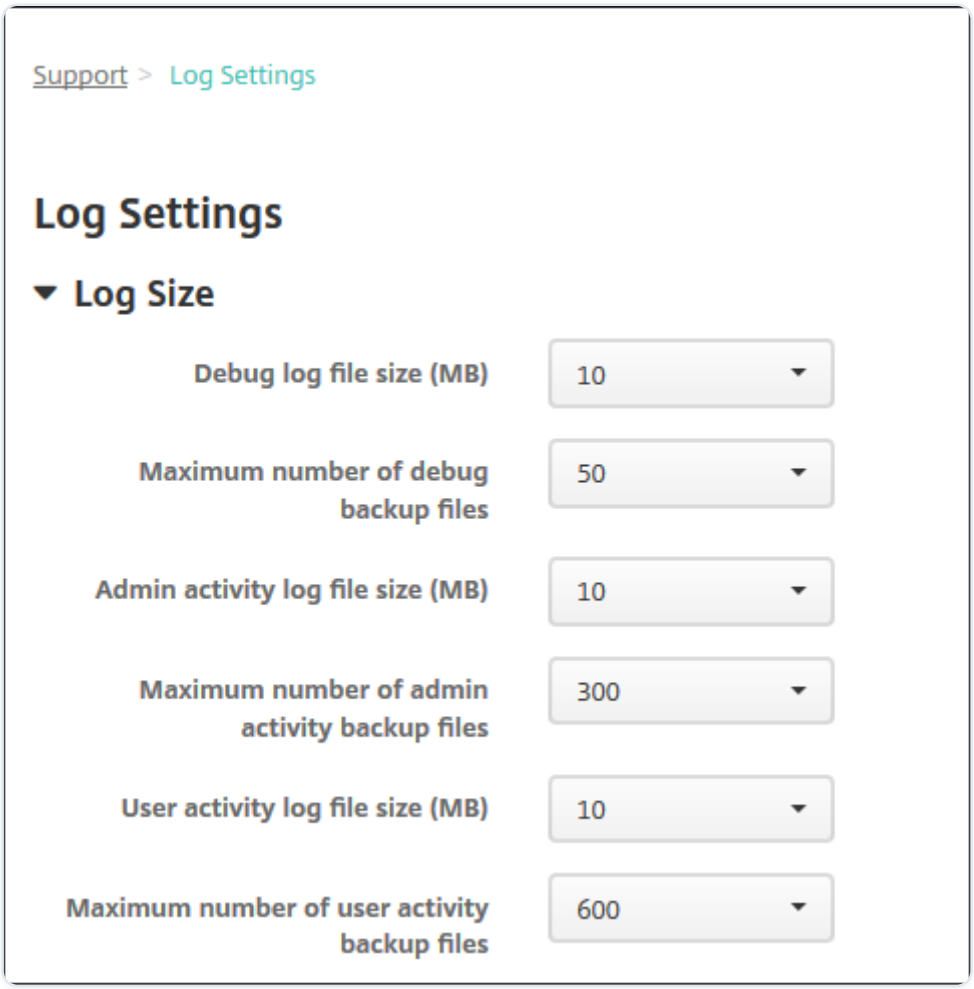


在**日志设置**页面上，您可以访问以下选项：

- **日志大小**。使用此选项可控制日志文件的大小以及数据库中保留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、管理员活动日志和用户活动日志）。
- **日志级别**。使用此选项可更改日志级别或保留设置。
- **自定义记录器**。使用此选项可创建自定义记录器；自定义日志需要类名和日志级别。

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：

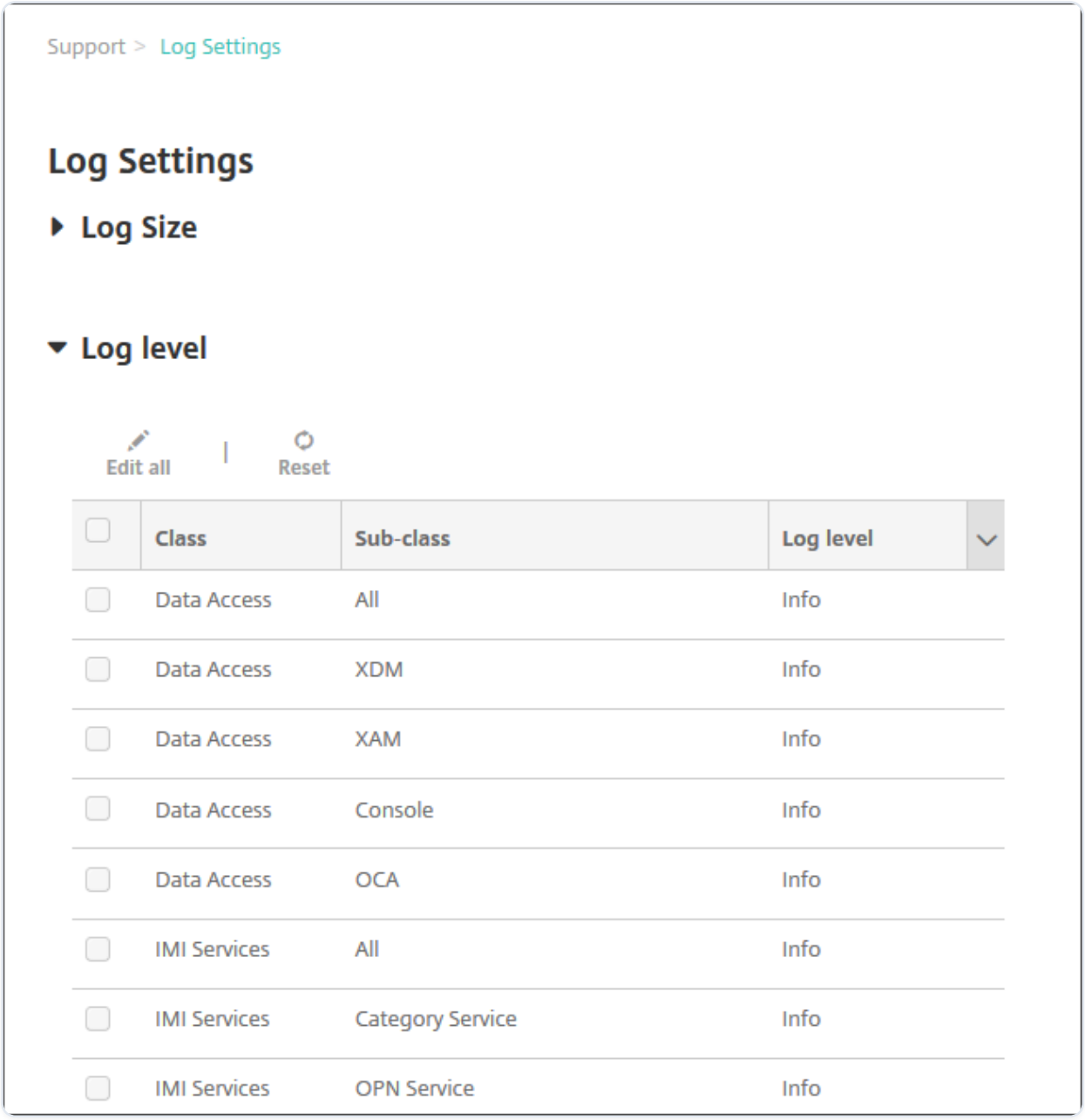
- **调试日志文件大小 (MB)：** 在列表中，单击 5 MB 到 20 MB 之间的某个大小以更改调试文件的最大大小。默认文件大小为 **10 MB**。
- **调试备份文件最大数量：** 在列表中，单击服务器保留的调试文件最大数量。默认情况下，XenMobile 在服务器上保留 50 个备份文件。
- **管理员活动日志文件大小 (MB)：** 在列表中，单击 5 MB 到 20 MB 之间的某个大小以更改管理员活动文件的最大大小。默认文件大小为 **10 MB**。

- **管理员活动备份文件的最大数量：** 在列表中，单击服务器保留的管理员活动文件的最大数量。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 之间的某个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**。
- **用户活动备份文件的最大数量：** 在列表中，单击服务器保留的用户活动文件的最大数量。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

日志级别允许您指定 XenMobile 在日志中收集的信息类型。您可以为所有类设置相同的级别，也可以为单个类设置特定级别。

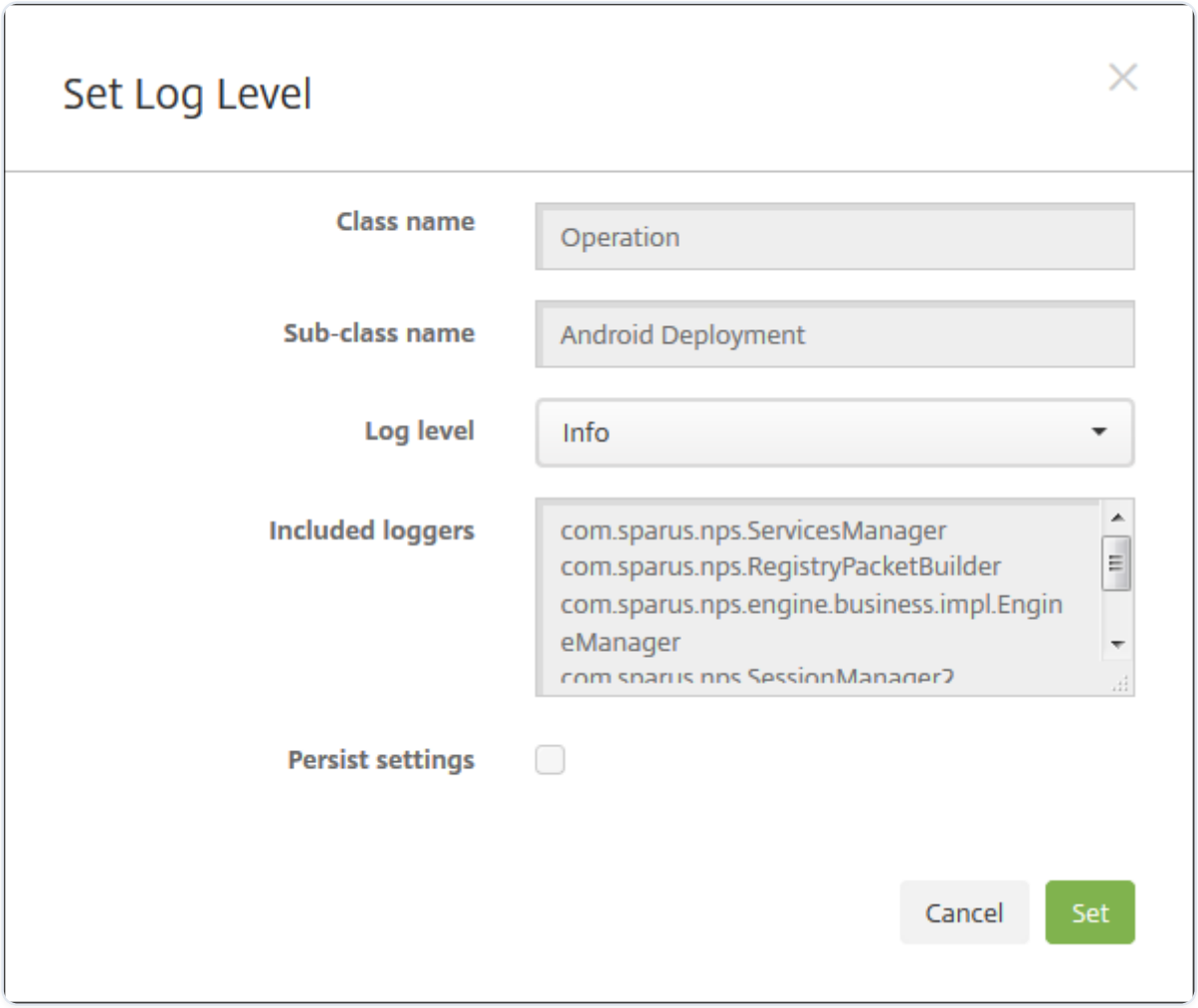
1. 在 **日志设置** 页面上，展开 **日志级别**。将显示所有日志类的表。



2. 执行以下操作之一：

   - 单击一个类旁边的复选框，然后单击 **设置级别** 以更改此类的日志级别。
   - 单击 **编辑** 全部以将日志级别更改应用于表中的所有类。

   将显示 **设置日志级别** 对话框，您可以在其中设置日志级别并选择在重新启动 XenMobile Server 时是否保留日志级别设置。



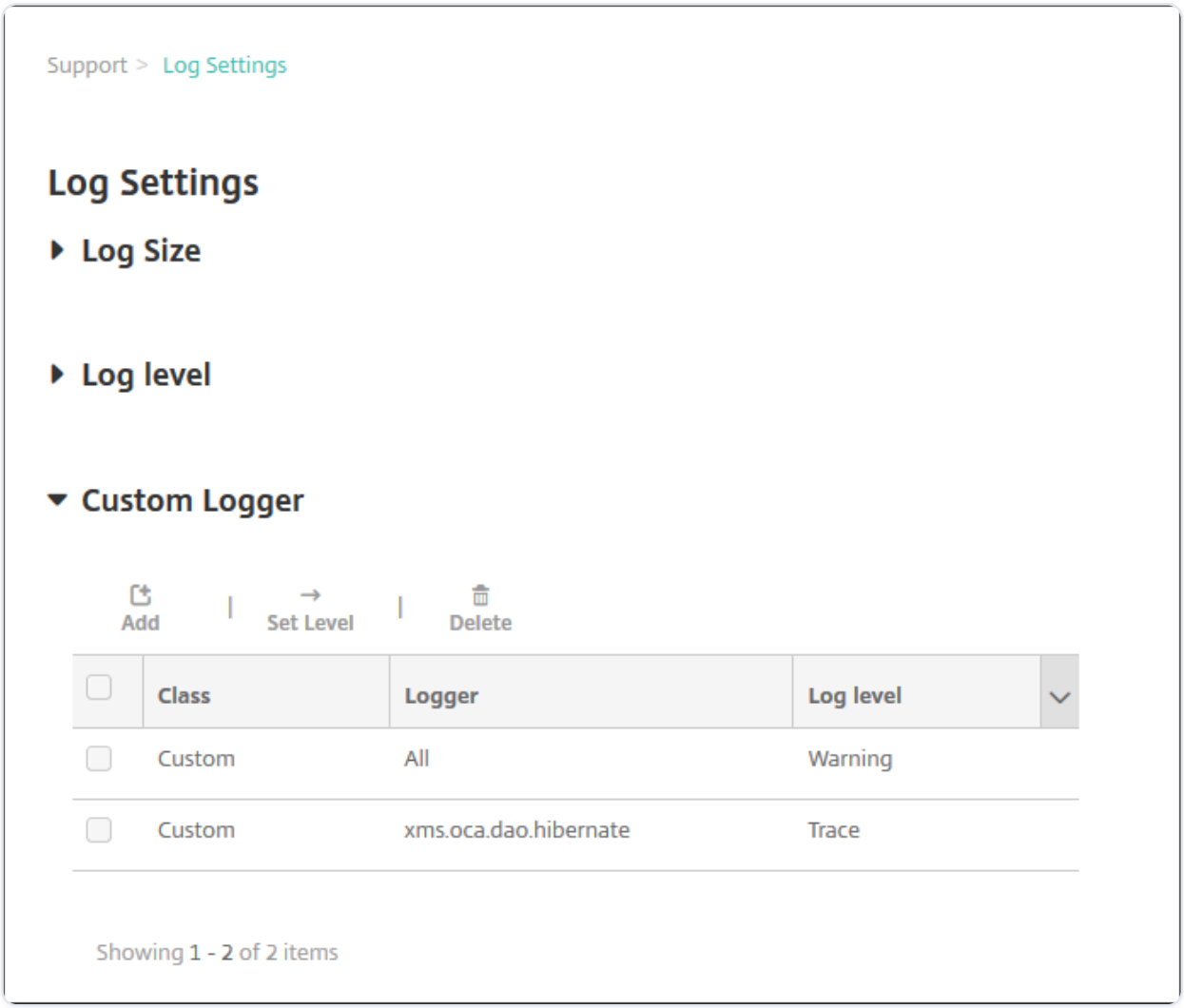
- **类名称**：当您更改所有类的日志级别时，此字段显示 **全部**，或者显示单个类名称。它不可编辑。
- **子类名称**：当您更改所有类的日志级别时，此字段显示 **全部**，或者显示单个类的子类名称。它不可编辑。
- **日志级别**：在列表中，单击一个日志级别。支持的日志级别包括：
  - 致命
  - 错误
  - 警告
  - 信息
  - 调试
  - 跟踪
  - 关闭
- **包含的记录器**：当您更改所有类的日志级别时，此字段为空；或者它显示单个类当前配置的记录器。此字段不可编辑。

- **保留设置**：如果您希望日志级别设置在服务器重新启动时保留，请选中此复选框。不选中此复选框意味着日志级别设置在服务器重新启动时将恢复为默认值。

3. 单击“**设置**”以提交您的更改。

添加自定义记录器

1. 在“**日志设置**”页面上，展开“**自定义记录器**”。将显示“**自定义记录器**”表。如果您尚未添加任何自定义记录器，则该表最初为空。



2. 单击“**添加**”。将显示“**添加自定义记录器**”对话框。

   记录配置的图像(/en-us/xenmobile/server/media/support-log-settings-custom-logger-add.png)

3. 配置以下设置：

   - **类名**： 此字段显示 **自定义**。不可编辑。
   - **日志级别**： 在列表中，单击一个日志级别。支持的日志级别包括：
     - 致命

  - 错误
  - 警告
  - 信息
  - 调试
  - 跟踪
  - 关闭

- **包含的日志记录器：** 键入要包含在自定义日志记录器中的特定日志记录器，或将此字段留空以包含所有日志记录器。

4. 单击 **添加**。自定义日志记录器将添加到 **自定义日志记录器** 表中。

   记录配置的图像(/en-us/xenmobile/server/media/support-log-settings-custom-logger-table.png)

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，询问您是否要删除自定义记录器。单击**确定**。

> **重要提示：**
>
> 此操作无法撤消。

移动服务提供商

您可以启用 XenMobile® 使用移动服务提供商界面来查询 BlackBerry 和 Exchange ActiveSync 设备并执行操作。

例如，您的组织可能有 1,000 名用户，每位用户可能使用一台或多台设备。在您通知所有用户必须将其设备注册到 XenMobile 进行管理后，XenMobile 控制台会显示用户注册的设备数量。通过配置此设置，您可以确定有多少设备连接到 Exchange Server。通过这种方式，您可以执行以下操作：

- 确定是否有任何用户仍需注册其设备。
- 向连接到 Exchange Server 的用户设备发出命令，例如数据擦除。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。**设置**页面随即显示。
2. 在**服务器**下，单击**移动服务提供商**。**移动服务提供商**页面随即显示。

移动服务提供商页面图像(/en-us/xenmobile/server/media/settings-server-mobile-service-provider.png)

3. 配置以下设置：

   - **Web 服务 URL：** 键入 Web 服务的 URL；例如，`https://<XmmServer>/services/xdmservice`
   - **用户名：** 键入格式为 domain\\admin 的用户名。
   - **密码：** 键入密码。
   - **自动更新 BlackBerry 和 ActiveSync 设备连接：** 选择是否自动更新设备连接。默认设置为**关闭**。
   - 单击**测试连接**以验证连接。

4. 单击**保存**。

报告

XenMobile® 提供以下预定义报告，可让您分析应用程序和设备部署。每个报告都以表格和图表的形式显示。您可以按列对表格进行排序和筛选。您可以选择图表中的元素以获取更详细的信息。

- **应用程序部署尝试总数：** 列出用户尝试在其设备上安装的已部署应用程序。
- **按平台列出的应用程序：** 按设备平台和版本列出应用程序和应用程序版本。
- **按类型列出的应用程序：** 按版本、类型和类别列出应用程序。
- **设备注册：** 列出所有已注册设备。
- **设备和应用程序：** 列出正在运行托管应用程序的设备。
- **非活动设备：** 列出在 XenMobile Server 属性 device.inactivity.days.threshold 指定的天数内没有任何活动的设备。
- **越狱/Root 设备：** 列出已越狱的 iOS 设备和已 Root 的 Android 设备。
- **条款和条件：** 列出已接受和拒绝条款和条件协议的用户。您可以选择图表区域以查看更多详细信息。
- **十大应用程序：** 部署失败 - 列出最多 10 个部署失败的应用程序。
- **按设备和用户列出的黑名单应用程序：** 列出用户设备上的被阻止应用程序。

> **注意：**

> XenMobile Server 控制台包含“黑名单”和“白名单”术语。我们将在即将发布的版本中将这些术语更改为“阻止列表”和“允许列表”。

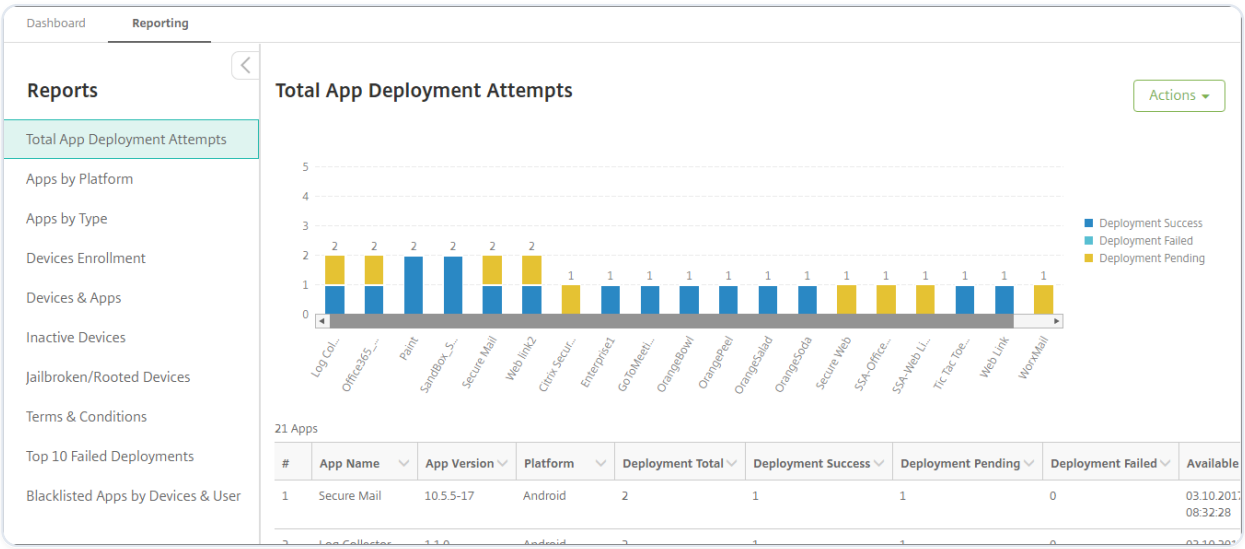
- **不合规设备：** 列出不符合合规性标准的设备，例如设备是否已越狱、正在运行的操作系统版本以及设备是否有密码。

您可以将每个表中的数据导出为 .csv 格式，该格式可以使用 Microsoft Excel 等程序打开。您可以将每个报告的图表导出为 PDF 格式。

- **前 100 个已安装应用程序：** 列出每个平台最多 100 个已安装的应用程序。有关详细信息，请参阅服务器属性

生成报告

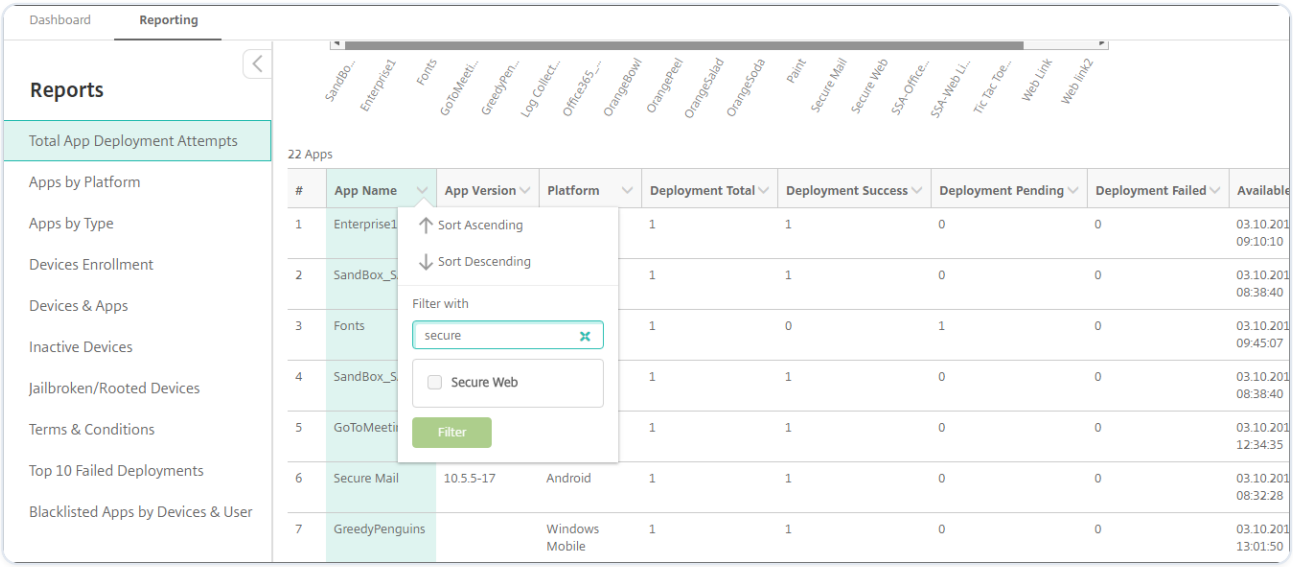
1. 在 XenMobile 控制台中，单击 **分析 > 报告**。将显示**报告**页面。
2. 单击要生成的报告。



查看报告的更多详细信息

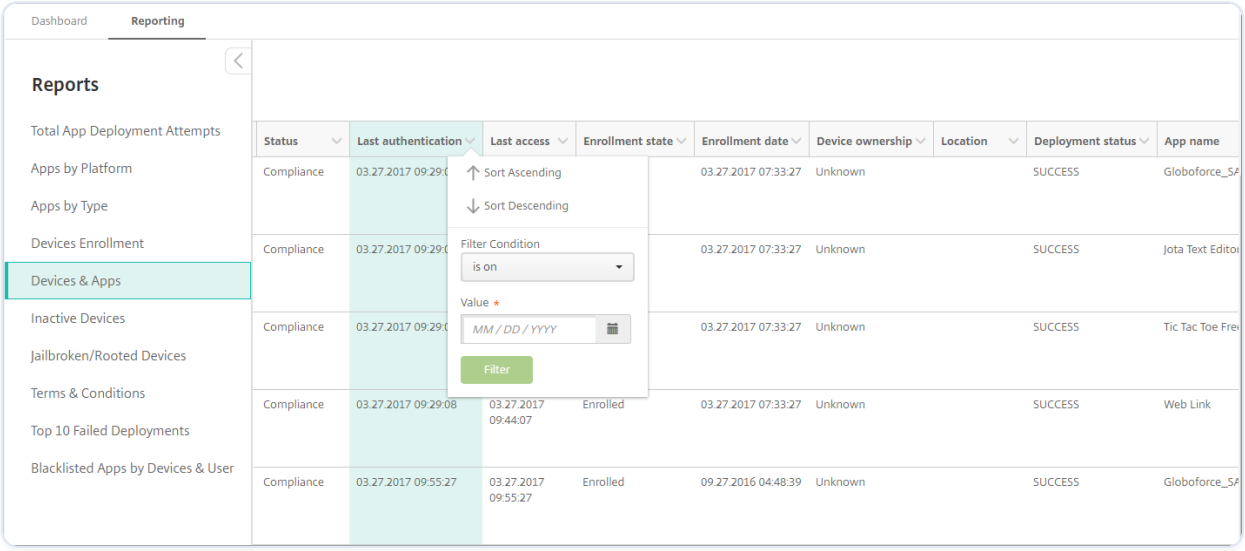
1. 单击图表区域以向下钻取并查看更详细的信息。

要对表列进行排序、筛选或搜索，请单击列标题

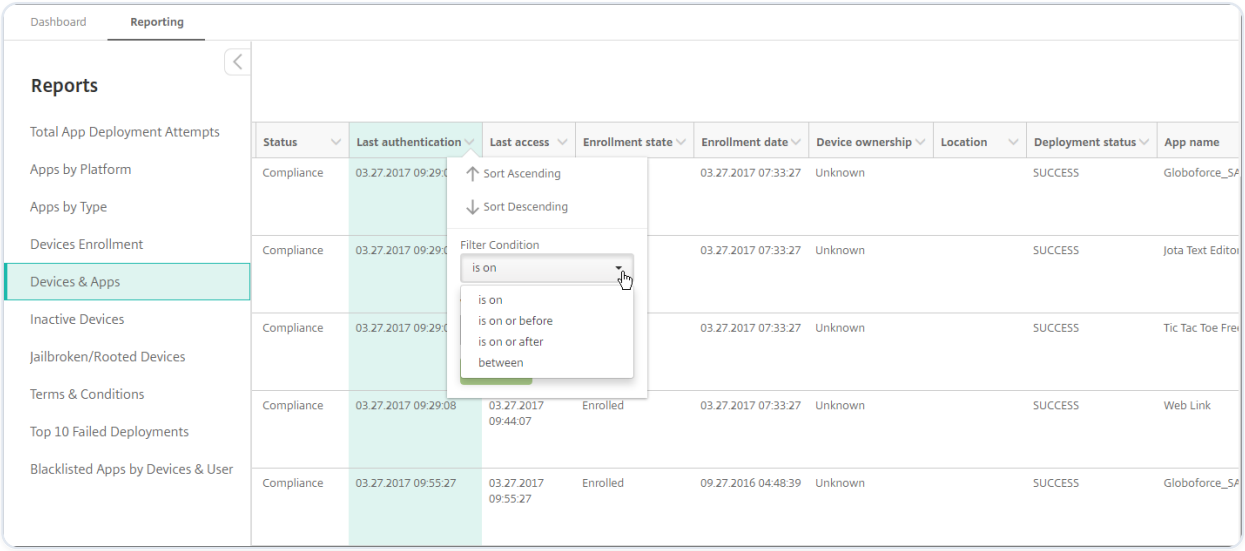


按日期筛选报告

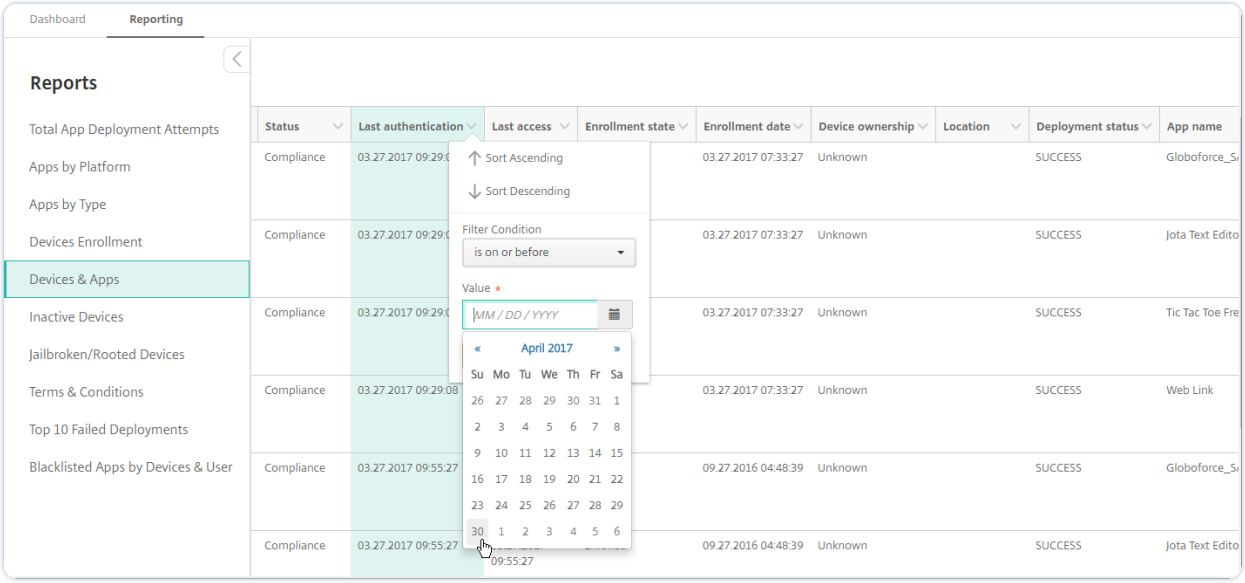
1. 单击列标题以查看筛选设置。



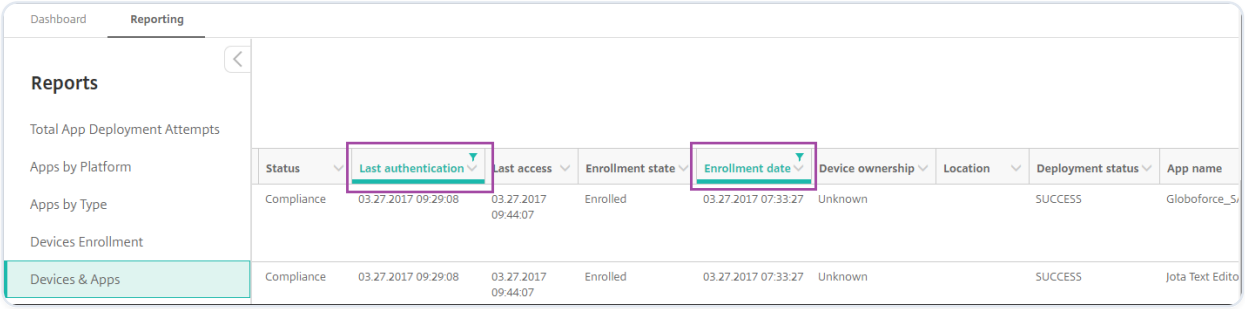
2. 从**筛选条件**中，选择要如何限制报告的日期。



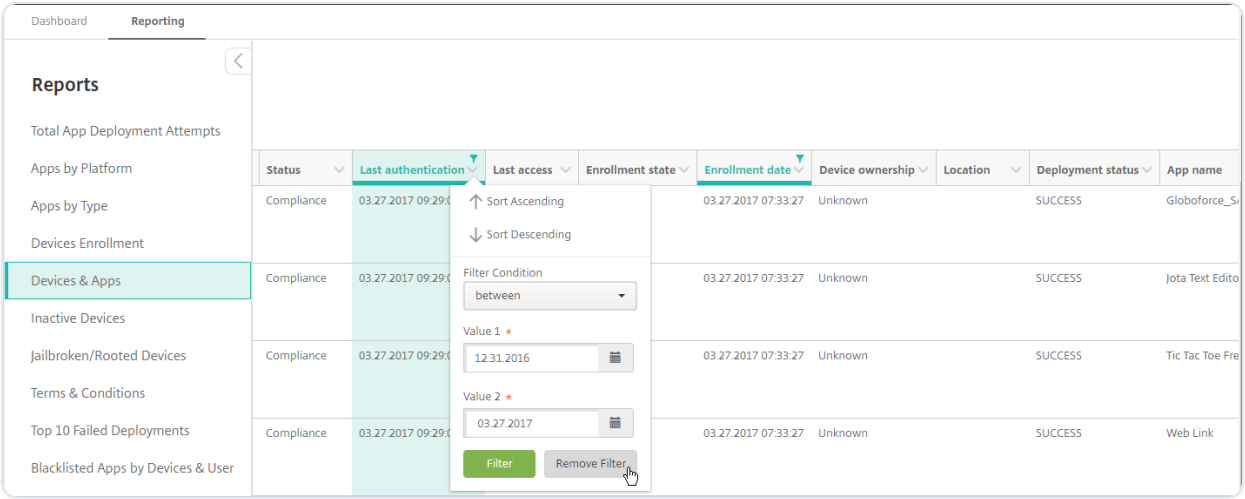
3. 使用日期选择器指定日期。



4. 带有日期筛选器的列显示如下例所示。

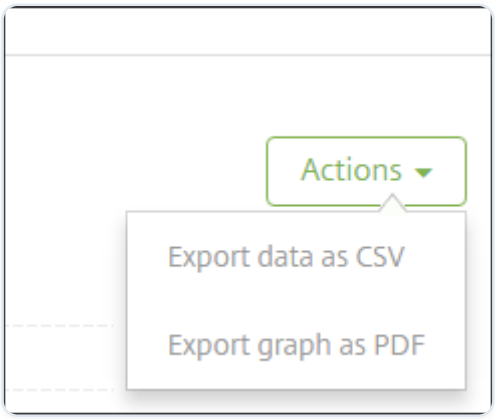


5. 要删除筛选器，请单击列标题，然后单击**删除筛选器**。



导出图表或表格

- 要以 PDF 格式导出图表，请单击**操作**，然后单击**将图表导出为 PDF**。
- 要以 CSV 格式导出表格数据，请单击**操作**，然后单击**将数据导出为 CSV**。



重要提示：

尽管可以使用 SQL Server 创建自定义报表，但 Citrix® 不建议使用此方法。Citrix 不会发布架构，并且可以在不通知的情况下更改架构。如果您确实决定采用此报表方法，请确保使用只读

> 帐户运行 SQL 查询。具有多个 JOIN 且需要一些时间才能运行的查询会在此期间影响 XenMobile Server 性能。

SNMP 监控

您可以在 XenMobile Server 中启用 SNMP 监控，以允许监控系统查询和获取有关 XenMobile 节点的信息。查询使用处理器负载、平均负载、内存使用情况和连接性等参数。有关 SNMP v3 的更多信息，例如身份验证和加密规范，请参阅 RFC 3414 的官方 SNMP 文档。

> **注意：**

> XenMobile Server 10.8 及更高版本支持 SNMP v3 监控。

> 您可以使用各种支持 SNMP 监控的监控应用程序，例如 SCOM。有关配置 SCOM 的详细信息，请参阅这篇 Citrix 支持知识中心文章。

先决条件

配置以下 TCP 端口：

- **端口 161 (UDP)：** 用于使用 UDP 协议的 SNMP 流量。源是 SNMP 管理器，目标是 XenMobile。
- **端口 162 (UDP)：** 用于将 SNMP 陷阱警报从 XenMobile 发送到 SNMP 管理器。源是 XenMobile，目标是 SNMP 管理器。

有关 XenMobile 端口配置的更多信息，请参阅 端口要求。

要查看包含 SNMP 的本地 XenMobile 部署的架构图，请参阅 本地部署的参考架构。

设置 SNMP 的一般步骤如下。

1. **添加用户：** 用户继承接收陷阱和监控 XenMobile Server 的权限。
2. **添加 SNMP 管理器以接收陷阱：** 陷阱是当您的 XenMobile 节点超出用户定义的阈值上限时 XenMobile 生成的警报。
3. **配置 SNMP 管理器以与 XenMobile 交互：** XenMobile Server 使用某些管理信息库 (MIB) 来执行操作。您可以从 XenMobile 控制台中的**设置 > SNMP 配置**页面下载 MIB。然后，使用 MIB 导入器将 MIB 导入 SNMP 管理器。

> **注意：**
>
> 每个 SNMP 管理器都有自己的 MIB 导入器。

4. **启用陷阱：** 您可以在 XenMobile 控制台中启用陷阱，并根据您的环境定义间隔和阈值。
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，您可以配置设置以启用管理器外部的通知。例如，您可以配置通知以在电子邮件中显示。

您可以从 XenMobile 生成以下陷阱。

陷阱名称： 处理器负载

- **监控对象 ID (OID)：** .1.3.6.1.2.1.25.3.3.1.2
- **描述：** 监控系统在用户定义的间隔内的 CPU 负载。如果负载超过自定义阈值，XenMobile 会生成 SNMP 陷阱。

陷阱名称： 一分钟平均负载

- **监控对象 ID (OID)：** .1.3.6.1.4.1.2021.10.1.5.1
- **描述：** 监控系统在用户定义的间隔内一分钟的平均负载。如果平均负载超过自定义阈值，XenMobile 会生成 SNMP 陷阱。

陷阱名称： 五分钟平均负载

- **监控对象 ID (OID)：** .1.3.6.1.4.1.2021.10.1.5.2
- **描述：** 监控系统在用户定义的间隔内五分钟的平均负载。如果平均负载超过自定义阈值，XenMobile 会生成 SNMP 陷阱。

陷阱名称： 十五分钟平均负载

- **监控对象 ID (OID)：** .1.3.6.1.4.1.2021.10.1.5.3
- **描述：** 监视每个用户定义的时间间隔内 15 分钟的平均系统负载。如果平均负载超过自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称： 总可用内存

- **监控对象 ID (OID)：** .1.3.6.1.4.1.2021.4.11
- **描述：** 监视每个用户定义的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：总可用内存包括 RAM 和交换内存（虚拟内存）。要检索总交换内

存，可以使用 SNMP OID .1.3.6.1.4.1.2021.4.3 进行查询。要检索可用交换内存，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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.2021.9.1.9.1
- **描述：** 监视每个用户定义的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 堆内存使用情况

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.2.4.0
- **描述：** 监视每个用户定义的时间间隔内 XenMobile 的 Java 虚拟机 (JVM) 堆内存使用情况。如果使用量超过自定义阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Java 元空间使用情况

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.2.5.0
- **描述：** 监视每个用户定义的时间间隔内 XenMobile 的 Java 元空间使用情况。如果使用量超过阈值，XenMobile 将生成 SNMP 陷阱。

陷阱名称： LDAP 连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **描述：** 监控 LDAP 服务器与 XenMobile 节点之间在每个用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： DNS 连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **描述：** 监控 DNS 服务器与 XenMobile 节点之间在每个用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Google Store 服务器连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **描述：** 监控 Google Store 服务器与 XenMobile 节点之间在每个用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Windows Tab Store 连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.5.0

- **描述：** 监控 Tab Store 服务器与 XenMobile 节点之间在用户定义的时间间隔内的连接。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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **描述：** 监控 Windows 安全令牌服务器与 XenMobile 节点之间在用户定义的时间间隔内的连接。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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **描述：** 监控 Windows 通知服务器与 XenMobile 节点之间在用户定义的时间间隔内的连接。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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **描述：** 监控 APNs 与 XenMobile 节点之间在用户定义的时间间隔内的连接。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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **描述：** 监控 Apple 反馈服务器与 XenMobile 节点之间在用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Apple Store 服务器连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **描述：** 监控 Apple Store 服务器与 XenMobile 节点之间在用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： XenMobile 数据库连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- **描述：** 监控 XenMobile 数据库与 XenMobile 节点之间在用户定义的时间间隔内的连接。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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.12.0

- **描述：** 监控 Firebase Cloud Messaging 服务器与 XenMobile 节点之间在用户定义的时间间隔内的连接。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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **描述：** 监控 Citrix 许可证服务器与 XenMobile 节点之间在用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： Citrix Gateway 连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **描述：** 监控 Citrix Gateway 与 XenMobile 节点之间在用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

陷阱名称： XenMobile 节点间连接

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **描述：** 监控 XenMobile 群集节点之间在用户定义的时间间隔内的连接。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

- **监控对象 ID (OID)：** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **描述：** 监控 XenMobile Tomcat 节点服务与 XenMobile 节点之间在用户定义的时间间隔内的连接。如果连接失败，XenMobile 将生成 SNMP 陷阱。

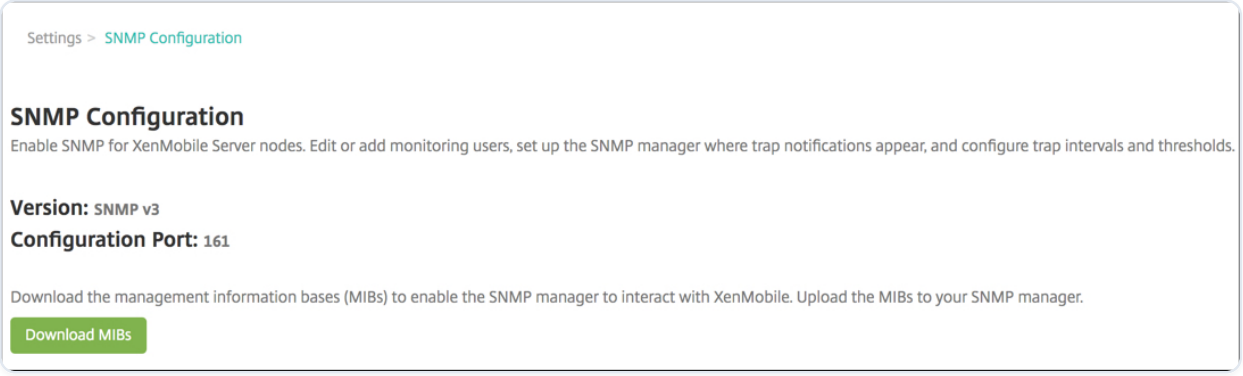
为获得最佳服务器性能，在配置 SNMP 阈值时，请记住以下因素：

- 呼叫频率
- 要收集的陷阱数据和阈值检查
- 节点间通信机制
- 连接性检查频率
- 检查期间任何故障的超时

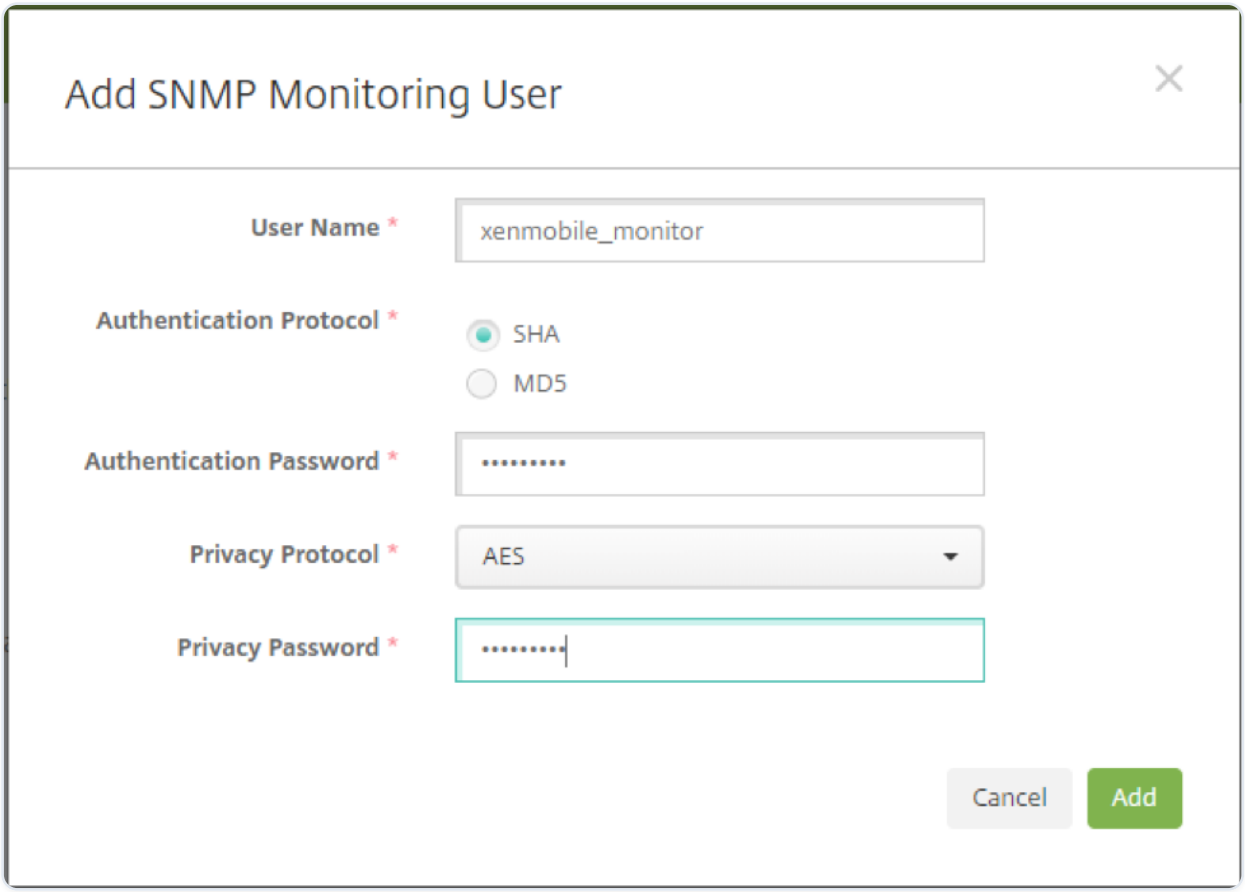
添加 SNMP 用户

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。将显示“**设置**”页面。
2. 在“**监视**”下，单击“**SNMP 配置**”。将显示“**SNMP 配置**”页面。



3. 在“**SNMP 监视用户**”下，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。尽管可以使用字母数字字符、下划线和连字符，但不能在用户名中使用空格和其他特殊字符。

> **注意：**
>
> 您不能添加用户名为“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。您可以包含字母数字和特殊字符。

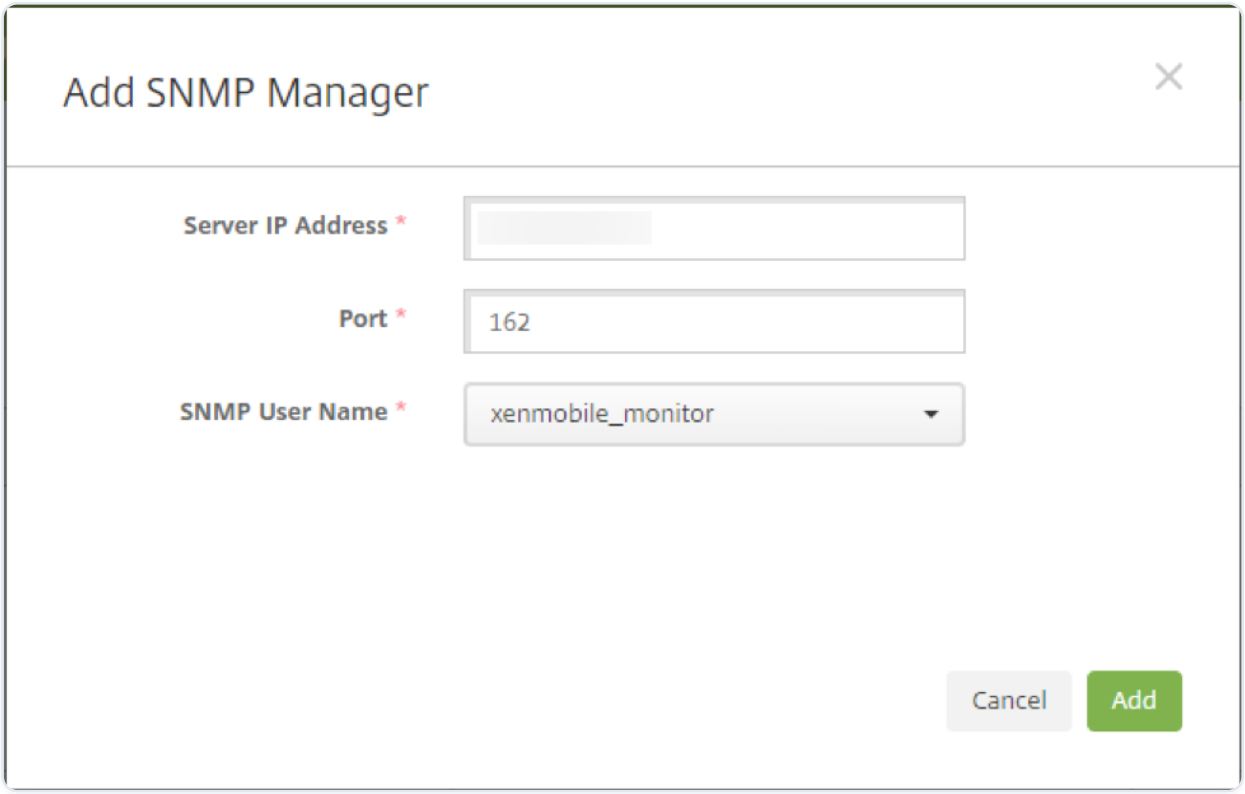
隐私协议：

- **DES**
- **AES 128**（推荐）

隐私密码： 键入 8 到 18 个字符的密码。您可以包含字母数字和特殊字符。

添加 SNMP 管理器

1. 在“**SNMP 管理器**”下，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。

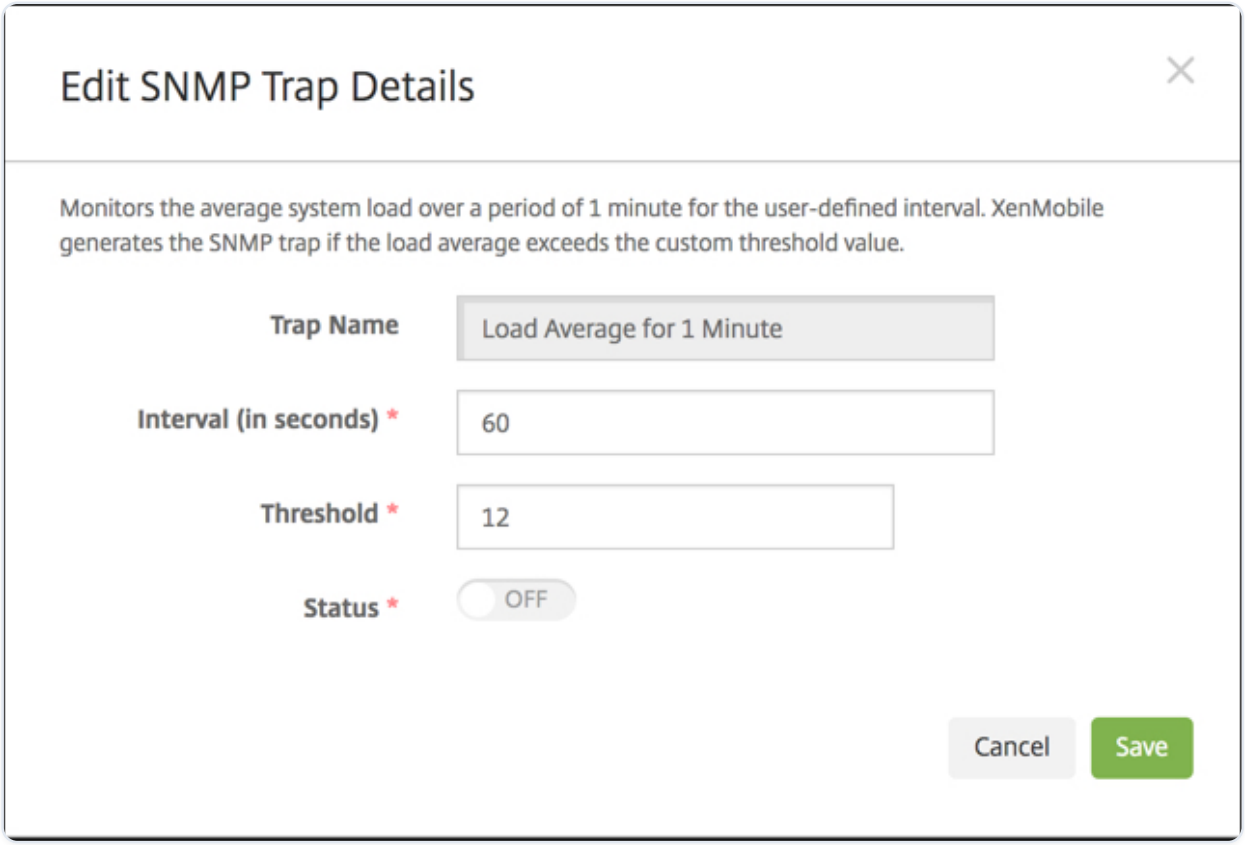
端口： 如有需要，更改端口号。默认值为 162。

SNMP 用户名： 选择有权访问管理器的用户的名称。

启用和配置 SNMP 陷阱

要帮助确定适合您环境的陷阱设置，请参阅 可伸缩性和性能。例如，要监控 XenMobile 一分钟平均负载，您可以启用“一分钟平均负载”并提供一个阈值。如果 XenMobile Server 一分钟平均负载超过指定阈值，您将在配置的 SNMP 管理器中收到一个陷阱。

1. 要启用单个陷阱，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. 要编辑陷阱，请选择参数，然后单击“**编辑**”。
3. 在“**编辑 SNMP 陷阱详细信息**”对话框中，您可以编辑单个陷阱的阈值。



陷阱名称： 陷阱的名称。您无法编辑此字段。

间隔（秒）： 允许的范围是 60 到 86400（24 小时）。

阈值： 您只能更改以下陷阱的阈值：

- 处理器负载
- 一分钟平均负载
- 五分钟平均负载

- 15 分钟平均负载
- 总可用内存
- 总已用磁盘存储
- Java 堆内存使用情况
- Java 元空间使用情况

状态： 选择 **ON** 以启用陷阱的 SNMP 监视。选择 **OFF** 以禁用监视。

有关使用 SNMP 监视 XenMobile 的更多有用信息，请参阅此博客文章。

支持包

要向 Citrix 报告问题或对问题进行故障排除，请创建支持包。然后，将支持包上传到 Citrix Insight Services (CIS)。

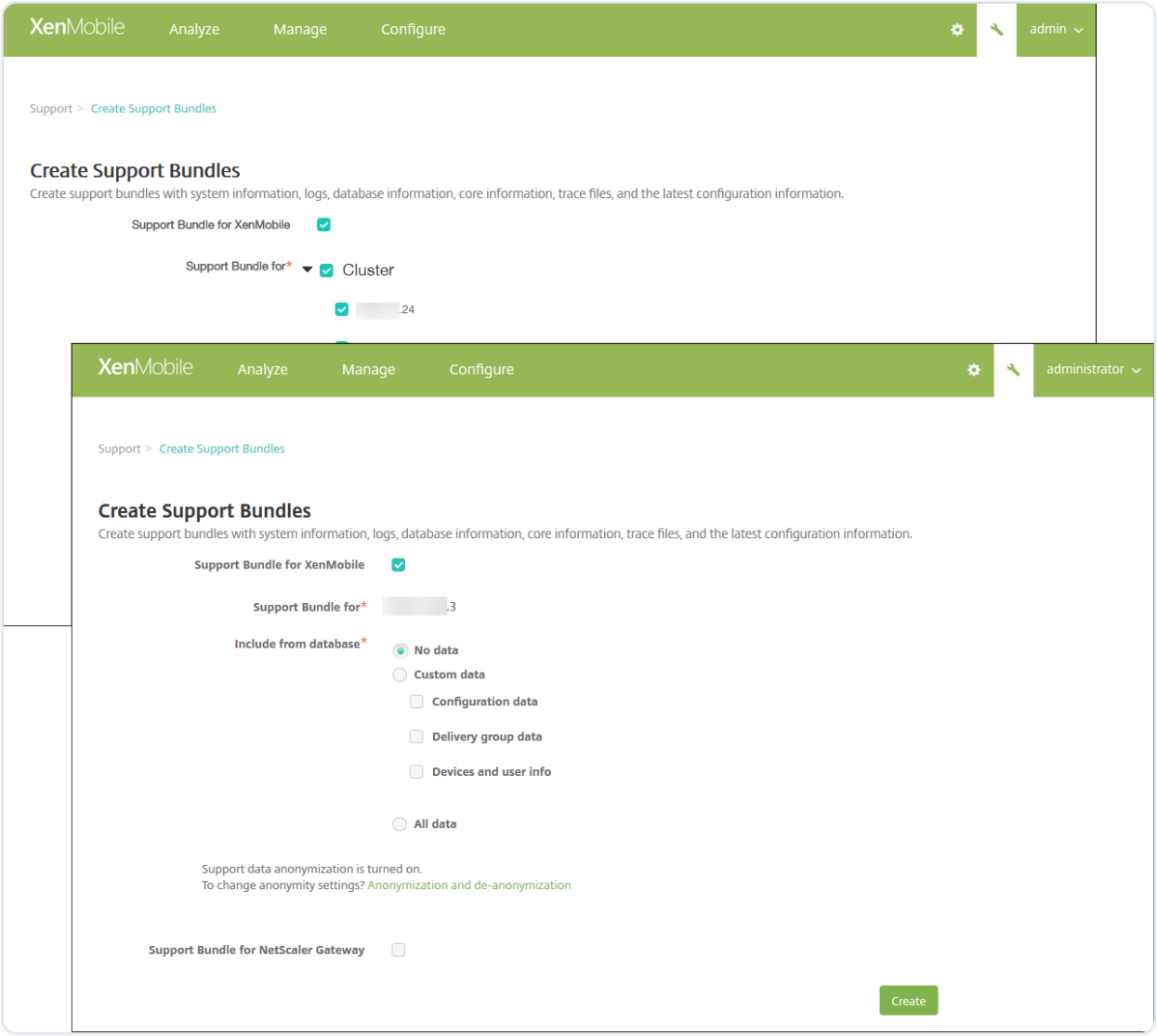
默认情况下，支持包最多包含以下文件的 100 个备份存档。这些文件的默认文件大小为 10 MB。

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

当支持包包含每个类别的 100 个日志存档文件时，日志文件将滚动更新。如果您配置的日志文件最大数量较少，XenMobile® 会立即删除该节点的多余日志文件。要配置日志文件数量，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：

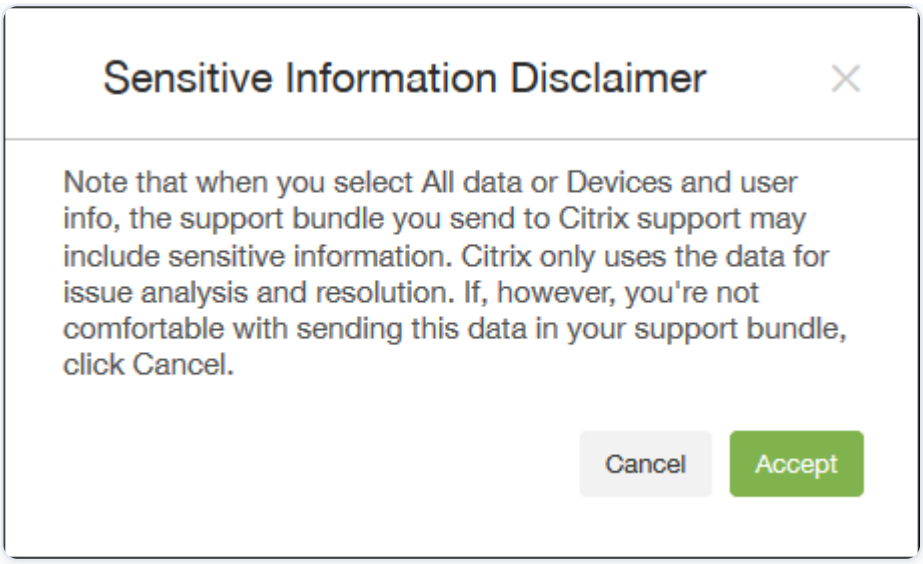
1. 在 XenMobile 控制台中，单击右上角的扳手图标。此时将显示**支持**页面。
2. 在**支持**页面上，单击**创建支持包**。此时将显示**创建支持包**页面。如果您的 XenMobile 环境具有群集节点，则会显示所有节点。



3. 确保选中**适用于 XenMobile 的支持包**复选框。
4. 如果您的 XenMobile 环境具有群集节点，在**支持包**中，您可以选择所有节点或任意组合的节点来提取数据。
5. 在**从数据库中包括**中，执行以下操作之一：
   - 点击**无数据**。
   - 点击**自定义数据**。默认情况下，所有这些选项都处于选中状态。
     - **配置数据：**包括证书配置和设备管理器策略。
     - **交付组数据：**包括包含应用程序类型和应用程序交付策略详细信息的应用程序交付组信息。
     - **设备和用户信息：**包括设备策略、应用程序、操作和交付组。
   - 点击**所有数据**。

注意：

如果您选择**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，则会出现**敏感信息免责声明**对话框。阅读免责声明，然后点击**接受**或**取消**。如果您点击**取消**，则无法将支持包上传到 Citrix。如果您点击**接受**，则可以将支持包上传到 Citrix，并且下次创建包含设备或用户数据的支持包时将不会看到此免责声明。

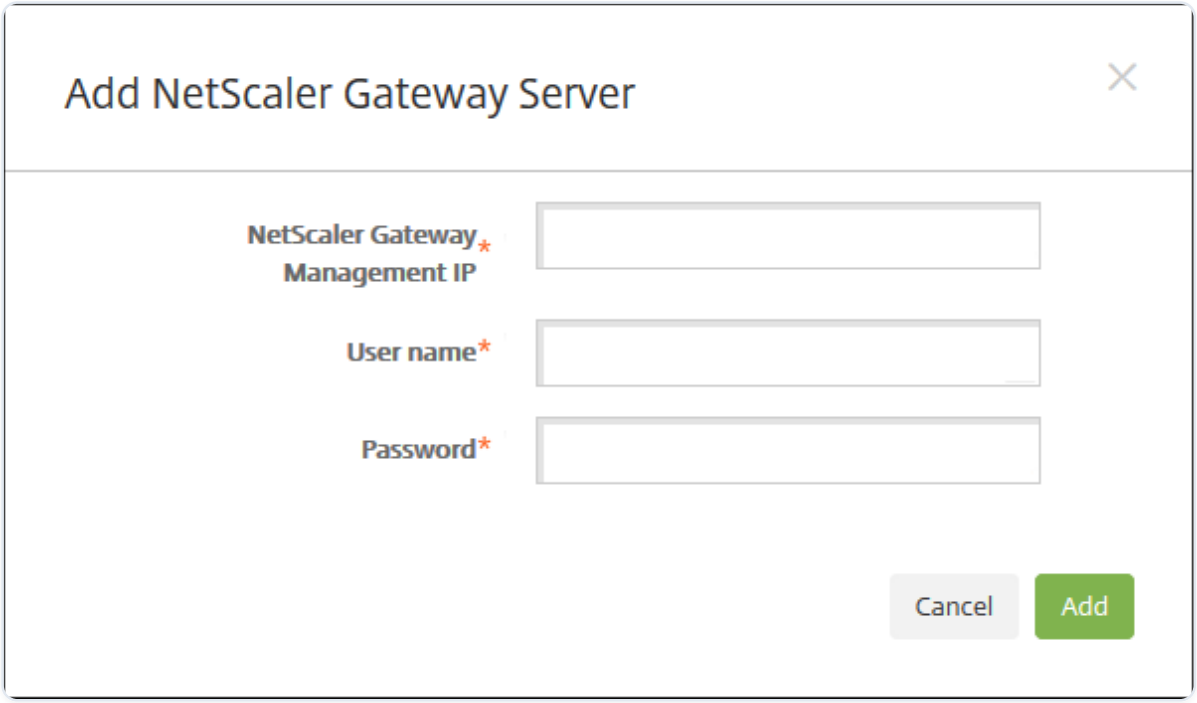


6. 选项**支持数据匿名化已开启**，表示默认设置为匿名化数据。数据匿名化意味着支持包中的敏感用户、服务器和网络数据将匿名化。

   要更改此设置，点击**匿名化和去匿名化**。有关数据匿名化的更多信息，请参阅支持包中的数据匿名化。

7. 要包含来自 Citrix Gateway 的支持包：选中**Citrix Gateway 支持包**复选框，然后执行以下操作：

   a. 点击**添加**。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：**
>
> 如果您正在从已添加的 Citrix Gateway 服务器创建捆绑包，则会提供 IP 地址。

c. 在**用户名**和**密码**中，键入访问运行 Citrix Gateway 的服务器所需的凭据。

> **注意：**
>
> 如果您正在从已添加的 Citrix Gateway 服务器创建捆绑包，则会提供用户名。

8. 单击**添加**。新的 Citrix Gateway 支持捆绑包将添加到表中。
9. 重复步骤 7 以添加更多 Citrix Gateway 支持捆绑包。
10. 单击**创建**。支持捆绑包已创建，并显示两个新按钮：**上传到 CIS** 和 **下载到客户端**。

将支持捆绑包上传到 Citrix Insight Services

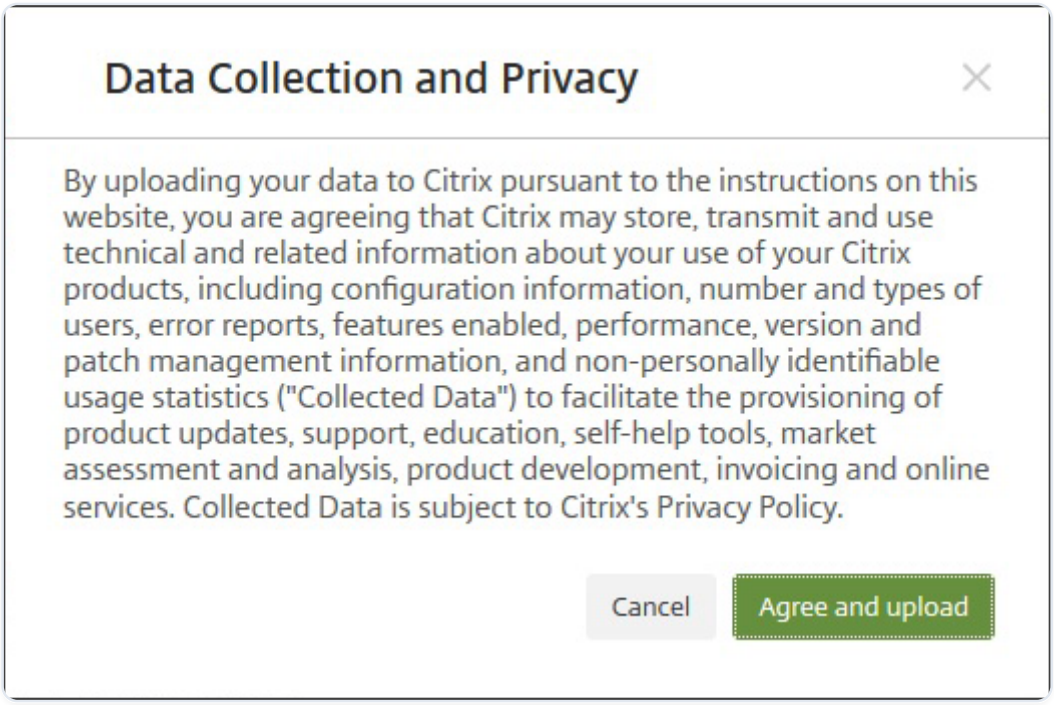
创建支持捆绑包后，您可以将捆绑包上传到 Citrix Insight Services (CIS) 或将捆绑包下载到您的计算机。

从 XenMobile 到 CIS 的上传通过 SSL 出站连接进行。向 CIS 服务器 IP 地址（52.88.24.76、52.88.118.220、52.11.72.119）打开端口 443。如果您有用于 HTTPS 流量的代理，请验证该代理是否可以访问 CIS 服务器 IP 地址。

以下步骤说明如何将捆绑包上传到 CIS。您需要 My Citrix ID 和密码才能上传到 CIS。

1. 在**创建支持捆绑包**页面上，单击**上传到 CIS**。此时将显示**上传到 Citrix Insight Services (CIS)** 对话框。
2. 在**用户名**中，键入您的 My Citrix ID。
3. 在**密码**中，键入您的 My Citrix 密码。
4. 如果您想将此捆绑包与现有服务请求号关联，请选中**关联到 SR#** 复选框，并在出现的两个新字段中执行以下操作：
   - 在 **SR#** 中，键入您要将此捆绑包关联的八位数字服务请求号。
   - 在 **SR Description** 中，键入 SR 的描述。
5. 单击**上传**。

   如果这是您首次将支持捆绑包上传到 CIS，并且您尚未通过其他产品在 CIS 上创建帐户并接受数据收集和隐私协议，则会出现以下对话框；您必须接受该协议才能开始上传。如果您在 CIS 上已有帐户并已接受该协议，则支持捆绑包将立即上传。



6. 阅读协议，然后单击**同意并上传**。支持捆绑包已上传。

将支持捆绑包下载到您的计算机

创建支持捆绑包后，您可以将捆绑包上传到 CIS 或下载到您的计算机。如果您想自行解决问题，请将支持捆绑包下载到您的计算机。

在**创建支持捆绑包**页面上，单击**下载到客户端**。捆绑包将下载到您的计算机。

支持捆绑包包含具有不同分析价值的文件。有关文件列表及其分析价值，请参阅下表。

文件名	类型	描述	价值
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 相关内存使用情况	高
MultiNodeClusterInfo.html	HTML 文件	集群配置	高
Patches.html	HTML 文件	补丁信息。最好是 xmspatches.txt	高
pg_dump0.sql	PG 转储	默认的 PostgreSQL 实例转储	中
rt_db/*	数据库副本（冗余，这是 pg_dump0.sql 的二进制表示）		不适用
sas_config/c3p0.properties	属性文件	C3P0 数据库配置属性	中
sas_config/catalina.policy	策略文件	Web 服务器 Catalina 策略 - 文件不会更改	低
sas_config/catalina.properties	属性文件	Web 服务器 Catalina 属性 - 文件不会更改	低
sas_config/ew-config.properties	属性文件	有关 XM 服务器配置的信息	高

文件名	类型	描述	价值
sas_config/ew-config-reloadable.properties	属性文件	安全模型信息	高
sas_config/hazelcast.xml	XML 文件	Hazelcast 日志 - 作用不大。	低
sas_config/pki.xml	XML 文件	可用于确定是否正在使用第三方 PKI 服务器。	高
sas_config/push_services.xml	XML 文件	推送服务 - 文件不会更改	低
sas_config/server.xml	XML 文件	此处包含密码信息 - 安全相关	高
sas_config/sftu_config/AppC.properties	属性文件	AppC 属性 - 文件不会更改	低
sas_config/sftu_config/catalina.policy	策略文件	Catalina 策略 - 文件不会更改	低
sas_config/sftu_config/catalina.properties	属性文件	Catalina 属性 - 文件不会更改	低
sas_config/sftu_config/logging.properties	属性文件	日志记录属性 - 文件不会更改	低
sas_config/sftu_config/server.xml	XML 文件	此处包含密码信息 - 与安全相关	高
sas_config/sftu_config/server_migration.xml	XML 文件	迁移信息	高

文件名	类型	描述	价值
sas_config/sftu_config/server_sftu.xml	XML 文件	首次用户设置	高
sas_config/sftu_config/tomcat-users.xml	XML 文件	TomCat 用户 - 文件不变	低
sas_config/sftu_config/web.xml	XML 文件	Web - 文件不变	低
sas_config/sftu.properties	属性文件	SFTU 配置属性	高
sas_config/variables.xml	XML 文件	变量 - 文件不变	低
sas_config/web.xml	XML 文件	Web 服务器相关信息	中
sas_log/AdminAuditLogFile.log	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.log	Linux 日志文件	所有功能日志	高
sas_log/HibernateStats.log	Linux 日志文件	Hibernate 统计日志	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

文件名	类型	描述	价值
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	后端审计级别信息	高
sas_log/PlatformDebugLogFile.txt	文本文件	后端服务器相关日志	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.log	Linux 日志文件	本地主机	低
sas_log/updates.log	Linux 日志文件	修补过程输出	中
sas_log/UserAuditLogFile.log	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_netsnmp.conf	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	描述	价值
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_usage.txt	文本文件	磁盘空间使用情况	高
sys_info/firewall_rules.txt	文本文件	XMS 中定义的防火墙规则	中
sys_info/interface_config.txt	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_info.txt	文本文件	系统命令输出	中
sys_info/routing_table.txt	文本文件	高价值	高
sys_info/running_process.txt	文本文件	高价值	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

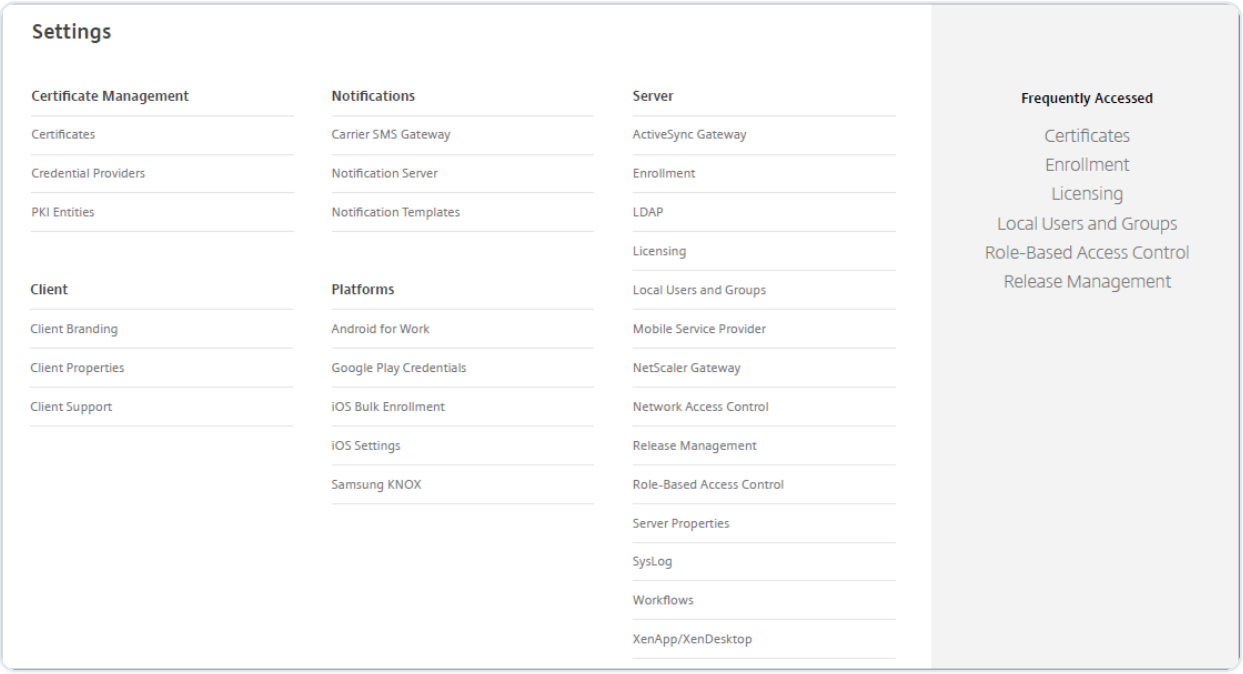
文件名	类型	描述	价值
var_log/lastlog	Linux 日志文件	操作系统级别日志	中
var_log/mail.log	Linux 日志文件	操作系统级别日志	中
var_log/sys.log	Linux 日志文件	操作系统级别日志	中
var_log/user.log	Linux 日志文件	操作系统级别日志	中
var_log/wtmp	Linux 日志文件	操作系统级别日志	中
version.txt	文本文件	XM 服务器版本	中
XENMOBILE-`<IP Address>`-ConnectivityCheckResults.xml	XML 文件	XMS 服务器上的连接检查结果	中
xmspatches.txt	文本文件	补丁信息。	高

支持选项和远程支持

您可以提供一个电子邮件地址，供用户联系支持人员。当用户从其设备请求帮助时，他们会看到该电子邮件地址。

您还可以配置用户如何从其设备向技术支持部门发送日志。您可以配置日志直接发送或通过电子邮件发送。

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，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 技术支持部门）：** 键入您的 IT 技术支持部门联系人的电子邮件地址。
   - **将设备日志发送到 IT 技术支持部门：** 选择设备日志是**直接**发送还是**通过电子邮件**发送。默认值为**通过电子邮件**。
     - 当您启用**直接**时，将显示“在 ShareFile 上存储日志”（现在称为 ShareFile）的设置。如果启用“在 ShareFile 上存储日志”，日志将直接发送到 Citrix Files。否则，日志将发送到 XenMobile，然后通过电子邮件发送到技术支持部门。此外，还会显示“**如果直接发送失败，则使用电子邮件**”选项，该选项默认处于启用状态。当您不希望使用客户端电子邮件发送服务器问题的日志时，可以禁用此选项。但是，如果您禁用此选项并且发生服务器问题，则不会发送日志。
     - 当您启用**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：**
>
> 从 January 1, 2019 起，远程支持不再适用于新客户。现有客户可以继续使用该产品，但 Citrix 不会提供增强功能或修复。

> 对于本地部署的 XenMobile Server，远程支持使您的服务台代表能够远程控制受管的 Android 移动设备。屏幕投射仅在 Samsung Knox 设备上受支持。

远程支持不适用于群集本地部署的 XenMobile Server。

在远程控制会话期间：

- 用户在其移动设备上会看到一个图标，指示远程控制会话处于活动状态。
- 远程支持用户会看到远程支持应用程序窗口以及一个显示受控设备渲染的远程控制窗口。

远程支持(/en-us/xenmobile/server/media/remote-support-with-rendered-device.png)

通过使用远程支持，您可以执行以下操作：

- 远程登录用户设备并控制屏幕。用户可以观看您操作其屏幕，这对于培训目的也很有帮助。
- 实时导航和修复远程设备。您可以更改配置、排查操作系统问题以及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、停止恶意进程以及删除应用程序或恶意软件，在威胁扩散到其他移动设备之前将其隔离和遏制。
- 远程启用设备铃声并呼叫手机，以帮助用户定位设备。当用户找不到设备时，您可以擦除设备以确保敏感数据不会泄露。

远程支持还使支持人员能够：

- 显示一个或多个 XenMobile 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、国际移动设备识别码 (IMEI)、序列号、内存和电池状态以及连接性。
- 显示 XenMobile 的用户和组。
- 运行设备任务管理器，您可以在其中显示活动进程、结束活动进程并重新启动移动设备。
- 运行远程文件传输，其中包括移动设备与中央文件服务器之间的双向文件传输。
- 将软件程序批量下载并安装到一个或多个移动设备。
- 配置设备上的远程注册表项设置。
- 通过使用实时设备屏幕远程控制，优化低带宽蜂窝网络上的响应时间。
- 显示大多数移动设备品牌和型号的设备外观。显示外观编辑器以添加新的设备型号并映射物理按键。
- 启用设备屏幕捕获、录制和回放功能，能够捕获设备上的一系列交互并创建视频 AVI 文件。

- 通过使用共享白板、基于 VoIP 的语音通信以及移动用户和支持人员之间的聊天来举行实时会议。

远程支持系统要求

远程支持软件安装在满足以下要求的基于 Windows 的计算机上。有关端口要求，请参阅端口要求。

支持的平台：

- Intel Xeon/Pentium 4 -1 GHz 最低工作站级别
- 512 MB RAM 最低
- 100 MB 可用磁盘空间最低

支持的操作系统：

- Microsoft Windows 2003 Server 标准版或企业版 SP1 或更高版本
- Microsoft Windows 2000 专业版 SP4
- Microsoft Windows XP SP2 或更高版本
- Microsoft Windows Vista SP1 或更高版本
- 微软 Windows 10 或 Windows 11
- 微软 Windows 8
- 微软 Windows 7

从命令行安装 Remote Support

运行以下命令：

```
*RemoteSupport*.exe /S
```

RemoteSupport 是安装程序的名称。例如：

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

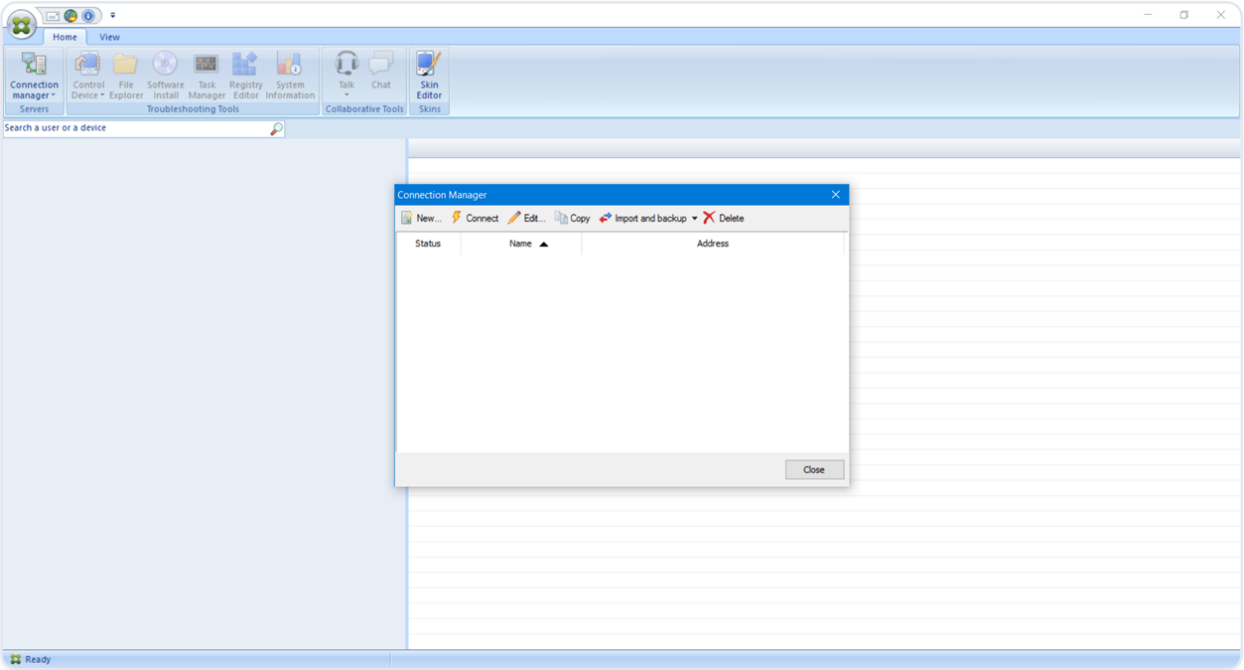
安装 Remote Support 软件时，可以使用以下变量：

- /S: 以默认参数静默安装 Remote Support 软件。
- /D=dir: 指定自定义安装目录。

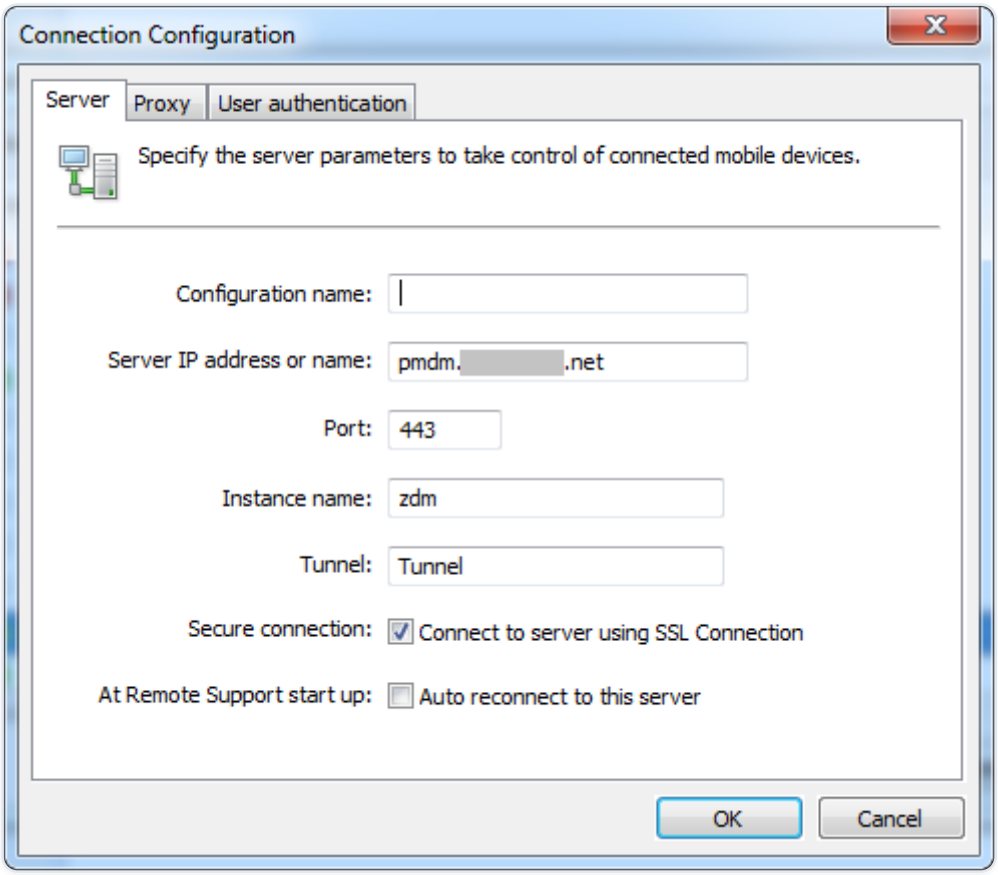
将 Remote Support 连接到 XenMobile

要建立与托管设备的远程支持连接，必须从 Remote Support 添加一个连接到一个或多个管理这些设备的 XenMobile Server。该连接通过您在 Tunnel MDM 策略（适用于 Android 设备的设备策略）中定义的应用程序隧道运行。在将 Remote Support 连接到 XenMobile 之前，请先定义应用程序隧道。有关详细信息，请参阅应用程序隧道设备策略。

1. 启动远程支持软件并使用您的 XenMobile 凭据登录。
2. 在 **连接管理器** 中，单击 **新建**。



3. 在 **连接配置** 对话框的 **服务器** 选项卡中，键入以下值：
   a. 在 **配置名称** 中，键入配置条目的名称。
   b. 在 **服务器 IP 地址或名称** 中，键入 XenMobile 服务器的 IP 地址或 DNS 名称。
   c. 在 **端口** 中，键入 XenMobile 服务器配置中定义的 TCP 端口号。
   d. 在 **实例名称** 中，当 XenMobile 是多租户部署的一部分时，键入实例名称。
   e. 在 **隧道** 中，键入隧道策略的名称。
   f. 选中 **使用 SSL 连接连接到服务器** 复选框。
   g. 选中 **自动重新连接到此服务器** 复选框，以便在每次远程支持应用程序启动时连接到配置的 XenMobile 服务器。



4. 在 **代理** 选项卡上，选择 **使用 http 代理服务器**，然后键入以下信息：

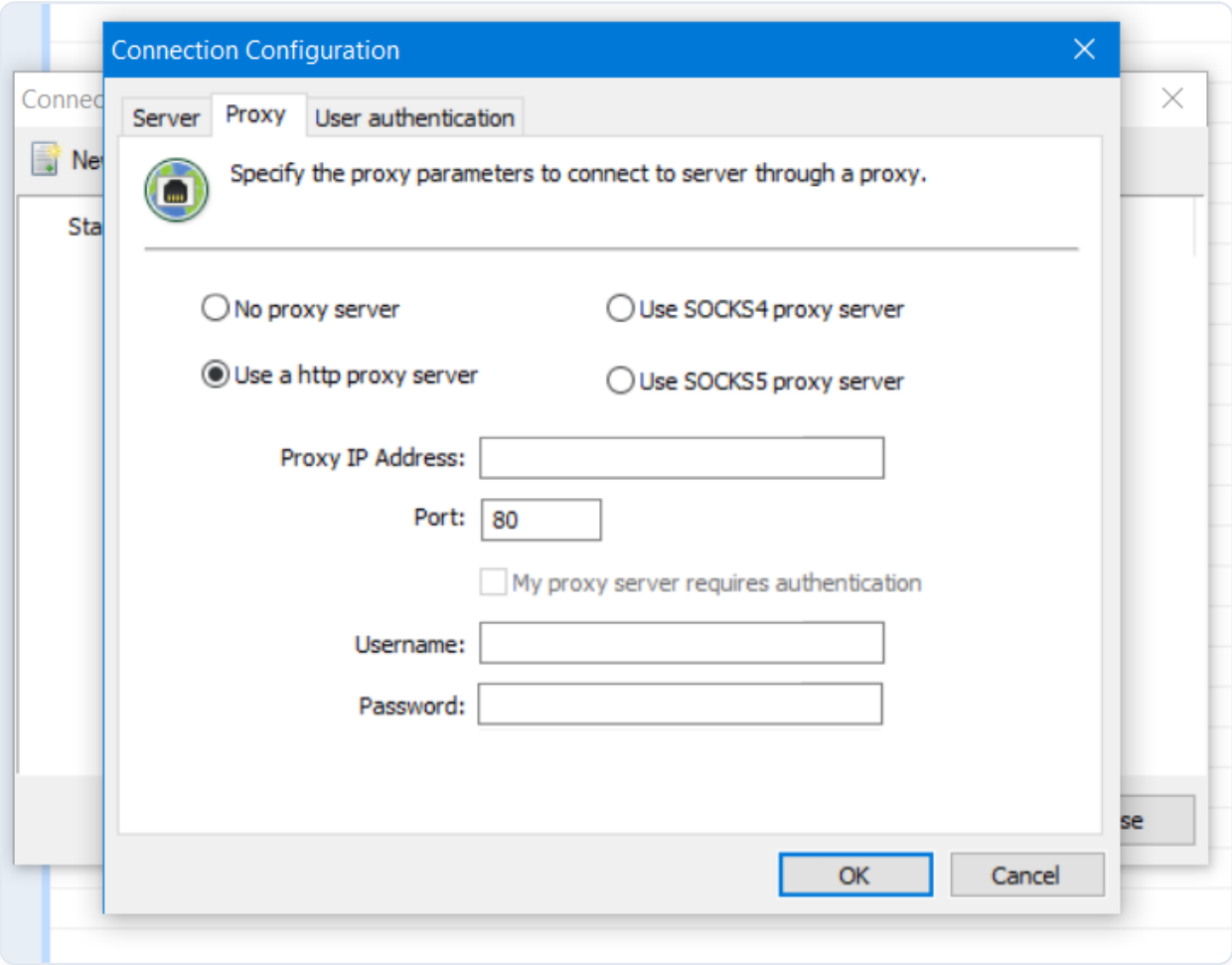
   a. 在 **代理 IP 地址** 中，键入代理服务器的 IP 地址。

   b. 在 **端口** 中，键入代理使用的 TCP 端口号。

   c. 当代理服务器需要身份验证才能允许流量时，选中“**我的代理服务器需要身份验证**”复选框。

   d. 在“**用户名**”中，键入要在代理服务器上进行身份验证的用户名。

   e. 在“**密码**”中，键入要在代理服务器上进行身份验证的密码。



5. 在“**用户身份验证**”选项卡上，选中“**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，请双击您创建的连接，然后输入您为该连接配置的用户名和密码。

为 Samsung Knox 设备启用远程支持

您可以在 XenMobile 中创建远程支持策略，以便远程访问 Samsung Knox 设备。您可以配置两种类型的支持：

- **基本：** 允许您查看设备的诊断信息。例如，系统信息、正在运行的进程、任务管理器（内存和 CPU 使用情况）以及已安装软件文件夹的内容。
- **高级：** 允许您远程控制设备屏幕。例如，控制窗口颜色、在技术支持人员和用户之间建立 VoIP 会话，以及在技术支持人员和用户之间建立聊天会话。

  高级支持要求您在 XenMobile 控制台中配置 Samsung MDM 许可证密钥设备策略。配置此策略时，仅选择“**Samsung KNOX**”平台。对于 Samsung SAFE 平台，ELM 密钥会在 Samsung 设备注册到 XenMobile 时自动部署。因此，请勿为此策略选择 Samsung SAFE 平台。有关详细信息，请参阅Samsung MDM 许可证密钥。

有关配置远程支持策略的信息，请参阅远程支持设备策略。

使用远程支持会话

启动远程支持后，远程支持应用程序窗口的左侧会显示您在 XenMobile 控制台中定义的 XenMobile 用户组。默认情况下，仅显示当前有用户连接的组。您可以在每个用户条目旁边看到该用户的设备。

1. 要查看所有用户，请展开左侧列中的每个组。 当前连接到 XenMobile Server 的用户会显示一个绿色图标。
2. 要显示所有用户（包括当前未连接的用户），请单击 **查看** 并选择 **未连接的设备**。 未连接的用户不会显示小绿色图标。

连接到 XenMobile Server 但未分配给用户的设备以匿名模式显示。（字符串 **匿名** 会显示在列表中。）您可以像控制已登录用户的设备一样控制这些设备。

要控制设备，请通过单击其行然后单击 **控制设备** 来选择设备。设备的渲染图像会显示在远程控制窗口中。您可以通过以下方式与受控设备进行交互：

- 在主窗口或单独的浮动窗口中控制设备屏幕，包括颜色控制。
- 在技术支持人员和用户之间建立 VoIP 会话。配置 VoIP 设置。
- 与用户建立聊天会话。
- 访问设备任务管理器，以管理内存使用情况、CPU 使用情况和正在运行的应用程序等项目。
- 浏览移动设备本地目录。传输文件。
- 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。

系统日志

您可以配置 XenMobile® Server（仅限本地部署）以将日志文件发送到系统日志 (syslog) 服务器。您需要服务器主机名或 IP 地址。

Syslog 是一种标准日志记录协议，包含两个组件：一个审计模块（在设备上运行）和一个服务器（可在远程系统上运行）。Syslog 协议使用用户数据协议 (UDP) 进行数据传输。将记录管理员事件和用户事件。

您可以配置服务器以收集以下类型的信息：

- 系统日志，其中包含 XenMobile 执行的操作记录。
- 审计日志，其中包含 XenMobile 系统活动的按时间顺序排列的记录。

syslog 服务器从设备收集的日志信息以消息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 appender 发送 RFC5424 格式的 syslog 消息。syslog 消息数据是纯文本，没有特定格式。

您可以使用此信息分析警报源并在必要时采取纠正措施。

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. 点击 **Syslog**。**Syslog** 页面出现。
3. 配置以下设置：
   - **服务器：** 输入您的 syslog 服务器的 IP 地址或完全限定域名 (FQDN)。
   - **端口：** 输入端口号。默认情况下，端口设置为 514。
   - **要记录的信息：** 选择或清除 **系统日志** 和 **审核**。
     - 系统日志记录了 XenMobile 执行的操作。
     - 审核日志记录了 XenMobile 系统活动的按时间顺序排列的记录。
     - 用于 XenMobile 的调试日志。
4. 点击 **保存**。

在 XenMobile® 中查看日志文件

查看、操作和下载日志以帮助管理 XenMobile。

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，单击“**日志**”。此时将显示“**日志**”页面。各个日志显示在一个表中。

   支持日志的图像(/en-us/xenmobile/server/media/support-logs.png)
3. 选择要查看的日志：
   - 调试日志文件包含对 Citrix 支持有用的信息，例如错误消息和服务器相关操作。
   - 管理员审核日志文件包含有关 XenMobile 控制台活动的审核信息。

- 用户审核日志文件包含与配置的用户相关的信息。
- 错误日志文件仅包含从调试日志中筛选出的错误消息。

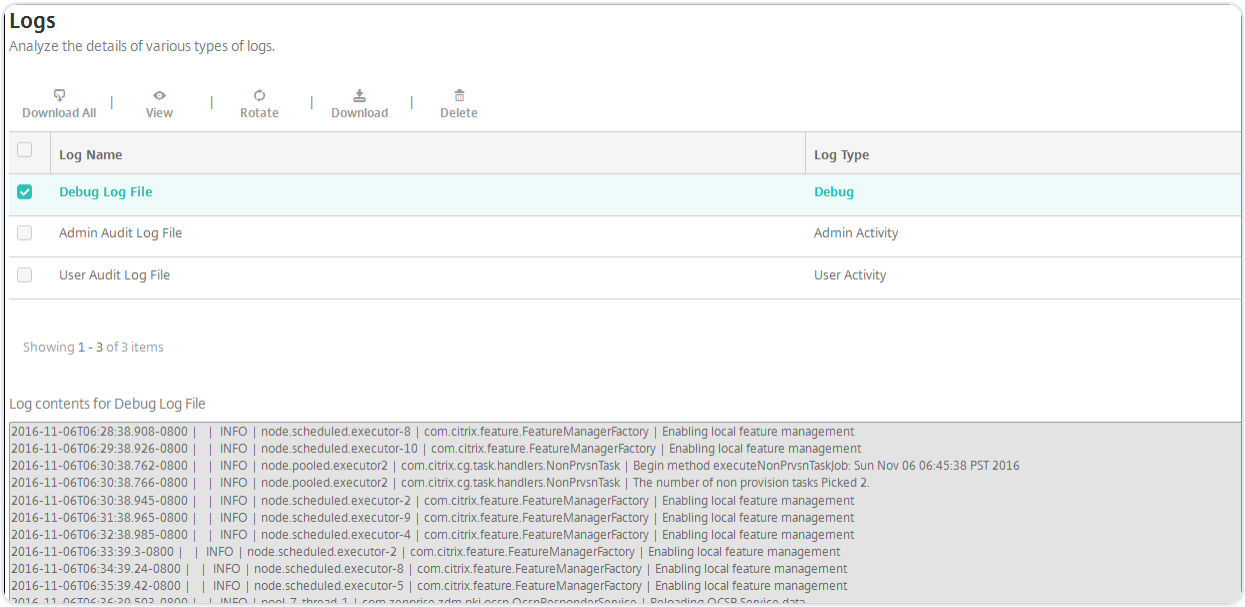
4. 使用表顶部的操作可下载所有日志、查看、轮换、下载单个日志或删除选定的日志。

   分析支持日志的图像(/en-us/xenmobile/server/media/analyze-logs.png)

> **注意：**
>
> - 如果选择多个日志文件，则只有“**下载所有**”和“**轮换**”可用。
> - 如果您有群集 XenMobile 服务器，则只能查看所连接服务器的日志。要查看其他服务器的日志，请使用其中一个下载选项。

5. 执行以下操作之一：

   - **下载所有：** 控制台下载系统中存在的所有日志（包括调试日志、管理员审计日志、用户审计日志、服务器日志等）。
   - **查看：** 在表格下方显示所选日志的内容。
   - **轮换：** 归档当前日志文件并创建一个文件以捕获日志条目。归档日志文件时会出现一个对话框；单击“轮换”以继续。
   - **下载：** 控制台仅下载所选的单个日志文件类型。它还会下载该相同类型的所有已归档日志。
   - **删除：** 永久删除所选日志文件。



XenMobile® Server 遥测数据元素

XenMobile Server 配置

事件头

键	描述	示例
版本	指示标头版本。	1
id	指示唯一的事件 ID (GUID)。	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
类型	指示事件类型名称。	SYSTEM_CONFIGURATION
st	表示 UTC 格式的时间戳。	2011-08-12T20:17:46.384Z
生产	表示产品名称。	XenMobile.OnPrem
prodVer	表示产品版本。	10.16.0.10123

事件负载

键	描述	示例
版本	表示 XenMobile Server 配置负载版本号。	1.1
xmsVer	指示 XenMobile Server 版本号。	10.16.0.48
xmsrpVer	指示 XenMobile Server 滚动修补程序版本号。	10.16.0.10323
dbType	指示 XenMobile Server 数据库类型。	MSSQL
dbVer	指示 XenMobile Server 数据库版本号。	Microsoft SQL Server 2019 (RTM-CU8) (KB4577194) - 15.0.4073.23 (X64) Sep 23 2020

键	描述	示例
		16:03:08 版权所有 (C) 2019 Microsoft Corporation 标准版 (64 位) 在 Windows Server 2016 Standard 10.0 X64 (内部版本 14393:) (虚拟机监控程序)
hostType	指示 XenMobile Server 虚拟机监控程序类型。	本地部署 - XenServer®
instanceName	指示 XenMobile Server 实例名称。	/XenMobile 设备管理器
licenseType	指示 XenMobile Server 激活的许可证类型。	CXM_ENTU_UD
sp	指示要收集的所有服务器属性。	sp: {AFW限制v2: 真 设备页面增强新: 真 多模式: 是 http2_alternate_port: 否 playemmapi_update: 是 afw_efota: 是 password_strength: 是 模式: ENT wsdl: 否 afw_restriction_cope: 是

键	描述	示例
		playemmapi: true mac_app_push: 是 ga: 是 zdm_pki: 是 tiffany: 禁用 ios_mdm: 是 nac_mail: 否 console_ceip: 启用 ssl_sign: 启用 wip: 启用 zebra: 启用 apple_apns_http2: 启用 afw_hide_vpn_always_on: 真 force_push_apps: 真 ftu: 假 afw_vpn_always_on_lockdown: 真 mfa: 真 mobile_service_provider: 真 afw_network_domain: 真

键	描述	示例	
		deprecate_sms: 真 cert_self_signed: 真 ios_http2_pushtype_bg: 假 device_update_awapppushtask: 真 android.deprecate.policy: 真 device_page_enhancement: 真 macos_http2_pushtype_bg: 假 edu_shared_ipad: 真 sync_license: 禁用 force_push_apps_flag: 真 shp: 假 wsapi: 否 aw_dg_performance: 是 apple_profile_renew: 真 afw_priority_update_apps: 真 esim: 真	

键	描述	示例
		wpcod: 真 knox: 真 device_report: 真 ios_app_update: 真 mspki_revert: 真}

键	描述	示例
cp	指示要收集的所有客户端属性。	cp: {PASSCODE_STRENGTH: 中等 ENABLE_WORXHOME_CEIP: 假 启用 FIPS 模式: false 将设备日志发送到 IT 帮助台: false 启用 WorxHome GA: true 使用密码加密密钥: false 启用密码身份验证: false ON_FAILURE_USE_EMAIL: 是 PASSCODE_TYPE: 数字型 CONTAINER_SELF_DESTRUCT_PERIOD: 0 PASSCODE_MIN_LENGTH: 6 ENABLE_CRASH_REPORTING: 是 PASSCODE_EXPIRY: 90

键	描述	示例
		INACTIVITY_TIMER: 15 ENABLE_PASSWORD_CACHING: 否 PASSCODE_MAX_ATTEMPTS: 15 PASSCODE_HISTORY: 5 禁用日志记录: 否 启用触控 ID 认证: 否 启用信标检查: 否}
enrolledDevices	指示已注册设备的数量。	enrolledDevices: {ANDROID:1,iOS:2, MACOSX:1}
完全限定域名	指示客户的公共 FQDN。	zl225.xmqa.cloud.com
ladpAuthType	指示 LDAP 身份验证类型。	域
nodeCount	指示集群中的节点数量。	4
managedApps	指示 XenMobile Server 管理的应用程序数量。	1000
usersUsingMicroVPN	指示 MicroVPN 用户数量。	9999
isIntuneIntegrated	指示 Intune 是否与 XenMobile Server 集成。	真

键	描述	示例
configuratedPolicies	指示 XenMobile Server 配置的策略数量。	7777

XenMobile Server 使用情况

事件标头

键	描述	示例
版本	指示标头版本。	1
id	指示唯一的事件 ID (GUID)。	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
类型	指示事件类型名称。	DEVICE_CHECKIN
st	指示 UTC 格式的时间戳。	2011-08-12T20:17:46.384Z
产品	指示产品名称。	XenMobile.OnPrem
prodVer	指示产品版本。	10.16.0.10123
用户	指示用户信息。对于本地用户，有效负载中没有 sid。**值已打乱。**	**AD 用户** 用户: { upn: C982F651A44B3F7 **(始终混淆)** domain: C982F651A44B3F7 **(始终混淆)** email: C982F651A44B3F7 **(始终混淆)**

键	描述	示例
		sid: C982F651A44B3F7 **(始终混淆)**} **本地用户** 用户: { upn: C982F651A44B3F7 **（始终乱码）** sAMAccountName: C982F651A44B3F7 **（始终乱码）**}

事件负载

键	描述	示例
版本	指示 XenMobile Server 使用情况负载的版本号。	1.1
deviceType	指示设备类型。	iPhone
hostName	指示客户用于本地部署的 fqdn。	test.xmqa.cloud.com
platformInfo	指示设备平台。	iPhone - iPhone
jailBroken	此密钥仅在设备已**越狱**或已**Root**时可用。如果此标记不存在，则表示设备未越狱或未 Root。	是或否
serialNum	指示设备的序列号，默认情况下已哈希处理。	KsPRhShj0h9IhbVkFEU7ZQ==
os	指示设备的操作系统类型。	iOS

键	描述	示例
managementMode	指示设备管理模式。	mdm 或 mam 或 xme 或 未受管
deviceId	指示设备的内部唯一 ID。	41CC018E-7CC0-4697-B07E-1E8CCEF7F592
受监管	指示设备是否受监管。	是或否
osVersion	指示设备的操作系统版本号。	16.4.1 (a)
国际移动设备识别码	指示设备的 IMEI 号码（如果可用），默认情况下已哈希处理。	6M6iBmcsokQxPQyeVwiaQQ==
deviceModel	指示设备的型号。	iPhone
lastActivity	指示设备的上次活动时间戳。	2024-03-29 14:17:14.277
corporateOwned	指示设备是否为公司所有。	否
enabledFeatures	指示多个功能的启用情况。	1
lpe 标识符	表示可用于识别唯一 XMS 站点的唯一环境 ID。	95ba4968cfaf069c20949d76473ecd4f3994f556d0fef7f2fa11912731d720bf 如果 LAS 不可用，则为空白

REST API

> **注意：**
>
> 本文介绍 XenMobile Server 的 REST API。有关 Endpoint Management 的 REST API，请参阅 REST API。
>
> 借助 XenMobile® REST API，您可以调用通过 XenMobile 控制台公开的服务。您可以使用任何 REST 客户端调用 REST 服务。此 API 不需要您登录 XenMobile 控制台即可调用服务。

有关可用 API 的完整当前集，请下载 REST 服务公共 API PDF。

访问 REST API 所需的权限

访问 REST API 需要以下权限之一：

- 作为基于角色的访问配置的一部分设置的公共 API 访问权限。有关信息，请参阅 使用 RBAC 配置角色。
- 超级用户权限

调用 REST API 服务

您可以使用 REST 客户端或 cURL 命令调用 REST API 服务。以下示例使用适用于 Chrome 的 Advanced REST 客户端。

> **注意：**
>
> 在以下示例中，请更改主机名和端口号以匹配您的环境。

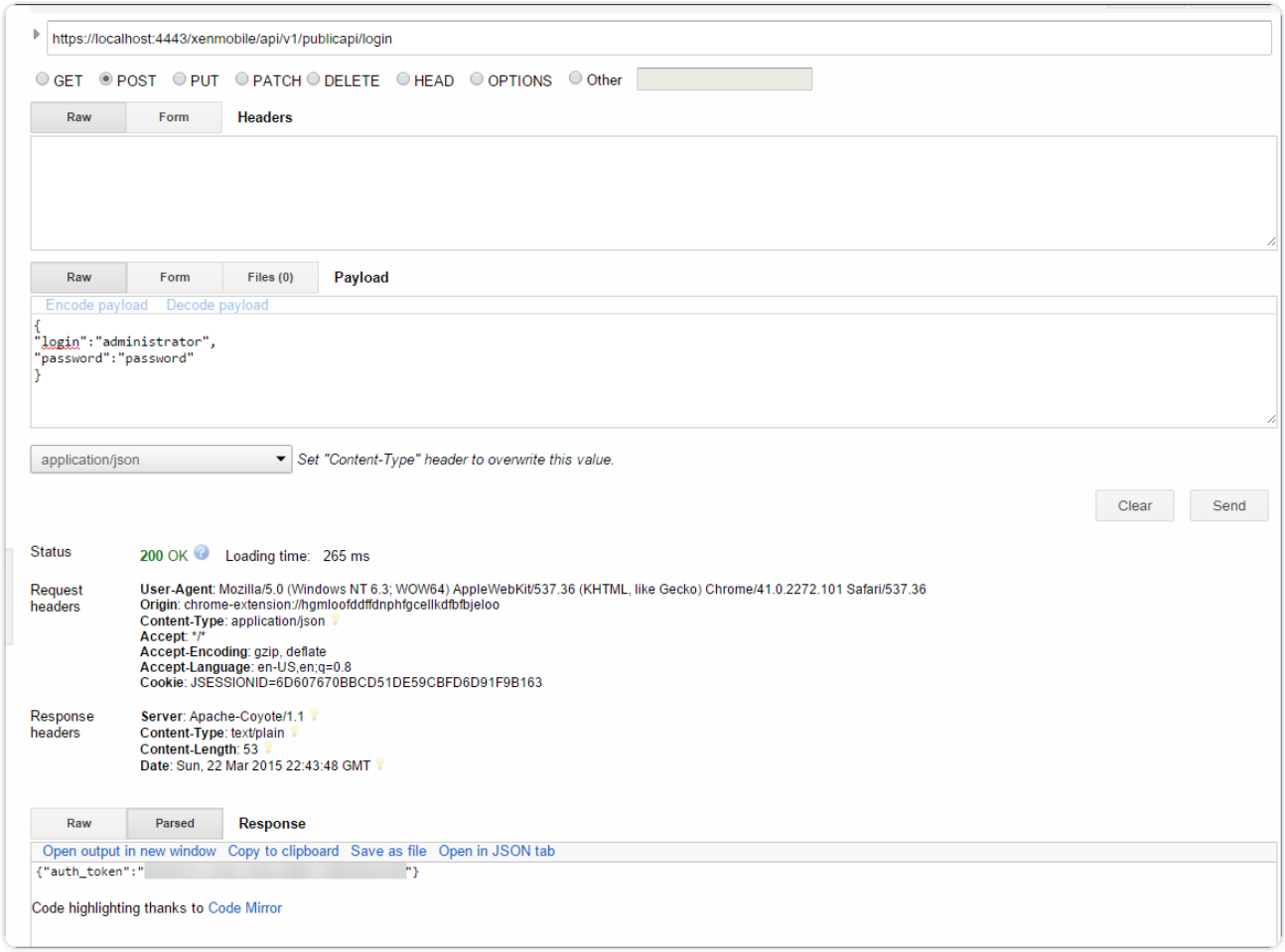
登录

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

XenMobile Mail Manager 现在是适用于 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。

此连接器通过以下方式扩展了 XenMobile® 的功能：

- 适用于 Exchange Active Sync (EAS) 设备的动态访问控制。EAS 设备可以自动允许或阻止访问 Exchange 服务。
- XenMobile 能够访问由 Exchange 提供的 EAS 设备伙伴关系信息。
- XenMobile 能够根据 EAS 状态擦除移动设备。
- XenMobile 能够访问有关 Blackberry 设备的信息，并执行 Wipe 和 ResetPassword 等控制操作。

要根据 EAS 状态擦除设备，请使用 ActiveSync 触发器配置自动化操作。请参阅自动化操作。

要下载适用于 Exchange ActiveSync 的 Endpoint Management 连接器：

1. 转至 `<https://www.citrix.com/downloads>`。
2. 导航到 **Citrix Endpoint Management™（和 Citrix XenMobile Server）> XenMobile Server（本地部署）> 产品软件 > XenMobile Server 10 > 服务器组件**。
3. 在**适用于 Exchange ActiveSync 的 Citrix Endpoint Management 连接器**磁贴上，单击**下载文件**。

> **重要提示：**
>
> 自 2022 年 10 月起，适用于 Exchange ActiveSync 的 Endpoint Management 和 Citrix Gateway 连接器将不再支持 Exchange Online，鉴于 Microsoft 此处 宣布的身份验证更改。适用于 Exchange 的 Endpoint Management 连接器将继续与 Microsoft Exchange Server（本地部署）配合使用。

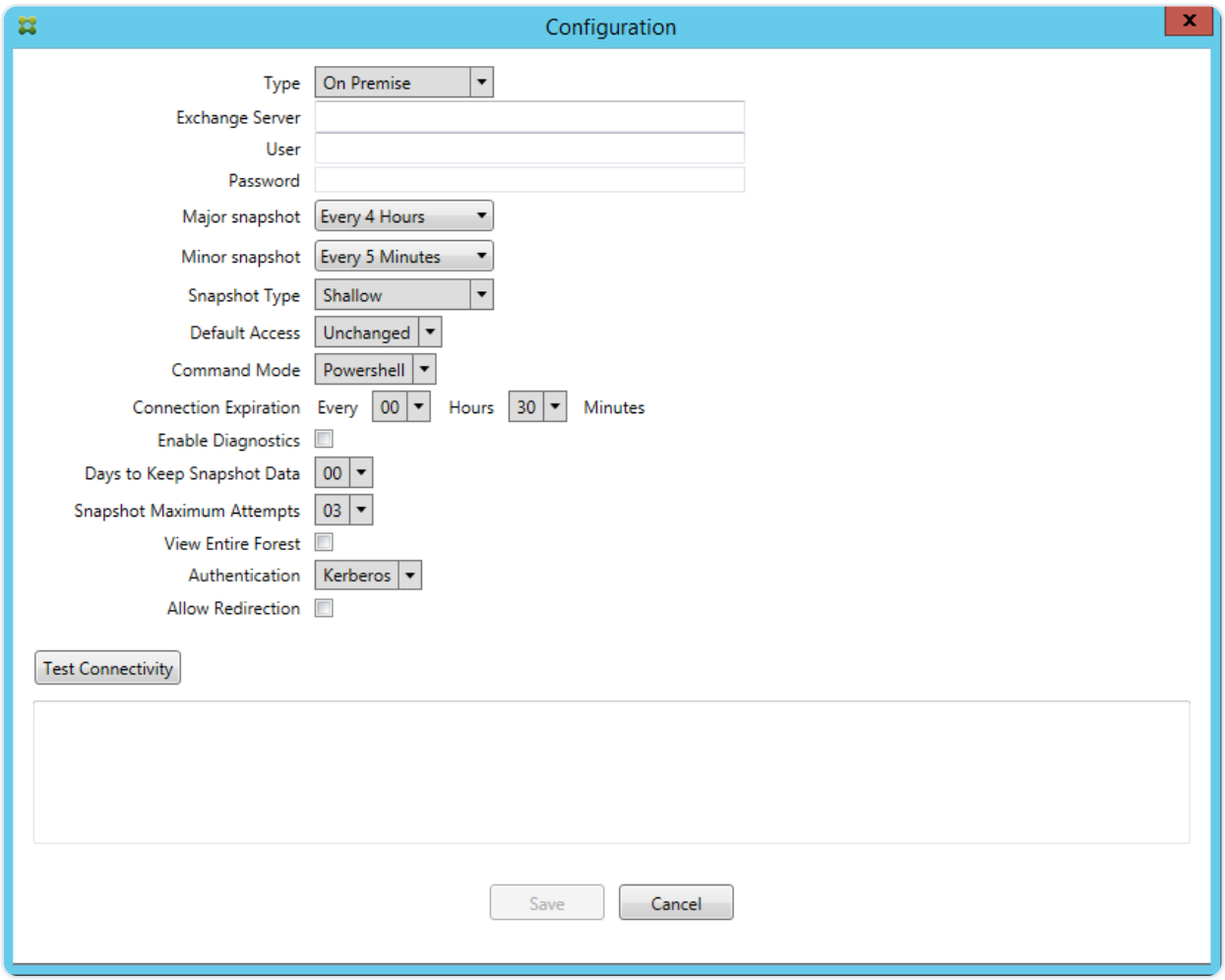
新增功能

以下部分列出了 Endpoint Management 连接器 for Exchange ActiveSync（以前称为 XenMobile Mail Manager）中的新增功能。

版本 10.1.10 中的新增功能

版本 10.1.10 中修复了以下问题：

- 遇到频繁网络问题的客户可能无法在之前提供的三次尝试内完成快照。在此版本中，管理员可以配置最大尝试次数 (1-10)。此修复允许快照在通信中断多次的情况下，无需完全放弃快照过程。



- 在以前的版本中，“快照”类型未显示在 Exchange 配置列表中。现在，“快照”类型已显示。
- PowerShell 报告的 PSRemotingTransport 异常表示与 Exchange 的会话不再可用。默认情况下，此状态会添加到配置文件中的“严重错误”列表中。这样，当检测到 PSRemotingTransportException 时，连接将被标记为“错误”，以便稍后处理。下一次通信将使用有效连接或创建新连接。

- 保存配置更改时，可能并非所有先前配置的内部组件都在加载新配置之前得到正确处理。此问题可能导致不可预测的行为。行为取决于具体的更改以及更改是否与以前的配置冲突。在此版本中，所有内部组件在加载新配置之前都会被处理。

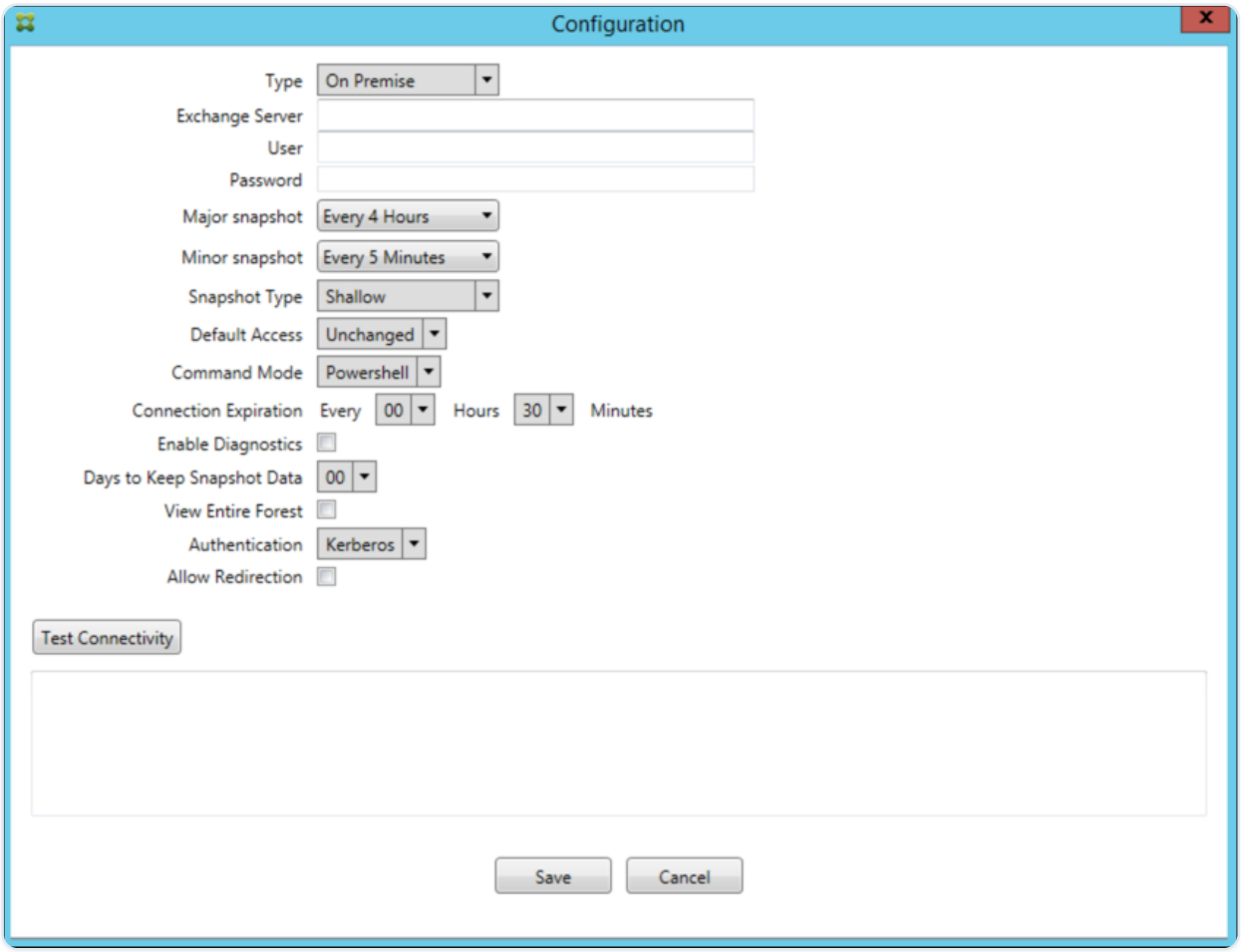
早期版本中的新增功能

以下部分列出了 Endpoint Management 连接器 for Exchange ActiveSync 早期版本中的功能和已修复问题。

版本 10.1.9 中的新增功能

版本 10.1.9 中修复了以下问题：

- 配置更改现在以更一致的方式处理。当服务检测到配置更改时，每个内部子系统都会停止，这意味着任何活动或计划的处理都会中断。接下来，加载新配置并重新启动子系统，这意味着所有计划和其他内部基础结构都将使用新设置重新建立。此问题纠正了版本 10.1.8 中的一个已知问题。
- 在升级过程中，现有数据库配置未合并到新的配置文件中。现在，数据库配置已合并到升级后的配置文件中。
- 在与快照相关的诊断文件中，缺少列标题。现在，标题已恢复。
- 从以前的版本升级时，配置文件的默认设置部分会被正在使用的配置文件的类似部分覆盖。此问题导致升级后服务无法加载默认设置部分的添加或改进。从该版本开始，默认设置部分始终反映最新的配置。
- 管理员在运行应用程序时，无法再通过按 Shift 键访问某些选项。这些选项以前需要 Citrix 权限才能使用。某些选项（例如“允许重定向”）现已完全可用，而其他选项（例如“挂起检测”和“计数校正”）则已弃用。



10.1.8 版中的新增功能

10.1.8 版中修复了以下问题：

- Exchange 可能会限制 Citrix Endpoint Management 连接器对 Exchange ActiveSync 服务发出命令的频率。这在连接到 Office 365 时很常见。限制的效果是要求服务在发送下一个命令之前暂停指定的时间。“配置”控制台现在会显示暂停的剩余时间。
- 当对配置文件 (config.xml) 的“Watchdog”或“SpecialistsDefaults”部分进行修改时，升级后这些更改不会反映在配置文件中。在此版本中，修改已正确合并到新的配置文件中。
- 发送到 Google Analytics 的分析数据已添加更多详细信息，尤其是关于快照的详细信息。
- Exchange 测试连接功能只会尝试初始化连接一次。由于 Office 365 连接可能会受到限制，因此在受到限制时，测试连接可能会显示为失败。Citrix Endpoint Management 连接器 for Exchange ActiveSync 现在会尝试最多三次发起连接。
- 为了在 Exchange 上实施策略，Citrix Endpoint Management 连接器 for Exchange ActiveSync 必须编译一个 **Set-CASMailbox** 命令，该命令包含每个邮箱的所有相关设备，分为两个列表：允许和阻止。如果设备未包含在任一列表中，Exchange 将回退到其默认访问状态。如果该默认访问状态与设备的所需状态不同，则该设备将变得不合规。因此，如果 Exchange 默认访问状态被阻止而应被允许，用户可能会失去对其电子邮件的访问权限。或者，本应被阻止访问电子邮件

的用户可能会被授予访问权限。Citrix Endpoint Management 连接器 for Exchange ActiveSync 现在确保每个 **Set-CasMailbox** 命令中都包含所有具有有效所需状态的设备。

10.1.8 版中存在以下已知问题：

如果管理员在“配置”应用程序中进行更改以修改配置数据，而服务正在执行长时间操作（例如快照或策略评估），则服务可能会进入不确定状态。可能的症状是策略更改未被处理，或者快照未启动。要使服务恢复正常工作状态，必须重新启动服务。您可能需要使用 Windows 服务管理器在启动服务之前终止服务进程。

10.1.7 版中的新增功能

- XenMobile Mail Manager 现在是 Exchange ActiveSync 的 Endpoint Management 连接器。
- 我们已弃用 Exchange 配置对话框中的“**禁用管道**”选项。您可以通过在 config.xml 文件中为每个命令配置多个步骤来实现相同的功能。

10.1.7 版中修复了以下问题：

- 在快照历史记录窗口中，错误消息可能显示时上下文很少。现在，错误消息会以其发生位置的上下文作为前缀。
- XmmGoogleAnalytics .dll 没有对应的发布文件版本。
- 为了改进诊断，我们最近更改了用于设置邮箱允许/阻止状态的设备 ID 列表的字符串格式。然而，指定过多设备会超出最大字符串大小。现在，我们使用内部数组数据结构。此结构没有大小限制，并且还能以适合诊断目的的方式格式化数据。
- 当检测到与 Exchange 不同步的设备策略时，其命令可能包含不属于相关邮箱的设备。Endpoint Management connector for Exchange ActiveSync 现在确保发送到 Exchange 的命令仅代表属于其各自邮箱的设备。
- 在某些环境中，Microsoft 程序集不可用。现在，所需的程序集会随应用程序一起明确安装。
- 如果设备或邮箱的专有名称在属性名称和等号之间，和/或在等号之后和值之前包含空格，则 端点管理 连接器 for Exchange ActiveSync 可能无法正确地将设备与其邮箱匹配，反之亦然。这可能导致某些设备和/或邮箱在快照协调期间被拒绝。

注意：

以下各节将 Endpoint Management connector for Exchange ActiveSync 称为其旧名称 XenMobile Mail Manager。该名称自版本 10.1.7 起更改。

版本 10.1.6.20 中的更新

10.1.6 的更新包含版本 10.1.6.20 中的以下修复：

- 当检测到与 Exchange 不同步的设备策略时，其命令可能包含不属于相关邮箱的设备。XenMobile Mail Manager 现在确保发送到 Exchange 的命令仅代表属于其各自邮箱的设备。

版本 10.1.6 中的新增功能

XenMobile Mail Manager 版本 10.1.6 包含以下已修复问题和增强功能：

- 快照历史记录窗口有时会进入不再更新的状态。窗口刷新机制已得到改进，可以更可靠地进行更新。
- 分区快照和非分区快照使用了两种独立的模式和代码路径。由于非分区快照等同于使用单个“*”分区的配置的分区快照，因此已取消非分区快照模式。默认快照模式现在是具有 36 个分区（0–9，A–Z）的分区快照。
- 在快照历史记录窗口中，错误消息会被状态消息覆盖。现在，XenMobile Mail Manager 提供了两个单独的字段，以便用户可以同时查看状态和错误。
- 连接到 Exchange Online (Office 365) 时，与快照相关的查询可能会导致数据集被截断。当 XenMobile Mail Manager 运行多命令管道脚本时，可能会出现此问题。上游命令无法足够快地将数据传递给下游命令，导致下游命令过早完成工作。结果是数据不完整。XenMobile Mail Manager 现在可以模拟管道本身，并等待上游命令完成后再调用下游命令。此更改应确保所有数据都得到处理和捕获。
- 如果向 Exchange 发送的策略更新命令中发生无法解决的错误，则同一命令会长时间重复返回到工作队列。这种情况导致该命令多次发送到 Exchange。在此版本的 XenMobile Mail Manager 中，导致错误的命令只会以离散的次数返回到工作队列。
- 如果特定邮箱的策略更新涉及允许或阻止所有设备：发出的 **Set-CASMailbox** 命令将失败，因为空列表被转换为一个空字符串而不是 **NULL**。现在已发送正确的数据。
- 处理新设备时，Exchange 可能会在一段时间内（通常为 15 分钟）将状态返回为“DeviceDiscovery”。XenMobile Mail Manager 以前未专门处理此状态。XenMobile Mail Manager 现在可以处理此状态。在 UI 的“监视器”选项卡中，用户可以筛选处于此状态的设备。
- XenMobile Mail Manager 未检查写入 XenMobile Mail Manager 数据库的能力。因此，如果权限受限，则无法预测其行为。XenMobile Mail Manager 现在会从数据库捕获并验证所需的权限。在测试连接（显示消息）或在主“配置”窗口底部的“数据库”指示器（悬停以显示消息）中，XenMobile Mail Manager 会指示权限已降低。
- 根据当前工作负载，当收到停止指令时，XenMobile Mail Manager 服务可能无法及时停止。因此，该服务似乎处于无响应状态。改进措施允许中断正在进行的任务，从而实现更优雅的关机。

版本 10.1.5 中的新增功能

XenMobile Mail Manager 版本 10.1.5 包含以下已修复问题：

- 当 Exchange 对 XenMobile Mail Manager 活动应用限制时，除了日志之外，没有迹象表明正在进行限制。在此版本中，用户可以将鼠标悬停在活动快照上，此时会显示“限制”状态。此外，当 XenMobile Mail Manager 受到限制时，在 Exchange 解除限制禁令之前，禁止启动主要快照。
- 如果在主要快照期间 XenMobile Mail Manager 受到 Exchange 的限制：在运行下一次快照尝试之前，可能没有足够的时间间隔。此问题会导致进一步的限制和快照失败。XenMobile Mail Manager 现在会至少等待 Exchange 指定的快照尝试之间的等待时间。
- 启用诊断时，命令文件会显示 **Set-CasMailbox** 命令，其中每个属性名称前都缺少连字符。此问题仅发生在诊断文件的格式中，而不是实际发送到 Exchange 的命令中。缺少连字符会阻止用户剪切命令并直接将其粘贴到 PowerShell 提示符进行测试或验证。现在已添加连字符。
- 如果邮箱标识符的形式为“姓氏, 名字”，则 Exchange 在从查询返回数据时会在逗号前添加反斜杠。当 XenMobile Mail Manager 使用此标识符查询更多数据时，必须去除此反斜杠。

已知限制

> **注意：**

> 版本 10.1.6 中解决了以下限制。

> XenMobile Mail Manager 存在一个已知限制，可能导致发送到 Exchange 的命令失败。要将策略更改应用于 Exchange，XenMobile Mail Manager 会发出 **Set_CASMailbox** 命令。此命令可以接受两个设备列表：一个用于允许，一个用于阻止。该命令应用于与邮箱关联的设备。

这些列表通过 Microsoft API 限制为每个 256 个字符。如果其中一个列表超出限制，则整个命令将失败，从而阻止设置邮箱中这些设备的所有策略。报告的错误将显示在 XenMobile Mail Manager 日志中，如下所示。此示例适用于阻止列表。

“Message:'无法将参数 'ActiveSyncBlockedDeviceIDs' 绑定到目标。设置 "ActiveSyncBlockedDeviceIDs" 时出现异常："属性的长度过长。最大长度为 256，提供的值的长度为…”

设备 ID 长度可能有所不同，但一个好的指导原则是，同时允许或阻止大约 10 个或更多设备可能会超出限制。尽管与特定邮箱关联的设备数量如此之多的情况很少见，但仍有可能发生。在 XenMobile Mail Manager 改进以处理此类情况之前，我们建议您将与用户和邮箱关联的设备数量限制为 10 个或更少。

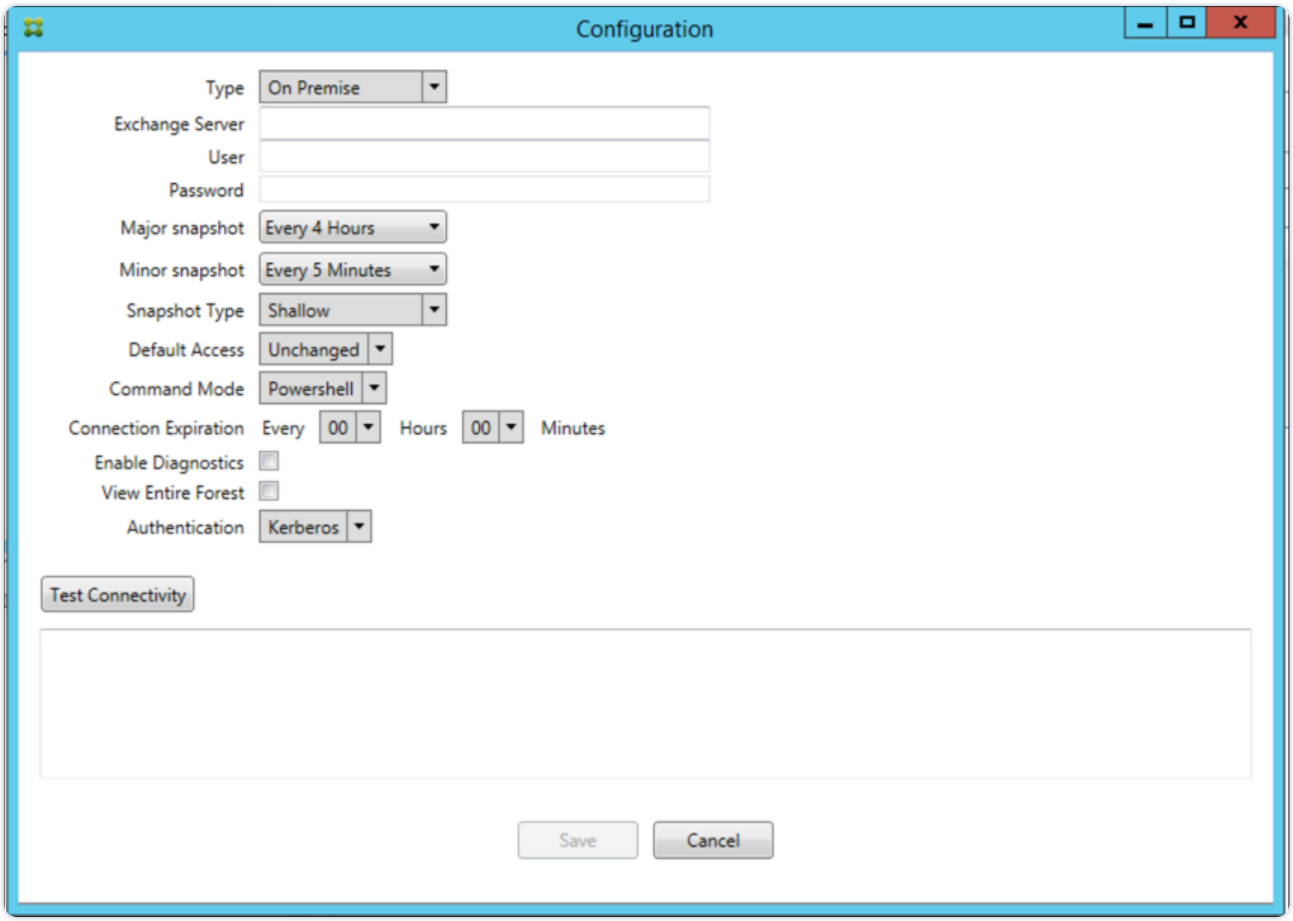
版本 10.1.4 中的新增功能

XenMobile Mail Manager 版本 10.1.4 包含以下已修复问题：

- 由于其安全性减弱，PCI Council 正在弃用 TLS 1.0。XenMobile Mail Manager 中增加了对 TLS 1.1 和 1.2 的支持。
- XenMobile Mail Manager 包含一个新的诊断文件。在 Exchange 规范中选择 **Enable Diagnostics**（启用诊断）时，会生成一个新的 Snapshot History（快照历史记录）文件。每次快照尝试都会在文件中添加一行，其中包含快照结果。
- 在 Commands 诊断文件中，**Set-CASMailbox** 命令的允许或阻止设备列表未显示。相反，文件中显示了相关参数的内部类名称。XenMobile Mail Manager 现在将 deviceID 列表显示为逗号分隔列表。
- 当由于错误的规范而导致尝试获取与 Exchange 的连接失败时：错误消息被不正确的“所有连接都在使用中”消息覆盖。现在显示更具描述性的消息，例如“所有连接都无法操作”、“连接池为空”、“所有连接都受到限制”和“没有可用连接”。
- 有时，允许/阻止/擦除命令会在 XenMobile Mail Manager 内部缓存中多次排队。此问题会导致命令发送到 Exchange 的延迟。XenMobile Mail Manager 现在只对每个命令排队一个实例。

版本 10.1.3 中的新增功能

- **Google Analytics 支持：** 我们希望了解您如何使用 XenMobile Mail Manager，以便我们能够专注于改进产品。
- **启用诊断的设置：** 在 Configure 控制台的 **Configuration**（配置）对话框中显示一个 **Enable Diagnostic**（启用诊断）复选框。



版本 10.1.3 中已修复的问题

- 在**快照历史记录**窗口中，显示快照当前状态的工具提示无法反映实际状态。 有时，XenMobile Mail Manager 无法写入命令诊断文件。发生这种情况时，命令历史记录不会完整记录。
- 当连接发生错误时，该连接可能不会被标记为“出错”。因此，后续命令可能会尝试使用该连接并导致另一个错误。
- 当 Exchange Server 发生限制时，Check Health 例程中可能会抛出异常。因此，已发生错误或已过期的连接可能不会被清除。此外，XenMobile Mail Manager 可能不会创建连接，直到限制时间到期。
- 当超出 Exchange 的最大会话数时，XenMobile Mail Manager 会报告错误“设备捕获失败”，这不是一条准确的消息。相反，该消息应指示 XenMobile Mail Manager 通常用于 Exchange 通信的两个会话正在使用中。

版本 10.1.2 中的新增功能

- **改进了与 Exchange 的连接**：XenMobile Mail Manager 使用 PowerShell 会话与 Exchange 通信。PowerShell 会话（尤其是在处理 Office 365 时）在一段时间后可能会变得不稳定，从而阻止后续命令成功执行。XenMobile Mail Manager 现在可以为连接设置过期时间。当连接达到其

过期时间时，XenMobile Mail Manager 会正常关闭 PowerShell 会话并创建一个新会话。通过这样做，PowerShell 会话变得不稳定的可能性会降低，从而显著减少快照失败的可能性。

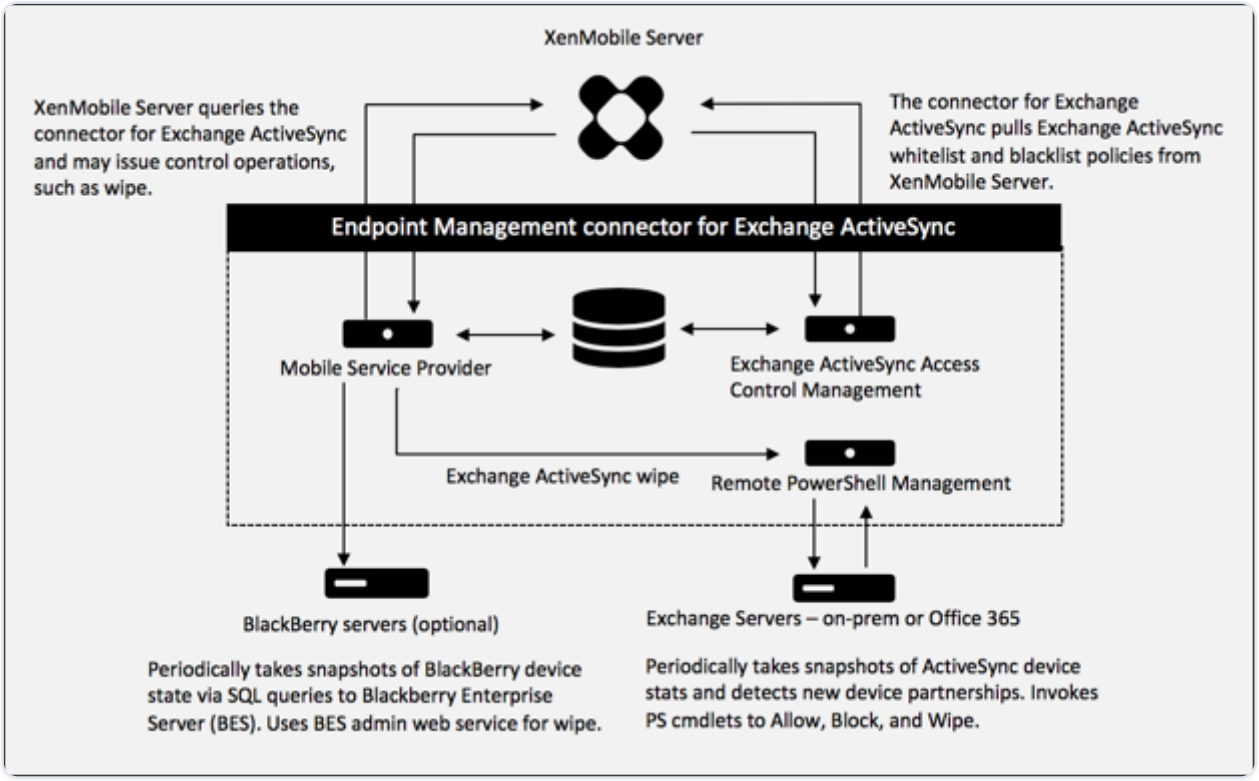
- **改进的快照工作流**：主要快照是一项耗时且占用大量处理资源的操作。如果在快照期间发生错误，XenMobile Mail Manager 现在会尝试多次（最多三次）完成快照。后续尝试不会从头开始。XenMobile Mail Manager 会从上次中断的地方继续。此增强功能通过允许瞬时错误在快照仍在进行时通过，从而提高了快照的总体成功率。
- **改进的诊断功能**：通过在快照期间可选生成的三个新诊断文件，现在可以更轻松地对快照操作进行故障排除。这些文件有助于识别 PowerShell 命令问题、信息缺失的邮箱以及无法与邮箱关联的设备。管理员可以使用这些文件来识别 Exchange 中可能不正确的数据。
- **改进的内存使用**：XenMobile Mail Manager 现在内存使用效率更高。管理员可以安排 XenMobile Mail Manager 自动重启，以便为系统提供一个干净的环境。
- **Microsoft .NET Framework 4.6 先决条件**：Microsoft .NET Framework 的先决条件现在是版本 4.6。

已修复的问题

- 凭据提示错误：Office 365 会话不稳定通常会导致此错误。改进的 Exchange 连接增强功能解决了此问题。(XMHELP-293, XMHELP-311, XMHELP-801)
- 邮箱和设备计数不准确：XenMobile Mail Manager 具有改进的邮箱到设备关联算法。改进的诊断功能有助于识别 XenMobile Mail Manager 认为不在其职责范围内的邮箱和设备。(XMHELP-623)
- 允许/阻止/擦除命令无法识别：已修复一个错误，该错误导致 XenMobile 邮件管理器 的允许/阻止/擦除命令有时无法识别。(XMHELP-489)
- 内存管理：更好的内存管理和缓解措施。(XMHELP-419)

体系结构

下图显示了用于 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。



三个主要组件是：

- **Exchange ActiveSync 访问控制管理：**与 XenMobile 通信以从 XenMobile 检索 Exchange ActiveSync 策略，并将此策略与任何本地定义的策略合并，以确定应允许或拒绝访问 Exchange 的 Exchange ActiveSync 设备。本地策略允许扩展策略规则，以通过 Active Directory 组、用户、设备类型或设备用户代理（通常是移动平台版本）进行访问控制。
- **远程 PowerShell 管理：**负责调度和调用远程 PowerShell 命令，以执行由 Exchange ActiveSync 访问控制管理编译的策略。定期获取 Exchange ActiveSync 数据库的快照，以检测新增或更改的 Exchange ActiveSync 设备。
- **移动服务提供商：**提供 Web 服务接口，以便 XenMobile 可以查询 Exchange ActiveSync、查询 Blackberry 设备，并对 ActiveSync 和 Blackberry 设备执行擦除等控制操作。

系统要求和必备条件

使用用于 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 January 14, 2020 结束，对 Windows Server 2012 R2 的支持将于 October 10, 2023 结束。
- Microsoft SQL Server 2016 服务包 2 或 SQL Server 2014 服务包 3。
- Microsoft .NET 框架 4.6。
- 黑莓企业服务，版本 5（可选）。

Microsoft Exchange Server 支持的最低版本：

- 微软 Office 365
- Exchange 服务器 2016
- Exchange 服务器 2013（支持将于 April 11, 2023 结束）
- Exchange 服务器 2010 Service Pack 3（支持将于 January 14, 2020 结束）

必备条件

- 必须安装 Windows 管理框架。
  - PowerShell V5、V4 和 V3
- 必须通过 Set-ExecutionPolicy RemoteSigned 将 PowerShell 执行策略设置为 RemoteSigned。
- 运行适用于 Exchange ActiveSync 的 Endpoint Management 连接器 的计算机与远程 Exchange Server 之间必须打开 TCP 端口 80。
- **设备电子邮件客户端**：并非所有电子邮件客户端都始终为设备返回相同的 ActiveSync ID。由于适用于 Exchange ActiveSync 的 Endpoint Management 连接器 要求每个设备具有唯一的 ActiveSync ID，因此仅支持始终为每个设备生成相同唯一 ActiveSync ID 的电子邮件客户端。Citrix 已对以下电子邮件客户端进行测试，且未发现错误：
  - 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：

  Exchange 配置 UI 中指定的凭据必须能够连接到 Exchange Server，并被授予完全访问权限以运行以下 Exchange 特定的 PowerShell cmdlet。

  - **对于 Exchange 服务器 2010 SP2：**
    - 获取 CAS 邮箱
    - 设置 CAS 邮箱
    - 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
    - 获取邮箱
    - Get-MobileDevice
    - Get-MobileDeviceStatistics
    - 清除移动设备
    - Get-ExchangeServer
    - Get-ManagementRole
    - Get-ManagementRoleAssignment
  - 如果 Endpoint Management 的 Exchange ActiveSync 连接器配置为查看整个林，则必须已授予运行以下命令的权限：**Set-AdServerSettings -ViewEntireForest $true**
  - 提供的凭据必须已获得通过远程 Shell 连接到 Exchange Server 的权限。默认情况下，安装 Exchange 的用户拥有此权限。
  - 要建立远程连接并运行远程命令，凭据必须对应于远程计算机上的管理员用户。您可以使用 Set-PSSessionConfiguration 来消除管理要求，但该命令的讨论超出了本文档的范围。有关详细信息，请参阅 Microsoft 文章 关于会话配置。
  - 必须将 Exchange Server 配置为通过 HTTP 支持远程 PowerShell 请求。通常，只需管理员在 Exchange Server 上运行以下 PowerShell 命令即可：WinRM QuickConfig。
  - Exchange 有许多限制策略。其中一项策略控制每个用户允许的并发 PowerShell 连接数。在 Exchange 2010 上，每个用户允许的默认并发连接数为 18。当达到连接限制时，Endpoint Management 的 Exchange ActiveSync 连接器将无法连接到 Exchange Server。有多种方法可以通过 PowerShell 更改允许的最大并发连接数，但这超出了本文档的范围。如果感兴趣，请研究与 PowerShell 远程管理相关的 Exchange 限制策略。

Office 365 Exchange 的要求

- **权限：** Exchange 配置 UI 中指定的凭据必须能够连接到 Office 365，并被授予完全访问权限以运行以下 Exchange 特定的 PowerShell cmdlet：
  - 获取 CAS 邮箱

  - 设置 CAS 邮箱
  - 获取邮箱
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice 命令
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- **权限：** 提供的凭据必须已获得通过远程 Shell 连接到 Office 365 服务器的权限。默认情况下，Office 365 在线管理员拥有所需的权限。
- **限制策略：** Exchange 有许多限制策略。其中一项策略控制每个用户允许的并发 PowerShell 连接数。在 Office 365 上，每个用户允许的默认并发连接数为三个。当达到连接限制时，Endpoint Management 的 Exchange ActiveSync 连接器将无法连接到 Exchange Server。可以通过 PowerShell 更改允许的最大并发连接数，但这超出了本文档的范围。如果感兴趣，请研究与 PowerShell 远程管理相关的 Exchange 限制策略。

安装和配置

1. 单击 XmmSetup.msi 文件，然后按照安装程序中的提示安装 Endpoint Management 的 Exchange ActiveSync 连接器。
2. 在安装向导的最后一个屏幕中，保持选中“**启动配置实用程序**”。或者，从“**开始**”菜单中打开 Endpoint Management 的 Exchange ActiveSync 连接器。
3. 配置以下数据库属性：
   - 选择“**配置 > 数据库**”选项卡。
   - 输入 SQL Server 的名称（默认为 localhost）。
   - 将数据库保留为默认值 **CitrixXmm**。
4. 选择以下用于 SQL 的身份验证模式之一：
   - **SQL：** 输入有效 SQL 用户的用户名和密码。
   - **Windows 集成：** 如果选择此选项，则必须将 Endpoint Management connector for Exchange ActiveSync Service 的登录凭据更改为具有访问 SQL Server 权限的 Windows 帐户。为此，请打开**控制面板 > 管理工具 > 服务**，右键单击 Endpoint Management connector for Exchange ActiveSync Service 条目，然后单击**登录**选项卡。

如果 BlackBerry 数据库连接也选择了 Windows 集成，则此处指定的 Windows 帐户也必须被授予访问 BlackBerry 数据库的权限。

5. 单击**测试连接**以检查是否可以连接到 SQL Server，然后单击**保存**。
6. 系统会提示您重新启动服务。单击**是**。

Endpoint Management connector for Exchange ActiveSync 设置屏幕的图像(/en-us/xenmobile/server/media/xmm-install-2.png)

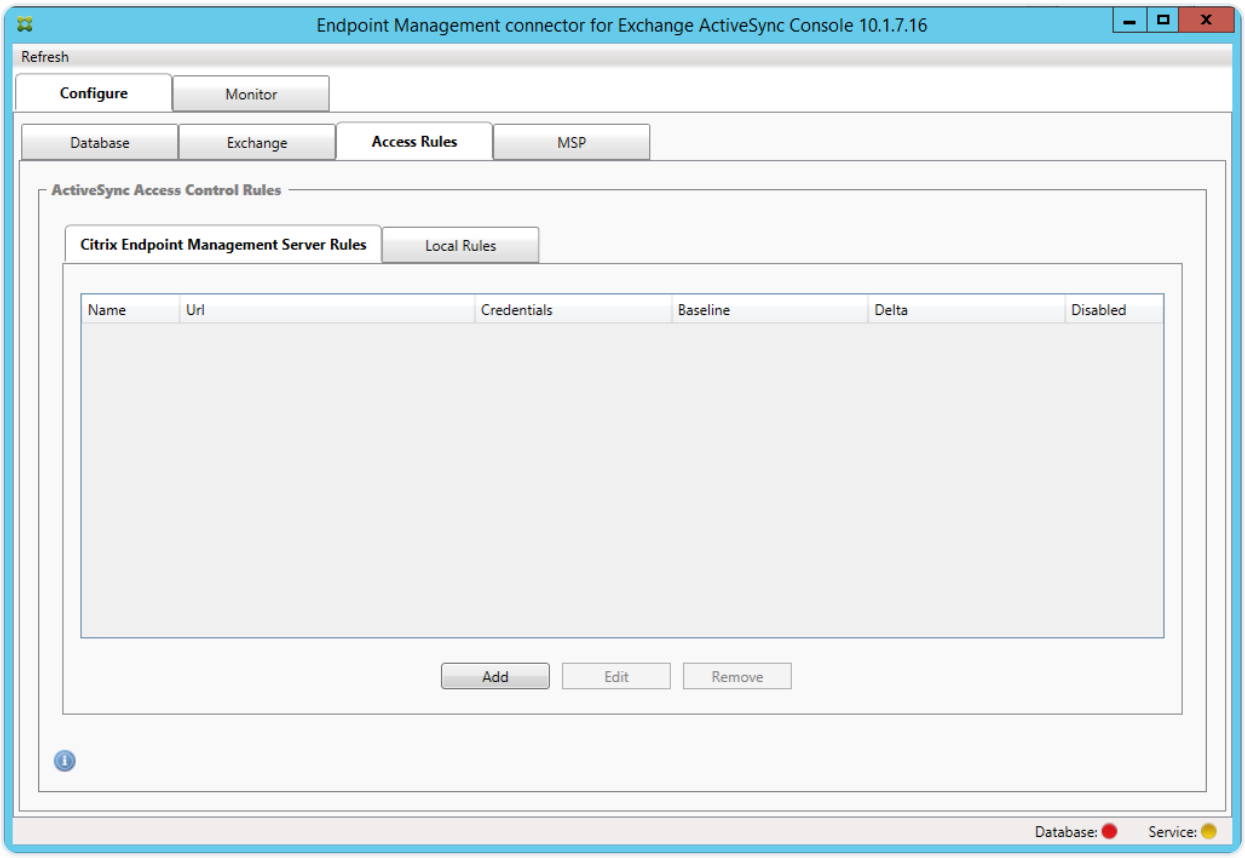
7. 配置一个或多个 Exchange Server：
   - 如果管理单个 Exchange 环境，则仅指定一个服务器。如果管理多个 Exchange 环境，则为每个 Exchange 环境指定一个 Exchange Server。
   - 单击**配置 > Exchange**选项卡，然后单击**添加**。

用于 Exchange ActiveSync 的端点管理连接器屏幕的图像(/en-us/xenmobile/server/media/connector_exchange.png)

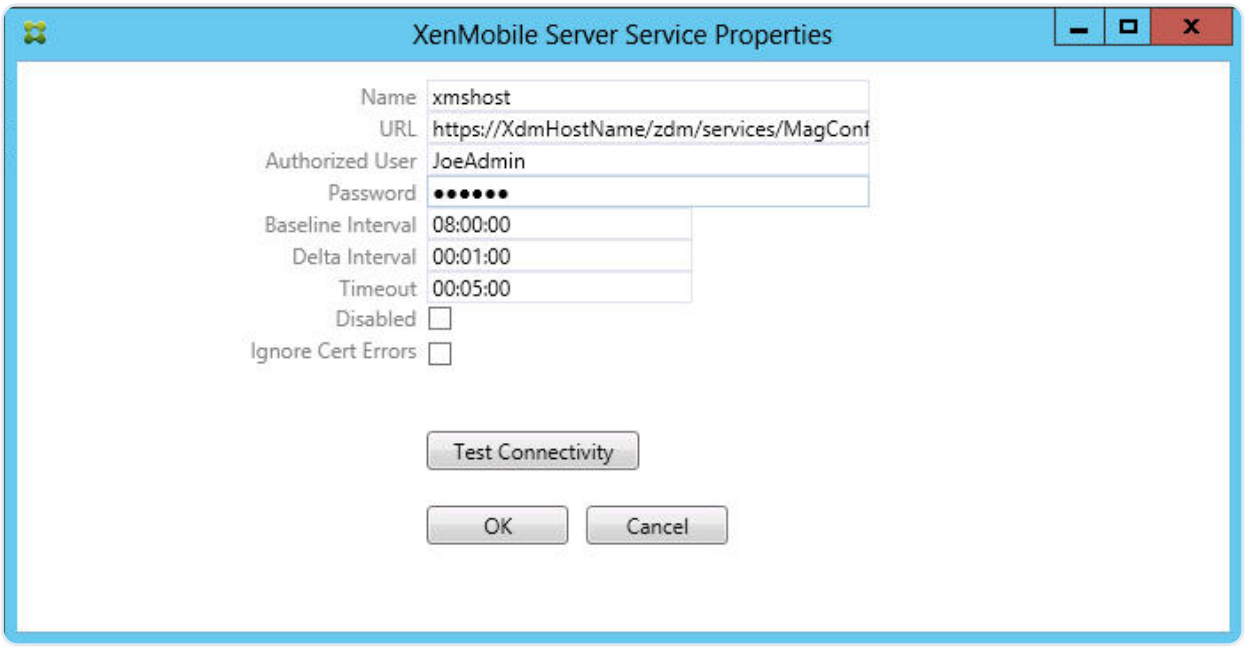
8. 选择 Exchange Server 环境类型：**本地部署**或 **Office 365**。
   - 如果选择**本地部署**，请输入用于远程 PowerShell 命令的 Exchange Server 名称。
   - 输入在“要求”部分中指定的、在 Exchange Server 上具有相应权限的 Windows 身份的**用户名**，然后输入该用户的**密码**。
   - 选择运行主要快照的计划。主要快照会检测每个 Exchange ActiveSync 伙伴关系。
   - 选择运行次要快照的计划。次要快照可检测新创建的 Exchange ActiveSync 合作伙伴关系。
   - 选择快照类型：**深度**或**浅层**。浅层快照通常速度快得多，足以执行 Endpoint Management connector for Exchange ActiveSync 的所有 Exchange ActiveSync 访问控制功能。深度快照可能需要更长时间，仅当为 ActiveSync 启用了移动服务提供商时才需要。此选项允许 XenMobile 查询非托管设备。
   - 选择默认访问权限：**允许**、**阻止**或**不变**。此设置控制除由显式 XenMobile 或本地规则标识的设备之外的所有设备的处理方式。如果选择**允许**，则允许所有此类设备访问 ActiveSync。如果选择**阻止**，则拒绝访问。如果选择**不变**，则不进行任何更改。
   - 选择 ActiveSync 命令模式：**PowerShell** 或**模拟**。
   - 在 **PowerShell** 模式下，Endpoint Management connector for Exchange ActiveSync 会发出 PowerShell 命令以实施所需的访问控制。在模拟模式下，Endpoint Management connector for Exchange ActiveSync 不会发出 PowerShell 命令，而是将预期命令和预期结果记录到数据库中。在模拟模式下，用户可以使用**监视**选项卡查看如果启用了 PowerShell 模式会发生什么情况。

- 在**连接过期**中，设置连接的生命周期（小时和分钟）。当连接达到指定时长时，该连接将被标记为已过期，因此该连接将不再使用。当不再使用过期连接时，Endpoint Management connector for Exchange ActiveSync 会正常关闭连接。当再次需要连接时，如果没有可用连接，则会初始化新连接。如果未指定，则使用默认值 30 分钟。
- 选择**查看整个林**以配置 Endpoint Management connector for Exchange ActiveSync，使其在 Exchange 环境中查看整个 Active Directory 林。
- 选择身份验证协议：**Kerberos** 或**基本**。Endpoint Management connector for Exchange ActiveSync 支持本地部署的基本身份验证。这使得 Endpoint Management connector for Exchange ActiveSync 可以在 Endpoint Management connector for Exchange ActiveSync 服务器不是 Exchange 服务器所在域的成员时使用。
- 单击**测试连接**以检查是否可以连接到 Exchange Server，然后单击**保存**。
- 系统会提示您重新启动服务。单击**是**。

9. 配置访问规则：选择**配置 > 访问规则**选项卡，单击 **XMS 规则**选项卡，然后单击**添加**。



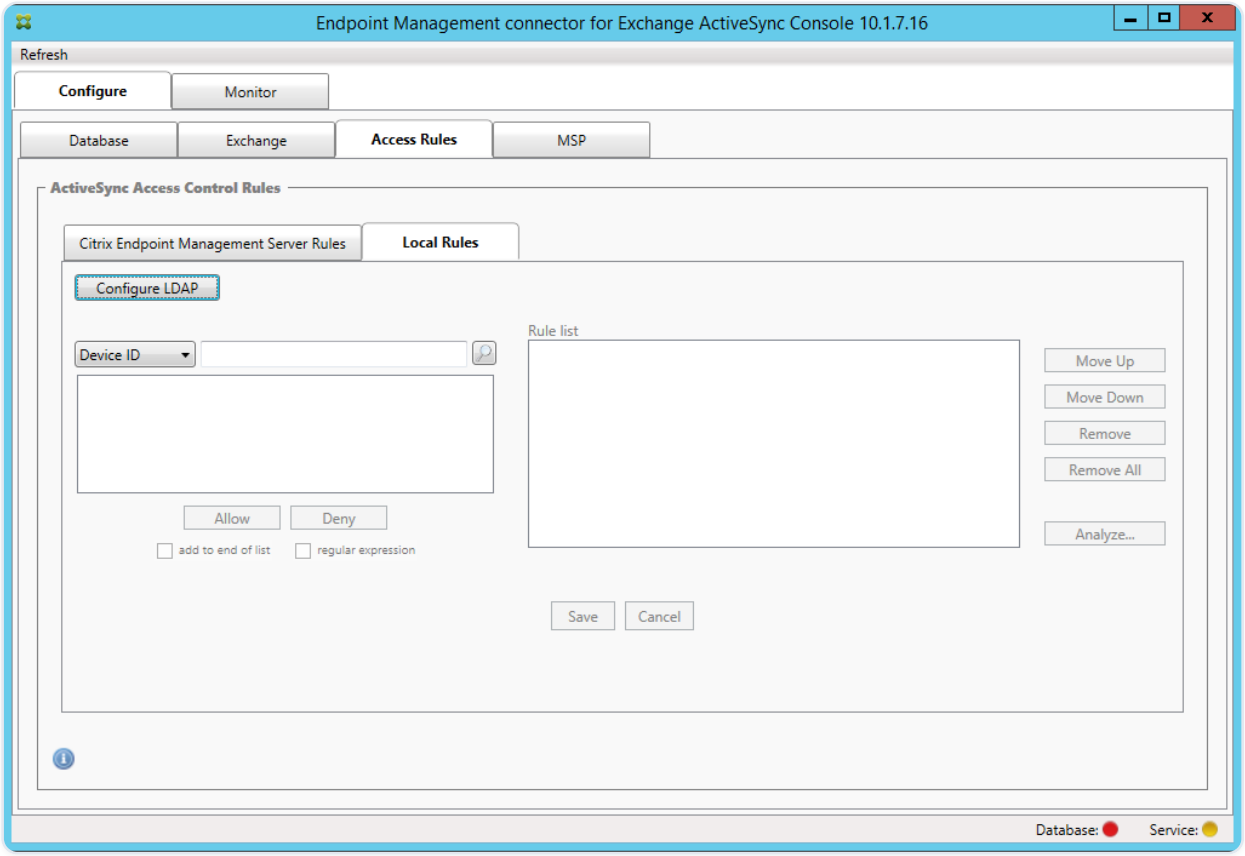
10. 在 **XenMobile 服务器服务属性**页面上，修改 URL 字符串以指向 XenMobile 服务器。例如，如果实例名称为 **zdm**，请输入 `https://<XdmHostName>/zdm/services/MagConfigService`。在此示例中，将 **XdmHostName** 替换为 XenMobile 服务器的 IP 或 DNS 地址。



- 输入服务器的授权用户。
- 输入用户的密码。
- 保留 **Baseline Interval**、**Delta Interval** 和 **Timeout** 值的默认设置。
- 单击 **Test Connectivity** 检查与服务器的连接，然后单击 **OK**。

如果选中了 **Disabled** 复选框，XenMobile Mail Service 将不会从 XenMobile 收集策略。

11. 单击 **Local Rules** 选项卡。

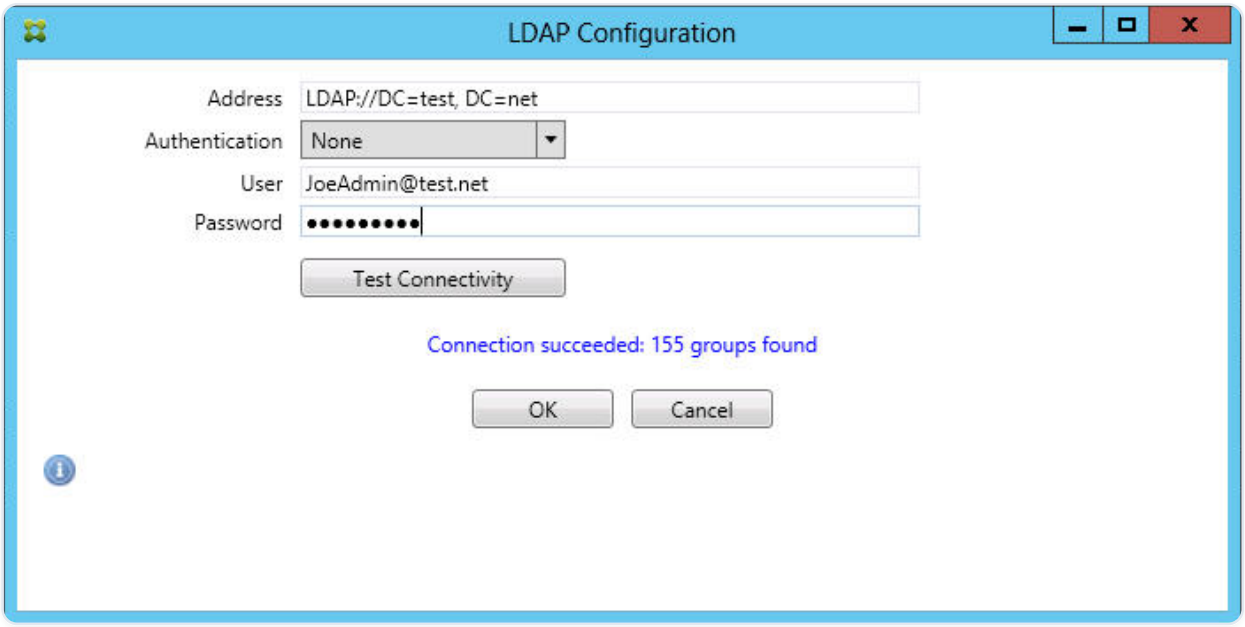


- 您可以根据 ActiveSync 设备 ID、设备类型、AD 组、用户或设备 UserAgent 添加本地规则。在列表中，选择相应的类型。
- 在文本框中输入文本或文本片段。或者，单击查询按钮以查看与该片段匹配的实体。

对于除组以外的所有类型，系统都依赖于在快照中找到的设备。因此，如果您刚开始并且尚未完成快照，则没有可用的实体。

- 选择一个文本值，然后单击 **Allow** 或 **Deny** 将其添加到右侧的 **Rule List** 窗格。您可以使用 **Rule List** 窗格右侧的按钮更改规则的顺序或将其删除。顺序很重要，因为对于给定的用户和设备，规则将按所示顺序进行评估，并且与优先级更高的规则（更靠近顶部）匹配会导致后续规则失效。例如，如果您有一条允许所有 iPad 设备的规则，以及一条后续阻止用户 Matt 的规则，Matt 的 iPad 仍将被允许，因为 iPad 规则的有效优先级高于 Matt 规则。
- 要对规则列表中的规则执行分析以查找任何潜在的覆盖、冲突或补充构造，请单击 **Analyze**，然后单击 **Save**。

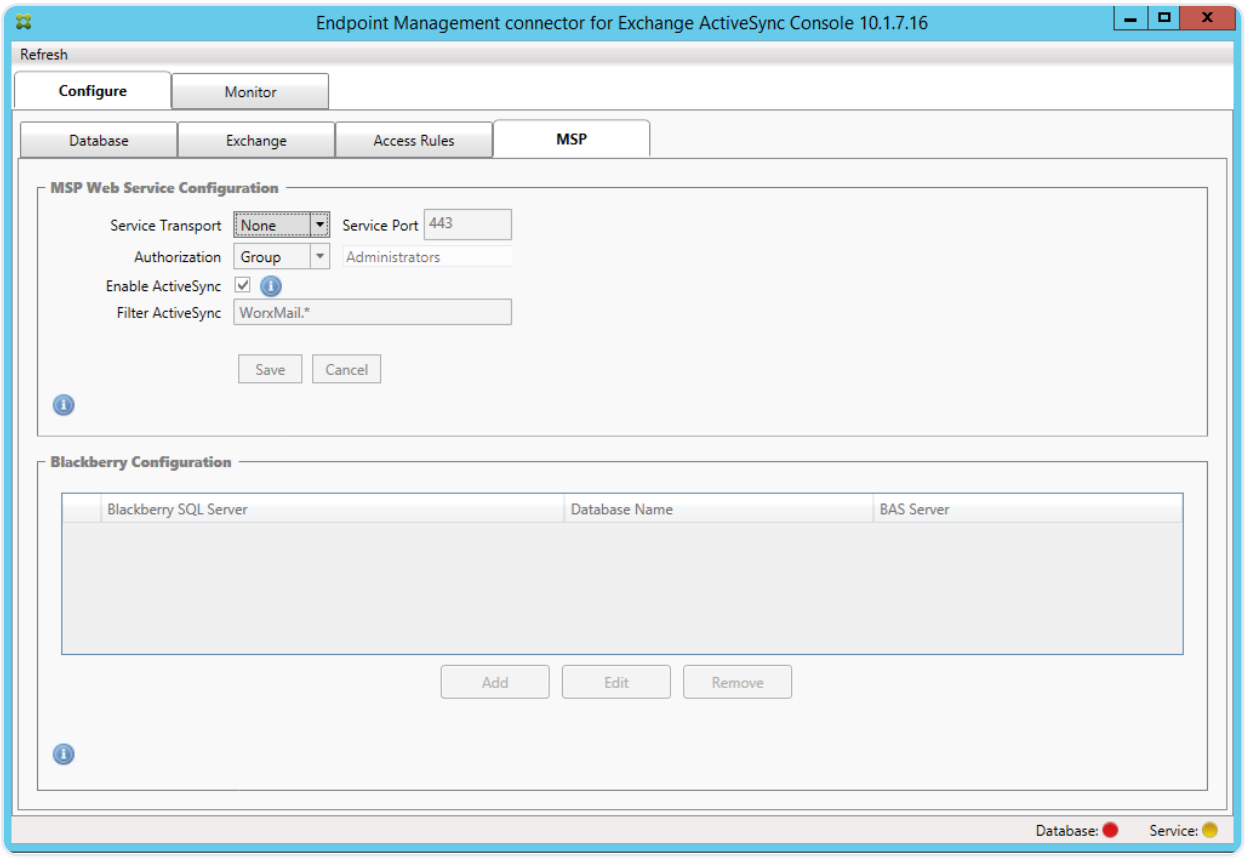
12. 如果要构建对 Active Directory 组进行操作的本地规则，请单击 **Configure LDAP**，然后配置 LDAP 连接属性。



13. 配置移动服务提供商。

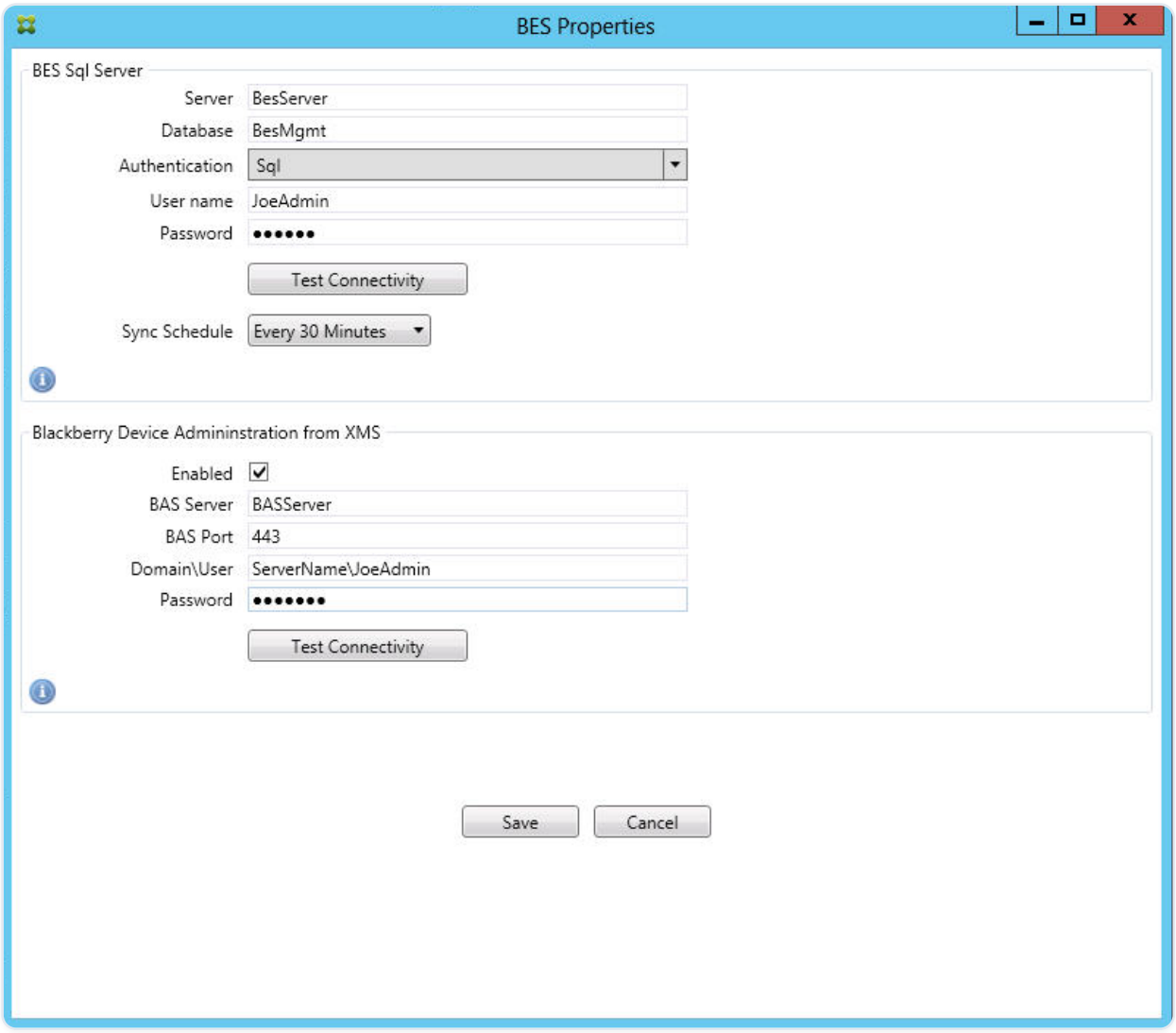
移动服务提供商是可选的。仅当 XenMobile 也配置为使用移动服务提供商接口查询非托管设备时，此设置才必要。

- 点击“**配置 > MSP**”选项卡。



- 将移动服务提供商服务的服务传输类型设置为 **HTTP** 或 **HTTPS**。
- 为移动服务提供商服务设置**服务端口**（通常为 80 或 443）。如果您使用端口 443，则该端口需要在 IIS 中绑定 SSL 证书。
- 设置**授权组**或**用户**。这将设置能够从 XenMobile 连接到移动服务提供商服务的用户或用户集。
- 设置是否启用 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“**深度**”。该设置可能会导致快照的性能成本显著增加。
- 默认情况下，与正则表达式 WorxMail.* 匹配的 ActiveSync 设备将不会发送到 XenMobile。要更改此行为，请根据需要修改“**筛选 ActiveSync**”字段。 空白表示所有设备都将转发到 XenMobile。
- 点击“**保存**”。

14. （可选）配置一个或多个 BlackBerry Enterprise Server (BES) 实例：点击“**添加**”，然后输入 BES SQL Server 的服务器名称。



- 输入 BES 管理数据库的数据库名称。
- 选择**身份验证**模式。如果选择 Windows 集成身份验证，则 Endpoint Management connector for Exchange ActiveSync 服务的用户帐户是用于连接到 BES SQL Server 的帐户。如果您还为 Endpoint Management connector for Exchange ActiveSync 数据库连接选择 Windows 集成，则此处指定的 Windows 帐户也必须被授予访问 Endpoint Management connector for Exchange ActiveSync 数据库的权限。
- 如果选择 **SQL 身份验证**，请输入用户名和密码。
- 设置**同步计划**。这是用于连接到 BES SQL Server 并检查任何设备更新的计划。
- 点击“**测试连接**”以检查与 SQL Server 的连接。如果选择 Windows 集成，此测试将使用当前登录的用户，而不是 Endpoint Management connector for Exchange ActiveSync 服务用户，因此无法准确测试 SQL 身份验证。
- 为了支持从 XenMobile 远程擦除和重置 BlackBerry 设备的密码，请选中“**已启用**”复选框。
- 输入 BES 完全限定域名 (FQDN)。
- 输入用于管理员 Web 服务的 BES 端口。

- 输入 BES 服务所需的完全限定用户和密码。
- 单击“**测试连接**”以测试与 BES 的连接。
- 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能规定某些设备未经批准不得用于企业电子邮件。为了遵循此策略，您需要确保员工无法从此类设备访问企业电子邮件。Endpoint Management connector for Exchange ActiveSync 和 XenMobile 协同工作以强制执行此类电子邮件策略。XenMobile 设置企业电子邮件访问策略，当未经批准的设备注册到 XenMobile 时，Endpoint Management connector for Exchange ActiveSync 会强制执行该策略。

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）通告自身。Secure Hub 获取一个类似的标识符，并在设备注册时将其发送给 XenMobile。通过比较这两个设备 ID，Endpoint Management connector for Exchange ActiveSync 可以确定特定设备是否应具有企业电子邮件访问权限。下图说明了此概念：

检测 ActiveSync ID 工作流图(/en-us/xenmobile/server/media/enforce-email-policies-figure.png)

如果 XenMobile 向 Endpoint Management connector for Exchange ActiveSync 发送的 ActiveSync ID 与设备发布到 Exchange 的 ID 不同，则 Endpoint Management connector for Exchange ActiveSync 无法向 Exchange 指示如何处理该设备。

ActiveSync ID 匹配在大多数平台上都能可靠工作。但是，Citrix 发现，在某些 Android 实现中，来自设备的 ActiveSync ID 与邮件客户端向 Exchange 通告的 ID 不同。为缓解此问题，您可以执行以下操作：

- 在 Samsung SAFE 平台上，从 XenMobile 推送设备 ActiveSync 配置。

为确保您的企业电子邮件访问策略得到正确执行，您可以采取防御性安全态势，并将 Endpoint Management connector for Exchange ActiveSync 配置为默认情况下通过将静态策略设置为“拒绝”来阻止电子邮件。这意味着，如果员工在 Android 设备上配置电子邮件客户端，并且 ActiveSync ID 检测无法正常工作，则该员工将被拒绝企业电子邮件访问。

访问控制规则

用于 Exchange ActiveSync 的 Endpoint Management 连接器提供了一种基于规则的方法，用于动态配置 Exchange ActiveSync 设备的访问控制。一个用于 Exchange ActiveSync 的 Endpoint Management 连接器访问控制规则由两部分组成：匹配表达式和所需的访问状态（允许或阻止）。可以针对给定的 Exchange ActiveSync 设备评估规则，以确定该规则是否适用于或匹配该设备。有

多种匹配表达式；例如，规则可以匹配给定设备类型的所有设备、特定的 Exchange ActiveSync 设备 ID，或特定用户的所有设备，等等。

在规则列表中添加、删除和重新排列规则的任何时候，单击“**取消**”按钮会将规则列表恢复到首次打开时的状态。除非您单击“**保存**”，否则如果您关闭“配置”工具，对该窗口所做的任何更改都将丢失。

用于 Exchange ActiveSync 的 Endpoint Management 连接器有三种类型的规则：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： 本地规则具有最高优先级：如果设备与本地规则匹配，则规则评估将停止。XenMobile Server 规则和默认访问规则都不会被咨询。本地规则通过“**配置 > 访问规则 > 本地规则**”选项卡在用于 Exchange ActiveSync 的 Endpoint Management 连接器上本地配置。支持匹配基于用户在给定 Active Directory 组中的成员身份。支持匹配基于以下字段的正则表达式：

- 活动同步设备 ID
- ActiveSync 设备类型
- 用户主体名称 (UPN)
- ActiveSync 用户代理（通常是设备平台或电子邮件客户端）

只要主要快照已完成并找到设备，您应该能够添加普通规则或正则表达式规则。如果主要快照尚未完成，您只能添加正则表达式规则。

XenMobile 服务器规则： XenMobile Server 规则是对外部 XenMobile Server 的引用，该服务器提供有关托管设备的规则。XenMobile Server 可以配置其自身的高级规则，这些规则根据 XenMobile 已知的属性（例如设备是否已越狱或设备是否包含禁用应用程序）识别要允许或阻止的设备。XenMobile 评估高级规则并生成一组允许或阻止的 ActiveSync 设备 ID，然后将这些 ID 传递给用于 Exchange ActiveSync 的 Endpoint Management 连接器。

默认访问规则： 默认访问规则的独特之处在于它可能匹配所有设备，并且始终最后评估。此规则是包罗万象的规则，这意味着如果给定设备不匹配本地规则或 XenMobile Server 规则，则设备的所需访问状态由默认访问规则的所需访问状态决定。

- **默认访问 – 允许：** 任何不匹配本地规则或 XenMobile Server 规则的设备都将被允许。
- **默认访问 – 阻止：** 任何不匹配本地规则或 XenMobile Server 规则的设备都将被阻止。
- **默认访问 - 未更改：** 任何不匹配本地规则或 XenMobile Server 规则的设备，其访问状态都不会通过用于 Exchange ActiveSync 的 Endpoint Management 连接器以任何方式修改。如果设备已被 Exchange 置于隔离模式，则不执行任何操作。例如，将设备从隔离模式中移除的唯一方法是让明确的本地规则或 XDM 规则覆盖隔离。

关于规则评估

对于 Exchange 报告给 Endpoint Management connector for Exchange ActiveSync 的每个设备，规则按以下从高到低的优先级顺序进行评估：

- 本地规则
- XenMobile Server 规则
- 默认访问规则

找到匹配项后，评估停止。例如，如果本地规则与给定设备匹配，则不会根据任何 XenMobile Server 规则或默认访问规则评估该设备。这在给定规则类型中也适用。例如，如果本地规则列表中给定设备有多个匹配项，则在遇到第一个匹配项时，评估停止。

当设备属性更改、设备添加或删除或规则本身更改时，Endpoint Management connector for Exchange ActiveSync 会重新评估当前定义的规则集。主要快照以可配置的间隔捕获设备属性更改和删除。次要快照以可配置的间隔捕获新设备。

Exchange ActiveSync 也有管理访问的规则。了解这些规则在 Endpoint Management connector for Exchange ActiveSync 环境中如何工作非常重要。Exchange 可能配置了三个级别的规则：个人豁免、设备规则和组织设置。Endpoint Management connector for Exchange ActiveSync 通过以编程方式发出远程 PowerShell 请求来影响个人豁免列表，从而实现访问控制自动化。这些是与给定邮箱关联的允许或阻止的 Exchange ActiveSync 设备 ID 列表。部署后，Endpoint Management connector for Exchange ActiveSync 有效地接管了 Exchange 中豁免列表功能的管理。有关详细信息，请参阅 Microsoft 文章 控制设备访问。

在为同一字段定义了多个规则的情况下，分析非常有用。您可以排查规则之间的关系。您从规则字段的角度执行分析。例如，规则根据匹配的字段（例如 ActiveSync 设备 ID、ActiveSync 设备类型、用户、用户代理）进行分组分析。

规则术语

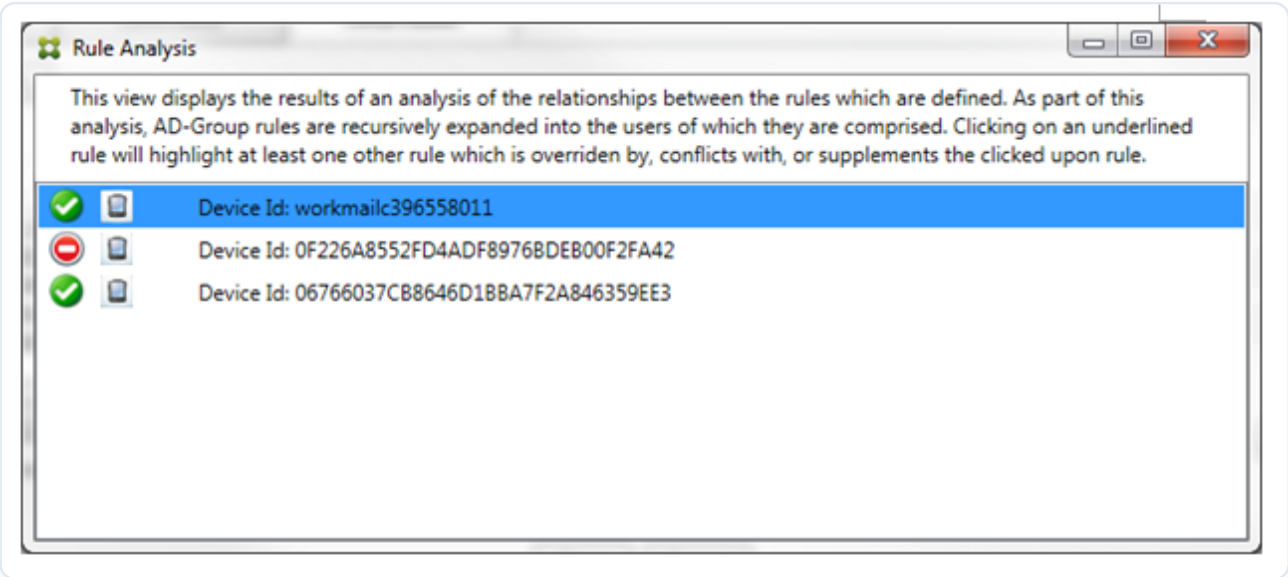
- **覆盖规则：** 当多个规则可以应用于同一设备时，就会发生覆盖。由于规则是按列表中的优先级进行评估的，因此可能适用的后续规则实例可能永远不会被评估。
- **冲突规则：** 当多个规则可能应用于同一设备但访问（允许/阻止）不匹配时，就会发生冲突。如果冲突规则不是正则表达式规则，则冲突总是隐含着覆盖。
- **补充规则：** 当多个规则是正则表达式规则时，就会发生补充，因此可能需要确保这两个（或更多）正则表达式可以合并为一个正则表达式规则，或者没有重复功能。补充规则的访问（允许/阻止）也可能发生冲突。

- **主规则：** 主规则是对话框中已单击的规则。该规则通过围绕它的实线边框在视觉上指示。该规则还将有一个或两个向上或向下的绿色箭头。如果箭头向上，则表示主规则之前存在辅助规则。如果箭头向下，则表示主规则之后存在辅助规则。任何时候只能有一个主规则处于活动状态。
- **辅助规则：** 辅助规则通过覆盖、冲突或补充关系以某种方式与主规则相关。这些规则通过围绕它们的虚线边框在视觉上指示。对于每个主规则，可以有一个到多个辅助规则。单击任何带下划线的条目时，突出显示的辅助规则始终是从主规则的角度来看的。例如，辅助规则被主规则覆盖，和/或辅助规则的访问将与主规则冲突，和/或辅助规则将补充主规则。

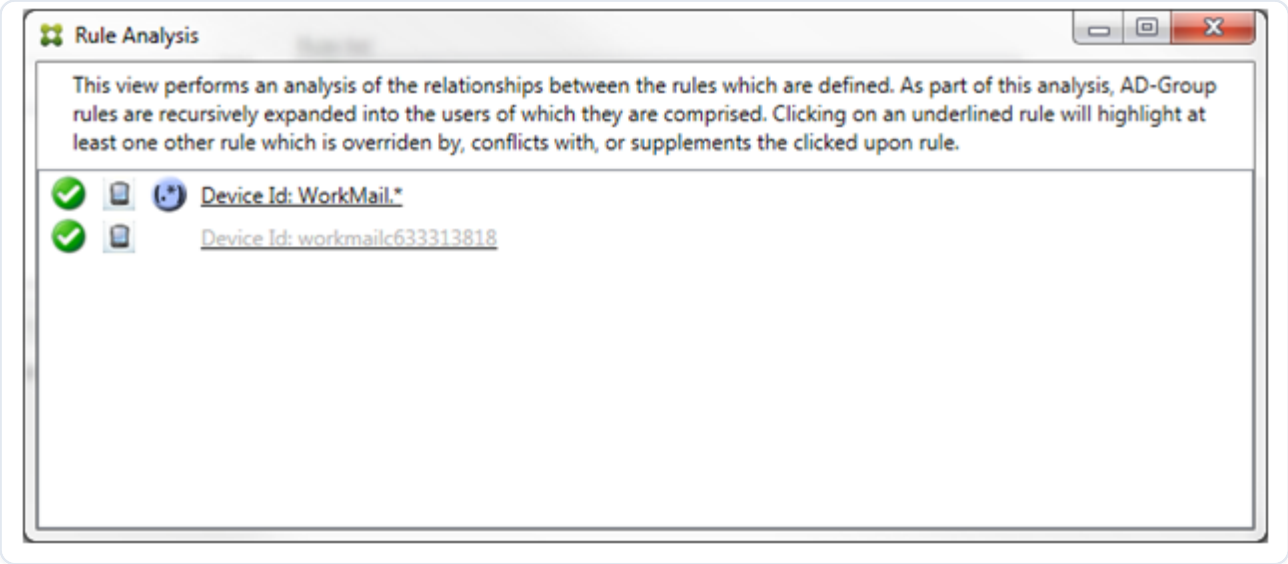
规则类型在“规则分析”对话框中的显示方式

当没有冲突、覆盖或补充时，“规则分析”对话框中没有带下划线的条目。单击任何项目都没有影响；例如，会显示正常的选中项目视觉效果。

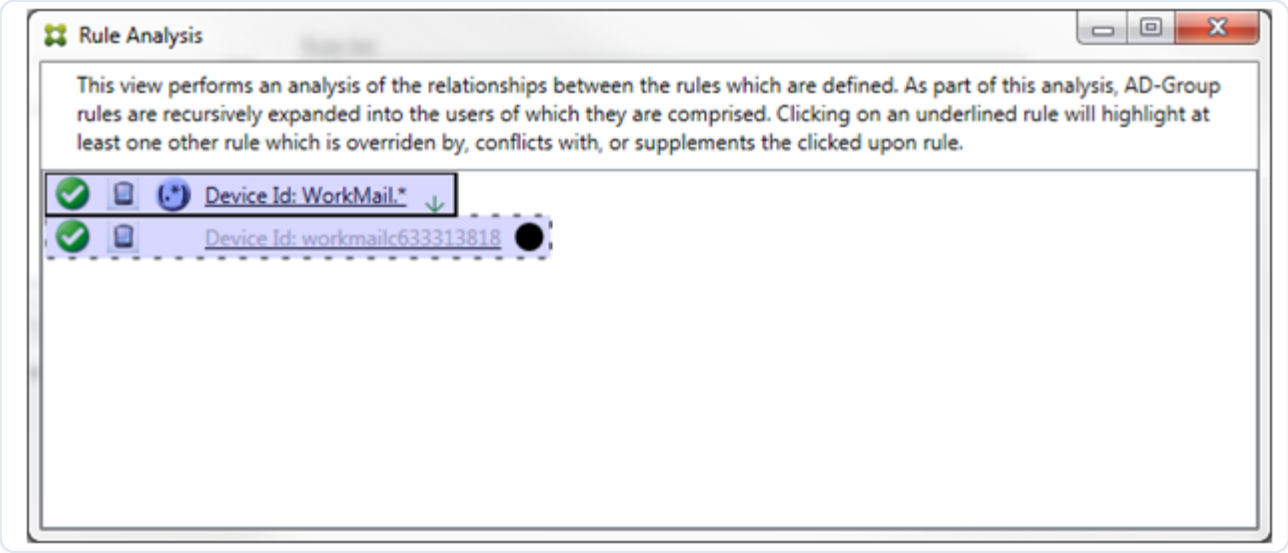
“规则分析”窗口有一个复选框，选中后，仅显示冲突、覆盖、冗余或补充的规则。



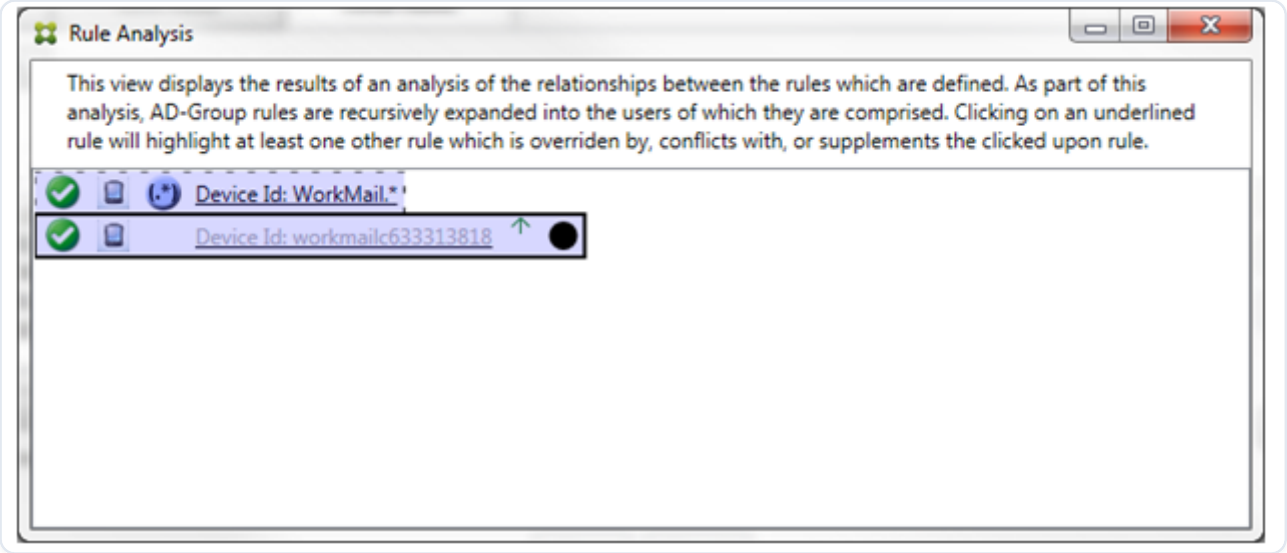
当发生覆盖时，至少有两条规则会带下划线：主要规则和辅助规则。至少有一条辅助规则以较浅的字体显示，表示该规则已被更高优先级的规则覆盖。您可以单击被覆盖的规则，以找出覆盖该规则的规则。每当被覆盖的规则因其是主要规则或辅助规则而被突出显示时，其旁边都会出现一个黑圈，作为该规则处于非活动状态的进一步视觉指示。例如，在单击该规则之前，对话框显示如下：



当您单击最高优先级的规则时，对话框显示如下：

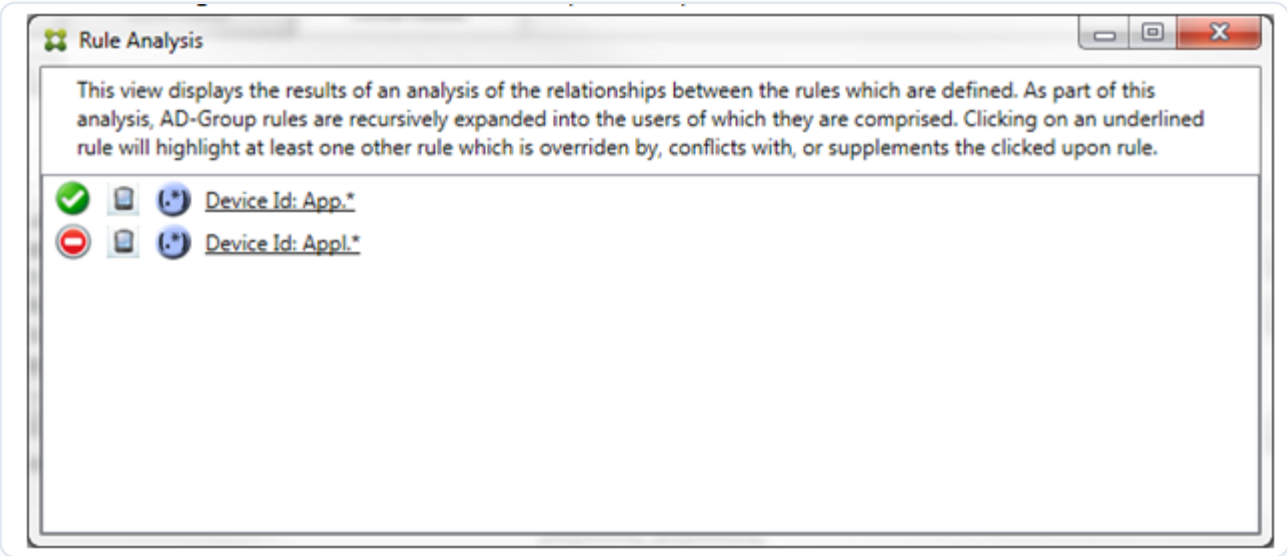


在此示例中，正则表达式规则 `WorkMail.*` 是主要规则（由实线边框指示），普通规则 `workmailc633313818` 是辅助规则（由虚线边框指示）。辅助规则旁边的黑点是一个视觉提示，进一步指示该规则由于其前面的更高优先级的正则表达式规则而处于非活动状态（永远不会被评估）。单击被覆盖的规则后，对话框显示如下：

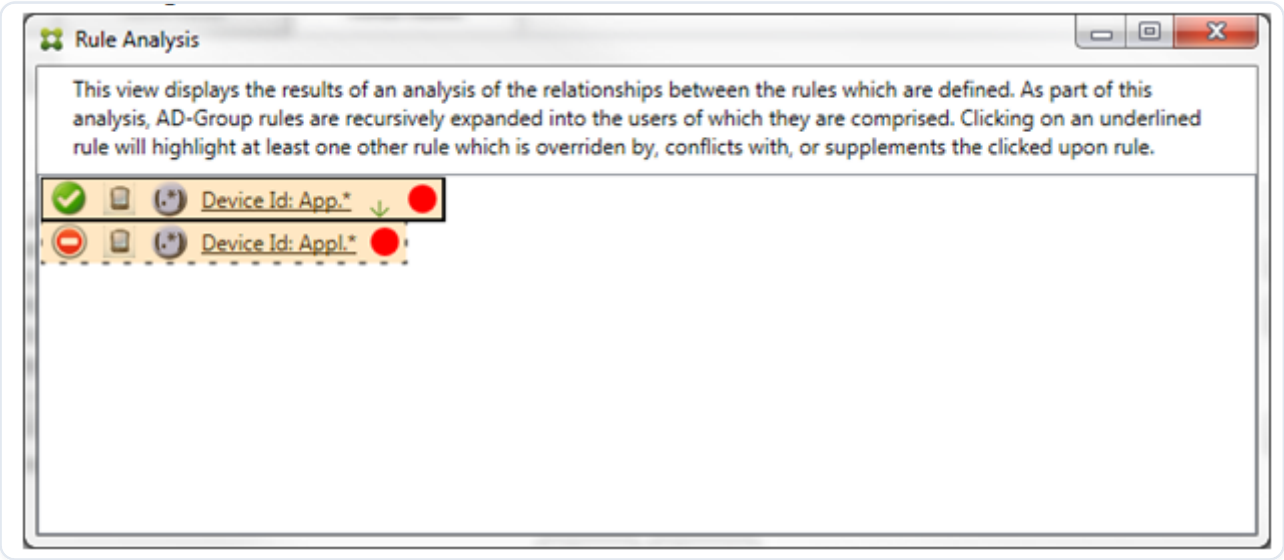


在上述示例中，正则表达式规则 `WorkMail.*` 是辅助规则（由虚线边框指示），普通规则 `workmailc633313818` 是主要规则（由实线边框指示）。对于这个简单的示例，没有太大区别。有关更复杂的示例，请参阅本主题稍后的复杂表达式示例。在定义了许多规则的场景中，单击被覆盖的规则将快速识别出是哪条或哪些规则覆盖了它。

当发生冲突时，至少有两条规则会带下划线：主要规则和辅助规则。冲突的规则由一个红点指示。仅相互冲突的规则只有在定义了两个或更多正则表达式规则时才可能出现。在所有其他冲突场景中，不仅会存在冲突，还会存在覆盖。例如，在单击其中任何一条规则之前，对话框显示如下：

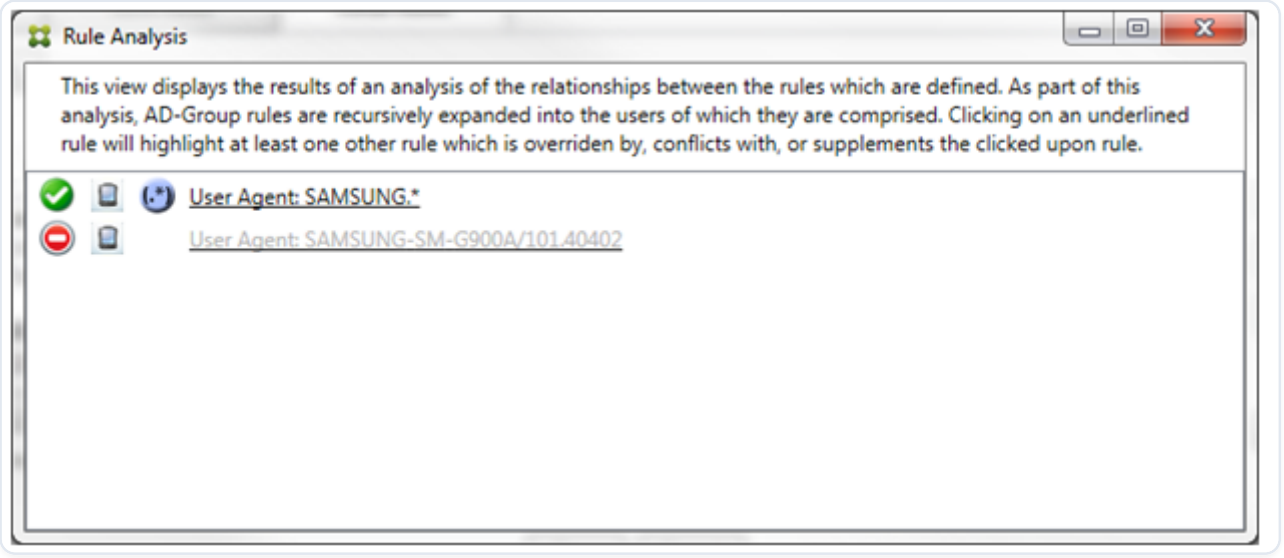


通过检查这两条正则表达式规则，显然，第一条规则允许设备 ID 包含“App”的所有设备，第二条规则拒绝设备 ID 包含“Appl”的所有设备。此外，尽管第二条规则拒绝设备 ID 包含“Appl”的所有设备，但由于允许规则的优先级更高，任何符合该条件的设备都不会被拒绝。单击第一条规则后，对话框显示如下：



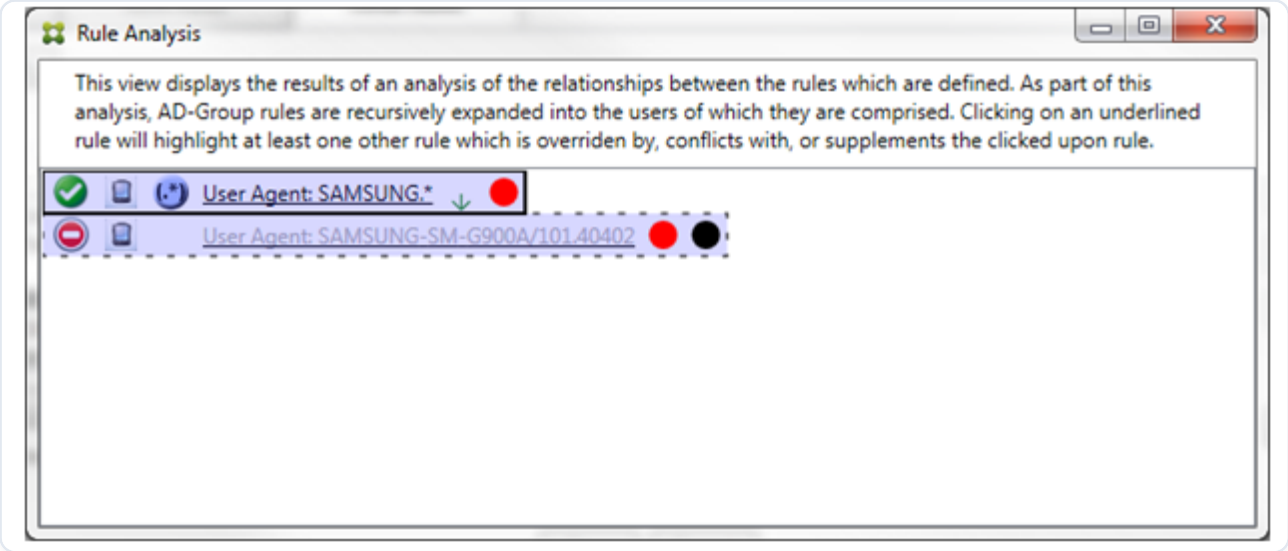
在上述场景中，主要规则（正则表达式规则 `App.*`）和辅助规则（正则表达式规则 `Appl.*`）都以黄色突出显示。这只是一个视觉警告，提醒您已将多个正则表达式规则应用于单个可匹配字段，这可能意味着冗余问题或更严重的问题。

在同时存在冲突和覆盖的场景中，主规则（正则表达式规则 `App.*`）和辅助规则（正则表达式规则 `Appl.*`）都以黄色突出显示。这只是一个视觉警告，提醒您已将多个正则表达式规则应用于单个可匹配字段，这可能意味着冗余问题或更严重的问题。



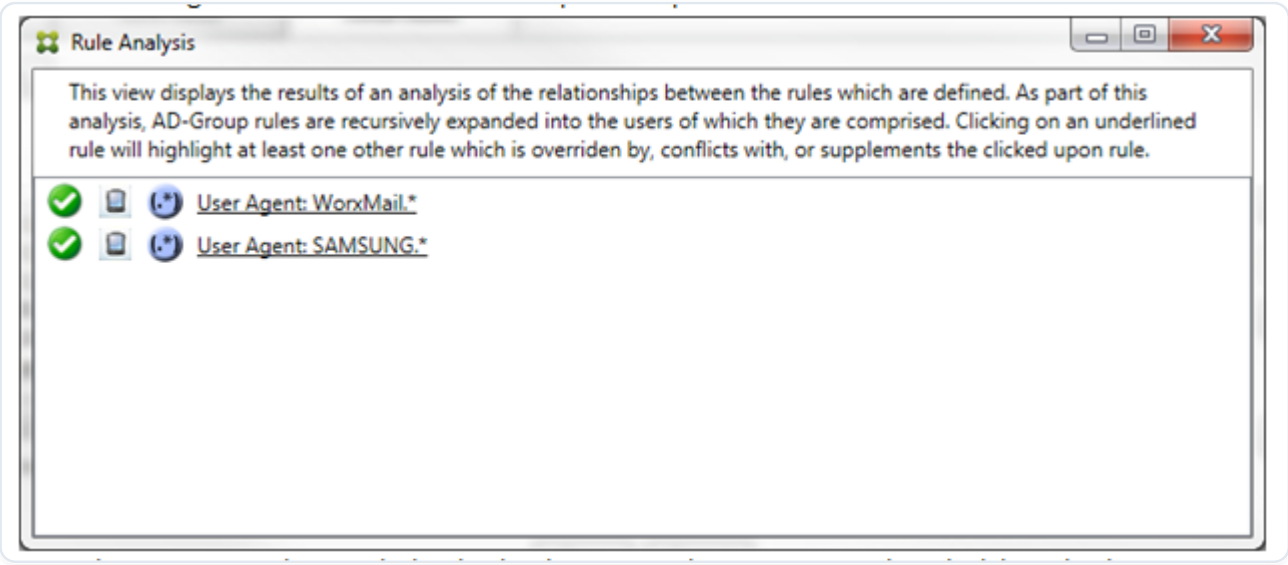
从前面的示例中很容易看出，第一个规则（正则表达式规则 `SAMSUNG.*`）不仅覆盖了下一个规则（普通规则 `SAMSUNG-SM-G900A/101.40402`），而且这两个规则的访问权限也不同（主规则指定“允许”，辅助规则指定“阻止”）。第二个规则（普通规则 `SAMSUNG-SM-G900A/101.40402`）以较浅的文本显示，表示它已被覆盖，因此处于非活动状态。

单击正则表达式规则后，对话框显示如下：

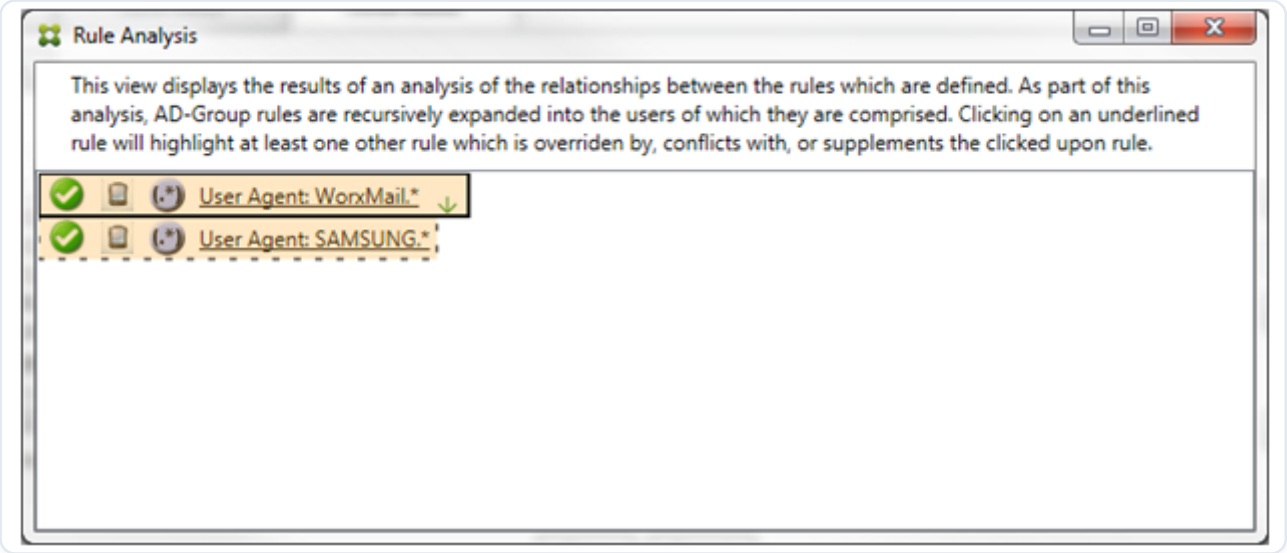


主规则（正则表达式规则 `SAMSUNG.*`）后面跟着一个红点，表示其访问状态与一个或多个辅助规则冲突。辅助规则（普通规则 `SAMSUNG-SM-G900A/101.40402`）后面跟着一个红点，表示其访问状态与主规则冲突。该规则后面还跟着一个黑点，表示它已被覆盖，因此处于非活动状态。

至少有两条规则会带下划线，即主规则和辅助规则。仅相互补充的规则将只涉及正则表达式规则。当规则相互补充时，它们会以黄色叠加层显示。在单击任一规则之前，在一个简单示例中，对话框显示如下：



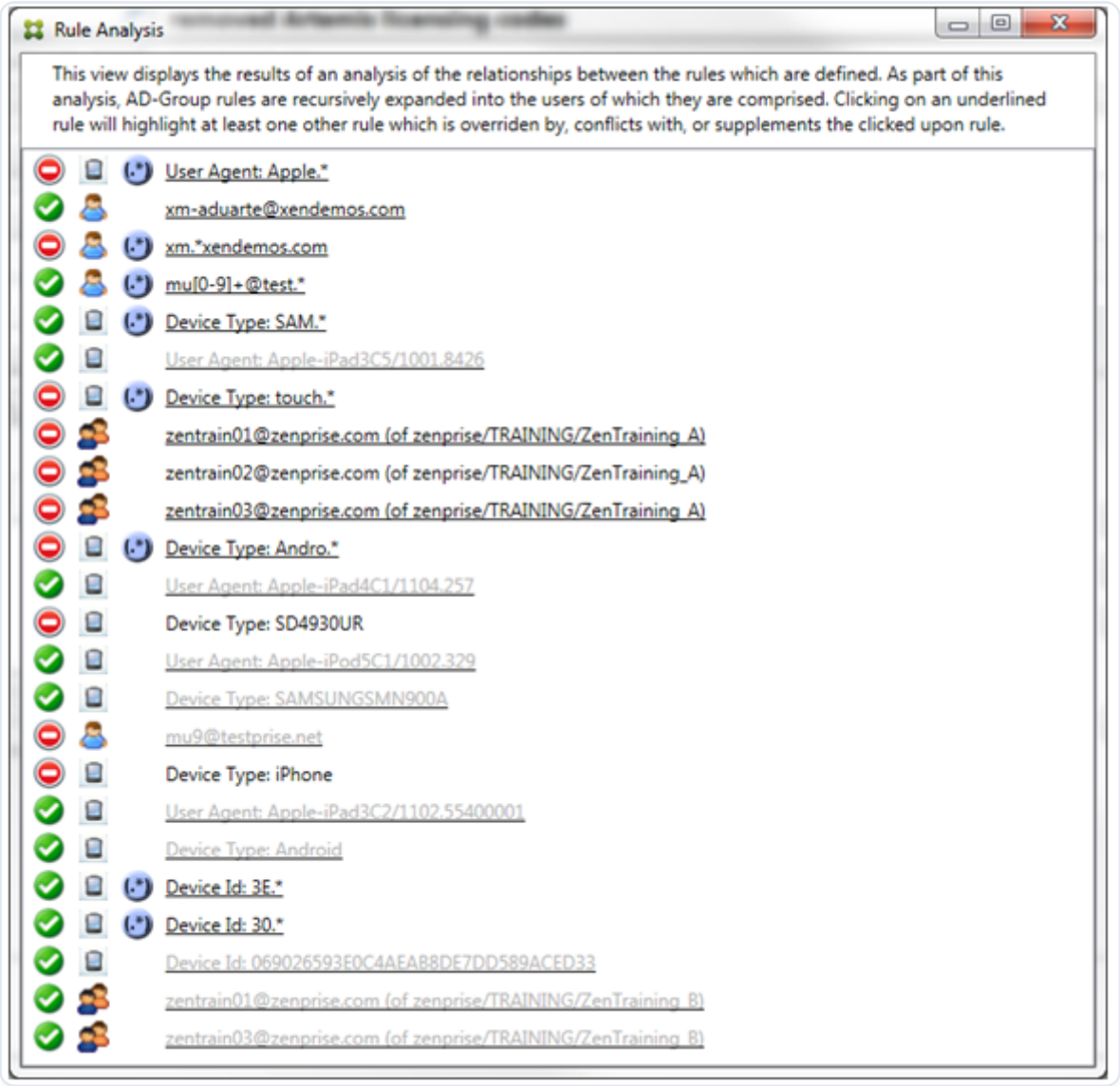
目视检查很容易发现，这两个规则都是正则表达式规则，并且都已应用于 Endpoint Management connector for Exchange ActiveSync 中的 ActiveSync 设备 ID 字段。单击第一个规则后，对话框显示如下：



主规则（正则表达式规则 `WorkMail.*`）以黄色叠加层突出显示，表示存在至少一个辅助规则也是正则表达式。辅助规则（正则表达式规则 `SAMSUNG.*`）以黄色叠加层突出显示，表示它和主规则都是应用于 Endpoint Management connector for Exchange ActiveSync 中同一字段的正则表达式规则。在这种情况下，该字段是 ActiveSync 设备 ID。正则表达式可能重叠，也可能不重叠。您需要自行决定您的正则表达式是否正确编写。

复杂表达式示例

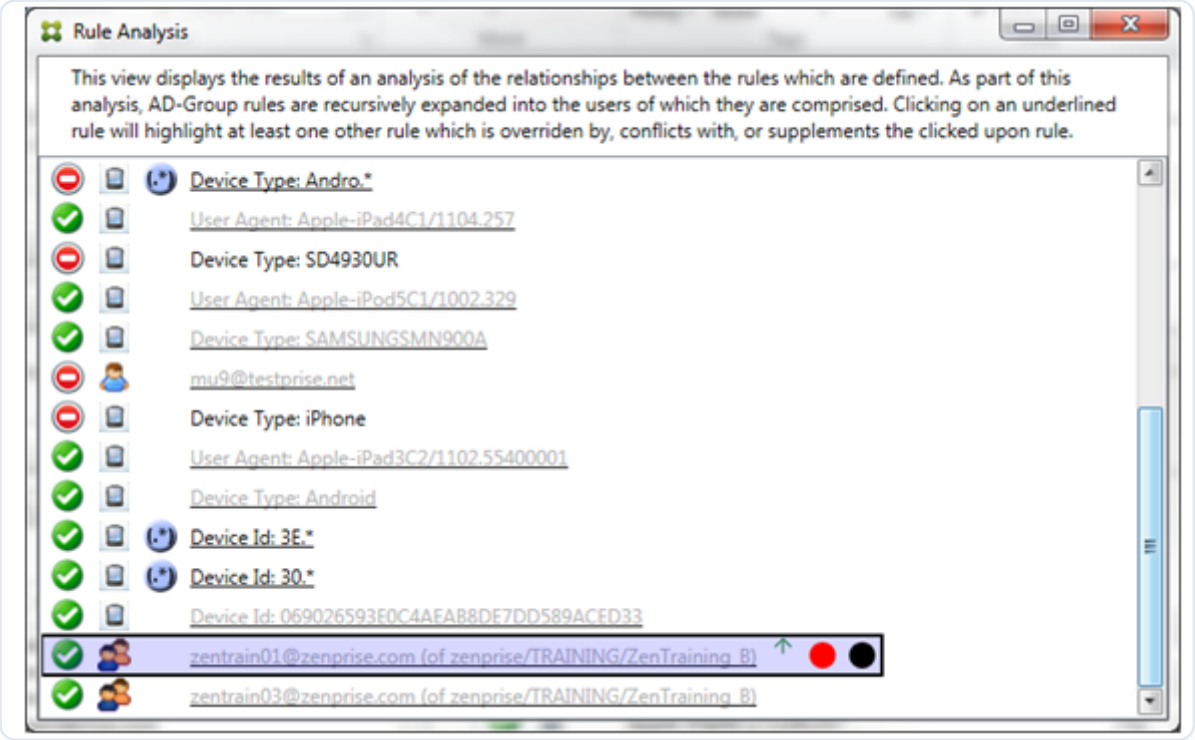
可能会出现许多潜在的覆盖、冲突或补充，因此无法给出所有可能场景的示例。以下示例讨论了不应做的事情，同时也说明了规则分析可视化构造的全部功能。下图中的大多数项目都带有下划线。许多项目以较浅的字体呈现，这表明相关规则已以某种方式被更高优先级的规则覆盖。列表中还包含各种正则表达式规则，如 图标所示。



如何分析覆盖

要查看哪些规则覆盖了特定规则，请单击该规则。

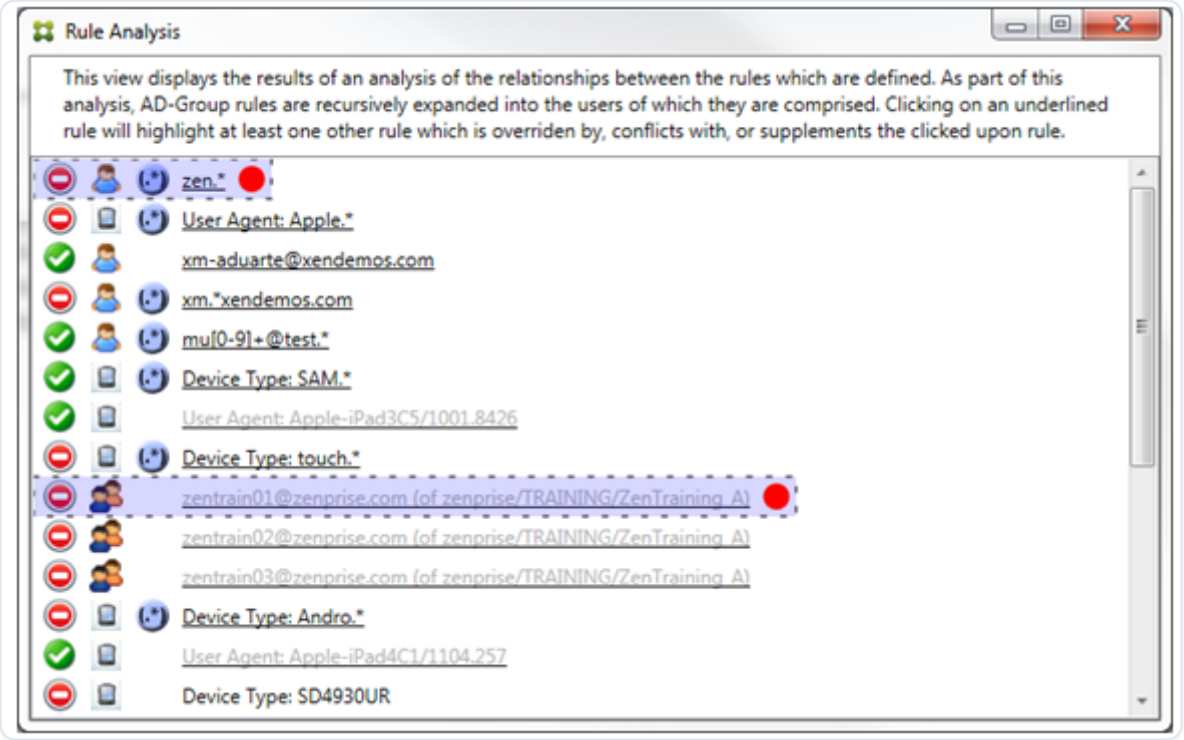
示例 1： 本示例探讨了 `zentrain01@zenprise.com` 被覆盖的原因。



主要规则（AD 组规则 `zenprise/TRAINING/ZenTraining B`，其中 `zentrain01@zenprise.com` 是成员）具有以下特征：

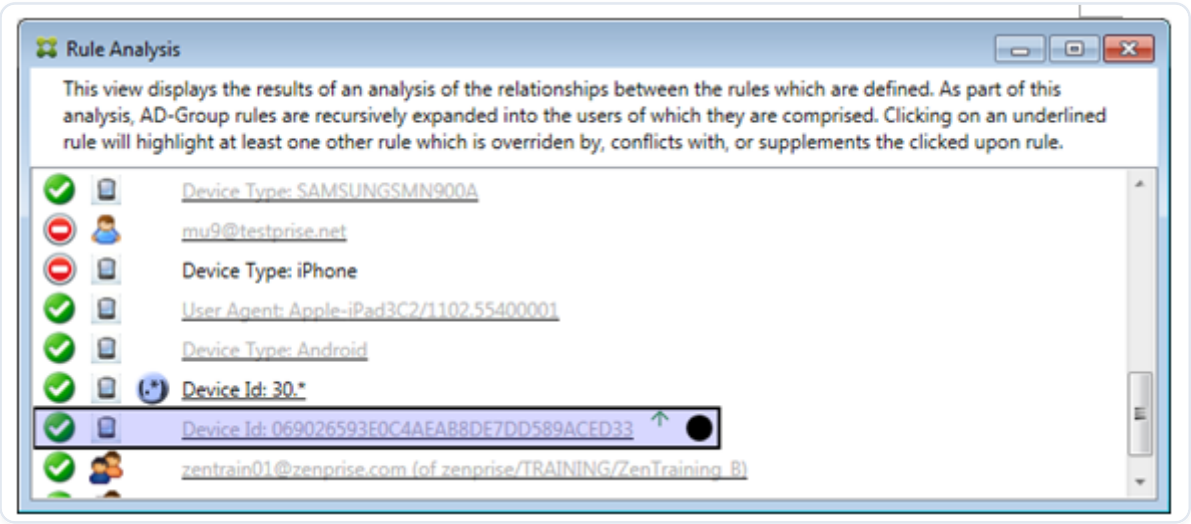
- 以蓝色突出显示并具有实心边框。
- 具有向上指向的绿色箭头（表示所有辅助规则都位于其上方）。
- 后面跟着一个红色圆圈和一个黑色圆圈，分别表示一个或多个辅助规则与其访问权限冲突，以及主要规则已被覆盖因此处于非活动状态。

向上滚动时，您会看到以下内容：



在这种情况下，有两个辅助规则覆盖了主要规则：正则表达式规则 `zen.*` 和普通规则 `zentrain01@zenprise.com` （属于 `zenprise/TRAINING/ZenTraining A` ）。对于后一个辅助规则，发生的情况是 Active Directory 组规则 `ZenTraining A` 包含用户 `zentrain01@zenprise.com`，并且 Active Directory 组规则 `ZenTraining B` 也包含用户 `zentrain01@zenprise.com`。然而，由于辅助规则的优先级高于主要规则，因此主要规则已被覆盖。主要规则的访问权限是“允许”，并且由于两个辅助规则的访问权限都是“阻止”，因此所有规则都带有一个红色圆圈，以进一步指示访问冲突。

示例 2： 本示例显示了 ActiveSync 设备 ID 为 `069026593E0C4AEAB8DE7DD589ACED33` 的设备为何被覆盖：



主要规则（普通设备 ID 规则 `069026593E0C4AEAB8DE7DD589ACED33` ）具有以下特征：

- 以蓝色突出显示并具有实心边框。

- 具有向上指向的绿色箭头（表示辅助规则位于其上方）。
- 后面跟着一个黑色的圆圈，表示辅助规则已覆盖主规则，因此处于非活动状态。

Endpoint Management 连接器 for Exchange ActiveSync 控制台页面图像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules26.png)

在这种情况下，单个辅助规则会覆盖主规则：正则表达式 ActiveSync 设备 ID 规则是 `3E.*`。因为正则表达式 `3E.*` 将匹配 `069026593E0C4AEAB8DE7DD589ACED33`，所以主规则将永远不会被评估。

如何分析补充和冲突

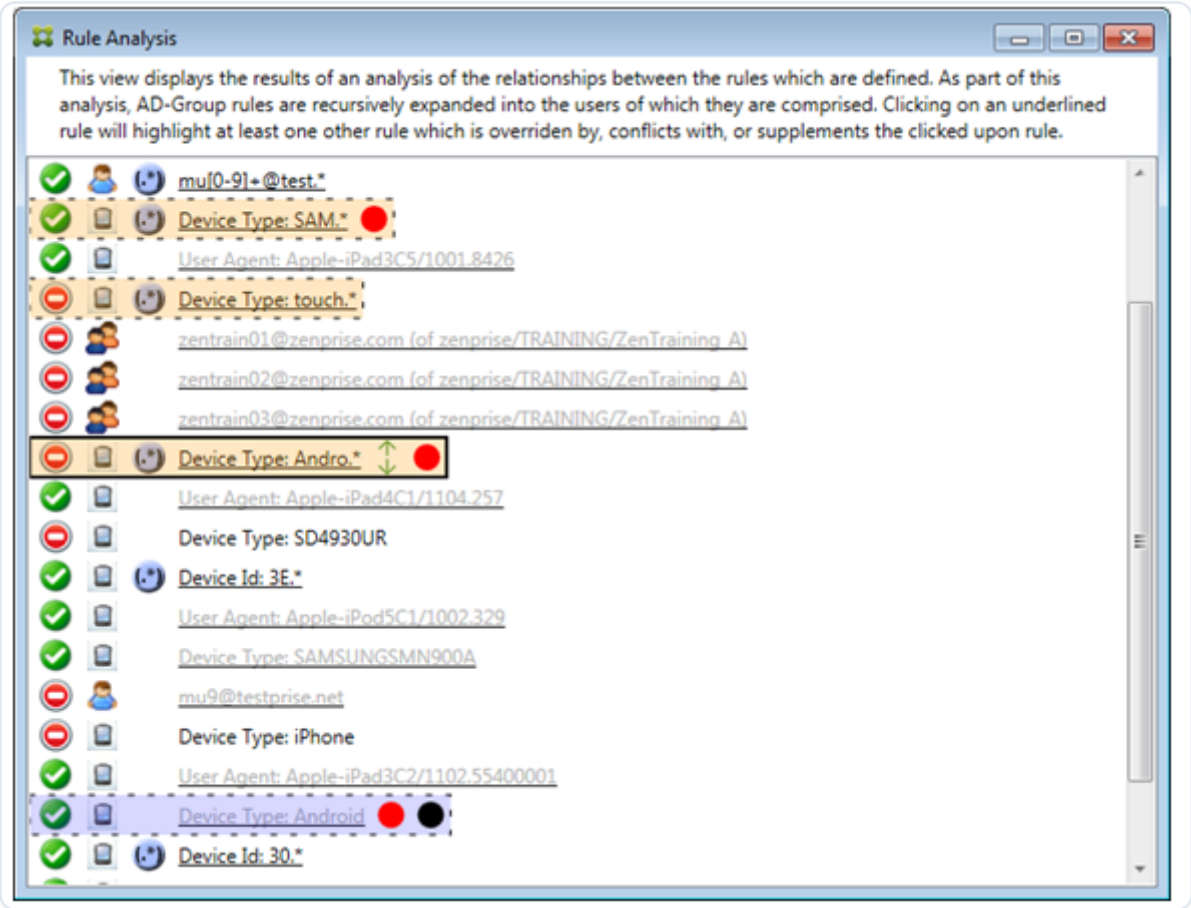
在这种情况下，主规则是正则表达式 ActiveSync 设备类型规则 `touch.*`。其特点如下：

- 由带有黄色叠加层的实心边框指示，作为警告，表示针对特定规则字段（在本例中为 ActiveSync 设备类型）运行的正则表达式规则不止一个。
- 两个箭头分别指向上和下，表示至少有一个优先级较高的辅助规则和至少一个优先级较低的辅助规则。
- 旁边的红色圆圈表示至少有一个辅助规则的访问权限设置为“允许”，这与主规则的“阻止”访问权限冲突。
- 有两个辅助规则：正则表达式 ActiveSync 设备类型规则 `SAM.*` 和正则表达式 ActiveSync 设备类型规则 `Andro.*`。
- 这两个辅助规则都用虚线边框表示它们是辅助规则。
- 这两个辅助规则都叠加了黄色，表示它们也应用于 ActiveSync 设备类型的规则字段。
- 在这种情况下，您应确保其正则表达式规则不是冗余的。

  Endpoint Management 连接器 for Exchange ActiveSync 控制台页面图像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules27.png)

如何进一步分析规则

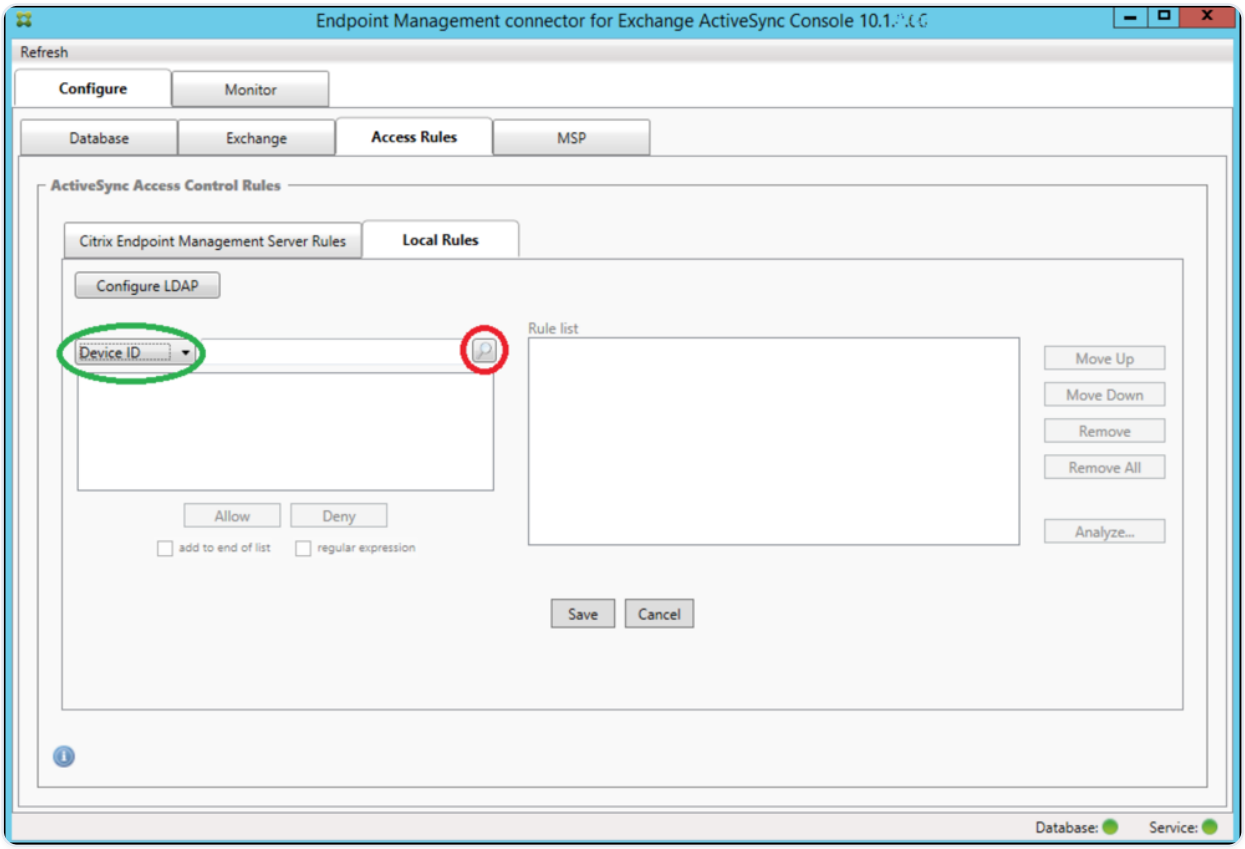
此示例探讨了规则关系始终从主规则的角度出发。前面的示例展示了如何单击应用于设备类型规则字段且值为 `touch.*` 的正则表达式规则。单击辅助规则 `Andro.*` 会显示一组不同的辅助规则被突出显示。



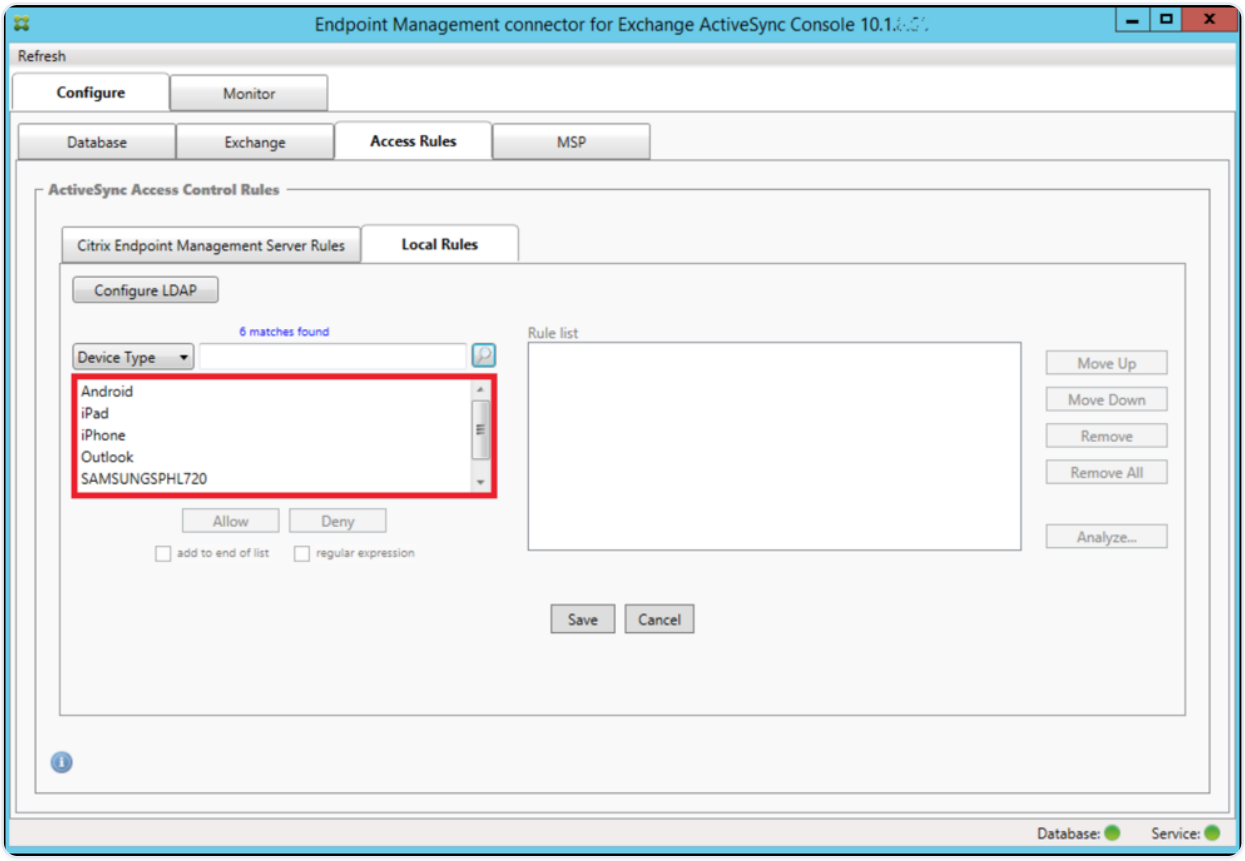
此示例显示了一个被覆盖的规则，该规则包含在规则关系中。此规则是正常的 ActiveSync 设备类型规则 `Android`，该规则已被覆盖（由变淡的字体和旁边的黑圈表示），并且其访问权限与主规则正则表达式 ActiveSync 设备类型规则 `Andro.*` 冲突。该规则在被点击之前曾是一个辅助规则。在前面的示例中，正常的 ActiveSync 设备类型规则 `Android` 未显示为辅助规则，因为从当时的主规则（正则表达式 ActiveSync 设备类型规则 `touch.*`）的角度来看，它与主规则不相关。

配置普通表达式本地规则

1. 单击**访问规则**选项卡。



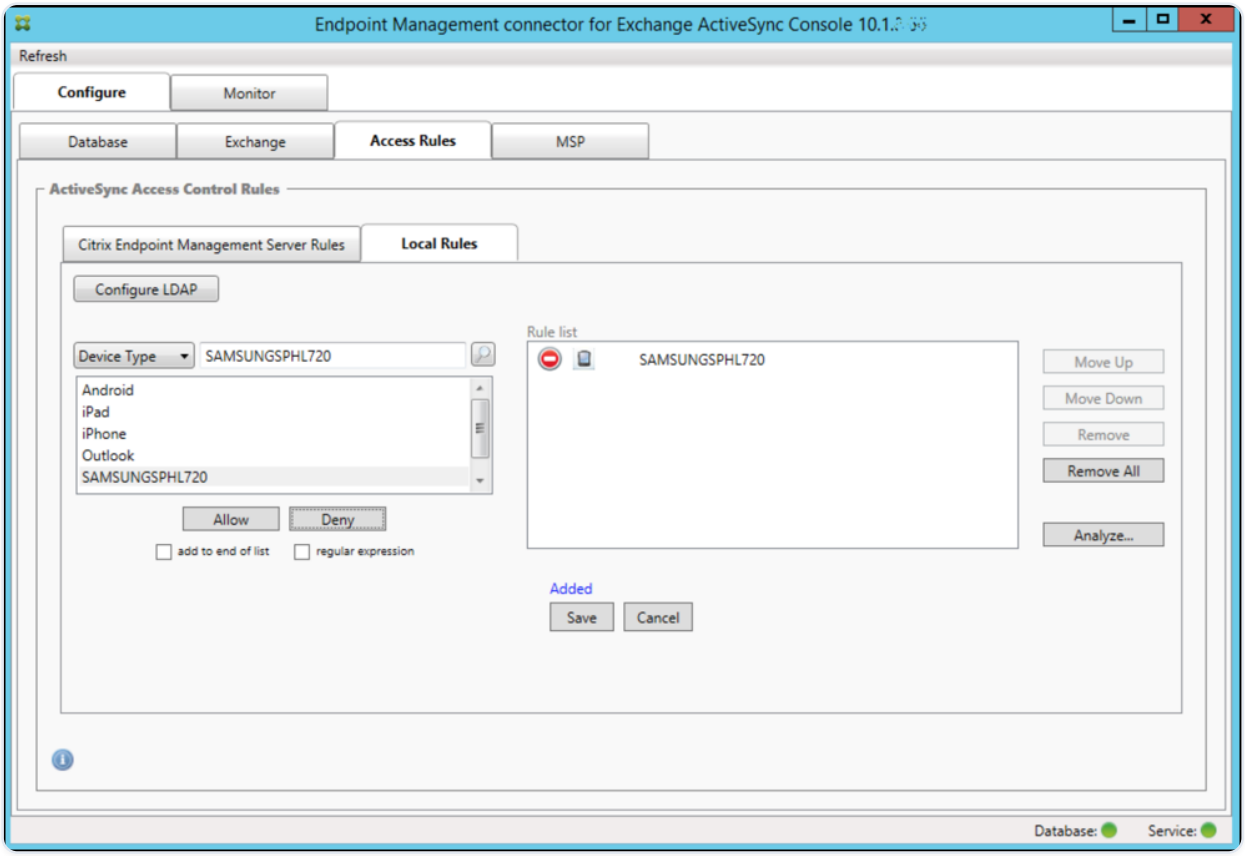
2. 在**设备 ID** 列表中，选择要为其创建本地规则的字段。
3. 单击放大镜图标以显示所选字段的所有唯一匹配项。在此示例中，已选择**设备类型**字段，并且选项显示在下面的列表框中。



4. 单击结果列表框中的某个项目，然后单击以下选项之一：

   - **允许**表示 Exchange 将配置为允许所有匹配设备的 ActiveSync 流量。
   - **拒绝**表示 Exchange 将配置为拒绝所有匹配设备的 ActiveSync 流量。

   在此示例中，设备类型为 SamsungSPhl720 的所有设备都将被拒绝访问。



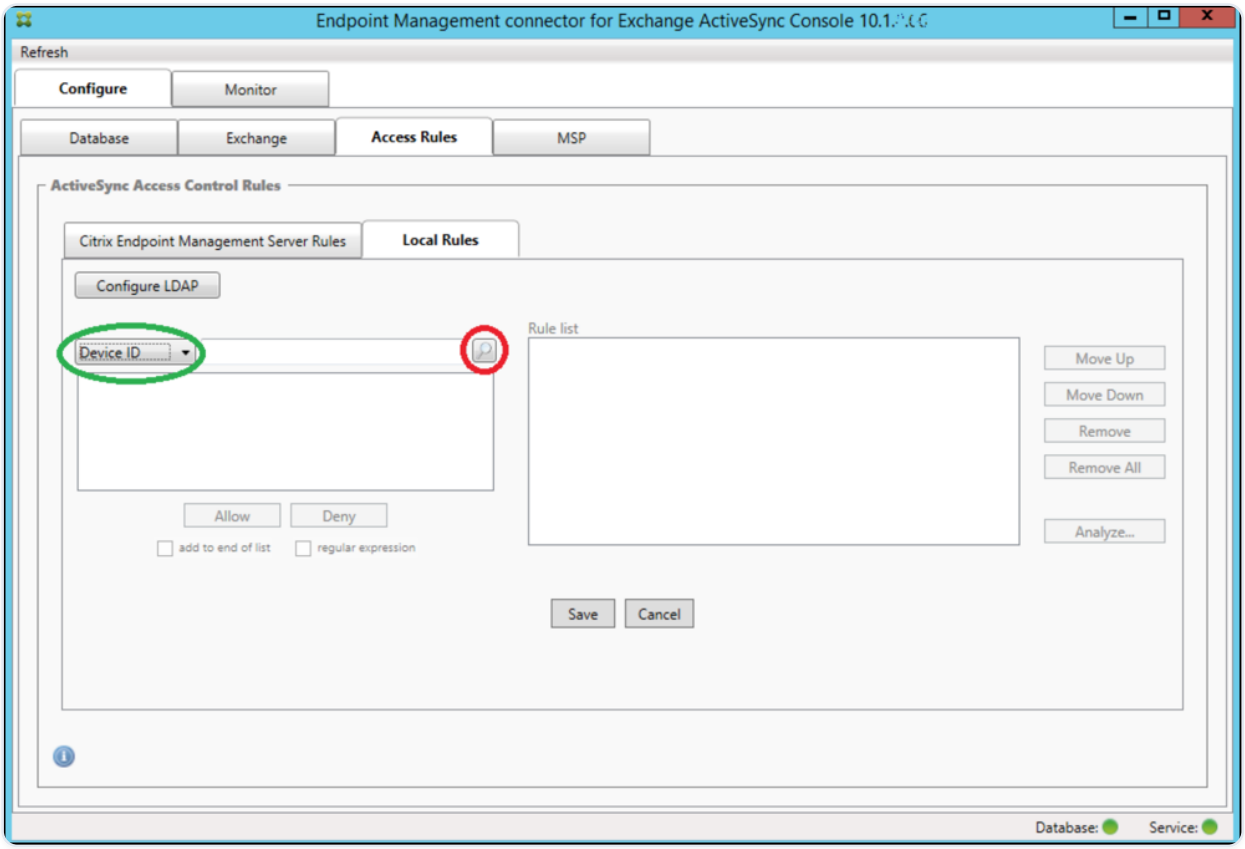
添加正则表达式

正则表达式本地规则可以通过其旁边显示的图标来区分 - 。

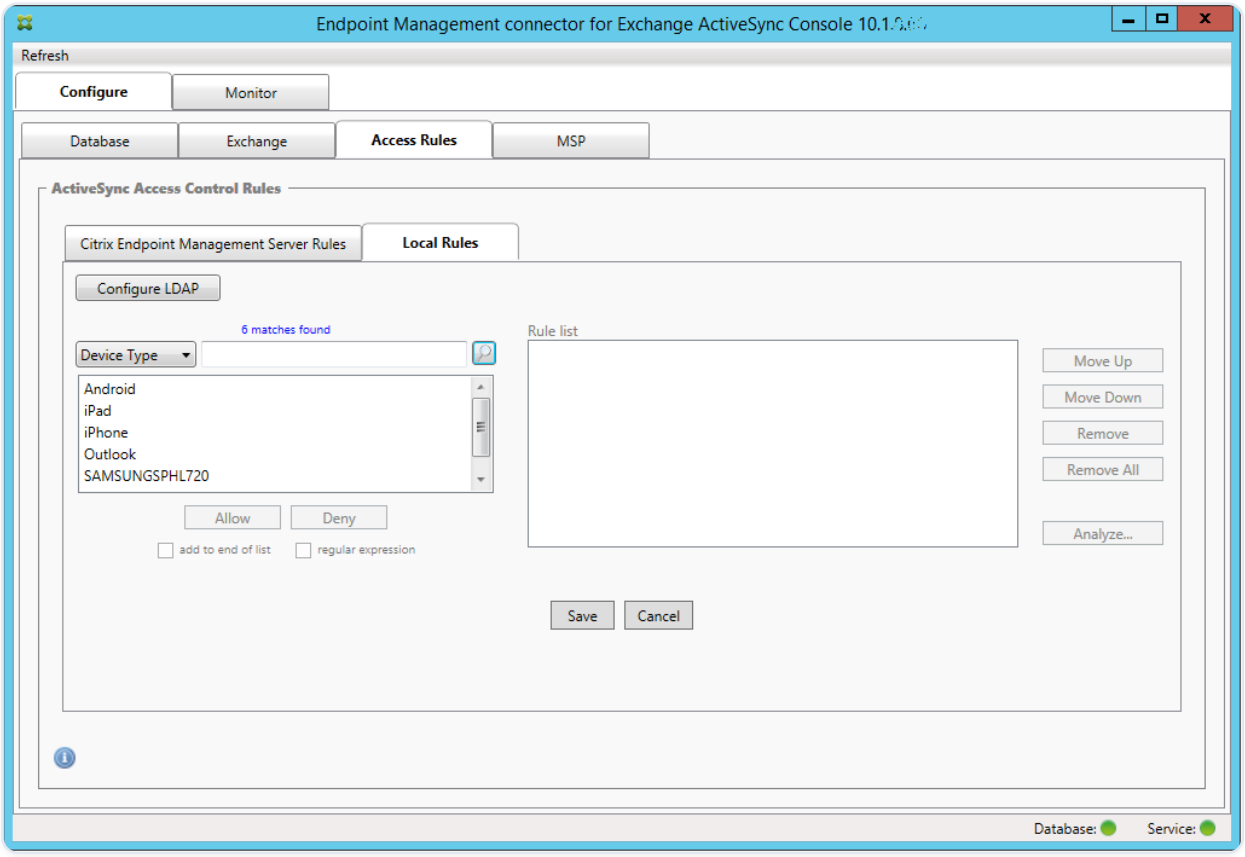
要添加正则表达式规则，您可以从给定字段的结果列表中现有值构建正则表达式规则（只要主要快照已完成），也可以直接键入所需的正则表达式。

从现有字段值构建正则表达式

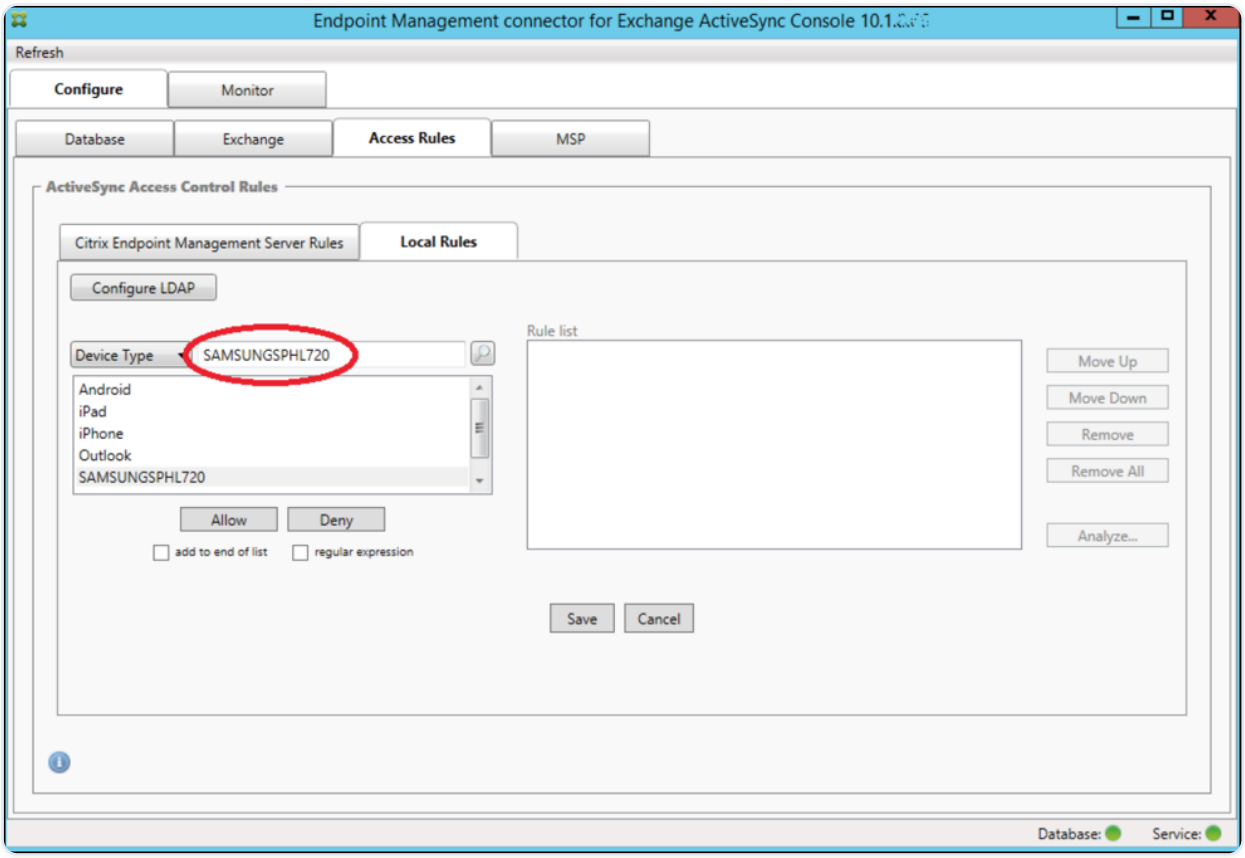
1. 单击**访问规则**选项卡。



2. 在**设备 ID** 列表中，选择要为其创建正则表达式本地规则的字段。
3. 单击放大镜图标以显示所选字段的所有唯一匹配项。在此示例中，已选择字段**设备类型**，并且选项显示在下面的列表框中。



4. 单击结果列表中的某个项目。在此示例中，已选择 **SAMSUNGSPHL720**，并显示在**设备类型**旁边的文本框中。



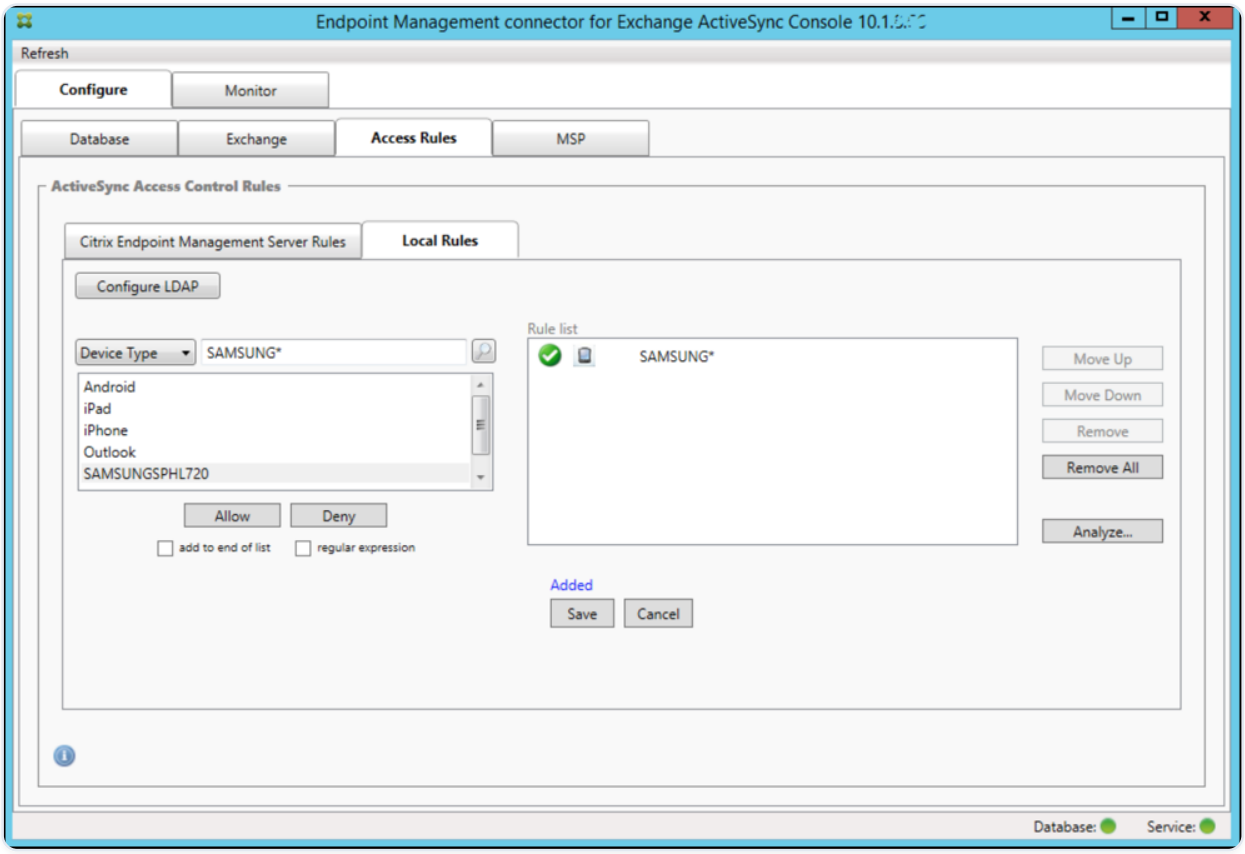
5. 要允许设备类型值中包含“Samsung”的所有设备类型，请按照以下步骤添加正则表达式规则：

   a. 单击所选项目文本框内。

   b. 将文本从 **SAMSUNGSPHL720** 更改为 **SAMSUNG.***。

   c. 确保已选中正则表达式复选框。

   d. 单击**允许**。



构建访问规则

1. 单击**本地规则**选项卡。
2. 要输入正则表达式，必须同时使用设备 ID 列表和选定项目文本框。

   Endpoint Management connector for Exchange ActiveSync 控制台页面的图像(/en-us/xenmobile/server/media/connector-exchangeactivesync-local-rule.png)

3. 选择要匹配的字段。此示例使用设备类型。
4. 键入正则表达式。此示例使用 `samsung.*`.
5. 确保选中正则表达式复选框，然后单击**允许**或**拒绝**。在此示例中，选择为**允许**。最终结果如下所示：

   Endpoint Management connector for Exchange ActiveSync 控制台页面的图像(/en-us/xenmobile/server/media/connector-exchangeactivesync-samsung-asterisk.png)

查找设备

通过选中正则表达式复选框，您可以搜索与给定表达式匹配的特定设备。此功能仅在主要快照成功完成后可用。即使不打算使用正则表达式规则，也可以使用此功能。例如，假设您要查找 ActiveSync 设备 ID 中包含文本“workmail”的所有设备。为此，请按照以下步骤操作。

1. 单击**访问规则**选项卡。

2. 确保设备匹配字段选择器设置为设备 ID（默认值）。

   Endpoint Management connector for Exchange ActiveSync 控制台页面的图像(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-tab.png)

3. 单击选定项目文本框内（如上图蓝色所示），然后键入 `workmail.*`。
4. 确保选中正则表达式复选框，然后单击放大镜图标以显示匹配项，如下图所示。

   Endpoint Management 连接器 for Exchange ActiveSync 控制台页面图像(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-localrules-regex.png)

将单个用户、设备或设备类型添加到静态规则

您可以在“**ActiveSync 设备**”选项卡上根据用户、设备 ID 或设备类型添加静态规则。

1. 单击“**ActiveSync 设备**”选项卡。
2. 在列表中，右键单击用户、设备或设备类型，然后选择是允许还是拒绝您的选择。

   下图显示了选择 user1 时的“允许/拒绝”选项。

   Endpoint Management 连接器 for Exchange ActiveSync 控制台页面图像(/en-us/xenmobile/server/media/connector-exchangeactivesync-devices-allowdeny.png)

设备监控

Endpoint Management 连接器 for Exchange ActiveSync 中的“**监视**”选项卡允许您浏览已检测到的 Exchange ActiveSync 和 BlackBerry 设备以及已发出的自动化 PowerShell 命令的历史记录。“**监视**”选项卡包含以下三个选项卡：

- **ActiveSync 设备**：
  - 您可以通过单击“**导出**”按钮导出显示的 ActiveSync 设备伙伴关系。
  - 您可以通过右键单击“**用户**”、“**设备 ID**”或“**类型**”列并选择相应的允许或阻止规则类型来添加本地（静态）规则。
  - 要折叠展开的行，请按住 Ctrl 键并单击展开的行。
- **Blackberry 设备**
- **自动化历史记录**

“**配置**”选项卡显示所有快照的历史记录。快照历史记录显示快照发生的时间、持续时间、检测到的设备数量以及发生的任何错误：

- 在“**Exchange**”选项卡上，单击所需 Exchange Server 的信息图标。
- 在“**MSP**”选项卡下，单击所需 BlackBerry Server 的信息图标。

故障排除和诊断

用于 Exchange ActiveSync 的 Endpoint Management 连接器将其错误和其他操作信息记录到其日志文件：*Install Folder*\log\XmmWindowsService.log。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

用于 Exchange ActiveSync 的 Endpoint Management 连接器包括以下日志记录级别：Error、Info、Warn、Debug 和 Trace。

> **注意：**
>
> 每个连续级别都会生成更多详细信息（更多数据）。例如，Error 级别提供的详细信息最少，而 Trace 级别提供的详细信息最多。

> 要更改日志记录级别，请执行以下操作：

1. 在 C:\Program Files\Citrix\Citrix Endpoint Management connector 中，打开 nlog.config 文件。
2. 在 `<rules>` 部分中，将 *minilevel* 参数更改为您首选的日志记录级别。例如：

```
<rules>



<logger name="*" writeTo="file" minlevel="Debug" />



</rules>
```

3. 保存文件。

   更改会立即生效。您无需重新启动用于 Exchange ActiveSync 的连接器。

常见错误

以下列表包含常见错误：

- 适用于 Exchange ActiveSync 的 Endpoint Management 连接器服务未启动

  检查日志文件和 Windows 事件日志以查找错误。典型原因如下：

  - Endpoint Management connector for Exchange ActiveSync 服务无法访问 SQL Server。这可能是由以下问题引起的：
    - SQL Server 服务未运行。
    - 身份验证失败。

    如果配置了 Windows 集成身份验证，则 Endpoint Management connector for Exchange ActiveSync 服务的用户帐户必须是允许的 SQL 登录。Endpoint Management connector for Exchange ActiveSync 服务的帐户默认为本地系统，但可以更改为具有本地管理员权限的任何帐户。如果配置了 SQL 身份验证，则必须在 SQL 中正确配置 SQL 登录。
  - 为移动服务提供商 (MSP) 配置的端口不可用。必须选择一个系统上其他进程未使用的侦听端口。

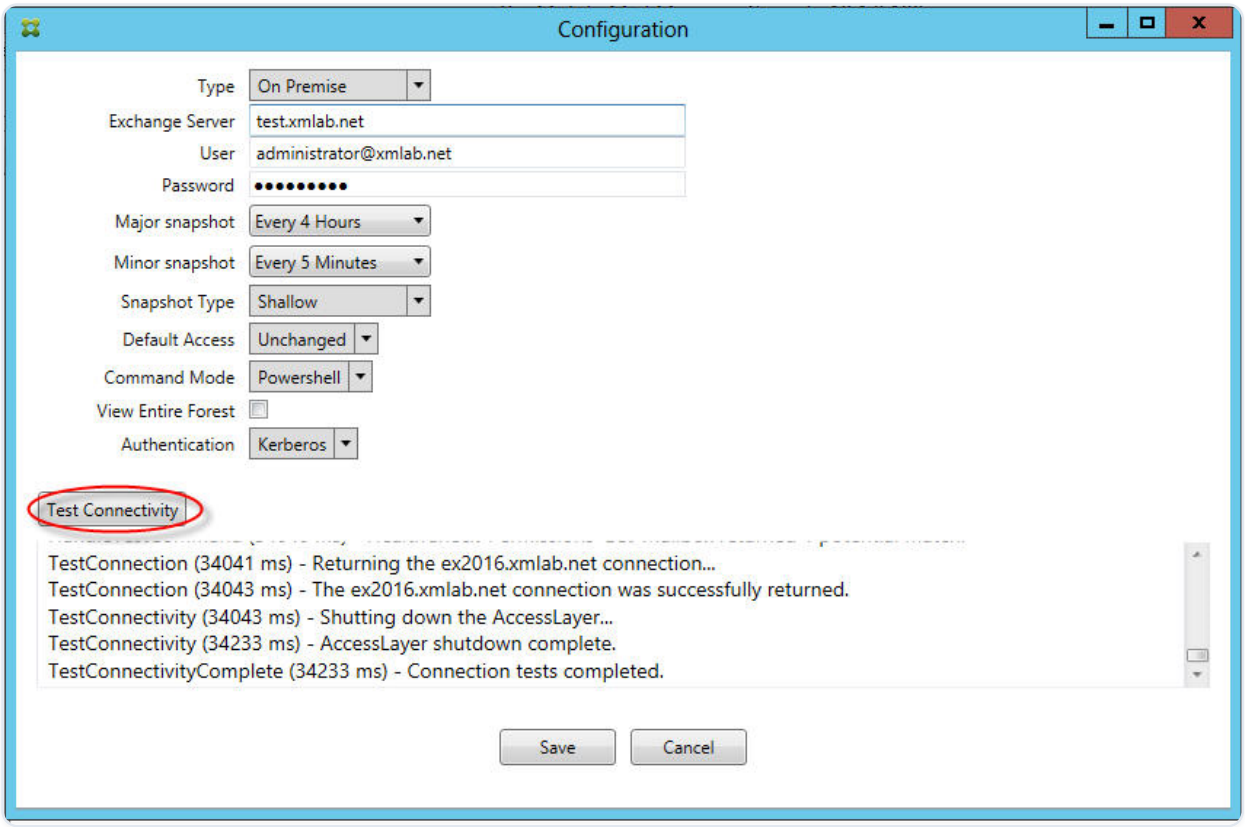
- XenMobile 无法连接到 MSP

  检查 Endpoint Management connector for Exchange ActiveSync 控制台的“**Configure > MSP**”选项卡中是否正确配置了 MSP 服务端口和传输。检查授权组或用户是否设置正确。

  如果配置了 HTTPS，则必须安装有效的 SSL 服务器证书。如果安装了 IIS，则可以使用 IIS 管理器安装证书。如果未安装 IIS，请参阅如何使用 SSL 证书配置端口以了解有关安装证书的详细信息。

  Endpoint Management connector for Exchange ActiveSync 包含一个用于测试与 MSP 服务连接的实用程序。运行 *InstallFolder*\MspTestServiceClient.exe 程序，并将 URL 和凭据设置为在 XenMobile 中配置的 URL 和凭据，然后单击“**Test Connectivity**”。这会模拟 XenMobile Server 发出的 Web 服务请求。如果配置了 HTTPS，则必须指定服务器的实际主机名（SSL 证书中指定的名称）。

  使用“**Test Connectivity**”时，请确保至少有一个 ActiveSyncDevice 记录，否则测试可能会失败。



故障排除工具

一组用于故障排除的 PowerShell 实用程序可在 **Support\PowerShell** 文件夹中找到。

故障排除工具可对用户邮箱和设备执行深入分析，检测错误情况和潜在故障区域，并对用户执行深入的 RBAC 分析。它可以将所有 cmdlet 的原始输出保存到文本文件中。

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器™

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 的连接器为充当 Exchange ActiveSync 协议反向代理的 Citrix ADC 提供 ActiveSync 客户端的设备级授权服务。授权由您在 XenMobile® 中定义的策略组合以及适用于 Exchange ActiveSync 的 Citrix Gateway 连接器在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 8.5.2。

> **重要提示：**

> 自 2022 年 10 月起，鉴于 Microsoft 此处 宣布的身份验证更改，适用于 Exchange ActiveSync 的 Endpoint Management 和 Citrix Gateway 连接器不再支持 Exchange Online。适用于 Exchange 的 Endpoint Management 连接器继续与 Microsoft Exchange Server（本地部署）配合使用。

新增功能

以下各节列出了适用于 Exchange ActiveSync 的 Citrix Gateway 连接器（前身为 XenMobile Citrix ADC Connector）当前版本和早期版本中的新增功能。

8.5.3 版中的新增功能

- 此版本增加了对 ActiveSync 协议 16.0 和 16.1 的支持。
- 已向 Google Analytics 发送的分析数据中添加了更多详细信息，尤其是关于快照的详细信息。

8.5.2 版中的新增功能

- 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了多个条件，并且其中一个条件涉及用户 ID，则可能会出现以下问题：如果用户有多个别名，则在应用规则时不会检查这些别名。

> **注意：**

> 以下“新增功能”部分将 Citrix Gateway connector for Exchange ActiveSync 称为其旧名称 XenMobile Citrix ADC Connector。该名称自 8.5.2 版起已更改。

8.5.1.11 版中的新增功能

- **系统要求更改：** 当前版本的 Citrix ADC Connector 需要 Microsoft .NET Framework 4.5。
- **Google Analytics 支持：** 我们希望了解您如何使用 XenMobile Citrix ADC Connector，以便我们能够专注于改进产品。
- **支持 TLS 1.1 和 1.2：** 由于其安全性减弱，PCI Council 正在弃用 TLS 1.0。XenMobile Citrix ADC Connector 中增加了对 TLS 1.1 和 1.2 的支持。

监控 Citrix Gateway 连接器用于 Exchange ActiveSync

Citrix Gateway connector for Exchange ActiveSync 配置实用程序提供详细的日志记录，您可以使用它来查看通过 Exchange Server 的所有流量，这些流量由 Secure Mobile Gateway 允许或阻止。

使用**日志**选项卡可查看由 Citrix ADC 转发到 connector for Exchange ActiveSync 以进行授权的 ActiveSync 请求的历史记录。

此外，为确保 Citrix Gateway connector for the Exchange ActiveSync Web 服务正在运行，请在连接器服务器上的浏览器中加载以下 URL `https://<host:port>/services/ActiveSync/Version`。如果 URL 返回产品版本字符串，则表示 Web 服务响应正常。

使用 Citrix Gateway connector for Exchange ActiveSync 模拟 ActiveSync 流量

您可以使用 Citrix Gateway connector for Exchange ActiveSync 模拟 ActiveSync 流量在您的策略下的表现。在连接器配置实用程序中，选择**模拟器**选项卡。结果将显示您的策略如何根据您配置的规则应用。

为 Citrix Gateway connector for Exchange ActiveSync 选择筛选器

Citrix Gateway connector for Exchange ActiveSync 筛选器通过分析设备是否存在给定策略违规或属性设置来工作。如果设备符合条件，则将其放入设备列表中。此设备列表既不是允许列表也不是阻止列表。它是符合所定义条件的设备列表。XenMobile 中连接器提供了以下筛选器。每个筛选器的两个选项是“**允许**”或“**拒绝**”。

- **匿名设备**：允许或拒绝已在 XenMobile 中注册但用户身份不明的设备。例如，这可能是已注册但其 Active Directory 密码已过期，或者使用未知凭据注册的用户。
- **Samsung KNOX 证明失败**：Samsung 设备具有安全和诊断功能。此筛选器确认设备已设置为 KNOX。有关详细信息，请参阅 Samsung Knox。
- **禁用应用**：根据阻止列表策略定义的设备列表和阻止应用的出现情况，允许或拒绝设备。
- **隐式允许/拒绝**： 创建一个设备列表，其中包含所有不符合任何其他筛选规则条件的设备，并根据该列表进行允许或拒绝。隐式允许/拒绝选项可确保 Citrix Gateway connector for Exchange ActiveSync 在“设备”选项卡中的状态已启用，并显示设备的连接器状态。隐式允许/拒绝选项还控制所有其他未选择的连接器筛选器。例如，连接器会拒绝被阻止的应用，但会允许所有其他筛选器，因为隐式允许/拒绝选项设置为“**允许**”。
- **非活动设备**：创建在指定时间内未与 XenMobile 通信的设备列表。这些设备被视为非活动设备。筛选器会相应地允许或拒绝这些设备。
- **缺少所需应用**：用户注册时，会收到必须安装的所需应用列表。“缺少所需应用”筛选器指示一个或多个应用不再存在；例如，用户删除了一个或多个应用。
- **非建议应用**：用户注册时，会收到必须安装的应用列表。“非建议应用”筛选器检查设备中是否存在不在该列表中的应用。
- **不合规密码**：创建设备上没有密码的所有设备的设备列表。
- **不合规设备**：允许您拒绝或允许符合您内部 IT 合规性标准的设备。合规性是由名为“不合规”的设备属性定义的任意设置，它是一个布尔标志，可以是“**True**”或“**False**”。（您可以手动创建此属性并设置值，也可以使用“自动化操作”在设备符合或不符合特定条件时在该设备上创建此属性。）

  - **不合规 = True**。如果设备不符合 IT 部门设置的合规性标准和策略定义，则该设备不合规。
  - **不合规 = False**。如果设备符合 IT 部门设置的合规性标准和策略定义，则该设备合规。
- **已吊销状态**：创建所有已吊销设备的设备列表，并根据已吊销状态允许或拒绝。
- **已 Root 的 Android/已越狱的 iOS 设备**。创建所有标记为已 Root 的设备的设备列表，并根据已 Root 状态允许或拒绝。
- **非托管设备**。创建 XenMobile 数据库中所有设备的设备列表。移动应用网关必须以阻止模式部署。

配置与 Exchange ActiveSync 的 Citrix Gateway 连接器 的连接

Exchange ActiveSync 的 Citrix Gateway 连接器 通过安全的 Web 服务与 XenMobile 和其他远程配置提供程序通信。

1. 在连接器配置实用程序中，单击“**配置提供程序**”选项卡，然后单击“**添加**”。
2. 在“**配置提供程序**”对话框的“**名称**”中，输入具有管理权限并用于与 XenMobile Server 进行基本 HTTP 授权的用户名。
3. 在“**URL**”中，输入 XenMobile GCS 的 Web 地址，通常采用 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 格式。*MagConfigService* 名称区分大小写。
4. 在“**密码**”中，输入用于与 XenMobile Server 进行基本 HTTP 授权的密码。
5. 在“**管理主机**”中，输入连接器服务器名称。
6. 在“**基线间隔**”中，指定从 Device Manager 拉取新的刷新动态规则集的时间段。
7. 在“**增量间隔**”中，指定拉取动态规则更新的时间段。
8. 在“**请求超时**”中，指定服务器请求超时间隔。
9. 在“**配置提供程序**”中，选择配置提供程序服务器实例是否提供策略配置。
10. 在“**启用事件**”中，如果您希望连接器在设备被阻止时通知 XenMobile，请启用此选项。如果您在任何 XenMobile 自动化操作中使用连接器规则，则此选项是必需的。
11. 单击“**保存**”，然后单击“**测试连接**”以测试网关到配置提供程序的连接。如果连接失败，请检查本地防火墙设置是否允许连接，或联系您的管理员。
12. 连接成功后，清除“**禁用**”复选框，然后单击“**保存**”。

添加新的配置提供程序时，Exchange ActiveSync 的 Citrix Gateway 连接器 会自动创建与该提供程序关联的一个或多个策略。这些策略由 `config\policyTemplates.xml` 中 NewPolicyTemplate 部分包含的模板定义。对于此部分中定义的每个策略元素，都会创建一个新策略。

如果满足以下条件，操作员可以添加、删除或修改策略元素：策略元素符合架构定义，并且标准替换字符串（括在花括号中）未被修改。接下来，为提供程序添加新组，并更新策略以包含新组。

从 XenMobile 导入策略

1. 在适用于 Exchange ActiveSync 配置实用程序的 Citrix Gateway 连接器中，单击“**配置提供程序**”选项卡，然后单击“**添加**”。
2. 在“**配置提供程序**”对话框的“**名称**”中，输入用于与 XenMobile Server 进行基本 HTTP 授权且具有管理权限的用户名。
3. 在“**URL**”中，输入 XenMobile Gateway 配置服务 (GCS) 的网址，通常采用 `https://<xdmHost>/xdm/services/<MagConfigService>` 格式。MagConfigService 名称区分大小写。
4. 在“**密码**”中，输入用于与 XenMobile Server 进行基本 HTTP 授权的密码。
5. 单击“**测试连接**”以测试网关到配置提供程序的连接。如果连接失败，请检查本地防火墙设置是否允许连接，或咨询管理员。
6. 成功建立连接后，清除“**已禁用**”复选框，然后单击“**保存**”。
7. 在“**管理主机**”中，保留本地主机的默认 DNS 名称。当多个 Forefront Threat Management Gateway (TMG) 服务器配置为阵列时，此设置用于协调与 XenMobile 的通信。

   保存设置后，打开 GCS。

配置适用于 Exchange ActiveSync 策略模式的 Citrix Gateway 连接器

适用于 Exchange ActiveSync 的 Citrix Gateway 连接器可以以下列六种模式运行：

- **全部允许**。此策略模式授予通过连接器的所有流量访问权限。不使用其他筛选规则。
- **全部拒绝**。此策略模式阻止通过连接器的所有流量访问。不使用其他筛选规则。
- **静态规则: 阻止模式**。此策略模式运行静态规则，并在末尾带有一个隐式拒绝或阻止语句。连接器会阻止通过其他筛选规则不允许或未获准的设备。
- **静态规则：允许模式**。此策略模式运行静态规则，并在末尾包含隐式允许或放行语句。未通过其他筛选规则阻止或拒绝的设备将通过连接器。
- **静态 + ZDM 规则**：阻止模式。此策略模式首先运行静态规则，然后运行来自 XenMobile 的动态规则，并在末尾包含隐式拒绝或阻止语句。设备根据定义的筛选器和设备管理器规则允许或拒绝。任何不符合定义的筛选器和规则的设备都将被阻止。

- **静态 + ZDM 规则**：允许模式。此策略模式首先运行静态规则，然后运行来自 XenMobile 的动态规则，并在末尾包含隐式允许或放行语句。设备根据定义的筛选器和 XenMobile 规则允许或拒绝。任何不符合定义的筛选器和规则的设备都将被允许。

Citrix Gateway connector for Exchange ActiveSync 进程根据从 XenMobile 接收的 iOS 和基于 Windows 的移动设备的唯一 ActiveSync ID 允许或阻止动态规则。Android 设备的行为因制造商而异，有些设备不会轻易公开唯一的 ActiveSync ID。为了弥补这一点，XenMobile 会发送 Android 设备的用户 ID 信息以做出允许或阻止的决定。因此，如果用户只有一个 Android 设备，则允许和阻止功能正常。如果用户有多个 Android 设备，则所有设备都将被允许，因为 Android 设备无法区分。如果已知这些设备的 ActiveSyncID，您可以将网关配置为通过 ActiveSyncID 静态阻止这些设备。您还可以根据设备类型或用户代理配置网关以进行阻止。

要在 SMG 控制器配置实用程序中指定策略模式，请执行以下操作：

1. 单击“**路径筛选器**”选项卡，然后单击“**添加**”。
2. 在“**路径属性**”对话框中，从“**策略**”列表中选择一个策略模式，然后单击“**保存**”。

您可以在配置实用程序的“**策略**”选项卡上查看规则。规则在 Citrix Gateway connector for Exchange ActiveSync 上从上到下处理。允许策略显示为绿色复选标记。拒绝策略显示为带斜线的红色圆圈。要刷新屏幕并查看最新规则，请单击“**刷新**”。您还可以修改 config.xml 文件中规则的顺序。

要测试规则，请单击“**模拟器**”选项卡。在字段中指定值。这些值也可以从日志中获取。将显示一条结果消息，指定“允许”或“阻止”。

配置静态规则

输入静态规则，其值由 ActiveSync 连接 HTTP 请求的 ISAPI 筛选读取。静态规则使 Citrix Gateway connector for Exchange ActiveSync 能够根据以下条件允许或阻止流量：

- **用户**： Citrix Gateway connector for Exchange ActiveSync 使用在设备注册期间捕获的授权用户值和名称结构。这通常以 domain\username 的形式出现，由通过 LDAP 连接到 Active Directory 的运行 XenMobile 的服务器引用。连接器配置实用程序中的“**日志**”选项卡显示通过连接器的值。如果必须确定值结构或值结构不同，则会传递这些值。
- **设备 ID (ActiveSyncID)**： 也称为连接设备的 ActiveSyncID。此值通常在 XenMobile 控制台中的特定设备属性页面中找到。此值也可以从连接器配置实用程序中的“日志”选项卡中筛选出来。
- **设备类型**： 连接器可以确定设备是 iPhone、iPad 还是其他设备类型，并可以根据该条件允许或阻止。与其他值一样，连接器配置实用程序可以显示正在为 ActiveSync 连接处理的所有连接设备类型。
- **用户代理**： 包含有关所用 ActiveSync 客户端的信息。通常，指定的值对应于移动设备平台的特定操作系统版本和内部版本。

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 控制器配置实用程序中，单击**静态规则**选项卡，然后单击**添加**。
2. 在**静态规则属性**对话框中，指定要用作条件的数值。例如，您可以通过输入用户名（例如 AllowedUser）来添加用户以允许访问，然后清除**禁用**复选框。
3. 单击**保存**。

   静态规则现已生效。此外，您可以使用正则表达式定义值，但必须在 config.xml 文件中启用规则处理模式。

配置动态规则

XenMobile 中的设备策略和属性定义动态规则，并且可以触发 Exchange ActiveSync 筛选器的动态 Citrix Gateway 连接器。触发器基于是否存在策略违规或属性设置。连接器筛选器通过分析设备是否存在给定策略违规或属性设置来工作。如果设备符合条件，则该设备将放置在设备列表中。此设备列表不是允许列表或阻止列表。它是符合所定义条件的设备列表。以下配置选项使您能够定义是否要使用连接器允许或拒绝设备列表中的设备。

> **注意：**
>
> 您必须使用 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，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. 仅限 Android，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。

   启用此选项后，当 XenMobile 没有 Android 设备用户的 ActiveSync 标识符时，XenMobile 会将 Android 设备信息发送到 Exchange ActiveSync 的 Citrix Gateway 连接器。

通过编辑 Exchange ActiveSync XML 文件的 Citrix Gateway 连接器来配置自定义策略

您可以在 Citrix Gateway connector for Exchange ActiveSync 配置实用程序的“**策略**”选项卡上查看默认配置中的基本策略。如果要创建自定义策略，可以编辑连接器 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），请将新的 **Group** 元素添加到 **GroupList** 部分。
3. （可选）您可以通过重新排列 **GroupRef** 元素来更改现有策略中组的顺序。

配置 Citrix Gateway 连接器 适用于 Exchange ActiveSync 的 XML文件

Citrix Gateway connector for Exchange ActiveSync 使用 XML 配置文件来决定连接器的操作。除其他条目外，该文件还指定了组文件以及筛选器在评估 HTTP 请求时采取的相关操作。默认情况下，该文件名为 config.xml，位于以下位置：..\Program Files\Citrix\XenMobile 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 节点中出现的顺序很重要。

> GroupRef 节点的 ID 值标识一个逻辑容器或成员集合，用于匹配特定的用户帐户或设备。操作属性指定筛选器如何处理集合中与规则匹配的成员。例如，与 AllowGroup 集中规则匹配的用户帐户或设备将“通过”。通过意味着允许访问 Exchange CAS。与 DenyGroup 集中规则匹配的用户帐户或设备将“被拒绝”。被拒绝意味着不允许访问 Exchange CAS。

当特定用户帐户/设备或组合同时满足两个组中的规则时，将使用优先级约定来决定请求的结果。优先级体现在 config.xml 文件中 GroupRef 节点从上到下的顺序。GroupRef 节点按优先级顺序排列。Allow 组中针对给定条件的规则将始终优先于 Deny 组中针对相同条件的规则。

Group 节点

此外，config.xml 定义了 Group 节点。这些节点将逻辑容器 AllowGroup 和 DenyGroup 链接到外部 XML 文件。存储在外部文件中的条目构成了筛选器规则的基础。

> **注意：**

> 在此版本中，仅支持外部 XML 文件。

> 默认安装在配置中实现两个 XML 文件：allow.xml 和 deny.xml。

配置 Citrix Gateway 连接器 用于 Exchange ActiveSync

您可以配置 Citrix Gateway connector for Exchange ActiveSync，以根据以下属性选择性地阻止或允许 ActiveSync 请求：**Active Sync 服务 ID**、**设备类型**、**用户代理**（设备操作系统）、**授权用户**和 **ActiveSync 命令**。

默认配置支持静态组和动态组的组合。您可以使用 SMG 控制器配置实用程序维护静态组。静态组可能包含已知类别的设备，例如使用给定用户代理的所有设备。

名为“网关配置提供程序”的外部源维护动态组。Citrix Gateway connector for Exchange ActiveSync 定期连接这些组。XenMobile 可以将允许和阻止的设备和用户组导出到连接器。

动态组由名为“网关配置提供程序”的外部源维护，并由 Citrix Gateway connector for Exchange ActiveSync 定期收集。XenMobile 可以将允许和阻止的设备和用户组导出到连接器。

策略是组的有序列表，其中每个组都有一个关联的操作（允许或阻止）和一个组成员列表。一个策略可以有任意数量的组。策略中的组排序很重要，因为当找到匹配项时，将执行该组的操作，并且不会评估后续组。

成员定义了匹配请求属性的方式。它可以匹配单个属性（例如设备 ID），也可以匹配多个属性（例如设备类型和用户代理）。

为 Citrix Gateway connector for Exchange ActiveSync 选择安全模型

建立安全模型对于任何规模的组织成功部署移动设备都至关重要。通常，默认情况下使用受保护或隔离的网络控制来允许用户、计算机或设备访问。这种做法并非总是理想的。每个管理 IT 安全的组织都可能对移动设备的安全采取略有不同或量身定制的方法。

同样的逻辑也适用于移动设备安全。由于移动设备和类型众多、每个用户的移动设备数量以及可用的操作系统平台和应用程序，使用宽松模型是一个糟糕的选择。在大多数组织中，限制性模型是最合乎逻辑的选择。

Citrix 允许将 Citrix Gateway connector for Exchange ActiveSync 与 XenMobile 集成的配置方案如下：

宽松模型（允许模式）

宽松安全模型基于以下前提运行：默认情况下，所有内容都允许或授予访问权限。只有通过规则和筛选，才能阻止某些内容并应用限制。宽松安全模型适用于对移动设备安全关注度相对较低的组织。该模型仅在适当情况下（当策略规则失败时）应用限制性控制来拒绝访问。

限制性模型 (阻止模式)

限制性安全模型基于默认情况下不允许或不授予任何访问权限的前提。所有通过安全检查点的流量都会被过滤和检查，除非通过允许访问的规则，否则将被拒绝访问。限制性安全模型适用于对移动设备有相对严格安全标准的企业。此模式仅在所有允许访问的规则都已通过时，才授予对网络服务的使用和功能访问权限。

管理适用于 Exchange ActiveSync 的 Citrix Gateway 连接器

您可以使用适用于 Exchange ActiveSync 的 Citrix Gateway 连接器来构建访问控制规则。这些规则可以允许或阻止来自托管设备的 ActiveSync 连接请求。访问权限基于设备状态、应用程序允许或阻止列表以及其他合规性条件。

通过使用适用于 Exchange ActiveSync 配置实用程序的 Citrix Gateway 连接器，您可以构建动态和静态规则，以强制执行企业电子邮件策略，从而阻止违反合规性标准的用户。您还可以设置电子邮件附件加密，以便所有通过 Exchange Server 传输到托管设备的附件都经过加密，并且只能由授权用户在托管设备上查看。

卸载适用于 Exchange ActiveSync 的 Citrix Gateway 连接器

1. 以管理员帐户运行 XncInstaller.exe。
2. 按照屏幕上的说明完成卸载。

安装、升级或卸载适用于 Exchange ActiveSync 的 Citrix Gateway 连接器

1. 以管理员帐户运行 XncInstaller.exe 以安装连接器，或允许升级或删除现有连接器。
2. 按照屏幕上的说明完成安装、升级或卸载。

安装连接器后，您必须手动重新启动 XenMobile 配置服务和通知服务。

安装适用于 Exchange ActiveSync 的 Citrix Gateway 连接器

您将适用于 Exchange ActiveSync 的 Citrix Gateway 连接器安装在其自己的 Windows Server 上。

连接器对服务器造成的 CPU 负载取决于所管理的设备数量。对于大量设备（超过 50,000 台），如果您没有群集环境，可能需要配置多个核心。连接器的内存占用量不足以需要更多内存。

Citrix Gateway 连接器 for Exchange ActiveSync 系统要求

Citrix Gateway 连接器 for Exchange ActiveSync 通过在 Citrix ADC 设备上配置的 SSL 网桥与 Citrix ADC 进行通信。该网桥使设备能够将所有安全流量直接桥接到 XenMobile。此连接器需要以下最低系统配置：

组件	要求
计算机和处理器	733 MHz Pentium III 733 MHz 或更高处理器。2.0 GHz Pentium III 或更高处理器（推荐）
思杰 ADC	Citrix ADC 设备，软件版本 10
内存	1 GB
硬盘	NTFS 格式的本地分区，具有 150 MB 可用硬盘空间
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 January 14, 2020 结束，对 Windows Server 2012 R2 的支持将于 October 10, 2023 结束。
其他设备	与主机操作系统兼容的网络适配器，用于与内部网络通信
微软 .NET 框架	版本 8.5.1.11 需要 Microsoft .NET Framework 4.5。
显示器	VGA 或更高分辨率的显示器

Citrix Gateway connector for Exchange ActiveSync 的主机计算机需要以下最低可用硬盘空间：

- **应用程序：** 10–15 MB（建议 100 MB）
- **日志记录：** 1 GB（建议 20 GB）

有关 Citrix Gateway connector for Exchange ActiveSync 的平台支持信息，请参阅支持的设备操作系统。

设备电子邮件客户端

并非所有电子邮件客户端都始终为设备返回相同的 ActiveSync ID。由于 Citrix Gateway connector for Exchange ActiveSync 要求每个设备具有唯一的 ActiveSync ID，因此以下情况属实：仅支持始终为每个设备生成相同且唯一 ActiveSync ID 的电子邮件客户端。Citrix 已测试过这些电子邮件客户端，并且这些客户端运行无误：

- 三星原生电子邮件客户端
- iOS 原生电子邮件客户端

部署思杰网关 Exchange ActiveSync 连接器

Citrix Gateway connector for Exchange ActiveSync 使您能够使用 Citrix ADC 代理和负载平衡 XenMobile Server 与 XenMobile 托管设备之间的通信。连接器定期与 XenMobile 通信以同步策略。连接器和 XenMobile 可以集群在一起或独立集群，并且可以通过 Citrix ADC 进行负载平衡。

Citrix Gateway 连接器 for Exchange ActiveSync 组件

- **Citrix Gateway connector for Exchange ActiveSync 服务：**此服务提供一个 REST Web 服务接口，Citrix ADC 可调用该接口来确定来自设备的 ActiveSync 请求是否已获得授权。
- **XenMobile 配置服务：**此服务与 XenMobile 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。通过这种方式，XenMobile 可以采取适当的措施，例如通知用户设备被阻止的原因。
- **Citrix Gateway connector for Exchange ActiveSync 配置实用程序：**此应用程序允许管理员配置和监视连接器。

为 Citrix Gateway connector for Exchange ActiveSync 设置侦听地址

要使 Citrix Gateway connector for Exchange ActiveSync 接收来自 Citrix ADC 的请求以授权 ActiveSync 流量，请执行以下操作。指定连接器侦听 Citrix ADC Web 服务调用的端口。

1. 从“**开始**”菜单中，选择 Citrix Gateway connector for Exchange ActiveSync 配置实用程序。
2. 单击“**Web 服务**”选项卡，然后键入连接器 Web 服务的侦听地址。您可以选择 **HTTP** 或 **HTTPS**，或两者都选。如果连接器与 XenMobile 共同驻留（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“**保存**”，然后单击“**启动服务**”以启动 Web 服务。

在 Citrix Gateway connector for Exchange ActiveSync 中配置设备访问控制策略

要配置要应用于托管设备的访问控制策略，请执行以下操作：

1. 在 Citrix Gateway connector for Exchange ActiveSync 配置实用程序中，单击“**路径筛选器**”选项卡。
2. 选择第一行“**Microsoft-Server-ActiveSync 用于 ActiveSync**”，然后单击“**编辑**”。
3. 从“**策略**”列表中，选择所需的策略。对于包含 XenMobile 策略的策略，请选择“**静态 + ZDM: 允许模式或静态 + ZDM: 阻止模式**”。这些策略将本地（或静态）规则与 XenMobile 中的规则结合起来。允许模式表示所有未由规则明确标识的设备都允许访问 ActiveSync。阻止模式表示此类设备将被阻止。
4. 设置策略后，单击“**保存**”。

配置与 XenMobile 的通信

指定要与 Citrix Gateway connector for Exchange ActiveSync 和 Citrix ADC 配合使用的 XenMobile Server（也称为配置提供程序）的名称和属性。

> **注意：**
>
> 此任务假定您已安装并配置 XenMobile。

1. 在 Citrix Gateway connector for Exchange ActiveSync 配置实用程序中，单击“**配置提供程序**”选项卡，然后单击“**添加**”。
2. 输入在此部署中使用的 XenMobile Server 的名称和 URL。如果您的多租户部署中部署了多个 XenMobile Server，则此名称对于每个服务器实例必须是唯一的。例如，对于“**名称**”，可以键入 **XMS**。
3. 在“**URL**”中，输入 XenMobile GlobalConfig Provider (GCP) 的 Web 地址，通常采用 `https://<FQDN>/<instanceName>/services/<MagConfigService>` 格式。*MagConfigService* 名称区分大小写。
4. 在“**密码**”中，输入用于与 XenMobile Web 服务器进行基本 HTTP 授权的密码。
5. 在“**管理主机**”中，输入安装 Citrix Gateway connector for Exchange ActiveSync 的服务器名称。
6. 在“**基线间隔**”中，指定从 XenMobile 拉取新刷新动态规则集的时间段。
7. 在“**请求超时**”中，指定服务器请求超时间隔。

8. 在“**配置提供程序**”中，选择配置提供程序服务器实例是否提供策略配置。
9. 在“**启用事件**”中，如果您希望 Secure Mobile Gateway 在设备被阻止时通知 XenMobile，请启用此选项。如果您在任何 Device Manager 自动化操作中使用 Secure Mobile Gateway 规则，则此选项是必需的。
10. 配置服务器后，单击“**测试连接**”以测试与 XenMobile 的连接。
11. 当连接建立后，点击 **保存**。

部署 Citrix Gateway connector for Exchange ActiveSync 以实现冗余和可伸缩性

如果您希望扩展您的 Citrix Gateway connector for Exchange ActiveSync 和 XenMobile 部署，可以在多台 Windows 服务器上安装连接器实例，所有实例都指向同一个 XenMobile 实例，然后您可以使用 Citrix ADC 对这些服务器进行负载均衡。

Citrix Gateway connector for Exchange ActiveSync 配置有两种模式：

- 在非共享模式下，每个 Citrix Gateway connector for Exchange ActiveSync 实例都与一个 XenMobile Server 通信，并保留其自己的策略私有副本。例如，如果您有一个 XenMobile Server 集群，则可以在每个 XenMobile Server 上运行一个连接器实例，并且该连接器将从本地 XenMobile 实例获取策略。
- 在共享模式下，一个连接器节点被选为主节点，并与 XenMobile 通信。生成的配置通过 Windows 网络共享或 Windows（或第三方）复制在其他节点之间共享。

整个连接器配置位于一个文件夹中（包含几个 XML 文件）。连接器进程会检测此文件夹中任何文件的更改并自动重新加载配置。在共享模式下，主节点没有故障转移。但是，系统可以容忍主服务器停机几分钟（例如，为了重新启动），因为上次已知的良好配置已缓存在连接器进程中。

高级概念

> **注意：**
>
> 本文涵盖 XenMobile Server 的高级概念。有关 Citrix Endpoint Management 的高级信息，请参阅 高级概念。
>
> XenMobile® 高级概念文章深入探讨了 XenMobile 的产品文档。其目的是通过专家技术帮助缩短部署时间。这些文章可能会引用撰写内容的专家。

有关端到端 XenMobile 环境的决策点、建议、常见问题和用例，请参阅本节中的 XenMobile 部署手册。

有关 XenMobile 的社区支持论坛，请参阅 Citrix Discussions。

本地部署的 XenMobile® 与 Active Directory 的交互

本文解释了 XenMobile Server 与 Active Directory 之间的交互。XenMobile Server 以内联和后台两种方式与 Active Directory 交互。以下部分提供了有关涉及 Active Directory 交互的内联操作和后台操作的更多信息。

> **注意：**
>
> 本文概述了交互，但未涵盖详细信息。有关在 XenMobile 控制台中配置 Active Directory 和 LDAP 的更多信息，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 设置与 Active Directory 通信。这些设置检索有关用户和组的信息。以下是导致 XenMobile Server 与 Active Directory 之间交互的操作。

1. **LDAP 配置。** Active Directory 本身的配置会导致与 Active Directory 的交互。XenMobile Server 尝试通过使用 Active Directory 验证信息来验证信息。服务器通过使用提供的互联网协议、端口和服务帐户凭据来执行此操作。成功的绑定表示连接已正确配置。
2. **基于组的交互。**

   a. 在基于角色的访问控制 (RBAC) 和交付组定义创建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 在选定的域中搜索所有包含所提供子字符串的组。然后，XenMobile Server 检索在搜索中识别的组的 objectGUID、sAMAccountName 和 Distinguished Name 属性。

   > **注意：**
   >
   > 此信息未存储在 XenMobile Server 数据库中。

   b. RBAC 和部署组定义的添加或更新。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 中逐个搜索特定组。XenMobile Server 搜索 objectGUID 属性并检索选定的属性，包括成员资格信息。组的成员资格信息有助于确定检索到的组与 XenMobile Server 数据库中现有用户或组之间的成员资格。组的成员资格更改会导致受影响用户成员的 RBAC 和部署组派生，从而产生用户权限。

   > **注意：**
   >
   > 部署组定义的更改可能导致受影响用户的应用程序或策略权限发生更改。

   c. **一次性 PIN (OTP) 邀请。** XenMobile Server 管理员从 XenMobile Server 数据库中存在的 Active Directory 组列表中选择一个组。对于此组，所有直接和间接用户都将从 Active Directory 中检索。OTP 邀请将发送给在上一步中识别的用户。

   > **注意：**
   >
   > 前面三种交互意味着基于组的交互是根据 XenMobile Server 配置更改触发的。当配置没有更改时，这些交互意味着没有与 Active Directory 的交互。它们还意味着不需要后台作业定期捕获组方面的更改。

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 的两次交互：

      - 用于使用提供的凭据对用户进行身份验证。
      - 将选定的用户属性（包括 objectGUID、Distinguished Name、sAMAccountName 和组的直接成员身份）添加或更新到 XenMobile Server 数据库。组员身份的更改会导致重新评估应用程序、策略和访问权限。

      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：**商店刷新会导致用户属性（包括直接组成员身份）的刷新。此操作允许重新评估用户权限。

   c. **设备签入：**管理员可以在 XenMobile 控制台中配置定期设备签入。每次设备签入时，都会刷新相应的用户属性，包括直接组成员身份。这些签入允许重新评估用户权限。

   d. **按组发送 OTP 邀请：**XenMobile Server 管理员从 XenMobile Server 数据库中存在的 Active Directory 组列表中选择一个组。直接和间接（由于嵌套）的用户成员将从 Active Directory 中检索并保存到 XenMobile Server 数据库中。OTP 邀请将发送给上一步中确定的用户成员。

   e. **按用户发送 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 并返回与输入文本字符串匹配的用户记录。然后管理员选择要发送 OTP 邀请的用户。XenMobile Server 从 Active Directory 中检索用户详细信息，并在向用户发送邀请之前更新数据库中的相同详细信息。

后台交互

与 Active Directory 的内联通信得出的一个结论是，基于组的交互是在 XenMobile Server 配置发生选定更改时触发的。当配置没有更改时，这意味着没有与 Active Directory 的组交互。

此交互需要后台作业，这些作业会定期与 Active Directory 同步，并更新相关更改到相关组。

以下是与 Active Directory 交互的后台作业。

1. **组同步作业**。此作业的目的是一次查询一个 Active Directory 中相关组，以查找 distinguished name 或 sAMAccountName 属性的更改。对 Active Directory 的搜索查询使用相关组的 objectGUID，以获取 distinguished name 和 sAMAccountName 属性的当前值。相关组的 distinguished name 或 sAMAccountName 值的更改将更新到数据库中。

   > **注意：**

> 此作业不更新用户到组的成员身份信息。

2. **嵌套组同步作业**。此作业更新相关组的嵌套层次结构中的更改。XenMobile Server 允许相关组的直接和间接成员获取授权。用户的直接成员身份在基于用户的内联交互期间更新。此作业在后台运行，跟踪间接成员身份。间接成员身份是指用户是一个组的成员，而该组又是相关组的成员。

   此作业从 XenMobile Server 数据库中收集 Active Directory 组列表。这些组是部署组或 RBAC 定义的一部分。对于此列表中的每个组，XenMobile Server 获取该组的成员。组的成员是表示用户和组的 distinguished name 列表。

   XenMobile Server 再次查询 Active Directory，以仅获取相关组的用户成员。这两个列表之间的差异仅提供相关组的组成员。成员组中的更改将更新到数据库中。对层次结构中的所有组重复相同的过程。

   嵌套的更改导致处理受影响用户的授权更改。

3. **禁用用户检查**。此作业仅在 XenMobile 管理员创建检查禁用用户的操作时运行。此作业在组同步作业的范围内运行。此作业查询 Active Directory，一次检查一个相关用户的禁用状态。

常见问题

默认情况下，后台作业的运行频率是多少？

- 组同步作业从当地时间 02:00 开始，每五小时运行一次。
- 嵌套组同步作业每天在当地时间午夜运行一次。

为什么需要组同步作业？

- Active Directory 中用户记录的 **memberOf** 属性提供了用户是其直接成员的组列表。如果组从一个 OU 移动到另一个 OU，**memberOf** 属性会反映 distinguished name 的最新值。XenMobile Server 数据库也具有上次刷新的值。组的 distinguished name 中的任何不匹配都可能导致用户失去对部署组的访问权限。用户还可能失去与该部署组关联的应用程序和策略。
- 后台作业使 XenMobile Server 数据库中的组 distinguished name 属性保持最新，以确保用户可以访问其授权。
- 同步作业每五小时调度一次，因为假定 Active Directory 中的组更改不常见。

可以关闭组同步作业吗？

- 如果您知道相关组不会从一个 OU 更改到另一个 OU，则可以关闭作业。

为什么需要嵌套组处理后台作业？

- Active Directory 中组的嵌套更改并非每天都会发生。相关组的嵌套层次结构更改会导致受影响用户的权限发生更改。当一个组被添加到层次结构中时，其成员用户将获得相应的角色权限。当一个组移出嵌套时，该组的成员用户可能会失去对基于角色的权限的访问。
- 用户刷新期间不会捕获嵌套更改。由于嵌套更改无法按需进行，因此通过后台作业捕获这些更改。
- 嵌套更改被认为不常见，因此后台作业每天运行一次以检查任何更改。

可以关闭嵌套组处理作业吗？

- 如果您知道相关组不会发生嵌套更改，则可以关闭作业。

XenMobile® 部署

规划 XenMobile 部署时，需要考虑很多因素：

- 选择哪些设备？
- 如何管理设备？
- 如何在确保网络安全的同时，仍提供出色的用户体验？
- 您需要哪些硬件以及如何对其进行故障排除？

本节中的文章旨在帮助回答此类问题。其中包含涵盖您部署关注点的用例和建议。

请记住，指南或建议可能不适用于所有环境或用例。在正式部署 XenMobile 之前，请务必设置测试环境。

本节中的文章涵盖以下领域：

- **评估：** 规划部署时要考虑的常见用例和问题。
- **设计与配置：** 有关设计和配置环境的建议
- **操作与监控：** 确保运行环境的平稳运行。

评估

与任何部署一样，评估您的需求是重中之重。您对 XenMobile 的主要需求是什么？您需要管理环境中的所有设备还是仅管理应用程序？也许您需要同时管理两者。您的 XenMobile 环境需要多安全？让我们来看看规划部署时需要考虑的常见用例和问题。

- 管理模式
- 设备要求
- 安全性和用户体验

- 应用程序
- 用户社区
- 电子邮件策略
- XenMobile 集成
- 多站点要求

设计和配置

完成部署需求评估后，即可确定环境的设计和配置。您需要规划以下几点：

- 选择服务器硬件
- 为应用程序和设备设置策略
- 让用户注册

本节包含针对这些场景及更多场景的用例和建议。

- 与 Citrix ADC 和 Citrix Gateway 集成
- MDX 应用程序的 SSO 和代理注意事项
- 身份验证
- 本地部署的参考架构
- 服务器属性
- 设备和应用程序策略
- 用户注册选项
- 优化 XenMobile 操作

操作和监控

XenMobile 环境启动并运行后，您需要对其进行监控以确保平稳运行。监控部分讨论以下内容：

- 在哪里可以找到 XenMobile 及其组件生成的各种日志和消息
- 如何读取这些日志

本节还包括您可以遵循的各种常见故障排除步骤，以减少客户支持反馈时间。

- 应用程序预配和取消预配
- 基于控制面板的操作
- 基于角色的访问控制和 XenMobile 支持

- 系统监控
- 灾难恢复
- Citrix 支持流程

管理模式

对于每个 XenMobile® 实例（单个服务器或节点群集），您可以选择管理设备、应用程序或两者。XenMobile 使用以下术语来表示设备和应用程序管理模式：

- 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)

> **重要提示：**

> 如果您配置了 MDM 模式，然后更改为 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。

> 借助 MDM，您可以配置、保护和支持移动设备。MDM 使您能够在系统级别保护设备和设备上的数据。您可以配置策略、操作和安全功能。例如，如果设备丢失、被盗或不合规，您可以选择性地擦除设备。尽管 MDM 模式下不提供应用程序管理，但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。以下是 MDM 模式的常见用例：

- 对于需要设备级管理策略或限制（例如完全擦除、选择性擦除或地理位置）的企业自有设备，MDM 是一个考虑因素。
- 当客户需要管理实际设备，但不需要 MDX 策略（例如应用程序容器化、应用程序数据共享控制或微型 VPN）时。
- 当用户只需要将电子邮件传送到其移动设备上的本机电子邮件客户端，并且 Exchange ActiveSync 或客户端访问服务器已可从外部访问时。在此用例中，您可以使用 MDM 配置电子邮件传送。
- 当您部署本机企业应用程序（非 MDX）、公共应用商店应用程序或从公共商店交付的 MDX 应用程序时。请注意，仅 MDM 解决方案可能无法阻止设备上应用程序之间机密信息的数据泄露。数据泄露可能发生在 Office 365 应用程序中的复制粘贴或“另存为”操作中。

移动应用程序管理 (MAM 模式)

MAM 保护应用程序数据并允许您控制应用程序数据共享。MAM 还允许独立于个人数据管理公司数据和资源。通过为 MAM 模式配置的 XenMobile，您可以使用支持 MDX 的移动应用程序提供每个应用程序的容器化和控制。术语 MAM 模式也称为纯 MAM 模式。此术语将此模式与旧版 MAM 模式区分开来。

通过使用 MDX 策略，XenMobile 可提供对网络访问（例如微 VPN）、应用程序和设备交互、数据加密以及应用程序访问的应用程序级控制。

MAM 通常适用于自带设备 (BYO)，因为尽管设备不受管理，但公司数据仍受到保护。MDX 具有许多仅限 MAM 的策略，这些策略不需要 MDM 控制。

MAM 还支持移动生产力应用程序。此支持包括向 Citrix Secure Mail 安全交付电子邮件、安全移动生产力应用程序之间的数据共享以及在 Citrix Files 中安全存储数据。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：

- 您交付移动应用程序，例如在应用程序级别管理的 MDX 应用程序。
- 您不需要在系统级别管理设备。

MDM+MAM（企业模式）

MDM+MAM 是一种混合模式，也称为企业模式，它支持 XenMobile 企业移动性管理 (EMM) 解决方案中所有可用的功能集。使用 MDM+MAM 模式配置 XenMobile 可同时启用 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，或者您是否需要设备管理。这种灵活性对于包含混合用例的环境非常有用。这些环境可能需要或可能不需要通过 MDM 策略管理设备才能访问您的 MAM 资源。

MDM+MAM 适用于以下示例：

- 您有一个同时需要 MDM 和 MAM 的单一用例。访问您的 MAM 资源需要 MDM。
- 某些用例需要 MDM，而另一些则不需要。
- 某些用例需要 MAM，而另一些则不需要。

您通过 **服务器模式** 属性指定 XenMobile Server 的管理模式。您在 XenMobile 控制台中配置此设置。模式可以是 MDM、MAM 或 ENT（用于 MDM+MAM）。

您拥有许可证的 XenMobile 版本决定了可用的管理模式和其他功能，如下表所示。

XenMobile MDM 版本	**XenMobile Advanced 版本**
MDM 功能	MDM 功能
-	MAM 功能
-	MAM SDK
安全中心	安全中心
-	安全邮件
-	安全 Web

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。您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，MDM+MAM 服务器模式可用的注册选项与 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 环境可以包含多种用例，其中一些用例需要通过 MDM 策略进行设备管理，以允许访问 MAM 资源。在向用户部署移动生产力应用程序之前，请充分评估您的用例并决定是否需要 MDM 注册。如果您以后决定更改 MDM 注册要求，则用户可能必须重新注册其设备。

> **注意：**
>
> 要指定是否要求用户注册 MDM，请在 XenMobile 控制台（**设置 > 服务器属性**）中使用 XenMobile Server 属性 **Enrollment Required**。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。

> 以下是 XenMobile Enterprise 模式部署中要求 MDM 注册的优点和缺点（以及缓解措施）的摘要。

当 MDM 注册是可选的

优点：

- 用户可以访问 MAM 资源，而无需将其设备置于 MDM 管理之下。此选项可以提高用户采用率。

- 能够安全访问 MAM 资源以保护企业数据。
- MDX 策略（例如 **App Passcode**）可以控制每个 MDX 应用程序的应用程序访问。
- 配置 Citrix ADC、XenMobile Server 和每个应用程序的超时，以及 Citrix PIN，可提供额外的保护层。
- 虽然 MDM 操作不适用于设备，但某些 MDX 策略可用于拒绝 MAM 访问。拒绝将基于系统设置，例如越狱或已 root 的设备。
- 用户可以在首次使用时选择是否将其设备注册到 MDM。

缺点：

- MAM 资源可用于未注册 MDM 的设备。
- MDM 策略和操作仅适用于已注册 MDM 的设备。

缓解选项：

- 让用户同意公司条款和条件，如果他们选择不合规，则需承担责任。让管理员监控未受管设备。
- 通过使用应用程序计时器管理应用程序访问和安全性。缩短超时值可提高安全性，但可能会影响用户体验。
- 另一个需要 MDM 注册的 XenMobile 环境是一个选项。在考虑此选项时，请记住管理两个环境的额外开销以及所需的额外资源。

需要 MDM 注册时

优点：

- 能够将 MAM 资源的访问权限仅限于 MDM 管理的设备。
- MDM 策略和操作可以根据需要应用于环境中的所有设备。
- 用户无法选择不注册其设备。

缺点：

- 要求所有用户注册 MDM。
- 可能会降低那些反对公司管理其个人设备的用户的使用率。

缓解选项：

- 教育用户了解 XenMobile 实际在其设备上管理的内容以及管理员可以访问的信息。
- 您可以使用第二个 XenMobile 环境，其服务器模式为 MAM（也称为仅 MAM 模式），用于不需要 MDM 管理的设备。在考虑此选项时，请记住管理两个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 引入了一种新的仅 MAM 服务器模式。为了区分以前和新的 MAM 模式，文档使用这些术语。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 模式下注册。

当 XenMobile 的 **服务器模式** 属性为 ENT 且用户选择退出设备管理时，旧版 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 管理的用户会收到旧版 MAM 功能。

下表总结了针对特定许可证类型和所需设备模式要使用的 **服务器模式** 设置：

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
企业版/高级版/MDM	MDM 模式	MDM
企业版/高级版	MAM 模式（也称为仅 MAM 模式）	MAM
企业版/高级版	MDM+MAM 模式	ENT（选择退出设备管理的用户在旧版 MAM 模式下运行。）

仅 MAM 模式支持以前仅适用于 ENT 的以下功能。

- **基于证书的身份验证：** 仅 MAM 模式支持基于证书的身份验证。即使用户的 Active Directory 密码过期，他们也能持续访问其应用程序。如果您对 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 Settings > Citrix Gateway** 中，“Deliver the user certificate for authentication”设置为 **Off**，这意味着使用用户名和密码身份验证。将该设置更改为 **On** 以启用证书身份验证。
- **自助服务门户：** 允许用户自行执行应用程序锁定和应用程序擦除。这些操作适用于设备上的所有应用程序。您可以在 **Configure > Actions** 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：** 包括通过 **Manage > Enrollment Invitations** 配置的“高安全性”、“邀请 URL”和“双重身份验证”。
- **Android 和 iOS 设备的设备注册限制：** 服务器属性 **Number of Devices Per User** 已移至 **Configure > Enrollment Profiles**，现在适用于所有服务器模式。
- **仅 MAM API：** 对于仅 MAM 设备，您可以使用任何 REST 客户端和 XenMobile REST API 调用 REST 服务，以调用 XenMobile 控制台公开的服务。
- 仅 MAM API 使您能够：
  - 发送邀请 URL 和一次性 PIN。
  - 在设备上执行应用程序锁定和擦除。

下表总结了旧版 MAM 和仅 MAM 功能之间的差异。

注册方案和其他功能	**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	不支持。	支持。对于证书身份验证，需要 Citrix Gateway。
部署要求	XenMobile Server 无需从设备直接访问。	XenMobile Server 无需从设备直接访问。
注册选项	使用 Citrix Gateway FQDN，或者在使用 MDM FQDN 时，选择不注册。	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、双因素、用户名 + PIN
应用程序锁定和擦除	支持。	支持。
应用程序锁定和擦除的自助服务门户选项	不支持。	支持。
应用程序擦除行为	应用程序保留在设备上，但无法使用。XenMobile 仅删除客户端上的帐户。	应用程序保留在设备上，但无法使用。XenMobile 仅删除客户端上的帐户。

针对仅限 MAM 用户的自动化操作。	支持事件、设备属性、用户属性操作。不支持基于已安装应用程序的自动化操作。	支持事件、设备属性、用户属性以及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。
当 Active Directory 用户被删除时的内置操作	支持应用程序擦除。	支持应用擦除。
注册限制	支持；通过注册配置文件配置。	支持；通过注册配置文件配置。
软件清单	支持。XenMobile 列出设备上安装的应用程序	不支持。

***关于通知：** SMTP 是发送注册邀请的唯一支持方法。

> **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，与 ENT 模式一样，设备使用 XenMobile Server FQDN 进行注册。（在旧版 MAM 模式下，设备使用 Citrix Gateway FQDN 进行注册。）

设备要求

对于任何部署而言，一个重要的考虑因素是您计划推出的设备。在 iOS、Android 和 Windows 平台上，有许多选项。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，支持多种平台是可能的。但是，在告知用户可以注册的设备时，请考虑“支持的设备平台”文章中的限制。即使您的环境中只允许一两种设备，XenMobile® 在 iOS、Android 和 Windows 设备上的功能也会略有不同。每个平台上都提供不同的功能集。

此外，并非所有应用程序设计都同时针对平板电脑和手机外形尺寸。在进行广泛更改之前，请测试应用程序以确保它们适合您想要推出的设备屏幕。

您还可以考虑注册因素。Apple 和 Google 提供企业注册计划。通过 Apple 部署计划 和 Google Android Enterprise，您可以购买预配置好并可供员工使用的设备。

有关注册的更多信息，请参阅 用户注册选项。

安全性与用户体验

安全性对任何组织都很重要，但您需要在安全性与用户体验之间取得平衡。例如，您可能有一个高度安全但用户难以使用的环境。或者，您的环境可能非常用户友好，但访问控制不够严格。本虚拟手册的其他部分详细介绍了安全功能。本文的目的是概述常见的安全问题以及 XenMobile 中可用的安全选项。

以下是每个用例需要牢记的一些关键注意事项：

- 您是想保护特定应用程序、整个设备，还是两者都保护？
- 您希望用户如何验证其身份？您打算使用 LDAP、基于证书的身份验证，还是两者的组合？
- 您希望如何处理用户会话超时？请记住，后台服务、Citrix ADC 以及离线访问应用程序都有不同的超时值。
- 您希望用户设置设备级密码、应用程序级密码，还是两者都设置？您希望为用户提供多少次登录尝试？请记住，通过 MAM 实施的额外每应用身份验证要求可能会如何影响用户体验。
- 您还想对用户施加哪些限制？您希望用户访问 Siri 等云服务吗？对于您提供给他们的每个应用程序，他们可以做什么，不能做什么？您是否希望部署企业 Wi-Fi 策略，以防止在办公场所内消耗蜂窝数据流量？

应用程序与设备

首先要考虑的是，是仅使用移动应用程序管理 (MAM) 来保护某些应用程序，还是也想使用移动设备管理 (MDM) 来管理整个设备。最常见的情况是，如果您不需要设备级控制，则只管理移动应用程序，尤其是在您的组织支持自带设备 (BYOD) 的情况下。

XenMobile 不管理的设备用户可以通过应用商店安装应用程序。您通过应用程序策略控制对应用程序的访问，而不是通过设备级控制（例如选择性擦除或完全擦除）。这些策略（取决于您设置的值）要求设备定期检查 XenMobile，以确认应用程序仍被允许运行。

MDM 允许您保护整个设备，包括清点设备上的所有软件。如果设备已越狱、已 root 或安装了不安全的软件，您可以阻止注册。然而，这种级别的控制会让用户对个人设备被赋予如此大的权力感到担忧，并可能降低注册率。

身份验证

身份验证是用户体验的重要组成部分。如果您的组织已运行 Active Directory，那么使用 Active Directory 是让用户访问系统的最简单方法。

身份验证用户体验的另一个重要部分是超时。高安全环境可以要求用户每次访问系统时都登录，但该选项并非适用于所有组织。例如，让用户每次访问电子邮件时都输入凭据会显著影响用户体验。

用户熵

为了增强安全性，您可以启用一项名为*用户熵*的功能。Citrix Secure Hub™ 和其他一些应用程序通常共享密码、PIN 和证书等常见数据，以确保一切正常运行。此信息存储在 Secure Hub 内的通用保管库中。如果您通过**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 会将信息从通用保管库移动到新保管库中。Secure Hub 或其他应用程序要访问数据，用户必须输入密码或 PIN。

启用用户熵可在多个位置增加一层身份验证。因此，每次应用程序需要访问 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。

您可以通过阅读 XenMobile 文档中的关于 MDX Toolkit 了解有关用户熵的更多信息。要启用用户熵，您可以在客户端属性中找到相关设置。

策略

MDX 和 MDM 策略都为组织提供了极大的灵活性，但它们也可能限制用户。例如，您可能希望阻止访问云应用程序，例如 Siri 或 iCloud，这些应用程序有可能将敏感数据发送到各种位置。您可以设置策略来阻止访问这些服务，但请记住，此类策略可能会产生意想不到的后果。iOS 键盘麦克风也依赖于云访问，您也可能会阻止访问该功能。

应用程序

企业移动管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 使组织能够保护和控制移动设备，而 MAM 则促进应用程序交付和管理。随着 BYOD 的日益普及，您通常可以实施 MAM 解决方案来协助应用程序交付、软件许可、配置和应用程序生命周期管理。

借助 XenMobile，您可以通过配置特定的 MAM 策略和 VPN 设置来进一步保护这些应用程序，以防止数据泄露和其他安全威胁。XenMobile 为组织提供了部署以下任何解决方案的灵活性：

- 仅限 MAM 的环境
- 仅限 MDM 的环境
- 统一的 XenMobile Enterprise 环境，在同一平台上提供 MDM 和 MAM 功能

除了能够将应用程序交付到移动设备之外，XenMobile 还通过 MDX 技术提供应用程序容器化。MDX 通过加密来保护应用程序，这种加密独立于平台提供的设备级加密。您可以擦除或锁定应用程序，并且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 Mobile Apps SDK 应用这些控制。

在企业环境中，用户使用各种移动应用程序来协助其工作。这些应用程序可以包括来自公共应用商店的应用程序、内部开发的应用程序和本机应用程序。XenMobile 将这些应用程序分类如下：

公共应用程序：这些应用程序包括公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。组织外部的供应商通常会在公共应用商店中提供其应用程序。此选项允许其客户直接从 Internet 下载应用程序。根据用户的需求，您可能在组织中使用许多公共应用程序。此类应用程序的示例包括 GoToMeeting、Salesforce 和 EpicCare 应用程序。

Citrix 不支持直接从公共应用商店下载应用程序二进制文件，然后使用 MDX Toolkit 对其进行打包以进行企业分发。要启用第三方应用程序的 MDX 功能，请联系您的应用程序供应商以获取应用程序二进制文件。您可以使用 MDX Toolkit 打包二进制文件，或将 MAM SDK 与二进制文件集成。

内部应用程序： 许多组织都有内部开发人员，他们创建提供特定功能的应用程序，并在组织内部独立开发和分发。在某些情况下，一些组织可能还拥有 ISV 提供的应用程序。您可以将此类应用程序部署为本机应用程序，也可以使用 XenMobile 等 MAM 解决方案对应用程序进行容器化。例如，医疗保健组织可以创建一个内部应用程序，允许医生在移动设备上查看患者信息。然后，组织可以启用 MAM SDK 或 MDM 封装该应用程序，以保护患者信息并启用对后端患者数据库服务器的 VPN 访问。

Web 和 SaaS 应用程序： 这些应用程序包括从内部网络（Web 应用程序）或通过公共网络 (SaaS) 访问的应用程序。XenMobile 还允许您使用应用程序连接器列表创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器可以促进对现有 Web 应用程序的单点登录 (SSO)。有关详细信息，请参阅 (/zh-cn/xenmobile/server/apps/app-connector-types.html)。例如，您可以将 Google Apps SAML 用于基于安全断言标记语言 (SAML) 的 Google Apps SSO。

移动生产力应用程序： 随 XenMobile 许可证提供的 Citrix 开发的应用程序。有关详细信息，请参阅关于移动生产力应用程序。Citrix 还提供其他业务就绪型应用程序，这些应用程序由 ISV 使用移动应用程序 SDK 开发。

HDX 应用程序： 您使用 StoreFront 发布的 Windows 托管应用程序。如果您有 Citrix Virtual Apps and Desktops™ 环境，则可以将应用程序与 XenMobile 集成，使已注册用户可以使用这些应用程序。

根据您计划使用 XenMobile 部署和管理的移动应用程序类型，底层配置和体系结构会有所不同。例如，如果具有不同权限级别的多个用户组使用单个应用程序，则可能需要单独的交付组来部署两个版本的应用程序。此外，您必须确保用户组成员资格是互斥的，以避免用户设备上出现策略不匹配。

您可能还希望通过 Apple 批量采购来管理 iOS 应用程序许可。此选项要求您注册 Apple 批量采购并在 XenMobile 控制台中配置 XenMobile 批量采购设置，以使用批量采购许可证分发应用程序。各种此类用例使得在实施 XenMobile 环境之前评估和规划您的 MAM 策略变得非常重要。您可以通过定义以下内容来开始规划您的 MAM 策略：

应用程序类型： 列出您计划支持的不同类型的应用程序，然后对其进行分类。例如：公共、本机、移动生产力应用程序、Web、内部、ISV 应用程序等。此外，还要根据不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。此分类有助于您调整每种应用程序所需的 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 来启用特殊的 API 以与其他应用程序进行交互。

网络要求： 使用适当的设置配置具有特定网络访问要求的应用程序。例如，某些应用程序可能需要通过 VPN 访问您的内部网络。某些应用程序可能需要 Internet 访问才能通过 DMZ 路由访问。要允许此类应用程序连接到所需的网络，您必须相应地配置各种设置。定义每个应用程序的网络要求有助于尽早确定您的架构决策，从而简化整个实施过程。

安全要求： 定义适用于单个应用程序或所有应用程序的安全要求至关重要。该规划可确保您在安装 XenMobile Server 时创建正确的配置。尽管 MDX 策略等设置适用于单个应用程序，但会话和身份验证设置适用于所有应用程序。某些应用程序可能具有特定的加密、容器化、封装、加密、身份验证、地理围栏、密码或数据共享要求，您可以提前概述这些要求以简化部署。

部署要求： 您可能希望使用基于策略的部署，以仅允许合规用户下载已发布的应用程序。例如，您可能希望某些应用程序需要以下任何一项：

- 启用基于设备平台的加密
- 设备已受管理
- 设备满足最低操作系统版本要求
- 某些应用程序仅供企业用户使用

您可能还希望某些应用程序仅供企业用户使用。请提前概述此类要求，以便您可以配置适当的部署规则或操作。

许可要求： 记录与应用程序相关的许可要求。这些记录有助于您有效管理许可证使用情况，并决定是否在 XenMobile 中配置特定功能以方便许可。例如，如果您部署免费或付费的 iOS 应用程序，Apple 会通过要求用户登录其 iTunes 帐户来强制执行应用程序的许可要求。您可以注册 Apple 批量采购，通过 XenMobile 分发和管理这些应用程序。批量采购允许用户下载应用程序，而无需登录其 iTunes 帐户。此外，Samsung SAFE 和 Samsung Knox 等工具也有特殊的许可要求，您需要在部署这些功能之前完成这些要求。

允许列表和阻止列表要求： 您可能希望阻止用户安装或使用某些应用程序。创建使设备不合规的应用程序的允许列表。然后，设置策略以在设备不合规时触发。另一方面，某个应用程序可能可以接受使用，但由于某种原因可能属于阻止列表。在这种情况下，您可以将该应用程序添加到允许列表，并指出该应用程序可以接受使用，但不是必需的。此外，请记住，新设备上预装的应用程序可能包含一些不属于操作系统的常用应用程序。这些应用程序可能与您的阻止列表策略冲突。

应用程序用例

一家医疗保健组织计划部署 XenMobile 作为其移动应用程序的 MAM 解决方案。移动应用程序将交付给企业用户和 BYOD 用户。IT 部门决定交付和管理以下应用程序：

- **移动生产力应用程序：** 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：** 提供 Internet 和内部网站点访问权限的安全 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：** 所有移动设备用于与 XenMobile 通信的客户端。IT 部门通过 Secure Hub 客户端将安全设置、配置和移动应用程序推送到移动设备。Android 和 iOS 设备通过 Secure Hub 注册到 XenMobile。
- **Citrix Receiver™：** 允许用户在移动设备上打开由 Virtual Apps and Desktops 托管的应用程序的移动应用程序。
- **GoToMeeting：** 一款在线会议、桌面共享和视频会议客户端，允许用户通过 Internet 与其他计算机用户、客户、客户端或同事实时会面。
- **Salesforce1：** Salesforce1 允许用户从移动设备访问 Salesforce，并将所有 Chatter、CRM、自定义应用程序和业务流程整合到一个统一的体验中，供任何 Salesforce 用户使用。
- **RSA SecurID：** 用于双因素身份验证的基于软件的令牌。
- **EpicCare 应用：** 这些应用为医疗从业者提供安全且便携的患者病历、患者列表、日程和消息访问权限。
    - **Haiku：** 适用于 iPhone 和 Android 手机的移动应用。
    - **Canto：** 适用于 iPad 的移动应用。
    - **Rover：** 适用于 iPhone 和 iPad 的移动应用。

HDX： 这些应用通过 Citrix Virtual Apps™ 和 Desktops 交付。

- **Epic Hyperspace：** 用于电子健康记录管理的 Epic 客户端应用程序。

ISV

- **Vocera：** 符合 HIPAA 规范的 IP 语音和消息移动应用，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

- **HCMail：** 此应用可帮助编写加密消息、在内部邮件服务器上搜索地址簿，并使用电子邮件客户端将加密消息发送给联系人。

内部 WEB 应用

- **PatientRounding：** 用于不同部门记录患者健康信息的 Web 应用程序。
- **Outlook Web Access：** 允许通过 Web 浏览器访问电子邮件。
- **SharePoint：** 用于组织范围内的文件和数据共享。

下表列出了 MAM 配置所需的基本信息。

应用程序名称	应用程序类型	MDX 封装	iOS	安卓
安全邮件	XenMobile 应用程序	版本 10.4.1 及更高版本不需要	是	是
安全 Web	XenMobile 应用程序	版本 10.4.1 及更高版本不需要	是	是
思杰文件	XenMobile App	版本 10.4.1 及更高版本不支持	是	是
安全中心	公共应用	不适用	是	是
思杰接收器	公共应用	不适用	是	是
GoToMeeting	公共应用	不适用	是	是
赛富时1	公共应用	不适用	是	是
RSA SecurID	公共应用	不适用	是	是
Epic 海库	公共应用	不适用	是	是
Epic 坎托	公共应用	不适用	是	否
Epic 罗孚	公共应用	不适用	是	否
Epic 超空间	HDX™ 应用	不适用	是	是
沃西拉	ISV 应用	是	是	是

HC邮件	内部应用	是	是	是
PatientRounding	Web 应用	不适用	是	是
Outlook Web 访问	Web 应用	不适用	是	是
SharePoint	Web 应用	不适用	是	是

以下表格列出了在 XenMobile 中配置 MAM 策略时可以参考的具体要求。

应用程序名称	需要 VPN	交互	交互	基于设备平台的加密
		（与容器外部的应用程序）	（来自容器外部的应用程序）	
安全邮件	是	选择性允许	允许	不需要
安全 Web	是	允许	允许	不需要
思杰文件	是	允许	允许	不需要
思杰安全中心	是	不适用	不适用	不适用
思杰接收器	是	不适用	不适用	不适用
GoToMeeting	否	不适用	不适用	不适用
赛富时1	否	不适用	不适用	不适用
RSA SecurID	否	N/A	N/A	N/A
艾派克海库	是	N/A	N/A	N/A
艾派克坎托	是	N/A	N/A	N/A
艾派克罗孚	是	不适用	不适用	不适用
埃匹克超空间	是	不适用	不适用	不适用
沃西拉	是	已阻止	已阻止	不需要

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）	（来自容器外部的应用程序）	
医院邮件	是	已阻止	已阻止	必需
PatientRounding	是	不适用	不适用	必需
Outlook Web 访问	是	不适用	不适用	非必需
SharePoint	是	不适用	不适用	不需要

应用程序名称	代理筛选	许可	地理围栏	移动应用程序 SDK	最低操作系统版本
安全邮件	必需	不适用	选择性必需	不适用	强制执行
安全 Web	必需	不适用	不需要	不适用	强制
思杰文件	必需	不适用	不需要	不适用	强制
安全中心	不需要	批量购买	不需要	不适用	未强制执行
思杰接收器	不需要	批量采购	不需要	不适用	未强制执行
GoToMeeting	不需要	批量采购	不需要	不适用	未强制执行
赛富时1	不需要	批量购买	不需要	不适用	未强制执行
RSA SecurID	不需要	批量购买	不需要	不适用	未强制执行
埃匹克俳句	不需要	批量购买	不需要	不适用	未强制执行
艾派克 坎托	不需要	批量采购	不需要	不适用	未强制执行
艾派克 罗孚	不需要	批量采购	不需要	不适用	未强制执行

应用程序名称	代理筛选	许可	地理围栏	移动应用程序 SDK	最低操作系统版本
埃匹克 超空间	不需要	不适用	不需要	不适用	未强制
沃塞拉	需要	不适用	需要	需要	已强制
医疗邮件	需要	不适用	必需	必需	已强制执行
PatientRound-ing	必需	不适用	非必需	不适用	未强制执行
Outlook 网页版	必需	不适用	非必需	不适用	未强制执行
SharePoint	必需	不适用	不需要	不适用	未强制执行

用户社区

每个组织都由在不同职能角色中运作的多元用户社区组成。这些用户社区通过您通过用户的移动设备提供的各种资源执行不同的任务和办公职能。用户可能在家或在远程办公室使用您提供的移动设备工作。或者，用户可能使用其个人移动设备，这使他们能够访问受某些安全合规规则约束的工具。

随着越来越多的用户社区使用移动设备，企业移动性管理 (EMM) 对于防止数据泄露和强制实施安全限制变得至关重要。为了实现高效且更复杂的移动设备管理，您可以对用户社区进行分类。这样做可以简化用户到资源的映射，并确保正确的安全策略应用于正确的用户。

以下示例说明了医疗保健组织的用户社区如何针对 EMM 进行分类。

用户社区用例

这个示例医疗保健组织为包括网络和附属员工以及志愿者在内的多个用户提供技术资源和访问权限。该组织已选择仅向非执行用户推出 EMM 解决方案。

该组织的用户角色和职能可分为以下子组：临床、非临床和承包商。一部分选定的用户会收到公司移动设备，而其他用户可以从其个人设备访问有限的公司资源。为了强制执行适当级别的安全限制并防止数据泄露，该组织决定由公司 IT 管理每个已注册的设备，无论是公司发放的还是 BYOD 设备。此外，用户只能注册一台设备。

以下部分概述了每个子组的角色和职能：

临床

- 护士
- 医生（内科医生、外科医生等）
- 专科医生（营养师、麻醉师、放射科医生、心脏病专家、肿瘤科医生等）
- 外部医生（非雇员医生和在远程办公室工作的办公室职员）
- 家庭健康服务（为患者上门就诊提供医生服务的办公室和移动工作人员）
- 研究专家（六个研究所的知识工作者和高级用户，他们进行临床研究以寻找医学问题的答案）
- 教育和培训（教育和培训领域的护士、医生和专家）

非临床

- 共享服务（执行各种后台职能的办公室职员，包括：人力资源、薪资、应付账款、供应链服务等）
- 医生服务（为提供者执行各种医疗保健管理、行政服务和业务流程解决方案的办公室职员，包括：行政服务、分析和商业智能、业务系统、客户服务、财务、管理式医疗管理、患者访问解决方案、收入周期解决方案等）
- 支持服务（执行各种非临床职能的办公室职员，包括：福利管理、临床整合、通信、薪酬和绩效管理、设施和物业服务、人力资源技术系统、信息服务、内部审计和流程改进等）
- 慈善项目（执行各种职能以支持慈善项目的办公室和移动工作人员）

承包商

- 制造商和供应商合作伙伴（通过站点到站点 VPN 在现场和远程连接，提供各种非临床支持功能）

根据上述信息，组织创建了以下实体。有关 XenMobile 中交付组的更多信息，请参阅部署资源。

ACTIVE DIRECTORY 组织单位 (OU) 和组

对于 OU = XenMobile Resources:

- OU = 临床；组 =
  - XM-护士
  - XM-医生
  - XM-专家
  - XM-外部医生
  - XM-家庭健康服务
  - XM-研究专家

  - XM-教育和培训
- OU = 非临床；组 =
  - XM-共享服务
  - XM-医生服务
  - XM-支持服务
  - XM-慈善项目

XENMOBILE 本地用户和组

对于组 = 承包商，用户 =

- 供应商1
- 供应商2
- 供应商 3
- … 供应商 10

XENMOBILE 交付组

- 临床-护士
- 临床-医生
- 临床-专家
- 临床-外部医生
- 临床-家庭健康服务
- 临床-研究专家
- 临床-教育和培训
- 非临床-共享服务
- 非临床-医生服务
- 非临床-支持服务
- 非临床-慈善项目

交付组和用户组映射

活动目录组	**XenMobile 交付组**
XM-护士	临床-护士

XM-医生	临床-医生
XM-专家	临床-专家
XM-外部医生	临床-外部医生
XM-家庭健康服务	临床-家庭健康服务
XM-研究专家	临床-研究专家
XM-教育和培训	临床-教育和培训
XM-共享服务	非临床-共享服务
XM-医生服务	非临床-医生服务
XM-支持服务	非临床-支持服务
XM-慈善项目	非临床-慈善项目

交付组和资源映射

以下表格说明了此用例中分配给每个交付组的资源。第一个表格显示了移动应用程序分配。第二个表格显示了公共应用程序、HDX 应用程序和设备管理资源。

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		
临床医生			
临床专家			
临床外部医生	X		
临床家庭健康服务	X		
临床研究专家	X		
临床教育和培训		X	X
非临床 - 共享服务		X	X

非临床 - 医生服务		X	X
非临床 - 支持服务	X	X	X
非临床 - 慈善项目	X	X	X
承包商	X	X	X

XenMobile 交付组	**公共应用：RSA SecurID**	**公共应用：EpicCare Haiku**	**HDX 应用程序：Epic Hyperspace**	**密码策略**	**设备限制**	**自动化操作**	**WiFi 策略**
临床护士							X
临床医生					X		
临床专家							
临床-外部医生							
临床-家庭健康服务							
临床-研究专家							
临床-教育和培训		X	X				
非临床-共享服务		X	X				

非临床-医生服务		X	X				
非临床支持服务		X	X				

注意事项

- XenMobile 在初始配置期间会创建一个名为“所有用户”的默认交付组。如果您不禁用此交付组，则所有 Active Directory 用户都有权注册到 XenMobile。
- XenMobile 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果用户属于未在 XenMobile 中映射的组，则该用户无法注册。同样，如果用户是多个组的成员，XenMobile 会将用户归类为仅属于映射到 XenMobile 的组。
- 要使 MDM 注册成为强制性，您必须在 XenMobile 控制台的“服务器属性”中将“需要注册”选项设置为“True”。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，从 XenMobile 交付组中删除用户组。 **注意：** 在执行此操作之前，请创建 XenMobile 和数据库的备份。

关于 XenMobile 中的设备所有权

您可以根据用户设备的拥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 设备如何连接到您的网络：在每种资源类型的部署规则中以及通过“**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。

您可以要求所有 BYOD 用户在访问应用程序之前接受对其设备的公司管理。或者，您可以允许用户访问公司应用程序，而无需管理其设备。

当您将服务器设置 **wsapi.mdm.required.flag** 设置为 **true** 时，XenMobile 会管理所有 BYOD 设备，并且任何拒绝注册的用户都将被拒绝访问应用程序。建议在企业 IT 团队在将用户设备注册到 XenMobile 时需要高安全性以及积极的用户体验的环境中，将 **wsapi.mdm.required.flag** 设置为 **true**。

如果您将 **wsapi.mdm.required.flag** 保留为 **false**（这是默认设置），用户可以拒绝注册，但仍可以通过 XenMobile Store 访问其设备上的应用程序。建议在隐私、法律或法规限制要求不进行设备管理，而只进行企业应用程序管理的环境中，将 **wsapi.mdm.required.flag** 设置为 **false**。

拥有 XenMobile 不管理的设备的用户可以通过 XenMobile Store 安装应用程序。与设备级控制（例如选择性擦除或完全擦除）不同，您通过应用程序策略控制对应用程序的访问。这些策略根据您设置的值，要求设备定期检查 XenMobile Server，以确认应用程序仍被允许运行。

安全要求

在部署 XenMobile 环境时，安全注意事项的数量可能很快变得令人应接不暇。有许多相互关联的组件和设置。为了帮助您入门并选择可接受的保护级别，Citrix 提供了针对高、更高和最高安全性的建议，如下表所示。

您的部署模式选择不仅仅涉及安全问题。在选择部署模式之前，还必须审查用例要求并确定是否可以缓解安全问题。

高： 使用这些设置可在保持大多数组织可接受的基本安全级别的同时，提供最佳用户体验。

更高： 这些设置在安全性和可用性之间实现了更强的平衡。

最高： 遵循这些建议可在牺牲可用性和用户采用率的情况下提供高水平的安全性。

部署模式安全注意事项

下表指定了每个安全级别的部署模式。

高安全性	**更高安全性**	**最高安全性**
MAM 或 MDM	MDM+MAM	MDM+MAM；加上 FIPS

注意：

- 根据用例，仅MDM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、微型VPN或应用程序特定策略，MDM足以管理和保护设备。
- 对于BYOD等用例，如果仅应用程序容器化即可满足所有业务和安全要求，Citrix 建议使用仅MAM模式。
- 对于高安全性环境（以及公司发放的设备），Citrix 建议使用MDM+MAM以利用所有可用的安全功能。请务必强制执行MDM注册。
- 适用于具有最高安全需求的环境（例如联邦政府）的FIPS选项。

如果启用FIPS模式，则必须将SQL Server配置为加密SQL流量。

Citrix ADC 和 Citrix Gateway 安全注意事项

下表指定了每个安全级别的 Citrix ADC 和 Citrix Gateway 建议。

高安全性	更高安全性	最高安全性
建议使用 Citrix ADC。MAM 和 ENT 需要 Citrix Gateway；MDM 建议使用。	如果 XenMobile 位于 DMZ 中，则使用带 SSL 桥接的 XenMobile 向导配置的标准 Citrix ADC。如果 XenMobile Server 位于内部网络中，则在必要时使用 SSL 卸载以满足安全标准。	具有端到端加密的 SSL 卸载

注意：

- 将 XenMobile Server 通过 NAT 或现有第三方代理和负载均衡器暴露给互联网可以是 MDM 的一个选项。但是，这种设置要求 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，具有默认 XenMobile 配置的 Citrix ADC 通常能满足或超出安全要求。
- 对于具有最高安全需求的 MDM 环境，在 Citrix ADC 上终止 SSL 可实现边界流量检查并保持端到端 SSL 加密。
- 定义 SSL/TLS 密码的选项。
- 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

下表列出了每个安全级别的 Citrix ADC 和 Citrix Gateway 建议。

高安全性	更高安全性	最高安全性
仅限 Active Directory 组成员身份。所有用户交付组已禁用。	仅限邀请的注册安全模式。仅限 Active Directory 组成员身份。所有用户交付组已禁用。	注册安全模式与设备 ID 绑定。仅限 Active Directory 组成员身份。所有用户交付组已禁用。

注意：

- Citrix 通常建议您将注册限制为仅限于预定义的 Active Directory 组中的用户。此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将注册限制为仅限收到邀请的用户。注册邀请不适用于 Windows 设备。

- 您可以使用一次性 PIN (OTP) 注册邀请作为双因素身份验证解决方案，并控制用户可以注册的设备数量。OTP 邀请不适用于 Windows 设备。

设备密码安全注意事项

下表列出了每个安全级别的设备密码建议。

高安全性	**更高安全性**	**最高安全性**
推荐。设备级加密需要高安全性。通过 MDM 强制执行。您可以使用 MDX 策略“不合规设备行为”将高安全性设置为仅适用于 MAM。	通过 MDM、MDX 策略或两者强制执行。	通过 MDM 和 MDX 策略强制执行。MDM 复杂密码策略。

注意：

- Citrix 建议使用设备密码。
- 您可以通过 MDM 策略强制执行设备密码。
- 您可以使用 MDX 策略将设备密码设置为使用托管应用程序的必要条件。例如，对于 BYOD 用例。
- Citrix 建议结合使用 MDM 和 MDX 策略选项，以提高 MDM+MAM 环境中的安全性。
- 对于具有最高安全要求的环境，您可以配置复杂的密码策略并通过 MDM 强制执行。您可以配置自动操作，以便在设备不符合密码策略时通知管理员或执行选择性/完全设备擦除。

应用程序

企业移动管理 (EMM) 分为移动设备管理 (MDM) 和移动应用程序管理 (MAM)。MDM 使组织能够保护和控制移动设备，而 MAM 则促进应用程序的交付和管理。为了支持 BYOD（自带设备）的采用，您通常可以实施 MAM 解决方案（例如 XenMobile®）来协助完成以下任务：

- 应用程序交付
- 软件许可
- 配置
- 应用程序生命周期管理

您可以要求或允许用户选择加入 MDM 管理。

借助 XenMobile，您可以通过配置特定的 MAM 策略和 VPN 设置来进一步保护这些应用程序，以防止数据泄露和其他安全威胁。XenMobile 为组织提供了灵活性，可以将其解决方案部署为：

- 仅限 MAM 的环境
- 仅限 MDM 的环境
- 统一的 XenMobile Enterprise 环境，提供 MDM 和 MAM 功能

除了能够将应用程序交付到移动设备之外，XenMobile 还通过 MDX 技术提供应用程序容器化。这些应用程序受精细的基于策略的控制。独立软件供应商 (ISV) 可以使用移动应用程序 SDK 应用这些控制。

在企业环境中，用户使用各种移动应用程序来协助其工作。这些应用程序可以包括来自公共应用商店的应用程序、内部开发的应用程序或本机应用程序。XenMobile 将这些应用程序分类如下：

- **公共应用程序：** 这些应用程序包括公共应用商店（例如 Apple App Store 或 Google Play）中提供的免费或付费应用程序。组织外部的供应商通常会在公共应用商店中提供其应用程序。此选项允许其客户直接从 Internet 下载应用程序。您可能根据用户的需求在组织中使用许多公共应用程序。此类应用程序的示例包括 GoToMeeting、Salesforce 和 EpicCare 应用程序。
  - **如果您使用 MAM SDK：** 从您的应用程序供应商处获取应用程序二进制文件。然后，将 MAM SDK 集成到应用程序中。
  - **如果您使用 MDX Toolkit：** Citrix® 不支持直接从公共应用商店下载应用程序二进制文件，然后使用 MDX Toolkit 对其进行封装以进行企业分发。要封装第三方应用程序，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 封装这些二进制文件。
- **内部应用：** 许多组织都有内部开发人员，他们创建提供特定功能并在组织内部独立开发和分发的应用程序。在某些情况下，一些组织可能还有 ISV 提供的应用程序。您可以将此类应用程序部署为本机应用程序，或者使用 MAM 解决方案（例如 XenMobile）对应用程序进行容器化。

  例如，医疗保健组织可能会创建一个内部应用程序，允许医生在移动设备上查看患者信息。然后，组织可以使用以下方法之一保护患者信息并启用对患者数据库的 VPN 访问：

  - MAM SDK
  - MDX 工具包
- **Web 和 SaaS 应用程序：** 这些应用程序包括从内部网络（Web 应用程序）或公共网络（SaaS）访问的应用程序。XenMobile 还允许您使用应用程序连接器列表创建自定义 Web 和 SaaS 应用程序。这些应用程序连接器可以促进对现有 Web 应用程序的单点登录 (SSO)。有关

详细信息，请参阅 应用程序连接器类型。例如，您可以将 Google Apps SAML 用于基于安全断言标记语言 (SAML) 的 SSO 以访问 Google Apps。

- **移动生产力应用程序：** 移动生产力应用程序是 Citrix 开发的应用程序，包含在 XenMobile 许可证中。有关详细信息，请参阅 关于移动生产力应用程序。Citrix 还提供其他 业务就绪应用程序，这些应用程序由 ISV 使用移动应用程序 SDK 开发。
- **HDX 应用程序：** HDX 应用程序是您使用 StoreFront 发布的 Windows 托管应用程序。如果您使用 Citrix Virtual Apps and Desktops™ 和 Citrix Workspace™，则已注册用户可以使用 HDX 应用程序。

根据您计划使用 XenMobile 部署和管理的移动应用程序类型，底层配置可能有所不同。例如，具有不同权限级别的多个用户组可能会使用单个应用程序。在这种情况下，您可以创建单独的交付组来部署同一应用程序的两个不同版本。此外，您必须确保用户组成员资格是互斥的，以避免用户设备上出现策略不匹配。

您还可以通过使用 Apple 批量采购来管理 iOS 应用程序许可。此选项要求您注册批量采购计划并在 XenMobile 控制台中配置批量采购设置。该配置允许您使用批量采购许可证分发应用程序。各种用例使得在实施 XenMobile 环境之前评估和规划您的 MAM 策略变得非常重要。您可以通过定义以下内容来开始规划您的 MAM 策略：

- **应用程序类型：** 列出您计划支持的不同类型的应用程序并对其进行分类，例如公共、本机、Web、内部或 ISV 应用程序。此外，还要根据不同的设备平台（例如 iOS 和 Android）对应用程序进行分类。这种分类有助于调整每种应用程序类型所需的各种 XenMobile 设置。例如，某些应用程序可能需要使用移动应用程序 SDK 来启用与其他应用程序交互的特殊 API。
- **网络要求：** 配置具有特定网络访问要求的应用程序的设置。例如，某些应用程序可能需要通过 VPN 访问您的内部网络。某些应用程序可能需要 Internet 访问才能通过 DMZ 路由访问。要允许此类应用程序连接到所需的网络，您必须相应地配置各种设置。定义每个应用程序的网络要求有助于尽早确定您的架构决策，从而简化整个实施过程。
- **安全要求：** 您可以定义适用于单个应用程序或所有应用程序的安全要求。
  - 设置（例如 MDX 策略）适用于单个应用程序
  - 会话和身份验证设置适用于所有应用程序
  - 某些应用程序可能具有特定的容器化、MDX、身份验证、地理围栏、密码或数据共享要求

  请提前概述这些要求，以简化部署。有关 Endpoint Management 中安全性的详细信息，请参阅 安全性与用户体验。
- **部署要求** - 您可能希望使用基于策略的部署，以仅允许合规用户下载已发布的应用程序。例如，某些应用程序可能要求设备受管理，或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供企业用户使用。请提前概述此类要求，以便您可以配置相应的部署规则或操作。

- **许可要求：** 记录与应用程序相关的许可要求。您的记录可以帮助您有效管理许可证使用情况，并决定是否在 XenMobile 中配置特定功能以方便许可。例如，如果您部署免费或付费的 iOS 应用程序，Apple 会对该应用程序强制执行许可要求。因此，用户必须登录其 Apple App Store 帐户。

  但是，您可以注册 Apple 批量采购，以使用 XenMobile 分发和管理这些应用程序。批量采购允许用户下载应用程序，而无需登录其 Apple App Store 帐户。

  某些平台（例如 Samsung SAFE 和 Samsung Knox）在部署这些功能之前需要完成特殊的许可要求。

- **允许列表和阻止列表要求：** 您可能会识别出不希望用户安装或使用的应用程序。创建阻止列表定义了一个不合规事件。然后，您可以设置策略以在事件发生时触发。另一方面，某个应用程序可能可以接受使用，但由于某种原因可能属于阻止列表。在这种情况下，您可以将该应用程序添加到允许列表，并指出该应用程序可以接受使用但不是必需的。此外，请记住，新设备上预安装的应用程序可能包含一些不属于操作系统的常用应用程序。此类应用程序可能与您的阻止列表策略冲突。

用例

一家医疗保健组织计划部署 XenMobile，作为其移动应用程序的 MAM 解决方案。移动应用程序将交付给企业用户和 BYOD 用户。IT 决定交付和管理以下应用程序：

移动生产力应用程序： 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™： 所有移动设备用于与 XenMobile 通信的客户端。您可以使用 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 注册到 XenMobile。

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： 一个在线会议、桌面共享和视频会议客户端，允许用户通过互联网实时与其他的计算机用户、客户、委托人或同事会面。

SalesForce1： Salesforce1 允许用户从移动设备访问 Salesforce，并将所有 Chatter、CRM、自定义应用程序和业务流程整合到一个统一的体验中，供任何 Salesforce 用户使用。

RSA SecurID： 用于双因素身份验证的基于软件的令牌。

EpicCare 应用程序： 这些应用程序为医护人员提供安全便携的患者病历、患者列表、日程和消息访问权限。

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 交付 HDX 应用程序。

- **Epic Hyperspace：** 用于电子健康记录管理的 Epic 客户端应用程序。

ISV：

- **Vocera：** 符合 HIPAA 规范的 IP 语音和消息移动应用程序，可通过 iPhone 和 Android 智能手机随时随地扩展 Vocera 语音技术的优势。

内部应用程序：

- **HCMail：** 可帮助撰写加密消息、在内部邮件服务器上搜索地址簿以及使用电子邮件客户端将加密消息发送给联系人的应用程序。

内部 Web 应用程序：

- **PatientRounding：** 用于由不同部门记录患者健康信息的 Web 应用程序。
- **Outlook Web Access：** 允许通过 Web 浏览器访问电子邮件。
- **SharePoint：** 用于组织范围的文件和数据共享。

下表列出了 MAM 配置所需的基本信息。

应用程序名称	应用程序类型	MAM SDK 集成或 MDX 封装	iOS	安卓
安全邮件	XenMobile 应用程序	版本 10.4.1 及更高版本不需要	是	是
安全 Web	XenMobile 应用程序	版本 10.4.1 及更高版本不需要	是	是
思杰文件	XenMobile 应用程序	版本 10.4.1 及更高版本不支持	是	是
安全中心	公共应用程序	不适用	是	是
思杰接收器	公共应用程序	不适用	是	是

GoToMeeting	公共应用	不适用	是	是
SalesForce1	公共应用	不适用	是	是
RSA SecurID	公共应用	不适用	是	是
Epic 海库	公共应用	不适用	是	是
Epic 坎托	公共应用	不适用	是	否
Epic 罗孚	公共应用	不适用	是	否
史诗超空间	HDX 应用程序	不适用	是	是
沃塞拉	ISV 应用程序	是	是	是
HC邮件	内部应用程序	是	是	是
患者查房	Web 应用	不适用	是	是
Outlook Web 访问	Web 应用	不适用	是	是
SharePoint	Web 应用	不适用	是	是

下表列出了在 XenMobile 中配置 MAM 策略时可以参考的具体要求。

应用程序名称	需要 VPN	交互（与容器外部应用）	交互（来自容器外部应用）	代理过滤	许可	地理围栏	移动应用 SDK	最低操作系统版本
安全邮件	是	选择性允许	允许	必需	不适用	选择性要求	不适用	强制执行
安全 Web	是	允许	允许	必需	不适用	不需要	不适用	强制执行
Citrix 文件	是	允许	允许	必需	不适用	不需要	不适用	强制执行

应用程序名称	需要VPN	交互（与容器外部应用）	交互（来自容器外部应用）	代理过滤	许可	地理围栏	移动应用SDK	最低操作系统版本
安全中心	是	不适用	不适用	不需要	批量购买	不需要	不适用	未强制执行
思杰接收器	是	不适用	不适用	不需要	批量购买	不需要	不适用	未强制执行
GoTo Meeting	否	不适用	不适用	不需要	批量采购	不需要	不适用	不强制执行
Sales Force 1	N	不适用	不适用	不需要	批量采购	不需要	不适用	不强制执行
RSA SecurID	N	不适用	不适用	不需要	批量采购	不需要	不适用	未强制执行
史诗俳句	是	不适用	不适用	不需要	批量采购	不需要	不适用	未强制执行
史诗坎托	是	不适用	不适用	不需要	批量采购	不需要	不适用	未强制执行
史诗罗弗	是	不适用	不适用	不需要	批量采购	不需要	不适用	未强制执行
艾派克超空间	是	不适用	不适用	不需要	不适用	不需要	不适用	未强制执行
沃塞拉	是	已阻止	已阻止	必需	不适用	必需	必需	已强制
艾驰邮件	是	已阻止	已阻止	必需	不适用	必需	必需	强制执行
患者查房	是	不适用	不适用	必需	不适用	不需要	不适用	未强制执行

应用程序名称	需要 VPN	交互（与容器外部应用）	交互（来自容器外部应用）	代理过滤	许可	地理围栏	移动应用 SDK	最低操作系统版本
Outlook Web 访问	是	不适用	不适用	必需	不适用	不需要	不适用	未强制执行
SharePoint	是	不适用	不适用	必需	不适用	不需要	不适用	未强制执行

用户社区

每个组织都由在不同职能角色中运作的多元用户社区组成。这些用户社区使用您通过用户移动设备提供的各种资源来执行不同的任务和办公功能。用户可能在家中或远程办公室使用您提供的移动设备工作，或者用户可能使用个人移动设备，这使他们能够访问受某些安全合规性规则约束的工具。

随着越来越多的用户社区使用移动设备，企业移动性管理 (EMM) 对于防止数据泄露和强制执行组织安全限制变得至关重要。为了实现高效且更复杂的移动设备管理，您可以对用户社区进行分类。这样做可以简化用户到资源的映射，并确保正确的安全策略应用于正确的用户。

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和资源，例如应用程序。从 Active Directory 安全组中删除用户会移除对先前允许的 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，您可以将其创建为本地 XenMobile 用户。您可以将本地用户添加到交付组，并以与 Active Directory 用户相同的方式向他们提供资源。

- XenMobile 交付组

  如果具有不同权限级别的多个用户组要使用单个应用程序，您可能需要创建单独的交付组。通过单独的交付组，您可以部署同一应用程序的两个不同版本。

- 交付组和用户组映射

  交付组到 Active Directory 组的映射可以是一对一，也可以是一对多。将基本策略和应用程序分配给一对多交付组映射。将特定于功能的策略和应用程序分配给一对一交付组映射。

- 交付组和应用程序资源映射

  将特定应用程序分配给每个交付组。

- 交付组和 MDM 资源映射

  将应用程序和特定的设备管理资源分配给每个交付组。例如，可以配置一个交付组，其中包含以下任意组合：应用程序类型（公共、HDX™ 等）、每种应用程序类型的特定应用程序，以及设备策略和自动化操作等资源。

以下示例说明了医疗保健组织的用户社区如何针对 EMM 进行分类。

用例

此示例医疗保健组织为包括网络和附属员工以及志愿者在内的多个用户提供技术资源和访问权限。该组织已选择仅向非执行用户推出 EMM 解决方案。

您可以将此组织的用户角色和职能划分为以下子组：临床、非临床和承包商。一部分选定的用户会收到公司移动设备，而其他用户则可以通过其个人设备 (BYOD) 访问有限的公司资源。为了实施适当级别的安全限制并防止数据泄露，该组织决定由公司 IT 管理每个注册设备。此外，用户只能注册一台设备。

以下部分概述了每个子组的角色和职能。

临床

- 护士
- 医生（内科医生、外科医生等）
- 专科医生（营养师、采血师、麻醉师、放射科医生、心脏病专家、肿瘤科医生等）
- 外部医生（非雇员医生和在远程办公室工作的办公室职员）
- 家庭医疗服务（为患者上门就诊提供医生服务的办公室和移动工作人员）
- 研究专家（六个研究所的知识工作者和高级用户，从事临床研究以寻找医学问题的答案）
- 教育和培训（教育和培训领域的护士、医生和专家）

非临床

- 共享服务（办公室工作人员执行各种后台职能，包括：人力资源、薪资、应付账款、供应链服务等）
- 医生服务（办公室工作人员为提供者执行各种医疗保健管理、行政服务和业务流程解决方案，包括：行政服务、分析和商业智能、业务系统、客户服务、财务、管理式医疗管理、患者访问解决方案、收入周期解决方案等）

- 支持服务（办公室工作人员执行各种非临床职能，包括：福利管理、临床整合、通信、薪酬和绩效管理、设施和物业服务、人力资源技术系统、信息服务、内部审计和流程改进等）
- 慈善项目（办公室和移动工作人员执行各种职能以支持慈善项目）

承包商

- 制造商和供应商合作伙伴（通过站点到站点 VPN 在现场和远程连接，提供各种非临床支持功能）

根据上述信息，组织创建了以下实体。有关 XenMobile 中交付组的更多信息，请参阅 XenMobile 产品文档中的部署资源。

Active Directory 组织单位 (OU) 和组

对于 OU = XenMobile 资源

- OU = 临床；组 =
  - XM-护士
  - XM-医生
  - XM-专家
  - XM-外部医生
  - 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-医生服务
  - XM-支持服务
  - XM-慈善项目

XenMobile 本地用户和组

对于组= 承包商，用户 =

- 供应商1
- 供应商2
- 供应商 3

- … 供应商 10

XenMobile 交付组

- 临床护士
- 临床-医生
- 临床-专家
- 临床-外部医生
- 临床-家庭健康服务
- 临床-研究专家
- 临床-教育和培训
- 非临床-共享服务
- 非临床-医生服务
- 非临床-支持服务
- 非临床-慈善项目

交付组和用户组映射

活动目录组	**XenMobile 交付组**
XM-护士	临床-护士
XM-医生	Clinical-医生
XM-专家	Clinical-专家
XM-外部医生	Clinical-外部医生
XM-家庭健康服务	Clinical-家庭健康服务
XM-研究专家	Clinical-研究专家
XM-教育和培训	Clinical-教育和培训
XM-共享服务	Non-Clinical-共享服务
XM-医生服务	非临床医生服务
XM-支持服务	非临床支持服务

XM-慈善项目	非临床慈善项目

交付组和应用程序的资源映射

	安全邮件	安全Web	Share File	接收器	Sales Force 1	RSA SecurID	爱佩克护理海库	爱佩克超空间
临床护士	X	X	X					
临床医生								
临床专家								
临床外部医生	X		X					
临床家庭健康服务	X		X					
临床研究专家	X		X					
临床教育和培训							X	X
非临床-共享服务							X	X
非临床-医师服务							X	X

非临床-支持服务	X		X				X	X
非临床-慈善项目	X		X				X	X
承包商	X		X	X	X		X	X

交付组和 MDM 资源的资源映射

	MDM: 密码策略	**MDM: 设备限制**	**MDM: 自动化操作**	**MDM: WiFi 策略**
临床-护士				X
临床-医生		X		
临床-专家				
临床-外部医生				
临床-家庭健康服务				
临床-研究专家				
临床-教育和培训				
非临床-共享服务				
非临床-医生服务				
非临床-支持服务				

非临床-慈善项目				
承包商				X

注意事项

- XenMobile 在初始配置期间创建了一个名为 All Users 的默认交付组。如果您不禁用此交付组，则所有 Active Directory 用户都有权注册到 XenMobile。
- XenMobile 使用与 LDAP 服务器的动态连接按需同步 Active Directory 用户和组。
- 如果用户所属的组未在 XenMobile 中映射，则该用户无法注册。同样，如果用户是多个组的成员，XenMobile 只会将该用户归类为已映射到 XenMobile 的组中的成员。
- 要在 XenMobile 控制台中强制执行 MDM 注册，请在**服务器属性**中将**需要注册**选项设置为**True**。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。

> **注意：**
>
> 在执行此操作之前，请创建 XenMobile 和数据库的备份。

关于 XenMobile 中的设备所有权

您可以根据用户设备的拥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 设备如何连接到您的网络：在部署规则中以及通过**设置**页面上的 XenMobile 服务器属性。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 用户在访问应用程序之前接受对其设备的公司管理。或者，您可以允许用户访问公司应用程序，而无需管理其设备。

当您将服务器属性 **wsapi.mdm.required.flag** 设置为 **true** 时，XenMobile 会管理所有 BYOD 设备，并且任何拒绝注册的用户都将被拒绝访问应用程序。在企业 IT 团队需要高安全性以及注册期间的积极用户体验的环境中，请考虑将 **wsapi.mdm.required.flag** 设置为 **true**。

如果您将 **wsapi.mdm.required.flag** 保留为默认设置 **false**，则用户可以拒绝注册。但是，他们可以通过 XenMobile Store 访问其设备上的应用程序。在隐私、法律或法规限制要求不进行设备管理，而只进行企业应用程序管理的环境中，请考虑将 **wsapi.mdm.required.flag** 设置为 **false**。

拥有 XenMobile 不管理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，而不是通过设备级控制（例如选择性擦除或完全擦除）。某些策略设置要求设备定期检查 XenMobile Server，以确认应用程序仍被允许运行。

电子邮件策略

从移动设备安全访问电子邮件是任何组织移动性管理计划背后的主要驱动力之一。确定正确的电子邮件策略通常是任何 XenMobile® 设计的关键组成部分。XenMobile 提供了多种选项，可根据安全性、用户体验和集成要求来适应不同的用例。本文涵盖了从客户端选择到邮件流量的典型设计决策过程和选择正确解决方案的注意事项。

选择您的电子邮件客户端

客户端选择通常是整体电子邮件策略设计的首要任务。您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包含的原生邮件，或通过公共应用商店提供的其他第三方客户端。根据您的需求，您可能可以使用单个（标准）客户端来支持用户社区，或者可能需要组合使用多个客户端。

下表概述了不同客户端选项的一些设计注意事项：

主题	安全邮件	原生（例如，iOS 邮件）	第三方邮件
最低 XenMobile 版本	高级版	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。所有其他客户端均被视为第三方客户端。	通常需要用户手动配置。
安全性	设计安全，提供最高安全性。使用 MDX 策略并增加了数据加密级别。Secure Mail	基于供应商/应用程序功能集。提供更高的安全性。使用设备加密设置（不通过	基于供应商/应用程序功能集。提供高安全性。

	是通过 MDX 策略完全管理的应用程序。通过 Citrix PIN 增加了额外的身份验证层。	MDX 策略提供安全性）。依赖设备级身份验证来访问应用程序。	
集成	默认允许与托管 (MDX) 应用程序交互。使用 Citrix Secure Web 打开 Web URL。将文件保存到 Citrix Files 并从 Citrix Files 附加文件。直接加入 GoToMeeting 并拨入。	默认情况下只能与其他非托管（非 MDX）应用程序交互。	默认情况下只能与其他非托管（非 MDX）应用程序交互。
部署/许可	您可以通过 MDM 或直接从公共应用商店推送 Secure Mail。包含在 XenMobile Advanced 和 Enterprise 许可中。	客户端应用程序随平台操作系统提供。无额外许可要求。	可以通过 MDM 作为企业应用程序推送，或直接从公共应用商店推送。相关的许可模式/成本取决于应用程序供应商。
支持	客户端和 EMM 解决方案（Citrix）的单一供应商支持。Secure Hub/应用调试日志记录功能中嵌入了支持联系信息。一个客户端需要支持。	供应商定义的（Apple/Google）支持。可能需要根据设备平台支持不同的客户端。	供应商定义的（Apple/Google）支持。一个客户端需要支持，前提是第三方客户端在所有托管设备平台上都受支持。

邮件流量流和筛选注意事项

本节讨论了 XenMobile 环境中邮件 (ActiveSync) 流量流动的三个主要场景和设计注意事项。

场景 1：公开的 Exchange

支持外部客户端的环境通常会将 Exchange ActiveSync 服务公开到互联网。移动 ActiveSync 客户端通过反向代理（例如 Citrix ADC）或边缘服务器，通过此面向外部的路径进行连接。此选项是使用本机或第三方邮件客户端所必需的，这使得这些客户端成为此场景的流行选择。虽然不常见，但您也可以在此场景中使用 Secure Mail 客户端。这样做，您可以从使用 MDX 策略和应用管理所提供的安全功能中受益。

场景 2：通过 Citrix ADC 隧道（微 VPN 和 STA）

由于其微 VPN 功能，此场景在使用 Secure Mail 客户端时是默认设置。在这种情况下，Secure Mail 客户端通过 Citrix Gateway 建立与 ActiveSync 的安全连接。本质上，您可以将 Secure Mail 视为直接从内部网络连接到 ActiveSync 的客户端。Citrix 客户通常将 Secure Mail 作为首选的移动 ActiveSync 客户端进行标准化。该决定是避免在公开的 Exchange Server 上将 ActiveSync 服务暴露给互联网的举措的一部分，如第一个场景所述。

只有启用了 MAM SDK 或经过 MDX 封装的应用才能使用微 VPN 功能。如果您使用 MDX 封装，此场景不适用于本机客户端。尽管可能可以使用 MDX Toolkit 封装第三方客户端，但这种做法并不常见。使用设备级 VPN 客户端为本机或第三方客户端提供隧道访问已被证明是繁琐且不可行的解决方案。

场景 3：云托管 Exchange 服务

云托管 Exchange 服务（例如 Microsoft Office 365）正变得越来越流行。在 XenMobile 的上下文中，此场景可以与第一个场景以相同的方式处理，因为 ActiveSync 服务也暴露在互联网上。在这种情况下，云服务提供商的要求决定了客户端的选择。这些选择通常包括支持大多数 ActiveSync 客户端，例如 Secure Mail 以及其他本机或第三方客户端。

对于此场景，XenMobile 可以在三个方面增加价值：

- 具有 MDX 策略和通过 Secure Mail 进行应用管理的客户端
- 在受支持的本机电子邮件客户端上使用 MDM 策略进行客户端配置
- ActiveSync 过滤选项，结合使用 Endpoint Management connector for Exchange ActiveSync

邮件流量过滤注意事项

与大多数暴露于互联网的服务一样，您必须保护路径并为授权访问提供过滤。XenMobile 解决方案包含两个专门设计用于为原生和第三方客户端提供 ActiveSync 过滤功能的组件：Citrix Gateway connector™ for Exchange ActiveSync 和 Endpoint Management connector for Exchange ActiveSync。

Citrix Gateway 的 Exchange ActiveSync 连接器

Citrix Gateway connector for Exchange ActiveSync 通过使用 Citrix ADC 作为 ActiveSync 流量的代理，在边界提供 ActiveSync 过滤。因此，过滤组件位于邮件流量路径中，拦截进入或离开环境的邮件。Citrix Gateway connector for Exchange ActiveSync 充当 Citrix ADC 和 XenMobile Server 之间的中介。当设备通过 Citrix ADC 上的 ActiveSync 虚拟服务器与 Exchange 通信时，Citrix ADC 会对 connector for Exchange ActiveSync 服务执行 HTTP 回调。该服务随后会向 XenMobile 检查设备状态。根据设备状态，connector for Exchange ActiveSync 会回复 Citrix ADC 以允许或拒绝连接。您还可以配置静态规则，根据用户、代理和设备类型或 ID 过滤访问。

此设置允许 Exchange ActiveSync 服务暴露于互联网，并增加了一层安全性以防止未经授权的访问。设计注意事项包括以下几点：

- Windows Server: Exchange ActiveSync 组件的连接器需要 Windows Server。
- 过滤规则集：connector for Exchange ActiveSync 旨在根据设备状态和信息而非用户信息进行过滤。尽管您可以配置静态规则按用户 ID 过滤，但没有基于 Active Directory 组成员身份进行过滤的选项。如果需要 Active Directory 组过滤，则可以使用 Endpoint Management connector for Exchange ActiveSync。
- Citrix ADC 可扩展性：鉴于需要通过 Citrix ADC 代理 ActiveSync 流量：Citrix ADC 实例的适当大小对于支持所有 ActiveSync SSL 连接的额外工作负载至关重要。
- Citrix ADC 集成缓存：Citrix ADC 上的 connector for Exchange ActiveSync 配置使用集成缓存功能来缓存来自 connector for Exchange ActiveSync 的响应。由于此配置，Citrix ADC 无需在给定会话中的每个 ActiveSync 事务都向 Citrix Gateway connector for Exchange ActiveSync 发出请求。此配置对于足够的性能和规模也至关重要。集成缓存可用于 Citrix ADC Platinum Edition，或者您可以为 Enterprise Editions 单独许可该功能。
- 自定义过滤策略：您可能需要创建自定义 Citrix ADC 策略，以限制标准原生移动客户端之外的某些 ActiveSync 客户端。此配置需要了解 ActiveSync HTTP 请求和 Citrix ADC 响应器策略的创建。
- Secure Mail 客户端：Secure Mail 具有微型 VPN 功能，无需在边界进行过滤。当通过 Citrix Gateway 连接时，Secure Mail 客户端通常被视为内部（受信任的）ActiveSync 客户端。如果需要同时支持原生和第三方（使用 connector for Exchange ActiveSync）以及 Secure Mail 客户端：Citrix 建议 Secure Mail 流量不要通过用于 connector for Exchange ActiveSync 的 Citrix ADC 虚拟服务器。您可以通过 DNS 实现此流量流，并防止 connector for Exchange ActiveSync 策略影响 Secure Mail 客户端。

有关 XenMobile 部署中 Citrix Gateway connector for Exchange ActiveSync 的图示，请参阅 本地部署参考架构。

用于 Exchange ActiveSync 的 端点管理 连接器

Endpoint Management connector for Exchange ActiveSync 是一个 XenMobile 组件，可在 Exchange 服务级别提供 ActiveSync 过滤。因此，过滤仅在邮件到达 Exchange 服务时发生，而不是在邮件进入 XenMobile 环境时发生。Mail Manager 使用 PowerShell 查询 Exchange ActiveSync 以获取设备伙伴关系信息，并通过设备隔离操作控制访问。这些操作根据 Endpoint Management connector for Exchange ActiveSync 规则标准将设备移入和移出隔离区。与 Citrix Gateway connector for Exchange ActiveSync 类似，Endpoint Management connector for Exchange

ActiveSync 会向 XenMobile 检查设备状态，以根据设备合规性过滤访问。您还可以配置静态规则，根据设备类型或 ID、代理版本和 Active Directory 组成员身份过滤访问。

此解决方案不需要使用 Citrix ADC。您可以部署用于 Exchange ActiveSync 的 Endpoint Management 连接器，而无需更改现有 ActiveSync 流量的路由。设计注意事项包括：

- Windows Server：用于 Exchange ActiveSync 组件的 Endpoint Management 连接器要求您部署 Windows Server。
- 筛选规则集：与用于 Exchange ActiveSync 的 Citrix Gateway 连接器一样，用于 Exchange ActiveSync 的 Endpoint Management 连接器包含用于评估设备状态的筛选规则。此外，用于 Exchange ActiveSync 的 Endpoint Management 连接器还支持基于 Active Directory 组成员身份进行筛选的静态规则。
- Exchange 集成：用于 Exchange ActiveSync 的 Endpoint Management 连接器需要直接访问托管 ActiveSync 角色并控制设备隔离操作的 Exchange 客户端访问服务器 (CAS)。此要求可能会根据环境架构和安全状况带来挑战。您必须预先评估此技术要求。
- 其他 ActiveSync 客户端：由于用于 Exchange ActiveSync 的 Endpoint Management 连接器在 ActiveSync 服务级别进行筛选，因此请考虑 XenMobile 环境之外的其他 ActiveSync 客户端。您可以配置用于 Exchange ActiveSync 的 Endpoint Management 连接器静态规则，以避免对其他 ActiveSync 客户端造成意外影响。
- 扩展的 Exchange 功能：通过与 Exchange ActiveSync 直接集成，用于 Exchange ActiveSync 的 Endpoint Management 连接器使 XenMobile 能够在移动设备上执行 Exchange ActiveSync 擦除。用于 Exchange ActiveSync 的 Endpoint Management 连接器还允许 XenMobile 访问有关 Blackberry 设备的信息并执行其他控制操作。

有关 XenMobile 部署中用于 Exchange ActiveSync 的 Endpoint Management 连接器图，请参阅本地部署的参考体系结构。

电子邮件平台决策树

下图可帮助您区分在 XenMobile 部署中使用本机电子邮件或 Secure Mail 解决方案的优缺点。每个选择都允许关联的 XenMobile 选项和要求，以启用服务器、网络和数据库访问。优缺点包括安全性、策略和用户界面方面的详细考虑。

What is the best mobile email platform for your situation?

Citrix Secure Mail

XenMobile options and requirements

Secure Mail - unrestricted
- Email traffic bypasses NetScaler Gateway
- MDX policies secure the app
- Exchange ActiveSync/CAS is exposed to the Internet

Secure Mail – tunneled to the internal network
- Email traffic leverages NetScaler Gateway
- Uses XenMobile as a STA server (optional)
- MDX policies secure the app

Pros for each option

WorxMail – unrestricted
- Better battery life on device
- Secured with MDX policies
- Supports client certificate authentication for security
- Integration with Citrix Secure apps
- Standard user interface across platforms

WorxMail – tunneled to the internal network
- Best battery life on device (with STA)
- Secured with MDX policies
- Support for client certificates
- Full control of app access
- Integration with Citrix Secure apps
- Exchange ActiveSync/CAS is not exposed to the Internet
- Standard user interface across platforms

Native email

XenMobile options and requirements

XenMobile Mail Manager
- Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
- Requires XenMobile Mail Manager server

XenMobile NetScaler Connector
- Can leverage internal-only Exchange access
- Requires XenMobile NetScaler Connector server and NetScaler

Native ActiveSync
- Existing Exchange ActiveSync/CAS infrastructure
- Exchange ActiveSync/CAS must be externally accessible

Pros for each option

XenMobile Mail Manager
- Ability to use native mail client
- Supports Microsoft Office 365
- Blacklist/whitelist access policies
- Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
- Can connect to BlackBerry BES and perform basic device controls
- Can filter Exchange ActiveSync access to non-MDM managed devices

XenMobile NetScaler Connector
- Ability to use devices-native mail client
- Rule-based allow and deny modes
- Uses NetScaler as a reverse proxy
- More secure than XenMobile Mail Manager and external access to Exchange ActiveSync/CAS

Native ActiveSync
- Ability to use native mail client
- Basic Exchange ActiveSync/CAS device management capabilities

XenMobile® 集成

本文介绍在规划 XenMobile 如何与您现有的网络和解决方案集成时需要考虑的因素。例如，如果您已将 Citrix ADC 用于 Virtual Apps and Desktops：

- 您是使用现有 Citrix ADC 实例，还是新的专用实例？
- 您是否希望将使用 StoreFront™ 发布的 HDX 应用程序与 XenMobile 集成？
- 您是否计划将 Citrix Files 与 XenMobile 结合使用？
- 您是否有希望集成到 XenMobile 中的网络访问控制解决方案？
- 您是否为网络中的所有出站流量部署了 Web 代理？

Citrix 应用交付控制器和 Citrix 网关

XenMobile ENT 和 MAM 模式强制要求使用 Citrix Gateway。Citrix Gateway 为访问所有公司资源提供了微型 VPN 路径，并提供强大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 位于您的 DMZ 或内部网络中（因此流量从设备流向 Citrix ADC 再流向 XenMobile）

您可以使用现有 Citrix ADC 实例，也可以为 XenMobile 设置新实例。以下部分将介绍使用现有或新的专用 Citrix ADC 实例的优缺点。

共享的 Citrix ADC MPX，带有为 XenMobile 创建的 Citrix Gateway VIP

优点：

- 使用一个通用 Citrix ADC 实例，用于所有 Citrix 远程连接：Citrix Virtual Apps and Desktops™、全 VPN 和无客户端 VPN。
- 使用现有的 Citrix ADC 配置，例如用于证书身份验证以及访问 DNS、LDAP 和 NTP 等服务。
- 使用单个 Citrix ADC 平台许可证。

缺点：

- 在同一 Citrix ADC 上处理两种不同的用例时，更难以规划扩展。
- 有时，Citrix Virtual Apps™ and Desktops 用例需要特定的 Citrix ADC 版本。同一版本可能对 XenMobile 存在已知问题。或者 XenMobile 可能对 Citrix ADC 版本存在已知问题。
- 如果存在 Citrix Gateway，则无法第二次运行 Citrix ADC for XenMobile 向导来创建 XenMobile 的 Citrix ADC 配置。

- 除非 Citrix Gateway 11.1 或更高版本使用 Platinum 许可证：安装在 Citrix ADC 上且 VPN 连接所需的用户访问许可证是共用的。由于这些许可证可用于所有 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

优点：

Citrix 建议使用 Citrix ADC 的专用实例。

- 更易于规划扩展，并将 XenMobile 流量与可能已受资源限制的 Citrix ADC 实例分离。
- 避免 XenMobile 和 Citrix Virtual Apps and Desktops 需要不同 Citrix ADC 软件版本时出现问题。通常建议对 XenMobile 使用最新兼容的 Citrix ADC 版本和内部版本。
- 允许通过内置的 Citrix ADC for XenMobile 向导配置 XenMobile 的 Citrix ADC。
- 服务的虚拟和物理分离。
- 除非 Citrix Gateway 11.1 或更高版本使用 Platinum 许可证：XenMobile 所需的用户访问许可证仅适用于 Citrix ADC 上的 XenMobile 服务。

缺点：

- 需要在 Citrix ADC 上设置额外的服务以支持 XenMobile 配置。
- 需要另一个 Citrix ADC 平台许可证。为每个 Citrix ADC 实例授予 Citrix Gateway 许可证。

有关将 Citrix ADC 和 Citrix Gateway 与每种 XenMobile Server 模式集成时要考虑的事项，请参阅与 Citrix ADC 和 Citrix Gateway 集成。

StoreFront

如果您有 Citrix Virtual Apps and Desktops 环境，可以使用 StoreFront 将 HDX™ 应用程序与 XenMobile 集成。将 HDX 应用程序与 XenMobile 集成时：

- 这些应用程序可供已注册 XenMobile 的用户使用。
- 这些应用程序会与其他移动应用程序一起显示在 XenMobile Store 中。
- XenMobile 使用 StoreFront 上的旧版 PNAgent（服务）站点。
- 当设备上安装了 Citrix Receiver™ 时，HDX 应用程序将开始使用 Receiver。

StoreFront 的限制是每个 StoreFront 实例只能有一个服务站点。假设您有多个应用商店，并且希望将其与其他生产用途分开。在这种情况下，Citrix 通常建议您为 XenMobile 考虑一个新的 StoreFront 实例和服务站点。

注意事项包括：

- StoreFront 是否有任何不同的身份验证要求？StoreFront 服务站点需要 Active Directory 凭据才能登录。仅使用基于证书的身份验证的客户无法通过 XenMobile 使用相同的 Citrix Gateway 枚举应用程序。
- 使用相同的应用商店还是创建新的应用商店？
- 使用相同还是不同的 StoreFront 服务器？

以下部分介绍了为 Receiver 和移动生产力应用程序使用单独或组合店面所带来的优缺点。

将现有 StoreFront 实例与 XenMobile Server 集成

优点：

- 相同店面：如果使用相同的 Citrix ADC VIP 进行 HDX 访问，则 XenMobile 无需额外的 StoreFront 配置。假设您选择使用相同的店面并希望将 Receiver 访问定向到新的 Citrix ADC VIP。在这种情况下，请将相应的 Citrix Gateway 配置添加到 StoreFront。
- 相同 StoreFront 服务器：使用现有的 StoreFront 安装和配置。

缺点：

- 相同店面：StoreFront 的任何重新配置以支持 Virtual Apps and Desktops 工作负载，也可能会对 XenMobile 产生不利影响。
- 相同 StoreFront 服务器：在大型环境中，请考虑 XenMobile 使用 PNAgent 进行应用程序枚举和启动所带来的额外负载。

使用新的专用 StoreFront 实例与 XenMobile Server 集成

优点：

- 新店面：XenMobile 的 StoreFront 店面的任何配置更改不得影响现有的 Virtual Apps and Desktops 工作负载。
- 新 StoreFront 服务器：服务器配置更改不得影响 Virtual Apps and Desktops 工作流。此外，XenMobile 使用 PNAgent 进行应用程序枚举和启动之外的负载不得影响可扩展性。

缺点：

- 新店面：StoreFront 店面配置。
- 新 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 访问 Virtual Apps and Desktops。

ShareFile 文件共享和 Citrix 文件

> **免责声明：**

> 如果 ShareFile（现为 Progress）停止支持，此功能将被弃用。

> Citrix Files 使用户能够从任何设备访问和同步其所有数据。借助 Citrix Files，用户可以安全地与组织内部和外部的人员共享数据。如果您将 ShareFile 与 XenMobile Advanced Edition 或 Enterprise Edition 集成，XenMobile 可以为 Citrix Files 提供：

- XenMobile App 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。

移动用户可以受益于完整的企业帐户功能集。

此外，您可以将 XenMobile 配置为仅与存储区域连接器集成。通过存储区域连接器，Citrix Files 提供对以下内容的访问：

- 文档和文件夹
- 网络文件共享
- 在 SharePoint 站点中：站点集和文档库。

连接的文件共享可以包括 Citrix Virtual Apps and Desktops 环境中使用的相同网络主驱动器。您可以使用 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。

以下部分列出了在为 Citrix Files 制定设计决策时需要考虑的问题。

与 Citrix Files 集成或仅与存储区域连接器集成

要问的问题：

- 您是否希望将数据存储在 Citrix 管理的存储区域中？
- 您是否希望为用户提供文件共享和同步功能？
- 您是否希望用户能够访问 Citrix Files 网站上的文件？或者从移动设备访问 Office 365 内容和个人云连接器？

设计决策：

- 如果这些问题中的任何一个答案是“是”，请与 Citrix Files 集成。
- 仅与存储区域连接器集成可为 iOS 用户提供对现有本地存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问。在此配置中，您无需设置 ShareFile 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 结合使用符合防止用户信息泄露到公司网络之外的安全限制。

存储区域控制器服务器位置

要问的问题：

- 您是否需要本地存储或存储区域连接器等功能？
- 如果使用 Citrix Files 的本地功能，存储区域控制器将位于网络的何处？

设计决策：

- 确定是将存储区域控制器服务器放置在 Citrix Files 云中、您的本地单租户存储系统中，还是受支持的第三方云存储中。
- 存储区域控制器需要一定的互联网访问权限才能与 Citrix Files 控制平面通信。您可以通过多种方式连接，包括直接访问、NAT/PAT 配置或代理配置。

存储区域连接器

要问的问题：

- CIFS 共享路径是什么？
- SharePoint URL 是什么？

设计决策：

- 确定是否需要本地存储区域控制器才能访问这些位置。
- 由于存储区域连接器与文件存储库、CIFS 共享和 SharePoint 等内部资源通信，Citrix 建议存储区域控制器位于 DMZ 防火墙后面的内部网络中，并由 Citrix ADC 提供前端服务。

SAML 与 XenMobile Enterprise 集成

要问的问题：

- 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？
- 您当前的环境中是否有标准 IdP？
- 使用 SAML 需要多少个域？
- Active Directory 用户是否有多个电子邮件别名？

- 是否有任何 Active Directory 域迁移正在进行或即将进行？

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。身份验证选项包括：

- 使用 XenMobile Server 作为 SAML 的身份提供程序 (IdP)

此选项可以提供出色的用户体验，自动创建 Citrix Files 帐户，并启用移动应用程序 SSO 功能。

- XenMobile Server 已针对此过程进行了增强：它不需要同步 Active Directory。
- 使用 Citrix Files 用户管理工具进行用户预配。
- 使用受支持的第三方供应商作为 SAML 的 IdP

如果您有现有且受支持的 IdP 并且不需要移动应用程序 SSO 功能，则此选项可能最适合您。此选项还需要使用 Citrix Files 用户管理工具进行帐户预配。

使用第三方 IdP 解决方案（例如 ADFS）也可以在 Windows 客户端提供 SSO 功能。在选择 Citrix Files SAML IdP 之前，请务必评估用例。

此外，为了满足这两种用例，您可以将 ADFS 和 XenMobile 配置为双 IdP。

移动应用程序

要问的问题：

- 您计划使用哪个 Citrix Files 移动应用程序（公共、MDM、MDX）？

设计决策：

- 您可以从 Apple App Store 和 Google Play Store 分发移动生产力应用程序。通过这种公共应用商店分发，您可以从 Citrix 下载页面获取封装的应用程序。
- 如果安全性要求不高且不需要容器化，则公共 Citrix Files 应用程序可能不适用。在仅 MDM 的环境中，您可以使用 XenMobile 的 MDM 模式交付 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

要提出的问题：

- 您对桌面、Web 和移动用户有哪些限制要求？
- 您希望为用户设置哪些标准访问控制设置？
- 您计划使用哪种文件保留策略？

设计决策：

- Citrix Files 允许您管理员工权限和设备安全性。有关信息，请参阅员工权限和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，其次是 Citrix Files 设备安全设置。示例：如果您在 Citrix Files 中禁用外部应用程序，但在 XenMobile 中启用它们，则外部应用程序将在 Citrix Files 中被禁用。您可以配置应用程序，使 XenMobile 不需要 PIN/密码，但 Citrix Files 应用程序需要 PIN/密码。

标准存储区域与受限存储区域

要提出的问题：

- 您是否需要受限存储区域？

设计决策：

- 标准存储区域用于非敏感数据，并允许员工与非员工共享数据。此选项支持涉及在域外共享数据的工作流。
- 受限存储区域可保护敏感数据：只有经过身份验证的域用户才能访问该区域中存储的数据。

Web 代理

通过 HTTP(S)/SOCKS 代理路由 XenMobile 流量最可能的情况如下：当 XenMobile Server 所在的子网无法出站访问所需的 Apple、Google 或 Microsoft IP 地址时。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。

下表描述了与 XenMobile 配合使用的最常见代理的优点和缺点。

选项	优点	缺点
将 HTTP(S)/SOCKS 代理与 XenMobile Server 结合使用。	在策略不允许 XenMobile Server 子网进行出站 Internet 连接的情况下：您可以配置 HTTP(S) 或 SOCKS 代理以提供 Internet 连接。	如果代理服务器出现故障，APNs (iOS) 或 Firebase Cloud Messaging (Android) 连接将中断。因此，所有 iOS 和 Android 设备的设备通知都将失败。
将 HTTP(S) 代理与 Secure Web 结合使用。	您可以监控 HTTP/HTTPS 流量，以确保 Internet 活动符合您组织的标准。	此配置要求所有 Secure Web Internet 流量在发送回 Internet 之前先隧道回公司网络。如果您的 Internet 连接限

		制了浏览：此配置可能会影响 Internet 浏览性能。

您的 Citrix ADC 分流隧道会话配置文件配置对流量的影响如下。

当 Citrix ADC 分流隧道处于**关闭**状态时：

- 如果 MDX **网络访问**策略设置为**隧道连接到内部网络**：所有流量都将强制使用微型 VPN 或无客户端 VPN (cVPN) 隧道返回到 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。

> **重要提示：**
>
> 请务必将 Secure Hub cVPN 流量从代理中排除。

- 有关详细信息，请参阅在安全浏览模式下通过代理服务器的 XenMobile Secure Hub 流量。

当 **Citrix ADC 拆分隧道**处于**开启**状态时：

- 当应用程序配置了 MDX **网络访问**策略并设置为**隧道连接到内部网络**时：应用程序首先尝试直接获取 Web 资源。如果 Web 资源不可公开访问，则这些应用程序将回退到 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。

> **重要提示：**
>
> 请务必将 Secure Hub cVPN 流量从代理中排除。

> 您的 Citrix ADC 会话配置文件中针对**拆分 DNS**（在**客户端体验**下）的配置功能类似于拆分隧道。

当**拆分 DNS**已启用并设置为**两者**时：

- 客户端首先尝试在本地解析 FQDN，然后在失败时回退到 Citrix ADC 进行 DNS 解析。

当**拆分 DNS**设置为**远程**时：

- DNS 解析仅在 Citrix ADC 上进行。

将 **拆分 DNS** 设置为 **本地** 时：

- 客户端尝试在本地解析 FQDN。Citrix ADC 不用于 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。诸如 XenMobile 之类的企业移动性管理解决方案非常擅长为移动设备提供安全性和控制，而与位置无关。但是，当您将它们与网络访问控制 (NAC) 解决方案结合使用时，您可以为网络内部的设备添加 QoS 和更精细的控制。这种组合使您能够通过 NAC 解决方案扩展 XenMobile 设备安全评估。您的 NAC 解决方案随后可以使用 XenMobile 安全评估来促进和处理身份验证决策。

您可以使用以下任何解决方案来强制执行 NAC 策略：

- 思杰网关
- 思科身份服务引擎 (ISE)
- ForeScout

Citrix 不保证与其他 NAC 解决方案的集成。

NAC 解决方案与 XenMobile 集成的优势包括：

- 为企业网络上的所有端点提供更好的安全性、合规性和控制。
- NAC 解决方案可以：
  - 在设备尝试连接到您的网络时立即检测到它们。
  - 查询 XenMobile 以获取设备属性。
  - 使用该设备信息来确定是允许、阻止、限制还是重定向这些设备。这些决策取决于您选择强制执行的安全策略。
- NAC 解决方案为 IT 管理员提供未受管和不合规设备的视图。

有关 XenMobile 支持的 NAC 合规性筛选器的说明和配置概述，请参阅网络访问控制。

多站点要求

您可以架构和配置包含多个站点的 XenMobile® 部署，以实现高可用性和灾难恢复。本文概述了 XenMobile 部署中使用的多站点高可用性和灾难恢复模型。

高可用性

- 对于 XenMobile 群集节点，Citrix ADC 负责负载平衡。有关详细信息，请参阅配置群集。

- XenMobile 服务器节点以主动/主动配置运行。
- 随着容量需求的增加，更多 XenMobile Server 节点会添加到高可用性群集。一个节点最多可处理大约 8,500 个用户设备（有关详细信息，请参阅可伸缩性和性能）。
- Citrix® 建议配置“n+1”个 XenMobile Server：每 8,500 个用户设备配置一个服务器，并额外配置一个服务器用于冗余。
- Citrix 建议尽可能为所有 Citrix ADC 实例配置高可用性，以允许配置与第二个 Citrix ADC 同步。
- 标准 Citrix ADC 高可用性对以主动/被动配置运行。

典型的 XenMobile 高可用性部署通常包括：

- 两个 Citrix ADC 实例（VPX 或 MPX）。如果使用 Citrix ADC SDX 平台，则还必须考虑高可用性。
- 两个或更多配置了相同数据库设置的 XenMobile Server。

灾难恢复

您可以配置 XenMobile 以在两个数据中心之间进行灾难恢复，其中一个数据中心处于活动状态，另一个数据中心处于被动状态。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，从而使用户体验与主动/主动设置相同。

对于灾难恢复，XenMobile 部署包括：

- 两个数据中心 - 每个数据中心包含一个或多个 Citrix ADC 实例、XenMobile 服务器和 SQL Server 数据库。
- 一个 GSLB 服务器，用于将流量定向到数据中心。GSLB 服务器配置为处理 XenMobile 注册 URL 和 Citrix Gateway URL 到站点的流量。
- 当您使用 Citrix ADC for XenMobile 向导配置 Citrix Gateway 时，默认情况下，GSLB 未启用以解析到 XenMobile 注册服务器的流量以及到 Citrix Gateway 的流量（在前往 MAM 负载平衡服务器的途中）。因此，需要更多步骤。有关准备和实施这些步骤的更多信息，请参阅灾难恢复。
- Always On 可用性组的群集 SQL Server。
- XenMobile 服务器和 SQL Server 之间的延迟必须小于 5 毫秒。

> **注意：**
>
> 本手册中描述的灾难恢复方法仅为访问层提供自动化灾难恢复。在设备连接 XenMobile Server 之前，您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。

与 Citrix Gateway 和 Citrix ADC 集成

与 XenMobile® 集成后，Citrix Gateway 为 MAM 设备远程访问内部网络提供了一种身份验证机制。此集成使移动生产力应用程序能够通过微型 VPN 连接到内网中的公司服务器。微型 VPN 是从移动设备上的应用程序到 Citrix Gateway 创建的。Citrix Gateway 提供微型 VPN 路径以访问所有公司资源，并提供强大的多因素身份验证支持。

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 位于您的 DMZ 或内部网络中（因此流量从设备流向 Citrix ADC 再流向 XenMobile）

XenMobile Server 模式的集成要求

Citrix Gateway 和 Citrix ADC 的集成要求因 XenMobile Server 模式（MAM、MDM 和 ENT）而异。

MAM

在 MAM 模式下使用 XenMobile Server 时：

- **Citrix Gateway** 是必需的。Citrix Gateway 提供微型 VPN 路径以访问所有公司资源，并提供强大的多因素身份验证支持。
- **Citrix ADC** 建议用于负载平衡。

  Citrix 建议您以高可用性配置部署 XenMobile，这需要在 XenMobile 前面部署负载平衡器。有关详细信息，请参阅 关于 MAM 和旧版 MAM 模式。

MDM

在 MDM 模式下使用 XenMobile Server 时：

- Citrix Gateway 不是必需的。对于 MDM 部署，Citrix 建议使用 Citrix Gateway 进行移动设备 VPN。
- Citrix ADC 推荐用于安全和负载平衡。

  Citrix 建议您在 XenMobile Server 前部署 Citrix ADC 设备，以实现安全和负载平衡。对于 DMZ 中 XenMobile 的标准部署，Citrix 建议使用 Citrix ADC for XenMobile 向导以及 SSL Bridge 模式下的 XenMobile Server 负载平衡。您还可以考虑在以下部署中进行 SSL 卸载：

  - XenMobile Server 位于内部网络而非 DMZ 中。
  - 或者您的安全团队需要 SSL Bridge 配置。

Citrix 不建议通过 NAT 或现有第三方代理或负载平衡器将 XenMobile Server 暴露给 Internet 以进行 MDM。即使 SSL 流量在 XenMobile Server (SSL Bridge) 上终止，这些配置也可能带来潜在的安全风险。

对于高安全性环境，具有默认 XenMobile 配置的 Citrix ADC 满足或超出了安全要求。

对于具有最高安全需求的 MDM 环境，在 Citrix ADC 上终止 SSL 允许您在边界检查流量，同时保持端到端 SSL 加密。有关更多信息，请参阅安全要求。Citrix ADC 提供了定义 SSL/TLS 密码和 SSL FIPS Citrix ADC 硬件的选项。

ENT (MAM+MDM)

当 XenMobile Server 处于 ENT 模式时：

- 需要 Citrix Gateway。Citrix Gateway 为访问所有公司资源提供微型 VPN 路径，并提供强大的多因素身份验证支持。

  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。
- Citrix ADC 推荐用于负载平衡。有关更多信息，请参阅本文前面“MDM”下的 Citrix ADC 部分。

> **重要提示：**
>
> 对于初始注册，无论您将负载平衡虚拟服务器配置为 SSL 卸载还是 SSL Bridge，来自用户设备的流量都会在 XenMobile Server 上进行身份验证。

设计决策

以下部分总结了在规划 Citrix Gateway 与 XenMobile 集成时需要考虑的许多设计决策。

许可和版本

决策详情：

- 您计划使用哪个版本的 Citrix ADC？
- 您是否已将平台许可证应用于 Citrix ADC？
- 如果您需要 MAM 功能，是否已应用 Citrix ADC 通用访问许可证？

设计指南：

确保将正确的许可证应用于 Citrix Gateway。如果您正在使用适用于 Exchange ActiveSync 的 Citrix Gateway connector™，则可能需要集成缓存。因此，您必须确保已部署适当的 Citrix ADC 版本。

启用 Citrix ADC 功能的许可证要求如下。

- XenMobile MDM 负载平衡至少需要 Citrix ADC 标准平台许可证。
- 带有存储区域控制器的 ShareFile 负载平衡至少需要 Citrix ADC 标准平台许可证。
- XenMobile Advanced Edition（本地）或 Citrix Endpoint Management™（云）包含 MAM 所需的 Citrix Gateway 通用许可证。
- Exchange 负载平衡需要 Citrix ADC Platinum 平台许可证或 Citrix ADC Enterprise 平台许可证，并附加集成缓存许可证。

适用于 XenMobile 的 Citrix ADC 版本

决策详情：

- XenMobile 环境中运行的 Citrix ADC 版本是什么？
- 您是否需要单独的实例？

设计指南：

Citrix 建议为您的 Citrix Gateway 虚拟服务器使用专用的 Citrix ADC 实例。请确保 XenMobile 环境中使用的 Citrix ADC 版本和内部版本达到最低要求。通常，最好使用与 XenMobile 兼容的最新 Citrix ADC 版本和内部版本。如果升级 Citrix Gateway 会影响现有环境，则为 XenMobile 使用第二个专用实例可能更合适。

如果您计划为 XenMobile 和其他使用 VPN 连接的应用程序共享一个 Citrix ADC 实例，请确保您有足够的 VPN 许可证。请记住，XenMobile 测试环境和生产环境不能共享一个 Citrix ADC 实例。

证书

决策详情：

- 您是否需要更高程度的安全性来注册和访问 XenMobile 环境？
- LDAP 不是一个选项吗？

设计指南：

XenMobile 的默认配置是用户名和密码身份验证。为了为 XenMobile 环境的注册和访问增加另一层安全性，请考虑使用基于证书的身份验证。您可以将证书与 LDAP 结合使用以进行双因素身份验证，从而在不需要 RSA 服务器的情况下提供更高程度的安全性。

如果您不允许 LDAP 并使用智能卡或类似方法，配置证书可让您将智能卡表示给 XenMobile。然后，用户使用 XenMobile 为他们生成的唯一 PIN 进行注册。用户获得访问权限后，XenMobile 会创建并部署用于向 XenMobile 环境进行身份验证的证书。

XenMobile 仅支持第三方证书颁发机构的证书吊销列表 (CRL)。如果您配置了 Microsoft CA，XenMobile 会使用 Citrix ADC 来管理吊销。当您配置基于客户端证书的身份验证时，请考虑是否需要配置 Citrix ADC 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh**（启用 CRL 自动刷新）。此步骤可确保仅在 MAM 中注册的设备用户无法使用设备上的现有证书进行身份验证。XenMobile 会重新颁发新证书，因为它不限制用户在证书被吊销时生成用户证书。当 CRL 检查过期的 PKI 实体时，此设置会提高 PKI 实体的安全性。

网络拓扑

决策详情：

- 需要哪种 Citrix ADC 拓扑？

设计指导：

Citrix 建议为 XenMobile 使用一个 Citrix ADC 实例。但是，您可能不希望流量从内部网络流向 DMZ。在这种情况下，请考虑设置一个额外的 Citrix ADC 实例。为内部用户使用一个 Citrix ADC 实例，为外部用户使用一个。当用户在内部和外部网络之间切换时，DNS 记录缓存可能会导致 Secure Hub 登录提示增加。

XenMobile 不支持 Citrix Gateway 双跳。

专用或共享 Citrix Gateway VIP

决策详情：

- 您目前是否将 Citrix Gateway 用于 Virtual Apps and Desktops？
- 您是否计划让 XenMobile 使用与 Virtual Apps and Desktops 相同的 Citrix Gateway？
- 两种流量的身份验证要求是什么？

设计指导：

当您的 Citrix 环境包含 XenMobile 以及 Virtual Apps and Desktops 时，您可以为两者使用相同的 Citrix ADC 实例和 Citrix Gateway 虚拟服务器。由于潜在的版本冲突和环境隔离，建议为每个 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 虚拟服务器来分离 Secure Hub 的流量。此配置替代了 XenMobile 和 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 可以毫无问题地向同一个 Citrix Gateway 进行身份验证。如果您使用基于证书的身份验证，XenMobile 会在 MDX 容器中推送一个证书，Secure Hub 使用该证书向 Citrix Gateway 进行身份验证。Receiver 独立于 Secure Hub，不能使用与 Secure Hub 相同的证书向同一个 Citrix Gateway 进行身份验证。

您可以考虑以下变通方法，它允许您为两个 Citrix Gateway VIP 使用相同的 FQDN。

- 创建两个具有相同 IP 地址的 Citrix Gateway VIP。Secure Hub 的 VIP 使用标准 443 端口，而 Virtual Apps and Desktops（部署 Receiver 的）的 VIP 使用 444 端口。
- 因此，一个 FQDN 解析到相同的 IP 地址。
- 对于此解决方法，您可以将 StoreFront™ 配置为返回端口 444 的 ICA 文件，而不是默认端口 443。此解决方法不需要用户输入端口号。

思杰网关超时

决策详情：

- 您希望如何为 XenMobile 流量配置 Citrix Gateway 超时？

设计指导：

Citrix Gateway 包含“会话超时”和“强制超时”设置。有关详细信息，请参阅推荐配置。请记住，后台服务、Citrix ADC 以及离线访问应用程序的超时值是不同的。

用于 MAM 的 XenMobile 负载均衡器 IP 地址

决策详情：

- 您是为 VIP 使用内部 IP 地址还是外部 IP 地址？

设计指导：

在可以使用公共 IP 地址作为 Citrix Gateway VIP 的环境中，以这种方式分配 XenMobile 负载均衡 VIP 和地址会导致注册失败。

确保负载均衡 VIP 使用内部 IP 地址，以避免在此场景中出现注册失败。此虚拟 IP 地址必须遵循 RFC 1918 私有 IP 地址标准。如果为此虚拟服务器使用非私有 IP 地址，Citrix ADC 将无法在身份验证过程中成功联系 XenMobile Server。有关详细信息，请参阅 `<https://support.citrix.com/article/CTX200430>`。

MDM 负载均衡机制

决策详情：

- Citrix Gateway 将如何对 XenMobile Server 进行负载均衡？

设计指南：

如果 XenMobile 位于 DMZ 中，请使用 SSL Bridge。如果 XenMobile 位于内部网络中，并且需要满足安全标准，请使用 SSL Offload。

- 当您在 SSL Bridge 模式下使用 Citrix ADC VIP 对 XenMobile Server 进行负载平衡时，Internet 流量直接流向 XenMobile Server，连接在此处终止。SSL Bridge 模式是设置和故障排除最简单的模式。
- 当您在 SSL Offload 模式下使用 Citrix ADC VIP 对 XenMobile Server 进行负载平衡时，Internet 流量直接流向 Citrix ADC，连接在此处终止。然后，Citrix ADC 会从 Citrix ADC 到 XenMobile Server 建立新的会话。SSL Offload 模式在设置和故障排除过程中涉及额外的复杂性。

采用 SSL Offload 的 MDM 负载平衡服务端口

决策详情：

- 如果您计划将 SSL Offload 模式用于负载平衡，后端服务将使用哪个端口？

设计指南：

对于 SSL Offload，请按如下方式选择端口 80 或 8443：

- 使用端口 80 返回 XenMobile Server，以实现真正的卸载。
- 不支持端到端加密，即流量的重新加密。有关详细信息，请参阅 Citrix 支持文章 NetScaler 和 XenMobile Server 之间支持的体系结构。

注册 FQDN

决策详情：

- 您计划使用什么作为用于注册和 XenMobile 实例/负载平衡 VIP 的 FQDN？

设计指南：

群集中第一个 XenMobile Server 的初始配置要求您提供 XenMobile Server FQDN。该 FQDN 必须与您的 MDM VIP URL 和内部 MAM LB VIP URL 匹配。（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，您必须使用与以下各项相同的证书：

- XenMobile SSL 侦听器证书
- 内部 MAM LB VIP 证书
- MDM VIP 证书（如果将 SSL 卸载用于 MDM VIP）

重要提示：

配置注册 FQDN 后，您无法更改它。新的注册 FQDN 需要新的 SQL Server 数据库和 XenMobile Server 重建。

Secure Web 流量

决策详情：

- 您是否计划将 Secure Web 限制为仅用于内部 Web 浏览？
- 您是否计划为内部和外部 Web 浏览启用 Secure Web？

设计指导：

如果您计划仅将 Secure Web 用于内部 Web 浏览，则 Citrix Gateway 配置非常简单。Secure Web 必须默认访问所有内部站点。您可能需要配置防火墙和代理服务器。

如果您计划将 Secure Web 用于内部和外部浏览，则必须启用 SNIP 以便进行出站 Internet 访问。IT 通常将已注册设备（使用 MDX 容器）视为公司网络的扩展。因此，IT 通常希望 Secure Web 连接返回到 Citrix ADC，通过代理服务器，然后访问 Internet。默认情况下，Secure Web 使用每个应用程序的 VPN 隧道返回到内部网络以进行所有网络访问。Citrix ADC 使用拆分隧道设置。

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

决策详情：

- 您是否计划使用推送通知？

iOS 设计指南：

您的 Citrix Gateway 配置可能包含安全票证颁发机构 (STA)，并关闭了拆分隧道。Citrix Gateway 必须允许 Secure Mail 的流量流向 iOS 版 Secure Mail 推送通知中指定的 Citrix 侦听器服务 URL。

Android 设计指南：

使用 Firebase Cloud Messaging (FCM) 来控制 Android 设备何时以及如何连接到 XenMobile。配置 FCM 后，任何安全操作或部署命令都会触发向 Secure Hub 发送推送通知，以提示用户重新连接到 XenMobile Server。

HDX™ STA

决策详情：

- 如果您计划集成 HDX 应用程序访问，应使用哪些 STA？

设计指南：

HDX STA 必须与 StoreFront 中的 STA 匹配，并且必须对 Virtual Apps and Desktops 场有效。

Citrix 文件和共享文件

决策详情：

- 您是否计划在环境中部署存储区域控制器？
- 您计划使用哪个 Citrix Files VIP URL？

设计指导：

如果您的环境中包含存储区域控制器，请确保正确配置以下各项：

- Citrix Files Switch VIP（由 Citrix Files 控制平面用于与存储区域控制器服务器通信）
- Citrix Files 负载平衡 VIP
- 所有必需的策略和配置文件

有关信息，请参阅(/zh-cn/storage-zones-controller/5-0.html)存储区域控制器文档。

SAML IdP

决策详情：

- 如果 Citrix Files 需要 SAML，您是否希望使用 XenMobile 作为 SAML IdP？

设计指导：

推荐的最佳实践是将 Citrix Files 与 XenMobile Advanced Edition 或 XenMobile Advanced Edition (本地) 或 Citrix Endpoint Management (云) 集成，这是一种比配置基于 SAML 的联合更简单的替代方案。当您将 Citrix Files 与这些 XenMobile 版本结合使用时，XenMobile 会为 Citrix Files 提供：

- 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

XenMobile 控制台使您能够执行 Citrix Files 配置，并监视服务级别和许可证使用情况。

Citrix Files 客户端有两种类型：适用于 XenMobile 客户端的 Citrix Files（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）。要了解这些差异，请参阅适用于 XenMobile 客户端的 Citrix Files 与 Citrix Files 移动客户端有何不同。

您可以将 XenMobile 和 ShareFile 配置为使用 SAML 提供对以下各项的 SSO 访问：

- Citrix Files 移动应用程序
- 非打包的 Citrix Files 客户端，例如网站、Outlook 插件或同步客户端

要将 XenMobile 用作 Citrix Files 的 SAML IdP，请确保已进行正确的配置。有关详细信息，请参阅使用 Citrix Files 进行 SSO 的 SAML。

ShareConnect 直接连接

决策详情：

- 用户是否必须使用直接连接，从运行 ShareConnect 的计算机或移动设备访问主机计算机？

设计指南：

ShareConnect 使户能够通过 iPad、Android 平板电脑和 Android 手机安全地连接到其计算机，以访问其文件和应用程序。对于直接连接，XenMobile 使用 Citrix Gateway 提供对本地网络外部资源的访问。有关配置详细信息，请参阅ShareConnect。

每种管理模式的注册 FQDN

管理模式	注册 FQDN
具有强制 MDM 注册的企业版 (MDM+MAM)	XenMobile Server 完全限定域名
企业版 (MDM+MAM)，可选 MDM 注册	XenMobile Server 完全限定域名 或 Citrix Gateway 完全限定域名
仅 MDM	XenMobile Server 完全限定域名
仅 MAM (旧版)	Citrix Gateway 完全限定域名
仅 MAM	XenMobile Server 完全限定域名

部署摘要

Citrix 建议您使用适用于 XenMobile 的 Citrix ADC 向导以确保正确配置。您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），则必须手动为其他环境配置 Citrix ADC。当您拥有一个正常运行的环境时，请在尝试手动为 XenMobile 配置 Citrix ADC 之前记下设置。

使用向导时，您做出的关键决定是使用 HTTPS 还是 HTTP 与 XenMobile Server 进行通信。HTTPS 提供安全的后端通信，因为 Citrix ADC 和 XenMobile 之间的流量是加密的。重新加密会影响

XenMobile Server 的性能。HTTP 提供更好的 XenMobile Server 性能。Citrix ADC 和 XenMobile 之间的流量未加密。下表显示了 Citrix ADC 和 XenMobile Server 的 HTTP 和 HTTPS 端口要求。

HTTPS

Citrix 通常建议将 SSL Bridge 用于 Citrix ADC MDM 虚拟服务器配置。对于 Citrix ADC SSL 卸载与 MDM 虚拟服务器结合使用，XenMobile 仅支持端口 80 作为后端服务。

管理模式	Citrix ADC 负载均衡方法	SSL 重新加密	XenMobile 服务器端口
MDM	SSL 桥接	N/A	443, 8443
MAM	SSL 卸载	已启用	8443
企业	MDM: SSL 桥接	N/A	443, 8443
企业	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 服务器端口
MDM	SSL 卸载	不支持	80
MAM	SSL 卸载	已启用	8443
企业	MDM: SSL 卸载	不支持	80
企业	MAM: SSL 卸载	已启用	8443

有关 XenMobile 部署中 Citrix Gateway 的图示，请参阅本地部署的参考架构。

MDX 应用程序的 SSO 和代理注意事项

XenMobile 与 Citrix ADC 集成，使您能够为用户提供对所有后端 HTTP/HTTPS 资源的单点登录 (SSO)。根据您的 SSO 身份验证要求，您可以将 MDX 应用程序的用户连接配置为使用以下任一选项：

- 安全浏览，这是一种无客户端 VPN

- 完整 VPN 隧道

如果 Citrix ADC 不是在您的环境中提供 SSO 的最佳方式，您可以设置一个 MDX 应用程序，并启用基于策略的本地密码缓存。本文探讨了各种 SSO 和代理选项，重点关注 Secure Web。这些概念也适用于其他 MDX 应用程序。

以下流程图总结了 SSO 和用户连接的决策流程。

SSO 和用户连接决策流程图(/en-us/xenmobile/server/media/sso-proxy-decision-flow.png)

Citrix ADC 身份验证方法

本节提供有关 Citrix ADC 支持的身份验证方法的常规信息。

SAML 身份验证

当您为安全断言标记语言 (SAML) 配置 Citrix ADC 时，用户可以连接到支持 SAML 协议的 Web 应用程序以实现单点登录。Citrix Gateway 支持 SAML Web 应用程序的身份提供程序 (IdP) 单点登录。

所需配置：

- 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对 Web 应用程序的 SSO，Citrix ADC 会自动执行 NTLM 身份验证。

所需配置：

- 在 Citrix ADC 会话或流量配置文件中启用 SSO。

Kerberos 模拟

XenMobile® 仅支持 Secure Web 的 Kerberos。当您为 Kerberos SSO 配置 Citrix ADC 时，如果 Citrix ADC 可以获取用户密码，则 Citrix ADC 会使用模拟。模拟意味着 Citrix ADC 使用用户凭据来获取访问服务（例如 Secure Web）所需的票证。

所需配置：

- 配置 Citrix ADC 的“Worx”会话策略，使其能够从您的连接中识别 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 XenMobile 网关上的流量策略。
- 有关这些和其他配置详细信息，请参阅 Citrix 博客：WorxWeb 和 Kerberos 模拟 SSO。

Kerberos 约束委派

XenMobile 仅支持 Secure Web 的 Kerberos。当您为 Kerberos SSO 配置 Citrix ADC 时，如果 Citrix ADC 无法获取用户密码，则 Citrix ADC 会使用约束委派。

通过约束委派，Citrix ADC 使用指定的管理员帐户代表用户和服务获取票证。

所需配置：

- 在 Active Directory 中配置具有所需权限的 KCD 帐户，并在 Citrix ADC 上配置 KCD 帐户。
- 在 Citrix ADC 流量配置文件中启用 SSO。
- 配置后端网站以进行 Kerberos 身份验证。

表单填充身份验证

当您将 Citrix ADC 配置为基于表单的单点登录时，用户可以一次登录以访问网络中的所有受保护应用程序。此身份验证方法适用于使用安全浏览或完整 VPN 模式的应用程序。

所需配置：

- 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

如果您在会话配置文件中为 Web 应用程序启用 SSO，Citrix ADC 会自动执行摘要式 HTTP 身份验证。此身份验证方法适用于使用安全浏览或完整 VPN 模式的应用程序。

所需配置：

- 在 Citrix ADC 会话或流量配置文件中启用 SSO。

基本 HTTP 身份验证

如果您在会话配置文件中为 Web 应用程序启用 SSO，Citrix ADC 会自动执行基本 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 隧道或带 PAC 的完整 VPN 隧道

以下部分介绍了 Secure Web 的用户连接类型。有关更多信息，请参阅 Citrix 文档中的这篇 Secure Web 文章：配置用户连接。

完整 VPN 隧道

隧道连接到内部网络的连接可以使用完整 VPN 隧道。使用 Secure Web 首选 VPN 模式策略来配置完整 VPN 隧道。Citrix 建议对使用客户端证书或端到端 SSL 连接到内部网络中资源的连接使用完整 VPN 隧道。完整 VPN 隧道可处理任何基于 TCP 的协议。您可以将完整 VPN 隧道与 Windows、Mac、iOS 和 Android 设备配合使用。

在完整 VPN 隧道模式下，Citrix ADC 无法查看 HTTPS 会话内部。

安全浏览

隧道连接到内部网络的连接可以使用无客户端 VPN 的变体，称为安全浏览。安全浏览是 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 会话分解为两部分：

- 从客户端到 Citrix ADC
- 从 Citrix ADC 到后端资源服务器。

通过这种方式，Citrix ADC 可以完全查看客户端和服务器之间的所有事务，从而能够提供 SSO。

在安全浏览模式下使用 Secure Web 时，您还可以配置代理服务器。有关详细信息，请参阅博客 XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode。

带 PAC 的完整 VPN 隧道

您可以将代理自动配置 (PAC) 文件与 iOS 和 Android 设备上的 Secure Web 的完整 VPN 隧道部署配合使用。XenMobile 支持 Citrix ADC 提供的代理身份验证。PAC 文件包含定义 Web 浏览器如何选择代理以访问给定 URL 的规则。PAC 文件规则可以指定内部和外部站点的处理方式。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 不知道 PAC 文件或代理服务器。

对于 HTTPS 网站的身份验证：Secure Web MDX 策略**启用 Web 密码缓存**使 Secure Web 能够通过 MDX 对代理服务器进行身份验证并提供 SSO。

Citrix ADC 拆分隧道

在规划 SSO 和代理配置时，您还必须决定是否使用 Citrix ADC 拆分隧道。Citrix 建议仅在需要时使用 Citrix ADC 拆分隧道。本节高级概述了拆分隧道的工作原理：Citrix ADC 根据其路由表确定流量路径。当 Citrix ADC 拆分隧道开启时，Secure Hub 会区分内部（受保护）网络流量和 Internet 流量。Secure Hub 根据 DNS 后缀和 Intranet 应用程序做出该决定。然后，Secure Hub 仅通过 VPN 隧道传输内部网络流量。当 Citrix ADC 拆分隧道关闭时，所有流量都通过 VPN 隧道。

- 如果您出于安全考虑更倾向于监控所有流量，请禁用 Citrix ADC 分流。因此，所有流量都将通过 VPN 隧道。
- 如果您将完整 VPN 隧道与 PAC 结合使用，则必须禁用 Citrix Gateway 分流。如果分流已启用并且您配置了 PAC 文件，则 PAC 文件规则将覆盖 Citrix ADC 分流规则。在流量策略中配置的代理服务器不会覆盖 Citrix ADC 分流规则。

默认情况下，Secure Web 的**网络访问**策略设置为**隧道连接到内部网络**。通过此配置，MDX 应用程序将使用 Citrix ADC 分流设置。某些其他移动生产力应用程序的**网络访问**策略默认值有所不同。

Citrix Gateway 还具有微 VPN 反向分流模式。此配置支持 IP 地址排除列表，这些地址不会通过隧道连接到 Citrix ADC。相反，这些地址将通过设备互联网连接发送。有关反向分流的更多信息，请参阅 Citrix Gateway 文档。

XenMobile 包含一个**反向分流排除列表**。为防止某些网站通过 Citrix Gateway 进行隧道连接：添加一个逗号分隔的完全限定域名 (FQDN) 或 DNS 后缀列表，这些域名或后缀将改用 LAN 连接。此列表仅适用于配置了反向分流的 Citrix Gateway 的安全浏览模式。

身份验证

在 XenMobile® 部署中，决定如何配置身份验证时需要考虑多个因素。本节通过讨论以下内容，帮助您了解影响身份验证的各种因素：

- 与身份验证相关的主要 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。

本文还包括三个推荐配置示例，以提高安全性。

广义而言，更强的安全性会导致用户体验不佳，因为用户需要更频繁地进行身份验证。如何平衡这些问题取决于您组织的需要和优先级。通过审阅这三个推荐配置，您将更好地了解可用的身份验证措施之间的相互作用，以及如何最佳地部署您自己的 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，并脱机访问项目，例如下载的邮件、缓存的网站和笔记。

身份验证方法

单因素

LDAP： 您可以在 XenMobile 中配置与一个或多个目录（例如符合轻型目录访问协议 (LDAP) 的 Active Directory）的连接。这是一种常用的方法，用于为公司环境提供单点登录 (SSO)。您可以选择使用 Citrix PIN 和 Active Directory 密码缓存来改善 LDAP 的用户体验，同时仍在注册、密码过期和帐户锁定方面提供复杂密码的安全性。

有关更多详细信息，请参阅 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，以使用证书作为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。当使用客户端证书作为主要的身份验证方法时，在仅限客户端证书的环境中需要 Citrix PIN 来保护设备上的证书。

XenMobile 仅支持第三方证书颁发机构的证书吊销列表 (CRL)。如果配置了 Microsoft CA，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“启用 CRL 自动刷新”。此步骤可确保处于仅 MAM 模式的设备用户无法使用设备上的现有证书进行身份验证。XenMobile 会重新颁发新证书，因为它不限制用户在证书被吊销时生成用户证书。当 CRL 检查过期的 PKI 实体时，此设置可提高 PKI 实体的安全性。

有关计划为用户使用基于证书的身份验证或需要使用企业证书颁发机构 (CA) 颁发设备证书所需的部署图，请参阅本地部署参考体系结构。

双因素

LDAP + 客户端证书： 在 XenMobile 环境中，此配置是安全性与用户体验的最佳组合，具有最佳的 SSO 可能性，并结合了 Citrix ADC 提供的双因素身份验证安全性。同时使用 LDAP 和客户端证书可提供安全性，既有用户知道的信息（其 Active Directory 密码），也有他们拥有的信息（其设备上的客户端证书）。Secure Mail（以及其他一些移动生产力应用程序）可以自动配置并提供无缝的首次用户体验，通过客户端证书身份验证，并结合正确配置的 Exchange 客户端访问服务器环境。为了获得最佳可用性，您可以将此选项与 Citrix PIN 和 Active Directory 密码缓存结合使用。

LDAP + 令牌： 此配置允许使用 RADIUS 协议进行 LDAP 凭据的经典配置，以及一次性密码。为了获得最佳可用性，您可以将此选项与 Citrix PIN 和 Active Directory 密码缓存结合使用。

身份验证中涉及的重要策略、设置和客户端属性

以下策略、设置和客户端属性适用于以下三种推荐配置：

MDX 策略

应用程序密码： 如果设置为“**开**”，则在应用程序启动或在一段时间不活动后恢复时，需要 Citrix PIN 或密码才能解锁应用程序。默认值为“**开**”。

要为所有应用程序配置不活动计时器，请在 XenMobile 控制台的“**设置**”选项卡上的“**客户端属性**”中设置 INACTIVITY_TIMER 值（以分钟为单位）。默认值为 15 分钟。要禁用不活动计时器，以便仅在应用程序启动时显示 PIN 或密码提示，请将该值设置为零。

> **注意：**
>
> 如果为“加密密钥”策略选择了“安全脱机”，则此策略将自动启用。
>
> **需要在线会话：** 如果设置为“**开**”，则用户必须连接到企业网络并具有活动会话才能访问设备上的应用程序。如果设置为“**关**”，则无需活动会话即可访问设备上的应用程序。默认值为“**关**”。

最长脱机时间（小时）： 定义应用程序在不重新确认应用程序授权和从 XenMobile 刷新策略的情况下可以运行的最长时间。当您设置最长脱机时间时，如果适用于 iOS 的 Secure Hub 具有有效的 Citrix Gateway 令牌，则应用程序会从 XenMobile 检索 MDX 应用程序的新策略，而不会中断用户。如果 Secure Hub 没有有效的 Citrix ADC 令牌，则用户必须通过 Secure Hub 进行身份验证才能更新应用程序策略。Citrix ADC 令牌可能会因 Citrix Gateway 会话不活动或强制会话超时策略而失效。当用户再次登录 Secure Hub 时，他们可以继续运行应用程序。

在期限到期前 30、15 和 5 分钟，系统会提醒用户登录。到期后，应用程序将被锁定，直到用户登录。默认值为“**72 小时（3 天）**”。最短期限为 1 小时。

> **注意：**
>
> 请记住，在用户经常出差并可以使用国际漫游的情况下，默认的 72 小时（3 天）可能太短。
>
> **后台服务票证过期：** 后台网络服务票证保持有效的时间段。当 Secure Mail 通过 Citrix Gateway 连接到运行 ActiveSync 的 Exchange Server 时，XenMobile 会颁发一个令牌，Secure Mail 使用该令牌连接到内部 Exchange Server。此属性设置确定 Secure Mail 在无需新令牌进行身份验证和连接到 Exchange Server 的情况下可以使用该令牌的持续时间。当时间限制到期时，用户必须再次登录以生成新令牌。默认值为 **168 小时（7 天）**。当此超时到期时，邮件通知将停止。

需要在线会话的宽限期： 确定用户在“需要在线会话”策略阻止其进一步使用（直到在线会话得到验证）之前可以离线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：

- 如果您使用 MAM SDK：MAM SDK 概述
- 如果您使用 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：**
>
> 客户端属性是适用于连接到 XenMobile 的所有设备的全局设置。
>
> **Citrix PIN：** 为了获得简单的登录体验，您可以选择启用 Citrix PIN。使用 PIN，用户无需重复输入其他凭据，例如其 Active Directory 用户名和密码。您可以将 Citrix PIN 配置为仅限独立的离线身份验证，或者将 PIN 与 Active Directory 密码缓存结合使用，以简化身份验证，从而实现最佳可用性。您可以在 XenMobile 控制台的 **设置 > 客户端 > 客户端属性** 中配置 Citrix PIN。

以下是几个重要属性的摘要。有关详细信息，请参阅客户端属性。

ENABLE_PASSCODE_AUTH

显示名称： 启用 Citrix PIN 身份验证

此密钥允许您启用 Citrix PIN 功能。使用 Citrix PIN 或密码，系统会提示用户定义一个 PIN，以代替其 Active Directory 密码。如果启用了 **ENABLE_PASSWORD_CACHING** 或 XenMobile 正在使用证书身份验证，则必须启用此设置。

可能的值： **true** 或 **false**

默认值： **false**

ENABLE_PASSWORD_CACHING

显示名称：启用用户密码缓存

此密钥允许您将用户的 Active Directory 密码缓存在移动设备本地。当您将此密钥设置为 true 时，系统会提示用户设置 Citrix PIN 或密码。当您将此密钥设置为 **true** 时，必须将 **ENABLE_PASSCODE_AUTH** 密钥设置为 true。

可能的值： true 或 **false**

默认值： false

PASSCODE_STRENGTH

显示名称：PIN 强度要求

此密钥定义 Citrix PIN 或密码的强度。更改此设置后，下次系统提示用户进行身份验证时，会要求他们设置新的 Citrix PIN 或密码。

可能的值： 低、**中**或**高**

默认值： 中

INACTIVITY_TIMER

显示名称：非活动计时器

此密钥定义用户可将其设备置于非活动状态，然后访问应用程序而无需提示输入 Citrix PIN 或密码的分钟数。要为 MDX 应用程序启用此设置，必须将“**应用程序密码**”设置设为“**开**”。如果“**应用程序密码**”设置设为“**关**”，用户将被重定向到 Secure Hub 以执行完全身份验证。更改此设置后，该值将在下次系统提示用户进行身份验证时生效。默认值为 15 分钟。

ENABLE_TOUCH_ID_AUTH

显示名称： 启用触控 ID 身份验证

允许使用指纹读取器（仅限 iOS）进行离线身份验证。在线身份验证仍需要主要身份验证方法。

ENCRYPT_SECRETS_USING_PASSCODE

显示名称： 使用密码加密密钥

此密钥允许将敏感数据存储在移动设备上的秘密保管库中，而不是存储在基于平台的本机存储（例如 iOS 钥匙串）中。此配置密钥可实现密钥工件的强加密，但也会增加用户熵（只有用户知道的用户生成的随机 PIN 码）。

可能的值： true 或 **false**

默认值： false

Citrix ADC 设置

会话超时： 如果启用此设置，当 Citrix ADC 在指定时间间隔内未检测到网络活动时，Citrix Gateway 将断开会话连接。此设置对使用 Citrix Gateway 插件、Citrix Receiver™、Secure Hub 或通过 Web 浏览器连接的用户强制执行。默认值为 **1440 分钟**。如果将此值设置为零，则禁用此设置。

强制超时： 如果启用此设置，无论用户正在做什么，Citrix Gateway 都会在超时时间间隔到期后断开会话连接。当超时时间间隔到期时，用户无法采取任何操作来阻止断开连接。此设置对使用 Citrix Gateway 插件、Citrix Receiver、Secure Hub 或通过 Web 浏览器连接的用户强制执行。如果 Secure Mail 正在使用 STA（一种特殊的 Citrix ADC 模式），则**强制超时**设置不适用于 Secure Mail 会话。默认值为 **1440 分钟**。如果将此值留空，则禁用此设置。

有关 Citrix Gateway 中超时设置的详细信息，请参阅 Citrix ADC 文档。

有关提示用户通过在其设备上输入凭据向 XenMobile 进行身份验证的场景的详细信息，请参阅身份验证提示场景。

默认配置设置

这些设置是以下各项提供的默认值：

- 适用于 XenMobile 的 NetScaler® 向导
- MAM SDK 或 MDX 工具包
- XenMobile 控制台

设置	设置位置	默认设置
会话超时	Citrix 网关	1440 分钟
强制超时	思杰网关	1440 分钟
最长脱机时间	MDX 策略	72 小时
后台服务票证过期	MDX 策略	168 小时（7 天）
需要在线会话	MDX 策略	关
需要在线会话宽限期	MDX 策略	0
应用程序密码	MDX 策略	开
使用密码加密机密	XenMobile 客户端属性	否

设置	设置位置	默认设置
启用 Citrix PIN 身份验证	XenMobile 客户端属性	否
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	否
非活动计时器	XenMobile 客户端属性	15
启用触控 ID 身份验证	XenMobile 客户端属性	否

推荐配置

本节提供了三个 XenMobile 配置示例，这些配置的范围从最低安全性、最佳用户体验到最高安全性、更具侵入性的用户体验。这些示例应为您提供有用的参考点，以确定您希望将自己的配置置于哪个级别。修改这些设置可能还需要您更改其他设置。例如，最大离线时间必须始终小于会话超时。

最高安全性

此配置提供了最高级别的安全性，但存在显著的可用性权衡。

设置	设置位置	推荐设置	行为影响
会话超时	Citrix 网关	1440	用户仅在需要在线身份验证时（每 24 小时）输入其 Secure Hub 凭据。
强制超时	思杰网关	1440	每 24 小时严格要求在线身份验证。活动不会延长会话生命周期。
最长离线时间	MDX 策略	23	每天需要刷新策略。
后台服务票证过期	MDX 策略	72 小时	STA 超时，允许在没有 Citrix Gateway 会话令牌的情况下进行长时间会话。对于

			Secure Mail，将 STA 超时设置得比会话超时长，可以避免在会话过期前用户未打开应用程序时，邮件通知停止而没有提示用户的情况。
需要在线会话	MDX 策略	关闭	确保有效的网络连接和 Citrix Gateway 会话以使用应用程序。
需要在线会话的宽限期	MDX 策略	0	无宽限期（如果您启用了“需要在线会话”）。
应用程序密码	MDX 策略	开启	要求应用程序使用密码。
使用密码加密密钥	XenMobile 客户端属性	是	从用户熵派生的密钥可保护保管库。
启用 Citrix PIN 身份验证	XenMobile 客户端属性	是	启用 Citrix PIN 以简化身份验证体验。
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 是字母数字序列。
启用密码缓存	XenMobile 客户端属性	否	Active Directory 密码不缓存，Citrix PIN 用于离线身份验证。
不活动计时器	XenMobile 客户端属性	15	如果用户在此期间不使用 MDX 应用程序或 Secure Hub，则提示进行离线身份验证。

启用触控 ID 身份验证	XenMobile 客户端属性	否	在 iOS 中禁用触控 ID 以用于离线身份验证用例。

更高安全性

这是一种更折中的方法，此配置要求用户更频繁地进行身份验证（最多每 3 天一次，而不是 7 天），并提供更强的安全性。增加的身份验证次数会更频繁地锁定容器，从而确保设备不使用时的数据安全。

设置	设置位置	建议设置	行为影响
会话超时	Citrix 网关	4320	用户仅在需要在线身份验证时（每 3 天）输入其 Secure Hub 凭据。
强制超时	Citrix 网关	无值	如果有任何活动，会话将延长。
最长离线时间	MDX 策略	71	每 3 天需要刷新策略。小时差是为了允许在会话超时之前进行刷新。
后台服务票证过期	MDX 策略	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，将 STA 超时设置得比会话超时长，可以避免在会话过期前用户未打开应用程序时邮件通知停止而不提示用户的情况。
需要在线会话	MDX 策略	关	确保有效的网络连接和 Citrix Gateway 会话以使用应用程序。

需要在线会话的宽限期	MDX 策略	0	无宽限期（如果您启用了“需要在线会话”）。
应用程序密码	MDX 策略	开	要求应用程序使用密码。
使用密码加密机密	XenMobile 客户端属性	否	不需要用户熵来加密保管库。
启用 Citrix PIN 身份验证	XenMobile 客户端属性	是	启用 Citrix PIN 以简化身份验证体验。
PIN 强度要求	XenMobile 客户端属性	中等	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	是	用户 PIN 缓存并保护 Active Directory 密码。
不活动计时器	XenMobile 客户端属性	30	如果用户在此期间未使用 MDX 应用程序或 Secure Hub，则提示进行离线身份验证。
启用触控 ID 身份验证	XenMobile 客户端属性	是	在 iOS 中为离线身份验证用例启用触控 ID。

高安全性

此配置对用户而言最方便，可提供基本级别的安全性。

设置	设置位置	推荐设置	行为影响
会话超时	思杰网关	10080	用户仅在需要在线身份验证时（每 7 天）

			输入其 Secure Hub 凭据。
强制超时	思杰网关	无值	如果存在任何活动，会话将延长。
最长离线期限	MDX 策略	167	需要每周（每 7 天）刷新策略。小时差是为了允许在会话超时之前进行刷新。
后台服务票证过期	MDX 策略	240	STA 超时，允许长时间会话，无需 Citrix Gateway 会话令牌。对于 Secure Mail，将 STA 超时时间设置得比会话超时时间长，可以避免邮件通知在用户未在会话过期前打开应用程序的情况下停止，而无需提示用户。
需要在线会话	MDX 策略	关	确保有效的网络连接和 Citrix Gateway 会话以使用应用程序。
需要在线会话宽限期	MDX 策略	0	无宽限期（如果您启用了“需要在线会话”）。
应用程序密码	MDX 策略	开	要求应用程序使用密码。
使用密码加密机密	XenMobile 客户端属性	否	不要求用户熵来加密保管库。
启用 Citrix PIN 身份验证	XenMobile 客户端属性	是	启用 Citrix PIN 以简化身份验证体验。
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	是	用户 PIN 缓存并保护 Active Directory 密码。
不活动计时器	XenMobile 客户端属性	90	如果用户在此期间未使用 MDX 应用程序或 Secure Hub，则提示进行脱机身份验证。
启用触控 ID 身份验证	XenMobile 客户端属性	是	为 iOS 中的脱机身份验证用例启用触控 ID。

使用增强型身份验证

某些应用程序可能需要增强型身份验证（例如，辅助身份验证因素，如令牌或激进的会话超时）。您可以通过 MDX 策略控制此身份验证方法。此方法还需要一个单独的虚拟服务器来控制身份验证方法（在相同或不同的 Citrix ADC 设备上）。

设置	查找设置的位置	推荐设置	行为影响
备用思杰网关	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型身份验证。

如果用户打开一个登录到备用 Citrix Gateway 实例的应用程序，则所有其他应用程序都将使用该 Citrix Gateway 实例与内部网络通信。会话仅在增强安全性的 Citrix Gateway 实例会话超时后，才会切换回安全性较低的 Citrix Gateway 实例。

使用“需要在线会话”

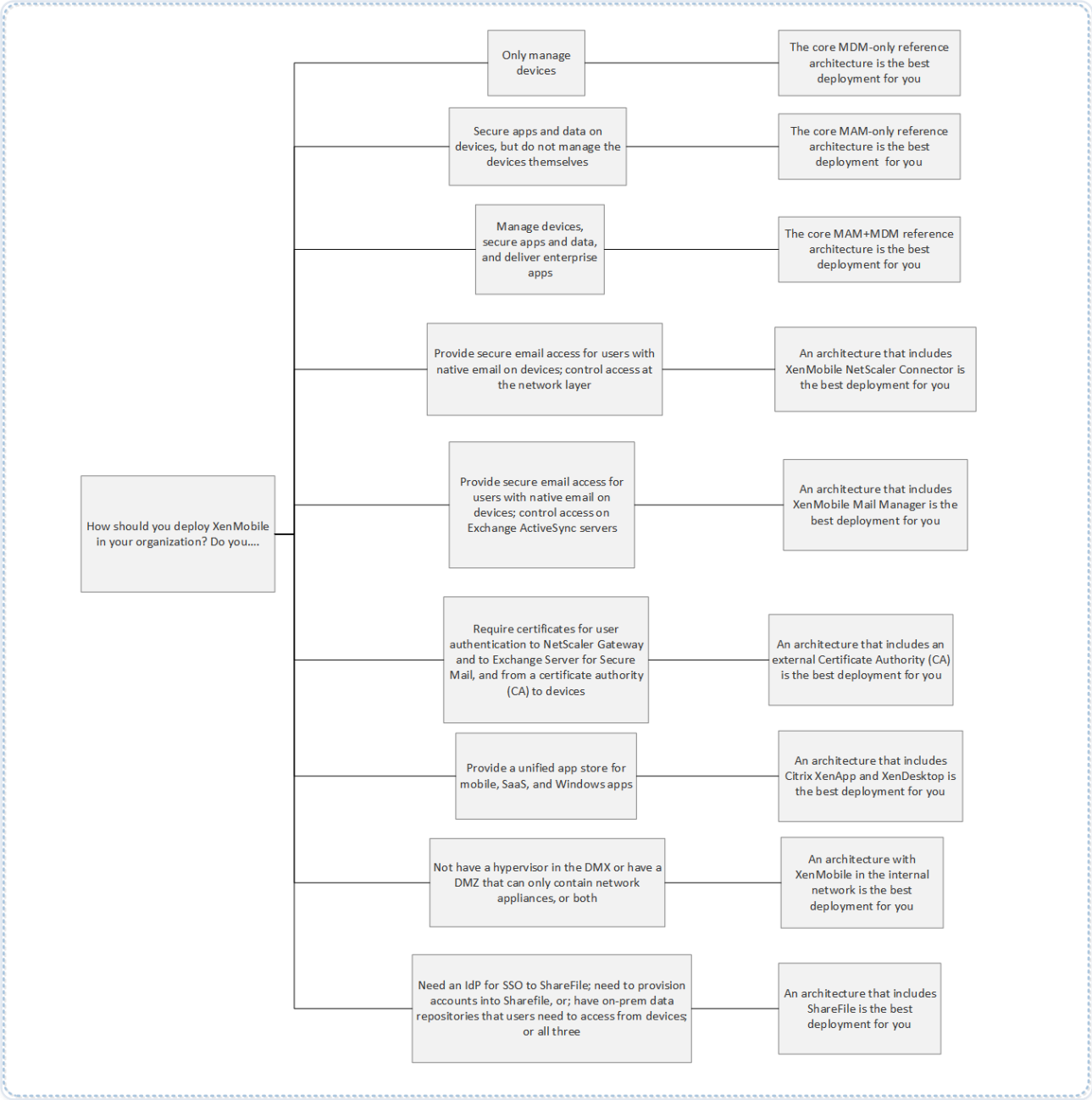
对于某些应用程序（例如 Secure Web），您可能希望确保用户仅在具有经过身份验证的会话且设备连接到网络时才运行应用程序。此策略强制执行该选项，并允许一个宽限期，以便用户可以完成其工作。

设置	设置位置	推荐设置	行为影响
需要在线会话	MDX 策略	开启	确保设备在线并具有有效的身份验证令牌。
在线会话要求宽限期	MDX 策略	15	允许 15 分钟的宽限期，之后用户将无法再使用应用程序。

本地部署的参考架构

本文中的图示说明了 XenMobile 本地部署的参考架构。部署方案包括仅 MDM、仅 MAM 和 MDM+MAM 作为核心架构，以及包含 SNMP 管理器、Citrix Gateway connector™ for Exchange ActiveSync、Endpoint Management connector for Exchange ActiveSync 和 Virtual Apps and Desktops 等组件的方案。这些图示显示了 XenMobile 所需的最小组件。

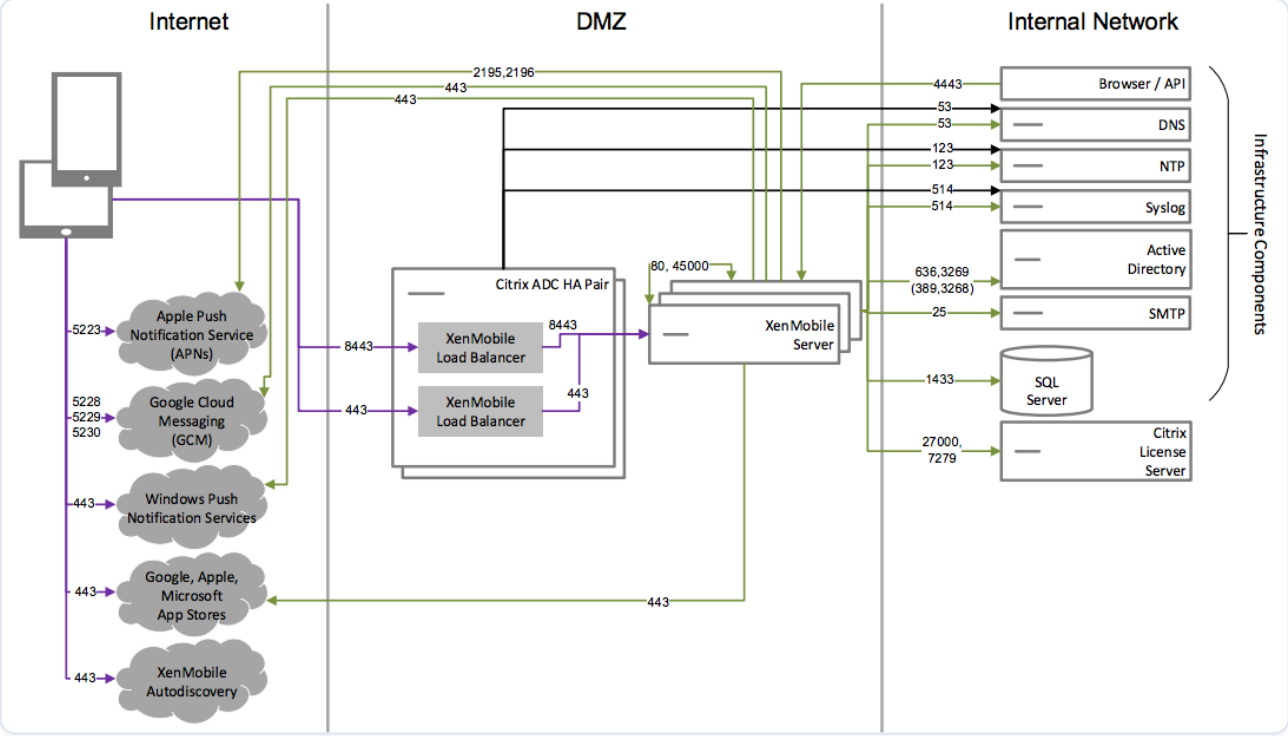
此图表可作为您部署决策的通用指南。



在图中，连接器上的数字表示您必须打开的端口，以允许组件之间建立连接。有关端口的完整列表，请参阅 XenMobile 文档中的端口要求。

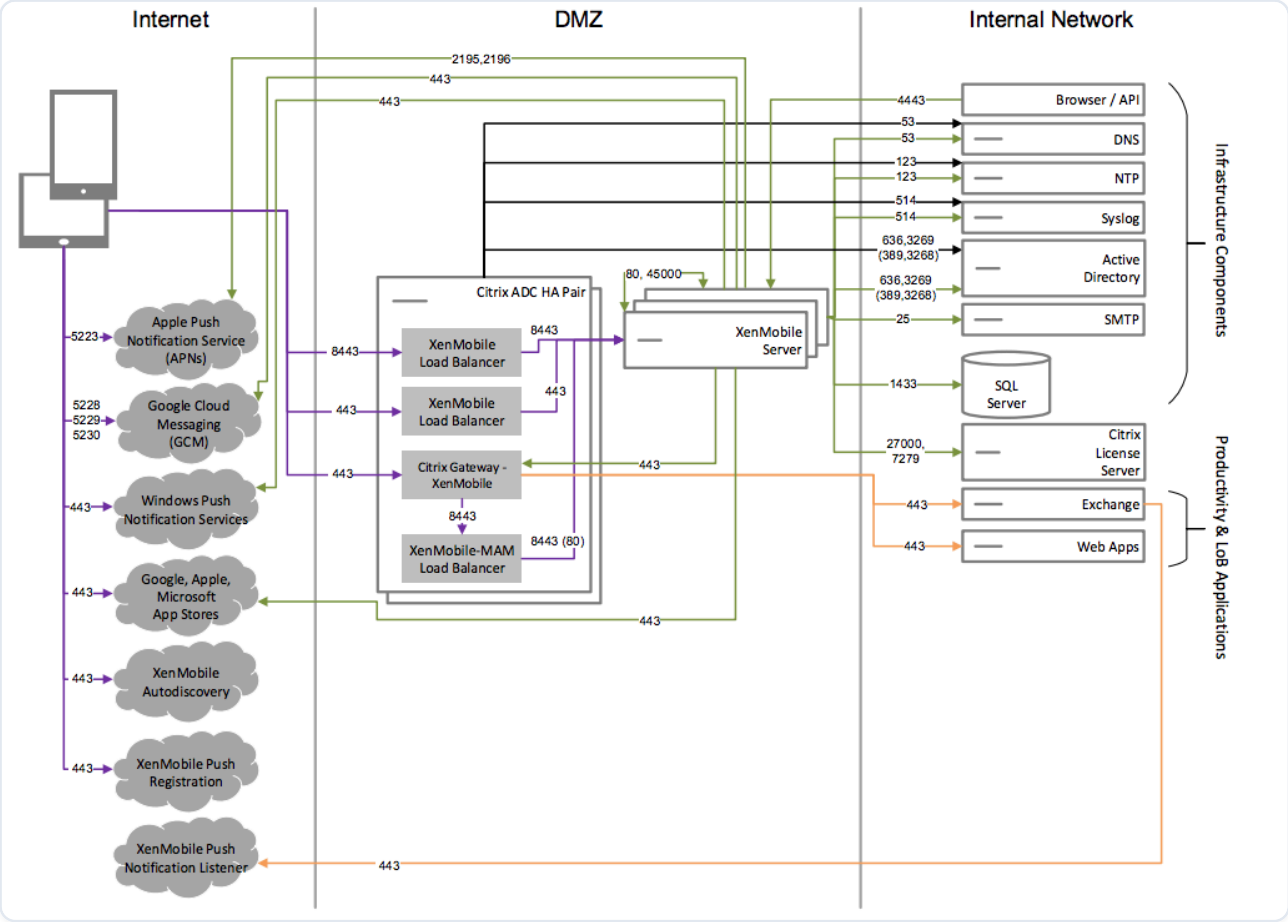
核心仅 MDM 参考架构

如果您计划仅使用 XenMobile 的 MDM 功能，请部署此架构。例如，您需要通过 MDM 管理公司发放的设备，以部署设备策略、应用程序并检索资产清单，并能够对设备执行操作，例如设备擦除。



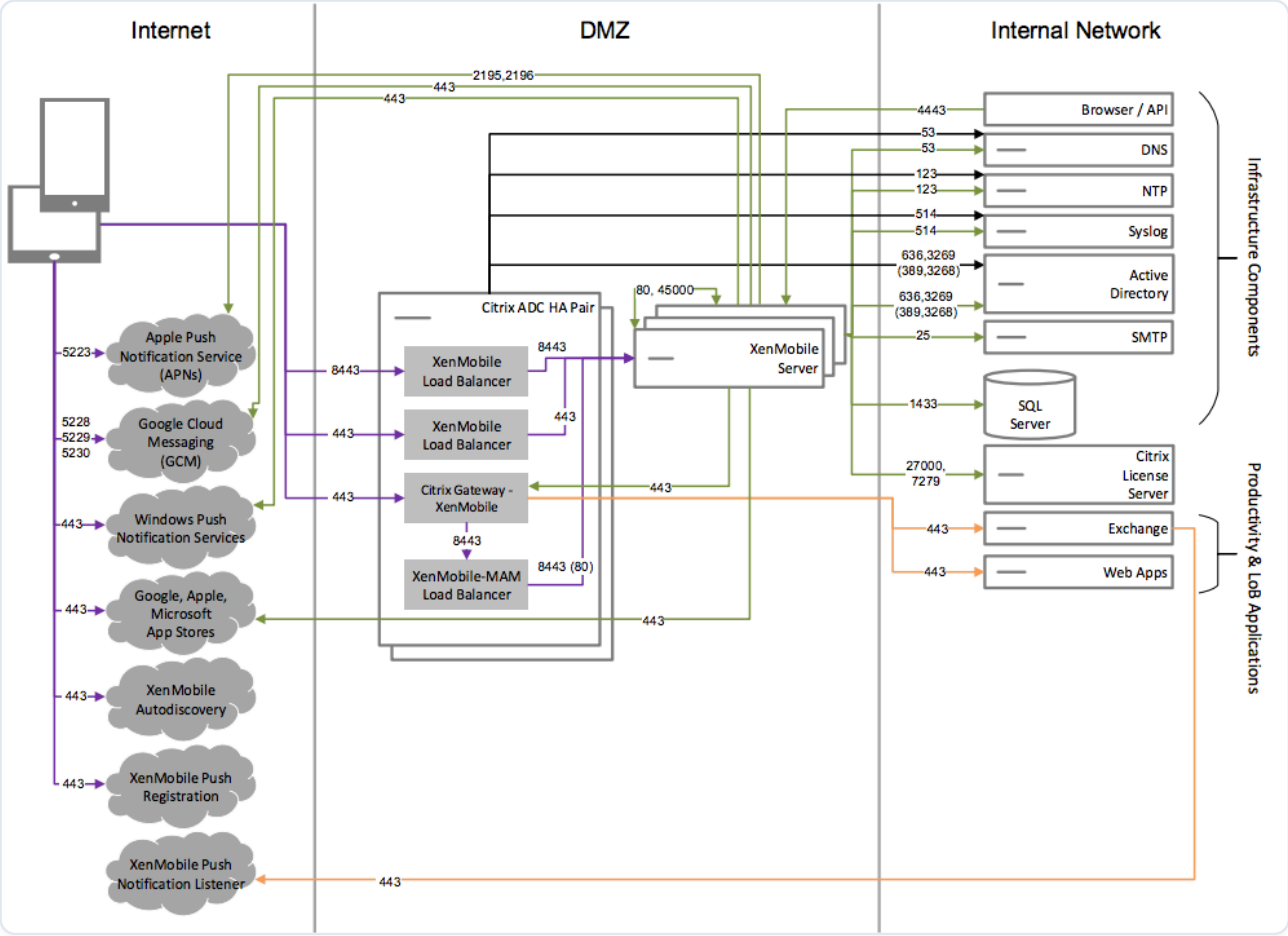
核心仅 MAM 参考架构

如果您计划仅使用 XenMobile 的 MAM 功能，而不让设备注册 MDM，请部署此架构。例如，您希望保护 BYO 移动设备上的应用程序和数据；您希望交付企业移动应用程序，并且可以锁定应用程序并擦除其数据。设备无法进行 MDM 注册。



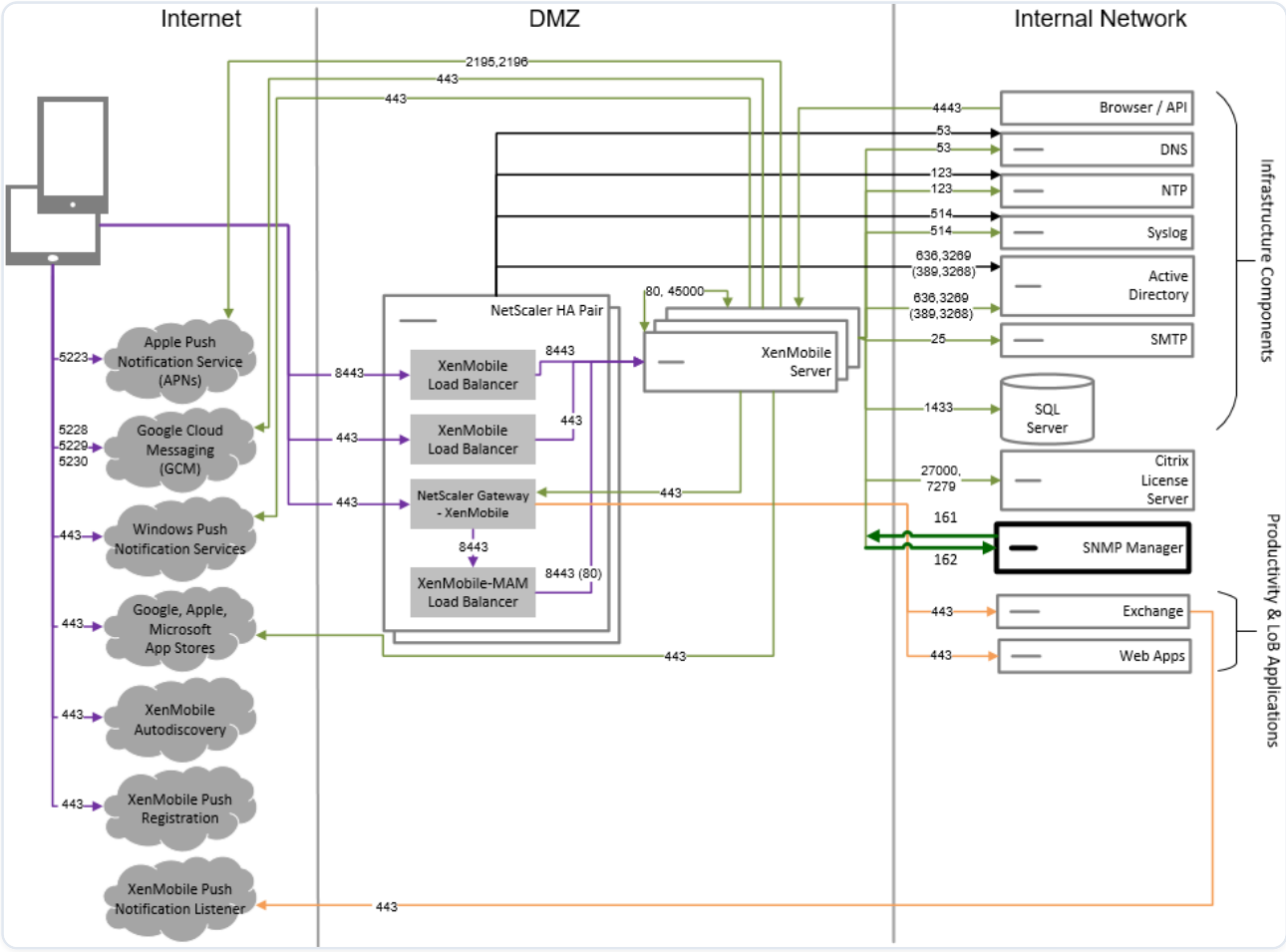
核心 MAM+MDM 参考架构

如果您计划使用 XenMobile 的 MDM+MAM 功能，请部署此架构。例如，您希望通过 MDM 管理公司发放的设备；您希望部署设备策略和应用程序，检索资产清单并可以擦除设备。您还希望交付企业移动应用程序，并且可以锁定应用程序并擦除设备上的数据。



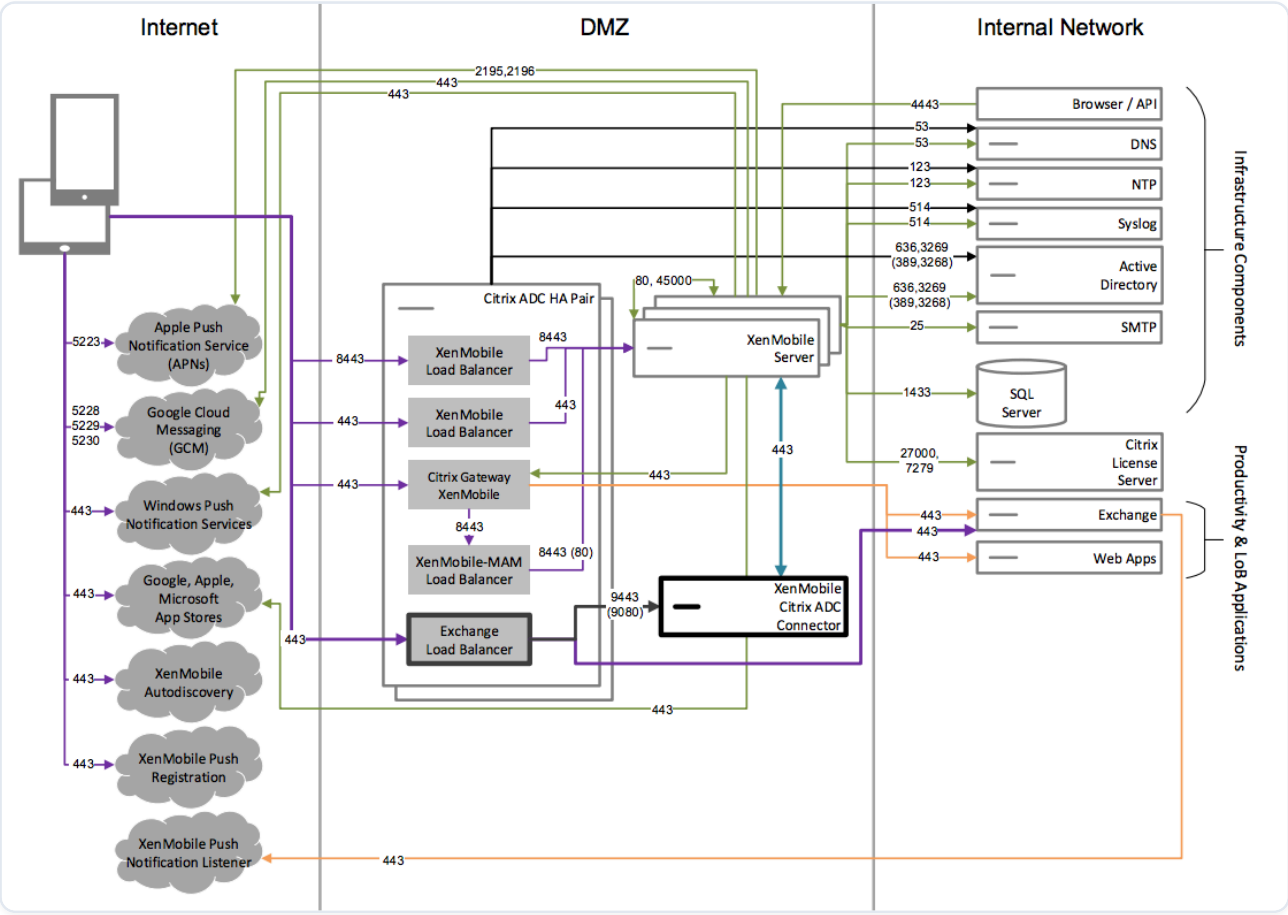
带 SNMP 的参考架构

如果您计划通过 XenMobile 启用 SNMP 监控，请部署此架构。例如，您希望允许监控系统查询并获取有关 XenMobile 节点的信息。有关详细信息，请参阅 SNMP 监控。



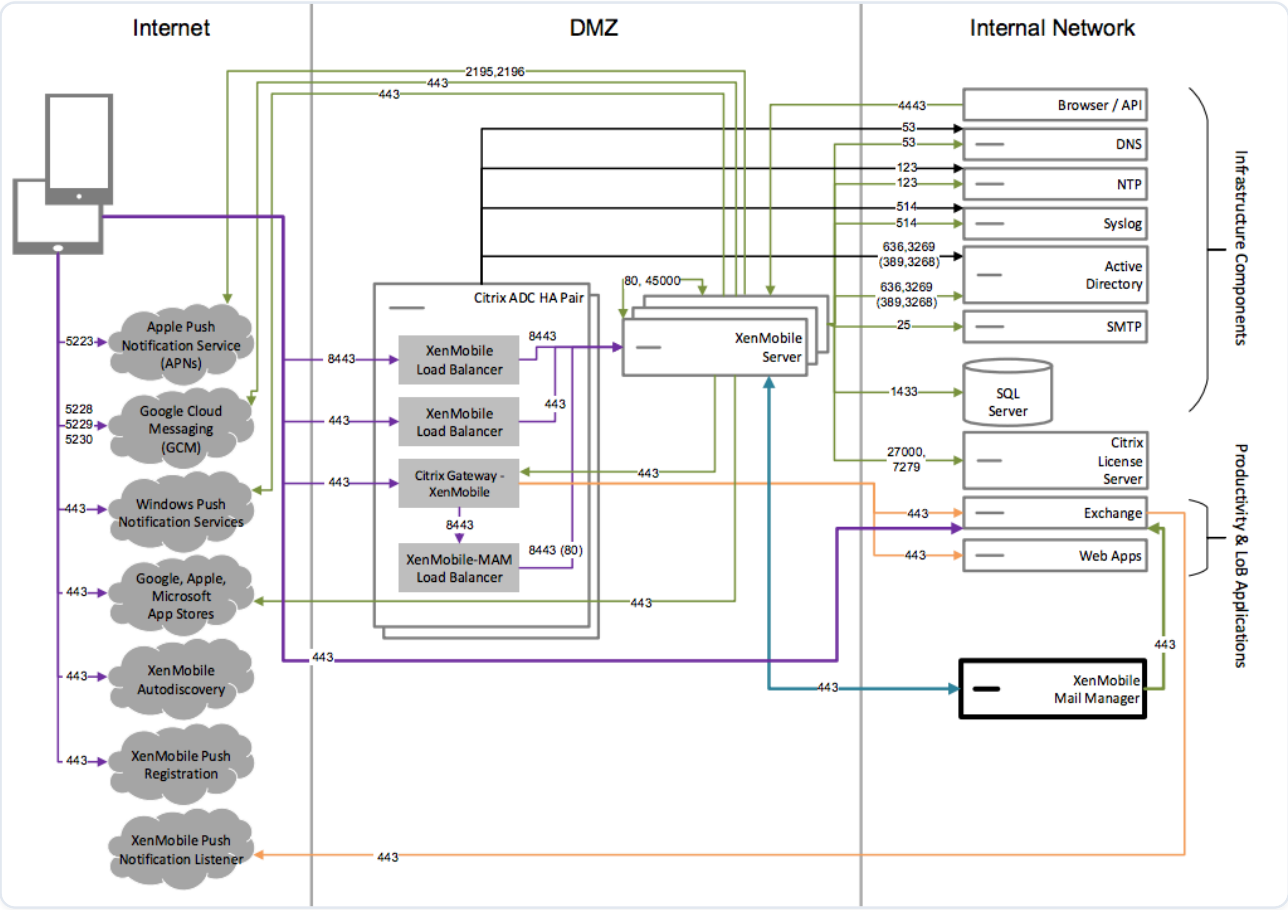
带 Citrix Gateway connector for Exchange ActiveSync 的参考架构

如果您计划将 Citrix Gateway connector for Exchange ActiveSync 与 XenMobile 结合使用，请部署此架构。例如，您需要为使用本机移动电子邮件应用程序的用户提供安全的电子邮件访问。这些用户将继续通过本机应用程序访问电子邮件，或者您可以随着时间的推移将他们过渡到 Citrix Secure Mail。访问控制需要在流量到达 Exchange Active Sync 服务器之前在网络层进行。尽管图中显示了在 MDM 和 MAM 架构中部署的 Exchange ActiveSync 连接器，但您也可以以相同的方式将其部署为仅 MDM 架构的一部分。



适用于 Exchange ActiveSync 的 Endpoint Management 连接器 参考架构

如果您计划将 Endpoint Management connector for Exchange ActiveSync 与 XenMobile 结合使用，请部署此架构。例如，您希望为使用本机移动电子邮件应用程序的用户提供安全的电子邮件访问。这些用户将继续通过本机应用程序访问电子邮件，或者您可以随着时间的推移将他们过渡到 Secure Mail。您可以在 Exchange ActiveSync 服务器上实现访问控制。尽管图中显示了在 MDM 和 MAM 架构中部署的 Endpoint Management connector for Exchange ActiveSync，但您也可以以相同的方式将其部署为仅 MDM 架构的一部分。

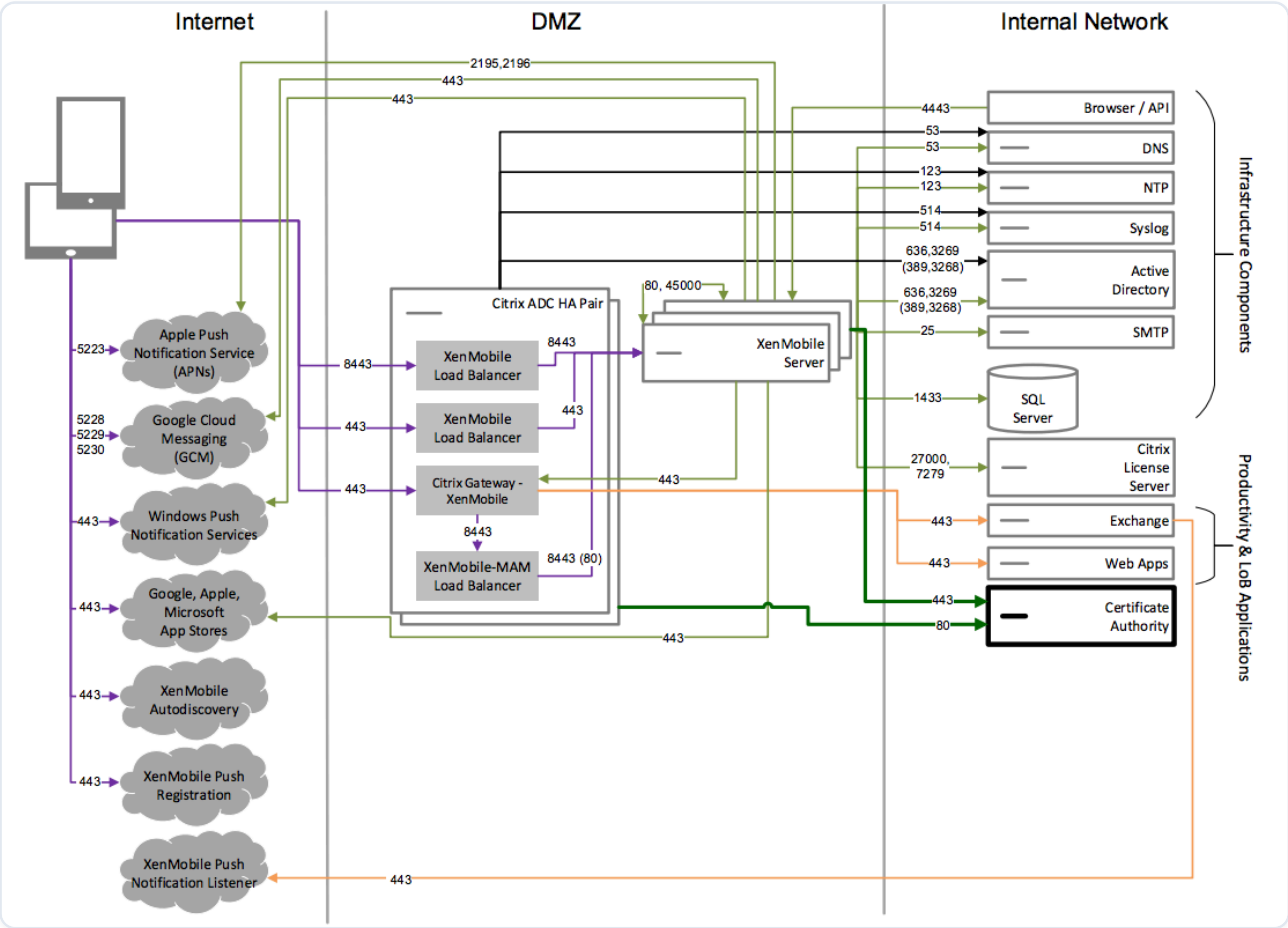


带外部证书颁发机构的参考架构

建议部署包含外部证书颁发机构的架构，以满足以下一个或多个要求：

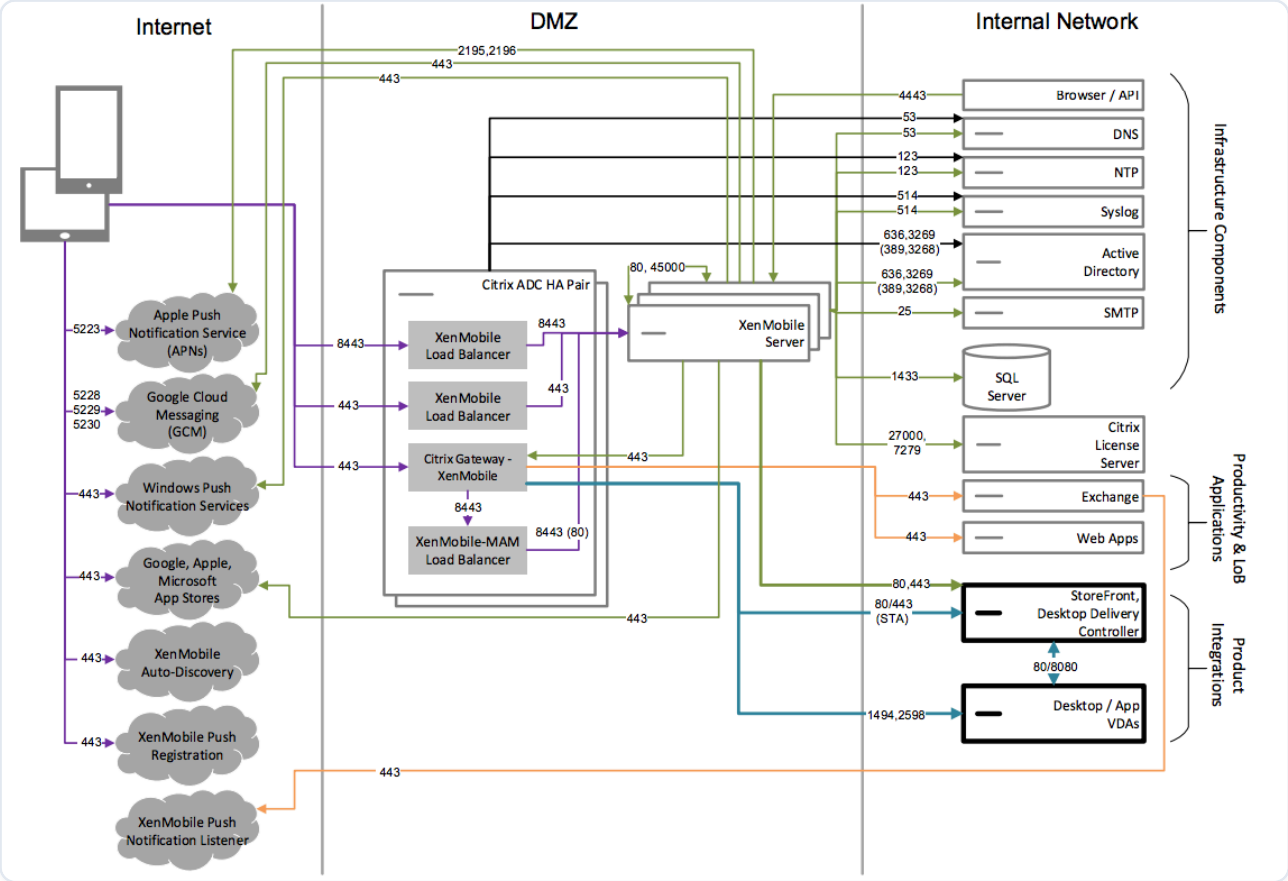
- 您需要用户证书才能对 Citrix Gateway 进行用户身份验证（用于内网访问）。
- 您需要 Secure Mail 用户使用用户证书对 Exchange Server 进行身份验证。
- 例如，您必须将企业证书颁发机构颁发的证书推送到移动设备以进行 Wi-Fi 访问。

尽管图中显示了在 MDM+MAM 架构中部署的外部证书颁发机构，但您也可以以相同的方式将其部署为仅 MDM 或仅 MAM 架构的一部分。



包含 Virtual Apps and Desktops 的参考架构

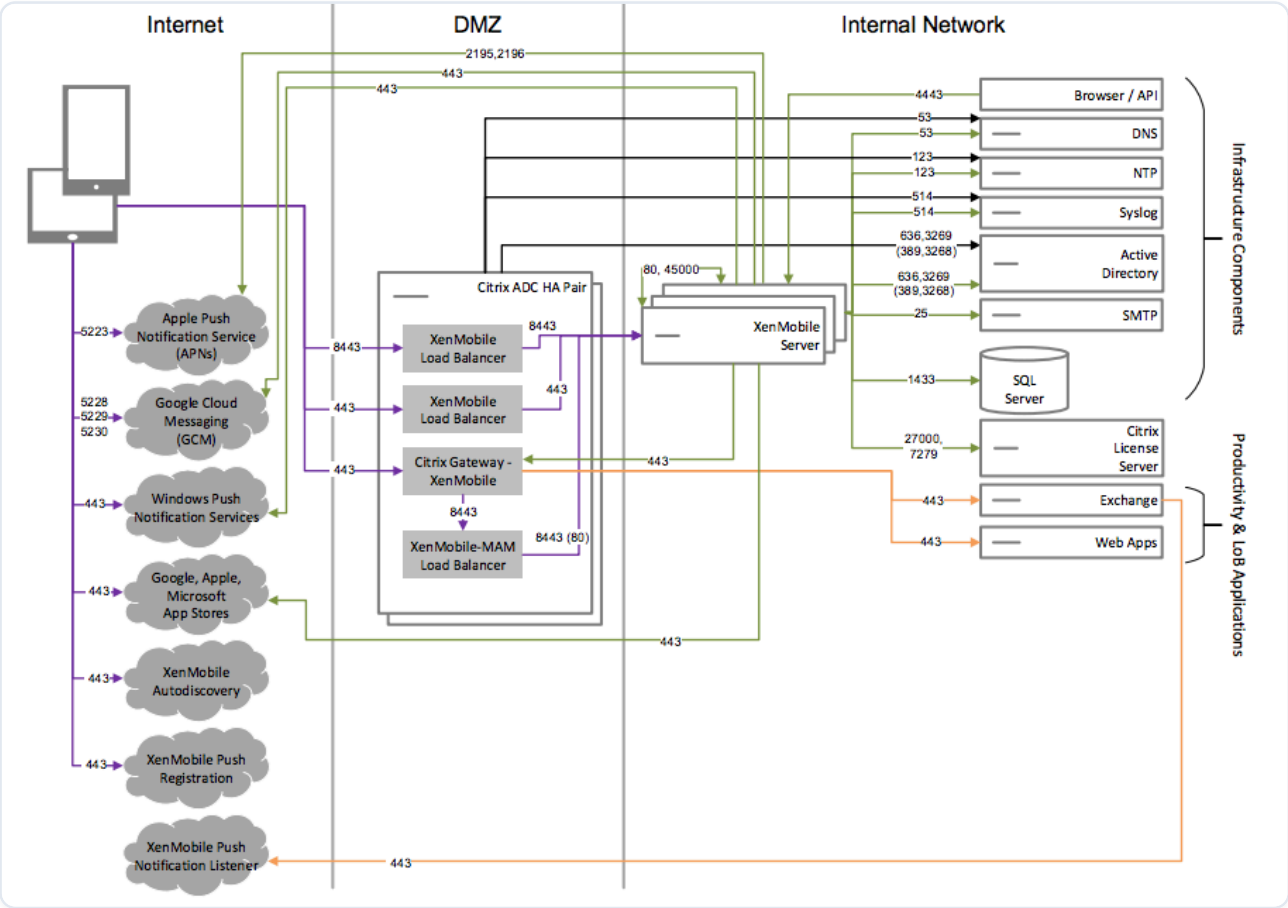
如果您计划将 Virtual Apps and Desktops 与 XenMobile 集成，请部署此架构。例如，您需要为移动用户提供一个统一的应用程序商店，以支持所有类型的应用程序（移动、SaaS 和 Windows）。尽管图表显示 Virtual Desktops 部署在 MDM 和 MAM 架构中，但您也可以以相同的方式将其部署为仅限 MAM 架构的一部分。



内部网络中包含 XenMobile 的参考架构

您可以在内部网络中部署包含 XenMobile 的架构，以满足以下一个或多个要求：

- 您在 DMZ 中没有或不允许拥有管理程序 (hypervisor)。
- 您的 DMZ 只能包含网络设备。
- 您的安全要求需要使用 SSL 卸载。



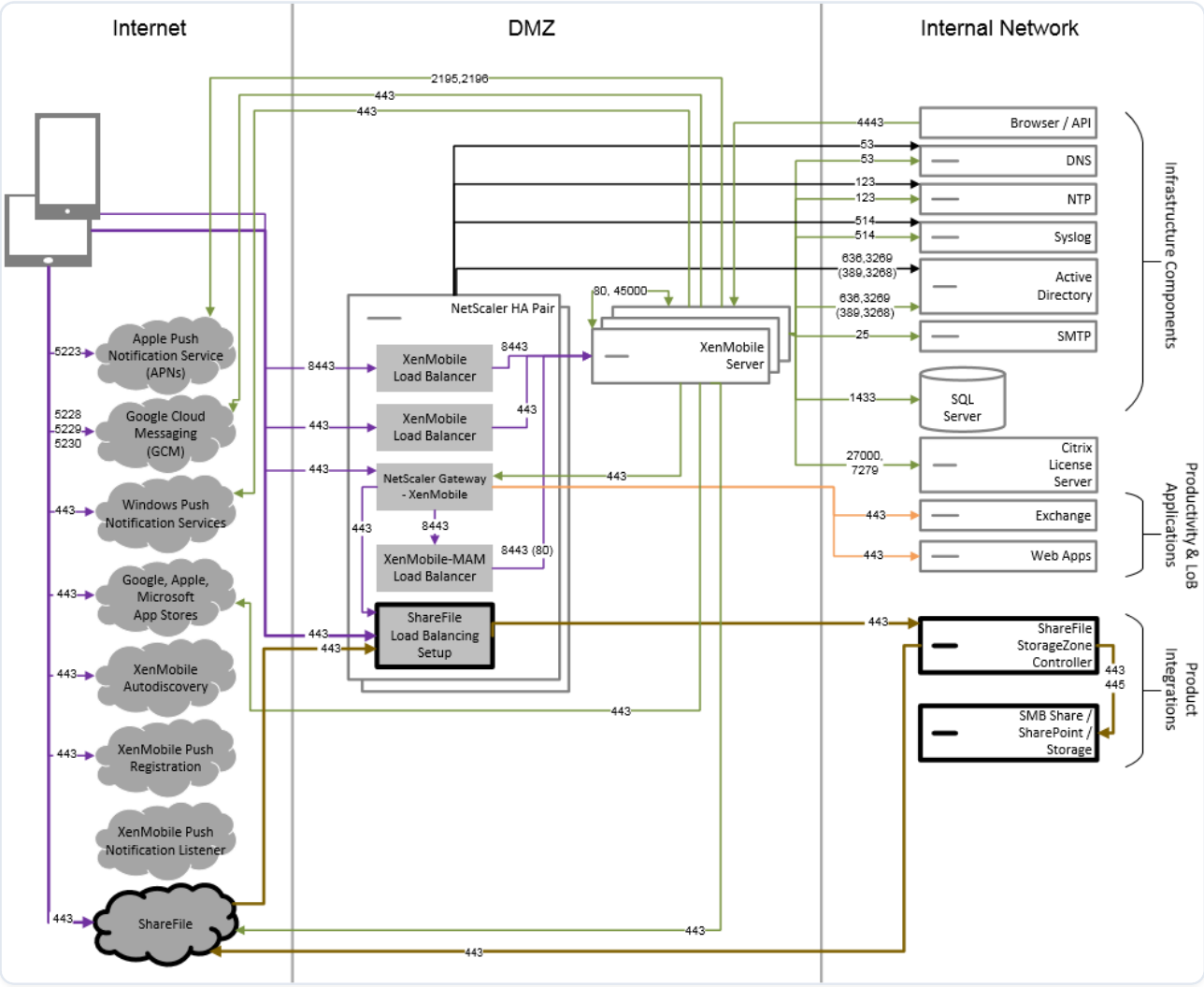
包含 ShareFile 的参考架构

如果您希望将 Citrix Files 或仅存储区域连接器与 XenMobile 集成，请部署此架构。Citrix Files 集成使您能够满足以下一个或多个要求：

- 您需要一个 IdP 来为用户提供对 ShareFile.com 的单点登录 (SSO)。
- 您需要一种将帐户预配到 ShareFile.com 的方法。
- 您拥有必须从移动设备访问的本地数据存储库。

仅与存储区域连接器集成可为用户提供对现有本地存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问。在此配置中，您无需设置 ShareFile 子域、将用户预配到 Citrix Files 或托管 Citrix Files 数据。

尽管此图显示 Citrix Files 部署在 MDM+MAM 体系结构中，但您也可以将 Citrix Files 以相同方式部署为仅限 MAM 体系结构的一部分。



服务器属性

服务器属性是全局属性，适用于整个 XenMobile® 实例中的操作、用户和设备。Citrix® 建议您评估本文中介绍的服务器属性是否适合您的环境。在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需要重新启动每个节点。XenMobile 会在需要重新启动时通知您。

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 `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 `false`，则 Android Enterprise 设备仅接收 Android Enterprise 应用程序。默认值为 `true`。

允许文件策略的文件扩展名： 使用逗号分隔的文件类型列表配置 `file.extension.allowlist`，管理员可以使用文件设备策略上传这些文件类型。即使您将以下文件类型添加到此允许列表中，也无法上传它们：

- .cab 文件

- .appx 文件
- .ipa 文件
- .apk 文件
- .xap 文件
- .mdx 文件
- .exe 文件

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,` 。

访问托管 Google Play 商店中的所有应用程序： 如果 `true`，XenMobile 会使公共 Google Play 商店中的所有应用程序都可从托管 Google Play 商店访问。将此属性设置为 `true` 允许所有 Android Enterprise 用户使用公共 Google Play 商店应用程序。管理员随后可以使用限制设备策略来控制对这些应用程序的访问。默认值为 `false`。

Android Enterprise 企业拥有设备上的工作配置文件注册：当 `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注册到企业拥有设备上的工作配置文件 (WPCOD) 模式。控制台会反映此注册模式的更改。如果设置为 `false`，则没有 WPCOD 设置可用。默认值为 `true`。

其他 Android Enterprise 限制设置：如果属性 `afw.restriction.policy.v2` 设置为 `true`，则以下限制设置可用于 Android Enterprise 设备：

- 允许卸载应用程序
- 允许蓝牙共享

有关这些设置的更多信息，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` 以启用限制设备策略中的应用于具有工作配置文件的完全托管设备/企业拥有设备上的工作配置文件设置。默认值为 `true`。有关此设置的更多信息，请参阅限制设备策略。

允许 iOS App Store 链接的主机名：属性 `ios.app.store.allowed.hostnames` 是在使用公共 API 将公共应用商店应用程序上传到服务器时使用的允许主机名列表。如果您计划使用公共 API 而不是通过服务器上传公共应用商店应用程序，请配置此属性。默认值为 `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`。

备用 APNs 端口：您可以使用端口 2197 而不是端口 443 从 `api.push.apple.com` 发送和接收 APNs 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 `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`，则可以创建使用弱密码的本地用户。默认值为 `true`。

阻止 Rooted Android 和越狱 iOS 设备注册：当此属性为 `true` 时，XenMobile 会阻止 Rooted Android 设备和越狱 iOS 设备的注册。默认值为 `true`。建议所有安全级别都设置为 `true`。

需要注册： `wsapi.mdm.required.flag` 仅在模式为 ENT 时适用，它指定是否要求用户注册 MDM。该属性适用于 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要强制要求 MDM。默认情况下，不需要注册。

当此属性为 `false` 时，用户可以拒绝注册，但仍可通过 XenMobile Store 访问其设备上的应用程序。当此属性为 `true` 时，任何拒绝注册的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此属性，则用户必须重新注册。

有关是否需要 MDM 注册的讨论，请参阅设备管理和 MDM 注册。

启用多模式注册：属性 `enable.multimode.xms` 允许您在一个 XenMobile Server 上创建注册配置文件，该配置文件控制 Android 和 iOS 设备的设备和应用程序管理的注册设置。此外，新的增强型注册配置文件功能支持 Android 专用设备的注册以及 Android 和 iOS 设备的仅 MAM 注册。当此属性为 `false` 时，设置注册配置文件时这些注册选项不可用。默认值为 `true`。如果将此属性更改为 `false`，则当此属性为 `true` 时注册的设备仍可正常工作。

启用自助服务门户： 如果 `shp.console.enable` 为 `false`，则会阻止访问自助服务门户。在端口 443 上导航到自助服务门户的用户会收到 404 错误。在端口 4443 上导航到门户的用户会收到“访问被拒绝”消息。如果 `true`，则通过端口 443 提供对自助服务门户的访问。默认为 `false`。

本地用户帐户锁定限制： 使用限制策略，您可以为 Active Directory 用户设置登录尝试次数限制。使用密钥 `local.user.account.lockout.limit` 对本地用户帐户执行相同的操作。用户尝试登录指定次数后，必须等待一段时间才能再次尝试。使用“**本地用户帐户锁定时间**”属性配置该时间。默认值为 `6`。

本地用户帐户锁定时间： 属性 `local.user.account.lockout.time` 允许您设置锁定本地用户帐户在再次尝试登录之前必须经过的分钟数。默认值为 `30` 分钟。

启用文件上传最大大小限制： 通过将 `max.file.size.upload.restriction` 设置为 `true` 来启用文件上传最大大小限制。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`。

允许的文件上传最大大小： 使用 `max.file.size.upload.allowed`，您可以为任何上传指定最大文件大小。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 在此分钟数后注销使用 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。超时值 `0` 意味着不活动用户保持登录状态。对于访问 API 的第三方应用程序，保持登录通常是必需的。默认值为 `5`。

iOS 设备管理注册（如果需要，安装根 CA）： Apple 最新的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 Apple Business Manager 或 Apple School Manager 中分配的服务器的 MDM 注册。但是，在 MDM 手动注册期间，iOS 设备用户在注册期间仅收到 MDM 设备证书提示。

为了在手动注册期间提供更好的用户体验，Citrix 建议将服务器属性 `ios.mdm.enrollment.installRootCaIfRequired` 更改为 **False**。默认值为 **True**。通过此更改，在 MDM 注册期间会打开一个 Safari 窗口，以简化用户的配置文件安装。

VPP 基线间隔： 属性 `vpp.baseline` 设置 XenMobile 从 Apple 重新导入批量购买许可证的最小间隔。刷新许可证信息可确保 XenMobile 反映所有更改，例如当您从批量购买中手动删除导入的应用程序时。默认情况下，XenMobile 至少每 `1440` 分钟刷新一次批量购买许可证基线。

如果您安装了许多批量购买许可证（例如，超过 50,000 个），Citrix 建议您增加基线间隔以减少导入许可证的开销。如果您预计 Apple 会频繁更改批量购买许可证，Citrix 建议您降低该值以使 XenMobile 保持最新状态。两个基线之间的最小间隔为 60 分钟。由于 cron 作业每 60 分钟运行一次，如果批量购买基线间隔为 60 分钟，则基线之间的间隔可能会延迟长达 119 分钟。

XenMobile MDM 自助服务门户控制台最大不活动间隔（分钟）： 此属性名称反映了较旧的 XenMobile 版本。该属性控制 XenMobile 控制台的最大不活动间隔。该间隔是 XenMobile 将不活动用户从 XenMobile 控制台注销的分钟数。超时值为 0 意味着不活动用户保持登录状态。默认值为 `30`。

已弃用对 Nexmo SMS 网关的支持： 属性 `deprecate.carrier.sms.gateway` 删除了对 Nexmo SMS 网关的支持，该网关默认设置为 **True**。Nexmo SMS 在自助服务门户中也已弃用。

已弃用对移动服务提供商 (MSP) 接口的支持： 属性 `deprecate.mobile.service.provider` 从控制台中删除了 MSP 接口，该接口默认设置为 **True**。

已弃用对 Windows 信息保护策略的支持： 根据 Windows 公告，已弃用对 Windows 信息保护 (WIP) 的支持。服务器属性 `windows.wip.deprecation` 删除了对 WIP 的支持，该属性默认设置为 **True**。

已弃用对 Android Enterprise 的“控制操作系统更新”策略中的“控制企业 FOTA”字段的支持： 如果属性 `afw.disable.osupdate.efota` 设置为 **True**，则 Android Enterprise 的“控制操作系统更新”策略中的“**控制企业 FOTA**”字段将被弃用。默认值设置为 **True**。

macOS 设备上的企业应用支持： 如果属性 `mac.app.push` 设置为 **True**，则企业应用在 macOS 设备上下载时会自动安装。默认值设置为 **True**。

iOS 设备上的 eSIM 支持： 如果属性 `ios.esim.support` 设置为 **True**，则 XenMobile Server 会从 iOS 设备获取 eSIM 信息，并在用户界面上显示 eSIM 相关的设备属性。

Android Enterprise 的 802.1x 设置中 Wi-Fi 策略对“域”字段的支持： 如果属性 `afw.network.domain.support` 设置为 **True**，则会在 **Android Enterprise 的 802.1x 设置**中添加 ***Domain*** 字段。

iOS 中可选应用的自动更新支持： 如果 `apple.ios.optional_app_update` 属性设置为 **True**，则从 Citrix Secure Hub 商店订阅的 iOS 可选应用也会自动更新。默认值设置为 **False**。

设备报告增强功能，用于“总应用部署尝试”和“前 100 个已安装应用”： 如果属性 `device.report.enhancement.enabled` 设置为 **True**，则会在“**总应用部署尝试**”中添加两个新列“**操作系统版本**”和“**设备型号**”，并添加新的设备报告“**前 100 个已安装应用**”以显示每个平台安装的前 100 个应用。

支持 iPhone 和 iPad 的“恢复服务”： 当属性 `ios.mdm.return.to.service` 设置为 **True** 时，您可以对运行 iOS 17 或更高版本的 iPhone 和 iPad 使用“恢复服务”功能。此属性的默认设置为 **True**。

Android Enterprise 的 VPN 策略中对始终开启 VPN 选项的支持： 如果属性 `afw.policy.vpn_always_on_lockdown` 设置为 **True**，则会在 Android Enterprise 平台的 **VPN** 策略中添加“**启用始终开启 VPN**”和“**启用锁定**”选项。默认值为 **True**。

Android Enterprise 选项策略中对始终开启 VPN 选项的弃用支持： 属性 `afw.policy.hide_vpn_always_on` 从 Android Enterprise 平台的 **XenMobile 选项**策略中删除了“**始终开启 VPN**”选项。默认值为 **True**。

旧版 MDX 弃用警报： 如果属性 `legacy.mdx.deprecation.alert` 设置为 **True**，则如果您发布了使用旧版 MDX 模式的 MDX 应用程序，XenMobile Server 控制台上会显示警报。默认值为 **True**。

支持 Firebase Cloud Messaging 迁移到使用新的 http v1 API： 如果属性 `afw.fcm.httpv1.migration` 设置为 **True**，则您可以使用新的 HTTP v1 API 的 Firebase Cloud Messaging。默认值为 **False**。

支持 iPhone 和 iPad 的“恢复服务”： 当属性 `ios.mdm.return.to.service` 设置为 **True** 时，您可以对运行 iOS 17 或更高版本的 iPhone 和 iPad 使用“恢复服务”功能。此属性的默认设置为 **True**。

支持从个人资料访问和使用工作资料电子邮件应用： 当 `afw.mailapp.crossworkprofile` 属性设置为 **True** 时，它会启用该功能，允许在 Android Enterprise 设置中从个人资料访问和使用工作资料电子邮件应用。默认值为 **True**。

支持在自动注册中强制执行最低操作系统版本以完成设置： 当 `ios.mdm.minimum_os_version.enrollment` 属性设置为 **True** 时，您可以强制要求在 iOS 17 或更高版本上自动注册期间完成设置的最低操作系统版本。默认值为 **True**。

支持 Samsung Knox 增强型认证 v3： 当 `afw.knox.attestation.v3` 属性设置为 **True** 时，您可以改进 Samsung Knox 设备上的安全功能。默认值为 **True**。

Android Enterprise 启用托管配置反馈： 如果 `afw.app_managed_configurations.feedback` 设置为 **True**，管理员可以从配置了托管配置策略的 Android 设备获取应用状态反馈。如果设置为 **False**，管理员将不会收到反馈。默认值为 **False**。

更新 Android Enterprise 托管配置反馈数据库的批处理大小： 如果 `android.managed.configuration.feedback.db.update.batch.size` 已设置，则它定义了更新 Android Enterprise 托管配置反馈数据库的批处理大小。该大小可根据数据库功能进行配置。默认值为 **100**，最大值为 **1000**。

Android Enterprise 托管配置反馈数据库更新时间间隔： 如果 `android.managed.configuration.feedback.db.update.time.interval` 已设置，则它定义了更新 Android Enterprise 托管配置反馈数据库的时间间隔。默认值为 **6** 小时。

强制执行 Android Enterprise 策略合规性： 如果 `afw.policy.compliance` 属性设置为 **True**，则在设备所有者模式下注册的 Android 设备允许管理员管理设备合规性。默认值为 **False**。

当 ABM 设备从 ABM MDM 服务器取消分配时，将其从 XMS 中删除： 如果 `remove.unassigned.abm.devices` 为 **true**，XMS 将删除不再分配给此服务器的设备。默认为 **false**。

支持基于证书身份验证的新强证书映射： 如果 `all_platforms.certificate.strong.mapping` 属性设置为 **True**，XenMobile Server 将支持来自 Microsoft 的新强证书映射。默认值为 **True**。

支持 Android Enterprise 设备上的 eSIM： 如果属性 `ae.esim.support` 设置为 **True**，则 XenMobile Server 会从 Android Enterprise 设备获取 eSIM 信息，并在用户界面上显示与 eSIM 相关的设备属性。默认值为 **True**。

支持声明式设备管理 (DDM)： 如果属性 `ios.mdm.declarative.management` 设置为 **True**，则 XenMobile Server 控制台允许您配置 iOS 声明式管理策略。默认值为 **False**。

支持 iOS 软件更新强制执行： 当属性 `ios.mdm.software.update.settings` 设置为 **True** 时，您可以在 XenMobile Server 控制台中配置软件更新强制执行设备策略。默认值为 **False**。

支持 Android Enterprise 设备上的自动启动应用程序： 当属性 `afw.launcher.auto_launch` 设置为 **True** 时，**自动启动应用程序**设置在启动器配置设备策略中适用于 Android Enterprise 设备。默认值为 **False**。

支持 iOS 27 DDM 策略： 当属性 `ios.mdm.ios27.ddm.support` 设置为 **True** 时，XenMobile Server 控制台允许您配置 iOS 27 中引入的 iOS 声明式管理策略。默认值为 **True**。

设备和应用策略

XenMobile® 设备和应用策略使您能够在以下因素之间优化平衡：

- 企业安全性
- 公司数据和资产保护
- 用户隐私
- 高效且积极的用户体验

这些因素之间的最佳平衡可能有所不同。例如，金融等高度受监管的组织比教育和零售等其他行业需要更严格的安全控制，在这些行业中，用户生产力是首要考虑因素。

您可以根据用户的身份、设备、位置和连接类型集中控制和配置策略，以限制对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。总体结果是一个既能提高员工满意度和生产力，又能确保安全性和管理控制的解决方案。

本文主要关注与安全性相关的多种设备和应用策略。

解决安全风险的策略

XenMobile 设备和应用策略可解决许多可能构成安全风险的情况，例如以下情况：

- 当用户尝试从不受信任的设备和不可预测的位置访问应用程序和数据时。
- 当用户在设备之间传递数据时。
- 当未经授权的用户尝试访问数据时。

- 当已离职的用户使用自己的设备 (BYOD) 时。
- 当用户放错设备时。
- 当用户必须始终安全地访问网络时。
- 当用户管理自己的设备并且您必须将工作数据与个人数据分开时。
- 当设备空闲并需要再次验证用户凭据时。
- 当用户将敏感内容复制并粘贴到未受保护的电子邮件系统时。
- 当用户在同时包含个人账户和公司账户的设备上接收带有敏感数据的电子邮件附件或网页链接时。

这些情况与保护公司数据时的两个主要关注领域有关，即数据处于以下状态时：

- 静态
- 传输中

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 通过 Citrix MAM SDK 提供的合规性检查等功能补充了基于平台的加密。

XenMobile 中的移动应用程序管理 (MAM) 功能可实现对移动生产力应用程序、启用 MDX 的应用程序及其相关数据的全面管理、安全和控制。

移动应用程序 SDK 通过使用 Citrix MDX 应用程序容器技术，为 XenMobile 部署启用应用程序。容器技术将用户设备上的公司应用程序和数据与个人应用程序和数据分开。数据分离使您能够通过全面的基于策略的控制来保护任何自定义开发、第三方或 BYO 移动应用程序。

XenMobile 还包括应用程序级加密。XenMobile 独立加密存储在任何启用 MDX 的应用程序中的数据，而无需设备密码，也无需您管理设备来强制执行策略。

策略和移动应用程序 SDK 使您能够：

- 在安全的移动容器中分离业务和个人应用及数据。
- 使用加密和其他移动数据丢失防护 (DLP) 技术保护应用。

MDX 策略提供了许多操作控制。您可以实现已启用 MAM SDK 或 MDX 封装的应用之间的无缝集成，同时控制所有通信。通过这种方式，您可以强制执行策略，例如确保数据只能由已启用 MAM SDK 或 MDX 封装的应用访问。

除了设备和应用策略控制之外，保护静态数据的最佳方法是加密。XenMobile 为存储在 MDX 启用应用中的任何数据添加了一层加密，使您能够对公共文件加密、私有文件加密和加密排除等功能进行

策略控制。移动应用 SDK 使用符合 FIPS 140-2 标准的 AES 256 位加密，密钥存储在受保护的 Citrix Secret Vault 中。

XenMobile 如何保护传输中的数据

在用户移动设备和内部网络之间传输的数据称为传输中的数据。MDX 应用容器技术通过 Citrix Gateway 提供对内部网络的特定于应用的 VPN 访问。

考虑以下情况：员工希望从移动设备访问安全企业网络中的以下资源：

- 公司电子邮件服务器
- 托管在公司内网上的启用 SSL 的 Web 应用程序
- 存储在文件服务器或 Microsoft SharePoint 上的文档

MDX 通过特定于应用的微型 VPN 允许从移动设备访问所有这些企业资源。每个设备都有自己专用的微型 VPN 隧道。

微型 VPN 功能不需要设备范围的 VPN，因为设备范围的 VPN 可能会损害不受信任的移动设备上的安全性。因此，内部网络不会暴露于可能感染整个公司系统的恶意软件或攻击。公司移动应用和个人移动应用可以在一台设备上共存。

为了提供更强的安全级别，您可以为 MDX 启用应用配置备用 Citrix Gateway 策略，该策略用于身份验证以及与应用的微型 VPN 会话。您可以将备用 Citrix Gateway 与“需要在线会话”策略结合使用，以强制应用重新向特定网关进行身份验证。此类网关通常具有不同的（更高保证）身份验证要求和流量管理策略。

除了安全功能之外，微型 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：

- 仅传输最少量的数据
- 传输以尽可能快的速度完成。速度可改善用户体验，这是移动设备普及的关键成功因素。

定期重新评估您的设备策略，例如在以下情况中：

- 当新版本 XenMobile 因设备操作系统更新的发布而包含新的或更新的策略时
- 添加设备类型时：

  尽管许多策略对所有设备通用，但每种设备都有一组特定于其操作系统的策略。因此，您可能会发现 iOS、Android 和 Windows 设备之间存在差异，甚至不同制造商的 Android 设备之间也存在差异。
- 使 XenMobile 操作与企业或行业变化（例如新的公司安全策略或合规性法规）保持同步
- 当新版本 MAM SDK 包含新的或更新的策略时

- 添加或更新应用程序时
- 由于新应用程序或新要求，为用户集成新工作流

应用程序策略和用例场景

尽管您可以选择通过 Secure Hub 提供哪些应用程序，但您可能还需要定义这些应用程序如何与 XenMobile 交互。使用应用程序策略：

- 如果您希望用户在经过一定时间后进行身份验证。
- 如果您希望为用户提供脱机访问其信息。

以下部分包括一些策略和用法示例。

- 有关您可以使用 MAM SDK 集成到您的 iOS 和 Android 应用程序中的第三方策略列表，请参阅 MAM SDK 概述。
- 有关每个平台的 MDX 策略列表，请参阅 MDX 策略一览。

身份验证策略

- **设备密码**

  为何使用此策略： 启用设备密码策略，以强制用户仅在设备启用了设备密码的情况下才能访问 MDX 应用程序。此功能可确保在设备级别使用 iOS 加密。

  用户示例： 启用此策略意味着用户必须在其 iOS 设备上设置密码，然后才能访问 MDX 应用程序。

- **应用程序密码**

  为何使用此策略： 启用应用程序密码策略，以使 Secure Hub 在用户打开应用程序并访问数据之前提示用户对托管应用程序进行身份验证。用户可以使用其 Active Directory 密码、Citrix PIN 或 iOS TouchID 进行身份验证，具体取决于您在 XenMobile Server 设置的客户端属性中配置的内容。您可以在客户端属性中设置不活动计时器，以便在持续使用的情况下，Secure Hub 不会在计时器到期之前再次提示用户对托管应用程序进行身份验证。

  应用程序密码与设备密码不同之处在于，当设备密码策略推送到设备时，Secure Hub 会提示用户配置密码或 PIN，用户必须解锁此密码或 PIN 才能在打开设备或不活动计时器到期时访问其设备。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，如果非活动期已过期，用户必须输入其 Citrix PIN 才能浏览网站。

- **需要联机会话**

为何使用此策略： 如果应用程序需要访问 Web 应用程序（Web 服务）才能运行，请启用此策略，以便 XenMobile 提示用户连接到企业网络或在使用应用程序之前拥有活动会话。

用户示例： 当用户尝试打开已启用“需要联机会话”策略的 MDX 应用程序时，他们无法使用该应用程序，直到他们使用蜂窝网络或 Wi-Fi 服务连接到网络。

- **最长脱机时间**

  为何使用此策略： 使用此策略作为附加安全选项，以确保用户无法在长时间脱机运行应用程序，而无需重新确认应用程序授权并从 XenMobile 刷新策略。

  用户示例： 如果您为 MDX 应用程序配置了最长脱机时间，用户可以脱机打开和使用该应用程序，直到脱机计时器期限到期。届时，用户必须通过蜂窝网络或 Wi-Fi 服务重新连接到网络，并在出现提示时重新进行身份验证。

杂项访问策略

- **应用程序更新宽限期（小时）**

  为何使用此策略： 应用程序更新宽限期是指用户必须更新 XenMobile Store 中发布了新版本的应用程序之前可用的时间。到期时，用户必须更新应用程序才能访问应用程序中的数据。设置此值时，请记住您的移动员工的需求，特别是那些在国际旅行时可能长时间离线的员工。

  用户示例： 您在 XenMobile Store 中加载了新版本的 Secure Mail，然后将应用程序更新宽限期设置为 6 小时。所有 Secure Mail 用户都会看到一条消息，要求他们更新 Secure Mail 应用程序，直到 6 小时到期。6 小时到期后，Secure Hub 会将用户路由到 XenMobile Store。

- **活动轮询周期（分钟）**

  为何使用此策略： 活动轮询周期是 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“活动轮询周期”策略设置为 60 分钟，则当您从 XenMobile 向设备发送应用程序锁定命令时，锁定会在上次轮询发生后的 60 分钟内发生。

不合规设备行为策略

当设备低于最低合规性要求时，“不合规设备行为”策略允许您选择要执行的操作。有关信息，请参阅不合规设备行为。

应用程序交互策略

为何使用这些策略： 使用应用程序交互策略来控制文档和数据从 MDX 应用程序到设备上其他应用程序的流动。例如，您可以阻止用户将数据移动到容器外部的个人应用程序，或者阻止用户将容器外部的数据粘贴到容器化应用程序中。

用户示例： 您将应用程序交互策略设置为“受限”，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个人 Safari 或 Chrome 浏览器。此外，用户可以将 Secure Mail 中的附件文档打开到 Citrix Files 或 Quick Edit 中，但不能在容器外部的个人文件查看应用程序中打开附件文档。

应用程序限制策略

为何使用这些策略： 使用应用程序限制策略来控制用户在 MDX 应用程序打开时可以访问哪些功能。这有助于确保在应用程序运行时不会发生恶意活动。应用程序限制策略在 iOS 和 Android 之间略有不同。例如，在 iOS 中，您可以在 MDX 应用程序运行时阻止访问 iCloud。在 Android 中，您可以在 MDX 应用程序运行时停止使用 NFC。

用户示例： 如果您在 MDX 应用程序中启用应用程序限制策略以阻止 iOS 上的听写功能，则用户在 MDX 应用程序运行时无法使用 iOS 键盘上的听写功能。因此，用户听写的数据不会传递给不安全的第三方云听写服务。当用户在容器外部打开其个人应用程序时，听写选项仍可供用户用于其个人通信。

应用程序网络访问策略

为什么要使用这些策略： 使用应用程序网络访问策略，可让设备上容器中的 MDX 应用程序访问公司网络内部的数据。对于网络访问策略，请将**隧道连接到内部网络**选项设置为自动从 MDX 应用程序通过 Citrix ADC 到后端 Web 服务或数据存储的微 VPN。

用户示例： 当用户打开启用了隧道功能的 MDX 应用程序（例如 Secure Web）时，浏览器会打开并启动内部网站点，而无需用户启动 VPN。Secure Web 应用程序使用微 VPN 技术自动访问内部站点。

应用程序地理位置和地理围栏策略

为什么要使用这些策略： 控制应用程序地理位置和地理围栏的策略包括中心点经度、中心点纬度和半径。这些策略将 MDX 应用程序中的数据访问限制在特定的地理区域。这些策略通过经纬度坐标的半径定义地理区域。如果用户尝试在定义的半径之外使用应用程序，则该应用程序将保持锁定状态，用户无法访问应用程序数据。

用户示例： 用户可以在其办公地点访问并购数据。当他们离开办公地点时，这些敏感数据将变得不可访问。

Secure Mail 应用程序策略

- **后台网络服务**

  为什么要使用此策略： Secure Mail 中的后台网络服务使用安全票证授权 (STA)，它实际上是一个 SOCKS5 代理，用于通过 Citrix Gateway 进行连接。与微 VPN 相比，STA 支持长时间连接

并提供更好的电池续航时间。因此，STA 非常适合需要持续连接的邮件。Citrix 建议您为 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： 如果未启用 STA，当 Android 用户打开 Secure Mail 时，系统会提示他们打开 VPN，该 VPN 会在设备上保持打开状态。如果启用了 STA，当 Android 用户打开 Secure Mail 时，Secure Mail 会无缝连接，无需 VPN。

- **默认同步间隔**

  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 的默认邮件天数。两周的邮件同步时间比 3 天长，会延长用户的设置过程。

  用户示例： 如果用户首次设置 Secure Mail 时默认同步间隔设置为 3 天，他们可以在收件箱中看到从现在到过去 3 天内收到的所有电子邮件。如果用户想查看 3 天前的电子邮件，他们可以进行搜索。Secure Mail 会显示存储在服务器上的旧电子邮件。安装 Secure Mail 后，每个用户都可以更改此设置以更好地满足其需求。

设备策略和用例行为

设备策略（有时称为 MDM 策略）决定了 XenMobile 如何与设备配合使用。尽管许多策略适用于所有设备，但每种设备都有一组特定于其操作系统的策略。以下列表包含一些设备策略，并讨论了如何使用它们。有关所有设备策略的列表，请参阅 设备策略 下的文章。

- **应用程序清单策略**

  为何使用此策略： 如果您必须查看用户安装的应用程序，请将应用程序清单策略部署到设备。如果您不部署应用程序清单策略，则只能看到用户从 XenMobile Store 安装的应用程序，而看不到任何个人安装的应用程序。如果您想阻止某些应用程序在公司设备上运行，则必须使用此策略。

  用户示例： 拥有 MDM 管理设备的用户无法禁用此功能。用户的个人安装应用程序对 XenMobile 管理员可见。

- **应用程序锁定策略**

  为何使用此策略： 适用于 Android 的应用程序锁定策略允许您阻止或允许应用程序。例如，通过允许应用程序，您可以配置自助服务终端设备。通常，您仅将应用程序锁定策略部署到公司拥有的设备，因为它限制了用户可以安装的应用程序。您可以设置一个覆盖密码，以向用户提供对被阻止应用程序的访问权限。

  用户示例： 假设您部署了一个阻止 Angry Birds 应用程序的应用程序锁定策略。用户可以从 Google Play 安装 Angry Birds 应用程序，但当他们打开该应用程序时，会收到一条消息，告知他们管理员已阻止该应用程序。

- **连接计划策略**

  为何使用此策略： 您必须使用连接计划策略，以便 Windows Mobile 设备可以连接回 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：

  - **始终：** 永久保持连接活动。Citrix 建议使用此选项以优化安全性。当您选择**始终**时，还要使用连接计时器策略以确保连接不会耗尽电池电量。通过保持连接活动，您可以按需将擦除或锁定等安全命令推送到设备。您还必须在部署到设备的每个策略中选择部署计划选项**部署用于始终在线连接**。
  - **从不：** 手动连接。Citrix 不建议将此选项用于生产部署，因为**从不**选项会阻止您将安全策略部署到设备；因此，用户永远不会收到任何新的应用程序或策略。
  - **每次：** 在指定的时间间隔连接。当此选项生效并且您发送安全策略（例如锁定或擦除）时，XenMobile 会在设备下次连接时在设备上处理该策略。
  - **定义计划：** 启用后，XenMobile 会在网络连接丢失后尝试将用户的设备重新连接到 XenMobile Server，并通过在您定义的时间范围内定期传输控制数据包来监控连接。

  用户示例： 您希望将密码策略部署到已注册的设备。计划策略可确保设备以固定间隔连接回服务器以收集新策略。

- **凭据策略**

  为何使用此策略： 凭据策略通常与 Wi-Fi 策略一起使用，它允许您部署证书以对需要证书身份验证的内部资源进行身份验证。

  用户示例： 您部署了一个 Wi-Fi 策略，用于在设备上配置无线网络。该 Wi-Fi 网络需要证书进行身份验证。凭据策略部署一个证书，该证书随后存储在操作系统密钥库中。用户连接到内部资源时可以选择该证书。

- **Exchange 策略**

  为何使用此策略： 借助 XenMobile，您可以通过两种方式交付 Microsoft Exchange ActiveSync 电子邮件。

  - **Secure Mail 应用程序：** 通过使用从公共应用程序商店或 XenMobile Store 分发的 Secure Mail 应用程序来交付电子邮件。
  - **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。通过用于本机电子邮件的 Exchange 策略，您可以使用宏从用户的 Active Directory 属性填充用户数据，例如使用 ${user.username} 填充用户名，使用 ${user.domain} 填充用户域。

用户示例： 推送 Exchange 策略时，您会将 Exchange Server 详细信息发送到设备。Secure Hub 随后会提示用户进行身份验证，然后他们的电子邮件便开始同步。

- **位置策略**

  为何使用此策略： 如果设备已为 Secure Hub 启用 GPS，位置策略允许您在地图上对设备进行地理定位。部署此策略并从 XenMobile Server 发送定位命令后，设备会返回位置坐标。

  用户示例： 当您部署位置策略且设备上启用了 GPS 时，如果用户放错了设备，他们可以登录 XenMobile 自助服务门户并选择定位选项，以在地图上查看其设备的位置。用户选择允许 Secure Hub 使用位置服务。当用户自行注册设备时，您无法强制使用位置服务。使用此策略的另一个考虑因素是对电池续航时间的影响。

- **密码策略**

  为何使用此策略： 密码策略允许您在托管设备上强制执行 PIN 码或密码。此密码策略允许您设置设备上密码的复杂性和超时时间。

  用户示例： 当您将密码策略部署到托管设备时，Secure Hub 会提示用户配置密码或 PIN，用户必须在打开设备或不活动计时器到期时解锁才能访问其设备。

- **配置文件删除策略**

  为何使用此策略： 假设您将策略部署到一组用户，但后来必须从部分用户中删除该策略。您可以通过创建配置文件删除策略并使用部署规则将配置文件删除策略仅部署到指定用户名来删除选定用户的策略。

  用户示例： 当您将配置文件删除策略部署到用户设备时，用户可能不会注意到更改。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，用户将不知道现在允许使用摄像头。请考虑在更改影响用户体验时通知用户。

- **限制策略**

  为何使用此策略： 限制策略为您提供了多种选项，用于锁定和控制受管设备上的功能。您可以为支持的设备启用数百种限制选项，从禁用设备上的摄像头或麦克风，到强制执行漫游规则以及访问应用商店等第三方服务。

  用户示例： 如果您向 iOS 设备部署限制，用户可能无法访问 iCloud 或 Apple App Store。

- **条款和条件策略**

  为何使用此策略： 您可能需要告知用户管理其设备的法律影响。此外，您可能希望确保用户了解企业数据推送到设备时的安全风险。自定义的条款和条件文档允许您在用户注册之前发布规则和通知。

用户示例： 用户在注册过程中会看到条款和条件信息。如果他们拒绝接受所述条件，注册过程将终止，并且他们无法访问企业数据。您可以生成一份报告，提供给人力资源/法律/合规团队，以显示谁接受或拒绝了这些条款。

- **VPN 策略**

为何使用此策略： 使用 VPN 策略可以通过较旧的 VPN 网关技术提供对后端系统的访问。此策略支持各种 VPN 提供商，包括 Cisco AnyConnect、Juniper 和 Citrix VPN。如果 VPN 网关支持此选项，还可以将此策略链接到 CA 并启用按需 VPN。

用户示例： 启用 VPN 策略后，当用户访问内部域时，用户的设备会打开 VPN 连接。

- **Webclip 策略**

为何使用此策略： 如果您想向设备推送一个直接打开网站的图标，请使用 Webclip 策略。Web 剪辑包含指向网站的链接，并且可以包含自定义图标。在设备上，Web 剪辑看起来像一个应用程序图标。

用户示例： 用户可以单击 Web 剪辑图标以打开提供他们必须访问的服务的互联网站点。使用 Web 链接比需要打开浏览器应用程序并键入链接地址更方便。

- **WiFi 策略**

为何使用此策略： Wi-Fi 策略允许您将 Wi-Fi 网络详细信息（例如 SSID、身份验证数据和配置数据）部署到受管设备。

用户示例： 当您部署 Wi-Fi 策略时，设备会自动连接到 Wi-Fi 网络并对用户进行身份验证，以便他们可以访问该网络。

- **Windows 信息保护策略**

为何使用此策略： 使用 Windows 信息保护 (WIP) 策略来防止企业数据可能泄露。您可以在设置的强制级别指定需要 Windows 信息保护的应用程序。例如，您可以阻止任何不适当的数据共享，或者警告不适当的数据共享并允许用户覆盖策略。您可以在记录和允许不适当数据共享的同时静默运行 WIP。

用户示例： 假设您将 WIP 策略配置为阻止不适当的数据共享。如果用户将受保护的文件复制或保存到非受保护位置，则会出现类似以下内容的消息：您无法将受工作保护的内容放置在此位置。

- **XenMobile Store 策略**

为何使用此策略： XenMobile Store 是一个统一的应用程序商店，管理员可以在其中发布用户所需的所有企业应用程序和数据资源。管理员可以添加：

- Web 应用程序、SaaS 应用程序以及启用了 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 和 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，可以通过 Citrix Secure Hub™ 应用程序访问 XenMobile Store。然后，用户可以看到所有可用的企业应用程序和服务。用户可以单击应用程序进行安装、访问数据、对应用程序进行评分和评论，以及从 XenMobile Store 下载应用程序更新。

用户注册选项

您可以通过多种方式让用户将其设备注册到 XenMobile。在考虑具体细节之前，请决定要将哪些设备注册到 MDM+MAM、MDM 或 MAM。有关这些管理模式的更多信息，请参阅管理模式。

从最高层面来看，有四种注册选项：

- **注册邀请：** 向用户发送注册邀请或邀请 URL。注册邀请和 URL 不适用于 Windows 设备。
- **自助服务门户：** 设置一个门户，用户可以访问该门户以下载 Secure Hub 并注册其设备或向自己发送注册邀请。
- **手动注册：** 发送电子邮件、手册或其他通信，告知用户系统可用于注册。然后，用户下载 Secure Hub 并手动注册其设备。
- **企业：** 设备注册的另一个选项是通过 Apple 部署计划和 Google Android Enterprise。通过这些计划，您可以购买预配置并可供员工使用的设备。有关更多信息，请参阅Apple 支持中的 Apple 部署计划文章和Android Enterprise 网站上的 Google Android Enterprise 文档。

注册邀请

您可以向使用 iOS、macOS、Android Enterprise 和旧版 Android 设备的用户发送注册邀请电子邮件。注册邀请和 URL 不适用于 Windows 设备。

您还可以通过 SMTP 或 SMS 向使用 iOS、macOS、Android 或 Windows 设备的用户发送安装链接。有关更多信息，请参阅注册设备。

如果您选择使用注册邀请方法，则可以：

- 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。

有关每个注册安全模式的信息，请参阅配置注册安全模式。

邀请函有多种用途。邀请函最常见的用途是通知用户系统可用，并且他们可以注册。邀请 URL 是唯一的。用户使用邀请 URL 后，该 URL 将不再可用。您可以使用此属性来限制注册到您系统的用户或设备。

配置注册配置文件时，您可以根据 Active Directory 组控制特定用户可以注册的设备数量。例如，您可能只允许财务部门的每个用户注册一台设备。

请注意某些注册选项的额外成本和潜在问题。例如，通过短信发送邀请需要额外的基础设施。有关此选项的更多信息，请参阅通知。

除了通过电子邮件发送邀请外，请确保用户可以在 Secure Hub 之外访问电子邮件。您可以使用一次性密码 (OTP) 注册安全模式作为 MDM 注册的 Active Directory 密码的替代方案。

自助服务门户

您可以通过自助服务门户请求注册邀请。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

通过手动注册，用户可以通过 AutoDiscovery 或输入服务器信息连接到 XenMobile。使用 AutoDiscovery 时，用户只需使用其电子邮件地址或用户主体名称格式的 Active Directory 凭据登录。如果没有 AutoDiscovery，他们必须输入服务器地址和其 Active Directory 凭据。有关设置 AutoDiscovery 的更多信息，请参阅XenMobile AutoDiscovery Service。

您可以通过多种方式促进手动注册。您可以创建一份指南，分发给用户，让他们自行注册。您可以让 IT 部门在特定时间段内手动注册用户组。您可以使用任何类似的方法，要求用户输入其凭据、服务器信息或两者。

用户入职

设置好环境后，您需要决定如何将用户引入您的环境。本文前面部分讨论了用户注册安全模式的具体细节。本节讨论了您联系用户的方式。

开放注册与选择性邀请

在用户入职时，您可以通过两种基本方法允许注册：

- 开放注册。默认情况下，任何具有 LDAP 凭据和 XenMobile® 环境信息的用户都可以注册。

- 受限注册。您可以通过仅允许持有邀请的用户注册来限制用户数量。您还可以通过 Active Directory 组来限制开放注册。

通过邀请方式，您还可以限制用户可以注册的设备数量。在大多数情况下，开放注册是可以接受的，但有几点需要考虑：

- 对于 MAM 注册，您可以通过 Active Directory 组成员身份轻松限制开放注册。
- 对于 MDM 注册，您可以根据 Active Directory 组成员身份限制可以注册的设备数量。如果您的环境中只允许公司设备，那么此限制通常不是问题。但是，如果您想限制环境中设备的数量，则在 BYOD 工作场所中可能需要考虑此方法。

选择性邀请通常较少使用，因为它比开放注册需要更多的工作。用户若要在您的环境中注册其设备，您必须向每个用户发送唯一的邀请。有关如何发送注册邀请的信息，请参阅发送注册邀请。

虽然您可以使用 Active Directory 组批量创建邀请，但您必须分批执行此方法。

首次联系用户

在您决定开放注册或选择性邀请并设置好这些环境后，您必须让用户了解他们的注册选项。

如果您使用选择性邀请方法，电子邮件和短信是该过程的一部分。您也可以通过 XenMobile 控制台发送电子邮件进行开放注册。有关详细信息，请参阅发送注册邀请。

无论哪种情况，请记住，对于电子邮件，您需要一个 SMTP 服务器。对于短信，您需要一个 SMS 服务器。在做出决定时，这些服务器可能会带来额外的成本。在选择方法之前，请考虑您希望新用户如何访问信息，例如电子邮件。如果您希望所有用户通过 XenMobile 访问其电子邮件，那么向他们发送邀请电子邮件将是一个问题。

您还可以通过 XenMobile 之外的其他方式为开放注册环境发送通信。对于该选项，请务必包含所有相关信息。让用户知道他们可以在哪里获取 Secure Hub 应用程序以及使用哪种方法进行注册。如果禁用了发现功能，还要向用户提供 XenMobile Server 地址。要了解有关 AutoDiscovery 的更多信息，请参阅XenMobile AutoDiscovery Service。

优化 XenMobile® 运行

XenMobile 运行的性能和稳定性涉及 XenMobile 中的许多设置，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的、与 XenMobile 调整和优化相关的设置。Citrix 建议您在部署 XenMobile 之前评估本文中的每个设置。

> **重要：**

> 这些指南假设 XenMobile Server 的 CPU 和 RAM 足以支持设备数量。有关可伸缩性的更多信息，请参阅可伸缩性和性能。

> 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需要重新启动每个 XenMobile Server 节点。XenMobile 会在需要重新启动时通知您。

这些调整指南适用于群集和非群集环境。

hibernate.c3p0.idle_test_period

此 XenMobile Server 属性（一个自定义密钥）确定连接自动验证之前的空闲时间（以秒为单位）。按如下方式配置密钥。默认值为 **30**。

- 密钥：**自定义密钥**
- 密钥：**hibernate.c3p0. idle_test_period**
- 值：**120**
- 显示名称：**hibernate.c3p0. idle_test_period**
- 描述：**Hibernate 空闲测试周期**

hibernate.c3p0.max_size

此自定义密钥确定 XenMobile 可以打开到 SQL Server 数据库的最大连接数。XenMobile 将您为此自定义密钥指定的值用作上限。仅当您需要时才打开连接。根据数据库服务器的容量设置。

请注意集群配置中的以下等式。您的 c3p0 连接数乘以节点数等于 XenMobile 可以打开到 SQL Server 数据库的实际最大连接数。

在集群和非集群配置中，如果 SQL Server 规模不足，将该值设置得过高可能会在高峰负载期间导致 SQL 端出现资源问题。将该值设置得过低则意味着您可能无法充分利用可用的 SQL 资源。

按如下方式配置密钥。默认值为 **1000**。

- 密钥：**hibernate.c3p0.max_size**
- 值：**1000**
- 显示名称：**hibernate.c3p0.max_size**
- 描述：到 SQL 的数据库连接

hibernate.c3p0.min_size

此自定义密钥确定 XenMobile 打开到 SQL Server 数据库的最小连接数。按如下方式配置密钥。默认值为 **100**。

- 密钥：**hibernate.c3p0.min_size**
- 值：**100**
- 显示名称：**hibernate.c3p0.min_size**
- 描述：到 SQL 的数据库连接

hibernate.c3p0.timeout

此自定义密钥确定空闲超时。如果您使用数据库集群故障转移，Citrix 建议您添加此自定义密钥并将其设置为缩短空闲超时。默认值为 **120**。

- 键: **自定义密钥**
- 键: **hibernate.c3p0.timeout**
- 值: **120**
- 显示名称: **hibernate.c3p0.timeout**
- 描述: 数据库空闲超时

推送服务心跳间隔

此设置确定 iOS 设备检查 APNs 通知是否在此期间未送达的频率。增加 APNs 心跳频率可以优化数据库通信。值过大可能会增加不必要的负载。此设置仅适用于 iOS。默认值为 **20** 小时。

如果您的环境中有很多 iOS 设备，心跳间隔可能会导致比必要更高的负载。选择性擦除、锁定和完全擦除等安全操作不依赖此心跳。原因是当执行这些操作时，APNs 通知会发送到设备。

此值控制在 Active Directory 组员资格更改后策略更新的速度。因此，通常适合将此值增加到 12 到 20 小时之间以减少负载。

iOS MDM APNS 连接池大小

当设备数量超过 100 台时，过小的 APNs 连接池可能会对 APNs 活动性能产生负面影响。性能问题包括向设备部署应用程序和策略的速度变慢以及设备注册速度变慢。默认值为 **1**。我们建议您每增加约 400 台设备，将此值增加 1。

auth.ldap.connect.timeout

为弥补 LDAP 响应缓慢的问题，Citrix 建议您为以下自定义密钥添加服务器属性。

- 键: **自定义密钥**
- 键: **auth.ldap.connect.timeout**
- 值: **60000**
- 显示名称: **auth.ldap.connect.timeout**
- 描述: **LDAP 连接超时**

auth.ldap.read.timeout

为弥补 LDAP 响应缓慢的问题，Citrix 建议您为以下自定义密钥添加服务器属性。

- 密钥: **自定义密钥**
- 密钥: **auth.ldap.read.timeout**
- 值: **60000**
- 显示名称: **auth.ldap.read.timeout**
- 描述: **LDAP 读取超时**

其他服务器优化

服务器属性	默认设置	为什么要更改此设置？
后台部署	1,440 分钟	后台策略部署的频率，以分钟为单位。仅适用于 Android 设备的常开连接。增加策略部署的频率可降低服务器负载。建议设置为 **1440**（24 小时）。
后台硬件清单	1,440 分钟	后台硬件清单的频率，以分钟为单位。仅适用于 Android 设备的常开连接。增加硬件清单的频率可降低服务器负载。建议设置为 **1440**（24 小时）。
检查已删除的 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 **0** 可阻止 XenMobile 检查已删除的 Active Directory 用户。建议设置为 **15** 分钟。

MaxNumberOfWorker	3	导入大量批量购买许可证时使用的线程数。默认为 **3**。如果需要进一步优化，可以增加线程数。但是，如果线程数较大（例如 6 个），批量购买导入会导致 CPU 使用率过高。

如何检查 SQL 数据库中的死锁并删除历史数据

当您看到死锁时，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
```

清理数据库

重要提示：

在更改表之前，请备份数据库。

1. 运行以下查询以检查历史数据。

```
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;
```

2. 从前面三个表中删除数据。

注意：

您可能在表中看不到历史数据。如果是这样，请跳过对该特定表运行截断查询。

```
truncate TABLE dbo.EWDEPLOY_HISTO;

truncate TABLE dbo.EWSESS;

truncate TABLE dbo.EWAUDIT;
```

3. 解除因死锁而阻塞的 SELECT 查询。此步骤可处理进一步的死锁。

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT ON
WITH ROLLBACK IMMEDIATE
```

4. 默认情况下，数据库清理会保留七天的会话保留和审计保留数据，这对于许多用户来说太高了。将清理值更改为 1 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
```

清理 KEYSTORE 表中的孤立项

如果 XenMobile 节点性能不佳，请检查 KEYSTORE 表是否过大。XenMobile Server 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 表中的证书会被删除。KEYSTORE 表中的条目会保留下来，这可能会导致性能问题。执行以下过程以清理 KEYSTORE 表中的孤立项。

重要提示：

在更改表之前，请备份数据库。

1. 运行以下查询以检查历史数据。

```
select COUNT(*) from KEYSTORE
```

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;
```

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'

    );
```

4. 为 KEYSTORE 表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");
```

应用调配和取消调配

应用程序调配围绕着移动应用生命周期管理：在 XenMobile® 环境中准备、配置、交付和管理移动应用。在某些情况下，开发或修改应用程序代码也可能是调配过程的一部分。XenMobile 配备了可用于应用调配的各种工具和流程。

在阅读这篇关于应用调配的文章之前，我们建议您阅读以下文章：

- 应用 - 用户社区

在确定了贵组织计划向用户交付的应用类型后，您可以概述在其整个生命周期中管理这些应用的过程。

在定义应用调配过程时，请考虑以下几点：

- **应用分析：** 您的组织可以从少量应用开始。但是，随着用户采用率的提高和环境的增长，您管理的应用数量可能会迅速增加。从一开始就定义特定的应用配置文件，以使应用调配易于管理。应用分析可帮助您从非技术角度将应用分类到逻辑组中。例如，您可以根据以下因素创建应用配置文件：
  - 版本：用于跟踪的应用版本
  - 实例：为不同用户集部署的多个实例，例如，具有不同访问级别
  - 平台：iOS、Android 或 Windows
  - 目标受众：标准用户、部门、C 级高管
  - 所有权：拥有该应用的部门
  - 类型：MDX、公共、Web 和 SaaS 或 Web 链接
  - 升级周期：应用升级的频率
  - 许可：许可要求和所有权
  - MAM SDK 或 MDX 策略：将 MDX 功能应用于您的移动应用程序
  - 网络访问：访问类型，例如安全浏览或完整 VPN

> **注意：**
>
> 隧道式 Web SSO 是 MDX 设置中安全浏览的名称。其行为相同。

示例：

因素	安全邮件	邮件	内部	埃匹克 罗孚
版本	10.1	10.1	X.x	X.x
实例	VIP	医生	临床	临床
平台	iOS	iOS	iOS	iOS
目标用户	VIP 用户	医生	临床用户	临床用户
所有权	IT	IT	IT	IT
类型	MDX	MDX	原生	公共
升级周期	每季度	每季度	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	公共

- **应用程序版本控制：** 维护和跟踪应用程序版本是预配过程的关键部分。版本控制对用户是透明的。他们只会在有新版本的应用程序可供下载时收到通知。从您的角度来看，在非生产环境中审查和测试每个应用程序版本对于避免对生产造成影响也至关重要。

  评估是否需要特定升级也很重要。应用程序升级通常有两种类型：一种是次要升级，例如修复特定错误。第二种是主要版本，它对应用程序引入了重大更改和改进。无论哪种情况，都请仔细查看应用程序的发行说明，以评估升级是否必要。

- **应用程序开发：** 当您将 MAM SDK 集成到您开发的移动应用程序中时，您将 MDX 功能应用于这些应用程序。请参阅 MAM SDK 概述。

  MAM SDK 将取代 MDX Toolkit，后者计划于 2023 年 7 月弃用。有关应用程序打包的信息，请参阅 MDX Toolkit。打包应用程序的应用程序预配过程与标准非打包应用程序的预配过程不同。

- **应用程序安全性：** 您在预配过程中定义单个应用程序或应用程序配置文件的安全要求。您可以在部署应用程序之前将安全要求映射到特定的 MDM 或 MAM 策略。这种规划简化并加快了应用程序部署。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 环境进行架构更改。这些更改取决于应用程序所需的安全合规性类型。例如，您可能希望设备加密以允许使用关键业务智能应用程序。或者某个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 允许您将应用程序作为 MDM 应用程序或 MAM 应用程序交付。MDM 应用程序显示在 XenMobile Store 中。此商店允许您方便地向用户交付公共或本机应用程序。您管理的唯一 MDM 应用程序控制是强制实施设备级别限制。但是，通过使用 MAM 交付应用程序可以完全控制应用程序交付和应用程序本身。通常，通过 MAM 交付应用程序更合适。
- **应用程序维护：**
  - 执行初始审核：跟踪生产环境中的应用程序版本以及上次升级周期。记下需要升级的特定功能或错误修复。
  - 建立基线：维护每个应用程序的最新稳定版本列表。此应用程序版本是升级后出现意外问题时的回退。还要制定回滚计划。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，首先将升级部署到一部分生产用户，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：及时了解应用程序的最新版本至关重要。早期访问版本 (EAR) 版本可能可用于测试。
  - 制定通知用户的策略：定义在应用程序升级可用时通知用户的策略。在部署前对用户进行培训。您可以在更新应用程序之前发送多个通知。根据应用程序的不同，最佳通知方法可能是电子邮件通知或网站。

应用程序生命周期管理代表应用程序从初始部署到退役的完整生命周期。应用程序的生命周期包括以下阶段：

1. 规范要求：从业务案例和用户要求开始。
2. 开发：验证应用程序是否满足业务需求。
3. 测试：识别测试用户、问题和错误。
4. 部署：将应用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，请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：作为一项安全要求，您需要一个容器化并支持 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 分配给测试用户组，并从 XenMobile Server 部署相应的 MDX 文件。测试用户验证他们可以成功发送和接收电子邮件，并具有日历和联系人访问权限。测试用户还会报告问题并识别错误。根据测试用户的反馈，您可以优化 Secure Mail 配置以用于生产。

4. 部署：测试阶段完成后，将 Secure Mail 分配给生产用户，并从 XenMobile 部署相应的 MDX 文件。
5. 维护：Secure Mail 有新的更新可用。从 Citrix 下载中下载新的 MDX 文件，并替换 XenMobile Server 上现有的 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，将应用程序上传到 XenMobile 生产环境并将其部署给用户。

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。

基于仪表板的操作

通过访问您的 XenMobile® 控制台仪表板，您可以一目了然地查看信息。利用这些信息，您可以通过使用小组件快速了解问题和成功之处。

仪表板通常是您首次登录 XenMobile 控制台时出现的屏幕。要从控制台的其他位置访问仪表板，请单击“**分析**”。在仪表板上单击“**自定义**”以编辑页面布局和显示的小组件。

- **我的仪表板：** 您最多可以保存四个仪表板。您可以单独编辑这些仪表板，并通过选择已保存的仪表板来查看每个仪表板。
- **布局样式：** 在此行中，您可以选择仪表板上显示的小组件数量以及小组件的布局方式。
- **小组件选择：** 您可以选择仪表板上显示的信息。
  - **通知：** 选中左侧数字上方的复选框，可在小组件上方添加一个通知栏。此栏显示合规设备、非活动设备以及在过去 24 小时内擦除或注册的设备数量。
  - **按平台划分的设备：** 按平台显示托管和非托管设备的数量。
  - **按运营商划分的设备：** 按运营商显示托管和非托管设备的数量。单击每个条形图可按平台查看详细信息。
  - **按平台划分的托管设备：** 按平台显示托管设备的数量。
  - **按平台划分的非托管设备：** 按平台显示非托管设备的数量。此图表中显示的设备可能已安装代理，但其权限已被撤销或已被擦除。
  - **按 ActiveSync 网关状态划分的设备：** 按 ActiveSync 网关状态显示设备数量。信息显示“已阻止”、“已允许”或“未知”状态。您可以单击每个条形图以按平台细分数据。
  - **按所有权划分的设备：** 按所有权状态显示设备数量。信息显示“公司所有”、“员工所有”或“未知”所有权状态。
  - **失败的交付组部署：** 显示每个软件包的失败部署总数。仅显示部署失败的软件包。
  - **按阻止原因划分的设备：** 显示 ActiveSync 阻止的设备数量。
  - **已安装应用：** 通过使用此小组件，您可以键入应用程序名称，图表将显示有关该应用程序的信息。

- **批量购买应用许可证使用情况：** 显示 Apple 批量购买应用的许可证使用情况统计信息。

用例

以下是您可以使用仪表板小组件监控环境的多种方式的一些示例。

- 您已部署移动生产力应用程序，并收到有关移动生产力应用程序无法在设备上安装的支持工单。使用**不合规设备**和**已安装应用**小组件查看未安装移动生产力应用程序的设备。
- 您希望监控非活动设备，以便可以从环境中移除这些设备并回收许可证。使用**非活动设备**小组件跟踪此统计信息。
- 您收到有关数据未正确同步的支持工单。您可能希望使用**按 ActiveSync 网关状态划分的设备**和**按阻止原因划分的设备**小组件来确定问题是否与 ActiveSync 相关。

报告

环境设置完毕且用户注册后，您可以运行报告以了解您的部署情况。XenMobile 内置了各种报告，可帮助您更好地了解环境中运行的设备。有关详细信息，请参阅报告。

> **重要提示：**
>
> 尽管可以使用 SQL Server 创建自定义报告，但 Citrix® 不建议使用此方法。以这种方式使用 SQL Server 数据库可能会对您的 XenMobile 部署造成不可预见的后果。如果您确实决定采用此报告方法，请确保使用只读帐户运行 SQL 查询。

基于角色的访问控制和 XenMobile® 支持

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，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，并包含有关为使用 RBAC 的 XenMobile 决定支持模型的注意事项。

> **注意：**
>
> 自 January 1, 2019 起，远程支持不再向新客户提供。现有客户可以继续使用该产品，但 Citrix® 不提供增强功能或修复。

内置角色

您可以更改授予以下内置角色的访问权限，也可以添加角色。有关与每个角色及其默认设置关联的完整访问和功能权限集，请从 XenMobile 文档中下载 基于角色的访问控制默认值。有关每个功能的定义，请参阅 XenMobile 文档中的 使用 RBAC 配置角色。

管理员角色

默认授予的访问权限：

- 完全系统访问权限，远程支持除外。
- 默认情况下，管理员可以执行一些支持任务，例如检查连接和创建支持包。

注意事项：

- 您的部分或所有管理员是否需要访问远程支持？如果是，您可以编辑管理员角色或添加管理员角色。
- 要进一步限制某些管理员或管理员组的访问权限，请添加基于管理员模板的角色并编辑权限。

支持

默认授予的访问权限：

- 访问远程支持。

注意事项：

- 对于本地 XenMobile Server 部署：远程支持使您的帮助台代表能够远程控制托管的 Android 移动设备。屏幕投射仅在 Samsung Knox 设备上受支持。
- 远程支持不适用于群集本地 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：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；响铃设备；重置容器密码）；添加、删除和发送注册邀请。

注意事项：

- 用户角色使您能够让用户自助。
- 为了支持共享设备，请为共享设备注册创建用户角色。

XenMobile 支持模型的注意事项

您可以采用的支持模型可能差异很大，并且可能涉及处理 1 级和 2 级支持的第三方，而员工处理 3 级和 4 级支持。无论您如何分配支持负载，请记住本节中针对您的 XenMobile 部署和用户群的特定注意事项。

用户拥有公司设备还是 BYO 设备？ 影响支持的主要问题是 XenMobile 环境中用户设备的归属。如果您的用户拥有公司设备，您可能会提供较低级别的支持，作为锁定设备的一种方式。在这种情况下，您可能会提供一个帮助台，协助用户解决设备问题以及如何使用设备。根据您需要支持的设备类型，请考虑如何为您的帮助台使用 RBAC 设备预配和支持角色。

如果您的用户拥有 BYO 设备，您的组织可能会期望用户自行寻找设备支持来源。在这种情况下，您的组织提供的支持更多是围绕 XenMobile 特定问题的管理角色。

您的桌面支持模型是什么？ 考虑您的桌面支持模型是否适用于其他公司拥有的设备。您可以使用相同的支持组织吗？他们需要哪些额外培训？

您是否希望用户访问XenMobile自助服务门户？ 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，允许他们注册其设备或向自己发送注册邀请。请参阅配置注册安全模式。

系统监控

为确保应用程序访问和连接的最佳正常运行时间，您必须监控 XenMobile® 环境中的以下核心组件。

XenMobile 服务器

XenMobile Server 在本地存储上生成并存储日志，您也可以将其导出到系统日志 (syslogs) 服务器。您可以配置日志设置以指定大小限制、日志级别，或者创建自定义日志记录器来筛选特定事件。您可以随时从 XenMobile 控制台查看 XenMobile Server 日志。您还可以通过 syslog 服务器将日志中的信息导出到您的生产 Splunk 日志服务器。

以下列表描述了 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 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>` 是一个唯一标识符，例如 sessionID。

- 其中 `<log message>` 是应用程序提供的消息。

管理员审计日志文件： 包含有关 XenMobile 控制台活动的审计信息。

> **注意：**
>
> 管理员审计日志和用户审计日志使用相同的格式。
>
> 消息格式：

除了必需的日期和时间戳值外，所有其他属性都是可选的。可选字段在消息中用“ ”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：

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
解除绑定应用程序	成功/失败
禁用应用程序	成功/失败

事件的管理员审核日志消息	状态
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
激活证书	成功/失败
CSR 证书	成功/失败
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

事件的管理员审核日志消息	状态
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
解除角色绑定	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 活动目录	成功/失败
更新 活动目录	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
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
更新接收器更新	成功/失败

事件的管理员审核日志消息	状态
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
更新接收器电子邮件	成功/失败
上传补丁	成功/失败
导入快照	成功/失败
获取应用商店应用详情	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
添加品牌	成功/失败
删除品牌	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

用户审计日志文件： 包含与已注册设备的用户活动相关的信息。

注意：

用户审计日志和管理员审计日志使用相同的格式。

消息格式：

除了必需的日期和时间戳值外，所有其他属性都是可选的。可选字段在消息中用“ ”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计日志事件：

事件的用户审计日志消息	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
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
密钥已保存	成功/失败
密钥已检索	成功/失败

事件的用户审计日志消息	状态
用户发起更改密码	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
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

MDM 功能	状态
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	成功/失败
外部应用	成功/失败
获取列表	成功/失败
发送列表	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
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

MDM 功能	状态
应用兑换码	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
品牌	成功/失败
安全浏览器	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 还会监控 XenMobile Web 服务状态，该状态配置有智能监控探针，用于模拟对每个 XenMobile Server 群集节点的 HTTP 请求。这些探针会确定服务是否在线，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，Citrix ADC 会将该服务器标记为关闭。此外，Citrix ADC 会将该节点从负载平衡池中移除，并记录该事件，以便通过 Citrix ADC 监控解决方案生成警报。

您还可以使用标准虚拟机管理程序监控工具来监控 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 服务。XenMobile 实例始终需要访问数据库，并且在 SQL 基础架构发生中断时会脱机（例如，停止响应）。在 SQL Server 出现任何磁盘空间问题后，XenMobile 控制台可能会继续运行一段时间。为确保数据库的最大正常运行时间以及 XenMobile 工作负载的足够性能，您必须主动监控 SQL Server 的状态。有关监控 SQL Server 的更多信息，请参阅性能监控和优化概述。此外，随着 XenMobile 环境的不断发展，您必须调整 CPU、内存和存储的资源分配，以保证服务级别协议。

思杰应用交付控制器

Citrix ADC 提供了将指标记录到内部存储或将日志发送到外部日志服务器的功能。您可以配置 syslog 服务器，将 Citrix ADC 日志导出到您的生产 Splunk 日志服务器。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

日志文件也存储在 Citrix ADC 存储的 /var/log/ns.log 目录中，并命名为 newnslog。Citrix ADC 使用 GZIP 算法轮转并压缩文件。日志文件名为 newnslog.xx.gz，其中 xx 表示运行编号。

Citrix ADC 还支持 SNMP 陷阱和警报作为监控选项。有关 SNMP 陷阱列表，请参阅 SNMP 监控。

灾难恢复

您可以架构和配置 XenMobile® 部署，其中包括使用主动-被动故障转移策略的多个站点以实现灾难恢复。

本文讨论的推荐灾难恢复策略包括：

- 位于一个地理位置数据中心中的单个 XenMobile 活动站点，为全球所有企业用户提供服务，称为主站点。
- 位于第二个地理位置数据中心中的第二个 XenMobile 站点，称为灾难恢复站点。如果主站点发生全站点数据中心故障，此灾难恢复站点将提供主动-被动站点故障转移。主站点包括 XenMobile、SQL 数据库和 Citrix ADC 基础结构，以促进故障转移并在主站点连接失败时为用户提供对 XenMobile 的访问。

灾难恢复站点的 XenMobile 服务器在正常运行期间保持脱机状态，仅在需要从主站点到灾难恢复站点进行完整站点故障转移的灾难恢复场景中才联机。灾难恢复站点的 SQL Server 必须处于活动状态并准备好提供连接服务，然后才能启动灾难恢复站点的 XenMobile 服务器。

此灾难恢复策略依赖于通过 DNS 更改手动故障转移 Citrix ADC 访问层，以便在发生中断时将 MDM 和 MAM 连接路由到灾难恢复站点。

> **注意：**

> 要使用此体系结构，您必须有一个用于数据库异步备份的流程，以及某种确保 SQL 基础结构高可用性的方法。

灾难恢复故障转移过程

1. 如果您正在测试灾难恢复故障转移过程，请关闭主站点中的 XenMobile 服务器以模拟站点故障。
2. 更改 XenMobile 服务器的公共 DNS 记录，使其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，使其指向灾难恢复站点的 SQL Server IP 地址。
4. 使灾难恢复站点的 XenMobile SQL 数据库联机。确保 SQL Server 和数据库处于活动状态，并准备好为本地 XenMobile 服务器提供连接服务。
5. 打开灾难恢复站点的 XenMobile 服务器。

XenMobile 服务器更新过程

随时按照以下步骤使用补丁和版本更新 XenMobile，以保持主服务器和灾难恢复服务器的代码一致。

1. 确保主站点中的 XenMobile 服务器已打补丁或已升级。
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 服务器联机。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. 将所需的补丁和更新应用于所有灾难恢复站点的 XenMobile 服务器。
5. 重新启动 XenMobile 服务器并确认补丁或升级成功。

灾难恢复参考架构图

下图显示了 XenMobile 灾难恢复部署的高级架构。

灾难恢复参考架构图(/en-us/xenmobile/server/media/disaster-recovery-diagram.png)

用于灾难恢复的 GSLB

此架构的一个关键要素是使用全局服务器负载平衡 (GSLB) 将流量定向到正确的数据中心。

默认情况下，XenMobile 向导的 Citrix ADC 配置 Citrix Gateway 的方式不支持将 GSLB 用于灾难恢复。因此，您必须采取额外的步骤。

GSLB 的工作原理

GSLB 的核心是一种 DNS 形式。参与的 Citrix ADC 设备充当权威 DNS 服务器，并将 DNS 记录解析为正确的 IP 地址（通常是应接收流量的 VIP）。Citrix ADC 设备在响应将流量定向到该系统的 DNS 查询之前，会检查系统运行状况。

当记录被解析时，GSLB 在解析流量方面的作用就完成了。客户端直接与目标虚拟 IP (VIP) 地址通信。DNS 客户端行为在控制记录何时以及如何过期方面起着重要作用。这在很大程度上超出了 Citrix ADC 系统的范围。因此，GSLB 受制于与 DNS 名称解析相同的限制。客户端会缓存响应，因此，这种方式的负载平衡不像传统的负载平衡那样实时。

Citrix ADC 上的 GSLB 配置，包括站点、服务和监视器，旨在提供正确的 DNS 名称解析。

用于发布服务器的实际配置（在此场景中，是 XenMobile 向导创建的 Citrix ADC 配置）不受 GSLB 的影响。GSLB 是 Citrix ADC 上的一项独立服务。

将 GSLB 与 XenMobile 结合使用时域委派的挑战

Citrix ADC for XenMobile 向导配置 XenMobile 的 Citrix Gateway。此向导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处理端口 443 和 8443 上的 MDM 流量。Citrix Gateway 接收 MAM 流量并将其转发到第三个服务器，即端口 8443 上的 MAM 负载平衡虚拟服务器。所有流向 MAM 负载平衡虚拟服务器的流量都通过 Citrix Gateway。

MAM 负载平衡虚拟服务器需要与 XenMobile 服务器相同的 SSL 证书，并使用与注册设备相同的 FQDN。MAM 负载平衡服务器还使用与其中一个 MDM 负载平衡服务器相同的端口 (8443)。为了使流量能够解析，Citrix ADC for XenMobile 向导在 Citrix Gateway 上创建了一个本地 DNS 记录。该 DNS 记录与用于注册设备的 FQDN 匹配。

当 XenMobile 服务器 URL 不是 GSLB 域 URL 时，此配置是有效的。如果将 GSLB 域 URL 用作 XenMobile 服务器 URL（灾难恢复所需），则本地 DNS 记录会阻止 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

为了解决 Citrix ADC for XenMobile 向导创建的默认配置所带来的挑战，您可以在父域 (`company.com`) 中为 XenMobile 服务器 FQDN 创建一个 CNAME 记录，并在 Citrix ADC 具有权威性的委派子区域 (`gslb.company.com`) 中指向一条记录。这样做允许为 MAM 负载平衡 VIP 地址创建静态 DNS A 记录，这是解析流量所必需的。

1. 在外部 DNS 上，为 XenMobile 服务器 FQDN 创建一个 CNAME，指向 Citrix ADC GSLB 上的 GSLB 域 FQDN。您需要两个 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 实例上，创建一个 GSLB 虚拟服务器，其 FQDN 是 CNAME 记录所指向的。

   示例：

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   使用 Citrix ADC for XenMobile 向导部署 Citrix Gateway 时，在配置 MAM 负载平衡服务器时，请使用 XenMobile Server URL。这会为 XenMobile Server URL 创建一个静态 DNS A 记录。

3. 使用 XenMobile Server URL (`xms.company.com`) 测试在 Secure Hub 上注册的客户端。

   本示例使用以下 FQDN：

   - `xms.company.com` 是 MDM 流量使用的 URL，供注册设备使用，本示例中通过使用 Citrix ADC for XenMobile 向导进行配置。
   - `xms.gslb.company.com` 是 XenMobile Server 的 GSLB 域 FQDN。

Citrix 支持流程

您可以求助于 Citrix 技术支持服务，以解决与 Citrix 产品相关的问题。该团队提供变通方法和解决方案，并与开发团队紧密合作以提供解决方案。

Citrix ConsultingSM 服务或 Citrix Education 服务提供与产品培训、产品使用建议、配置、安装或环境设计和架构相关的帮助。

Citrix Consulting 协助处理与 Citrix 产品相关的项目，包括概念验证、经济影响评估、基础设施健康检查、设计要求分析、架构设计验证、集成和运营流程开发。

Citrix EducationSM 提供关于 Citrix 虚拟化、云和网络技术的业界最佳 IT 培训和认证。

Citrix 建议您在创建支持案例之前充分利用 Citrix 自助资源和建议。例如，您可以在多个地方查阅 Citrix 技术专家撰写的文章和公告，查看 Citrix 解决方案和技术的产品文档，或者阅读 Citrix 高管、产品团队和技术专家的直接评论。请分别参阅 知识中心、产品文档 和 博客 页面。

如需更多互动帮助，您可以参与讨论论坛，在那里您可以向其他客户提问并获得实际答案，在用户组和兴趣组内分享想法、意见、技术信息和最佳实践，或者与监控 Citrix 支持社交网站的 Citrix 支持工程师互动。请分别参阅 支持论坛 和 Citrix 社区 页面。

您还可以访问培训和认证课程以提升您的技能。请参阅 Citrix Education。

Citrix Insight Services 为您的 Citrix 环境提供了一个简单的在线故障排除平台和健康检查工具。适用于 XenMobile、Citrix Virtual Apps and Desktops、Citrix Hypervisor 和 Citrix Gateway。请参阅 分析工具。

如需技术支持，您可以通过电话或网络创建支持案例。对于低严重性和中等严重性问题，您可以使用网络；对于高严重性问题，则可以使用电话选项。要联系 XenMobile 问题的支持，请参阅 Citrix 支持服务。

如果您需要一位经验丰富、能够提供 Citrix 解决方案的高度专业化的单一联系人，Citrix Services 提供技术关系经理。有关 Citrix 服务产品和优势的更多信息，请参阅 Citrix 全球服务。

在 XenMobile® 中发送组注册邀请

您可以在 XenMobile Server 中向组和嵌套组发送注册邀请。Windows 设备不支持注册邀请。

设置组邀请时，可以指定一个或多个设备平台。您还可以标记设备，以便例如区分公司拥有的设备和员工拥有的设备。然后，您可以设置用户设备的身份验证类型。

> **注意：**
>
> 如果您计划使用自定义通知模板，则必须在配置注册安全模式之前设置这些模板。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、注册安全模式和邀请的基本配置的详细信息，请参阅 用户帐户、角色和注册。

一般步骤

1. 在 XenMobile 控制台中，导航到 **Manage > Enrollment Invitations**。
2. 单击屏幕左上角的 **Add**，然后单击 **Add Invitation**。
3. 从 **Recipient** 菜单中单击 **Group**。

   此步骤允许您选择一个或多个平台。如果您的公司混合使用不同的操作系统平台，请选择所有平台。仅当您确定没有用户使用特定平台时，才清除平台选择。
4. 您可以在邀请过程中选择标记设备。选择 **Corporate** 或 **Employee**。

   标记可轻松区分公司拥有的设备和员工拥有的设备。
5. 在 **Domain** 列表中，选择组所在的域。

6. 在 **Group** 列表中，选择要向其发送邀请的 Active Directory 组。
7. 通过**注册模式**，您可以设置您为用户选择的身份验证安全类型。

   - 用户名 + 密码
   - 高安全性
   - 邀请 URL
   - 邀请 URL + PIN
   - 邀请 URL + 密码
   - 双因素
   - 用户名 + PIN

   > **注意：**
   >
   > 要发送注册邀请，您只能使用**邀请 URL**、**邀请 URL + PIN**或**邀请 URL + 密码**注册安全模式。对于使用**用户名 + 密码**、**双因素**或**用户名 + PIN**注册的设备，用户必须在 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选择列出的默认模板。

   如果您计划使用自定义通知模板，您必须在配置注册安全模式之前设置这些模板。有关通知模板的更多信息，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。请先设置您的 SMTP 信息，然后再继续。

   > **注意：**
   >
   > **过期时间**和**最大尝试次数**选项会根据您选择的**注册模式**选项而变化。您无法更改这些选项。

9. 选择“开”以**发送邀请**，然后点击**保存并发送**以完成此过程。

嵌套组支持

您可以使用嵌套组发送邀请。通常，嵌套组用于大规模环境中，其中具有相似权限的组相互绑定。

导航到**设置 > LDAP**，然后启用**支持嵌套组**选项。

故障排除和已知限制

问题： 即使已从 Active Directory 组中删除用户，邀请仍会发送给他们。

解决方案： 根据您的 Active Directory 环境的大小，更改传播到所有服务器可能需要长达六小时。如果用户或嵌套组最近被删除，XenMobile 可能仍会将这些用户视为组的一部分。

因此，最好等待长达六小时，然后再向您的组发送另一个组邀请。

配置本地设备健康证明服务器

您可以通过本地 Windows 服务器为 Windows 10 和 Windows 11 移动设备启用设备健康证明 (DHA)。要在本地启用 DHA，您首先需要配置 DHA 服务器。

配置 DHA 服务器后，您将创建 XenMobile Server 策略以启用本地 DHA 服务。有关创建此策略的信息，请参阅设备健康证明设备策略。

DHA 服务器的先决条件

- 运行 Windows Server Technical Preview 5 或更高版本，并使用桌面体验安装选项安装的服务器。
- 一个或多个 Windows 10 和 Windows 11 客户端设备。这些设备必须具有运行最新版本 Windows 的 TPM 1.2 或 2.0。
- 以下证书：
  - **DHA SSL 证书：** 链接到企业信任根的 x.509 SSL 证书，具有可导出私钥。此证书可保护传输中的 DHA 数据通信，包括以下通信：
    - 服务器到服务器（DHA 服务和 MDM 服务器）
    - 服务器到客户端（DHA 服务和 Windows 10 或 Windows 11 设备）
  - **DHA 签名证书：** 链接到企业信任根的 x.509 证书，具有可导出私钥。DHA 服务使用此证书进行数字签名。
  - **DHA 加密证书：** 链接到企业信任根的 x.509 证书，具有可导出私钥。DHA 服务也使用此证书进行加密。
- 选择以下证书验证模式之一：
  - **EKCert：** EKCert 验证模式针对未连接到 Internet 的组织中的设备进行了优化。连接到以 EKCert 验证模式运行的 DHA 服务的设备无法直接访问 Internet。

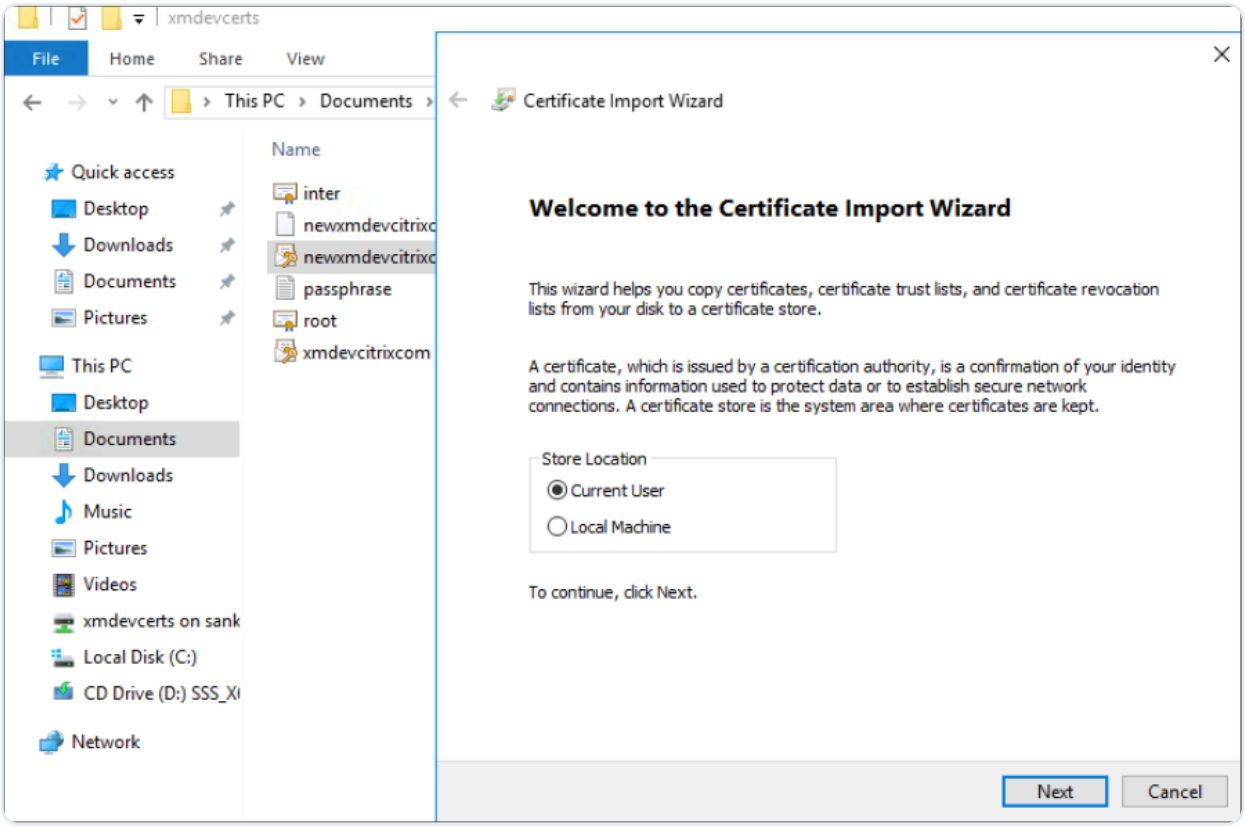
- **AIKCert：** AIKCert 验证模式针对可以访问 Internet 的操作环境进行了优化。连接到以 AIKCert 验证模式运行的 DHA 服务的设备必须能够直接访问 Internet，并且可以从 Microsoft 获取 AIK 证书。

将 DHA 服务器角色添加到 Windows 服务器

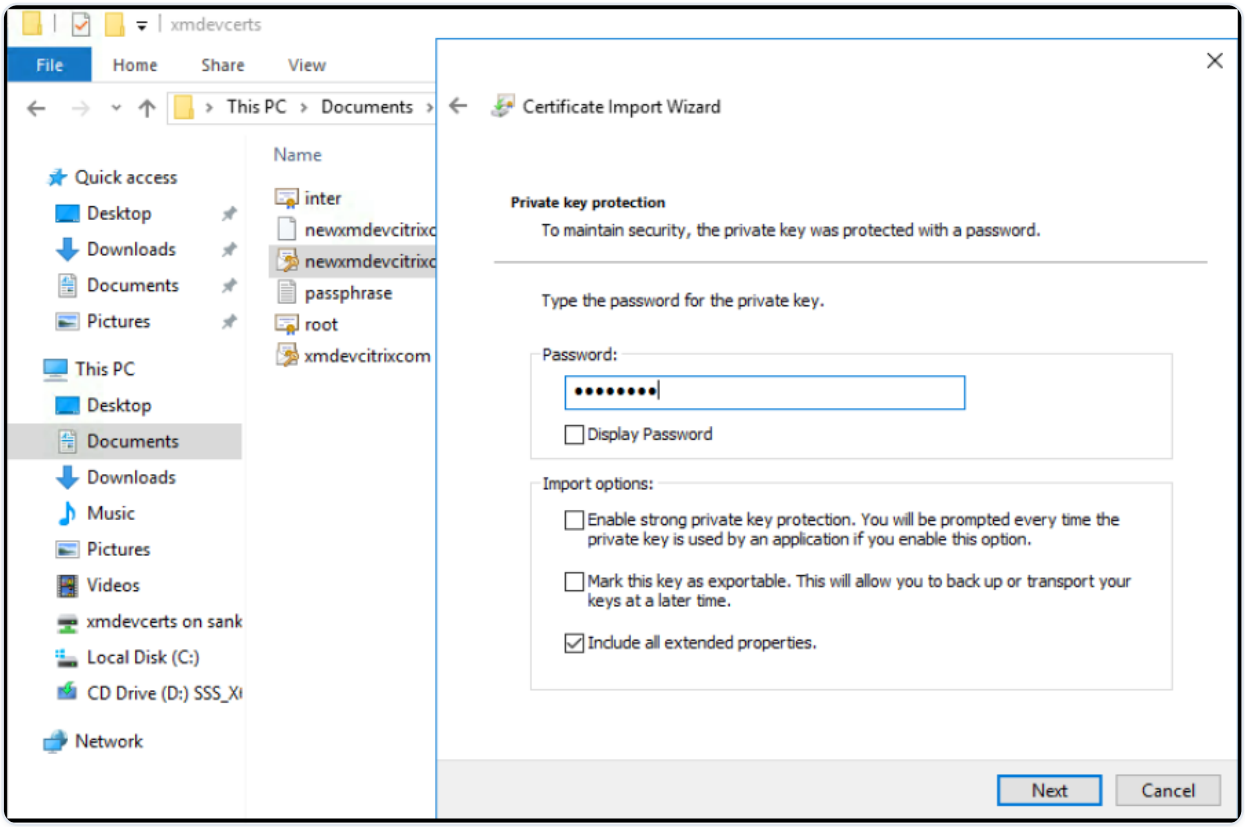
1. 在 Windows 服务器上，如果“服务器管理器”尚未打开，请单击“**开始**”，然后单击“**服务器管理器**”。
2. 单击“**添加角色和功能**”。
3. 在“**开始之前**”页面上，单击“**下一步**”。
4. 在“**选择安装类型**”页面上，单击“**基于角色或基于功能的安装**”，然后单击“**下一步**”。
5. 在“**选择目标服务器**”页面上，单击“**从服务器池中选择服务器**”，选择服务器，然后单击“**下一步**”。
6. 在“**选择服务器角色**”页面上，选中“设备健康状况证明”复选框。
7. 可选：单击“**添加功能**”以安装其他所需的角色服务和功能。
8. 单击“**下一步**”。
9. 在“**选择功能**”页面上，单击“**下一步**”。
10. 在“**Web 服务器角色 (IIS)**”页面上，单击“**下一步**”。
11. 在“**选择角色服务**”页面上，单击“**下一步**”。
12. 在“**设备健康状况证明服务**”页面上，单击“**下一步**”。
13. 在“**确认安装选择**”页面上，单击“**安装**”。
14. 安装完成后，单击“**关闭**”。

将 SSL 证书添加到服务器的证书存储区

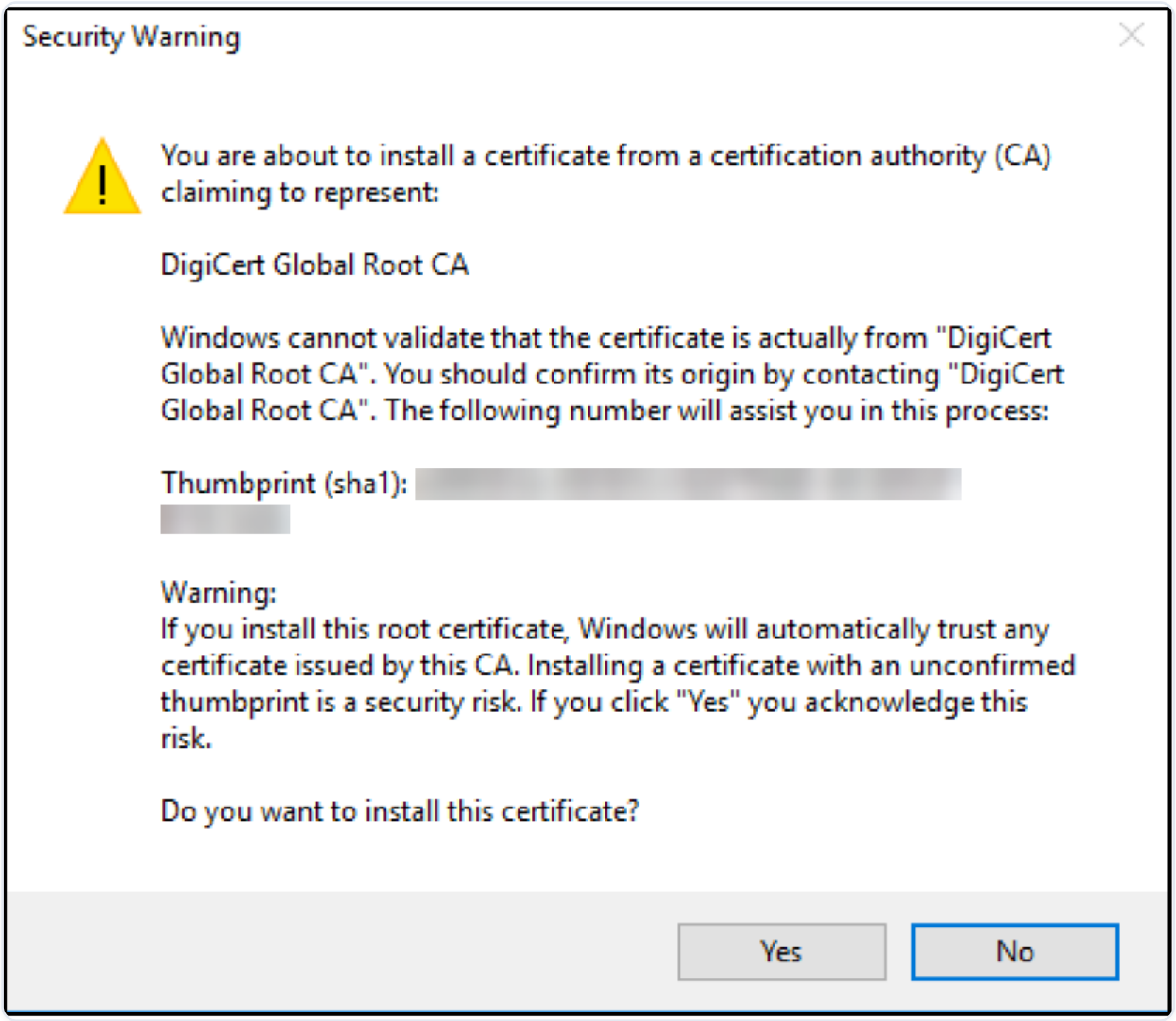
1. 转到 SSL 证书文件并选择它。
2. 选择 **当前用户** 作为存储位置，然后单击 **下一步**。



3. 键入私钥的密码。
4. 确保选中导入选项 **包括所有扩展属性**。单击 **下一步**。



5. 当此窗口出现时，单击 **是**。



6. 确认证书已安装：

   a. 打开“命令提示符”窗口。

   b. 键入 **mmc** 并按 Enter 键。要在本地计算机存储中查看证书，您必须具有管理员角色。

   c. 在“文件”菜单上，单击 **添加/删除管理单元**。

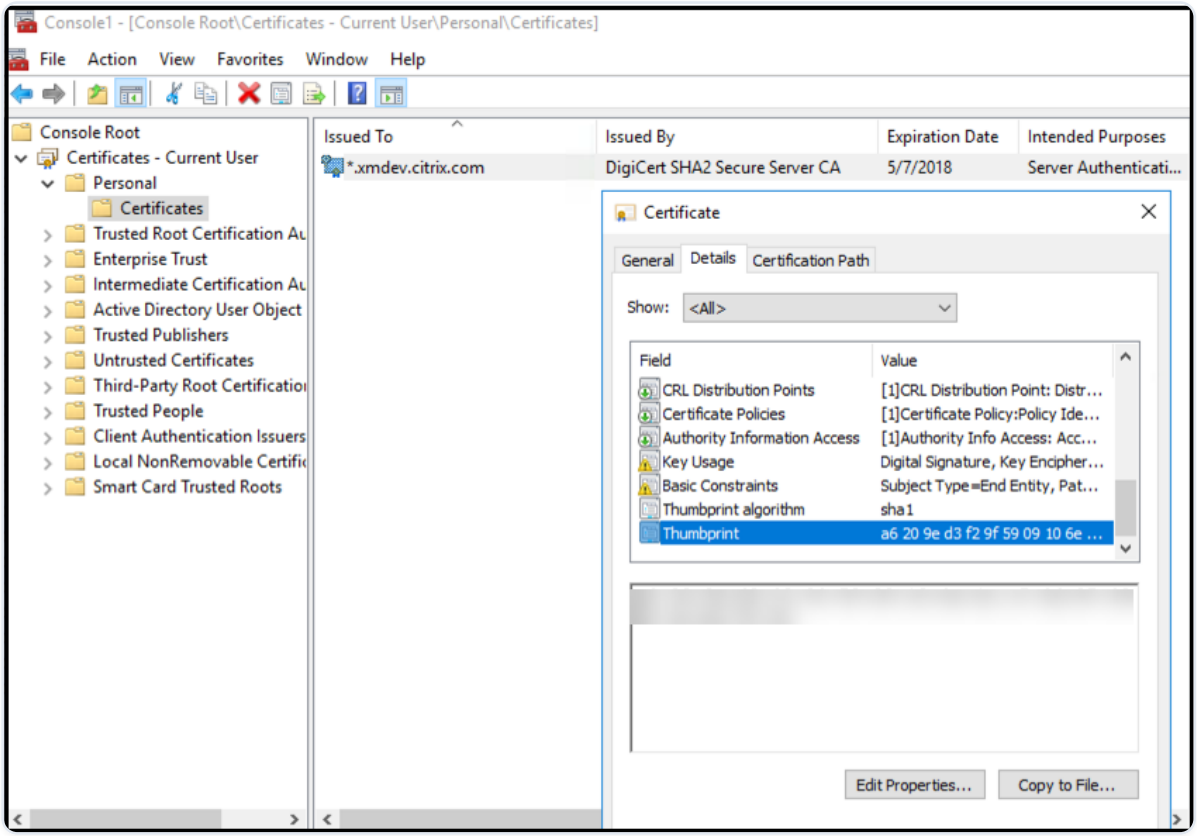
   d. 单击 **添加**。

   e. 在“添加独立管理单元”对话框中，选择 **证书**。

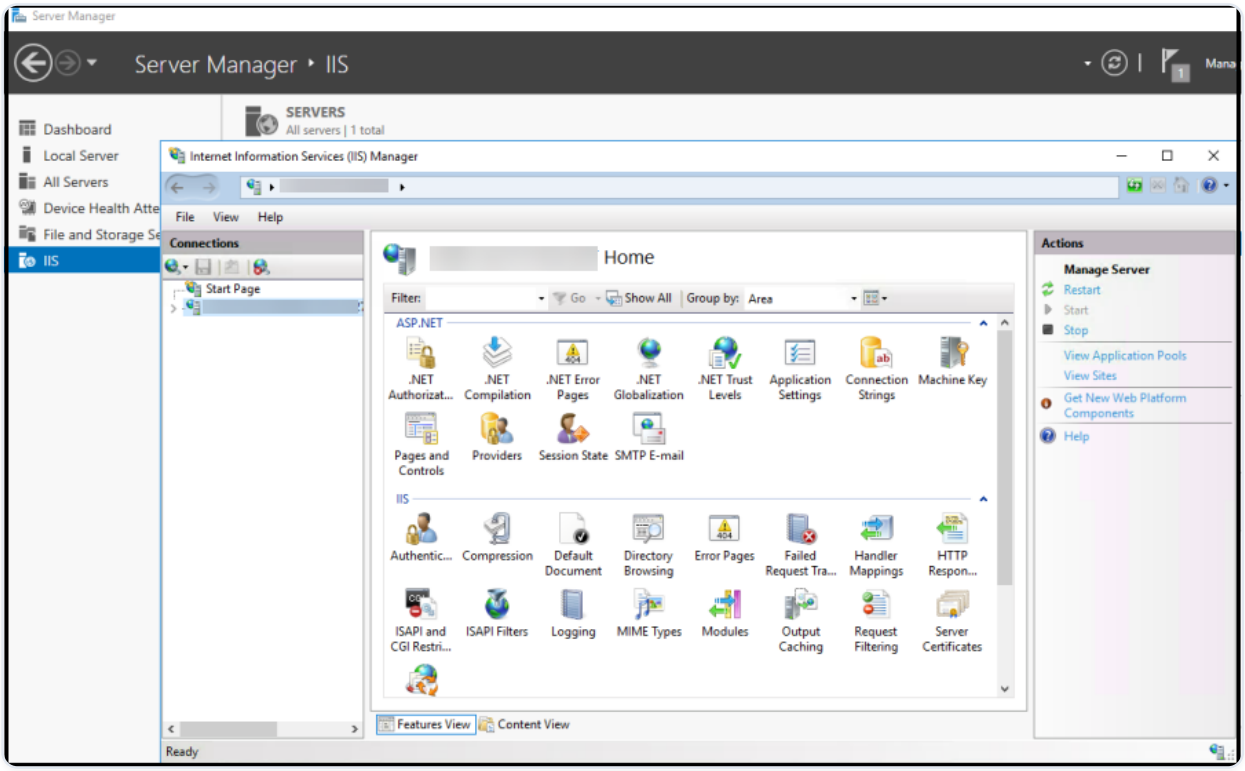
   f. 点击 **添加**。

   g. 在 **证书管理单元** 对话框中，选择 **我的用户帐户**。（如果您以服务帐户持有者身份登录，请选择 **服务帐户**。）

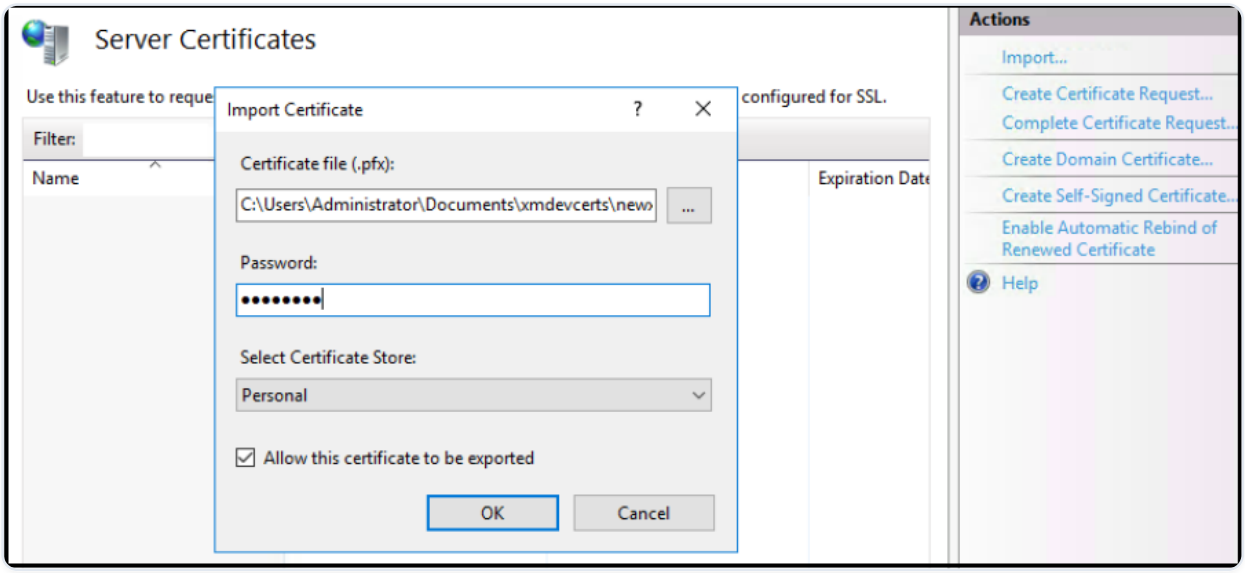
   h. 在“选择计算机”对话框中，点击 **完成**。



7. 转到 **服务器管理器 > IIS**，然后从图标列表中选择 **服务器证书**。

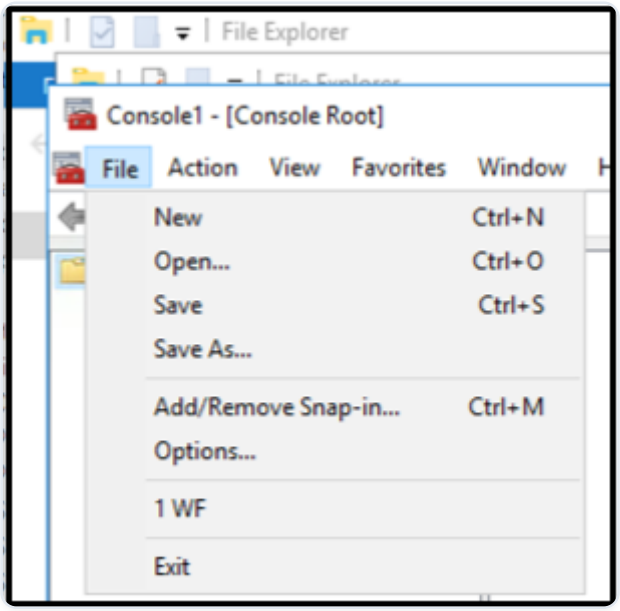


8. 从“操作”菜单中，选择 **导入...** 以导入 SSL 证书。

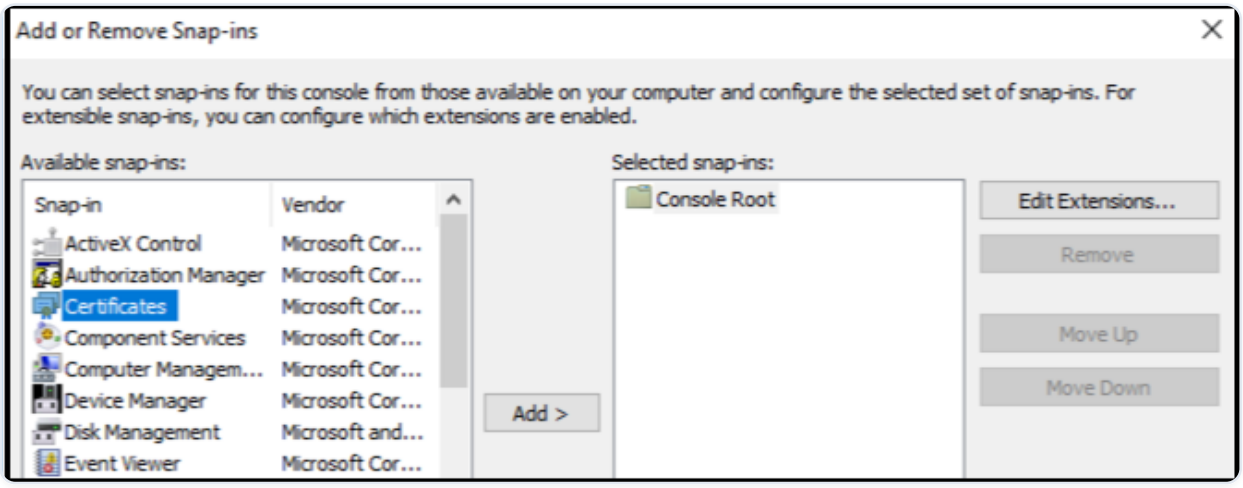


检索并保存证书的指纹

1. 在文件资源管理器搜索栏中，键入 **mmc**。
2. 在“控制台根目录”窗口中，点击 **文件 > 添加/删除管理单元...**。



3. 从可用的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**。

   Windows 添加或删除管理单元的图像(/en-us/xenmobile/server/media/configure-dha-thumbprint3.png)

5. 选择证书，然后单击 **确定**。

   Windows 添加或删除管理单元的图像(/en-us/xenmobile/server/media/configure-dha-thumbprint4.png)

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。

   Windows 添加或删除管理单元的图像(/en-us/xenmobile/server/media/configure-dha-thumbprint5.png)

7. 将指纹复制到文件。在 PowerShell 命令中使用指纹时，请删除空格。

安装签名和加密证书

在 Windows 服务器上运行这些 PowerShell 命令以安装签名和加密证书。

替换占位符 ReplaceWithThumbprint，并按所示将其括在双引号中。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint
-like "ReplaceWithThumbprint"}



$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
```

```
$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
$keyname icacls $keypath /grant IIS_IUSRS`:R
```

提取 TPM 根证书并安装受信任的证书包

在 Windows 服务器上运行这些命令：

```
mkdir .\TrustedTpm



expand -F:\* .\TrustedTpm.cab .\TrustedTpm



cd .\TrustedTpm



.\setup.cmd
```

配置 DHA 服务

在 Windows 服务器上运行此命令以配置 DHA 服务。

替换占位符 ReplaceWithThumbprint。

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
ReplaceWithThumbprint



-SigningCertificateThumbprint ReplaceWithThumbprint



-SslCertificateStoreName My -SslCertificateThumbprint
ReplaceWithThumbprint
```

```
-SupportedAuthenticationSchema "AikCertificate"
```

在 Windows 服务器上运行这些命令以设置 DHA 服务的证书链策略：

```
$policy = Get-DHASCertificateChainPolicy



$policy.RevocationMode = "NoCheck"



Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

请按如下方式响应这些提示：

```
  Confirm



    Are you sure you want to perform this action?



    Performing the operation "Install-DeviceHealthAttestation" on target
"WIN-N27D1FKCEBT".



    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): A



    Adding SSL binding to website 'Default Web Site'.



    Add SSL binding?
```

```
    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.


    Add application pool?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Adding web application 'DeviceHealthAttestation' to website 'Default
Web Site'.


    Add web application?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Adding firewall rule 'Device Health Attestation Service' to allow
inbound connections on port(s) '443'.


    Add firewall rule?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Setting initial configuration for Device Health Attestation Service.
```

```
Set initial configuration?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Registering User Access Logging.

Register User Access Logging?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

检查配置

要检查 DHASActiveSigningCertificate 是否处于活动状态，请在服务器上运行以下命令：

`Get-DHASActiveSigningCertificate`

如果证书处于活动状态，则会显示证书类型（签名）和指纹。

要检查 DHASActiveSigningCertificate 是否处于活动状态，请在服务器上运行以下命令

替换占位符 ReplaceWithThumbprint 并按所示将其用双引号括起来。

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
-Force


Get-DHASActiveEncryptionCertificate
```

如果证书处于活动状态，则会显示指纹。

要进行最终检查，请访问此 URL：

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1
```

如果 DHA 服务正在运行，则会显示“Method not allowed”。

为 Secure Mail 推送通知配置基于证书的 EWS 身份验证

贡献者：维贾伊·库马尔·昆查库里

为确保 Secure Mail 推送通知正常工作，您必须为 Exchange Server 配置基于证书的身份验证。当 Secure Hub 在 XenMobile® 中使用基于证书的身份验证进行注册时，需要执行此操作。

您需要在 Exchange 邮件服务器上为 Active Sync 和 Exchange Web Services (EWS) 虚拟目录配置基于证书的身份验证。

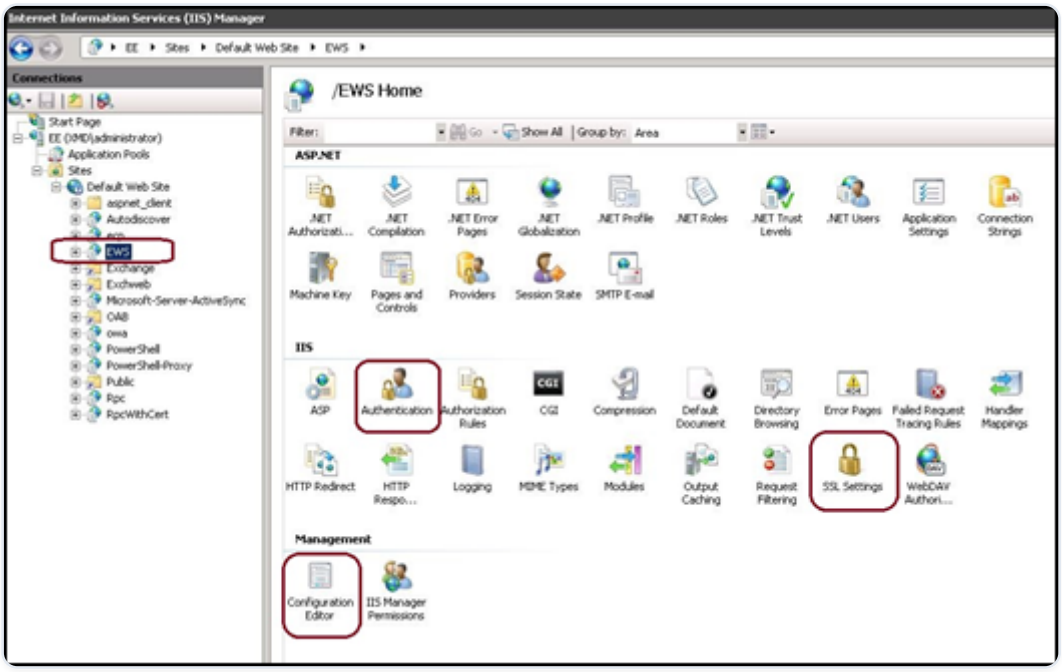
除非您完成这些配置，否则 Secure Mail 推送通知的订阅将失败，并且 Secure Mail 中不会出现徽章更新。

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。

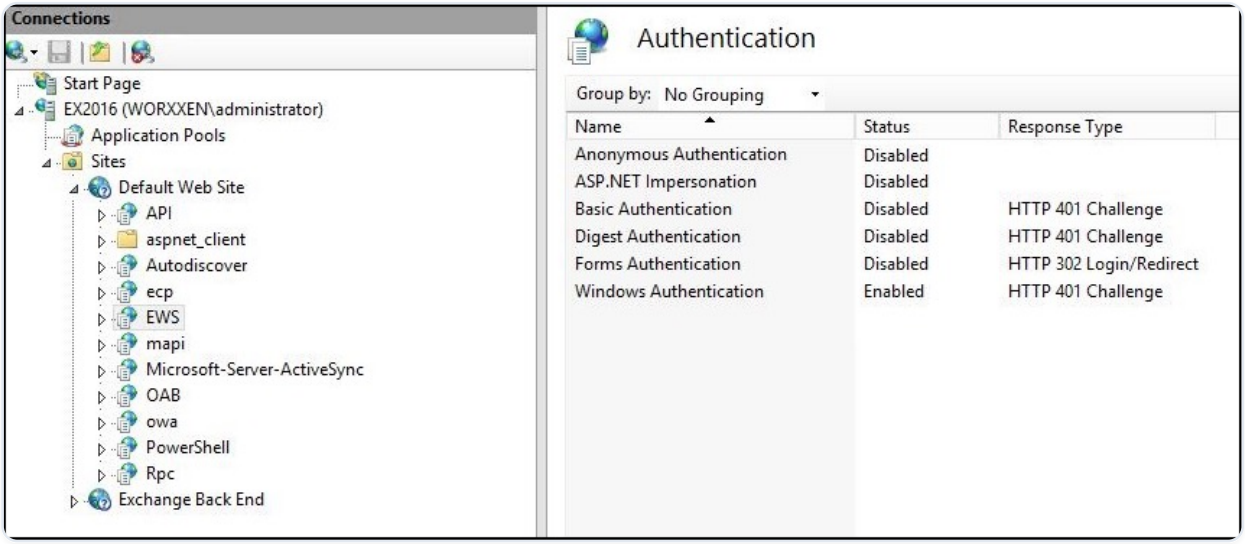
要开始配置，请执行以下操作：

1. 登录到安装了 EWS 虚拟目录的服务器。
2. 打开 IIS 管理器控制台。
3. 在 **默认网站** 下，单击 EWS 虚拟目录。

   身份验证、SSL、配置编辑器管理单元位于 IIS 管理器控制台的右侧



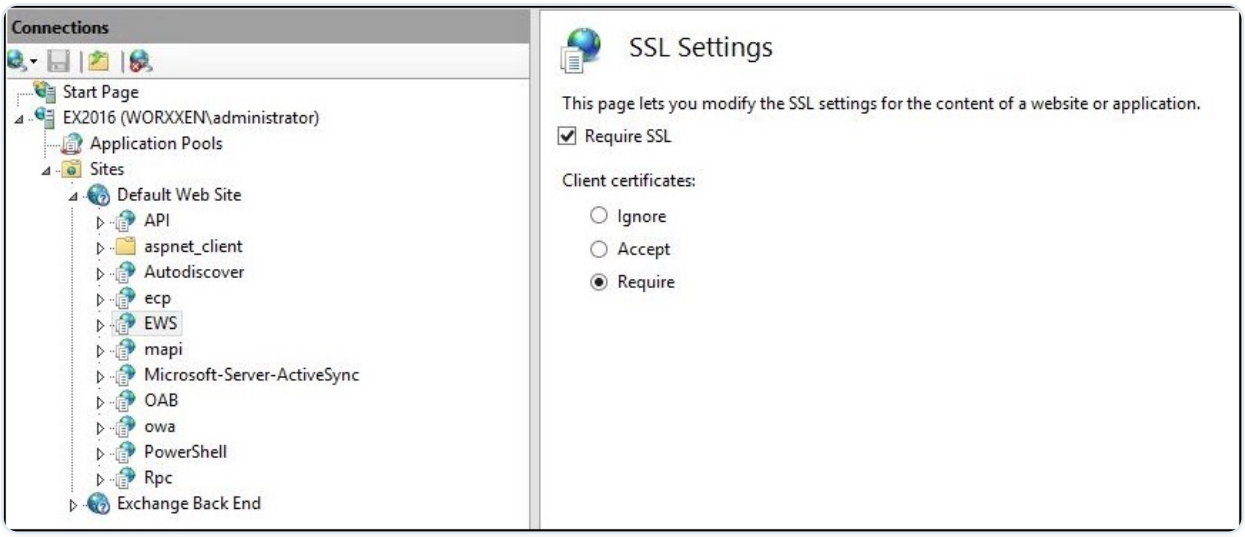
4. 确保 EWS 的 **身份验证** 设置已按以下图示配置。



5. 配置 EWS 虚拟目录的 **SSL 设置**。

   a. 选择“**Require SSL**”复选框。

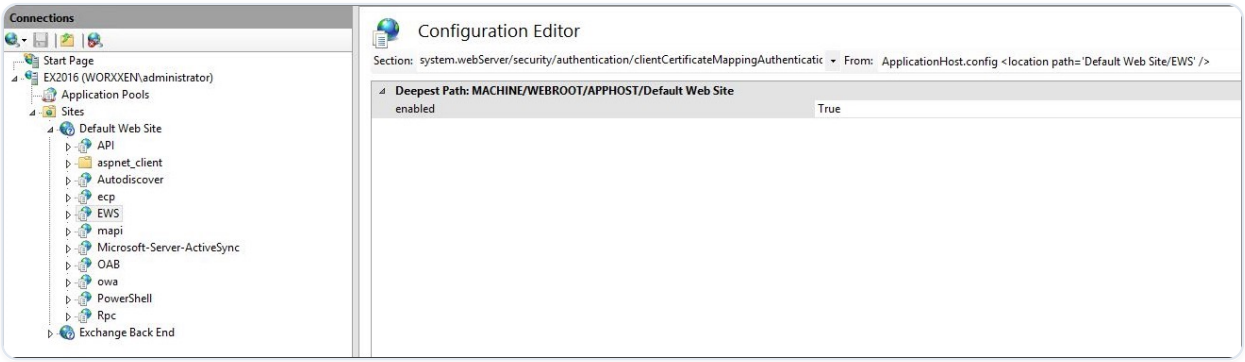
   b. 在“**Client Certificates**”下，单击“**Require**”。如果其他 EWS 邮件客户端使用用户名和密码作为凭据进行身份验证并连接到 Exchange Server，则可以将此选项设置为“**Accept**”。



6. 单击“**Configuration Editor**”。在“**Section**”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**”。在“**Section**”下拉列表中，导航到以下部分：

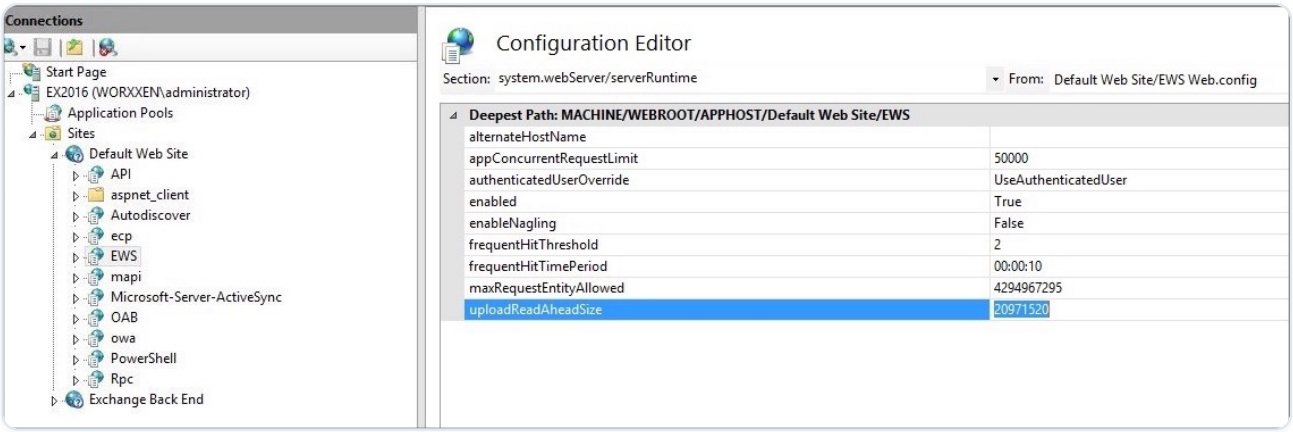
   - **system.webServer/serverRuntime**

9. 将 **uploadReadAheadSize** 值设置为 **10485760** (10 MB) 或 **20971520** (20 MB)，或设置为您的组织所需的值。

> **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



有关解决 iOS 推送通知的 Secure Mail 问题，请参阅此 Citrix 支持知识中心 文章。

相关信息

适用于 iOS 的 Secure Mail 推送通知

集成 XenMobile® 移动设备管理 (MDM) 与 Cisco 身份服务引擎 (ISE)

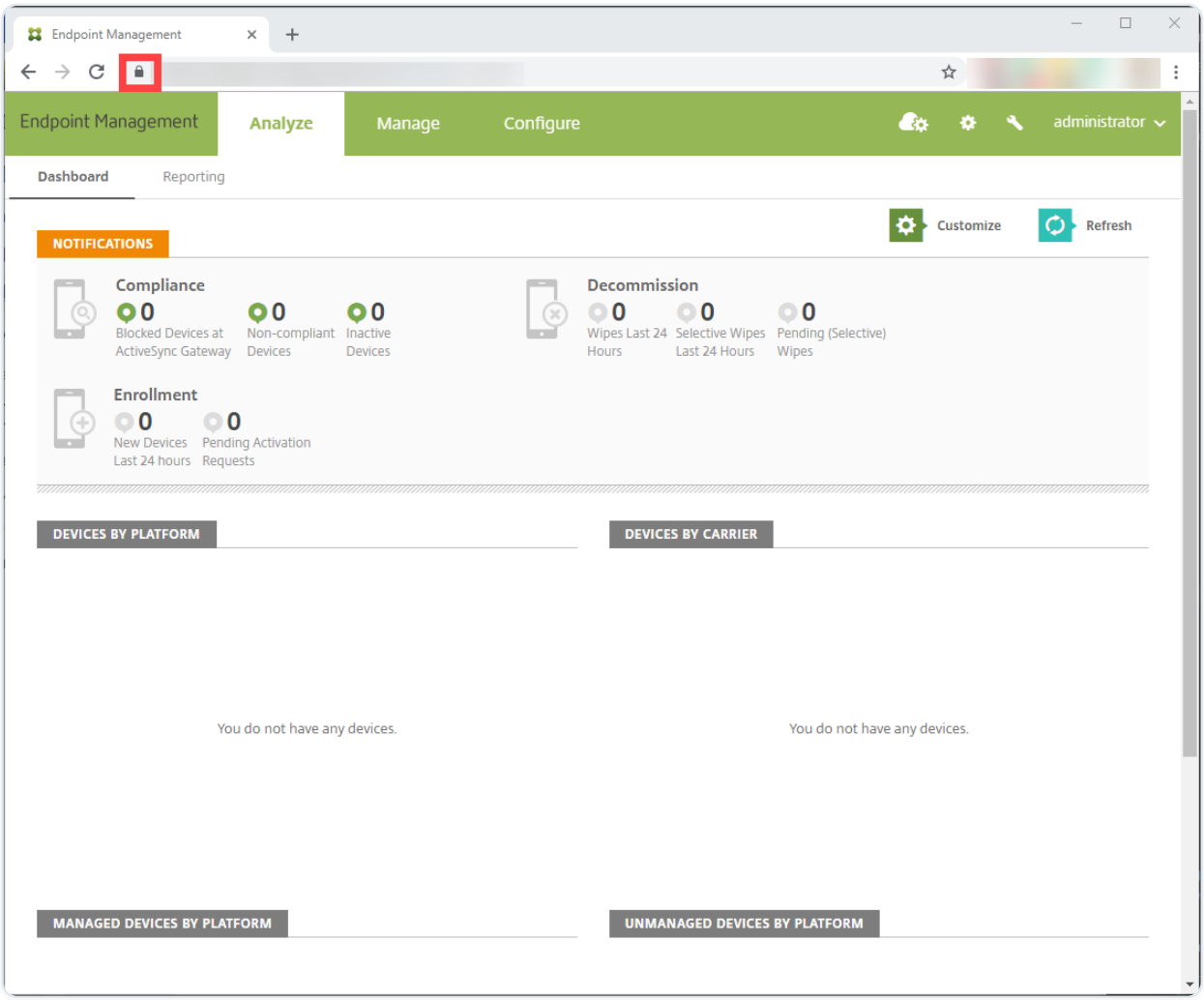
Cisco ISE 用于在工作场所部署、保护、监控、集成和管理移动设备。下载到移动设备上的软件控制以下内容：

- 应用程序和补丁的分发
- 端点上的数据和配置

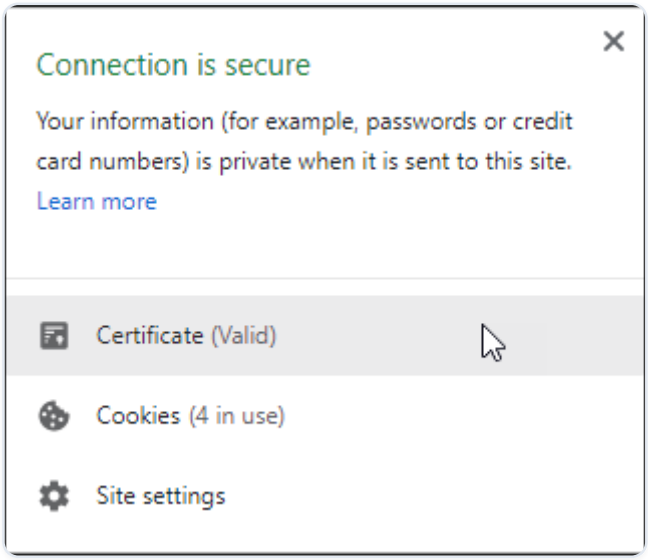
XenMobile 可以与 Cisco ISE 集成，以在 Cisco ISE 控制台上管理不合规和未受管的设备。XenMobile 还允许您选择性地允许、拒绝或隔离对企业服务的访问。

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。

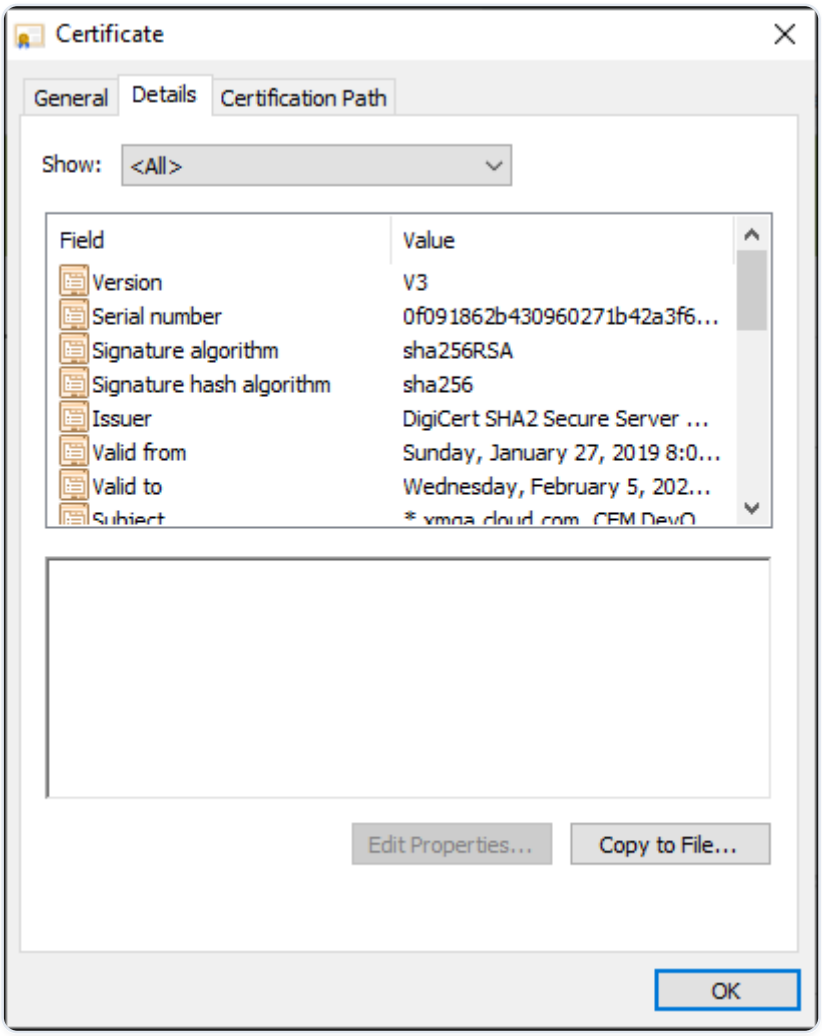
1. 登录后，单击地址栏中 URL 旁边的锁图标。



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. 按照向导将证书保存到本地。
5. 登录到您的 Cisco ISE 控制台，并导入您之前下载的 XenMobile 证书。将证书导入到 Cisco ISE 的受信任证书存储中。这对于 Cisco ISE 信任与 XenMobile Server 的通信是必需的。
   a. 导航到 **管理 > 系统 > 证书 > 证书管理 > 受信任证书**。单击 **导入**。
   b. 为证书命名，并勾选 **信任 ISE 内的身份验证** 和 **信任 Cisco 服务的身份验证** 旁边的复选框。
6. 在 Cisco ISE 中将 XenMobile 添加为外部 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：** 您的 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：** 键入为此任务创建的用户的名称。该用户必须是原始管理员 RBAC 组中的本地管理员帐户。

- **密码：** 您刚刚添加的用户的密码。
- 选中显示 **启用** 的位置。

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。

> **注意：**
>
> ISE 集成不支持托管的 Endpoint Management。

Citrix XenMobile® Server 文档历史记录

下表介绍了 XenMobile Server 产品文档的重要更改。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	描述
27 Jan 2026	XenMobile Server 10.16 滚动修补程序 8 的发行说明	
20 Nov 2025	XenMobile Server 10.15 滚动修补程序 13 的发行说明	
13 Nov 2025	XenMobile Server 10.16 滚动修补程序 7 的发行说明	
23 Oct 2025	XenMobile Server 10.15 滚动修补程序 12 的发行说明	
26 Sep 2025	XenMobile Server 10.16 滚动修补程序 6 的发行说明	
13 May 2025	XenMobile Server 10.15 滚动修补程序 11 的发行说明	请参阅支持文章 CTX693257 。
15 Apr 2025	XenMobile Server 10.16 滚动修补程序 5 的发行说明	请参阅支持文章 CTX692919 。
27 Jan 2025	XenMobile Server 10.15 滚动修补程序 10 的发行说明	请参阅支持文章 CTX692560 。
18 Dec 2024	XenMobile Server 10.16 滚动修补程序 4 的发行说明	请参阅支持文章 CTX692370 。
04 Dec 2024	XenMobile Server 10.15 滚动修补程序 9 的发行说明	请参阅支持文章 CTX692268 。
28 Aug 2024	XenMobile Server 10.16 滚动修补程序 3 的发行说明	请参阅支持文章 CTX691503 。

日期	更改	描述
11 Jul 2024	XenMobile Server 10.15 滚动修补程序 8 的发行说明	请参阅支持文章 CTX691107。
02 Jul 2024	XenMobile Server 10.16 滚动修补程序 2 的发行说明	请参阅支持文章 CTX678043。
17 Jun 2024	XenMobile Server 10.16 滚动修补程序 1 的发行说明	请参阅支持文章 CTX677872。
06 Jun 2024	XenMobile Server 10.15 滚动修补程序 7 的发行说明	请参阅支持文章 CTX677079。
08 Mar 2024	XenMobile Server 10.14 滚动修补程序 13 的发行说明	请参阅支持文章 CTX628921。
06 Mar 2024	XenMobile Server 10.15 滚动修补程序 6 的发行说明	请参阅支持文章 CTX625010。
13 Nov 2023	XenMobile Server 10.15 滚动修补程序 5 的发行说明	请参阅支持文章 CTX583748。
19 Oct 2023	XenMobile Server 10.14 滚动修补程序 12 的发行说明	请参阅支持文章 CTX582535。
18 Sep 2023	XenMobile Server 10.15 滚动修补程序 4 的发行说明	请参阅支持文章 CTX579528。
19 Jul 2023	XenMobile Server 10.15 滚动修补程序 3 的发行说明	请参阅支持文章 CTX565649。
31 May 2023	XenMobile Server 10.14 滚动修补程序 11 的发行说明	请参阅支持文章 CTX558678。
26 Apr 2023	XenMobile Server 10.15 滚动修补程序 2 的发行说明	请参阅支持文章 CTX546782。
11 Apr 2023	向 XenMobile Server 10.14 滚动修补程序 10 的发行说明中添加了一个已修复的问题	请参阅已修复的问题。
23 Mar 2023	XenMobile Server 10.14 滚动修补程序 10 的发行说明	请参阅支持文章 CTX491036。

日期	更改	描述
23 Feb 2023	XenMobile Server 10.15 滚动修补程序 1 的发行说明	请参阅支持文章 CTX478719 。
20 Dec 2022	XenMobile Server 10.14 滚动修补程序 9 的发行说明	请参阅支持文章 CTX477055 。
16 Nov 2022	XenMobile Server 10.15 版本的更新文章	有关新增功能和更改功能的摘要，请参阅 XenMobile Server 10.15 中的新增功能。
22 Sep 2022	XenMobile Server 10.14 滚动修补程序 8 的发行说明	请参阅支持文章 CTX464099 。
08 Sep 2022	XenMobile Server 10.13 滚动修补程序 10 的发行说明	请参阅支持文章 CTX463922 。
18 Aug 2022	XenMobile Server 10.14 滚动修补程序 7 的发行说明	请参阅支持文章 CTX463691 。
14 Jun 2022	XenMobile Server 10.13 滚动修补程序 9 的发行说明	请参阅支持文章 CTX460128 。
23 May 2022	XenMobile Server 10.14 滚动修补程序 6 的发行说明	请参阅支持文章 CTX459871 。
12 Apr 2022	XenMobile Server 10.13 滚动修补程序 8 的发行说明	请参阅支持文章 CTX447596 。
30 Mar 2022	XenMobile Server 10.14 滚动修补程序 5 的发行说明	请参阅支持文章 CTX399411 。
01 Mar 2022	XenMobile Server 10.13 滚动修补程序 7 的发行说明	请参阅支持文章 CTX341602 。
26 Jan 2022	XenMobile Server 10.14 滚动修补程序 4 的发行说明	请参阅支持文章 CTX339069 。
22 Dec 2021	XenMobile Server 10.14 滚动修补程序 3 的发行说明	请参阅支持文章 CTX335897 。
21 Dec 2021	XenMobile Server 10.13 滚动修补程序 6 的发行说明	请参阅支持文章 CTX335875 。

日期	更改	描述
21 Dec 2021	XenMobile Server 10.12 滚动修补程序 11 的发行说明	请参阅支持文章 CTX335861。
16 Dec 2021	XenMobile Server 10.12 滚动修补程序 10 的发行说明	请参阅支持文章 CTX335785。
15 Dec 2021	XenMobile Server 10.14 滚动修补程序 2 的发行说明	请参阅支持文章 CTX335763。
15 Dec 2021	XenMobile Server 10.13 滚动修补程序 5 的发行说明	请参阅支持文章 CTX335753。
19 Nov 2021	XenMobile Server 10.14 滚动修补程序 1 的发行说明	请参阅支持文章 CTX335342。
08 Oct 2021	XenMobile Server 10.12 滚动修补程序 9 的发行说明	请参阅支持文章 CTX331040。
15 Sep 2021	XenMobile Server 10.14 版本的更新文章	有关新增功能和更改功能的摘要，请参阅 XenMobile Server 10.14 中的新增功能。
11 Aug 2021	XenMobile Server 10.13 滚动修补程序 4 的发行说明	请参阅支持文章 CTX324159。
02 Jun 2021	XenMobile Server 10.12 滚动修补程序 8 的发行说明	请参阅支持文章 CTX316910。
13 May 2021	XenMobile Server 10.13 滚动修补程序 3 的发行说明	请参阅支持文章 CTX315034。
27 Apr 2021	更新了“定位”安全操作的描述	请参阅安全操作。
23 Apr 2021	添加了一个操作示例	请参阅自动化操作。
01 Apr 2021	添加了每应用 VPN 要求说明	请参阅 VPN 设备策略。
24 Feb 2021	添加了关于在将端点升级到 iOS 14.5 之前所需准备工作的公告	请参阅在将端点升级到 iOS 14.5 之前。

日期	更改	描述
17 Dec 2020	用于控制 Android Enterprise 上已安装的托管应用如何更新的新设备策略	请参阅自动更新托管应用设备策略
18 Nov 2020	添加了与本地 Citrix ADC 相关的单点登录问题的解决方法	请参阅在升级本地 Citrix ADC 之前。
26 Oct 2020	XenMobile Server 10.13 版本的更新文章	有关新增功能和更改功能的摘要，请参阅 XenMobile Server 10.13 中的新增功能。
02 Jul 2020	添加了 MDX 加密弃用的时间表和行动计划	请参阅为即将到来的更改准备您的 Android 设备。
19 Jun 2020	解决了文档中“黑名单”和“白名单”术语的问题。已更改为“阻止列表”和“允许列表”。	Endpoint Management 控制台目前包含“黑名单”和“白名单”术语。我们已更新文档。我们正在为即将发布的版本更改产品控制台中的术语。
04 May 2020	添加了关于 iOS、iPadOS 和 macOS 中受信任证书的新 TLS 证书要求的说明。	请参阅证书。
18 Feb 2020	更新了术语	在整个文档中，更新了 NetScaler®、NetScaler Gateway、ShareFile 和存储区域控制器术语。某些控制台组件可能仍显示旧名称。
06 Feb 2020	XenMobile Server 10.12 版本的更新文章	有关新增功能和更改功能的摘要，请参阅 XenMobile Server 10.12 中的新增功能。
06 Nov 2019	添加了关于从 Apple VPP 迁移到 ABM 或 ASM 的部分	请参阅Apple 批量采购计划迁移到 Apple Business Manager (ABM) 和 Apple School Manager (ASM)。

日期	更改	描述
04 Sep 2019	XenMobile Server 10.11 版本的更新文章	有关新增功能和更改功能的摘要，请参阅 XenMobile Server 10.11 中的新增功能。
15 May 2019	更新了 iOS 设备注册部分	添加了视频并更新了 iOS 12 设备注册步骤。请参阅注册 iOS 设备。
10 May 2019	关于 Entrust PKI 的新部分	向“PKI 实体”文章中添加了部分：PKI 实体。
03 Apr 2019	关于 Apple DEP 续订步骤的新部分	向“通过 Apple DEP 部署设备”中添加了部分：续订您在 Apple Deployment Program 中的注册。
02 Apr 2019	Exchange ActiveSync 8.5.3 版本的 Gateway 连接器的更新文章	有关新增功能和更改功能的摘要，请参阅 8.5.3 版本中的新增功能。
26 Mar 2019	更新了 Secure Hub 商店名称语法	在应用商店和 Citrix Secure Hub 品牌中添加了关于商店名称的字母数字要求的说明。
06 Mar 2019	Exchange ActiveSync 10.1.9 版本的 Endpoint Management 连接器的更新文章	有关新增功能和更改功能的摘要，请参阅 10.1.9 版本中的新增功能。
01 Feb 2019	Exchange ActiveSync 10.1.8 版本的 Endpoint Management 连接器的更新文章	有关新增功能和更改功能的摘要，请参阅 10.1.8 版本中的新增功能。
23 Jan 2019	更新了 Secure Browse 术语	在整个文档中，将 MDX 设置“Secure Browse”重命名为“Tunneled Web SSO”。有关信息，请参阅适用于 iOS 的应用网络访问和适用于 Android 的应用网络访问。