关于 XenMobile 服务器 10.3.6

Oct 21, 2016

只能从 XenMobile 10.3.5 直接升级到 XenMobile 10.3.6 Service Pack。

> **注意**
>
> 升级到 XenMobile 10.3.6 之前，您的 Citrix 许可证上的专享升级服务 (SA) 日期必须在 2016 年 6 月 1 日以后。 可以在许可证服务器中的许可证旁边查看您的 SA 日期。 要续订许可证上的 SA 日期，请从 Citrix 门户网站下载最新的许可证文件，然后将该文件上载到 Licensing 服务器。 有关详细信息，请参阅 http://support.citrix.com/article/CTX209580。

要执行升级，请使用 xms_10.3.6.310.bin。 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击**版本管理**。 单击**升级**，然后上载 xms_10.3.6.310.bin 文件。 有关在控制台中进行升级的详细信息，请参阅升级 XenMobile。

要完成 XenMobile 10.3.6 的全新安装，请参阅安装 XenMobile。

规划 XenMobile 部署有多个注意事项。 有关您的端到端 XenMobile 环境的建议、常见问题和用例，请参阅 XenMobile Deployment Handbook（《XenMobile 部署手册》）。

XenMobile 10.3.6 中的新增功能

XenMobile 10.3.6 版本侧重于质量和可扩展性。 有关众多缺陷修复的信息，请参阅 XenMobile 10.3.6 中的已知问题和已修复问题。 XenMobile 10.3.6 还包括以下新功能。

改进了可扩展性

XenMobile 10.3.6 服务器的质量明显提高，这样还在许多方面（例如从 XenMobile 服务器到数据库的通信、XenApp 集成、发送到设备的部署通知以及 LDAP 查找）提供了更高的可扩展性和性能。

- 与 XenMobile 10.3.5 相比，HDX 枚举性能大约提高了 40%。
- 现在，在 XenMobile CLI 主菜单（**高级设置**下的选项 **5**）中使用 **Server Tuning**（服务器调整）命令时，适用于以下设置的默认值有所差别，如下所示：

  Maximum connections on port 443（端口 443 上的最大连接数）：默认值从 **10000** 更改为 **12000**。

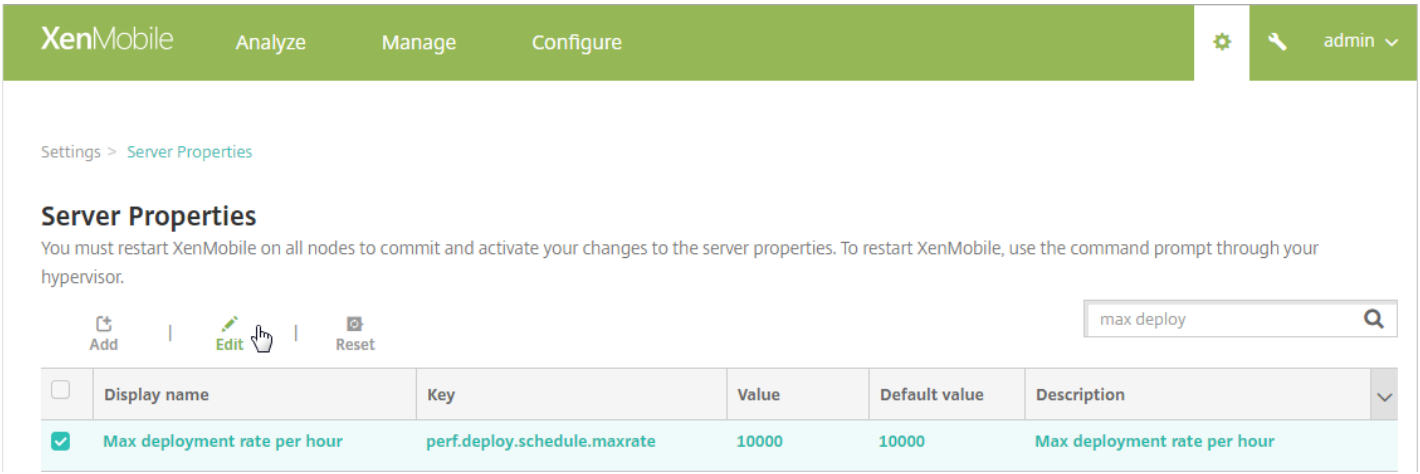
  Maximum connections on port 8443（端口 8443 上的最大连接数）：默认值从 **10000** 更改为 **12000**。

  Maximum threads on port 443（端口 443 上的最大线程数）：默认值从 **750** 更改为 **2000**。

  Maximum threads on port 8443（端口 8443 上的最大线程数）：默认值从 **750** 更改为 **2000**。

- 现在，XenMobile 将在分阶段部署中发送通知，以避免来自 iOS 和 Windows Phone 设备的重新连接请求以及为 Google Cloud Messaging 配置的 Android 设备的重新连接请求出现峰值。 默认部署速率为每小时 10000 台设备。 要更改此部署速率，请编辑 **Max deployment rate**（最大部署速率）服务器属性 (perf.deploy.schedule.maxrate)。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- 现在，XenMobile 部署操作仅针对目标交付组中的设备。 以前，无论角色为何，都会部署所有设备。

Worx 应用程序更新

Worx Home

- **通过 WorxMail 发送日志**。 现在，当用户在报告问题期间发送日志时，默认情况下会打开 WorxMail。 这使得用户能够成功发送大型文件。 在早期版本或 Worx Home 中，有时无法发送大型文件。

WorxMail

- **支持 Exchange Server 2016**。 现在可以将 WorxMail 集成到 Exchange Server 2016。 支持 Active Sync 14，但 WorxMail 也应与 Active Sync 16 兼容。
- **从 ShareFile 附加文件 (Android)**。 用户可以轻按**从 ShareFile 附加**将文件附加到电子邮件或日历事件中。
- **从 ShareFile 受限 StorageZones 和连接器附加文件 (iOS)**。 当用户在电子邮件或日历事件中轻按**从 ShareFile 附加**时，他们不仅能够从 ShareFile 附加文件，还能够从受限 StorageZones 和连接器（例如从 SharePoint 和网络共享）附加文件。
- **与 .vcard 文件共享联系人数据**。 用户可从以 .vcard 文件格式发送的附件中导入联系人信息。
- **新网络访问默认设置**。 MDX Toolkit 中的**网络访问**策略现在默认为**通过通道连接到内部网络**。 此更改将减少配置错误。

WorxWeb

- **默认情况下阻止弹出窗口**。 如果您需要在默认情况下阻止 Safari 浏览器的弹出窗口，请使用 XenMobile 控制台将**限制**设备策略选项**阻止弹出窗口**设置为**开**。 如果在升级到 10.3.6 版本之前已将**阻止弹出窗口**设置为**关**，则此设置仍会处于关闭状态。 否则，此设置为**开**状态，并阻止 Safari 弹出窗口。
- **在 ShareFile 中打开链接**。 ShareFile 4.0 允许用户选择是在浏览器中还是直接在 ShareFile 中打开链接。

WorxChat 技术预览版

- **支持 Android**。 现在可以在 Android 上使用 WorxChat。
- **支持 Lync 2013 和 Skype for Business 2015**。 可以在同一个池中集成 WorxChat 与 Lync 2013 和 Skype for Business 2015。

Secure Forms

- **支持 ShareFile Restricted Zones**。 现在，您可以通过 ShareFile Restricted Zones 配置 Secure Forms。 请按照将 Secure Forms 与 ShareFile 集成中的安装说明执行操作。
- **iBeacon 功能**。 通过使用 iBeacon 技术，您可以配置和跟踪信标。信标允许用户在移动应用程序上自动填充表单。 当用户

© 1999-2017 Citrix Systems, Inc. All rights reserved.

提交表单时，将包含信标信息。 有关如何设置信标的信息，请参阅信标。

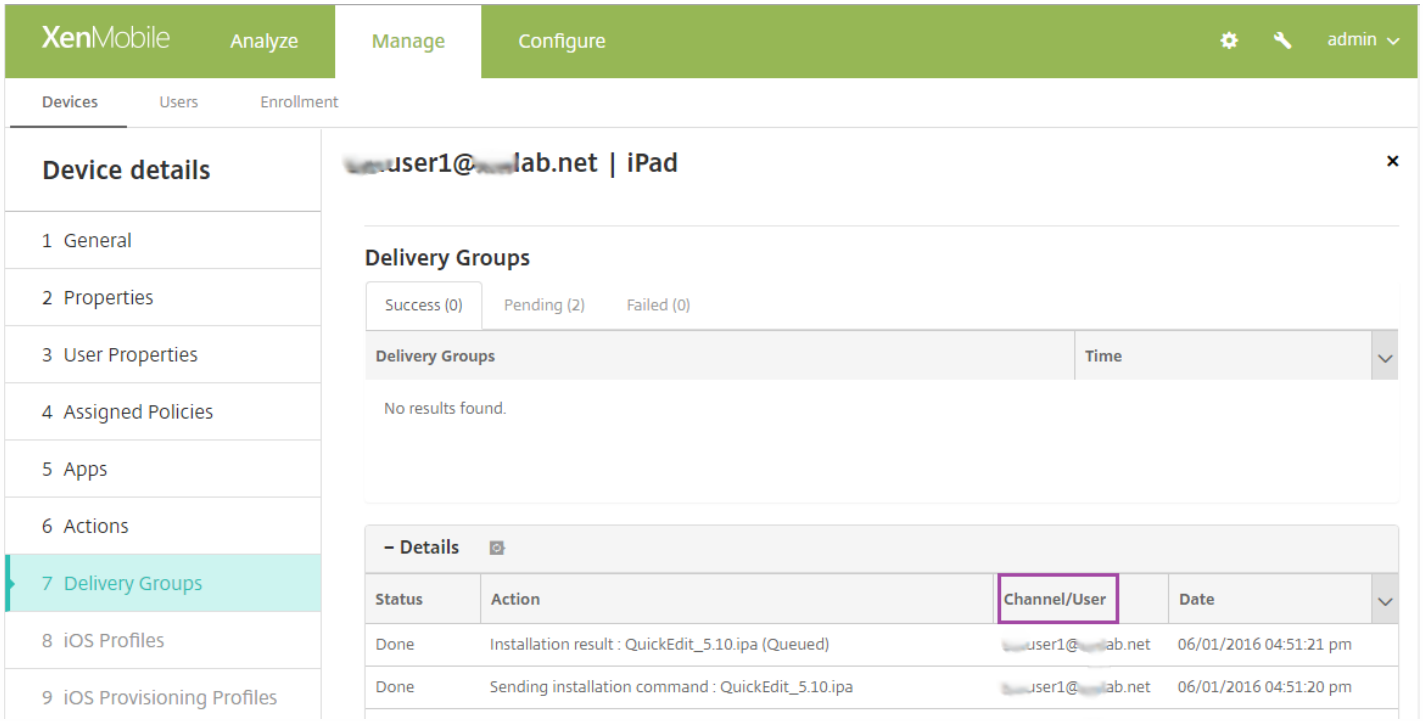
- **创建者姓名**。 Secure Forms Composer 现在可显示表单创建者的姓名。 当有多个用户访问 Composer 时，此功能可帮助执行跟踪操作。
- **编号范围**。 在 Composer 上的**编号**字段中，您可以指定一个编号范围，使用户能够在填写表单时输入这些编号。
- **新文件名格式。** 现在，会以含提交者姓名和时间戳的文件名保存在移动应用程序上提交的表格和附件，使得文件名更易于阅读和整理。

有关详细信息，请参阅 Worx 移动应用程序中的新增功能。

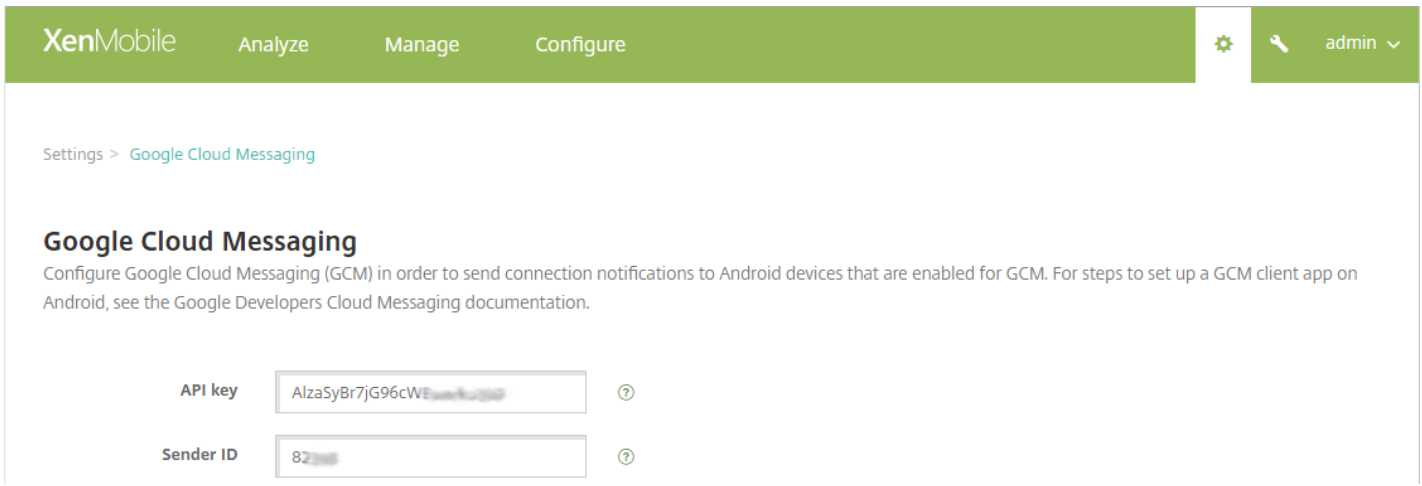
其他更新

- **支持其他 Citrix 组件版本。**
  - NetScaler Gateway 10.5.x、11.0.x 和 11.1.x（XenMobile 本地部署）
  - NetScaler Gateway 10.5.57.7 (XenMobile Cloud)
  - XenApp 以及 XenDesktop 7.9 和 7.8
  - StoreFront 3.6
  - 许可证服务器 11.13.1.2
- **列入白名单的 WiFi 网络。** “列入白名单的 WiFi 网络”策略允许您指定允许的网络。 应用程序仅会在连接到所列网络之一的情况下工作。 此功能仅在 MDM+MAM 模式下可用。
- **针对共享设备的 ShareFile 支持。** 现在，ShareFile 移动应用程序 4.4 版本在 MDM + MAM 模式中支持共享设备，从而允许多个用户共享一个设备，而无需重新注册。 有关详细信息，请参阅 XenMobile 中的共享设备。
- **图标操作 (iOS)。** 应用程序开发人员现在可以将图标文件放置在应用程序捆绑包根文件夹中，以替代将其放置在 info.plist 中的通常做法。 为了使工具包能够找到图标文件，图标文件的名称必须具有下列格式之一：
  - icon.png
  - icon-60x2.pn
  - icon-72.png
  - icon-76.png
- **改进的邮件同步 (iOS)。** 更新了邮件同步和 ShareFile 集成，使得邮件同步过程更可靠。
- **其他设备信息。** 现在，XenMobile 控制台中的**设备详细信息**页面包括**通道/用户**列，其中显示了设备上的部署操作的目标。 目标可能会显示已注册设备的用户、共享设备上的签入用户或者不绑定到特定用户的系统级设置或部署操作。 可以使用此信息来更好地跟踪部署过程，尤其是当您在特定平台（如 Mac OS X）上有很多将处理一个设备或多个容器的用户时。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



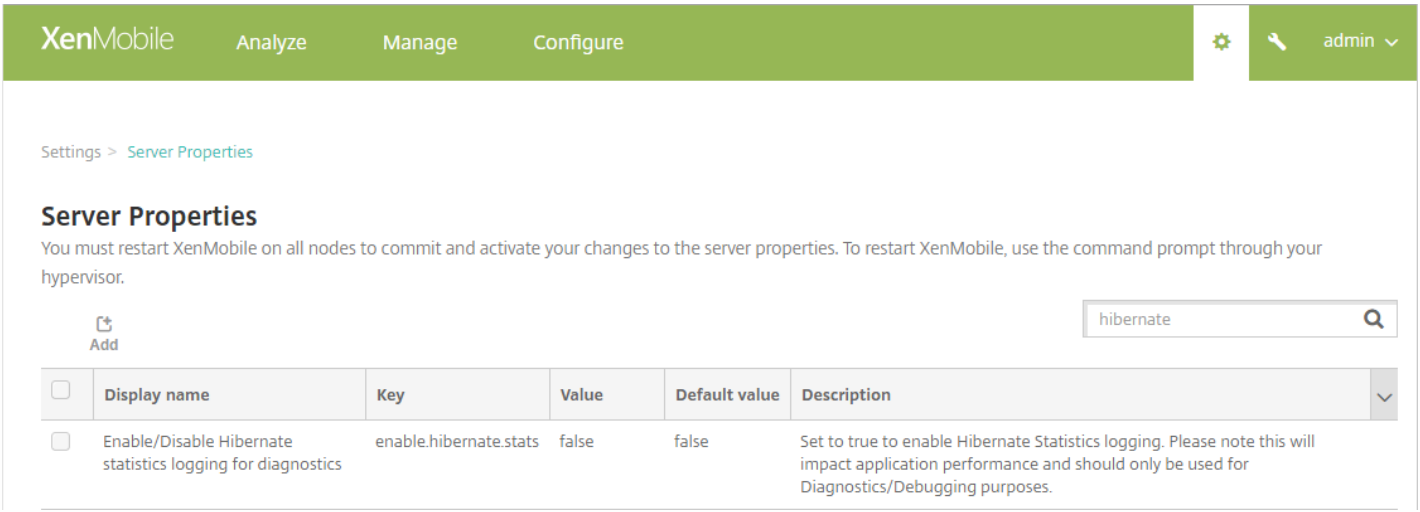
- **新 XenMobile 控制台页面。**XenMobile 控制台中包括一个新页面（即**设置 > Google Cloud Messaging**），您可以在此页面中指定 GCM **API key**（API 密钥）和 **Sender ID**（发件人 ID）。 以前这些项目只会出现在**服务器属性**中。



- **用于执行诊断的 Hibernate 统计日志。** 为了帮助排除应用程序性能问题，XenMobile 现在可提供针对 Hibernate（一个用于 XenMobile 与 Microsoft SQL Server 的连接的组件）的统计日志记录功能。

  要启用 Hibernate 统计日志记录功能，请将 **Enable/Disable Hibernate statistics logging for diagnostics**（启用/禁用用于执行诊断的 Hibernate 统计日志）服务器属性 (enable.hibernate.stats) 更改为 **true**。 默认情况下，此日志记录功能已禁用，因为它会影响应用程序的性能。 只应在短时间内启用日志记录功能，以避免生成巨大的日志文件。 XenMobile 将此日志写入 /opt/sas/logs/hibernate_stats.log。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **Android 应用商店中的更新。** 只有当 Android 设备上安装的版本比应用商店中的版本低时，Android 应用商店才会显示更新的应用程序版本。
- **XenMobile Analyzer 工具。**如果您的 XenMobile 环境出现问题，联系 Citrix 技术支持可能会消耗贵组织的时间和金钱。借助 XenMobile Analyzer，您可以在联系技术支持之前自己诊断常见问题。 XenMobile Analyzer 工具支持众多用例和部署选项（包括 MDM、MDM+MAM 以及仅 MAM）、5 个不同的身份验证方案以及 iOS 和 Android 移动环境。

  XenMobile Analyzer 可以执行以下操作：
  - 检查您的环境中存在的问题并建议解决方案。 XenMobile Analyzer 环境检查功能可以识别设备问题、用户注册问题和身份验证问题。
  - 引导您完成相关步骤以接收高级诊断结果。
  - 指导您使用工具检查 WorxMail Readiness 以及服务器连接检查。
  - 如果全部失败，该工具将提供指向 Citrix 支持的直接链接。

  有关详细信息，请参阅 XenMobile Analyzer 工具。
- **XenMobile 自动发现服务。**迄今为止，激活自动发现需要创建支持票据。 您可以自己在自动发现服务门户中设置自动发现。 该服务将引导您完成声明您的域并创建自动发现记录的步骤。 有关详细信息，请参阅 XenMobile 自动发现服务。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 10.3.6 中的已知问题和已修复问题

Aug 11, 2016

XenMobile 10.3.6 中的已知问题或已修复问题如下：

已知问题

用户尝试使用 Microsoft 工作帐户注册其个人设备时，注册失败。 [#597037]

用户通过 Azure Active Directory 帐户在 XenMobile 中注册时，即便擦除或吊销了设备，他们也可在未经授权的情况下重新注册。 这是第三方问题。 [#628865]

将 XenMobile 更新到 10.3.6 后，在群集配置中 iOS 设备注册可能会失败。 解决方法：参阅此知识中心文章。 [#650061]

已修复的问题

尝试访问 XenMobile 控制台的 XenMobile 管理员可能会被引导至 XenMobile 自助门户。 当使用基于角色的控制访问来创建 XenMobile 管理员组并将此组从一个 Active Directory OU 移到另一个 Active Directory OU 时，可能会发生这种情况。 [#585032]

此修补程序可确保当用户设置日志文件大小和最大备份日志文件数时，这些值在 XenMobile 中正确配置，并且文件正常滚动。 但是，XenMobile 控制台可能无法反映更新的值，如已知问题 #551199 中所述。 [#597772]

在包含统一 MDM 和 MAM 的 XenMobile 版本中，iOS 设备有时可能无法进行完整注册。 设备可能已进行 MDM 注册但未进行 MAM 注册，或者已进行 MAM 注册但未进行 MDM 注册。 [#610847]

当您为 Windows 配置 Exchange ActiveSync 设备策略并在部署规则中设置**仅当之前的部署失败时**选项时，会出现以下问题：在 Windows Phone 用户更改 Exchange Server 邮件同步时间后，XenMobile 下次向 Windows 设备推送 Exchange ActiveSync 策略时将覆盖用户的更改。 [#616725]

在数据库包含大量数据的情况下，当您在 XenMobile 控制台中搜索设备或用户时，会出现 SQL Server CPU 利用率峰值，并且搜索过程可能需要 1 分钟以上的时间。 [#618371]

当 iOS 设备上的用户在 Worx Home 中注册时，Worx Home 有时会停止响应达两分钟，然后才会提示用户创建 Worx PIN。 出现此问题后，当用户打开 WorxStore 时，Worx Home 会再次停止响应。 [#619945]

从 XenMobile 服务器向运行 Windows 10 的设备发送 SMS 通知的尝试可能会失败。 [#621229]

向包含 1500 个以上成员的父组添加子 Active Directory 组时，您在 XenMobile 控制台中执行的操作（例如交付组分配）不会应用到所添加的子组中的用户。 [#622523]

注册 iOS设备后，系统不会提示用户安装必需的应用程序，直至其打开 WorkStore 或尝试手动添加应用程序。 [#622789]

在从 XenMobile 9.0 升级到 XenMobile 10.1，并将 LDAP 选项“用户搜索依据”设置为 sAMAccountName，然后升级到 XenMobile 10.3.x 后，用户将无法在 Worx Home 中执行身份验证。 [#624340]

如果显式 UPN 与用户隐式 UPN 不匹配，策略部署和 RBAC 角色分配操作可能会失败。 [#624612]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在群集化服务器部署中，涉及到 Hazelcast 分布式图和 SQL Server 连接的问题可能导致 XenMobile 服务器间歇性不响应，阻止登录并造成注册失败。 [#624931]

当 Android 设备首次连接或重新连接到 XenMobile 服务器时，Android 应用程序下载缓慢或无法下载。 [#625199]

如果将其名称或说明信息中包含 ASCII 字符 16（数据行转义字符）的公用应用程序添加到 XenMobile 控制台，可能无法为 Worx Home 10.3 用户显示应用程序列表。 [#627059]

如果 Hazelcast 分发图已实现，群集服务器可能会间歇性停止响应。 [#627114]

将两个服务器实例升级到 XenMobile 10.3 后，在运行一段时间之后，第一台服务器变得无法响应。 [#628270]

成功注册后，iOS 设备有时无法登录到 WorxStore，并显示以下消息：“无法获取所需的资产以继续。 请重试。”之所以出现此问题，是因为 XenMobile 服务器无法通过 MAM 设备 ID 找到设备。 [#629900]

从 XenMobile 控制台中删除的设备继续允许访问 MAM 资源。 [#630137]

有时，会选择性地为 iOS 用户执行擦除。 [#630466]

在 XenMobile 10.3.x 中，Worx Home 的类别视图可能无法显示 HDX 应用程序。 默认情况下，以前 XenMobile 版本的类别视图中可能不会显示其中包含 HDX 应用程序的“Other”（其他）文件夹。 [#631439]

当用户注册设备时，MDM 注册成功，但 MAM 注册偶尔会失败并出现错误，并且您的应用程序将被锁定。 [#632073]

在 Android SDK 版本 22 或更高版本或者 Obfuscated with Dexguard 中编译的 Android 应用程序无法上载到 XenMobile。 [#632146]

用户在 Worx Home 中注册后，系统会间歇性提示用户卸载并重新安装 Worx Home。 [#633095]

当您执行选择性擦除、完全擦除或在 XenMobile 控制台中删除帐户或设备时，有时不会为设备中已配置的应用程序释放关联的 VPP 许可证。 [#633366]

某些 VPP 许可证的 ID 为负数，例如 -123441212，以致于无法分发公共应用程序。 [#631443]

当用户注册设备时，Worx Home 偶尔会崩溃，并显示 403 错误消息，指出应用商店已被锁定。 此外，用户可能会注册成功，但在下载应用程序时，会出现同样的错误，或出现错误并显示“无法获取详细信息。”[#633515]

当用户尝试在 XenMobile 控制台中通过共享密钥为基于 Windows 的设备配置 WiFi 设备策略时，在他们将身份验证类型更改为 WPA Personal 或 WPA-2 Personal 后，共享密钥选项不按预期显示。 [#633897]

如果已将 NetScaler 配置为转发代理，XenMobile 10.3 连接性检查过程会返回错误的结果。 [#633902]

升级到 XenMobile 10.3.5 后，设备不再在 MAM 模式中注册。 此外，对于在 MDM+MAM 模式中注册的设备，策略和应用程序部署将失败。 [#634034]

在含有统一 MDM 和 MAM 的 XenMobile 版本中，如果在 LDAP 设置中将“用户”搜索字段设置为 samAccountName，针对“授权 DEP”设备的 MAM 身份验证过程可能会失败。 因此，Worx Home 注册操作可能无法完成，并且设备可能仅会在 MDM 中注册。 [#637599]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 可扩展性和性能

Oct 21, 2016

理解扩展 XenMobile 基础结构在确定如何部署和配置 XenMobile 方面起着重要作用。 本文回答了与确定小型至大型企业部署的要求相关的常见问题。

性能和可扩展指南

本文中的数据可用作确定 XenMobile 10.3.6 基础结构的性能和可扩展性的指南。 用于确定如何配置服务器和数据库的两个关键因素是可扩展性（最大用户/设备数）和登录率。

- 可扩展性定义为执行所定义工作负载的最大并发用户数。 有关加载 XenMobile 基础结构的流程的详细信息，请参阅工作负载。
- 登录率定义为新用户的加入和现有用户的身份验证。
  - 加入率是指环境中首次可以注册的最大设备数。 本文中称为首次利用率或 FTU，此数据点在制定推行策略时非常重要。
  - 现有用户率：向环境进行身份验证的最大用户数，这些用户已经注册并连接其设备。 这些测试包括为已经注册的用户创建会话和执行 WorxMail 和 WorxWeb 应用程序。

下表显示了基于相应 XenMobile 环境测试结果的可扩展性指南。

可扩展性	最多 45,000 台设备	
登录率	加入率 (FTU)	每小时最多 833 台设备
	现有用户数	每小时最多 2,812 台设备
配置	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile 服务器 6 节点群集
	数据库	Microsoft SQL Server 外部数据库

> **Important**
>
> 本报告的自动化要求为 1000 到 60,000 台设备。 任何超过 60,000 台设备的要求都不在本报告范围内。

测试配置文件配置

本部分内容介绍用于每个硬件配置的测试配置文件以及用于派生本文中的测试结果的工作负载的 Active Directory 配置、XenMobile 策略的数量、应用程序的数量和类型、模拟用户操作和模拟管理员操作。

> **注意**
>
> 此测试配置文件旨在使用更多资源，而非仅使用用于测试早期 XenMobile 版本的可扩展性的配置文件。 因此，这些测试结果与来自早期版本的可扩展性结果没有直接可比性。

Active Directory (AD) 配置：

- 100000 个唯一的 AD 用户
- 200000 个唯一的 AD 组
- 适用于 AD 组的 5 个嵌套级别
- 每个 AD 组 200 个用户

交付组：

- 20 个交付组
- 50 个分配给交付组的应用程序
- 每个交付组 10 个 AD 组

XenMobile 设备策略：

- 300 个设备策略
- 每个用户 20 个设备策略

应用程序：

- 200 个来自公共应用商店的本机应用程序
- 50 个本机企业分发应用程序
- 100 个 Web 即服务和软件即服务 (SaaS) 应用程序
- 每个用户 50 个应用程序

XenMobile 用户操作：

- 共配置 50 项操作
- Worx Store 启动：
  - 新用户 (FTU)：4
  - 老用户 (RU)：1
- 应用程序启动：
  - MDX：1
  - Web/SaaS：1
- 每个用户 150 个 STA 验证

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 管理员操作：

- 枚举设备（以模拟技术支持呼叫场景）：每 8 小时执行 32 次操作，每隔 15 到 20 分钟执行一次。
- 生成报告：每 8 小时生成 2 次。

系统配置和测试结果

本部分描述运行加入 (FTU) 工作负载和现有用户工作负载可扩展测试所使用的硬件配置和结果。

下表定义了 XenMobile 从 1000 台设备扩展到 60,000 台设备时采用的硬件和配置建议。 这些指南基于测试结果及其相关工作负载。 建议考虑了退出条件中定义的可接受误差范围。

通过分析测试结果得出以下结论：

- 登录率是确定系统可扩展性的重要因素。 除了初始登录，登录率还与环境中配置的身份验证超时值相关。 例如，如果将身份验证超时值设置的太低，用户执行的登录请求会更加频繁。 因此，您需要清楚理解超时设置对环境的影响。
- NetScaler 上每个用户会话的连接数量是一个重要的考虑因素。
- 为实现最大可扩展性，增加了 XenMobile 上的 CPU 和 RAM 资源。
- 6 个节点的群集配置是经过验证的最大配置。 扩展到大于 6 个节点需要其他 XenMobile 实现。

下表显示了基于 XenMobile 配置、NetScaler Gateway 设备、群集设置和数据库得出的建议加入率和现有用户登录率。 使用此表中的数据构建新部署的最优注册计划和现有部署的返回用户/设备率。 “配置”部分将注册和登录性能数据与相应的硬件建议关联起来。

预期设备数	1000	10000	30000	45000
实际设备数	1000	9998	29977	44991
登录率				
加入率 (FTU)	250	625	833	833
现有用户数（仅限 Worx）	1000	1666	3750	883
配置				
参考环境	VPX-XenMobile 独立模式	MPX-XenMobile 独立模式	MPX-XenMobile 群集 (3)	MPX-XenMobile 群集 (6)
NetScaler Gateway	VPX，带 2 GB RAM 2 个虚拟 CPU	MPX-10500	MPX-11500	MPX-11500
XenMobile - 模式	独立*	独立*	群集	群集
XenMobile - 群集	不适用	不适用	3	6
XenMobile - 虚拟设备	8 GB RAM 和 4 个虚拟 CPU	8 GB RAM 和 4 个虚拟 CPU	16 GB RAM 和 6 个虚拟 CPU	16 GB RAM 和 8 个虚拟 CPU
Active Directory (AD)	8 GB RAM 和 4 个虚拟 CPU	8 GB RAM 和 4 个虚拟 CPU	16 GB RAM 和 4 个虚拟 CPU	16 GB RM 和 4 个虚拟 CPU
数据库	外部	外部 – Microsoft SQL Server 内存：16 GB vCPU = 12	外部 – Microsoft SQL Server 内存：32 GB vCPU = 12	外部 – Microsoft SQL Server 内存：48 GB vCPU = 16

MPX-XenMobile 群集 (3)

群集

群集

群集

群集

8 GB RAM 和 4 个虚拟 CPU

© 1999-2017 Citrix Systems, Inc. All rights reserved.

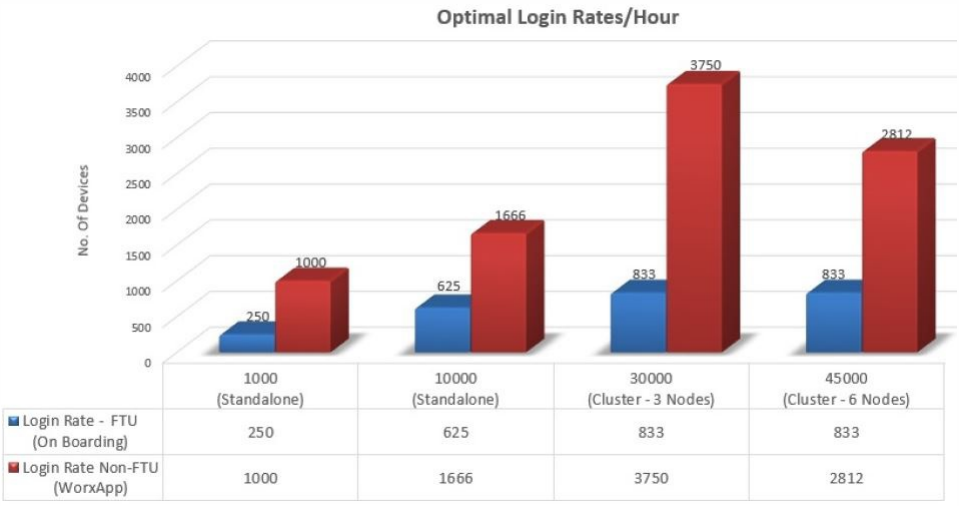
8 GB RAM 和 4 个虚拟 CPU

* 不建议对必须对用户高度可用的应用程序应用独立部署。 Citrix 建议对大多数客户应用高可用性群集化部署。

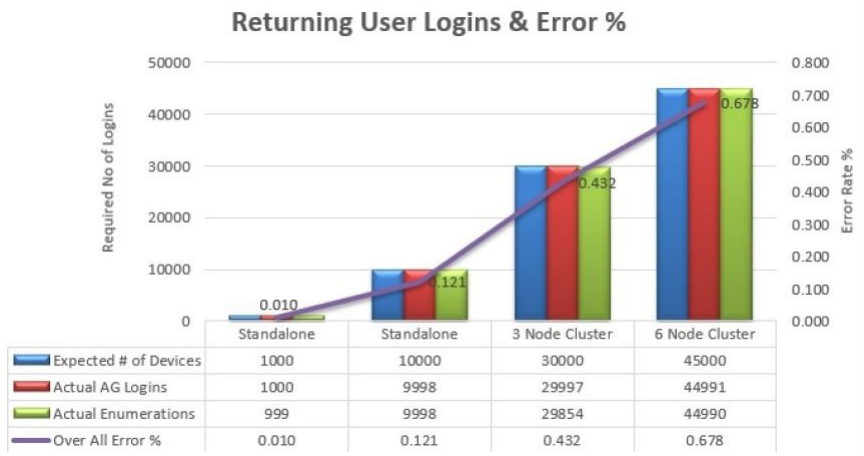
注意：调整系统时，如果超过建议的比率或硬件建议，会遇到以下问题。

以下信息提供了记录的额外数据点以及
影响上表中的结果的额外数据点。

- 注册或登录延迟（往返时间）
  - 平均总延迟：0.5 到 1.5 秒
  - NetScaler Gateway 登录的平均延迟：> 120 到 440 毫秒
  - Worx Store 请求的平均延迟：2 到 3 秒
- 达到扩展限制时，基础结构组件上会出现物理性能下降的情况，如 CPU 和内存耗尽。
  - NetScaler Gateway 和 XenMobile 设备上出现无效响应。
  - 高负载期间会延缓 XenMobile 控制台的响应时间。



	1000 (Standalone)	10000 (Standalone)	30000 (Cluster - 3 Nodes)	45000 (Cluster - 6 Nodes)
Login Rate - FTU (On Boarding)	250	625	833	833
Login Rate Non-FTU (WorxApp)	1000	1666	3750	2812

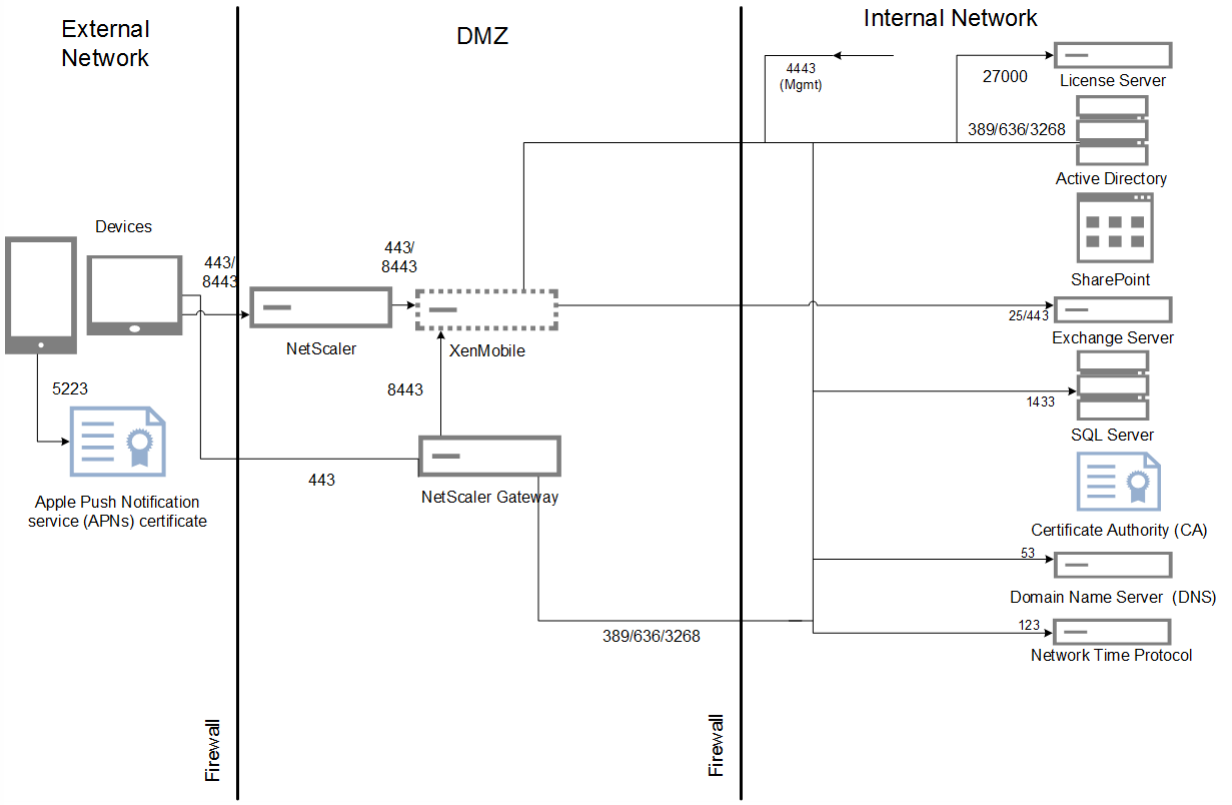


	Standalone	Standalone	3 Node Cluster	6 Node Cluster
Expected # of Devices	1000	10000	30000	45000
Actual AG Logins	1000	9998	29997	44991
Actual Enumerations	999	9998	29854	44990
Over All Error %	0.010	0.121	0.432	0.678

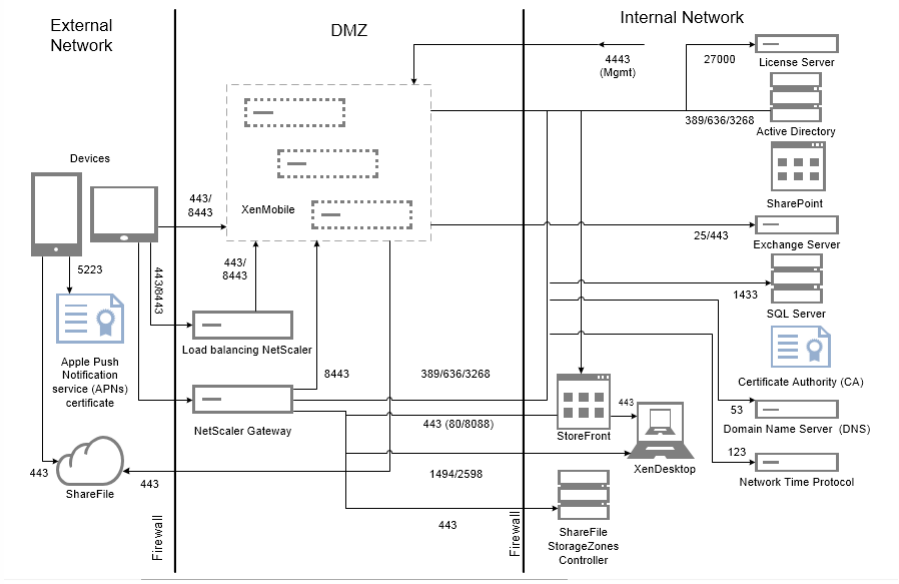
上图中的错误百分比包括遇到的总错误，考虑了每个操作对应的请求，并非仅限于登录。 根据退出条件中的定义，运行的每个测试的错误百分比都在可接受的限制 (1%) 内。

下图显示了小型部署的参考体系结构。 这是一个最多支持 10000 台设备的独立体系结构。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



下图显示了企业部署的参考体系结构。 这是一个群集体系结构，带有通过 HTTP 进行 SSL 卸载的 MAM 功能，可支持 10,000 台或更多设备。



测试方法

测试针对 XenMobile Enterprise 运行以建立标准。 为了同时面向小型和大型部署，测试使用了 1000 至 60,000 台设备。

创建工作负载以模拟实际使用情况。 针对每个测试运行这些工作负载，以了解对注册和登录率的影响。 测试的目的是为了在退出条件中描述的可接受误差范围内，获取最优登录率。 登录率是确定基础结构组件的硬件配置建议的关键因素。

加入 (FTU) 工作负载登录请求包括自动检测、身份验证和设备注册操作。 应用程序订阅、安装和启动操作在测试期间统一分发。 这样提供了对用户操作的最真实模拟。 在测试的结尾，注销会话。 现有用户工作负载登录请求仅包括身份验证请求。

工作负载

用户工作负载的定义如下：

用户会话/设备数	每个会话包括 NetScaler Gateway 登录、枚举、设备注册等。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Worx Store 启动	用户多次启动 Worx Store，每次订阅或安装多个应用程序，不管这些应用程序是移动应用程序 (web/SaaS/MDX) 还是 Windows 应用程序 (HDX)。
每台设备的 Web/SaaS 应用程序 SSO	web/SaaS 应用程序的启动序列的帐户数达到标识点，XenMobile 完成 SSO 并返回实际应用程序 URL。 流量不发送给实际应用程序。
每台设备的 MDX 应用程序下载数	MDX 应用程序的下载总数（可能会发生在两次 Worx Store 启动之间）。 对于 iOS，此数据还包括 Apple ITMS 的应用程序自动安装，Apple ITMS 利用 NetScaler Gateway 上的新令牌/tms 服务 API。

注意事项与假设

可扩展性测试不包括以下场景。 在以后增强扩展测试功能时会考虑这些场景：

- 未测试软件包部署。
- 未测试 Windows 平台。

已针对 iOS 和 Android 设备测试策略推送功能。
每个 XenMobile 最多同时支持 10000 个连接。

测试采用 LAN 在理想连接状态下运行，以避免网络延迟问题。 在实际场景中，可扩展性还取决于用户的可用带宽，尤其是应用程序下载问题。

“重新连接”测试

“重新连接”测试已与“首次使用”测试和“返回用户场景”测试分开完成。

“重新连接”测试已针对多达 15000 台设备运行。

Android 支持的重新连接率为每秒 17 台设备。 iOS 的重新连接率为每秒 8 台设备。 为实现此目标，已在 /opt/sas/tomcat/conf/server.xml 文件中将 maxThread 计数设置为 1000。

TO BE ADDED: INFORMATION ON RECOMMENDED DEVICE RECONNECTION POLICIES

加入 (FTU) 工作负载
加入 (FTU) 工作负载定义为用户首次访问 XenMobile 环境。 此工作负载中操作包括：
- 自动检测
- 注册
- 身份验证
- 设备注册
- 应用程序交付（web、SaaS 和移动 MDX 应用程序）
  - 应用程序订阅（包括图像和图标下载）
  - 已订阅 MDX 应用程序的安装
- 应用程序启动（Web、SaaS 和移动 MDX 应用程序），包括设备状态检查
- 策略推送（面向 iOS）
- WorxMail 和 WorxWeb 最小连接数（VPN 通道） — 两个连接
- 通过 XenMobile 安装必需的应用程序

工作负载参数通过下表定义：

设备	设备注册	枚举数	每台设备枚举的应用程序数	每个设备的 WorxStore 启动次数	每台设备的 Web/SaaS SSO	每台设备的 MDX 应用程序下载数	通过 XenMobile 服务器触发的必要应用程序下载次数	每个设备推送的策略数 (iOS)
1000	1000	1000	50	4	40	10	2	20
10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

仅使用 Worx 连接的工作负载的现有用户数

下表显示了现有用户（仅使用 Worx 连接）工作负载。 此工作负载模拟使用 WorxMail 和 WorxWeb 应用程序的用户。 此模拟用于测试 XenMobile 配置内 NetScaler Gateway 的可扩展性。 这是可以实现的，因为通过仅使用这两个 Worx 应用程序，网络将低于最小负载。 对于 WorxWeb 应用程序，用户访问内部 Web 站点，不会触发 XenMobile 服务器 SSO。 本模式中的操作包括：

- 身份验证（NetScaler Gateway 和 XenMobile）
- WorxMail 和 WorxWeb 连接（VPN 通道） — 四个连接

下表显示了现有用户的工作负载参数。

设备	枚举数	每台设备枚举的应用程序数	每个设备的 VPN 通道数[1]
1000	1000	50	3

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. VPN 通道数与 WorxMail 和 WorxWeb 连接数相对应。

下表显示了 WorxMail 和 WorxWeb 的连接配置文件：

设备连接	连接类型	每个会话发送的数据[1]	每个会话接收的数据[1]
WorxMail 连接 #1	类型 1[2]	4.1 MB	4.1 MB
WorxMail 连接 #2	类型 1	6.3 MB	12.5 MB
WorxWeb 连接 #1	类型 2[3]	5.2 MB	15.7 MB
WorxWeb 连接 #2	类型 2	4.1 MB	3.4 MB
每个会话传输的总字节数[1]		~19.7 MB	~ 40.7 MB

1. 每个会话：8 小时。

2. 类型 1：通过长时间有效的连接，进行非对称发送和接收（即，WorxMail 使用专用的 Microsoft Exchange 邮箱连接）。

3. 类型 2：通过关闭后经过延迟再重新打开的连接，进行非对称发送和接收（即，WorxWeb 连接）。

这些建议建立在用于自动执行“中型”工作负载的 WorxMail 和 WorxWeb 配置文件
的基础之上。 修改连接详细信息会影响分析结果。 例如，如果每个用户的连接数增加，所支持的 NetScaler Gateway 会话数可能会减少。

WorxMail 和 WorxWeb 配置文件

用于每个应用程序的配置文件的目的在于自动执行“非常繁重”的工作负载。下表显示了 WorxMail 和 WorxWeb 配置文件详细信息。

中等工作负载的 WorxMail 配置文件

每天发送的消息数	20
每天接收的消息数	80
每天读取的消息数	80
每天删除的消息数	20
消息平均大小 (KB)	200

中等工作负载的 WorxWeb 配置文件

启动的 Web 应用程序数	10
手动打开的 Web 页面数	10
平均每个 Web 应用程序的请求-响应对数	100
请求的平均大小（字节）	300
响应的平均大小（字节）	1000

配置和参数

运行可扩展性测试时使用了以下配置：

- NetScaler Gateway 和负载平衡 (LB) 虚拟服务器同时存在于同一个 NetScaler Gateway 设备上。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- NetScaler 会话超时配置为 60 分钟。
- NetScaler Gateway 上使用 2048 位密钥执行 SSL 事务。

退出条件

登录率是此分析的基础。 它们为基础结构组件及其各自的配置提供指南。 一定要注意，登录率所考虑的错误包括以下各项：

- 无效响应
  - 状态代码为 401/404 而非 200 的响应为无效响应。
- 请求超时
  - 响应应在 120 秒之内发生。
- 连接错误
  - 发生连接重置。
  - 出现连接突然中止。

如果总错误率低于从给定设备发送的总请求数的 1%，则登录率为可接受。 错误率包括对应于各个单独工作负载操作的错误，以及与基础结构组件的物理性能相关的错误，如 CPU 和内存耗尽。

软件和硬件详细信息

下表列出了用于这些测试的 XenMobile 基础结构软件。

组件	版本
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
外部数据库	Microsoft SQL Server 2014

可扩展性测试在 XenServer 平台上运行，如下表所示。

供应商	Genuine Intel
型号	Intel Xeon CPU — E5645，2.40 GHz (CPU = 24)

包括基础结构核心服务（例如，Active Directory、Windows 域名服务 (DNS)、证书颁发机构、Microsoft Exchange 等），以及 XenMobile 组件（XenMobile 虚拟设备和 NetScaler Gateway VPX 虚拟设备，如适用）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 可扩展性和性能

Aug 11, 2016

理解扩展 XenMobile 基础结构在确定如何部署和配置 XenMobile 方面起着重要作用。 本文回答了与确定小型至大型企业部署的要求相关的常见问题。

性能和可扩展指南

本文中的数据可用作确定 XenMobile 10.3.6 基础结构的性能和可扩展性的指南。 用于确定如何配置服务器和数据库的两个关键因素是可扩展性（最大用户/设备数）和登录率。

- 可扩展性定义为执行所定义工作负载的最大并发用户数。 有关加载 XenMobile 基础结构的流程的详细信息，请参阅工作负载。
- 登录率定义为新用户的加入和现有用户的身份验证。
  - 加入率是指环境中首次可以注册的最大设备数。 本文中称为首次利用率或 FTU，此数据点在制定推行策略时非常重要。
  - 现有用户率：向环境进行身份验证的最大用户数，这些用户已经注册并连接其设备。 这些测试包括为已经注册的用户创建会话和执行 WorxMail 和 WorxWeb 应用程序。

下表显示了基于相应 XenMobile 环境测试结果的可扩展性指南。

可扩展性	最多 45,000 台设备	
登录率	加入率 (FTU)	每小时最多 833 台设备
	现有用户数	每小时最多 2,812 台设备
配置	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile 服务器 6 节点群集
	数据库	Microsoft SQL Server 外部数据库

> **Important**
>
> 本报告的自动化要求为 1000 到 60,000 台设备。 任何超过 60,000 台设备的要求都不在本报告范围内。

测试配置文件配置

本部分内容介绍用于每个硬件配置的测试配置文件以及用于派生本文中的测试结果的工作负载的 Active Directory 配置、XenMobile 策略的数量、应用程序的数量和类型、模拟用户操作和模拟管理员操作。

> **注意**
>
> 此测试配置文件旨在使用更多资源，而非仅使用用于测试早期 XenMobile 版本的可扩展性的配置文件。 因此，这些测试结果与来自早期版本的可扩展性结果没有直接可比性。

Active Directory (AD) 配置：

- 100000 个唯一的 AD 用户
- 200000 个唯一的 AD 组
- 适用于 AD 组的 5 个嵌套级别
- 每个 AD 组 200 个用户

交付组：

- 20 个交付组
- 50 个分配给交付组的应用程序
- 每个交付组 10 个 AD 组

XenMobile 设备策略：

- 300 个设备策略
- 每个用户 20 个设备策略

应用程序：

- 200 个来自公共应用商店的本机应用程序
- 50 个本机企业分发应用程序
- 100 个 Web 即服务和软件即服务 (SaaS) 应用程序
- 每个用户 50 个应用程序

XenMobile 用户操作：

- 共配置 50 项操作
- Worx Store 启动：
  - 新用户 (FTU)：4
  - 老用户 (RU)：1
- 应用程序启动：
  - MDX：1
  - Web/SaaS：1
- 每个用户 150 个 STA 验证

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 管理员操作：

- 枚举设备（以模拟技术支持呼叫场景）：每 8 小时执行 32 次操作，每隔 15 到 20 分钟执行一次。
- 生成报告：每 8 小时生成 2 次。

系统配置和测试结果

本部分描述运行加入 (FTU) 工作负载和现有用户工作负载可扩展测试所使用的硬件配置和结果。

下表定义了 XenMobile 从 1000 台设备扩展到 60,000 台设备时采用的硬件和配置建议。 这些指南基于测试结果及其相关工作负载。 建议考虑了退出条件中定义的可接受误差范围。

通过分析测试结果得出以下结论：

- 登录率是确定系统可扩展性的重要因素。 除了初始登录，登录率还与环境中配置的身份验证超时值相关。 例如，如果将身份验证超时值设置的太低，用户执行的登录请求会更加频繁。 因此，您需要清楚理解超时设置对环境的影响。
- NetScaler 上每个用户会话的连接数量是一个重要的考虑因素。
- 为实现最大可扩展性，增加了 XenMobile 上的 CPU 和 RAM 资源。
- 6 个节点的群集配置是经过验证的最大配置。 扩展到大于 6 个节点需要其他 XenMobile 实现。

下表显示了基于 XenMobile 配置、NetScaler Gateway 设备、群集设置和数据库得出的建议加入率和现有用户登录率。 使用此表中的数据构建新部署的最优注册计划和现有部署的返回用户/设备率。 “配置”部分将注册和登录性能数据与相应的硬件建议关联起来。

预期设备数	1000	10000	30000	45000
实际设备数	1000	9998	29977	44991
登录率				
加入率 (FTU)	250	625	833	833
现有用户数（仅限 Worx）	1000	1666	3750	883
配置				
参考环境	VPX-XenMobile 独立模式	MPX-XenMobile 独立模式	MPX-XenMobile 群集 (3)	MPX-XenMobile 群集 (6)
NetScaler Gateway	VPX，带 2 GB RAM 2 个虚拟 CPU	MPX-10500	MPX-11500	MPX-11500
XenMobile - 模式	独立*	独立*	群集	群集
XenMobile - 群集	不适用	不适用	3	6
XenMobile - 虚拟设备	8 GB RAM 和 4 个虚拟 CPU	8 GB RAM 和 4 个虚拟 CPU	16 GB RAM 和 6 个虚拟 CPU	16 GB RAM 和 8 个虚拟 CPU
Active Directory (AD)	8 GB RAM 和 4 个虚拟 CPU	8 GB RAM 和 4 个虚拟 CPU	16 GB RAM 和 4 个虚拟 CPU	16 GB RM 和 4 个虚拟 CPU
数据库	外部	外部 – Microsoft SQL Server 内存：16 GB vCPU = 12	外部 – Microsoft SQL Server 内存：32 GB vCPU = 12	外部 – Microsoft SQL Server 内存：48 GB vCPU = 16

MPX-XenMobile 群集 (3)

群集

群集

群集

群集

8 GB RAM 和 4 个虚拟 CPU

© 1999-2017 Citrix Systems, Inc. All rights reserved.

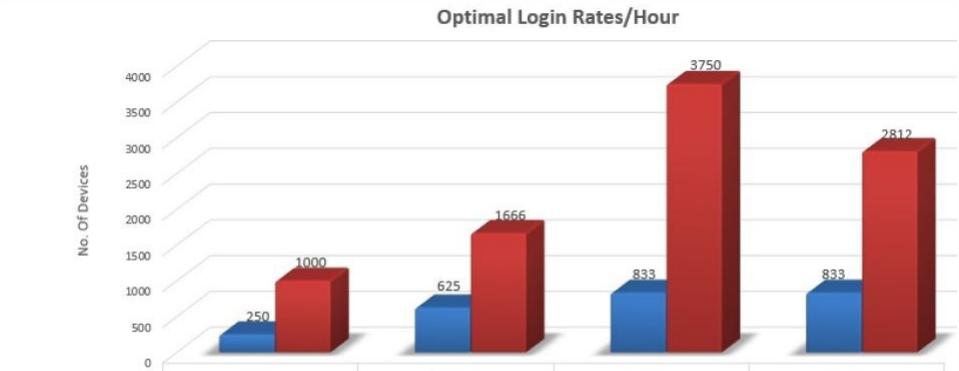
8 GB RAM 和 4 个虚拟 CPU

* 不建议对必须对用户高度可用的应用程序应用独立部署。 Citrix 建议对大多数客户应用高可用性群集化部署。

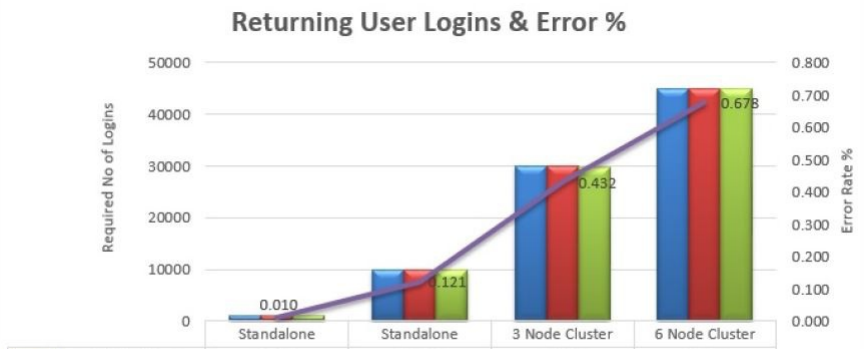
注意：调整系统时，如果超过建议的比率或硬件建议，会遇到以下问题。

以下信息提供了记录的额外数据点以及
影响上表中的结果的额外数据点。

- 注册或登录延迟（往返时间）
  - 平均总延迟：0.5 到 1.5 秒
  - NetScaler Gateway 登录的平均延迟：> 120 到 440 毫秒
  - Worx Store 请求的平均延迟：2 到 3 秒
- 达到扩展限制时，基础结构组件上会出现物理性能下降的情况，如 CPU 和内存耗尽。
  - NetScaler Gateway 和 XenMobile 设备上出现无效响应。
  - 高负载期间会延缓 XenMobile 控制台的响应时间。



	1000 (Standalone)	10000 (Standalone)	30000 (Cluster - 3 Nodes)	45000 (Cluster - 6 Nodes)
Login Rate - FTU (On Boarding)	250	625	833	833
Login Rate Non-FTU (WorxApp)	1000	1666	3750	2812

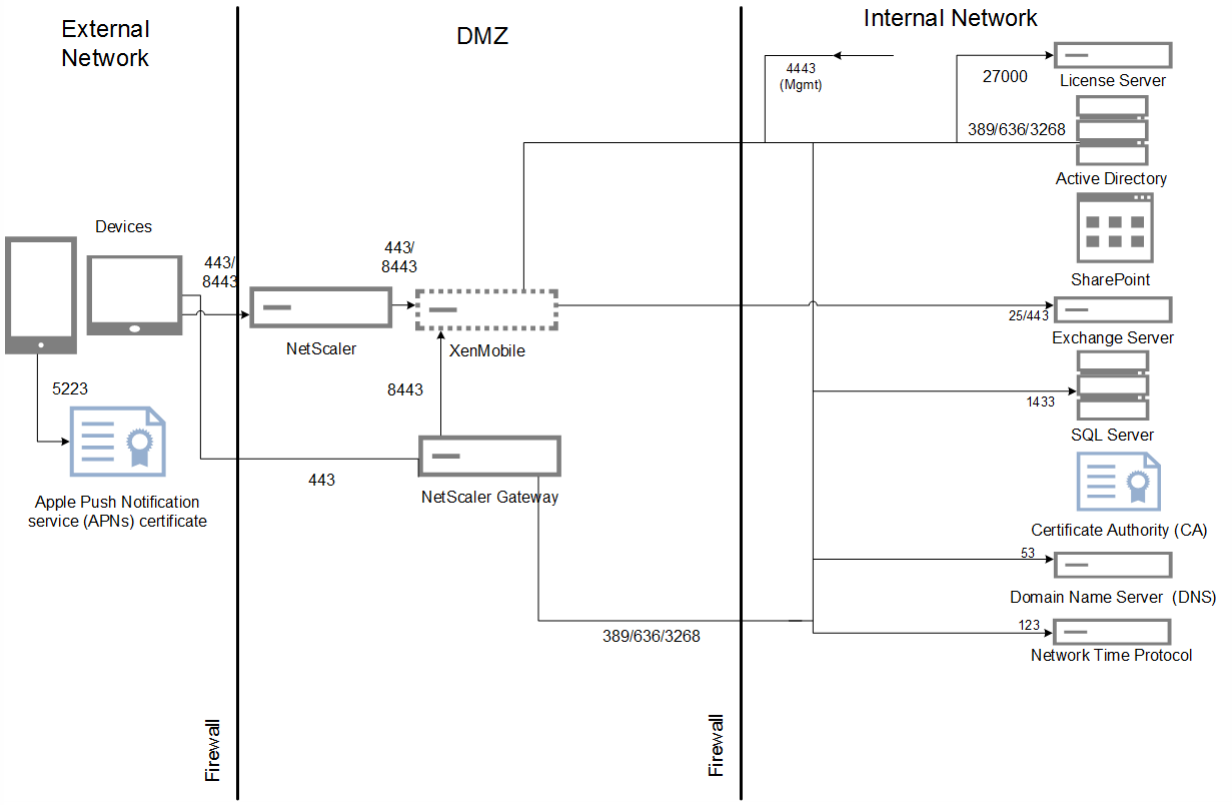


	Standalone	Standalone	3 Node Cluster	6 Node Cluster
Expected # of Devices	1000	10000	30000	45000
Actual AG Logins	1000	9998	29997	44991
Actual Enumerations	999	9998	29854	44990
Over All Error %	0.010	0.121	0.432	0.678

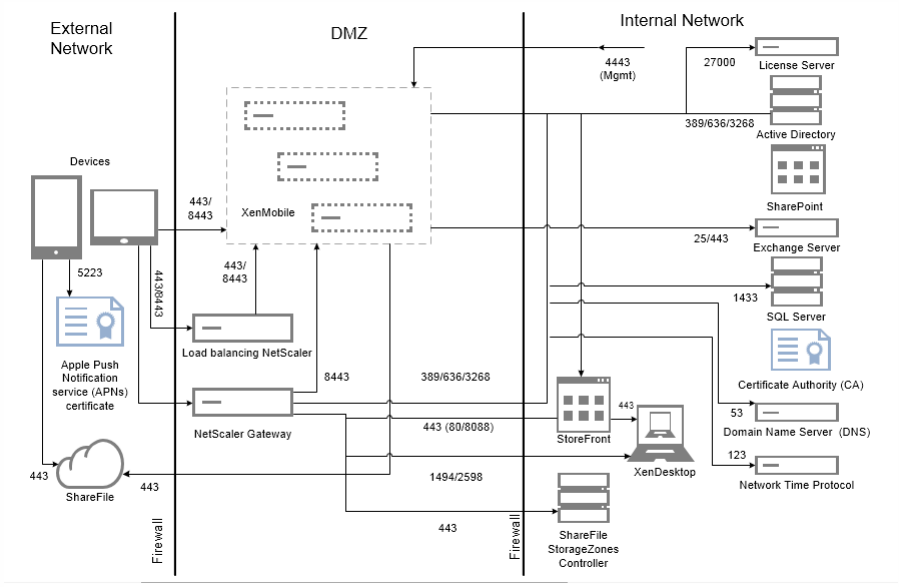
上图中的错误百分比包括遇到的总错误，考虑了每个操作对应的请求，并非仅限于登录。 根据退出条件中的定义，运行的每个测试的错误百分比都在可接受的限制 (1%) 内。

下图显示了小型部署的参考体系结构。 这是一个最多支持 10000 台设备的独立体系结构。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



下图显示了企业部署的参考体系结构。 这是一个群集体系结构，带有通过 HTTP 进行 SSL 卸载的 MAM 功能，可支持 10,000 台或更多设备。



测试方法

测试针对 XenMobile Enterprise 运行以建立标准。 为了同时面向小型和大型部署，测试使用了 1000 至 60,000 台设备。

创建工作负载以模拟实际使用情况。 针对每个测试运行这些工作负载，以了解对注册和登录率的影响。 测试的目的是为了在退出条件中描述的可接受误差范围内，获取最优登录率。 登录率是确定基础结构组件的硬件配置建议的关键因素。

加入 (FTU) 工作负载登录请求包括自动检测、身份验证和设备注册操作。 应用程序订阅、安装和启动操作在测试期间统一分发。 这样提供了对用户操作的最真实模拟。 在测试的结尾，注销会话。 现有用户工作负载登录请求仅包括身份验证请求。

工作负载

用户工作负载的定义如下：

用户会话/设备数	每个会话包括 NetScaler Gateway 登录、枚举、设备注册等。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Worx Store 启动	用户多次启动 Worx Store，每次订阅或安装多个应用程序，不管这些应用程序是移动应用程序 (web/SaaS/MDX) 还是 Windows 应用程序 (HDX)。
每台设备的 Web/SaaS 应用程序 SSO	web/SaaS 应用程序的启动序列的帐户数达到标识点，XenMobile 完成 SSO 并返回实际应用程序 URL。 流量不发送给实际应用程序。
每台设备的 MDX 应用程序下载数	MDX 应用程序的下载总数（可能会发生在两次 Worx Store 启动之间）。 对于 iOS，此数据还包括 Apple ITMS 的应用程序自动安装，Apple ITMS 利用 NetScaler Gateway 上的新令牌/tms 服务 API。

注意事项与假设

可扩展性测试不包括以下场景。 在以后增强扩展测试功能时会考虑这些场景：

- 未测试软件包部署。
- 未测试 Windows 平台。

已针对 iOS 和 Android 设备测试策略推送功能。
每个 XenMobile 最多同时支持 10000 个连接。

测试采用 LAN 在理想连接状态下运行，以避免网络延迟问题。 在实际场景中，可扩展性还取决于用户的可用带宽，尤其是应用程序下载问题。

“重新连接”测试

“重新连接”测试已与“首次使用”测试和“返回用户场景”测试分开完成。

“重新连接”测试已针对多达 15000 台设备运行。

Android 支持的重新连接率为每秒 17 台设备。 iOS 的重新连接率为每秒 8 台设备。 为实现此目标，已在 /opt/sas/tomcat/conf/server.xml 文件中将 maxThread 计数设置为 1000。

TO BE ADDED: INFORMATION ON RECOMMENDED DEVICE RECONNECTION POLICIES

加入 (FTU) 工作负载
加入 (FTU) 工作负载定义为用户首次访问 XenMobile 环境。 此工作负载中操作包括：
- 自动检测
- 注册
- 身份验证
- 设备注册
- 应用程序交付（web、SaaS 和移动 MDX 应用程序）
  - 应用程序订阅（包括图像和图标下载）
  - 已订阅 MDX 应用程序的安装
- 应用程序启动（Web、SaaS 和移动 MDX 应用程序），包括设备状态检查
- 策略推送（面向 iOS）
- WorxMail 和 WorxWeb 最小连接数（VPN 通道） — 两个连接
- 通过 XenMobile 安装必需的应用程序

工作负载参数通过下表定义：

设备	设备注册	枚举数	每台设备枚举的应用程序数	每个设备的 WorxStore 启动次数	每台设备的 Web/SaaS SSO	每台设备的 MDX 应用程序下载数	通过 XenMobile 服务器触发的必要应用程序下载次数	每个设备推送的策略数 (iOS)
1000	1000	1000	50	4	40	10	2	20
10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

仅使用 Worx 连接的工作负载的现有用户数

下表显示了现有用户（仅使用 Worx 连接）工作负载。 此工作负载模拟使用 WorxMail 和 WorxWeb 应用程序的用户。 此模拟用于测试 XenMobile 配置内 NetScaler Gateway 的可扩展性。 这是可以实现的，因为通过仅使用这两个 Worx 应用程序，网络将低于最小负载。 对于 WorxWeb 应用程序，用户访问内部 Web 站点，不会触发 XenMobile 服务器 SSO。 本模式中的操作包括：

- 身份验证（NetScaler Gateway 和 XenMobile）
- WorxMail 和 WorxWeb 连接（VPN 通道） — 四个连接

下表显示了现有用户的工作负载参数。

设备	枚举数	每台设备枚举的应用程序数	每个设备的 VPN 通道数[1]
1000	1000	50	3

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. VPN 通道数与 WorxMail 和 WorxWeb 连接数相对应。

下表显示了 WorxMail 和 WorxWeb 的连接配置文件：

设备连接	连接类型	每个会话发送的数据[1]	每个会话接收的数据[1]
WorxMail 连接 #1	类型 1[2]	4.1 MB	4.1 MB
WorxMail 连接 #2	类型 1	6.3 MB	12.5 MB
WorxWeb 连接 #1	类型 2[3]	5.2 MB	15.7 MB
WorxWeb 连接 #2	类型 2	4.1 MB	3.4 MB
每个会话传输的总字节数[1]		~19.7 MB	~ 40.7 MB

1. 每个会话：8 小时。

2. 类型 1：通过长时间有效的连接，进行非对称发送和接收（即，WorxMail 使用专用的 Microsoft Exchange 邮箱连接）。

3. 类型 2：通过关闭后经过延迟再重新打开的连接，进行非对称发送和接收（即，WorxWeb 连接）。

这些建议建立在用于自动执行“中型”工作负载的 WorxMail 和 WorxWeb 配置文件
的基础之上。 修改连接详细信息会影响分析结果。 例如，如果每个用户的连接数增加，所支持的 NetScaler Gateway 会话数可能会减少。

WorxMail 和 WorxWeb 配置文件

用于每个应用程序的配置文件的目的在于自动执行“非常繁重”的工作负载。下表显示了 WorxMail 和 WorxWeb 配置文件详细信息。

中等工作负载的 WorxMail 配置文件

每天发送的消息数	20
每天接收的消息数	80
每天读取的消息数	80
每天删除的消息数	20
消息平均大小 (KB)	200

中等工作负载的 WorxWeb 配置文件

启动的 Web 应用程序数	10
手动打开的 Web 页面数	10
平均每个 Web 应用程序的请求-响应对数	100
请求的平均大小（字节）	300
响应的平均大小（字节）	1000

配置和参数

运行可扩展性测试时使用了以下配置：

- NetScaler Gateway 和负载平衡 (LB) 虚拟服务器同时存在于同一个 NetScaler Gateway 设备上。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- NetScaler 会话超时配置为 60 分钟。
- NetScaler Gateway 上使用 2048 位密钥执行 SSL 事务。

退出条件

登录率是此分析的基础。 它们为基础结构组件及其各自的配置提供指南。 一定要注意，登录率所考虑的错误包括以下各项：

- 无效响应
  - 状态代码为 401/404 而非 200 的响应为无效响应。
- 请求超时
  - 响应应在 120 秒之内发生。
- 连接错误
  - 发生连接重置。
  - 出现连接突然中止。

如果总错误率低于从给定设备发送的总请求数的 1%，则登录率为可接受。 错误率包括对应于各个单独工作负载操作的错误，以及与基础结构组件的物理性能相关的错误，如 CPU 和内存耗尽。

软件和硬件详细信息

下表列出了用于这些测试的 XenMobile 基础结构软件。

组件	版本
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
外部数据库	Microsoft SQL Server 2014

可扩展性测试在 XenServer 平台上运行，如下表所示。

供应商	Genuine Intel
型号	Intel Xeon CPU — E5645，2.40 GHz (CPU = 24)

包括基础结构核心服务（例如，Active Directory、Windows 域名服务 (DNS)、证书颁发机构、Microsoft Exchange 等），以及 XenMobile 组件（XenMobile 虚拟设备和 NetScaler Gateway VPX 虚拟设备，如适用）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

关于 XenMobile Server 10.3.5

Oct 21, 2016

在 XenMobile 控制台中，您可以直接从以下版本升级到 XenMobile 10.3.5：

- XenMobile 10.3 Rolling Patch 1
- XenMobile 10.3
- XenMobile 10.1 Rolling Patch 4
- XenMobile 10.1

要执行升级，请使用 xms_10.3.5.354.bin。 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击**版本管理**。 单击**升级**，然后上载 xms_10.3.5.354.bin 文件。 有关在控制台中进行升级的详细信息，请参阅升级 XenMobile。

要全新安装 XenMobile 10.3.5，请参阅安装 XenMobile。

规划 XenMobile 部署有多个注意事项。 有关您的端到端 XenMobile 环境的建议、常见问题和用例，请参阅 XenMobile Deployment Handbook（《XenMobile 部署手册》）。

XenMobile 10.3.5 中的新增功能

XenMobile 10.3.5 修复了一些缺陷，并提供了以下新功能。

XenMobile 服务器 10.3.5 云更新

Cloud Services 团队可以在不停机的情况下将您的 XenMobile 服务器云部署从版本 10.3 更新到 10.3.5。

Android M 的动态权限

可以允许 Android M 用户启用或阻止四种类型的权限。 当用户在 Worx Home 中注册时，系统会先后显示四条消息，请求其允许或拒绝授予 Worx Home 以下权限：

- 访问 Worx Home 的设备信息以正常运行。
- 能够拨打和管理电话。
- 访问设备上的照片、媒体和文件。
- 访问设备所在的位置。

iOS 中的 Touch ID 身份验证

在本版本中，您现在可以允许 iOS 用户对 Worx Home 以及使用 Touch ID 的 Worx 应用程序重新进行身份验证。 对于 iOS 8 和 iOS 9 设备，如果为 Worx Home 启用了单点登录，并且启用了 Touch ID 时，此组合将代替使用 PIN。 无论何时需要通过 NetScaler Gateway 进行联机身份验证，用户都需要输入 PIN 码。 在以下实例中需要执行此操作：

- 用户的会话已过期。
- 用户重新启动设备。
- Worx Home 当前未运行，用户启动该应用程序或 MDX 应用程序。

注册配置文件

现在，您可以在 XenMobile 控制台的全新**配置 > 注册配置文件**页面为 Android 和 iOS 设备创建注册配置文件。 注册配置文件会应用于所有服务器模式。 您可以创建多个注册配置文件，并将它们与不同交付组关联起来。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：注册配置文件页面不适用于 Windows 设备。 有关注册 Windows 设备的信息，请参阅 Windows 设备。

每用户设备限制发生的变化

以前，每用户设备限制通过**每个用户的设备数**这一服务器属性进行设置。 该服务器属性现已弃用。 现在，您可以在全新**配置 > 注册配置文件**页面中配置设备限制。 以前，您只能为 MDM 限制设备数。 现在，您也可以为 MAM 限制设备数。

默认情况下，每个用户可注册的设备数不受限制。 有关详细信息，请参阅设备注册限制。

语言支持

XenMobile 10.3.5 为 WorxStore 提供了希伯来语和繁体中文支持。

全新的仅 MAM 模式

XenMobile 10.3.5 引入了新的“仅 MAM”服务器模式。 为了区分旧模式和新 MAM 模式，Citrix 文档中将此新模式称为“仅 MAM”，将旧 MAM 模式为“旧 MAM 模式”。虽然旧 MAM 功能和以前相同，但是 Citrix 不会在将来的版本中对它进行增强。

当 XenMobile 的服务器模式属性为 **MAM** 时“仅 MAM”模式生效。 设备在 MAM 模式中注册。

当 XenMobile 的服务器模式属性为 **ENT** 以及用户选择退出设备管理时，旧 MAM 功能生效。 设备在 MDM + MAM 模式中注册。 在 MAM+MDM 模式下，选择退出 MDM 管理程序的用户将继续接收到旧版 MAM 功能，而无论您是否升级到 XenMobile 10.3.5。

注意：在以前，将“服务器模式”属性设置为 **MAM** 与将此属性设置为 **ENT** 具有相同的效果：设备在 MDM + MAM 模式中注册；选择退出 MDM 管理的用户已接收旧 MAM 功能。

仅 MAM 模式的优势包括附加加密（不仅限于设备通行码）、移动 VPN 以及更加完善的最终用户隐私政策，这使得仅 MAM 模式适用于 BYO 设备。

如果您的 XenMobile 服务器模式当前为 MAM，则可以升级到新的仅 MAM 模式，以从以前仅对 MDM 可用的以下功能中获益。 这些功能不适用于 Windows Phone。

- **基于证书的身份验证**
  仅 MAM 模式支持基于证书的身份验证。 用户会遇到持续访问其应用程序的情况，即使其 AD 密码过期也是如此。 如果您选择为 MAM 设备切换到基于证书的身份验证，则必须配置 NetScaler Gateway。 默认情况下，在 XenMobile 的**设置 > NetScaler Gateway** 中，**向用户提供用于身份验证的证书**设置为**关**，则表示使用用户名和密码身份验证。 必须将该设置更改为**开**，才能启用证书身份验证。
- **自助服务门户**，允许最终用户执行各自的应用程序锁定和应用程序擦除操作。 这些操作适用于设备上的所有应用程序。 可以在**配置 > 操作**中配置“应用程序锁定”和“应用程序擦除”操作。
- **所有注册模式**，包括“高安全性”、“邀请 URL”和“双重身份验证”，通过管理 > 注册进行配置。
- 面向 Android 和 iOS 设备的**设备注册限制**。 服务器属性**每个用户的设备数**已移至新的**配置 > 注册配置文件**页面，现在还适用于新的仅 MAM 模式。
- **仅 MAM API**。 对于仅 MAM 设备，您可以通过使用任何 REST 客户端和 XenMobile REST API 调用通过 XenMobile 控制台展现的 REST 服务。
- 通过本版本中提供的仅 MAM API，您可以执行以下操作：
  - 发送邀请 URL 和一次性 PIN
  - 在设备上发出应用程序锁定和擦除命令

Important

© 1999-2017 Citrix Systems, Inc. All rights reserved.

要使用新的仅 MAM 模式，必须按本文所述配置 XenMobile，并且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 服务器 FQDN。

在新的仅 MAM 模式下，设备使用 XenMobile 服务器 FQDN 进行注册，这一点与 ENT 模式相同。 （在旧版 MAM 模式下，设备使用 NetScaler Gateway FQDN 进行注册。）

此升级如何影响已注册的设备

下表概述了 XenMobile 10.3.5 中的新增功能如何影响已注册的设备。

当前注册为此项目的设备	XenMobile 10.3.5 提供程序	管理员任务	用户任务
MDM • 服务器模式 = MDM	• 缺陷修复 • 新增功能	安装 XenMobile 10.3.5	无
MDM+MAM • 服务器模式 = ENT • 用户选择进行设备管理	• 缺陷修复 • 新增功能	安装 XenMobile 10.3.5	无
MAM • 服务器模式 = ENT • 用户选择退出设备管理	• 缺陷修复 • 新增功能 注意：在此用例中，设备在旧版 MAM 模式下进行注册。 如果要向这些用户提供新的 MAM 功能，请为其设置新 XenMobile 服务器。	安装 XenMobile 10.3.5	无
MAM • 服务器模式 = MAM	• 缺陷修复 • 新增功能 • 升级到新的仅 MAM 模式（可选）	要继续使用旧版 MAM 功能，请执行以下操作： 安装 XenMobile 10.3.5 要升级到仅 MAM 模式，请执行以下操作： 1. 安装 XenMobile 10.3.5。 2. 有关所需的其他信息，请参阅下文“仅 MAM 模式配置概览”。	无 重新注册设备

© 1999-2017 Citrix Systems, Inc. All rights reserved.

仅 MAM 模式配置概览

*仅 MAM 模式*是指与 Enterprise 或 Advanced 许可证结合使用时的 MAM 服务器模式。 仅 MAM 模式与 *MAM+MDM 模式*不同，后者在您的 XenMobile 服务器的服务器模式为 ENT 时使用。 在 MAM+MDM 模式下，系统会向选择退出 MDM 管理的用户提供旧版 MAM 功能，而无论您是否升级到 XenMobile 10.3.5。

> **Important**
>
> 旧版 MAM 功能的运行方式与早期版本相同，并且在将来的版本中不会增强。

下表概述了用于特定许可证类型的“服务器模式”设置以及所需的设备模式：

您的许可证适用于此版本	**您希望设备在此模式下注册**	**将“服务器模式”属性设置为**
ENT/ADV/MDM	MDM 模式	MDM
ENT/ADV	MAM 模式（又称为“仅 MAM 模式”）	MAM
ENT/ADV	MDM+MAM 模式	ENT 选择退出设备管理的用户将在旧版 MAM 模式下操作。

*仅*在以下情况下才能配置仅 MAM 模式：

- 您的 XenMobile 服务器当前的**服务器模式**为 **MAM**，并且您希望将其更改为新的仅 MAM 模式以便从附加功能中获益。
- 您希望设置 XenMobile 服务器以向连接到该服务器的所有用户提供仅 MAM 功能。

仅 MAM 模式的常规配置步骤如下：

1. 安装或升级到 XenMobile 10.3.5。
2. 在**管理 > 设备**页面上，检查**服务器模式**。 如果**服务器模式**是 **MDM** 或 **ENT**，则不要执行此过程中的步骤，因为这会产生不支持设备管理功能的配置。
3. 在 XenMobile 服务器上打开端口 8443 和 443 以及 Internet 防火墙，以便设备能够连接到 XenMobile 服务器。 注册必须在 XenMobile 服务器上进行。
4. 如果要升级**服务器模式**已设置为 **MAM** 的服务器，请跳过下一步骤。 如果要执行 XenMobile 10.3.5 的全新安装，XenMobile 服务器的默认**服务器模式**为 **ENT**。 要启用仅 MAM 模式，必须将服务器属性**服务器模式**设置为 **MAM**。 有关信息，请参阅为仅 MAM 配置服务器模式。
5. 如果要使用基于证书的身份验证，请将 XenMobile 和您的 NetScaler Gateway 配置为支持基于证书的身份验证。 默认情况下，在 XenMobile 的**设置 > NetScaler Gateway** 中，**向用户提供用于身份验证的证书**设置为**关**，则表示使用用户名和密码身份验证。 必须将该设置更改为**开**。 有关配置详细信息，请参阅面向仅 MAM 模式的证书身份验证。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 选择或设置与仅 MAM 模式结合使用的通知模板时，请注意，SMTP 是唯一受支持的发送注册邀请的方法。
7. 如果正在将您的用户升级到新的仅 MAM 模式，请向其提供 XenMobile 服务器 FQDN 并告知其必须重新注册。
   在新的仅 MAM 模式下，设备使用 XenMobile 服务器 FQDN 进行注册，这一点与 ENT 模式相同。（在旧版 MAM 模式下，设备使用 NetScaler Gateway FQDN 进行注册。）

下表概述了旧版 MAM 功能（XenMobile 10.3 和 XenMobile 10.3.5）与新的仅 MAM 模式 (XenMobile 10.3.5) 之间的差别。

注册场景及其他功能	**XenMobile 10.3 旧版 MAM（服务器模式为 ENT）**	**XenMobile 10.3.5 旧版 MAM（服务器模式为 ENT）**	**XenMobile 10.3.5 仅 MAM 模式（服务器模式为 MAM）**
证书身份验证	不受支持。	不受支持。	支持。 要使用证书身份验证，需要配置 NetScaler Gateway。
部署要求	XenMobile 服务器不需要能够直接从设备访问。	XenMobile 服务器不需要能够直接从设备访问。	XenMobile 服务器必须可从设备访问。
注册选项	使用 NetScaler Gateway FQDN 或选择退出注册。	使用 NetScaler Gateway FQDN 或选择退出注册。	使用 XenMobile 服务器 FQDN。
注册方法	用户名 + 密码	用户名 + 密码	用户名 + 密码、高安全性、邀请 URL、邀请 URL+PIN、邀请 URL + 密码、双重身份验证、用户名 + PIN
应用程序锁定和擦除	支持。	支持。	支持。
用于应用程序锁定和擦除的自助服务门户选项	不受支持。	不受支持。	支持。
应用程序擦除行为	应用程序保留在设备上，但不可使用。 只能在客户端上删除帐户。	应用程序保留在设备上，但不可使用。 只能在客户端上删除帐户。	应用程序保留在设备上，但不可使用。 只能在客户端上删除帐户。
面向仅 MAM 用户的自动化操作。	不受支持。	支持事件、设备属性和用户属性操作。 不支持基于已安装的应用程序的自动化操作。	支持事件、设备属性和用户属性操作。 不支持基于已安装的应用程序的自动化操作。
删除了 AD 用户时的内置操作	不受支持。	支持应用程序擦除。	支持应用程序擦除。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注册限制	支持仅 MDM 模式；通过服务器属性进行配置。	支持；通过注册配置文件进行配置。	支持；通过注册配置文件进行配置。
软件清单	支持；XenMobile 列出了安装在设备上的应用程序	支持；XenMobile 列出了安装在设备上的应用程序	不受支持。

仅 MAM 模式的参考体系结构

在 XenMobile 的仅 MAM 部署中，可以在 DMZ 中或内部网络中部署 XenMobile 服务器的群集。 在每个场景中，身份验证都会通过 NetScaler Gateway 进行。

请注意，与在 XenMobile Enterprise 部署中不同，不需要配置 XenMobile NetScaler Connector (XNC) 和 XenMobile Mail Manager (XMM)。

有关参考体系结构图，请参阅《XenMobile 部署手册》文章适用于本地部署的参考体系结构。

仅 MAM 使用备注

- 所需的应用程序不自动安装。 用户必须从 WorxStore 手动安装这些应用程序。
- iOS 用户必须信任 iOS 开发人员证书。 Android 用户必须启用从第三方应用商店安装的设置。
- 用户仅在 WorxStore 中接收应用程序更新通知。
- 用户删除 Worx Home 或从 Worx Home 取消注册后，已安装的应用程序会保留在设备上，直到用户将其删除为止。
- 仅 MAM 模式不支持 APNs 或 Google Cloud Messaging。
- XenMobile 控制台不包含以仅 MAM 模式注册的设备的已越狱/已获得 root 权限状态，但**阻止越狱或已获得 root 权限的设备**策略适用于那些设备。

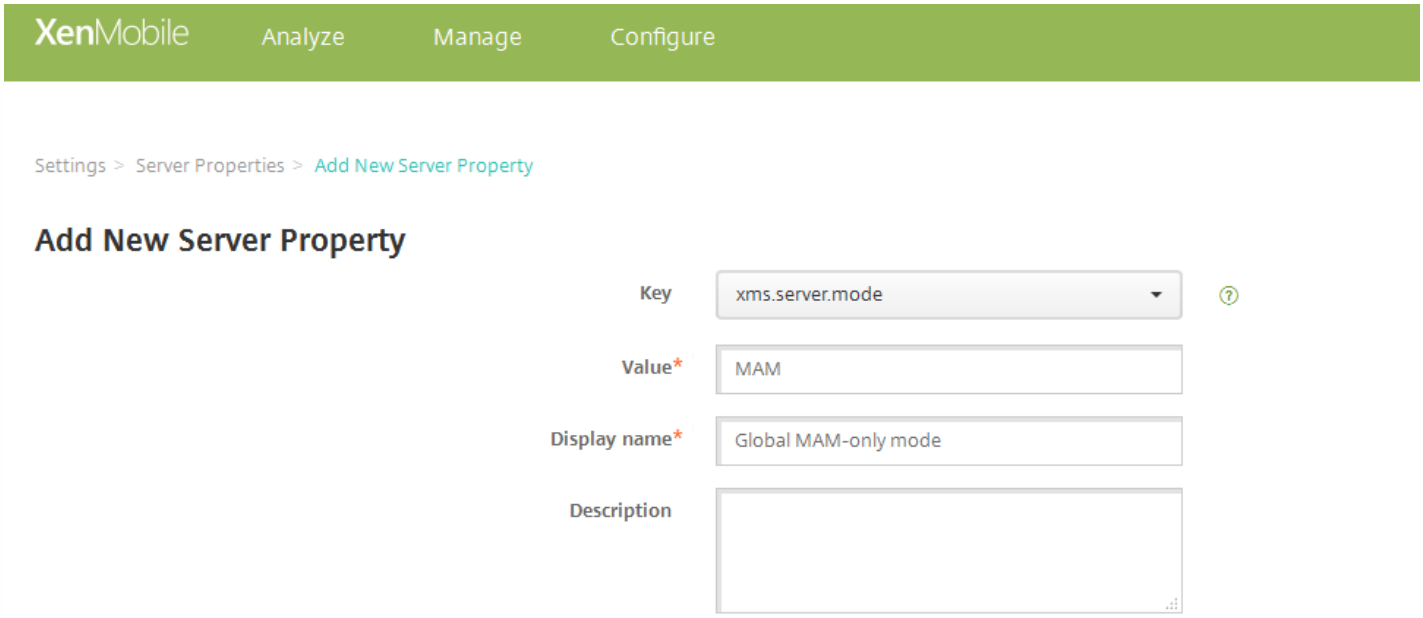
为仅 MAM 配置服务器模式

全新安装后，服务器默认处于 ENT 模式。 要为 XenMobile 10.3.5 启用仅 MAM 模式，请按如下所示配置服务器：

1. 在 XenMobile 控制台中，单击右上角的嵌齿图标以打开**设置**页面。
2. 在**设置**页面上，单击**服务器属性**。
3. 单击**添加**。
4. 在**密钥**中，单击 **xms.server.mode**。
5. 在**值**中，输入 **MAM**。
6. 在**显示名称**中，输入要在**服务器属性**表中显示的说明。

或者，输入说明，然后单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Important

将 xms.server.mode 属性设置为仅 MAM 后，XenMobile 控制台仍显示适用于 MDM 模式的区域，例如设备属性。 但是，这些设置不起作用。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

面向仅 MAM 模式的证书身份验证

Aug 11, 2016

必须依次配置 Microsoft 服务器、XenMobile 服务器和 NetScaler Gateway 服务器，才能在仅 MAM 模式下使用证书身份验证。 本文详细介绍了以下常规步骤。

在 Microsoft 服务器上：

1. 向 Microsoft 管理控制台中添加证书管理单元。
2. 向证书颁发机构 (CA) 中添加模板。
3. 从 CA 服务器创建一个 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. 将 NetScaler Gateway 配置为提供用于进行身份验证的用户证书。

在 NetScaler Gateway 上：

1. 为 XenMobile 仅 MAM 模式证书身份验证配置 NetScaler Gateway

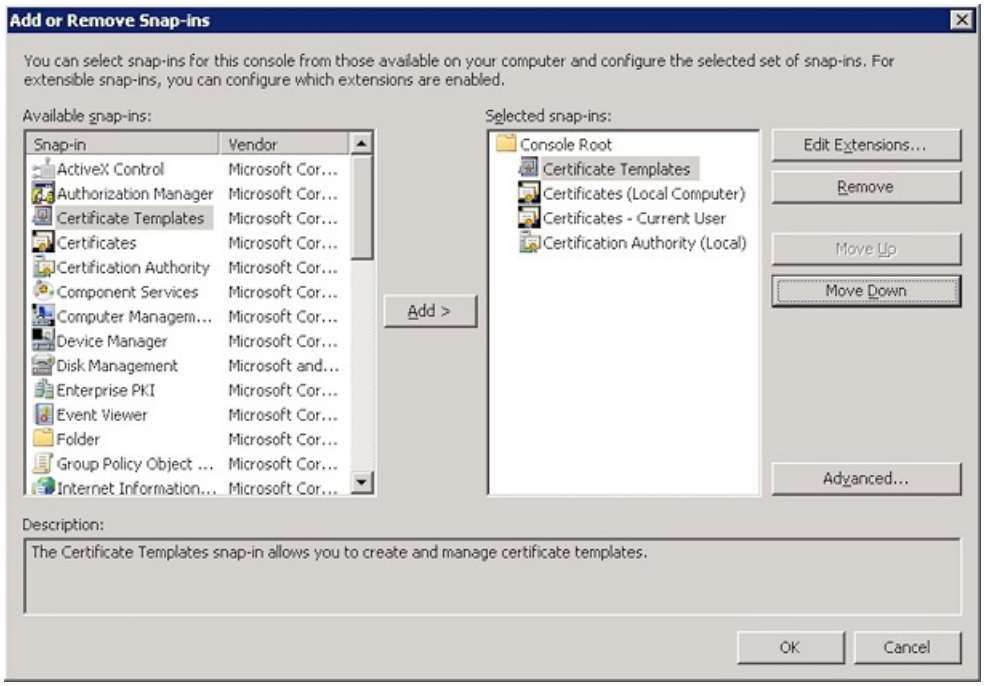
向 Microsoft 管理控制台中添加证书管理单元

1. 打开该控制台，然后单击**Add/Remove Snap-Ins**（添加/删除管理单元）。

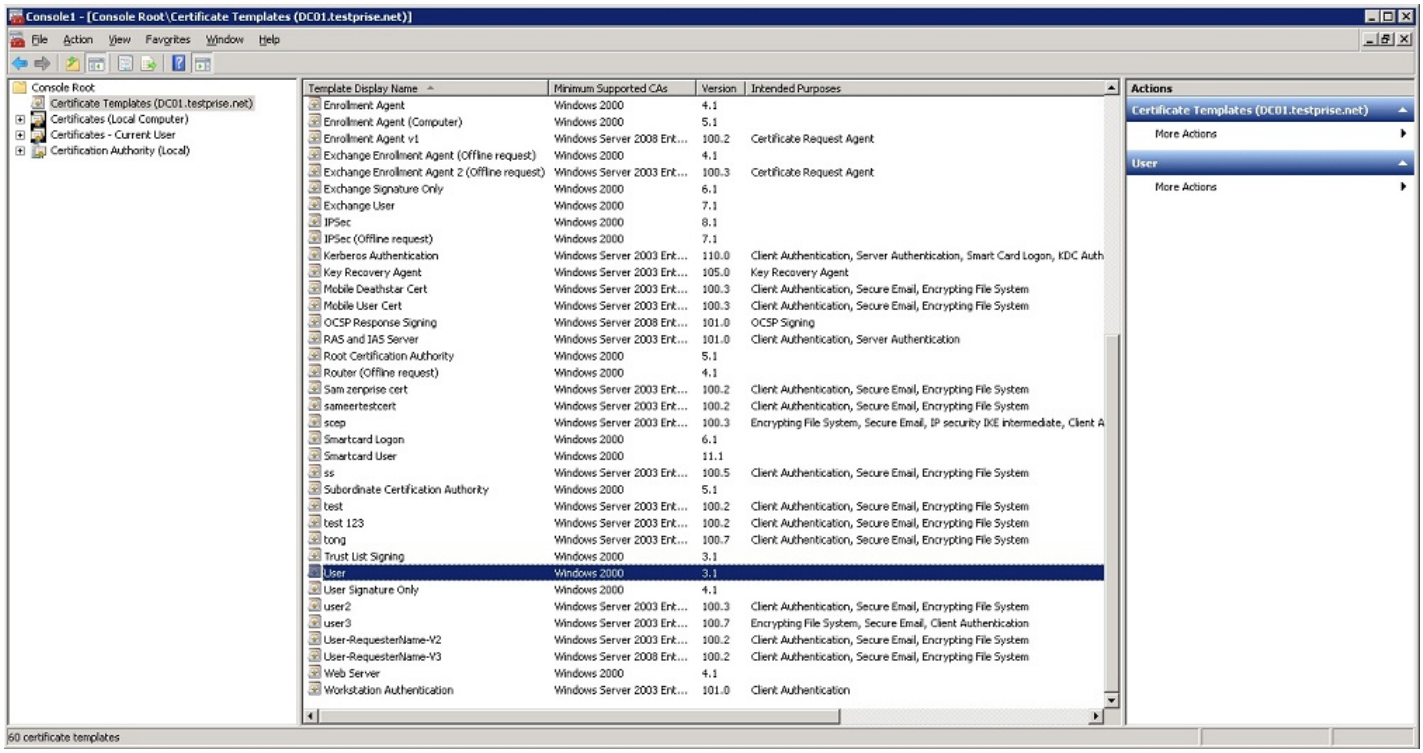
2. 添加以下管理单元：

    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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

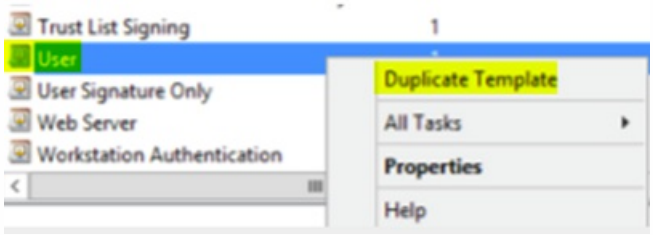


3. 展开**证书模板**。



4. 选择**用户**模板和**复制模板**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



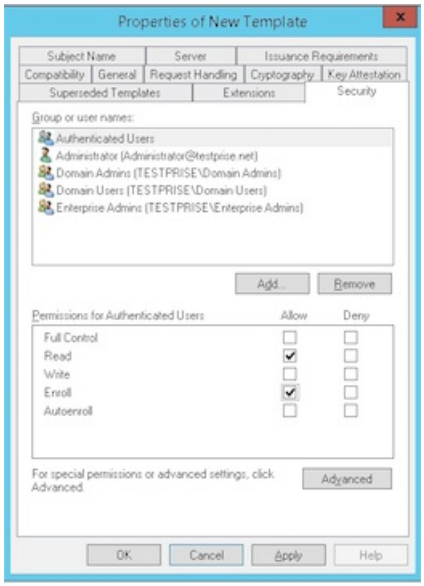
5. 提供模板显示名称。

> **重要：**除非需要，否则请勿选中**在 Active Directory 中发布证书**复选框。 如果选中了此选项，则将在 Active Directory 中推送/创建所有用户客户端证书，这可能会导致您的 Active Directory 数据库混乱不堪。

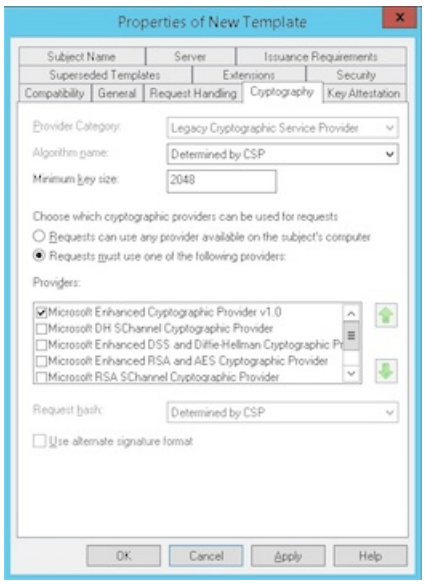
6. 选择“Windows 2003 Server”作为模板类型。 在 Windows 2012 R2 Server 中的**兼容性**下，选择**证书颁发机构**并将收件人设置为 Windows 2003。

7. 在**安全**下，在已通过身份验证的用户对应的**允许**列下选择**注册**选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

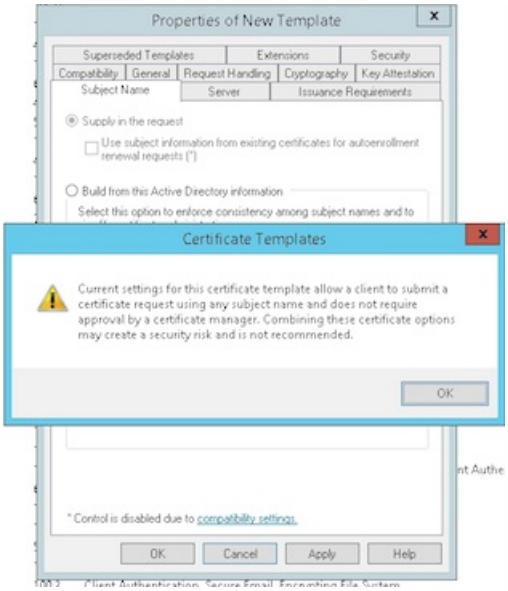


8. 在**加密**下，请务必提供需要在 XenMobile 配置过程中输入的密钥大小。



9. 在**使用者名称**下，选择**在请求中提供**。 应用更改并保存。

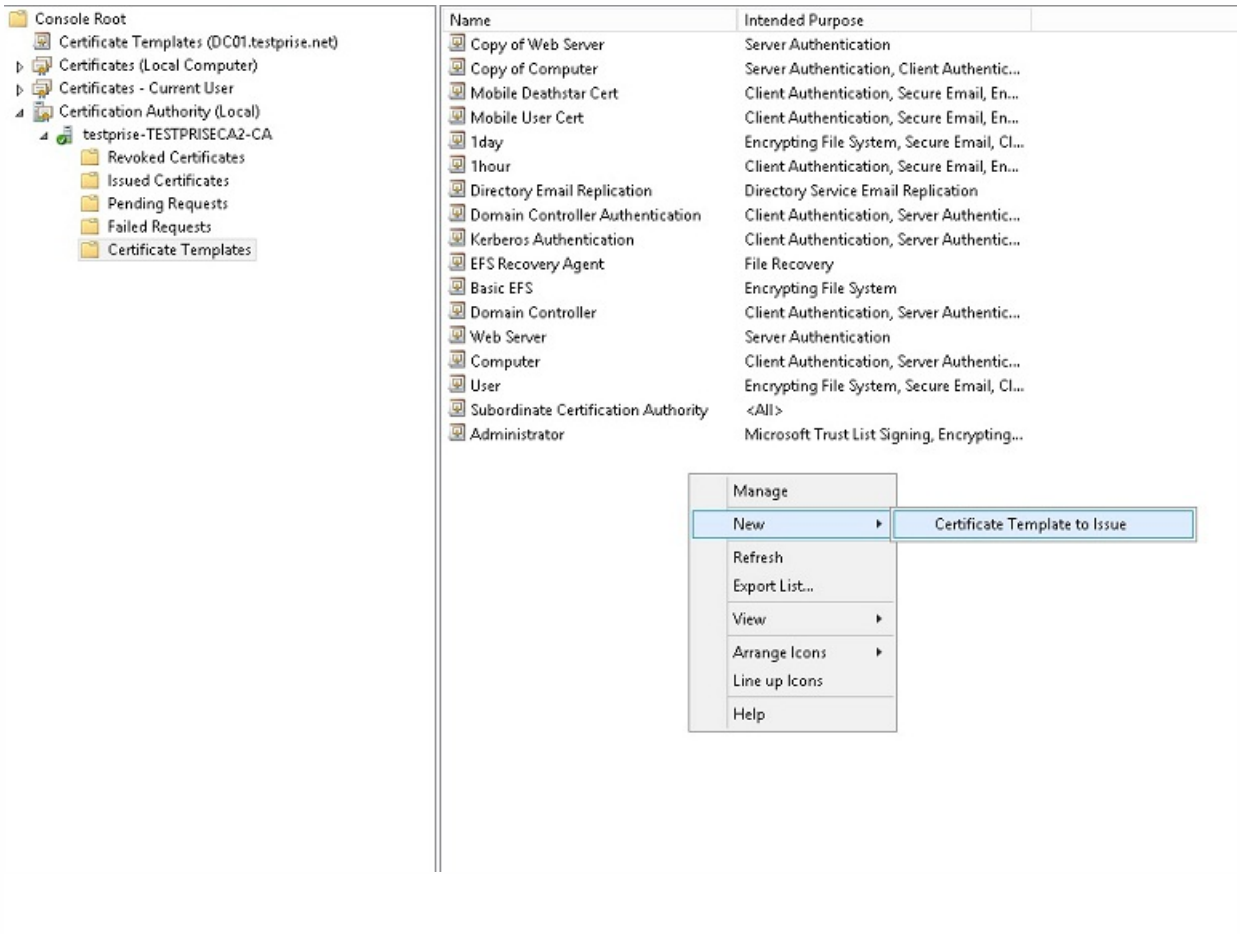
© 1999-2017 Citrix Systems, Inc. All rights reserved.



向证书颁发机构中添加模板

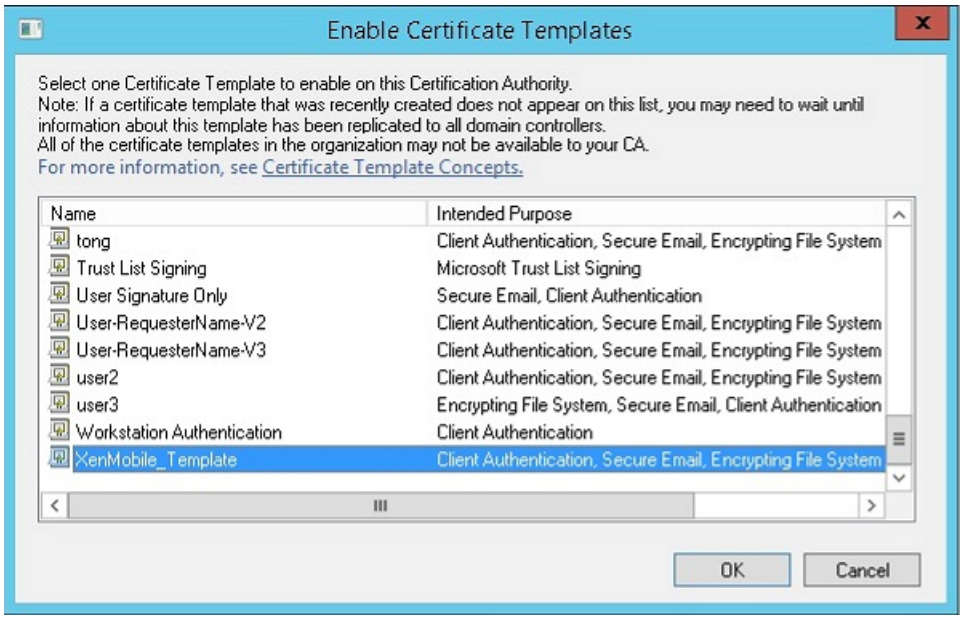
1. 转至**证书颁发机构**并选择**证书模板**。

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



© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 选择在上一步中创建的模板，然后单击**确定**将其添加到证书颁发机构。

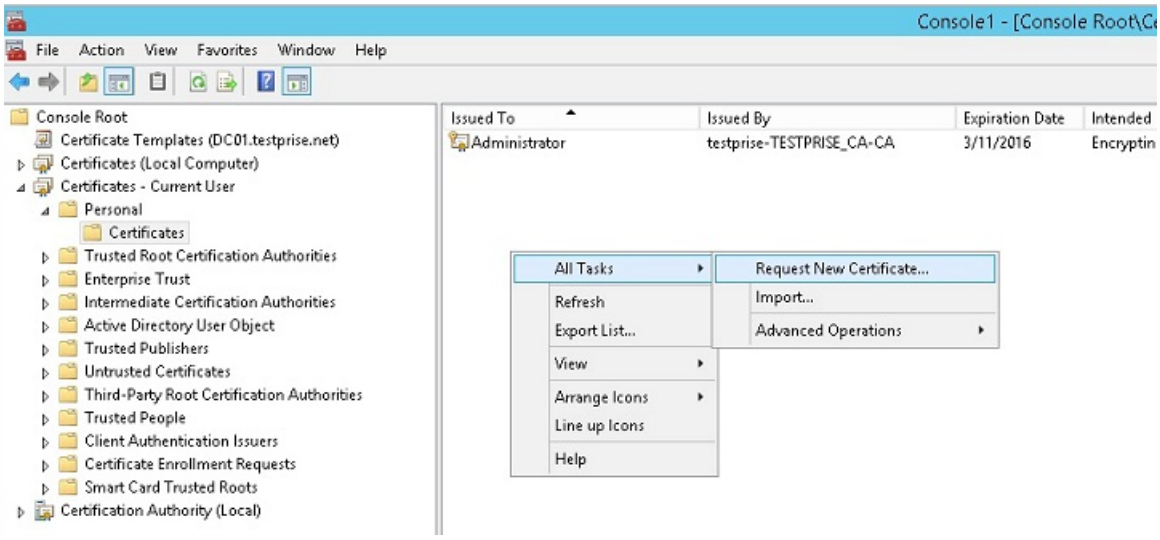


从 CA 服务器创建 PFX 证书

1. 使用登录时使用的服务帐户创建一个用户 .pfx 证书。 此 .pfx 将上载到 XenMobile 中，而 XenMobile 将代表注册设备的用户申请用户证书。

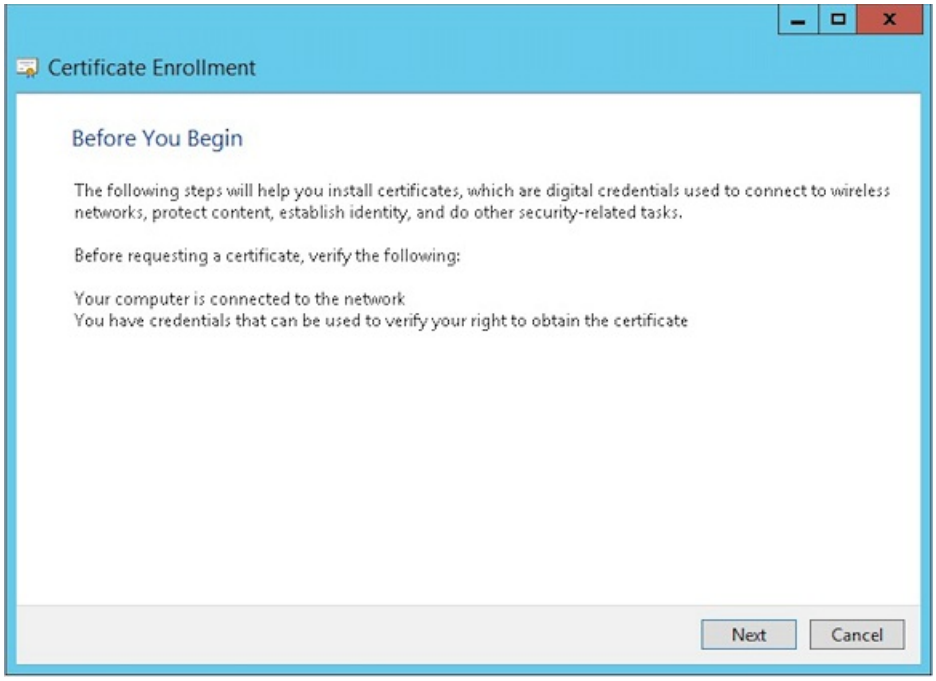
2. 在**当前用户**下，展开**证书**。

3. 在右侧窗格中单击鼠标右键，然后单击**申请新证书**。

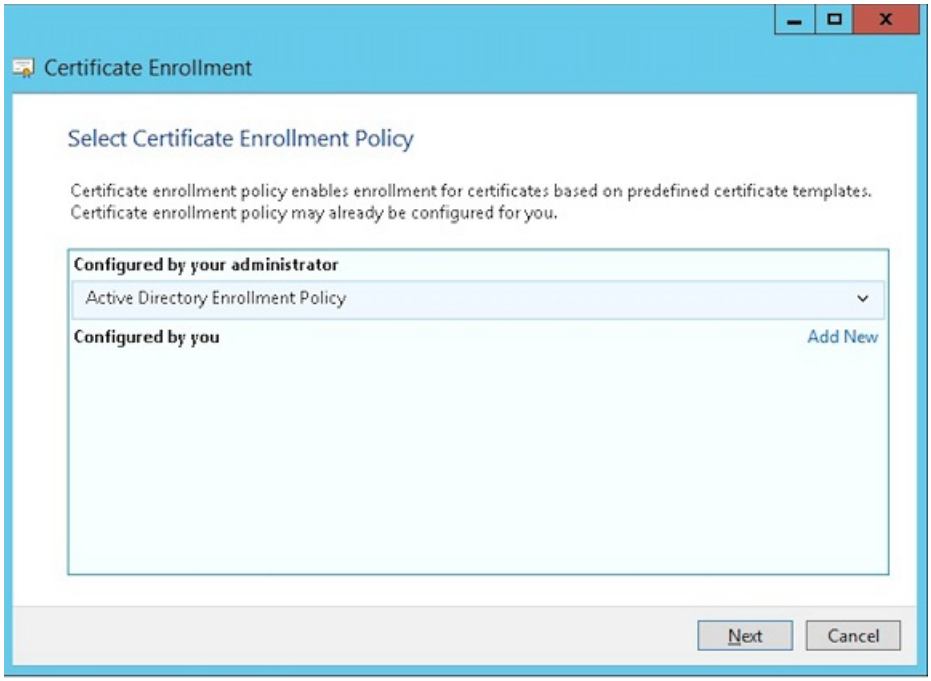


4. 此时将显示**证书注册**屏幕。 单击**下一步**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

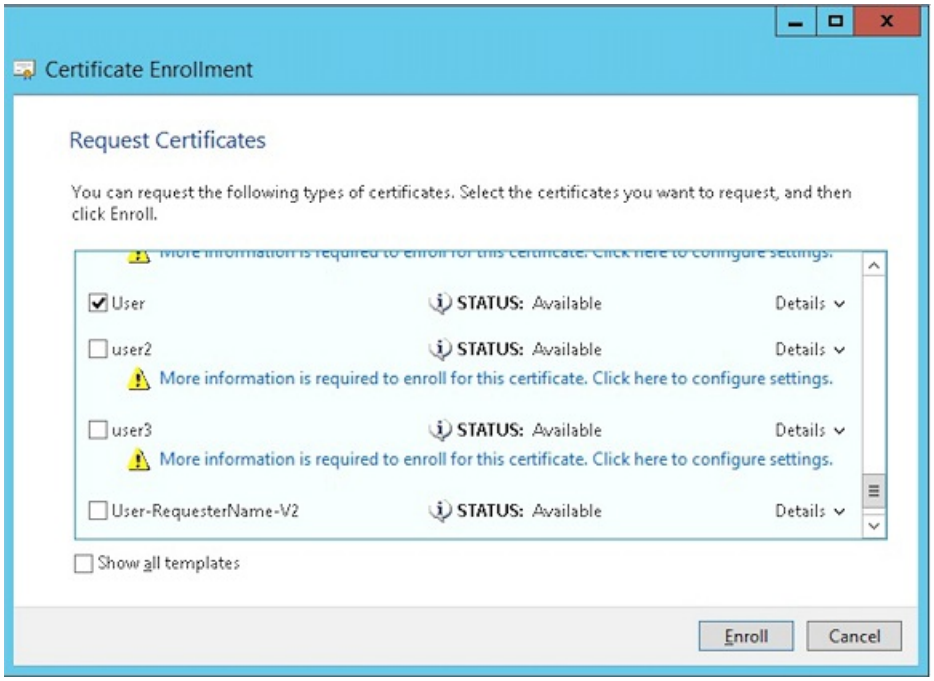


5. 选择 **Active Directory 注册策略**，然后单击**下一步**。

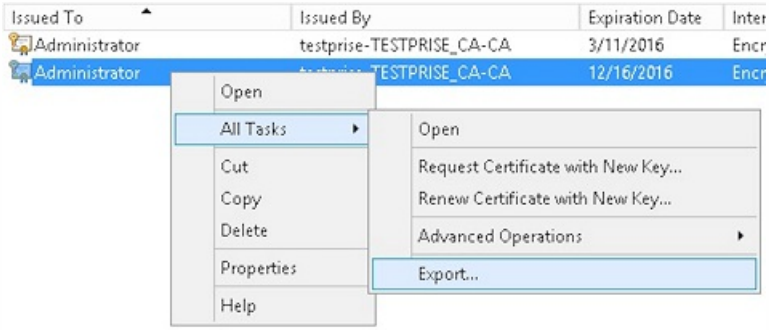


6. 选择**用户**模板，然后单击**注册**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

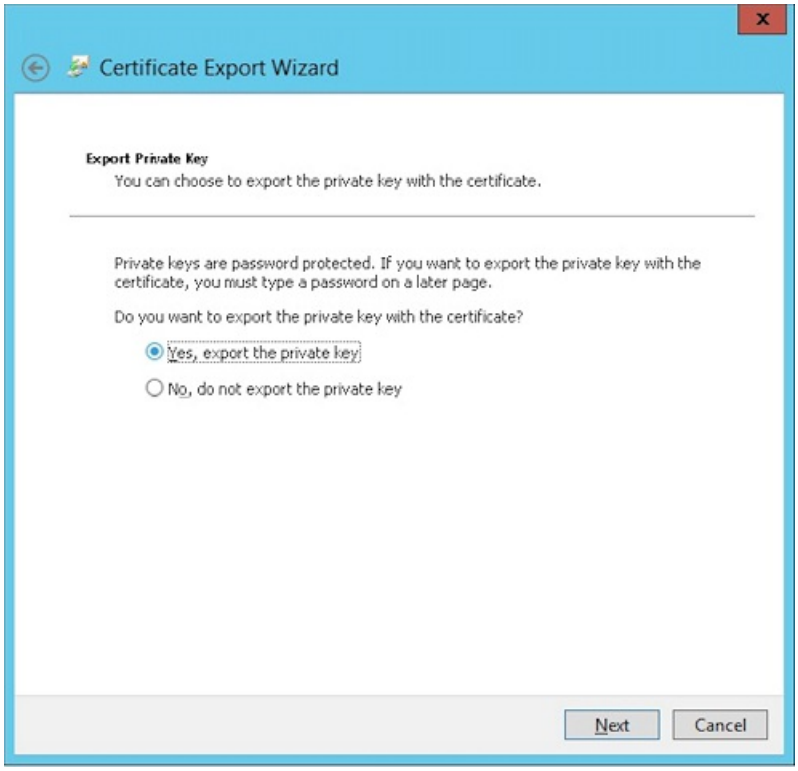


7. 导出在上一步中创建的 .pfx 文件。

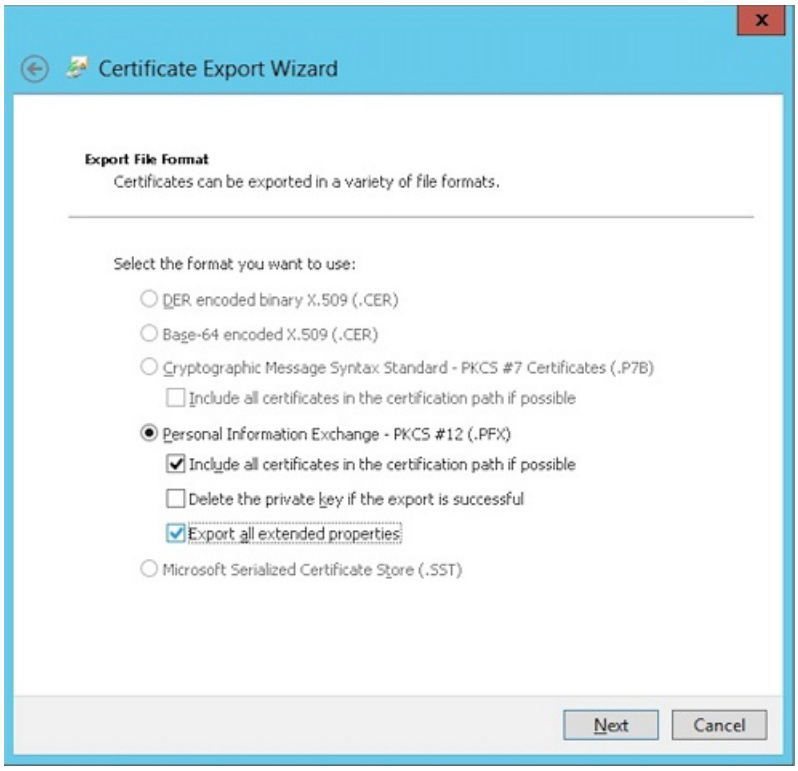


8. 单击**是**，**导出私钥**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

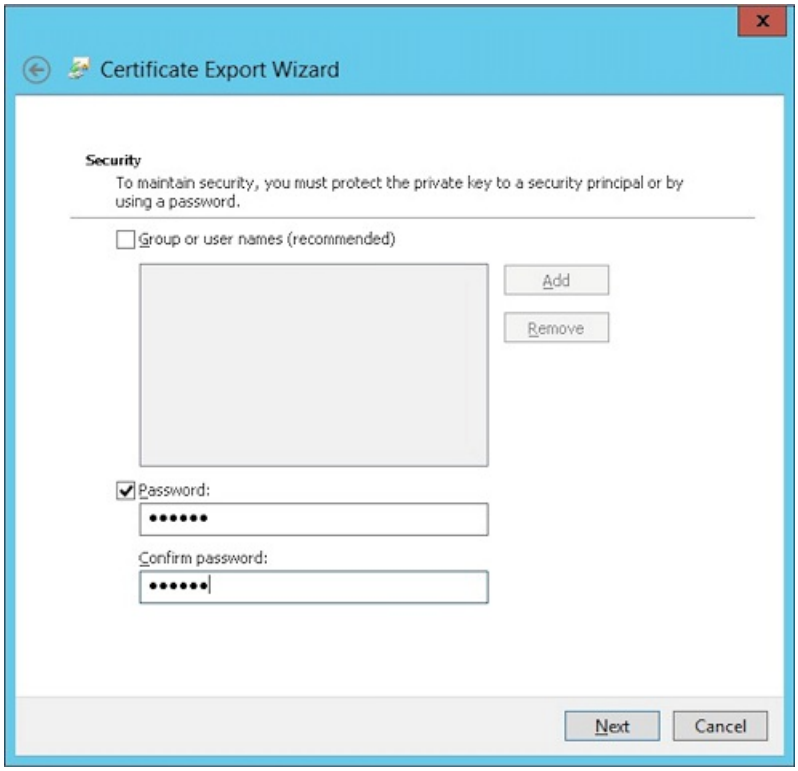


9. 选中**如果可能，则包括证书路径中的所有证书**和**导出所有扩展属性**复选框。



10. 设置要在将此证书上载到 XenMobile 中时使用的密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



11. 将证书保存到您的硬盘驱动器。

将证书上载到 XenMobile

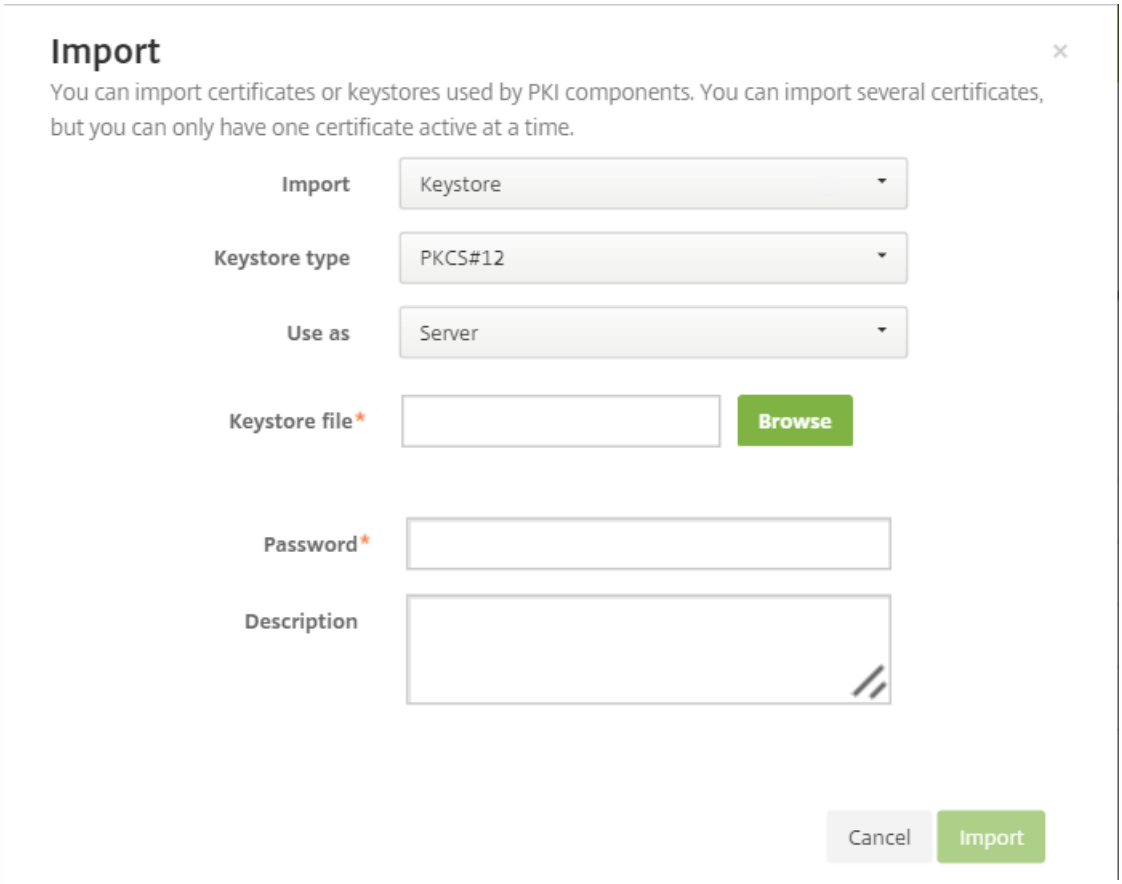
1. 在 XenMobile 控制台中，单击右上角的齿轮图标。 此时将显示**设置**屏幕。

2. 依次单击**证书**和**导入**。

3. 输入以下参数：

- **导入**：密钥库
- **密钥库类型**：PKCS#12
- **使用目的**：服务器
- **密钥库文件**：单击**浏览**选择刚刚创建的 .pfx 证书。
- **密码**：输入为此证书创建的密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 单击**导入**。

6. 验证是否已正确安装证书。 证书应显示为用户证书。

为基于证书的身份验证创建 PKI 实体

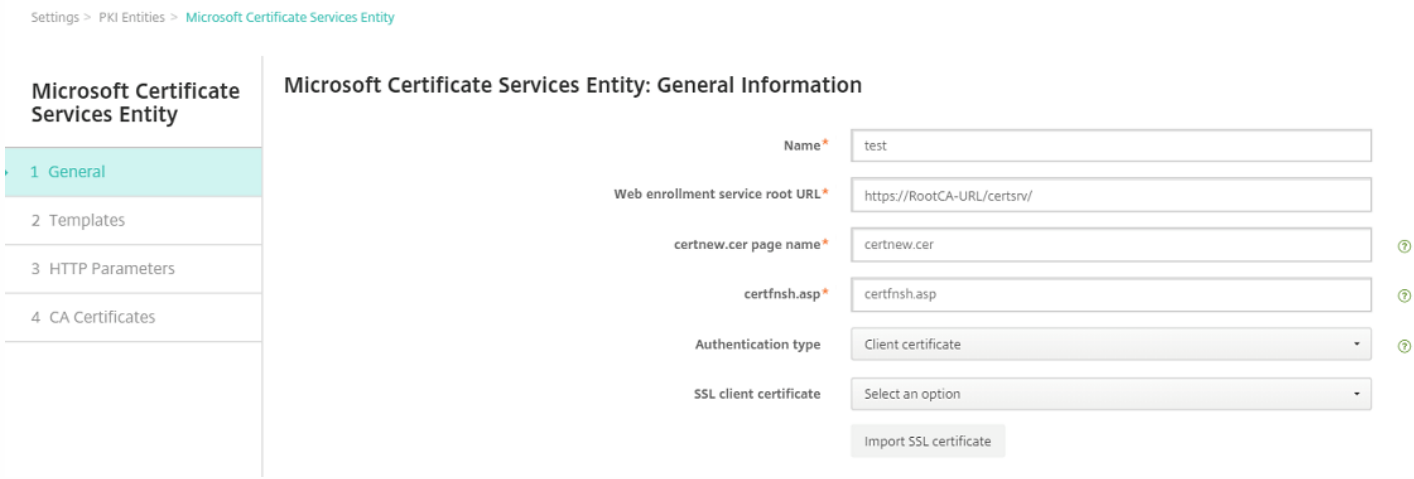
1. 在**设置**中，转至**更多 > 证书管理 > PKI 实体**。

2. 依次单击**添加**和 **Microsoft 证书服务实体**。 此时将显示“Microsoft 证书服务实体: 常规信息”屏幕。

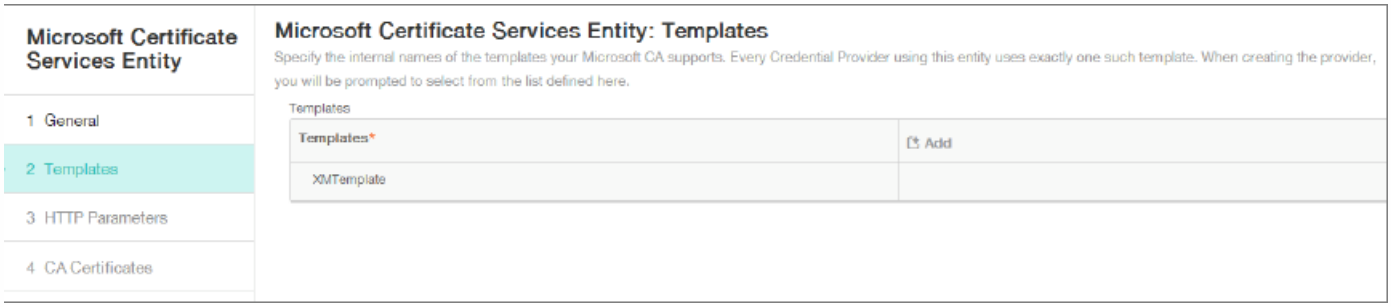
3. 输入以下参数：

- **名称**：键入任意名称
- **Web 注册服务根 URL**：https://RootCA-URL/certsrv/
  注意：请务必在 URL 路径结尾添加一个斜杠 (/)。
- **certnew.cer 页面名称**：certnew.cer（默认值）
- **certfnsh.asp**：certfnsh.asp（默认值）
- **身份验证类型**：客户端证书
- **SSL 客户端证书**：选择签署了 XenMobile 客户端证书的根 CA。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

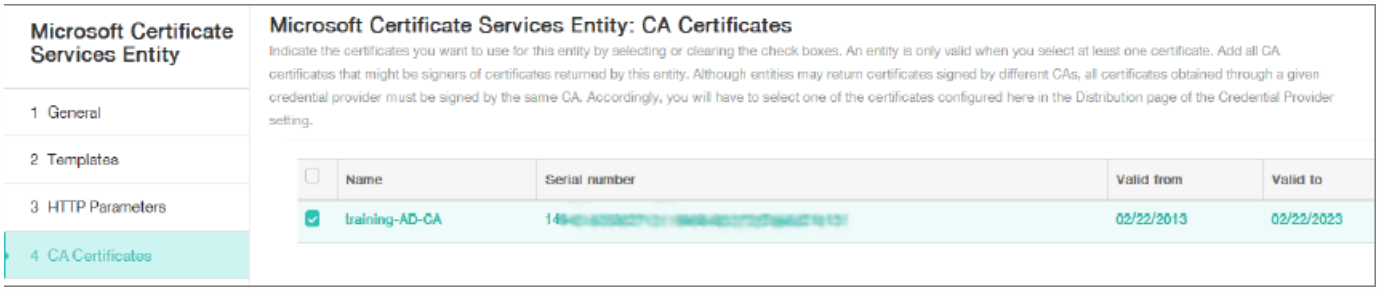


4. 在**模板**下，添加配置 Microsoft 证书时创建的模板。 请勿添加空格。



5. 跳过“HTTP 参数”，然后单击 **CA 证书**。

6. 选择要用于颁发 XenMobile 客户端证书的用户证书。 这是从 XenMobile 客户端证书中导入的链的一部分。



7. 单击**保存**。

配置凭据提供程序

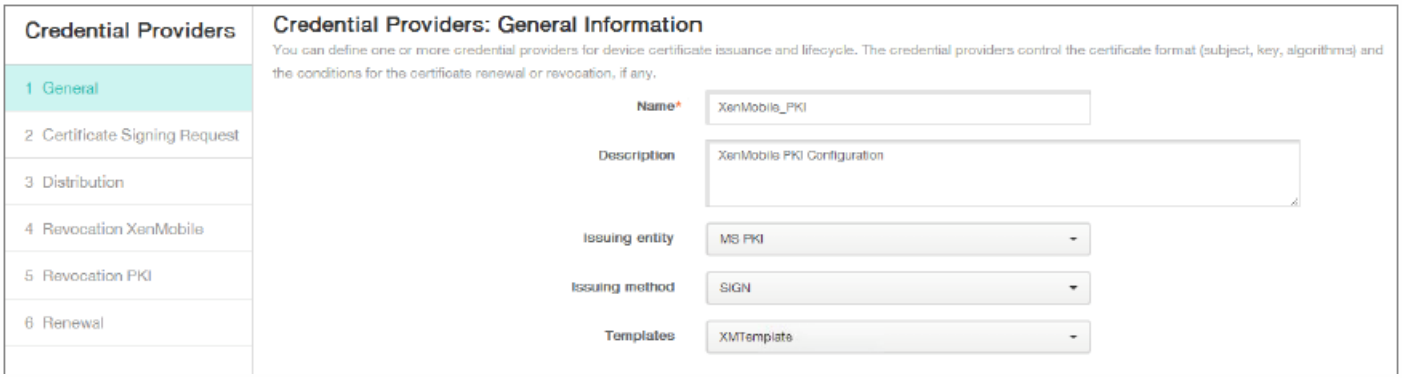
1. 在“设置”中，转至**更多 > 证书管理 > 凭据提供程序**。

2. 单击**添加**。

3. 在**常规**下，输入以下参数：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **名称**：键入任意名称。
- **说明**：键入任意说明。
- **颁发实体**：选择之前创建的 PKI 实体。
- **颁发方法**：签名
- **模板**：选择在“PKI 实体”下添加的模板。



4. 下一步，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**：SHA1withRSA
- **使用者名称**：cn=$user.username

  使用者名称引用 sAMAccountName。 这将允许 NetScaler 使用“用户名”字段进行身份验证。

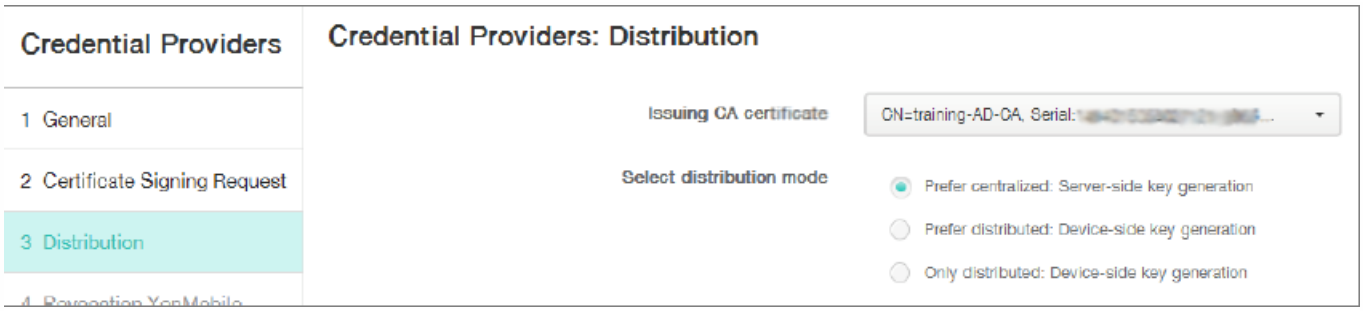
5. 对于**使用者备用名称**，请单击**添加**，然后输入以下参数：

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

6. 单击**分发**并输入以下参数：

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

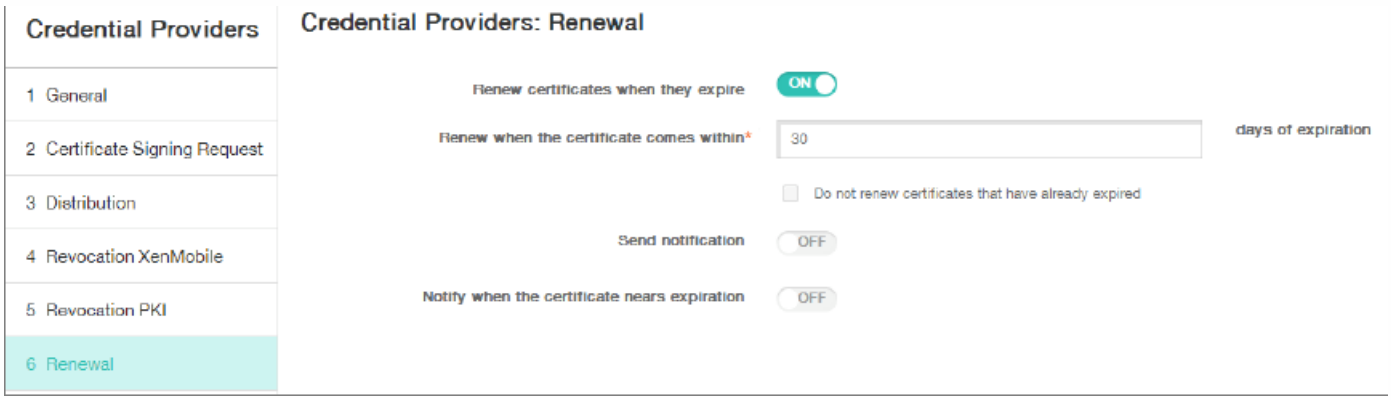


7. 对于下面两个部分，即**吊销 XenMobile** 和**吊销 PKI**，请根据需要设置参数。 鉴于本文的目的，我们将跳过这两个选项。

8. 单击**续订**。

9. 对于**在证书过期时续订**，请选择**开**。

10. 将所有其他设置保留为默认设置，或者根据需要进行更改。



11. 单击**保存**。

在 XenMobile 中配置 NetScaler 证书交付

1. 登录到 XenMobile 控制台并单击右上角的齿轮图标。 此时将显示**设置**屏幕。

2. 在**服务器**下，单击 **NetScaler Gateway**。

3. 如果尚未添加 NetScaler Gateway，请单击**添加**并指定以下设置：

    外部 URL：https://YourNetScalerGatewayURL

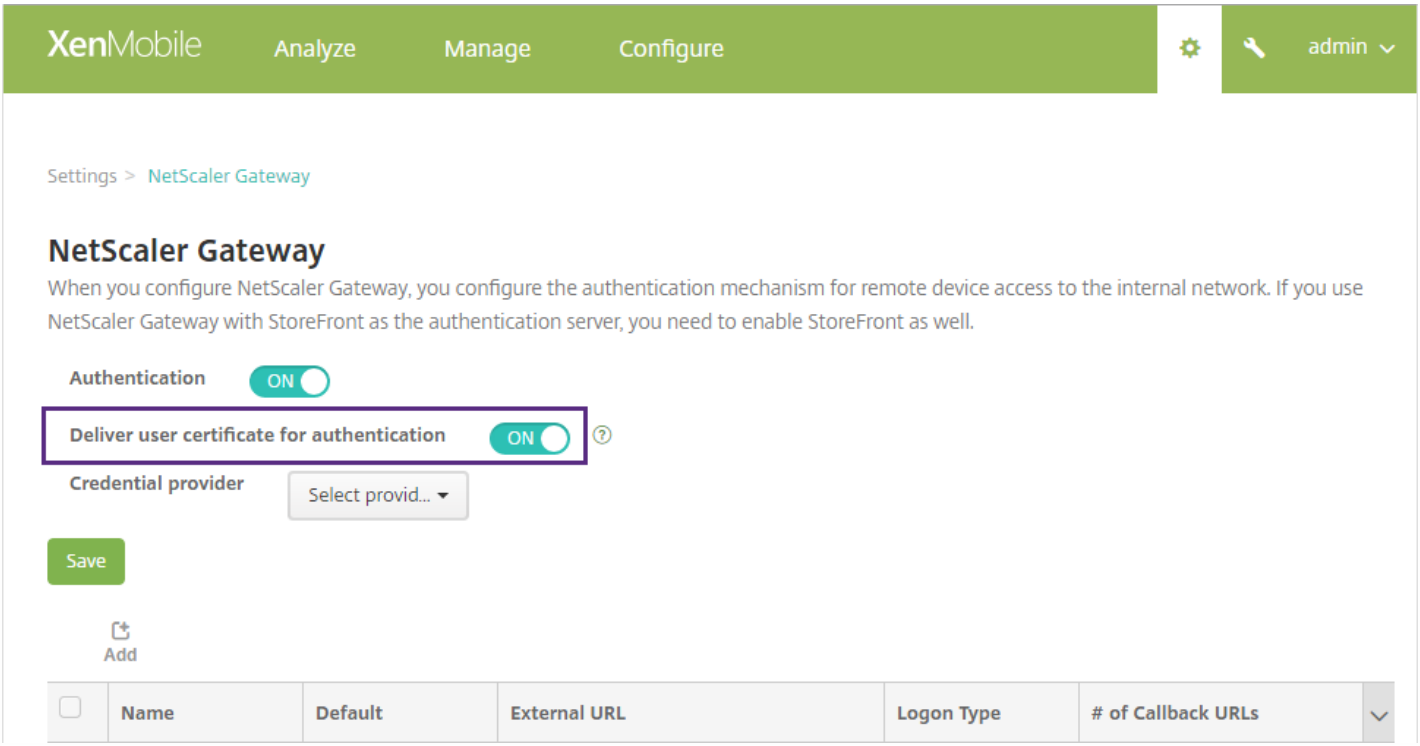
    登录类型：证书

    需要密码：关

    设为默认值：开

4. 对于**向用户提供用于身份验证的证书**，请选择**开**，然后单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 对于**凭据提供程序**，请选择一个提供程序，然后单击**保存**。

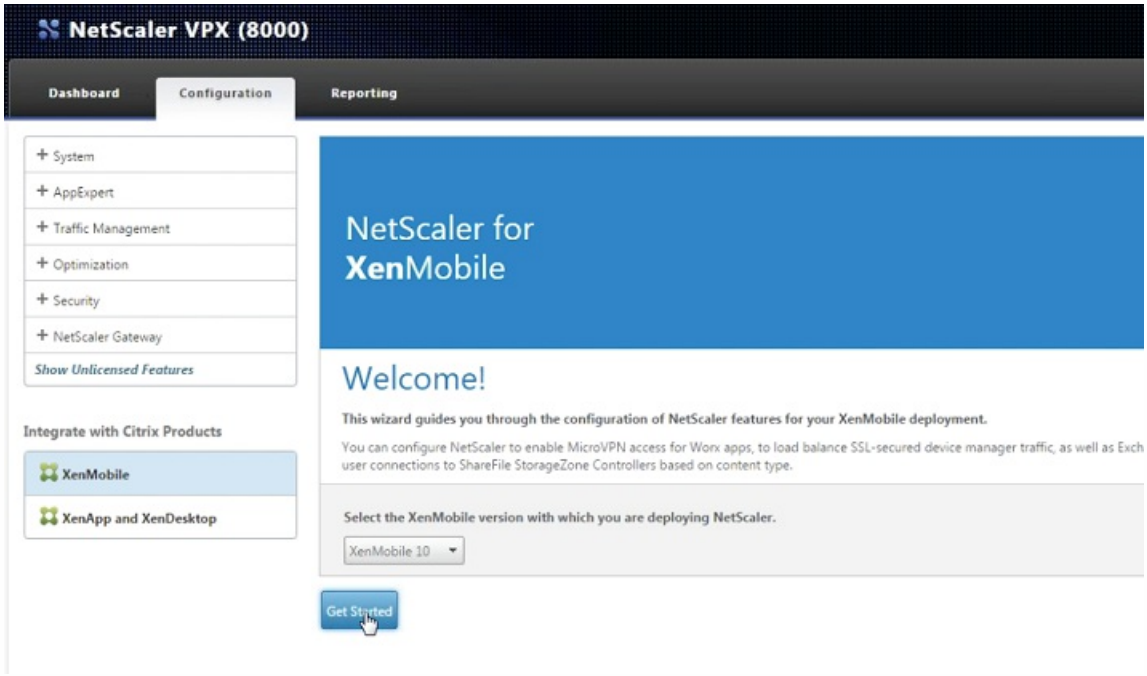
配置 NetScaler Gateway 以进行证书身份验证

请在 NetScaler 设备上执行以下步骤，在处于仅 MAM 模式的 XenMobile 中配置证书身份验证。

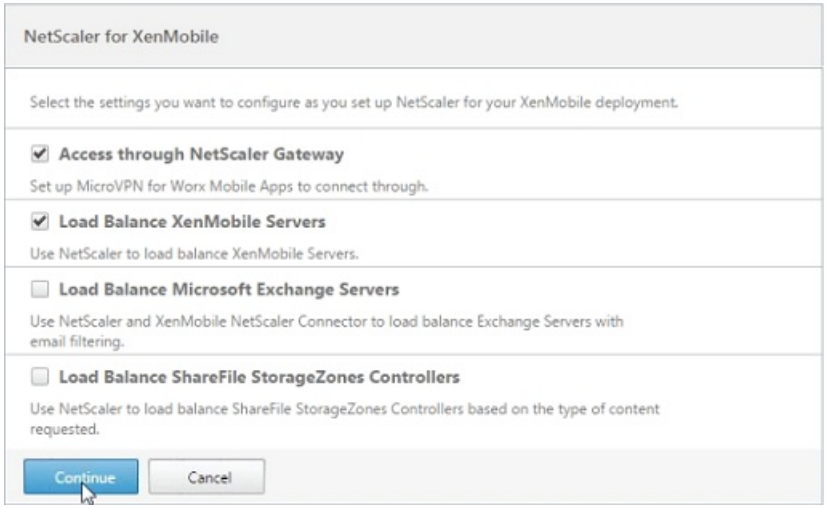
1. 登录到 NetScaler。
2. 在 **Configuration**（配置）下，转至 **Integrate with Citrix Products**（与 Citrix 产品集成），然后选择 **XenMobile**。

   此时会打开一个向导，从中可以为 XenMobile 部署配置 NetScaler 功能。
3. 选择 **XenMobile 10**。
4. 单击 **Get Started**（开始）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 在下一个屏幕上，选择 **Access through NetScaler Gateway**（通过 NetScaler Gateway 访问）和 **Load Balance XenMobile Servers**（对 XenMobile 服务器进行负载平衡），然后单击 **Continue**（继续）。



6. 在下一个屏幕上，输入面向外部的 NetScaler Gateway IP 地址，然后单击 **Continue**（继续）。

   此时会出现“Server Certificate for NetScaler Gateway”（NetScaler Gateway 服务器证书）屏幕。

7. 您可以使用现有证书，也可以安装一个。 单击 **Continue**（继续）。

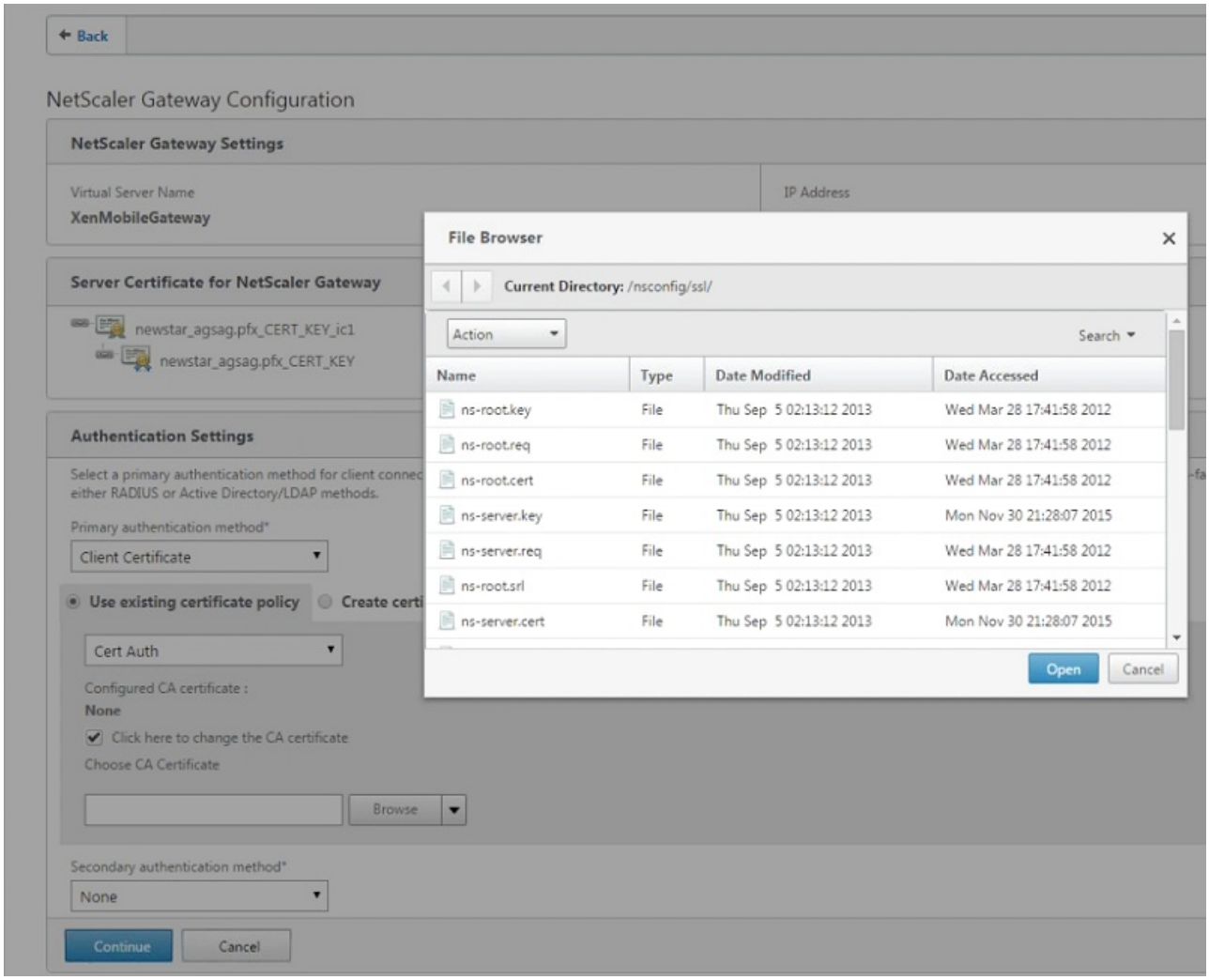
   此时会出现 **Authentication Settings**（身份验证设置）屏幕。

8. 在 **Primary authentication method**（首选身份验证方法）字段中，选择 **Client Certificate**（客户端证书）。

   此时会为接下来两个字段自动选择 **Use existing certificate policy**（使用现有证书策略）和 **Cert Auth**（证书身份验证）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

9. 选择 **Click here to change the CA certificate**（单击此处更改 CA 证书），然后在 **Browse**（浏览）列表中，导航至所需的 CA 证书。



10. 将 **Second authentication method**（辅助身份验证方法）保留为 **None**（无），然后单击 **Continue**（继续）。

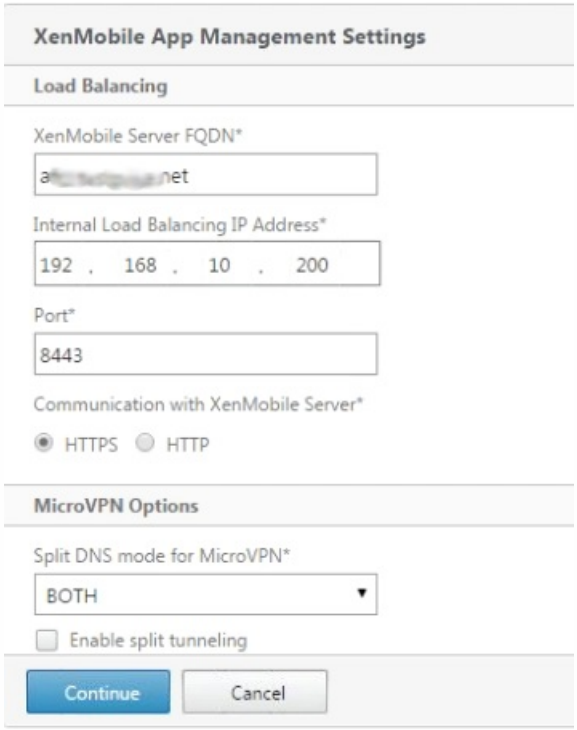
11. 在 **Load Balancing**（负载平衡）屏幕中，输入 XenMobile 服务器 FQDN 和仅 MAM 内部负载平衡 IP 地址。

12. 由于这是一个 SSL 卸载部署，请在 **Communication with XenMobile Server**（与 XenMobile 服务器通信）中选择 **HTTP**。

    此时 **Split DNS mode for MicroVPN**（为 MicroVPN 拆分 DNS 模式）字段会显示为 **BOTH**（两者）。

13. 单击 **Continue**（继续）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



14. 在 **XenMobile Server Certificate**（XenMobile 服务器证书）屏幕中，选择现有服务器证书或安装一个新证书。 如果正在运行多个 XenMobile 服务器，则需要为每个服务器添加一个证书。 单击 **Continue**（继续）。

15. 在 **Device certificate**（设备证书）屏幕中，如果尚未安装任何证书，则需要从 XenMobile 控制台导出此证书。 对此，请执行以下操作：

a. 在控制台中单击右上角齿轮图标，打开 **Settings**（设置）屏幕。

b. 单击 **Certificate**（证书），然后从列表中选择 CA 证书。

c. 单击 **Export**（导出）。

d. 返回 NetScaler 向导，选择已导出（已下载）的证书进行安装。

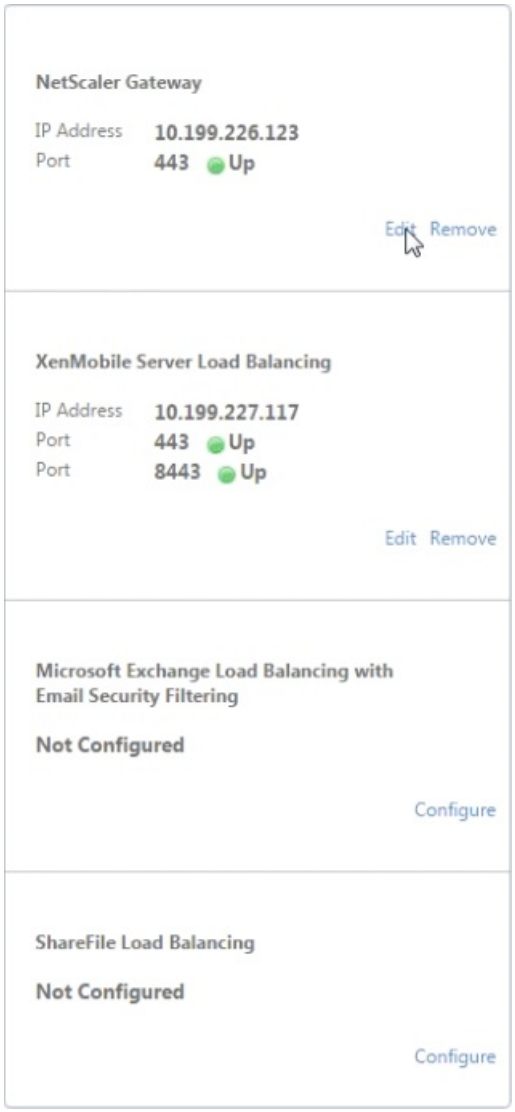
e. 单击 **Continue**（继续）。

此时会显示已配置的 XenMobile 服务器 IP 地址。

16. 单击 **Continue**（继续）。

在 NetScaler 控制板上，确认已配置 NetScaler Gateway 和 XenMobile 负载平衡：

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备注册限制

Aug 11, 2016

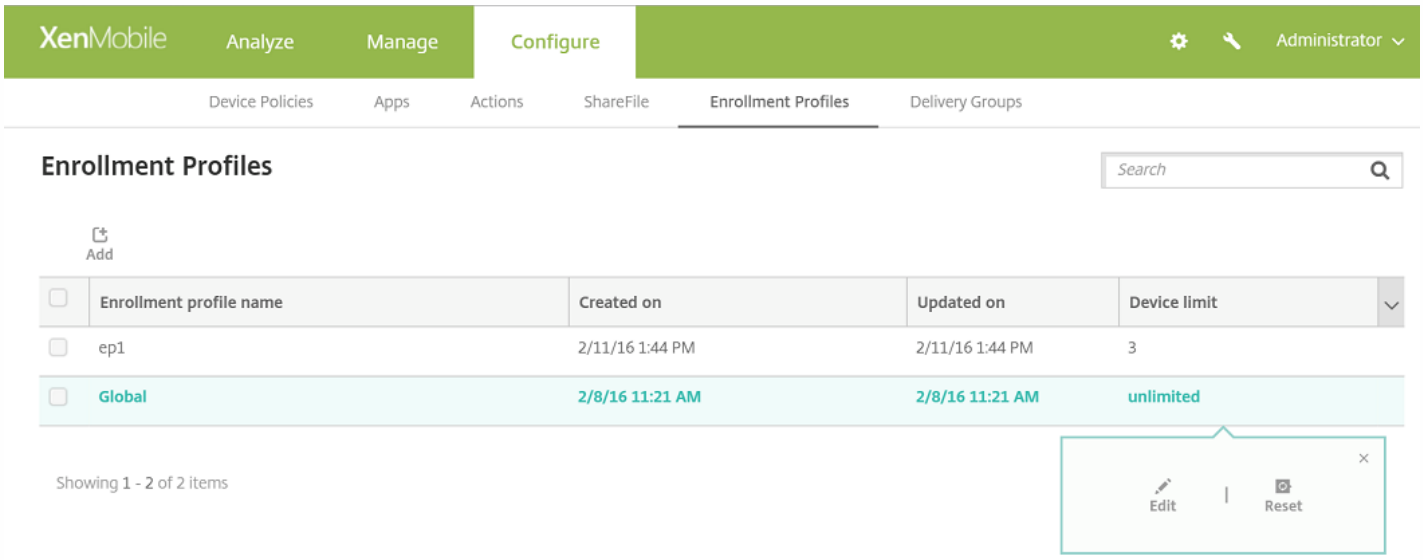
处于 ENT、MDM 和 MAM 服务器模式时，您可以在 XenMobile 控制台的**配置 > 注册配置文件**下，限制用户可注册的设备数量。 这些限制可应用到全局，或按交付组应用。 您可以创建多个注册配置文件，并将它们与不同交付组关联起来。

如果未设置限制，则用户可以注册的设备数量不受限制。 此功能仅支持在 iOS 和 Android 设备上使用。 有关注册 Windows 设备的信息，请参阅 Windows 设备。

配置全局设备注册限制

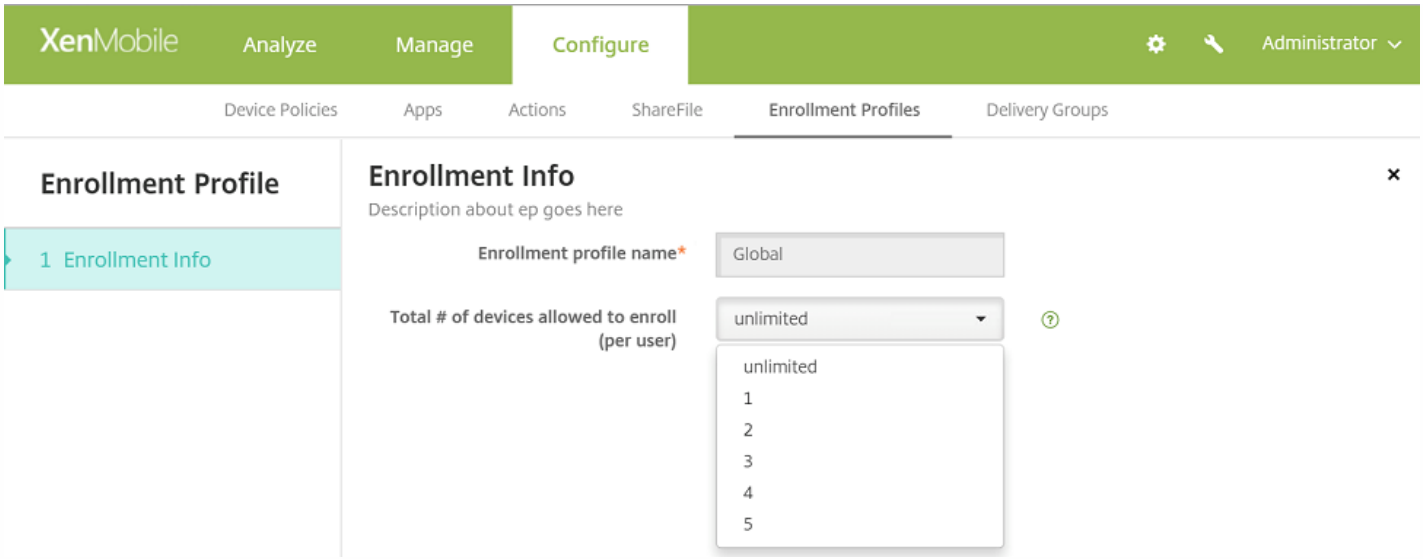
1. 转至**配置 > 注册配置文件**。

2. 单击**全局**，然后选择**编辑**。



此时会显示**注册信息**屏幕，其中**全局**自动填充为配置文件名称。 在此屏幕中，您可以选择允许用户注册的设备总数。 此限制会应用于所有 XenMobile 注册人。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

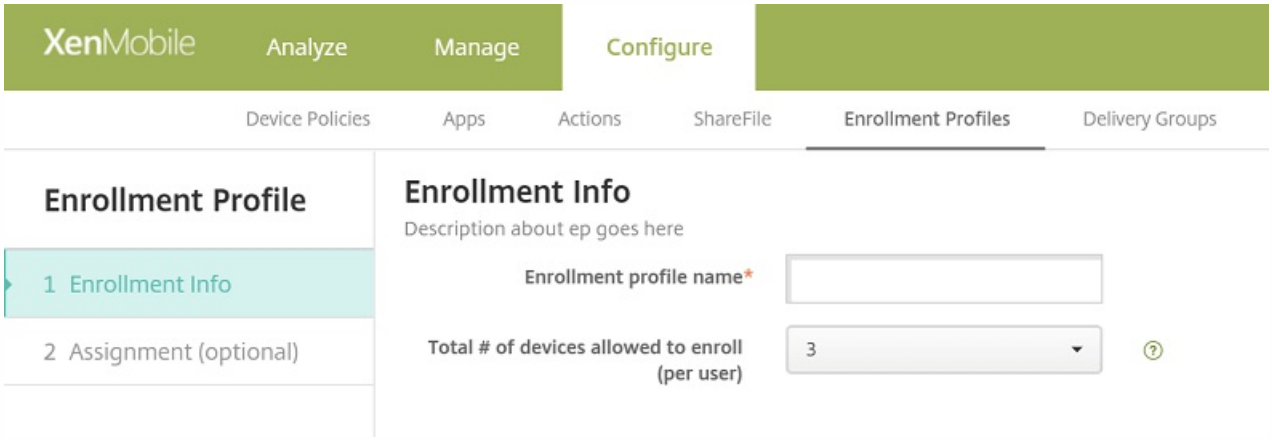


配置交付组设备注册限制

1. 转至**配置 > 注册配置文件 > 添加**。

   此时会显示**注册信息**屏幕。

2. 输入新的注册配置文件的名称，然后选择此配置文件的成员允许注册的设备数量。

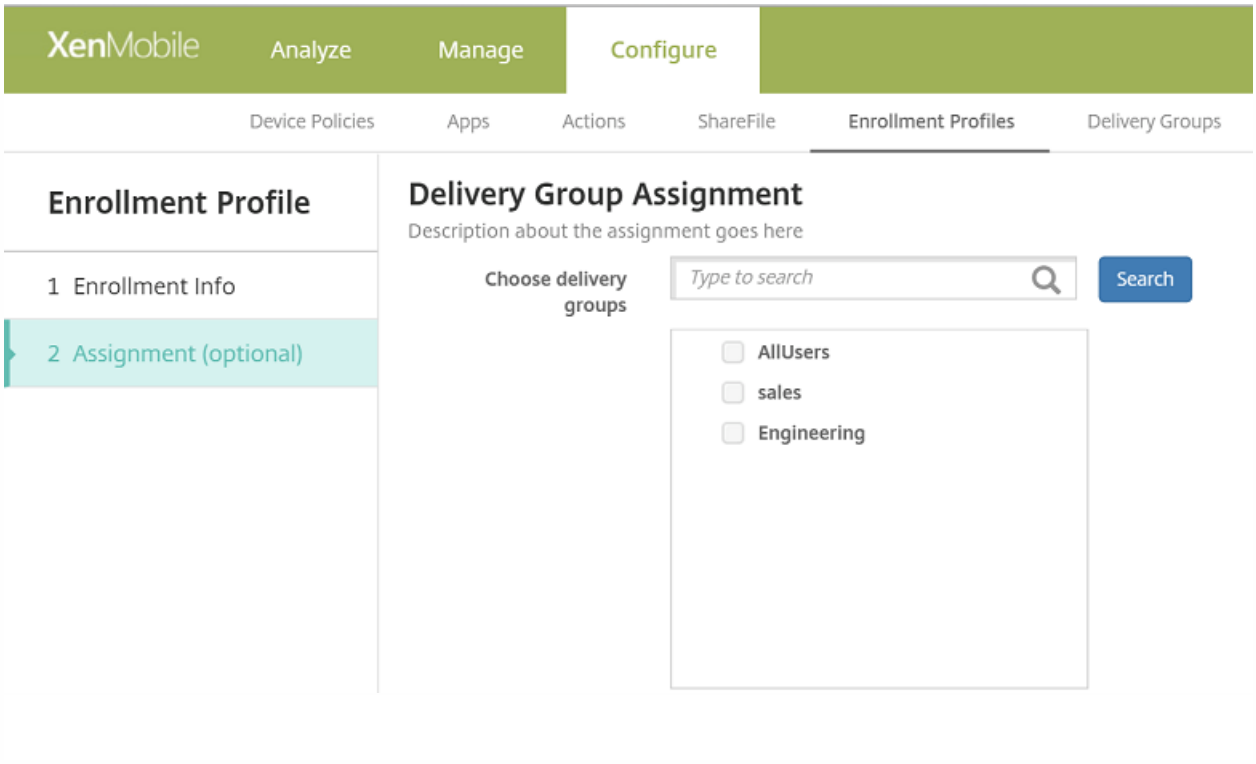


3. 单击**下一步**。

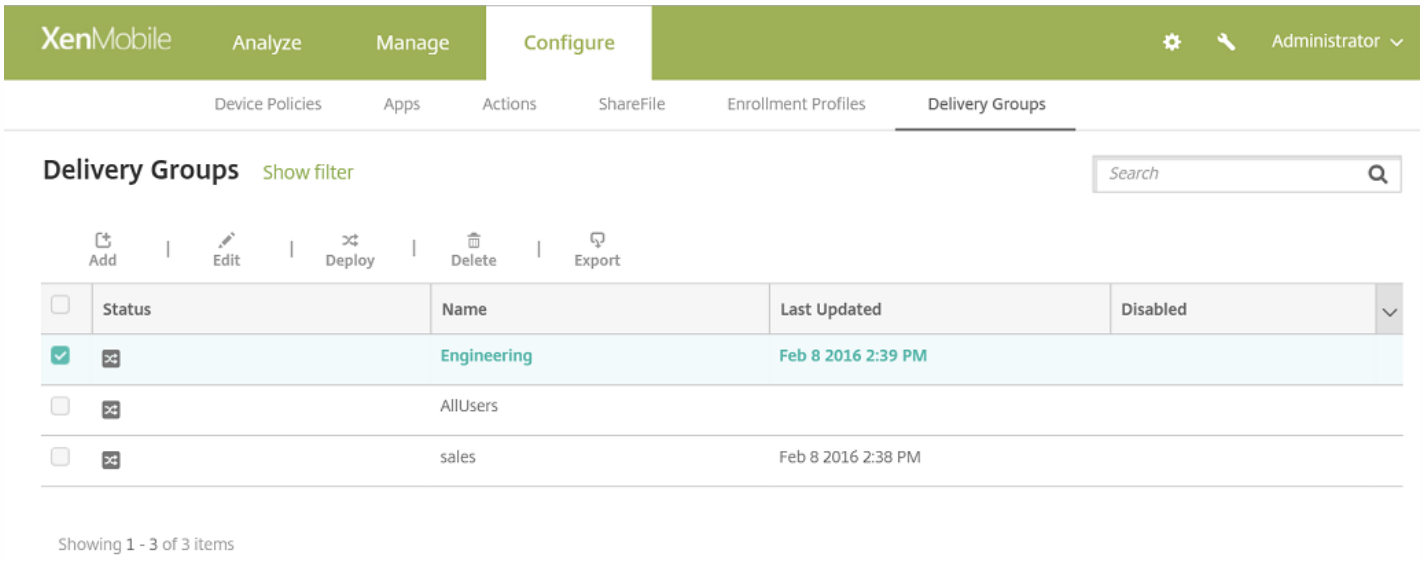
   此时会显示**交付组分配**屏幕。

4. 选择要将设备注册限制应用到的交付组，然后单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



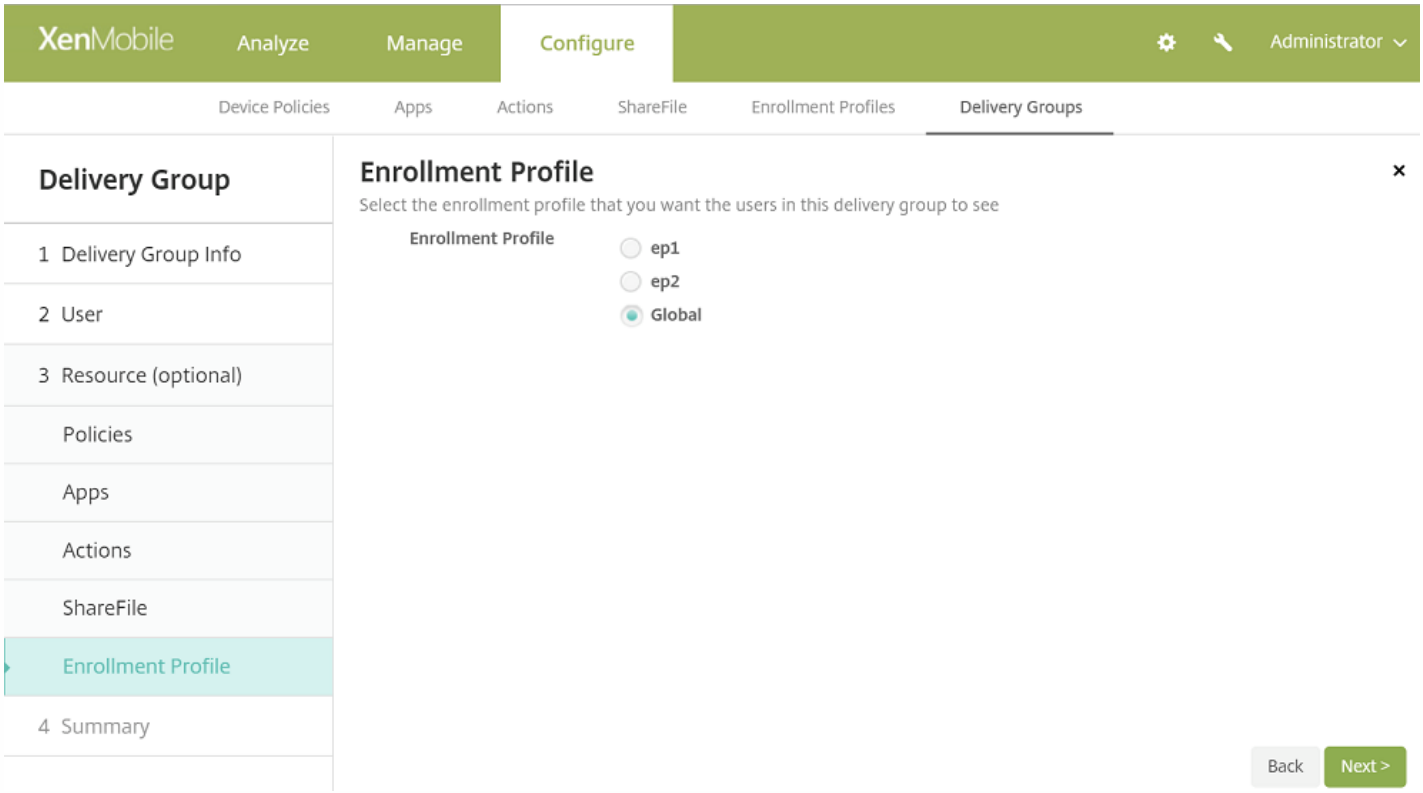
如果以后要更改交付组的注册配置文件，请转至**配置 > 交付组**。 选择所需的交付组，然后单击**编辑**。



此时会显示**注册配置文件**屏幕。

5. 在此屏幕中，选择要应用到此交付组的注册配置文件，然后单击**下一步**查看并保存更改。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



实行设备注册限制时的用户体验

设置了设备注册限制后，如果用户尝试注册一个新设备，他们要遵循以下步骤：

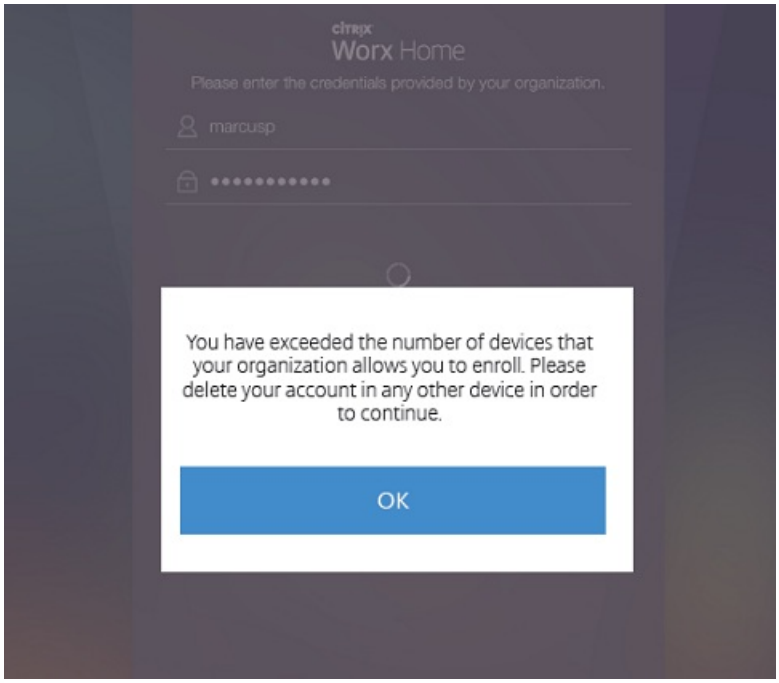
1. 登录到 Worx Home。

2. 输入要注册的服务器地址。

3. 输入凭据。

4. 如果达到了设备限制，则会显示一条错误消息，告知用户注册设备数已超过上限，他们应联系管理员。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



此时会再次显示 Worx Home 注册屏幕。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

面向仅 MAM 模式的应用程序锁定和应用程序擦除操作

Aug 15, 2016

您可以通过创建操作，在用户设备上针对特定触发器（例如安装不允许使用的应用程序或将用户从 Active Directory 中删除）建立自动响应机制。 您也可以向用户发送通知，要求他们解决问题，以免将来需要采取更重大的措施。

从 XenMobile 10.3.5 起，您可以针对 XenMobile 控制台中列出的全部四种类型触发器（即事件、设备属性、用户属性和已安装应用程序的名称），采取擦除或锁定应用程序这一响应方式。 以前，只有事件类型触发器具备此功能。

要配置自动擦除或锁定应用程序的功能，请执行以下操作：

1. 在 XenMobile 控制台中，单击**配置 > 操作**。

2. 在**操作**页面上，单击**添加**。

3. 在**操作信息**页面上，输入操作名称和可选的说明。

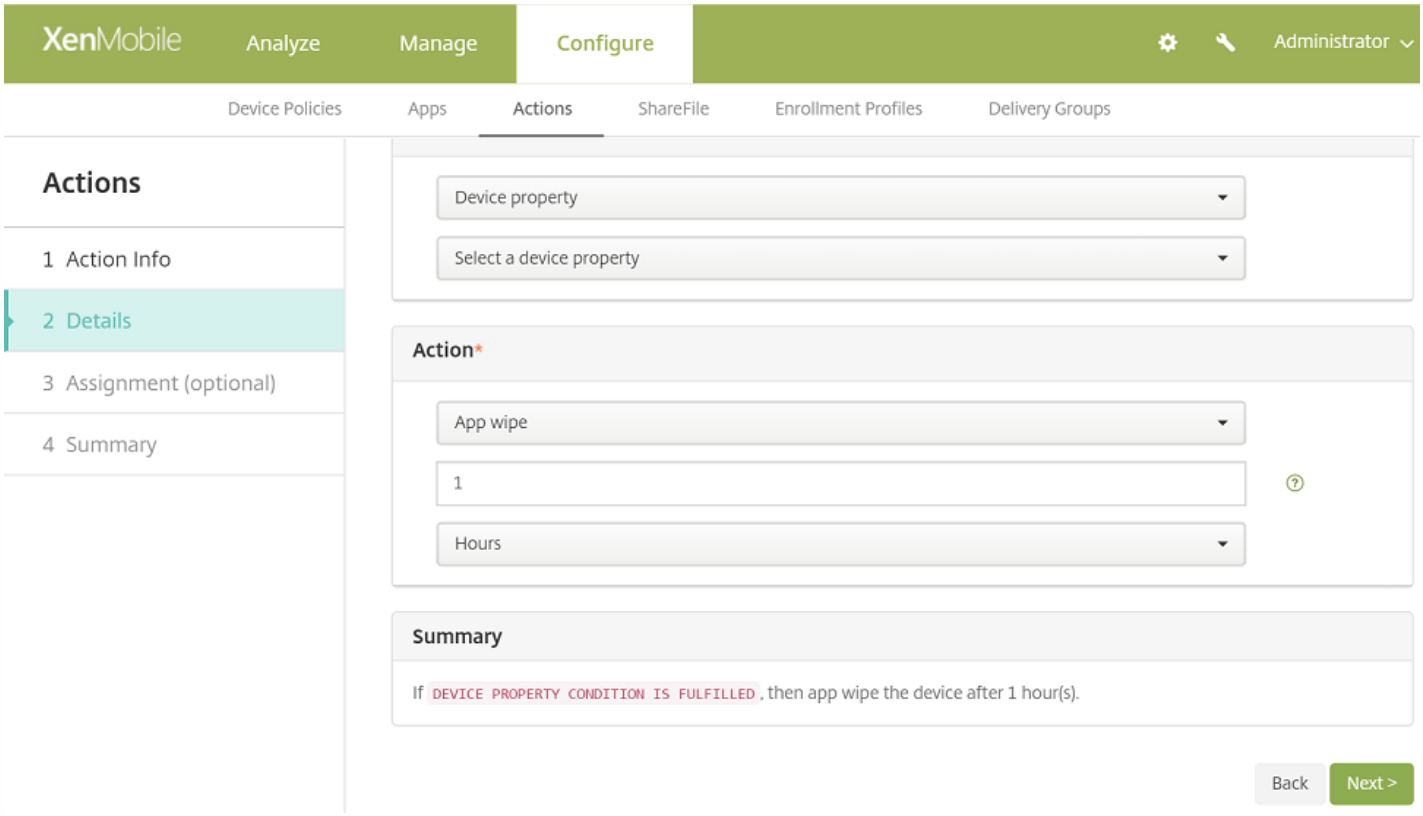
4. 在**操作详细信息**页面上，选择所需的触发器。

5. 在**操作**中，选择**应用程序擦除**或**应用程序锁定**。

每个选项都会自动设置 1 小时延迟，但也可选择以分钟、小时或天为单位的延迟期限。 设置延迟后，用户便有时间在系统执行操作前修复问题。 可以在 RBAC 角色和权限一文中了解与应用程序擦除和应用程序锁定操作有关的更多信息。

> **注意**
>
> 在系统执行操作前，操作还可能会再延迟一小时左右，以便允许 Active Directory 数据库与 XenMobile 同步。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**。

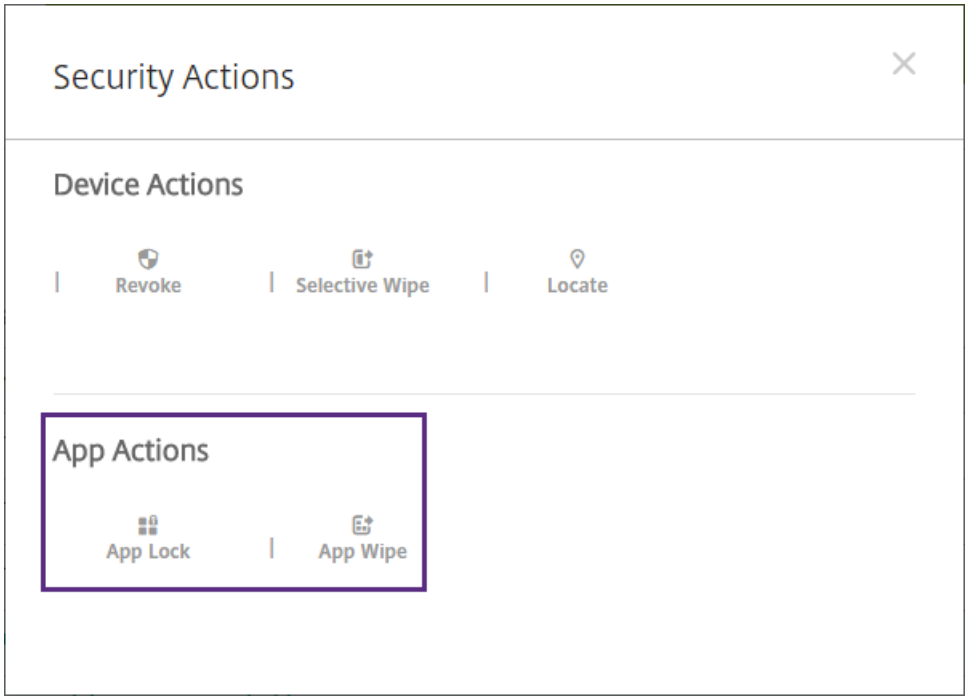
要执行应用程序锁定、解锁、擦除或取消擦除操作，请执行以下步骤：

1. 转至**管理 > 设备**，选择设备，然后单击**安全**。

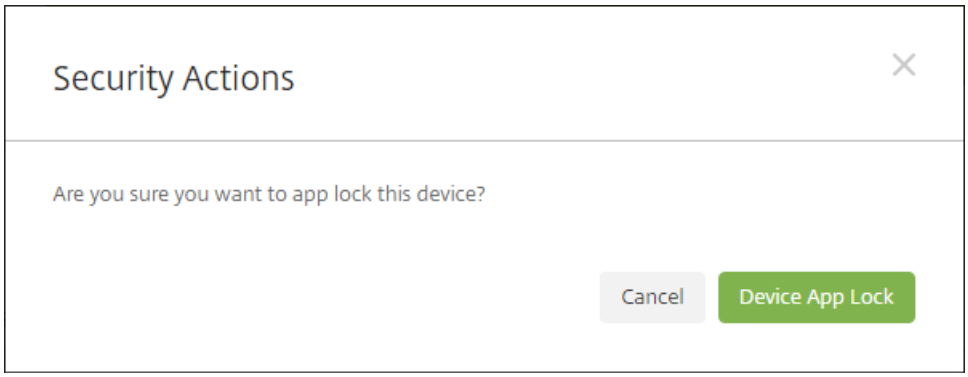
2. 在**安全操作**对话框中，单击某项操作。

> 注意：还可以使用此对话框为已知被禁用或从 Active Directory 中删除的用户检查设备的状态。 “应用程序解锁”或“应用程序取消擦除”操作的存在指示用户的应用程序当前已被锁定或被擦除。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



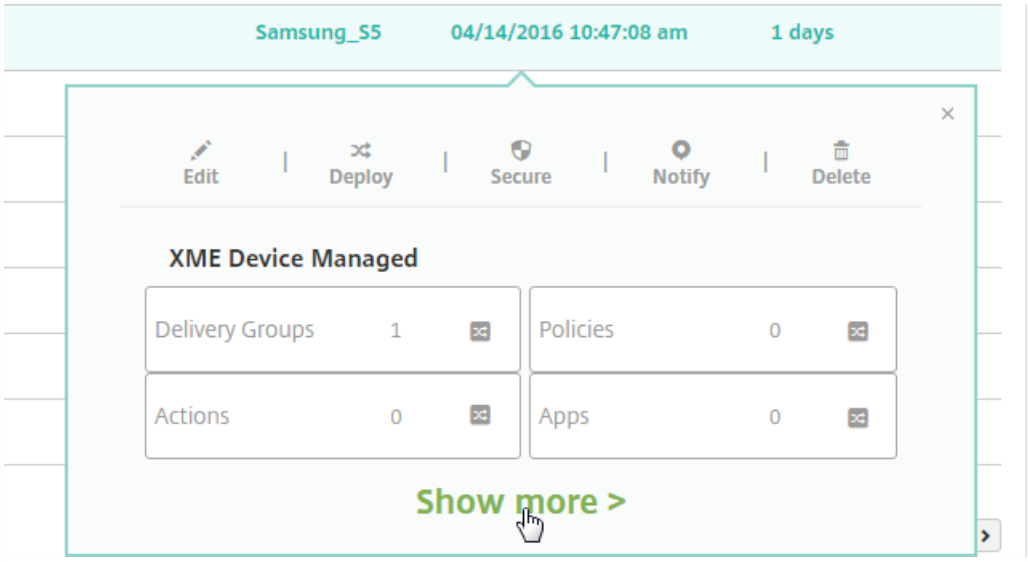
3. 确认操作。



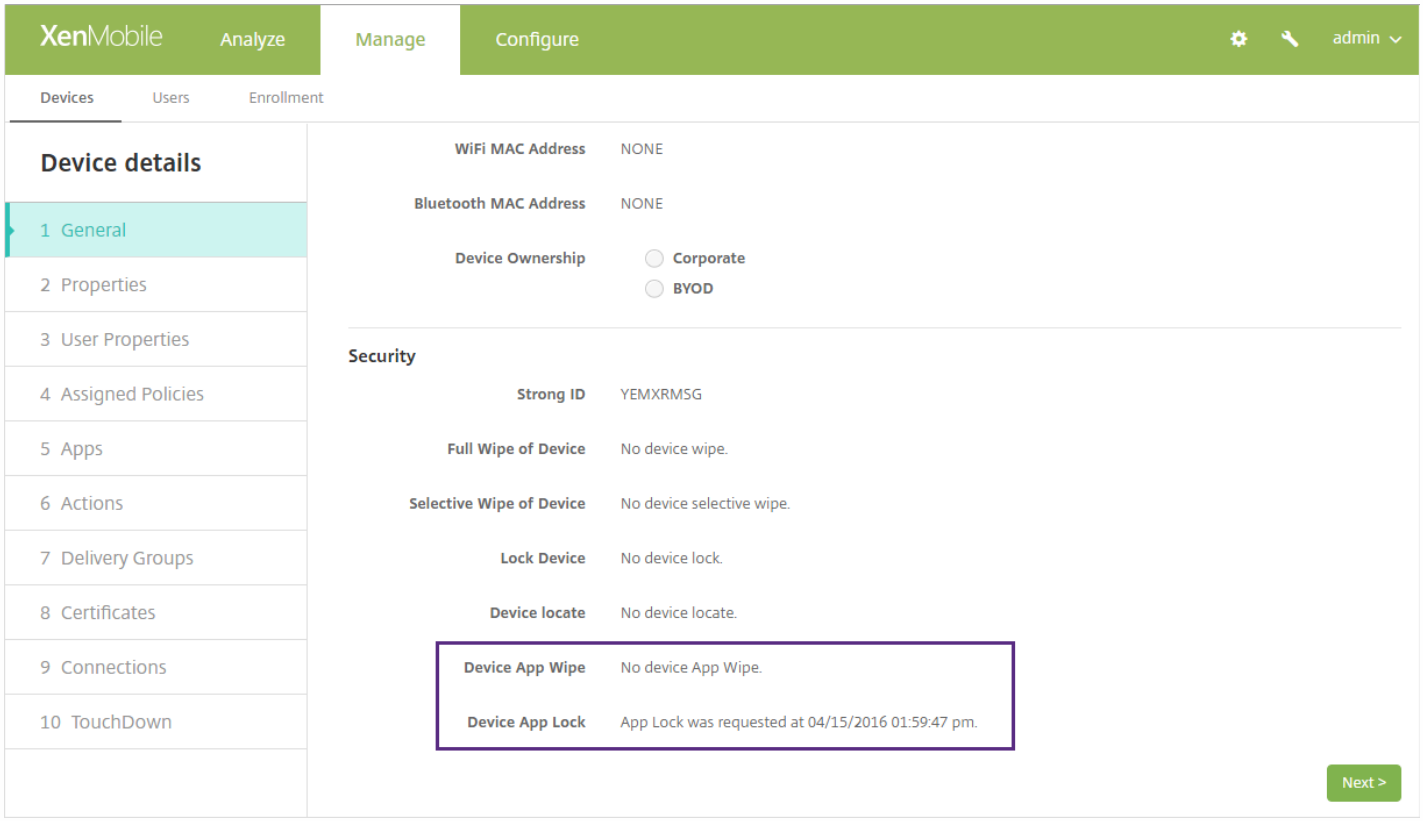
要检查应用程序锁定或应用程序擦除状态，请执行以下步骤：

1. 转至**管理 > 设备**，单击某个设备，然后单击**显示更多**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 滚动到**设备应用程序擦除**和**设备应用程序锁定**。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

面向仅 MAM 模式的 REST 服务 API

Aug 11, 2016

在仅使用 MAM 的设备上，可以使用任意 REST 客户端和 XenMobile REST API 调用通过 XenMobile 控制台公开的 REST 服务。 使用该 API 时，无需登录 XenMobile 控制台即可调用本部分中所述的任何服务。

可以使用 REST 客户端调用 REST API 服务。

通过新的 REST API，您可以：

- **发送邀请 URL 和一次性 PIN**

  可以通过 XenMobile REST API 允许用户利用自助服务门户为自带设备申请访问权限。 申请获得批准后，系统会调用 XenMobile 服务器，并发出一个请求以执行下列操作：

  - 生成注册邀请 URL 并发送给用户。

  - 生成一次性 PIN 并发送给用户。

  注意：此功能仅支持 iOS 和 Android 设备，不支持 Windows 设备。

- **在设备上发出应用程序锁定和应用程序擦除**

  您可以使用 XenMobile API 搜索所有设备，然后从中找到属于某个用户的设备，以便擦除该设备上的所有应用程序或锁定应用程序。

本文其余部分将列出自发布 XenMobile 10.3.5 以来推出的设备 API 和一次性 PIN 注册 API。 要查看有关当前可用的一组 API 的完整文档，请下载 XenMobile REST API 参考 PDF。

设备 APIs

- 通过过滤器获取设备
- 通过 ID 获取设备信息
- 通过设备 ID 获取设备应用程序
- 通过设备 ID 获取设备操作
- 通过设备 ID 获取设备交付组
- 通过设备 ID 获取设备管理的软件清单
- 通过设备 ID 获取设备策略
- 通过设备 ID 获取设备软件清单
- 通过设备 ID 获取设备 GPS 坐标
- 向一系列设备/用户发送通知
- 向一系列设备授权
- 在一系列设备上执行激活锁跳过
- 在一系列设备上执行应用程序锁定
- 在一系列设备上执行应用程序擦除
- 在一系列设备上执行容器锁定
- 在一系列设备上取消容器锁定
- 在一系列设备上执行容器解锁

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在一系列设备上取消容器解锁
- 在一系列设备上重置容器密码
- 在一系列设备上取消重置容器密码
- 否认拥有一系列设备
- 定位一系列设备
- 取消定位一系列设备
- 对一系列设备执行 GPS 跟踪
- 对一系列设备取消 GPS 跟踪
- 锁定一系列设备
- 取消锁定一系列设备
- 解锁一系列设备
- 取消解锁一系列设备
- 部署一系列设备
- 在一系列设备上请求 AirPlay 镜像
- 在一系列设备上取消请求 AirPlay 镜像
- 在一系列设备上停止 AirPlay 镜像
- 在一系列设备上取消停止 AirPlay 镜像
- 在一系列设备上清除限制
- 在一系列设备上取消清除限制
- 吊销一系列设备
- 在一系列设备上响铃
- 在一系列设备上取消响铃
- 擦除一系列设备
- 取消擦除一系列设备
- 在一系列设备上执行选择性擦除
- 在一系列设备上取消选择性擦除
- 在一系列设备上执行 SD 卡擦除
- 在一系列设备上取消 SD 卡擦除
- 获取设备的所有已知属性
- 获取设备的所有已使用属性
- 通过设备 ID 检索所有设备属性
- 通过设备 ID 批量更新所有设备属性。
- 通过设备 ID 添加或更新设备属性
- 通过设备 ID 删除设备属性
- 通过设备 ID 检索设备的 iOS MDM 状态
- 生成 PIN 代码

一次性 PIN 注册 API

- 获取注册模式
- 获取注册信息
- 触发注册通知
- 创建注册邀请
- 通过过滤器获取注册记录

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 10.3.5 中的已知和已修复问题

Aug 15, 2016

XenMobile 10.3.5 中的已知问题或已修复问题如下：

已知问题

- 限制：新的仅 MAM 模式的功能（例如，基于证书的身份验证、应用程序锁定和应用程序擦除操作以及仅 MAM API）对 Windows Phone 不可用。
- 用户多次在 Worx Home 中重新注册，然后尝试从 WorxStore 中安装应用程序时，显示一条错误，指出已删除该应用程序。 解决方法：可以在 XenMobile 控制台的**管理 > 设备**中删除该设备，然后请求该用户重新注册。 [#611172]
- SSL 侦听器证书必须是公用证书，才能注册 Windows 设备。 如果上载了自签名 SSL 证书，注册将失败。 [#618390]
- 设备注册数达到在 XenMobile 控制台中设置的限制时，设备上并未显示相应的错误消息，但用户无法注册。 [#623475]
- 用户通过 Azure Active Directory 帐户在 XenMobile 中注册时，即便擦除或吊销了设备，他们也可在未经授权的情况下重新注册。 这是第三方问题。 [#628865]
- 在 XenMobile 控制台中删除 iOS 设备后，如果用户在 XenMobile Enterprise 模式（MAM 和 MDM）以及 MAM 模式下重新注册设备，偶尔会出现注册失败的情况。 [#629021]
- 在 XenMobile 服务器中禁用证书续订选项时，用户仍可在 Worx Home 中续订过期证书。 [#630894]
- 某些 VPP 许可证的 ID 为负数，例如 -123441212，以致于无法分发公共应用程序。 [#631443]
- 如果为 Google Play 凭据配置了无效的设备 ID，则当您为 Google Play 添加公共应用商店应用程序并单击以在 Google Play 应用商店中搜索该应用程序名称时，搜索失败，或者呈现不正确的搜索结果。 [#633845]
- 根据 XenMobile **设置 > Google Play 凭据**页面上的说明，当前不能在您的手机上通过输入 *#*#8255#*#* 查找 Android ID。 请使用 Google Play 应用商店中的设备 ID 应用程序查找您的设备 ID。 [#633854]
- 在 XenMobile 控制台中，**设置 > 基于角色的访问控制**存在下列与默认设置相关的问题。
  - 在适用于云部署的 XenMobile 控制台中，默认情况下会为管理员角色设置**共享设备注册人员**权限。 默认情况下不应设置此权限。 [#638069]
  - 现在，控制台功能权限**否认拥有设备**已弃用，不应出现。 [#638303]
  - 在适用于内部部署的 XenMobile 控制台中，默认情况下不会为管理员角色选择以下功能。 请务必根据需要为默认管理员角色选择这些设置，或为您已通过管理模板创建的任何角色选择这些设置。 [#638314]

    锁定容器
    解锁容器
    重置容器密码
    不使用激活锁
    使设备响铃

  - 在适用于内部部署和云部署的 XenMobile 控制台中，默认情况下不会为管理员角色选择以下功能。 请务必根据需要为默认管理员角色选择这些设置，或为您已通过管理模板创建的任何角色选择这些设置。 [#638322]

    请求使用 AirPlay 镜像
    停止使用 AirPlay 镜像

已修复的问题

- XenMobile 和 Hyper-V 之间的时间同步问题会导致 ShareFile SSO 身份验证失败。 [#588249]
- 如果在 XenMobile LDAP 设置中启用嵌套，并为交付组和 RBAC 设置配置了对应的域组，则以后在 LDAP 设置中删除域时，嵌套的组信息仍会保留在数据库中。 [#590363]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 从 Active Directory 中删除用户后，他们仍可打开 WorxStore 并订阅应用程序。 [#592825]
- 在 XenMobile 控制台中检查公共应用商店的应用程序更新时，Worx Home 会将公共应用程序商店的应用程序更新至最新版本，但设备上的应用程序仍出现在待更新列表中。 [#593034]
- 用户在 WorxMail 中收到来自 Exchange 帐户的日历邀请时，邀请并未按预期立即抵达。 [#594542]
- 将 iOS 设备注册至 Device Enrollment Program (DEP) 时，Worx Home 可能不会下载到 iOS 设备上。 [#595822]
- 未配置 NTP 客户端时，XenMobile 服务器可能会出现时间偏移问题，例如 ShareFile 的 SAML Single Sign-On (SSO) 失败。

  注意：请执行以下配置以启用修复：

  1. 在安装了 XenMobile 的虚拟机管理程序（Citrix XenServer 或 VMware ESXi）上登录 XenMobile 命令行接口。

  2.转至 **[2] System**（[2] 系统）。

  3.转至 **[3] Set NTP Server**（[3] 设置 NTP 服务器），并提供 NTP 服务器详细信息。

  4.重新启动服务器。

  重要：如果系统配置为群集模式，请在每个节点上执行上述配置。 [#597757]

- 用户尝试在 Worx Home 中删除应用程序或 Web 链接时，出现以下错误：无法连接 Worx Home。 [#599934]
- 如果用户的多个 PIN 处于挂起状态，基于 PIN 的注册可能会失败。 [#600264]
- 将 VPP 许可证导入 XenMobile 时，如果某些许可证由 Apple 安排了退款，这些许可证在 XenMobile 中仍被错误地视为有效。 因此，用户无法通过 WorxStore 在 iOS 设备上安装应用程序。 [#601845]
- 创建一项操作后，如果重命名操作时使用的名称与某个设备策略或应用程序名称相同，则以后无法删除该操作。 [#602958]
- 使用 Samsung Galaxy Note 5 访问 Worx Store 时，WorxStore 在平板电脑视图下显示的屏幕不完整，而不是像在手机视图那样显示完整屏幕。 [#604295]
- 创建要求使用一次性 PIN 的注册邀请时，如果受邀人位于 Active Directory 组的顶层，则嵌套组会收到邀请，但处于第三层的嵌套组会注册失败。 此问题即便在邀请第三层组时也会出现。 [#603434]
- 拥有高级许可证类型且在 XenMobile 控制台中选中了“Enrollment required”（要求注册）复选框时，用户可在仅 MAM 模式下注册，并可访问 WorxStore。 [#604113]
- **$user.dnsroot** 和 **$user.netbiosename** 属性会在宏中使用，以部署使用用户属性的策略。 **dnsroot** 和 **netbiosename** 用户属性在 XenMobile 10.1 中已弃用。 此修复会在 XenMobile 10.3 中重新启用这些属性。 [#604240]
- 尝试在 XenMobile 控制台中配置 iOS Device Enrollment Program 时会出现无效配置文件错误。 这是第三方问题。 [#607143]
- 在 XenMobile 控制台的客户端外观方案设置中，应用商店名称仅支持数字字母 (ASCII) 字符；如果将默认名称更改为非 ASCII 字符，用户将无法登录到 Worx Home。 [#609535]
- 如果在 LDAP 中为用户和组配置了不同的基础 DN，则在更新到 XenMobile 10.3 后，您将无法向交付组添加新组。 [#610014]
- 配置 WiFi 设备策略时，即便将部署计划设置为**仅当之前的部署失败时**，此 WiFi 策略也会在每次设备连接时推送到设备。 [#610325]
- 此修复解决了 Apache Commons Collections 中的对象反序列化 Java 零日漏洞问题。 [#610427]
- 如果设置的 RBAC 角色允许用户使用 sAMAccountName 格式的用户名登录到 XenMobile 控制台，则这些用户将重定向到自助服务门户。 [#610915]
- 首次安装 XenMobile 10.1 或从 XenMobile 9 MAM 和 MDM 模式升级到 XenMobile 10.1 后，如果刷新交付组和策略，XenMobile 控制台的**管理** > **设备**下会显示不同信息；交付组和策略数量也不准确。 [#611630]
- 如果在 XenMobile 10.1 之前的 XenMobile 版本或 XenMobile 10 中配置了 10 个以上的 LDAP 域，或者在升级到 XenMobile 10.1 后配置了 10 个以上的 LDAP 域，则 XenMobile 控制台将仅显示 10 个域。 [#613502]
- 如果没有为用户设置包含公共应用程序权限的 RBAC 角色，您将无法添加或更新 MDX 应用程序。 [#614496]
- 如果在首次配置 XenMobile 期间更改了默认实例名称，则升级到 10.3 版后，所做更改不会保留下来。 因此，注册的设备将

© 1999-2017 Citrix Systems, Inc. All rights reserved.

无法连接。 [#614604]

- 如果为 LDAP 配置了锁定限制，则升级到 XenMobile 10.3 后，如果同一个域中的新用户在 Worx Home 中使用无效凭据（例如输错密码）注册设备，则 Worx Home 会停止响应且 SQL Server 会失败。 [#615179]
- 从 XenMobile 10.1 更新到 XenMobile 10.3 后，无法使用**添加邀请**选项向用户发送注册邀请。 [#616584]
- 使用此修复可在单个林中支持 LDAP 多域 root 用户。 此支持适用于 XenMobile 9，但不适用于 XenMobile 10.x。 [#616633、#618899、#620541]
- 如果在 XenMobile 控制台中配置了 iOS 限制设备策略，并更改了**允许用户删除策略**选项的默认值，则不会保存更改后的值。 [#616751]
- 如果服务器具有自定义实例名称，则从 XenMobile 10.1 更新至 XenMobile 10.3 后，用户将无法注册设备。 [#616954]
- 用户在 XenMobile Enterprise 模式下注册 DEP 设备时，如果他们将自己的设备重置为出厂设置（完全擦除），然后又重新注册设备，则不会按预期自动将 Worx Home 部署到设备。 [#616986]
- 受一个 Java Runtime Environment (JRE) 已知问题的影响，XenMobile 服务器偶尔会在 20 至 30 分钟左右时间后进入恢复模式。 重新启动服务器后，此问题再次出现。 [#616992]
- 在 iOS 和 Android 设备上，如果您在**设置 > 客户端外观方案**中删除了**应用商店名称**，用户将无法从 Worx Home 中打开 WorxStore。 [#617003]
- 将 .ipa 文件上载到 XenMobile 控制台时，出现“no icon found”（找不到图标）错误。 [#617195]
- 如果部署“启用为应用单独设置 VPN”和“按需匹配应用程序已启用”选项设置为**开**的 VPN 设备策略，并为应用了该 VPN 策略的托管应用程序部署应用程序属性策略，则用户打开该托管应用程序时会出现以下问题：VPN 连接并未按预期自动初始化。 用户必须在设备上手动启用**Connect On Demand**（按需连接）设置。 [#617803]
- 在 XenMobile 控制台的**管理 > 用户**下显示现有用户时出现延迟。 因此，您无法执行本地用户操作。 [#618094]
- XenMobile 10.x 支持在单个 Active Directory 林中使用 LDAP 多域。 [#618375]
- 发送注册邀请并输入 HTML 代码时，用户收到的电子邮件中只有普通文本，而没有 HTML 链接。 [#618504]
- 用户将 .appx 文件作为 Windows 10 设备的企业应用程序进行上载时，应用程序并未部署到设备。 [#628611]
- 如果用户的用户 ID 或密码字段中包含任何特殊字符，他们无法将 Windows 10 设备注册到处于 MDM 模式的 XenMobile。 [#618870]
- 在 iPad 上，XenMobile 10.3 始终首先执行删除操作，与您在 XenMobile 控制台中设置的顺序无关。 [#620459]
- 如果在 XenMobile 控制台中更新现有 iOS 企业应用程序，并且 .ipa 具有不同的捆绑包 ID，则将更新的应用程序上载至设备时，在设备上部署应用程序会出现问题。 [#621009]
- 在 XenMobile 服务器中添加 Google Play 凭据时，显示错误“无效设备 ID”，您将无法登录。 [#623182]
- 如果在 XenMobile 中删除使用 VPP 导入的应用程序，该应用程序不会自动重新导入，直至删除令牌后再重新添加。 [#623403]
- 如果删除或擦除设备，与此设备关联的任何 VPP 许可证都不会自动释放。 因此，您必须手动取消关联许可证，然后才能将该许可证用于另一台设备。 [#623716]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

关于 XenMobile Server 10.3

Oct 21, 2016

可以在 XenMobile 控制台上将 XenMobile 10.1 升级到 XenMobile 10.3。 要执行升级，请使用 xms_10.3.0.824.bin。 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击**版本管理**。 单击**升级**，然后上载 xms_10.3.0.824.bin 文件。 有关在控制台中进行升级的详细信息，请参阅升级 XenMobile。

要完成 XenMobile 10.3 的全新安装，请参阅安装 XenMobile。

> **注意**
>
> 此 Remote Support 客户端在适用于 Windows CE 和 Samsung Android 设备的 XenMobile Cloud 10.x 中不可用。

规划 XenMobile 部署有多个注意事项。 有关您的端到端 XenMobile 环境的建议、常见问题和用例，请参阅 XenMobile Deployment Handbook（《XenMobile 部署手册》）。

XenMobile 10.3 中的新增功能

XenMobile 10.3 中新增了以下功能。

全新的控制台外观

XenMobile 10.3 采用全新的外观。 控制台更新了颜色、字体、选项卡并包含经过改善的功能。

- 先前控制台版本中的“控制板”选项卡已移至新“分析”选项卡下面，“分析”选项卡现在还包含“报告”选项卡。 有关详细信息，请参阅报告。
- “管理”选项卡现在包含新的用于管理本地用户和组的“用户”选项卡。
- “配置”选项卡限制包含新的“ShareFile”选项卡，此选项卡用于配置连接到 ShareFile 帐户的设置。
- 可以通过单击控制台右上角的齿轮图标访问“设置”，此选项卡之前位于“配置”选项卡下面。
- “支持”选项卡现在在与控制台相同的选项卡中打开，而不是在新选项卡中打开。

新的平台支持

XenMobile 10.3 现在支持以下平台：

- Mac OS X
- Android HTC
- Android Sony
- Samsung SEAMS
- Windows Mobile/CE
- Windows 10 Phone：XenMobile MDM 和 Enterprise 模式下的设备管理。
- Windows 10 Desktop/Tablet：XenMobile MDM 和 Enterprise 模式下的设备管理。

有关注册 Mac OS X 设备的步骤，请参阅 Mac OS X 设备。

有关注册 Windows 10 设备的步骤，请参阅 Windows 设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> XenMobile 10.3 已终止对 Symbian 设备的支持。

设备策略

XenMobile 10.3 中提供了下列新 MDM 策略：

- **应用程序锁定**。 用于定义允许在设备上运行的应用程序列表，或阻止在设备上运行的应用程序列表。 适用于 iOS 和 Android。 虽然设备策略在大多数 Android L 和 M 设备上起作用，但是，由于 Google 弃用了所需的 API，因此，应用程序锁定策略在 Android N 或更高版本的设备上不起作用。
- **应用程序网络使用。** 用于设置网络使用规则，以指定托管应用程序使用网络（如手机数据网络）的方式。 规则仅适用于托管应用程序。 适用于 iOS。
- **连接管理器**。 配置应用程序连接到 Internet 或专用网络的方式。 这些设置仅在掌上电脑（触摸屏设备）上可用。 适用于 Windows Mobile/CE。
- **将应用程序复制到 Samsung 容器**。 允许您在 Samsung 设备上为应用程序创建 SEAMS 或 KNOX 容器。 适用于 Samsung SEAMS 或 Samsung KNOX。
- **删除文件和文件夹**。 允许指定需要删除的文件或文件夹。 适用于 Windows Mobile/CE。
- **设备运行状况证明**。 启用设备运行状况证明，这是 Windows 10 中的一项安全和数据丢失防护 (DLP) 功能，使您可以确定 Windows 10 设备的运行状况，并在必要时采用合规措施。 负载仅在 Windows 10 及更高版本的受监督设备上受支持。 适用于 Windows Phone 和 Windows Tablet。
- **设备名称。** 允许您在 iOS 和 Mac OS X 设备上设置名称，以便轻松识别设备。 可以使用宏、文本或二者的组合定义设备的名称。
- **删除注册表项和值**。 运行您指定需要删除的注册表项和值。 空值表示条目为注册表项。 适用于 Windows Mobile/CE。
- **企业数据保护。** 允许您指定需要在所需的强制级别执行企业数据保护的应用程序。 此策略适用于 Windows 手机和 Windows 平板电脑。
- **导入 iOS 和 Mac OS X 配置文件**。 为 Mac OS X 配置此策略的选项是 XenMobile 10.3 中的新增选项。 此策略允许您导入 iOS 或 Mac OS X 的设备配置 XML 文件。 此文件包含您使用 Apple Configurator 准备的设备安全策略和限制。
- **注册表**。 Windows Mobile/CE 注册表存储关于应用程序、驱动器、用户首选项和配置设置的数据。 您可以定义用于管理 Windows Mobile/CE 设备的注册表项和值。
- **墙纸。** 允许您添加 .png 或 .jpg 文件，以设置 iOS 设备锁定屏幕、主屏幕或二者的墙纸。 适用于 iOS 7.1.2 及更高版本。 要在 iPad 和 iPhone 上使用不同的墙纸，需要创建不同的墙纸策略并将其部署到相应的用户。
- **Windows CE 证书**。 允许您从外部 PKI 创建证书并将其交付到用户设备。

有关按平台介绍的所有新设备策略和现有设备策略的矩阵，请参阅 XenMobile 设备策略（按平台）。

各平台类型的新功能和增强功能总结

iOS

- **新设备策略**。 应用程序网络使用情况、设备名称和墙纸。
- **将应用程序从托管指定为非托管**。 用于将应用程序从托管指定为非托管的 iOS 9.0 选项。 在 XenMobile 控制台中为 iOS 的公共应用商店应用程序添加和配置设置时，可以配置一个**强制管理应用程序**选项。 默认情况下，此选项设置为**关**。 如果选择**开**，当应用程序以非托管状态安装时，系统会提示用户是否允许在未受监督的设备上管理此应用程序。 有关详细信息，请参阅向 XenMobile 中添加公共应用商店应用程序。
- **新的限制和 Apple Configurator 1.7.2 策略选项**。 有关详细信息，请参阅限制设备策略。
- **支持 RequestMirroring 和 StopMirroring 命令**。 有关详细信息，请参阅 XenMobile REST API 参考。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **DEP 设备设置辅助增强功能**。 有关详细信息，请参阅批量注册 iOS 设备。
- **VPN OnDemandRules 密钥**。 有关详细信息，请参阅 VPN 设备策略。

Android

- **Samsung KNOX 容器配置**。 有关详细信息，请参阅将应用程序复制到 Samsung 容器设备策略。
- **Samsung SAFE API**。 有关详细信息，请参阅 XenMobile REST API 参考。
- **用于 Samsung Android 设备的 ELM 密钥**。
- **应用程序锁定设备策略**。 有关详细信息，请参阅应用程序锁定设备策略。

Windows CE

- **凭据提供程序配置**。 有关详细信息，请参阅凭据设备策略。
- **Windows CE 证书配置**。 有关详细信息，请参阅 Windows CE 证书设备策略。
- **注册表存储设备策略**。 有关详细信息，请参阅注册表设备策略。
- **能够在接收 SMS 时连接/在呼叫时连接**。
- **其他新设备策略**：连接管理器、删除文件和文件夹、删除注册表项和值。

Windows Phone 10 和 Windows Tablet 10

- 新设备策略：企业数据保护和设备运行状况认证
- 面向 Windows Phone 和 Windows Tablet 的新设备策略选项：

  应用程序清单
  凭据
  自定义 XML
  需要通行码
  限制
  条款和条件
  VPN
  WiFI

- 面向 Windows Tablet 的新设备策略选项：

  应用程序卸载
  旁加载密钥
  签署证书
  Web 剪辑
  WorxStore

- 面向 Windows Phone 的新设备策略选项：

  企业 Hub
  存储加密

Mac OS X

- 通过 OTAE 注册。 有关详细信息，请参阅 Mac OS X。
- XenMobile 控制台中的设备管理信息显示设备属性、证书、报告和支持的配置文件。
- 针对 Mac OS X 设备的安全操作 - 选择性擦除、锁定、吊销、擦除。
- 新设备策略选项：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备名称
导入 iOS 和 Mac OS X 配置文件
AirPlay 镜像
应用程序清单
日历 (CalDav)
联系人 (CardDAV)
凭据
Exchange
字体
LDAP
邮件
需要通行码
配置文件删除
限制
SCEP
VPN
Web 剪辑
WiFI

支持 Android for Work 的新功能和增强功能

- **支持 Android 之前的设备**。
- **置备面向 Android for Work 的设备所有者模式**

  除管理 Android for Work 应用程序或处于 BYOD 模式的 Android 设备外，还可以通过置备设备所有者模式来管理企业拥有的设备。 为此，请在设备之间使用近场通信 (NFC) 凸起。 一台设备运行 Worx Provisioning Tool 应用程序，阻碍使用新的开箱即用设备或恢复出厂设置的设备。 设备所有者模式是适用于大多数运行 Android 5.x.x 的设备的企业拥有的设备模式。

- **Android for Work 批量购买**

  可以在 XenMobile 控制台中为针对 Android for Work 启用的应用程序管理批量购买许可。 面向 Android for Work 的批量购买计划简化了组织批量查找、购买和分发应用程序及其他数据的过程。 向 XenMobile 中添加面向 Android for Work 的付费公共应用商店应用程序时，可以查看批量购买许可状态，即可用许可证总数。 为用户部署应用程序后，稍后可以查看当前正在使用的许可证数量以及使用这些许可证的每个用户的电子邮件地址。 可以选择一个用户，然后单击**解除关联**以结束其许可证分配，释放一个许可证以供其他用户使用。 但是，如果该用户不属于包含特定应用程序的交付组的一部分，您将只能解除该许可证的关联。

共享设备

XenMobile 允许配置可由多个用户共享的设备。 有关详细信息，请参阅 XenMobile 中的共享设备。

语言支持

XenMobile 10.3 中的 XenMobile 控制台可以采用韩语、德语和葡萄牙语。 在 XenMobile 控制台中查看的 MDX 策略现已本地化。 有关详细信息，请参阅 XenMobile 语言支持。

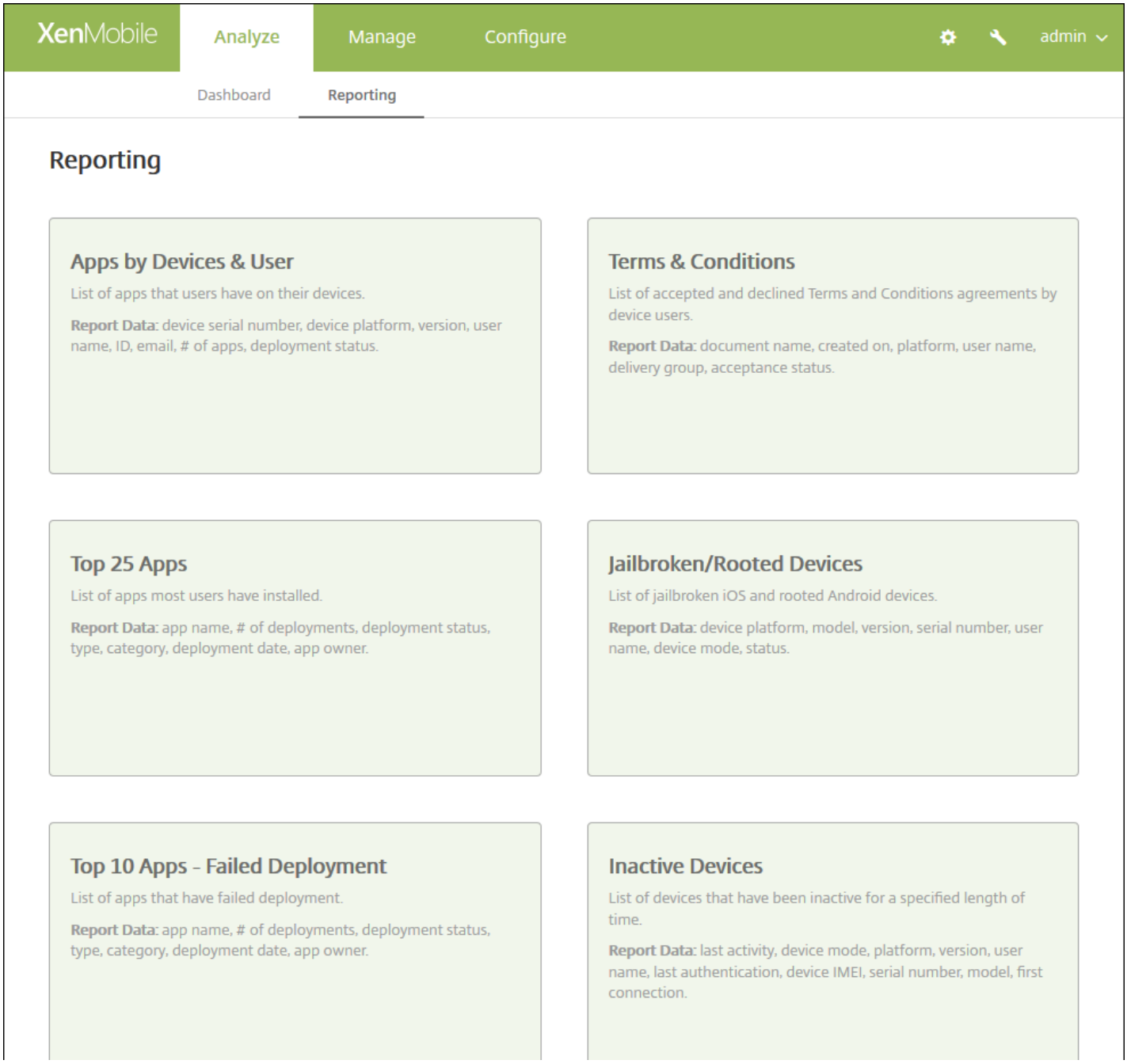
报告

从 XenMobile 控制台的**报告**选项卡，可以生成 10 种预定义报告：

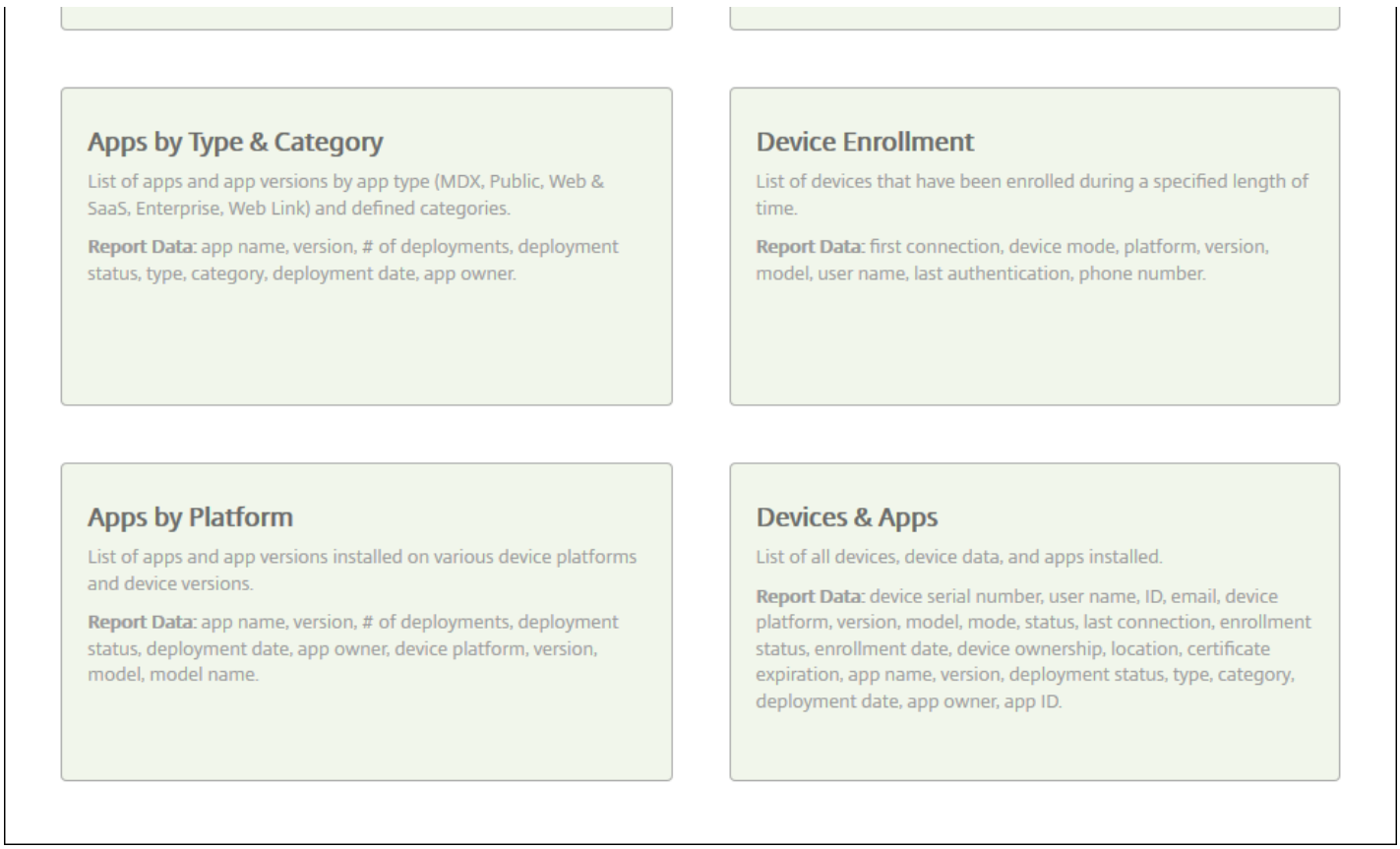
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **应用程序(按设备和用户)**：列出用户设备上具有的应用程序。
- **条款和条件**：列出接受条款和条件协议和拒绝条款和条件协议的用户。
- **排名前 25 的应用程序**：列出用户在其设备上使用最多的 25 个应用程序。
- **已越狱/获得 Root 权限的设备**：列出获得 Root 权限的 iOS 设备和已越狱的 Android 设备。
- **排名前 10 的应用程序 - 部署失败**：列出部署失败的应用程序。
- **非活动设备**：列出处于非活动状态的时间已达到指定时间段的设备。
- **应用程序(按类型和类别)**：按版本、类型和类别列出应用程序。
- **设备注册**：列出在指定时间段内已注册的设备。
- **应用程序(按平台)**：按设备平台和版本列出应用程序和应用程序版本。
- **设备和应用程序**：列出所有设备、设备数据和已安装的应用程序。

要运行报告，请单击 XenMobile 控制台中的**分析**选项卡，然后单击**报告**。 报告采用 .csv 格式，您可以使用 Microsoft Excel 等程序打开此类文件。 有关详细信息，请参阅 XenMobile 中的报告。

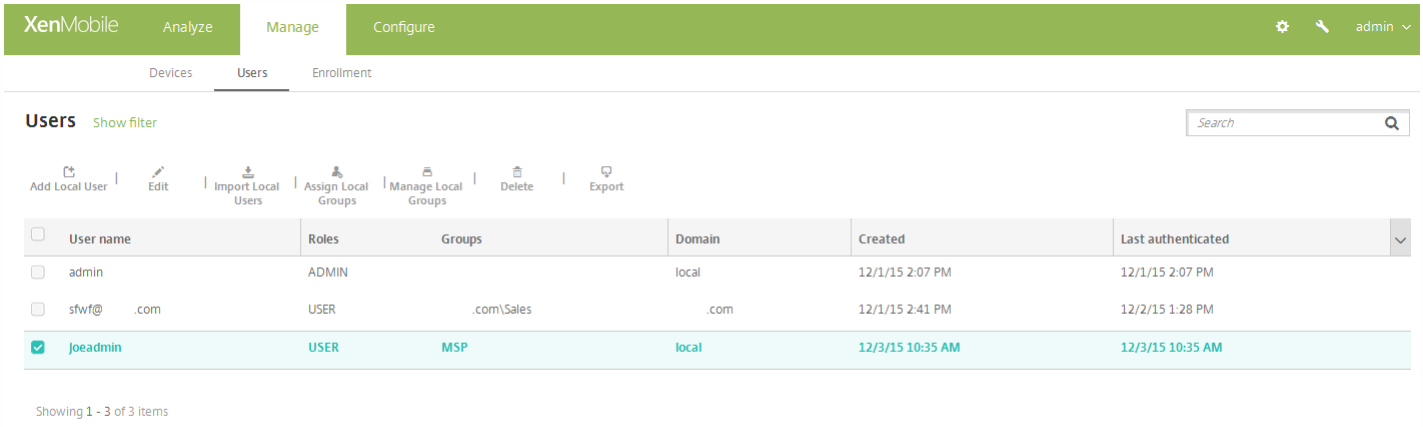


© 1999-2017 Citrix Systems, Inc. All rights reserved.



将 LDAP 成员（本地用户）添加到组

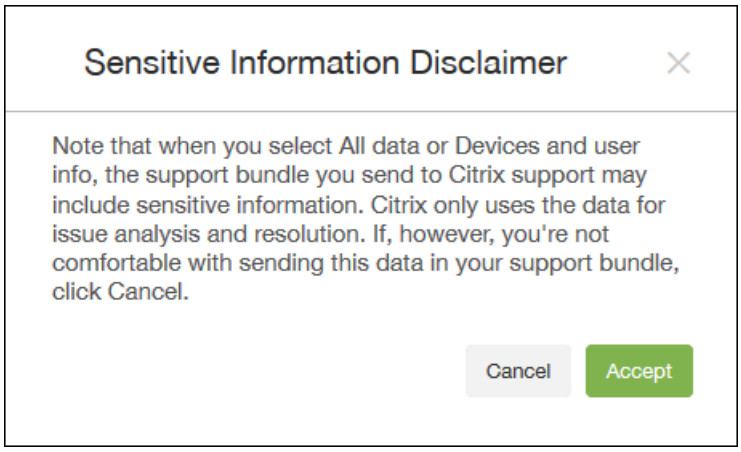
很多组织不配置 Active Directory 组，但是需要通过本地组实现特定目的，例如试验。 在 XenMobile 10.3 中，可以将 LDAP（本地用户）设为本地组的成员。 然后，可以定义包含此本地组的交付组。 此组用户无需重新注册其设备，即可以访问分配给此交付组的应用程序和策略。 有关详细信息，请参阅在 XenMobile 中添加、编辑或删除本地用户。



支持包法律协议

首次将支持包上载到 Citrix Insight Services (CIS) 时，系统会提示您接受法律协议。 有关详细信息，请参阅在 XenMobile 中创建支持包。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



匿名化支持包中的数据

在 XenMobile 中创建支持包时，默认情况下会将敏感用户、服务器和网络数据设为匿名。 可以在“匿名和取消匿名”页面更改此行为。 还可以下载 XenMobile 在匿名化数据时保存的映射文件。 Citrix 支持人员可能会要求此文件对数据取消匿名，并查找特定用户和设备的问题。 有关详细信息，请参阅匿名化支持包中的数据。

连接检查

从 XenMobile 的支持页面，可以检查 XenMobile 与 NetScaler Gateway 及其他服务器和位置的连接性。 有关详细信息，请参阅执行连接检查。

Microsoft Azure

可以将 Windows 10 设备加入到 Microsoft Azure AD 中，以允许设备采用联合 Active Directory 身份验证方法向 Azure 注册。 有关详细信息，请参阅 Microsoft Azure 设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Server 10.3 已修复的问题

Aug 11, 2016

XenMobile 10.3 中修复了以下问题。 有关 XenMobile 10.3.5 中修复的问题，请参阅 XenMobile 10.3.5 中的已知和已修复问题。

通过运营商 SMS 网关从 SMTP 发送电子邮件时，可以向电子邮件地址添加电子邮件发送前缀两次。 [#492629]

从 Cisco Identity Service Engine 发送到 XenMobile 的 HTTP GET 请求可能会失败，出现 404 错误。 [#555554]

文件上载策略设置为将文件推送到 Android 设备时，向设备推送文件可能会失败。 设备上反而可能会显示“条款和条件”声明。 [#564144]

在某些情况下，如果 MDM 身份证书通过 SCEP 分发并使用内置 PKI 颁发，则续订这些身份时，XenMobile 无法正确吊销以前的证书。 因此，在某些情况下，受影响的设备会丢失 MDM 功能。 [#569999]

配置代理服务器后，连接性检查会创建不通过代理服务器传输的网络流量，连接失败。 [#571467]

如果用户属于某个子域的成员，连接到 SAML 应用程序将失败。 [#571851]

如果 iOS MDX 应用程序位于“排除的设备”列表中，则当设备处于仅移动应用程序管理模式（MAM 模式）时，该应用程序不在 Worx Store 中显示。 [#571900]

升级到 XenMobile 10 后，搜索设备所需的时间长达 30 秒，CPU 使用率也会增加到 100%。 [#577010]

在多节点群集环境中通过 WorxWeb 浏览 Intranet 站点时，用户可能无法访问 URL 并看到消息“Error Invalid OTT”（错误 无效 OTT）。 [#577273]

如果为 XenMobile 配置了代理服务器，尝试添加 Google Play 凭据或创建 Android 公共商店应用程序可能会失败。 [#578727]

尝试在 Internet Explorer 11 的已发布版本中打开 XenMobile 控制台时显示空白页面。 [#578729]

本版本现在支持面向 iOS 8 的 WPA2 Personal 和 WPA2 Enterprise。 [#579616]

如果在 XenMobile 控制台中添加或上载应用程序，使用与现有应用程序相同的应用程序文件名向 XenMobile 上载应用程序时可能会出现错误。 [#580359]

在 Android 设备上，尝试从 Worx Store 下载 Worx 应用程序失败。 [#582044]

输入包含用户名和电话号码的宏时，转换无法正确翻译电话号码。 [#589130]

跳过激活锁命令在某些 iOS 设备上不起作用。 [#589991]

如果“memberOf”属性的值超过 255 个字符，则会显示错误消息“No groups found”（找不到任何组）。
如果用户尝试通过 Worx Home 打开 Windows 应用程序，枚举成功，但该应用程序未打开。 用户收到错误消息“无法添加帐户”。 [#590046]

如果您创建了需要质询密码的简单证书注册协议 (SCEP) 策略，则无法保存策略。 在本版本中，质询密码字段为可选字段。 [#590798]

如果将 XenMobile 配置为使用代理服务器，Android for Work 将无法连接到外部 Web 站点。 [#591707]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

尝试将 IPA 应用程序上载到 App Controller 失败并显示错误消息“Invalid package type for selected app”（选定应用程序的包类型无效）。PNG 图片中出现错误时会显示此消息。 [#592748]

用户尝试注册时收到错误消息“用户 不存在”。删除用户的注册并重新注册后出现此错误。 出现此错误时，请在 Active Directory 中重新创建用户。 [#593028]

如果从 Microsoft Outlook 或 Microsoft Exchange 帐户创建诶里邀请，该邀请需要很长时间才能在 WorxMail 中显示。 [#594542]

如果您配置了工作流并使用除 443（默认端口）以外的端口号，用户无法打开工作流链接。 [#599441]

用户无法从 XenMobile 服务器更新其设备上的 Android 应用程序。 [#601251]

通过 Azure Active Directory 注册时，用户无法登录到 Worx 应用程序。 [#608505]

截至 2015 年 12 月，Nexmo SMS 仅支持 HTTPS 连接。 在 XenMobile 中，默认设置为**开**。 将该值更改为**关**不会产生任何影响。 升级后，该值仍显示为**关**，但连接安全。 [#609306]

即使许可证仅适用于设备，Worx Store 也需要 Volume Purchase Program (VPP) 用户。 [#610338]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Server 10.3 已知问题

Aug 11, 2016

下面是 XenMobile 10.3 中的已知问题。 有关 XenMobile 10.3.5 中的已知问题，请参阅 XenMobile 10.3.5 中的已知和已修复问题。

- 以下缺陷与在 NetScaler 上配置了 TLS 1.2 安全协议时 XenMobile 与以下版本的 NetScaler 的集成有关的缺陷：
  - 11.0.64 之前的 NetScaler 11.x 版本
  - 10.5.59
  - 10.5.58

  请注意，当您的 XenMobile MAM 部署包括 XenMobile 服务器与 NetScaler Gateway 之间的 NetScaler 负载平衡器时，此问题不会出现。

  在 MAM 模式下 NetScaler Gateway 与 XenMobile 之间的通信由于存在后端 TLS 1.2 会话而失败。 因此，连接到内部网络时，用户无法从 WorxStore 下载应用程序，也无法从 ShareFile 下载文件。
  [#591600，#595713，#596566，#604409]
- 卸载企业应用程序后，应用程序推送失败。 [#591450]
- 从应用程序中删除许可证后，该应用程序仍保留在用户设备上。 这是第三方问题。 [#596656]
- 用户尝试使用 Microsoft 工作帐户注册其个人设备时，注册失败。 [#597037]
- 在 XenMobile 控制台中，“条款和条件”策略不显示已安装或待定状态，即使在设备上成功部署了该策略也是如此。 [#598407]
- 限制策略在 Windows 10 设备上有效。 但是，用户不会收到指出禁用了阻止功能的消息。 [#599064，#606651]
- 如果添加了包含公共应用程序和企业应用程序的类别，然后在 XenMobile 中注册设备，则当用户在 Worx Home 中同步应用程序时，则不显示类别。 [#599495]
- 如果您在创建共享设备 RBAC 时未添加“选择性擦除设备”权限，则当用户尝试删除 iOS 设备上 Worx Home 中的帐户时（在 XenMobile Enterprise 模式下），用户必须从设备中手动删除 Device Manager 配置文件。 [#600705]
- 为应用程序部署“应用程序清单”和“Enterprise Hub”策略，并使用其他名称和说明创建公共应用程序后，用户从 Worx Home 打开应用程序时，应用程序名称和说明将相同。 [#600369]
- 如果您在首次使用过程中在 SSL 模式下配置了 Microsoft SQL Server，并且 CA 证书与 SQL Server 证书不对应，连接将失败。 如果尝试与 SQL server 证书对应的相应 CA 证书建立连接，连接仍将失败。 要允许证书起作用，请重新启动 XenMobile 服务器以清除信任存储区缓存。 [#602609]
- 共享用户设备上的用户名必须是英文格式。 共享设备不支持非 ASCII 用户名。 [#605544]
- 用户收到用于 IMEI 绑定（用户名和密码）以及 SMTP 和 SMS 通知的一次性密码邀请时，第一个配置文件将成功安装，但第二个配置文件安装失败并显示错误消息“Profile Installation Fails. A connection to the server could not be established”（配置文件安装失败。无法与服务器建立连接）。 在 iPhone 6 和 iPhone 6 Plus 设备上，存在 IMEI 编号和 MEID 编号，并且一次性密码绑定到 MEID 编号而非 IMEI 编号。 可以将 IMEI 编号替换为 iPhone 的唯一设备标识符 (UDID) 或者使用常规电话号码。 [#606162]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 升级到 XenMobile 10.3 后，许可信息将显示试用期设置为 30 天，许可证服务器配置标志设置为 true。 升级 XenMobile 服务器后，请将相同的许可证上载到服务器，这样将删除试用版许可证期限。 [#607939]
- 在 Windows 8.1 平板电脑上，用户可以从设备中成功删除应用程序。 企业应用程序将继续在 XenMobile 控制台的设备属性中显示。 [#608184]
- 选项“应用程序擦除”和“选择性擦除”在 XenMobile Enterprise 模式下功能相同。 [#608715]
- 在 Internet Explorer 中保存或打开文件时，XenMobile 服务器停止响应。 可以重新启动服务器以继续工作。 [#608724]
- 升级到 XenMobile 10.3 后，Android for Work 在浏览器策略中不存在，即使存在阻止的 Web 地址和书签也是如此。 [#609002]
- 在使用 Windows 8.1 和 Windows 10 的平板电脑上，从设备中手动删除帐户后，某些策略将保留。 [#609201]
- 在 Windows 10 平板电脑上，如果用户更改了设备上的“自动更新”设置，更改不在 XenMobile 控制台的“设备属性”中的“安全信息”部分中显示。 [#609254]
- Worx Store 名称仅支持英语 (ASCII) 字符。 [#609535]
- 尝试从 Internet Explorer 和 Firefox Web 浏览器下载证书签名请求 (CSR) 失败，出现错误“无法显示该网页”。可以从 Chrome Web 浏览器下载 CSR。 [#609552]
- 如果登录 XenMobile 控制台，导航到**分析** > **报告**，然后单击**不活动设备**，则将显示空白页面，而非下载文件。 [#609649]
- 在 Citrix Workspace Cloud 中配置工作区时，不使用属于子域和孙域的 Active Directory 用户或组更新交付组。 [#609673]
- 如果部署了多个“条款和条件”策略，并且所有策略都不属于默认条款和条件，注册 Windows 10 设备将失败。 [#609694]
- 如果从交付组中删除一条策略，单击**摘要**按钮并保存该策略，该资源将保留在交付组中。 单击**下一步**而非**摘要**将从交付组中删除该策略。 [#610109]
- 要在 Windows CE 设备上保留原始文件扩展名，请勿在策略中指定目标文件名。 [#610601]
- 为 Mac OS X 配置 VPN 设备策略时，**VPN** 选项将在**连接类型**列表中显示。 但是，不能为 Mac OS X 设备配置此选项。 [#612846]
- 从 XenMobile 10.1 更新到版本 10.3 时，如果 WorxStore 具有自定义名称，则必须先将应用商店名称更改为**应用商店**的默认设置，并在设备上部署这些设置，然后进行更新。 如果未执行上述操作，自定义应用商店名称会导致 XenMobile 10.3 注册、访问 Worx Home 和 WorxStore 以及在 iOS 设备上部署应用程序出现问题。 [#614049]
- 不能在 XenMobile 控制台中启用 Android for Work。 配置 Android for Work 帐户设置并输入从 Google 获取的服务帐户 ID（仅包含数字）时，保存设置时将显示错误消息。 如果使用以前包含数字和字符的 Google 格式输入服务帐户 ID，则会出现相同的错误，因为此格式与 XenMobile 服务器中的服务帐户 ID 不对应。 这是第三方问题。

  解决方法为，启用 Android for Work，并为 Google 客户端 ID 添加服务器属性。

  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**添加**。 此时将显示**添加新服务器属性**页面。
  3. 在**密钥**列表中，单击**自定义密钥**。
  4. 在**密钥**中，输入 **google.aw.enterprise.client.id**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. 在**值**中，输入客户端 ID 的数字部分，例如 3838383838388383。

6. 输入**显示名称**，例如“Google 域客户端 ID”。

7. 单击**保存**。

[#615118]

- 在 Mac OS X 计算机和 iPad 上，XenMobile 10.3 始终首先执行删除操作，与您在 XenMobile 控制台中设置的顺序无关。 [#620459]
- 启用 iOS 批量注册并更新 XenMobile SSL 证书的根证书颁发机构 (CA) 后，设备注册或重新注册可能会失败。 从自签名证书更改为公用证书、从新提供商处购买证书或移至内部企业 CA 时可能会出现此问题。 此问题不影响现有的已注册设备。 解决方法为执行以下步骤：

  1. 在 XenMobile 控制台中，单击**设置** > **iOS 批量注册**。
  2. 在 **DEP 配置**下的**允许加入 Device Enrollment Program (DEP)** 旁边，单击**否**，然后单击**保存**。 等待几秒钟。 此步骤将在 Apple DEP 门户上从 DEP 设备中删除以前的 DEP 配置文件。
  3. 单击**管理** > **设备**。 检查以确认**已注册 DEP** 列中不显示任何已注册 DEP 设备。
  4. 再次单击**设置** > **iOS 批量注册**。
  5. 在 **DEP 配置**下的**允许加入 Device Enrollment Program (DEP)** 旁边，单击**是**，然后单击**保存**。 等待几秒钟。 此步骤将强制向所有 DEP 设备中添加新配置文件。
  6. 单击**测试连接**以确保 XenMobile 服务器与 Apple DEP 服务器之间的连接仍在运行。
  7. 再次单击**管理** > **设备**。 检查以确认**已注册 DEP** 列中新注册了所有 DEP 设备。

有关 Apple DEP 的详细信息，请参阅批量注册 iOS 设备。
[#635699]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

体系结构概述

Oct 21, 2016

您选择部署的 XenMobile 参考体系结构中的 XenMobile 组件建立在您所在组织的设备或应用程序管理要求的基础之上。 XenMobile 的组件为模块式，彼此在对方的基础之上构建。 例如，如果您需要向贵组织中的用户授予对移动应用程序的远程访问权限，并且需要跟踪用户连接时使用的设备类型。 在此情况下，需要部署 XenMobile 和 NetScaler Gateway。 XenMobile 用于管理应用程序和设备，而 NetScaler Gateway 使用户可以连接到您的网络。

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

- 连接到内部网络。 如果您的用户为远程用户，则可以使用 VPN 或 Micro VPN 连接通过 NetScaler Gateway 进行连接，以访问内部网络中的应用程序和桌面。
- 设备注册。 用户可以在 XenMobile 中注册移动设备，这样一来，您便可以在 XenMobile 控制台中管理连接到网络资源的设备。
- Web、SaaS 和移动应用程序。 用户可以从 XenMobile 通过 Worx Home 访问其 Web、SaaS 和移动应用程序。
- 基于 Windows 的应用程序和虚拟桌面。 用户可以通过 Citrix Receiver 或 Web 浏览器进行连接，以从 StoreFront 或 Web Interface 访问基于 Windows 的应用程序和虚拟桌面。

要实现部分或全部功能，Citrix 建议按以下顺序部署 XenMobile 组件：

- 桌面和应用程序。 可以使用快速配置向导在 NetScaler Gateway 中配置设置，以实现与 XenMobile、StoreFront 或 Web Interface 的通信。 在 NetScaler Gateway 中使用快速配置向导前，必须安装 XenMobile、StoreFront 或 Web Interface，才能与其建立通信。
- XenMobile。 安装 XenMobile 后，可以在 XenMobile 控制台中配置策略和设置，以允许用户注册其移动设备。 您也可以配置移动应用程序、Web 应用程序和 SaaS 应用程序。 移动应用程序可以包括 Apple App Store 或 Google Play 中的应用程序。 用户还可以连接到您通过 MDX Toolkit 打包并上载到控制台的移动应用程序。
- MDX Toolkit。 MDX Toolkit 可以安全地打包在组织内部开发的应用程序或在公司外部开发的移动应用程序，如 Citrix Worx 应用程序。 打包应用程序后，可以使用 XenMobile 控制台将该应用程序添加到 XenMobile 并根据需要更改策略配置。 还可以添加应用程序类别、应用工作流并将应用程序部署到交付组。 请参阅关于 MDX Toolkit。
- StoreFront（可选）。 可以通过连接到 Receiver 从 StoreFront 提供对基于 Windows 的应用程序和虚拟桌面的访问权限。
- ShareFile Enterprise（可选）。 如果部署 ShareFile，您可以通过 XenMobile 启用企业目录集成，XenMobile 的作用是安全声明标记语言 (SAML) 身份提供程序。 有关为 ShareFile 配置身份提供程序的详细信息，请参阅 ShareFile 支持站点。

XenMobile 支持通过 XenMobile 控制台提供设备管理以及应用程序管理的集成解决方案。 此部分介绍 XenMobile 部署的参考体系结构。

在生产环境中，Citrix 建议采用群集配置部署 XenMobile 解决方案，以实现可扩展性和服务器冗余目的。 此外，利用 NetScaler SSL Offload 功能可以进一步降低 XenMobile 服务器的负载，并增加吞吐量。 有关如何通过在 NetScaler 上配置两个负载平衡虚拟 IP 地址来设置 XenMobile 10.x 群集的详细信息，请参阅配置 XenMobile 10 的群集。

有关如何为灾难恢复部署配置 XenMobile 10 Enterprise Edition 的详细信息（包括体系结构图），请参阅 XenMobile 的灾难恢复指南。

下面各部分内容说明了 XenMobile 部署的不同参考体系结构。 有关参考体系结构图，请参阅《XenMobile 部署手册》文章适用于本地部署的参考体系结构和适用于云部署的参考体系结构。 有关完整端口列表，请参阅 XenMobile 端口要求。

移动设备管理 (MDM) 模式

XenMobile MDM Edition 提供适用于 iOS、Android、Amazon 和 Windows Phone 的移动设备管理（请参阅 XenMobile 中支

© 1999-2017 Citrix Systems, Inc. All rights reserved.

持的设备平台）。如果要仅使用 XenMobile 的 MDM 功能，请在 MDM 模式下部署 XenMobile。 例如，您需要通过 MDM 管理企业所发放的设备以部署设备策略、应用程序，以及检索资产清单，并且能够在设备上进行擦除操作（例如设备擦除）。

在建议的模型中，XenMobile 服务器位于 DMZ 中，可选 NetScaler 位于前端，后者为 XenMobile 提供额外的保护。

移动应用程序管理 (MAM) 模式

MAM 支持 iOS 和 Android 设备，但不支持 Windows Phone 设备（请参阅 XenMobile 中支持的设备平台）。如果要仅使用 XenMobile 的 MAM 功能，但不为 MAM 注册设备，请在 MAM 模式下部署 XenMobile（另请参阅“仅 MAM”模式）。 例如，需要在 BYO 移动设备上保护应用程序和数据；需要提供企业移动应用程序并且能够锁定应用程序和擦除其数据。 设备不能进行 MDM 注册。

在此部署模型中，XenMobile 服务器与 NetScaler Gateway 位于前端，后者为 XenMobile 提供额外的保护。

MDM+MAM 模式

同时使用 MDM 和 MAM 模式可以为 iOS、Android 和 Windows Phone 提供移动应用程序和数据管理以及移动设备管理（请参阅 XenMobile 中支持的设备平台）。如果要使用 XenMobile 的 MDM+MAM 功能，请在 ENT（企业）模式下部署 XenMobile。 例如，需要通过 MDM 管理企业所发放的设备；需要部署设备策略和应用程序以及检索资产清单，并且能够擦除设备。 您还需要提供企业移动应用程序并且能够锁定应用程序和擦除设备上的数据。

在建议的部署模型中，XenMobile 服务器位于 DMZ 中，NetScaler Gateway 位于前端，后者为 XenMobile 提供额外的保护。

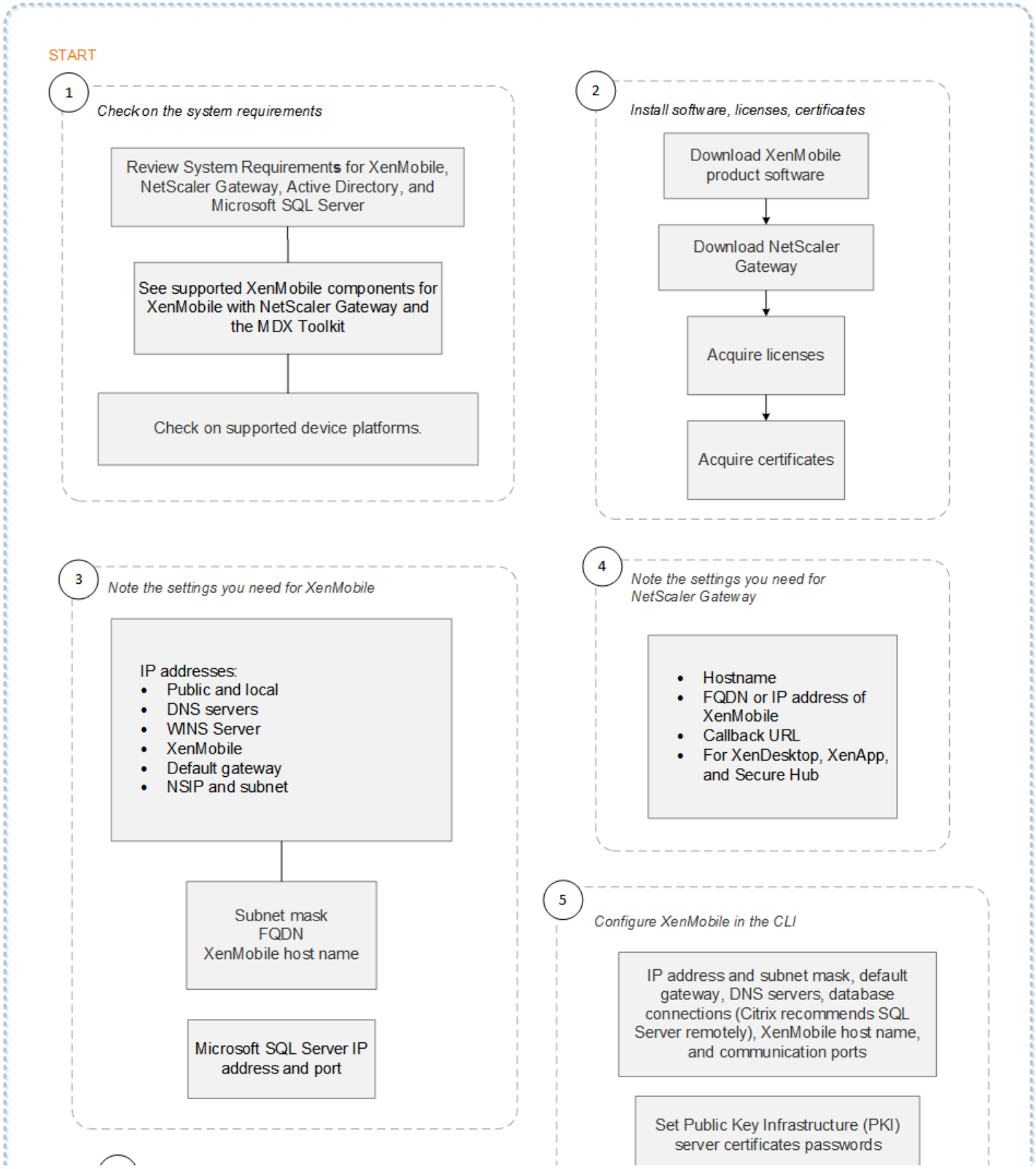
XenMobile 在内部网络中 - 另一种部署方案是将 XenMobile 服务器放置在内部网络中，而非放置在 DMZ 中。 如果您的安全策略要求只能将网络设备放置到 DMZ 中，请使用此部署。 在此部署中，由于 XenMobile 服务器不在 DMZ 中，因此，您不需要在内部防火墙上打开端口即可允许从 DMZ 访问 SQL Server 和 PKI 服务器。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

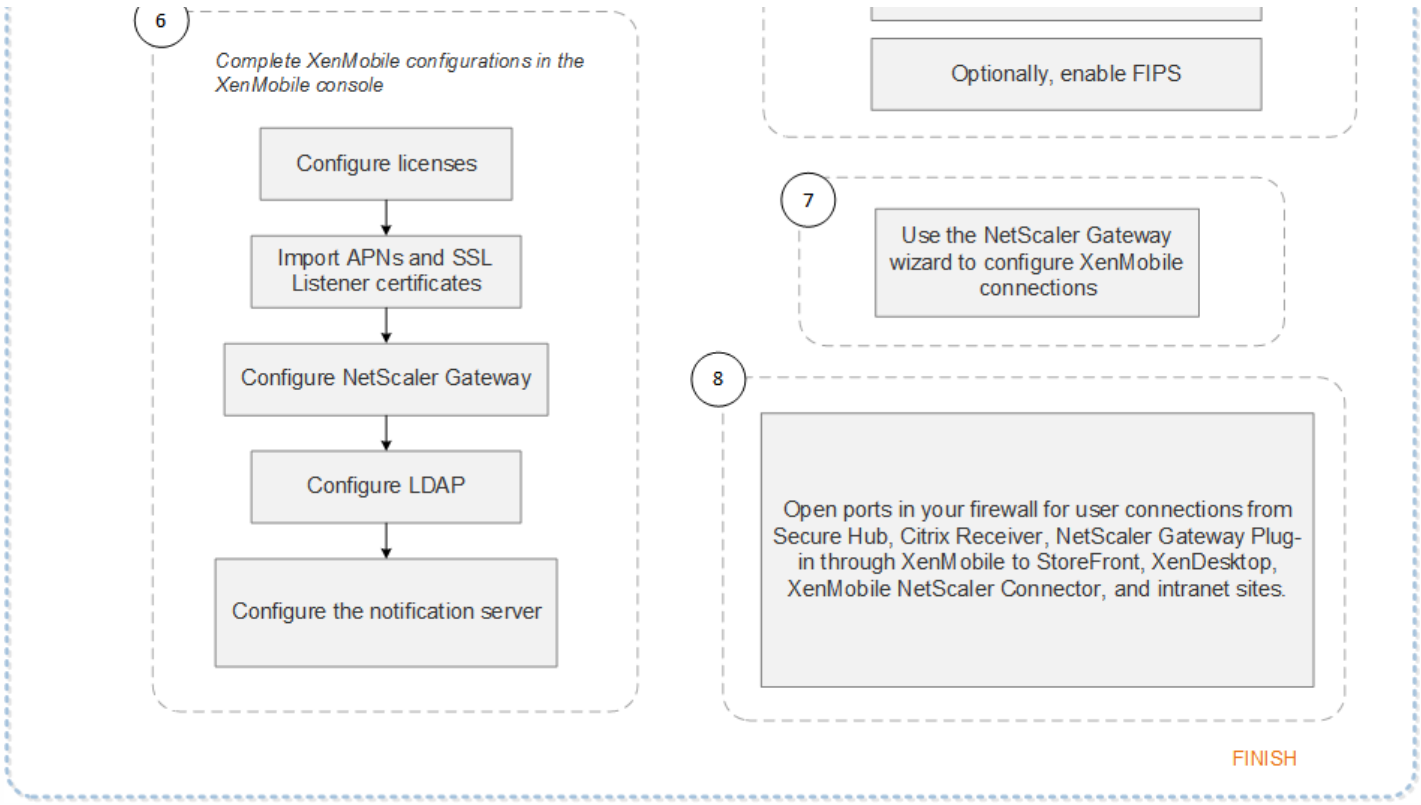
部署 XenMobile 与 NetScaler Gateway 的流程图

Oct 21, 2016

可以使用此流程图作为指导以完成部署 XenMobile 10.3 与 NetScaler Gateway 的主要步骤。 图后面提供每个步骤的主题链接。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



1

- XenMobile 10.3 的系统要求
- XenMobile 兼容性
- XenMobile 10.3 支持的设备平台

2

- 安装 XenMobile
- XenMobile 中的证书
- XenMobile 许可

3

- XenMobile 预安装核对表

4

- XenMobile 预安装核对表

5

- 在命令提示窗口中配置 XenMobile

6

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在 Web 浏览器中配置 XenMobile

7

- 配置 XenMobile 环境的设置

8

- XenMobile 端口要求

流程图还以 PDF 格式提供。

部署 XenMobile 的流程图

© 1999-2017 Citrix Systems, Inc. All rights reserved.

扩展 XenMobile

Oct 21, 2016

理解扩展 XenMobile 基础结构在确定如何部署和配置 XenMobile 方面起着重要作用。 本文回答了与确定小型至大型企业部署的要求相关的常见问题。

性能和可扩展性指南

本文中的数据可用作确定 XenMobile 10.3 基础结构的性能和可扩展性的指南。 用于确定如何配置服务器和数据库的两个关键因素是可扩展性（最大用户/设备数）和登录率。

- 可扩展性定义为执行所定义工作负载的最大并发用户数。 有关加载 XenMobile 基础结构的流程的详细信息，请参阅工作负载。
- 登录率定义为新用户的加入和现有用户的身份验证。
  - 加入率是指环境中首次可以注册的最大设备数。 本文中称为首次利用率或 FTU，此数据点在制定推行策略时非常重要。
  - 现有用户率：向环境进行身份验证的最大用户数，这些用户已经注册并连接其设备。 这些测试包括为已经注册的用户创建会话和执行 WorxMail 和 WorxWeb 应用程序。

下表显示了基于相应 XenMobile 环境测试结果的可扩展性指南。

可扩展性	最多 100,000 台设备	
登录率	加入率 (FTU)	每小时最多 2,777 台设备
	现有用户数	每小时最多 16,667 台设备
配置	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile 服务器 10 节点群集
	数据库	Microsoft SQL Server 外部数据库

> **Important**
>
> 本报告的自动化要求为 1000 到 100000 台设备。 任何超过 100000 台设备的要求都不在本报告范围内。

系统配置和测试结果

本部分描述运行加入 (FTU) 工作负载和现有用户工作负载可扩展测试所使用的硬件配置和结果。

下表定义了 XenMobile 从 1000 台设备扩展到 100000 台设备时采用的硬件和配置建议。 这些指南基于测试结果及其相关工作负载。 建议考虑了退出标准中定义的可接受误差范围。

通过分析测试结果得出以下结论：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 登录率是确定系统可扩展性的重要因素。 除了初始登录，登录率还与环境中配置的身份验证超时值相关。 例如，如果将身份验证超时值设置的太低，用户执行的登录请求会更加频繁。 因此，您需要清楚理解超时设置对环境的影响。
- NetScaler 上每个用户会话的连接数量是一个重要的考虑因素。
- 测试使用的是具有 128 GB RAM 的外部数据库 (SQL Server)、300 GB 的磁盘空间和 24 个虚拟 CPU，这也是生产环境的建议配置。
- 为实现最大可扩展性，增加了 XenMobile 上的 CPU 和 RAM 资源。
- 10 个节点的群集配置是经过验证的最大配置。 扩展到大于 10 个节点需要其他 XenMobile 实现。

下表显示了基于 XenMobile 配置、NetScaler Gateway 设备、群集设置和数据库得出的建议加入率和现有用户登录率。 使用此表中的数据构建新部署的最优注册计划和现有部署的返回用户/设备率。 “配置”部分将注册和登录性能数据与相应的硬件建议关联起来。

预期设备数	1,000	10,000	30,000	60,000	100,000
实际设备数	1,000	9,997	29,976	59,831	99645
登录率					
加入率 (FTU)	125	1250	2,500	2,500	2,777
现有用户数（仅限 Worx）	1,000	2,500	7,500	15,000	16667
配置					
参考环境	VPX-XenMobile 独立模式	MPX-XenMobile 独立模式	MPX-XenMobile 群集 (3)	MPX-XenMobile 群集 (6)	MPX-XenMobile 群集 (10)
NetScaler Gateway	VPX，带 2 GB RAM 2 个虚拟 CPU	MPX-10500		MPX-20500	
XenMobile - 模式	独立	独立	群集		
XenMobile - 群集	不适用	不适用	3	6	10
XenMobile - 虚拟设备	8 GB RAM 和 4 个虚拟 CPU	8 GB RAM 和 4 个虚拟 CPU	8 GB RAM 和 4 个虚拟 CPU	16 GB RAM 和 4 个虚拟 CPU	16 GB RAM 和 4 个虚拟 CPU
数据库	外部	外部 –	外部 –	外部 –	外部 –

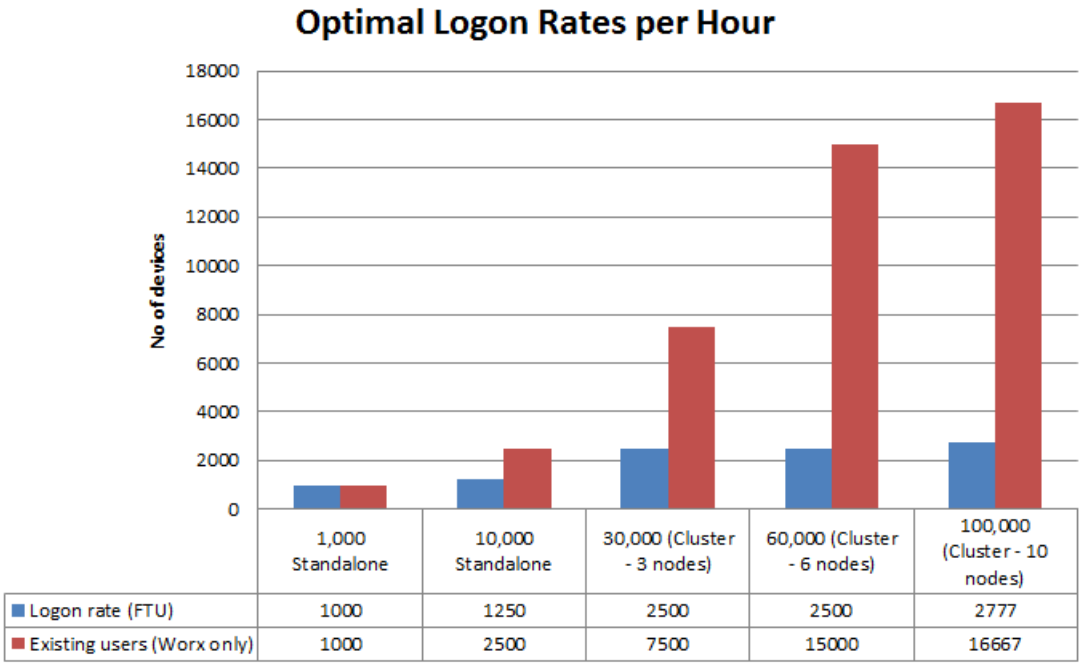
© 1999-2017 Citrix Systems, Inc. All rights reserved.

		Microsoft SQL Server 内存：16 GB vCPU = 12	Microsoft SQL Server 内存：16 GB vCPU = 12	Microsoft SQL Server 内存：32 GB vCPU = 12	Microsoft SQL Server 内存：32 GB vCPU = 16

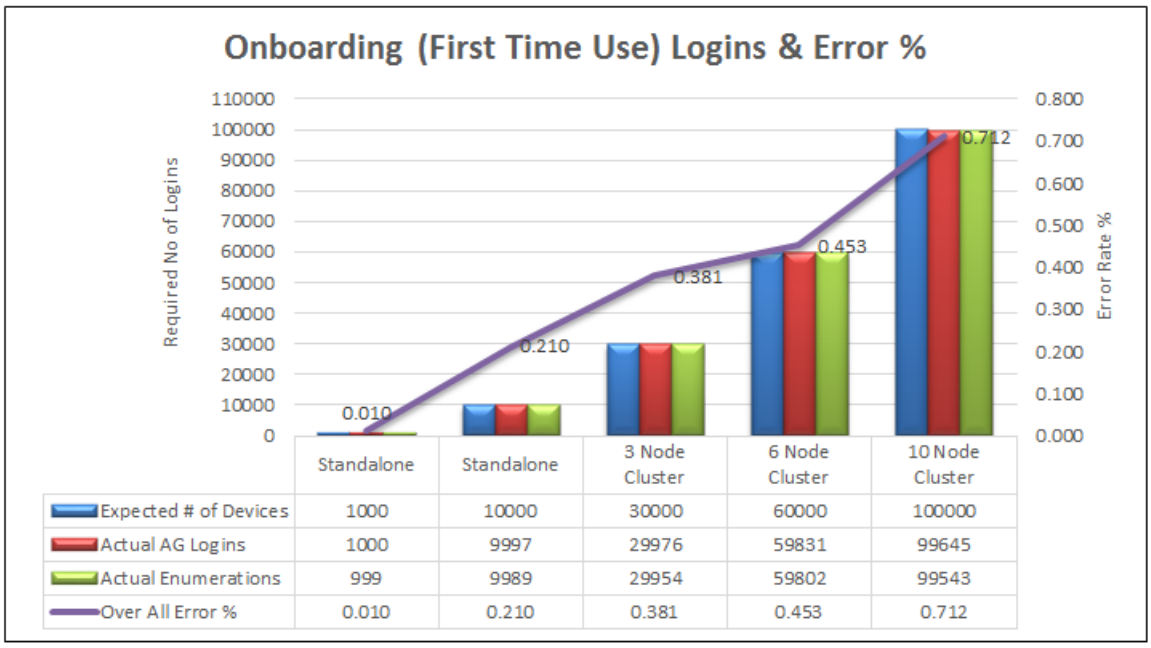
注意：调整系统时，如果超过建议的比率或硬件建议，会遇到以下问题。

以下信息提供了记录的额外数据点以及
影响上表中的结果的额外数据点。

- 注册或登录延迟（往返时间）
  - 平均总延迟：0.5 到 1.5 秒
  - NetScaler Gateway 登录的平均延迟：> 120 到 440 毫秒
  - Worx Store 请求的平均延迟：2 到 3 秒
- 达到扩展限制时，基础结构组件上会出现物理性能下降的情况，如 CPU 和内存耗尽。
  - NetScaler Gateway 和 XenMobile 设备上出现无效响应。
  - 高负载期间会延缓 XenMobile 控制台的响应时间。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



上图中的错误百分比包括遇到的总错误，考虑了每个操作对应的请求，并非仅限于登录。 根据退出条件中的定义，运行的每个测试的错误百分比都在可接受的限制 (1%) 内。

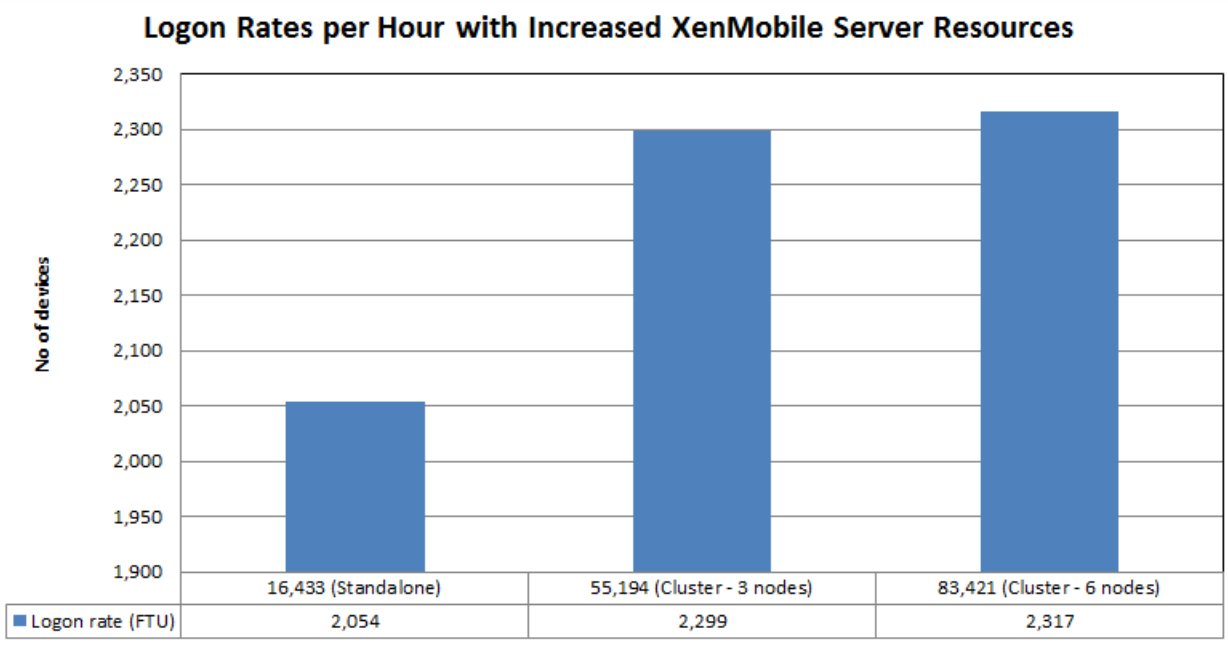
资源增加的情况下 XenMobile Enterprise Edition 的扩展测试

此测试结果深度揭示了使用更少数量的节点来支持更多设备的 XenMobile Enterprise Edition 的部署策略。 此测试已针对资源增加的情况下每个 XenMobile 服务器节点的硬件组件（CPU 和内存）运行，以衡量其扩展功能。 与在资源数正常且节点数相同的情况下运行的测试相比，这会导致 XenMobile 服务器节点支持的最大会话/设备数增加。

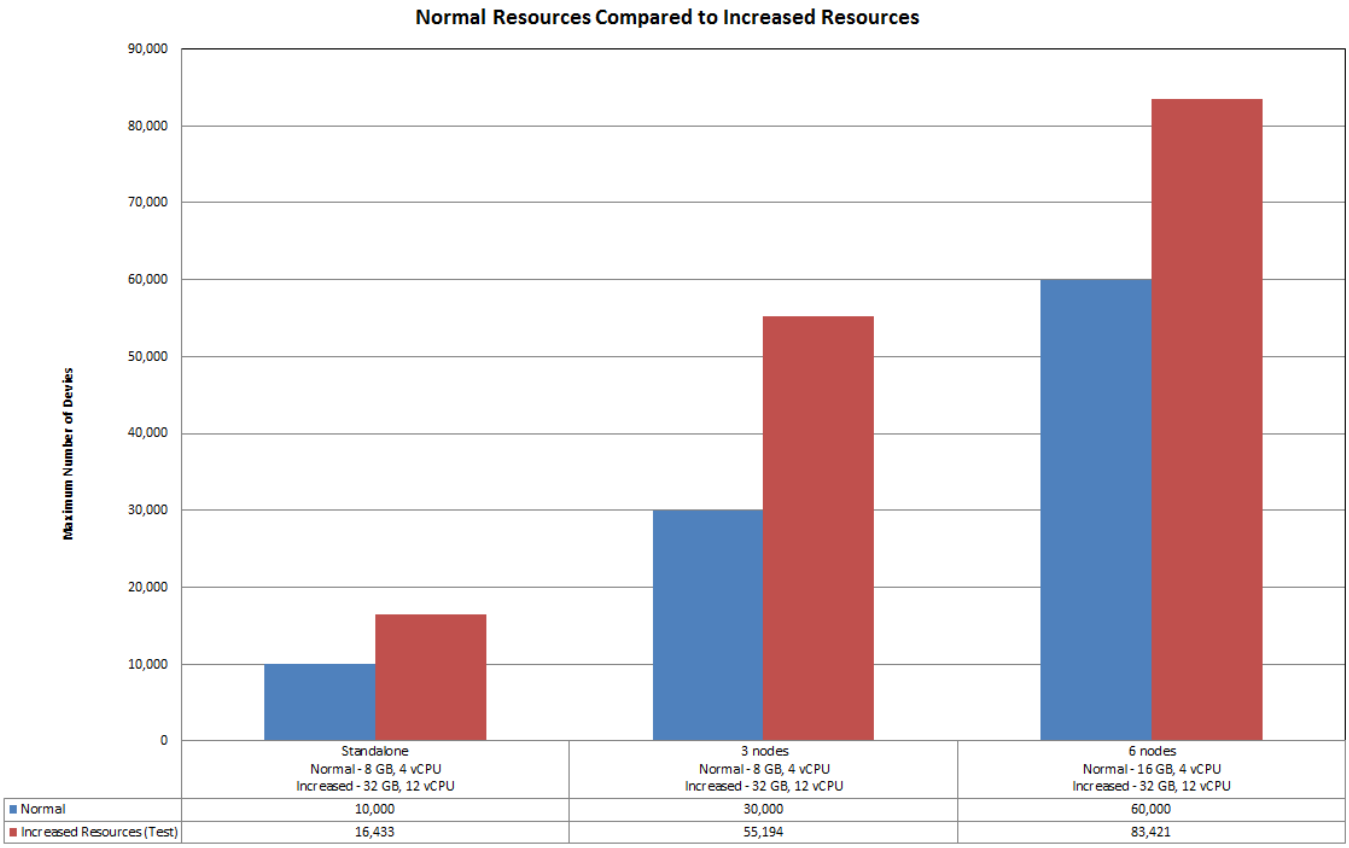
可扩展性			
实际最大设备数	16,433	55,194	83,421
登录率			
实际首次使用 - 增加新用户	2,054	2,299	2,317
配置			
参考环境	VPX-XenMobile 独立模式	MPX-XenMobile 群集 3	MPX-XenMobile 群集 6
NetScaler Gateway	MPX-10500	MPX-10500	MPX-20500
XenMobile - 模式	独立	群集	群集

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile - 群集	不适用	3	6
XenMobile - 虚拟设备	内存 - 32 GB vCPU - 12	内存 – 32 GB vCPU - 12	内存 - 32 GB vCPU - 12
Device Manager 数据库	外部 – S SQL Server 内存 – 16 GB vCPU - 12	外部 - SQL Server 内存 – 32 GB vCPU - 12	外部 - SQL Server 内存 - 32GB vCPU - 16
Active Directory	内存 – 8 GB vCPU = 4	内存 - 16 GB vCPU - 4	内存 – 16 GB vCPU - 4

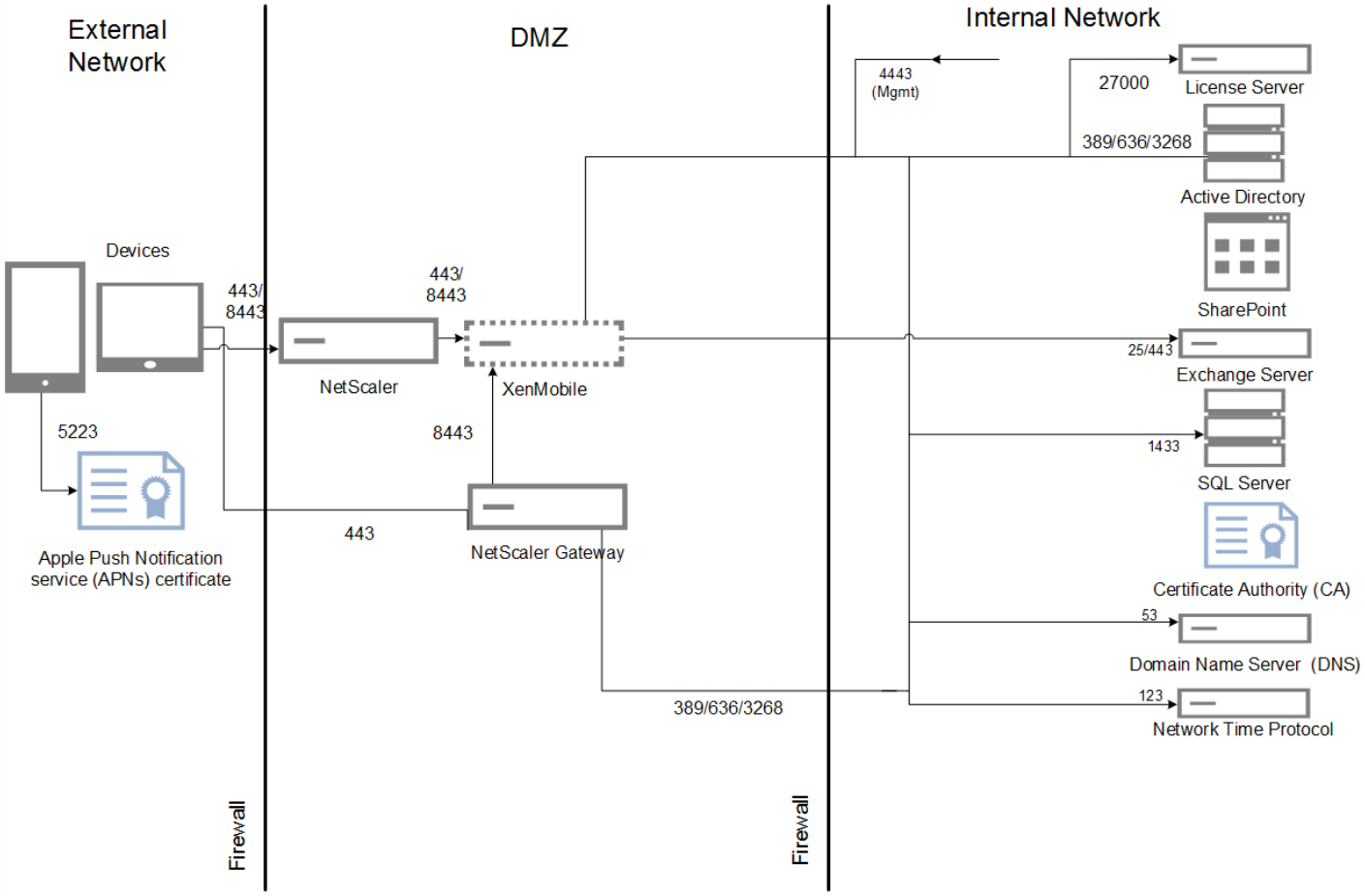


© 1999-2017 Citrix Systems, Inc. All rights reserved.



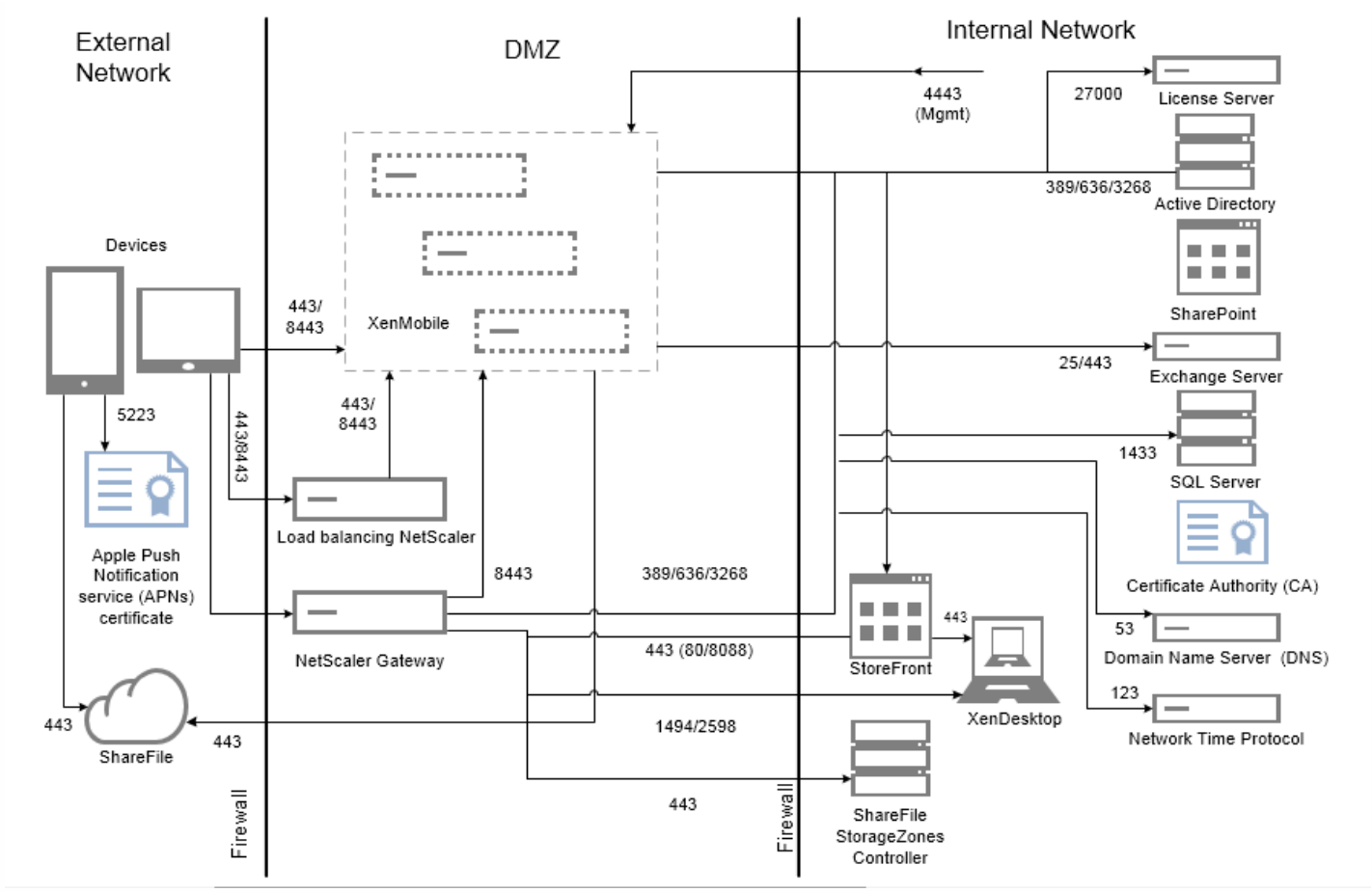
下图显示了小型部署的参考体系结构。 这是一个最多支持 10000 台设备的独立体系结构。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



下图显示了企业部署的参考体系结构。 这是一个群集体系结构，带有通过 HTTP 进行 SSL 卸载的 MAM 功能，可支持 10,000 台或更多设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



测试方法

测试针对 XenMobile Enterprise 运行以建立标准。 为了同时面向小型和大型部署，测试使用了 1000 至 100000 台设备。

创建工作负载以模拟实际使用情况。 针对每个测试运行这些工作负载，以了解对注册和登录率的影响。 测试的目的是为了在退出标准中描述的可接受误差范围内，获取最优登录率。 登录率是确定基础结构组件的硬件配置建议的关键因素。

加入 (FTU) 工作负载登录请求包括自动检测、身份验证和设备注册操作。 应用程序订阅、安装和启动操作在测试期间统一分发。 这样提供了对用户操作的最真实模拟。 在测试的结尾，注销会话。 现有用户工作负载登录请求仅包括身份验证请求。

工作负载

用户工作负载的定义如下：

用户会话/设备数	每个会话包括 NetScaler Gateway 登录、枚举、设备注册等。
Worx Store 启动	用户多次启动 Worx Store，每次订阅或安装多个应用程序，不管这些应用程序是移动应用程序 (web/SaaS/MDX) 还是 Windows 应用程序 (HDX)。
每台设备的 Web/SaaS 应用程序 SSO	web/SaaS 应用程序的启动序列的帐户数达到标识点，XenMobile 完成 SSO 并返回实际应用程序 URL。 流量不发送给实际应用程序。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

每台设备的 MDX 应用程序下载数	MDX 应用程序的下载总数（可能会发生在两次 Worx Store 启动之间）。 对于 iOS，此数据还包括 Apple ITMS 的应用程序自动安装，Apple ITMS 利用 NetScaler Gateway 上的新令牌/tms 服务 API。

注意事项与假设

为了将 XenMobile 扩展到超过 30000 台设备，应调整以下服务器参数：

配置文件 - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/push_services.xml

-

配置文件 - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/ew-config.properties

- ios.mdm.apns.connectionPoolSize=15
- hibernate.c3p0.max_size=1000

应在所有 XenMobile 节点上执行这些更改，然后重新启动服务器。

可扩展性测试不包括以下场景。 在以后增强扩展测试功能时会考虑这些场景：

- 未测试连接到 Android 的设备。
- 未测试软件包部署。
- 未测试 Windows 平台。

每个 XenMobile 最多同时支持 10000 个连接。

测试采用 LAN 在理想连接状态下运行，以避免网络延迟问题。 在实际场景中，可扩展性还取决于用户的可用带宽，尤其是应用程序下载问题。

加入 (FTU) 工作负载

加入 (FTU) 工作负载定义为用户首次访问 XenMobile 环境。 此工作负载中操作包括：

- 自动检测
- 注册
- 身份验证
- 设备注册
- 应用程序交付（web、SaaS 和移动 MDX 应用程序）
  - 应用程序订阅（包括图像和图标下载）
  - 已订阅 MDX 应用程序的安装
- 应用程序启动（Web、SaaS 和移动 MDX 应用程序），包括设备状态检查
- 策略推送（面向 iOS）
- WorxMail 和 WorxWeb 最小连接数（VPN 通道） — 两个连接
- 通过 XenMobile 安装必需的应用程序

工作负载参数通过下表定义：

设备	设备注册	枚举数	每台设备枚举的应用	每个设备的 WorxStore 启动次数	每台设备的 Web/SaaS SSO	每台设备的 MDX 应用程序下载数	通过 XenMobile 服务器触发	每个设备推送的策略

© 1999-2017 Citrix Systems, Inc. All rights reserved.

			程序数				的必要应用程序下载次数	数 (iOS)
1000	1000	1000	14	4	4	2	2	2
10000	10000	10000	14	4	4	2	2	2
30000	30000	30000	14	4	4	2	2	2
60000	60000	60000	14	4	4	2	2	2
100000	100000	100000	14	4	4	2	2	2

仅使用 Worx 连接的工作负载的现有用户数

下表显示了现有用户（仅使用 Worx 连接）工作负载。 此工作负载模拟使用 WorxMail 和 WorxWeb 应用程序的用户。 此模拟用于测试 XenMobile 配置内 NetScaler Gateway 的可扩展性。 这是可以实现的，因为通过仅使用这两个 Worx 应用程序，网络将低于最小负载。 对于 WorxWeb 应用程序，用户访问内部 Web 站点，不会触发 XenMobile 服务器 SSO。 本模式中的操作包括：

- 身份验证（NetScaler Gateway 和 XenMobile）
- WorxMail 和 WorxWeb 连接（VPN 通道） — 四个连接

下表显示了现有用户的工作负载参数。

设备	枚举数	每台设备枚举的应用程序数	每个设备的 VPN 通道数[1]
1000	1000	14	4
10000	10000	14	4
30000	30000	14	4
60000	60000	14	4
100000	100000	14	4

1. VPN 通道数与 WorxMail 和 WorxWeb 连接数相对应。

下表显示了 WorxMail 和 WorxWeb 的连接配置文件：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备连接	连接类型	每个会话发送的数据[1]	每个会话接收的数据[1]
WorxMail 连接 #1	类型 1[2]	4.1 MB	4.1 MB
WorxMail 连接 #2	类型 1	6.3 MB	12.5 MB
WorxWeb 连接 #1	类型 2[3]	5.2 MB	15.7 MB
WorxWeb 连接 #2	类型 2	4.1 MB	3.4 MB
每个会话传输的总字节数[1]		~19.7 MB	~ 40.7 MB

1. 每个会话：8 小时。

2. 类型 1：通过长时间有效的连接，进行非对称发送和接收（即，WorxMail 使用专用的 Microsoft Exchange 邮箱连接）。

3. 类型 2：通过关闭后经过延迟再重新打开的连接，进行非对称发送和接收（即，WorxWeb 连接）。

这些建议建立在用于自动执行“中型”工作负载的 WorxMail 和 WorxWeb 配置文件
的基础之上。 修改连接详细信息会影响分析结果。 例如，如果每个用户的连接数增加，所支持的 NetScaler Gateway 会话数可能会减少。

WorxMail 和 WorxWeb 配置文件

用于每个应用程序的配置文件的目的在于自动执行“非常繁重”的工作负载。下表显示了 WorxMail 和 WorxWeb 配置文件详细信息。

中等工作负载的 WorxMail 配置文件

每天发送的消息数	20
每天接收的消息数	80
每天读取的消息数	80
每天删除的消息数	20
消息平均大小 (KB)	200

中等工作负载的 WorxWeb 配置文件

启动的 Web 应用程序数	10

© 1999-2017 Citrix Systems, Inc. All rights reserved.

手动打开的 Web 页面数	10
平均每个 Web 应用程序的请求-响应对数	100
请求的平均大小（字节）	300
响应的平均大小（字节）	1000

配置和参数

运行可扩展性测试时使用了以下配置：

- NetScaler Gateway 和负载平衡 (LB) 虚拟服务器同时存在于同一个 NetScaler Gateway 设备上。
- NetScaler Gateway 上使用 2048 位密钥执行 SSL 事务。

退出标准

登录率是此分析的基础。 它们为基础结构组件及其各自的配置提供指南。 一定要注意，登录率所考虑的错误包括以下各项：

- 无效响应
  - 状态代码为 401/404 而非 200 的响应为无效响应。
- 请求超时
  - 响应应在 120 秒之内发生。
- 连接错误
  - 发生连接重置。
  - 出现连接突然中止。

如果总错误率低于从给定设备发送的总请求数的 1%，则登录率为可接受。 错误率包括对应于各个单独工作负载操作的错误，以及与基础结构组件的物理性能相关的错误，如 CPU 和内存耗尽。

软件和硬件详细信息

下表列出了用于这些测试的 XenMobile 基础结构软件。

组件	版本
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
外部数据库	Microsoft SQL Server 2014

© 1999-2017 Citrix Systems, Inc. All rights reserved.

可扩展性测试在 XenServer 平台上运行，如下表所示。

供应商	Genuine Intel
型号	Intel Xeon CPU — E5645，2.40 GHz (CPU = 24)

包括基础结构核心服务（例如，Active Directory、Windows 域名服务 (DNS)、证书颁发机构、Microsoft Exchange 等），以及 XenMobile 组件（XenMobile 虚拟设备和 NetScaler Gateway VPX 虚拟设备，如适用）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

关于 XenMobile 云

Aug 11, 2016

XenMobile Cloud 是一项产品服务，可提供用于管理应用程序和设备以及用户或用户组的 XenMobile 企业移动性管理 (EMM) 环境。 借助 XenMobile Cloud，Citrix 通过 Citrix Cloud Operations 组处理基础结构现场的配置和维护。 此分离结构使您可以专注于用户体验以及设备、策略和应用程序的管理。 XenMobile Cloud 使用订阅费用省去了购买和管理许可证的需要。

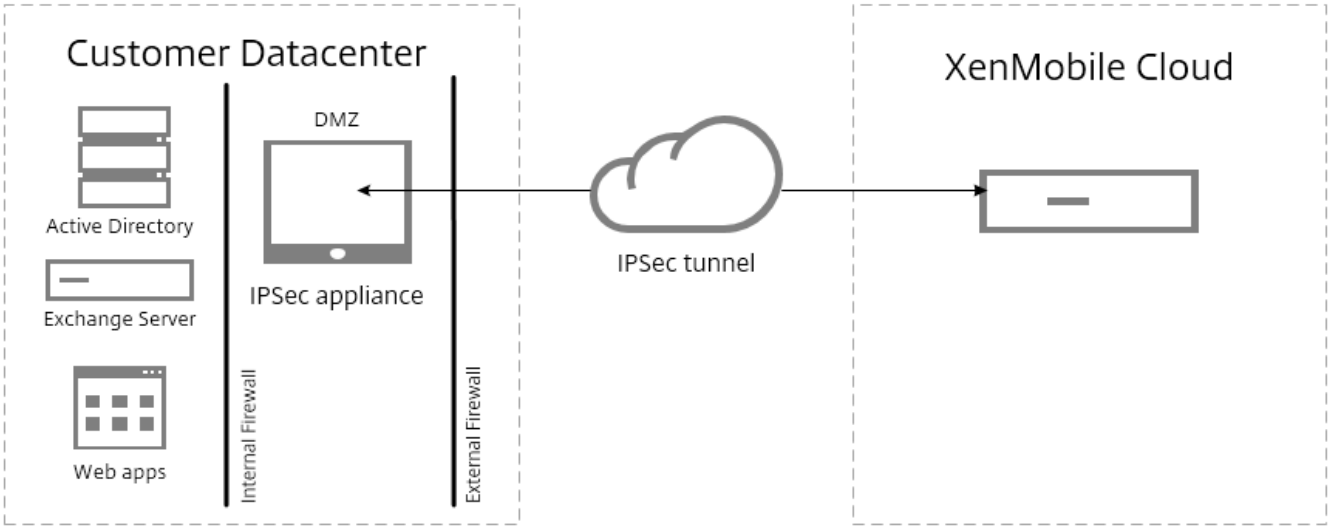
Cloud Operations 管理员处理网络连接的维护和配置，以及 Citrix 产品的集成，如 NetScaler、XenApp、XenDesktop、StoreFront 和 ShareFile。 Cloud 环境托管于遍及全球的 Amazon 数据中心内，可提供高性能、快速响应和支持。

要了解 XenMobile Cloud，请访问 https://www.citrix.com/products/xenmobile/tech-info/cloud.html

注意

- 此 Remote Support 客户端在适用于 Windows CE 和 Samsung Android 设备的 XenMobile Cloud 10.x 中不可用。
- XenMobile Cloud 服务器端组件不遵从 FIPS 140-2。
- Citrix 不支持在 XenMobile Cloud 中将 syslog 与本地 syslog 服务器相集成。 相反，可以在 XenMobile 控制台中从“支持”页面下载这些日志。 为此，必须单击**全部下载**才能获取系统日志。 有关详细信息，请参阅在 XenMobile 中查看和分析日志文件。

下图显示了 XenMobile Cloud 的基本体系结构。有关详细的参考体系结构图，请参阅 XenMobile Deployment Handbook（《XenMobile 部署手册》）中的“Reference Architecture for Cloud Deployments”（适用于云部署的参考体系结构）部分。



可以通过安装和部署 Citrix CloudBridge 或通过使用数据中心内的现有 IPsec 网关，将 XenMobile Cloud 体系结构集成到您的现有基础结构中。

利用此体系结构，您可以在云中（由 Cloud Operations 组处理）或在数据中心内使用 NetScaler 并从中受益。 在数据中心内使用时，NetScaler 为您提供单点管理，用于根据用户身份和端点设备控制访问权限和限制会话内的操作。 此部署可提供更好

© 1999-2017 Citrix Systems, Inc. All rights reserved.

的应用程序安全性、数据保护和合规性管理。

要下载并安装 Citrix CloudBridge，请转至 https://www.citrix.com/downloads/cloudbridge.html

XenMobile Cloud 中的角色

XenMobile Cloud 与 XenMobile 内部部署使用相同的基于角色的访问控制 (Role Based Access Control, RBAC)。 XenMobile Cloud 的不同之处在于 Citrix Cloud Operations 组处理用于基础结构的所有角色，包括置备。

下图显示了 XenMobile Cloud 的 RBAC 控制台。

XenMobile 实现四种默认用户角色，用于在逻辑上区分系统功能的访问权限。 默认角色如下：

- **管理员**。 授予完整系统访问权限。
- **支持**。 授予对远程支持的访问权限。
- **用户**。 向用户授予注册设备和使用自助服务门户的访问权限。
- **置备**。 向管理员授予使用设备置备工具以组的形式置备所有 Windows Mobile/CE 设备的功能。 此角色由 Cloud Operation 组控制。

您可以使用默认角色作为模板，通过自定义来创建具有这些默认角色定义的功能之外的其他特定系统功能的访问权限的新用户角色。

您可以将角色分配给用户（在用户级别）或 Active Directory 组（此组中的所有用户具有相同的权限）。 如果用户属于多个 Active Directory 组，则所有权限合并起来，以定义该用户的权限。 例如，如果 ADGroupA 可以查找管理员设备，ADGroupB 用户可以擦除员工设备，则同时属于这两个组的用户可以查找和擦除管理员和员工的设备。

注意：本地用户可以仅分配有一个角色。

可以使用 XenMobile 中的 RBAC 功能执行以下操作：

- 创建新角色。
- 将组添加到角色。
- 向本地用户分配角色。

您可以分配以下角色： Citrix Cloud Operations 组控制此列表上的所有角色。

主要部分	节	页面	页面面向

© 1999-2017 Citrix Systems, Inc. All rights reserved.

控制板	ALL	ALL	IT 管理员
管理	设备	ALL	IT 管理员
管理	注册	ALL	IT 管理员
配置	设备策略	ALL	IT 管理员
配置	应用程序	ALL	IT 管理员
配置	操作	ALL	IT 管理员
配置	交付组	ALL	IT 管理员
配置	设置	证书	Cloud 管理员和 IT 管理员
配置	设置	通知模板	IT 管理员
配置	设置	基于角色的访问控制	Cloud 管理员和 IT 管理员
配置	设置	注册	IT 管理员
配置	设置	本地用户和组	Cloud 管理员和 IT 管理员
配置	设置	版本管理	Cloud 管理员和 IT 管理员
配置	设置	工作流	IT 管理员
配置	设置	凭据提供程序	IT 管理员
配置	设置	PKI 实体	IT 管理员
配置	设置	客户端属性	IT 管理员
配置	设置	NetScaler Gateway	仅 Cloud 管理员或仅 IT 管理员
配置	设置	运营商 SMS 网关	IT 管理员

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置	设置	通知服务器	Cloud 管理员和 IT 管理员
配置	设置	ActiveSync Gateway	IT 管理员
配置	设置	iOS VPP	IT 管理员
支持	日志操作	日志设置	Cloud 管理员和 IT 管理员以及技术支持人员
配置	设置	服务器属性	Cloud 管理员和 IT 管理员以及技术支持人员
配置	设置	Google Play 凭据	IT 管理员
配置	设置	LDAP	IT 管理员
配置	设置	网络访问控制	IT 管理员
支持	支持包	创建支持包	Cloud 管理员和技术支持人员
配置	设置	iOS Device Enrollment Program	IT 管理员
配置	设置	移动服务提供商	IT 管理员
配置	设置	Samsung KNOX	IT 管理员
配置	设置	XenApp/XenDesktop	IT 管理员
配置	设置	ShareFile	IT 管理员
支持	Advanced	群集信息	Cloud 管理员和技术支持人员
支持	Advanced	垃圾回收	Cloud 管理员和技术支持人员
支持	Advanced	Java 内存属性	Cloud 管理员和技术支持人员
支持	Advanced	宏	IT 管理员
FTU向导	初始配置	NetScaler Gateway	仅 Cloud 管理员或仅 IT 管理员

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置	设置	Worx Home 支持	IT 管理员
配置	设置	Worx Store 外观方案	IT 管理员
支持	诊断	NetScaler Gateway 连接检查	Cloud 管理员和 IT 管理员以及技术支持人员
支持	诊断	XenMobile 连接检查	Cloud 管理员和 IT 管理员以及技术支持人员
支持	日志操作	日志	Cloud 管理员和 IT 管理员以及技术支持人员
支持	Advanced	PKI 配置	Cloud 管理员和 IT 管理员
支持	工具	APNS 签名实用程序	客户和技术支持人员
支持	工具	Citrix Insight Services	Cloud 管理员和 IT 管理员以及技术支持人员
FTU 向导	初始配置	SSL 证书	Cloud 管理员和 IT 管理员
FTU 向导	初始配置	LDAP 配置	IT 管理员
FTU 向导	初始配置	通知服务器	Cloud 管理员和 IT 管理员
FTU 向导	初始配置	摘要	Cloud 管理员和 IT 管理员
支持	链接	Citrix 知识中心	Cloud 管理员和 IT 管理员以及技术支持人员
支持	工具	设备 NetScaler Connector 状态	IT 管理员
支持	日志操作	日志设置->日志大小	Cloud 管理员和技术支持人员

有关自定义角色的分步说明，请参谋使用 RBAC 配置角色。

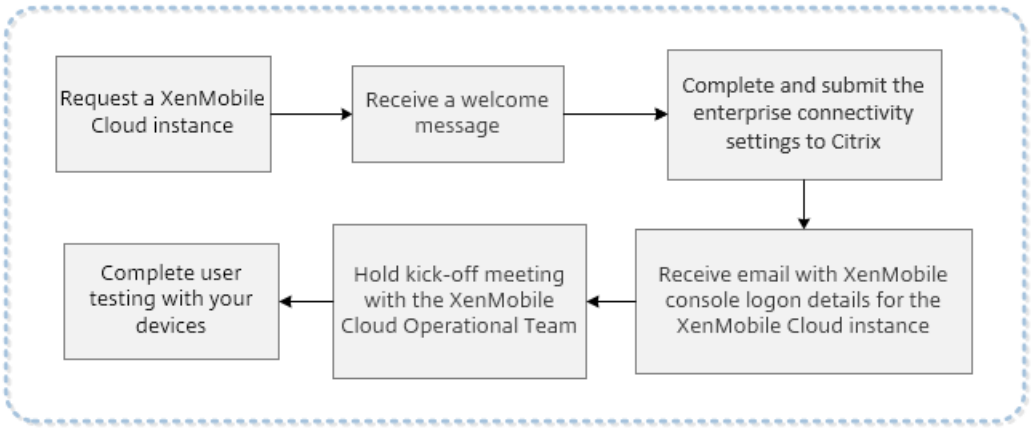
要请求重新启动服务器节点，请在 https://www.citrix.com/contact/technical-support.html 联系技术支持人员

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 云必备条件和管理

Aug 11, 2016

下图显示了自您向使用贵组织中的设备进行测试的用户请求 XenMobile 云实例的服务过程的步骤。 评估或购买 XenMobile 云时，XenMobile 云运营团队将提供实时入门帮助和沟通，以确保核心 XenMobile 云服务正在运行且配置正确无误。



Citrix 托管和交付 XenMobile 云解决方案。 但是，需要满足某些通信和端口要求才能将 XenMobile 云基础结构连接到公司服务，例如 Active Directory。 请查看以下部分，为您的 XenMobile 云部署做好准备。

XenMobile 云 IPSec 通道网关

可以使用 XenMobile Enterprise Connector，这是一个 IPsec 通道，用于将 XenMobile Cloud 基础结构与公司服务相连接，例如 Active Directory。

以下 Amazon Web Services (AWS) Web 站点中列出的 IPsec 网关已通过官方测试，支持 XenMobile Cloud 解决方案：http://aws.amazon.com/vpc/faqs/。 滚动到“问： 可以使用哪种客户网关设备连接 Amazon VPC？”部分，找到受支持的网关列表。

> **注意**
>
> 如果您的 IPSec 网关不在已批准的列表中，IPsec 网关可能仍适用于 XenMobile 云，但设置所需的时间会延长，并且可能要求您使用官方宣布支持的 IPSec 网关作为回退计划。

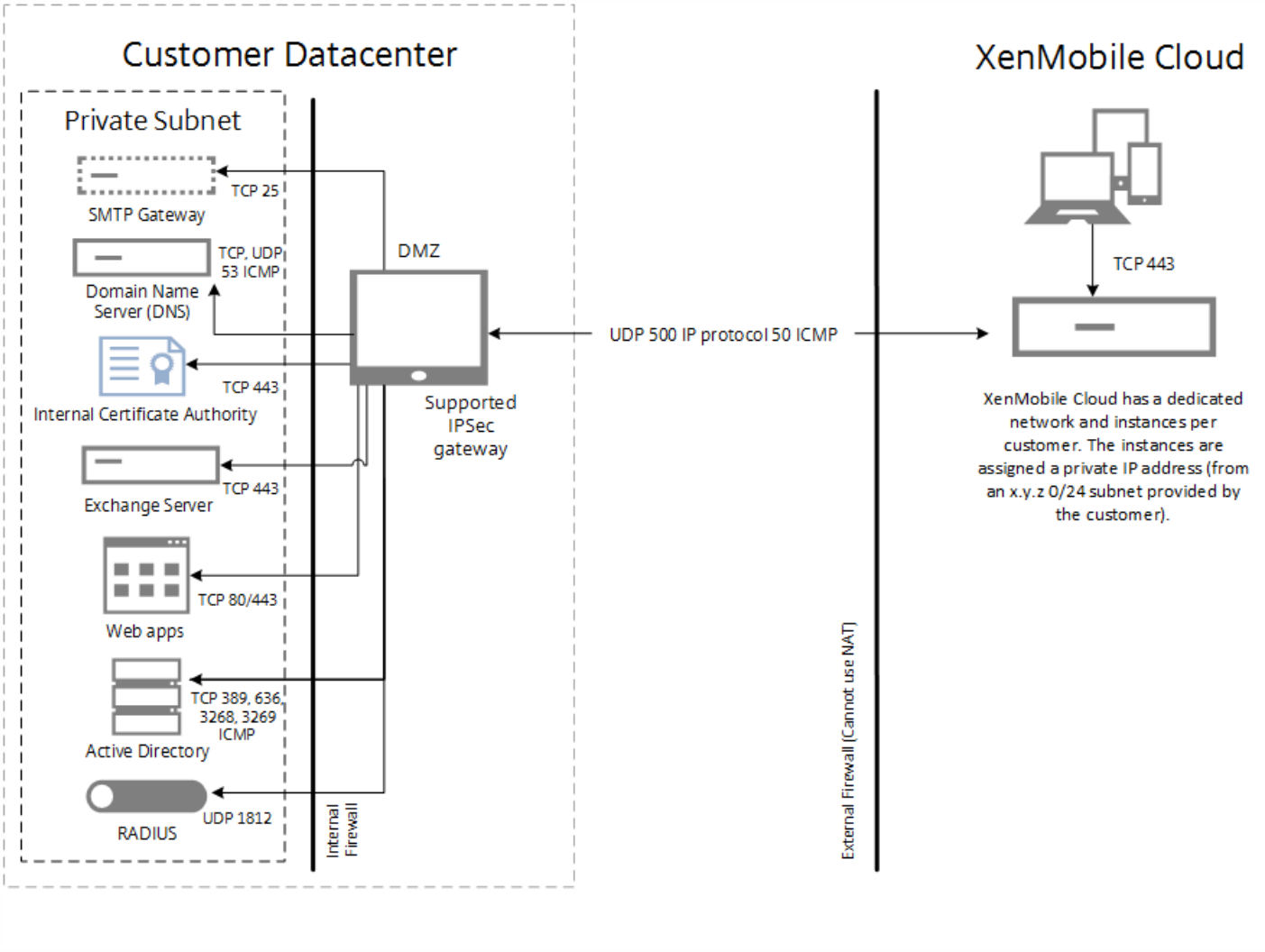
您的 IPSec 网关需要具有直接分配给自身的公用 IP 地址，并且该地址不能使用网络地址转换 (NAT)。

您的 AWS VPN 连接需永久保持活动状态（从客户端启动）。 配置从您的环境到 Amazon VPC 子网的永久 ping 以确保服务连续性。

您的 AWS VPN 连接不支持在 IPsec 网关上配置的多个安全关联。 已将您限制为对每个通道使用一个唯一的安全关联对，即一个入站安全关联和一个出站安全关联。 合并您的规则并进行过滤，以确保这些规则不允许传输不需要的流量。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

下图显示了如何在 XenMobile Cloud 解决方案中配置 IPsec 通道，使其通过各种端口连接到您的公司服务。



下表显示了 XenMobile 云部署的通信和端口要求，包括 IPSec 通道要求。

源	目标	协议	端口	说明
外部（边缘）防火墙 – 入站规则				
XenMobile 云 (AWS) IPCSEC VPN [1] 的公共 IP 地址	客户 IPSec 设备	UPD	500	IPSec IKE 配置。
XenMobile 云 (AWS) IPCSEC VPN [1] 的公共 IP 地址	客户 IPSec 设备	IP 协议 ID	50	IPSec ESP 协议。
XenMobile 云 (AWS) IPCSEC VPN [1] 的公共	客户 IPSec 设备	ICMP		适用于故障排除（可以在设置后删除）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

IP 地址				
外部（边缘）防火墙 – 出站规则				
客户 DMZ 子网	XenMobile 云 (AWS) IPSec VPN [1] 的公共 IP 地址	UDP	500	IPSec IKE 配置。
客户 DMZ 子网	XenMobile 云 (AWS) IPSec VPN [1] 的公共 IP 地址	IP 协议 ID	50、51	IPSec ESP 协议。
客户 DMZ 子网	XenMobile 云 (AWS) IPSec VPN [1] 的公共 IP 地址	ICMP		适用于故障排除（可以在设置后删除）。
内部防火墙 – 入站规则				
未使用的可路由 /24 客户子网 [2]	客户数据中心中的内部 DNS 服务器	TCP、UPP、ICMP	53	DNS 解析。
未使用的可路由 /24 客户子网 [2]	客户数据中心中的 Active Directory 域控制器	LDAP(TCP)	389、636 3268、3269	适用于用户 Active Directory 身份验证以及对域控制器的目录查询。
未使用的可路由 /24 客户子网 [2]	客户数据中心中的 Active Directory 域控制器	ICMP		适用于故障排除（可以在完成完整设置后删除）。
未使用的可路由 /24 客户子网 [2]	客户数据中心中的 Exchange Server	SMTP (TCP)	25	可选：适用于 XenMobile 电子邮件通知。
未使用的可路由 /24 客户子网 [2]	客户数据中心中的 Exchange Server	HTTP、HTTPS (TCP)	80、443	Exchange ActiveSync，需要在 ActiveSync 流量从设备发送到 XenMobile 云基础结构（通过 IPSec 通道），再发送至 Exchange Server 时使用 如果用户设备将通过 Internet 与公共 ActiveSync FQDN 通信，而不需要通

© 1999-2017 Citrix Systems, Inc. All rights reserved.

				过 XenMobile IPSec 通道发送到 Exchange Server，则不需要使用。
未使用的可路由 /24 客户子网 [2]	应用程序服务器，例如 Intranet/Web 服务器、SharePoint 服务器等。	HTTP、HTTPS (TCP)	80、443	通过 XenMobile IPSec 通道从用户的移动设备访问 Intranet 和/或应用程序服务器。 需要将每个应用程序服务器添加到防火墙规则中，同时添加访问应用程序所需的端口号（通常为端口 80 和/或 443）。
未使用的可路由 /24 客户子网 [2]	PKI 服务器（如果使用本地 PKI）	HTTPS (TCP)	443	可选（不用于 XenMobile POC）： 可以利用此端口在 XenMobile 云基础结构与本地 PKI 基础结构（例如 Microsoft CA）之间创建集成，以便在 XenMobile 解决方案内部建立基于证书的身份验证。
未使用的可路由 /24 客户子网 [2]	RADIUS 服务器	UDP	1812	可选（不用于 XenMobile POC）： 可以使用此端口在 XenMobile 解决方案内部建立双因素身份验证。
内部防火墙 – 出站规则				
内部客户子网，XenMobile 控制台需要通过该子网提供	未使用的可路由 /24 客户子网 [2]	TCP	4443	XenMobile 云基础结构中的 XenMobile App Controller (MAM) 控制台。

[1] 如果 XenMobile 云实例和 IPSec 组件在 XenMobile 云基础结构中置备，则由 XenMobile 云团队提供。

[2] 未使用的 /24 子网，由客户在置备过程中提供，与客户数据中心中的内部子网不冲突，可以路由。

如果您计划部署 XenMobile Mail Manager 或 XenMobile NetScaler Connector 用于本机电子邮件过滤（例如，阻止或允许在用户的移动设备上从本机电子邮件客户端建立电子邮件连接的功能），请查看以下附加要求。

XenMobile Apple APNS 证书

如果您打算通过 XenMobile 云部署管理 IOS 设备，则需要使用 Apple APNS 证书。 应在部署 XenMobile 云解决方案之前准备该证书。 有关步骤，请参阅请求 APNs 证书。

WorxMail for iOS 推送通知证书

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果要对您的 WorxMail 部署使用推送通知，应为 iOS WorxMail 推送通知准备一个 Apple APNS 证书。 有关详细信息，请参阅 WorxMail for iOS 的推送通知。

XenMobile MDX Toolkit

MDX Toolkit 是一项应用程序打包技术，用于将应用程序准备好用于 XenMobile 部署。 如果要打包应用程序，例如 Citrix WorxMail、WorxMail、WorxNotes、QuickEdit 等，则需要安装 MDX Toolkit。 有关详细信息，请参阅关于 MDX Toolkit。

如果要打包 iOS 应用程序，则需要使用 Apple 开发者帐户来创建必要的 Apple 分发配置文件。 有关详细信息，请参阅 MDX Toolkit 系统要求和 Apple 开发者帐户 Web 站点。

如果要打包适用于 Windows Phone 8.1 设备的应用程序，请参阅系统要求。

面向 Windows Phone 注册的 XenMobile 自动发现功能

如果要使用面向 Windows Phone 8.1 注册的 XenMobile 自动发现功能，请确保您具有可用的公共 SSL 证书。 有关详细信息，请参阅在 XenMobile 中启用自动发现以执行用户注册。

XenMobile 控制台

XenMobile 云解决方案使用与本地 XenMobile 部署相同的 Web 控制台。 这样，云解决方案的日常管理（例如，策略管理、应用程序管理、设备管理等）的执行方式将与本地 XenMobile 部署相似。 有关在 XenMobile 控制台中管理应用程序和设备的信息，请参阅 XenMobile 控制台入门。

XenMobile 设备注册

有关适用于不同设备平台的 XenMobile 注册选项的信息，请参阅注册用户和设备。

XenMobile 支持

有关如何在 XenMobile 控制台中访问支持相关信息的详细信息，请参阅 XenMobile 支持和维护。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 云中支持的移动平台

Aug 11, 2016

请求 XenMobile 云实例后，如果需要，可以开始为支持 Android、iOS 和 Windows 平台做好准备。 完成适用于您的环境的步骤过程中，请将信息保存在方便的位置，以便能够在 XenMobile 控制台中配置设置时使用。

请注意，这些要求只是组成 XenMobile 云服务过程的完整通信和端口要求的一部分。 有关详细信息，请参阅 XenMobile 云必备条件和管理。

Android

- 创建 Google Play 凭据。 有关详细信息，请参阅 Google Play Getting Started with Publishing（发布入门）。
- 创建一个 Android for Work 管理员帐户。 有关详细信息，请参阅 Managing Devices with Android for Work in XenMobile（在 XenMobile 中使用 Android for Work 管理设备）。
- 通过 Google 验证您的域名。 有关详细信息，请参阅 Verify your domain for Google Apps（验证您的 Google 应用程序域）。
- 启用 API 并为 Android for Work 创建一个服务帐户。 有关详细信息，请参阅 Google for Work Android。

iOS

- 创建一个 Apple ID 和开发者帐户。 有关详细信息，请参阅 Apple Developer Program（Apple 开发者计划）Web 站点。
- 创建一个 Apple 推送通知服务 (APNs) 证书。 有关详细信息，请参阅 Apple Push Certificates Portal（Apple 推送证书门户）。
- 创建一个 Volume Purchase Program (VPP) 公司令牌。 有关详细信息，请参阅 Apple Volume Purchasing Program。

Windows

- 创建一个 Microsoft Windows Store 开发者帐户。 有关详细信息，请参阅 Microsoft Windows Dev Center（Microsoft Windows 开发中心）。
- 获取一个 Microsoft Windows Store Publisher ID。 有关详细信息，请参阅 Microsoft Windows Dev Center（Microsoft Windows 开发中心）。
- 从 Symantec 获取一个企业证书。 有关详细信息，请参阅 Microsoft Windows Dev Center（Microsoft Windows 开发中心）。
- 创建一个应用程序注册令牌 (AET)。 有关详细信息，请参阅 Microsoft Windows Dev Center（Microsoft Windows 开发中心）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

系统要求

Oct 21, 2016

要运行 XenMobile 10.3，需要满足以下最低系统要求：

- 以下其中一种：
  - XenServer（支持的版本：6.5.x 或 6.2.x）；有关详细信息，请参阅 XenServer
  - VMware（支持的版本：ESXi 5.1、ESXi 5.5 或 ESXi 6.0）；有关详细信息，请参阅 VMware。 注意：ESXi 6.0 仅在 XenMobile 10.3.x 上受支持
  - Hyper-V（支持的版本：Windows Server 2008 R2、Windows Server 2012 或 Windows Server 2012 R2）；有关详细信息，请参阅 Hyper-V
- 双核处理器
- 4 个虚拟 CPU
- 8 GB RAM
- 50 GB 磁盘空间

1 万台或更多设备建议进行如下配置：

- 四核处理器，每个节点 8 GB RAM。

XenMobile 10.3.x 版要求使用 11.12.1 Citrix 许可证服务器或更高版本。

NetScaler Gateway 系统要求

要在 XenMobile 10.3 中运行 NetScaler Gateway，需要满足以下最低系统要求：

- 以下其中一种：
  - XenServer（支持的版本：6.2.x、6.1.x 或 6.0.x）
  - VMWare（支持的版本：ESXi 4.1、ESXi 5.1、ESXi 5.5、ESXi 6.0）
  - Hyper-V（支持的版本：Windows Server 2008 R2、Windows Server 2012 或 Windows Server 2012 R2）
- 两个虚拟 CPU
- 2 GB RAM
- 20 GB 磁盘空间

您还需要与 Active Directory 通信，这需要使用服务帐户。 您只需具有查询和读取权限。

XenMobile 10.3 的数据库要求

XenMobile 需要使用以下数据库之一：

- Microsoft SQL Server

  XenMobile 存储库支持在以下受支持的版本之一上运行的 Microsoft SQL Server 数据库（有关 Microsoft SQL Server 数据库的详细信息，请参阅 Microsoft SQL Server）：

  Microsoft SQL Server 2016
  Microsoft SQL Server 2014
  Microsoft SQL Server 2012
  Microsoft SQL Server 2008 R2
  Microsoft SQL Server 2008

  XenMobile 10.1 支持 SQL Server AlwaysOn 可用性组。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix 建议远程使用 Microsoft SQL。

注意：确保要用于 XenMobile 的 SQL Server 服务帐户具有 DBcreator 角色权限。 有关 SQL Server 服务帐户的详细信息，请参阅 Microsoft Developer Network 站点上的以下页面（这些链接指向有关 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：

Server Configuration - Service Accounts（服务器配置 - 服务帐户）

Configure Windows Service Accounts and Permissions（配置 Windows 服务帐户和权限）

Server-Level 角色

- PostgreSQL

  PostgreSQL 随附在 XenMobile 中。 您可以在本地或远程使用它。

  注意：所有 XenMobile 版本都支持 Remote PostgreSQL 9.3.11 for Windows，但存在以下限制：

  - 最多支持 300 个设备

  对于超出 300 个设备的情况，可使用内部部署的 SQL Server。

  - 不支持群集

StoreFront 兼容性

StoreFront 3.6
StoreFront 3.5
StoreFront 3.0
StoreFront 2.6
Web Interface 5.4
XenApp 和 XenDesktop 7.9
XenApp 和 XenDesktop 7.8
XenApp 和 XenDesktop 7.7
XenApp 和 XenDesktop 7.6
XenApp 和 XenDesktop 7.5
XenApp 6.5

XenMobile 10.3 的邮件服务器要求

XenMobile 10.3 支持以下邮件服务器：

- Exchange 2016
- Exchange 2013
- Exchange 2010

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 兼容性

Aug 11, 2016

有关能够集成的 XenMobile 组件的摘要，请参阅 XenMobile 兼容性。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

支持的设备平台

Aug 11, 2016

可以在 XenMobile 中支持的设备平台中找到 XenMobile 10.x 支持用于企业移动性管理的完整设备列表。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

端口要求

Oct 21, 2016

要使设备和应用程序能够与 XenMobile 通信，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 NetScaler Gateway 和 XenMobile 打开端口以管理应用程序

必须打开下列端口，以允许用户通过 NetScaler Gateway 从 Worx Home、Citrix Receiver 以及 NetScaler Gateway 插件连接到 XenMobile、StoreFront、XenDesktop、XenMobile NetScaler Connector 以及其他内部网络资源，例如 Intranet Web 站点。 有关 NetScaler Gateway 的详细信息，请参阅 NetScaler Gateway 文档中的配置 XenMobile 环境的设置。 有关 NetScaler 拥有的 IP 地址的详细信息，例如 NetScaler IP (NSIP)、虚拟服务器 IP (VIP) 和子网 IP (SNIP) 地址，请参阅 NetScaler 文档中的 NetScaler 如何与客户端和服务器进行通信。

TCP 端口	说明	源	目标
21 或 22	用于将支持包发送到 FTP 或 SCP 服务器。	XenMobile	FTP 或 SCP 服务器
53	用于 DNS 连接。	NetScaler Gateway XenMobile	DNS 服务器
80	NetScaler Gateway 通过第二个防火墙将 VPN 连接传递到内部网络资源。 用户使用 NetScaler Gateway 插件登录时，通常会发生此情况。	NetScaler Gateway	Intranet Web 站点
80 或 8080 443	用于枚举、票据记录和身份验证的 XML 和 Secure Ticket Authority (STA) 端口。 Citrix 建议使用端口 443。	StoreFront 和 Web Interface XML 网络流量 NetScaler Gateway STA	XenDesktop 或 XenApp
123	用于网络时间协议 (NTP) 服务。	NetScaler Gateway	NTP 服务器
389	用于非安全 LDAP 连接。	NetScaler Gateway XenMobile	LDAP 身份验证服务器或 Microsoft Active Directory
443	用于从 Citrix Receiver 连接到 StoreFront 或从	Internet	NetScaler Gateway

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Receiver for Web 连接到 XenApp 和 XenDesktop。		
	用于连接到 XenMobile 以实现 Web、移动和 SaaS 应用程序交付。	Internet	NetScaler Gateway
	用于与 XenMobile 服务器的一般设备通信	XenMobile	XenMobile
	注册时用于从移动设备到 XenMobile 的连接。	Internet	XenMobile
	用于从 XenMobile 到 XenMobile NetScaler Connector 的连接。	XenMobile	XenMobile NetScaler Connector
	用于从 XenMobile NetScaler Connector 到 XenMobile 的连接。	XenMobile NetScaler Connector	XenMobile
	用于在未进行证书身份验证的部署中的回调 URL。	XenMobile	NetScaler Gateway
514	用于 XenMobile 与 Syslog 服务器之间的连接。	XenMobile	Syslog 服务器
636	用于安全 LDAP 连接。	NetScaler Gateway XenMobile	LDAP 身份验证服务器或 Active Directory
1494	用于与内部网络中基于 Windows 应用程序的 ICA 连接。 Citrix 建议保持此端口处于打开状态。	NetScaler Gateway	XenApp 或 XenDesktop
1812	用于 RADIUS 连接。	NetScaler Gateway	RADIUS 身份验证服务器
2598	用于使用会话可靠性连接到内部网络中基于 Windows 的应用程序。 Citrix 建议保持此端口处于打开状态。	NetScaler Gateway	XenApp 或 XenDesktop
3268	用于 Microsoft Global Catalog 非安全 LDAP 连接。	NetScaler Gateway XenMobile	LDAP 身份验证服务器或 Active Directory
3269	用于 Microsoft Global Catalog 安全 LDAP 连接。	NetScaler Gateway XenMobile	LDAP 身份验证服务器或 Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

9080	用于 NetScaler 和 XenMobile NetScaler Connector 之间的 HTTP 流量。	NetScaler	XenMobile NetScaler Connector
9443	用于 NetScaler 和 XenMobile NetScaler Connector 之间的 HTTPS 流量。	NetScaler	XenMobile NetScaler Connector
45000 80	用于部署在群集中的两个 XenMobile VM 之间的通信。	XenMobile	XenMobile
8443	用于注册、XenMobile Store 和移动应用程序管理 (MAM)。	XenMobile NetScaler Gateway 设备 Internet	XenMobile
4443	用于管理员通过浏览器访问 XenMobile 控制台。	访问点（浏览器）	XenMobile
	用于从一个节点为所有 XenMobile 群集节点下载日志和支持捆绑包。	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

必须打开以下端口以允许 XenMobile 在网络中通信。

TCP 端口	**说明**	**源**	**目标**
25	用于 XenMobile 通知服务的 SMTP 端口。 如果 SMTP 服务器使用其他端口，请确保防火墙不会阻止该端口。	XenMobile	SMTP 服务器
80 和 443	与 Apple iTunes App Store (ax.itunes.apple.com)、Google Play（必须使用 80）或 Windows Phone 应用商店建立的企业应	XenMobile	Apple iTunes App Store（ax.itunes.apple.com 和 *.mzstatic.com）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	用商店连接。 用于通过 iOS 上的 Citrix Mobile Self-Serve、适用于 Android 的 Worx Home 或适用于 Windows Phone 的 Worx Home 从应用商店推送应用程序。		Apple Volume Purchase Program (vpp.itunes.apple.com) 对于 Windows Phone：login.live.com 和 *.notify.windows.com Google Play (play.google.com)
80 或 443	用于 XenMobile 与 Nexmo SMS Notification Relay 之间的出站连接。	XenMobile	Nexmo SMS Relay 服务器
389	用于非安全 LDAP 连接。	XenMobile	LDAP 身份验证服务器或 Active Directory
443	用于 Android 和 Windows Mobile 的注册和代理安装。	Internet	XenMobile
	用于 Android 和 Windows 设备、XenMobile Web 控制台和 MDM 远程支持客户端的注册和代理安装。	内部 LAN 和 WiFi	
1433	默认用于与远程数据库服务器的连接（可选）。	XenMobile	SQL Server
2195	用于 Apple 推送通知服务 (APNs) 到 gateway.push.apple.com 的出站连接，适用于 iOS 设备通知和设备策略推送。	XenMobile	Internet（使用公用 IP 地址 17.0.0.0/8 的 APNs 主机）
2196	用于到 feedback.push.apple.com 的 APNs 出站连接，适用于 iOS 设备通知和设备策略推送。		
5223	用于从 Wi-Fi 网络上的 iOS 设备到 *.push.apple.com 的 APNs 出站连接。	WiFi 网络上的 iOS 设备	Internet（使用公用 IP 地址 17.0.0.0/8 的 APNs 主机）
8081	用于来自可选 MDM 远程支持客户端的应用程序通道。 默认为 8081。	远程支持客户端	Internet，针对用户设备的应用程序通道（仅适用于 Android 和 Windows）
8443	用于 iOS 和 Windows Phone 设备注册。	Internet LAN 和 WiFi	XenMobile

© 1999-2017 Citrix Systems, Inc. All rights reserved.

此端口配置可确保从 Worx Home for Android 10.2 和 10.3 连接的 Android 设备能够从内部网络访问 Citrix Auto Discovery Service (ADS)。 下载通过 ADS 提供的任何安全更新时能够访问 ADS 非常重要。

注意：ADS 连接可能不适用于您的代理服务器。 在这种情况下，允许 ADS 连接绕过代理服务器。

对启用证书固定功能感兴趣的客户必须完成以下必需操作：

- **收集 XenMobile 服务器和 NetScaler 证书**。 证书的格式必须为 PEM，并且必须是公用证书，而非私钥。
- **联系 Citrix 技术支持并请求启用证书固定功能**。 在此过程中，系统会要求您提供证书。

新的证书固定改进功能要求设备先连接到 ADS， 然后再注册。 这样可确保最新的安全信息对正在其中注册设备的环境中的 Worx Home 可用。 Worx Home 不注册无法访问 ADS 的设备。 因此，在内部网络中打开 ADS 访问功能对启用设备注册非常重要。

要允许访问 Worx Home 10.2 for Android 的 ADS，请为以下 FQDN 和 IP 地址打开端口 443：

FQDN	IP 地址
discovery.mdm.zenprise.com	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
	184.72.219.144
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

© 1999-2017 Citrix Systems, Inc. All rights reserved.

FIPS 140-2 合规性

Aug 11, 2016

美国国家标准和技术研究所 (US National Institute of Standards and Technologies, NIST) 发布的联邦信息处理标准 (Federal Information Processing Standard, FIPS) 指定了安全系统中使用的加密模块的安全要求。 FIPS 140-2 是此标准的第二版。 有关 NIST 认证的 FIPS 140 模块的详细信息，请参阅 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf。

重要：只可以在初始安装时启用 XenMobile FIPS 模式。
注意：只要未使用任何 HDX 应用程序，XenMobile 仅移动设备管理、XenMobile 仅移动应用程序管理和 XenMobile Enterprise 均与 FIPS 兼容。
在 iOS 上执行的所有静态数据 (data-at-rest) 和传输中数据 (data-in-transit) 加密操作使用 OpenSSL 和 Apple 提供的 FIPS 认证加密模块。 在 Android 上，从移动设备到 NetScaler Gateway 的所有静态数据加密操作和所有传输中数据加密操作使用 OpenSSL 提供的 FIPS 认证加密模块。

Windows RT、Microsoft Surface、Windows 8 Pro 和 Windows Phone 8 上 Mobile Device Management (MDM) 的所有静态数据和传输中数据加密操作使用 Microsoft 提供的 FIPS 认证加密模块。

XenMobile Device Manager 上的所有静态数据和传输中数据加密操作使用 OpenSSL 提供的 FIPS 认证加密模块。 与上面介绍的移动设备加密操作以及移动设备与 NetScaler Gateway 之间的加密操作结合时，MDM 流的所有静态数据和传输中数据在端到端传输时使用 FIPS 合规加密模块。

iOS、Android 和 Windows 移动设备与 NetScaler Gateway 之间的所有传输中数据加密操作使用 FIPS 认证加密模块。 XenMobile 使用配备了认证 FIPS 模块的 DMZ 托管 NetScaler FIPS Edition 设备来确保这些数据的安全。 有关详细信息，请参阅 NetScaler FIPS 文档。

MDX 应用程序在 Windows Phone 8.1 上受支持，在 Windows Phone 8 上使用 FIPS 兼容的加密库和 API。 Windows Phone 8.1 上 MDX 应用程序的所有静态数据和 Windows Phone 8.1 设备与 NetScaler Gateway 的所有传输中数据使用这些库和 API 进行加密。

MDX Vault 使用 OpenSSL 提供的 FIPS 认证加密模块加密 iOS 和 Android 设备上 MDX 打包的应用程序以及关联静态数据。

有关完整的 XenMobile FIPS 140-2 合规声明（包括在每种情况下使用的特定模块），请与 Citrix 代表联系。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 语言支持

Oct 21, 2016

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

X 表示应用程序可提供相应语言版本。 Secure Forms 当前只提供英文版本。

iOS						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
日语	X	X	X	X	X	X
简体中文	X	X	X	X	X	X
繁体中文	X	X	X	X	X	X
法语	X	X	X	X	X	X
德语	X	X	X	X	X	X
西班牙语	X	X	X	X	X	X
韩语	X	X	X	X	X	X
葡萄牙语	X	X	X	X	X	X
荷兰语	X	X	X	X	X	X
意大利语	X	X	X	X	X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

丹麦语	X	X	X	X	X	X
瑞典语	X	X	X	X	X	X
希伯来语	X	X	X	X	X	X
阿拉伯语	X	X	X	X	X	X

Android						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
日语	X	X	X	X	X	X
简体中文	X	X	X	X	X	X
繁体中文	X	X	X	X	X	
法语	X	X	X	X	X	X
德语	X	X	X	X	X	X
西班牙语	X	X	X	X	X	X
韩语	X	X	X	X	X	X
葡萄牙语	X	X	X	X	X	X
荷兰语	X	X	X	X	X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

意大利语	X	X	X	X	X	X
丹麦语	X	X	X	X	X	X
瑞典语	X	X	X	X	X	X
希伯来语	X	X	X	X	X	
阿拉伯语	X	X	X	X	X	

Windows			
	Worx Home	**WorxMail**	**WorxWeb**
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

有关 Citrix 产品的完整全球化状态，请参阅 Citrix 知识中心。

XenMobile 控制台提供简体中文、德语、法语、韩语及葡萄牙语版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

下表概述了每个应用程序对中东语言文本的支持情况。 **X** 指示此功能是否对该平台可用。

App	iOS	Android	Windows Phone
Worx Home	X	X	
WorxMail	X	X	
WorxWeb	X	X	
WorxTasks	X	X	
WorxNotes	X	X	
QuickEdit	X	X	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

预安装核对表

Aug 11, 2016

可以使用此核对表记录安装 XenMobile 的必备条件和设置。 每项任务或记录都包含一列，指明适用此要求的组件或功能。 有关安装步骤，请参阅安装 XenMobile。

以下是 XenMobile 解决方案需要的网络设置。

	必备条件或设置	组件或功能	记录设置
	记录远程用户连接到的完全限定的域名 (FQDN)。	XenMobile NetScaler Gateway	
	记录公用和本地 IP 地址。 您需要这些 IP 地址来配置防火墙以设置网络地址转换 (NAT)。	XenMobile NetScaler Gateway	
	记录子网掩码。	XenMobile NetScaler Gateway	
	记录 DNS IP 地址。	XenMobile NetScaler Gateway	
	记下 WINS 服务器 IP 地址（如果适用）。	NetScaler Gateway	
	识别并记下 NetScaler Gateway 主机名。 注意：此项不是 FQDN。 FQDN 位于绑定到用户所连接的虚拟服务器的已签名服务器证书中。 您可以使用 NetScaler Gateway 中的安装向导来配置主机名。	NetScaler Gateway	
	记录 XenMobile 的 IP 地址。 如果安装一个 XenMobile 实例，请保留一个 IP 地址。 配置群集时，请记录需要的所有 IP 地址。	XenMobile	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	必备条件或设置	组件或功能	记录设置
	• NetScaler Gateway 上配置的一个公用 IP 地址 • NetScaler Gateway 的一个外部 DNS 条目	NetScaler Gateway	
	记录 Web 代理服务器的 IP 地址、端口、代理主机列表，以及管理员用户名和密码。 如果您在网络中部署代理服务器，这些设置是可选的（如果适用）。 注意： 配置 Web 代理的用户名时，可以使用 sAMAccountName 或用户主体名称 (UPN)。	XenMobile NetScaler Gateway	
	记录默认网关 IP 地址。	XenMobile NetScaler Gateway	
	记录系统 IP (NSIP) 地址和子网掩码。	NetScaler Gateway	
	记录子系统 IP (SNIP) 地址和子网掩码。	NetScaler Gateway	
	记录证书中的 NetScaler Gateway 虚拟服务器 IP 地址和 FQDN。 如果需要配置多个虚拟服务器，则记录证书中的所有虚拟 IP 地址和 FQDN。	NetScaler Gateway	
	记录用户可经由 NetScaler Gateway 访问的内部网络。 例如：10.10.0.0/24 输入用户通过 Worx Home 或 NetScaler Gateway 插件进行连接时需要访问的所有内部网络和网段（拆分通道设置为开时）。	NetScaler Gateway	
	确保 XenMobile 服务器、NetScaler Gateway、外部 Microsoft SQL Server 与 DNS 服务器之间的网络连接良好。	XenMobile NetScaler Gateway	

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

	必备项	组件	记录位置
	从 Citrix Web 站点获取通用许可证。 有关详细信息，请参阅 NetScaler Gateway 许可证。	NetScaler Gateway	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	必备项	组件	记录位置
		XenMobile Citrix 许可证服务器	

XenMobile 和 NetScaler Gateway 需要使用证书来启用用户设备与其他 Citrix 产品和应用程序的连接。 有关详细信息，请参阅 XenMobile 中的证书。

	必备项	组件	备注
	获取并安装必需证书。	XenMobile NetScaler Gateway	

您需要打开端口，以允许与 XenMobile 组件进行通信。 有关需要打开的端口的完整列表，请参阅 XenMobile 端口要求。

	必备项	组件	备注
	打开用于 XenMobile 的端口	XenMobile NetScaler Gateway	

需要配置数据库连接。 XenMobile 存储库要求 Microsoft SQL Server 数据库在以下支持版本之一上运行：Microsoft SQL Server 2014、SQL Server 2012、SQL Server 2008 R2 或 SQL Server 2008。 Citrix 建议远程使用 Microsoft SQL。 PostgreSQL 包含在 XenMobile 中，并且应仅在测试环境中本地或远程使用。

	必备项	组件	记录设置
	Microsoft SQL Server IP 地址和端口。 确保要用于 XenMobile 的 SQL Server 服务帐户具有 DBcreator 角色权限。	XenMobile	

	必备项	组件	记录设置
	记录主服务器和辅助服务器的 Active Directory IP 地址和端口。 如果使用端口 636，请在 XenMobile 上安装 CA 的根证书，并将使用安全连接选项设置	XenMobile NetScaler	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	必备项	组件	记录设置
	为是	Gateway	
	记录 Active Directory 域名。	XenMobile NetScaler Gateway	
	记录 Active Directory 服务帐户，该帐户需要用户 ID、密码和域别名。 Active Directory 服务帐户是 XenMobile 用来查询 Active Directory 的帐户。	XenMobile NetScaler Gateway	
	记录用户基础 DN。 此为用户所在的目录级别；例如，cn=users, dc=ace, dc=com。 NetScaler Gateway 和 XenMobile 使用它来查询 Active Directory。	XenMobile NetScaler Gateway	
	记录组基础 DN。 此为组所在的目录级别。 NetScaler Gateway 和 XenMobile 使用它来查询 Active Directory。	XenMobile NetScaler Gateway	

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

Citrix 建议在 NetScaler 中使用快速配置向导来配置 XenMobile 与 NetScaler Gateway 之间以及 XenMobile 与 Worx Home 之间的连接设置。 创建第二个虚拟服务器，使用户能够从 Receiver 和 Web 浏览器连接到 XenApp 和 XenDesktop 中基于 Windows 的应用程序和虚拟桌面。 Citrix 建议您在 NetScaler Gateway 中也使用快速配置向导来配置这些设置。

	必备项	组件	记录设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

必备项		组件	记录设置
✓	记录 NetScaler Gateway 主机名和外部 URL。 外部 URL 是用户用来进行连接的 Web 地址。	XenMobile	
	记录 NetScaler Gateway 回调 URL。	XenMobile	
	记录虚拟服务器的 IP 地址和子网掩码。	NetScaler Gateway	
	记录 Program Neighborhood Agent 或 XenApp Services 站点的路径。	NetScaler Gateway XenMobile	
	记录运行 Secure Ticket Authority (STA) 的 XenApp 或 XenDesktop 服务器的 FQDN 或 IP 地址（仅限 ICA 连接）。	NetScaler Gateway	
	记录 XenMobile 的公共 FQDN。	NetScaler Gateway	
	记录 Worx Home 的公共 FQDN。	NetScaler Gateway	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装 XenMobile

Oct 21, 2016

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

开始之前的准备工作：规划 XenMobile 部署需要注意多个事项。 有关您的端到端 XenMobile 环境的建议、常见问题和用例，请参阅《XenMobile 部署手册》。 此外，还请参阅 XenMobile 10.3 的系统要求和 XenMobile 安装前核对清单。

> **注意**
>
> 确保使用正确的时间配置虚拟机管理程序（使用 NTP 服务器或手动配置），因为 XenMobile 会使用该时间。

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

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

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

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

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

由于有两个不同版本的 Hyper-V 清单文件可以表示 VM 配置 (.exp and .xml)，因此这些步骤十分必要。 Windows Server 2008 R2 和 Windows Server 2012 版本仅支持 .exp。 对于这些版本，您在安装前必须只具有 .exp 清单文件。

Windows Server 2012 R2 不要求执行这些额外步骤。

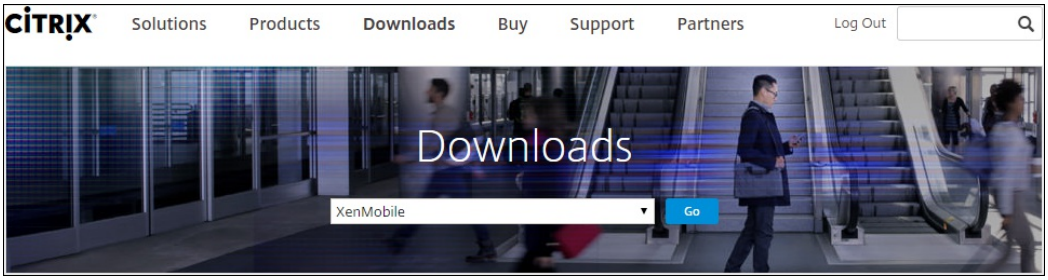
FIPS 140-2 模式：如果您打算在 FIPS 模式下安装 XenMobile 服务器，则需要完成一组必备条件，如 Configuring FIPs with XenMobile（在 XenMobile 中配置 FIPs）中所述。

可以从 Citrix Web 站点下载产品软件。 您需要首先登录站点，然后使用 Citrix Web 页面上的下载链接，导航到包含要下载的软件的页面。

下载 XenMobile 的软件

1. 转至 Citrix Web 站点。
2. 在“搜索”框旁边，单击登录以登录您的帐户。
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 XenMobile。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 单击转到。 此时将显示 XenMobile 页面。
6. 展开 XenMobile 10。
7. 单击 XenMobile 10.0 Server。
8. 在 XenMobile 10.0 Server 版本页面上，单击用于在 XenServer、VMware 或 Hyper-V 上安装 XenMobile 的相应虚拟映像旁边的下载。
9. 按照屏幕上的说明下载软件。

下载 NetScaler Gateway 的软件

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

1. 转至 Citrix Web 站点。
2. 如果尚未登录 Citrix Web 站点，在“搜索”框旁边，单击登录以登录您的帐户。
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 NetScaler Gateway。
5. 单击转到。 此时将显示 NetScaler Gateway 页面。
6. 在 NetScaler Gateway 页面上，展开您所使用的 NetScaler Gateway 版本。
7. 在固件下面，单击要下载的设备软件版本。
   注意：还可以单击 Virtual Appliances（虚拟设备）以下载 NetScaler VPX。 选择此选项时，将显示适用于每个虚拟机管理程序所对应的虚拟机的软件列表。
8. 单击要下载的设备软件版本。
9. 在要下载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。

为首次使用配置 XenMobile 的过程包括两个部分。

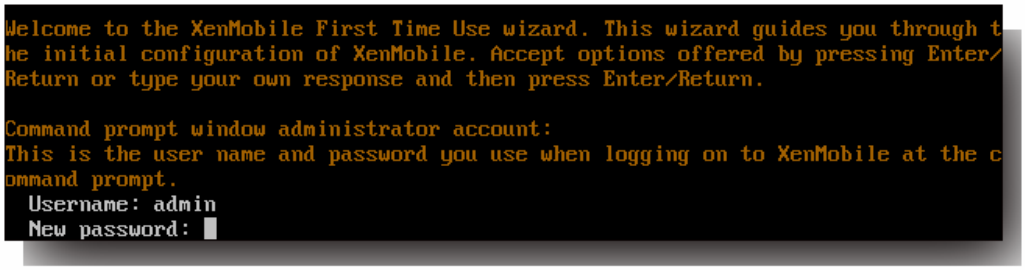
1. 通过使用 XenCenter 或 vSphere 命令行控制台，配置 XenMobile 的 IP 地址和子网掩码、默认网关、DNS 服务器等
2. 登录 XenMobile 管理控制台并按照初始登录屏幕上的步骤操作

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

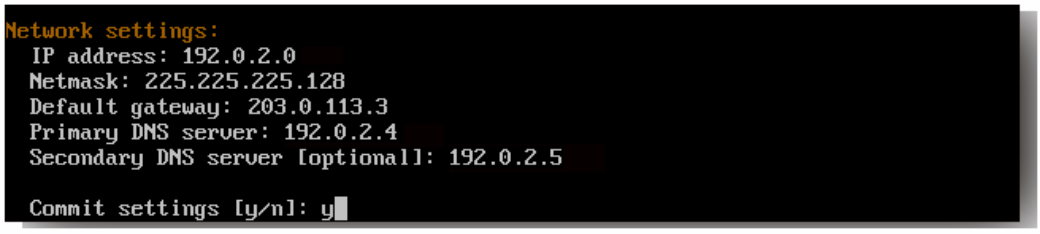
在命令提示窗口中配置 XenMobile

1. 将 XenMobile 虚拟机导入 Citrix XenServer、Microsoft Hyper-V 或 VMware ESXi。 有关详细信息，请参阅 XenServer、Hyper-V 或 VMware 文档。
2. 在虚拟机管理程序中，选择导入的 XenMobile 虚拟机并启动命令提示窗口视图。 有关详细信息，请参阅您的虚拟机管理程序的文档。
3. 从虚拟机管理程序的控制台页面，通过在命令提示窗口中键入管理员用户名和密码，为 XenMobile 创建管理员帐户。
   重要：
   创建或更改命令提示窗口管理员帐户、公钥基础结构 (PKI) 服务器证书和 FIPS 的密码时，XenMobile 针对除 Active Directory 用户（其密码在 XenMobile 外部管理）之外的所有用户强制执行以下规则：
   - 密码的长度至少为 8 个字符，并且必须至少满足以下复杂条件中的三项：
     - 大写字母（A 至 Z）
     - 小写字母（a 至 z）
     - 数字（0 至 9）
     - 特殊字符（如 !、#、$、%）

   注意：键入新密码时，不会显示字符，如星号。 不会显示任何内容。

4. 提供以下网络信息，然后键入y 以提交设置：
   1. IP 地址
   2. 网络掩码
   3. 默认网关
   4. 主 DNS 服务器
   5. 辅助 DNS 服务器（可选）

   注意：本图片和后面的图片中显示的地址并不可用，仅作为示例提供。

5. 类型y 可通过生成随机的加密密码增加安全性，或者键入n 提供主机的密码。 Citrix 建议键入y 以生成随机密码。 密码是加密密钥（用于保护敏感数据）保护措施的一部分。 密码哈希存储在服务器文件系统中，用于在加密数据和解密数据过程中提取密钥。 无法查看密码。

   注意：如果打算扩展您的环境并配置其他服务器，则应提供自己的密码。 如果选择随机密码，将无法查看密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Encryption passphrase:
  Generate a random passphrase to secure the server data? [y/n]: y
```

6. （可选）启用美国联邦信息处理标准 (FIPS)。 有关 FIPS 的详细信息，请参阅 XenMobile FIPS 140-2 合规性。 此外，请务必完成一组必备条件，如 Configuring FIPs with XenMobile（在 XenMobile 中配置 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: 198.0.2.10
  Port: 5432
  Username: postgres
  Password:
```

   1. 数据库可以是本地数据库或远程数据库。 类型l （本地）或r （远程）。
   2. 选择数据库类型。 类型mi （用于 Microsoft SQL）或键入p （用于 PostgreSQL）。
      重要：
      - Citrix 建议远程使用 Microsoft SQL。 PostgreSQL 包含在 XenMobile 中，并且应仅在测试环境中本地或远程使用。
      - 不支持数据库迁移。 在测试环境下创建的数据库不能移动到生产环境中。
   3. 可选，键入y 可为数据库使用 SSL 身份验证。
   4. 提供托管 XenMobile 的服务器的完全限定的域名 (FQDN)。 此单个主机服务器同时提供设备管理服务和应用程序管理服务。
   5. 如果数据库端口号不同于默认端口号，请键入您的数据库端口号。 Microsoft SQL 的默认端口为 1433，PostgreSQL 的默认端口为 5432。
   6. 键入数据库管理员用户名。
   7. 键入您的数据库管理员密码。
   8. 键入数据库名称。
   9. 按 Enter 提交数据库设置。
8. 可选，键入y 以启用群集 XenMobile 节点或实例。
   重要：如果启用 XenMobile 群集，完成系统配置后，请确保打开端口 80，以便在群集成员之间启用实时通信。 必须在所有群集节点上完成此操作。
9. 键入 XenMobile 服务器完全限定的域名 (FQDN)。

```
XenMobile hostname:
  Hostname: justan.example.com
```

10. 按 Enter 提交设置。
11. 识别通信端口。 有关端口及其用法的详细信息，请参阅 XenMobile 端口要求。
    注意：通过按 Enter（在 Mac 上为 Return）接受默认端口。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

12. 由于您是首次安装 XenMobile，请跳过下一个关于从之前的 XenMobile 版本进行升级的问题。
13. 类型y 。 有关 XenMobile PKI 功能的详细信息，请参阅在 XenMobile 中上载证书。

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

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

14. 键入新密码，然后重新输入新密码以提交。
    注意：键入新密码时，不会显示字符，如星号。 不会显示任何内容。

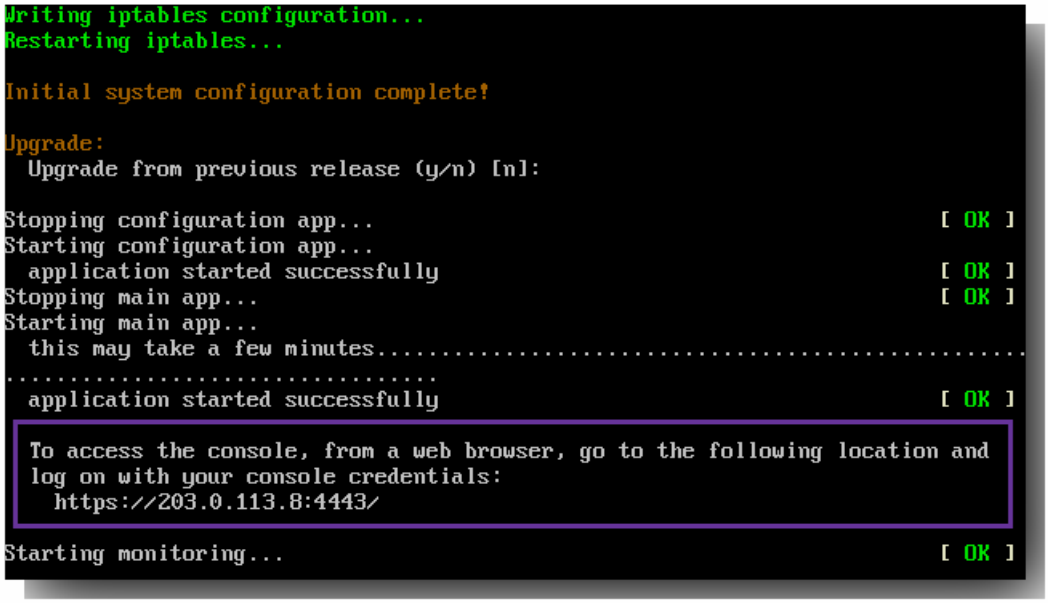
15. 按 Enter 提交设置。
16. 创建管理员帐户以便使用 Web 浏览器登录 XenMobile 控制台。 请务必记住这些凭据，供稍后使用。

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

注意：键入新密码时，不会显示字符，如星号。 不会显示任何内容。

17. 按 Enter 提交设置。 此时已保存初始系统配置。
18. 当询问是否为升级时，请键入n ，因为这是全新安装。
19. 完整复制屏幕上显示的 URL，并在 Web 浏览器中继续此初始 XenMobile 配置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在 Web 浏览器中配置 XenMobile

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

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

3. 在“入门”页面中，单击开始。 此时将显示“Licensing”（许可）页面。
4. 配置许可证。 XenMobile 附带的是评估版许可证，有效期为 30 天。 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 XenMobile 许可。
   重要：如果打算通过添加 XenMobile 的群集节点或实例来使用 XenMobile 群集，需要在远程服务器上使用 Citrix Licensing。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. 在证书页面上，单击导入。 此时将显示导入对话框。
6. 导入您的 APNs 和 SSL 侦听器证书。 有关使用证书的详细信息，请参阅 XenMobile 中的证书。
   注意：此步骤需要重新启动服务器。
7. 如果适用于环境，请配置 NetScaler Gateway。 有关配置 NetScaler 网关的详细信息，请参阅 NetScaler Gateway 和 XenMobile 以及为 XenMobile 环境配置设置。
   注意：
   - 可以将 NetScaler Gateway 部署在组织内部网络（或 Intranet）的外围，以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，所有远程用户必须先连接到 NetScaler Gateway，才能访问内部网络中的任何资源。
   - 尽管 NetScaler Gateway 为可选设置，但在页面上输入数据后，必须清除或完成必填字段，才能离开页面。
8. 完成 LDAP 配置，以便从 Active Directory 访问用户和组。 有关配置 LDAP 连接的详细信息，请参阅 LDAP 配置。
9. 配置能够向用户发送消息的通知服务器。 有关通知服务器配置的详细信息，请参阅 XenMobile 中的通知。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中配置 FIPS

Aug 11, 2016

XenMobile 中的联邦信息处理标准 (Federal Information Processing Standards, FIPS) 模式 通过将服务器配置为仅对所有加密操作使用通过 FIPS 140-2 认证的库来支持美国联邦政府客户。 在 FIPS 模式下安装 XenMobile 服务器可确保 XenMobile 客户端与服务器的未使用的所有数据以及传输中的数据完全遵从 FIPS 140-2。

在 FIPS 模式下安装 XenMobile 服务器之前，需要完成以下必备条件。

- 必须对 XenMobile 数据库使用外部 SQL Server 2012 或 SQL Server 2014。 还必须配置 SQL Server 以实现安全 SSL 通信。 有关配置与 SQL Server 的安全 SSL 通信的说明，请参阅 SQL Server 联机丛书。
- 安全 SSL 通信要求在 SQL Server 上安装 SSL 证书。 SSL 证书可以是来自商业 CA 的公用证书或来自内部 CA 的自签名证书。 请注意，SQL Server 2014 无法接受通配符证书。 因此，Citrix 建议您通过 SQL Server 的 FQDN 请求 SSL 证书。
- 如果使用 SQL Server 的自签名证书，则需要颁发了您的自签名证书的根 CA 证书的副本。 必须在安装过程中将根 CA 证书导入到 XenMobile 服务器中。

可以在 XenMobile 服务器的初始安装过程中启用 FIPS 模式。 安装完成后则无法启用 FIPS。 因此，如果您打算使用 FIPS 模式，则必须在开始时在 FIPS 模式下安装 XenMobile 服务器。 此外，如果您有 XenMobile 群集，则所有群集节点都必须启用 FIPS；不能在同一个群集中同时包含 FIPS 和非 FIPS XenMobile 服务器。

XenMobile 命令行界面中存在一个不供生产使用的 **Toggle FIPS mode**（切换 FIPS 模式）选项。 此选项专用于非生产诊断，在生产型 XenMobile 服务器上不受支持。

1. 初始安装过程中，启用 **FIPS mode**（FIPS 模式）。

2. 上载 SQL Server 的根 CA 证书。 如果在 SQL Server 上使用自签名 SSL 证书而非公用证书，请为此选项选择 **Yes**（是），然后执行以下操作之一：

    a. 复制并粘贴 CA 证书。

    b. 导入 CA 证书。 要导入 CA 证书，必须将该证书发布到可通过 HTTP URL 从 XenMobile 服务器访问的 Web 站点。 有关详细信息，请参阅本文后面的导入证书部分。

3. 指定 SQL Server 的服务器名称和端口，用于登录 SQL Server 的凭据以及要为 XenMobile 创建的数据库名称。

注意：可以使用 SQL 登录凭据或 Active Directory 帐户访问 SQL Server，但该登录凭据必须具有 DBcreator 角色。

4. 要使用 Active Directory 帐户，请以“域\用户名”格式输入凭据。

5. 这些步骤完成后，请继续执行 XenMobile 初始安装。

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

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SQL 必备条件

1. 从 XenMobile 到 SQL 实例的连接必须安全，且必须是 SQL Server 2012 或 SQL Server 2014。 要确保连接安全，请参阅 How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console（如何使用 Microsoft 管理控制台为 SQL Server 的实例启用 SSL 加密）。

2. 如果该服务未正确重新启动，请检查以下项：打开 **Services.msc**。

    a. 复制用于 SQL Server 服务的登录帐户信息。

    b. 在 SQL Server 上打开 MMC.exe。

    c. 转至**文件** > **添加/删除管理单元**，然后双击证书项以添加证书管理单元。 在向导中的两个页面上选择计算机帐户和本地计算机。

    d. 单击 **OK**（确定）。

    e. 展开**证书(本地计算机)** > **个人** > **证书**，找到导入的 SSL 证书。

    f. 右键单击导入的证书（在 SQL Server 配置管理器中进行选择），然后单击**所有任务** > **管理私钥**。

    g. 在**组或用户名**下，单击**添加**。

    h. 输入在之前的步骤中复制的 SQL 服务帐户名称。

    i. 取消选中**允许完全控制**选项。 默认情况下，该服务帐户将被同时授予完全控制和读取权限，但只需要能够读取私钥。

    j. 关闭 **MMC** 并启动 SQL 服务。

3. 确保 SQL 服务已正确启动。

Internet Information Services (IIS) 必备条件

1. 下载 rootcert (base 64)。

2. 将 rootcert 复制到 IIS 服务器上的默认站点 C:\inetpub\wwwroot。

3. 选中默认站点的**身份验证**复选框。

4. 将**匿名**设置为**已启用**。

5. 选中**失败请求跟踪**规则复选框。

6. 确保 .cer 不被阻止。

7. 在 Internt Explorer 浏览器中从本地服务器浏览到 .cer 所在的位置 http://localhost/certname.cer。 根证书文本应在浏览器中显示。

8. 如果根证书不在 Internet Explorer 浏览器中显示，请务必按如下所示在 IIS 服务器上启用 ASP。

    a. 打开服务器管理器。

    b. 在**管理** > **添加角色和功能**中导航到向导。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

c. 在服务器角色中，依次展开 **Web 服务器(IIS)**、**Web 服务器**和**应用程序开发**，然后选择 **ASP**。

d. 安装完成后，单击**下一步**。

9. 打开 Internet Explorer 并浏览到 http://localhost/cert.cer。

有关详细信息，请参阅 Internet Information Services (IIS) 8.5。

> **注意**
>
> 可以为此过程使用 CA 的 IIS 实例。

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

- 启用 FIPS：是
- 上载根证书：是
- 复制 (c) 或导入 (i)：i
- 输入 HTTP URL 以导入：http://*IIS 服务器的 FQDN*/cert.cer
- 服务器：*SQL Server 的 FQDN*
- 端口：1433
- 用户名：能够创建数据库的服务帐户（域\用户名）。
- 密码：服务帐户的密码。
- 数据库名称：这是您选择的名称。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

升级 XenMobile

Oct 21, 2016

当有 XenMobile 的新版本或重要更新可用时，我们会将其会发布到 Citrix.com 上，并向每个客户的在案联系人发送通知。 有三个用于升级 XenMobile 的主要选项，具体取决于您当前正在使用的版本：

- **从 XenMobile 9.0 进行升级** - MDM Edition、App Edition 和 Enterprise Edition
  必须先使用升级工具升级到 XenMobile 10.1。 可以从 Citrix.com 下载页面下载该工具。 有关使用升级工具的详细信息，请参阅升级 XenMobile。

  从 XenMobile 9 升级到 XenMobile 10.1，然后安装 XenMobile 10.3.x 的更新时，借助最新版本的升级工具，您现在可以迁移以下设备类型的数据：

  Windows CE
  Windows 10 Phone
  Windows 10 Tablet

  在当前版本的升级工具中，如果在 XenMobile 9.0 上启用了多租户控制台 (MTC)，则可以将 MTC 托管的 XenMobile 9 实例迁移到独立的 XenMobile 10 实例。 XenMobile 10 不支持 MTC，因此，必须基于各个实例管理这些升级后的实例。 有关详细信息，请参阅将 MTC 租户服务器升级到 XenMobile 10.1。

- **从 XenMobile 10.1 升级到 XenMobile 10.3.x**
  按本文中的内容所述，使用 XenMobile 控制台中的**版本管理**页面。 请勿使用升级工具安装 XenMobile 10.3.x。

- **安装 XenMobile 10.3.x 软件、Service Pack 和系统修补程序的新版本**
  按本文中的内容所述，使用 XenMobile 控制台中的**版本管理**页面。

Important

- 从 XenMobile 10.1 更新到版本 10.3.x 时，如果 WorxStore 具有自定义名称，则必须先将应用商店名称更改为**应用商店**的默认设置，并在设备上部署这些设置，然后进行更新。 如果未执行上述操作，自定义应用商店名称会导致 XenMobile 10.3 注册、访问 Worx Home 和 WorxStore 以及在 iOS 设备上部署应用程序出现问题。 有关配置 WorxStore 外观方案的详细信息，请参阅为 iOS 设备创建自定义 WorxStore 外观方案。
- 升级到 XenMobile 10.3.x 后，如果在 XenMobile 10.3.x 中更新先前在早期版本中配置的 Worx 移动应用程序，则该应用程序的设置将不再显示在 XenMobile 控制台中。 您需要重新编辑并配置这些应用程序的设置。 不需要重新安装这些应用程序。 此步骤只需执行一次；如果您将来更新应用程序或服务器，这些值将不受影响。

XenMobile 服务器版本	版本号	升级到	版本号	升级路径	位置
具有 App Controller Patch 5 的 XenMobile 服务器 9	9.0.0.97582	XenMobile 服务器 10.1	10.1.0.63030	XenMobile 服务器 9 到 XenMobile 服务器 10.1	下载（App Controller Patch 5 或 Upgrade Tool）
XenMobile 服务器 10 或 10.1	10.1.0.63030	XenMobile 服务器 10.3	10.3.0.824	XenMobile 服务器 10 或 10.1 升级到 10.3	下载
XenMobile 服务器 10.3	10.3.0.10004、10.3.0.10008、10.3.0.10010、10.3.0.10014、10.3.0.10016、10.3.0.10032、10.3.0.10036	XenMobile 服务器 10.3 Rollup Patch 3	10.3.0.10048	XenMobile 服务器 10.3 升级到 10.3 Rolling Patch 3	下载
XenMobile 服务器 10.3	10.3.0.x	XenMobile 服务器 10.3.5	10.3.5.354	XenMobile 服务器 10.3 升级到 10.3.5	下载
XenMobile 服务器 10.3.5	10.3.5.354	XenMobile 服务器 10.3.6 (Service Pack)	10.3.6.310	XenMobile 服务器 10.3.5 升级到 10.3.6	下载

必备条件：

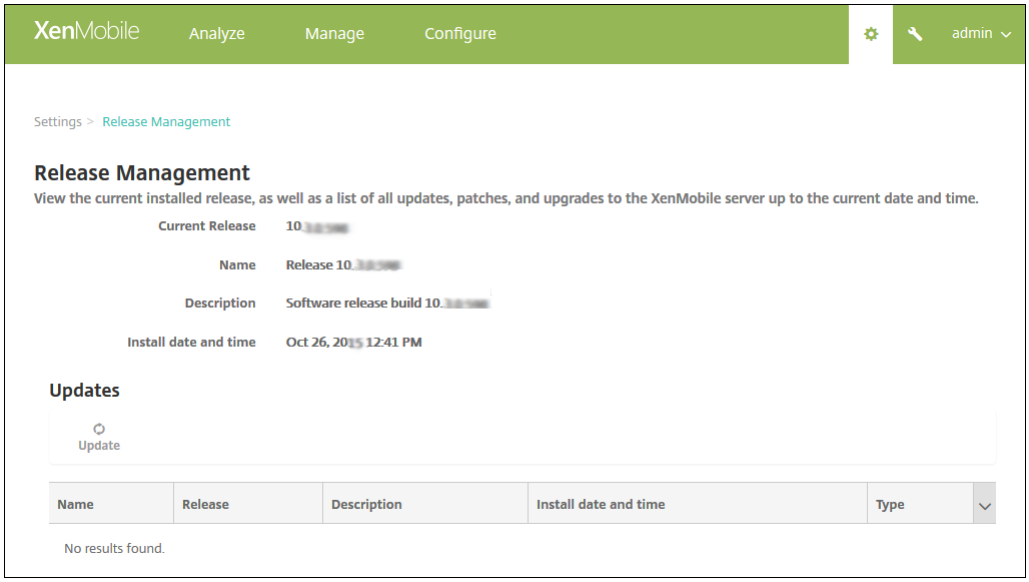
- 安装 XenMobile 更新前，请使用虚拟机 (VM) 中的设备创建系统的快照。
- 备份系统配置数据库。
- 检查要更新到的版本的系统要求。 对于 XenMobile 10.3，请参阅系统要求。

1. 在 Citrix Web 站点上登录您的帐户，然后将 XenMobile 升级 (.bin) 文件下载到合适的位置。

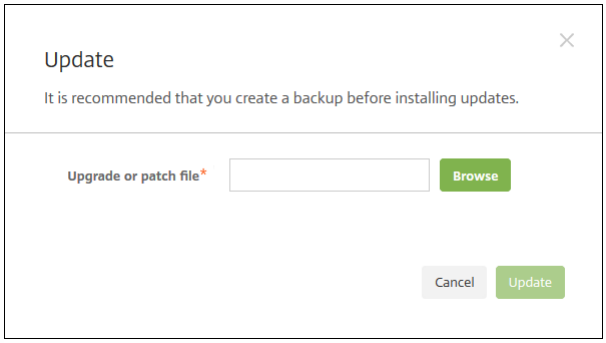
2. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

3. 单击**版本管理**。 此时将显示**版本管理**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 在**更新**下面，请单击**更新**。 此时将显示**更新**对话框。



4. 选择从 Citrix.com 下载的 XenMobile 升级文件，可通过单击**浏览**导航到此文件的位置。

5. 单击**更新**，然后在收到提示时，重新启动 XenMobile。

注意：安装更新后，XenMobile 可能不需要重新启动。 这种情况下，将出现一条消息，指出更新已安装成功。 但是，如果 XenMobile 确实要求重新启动，您必须使用命令行。 系统重新启动后清除浏览器缓存非常重要。

重要：如果系统是在群集模式下配置的，请按照以下步骤更新每个节点：

1. 在所有节点上从**设置** > **版本管理**中上载 .bin 文件。

2. 在命令行界面中从**设置**关闭所有节点。

3. 提出一个节点并检查服务是否正在运行。

4. 按顺序逐一对其他节点执行操作。

如果由于某些原因，更新未能成功完成，会显示一条指出问题的错误消息。 系统会恢复其状态，之后再尝试更新。

4. 单击“浏览”，导航到您从 Citrix.com 下载的 XenMobile 升级文件的保存位置，然后选择此文件。

5. 单击“更新”，然后在收到提示时，重新启动 XenMobile。

注意：安装更新后，XenMobile 可能不需要重新启动。 这种情况下，将出现一条消息，指出更新已安装成功。 但是，如果 XenMobile 确实要求重新启动，您必须使用命令行。

重要：如果系统是在群集模式下配置的，请按照以下步骤更新每个节点：

1. 关闭除一个节点之外的所有节点。
2. 更新该节点。
3. 在更新下一个节点之前，确认服务正在运行。

如果由于某些原因，更新未能成功完成，会显示一条指出问题的错误消息。 系统会恢复其状态，之后再尝试更新。

4. 单击“浏览”，导航到您从 Citrix.com 下载的 XenMobile 升级文件的保存位置，然后选择此文件。

5. 单击“更新”，然后在收到提示时，重新启动 XenMobile。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：安装更新后，XenMobile 可能不需要重新启动。 这种情况下，将出现一条消息，指出更新已安装成功。 但是，如果 XenMobile 确实要求重新启动，您必须使用命令行。

重要：如果系统是在群集模式下配置的，请按照以下步骤更新每个节点：

1. 关闭除一个节点之外的所有节点。
2. 更新该节点。
3. 在更新下一个节点之前，确认服务正在运行。

如果由于某些原因，更新未能成功完成，会显示一条指出问题的错误消息。 系统会恢复其状态，之后再尝试更新。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

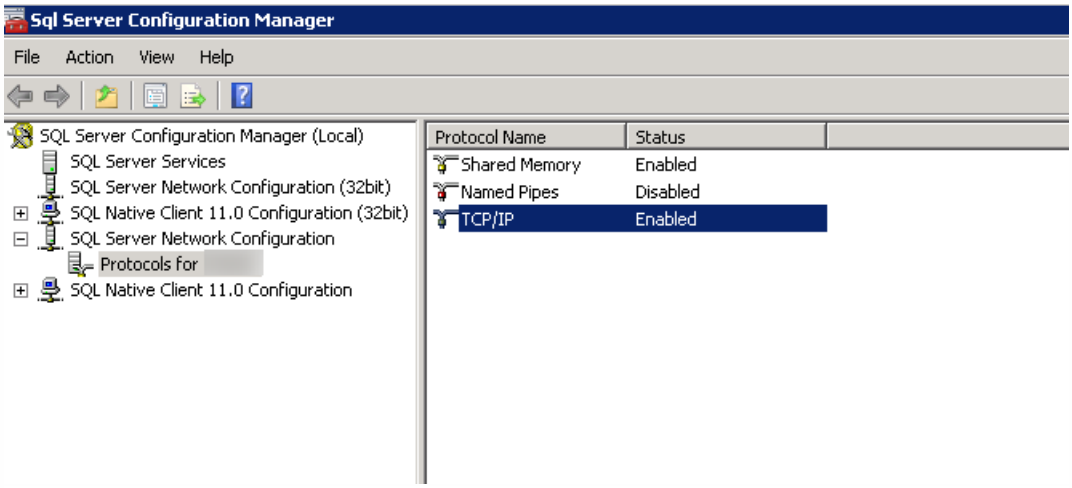
支持命名 SQL 实例

Aug 11, 2016

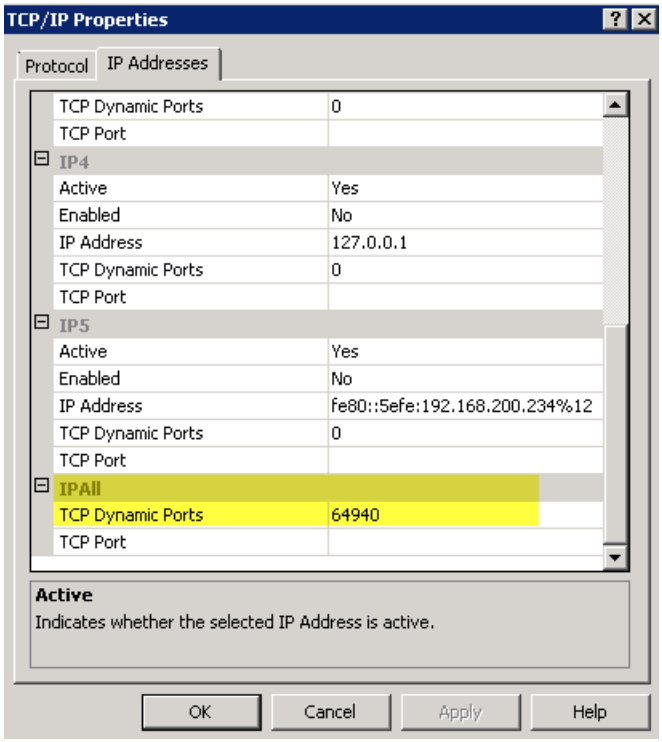
可以使用升级工具从 XenMobile 9 升级到 XenMobile 10 以及从 XenMobile 9 升级到 XenMobile 10.1。 如果您的 XenMobile 9 安装基于指定的 SQL 实例，您需要遵循特定于此情况的步骤。 如果您的 XenMobile 9 环境满足以下必备条件，请按照本文中的步骤进行升级。

- XenMobile 9 MDM Edition 或 Enterprise Edition 设置了一个外部 SQL Server 数据库。
- SQL Server 数据库在非默认命名实例上运行。
- SQL Server 命名实例在静态或动态 TCP 端口上侦听。 可以通过查看命名实例的 TCP/IP 协议的 IP 地址来确认此必备条件，如下图所示。

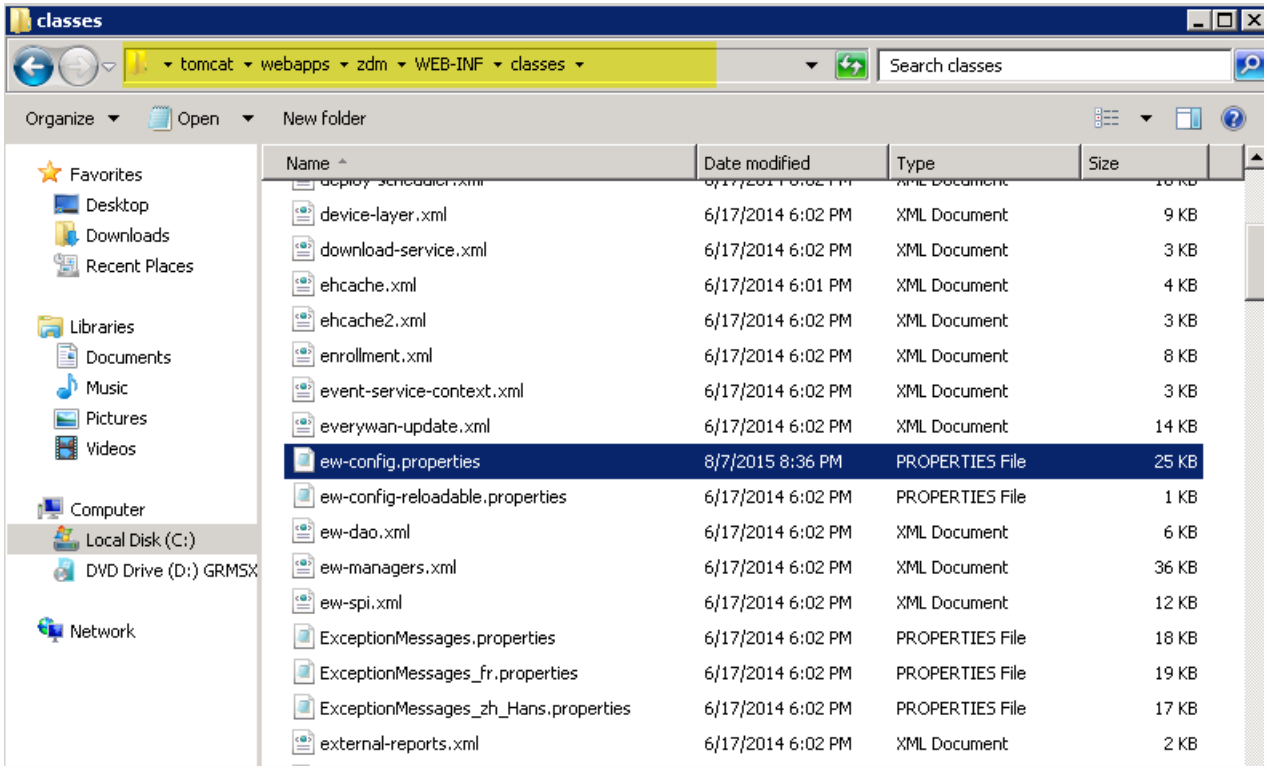
> **注意**
>
> Citrix 建议 SQL Server 数据库实例始终在静态端口上运行，因为 XenMobile 服务器需要继续访问该数据库。 此连接通常通过防火墙遍历。 因此，您需要在防火墙中打开恰当的端口，并且需要在静态端口上运行数据库实例。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. 转至 Device Manager 安装目录并打开 ew-config.properties 文件。 此文件位于 tomcat\webapps\zdm\WEB-INF\classes 中。

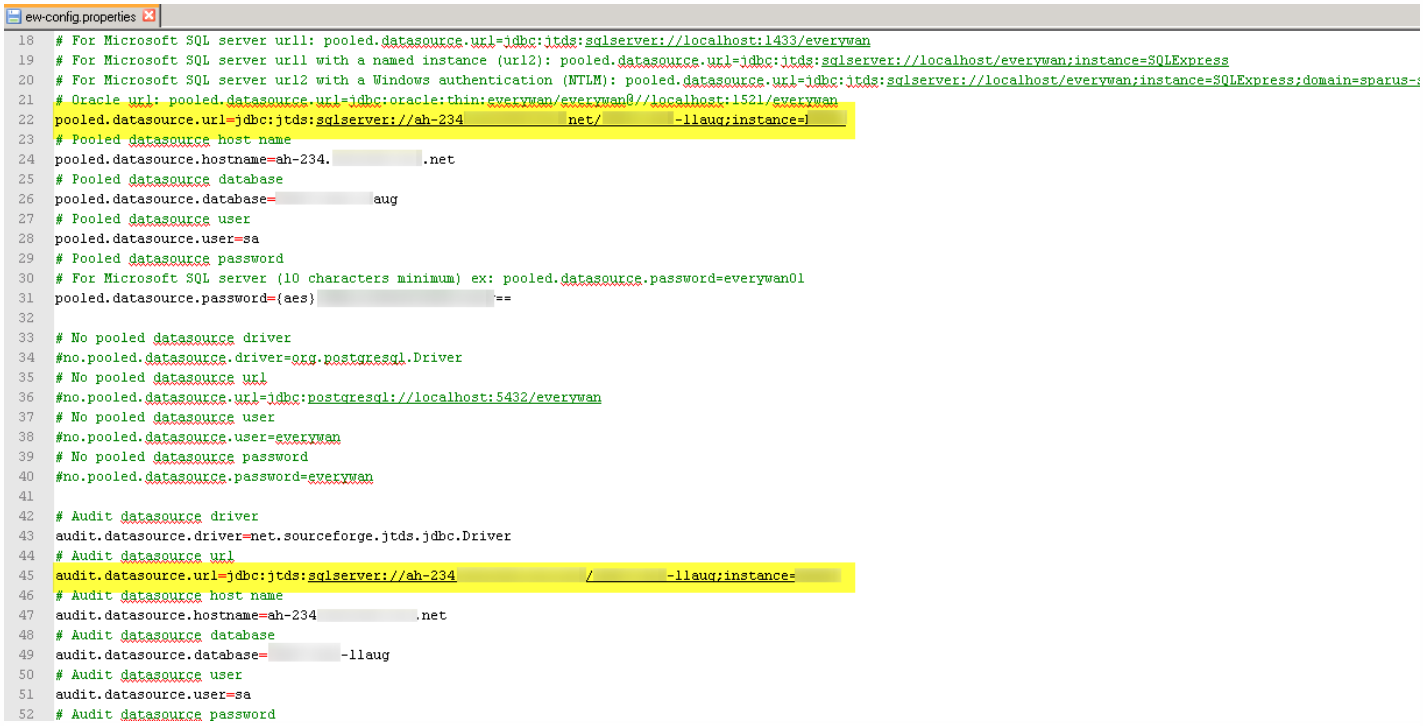


2. 在 ew-config.properties 文件中，在“DATASOURCE Configuration”部分中搜索以下 URL：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

pooled.datasource.url= jdbc:jtds:sqlserver:///;instance=

audit.datasource.url= jdbc:jtds:sqlserver:///;instance=



3. 删除上述 URL 中的实例名称，然后添加端口以及 SQL Server FQDN。 在这种情况下，必需端口为 64940。

pooled.datasource.url=jdbc:jtds:sqlserver:// :64940/

audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

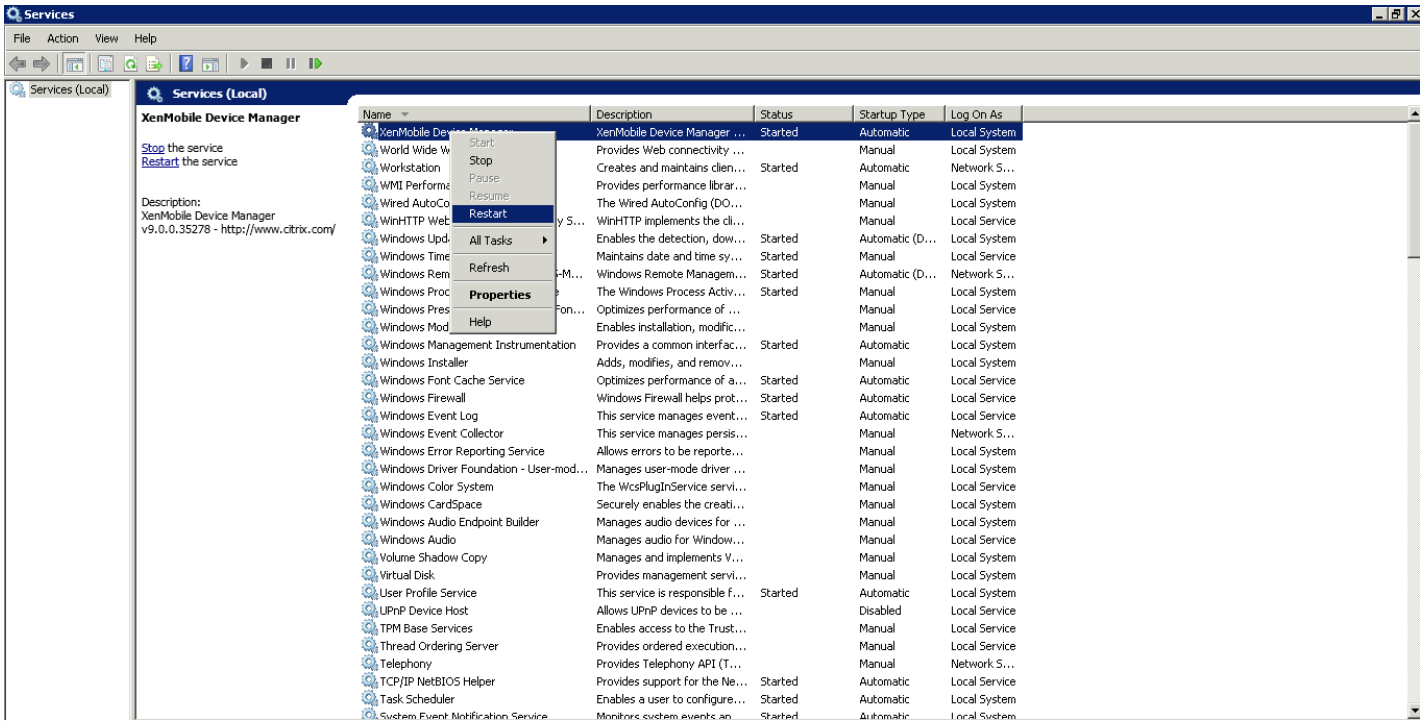
> ## 注意
>
> Citrix 建议您备份、 复制 或记录在 ew-config.properties 文件中所做的更改。 此信息在迁移失败时非常有用。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ew-config.properties

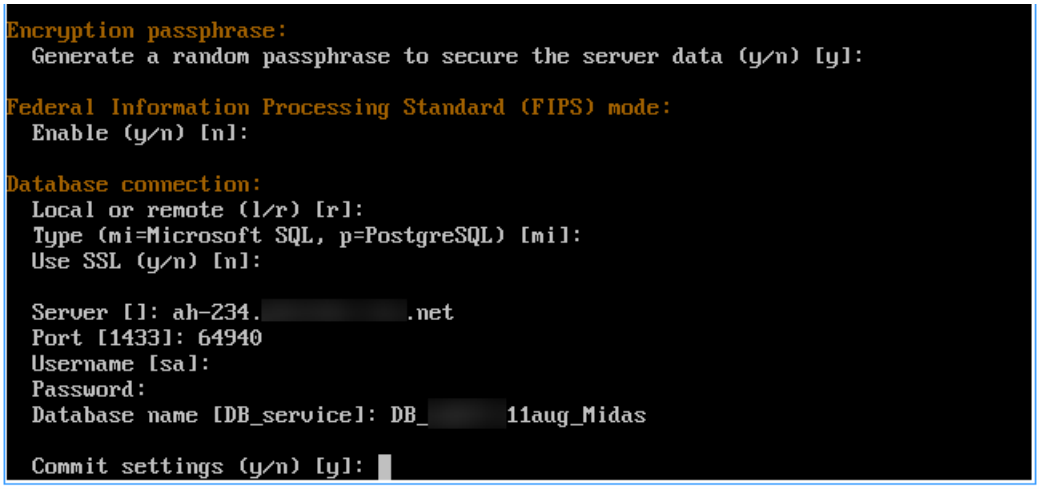
```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.                net:                -llaug
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=          -llaug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}                    ==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://              -inc.net:              -llaug
# Audit datasource host name
audit.datasource.hostname=ah-234.          .net
# Audit datasource database
audit.datasource.database=          -llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

4. 重新启动 Device Manager 服务。 Device Manager 实例返回时刷新设备连接。



5. 确定新 XenMobile 10 服务器是否需要与命名 SQL 实例一起运行。 如果需要，请识别运行命名实例的端口。 如果该端口为动态端口，Citrix 建议您将其转换为静态端口；然后在数据库设置过程中，在新 XenMobile 服务器上配置该静态端口。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 按照这些步骤进行操作，继续升级您的 XenMobile 环境：

要从 XenMobile 9.0（MDM Edition、App Edition 和 Enterprise Edition）升级到 XenMobile 10.1，请使用升级工具。 可以从 Citrix.com 下载页面下载升级工具。 有关详细信息，请参阅升级 XenMobile。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

为 XenMobile 10 配置群集

Aug 11, 2016

在版本 10 之前的 XenMobile 版本中，将 Device Manager 配置为群集，将 App Controller 配置为高可用性对。 XenMobile 10 集成了 XenMobile 9 Device Manager 和 App Controller。 从版本 10 开始，高可用性不再适用于 XenMobile。 因此，要配置群集，需要在 NetScaler 上配置下面两个负载平衡虚拟 IP 地址。

- **移动设备管理 (MDM) 负载平衡虚拟 IP 地址**：与群集中配置的 XenMobile 节点进行通信需要使用 MDM 负载平衡虚拟 IP 地址。 此负载平衡在 SSL 桥接模式下完成。
- **移动应用程序管理 (MAM) 负载平衡虚拟 IP 地址**：NetScaler Gateway 与群集中配置的 XenMobile 节点进行通信需要使用 MAM 负载平衡虚拟 IP 地址。 在 XenMobile 10 中，默认情况下，来自 NetScaler Gateway 的所有流量在端口 8443 上路由到负载平衡虚拟 IP 地址。

本文中的步骤解释了创建新 XenMobile 虚拟机 (VM)、将新 VM 加入现有 VM 从而创建群集设置的方法。

必备条件

- 已完整配置所需的 XenMobile 节点。
- 一个用于 MDM L 区段的公用 IP 地址和一个用于 MAM 的专用 IP 地址。
- 服务器证书。
- 一个用作 NetScaler Gateway 虚拟 IP 地址的可用 IP。

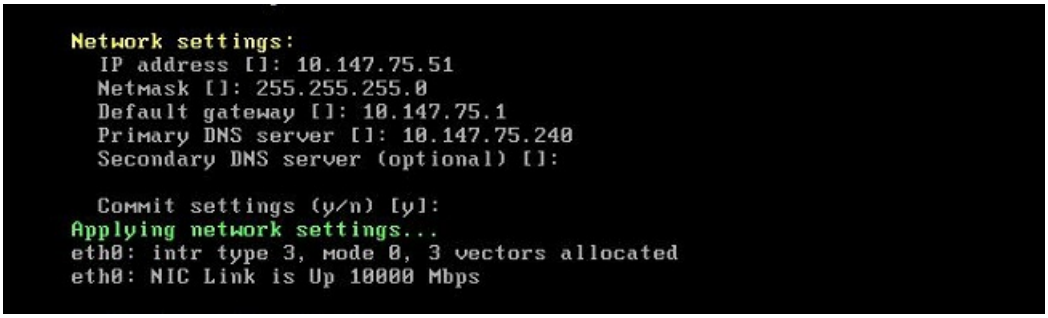
有关群集配置中 XenMobile 10.x 的参考体系结构图，请参阅体系结构概述。

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

1. 打开新 VM 的命令行控制台，并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。

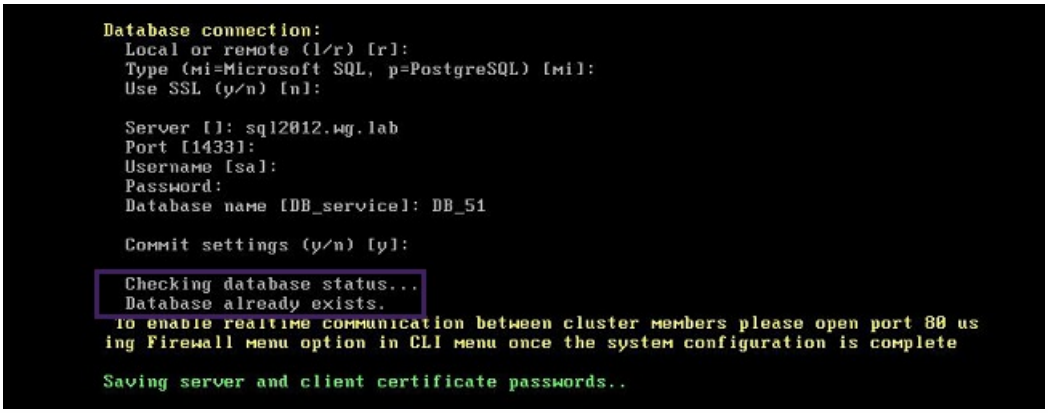
© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 如果希望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。

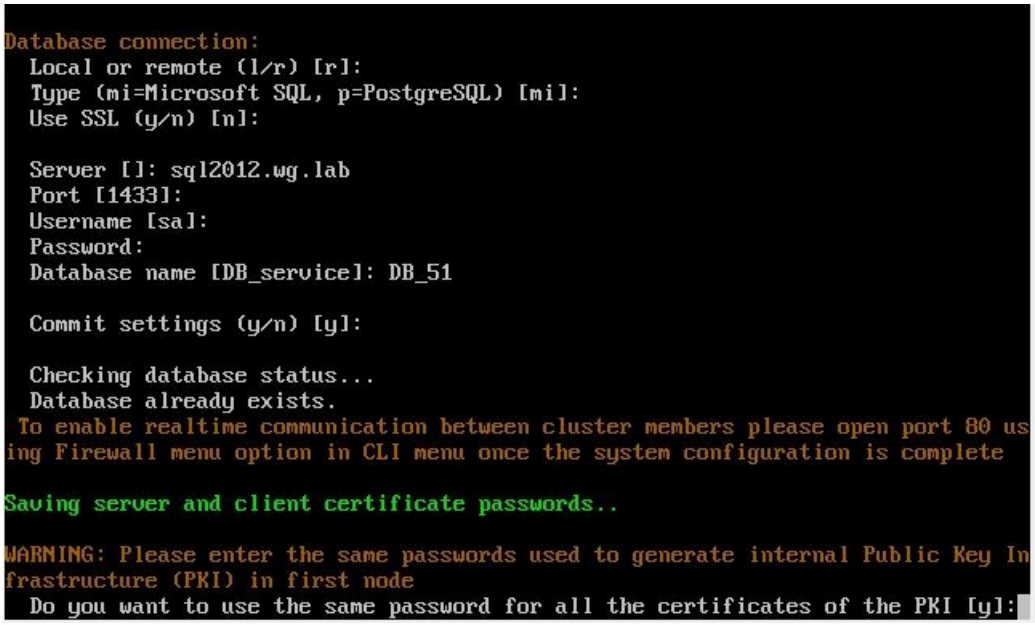
4. 如果要使用 FIPS，请键入y；否则，请键入n。

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



6. 输入与为第一个 VM 提供的证书相同的密码。

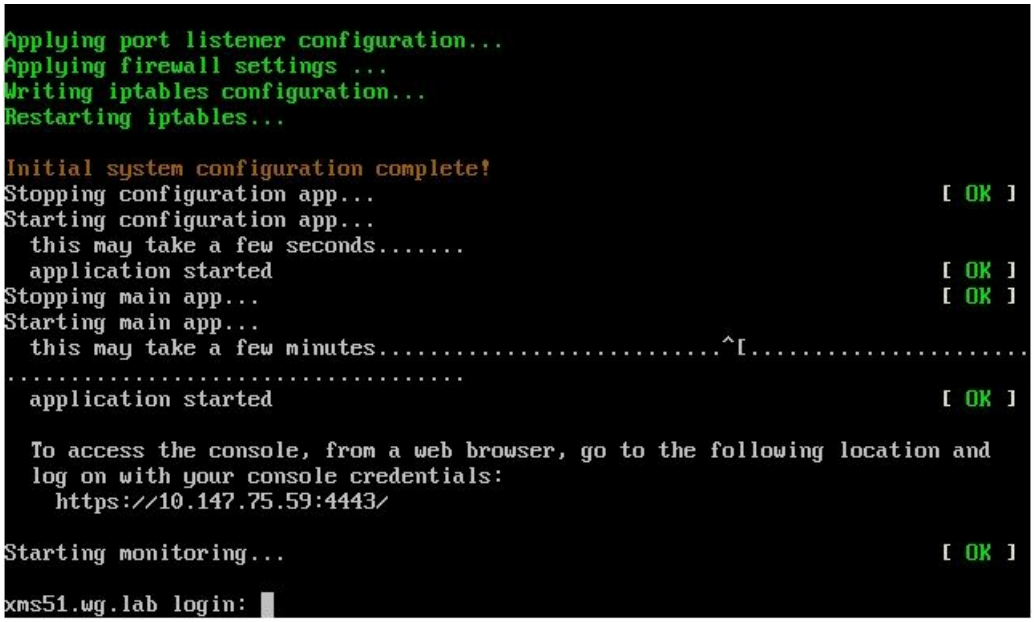
© 1999-2017 Citrix Systems, Inc. All rights reserved.



输入密码后，第二个节点上的初始配置将完成。

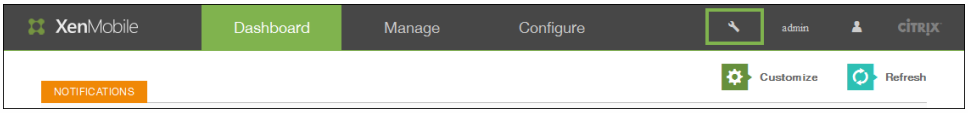
7. 配置完成后，服务器重新启动并显示登录对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

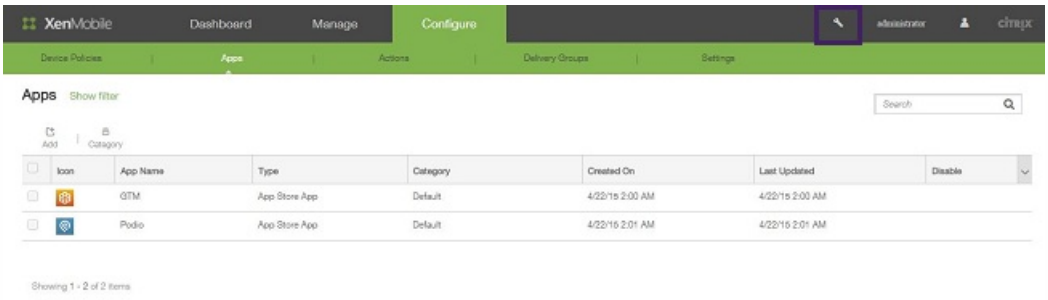


注意：登录对话框与第一个 VM 的登录对话框相同。 这种相同是供您确认两个 VM 使用相同的数据库服务器的一种途径。

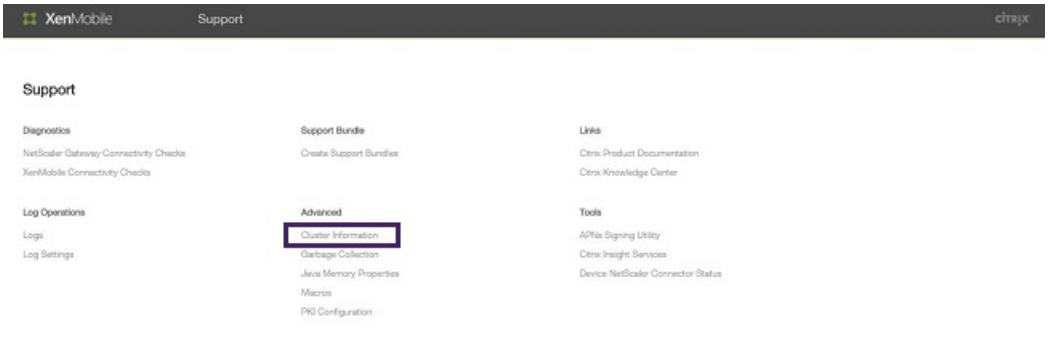
8. 使用 XenMobile 的完全限定的域名 (FQDN) 在 Web 浏览器中打开 XenMobile 控制台。
9. 在控制板上，单击屏幕右上角的工具图标。



此时将打开“支持”页面。

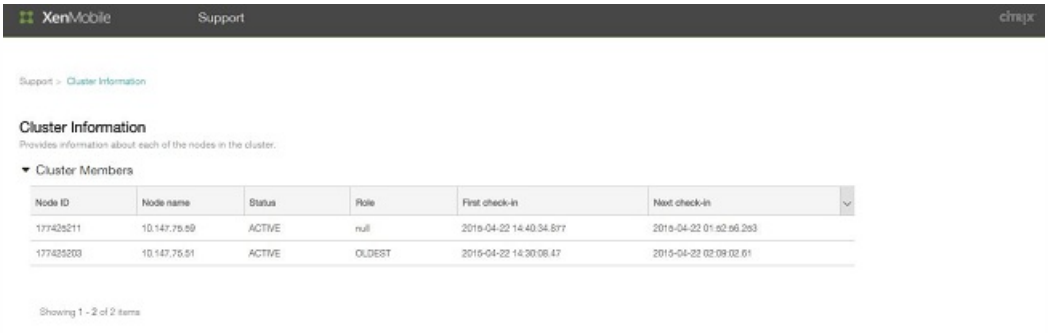


10. 在高级下面，单击群集信息。



将显示关于此群集的所有信息，包括群集成员、设备连接信息、任务等。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

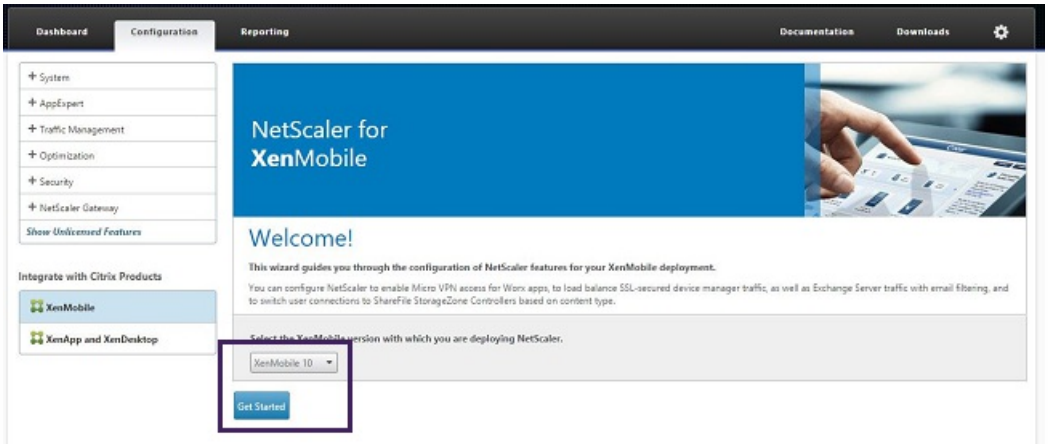


新节点现在属于群集的成员。 您可以按照相同的步骤添加其他节点。

将所需的节点作为成员添加到 XenMobile 群集中后，需要对节点进行负载平衡才能访问群集。 负载平衡通过运行 NetScaler 10.5.x 中提供的 XenMobile 向导完成。 您可以通过运行此向导，按照本过程中的步骤对 XenMobile 进行负载平衡。

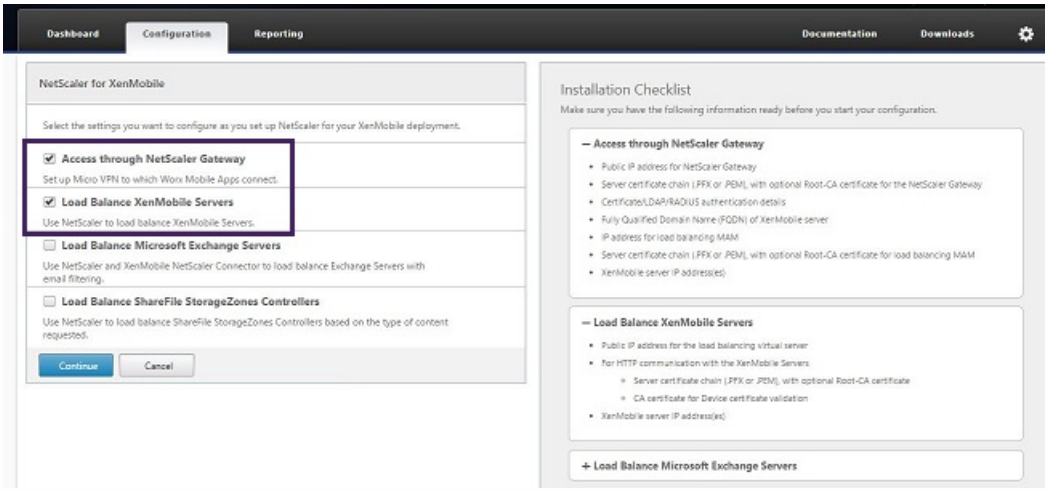
1. 登录 NetScaler。

2. 在 Configuration（配置）选项卡上，单击 XenMobile，然后单击 Get Started（开始）。

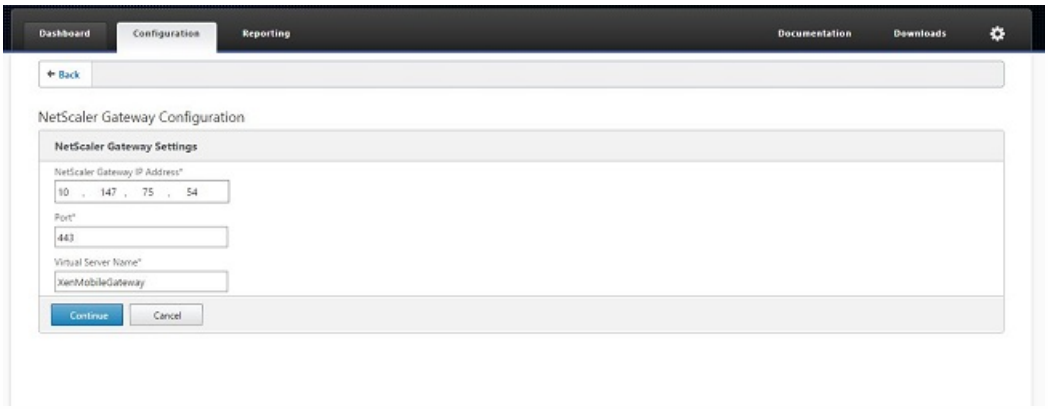


3. 选中 Access through NetScaler Gateway（通过 NetScaler Gateway 访问）复选框和 Load Balance XenMobile Servers（XenMobile 服务器负载平衡）复选框，然后单击 Continue（继续）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



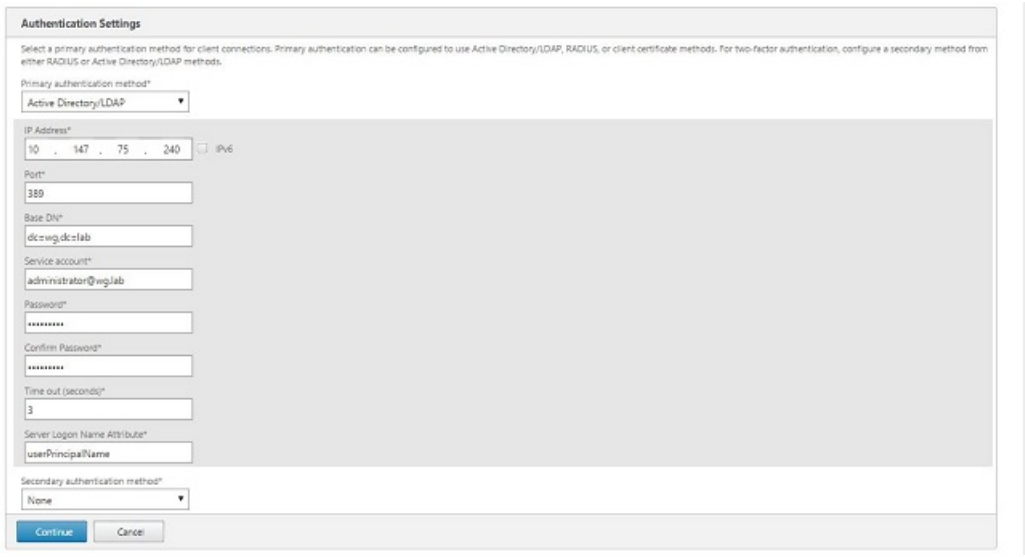
4. 输入 NetScaler Gateway 的 IP 地址，然后单击 Continue（继续）。



5. 通过执行以下操作将服务器证书绑定到 NetScaler Gateway 虚拟 IP 地址，然后单击 Continue（继续）。
   - 在 Use existing certificate（使用现有证书）中，从列表中选择服务器证书。
   - 单击 Install Certificate（安装证书）选项卡以上载新的服务器证书。

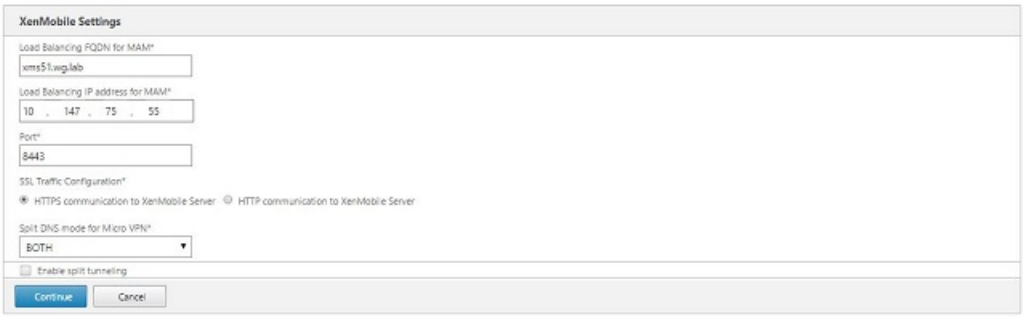
6. 输入身份验证服务器详细信息，然后单击 Continue（继续）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

7. 在 XenMobile settings（XenMobile 设置）中，输入 Load Balancing FQDN for MAM（MAM 的负载平衡 FQDN），然后单击 Continue（继续）。



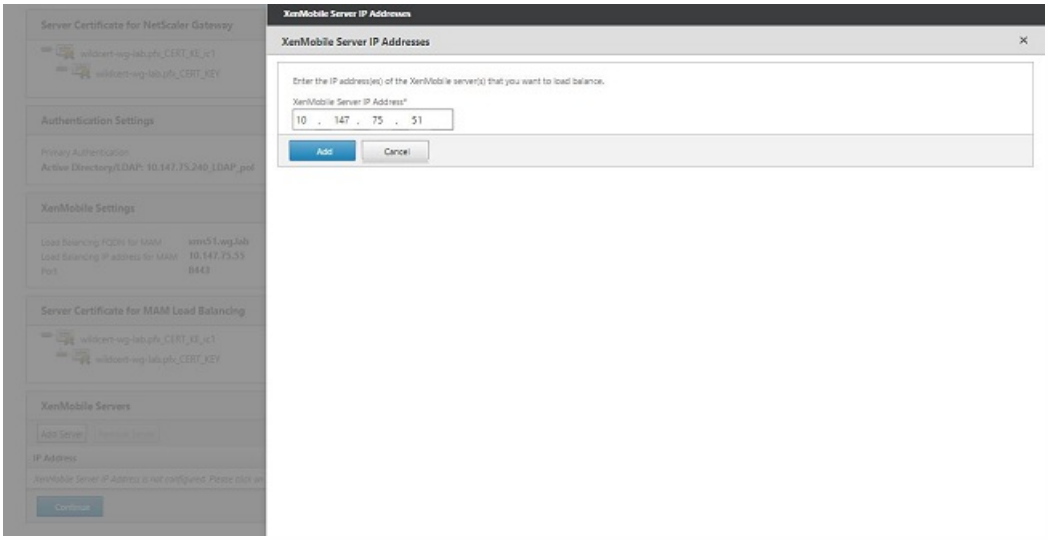
注意：确保 MAM 负载平衡虚拟 IP 地址的 FQDN 与 XenMobile 的 FQDN 相同。

8. 如果使用 SSL 桥接模式 (HTTPS)，请选择 HTTPS communication to XenMobile Server（与 XenMobile 服务器进行 HTTPS 通信）。 但是，如果要使用 SSL 卸载，请选择 HTTP communication to XenMobile Server（与 XenMobile 服务器进行 HTTP 通信），如上图所示。 为实现本文的目的，请选择 SSL 桥接模式 (HTTPS)。
9. 绑定 MAM 负载平衡虚拟 IP 地址的服务器证书，然后单击 Continue（继续）。

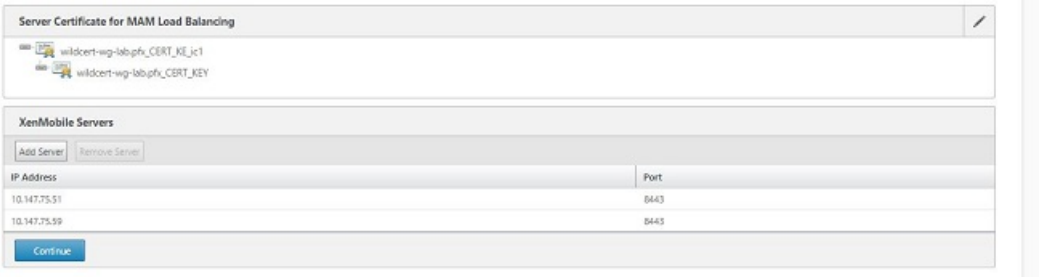
10. 在 XenMobile Servers（XenMobile 服务器）下面，单击 Add Server（添加服务器）以添加 XenMobile 节点。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

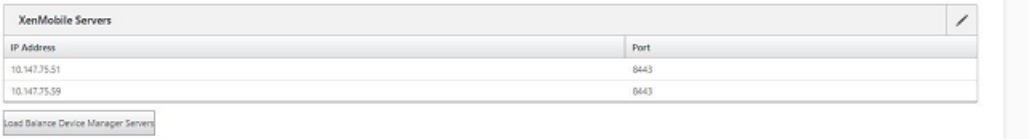
11. 输入 XenMobile 节点的 IP 地址，然后单击 Add（添加）。



12. 重复步骤 10 和 11 以添加其他 XenMobile 节点，作为 XenMobile 群集的一部分。 您将看到已添加的所有 XenMobile 节点。单击 Continue（继续）。

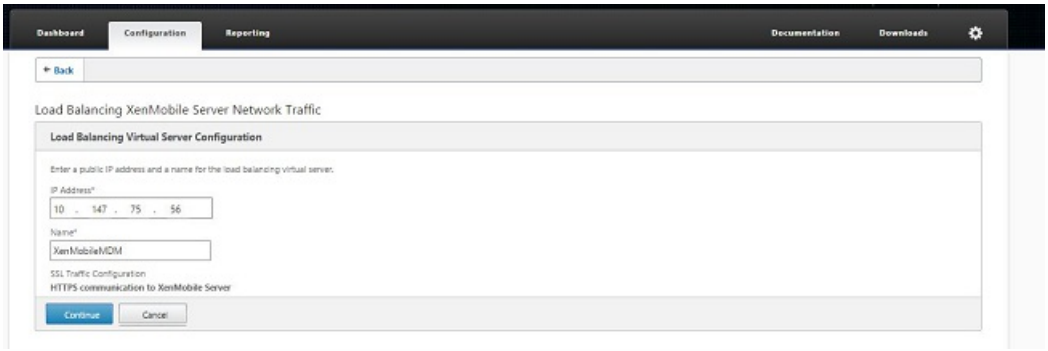


13. 单击 Load Balance Device Manager Servers（Device Manager 服务器负载平衡）以继续执行 MDM 负载平衡配置。

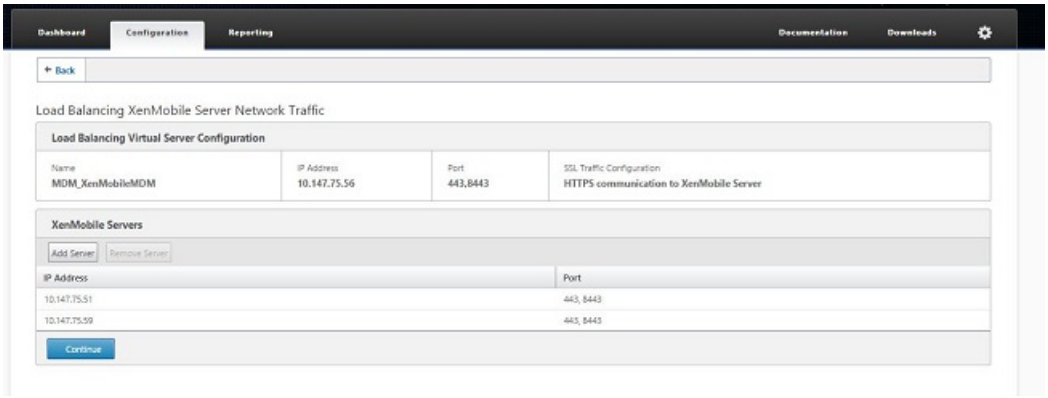


14. 输入要用作 MDM 负载平衡 IP 地址的 IP 地址，然后单击 Continue（继续）。

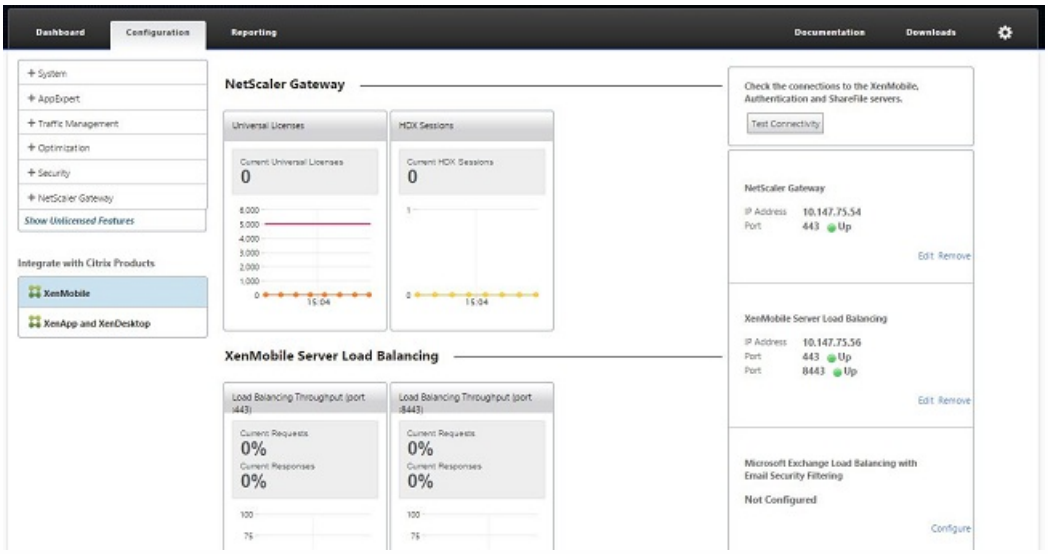
© 1999-2017 Citrix Systems, Inc. All rights reserved.



15. 列表中显示 XenMobile 节点后，单击 Continue（继续），然后单击 Done（完成）以完成此过程。

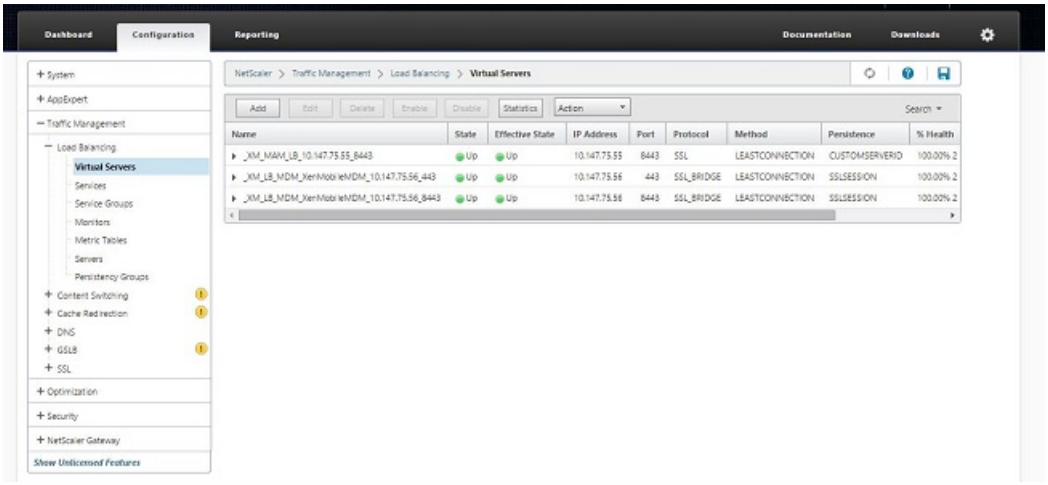


您将在 XenMobile 页面上看到虚拟 IP 地址状态。

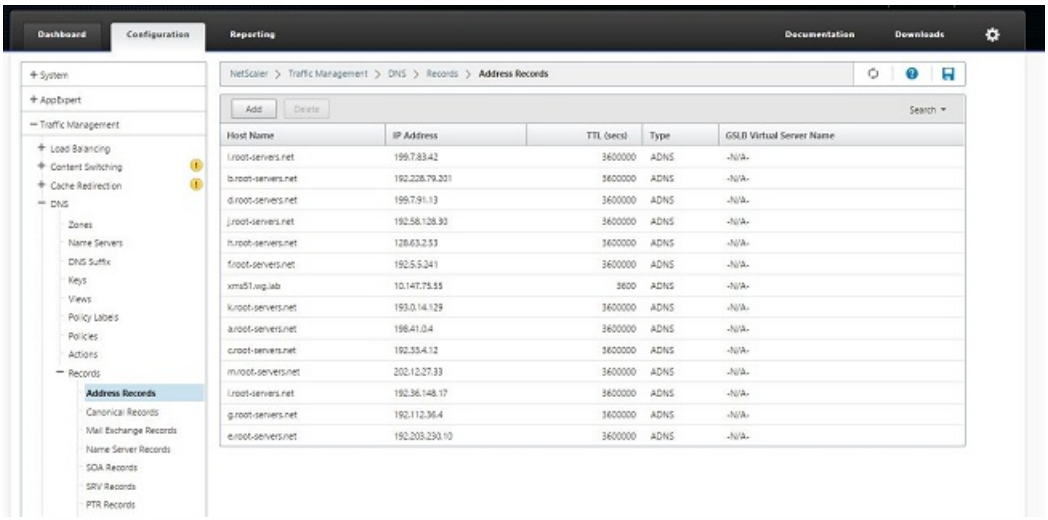


16. 要确认虚拟 IP 地址是否已启用并运行，请单击 Configuration（配置）选项卡，然后导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）> Virtual Servers（虚拟服务器）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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



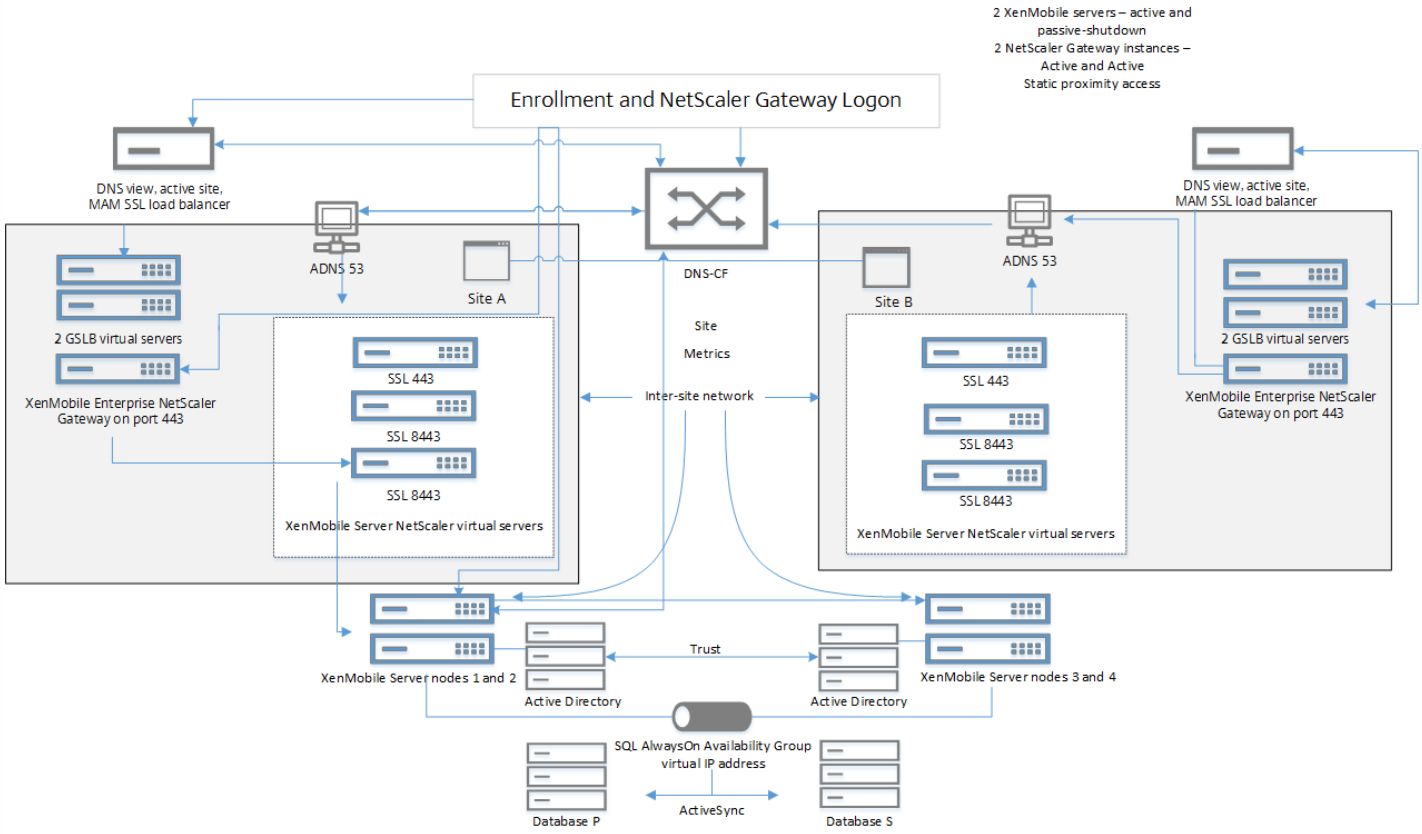
© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 的灾难恢复指南

Aug 11, 2016

本指南以 PDF 格式提供，主要介绍如何为灾难恢复部署配置 XenMobile 10 Enterprise Edition。

此部署的体系结构如下图所示，该结构图也可以 PDF 格式下载。



XenMobile 灾难恢复指南

XenMobile 灾难恢复体系结构图。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

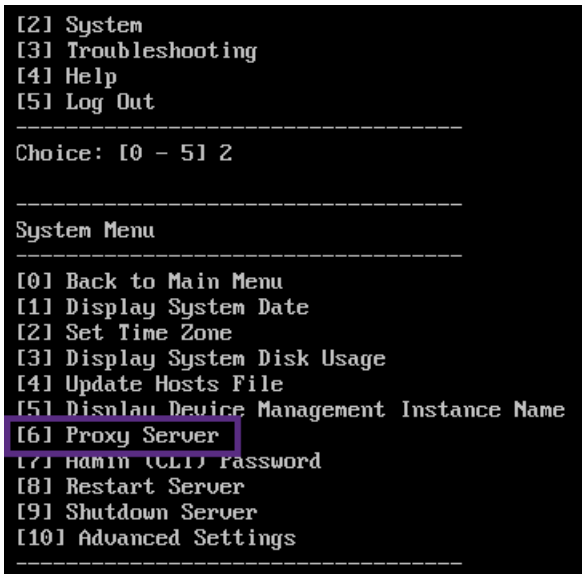
在 XenMobile 中启用代理服务器

Aug 11, 2016

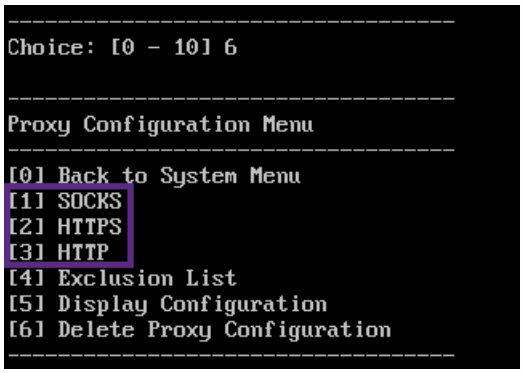
如果想要控制出站 Internet 流量，可以在 XenMobile 中设置代理服务器来承载此流量。 为此，需要通过命令行接口 (CLI) 设置代理服务器。 请注意，设置代理服务器需要重新启动系统。

1. 在 XenMobile CLI 主菜单中，键入 **2** 以选择“System Menu”（系统菜单）。

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



3. 在“Proxy Configuration Menu”（代理配置菜单）中，键入 **1** 以选择 SOCKS，键入 **2** 以选择 HTTPS，或键入 **3** 以选择 HTTP。

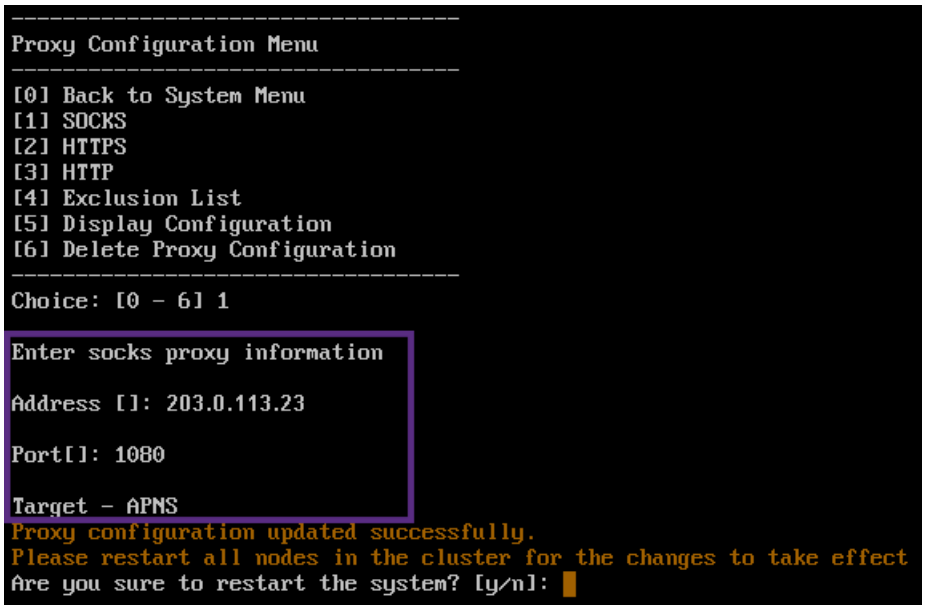


4. 键入代理服务器 IP 地址、端口号和目标。 有关每种代理服务器类型支持的目标类型，请参阅下表。

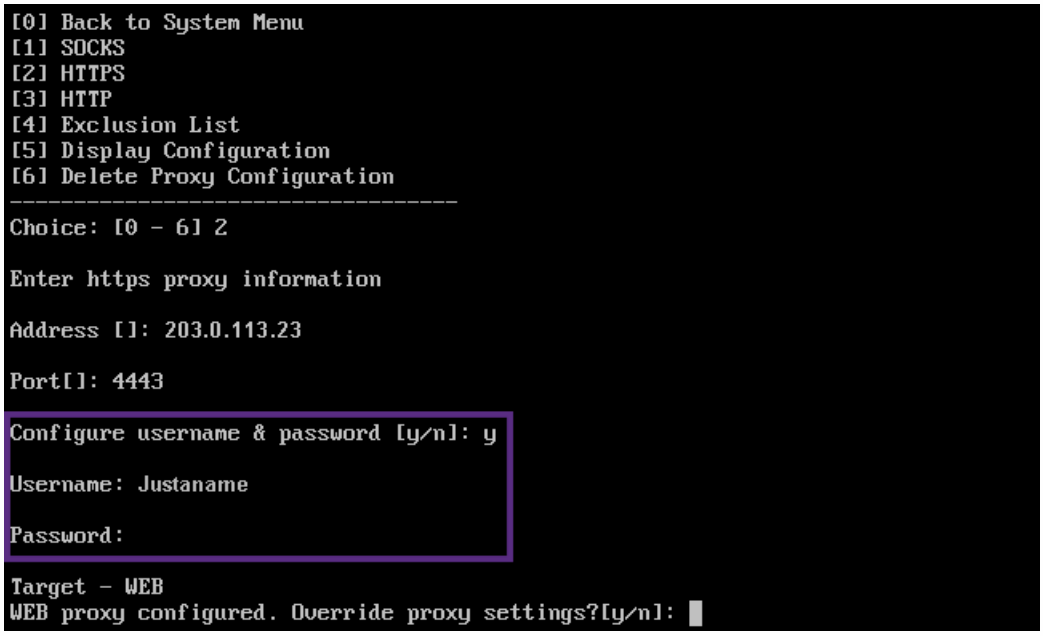
代理类型	支持的目标
SOCKS	APNS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HTTP	APNS、Web。 PKI
HTTPS	Web、PKI
HTTP 并进行身份验证	Web、PKI
HTTPS 并进行身份验证	Web、PKI



5. 如果选择在 HTTP 或 HTTPS 代理服务器上配置用户名和密码以进行身份验证，请键入 **y**，然后键入用户名和密码。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 键入 **y** 将完成代理服务器设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Licensing

Oct 21, 2016

XenMobile 和 NetScaler Gateway 需要许可证。 有关显示每个版本中可用的 XenMobile 功能的数据表，请参阅此 PDF。

有关 NetScaler Gateway 许可的详细信息，请参阅 NetScaler Gateway 许可证。XenMobile 使用 Citrix Licensing 管理许可证。 有关 Citrix Licensing 的详细信息，请参阅 The Citrix Licensing System（Citrix Licensing 系统）。

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

必须先安装 Citrix Licensing，然后再下载 XenMobile 许可证。 需要安装了 Citrix Licensing 的服务器的名称才能生成许可证文件。 安装 XenMobile 时，默认在服务器上安装 Citrix Licensing。 您也可以使用现有 Citrix Licensing 部署管理 XenMobile 许可证。 有关安装、部署和管理 Citrix Licensing 的详细信息，请参阅许可使用本产品。

注意

XenMobile 10.3.x 版要求 11.12.1 Citrix 许可证服务器或更高版本的许可证服务器；较旧的许可证服务器版本与 XenMobile 10.3.x 不兼容。

Important

如果打算将 XenMobile 的节点或实例群集在一起，需要在远程服务器上使用 Citrix Licensing。

Citrix 建议您保留收到的所有许可证文件的一份本地副本。 保存配置文件的备份副本时，所有许可证文件都包含在备份中。 但是，如果您在未提前备份配置文件的情况下重新安装 XenMobile，则需要使用原始许可证文件。

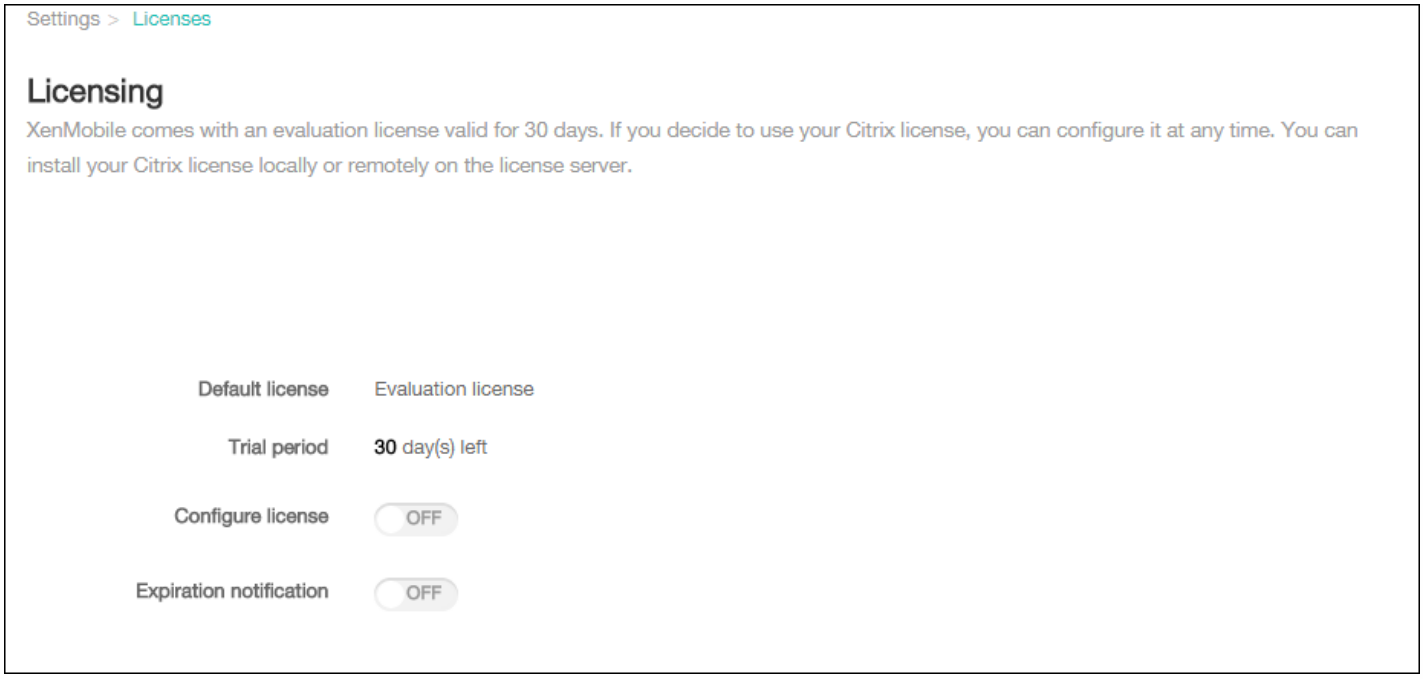
在不提供许可证的情况下，XenMobile 将在宽限期为 30 天的试用模式下运行，功能齐全。 此试用模式只能使用一次，期限为从安装 XenMobile 开始持续 30 天。 无论是否有可用的有效 XenMobile 许可证，均不会阻止对 XenMobile Web 控制台的访问。 在 XenMobile 控制台上，您可以查看您的试用期还剩多少天。

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

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

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

2. 单击**许可**。 此时将显示**许可**页面。

添加新许可证时，新许可证将显示在表格中。 添加的第一个许可证自动被激活。 如果添加同一类别（如企业）或同一类型（如设备）的多个许可证，这些许可证将显示在表格的同一行中。 在这些情况下，**许可证总数**和**使用的数量**反应公共许可证的总数。 **过期日期**显示公共许可证中的最新过期日期。

通过 XenMobile 控制台管理所有本地许可证。

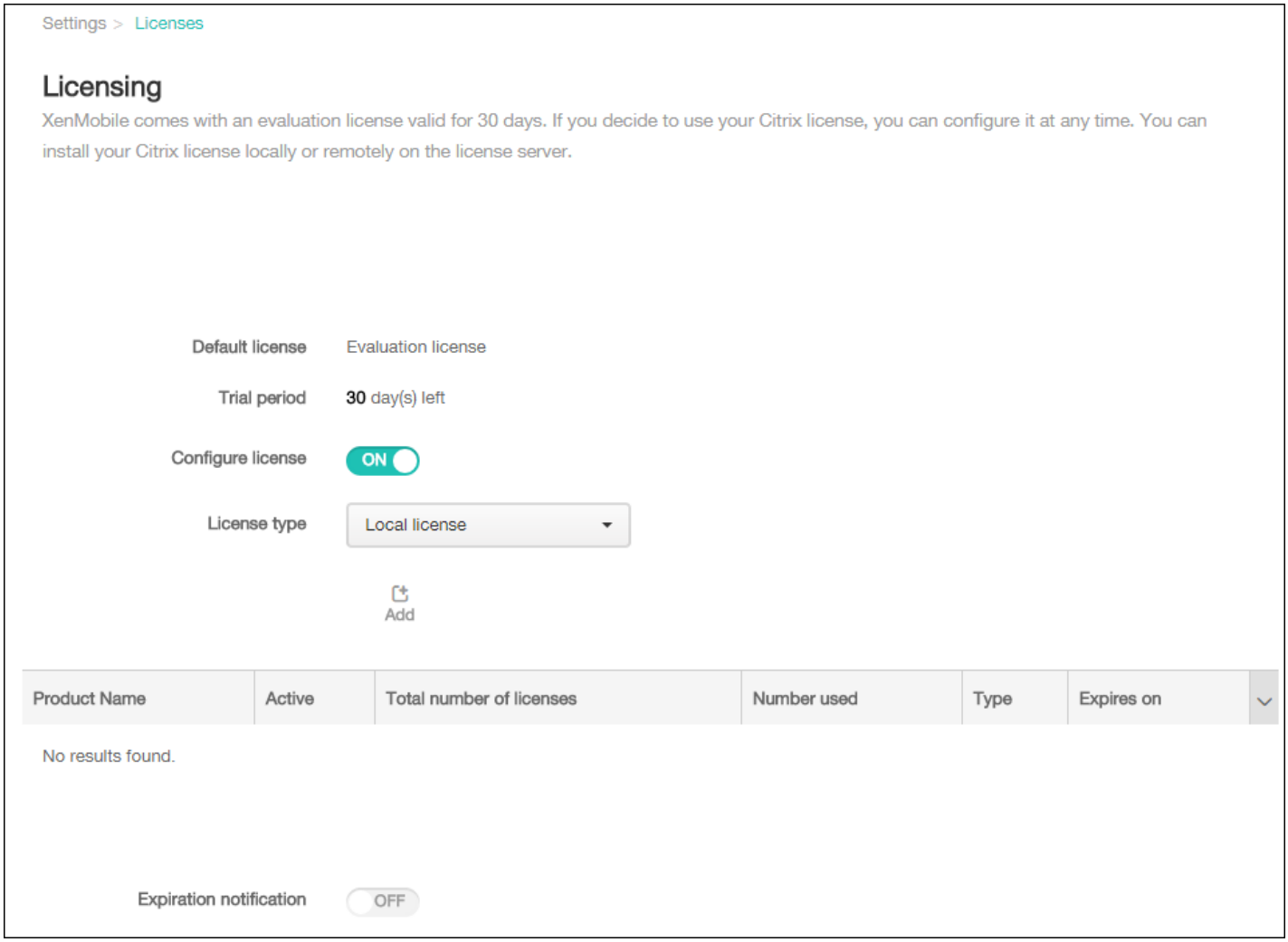
1. 从 Simple License Service 获取许可证文件，方法是通过许可证管理控制台或直接利用您在 Citrix.com 上的帐户。 有关详细信息，请参阅获取许可证文件。

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

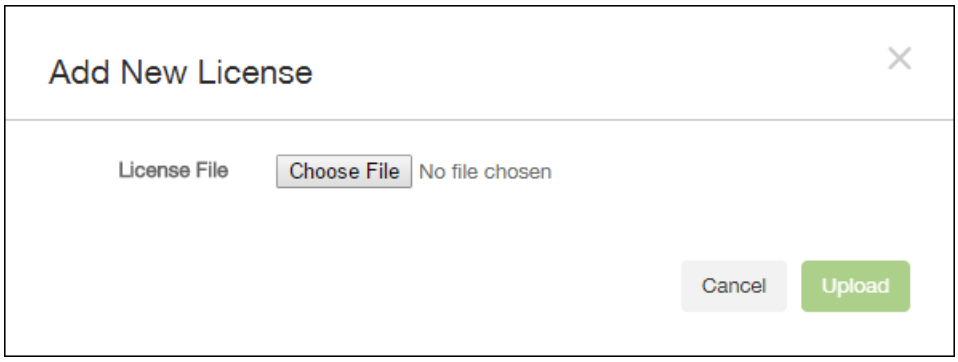
3. 单击**许可**。 此时将显示**许可**页面。

4. 将**配置许可证**设置为**开**。 在**许可证类型**列表中，单击**添加**按钮，将显示**许可**表。 **许可**表包含已用于 XenMobile 的许可证。 如果尚未添加任何 Citrix 许可证，此表为空。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



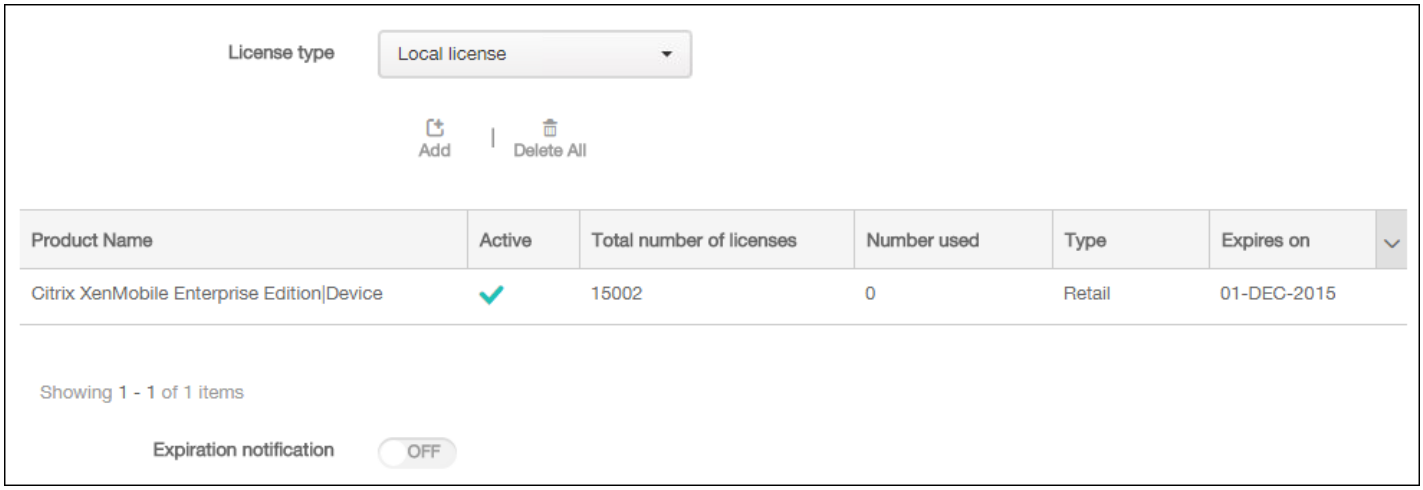
5. 确保将**许可证类型**设置为**本地许可证**，然后单击**添加**。 此时将显示**添加新许可证**对话框。



6. 在**添加新许可证**对话框中，单击**选择文件**，然后浏览到许可证文件的位置。

7. 单击**上载**。 许可证将上载到本地并显示在表格中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

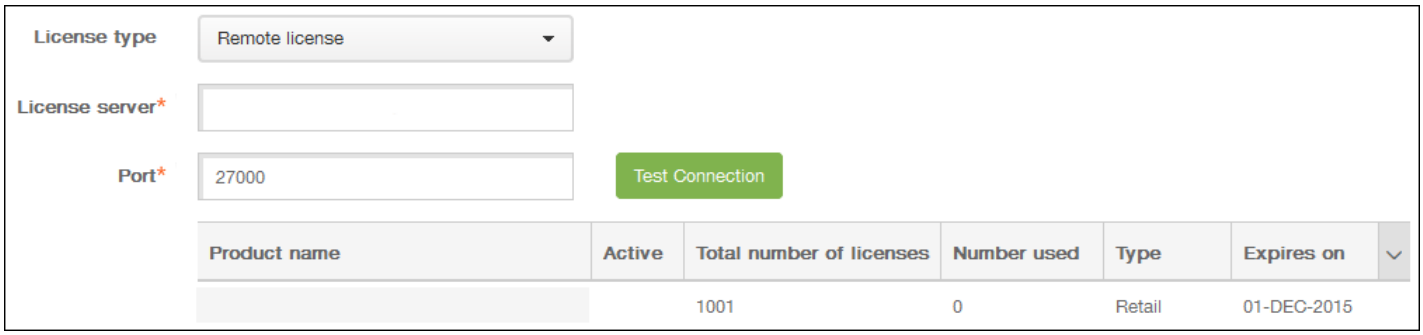


8. 许可证显示在**许可**页面上的表格中以后，请将其激活。 如果此许可证是表格中的第一个许可证，此许可证会自动激活。

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

1. 在**许可**页面上，将**配置许可证**设为**开**。 在**许可证类型**列表中，单击**添加**按钮，将显示**许可**表。 **许可**表包含已用于 XenMobile 的许可证。 如果尚未添加任何 Citrix 许可证，此表为空。

3. 将**许可证类型**设置为**远程许可证**。 **添加**按钮将替换为**许可证服务器**和**端口**字段以及**测试连接**按钮。



4. 配置以下设置：

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

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

单击**测试连接**后，XenMobile 会确认以下信息：

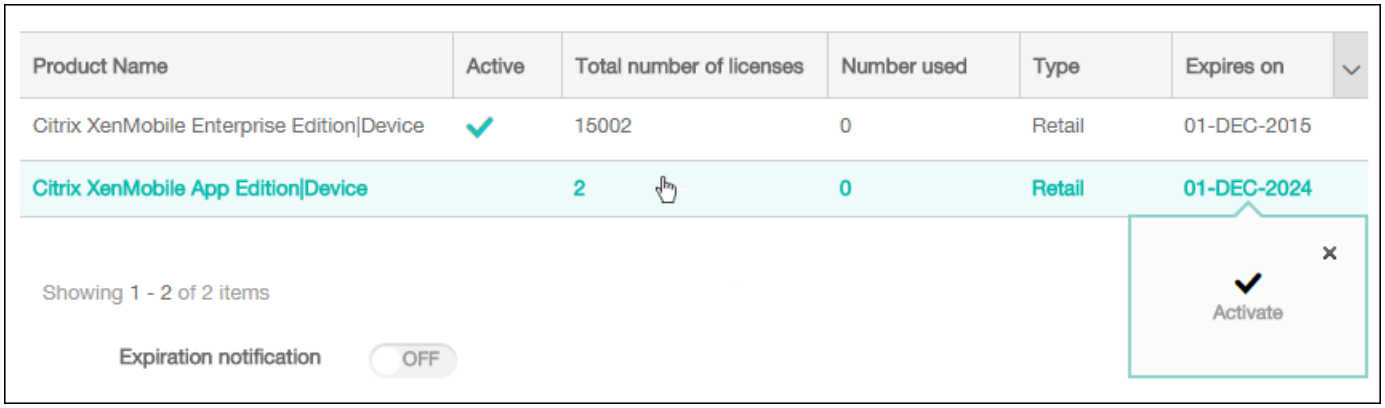
- XenMobile 可以与许可证服务器通信。
- 许可证服务器上的许可证有效。
- 许可证服务器与 XenMobile 兼容。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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

1. 在**许可**页面的**许可表**中，单击要激活的许可证所在的行。 行旁边将显示**激活**确认对话框。



2. 单击**激活**。 将显示**激活**对话框。

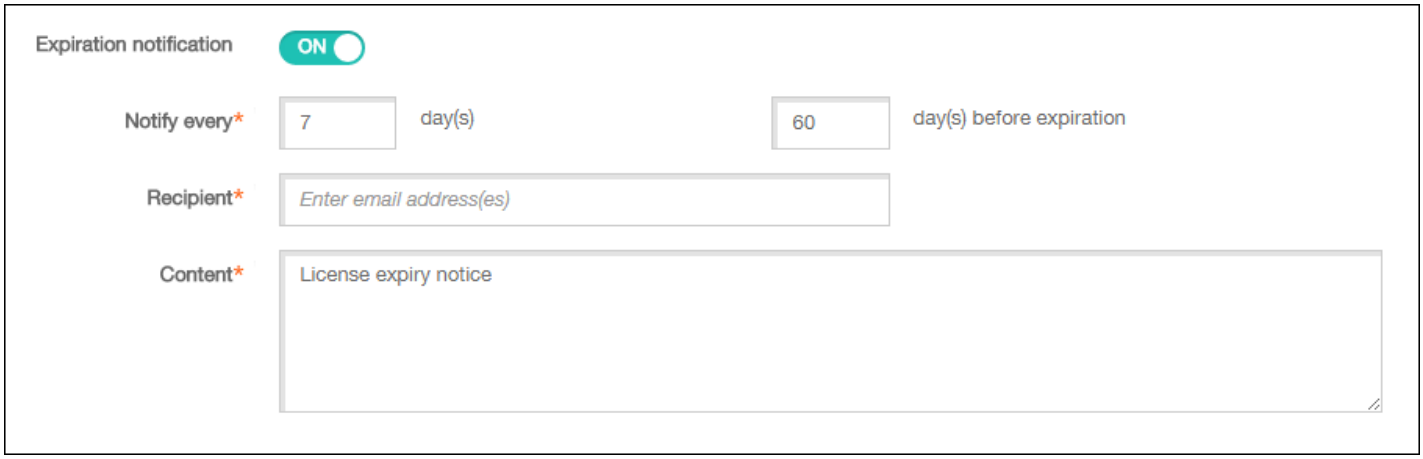
3. 单击**激活**。 所选许可证现已激活。

> **Important**
>
> 如果激活所选许可证，当前激活的许可证将取消激活。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

激活远程或本地许可证后，可以将 XenMobile 配置为在接近许可证过期日期时自动通知您，或配置一个委派。

1. 在**许可**页面上，将**到期通知**设为**开**。 将显示新的与通知相关的字段。



2. 配置以下设置：

- **通知时间间隔**：键入：
  - 发送通知的频率，如每 7 天一次。
  - 开始发送通知的时间，如在许可证过期前 60 天发送。
- **收件人**：键入您的电子邮件地址或许可证负责人的电子邮件地址。
- **内容**：键入收件人在通知中看到的过期通知消息。

3. 单击**保存**。 在距离过期还剩所设定的天数时，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。 通知按照您设置的频率发送。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

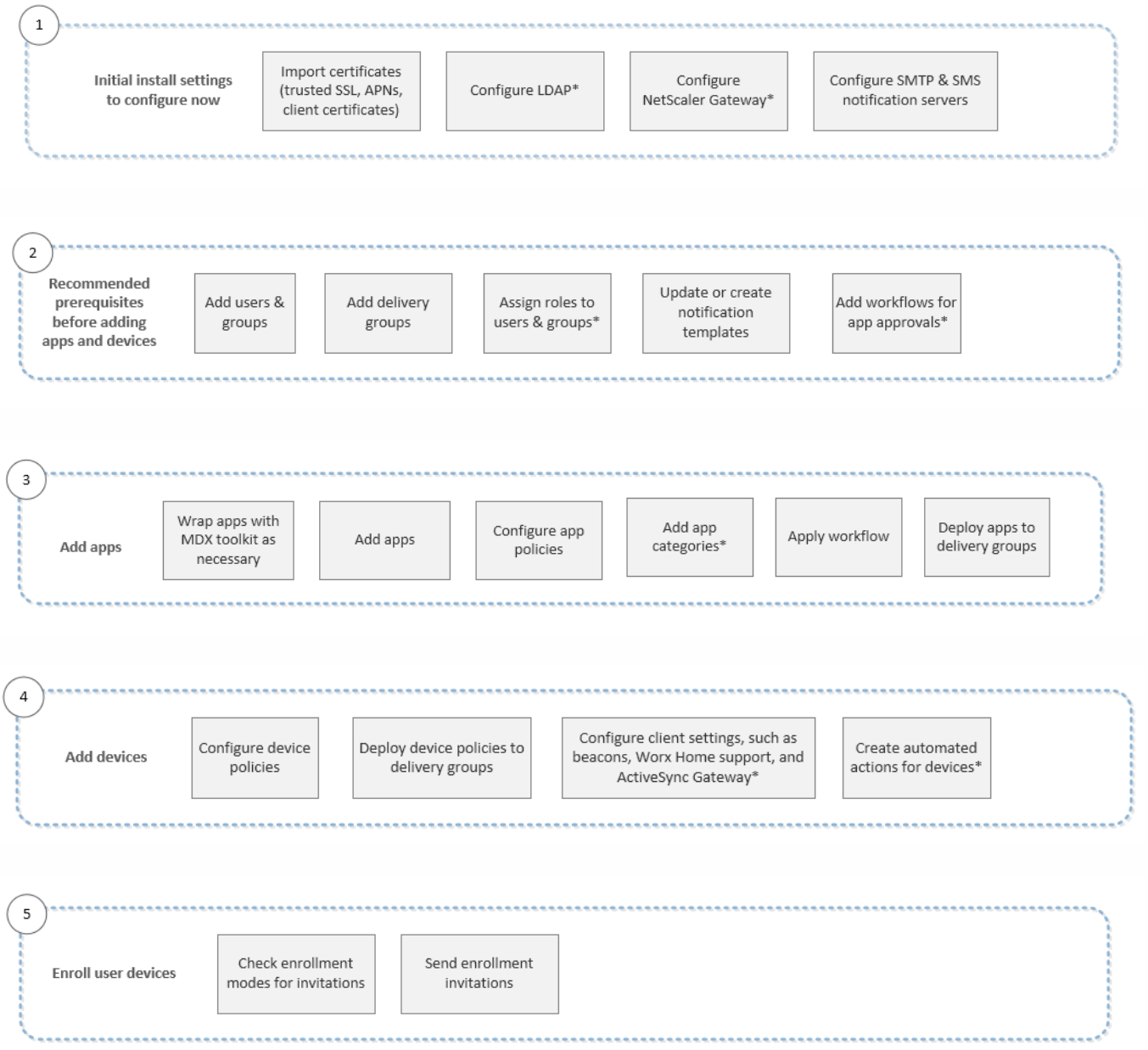
XenMobile 控制台入门

Aug 11, 2016

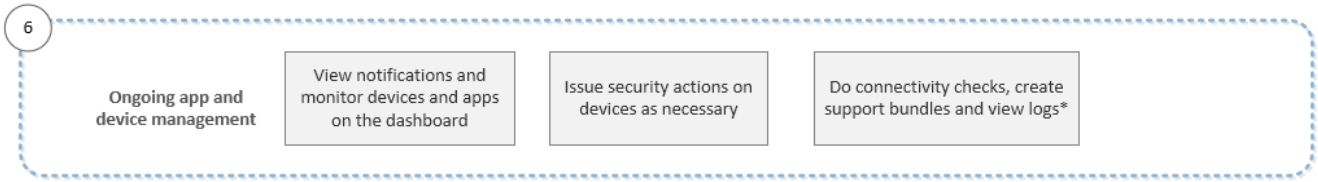
XenMobile 控制台是 XenMobile 中的统一管理工具。 此主题假设您已安装了 XenMobile，并准备好使用此控制台。 如果要安装 XenMobile，请参阅安装 XenMobile。 有关 XenMobile 控制台支持的浏览器的详细信息，请参阅“XenMobile 兼容性”一文中的浏览器支持。

为帮助您了解在控制台中的执行顺序，下图显示了准备正在进行的应用程序和设备管理所需的建议工作流。 第一组建议介绍了您可能在安装步骤中跳过的初始设置。

注意：带星号的项目为可选项目。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



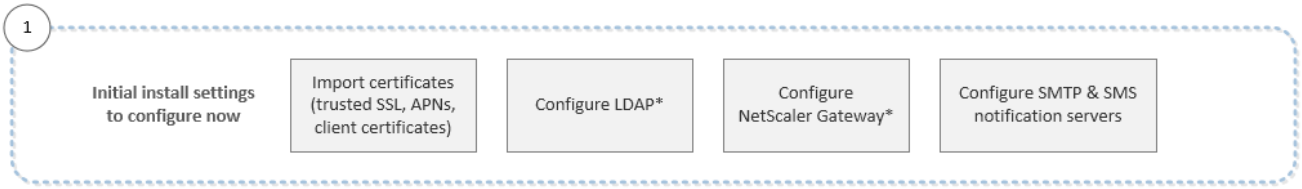
© 1999-2017 Citrix Systems, Inc. All rights reserved.

初始设置工作流

Aug 11, 2016

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。 由于无法返回到初始配置屏幕，如果您已跳过某些安装配置，可以在控制台中配置以下设置。 开始添加用户、应用程序和设备之前，应考虑完成这些安装设置。 开始时，请单击控制台右上角的齿轮图标。 要查看整个流程，请参阅 XenMobile 控制台入门。

注意：带星号的项目为可选项目。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- XenMobile 中的证书
- LDAP 配置
- NetScaler Gateway 和 XenMobile
- XenMobile 中的通知

© 1999-2017 Citrix Systems, Inc. All rights reserved.

控制台必备条件工作流

Oct 21, 2016

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。 如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。 要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示建议在添加应用程序和设备前配置的必备条件。
注意：带星号的项目为可选项目。

有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 配置用户帐户、角色和注册设置
- 在 XenMobile 中管理交付组
- 使用 RBAC 配置角色
- 在 XenMobile 中创建或更新通知模板
- 配置注册模式并启用自助服务门户
- 创建和管理工作流

© 1999-2017 Citrix Systems, Inc. All rights reserved.

添加应用程序工作流

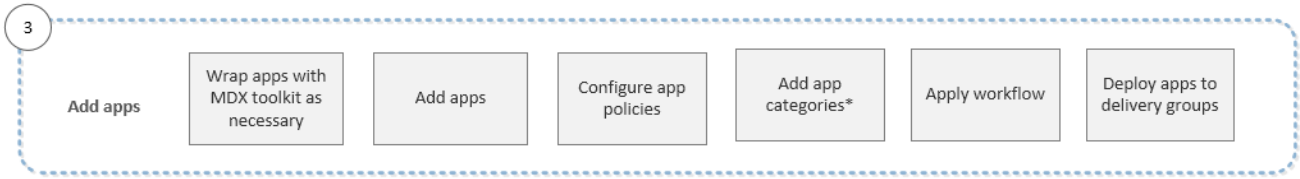
Oct 21, 2016

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。 如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。

接下来，可以按照控制台必备条件工作流中的说明，在添加应用程序和设备之前配置某些必备条件。 要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示了向 XenMobile 中添加应用程序时应遵循的建议顺序。

注意：带星号的项目为可选项目。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 关于 MDX Toolkit
- 向 XenMobile 添加应用程序
- MDX 策略概览
- 添加应用程序类别
- 创建和管理工作流
- 在 XenMobile 中管理交付组

© 1999-2017 Citrix Systems, Inc. All rights reserved.

添加设备工作流

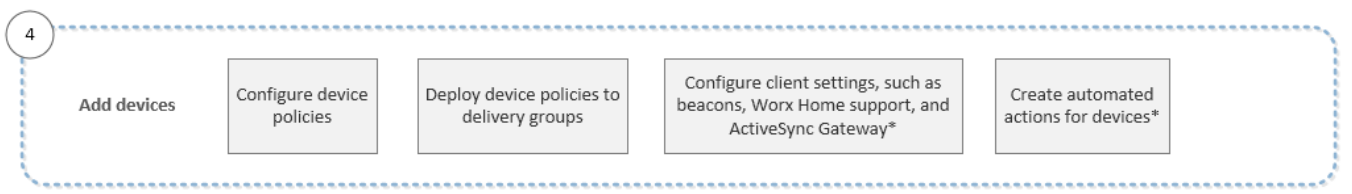
Aug 11, 2016

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。 如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。

接下来，可以按照控制台必备条件工作流中的说明，在添加应用程序和设备之前配置某些必备条件。 然后，您可以按照添加应用程序工作流中的说明添加应用程序。 要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示了向 XenMobile 中添加和注册设备时应遵循的建议顺序。

注意：带星号的项目为可选项目。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 在 XenMobile 中添加设备和查看设备详细信息
- XenMobile 设备策略（按平台）
- 在 XenMobile 中管理交付组
- 配置 XenMobile 客户端设置
- 在 XenMobile 中创建自动化操作

© 1999-2017 Citrix Systems, Inc. All rights reserved.

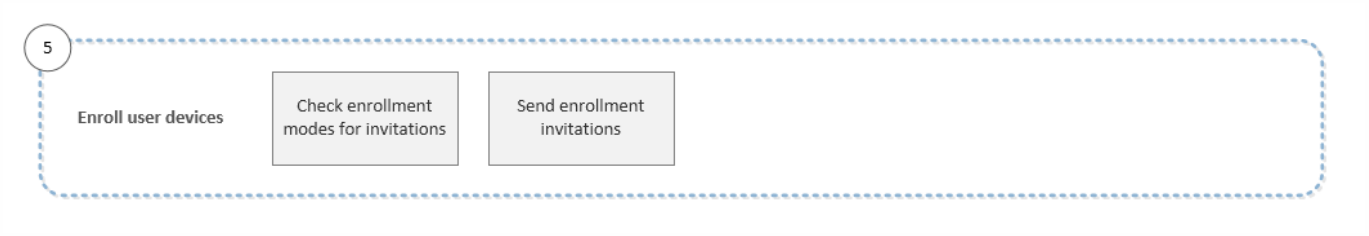
注册用户设备工作流

Aug 11, 2016

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。 如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。

接下来，可以按照控制台必备条件工作流中的说明，在添加应用程序和设备之前配置某些必备条件。 然后，按照添加应用程序工作流中的说明添加应用程序，并按照添加设备工作流中的说明添加和注册设备。 要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示了在 XenMobile 中注册用户设备时应遵循的建议顺序。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 配置用户帐户、角色和注册设置
- 配置注册模式并启用自助服务门户

© 1999-2017 Citrix Systems, Inc. All rights reserved.

正在进行的应用程序和设备管理工作流

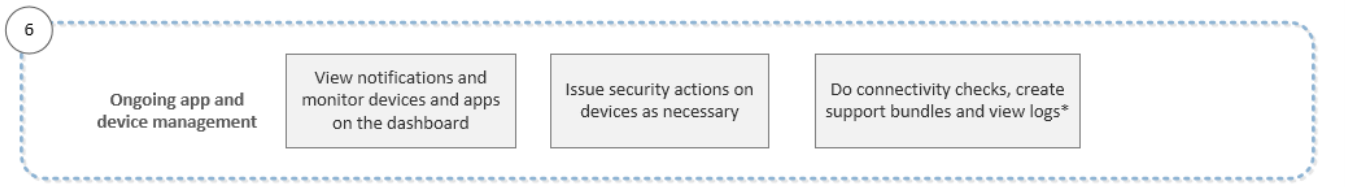
Aug 11, 2016

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。 如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。

接下来，可以按照控制台必备条件工作流中的说明，在添加应用程序和设备之前配置某些必备条件。 然后，按照添加应用程序工作流中的说明添加应用程序，并可以按照添加设备工作流中的说明添加和注册设备。 完成前四个工作流之后，按照注册用户设备工作流中的说明注册用户设备。 要查看整个工作流，请参阅 XenMobile 控制台入门。

第六和最后一个工作流显示正在进行的应用程序和设备管理的建议活动，您可以在控制台中执行这些活动。

注意：带星号的项目为可选项目。



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 控制台中的过滤器和表格

Aug 11, 2016

可以查找整个 XenMobile 控制台中的过滤器和表格。 这些过滤器和表格位于“设备”、“注册”、“设备策略”、“应用程序”、“操作”和“交付组”选项卡上以及“设置”选项卡下的多个页面上。 通过过滤器，您可以缩小控制台的任何区域中的信息的范围，以查找要查看或要对其执行操作的准确信息。 在表格中，您可以单击一个或多个项目以查看用于对选定项目执行操作的选项。 选项可能会随选定的项目数量而变化。

下表列出了某些常用选项及其所在表格。

菜单选项	操作	选项所在的表格
添加	将新项目添加到表格中。	全部
类别	添加和管理应用程序的类别。	应用程序
复制 URL	将 URL 复制到剪贴板。	注册
删除或全部删除	永久删除选定项目。	全部
部署	将资源部署到用户和设备。	设备和交付组
禁用	禁用某个应用程序或 AllUsers 交付组。	应用程序和交付组
编辑	更改现有项目。	除“注册”外的所有表格
导出	将表格的内容发送到 .csv 文件。	全部
导入	从置备文件中添加设备。	设备
	从文件中添加本地用户和组。	本地用户和组
管理本地组	添加本地组用于管理。	本地用户和组
通知	将通知发送到选定用户和设备。	“注册”和“设备”
刷新	更新表格。	设备
安全	调用选定设备上的安全选项。	设备
自助服务门户	启用自助服务门户作为注册模式。	注册

© 1999-2017 Citrix Systems, Inc. All rights reserved.

菜单选项	操作	选项所在的表格
更新	更新表格中的值。	版本管理

在 XenMobile 控制台中查看表格中的选项

要在控制台中针对表格中的信息采取操作，可以采用几种不同的方式查看各种选项：

- 可以选中某个项目旁边的复选框以在列表上方显示选项菜单。
- 可以选中多个项目旁边的复选框以同时对所有选定项目执行操作。 能够对多个项目执行的操作取决于正在查看的表格。
- 可以单击列表中的某个项目以在此列表的右侧显示选项菜单。 单击显示更多将显示与该项目有关的详细信息。 显示的详细信息取决于正在查看的表格。
- 可以在搜索框中键入完整名称或部分名称，以限制列出的项目数。

控制台的“设备策略”区域中每个页面仅列出 10 项。 单击页面右下角的三角形可以向前和向后移动页面。

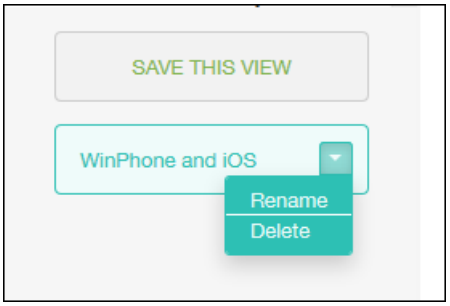
在 XenMobile 控制台中过滤信息

要在控制台的某个区域中查看信息的特定子集，例如“设备”、“注册”、“设备策略”、“应用程序”、“操作”、“交付组”和“本地用户和组”，可以根据选择的条件过滤列表。 此过程以“设备”页面为例，但过滤步骤在整个控制台中均相同。

1. 在设备页面，单击显示过滤器。
   此时将显示过滤器面板，其中列出了过滤设备列表可以依据的条件。 首次显示过滤器时，所有条件 处于折叠状态。
2. 单击过滤器左侧的三角形可显示该过滤器可以使用的条件。 每个条件右侧的数字表示满足该条件的设备数。
3. 选择要使用的过滤条件。 设备列表被限制到满足选定条件的设备。
4. 执行以下操作之一：
   - 单击 Hide Filter（隐藏过滤器）以继续使用过滤后的列表。
   - 单击全部清除以还原到完整列表。
   - 单击特定条件旁边的清除可删除该过滤器，并从过滤后的列表中删除这些项目。
5. 如果要将所选条件另存为自定义过滤器，请在过滤器面板底部的 Save the filter（保存过滤器）字段中，键入描述性名称，然后单击完成。 如果决定不保存过滤器，请单击取消。

6. 保存过滤器后，可以在过滤器面板底部选中该过滤器以过滤表格中的信息。
   注意：如果单击过滤器名称右侧的三角形，则可以重命名或删除该过滤器。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 中的报告

Aug 11, 2016

XenMobile 提供 10 种预定义报告，您可以利用这些报告分析应用程序和设备部署情况。

- **应用程序(按设备和用户)** – 列出用户设备上具有的应用程序。
- **条款和条件** – 列出接受条款和条件协议和拒绝条款和条件协议的用户。
- **排名前 25 的应用程序** – 列出用户在其设备上使用最多的 25 个应用程序。
- **已越狱/获得 Root 权限的设备** – 列出获得 Root 权限的 iOS 设备和已越狱的 Android 设备。
- **排名前 10 的应用程序 - 部署失败**：列出部署失败的应用程序。
- **非活动设备** – 列出处于非活动状态的时间已达到指定时间段的设备。
- **应用程序(按类型和类别)** – 按版本、类型和类别列出应用程序。
- **设备注册** – 列出在指定时间段内已注册的设备。
- **应用程序(按平台)** – 按设备平台和版本列出应用程序和应用程序版本。
- **设备和应用程序** – 列出所有设备、设备数据和已安装的托管应用程序。

报告采用 .csv 格式，您可以使用 Microsoft Excel 等程序打开此类文件。 下表列出了标题和使用这些标题的报告。

标题	说明	使用位置
ACCEPTANCE_STATUS	条款和条件接收状态	条款和条件
APP_CATEGORY	应用程序在设备上显示的类别（例如，公共应用商店应用程序或企业应用程序）	排名前 10 的应用程序 - 部署失败、应用程序(按类型和类别)、设备和应用程序
APP_ID	唯一应用程序标识符	设备和应用程序
APP_NAME	应用程序名称	排名前 25 的应用程序、排名前 10 的应用程序 - 部署失败、应用程序(按类型和类别)、设备和应用程序
APP_OWNER	应用程序所有者（例如，Worx 应用程序的所有者为 Citrix.com）	排名前 25 的应用程序、排名前 10 的应用程序 - 部署失败、应用程序(按类型和类别)、应用程序(按平台)、设备和应用程序
APP_TYPE	应用程序类型（例如，公共应用商店或企业）	排名前 25 的应用程序、排名前 10 的应用程序 - 部署失败、应用程序(按类型和类别)、设备和应用程序
APP_VERSION	应用程序版本	排名前 25 的应用程序、排名前 10 的应用程序 - 部署失败、应用程序

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		(按类型和类别)、应用程序(按平台)、设备和应用程序
APPS_ON_DEVICE	设备上已安装的应用程序数	应用程序(按设备和用户)
CERTIFICATE_EXPIRATION	设备证书过期日期	设备和应用程序
CREATION_DATE	条款和条件文件创建的日期	条款和条件
DELIVERY_GROUP	与已部署资源关联的交付组	条款和条件
DEPLOYMENT_DATE	资源的部署日期	排名前 25 的应用程序、排名前 10 的应用程序 - 部署失败、应用程序(按类型和类别)、设备和应用程序
DEPLOYMENT_SUCCESS、DEPLOYMENT_FAILED、DEPLOYMENT_PENDING	部署状态	应用程序(按设备和用户)、排名前 25 的应用程序、排名前 10 的应用程序 - 部署失败、应用程序(按类型和类别)、应用程序(按平台)、设备和应用程序
DEPLOYMENT_TOTAL	尝试部署的总次数	排名前 25 的应用程序、排名前 10 的应用程序 - 部署失败、应用程序(按类型和类别)、应用程序(按平台)、设备和应用程序
DEVICE_MODE	设备模式（托管或未托管）	已越狱/获得 Root 权限的设备、不活动设备、设备注册、设备和应用程序
DEVICE_OWNERSHIP	设备所有权分类方式（BYOD、企业或未知）	设备和应用程序
DEVICE_PLATFORM	设备平台	应用程序(按平台)
DEVICE_STATUS	设备兼容性状态	设备和应用程序
DEVICE_VERSION	设备操作系统版本号	应用程序(按平台)
DOCUMENT_NAME	条款和条件文件名	条款和条件

© 1999-2017 Citrix Systems, Inc. All rights reserved.

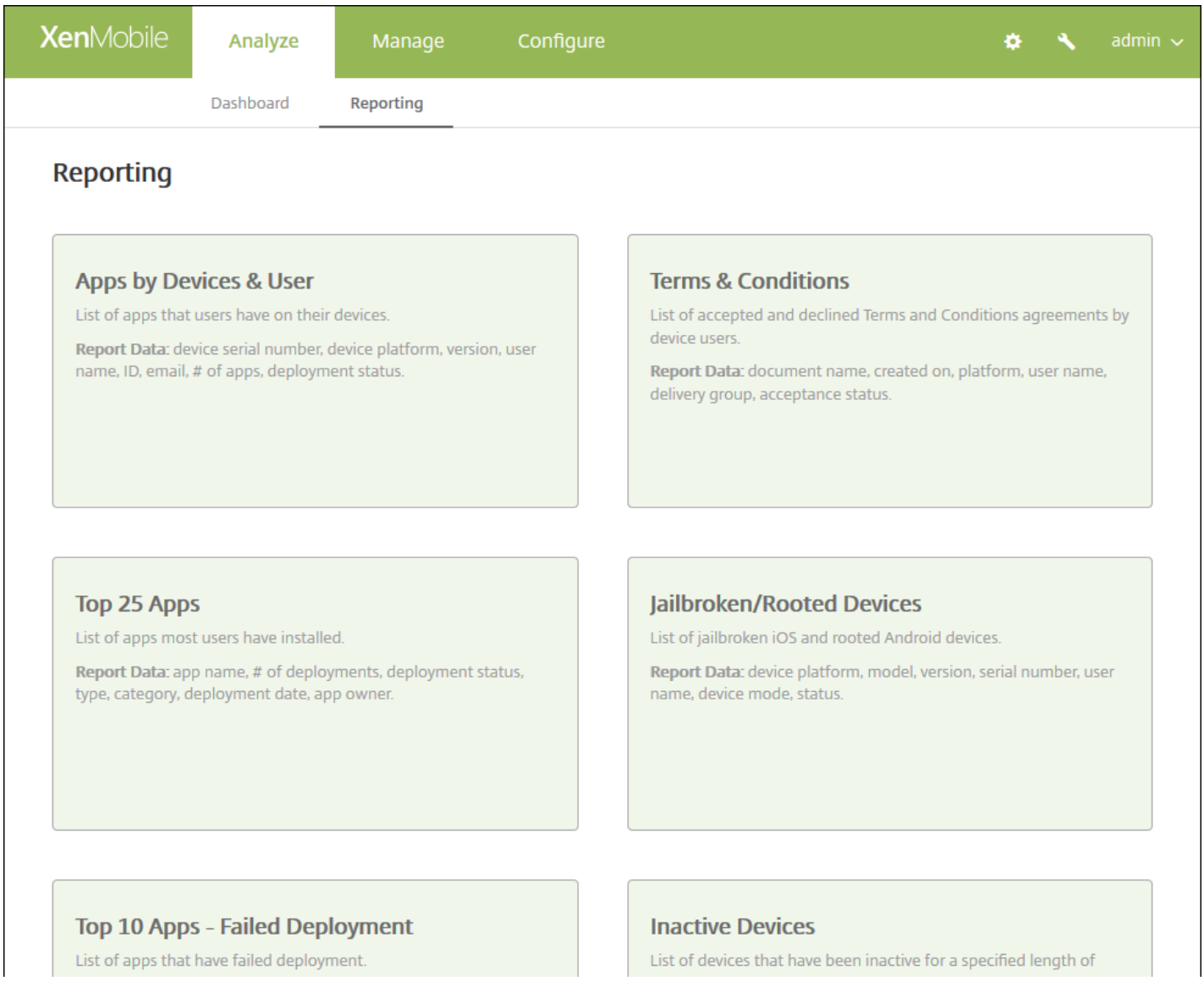
EMAIL	用户电子邮件地址	设备和应用程序
ENROLLMENT_DATE	设备在 XenMobile 中的注册时间	设备和应用程序
ENROLLMENT_STATUS	设备注册状态（已注册或未注册）	设备和应用程序
FIRST_CONNECTION_DATE	设备首次连接到 XenMobile 的日期	非活动设备、设备注册
IMEI	国际移动设备标识 (IMEI) 号	非活动设备
LAST_ACTIVITY	设备上次活动日期	非活动设备
LAST_AUTH_DATE	设备上次向 XenMobile 进行身份验证的日期	非活动设备、设备注册、设备和应用程序
LAST_USERNAME	与设备关联的姓氏	已越狱/获得 Root 权限的设备、非活动设备、设备注册
LOCATION	设备的地理位置	设备和应用程序
MANAGED	设备是否托管	已越狱/获得 Root 权限的设备
MODEL	设备型号	已越狱/获得 Root 权限的设备、非活动设备、设备注册、应用程序(按平台)
MODEL_NAME	设备型号	设备和应用程序
OS_VERSION	设备上的操作系统版本	应用程序(按设备和用户)、非活动设备、设备注册、设备和应用程序
PHONE_NUMBER	用户的电话号码	设备注册
PLATFORM	设备平台	应用程序(按设备和用户)、条款和条件、已越狱/获得 Root 权限的设备、非活动设备、设备注册、设备和应用程序
SERIAL_NUMBER	设备序列号	应用程序(按设备和用户)。 已越狱/

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		获得 Root 权限的设备、非活动设备、设备和应用程序
USER EMAIL	用户电子邮件地址	应用程序(按设备和用户)
USER_ID	用户的唯一编号	设备和应用程序
USER_NAME	用户名	应用程序(按设备和用户)、条款和条件、设备和应用程序
USERID	用户 ID	应用程序(按设备和用户)

按照以下步骤创建报告：

1. 在 XenMobile 控制台中，单击**分析**选项卡，然后单击**报告**。 此时将显示**报告**页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

time.

Report Data: last activity, device mode, platform, version, user name, last authentication, device IMEI, serial number, model, first connection.

Apps by Type & Category

List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

Device Enrollment

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

Devices & Apps

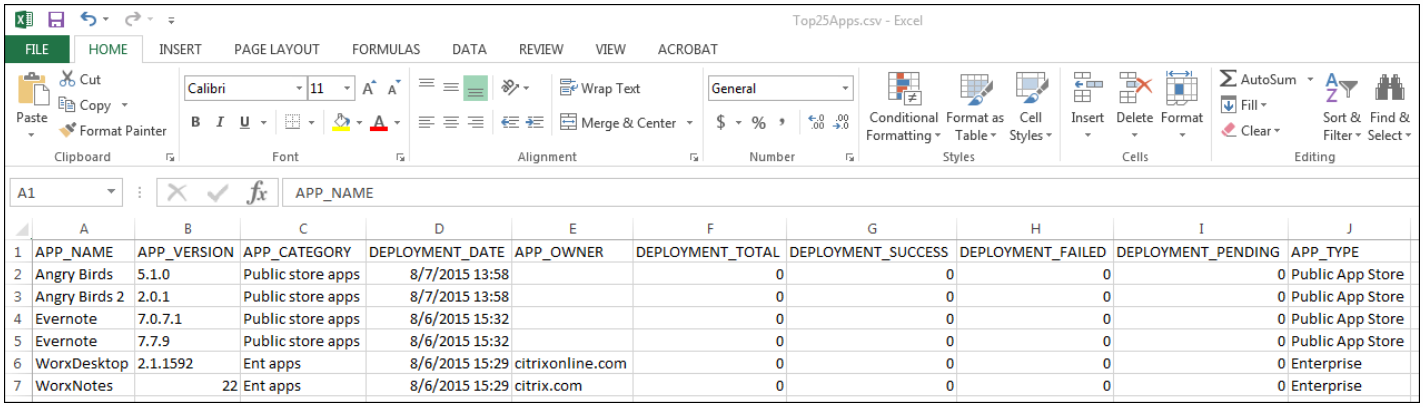
List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

2. 单击要创建的报告。 根据您所使用的浏览器，系统会自动下载文件或询问您是否保存文件。

3. 为要创建的每个报告重复步骤 2。

以下是使用 Microsoft Excel 打开的“排名前 25 的应用程序”报告示例：



	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORY	DEPLOYMENT_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	Angry Birds	5.1.0	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
3	Angry Birds 2	2.0.1	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
4	Evernote	7.0.7.1	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
5	Evernote	7.7.9	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
6	WorxDesktop	2.1.1592	Ent apps	8/6/2015 15:29	citrixonline.com	0	0	0	0	Enterprise
7	WorxNotes	22	Ent apps	8/6/2015 15:29	citrix.com	0	0	0	0	Enterprise

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通知

Aug 11, 2016

可以将 XenMobile 中的通知用于以下目的：

- 与选择的用户组通信以使用多个系统相关功能。 您也可以将这些通知发送给特定用户，如使用 iOS 设备的所有用户、设备不合规的用户、使用员工自带设备的用户等。
- 注册用户及其设备
- 在满足某些条件时自动通知用户（使用自动化操作），例如，由于合规性问题阻止用户设备访问企业域时，或设备已被越狱或获得 Root 权限时。 有关自动化操作的详细信息，请参阅自动化操作。

要使用 XenMobile 发送通知，必须配置网关和通知服务器。 可以在 XenMobile 中设置通知服务器，以配置简单邮件传输协议 (SMTP) 和短信服务 (SMS) 网关服务器，以便向用户发送电子邮件和文本 (SMS) 通知。 可以使用通知经两种不同的通道发送消息：SMTP 或 SMS。

- SMTP 是面向连接的文本协议，邮件发送方通常通过传输控制协议 (TCP) 发布命令字符串并提供必需的数据，从而与邮件接收方通信。 SMTP 会话包括来自 SMTP 客户端（邮件发送人员）的命令和来自 SMTP 服务器的相应响应。
- SMS 是手机、Web 或移动通信系统的文本消息服务。 它使用标准化通信协议，使固定线路或移动电话设备可以交换短文本消息。

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 网关发送和接受来往于电信网络的 SMS 传输。 这些基于文本的消息使用标准化通信协议，允许固定线路或移动电话设备交换短文本消息。

本文中的过程讨论如何配置 SMTP 服务器和 SMS 网关，以及运营商 SMS 网关。

必备条件

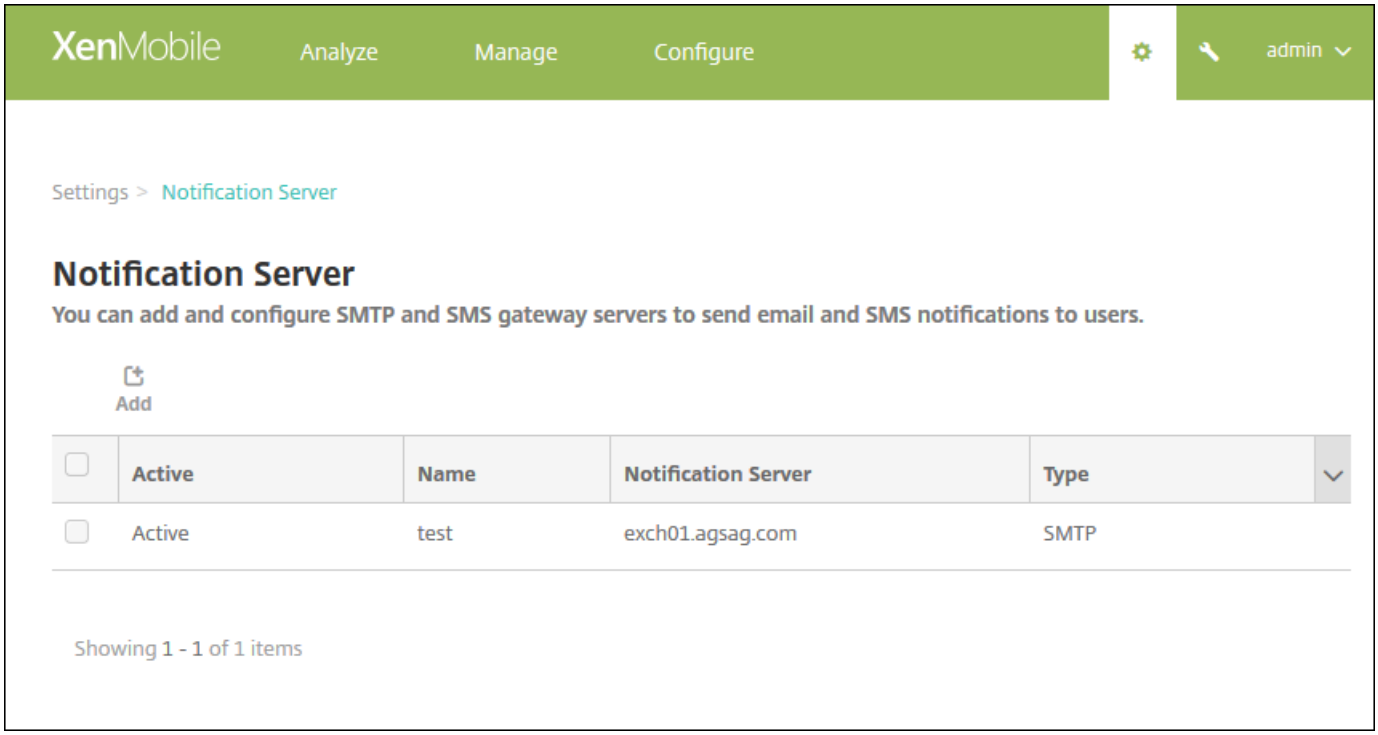
- 配置 SMS 网关之前，请咨询系统管理员以确定服务器信息。 了解 SMS 服务器是否托管在内部企业服务器上或者服务器是否属于托管电子邮件服务（在这种情况下，您需要服务提供商 Web 站点上的信息）至关重要。
- 必须配置 SMTP 通知服务器才能向用户发送消息。 如果此服务器托管在内部服务器上，请联系系统管理员以获取配置信息。 如果此服务器是托管的邮件服务，请在服务提供商的 Web 站点上查找相应的配置信息。
- 同一时间只能激活一个 SMTP 服务器和一个 SMS 服务器。
- 必须从位于网络的 DMZ 中的 XenMobile 打开端口 25 以指回内部网络上的 SMTP 服务器，以便能够成功发送通知。

配置 SMTP 服务器和 SMS 网关

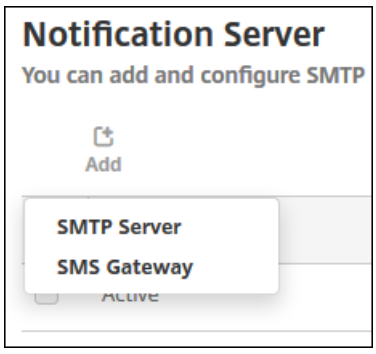
1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

2. 在**通知**下面，单击**通知服务器**。 此时将显示**通知服务器**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



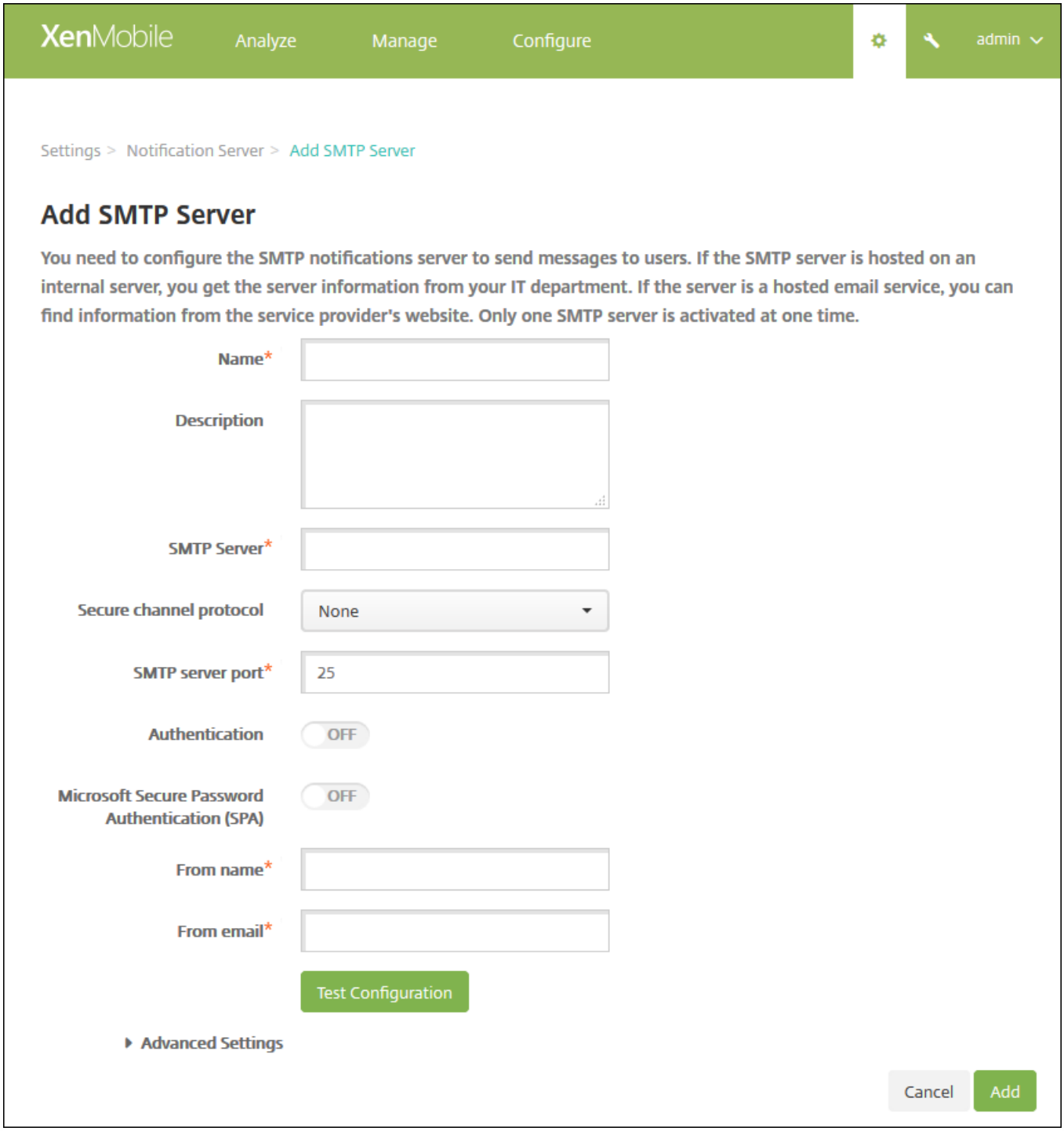
2. 单击**添加**。 此时将显示一个菜单，其中包含用于配置 SMTP 服务器或 SMS 网关的选项。



- 要添加 SMTP 服务器，请单击 **SMTP 服务器**，然后参阅添加 SMTP 服务器了解配置此设置的步骤。
- 要添加 SMS 网关，请单击 **SMS 网关**，然后参阅添加 SMS 网关了解配置此设置的步骤。

添加 SMTP 服务器

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. 配置以下设置：

- **名称**：键入与此 SMTP 服务器帐户关联的名称。
- **说明**：可选，输入服务器的说明。
- **SMTP 服务器**：键入服务器的主机名。 主机名可以是完全限定的域名 (FQDN) 或 IP 地址。
- **安全通道协议**：在列表中，单击服务器使用的相应安全通道协议（如果服务器配置为使用安全身份验证）**SSL**、**TLS** 或**无**。默认值为**无**。
- **SMTP 服务器端口**：键入 SMTP 服务器使用的端口。 默认情况下，此端口设置为 25；如果 SMTP 连接使用 SSL 安全通道协议，则此端口设置为 465。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **身份验证**：选择**开**或**关**。 默认值为**关**。
- 如果启用**身份验证**，可以配置以下设置：
  - **用户名**：键入进行身份验证时使用的用户名。
  - **密码**：键入身份验证用户的密码。
- **Microsoft 安全密码身份验证(SPA)**：如果 SMTP 服务器使用的是 SPA，请单击**开**。 默认值为**关**。
- **发件人姓名**：键入客户端接收来自此服务器的通知电子邮件时，显示在**发件人**框中的名称。 例如，公司 IT。
- **发件人电子邮件**：键入电子邮件收件人回复 SMTP 服务器发送的通知时使用的电子邮件地址。

2. 单击**测试配置**以发送测试电子邮件通知。

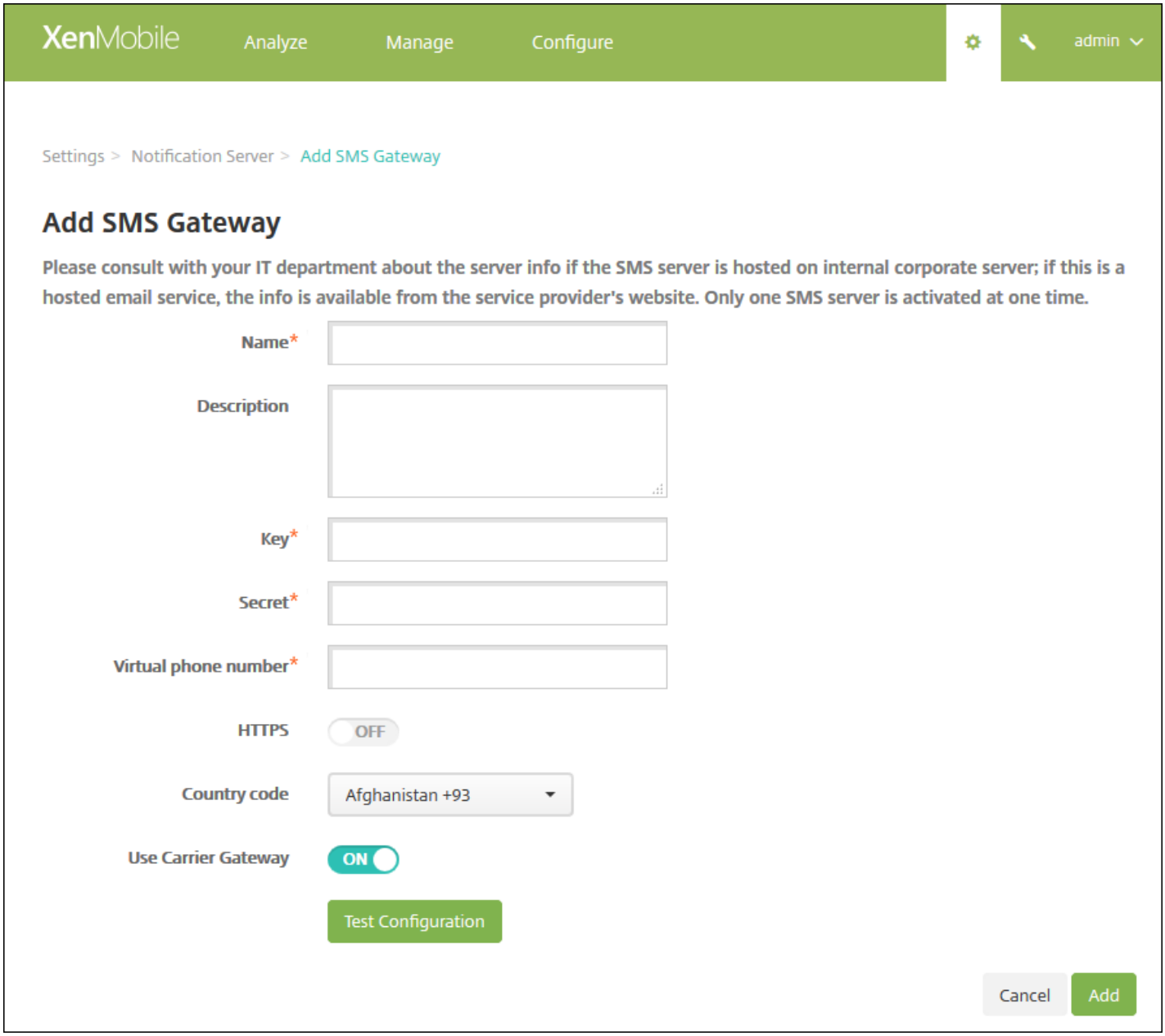
3. 展开**高级设置**，然后配置以下设置：

- **SMTP 重试次数**：键入 SMTP 服务器发送邮件失败的重试次数。 默认值为 5。
- **SMTP 超时**：键入发送 SMTP 请求时等待的持续时间（以秒为单位）。 如果频繁出现因超时导致消息发送失败的情况，请增加此值。 降低此值时请格外小心；此操作可增加超时次数和未送达的消息。 默认值为 30 秒。
- **最大 SMTP 收件人数**：键入 SMTP 服务器发送的每个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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



注意

XenMobile 仅支持 Nexmo SMS 消息传递。 如果尚未具有使用 NexMo 消息传递的帐户，请访问其 Web 站点以创建帐户。

1. 配置以下设置：

- **名称**：键入 SMS 网关配置的名称。 此字段为必填字段。
- **说明**：可选，键入配置的说明。
- **密钥**：键入系统管理员在激活帐户时提供的数字标识符。 此字段为必填字段。
- **密码**：键入系统管理员提供的密码，当密码丢失或被盗时用于访问您的帐户。 此字段为必填字段。
- **虚拟电话号码**：向北美电话号码（前缀为 +1）发送时使用此字段。 必须键入 Nexmo 虚拟电话号码；否则，请键入有意义的标签或名称。 可以在 Nexmo Web 站点上购买虚拟电话号码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **HTTPS**：如果是否使用 HTTPS 将 SMS 请求传输到 Nexmo。 默认值为**关**。
- **国家/地区代码**：在此列表中，单击贵组织收件人的默认 SMS 国家/地区代码前缀。 此字段始终以 + 符号开头。 默认值为**阿富汗 +93**。

2. 单击**测试配置**以使用当前的配置发送测试消息。 系统将立即检测并显示连接错误，如身份验证或虚拟电话号码错误。 接收消息的时间范围与移动电话之间发送消息的时间范围相同。

2. 单击**添加**。

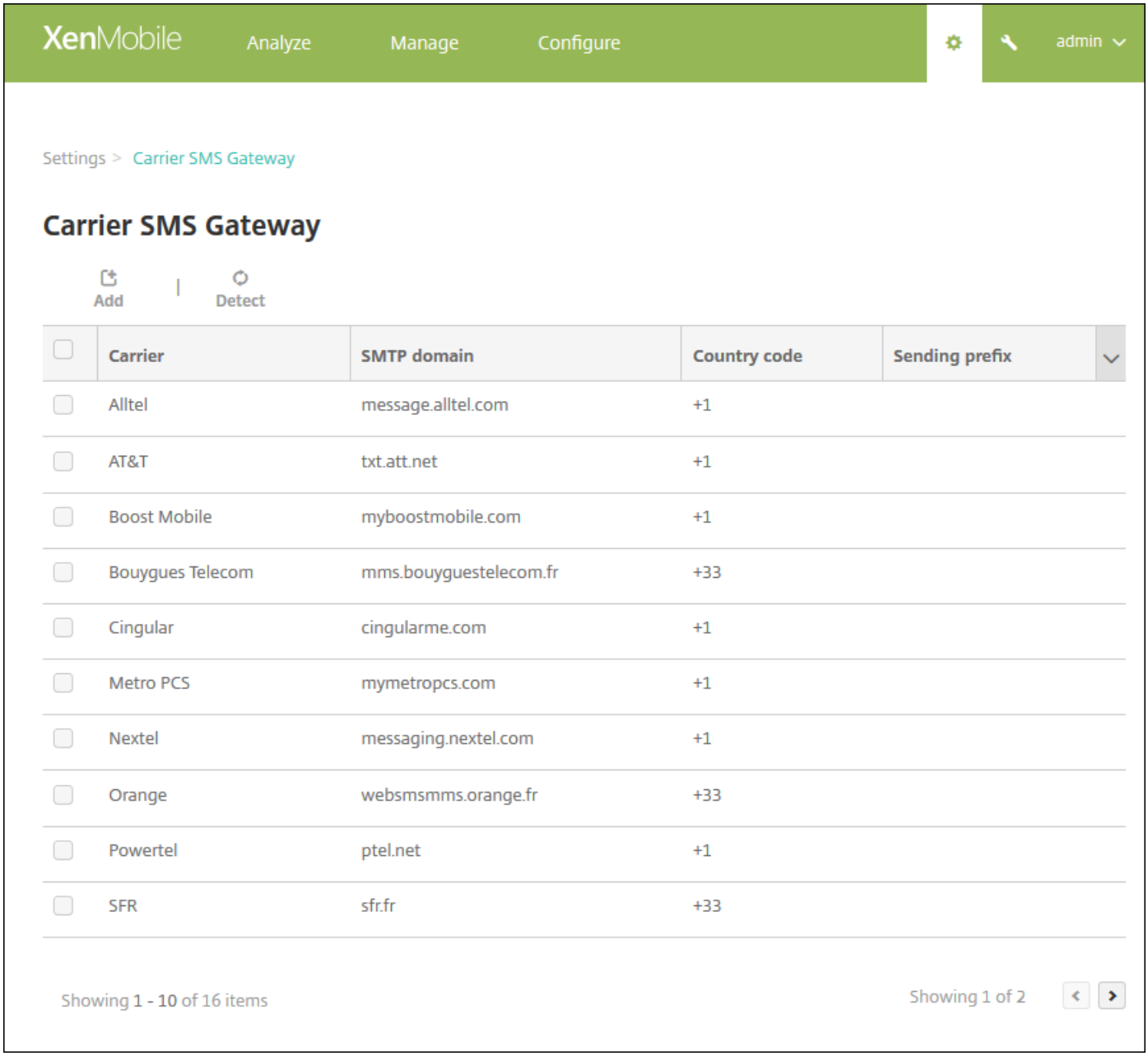
添加运营商 SMS 网关

您可以在 XenMobile 中设置运营商 SMS 网关，以配置通过运营商的 SMS 网关发送的通知。 运营商使用短信服务 (SMS) 网关发送或接受来往于电信网络的 SMS 传输。 这些基于文本的消息使用标准化通信协议，允许固定线路或移动电话设备交换短文本消息。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

2. 在**通知**下面，单击**运营商 SMS 网关**。 此时将显示**运营商 SMS 网关**页面。

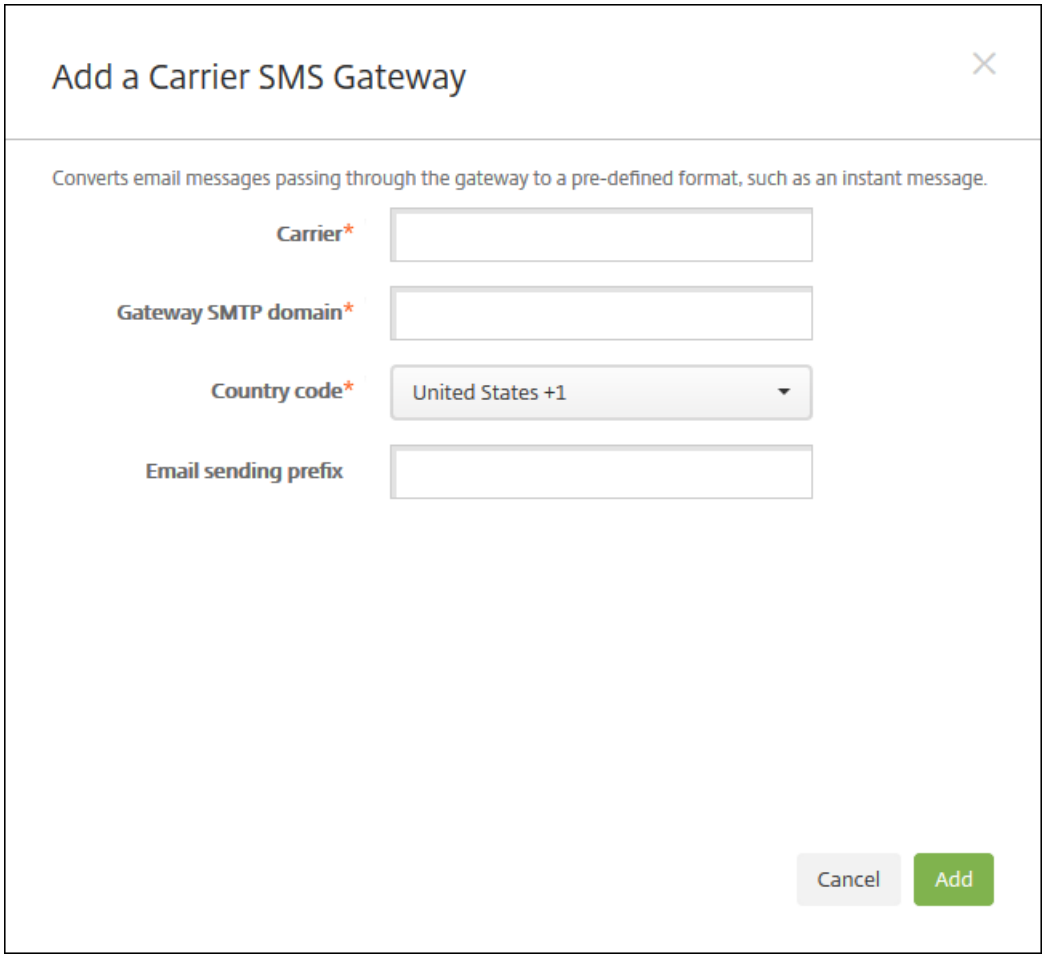
© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 执行以下操作之一：

- 单击**检测**以自动发现网关。 此时将显示一个对话框，指出没有检测到新的运营商或列出在已注册设备中间检测到的新运营商。
- 单击**添加**。 此时将显示 **Add a Carrier SMS Gateway**（添加运营商 SMS 网关）对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



注意：XenMobile 仅支持 Nexmo SMS 消息传递。 如果尚未具有使用 NexMo 消息传递的帐户，请访问其 Web 站点以创建帐户。

4. 配置以下设置：

- **运营商**：键入运营商的名称。
- **网关 SMTP 域**：键入与 SMTP 网关关联的域。
- **国家/地区代码**：在列表中，单击运营商的国家/地区代码。
- **电子邮件发送前缀**：可选，指定电子邮件发送前缀。

5. 单击**添加**以添加新运营商，或单击**取消**不添加新运营商。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway 和 XenMobile

Oct 21, 2016

使用 XenMobile 配置 NetScaler Gateway 时，为远程设备访问内部网络建立身份验证机制。 利用此功能，移动设备上的应用程序可以访问位于 Intranet 上的企业服务器，方法是在设备上的应用程序与 NetScaler Gateway 之间创建 Micro VPN。 可以在 XenMobile 控制台中配置 NetScaler Gateway。

注意：有关 XenMobile 支持的 NetScaler Gateway 版本，请参阅 XenMobile 兼容性。 有关在 NetScaler 上为 XenMobile 设置 NetScaler Gateway 的信息，请参阅为 XenMobile 环境配置设置。

身份验证

在 XenMobile 操作过程中，会使用多个组件进行身份验证：

- **XenMobile 服务器**：您可以在 XenMobile 服务器上定义注册所涉及的安全性以及注册体验。 对于首次加入的用户，选项包括允许所有人注册还是仅允许收到邀请的人注册，以及要求双重身份验证还是三重身份验证。 通过 XenMobile 中的客户端属性，您可以启用 Worx PIN 身份验证，并配置 PIN 的复杂度和过期时间。
- **NetScaler**：NetScaler 可用于终止 Micro VPN SSL 会话、提供网络传输安全性以及定义每次用户访问应用程序时的身份验证体验。
- **Worx Home**：在注册操作中，Worx Home 会与 XenMobile 服务器结合使用。 Worx Home 是设备上与 NetScaler 通信的实体：如果会话过期，Worx Home 会从 NetScaler 获得身份验证票据并将其传送至 MDX 应用程序。 Citrix 建议使用证书固定，这样可以防止中间人攻击。 有关详细信息，请参阅 Worx Home 文章中有关证书固定的部分。

  此外，Worx Home 还可以为 MDX 安全容器提供支持：Worx Home 可以推送策略、在应用程序超时后创建与 NetScaler 的新会话，以及定义 MDX 超时和身份验证体验。 Worx Home 还会负责进行越狱检测、地理位置检查以及实施您应用的任何策略。

- **MDX 策略**：MDX 策略可在设备上创建数据保管库。 MDX 策略会将 Micro VPN 连接指回 NetScaler、强制执行脱机模式限制，以及强制执行客户端策略（例如超时）。

有关身份验证（包括单重和双重身份验证方法）、策略、设置和身份验证中涉及的客户端属性的详细信息，以及从最低安全性到最高安全性的三个 XenMobile 配置示例，请参阅身份验证。

有关配置详细信息，请参阅以下文章：

配置域和安全令牌身份验证

配置客户端证书身份验证

配置 XenMobile 以进行证书和安全令牌身份验证

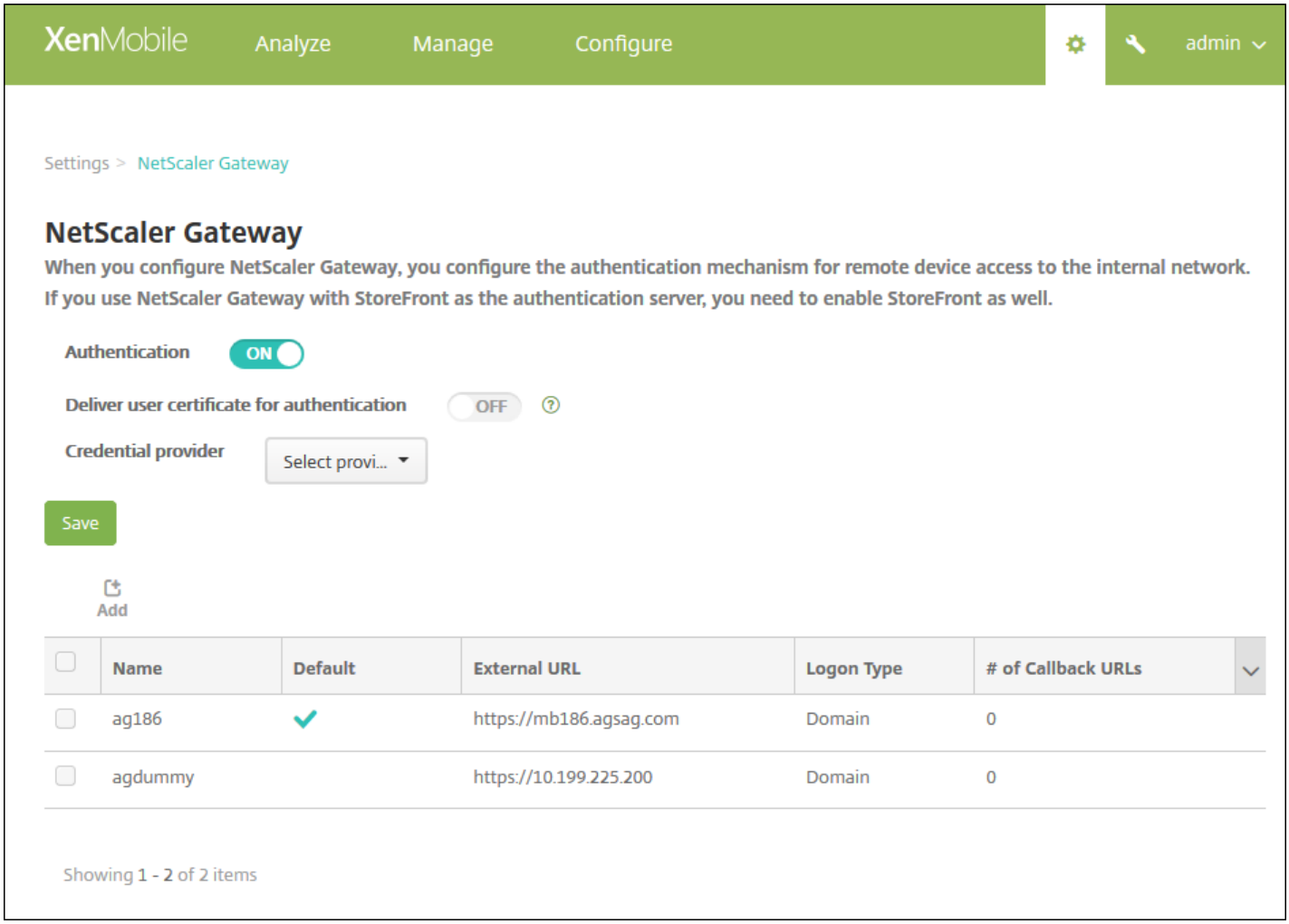
将 XenMobile 和 ShareFile 应用程序配置为使用 SAML 进行单点登录

配置 NetScaler Gateway

1. 在 XenMobile Web 控制台中，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

2. 在**服务器**下面，单击 **NetScaler Gateway**。 此时将显示 **NetScaler Gateway** 页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **身份验证**：选择是否启用身份验证。 默认值为 **ON**。
- **向用户提供用于身份验证的证书**：选择是否希望 XenMobile 与 Worx Home 共享身份验证证书，以便 NetScaler Gateway 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。

3. 单击**保存**。

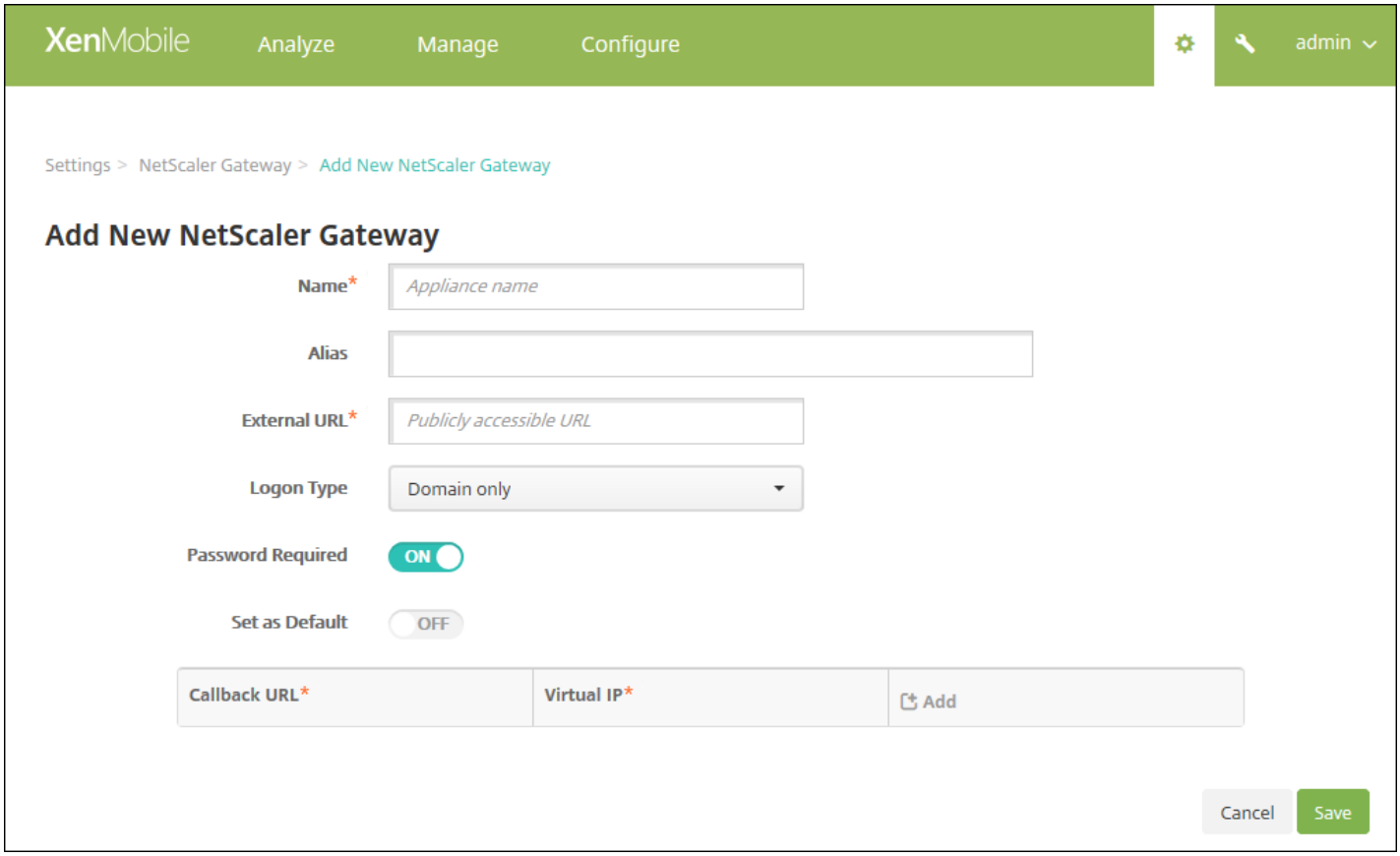
添加新的 NetScaler Gateway 实例

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将打开**设置**页面。

2. 在**服务器**下面，单击 **NetScaler Gateway**。 此时将显示 **Netscaler Gateway** 页面。

3. 单击**添加**。 此时将显示**添加新的 NetScaler Gateway** 页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 配置以下设置：

- **名称**：键入 NetScaler Gateway 实例的名称。
- **别名**：可以选择包含别名。
- 外部 URL：键入 NetScaler Gateway 的公共访问 URL。 例如，https://receiver.com。
- **登录类型**：在列表中，单击某个登录类型。 类型包括**仅限域**、**仅限安全令牌**、**域和安全令牌**、**证书**、**证书和域**以及**证书和安全令牌**。 默认值为**仅限域**。

  如果您拥有多个域，**仅限域**类型将不可用，您必须使用**证书和域**。 对于某些选项，例如**仅限域**，无法更改**密码**字段。

  对于此登录类型，此字段始终为**开**。 此外，**需要密码**字段的默认值会根据所选的**登录类型**发生变化。

  如果使用**证书和安全令牌**，则需要在 NetScaler Gateway 上设置一些其他配置才能支持 Worx Home。 有关信息，请参阅配置 XenMobile 以进行证书和安全令牌身份验证。
- **需要密码**：选择是否希望使用需要密码的身份验证。 默认值为 **ON**。
- **设为默认值**：选择是否将此 NetScaler Gateway 用作默认选项。 默认值为**关**。

5. 单击**保存**。 此时 NetScaler Gateway 已添加并显示在表格中。 可以通过单击列表中的名称编辑或删除实例。

添加 NetScaler Gateway 实例后，可以添加一个回调 URL 并指定 NetScaler Gateway VPN 虚拟 IP 地址。 **注意**：这是可选字段，但是可以进行配置以增强安全性，特别是当 XenMobile 服务器位于 DMZ 时。

1. 在 NetScaler Gateway 屏幕中，选择表格中的 NetScaler Gateway，然后单击**添加**。 此时将显示**添加新的 NetScaler Gateway** 页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 在列出回调 URL 的表格中，单击**添加**。

3. 指定回调 URL。 此字段表示完全限定的域名 (FQDN)，并验证请求是否来自 NetScaler Gateway。

4. 输入 NetScaler Gateway 虚拟 IP 地址，然后单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

LDAP 配置

Aug 15, 2016

在 XenMobile 中，可以配置到一个或多个与轻型目录访问协议 (LDAP) 兼容的目录（如 Active Directory）的连接。 然后，使用 LDAP 配置来导入组、用户帐户和相关属性。 LDAP 是一个独立于供应商的开源应用程序协议，用于通过 Internet 协议 (IP) 网络访问和维护分布式目录信息服务。 目录信息服务用于共享通过网络可用的用户、系统、网络、服务和应用程序信息。 LDAP 的常见用处是为用户提供单点登录 (SSO)，即每个用户在多项服务之间共享一个密码，使用户登录一次公司 Web 站点之后，即可自动登录到公司的 Intranet。

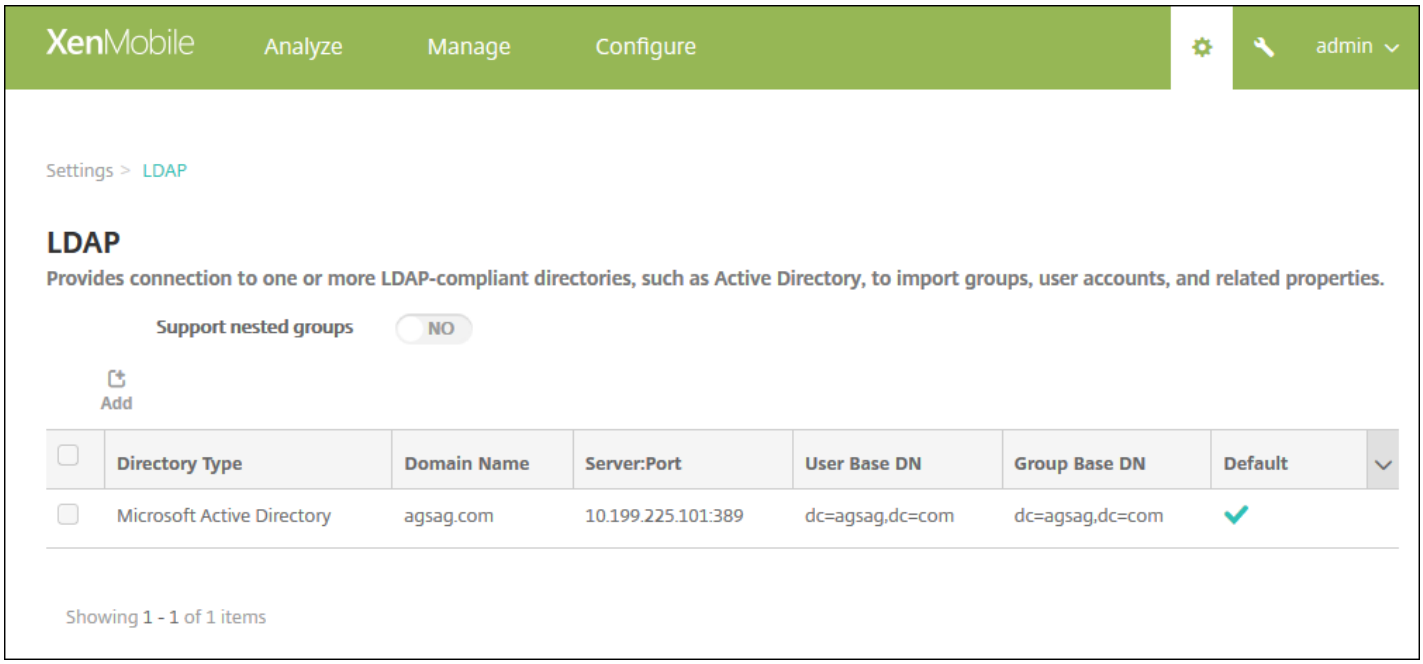
LDAP 的工作方式

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

在 XenMobile 中添加 LDAP 连接

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

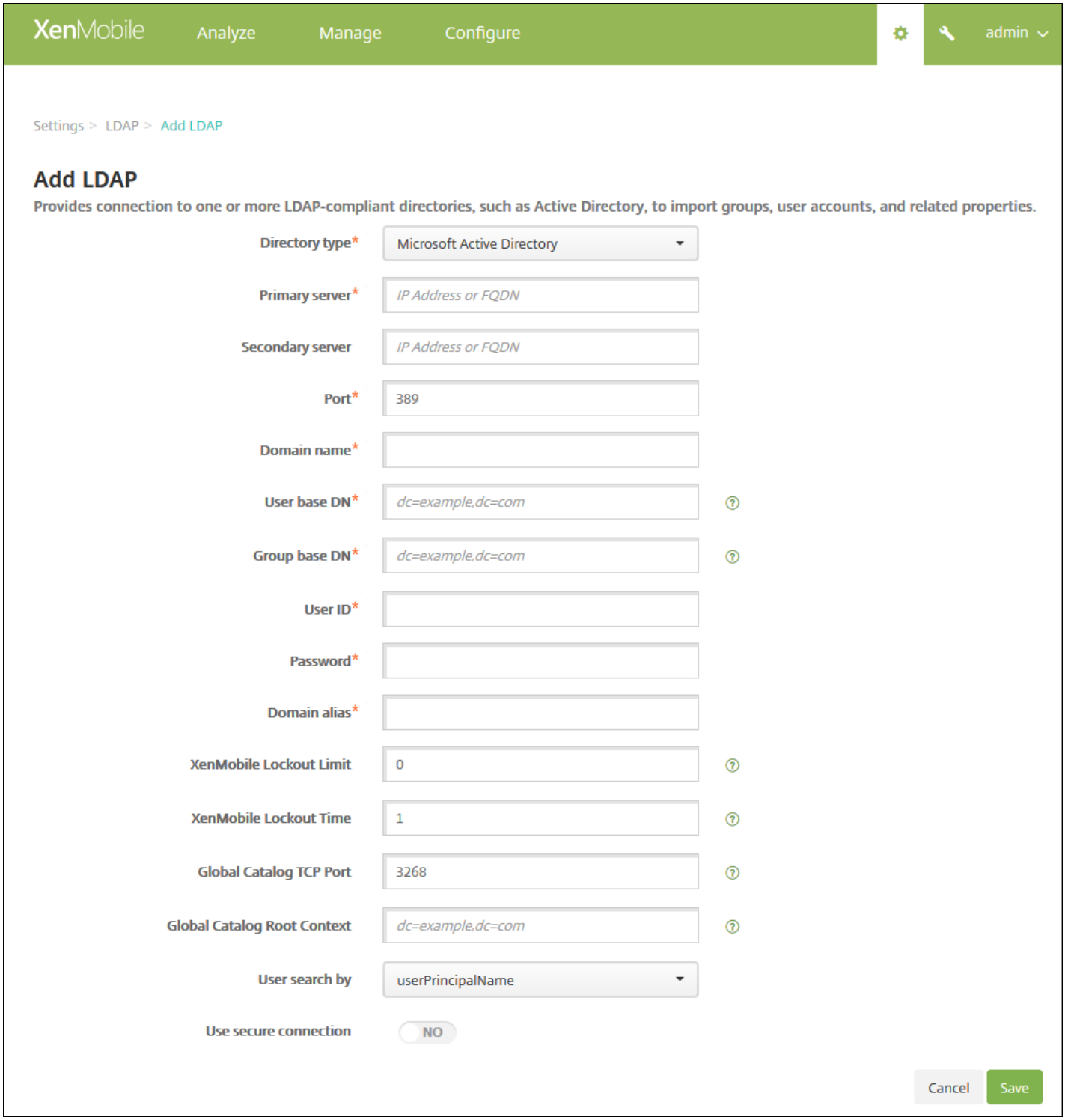
2. 在**服务器**下面，单击 **LDAP**。 此时将显示 **LDAP** 页面。 可以从此页面添加、编辑或删除兼容 LDAP 的目录。



添加兼容 LDAP 的目录

1. 在 **LDAP** 页面上，单击**添加**。 此时将显示 **Add LDAP**（添加 LDAP）页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 配置以下设置：

- **目录类型**：在列表中，单击相应的目录类型。 默认值为 **Microsoft Active Directory**。
- **主服务器**：键入用于 LDAP 的主服务器；可以输入 IP 地址或完全限定的域名 (FQDN)。
- **辅助服务器**：可选。如果配置了辅助服务器，键入辅助服务器的 IP 地址或 FQDN。
- **端口**：键入用于 LDAP 服务器的端口号。 默认情况下，对于不安全的 LDAP 连接，端口号设置为 389。 请为安全的 LDAP 连接使用端口号 636，为 Microsoft 的不安全 LDAP 连接使用 3268，或者为 Microsoft 的安全 LDAP 连接使用 3269。
- **域名**：键入域名。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **用户基本 DN**：通过唯一的标识符在 Active Directory 中键入用户的位置。 语法示例包括：ou=users、dc=example 或 dc=com。
- **组基础 DN**：键入组基础 DN 组名，以 cn=groupname 的形式指定。 例如，cn=users, dc=servername, dc=net，其中 cn=users 是组名；DN 和 servername 表示运行 Active Directory 的服务器的名称。
- **用户 ID**：键入与 Active Directory 帐户关联的用户 ID。
- **密码**：键入与用户关联的密码。
- **域别名**：键入域名称的别名。
- **XenMobile 锁定限制**：键入介于 0 至 999 之间的数字，表示失败登录尝试次数。 将此字段设为 0 表示 XenMobile 始终不会根据失败登录尝试次数锁定用户。
- **XenMobile 锁定时间**：键入介于 0 至 99999 之间的数字，表示用户超过锁定限制后必须等待的分钟数。 将此字段设为 0 表示不会强制用户在锁定后等待。
- **全局目录 TCP 端口**：键入全局目录服务器的 TCP 端口号。 默认情况下，TCP 端口号设为 3268；对于 SSL 连接，使用端口号 3269。
- **全局目录根上下文**：可选，键入用于在 Active Directory 中启用全局目录搜索的全局根上下文值。 此搜索是除标准 LDAP 搜索之外的方法，可在任何域中使用，无需指定实际的域名。
- **用户搜索依据**：在此列表中，单击 **userPrincipalName** 或 **sAMAccountName**。 默认值为 **userPrincipalName**。
- **使用安全连接**：选择是否使用安全连接。 默认值为 **NO**。

3. 单击**保存**。

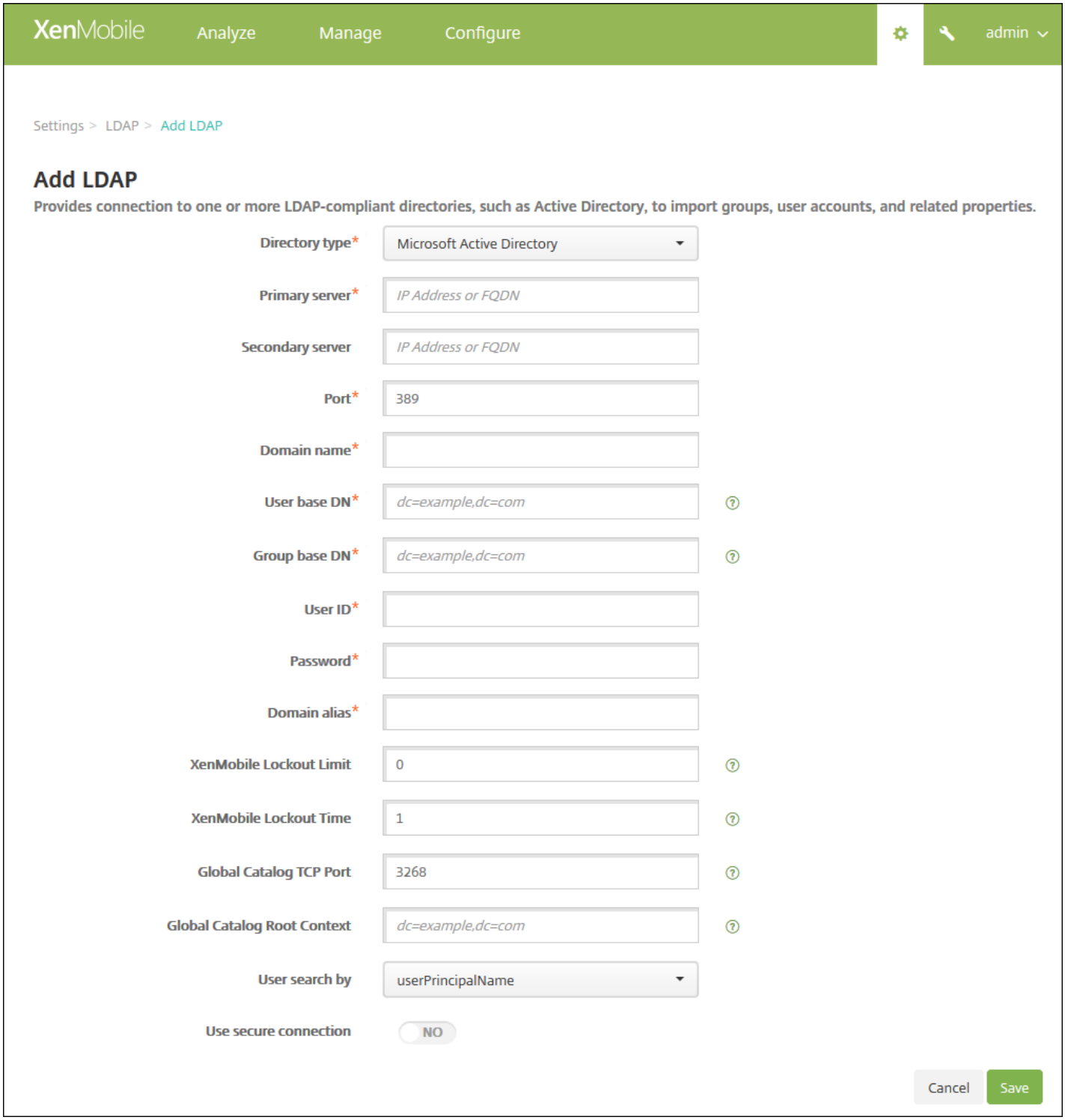
编辑兼容 LDAP 的目录

1. 在 **LDAP** 表格中，选择要编辑的目录。

   注意：如果选中某个目录旁边的复选框，选项菜单将显示在 LDAP 列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。

2. 单击**编辑**。 此时将显示**添加 LDAP** 页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 适当更改以下信息：

- **目录类型**：在列表中，单击相应的目录类型。
- **主服务器**：键入用于 LDAP 的主服务器；可以输入 IP 地址或完全限定的域名 (FQDN)。
- **辅助服务器**：可选。如果配置了辅助服务器，键入辅助服务器的 IP 地址或 FQDN。
- **端口**：键入用于 LDAP 服务器的端口号。 默认情况下，对于不安全的 LDAP 连接，端口号设置为 389。 请为安全的 LDAP 连接使用端口号 636，为 Microsoft 的不安全 LDAP 连接使用 3268，或者为 Microsoft 的安全 LDAP 连接使用 3269。
- **域名**：无法更改此字段。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **用户基本 DN**：通过唯一的标识符在 Active Directory 中键入用户的位置。 语法示例包括：ou=users、dc=example 或 dc=com。
- **组基础 DN**：键入组基础 DN 组名，以 cn=groupname 的形式指定。 例如，cn=users, dc=servername, dc=net，其中 cn=users 是组名；DN 和 servername 表示运行 Active Directory 的服务器的名称。
- **用户 ID**：键入与 Active Directory 帐户关联的用户 ID。
- **密码**：键入与用户关联的密码。
- **域别名**：键入域名称的别名。
- **XenMobile 锁定限制**：键入介于 0 至 999 之间的数字，表示失败登录尝试次数。 将此字段设为 0 表示 XenMobile 始终不会根据失败登录尝试次数锁定用户。
- **XenMobile 锁定时间**：键入介于 0 至 99999 之间的数字，表示用户超过锁定限制后必须等待的分钟数。 将此字段设为 0 表示不会强制用户在锁定后等待。
- **全局目录 TCP 端口**：键入全局目录服务器的 TCP 端口号。 默认情况下，TCP 端口号设为 3268；对于 SSL 连接，使用端口号 3269。
- **全局目录根上下文**：可选，键入用于在 Active Directory 中启用全局目录搜索的全局根上下文值。 此搜索是除标准 LDAP 搜索之外的方法，可在任何域中使用，无需指定实际的域名。
- **用户搜索依据**：在此列表中，单击 **userPrincipalName** 或 **sAMAccountName**。
- **使用安全连接**：选择是否使用安全连接。

4. 单击**保存**以保存您的更改，或单击**取消**保持属性不发生更改。

删除兼容 LDAP 的目录

1. 在 **LDAP** 表格中，选择要删除的目录。

   注意：可以通过选中每个属性旁边的复选框，选择要删除的多个属性。

2. 单击**删除**。 此时将显示确认对话框。 再次单击**删除**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置域和安全令牌身份验证

Oct 21, 2016

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

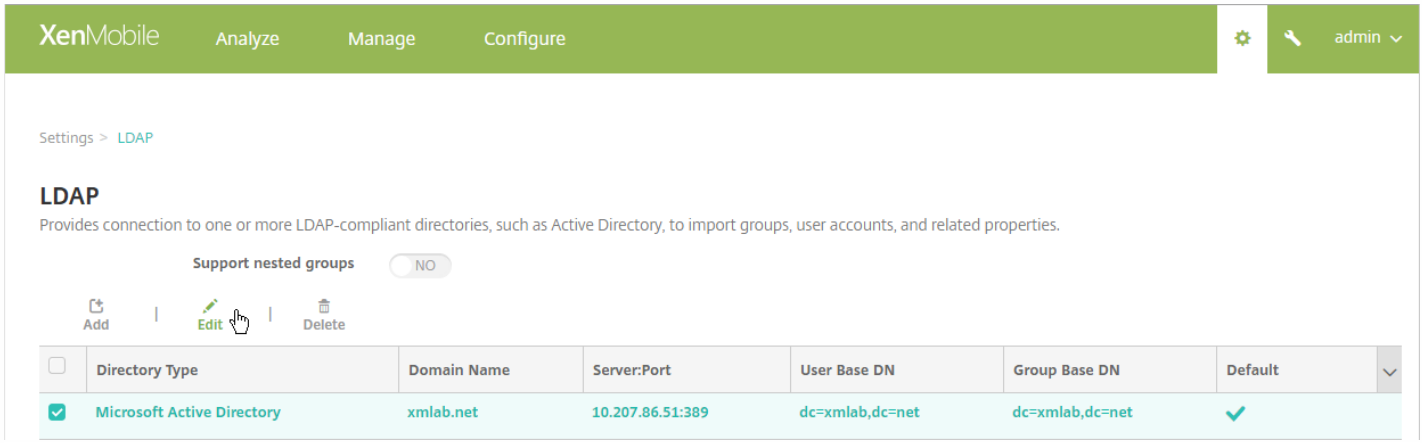
为实现最佳可用性，您可以将此配置与 Worx PIN 和 Active Directory 密码缓存组合在一起，以便用户不需要重复输入其 Active Directory 用户名和密码。 用户需要在注册、密码过期和帐户锁定时输入用户名和密码。

配置 LDAP 设置

使用 LDAP 进行身份验证要求您在 XenMobile 上安装证书颁发机构颁发的 SSL 证书。 有关详细信息，请参阅在 XenMobile 中上载证书。

1. 在**设置**中，单击 **LDAP**。

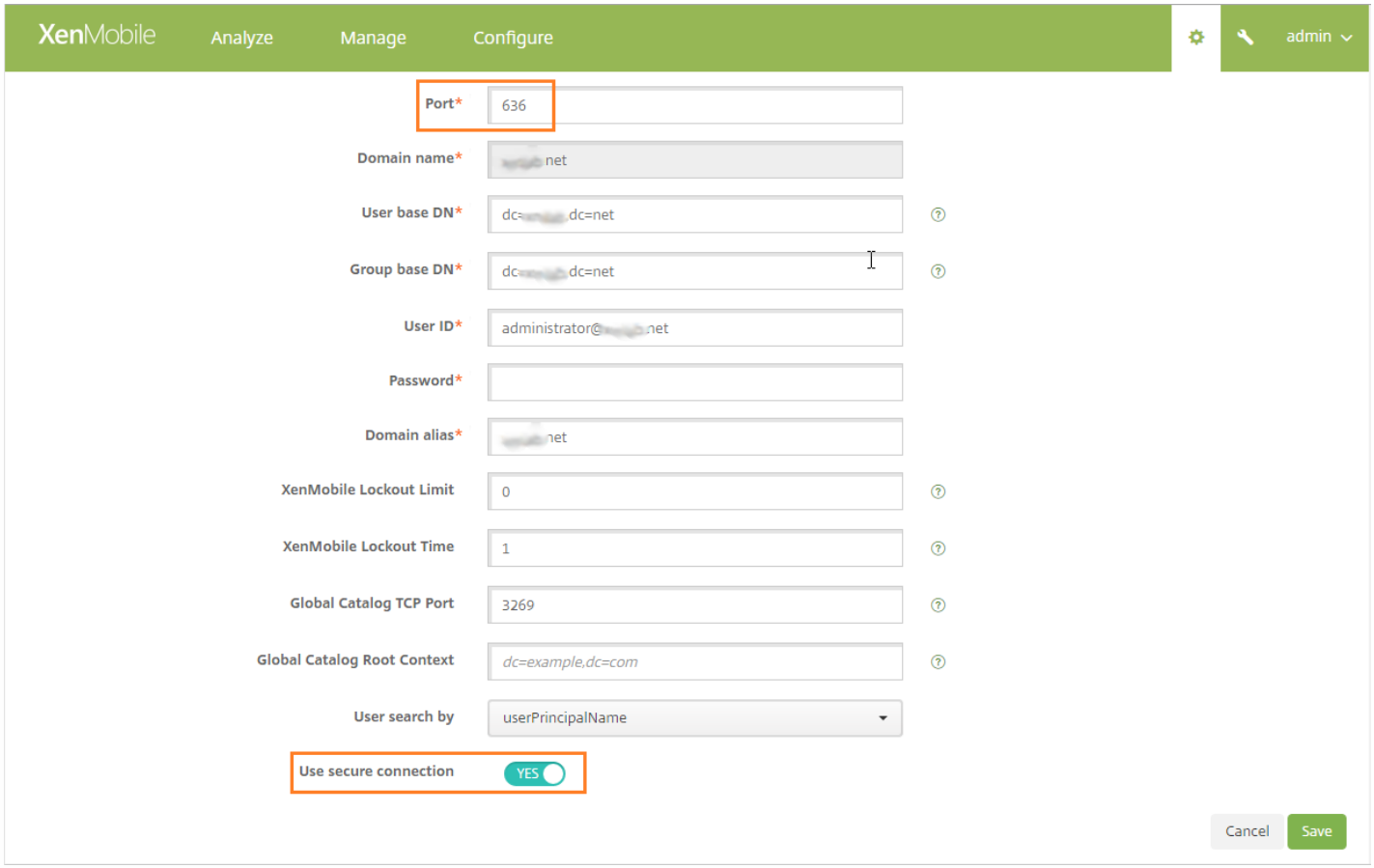
2. 选择 **Microsoft Active Directory**，然后单击**编辑**。



3. 确认 **Port**（端口）为 **636**（适用于安全 LDAP 连接）还是 **3269**（适用于 Microsoft 安全 LDAP 连接）。

4. 将**使用安全连接**更改为**是**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置 NetScaler Gateway 设置

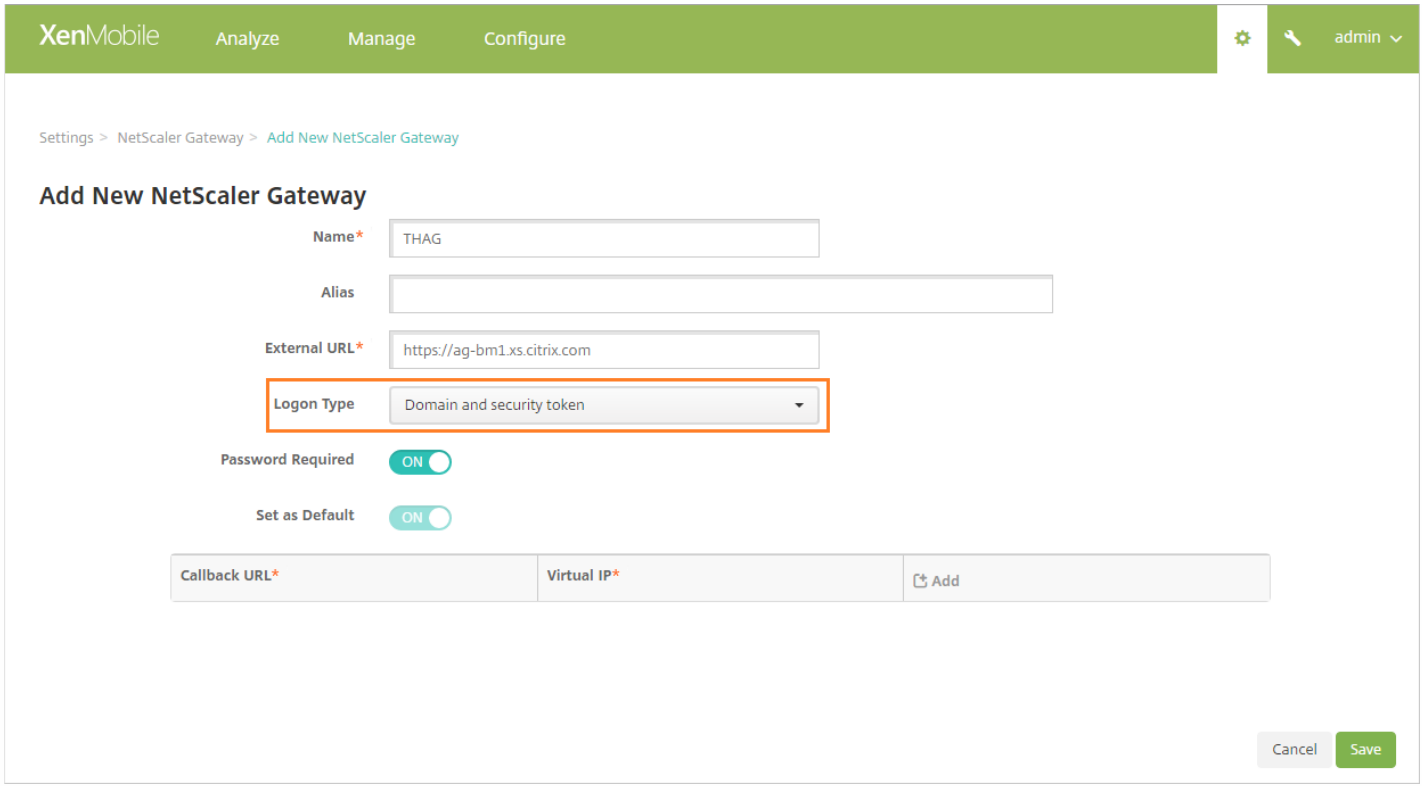
以下步骤假定您已向 XenMobile 中添加 NetScaler Gateway 实例。 要添加 NetScaler Gateway 实例，请参阅 NetScaler Gateway 和 XenMobile。

1. 在**设置**中，单击 **NetScaler Gateway**。

2. 选择 NetScaler Gateway，然后单击**编辑**。

3. 在**登录类型**中，选择**域和安全令牌**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



启用 Worx PIN 和 Active Directory 密码缓存

要启用 Worx PIN 和 Active Directory 密码缓存，请转至**设置 > 客户端属性**，然后选中复选框**启用 Worx PIN 身份验证**和**启用用户密码缓存**。 有关详细信息，请参阅客户端属性参考。

配置 NetScaler Gateway 以进行域和安全牌令牌身份验证

为与 XenMobile 配合使用的虚拟服务器配置 NetScaler Gateway 会话配置文件和策略。 有关信息，请参阅 NetScaler Gateway 文档中的为 XenMobile 配置域和安全令牌身份验证。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

证书

Oct 21, 2016

使用 XenMobile 中的证书创建安全连接并对用户进行身份验证。

默认情况下，XenMobile 附带在安装期间生成的自签名安全套接字层 (SSL) 证书，用于确保与服务器之间的通信流安全。 Citrix 建议您使用知名证书颁发机构 (CA) 发布的可信 SSL 证书替换此 SSL 证书。

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

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

要在 XenMobile 中注册并管理 iOS 设备，需要从 Apple 设置并创建 Apple 推送通知服务 (APNs) 证书。 有关步骤，请参阅请求 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**	**所需的证书类型**
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL、根 NetScaler Gateway 自动将 PFX 转换为 PEM。
XenMobile 服务器	PEM 或 PFX (PKCS#12)	SSL、SAML、APNs XenMobile 还在安装过程中生成完全 PKI。 XenMobile 服务器不支持扩展名为 .pem 的证书。 使用 openssl 命令可从 PEM 文件生成 PFX 文件： openssl pkcs12 -export -out certificate.pfx -in certificate.pem
StoreFront	PFX (PKCS#12)	SSL、根

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

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

用于身份验证的客户端证书

在 XenMobile 环境中，客户端证书和 LDAP 身份验证的组合是用于实现安全性和用户体验的最佳解决方案，同时，通过

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScaler 进行的双重身份验证还能提供最佳 SSO 可能性和安全性。 同时使用客户端证书和 LDAP 通过用户所知晓的内容（其 Active Directory 密码）和用户所拥有的内容（设备上的客户端证书）提供安全性。 WorxMail（以及某些其他 Worx 应用程序）在正确配置的 Exchange 客户端访问服务器环境中可以自动配置，并通过客户端证书身份验证提供无缝首次用户体验。 要实现最佳可用性，可以将此选项与 Worx PIN 和 Active Directory 密码缓存组合在一起。

客户端证书身份验证建立在向虚拟服务器提供的客户端证书的属性基础之上。 必须在 NetScaler Gateway 上将根证书与虚拟服务器绑定在一起。 用户登录到 NetScaler Gateway 后，将从证书的指定字段提取用户名信息。 此字段通常为 Subject:CN。 如果成功提取用户名，则用户将通过身份验证。 如果用户在安全套接字层 (SSL) 握手期间未提供有效的证书，或者如果用户名提取失败，则身份验证将失败。

注意：

- 也可以将客户端证书身份验证与另一种身份验证类型结合使用，例如 RADIUS。
- 可以通过将默认身份验证类型设置为使用客户端证书，基于客户端证书对用户进行身份验证。 还可以基于客户端 SSL 证书创建一个证书操作，用于定义身份验证过程中要执行的操作。
- WorxMail（以及某些其他 Worx 应用程序）在正确配置的 Exchange 客户端访问服务器环境中可以自动配置，并通过客户端证书身份验证提供无缝首次用户体验。 要实现最佳可用性，可以将此选项与 Worx PIN 和 Active Directory 密码缓存组合在一起。
- 通过任意 CA 获取的证书不支持通过 Netscaler Gateway 对设备进行身份验证。
- XenMobile 不支持对共享设备进行客户端证书身份验证。

XenMobile PKI

借助 XenMobile 公钥基础结构 (PKI) 集成功能，您可以管理设备上使用的安全证书的分发和生命周期。

XenMobile 会在安装过程中生成用于设备验证的内部 PKI。

也可以使用外部 PKI 向设备颁发证书，用于配置策略或客户端向 NetScaler Gateway 进行身份验证。

PKI 系统的主要功能是 PKI 实体。 PKI 实体可以为 PKI 操作的后端组件提供模型。 此组件属于企业基础结构的一部分，如 Microsoft、RSA、Entrust、Symantex 或 OpenTrust PKI。 PKI 实体可处理后端证书的颁发和吊销。 PKI 实体是证书状态的权威来源。 对于每个后端 PKI 组件，XenMobile 配置通常仅包含一个 PKI 实体。

PKI 系统的第二项功能是凭据提供程序。 凭据提供程序是证书颁发和生命周期的特定配置。 凭据提供程序控制证书格式（主题、密钥、算法）及其续订或吊销的条件（如有）等事项。 凭据提供程序向 PKI 实体委派操作。 换言之，凭据提供程序控制 PKI 操作的执行时间以及所使用的数据，而 PKI 实体则控制这些操作的执行方式。 对于每个 PKI 实体，XenMobile 配置通常包含多个凭据提供程序。

XenMobile 证书管理

我们建议您跟踪在您的 XenMobile 部署中使用的证书，尤其是其过期日期和关联的密码。 本部分内容目的是帮助您更轻松地在 XenMobile 中进行证书管理。

您的环境中可能包含以下部分或所有证书：

XenMobile 服务器
用于 MDM FQDN 的 SSL 证书
SAML 证书（用于 ShareFile）
用于以上证书和任何其他内部资源（StoreFront/代理等）的根和中间 CA 证书

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用于 iOS 设备管理的 APNs 证书
用于 XenMobile 服务器 Worx Home 通知的内部 APNs 证书
用于连接到 PKI 的 PKI 用户证书

MDX Toolkit
Apple 开发人员证书
Apple 置备配置文件（按应用程序）
Apple APNs 证书（用于 WorxMail）
Android 密钥库文件
Windows Phone – Symantec 证书

NetScaler
用于 MDM FQDN 的 SSL 证书
用于网关 FQDN 的 SSL 证书
用于 ShareFile SZC FQDN 的 SSL 证书
用于 Exchange 负载平衡（卸载配置）的 SSL 证书
用于 StoreFront 负载平衡的 SSL 证书
用于以上证书的根和中间 CA 证书

XenMobile 证书过期策略

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

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

用于 WorxMail 的 APNs 证书

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

用于 iOS 设备管理的 APNs 证书

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

可以通过登录 **Apple 推送证书门户**来查看 APNS 证书状态和过期日期。 请务必使用创建证书的同一用户身份登录。

在过期日期之前 30 天和 10 天，您还将收到 Apple 发送的电子邮件通知，其中包含以下信息：

"The following Apple Push Notification Service certificate, created for AppleID *CustomersID* 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.（为 AppleID CustomersID 创建的以下 Apple 推送通知服务证书将于 Date 过期。吊销此证书或允许此证书过期需要为现有设备重新注册新的推送证书。请联系您的供应商以生成新请求（签名的 CSR），然后访问 https://identity.apple.com/pushcert 以续订您的 Apple 推送通知服务证书。）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Thank You,（顺祝商祺）

Apple Push Notification Service（Apple 推送通知服务）

MDX Toolkit（iOS 分发证书）

在物理 iOS 设备上运行的任何应用程序（Apple App Store 中的应用程序除外）必须通过置备描述文件和相应的分发证书进行签名。

请注意，现有 iOS Developer for Enterprise 证书和置备配置文件可能与 iOS 9 不兼容。 有关详细信息，请参阅“打包适用于 iOS 9 的 Worx 应用程序”。

要验证您的 iOS 分发证书是否有效，请执行以下操作：

1. 从 Apple 企业开发者门户中，为计划使用 MDX Toolkit 打包的每个应用程序创建一个显式应用程序 ID。 可接受的应用程序 ID 示例：com.CompanyName.ProductName。
2. 从 Apple 企业开发者门户中，转到 **Provisioning Profiles**（置备配置文件）> **Distribution** （分发），并创建一个内部置备配置文件。 对在上一步中创建的每个应用程序 ID 重复此步骤。
3. 下载所有置备配置文件。 有关详细信息，请参阅打包 iOS 移动应用程序。

要确认所有 XenMobile 服务器证书是否有效，请执行以下操作：

1. 在 XenMobile 控制台中，单击**配置**，然后单击**证书**。
2. 确保包含 APNS、SSL 侦听器、根和中间证书的所有证书都有效。

Android 密钥库

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

Symantec 提供的用于 Windows Phone 的企业证书

Symantec 是用于 Microsoft 应用程序中心服务的代码签名证书的独家提供商。 开发者和软件发行者加入应用程序中心来分发 Windows Phone 和 Xbox 360 应用程序，以便通过 Windows Marketplace 下载。 有关详细信息，请参阅 Symantec 文档中的 Symantec Code Signing Certificates for Windows Phone（Symantec 用于 Windows Phone 的代码签名证书）。

如果证书过期，Windows Phone 用户将无法注册和安装公司发布和签名的应用程序，也不能启动手机上安装的公司应用程序。

NetScaler

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

如果 NetScaler 证书过期，用户将无法注册、访问 Worx Store、使用 WorxMail 时连接至 Exchange Server 以及枚举和打开 HDX 应用程序（取决于过期的证书）。

Expiry Monitor 和 Command Center 可以帮助您跟踪 NetScaler 证书，并在证书过期时通知您。 这两个工具可以协助监视以下 Netscaler 证书：

用于 MDM FQDN 的 SSL 证书

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用于网关 FQDN 的 SSL 证书
用于 ShareFile SZC FQDN 的 SSL 证书
用于 Exchange 负载平衡（卸载配置）的 SSL 证书
用于 StoreFront 负载平衡的 SSL 证书
用于以上证书的根和中间 CA 证书

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中上载证书

Oct 21, 2016

XenMobile 服务器功能性地使用证书。 通过 XenMobile 控制台的**证书**区域将证书上载到 XenMobile。 这些证书包括证书颁发机构 (CA) 证书、注册机构 (RA) 证书以及用于您基础结构其他组件的客户端身份验证的证书。 此外，您还可以将“证书”区域用作您希望部署到设备的证书的存储位置。 此用法特别适用于在设备上建立信任所使用的 CA。

您上载的每个证书将以证书表中的一个条目来表示，并提供其内容摘要。 配置需要证书的 PKI 集成组件时，系统将提示您从满足上下文相关条件的服务器证书列表中进行选择。 例如，您可能希望将 XenMobile 配置为与 Microsoft CA 集成。 与 Microsoft CA 的连接应使用客户端证书进行身份验证。

本部分内容介绍了上载证书的常规过程。 有关创建、上载和配置客户端证书的详细信息，请参阅配置客户端证书身份验证。

私钥要求

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

向控制台上载证书

您可以上载 CA 用来对请求进行签名的 CA 证书（不带私钥），以及用于客户端身份验证的 SSL 客户端证书（带私钥）。 配置 Microsoft CA 实体时，需要指定 CA 证书，此证书可从包含属于 CA 证书的所有服务器证书的列表中进行选择。 同样，配置客户端身份验证时，您可以从包含 XenMobile 具有私钥的所有服务器证书的列表中进行选择。

XenMobile 支持以下证书输入格式：

- PEM 或 DER 编码的证书文件
- 带有关联 PEM 或 DER 编码的私钥文件的 PEM 或 DER 编码证书文件
- PKCS#12 密钥库（P12；在 Windows 上也称为 PFX）

重要：XenMobile 服务器不支持扩展名为 .pem 的证书。 使用 openssl 命令可基于 PEM 文件生成 PFX 文件：

```
openssl pkcs12 -export -out certificate.pfx  -in certificate.pem
```

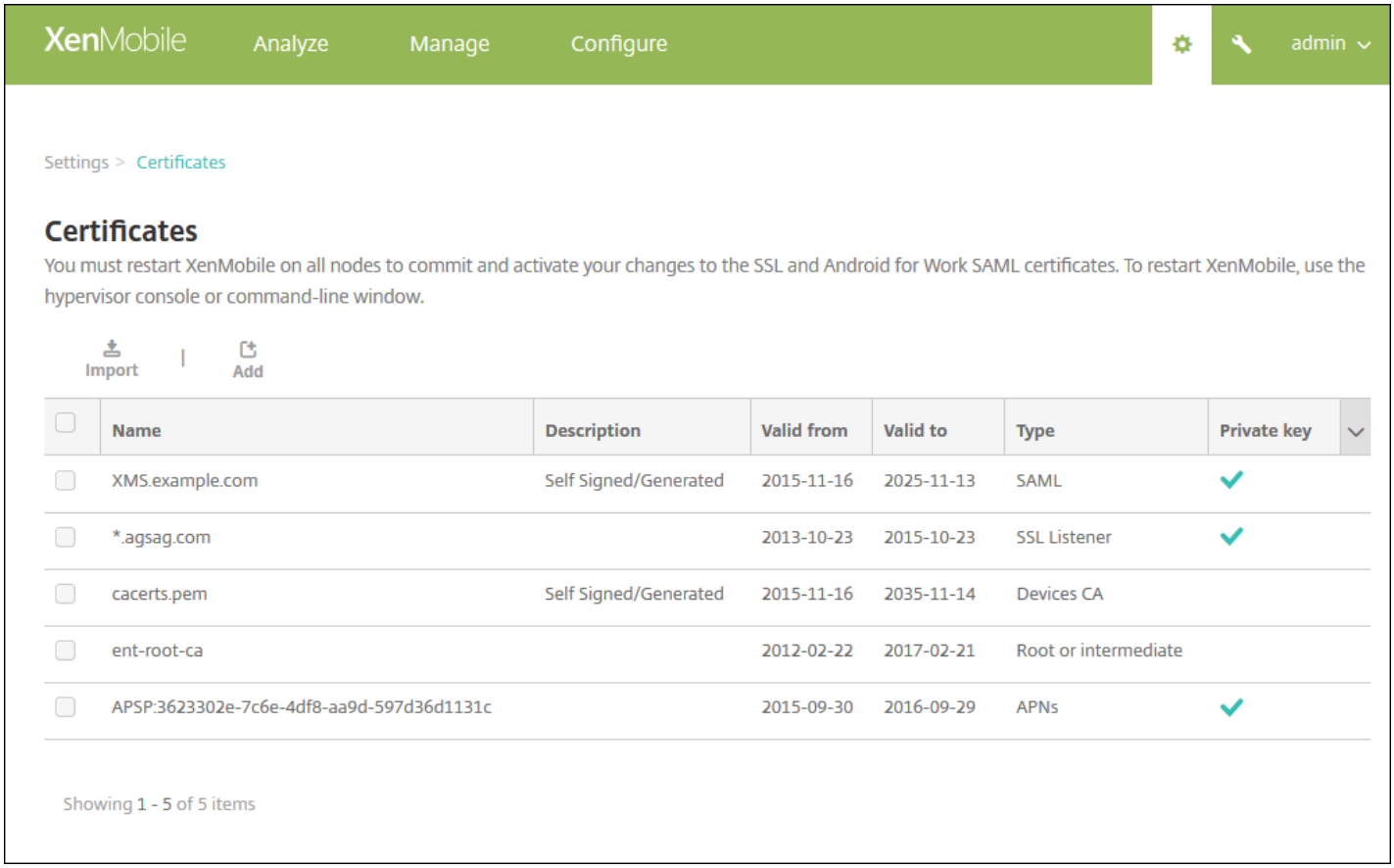
导入密钥库

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

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

2. 单击**证书**。 此时将显示**证书**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

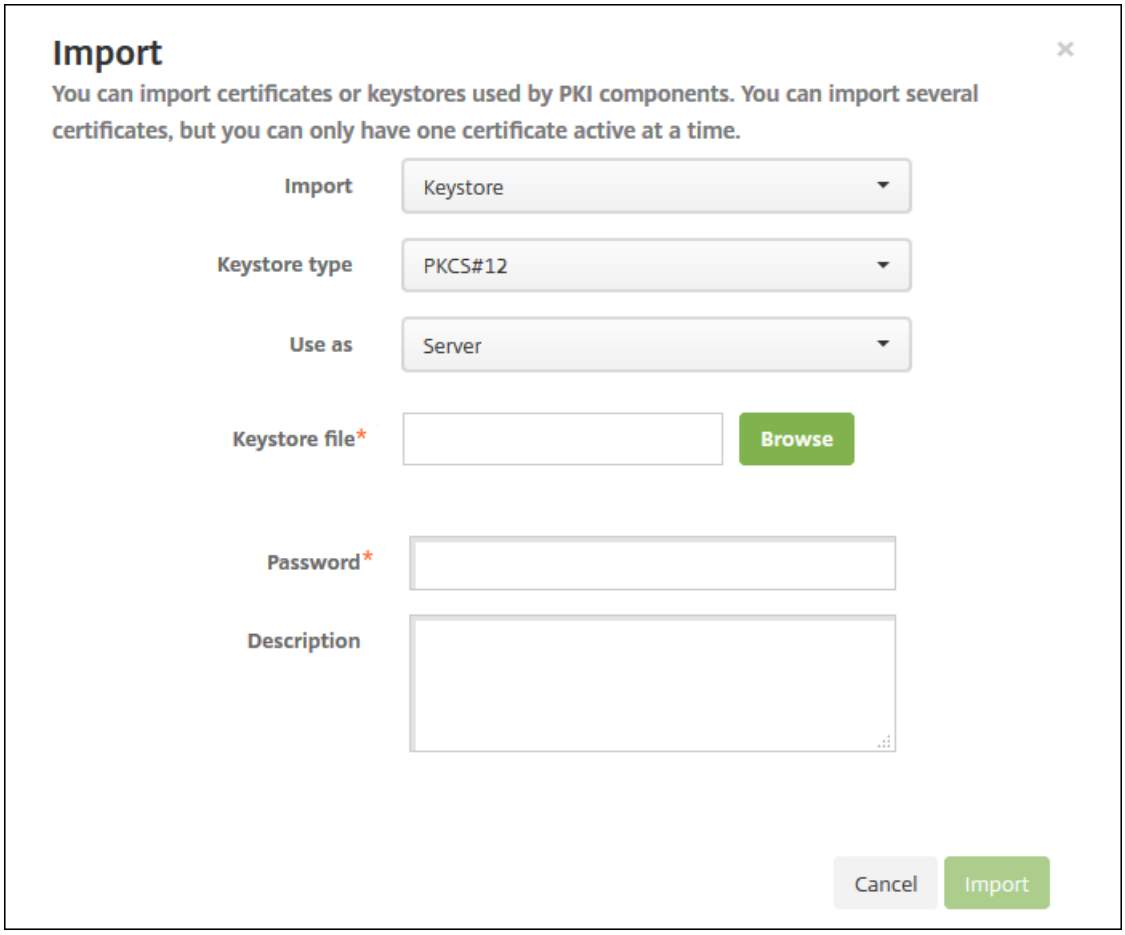


3. 单击**导入**。 此时将显示**导入**对话框。

4. 配置以下设置：

- **导入**：在列表中，单击**密钥库**。 **导入**对话框将更改以反应可用的密钥库选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **密钥库类型**：在列表中，单击 **PKCS#12**。
- **用作**：在列表中，单击使用密钥库的方式。 可用选项如下：
  - **服务器**。 服务器证书是 XenMobile 服务器功能性使用的证书，已上载到 XenMobile Web 控制台中。 这些证书包括 CA 证书、RA 证书以及用于您基础结构其他组件的客户端身份验证的证书。 此外，您还可以使用服务器证书来存储您希望部署到设备的证书。 此用法特别适用于在设备上建立信任所使用的 CA。
  - **SAML**。 安全声明标记语言 (SAML) 允许您提供对服务器、Web 站点和应用程序的单点登录 (SSO) 访问权限。
  - **APNs**。 利用 Apple 提供的 Apple 推送通知服务 (APNs) 证书，可以通过 Apple 推送网络启用移动设备管理。
  - **SSL 侦听器**。 安全套接字层 (SSL) 侦听器向 XenMobile 通知 SSL 加密活动。
- **密钥库文件**：单击**浏览**，导航到要导入的密钥库文件所在的位置，选择此文件。
- **密码**：键入分配给证书的密码。
- **说明**：可选，键入密钥库的说明，以帮助您将其与其他密钥库区分开。

5. 单击**导入**。 密钥库将添加到**证书**表中。

导入证书

从文件或 密钥库 条目导入证书时，XenMobile 将尝试基于输入内容构建证书链，并导入链中的所有证书（为每个证书创建一个服务器证书条目）。 只有文件或 密钥库 条目中的证书确实形成一个链时，比如链中的每个后续证书都是前一个证书的 颁发者 时，此操作才有效。

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

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击**证书**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 在**证书**页面上，单击**导入**。 此时将显示**导入**对话框。

3. 在**导入**对话框的**导入**中，如果尚未选择，请单击**证书**。

4. **导入**对话框将更改以反应可用的证书选项。 在**用作**中，单击使用 密钥库的方式。 可用选项如下：

- **服务器**。 服务器证书是 XenMobile 服务器功能性使用的证书，已上载到 XenMobile Web 控制台中。 这些证书包括 CA 证书、RA 证书以及用于您基础结构其他组件的客户端身份验证的证书。 此外，您还可以使用服务器证书来存储您希望部署到设备的证书。 此用法特别适用于在设备上建立信任所使用的 CA。
- **SAML**。 安全声明标记语言 (SAML) 允许您提供对服务器、Web 站点和应用程序的单点登录 (SSO) 访问权限。
- **SSL 侦听器**。 安全套接字层 (SSL) 侦听器向 XenMobile 通知 SSL 加密活动。

5. 浏览以查找要导入的证书。

6. 浏览以查找证书的可选私钥文件。 私钥用于与证书结合使用以便进行加密和解密。

7. 键入证书的说明（可选），以帮助您将其与其他证书区分开。

8. 单击**导入**。 证书将添加到证书表中。

更新证书

在任何时间，XenMobile 都只允许系统中每个公钥仅 存在 一个证书。 如果您尝试为已导入证书的同一密钥对导入证书，则需要选择是取代现有条目还是将其删除。

要最有效地更新证书，请在 XenMobile 控制台中单击控制台右上角的齿轮图标以打开设置页面，然后单击证书。 在导入对话框中，导入新证书。 当更新服务器证书时，使用先前证书的组件将自动切换到使用新证书。 同样，如果已经在设备上部署服务器证书，证书将在下一次部署时自动更新。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置客户端证书身份验证

Aug 11, 2016

必须依次配置 Microsoft 服务器、XenMobile 服务器和 NetScaler Gateway，才能对 XenMobile ENT 和 MAM 模式使用客户端证书身份验证。 本文详细介绍了以下常规步骤。

在 Microsoft 服务器上：

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

在 XenMobile 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. 将 NetScaler Gateway 配置为提供用于进行身份验证的用户证书。

在 NetScaler Gateway 上：

1. 为 XenMobile MAM 模式证书身份验证配置 NetScaler Gateway。

必备条件

- 对于使用客户端证书身份验证和 SSL 卸载的 Windows Phone 8.1 设备，必须在 NetScaler 中的两个负载平衡服务器上对端口 443 禁用 SSL 会话重用。 为此，请在虚拟服务器上对端口 443 运行以下命令：

  set ssl vserver sessReuse DISABLE

  注意：如果禁用 SSL 会话重用，还将禁用 NetScaler 提供的某些优化功能，这会导致 NetScaler 上的性能下降。

- 要为 Exchange ActiveSync 配置基于证书的身份验证，请参阅此 Microsoft 博客。
- 如果正在使用专用服务器证书来保护流向 Exchange Server 的 ActiveSync 流量安全，请确保移动设备具有所有根证书/中间证书。 否则，在 WorxMail 中设置邮箱时，基于证书的身份验证将失败。 在 Exchange IIS 控制台中，必须执行以下操作：
  - 添加一个 Web 站点以供 XenMobile 和 Exchange 使用，并绑定 Web 服务器证书。
  - 使用端口 9443。
  - 对于该 Web 站点，必须添加两个应用程序，一个用于 Microsoft-Server-ActiveSync，一个用于 EWS。 对于这两个应用程序，请在 **SSL Settings**（SSL 设置）下选择 **Require SSL**（需要 SSL）。
- 确保通过最新的 MDX Toolkit 打包 WorxMail for iOS、WorxMail for Android 和 WorxMail for Windows Phone。

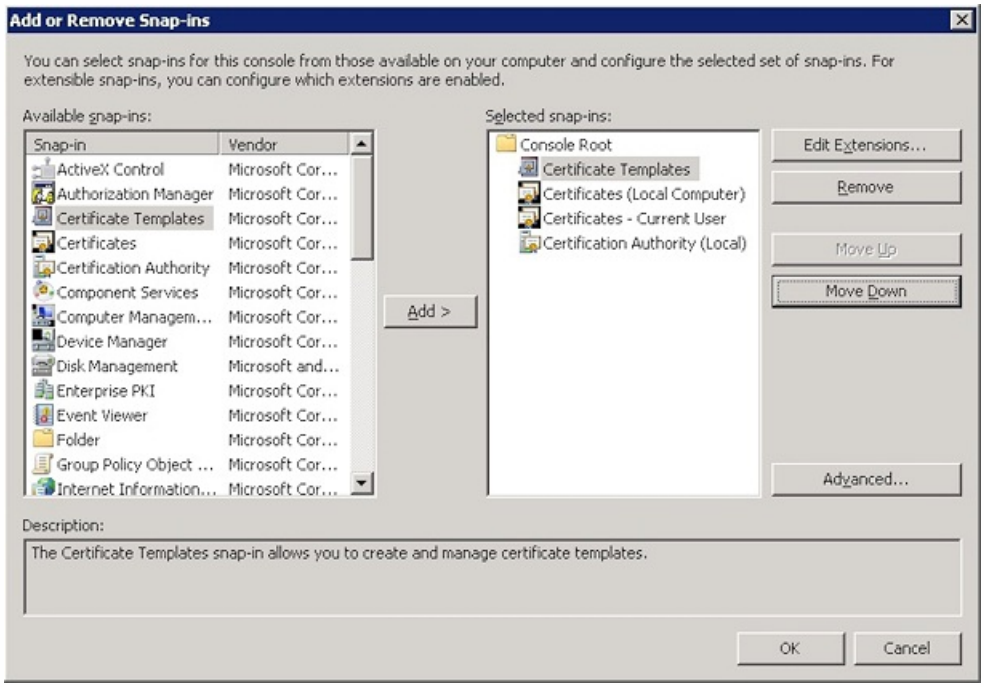
向 Microsoft 管理控制台中添加证书管理单元

1. 打开该控制台，然后单击**Add/Remove Snap-Ins**（添加/删除管理单元）。

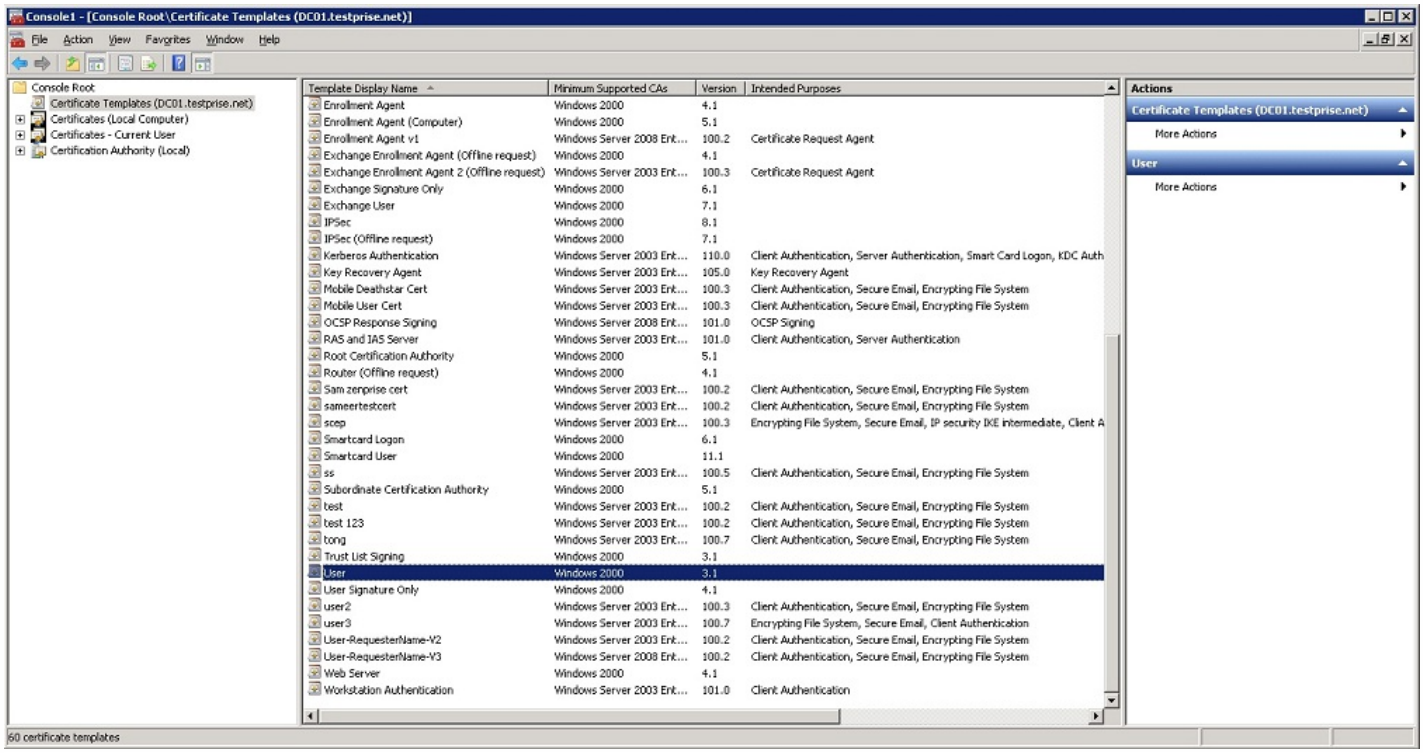
2. 添加以下管理单元：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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)

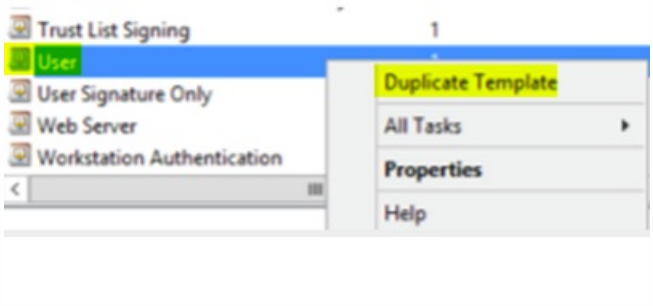


3. 展开**证书模板**。



4. 选择**用户**模板和**复制模板**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

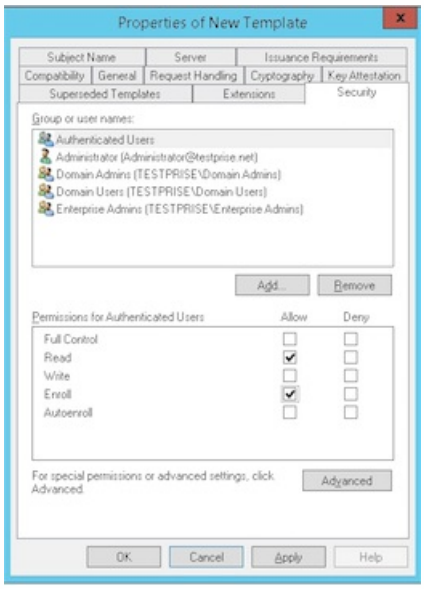


5. 提供模板显示名称。

> **重要：**除非需要，否则请勿选中**在 Active Directory 中发布证书**复选框。 如果选中了此选项，则将在 Active Directory 中推送/创建所有用户客户端证书，这可能会导致您的 Active Directory 数据库混乱不堪。

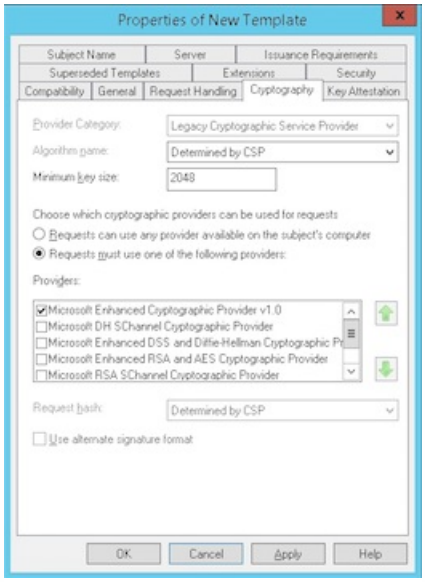
6. 选择 **Windows 2003 Server** 作为模板类型。在 Windows 2012 R2 Server 中，请在**兼容性**下选择**证书颁发机构**，然后设置接受方 **Windows 2003**。

7. 在**安全**下，在已通过身份验证的用户对应的**允许**列下选择**注册**选项。

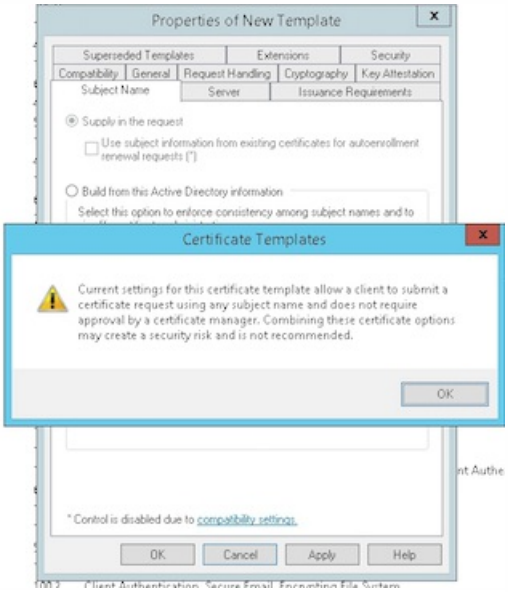


8. 在**加密**下，请务必提供需要在 XenMobile 配置过程中输入的密钥大小。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 在**使用者名称**下，选择**在请求中提供**。 应用更改并保存。

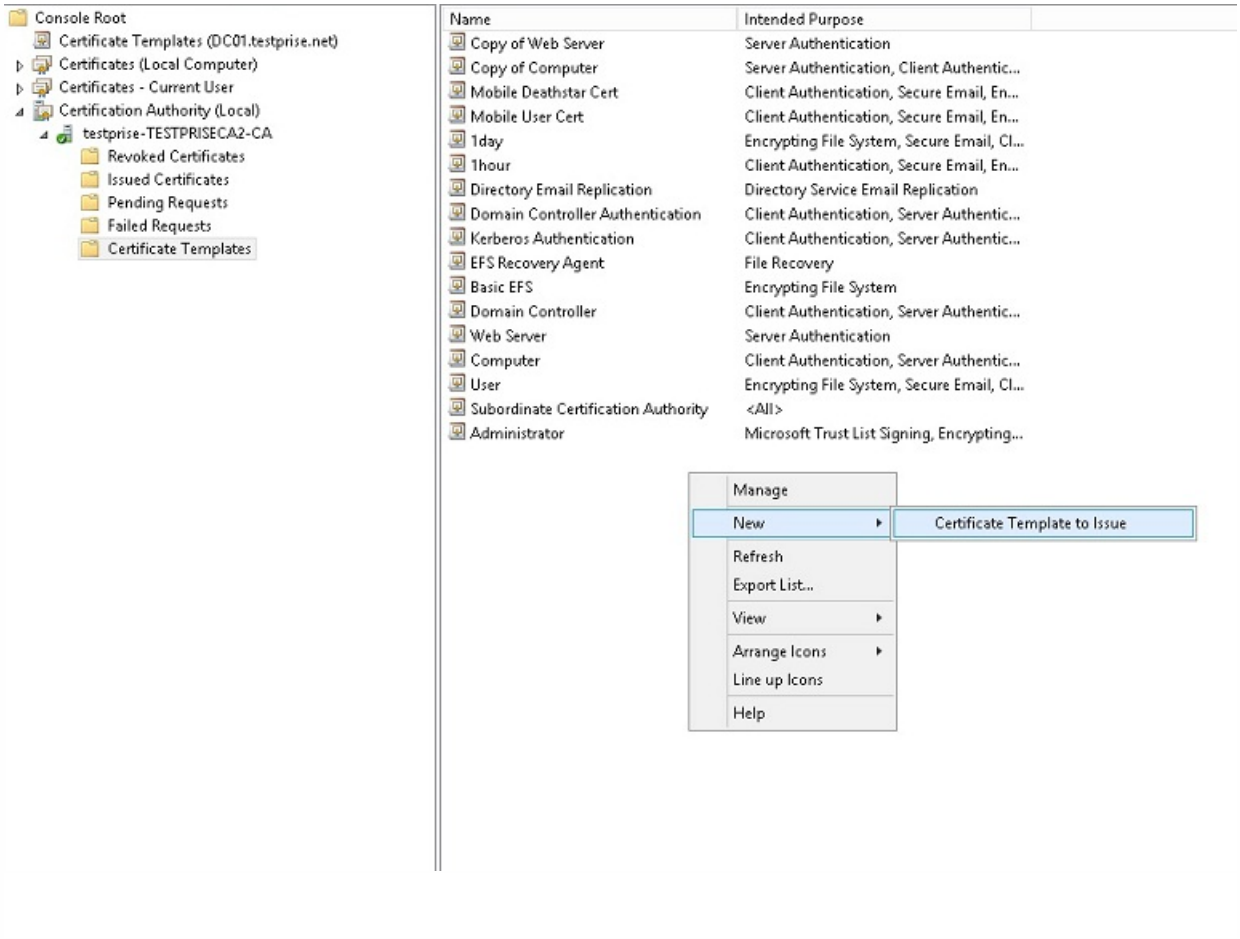


向证书颁发机构中添加模板

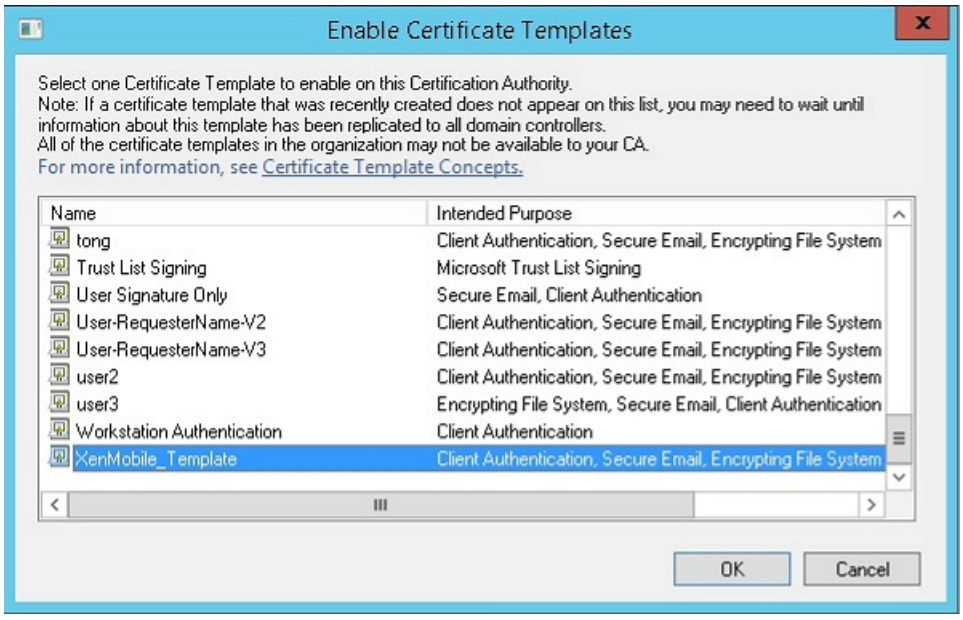
1. 转至**证书颁发机构**并选择**证书模板**。

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 选择在上一步中创建的模板，然后单击**确定**将其添加到**证书颁发机构**。



从 CA 服务器创建 PFX 证书

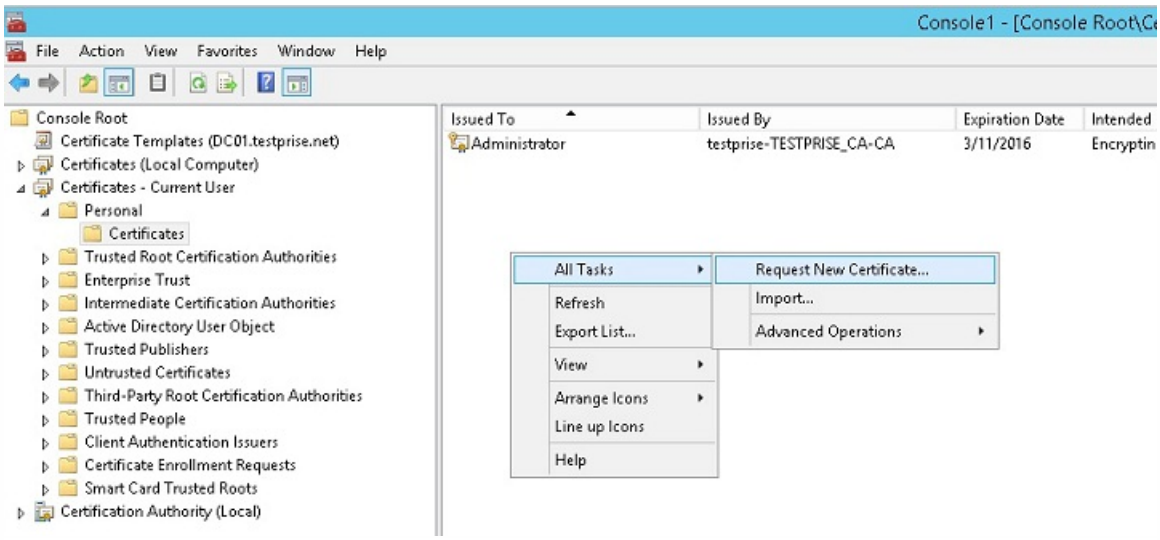
1. 使用登录时使用的服务帐户创建一个用户 .pfx 证书。 此 .pfx 将上载到 XenMobile 中，而 XenMobile 将代表注册设备的用户

© 1999-2017 Citrix Systems, Inc. All rights reserved.

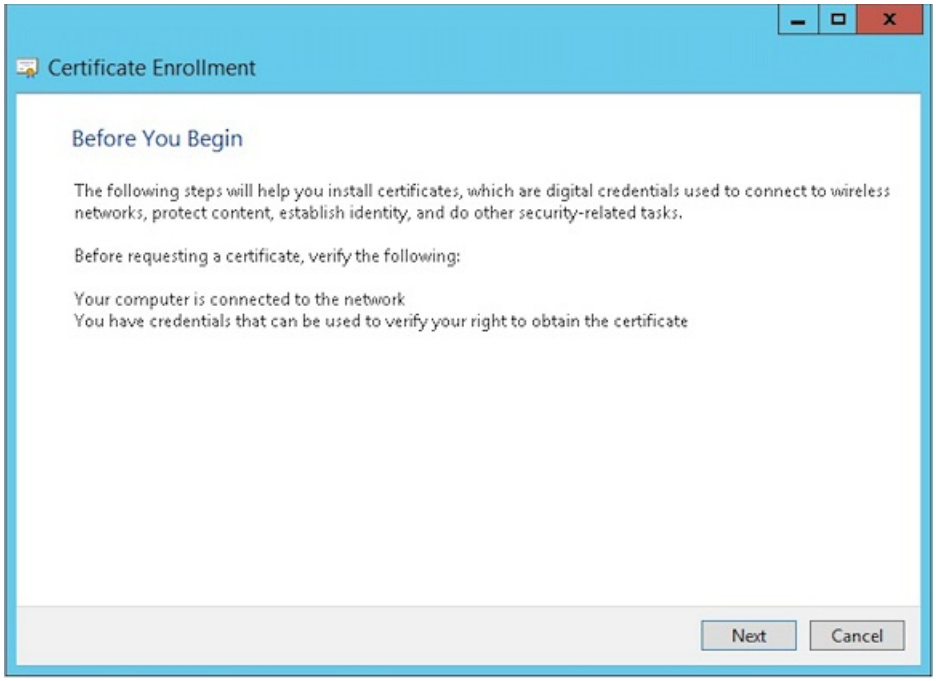
申请用户证书。

2. 在**当前用户**下，展开**证书**。

3. 在右侧窗格中单击鼠标右键，然后单击**申请新证书**。

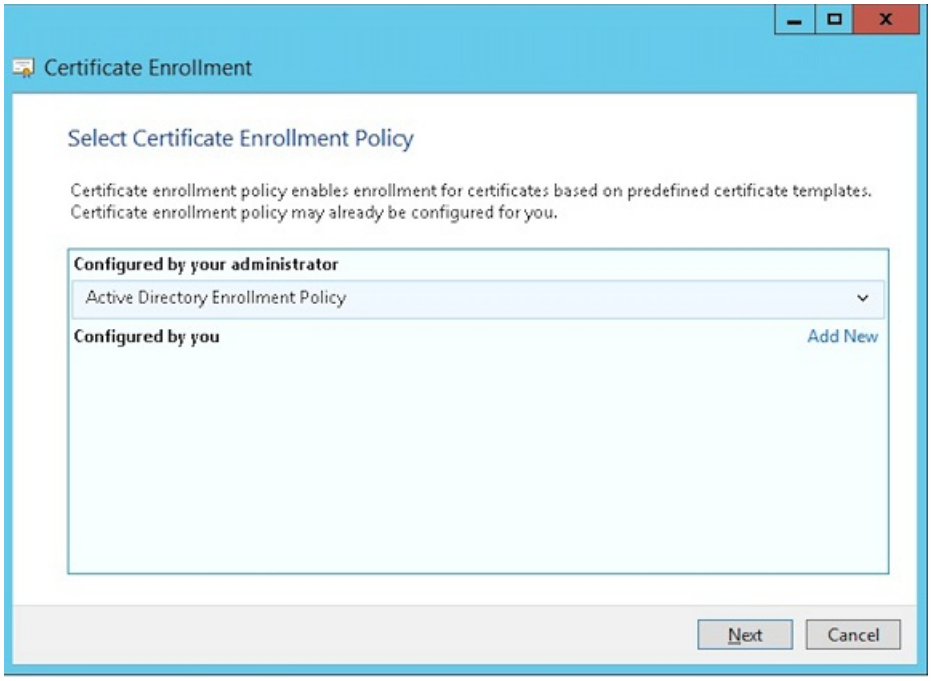


4. 此时将显示**证书注册**屏幕。 单击**下一步**。

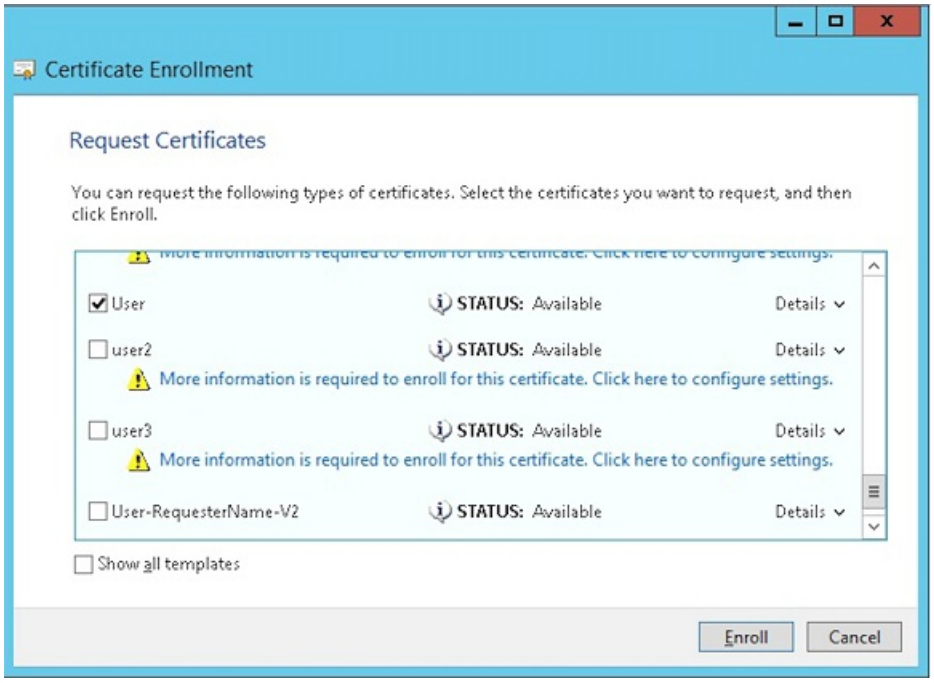


5. 选择 **Active Directory 注册策略**，然后单击**下一步**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

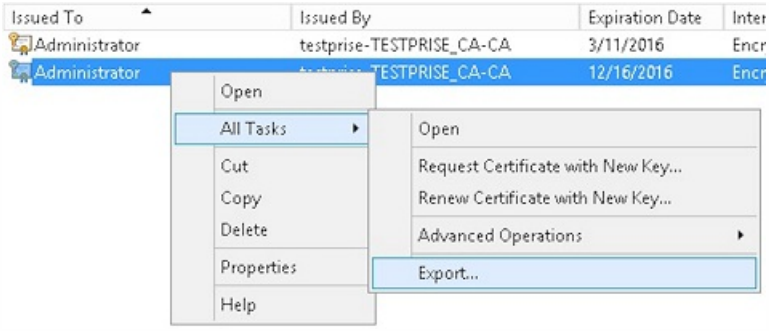


6. 选择**用户**模板，然后单击**注册**。

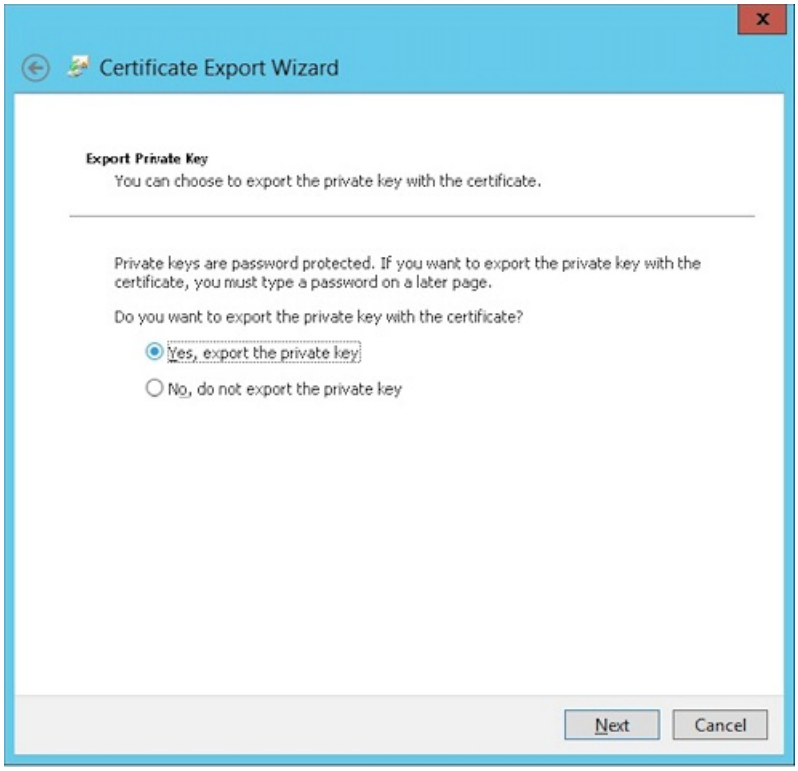


7. 导出在上一步中创建的 .pfx 文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

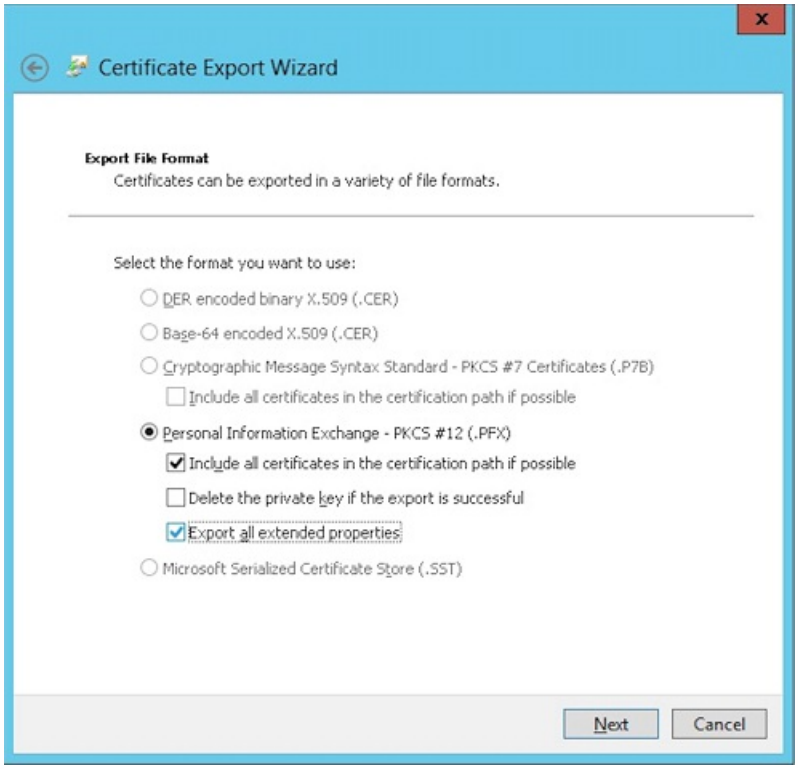


8. 单击**是，导出私钥**。

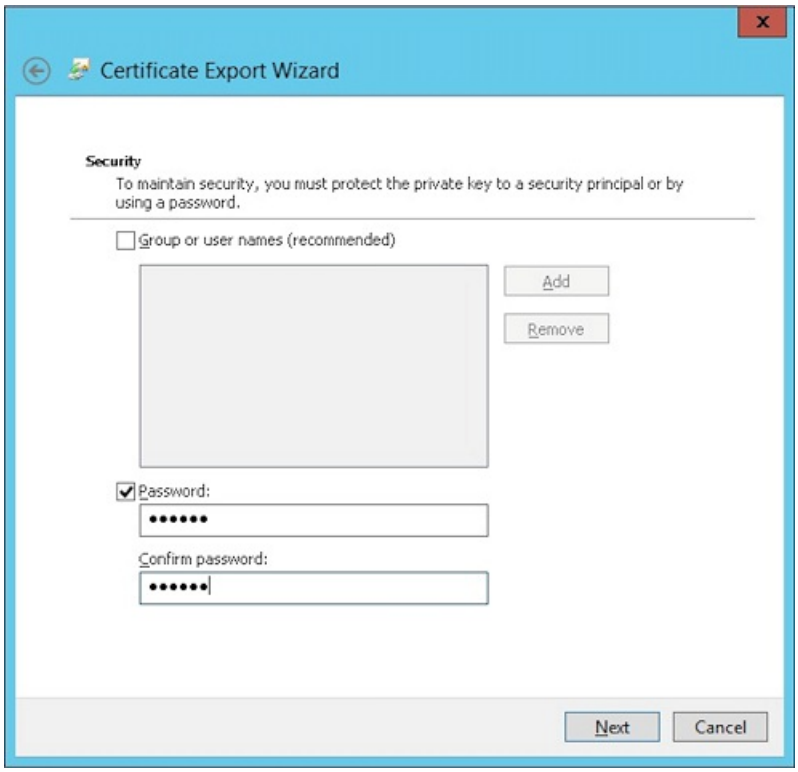


9. 选中**如果可能，则包括证书路径中的所有证书**和**导出所有扩展属性**复选框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



10. 设置要在将此证书上载到 XenMobile 中时使用的密码。



11. 将证书保存到您的硬盘驱动器。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

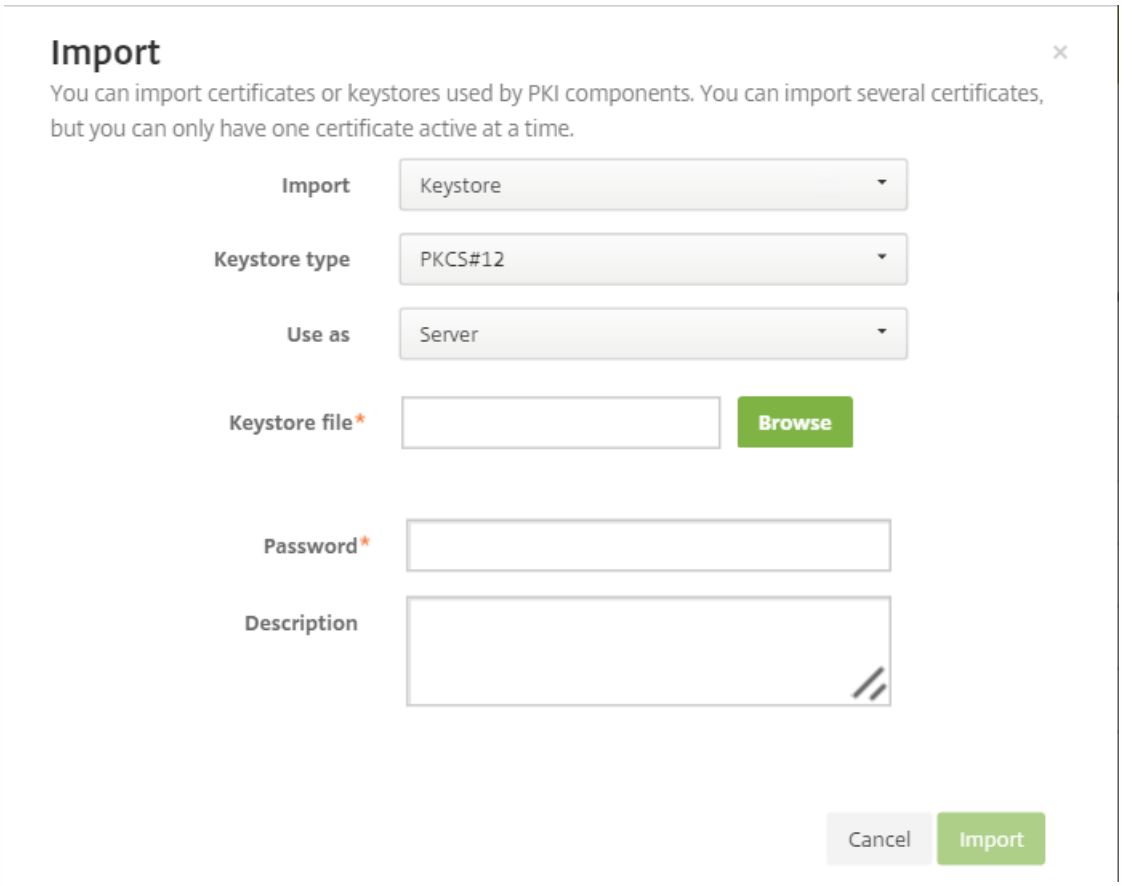
将证书上载到 XenMobile

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。 此时将显示**设置**屏幕。

2. 依次单击**证书**和**导入**。

3. 输入以下参数：

- **导入**：密钥库
- **密钥库类型**：PKCS#12
- **使用目的**：服务器
- **密钥库文件**：单击浏览选择刚刚创建的 .pfx 证书。
- **密码**：输入为此证书创建的密码。



4. 单击**导入**。

5. 验证是否已正确安装证书。 证书应显示为用户证书。

为基于证书的身份验证创建 PKI 实体

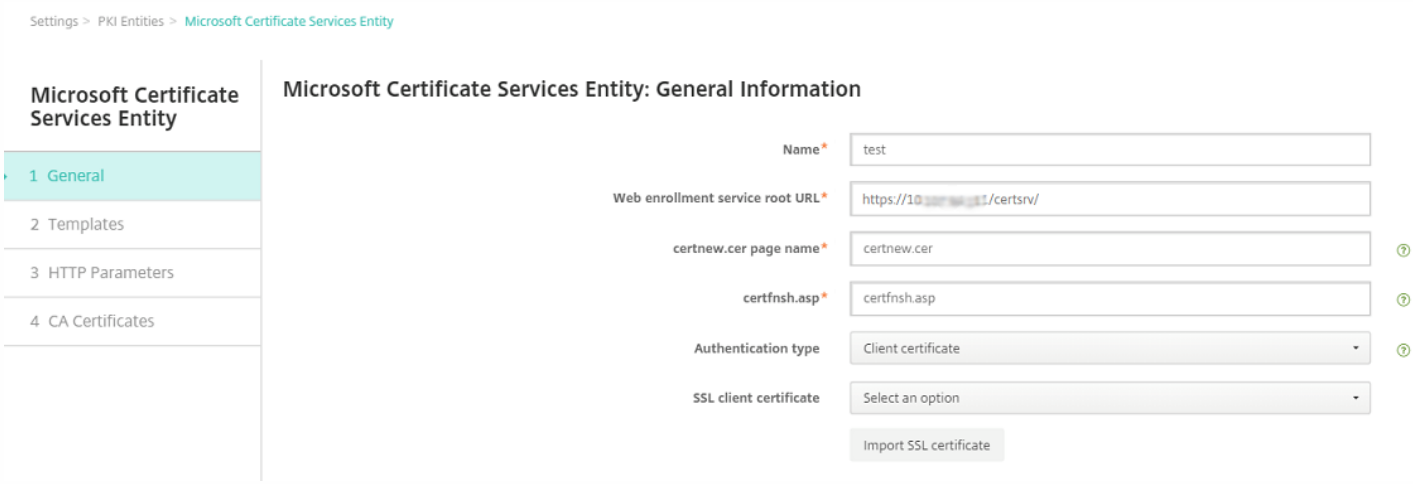
1. 在**设置**中，转至**更多 > 证书管理 > PKI 实体**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

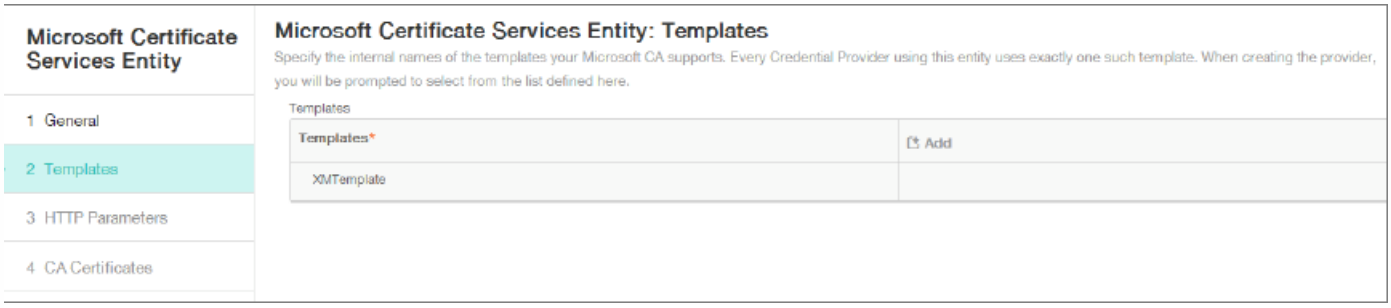
2. 依次单击**添加**和 **Microsoft 证书服务实体**。 此时将显示 **Microsoft 证书服务实体: 常规信息**屏幕。

3. 输入以下参数：

- **名称**：键入任意名称
- **Web 注册服务根 URL**：https://RootCA-URL/certsrv/
  请务必在 URL 路径结尾添加一个斜杠 (/)。
- **certnew.cer 页面名称**：certnew.cer（默认值）
- **certfnsh.asp**：certfnsh.asp（默认值）
- **身份验证类型**：客户端证书
- **SSL 客户端证书**：选择要用于颁发 XenMobile 客户端证书的用户证书。

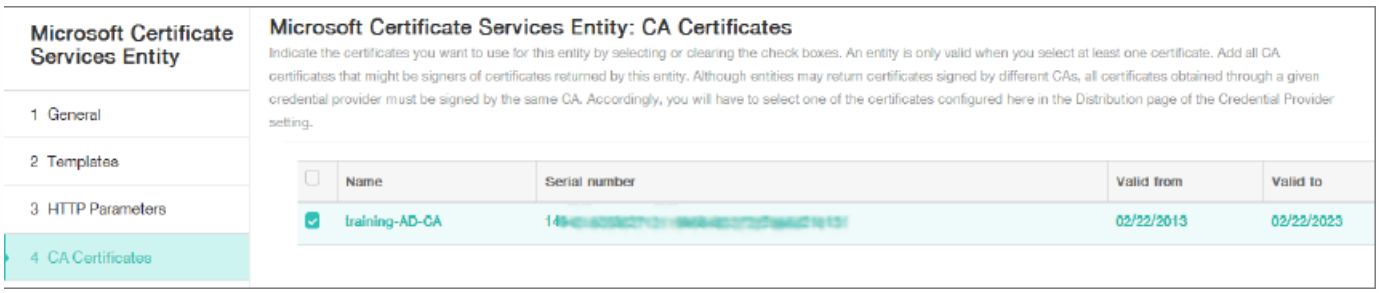


4. 在**模板**下，添加配置 Microsoft 证书时创建的模板。 请勿添加空格。



5. 跳过“HTTP 参数”，然后单击 **CA 证书**。

6. 选择与您的环境对应的根 CA 名称。 此根 CA 属于从 XenMobile 客户端证书中导入的链的一部分。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 单击**保存**。

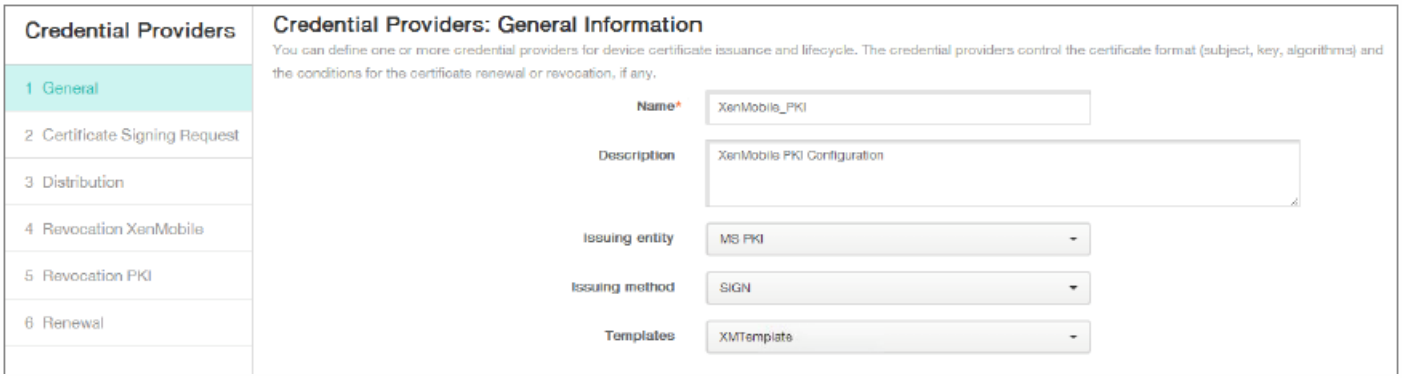
配置凭据提供程序

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**：键入任意名称。
- **说明**：键入任意说明。
- **颁发实体**：选择之前创建的 PKI 实体。
- **颁发方法**：签名
- **模板**：选择在“PKI 实体”下添加的模板。



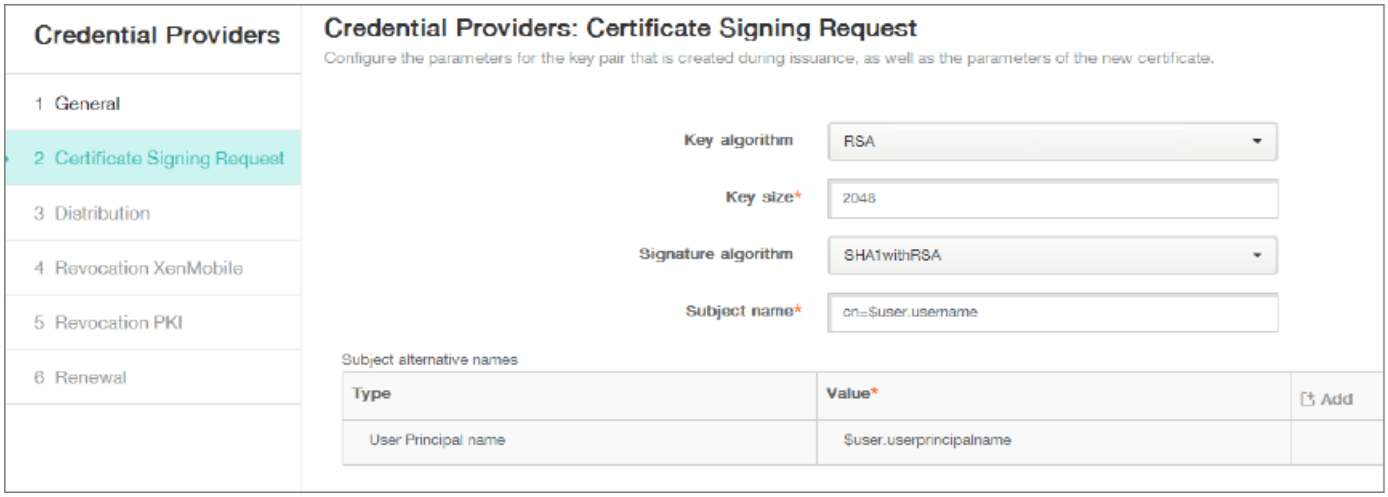
4. 单击**证书签名请求**，然后输入以下参数：

- **密钥算法**：RSA
- **密钥大小**：2048
- **签名算法**：SHA1withRSA
- **使用者名称**：cn=$user.username

对于**使用者备用名称**，请单击**添加**，然后输入以下参数：

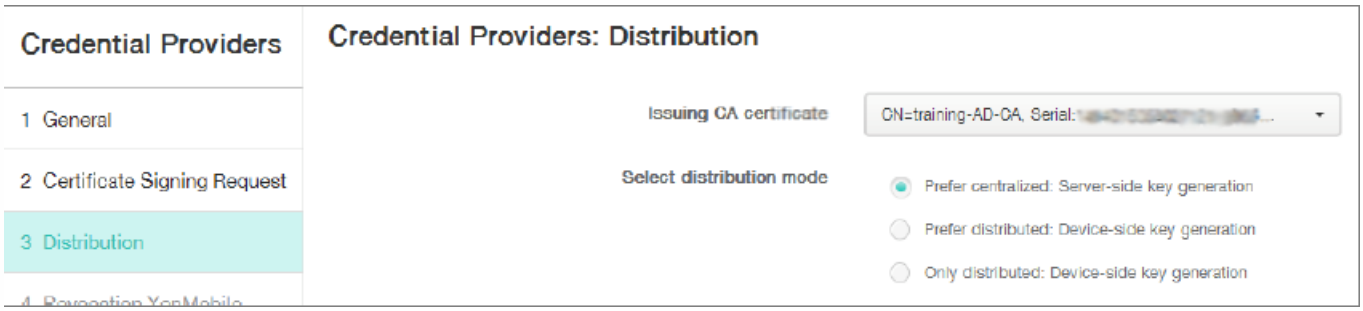
- **类型**：用户主体名称
- **值**：$user.userprincipalname

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 单击**分发**并输入以下参数：

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

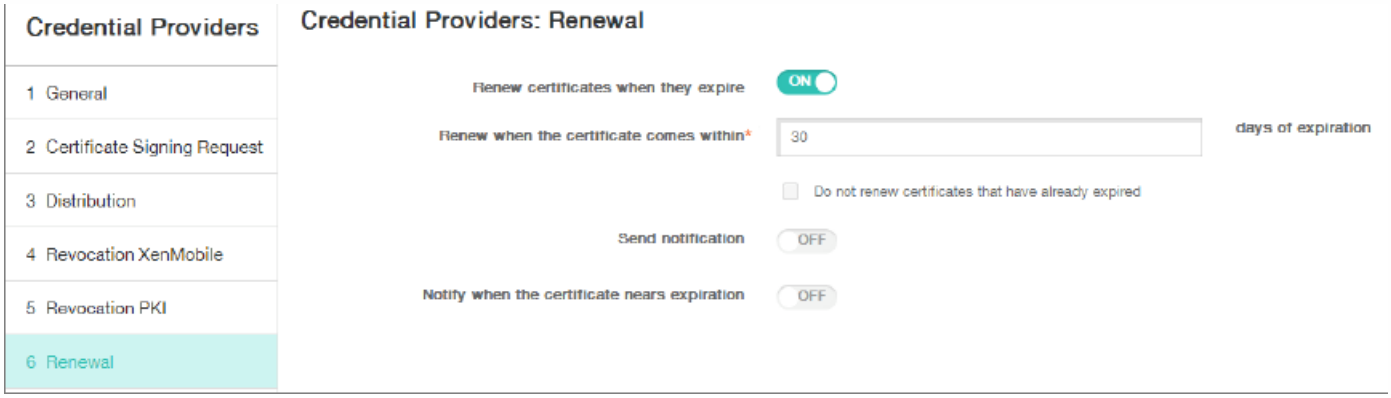


6. 对于下面两个部分，即**吊销 XenMobile** 和**吊销 PKI**，请根据需要设置参数。 鉴于本文的目的，我们将跳过这两个选项。

7. 单击**续订**。

8. 对于**在证书过期时续订**，请选择**开**。

9. 将所有其他设置保留为默认设置，或者根据需要进行更改。

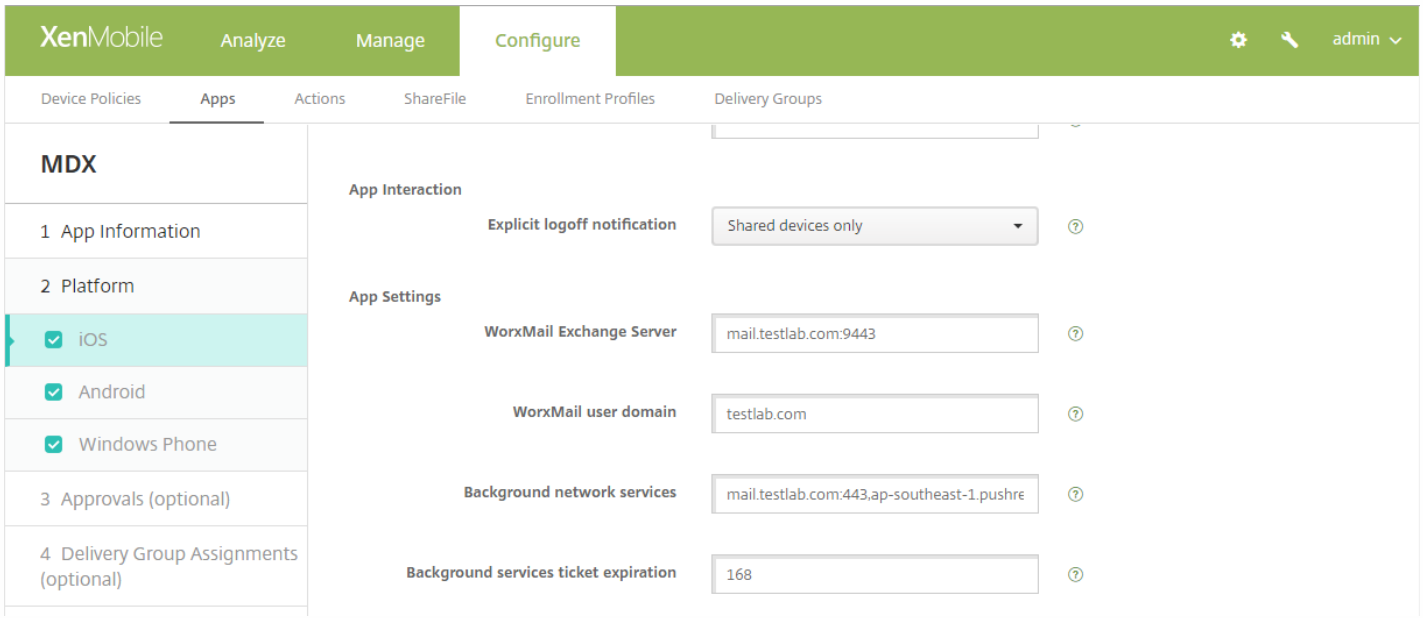


10. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

将 WorxMail 配置为使用基于证书的身份验证

将 WorxMail 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 NetScaler 证书交付

1. 登录到 XenMobile 控制台并单击右上角的齿轮图标。 此时将显示**设置**屏幕。

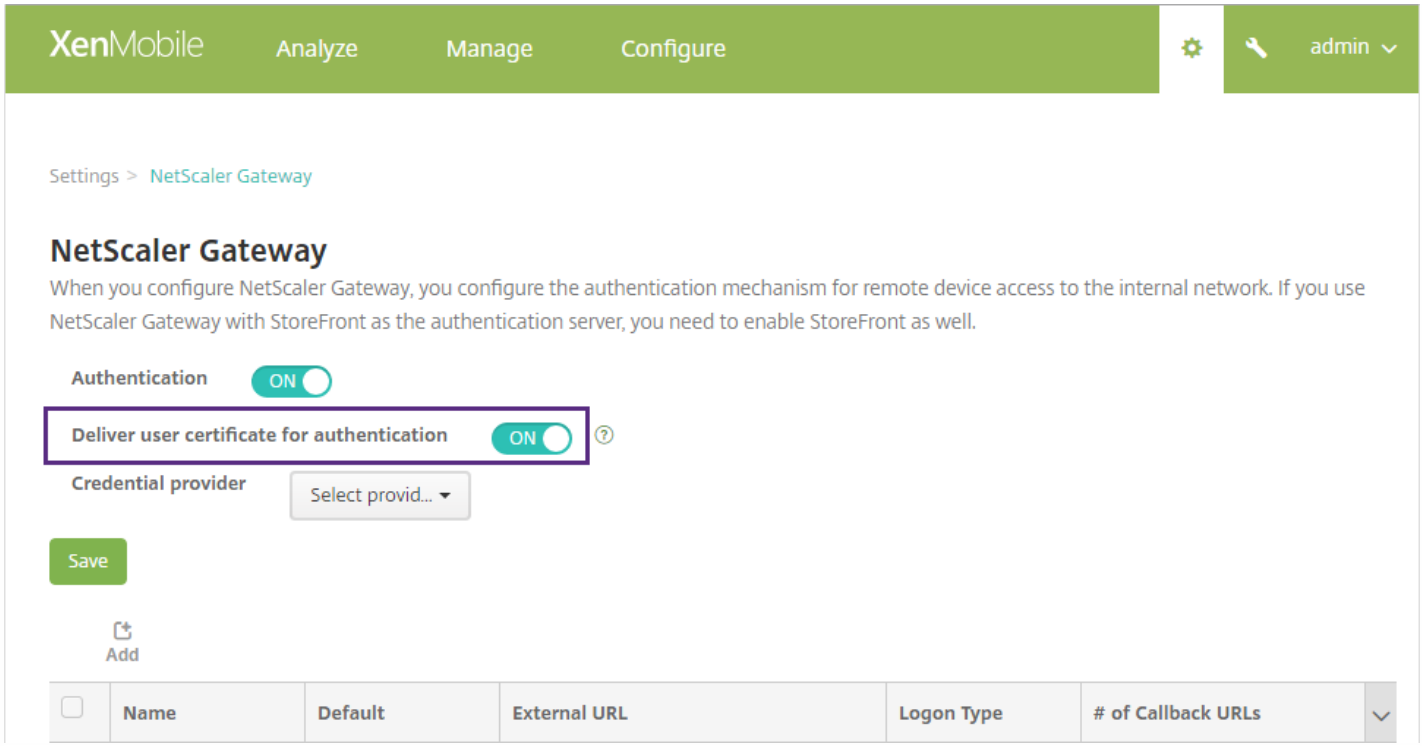
2. 在**服务器**下，单击 **NetScaler Gateway**。

3. 如果尚未添加 NetScaler Gateway，请单击**添加**并指定以下设置：

- **外部 URL**：https://YourNetScalerGatewayURL
- **登录类型**：证书
- **需要密码**：关
- **设为默认值**：开

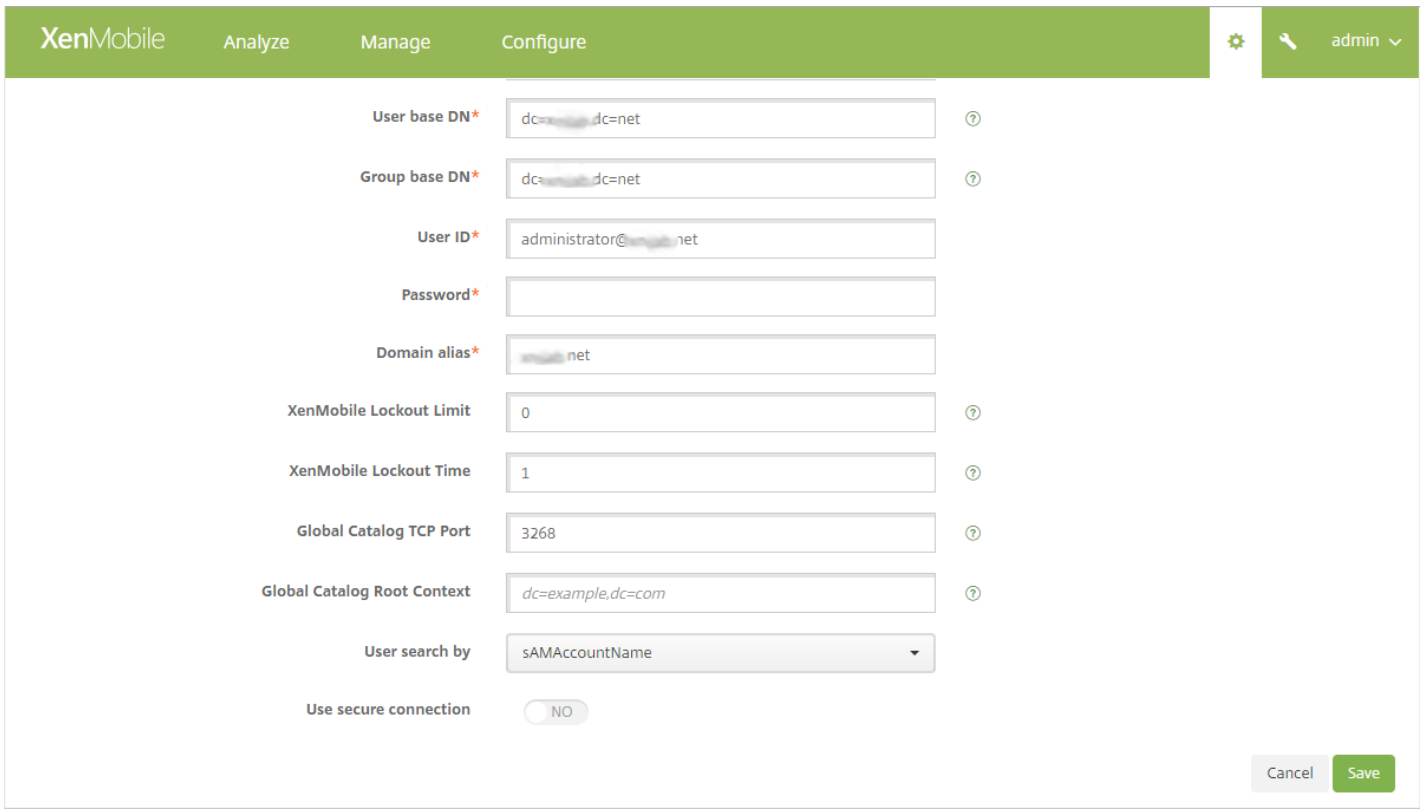
4. 对于**向用户提供用于身份验证的证书**，请选择**开**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 对于**凭据提供程序**，请选择一个提供程序，然后单击**保存**。

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



© 1999-2017 Citrix Systems, Inc. All rights reserved.

为 Windows Phone 8.1 创建企业中心策略

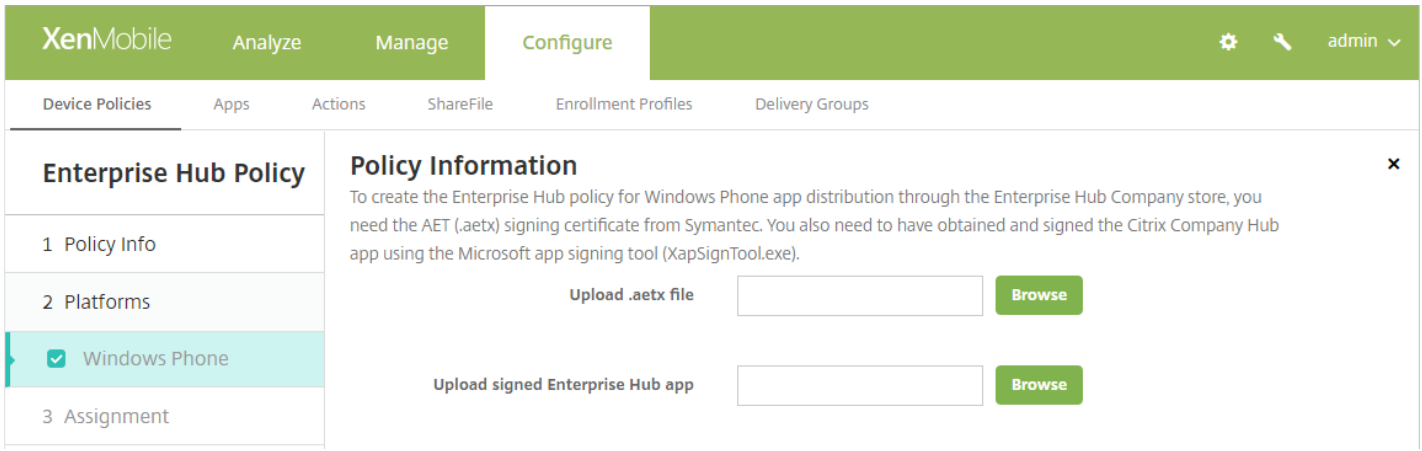
对于 Windows Phone 8.1 设备，必须创建企业中心设备策略才能交付 AETX 文件和 Worx Home 客户端。

> **注意**
>
> 请确保 AETX 和 Worx Home 文件都使用证书提供程序提供的相同企业证书以及来自 Windows 应用商店开发人员帐户的相同发布者 ID。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。

2. 单击**添加**，然后在**更多 > XenMobile 代理**下单击**企业中心**。

3. 命名该策略后，请务必为企业中心选择正确的 .AETX 文件和签名 Worx Home 应用程序。



4. 将该策略分配给交付组并保存。

使用 NetScaler for XenMobile 向导为证书身份验证配置 NetScaler Gateway

> **注意**
>
> 只能运行一次 NetScaler for XenMobile 向导。 如果已使用该向导，请按照下文“手动为证书身份验证配置 NetScaler Gateway”中的说明进行操作。

请在 NetScaler 设备上执行以下步骤，在 XenMobile 中配置证书身份验证。

1. 登录到 NetScaler。

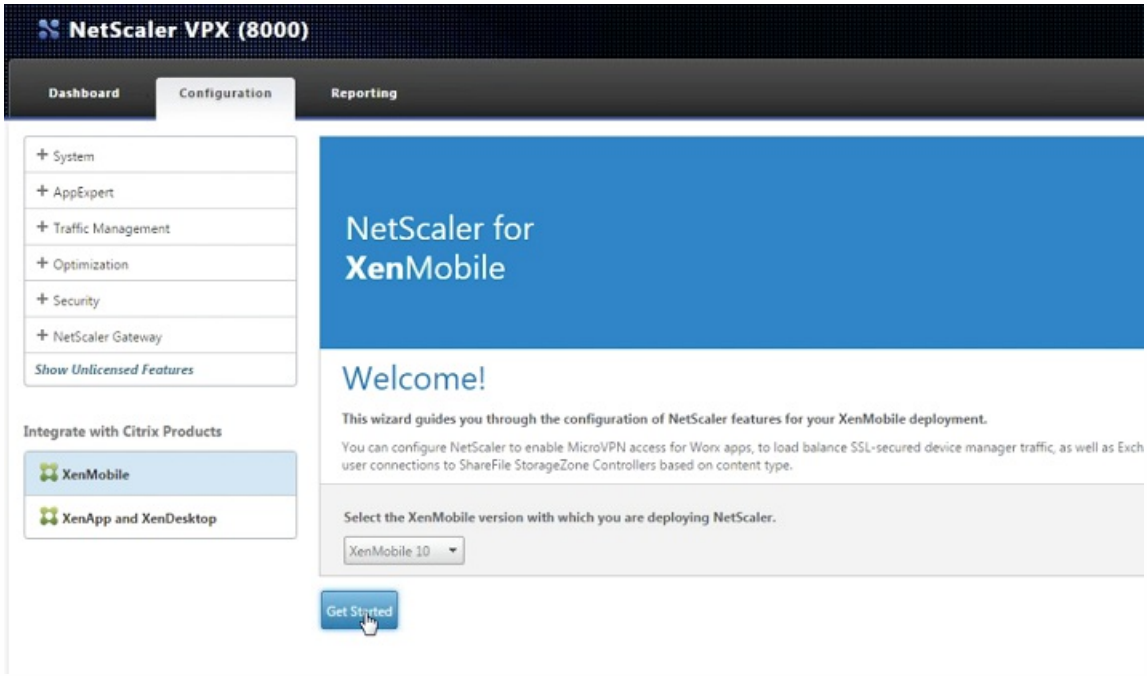
© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 在 **Configuration**（配置）下，转至 **Integrate with Citrix Products**（与 Citrix 产品集成），然后选择 **XenMobile**。

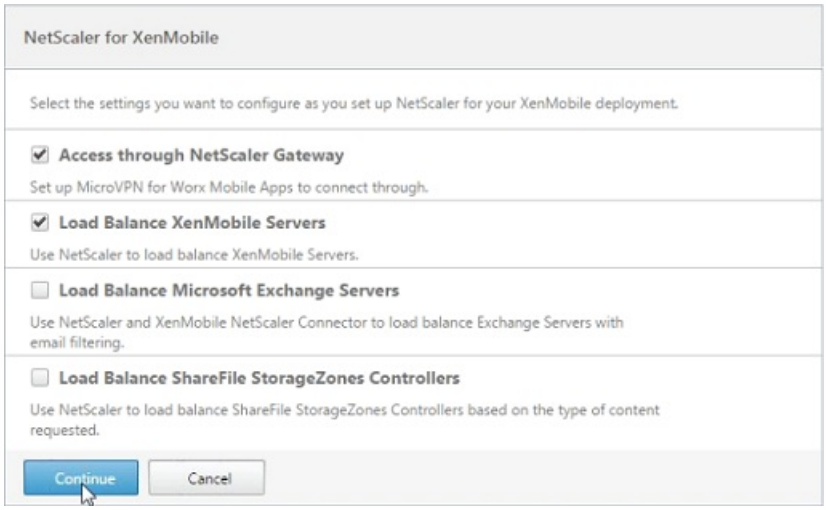
此时会打开一个向导，从中可以为 XenMobile 部署配置 NetScaler 功能。

3. 选择 **XenMobile 10**。

4. 单击 **Get Started**（开始）。



5. 在下一个屏幕上，选择 **Access through NetScaler Gateway**（通过 NetScaler Gateway 访问）（适用于 ENT 和 MAM 模式）和 **Load Balance XenMobile Servers**（对 XenMobile 服务器进行负载平衡），然后单击 **Continue**（继续）。



6. 在下一个屏幕上，输入面向外部的 NetScaler Gateway IP 地址，然后单击 **Continue**（继续）。

此时会出现“Server Certificate for NetScaler Gateway”（NetScaler Gateway 服务器证书）屏幕。

7. 您可以使用现有证书，也可以安装一个。 单击 **Continue**（继续）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

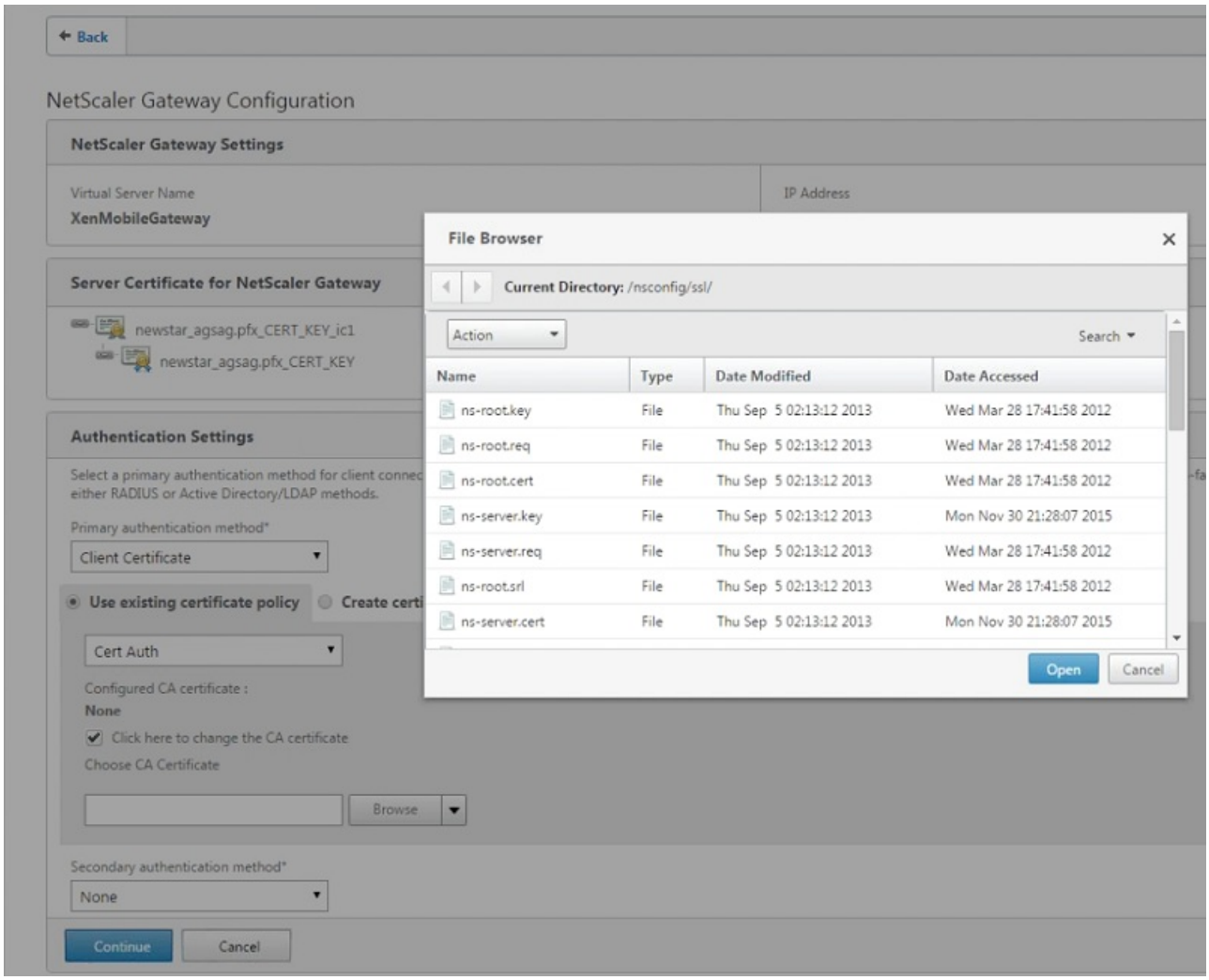
此时会出现 **Authentication Settings**（身份验证设置）屏幕。

8. 在 **Primary authentication method**（首选身份验证方法）字段中，选择 **Client Certificate**（客户端证书）。

此时会为接下来两个字段自动选择 **Use existing certificate policy**（使用现有证书策略）和 **Cert Auth**（证书身份验证）。以下各步骤假定您已配置证书策略。

如果需要创建证书策略，请单击 **Create certificate policy**（创建证书策略）并完成设置。 在 **XenMobile Server Certificate**（XenMobile 服务器证书）屏幕中，选择现有服务器证书或安装一个新证书。 如果正在运行多个 XenMobile 服务器，则需要为每个服务器添加一个证书。 对于 **Server Logon Name Attribute**（服务器登录名称属性），请指定 **userPrincipalName** 或 **samAccountName**。

9. 选择 **Click here to change the CA certificate**（单击此处更改 CA 证书），然后在 **Browse**（浏览）列表中，导航至所需的 CA 证书。



10. 将 **Second authentication method**（辅助身份验证方法）保留为 **None**（无），然后单击 **Continue**（继续）。

11. 在 **Device certificate**（设备证书）屏幕上，如果尚未安装证书，则必须从 XenMobile 控制台中导出此证书。 对此，请执行以下操作：

a. 在控制台中单击右上角齿轮图标，打开 **Settings**（设置）屏幕。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

b. 单击 **Certificate**（证书），然后从列表中选择 CA 证书。

c. 单击 **Export**（导出）。

d. 返回 NetScaler 向导，选择已导出（已下载）的证书进行安装。

e. 单击 **Continue**（继续）。

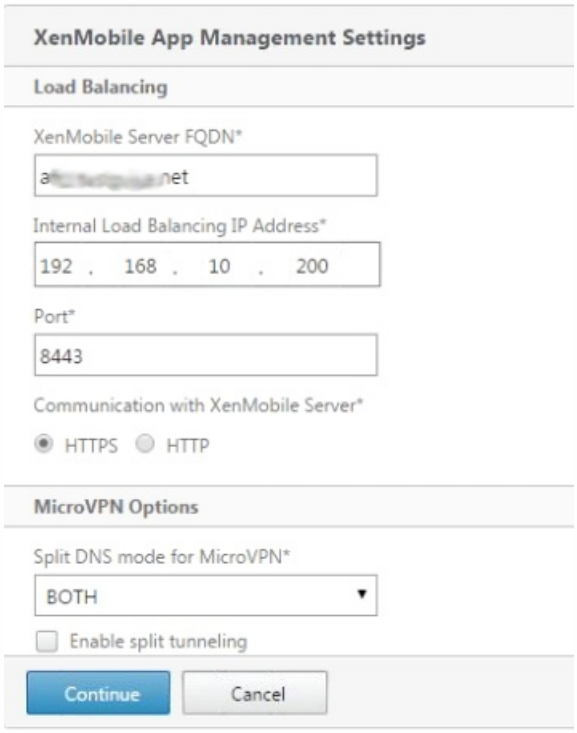
此时会显示已配置的 XenMobile 服务器 IP 地址。

12. 在 **Load Balancing**（负载平衡）屏幕中，输入 XenMobile 服务器 FQDN 和仅 MAM 内部负载平衡 IP 地址。

13. 由于这是一个 SSL 卸载部署，请在 **Communication with XenMobile Server**（与 XenMobile 服务器通信）中选择 **HTTP**。

此时 **Split DNS mode for MicroVPN**（为 MicroVPN 拆分 DNS 模式）字段会显示为 **BOTH**（两者）。

14. 单击 **Continue**（继续）。

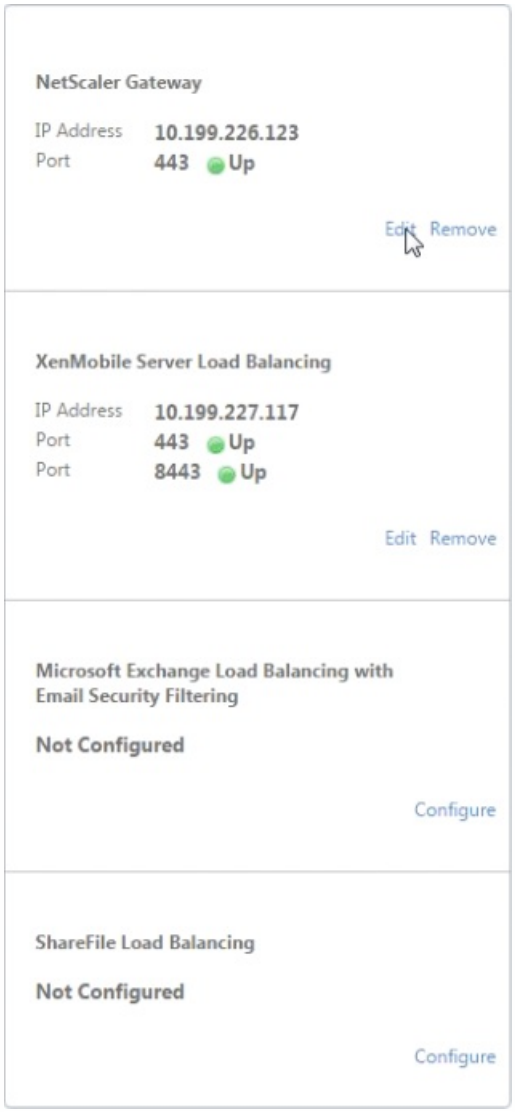


此时会显示已配置的 XenMobile 服务器 IP 地址。

15. 单击 **Continue**（继续）。

在 NetScaler 控制板上，确认已按如下所示配置 NetScaler Gateway 和 XenMobile 负载平衡。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



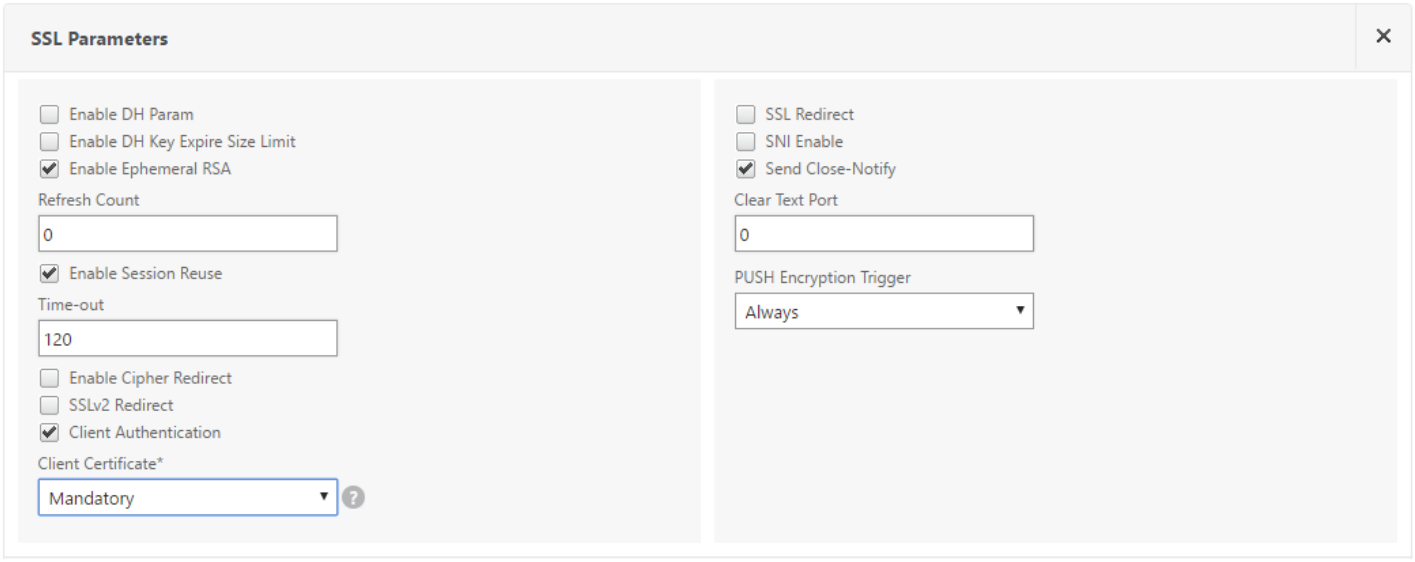
16. 如果要使用用户证书中的 sAMAccount 属性作为用户主体名称 (UPN) 的备选名称，请按下一部分内容所述配置证书配置文件。

手动为证书身份验证配置 NetScaler Gateway

1. 在 **Traffic Management（流量管理）> Load Balancing（负载平衡）> Virtual Servers（虚拟服务器）**下，转至每个虚拟服务器（443 和 8443），更新 **SSL Parameters**（SSL 参数），然后将 **Enable Session Reuse**（启用会话重用）设置为 **DISABLED**（已禁用）。

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 在 NetScaler Gateway 虚拟服务器上，在 **Enable Client Authentication（启用客户端身份验证）-> Client Certificate（客户端证书）**上，选择 **Client Authentication**（客户端身份验证），对于 **Client Certificate**（客户端证书），请选择 **Mandatory**（强制）。



3. 创建一个新身份验证证书策略，以使 XenMobile 能够从 Worx Home 向 NetScaler Gateway 提供的客户端证书中提取 **User Principal Name**（用户主体名称）或 **sAMAccount**。

4. 为证书配置文件设置以下参数：

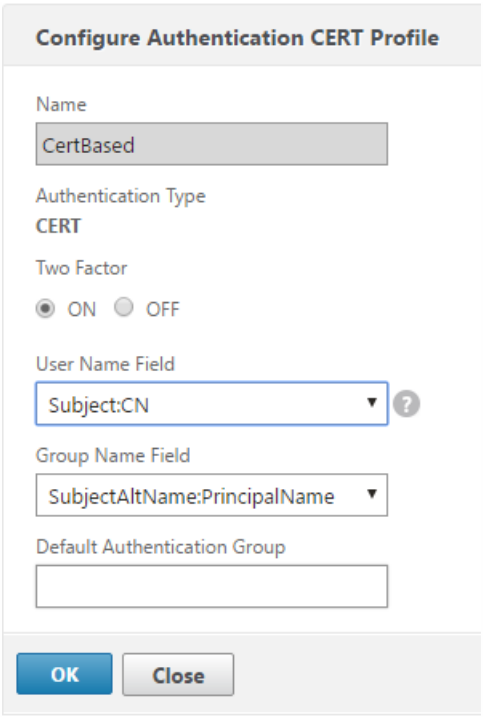
身份验证类型：**CERT**

双重：**ON** 或 **OFF**

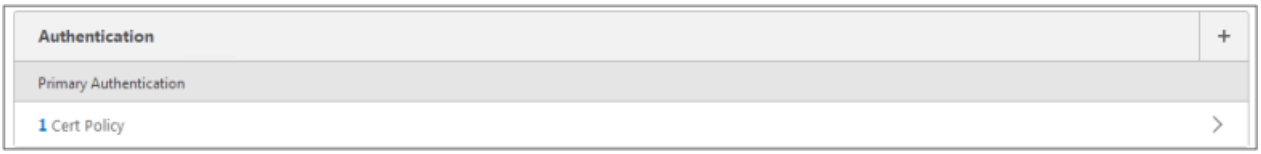
用户名字段：**Subject:CN**

组名称字段：**SubjectAltName:PrincipalName**

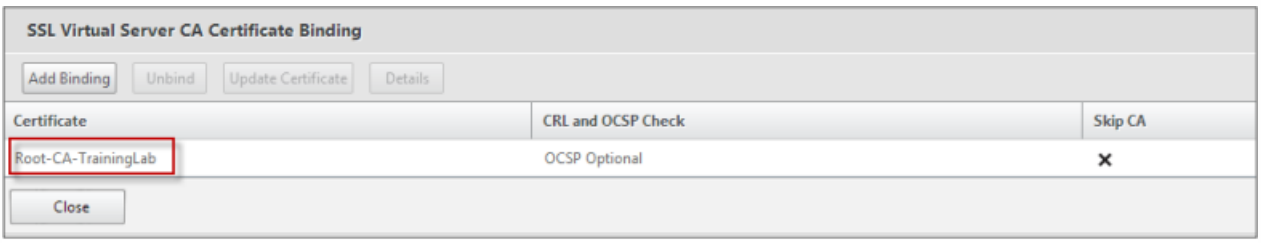
© 1999-2017 Citrix Systems, Inc. All rights reserved.

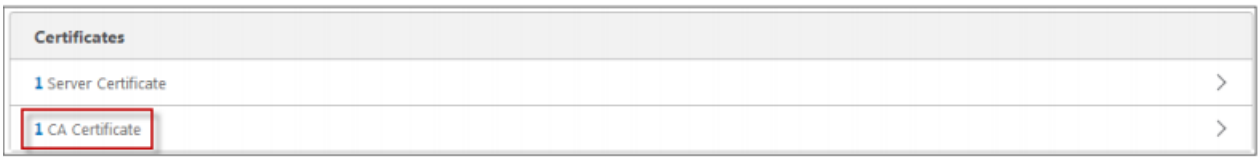


5. 仅绑定证书身份验证策略作为 NetScaler Gateway 虚拟服务器中的 **Primary Authentication**（主身份验证）。



6. 绑定根 CA 证书以验证向 NetScaler Gateway 提供的客户端证书的信任关系。





客户端证书配置故障排除

成功配置后，用户工作流将如下所示：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 用户注册其移动设备。

2. XenMobile 提示用户创建 Worx PIN。

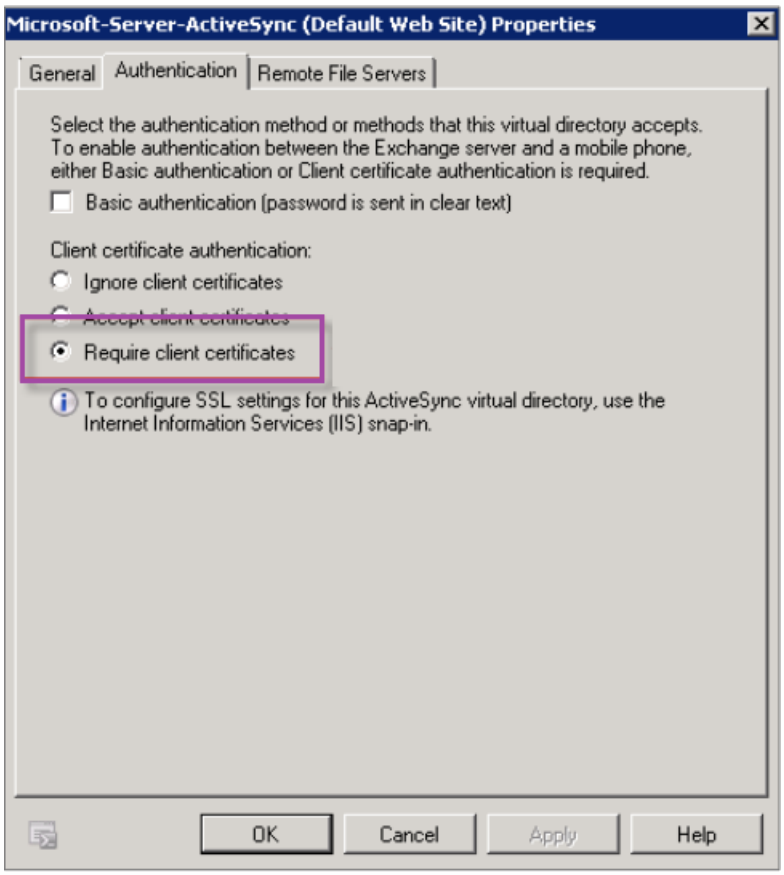
3. 随后用户被重定向到 Worx Store。

4. 用户启动 WorxMail for iOS、WorxMail for Android 或 WorxMail for Windows Phone 8.1 时，XenMobile 将不提示其提供用户凭据以配置其邮箱。 相反，WorxMail 将从 Worx Home 请求客户端证书，并将其提交给 Microsoft Exchange Server 以进行身份验证。 如果 XenMobile 在用户启动 WorxMail 时提示用户提供凭据，请检查您的配置。

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

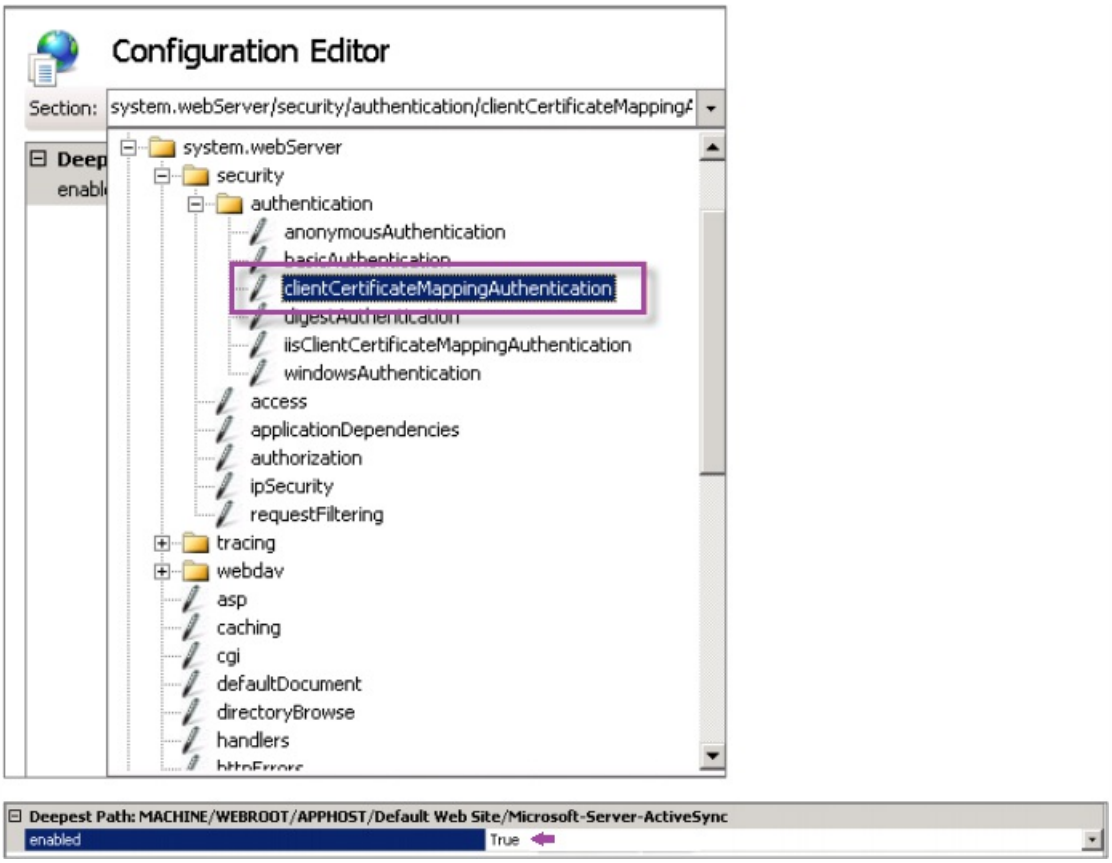
1. 如果 Microsoft Exchange Server ActiveSync 使用专用 SSL 服务器证书来确保通信安全，请确认是否已在移动设备上安装根证书/中间证书。

2. 验证为 ActiveSync 选择的身份验证类型是否为 **Require client certificates**（需要客户端证书）。



3. 在 Microsoft Exchange Server 上，检查 **Microsoft-Server-ActiveSync** 站点是否已启用客户端证书映射身份验证（默认禁用）。 该选项位于 **Configuration Editor（配置编辑器）> Security（安全性）> Authentication（身份验证）**下。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



注意：选择 **True**（真）后，请务必单击 **Apply**（应用）以使更改生效。

4. 在 XenMobile 控制台中检查 NetScaler Gateway 设置：确保**向用户提供用于身份验证的证书**设置为**开**，并且**凭据提供程序**选择了正确的配置文件，如上文“在 XenMobile 中配置 NetScaler 证书交付”中所述。

要确定是否已向移动设备提供客户端证书，请执行以下操作：

1. 在 XenMobile 控制台中，转至**管理 > 设备**，然后选择设备。

2. 单击**编辑**或**显示更多**。

3. 转至**交付组**部分，并搜索以下条目：

    NetScaler Gateway Credentials : Requested credential, CertId=

要验证是否已启用客户端证书协商，请执行以下操作：

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

    netsh http show sslcert

2. 如果 **Negotiate Client Certificate**（协商客户端证书）的值为 **Disabled**（已禁用），请运行以下命令将其启用：

    netsh http delete sslcert ipport=0.0.0.0:443

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

如果无法通过 XenMobile 向 Windows Phone 8.1 设备提供根证书/中间证书，请执行以下操作：

- 通过电子邮件将根证书/中间证书 (.cer) 文件发送到 Windows Phone 8.1 设备并直接安装。

如果无法在 Windows Phone 8.1 上成功安装 WorxMail，请执行以下操作：

- 验证应用程序注册令牌 (.AETX) 文件是否已使用企业中心设备策略通过 XenMobile 提供。
- 验证创建应用程序注册令牌时使用的证书提供程序提供的企业证书是否与用于打包 WorxMail 并对 Worx Home 应用程序进行签名的企业证书相同。
- 验证是否正在使用相同的发布者 ID 签名并打包 Worx Home、WorxMail 和应用程序注册令牌。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PKI 实体

Oct 21, 2016

XenMobile 公钥基础结构 (PKI) 实体配置代表执行实际 PKI 操作（颁发、吊销和状态信息）的组件。 这些组件可能是 XenMobile 的内部组件（在此情况下称为任意实体）或者 XenMobile 外部组件（如果组件是企业基础结构的一部分）。

XenMobile 支持以下类型的 PKI 实体：

- 任意证书颁发机构 (CA)
- 通用 PKI (GPKI)
- Microsoft Certificate Services

XenMobile 支持以下 CA 服务器：

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

常见 PKI 概念

无论何种类型，每个 PKI 实体均拥有下列功能的子集：

- 签名：基于证书签名请求 (CSR) 颁发新证书。
- 提取：恢复现有证书和密钥对。
- 吊销：吊销客户端证书。

关于 CA 证书

配置 PKI 实体时，必须向 XenMobile 指明哪个 CA 证书将成为该实体所颁发（或从该实体恢复）的证书的签署者。 同一 PKI 实体可以返回任意多个不同 CA 签名（提取或新签名）的证书。 必须在 PKI 实体配置时提供其中每个 CA 的证书。 为此，需要将证书上载到 XenMobile，然后在 PKI 实体中引用这些证书。 对于任意 CA，证书是隐式签名 CA 证书，但对于外部实体，必须手动指定证书。

通用 PKI

通用 PKI (GPKI) 协议是 XenMobile 专有协议，在 SOAP Web 服务层之上运行，用于实现与各种 PKI 解决方案的统一交互。 GPKI 协议定义以下三个基本 PKI 操作：

- 签名：适配器可以接收 CSR，将其传输到 PKI 并返回新签名的证书。
- 提取：适配器能够从 PKI 检索（恢复）现有证书和密钥对（取决于输入参数）。
- 吊销：适配器能够让 PKI 吊销给定证书。

GPKI 协议的接收端是 GPKI 适配器。 该适配器将基本操作转换为其构建所针对的特定类型的 PKI。 换言之，RSA 有一个 GPKI 适配器，EnTrust 有另一个适配器，依此类推。

作为 SOAP Web 服务端点，GPKI 适配器可发布自我描述的 Web 服务描述语言 (WSDL) 定义。 创建 GPKI PKI 实体相当于通过 URL 或上载文件本身为 XenMobile 提供该 WSDL 定义。

可以选择是否支持适配器中的各个 PKI 操作。 如果适配器支持某个给定操作，可以称之为拥有相应功能（签名、提取或吊销）。 这些功能中的每一项均可与一组用户参数相关联。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用户参数是指由 GPKI 适配器针对特定操作定义的参数，您需要为 XenMobile 提供这些参数的值。 XenMobile 通过解析 WSDL 文件，决定适配器支持哪些操作（拥有哪些功能）以及适配器针对每个操作所需的参数。 如果选择此项，则使用 SSL 客户端身份验证保护 XenMobile 与 GPKI 适配器之间的连接。

添加通用 PKI

1. 在 XenMobile 控制台中，单击**配置** > **设置** > **更多** > **PKI 实体**。

2. 在 **PKI 实体**页面上，单击**添加**。

此时将显示一个列表，其中显示了可以添加的 PKI 实体的类型。

3. 单击**通用 PKI 实体**。

此时将显示“通用 PKI 实体: 常规信息”页面。

4. 在**通用 PKI 实体: 常规信息**页面上，执行以下操作：

- **名称**：键入 PKI 实体的描述性名称。
- **WSDL URL**：键入描述适配器的 WSDL 的位置。
- **身份验证类型**：单击要使用的身份验证方法。
- **无**
- **HTTP Basic**：提供连接到适配器所需的 用户名 和密码。
- **客户端证书**：选择正确的 SSL 客户端证书。

5. 单击**下一步**。

此时将显示“通用 PKI 实体: 适配器功能”页面。

6. 在 **通用 PKI 实体: 适配器功能**页面上，检查与适配器关联的功能和参数，然后单击**下一步**。

此时将显示**通用 PKI 实体: 颁发 CA 证书**页面。

7. 在“通用 PKI 实体: 颁发 CA 证书”页面上，选择要用于此实体的证书。

注意：尽管实体可能会返回不同 CA 签发的证书，但通过给定证书提供商获取的所有证书必须由同一个 CA 颁发。 相应地，在配置**凭据提供程序**设置时，在**分发**页面上，选择在此处配置的证书之一。

8. 单击**保存**。

实体将显示在 PKI 实体表格中。

Microsoft Certificate Services

XenMobile 通过其 Web 注册界面与 Microsoft Certificate Services 交互。 XenMobile 仅支持通过该界面颁发新证书（相当于 GPKI 签名功能）。

要在 XenMobile 中创建 Microsoft CA PKI 实体，必须指定证书服务 Web 界面的基本 URL。 如果选择此项，则使用 SSL 客户端身份验证保护 XenMobile 与证书服务 Web 界面之间的连接。

添加 Microsoft 证书服务实体

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击**更多** > **PKI 实体**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 在 **PKI 实体**页面上，单击**添加**。

此时将显示一个列表，其中显示了可以添加的 PKI 实体的类型。

3. 单击 **Microsoft 证书服务实体**。

此时将显示 **Microsoft 证书服务实体: 常规信息**页面。

4. 在 Microsoft 证书服务实体: 常规信息页面上，执行以下操作之一：

- 名称：为新建实体键入一个名称，此名称以后将用于指代该实体。 实体名称必须唯一。
- Web enrollment service root URL（Web 注册服务根 URL）：键入 Microsoft CA Web 注册服务的基本 URL，例如，https://192.0.2.13/certsrv/。 该 URL 可能会使用纯 HTTP 或 HTTP-over-SSL。
- certnew.cer 页面名称：certnew.cer 页面的名称。 若非因为某些原因重命名了此页面，请使用默认名称。
- certfnsh.asp：certfnsh.asp 页面的名称。 若非因为某些原因重命名了此页面，请使用默认名称。
- 身份验证类型：单击要使用的身份验证方法。
- 无
- HTTP 基本认证：提供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**下一步**。

此时将显示 **Microsoft 证书服务实体: 模板**页面。 在此页面上，指定 Microsoft CA 所支持模板的内部名称。 创建凭据提供程序时，从此处定义的列表中选择模板。 使用此实体的每个凭据提供程序仅使用一个此类模板。

有关 Microsoft 证书服务模板要求，请参阅适用于您的 Microsoft 服务器版本的 Microsoft 文档。 除证书中所述证书格式外，XenMobile 对其分发的证书没有任何要求。

6. 在 **Microsoft 证书服务实体: 模板**页面上，单击**添加**，键入模板的名称，然后单击**保存**。 为要添加的每个模板重复执行此步骤。

7. 单击**下一步**。

此时将显示 **Microsoft 证书服务实体: HTTP 参数**页面。 在此页面上，您可以指定 XenMobile 应在 Microsoft Web 注册界面的 HTTP 请求中引入的自定义参数。 仅当您已在 CA 上自定义脚本时，此操作才有用。

8. 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，您需要将系统通过该实体获取的证书的签署者告诉 XenMobile。 续订 CA 证书时，在 XenMobile 中更新此证书，随之更改将以透明方式应用于实体。

9. 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。

10. 单击**保存**。

实体将显示在 PKI 实体表格中。

NetScaler 证书吊销列表 (CRL)

XenMobile 支持对第三方证书颁发机构使用证书吊销列表 (CRL)。 如果您配置了 Microsoft CA，XenMobile 将使用 NetScaler 管理吊销。 配置基于客户端证书的身份验证时，请考虑是否需要配置 NetScaler 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh**（启用 CRL 自动刷新）。 此步骤可确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证；XenMobile 将重新颁发新证书，因为 XenMobile 在某个证书被吊销的情况下不限制用户生成用户证书。 此设置提高了 CRL 检

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

查过期的 PKI 实体时 PKI 实体的安全性。

任意 CA

向 XenMobile 提供 CA 证书及关联的私钥时，将创建任意 CA。 XenMobile 将根据您指定的参数，在内部处理证书颁发、吊销和状态信息。

配置任意 CA 时，可以选择为此 CA 激活在线证书状态协议(OCSP) 支持。 当且仅当启用 OCSP 支持时，CA 会向 CA 颁发的证书添加 id-pe-authorityInfoAccess 扩展，并在后面的位置指向 XenMobile 内部 OCSP 响应者。

https://server/instance/ocsp
配置 OCSP 服务时，必须为相关任意实体指定 OCSP 签名证书。 可以将 CA 证书本身用作签署者。 如果要避免 CA 私钥的不必要暴露（建议避免），必须创建一个由 CA 证书签名并包含 id-kp-OCSPSigning extendedKeyUsage 扩展的委派 OCSP 签名证书。

XenMobile OCSP Responder Service 支持在请求中使用基本 OCSP 响应及以下散列算法：

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

响应通过 SHA-256 及签名证书的密钥算法（DSA、RSA 或 ECDSA）进行签名。

添加任意 CA

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击**更多** > **PKI 实体**。

2. 在 **PKI 实体**页面上，单击**添加**。

此时将显示一个列表，其中显示了可以添加的 PKI 实体的类型。

3. 单击**任意 CA**。

此时将显示**任意 CA: 常规信息**页面。

4. 在**任意 CA: 常规信息**页面上，执行以下操作：

- **名称**：键入任意 CA 的描述性名称。
- **用于对证书请求进行签名的 CA 证书**：单击任意 CA 用于为证书请求签名的证书。 此证书列表使用您通过**配置** > **设置** > **证书**上载到 XenMobile 的私钥从 CA 证书生成。

5. 单击**下一步**。

此时将显示**任意 CA: 参数**页面。

6. 在**任意 CA: 参数**页面上，执行以下操作：
- **序列号生成器**：任意 CA 为其颁发的证书生成序列号。 从此列表中，单击**按顺序**或**不按顺序**，以确定生成此序列号的方式。
- **下一个序列号**：键入一个值，用于确定颁发的下一个号码。
- **证书有效期**：键入证书有效的天数。
- **密钥用法**：通过将相应的密钥设置为**开**，标识任意 CA 所颁发证书的目的。 设置后，CA 仅限于为这些目的颁发证书。
- **扩展密钥用法**：要添加其他参数，请单击**添加**，键入密钥名称，然后单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 单击**下一步**。

此时将显示**任意 CA: 分发**页面。

8. 在**任意 CA: 分发**页面上，选择分发模式:

- **集中式: 服务器端密钥生成**。 Citrix 建议使用集中选项。 在服务器上生成并存储私钥，然后分发到用户设备。
- **分布式: 设备端密钥生成**。 私钥在用户设备上生成。 分布式模式使用 SCEP 并需要采用 keyUsage keyEncryption 的 RA 加密证书和采用 KeyUsage digitalSignature 的 RA 签名证书。 同一个证书可以同时用于加密和签名。

9. 单击**下一步**。

此时将显示**任意 CA: 联机证书状态协议(OCSP)** 页面。

在**任意 CA: 联机证书状态协议(OCSP)**页面上，执行以下操作：

- 如果要向此 CA 签署的证书添加 AuthorityInfoAccess (RFC2459) 扩展，请将**为此 CA 启用 OCSP 支持**设置为**开**。 此扩展指向位于 https://server/instance/ocsp 的 CA OCSP 响应者。
- 如果启用了 OCSP 支持，请选择 OSCP 签名 CA 证书。 此证书列表使用您上载到 XenMobile 的 CA 证书生成。

10. 单击**保存**。

任意 CA 将显示在 PKI 实体表格中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

凭据提供程序

Aug 11, 2016

凭据提供程序是在 XenMobile 系统的各个部分中使用的实际证书配置。 它们定义证书的来源、参数和生命周期，无论这些证书是设备配置的一部分还是独立的配置，都将按原样推送到设备。

设备注册约束证书生命周期。 也就是说，XenMobile 在注册前不颁发证书，尽管 XenMobile 可能会在注册的过程中颁发某些证书。 此外，在某个注册环境下从内部 PKI 颁发的证书会在注册被吊销时吊销。 管理关系终止后，不保留任何有效证书。

一个凭据提供程序配置可用于多个位置，从而达到通过一个配置同时控制任意多个证书的效果。 这时，其唯一性在于部署资源和部署。 例如，如果凭据提供程序 P 在配置 C 中部署到设备 D，则 P 的颁发设置决定着部署到 D 的证书。 同样，更新 C 时将应用 D 的续订设置，删除 C 或吊销 D 时将应用 D 的吊销设置。

基于此，XenMobile 中的凭据提供程序配置执行以下操作：

- 确定证书的来源。
- 确定获取证书的方法：签发新证书还是提取（恢复）现有证书和密钥对。
- 确定用于颁发或恢复的参数。 例如，密钥大小、密钥算法、标识名、证书扩展名等证书签名请求 (CSR) 参数。
- 确定将证书交付给设备的方式。
- 决定吊销条件。 尽管在管理关系终止后 XenMobile 中的所有证书都将被吊销，但该配置可以指定在更早时间吊销，例如在删除关联设备配置时吊销。 此外，在某些情况下，XenMobile 中关联证书的吊销可能会发送给后端公钥基础结构 (PKI)；也就是说，XenMobile 中关联证书的吊销可能导致其在 PKI 上也随之吊销。
- 决定续订设置。 通过指定凭据提供程序获取的证书可以在即将过期时自动续订，或者采用与之不同的方式，在接近过期时由系统发送通知。

各种配置选项的可用程度主要取决于为凭据提供程序选择的 PKI 实体的类型和颁发方法。

证书颁发方法

可以采用两种途径获取证书（称为颁发方法）：

- 签名。 利用此方法，颁发包括创建新私钥、创建 CSR 和将 CSR 提交给证书颁发机构 (CA) 进行签名。 XenMobile 支持对三种 PKI 实体（MS 证书服务实体、通用 PKI 和任意 CA）使用此签名方法。
- 提取。 利用此方法，用于 XenMobile 的颁发是指对现有密钥对的恢复。XenMobile 仅支持对通用 PKI 使用提取方法。

凭据提供程序使用签名或提取颁发方法。 所选方法会影响可用配置选项。 具体而言，仅当颁发方法为签名时，才可以使用 CSR 配置和分散交付。 提取的证书始终作为 PKCS#12 发送给设备，相当于签名方法的集中交付模式。

证书交付

XenMobile 中可用的证书交付模式共有两种：集中和分散。 分散模式使用简单证书注册协议 (SCEP)，并且只有在客户端支持该协议时方可使用（仅限 iOS）。 在某些情况下，必须采用分散模式。

对于支持分散式（SCEP 辅助）交付的凭据提供程序，需要特殊的配置步骤：设置注册机构 (RA) 证书。 需要 RA 证书是因为，使用 SCEP 协议时，XenMobile 充当实际 CA 的委派者（注册者），并且必须向客户端证明其拥有充当此类角色的机构。 通过向 XenMobile 提供上述证书，可以建立该机构。

需要两种不同的证书角色（尽管同一证书即可满足这两项要求）：RA 签名和 RA 加密。 这些角色的限制如下：

- RA 签名证书必须拥有 X.509 密钥用法数字签名。
- RA 加密证书必须拥有 X.509 密钥用法密钥加密。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

要配置凭据提供程序的 RA 证书，必须首先将证书上载到 XenMobile，然后在凭据提供程序中链接到这些证书。

仅当凭据提供程序为证书角色配置了证书时，才可将凭据提供程序视为支持分散式交付。 每个凭据提供程序均可配置为首选集中模式、首选分散模式或要求分散模式。 实际结果取决于具体环境：如果环境不支持分散模式，但是凭据提供程序要求使用该模式，部署将失败。 同样地，如果环境要求使用分散模式，但凭据提供程序不支持该模式，部署也将失败。 在所有其他情况下，将会应用首选设置。

下面显示了 SCEP 在整个 XenMobile 的分布：

上下文	支持 SCEP	需要 SCEP
iOS 配置文件服务	是	是
iOS 移动设备管理注册	是	否
iOS 配置文件	是	否
SHTP 注册	否	否
SHTP 配置	否	否
Windows Phone 注册	否	否
Windows Phone 配置	否	否

证书吊销

有三种类型的吊销。

- **内部吊销**。 内部吊销影响由 XenMobile 维护的证书状态。 在 XenMobile 评估收到的证书时，或者 XenMobile 必须提供某些证书的 OCSP 状态信息时，将考虑此状态。 凭据提供程序配置决定在各种条件下此状态受到的影响。 例如，凭据提供程序可以指定：将通过证书提供商获取的证书从设备中删除后，将这些证书标记为已吊销。
- **外部传播的吊销**。 又称“吊销 XenMobile”，这种类型的吊销适用于从外部 PKI 获取的证书。 在凭据提供程序配置定义的条件下，当证书由 XenMobile 在内部吊销时也会同时在 PKI 上吊销。 用于执行吊销的调用需要使用支持吊销的通用 PKI (GPKI) 实体。
- **外部引起的吊销**。 又称“吊销 PKI”，这种类型的吊销适用于从外部 PKI 获取的证书。 每次 XenMobile 评估指定证书的状态时，XenMobile 都将向 PKI 查询该状态。 如果证书已吊销，XenMobile 将在内部吊销该证书。 此机制使用 OCSP 协议。

这三种类型并不互斥，而是可以一起应用：外部吊销或独立查询结果导致内部吊销，内部吊销进而潜在影响外部吊销。

证书续订

证书续订由吊销现有证书和颁发另一个证书两个过程组成。

请注意，XenMobile 将首先尝试获取新证书，然后再吊销之前的证书，以避免在颁发失败时造成服务中断。 如果采用分散式（支持 SCEP）交付，仅当证书成功安装到设备后再进行吊销，否则，将在新证书发送给设备之前进行吊销，无论新证书是否

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装成功。

配置吊销时，需要指定特定的持续时间（天）。 如果设备已连接，服务器将验证证书的“不晚于”日期是否晚于当前日期减去指定的持续时间。 如果晚于两者之差，则尝试续订。

创建凭据提供程序

凭据提供程序的配置方式有多种，主要取决于为其选择的颁发实体和颁发方法。 可以将使用内部实体（如任意实体）和使用外部实体（如 Microsoft CA 或 GPKI）的凭据提供程序区分开。 任意实体的颁发方法始终为签名。这意味着，在执行每个颁发操作时，XenMobile 都将使用为该实体选择的 CA 证书给新密钥对签名。 该密钥对是在设备上生成还是在服务器上生成取决于所选的分发方法。

1. 在 XenMobile Web 控制台中，单击控制台右上角的齿轮图标，然后单击**更多** > **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。 此名称之后将用于在 XenMobile 控制台的其他部分引用该配置。
- **说明**：凭据提供程序的说明。 尽管此字段为可选字段，但说明在以后可帮助您记住此凭据提供程序的详细信息。
- **颁发实体**：单击凭据颁发实体。
- **颁发方法**：单击 **Sign**（签名）或 **Fetch**（提取）以选择系统用于从已配置的实体获取证书的方法。对于客户端证书身份验证，请使用 **Sign**（签名）。
- 如果模板列表可用，请为凭据提供程序选择模板。

4. 单击**下一步**。

注意：在**设置** > **更多** > **PKI 实体**中添加 Microsoft 证书服务实体后，这些模板将变为可用。

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，执行以下操作：

- **密钥算法**：单击用于获取新密钥对的密钥算法。 可用值为 **RSA**、**DSA** 和 **ECDSA**。
- **密钥大小**：键入密钥对的大小，以位为单位。 此字段为必填字段。
  注意：允许的值取决于密钥类型；例如，DSA 密钥的最大大小为 1024 位。 为避免错误的负值（取决于基础硬件或软件），XenMobile 不强制实施密钥大小。 您应始终先在测试环境中测试凭据提供程序配置，然后在生产环境中激活这些配置。

- **签名算法**：单击用于新证书的值。 值取决于密钥算法。
- **使用者名称**：键入新证书使用者的标识名 (DN)。 例如：
  CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation。 此字段为必填字段。

  例如，对于客户端证书身份验证，请好似用以下设置：

  密钥算法：RSA
  密钥大小：2048
  签名算法：SHA1withRSA
  使用者名称：cn=$user.username

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 要向**使用者备用名称**表格中添加新条目，请单击**添加**。 选择备用名称的类型，然后在第二列中键入一个值。

对于客户端证书身份验证，请指定以下设置：

类型：用户主体名称
值：$user.userprincipalname

注意：与使用者名称相同，可以在值字段中使用 XenMobile 宏。

7. 单击**下一步**。

此时将显示**凭据提供程序: 分发**页面。

8. 在**凭据提供程序: 分发**页面上，执行以下操作：

- 在**颁发 CA 证书**列表中，单击提供的 CA 证书。 由于凭据提供程序使用任意 CA 实体，因此该凭据提供程序的 CA 证书将始终为在该实体上配置的 CA 证书；该证书在此显示是为了与使用外部实体的配置保持一致。
- 在**选择分发模式**中，单击以下生成和分发密钥方式中的一种：
  - **首选集中式: 服务器端密钥生成**。 Citrix 建议采用此集中模式选项。 它支持 XenMobile 支持的所有平台，并且在使用 NetScaler Gateway 身份验证时也需要使用此模式。 在服务器上生成并存储私钥，然后分发到用户设备。
  - **首选分布式: 设备端密钥生成**。 在用户设备上生成并存储私钥。 分散模式使用 SCEP 并需要采用 keyUsage keyEncryption 的 RA 加密证书和采用 KeyUsage digitalSignature 的 RA 签名证书。 同一个证书可以同时用于加密和签名。
  - **仅限分布式: 设备端密钥生成**。 此选项与“首选分布式: 设备端密钥生成”的工作方式相同，但是此选项是“仅限”而非“首选”，当设备端生成密钥失败或不可用时，没有其他选项可用。

如果选择 **Prefer distributed: Device-side key generation**（首选分散模式: 设备端生成密钥）或 **Only distributed: Device-side key generation**（仅限分散模式: 设备端生成密钥），请单击 RA 签名证书和 RA 加密证书。 同一个证书可用于这两个目的。 此时将显示有关这些证书的新字段。

9. 单击**下一步**。

此时将显示**凭据提供程序: 吊销 XenMobile** 页面。 在此页面上，配置 XenMobile 在内部将通过此提供程序配置颁发的证书标记为吊销的条件。

12. 在**凭据提供程序: 吊销 XenMobile** 页面上，执行以下操作：

- 在**吊销已颁发的证书**中，选择一个表明何时应吊销证书的选项。
- 如果希望 XenMobile 在吊销证书时发送通知，请将**发送通知**设置为**开**并选择通知模板。
- 如果要在从 XenMobile 吊销证书后也在 PKI 上吊销此证书，请将**吊销 PKI 上的证书**设置为**开**，并在**实体**列表中，单击某个模板。 “实体”列表将显示具有吊销功能的所有可用 GPKI 实体。 从 XenMobile 吊销证书后，吊销调用将发送给在“实体”列表中选择的 PKI。

13. 单击**下一步**。

此时将显示**凭据提供程序: 吊销 PKI** 页面。 请在此页面上指出吊销证书时应对 PKI 执行的操作。 您还可以选择创建通知消息。

14. 在**凭据提供程序: 吊销 PKI** 页面上，如果要从 PKI 吊销证书，请执行以下操作：

- 将**启用外部吊销检查**设置更改为**开**。 此时将显示其他与吊销 PKI 相关的字段。
- 在 **OCSP 响应者 CA 证书**列表中，单击证书使用者的标识名 (DN)。 **注意**：可以为 DN 字段值使用 XenMobile 宏。 例如：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation

- 在**吊销证书时**列表中，单击吊销证书时对 PKI 实体执行的以下操作之一：

  不执行任何操作。

  续订证书。

  吊销和擦除设备。

- 如果希望 XenMobile 在吊销证书时发送通知，请将**发送通知**的值设置为**开**。

可以从两个通知选项中选择：

- 如果选择**选择通知模板**，则可以选择预先写好的通知消息，且之后可以进行自定义。 这些模板位于“通知模板”列表中。
- 如果选择**输入通知详细信息**，则可以自行编写通知消息。 除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

15. 单击**下一步**。

此时将显示**凭据提供程序: 续订**页面。 在此页面上，您可以配置 XenMobile 以使其执行以下操作：

- 续订证书、在证书完成续订时发送通知（续订时通知）并从操作中排除已过期的证书（后两项操作为可选操作）。
- 为即将过期的证书发送通知（续订前通知）。

16. 在**凭据提供程序: 续订**页面上，如果要在证书过期时进行续订，请执行以下操作：将**续订证书**设置为**开**。

此时将显示其他字段。

- 在 **Renew when the certificate comes within**（当证书在此范围内时续订）字段中，键入应在过期前多少天续订证书。
- （可选）选择**不续订已过期的证书**。 **注意**：在此情况下，“已过期”表示证书的“不晚于”日期在过去，不是指证书已经被吊销。 内部吊销后，XenMobile 将不会续订证书。

17. 如果希望 XenMobile 在续订证书后发送通知，请将**发送通知**设置为**开**。 可以从两个通知选项中选择：

- 如果选择**选择通知模板**，则可以选择预先写好的通知消息，且之后可以进行自定义。 这些模板位于通知模板列表中。
- 如果选择**输入通知详细信息**，则可以自行编写通知消息。 除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

18. 如果希望 XenMobile 在证书接近过期时发送通知，请将**证书即将过期时发送通知**设置为**开**。 可以从两个通知选项中选择：

- 如果选择**选择通知模板**，则可以选择预先写好的通知消息，且之后可以进行自定义。 这些模板位于**通知模板**列表中。
- 如果选择**输入通知详细信息**，则可以自行编写通知消息。 除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

19. 在**证书在此时间内提供时通知**字段中，键入应在证书过期前多少天发送通知。

20. 单击**保存**。

凭据提供程序将添加到凭据提供程序表格中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求 APNs 证书

Aug 11, 2016

要使用 Device Manager 注册并管理 iOS 设备，需要从 Apple 设置并创建 Apple 推送通知服务 (APNS) 证书。 本节概述了用于请求 APNs 证书的以下基本步骤：

- 使用 Windows Server 2012 R2 或 Windows 2008 R2 Server 和 Microsoft Internet Information Server (IIS) 或 Mac 计算机生成证书签名请求 (CSR)。
- 要求 Citrix 为 CSR 签名。
- 从 Apple 请求 APNs 证书。
- 将证书导入到 XenMobile。

注意：

- 利用 Apple 的 APNs 证书可通过 Apple 推送网络启用移动设备管理。 如果您无意或有意吊销了该证书，则无法管理自己的设备。
- 如果使用 iOS Developer Enterprise Program 创建 Mobile Device Manager 推送证书，则可能会因为将现有证书迁移到 Apple 推送证书门户而需要采取相应措施。

这些主题逐步概述了操作步骤，在本节中依次列出，如下所示：

步骤 1	在 IIS 上创建 CSR 在 Mac 上创建 CSR	使用 Windows Server 2012 R2 或 Windows 2008 R2 Server 和 Microsoft IIS 或在 Mac 计算机上生成 CSR。 Citrix 建议采用这种方法。
步骤 2	为 CSR 签名	在 XenMobile APNs CSR Signing Web 站点上 CSR 提交给 Citrix（需要具有 MyCitrix ID）。 Citrix 使用其移动设备管理 签名证书给 CSR 签名并返回 .plist 格式的已签名文件。
步骤 3	将已签名 CSR 提交到 Apple	在 Apple 推送证书门户（需要具有 Apple ID）将已签名 CSR 提交给 Apple，然后从 Apple 下载 APNS 证书。
步骤 4	使用 Microsoft IIS 创建 .pfx APNs 证书 在 Macintosh 计算机上创建 .pfx APNS 证书 使用 OpenSSL 创建 .pfx APNs 证书	将 APNS 证书导出为 PCKS #12 (.pfx) 证书（在 IIS、Mac 或 SSL 上）。
步骤 5	将 APNs 证书导入到 XenMobile	将证书导入到 XenMobile。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Apple MDM 推送证书迁移信息

在 iOS Developer Enterprise Program 中创建的移动设备管理 (MDM) 推送证书已迁移到 Apple 推送证书门户。 此迁移影响新 MDM 推送证书的创建以及现有 MDM 推送证书的续订、吊销和下载。 迁移不影响其他（非 MDM）APNs 证书。

如果 MDM 推送证书是在 iOS Developer Enterprise Program 中创建的，则以下情况适用：

- 已为您自动迁移证书。
- 可以在 Apple 推送证书门户续订证书，不会影响您的用户。
- 需要使用 iOS Developer Enterprise Program 吊销或下载预先存在的证书。

如果没有即将过期的 MDM 推送证书，则无需进行任何操作。 如果有即将过期的 MDM 推送证书，请联系您的 MDM 解决方案提供商。 然后将 iOS Developer Program Agent 登录到 Apple 推送证书门户（使用其 Apple ID ）。

所有新的 MDM 推送证书都必须在 Apple 推送证书门户中创建。 iOS Developer Enterprise Program 不再允许创建带有包含 com.apple.mgmt 的产品组合 ID（APNS 主题）的 App ID。

注意：必须跟踪用于创建证书的 Apple ID。 此外，该 Apple ID 应是公司 ID，而不是个人 ID。

使用 Microsoft IIS 创建 CSR

生成 iOS 设备的 APNS 证书请求的第一步是创建证书签名请求 (CSR)。 在 Windows 2012 R2 或 Windows 2008 R2 Server 上，可以使用 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. 键入相应的标识名 (DN) 信息，然后单击**下一步**。
5. 为加密服务提供程序选择 **Microsoft RSA SChannel Cryptographic Provider**，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**。

在 Mac 计算机上创建 CSR

1. 在运行 Mac OS X 的 Mac 计算机上，在**应用程序** > **实用工具**下面，启动钥匙串访问应用程序。
2. 打开**钥匙串访问**菜单，然后单击**偏好设置**。
3. 单击**证书**选项卡，将 **OCSP** 和 **CRL** 的选项改为**关闭**，然后关闭“偏好设置”窗口。
4. 在**钥匙串访问**菜单上，单击**证书助理** > **从证书颁发机构请求证书**。
5. “证书助理”将提示您输入以下信息：
    1. **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。
    2. **常用名称**。 负责管理证书的个人或角色帐户的公用名。
    3. **CA 电子邮件地址**。 证书颁发机构的电子邮件地址。
6. 选择**存储到磁盘**和**让我指定密钥对信息**选项，然后单击**继续**。
7. 输入 CSR 文件的名称，在您的计算机上保存此文件，然后单击**保存**。
8. 通过将**密钥大小**选择为 2048 位以及 **RSA 算法**指定密钥对信息，然后单击**继续**。 作为 APNs 证书流程的一部分，CSR 文件已可供上载。
9. 证书助理完成 CSR 流程后，单击**完成**。

使用 OpenSSL 创建 CSR

如果不能使用 Windows 2012 R2 或 Windows 2008 R2 Server 和 Microsoft Internet Information Server (IIS) 或 Mac 计算机生成证书签名请求 (CSR)，以提交到 Apple 来获取 Apple 推送通知服务 (APNS) 证书，可以使用 OpenSSL。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：要使用 OpenSSL 创建 CSR，首先需要从 OpenSSL Web 站点下载并安装 OpenSSL。

1. 在安装 OpenSSL 的计算机上，从命令提示窗口或 Shell 执行以下命令。
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

2. 此时将显示以下要求证书命名信息的消息。 根据请求输入信息。
   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. 将生成的 CSR 发送给 Citrix。

Citrix 会准备签名的 CSR 并通过电子邮件向您返回相关文件。

为 CSR 签名

证书需要通过 Citrix 签名以便可用于 XenMobile，然后您才能将其提交给 Apple。

1. 在浏览器中，转到 XenMobile APNs CSR Signing Web 站点。
2. 单击 **Upload the CSR**（上载 CSR）。
3. 浏览并选择证书。
   注意：证书必须采用 .pem/txt 格式。

4. 在“XenMobile APNs CSR Signing”页面，单击 **Sign**（签名）。 将为 CSR 签名并将签名后的 CSR 自动保存到已配置的下载文件夹。

将签名后的 CSR 提交给 Apple 以获取 APNs 证书

从 Citrix 收到已签名的证书签名请求 (CSR) 后，需要将其提交给 Apple，以获取 APNS 证书。

注意：有些用户报告登录 Apple 推送门户时遇到问题。 作为替代方法，可以先登录到 Apple 开发人员门户 (http://developer.apple.com/devcenter/ios/index.action)，之后再转到第 1 步中的 identity.apple.com 链接。

1. 在浏览器中，转到 https://identity.apple.com/pushcert。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 单击 **Create a Certificate**（创建证书）。
3. 如果是首次使用 Apple 创建证书，请选中 **I have read and agree to these terms and conditions**（我已阅读并同意这些条款和条件）复选框，然后单击 **Accept**（接受）。
4. 单击 **Choose File**（选择文件），浏览到计算机上已签名的 CSR，然后单击 **Upload**（上载）。 此时应显示一条确认消息，表明上载成功。
5. 单击 **Download**（下载）以检索 .pem 证书。
   注意：如果您使用的是 Internet Explorer 且文件扩展名丢失，则单击 **Cancel**（取消）两次，然后从下一窗口下载。

使用 Microsoft IIS 创建 .pfx APNs 证书

要将来自 Apple 的 APNs 证书用于 XenMobile，需要在 Microsoft IIS 中完成证书请求，将证书导出为 PCKS #12 (.pfx) 文件，然后将 APNs 证书导入 XenMobile。

重要：此任务需要使用用于生成 CSR 的 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**完成证书申请**。
4. 浏览至来自 Apple 的 Certificate.pem 文件。 然后，键入易于记忆的名称或证书名并单击**确定**。
5. 选择在第 4 步确定的证书，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**。
   注意：在 XenMobile 安装期间需要该证书密码。
7. 将 .pfx 证书复制到要安装 XenMobile 的服务器上。
8. 以管理员身份登录到 XenMobile 控制台。
9. 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。
10. 单击**证书**。 此时将显示**证书**页面。
11. 单击**导入**。 此时将显示**导入**对话框。
12. 在**导入**菜单中，选择**密钥库**。
13. 在**用作**中，选择 **APNs**。
14. 在**密钥库文件**中，单击**浏览**并导航到要导入的密钥库文件所在的位置，选择相应的文件。
15. 在**密码**中，键入分配给证书的密码。
16. 单击**导入**。

在 Macintosh 计算机上创建 .pfx APNS 证书

1. 在用于生成 CSR 的运行 Mac OS X 的 Mac 计算机上，找到从 Apple 接收的生产标识 (.pem) 证书。
2. 双击证书文件，将文件导入到密钥链。
3. 如果提示将证书添加到指定密钥链，则保持已选择的默认登录密钥链，然后单击**确定**。 新添加的证书会出现在证书列表中。
4. 单击该证书，然后在**文件**菜单上单击**导出**，开始将证书导出到 PCKS #12 (.pfx) 证书中。
5. 为证书文件命名用于 XenMobile 服务器的唯一名称，为保存的证书选择文件夹位置，选择 .pfx 文件格式，然后单击**保存**。
6. 输入用于导出证书的密码。 Citrix 建议使用具有唯一性的强密码。 还要确保证书和密码的安全性，以供以后使用和引用。
7. 钥匙串访问应用程序会提示您输入登录密码或选定的密钥链。 输入密码，然后单击**确定**。 保存的证书现在即可用于 XenMobile 服务器。
   注意：如果计划不保存和保留最初用于生成 CSR 并完成证书导出过程的计算机及用户帐户，Citrix 建议从本地系统保存或导出个人密钥及公钥。 否则，不能访问 APNs 证书以重新使用，且必须重复整个 CSR 和 APNs 过程。

使用 OpenSSL 创建 .pfx APNs 证书

使用 OpenSSL 创建证书签名请求 (CSR) 后，还可使用 OpenSSL 创建 .pfx APNS 证书。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 在命令提示窗口或者 Shell 中，执行以下命令。
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
2. 输入 .pfx 证书文件的密码。 记住此密码，因为在将证书上载到 XenMobile 时需要再次使用该密码。
3. 记下 .pfx 证书文件的位置，然后将该文件复制到 XenMobile 服务器中，以便可以使用 XenMobile Web 控制台来上载文件。

将 APNs 证书导入到 XenMobile

在请求并接收到新 APNs 证书后，可将 APNs 证书导入 XenMobile，以便首次添加该证书或者替换现有证书。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。
2. 单击**证书**。 此时将显示**证书**页面。
3. 单击**导入**。 此时将显示**导入**对话框。
4. 在**导入**菜单中，选择**密钥库**。
5. 在**用作**中，选择 **APNs**。
6. 浏览到计算机上的 .p12 文件。
7. 输入密码，然后单击**导入**。

有关 XenMobile 中的证书的详细信息，请参阅证书部分。

续订 APNs 证书

要续订 APNs 证书，需要执行与创建新证书相同的步骤。 然后，访问 Apple 推送证书门户并上载新证书。 登录后，就可看见自己的现有证书，或者看见从自己之前的 Apple 开发人员帐户导入的证书。 在“证书门户”上，续订证书的唯一区别是要单击**续订**。 要访问该站点，您必须拥有证书门户的开发人员帐户。

注意：要确定 APNs 证书的过期时间，请在 XenMobile 控制台中单击**配置** > **设置** > **证书**。 如果证书已过期，请勿吊销它。

1. 请使用 Microsoft Internet Information Services (IIS) 生成 CSR。
2. 在 XenMobile APNs CSR Signing Web 站点，上载新的 CSR，然后单击 **Sign**（签名）。
3. 将签名后的 CSR 提交给 Apple，站点为 Apple 推送证书门户。
4. 单击**续订**。
5. 使用 Microsoft IIS 生成 PCKS #12 (.pfx) APNs 证书。
6. 在 XenMobile 控制台中更新新 APNs 证书。 单击控制台右上角的齿轮图标。 此时将显示**设置**页面。
7. 单击**证书**。 此时将显示**证书**页面。
8. 单击**导入**。 此时将显示**导入**对话框。
9. 在**导入**菜单中，选择**密钥库**。
10. 在**用作**中，选择 **APNs**。
11. 浏览到计算机上的 .p12 文件。
12. 输入密码，然后单击**导入**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用户帐户、角色和注册设置

Aug 11, 2016

在 XenMobile 中，在 XenMobile 控制台的设置页面配置用户和组、用户和组的角色以及注册模式和邀请。 要打开**设置**页面，请单击控制台右上角的齿轮图标。

在**设置**页面上，可以执行以下操作：

- 单击**本地用户和组**，手动添加用户帐户或使用 .csv 置备文件导入帐户并管理本地组。 有关详细信息，请参阅：
  - 在 XenMobile 中添加、编辑或删除本地用户
  - 使用 .csv 置备文件导入用户帐户和置备文件格式
  - 在 XenMobile 中添加或删除组
- 单击**注册**可配置最多七种模式（每种模式均具有自己的安全级别和用户注册自己的设备必须采取的步骤数）并发送注册邀请。 有关详细信息，请参阅：
  - 配置注册模式并启用自助服务门户
  - 在 XenMobile 中启用自动发现以执行用户注册
- 单击**基于角色的访问控制**，向用户和组分配预定义角色或权限集合。 这些权限控制用户对系统功能的访问级别。 有关详细信息，请参阅：
  - 使用 RBAC 配置角色和 RBAC 角色和权限
- 单击**通知模板**以用于自动化操作、注册和发送给用户的标准通知消息。 配置通知模板以通过三种不同的通道发送消息：Worx Home、SMTP 或 SMS。 有关详细信息，请参阅：
  - 创建和更新通知模板

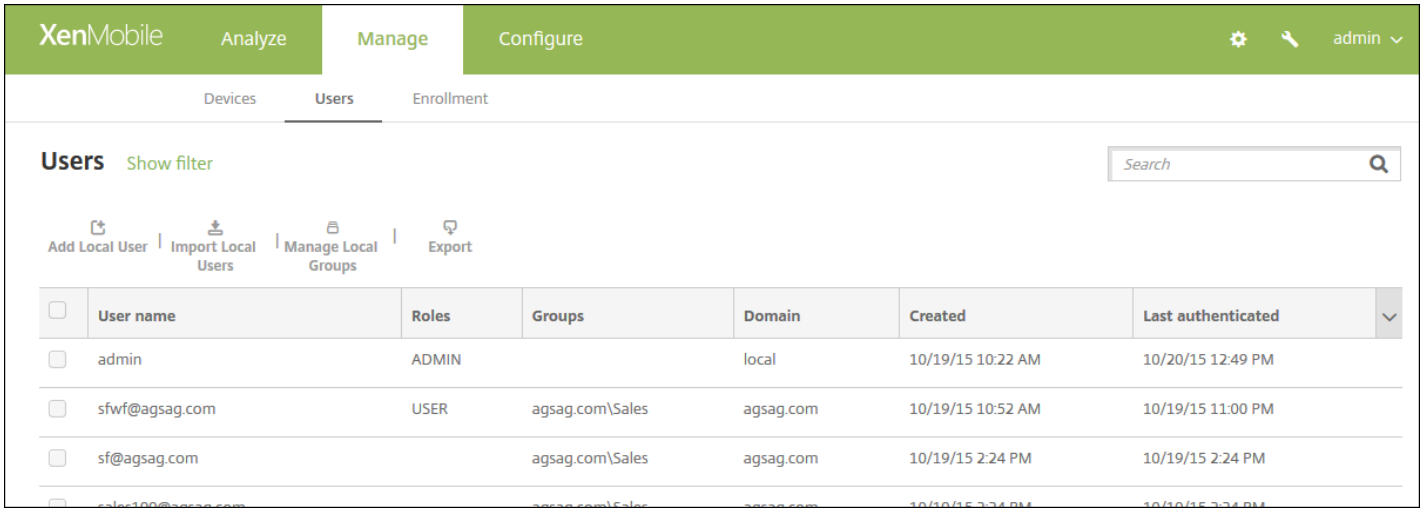
© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中添加、编辑或删除本地用户

Aug 11, 2016

可以手动向 XenMobile 中添加本地用户帐户，也可以使用置备文件导入帐户。 有关从置备文件导入用户的步骤，请参阅使用 .csv 置备文件导入用户帐户。

1. 在 XenMobile 控制台中，单击**管理 > 用户**。 此时将显示**用户**页面。

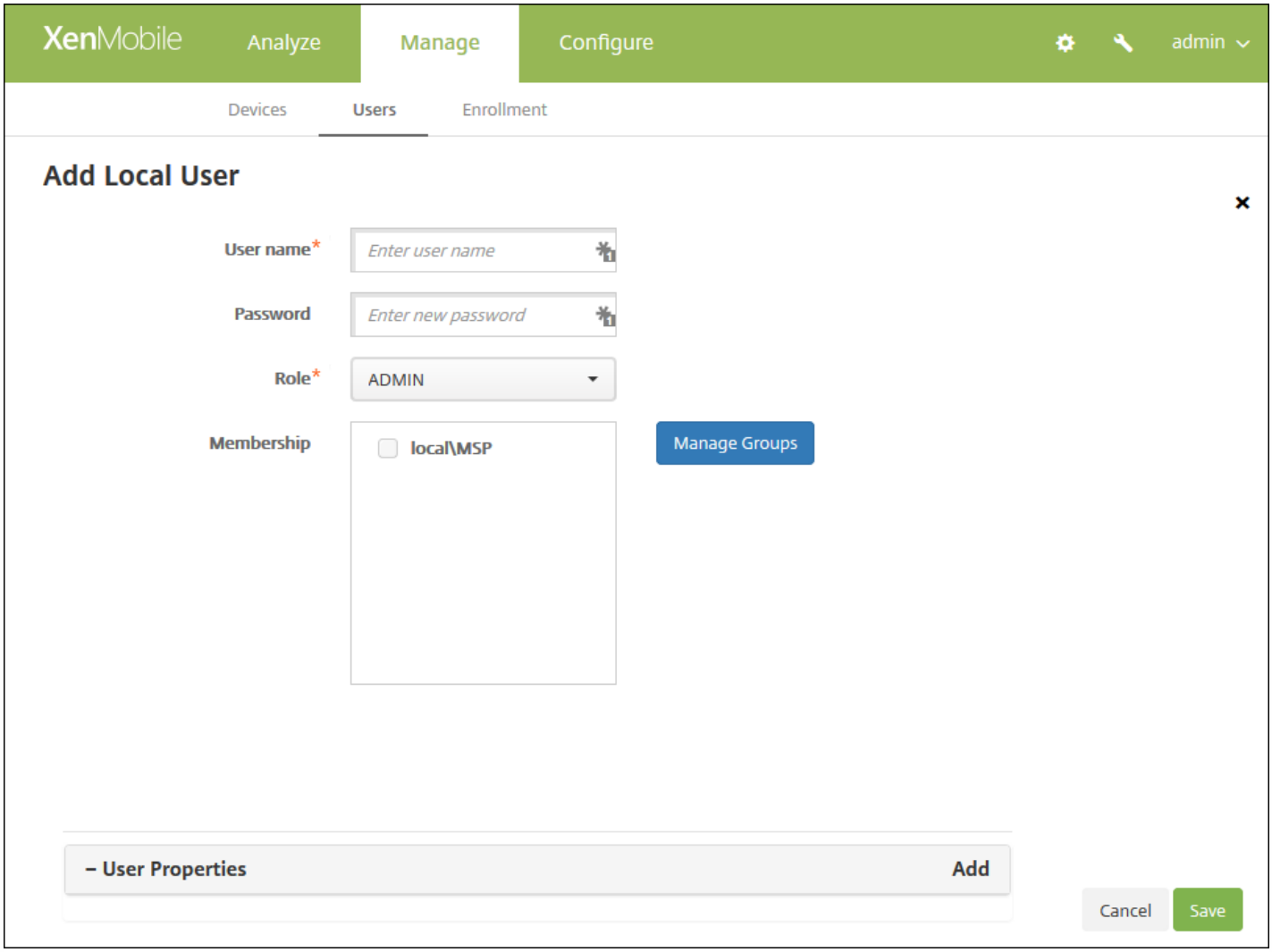


添加本地用户

此过程每次向 XenMobile 中添加一个用户。 要添加多个用户，请参阅使用 .csv 置备文件导入用户帐户。

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。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



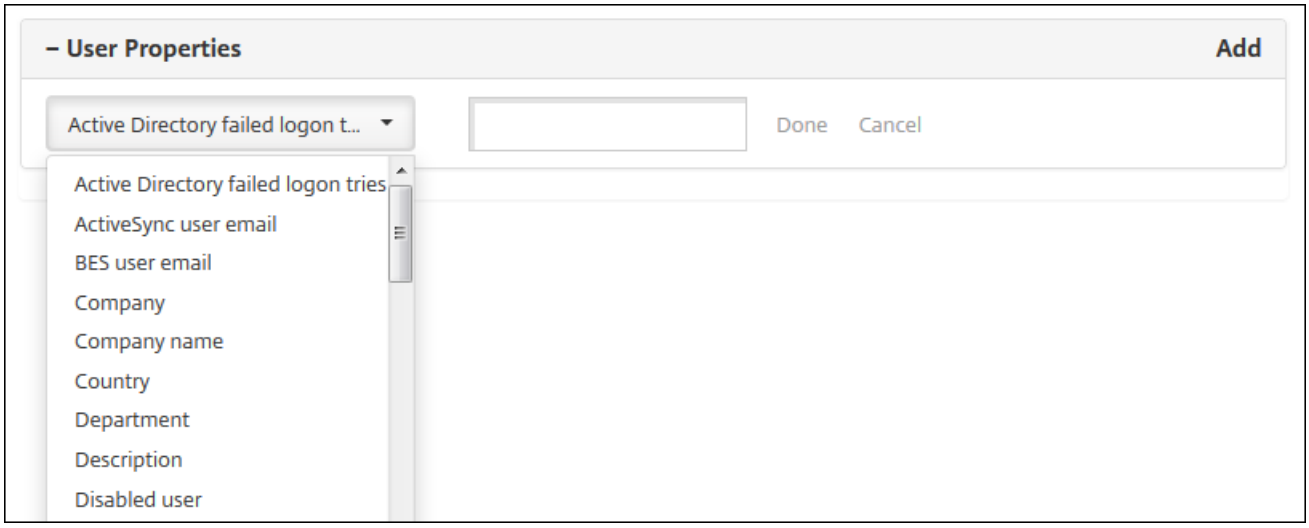
2. 配置以下设置：

- **用户名**：键入用户的名称。 此字段为必填字段。 可以在名称中包含空格，也可以包含大写和小写字母。
- **密码**：键入可选用户密码。
- **角色**：在列表中，单击用户的角色。 有关角色的详细信息，请参阅使用 RBAC 配置角色和 RBAC 角色和权限。 可用选项包括：
  - ADMIN
  - DEVICE_PROVISIONING、
  - SUPPORT
  - USER
- **成员身份**：在列表中，单击要添加此用户的一个或多个组。
- **用户属性**：添加可选用户属性。 对于您要添加的各个用户属性，单击**添加**，然后执行以下操作：
  - **用户属性**：在列表中，单击某个属性，然后在此属性旁边的字段中键入用户属性。
  - 单击**完成**保存用户属性或单击**取消**不保存用户属性。

    注意：要删除现有用户属性，请将鼠标悬停在包含此属性的行上方，然后单击右侧的 X。 属性立即被删除。

    要编辑现有用户属性，请单击属性并进行更改。 单击**保存**以保存更改后的列表，或单击**取消**保持列表不发生更改。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

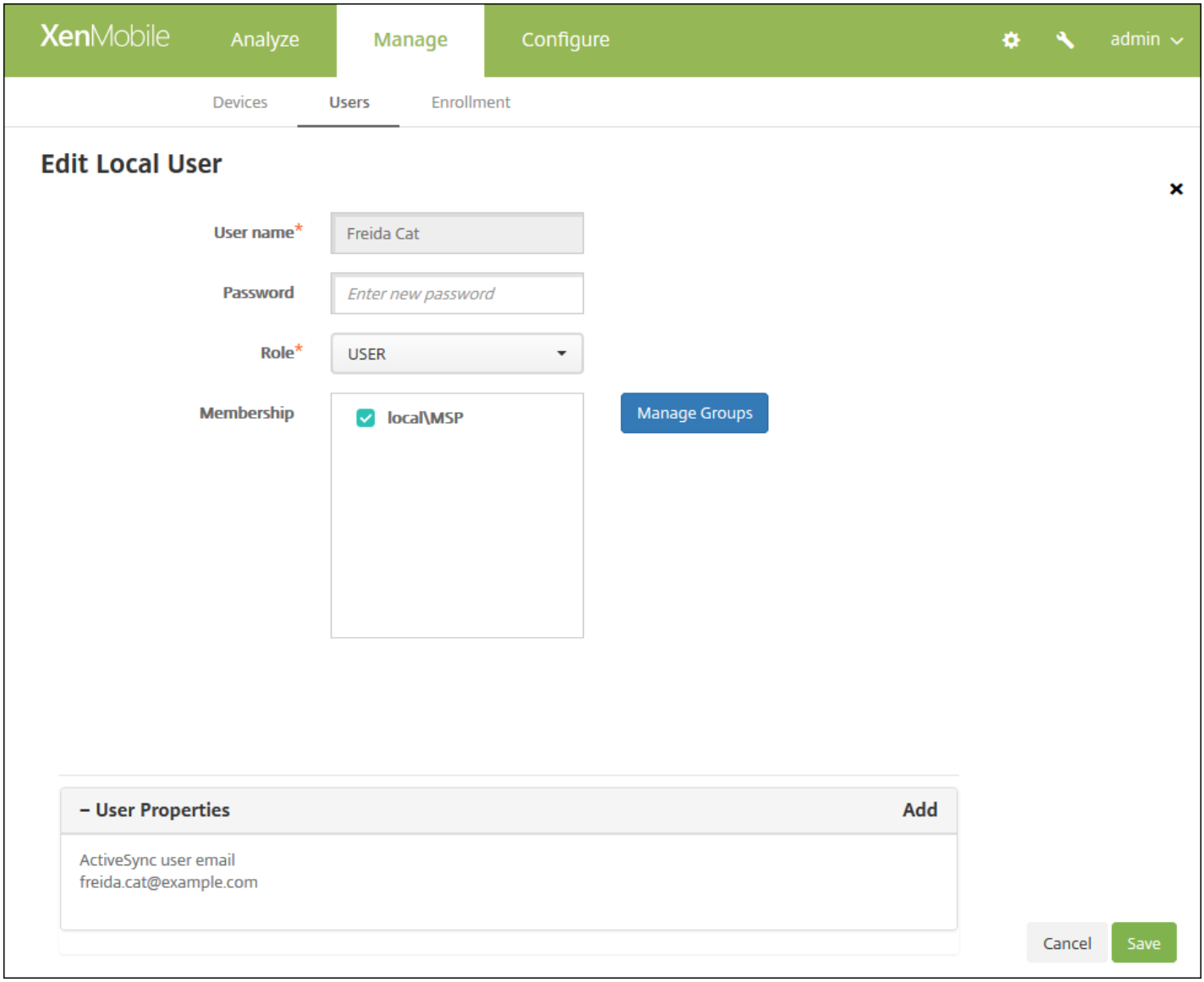


3. 单击**保存**。

编辑本地用户

1. 在**用户**页面上的用户列表中，单击以选中某个用户，然后单击**编辑**。 此时将显示**编辑本地用户**页面。 有关选择表格中的项目的详细信息，请参阅 XenMobile 控制台中的过滤器和表格。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 适当更改以下信息：

- **用户名**：无法更改用户名。
- **密码**：更改或添加用户密码。
- **角色**：在列表中，单击用户的角色。
- **成员身份**：在列表中，单击要添加此用户的一个或多个组。 要从组删除用户，请取消选中组名称旁边的复选框。
- **用户属性**：请执行以下操作之一：
  - 对于您要更改的各个用户属性，请单击属性并进行更改。 单击**保存**以保存更改后的列表，或单击**取消**保持列表不发生更改。
  - 对于您要添加的各个用户属性，单击**添加**，然后执行以下操作：
    - **用户属性**：在列表中，单击某个属性，然后在此属性旁边的字段中键入用户属性。
    - 单击**完成**保存用户属性或单击**取消**不保存用户属性。
  - 对于要删除的各个现有用户属性，请将鼠标悬停在包含此属性的行上方，然后单击右侧的 X。 属性立即被删除。

3. 单击**保存**以保存您的更改，或单击**取消**保持用户不发生更改。

删除本地用户

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 在**用户**页面上的用户列表中，单击以选中某个用户。

   注意：可以通过选中每个属性旁边的复选框，选择要删除的多个用户。

2. 单击**删除**。 此时将显示确认对话框。

3. 单击**删除**以删除用户，或者单击**取消**不删除用户。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

导入用户帐户

Oct 21, 2016

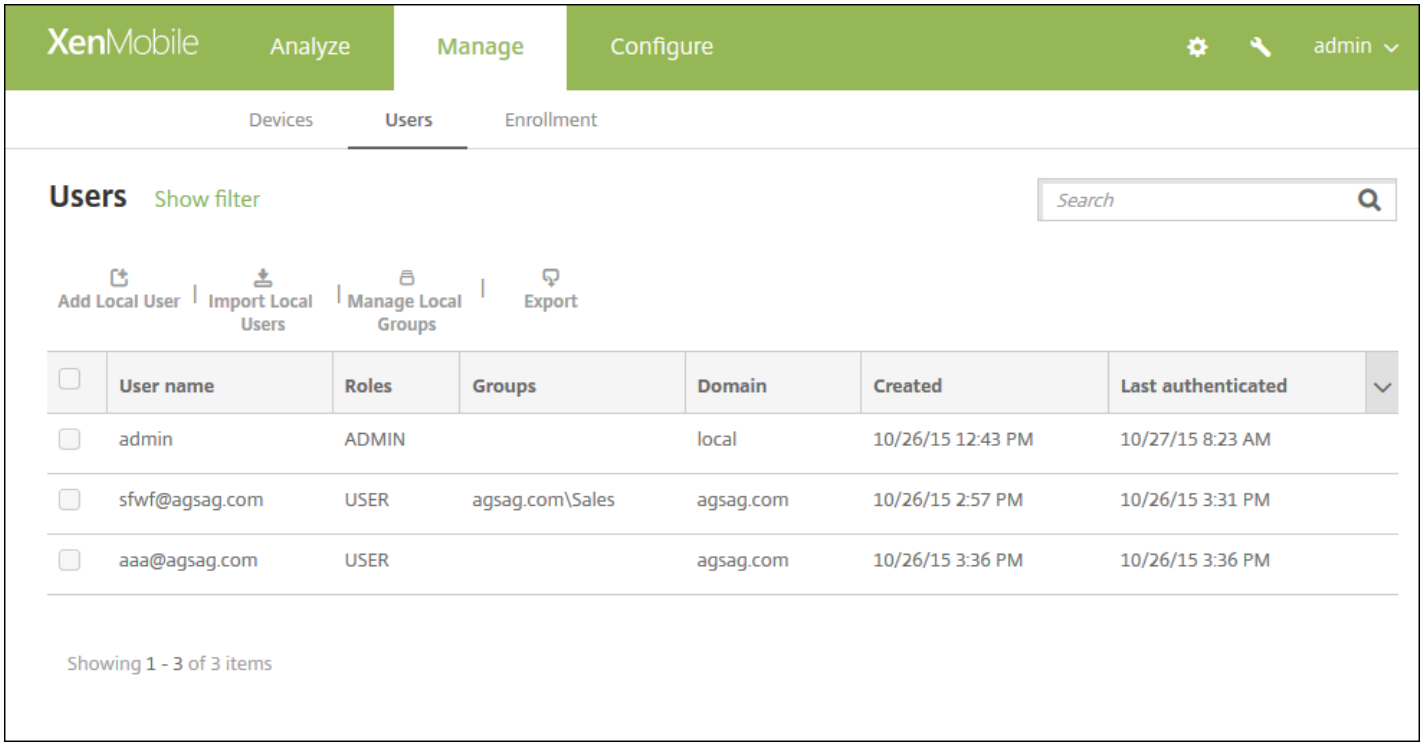
您可以从称为置备文件的 .csv 文件导入用户帐户和属性，该文件可以手动创建。 有关置备文件格式的信息，请参阅置备文件的格式。

注意：

- 如果您从 LDAP 目录导入用户，应将域名与导入文件中的用户名结合使用。 例如，指定 username@domain.com。 此语法可阻止进行会降低导入速度的其他查找。
- 如果将用户导入到 XenMobile 内部用户目录，请禁用默认域以加快导入过程。 您可以在内部用户导入完成后重新启用默认域。
- 本地用户可以采用用户主体名称 (UPN) 格式，但是，Citrix 建议不要使用托管域；例如，如果 example.com 是托管域，请勿使用以下 UPN 格式创建本地用户：user@example.com。

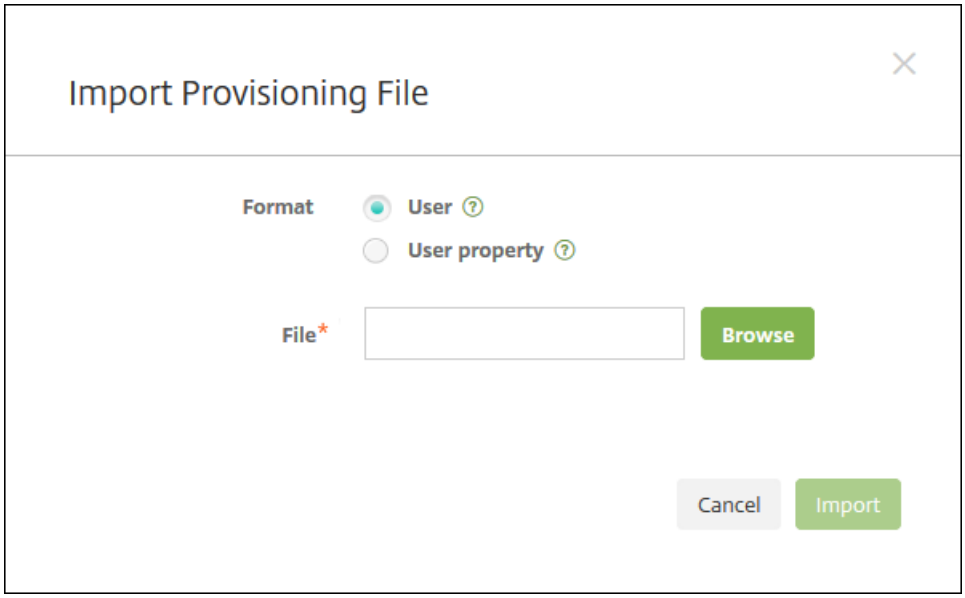
准备好置备文件后，请按照以下步骤将此文件导入到 XenMobile 中。

1. 在 XenMobile 控制台中，单击**管理 > 用户**。 此时将显示**用户**页面。



2. 单击**导入本地用户**。 此时将显示**导入置备文件**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 对于要导入的置备文件的格式，请选择**用户**或**属性**。

4. 通过单击**浏览**并导航到要使用的置备文件的位置，选择此文件。

5. 单击**导入**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

置备文件的格式

Aug 15, 2016

手动创建且用于将用户帐户和属性导入到 XenMobile 中的置备文件必须采用以下格式之一：

- 用户置备文件字段：user;passowrd;role;group1;group2
- 用户属性置备文件字段：user;propertyName1;propertyValue1;propertyName2;propertyValue2

注意：

- 置备文件中的字段使用分号 (;) 隔开。 如果某个字段的某一部分包含分号，则必须使用反斜杠字符 (\) 进行转义。 例如，在置备文件中，属性 propertyV;test;1;2 应按 propertyV\;test\;1\;2 格式键入。
- Role 的有效值为预定义的角色 USER、ADMIN、SUPPORT 和 DEVICE_PROVISIONING 以及您定义的其他角色。
- 句点字符 (.) 用作创建组层次结构的分隔符；因此，不能在组名称中使用句点。
- 属性置备文件中的属性必须小写。 数据库区分大小写。

用户置备内容示例

user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01 条目表示：

- 用户：user01
- 密码：pwd;01
- 角色：USER
- 组：
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

另一个示例 AUser0;1.password;USER;ActiveDirectory.test.net 表示：

- 用户：AUser0
- 密码：1.password
- 角色：USER
- 组：ActiveDirectory.test.net

用户属性置备内容示例

user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value 条目表示：

- 用户：user01
- 属性 1
  - 名称：propertyN
  - 值：propertyV;test;1;2
- 属性 2：
  - 名称：prop 2
  - 值：prop2 value

© 1999-2017 Citrix Systems, Inc. All rights reserved.

添加或删除组

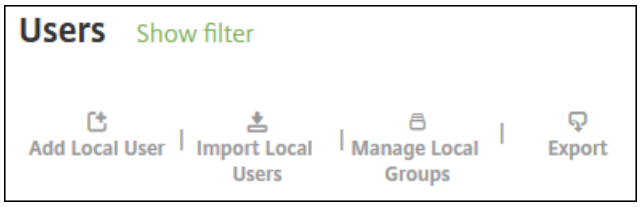
Aug 11, 2016

在 XenMobile 控制台的管理组对话框中管理组，您可以在**用户**页面、**添加本地用户**页面或**编辑本地用户**页面上找到此对话框。 没用组编辑命令。 如果删除组，请注意删除组不影响用户帐户。 删除组只会删除用户与此组的关联。 用户还会丧失此组关联的交付组提供的应用程序或配置文件的访问权限，但是其他组关联性不受影响。 如果用户不与任何其他本地组关联，它们将在顶层关联。

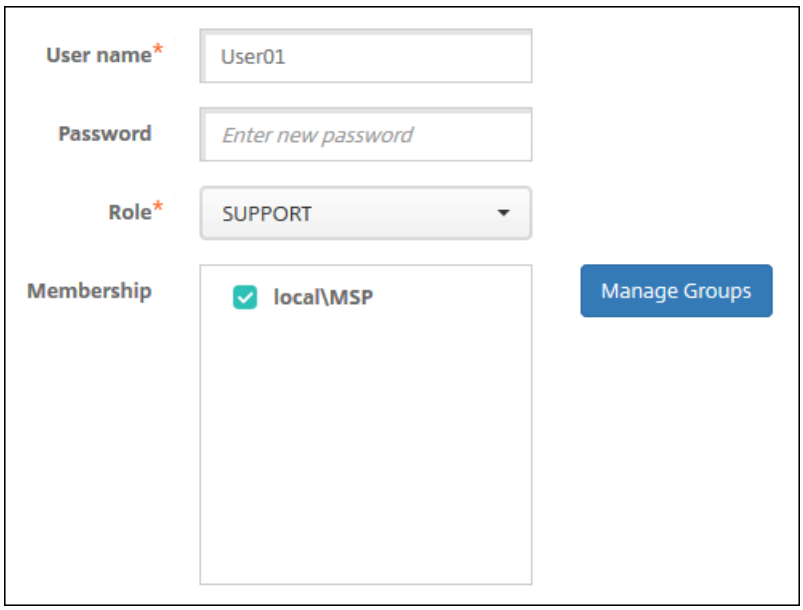
添加本地组

1. 执行以下操作之一：

- 在**用户**页面上，单击**管理本地组**。

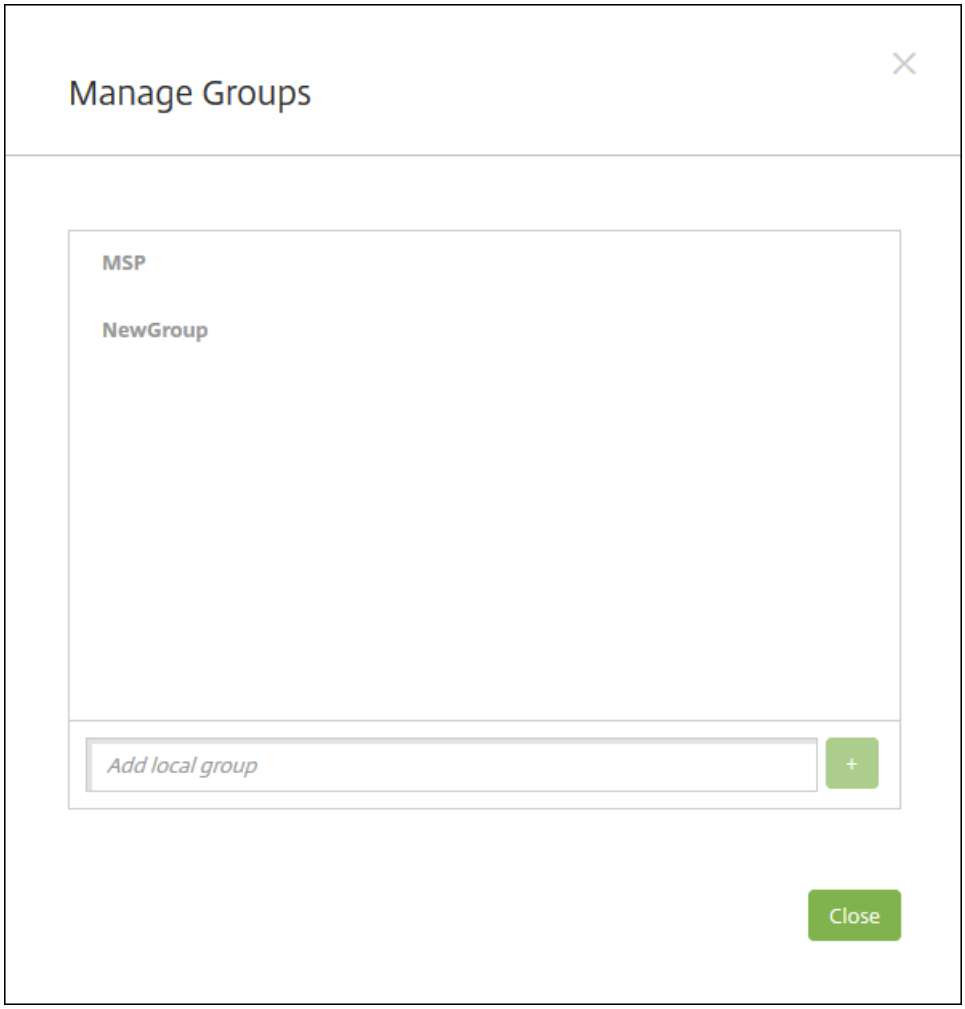


- 在**添加本地用户**页面或**编辑本地用户**页面上，单击**管理组**。



此时将显示**管理组**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 在组列表下方，键入组名称，然后单击加号 (+)。 用户组已添加到列表中。

3. 单击**关闭**。

删除组

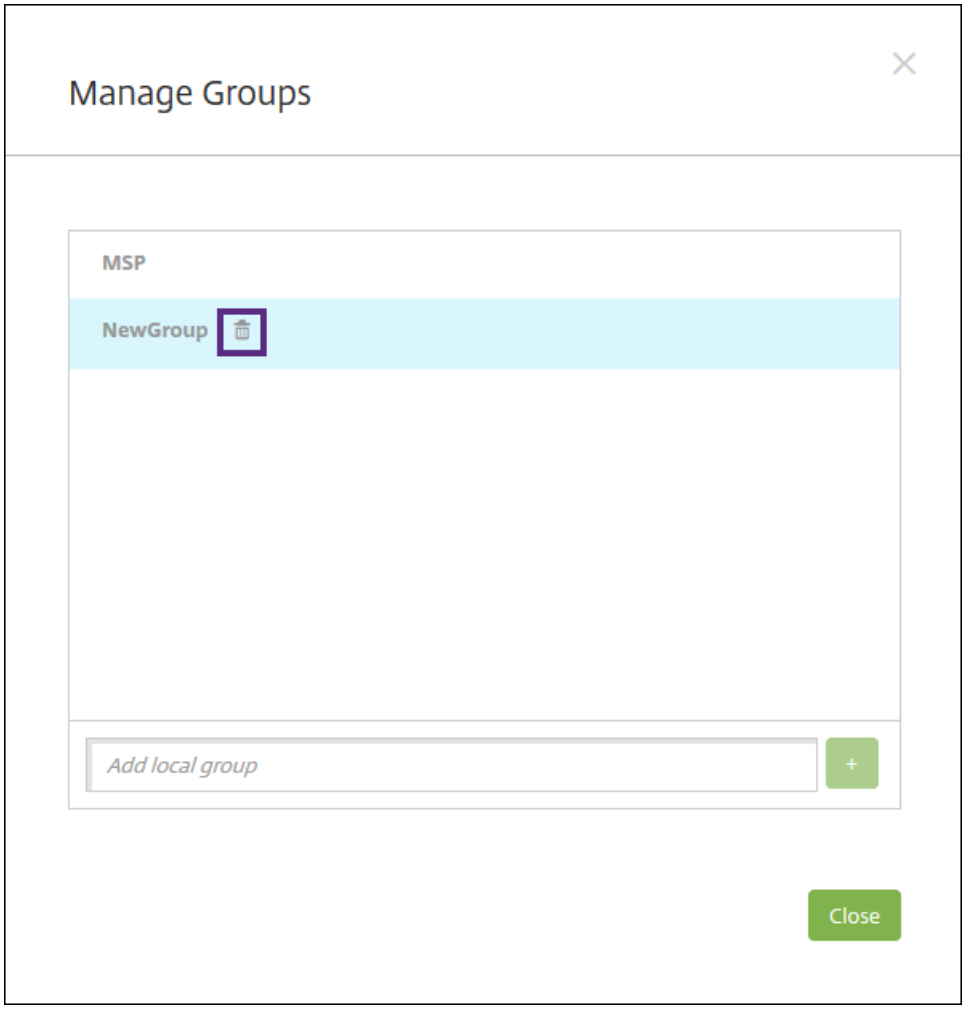
注意：删除组不会影响用户帐户。 删除组只会删除用户与此组的关联。 用户还会丧失此组关联的交付组提供的应用程序或配置文件的访问权限，但是其他组关联性不受影响。 如果用户不与任何其他本地组关联，它们将在顶层关联。

1. 执行以下操作之一：

- 在用户页面上，单击**管理本地组**。
- 在**添加本地用户**页面或**编辑本地用户**页面上，单击**管理组**。

此时将显示**管理组**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 在**管理组**对话框上，单击要删除的组。

3. 单击组名称右侧的垃圾箱图标。 此时将显示确认对话框。

4. 单击**删除**以确认操作并删除该组。

   重要：此操作无法撤消。

5. 在**管理组**对话框上，单击**关闭**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用 RBAC 配置角色

Oct 21, 2016

通过 XenMobile 中基于角色的访问控制 (RBAC) 功能，可以向用户和组分配预定义的角色（或称权限集）。 这些权限控制用户对系统功能的访问级别。

XenMobile 实现四种默认用户角色，用于在逻辑上区分系统功能的访问权限：

- **管理员**。 授予完整系统访问权限。
- **设备置备**： 授权访问针对 Windows CE 设备的基本设备管理。
- **支持**。 授予对远程支持的访问权限。
- **用户**。 供可以注册设备和访问自助服务门户的用户使用。

您可以使用默认角色作为模板，通过自定义来创建具有默认角色定义的功能之外的其他特定系统功能的访问权限的新用户角色。

角色可以分配给本地用户（在用户级别）或 Active Directory 组（此组中的所有用户具有相同的权限）。 如果用户属于多个 Active Directory 组，则所有权限合并起来，以定义该用户的权限。 例如，如果 ADGroupA 可以查找管理员设备，ADGroupB 用户可以擦除员工设备，则同时属于这两个组的用户可以查找和擦除管理员和员工的设备。

注意：本地用户可以仅分配有一个角色。

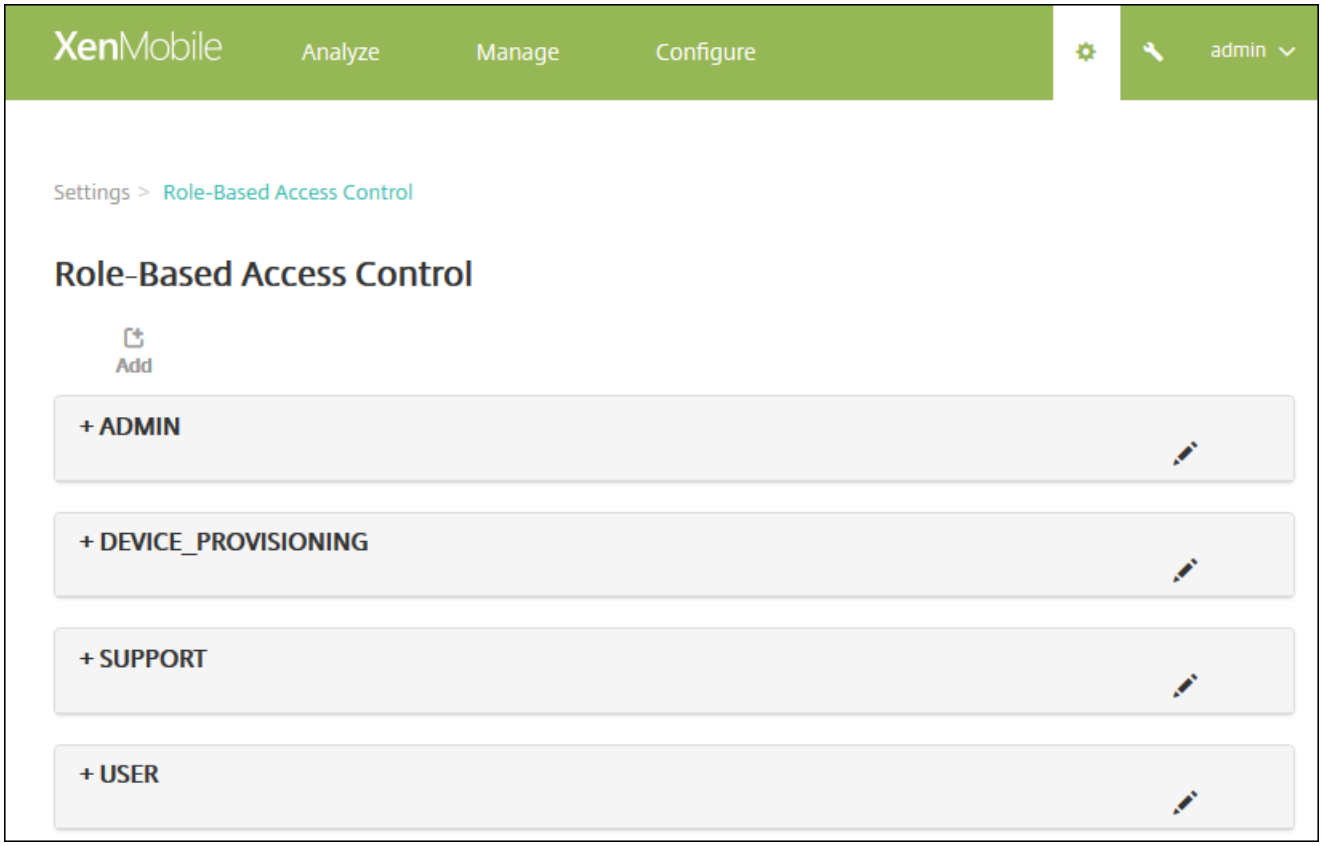
可以使用 XenMobile 中的 RBAC 功能执行以下操作：

- 创建新角色。
- 将组添加到角色。
- 向本地用户分配角色。

1. 在 XenMobile 控制台中，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**基于角色的访问控制**。 此时将出现**基于角色的访问控制**页面，其中显示了四种默认用户角色以及您之前添加的任何角色。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



如果单击某个角色旁边的加号 (+)，角色将展开以显示此角色的所有权限，如下图所示。

3. 单击**添加**可添加新用户角色，单击现有角色右侧的铅笔图标可以编辑此角色，单击您之前所定义角色右侧的垃圾桶图标可以删除此角色。 无法删除默认用户角色。

- 单击**添加**或铅笔图标时，将显示**添加角色**或**编辑角色**页面。
- 单击垃圾桶图标时，将显示一个确认对话框。 单击**删除**将删除选定角色。

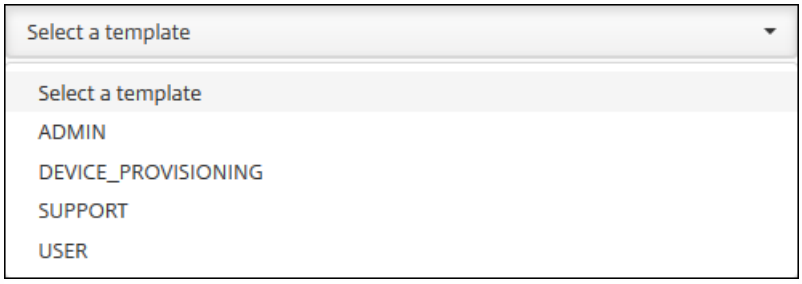
4. 要创建新用户角色或编辑现有用户角色，请输入以下信息：

- **RBAC 名称**：输入新用户角色的描述性名称。 无法更改现有角色的名称。
- **RBAC 模板**：可选，单击某个模板以将其作为新角色的起点。 如果正在编辑现有角色，则无法选择模板。

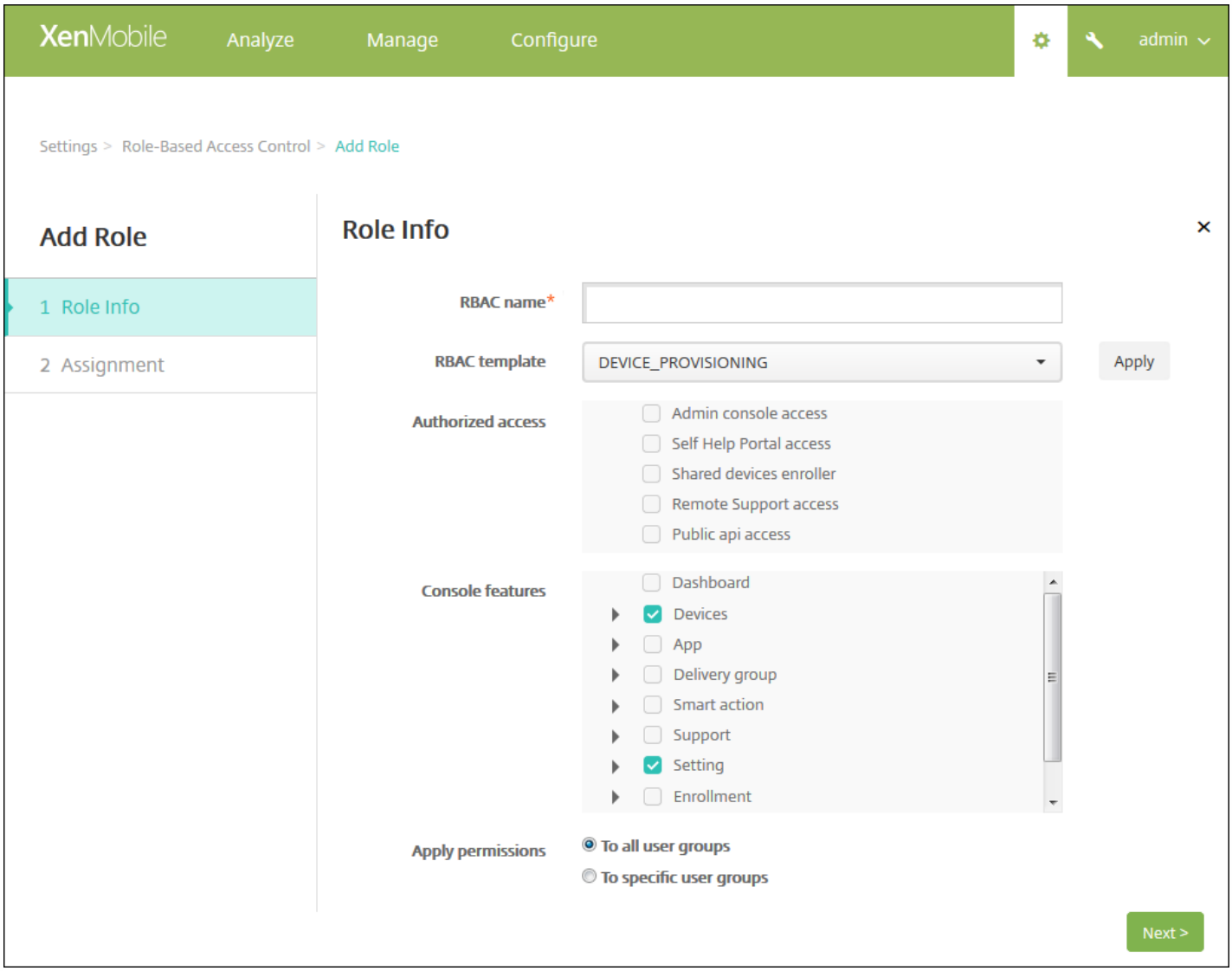
RBAC 模板是默认用户角色。 它们定义与此角色关联的用户对系统功能的访问权限。 选择某个 RBAC 模板后，可以在**授**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

权访问和**控制台功能**字段看到此角色关联的所有权限。 使用模板为可选操作；您也可以直接在**授权访问**和**控制台功能**字段选择要分配给角色的选项。



5. 单击 **RBAC 模板**字段右侧的**应用**以使用选定模板的预定义访问权限和功能权限填充**授权访问**和**控制台功能**复选框。

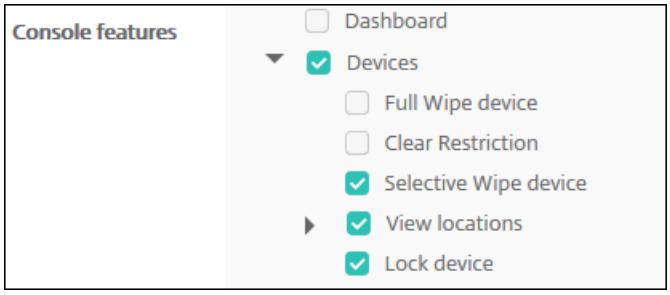


6. 选中或取消选中**授权访问**和**控制台功能**复选框可自定义角色。

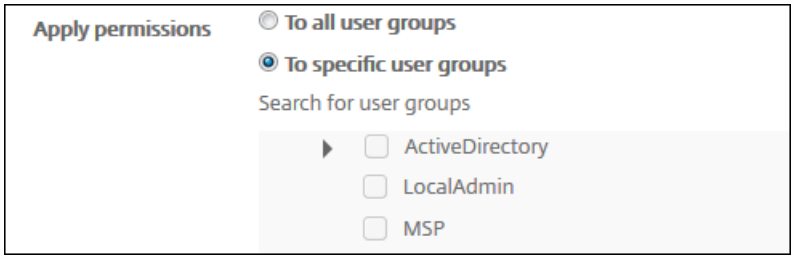
如果单击某项控制台功能旁边的三角形，将显示特定于此功能的权限，您可以选中或取消选中相应的权限。 单击顶层的复选框可以阻止访问此控制台部分；您必须选择顶层下面的单独选项，才能启用这些选项。 例如，在下图中，对于分配给此角色的用

© 1999-2017 Citrix Systems, Inc. All rights reserved.

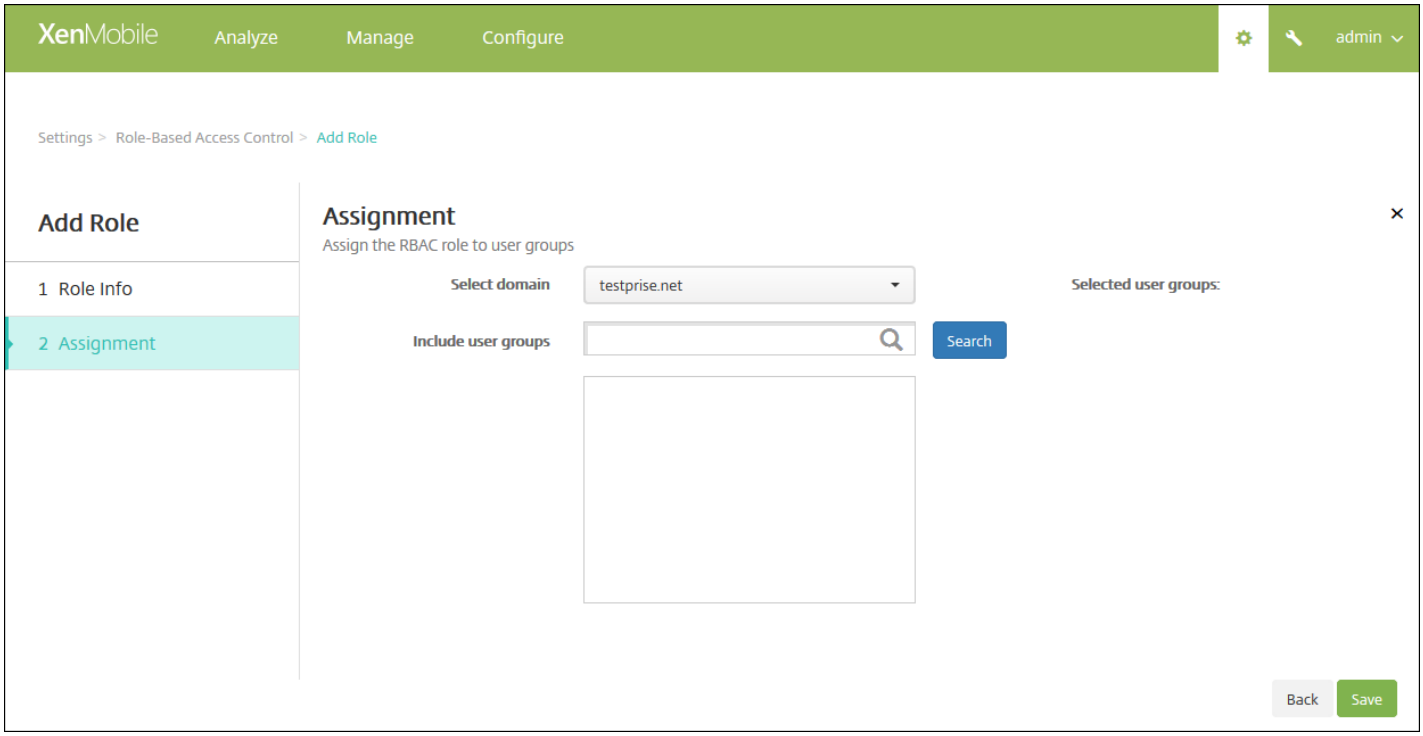
户，**完全擦除设备**和**清除限制**选项不会显示在控制台上，但选中的选项会显示。



7. **应用权限**：选择要向其应用选定权限的组。 如果单击**至特定用户组**，将显示组的列表，您可以从中选择一个或多个组。



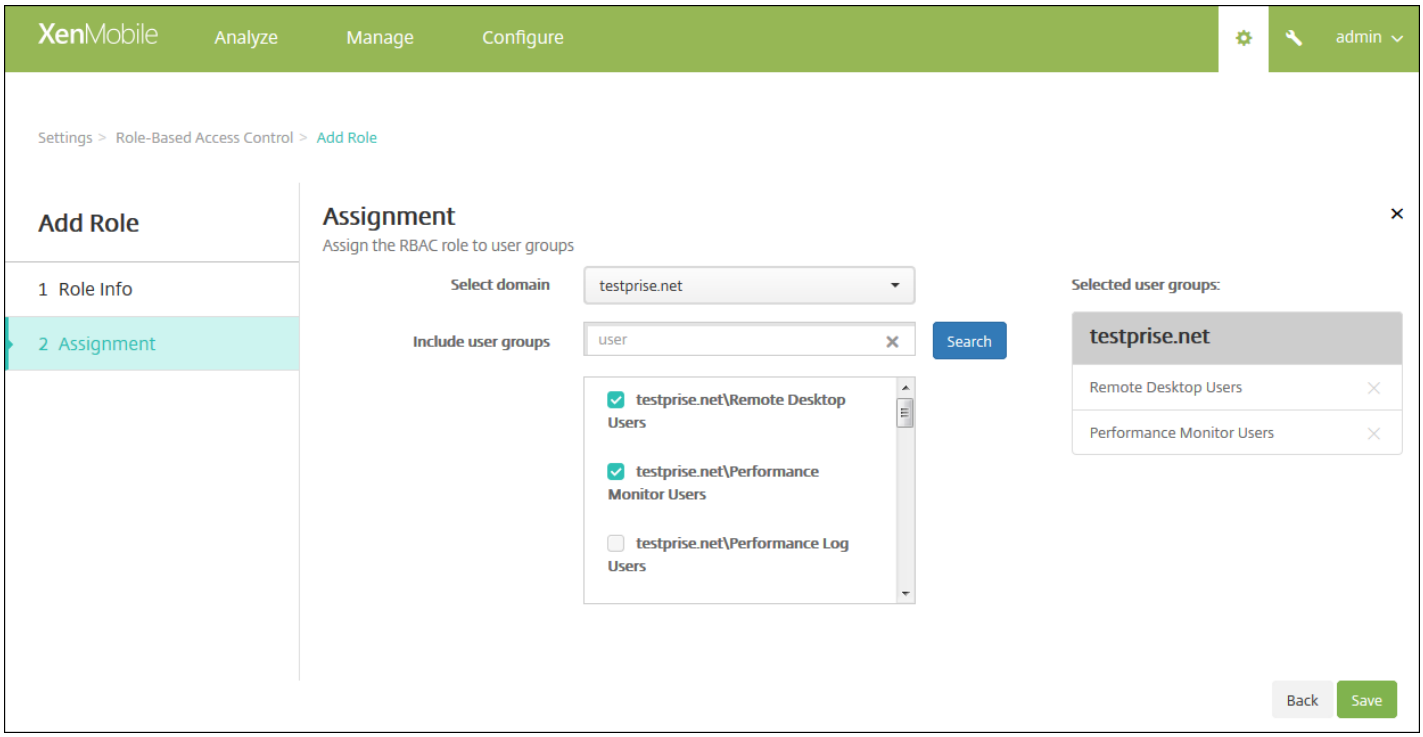
8. 单击 **Next**（下一步）。 此时将显示**分配**页面。



9. 输入下列信息，以将角色分配给用户组。

- **选择域**：在列表中，单击某个域。
- **包括用户组**：单击**搜索**以查看所有可用组的列表，或键入完整或部分组名称以将列表限制为仅显示具有此名称的组。
- 在显示的列表中，选择要向其分配角色的用户组。 选择某个用户组后，此组将显示在**选定用户组**列表中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



注意：要从**选定用户组**列表删除用户组，请单击用户组名称旁边的 X。

10. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

RBAC 角色和权限

Aug 15, 2016

每个预定义的基于角色的访问控制 (RBAC) 角色具有某些与该角色关联的访问权限和功能权限。 本文描述其中的每个权限可以执行的操作。 要获取每个内置角色的默认权限的完整列表，请下载基于角色的访问控制默认设置。

有关如何配置 RBAC 角色的详细信息，请参阅使用 RBAC 配置角色。

- 管理角色
- 设备置备角色
- 支持角色
- 用户角色

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置注册模式并启用自助服务门户

Aug 11, 2016

配置设备注册模式以允许用户在其 XenMobile 中注册其设备。 XenMobile 提供七种模式，每种均具有自己的安全级别和用户注册其设备必须执行的步骤。 您可以在自助服务门户中提供某些模式，用户可以在此处登录并生成注册链接，并通过这些链接注册其设备，也可以选择向他们发送注册邀请。

在 XenMobile 控制台的**设置 > 注册**页面配置注册模式。 在 XenMobile 控制台中从**管理 > 注册**页面发送注册邀请（请参阅在 XenMobile 中注册用户和设备）。

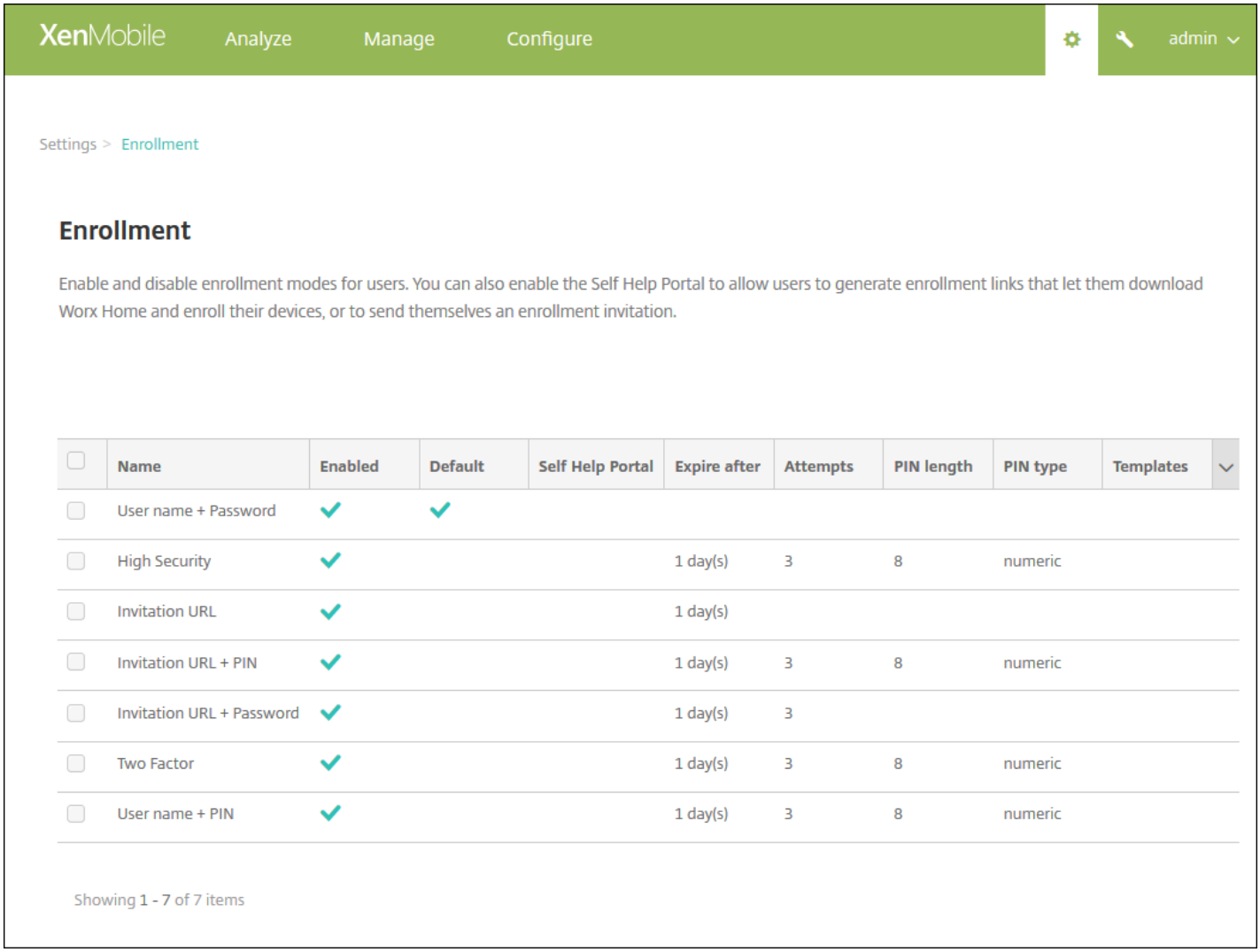
注意：如果您打算使用自定义通知模板，必须在配置注册模式之前设置模板。 有关通知模板的详细信息，请参阅创建或更新通知模板。

1. 在 XenMobile 控制台上，单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

2. 单击**注册**。 此时将显示**注册**页面，其中包含所有可用注册模式的表格。 默认情况下，启用所有注册模式。

在列表中选择任一注册模式进行编辑，然后将此模式设置为默认模式、删除此模式或允许用户通过自助服务门户访问。

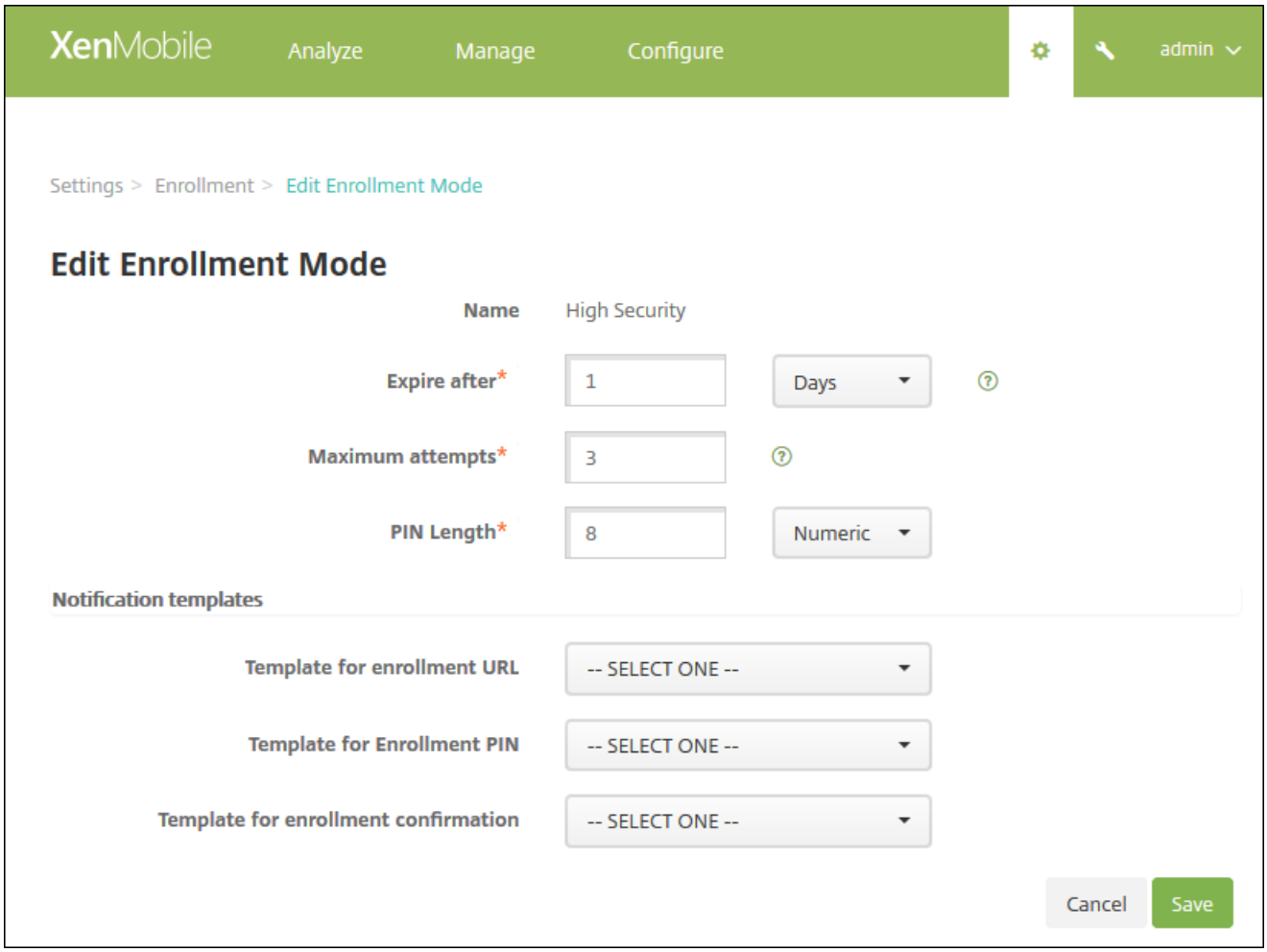
注意：如果选中某个注册模式旁边的复选框，选项菜单将显示在注册模式列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

编辑注册模式

1. 在**注册**列表中，选择注册模式，然后单击编辑。 此时将显示**编辑注册模式**页面。 根据所选择的模式，您会看到不同的选项。



2. 适当更改以下信息：

- **此时间后 过期**： 键入过期期限，此时间后用户将无法注册其设备。 此值显示在用户和组注册邀请配置页面。
  注意：键入 0 可防止邀请过期。

- **天**：在列表中，单击**天**或**小时**，对应于您在**此时间后过期**中输入的过期期限。
- **最大尝试次数**：键入用户可以尝试注册的次数，超出此次数后用户将被锁定，无法开始注册过程。 此值显示在用户和组注册邀请配置页面。
  注意：键入 0 表示尝试次数不受限制。

- **PIN 长度**：键入一个数字，表示生成的 PIN 将包含的数字/字符数。
- **数字**：在列表中，单击**数字**或**字母数字**以选择 PIN 类型。
- **通知模板**：
  - **注册 URL 模板**：在列表中，单击用于注册 URL 的模板。 例如，根据您配置模板的方式，注册邀请模板将向用户发送一封电子邮件或 SMS，使用户在 XenMobile 中注册其设备。 有关通知模板的详细信息，请参阅创建或更新通知模板。
  - **注册 PIN 模板**：在列表中，单击用于注册 PIN 的模板。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **注册确认模板**：在列表中，单击用于通知用户注册已成功的模板。

3. 单击**保存**。

将注册模式设为默认模式

将注册模式设为默认模式后，若不选择其他注册模式，此模式将用于所有设备注册请求。 如果未将任何注册模式设为默认模式，必须为每个设备注册创建注册请求。

注意：只能将**用户名 + 密码**、**双因素**或**用户名 + PIN** 设为默认注册模式。
1. 从**用户名 + 密码**、**双因素**或**用户名 + PIN** 中选择一项，设置 为 默认注册模式

注意：选择的模式必须启用后才能设为默认模式。
2. 单击**默认**。 所选模式现已成为默认模式。 如果将任何其他注册模式设为默认模式，此模式将不再作为默认模式。

禁用注册模式

禁用注册模式将使此模式不可供用户使用，既不可用于组注册邀请，也不可在自助服务门户中提供。 通过禁用某种注册模式并启用另一种注册模式，可以更改允许用户注册其设备的方式。

1. 选择注册模式。

注意：无法禁用默认注册模式。 如果要禁用默认注册模式，必须首先删除其默认状态。
2. 单击**禁用**。 注册模式不再处于启用状态。

在自助服务门户上启用注册模式

通过在自助服务门户上启用注册模式，可允许用户单独在 XenMobile 中注册其设备。

注意：

- 注册模式必须启用并绑定通知模板，才能在自助服务门户上提供。
- 同一时间只能在自助服务门户上启用一种注册模式。

1. 选择注册模式。

2. 单击**自助服务门户**。 此注册模式现已在自助服务门户上提供，可供用户使用。 已经在自助服务门户上启用的任何模式均不再可供用户使用。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中为用户注册启用自动发现

Aug 11, 2016

自动发现可简化用户的注册流程。 用户可以使用他们的网络用户名和 Active Directory 密码注册其设备，无需再输入 XenMobile 服务器的详细信息。 用户以用户主体名称 (UPN) 格式输入其用户名，例如，user@mycompany.com。

要启用自动发现，可以访问自动发现服务门户（网址为 https://xenmobiletools.citrix.com）。有关自动发现服务门户的更多信息，请参阅 XenMobile 自动发现服务上的主题。

在有限的几种情况下，您可能需要联系 Citrix 技术支持以启用自动发现。 为此，可以按照下面的步骤，将部署信息告知 Citrix 技术支持团队，如果使用 Windows 设备，则应将 SSL 证书告知 Citrix 技术支持团队。 Citrix 收到此信息后，会在用户注册其设备时，提取域信息并将其映射到服务器地址。 此信息保留在 XenMobile 数据库中，以便用户注册时随时访问和获取。

1. 如果无法使用自动发现服务门户（网址为 https://xenmobiletools.citrix.com）启用自动发现，请使用 Citrix 支持门户打开一个技术支持案例，然后提供以下信息：

- 包含用户注册所用帐户的域。
- XenMobile 服务器完全限定的域名 (FQDN)。
- XenMobile 实例名称。 默认情况下，实例名称为 zdm，并且区分大小写。
- 用户 ID 类型，可以是 UPN 或电子邮件。 默认情况下，类型为 UPN。
- 用于 iOS 注册的端口（如果更改了默认端口号 8443）。
- XenMobile 服务器通过其接受连接的端口（如果更改了默认端口号 443）。
- （可选）XenMobile 管理员的电子邮件地址。

2. 如果计划注册 Windows 设备，请执行以下操作：

- 请获取 enterpriseenrollment.mycompany.com 的公共签名非通配符 SSL 证书，其中 mycompany.com 为包含用户注册时要使用的帐户的域。 请在您的请求中附上 .pfx 格式的 SSL 证书及其密码。
- 在您的 DNS 中创建一条规范名称 (CNAME) 记录，并将 SSL 证书的地址 (enterpriseenrollment.mycompany.com) 映射到 autodisc.zc.zenprise.com。 Windows 设备用户使用 UPN 注册时，除了提供 XenMobile 服务器的详细信息外，Citrix 注册服务器还指导设备从 XenMobile 服务器申请有效证书。

当您的详细信息和证书（如适用）添加到 Citrix 服务器时，您的技术支持案例将更新。 此时，用户可使用自动发现开始注册。

注意：如果要使用多个域进行注册，还可以使用多域证书。 多域证书应具有以下结构：

- SubjectDN，包含用于指定所服务的主域的 CN（例如 enterpriseenrollment.mycompany1.com）。
- 适用于其余域的恰当 SAN（例如 enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.com 等）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建和更新通知模板

Aug 11, 2016

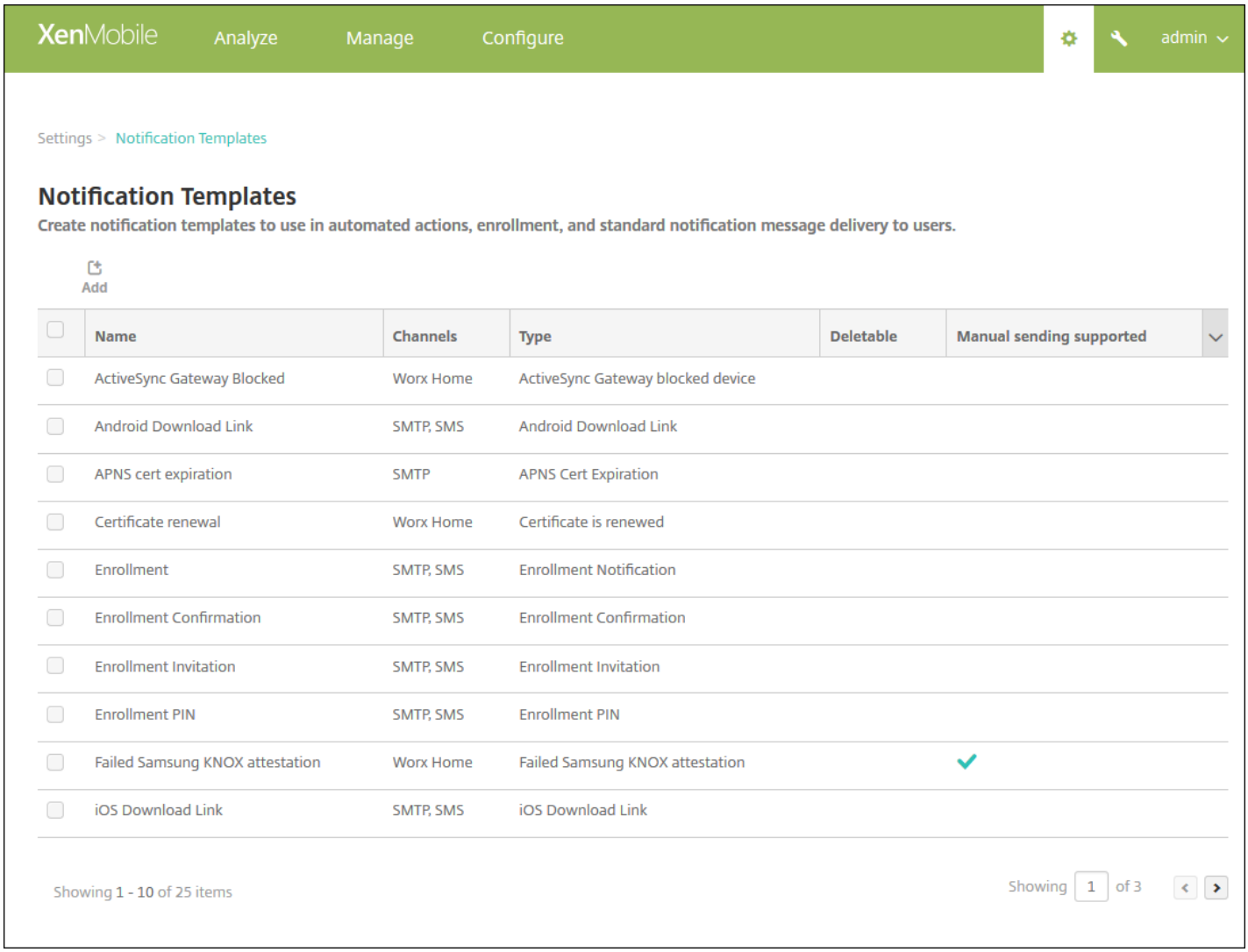
可以在 XenMobile 中创建或更新用于自动化操作、注册和发送给用户的标准通知消息的通知模板。 配置通知模板以通过三种不同的通道发送消息：Worx Home、SMTP 或 SMS。

XenMobile 包含很多反应不同事件类型的预定义通知模板，XenMobile 会自动针对这些事件类型向系统中的每台设备发出响应。

注意：如果计划使用 SMTP 或 SMS 通道向用户发送通知，必须设置通道后才能将其激活。 如果尚未设置通道，当添加通知模板时，XenMobile 会提示您设置通道。 有关详细信息，请参阅 XenMobile 中的通知。

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。



添加通知模板

1. 单击**添加**。 如果尚未设置任何 SMS 网关或 SMTP 服务器，会显示一条关于使用 SMS 和 SMTP 通知的消息。 可以选择立即

© 1999-2017 Citrix Systems, Inc. All rights reserved.

或稍后设置 SMTP 服务器或 SMS 网关。 此时将显示**添加通知模板**页面。

如果选择立即设置 SMS 或 SMTP 服务器设置，将重定向到**设置**页面上的**通知服务器**页面。 设置完要使用的通道后，可以返回到**通知模板**页面，继续添加或修改通知模板。

> **Important**
>
> 如果选择稍后设置 SMS 或 SMTP 服务器设置，将无法在添加或编辑通知模板时激活这些通道，这意味着这些通道将不能用于发送用户通知。

2. 配置以下设置：

- **名称**：键入模板的描述性名称。
- **说明**：键入模板的说明。
- **类型**：在列表中，单击通知类型。 仅显示选定类型支持的通道。 仅允许一个 APNS 证书过期模板，此为预定义模板。 这表示您无法添加此类型的新模板。

注意：对于某些模板类型，类型的下面会显示短语*支持手动发送*。 这表示此模板会显示在**控制板**和**设备**页面上的**通知**列表中，允许您手动向用户发送模板。 在“主题”或“消息”字段中使用以下宏的任何模板在任何通道上均不可以使用手动发送。

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

3. 在**通道**下面，配置用于此通知的各个通道的信息。 可以选择任何通道或所有通道。 您选择的通道取决于您希望发送通知的方式。

- 如果选择 **Worx Home**，则仅 iOS 和 Android 设备接收通知，通知将显示在设备的通知托盘中。
- 如果选择 **SMTP**，大多数用户应该都可以接收消息，因为他们已使用其电子邮件地址注册。
- 如果选择 **SMS**，则仅使用的设备带有 SIM 卡的用户接收通知。

Worx Home：

- **激活**：单击以启用通知通道。
- **消息**：键入要发送给用户的消息。 如果使用的是 Worx Home，此字段为必填字段。
- **声音文件**：在列表中，单击用户收到通知时听到的通知声音。

SMTP：

- **激活**：单击以启用通知通道。

  重要：如果已设置 SMTP 服务器，则仅可以激活 SMTP 通知。

- **发件人**：键入通知的可选发件人，可以是名称、电子邮件地址或同时包含二者。
- **收件人**：此字段包含除临时通知以外的所有通知的预置宏，以确保将通知发送给正确的 SMTP 收件人地址。 Citrix 建议您不要修改模板中的宏。 除了用户，您还可以通过添加以分号 (;) 分隔的收件人地址，添加其他收件人（如企业管理员）。 要发送临时通知，可以在此页面上输入特定收件人，或从**管理** > **设备**页面选择设备并从此处发送通知。 有关详细信息，请参阅在 XenMobile 中添加设备和查看设备详细信息。
- **主题**：键入通知的描述性主题。 此字段为必填字段。
- **消息**：键入要发送给用户的消息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SMS：

- **激活**：单击以启用通知通道。

  重要：如果已设置 SMS 网关，则仅可以激活 SMS 通知。
- **收件人**：此字段包含除临时通知以外的所有通知的预置宏，以确保将通知发送给正确的 SMS 收件人地址。 Citrix 建议您不要修改模板中的宏。 要发送临时通知，可以输入特定收件人，或从**管理** > **设备**页面选择设备。
- **消息**：键入要发送给用户的消息。 此字段为必填字段。

5. 单击**添加**。 正确配置所有通道后，通道将按照以下顺序显示在**通知模板**页面：SMTP、SMS 和 Worx Home。 未正确配置的通道将在经过正确配置后显示。

编辑通知模板

1. 选择通知模板。 此时将显示特定于此模板的编辑页面，您可以在此页面更改除**类型**字段之外的所有内容，以及激活或取消激活通道。

2. 单击**保存**。

删除通知模板

注意：您只能删除自己添加的通知模板；不能删除预定义通知模板。

1. 选择现有通知模板。

2. 单击**删除**。 此时将显示确认对话框。

2. 单击**删除**以删除通知模板，或者单击**取消**以取消删除通知模板。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

管理交付组

Aug 11, 2016

在设备配置和管理过程中，通常需在 XenMobile 控制台中创建资源（策略和应用程序）和操作，然后使用交付组对它们进行打包。 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；如何更改交付组中的资源和操作的部署顺序；XenMobile 如何确定部署顺序（当用户处于具有重复策略或矛盾策略的多个交付组中时）。

交付组指定您向其设备部署策略、应用程序和操作组合的用户类别。 交付组包含的内容通常根据用户的特征而定，如公司、国家/地区、部门、办公地址、职务等。 利用交付组可以很好地控制哪些人可以访问哪些资源以及访问时间。 可以针对每个人部署交付组，也可以针对严格定义的用户组部署交付组。

部署到交付组意味着向使用 iOS、Windows Phone 和 Windows Tablet 设备且属于此交付组的所有用户发送推送通知，使其重新连接到 XenMobile，以便您重新评估这些设备并部署应用程序、策略和操作；使用其他平台设备的用户如果已经连接，则可以立即接收资源，或者根据其计划策略，在下次连接时接收资源。

安装和配置 XenMobile 时会创建默认的 AllUsers 交付组。 它包含所有本地用户和 Active Directory 用户。 您无法删除 AllUsers 组，但是，如果您不希望向所有用户推送资源，可以禁用此组。

部署顺序

部署顺序是指 XenMobile 向设备推送资源的顺序。 仅 MDM 模式支持部署顺序。

在确定部署顺序时，XenMobile 将向策略、应用程序、操作和交付组应用过滤器和控制标准，例如部署规则和部署计划。 在添加交付组前，请考虑本节信息与您的部署目标的相关性。

下面是有关部署顺序的主要概念的汇总：

- **部署顺序**：XenMobile 向设备推送资源（策略和应用程序）和操作的顺序。 某些策略（如条款和条件以及软件清单）的部署顺序对其他资源没有影响。 操作的部署顺序对其他资源没有影响，因此，XenMobile 部署资源时会忽略操作的位置。
- **部署规则**：XenMobile 使用您为设备属性指定的部署规则来过滤策略、应用程序、操作和交付组。 例如，某个部署规则可能指定当域名与特定值匹配时推送部署包。
- **部署计划**：XenMobile 使用您为操作、应用程序和设备策略指定的部署计划来控制这些项目的部署。 可以将部署过程指定为立即执行、在特定日期和时间执行或根据部署条件执行。

下表显示了这些条件，以及可与特定对象或资源关联（以过滤它们或控制它们的部署）的其他条件。

对象/资源	**过滤器/控制条件**
设备策略	设备平台 部署规则（基于设备属性） 部署计划
	设备平台

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App	部署规则（基于设备属性） 部署计划
操作	部署规则（基于设备属性） 部署计划
交付组	用/户组 部署规则（基于设备属性）

在典型的环境中，很可能会将多个交付组分配给单个用户，这将产生以下可能结果：

- 交付组中存在重复的对象。
- 在分配给一个用户的多个交付组对某特定策略进行不同的配置。

当发生任一情况时，XenMobile 将为必须传递给设备或操作的所有对象计算部署顺序。 计算步骤独立于设备平台。

计算步骤：

1. 基于用户/组过滤器和部署规则确定特定用户的所有交付组。
2. 创建选定交付组中所有资源（策略、操作和应用程序）的有序列表，以基于设备平台、部署规则和部署计划的过滤器进行应用。 排序算法如下所述：

    a. 将交付组中具有用户定义的部署顺序的资源放置在不具有此类部署顺序的资源之前。 将在这些步骤后的内容中说明这样做的理由。

    b. 作为交付组之间的一个决定项，按交付组名称对交付组中的资源排序。 例如，将交付组 A 中的资源放置在交付组 B 之前。

    c. 在排序时，如果为交付组的资源指定了用户定义的部署顺序，将保持该顺序。 否则，按资源名称对交付组内的资源进行排序。

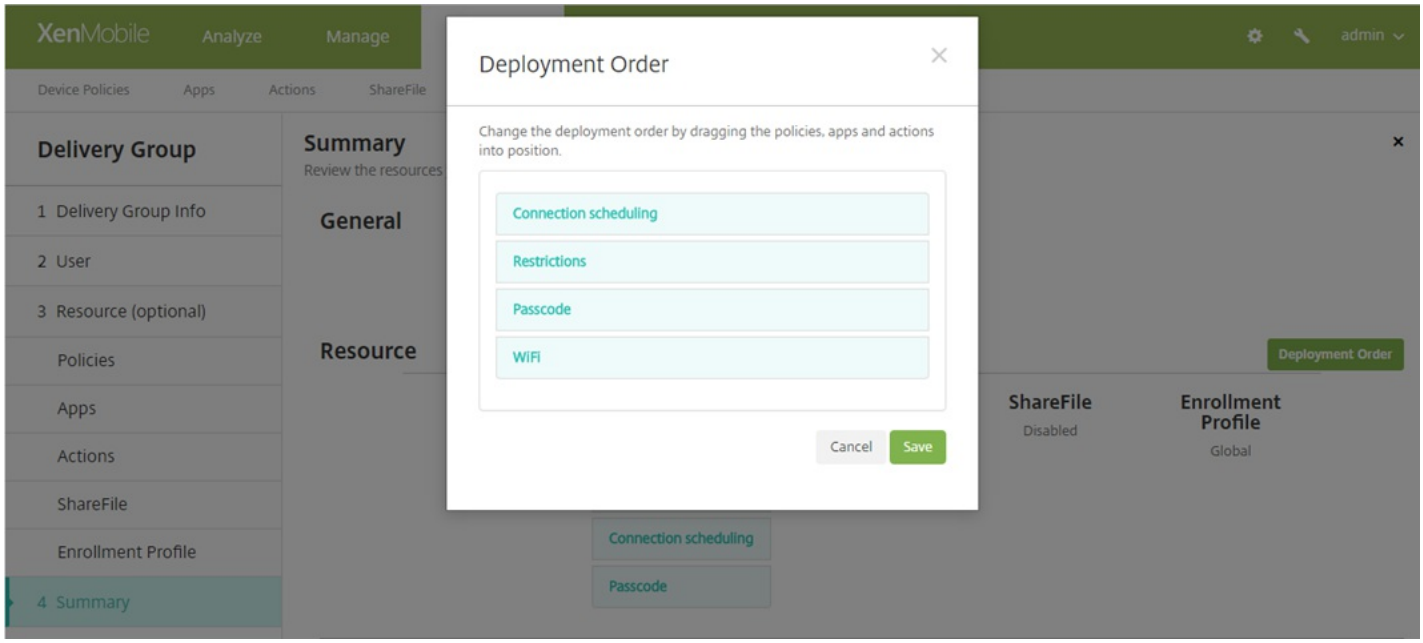
    d. 如果同一个资源出现不止一次，则删除重复的资源。

已与用户定义的顺序关联的资源将先于不具备此类顺序的资源进行部署。 一个资源可位于被分配给用户的多个交付组中。 如上述步骤所示，计算算法将删除冗余资源，仅提供列表中的第一个资源。通过以此方式删除重复资源，XenMobile 可强制执行由 XenMobile 管理员定义的顺序。

例如，假设您具有如下两个交付组：

- 交付组 Account Managers 1：资源顺序**未指定**，包含策略 **WiFi** 和**通行码**。
- 交付组 Account Managers 2：资源顺序**已指定**，包含策略**连接计划**、**限制**、**通行码**和 **WiFi**。 在此示例中，您希望在交付 **WiFi** 策略之前交付**通行码**策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

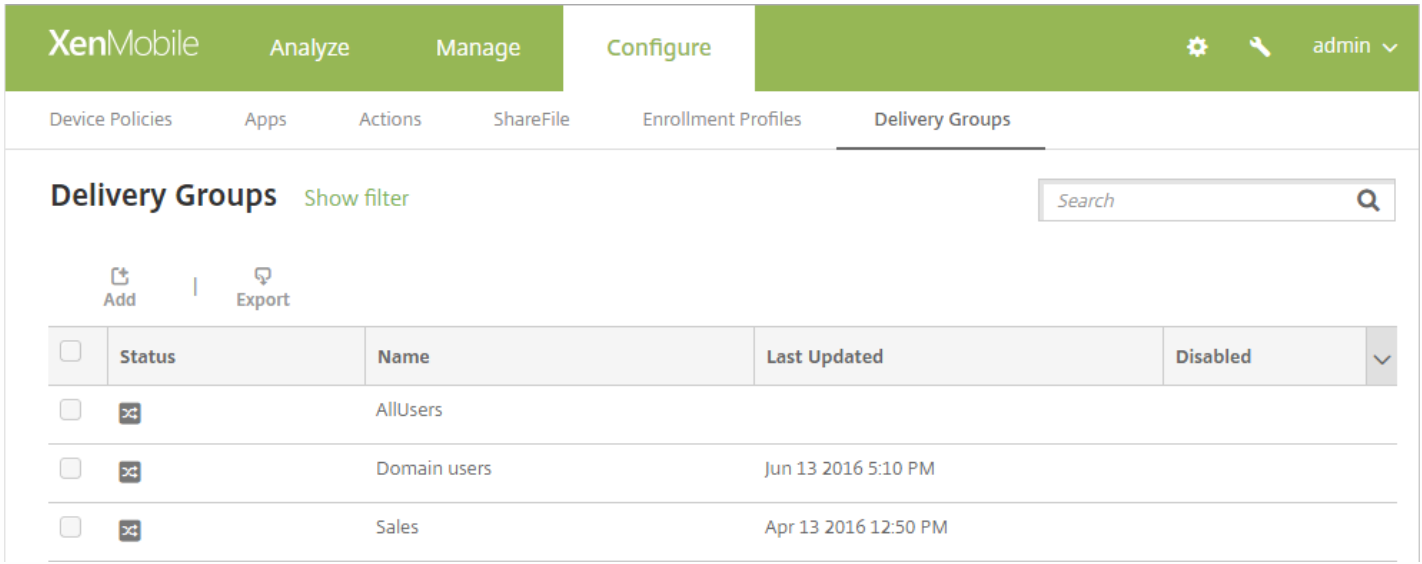


如果计算算法仅按名称对部署组进行排序，XenMobile 将按此顺序执行部署，首先部署交付组 Account Managers 1：**WiFi**、**通行码**、**连接计划**和**限制**。 XenMobile 将忽略 Account Managers 2 交付组中的重复策略，即**通行码**和 **WiFi**。

但是，由于 Account Managers 2 组具有管理员指定的部署策略，因此，计算算法会将 Account Managers 2 交付组中的资源放置在列表中较 Account Managers 1 交付组中的资源靠前的位置。 因此，XenMobile 将按以下顺序部署策略：**连接计划**、**限制**、**通行码**和 **WiFi**。 XenMobile 将忽略 Account Managers 1 交付组中的策略 **WiFi** 和**通行码**，因为这些策略重复。 因此，该算法采用由 XenMobile 管理员指定的顺序。

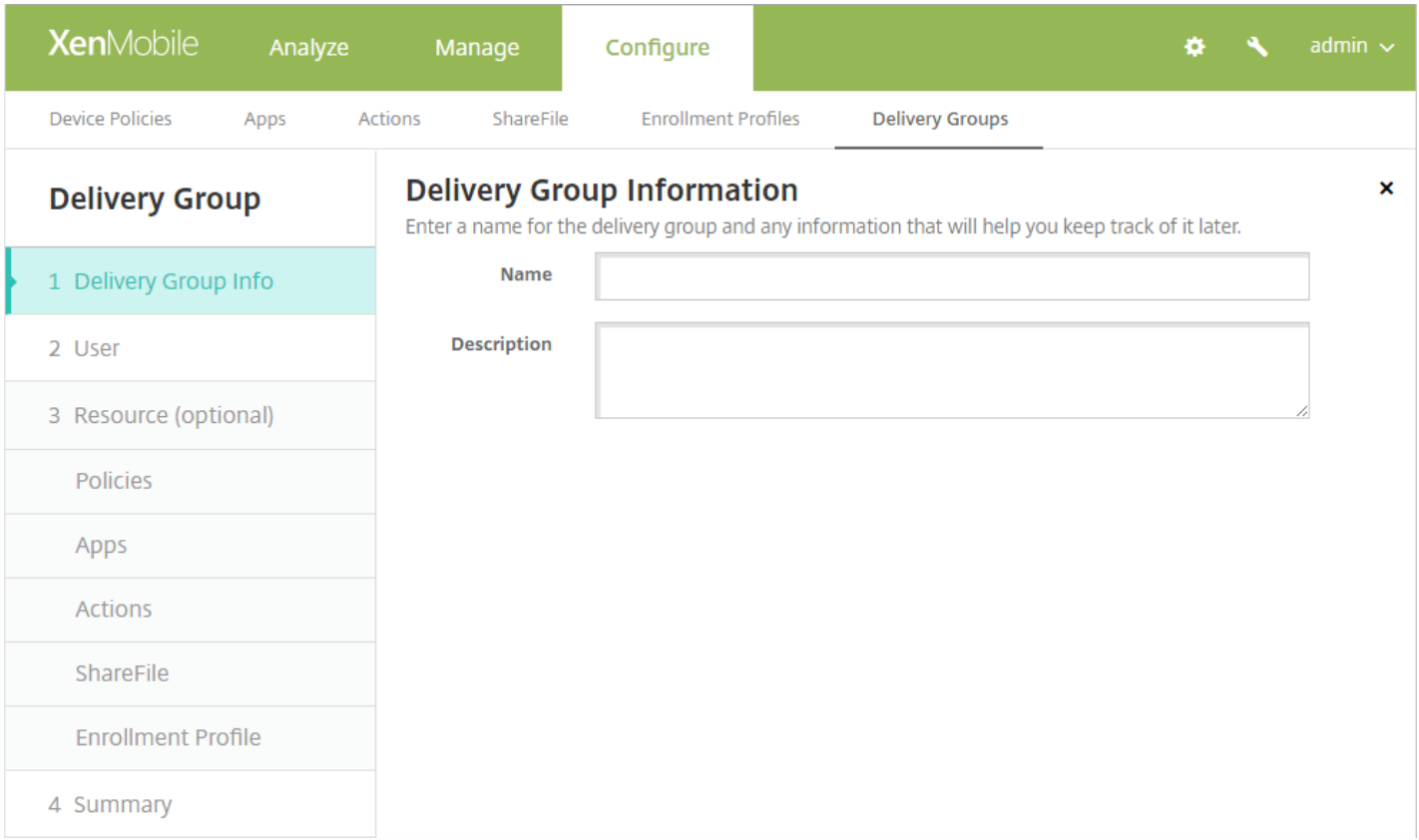
添加交付组

1. 在 XenMobile 控制台中，单击 **配置 > 交付组**。将出现**交付组** 页面。



2. 从**交付组**页面中，单击**添加**。将出现**交付组信息**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

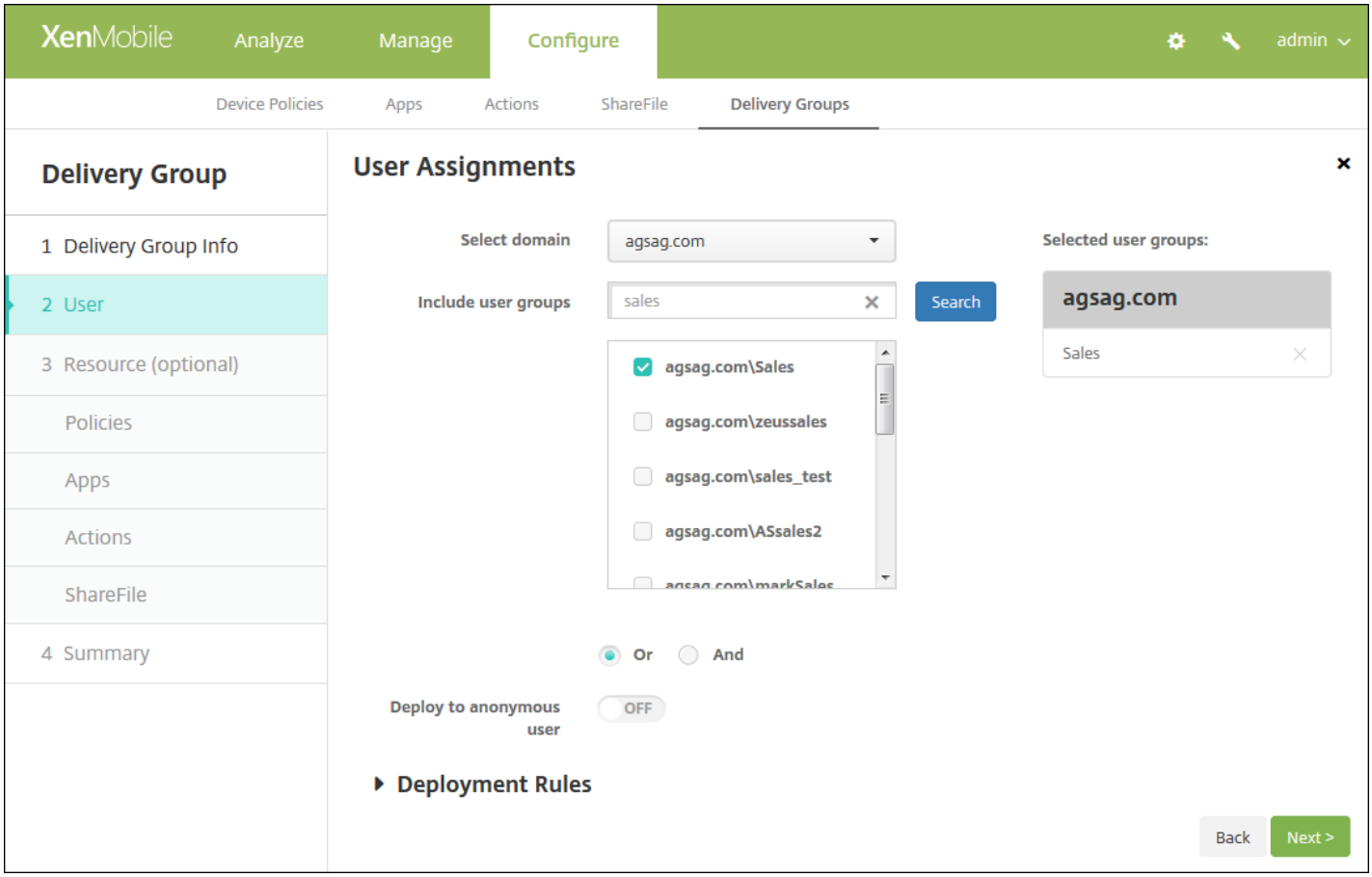


3. 在**交付组信息**页面中，输入以下信息：

- **名称**：键入交付组的描述性名称。
- **说明**：键入交付组的可选说明。

4. 单击**下一步**。将出现**用户分配**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 配置以下设置：

- **选择域**：在列表中，选择要从中选择用户的域。
- **包括用户组**：请执行以下操作之一：
  - 在用户组列表中，单击要添加的组。所选的组将显示在**选定用户组**列表中。
  - 单击**搜索**以查看选定域中所有用户组的列表。
  - 在搜索框中键入完整或部分组名称，然后单击**搜索**以限制用户组列表。
    - 要从**选定用户组**列表中移除某个用户组，请执行以下操作：
      - 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** 可查看到选定域中所有用户组的列表。滚动此列表，并清除需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，并取消选中要删除的各个组旁边的复选框。
- **Or/And**：选择用户是位于任意组 (Or) 即可，还是必须位于所有组中 (And)，才能向其置备资源。
- **Deploy to anonymous user**（部署到匿名用户）：选择是否部署到交付组中未经身份验证的用户。

  注意：未经身份验证的用户是指您无法对其进行身份验证、但仍允许其设备与 XenMobile 进行连接的用户。

6. 配置部署规则

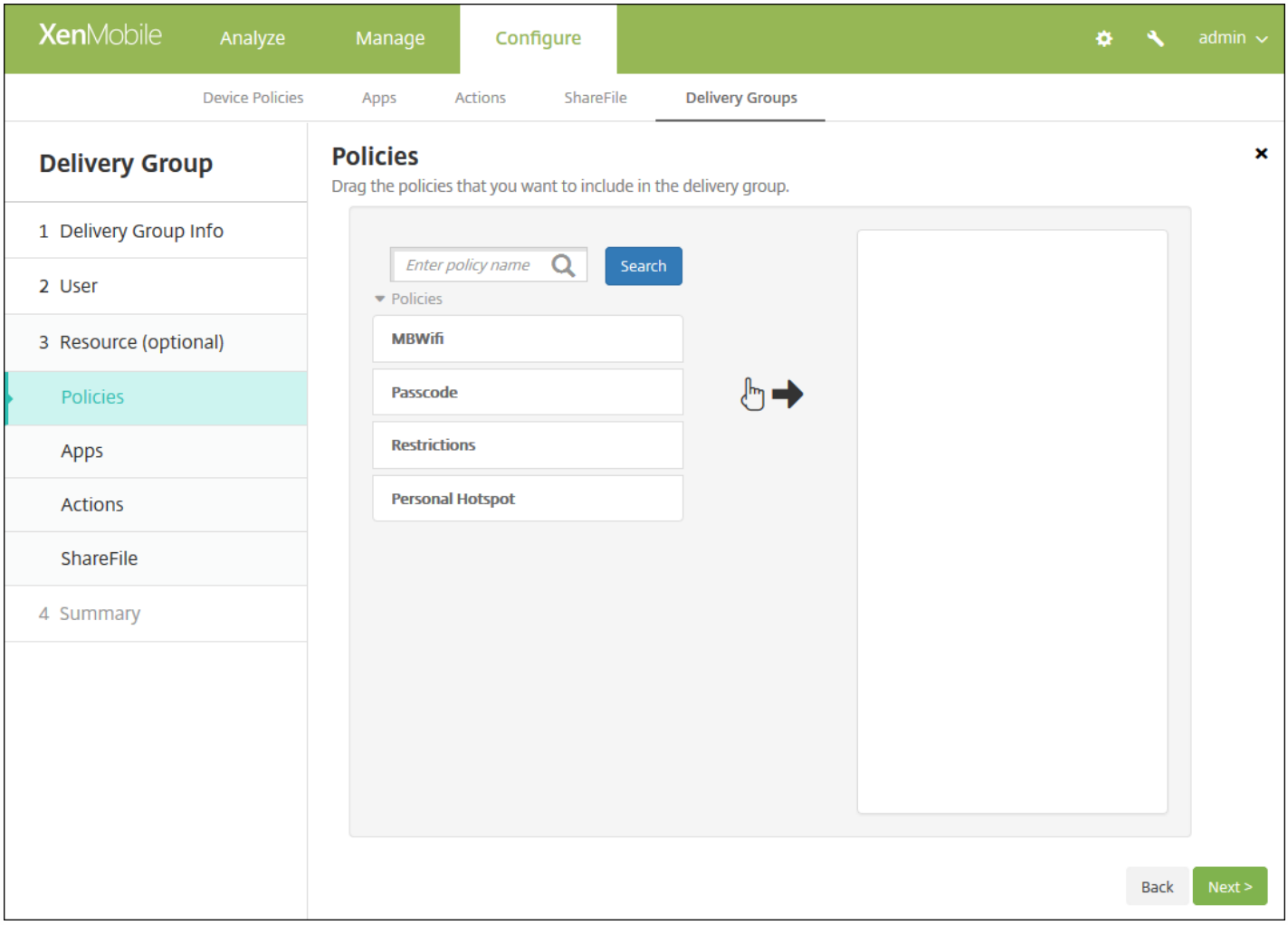
向交付组添加可选资源

您可以向交付组中添加可选资源以应用特定策略，提供必需的应用程序和可选应用程序，添加自动化操作，并启用 ShareFile 以实现对内容和数据的单点登录。 以下部分介绍如何添加策略、应用程序、操作和启用 ShareFile。 您可以向交付组中添加这些资源中的任意或全部资源，也可以不添加任何资源。 要跳过添加资源，请单击要添加的资源或单击**摘要**以跳过添加任何资

© 1999-2017 Citrix Systems, Inc. All rights reserved.

源。

添加策略



1. 对于要添加的各项策略，请执行以下操作：

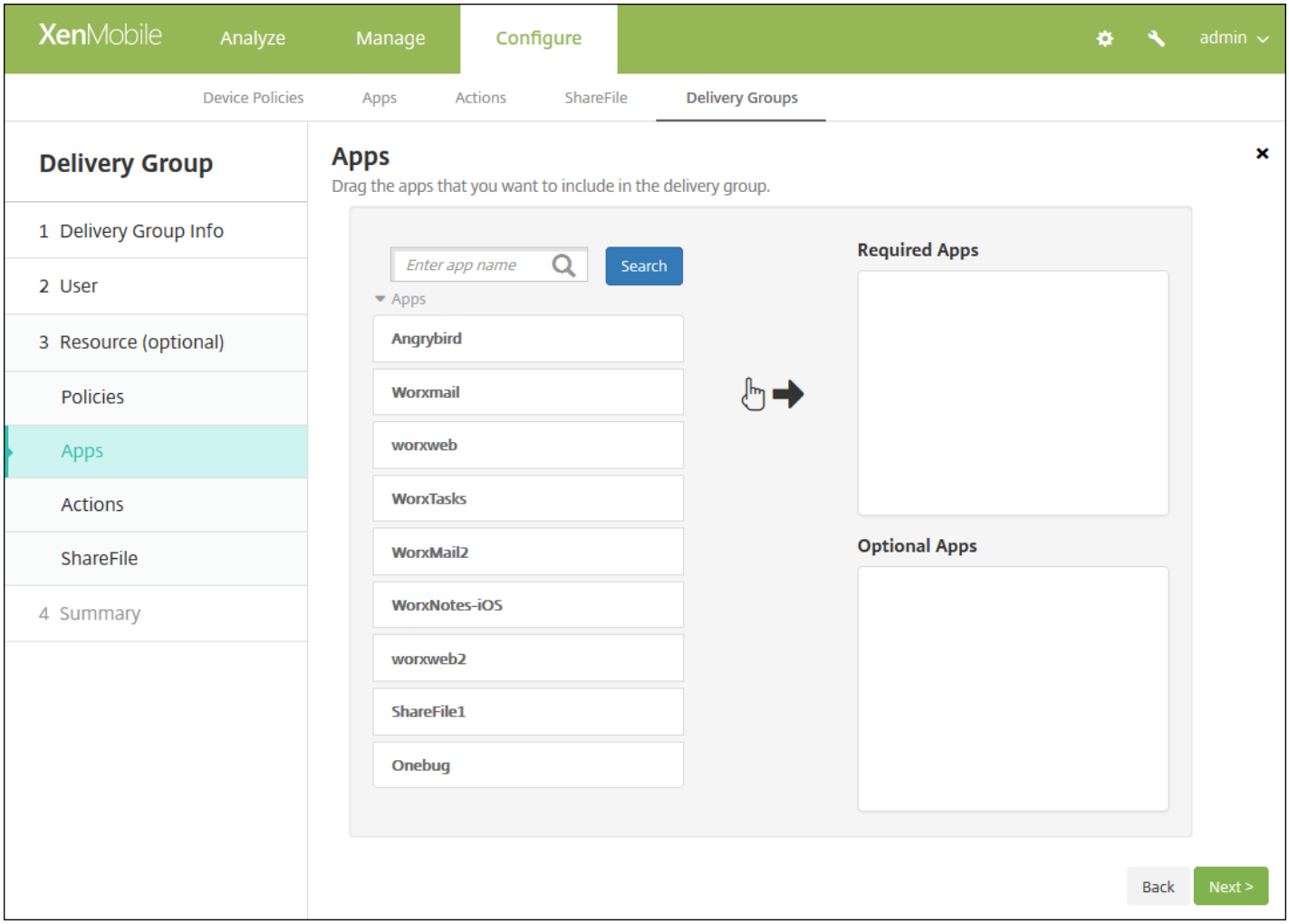
- 滚动可用策略的列表以查找要添加的策略。
- 或者，若要限制策略的列表，请在搜索框中键入完整或部分策略名称，然后单击**搜索**。
- 单击要添加的策略并将其拖动到右侧的框中。

注意：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**。 此时将显示**应用程序**页面。

添加应用程序

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. 对于要添加的每个应用程序，请执行以下操作：

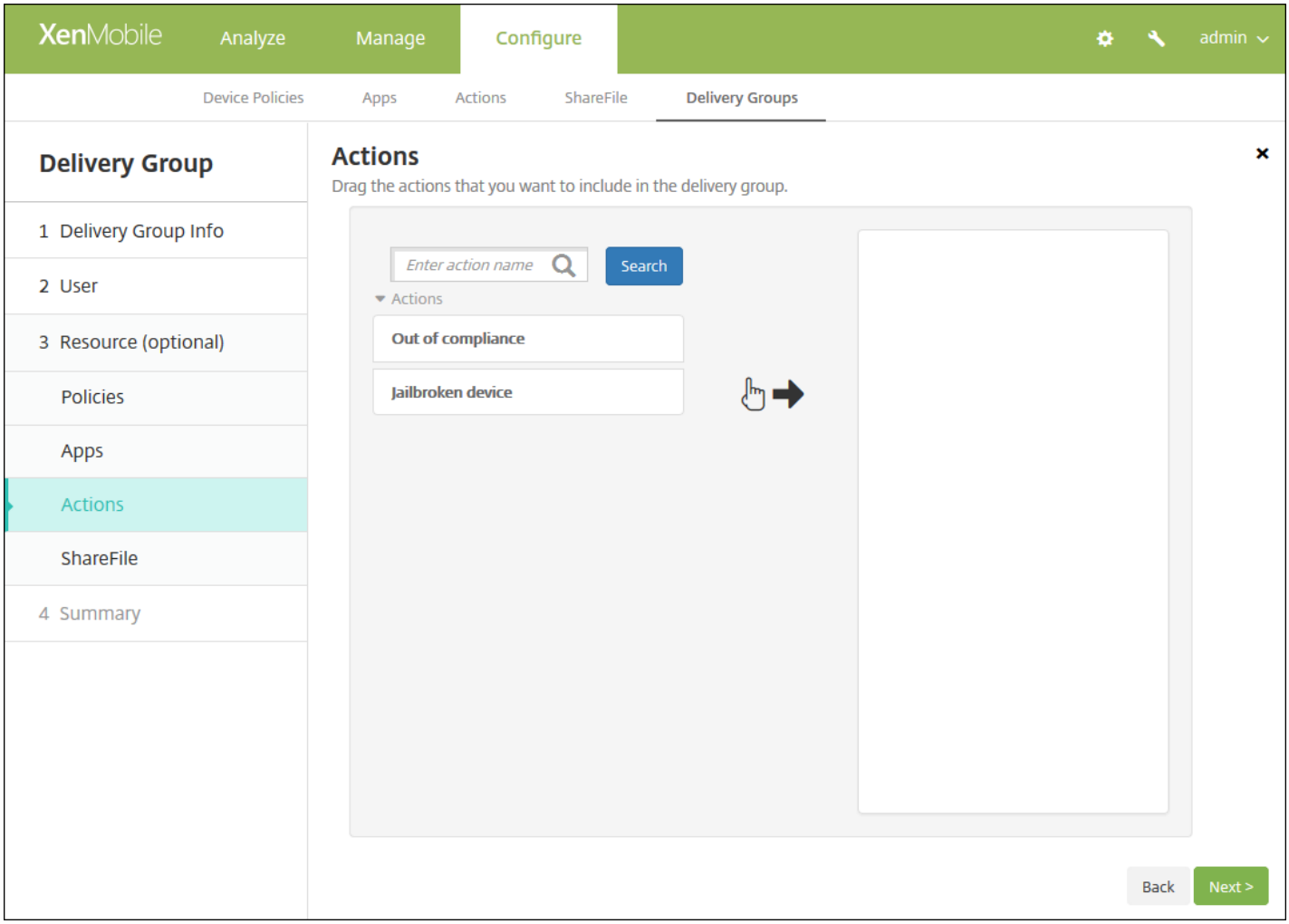
- 滚动可用应用程序的列表以查找要添加的应用程序。
- 或者，若要限制应用程序的列表，请在搜索框中键入完整或部分应用程序名称，然后单击**搜索**。
- 单击要添加的应用程序，将其拖动到**必需应用程序**框或**可选应用程序**框中。

注意：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**。 此时将显示**操作**页面。

添加操作

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. 对于要添加的每项 操作 ，请执行以下操作：

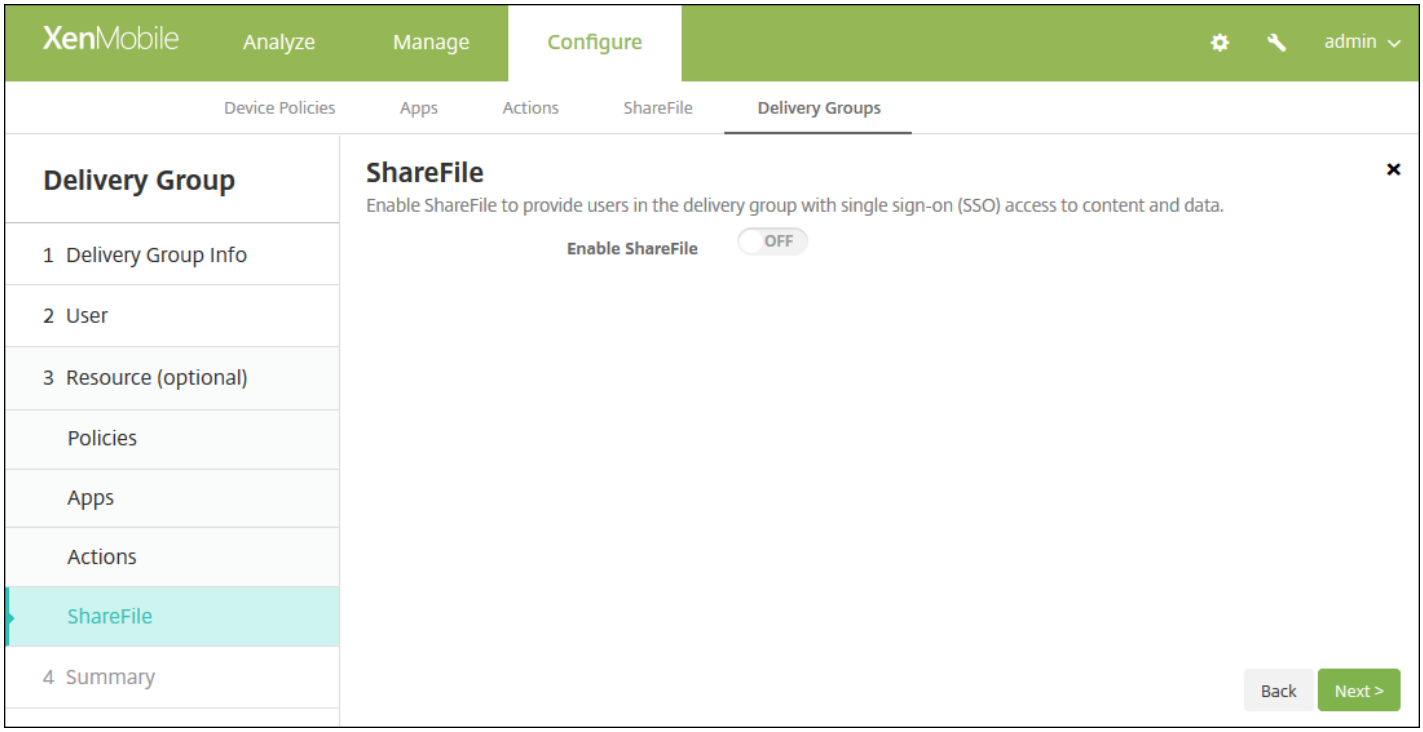
- 滚动可用操作的列表以查找要添加的操作。
- 或者，若要限制操作的列表，请在搜索框中键入完整或部分操作名称，然后单击**搜索**。
- 单击要添加的操作并将其拖动到右侧的框中。

注意：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。

启用 ShareFile

© 1999-2017 Citrix Systems, Inc. All rights reserved.



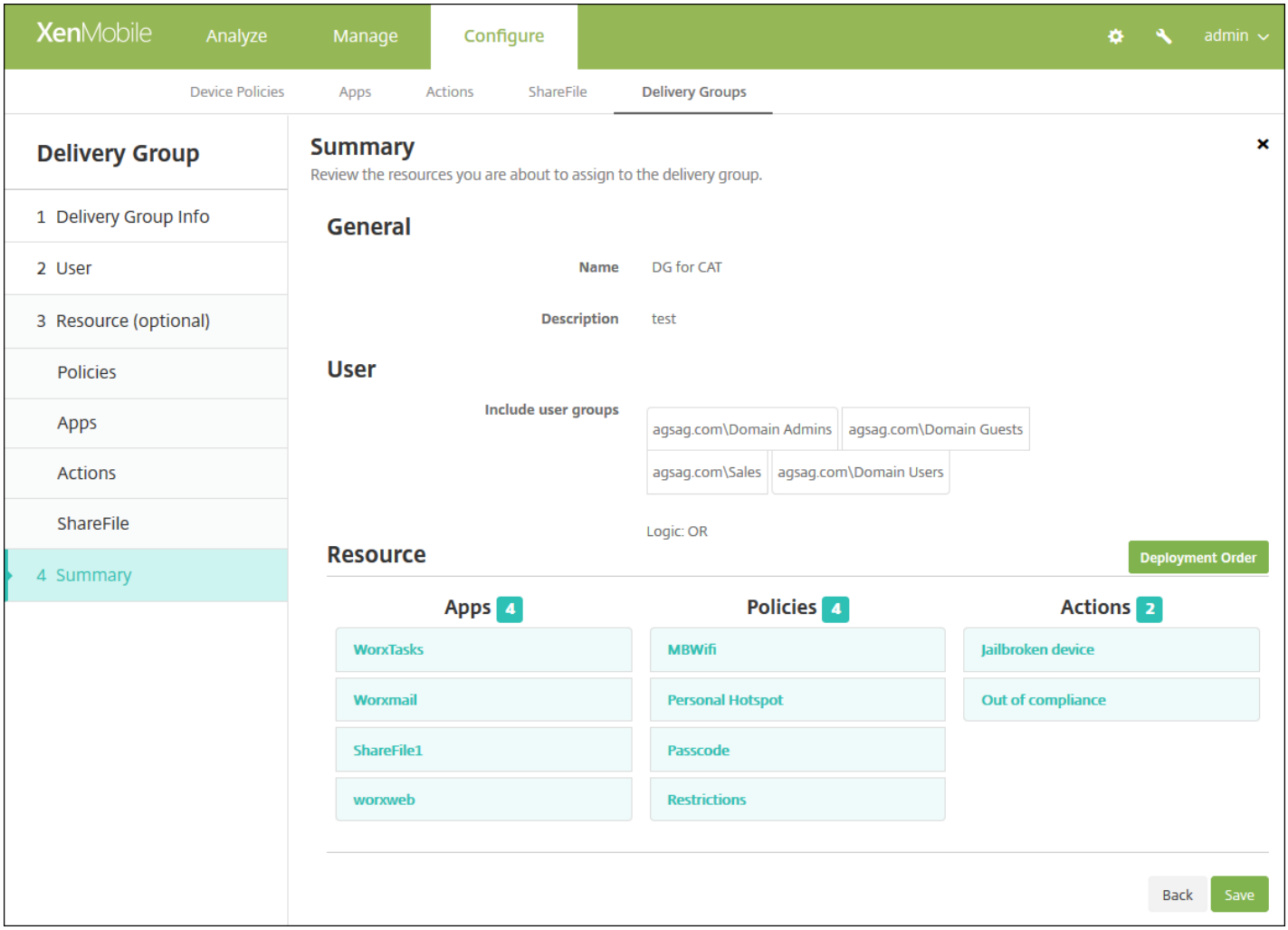
1. 配置以下设置：

- **启用 ShareFile**：单击**开**以启用对内容和数据的 ShareFile 单点登录访问。

2. 单击**下一步**。 此时将显示**摘要**页面。

检查已配置的选项并更改部署顺序

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在**摘要**页面上，可以查看已经为交付组配置的选项和更改资源的部署顺序。 “摘要”页面按顺序显示您的资源；不反映部署顺序。

1. 单击**后退**可返回到上一个页面，对配置进行必需的调整。

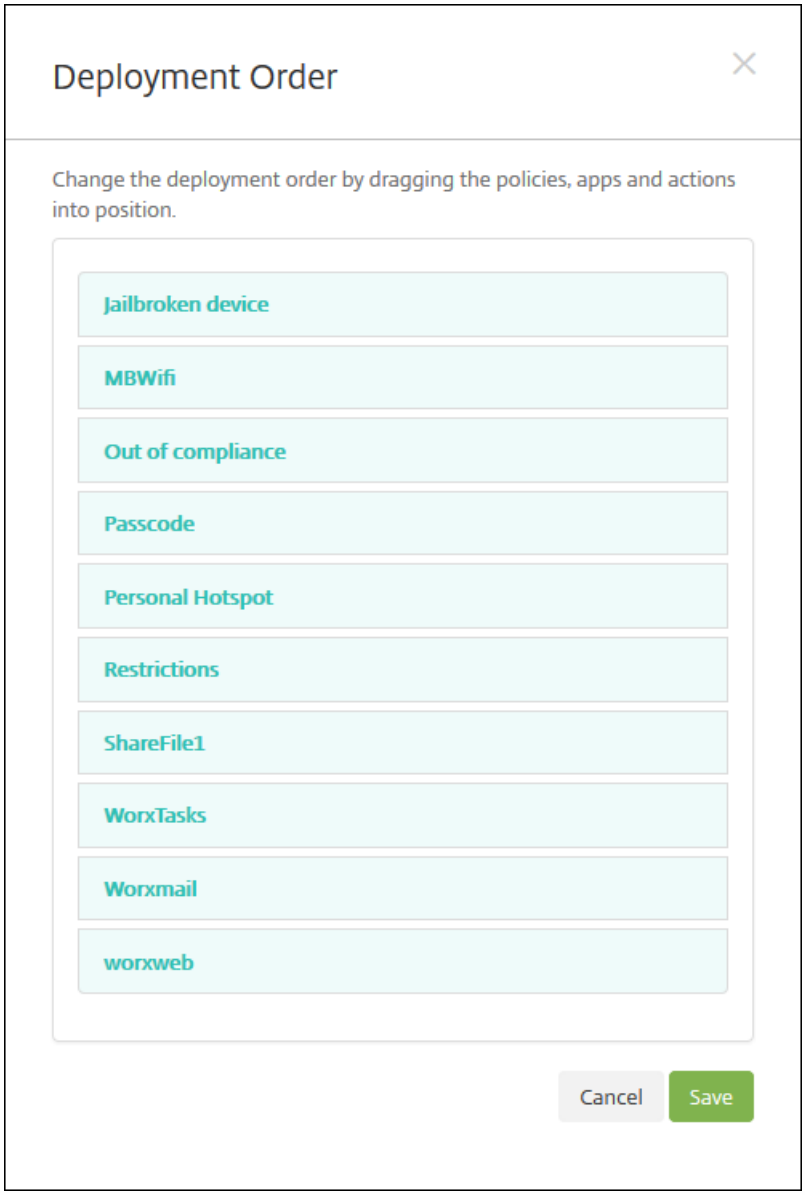
2. 单击**部署顺序**查看部署顺序或对部署顺序重新排序。

3. 单击**保存**以保存交付组。

更改部署顺序

1. 单击**部署顺序**按钮。 将显示**部署顺序**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 单击某个资源并将其拖动到您希望部署此资源的位置。 更改部署顺序后，XenMobile 按照从上到下的顺序部署列表中的资源。

3. 单击**保存**以保存部署顺序。

编辑交付组

1. 在**交付组**页面上，通过选择要编辑的交付组名称旁边的 复选框 或单击包含其名称的行选择此交付组，然后单击**编辑**。 此时将显示**交付组信息**编辑页面。

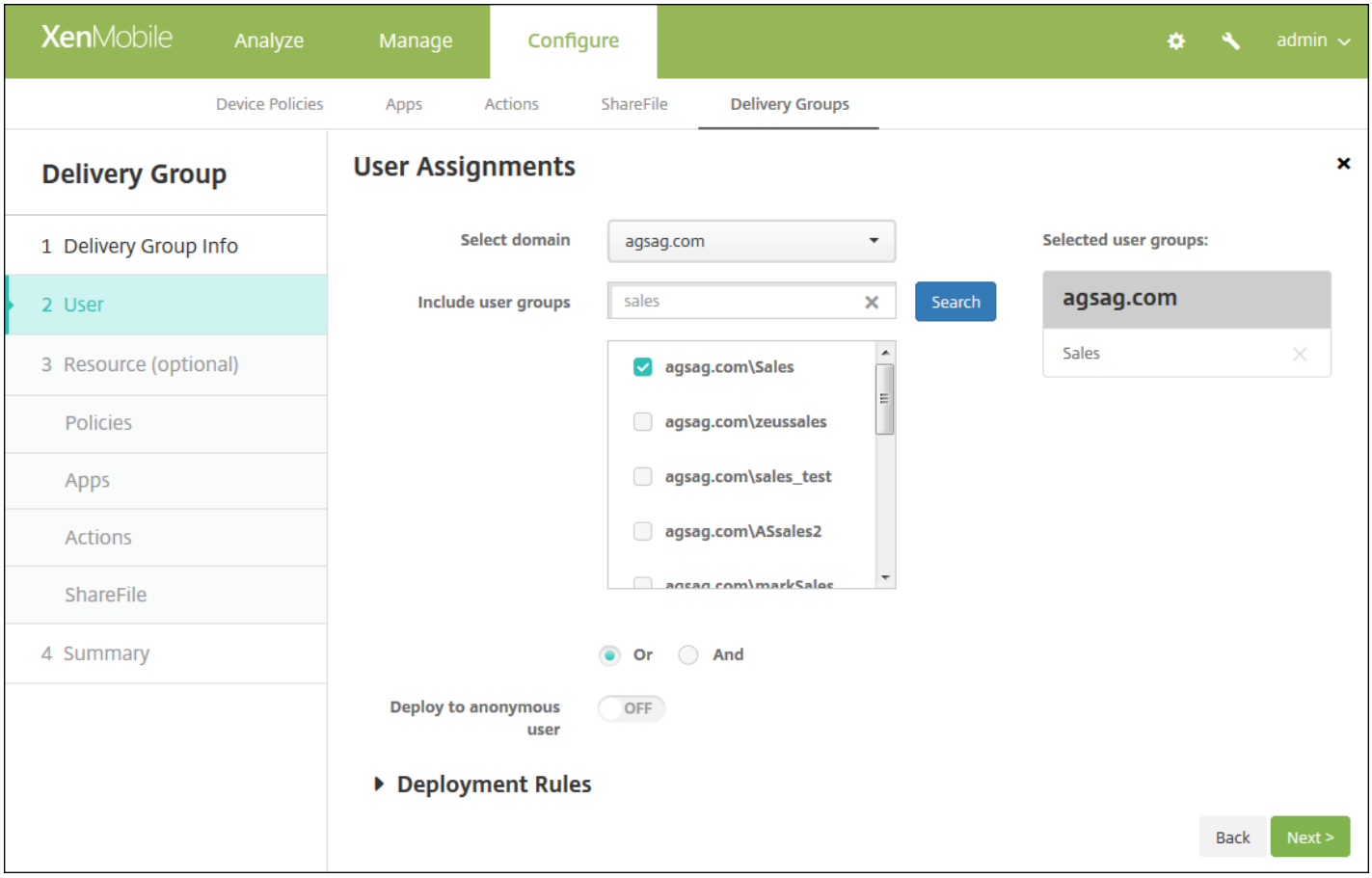
> **注意**
>
> 根据您选择交付组的方式，**编辑**命令将显示在交付组的上方或右侧。

2. 添加或更改**说明**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：无法更改现有组的名称。

3. 单击**下一步**。 此时将显示**用户分配**页面。



4. 在**选择用户组**页面中，输入或更改以下信息：

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

    注意：要删除用户组，请单击**搜索**，然后在用户组列表中，取消选中要删除的一个或多个组旁边的 复选框 。 您可以在搜索框中键入完整或部分组名称，然后单击**搜索**以限制列表中显示的用户组数。

- **Or/And**：选择用户是位于任意组 (Or) 即可，还是必须位于所有组中 (And) 才可以进行部署。
- **部署到 匿名 用户**：选择是否部署到交付组中未经身份验证的用户。

  注意：未经身份验证的用户是指您无法对其进行身份验证、但仍允许其设备与 XenMobile 进行连接的用户。

5. 展开**部署规则**，然后按照之前在此过程中的第 5 步执行的操作配置设置。

6. 单击**下一步**。 此时将显示**交付组资源**页面。 可以在此处添加或删除策略、应用程序和操作。 要跳过此步骤，请在**交付组**下面，单击**摘要**以查看交付组配置的摘要。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 修改完资源后，单击**下一步**，或在**交付组**下面，单击**摘要**。

8. 在**摘要**页面上，可以查看已经为交付组配置的选项和更改资源的部署顺序。

9. 单击**后退**可返回到上一个页面，对配置进行必需的调整。

10. 单击**部署顺序**可重新排列资源部署顺序；有关更改部署顺序的信息，请参阅更改部署顺序。

11. 单击**保存**以保存交付组。

启用和禁用 AllUsers 交付组

> **注意**
>
> AllUsers 是唯一一个您可以启用或禁用的交付组。

1. 从**交付组**页面，选中 **AllUsers** 旁边的复选框或单击包含 AllUsers 的行，以选择 AllUsers 交付组。 然后执行以下操作之一：

注意：根据您选择 AllUsers 的方式，**启用**或**禁用**命令将显示在 AllUsers 交付组的上方或右侧。

- 单击**禁用**可禁用 AllUsers 交付组。 此命令仅在已启用 AllUsers（默认）时才可用。 **禁用的交付组**将显示在交付组表格中的**已禁用**标题下。
- 单击**启用**可启用 AllUsers 交付组。 此命令仅在当前已禁用 AllUsers 时才可用。 **禁用的交付组**不再显示在交付组表格中的**已禁用**标题下。

部署交付组

部署到交付组意味着向该交付组中包含的所有 iOS、Windows Phone 和 Windows 平板电脑设备用户发送推送通知以重新连接到 XenMobile。 这样，您就可以重新评估设备以及部署应用程序、策略和操作。 其他平台设备的用户将立即收到资源（如果他们已连接）；或者，基于用户的计划策略在下次连接时收到资源。

注意：要使已更新的应用程序显示在用户 Android 设备上 Worx Store 中的“Updated Available”（更新可用）列表中，必须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：

- 要同时部署多个交付组，请选中要部署的组旁边的复选框。
- 要部署单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。

2. 单击**部署**。

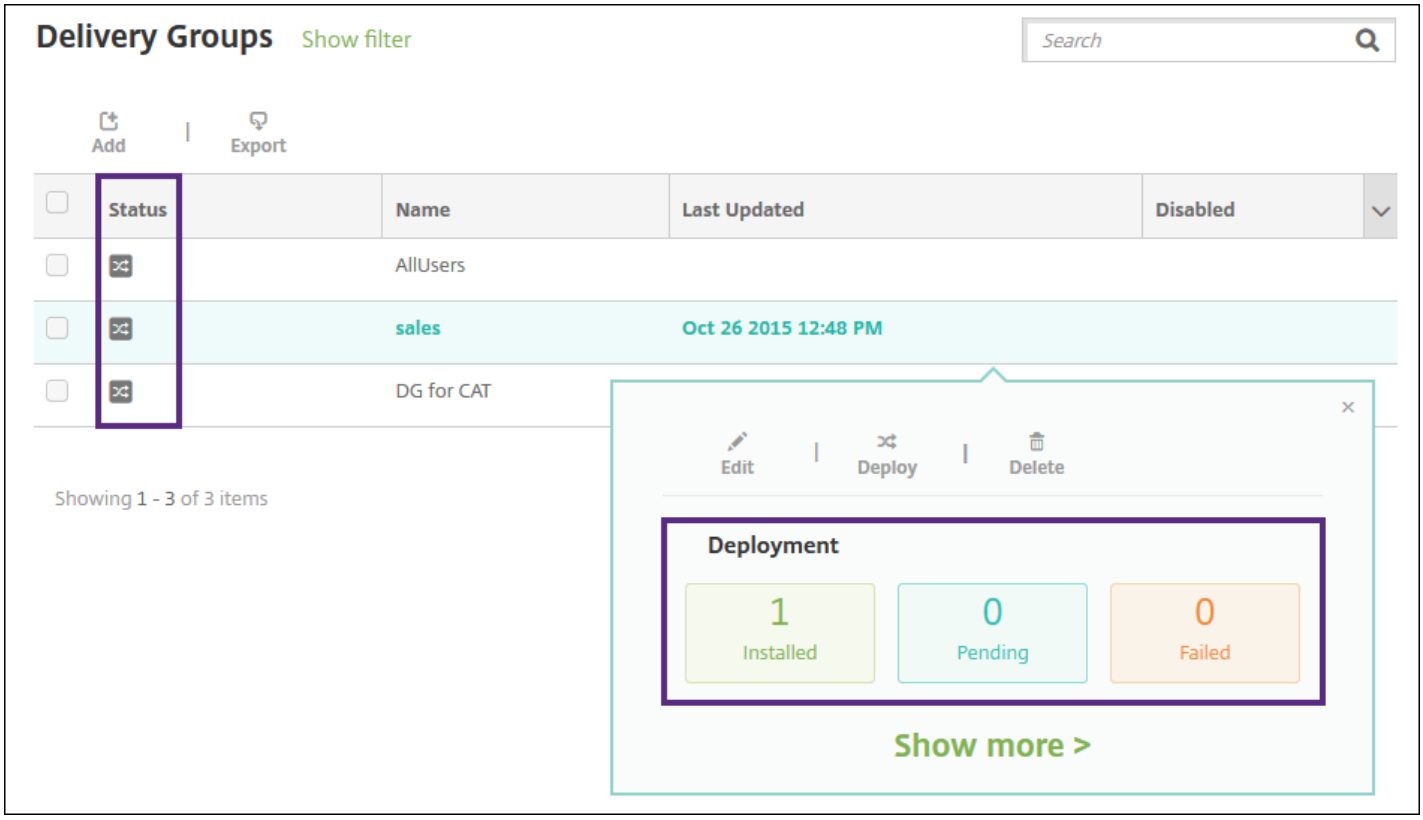
注意：根据您选择单个交付组的方式，**部署**命令将显示在交付组的上方或右侧。

验证是否已列出要向其中部署应用程序、策略和操作的组，然后单击**部署**。会基于设备平台和计划策略将应用程序、策略和操作部署到所选组。

可以通过以下方式之一在**交付组**页面上检查部署状态。

- 查看 **状态**标题下此交付组的部署图标，此图标会指出部署失败状态。
- 单击包含此交付组的行，以显示指示**已安装**、**待定**和**失败**部署的叠加项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



删除交付组

> **注意**
>
> 您无法删除 AllUsers 交付组，但是，如果您不希望向所有用户推送资源，可以禁用此组。

1. 在**交付组**页面上，执行以下操作之一：

- 要同时删除多个交付组，请选中要删除的组旁边的复选框。
- 要删除单个交付组，请选中其名称旁边的复选框或单击包含其名称的行。

2. 单击**删除**。 将显示**删除**对话框。

注意：根据您选择单个交付组的方式，**删除**命令将显示在交付组的上方或右侧。

3. 单击**删除**。

> **Important**
>
> 此操作无法撤消。

导出交付组表

1. 单击**交付组**表上方的**导出**按钮。 XenMobile 提取**交付组**表中的信息，并将其转换为 .csv 文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 打开或保存 .csv 文件。 执行此操作的方式取决于所使用的浏览器。 您也可以取消此操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注册用户和设备

Aug 15, 2016

为了安全地远程管理用户设备，需要在 XenMobile 中注册这些设备。 将 XenMobile 客户端软件安装在用户设备上，用户经过身份验证，然后安装 XenMobile 和用户配置文件。 完成设备注册后，可以在 XenMobile 控制台中执行各种设备管理任务，例如应用策略、部署应用程序、将数据推送到设备、锁定、擦除和查找丢失或被盗设备。

注意：需要先请求 APNS 证书后才能注册 iOS 设备用户。 有关详细信息，请参阅 XenMobile 中的证书。

在 XenMobile 控制台中，单击**管理 > 注册**，访问用户和设备的配置选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Android 设备

Aug 11, 2016

1. 在 Android 设备上转到 Google Play 或 Amazon 应用商店，下载 Citrix Worx Home 应用程序，然后轻按该应用程序。
2. 提示安装应用程序时，单击下一步，然后单击安装。
3. Worx Home 安装完毕后，轻按打开。
4. 输入企业凭据，如组织的 XenMobile 服务器名称、用户主体名称 (UPN) 或电子邮件地址，然后单击下一步。
5. 在 Activate device administrator（激活设备管理员）屏幕上，轻按 Activate（激活）。
6. 输入贵公司密码，然后轻按登录。
7. 系统可能要求您创建 Worx PIN（这取决于 XenMobile 的配置方式），可使用它来登录 Worx Home 和其他支持 Worx 的应用程序，如 WorxMail、WorxWeb、ShareFile，等。 需要输入 Worx PIN 两次。 在创建 Worx PIN 屏幕上，输入包含任意六个数字序列的 PIN。
8. 重新输入 PIN。 Worx Home 打开。 这时即可访问 Worx Store 来查看您可以安装在 Android 设备上的应用程序。
9. 如果您在注册后将 XenMobile 配置为向用户的设备自动推送应用程序，将显示提示他们安装应用程序的消息。 轻按安装，安装应用程序。

取消注册和重新注册 Android 设备

重新注册设备前，首先要取消注册设备。 设备已取消注册但尚未重新注册期间，尽管仍显示在 XenMobile 控制台的设备清单列表中，但不受 XenMobile 管理。 设备不受 XenMobile 管理时，您无法跟踪设备，也无法监视设备合规性。

1. 轻按以打开 Worx Home 应用程序。
2. 轻按应用程序窗口左上角的“设置”图标。
3. 轻按重新注册。 将出现一条确认您是否要重新注册自己设备的消息。
4. 轻按确定。 此操作将会取消注册您的设备。
5. 请按照屏幕上的说明重新注册设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

iOS 设备

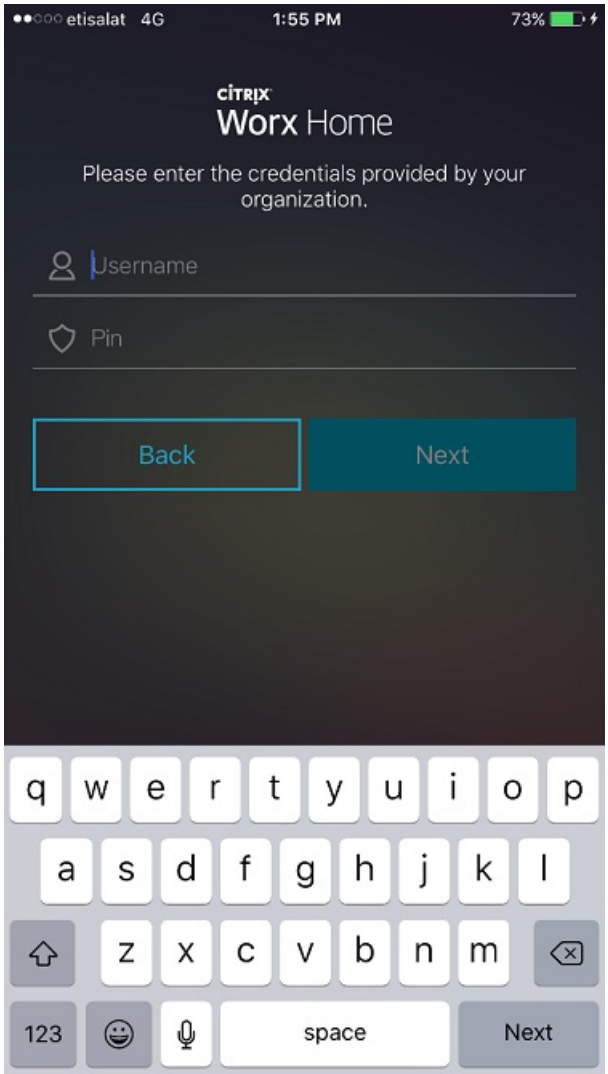
Aug 11, 2016

1. 从设备上的 Apple iTunes App Store 下载 Worx Home 应用程序，然后安装到设备上。

2. 在 iOS 设备主屏幕上，轻按 Worx Home 应用程序。

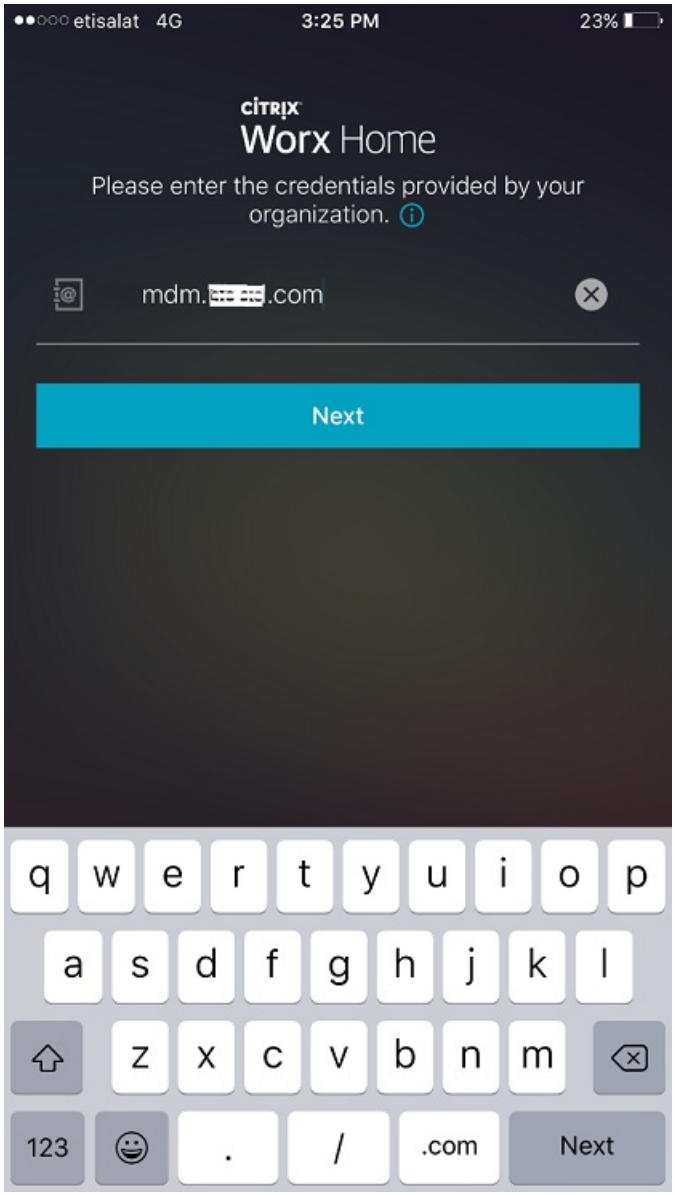
3. Worx Home 应用程序打开后，输入您的企业凭据，如贵公司 XenMobile 服务器的名称、用户主体名称 (UPN) 或者您的电子邮件，然后单击**下一步**。

这些示例中显示的屏幕可能因 XenMobile 的配置方式而异。



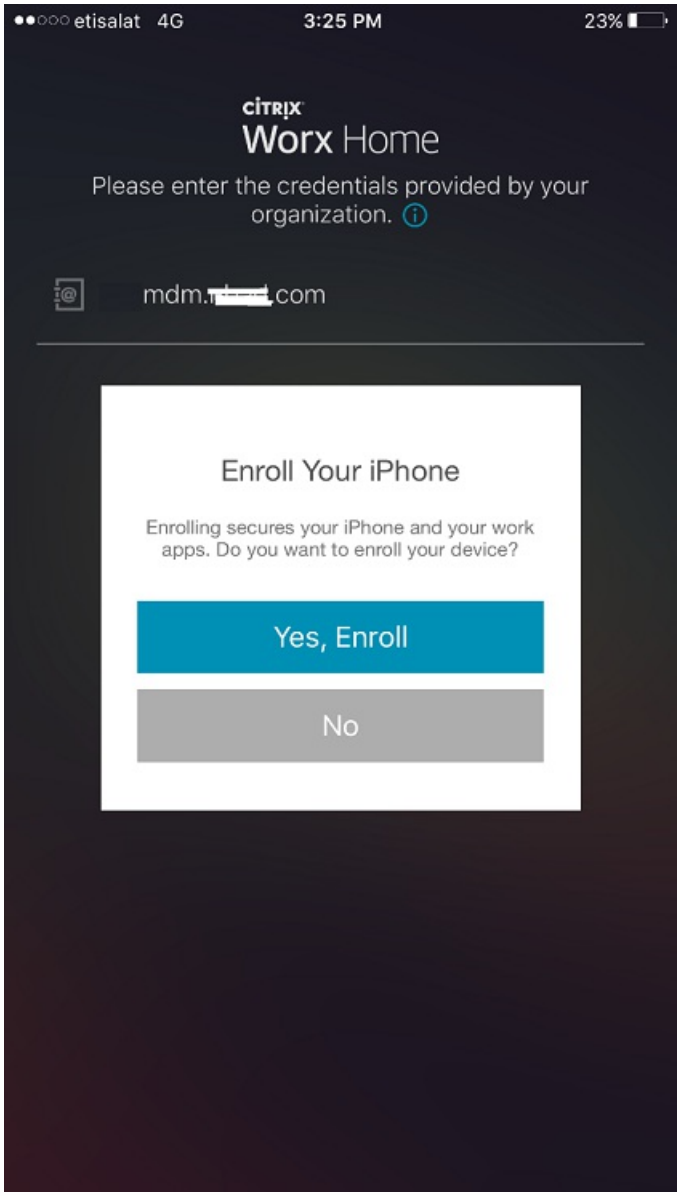
4. 输入技术支持人员提供的地址。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

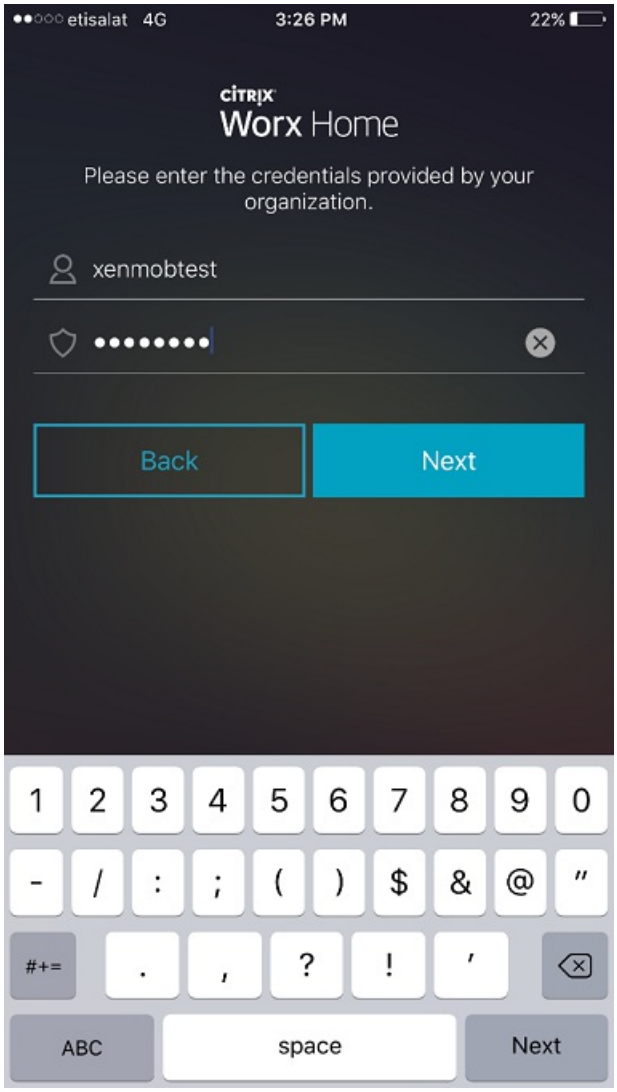


5. 系统提示注册时，单击**是，注册**，然后在收到提示时输入您的凭据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



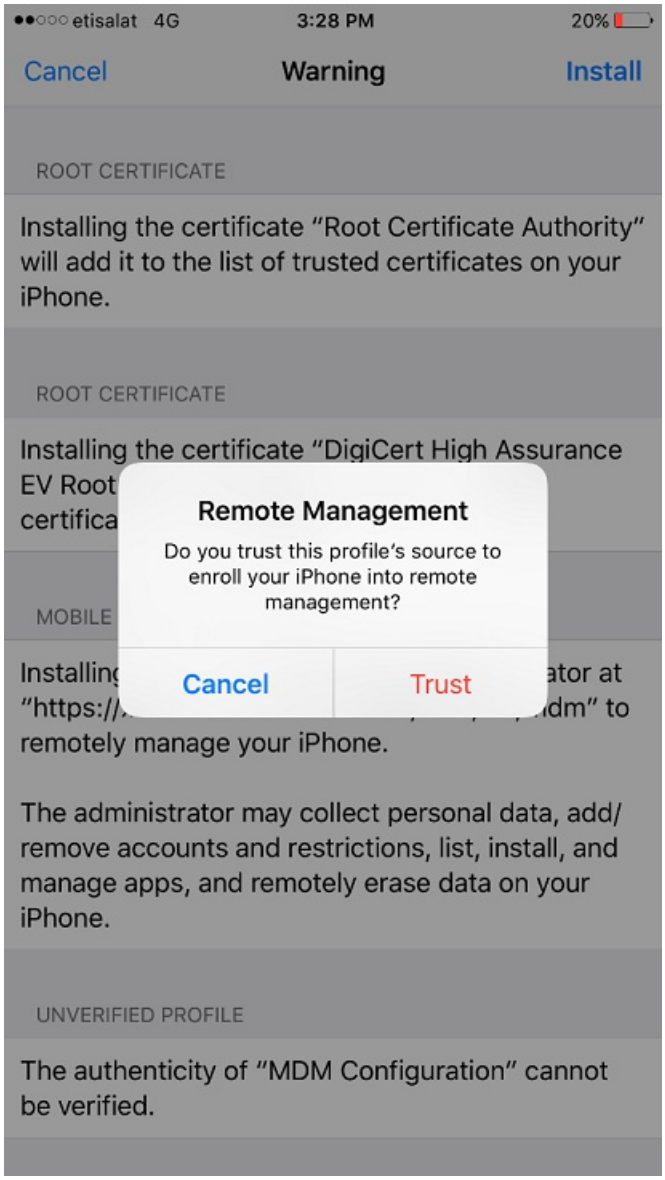
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 轻按**安装**，安装 Citrix Profile Service。

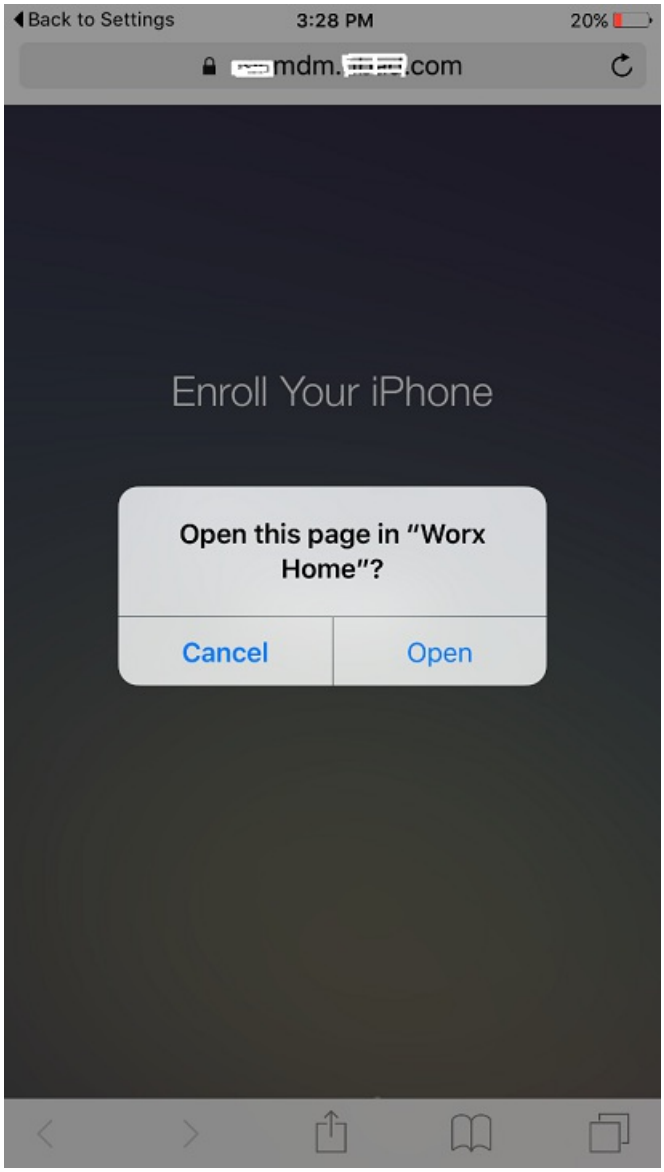
© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 轻按**信任**。

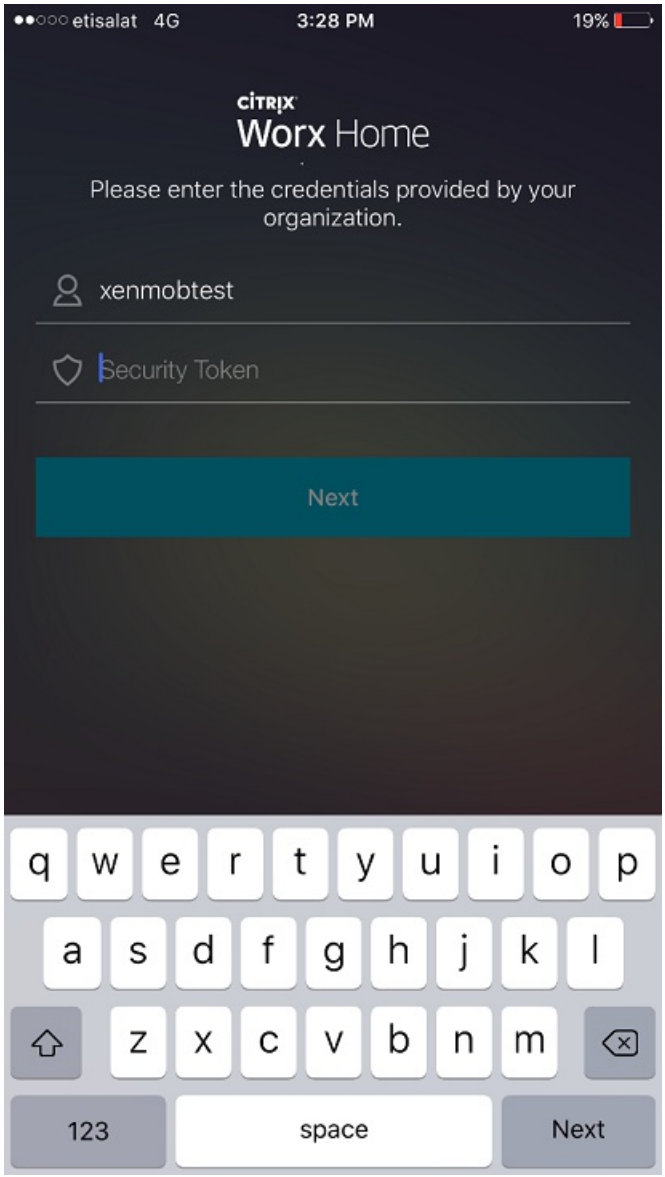


8. 轻按**打开**，然后输入您的凭据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mac OS X 设备

Aug 11, 2016

可以在 XenMobile 中注册运行 OS X 的 Mac 设备。 Mac 用户直接从其设备进行注册即可。

注册 Mac 的步骤包括：

1. 可选。在 XenMobile 控制台中注册 Mac 设备策略。 有关设备策略的详细信息，请参阅设备策略。 要了解可以为 Mac 配置的设备策略，请参阅 XenMobile 设备策略（按平台）。

2. 发送注册链接 https://serverFQDN:8443/zdm/macos/otae，用户可以在 Safari 中打开此链接。 其中

- serverFQDN 是运行 XenMobile 的服务器的完全限定的域名 (FQDN)。
- 端口 8443 是默认安全端口；如果已配置其他端口，请使用该端口替换 8443。
- zdm 是服务器安装期间使用的实例名称。

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。 用户是否会收到安装证书的提示取决于您是否为 iOS 和 Mac OS 配置了公众信任的 SSL 证书和公众信任的数字签名证书。 有关证书的详细信息，请参阅证书。

4. 用户登录其 Mac 设备。

5. 安装 Mac 设备策略。

现在即可以像管理移动设备一样使用 XenMobile 管理 Mac。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows 设备

Aug 11, 2016

可以在 XenMobile 中注册运行以下 Windows 操作系统的设备：

- Windows 8.1 和 10
- Windows Phone 8.1 和 10

Windows 和 Windows Phone 用户直接通过其设备注册。

必须为用户注册配置自动发现和 Windows 发现服务，才能启用对 Windows 和 Windows Phone 设备的管理。

> **注意**
>
> SSL 侦听器证书必须是公用证书，才能注册 Windows 设备。 如果上载了自签名 SSL 证书，注册将失败

在配置自动发现的情况下注册 Windows 设备

用户可注册运行 Windows RT 8.1、以及 32 位和 64 位版本的 Windows 8.1 Pro 和 Windows 8.1 Enterprise 以及 Windows 10 的设备。 要启用对 Windows 设备的管理，Citrix 建议您配置自动发现和 Windows 发现服务。 有关详细信息，请参阅在 XenMobile 中启用自动发现以执行用户注册。

1. 在设备上，找到并安装所有可用的 Windows 更新。 此步骤在从 Windows 8 升级到 Windows 8.1 时特别重要，因为不会自动通知用户所有可用的更新。

2. 在超级按钮菜单中，轻按**设置**，然后执行以下操作：

- 对于 Windows 8.1，请轻按**网络** > **工作区**。
- 对于 Windows 10，请轻按**帐户** > **工作单位访问** > **注册设备管理**。

3. 输入您的公司电子邮件地址，然后轻按**打开**（在 Windows 8.1 上）或**继续**（在 Windows 10 上）。 要注册为本地用户，输入带有正确域名的不存在的电子邮件地址（例如，foo@mydomain.com）。 这将允许您跳过已知 Microsoft 限制，即注册由 Windows 上的内置设备管理执行；在**正在连接到服务**对话框中，输入与本地用户关联的用户名和密码。 设备即会自动发现 XenMobile 服务器并开始注册过程。

4. 输入您的密码。 使用与某帐户相关的密码，该帐户应该是 XenMobile 中用户组的一部分。

5. 对于 Windows 8.1，请在**允许 IT 管理员提供的应用和服务**对话框中，指出您同意托管自己的设备，然后轻按**打开**。 对于 Windows 10，请在**使用条款**对话框中，指出您同意托管自己的设备，然后轻按**接受**。

在不配置自动发现的情况下注册 Windows 设备

可以在不配置自动发现的情况下注册 Windows 设备。 但是，Citrix 建议您配置自动发现。 由于在不配置自动发现的情况下进行注册会导致在连接到所需的 URL 前调用端口 80，因此，这不是用于生产部署的最佳做法。 Citrix 建议您仅在测试环境和概念验证部署中使用此过程。

1. 在设备上，找到并安装所有可用的 Windows 更新。 此步骤在从 Windows 8 升级到 Windows 8.1 时特别重要，因为不会自动通知用户所有可用的更新。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 在超级按钮菜单中，轻按**设置**，然后执行以下操作：

- 对于 Windows 8.1，请轻按**网络** > **工作区**。
- 对于 Windows 10，请轻按**帐户** > **工作单位访问** > **注册设备管理**。

3. 输入企业电子邮件地址。

4. 在 Windows 10 上，如果未配置自动发现，将显示一个选项，您可以在此处输入服务器详细信息，如第 5 步所述。 在 Windows 8.1 上，如果**自动检测服务地址**设置为启用，请轻按以关闭此选项。

5. 在**输入服务器地址**字段中：

- 对于 Windows 8.1，采用以下格式键入服务器地址：https://*服务器 FQDN:8443/服务器实例*/Discovery.svc 如果用于未经身份验证 SSL 连接的端口不是 8443，请使用相应的端口号替换此地址中的 *8443*。
- 对于 Windows 10，请使用此地址：https://beta.managedm.com:8443/zdm/wpe。 如果用于未经身份验证 SSL 连接的端口不是 8443，请使用相应的端口号替换此地址中的 *8443*。

6. 输入您的密码。

7. 对于 Windows 8.1，请在**允许 IT 管理员提供的应用和服务**对话框中，指出您同意托管自己的设备，然后轻按**打开**。 对于 Windows 10，请在**使用条款**对话框中，指出您同意托管自己的设备，然后轻按**接受**。

在 XenMobile 中注册 Windows Phone 设备

要在 XenMobile 中注册 Windows Phone 设备，用户需要使用其 Active Directory 或内部网络电子邮件地址和密码。 如果未设置自动发现，用户还需要 XenMobile 服务器的服务器 Web 地址。 然后，他们需要按照此过程在设备上完成注册。

注意：如果您计划通过 Windows Phone 企业应用商店部署应用程序，则在用户注册前，请确保您已配置企业 Hub 策略（以及经过签名的 Citrix Worx Home、适用于您支持的每个平台的 Windows Phone 应用程序）。
1. 在 Window 手机的主屏幕上，轻按**设置**图标。

2. 对于 Windows Phone 8.1，请轻按**系统** > **工作区**，然后轻按**添加帐户**。 对于 Windows 10 Phone，请轻按**帐户** > **工作单位访问** > **注册设备管理**。

3. 在下一屏幕上，输入电子邮件地址和密码，然后轻按**登录**。

   如果为域配置了自动发现，随后几个步骤中所需的信息将会自动填充。 继续执行步骤 8。

   如果没有为域配置自动发现，请继续执行下一步。 要注册为本地用户，输入带有正确域名的不存在的电子邮件地址（例如，foo@mydomain.com）。 这样允许您绕过已知的 Microsoft 限制；在**正在连接到服务**对话框中，输入与本地用户关联的用户名和密码。

4. 在下一屏幕上，键入 XenMobile 服务器的 Web 地址，例如 https://://wpe。 例如，https://mycompany.mdm.com:8443/zdm/wpe。 **注意**：端口号必须适应您的实现，但应该与您进行 iOS 注册时使用的端口相同。

5. 如果通过用户名和域进行身份验证，请输入用户名和域，然后轻按**登录**。

6. 如果出现提示证书有问题的屏幕，则该错误是由于使用自签名证书造成的。 如果服务器可信，轻按**继续**。 否则，轻按**取消**。

7. 在 Windows Phone 8.1 上，添加帐户时，您可以选择 **Install company app**（安装公司应用程序）。 如果管理员已配置 Company App Store，请选中此选项，然后轻按**完成**。 如果取消选中此选项，您需要重新注册设备才能接收 Company App Atore。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 在 Windows Phone 8.1 上，在**已添加帐户**屏幕上，轻按**完成**。

9. 要强制连接到服务器，请轻按“刷新”图标。 如果设备没有手动连接到服务器，XenMobile 会尝试重新连接。 XenMobile 会每 3 分钟连续 5 次连接设备，然后间隔改为 2 小时。 您可以在 **Server properties**（服务器属性）中的 Windows **WNS Heartbeat Interval**（Windows WNS 检测信号间隔）中修改此连接率。 注册完成后，Worx Home 将在后台注册。 安装完成时不会提示。 从**所有应用程序**屏幕打开 Worx Home。

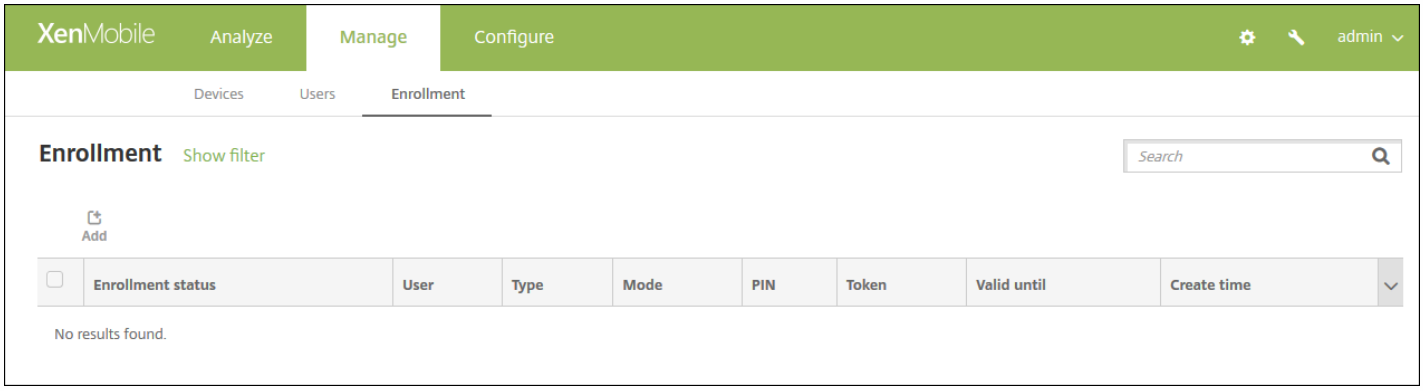
© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中发送注册邀请

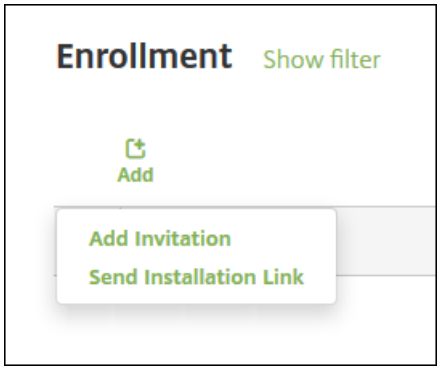
Oct 21, 2016

在 XenMobile 控制台中，可以向 iOS 或 Android 设备的用户发送注册邀请。 还可以向 iOS、Android、Windows 或 Mac 设备的用户发送安装链接。

1. 在 XenMobile 控制台中，单击**管理 > 注册**。 此时将显示**注册**页面。



2. 单击**添加**。 将显示一个菜单，其中列出了注册选项。

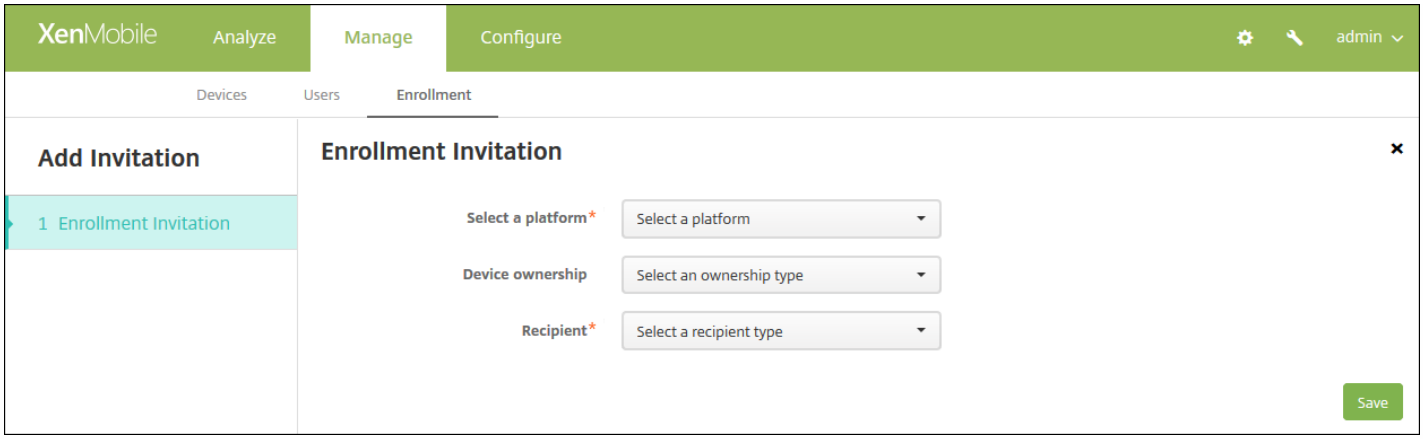


- 要向用户或组发送注册邀请，请单击**添加邀请**，然后，请参阅发送邀请了解配置此设置的步骤。
- 要通过 SMTP 或 SMS 向一系列收件人发送注册安装链接，请单击**发送安装链接**，然后，请参阅发送安装链接以了解配置此设置的步骤。

发送邀请

1. 单击**添加邀请**。 将显示**注册邀请**屏幕。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



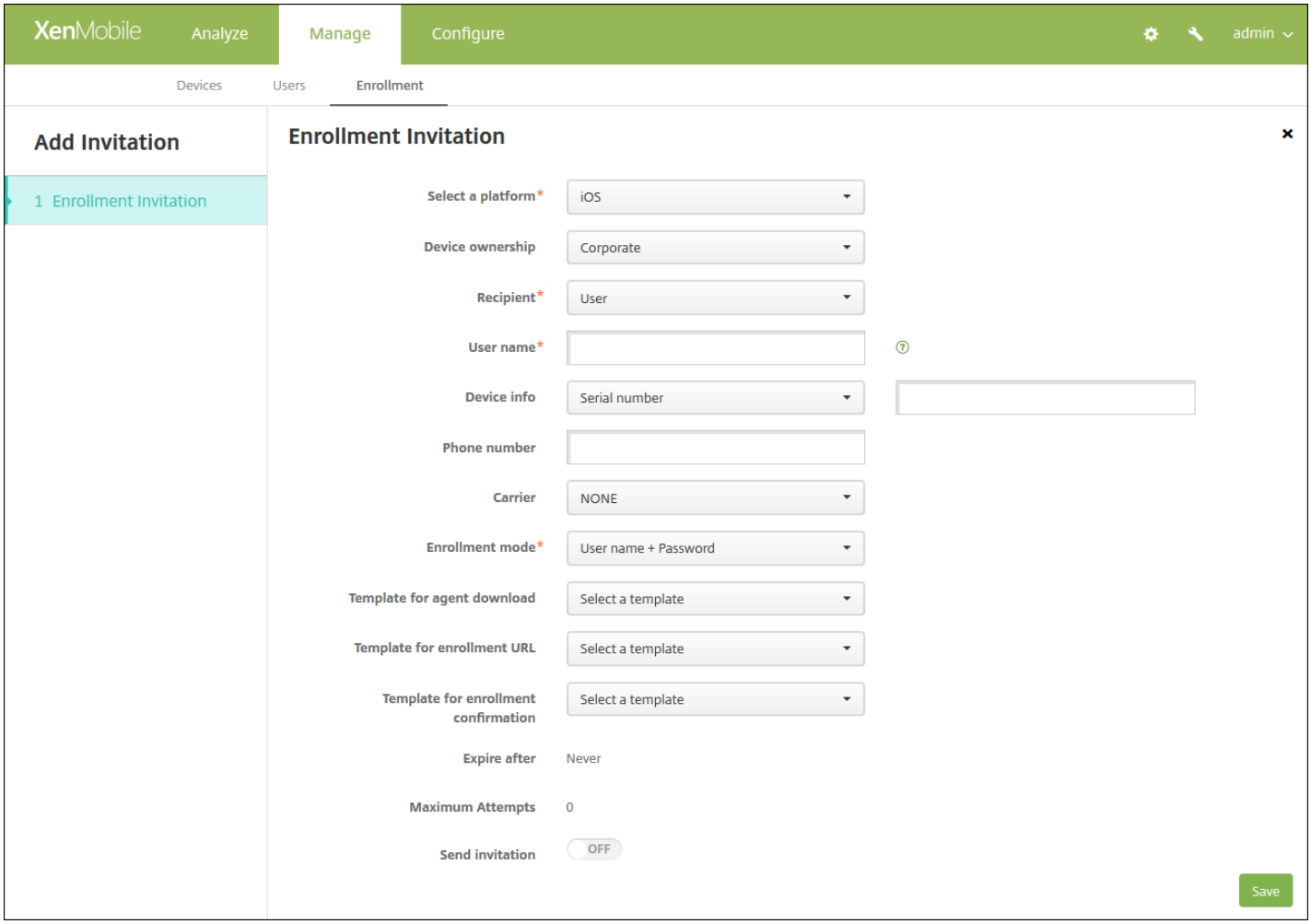
2. 配置以下设置：

- **选择平台**：在列表中，单击 **iOS** 或 **Android**。
- **设备所有权**：在列表中，单击**公司**或**员工**。
- **收件人**：在列表中，单击**用户**或**组**。

根据您选择的收件人，您将看到要配置的更多设置。 对于**用户**设置，请参阅向用户发送注册邀请；对于**组**设置，请参阅向组发送注册邀请。

向用户发送注册邀请

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. 配置以下**用户**设置：

- **用户名**：键入用户名。 用户必须作为本地用户或 Active Directory 中的用户存在于 XenMobile 服务器中。 如果用户是本地用户，确保设置用户的电子邮件属性以便发送用户通知。 如果用户是 Active Directory 中的用户，请确保配置 LDAP。
- **设备信息**：在列表中，单击 **序列 号**、**UDID** 或 **IMEI**。 选择某个选项后，将显示一个字段，您可以在此处键入设备的相应值。
- **电话号码**：可选，键入用户的电话号码。
- **运营商**：在列表中，单击用户电话号码关联的运营商。
- **注册模式**：在列表中，单击希望用户采用的注册模式。 默认值为 **用户名 + 密码**。 可用选项包括：
  - 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：选择包含 PIN 的注册模式时，会显示**注册 PIN 模板**字段，您可以在此处单击**注册 PIN**。

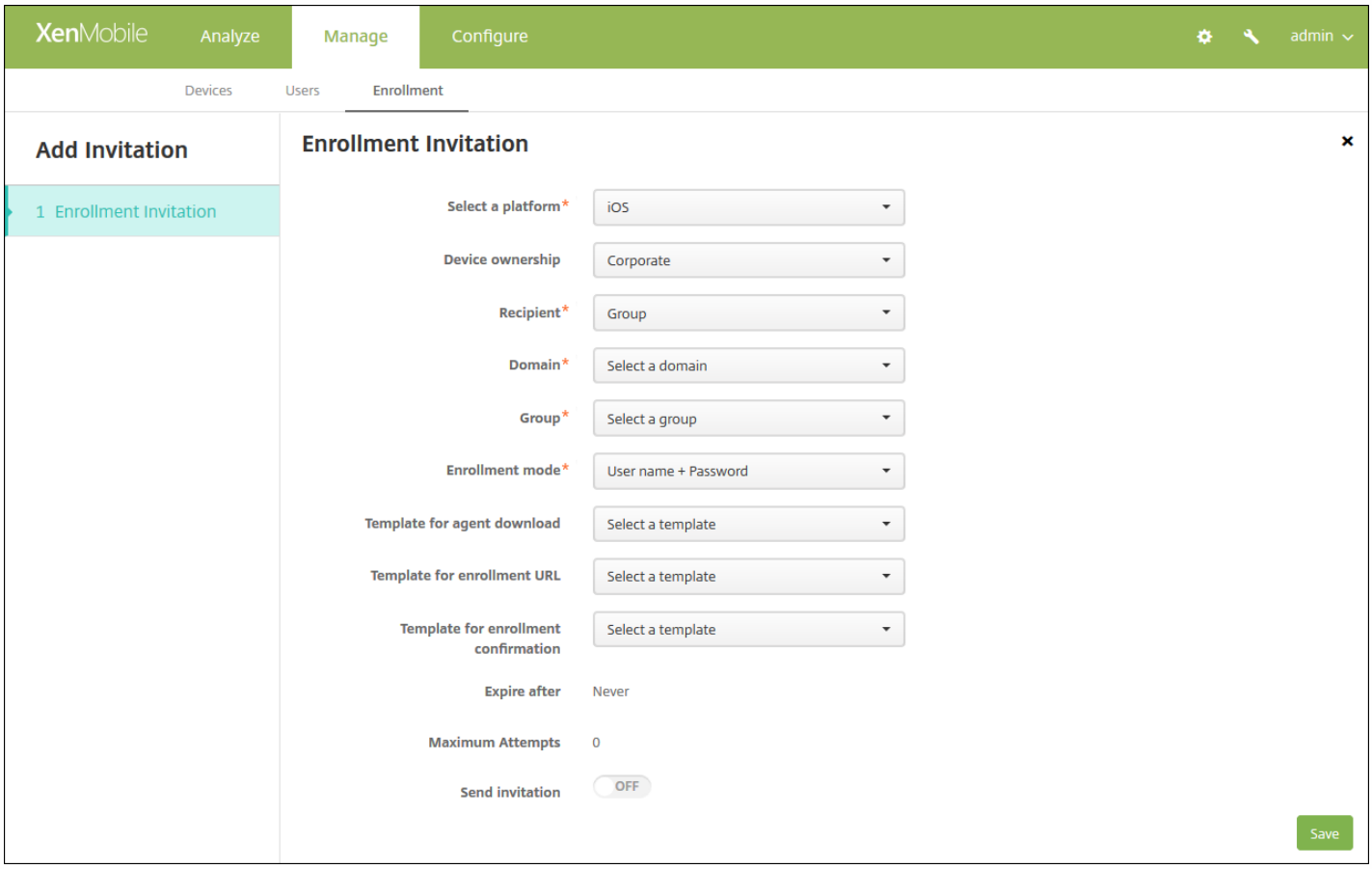
- **代理下载模板**：在列表中，单击用于注册邀请的模板。对此选项的选择基于平台类型。 例如，如果选择 **iOS** 平台，将显示 **iOS Download Link**（iOS 下载链接）选项。
- **注册 URL 模板**：在列表中，单击**注册邀请**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **注册确认模板**：在列表中，单击**注册确认**。
- **此时间后过期**：此字段在配置注册模式时设置，用于指出注册的过期时间。 有关配置注册模式的详细信息，请参阅配置注册模式。
- **最大尝试次数**：此字段在配置注册模式时设置，用于指出注册过程发生的最大次数。 有关配置注册模式的详细信息，请参阅配置注册模式。
- **发送邀请**：选择**开**以立即发送邀请，或单击**关**仅将邀请添加到**注册**页面上的表格中。

2. 如果已启用**发送邀请**，请单击**保存并发送**；否则，请单击**保存**。 邀请将显示在**注册**页面上的表格中。

向组发送注册邀请



1. 配置以下设置：

- **域**：在列表中，单击要从中选择组的域。
- **组**：在列表中，单击要接受邀请的组。
- **注册模式**：在列表中，单击希望组中的用户采用的注册方法。 默认值为 **用户名 + 密码**。 可用选项包括：
  - 高安全性
  - 邀请 URL
  - 邀请 URL + PIN
  - 邀请 URL + 密码
  - 双因素
  - 用户名 + PIN

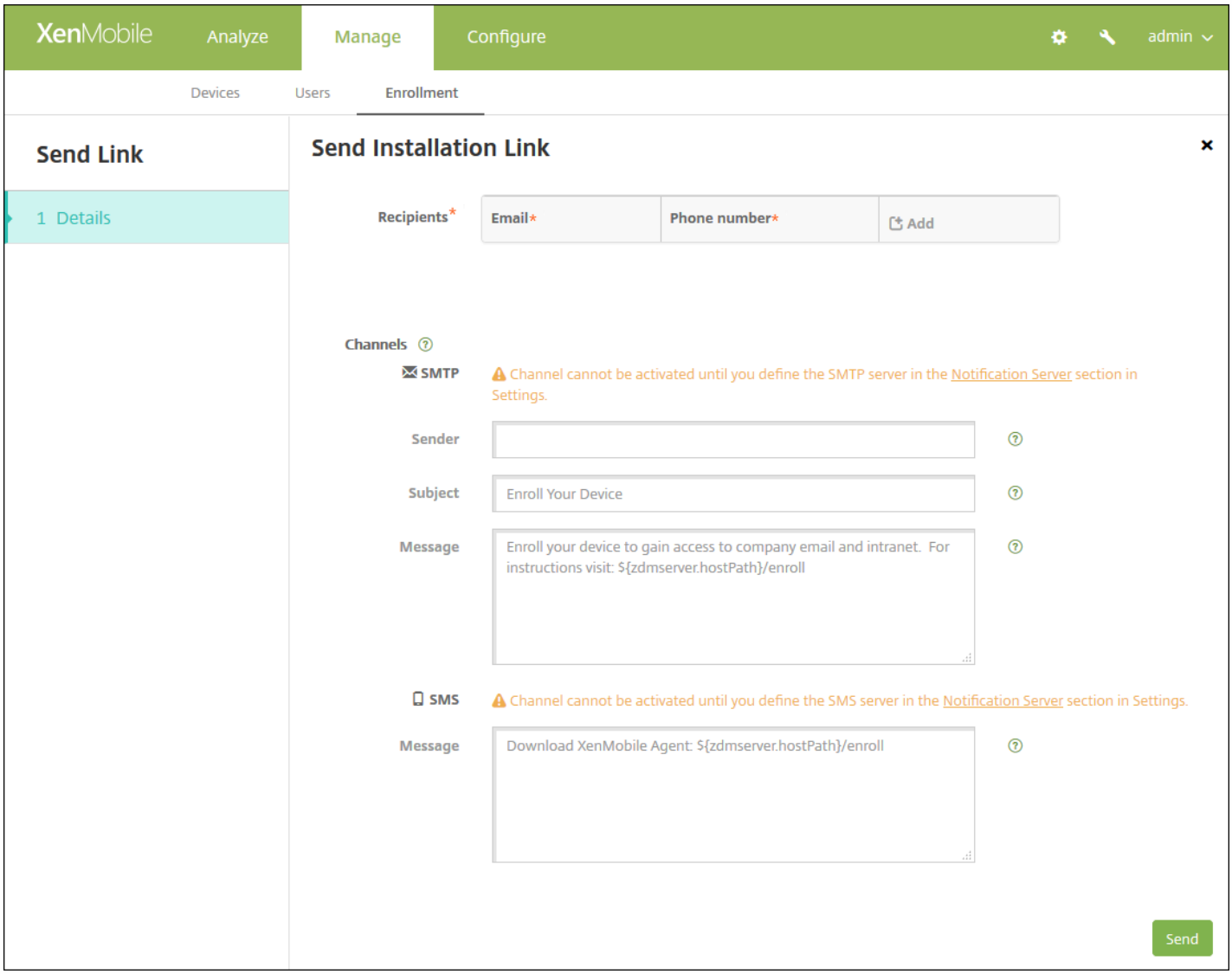
  注意：选择包含 PIN 的注册模式时，会显示**注册 PIN 模板**字段，您可以在此处单击**注册 PIN**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **代理下载模板**：在列表中，单击用于注册邀请的模板。对此选项的选择基于平台类型。 例如，如果选择 **iOS** 平台，将显示 **iOS Download Link**（iOS 下载链接）选项。
- **注册 URL 模板**：在列表中，单击**注册邀请**。
- **注册确认模板**：在列表中，单击**注册确认**。
- **此时间后过期**：此字段在配置注册模式时设置，用于指出注册的过期时间。 有关配置注册模式的详细信息，请参阅配置注册模式。
- **最大尝试次数**：此字段在配置注册模式时设置，用于指出注册过程发生的最大次数。 有关配置注册模式的详细信息，请参阅配置注册模式。
- **发送邀请**：选择**开**以立即发送邀请，或单击**关**仅将邀请添加到**注册**页面上的表格中。

2. 如果已启用**发送邀请**，请单击**保存并发送**；否则，请单击**保存**。 邀请将显示在**注册**页面上的表格中。

发送安装链接



您必须通过**设置**页面在通知服务器上配置通道（SMTP 或 SMS），才能发送注册安装链接。 有关详细信息，请参阅通知。

1. 配置以下设置：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **收件人**：对于您要添加的每个收件人，请单击**添加**并执行以下操作：
  - **电子邮件**：键入收件人的电子邮件地址。 此字段为必填字段。
  - **电话号码**：键入收件人的电话号码。 此字段为必填字段。
  - 单击**保存**。

    注意：要删除现有收件人，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有收件人，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **通道**：选择用于发送注册安装链接的通道。 可以通过 SMTP 或 SMS 发送通知。 在**通知服务器**的**设置**页面上配置服务器设置后，才能激活这些通道。 有关详细信息，请参阅通知。
  - **SMTP**：配置以下可选设置。 如果不在这些字段中键入任何内容，将使用为所选平台配置的通知模板中指定的默认值：
    - **发件人**。 键入可选发件人。
    - **主题**：键入消息的可选主题。 例如，“注册您的设备”。
    - **消息**：键入要发送给收件人的可选消息。 例如，“注册您的设备以获取组织应用程序和电子邮件的访问权限。”
  - **SMS**：配置以下设置。 如果不在此字段中键入任何内容，将使用为所选平台配置的通知模板中指定的默认值：
    - **消息**：键入要发送给收件人的消息。 对于基于 SMS 的通知，此为必填字段。

      注意：在北美，超过 160 个字符的 SMS 消息将通过多条消息发送。

2. 单击**发送**。

> ## 注意
>
> 如果您的环境使用 SAMAccountName，则当用户收到邀请并单击链接后，必须编辑用户名才能完成身份验证。 例如，用户需要从 SAMAccountName@domainname.com 中删除 domainname。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 中的共享设备

Aug 11, 2016

XenMobile 允许配置可由多个用户共享的设备。 例如，利用共享设备功能，医院的临床医生可以使用附近的任何设备访问应用程序和数据，而无需随身携带特定设备。 您可能还希望执法、零售和制造等领域的工作者转向使用共享设备，以降低装备成本。

关于共享设备的要点

MDM 模式

- 可在 iOS 和 Android 平板电脑和手机上使用。 XenMobile Enterprise 共享设备不支持基本 Device Enrollment Program (DEP) 注册。 必须使用经过授权的 DEP 在此模式下注册共享设备。
- 不支持客户端证书身份验证、Worx PIN、Touch ID 和用户熵。

MDM+MAM 模式

- 只能在 iOS 和 Android 平板电脑上使用。
- 仅在 XenMobile 10.3.x 服务器和客户端上支持使用。
- 不支持仅 MAM 模式。 设备必须在 MDM 下注册。
- 仅支持 WorxMail、WorxWeb 和 ShareFile 移动应用程序（版本 4.4）。 不支持 HDX 应用程序。
- 仅支持 Active Directory 用户；不支持本地用户和组
- 现有仅 MDM 共享设备要更新到 MDM+MAM 模式需要重新注册。
- 用户只能共享 Worx 应用程序以及 MDX 打包应用程序；他们无法共享设备上的本机应用程序。
- 在首次注册期间下载好 Worx 应用程序后，不必在新用户每次登录设备时重新下载。 新用户拿到设备后，只需登录即可使用。
- 在 Android 设备上，为了出于安全考虑隔离每个用户的数据，应在 XenMobile 控制台中将**Disallow rooted devices**（不允许已获得 root 权限的设备）策略设置为**开**。

注册共享设备的必备条件

您必须先执行以下操作，才能注册共享设备：

- 创建共享设备注册用户角色。 请参阅使用 RBAC 配置角色。
- 创建共享设备用户。 请参阅在 XenMobile 中添加、编辑或删除本地用户。
- 创建包含要应用于共享设备注册用户的基本策略、应用程序和操作的交付组。 请参阅管理交付组。

使用 MDM+MAM 模式的必备条件

1. 创建一个名称类似于 **Shared Device Enrollers** 的 Active Directory 组。
2. 将要注册共享设备的 Active Directory 用户添加到此组。 如果要使用一个专用于注册共享设备的新帐户，请创建新的 Active Directory 用户（例如 **sdenroll**），并将该用户添加到 Active Directory 组。

共享设备要求

© 1999-2017 Citrix Systems, Inc. All rights reserved.

为提供最佳用户体验，包括无提示安装和应用程序删除，Citrix 建议在下列平台上配置共享设备：

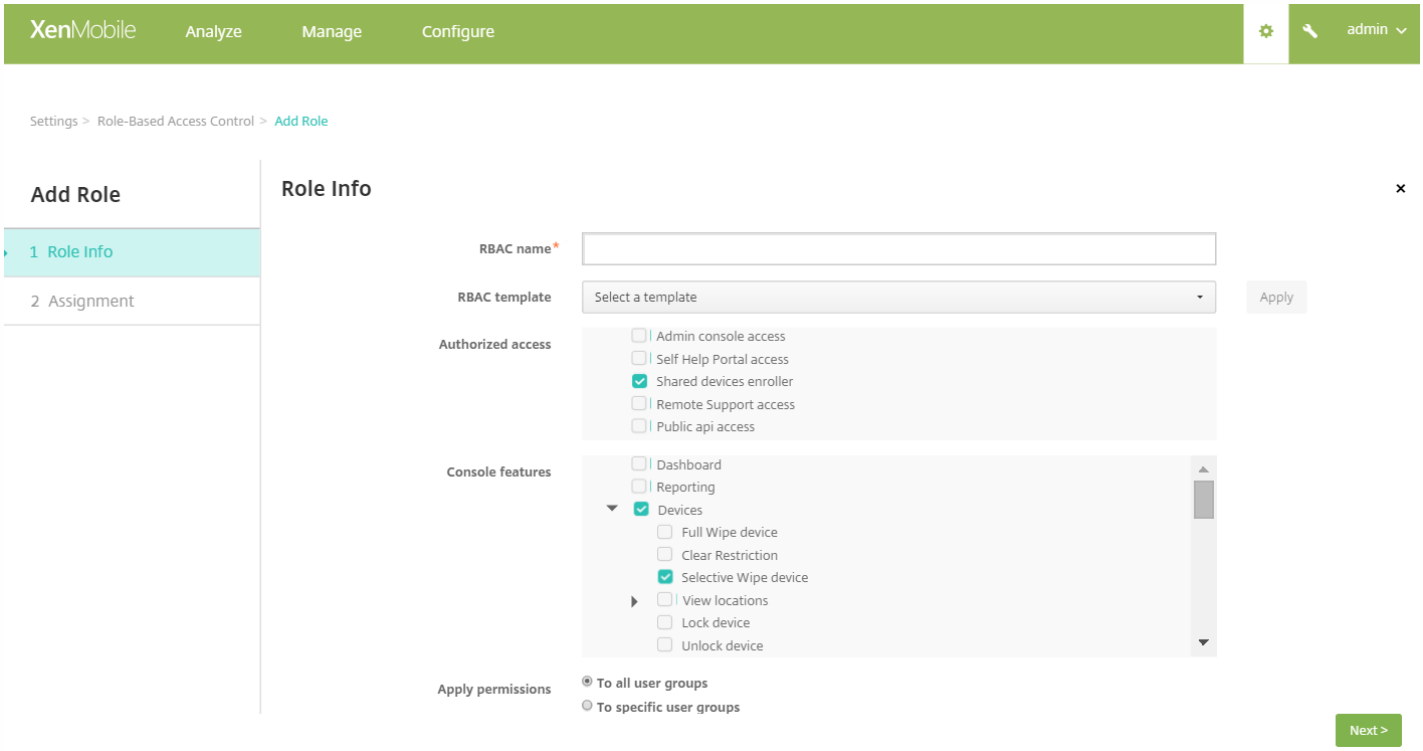
- iOS 9
- iOS 8
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x（仅 MDM 模式）

配置共享设备

按照以下步骤配置共享设备。

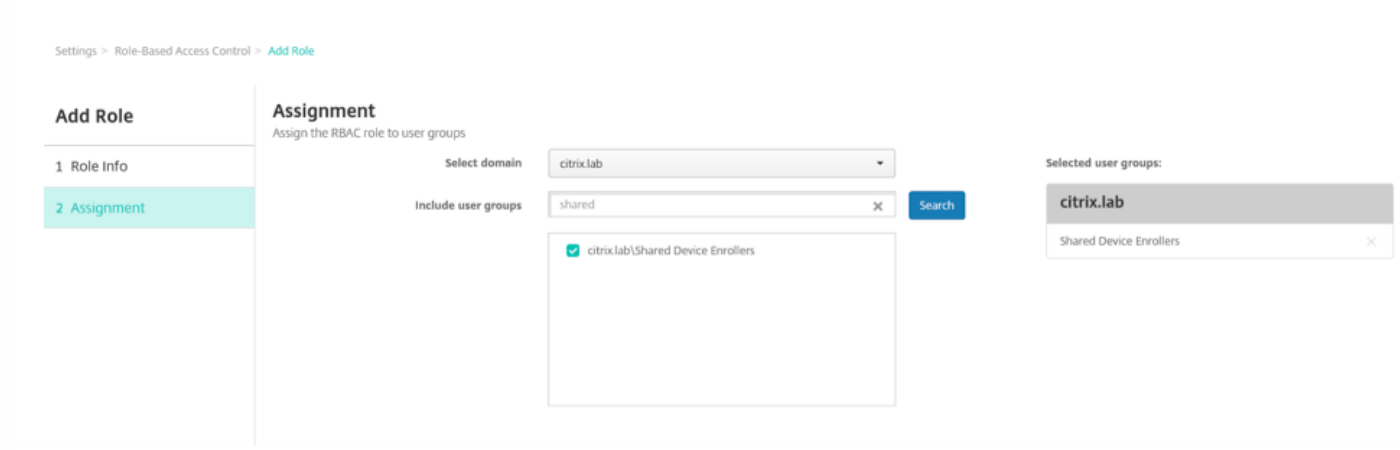
1. 从 XenMobile 控制台，单击右上角的齿轮图标。 此时将显示设置页面。
2. 单击**基于角色的访问控制**，然后单击**添加**。 此时会显示**添加角色**屏幕。
3. 创建一个名为**共享设备注册用户**的共享设备注册用户角色，并在**授权访问**下设置**共享设备注册人员**权限。 请务必展开**控制台功能**中的**设备**，然后选择**选择性擦除设备**。 此设置可确保在取消设备注册后，使用共享设备注册人员帐户置备的应用程序和策略通过 Worx Home 被删除。

   请保留**应用权限**的默认设置**至所有用户组**，或者使用**至特定用户组**向特定 Active Directory 用户组分配权限。

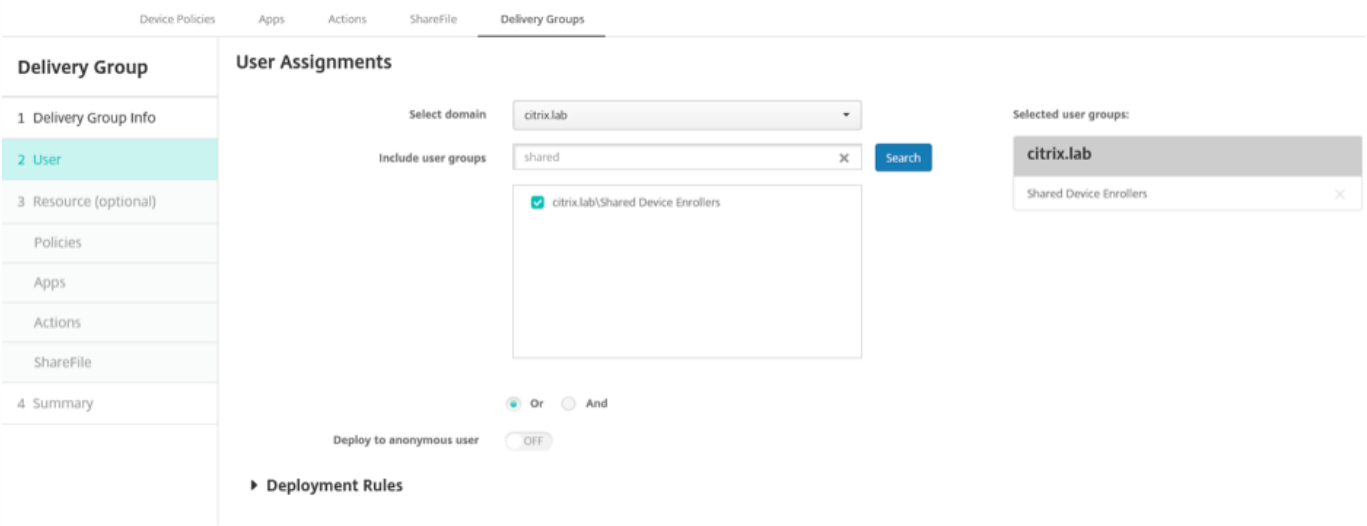


单击**下一步**转至**分配**屏幕。 将刚创建的共享设备注册角色分配给在步骤 1 中的“必备项”下为共享设备注册用户创建的 Active Directory 组。 在下图中，**citrix.lab** 是 Active Directory 域，而**共享设备注册人员**是 Active Directory 组。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 创建一个交付组以包含要在用户未登录时应用于设备的基本策略、应用程序和操作，然后将该交付组与共享设备注册用户 Active Directory 组相关联。



5. 在共享设备上安装 Worx Home，然后使用共享设备注册用户帐户将其注册到 XenMobile 中。 现在即可通过 XenMobile 控制台查看并管理设备。 有关详细信息，请参阅注册设备。

6. 要为已验证身份的用户应用不同的策略或提供额外的应用程序，必须创建与这些用户关联的交付组，并将该交付组仅部署到共享设备。 在创建交付组时，请配置相应的部署规则，以确保将软件包部署到共享设备。 有关详细信息，请参阅配置部署规则。

7. 要停止共享设备，请执行选择性擦除，从设备中删除共享设备注册用户帐户以及部署到该设备的所有应用程序和策略。

共享设备用户体验

MDM 模式

用户只会看到他们可用的资源，而且在每个共享设备上都能获得同样的使用体验。 共享设备注册策略和应用程序会始终保留在设备上。 当未在共享设备中注册的用户登录到 Worx Home 时，该用户的策略和应用程序将部署到设备中。 在用户注销时，与

© 1999-2017 Citrix Systems, Inc. All rights reserved.

共享设备注册不同的策略和应用程序会被删除，而共享设备注册资源则保持不变。

MDM+MAM 模式

WorxMail 和 WorxWeb 将在由共享设备注册用户注册后部署到设备中。 用户数据会安全地保留在设备上。 当其他用户登录到 WorxMail 或 WorxWeb 时，系统不会将这些数据公开给这些用户。

一次只能有一个用户登录到 Worx Home。 上一个用户必须注销，下一个用户才能登录。 出于安全原因，Worx Home 不在共享设备上存储用户凭据，因此用户必须在每次登录时输入其凭据。 为确保新用户不能访问为前面的用户提供的资源，Worx Home 在删除与以前用户相关的策略、应用程序和数据时不允许新用户登录。

共享设备注册不会更改应用程序升级过程。 您可以照常将升级推送给共享设备的用户，而共享设备的用户可以直接在其设备上升级应用程序。

推荐的 WorxMail 策略

- 要确保 WorxMail 获得最佳性能，请根据要共享设备的用户数设置**Max sync period**（最长同步期限）。 不建议允许无限同步。

共享设备的用户数量	建议的最长同步期限
21 至 25	1 周或更短
6 至 20	2 周或更短
5 或更少	1 个月或更短

- 阻止**启用联系人导出**以避免向共享设备的其他用户显示用户的联系人。
- 在 iOS 设备上，只能为每个用户设定以下设置。 所有其他设置在共享设备的用户之间将为通用设置：

  通知
  签名
  外出
  同步邮件周期
  S/MIME
  检查拼写

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中使用 Android for Work 管理设备

Oct 21, 2016

Android for Work 是运行 Android 5.0 及更高版本的 Android 设备上的一个安全工作区，可以将企业帐户、应用程序和数据与个人帐户、应用程序和数据隔离开。 在 XenMobile 中，通过让用户组合使用硬件加密和您部署的策略，在其设备上创建单独的工作配置文件，可以安全地分隔开设备上的企业区域和个人区域，实现同时管理自带设备 (BYOD) 和公司拥有的 Android 设备。 您可以在不影响用户个人区域的情况下，远程管理所有公司策略、应用程序和数据，并可以擦除这些策略、应用程序和数据。 有关支持的 Android 设备的详细信息，请参阅 Google 的设备页面。

在 XenMobile 中，还可以通过让用户下载和安装 Android for Work 应用程序来管理运行 Android 4.0 - 4.4 的设备，这样可提供与运行 Android 5.0 及更高版本的设备中内置的安全工作区相同的功能。

使用 Google Play for Work 可添加、购买和审批应用程序，以便部署到设备的 Android for Work 工作区。 您可以使用 Google Play for Work 来部署您的私有 Android 应用程序，以及公共和第三方应用程序。 为 Android for Work 向 XenMobile 添加付费公共应用商店应用程序时，可以查看批量购买许可状态，即可用的许可证总数以及当前正在使用的许可证数量，以及使用这些许可证的每个用户的电子邮件地址。 有关详细信息，请参阅向 XenMobile 中添加公共应用商店应用程序。

Android for Work 的要求：

- 可公开访问的域
- Google 管理帐户
- 运行 Android 5.0+ Lollipop 并具有托管配置文件支持的设备，或运行 Android 4.0 - 4.4（Ice Cream Sandwich、Jelly Bean 和 KitKat）并具有 Android for Work 应用程序的设备
- 在用户的个人配置文件中安装了 Google Play 的 Google 帐户
- 用户设备上设置的工作配置文件

必须执行以下操作，才能设置 Android for Work 应用程序限制：

- 在 Google 上完成 Android for Work 设置任务。
- 创建一组 Google Play 凭据。
- 配置 Android for Work 服务器设置。
- 至少创建一个 Android for Work 设备策略。
- 在 Google Play for Work 应用商店中添加、购买和审批 Android for Work 应用程序。

管理 Android for Work 时可以使用以下链接：

- Google Admin 控制台：https://admin.google.com/AdminHome
- Play for Work 管理控制台：https://play.google.com/work/apps
- 用于专有通道和自托管应用程序的 Play 发布：https://play.google.com/apps/publish
- 用于创建服务帐户的 Google Developer Console：https://console.developers.google.com

Android for Work 必备条件

必须先执行以下操作，才能在 XenMobile 中管理 Android for Work：

- 创建 Android for Work 帐户。
- 设置一个服务帐户。
- 下载 Android for Work 证书
- 启用并授权 Google Admin SDK 和 MDM API。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 授权服务帐户使用目录和 Google Play。
- 获取一个绑定的令牌。

以下部分将分别介绍如何执行这些任务。 完成这些任务后，可以创建一组 Google Play 凭据，配置 Android for Work 设置，并在 XenMobile 中管理 Android for Work 应用程序。

> **警告**
>
> 存在阻止您使用 XenMobile 控制台启用 Android for Work 的已知第三方问题。 有关该问题以及如何配置服务器属性作为解决方法的详细信息，请参阅 XenMobile 服务器 10.3 已知问题中的问题 #615118。

创建 Android for Work 帐户

必须满足以下必备条件，才可以设置 Android for Work 帐户：

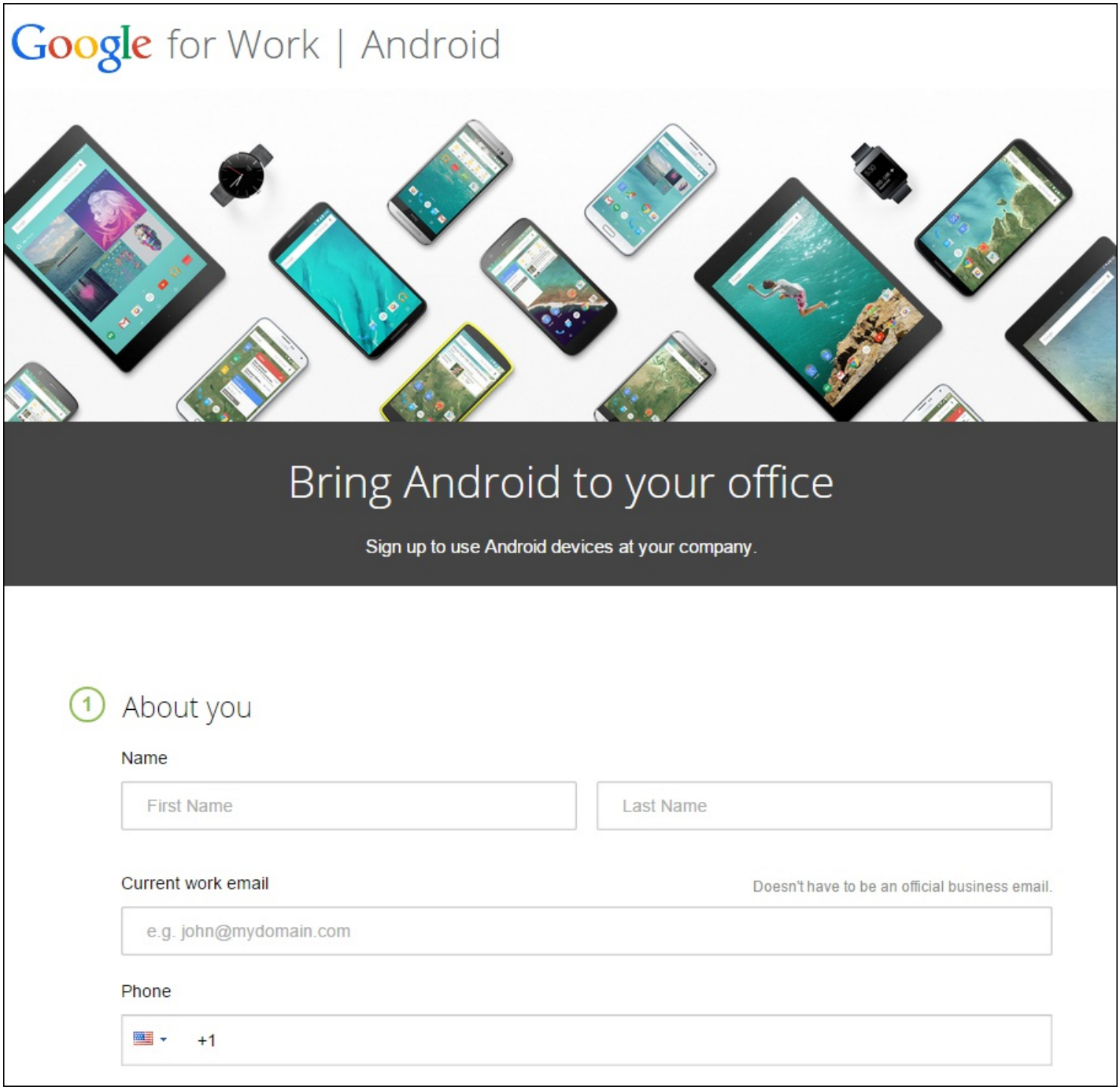
- 必须拥有域名；例如 example.com。
- 必须允许 Google 验证您是否拥有该域。
- 必须通过 Enterprise Mobility Management (EMM) 提供程序（XenMobile 10.1 或更高版本）启用和管理 Android for Work。

如果已向 Google 验证您的域名，可以跳至此步骤：设置 Android for Work 服务帐户并下载 Android for Work 证书。

1. 导航到 https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK。

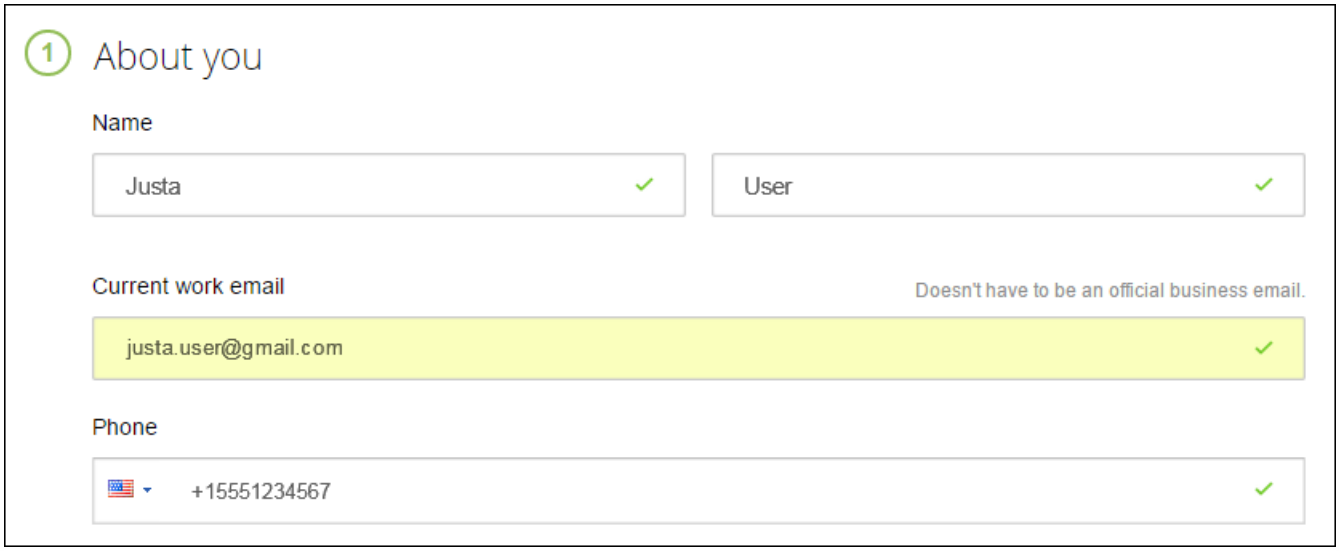
此时将转到以下页面，您可以在此页面上输入管理员信息和公司信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

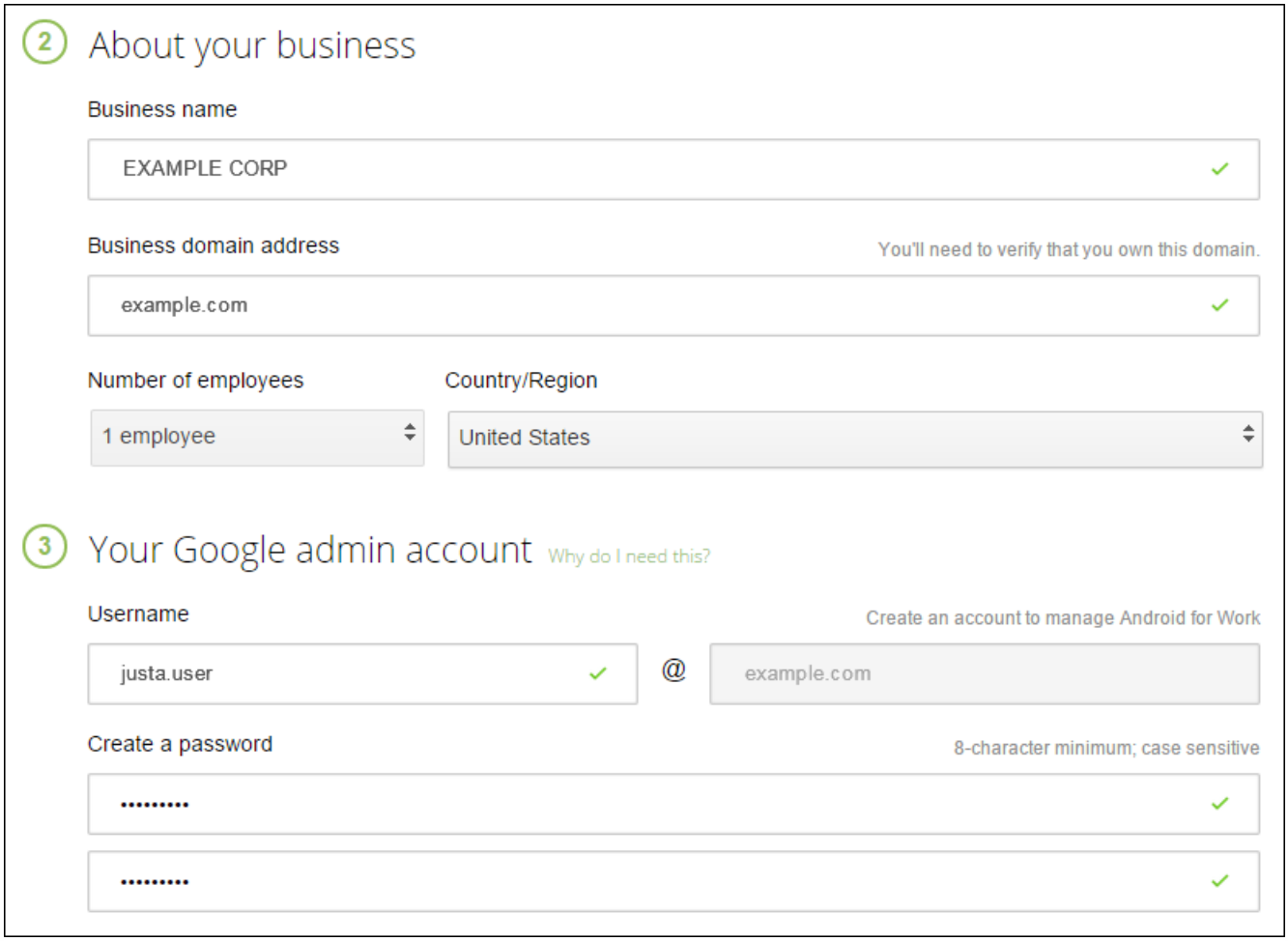


2. 输入管理员用户信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

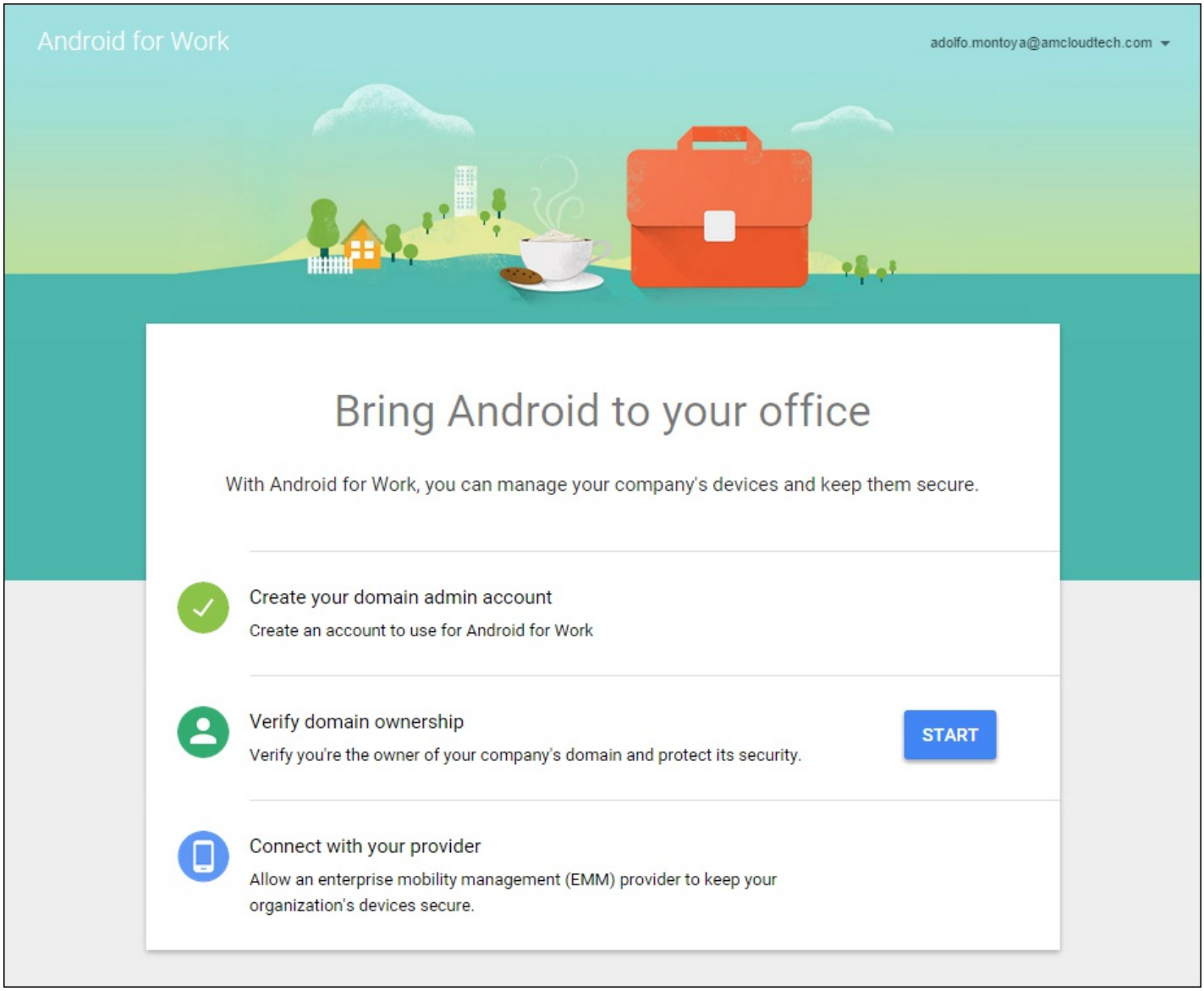


3. 输入公司信息，以及管理帐户信息。



此过程中的第一个步骤已完成，请继续查看下面的页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



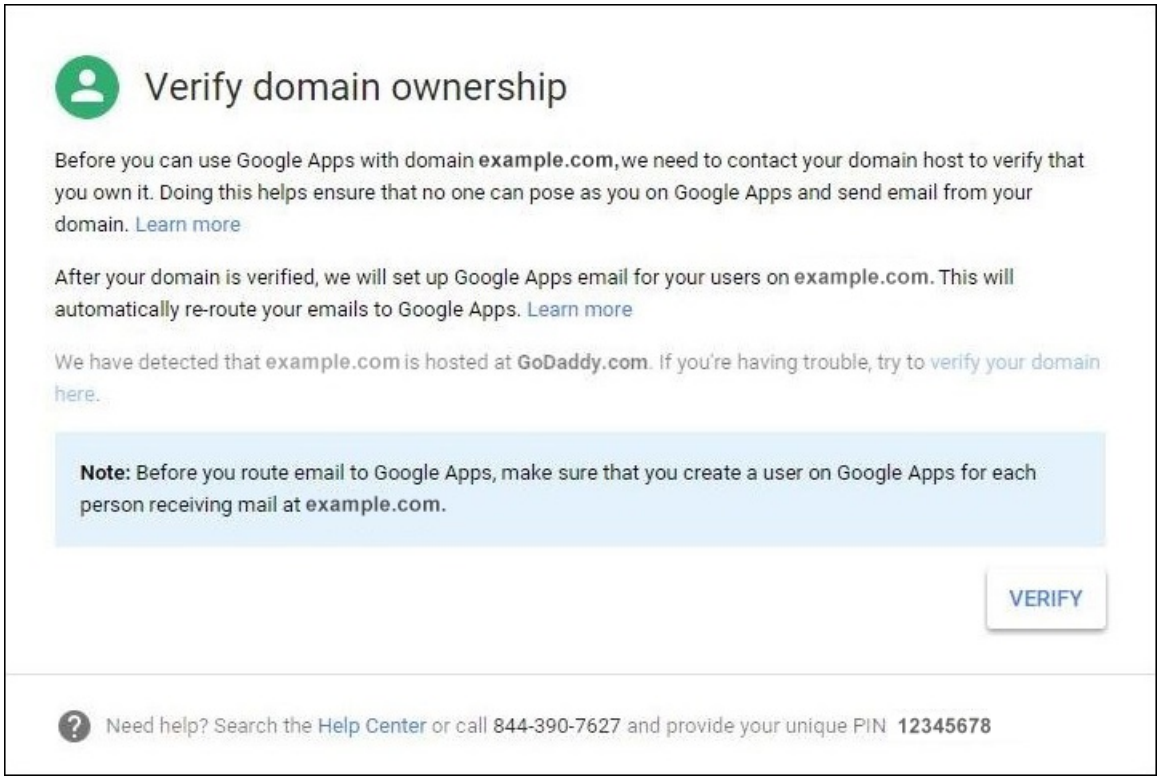
验证域所有权

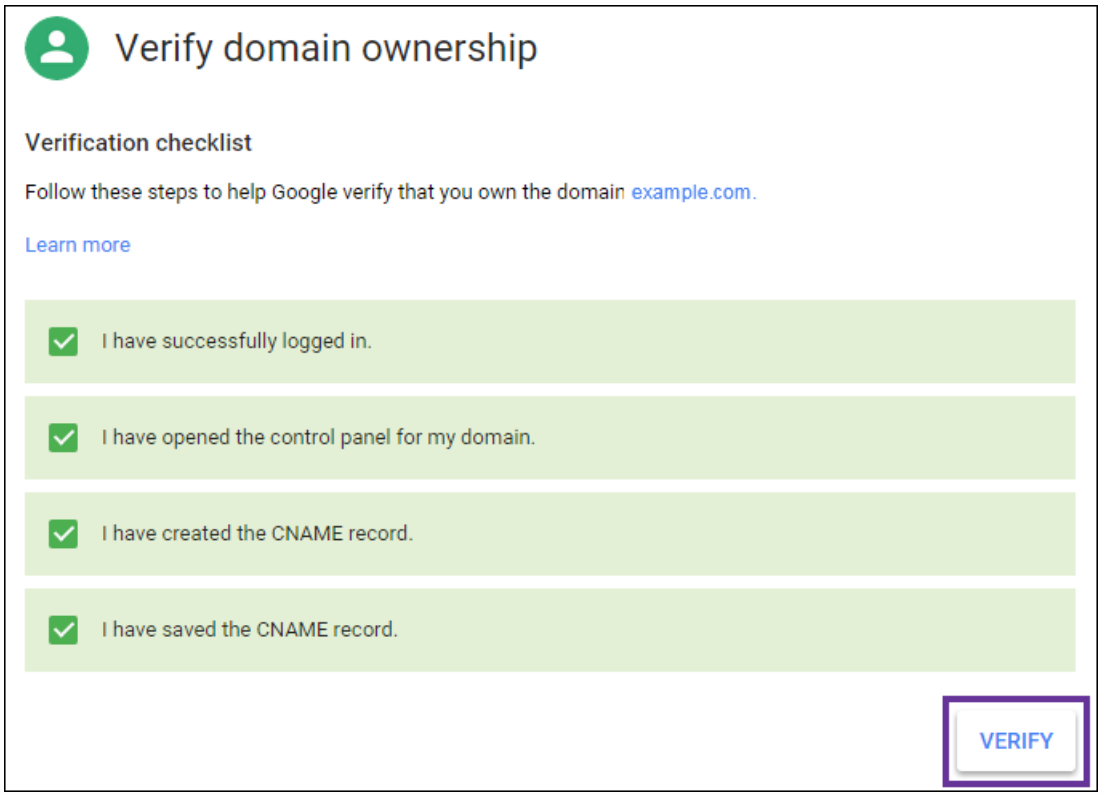
您现在必须允许 Google 验证您的域。 可以通过三种方法验证您的域：将 TXT 或 CNAME 记录添加到域主机的 Web 站点，将 HTML 文件上载到域的 Web 服务器，或者向主页中添加一个 标记。 Google 建议使用第一种方法。 本文中不包括验证域所有权的步骤，但您可以从以下网址找到所需的信息：https://support.google.com/a/answer/6095407/。

1. 单击 **Start**（开始）开始验证您的域。 此时将显示 **Verify domain ownership**（验证域所有权）页面。 请按照此页面上显示的说明验证您的域。

2. 操作完成后，单击 **Verify**（验证）。

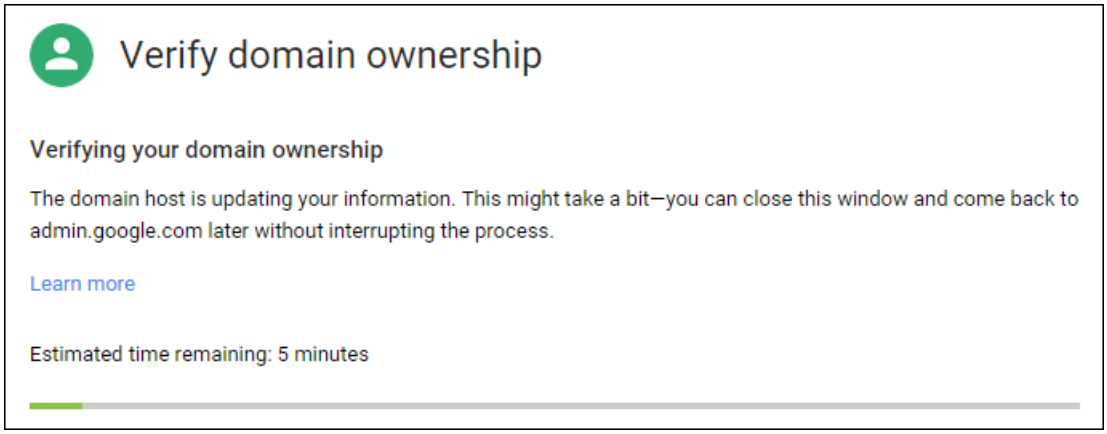
© 1999-2017 Citrix Systems, Inc. All rights reserved.



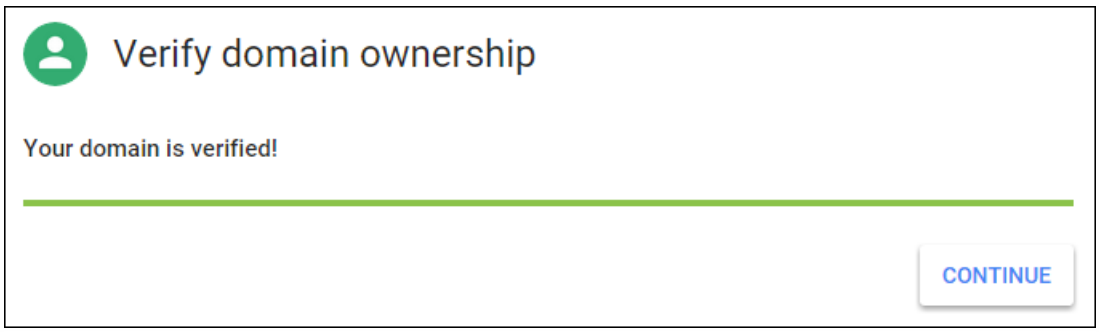


3. Google 验证您的域所有权。

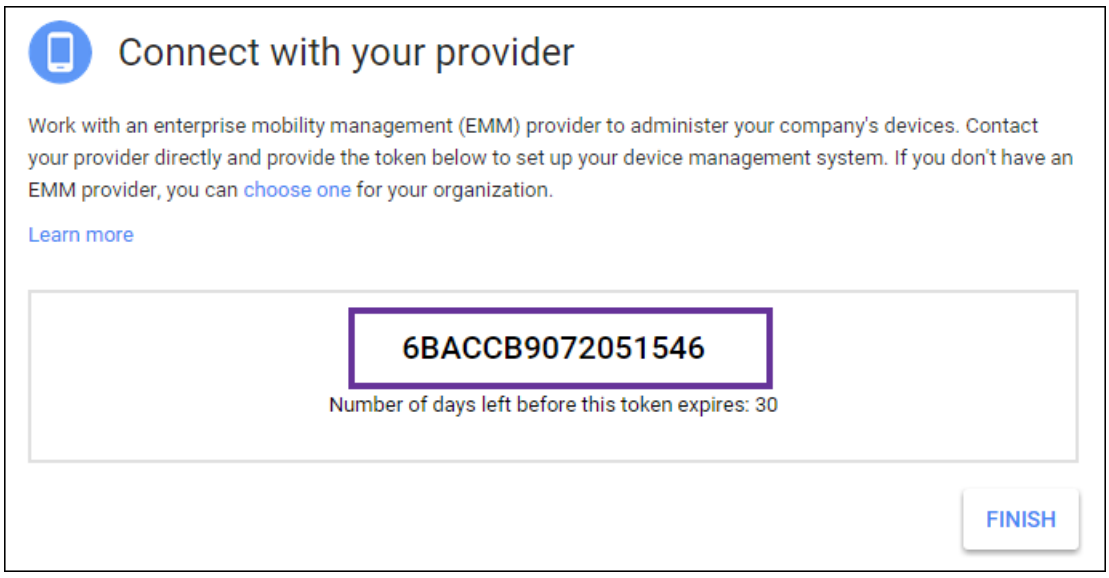
© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 成功验证后您将看到以下页面。 单击 **Continue**（继续）。

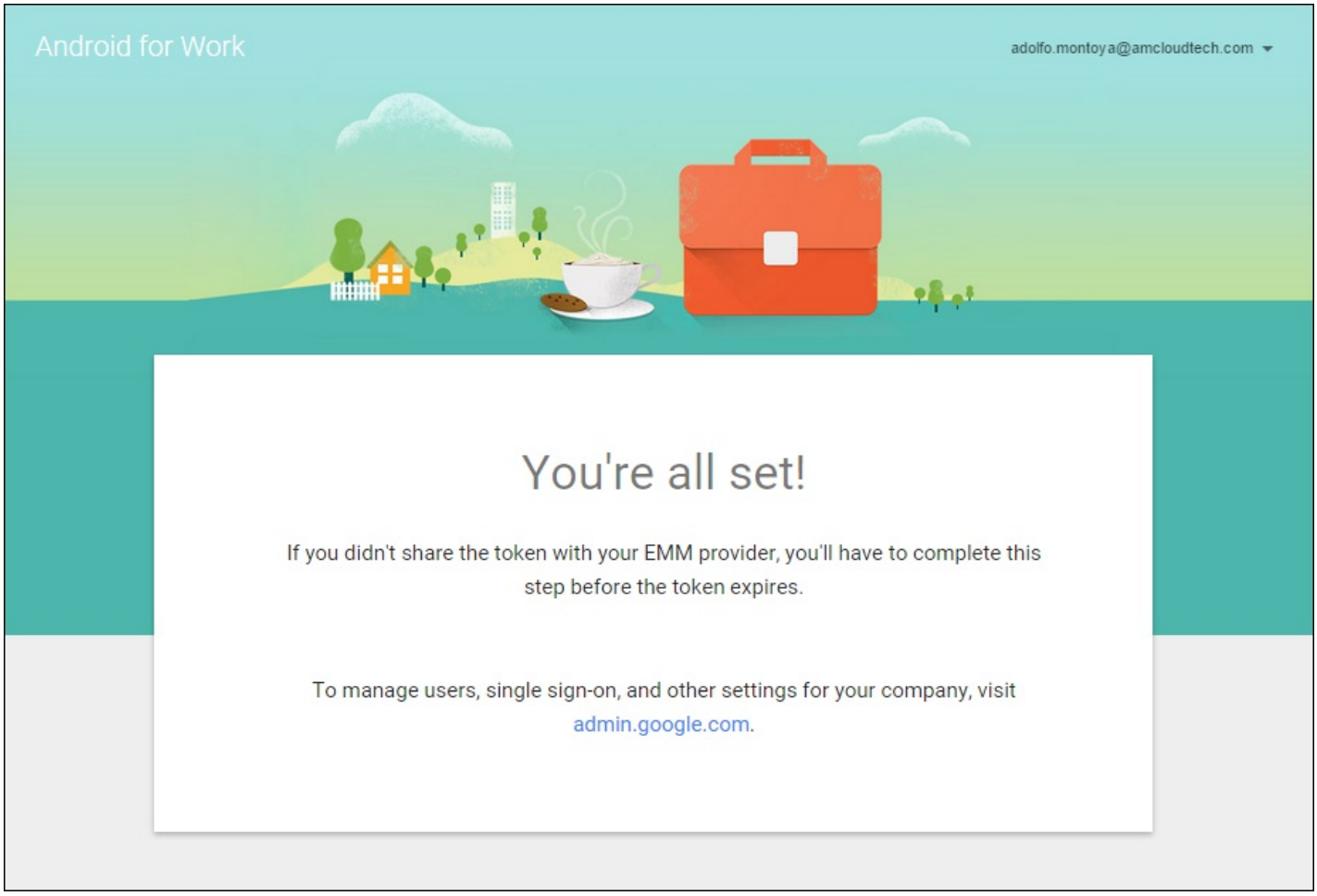


5. Google 创建一个需要向 Citrix 提供的 EMM 绑定令牌，您在配置 Android for Work 设置时需要使用该令牌。 复制并保存该令牌；稍后的设置过程中需要使用该令牌。



6. 单击 **Finish**（完成）以完成 Android for Work 设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



创建 Android for Work 服务帐户后，可以登录 Google Admin 控制台，以管理 Android for Work 移动性管理设置。

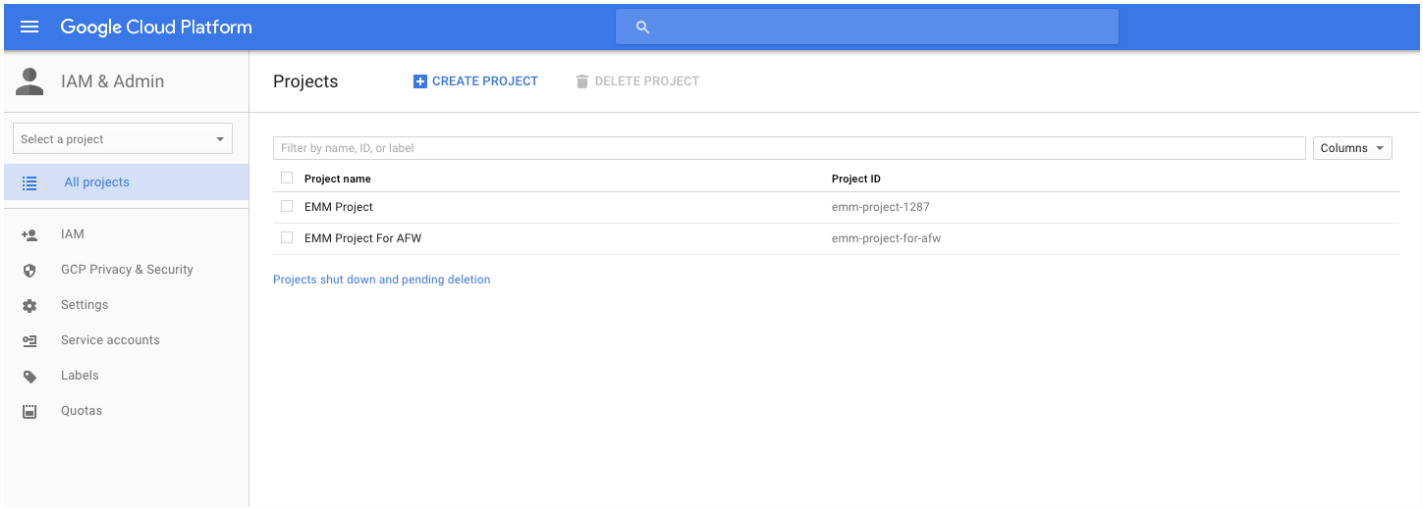
设置 Android for Work 服务帐户并下载 Android for Work 证书

要允许 XenMobile 联系 Google Play 和 Directory 服务，必须使用 Google 的开发人员项目门户创建新的服务帐户。 此服务帐户用于 XenMobile 和 Android for Work Google 服务之间的服务器至服务器通信。 有关所使用的身份验证协议的详细信息，请参阅 https://developers.google.com/identity/protocols/OAuth2ServiceAccount。

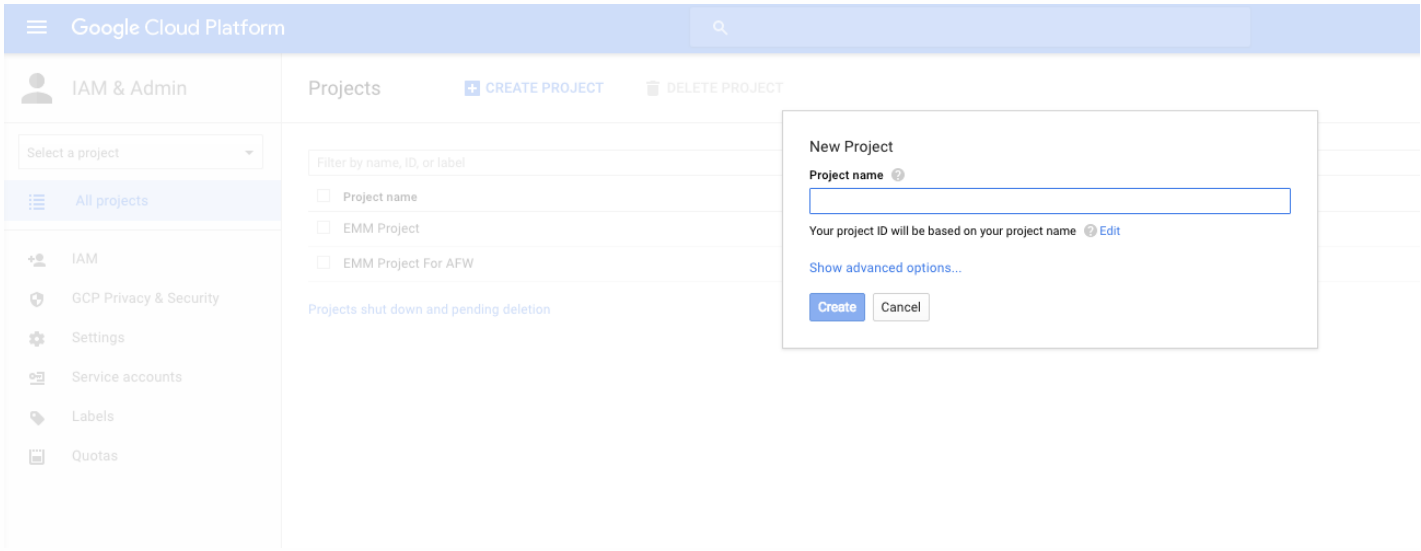
1. 在 Web 浏览器中，转至 https://console.cloud.google.com/project 并使用您的 Google 管理员凭据登录。

2. 在**项目**列表中，单击**创建项目**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

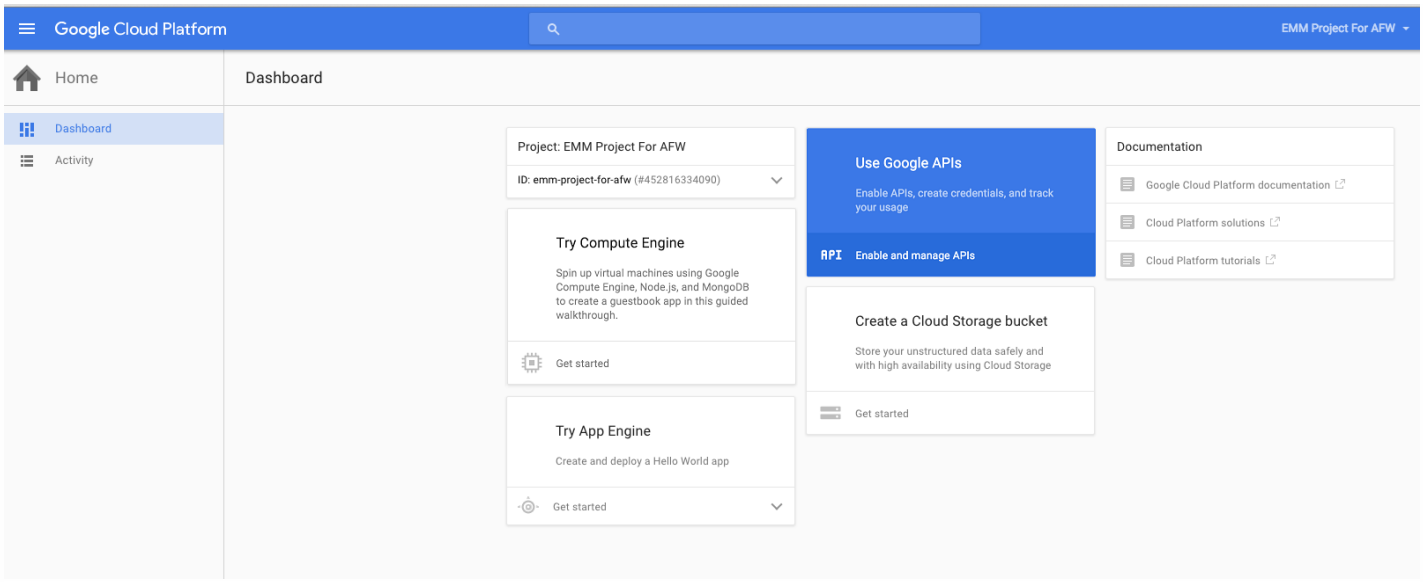


3. 在**项目名称**中，输入项目的名称。

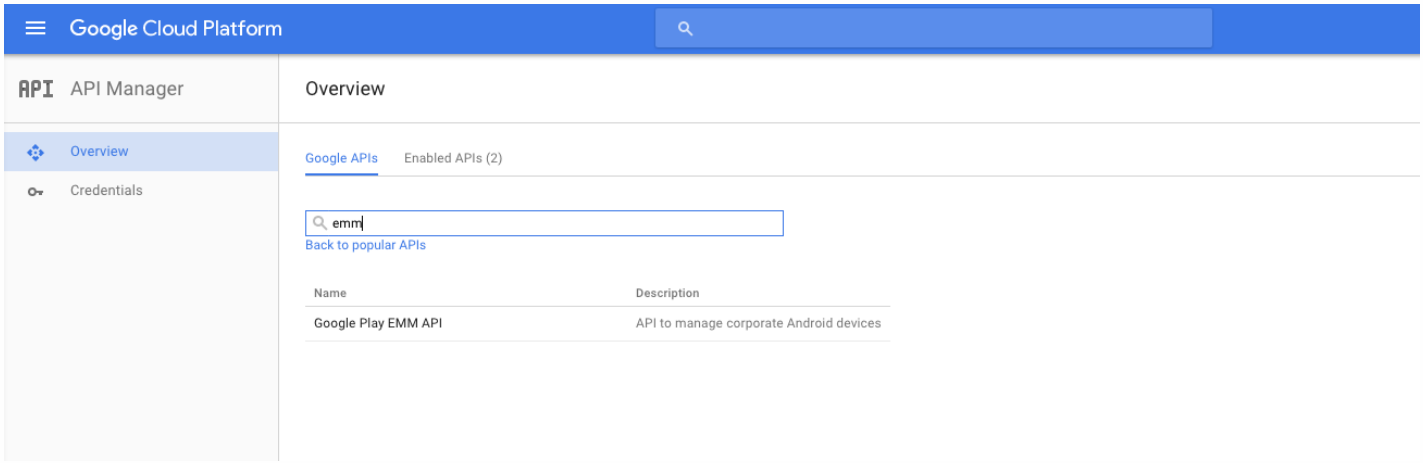


4. 在“仪表板”上，单击**使用 Google API**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

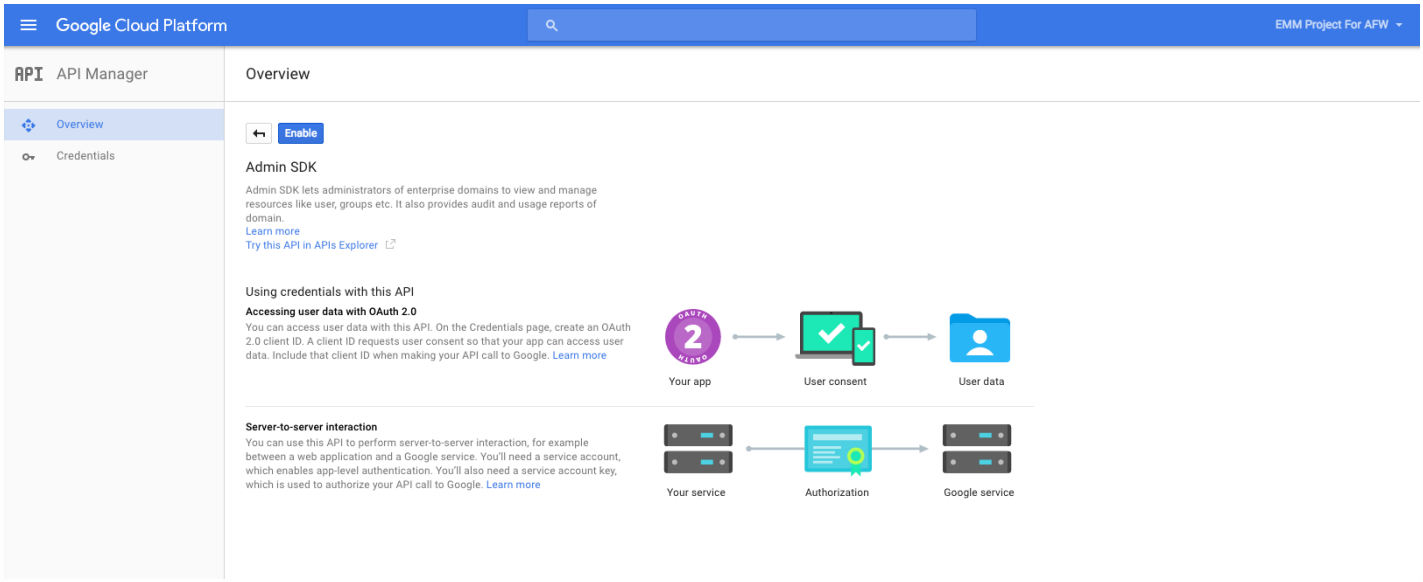


5. 在“Google API”页面上，在**搜索**中输入 **EMM**，然后单击搜索结果。

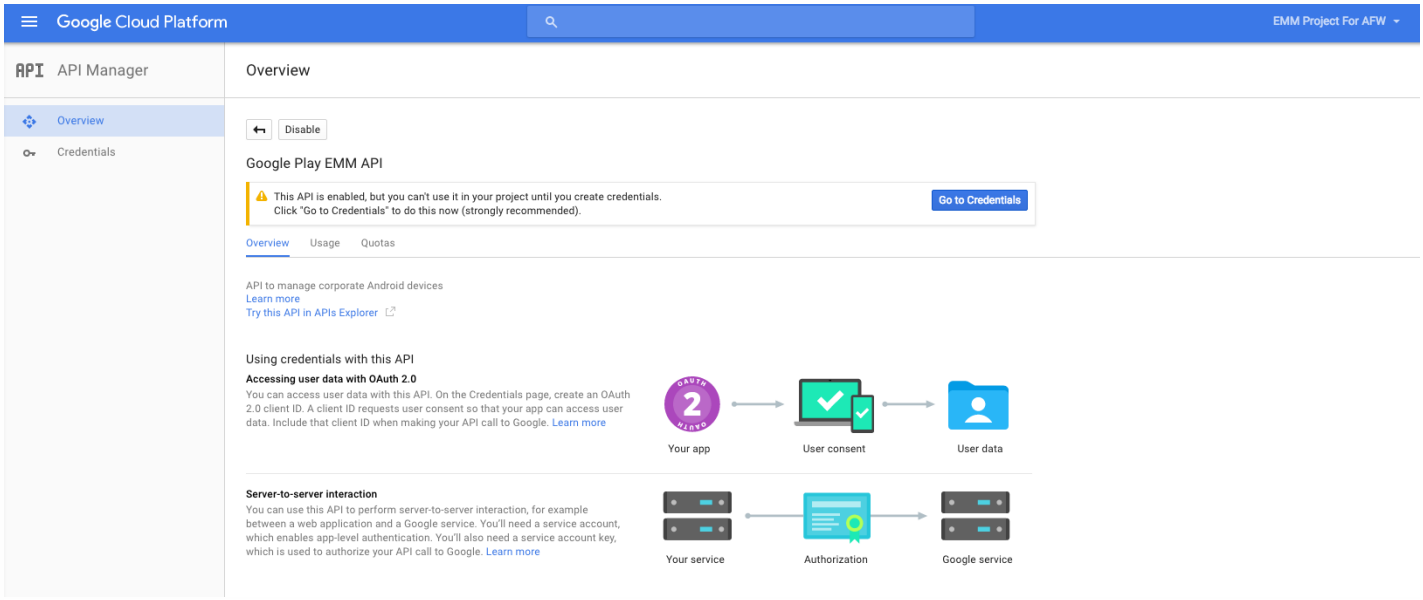


6. 在“Overview”（概览）页面上，单击 **Enable**（启用）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

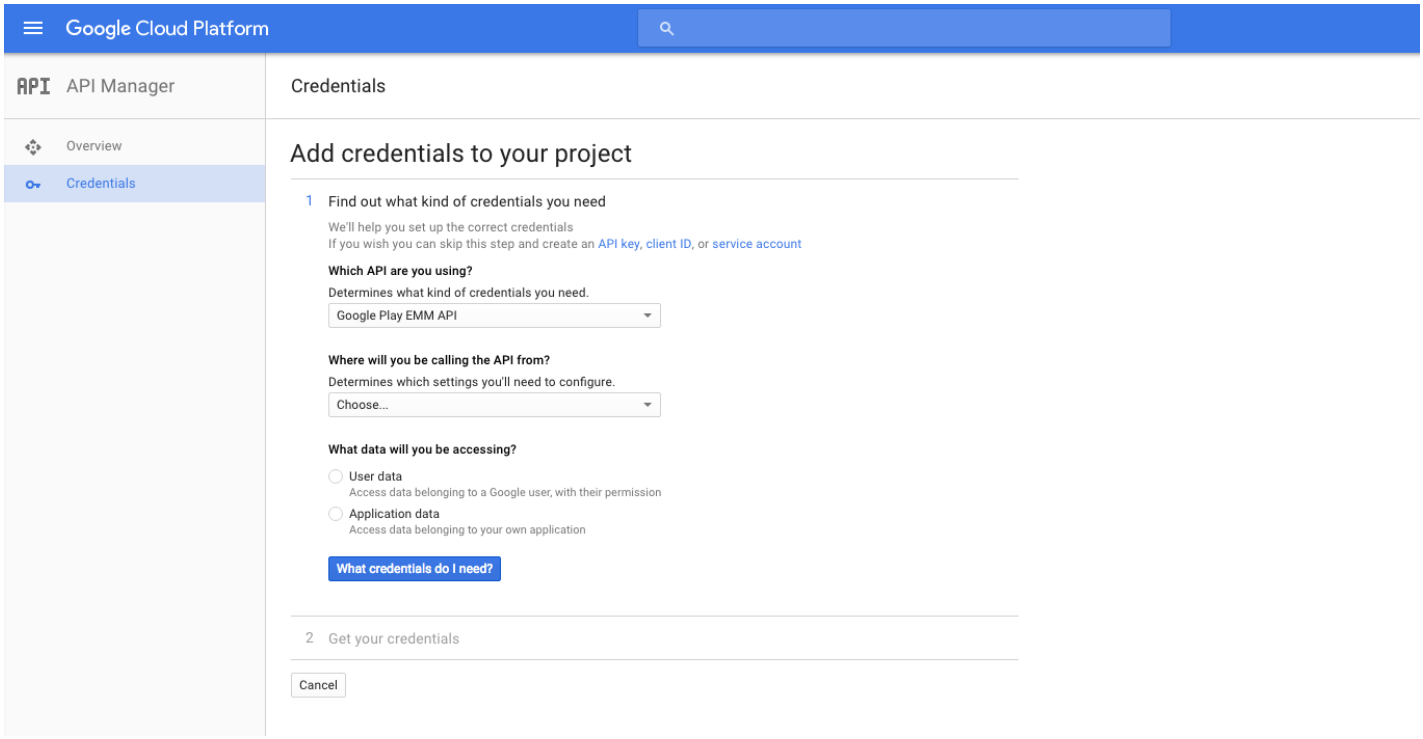


7. 在 **Google Play EMM API** 旁边，单击 **Go to Credentials**（转至凭据）。

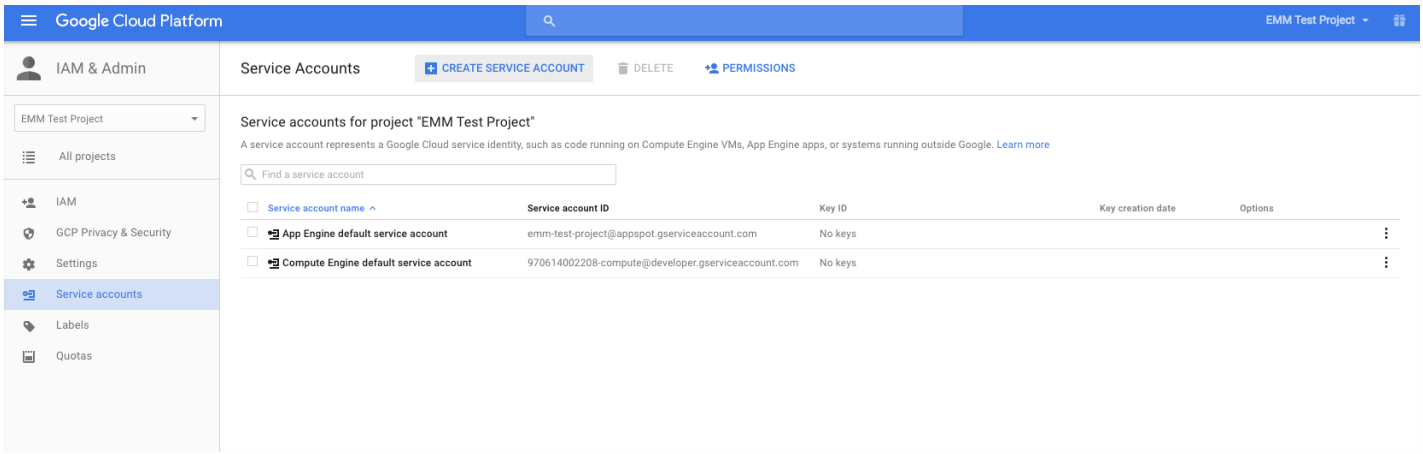


8. 在 **Add credentials to our project**（向我们的项目中添加凭据）列表中，在步骤 1 中单击 **service account**（服务帐户）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

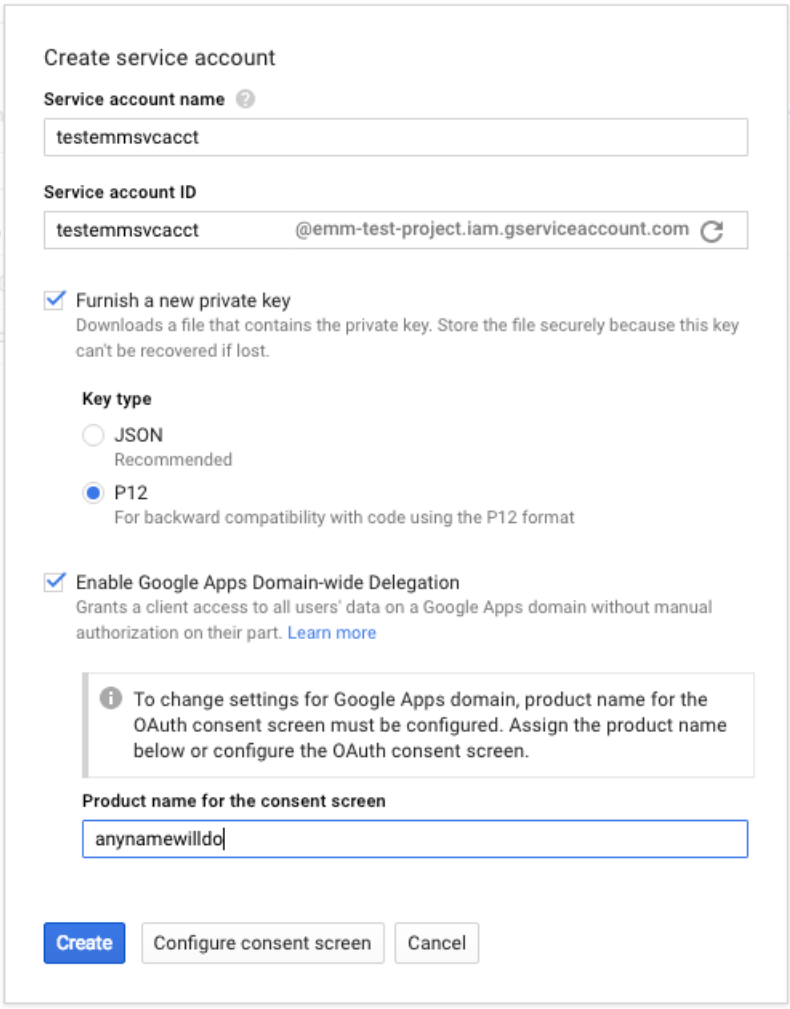


9. 在 **Service Accounts**（服务帐户）页面上，单击 **Create Service Account**（创建服务帐户）。



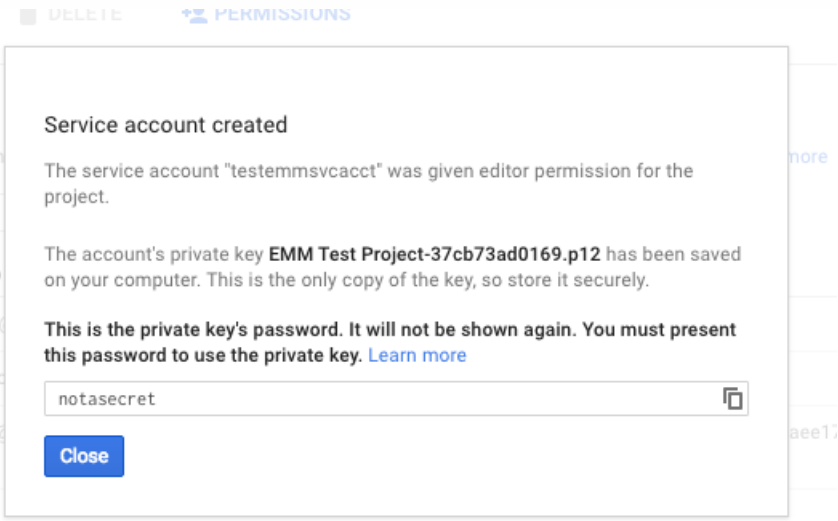
10. 在 **Create service account key**（创建服务帐户密钥）中，命名该帐户，选中 **Furnish a new private key**（提供新密钥）复选框，单击 **P12**，选中 **Enable Google Apps Domain-wide Delegation** （启用 Google 应用程序域范围内的委派）复选框，然后单击 **Create**（创建）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



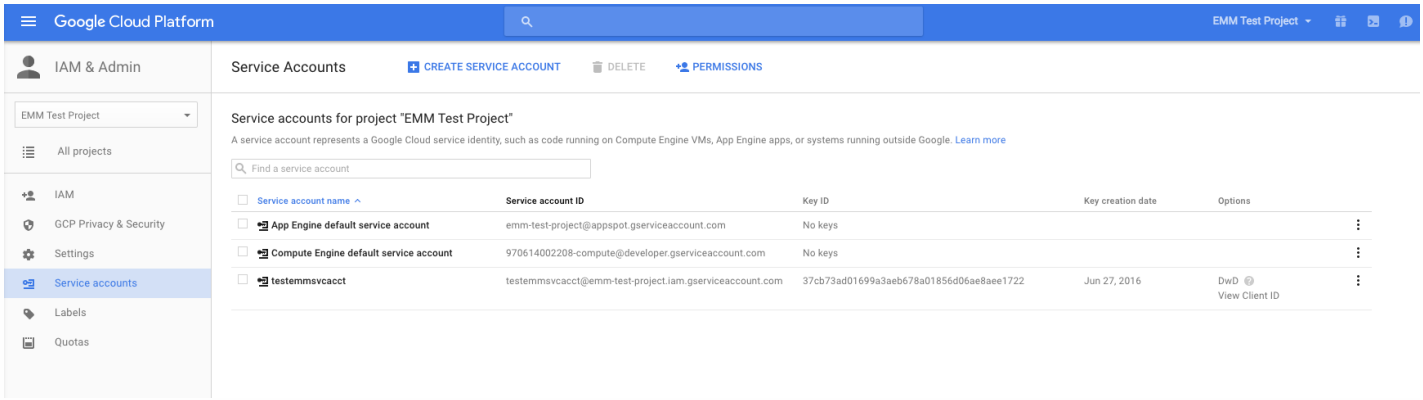
证书（P12 文件）将下载到您的计算机。 请务必将该证书保存到一个安全的位置。

11. 在 **Service account created**（已创建服务帐户）确认屏幕上，单击 **Close**（关闭）。

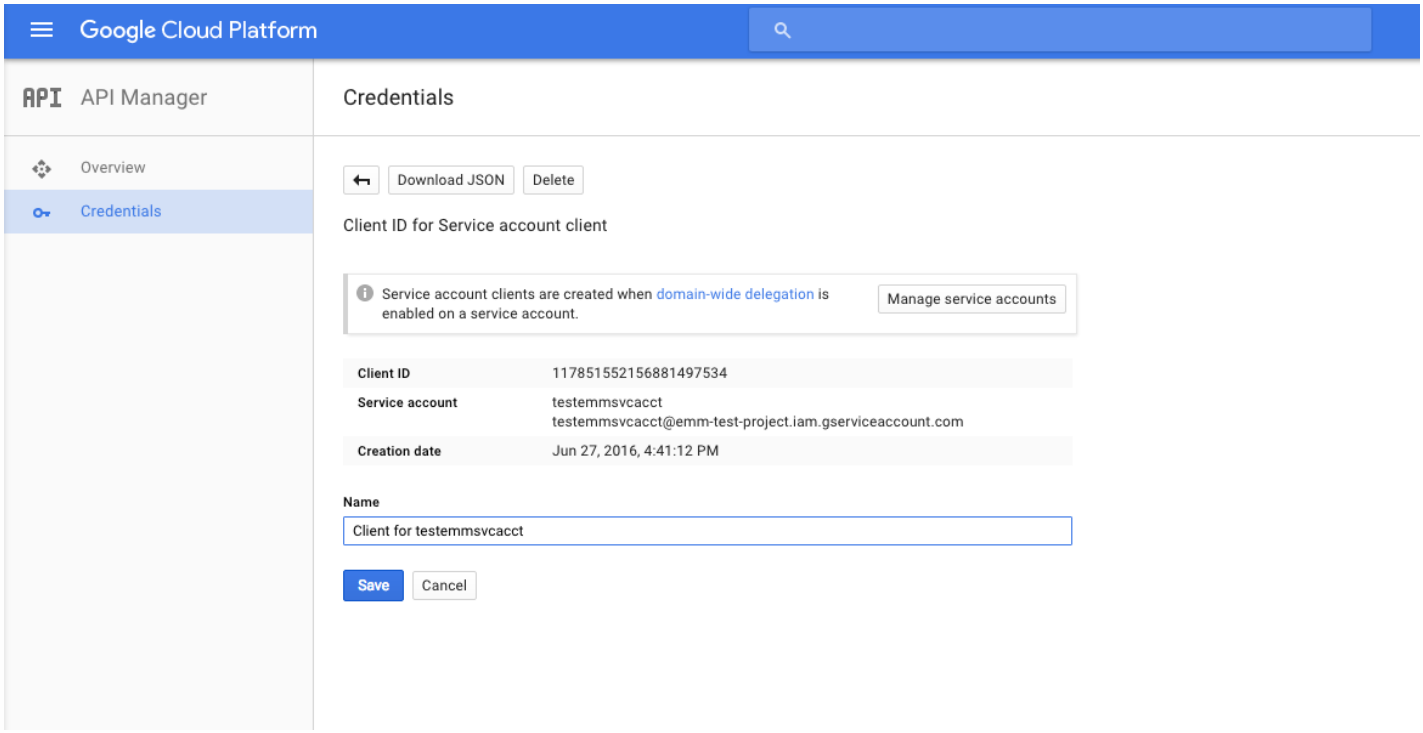


© 1999-2017 Citrix Systems, Inc. All rights reserved.

12. 在 **Permissions**（权限）中，单击 **Service accounts**（服务帐户），然后在您的服务帐户对应的 **Options**（选项）下，单击 **View Client ID**（查看客户端 ID）。

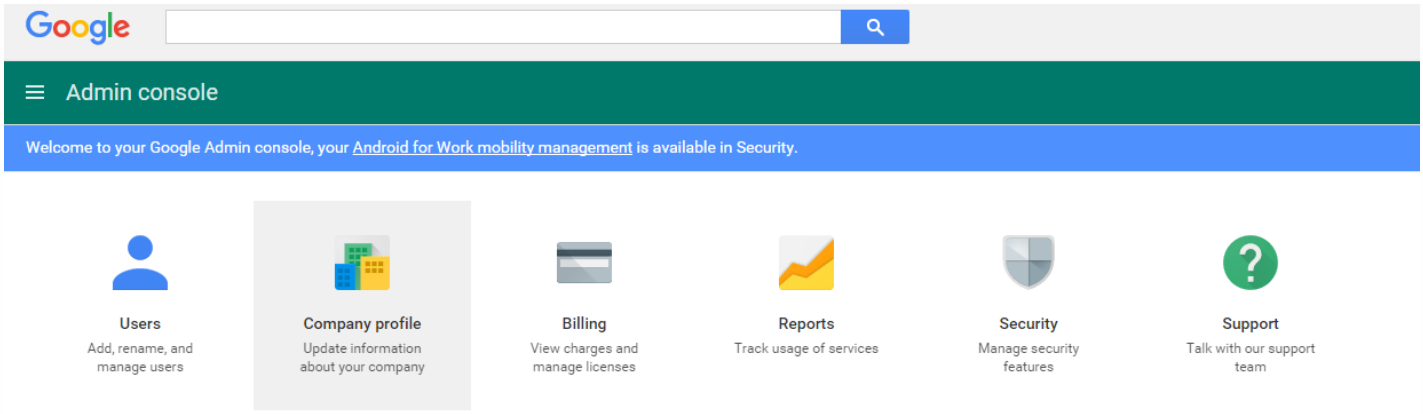


13. 此时将显示 Google 管理控制台上的帐户授权所需的详细信息。 将 **Client ID**（客户端 ID）和 **Service account ID**（服务帐户 ID）复制到以后能够从中检索信息的位置。 需要提供此信息以及域名，才能发送给 Citrix 技术支持用于添加到白名单。

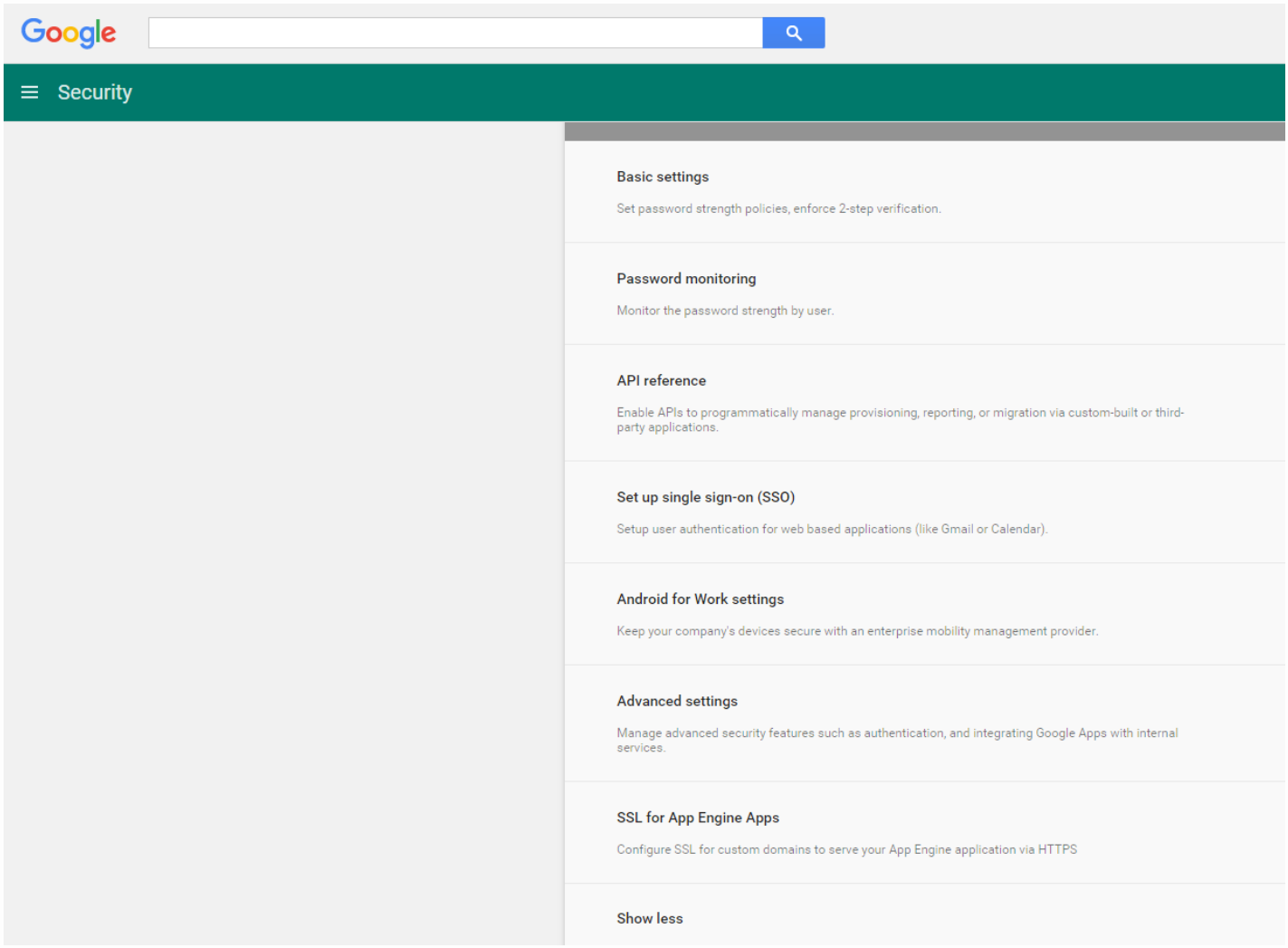


14. 打开您的域对应的 Google 管理控制台，然后单击 **Security**（安全）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

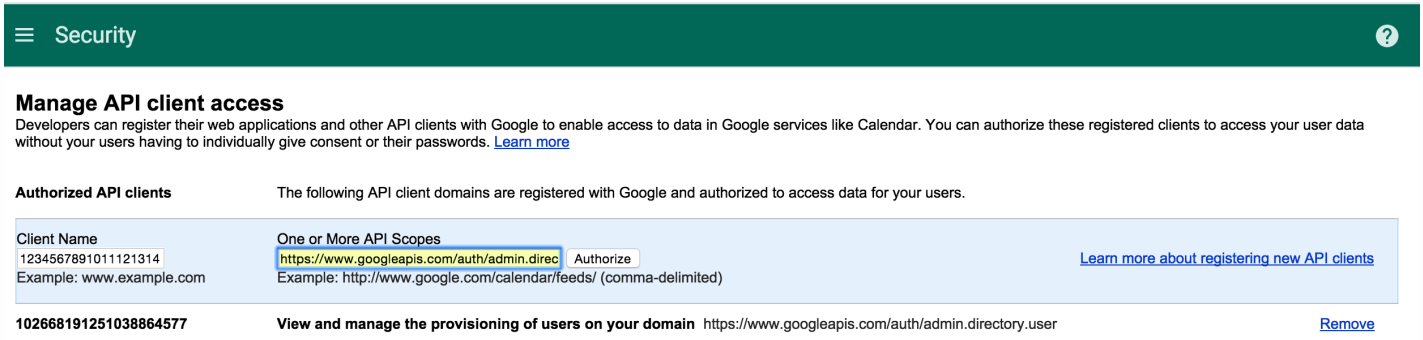


15. 单击 **Android for Work** 设置。



16. 在 **Client Name**（客户端名称）中，输入您之前保存的客户端 ID，在 **One or More API Scopes**（一个或多个 API 作用域）中，输入 https://www.googleapis.com/auth/admin.directory.user，然后单击 **Authorize**（授权）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

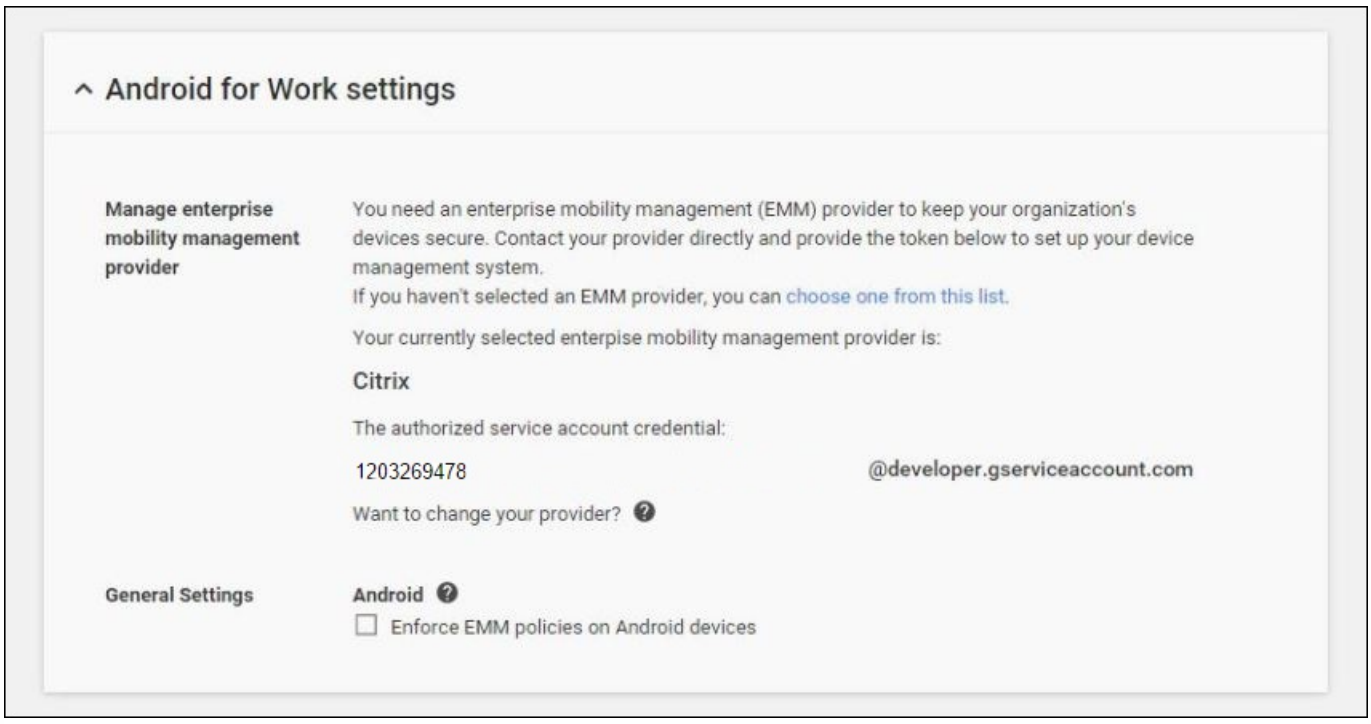


绑定到 EMM

必须先联系 Citrix 技术支持 (https://www.citrix.com/contact/technical-support.html) 并提供您的域名、服务帐户和绑定令牌，才能使用 XenMobile 管理您的 Android for Work 设备。 Citrix 会将该令牌绑定到 XenMobile 作为 Enterprise Mobility Management (EMM) 提供程序。

1. 要确认绑定，请登录 Google 管理门户，然后单击 **Security**（安全）。

2. 单击 **Android for Work settings**（Android for Work 设置）。 您将看到自己的 Google Android for Work 帐户绑定到 Citrix，用作 EMM 提供程序。



确认令牌绑定后，可以开始使用 XenMobile 管理您的 Android for Work 设备。 必须导入在步骤 14 中生成的 P12 证书，设置 Android for Work 服务器设置，启用基于 SAML 的单点登录，并至少定义一条 Android for Work 设备策略。

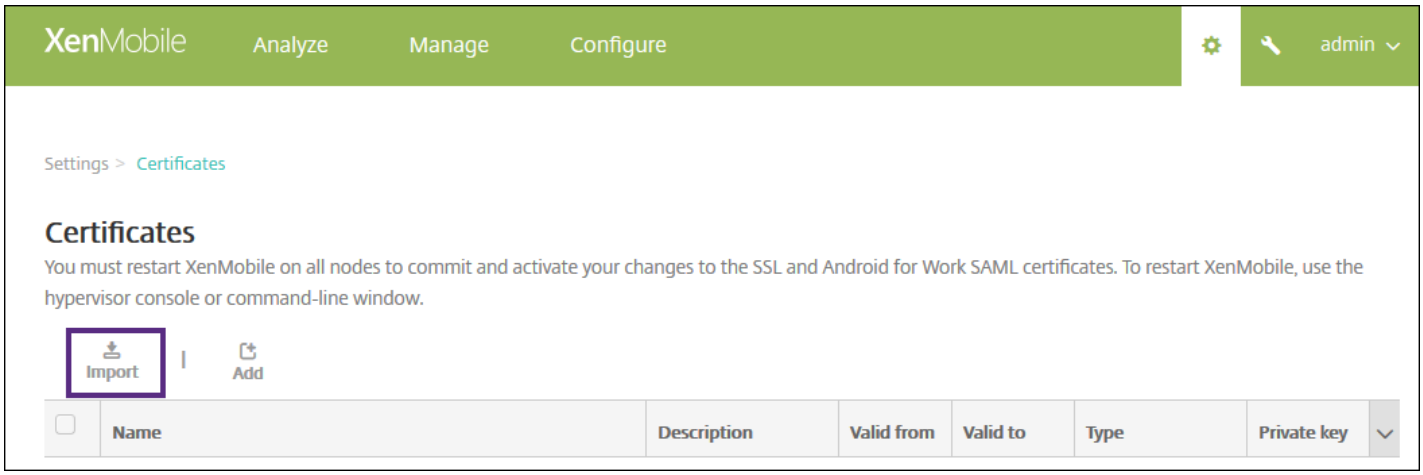
导入 P12 证书

请按照以下步骤导入 Android for Work P12 证书：

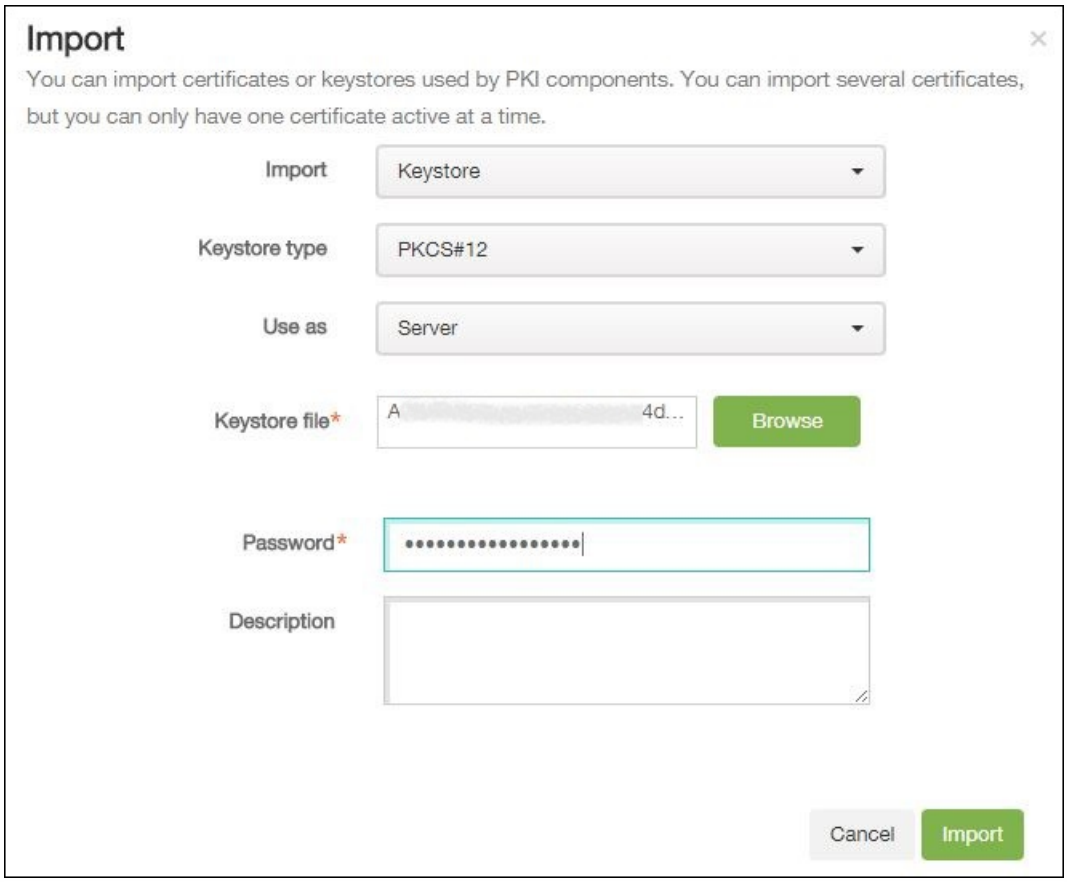
1. 登录到 XenMobile 控制台。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 单击控制台右上角的齿轮图标以打开**设置**页面，然后单击**证书**。 此时将显示**证书**页面。



3. 单击**导入**。 此时将显示**导入**对话框。



配置以下设置：

- **导入**：在列表中，单击**密钥库**。
- **密钥库类型**：在列表中，单击 **PKCS#12**。
- **用作**：在列表中，单击**服务器**。
- **密钥库文件**：单击**浏览**，然后导航到 P12 证书。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

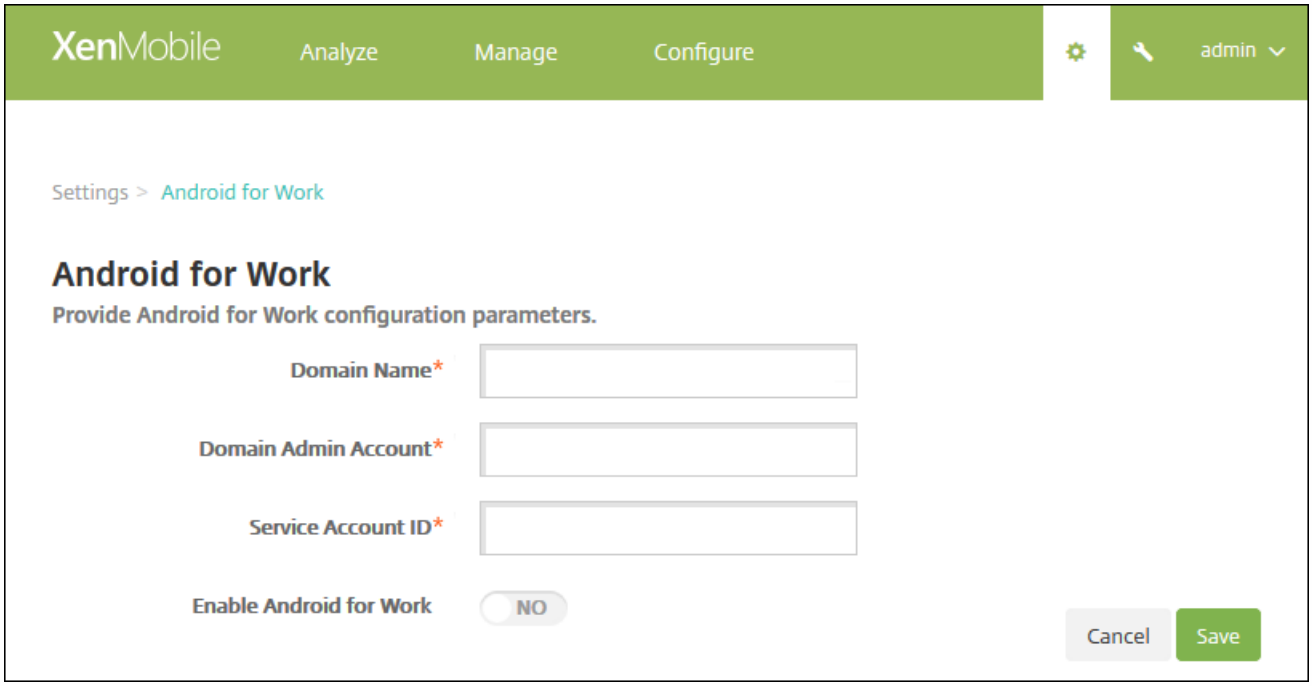
- **密码**：键入密钥库密码。
- **说明**：（可选）键入证书的说明。

4. 单击**导入**。

设置 Android for Work 服务器设置。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。 此时将打开**设置**页面。

2. 在**服务器**下，单击 **Android for Work**。 此时将显示 **Android for Work** 页面。



配置以下设置：

- **域名**：键入 Android for Work 的域名，例如 domain.com。
- **域管理员帐户**：键入域管理员的用户名，例如，用于 Google 开发人员门户的电子邮件帐户。
- **服务帐户 ID**：键入服务帐户 ID，例如，Google 服务帐户中关联的电子邮件 (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com)。
- **启用 Android for Work**：单击可启用或禁用 Android for Work。

3. 单击**保存**。

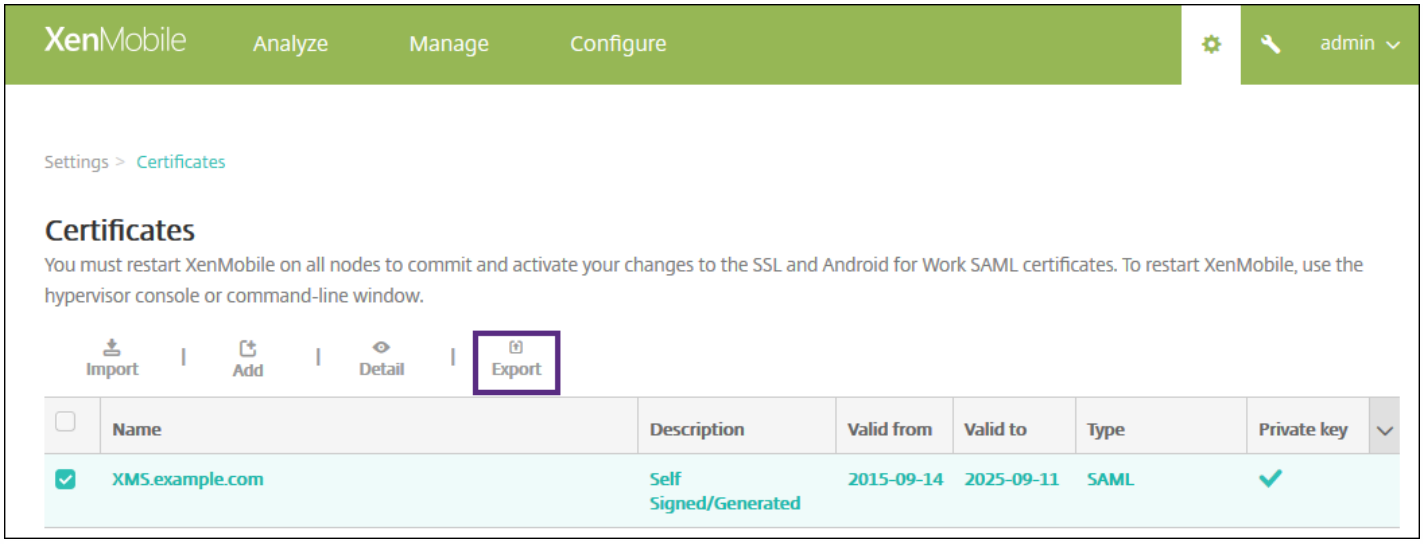
启用基于 SAML 的单点登录

1. 登录到 XenMobile 控制台。

2. 单击控制台右上角的齿轮图标。 此时将显示**设置**页面。

3. 单击**证书**。 此时将打开**证书**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

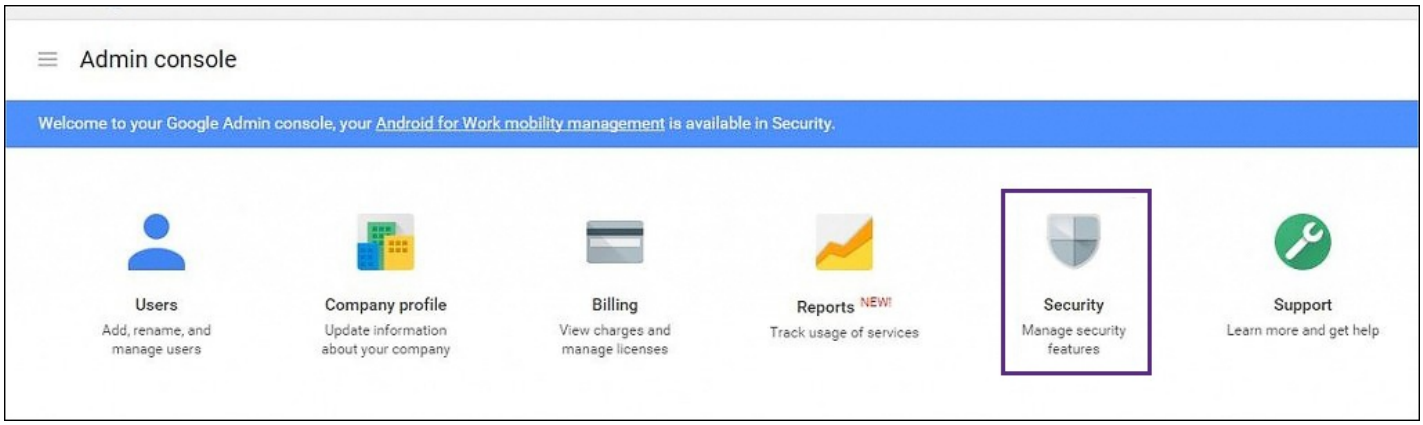


3. 在证书列表中，单击 SAML 证书。

4. 单击**导出**并将证书保存到您的计算机。

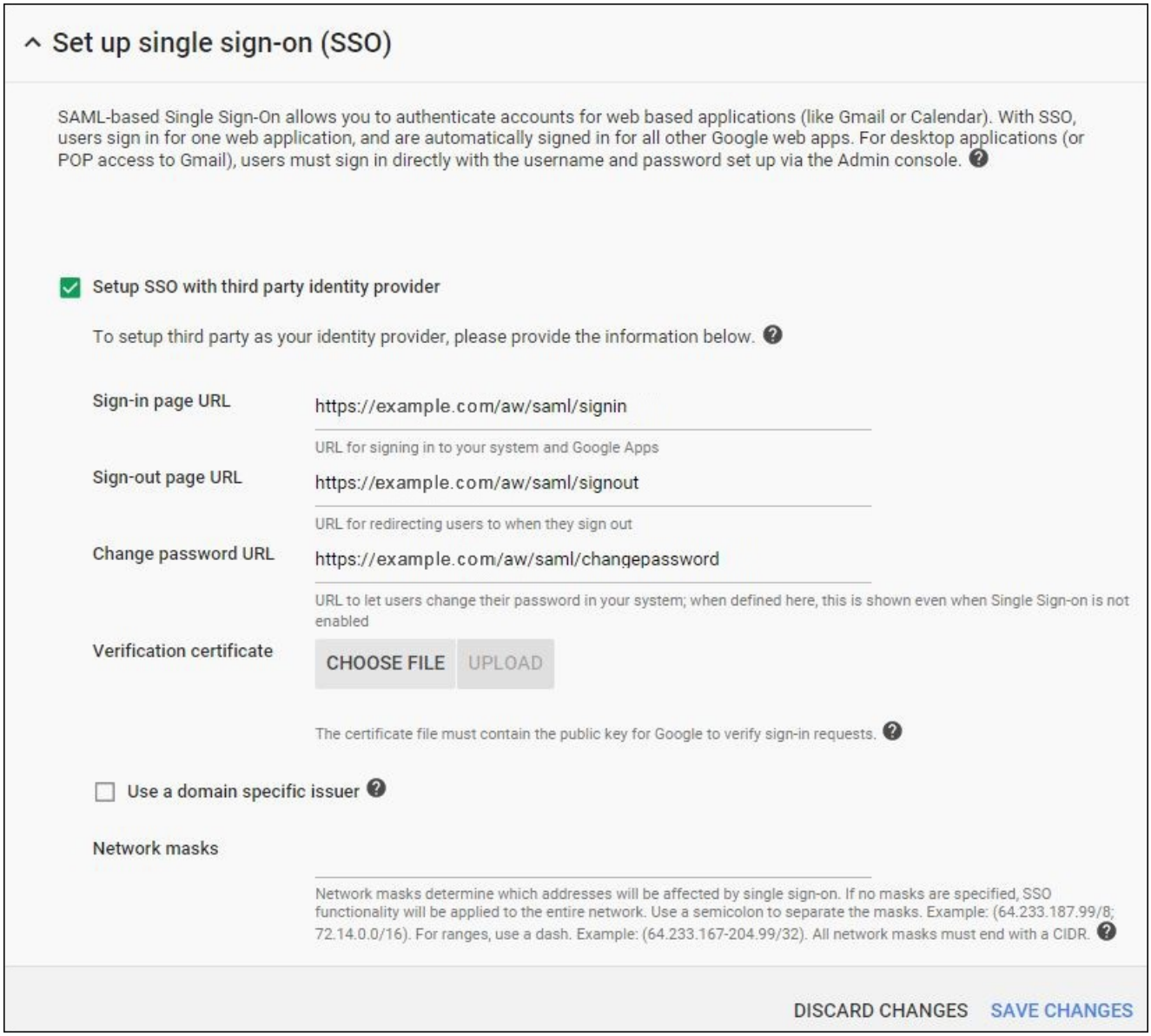
5. 使用您的 Android for Work 管理员凭据登录 Google 管理门户，网址为 https://admin.google.com。

6. 单击 **Security**（安全）。



7. 在 **Security**（安全）下，单击 **Set up single sign-on (SSO)**（设置单点登录(SSO)），然后配置以下设置：

© 1999-2017 Citrix Systems, Inc. All rights reserved.



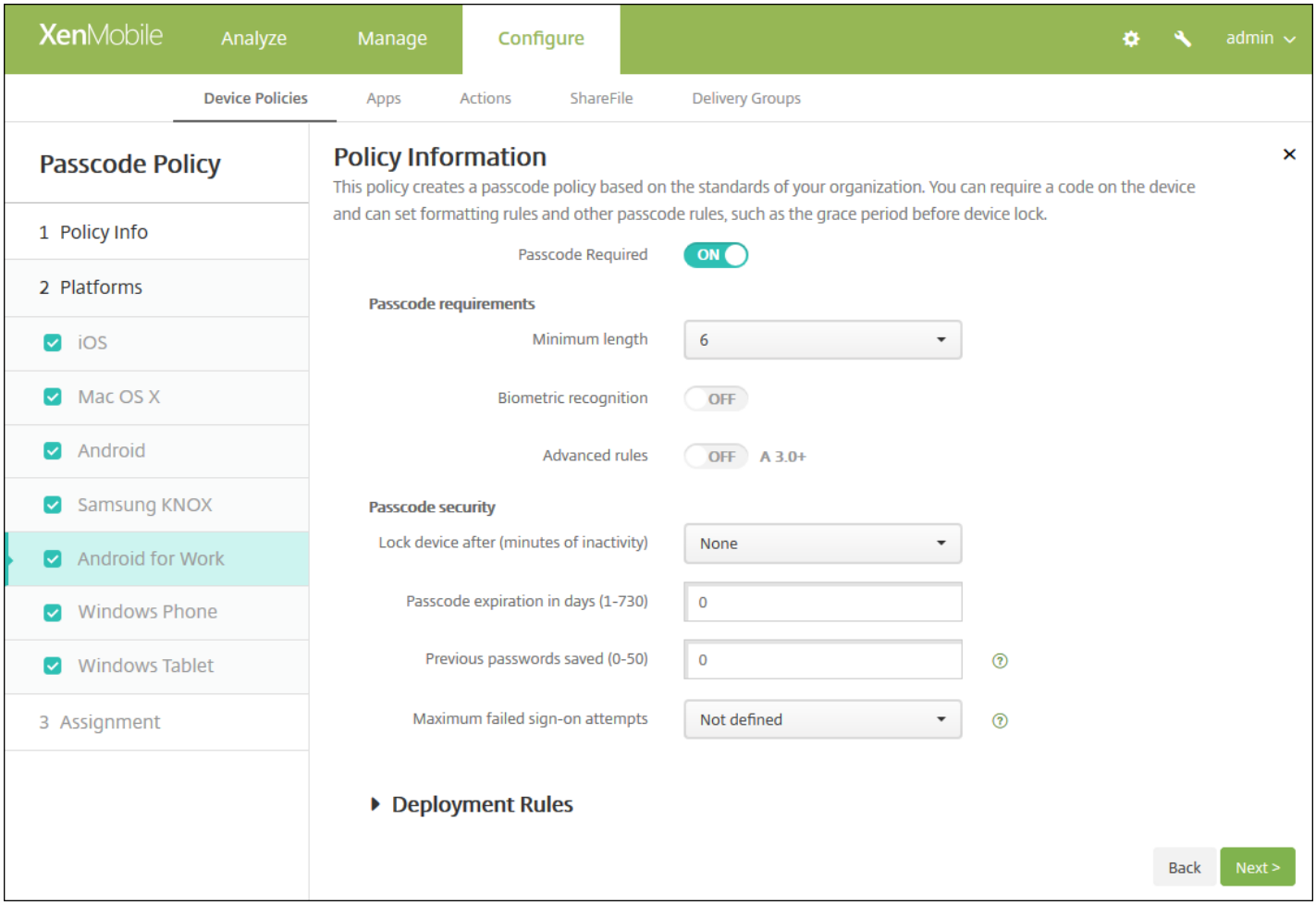
- **登录页面 URL**：键入用户登录您的系统和 Google 应用程序使用的 URL。 例如：https:///aw/saml/signin。
- **注销页面 URL**：键入注销时用户被定向到的 URL。 例如：https:///aw/saml/signout。
- **Change password URL**（更改密码 URL）：键入 URL 以允许用户更改其系统中的密码。 例如：https:///aw/saml/changepassword。 在此处定义时，即使 SSO 不可用，用户也可以看到此信息。
- **Verification certificate**（验证证书）：单击“CHOOSE FILE”（选择文件）并导航到从 XenMobile 导出的 SAML 证书。

8. 单击 **SAVE CHANGES**（保存证书）。

设置 Android for Work 设备策略

可以设置所需的任何设备策略，但最好设置通行码策略，以便要求用户在首次注册时在其设备上创建通行码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



设置任何设备策略的基本步骤如下：

1. 登录到 XenMobile 控制台。

2. 单击**配置 -> 设备策略**。

3. 单击**添加**，然后选择要从**添加新策略**对话框中添加的策略（在此示例中，请单击**通行码**）。

4. 完成**策略信息**页面。

5. 单击 **Android for Work** 并配置策略设置。

6. 将策略分配到交付组。

有关设置适用于 Android for Work 的其他设备策略的详细信息，请参阅 XenMobile 设备策略（按平台）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置 Android for Work 帐户设置

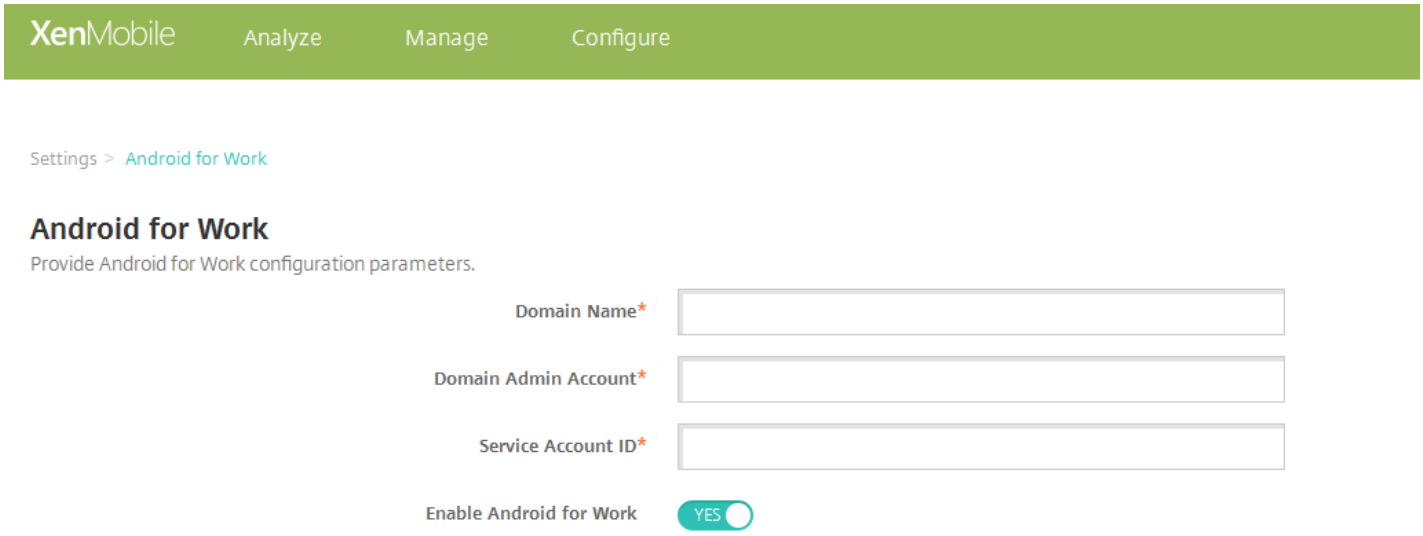
Aug 11, 2016

> **警告**
>
> 存在阻止您使用 XenMobile 控制台启用 Android for Work 的已知第三方问题。 有关该问题以及如何配置服务器属性作为解决方法的详细信息，请参阅 XenMobile 服务器 10.3 已知问题中的问题 #615118。

您必须在 XenMobile 中设置 Android for Work 域和帐户信息，才能管理用户设备上的 Android for Work 应用程序和策略。 但是，执行此操作前，还必须在 Google 上完成 Android for Work 设置任务以设置域管理员，并获取服务帐户 ID 和绑定令牌。有关在 Google 上执行 Android for Work 设置任务的详细信息，请参阅使用 Android for Work 管理设备。

1. 在 XenMobile Web 控制台中，单击右上角的齿轮图标。 此时将显示**设置**页面。

2. 在**服务器**下，单击 **Android for Work**。 此时将显示 **Android for Work** 配置页面。



3. 在 **Android for Work** 页面上，配置以下设置：

- **域名**：键入域名。
- **域管理员帐户**：键入域管理员用户名。
- **服务帐户 ID**：键入 Google 服务帐户 ID。
- **启用 Android for Work**：选择是否启用 Android for Work。

4. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 Android for Work 中置备设备所有者模式

Aug 11, 2016

必须按照本文档中说明的步骤在两台设备（一台设备运行 Worx Provisioning Tool，一台设备还原到其出厂设置）之间通过近场通信 (NFC) 碰撞传输数据，才能在设备所有者模式下置备 Android for Work。 设备所有者模式仅适用于企业拥有的设备。

为什么通过 NFC？ 蓝牙、WiFi 和其他通信模式在恢复出厂设置的设备上处于禁用状态。 NFC 是此状态下设备理解的唯一通信协议。

有关在 XenMobile 环境中部署 Android for Work 的概述，请参阅在 XenMobile 中使用 Android for Work 管理设备。

必备条件

- 启用了 Android for Work 的 XenMobile 服务器 – 版本 10.1 和 10.3。
- 恢复出厂设置的设备，在设备所有者模式下针对 Android for Work 置备。 此操作需要执行的步骤在下文中进行介绍。
- 另一台设备具有 NFC 功能，运行已配置的 Worx Provisioning Tool。 Worx Provisioning Tool 在 Worx Home 10.3 或 Citrix 下载页面上提供。

每台设备只能有一个 Android for Work 配置文件，通过企业移动管理 (Enterprise Mobility Management, EMM) 应用程序进行管理。 在 XenMobile 中，Worx Home 属于 EMM 应用程序。 一台设备上仅允许存在一个配置文件。 尝试添加第二个 EMM 应用程序将删除第一个 EMM 应用程序。

可以在现有设备上或还原为出厂设置的设备上启动设备所有者模式。 您将通过 XenMobile 管理整个设备。

设备所有者模式下的 NFC 碰撞

置备恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以启动 Android for Work：

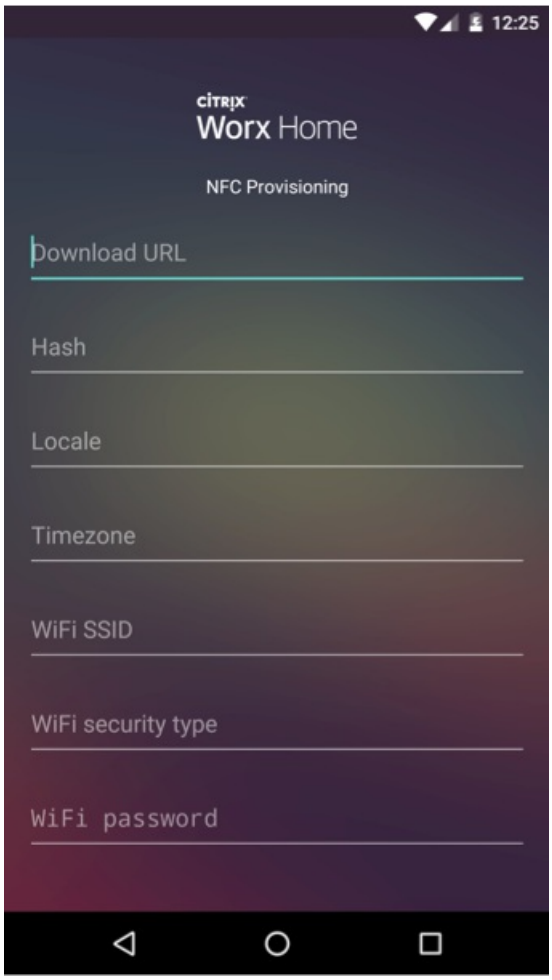
- 要作为设备所有者 (Worx Home) 的 EMM 提供程序应用程序的包名称。
- 可以从中下载 EMM 提供程序应用程序的 Intranet/Internet 位置。
- 用于验证下载是否成功的 EMM 提供程序应用程序的 SHA1 散列。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备能够连接和下载 EMM 提供程序应用程序。 （Android 当前不支持对此流程使用 802.1x Wi-Fi）。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

碰撞两台设备时，来自 Worx Provisioning Tool 的数据将发送到恢复出厂设置的设备。 该数据随后用于下载使用管理员设置的 Worx Home。 如果未输入时区和位置值，Android 将在新设备上进行自动配置。

配置 Worx Provisioning Tool

执行 NFC 碰撞之前，必须配置 Worx Provisioning Tool。 此配置随后在 NFC 碰撞过程中被传输到恢复出厂设置的设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



可以将数据输入到必填字段中，或者通过文本文件进行填充。 输入后，该应用程序不保存信息，因此，您可能希望创建一个文本文件以保留该信息供将来使用。

通过文本文件配置

将文件命名为 **nfcprovisioning.txt** 并将其放置在设备的 SD 卡中的 /sdcard/Downloads 文件夹下。 该应用程序随后可以读取文本文件并填充值。

文本文件必须包含以下数据：

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=
这是 EMM 提供程序应用程序的 Intranet/Internet 位置。 恢复出厂设置的设备在连接到 WiFi 并进行 NFC 碰撞之后（使用在上面的屏幕中输入的 SSID、安全性类型和密码），必须能够访问此位置以进行下载。 该 URL 为常规 URL，不需要特殊格式。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=
这是 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下文中进行介绍。

android.app.extra.PROVISIONING_WIFI_SSID=
这是运行 Worx Provisioning Tool 的设备的已连接 WiFi SSID。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=
支持的值为 WEP 和 WPA2。 如果 WiFi 未受保护，此字段必须留空。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

android.app.extra.PROVISIONING_WIFI_PASSWORD=
如果 WiFi 未受保护，此字段必须留空。

android.app.extra.PROVISIONING_LOCALE=
输入语言和国家/地区代码。 语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。 国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 Us），如 ISO 3166-1 所定义。 例如，请输入 en_US 表示在美国所讲的英语。 如果未输入任何代码，则会自动填充国家/地区和语言。

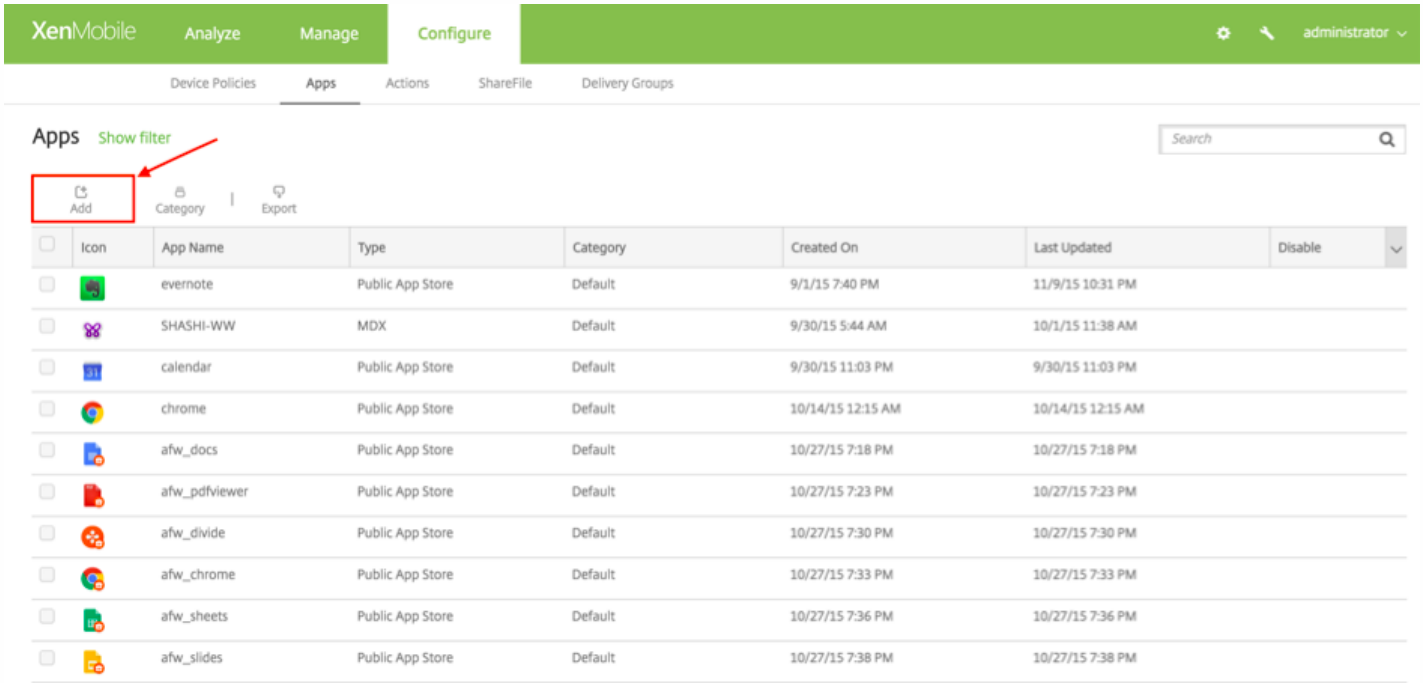
android.app.extra.PROVISIONING_TIME_ZONE=
设备运行时所在的时区。 请输入表单区域/位置的 Olson 名称。 例如，America/Los_Angeles 表示太平洋时间。 如果未输入，则将自动填充时区。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=
非必需，因为值 Worx Home 被硬编码到应用程序中。 在本文中提及的目的只是为了保持完整性。

获取 Worx Home 校验和

要获取任何应用程序的校验和，请添加该应用程序作为企业应用程序。

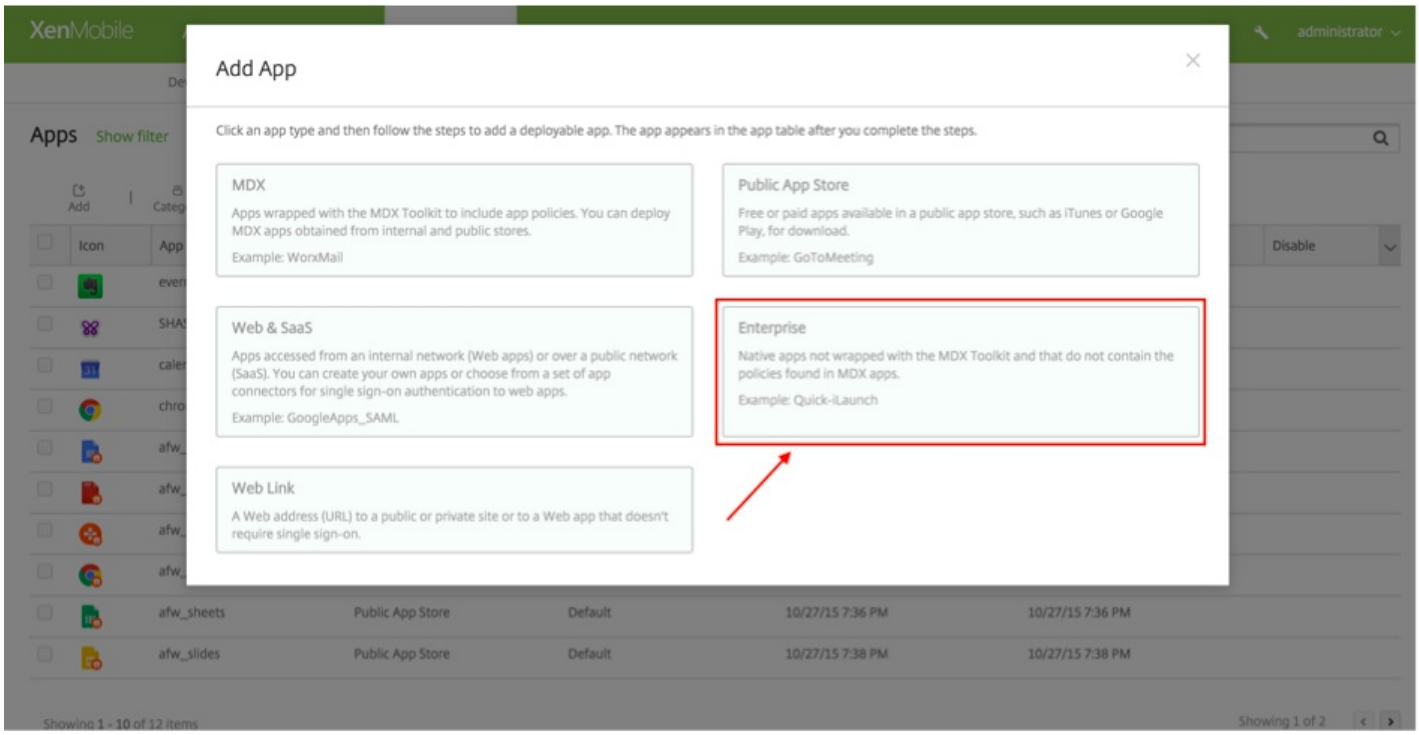
1. 在 XenMobile 控制台中，导航到**配置 > 应用程序 > 添加**。



此时将显示“添加应用程序”窗口。

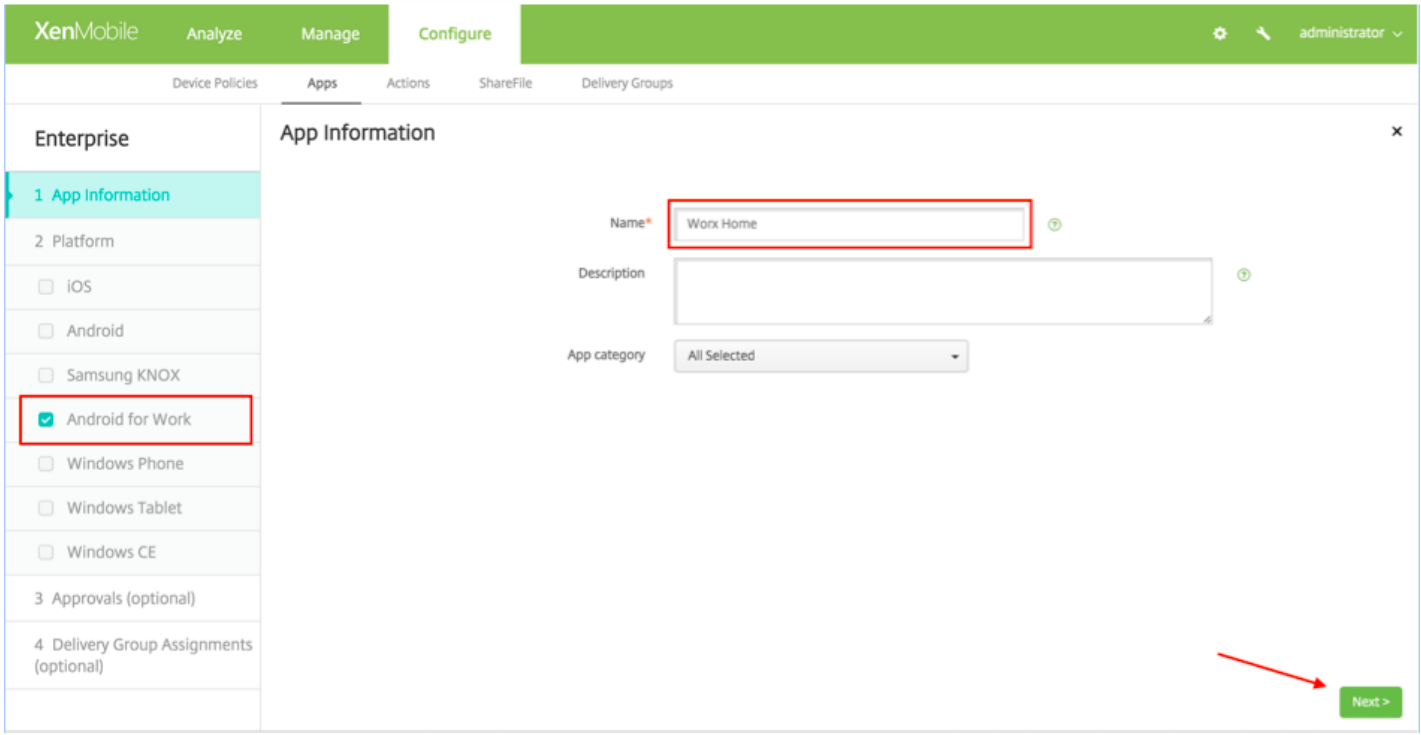
2. 单击**企业**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



此时将显示**应用程序信息**屏幕。

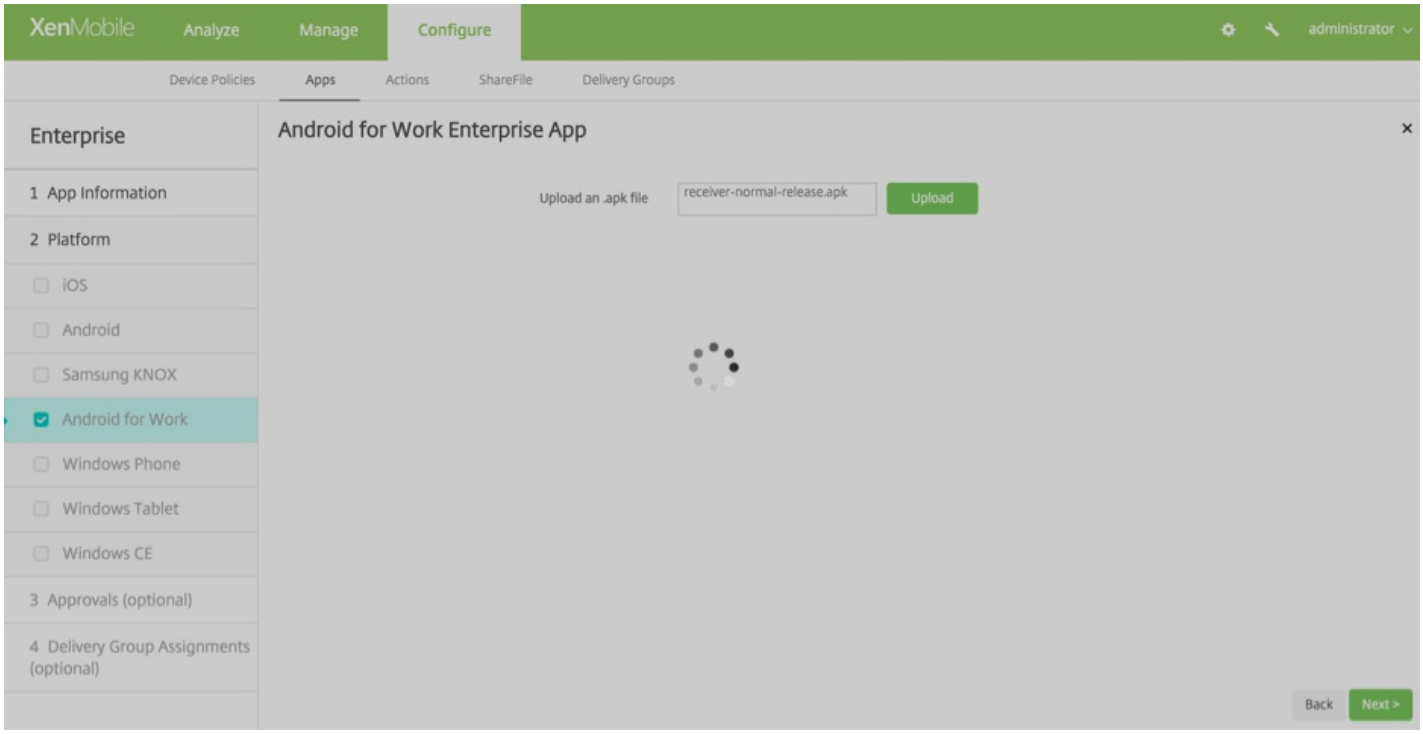
3. 选择以下配置并单击**下一步**。



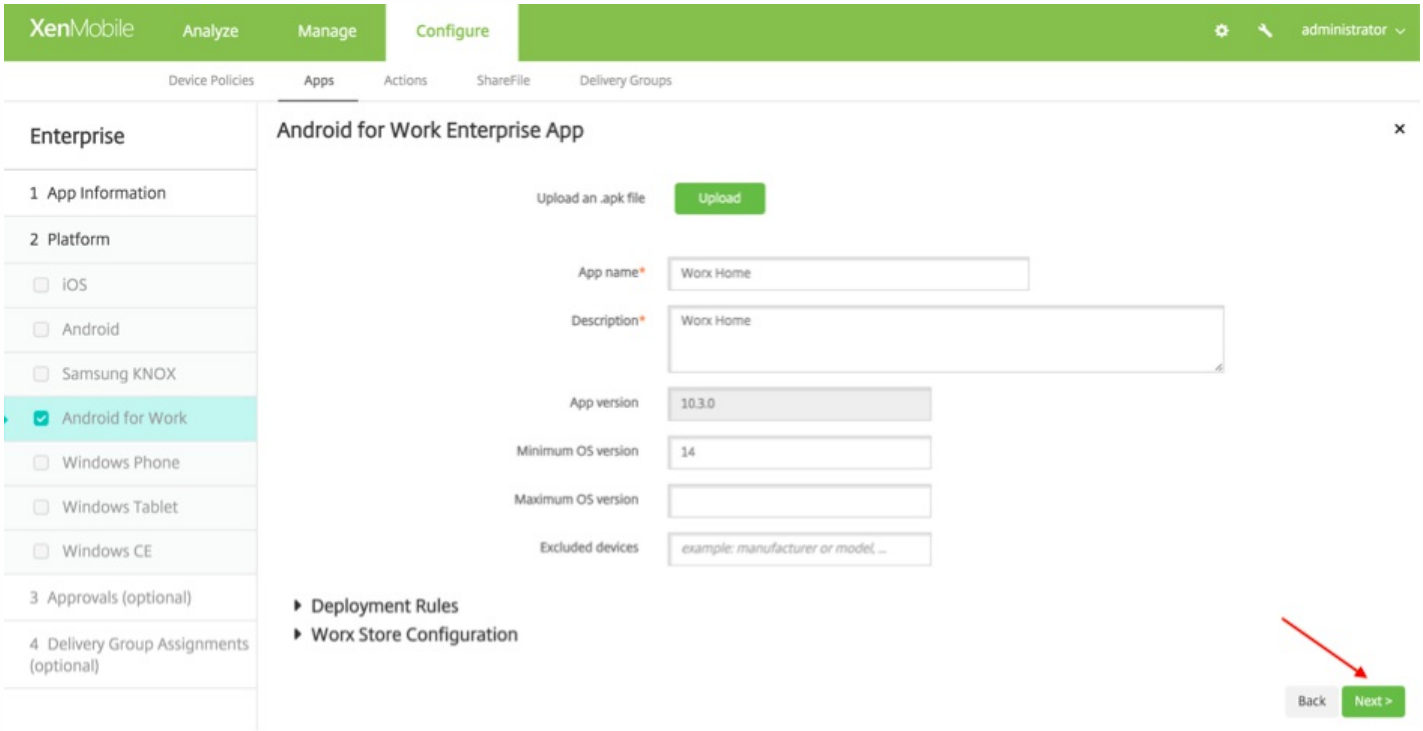
此时将显示 **Android for Work 企业应用程序**屏幕。

4. 提供 .apk 的路径，然后单击**下一步**以上载文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

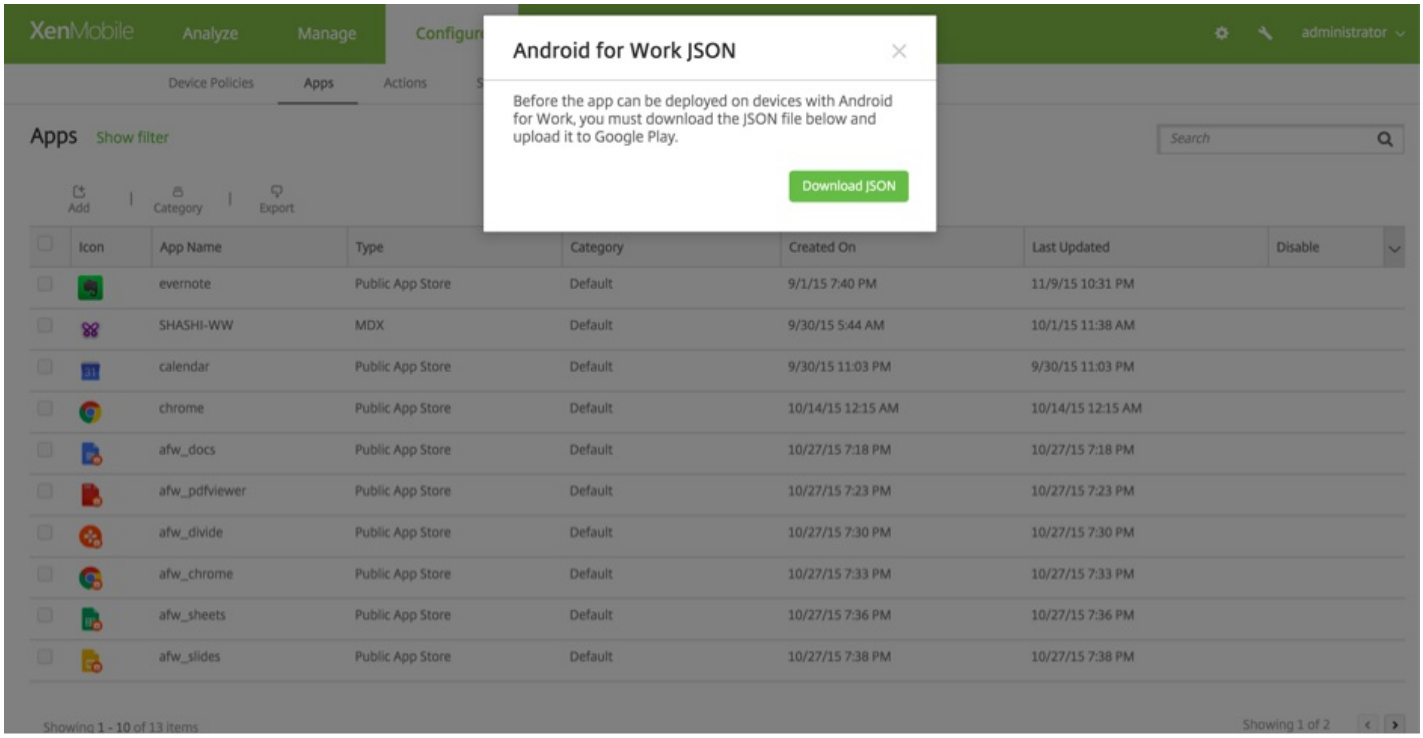


上载完成后，系统将显示上载的软件包的详细信息。



5. 单击**下一步**显示下载 JSON 文件的屏幕，随后可以在该屏幕中上载到 Google Play。 对于 Worx Home，不需要上载到 Google Play，但需要 JSON 文件才能从中读取 SHA1 值。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



典型的 JSON 文件格式如下：

6. 复制 **file_sha1_base64 value** 并在 Worx Provisioning Tool 中的 **Hash**（散列）字段中使用。 **注意：**散列的 URL 必须安全。

- 将所有 **+** 符号转换为 **-**
- 将所有 **/** 符号转换为 **_**
- 将尾部的 **\u003d** 替换为 **=**

如果您将散列存储在设备的 SD 卡上的 nfcprovisioning.txt 文件中，该应用程序将不执行安全性转换。 但是，如果选择手动输入散列，您将负责确保其 URL 的安全性。

使用的库

Worx Provisioning Tool 在其源代码中使用以下库：

- Google 在 Apache License 2.0 下提供的 v7 appcompat library
- Google 在 Apache License 2.0 下提供的 Design support library
- Google 在 Apache License 2.0 下提供的 v7 Palette library
- Jake Wharton 在 Apache License 2.0 下提供的 Butter Knife

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置部署规则

Oct 21, 2016

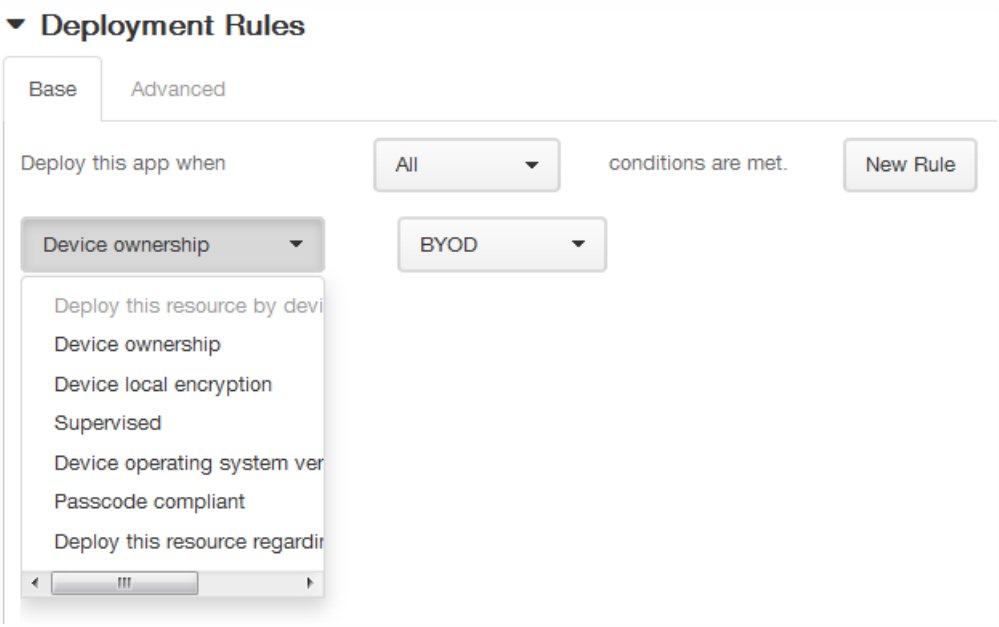
本部分介绍以下内容：

- 部署规则 - 影响软件包部署结果的参数。
- 部署计划 - 用于指定 XenMobile 何时将软件包推送到设备的选项。

配置部署规则

部署规则是一些用于控制软件包部署结果的参数。 您可以指定针对设备属性、应用程序和操作的部署规则。 在确定软件包的部署顺序时，XenMobile 将使用您为设备属性指定的部署规则来过滤策略、应用程序、操作和交付组。 有关详细信息，请参阅部署顺序。

可以基于特定操作系统版本、特定硬件平台或其他一些组合执行软件包部署。 在此用于添加和编辑设备属性、应用程序和操作的向导中，同时为**基本**和**高级**规则编辑器。 **高级**视图是一种自由形式编辑器。 下图说明了添加或编辑应用程序时显示的**部署规则**屏幕：



基础部署规则

基础部署规则由预先定义的测试和所生成的操作组成。 结果尽可能预先内置在示例测试中。 例如，基于硬件平台部署软件包时，现有的所有已知平台将填入生成的测试中，从而大大缩短规则创建时间，并限制了可能出现的错误。

单击**新建规则**以向软件包添加规则。

注意：规则生成器包含特定于每个测试的详细信息。

要创建新的规则，请选择规则模板，选择条件类型，然后自定义规则。 自定义规则涉及到修改说明。 完成对设置的配置时，将规则添加到软件包中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

您可以根据需要添加多个规则。 当所有的规则都匹配时，将部署软件包。

高级部署规则

如果单击**高级**选项卡，将出现**高级规则编辑器**。

在此模式中，您可以指定规则之间所设置的关系。 运算符 **AND**、**OR** 和 **NOT** 可用。

配置部署计划

XenMobile 使用您为操作、应用程序和设备策略指定的部署计划来控制这些项目的部署。 可以将部署过程指定为立即执行、在特定日期和时间执行或根据部署条件执行。 配置的部署计划对所有平台相同。

您所做的更改适用于所有平台，但**为始终启用的连接部署**除外，此设置不适用于 iOS。 iOS 使用 APN。

如果不更改部署计划选项，则将在每次连接时立即执行部署。 部署计划选项包括：

部署：默认值为**开**。 要阻止部署，请将此设置更改为**关**。

部署计划：默认为**立即**。 要指定部署时间，请选择**稍后**，然后选择日期并输入时间。

部署条件：默认为**每次连接时**。 要限制部署，请将此设置更改为**仅当之前的部署失败时**。

为始终启用的连接部署：默认为**关**。 此策略仅适用于 Android 设备。 XenMobile 服务器属性**后台部署**要求您将部署到 Android 设备的每个策略的**为始终启用的连接部署**设置为**开**。 有关始终启用的连接的详细信息，请参阅《XenMobile 部署手册》文章调整 XenMobile 操作中的“其他服务器优化”和“为 Android 设备优化部署计划”以及设备和应用程序策略中的“计划策略”。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

添加设备并查看设备详细信息

Aug 11, 2016

XenMobile 服务器数据库存储移动设备的列表。 每个移动设备通过唯一的序列号或国际移动设备标识 (IMEI)/移动设备标识符 (MEID) 标识定义。 要将设备填充到 XenMobile 控制台中，可以手动添加设备或从文件导入设备列表。 有关设备置备文件格式的详细信息，请参阅设备置备文件的格式。

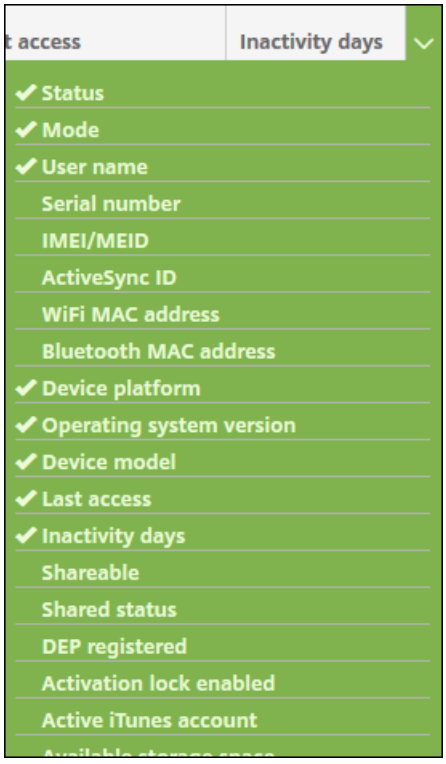
在 XenMobile 控制台的**设备**页面中，会显示列出每台设备的表格，以及下列信息：**状态**（表示设备越狱状态、是否托管、Active Sync Gateway 是否可用及设备部署状态的图标）、**模式**（模式为 MDM、MAM 还是二者）、**用户名**、**设备平台**、**操作系统版本**、**设备型号**、**上次访问时间**和**不活动天数**。

可以手动添加设备，从设备配置文件中导入设备，编辑设备详细信息，向设备发送通知以及删除设备。 还可以将所有设备表数据导出到 .csv 文件，这样将允许您生成自定义报告。 服务器将导出所有设备属性，如果应用过滤器，创建 .csv 文件时会考虑这些过滤器。

注意：上述标题为默认选项。 您可以自定义**设备**表格中显示的内容，方法是单击最后一个标题上的向下箭头，然后单击要在表格中显示的其他标题，或取消选中不希望看到的标题。

有关可用**设备**表操作的步骤，请参阅以下部分：

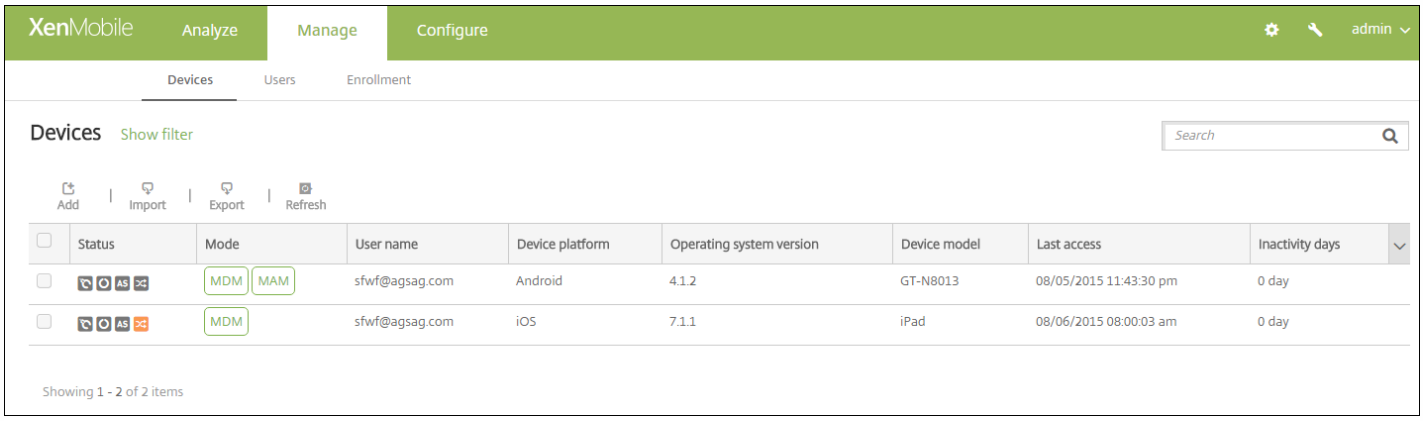
- 手动添加设备
- 从设备置备文件导入设备
- 编辑设备
- 向设备发送通知
- 删除设备
- 将**设备**表格导出到 .csv 文件中



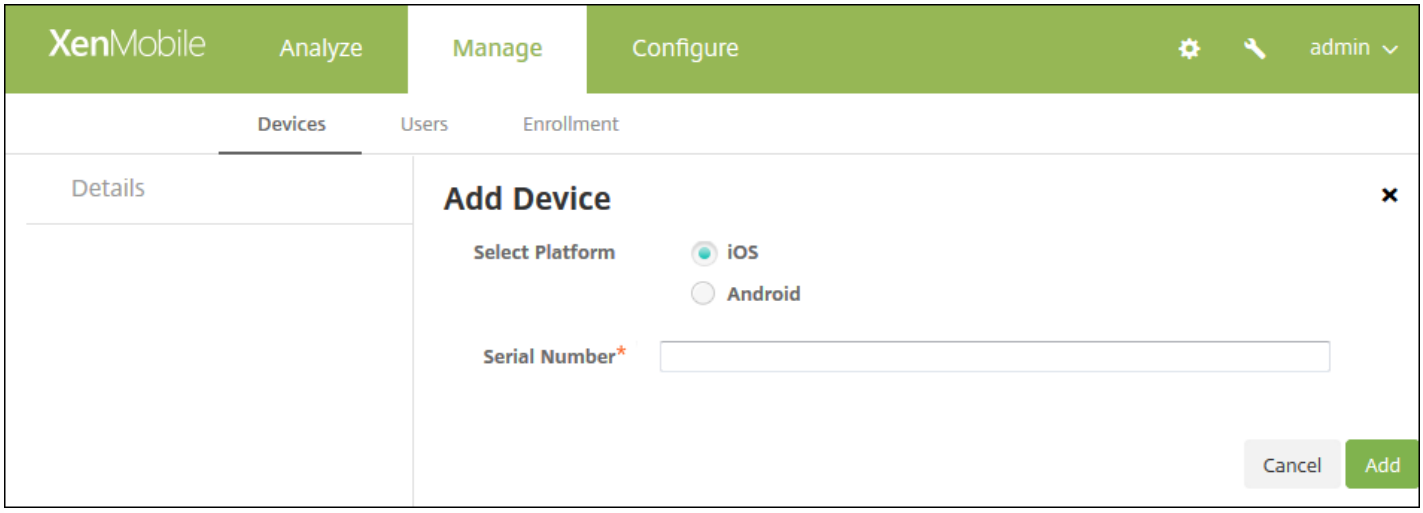
© 1999-2017 Citrix Systems, Inc. All rights reserved.

手动添加设备

1. 在 XenMobile 控制台中，单击**管理 > 设备**。 此时将显示**设备**页面。



2. 单击**添加**。 此时将显示**添加设备**页面。



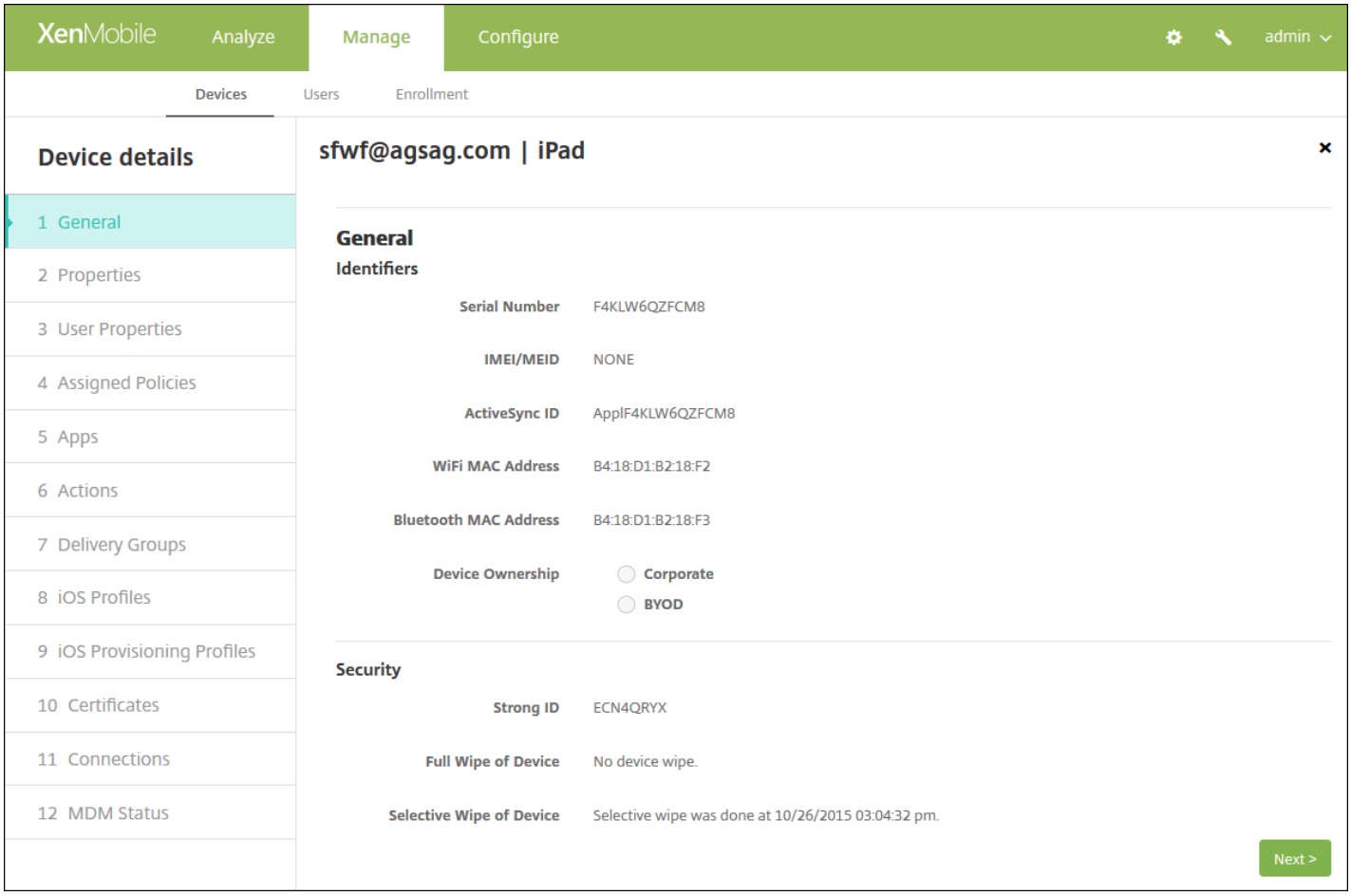
3. 配置以下设置：

- **选择平台**：单击 **iOS** 或 **Android**。
- **序列号**：键入设备序列号。
- **IMEI/MEID**：（可选，仅适用于 Android 设备）键入设备的 IMEi/MEID 信息。

4. 单击**添加**。 设备将添加到所显示**设备**表格的列表底部。 在此列表中，选择您所添加的设备，然后在显示的菜单中，单击**编辑**以查看并确认设备详细信息。

注意：如果选中某个设备旁边的复选框，选项菜单将显示在设备列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 在 **General Identifiers**（常规标识符）下面，确认显示的信息（确切的列表因平台类型而异）：

- 序列号
- IMEI/MEID
- ActiveSync ID
- WiFi MAC 地址
- 蓝牙 MAC 地址
- 设备所有权

6. 在**安全性**下面，确认显示的信息（确切的列表因平台类型而异）：

- 强 ID
- 完全擦除设备
- 选择性擦除设备
- 锁定设备
- 设备解锁
- 设备定位
- 设备启用跟踪
- 设备否认拥有
- 激活锁跳过
- 设备清除限制
- 请求使用 AirPlay 镜像

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 停止使用 AirPlay 镜像

注意：iOS 的锁定设备适用于 iOS 7 及更高版本。

7. 单击**下一步**。 将显示**属性**页面，您可以在此页面添加设备的属性。

8. 单击**添加**。 将显示可用属性的列表。

9. 对于要添加的每个属性，请执行以下操作：

- 单击要置备的属性，然后设置其值。 例如，您可以选择属性**已启用激活锁**并将值设置为**是**或**否**。
- 单击**完成**。

10. 单击**下一步**。

注意：添加属性后，这些属性将在**属性**下面列出。 稍后返回到**属性**页面时，属性将被分为不同的类别。

已分配的策略部分及其后面的部分包含设备的摘要信息。

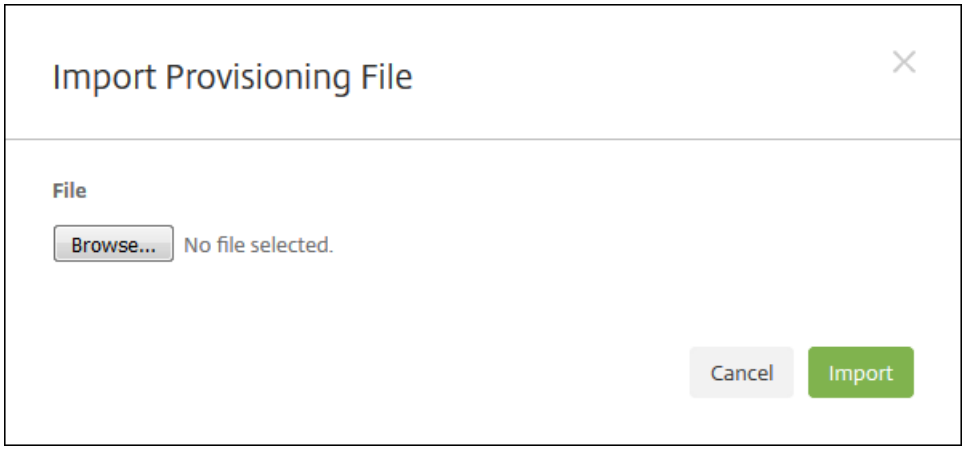
- **已分配的策略**：显示已分配策略的数量，包括已部署的策略数、待定策略数和失败的策略数。 也会显示每个策略的名称、类型和上次部署信息。
- **应用程序**：以清单形式显示应用程序的数量，包括已安装的应用程序数、待定应用程序数和失败的应用程序数。
- **已安装**：显示以下信息：名称、所有权、版本、作者、大小、安装时间、标识符和类型。
- **待安装和安装失败的应用程序**：显示以下信息：名称、上次部署时间、标识符和类型。
- **操作**：显示操作数，包括已部署的操作数、待定操作数和失败的操作数。 每个操作显示名称和上次部署信息。
- **交付组**：显示成功、待安装和失败的交付组数量。 显示每项操作的**交付组**和时间信息。 此外，还显示**交付组**的更多详细信息，包括状态、操作、所有者和日期。
- **iOS 配置文件**（仅限 iOS 设备）：显示上一个 iOS 配置文件清单，包括名称、类型、组织和说明。
- **证书**：显示有效证书和已过期或已吊销的证书数，包括类型、提供商、颁发者、序列号、有效期开始时间和有效期结束时间信息。
- **连接**：显示第一个连接状态和最后一个连接状态。 对于每个连接，会显示用户名、倒数第二次身份验证和上次身份验证。
- **TouchDown**（仅限 Android 设备）：显示上次设备身份验证时间和上次用户身份验证时间。 显示每个适用策略名称和策略值。

12. 单击**保存**。

从置备文件导入设备

您可以导入移动运营商或设备制造商支持的文件，或创建自己的设备置备文件。 请参阅设备置备文件格式。
1. 在**设备**表格上方的菜单中，单击**导入**。 此时将显示**导入置备文件**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

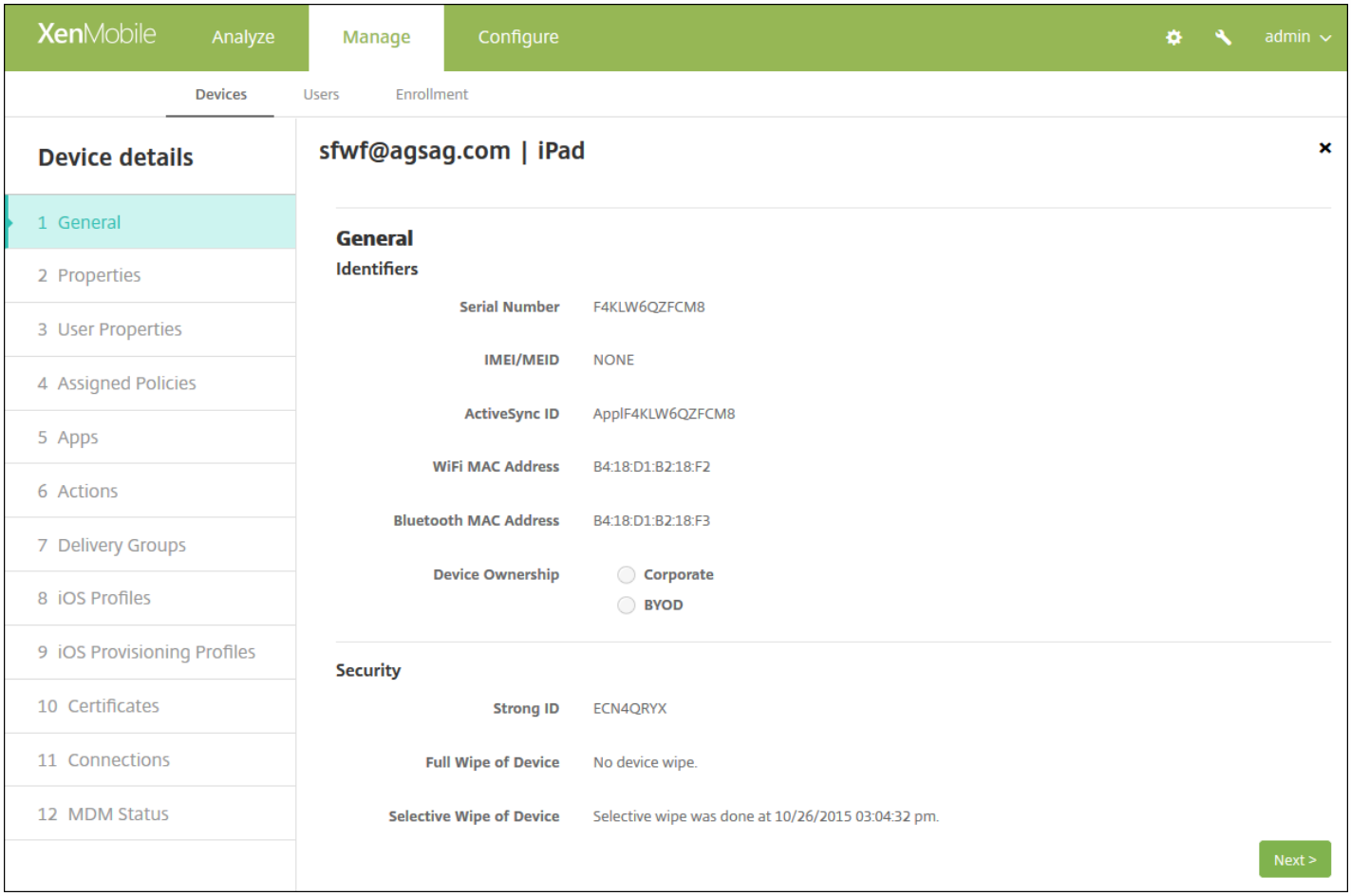


2. 通过单击**浏览**并导航到要导入的文件的位置，选择此文件。

3. 单击**导入**。 导入后的文件将添加到**设备**表格中。

编辑设备

1. 选择要编辑的设备，然后单击编辑。 此时将显示设备详细信息页面。



2. 在 **General Identifiers**（常规标识符）下，只能更改**设备所有权**字段，可以将其设置为**公司**或 **BYOD**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 单击**下一步**。此时将显示**属性**页面。

4. 在**属性**页面上，可以添加、编辑或删除属性。

- 要添加属性，请在要将属性添加到的类别中单击“添加”，单击所显示列表中的属性，然后添加属性的值。 单击**完成**。
- 要编辑某个属性，请单击此属性，修改其设置，然后单击**完成**或**取消**。
- 要删除某个属性，请悬停在此列表的上方，然后单击右侧的 X。 项目立即被删除。

5. 单击**下一步**。下面显示的页面取决于选择的设备。 对于某些设备，将显示**用户属性**，对于其他设备，则显示 **Assigned Policies**（已分配的策略）。

6. 如果显示**用户属性**，则可以按如下所述添加、编辑或删除用户属性；否则，剩余页面将包含设备的摘要信息。 有关这些页面的说明，请参阅手动添加设备。

注意：用户属性页面的上部分无法编辑。

- 对于您要添加的各个用户属性，单击**添加**，然后执行以下操作：
  - 在显示的列表中，单击要添加的属性，输入属性的值，然后单击**完成**或**取消**。
- 要编辑某个属性，请单击此属性，修改其设置，然后单击**完成**或**取消**。
- 要删除某个属性，请悬停在此列表的上方，然后单击右侧的 X。 项目立即被删除。

7. 在后面的每个页面中，查看摘要信息并单击**下一步**。

8. 在最后一个页面上，单击**保存**以保存对设备所做的更改。

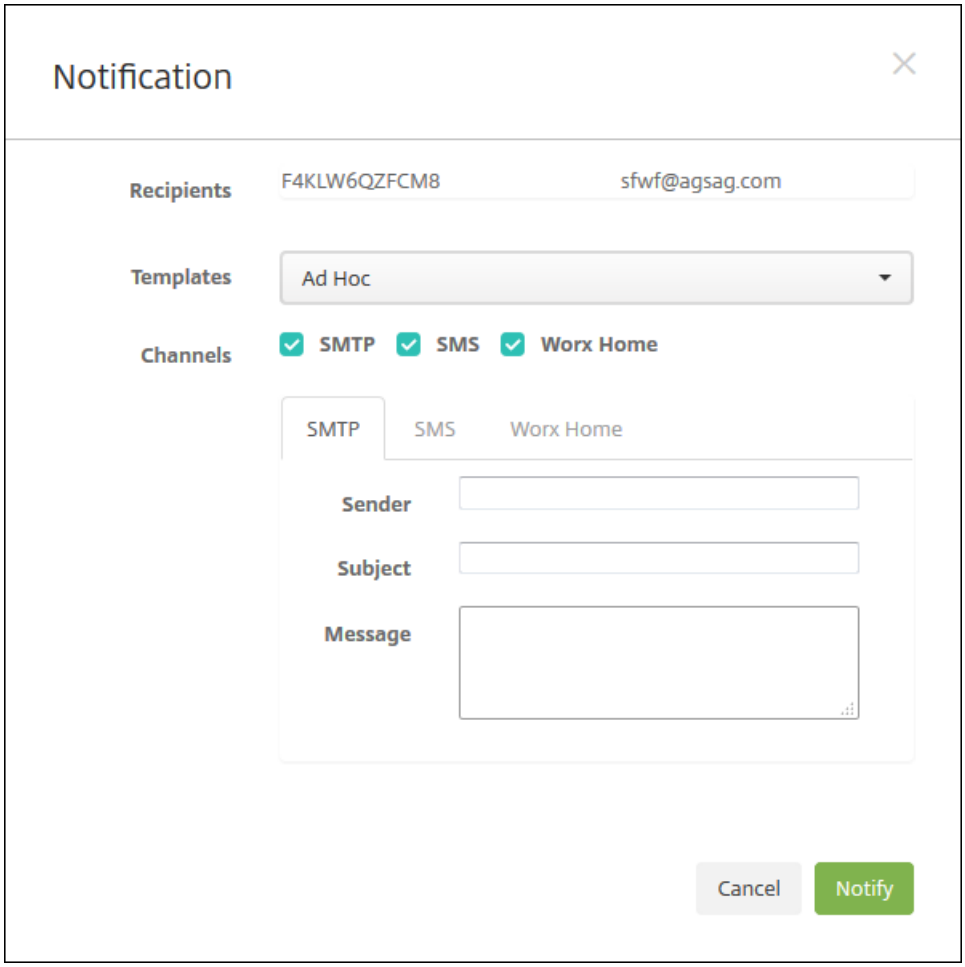
向设备发送通知

您可以从设备页面向设备发送通知。 有关通知的详细信息，请参阅在 XenMobile 中创建或更新通知模板

1. 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**字段中列出要接收通知的所有设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 配置以下设置：

- **模板**：在列表中，单击要发送的通知类型。 **主题**和**消息**字段中将填充为所选模板配置的文本，**临时**除外。
- **通道**：选择发送消息的方式。 默认值为 **SMTP**、**SMS** 和 **Worx Home**。 可以单击 **SMTP**、**SMS** 和 **Worx Home** 选项卡以查看每种方式的消息格式。
- **发件人**：输入可选发件人。
- **主题**：输入**临时**消息的主题。
- **消息**：输入**临时**消息的消息。

4. 单击**通知**。

删除设备

1. 在设备表格中，选择要删除的一个或多个设备。
2. 单击删除。 此时将显示确认对话框。 再次单击删除。
   重要：此操作无法撤消。

导出设备表

1. 单击**设备**表上方的**导出**按钮。 XenMobile 提取设备表中的信息，并将其转换为 .csv 文件。

2. 打开或保存 .csv 文件。 执行此操作的方式取决于所使用的浏览器。 您也可以取消此操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

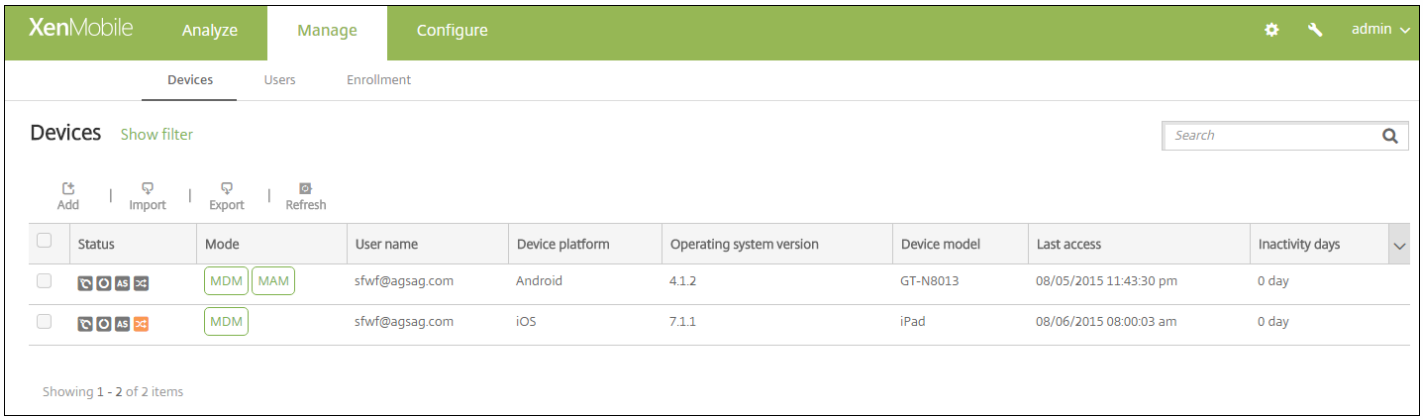
锁定 iOS 设备

Aug 11, 2016

您可以锁定 iOS 设备，同时在设备锁定屏幕上显示消息和电话号码。 iOS 7 和 8 设备支持此功能。

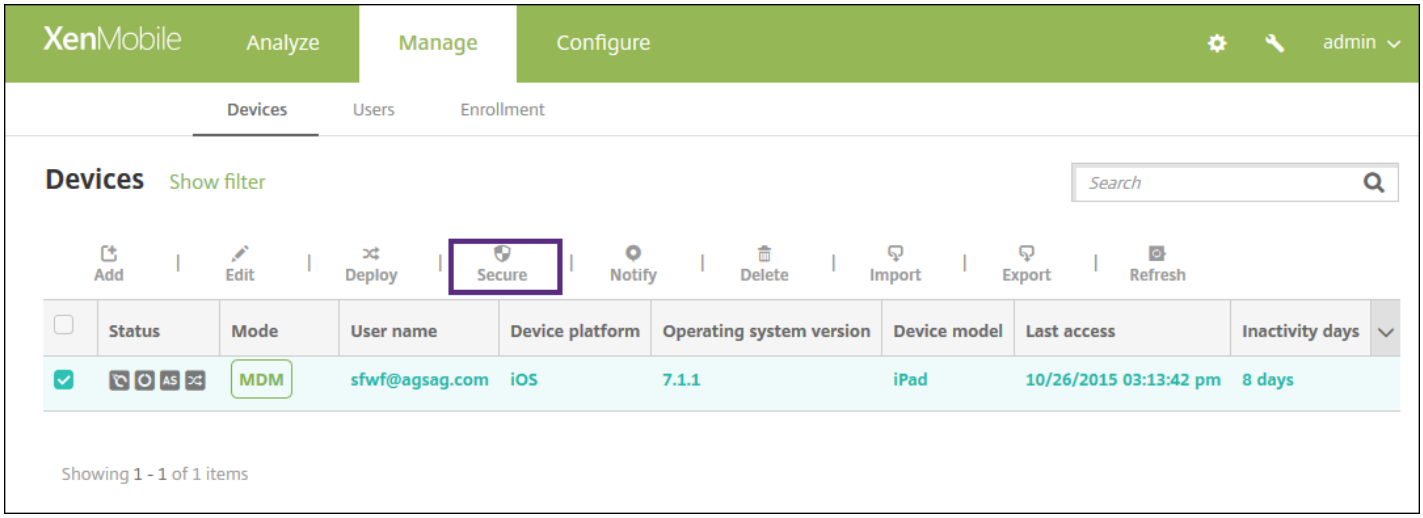
如果选择在锁定屏幕上显示消息和电话号码，同时，如果您在 XenMobile 控制台中设置了通行码策略，或者如果用户已在设备上手动启用通行码，消息和电话号码将仅显示在锁定设备上。

1. 在 XenMobile 控制台中，单击**管理 > 设备**。 此时将显示**设备**页面。

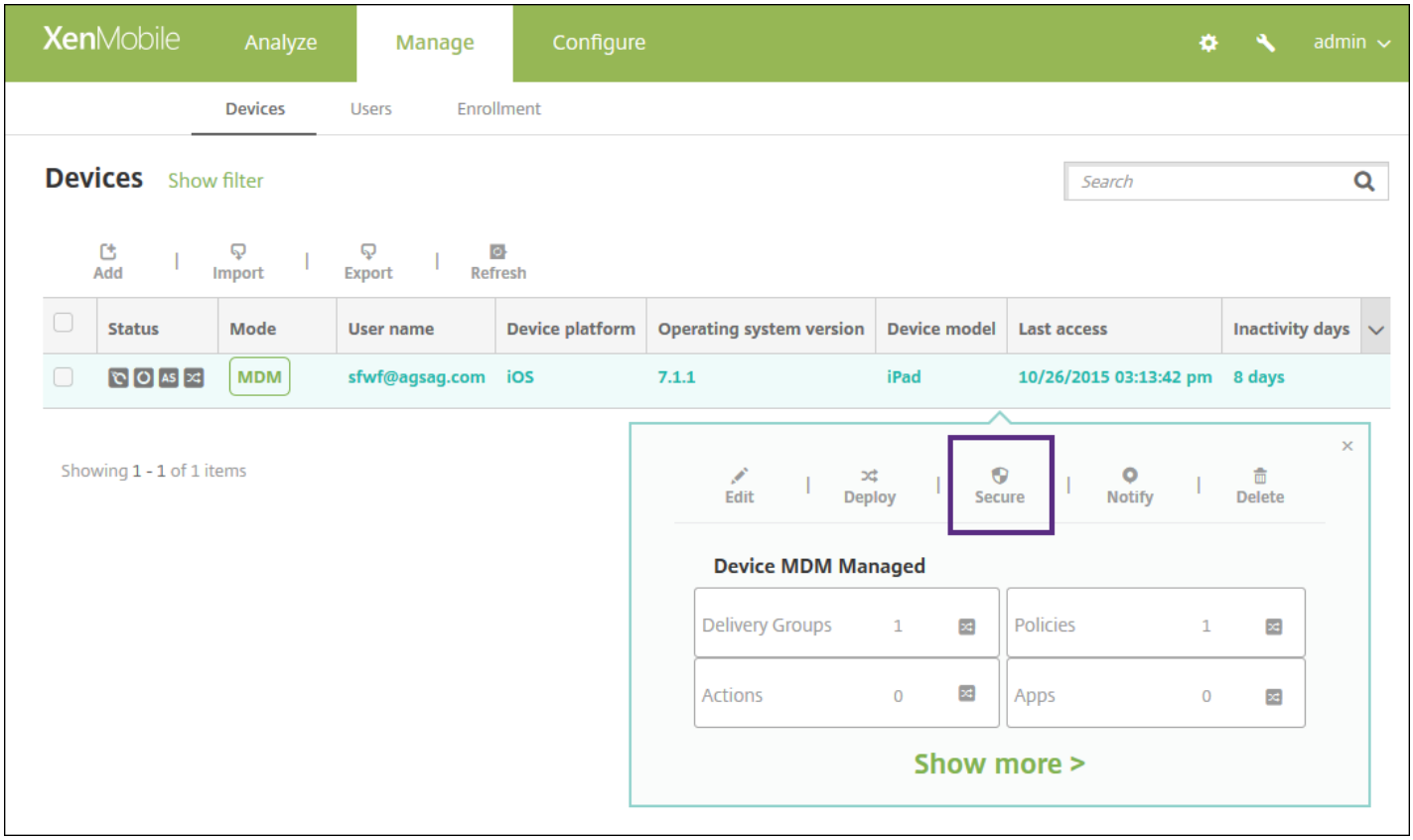


2. 选择要锁定的 iOS 设备。

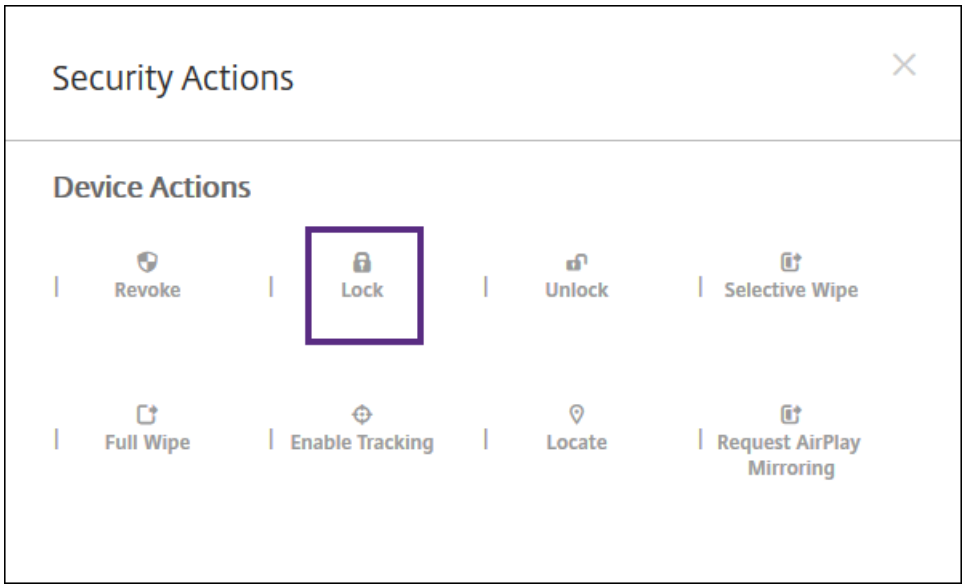
如果选中某个设备旁边的复选框，选项菜单将显示在设备列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

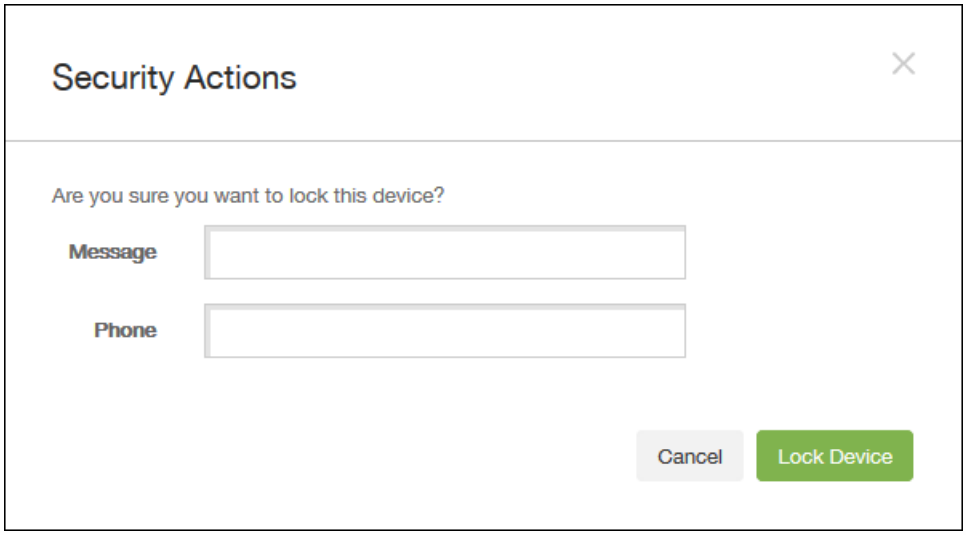


3. 在选项菜单中，选择**安全**。 此时将显示**安全操作**对话框。



4. 选择**锁定**。 此时将显示**安全操作**确认对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5.（可选）输入将显示在设备锁定屏幕上的消息和电话号码。

6. 单击**锁定设备**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

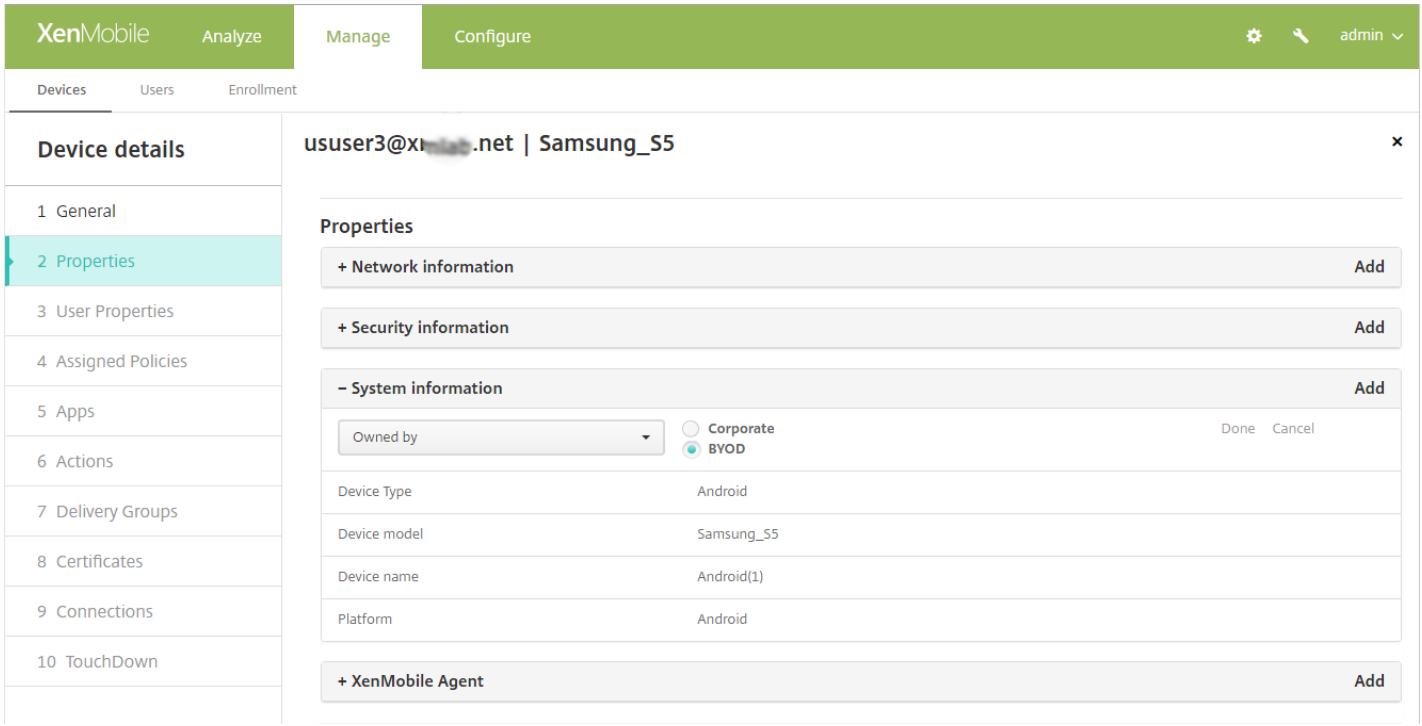
手动标记用户设备

Aug 11, 2016

可以在 XenMobile 中通过以下方式手动标记设备：

- 在基于邀请的注册过程中。
- 在自助服务门户注册过程中。
- 通过添加设备所有权作为设备属性

您可以选择将设备标记为公司所有或员工所有。 使用自助门户自助注册设备时，也可以将设备标记为公司所有或员工所有。 如下图所示，您也可以通过从 XenMobile 控制台中的**设备**选项卡向设备添加某个属性，添加名为**所有者**的属性，然后选择**公司**或**BYOD**（员工所有），来手动标记设备。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备置备文件格式

Aug 11, 2016

许多移动运营商或设备制造商都提供了授权移动设备的列表，可以利用这些列表来避免手动输入冗长的移动设备列表。XenMobile 支持以下三个受支持设备类型通用的导入文件格式：Android、iOS 和 Windows。

手动创建并用于将设备导入 XenMobile 的置备文件必须采用以下格式：

> 序列号;IMEI;操作系统系列;属性名1;属性值1;属性名2;属性值2; ... 属性名N;属性值N

注意：

- 文件字符集必须是 UTF-8。
- 置备文件中的字段使用分号 (;) 隔开。 如果某个字段的某一部分包含分号，则必须使用反斜杠字符 (\) 进行转义。 例如，在置备文件中，属性 propertyV;test;1;2 应 按照 propertyV\;test\;1\;2 形式输入。
- 如果未提供 IMEI，则“序列号”为必填项。
- 对于 iOS 设备，必须提供序列号，因为序列号是 iOS 设备标识符。
- 如果未提供序列号，则 IMEI 为必填项。
- 操作系统系列的有效值 包括： WINDOWS、ANDROID 或 iOS。

设备置备文件示例

设备置备文件中的以下每行均描述一个设备。

1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

第一个条目的含义如下：

- 序列号：1050BF3F51730108161006551059039 1
- IMEI：15244201625379901
- 操作系统系列：WINDOWS
- 属性名：propertyN
- 属性值：propertyV\;test\;1\;2;prop 2

© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备策略

Oct 21, 2016

可以通过创建策略，配置 XenMobile 与您的设备结合使用的方式。 尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。 因此，您可能会发现 iOS、Android 和 Windows 设备之间的差异，甚至运行 Android 的不同制造商的设备之间也存在差异。 有关按平台列出的策略列表，请参阅 XenMobile 设备策略（按平台）。

在创建新策略之前，请确保完成以下步骤：

- 创建计划使用的交付组。
- 安装所有必需的 CA 证书。

创建设备策略的基本步骤如下：

1. 为策略命名并添加说明。
2. 配置一个或多个平台。
3. 创建部署规则（可选）。
4. 将策略分配到交付组。
5. 配置部署计划（可选）。

可以在 XenMobile 中配置以下设备策略。

设备策略名称	**设备策略说明**
AirPlay 镜像	您可以在 XenMobile 中添加一个设备策略，从而将特定 AirPlay 设备（如 Apple 电视或其他 Mac 计算机）添加到用户的 iOS 设备。 您还可以将设备添加到受监督设备的白名单，从而使用户仅限于白名单上的 AirPlay 设备。
AirPrint	AirPrint 设备策略允许您向用户 iOS 设备上的 AirPrint 打印机列表添加 AirPrint 打印机。 这样可以更加轻松地为打印机和设备位于不同子网的环境提供支持。 注意： - 此策略适用于 iOS 7.0 及更高版本。 - 请确保知道每个打印机的 IP 地址和资源路径。
Android for Work 应用程序限制	此策略允许您修改与 Android for Work 应用程序关联的限制，但是在执行此操作前，必须满足以下必备条件： - 在 Google 上完成 Android for Work 设置任务。 有关详细信息，请参阅使用 Android for Work 管理设备。 - 创建一组 Google Play 凭据。 有关详细信息，请参阅 Google Play 凭据。 - 创建 Android for Work 帐户。 有关详细信息，请参阅创建 Android for Work 帐户。 - 将 Android for Work 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。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

APN	如果贵组织不使用客户 APN 从移动设备连接到 Internet，可以使用此策略。 APN 策略确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。 大多数新式电话中已经定义此设置。
应用程序访问权限	利用 XenMobile 中的“用程序访问”设备策略，可以定义需要安装到设备上、可以安装到设备上或不得安装到设备上的应用程序列表。 然后，可以创建自动化操作，以使设备符合此应用程序列表。
应用程序属性	如果在“设置”>“服务器属性”中配置了计划后台部署密钥，则适用此选项。 始终启用选项不适用于 iOS 设备。
应用程序配置	利用此策略，您可以远程配置可支持托管配置的 App Store 应用程序，方法是向用户的 iOS 设备部署一个 XML 配置文件（称为属性列表或 plist）以配置应用程序中的各种设置和行为。
应用程序清单	利用“应用程序清单”策略，您可以收集托管设备上应用程序的清单，然后根据该清单对比部署到这些设备上的任何应用程序访问策略。 这样，您可以发现出现在应用程序黑名单（在应用程序访问策略中禁止）或白名单（在应用程序访问策略中需要）上的应用程序，并采取相应的操作。
应用程序锁定	可以在 XenMobile 中创建一个策略，用于定义允许在设备上运行的应用程序列表，或阻止在设备上运行的应用程序列表。 可以同时为 iOS 和 Android 设备配置此策略，但策略具体的执行方式则因平台而异。 例如，不能阻止在 iOS 设备上运行多个应用程序。 注意：虽然设备策略在大多数 Android L 和 M 设备上起作用，但由于 Google 弃用了所需的 API，因此，应用程序锁定策略在 Android N 或更高版本的设备上不起作用。 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一个应用程序。 在强制执行应用程序锁定策略时，用户无法在设备上执行除您明确允许的选项之外的任何其他活动。
应用程序网络使用	您可以设置网络使用规则，以指定 iOS 设备上托管应用程序使用网络（如手机网络数据网络）的方式。 规则仅适用于托管应用程序。 托管应用程序是指您通过 XenMobile 部署到用户设备的应用程序。 其中不包括用户直接下载到设备上且未通过 XenMobile 部署的应用程序，或者在设备向 XenMobile 注册时已经安装到设备上的应用程序。
应用程序限制	通过此策略，您可以为需要阻止用户在 Samsung KNOX 设备上安装的应用程序创建黑名单，以及为希望允许用户安装的应用程序创建白名单。
应用程序通道	可以配置“应用程序通道”策略，以提高移动应用程序的服务连续性和数据传输可靠性。 应用程序通道定义移动设备应用程序的客户端组件与应用程序服务器组件之间的代理参数。 还可以使用应用程序通道创建设备的远程支持通道以使用管理支持。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	注意：通过在此策略中定义的通道发送的任何应用程序流量均先通过 XenMobile，然后再被重定向到运行此应用程序的服务器。
应用程序卸载	通过“应用程序卸载”策略，您可以因各种原因将应用程序从用户设备中删除。 原因可以是您不再想要支持某些应用程序，贵公司可能要将现有应用程序替换为其他供应商的类似应用程序等等。 当此策略部署到用户的设备时，应用程序被删除。 用户会收到卸载应用程序的提示，但是 Samsung KNOX 设备除外；Samsung KNOX 设备用户不会收到卸载应用程序的提示。
应用程序卸载限制	利用此策略，您可以指定用户可以或无法卸载的应用程序。
浏览器	可以创建浏览器设备策略以定义用户设备是否可以使用浏览器，或限制用户设备可以使用的浏览器功能。 在 Samsung 设备上，可以完全禁用浏览器，也可以启用或禁用弹出消息、JavaScript、Cookie、自动填充和是否强制显示欺诈警告。 在 Android for Works 设备上，可以将特定 URL 列入黑名单或白名单，以及添加特定安全浏览器书签。
日历 (CalDav)	可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 或 Mac OS X 设备添加日历 (CalDAV) 帐户，使用户可以将其计划数据与任何支持 CalDAV 的服务器同步。
手机网络	该策略允许您配置手机网络设置。
连接管理器	在 XenMobile 中，可以为自动连接到 Internet 的应用程序指定连接设置并提供网络。 此策略仅适用于 Windows Pocket PC。
连接计划	此策略是必需的策略，用于使 Android 和 Windows Mobile 设备重新连接到 XenMobile 服务器以进行 MDM 管理、应用程序推送和策略部署。 如果不向下发送该策略并且未启用 Google GCM，设备将无法重新连接回服务器。 因此，请务必在基础软件包中向下推送此策略以注册设备。
联系人 (CardDAV)	可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 或 Mac OS X 设备添加 iOS 联系人 (CardDAV) 帐户，使用户可以将其联系人数据与任何支持 CardDAV 的服务器同步。
将应用程序复制到 Samsung 容器	可以指定将已安装在设备上的应用程序复制到 SEAMS 容器，或复制到受支持的 Samsung 设备上的 KNOX 容器。 复制到 SEAMS 容器的应用程序在用户的主屏幕上可用；复制到 KNOX 容器的应用程序仅当用户登录 KNOX 容器时可用。
凭据	可以在 XenMobile 中创建凭据设备策略，以使用 XenMobile 中的 PKI 配置启用集成身份验证，例如 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 XenMobile 中的证书。 每种设备平台都需要一组不同的值，“凭据策略”一文将对此进行介绍。 注意：创建此策略前，需要具有计划用于各平台的凭据信息，以及任何证书和密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

将应用程序复制到 Samsung 容器	可以指定将已安装在设备上的应用程序复制到 SEAMS 容器，或复制到受支持的 Samsung 设备上的 KNOX 容器。 有关支持的设备的信息，请参阅 Samsung 文章支持 Samsung KNOX 的设备。 复制到 SEAMS 容器的应用程序在用户的主屏幕上可用；复制到 KNOX 容器的应用程序仅当用户登录 KNOX 容器时可用。
凭据	此策略常与 WiFi 策略结合使用，允许公司向需要证书身份验证的内部资源部署证书以进行身份验证。
自定义 XML	当您需要自定义以下功能时，可以在 XenMobile 中创建自定义 XML 策略： • 置备，包括配置设备以及启用或禁用功能 • 设备配置，包括允许用户更改设置和设备参数 • 软件升级，包括提供要加载到设备中的新软件或缺陷修复（包括应用程序和系统软件） • 故障管理，包括接收来自设备的错误和状态报告 可以在 Windows 中使用 Open Mobile Alliance Device Management (OMA DM) API 创建自己的自定义 XML 配置。 本主题中不介绍如何使用 OMA DM API 创建自定义 XML。 有关使用 OMA DM API 的详细信息，请参阅 Microsoft Developer Network 站点上的 OMA 设备管理。
删除文件和文件夹	可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的文件或文件夹。
删除注册表项和值	可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的注册表项和值。
设备运行状况证明	在 XenMobile 中，您可以创建一个策略，以要求 Windows 10 设备报告其运行状况，方法是让这些设备将特定数据和运行时信息发送给 Health Attestation Service (HAS) 进行分析。 HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 XenMobile。 XenMobile 收到运行状况证明证书后，根据运行状况证明证书的内容，部署您之前设置的自动操作。 HAS 验证的数据包括： • AIK 是否存在 • Bit Locker 状态 • 启动调试是否已启用 • 启动管理器修订列表版本 • 代码完整性是否已启用 • 代码完整性修订列表版本 • DEP 策略 • ELAM 驱动程序是否已加载 • 颁发时间 • 内核调试是否已启用 • PCR • 重置计数 • 重新启动计数

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	• 安全模式是否已启用 • SBCP 哈希 • 安全启动是否已启用 • 测试签名是否已启用 • 已启用 VSM • 已启用 WinPE 有关详细信息，请参阅 Microsoft HealthAttestation CSP 页面。
设备名称	利用“设备名称”策略，您可以设置 iOS 和 Mac OS X 设备上的名称，以便轻松识别设备。 可以使用宏、文本或二者的组合定义设备的名称。 有关宏的详细信息，请参阅 XenMobile 中的宏。
企业 Hub	面向 Windows Phone 的企业中心设备策略允许您通过企业中心公司应用商店分发应用程序。 需要具备以下各项才能创建策略： • 来自 Symantec 的 AET (.aetx) 签名证书 • 使用 Microsoft 应用程序签名工具 (XapSignTool.exe) 签名的 Citrix Company Hub 应用程序 注意：对于一种 Windows Phone Worx Home 模式，XenMobile 仅支持一种企业中心策略。 例如，要上载 Windows Phone Worx Home for XenMobile Enterprise Edition，不应该使用不同版本的 Work Home for XenMobile Enterprise Edition 创建多个企业中心策略。 设备注册期间只能部署初始企业 Hub 策略。
Exchange	在 XenMobile 中，您可以使用两个选项传递电子邮件。 可以使用容器化 WorxMail 应用程序传递 ActiveSync 电子邮件，或者也可以使用此 MDM Exchange 策略为设备上的本地电子邮件客户端启用 ActiveSync 电子邮件。
文件	通过此策略，您可以在 XenMobile 中为用户添加执行某些功能的脚本文件，或者也可添加 Android 设备用户能够在其设备上访问的文档文件。 添加文件时，还可以指定设备上要存储该文件的目录。 例如，如果您希望 Android 用户接收公司文档或 .pdf 文件，则可以将该文件部署到设备，然后将文件位置告知用户。 利用此策略可以添加以下文件类型： • 文本文件（.xml、.html、.py 等） • 其他文件，如文档、图片、电子表格或演示文稿 • 仅适用于 Windows Mobile 和 Windows CE：通过 MortScript 创建的脚本文件
字体	可以在 XenMobile 中添加此设备策略，以向用户的 iOS 和 Mac OS X 设备添加其他字体。 字体必须是 TrueType (.ttf) 或 OpenType (.oft) 字体。 不支持字体集合（.ttc 或 .otc）。 注意：对于 iOS，此策略仅适用于 iOS 7.0 及更高版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

导入 iOS 和 Mac OSx 配置文件	可以将 iOS 和 OS X 设备的设备配置 XML 文件导入到 XenMobile 中。 此文件包含您使用 Apple Configurator 准备的设备安全策略和限制。 有关使用 Apple Configurator 创建配置文件的详细信息，请参阅 Apple Configurator 页面。
是否需要 Kiosk	可以在 XenMobile 中创建 Kiosk 策略以便能够指定只能在 Samsung SAFE 设备上使用一个或多个特定的应用程序。 此策略对旨在仅运行特定类型或类别的应用程序的企业设备非常有用。 此策略还允许您为设备选择处于 Kiosk 模式时设备主屏幕和锁屏界面墙纸使用的自定义图片。 注意： • 为 Kiosk 模式指定的所有应用程序必须已安装在用户设备上。 • 某些选项仅适用于 Samsung Mobile Device Management API (MDM) 4.0 及更高版本。
LDAP	可以在 XenMobile 中为 iOS 设备创建 LDAP 策略，以提供与要使用的 LDAP 服务器有关的信息，包括任何必要的帐户信息。 此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。 配置此策略之前，您需要提供 LDAP 主机名。
位置	位置策略可用于在地图上对设备进行地理定位（假定该设备已为 WorxHome 启用 GPS）。 一旦将此策略下推到设备，管理员就可以从 XenMobile 服务器发送定位命令，并且设备将使用其位置坐标进行回应。 也支持地理围栏和跟踪策略。
邮件	可以在 XenMobile 中添加邮件设备策略以在用户的 iOS 或 Mac OX X 设备上配置电子邮件帐户。
托管域	可以通过此策略定义将应用到电子邮件和 Safari 浏览器的托管域。 托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护企业数据。 指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。 此策略仅在 iOS 8 及更高版本的受监督设备上可用。 有关将 iOS 设备置于受监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。 用户向域不在托管电子邮件域列表上的收件人发送电子邮件时，在用户的设备上此邮件将带有标记，以警告用户正在向企业域外部的人员发送邮件。 当用户尝试使用 Safari 从位于托管 Web 域列表上的 Web 域打开某个项目（文档、附件或下载内容）时，将由合适的企业应用程序打开此项目。 如果此项目所在的 Web 域不在托管 Web 域列表上，用户无法使用合适的企业应用程序打开此项目；他们必须使用未托管的个人应用程序。
Microsoft Exchange ActiveSync	可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以允许其访问 Exchange 上托管的企业电子邮件。 每种平台需要一组不同的值，本节的 Microsoft Exchange ActiveSync 文章中详细介绍了相关内容。
MDM 选项	可以在 XenMobile 中创建一个设备策略，用于在受监督的 iOS 7.0 及更高版本的手机设备上管理“查找我的 iPhone/iPad 激活锁”。 有关将 iOS 设备设置为受监督模式的步骤，请参阅使用

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Apple Configurator 将 iOS 设备置于受监督模式或 iOS 批量注册。 激活锁是一项“查找我的 iPhone/iPad”功能，目的是在任何人都可以关闭“查找我的 iPhone”、擦除设备或重新激活并使用设备之前，通过要求提供用户的 Apple ID 和密码阻止重新激活丢失或失窃的设备。 在 XenMobile 中，可以通过在 MDM 选项设备策略中启用激活锁，跳过 Apple ID 和密码要求。 当用户返回已启用“查找我的 iPhone”功能的设备时，您无需具有其 Apple 凭据便可以从 XenMobile 控制台管理此设备。
组织信息	可以在 XenMobile 中添加设备策略以指定贵组织从 XenMobile 推送到 iOS 设备的警报消息信息。 此策略适用于 iOS 7 及更高版本的设备。
需要通行码	通行码策略允许您在托管设备上强制执行 PIN 码或密码。 此通行码策略允许您为设备上的通行码设置复杂性和超时。
个人热点	通过此策略，可允许不在 WiFi 网络范围内的用户通过其 iOS 设备的个人热点功能，使用手机数据网络来连接到 Internet。 iOS 7.0 及以上版本支持此功能。
配置文件删除	可以在 XenMobile 中创建应用程序配置文件删除设备策略。 此策略在部署时，将从用户的 iOS 或 Mac OS X 设备删除应用程序配置文件。
置备配置文件	开发或代码签名 iOS 企业应用程序时，通常包含企业分发置备配置文件，Apple 需要此配置文件才能允许应用程序在 iOS 设备上运行。 如果置备配置文件缺失或已过期，用户轻按应用程序以将其打开时，应用程序将崩溃。 置备配置文件的主要问题是，它们在 Apple 开发人员门户上生成一年之后将过期，您必须跟踪用户注册的所有 iOS 设备上的所有置备配置文件的过期日期。 跟踪过期日期不仅涉及到跟踪实际的过期日期，还要跟踪每个用户正在使用的应用程序版本。 有两个解决方案：通过电子邮件向用户发送置备配置文件，或者将其放在 Web 门户上供下载和安装。 这些解决方案可行，但容易出错，因为需要用户响应电子邮件中的说明，或访问 Web 门户并下载正确的配置文件，然后再进行安装。 要使此过程对用户透明，您可以在 XenMobile 使用设备策略来安装和删除置备配置文件。 在必要时删除缺失或过期的置备配置文件并在用户设备上安装最新的配置文件，这样一来，只需轻按应用程序，即可将其打开并使用。
删除置备配置文件	您可以通过设备策略删除 iOS 置备配置文件。 有关置备配置文件的详细信息，请参阅添加置备配置文件。
代理	可以在 XenMobile 中添加一个设备策略，为运行 Windows Mobile/CE 和 iOS 6.0 或更高版本的设备指定全局 HTTP 代理设置。 只能为每个设备部署一个全局 HTTP 代理策略。 注意：在部署此策略之前，请务必将要为其设置全局 HTTP 代理的所有 iOS 设备设置为“受监督”模式。 有关详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注册表	Windows Mobile/CE 注册表存储关于应用程序、驱动器、用户首选项和配置设置的数据。 在 XenMobile 中，可以定义用于管理 Windows Mobile/CE 设备的注册表项和值。
远程支持	可以在 XenMobile 中创建远程支持策略以授予远程访问用户的 Samsung KNOX 设备所需的权限。 可以配置两种类型的支持： • 基本：使用此选项，您可以查看与设备有关的诊断信息（例如系统信息）、正在运行的进程、任务管理器（内存和 CPU 使用率）、已安装的软件文件夹内容等。 • 高级：此选项允许您远程控制设备的屏幕，包括控制颜色（在主窗口中或者在独立的浮动窗口中）、在技术支持人员与用户之间建立 VoIP 会话、配置设置以及在技术支持人员与用户之间建立聊天会话的功能。
限制	限制策略允许管理员使用许多选项来锁定和控制托管设备上的特性和功能。 可对支持设备使用数以百计的限制选项，其用途包括禁用设备上的摄像头或麦克风、对第三方服务（类似应用商店）执行漫游规则和访问，等等 可以在 XenMobile 中添加一个设备策略，以限制用户设备、手机、平板电脑等设备上的某些功能或特征。 每种平台需要一组不同的值，本文将对此进行介绍。 此策略允许或限制用户在其设备上使用某些功能，例如相机。 您还可以设置安全限制、对媒体内容的限制以及对用户能够和不能安装的应用程序类型的限制。 大多数限制设置的默认值为“开”或允许。 主要的例外情况是 iOS 安全 - 强制功能和所有 Windows 平板电脑功能，其默认设置为“关”或限制。 提示：如果您为任何选项选择“开”，则意味着用户可以执行该操作或使用该功能。 例如： • 相机。 如果选择“开”，则用户可以在其设备上使用相机。 如果选择“关闭”，则用户无法在其设备上使用相机。 • 屏幕快照。 如果选择“开”，则设备用户可以在其设备上创建屏幕快照。 如果选择“关”，则设备用户无法在其设备上创建屏幕快照。
漫游	可以在 XenMobile 中添加一个设备策略，以配置在用户 iOS 和 Windows Mobile/CE 设备上是否允许语音和数据漫游。 禁用语音漫游时，会自动禁用数据漫游。 对于 iOS，此策略仅适用于 iOS 5.0 及更高版本的设备。
Samsung SAFE 防火墙	利用此策略可以为 Samsung 设备配置防火墙设置。 输入允许设备访问或阻止设备访问的 IP 地址、端口和主机名。 还可以配置代理和代理重新路由设置。
Samsung MDM 许可证密钥	XenMobile 支持并扩展了 Samsung for Enterprise (SAFE) 和 Samsung KNOX 策略。 SAFE 是一个解决方案系列，它通过与移动设备管理解决方案集成为业务使用提供安全性和增强功能。 Samsung KNOX 属于提供更安全的 Android 平台以供企业使用的 SAFE 计划中的一种解决方案。 必须通过向设备部署内置 Samsung Enterprise License Management (ELM) 密钥来启用 SAFE API，才能部署 SAFE 策略和限制。 要启用 Samsung KNOX API，除部署 Samsung ELM 密钥外，还需要使用 Samsung KNOX License Management System (KLMS) 购买 Samsung KNOX 许可证。 Samsung KLMS 为移动设备管理解决方案提供有效的许可证，以使其能够在移动设

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	备上激活 Samsung KNOX API。 必须从 Samsung 获取这些许可证，Citrix 不提供。 要启用 SAFE 和 Samsung KNOX API，必须部署 Worx Home 以及 Samsung ELM 密钥。 可以通过检查设备属性来验证是否已启用 SAFE API。 部署 Samsung ELM 密钥时，将 Samsung MDM API 可用性设置为 True。
SCEP	利用此策略，可以将 iOS 和 Mac OS X 设备配置为使用简单证书注册协议 (SCEP) 从外部 SCEP 服务器检索证书。 如果希望从连接到 XenMobile 的 PKI 向使用 SCEP 的设备交付证书，应采用分布式模式创建 PKI 实体和 PKI 提供程序。 有关详细信息，请参阅 PKI 实体。
旁加载密钥	借助 XenMobile 中的旁加载，您可以在 Windows 8.1 设备上部署还未从 Windows 应用商店中购买的应用程序。 需要旁加载应用程序的最常见情况是，您不希望在 Windows 应用商店中公开为企业开发的应用程序。 要旁加载应用程序，需要配置旁加载密钥和密钥激活，然后再将应用程序部署到用户的设备。 创建此策略之前，需要提供以下信息： ● 旁加载产品密钥，需要登录 Microsoft Volume Licensing Service Center（Microsoft 批量许可服务中心）获取此信息 ● 密钥激活，需要在获取旁加载产品密钥之后通过命令行创建
签署证书	可以在 XenMobile 中添加一个设备策略，以配置用于签署 APPX 文件的签名证书。 如果要向用户分发 APPX 文件以允许用户在其 Windows 平板电脑上安装应用程序，需要使用签名证书。
Single Sign On (SSO) 帐户	在 XenMobile 中创建 Single Sign-On (SSO) 帐户，使用户只需登录设备一次，即可从各种应用程序访问 XenMobile 和内部的公司资源。 用户无需在设备上存储任何凭据。 可以跨应用程序（包括 App Store 中的应用程序）使用此 SSO 帐户企业用户凭据。 此策略专为 Kerberos 身份验证后端设计。 注意：此策略仅适用于 iOS 7.0 及更高版本。
存储加密	在 XenMobile 中创建存储加密设备策略，以加密内部存储和外部存储，并根据设备阻止用户在其设备上使用存储卡。 可以创建适用于 Samsung SAFE、Windows Phone 和 Android Sony 设备的策略。 每个平台需要一组不同的值，相关内容将在本节的“存储加密策略”文章中详细介绍。
订阅日历	您可以在 XenMobile 中添加一个设备策略，以便在用户的 iOS 设备上向日历列表中添加已订阅的日历。 www.apple.com/downloads/macosx/calendars 提供了您可以订阅的公共日历列表。 注意：必须已经订阅某个日历，才能将其添加到用户设备上已订阅的日历列表中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

条款和条件	如果希望用户接受贵公司用于控制企业网络连接的特定政策，可以在 XenMobile 中创建“条款和条件”设备策略。 当用户向 XenMobile 注册其设备时，系统会向其显示条款和条件，用户必须接受这些条款和条件才能注册其设备。 拒绝这些条款和条件会取消注册过程。 如果贵公司具有国际用户，并且希望用户接受采用其本地语言描述的条款和条件，则可以采用不同的语言创建不同的条款和条件策略。 必须为计划部署的每个平台和语言组合提供一个文件。 对于 Android 和 iOS 设备，必须提供 PDF 文件。 对于 Windows 设备，必须提供文本 (.txt) 文件和随附的图像文件。
VPN	对于希望使用旧版 VPN 网关技术提供后端系统访问功能的客户，此 VPN 策略可用于向设备下推 VPN 网关连接详细信息。 通过其中包括 Cisco AnyConnect、Juniper 及 Citrix VPN 的策略，可支持许多 VPN 提供商。 此外，也可以将策略链接到 CA 并按需启用 VPN（假定 VPN 网关支持此选项）。 可以在 XenMobile 中添加用于配置虚拟专用网络 (VPN) 设置的设备策略，使用户设备安全地连接到企业网络。 每种平台需要使用一组不同的值，本节的 VPN 文章中详细介绍了相关内容。
墙纸	您可以添加 .png 或 .jpg 文件，以设置 iOS 设备锁屏界面、主屏幕或二者的墙纸。 适用于 iOS 7.1.2 及更高版本。 要在 iPad 和 iPhone 上使用不同的墙纸，需要创建不同的墙纸策略并将其部署到相应的用户。
Web 内容过滤器	可以在 XenMobile 中添加一个设备策略，通过结合使用 Apple 的自动过滤功能和添加到白名单和黑名单中的特定站点，在 iOS 设备上过滤 Web 内容。 此策略仅适用于采用受监督模式的 iOS 7.0 及更高版本。 有关将 iOS 设备置于“受监督”模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。
Web 剪辑	利用此策略，您可以向 Web 站点中放置快捷方式或 Web 剪辑，使它们和应用程序一起出现在用户的设备上。 您可以指定自己的图标来表示 iOS、Mac OS X 和 Android 设备的 Web 剪辑；Windows 平板电脑只需要使用标签和 URL。
WiFi	通过 WiFi 策略，管理员可以向托管设备轻松推送 WiFi 路由器详细信息 - SSID、身份验证和配置数据。 利用 WiFi 策略，可以通过为所选设备平台上的所有用户一致定义网络名称和类型、身份验证和安全策略、是否使用代理服务器和其他 WiFi 相关信息来管理用户将其设备连接到 WiFi 网络的方式。 可以为用户配置针对左侧所列的关联平台的 WiFi 设置，但是每个平台需使用不同的值，本节的 WiFi 文章中对此进行了详细描述。
Windows CE 证书	添加此设备策略以创建并从外部 PKI 向用户设备提供 Windows Mobile/CE 证书。 有关证书和 PKI 实体的详细信息，请参阅证书。
Worx Store	可以在 XenMobile 中创建一个策略，以指定 iOS、Android 或 Windows 平板电脑设备是否在设备的主屏幕上显示 Worx Store Web 剪辑。

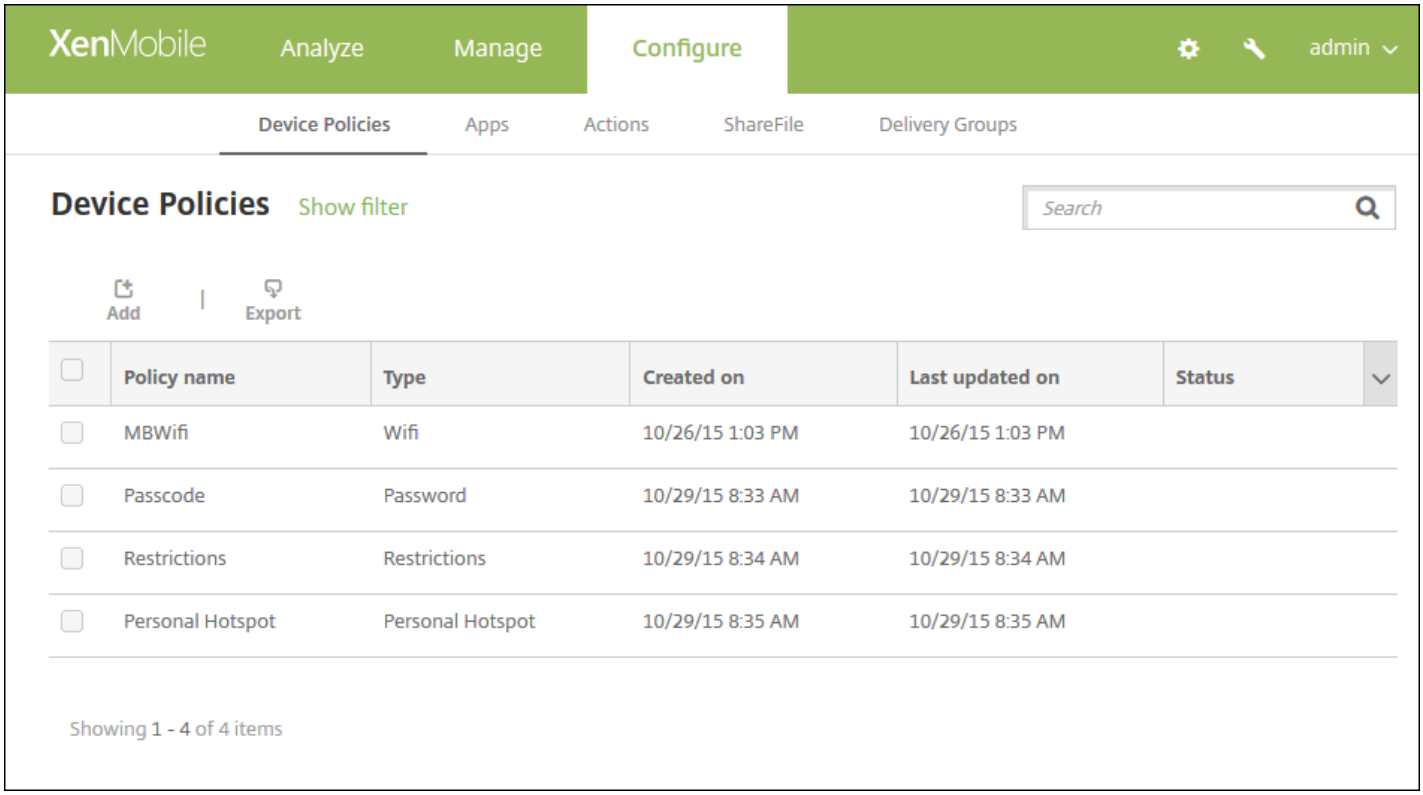
© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 选项	添加 XenMobile 选项策略，用于配置在从 Android 和 Windows Mobile/CE 设备连接到 XenMobile 时 Worx Home 的行为。
XenMobile 卸载	可以在 XenMobile 中添加此设备策略，用于从 Android 和 Window Mobile/CE 设备卸载 XenMobile。 部署此策略时，它将从部署组中的所有设备上删除 XenMobile。

控制台中的“设备策略”页面

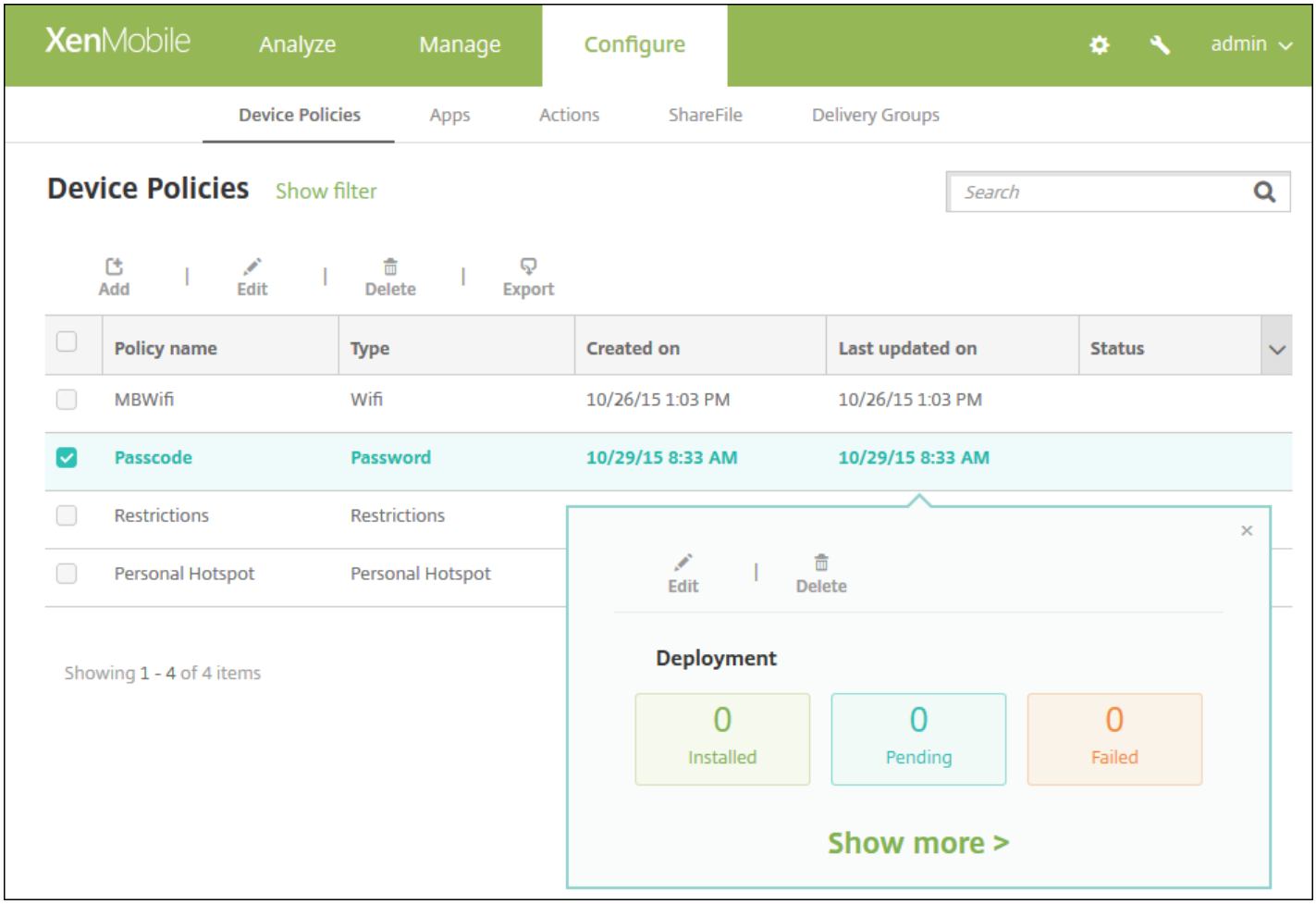
在 XenMobile 控制台**设备策略**页面处理设备策略。 要进入**设备策略**页面，请单击**配置 > 设备策略**。 在此处，可以添加新策略，查看现有策略的状态，以及编辑或删除策略。

设备策略页面包含一个表格，其中显示了当前的所有策略。



要在**设备策略**页面编辑或删除策略，可以选中策略旁边的复选框，从而在策略列表上方显示选项菜单，或者单击列表中的策略，在列表的右侧显示选项菜单。 如果单击**显示更多**，将会显示策略的详细信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



添加设备策略

1. 在**设备策略**页面上，单击**添加**。

此时将显示**添加新策略**对话框。 可以展开**更多**以查看其它策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

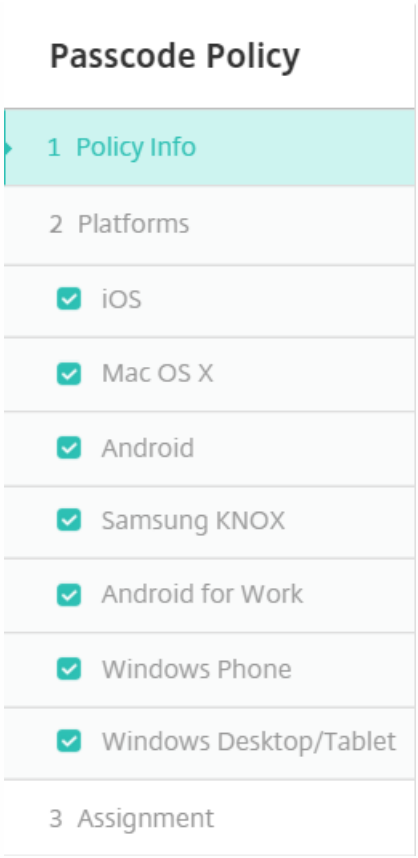
2. 查找要添加的策略，执行以下操作之一：

- 单击策略。
  此时将显示所选策略的**策略信息**页面。
- 在搜索字段中键入策略的名称。 随着键入，将显示可能的匹配项。 如果列表中存在您的策略，请单击此策略。 只有选中的策略保留在对话框中。 单击此策略以打开其**策略信息**页面。
  重要：如果选定的策略位于**更多**区域，则只有展开**更多**才会显示此策略。

3. 选择要包含在策略中的平台。 选定平台的配置页面显示在步骤 5 中。

注意：只有策略支持的平台才会被列出。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

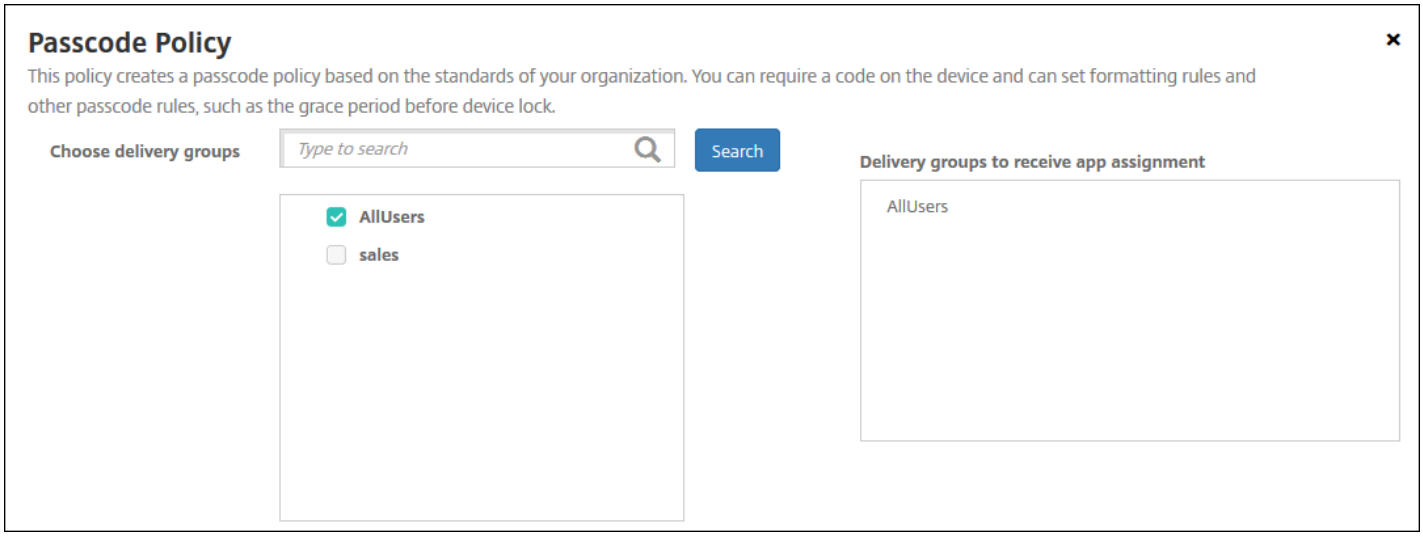


4. 完成**策略信息**页面，然后单击**下一步**。 **策略信息**页面收集策略名称等信息，以帮助您识别和跟踪自己的策略。 此页面在所有策略之间相似。

5. 完成平台页面。 显示在步骤 3 选择的每个平台的平台页面。 这些页面因策略而异。 每个策略因平台而异。 并非所有策略均受所有平台的支持。 单击**下一步**移动到下一个平台页面，或者在完成所有平台页面后移动到**分配**页面。

6. 在**分配**页面上，选择要应用此策略的交付组。 单击某个交付组时，此组将显示在**用于接收应用程序分配的交付组**框中。

注意：用于接收应用程序分配的交付组框在您选中某个交付组之后才显示。



 © 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 单击**保存**。

此策略将添加到**设备策略**表中。

编辑或删除设备策略

1. 在**设备策略**表中，选中要编辑或删除的策略旁边的复选框。

2. 单击**编辑**或**删除**。

- 如果单击**编辑**，可以编辑任意设置和所有设置。
- 如果单击**删除**，在确认对话框中，应再次单击**删除**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 设备策略（按平台）

Aug 15, 2016

要按平台查看策略，请下载 Device Policies by Platform Matrix PDF（按平台介绍的设备策略矩阵 PDF）

在 XenMobile 控制台中，可以从**配置 > 设备策略**添加和配置设备策略。
XenMobile 10.3 支持适用于以下平台的设备策略：

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Phone 8/Windows 10 Mobile
- Windows 8 和 Windows 10 Desktop/Tablet (.86)

> **注意**
>
> XenMobile 10.3 已终止对 Symbian 设备的支持。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AirPlay 镜像设备策略

Aug 15, 2016

Apple AirPlay 功能允许用户通过 Apple 电视采用流技术将 iOS 设备中的内容无线推送到电视屏幕，或将设备上显示的内容精确显示到电视屏幕或其他 Mac 计算机上。

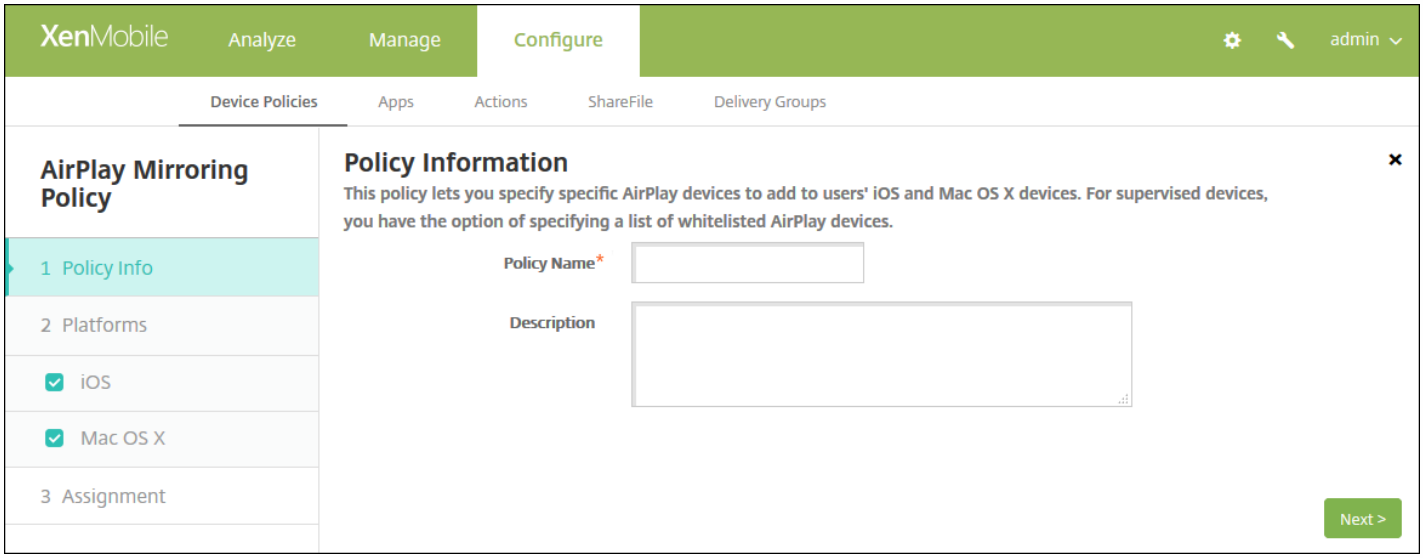
您可以在 XenMobile 中添加一个设备策略，从而将特定 AirPlay 设备（如 Apple 电视或其他 Mac 计算机）添加到用户的 iOS 设备。 您还可以将设备添加到受监督设备的白名单，从而使用户仅限于白名单上的 AirPlay 设备。 有关将设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

注意：继续操作前，请确保您具有要添加的所有设备的设备 ID 和任何密码。

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**最终用户**下面，单击 **AirPlay 镜像**。 此时将显示 **AirPlay 镜像策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

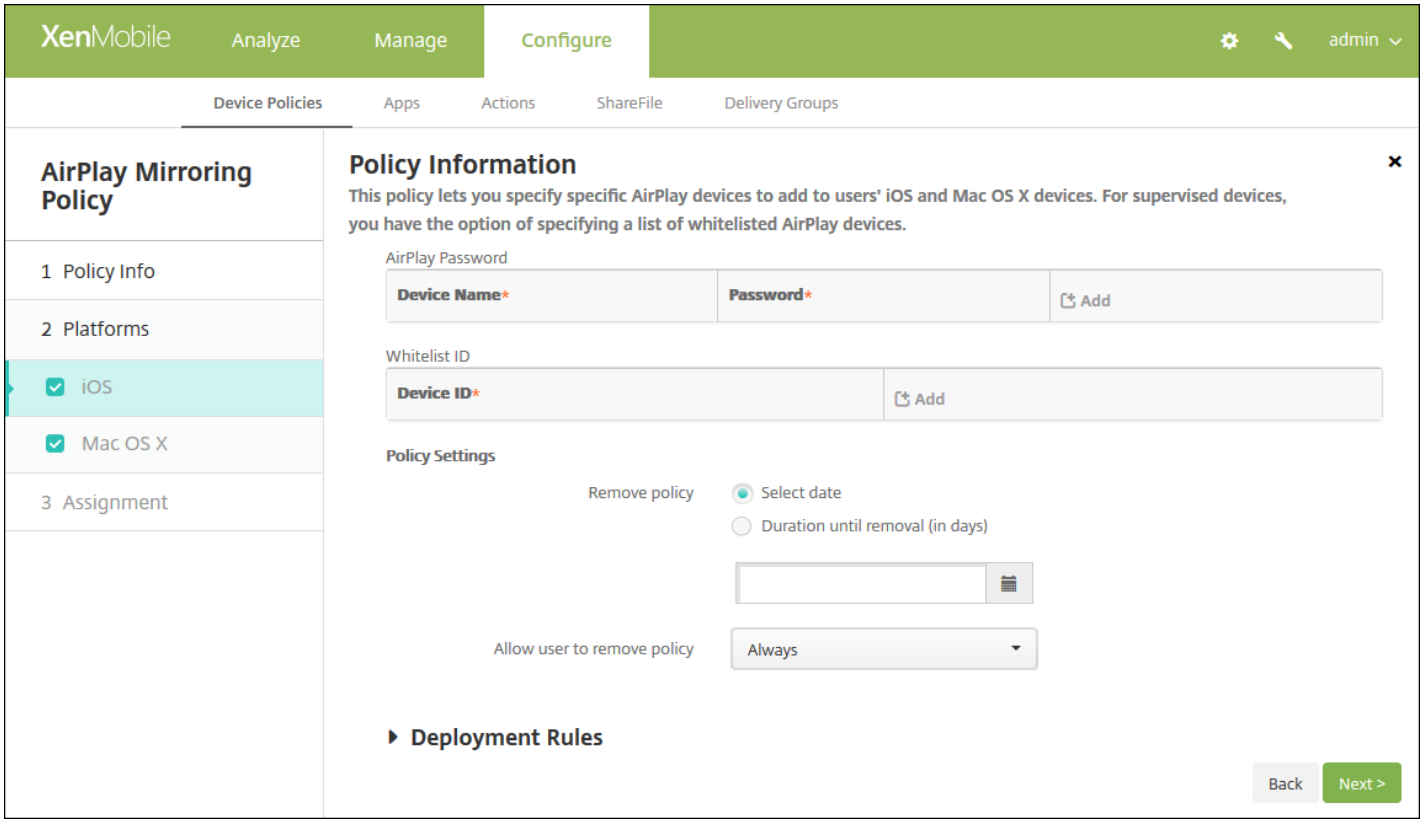
5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **AirPlay 密码**：对于您要添加的各个设备，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**：未受监督的设备请忽略此列表。 此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。 对于希望添加到此列表中的每个 AirPlay 设备，请单击**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。

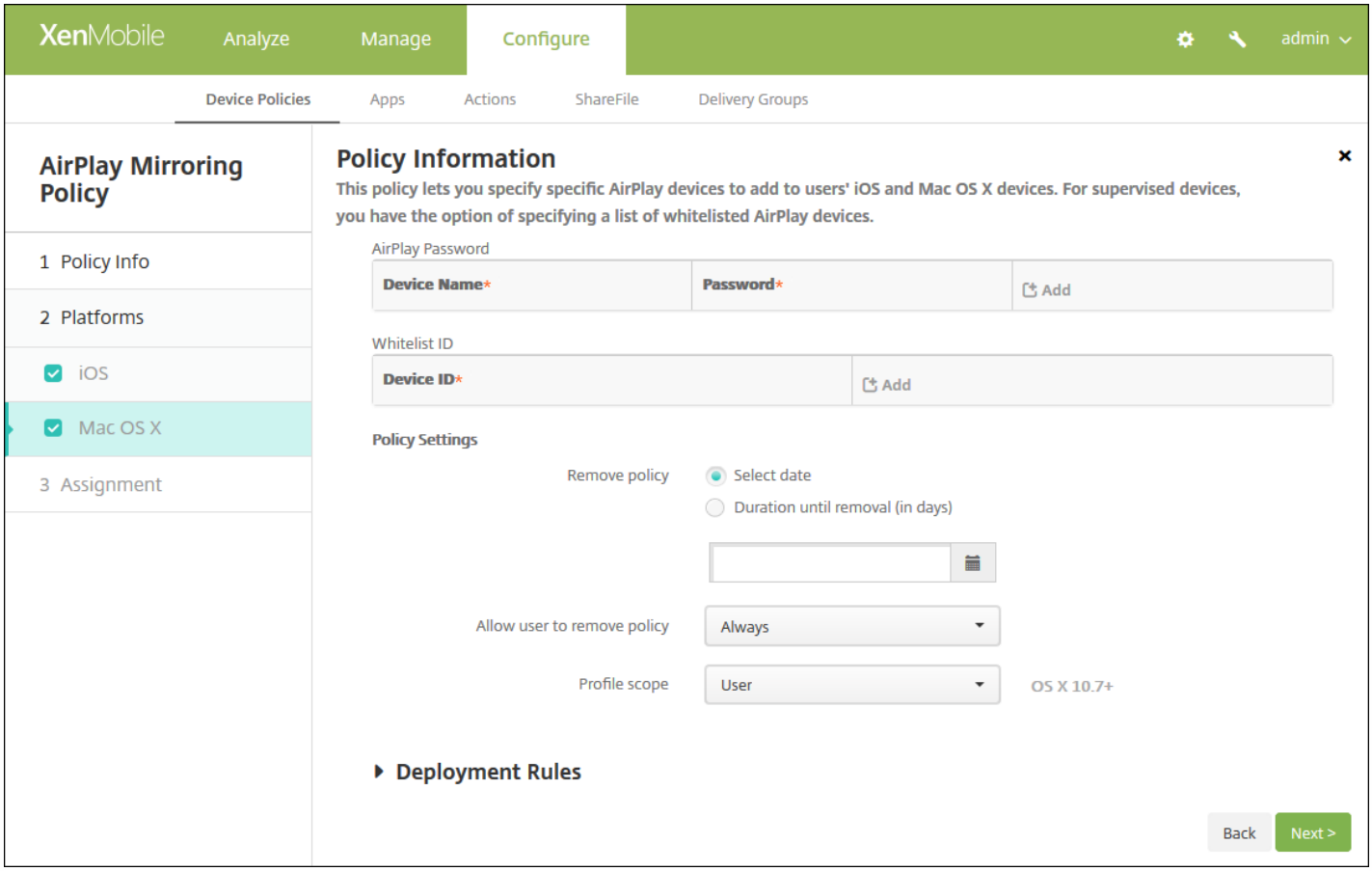
    注意：要删除现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **AirPlay 密码**：对于您要添加的各个设备，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**：未受监督的设备请忽略此列表。 此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。 对于希望添加到此列表中的每个 AirPlay 设备，请单击**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。

    注意：要删除现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

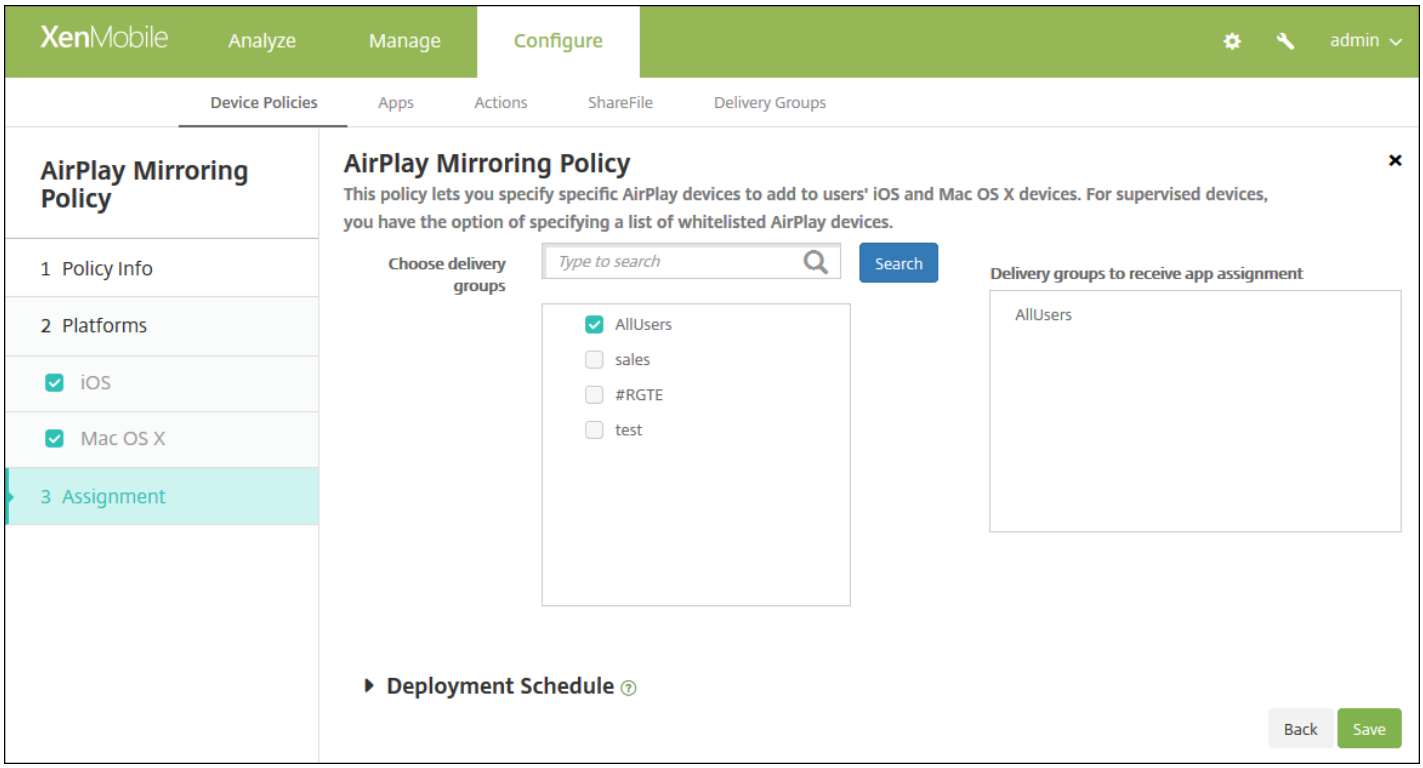
    要编辑现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **AirPlay 镜像策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所作的更改适用于所有平台，**为 始终启用 的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AirPrint 设备策略

Aug 11, 2016

您可以在 XenMobile 中添加一个设备策略，以便在用户的 iOS 设备上向 AirPrint 打印机列表中添加 AirPrint 打印机。 这样可以更加轻松地为打印机和设备位于不同子网的环境提供支持。

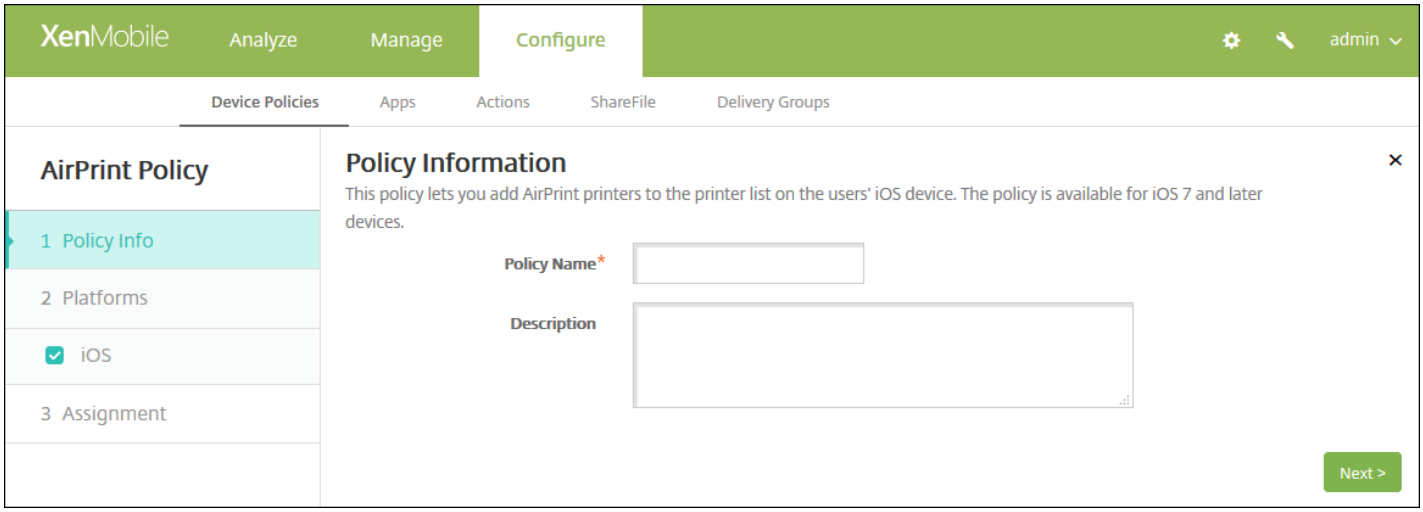
注意：

- 此策略适用于 iOS 7.0 及更高版本。
- 请确保知道每个打印机的 IP 地址和资源路径。

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. 单击**更多**，然后在**最终用户**下面，单击 **AirPrint**。 此时将显示 **AirPrint Policy**（AirPrint 策略）页面。

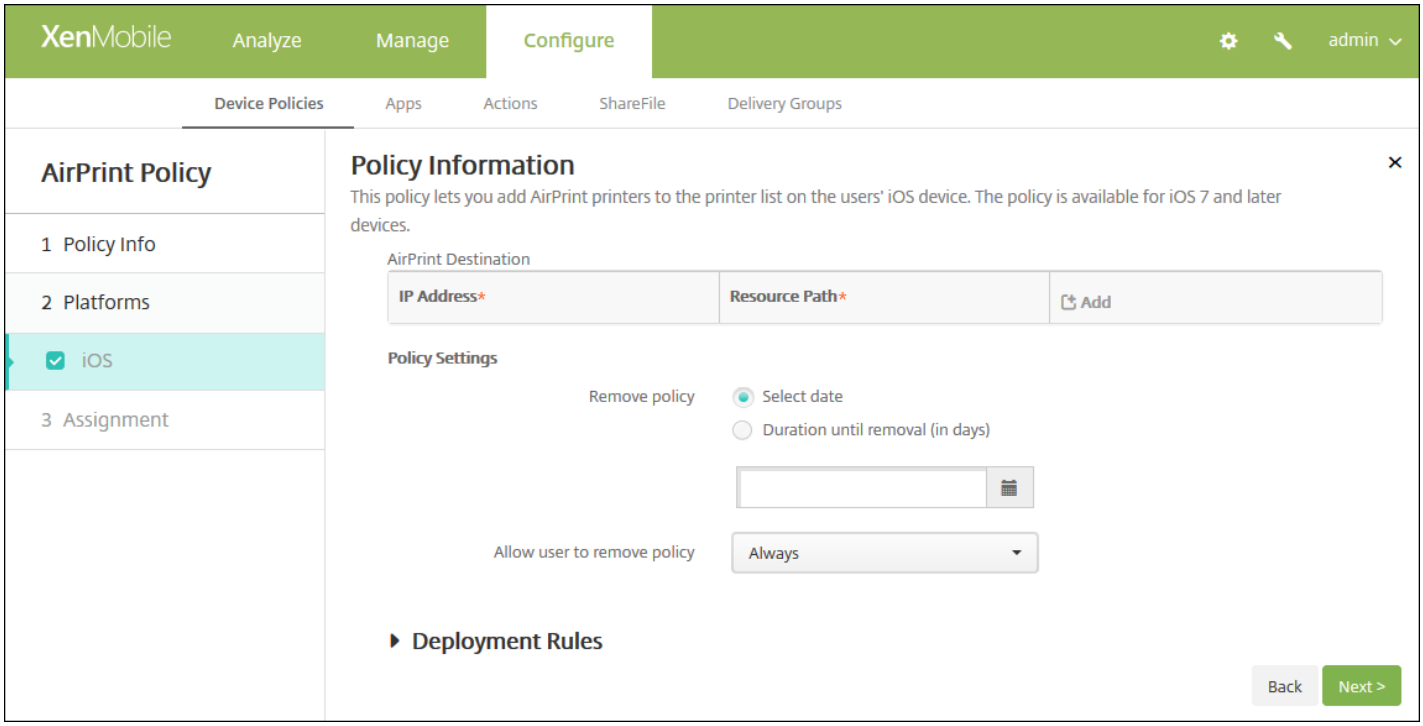


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台信息**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 配置以下设置：

- **AirPrint 目标**：对于您要添加的各个 AirPrint 目标，单击**添加**，然后执行以下操作：
  - **IP 地址**：输入 AirPrint 打印机 IP 地址。
  - **资源路径**：输入与打印机关联的资源路径。 此值与 _ipps.tcp Bonjour 记录的参数相对应。 例如，printers/Canon_MG5300_series 或 printers/Xerox_Phaser_7600。
  - 单击**保存**以添加打印机，或单击**取消**以取消添加打印机。

    注意：要删除现有打印机，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击删除以删除列表，或单击取消以保留此列表。

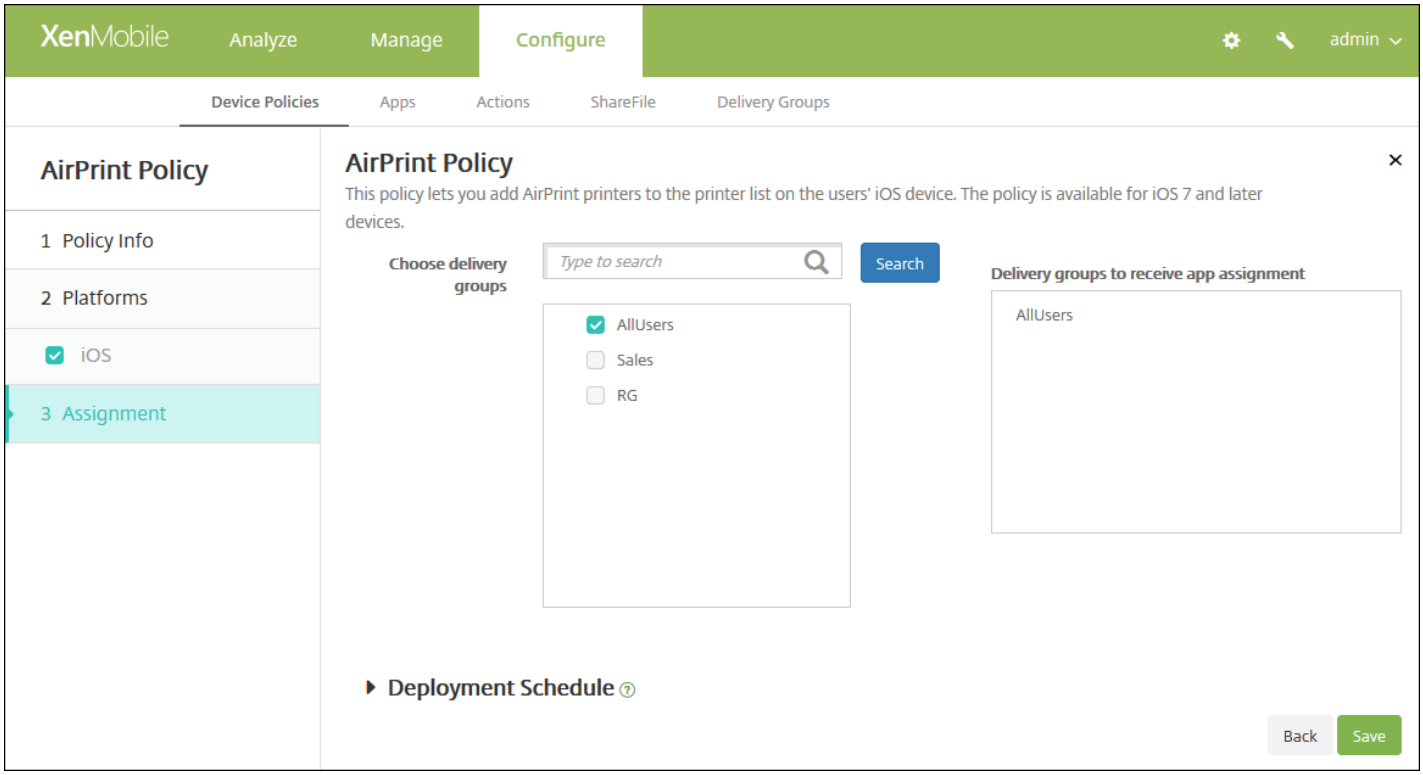
    要编辑现有打印机，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

- **策略设置**
  - 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **AirPrint 策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Android for Work 应用程序限制策略

Aug 11, 2016

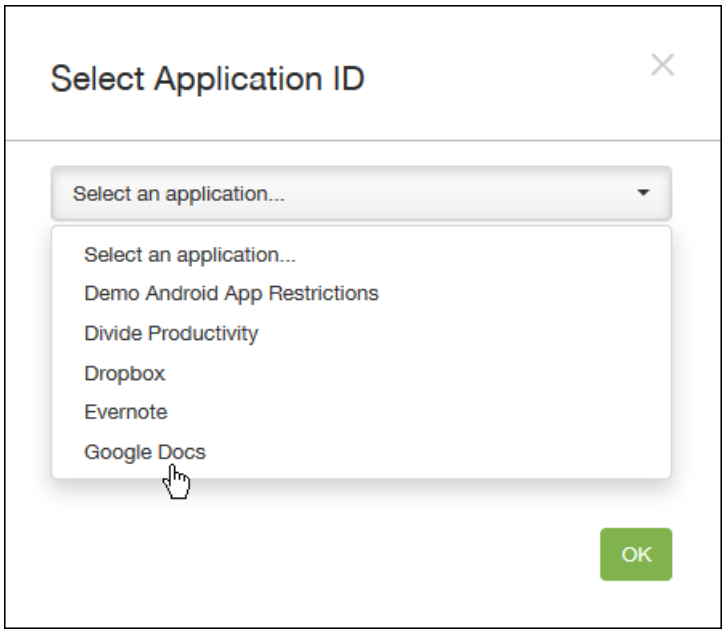
可以修改与 Android for Work 应用程序关联的限制，但是在执行此操作前，必须满足以下必备条件：

- 在 Google 上完成 Android for Work 设置任务。 有关详细信息，请参阅使用 Android for Work 管理设备。
- 创建一组 Google Play 凭据。 有关详细信息，请参阅 Google Play 凭据。
- 创建 Android for Work 帐户。 有关详细信息，请参阅创建 Android for Work 帐户。
- 将 Android for Work 应用程序添加到 XenMobile。 有关详细信息，请参阅向 XenMobile 添加应用程序。

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**添加新策略。 将显示**添加新策略**页面。

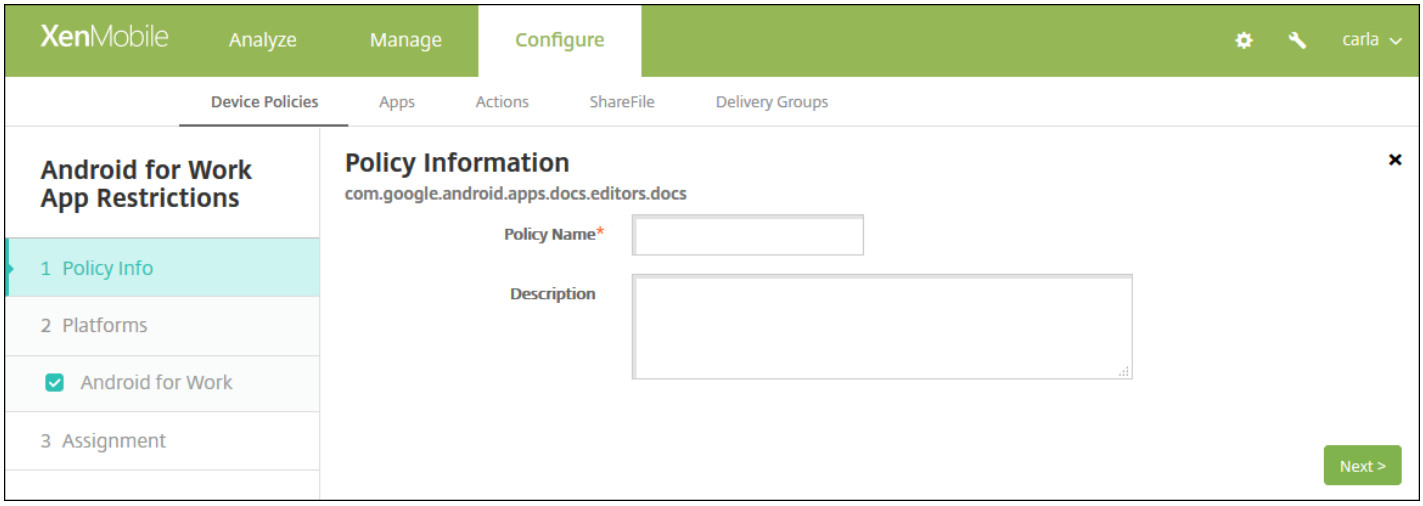
3. 展开**更多**，然后在**安全性**下面，单击 **Android for Work 应用程序限制**。 此时将显示一个请求您选择应用程序的对话框。



4. 在列表中，选择要应用限制的应用程序，然后单击**确定**。

- 如果没有要添加到 XenMobile 中的 Android for Work 应用程序，将无法继续操作。 有关向 XenMobile 添加应用程序的详细信息，请参阅向 XenMobile 添加应用程序。
- 如果应用程序没有关联任何限制，将显示有关相关影响的通知。 单击**确定**取消对话框。
- 如果应用程序具有与之关联的限制，将显示 **Android for Work 应用程序限制策略**信息页面。

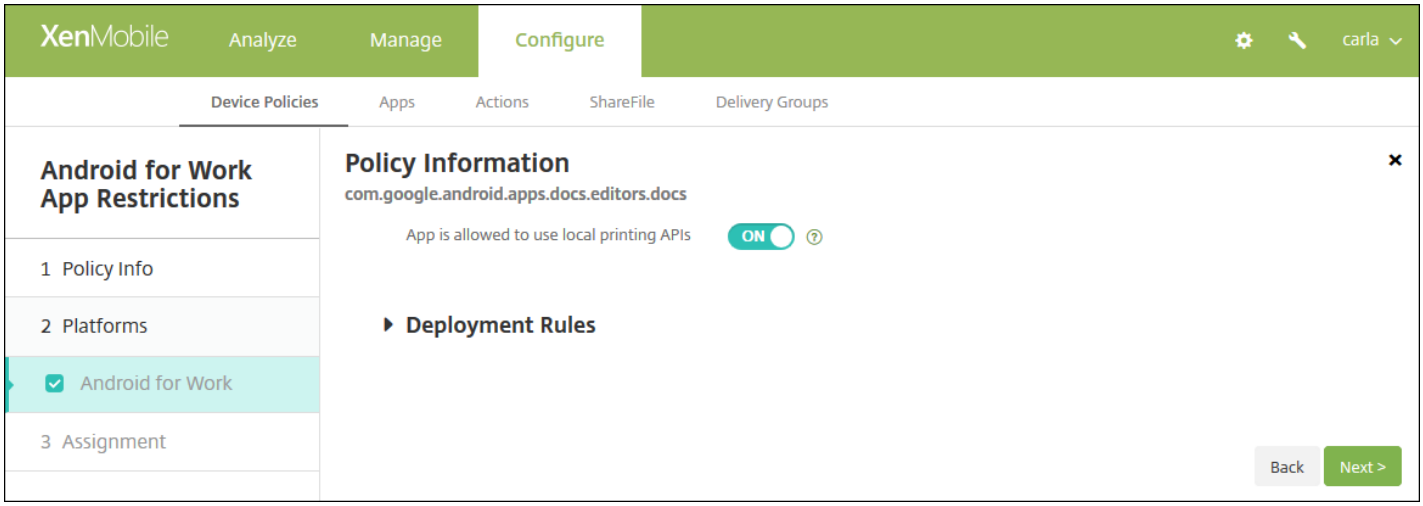
© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

6. 单击**下一步**。 此时将显示 **Android for Work 平台**页面。

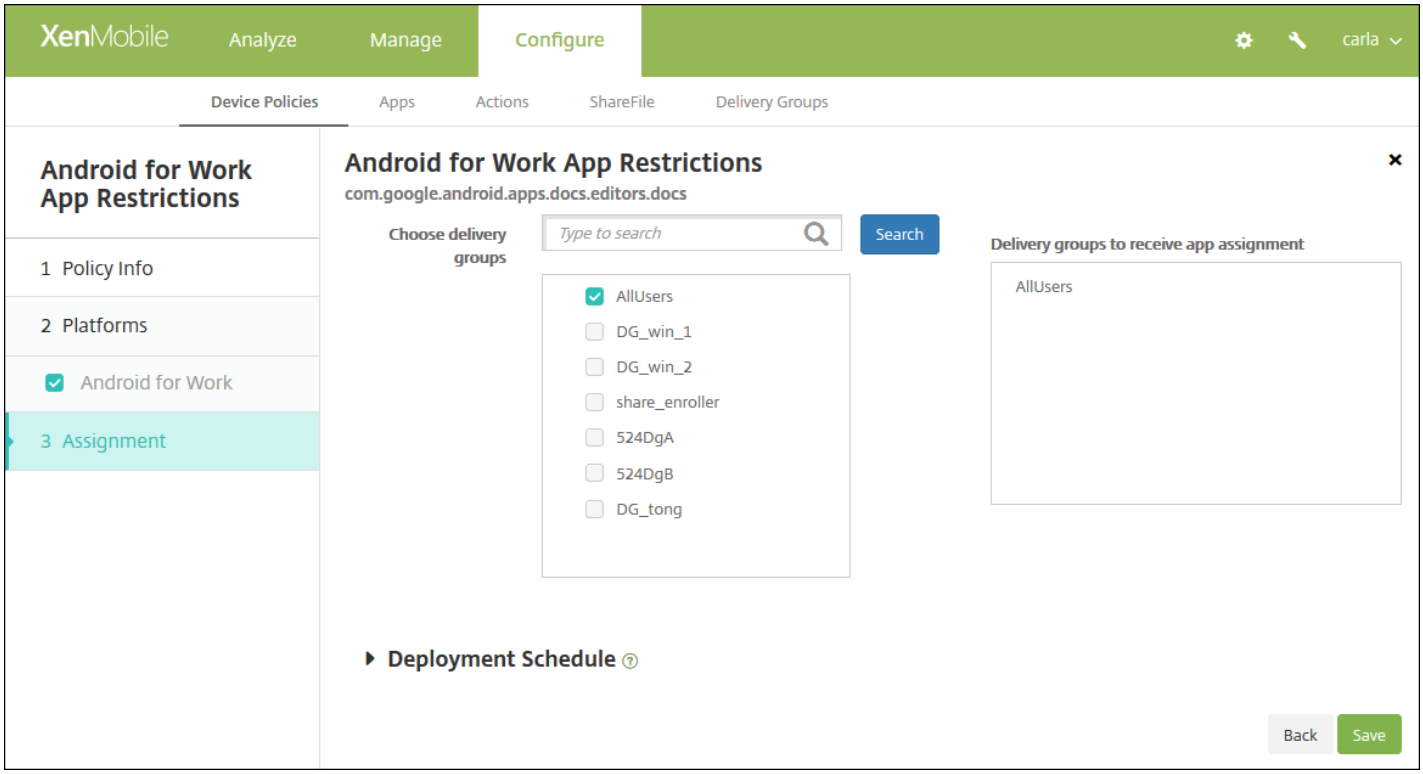


7. 为选择的应用程序配置设置。 显示的设置取决于与所选应用程序关联的限制。

8. 配置部署规则

9. 单击**下一步**。 此时将显示 **Android for Work 应用程序限制策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



10. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

11. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所作的更改适用于所有平台，**为 始终启用 的连接部署**除外，它不适用。

12. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

APN 设备策略

Aug 11, 2016

可以为 iOS、Android 和 Windows Mobile/CE 设备添加接入点名称 (APN) 设备策略。 如果贵组织不使用客户 APN 从移动设备连接到 Internet，可以使用此策略。 APN 策略确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。 大多数新式电话中已经定义此设置。

iOS 设置

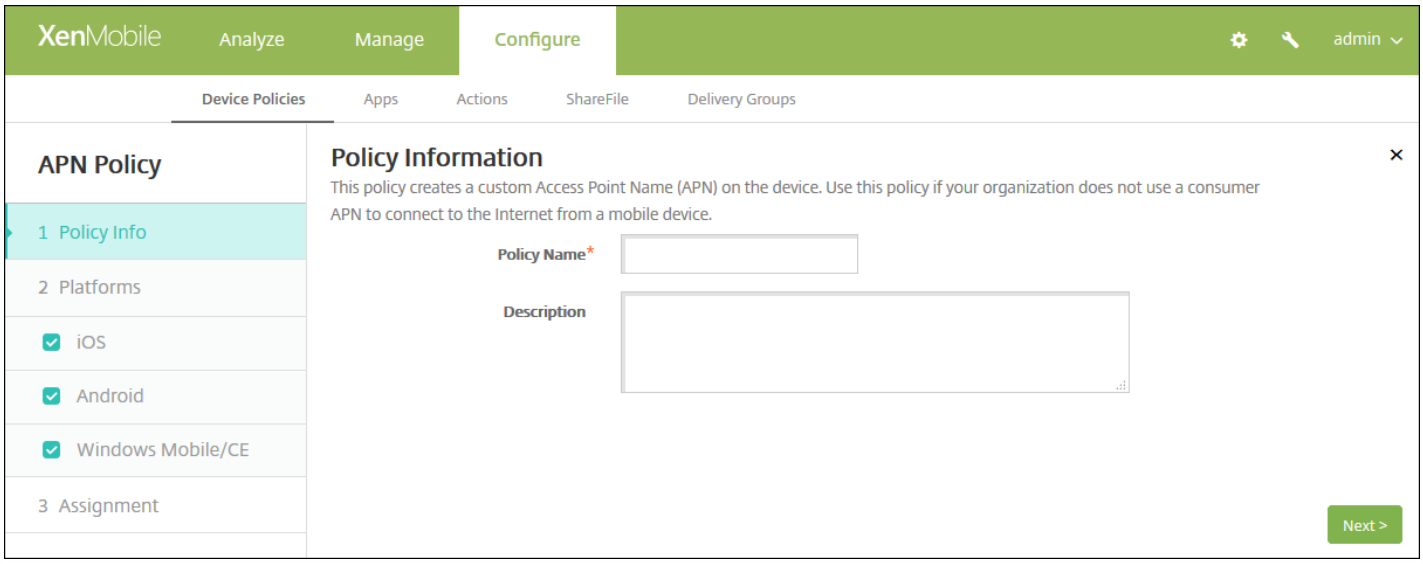
Android 设置

Windows Mobile/CE 设置

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. 单击**更多**，然后在**网络访问权限**下面，单击 **APN**。 此时将显示 **APN 策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

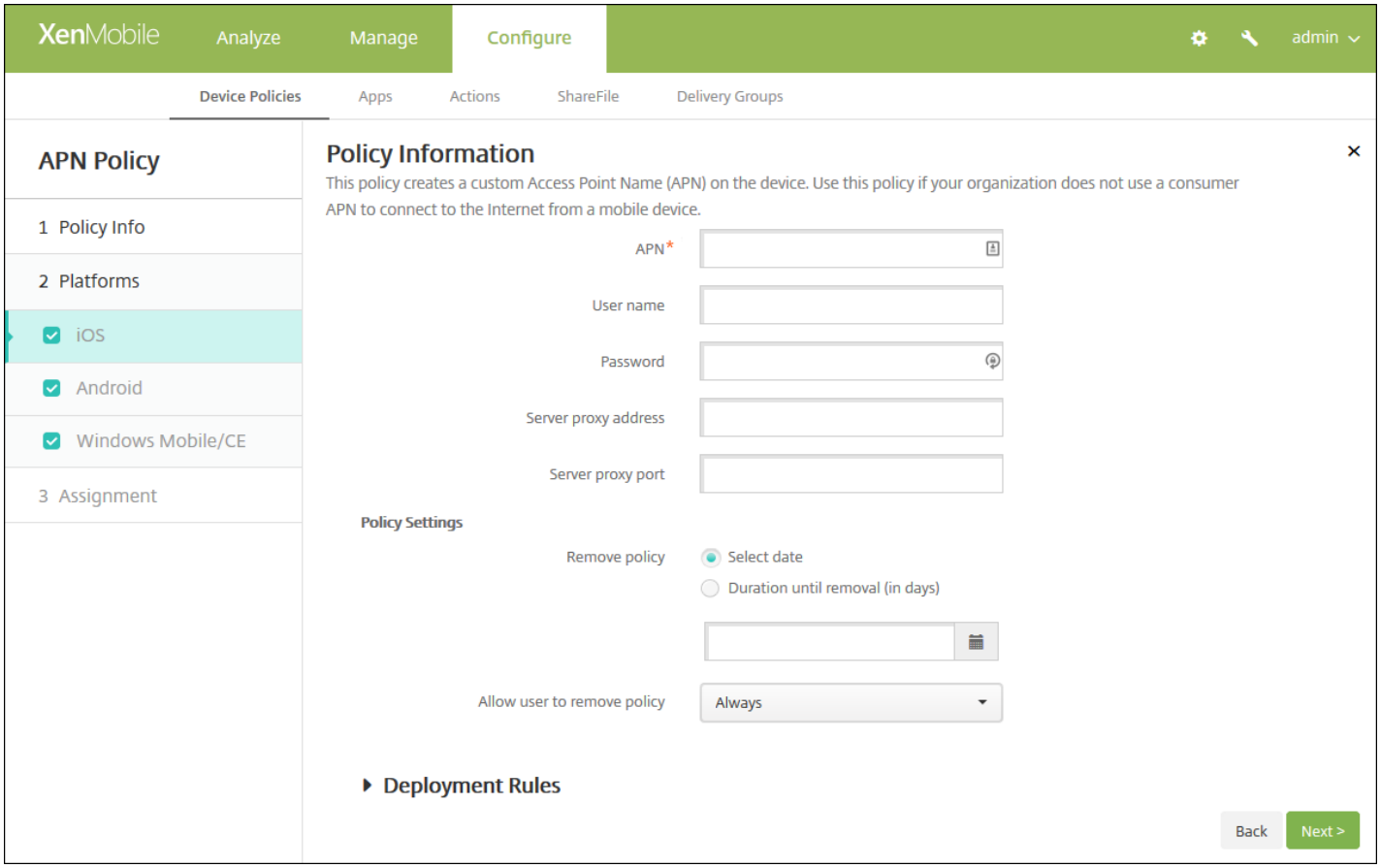
注意：显示**策略平台**页面时，会选中所有平台，并且首先看到 iOS 平台。

6. 在**平台**下面，选择要添加的平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

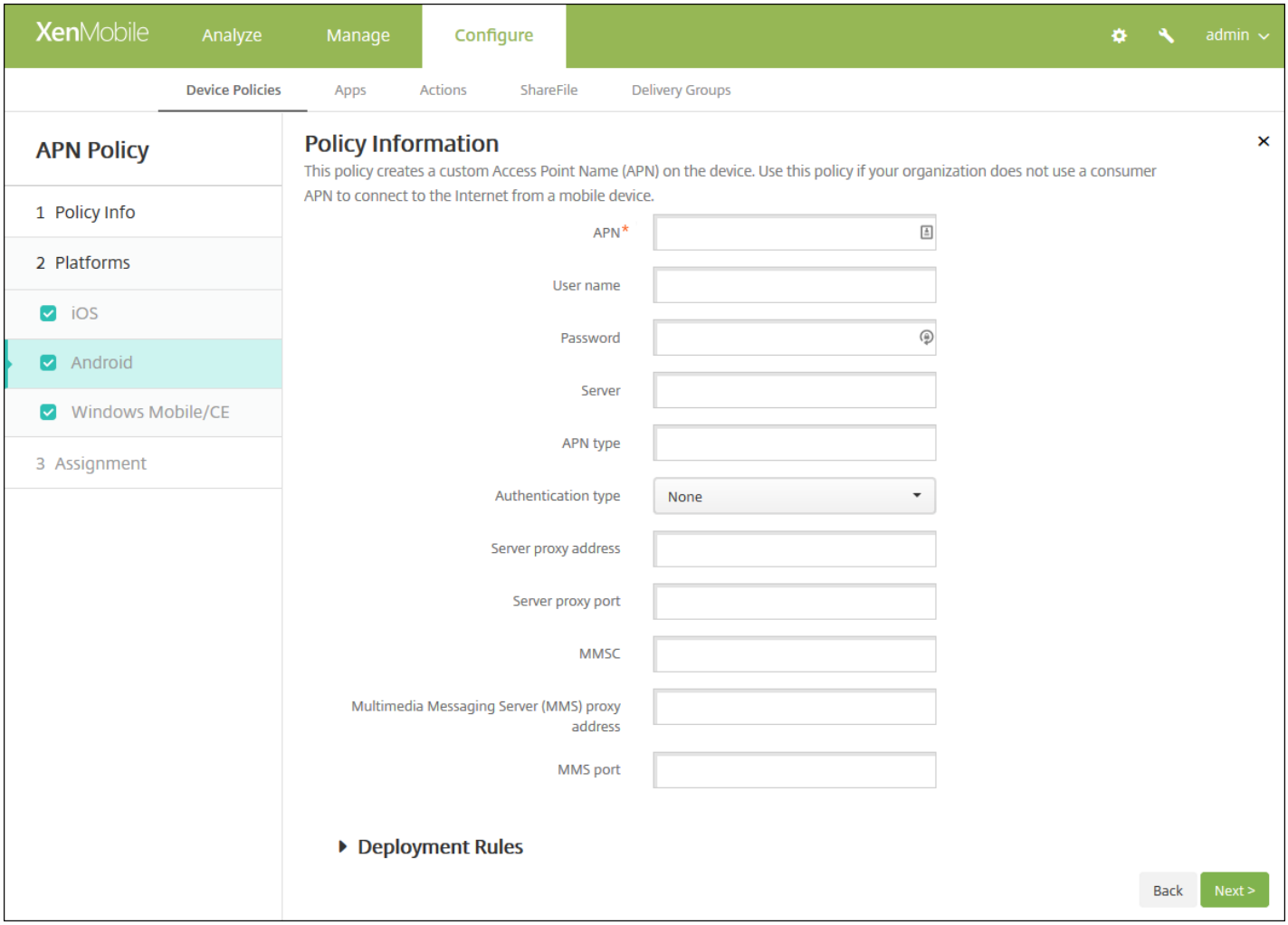


配置以下设置：

- **APN**：键入接入点的名称。 此信息必须与接受的某个 iOS APN 匹配，否则策略将失败。
- **用户名**：该字符串指定此 APN 的用户名。 如果用户名缺失，在配置文件安装期间设备会提示输入该字符串。
- **密码**：此 APN 的用户密码。 为进行混码处理，对密码进行了编码。 如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- **服务器代理地址**：APN 代理的 IP 地址或 URL。
- **服务器代理端口**：APN 代理的端口号。 如果已输入服务器代理地址，则此字段为必填字段。
- 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Android 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



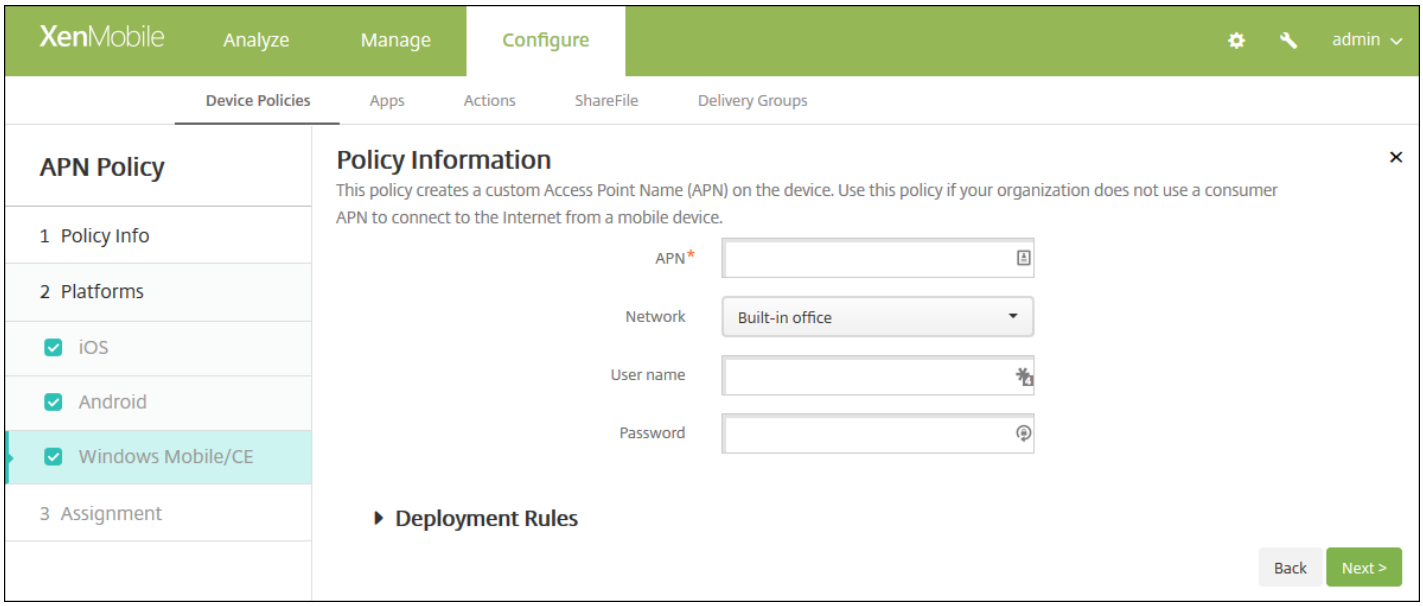
配置以下设置：

- **APN**：键入接入点的名称。 此信息必须与接受的某个 Android APN 匹配，否则策略将失败。
- **用户名**：该字符串指定此 APN 的用户名。 如果用户名缺失，在配置文件安装期间设备会提示输入该字符串。
- **密码**：此 APN 的用户密码。 为进行混码处理，对密码进行了编码。 如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- **服务器**：此设置出现在智能手机出现之前，通常为空。 它是指无法访问或显示标准 Web 站点的手机的无线应用协议 (WAP) 网关服务器。
- **APN 类型**：此设置必须匹配运营商的接入点用途。 它是 APN 服务说明符的逗号分隔字符串，必须与无线运营商的发布定义匹配。 示例包括：
  - *. 所有流量均通过此接入点。
  - mms。 多媒体流量通过此接入点。
  - default（默认）。 包括多媒体在内的所有流量均通过此接入点。
  - supl。 与 GPS 关联的安全用户层面定位 (Secure User Plane Location)
  - dun。 拨号网络已经过时，很少使用。
  - hipri。 高优先级网络。
  - fota。 无线固件升级用于接收固件更新。
- **身份验证类型**：在列表中，单击要使用的身份验证类型。 默认为“无”。
- **服务器代理地址**：运营商的 APN HTTP 代理的 IP 地址或 URL。
- **服务器代理端口**：APN 代理的端口号。 如果已输入服务器代理地址，则此字段为必填字段。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **MMSC**：运营商提供的 MMS 网关服务器地址。
- **多媒体消息服务器(MMS)代理地址**：指 MMS 通信的多媒体消息服务服务器。 MMS 使得 SMS 可以发送包含多媒体内容（如图片或视频）的大型消息。 这些服务器需要特定的协议（如 MM1、... MM11）。
- **MMS 端口**：用于 MMS 代理的端口。

配置 Windows Mobile/CE 设置



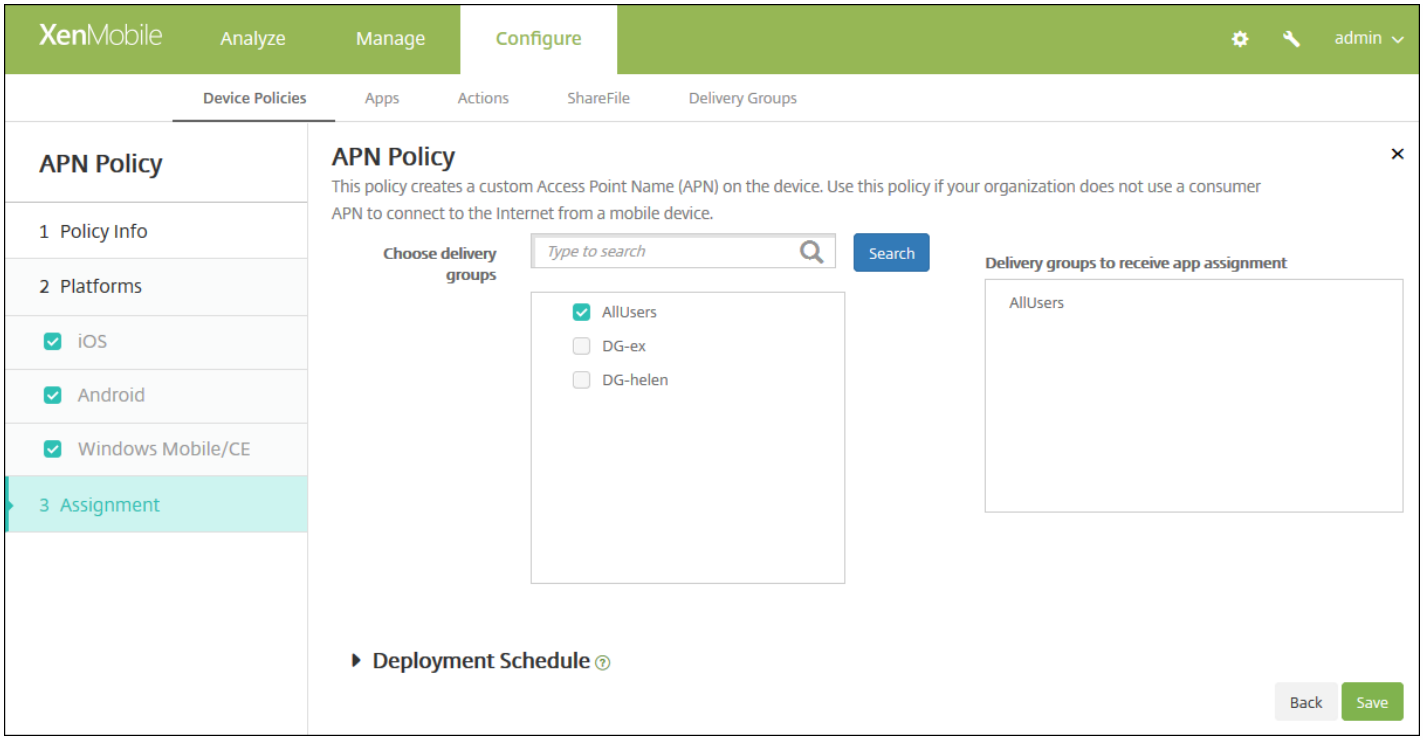
配置以下设置：

- **APN**：键入接入点的名称。 此信息必须与接受的某个 Android APN 匹配，否则策略将失败。
- **网络**：在列表中，单击要使用的网络类型。 默认值为**内置办公网络**。
- **用户名**：该字符串指定此 APN 的用户名。 如果用户名缺失，在配置文件安装期间设备会提示输入该字符串。
- **密码**：此 APN 的用户密码。 为进行混码处理，对密码进行了编码。 如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **APN 策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

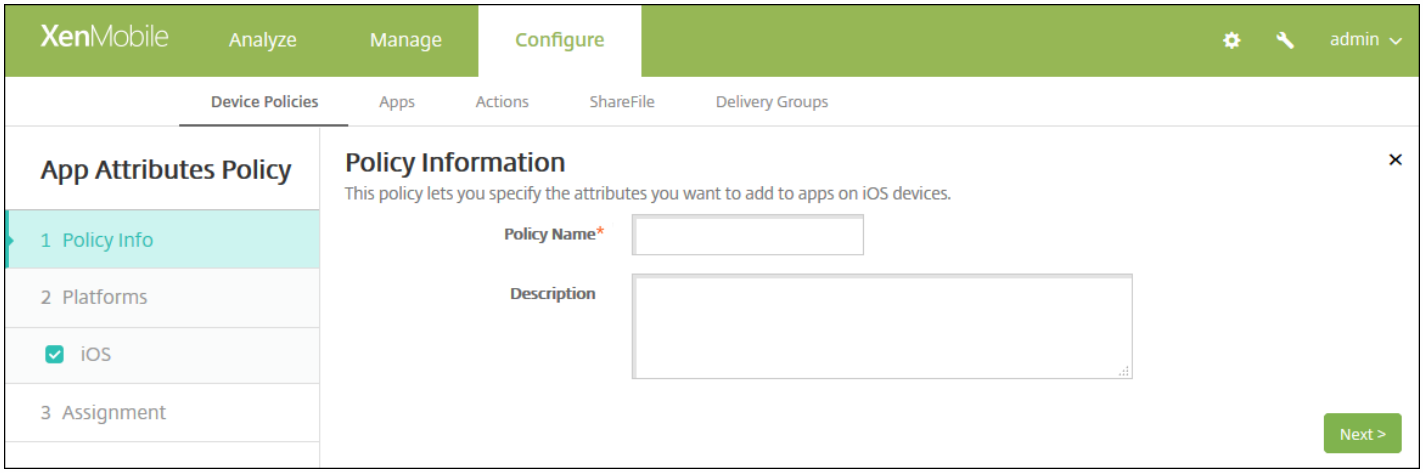
- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序属性设备策略

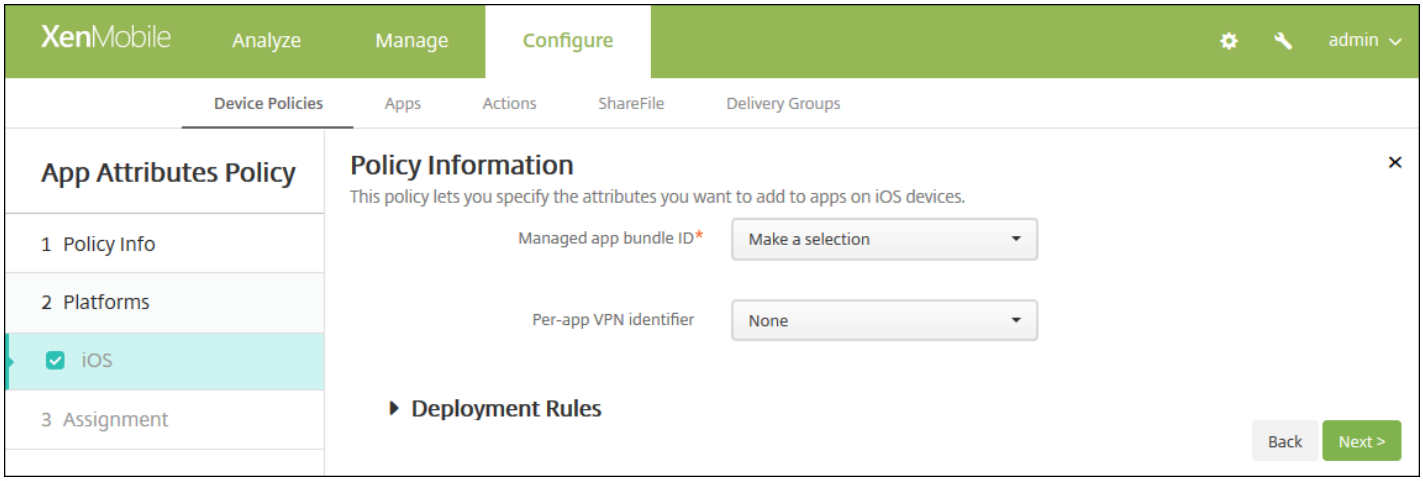
Aug 11, 2016



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示**应用程序属性**平台信息页面。



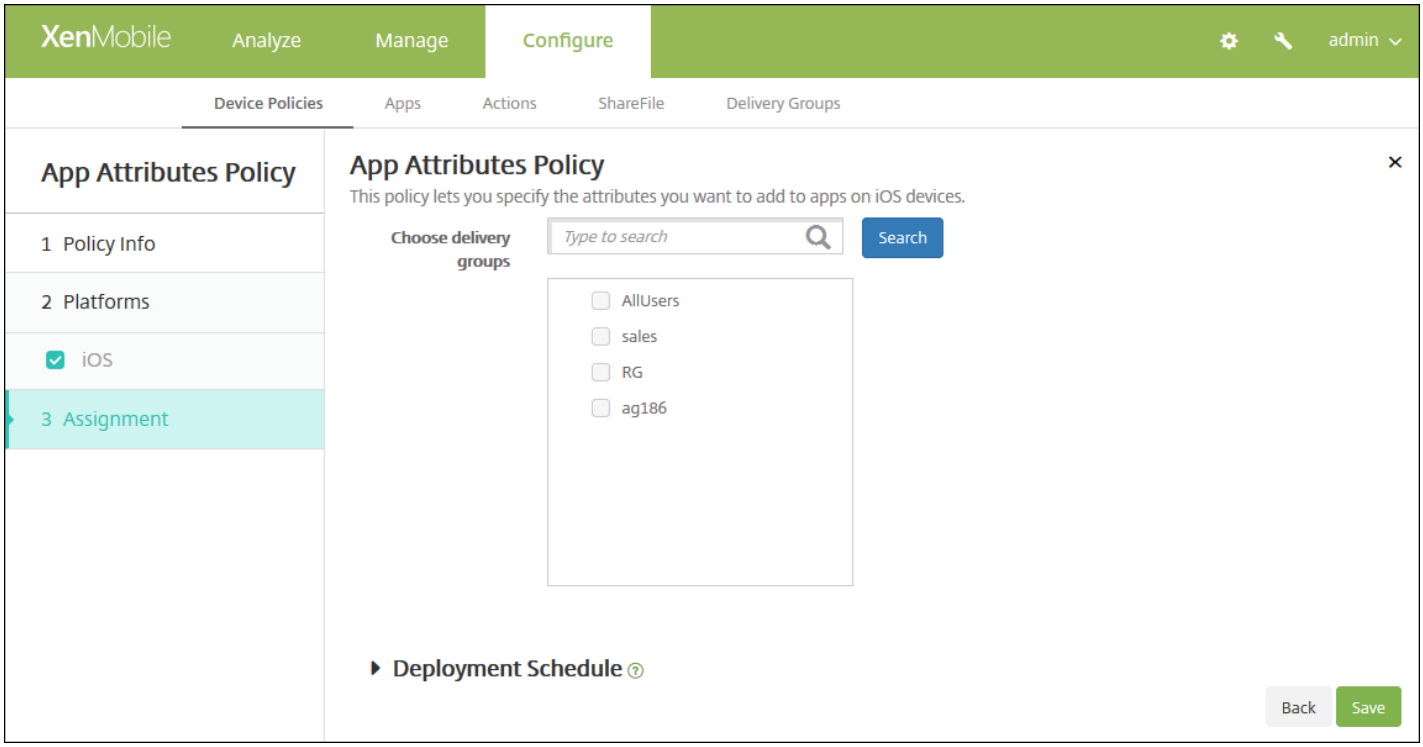
6. 配置以下设置：

- **托管应用程序捆绑包 ID**：在列表中，单击某个应用程序捆绑包 ID 或单击**新增**。
  - 如果单击**新增**，请在显示的字段中键入应用程序捆绑包 ID。
- **“为应用单独设置 VPN”标识符**：在列表中，单击“为应用单独设置 VPN”标识符。

7. 配置部署规则

8. 单击**下一步**。 此时将显示应用程序属性策略分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，“为始终启用的连接部署”除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序访问设备策略

Aug 11, 2016

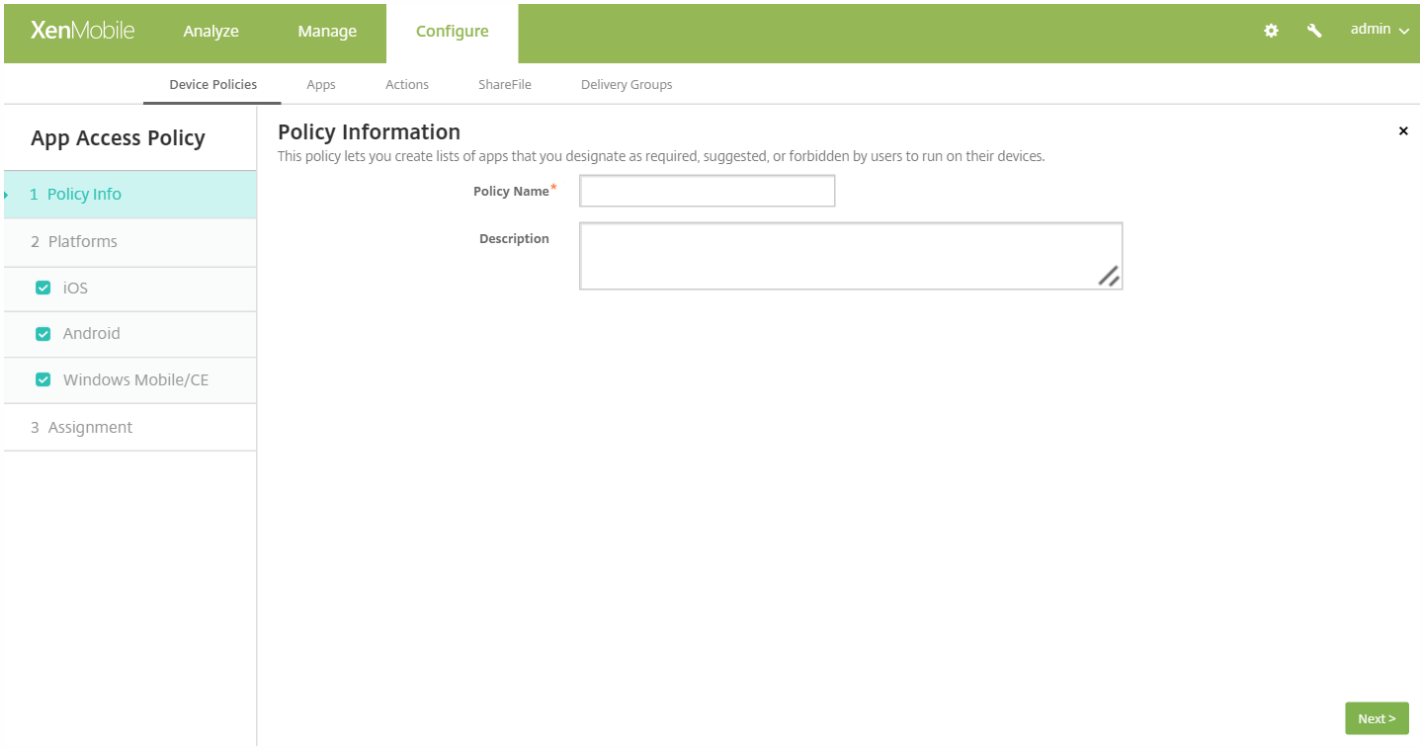
利用 XenMobile 中的应用程序访问设备策略，可以定义需要安装到设备上、可以安装到设备上或不得安装到设备上的应用程序列表。 然后，可以创建自动化操作，以使设备符合此应用程序列表。 可以创建适用于 iOS、Android 和 Windows Mobile/CE 设备的应用程序访问策略。

一次只能配置一种类型的访问策略。 可以针对必选的应用程序列表、推荐的应用程序列表或禁止的应用程序列表添加策略，但不能在一个应用程序访问策略中混合这些应用程序列表。 如果为每种列表类型创建一个策略，建议谨慎地为每个策略命名，以便于了解 XenMobile 中的哪项策略适用于哪种应用程序列表。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。

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**应用程序**下面，单击**应用程序访问**。 此时将显示 **App Access Policy**（应用程序访问策略）信息页面。



4. 在**策略信息**窗格上，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

6. 分别为选择的每个平台配置以下设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **访问策略**：单击必需、推荐或禁止。 默认设置为必选。
- 要向列表中添加一个或多个应用程序，请单击**添加**，然后执行以下操作：
  - **应用程序名称**：输入应用程序的名称。
  - **应用程序标识符**：输入可选应用程序标识符。
  - 单击**保存**或**取消**。
  - 对要添加的每个应用程序重复这些步骤。

  注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

  要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击下一步。 此时将显示下一个平台页面或**应用程序访问策略**分配页面。

9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序配置设备策略

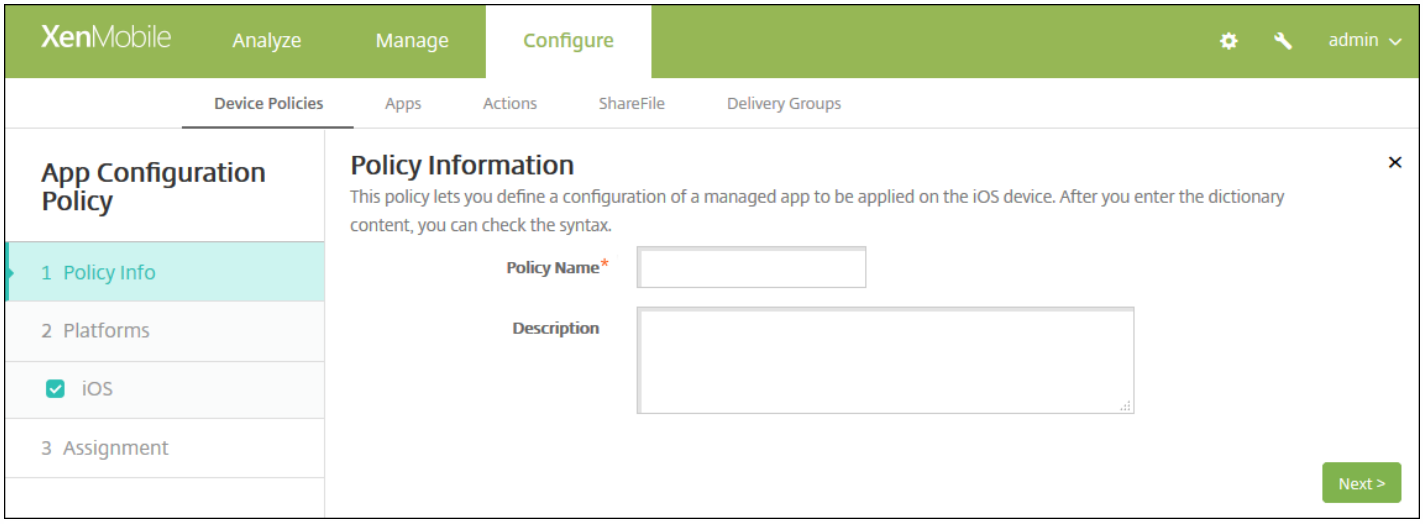
Aug 11, 2016

您可以通过向用户的 iOS 设备部署 XML 配置文件（称为属性列表或 plist）远程配置支持托管配置的应用商店应用程序，以配置应用程序中的各种设置和行为。 您实际可以配置的设置和行为取决于应用程序，这些内容不在本文讨论范围之内。

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**。 将显示**添加新策略**页面。

3. 展开**更多**，然后在**应用程序**下面，单击**应用程序配置**。 将显示**应用程序配置策略**信息页面。

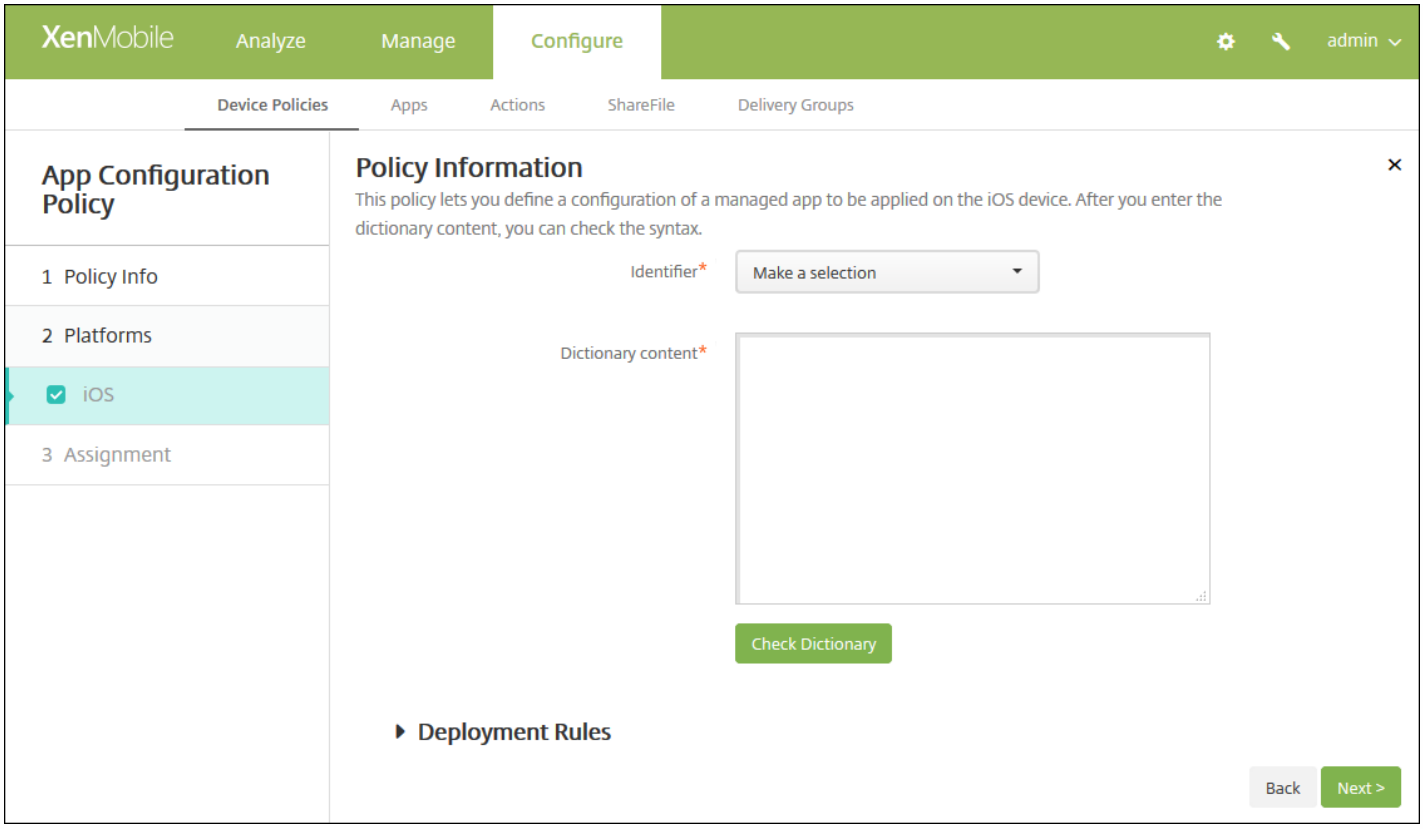


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS** 平台信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



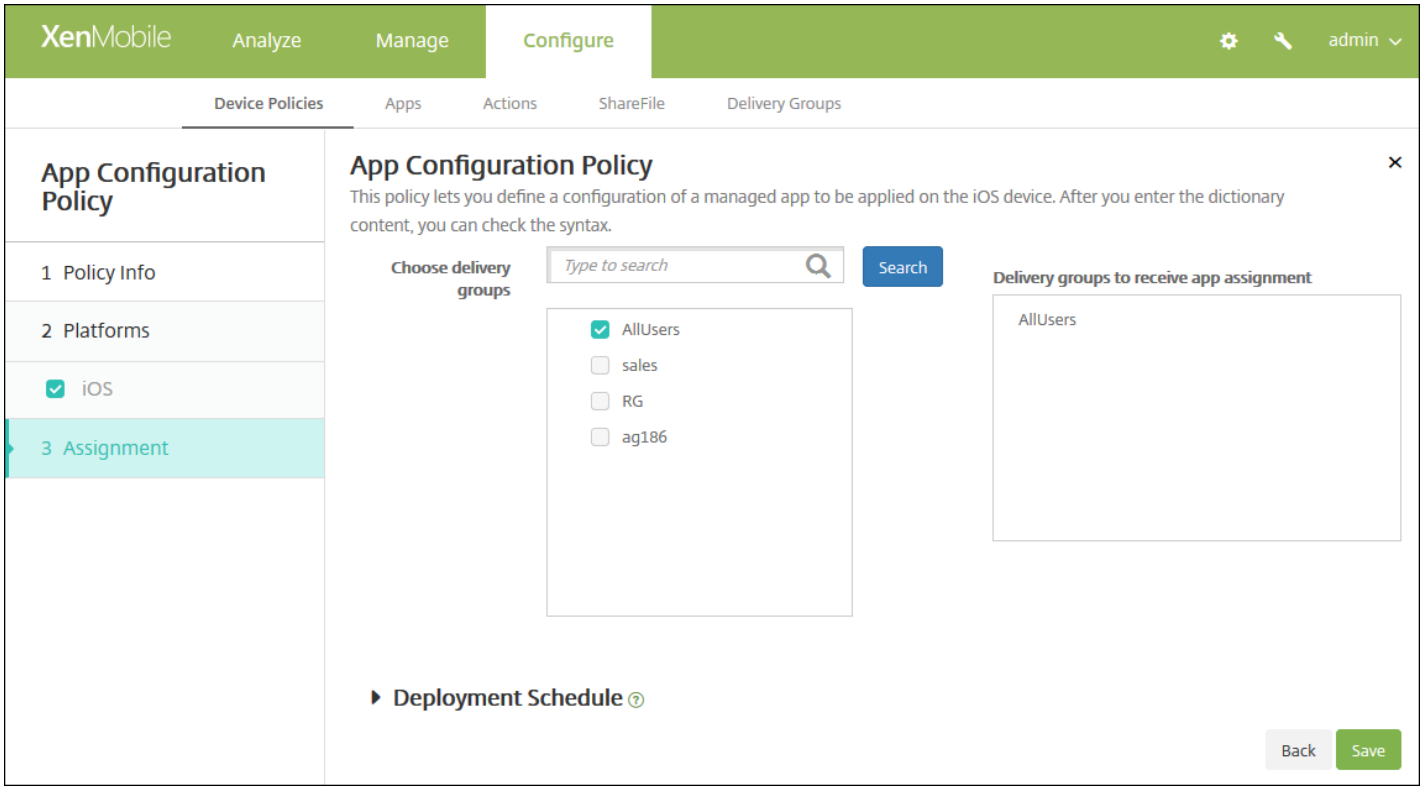
6. 配置以下设置：

- **标识符**：在列表中，单击要配置的应用程序，或单击**新增**向列表中添加新应用程序。
  - 如果单击**新增**，请在显示的字段中键入应用程序标识符。
- **字典内容**：键入或复制并粘贴 XML 属性列表 (plist) 配置信息。
- 单击**检查字典**。 XenMobile 验证 XML。 如果没有错误，将在内容框下面显示**有效 XML**。 如果内容框下面显示语法错误，必须纠正这些错误，然后才能继续操作。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**应用程序配置策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序清单设备策略

Aug 11, 2016

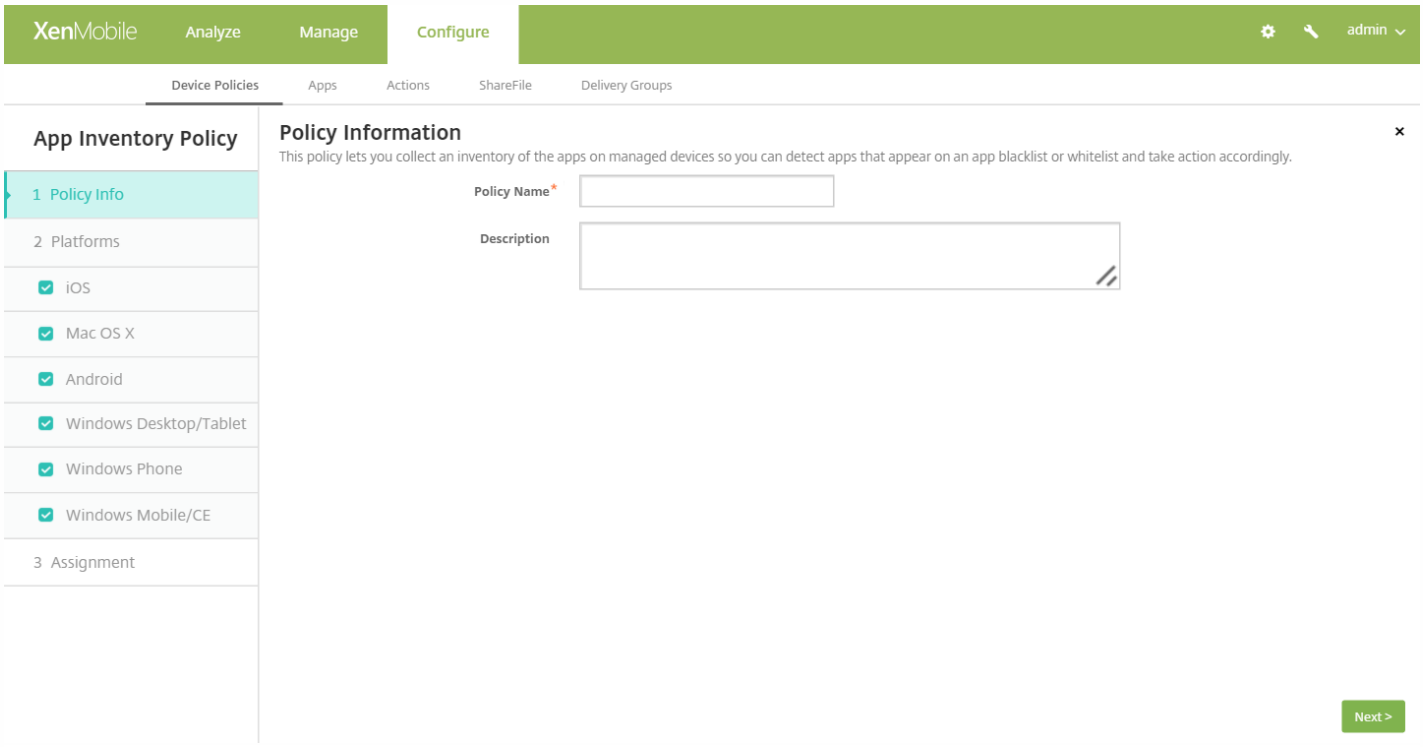
借助 XenMobile 中的应用程序清单策略，您可以收集托管设备上应用程序的清单，然后根据该清单对比部署到这些设备上的任何应用程序访问策略。 这样，您可以发现出现在应用程序黑名单（在应用程序访问策略中禁止）或白名单（在应用程序访问策略中需要）上的应用程序，并采取相应的操作。 可以为 iOS、Mac OS X、Android（包括为 Android for Work 启用的设备）、Windows Desktop/Tablet、Windows Phone 或 Windows Mobile/CE 设备创建应用程序访问策略。

> **Important**
>
> 要使已更新的应用程序显示在用户 Android 设备上 WorxStore 中的“Updates Available”（更新可用）列表中，必须首先向用户设备部署此策略。

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**。 将显示**添加新策略**页面。

3. 展开**更多**，然后在**应用程序**下面，单击**应用程序清单**。 将显示**应用程序清单策略**页面。

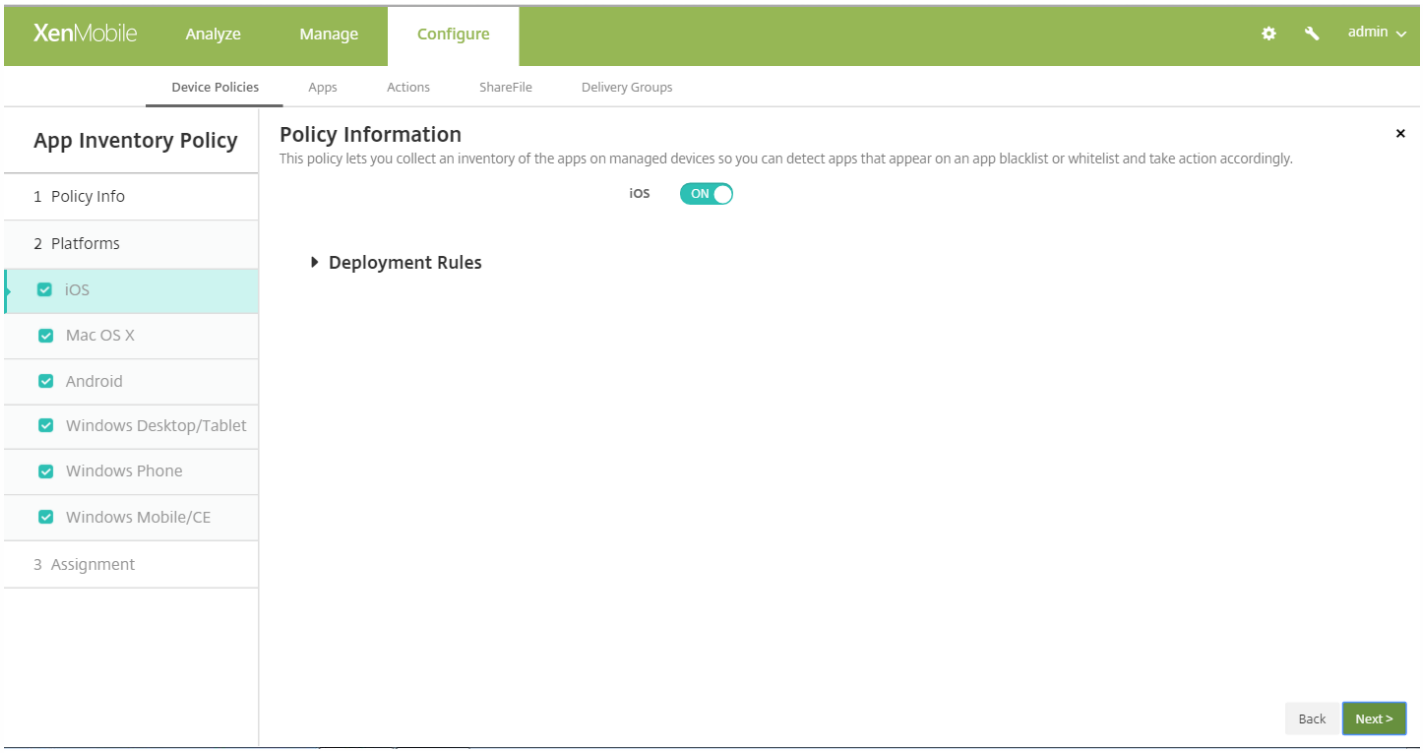


4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

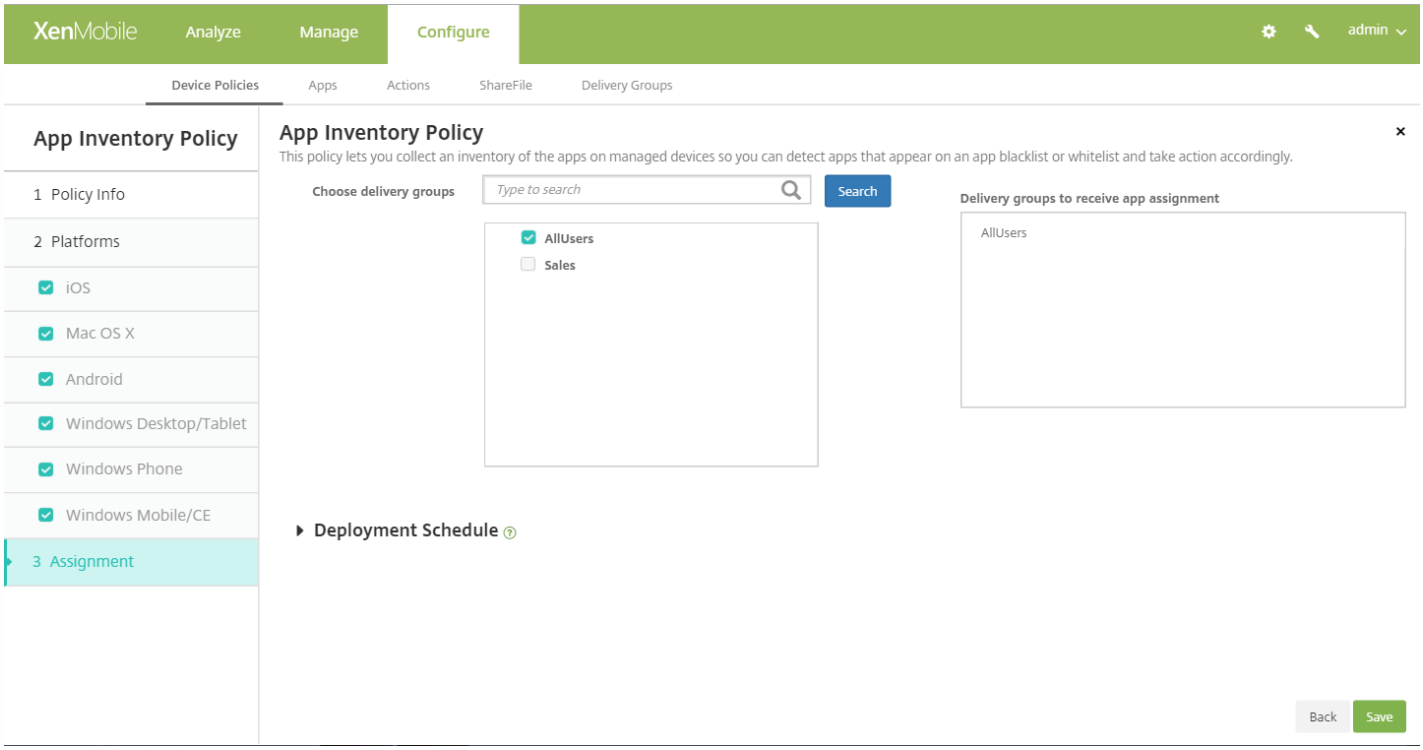
完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

6. 对于所选的每个平台，保留默认设置或将设置更改为**关**。 默认值为**开**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**应用程序清单策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。

10. 展开部署计划，然后配置以下设置：

- 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。 如果选择关，无需配置其他选项。
- 在部署计划旁边，单击立即或稍后。 默认选项为立即。
- 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 之前的 部署失败时。 默认选项为每次连接时。
- 在为始终启用的连接部署旁边，单击开或关。 默认选项为关。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序锁定设备策略

Aug 15, 2016

可以在 XenMobile 中创建一条策略，用于定义允许在设备上运行的应用程序列表，或阻止在设备上运行的应用程序列表。 可以同时为 iOS 和 Android 设备配置此策略，但策略具体的执行方式则因平台而异。 例如，不能阻止在 iOS 设备上运行多个应用程序。

同样，对于 iOS 设备，每个策略只能选择一个 iOS 应用程序。 这意味着用户只能使用其设备运行一个应用程序。 强制执行应用程序锁定策略时，不能在设备上执行除您明确允许的选项之外的任何其他活动。

此外，必须监督 iOS 设备才能推送应用程序锁定策略。

虽然设备策略在大多数 Android L 和 M 设备上起作用，但是，由于 Google 弃用了所需的 API，因此，应用程序锁定策略在 Android N 或更高版本的设备上不起作用。

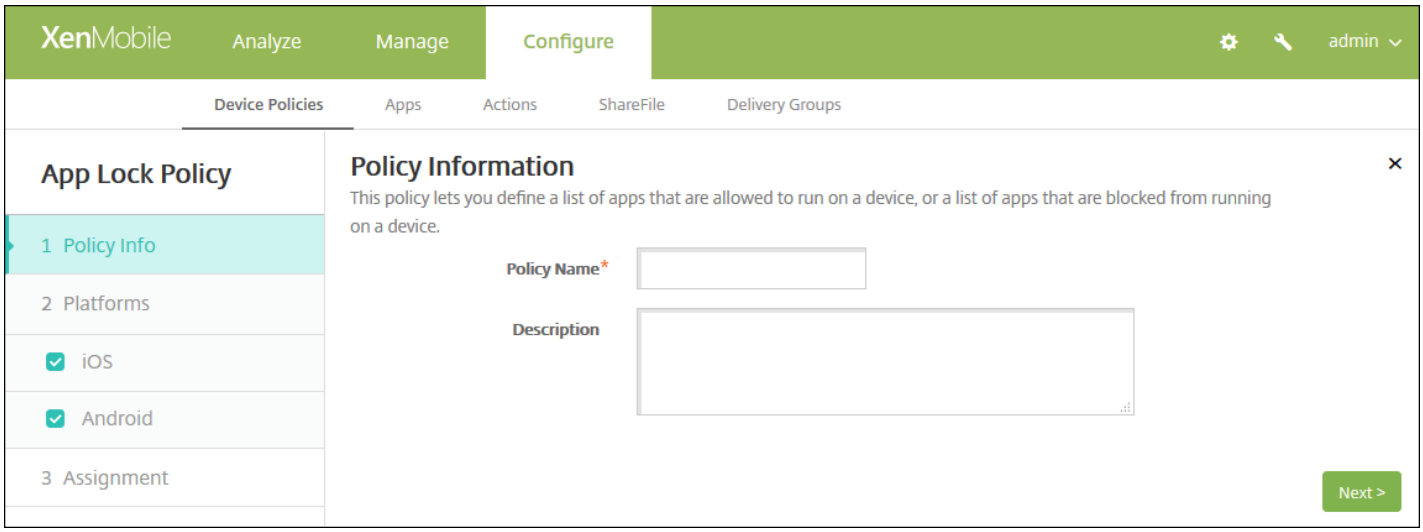
iOS 设置

Android 设置

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**下面，单击**应用程序锁定**。 此时将显示**应用程序锁定策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：如有需要，请键入策略的说明。

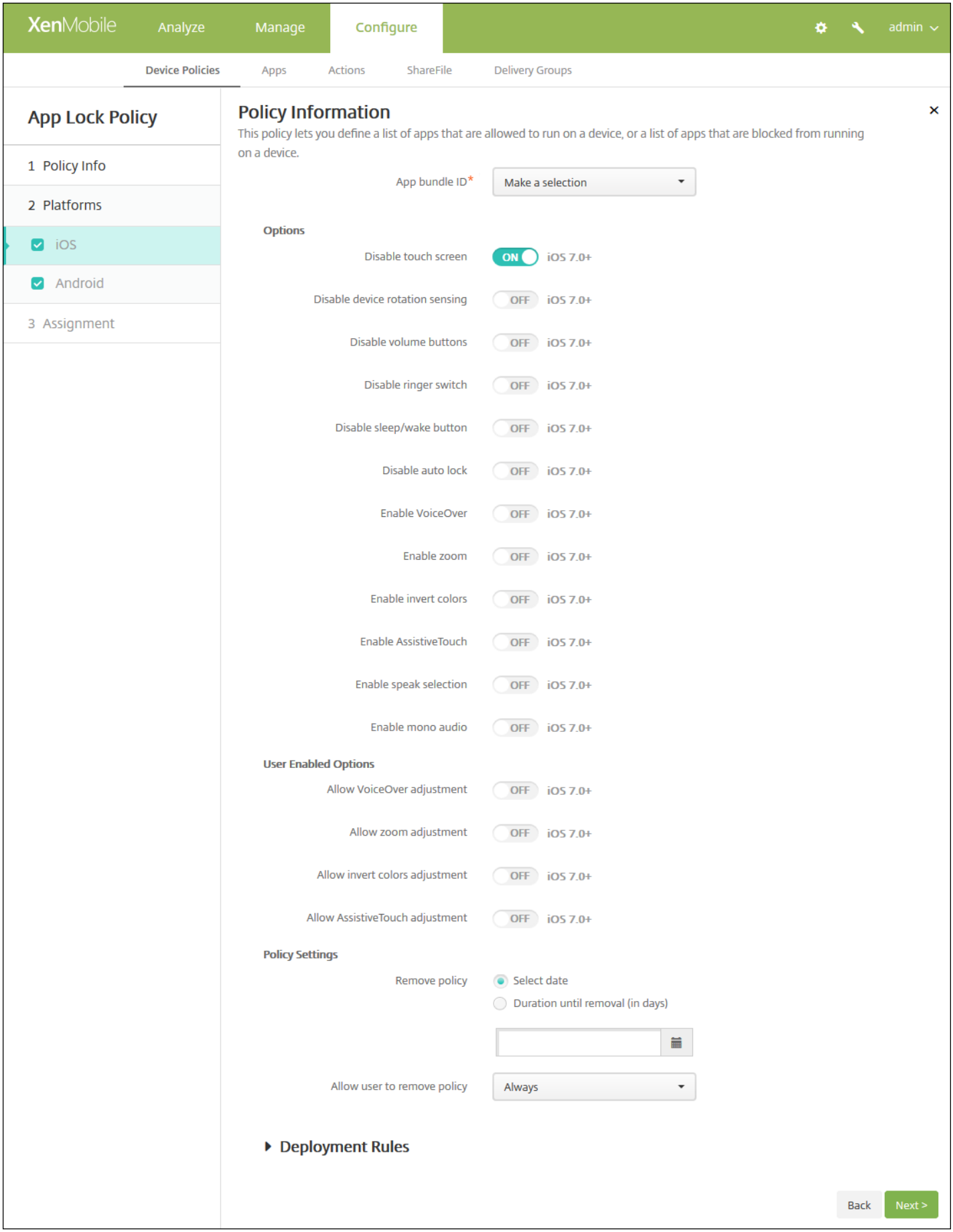
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.



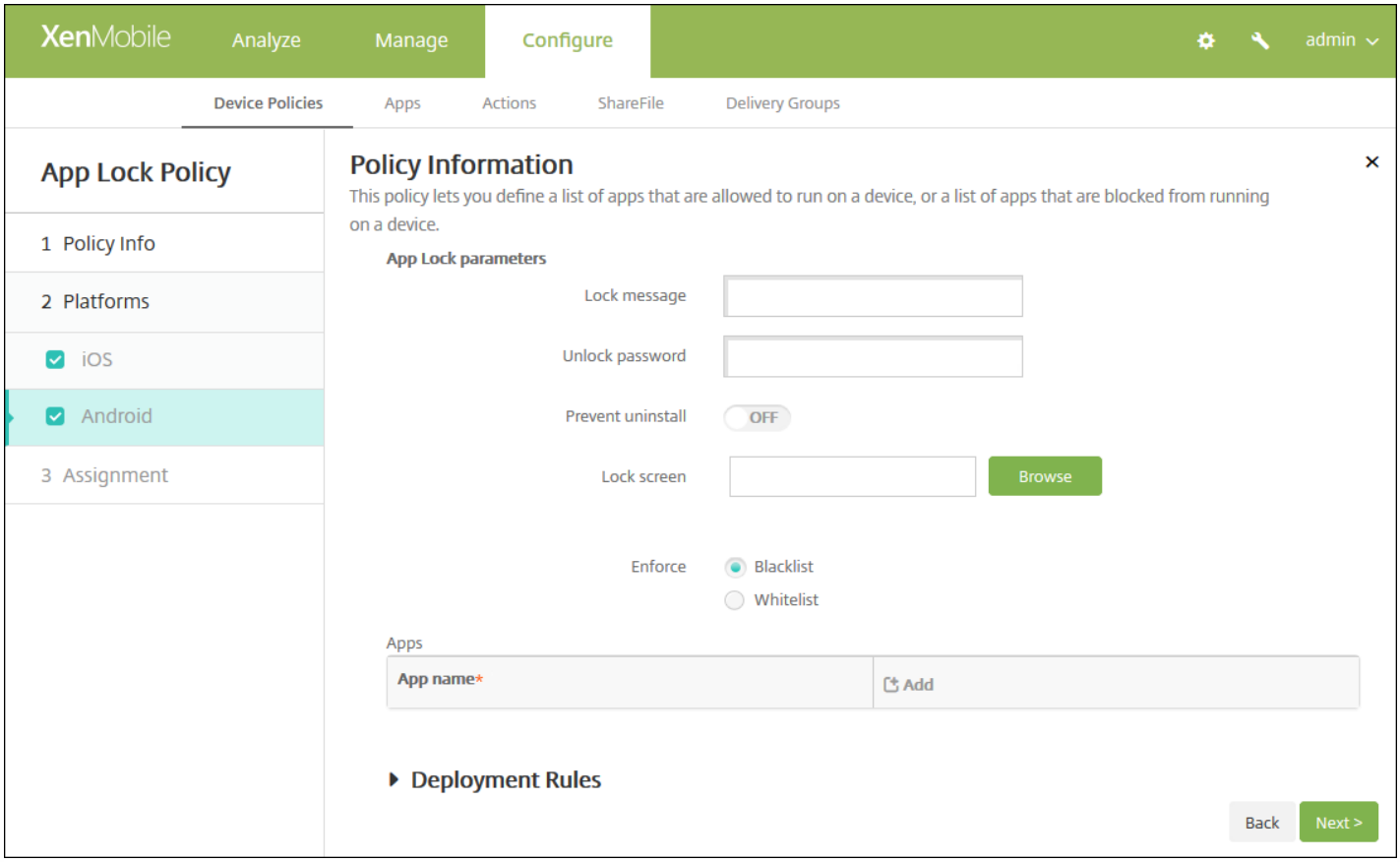
© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置以下设置：

- **应用程序捆绑包 ID**：在列表中，单击此策略适用的应用程序，或单击**新增**向列表中添加新应用程序。 如果选择**新增**，请在显示的字段中键入应用程序名称。
- **选项**：以下各选项仅适用于 iOS 7.0 或更高版本。 对于每个选项，除“禁用触摸屏”默认设置为**开**之外，默认情况下均设置为**关**。
  - 禁用触摸屏
  - 禁用设备旋转感应
  - 禁用音量按钮
  - 禁用铃声开关 - **注意**：禁用此选项时，铃声行为取决于首次禁用时开关所处的位置。
  - 禁用睡眠/唤醒按钮
  - 禁用自动锁定
  - 禁用 VoiceOver
  - 启用缩放
  - 启用反转颜色
  - 启用 AssistiveTouch
  - 启用朗读所选内容
  - 启用单声道音频
- **用户已启用的选项**：以下各选项仅适用于 iOS 7.0 或更高版本。 对于各选项，默认设置为**关**。
  - 允许 VoiceOver 调整
  - 允许缩放调整
  - 允许反转颜色调整
  - 允许 AssitiveTouch 调整
- **策略设置**
  - o 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - o 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - o 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - o 如果单击**需要密码**，在**删除密码**旁边键入必需的密码。

配置 Android 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **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**：键入解锁应用程序的密码。
  - **阻止卸载**：选择是否允许用户卸载应用程序。 默认值为**关**。
  - **锁定屏幕**：单击“浏览”并导航到显示在设备锁定屏幕上的图像所在的位置，选择此图像。
  - **强制执行**：单击**黑名单**以创建不允许在设备上运行的应用程序的列表，或单击**白名单**以创建允许在设备上运行的应用程序的列表。
- **应用程序**：单击**添加**，然后执行以下操作：
  - **应用程序名称**：在列表中，单击要添加到白名单或黑名单的应用程序的名称，或单击**新增**向可用应用程序列表中添加新应用程序。
  - 如果选择**新增**，请在显示的字段中键入应用程序名称。
  - 单击**保存**或**取消**。
  - 为要添加到白名单或黑名单中的每个应用程序重复执行这些步骤。

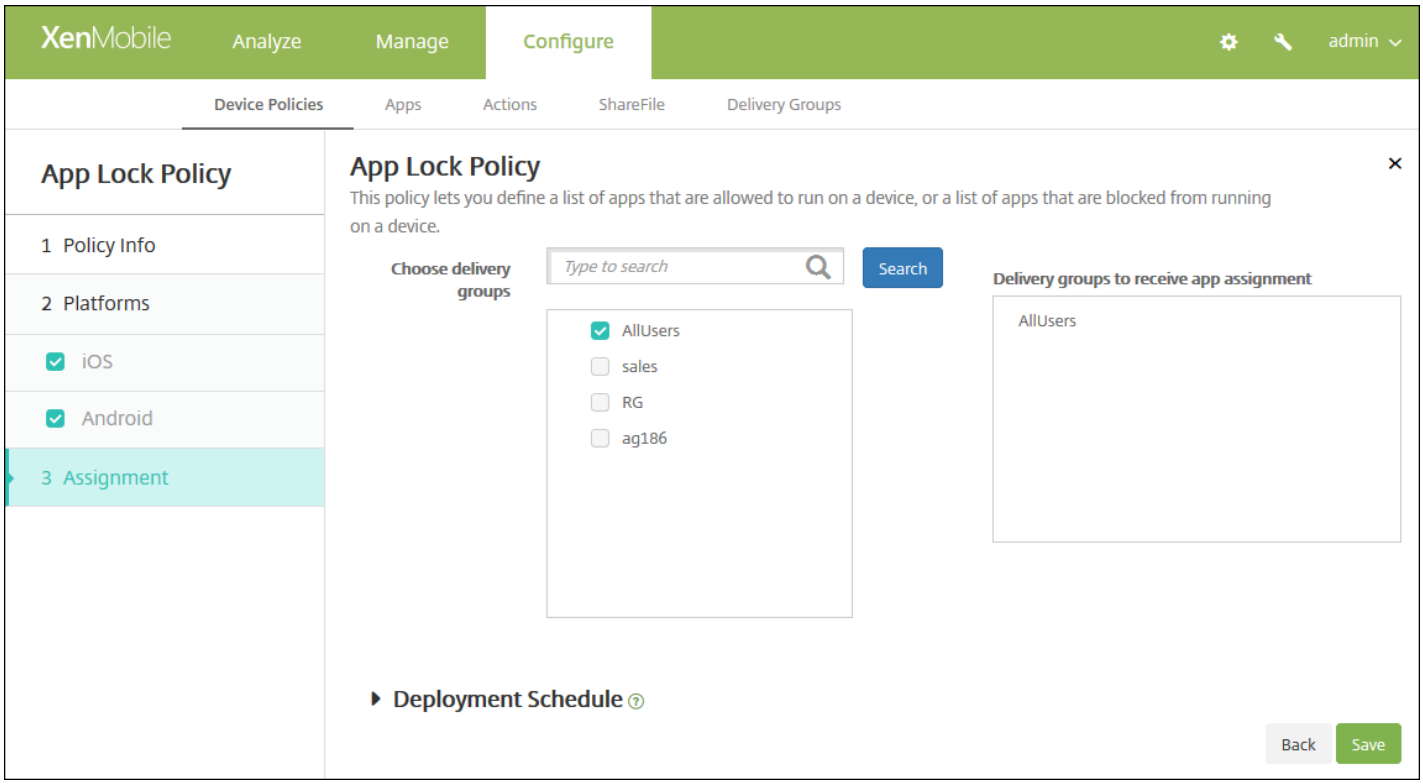
    注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 单击**下一步**，将显示**应用程序锁定策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序网络使用设备策略

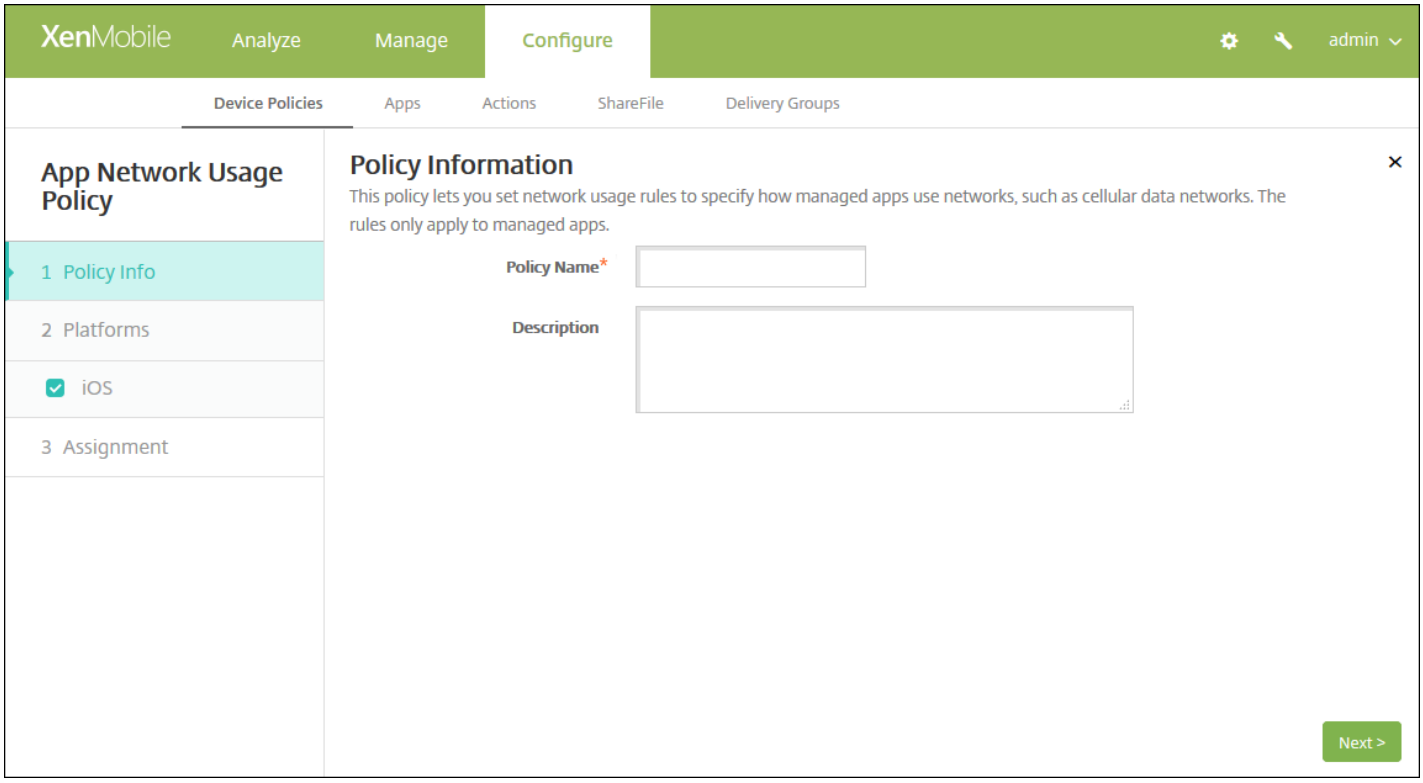
Aug 11, 2016

您可以设置网络使用规则，以指定 iOS 设备上托管应用程序使用网络（如手机数据网络）的方式。 规则仅适用于托管应用程序。 托管应用程序是您通过 XenMobile 部署到用户设备的应用程序。 其中不包括用户直接下载到设备上且未通过 XenMobile 部署的应用程序，或者在设备向 XenMobile 注册时已经安装到设备上的应用程序。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。

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**应用程序**下面，单击**应用程序网络使用**。 此时将显示**应用程序网络使用策略**信息页面。

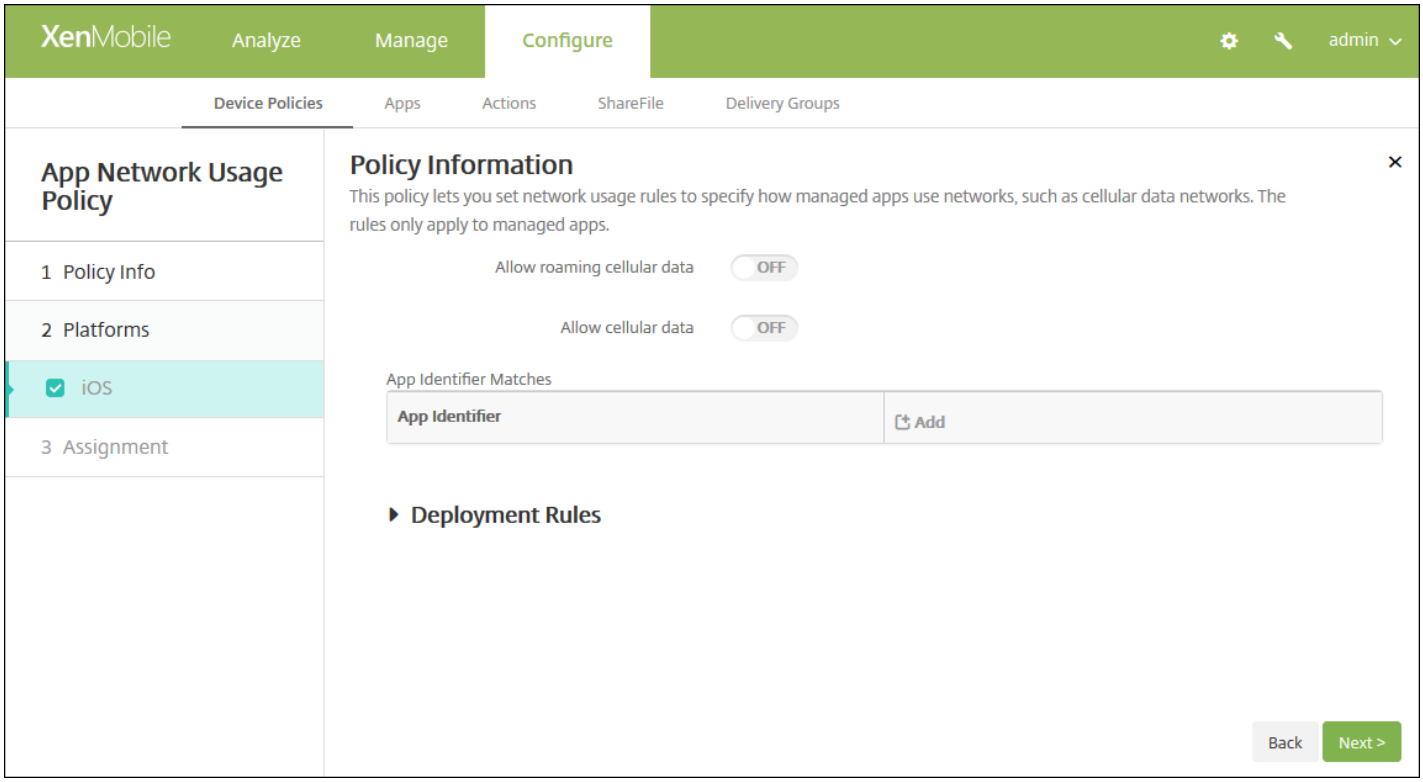


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 配置以下设置。

- **允许手机网络数据漫游**：选择指定应用程序是否可以在漫游时使用手机网络数据连接。 默认值为**关**。
- **允许手机网络数据**：选择指定应用程序是否可以使用手机网络数据连接。 默认值为**关**。
- **应用程序标识符匹配**：对于要添加到此列表中的每个应用程序，请单击**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中。

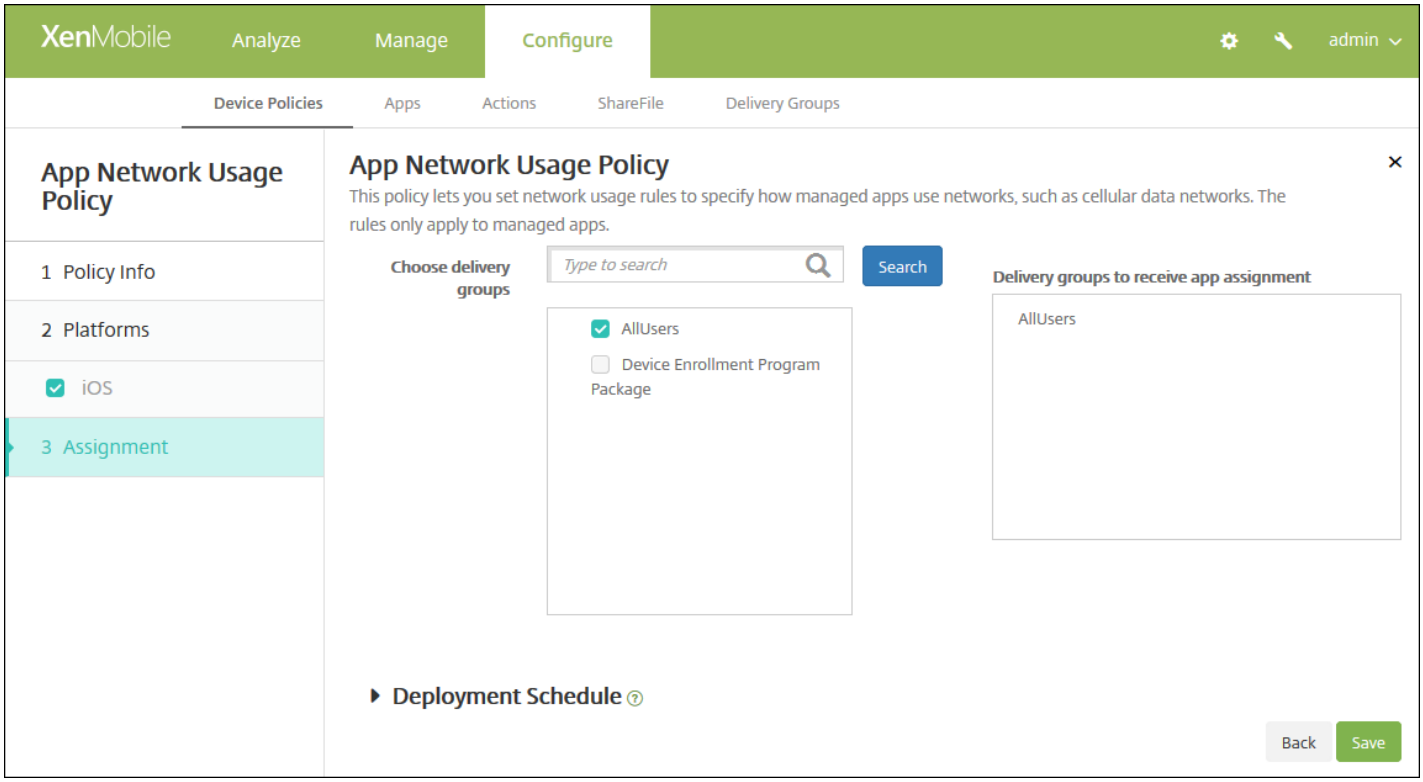
    注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**应用程序网络使用策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序限制设备策略

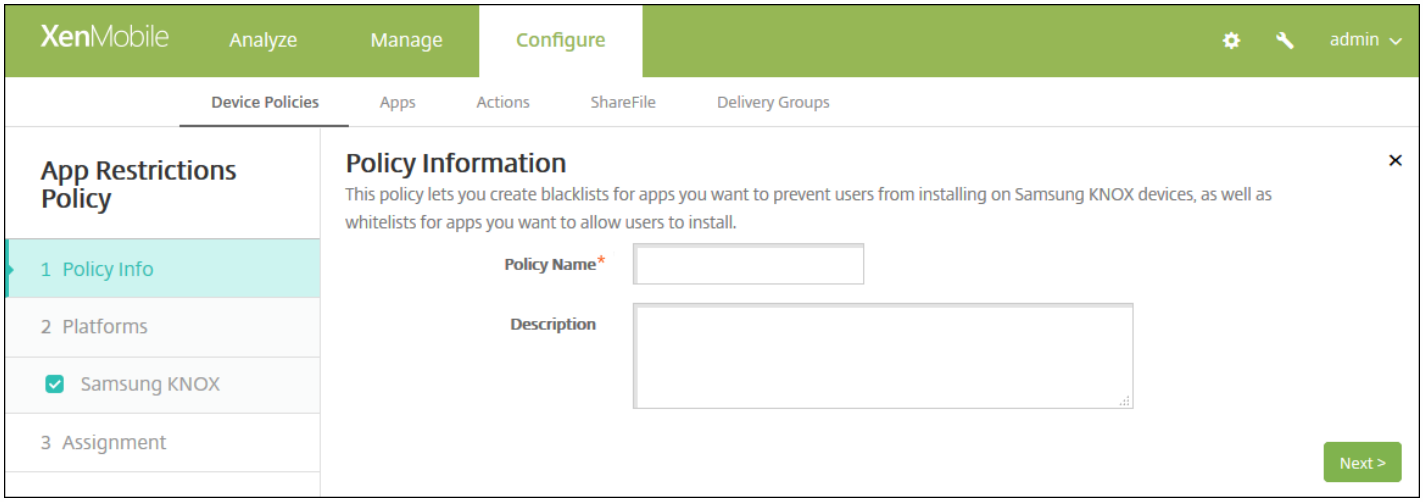
Aug 11, 2016

可以为希望阻止用户在 Samsung KNOX 设备上安装的应用程序创建黑名单，以及为希望允许用户安装的应用程序创建白名单。

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。

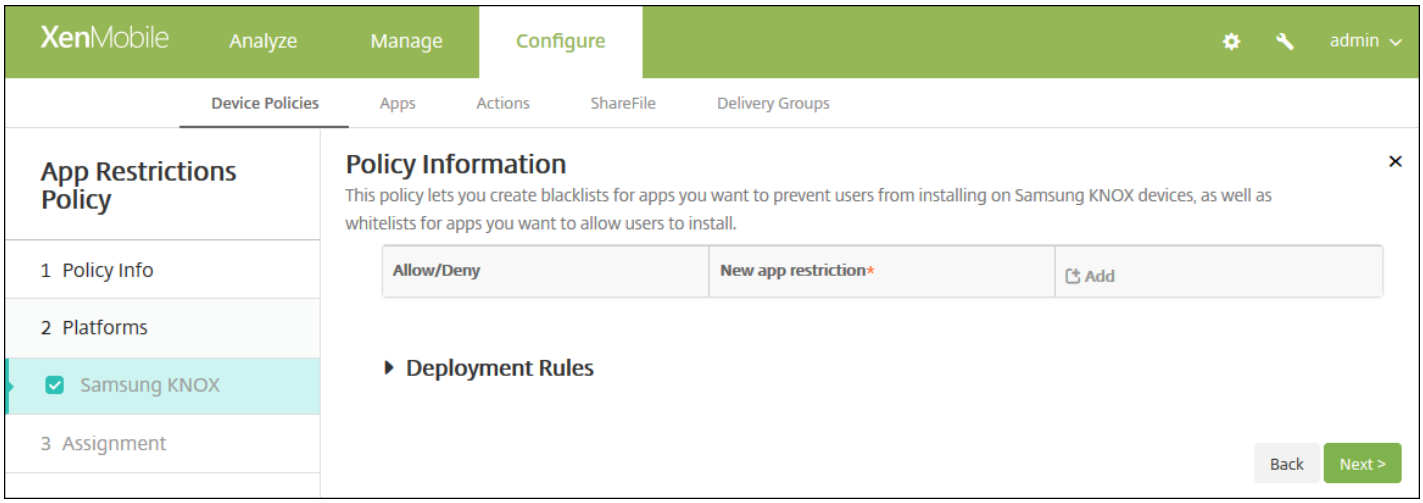
3. 展开**更多**，然后在**安全性**下面，单击**应用程序限制**。 此时将显示**应用程序限制策略**信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Samsung KNOX 平台**页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 对于要添加到“允许/拒绝”列表中的每个应用程序，请单击**添加**，然后执行以下操作：

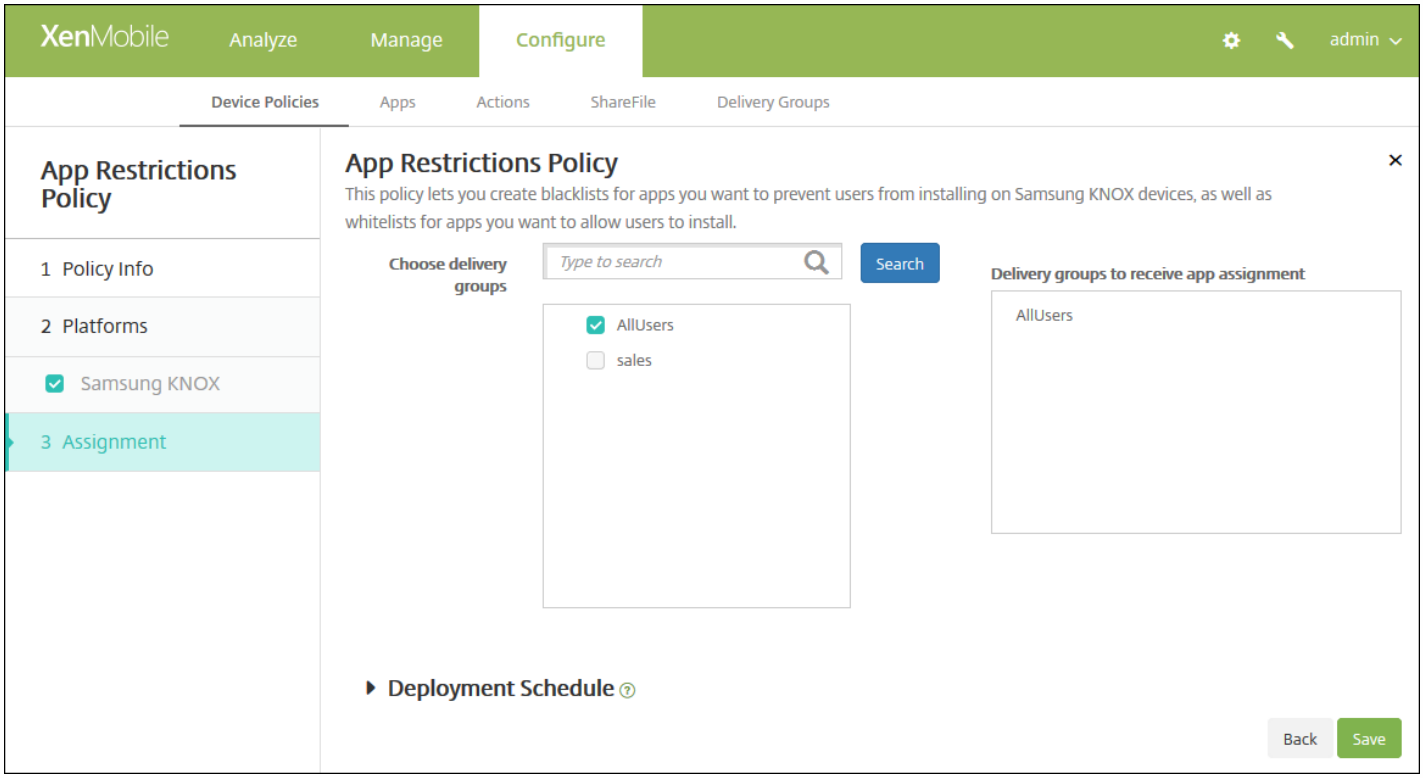
- **允许/拒绝**：选择是否允许用户安装应用程序。
- **新应用程序限制**：键入应用程序软件包 ID；例如 com.kmdm.af.crackle。
- 单击**保存**将应用程序保存到“允许/拒绝”列表，或单击**取消**不将应用程序保存到“允许/拒绝”列表中。

  注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

  要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**应用程序限制策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序通道设备策略

Aug 11, 2016

应用程序通道旨在提高移动应用程序的服务连续性及数据传输可靠性。 应用程序通道定义移动设备应用程序的客户端组件与应用程序服务器组件之间的代理参数。 还可以使用应用程序通道创建设备的远程支持通道以使用管理支持。 可以为 Android 和 Windows Mobile/CE 设备配置应用程序通道策略。

注意： 通过在此策略中定义的通道发送的任何应用程序流量均先通过 XenMobile，然后再被重定向到运行此应用程序的服务器。

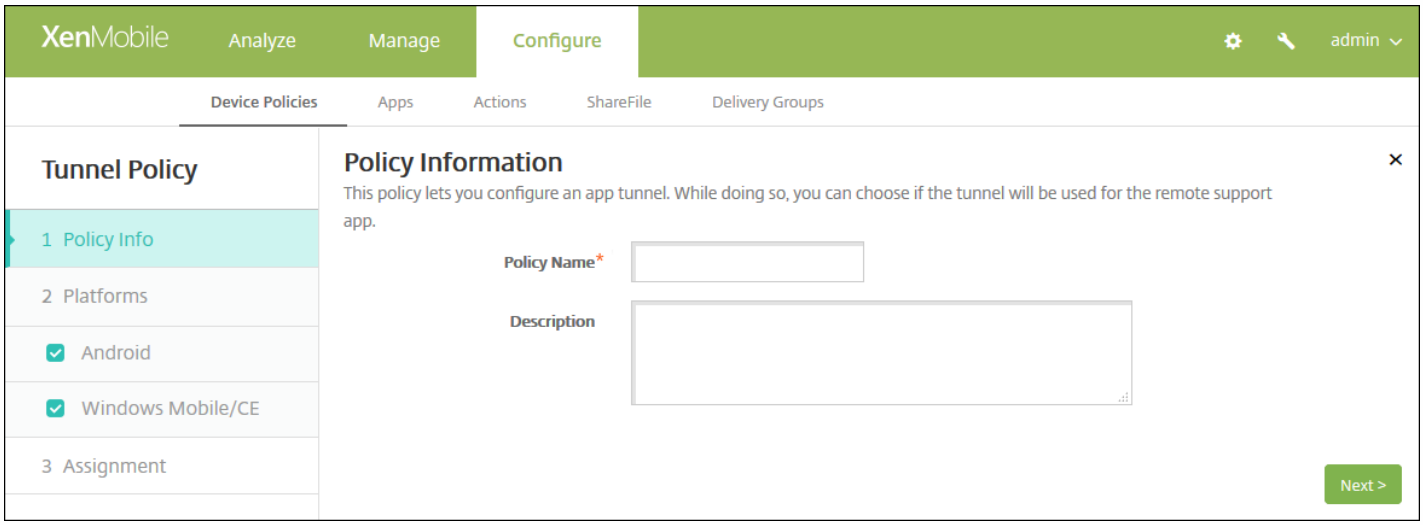
Android 设置

Windows Mobile/CE 设置

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. 单击**更多**，然后在**网络访问权限**下面，单击**通道**。 此时将显示**通道策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

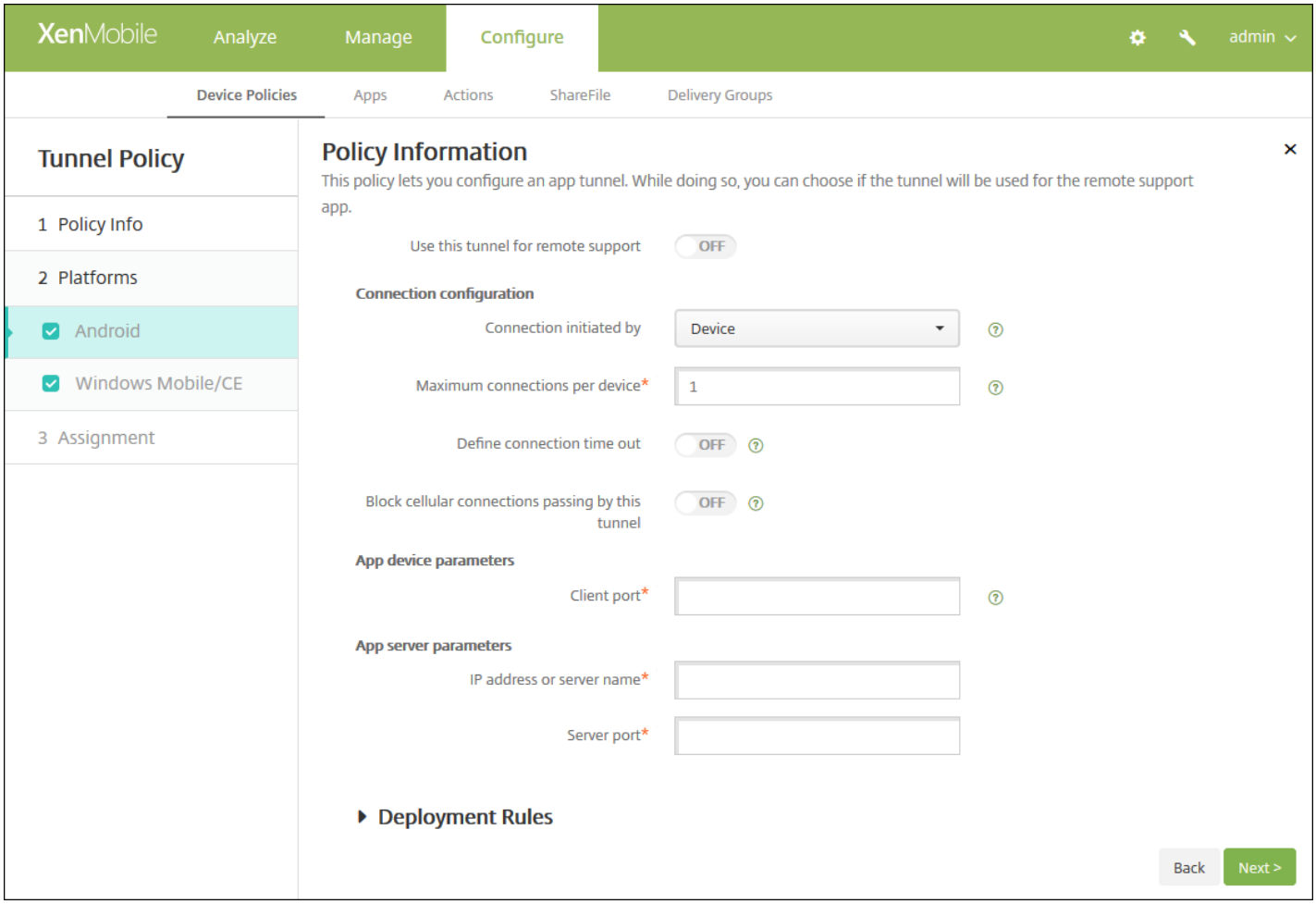
5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Android 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **使用此通道进行远程支持**：选择是否将此通道用于远程支持。

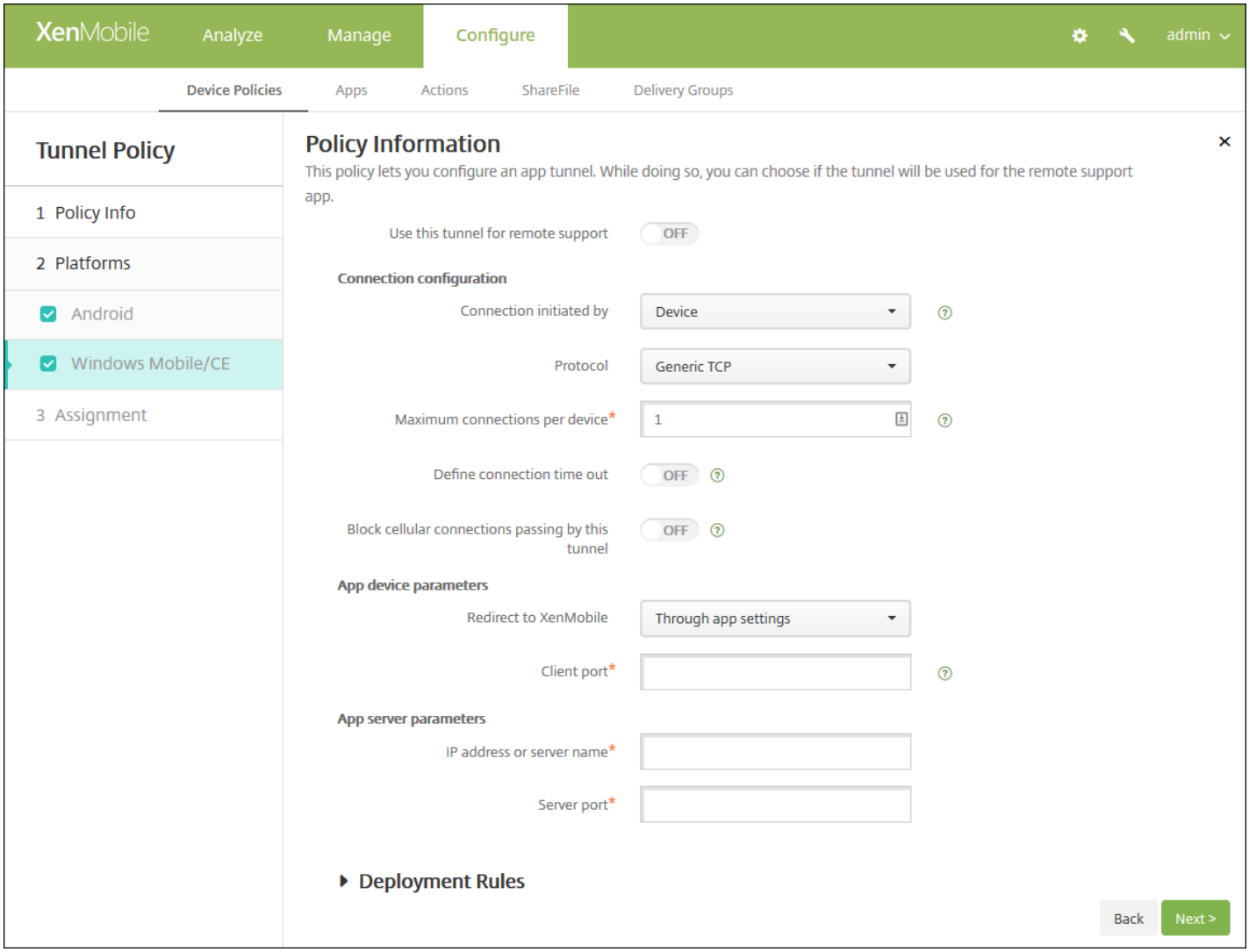
  注意：根据是否选择远程支持，配置步骤会有所不同。

- 如果不选择远程支持，请执行以下操作：
  - **连接发起者**：单击**设备**或**服务器**以指定发起连接的源。
  - **每台设备最大连接数**：键入一个数字，用于指定应用程序可以建立的并发 TCP 连接数。 此字段仅适用于设备发起的连接。
  - **定义连接超时**：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - **连接超时**：如果将**定义连接超时**设置为**开**，则键入通道关闭前应用程序可以空闲的时间长度，以秒为单位。
  - **阻止手机网络连接通过此通道**：选择是否在漫游时阻止此通道。
    注意：不会阻止 WiFi 和 USB 连接。
  - **客户端端口**：键入客户端端口号。 在大多数情况下，此值与服务器端口相同。
  - **IP 地址或服务器名称**：键入应用程序服务器的 IP 地址或名称。 此字段仅适用于设备发起的连接。
  - **服务器端口**：键入服务器端口号。
- 如果选择远程支持，请执行以下操作：
  - **使用此通道进行远程支持**：设置为**开**。
  - **定义连接超时**：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - **连接超时**：如果将**定义连接超时**设置为开，则键入通道关闭前应用程序可以空闲的时间长度，以秒为单位。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **使用 SSL 连接**：选择是否为此通道使用安全 SSL 连接。
- **阻止手机网络连接通过此通道**：选择是否在漫游时阻止此通道。
  注意：不会阻止 WiFi 和 USB 连接。

配置 Windows Mobile/CE 设置



配置以下设置：

- **使用此通道进行远程支持**：选择是否将此通道用于远程支持。

  注意：根据是否选择远程支持，配置步骤会有所不同。

- 如果不选择远程支持，请执行以下操作：
  - **连接发起者**：单击**设备**或**服务器**以指定发起连接的源。
  - **协议**：在列表中，单击要使用的协议。 默认值为**通用 TCP**。
  - **每台设备最大连接数**：键入一个数字，用于指定应用程序可以建立的并发 TCP 连接数。 此字段仅适用于设备发起的连接。
  - **定义连接超时**：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - **连接超时**：如果将**定义连接超时**设置为**开**，则键入通道关闭前应用程序可以空闲的时间长度，以秒为单位。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

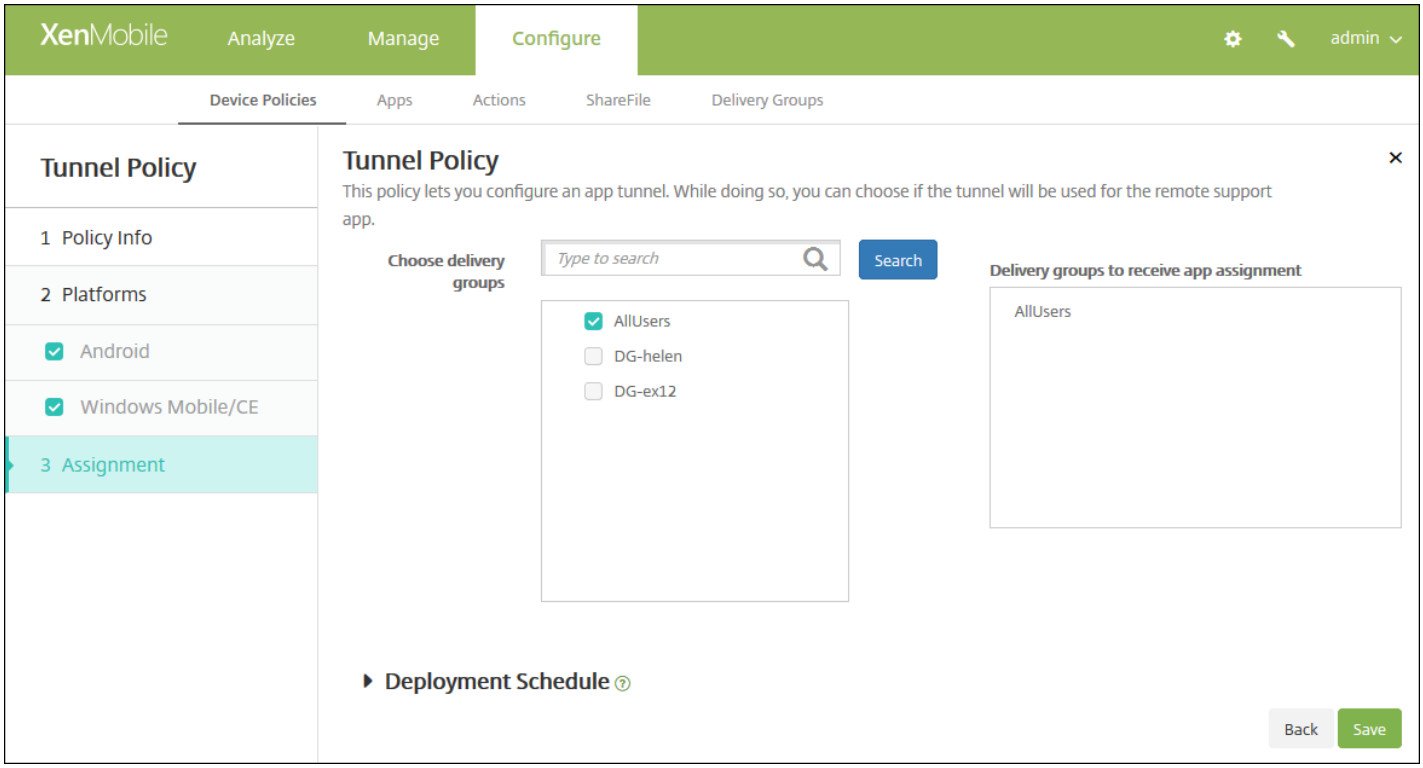
- **阻止手机网络连接通过此通道**：选择是否在漫游时阻止此通道。
  注意：不会阻止 WiFi 和 USB 连接。

- **重定向到 XenMobile**：在列表中，单击设备连接到 XenMobile 的方式。 默认值为**通过应用程序设置**。
  - 如果选择**使用本地别名**，请在**本地别名**中键入别名。 默认值为 **localhost**。
  - 如果选择 **IP 地址范围**，请在 **IP 地址范围起点**中键入起始 IP 地址，在 **IP 地址**范围终点中键入结束 IP 地址。
- **客户端端口**：键入客户端端口号。 在大多数情况下，此值与服务器端口相同。
- **IP 地址或服务器名称**：键入应用程序服务器的 IP 地址或名称。 此字段仅适用于设备发起的连接。
- **服务器端口**：键入服务器端口号。

- 如果选择远程支持，请执行以下操作：
  - **使用此通道进行远程支持**：设置为**开**。
  - **定义连接超时**：选择是否设置通道关闭前应用程序可以空闲的时间长度。
    - **连接超时**：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度，以秒为单位。
  - **使用 SSL 连接**：选择是否为此通道使用安全 SSL 连接。
  - **阻止手机网络连接通过此通道**：选择是否在漫游时阻止此通道。
    注意：不会阻止 WiFi 和 USB 连接。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Tunnel Policy**（通道策略）分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 如果单击**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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序卸载设备策略

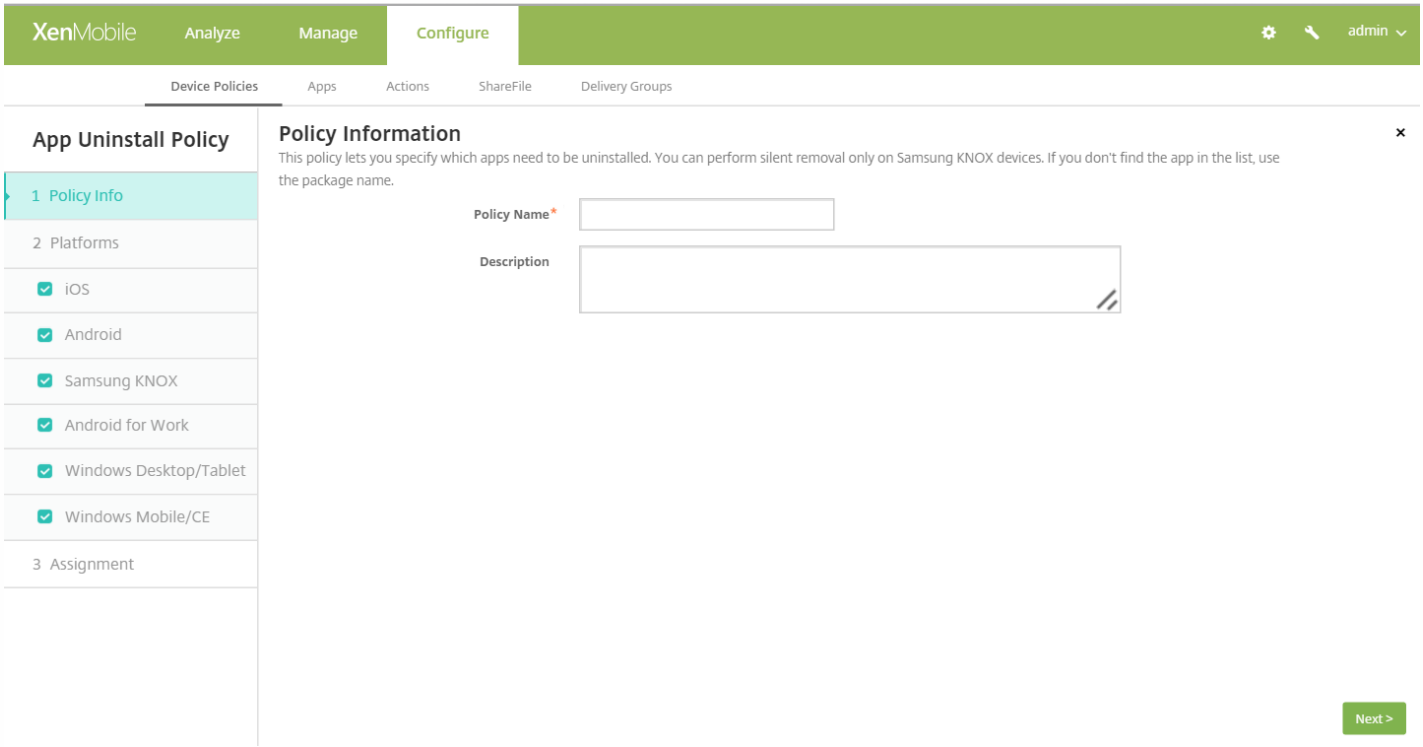
Aug 11, 2016

您可以为 iOS、Android、Samsung KNOX、Android for Work、Windows Desktop/Tablet 和 Windows Mobile/CE 平台创建应用程序卸载策略。 通过应用程序卸载策略，您可以因任何原因将应用程序从用户设备中删除。 原因可以是您不再想要支持某些应用程序，贵公司可能要将现有应用程序替换为其他供应商的类似应用程序等等。 当此策略部署到用户的设备时，应用程序被删除。 用户会收到卸载应用程序的提示，但是 Samsung KNOX 设备除外；Samsung KNOX 设备用户不会收到卸载应用程序的提示。

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**应用程序**下面，单击**应用程序卸载**。 此时将显示**应用程序卸载策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

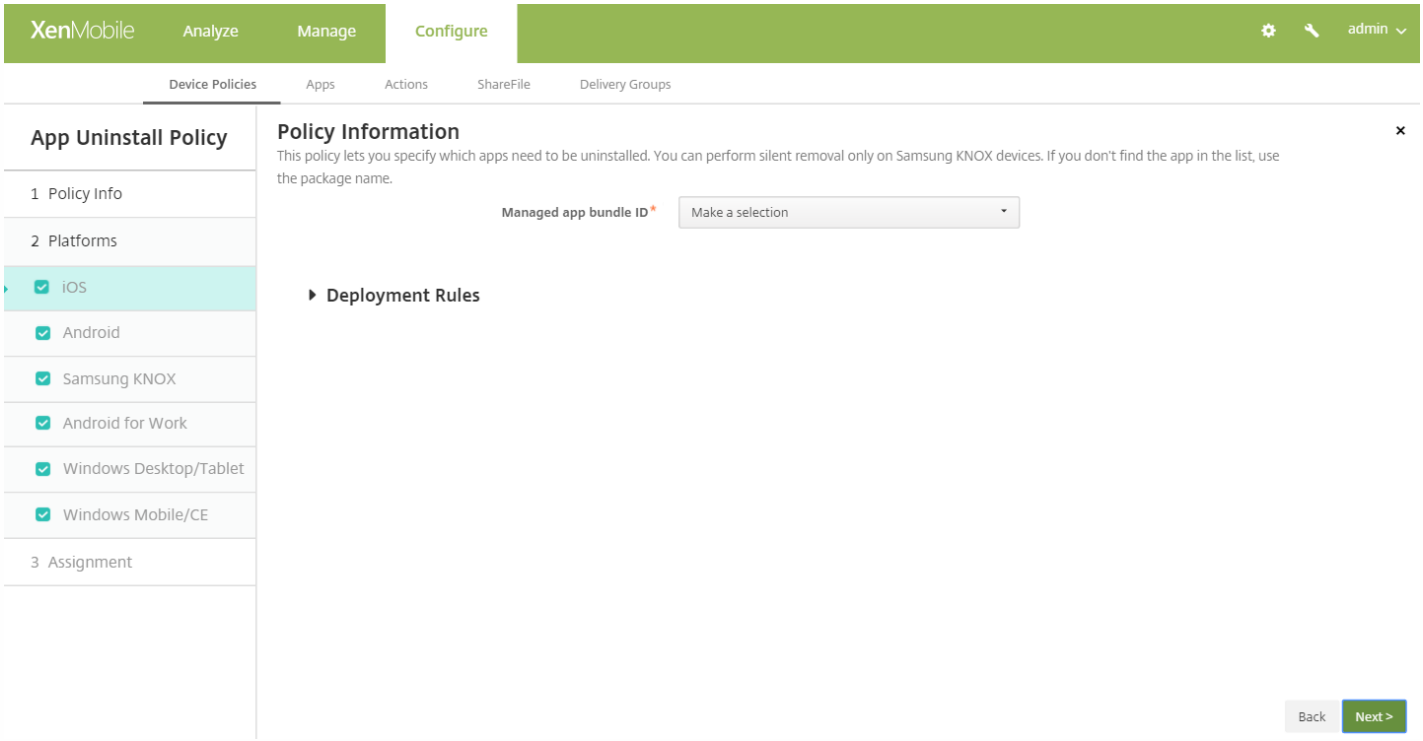
5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

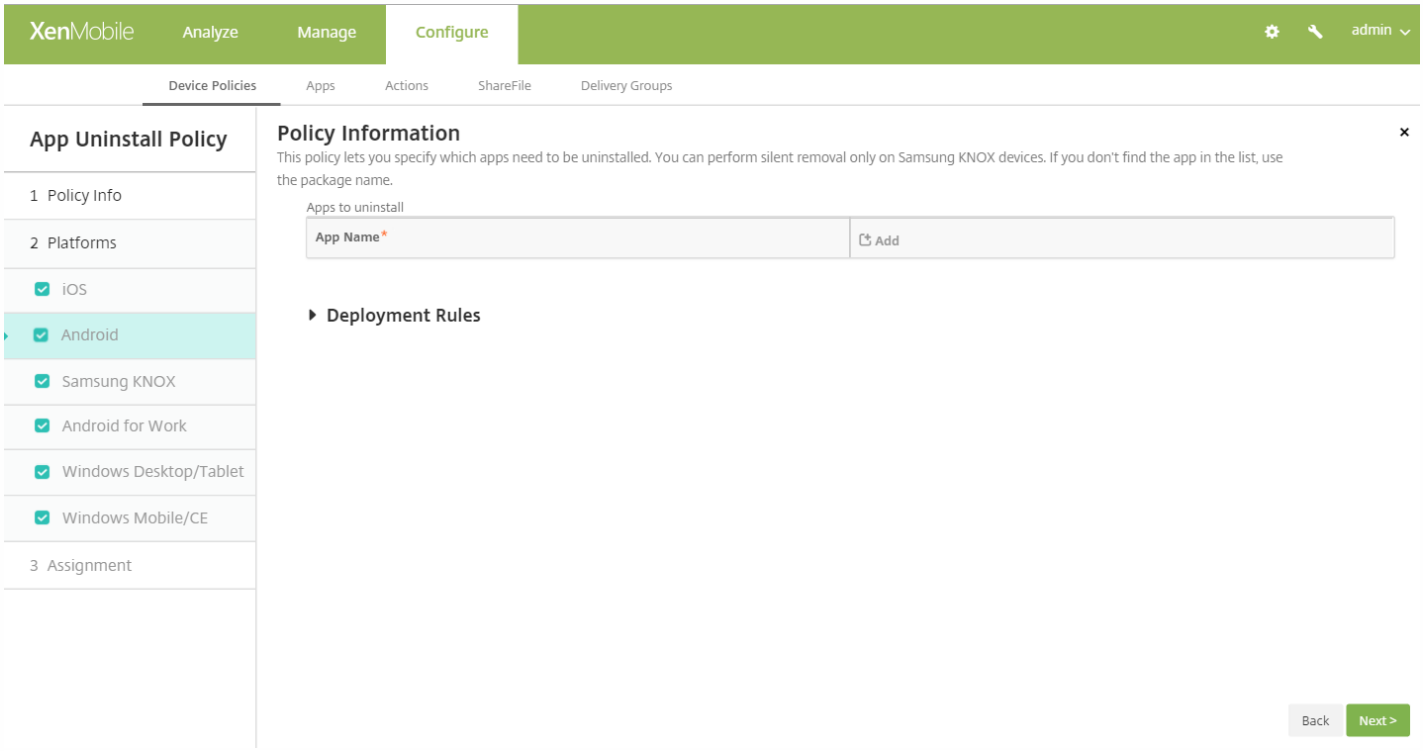
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **托管应用程序捆绑包 ID**：在列表中，单击现有应用程序或单击**新增**。 如果此平台没有配置应用程序，该列表将是空的，您必须添加新的应用程序。
  - 如果单击**添加**，您可在出现的字段中键入应用程序的名称。

配置所有其他平台设置



© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置以下设置：

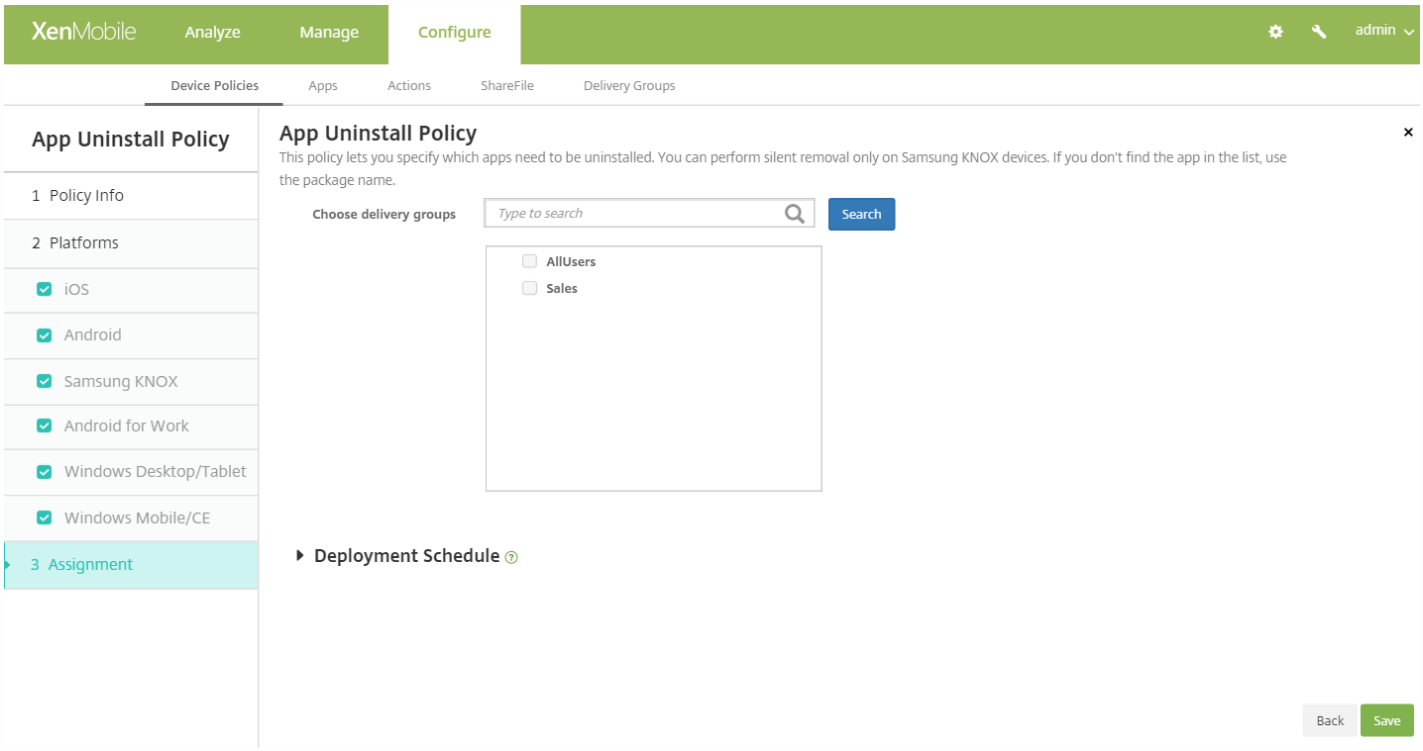
- **要卸载的应用程序**：对于您要添加的各个应用程序，单击**添加**，然后执行以下操作：
  - **应用程序名称**：在列表中，单击现有的应用程序，或单击**新增**输入新的应用程序名称。 如果此平台没有配置应用程序，该列表将是空的，您必须添加新的应用程序。
  - 单击**添加**以添加应用程序，或单击**取消**以取消添加应用程序。

    注意：要从卸载策略删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**应用程序卸载策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序卸载限制设备策略

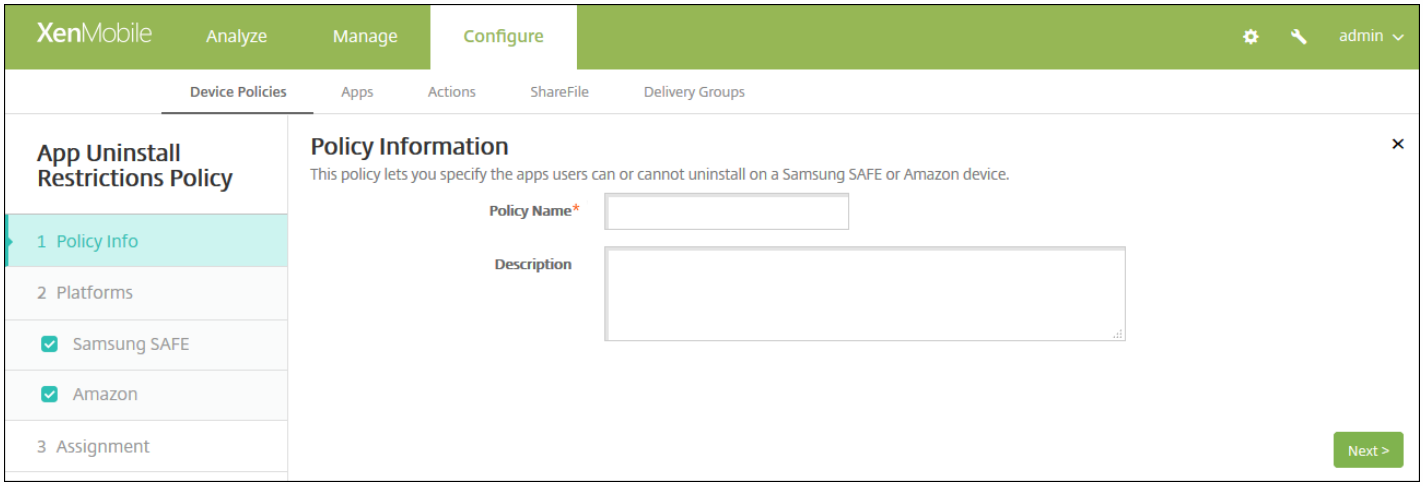
Aug 11, 2016

可以指定用户在 Samsung SAFE 或 Amazon 上可以卸载或不可以卸载的应用程序。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。

2. 单击**添加**。 此时将显示**添加新策略**对话框。

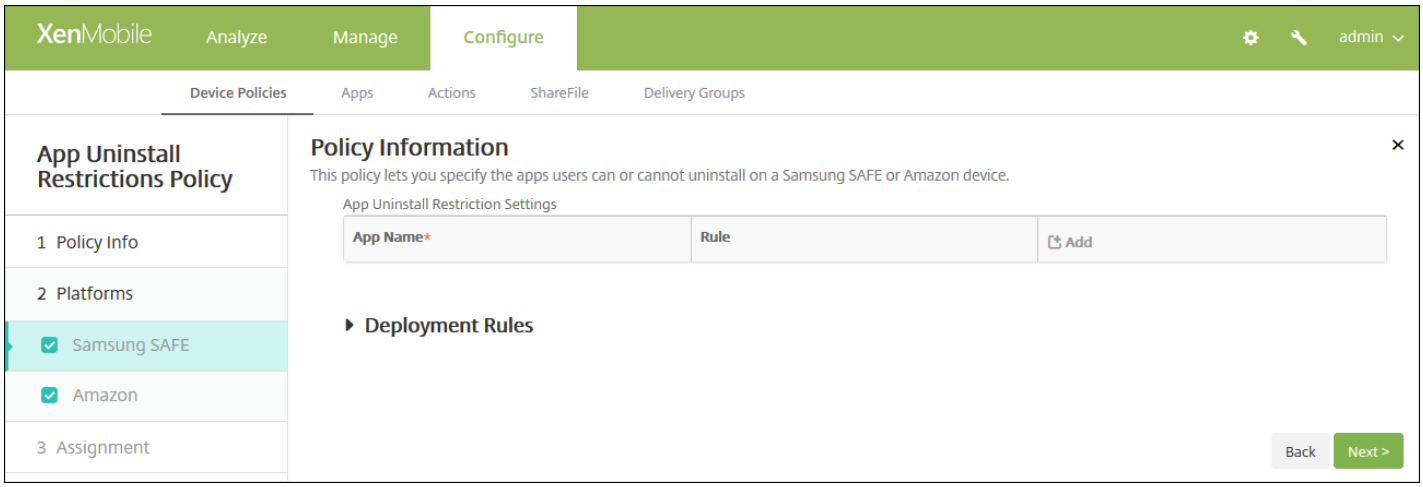
3. 展开**更多**，然后在**应用程序**下面，单击**应用程序卸载限制**。 此时将显示**应用程序卸载限制策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。



6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 为您选择的每个平台配置以下设置：

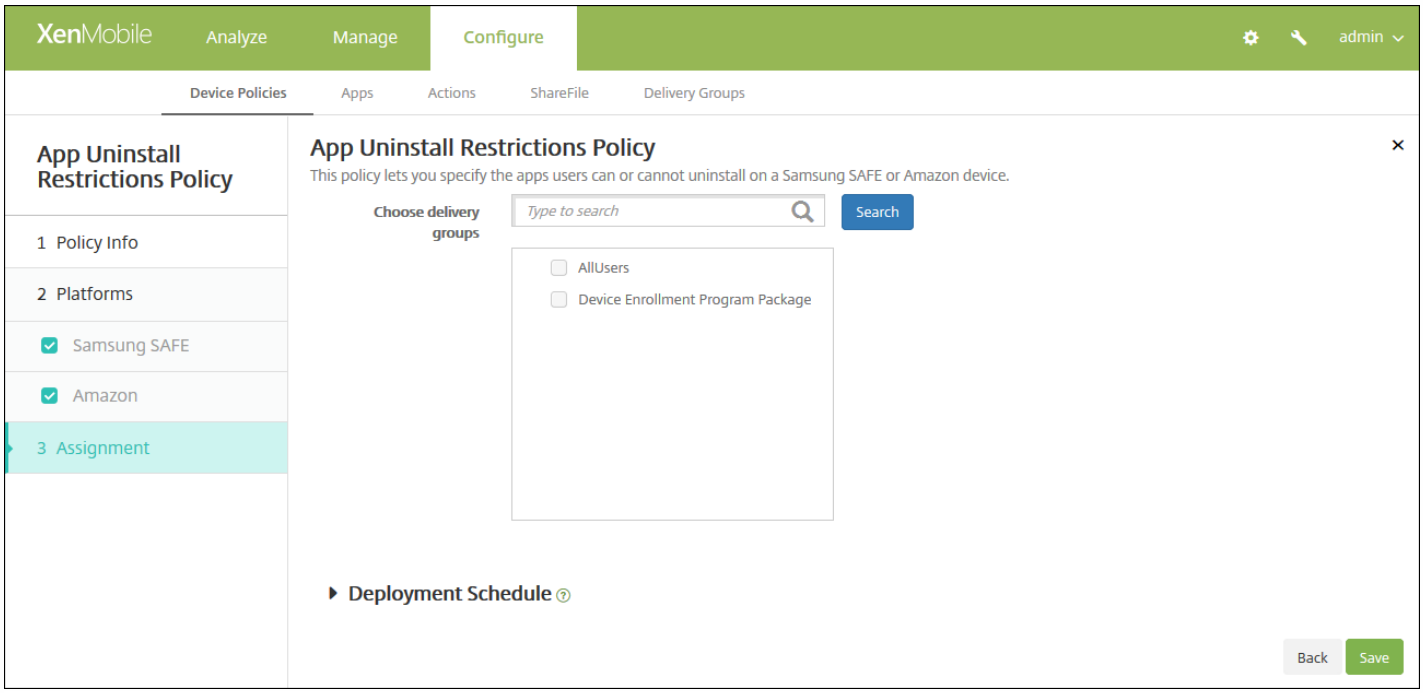
- **应用程序卸载限制设置**：对于要添加的各个应用程序规则，单击**添加**，然后执行以下操作：
  - **应用程序名称**：在列表中，单击某个应用程序，或单击**新增**以添加新应用程序。
  - **规则**：选择用户是否可以卸载应用程序。 默认设置为允许卸载。
  - 单击**保存**或**取消**。

    注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

8. 配置部署规则

9. 单击**下一步**。 此时将显示**应用程序卸载限制策略**分配页面。



10. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

11. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

浏览器设备策略

Aug 11, 2016

可以创建 适用于 Samsung SAFE、Samsung KNOX 和 Android for Word 设备的浏览器设备策略，以定义用户的设备是否可以使用浏览器，或限制用户的设备可以使用的浏览器功能。 在 Samsung 设备上，可以完全禁用浏览器，也可以启用或禁用弹出消息、JavaScript、Cookie、自动填充和是否强制显示欺诈警告。 在 Android for Works 设备上，可以将特定 URL 加入黑名单或白名单，以及添加特定安全浏览器书签。

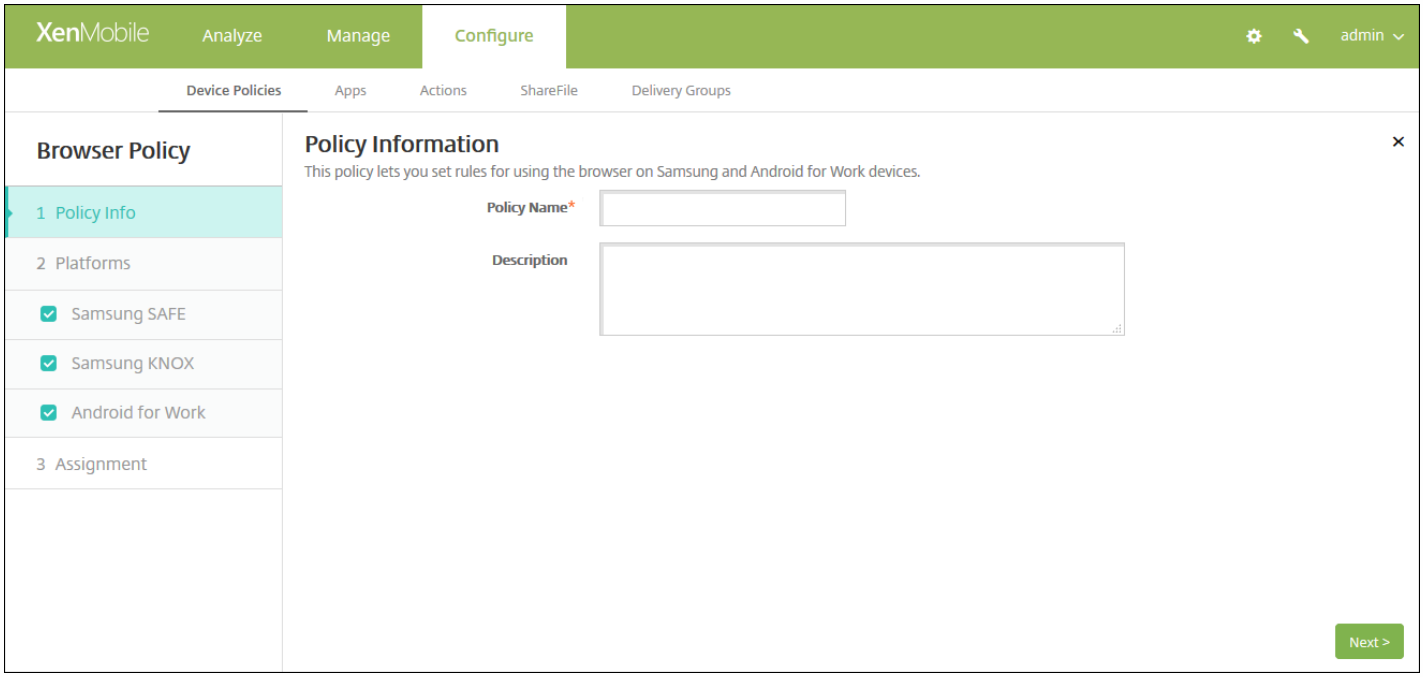
Samsung SAFE 和 Samsung KNOX 设置

Android for Work 设置

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**添加新策略。 此时将显示**添加新策略**对话框。

3. 单击**更多**，然后在**应用程序**下面，单击**浏览器**。 此时将显示**浏览器策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

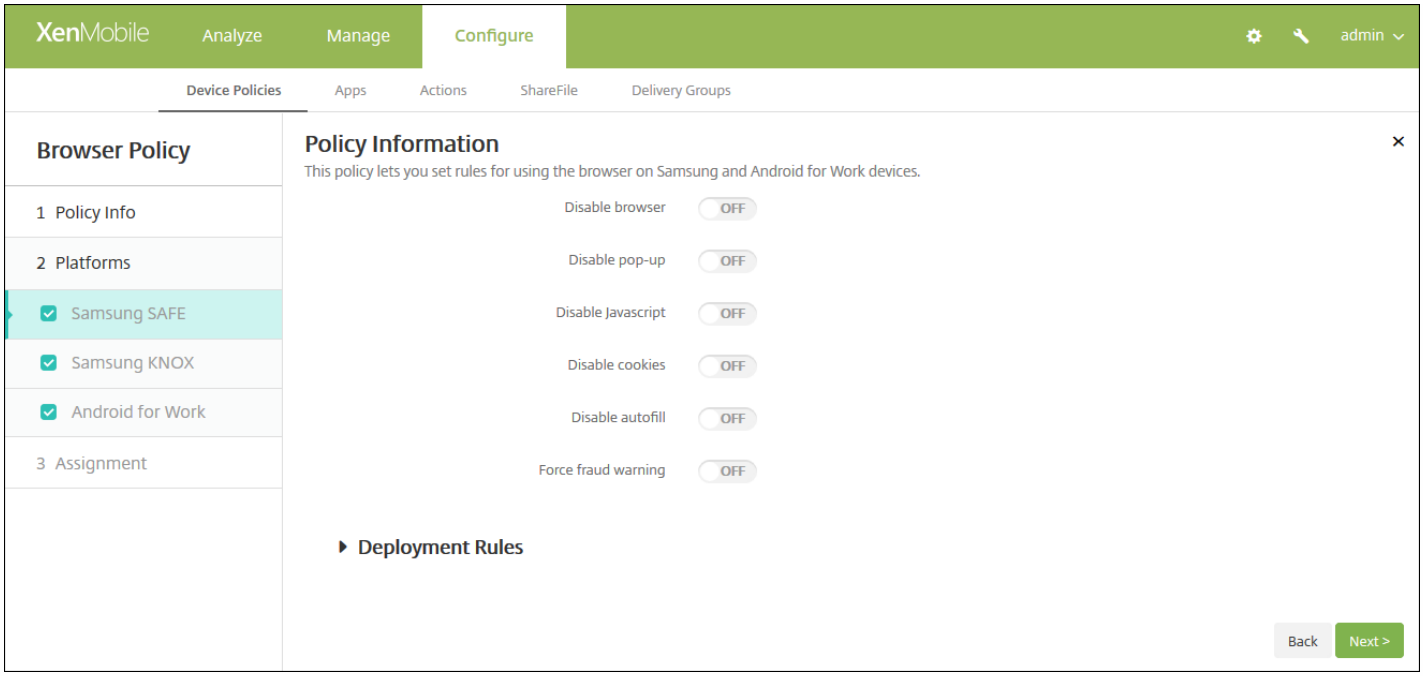
5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Samsung SAFE 和 Samsung KNOX 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

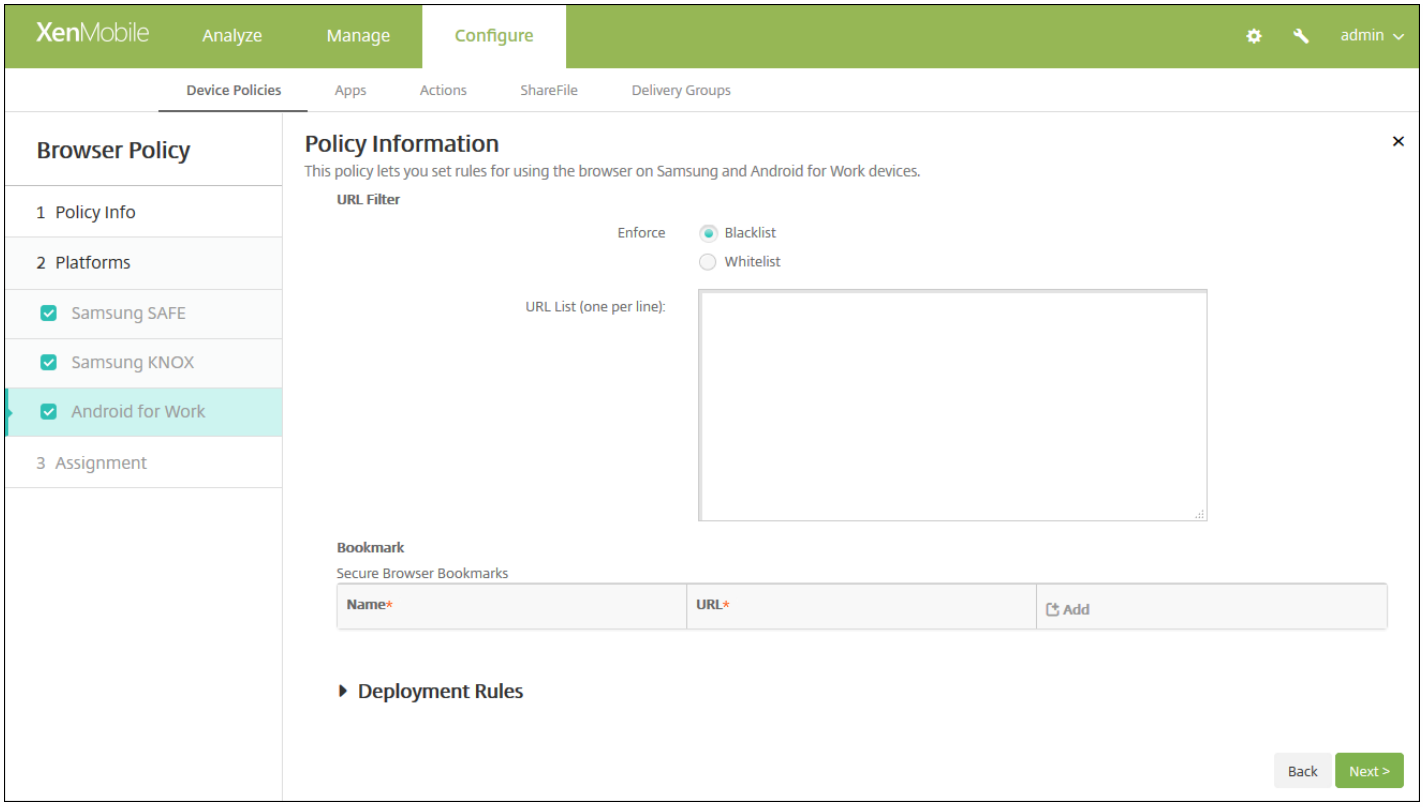


配置以下设置：

- **禁用浏览器**：选择是否在用户设备上完全禁用 Samsung 浏览器。 默认设置为**关**，表示允许用户使用此浏览器。 禁用此浏览器后，将不再显示以下选项。
- **禁用弹出窗口**：选择是否允许在此浏览器上显示弹出消息。
- **禁用 Javascript**：选择是否允许在此浏览器上运行 Javascript。
- **禁用 Cookie**：选择是否允许 Cookie。
- **禁用自动填充**：选择是否允许用户启用此浏览器的自动填充功能。
- **强制显示欺诈警告**：选择在用户访问欺诈性或存在漏洞的 Web 站点时是否显示警告。

配置 Amazon for Work 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



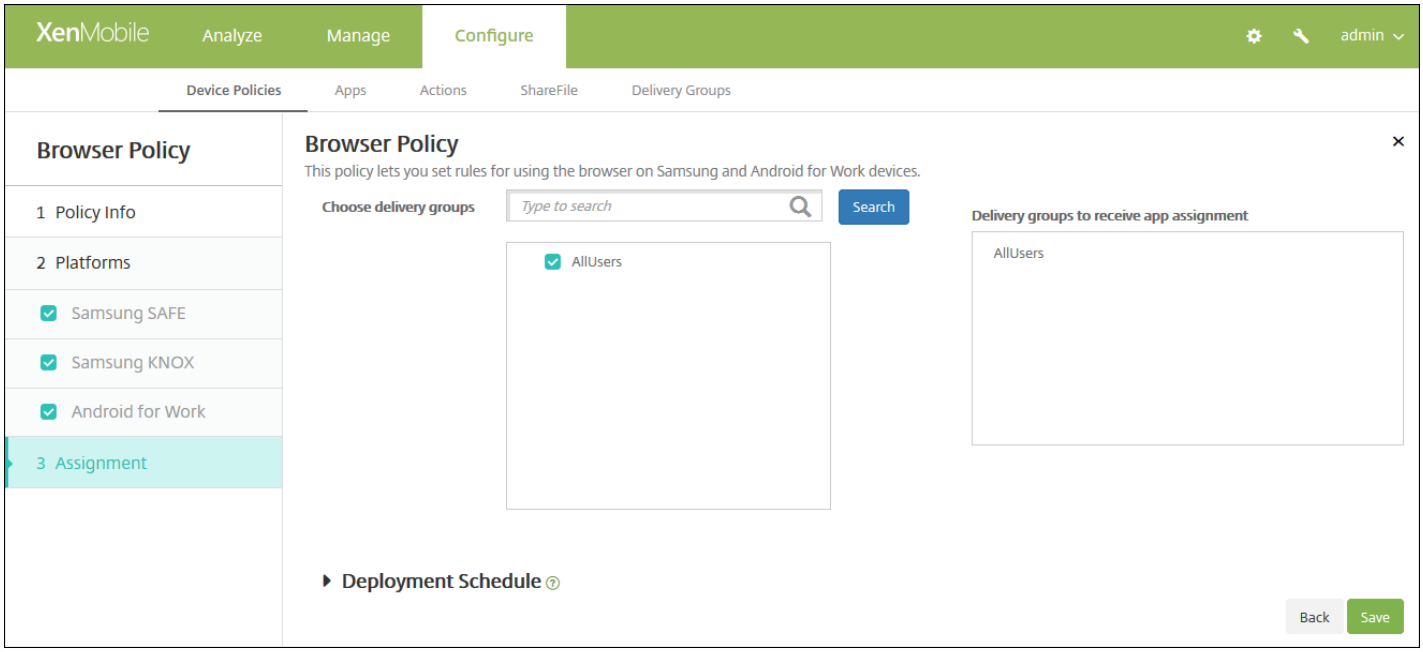
配置以下设置：

- 在 **URL 过滤器**下，配置以下设置：
  - **强制执行**：选择**黑名单**或**白名单**。 如果选择**黑名单**，用户可以访问*除*您指定的 URL 之外的所有 URL。 如果选择**白名单**，用户*只可以*访问您指定的 URL。
  - **URL 列表**：为您在**强制执行**中选择的列表类型键入 URL（每行一个）。
- 在**书签**下面，单击**添加**，键入显示在用户安全浏览器上的书签**名称**和 **URL**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**浏览器策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

日历 (CalDav) 设备策略

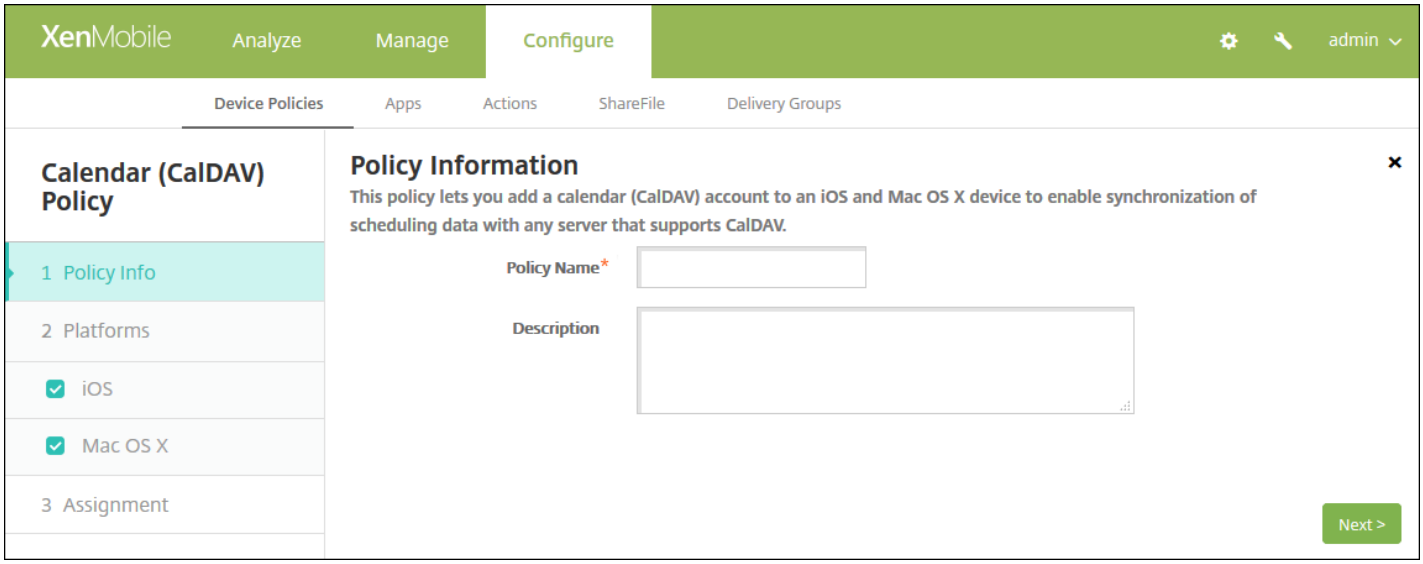
Aug 11, 2016

可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 或 Mac OS X 设备添加日历 (CalDAV) 帐户，使用户可以将其计划数据与任何支持 CalDAV 的服务器同步。

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**最终用户**下面，单击**日历(CalDav)**。 此时将显示**日历(CalDav)策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

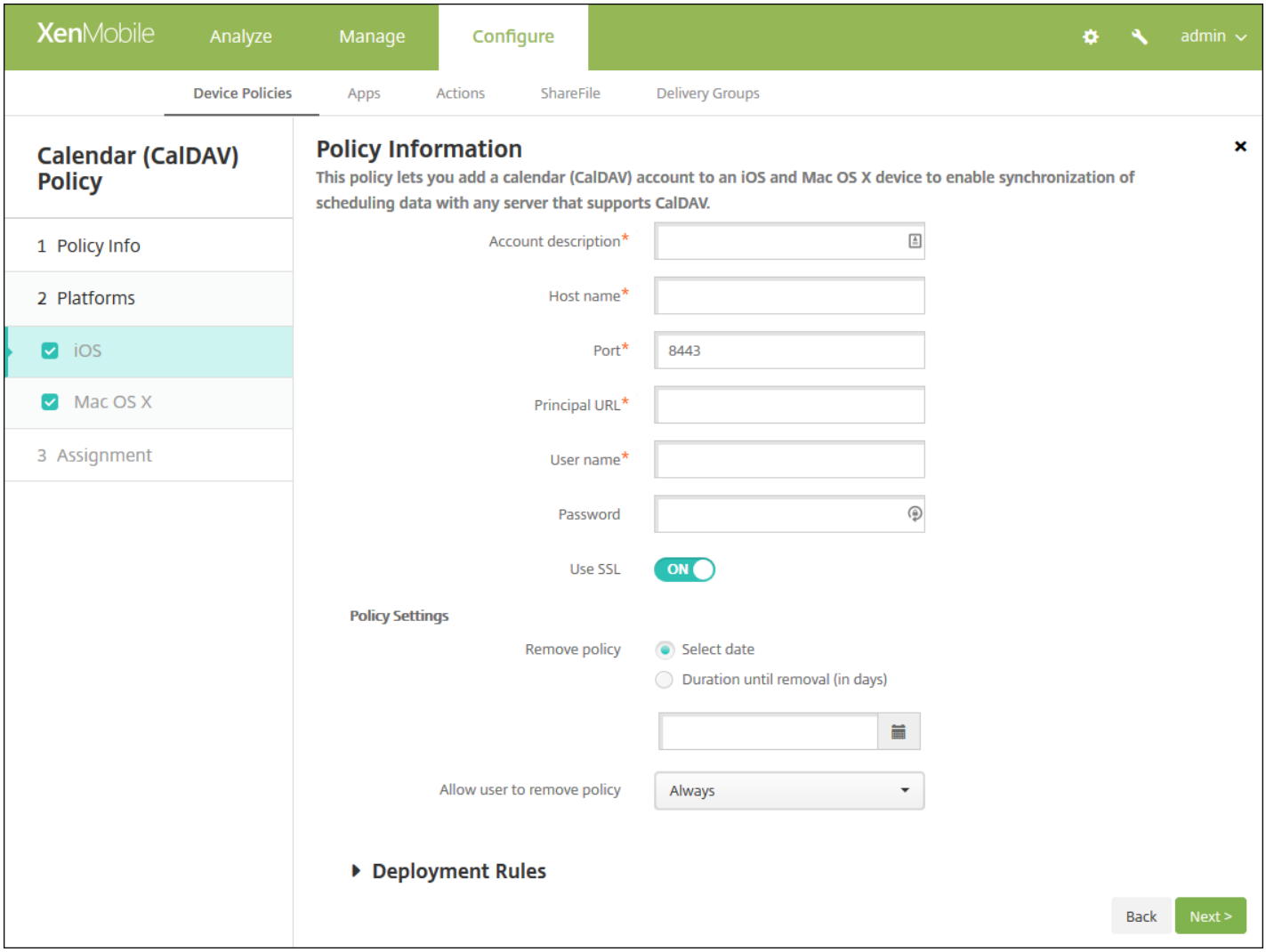
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

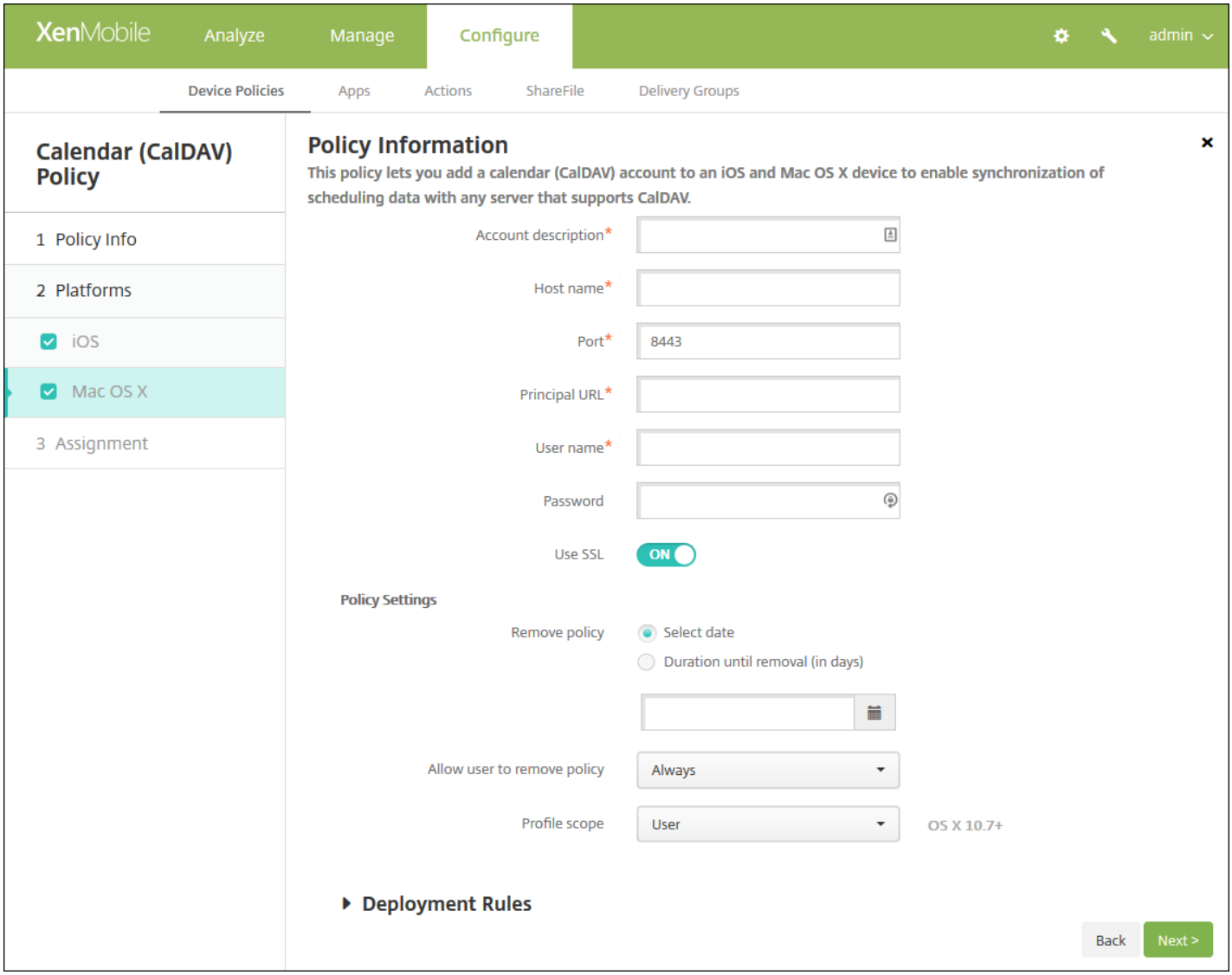


配置以下设置：

- **帐户说明**：键入帐户说明。 此字段为必填字段。
- **主机名**：键入 CalDAV 服务器的地址。 此字段为必填字段。
- **端口**：键入连接到 CalDAV 服务器使用的端口。 此字段为必填字段。 默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的登录名称。 此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。 默认值为**开**。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



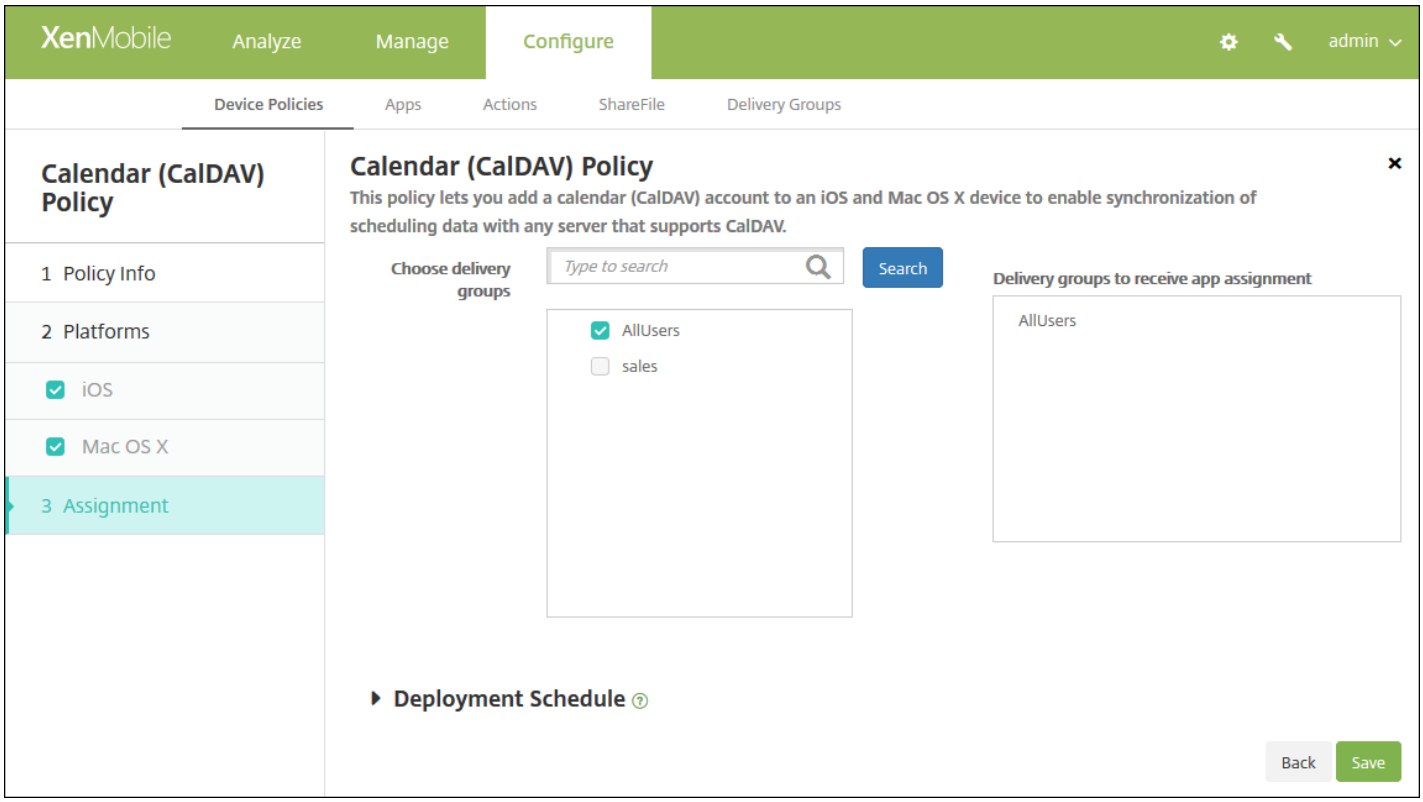
配置以下设置：

- **帐户说明**：键入帐户说明。 此字段为必填字段。
- **主机名**：键入 CalDAV 服务器的地址。 此字段为必填字段。
- **端口**：键入连接到 CalDAV 服务器使用的端口。 此字段为必填字段。 默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的 登录 名。 此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。 默认值为**开**。
- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 单击**下一步**。 此时将显示**日历(CalDAV)策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

手机网络设备策略

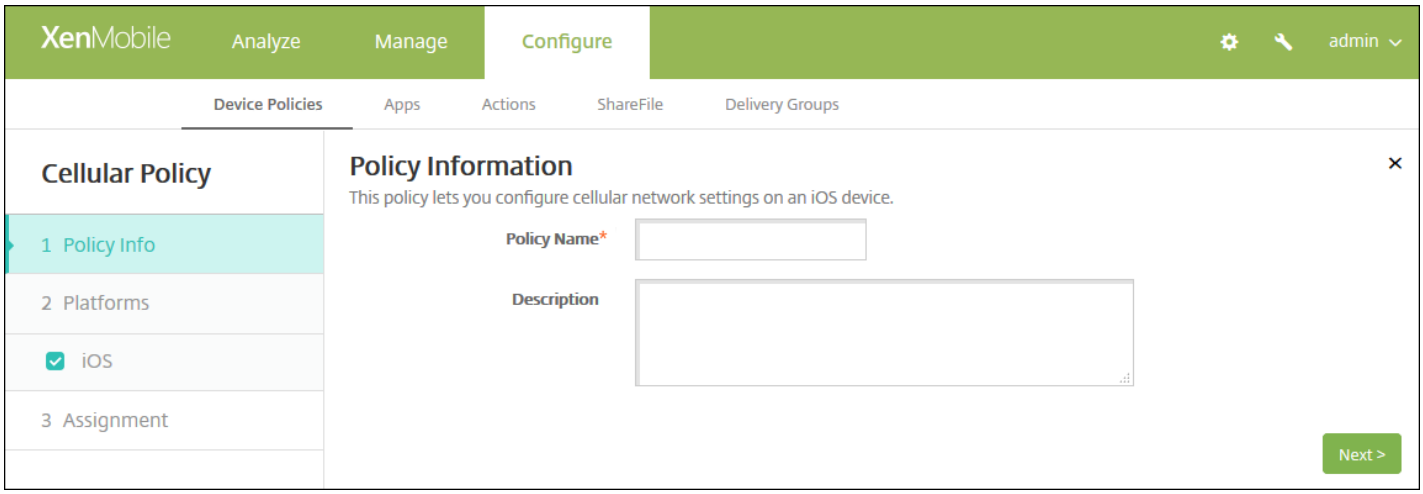
Aug 11, 2016

此策略允许您在 iOS 设备上配置手机网络设置。

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**。 将显示**添加新策略**页面。

3. 展开**更多**，然后在**网络访问权限**下，单击**手机网络**。 此时 **Cellular Network Policy**（手机网络策略）信息页面出现。

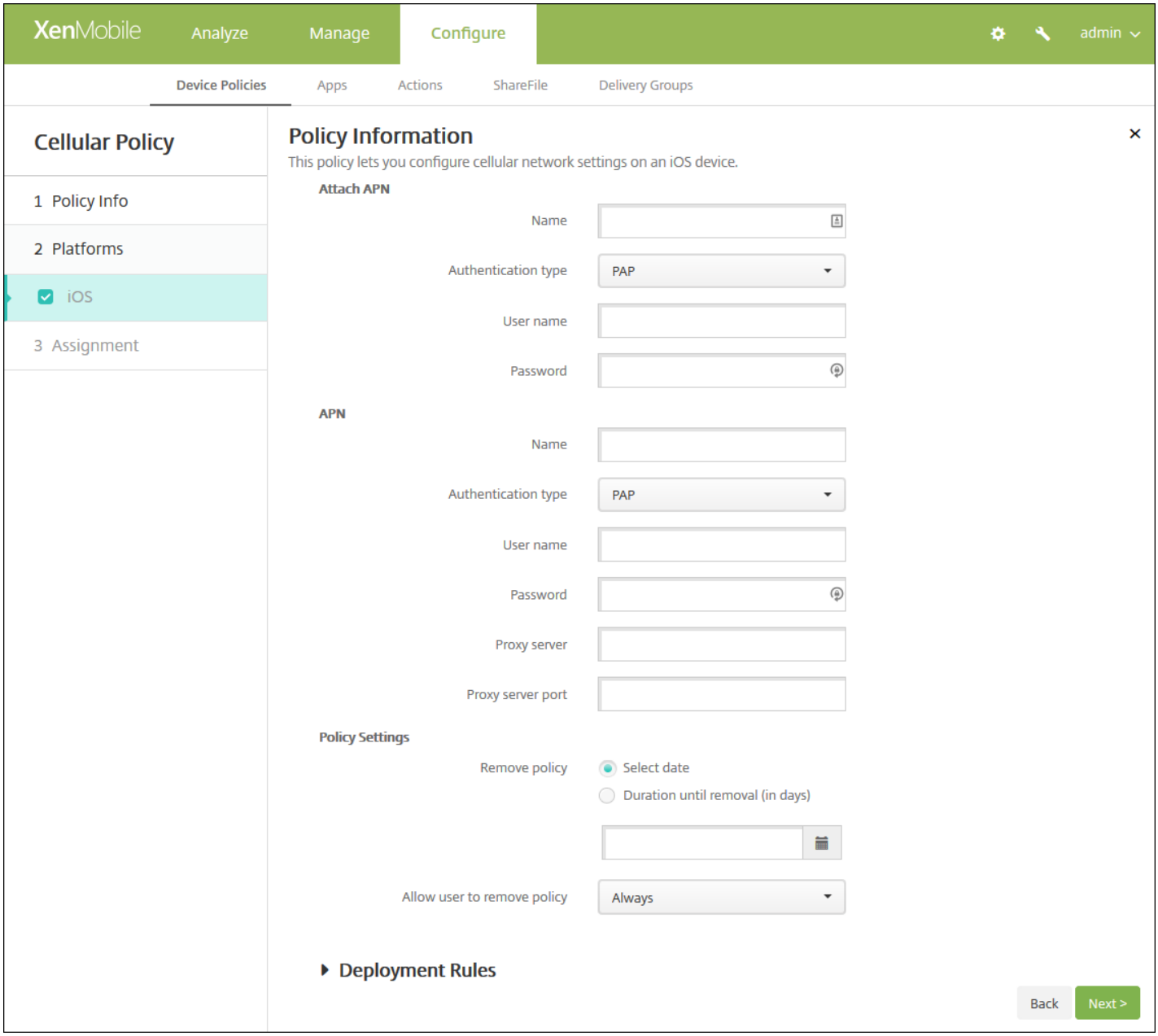


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS** 平台信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 配置以下设置：

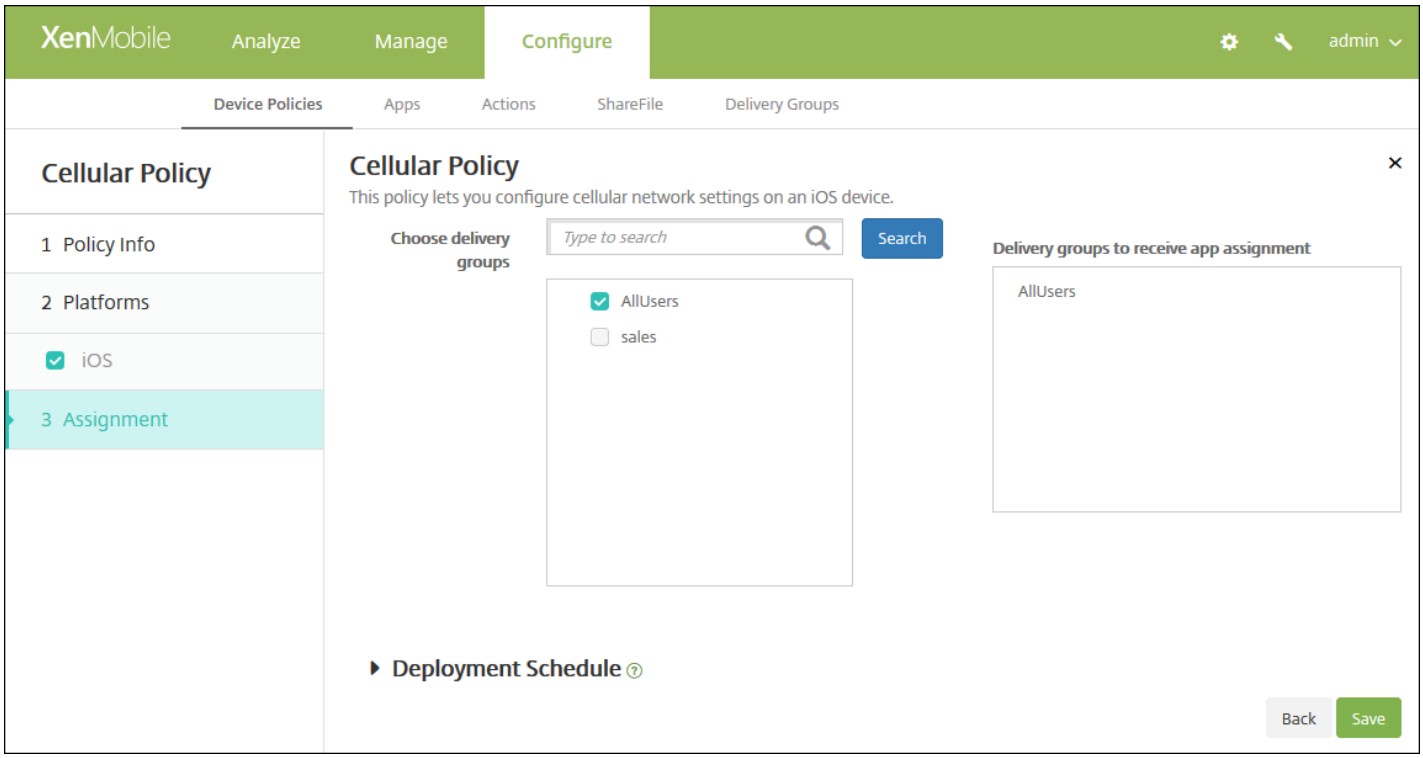
- **连接 APN**
  - **名称**：键入此配置的名称。
  - **身份验证类型**：在清单上，单击质询握手身份验证协议 (**CHAP**) 或密码身份验证协议 (**PAP**)。 默认值为 **PAP**。
  - **用户名**：键入用于身份验证的用户名。
- **APN**
  - **名称**：键入访问点名称 (APN) 配置的名称。
  - **身份验证类型**：在列表中，单击 **CHAP** 或 **PAP**。 默认值为 **PAP**。
  - **用户名**：键入用于身份验证的用户名。
  - **密码**：键入用于身份验证的密码。
  - **代理服务器**：键入代理服务器网络地址。
- **策略设置**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
- 如果单击**选择日期**，请单击日历以选择具体删除日期。
- 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
- 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**手机网络策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

连接管理器设备策略

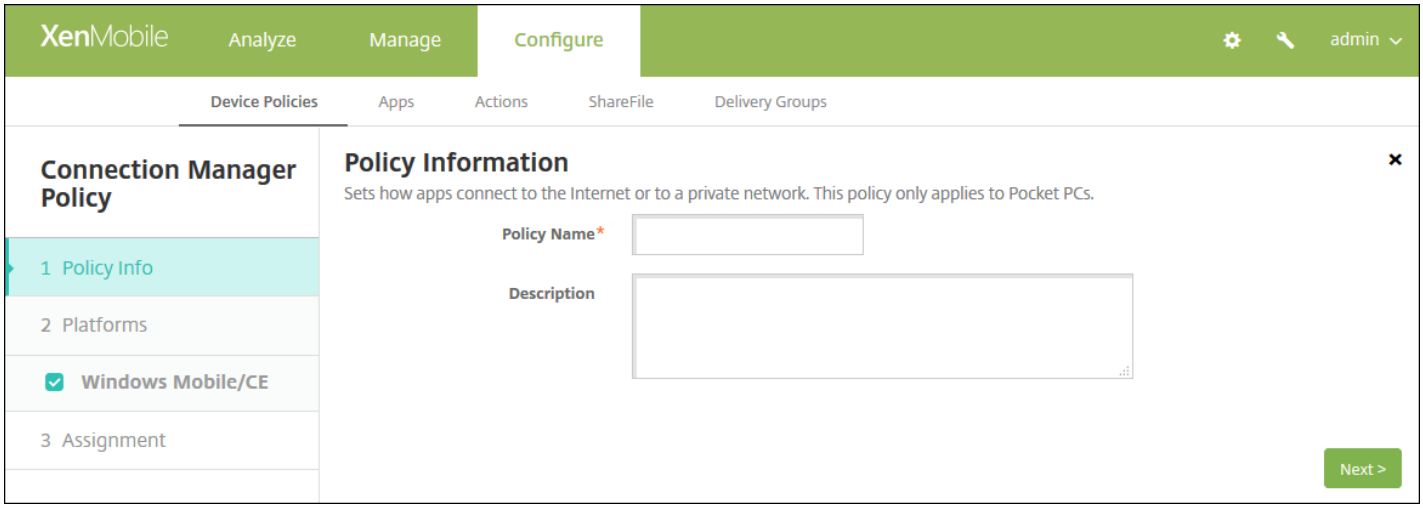
Aug 11, 2016

在 XenMobile 中，可以为自动连接到 Internet 的应用程序指定连接设置并提供网络。 此策略仅适用于 Windows Pocket PC。

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。

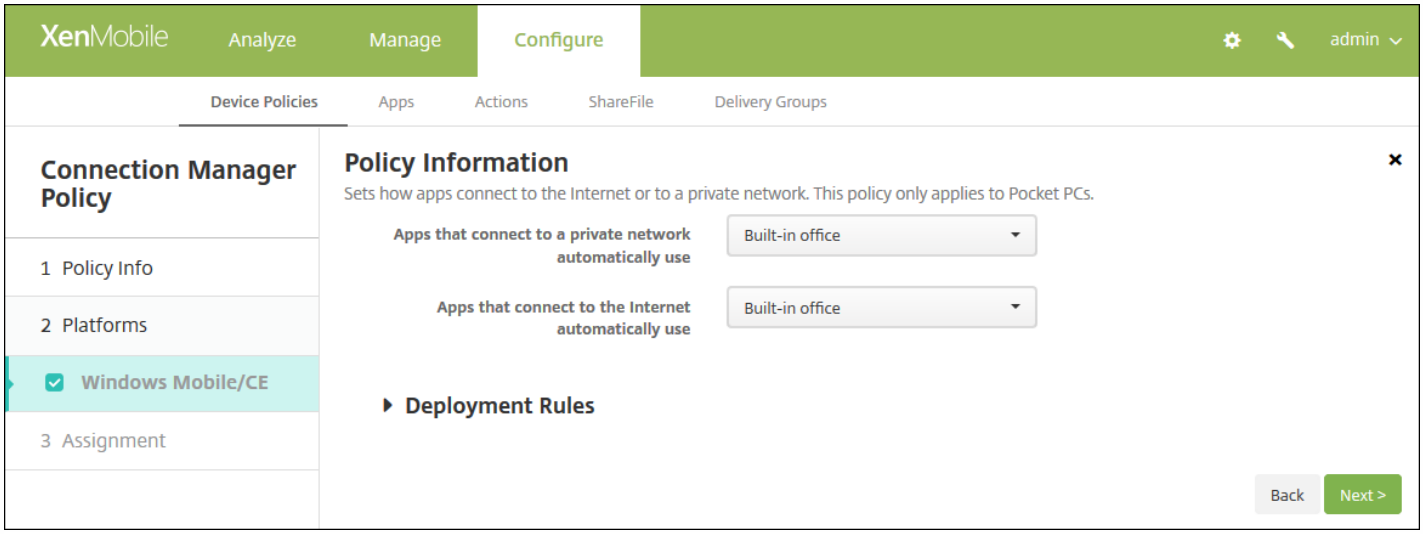
3. 单击**更多**，然后在**网络访问权限**下面，单击**连接管理器**。 将显示**连接管理器**策略信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Windows Mobile/CE 平台**页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

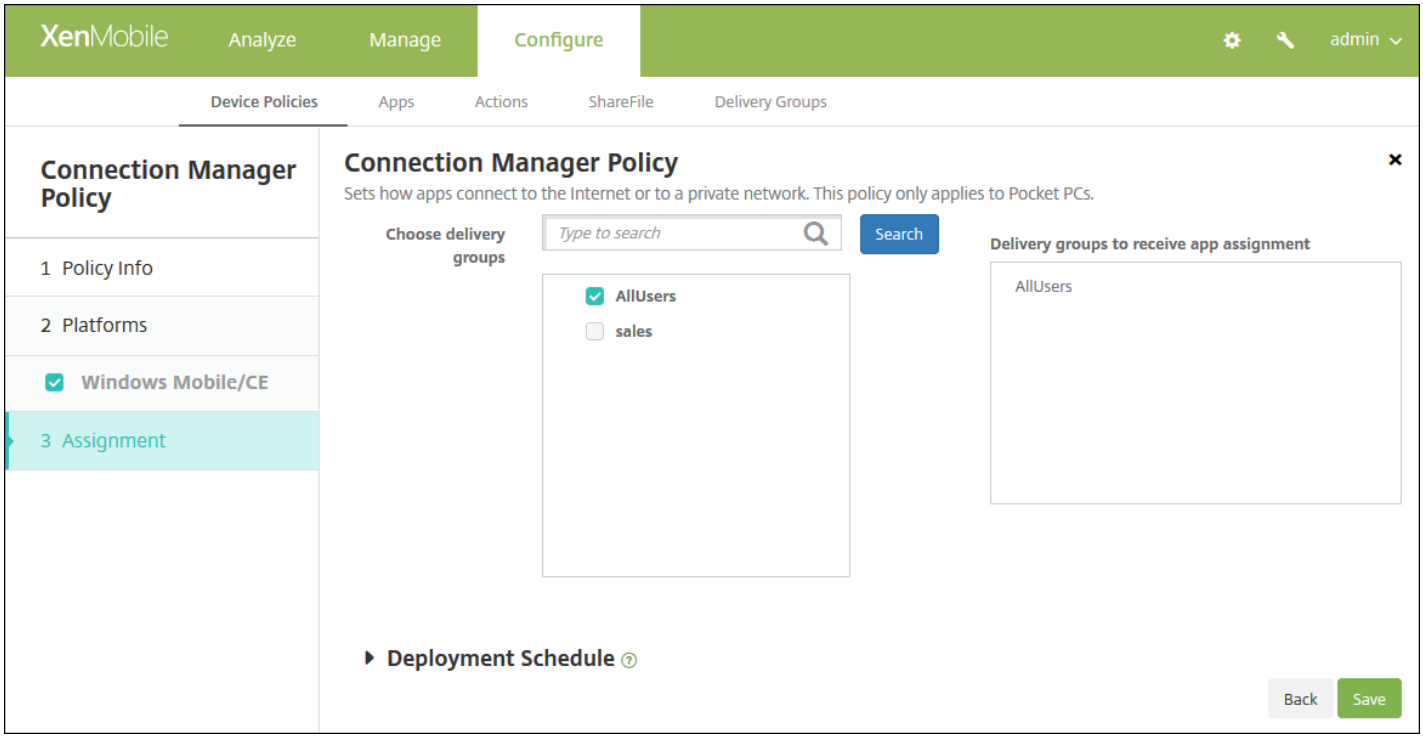
6. 配置以下设置。

注意：**内置办公网络**表示所有连接均指向公司的 Intranet，**内置 Internet** 表示所有连接均指向 Internet。

- **自动连接到专用网络的应用程序使用**：在列表中，单击**内置办公网络**或**内置 Internet**。 默认值为**内置办公网络**。
- **自动连接到 Internet 的应用程序使用**：在列表中，单击**内置办公网络**或**内置 Internet**。 默认值为**内置办公网络**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**连接管理器**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

连接计划设备策略

Aug 11, 2016

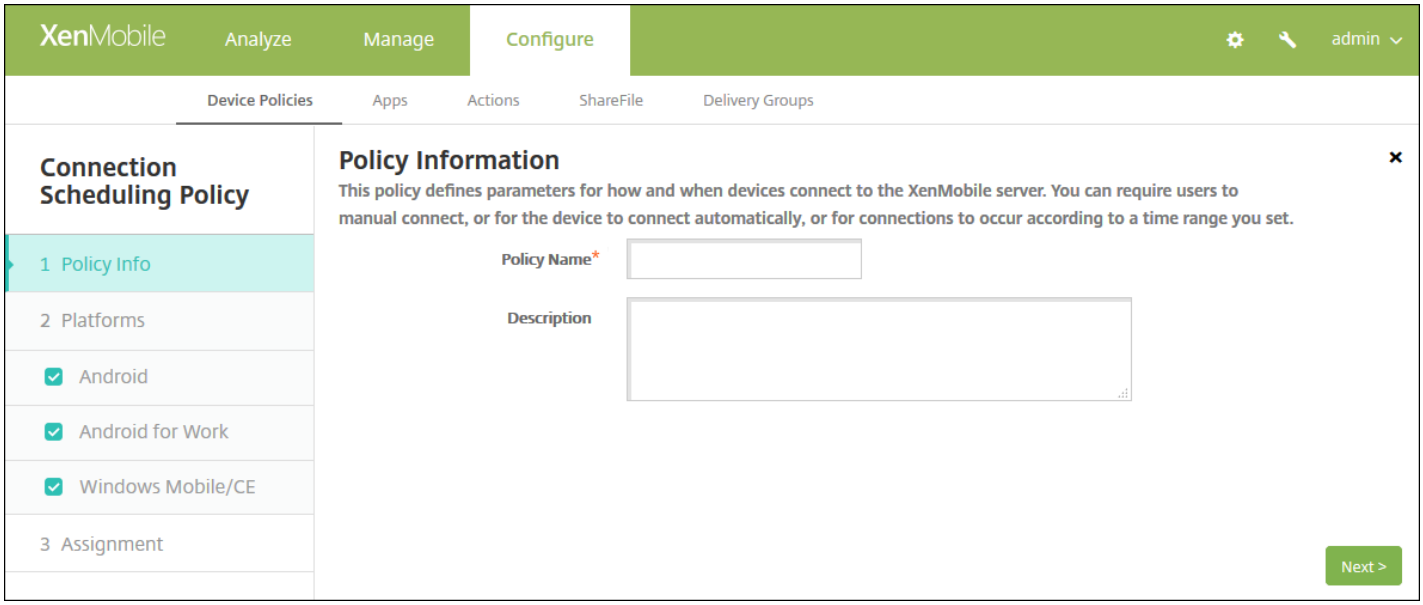
可以创建连接计划策略，用于控制用户的设备连接到 XenMobile 的方式和时间。 请注意，对于为 Android for Work 启用的设备，也可以配置此策略。

可以指定用户需要手动连接其设备、设备永久保持连接状态或设备在定义的时间范围内进行连接。

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. 单击**计划**。 此时将显示 **Connection Scheduling Policy**（连接计划策略）信息页面。

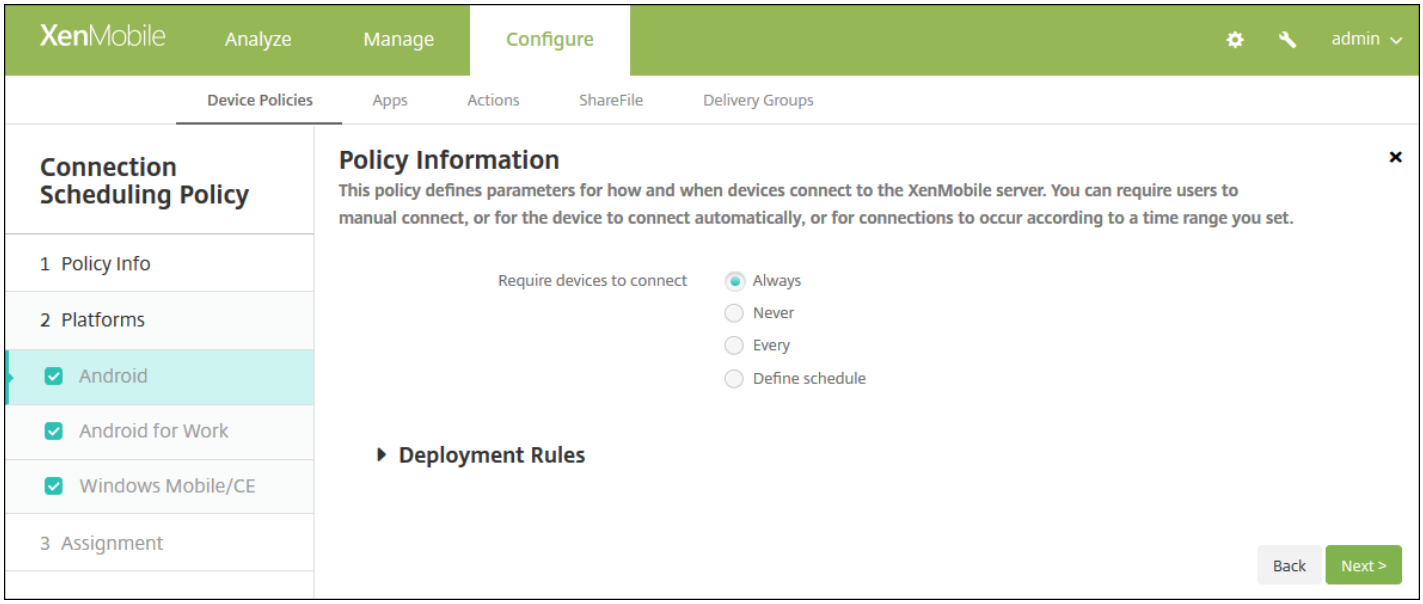


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 8 以了解如何设置此平台的部署规则。

7. 分别为选择的每个平台配置以下设置：

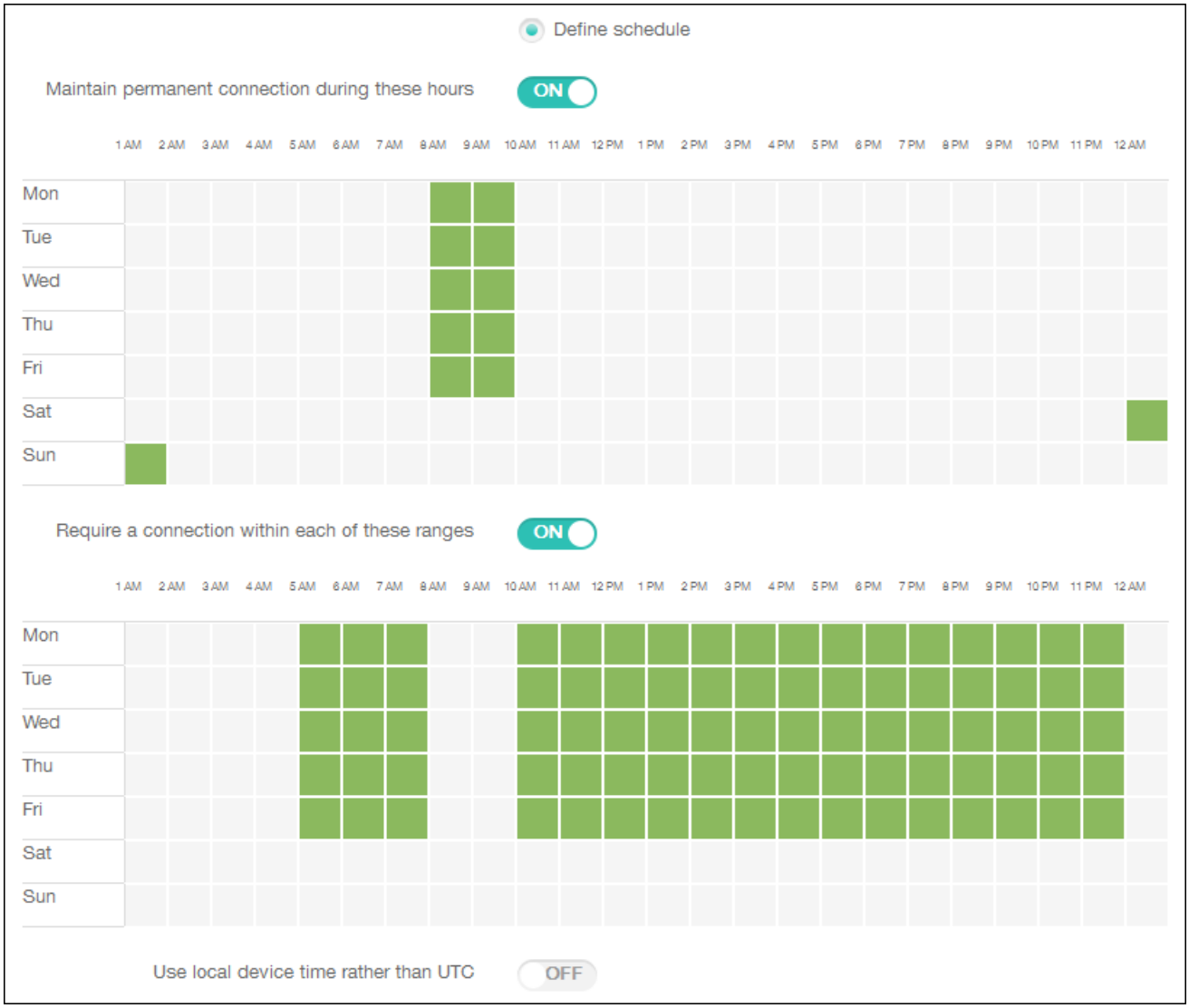
- **需要连接设备**：单击要为此计划设置的选项。
  - **总是**：连接永久保持活动状态。 在断开网络连接后，用户设备上的 XenMobile 尝试重新连接到 XenMobile 服务器，并通过以固定间隔传输控制数据包监视连接。 Citrix 建议使用此选项以优化安全性。 选择**总是**时（还适用于设备**通道策略**），**定义连接超时**设置可确保连接不会耗尽电池电量。 通过保持连接处于活动状态，您可以根据需要将擦除或锁定等安全命令推送到设备。 还必须在部署到设备的每个策略中选择**部署计划**选项**为始终启用的连接部署**。
  - **从不**：手动进行连接。 用户必须从其设备上的 XenMobile 启动连接。 Citrix 建议不要对生产部署使用此选项，因为这会阻止您将安全策略部署到设备，因此，用户从不会收到任何新应用程序或策略。
  - **每**：按照指定间隔进行连接。 如果此选项生效，则当您发送锁定或擦除等安全策略时，XenMobile 将在下次设备连接时在设备上处理该操作。 选择此选项后，将显示**每隔 N 分钟连接一次**字段，您必须在此处输入分钟数，在经过此分钟数之后，设备必须重新连接。 默认值为 **20**。
  - **定义计划**：如果启用，在丢失网络连接后，用户设备上的 XenMobile 尝试重新连接到 XenMobile 服务器，并在您定义的时间范围内通过以固定间隔传输控制数据包监视连接。 有关如何定义连接时间范围的信息，请参阅定义连接的时间范围。
    - **在此时段内保持永久连接**：在定义的时间范围内，用户设备必须连接。
    - **要求每个范围内存在一个连接**：在定义的任一时间范围内用户必须连接一次。
    - **使用本地设备时间而非 UTC**：将定义的时间范围与本地设备时间而非世界协调时间 (UTC) 同步。

定义连接的时间范围

启用下列选项时，将显示一个时间表，您可以利用此时间表设置所需的时间范围。 您可以启用其中一个选项，也可以同时启用两个选项，以满足在指定时间需要永久连接或在特点时限内需要连接的需求。 时间表中的每个方格代表 30 分钟，因此，如果您希望在每个工作日的上午 8:00 到上午 9:00 之间连接，应单击时间表上每个工作日的上午 8:00 到上午 9:00 之间的两个方格。

例如，下图中的两个时间表需要在每个工作日的上午 08:00 到上午 09:00 之间进行永久连接，在周六上午 12:00 到周日上午 1:00 之间进行永久连接，在每个工作日的上午 5:00 到上午 8:00 或上午 10:00 到下午 11:00 点之间至少有一个连接。

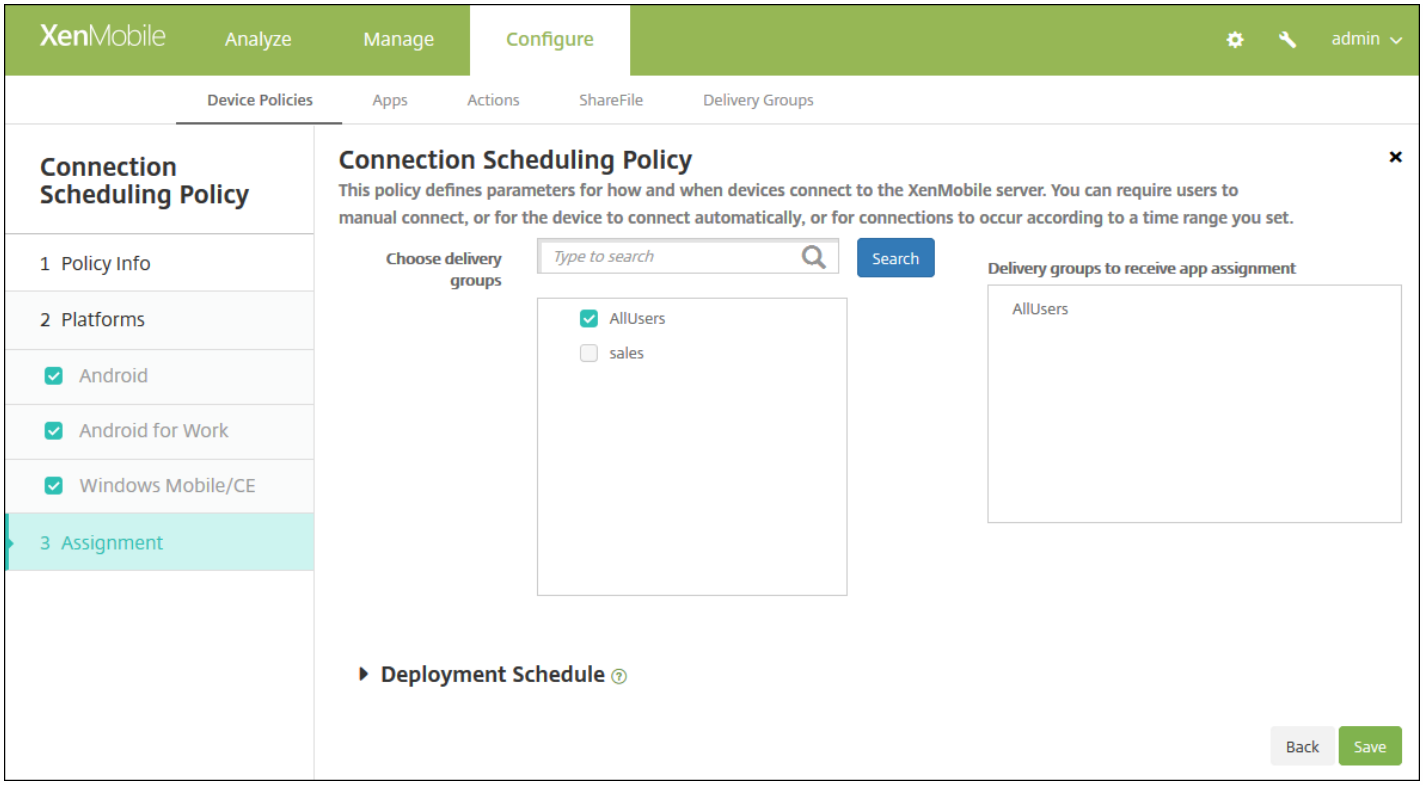
© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. 配置部署规则

9. 单击**下一步**。 此时将显示**连接计划策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



10. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

11. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

12. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

联系人 (CardDAV) 设备策略

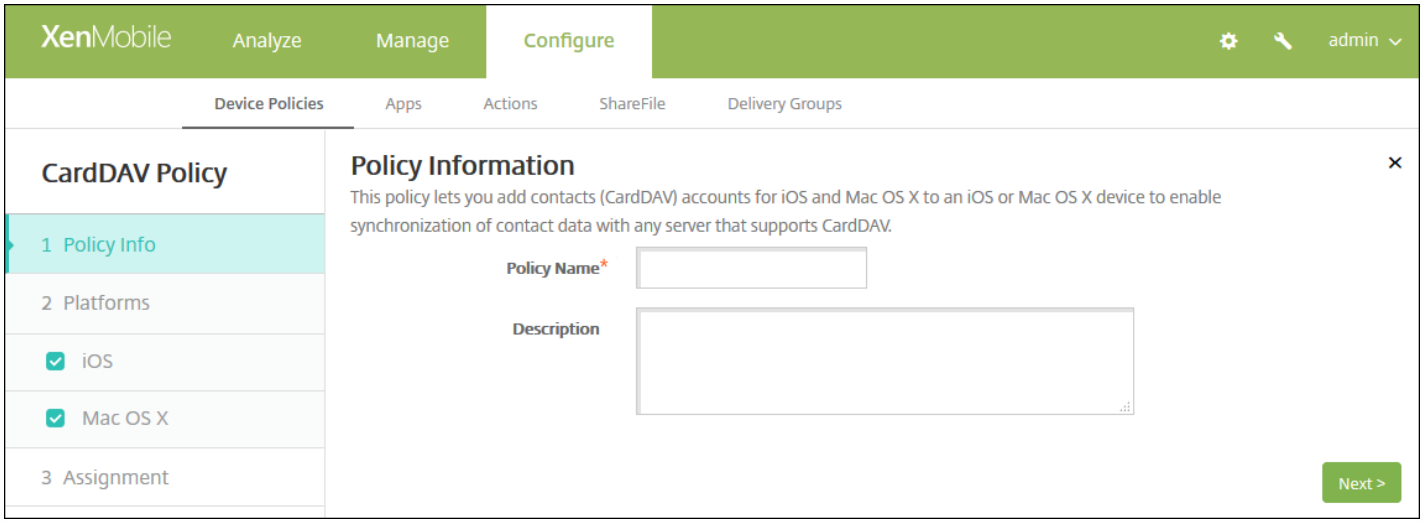
Aug 11, 2016

可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 或 Mac OS X 设备添加 iOS 联系人 (CardDAV) 帐户，使用户可以将其联系人数据与任何支持 CardDAV 的服务器同步。

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**下面，单击**联系人 CardDAV**。 此时将显示 **CardDAV Policy**（CardDAV 策略）页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

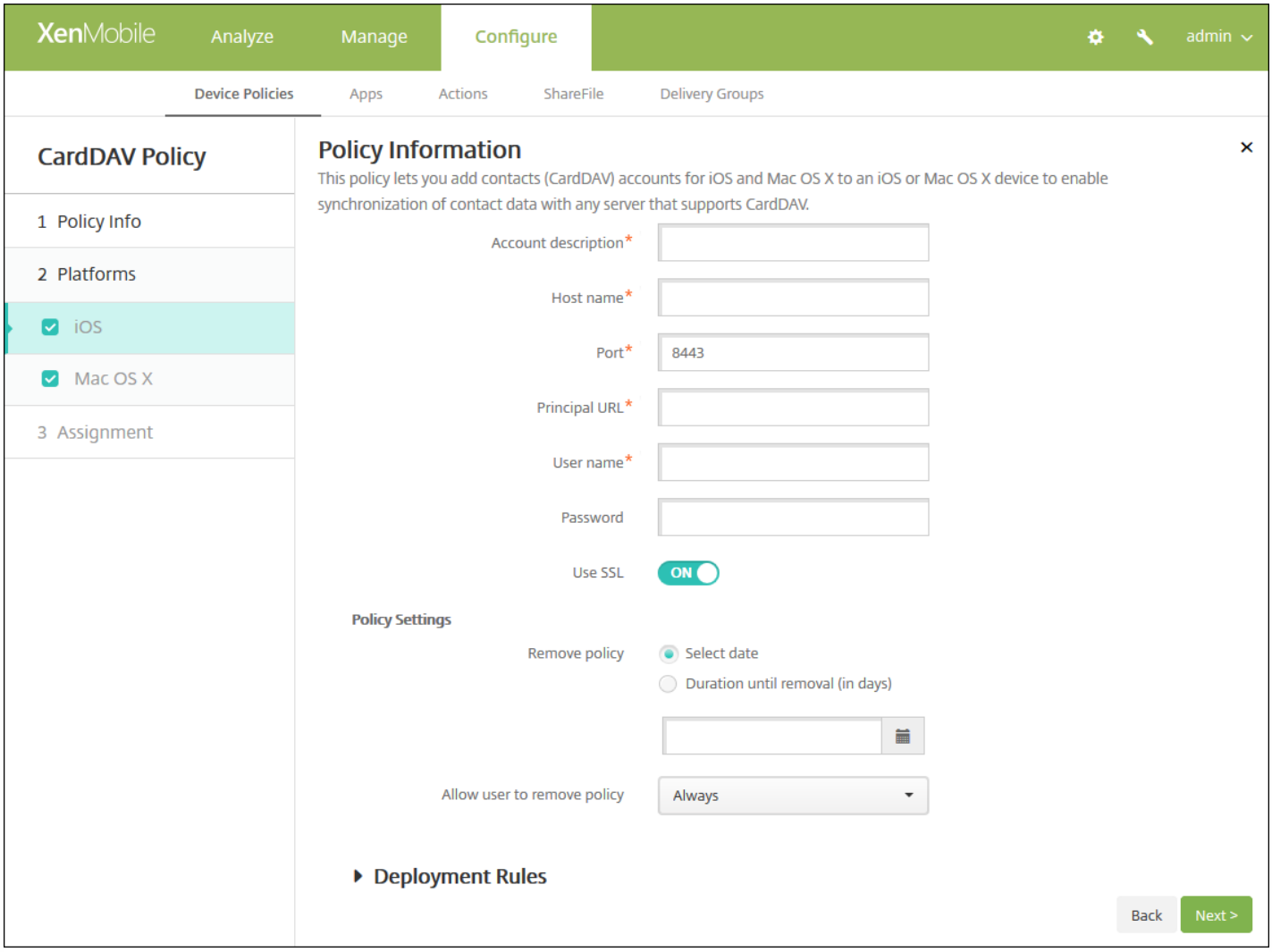
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

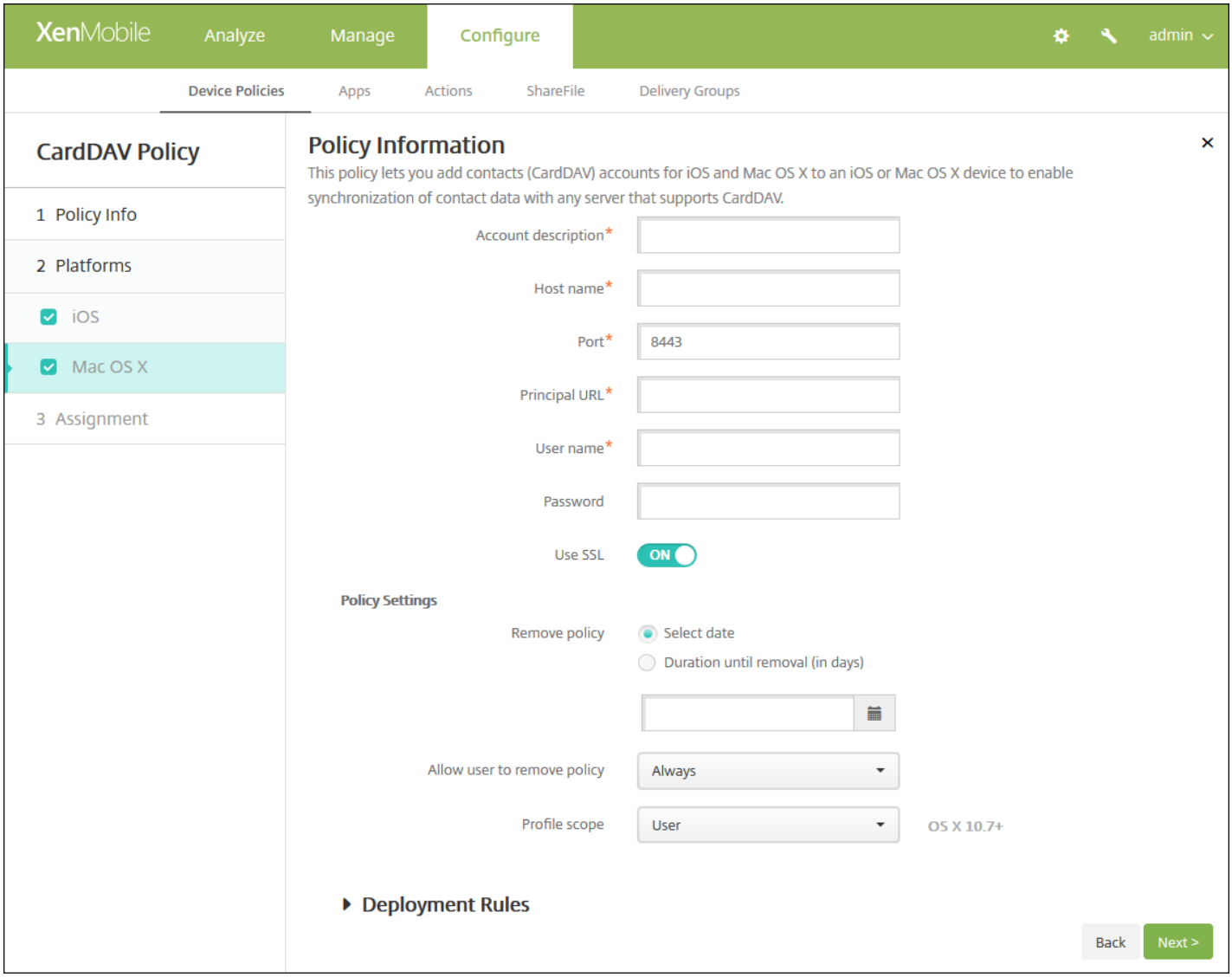


配置以下设置：

- **帐户说明**：键入帐户说明。 此字段为必填字段。
- **主机名**：键入 CardDAV 服务器的地址。 此字段为必填字段。
- **端口**：键入连接到 CardDAV 服务器使用的端口。 此字段为必填字段。 默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的登录名称。 此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。 默认值为**开**。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 Removal password（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



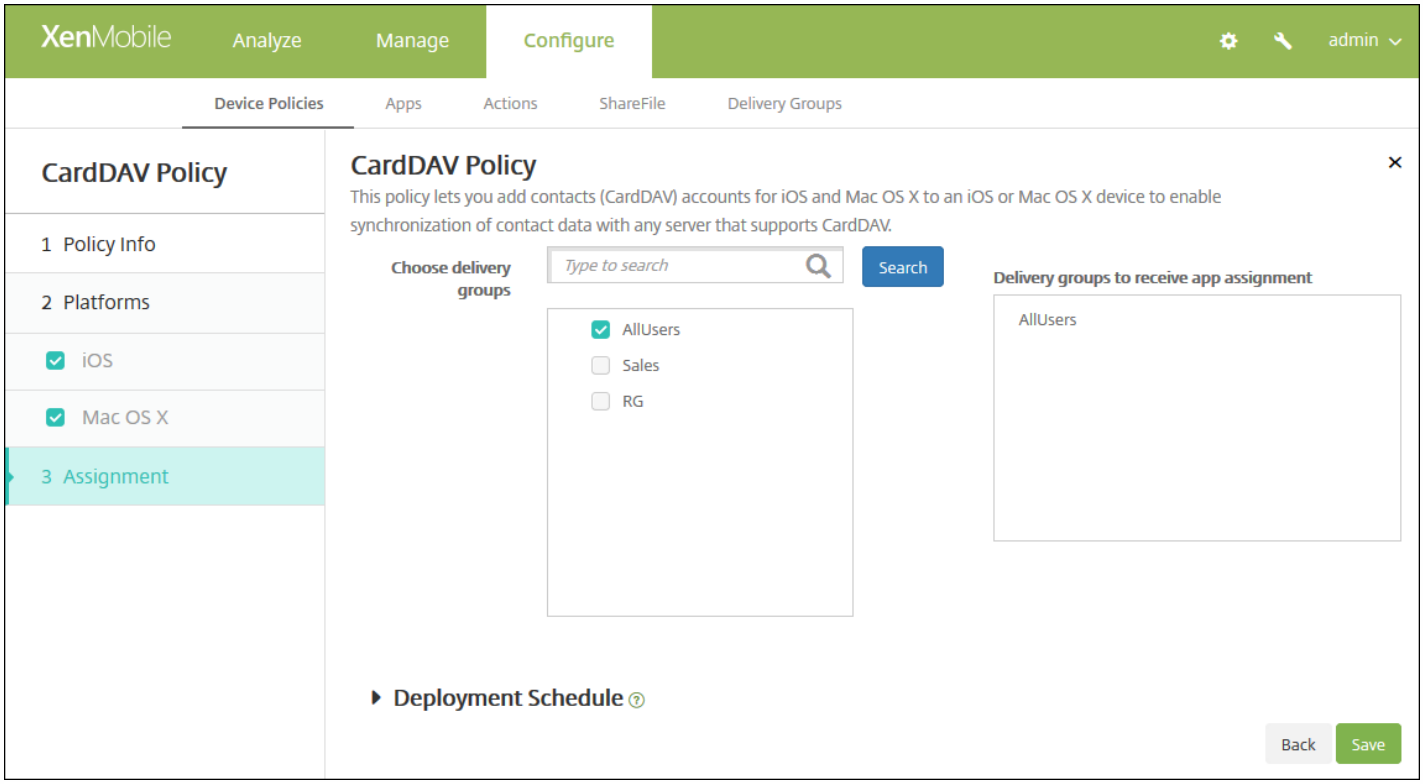
配置以下设置：

- **帐户说明**：键入帐户说明。 此字段为必填字段。
- **主机名**：键入 CardDAV 服务器的地址。 此字段为必填字段。
- **端口**：键入连接到 CardDAV 服务器使用的端口。 此字段为必填字段。 默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的登录名称。 此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。 默认值为**开**。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在“Removal password”（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 单击**下一步**。 此时将显示 **CardDAV 策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

将应用程序复制到 Samsung 容器设备策略

Aug 11, 2016

您可以指定将设备上已经安装的应用程序复制到受支持 Samsung 设备上的 SEAMS 容器或 KNOX 容器（有关受支持设备的信息，请参阅 Samsung 的 Samsung KNOX Supported Devices（Samsung KNOX 支持的设备）页面）。 复制到 SEAMS 容器的应用程序在用户的主屏幕上可用；复制到 KNOX 容器的应用程序仅当用户登录 KNOX 容器。

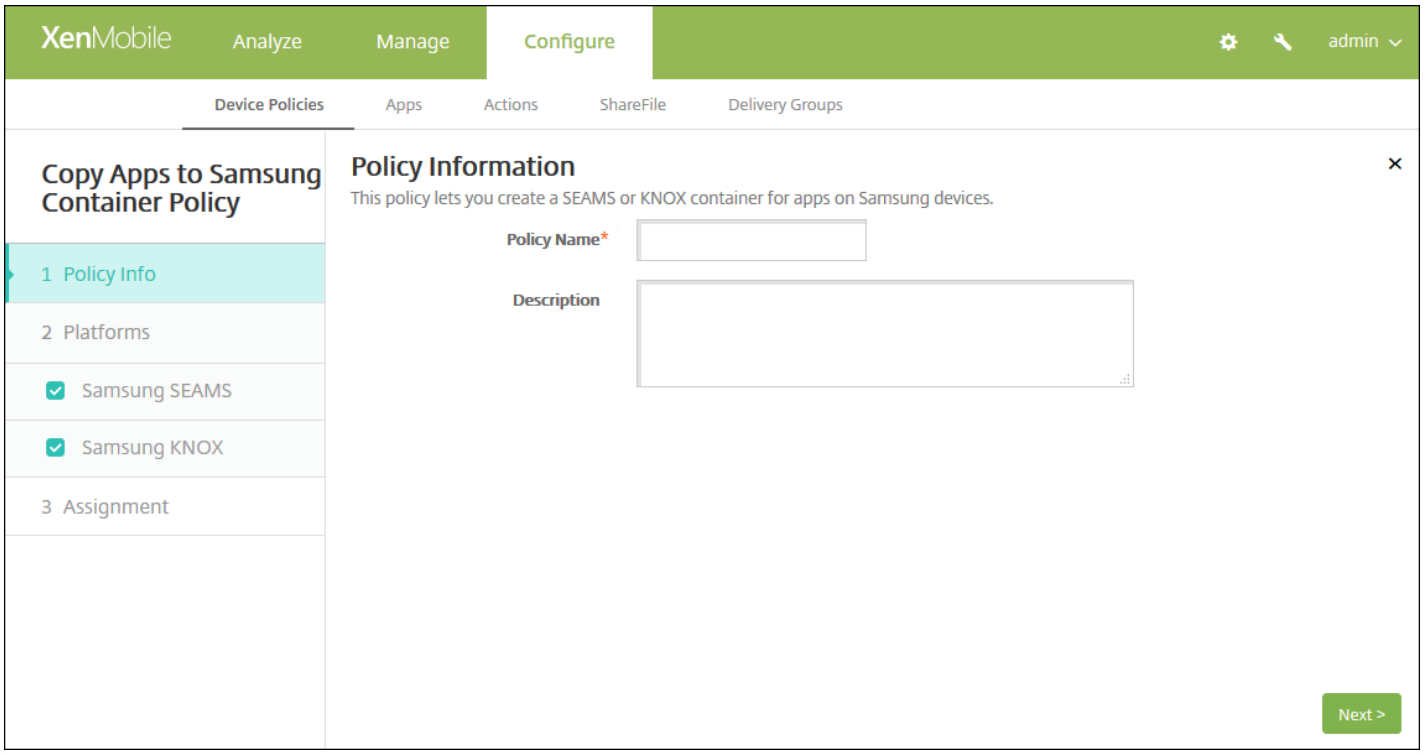
必备条件：

- 设备必须在 XenMobile 上注册。
- 必须部署 Samsung MDM 密钥（ELM 和 KLM）（有关操作方法，请参阅 Samsung MDM 许可证密钥设备策略）。
- 应用程序已经安装到设备上
- 在设备上初始化 KNOX 以将应用程序复制到 KNOX 容器。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。

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**下面，单击**将应用程序复制到 Samsung 容器**。 此时将显示**将应用程序复制到 Samsung 容器策略**信息页面。

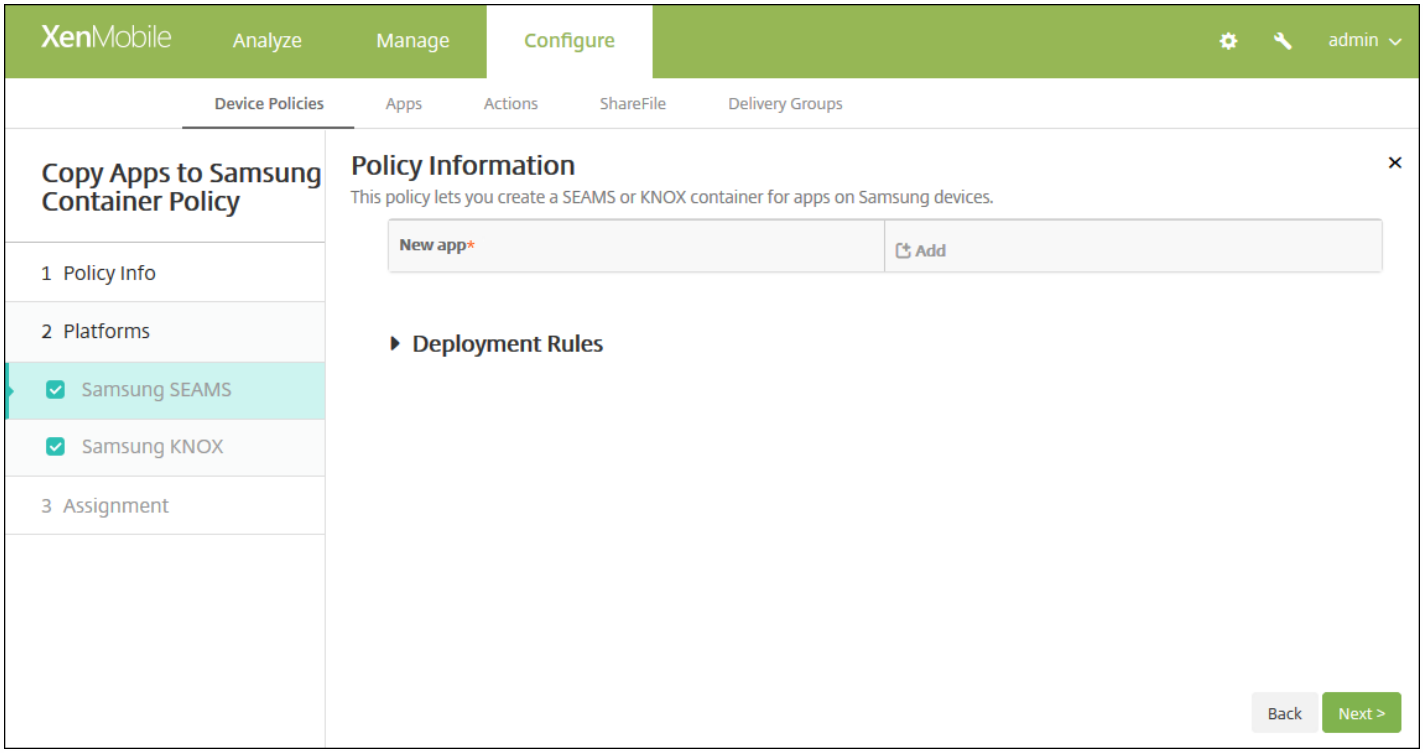


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 在平台下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 8 以了解如何设置此平台的部署规则。

7. 分别为选择的每个平台配置以下设置。

- **新建应用程序**：对于要添加到此列表中的每个应用程序，请单击**添加**，然后执行以下操作：
  - 键入包 ID，例如，对于 LacingArt 应用程序，请键入 com.mobiwolf.lacingart。
  - 单击**保存**或**取消**。

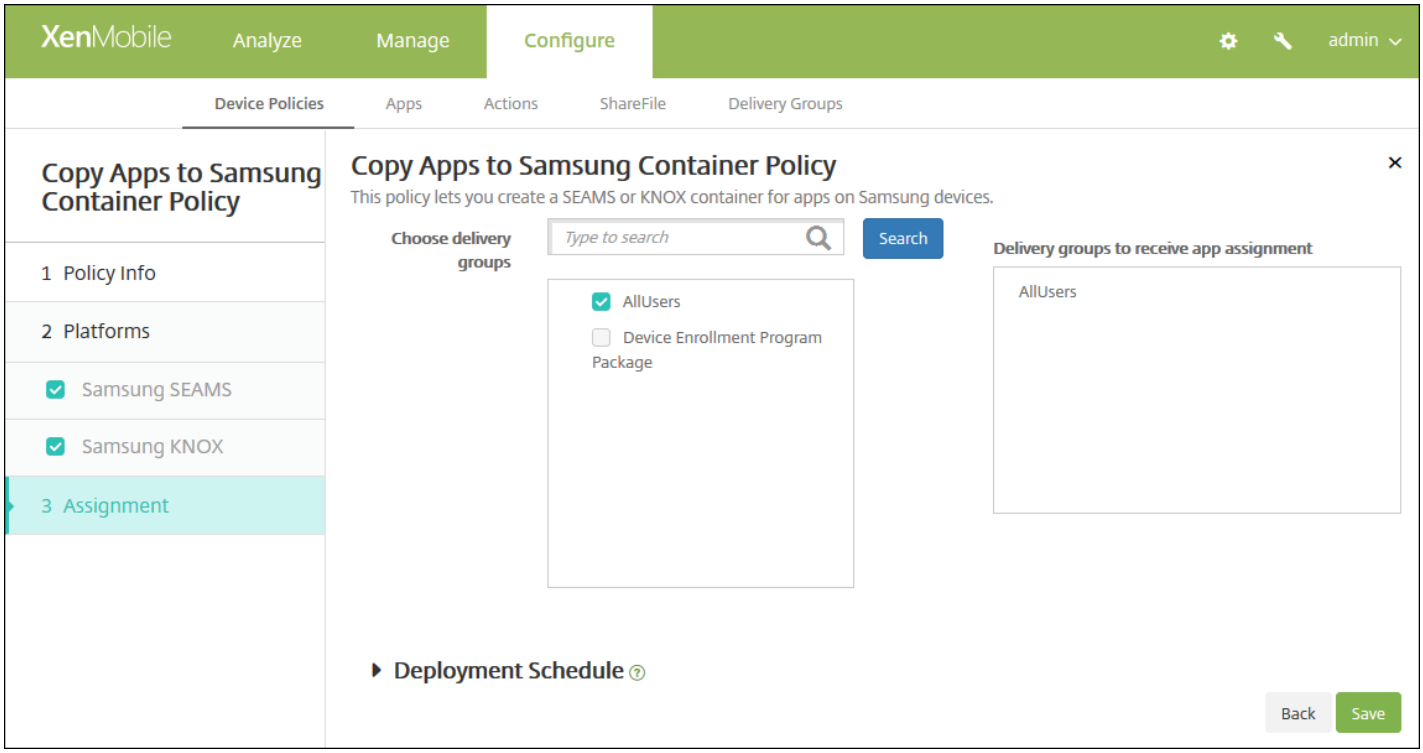
    注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

8. 配置部署规则

8. 单击**下一步**。 此时将显示下一个平台页面或**将应用程序复制到 Samsung 容器策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，“为始终启用的连接部署”除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

成功部署策略后，SEAMS 应用程序显示在**设备详细信息**页面上标题**位置: 企业 SEAMS 位置**下面，KNOX 应用程序显示在标题**位置: 企业位置**下面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

凭据设备策略

Aug 11, 2016

可以在 XenMobile 中创建凭据设备策略，以使用 XenMobile 中的 PKI 配置启用集成身份验证，例如 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。

可以为 iOS、Mac OS X、Android、Android for Work、Windows Desktop/Tablet、Windows Mobile/CE 和 Windows Phone 设备创建凭据策略。 每种平台需要一组不同的值，本文将对此进行介绍。

iOS 设置

Mac OS X 设置

Android 和 Android for Work 设置

Windows Desktop/Tablet 设置

Windows Mobile/CE 设置

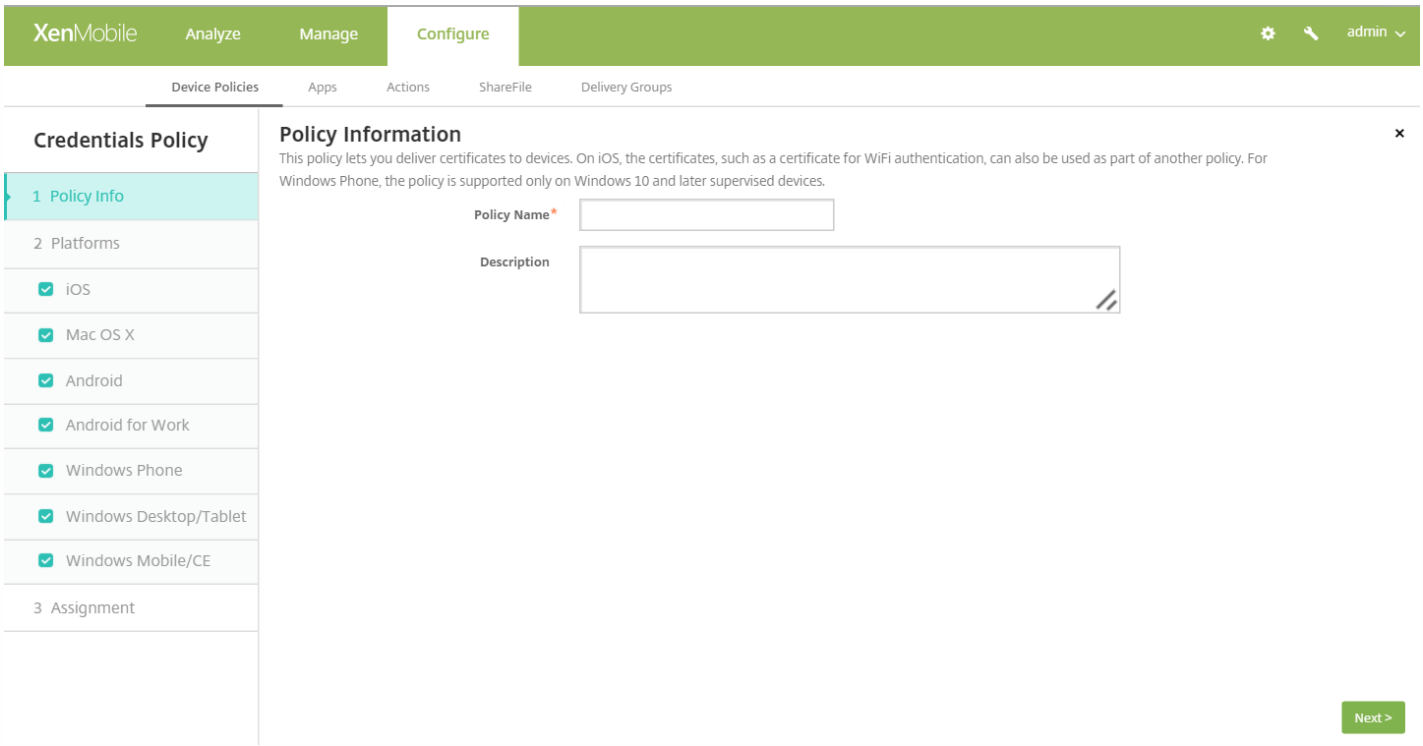
Windows Phone 设置

创建此策略前，需要具有计划用于各平台的凭据信息，以及任何证书和密码。

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**下面，单击**凭据**。 此时将显示**凭据策略**信息页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. 在**策略信息**窗格中，键入以下信息：

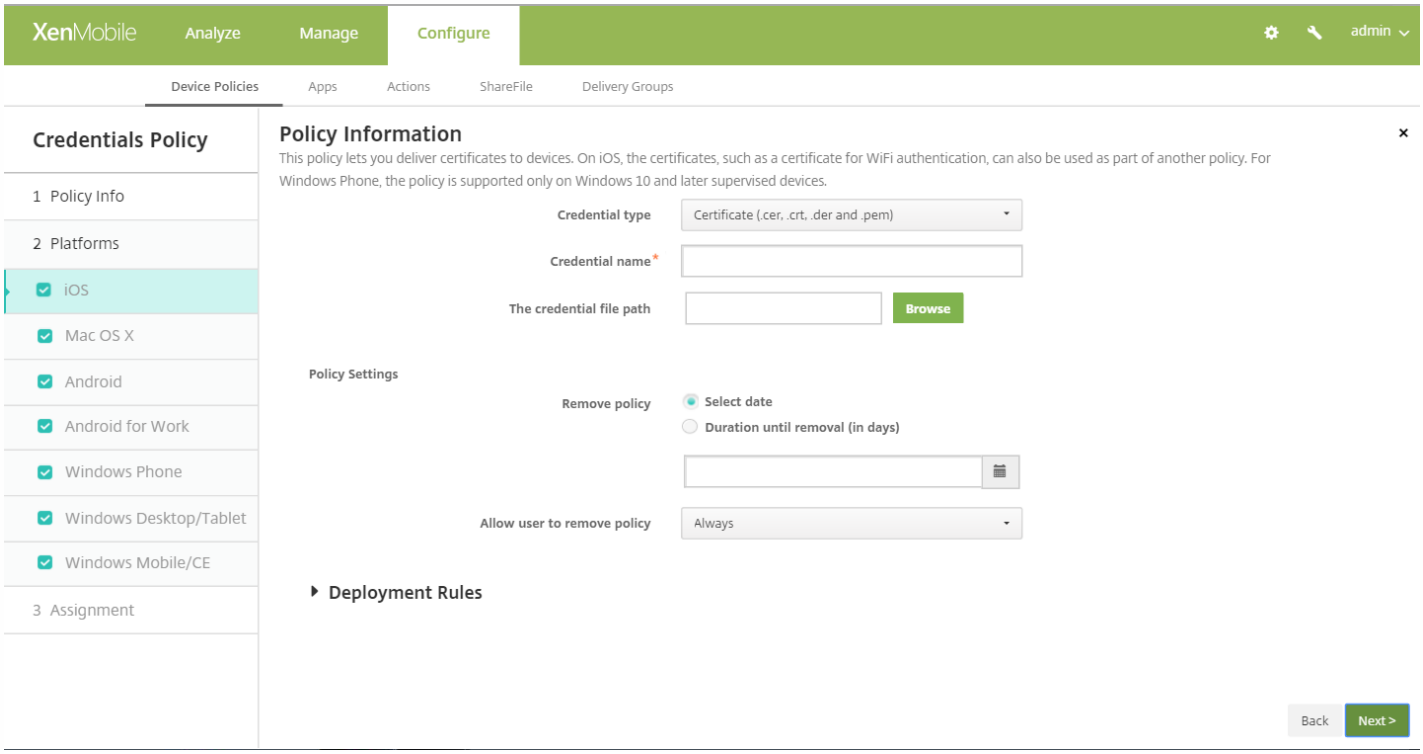
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置



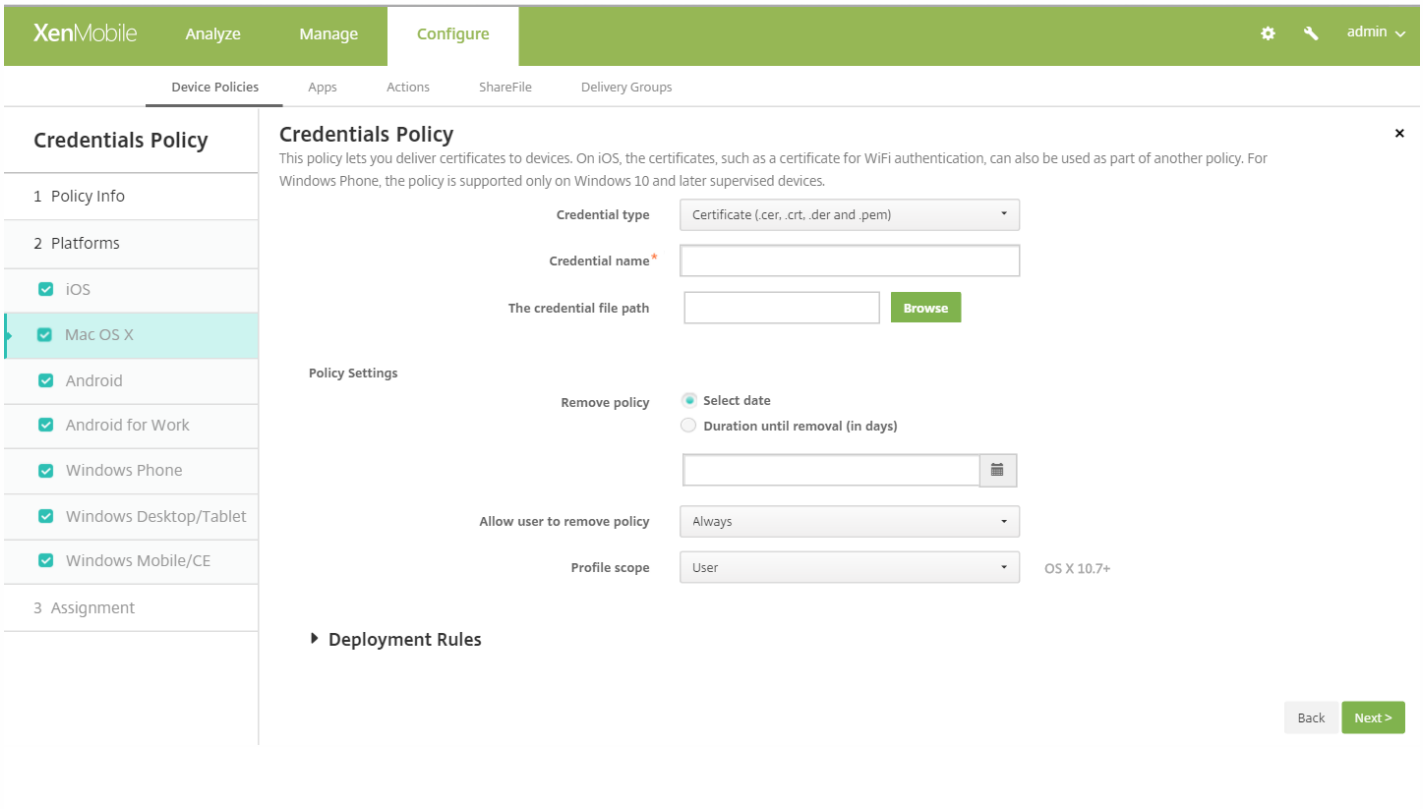
配置以下设置：

- **凭据类型**：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - **证书**
    - **凭据名称**：输入凭据的唯一名称。
    - **凭据文件路径**：单击浏览，导航到凭据文件的位置，以选择此凭据文件。
  - **密钥库**
    - **凭据名称**：输入凭据的唯一名称。
    - **凭据文件路径**：单击浏览，导航到凭据文件的位置，以选择此凭据文件。
    - **密码**：输入凭据的密钥库密码。
  - **服务器证书**
    - **服务器证书**：在列表中，单击要使用的证书。
  - **凭据提供程序**
    - **凭据提供程序**：在列表中，单击凭据提供程序的名称。
- **策略设置**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
- 如果单击**选择日期**，请单击日历以选择具体删除日期。
- 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
- 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置

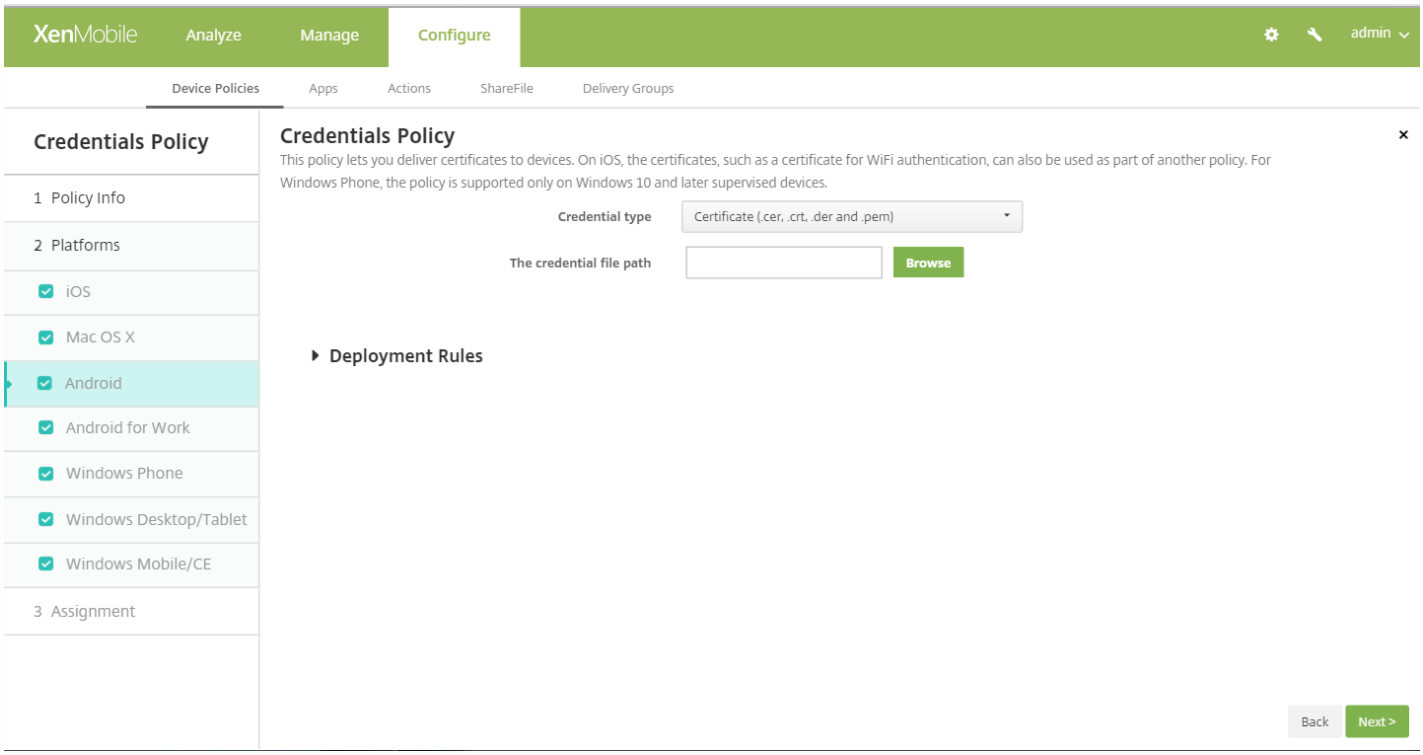


配置以下设置：

- **凭据类型**：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - **证书**
    - **凭据名称**：输入凭据的唯一名称。
    - **凭据文件路径**：单击浏览，导航到凭据文件的位置，以选择此凭据文件。
  - **密钥库**
    - **凭据名称**：输入凭据的唯一名称。
    - **凭据文件路径**：单击浏览，导航到凭据文件的位置，以选择此凭据文件。
    - **密码**：输入凭据的密钥库密码。
  - **服务器证书**
    - **服务器证书**：在列表中，单击要使用的证书。
  - **凭据提供程序**
    - **凭据提供程序**：在列表中，单击凭据提供程序的名称。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在 **Policy scope**（策略范围）旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置 Android 和 Android for Work 设置

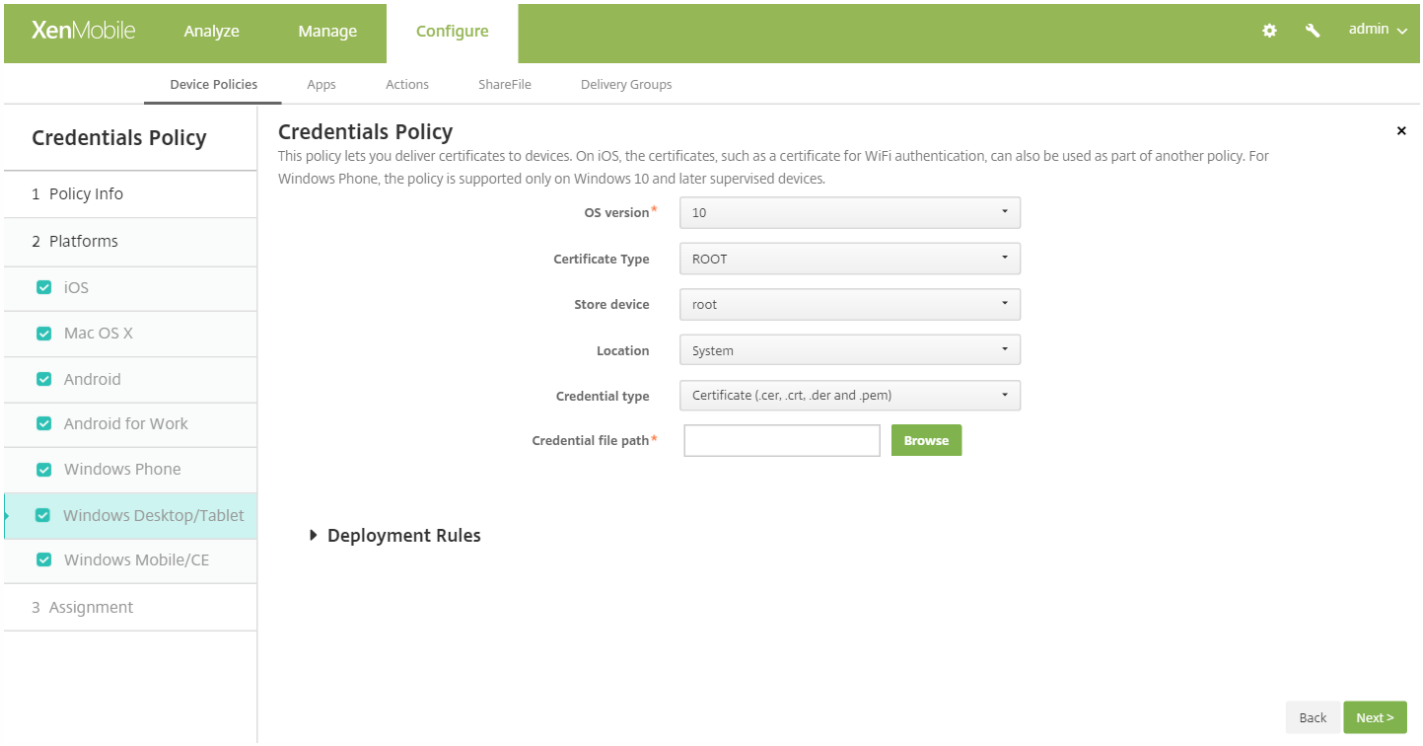


配置以下设置：

- **凭据类型**：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
  - **证书**
    - **凭据名称**：键入凭据的唯一名称。
    - **凭据文件路径**：单击浏览，然后导航到凭据文件的位置，以选择此凭据文件。
  - **密钥库**
    - **凭据名称**：键入凭据的唯一名称。
    - **凭据文件路径**：单击浏览，然后导航到凭据文件的位置，以选择此凭据文件。
    - **密码**：键入凭据的密钥库密码。
  - **服务器证书**
    - **服务器证书**：在列表中，单击要使用的证书。
  - **凭据提供程序**
    - **凭据提供程序**：在列表中，单击凭据提供程序的名称。

配置 Windows Desktop/Tablet 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

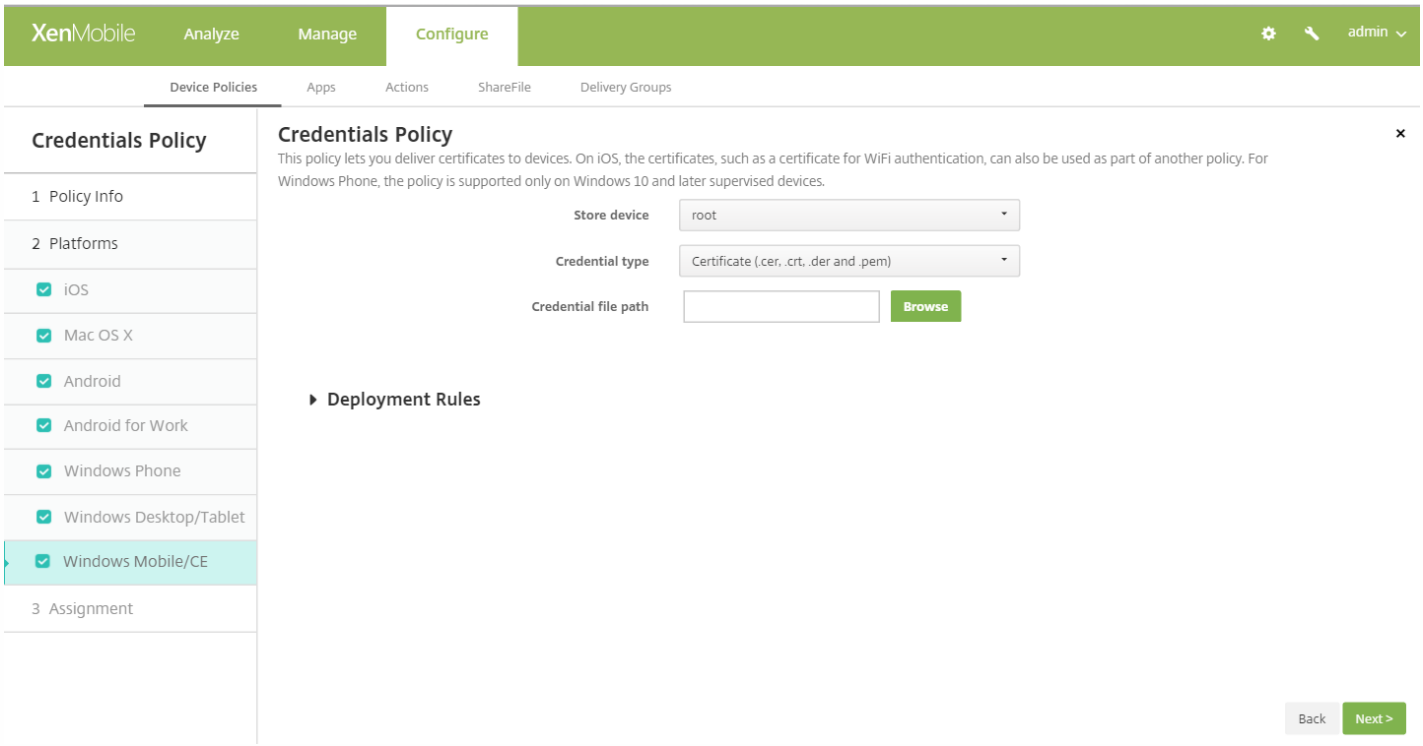
- **操作系统版本**：在列表中，单击 **8.1** 以使用 Windows 8.1 或单击 **10** 以使用 Windows 10。 默认值为 **10**。

Windows 10 设置

Windows 8.1 设置

配置 Windows Mobile/CE 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

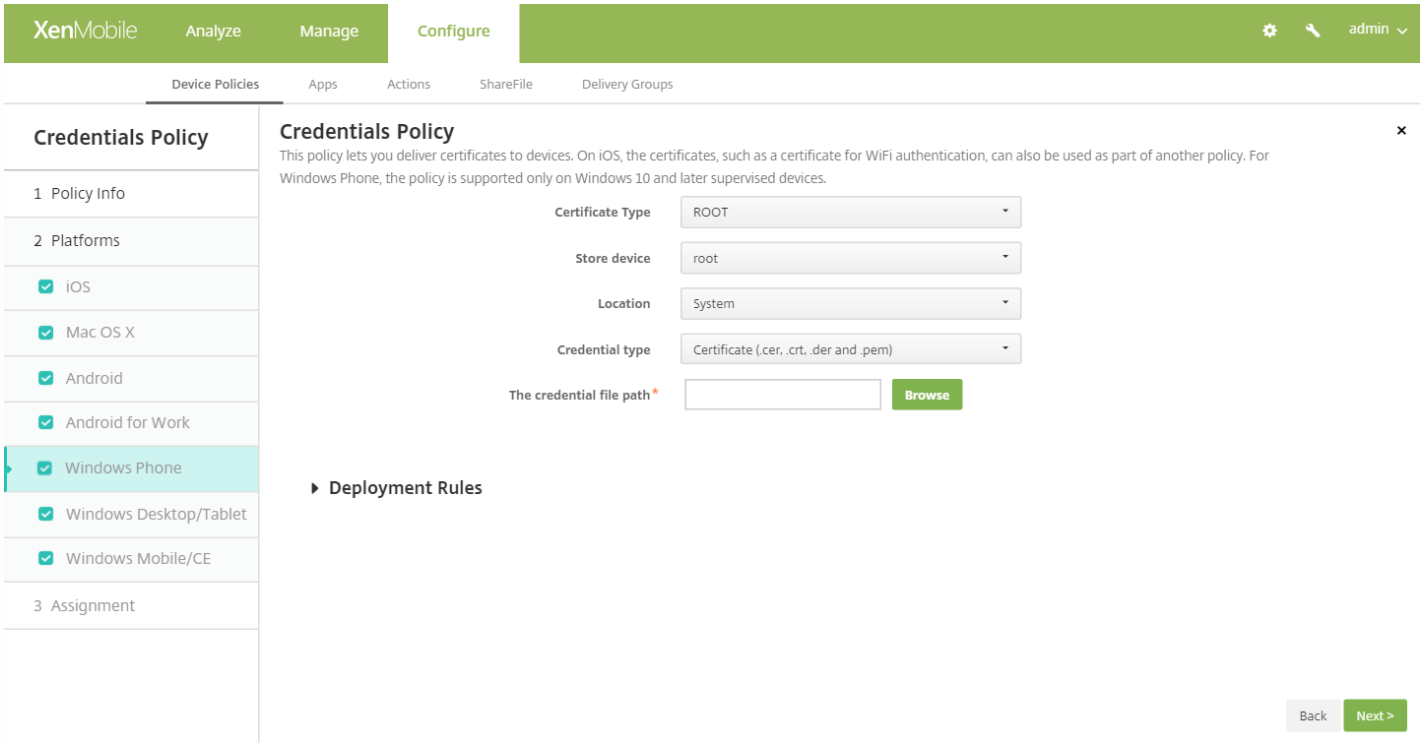


配置以下设置：

- **存储设备**：在列表中，单击凭据的证书存储位置。 默认为**根存储**。 选项包括：
  - **特许执行信任颁发机构** - 使用属于此存储的证书签名的应用程序将在特许信任级别下运行。
  - **非特许执行信任颁发机构** - 使用属于此存储的证书签名的应用程序将在一般信任级别下运行。
  - **SPC(软件发行程序证书)** - 软件发行程序证书 (SPC) 用于签名 .cab 文件。
  - **根** - 包含根证书或自签名证书的证书存储。
  - **CA** - 包含加密信息（包括中间证书颁发机构）的证书存储。
  - **我的** - 包含最终用户个人证书的证书存储。
- **凭据类型**：证书是适用于 Windows Mobile/CE 设备的唯一凭据类型。
- **凭据文件路径**：单击**浏览**，然后导航到凭据文件的位置，以选择此凭据文件。

配置 Windows Phone 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



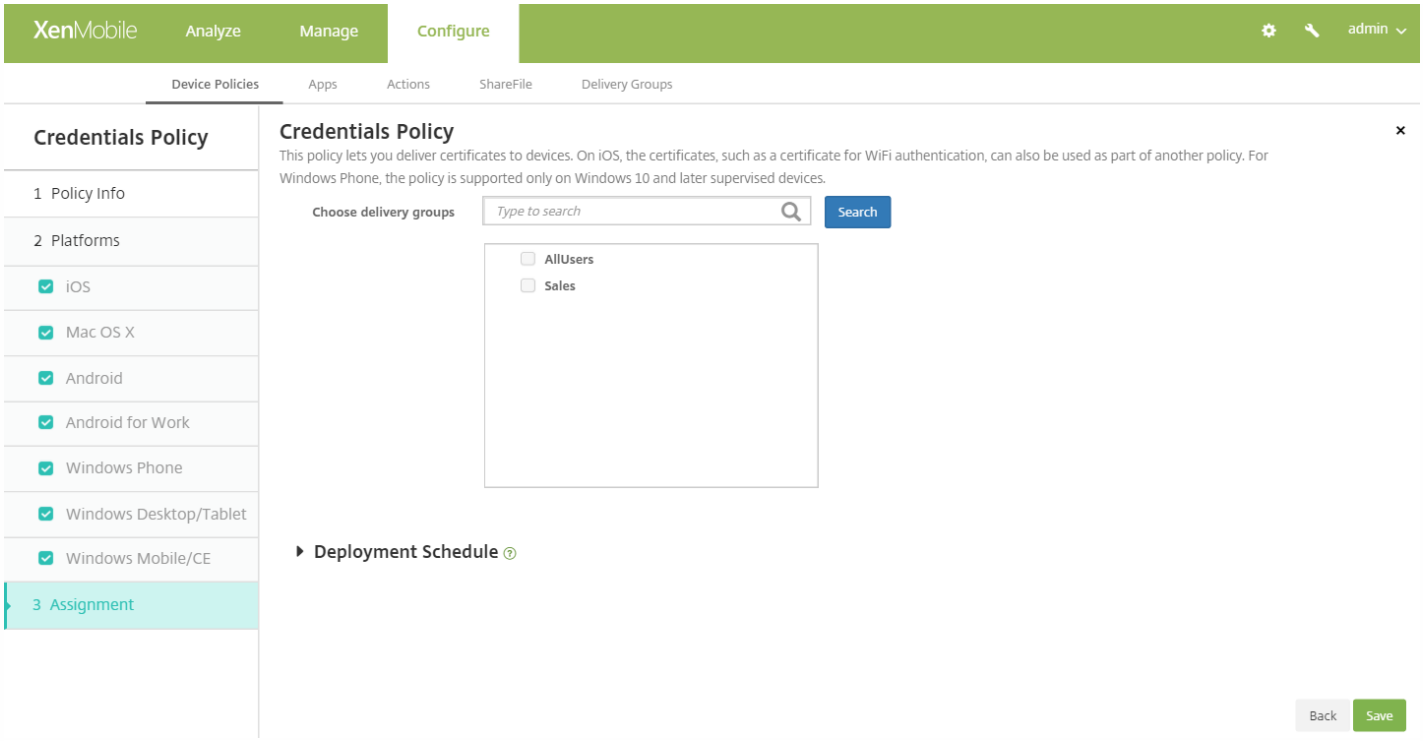
配置以下设置：

- **证书类型**：在列表中，单击“根证书”或“客户端证书”。
- 如果单击**根证书**，可以配置以下设置：
  - **存储设备**：在列表中，单击**根存储**、**我的**或 **CA** 以选择凭据的证书存储位置。 **我的**将证书存储在用户证书存储中。
  - **位置**：“系统”是适用于 Windows Phone 的唯一位置。
  - **凭据类型**：“证书”是适用于 Windows Phone 的唯一凭据类型。
  - **凭据文件路径**：单击**浏览**，导航到证书文件的位置，以选择此证书文件。
- 如果单击**客户端证书**，可以配置以下设置：
  - **位置**：**系统**是适用于 Windows Phone 的唯一位置。
  - **凭据类型**：**密钥库**是适用于 Windows Phone 的唯一凭据类型。
  - **凭据名称**：键入凭据的名称。 此字段为必填字段。
  - **凭据文件路径**：单击“浏览”，导航到证书文件的位置，以选择此证书文件。
  - **密码**：键入与凭据关联的密码。 此字段为必填字段。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**凭据策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

自定义 XML 设备策略

Aug 11, 2016

如果需要在 Windows Phone、Windows Desktop/Tablet 和 Windows Mobile/CE 设备上自定义以下功能，可以在 XenMobile 中创建自定义 XML 策略：

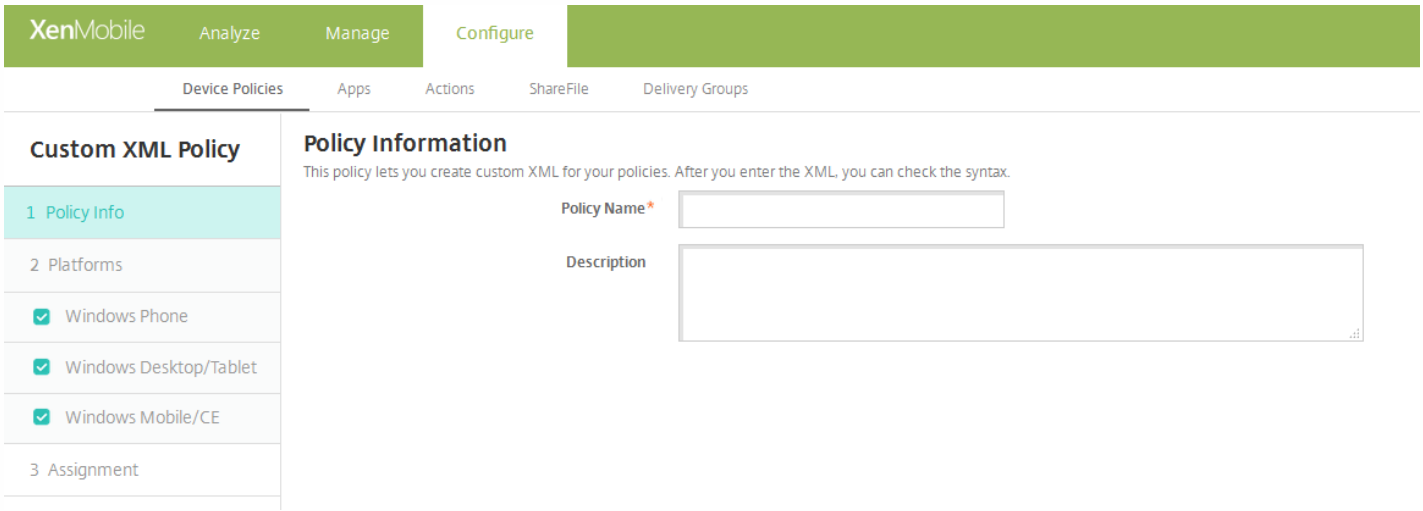
- 置备，包括配置设备以及启用或禁用功能
- 设备配置，包括允许用户更改设置和设备参数
- 软件升级，包括提供要加载到设备中的新软件或缺陷修复（包括应用程序和系统软件）
- 故障管理，包括接收来自设备的错误和状态报告

在 Windows 中使用 Open Mobile Alliance Device Management (OMA DM) API 创建自己的自定义 XML 配置。 本主题中不介绍如何使用 OMA DM API 创建自定义 XML。 有关使用 OMA DM API 的详细信息，请参阅 Microsoft Developer Network 站点上的 OMA 设备管理。

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**自定义**下面，单击**自定义 XML**。 此时将显示 **Custom XML Policy**（自定义 XML 策略）信息页面。

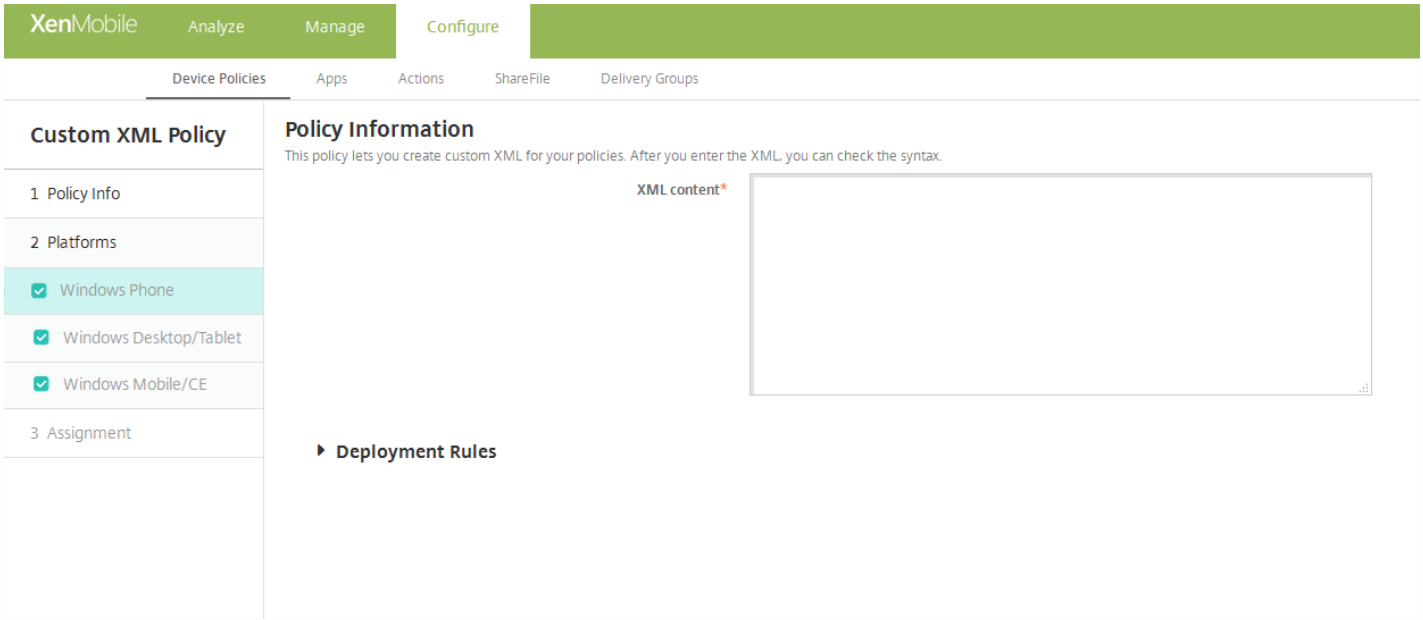


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

7. 分别为选择的每个平台配置以下设置：

- **XML 内容**：键入或复制并粘贴要添加到策略中的自定义 XML 代码。

8. 配置部署规则

9. 单击**下一步**。 XenMobile 检查 XML 内容语法。 内容框下将显示所有语法错误。 必须先修复所有错误才能继续。

如果没有语法错误，将显示**自定义 XML 策略**分配页面。

10. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

11. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。
- 配置的部署计划对所有平台相同。 您做出的任何更改都会应用到所有平台。

12. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

删除文件和文件夹设备策略

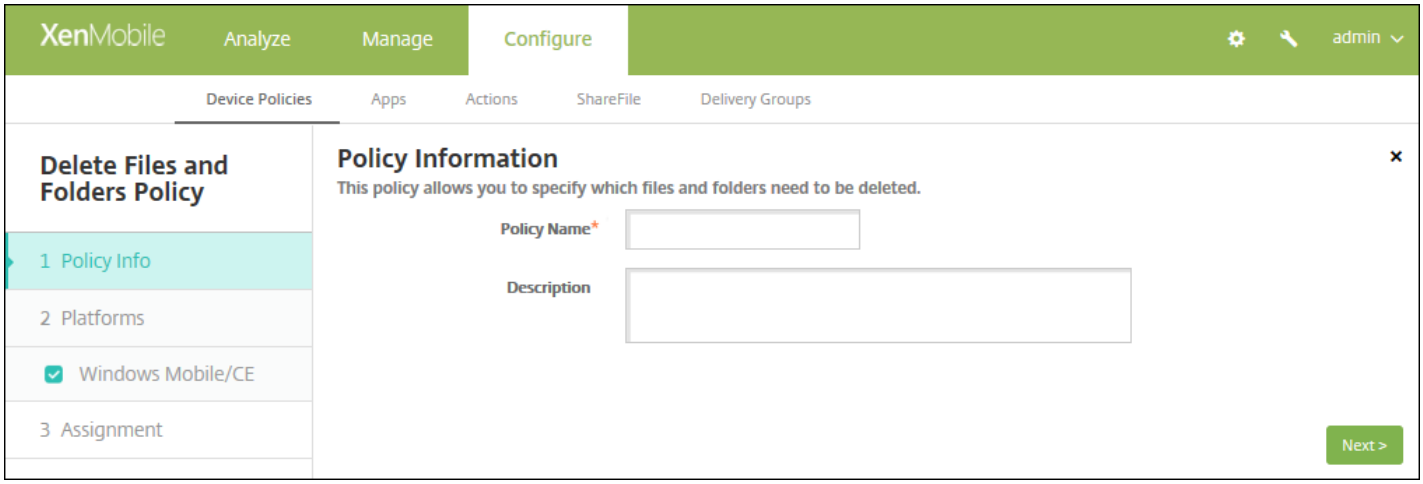
Aug 11, 2016

可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的文件或文件夹。

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。

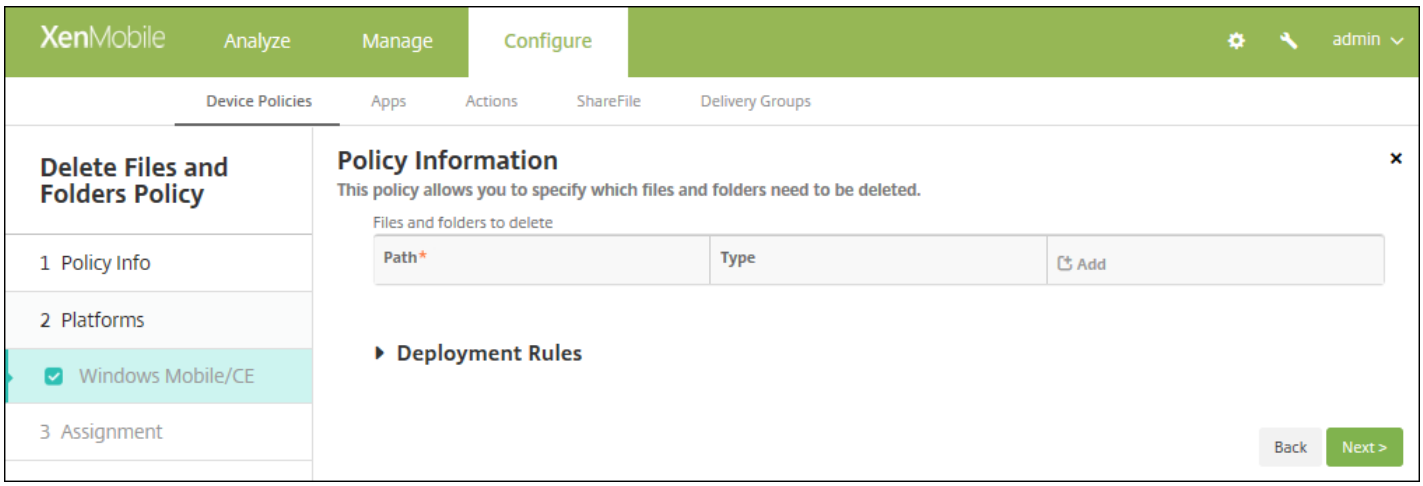
3. 展开**更多**，然后在**应用程序**下面，单击**删除文件和文件夹**。 此时将显示**删除文件和文件夹策略**信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Windows Mobile/CE 平台**页面。



6. 配置以下设置：

- **要删除的文件和文件夹**：对于要删除的每个文件或文件夹，单击“添加”，然后执行以下操作：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

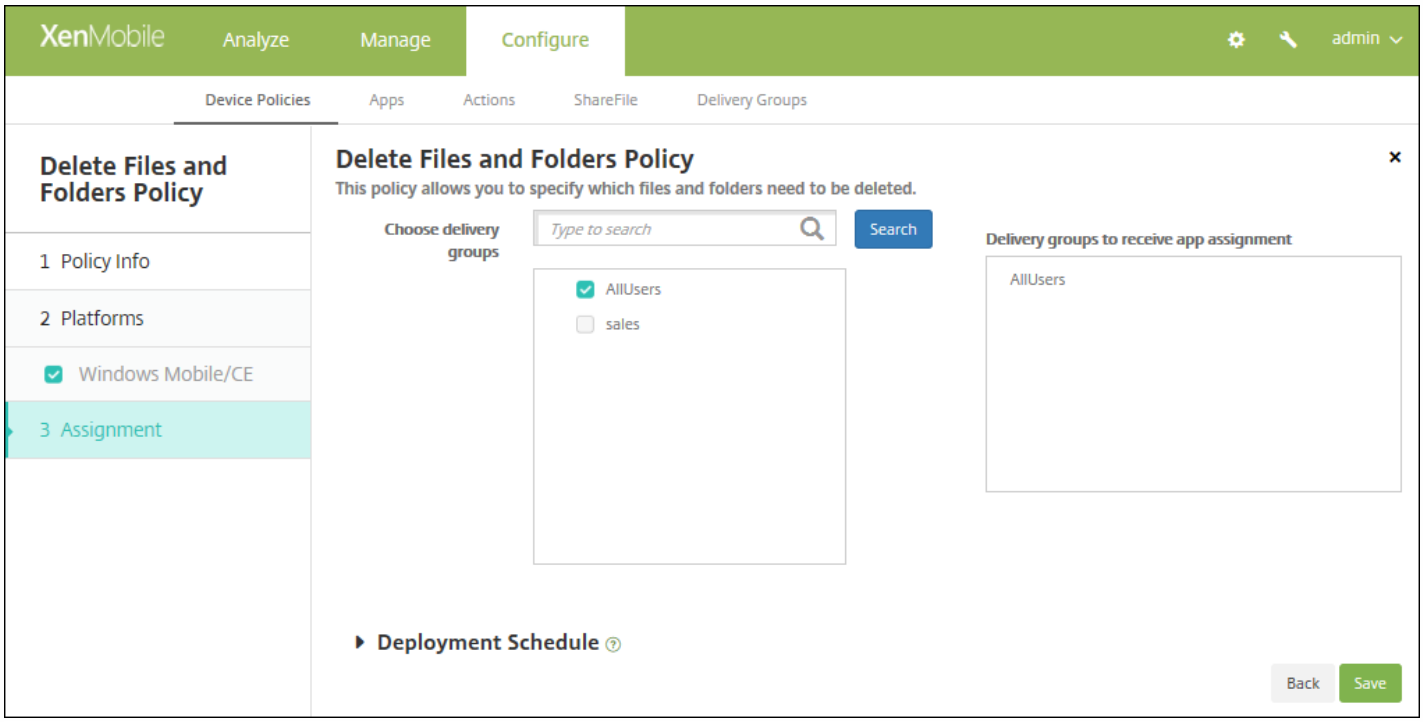
- **路径**：键入文件或文件夹的路径。
- **类型**：在列表中，单击“文件”或“文件夹”。 默认值为“文件”。
- 单击**保存**将保存此文件或文件夹，或单击**取消**不保存此文件夹或文件夹。

  注意：要删除现有列表，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

  要编辑现有列表，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**删除文件和文件夹策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

删除注册表项和值设备策略

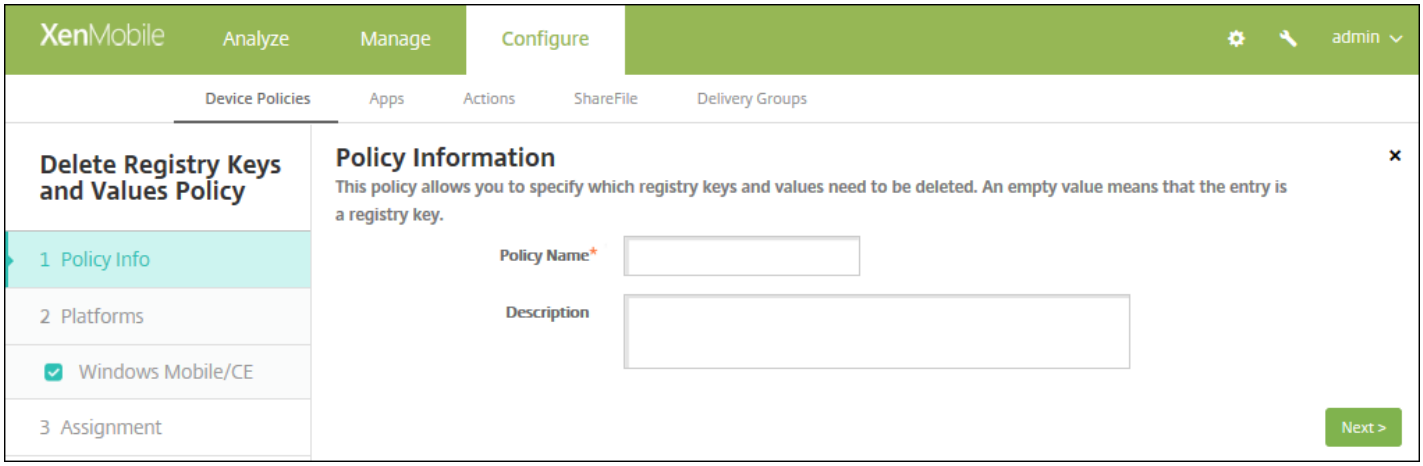
Aug 11, 2016

可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的注册表项和值。

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。

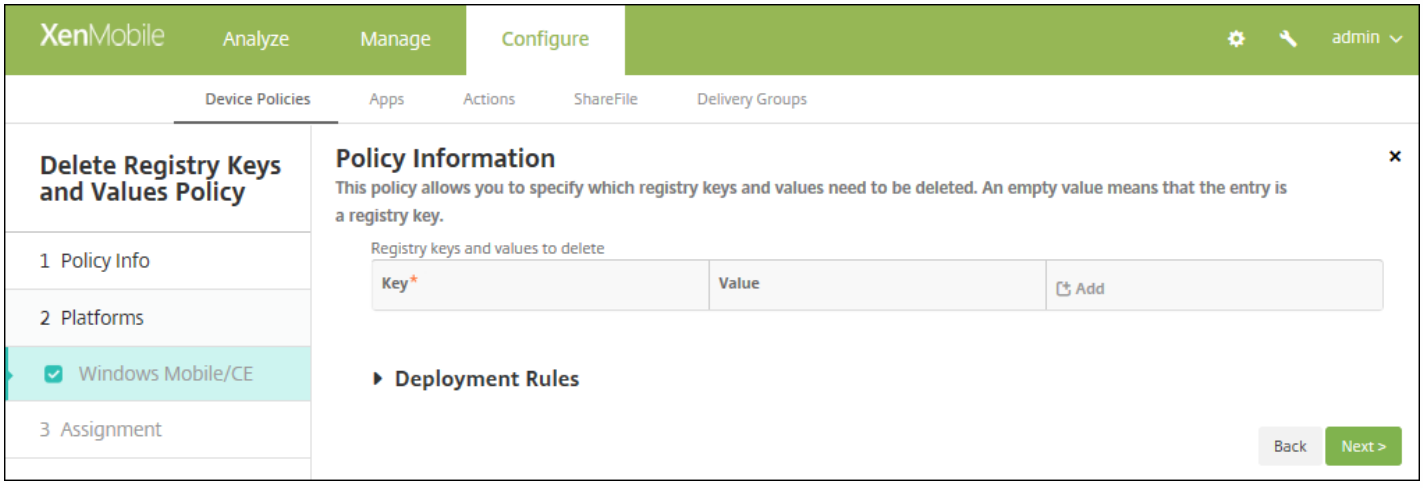
3. 展开**更多**，然后在**应用程序**下面，单击**删除注册表项和值**。 此时将显示**删除注册表项和值**信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Windows Mobile/CE** 平台页面。



6. 配置以下设置：

- **要删除的注册表项和值**：对于要删除的每个注册表项和值，单击**添加**，然后执行以下操作：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

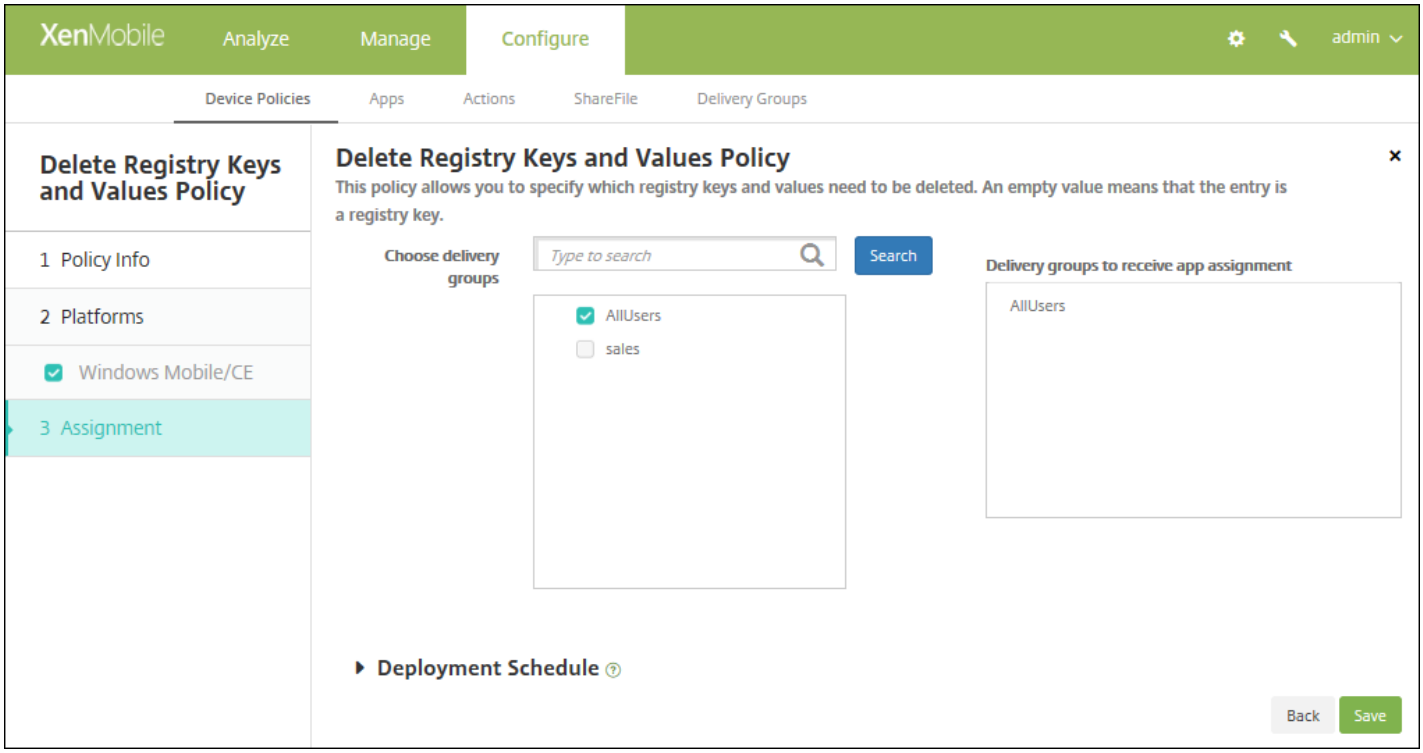
- **注册表项**：键入注册表项路径。 此为必填字段。注册表项路径应以 HKEY_CLASSES_ROOT\ 或 HKEY_CURRENT_USER\ or HKEY_LOCAL_MACHINE\ 或 HKEY_USERS\ 开头。
- **值**：键入要删除的值名称，或将此字段留空以删除整个注册表项。
- 单击**保存**将保存此注册表项和值，或单击**取消**不保存此注册表项和值。

  注意：要删除现有列表，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

  要编辑现有列表，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**删除注册表项和值**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备运行状况证明设备策略

Aug 11, 2016

在 XenMobile 中，您可以要求 Windows 10 设备报告其运行状况，方法是让这些设备将特定数据和运行时信息发送给 Health Attestation Service (HAS) 进行分析。 HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 XenMobile。 XenMobile 收到运行状况证明证书后，根据运行状况证明证书的内容，部署您之前设置的自动操作。

HAS 验证的数据包括：

- AIK 是否存在
- Bit Locker 状态
- 启动调试是否已启用
- 启动管理器修订列表版本
- 代码完整性是否已启用
- 代码完整性修订列表版本
- DEP 策略
- ELAM 驱动程序是否已加载
- 颁发时间
- 内核调试是否已启用
- PCR
- 重置计数
- 重新启动计数
- 安全模式是否已启用
- SBCP 哈希
- 安全启动是否已启用
- 测试签名是否已启用
- 已启用 VSM
- 已启用 WinPE

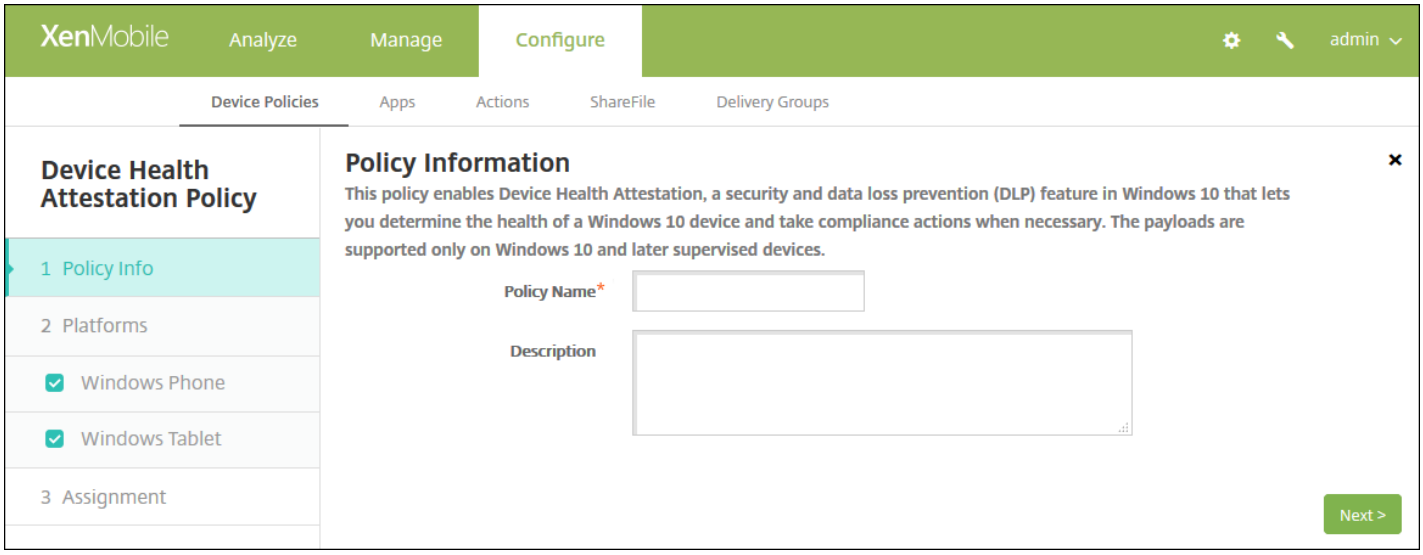
有关详细信息，请参阅 Microsoft 的 HealthAttestation CSP 页面。

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**添加新策略。 此时将显示**添加新策略**对话框。

3. 单击**更多**，然后在**自定义**下面，单击**设备运行状况证明策略**。 此时将显示**设备运行状况证明策略**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 在**策略信息**窗格中，输入以下信息：

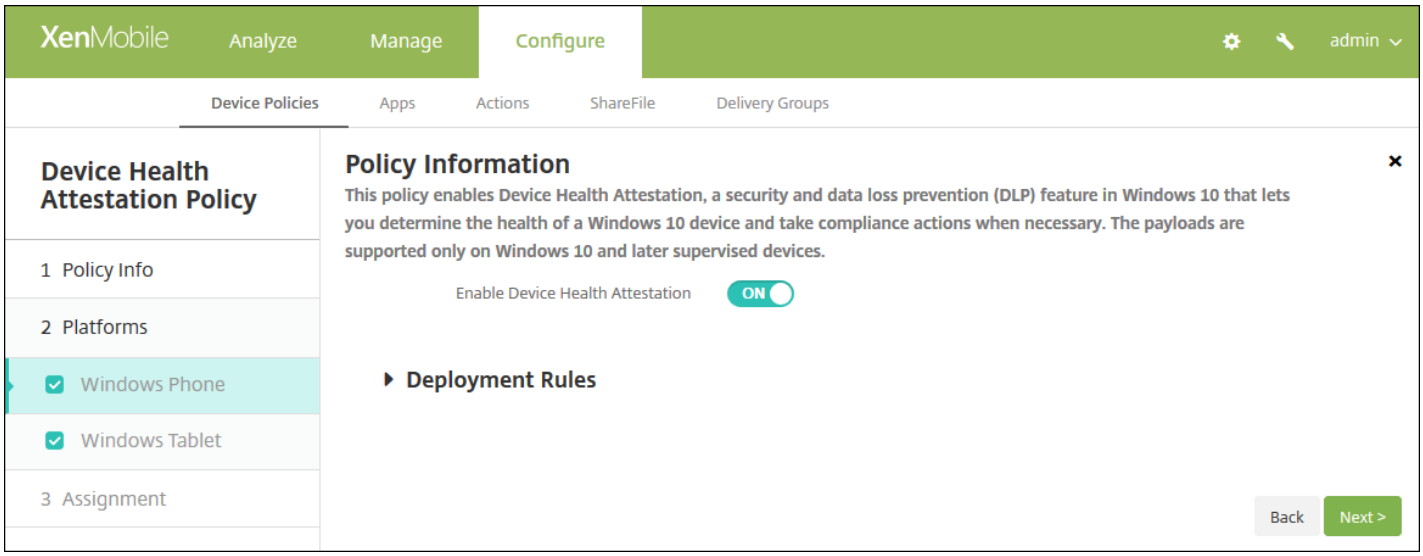
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Windows Phone 和 Windows Tablet 设置



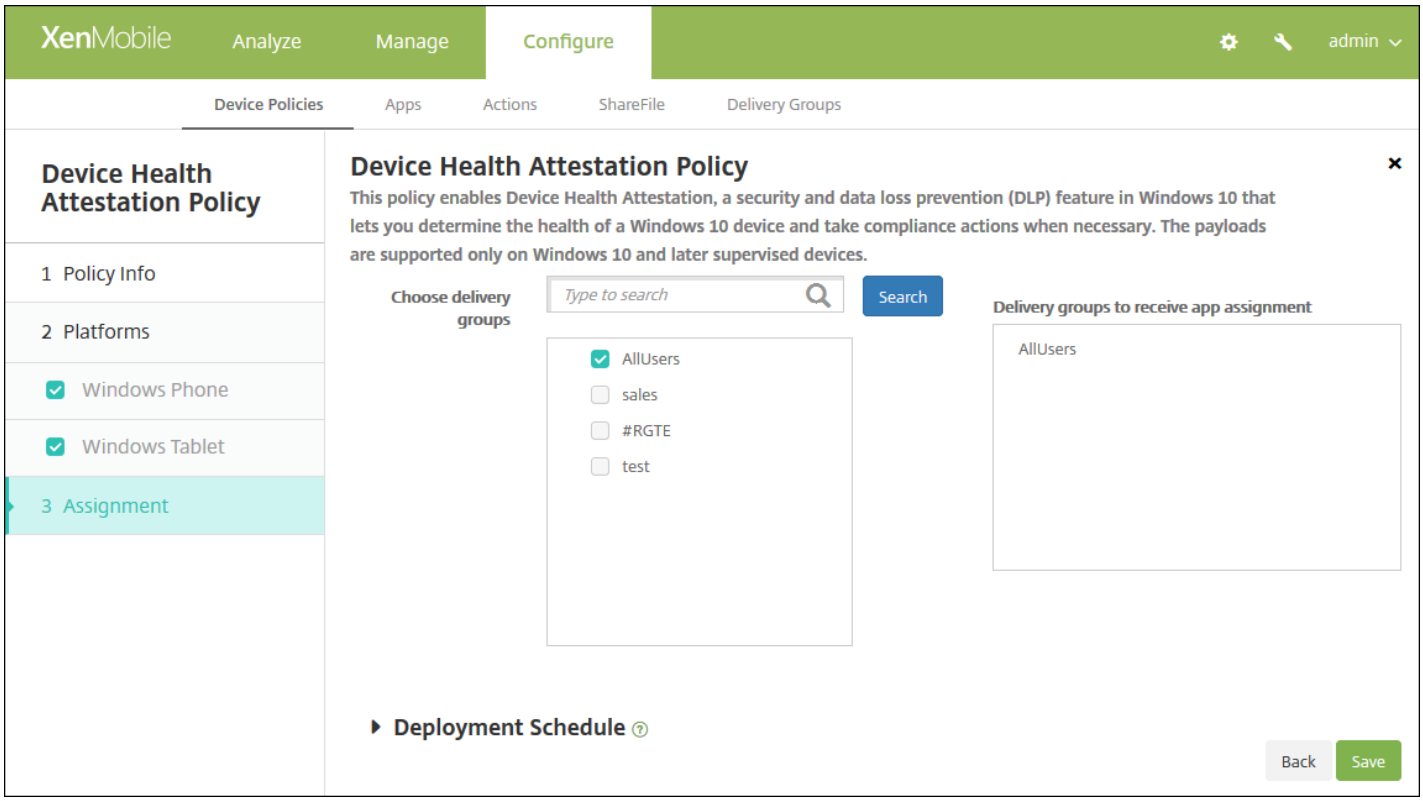
为您选择的各个平台配置此设置：

- **启用设备运行状况证明策略**：选择是否需要设备运行状况证明。 默认值为**关**。

7. 配置部署规则

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 单击**下一步**。 此时将显示**设备运行状况证明**策略分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备名称设备策略

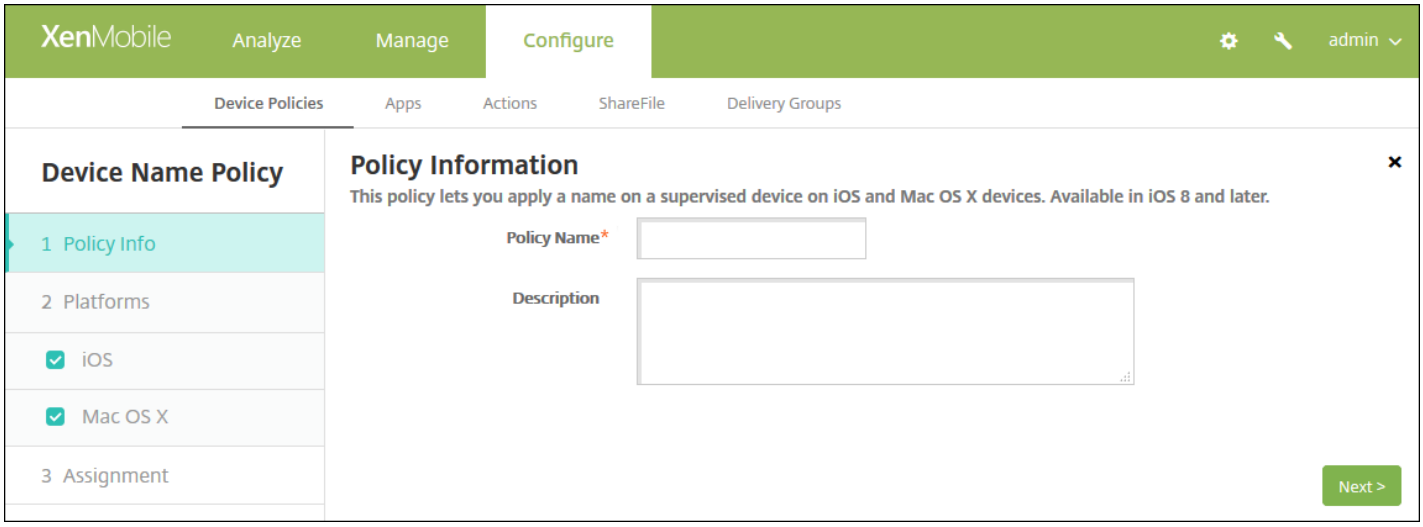
Aug 11, 2016

您可以在 iOS 和 Mac OS X 设备上设置 名称 ，以便轻松识别设备。 可以使用宏、文本或二者的组合定义设备的名称。 例如，要将设备名称设置为设备的序列号，可以使用 ${device.serialnumber}。 要将设备的名称设置为用户名和域的组合，可以使用 ${user.username}@example.com。 有关宏的详细信息，请参阅 XenMobile 中的宏。

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**。 将显示**添加新策略**页面。

3. 展开**更多**，然后在**最终用户**下面，单击**设备名称**。 此时将显示**设备名称策略**信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

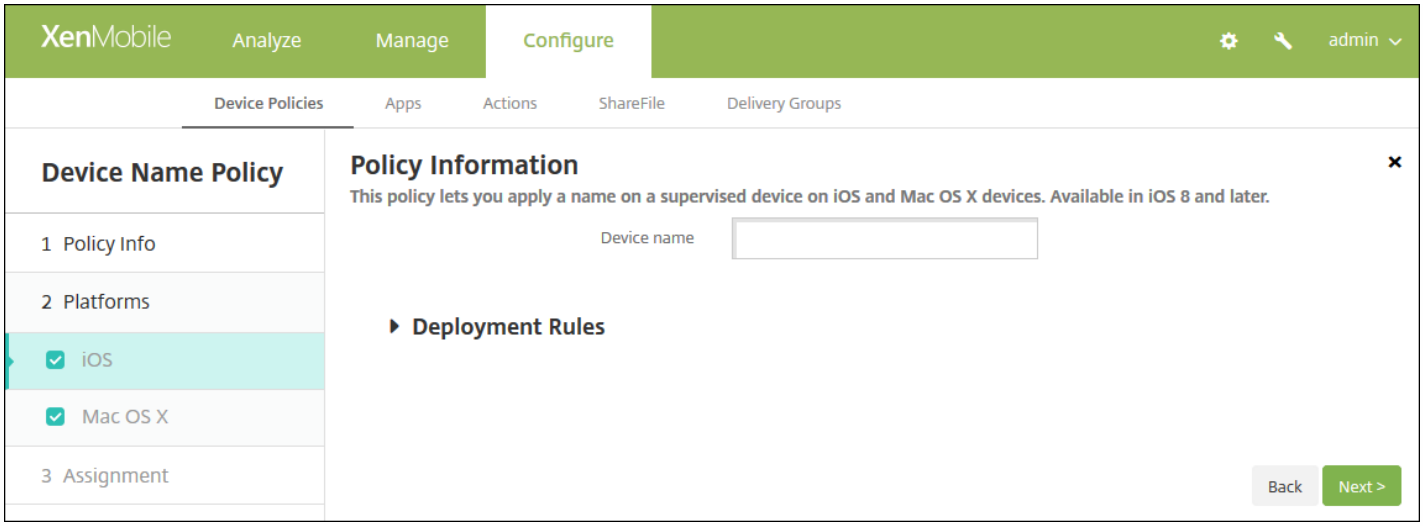
5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 和 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

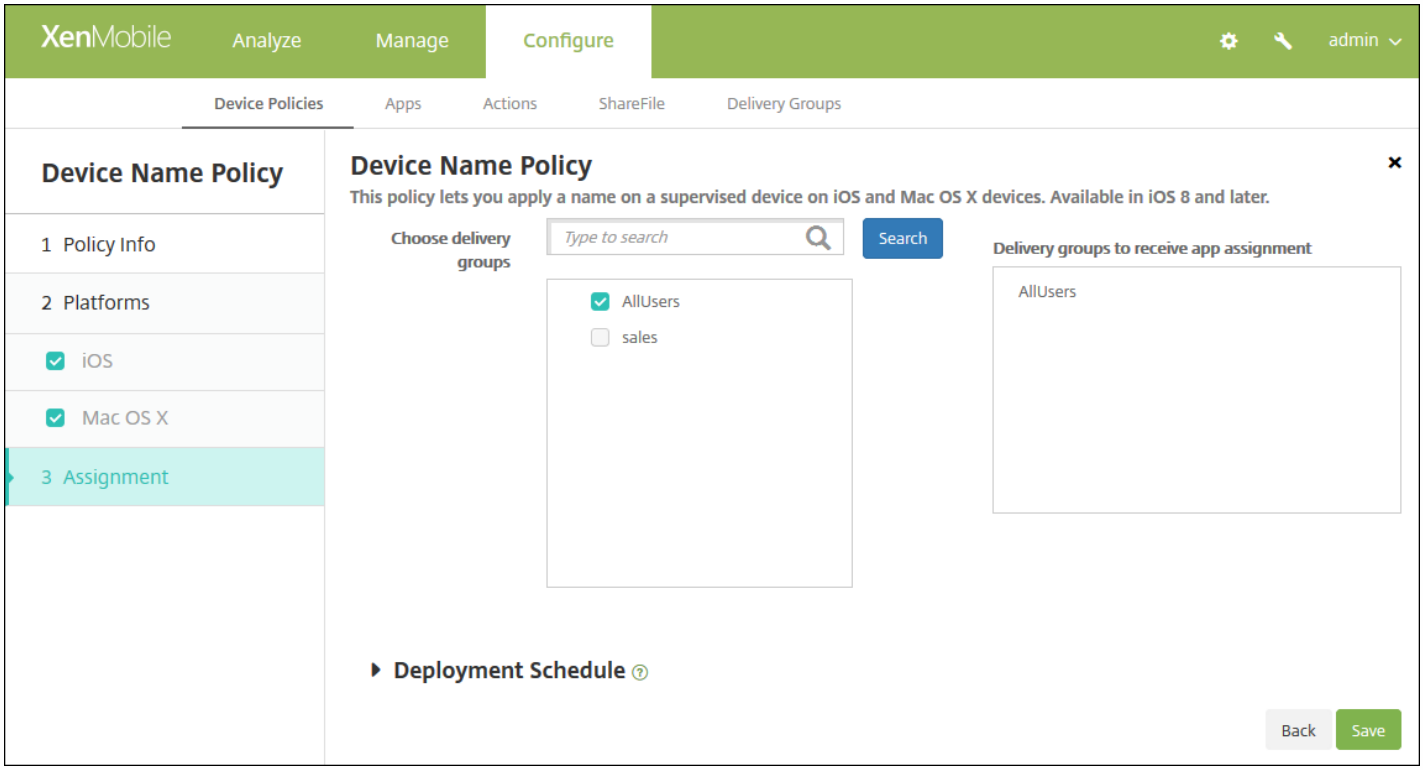


为您选择的平台配置此设置：

- **设备名称**：键入宏、宏的组合或宏和文本的组合，为每个设备设置唯一名称。 例如，使用 ${device.serialnumber} 将设备名称设置为每个设备的序列号，或使用 ${device.serialnumber} ${ user.username } 使设备名称中包含用户名。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**设备名称策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

企业中心设备策略

Aug 11, 2016

面向 Windows Phone 的企业中心设备策略允许您通过企业中心公司应用商店分发应用程序。

需要具备以下各项才能创建策略：

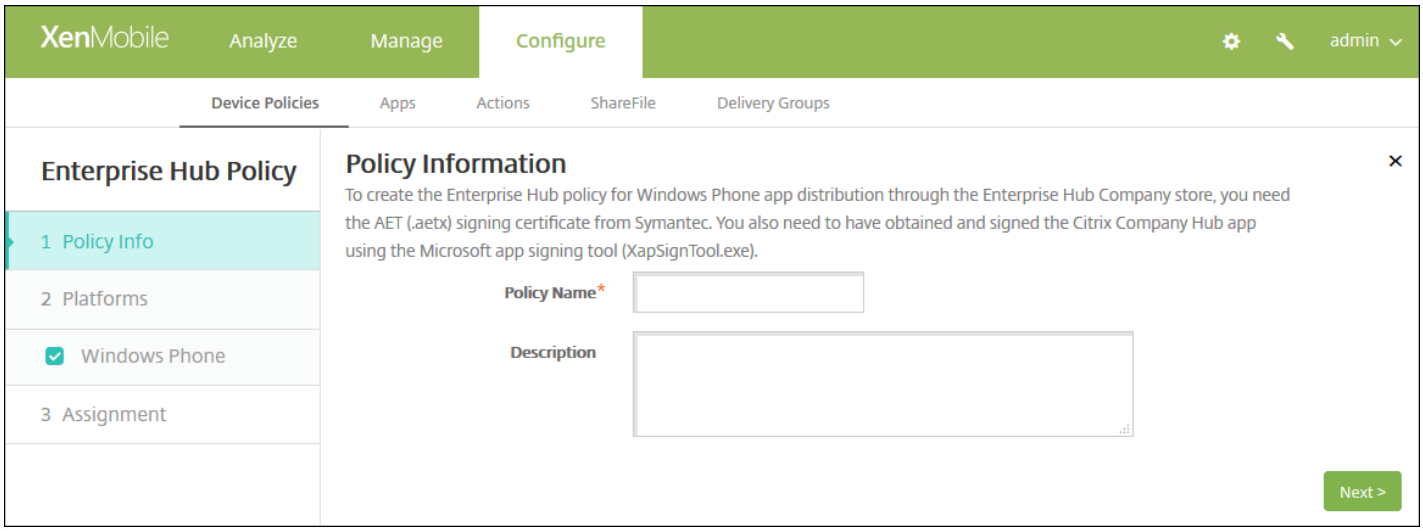
- 来自 Symantec 的 AET (.aetx) 签名证书
- 使用 Microsoft 应用程序签名工具 (XapSignTool.exe) 签名的 Citrix Company Hub 应用程序

注意：对于一种 Windows Phone Worx Home 模式，XenMobile 仅支持一种企业中心策略。 例如，要上载 Windows Phone Worx Home for XenMobile Enterprise Edition，不应该使用不同版本的 Work Home for XenMobile Enterprise Edition 创建多个企业中心策略。 设备注册期间只能部署初始企业 Hub 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 **XenMobile Agent** 下单击**企业中心**。 此时将显示 **Enterprise Hub Policy**（企业 Hub 策略）页面。

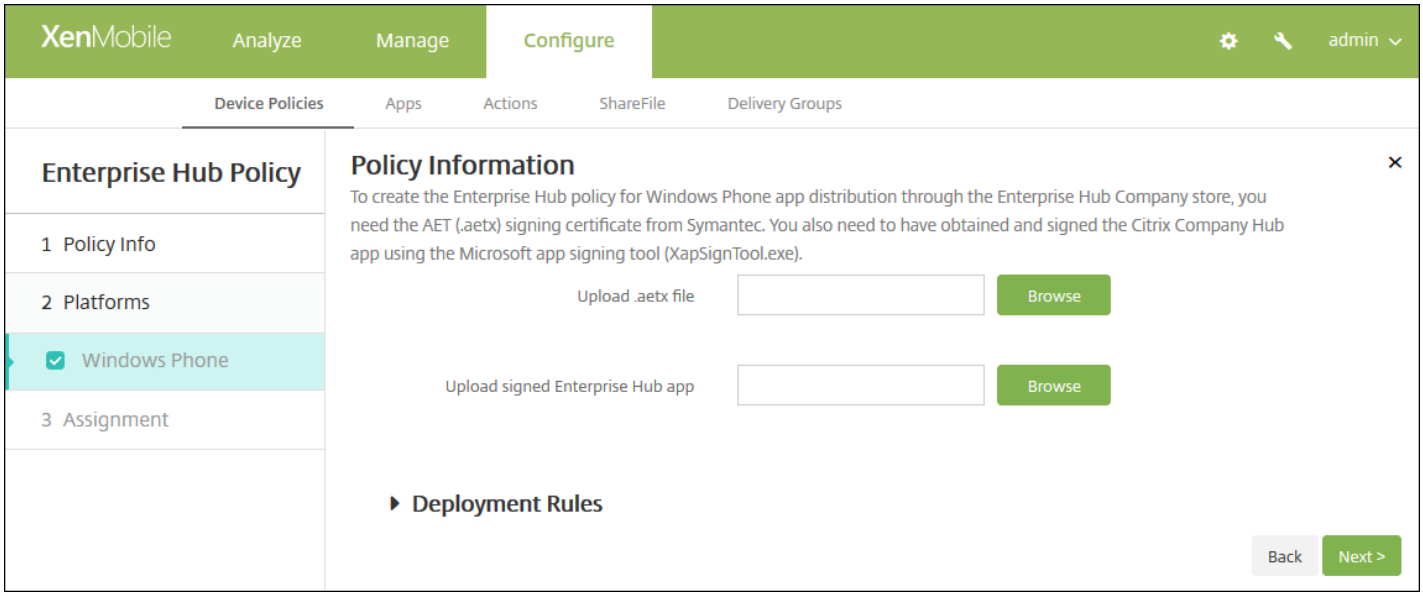


4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Windows Phone** 平台页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

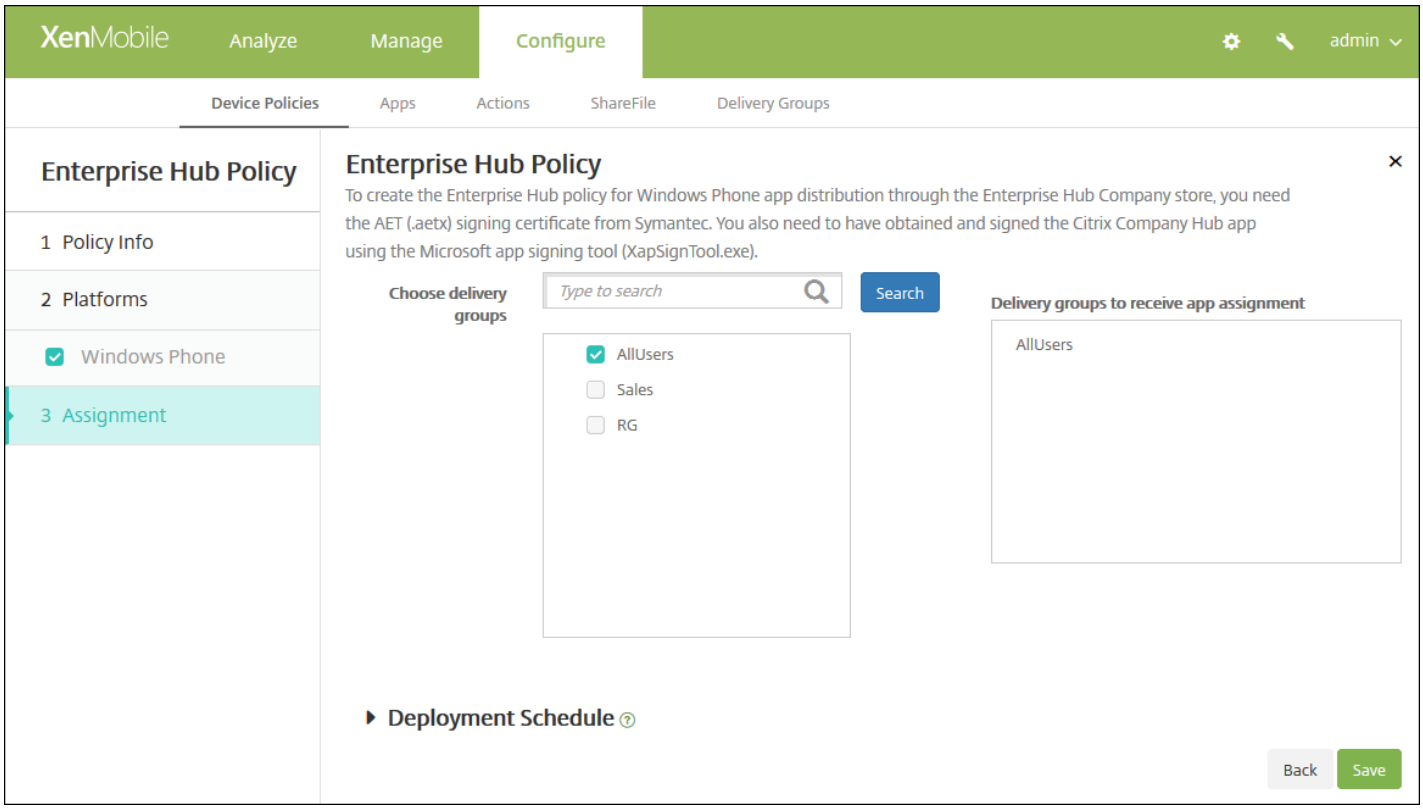


6. 配置以下设置：

- **上载 .aetx 文件**：单击**浏览**，导航到 .aetx 文件的位置，选择此文件。
- **上载签名的企业中心应用程序**：单击**浏览**，导航到企业中心应用程序的位置，选择此应用程序。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**企业中心策略**分配页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

文件设备策略

Aug 11, 2016

您可以在 XenMobile 中为用户添加执行某些功能的脚本文件，或者也可添加 Android 设备用户能够在其设备上访问的文档文件。 添加文件时，还可以指定设备上要存储该文件的目录。 例如，如果您希望 Android 用户接收公司文档或 .pdf 文件，则可以将该文件部署到设备，然后将文件位置告知用户。

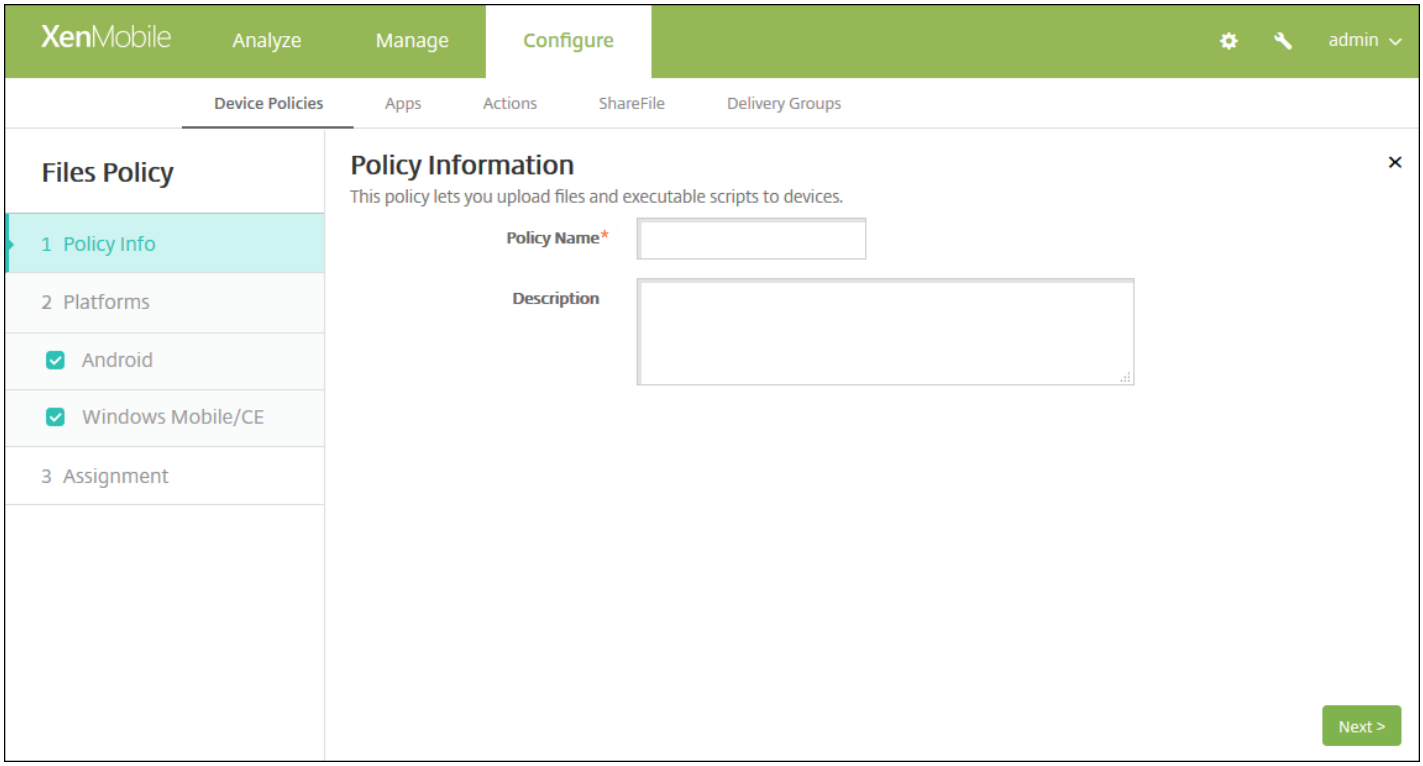
利用此策略可以添加以下文件类型：

- 文本文件（.xml、.html、.py 等）
- 其他文件，如文档、图片、电子表格或演示文稿
- 仅适用于 Windows Mobile 和 Windows CE：通过 MortScript 创建的脚本文件

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**应用程序**下面，单击**文件**。 此时将显示**文件策略**信息页面。

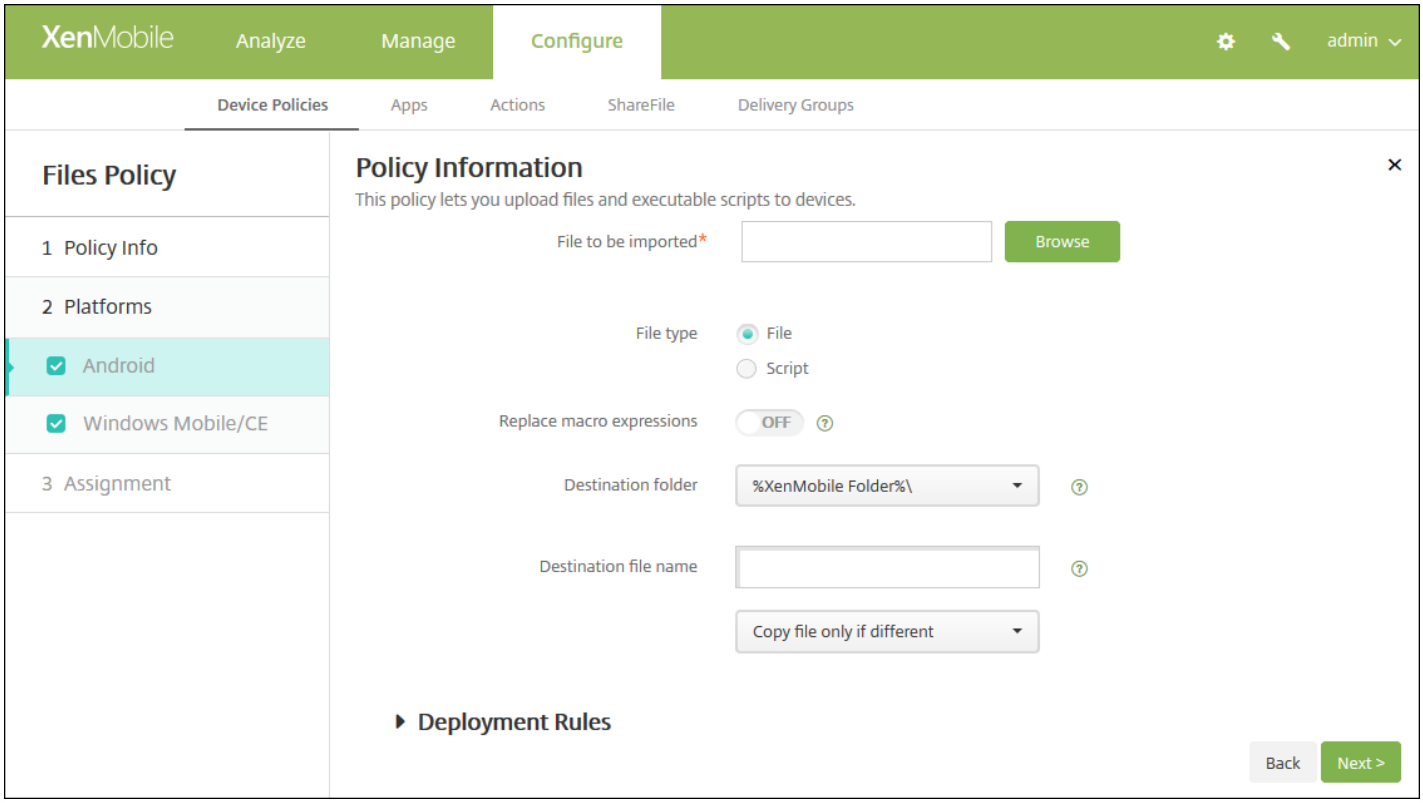


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

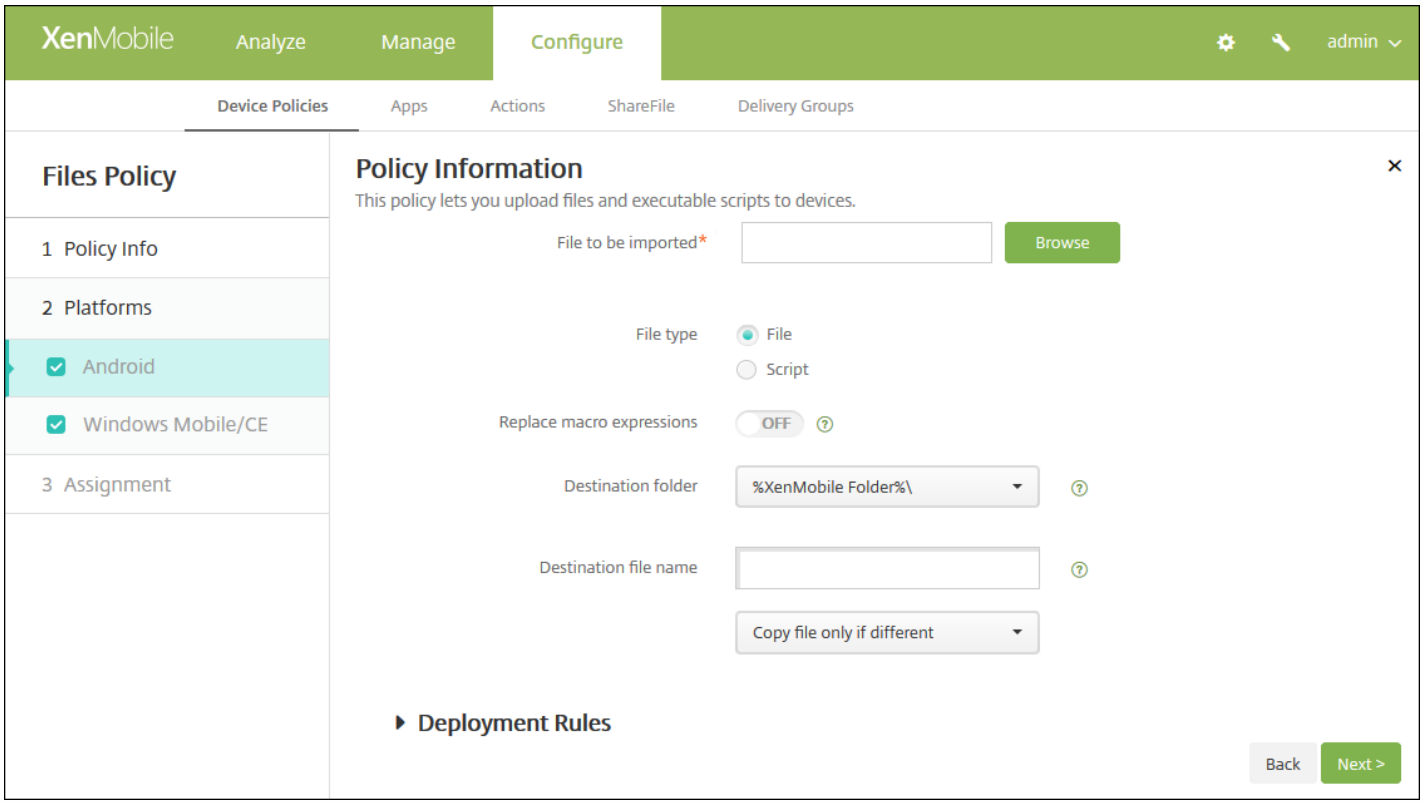
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Android 设置

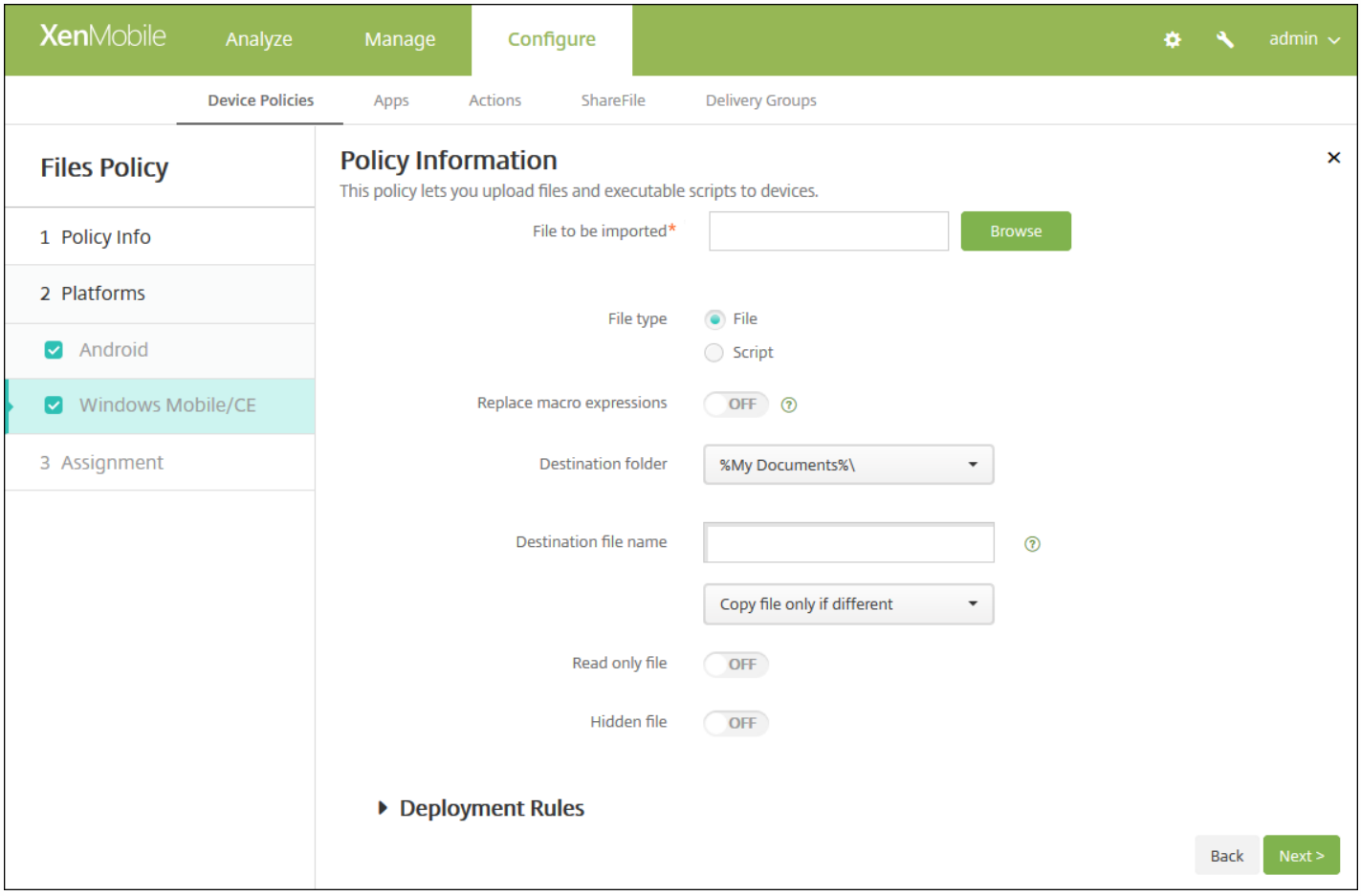


© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置以下设置：

- **要导入的文件**：单击浏览，然后导航到文件的位置，选择要导入的文件。
- **文件类型**：选择**文件**或**脚本**。 如果选择**脚本**，将显示**立即执行**。 选择是否在上载文件后立即执行脚本。 默认值为**关**。
- **替换宏表达式**：选择是否将脚本中的宏令牌名称替换为设备或用户属性。 默认值为**关**。
- **目标文件夹**：在列表中，选择存储已上载文件的位置，或单击**新增**选择未列出的文件位置。 此外，还可以使用宏 %XenMobile Folder%\ 或 %Flash Storage%\ 作为路径标识符的开头。
- **目标文件夹名**：（可选）如果必须在部署到设备上之前更改文件名，请键入一个不同名称。
- **仅在不同时复制文件**：在列表中，选择是否仅在与现有文件存在差异时复制文件。 默认设置为仅在文件存在差异时复制文件

配置 Windows Mobile/CE 设置



配置以下设置：

- **要导入的文件**：单击浏览，然后导航到文件的位置，选择要导入的文件。
- **文件类型**：选择**文件**或**脚本**。 如果选择**脚本**，将显示**立即执行**。 选择是否在上载文件后立即执行脚本。 默认值为**关**。
- **替换宏表达式**：选择是否将脚本中的宏令牌名称替换为设备或用户属性。 默认值为**关**。
- **目标文件夹**：在列表中，选择存储已上载文件的位置，或单击**新增**选择未列出的文件位置。 此外，还可以使用以下宏作为路径标识符的开头：
  - %Flash Storage%\
  - %XenMobile Folder%\

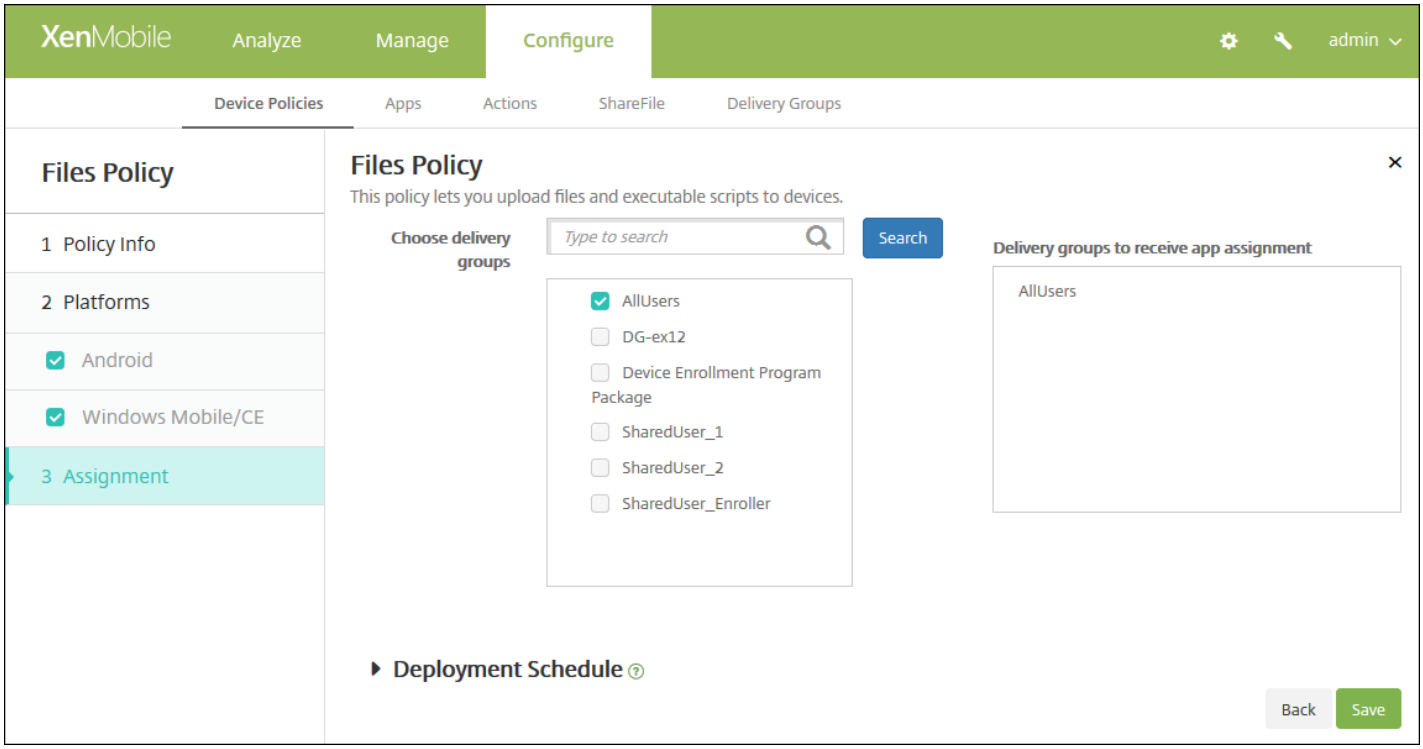
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- %Program Files%\
- %My Documents%\
- %Windows%\

- **目标文件夹名**：（可选）如果必须在部署到设备上之前更改文件名，请键入一个不同名称。
- **仅在不同时复制文件**：在列表中，选择是否仅在与现有文件存在差异时复制文件。 默认设置为仅在文件存在差异时复制文件
- **只 读 文件**：选择文件是否为只读文件。 默认值为**关**。
- **隐藏文件**：选择文件是否显示在文件列表中。 默认值为**关**。

7. 配置部署规则

8. 单击**下一步**。 将显示**文件策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

字体设备策略

Aug 11, 2016

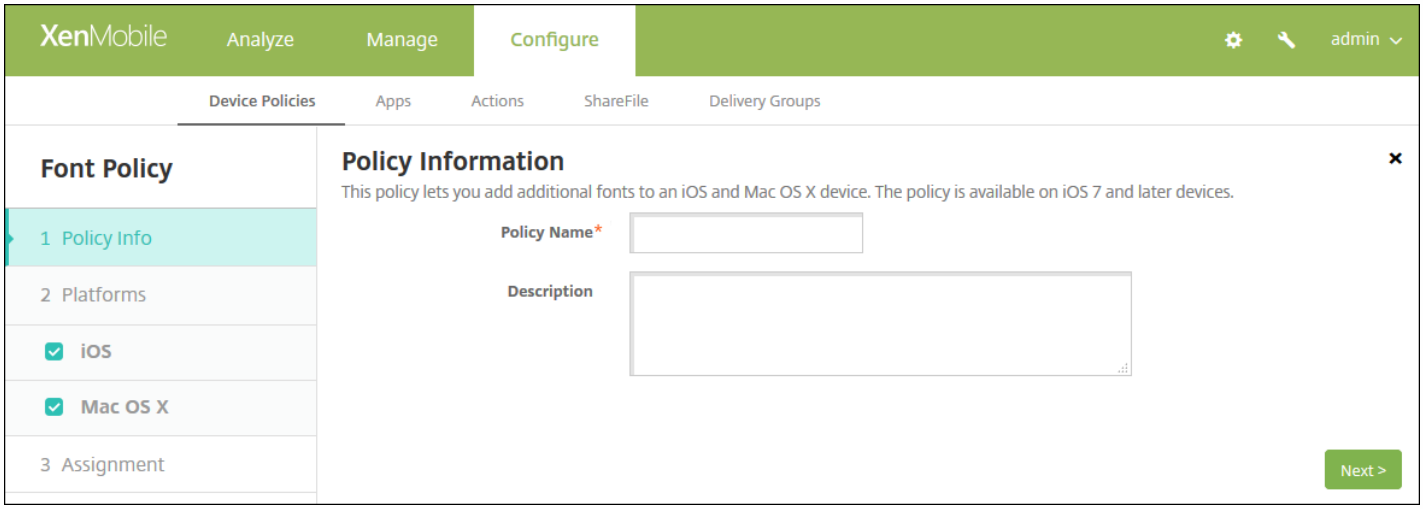
可以在 XenMobile 中添加一个设备策略，以向用户的 iOS 和 Mac OS X 设备添加其他字体。 字体必须是 TrueType (.ttf) 或 OpenType (.oft) 字体。 不支持字体集合（.ttc 或 .otc）。

注意：对于 iOS，此策略仅适用于 iOS 7.0 及更高版本。

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**最终用户**下面，单击**字体**。 此时将显示 **Font Policy**（字体策略）页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

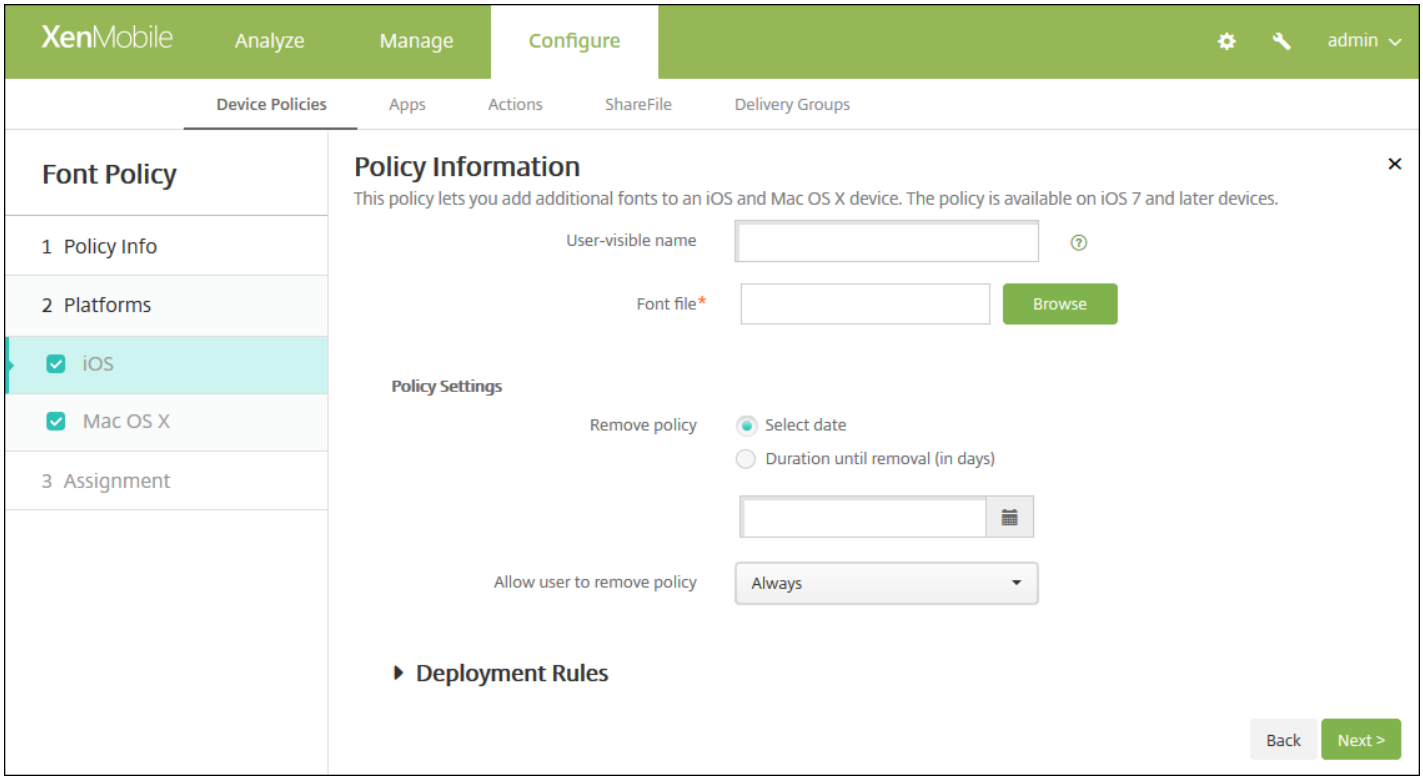
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

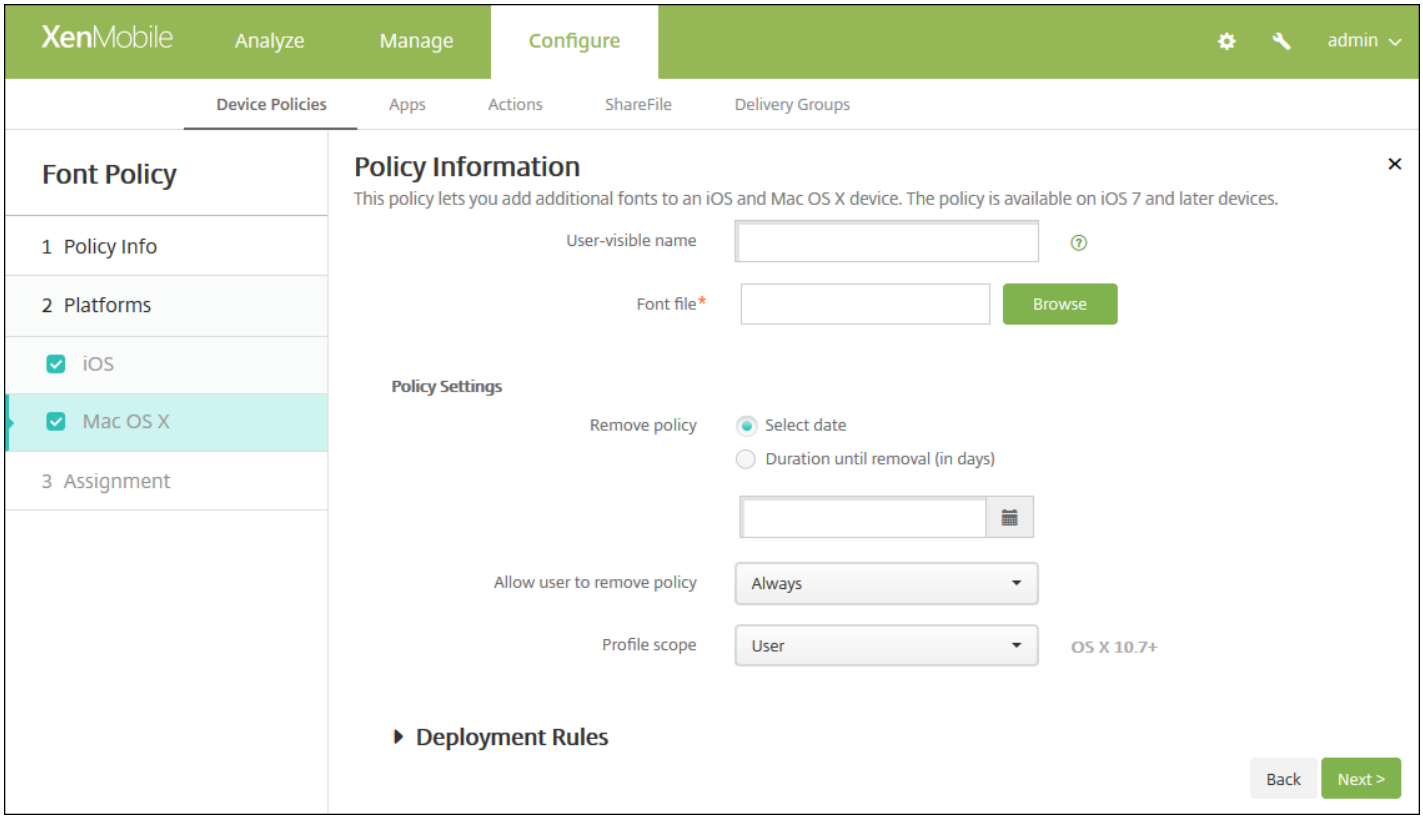


配置以下设置：

- **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**：选择要添加到用户设备的字体文件，可以单击**浏览**，然后导航到该文件的位置。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



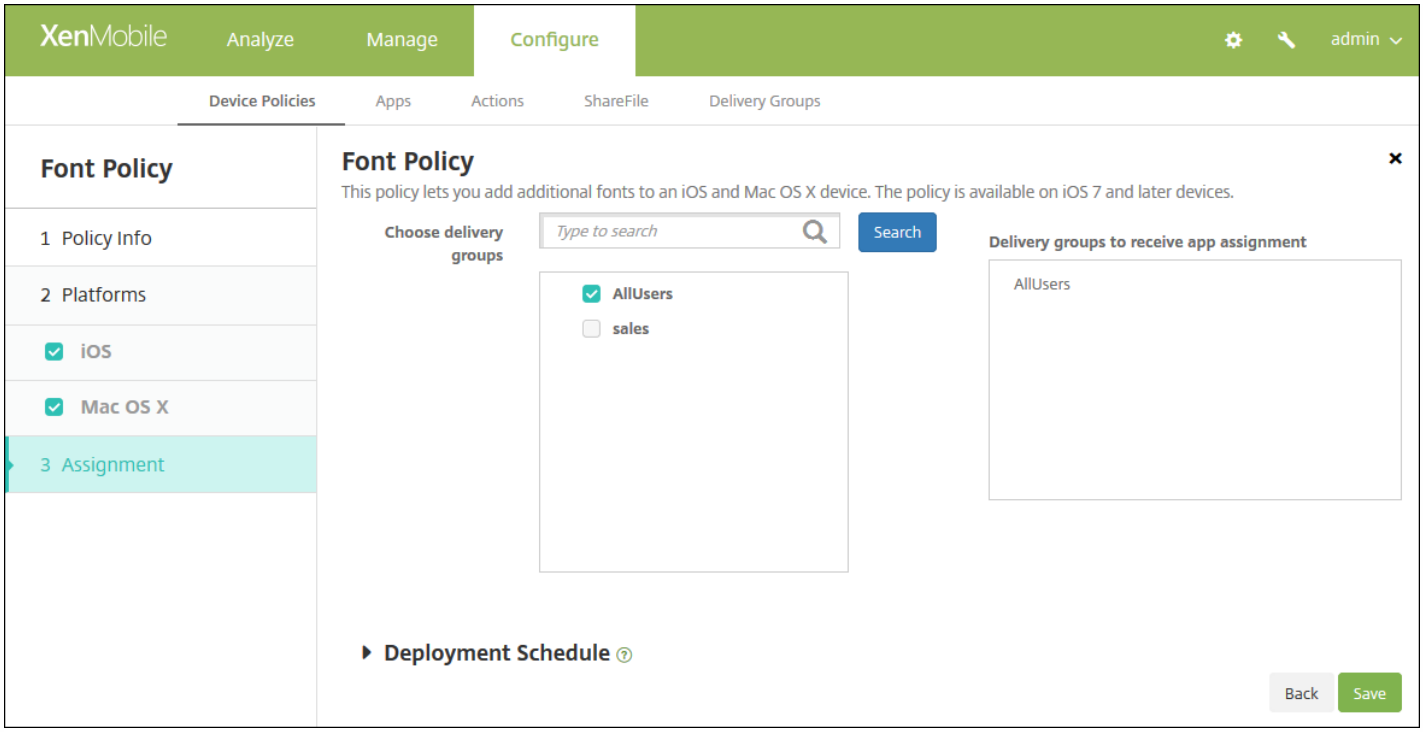
配置以下设置：

- **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**：选择要添加到用户设备的字体文件，可以单击**浏览**，然后导航到该文件的位置。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Font Policy**（字体策略）分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

导入 iOS 和 Mac OS X 配置文件设备策略

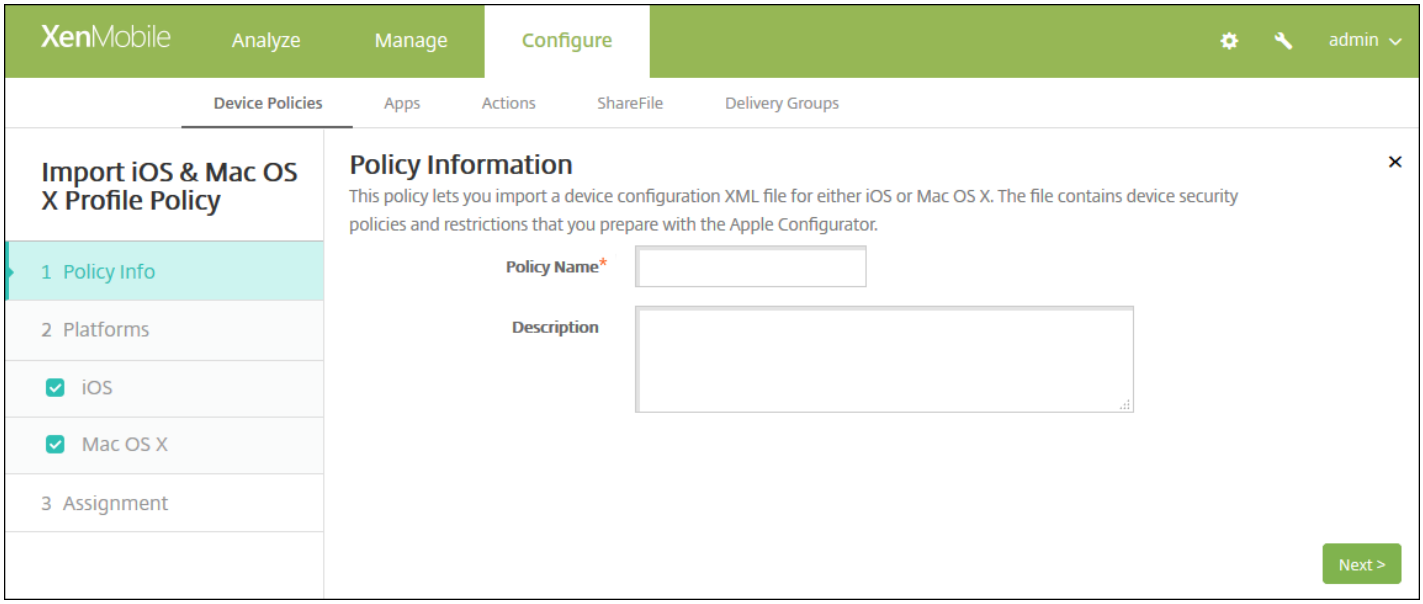
Aug 11, 2016

可以将 iOS 和 OS X 设备的设备配置 XML 文件导入到 XenMobile 中。 此文件包含您使用 Apple Configurator 准备的设备安全策略和限制。 有关使用 Apple Configurator 创建配置文件的详细信息，请参阅 Apple 的 Apple Configurator 页面。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。

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**自定义**下面，单击**导入 iOS 和 Mac OS X 配置文件**。 此时将显示**导入 iOS 和 Mac OS X 配置文件策略**信息页面。

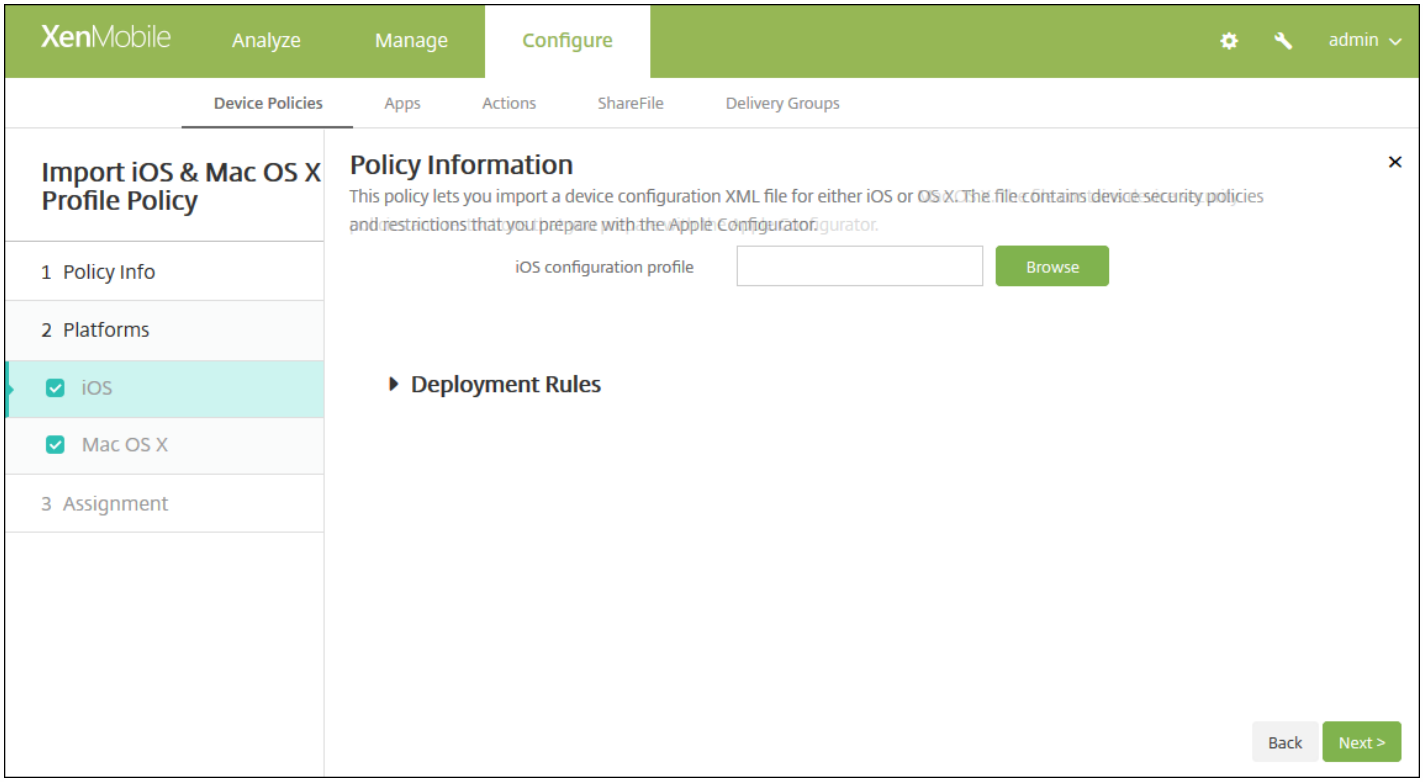


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 8 以了解如何设置此平台的部署规则 。

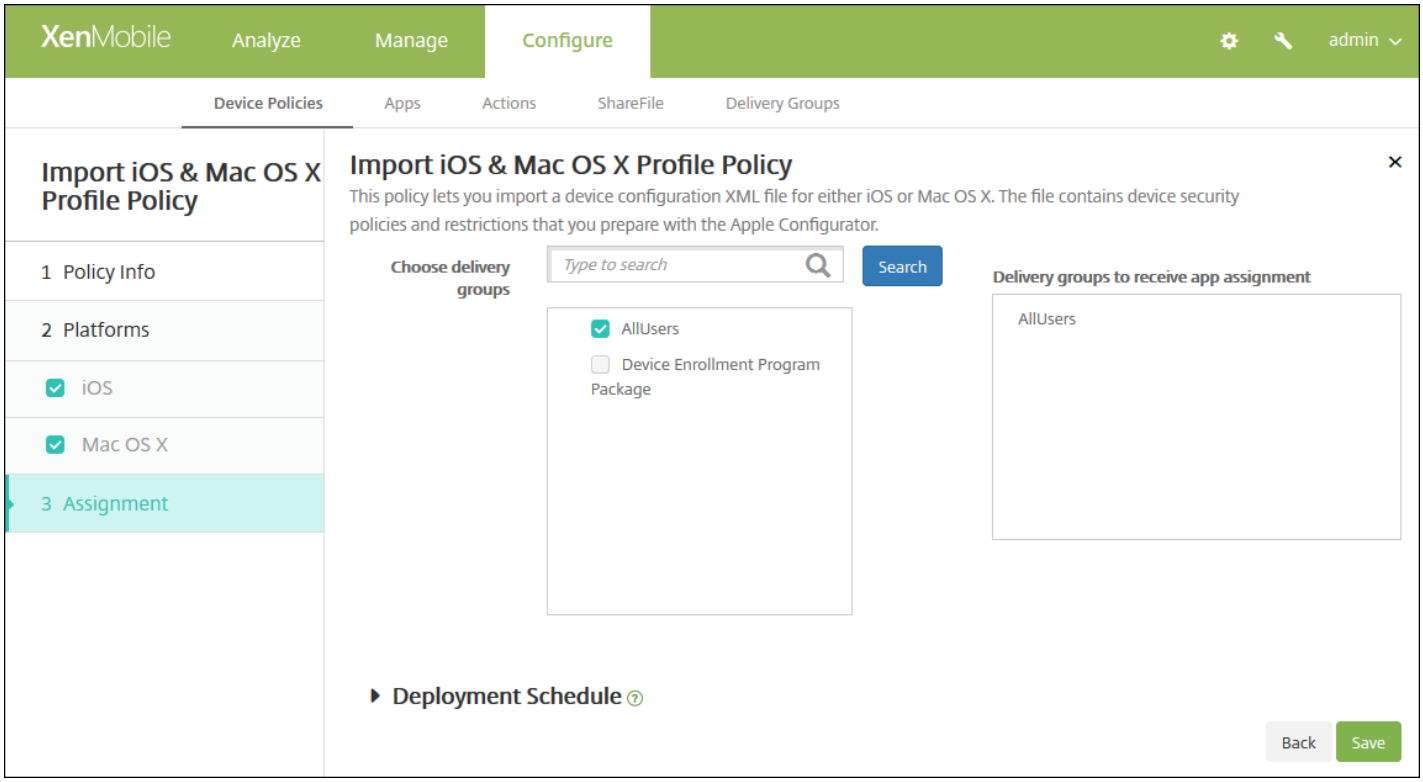
7. 为您选择的每个平台配置以下设置：

- **iOS 配置文件**或 **Mac OS X 配置文件**：单击**浏览**并导航到要导入的配置文件的位置，选择次文件。

8. 配置部署规则

8. 单击**下一步**。 此时将显示**导入 iOS 和 Mac OS X 配置文件策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Kiosk 设备策略

Aug 11, 2016

可以在 XenMobile 中创建 Kiosk 策略以便能够指定只能在 Samsung SAFE 设备上使用一个或多个特定的应用程序。 此策略对旨在仅运行特定类型或类别的应用程序的企业设备非常有用。 此策略还允许您为设备选择处于 Kiosk 模式时设备主屏幕和锁定屏幕墙纸使用的自定义图片。

将 Samsung SAFE 设备置于 Kiosk 模式

1. 在移动设备上启用 Samsung SAFE API 密钥，如 Samsung MDM 许可证密钥设备策略中所述。 此步骤允许您在 Samsung SAFE 设备上启用策略。

2. 为 Android 设备启用“连接计划策略”，如连接计划设备策略中所述。 此步骤允许 Android 设备连接回 XenMobile。

3. 添加 Kiosk 设备策略，如下一部分内容中所述。

4. 将这三条设备策略分配给恰当的交付组。 考虑是否要在这些交付组中包括其他策略，例如“应用程序清单”。

如果以后要从 Kiosk 模式中删除设备，请创建一个 **Kiosk 模式**设置为**禁用**的新 Kiosk 设备策略。 更新交付组以删除启用了 Kiosk 模式的 Kiosk 策略以及添加禁用了 Kiosk 模式的 Kiosk 策略。

添加 Kiosk 设备策略

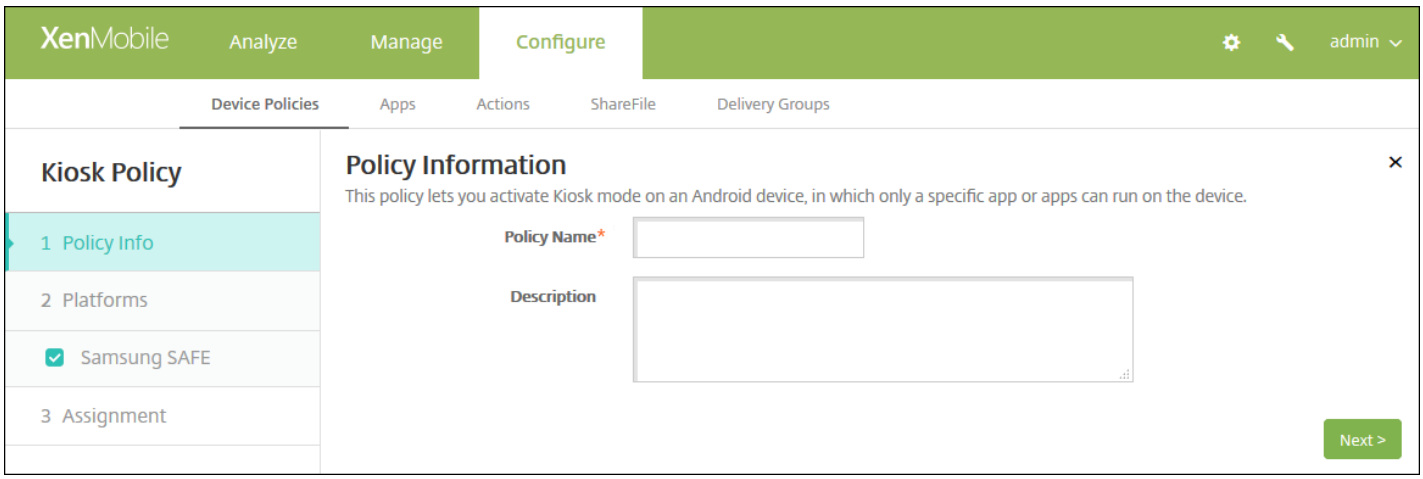
注意：

- 为 Kiosk 模式指定的所有应用程序必须已安装在用户设备上。
- 某些选项仅适用于 Samsung Mobile Device Management API (MDM) 4.0 及更高版本。

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**下面，单击 **Kiosk**。 此时将显示 **Kiosk 策略**页面。



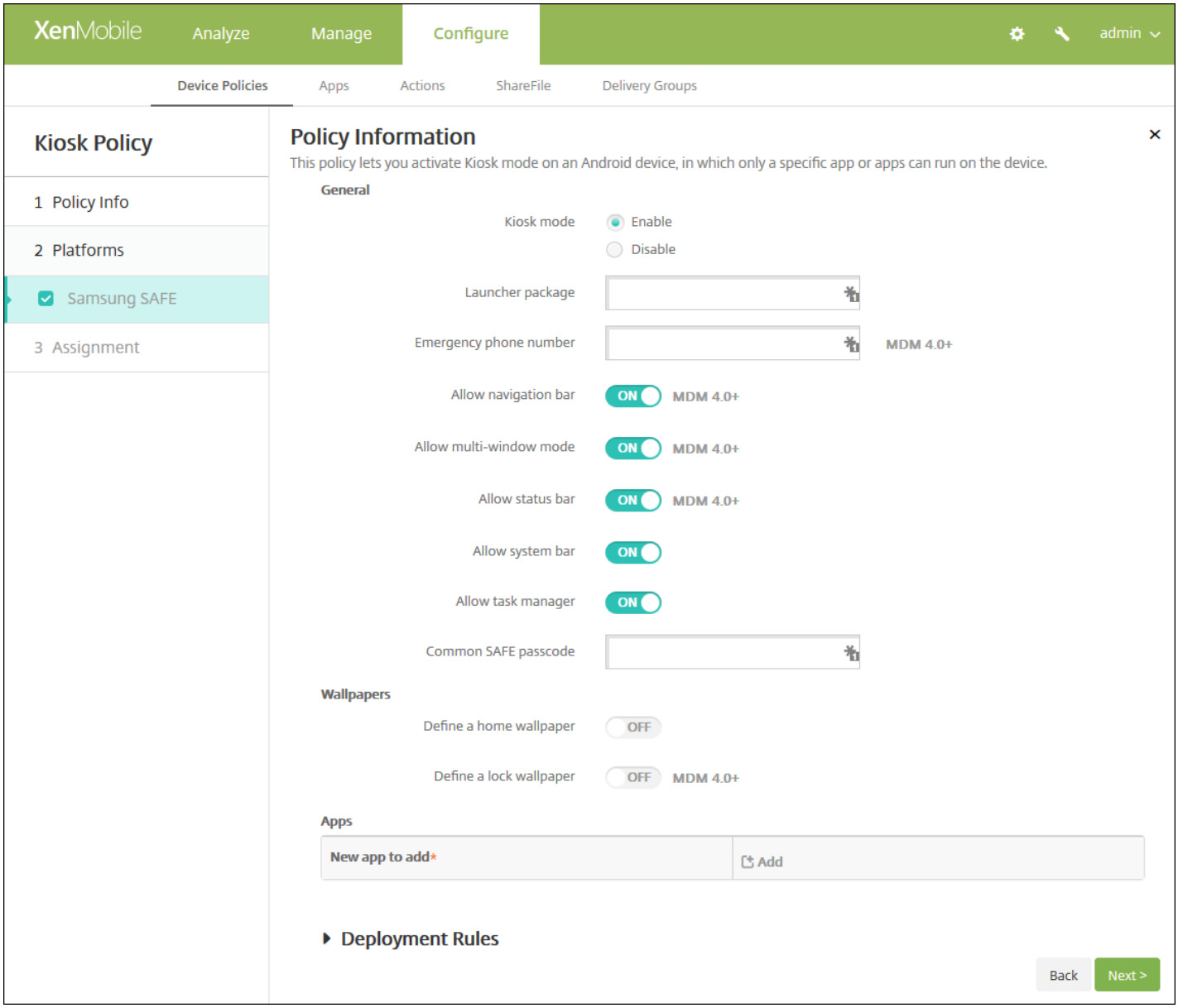
4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Samsung SAFE** 平台信息页面。



6. 配置以下设置：

- **Kiosk 模式**：单击**启用**或**禁用**。 默认值为**启用**。 单击**禁用**时，以下所有选项将消失。
- **启动程序软件包**：除非您开发了内部启动程序以使用户能够打开一个或多个 Kiosk 应用程序，否则 Citrix 建议您将此字段留空。 如果您使用的是内部启动程序，请输入启动程序应用程序软件包的完整名称。
- **紧急电话号码**：输入可选电话号码。 查找所丢失设备的任何人都可以使用此号码与贵公司联系。 仅适用于 MDM 4.0 及更高版本。
- **允许使用导航栏**：选择是否允许用户在处于 Kiosk 模式时看到和使用导航栏。 仅适用于 MDM 4.0 及更高版本。 默认值为**开**。
- **允许多窗口模式**：选择是否允许用户在处于 Kiosk 模式时使用多个窗口。 仅适用于 MDM 4.0 及更高版本。 默认值为**开**。
- **允许使用状态栏**：选择是否允许用户在处于 Kiosk 模式时看到状态栏。 仅适用于 MDM 4.0 及更高版本。 默认值为**开**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

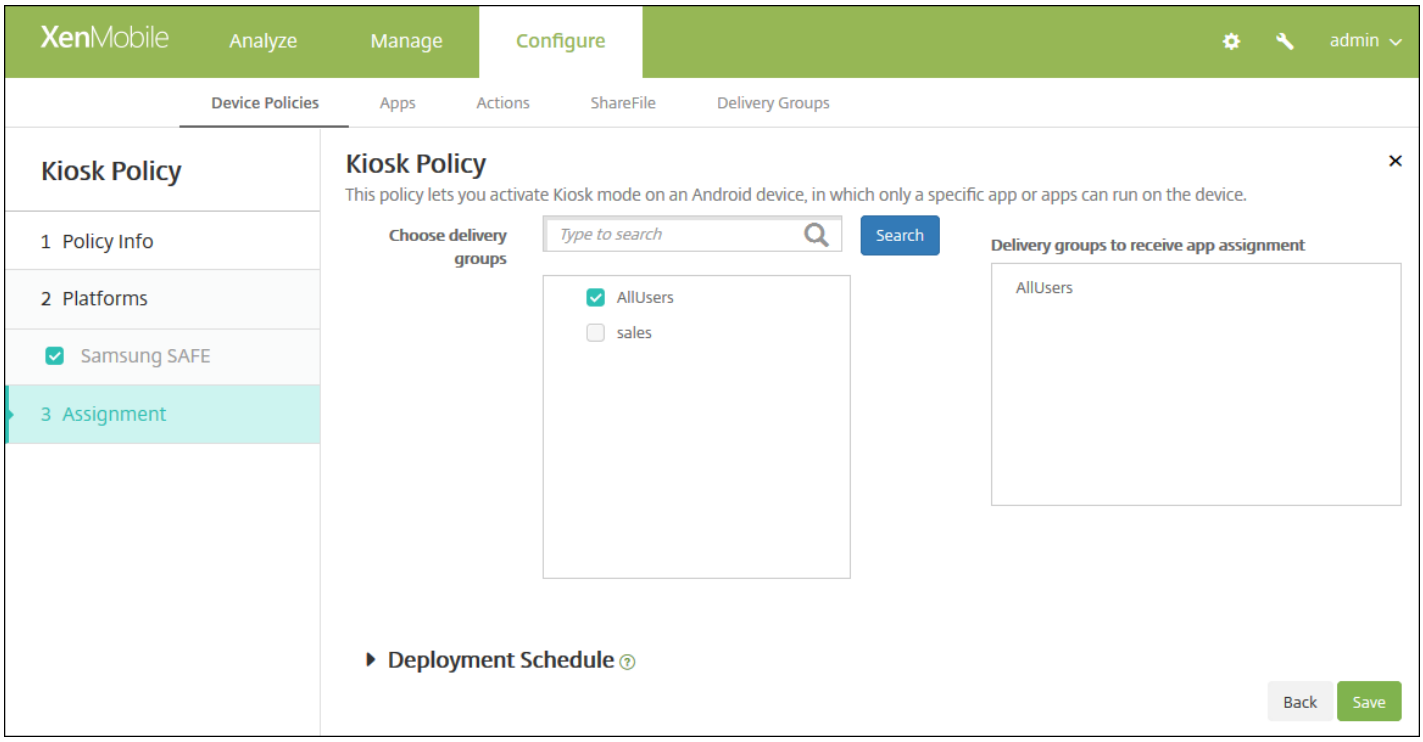
- **允许使用系统栏**：选择是否允许用户在处于 Kiosk 模式时看到系统栏。 默认值为**开**。
- **允许使用任务管理器**：选择是否允许用户在处于 Kiosk 模式时看到和使用任务管理器。 默认值为**开**。
- **通用 SAFE 通行码**：如果您为所有 Samsung SAFE 设备设置了一个通用通行码策略，请在此字段中输入该可选通行码。
- **墙纸**
  - **定义主页墙纸**：选择是否允许用户在处于 Kiosk 模式时为主屏幕使用自定义图片。 默认值为**关**。
    - **主页图片**：启用**定义主页墙纸**时，单击**浏览**并导航到图片文件的位置，选择此文件。
  - **定义锁定墙纸**：选择是否允许用户在处于 Kiosk 模式时为锁定屏幕使用自定义图片。 默认值为**关**。 仅适用于 MDM 4.0 及更高版本。
    - **锁屏图片**：启用**定义锁屏墙纸**时，单击**浏览**并导航到图片文件的位置，选择此文件。
- **应用程序**：对于要添加到 Kiosk 模式的每个应用程序，请单击**添加**，然后执行以下操作：
  - **新建要添加的应用程序**：输入要添加的应用程序的完整名称。 例如，com.android.calendar 允许用户使用 Android 日历应用程序。
  - 单击**保存**以添加应用程序，或单击**取消**以取消添加应用程序。

    注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

    要编辑现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Kiosk 策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

LDAP 设备策略

Aug 11, 2016

可以在 XenMobile 中为 iOS 设备创建 LDAP 策略，以提供与要使用的 LDAP 服务器有关的信息，包括任何必要的帐户信息。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。

配置此策略之前，您需要提供 LDAP 主机名。

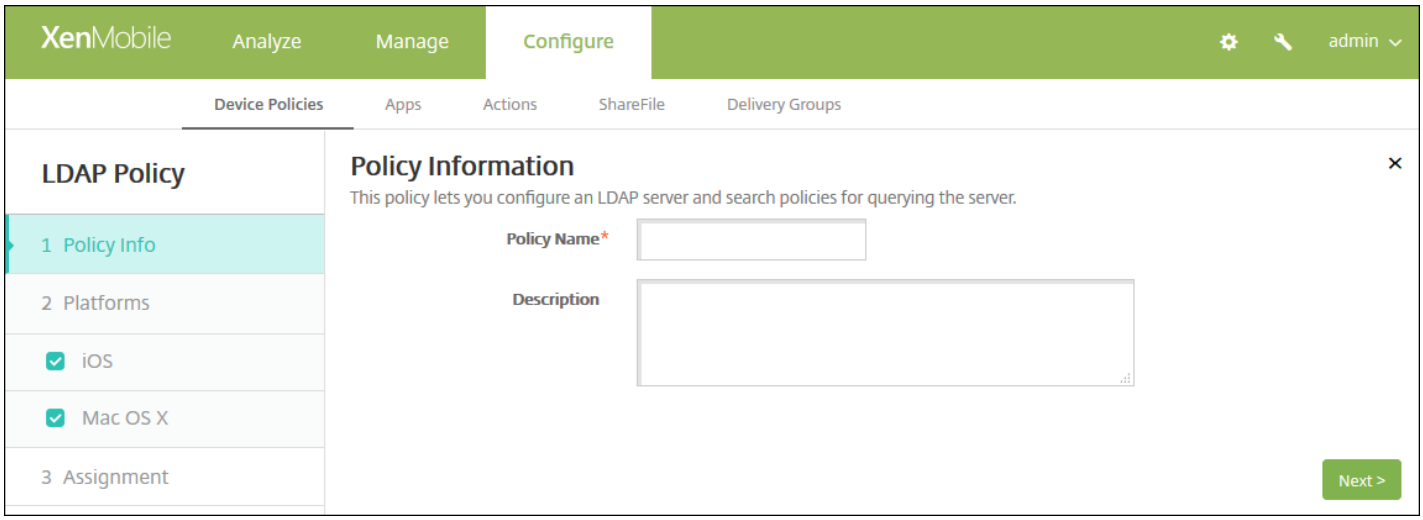
iOS 设置

Mac OS X 设置

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**添加新策略。 此时将显示**添加新策略**对话框。

3. 展开**更多**，然后在**最终用户**下面，单击 **LDAP**。 此时将显示 **LDAP 策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

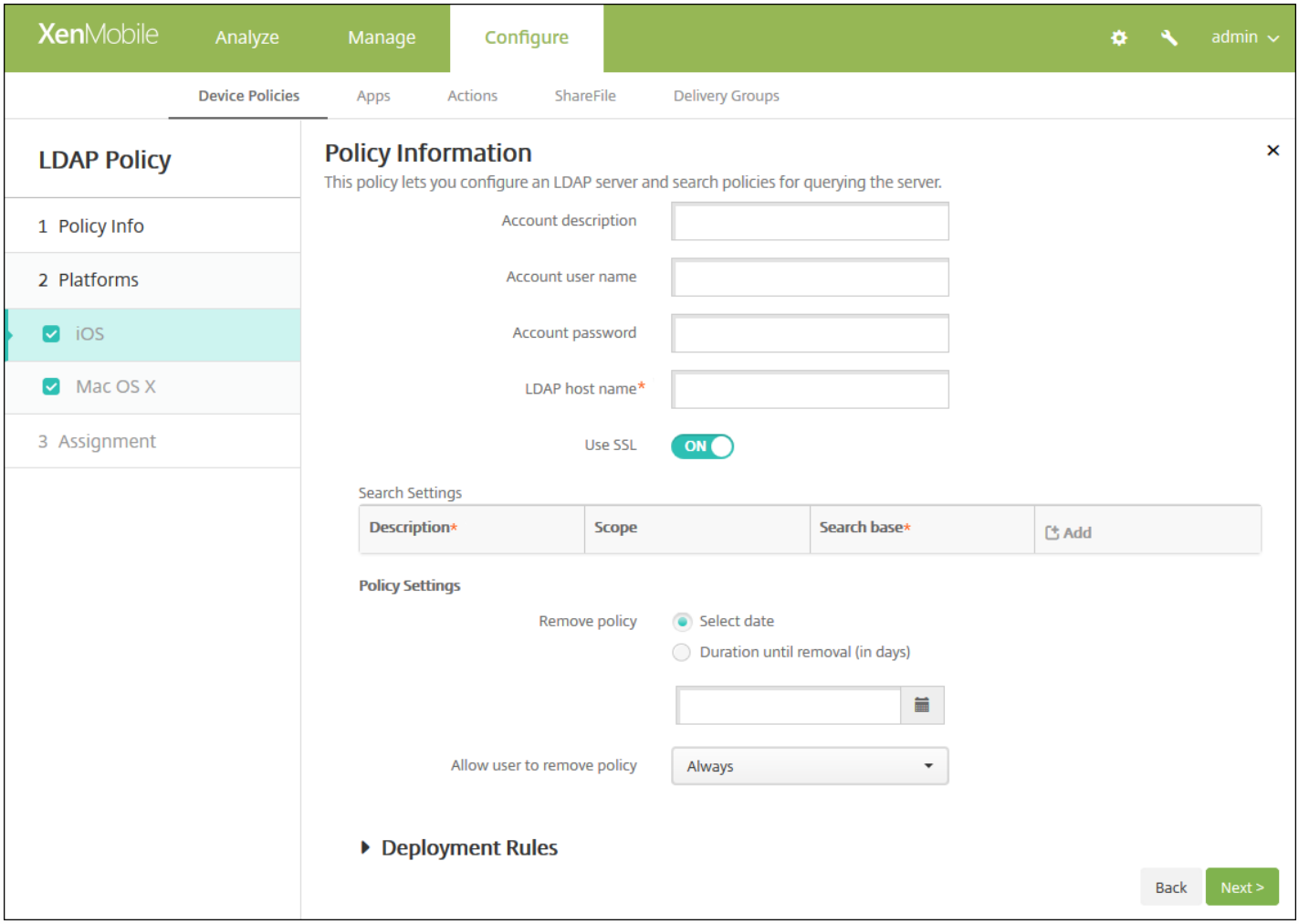
5. 单击**下一步**。 此时将显示**策略平台**信息页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **帐户说明**：输入可选帐户说明。
- **帐户用户名**：输入可选用户名。
- **帐户密码**：输入可选密码。 此选项仅适用于加密的配置文件。
- **LDAP 主机名**：输入 LDAP 服务器的主机名。 此字段为必填字段。
- **使用 SSL**：选择是否使用安全套接字层连接到 LDAP 服务器。 默认值为**开**。
- **搜索设置**：添加查询 LDAP 服务器时要使用的搜索设置。 可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。 单击**添加**，然后执行以下操作：
  - **说明**：输入搜索设置的说明。 此字段为必填字段。
  - **范围**：在列表中，单击**基础**、**一级**或**子树**以定义要搜索的 LDAP 树的深度。 默认值为基础。
    - 范围搜索搜索基础指向的节点。
    - 一级搜索范围节点及其下一级节点。
    - 子树搜索范围节点及其所有子节点，而无论深度为何。
  - **搜索基础**：输入开始搜索时所在节点的路径。 例如 ou=people 或 0=example corp。 此字段为必填字段。
  - 单击**保存**添加搜索设置，或单击“取消”以取消添加搜索设置。
  - 为要添加的每个搜索设置重复执行这些步骤。

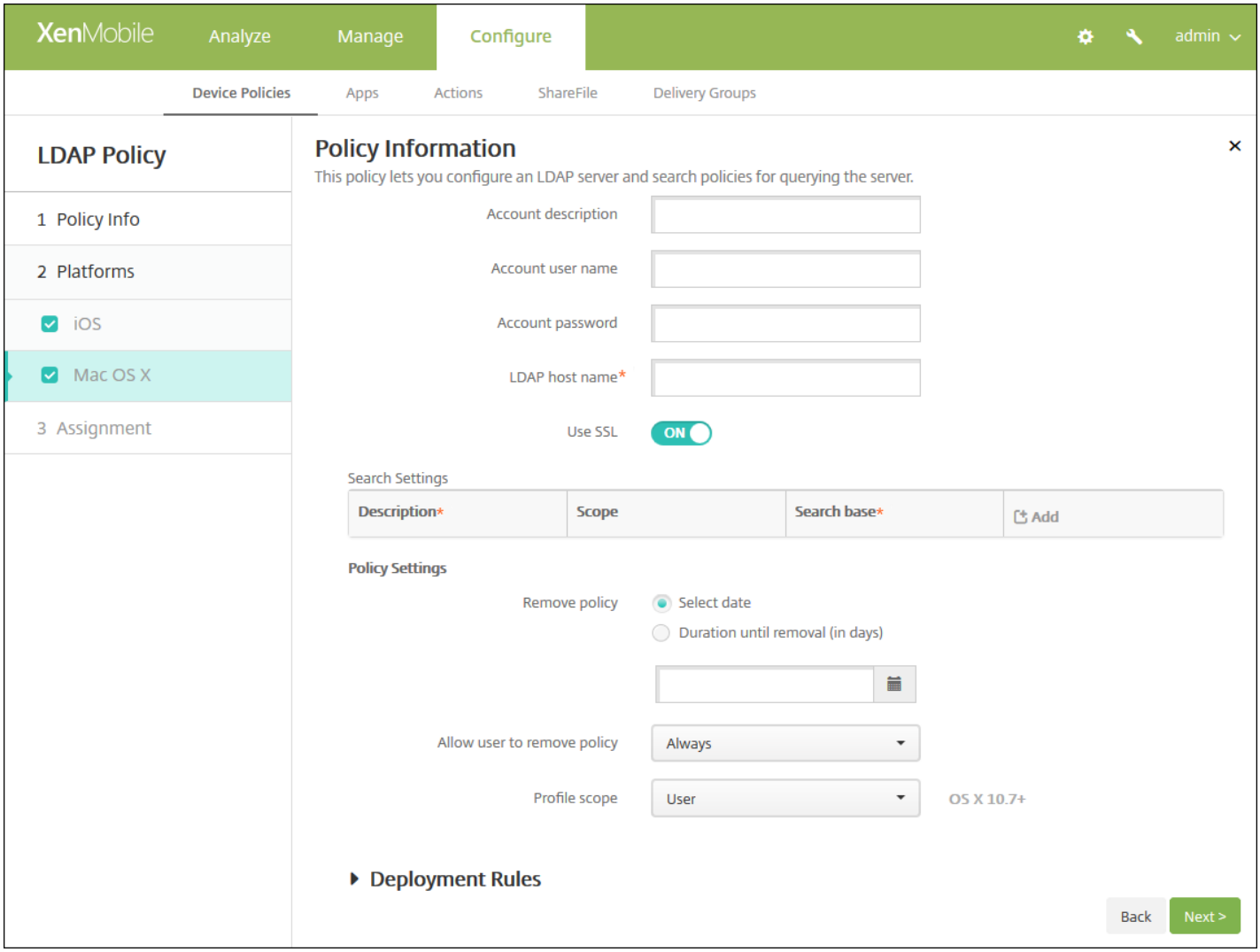
> **注意**：要删除现有搜索设置，请将鼠标悬停在包含列表的行上方，然后单击右侧的垃圾桶图标。 此时将显示确认对话框。 单击删除以删除列表，或单击取消以保留此列表。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

要编辑现有搜索设置，请将鼠标悬停在包含列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

- 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
- 如果单击**选择日期**，请单击日历以选择具体删除日期。
- 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
- 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置



配置以下设置：

- **帐户说明**：输入可选帐户说明。
- **帐户 用户名**：输入可选用户名。
- **帐户密码**：输入可选密码。 此选项仅适用于加密的配置文件。
- **LDAP 主机名**：输入 LDAP 服务器的主机名。 此字段为必填字段。
- **使用 SSL**：选择是否使用安全套接字层连接到 LDAP 服务器。 默认值为**开**。
- **搜索设置**：添加查询 LDAP 服务器时要使用的搜索设置。 可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。 单击**添加**，然后执行以下操作：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **说明**：输入搜索设置的说明。 此字段为必填字段。
- **范围**：在列表中，单击**基础**、**一级**或**子树**以定义要搜索的 LDAP 树的深度。 默认值为基础。
  - 范围搜索搜索基础指向的节点。
  - 一级搜索范围节点及其下一级节点。
  - 子树搜索范围节点及其所有子节点，而无论深度为何。
- **搜索基础**：输入开始搜索时所在节点的路径。 例如 ou=people 或 0=example corp。 此字段为必填字段。
- 单击**保存**添加搜索设置，或单击“取消”以取消添加搜索设置。
- 为要添加的每个搜索设置重复执行这些步骤。

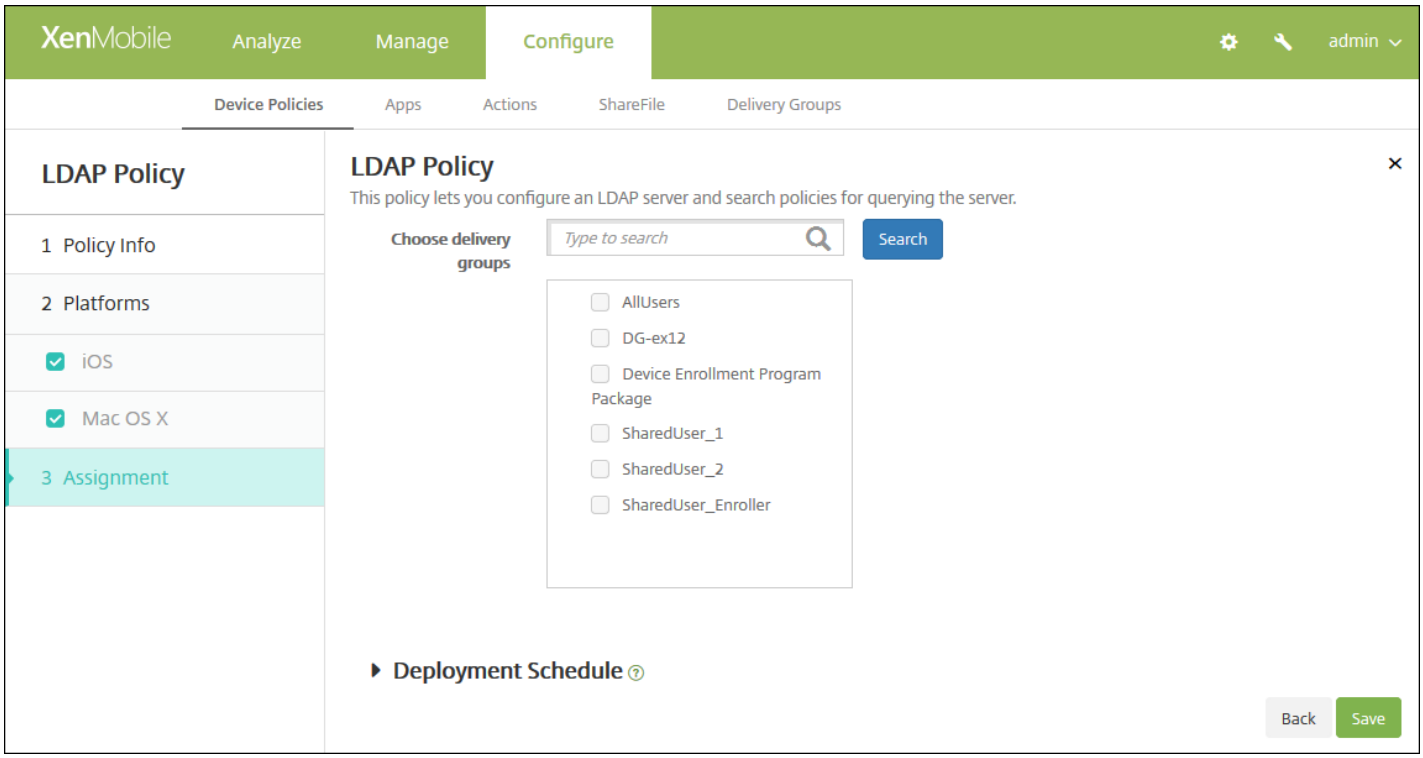
  注意：要删除现有搜索设置，请将鼠标悬停在包含列表的行上方，然后单击右侧的垃圾桶图标。 此时将显示确认对话框。 单击删除以删除列表，或单击取消以保留此列表。

  要编辑现有搜索设置，请将鼠标悬停在包含列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

- 在**策略设置**下面，**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
- 如果单击**选择日期**，请单击日历以选择具体删除日期。
- 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
- 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
- 在**配置文件作用域**中，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **LDAP 策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

定位设备策略

Aug 11, 2016

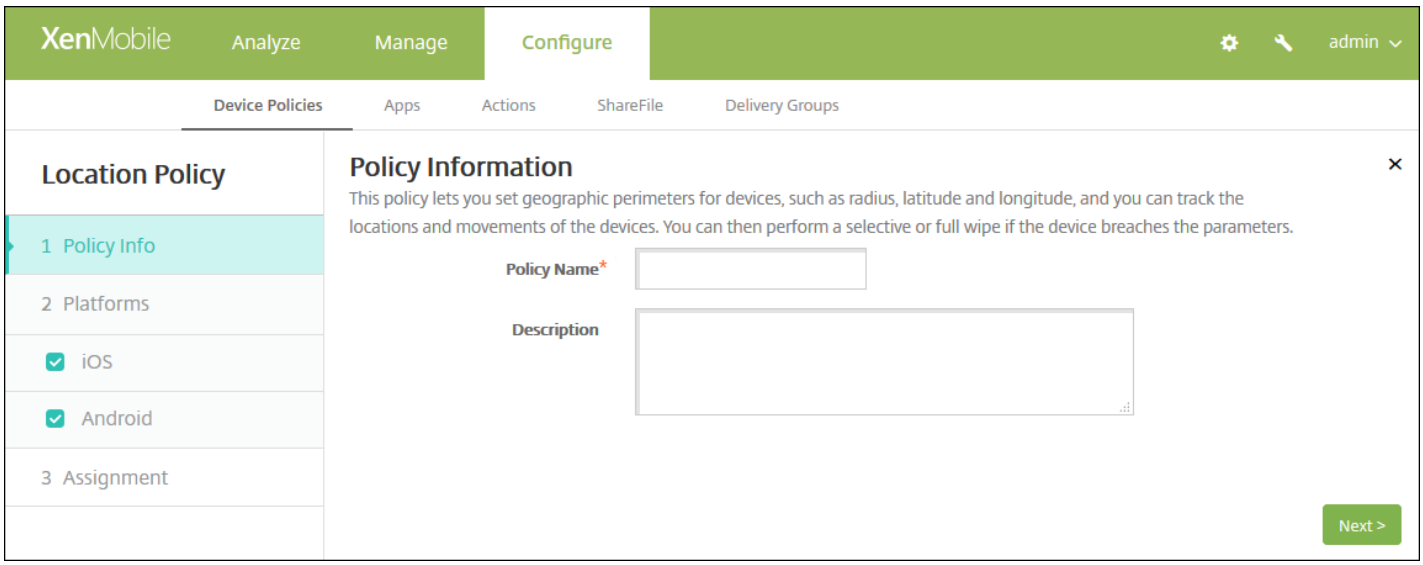
可以在 XenMobile 中创建定位设备策略以强制遵从地理边界以及跟踪用户设备的位置和移动情况。 用户超出定义的边界（又称*地理围栏*）时，XenMobile 可以立即执行选择性擦除或完全擦除，或者在特定时间段后执行擦除，以允许用户返回到允许的位置。

可以为 iOS 和 Android 创建定位设备策略。 每种平台需要一组不同的值，本文将对此进行介绍。

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. 单击**位置**。 此时将显示 **Location Policy**（定位策略）信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

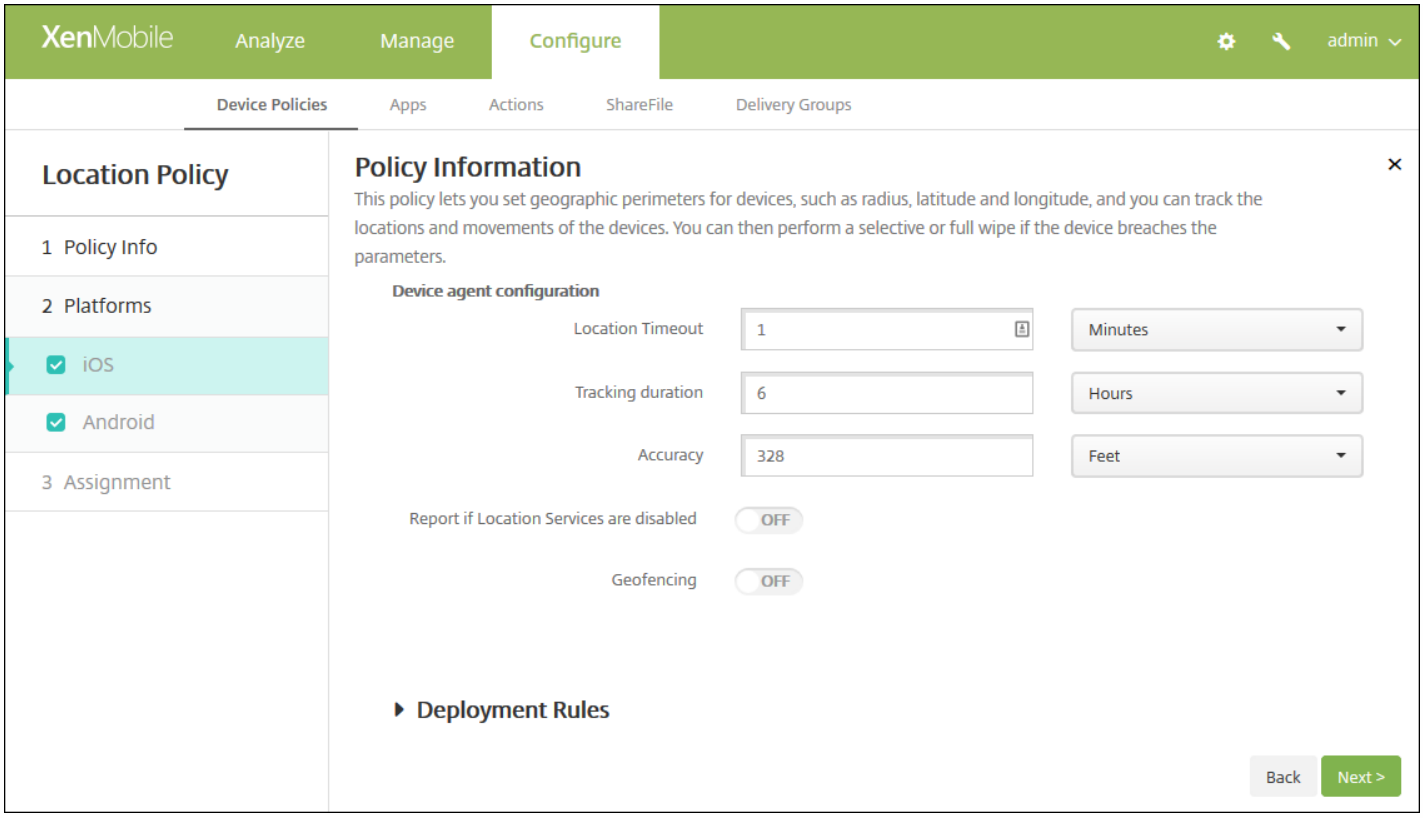
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

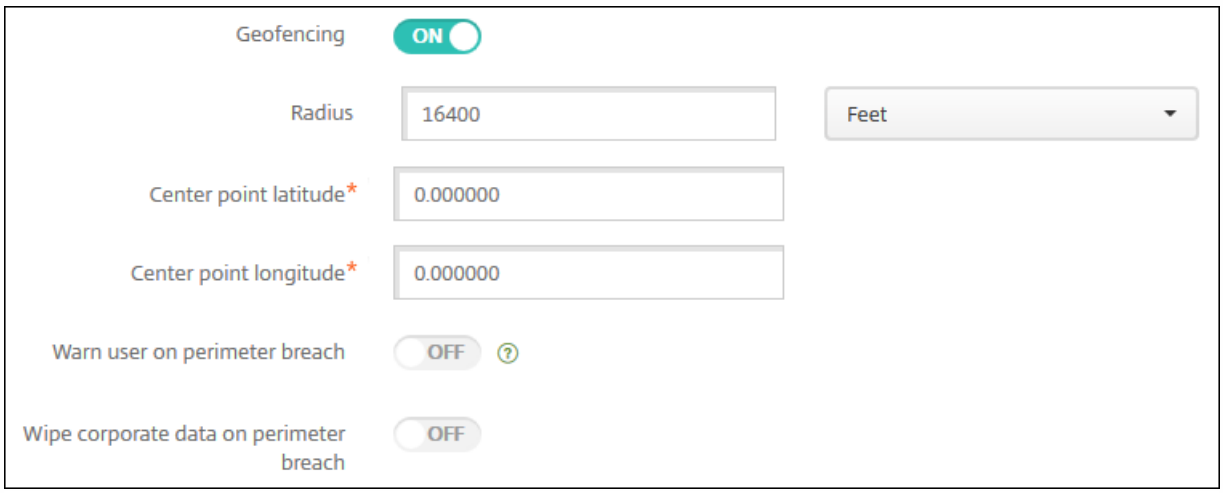
配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **定位超时**：键入数值，然后在列表中单击**秒**或**分钟**以设置 XenMobile 尝试修复设备位置的频率。 有效值为 60–900 秒或 1–15 分钟。 默认值为 1 分钟。
- **跟踪持续时间**：键入数值，然后在列表中单击**小时**或**分钟**以设置 XenMobile 跟踪设备的时间长度。 有效值为 1-6 小时或 10-360 分钟。 默认值为 6 小时。
- **准确度**：键入数值，然后在列表中单击**米**、**英尺**或**码**以设置 XenMobile 跟踪设备的接近程度。 有效值为 10–5000 码或米，或者 30–15000 英尺。 默认值为 328 英尺。
- **禁用定位服务时报告**：选择禁用 GPS 时设备是否向 XenMobile 发送报告。 默认值为**关**。
- **地理围栏**

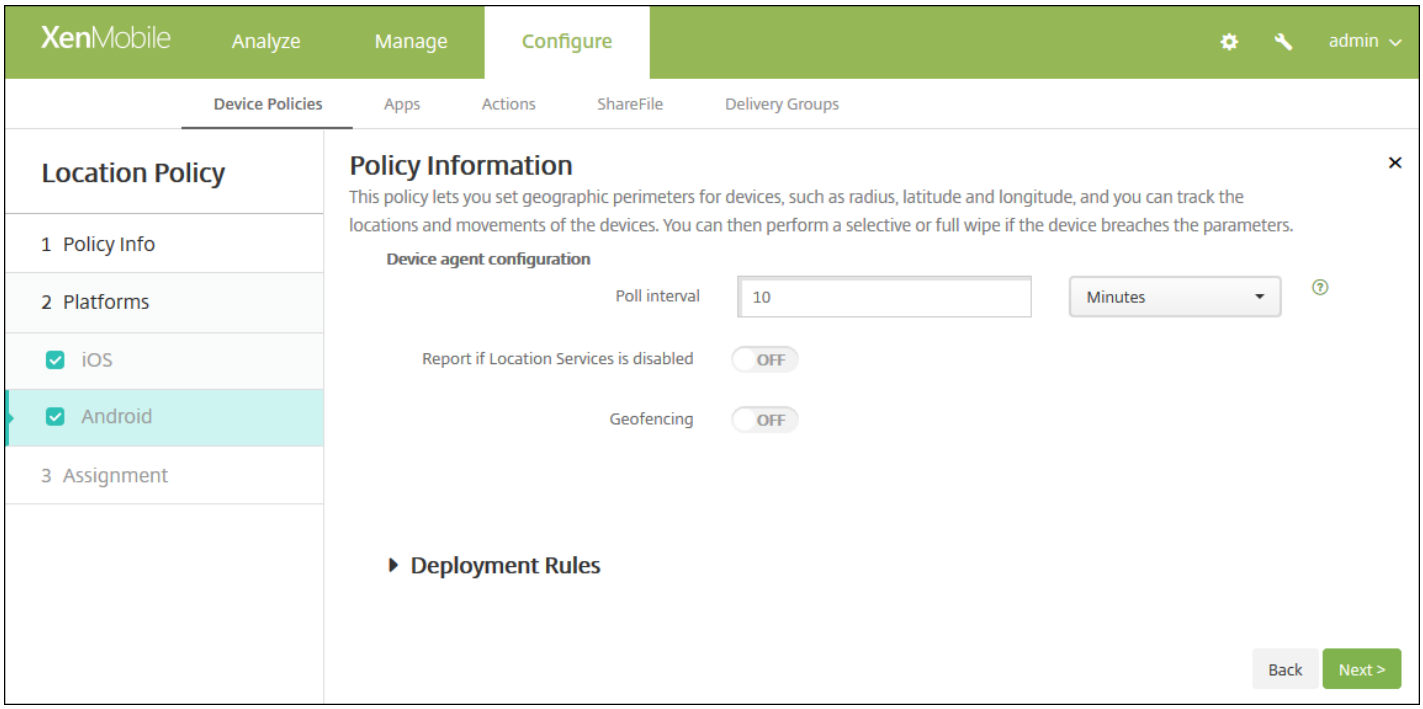


© 1999-2017 Citrix Systems, Inc. All rights reserved.

启用地理围栏时，请配置以下设置：

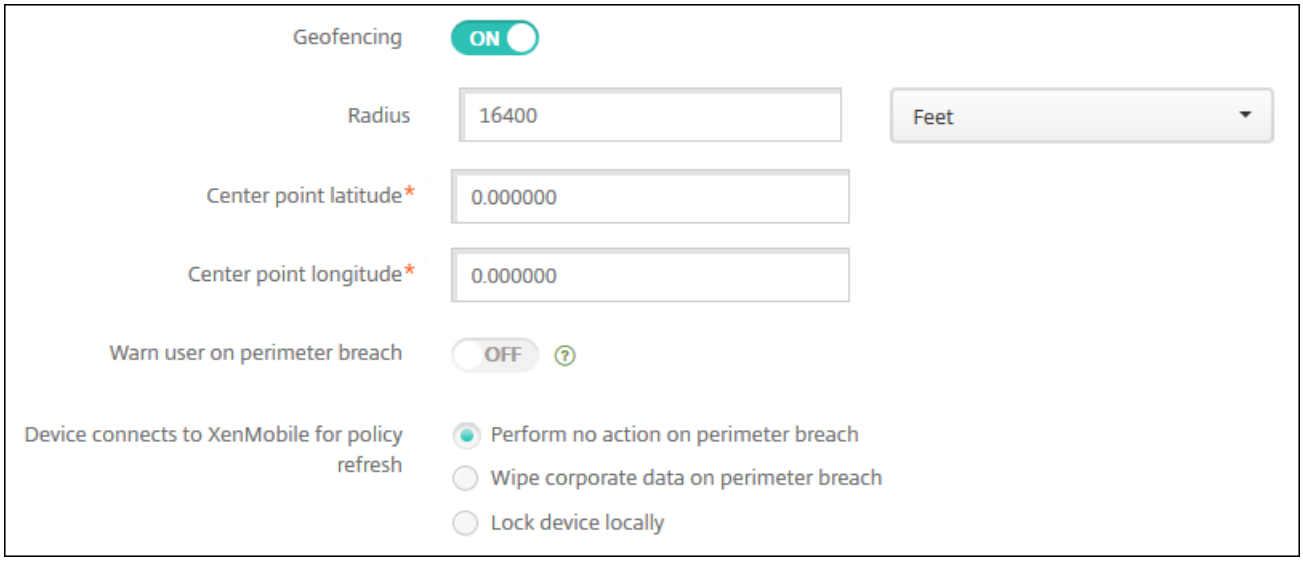
- **半径**：键入数值，然后在列表中，单击要用于衡量半径的单位。 默认值为 16,400 英尺。 半径的有效值如下：
  - 164–164000 英尺
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- **中心点纬度**：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- **中心点经度**：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- **Warn user on perimeter breach**（警告用户超出边界）：选择用户超出定义的边界时是否发出警告消息。 默认值为**关**。 不需要连接到 XenMobile 即可显示警告消息。
- **Wipe corporate data on perimeter breach**（超出边界时擦除企业数据）：选择当用户超出边界时是否擦除用户设备。 默认值为**关**。 启用此选项时，将显示**本地擦除延迟**字段。
  - 键入数值，然后在列表中单击**秒**或**分钟**以设置从用户设备中擦除公司数据之前延迟的时间长度。 这使用户有机会在 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。

配置 Android 设置



- **轮询间隔**：键入数值，然后在列表中单击**分钟**、**小时**或**天**以设置 XenMobile 尝试修复设备位置的频率。 有效值为 1–1440 分钟、1–24 小时或任意天数。 默认值为 10 分钟。 将此值设置为小于 10 分钟可能会对设备的电池寿命产生不利影响。
- **禁用定位服务时报告**：选择禁用 GPS 时设备是否向 XenMobile 发送报告。 默认值为**关**。
- **地理围栏**

© 1999-2017 Citrix Systems, Inc. All rights reserved.



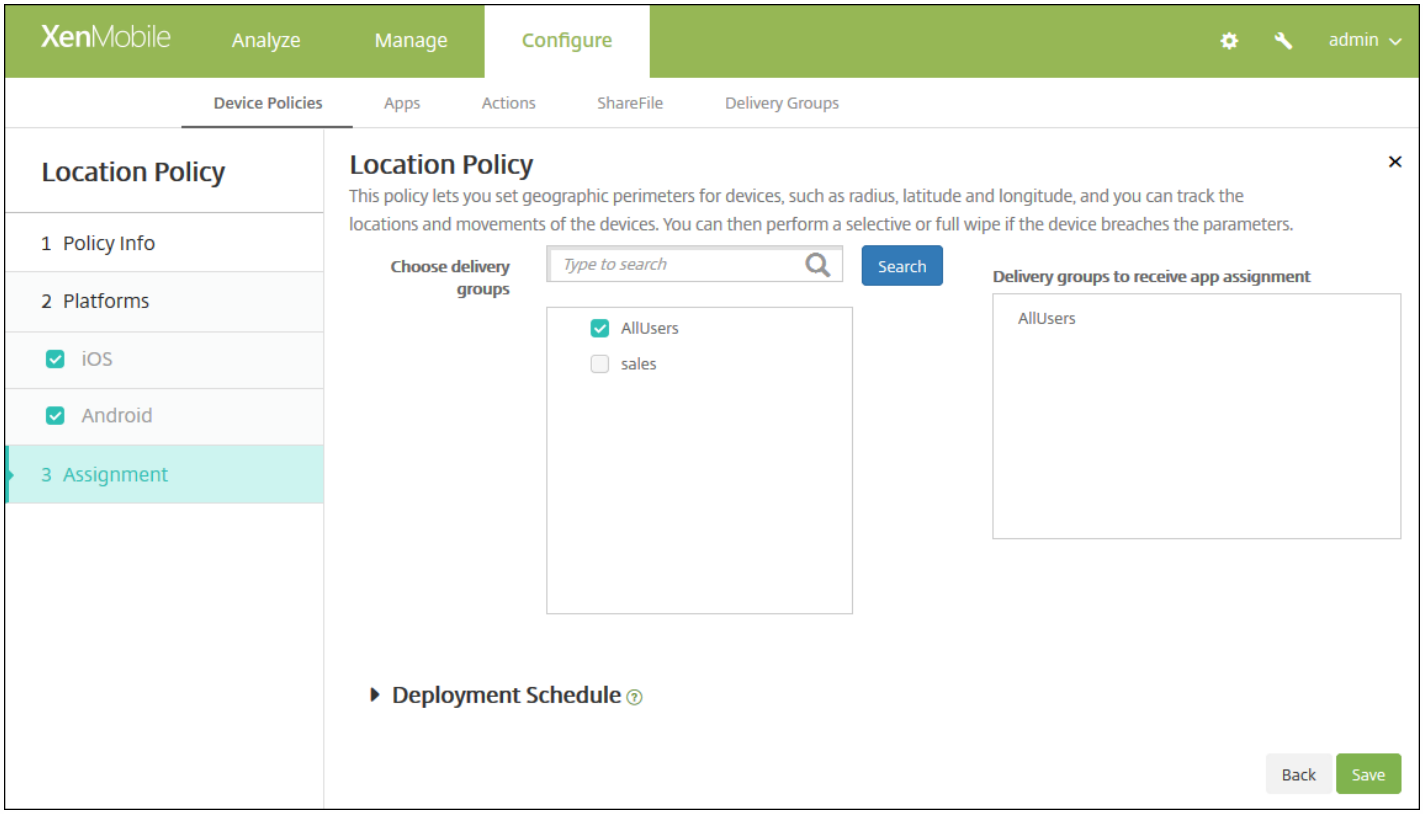
启用地理围栏时，请配置以下设置：

- **半径**：键入数值，然后在列表中，单击要用于衡量半径的单位。 默认值为 16,400 英尺。 半径的有效值如下：
  - 164–164000 英尺
  - 1–50 千米
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- **中心点纬度**：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- **中心点经度**：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- **Warn user on perimeter breach**（警告用户超出边界）：选择用户超出定义的边界时是否发出警告消息。 默认值为**关**。 不需要连接到 XenMobile 即可显示警告消息。
- **Device connects to XenMobile for policy refresh**（设备连接到 XenMobile 以刷新策略）：为用户超出边界时选择以下选项之一：
  - **Perform no action on perimeter breach**（超出边界时不执行任何操作）：不执行任何操作。 这是默认值。
  - **Wipe corporate data on perimeter breach**（超出边界时擦除公司数据）：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。
    - 键入数值，然后在列表中单击秒或分钟以设置从用户设备中擦除公司数据之前延迟的时间长度。 这使用户有机会在 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**：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。
    - 键入数值，然后在列表中单击秒或分钟以设置锁定用户设备之前延迟的时间长度。 这使用户有机会在 XenMobile 锁定其设备之前返回到允许的位置。 默认值为 0 秒。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**定位策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

邮件设备策略

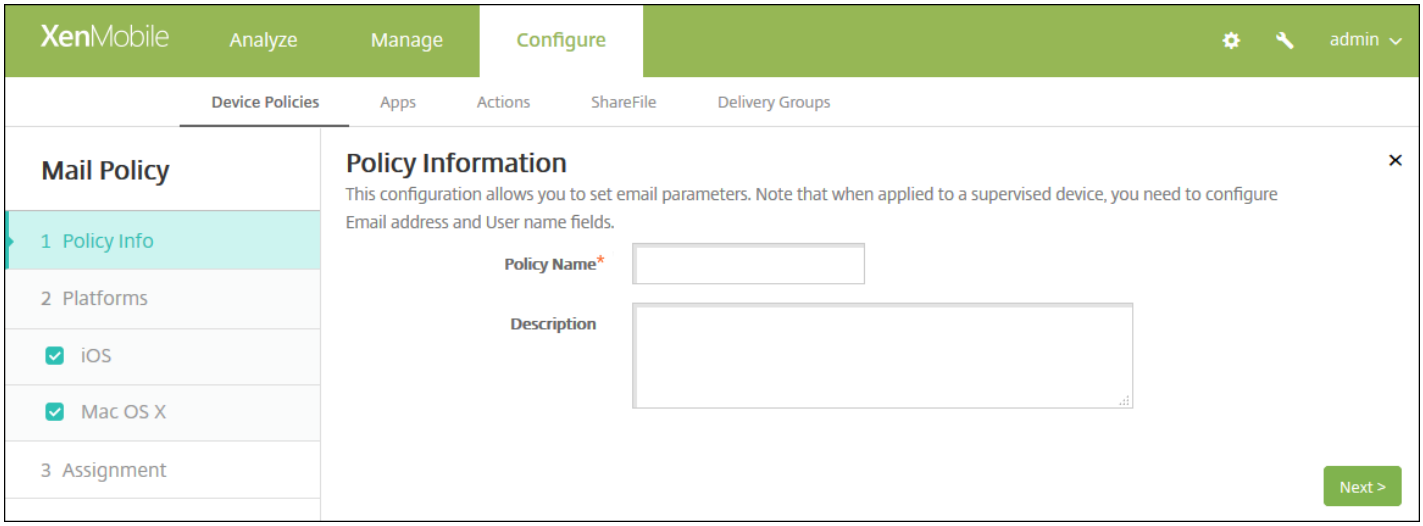
Aug 11, 2016

可以在 XenMobile 中添加邮件设备策略以在用户的 iOS 或 Mac OX X 设备上配置电子邮件帐户。

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**添加新策略。 此时将显示**添加新策略**对话框。

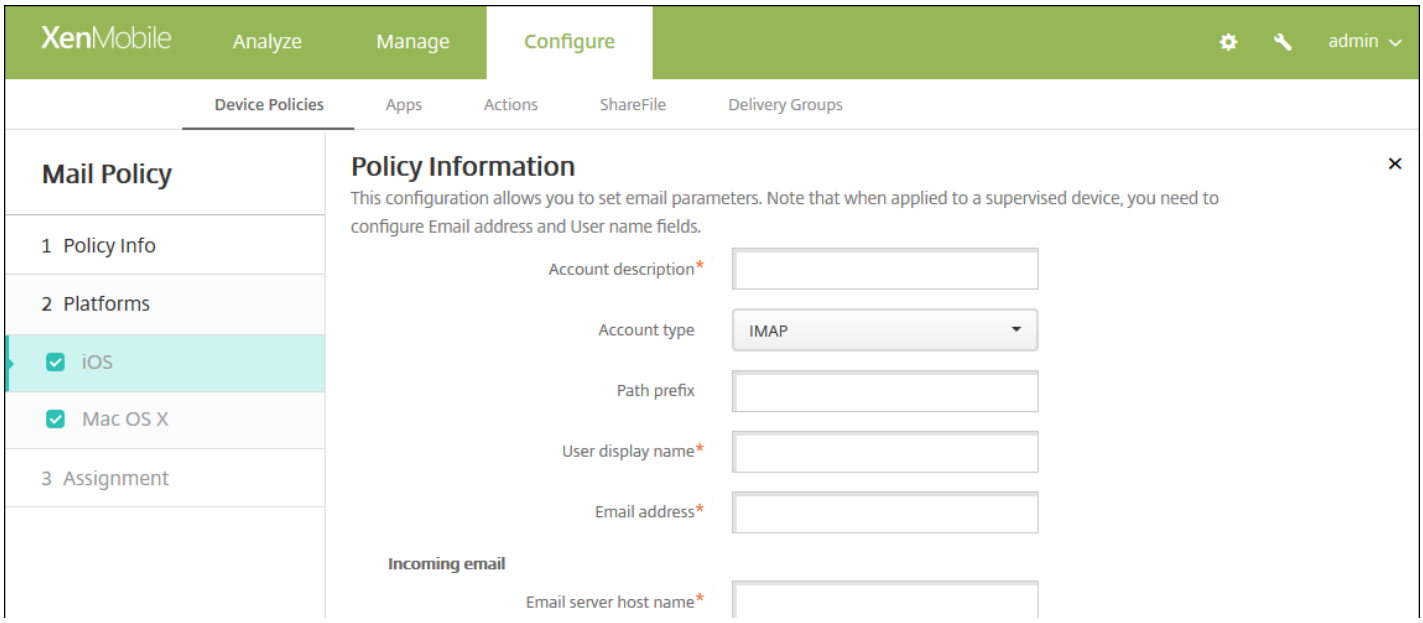
3. 单击**更多**，然后在**最终用户**下，单击**邮件**。 此时将显示**邮件策略**页面。



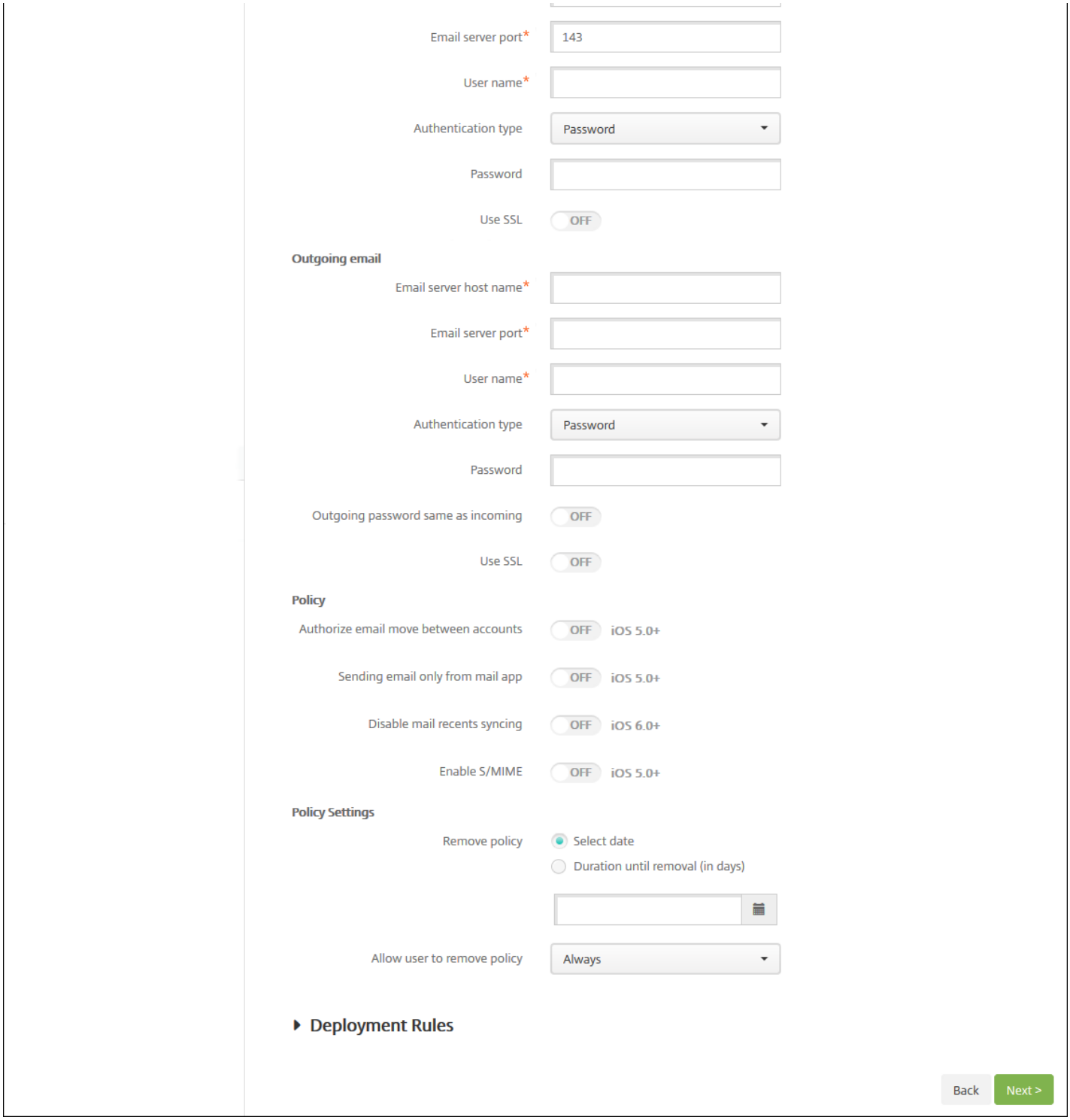
4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示**邮件策略平台**页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 8 以了解如何设置此平台的部署规则。

7. 为选择的平台配置以下设置。

- **帐户说明**：键入在“邮件”和“设置”应用程序中显示的帐户说明。 此字段为必填字段。
- **帐户类型**：在列表中，单击 **IMAP** 或 **POP** 以选择要对用户帐户使用的协议。 默认值为 **IMAP**。 选择 **POP** 时，以下**路径前缀**选项将消失。

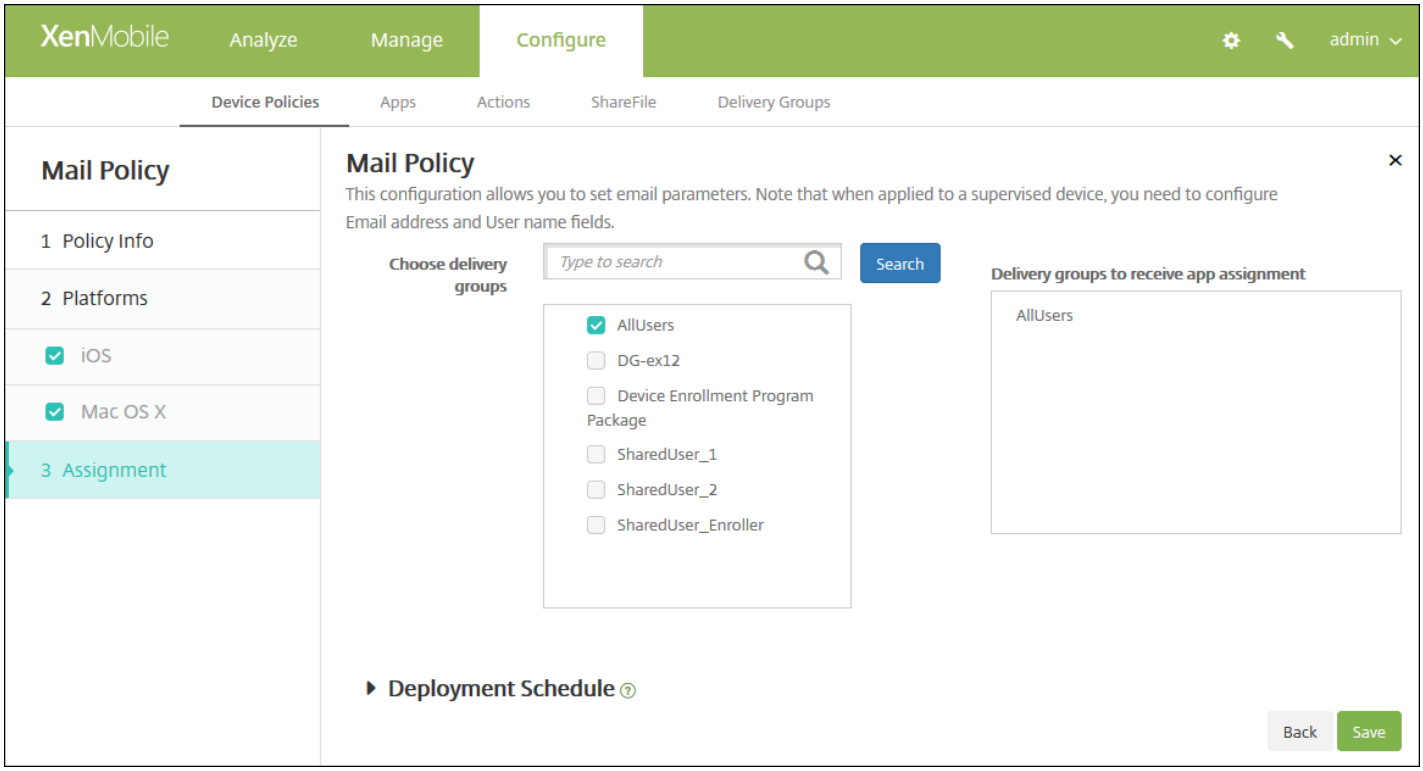
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **路径前缀**：键入 **INBOX** 或您的 IMAP 邮件帐户路径前缀（如果不是 **INBOX**）。 此字段为必填字段。
- **用户显示名称**：键入用于邮件等内容的完整 用户名 。 此字段为必填字段。
- **电子邮件地址**：键入帐户的完整电子邮件地址。 此字段为必填字段。
- **传入电子邮件设置**
  - **电子邮件服务器主机名**：键入传入电子邮件服务器主机名或 IP 地址。 此字段为必填字段。
  - **电子邮件服务器端口**：键入传入邮件服务器端口号。 默认值为 **143**。 此字段为必填字段。
  - **用户名**：键入电子邮件帐户的 用户名 。 此名称通常与用户的电子邮件地址中 @ 字符前面的部分相同。 此字段为必填字段。
  - **身份验证类型**：在列表中，单击以选择要使用的身份验证类型。 默认值为**密码**。 选中**无**时，以下**密码**字段将消失。
  - **密码**：键入传入邮件服务器的可选密码。
  - **使用 SSL**：选择传入邮件服务器是否使用安全套接字层身份验证。 默认值为**关**。
- **传出电子邮件设置**
  - **电子邮件服务器主机名**：输入传出邮件服务器主机名或 IP 地址。 此字段为必填字段。
  - **电子邮件服务器端口**：键入传出邮件服务器端口号。 如果未输入端口号，将使用指定协议的默认端口。
  - **用户名**：键入电子邮件帐户的 用户名 。 此名称通常与用户的电子邮件地址中 @ 字符前面的部分相同。 此字段为必填字段。
  - **身份验证类型**：在列表中，单击以选择要使用的身份验证类型。 默认值为**密码**。 选中**无**时，以下**密码**字段将消失。
  - **密码**：键入传出邮件服务器的可选密码。
  - **传出密码和传入密码相同**：选择传入和传出密码是否相同。 默认值为关，表示密码不相同。 设置为**开**时，上述**密码**字段将消失。
  - **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**
  - **注意**：配置 iOS 设置时，这些选项仅适用于 iOS 5.0 及更高版本；配置 Mac OS X 时无限制。
  - **授权电子邮件在帐户之间移动**：选择是否允许用户将 电子邮件 从此帐户移出到另一个帐户以及从不同帐户进行转发和回复。 默认值为**关**。
  - **只从邮件应用程序发送电子邮件**：选择是否将用户限制为从 iOS 邮件应用程序发送 电子邮件。
  - **禁用 最新 邮件同步**：选择是否阻止用户同步最近使用的地址。 默认值为**关**。 此选项仅适用于 iOS 6.0 及更高版本。
  - **启用 S/MIME**：选择此帐户是否支持 S/MIME 身份验证和加密。 默认值为**关**。 设置为开时，将显示以下两个字段。
  - **签署身份凭据**：在列表中，选择要使用的签名凭据。
  - **加密身份凭据**：在列表中，选择要使用的加密凭据。
- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边：在列表中，单击**用户**或**系统**。 默认值为**用户**。 此选项仅在 Mac OS X 10.7 及更高版本上可用。

8. 配置部署规则

9. 单击**下一步**。 此时将显示**邮件策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



10. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

11. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

12. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

托管域设备策略

Aug 11, 2016

可以定义应用到电子邮件和 Safari 浏览器的托管域。 托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护企业数据。 指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。 此策略仅在 iOS 8 及更高版本的受监督设备上可用。 有关将 iOS 设备置于受监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

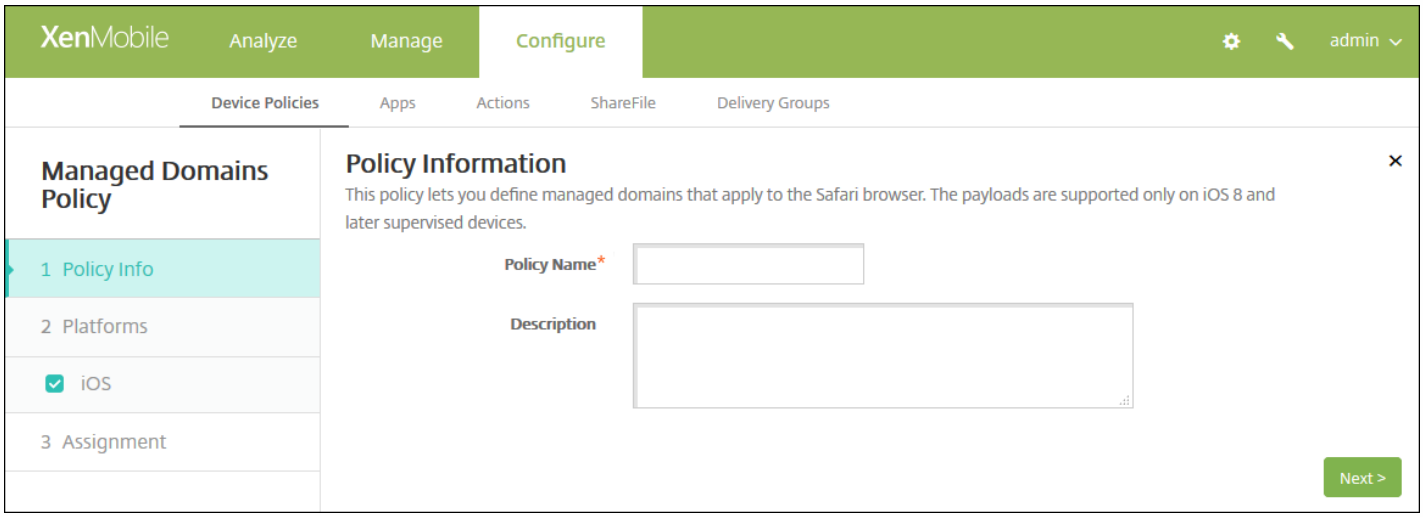
用户向域不在托管电子邮件域列表上的收件人发送电子邮件时，在用户的设备上此邮件将带有标记，以警告用户正在向企业域外部的人员发送邮件。

当用户尝试使用 Safari 从位于托管 Web 域列表上的 Web 域打开某个项目（文档、附件或下载内容）时，将由合适的企业应用程序打开此项目。 如果此项目所在的 Web 域不在托管 Web 域列表上，用户无法使用合适的企业应用程序打开此项目；他们必须使用未托管的个人应用程序。

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**下面，单击**托管域**。 将显示**托管域策略**信息页面。

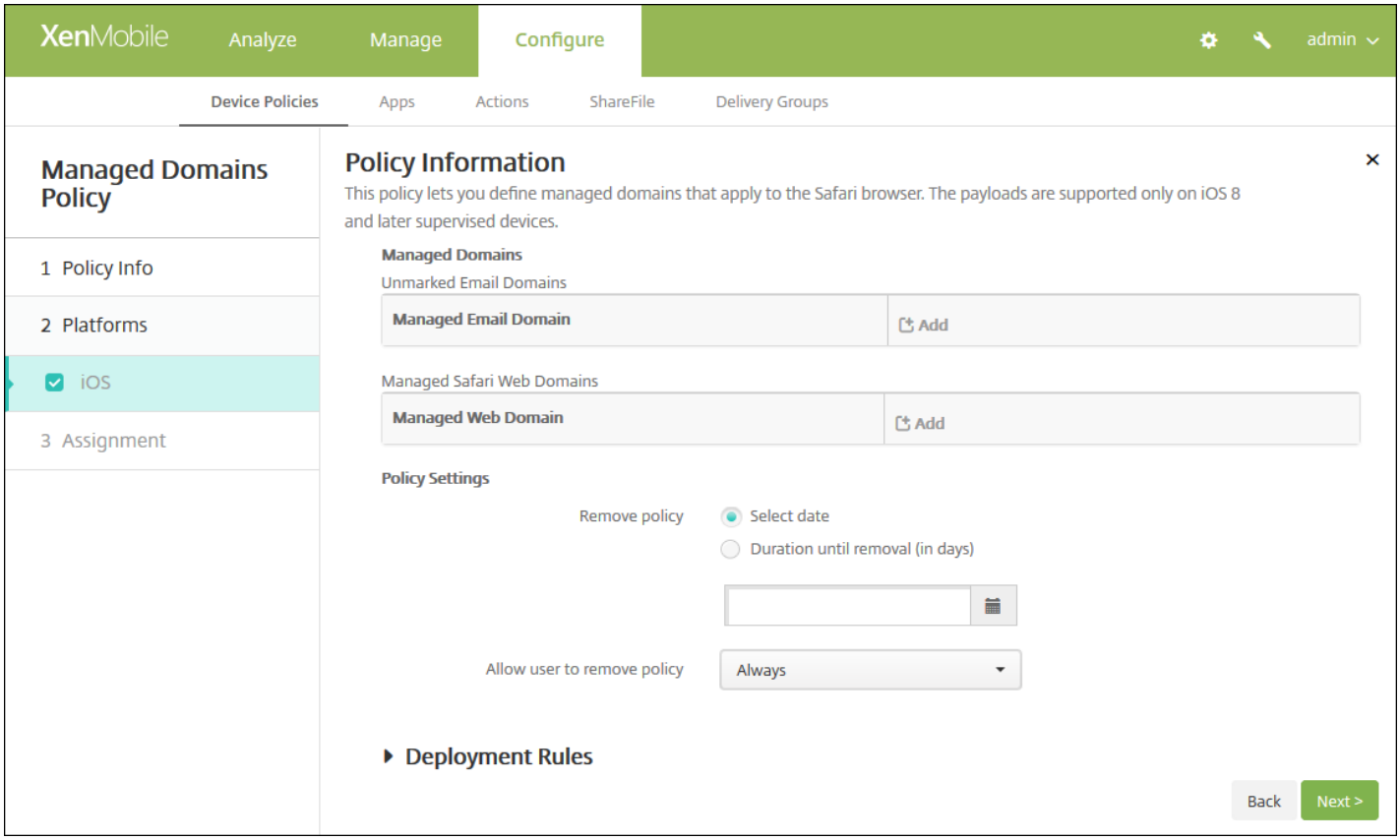


4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **iOS 平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



如何指定域

6. 配置以下设置：

- **托管域**
  - **取消标记电子邮件域**：对于要包含在列表中的每个电子邮件域，请单击**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，或者单击**取消**不保存电子邮件域。
  - **托管 Safari Web 域**：对于要包含在列表中的每个 Web 域，请单击**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，或者单击**取消**不保存 Web 域。

      注意：要删除现有域，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

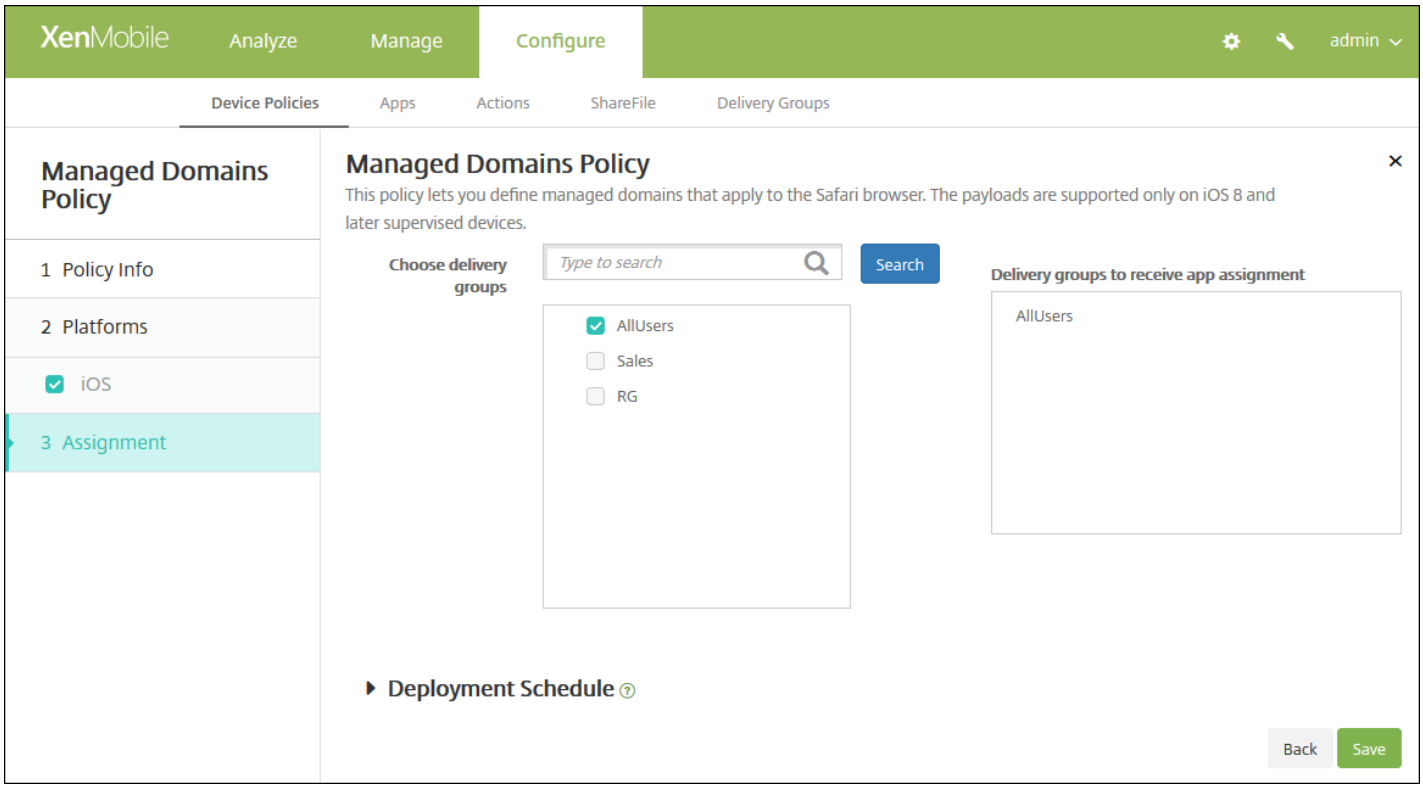
      要编辑现有域，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **策略设置**
  - 在**策略设置**下面，**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

7. 配置部署规则

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 单击**下一步**。 此时将显示**托管域策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择关，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为关。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

MDM 选项设备策略

Aug 11, 2016

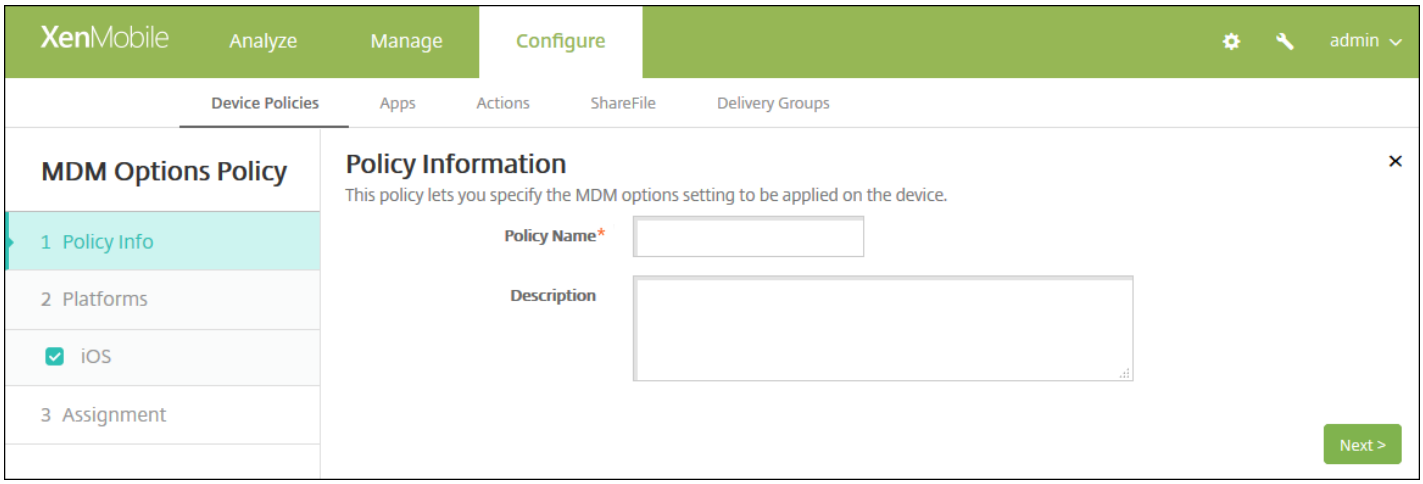
可以在 XenMobile 中创建一个设备策略，用于在受监督的 iOS 7.0 及更高版本的手机设备上管理“查找我的 iPhone/iPad 激活锁”。 有关将 iOS 设备置于受监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式或 iOS 批量注册。

激活锁是一项“查找我的 iPhone/iPad”功能，目的是在任何人都可以关闭“查找我的 iPhone”、擦除设备或重新激活并使用设备之前，通过要求提供用户的 Apple ID 和密码阻止重新激活丢失或失窃的设备。 在 XenMobile 中，可以通过在 MDM 选项设备策略中启用激活锁，绕过 Apple ID 和密码要求。 当用户返回已启用“查找我的 iPhone”功能的设备时，您无需具有其 Apple 凭据便可以从 XenMobile 控制台管理此设备。

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**最终用户**下面，单击 **MDM 选项**。 此时将显示 **MDM 选项策略**信息页面。

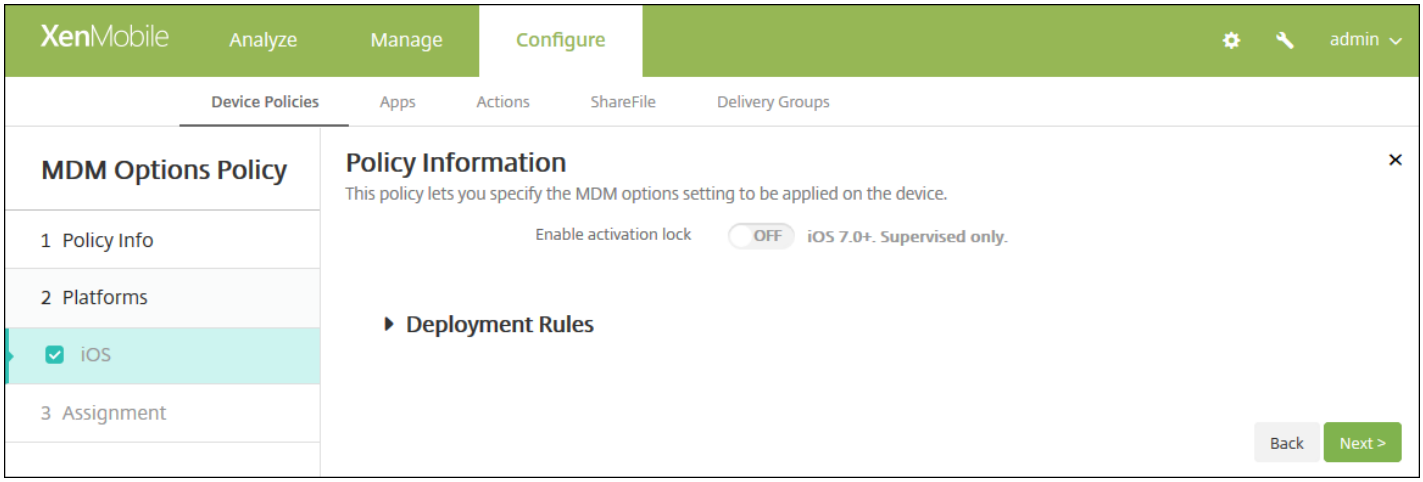


4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **iOS MDM 策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

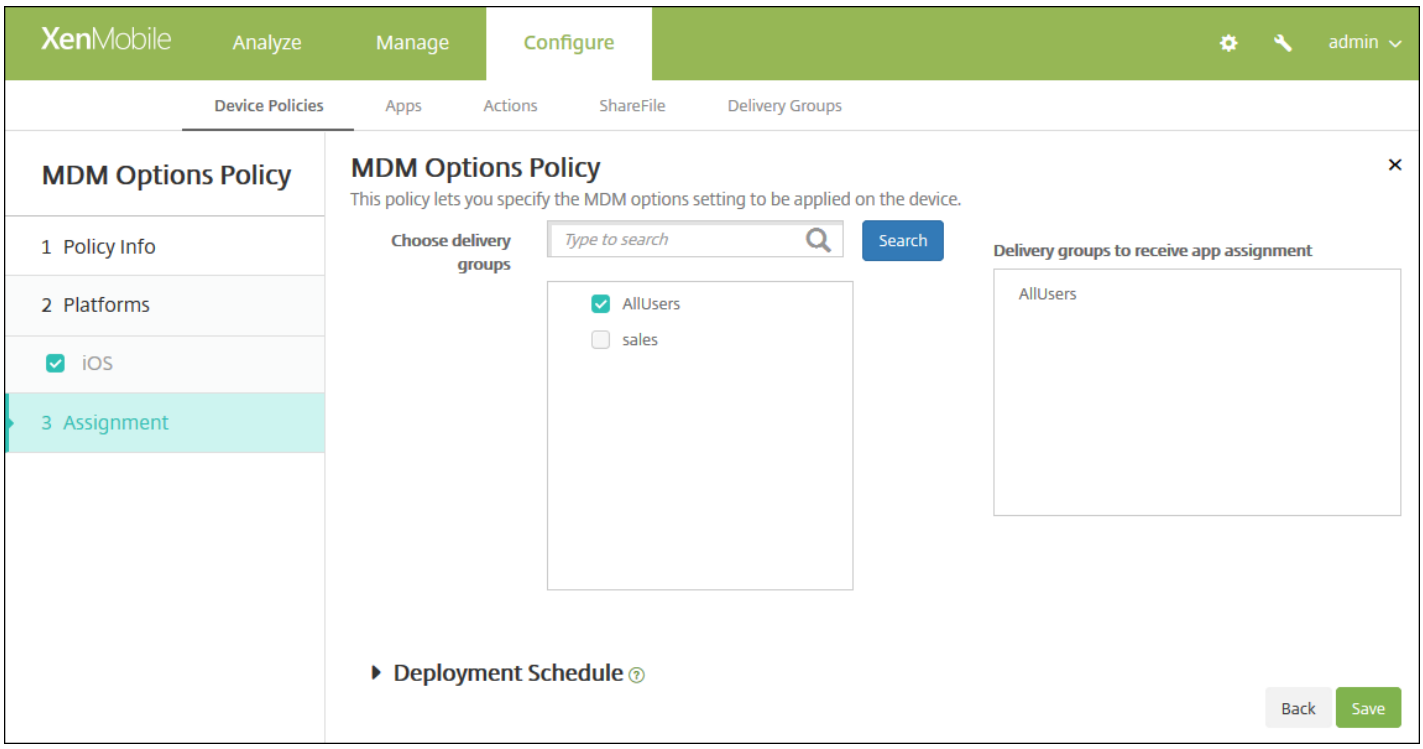


6. 配置以下设置：

- **启用激活锁**：选择是否要在部署此策略的设备上启用激活锁。 默认值为**关**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **MDM Options Policy**（XenMobile 选项策略）分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 如果单击**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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Exchange ActiveSync 设备策略

Aug 11, 2016

可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以允许其访问 Exchange 上托管的企业电子邮件。 可以为 iOS、Mac OS X、Android HTC、Android TouchDown、Android for Work、Samsung SAFE、Samsung KNOX 和 Windows Phone 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说明。

iOS 设置

Mac OS X 设置

Android HTC 设置

Android TouchDown 设置

Android for Work 设置

Samsung SAFE 和 Samsung KNOX 设置

Windows Phone 设置

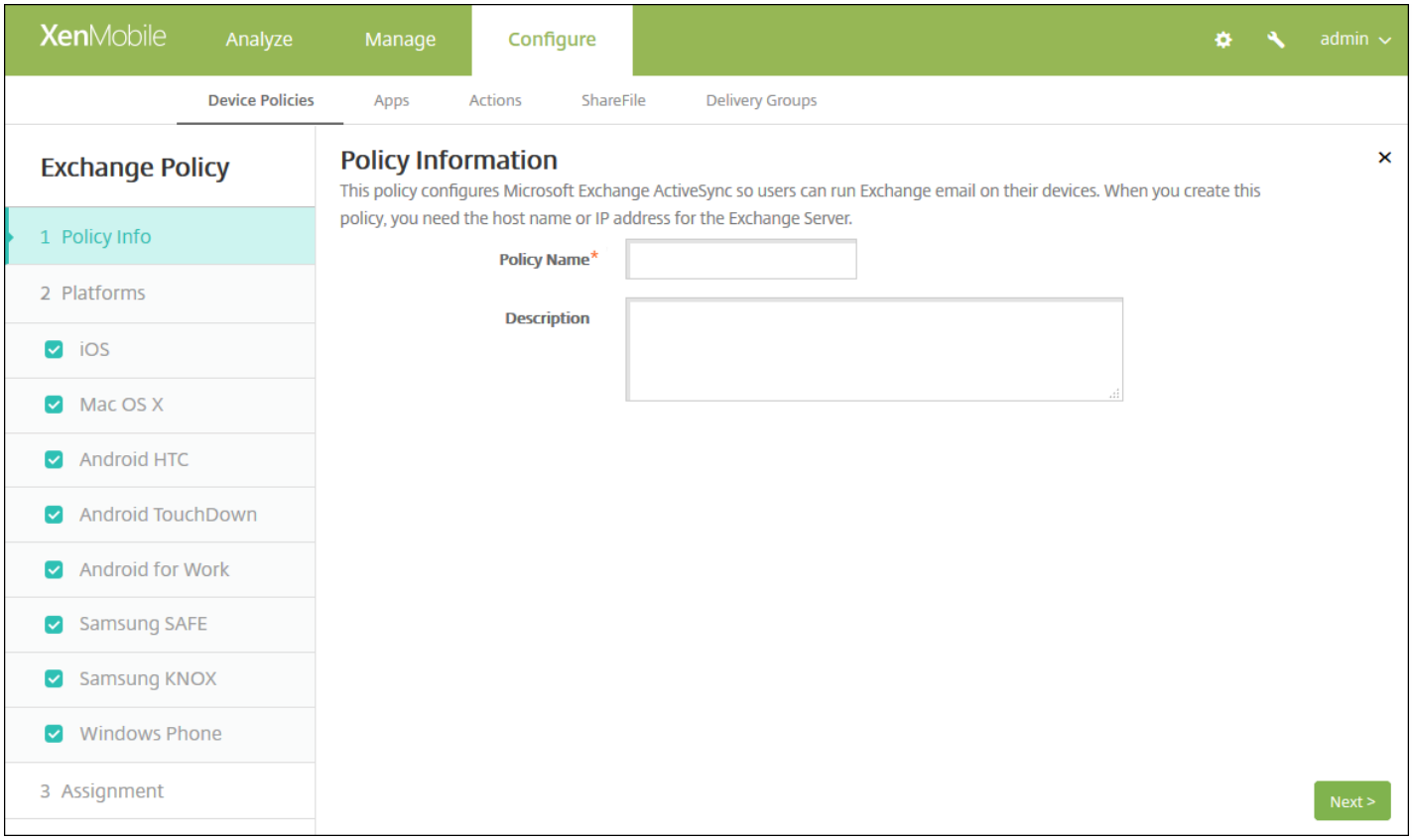
创建此策略前，需要知道 Exchange Server 的 主机名 或 IP 地址。

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. 单击 **Exchange**。 此时将显示 **Exchange 策略**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 在**策略信息**窗格中，键入以下信息：

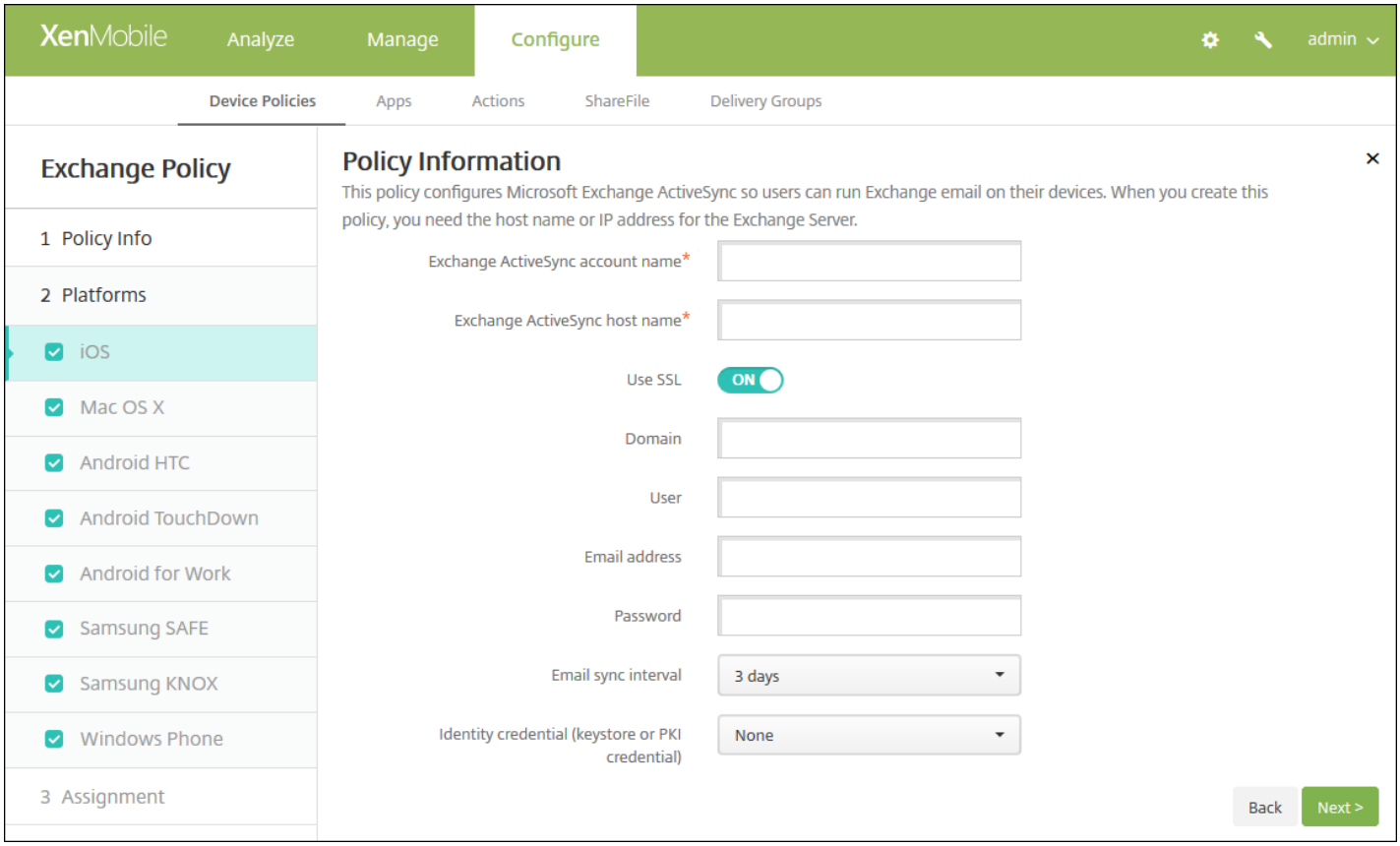
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

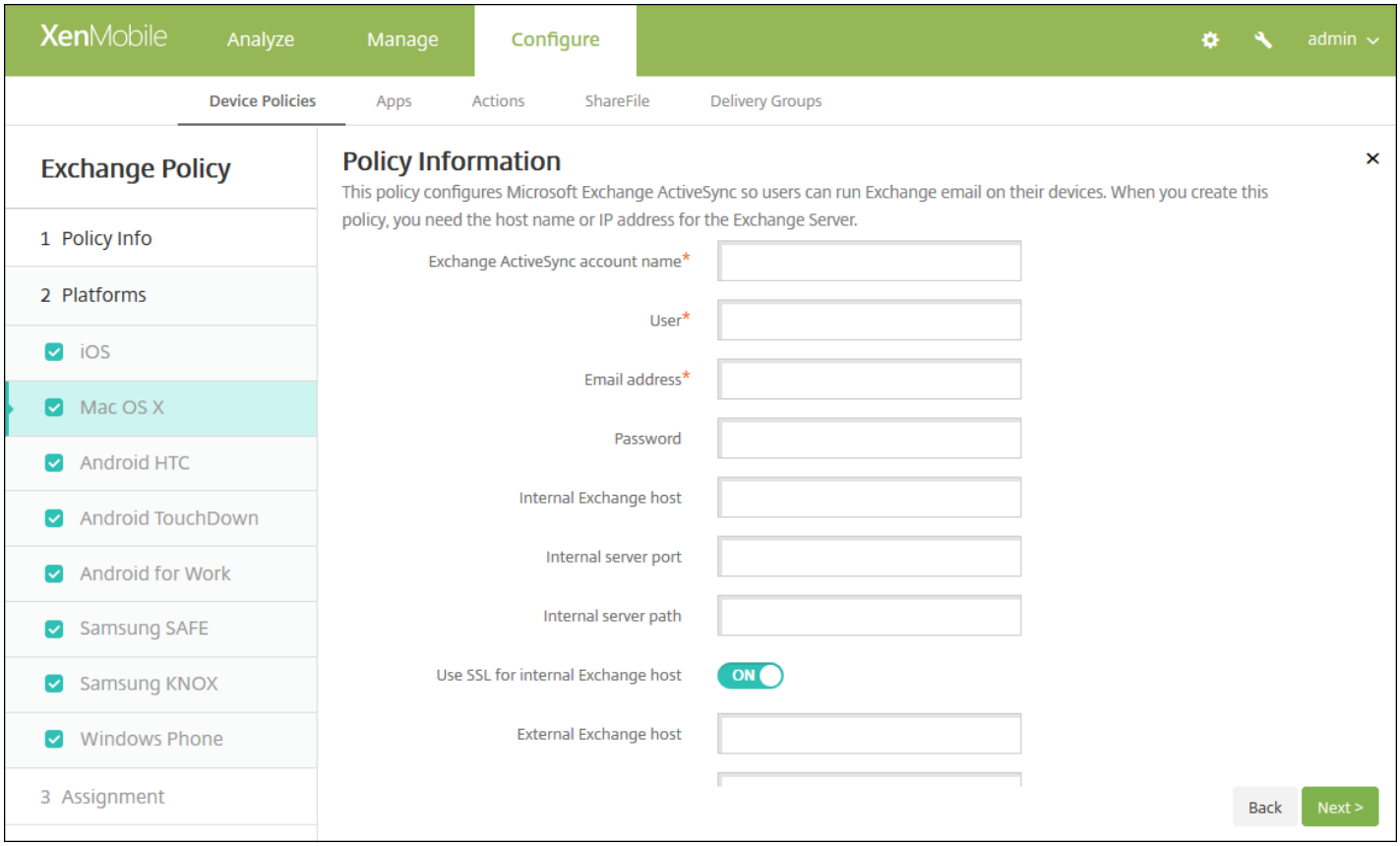


配置以下设置：

- **Exchange ActiveSync 帐户名称**：键入显示在用户设备上的电子邮件帐户的说明。
- **Exchange ActiveSync 主机名**：键入电子邮件服务器的地址。
- **使用 SSL**：选择是否确保用户设备与 Exchange Server 之间的连接安全。 默认值为**开**。
- **域**：输入 Exchange Server 所在的域。 可以在此字段中使用系统宏 ${user.domainname} 自动查找用户的域名。
- **用户**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 ${user.mail} 自动查找用户的电子邮件帐户。
- **密码**：输入 Exchange 用户帐户的可选密码。
- **电子邮件同步时间间隔**：在列表中，选择电子邮件与 Exchange Server 同步的频率。 默认值为 **3 天**。
- **身份凭据(密钥库 或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。 仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。 默认值为**无**。
- **授权电子邮件在帐户之间移动**：选择是否允许用户将 电子邮件 从此帐户移出到另一个帐户以及从不同帐户进行转发和回复。 默认值为**关**。
- **仅从电子邮件应用程序发送电子邮件**：选择是否限制用户只能从 iOS 邮件应用程序发送电子邮件。 默认值为**关**。
- **禁用最新电子邮件同步**：选择是否阻止用户同步最近使用的地址。 默认值为**关**。 此选项仅适用于 iOS 6.0 及更高版本。
- **启用 S/MIME**：选择此帐户是否支持 S/MIME 身份验证和加密。 默认值为**关**。 设置为**开**时，将显示以下两个字段：
  - **签署身份凭据**。 默认值为**无**。
  - **加密身份凭据**。 默认值为**无**。
- **启用“为消息单独设置 S/MIME”开关**：选择是否允许用户基于每个消息加密传出电子邮件。 默认值为**关**。

配置 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

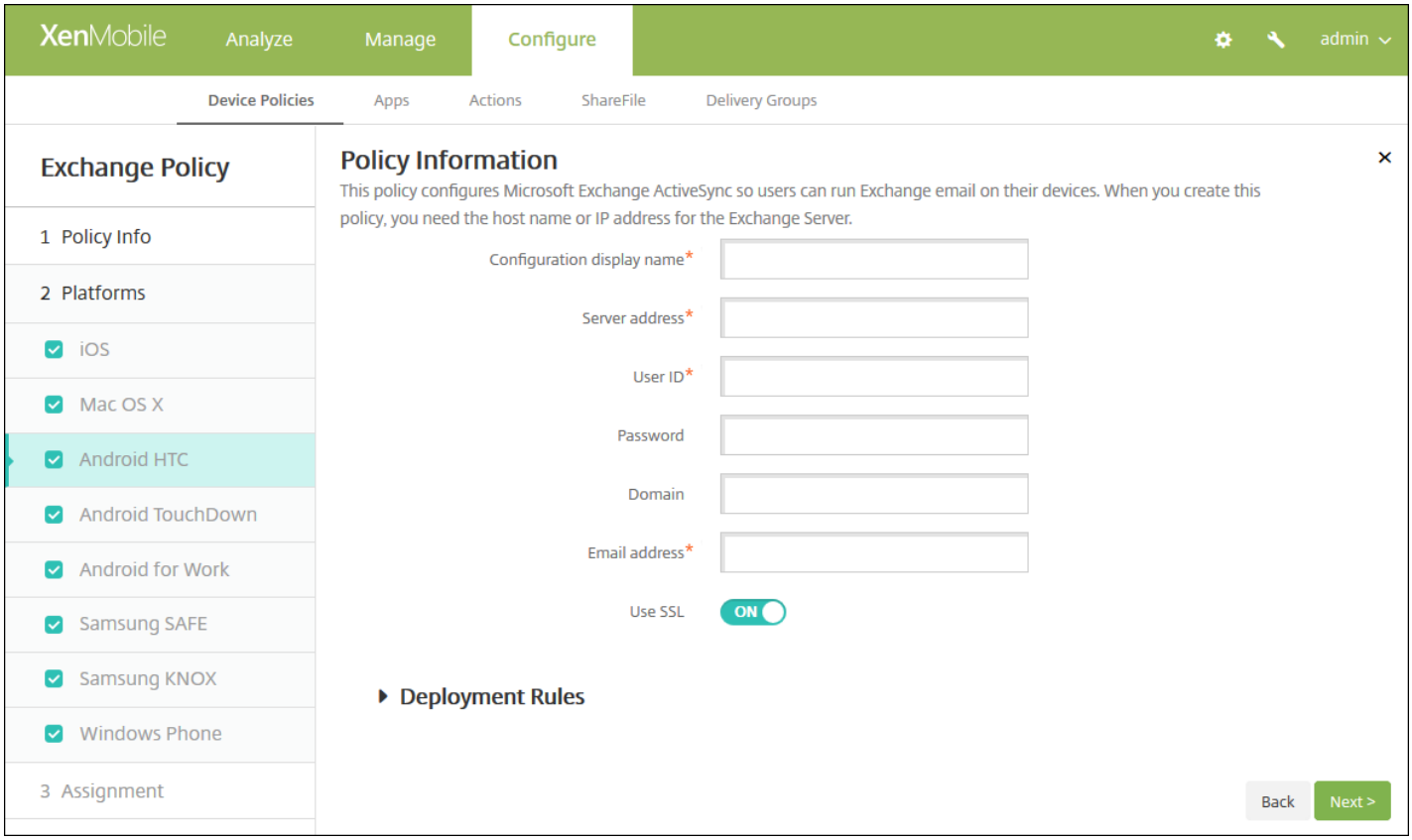


配置以下设置：

- **Exchange ActiveSync 帐户名称**：键入显示在用户设备上的电子邮件帐户的说明。
- **用户**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 ${user.mail} 自动查找用户的电子邮件帐户。
- **密码**：输入 Exchange 用户帐户的可选密码。
- **内部 Exchange 主机**：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选内部 Exchange 主机名。
- **内部服务器端口**：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选内部 Exchange Server 端口。
- **内部服务器路径**：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选内部 Exchange Server 路径。
- **对内部 Exchange 主机使用 SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。 默认值为**开**。
- **外部 Exchange 主机**：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选外部 Exchange 主机名。
- **外部服务器端口**：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选外部 Exchange Server 端口。
- **外部服务器路径**：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选外部 Exchange Server 路径。
- **对外部 Exchange 主机使用 SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。 默认值为**开**。
- **允许投递邮件**：选择是否允许用户在两个 Mac 之间通过无线共享文件，且无须连接到现有网络。 默认值为**关**。

配置 Android HTC 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

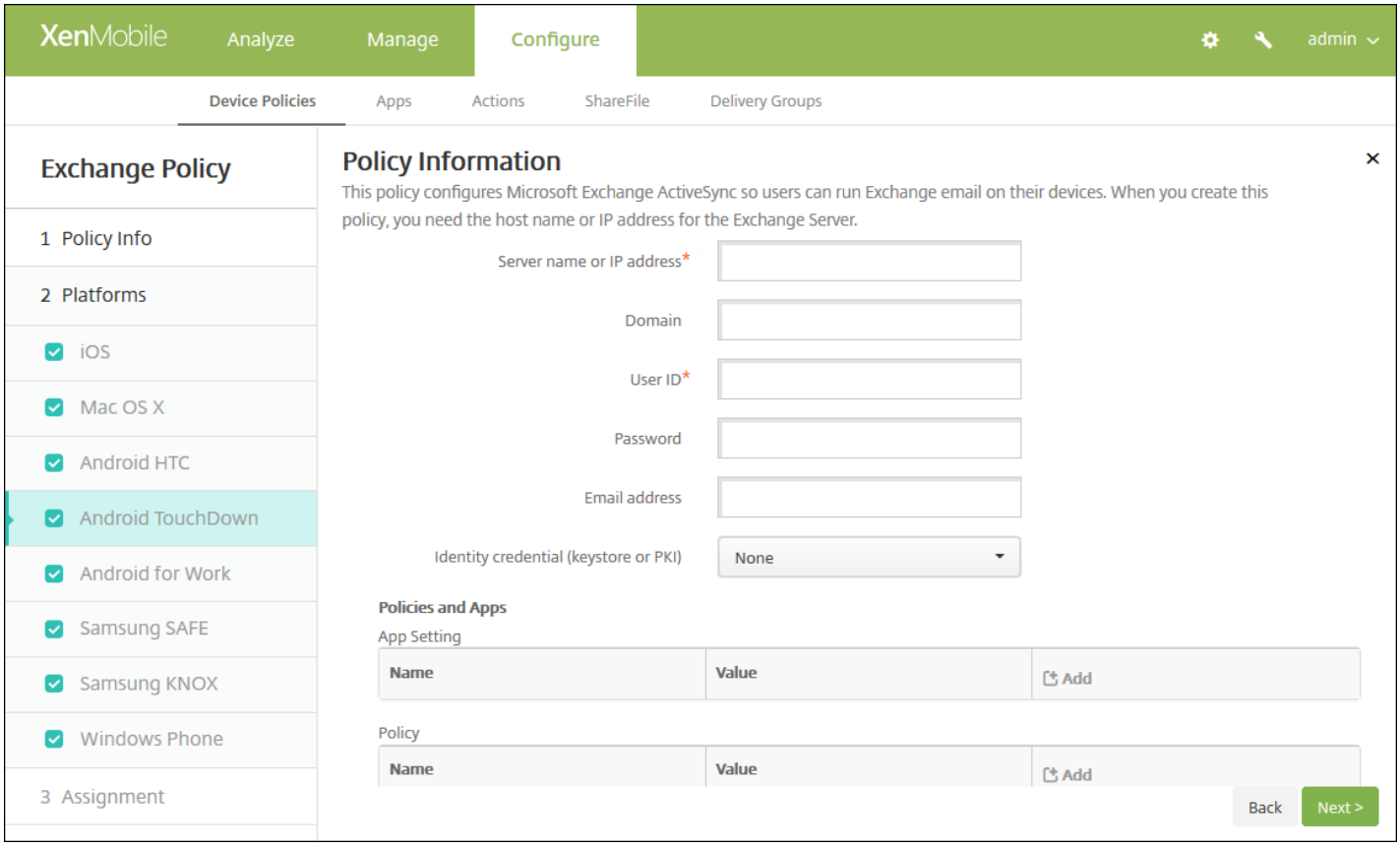


配置以下设置：

- **配置显示名称**：为此策略键入要在用户设备上显示的名称。
- **服务器地址**：键入 Exchange Server 的 主机名 或 IP 地址。
- **用户 ID**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
- **密码**：输入 Exchange 用户帐户的可选密码。
- **域**：输入 Exchange Server 所在的域。 可以在此字段中使用系统宏 ${user.domainname} 自动查找用户的域名。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 ${user.mail} 自动查找用户的电子邮件帐户。
- **使用 SSL**：选择是否确保用户设备与 Exchange Server 之间的连接安全。 默认值为开。

配置 Android TouchDown 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

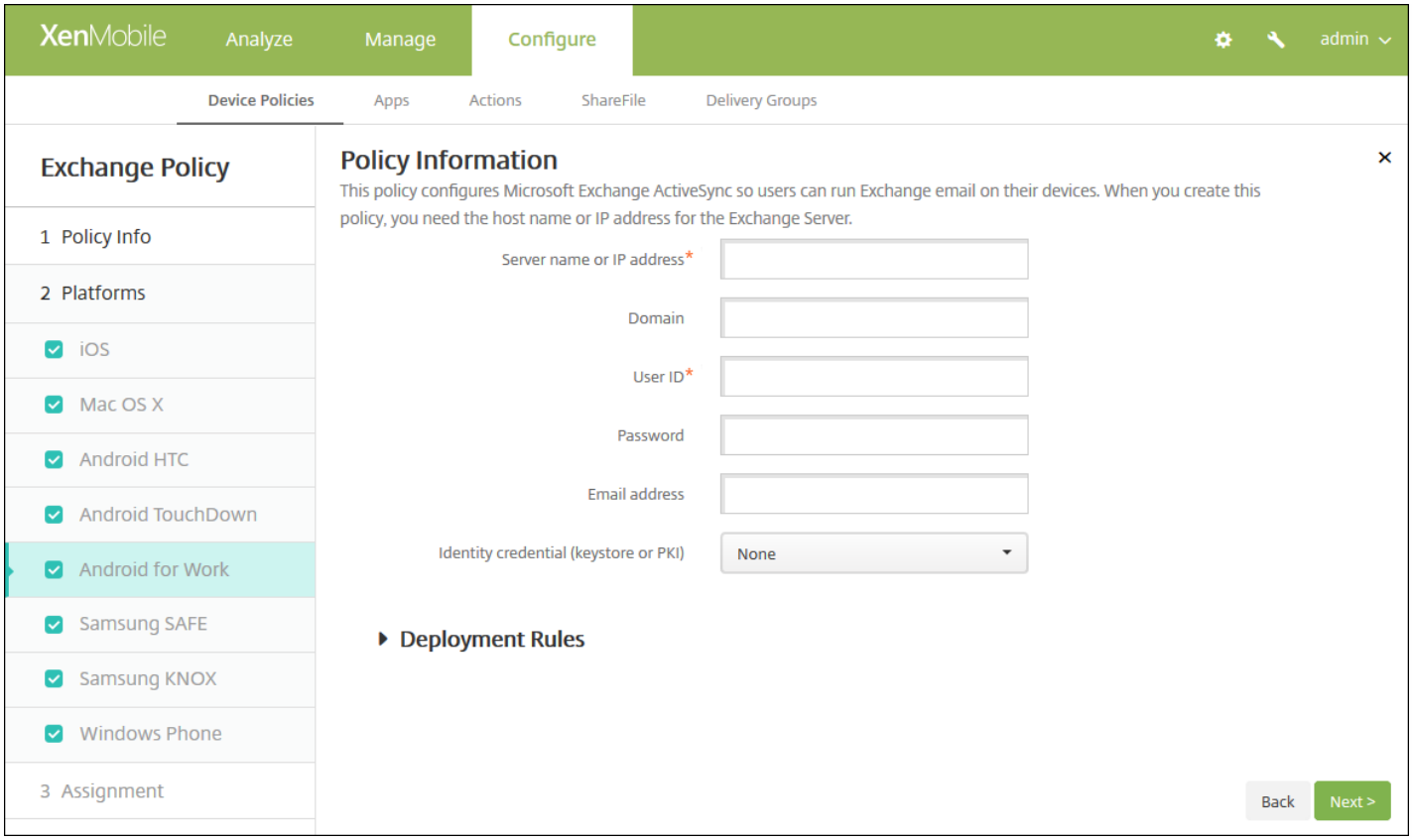


配置以下设置：

- **服务器名称或 IP 地址**：键入 Exchange Server 的 主机名 或 IP 地址。
- **域**：键入 Exchange Server 所在的域。 可以在此字段中使用系统宏 ${user.domainname} 自动查找用户的域名。
- **用户 ID**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
- **密码**：键入 Exchange 用户帐户的可选密码。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 ${user.mail} 自动查找用户的电子邮件帐户。
- **身份凭据(密钥库 或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。 仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。 默认值为**无**。
- **应用程序设置**：为此策略选择性添加 TouchDown 应用程序设置。
- **策略**：为此策略选择性添加 TouchDown 策略。

配置 Android for Work

© 1999-2017 Citrix Systems, Inc. All rights reserved.

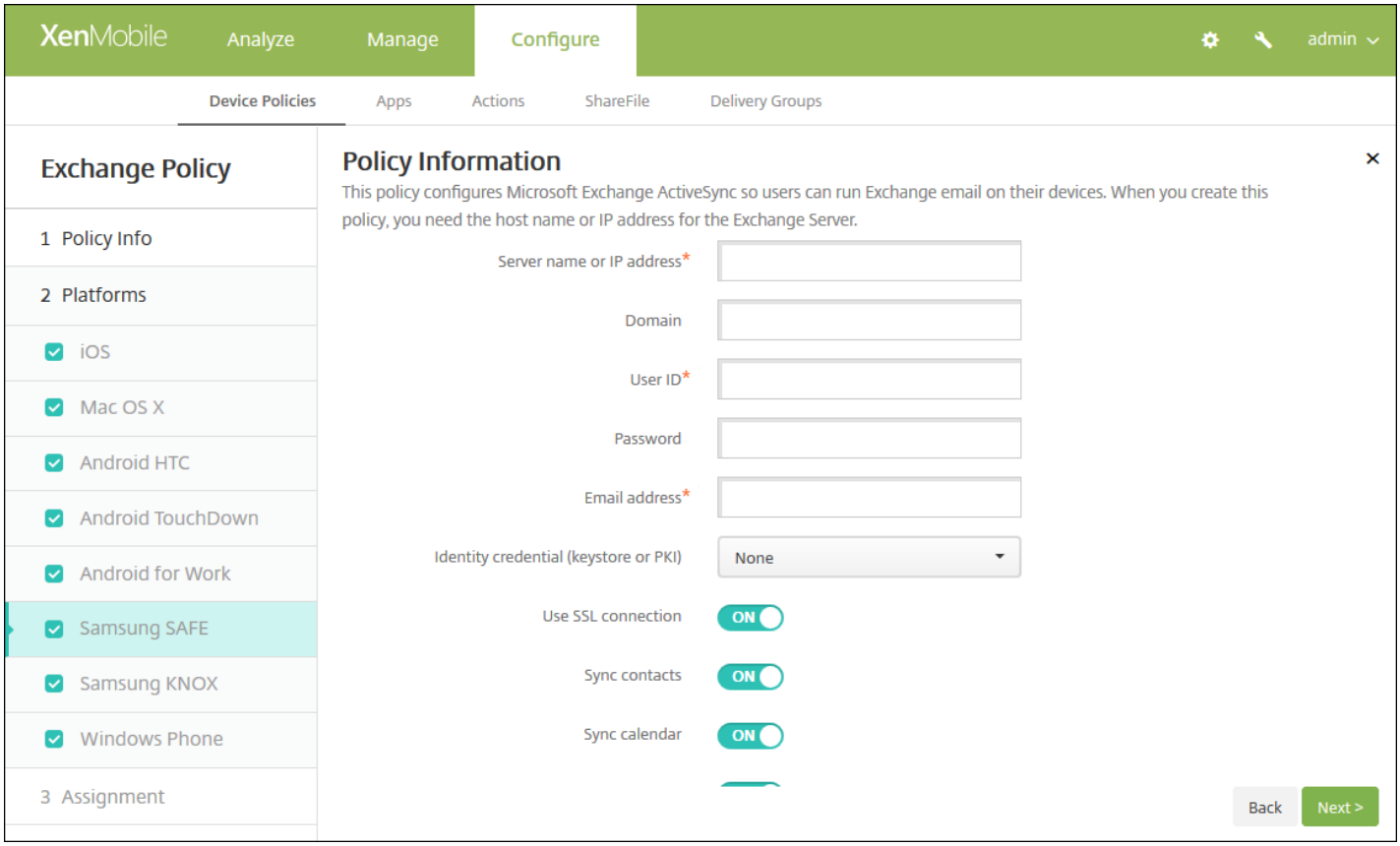


配置以下设置：

- **服务器名称或 IP 地址**：键入 Exchange Server 的 主机名 或 IP 地址。
- **域**：键入 Exchange Server 所在的域。 可以在此字段中使用系统宏 ${user.domainname} 自动查找用户的域名。
- **用户 ID**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
- **密码**：键入 Exchange 用户帐户的可选密码。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 ${user.mail} 自动查找用户的电子邮件帐户。
- **身份凭据(密钥库 或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。 仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。 默认值为**无**。

配置 Samsung SAFE 和 Samsung KNOX 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

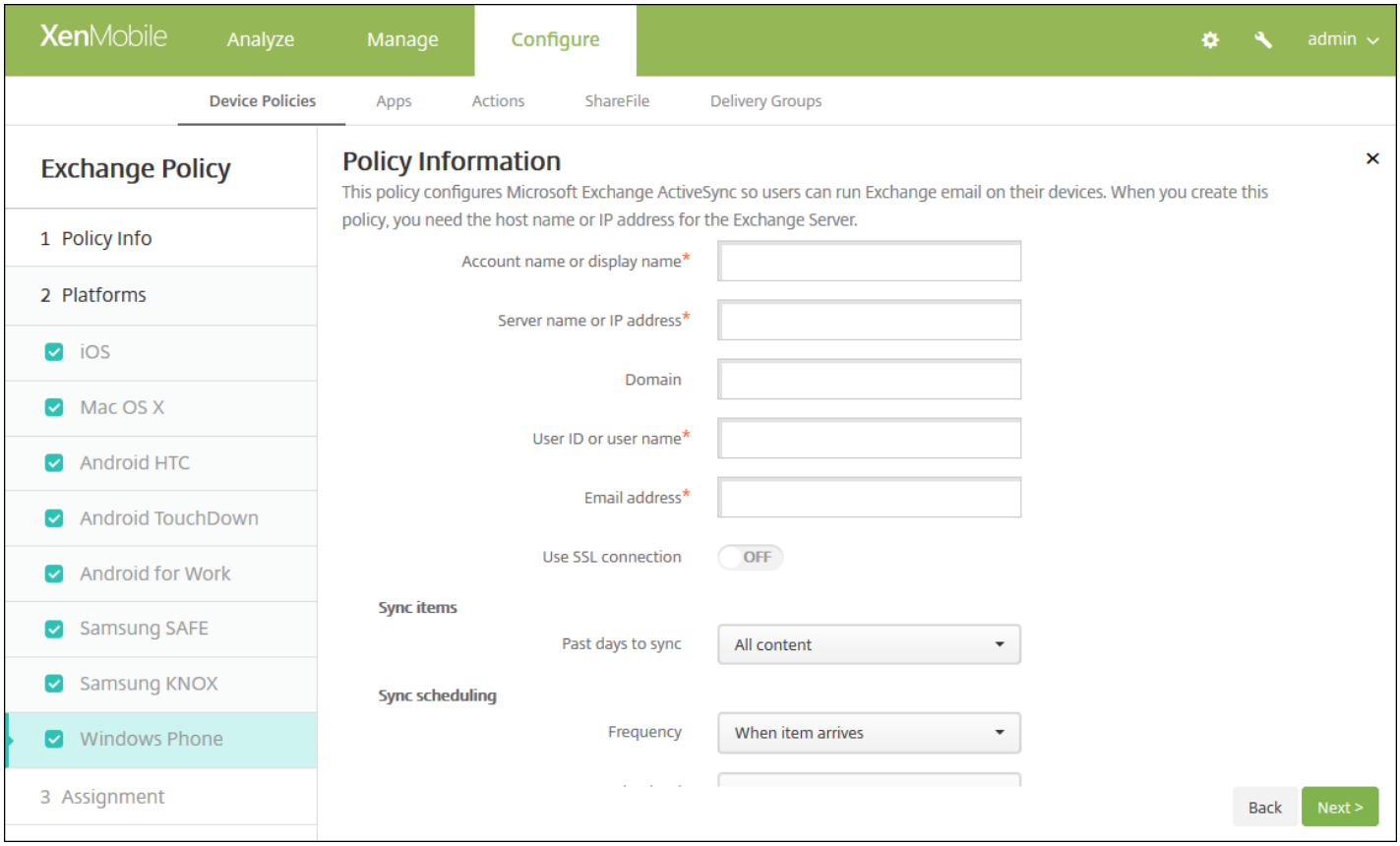


配置以下设置：

- **服务器名称或 IP 地址**：键入 Exchange Server 的 主机名 或 IP 地址。
- **域**：键入 Exchange Server 所在的域。 可以在此字段中使用系统宏 ${user.domainname} 自动查找用户的域名。
- **用户 ID**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
- **密码**：键入 Exchange 用户帐户的可选密码。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 ${user.mail} 自动查找用户的电子邮件帐户。
- **身份凭据(密钥库 或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。 仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。
- **使用 SSL 连接**：选择是否确保用户设备与 Exchange Server 之间的连接安全。 默认值为**开**。
- **同步联系人**：选择是否在用户设备与 Exchange Server 之间启用用户联系人的同步。 默认值为**开**。
- **同步日历**：选择是否在用户设备与 Exchange Server 之间启用用户日历的同步。 默认值为**开**。
- **默认 帐户**： 选择是否将用户的 Exchange 帐户设置为用于从其设备发送电子邮件的默认帐户。 默认值为**开**。

配置 Windows Phone 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

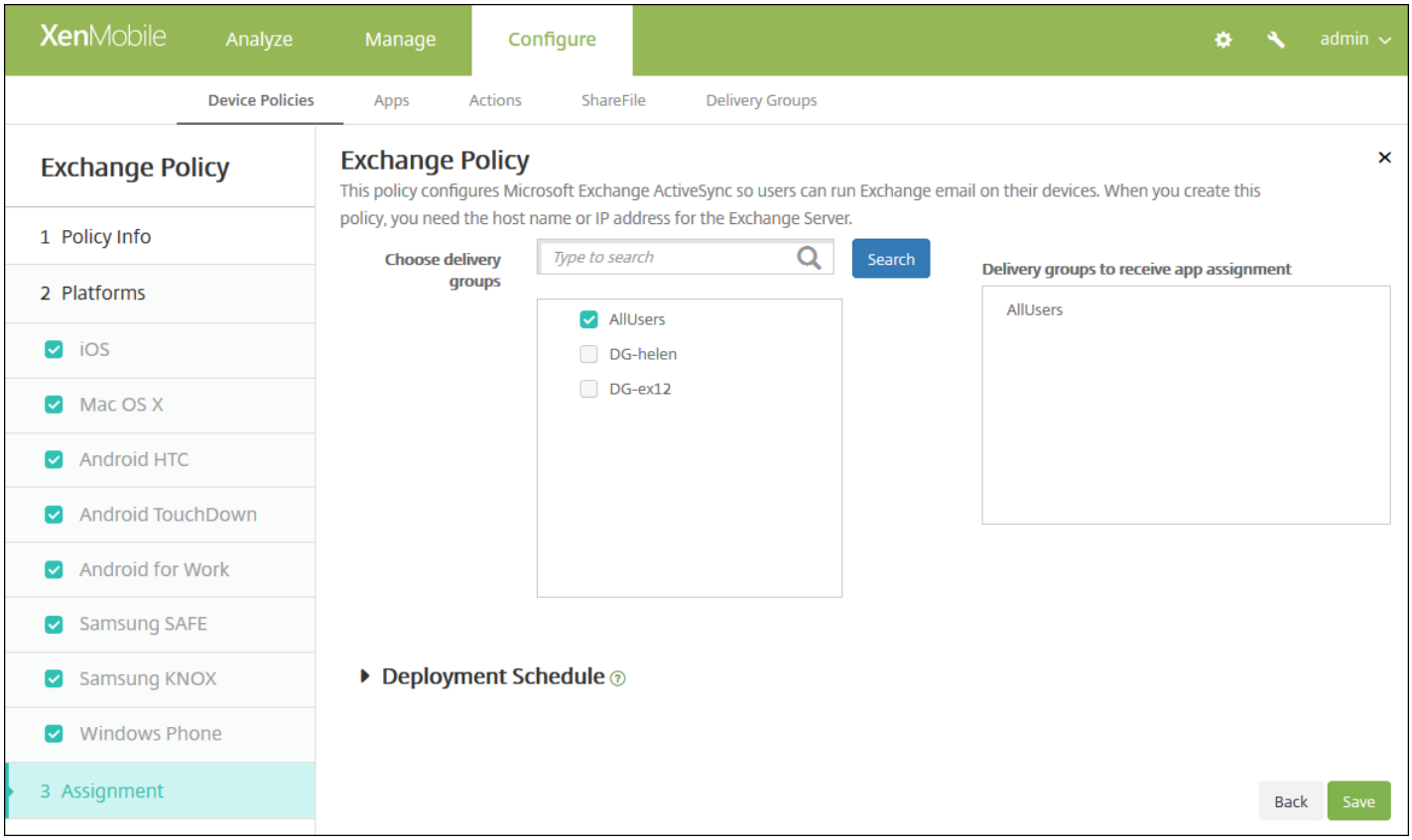
注意：此策略不允许您设置用户密码。 用户在推送策略后必须从其设备设置该参数。

- **帐户名称或显示名称**：键入 Exchange ActiveSync 帐户名称。
- **服务器名称或 IP 地址**：键入 Exchange Server 的主机名或 IP 地址。
- **域**：输入 Exchange Server 所在的域。 可以在此字段中使用系统宏 ${user.domainname} 自动查找用户的域名。
- **用户 ID 或用户名**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 ${user.mail} 自动查找用户的电子邮件帐户。
- **使用 SSL 连接**：选择是否确保用户设备与 Exchange Server 之间的连接安全。 默认值为**关**。
- **同步内容天数**：在列表中，请单击要将设备上过去多少天内的所有内容与 Exchange Server 同步。 默认值为**所有内容**。
- **频率**：在列表中，请单击同步从 Exchange Server 发送到设备的数据时要使用的计划。 默认值为 **When it arrives**（当其到达时）。
- **日志记录级别**：在列表中，请单击**已禁用**、**基本**或**高级**以指定记录 Exchange 活动时的详细级别。 默认值为**已禁用**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Exchange 策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

组织信息设备策略

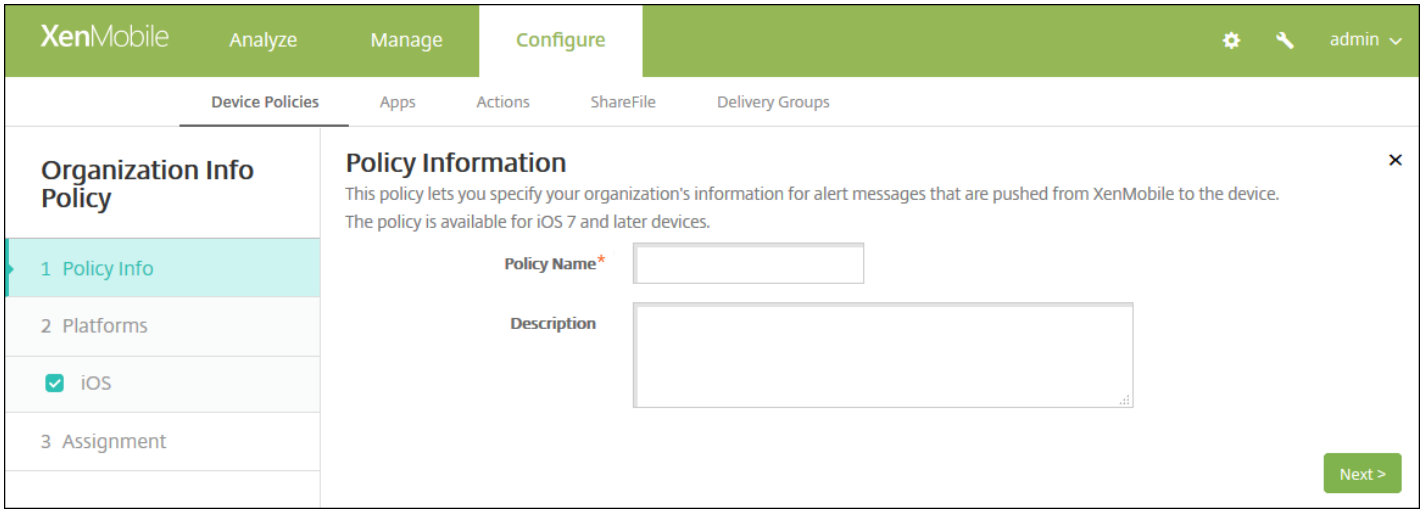
Aug 11, 2016

可以在 XenMobile 中添加设备策略以指定贵组织从 XenMobile 推送到 iOS 设备的警报消息信息。 此策略适用于 iOS 7 及更高版本的设备。

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. 单击**更多**，然后在**最终用户**下，单击**组织信息**。 此时将显示 **Organization Info Policy**（组织信息策略）页面。

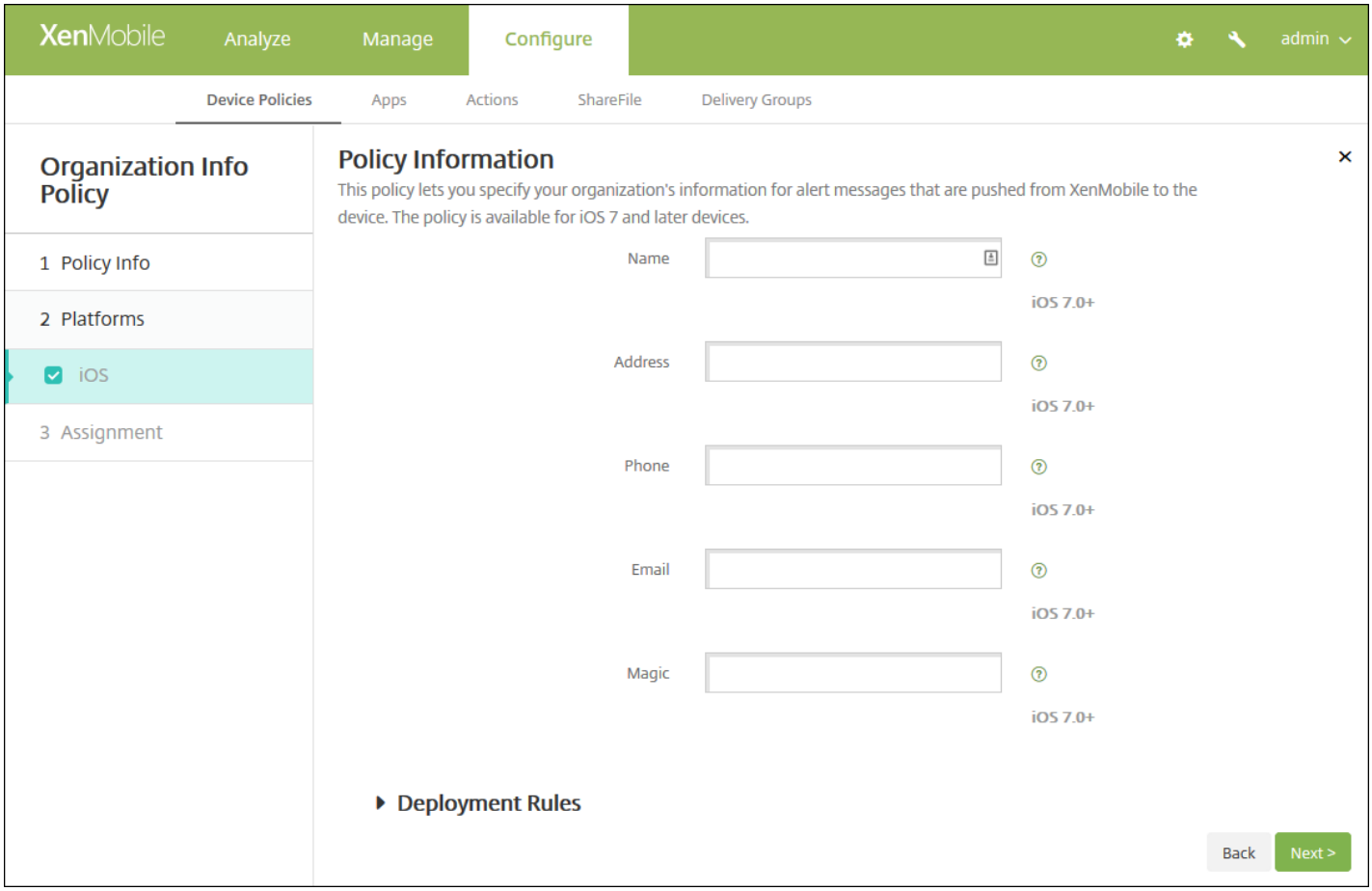


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：如有需要，请键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台信息**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



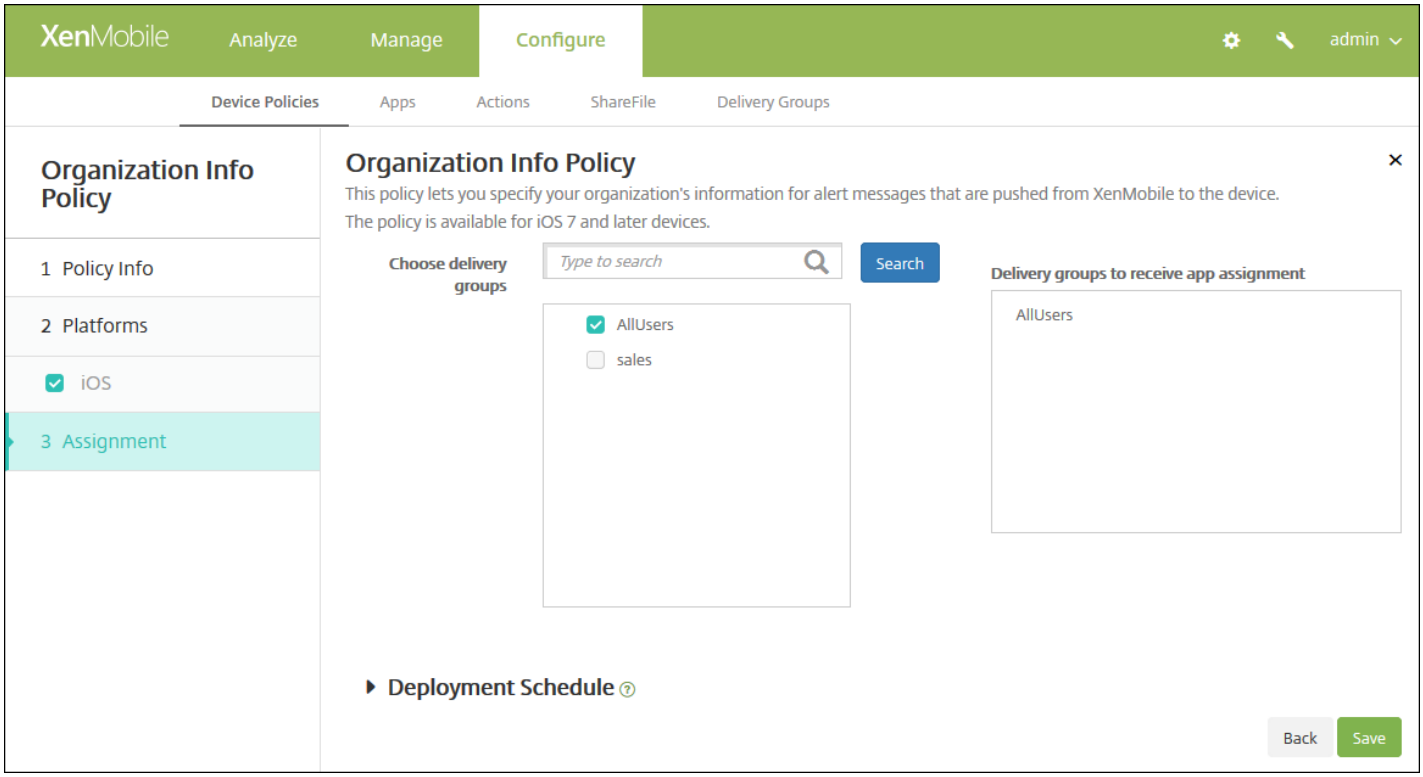
配置以下设置：

- **名称**：键入运行 XenMobile 的组织的名称。
- **地址**：键入组织的地址。
- **电话**：键入组织的技术支持电话号码。
- **电子邮件**：键入技术支持电子邮件地址。
- **魔术字**：键入用于描述组织托管的服务的单词或短语。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**组织信息策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通行码设备策略

Aug 11, 2016

可以根据贵组织的标准在 XenMobile 中创建通行码策略。 可以要求在用户设备上输入通行码，并且可以设置各种格式和通行码规则。 您可以为 iOS、Mac OS X、Android、Samsung KNOX、Android for Work、Windows Phone 和 Windows Desktop/Tablet 创建策略。 每种平台需要一组不同的值，本文将对此进行介绍。

iOS 设置

Mac OS X 设置

Android 设置

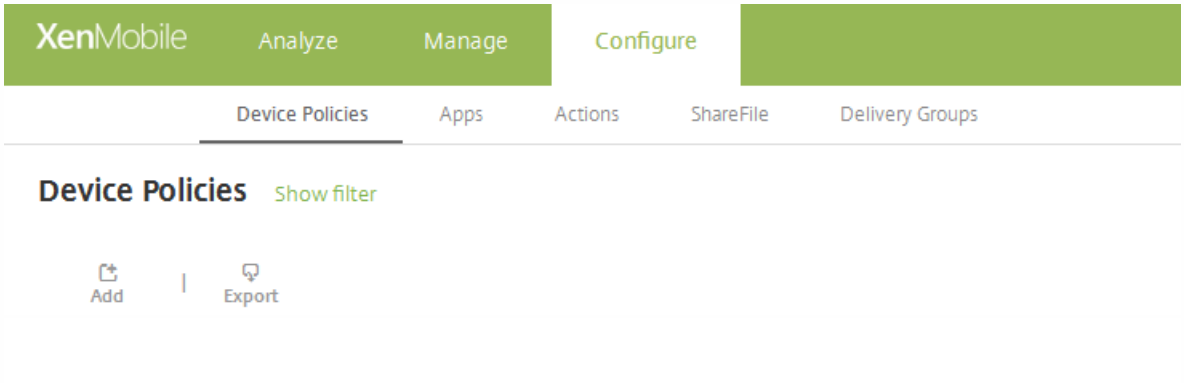
Samsung KNOX 设置

Android for Work 设置

Windows Phone 设置

Windows Desktop/Tablet 设置

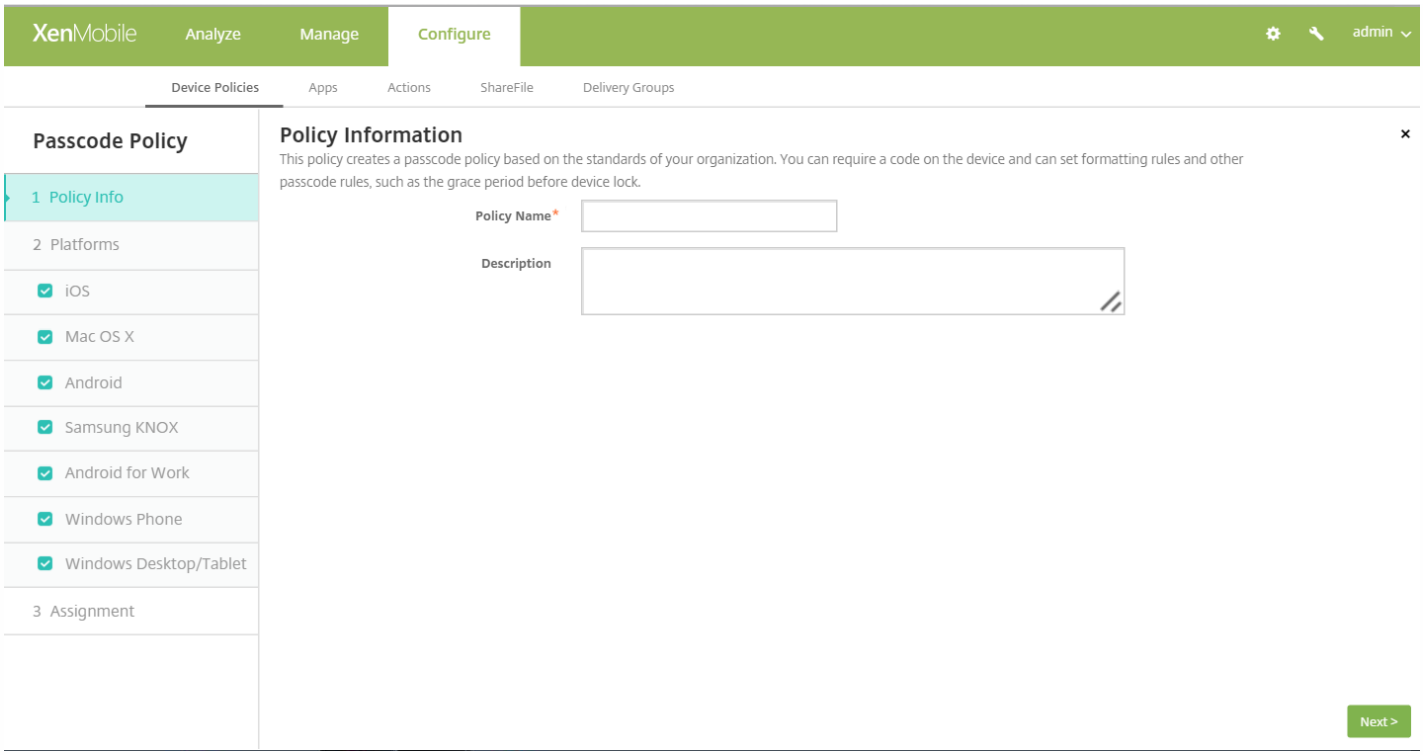
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。 此时将显示**设备策略**页面。



2. 单击**添加**。 此时将显示添加新策略页面。

3. 单击**通行码**。 此时将显示通行码策略信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

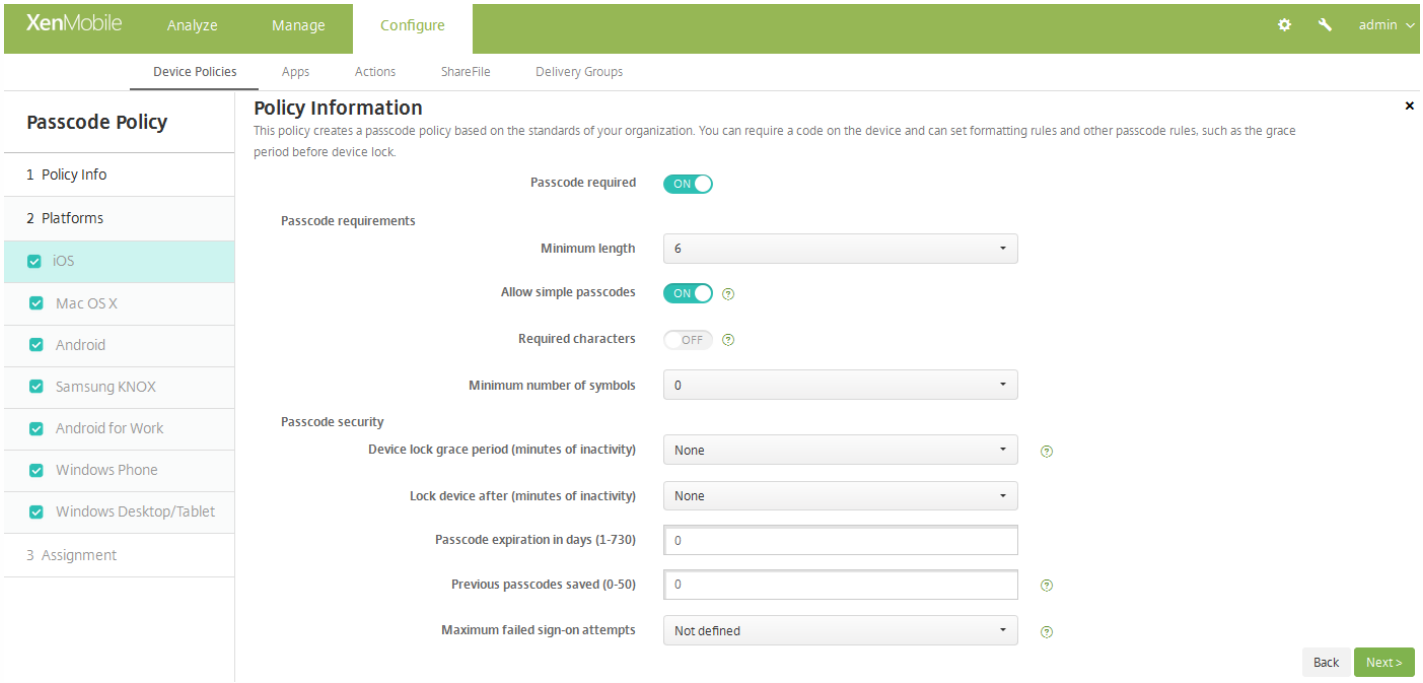
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

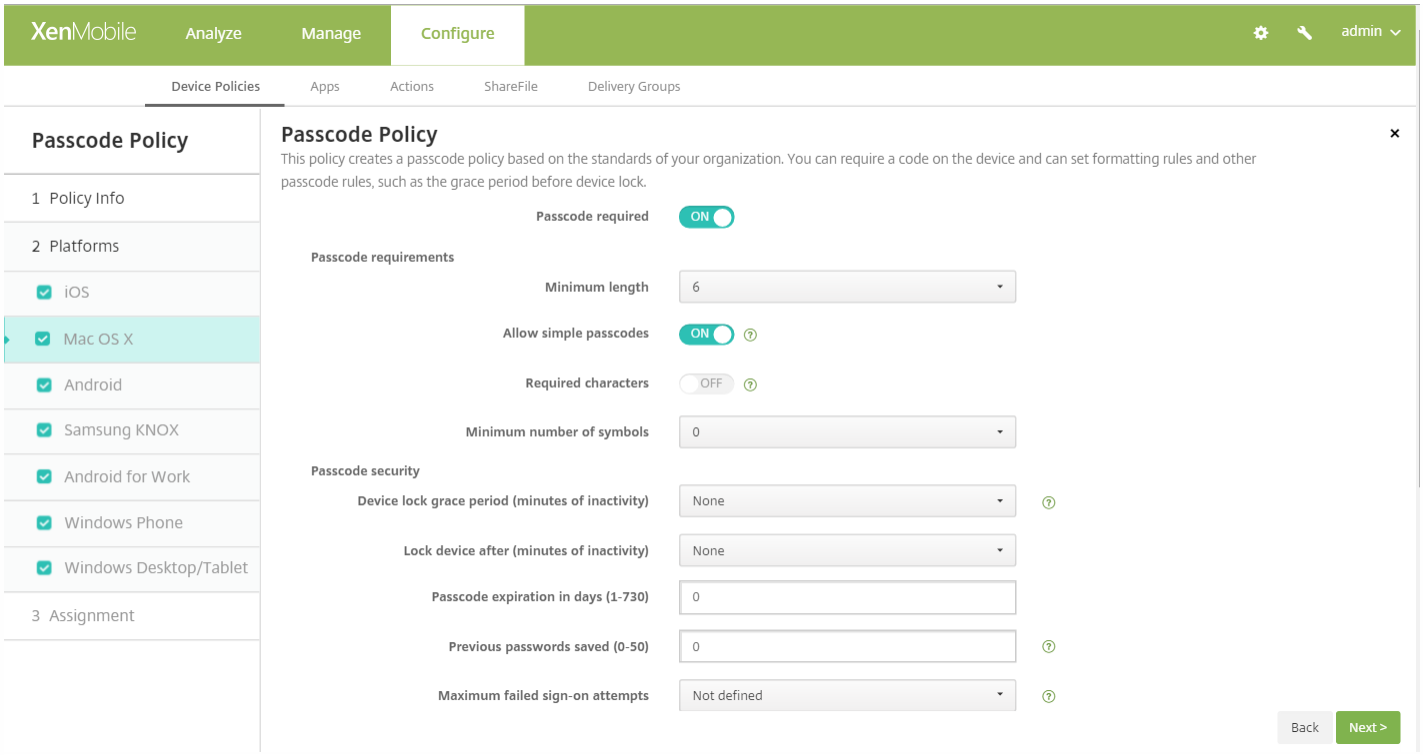


配置以下设置：

- **需要通行码**：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。 页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。
- **通行码要求**
  - **最小长度**：在列表中，单击通行码的最小长度。 默认值为 **6**。
  - **允许使用简单通行码**：选择是否允许使用简单通行码。 简单通行码是指重复或连续的字符集。 默认值为 **ON**。
  - **需含字符**：选择是否要求通行码至少包含一个字母。 默认值为**关**。
  - **符号数下限**：在列表中，单击通行码必须包含的符号数量。 默认值为 **0**。
- **通行码安全**
  - **设备锁定宽限期(不活动分钟)**：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。 默认值为**无**。
  - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的时间长度。 默认值为“无”。
  - **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。 有效值为 1–730。 默认值为 **0**，表示通行码永不过期。
  - **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。 用户无法使用在此列表中找到的任何密码。 有效值为 0–50。 默认值为 **0**，表示用户可以重复使用密码。
  - **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被完全擦除。 默认值为**未定义**。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



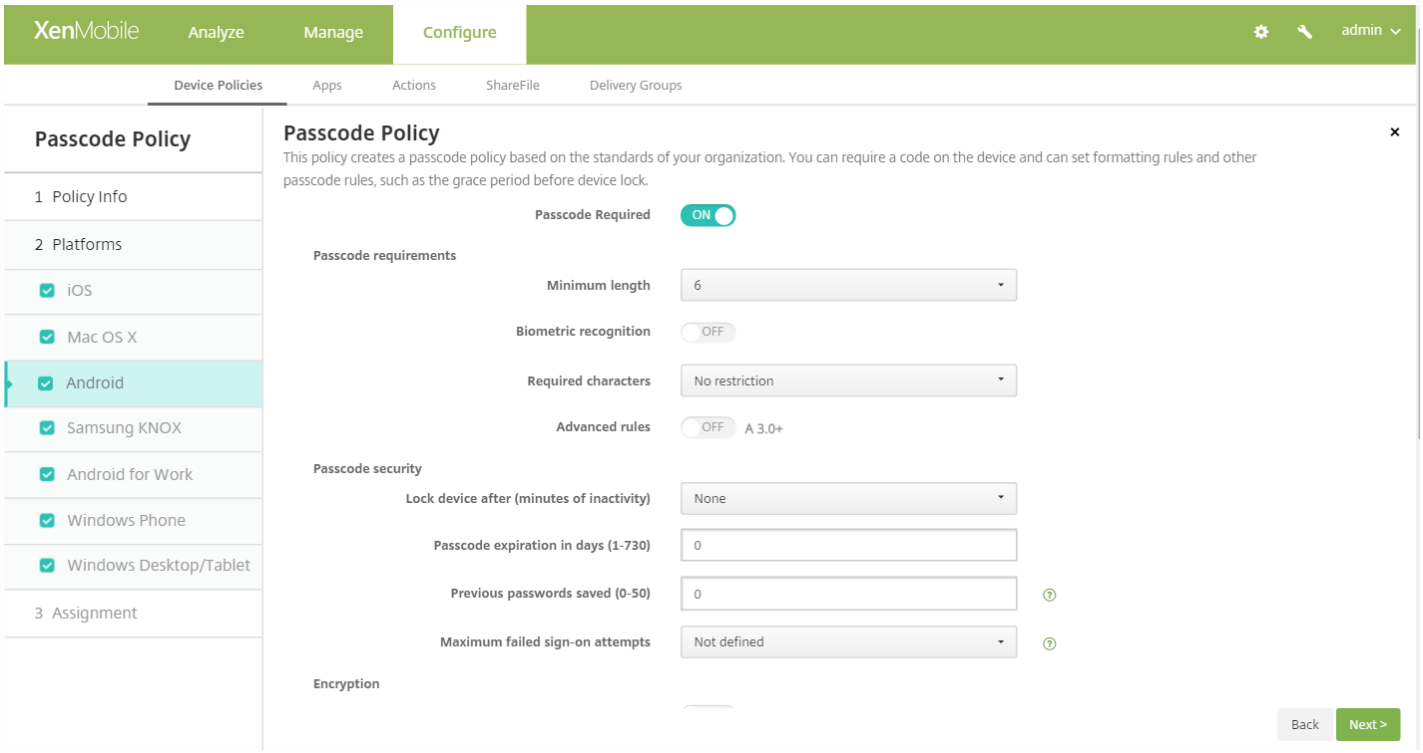
配置以下设置：

- **需要通行码**：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。 页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。
- 如果未启用**需要通行码**，请在**尝试登录失败后的延迟时间(分钟)**旁边，键入允许用户重新输入其通行码之前延迟的分钟数。
- 如果启用**需要通行码**，可以配置以下设置：
- **通行码要求**
  - **最小长度**：在列表中，单击通行码的最小长度。 默认值为 **6**。
  - **允许使用简单通行码**：选择是否允许使用简单通行码。 简单通行码是指重复或连续的字符集。 默认值为**开**。
  - **需含字符**：选择是否要求通行码至少包含一个字母。 默认值为**关**。
  - **符号数下限**：在列表中，单击通行码必须包含的符号数量。 默认值为 **0**。
- **通行码安全**
  - **设备锁定宽限期(不活动分钟)**：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。 默认值为**无**。
  - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的时间长度。 默认值为**无**。
  - **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。 有效值为 1–730。 默认值为 **0**，表示通行码永不过期。
  - **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。 用户无法使用在此列表中找到的任何密码。 有效值为 0–50。 默认值为 **0**，表示用户可以重复使用密码。
  - **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被锁定。 默认值为**未定义**。
  - **尝试登录失败后的延迟时间(分钟)**：键入允许用户重新输入其通行码之前延迟的分钟数。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

配置 Android 设置



配置以下设置：

注意：Android 的默认设置为**关**。

- **需要通行码** ：选择此选项以要求输入通行码并显示 Android 通行码设备策略的配置选项。 页面将展开以允许您配置通行码要求、通行码安全性、加密和 Samsung SAFE 的相关设置。
- **通行码要求**
  - **最小长度**：在列表中，单击通行码的最小长度。 默认值为 6。
  - **生物特征识别**：选择是否启用生物特征识别。 如果启用此选项，需含字符字段将隐藏。 默认值为**关**。
  - **需含字符**：在列表中，单击“无限制”、“数字和字母”、“仅限数字”或“仅限字母”以配置通行码的组成方式。 默认值为“无限制”。
  - **高级规则**：选择是否应用高级通行码规则。 此选项适用于 Android 3.0 及更高版本。 默认值为**关**。
  - 启用**高级设置**时，请在下面每个列表中，单击通行码必须包含的下列各字符类型的最小数量：
    - **符号**：符号的最小数量。
    - **字母**：字母的最小数量。
    - **小写字母**：小写字母的最小数量。
    - **大写字母**：大写字母的最小数量。
    - **数字或符号**：数字或符号的最小数量。
    - **数字**：数字的最小数量。
- **通行码安全**
  - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的时间长度。 默认值为**无**。
  - **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。 有效值为 1–730。 默认值为 **0**，表示通行码永不过期。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。 用户无法使用在此列表中找到的任何密码。 有效值为 0–50。 默认值为 **0**，表示用户可以重复使用密码。
- **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被擦除。 默认值为**未定义**。

- **加密**
  - **启用加密**：选择是否启用加密。 此选项适用于 Android 3.0 及更高版本。 无论**需要通行码**设置为何，此选项都可用。

    注意：要加密其设备，用户必须首先具有充电电池并将此设备接通电源一个小时或更长时间，以便进行加密。 如果中断加密过程，可能会丢失其设备上的部分或全部数据。 设备加密后，过程无法逆转，除非执行出厂重置，但这样会擦除设备上的所有数据。

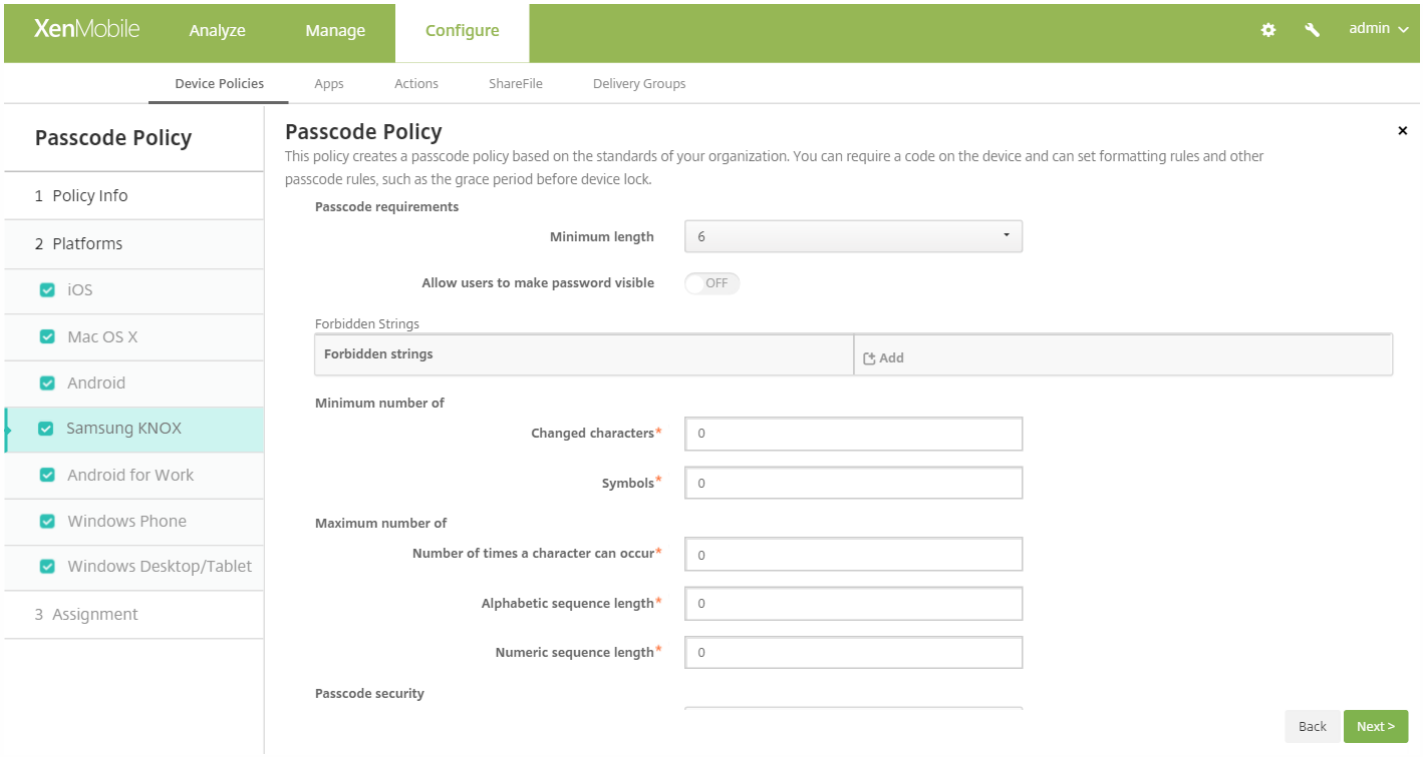
- **Samsung SAFE**
  - **对所有用户使用 相同 的通行码**：选择是否对所有用户使用相同的通行码。 默认值为**关**。 此设置仅适用于 Samsung SAFE 设备，无论**需要通行码**设置为何，此选项都可用。
  - 启用**对所有用户使用相同的通行码**时，在**通行码**字段键入供所有用户使用的通行码。
  - 如果启用**需要通行码**，可以配置以下 Samsung SAFE 设置：
    - **更改的字符**：键入以前的通行码中用户必须更改的字符数量。 默认值为 **0**。
    - **字符 可以出现的次数**：键入某个字符可以在通行码中出现的最大次数。 默认值为 **0**。
    - **字母序列长度**：键入通行码中字母序列的最大长度。 默认值为 **0**。
    - **数字序列长度**：键入通行码中数字序列的最大长度。 默认值为 **0**。
    - **允许用户将 密码 设为可见**：选择用户是否可以将其通行码设为可见。 默认值为**开**。
    - **禁止的字符**：可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。 对于要拒绝使用的每个 字符串 ，请单击**添加**，然后执行以下操作：
      - **禁止的字符**：键入用户不可以使用的字符串。
      - 单击**保存**以添加字符串，或单击**取消**以取消添加字符串。

        注意：要删除现有字符串，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

        要编辑现有字符串，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

配置 Samsung KNOX 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **通行码要求**
  - **最小长度**：在列表中，单击通行码的最小长度。 默认值为 **6**。
  - **允许用户将密码设为可见**：选择是否允许用户将密码设为可见。
  - **禁止的字符**：可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。 对于要拒绝的每个字符串，请单击“添加”并执行以下操作：
    - **禁止的字符**：键入用户不可以使用的字符串。
    - 单击**保存**以添加字符串，或单击**取消**以取消添加字符串。

      注意：要删除现有字符串，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

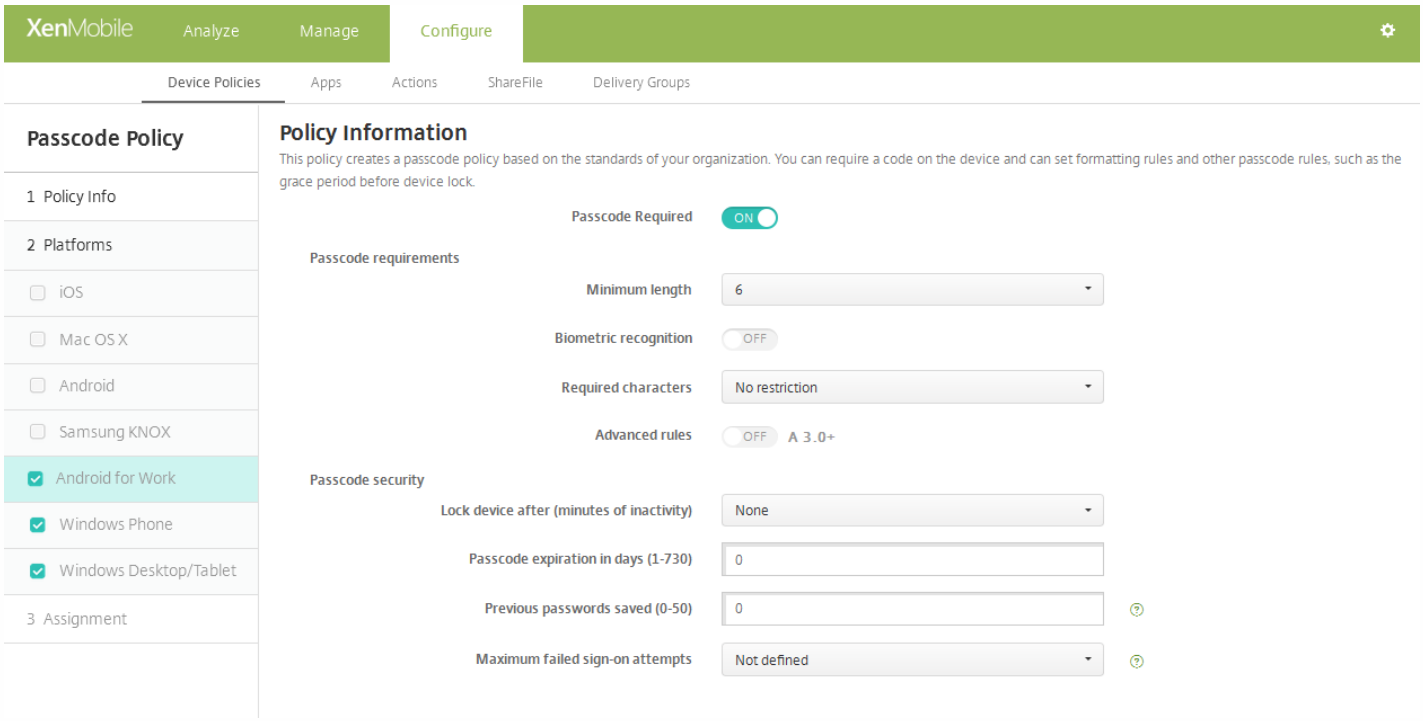
      要编辑现有字符串，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **最小数目**
  - **更改的字符**：键入以前的通行码中用户必须更改的字符数量。 默认值为 **0**。
  - **符号**：键入通行码中所需符号的最小数量。 默认值为 **0**。
- **最大数目**
  - **字符可以出现的次数**：键入某个字符可以在通行码中出现的最大次数。 默认值为 **0**。
  - **字母序列长度**：键入通行码中字母序列的最大长度。 默认值为 **0**。
  - **数字序列长度**：键入通行码中数字序列的最大长度。 默认值为 **0**。
- **通行码安全**
  - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的秒数。 默认值为**无**。
  - **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。 有效值为 1–730。 默认值为 **0**，表示通行码永不过期。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。 用户无法使用在此列表中找到的任何密码。 有效值为 0–50。 默认值为 **0**，表示用户可以重复使用密码。
- **如果超过失败登录尝试次数，设备将锁定**：在列表中，单击用户在成功登录之前能够失败的次数，超过此次数后，设备将被锁定。 默认值为**未定义**。
- **如果超过失败登录尝试次数，设备将被擦除**：在列表中，单击用户在成功登录之前能够失败的次数，超过此次数后，将从设备中擦除 KNOX 容器（以及 KNOX 数据）。 擦除后，用户需要重新初始化 KNOX 容器。默认设置为**未定义**。

配置 Android for Work 设置



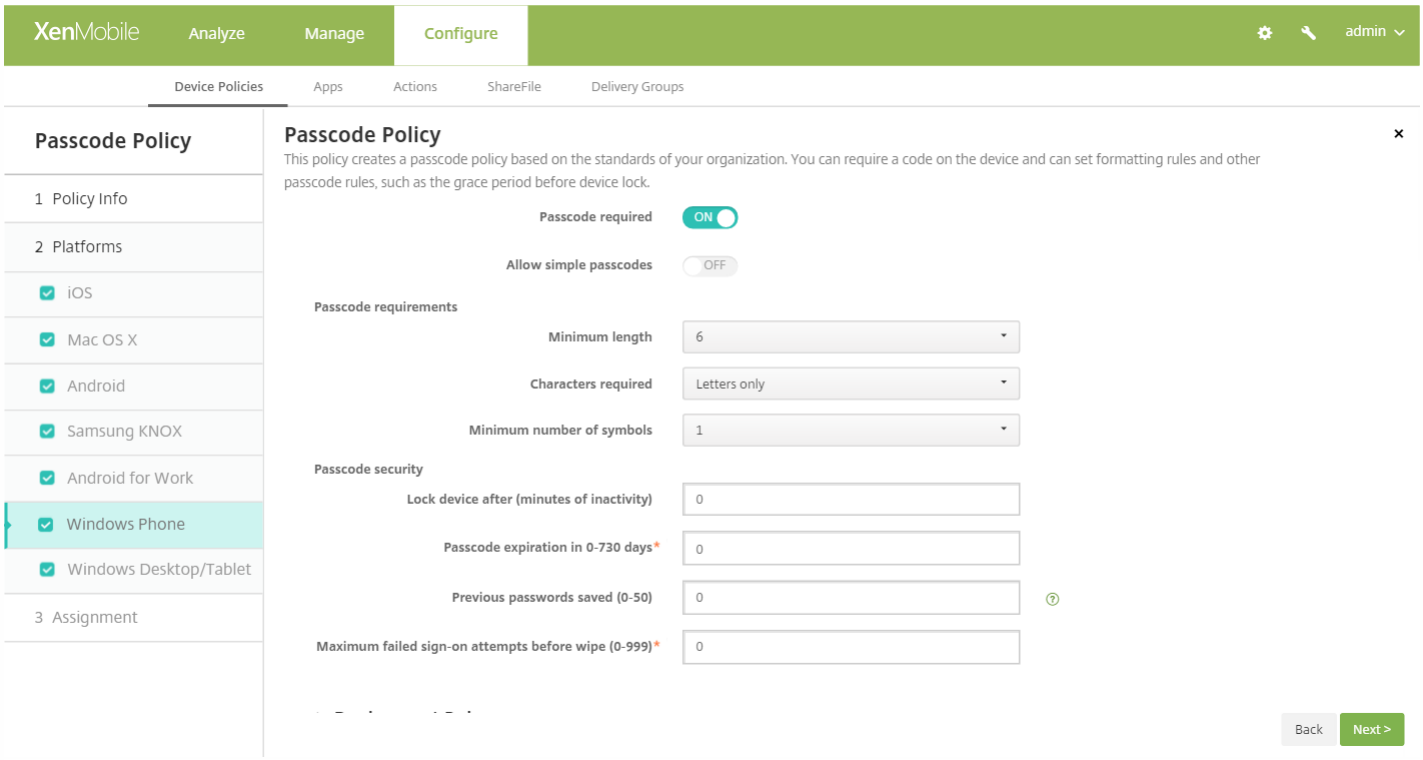
配置以下设置：

- **需要通行码**：选择此选项以要求输入通行码并显示 Android for Work 通行码设备策略的配置选项。 页面将展开以允许您配置通行码要求和通行码安全性的相关设置。
- **通行码要求**
  - **最小长度**：在列表中，单击通行码的最小长度。 默认值为 **6**。
  - **生物特征识别**：选择是否启用生物特征识别。 如果启用此选项，**需含字符**字段将隐藏。 默认值为**关**。 请注意，目前尚不支持此功能。
  - **需含字符**：在列表中，单击**无限制**、**数字和字母**、**仅限数字**或**仅限字母**以配置通行码的组成方式。 默认值为**无限制**。
  - **高级规则**：选择是否应用高级通行码规则。 此选项不适用于 Android 5.0 之前的 Android 设备。 默认值为**关**。
  - 启用**高级设置**时，请在下面每个列表中，单击通行码必须包含的下列各字符类型的最小数量：
    - **符号**：符号的最小数量。
    - **字母**：字母的最小数量。
    - **小写字母**：小写字母的最小数量。
    - **大写字母**：大写字母的最小数量。
    - **数字或符号**：数字或符号的最小数量。
    - **数字**：数字的最小数量。
- **通行码安全**
  - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的分钟数。 默认值为**无**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。 有效值为 1–730。 默认值为 **0**，表示通行码永不过期。
- **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。 用户无法使用在此列表中找到的任何密码。 有效值为 0–50。 默认值为 **0**，表示用户可以重复使用密码。
- **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前能够失败的次数，超过此次数后，将从设备中擦除 KNOX 容器（以及 KNOX 数据）。 擦除后，用户需要重新初始化 KNOX 容器。默认设置为**未定义**。

配置 Windows Phone 设置

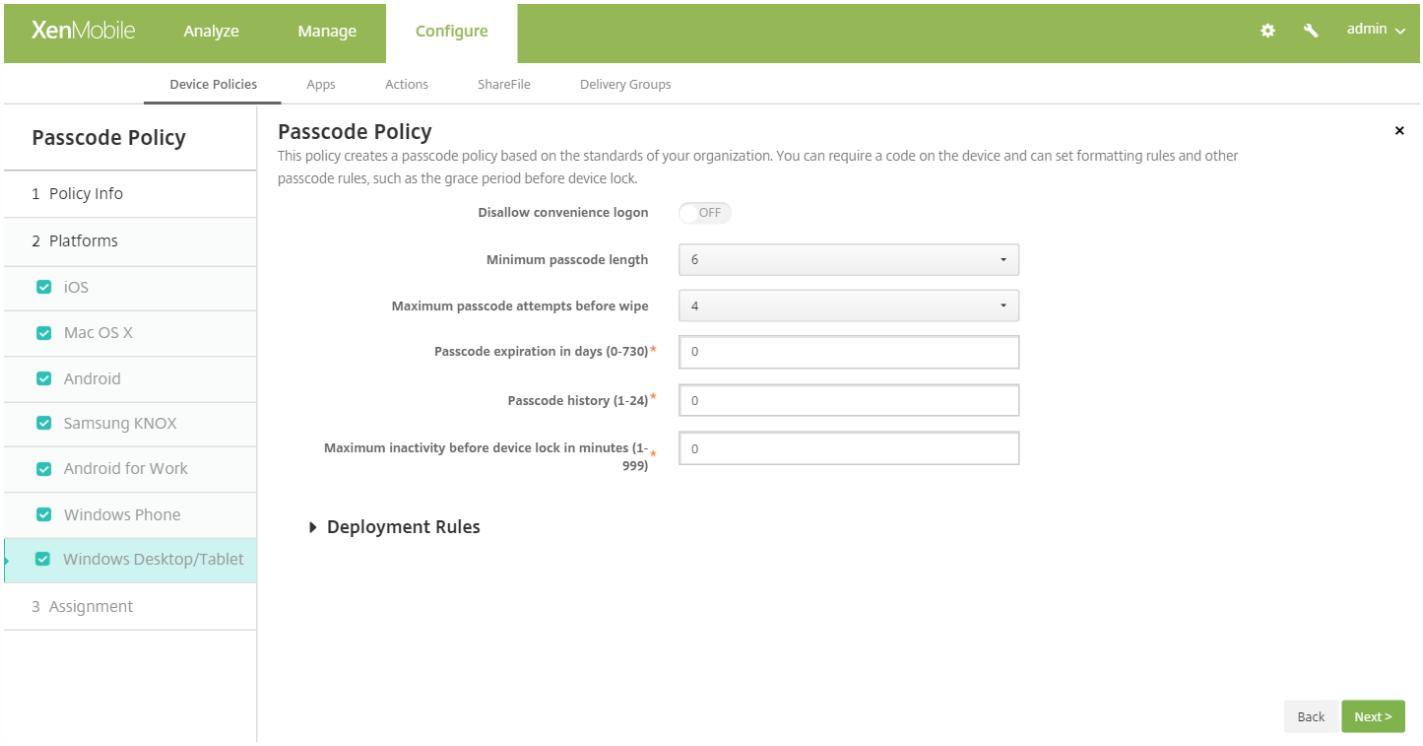


配置以下设置：

- **需要通行码**：选择此选项将不要求提供 Windows Phone 设备的通行码。 默认设置为**开**，表示需要提供通行码。 禁用此设置时，页面折叠，不再显示以下选项。
- **允许使用简单通行码**：选择是否允许使用简单通行码。 简单通行码是指重复或连续的字符集。 默认值为关。
- **通行码要求**
  - **最小长度**：在列表中，单击通行码的最小长度。 默认值为 **6**。
  - **需含字符**：在列表中单击**数字或字母数字**、**仅限字母**或**仅限数字**以配置通行码的组成方式。 默认值为**仅限字母**。
  - **符号数下限**：在列表中，单击通行码必须包含的符号数量。 默认值为 **1**。
- **通行码安全**
  - **此时间后锁定设备(不活动分钟数)**：键入设备在锁定之前能够不活动的分钟数。 默认值为 **0**。
  - **通行码在 0 - 730 天内有效**：键入有效天数，超过此天数后，通行码将过期。 有效值为 0–730。 默认值为 **0**，表示通行码永不过期。
  - **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。 用户无法使用在此列表中找到的任何密码。 有效值为 0–50。 默认值为 **0**，表示用户可以重复使用密码。
  - **擦除前的最大失败登录尝试次数(0 - 999)**：键入用户在成功登录之前能够失败的次数，超过此次数后，将擦除设备中的企业数据。 默认值为 **0**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置 Windows Desktop/Tablet 设置



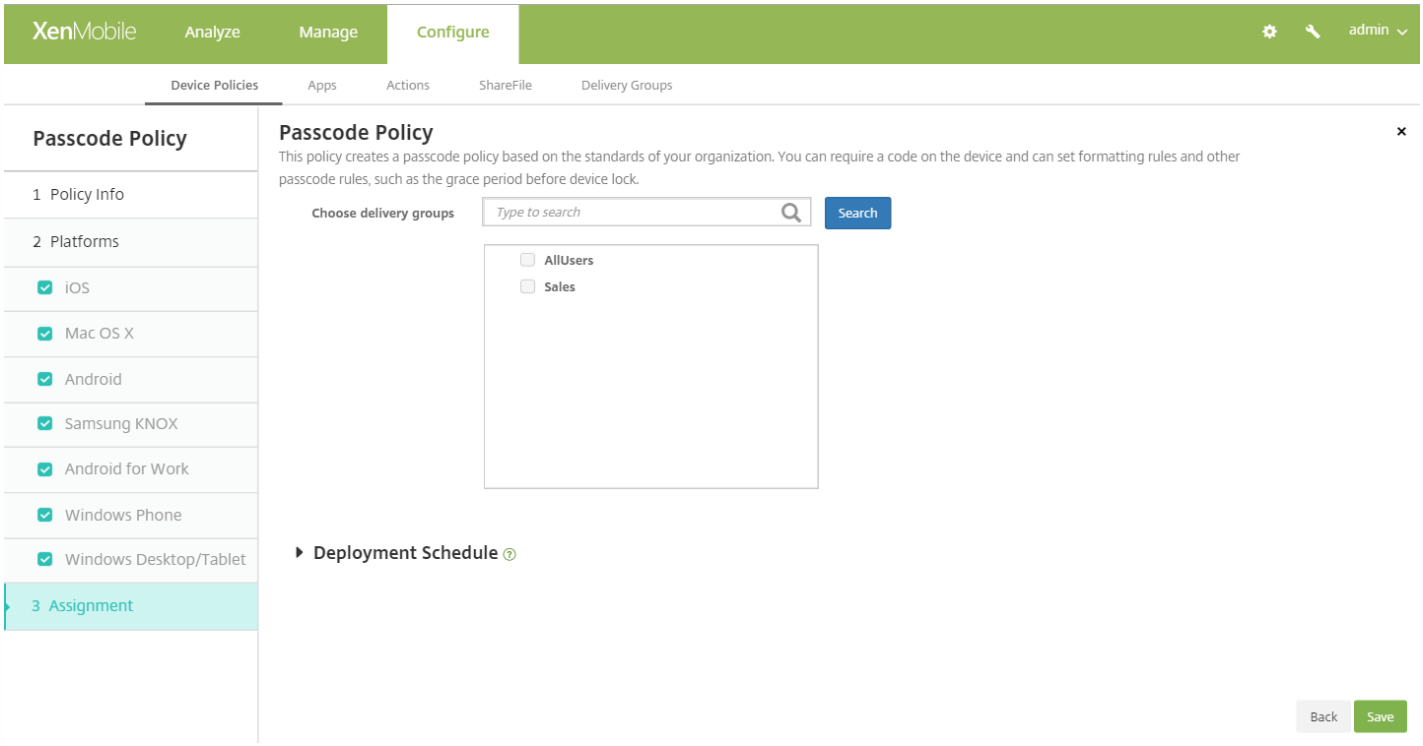
配置以下设置：

- **不允许便捷登录**：选择是否允许用户使用图片密码或生物统计登录访问其设备。 默认值为**关**。
- **最小通行码长度**：在列表中，单击通行码的最小长度。 默认值为 **6**。
- **擦除前的通行码尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，将擦除设备中的企业数据。 默认值为 **4**。
- **通行码有效期限(0 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。 有效值为 0–730。 默认值为 **0**，表示通行码永不过期。
- **通行码历史记录: (1-24)**：键入要保存的使用过的通行码数量。 用户无法使用在此列表中找到的任何通行码。 有效值为 1–24。 必须在此字段中输入介于 1 到 24 之间的数值。 默认值为 **0**。
- **设备锁定前的最长不活动时间(1 - 999 分钟)**：输入设备在锁定之前可以不活动的时间长度，单位为分钟。 有效值为 1–999。 必须在此字段中输入介于 1 到 999 之间的数值。 默认值为 **0**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**通行码策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

个人热点设备策略

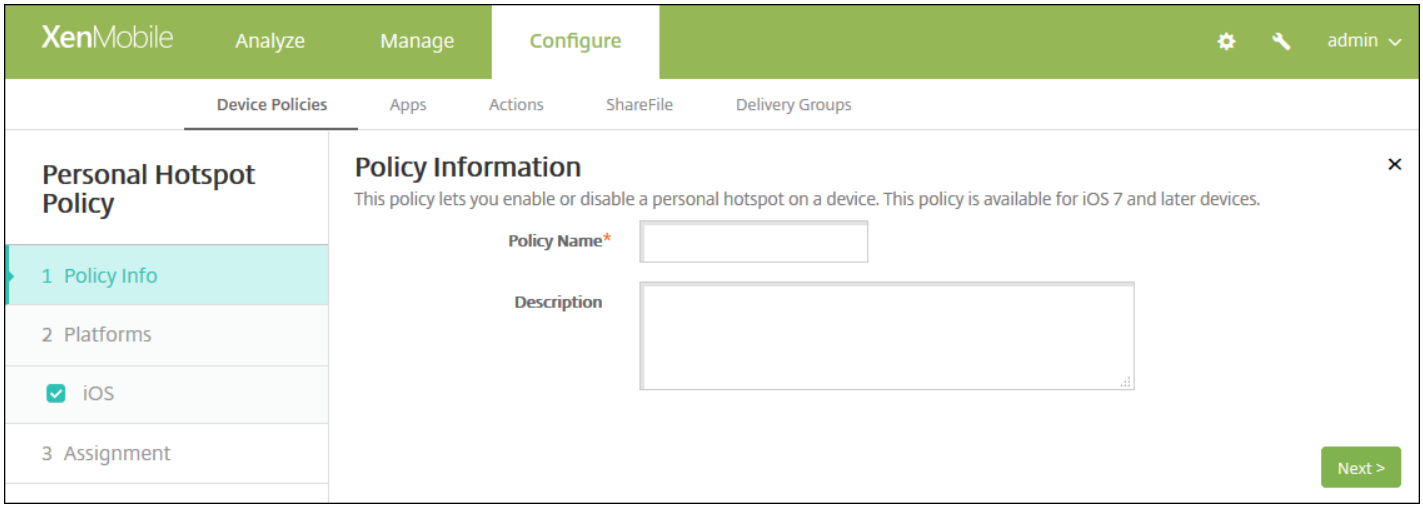
Aug 11, 2016

当用户不在 WiFi 网络范围内，可以允许用户通过其 iOS 设备的个人热点功能，使用手机数据网络连接到 Internet。 iOS 7.0 及以上版本支持此功能。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。 此时将显示**设备策略**页面。

2. 单击**添加**。 将显示**添加新策略**页面。

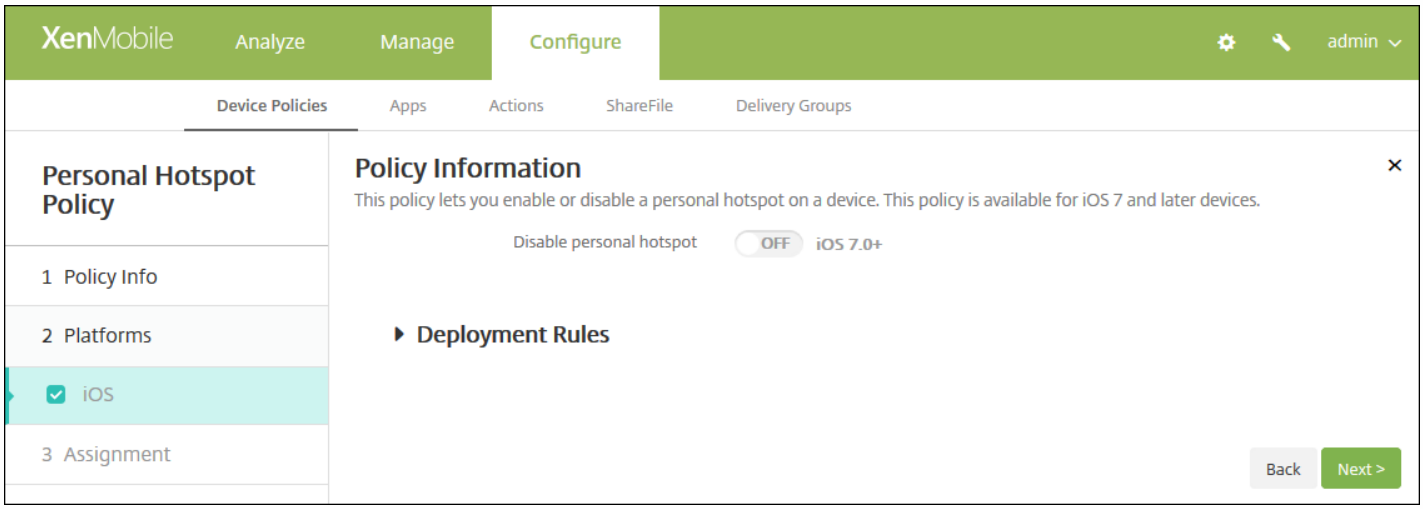
3. 展开**更多**，然后在**网络访问权限**下，单击**个人热点**。 将显示**个人热点策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台**信息页面。



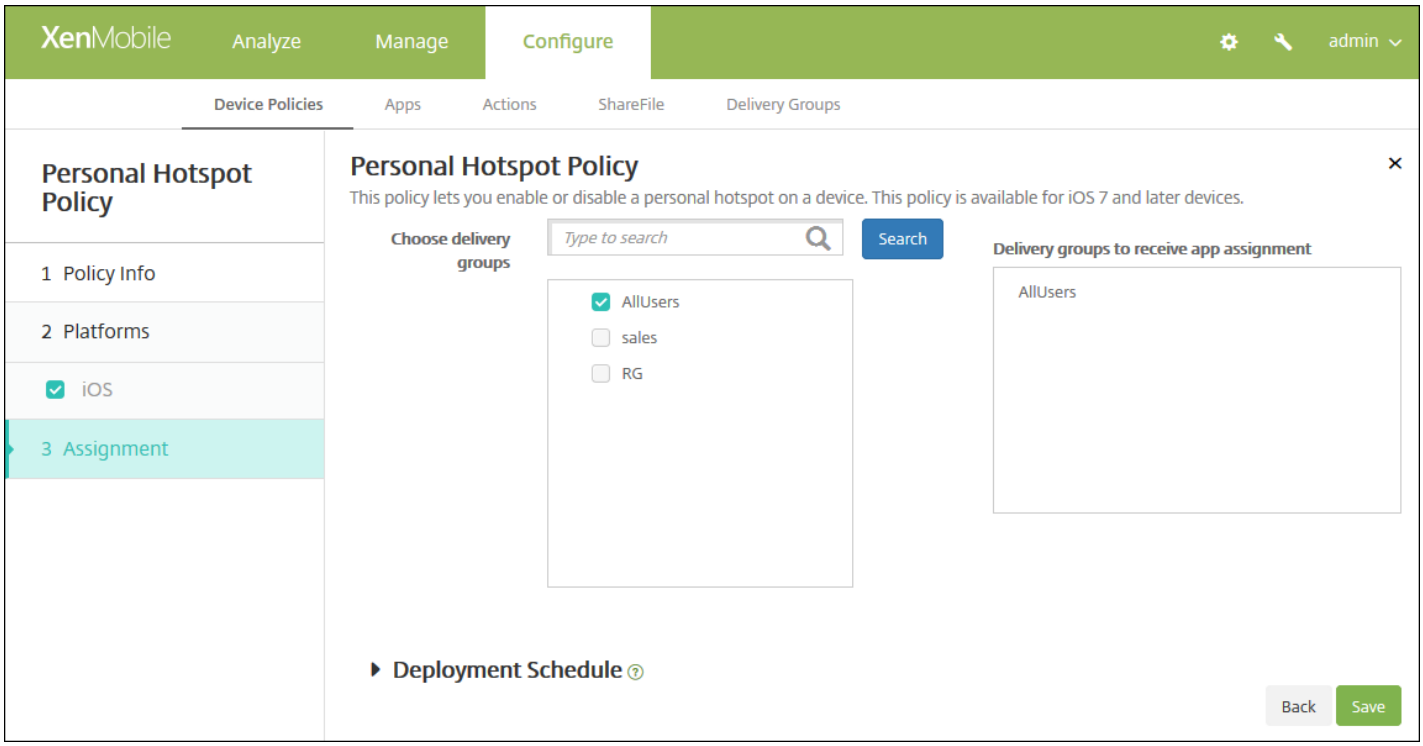
© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 配置以下设置：

- **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**，即在用户设备上关闭个人热点。 此策略不禁用该功能；用户仍可以在其设备上使用个人热点，但是部署此策略后，将关闭个人热点功能，因此默认情况下不打开此功能。

7. 配置部署规则

8. 单击**下一步**。 将显示**个人热点策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置文件删除设备策略

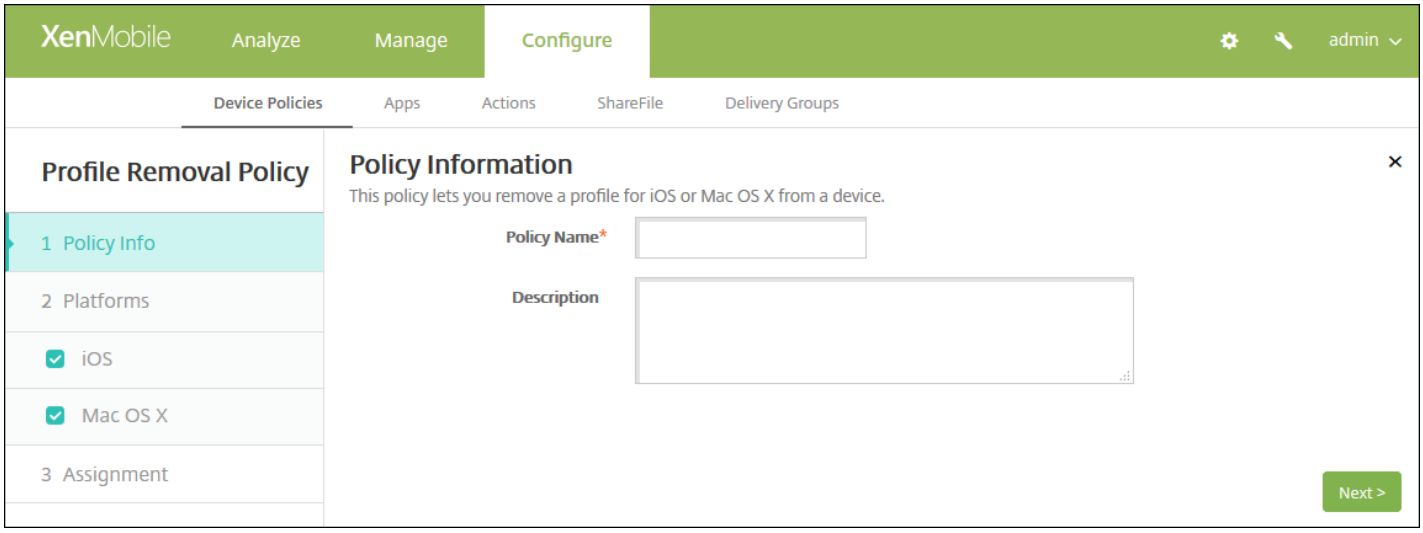
Aug 11, 2016

可以在 XenMobile 中创建应用程序配置文件删除设备策略。 此策略在部署时，将从用户的 iOS 或 Mac OS X 设备删除应用程序配置文件。

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**删除**下面，单击**配置文件删除**。 将显示**配置文件删除策略**信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

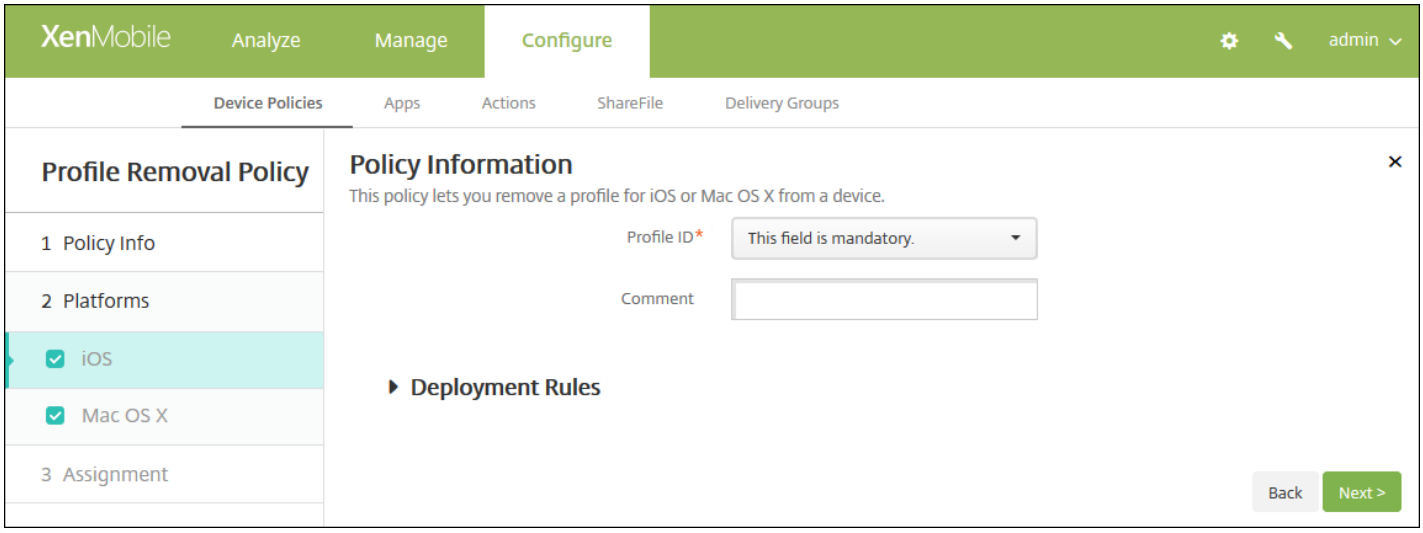
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

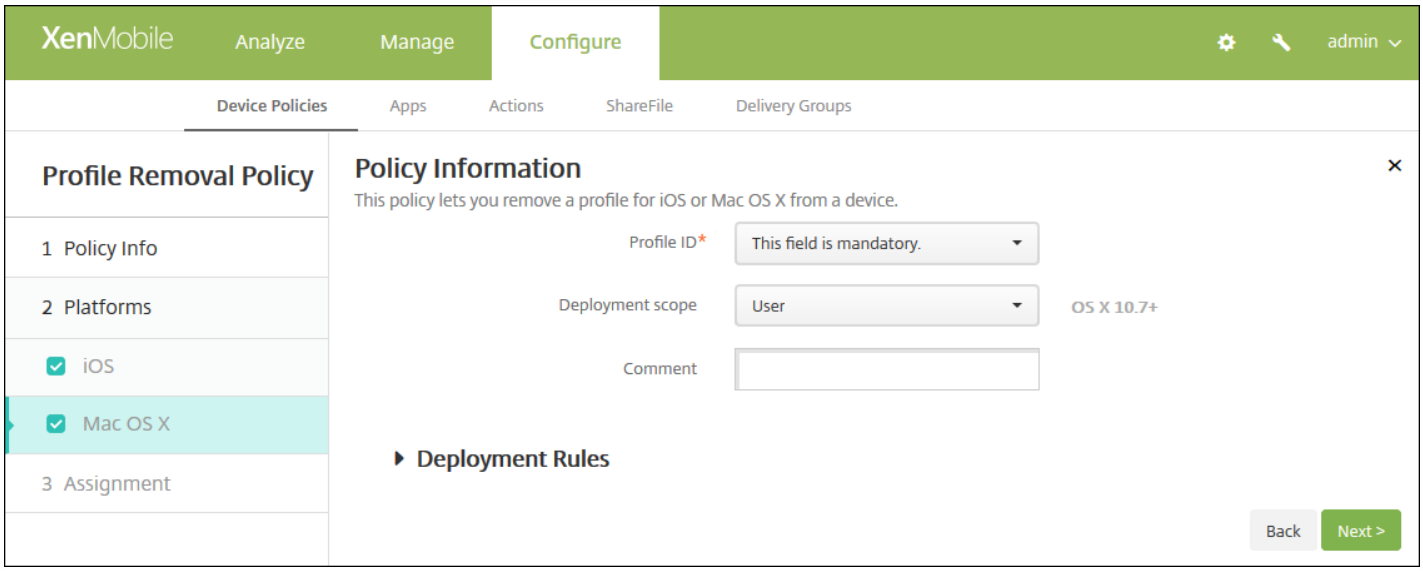
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **配置文件 ID**：在列表中，单击应用程序配置文件 ID。 此字段为必填字段。
- **备注**：键入可选备注。

配置 Mac OS X 设置



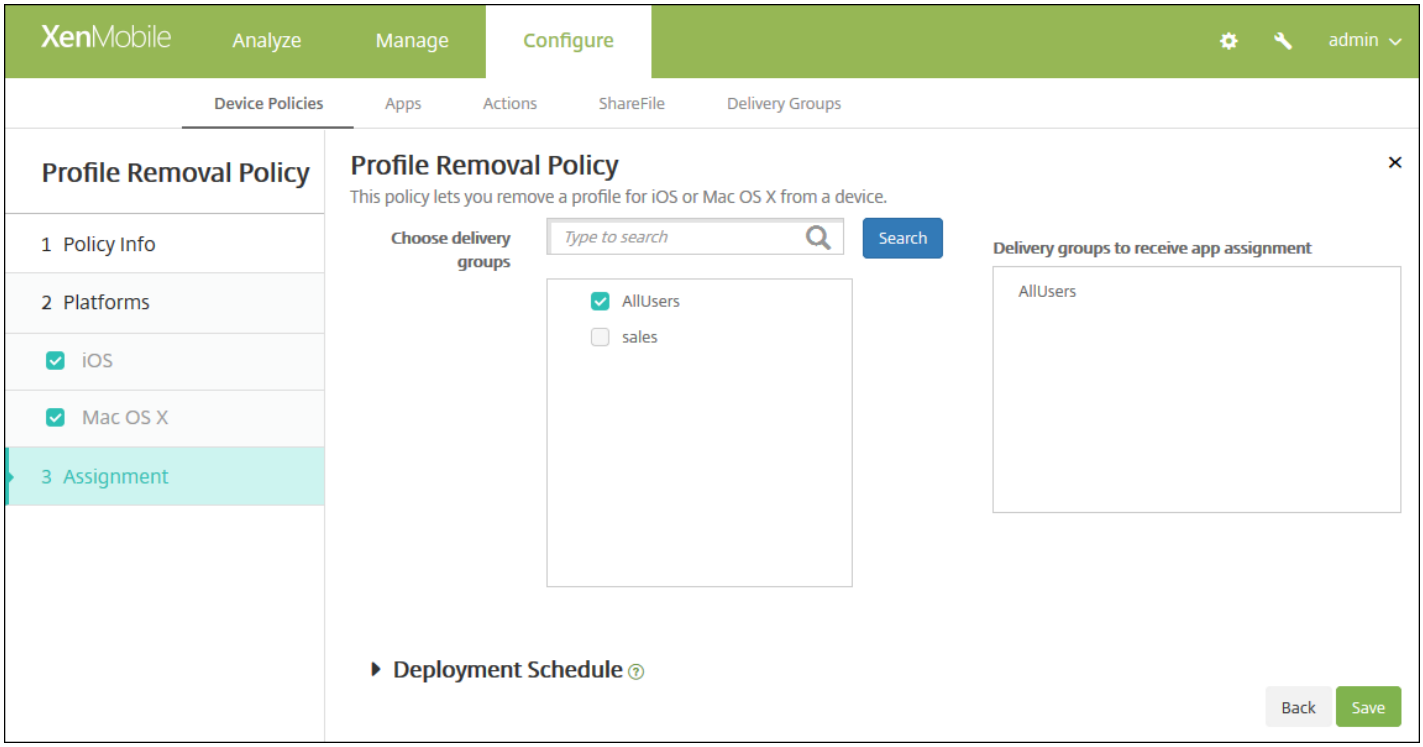
配置以下设置：

- **配置文件 ID**：在列表中，单击应用程序配置文件 ID。 此字段为必填字段。
- **部署范围**：在列表中，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。
- **备注**：键入可选备注。

7. 配置部署规则

8. 单击**下一步**。 将显示**配置文件删除策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所作的更改适用于所有平台，**为 始终启用 的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

置备配置文件设备策略

Aug 11, 2016

开发或代码签名 iOS 企业应用程序时，通常包含企业分发置备配置文件，Apple 需要此配置文件才能允许应用程序在 iOS 设备上运行。 如果置备配置文件缺失或已过期，用户轻按应用程序以将其打开时，应用程序将崩溃。

置备配置文件的主要问题是，它们在 Apple 开发人员门户上生成一年之后将过期，您必须跟踪用户注册的所有 iOS 设备上的所有置备配置文件的过期日期。 跟踪过期日期不仅涉及到跟踪实际的过期 日期， 还要跟踪每个用户正在使用的应用程序版本。 有两个解决方案：通过电子邮件向用户发送置备配置文件，或者将其放在 Web 门户上供下载和安装。 这些解决方案可行，但容易出错，因为需要用户响应电子邮件中的说明，或访问 Web 门户并下载正确的配置文件，然后再进行安装。

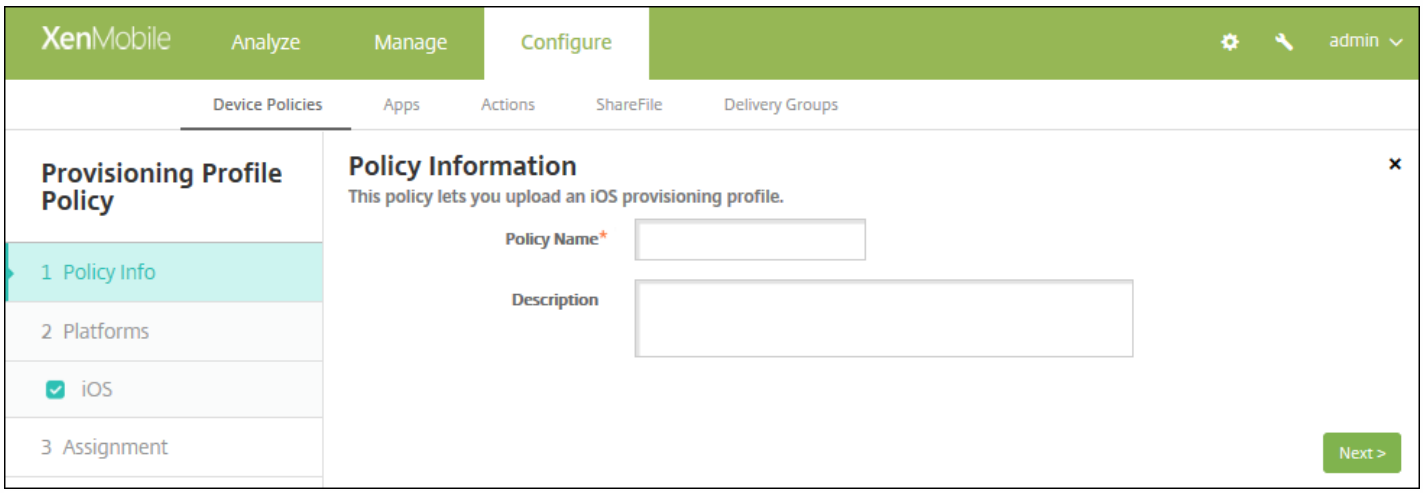
要使此过程对用户透明，您可以在 XenMobile 使用设备策略来安装和删除置备配置文件。 在必要时删除缺失或过期的配置文件并在用户 设备 上安装最新的配置文件，这样一来，只需轻按应用程序，即可将其打开并使用。

创建置备配置文件策略之前，必须创建置备配置文件。 有关详细信息，请参阅 Apple 开发人员站点上的 Creating Provisioning Profiles（创建置备配置文件）。

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**。 将显示**添加新策略**页面。

3. 展开**更多**，然后在**应用程序**下面，单击**置备配置文件**。 此时将显示**置备配置文件策略**信息页面。

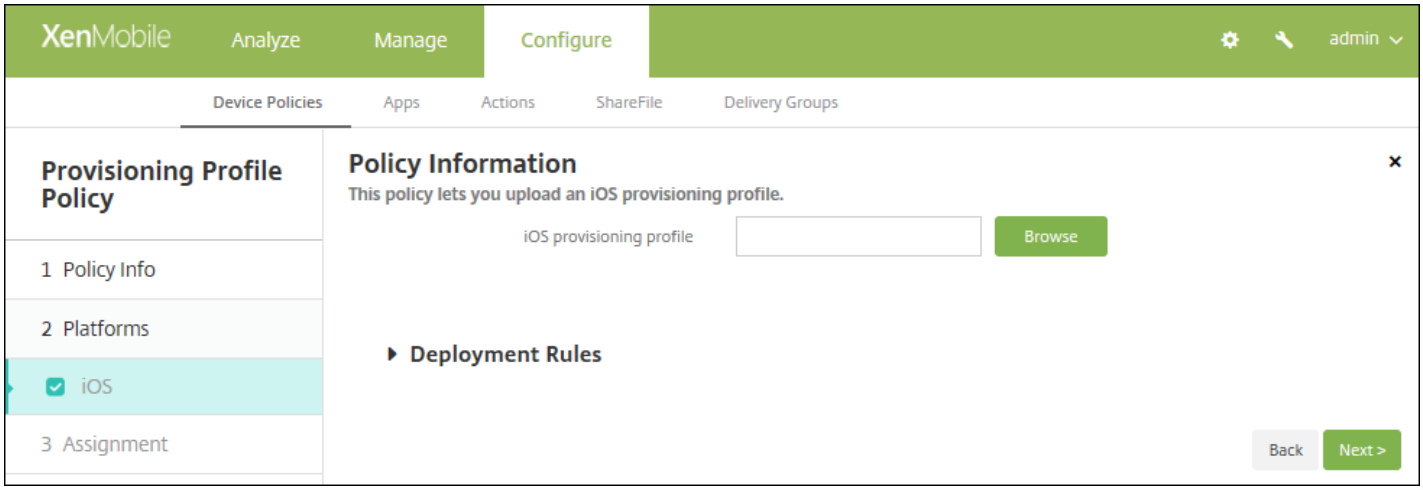


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

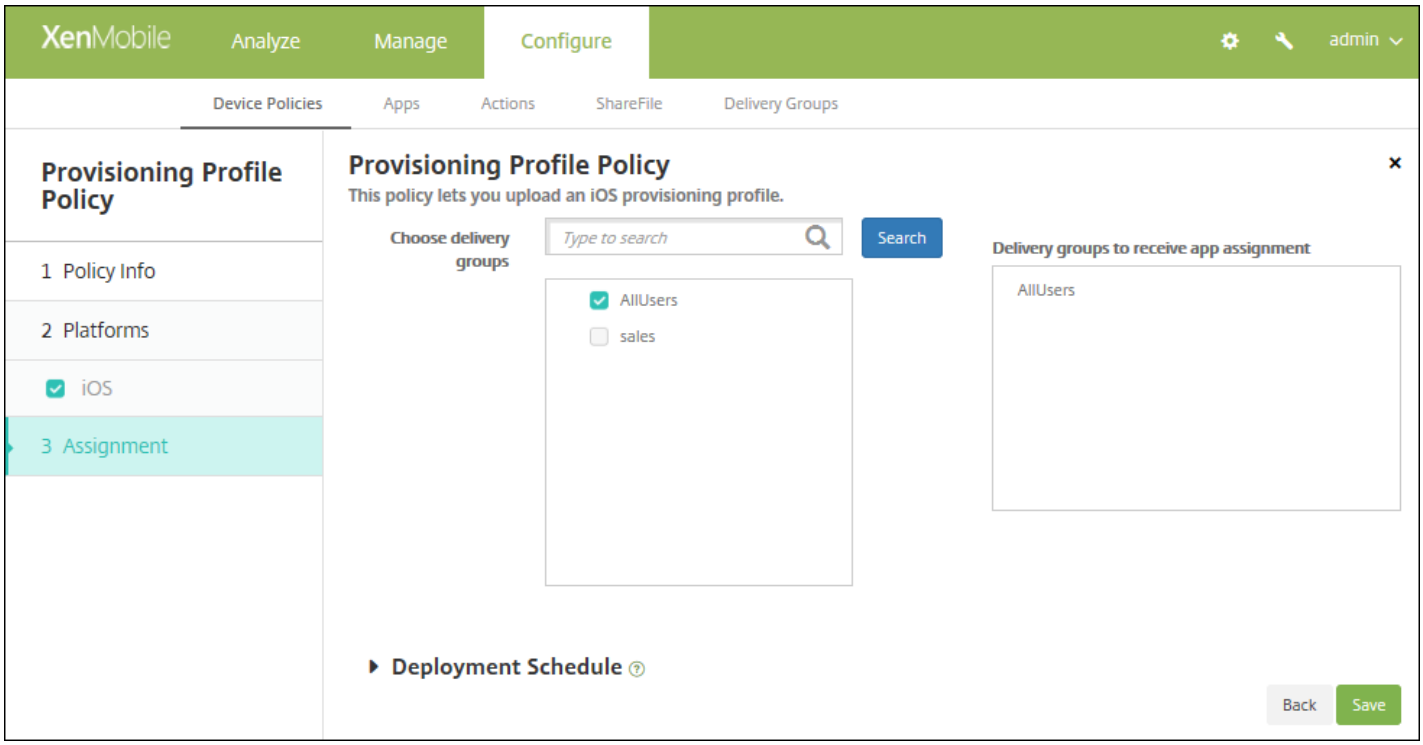


6. 配置以下 设置：

- **iOS 置备配置文件**：单击**浏览**，然后导航到要导入的置备配置文件所在的位置，选择此文件。

7. 配置部署规则

8. 单击**下一步**。 此时将显示置**备配置文件策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 如果单击**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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

删除置备配置文件设备策略

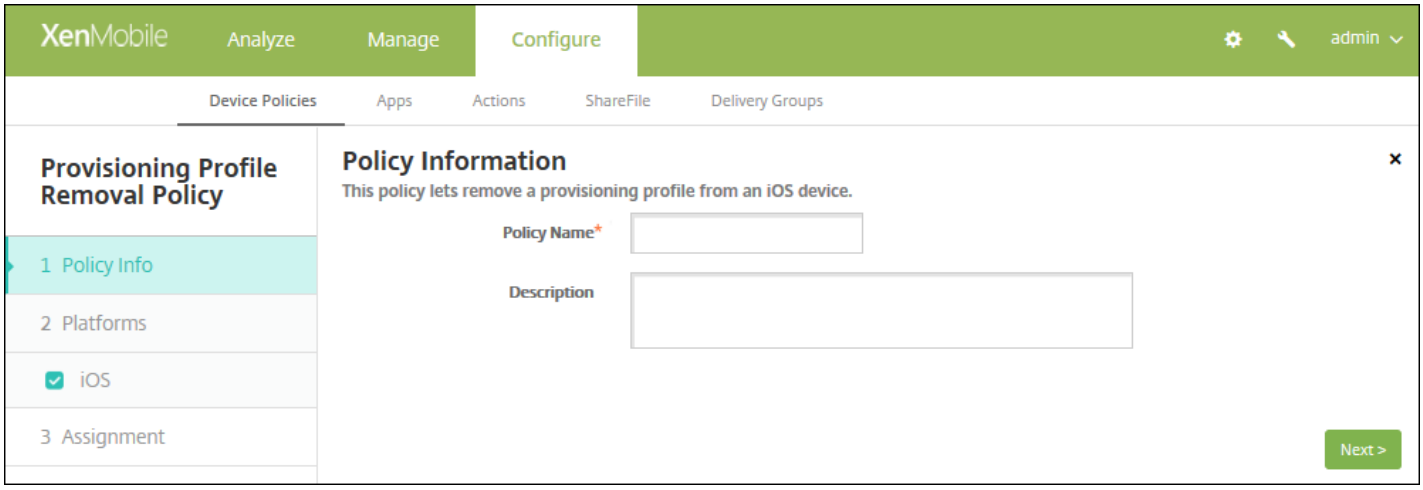
Aug 11, 2016

您可以通过设备策略删除 iOS 置备配置文件。 有关置备配置文件的详细信息，请参阅添加置备配置文件。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。 此时将显示**设备策略**页面。

2. 单击**添加**。 此时将显示**添加新策略**页面。

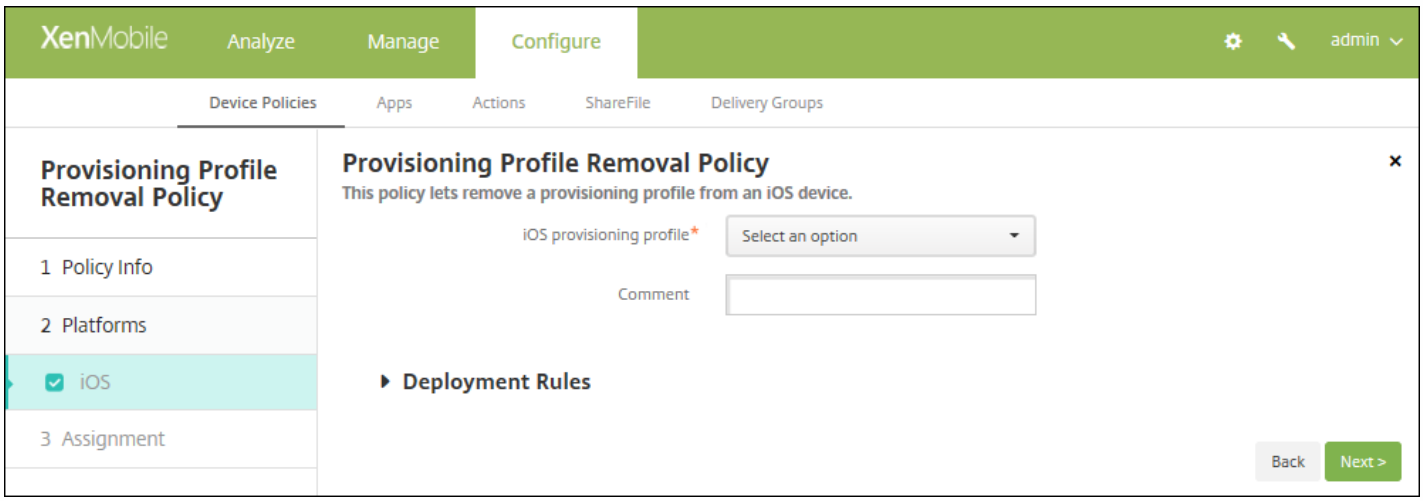
3. 展开**更多**，然后在**删除**下面，单击**删除置备配置文件**。 此时将显示**置备配置文件删除策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台**页面。



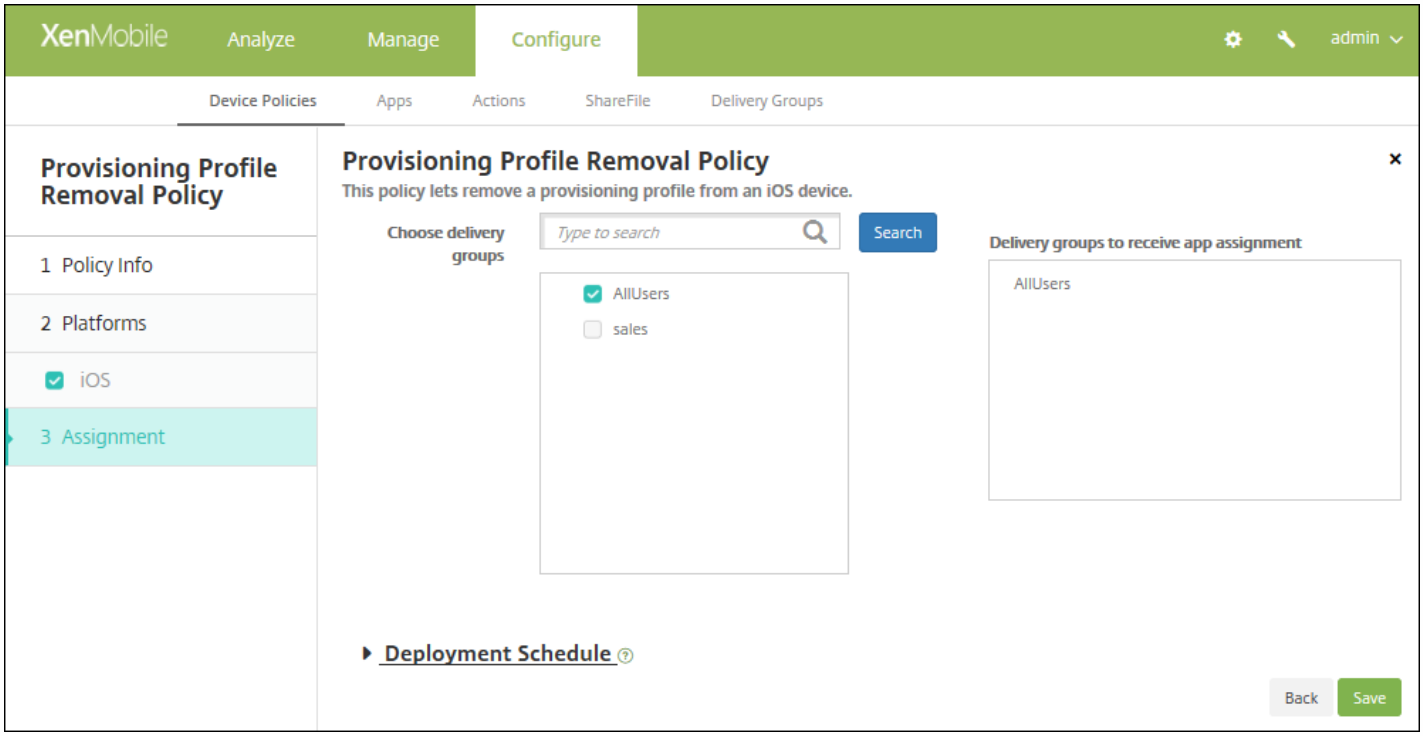
6. 配置以下设置：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **iOS 置备配置文件**：在列表中，单击要删除的置备配置文件。
- **备注**：可选，添加备注。

7. 配置部署规则

8. 单击**下一步**。 此时将显示置**备配置文件删除策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

代理设备策略

Aug 11, 2016

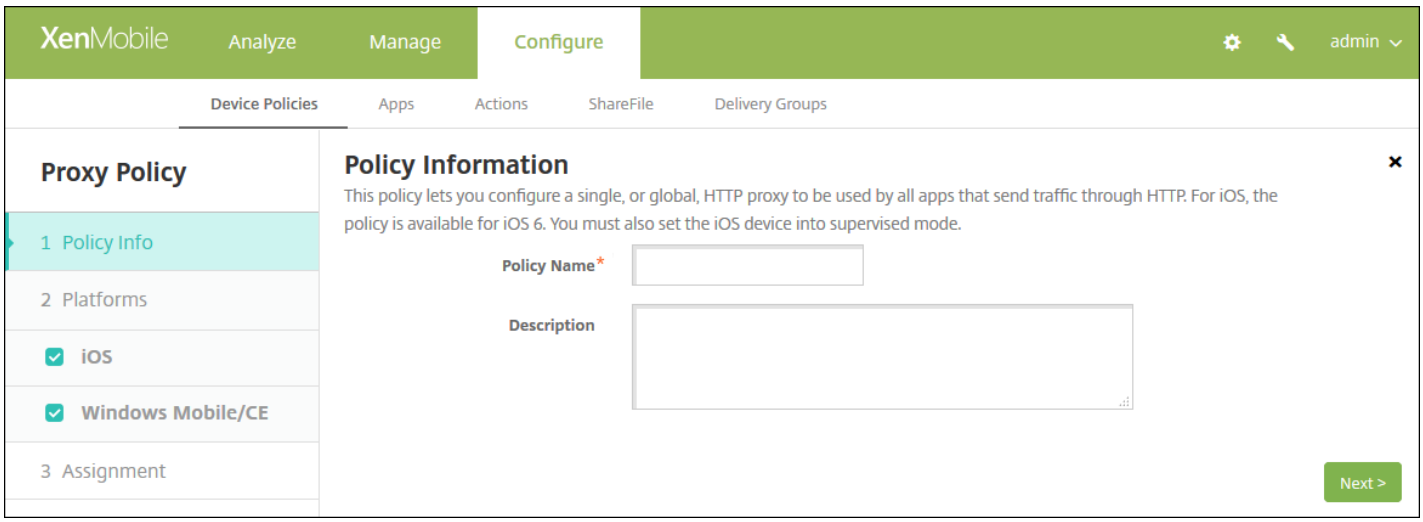
可以在 XenMobile 中添加一个设备策略，为运行 Windows Mobile/CE 和 iOS 6.0 或更高版本的设备指定全局 HTTP 代理设置。 只能为每个设备部署一个全局 HTTP 代理策略。

注意：在部署此策略之前，请务必将要设置全局 HTTP 代理的所有 iOS 设备设置为受监督模式。 有关详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

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. 单击**更多**，然后在**网络访问权限**下面，单击**代理**。 此时将显示 **Proxy Policy**（代理策略）页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：输入策略的描述性名称。
- **说明**：选择性输入策略的说明。

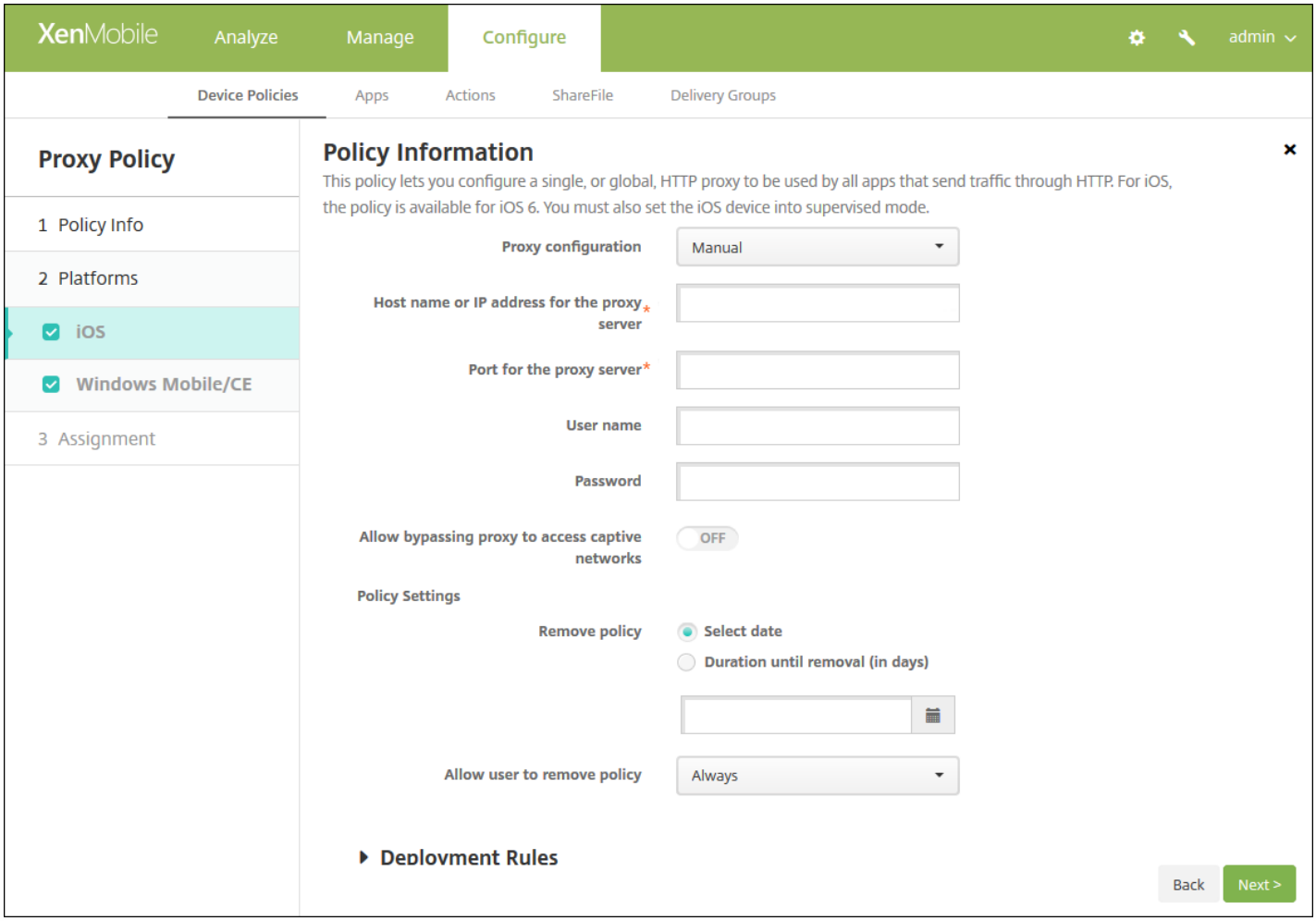
5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

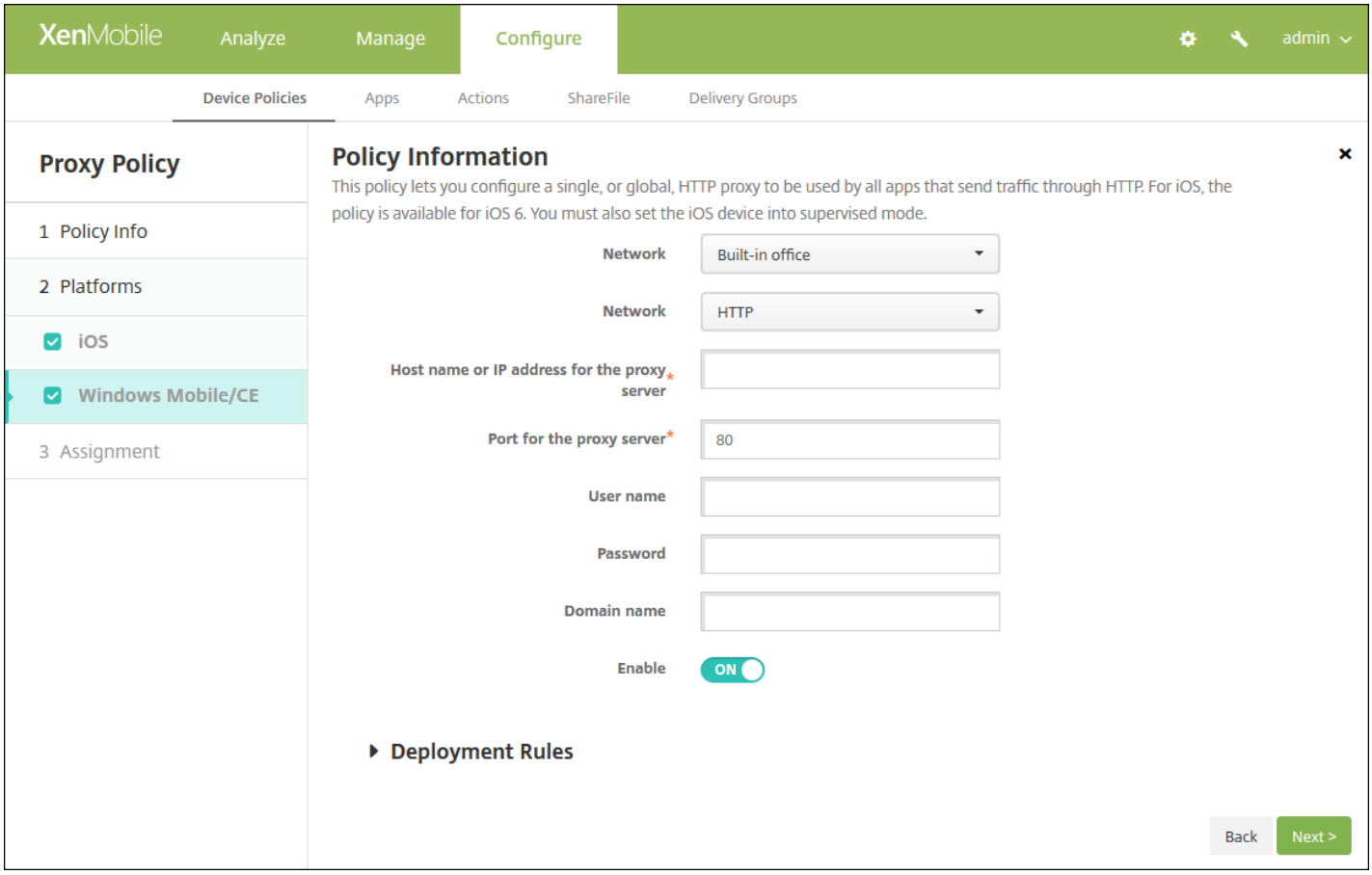


配置以下设置：

- **代理配置**：单击**手动**或**自动**以设置代理在用户设备上的配置方式。
  - 如果选择**手动**，可以配置以下设置：
    - **代理服务器的主机名或 IP 地址**：键入代理服务器的主机名或 IP 地址。 此字段为必填字段。
    - **代理服务器的端口**：键入代理服务器的端口号。 此字段为必填字段。
    - **用户名**：键入向代理服务器进行身份验证的可选用户名。
    - **密码**：键入向代理服务器进行身份验证的可选密码。
  - 如果单击**自动**，可以配置以下设置：
    - **代理 PAC URL**：键入用于定义代理配置的 PAC 文件的 URL。
    - **允许在无法访问 PAC 时直接连接**：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。 默认值为**开**。 此选项仅适用于 iOS 7.0 及更高版本。
- **允许旁路代理以访问俘获型网络**：选择是否允许绕过代理来访问俘获型网络。 默认值为**关**。
- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Windows Mobile/CE 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



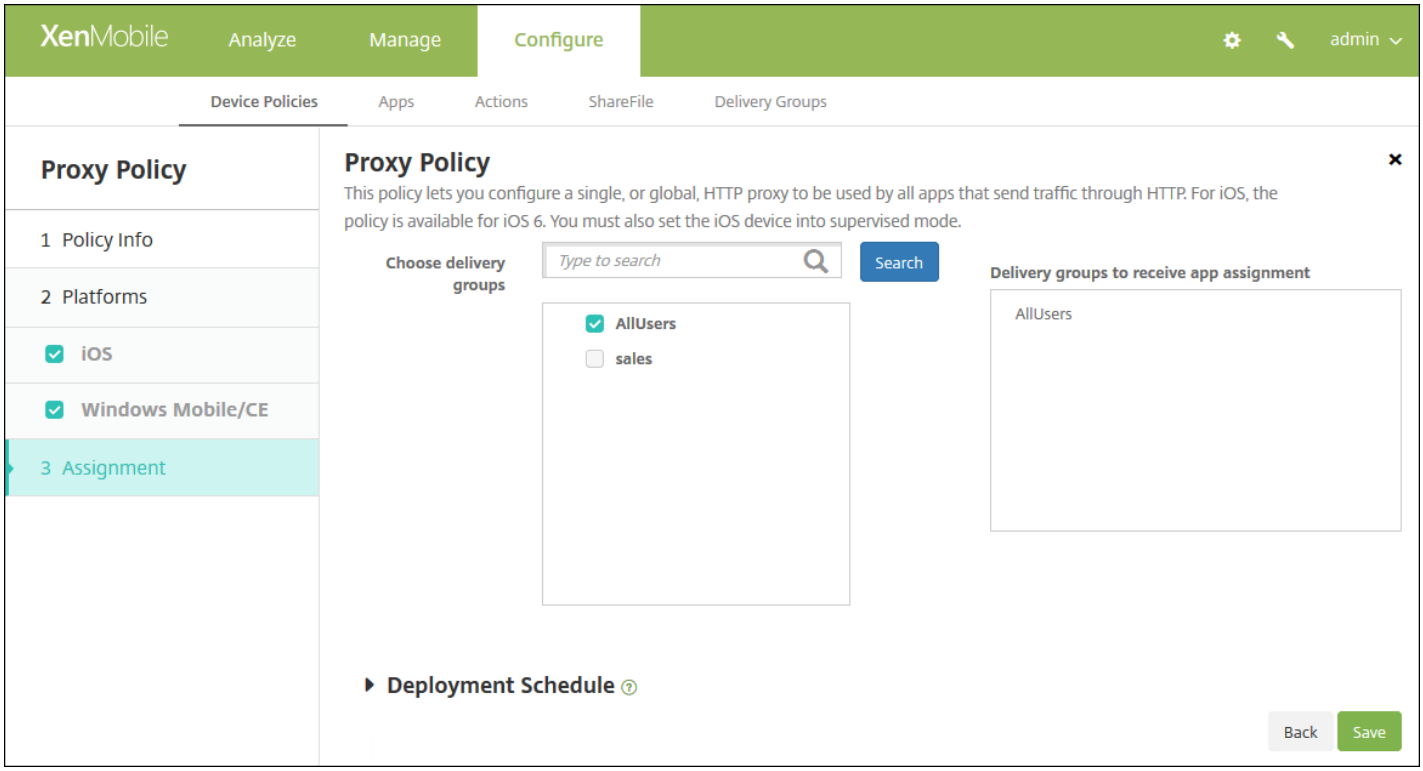
配置以下设置：

- **网络**：在列表中，单击要使用的网络类型。 默认值为**内置办公网络**。 可用选项包括：
  - 用户定义的办公网络
  - 用户定义的 Internet
  - 内置办公网络
  - 内置 Internet
- **网络**：在列表中，单击要使用的网络连接协议。 默认值为 **HTTP**。 可用选项包括：
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- **代理服务器的主机名或 IP 地址**：键入代理服务器的主机名或 IP 地址。 此字段为必填字段。
- **代理服务器的端口**：键入代理服务器的端口号。 此字段为必填字段。 默认值为 **80**。
- **用户名**：键入向代理服务器进行身份验证的可选用户名。
- **密码**：键入向代理服务器进行身份验证的可选密码。
- **域名**：键入可选域名。
- **启用**：选择是否启用代理。 默认值为**开**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Proxy Policy**（代理策略）分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注册表设备策略

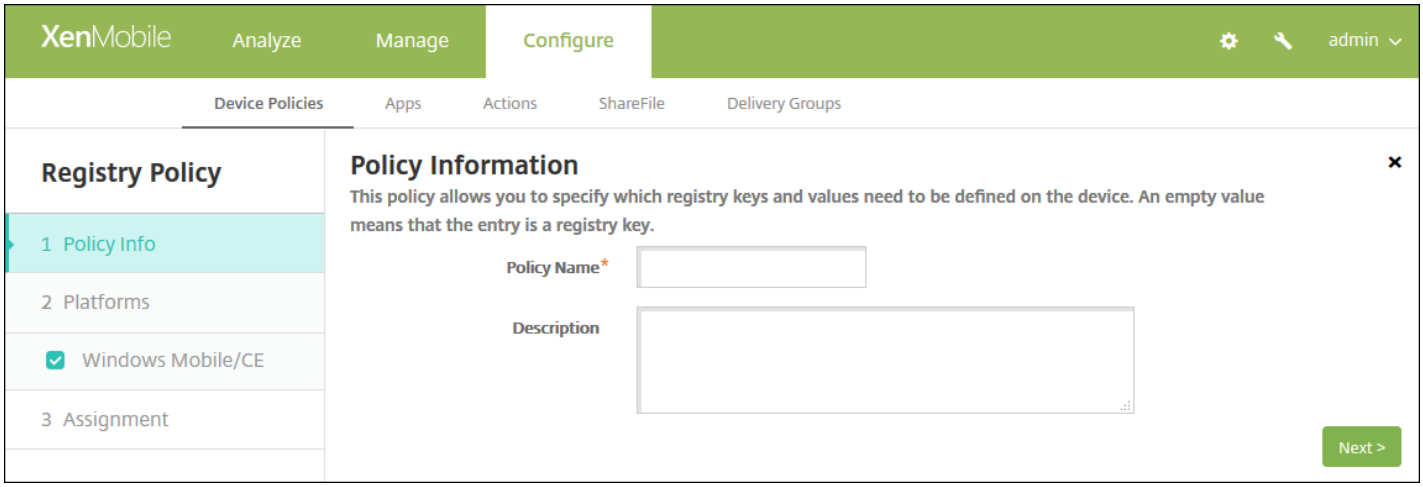
Aug 11, 2016

Windows Mobile/CE 注册表存储关于应用程序、驱动器、用户首选项和配置设置的数据。 在 XenMobile 中，可以定义用于管理 Windows Mobile/CE 设备的注册表项和值。

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。

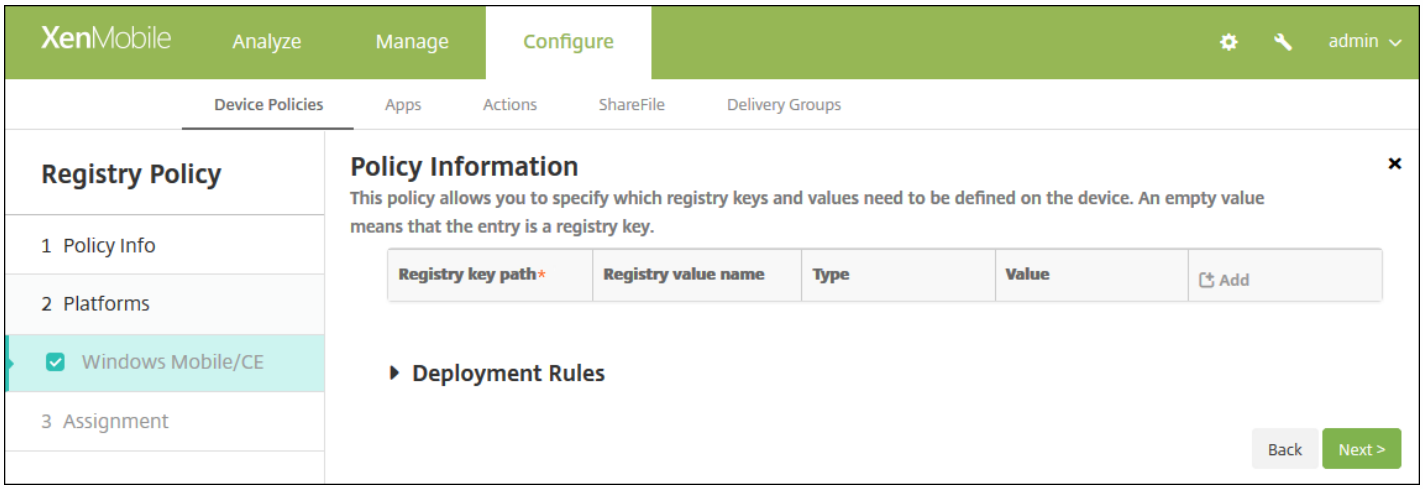
3. 展开**更多**，然后在**自定义**下面，单击**注册表**。 此时将显示 **注册表策略**信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Windows Mobile/CE 平台**页面。



6. 配置以下设置：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

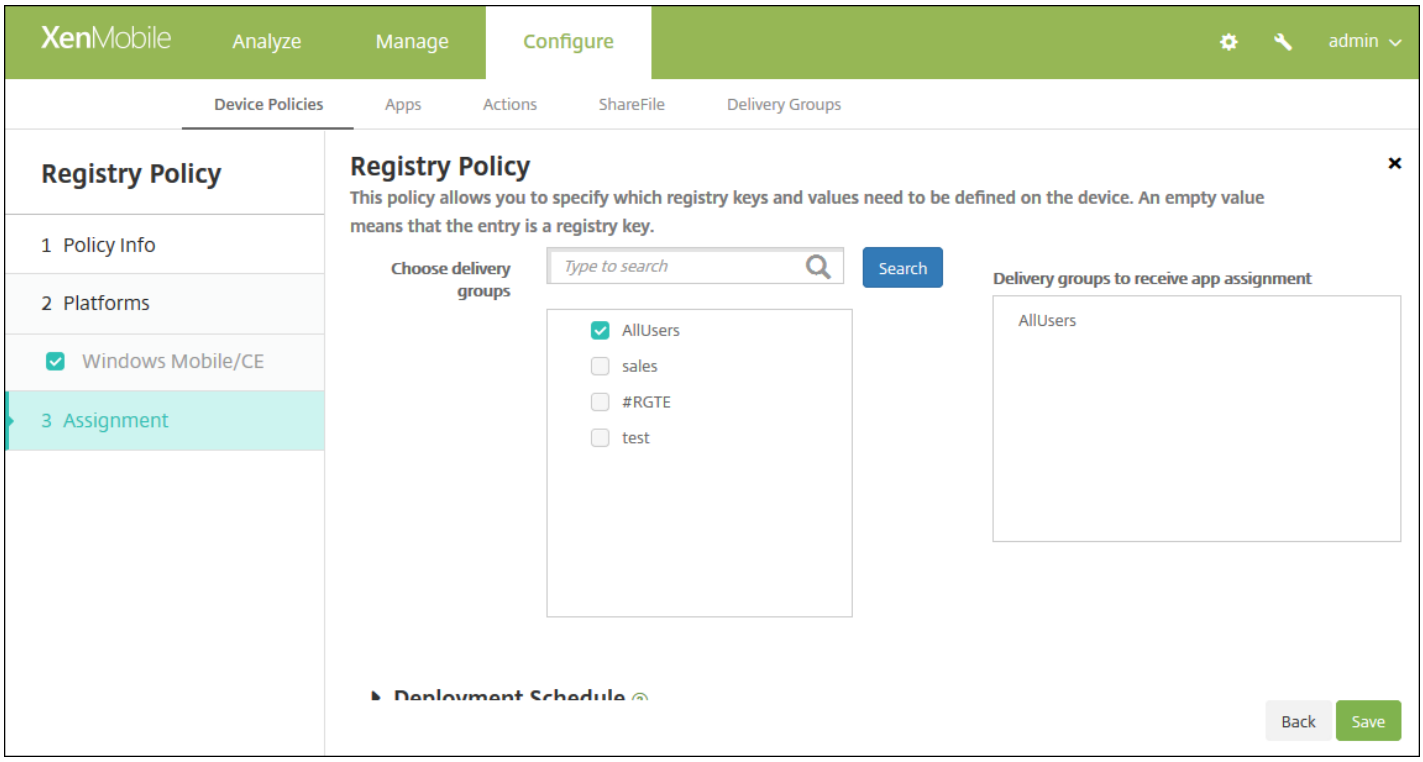
- 对于要添加的每个注册表项或注册表项/值对，请单击**添加**并执行以下操作：
- **注册表项路径**：键入注册表项的完整路径。 例如，键入 *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* 以指定从 HKEY_LOCAL_MACHINE 根注册表项到 Windows 注册表项的路由。
- **注册表值的名称**：键入注册表项值的名称。 例如，键入 *ProgramFilesDir* 将该值名称添加到注册表项路径 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion。 如果将此字段留空，表示将添加注册表项而非注册表项/值对。
- **类型**：在列表中，单击值的数据类型。 默认值为 **DWORD**。 可用选项包括：
  - **DWORD**：32 位无符号整数。
  - **字符串**：任意字符串。
  - **扩展字符串**：可以包含环境变量（如 %TEMP% 或 %USERPROFILE%）的字符串值。
  - **二进制**：任意二进制数据。
- **值**：键入与注册表值名称关联的值。 例如，要指定 ProgramFilesDir 的值，请键入 *C:\Program Files*。
- 单击**保存**以保存注册表项信息，或单击**取消**不保存注册表项信息。

  注意：要删除现有注册表项，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

  要编辑现有注册表项，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**注册表策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所作的更改适用于所有平台，**为 始终启用 的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

远程支持设备策略

Aug 11, 2016

可以在 XenMobile 中创建远程支持策略以授予远程访问用户的 Samsung KNOX 设备所需的权限。 可以配置两种类型的支持：

- **基本**：使用此选项，您可以查看与设备有关的诊断信息（例如系统信息）、正在运行的进程、任务管理器（内存和 CPU 使用率）、已安装的软件文件夹内容等。
- **高级**：使用此选项，您可以远程控制设备的屏幕，包括控制颜色（在主窗口中或者在独立的浮动窗口中）、在技术支持人员与用户之间建立 VoIP 会话、配置设置以及在技术支持人员与用户之间建立文字消息会话的功能。

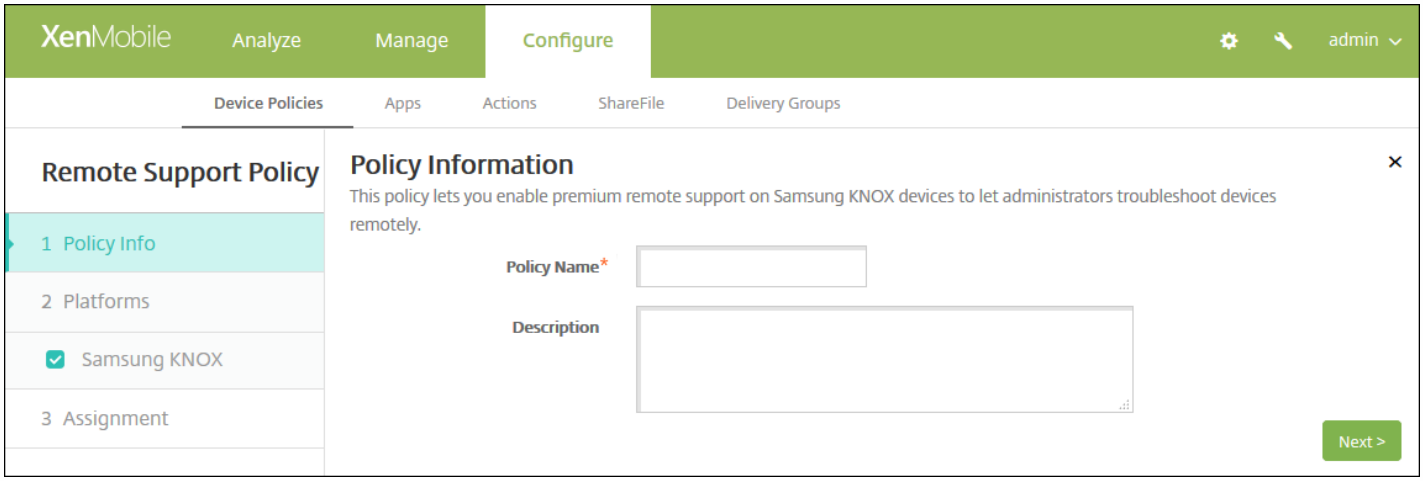
注意：要实施此策略，必须执行以下操作：

- 在您的环境中安装 XenMobile Remote Support 应用程序。
- 配置远程支持应用程序通道。 有关详细信息，请参阅应用程序通道设备策略。
- 按本主题中所述配置 Samsung KNOX 远程支持设备策略。
- 同时对用户设备部署应用程序通道远程支持策略和 Samsung KNOX 远程支持策略。

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**网络访问权限**下，单击**远程支持**。 此时将显示 **Remote Support Policy**（远程支持策略）页面。

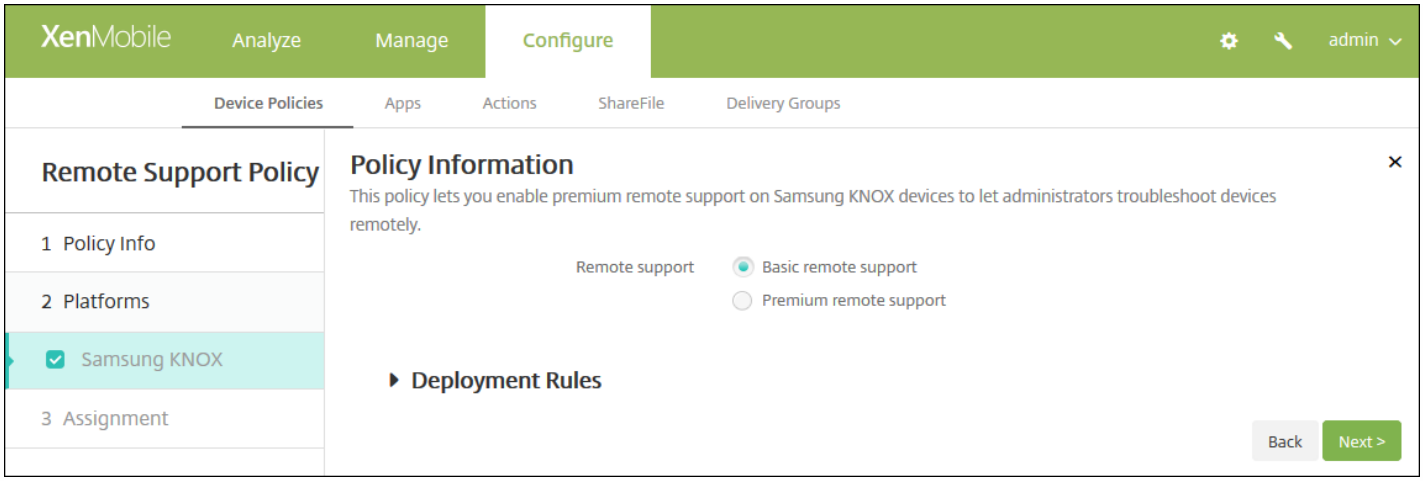


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **Samsung KNOX** 平台信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

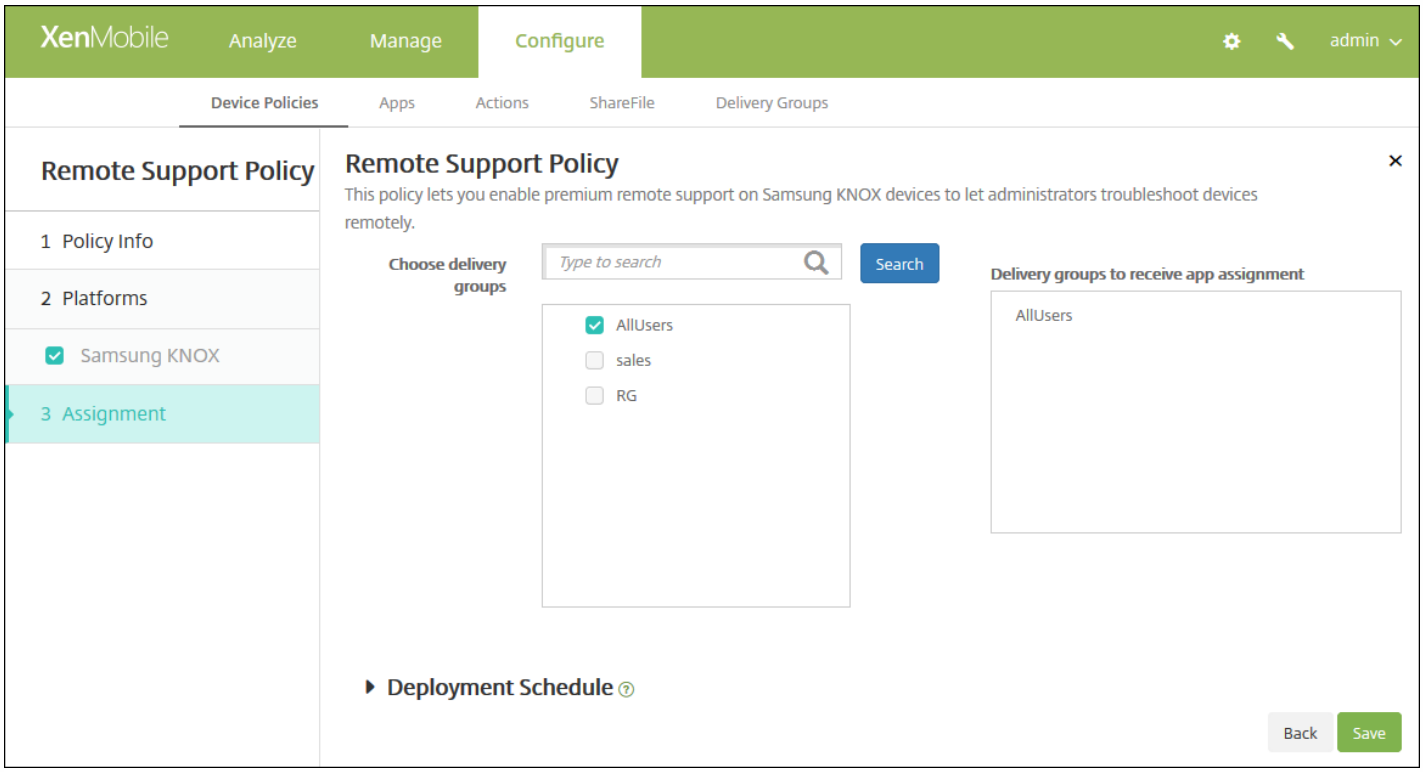


6. 配置以下设置：

- **远程支持**：选择**基本远程支持**或**高级远程支持**。 默认设置为**基本远程支持**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Remote Support Policy**（远程支持策略）分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 如果单击**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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

限制设备策略

Aug 11, 2016

可以在 XenMobile 中添加一个设备策略，以限制用户设备、手机、平板电脑等设备上的某些功能或特征。 可以配置适用于以下平台的设备限制策略：iOS、Mac OS X、Samsung SAFE、Samsung KNOX、Windows Tablet、Windows Phone、Amazon 和 Windows Mobile/CE。 每种平台需要一组不同的值，本文将对此进行介绍。

此策略允许或限制用户在其设备上使用某些功能，例如相机。 您还可以设置安全限制、对媒体内容的限制以及对用户能够和不能安装的应用程序类型的限制。 大多数限制设置的默认为**开**或*允许*。 主要的例外情况是 iOS 安全 - 强制功能和所有 Windows Tablet 功能，其默认设置为**关**或*限制*。

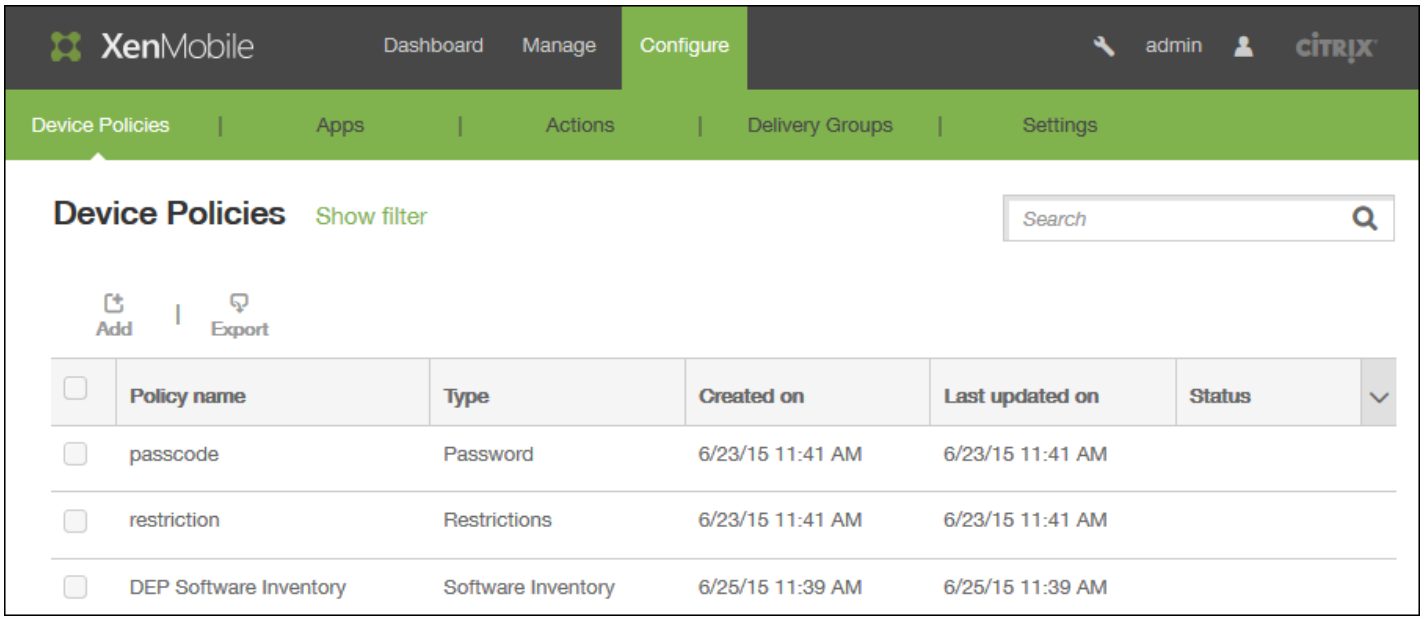
提示：如果您为任何选项选择**开**，则意味着用户

— 可以

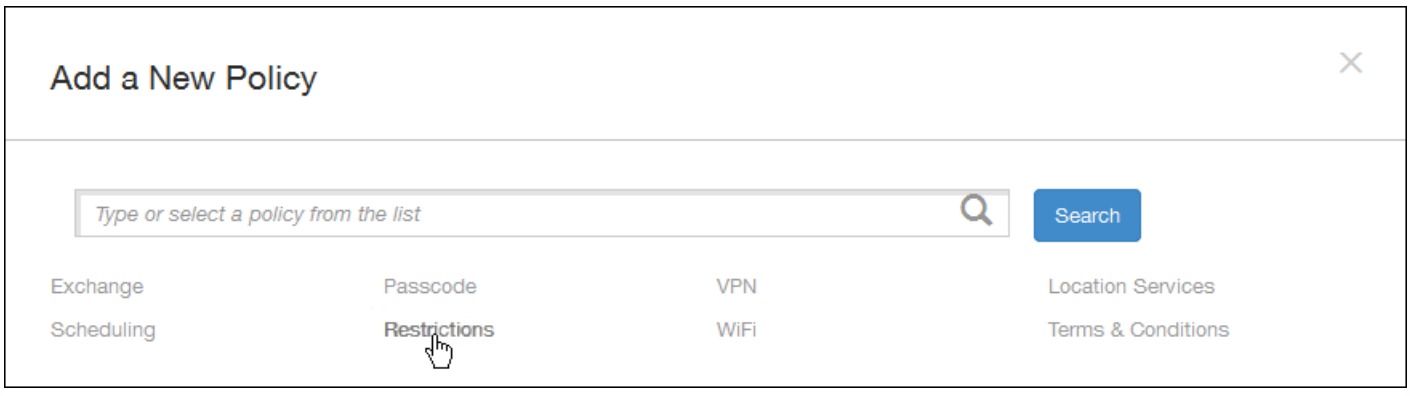
执行该操作或使用该功能。 例如：

- **相机**。 如果选择开**开**，用户将可以使用其设备上的相机。 如果选择**关**，用户将无法使用其设备上的相机。
- **屏幕快照**。 如果选择**开**，则设备用户可以在设备上创建屏幕快照。 如果选择**关**，则设备用户无法在设备上创建屏幕快照。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**将显示**设备策略**页面。

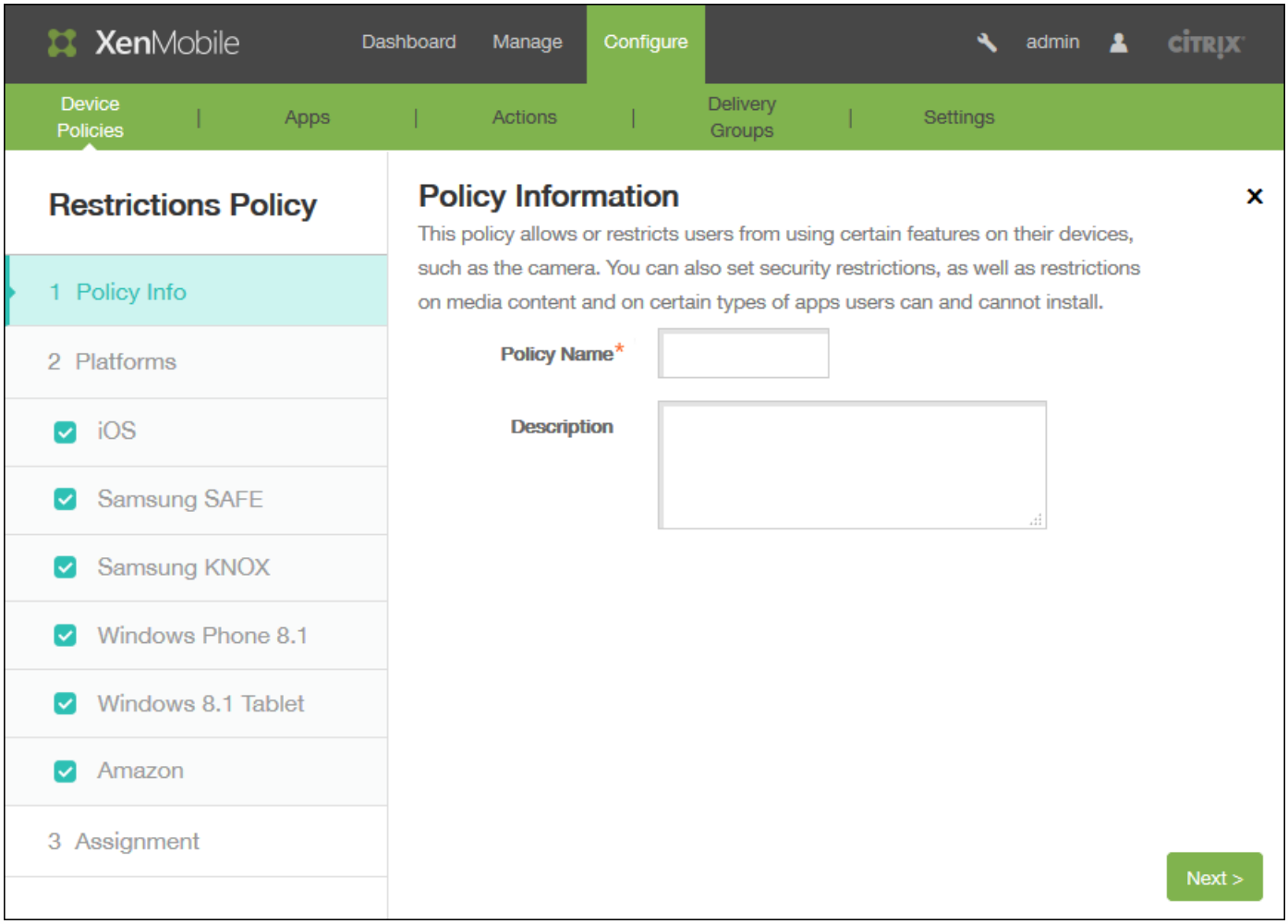


2.单击**添加**。将出现**添加新策略**页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 单击**限制**。将出现限制**策略信息**页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

4. 单击**下一步**。 此时将显示**策略平台**页面。

5. 在**平台**中，选择要添加的一个或多个平台。可以更改您选择的每个平台的策略信息。 在下面的步骤中，单击以将设置更改为**关**，从而限制相应功能。 除非另有说明，否则默认设置为启用该功能。

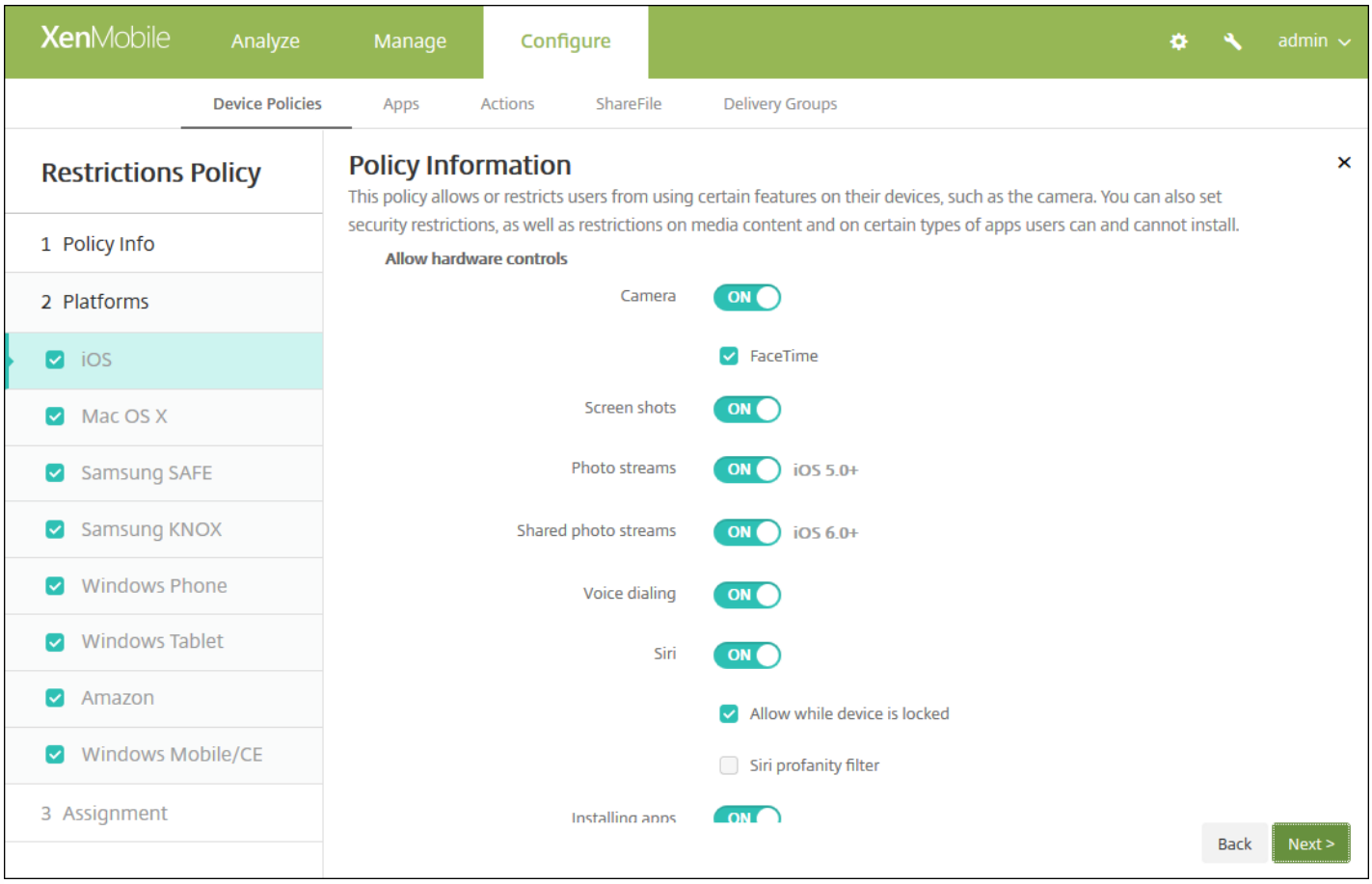
如果选择：

iOS，配置这些设置
Mac OS X，配置这些设置
Samsung SAFE，配置这些设置
Samsung KNOX，配置这些设置
Windows Phone，配置这些设置
Windows 平板电脑，配置这些设置
Amazon，配置这些设置
Windows Mobile/CE，配置这些设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

设置完平台限制后，请参阅本文后面的步骤 7 以了解如何设置此平台的部署规则。

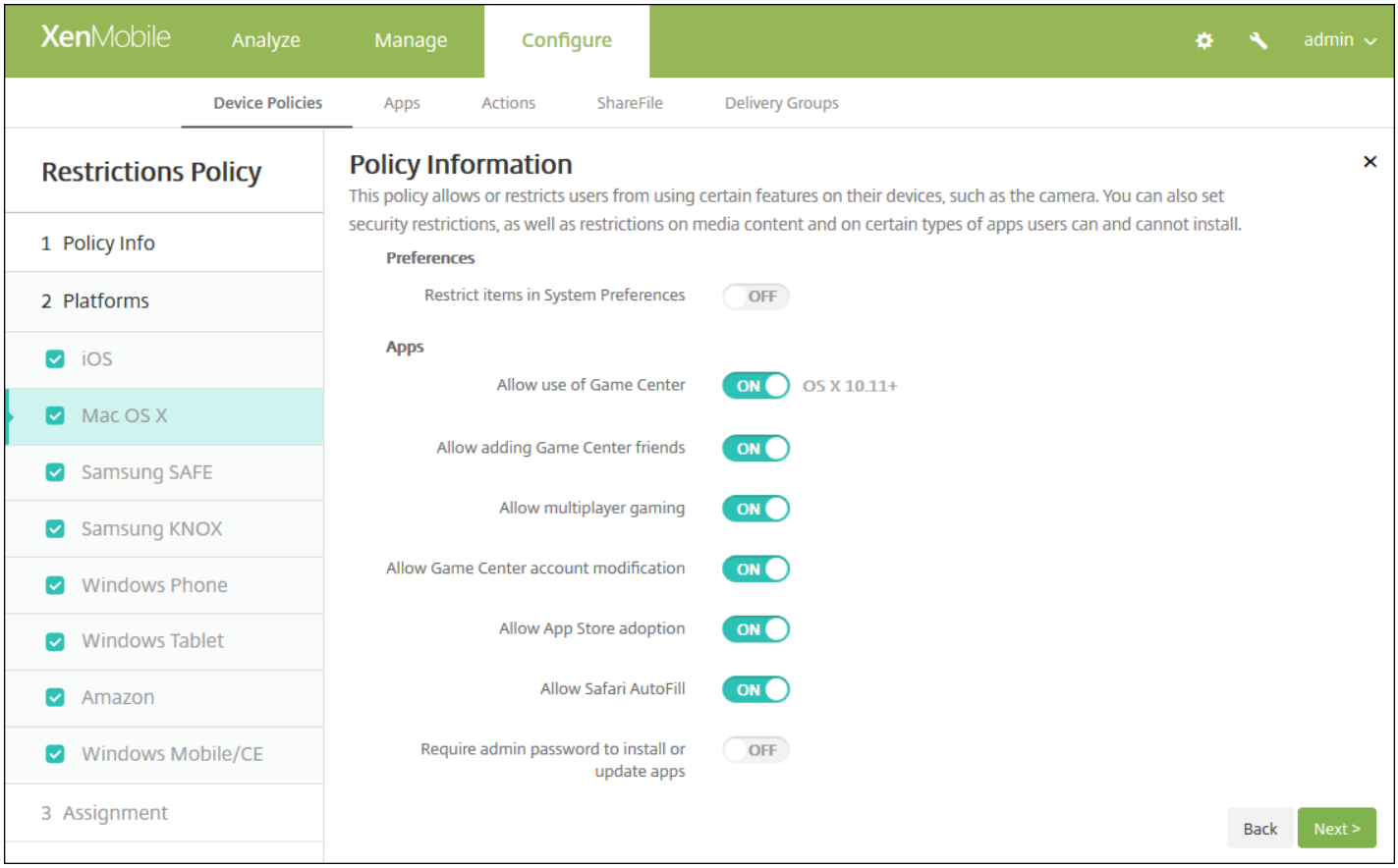
如果选择 iOS，可以配置以下设置



iOS 设置

配置 Mac OS X 设置

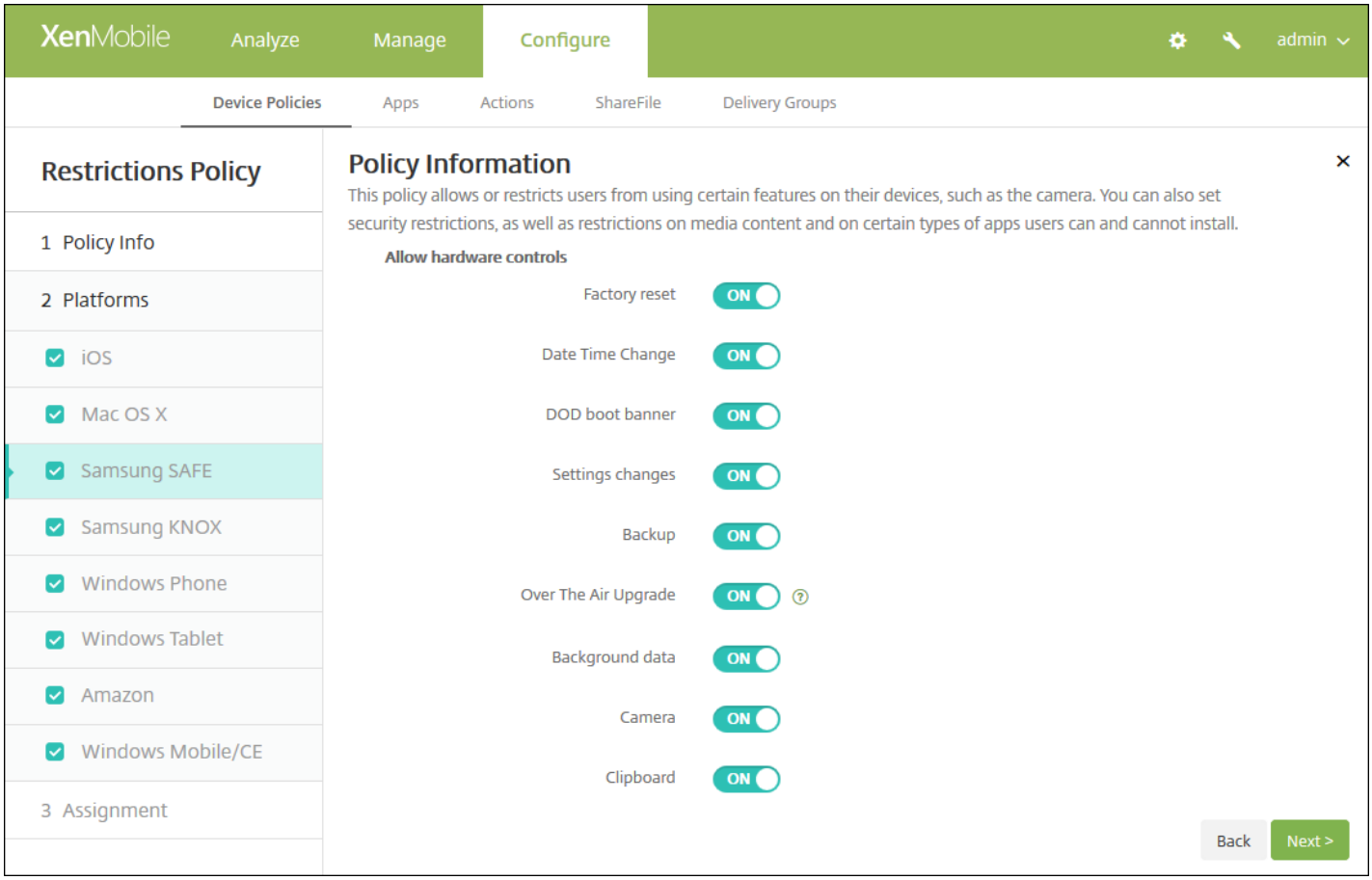
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Mac OS X 设置

配置 Samsung SAFE 设置

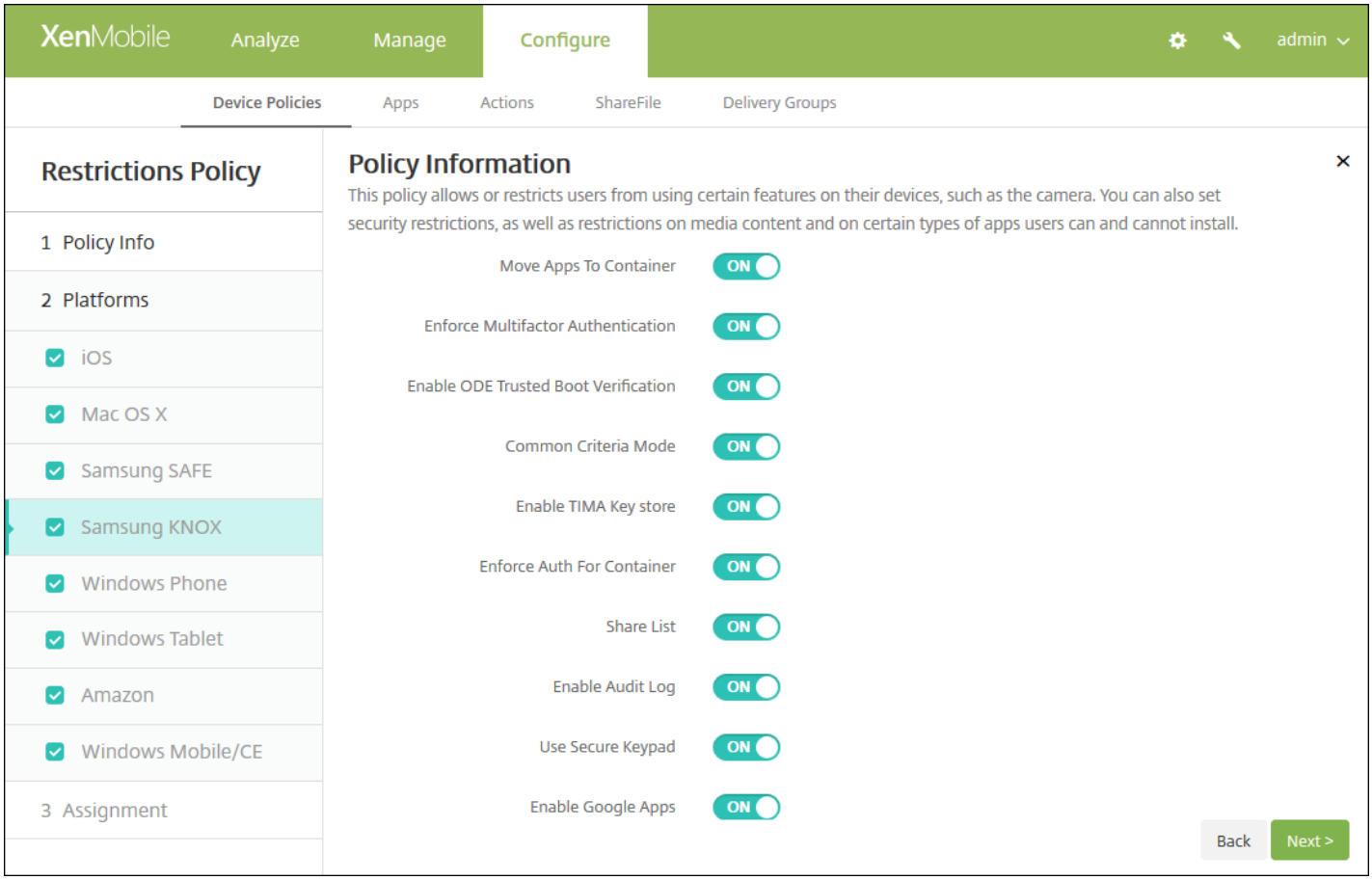
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Samsung SAFE 设置

配置 Samsung KNOX 设置

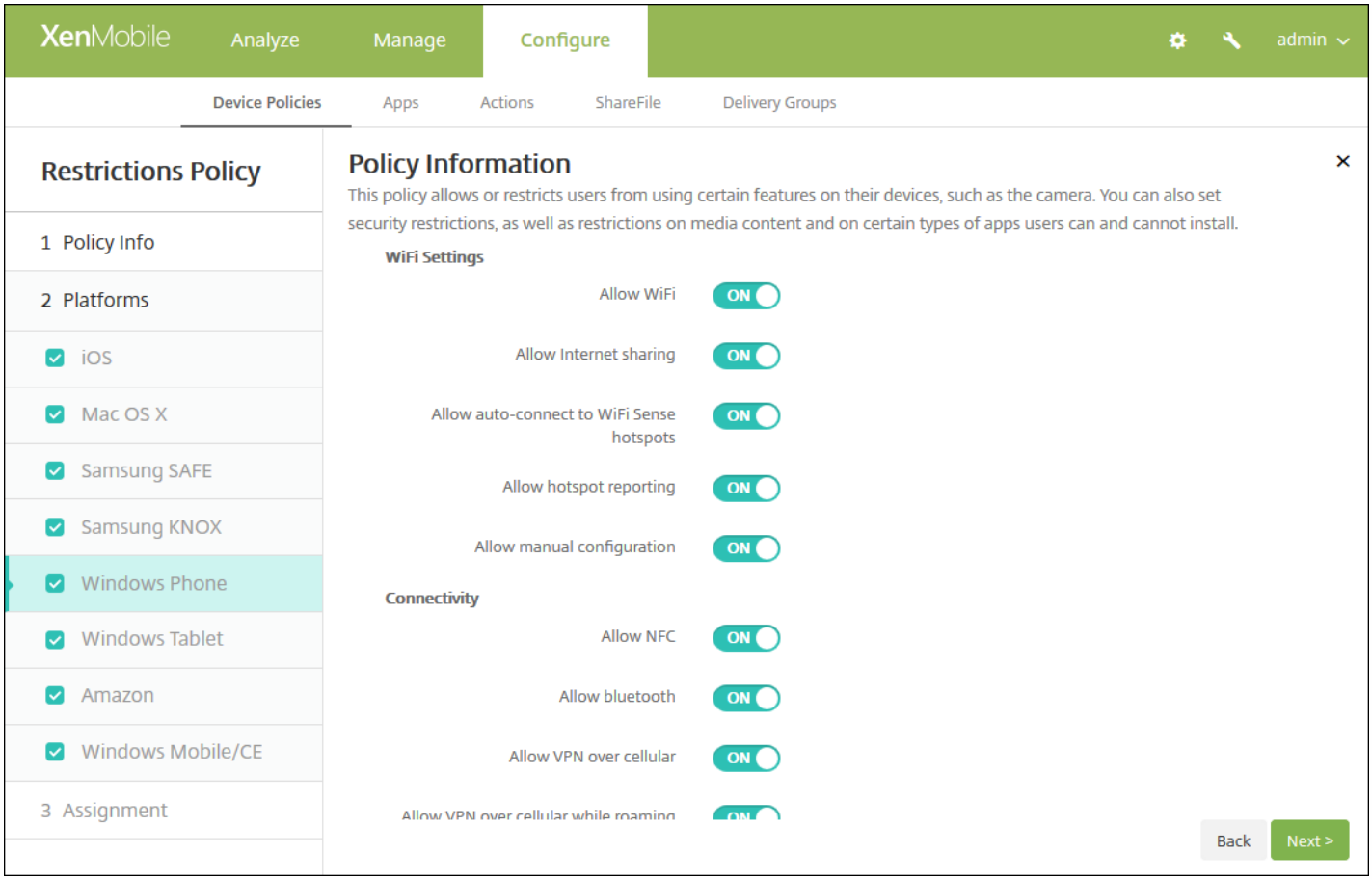
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Samsung KNOX 设置

配置 Windows Phone 设置

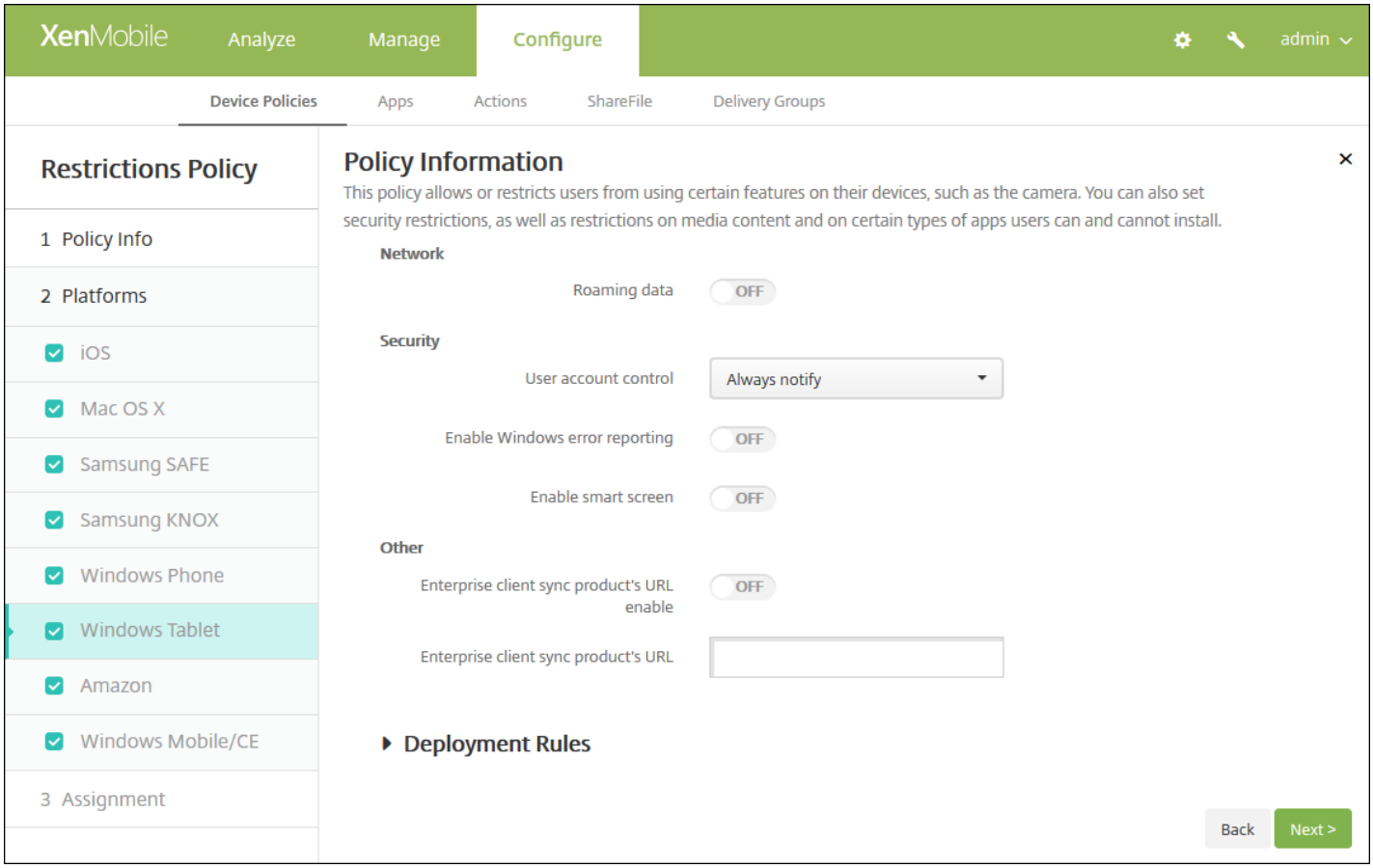
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Windows Phone 设置

配置 Windows Tablet 设置

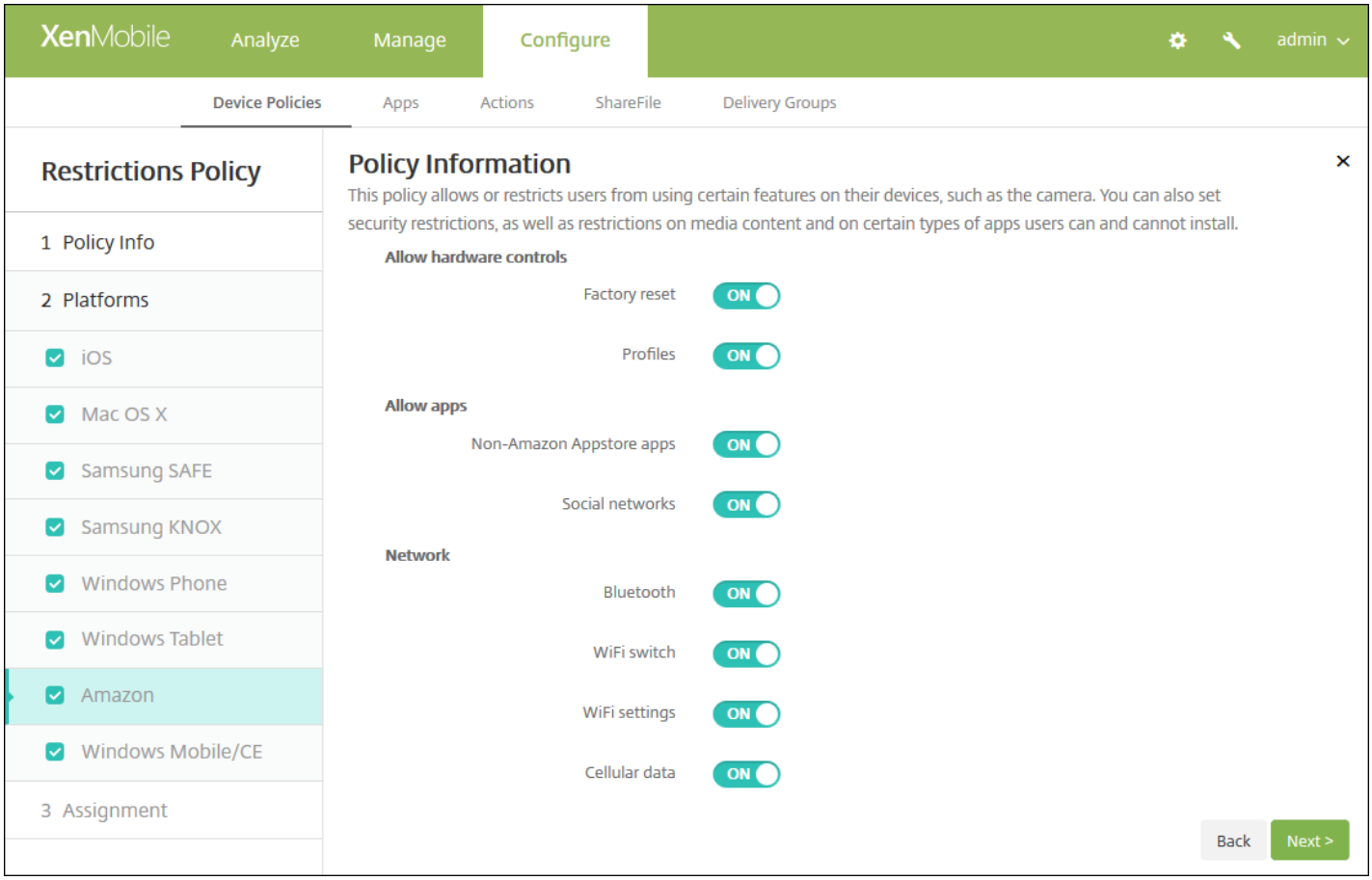
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Windows Tablet 设置

配置 Amazon 设置

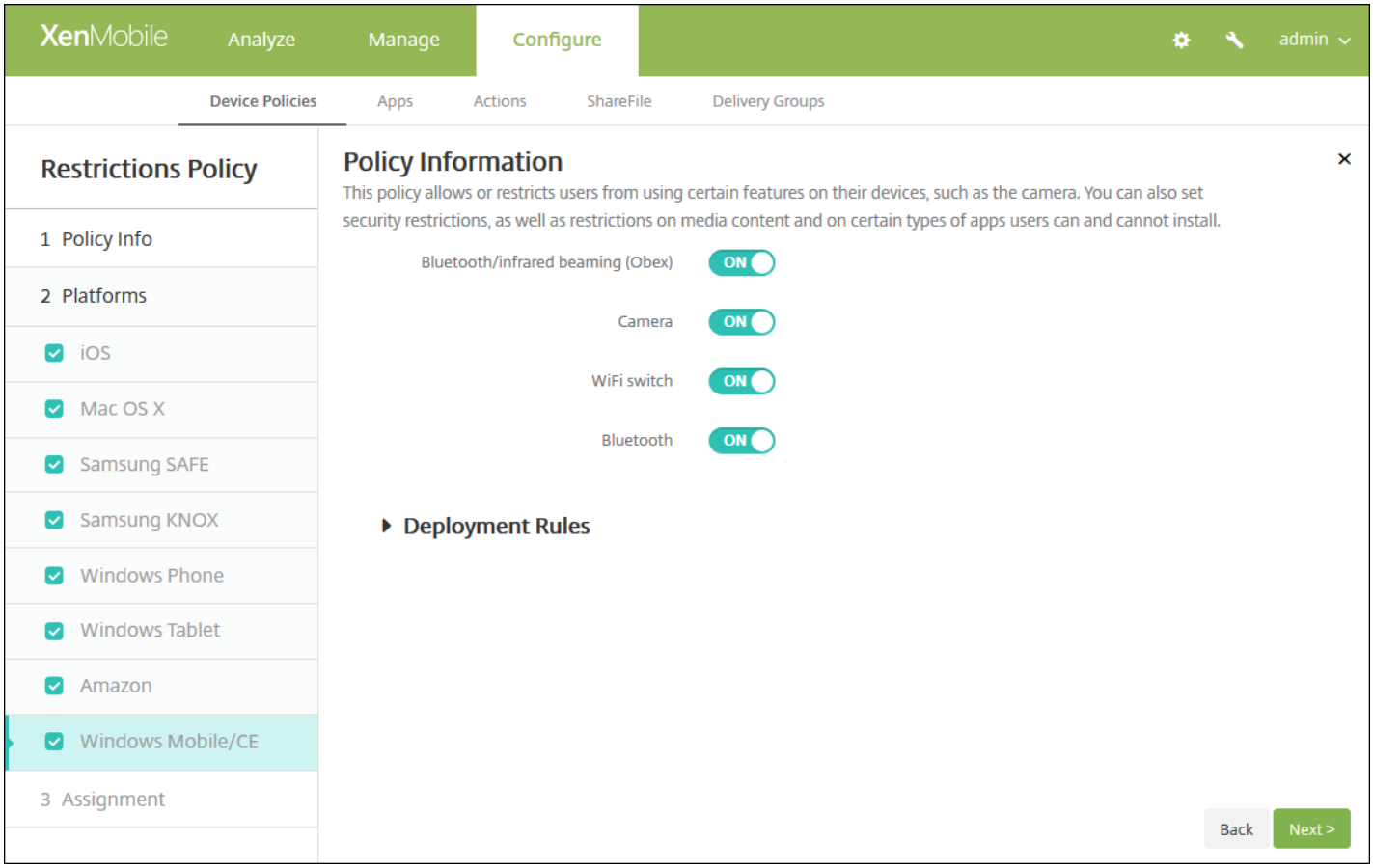
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Amazon 设置

配置 Windows Mobile/CE 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

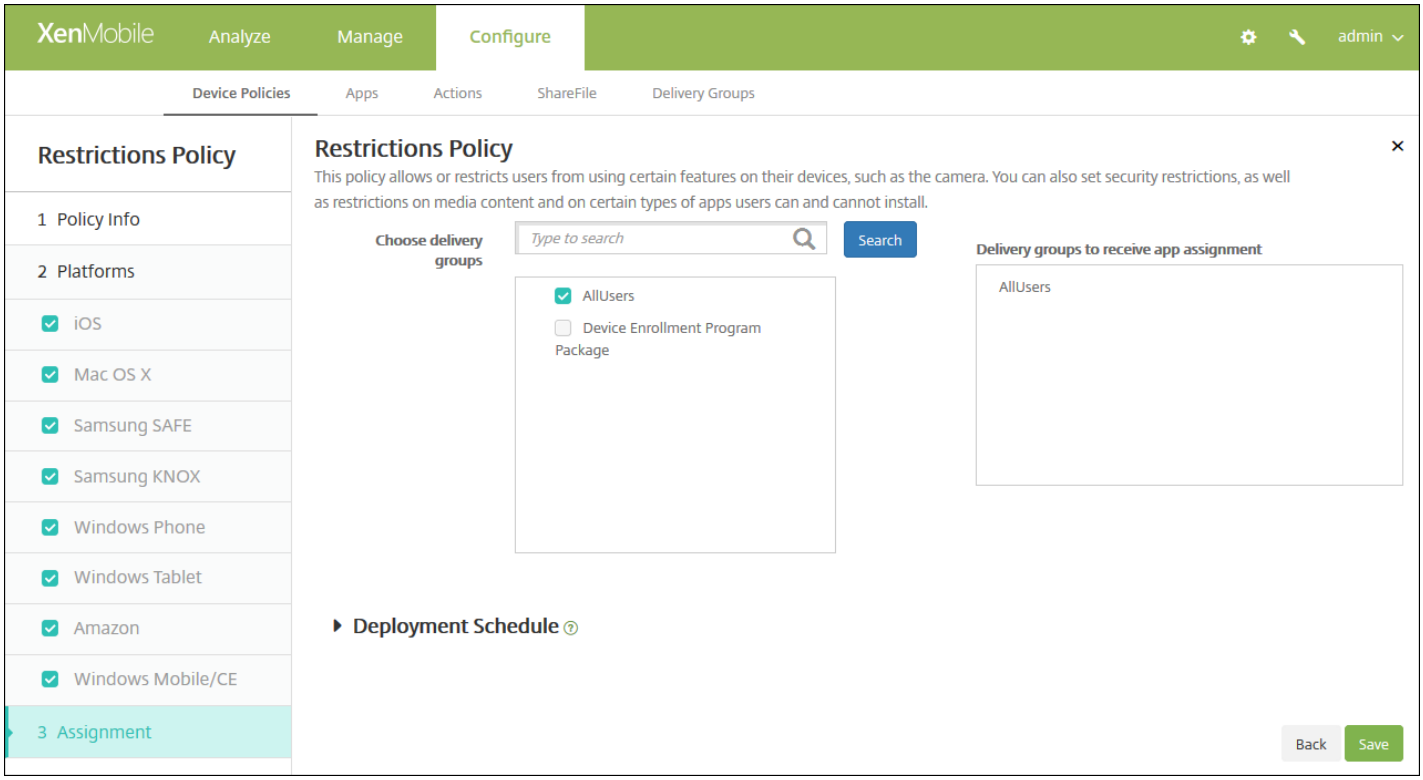


Windows Mobile/CE 设置

7. 配置部署规则

8. 单击**下一步**，将显示**限制策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

10. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

漫游设备策略

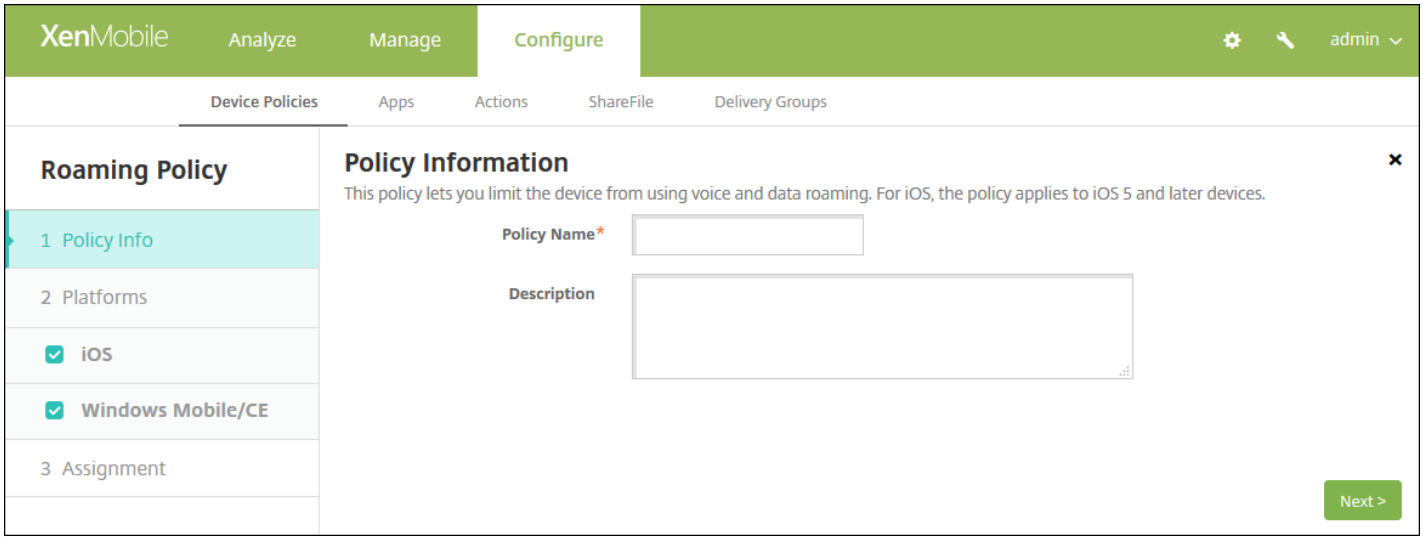
Aug 11, 2016

可以在 XenMobile 中添加一个设备策略，以配置在用户 iOS 和 Windows Mobile/CE 设备上是否允许语音和数据漫游。 禁用语音漫游时，会自动禁用数据漫游。 对于 iOS，此策略仅适用于 iOS 5.0 及更高版本的设备。

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. 单击**更多**，然后在**网络访问权限**下面，单击**漫游**。 此时将显示**漫游策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

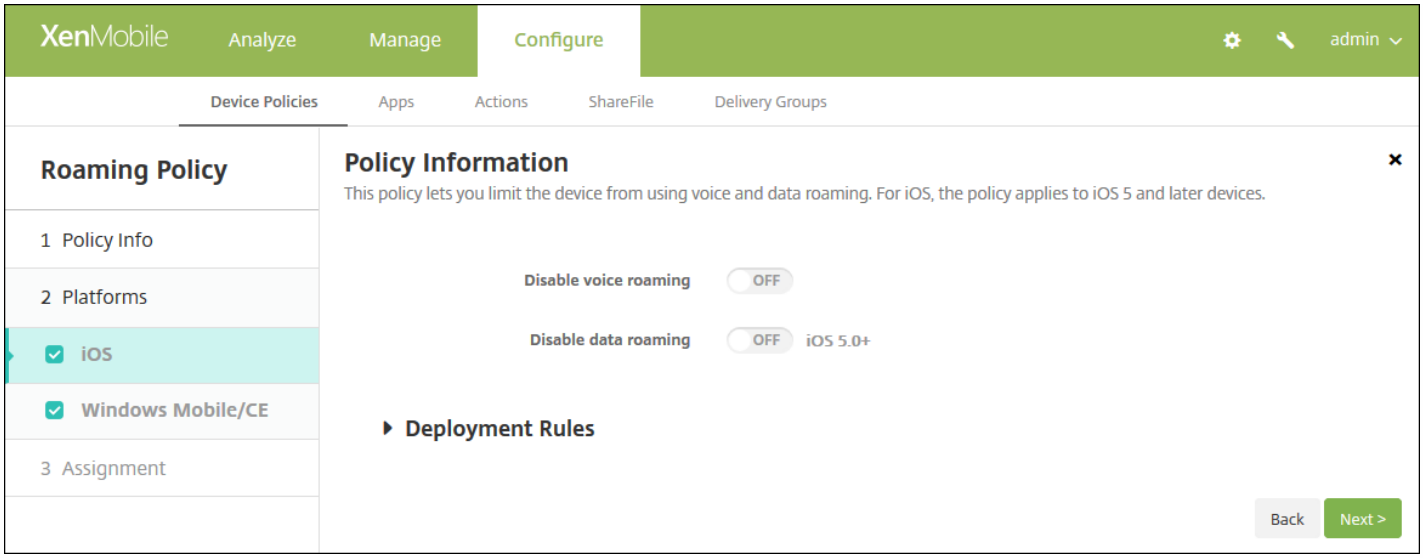
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

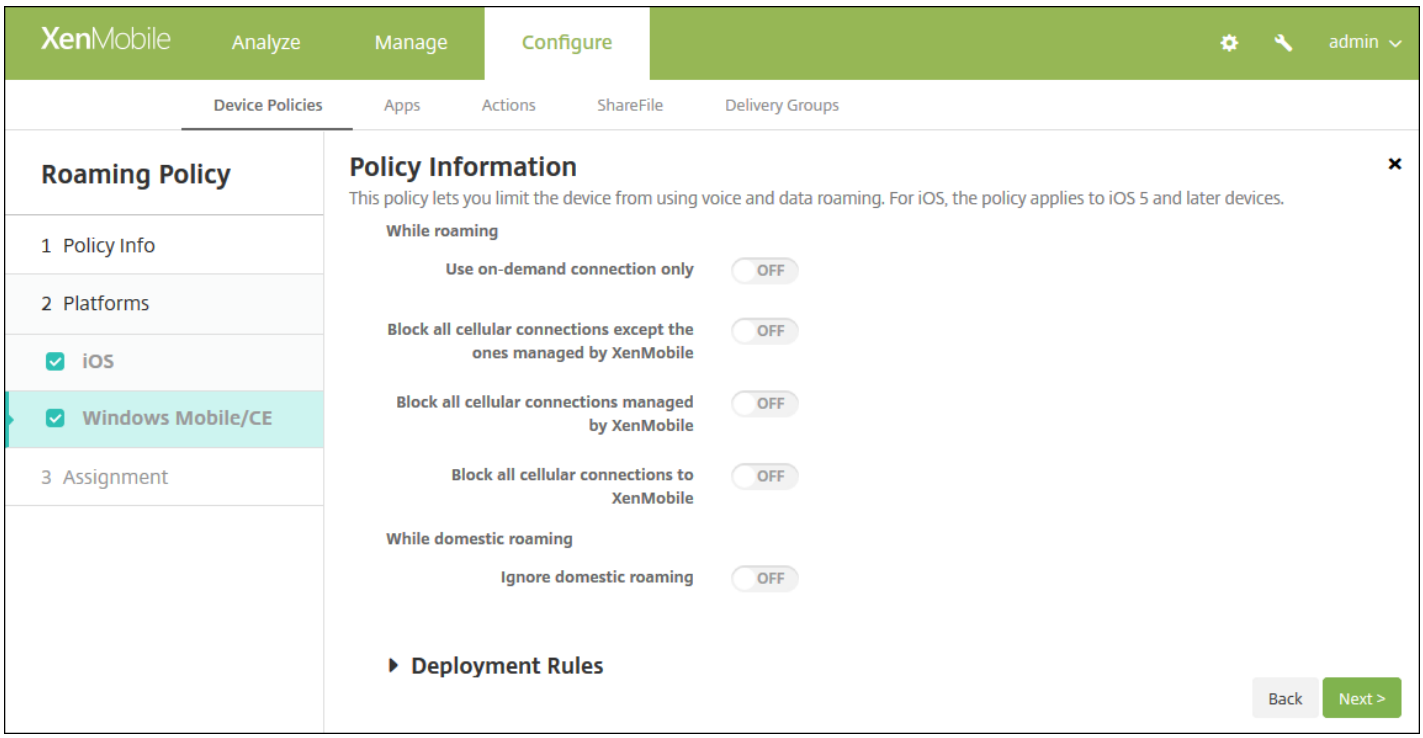
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **禁用语音漫游**：选择是否禁用语音漫游。 启用此选项时，会自动禁用数据漫游。 默认设置为 **Off**（禁用），表示允许语音漫游。
- **禁用数据漫游**：选择是否禁用数据漫游。 此选项仅在启用语音漫游时可用。 默认设置为 **Off**（禁用），表示允许数据漫游。

配置 Windows Mobile/CE 设置



配置以下设置：

- **在漫游时**

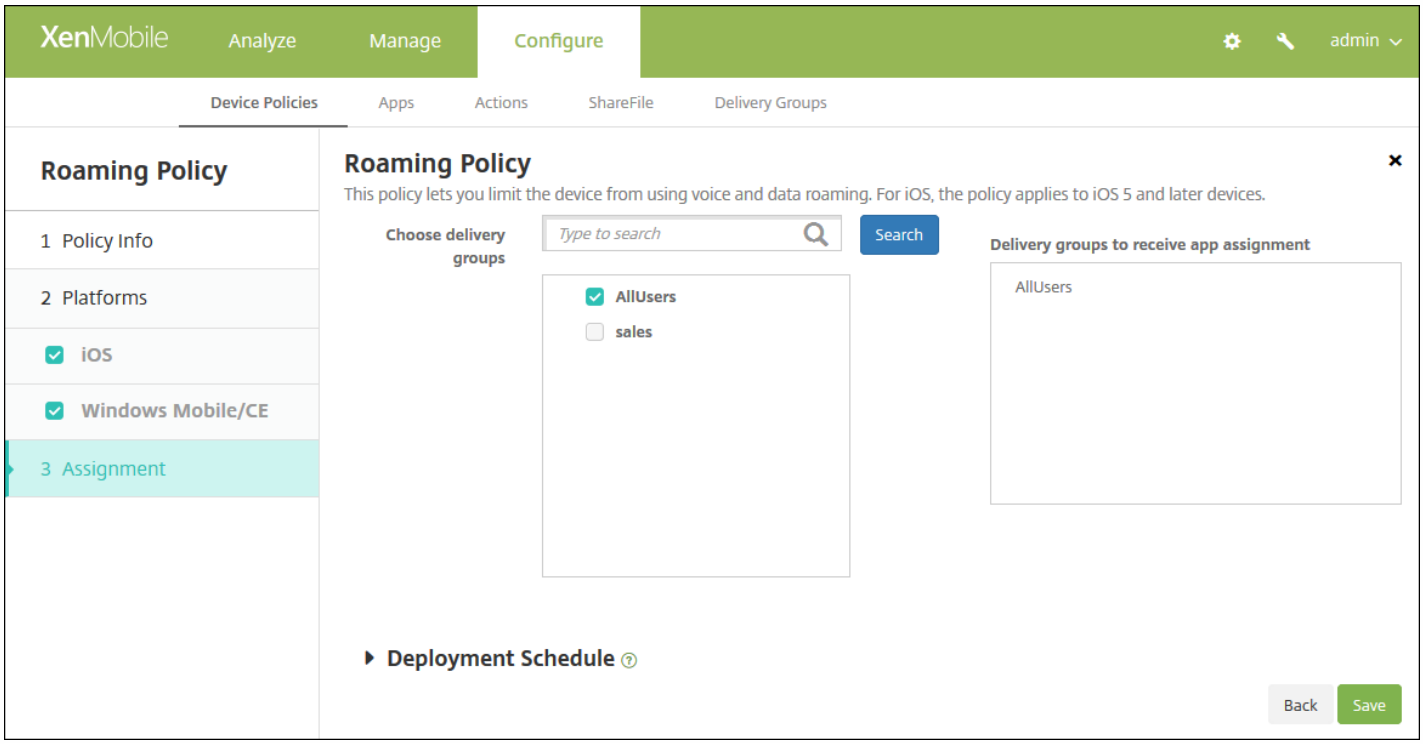
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **只使用按需连接**：如果用户在其设备上手动触发连接，或者如果移动应用程序请求强制进行连接（例如在已相应设置 Exchange Server 时的推送邮件请求），设备才会连接到 XenMobile。 请注意，此选项会临时禁用默认设备连接计划策略。
- **阻止所有手机网络连接，但 XenMobile 管理的连接除外**：除了在 XenMobile 应用程序通道或其他 XenMobile 设备管理任务中正式声明的数据流量外，该设备不会发送或接收任何其他数据。 例如，此选项将禁用所有通过设备的 Web 浏览器到 Internet 的连接。
- **阻止 XenMobile 管理的所有手机网络连接**：所有通过 XenMobile 通道传输的应用程序数据都将被阻止（包括 XenMobile Remote Support）。 但是，不会阻止与纯“设备管理”相关的数据流量。
- **阻止与 XenMobile 的所有手机网络连接**：在这种情况下，除非设备通过 USB、WiFi 或其默认移动运营商手机网络重新进行连接，否则在设备和 XenMobile 之间不会传输任何流量。

- **国内漫游时**
  - **忽略国内漫游**：用户在国内漫游时不阻止任何数据。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**漫游策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Samsung MDM 许可证密钥设备策略

Aug 11, 2016

XenMobile 支持并扩展了 Samsung for Enterprise (SAFE) 和 Samsung KNOX 策略。 SAFE 是一个解决方案系列，它通过与移动设备管理解决方案集成为业务使用提供安全性和增强功能。 Samsung KNOX 属于提供更安全的 Android 平台以供企业使用的 SAFE 计划中的一种解决方案。

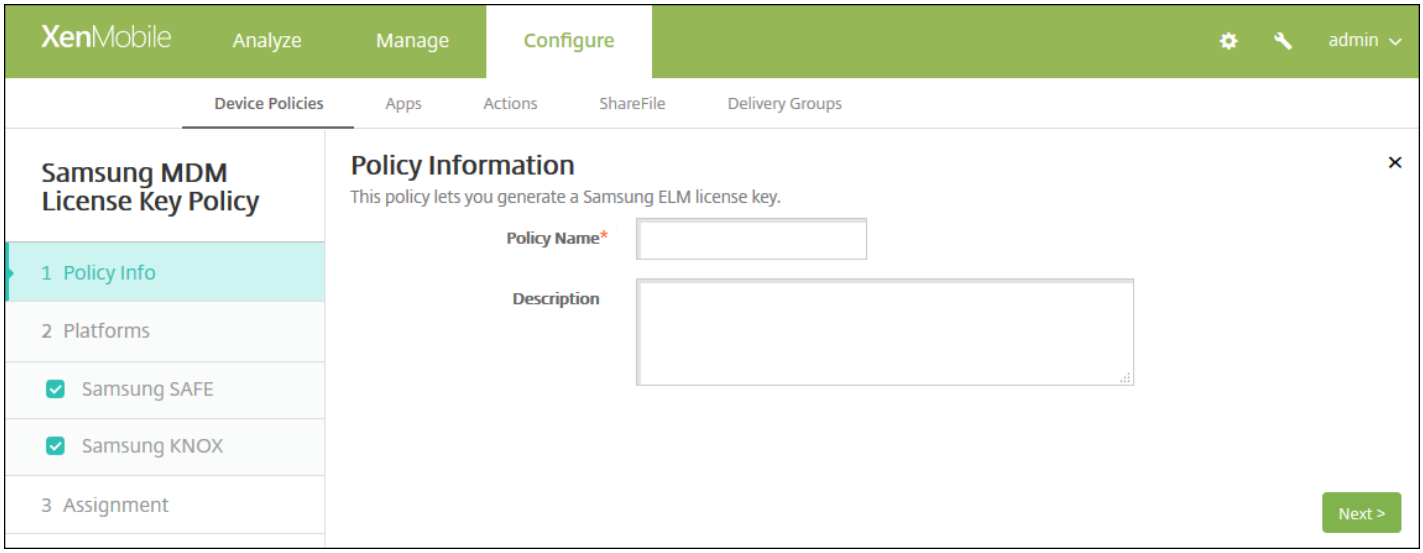
必须通过向设备部署内置 Samsung Enterprise License Management (ELM) 密钥来启用 SAFE API，才能部署 SAFE 策略和限制。 要启用 Samsung KNOX API，除部署 Samsung ELM 密钥外，还需要使用 Samsung KNOX License Management System (KLMS) 购买 Samsung KNOX Workspace 许可证。 Samsung KLMS 为移动设备管理解决方案提供有效的许可证，以使其能够在移动设备上激活 Samsung KNOX API。 必须从 Samsung 获取这些许可证，Citrix 不提供。

要启用 SAFE 和 Samsung KNOX API，必须部署 Worx Home 以及 Samsung ELM 密钥。 可以通过检查设备属性来验证是否已启用 SAFE API。 部署 Samsung ELM 密钥时，将 Samsung MDM API 可用性设置为 **True**。

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. 单击**更多**，然后在**安全性**下面，单击 **Samsung MDM 许可证密钥**。 此时将显示 **Samsung MDM 许可证密钥策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

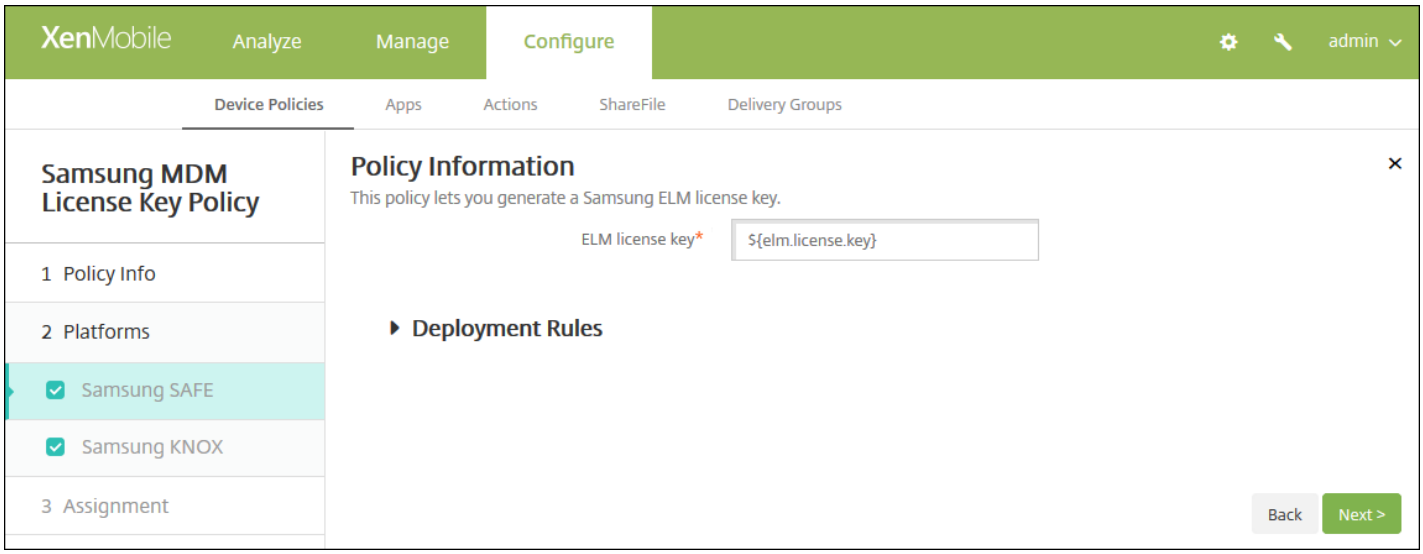
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Samsung SAFE 设置

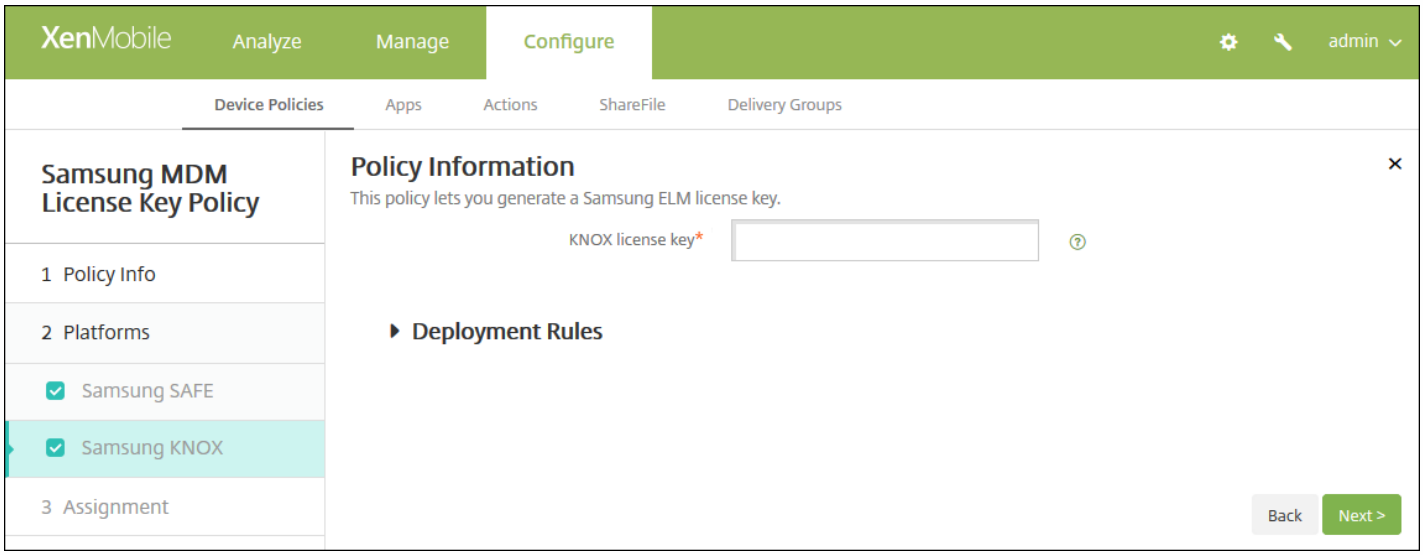
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **ELM 许可证密钥**：此字段应该已包含生成 ELM 许可证密钥的宏。 如果此字段为空，请键入宏 ${elm.license.key}。

配置 Samsung KNOX 设置



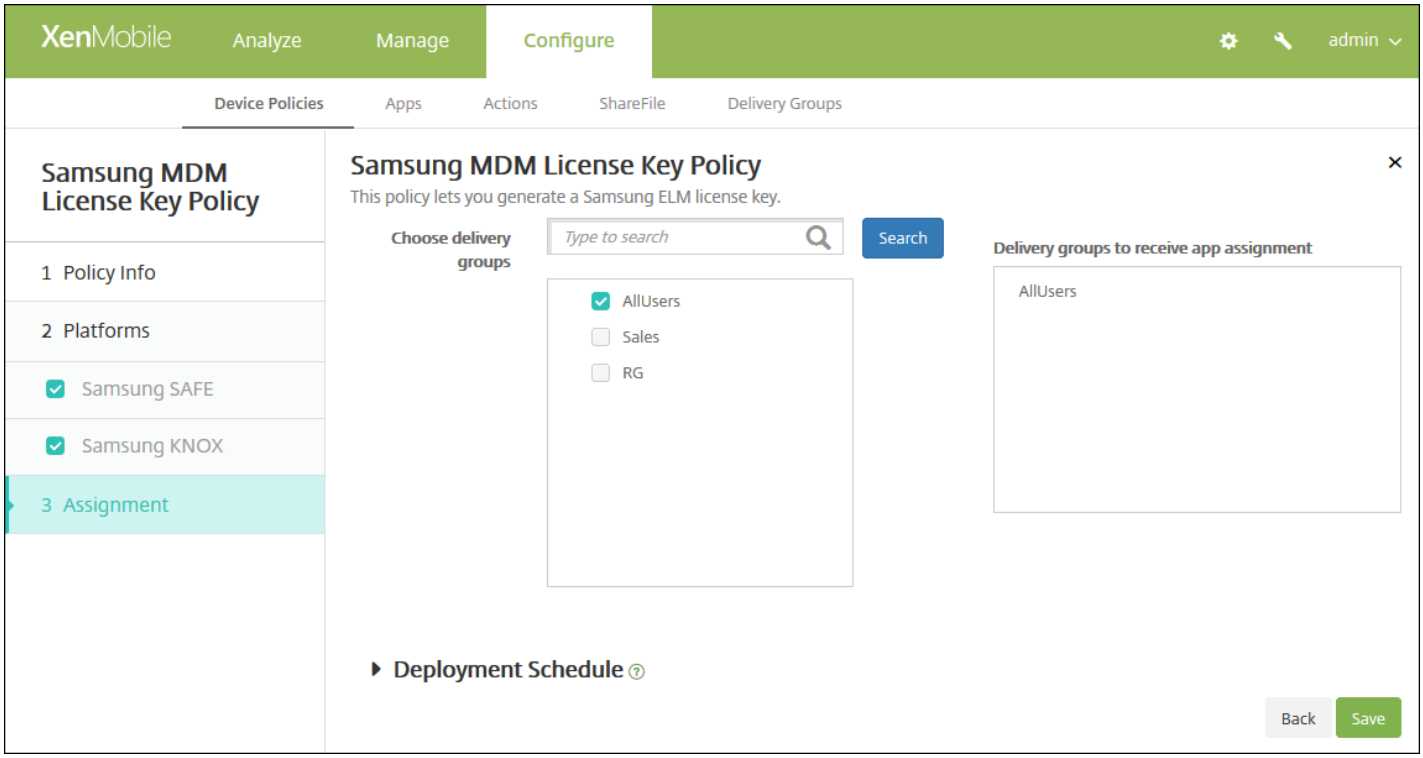
配置以下设置：

- **KNOX 许可证密钥**：键入从 Samsung 获取的 25 位 KNOX 许可证密钥。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Samsung MDM 许可证密钥策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Samsung SAFE 防火墙设备策略

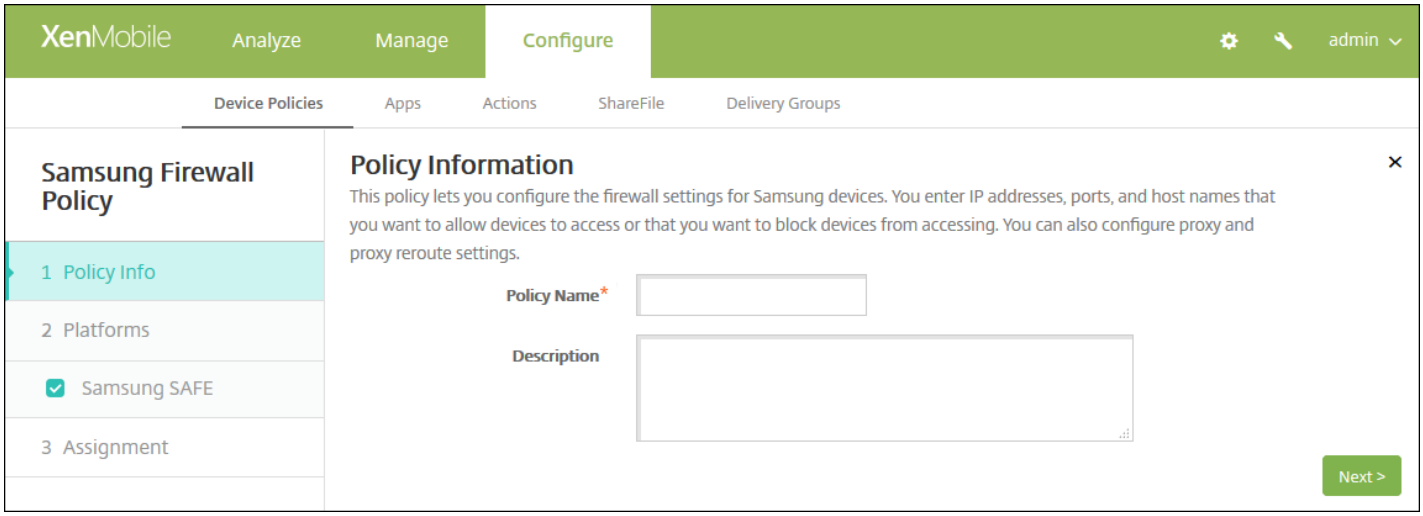
Aug 11, 2016

利用此策略可以为 Samsung 设备配置防火墙设置。 输入允许设备访问或阻止设备访问的 IP 地址、端口和主机名。 还可以配置代理和代理重新路由设置。

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**网络访问权限**下，单击 **Samsung 防火墙**。 此时将显示 **Samsung 防火墙策略**页面。

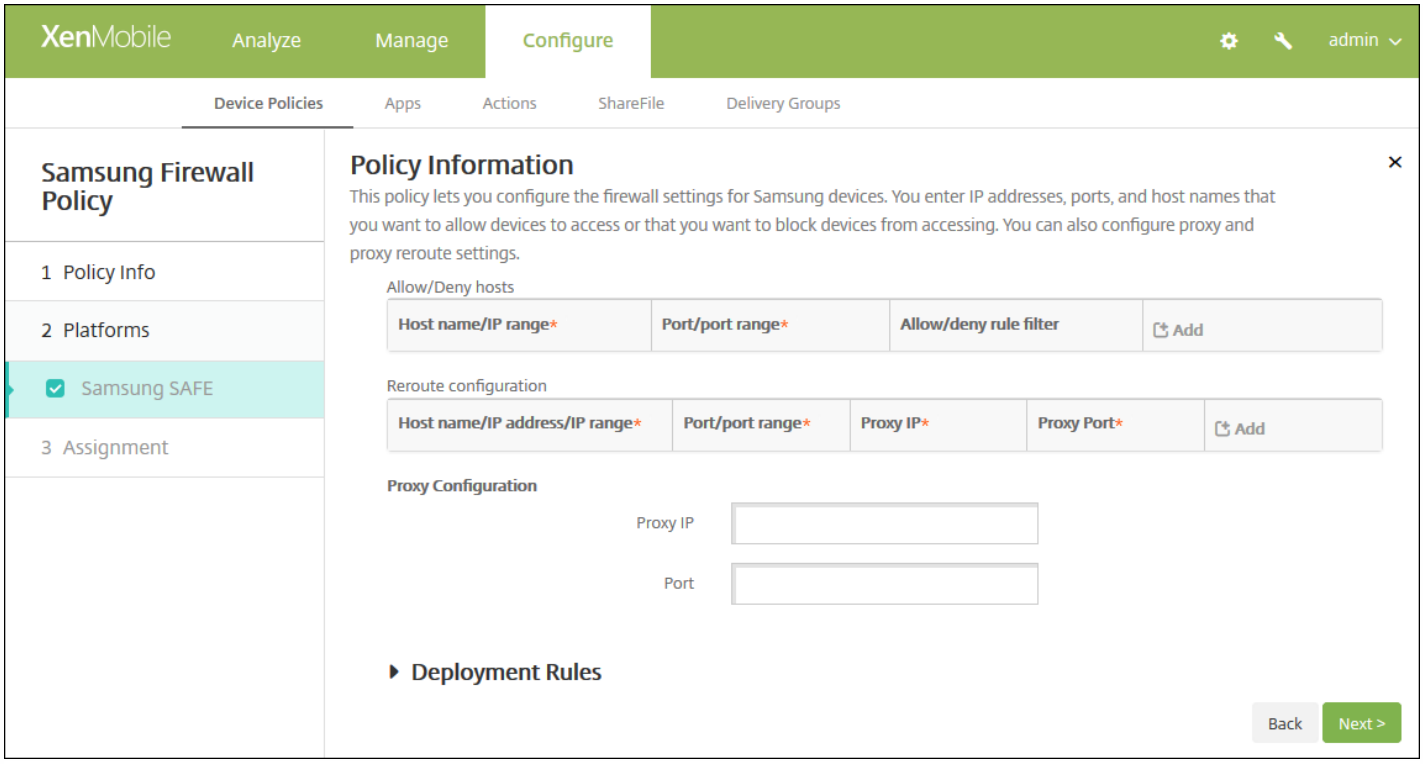


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **Samsung SAFE** 平台信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 配置以下设置：

- **允许/拒绝主机**
  - 对于希望允许访问或拒绝访问的每个主机，请单击**添加**并执行以下操作：
    - **主机名/IP 范围**：键入希望影响的站点的主机名和 IP 地址范围。
    - **端口/端口范围**：键入端口/端口范围。
    - **允许/拒绝规则过滤**：选择“白名单”以允许访问站点或单击“黑名单”以拒绝访问站点。
    - 单击**保存**或**取消**。
- **重新路由配置**
  - 对于要配置的每个代理，单击**添加**并执行以下操作：
    - **主机名/IP 范围**：键入代理重新路由的主机名或 IP 地址范围。
    - **端口/端口范围**：键入端口/端口范围。
    - **代理 IP**：键入代理 IP 地址。
    - **代理端口**：键入代理端口。
    - 单击**保存**或**取消**。

    注意：要删除现有项目，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。单击**删除**以删除列表，或单击**取消**以保留此列表。

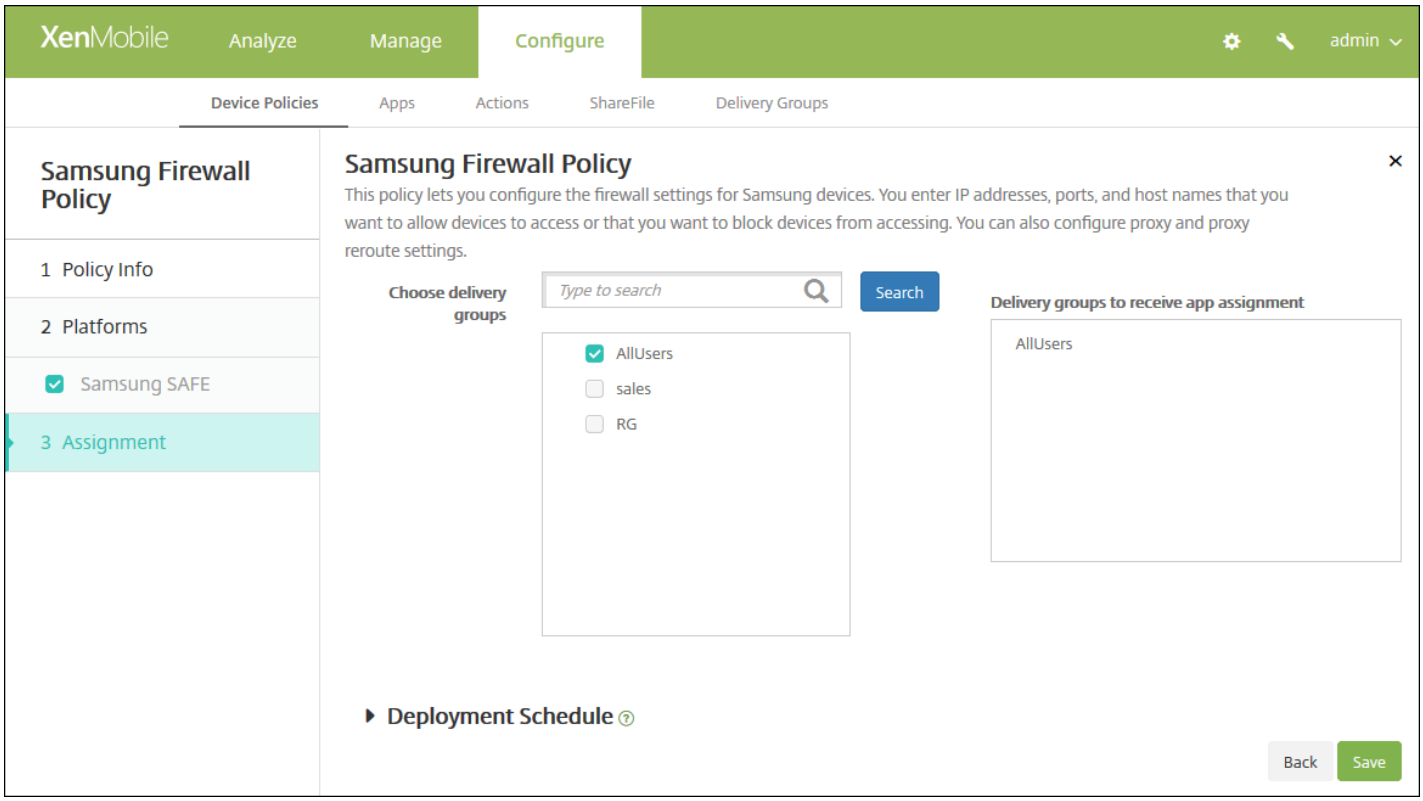
    要编辑现有项目，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **代理配置**
  - **代理 IP**：键入代理服务器的 IP 地址。
  - **端口**：键入代理服务器端口。

7. 配置部署规则

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 单击**下一步**。 此时将显示 **Samsung 防火墙策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SCEP 设备策略

Aug 11, 2016

利用此策略，可以将 iOS 和 Mac OS X 设备配置为使用简单证书注册协议 (SCEP) 从外部 SCEP 服务器检索证书。 如果希望从连接到 XenMobile 的 PKI 向使用 SCEP 的设备交付证书，应采用分散模式创建 PKI 实体和 PKI 提供程序。 有关详细信息，请参阅 PKI 实体。

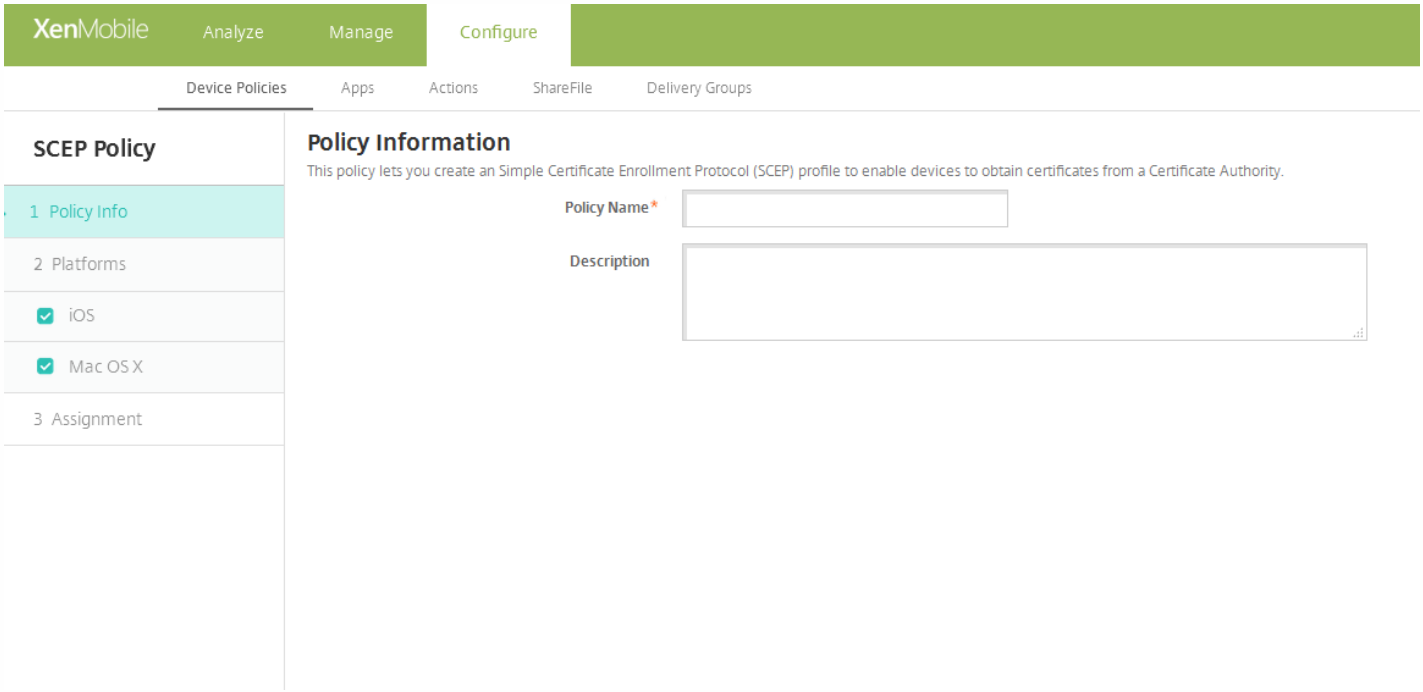
iOS 设置

Mac OS X 设置

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**下面，单击 **SCEP**。 此时将显示 **SCEP 策略**信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

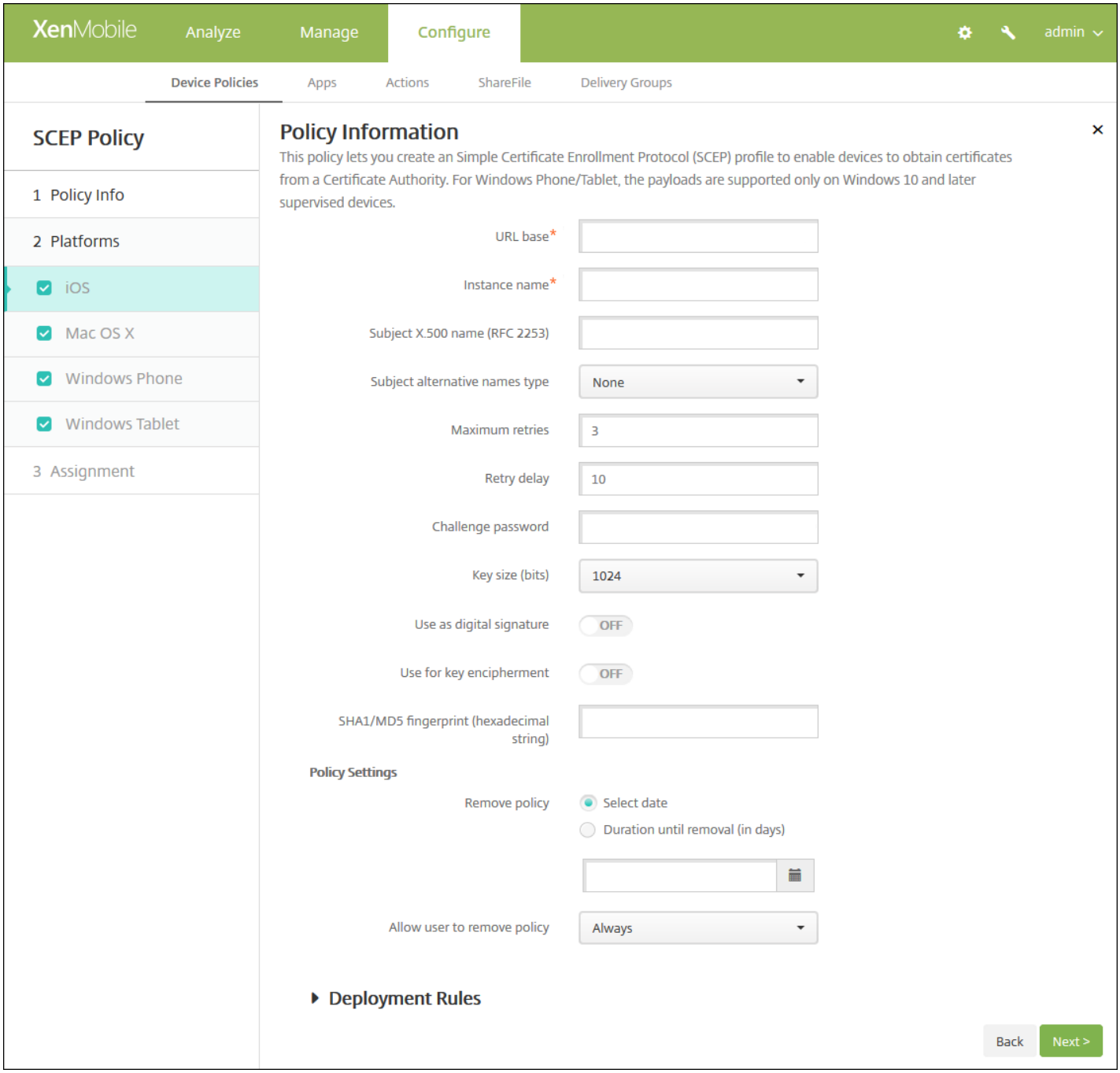
5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

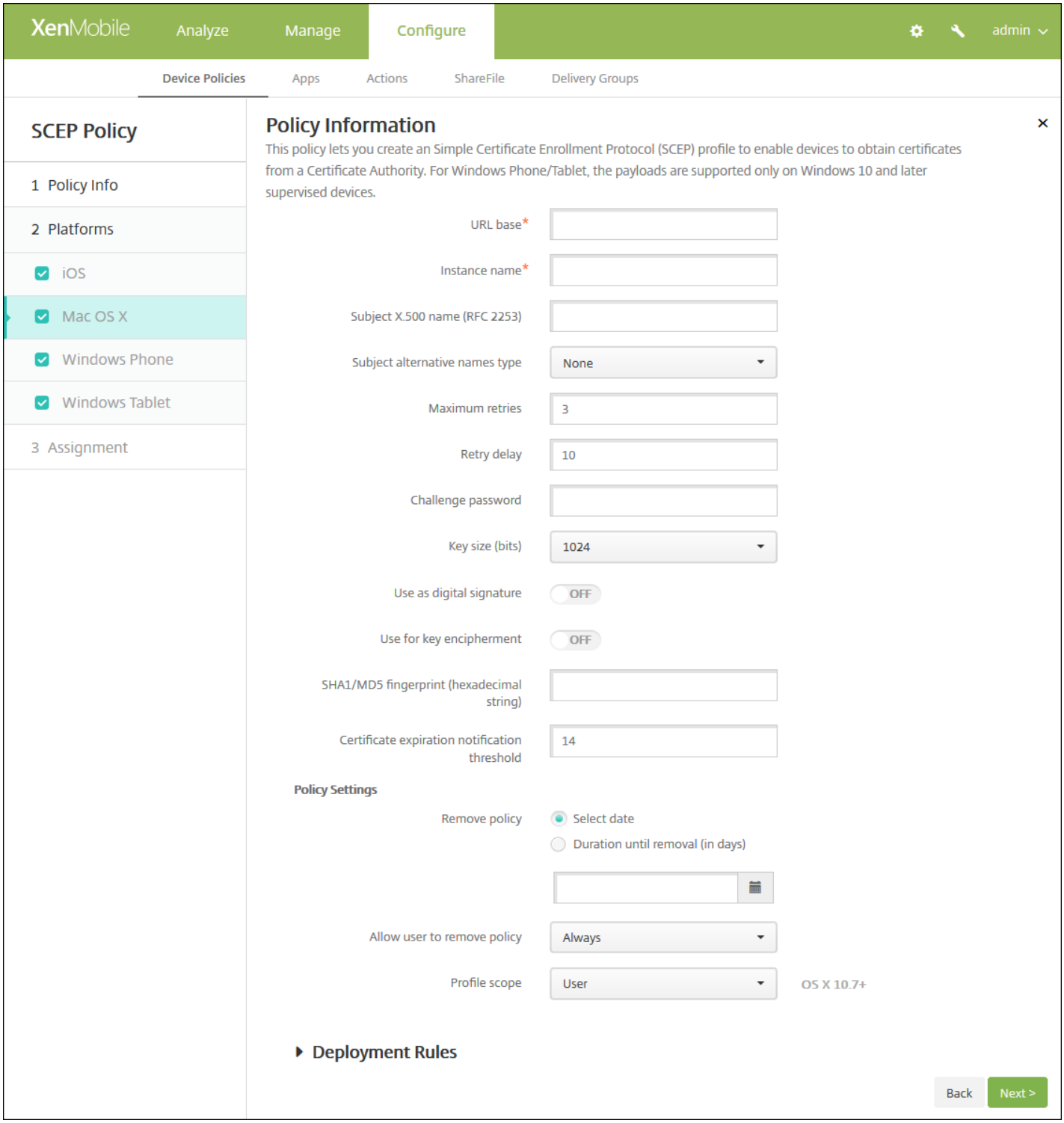
- **URL 库**：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。 由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。 但是，如果允许重复使用一次性密码，则应该使用 HTTPS 来保护密码。 此步骤不是必需步骤。
- **实例名称**：键入任何 SCEP 服务器可以识别的字符串。 例如，可以是类似 example.org 的域名。 如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。 此步骤不是必需步骤。
- **使用者 X.500 名称 (RFC 2253)**：键入表示为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。 例如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 将转换为：[[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]。 OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **使用者备用名称类型**：在列表中，单击备用名称类型。 SCEP 策略可指定可选的备用名称类型，用于提供 CA 颁发证书所需的值。 可以指定**无**、**RFC 822 名称**、**DNS 名称**或 **URI**。
- **最大重试次数**：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。 默认值为 **3**。
- **重试延迟**：键入执行下次重试之前需要等待的秒数。 第一次重试尝试没有延迟。 默认值为 **10**。
- **质询密码**：输入预共享密钥。
- **密钥大小(位)**：在列表中，单击以位为单位的密钥大小 **1024** 或 **2048**。 默认值为 **1024**。
- **用作数字签名**：指定是否要将证书用作数字签名。 如果有人使用证书来验证数字签名，如验证证书是否由 CA 颁发，SCEP 服务器将在使用公钥解密哈希之前确认该证书是否可以用于此目的。
- **用于密匙加密**：指定是否要将证书用于密匙加密。 如果服务器正在使用客户端提供的证书中包含的公钥来验证数据段是否使用私钥进行加密，服务器将首先检查证书是否可用于密钥加密。 否则，操作将失败。
- **SHA1/MD5 指纹(十六进制字符串)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹，供设备在注册期间用于确认 CA 响应的可靠性。 可以输入 SHA1 或 MD5 指纹，或选择证书来导入其签名。
- **策略设置**
  - 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

配置 Mac OS X 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **URL 库**：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。 由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。 但是，如果允许重复使用一次性密码，则应该使用 HTTPS 来保护密码。 此步骤不是必需步骤。
- **实例名称**：键入任何 SCEP 服务器可以识别的字符串。 例如，可以是类似 example.org 的域名。 如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。 此步骤不是必需步骤。
- **使用者 X.500 名称 (RFC 2253)**：键入表示为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。 例

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 将转换为：[[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]。 OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。

- **使用者备用名称类型**：在列表中，单击备用名称类型。 SCEP 策略可指定可选的备用名称类型，用于提供 CA 颁发证书所需的值。 可以指定**无**、**RFC 822 名称**、**DNS 名称**或 **URI**。
- **最大重试次数**：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。 默认值为 **3**。
- **重试延迟**：键入执行下次重试之前需要等待的秒数。 第一次重试尝试没有延迟。 默认值为 **10**。
- **质询密码**：键入预共享密钥。
- **密钥大小(位)**：在列表中，单击以位为单位的密钥大小 **1024** 或 **2048**。 默认值为 **1024**。
- **用作数字签名**：指定是否要将证书用作数字签名。 如果有人使用证书来验证数字签名，如验证证书是否由 CA 颁发，SCEP 服务器将在使用公钥解密哈希之前确认该证书是否可以用于此目的。
- **用于密匙加密**：指定是否要将证书用于密匙加密。 如果服务器正在使用客户端提供的证书中包含的公钥来验证数据段是否使用私钥进行加密，服务器将首先检查证书是否可用于密钥加密。 否则，操作将失败。
- **SHA1/MD5 指纹(十六进制字符串)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹，供设备在注册期间用于确认 CA 响应的可靠性。 可以输入 SHA1 或 MD5 指纹，或选择证书来导入其签名。
- **策略设置**
  - 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **SCEP 策略**分配页面。

9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为立即。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

旁加载密钥设备策略

Aug 11, 2016

借助 XenMobile 中的旁加载，您可以在 Windows 8.1 设备上部署还未从 Windows 应用商店中购买的应用程序。 需要旁加载应用程序的最常见情况是，您不希望在 Windows 应用商店中公开为企业开发的应用程序。 要旁加载应用程序，需要配置旁加载密钥和密钥激活，然后再将应用程序部署到用户的设备。

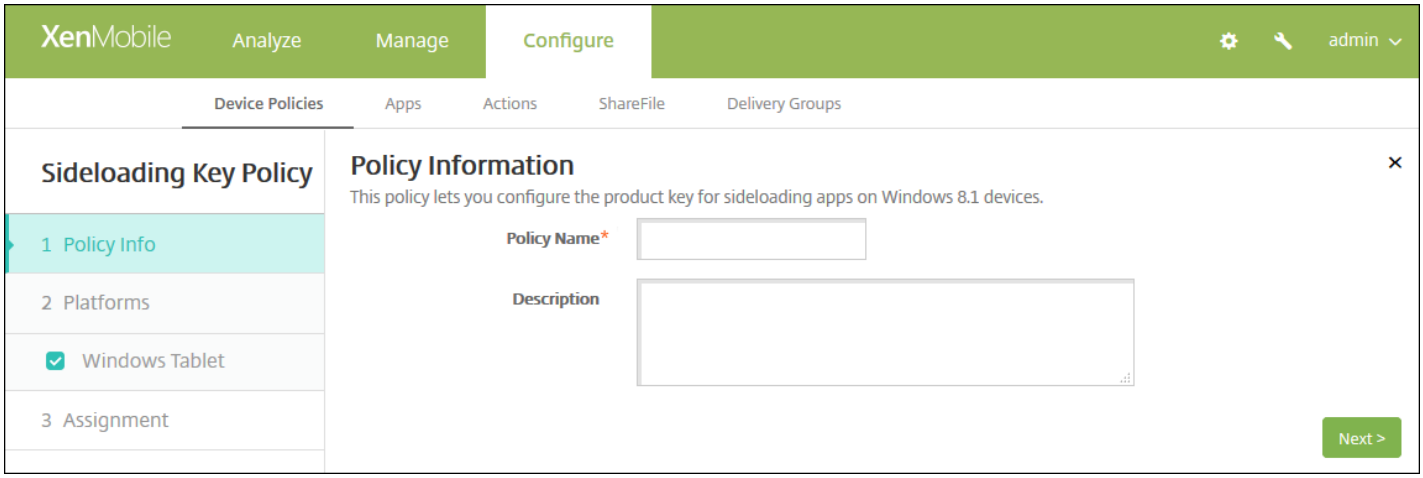
创建此策略之前，需要提供以下信息：

- 旁加载产品密钥，需要登录 Microsoft Volume Licensing Service Center（Microsoft 批量许可服务中心）获取此信息
- 密钥激活，需要在获取旁加载产品密钥之后通过命令行创建

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**应用程序**下面，单击**旁加载密钥**。 此时将显示 **Sideloading Key Policy**（旁加载密钥策略）页面。

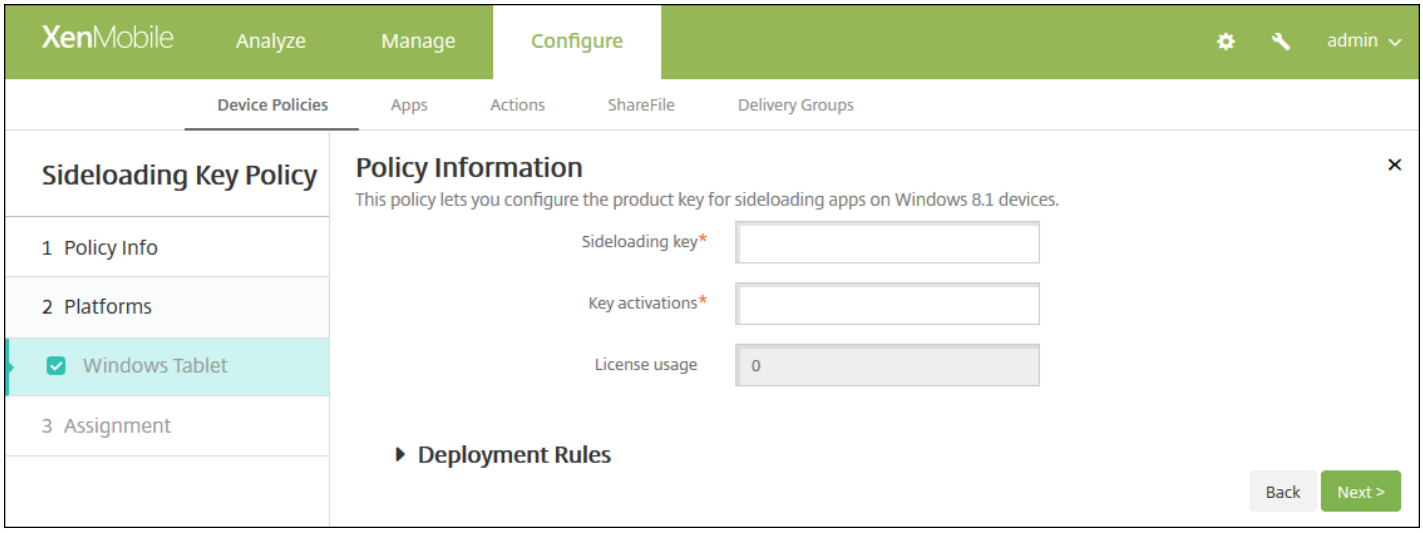


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **Windows Tablet 平台**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

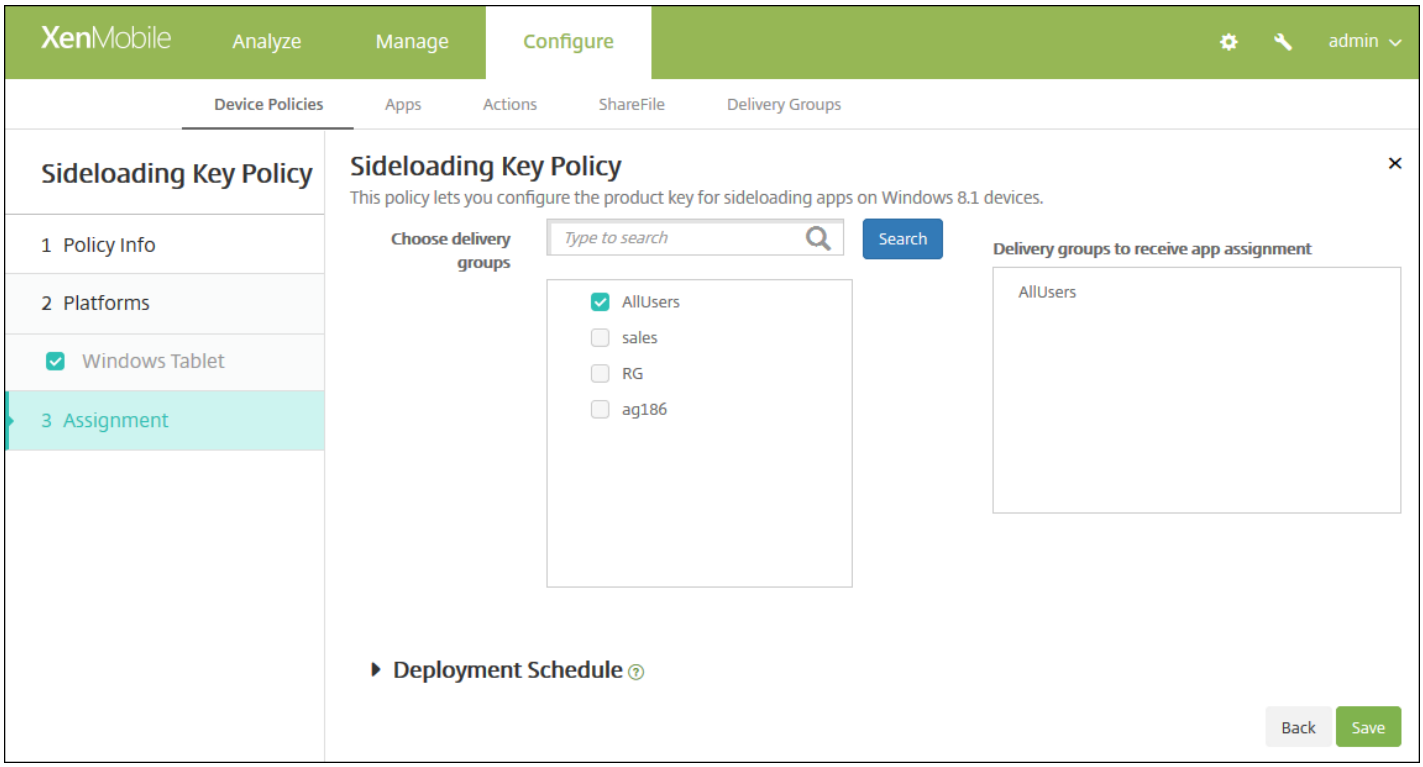


6. 配置以下设置：

- **旁加载密钥**：键入从 Microsoft 批量许可服务中心获取的旁加载密钥。
- **密钥激活**：键入为旁加载密钥创建的密钥激活。
- **许可证使用情况**：XenMobile 根据注册的平板电脑数计算此值。 无法更改此字段。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**旁加载密钥策略分配**页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. 展开部署计划，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

签名证书设备策略

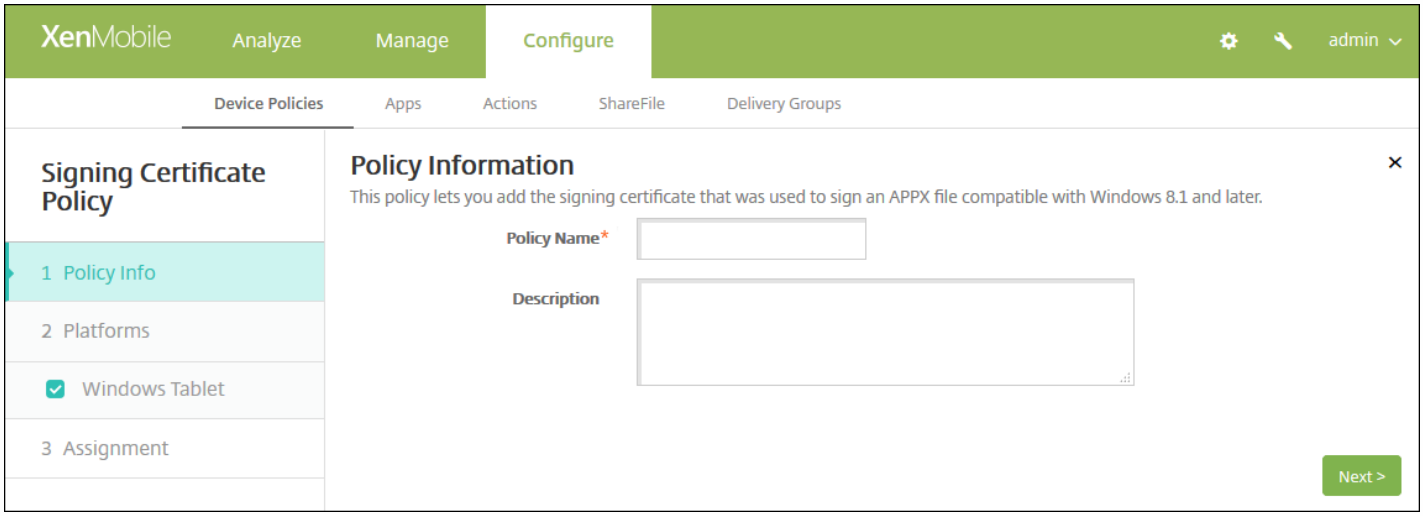
Aug 11, 2016

可以在 XenMobile 中添加一个设备策略，以配置用于签署 APPX 文件的签名证书。 如果要向用户分发 APPX 文件以允许用户在其 Windows Tablet 上安装应用程序，需要使用签名证书。

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。

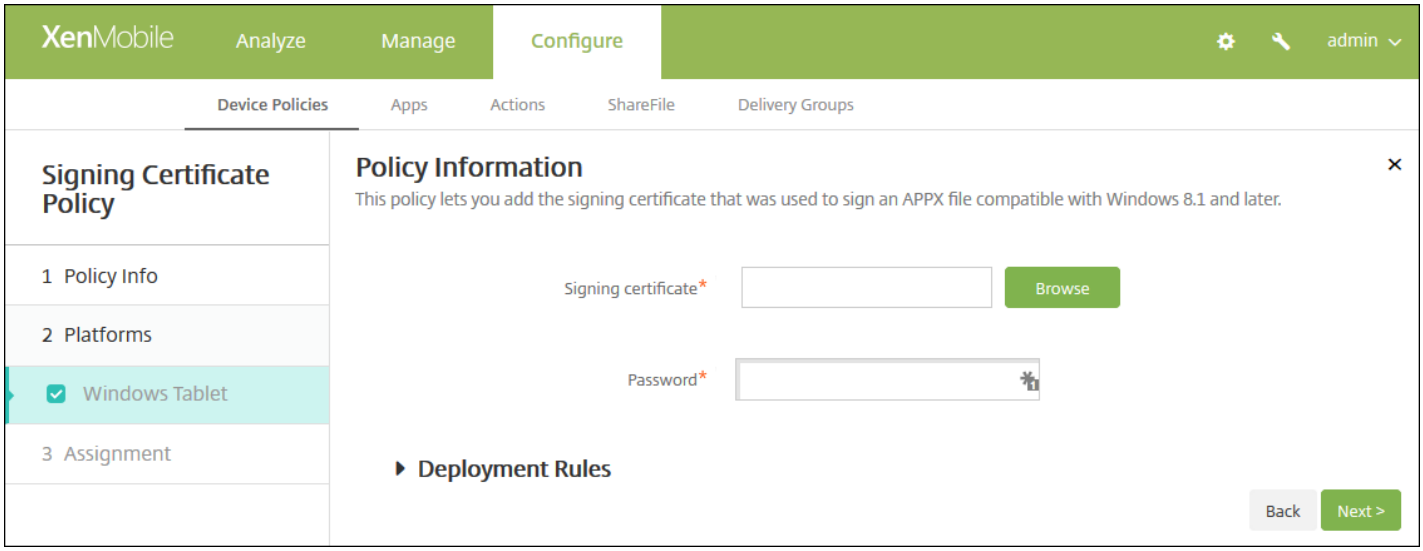
3. 单击**更多**，然后在**应用程序**下面，单击**签名证书**。 此时将显示**签名证书策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：如有需要，请键入策略的说明。

5. 单击**下一步**。 此时将显示 **Windows Tablet 平台**页面。



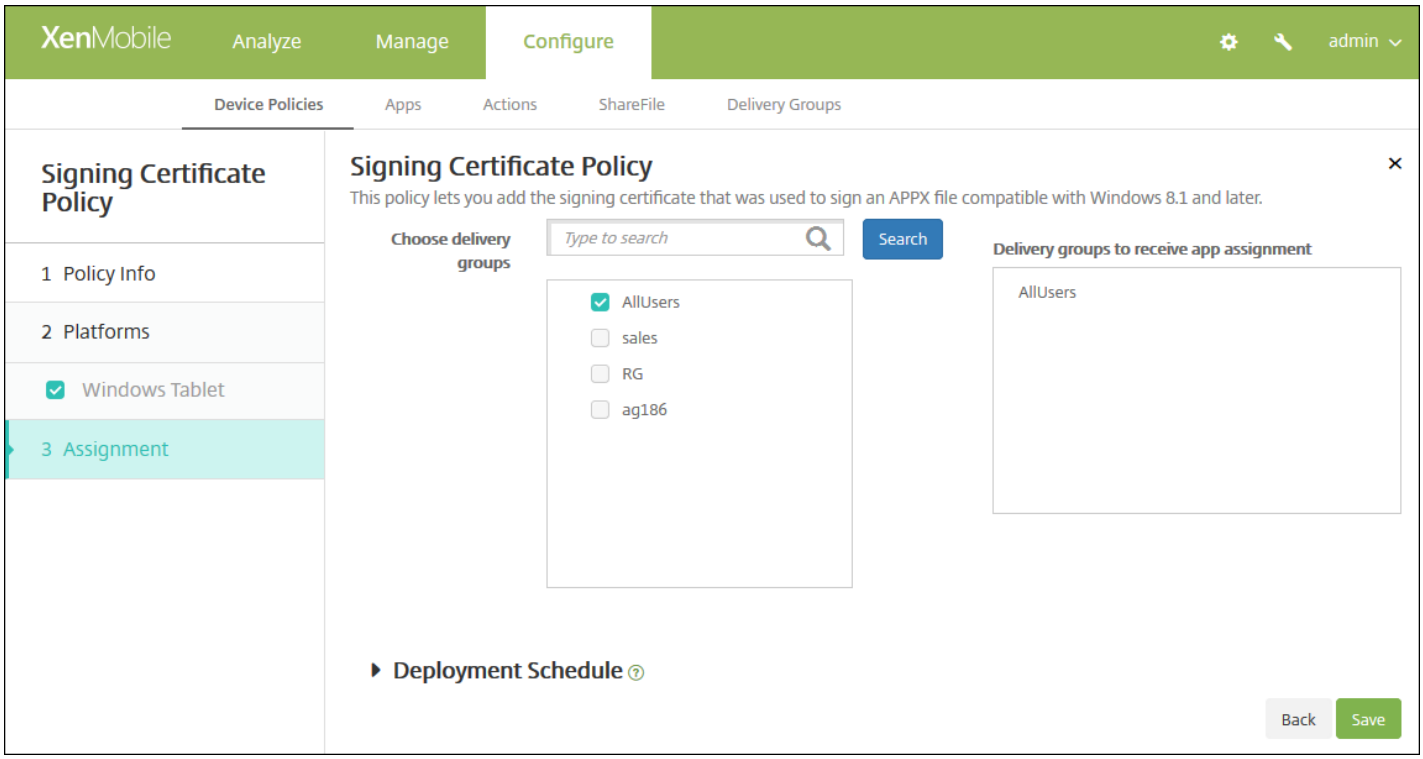
© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 配置以下设置：

- **签名证书**：单击**浏览**并导航到用于对 APPX 文件进行签名的证书所在的位置，选择此证书。
- **密码**：键入访问签名证书所需的密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**签名证书策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所作的更改适用于所有平台，**为 始终启用 的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

单点登录帐户交付组

Aug 11, 2016

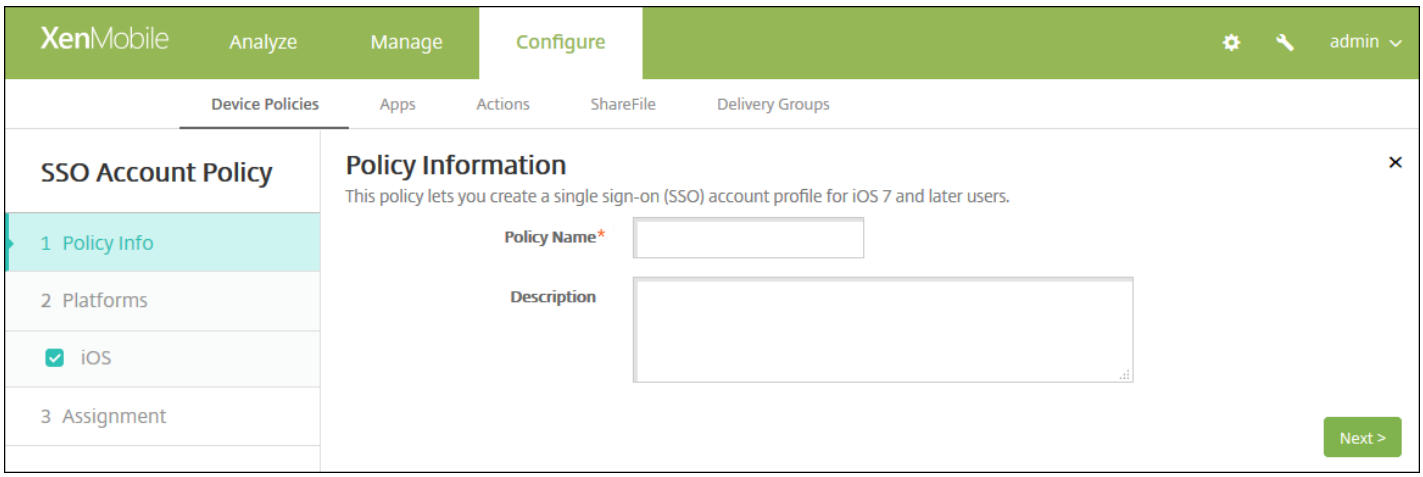
在 XenMobile 中创建 Single Sign-On (SSO) 帐户，使用户只需登录设备一次，即可从各种应用程序访问 XenMobile 和内部的公司资源。 用户无需在设备上存储任何凭据。 可以跨应用程序（包括 App Store 中的应用程序）使用此 SSO 帐户企业用户凭据。 此策略专为 Kerberos 身份验证后端设计。

注意：此策略仅适用于 iOS 7.0 及更高版本。

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. 单击**更多**，然后在**最终用户**下面，单击 **SSO 帐户**。 此时将显示 **SSO Account Policy**（SSO 帐户策略）页面。

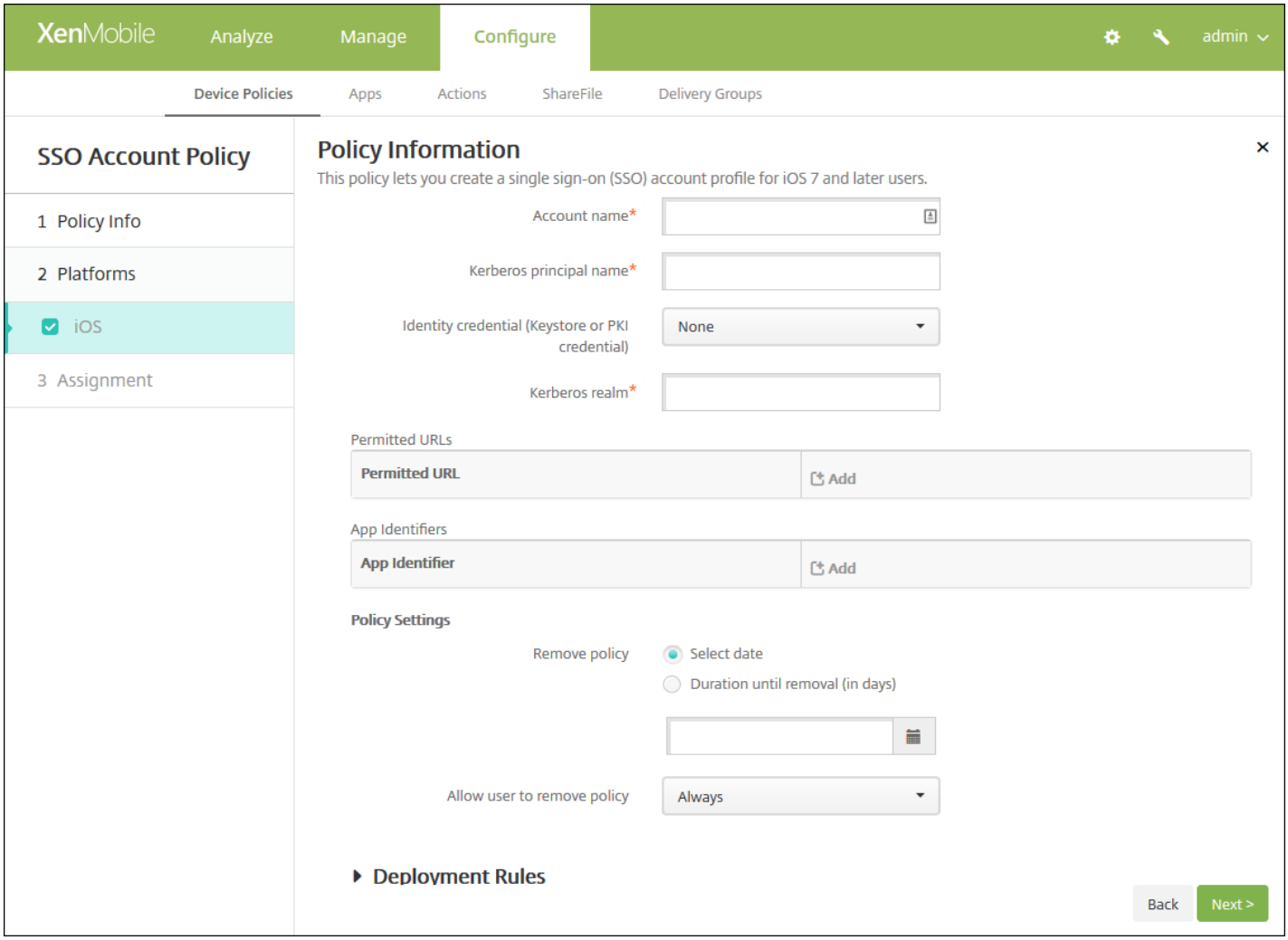


4. 在 **SSO 帐户策略**信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 配置以下设置：

- **帐户名称**：输入显示在用户设备上的 Kerberos SSO 帐户名称。 此字段为必填字段。
- **Kerberos 主体名称**：输入 Kerberos 主体名称。 此字段为必填字段。
- **身份凭据(密钥库或 PKI 凭据)**：在此列表中，单击可用于在无需用户交互的情况下续订 Kerberos 凭据的可选身份凭据。
- **Kerberos 领域**：输入此策略的 Kerberos 领域。 这通常是您的域名，所有字母均大写（例如，EXAMPLE.COM）。 此字段为必填字段。
- **允许访问的 URL**：对于需要 SSO 的各个 URL，单击**添加**，然后执行以下操作：
  - **允许访问的 URL**：输入当用户从 iOS 设备访问时需要 SSO 的 URL。 例如，当用户尝试浏览某个站点，且该 Web 站点发起 Kerberos 质询时，如果该站点不在此 URL 列表中，iOS 将不会通过提供 Kerberos 在以前的 Kerberos 登录中缓存到设备上的 Kerberos 令牌来尝试 SSO。 URL 的主机部分必须完全匹配，例如：http://shopping.apple.com 可以，但 http://*.apple.com 却不行。 此外，如果 Kerberos 未基于主机匹配激活，URL 将仍然回退到标准 HTTP 调用。 如果 URL 仅配置为使用 Kerberos 实现 SSO，这可能意味着一切，包括标准密码质询或 HTTP 错误。
  - 单击**添加**以添加 URL，或单击**取消**以取消添加 URL。
- **应用程序标识符**：对于允许使用此登录的每个应用程序，单击**添加**，然后执行以下操作：
  - **应用程序标识符**：输入允许使用此登录方式的应用程序的应用程序标识符。 如果不添加任何应用程序标识符，此登录将匹配**所有**应用程序标识符。
  - 单击**添加**添加应用程序标识符，或单击**取消**取消添加应用程序标识符。

注意：要删除现有 URL 或应用程序标识符，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将

© 1999-2017 Citrix Systems, Inc. All rights reserved.

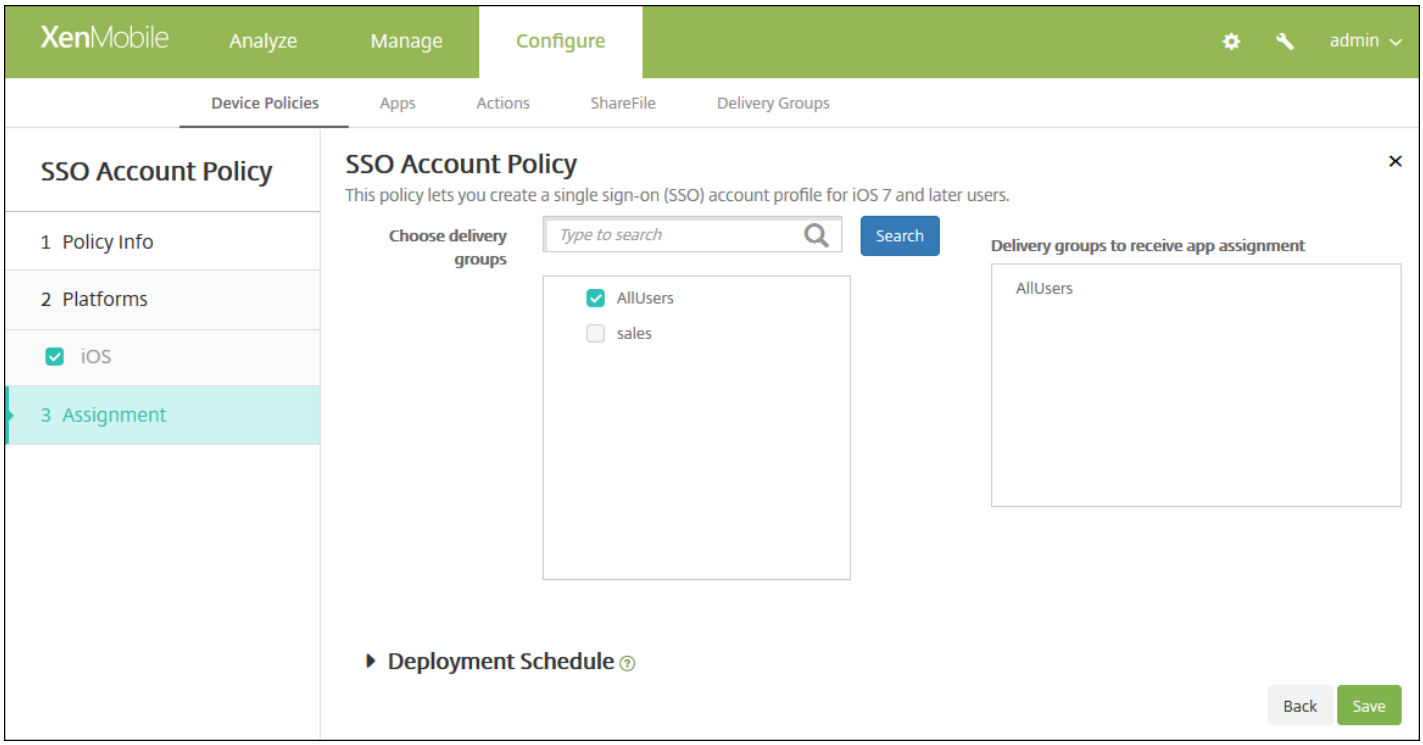
显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

要编辑现有 URL 或应用程序标识符，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **SSO 帐户策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

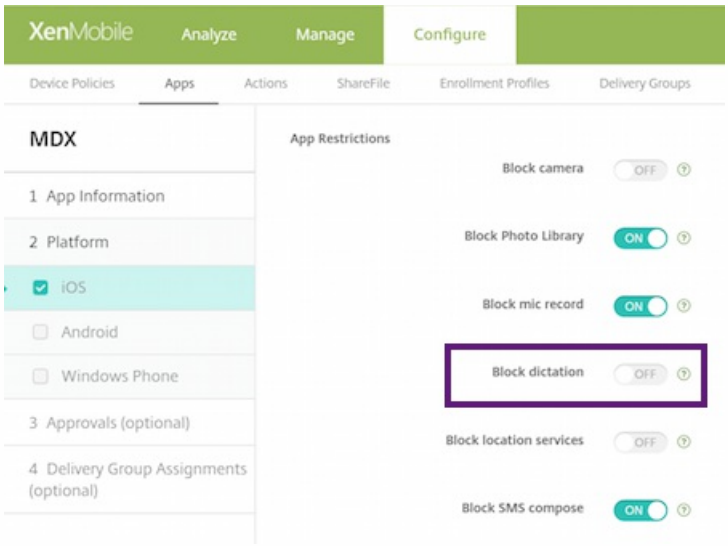
Siri 和听写策略

Aug 11, 2016

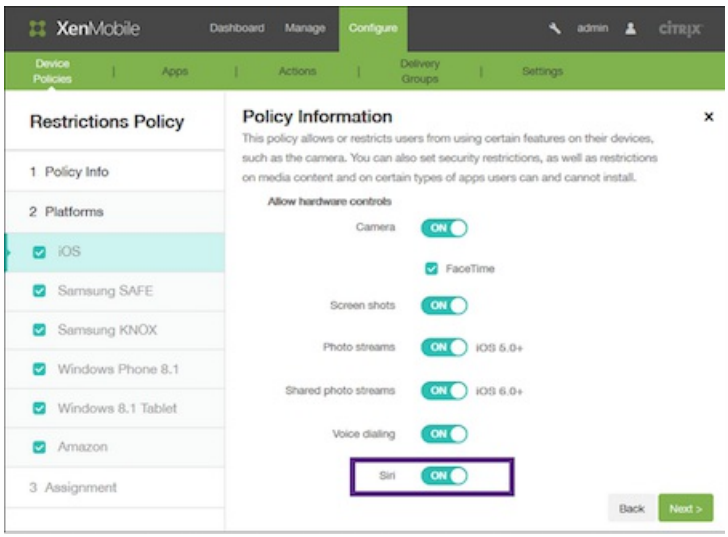
用户向 Siri 提问时或在托管 iOS 设备上听写文本时，Apple 将收集语音数据以改进 Siri 的功能。 语音数据通过 Apple 的基于云的服务传输，因此存在于安全的 XenMobile 容器外部。 但是，由听写产生的文本仍保留在容器内部。

XenMobile 允许您根据安全性要求阻止 Siri 和听写服务。

在 MAM 部署中，每个应用程序的**阻止听写**策略都默认设置为**开**，这样将禁用设备的麦克风。 如果要允许听写，请将其设置为**关**。 可以在 XenMobile 控制台的**配置 > 应用程序**下找到该策略。 选择应用程序，单击**编辑**，然后单击 **iOS**。



在 MDM 部署中，还可以通过**配置 > 设备策略 > 限制策略 > iOS** 下的 Siri 策略禁用 Siri。 默认允许使用 Siri。



决定是否允许使用 Siri 和听写服务时，需要注意以下几点事项：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 根据 Apple 公开发布的信息，Apple 最长将保留 Siri 和听写语音数据两年时间。 该数据将被分配一个随机编号以代表用户，并且语音文件与此随机编号相关联。 有关详细信息，请参阅此 Wired 文章 Apple reveals how long Siri keeps your data（Apple 揭示 Siri 保留数据的时长）。
- 可以通过在任意 iOS 设备上转至**设置 > 通用 > 键盘**并轻按**启用听写**下的链接来查看 Apple 的隐私政策。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

存储加密设备策略

Aug 11, 2016

在 XenMobile 中创建存储加密设备策略，以加密内部存储和外部存储，并根据设备阻止用户在其设备上使用存储卡。

可以创建适用于 Samsung SAFE、Windows Phone 和 Android Sony 设备的策略。 每种平台需要一组不同的值，本文将对此进行详细介绍。

Samsung SAFE 设置

Windows Phone 设置

Android Sony 设置

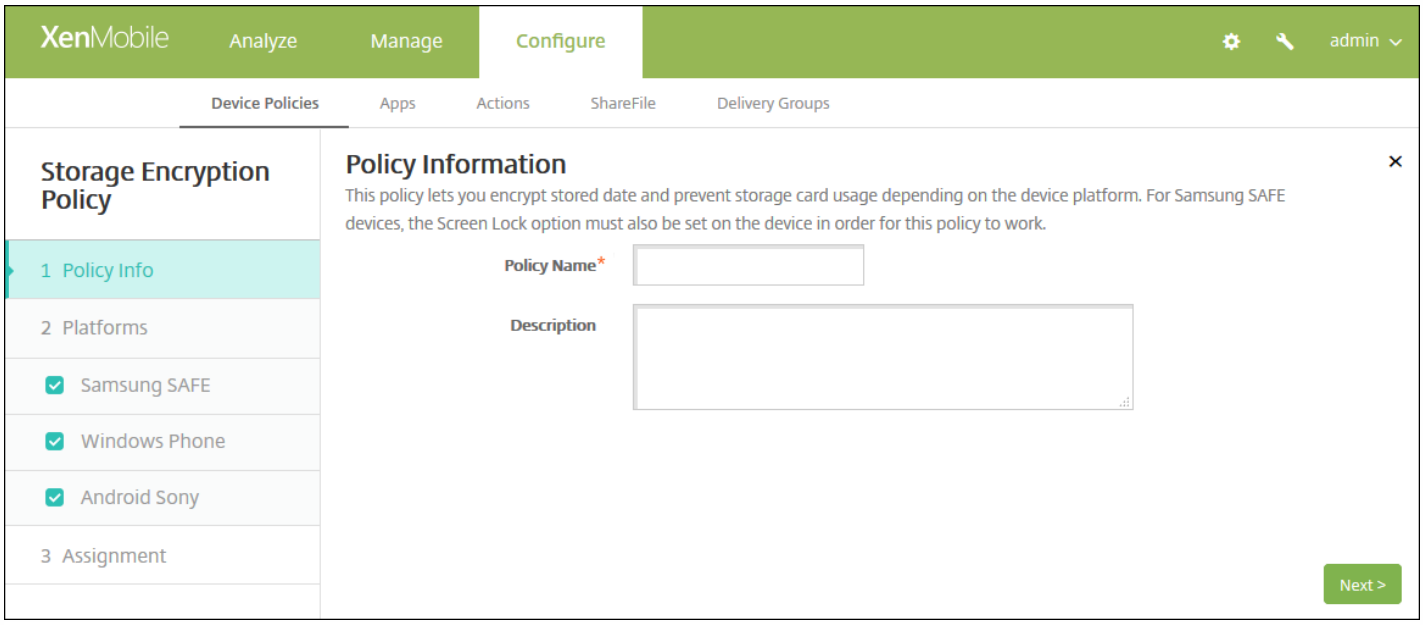
注意：对于 Samsung SAFE 设备，在配置此策略之前，请确保满足以下要求：

- 必须在用户设备上设置屏幕锁定选项。
- 用户设备必须已接通电源并且已充电 80%。
- 设备必须使用包含数字和字母或符号的密码。

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. 单击**更多**，然后在**安全性**下面，单击**存储加密**。 此时将显示 **Storage Encryption Policy**（存储加密策略）信息页面。



4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

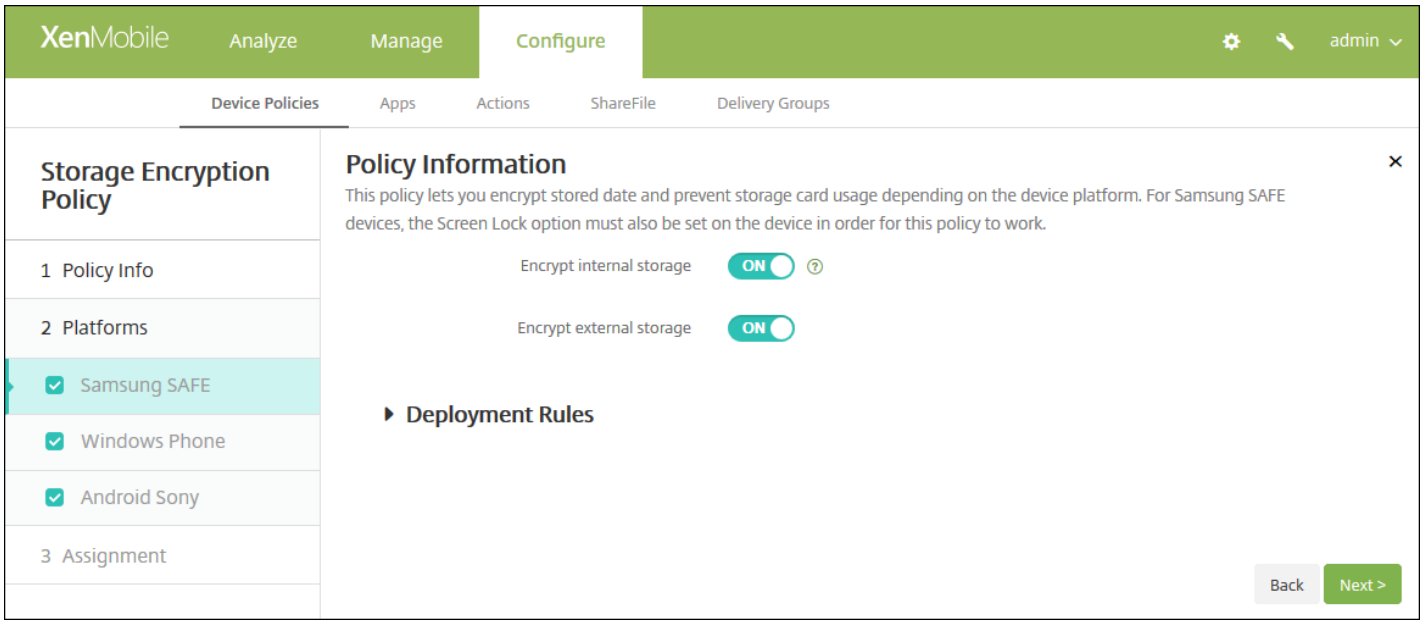
5. 单击**下一步**。 此时将显示**策略平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

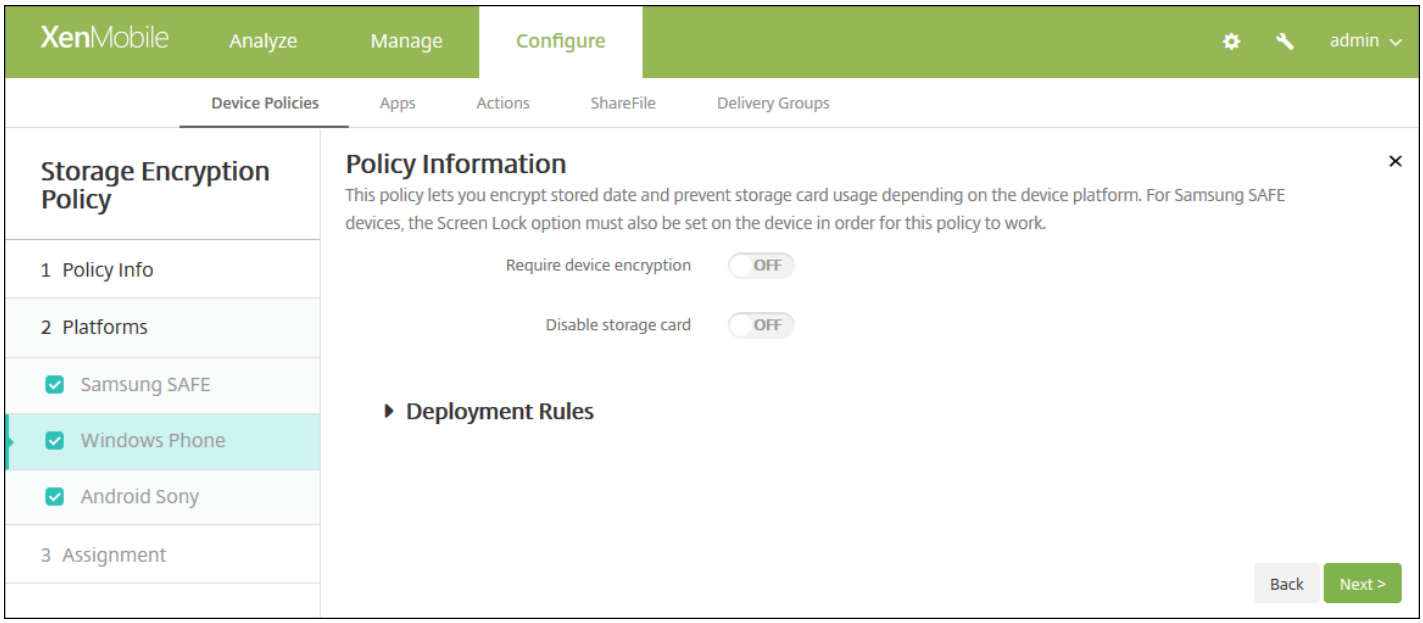
配置 Samsung SAFE 设置



配置以下设置：

- **加密内部存储**：选择是否加密用户设备上的内部存储。 内部存储包括设备内存和内部存储器。 默认值为**开**。
- **加密外部存储**：选择是否加密用户设备上的外部存储。 默认值为**开**。

配置 Windows Phone 设置

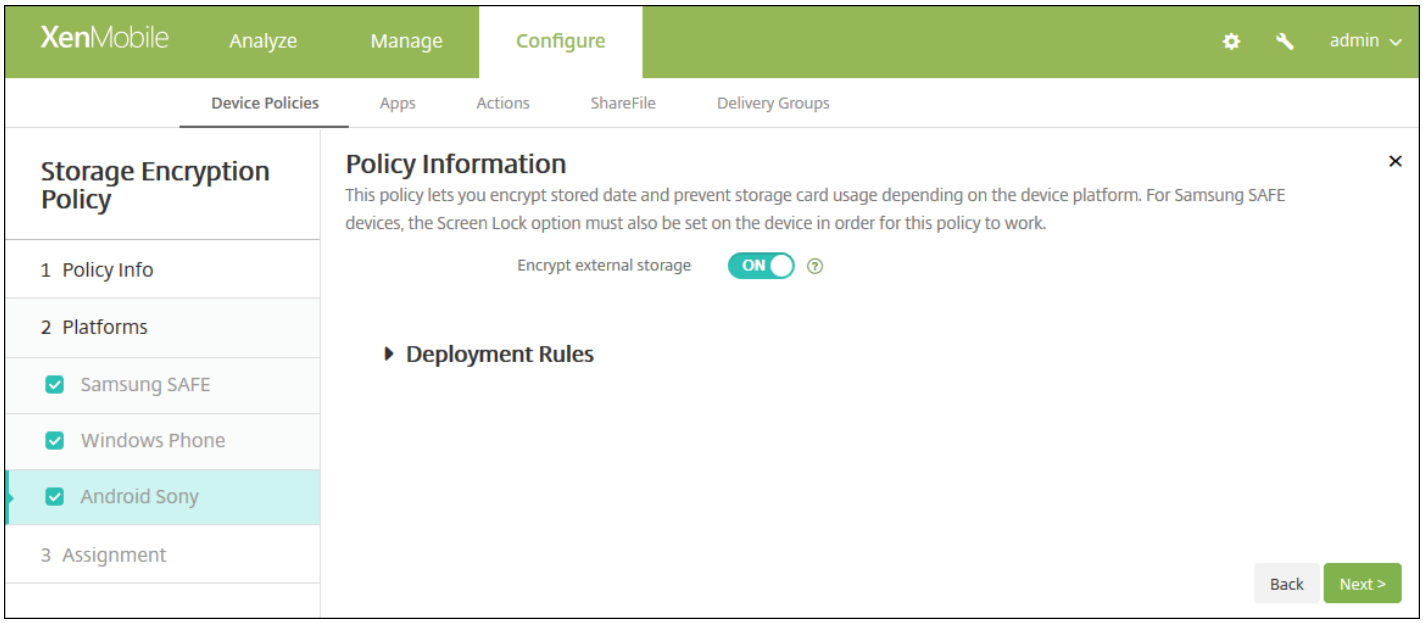


配置以下设置：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **要求设备加密**：选择是否加密用户的设备。 默认值为**关**。
- **禁用存储卡**：选择是否阻止用户在其设备上使用存储卡。 默认值为**关**。

配置 Android Sony 设置



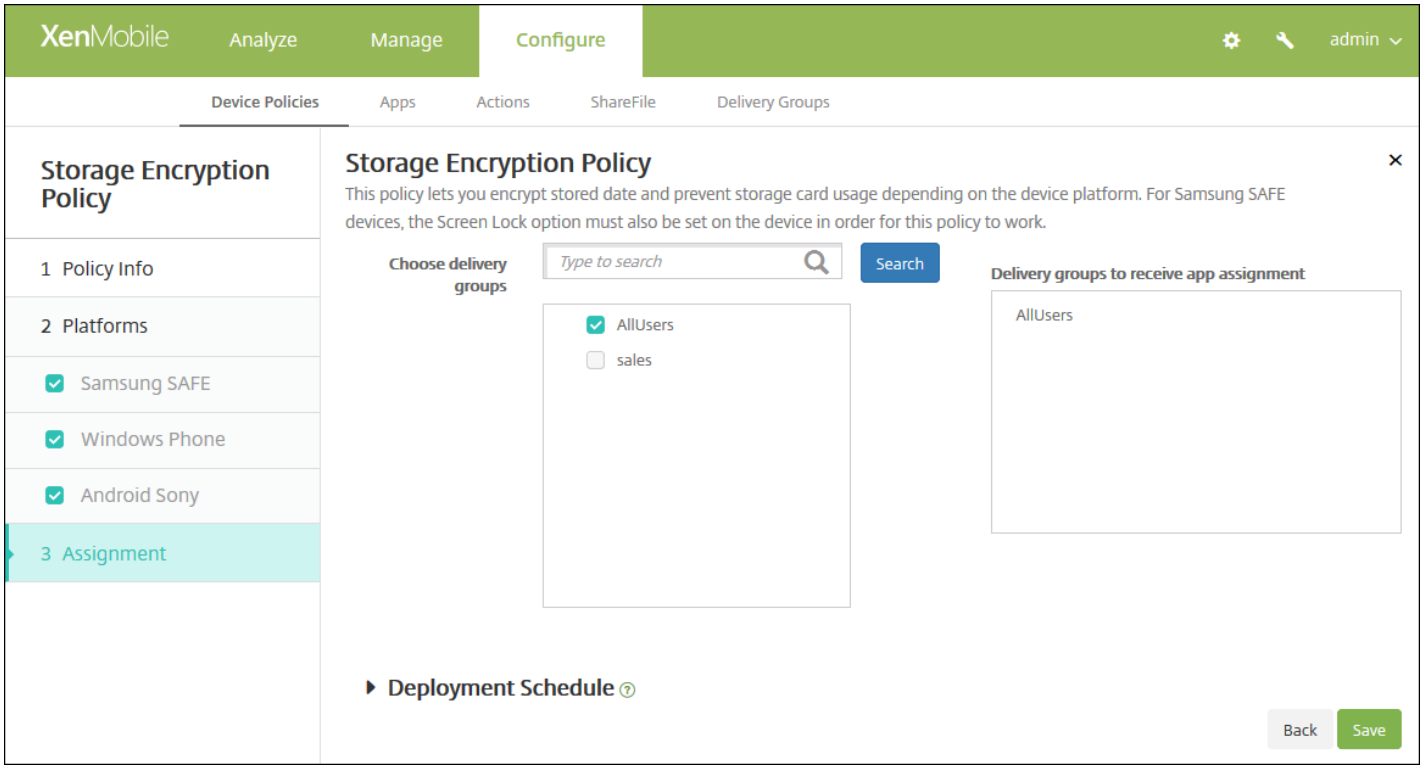
配置以下设置：

- **加密外部存储**：选择是否加密用户设备上的外部存储。 设备必须使用包含数字和字母或符号的密码。 默认值为**开**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**存储加密策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

已订阅的日历设备策略

Aug 11, 2016

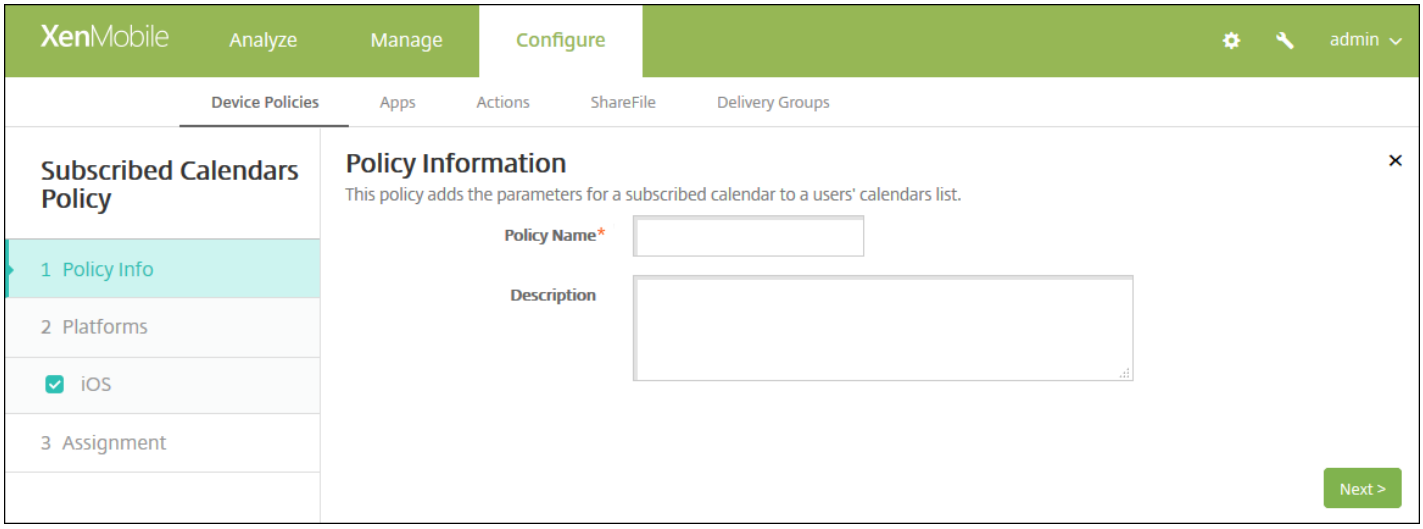
您可以在 XenMobile 中添加一个设备策略，以便在用户的 iOS 设备上向日历列表中添加已订阅的日历。www.apple.com/downloads/macosx/calendars 提供了您可以订阅的公共日历列表。

注意：必须已经订阅某个日历，才能将其添加到用户设备上已订阅的日历列表中。

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. 单击**更多**，然后在**最终用户**下，单击**已订阅的日历**。 此时将显示**已订阅的日历策略**页面。

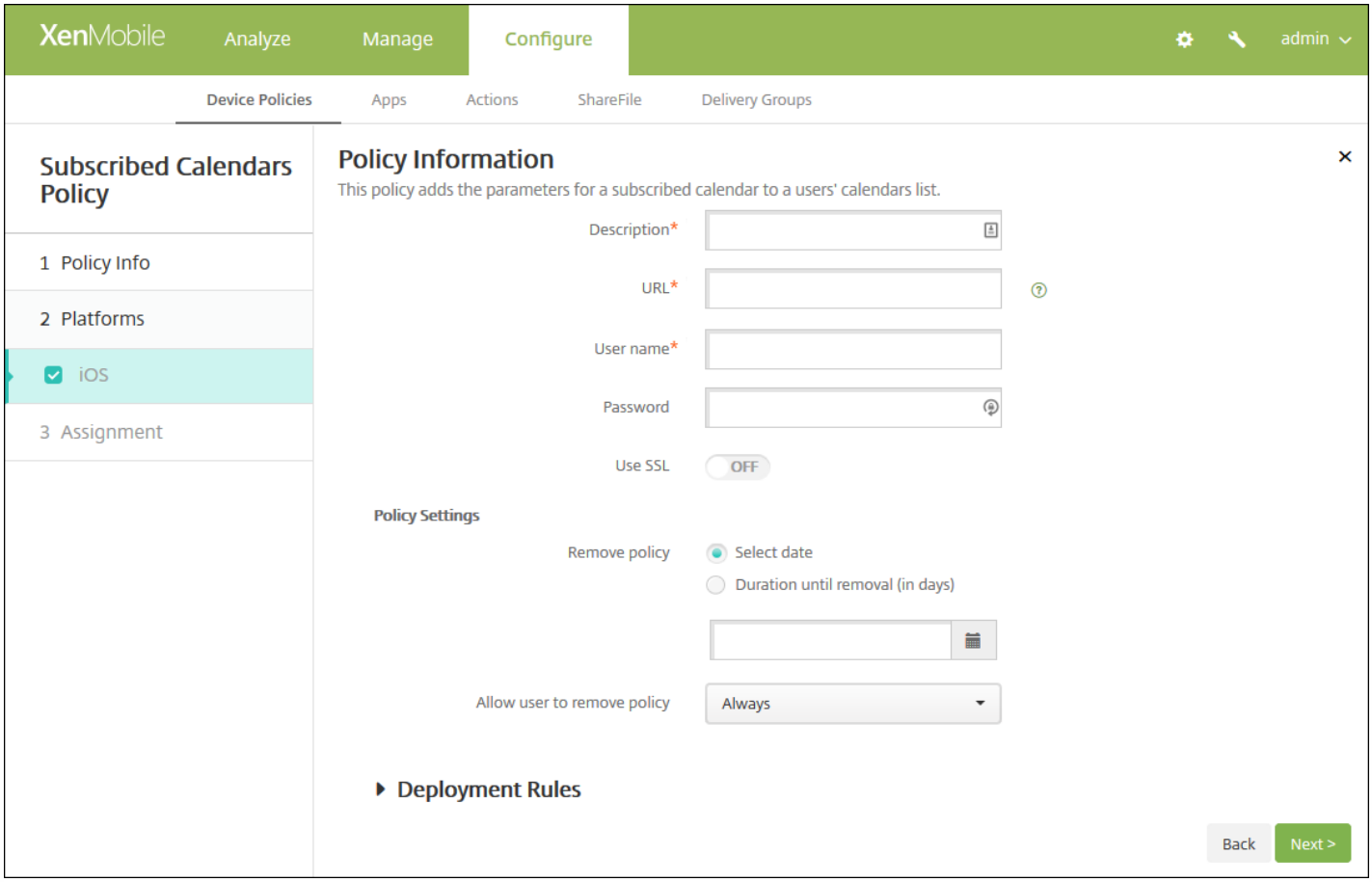


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台信息**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



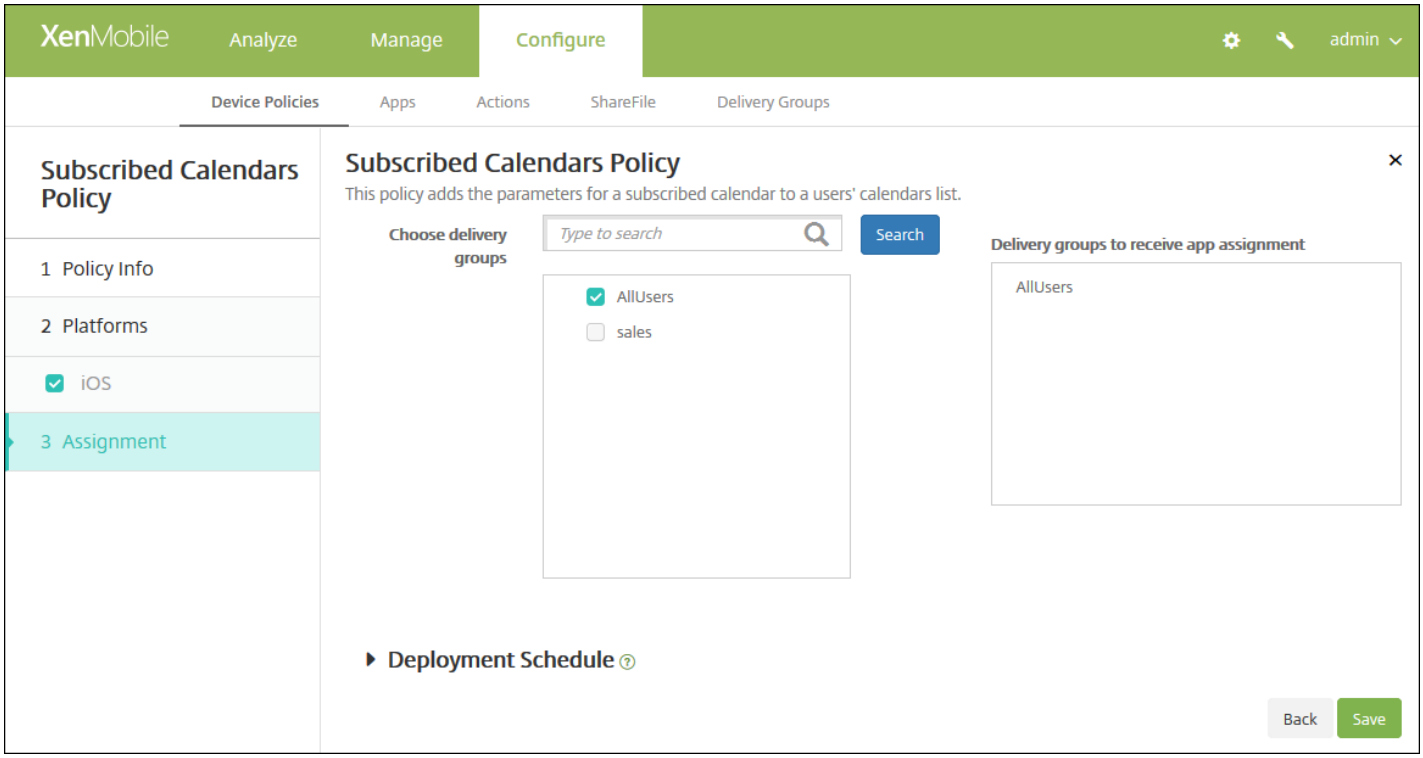
6. 配置以下设置：

- **说明**：输入日历的说明。 此字段为必填字段。
- **URL**：输入日历 URL。 可以输入 iCalendar 文件 (.ics) 的 webcal:// URL 或 http:// 链接。 此字段为必填字段。
- **用户名**：输入用户的 登录 名。 此字段为必填字段。
- **密码**：输入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到日历。 默认值为“关”。
- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**已订阅的日历策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

条款和条件设备策略。

Aug 11, 2016

如果希望用户接受贵公司用于控制企业网络连接的特定政策，可以在 XenMobile 中创建条款和条件设备策略。 当用户向 XenMobile 注册其设备时，系统会向其显示条款和条件，用户必须接受这些条款和条件才能注册其设备。 拒绝这些条款和条件会取消注册过程。

如果贵公司具有国际用户，并且希望用户接受采用其本地语言描述的条款和条件，则可以采用不同的语言创建不同的条款和条件策略。 必须为计划部署的每个平台和语言组合提供一个文件。 对于 Android 和 iOS 设备，必须提供 PDF 文件。 对于 Windows 设备，必须提供文本 (.txt) 文件和随附的图像文件。

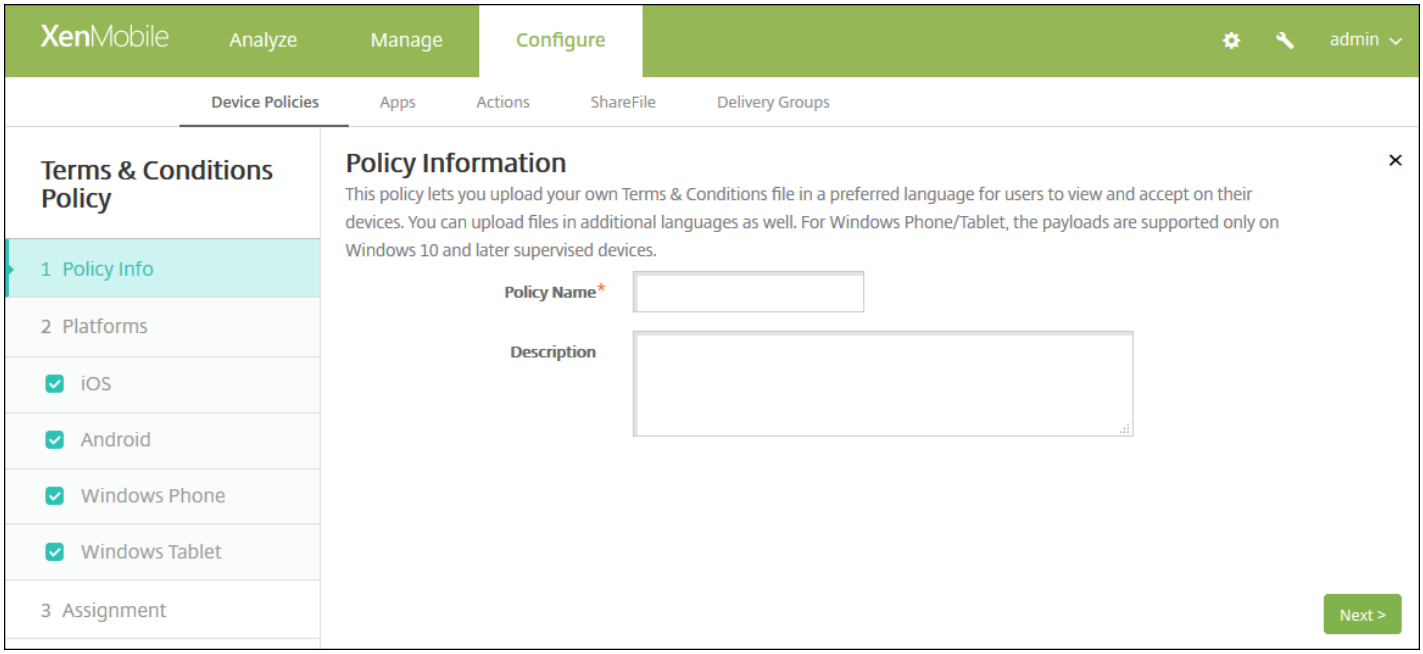
iOS 和 Android 设置

Windows Phone 和 Windows Tablet 设置

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. 单击**条款和条件**。 此时将显示**条款和条件策略**页面。

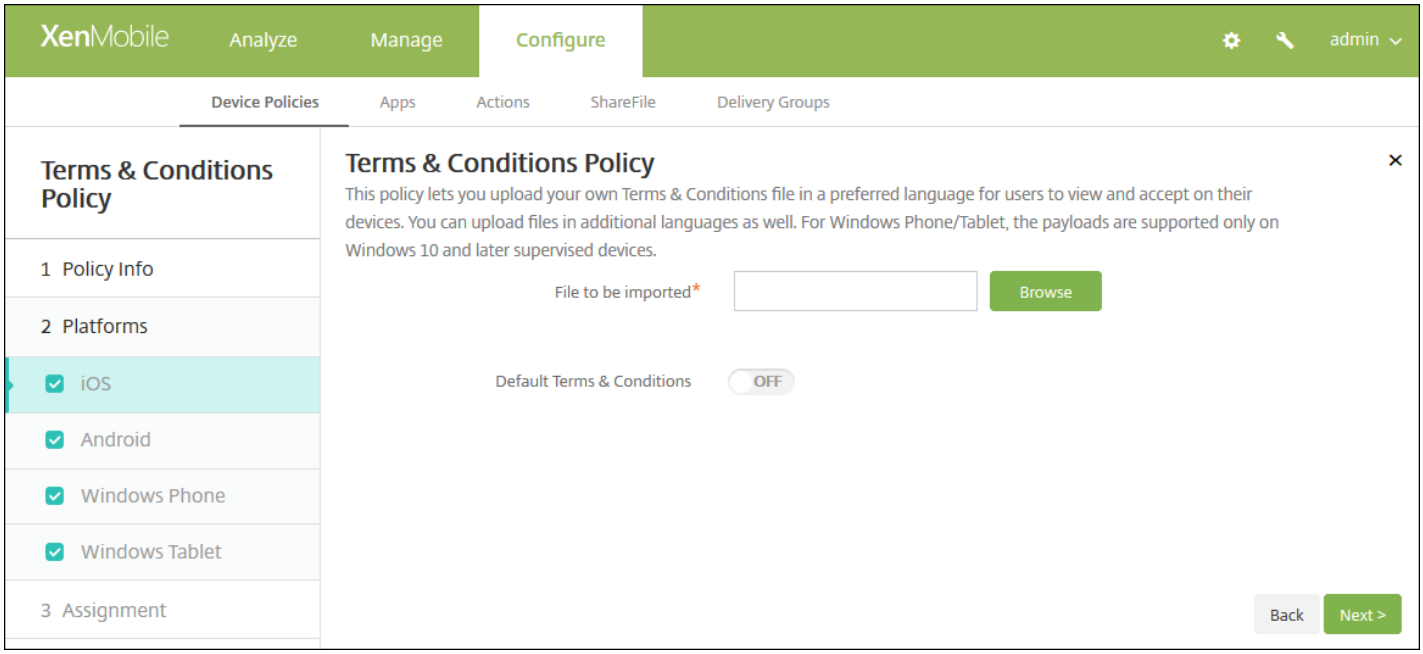


4. 在**策略信息**窗格中，输入以下信息：

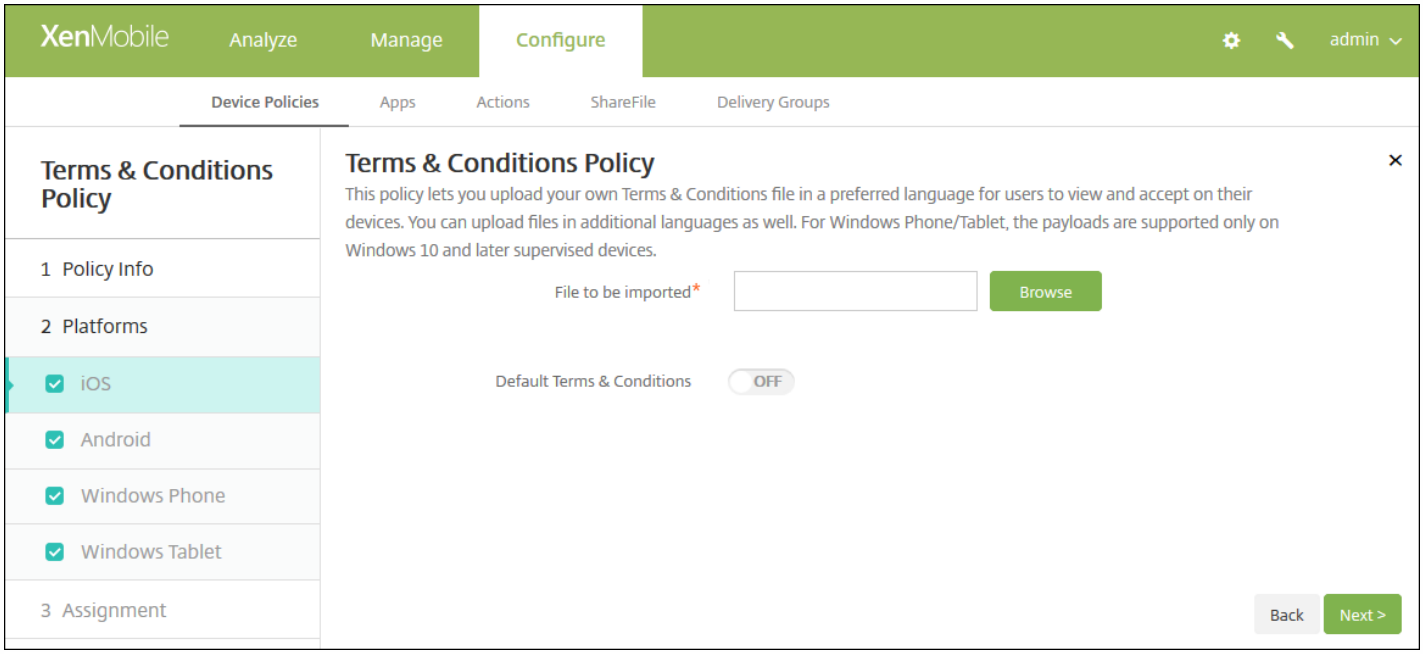
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示**条款和条件平台**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



iOS 和 Android 设置

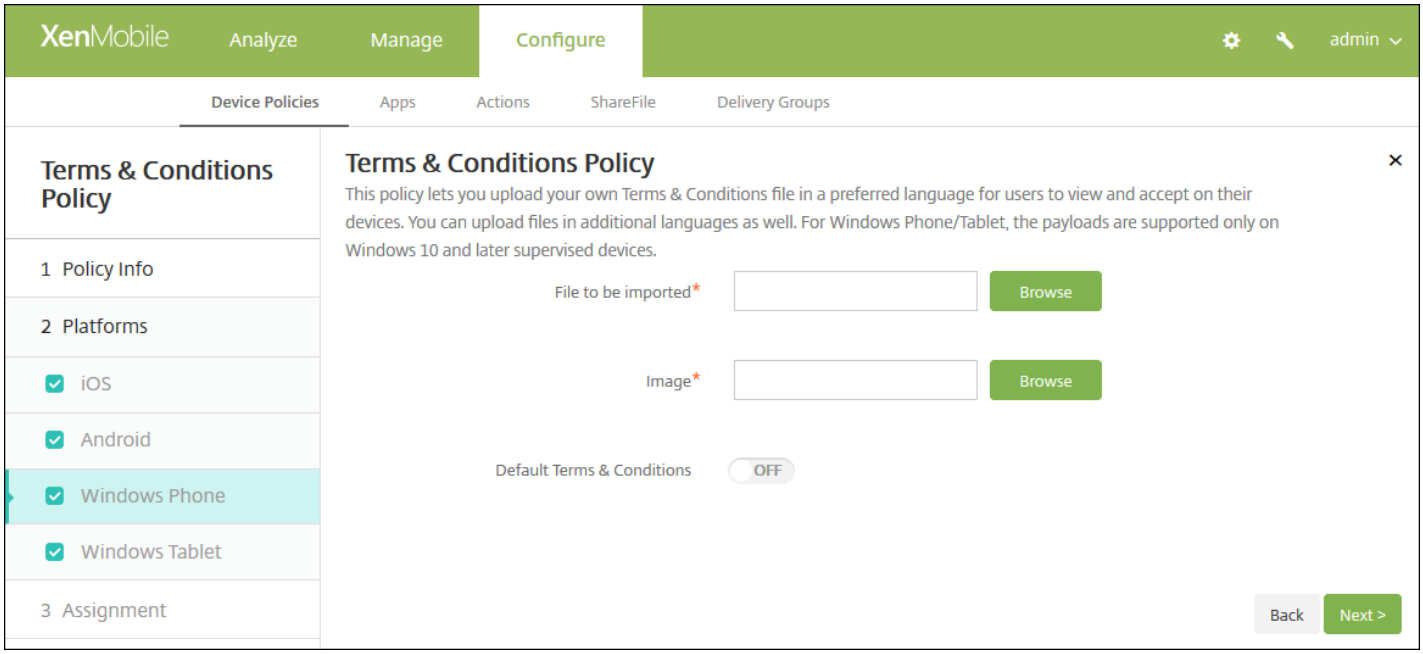


配置以下设置：

- **要导入的文件**：单击**浏览**，然后导航到要导入的条款和条件文件的位置，选择此文件。
- **默认条款和条件**：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。 默认值为**关**。

Windows Phone 和 Windows Tablet 设置

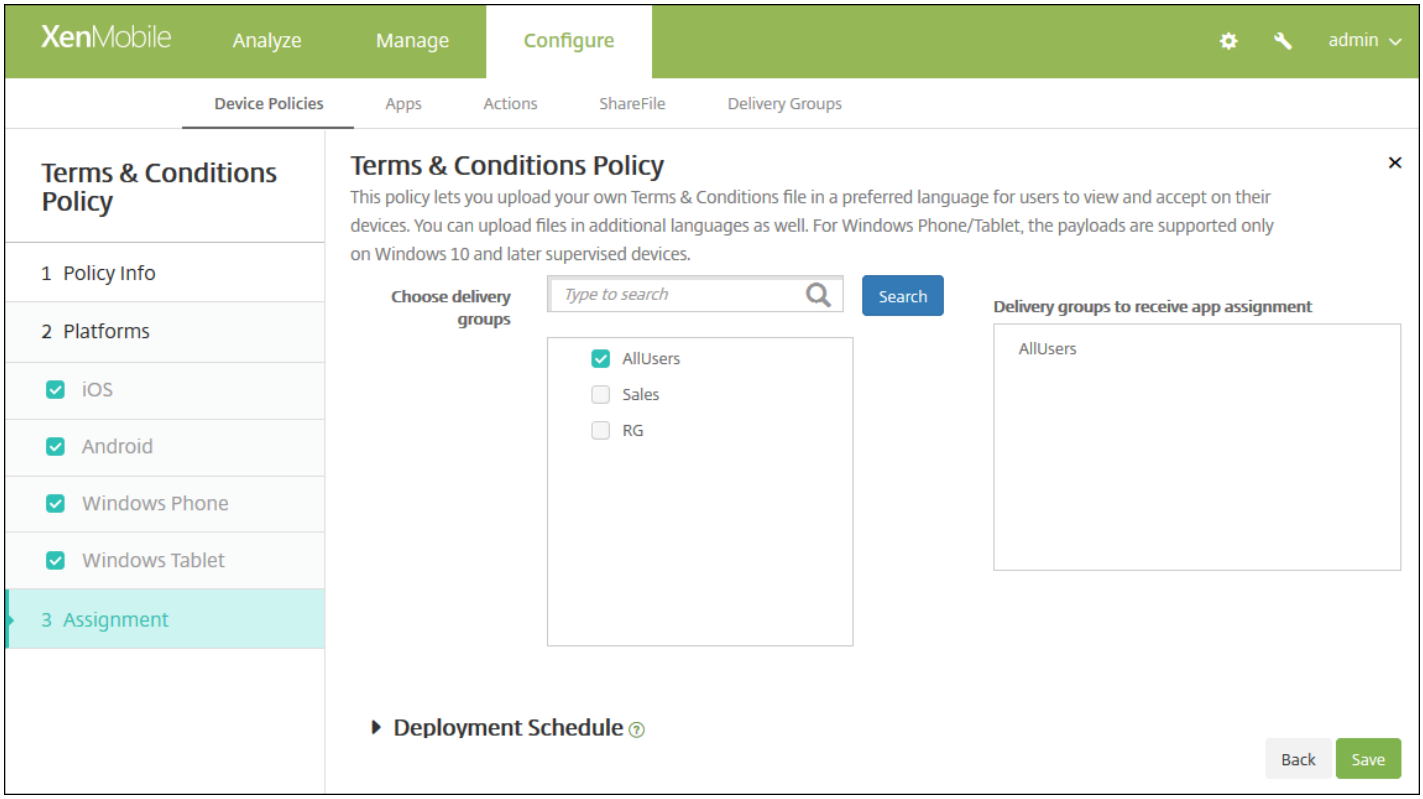
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **要导入的文件**：单击**浏览**，然后导航到要导入的条款和条件文件的位置，选择此文件。
- **图片**：单击**浏览**并导航到要导入的图片文件的位置，选择此文件。
- **默认条款和条件**：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。 默认值为**关**。

6. 单击**下一步**。 此时将显示**条款和条件策略**分配页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

8. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用 Apple Configurator 将 iOS 设备置于受监督模式

Aug 11, 2016

要使用 Apple Configurator，需要一台运行 OS X 10.7.2 或更高版本的 Apple 计算机。

> **Important**
>
> 将设备置于受监督模式时，系统将会在设备上安装所选版本的 iOS，同时完全擦除设备上以前存储的任何用户数据或应用程序。

1. 从 iTunes 安装 Apple Configurator。
2. 将 iOS 设备连接到 Apple 电脑。
3. 启动 Apple Configurator。 Configurator 显示您有一台设备需要进行监督前的准备工作。
4. 设备监督前准备工作：
    1. 将 Supervision（监督）控件值切换到 On（启用）。 如果您打算通过定期重新应用配置来随时维护对设备的控制，Citrix 建议您选择此设置。
    2. 提供设备的名称（可选）。
    3. 在 iOS 中，单击 Latest（最新），获取您要安装的最新版本的 iOS。
5. 当您准备进行设备监督前的准备工作时，请单击 Prepare（准备）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VPN 设备策略

Oct 21, 2016

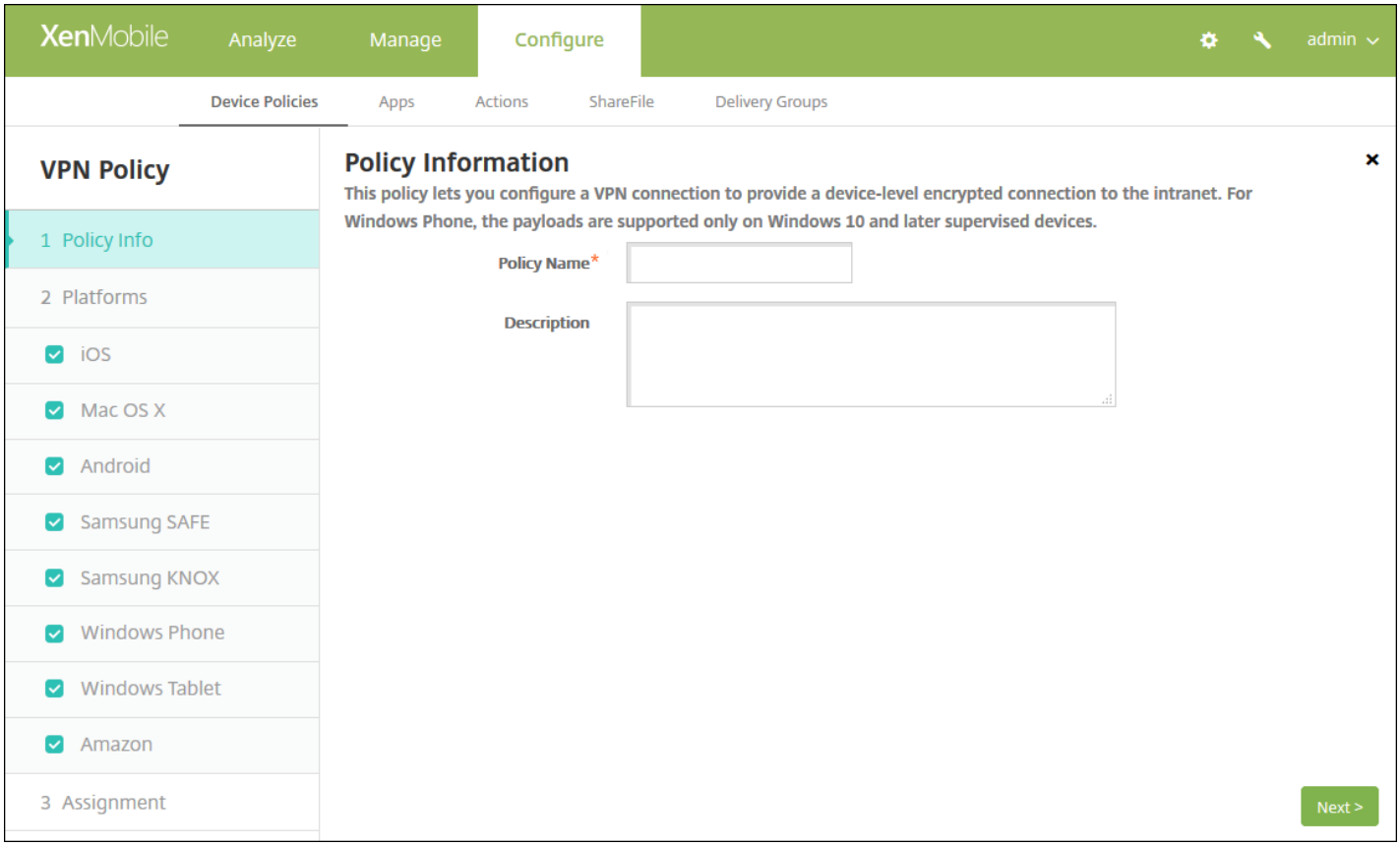
可以在 XenMobile 中添加用于配置虚拟专用网络 (VPN) 设置的设备策略，使用户设备安全地连接到企业网络。 可以为以下平台配置 VPN 策略：iOS、Android（包括为 Android for Work 启用的设备）、Samsung SAFE、Samsung KNOX、Windows Tablet、Windows Phone 和 Amazon。 每种平台需要一组不同的值，本文将对此进行详细介绍。

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. 单击 **VPN**。 此时将显示 **VPN 策略**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 在**策略信息**窗格中，输入以下信息：

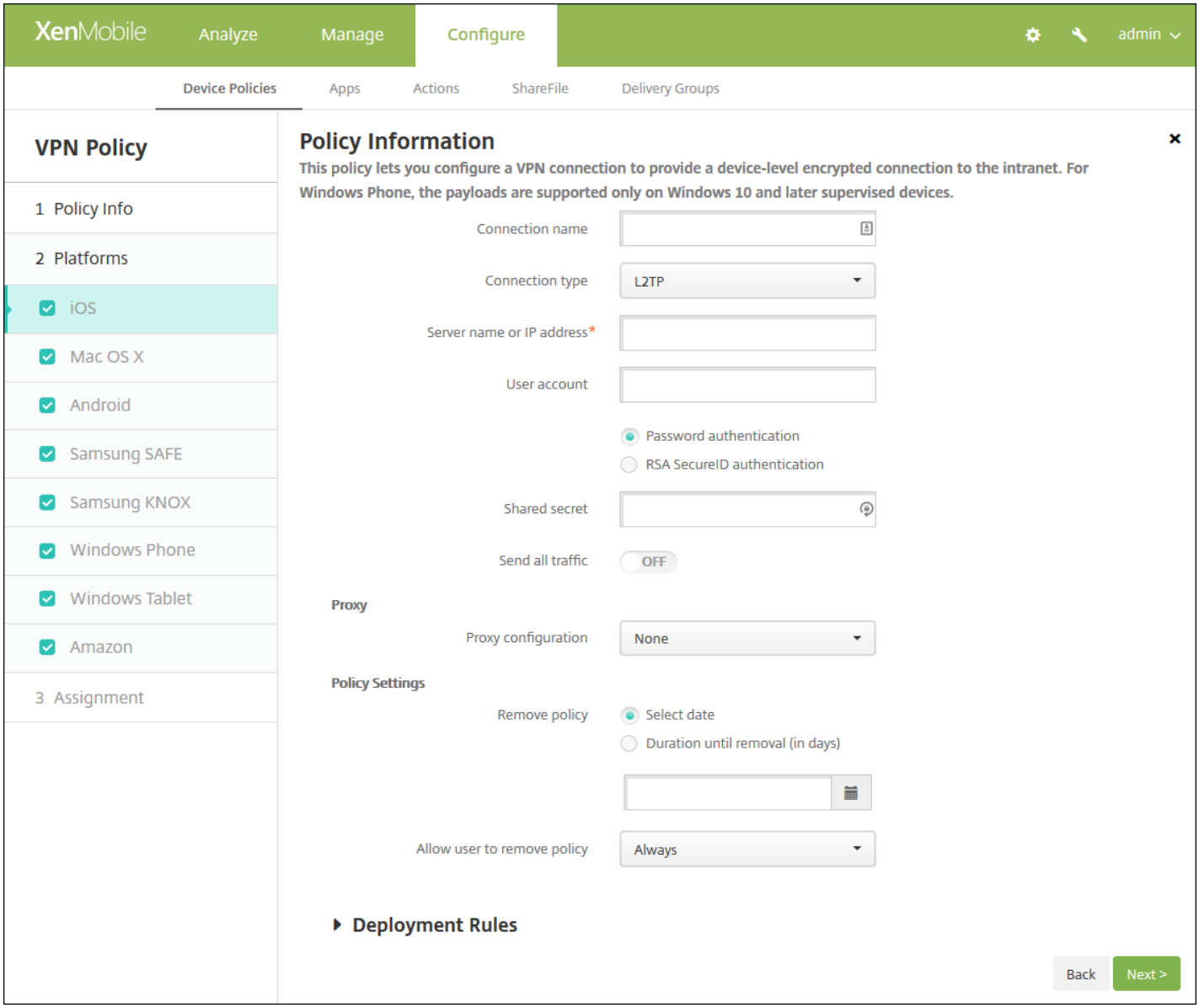
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。 显示**策略平台**页面时，会选中所有平台，并且首先看到 iOS 平台。

6. 在**平台**下面，选择要添加的一个或多个平台。 清除不希望配置的平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置

- **连接名称**：键入连接的名称。
- **连接类型**：在列表中，单击将用于此连接的协议。 默认值为 **L2TP**。
  - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
  - **PPTP**：点对点通道。
  - **IPSec**：企业 VPN 连接。
  - **Cisco AnyConnect**：Cisco AnyConnect VPN 客户端。
  - **Juniper SSL**：Juniper Networks SSL VPN 客户端。
  - **F5 SSL**：F5 Networks SSL VPN 客户端。
  - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。
  - **Ariba VIA**：Ariba Networks Virtual Internet Access 客户端。
  - **IKEv2（仅限 iOS）**：仅限适用于 iOS 的 Internet Key Exchange 2。
  - **Citrix VPN**：适用于 iOS 的 Citrix VPN 客户端。
  - **自定义 SSL**：自定义安全套接字层。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

以下部分列出了前面每种连接类型的配置选项。

配置 L2TP 协议

配置 PPTP 协议

配置 IPSec 协议

配置 Cisco AnyConnect 协议

配置 Juniper SSL 协议

配置 F5 SSL 协议

配置 SonicWALL 协议

配置 Ariba VIA 协议

配置 IKEv2 协议

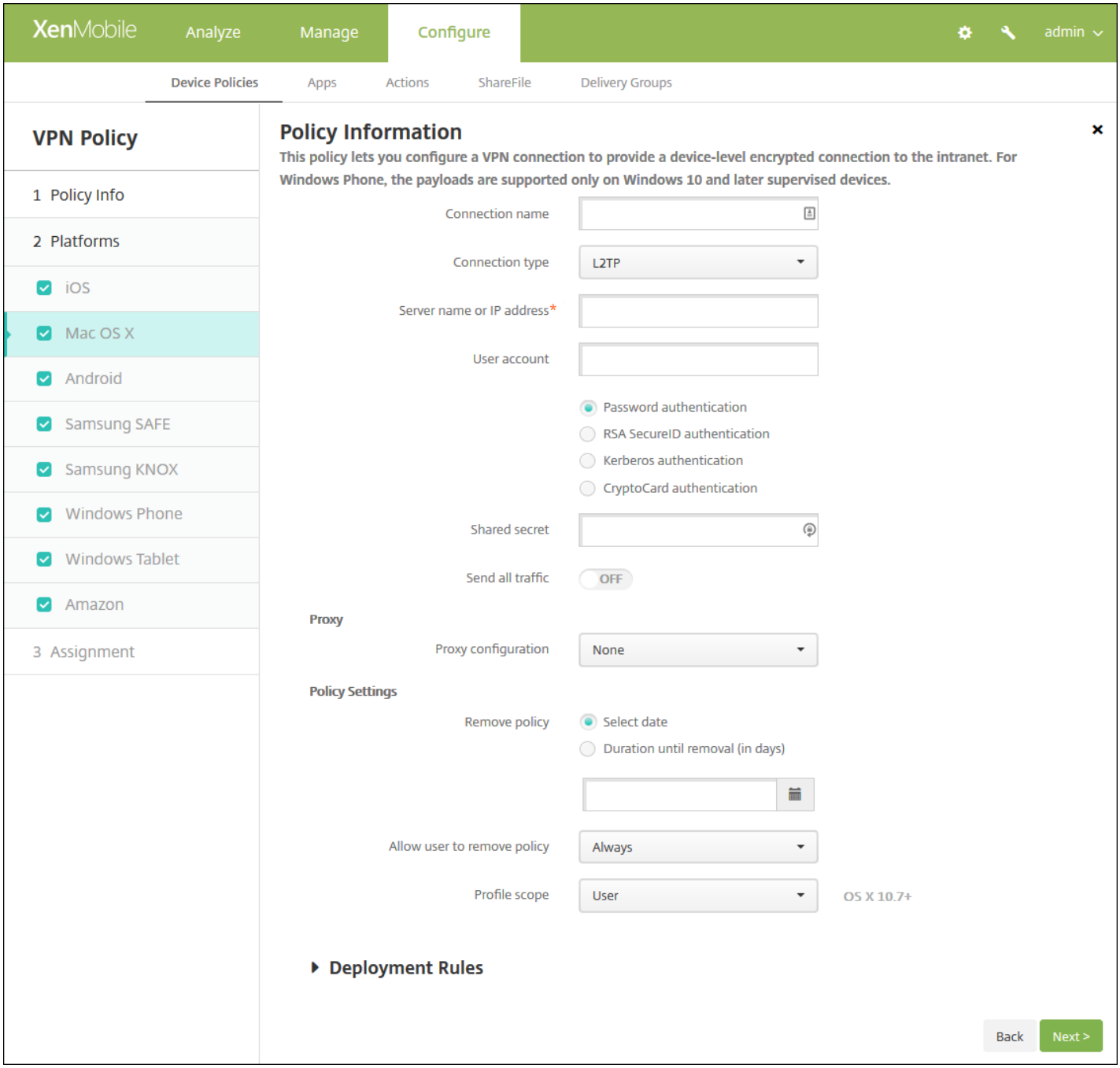
配置 Citrix VPN 协议

配置自定义 SSL 协议

配置“按需启用 VPN”选项

- **代理**
  - **代理配置**：在列表中，选择 VPN 连接通过代理服务器进行路由的方式。 默认值为**无**。
    - 如果启用**手动**，可以配置以下设置：
      - **代理服务器的主机名或 IP 地址**：键入代理服务器的主机名或 IP 地址。 此字段为必填字段。
      - **代理服务器的端口**：键入代理服务器的端口号。 此字段为必填字段。
      - **用户名**：键入可选代理服务器用户名。
      - **密码**：键入可选代理服务器密码。
    - 如果配置**自动**，可以配置以下设置：
      - **代理服务器 URL**：键入代理服务器的 URL。 此字段为必填字段。
- **策略设置**
  - 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **连接名称**：键入连接的名称。
- **连接类型**：在列表中，单击将用于此连接的协议。 默认设置为 L2TP。
  - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
  - **PPTP**：点对点通道。
  - **IPSec**：企业 VPN 连接。
  - **Cisco AnyConnect**：Cisco AnyConnect VPN 客户端。
  - **Juniper SSL**：Juniper Networks SSL VPN 客户端。
  - **F5 SSL**：F5 Networks SSL VPN 客户端。
  - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Ariba VIA**：Ariba Networks Virtual Internet Access 客户端。
- **Citrix VPN**：Citrix VPN 客户端。
- **自定义 SSL**：自定义安全套接字层。

以下部分列出了前面每种连接类型的配置选项。

配置 L2TP 协议

配置 PPTP 协议

配置 IPSec 协议

配置 Cisco AnyConnect 协议

配置 Juniper SSL 协议

配置 F5 SSL 协议

配置 SonicWALL 协议

配置 Ariba VIA 协议

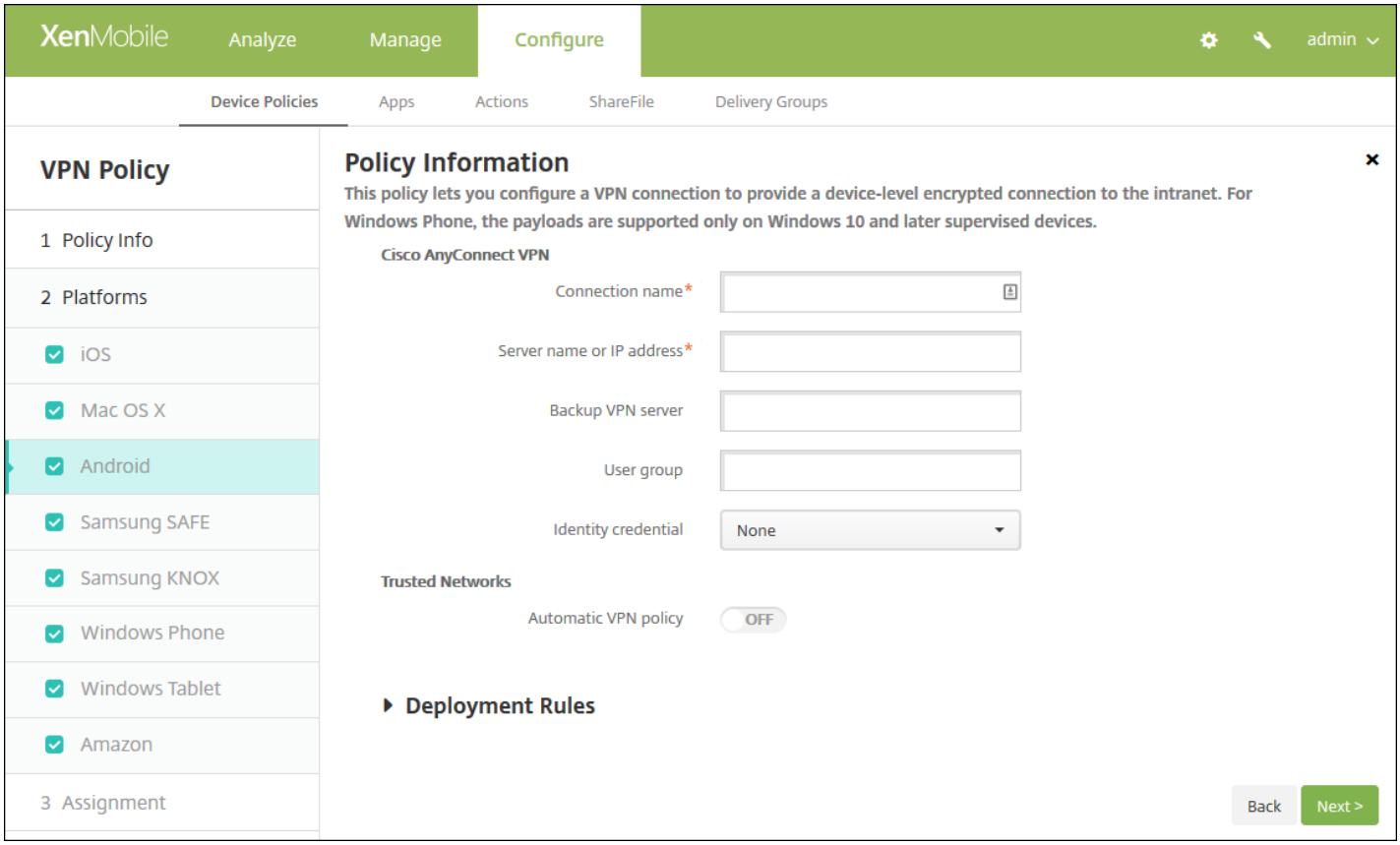
配置 Citrix VPN 协议

配置自定义 SSL 协议

配置“按需启用 VPN”选项

- **代理**
  - **代理配置**：在列表中，选择 VPN 连接通过代理服务器进行路由的方式。 默认值为**无**。
    - 如果启用**手动**，可以配置以下设置：
      - **代理服务器的主机名或 IP 地址**：键入代理服务器的主机名或 IP 地址。 此字段为必填字段。
      - **代理服务器的端口**：键入代理服务器的端口号。 此字段为必填字段。
      - **用户名**：键入可选代理服务器用户名。
      - **密码**：键入可选代理服务器密码。
    - 如果配置**自动**，可以配置以下设置：
      - **代理服务器 URL**：键入代理服务器的 URL。 此字段为必填字段。
- **策略设置**
  - 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

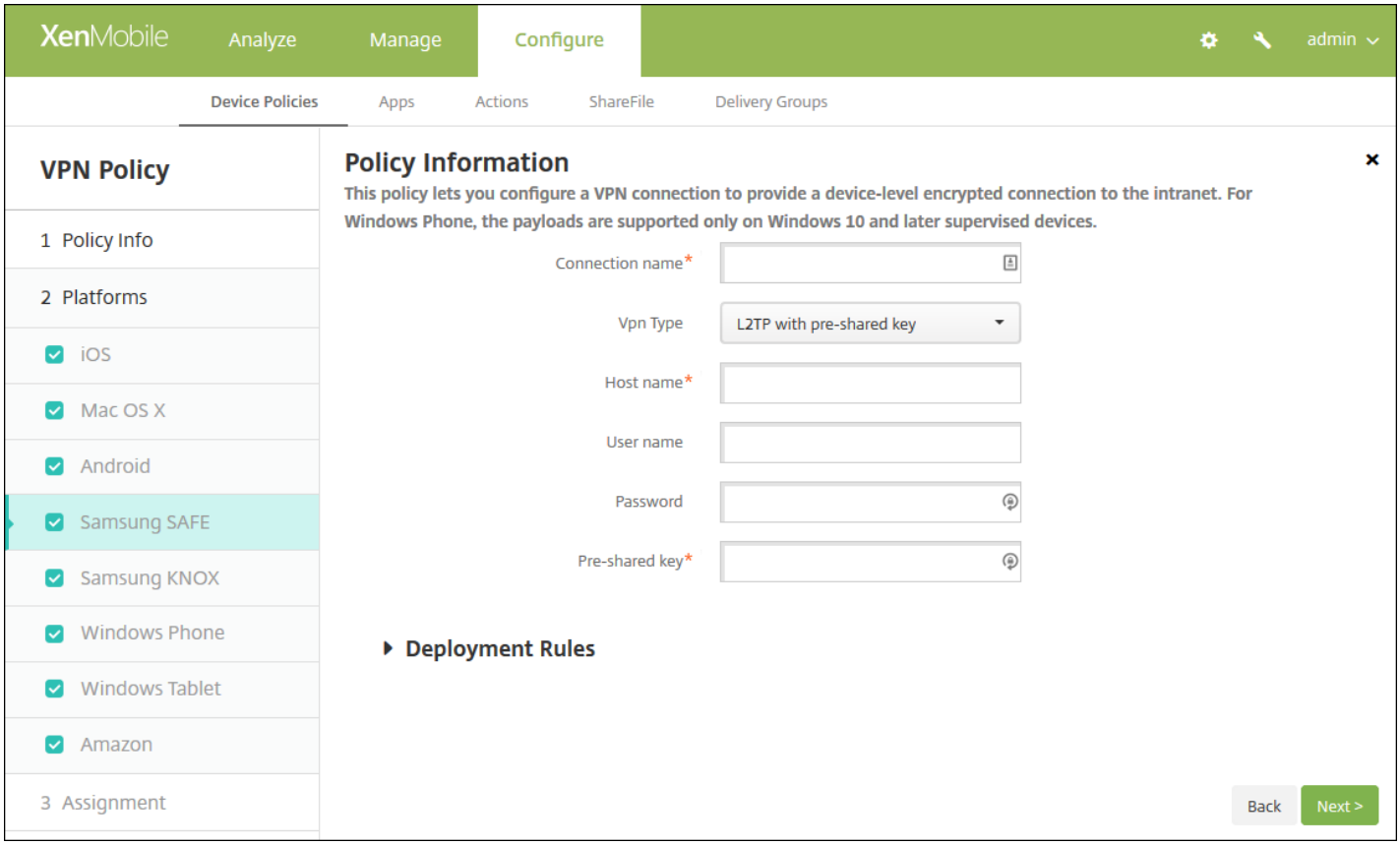
- **Cisco AnyConnect VPN**
  - **连接名称**：输入 Cisco AnyConnect VPN 连接的名称。 此字段为必填字段。
  - **服务器名称或 IP 地址**：键入 VPN 服务器的名称或 IP 地址。 此字段为必填字段。
  - **备份 VPN 服务器**：键入备份 VPN 服务器信息。
  - **用户组**：键入用户组信息。
  - **身份凭据**：在列表中，选择身份凭据。
- **可信网络**
  - **自动 VPN 策略**：启用或禁用此选项，以设置 VPN 响应可信网络和不可信网络的方式。 如果启用，可以配置以下设置：
    - **可信网络策略**：在列表中，单击所需的策略。 默认值为**断开连接**。 可用选项包括：
      - **断开连接**：客户端终止可信网络中的 VPN 连接。 这是默认值。
      - **连接**：客户端在可信网络中启动 VPN 连接。
      - **不执行任何操作**：客户端不执行任何操作。
      - **暂停**：用户在可信网络外部建立 VPN 会话后进入配置为可信的网络时，挂起 VPN 会话（而不是断开会话的连接）。 用户再次离开可信网络时，会话恢复。 这样无需在离开可信网络后建立新的 VPN 会话。
    - **不可信网络策略**：在列表中，单击所需的策略。 默认值为**连接**。 可用选项包括：
      - **连接**：客户端在不可信网络中建立 VPN 连接。
      - **不执行任何操作**：客户端在不可信网络中启动 VPN 连接。 此选项将禁用始终启用 VPN。
  - **可信域**：对于客户端位于可信网络时网络接口可能具有的每个域后缀，请单击**添加**以执行下列操作：
    - **域**：键入要添加的域。
    - 单击**保存**以保存域，或者单击**取消**不保存域。
  - **可信服务器**：对于客户端位于可信网络时网络接口可能具有的每个服务器地址，请单击**添加**以执行下列操作：
    - **服务器**：键入要添加的服务器。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 单击**保存**以保存服务器，或者单击**取消**不保存服务器。

  注意：要删除现有服务器，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击**删除**以删除列表，或单击**取消**以保留此列表。

  要编辑现有服务器，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。



配置以下设置：

- **连接名称**：键入连接的名称。
- **Vpn 类型**：在列表中，单击将用于此连接的协议。 默认值是**带有预共享密钥的 L2TP**. 可用选项包括：
  - **带有预共享密钥的 L2TP**：使用预共享密钥身份验证的第二层通道协议。 此为默认设置。
  - **带有证书的 L2TP**：使用证书的第二层通道协议。
  - **PPTP**：点对点通道。
  - **Enterprise**：企业 VPN 连接。 适用于 SAFE 2.0 之前的版本。
  - **通用**：通用 VPN 连接。 适用于 SAFE 2.0 版或更高版本。

以下部分列出了前面每种 VPN 类型的配置选项。

配置带有预共享密钥的 L2TP 协议

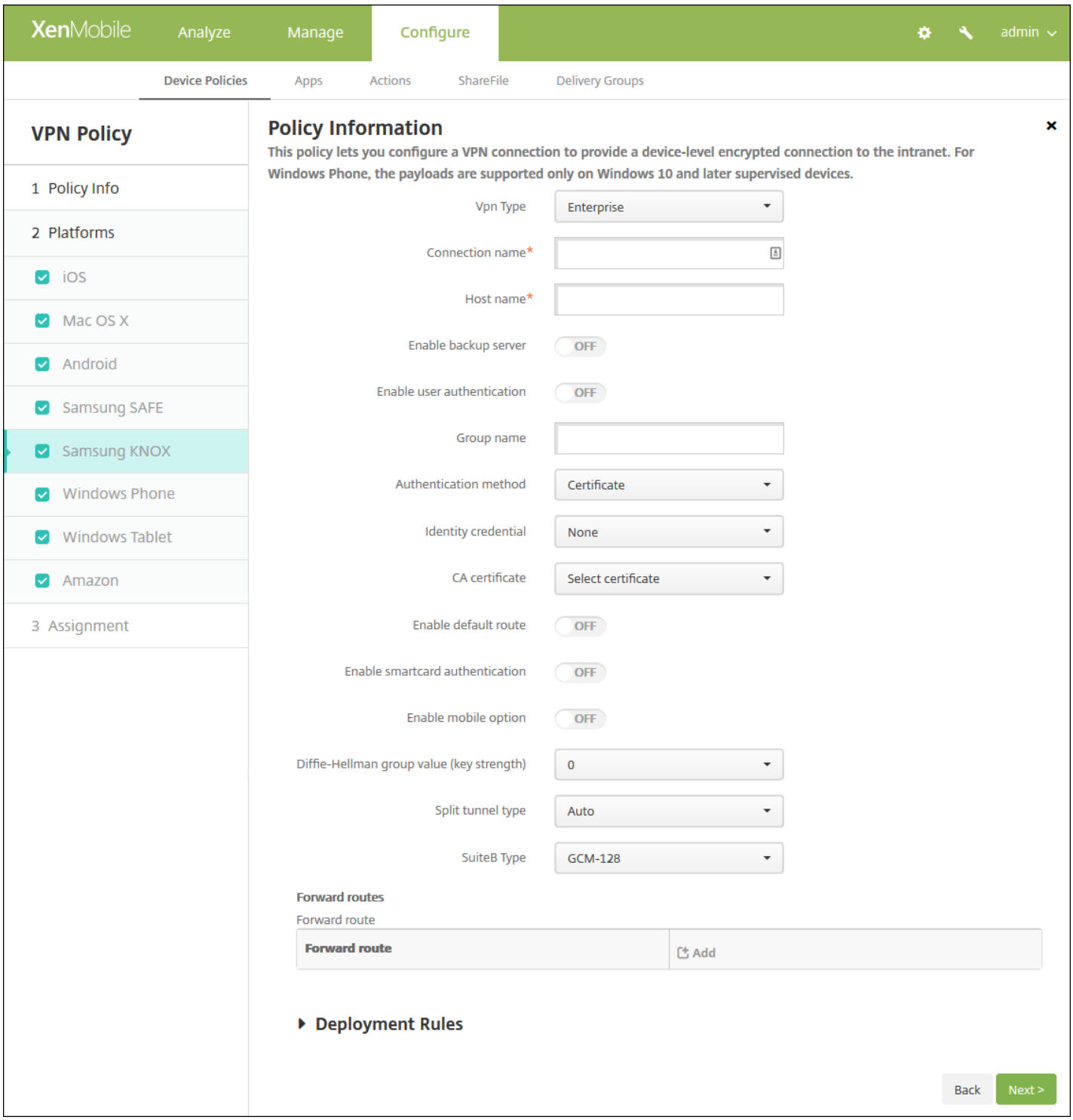
配置使用证书的 L2TP 协议

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置 PPTP 协议

配置企业协议

配置通用协议



© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：为 Samsung KNOX 配置任何策略时，策略仅在 Samsung KNOX 容器内适用。

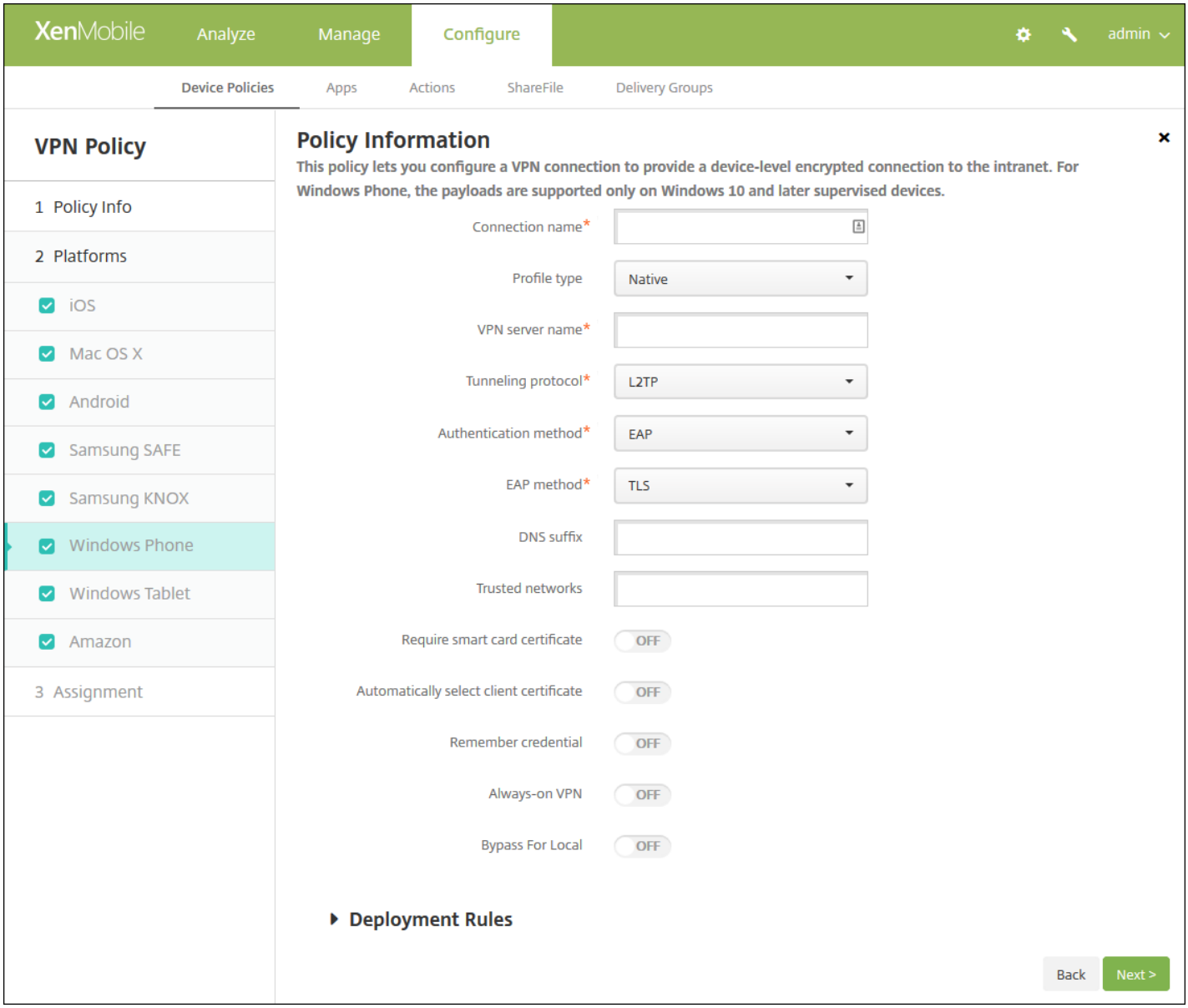
配置以下设置：

- **Vpn 类型**：在列表中，单击**企业**（适用于 KNOX 2.0 之前的版本）或**通用**（适用于 KNOX 2.0 版或更高版本）以配置 VPN 连接类型。 默认值为**企业**。

以下部分列出了前面每种连接类型的配置选项。

配置企业协议

配置通用协议



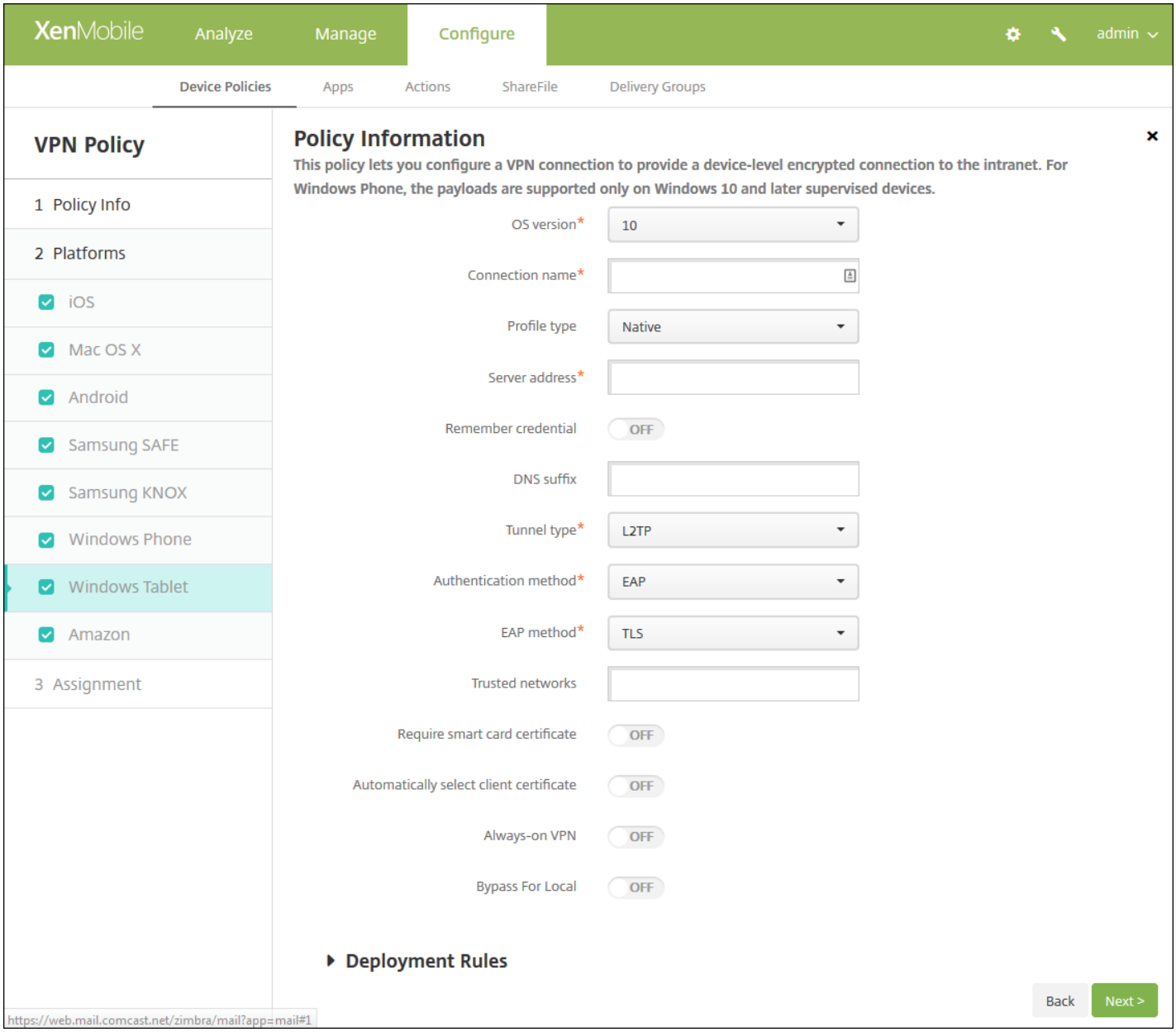
注意：这些设置仅在 Windows 10 及更高版本的受监督设备上受支持。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置以下设置：

- **连接名称**：输入连接的名称。 此字段为必填字段。
- **配置文件类型**：在列表中，单击**本机**或**插件**。 默认值为**本机**。 以下部分将分别介绍这些选项的设置。
- **配置本机配置文件类型设置** - 这些设置适用于内置于用户 Windows 手机的 VPN。
  - **VPN 服务器名称**：键入 VPN 服务器的 FQDN 或 IP 地址。 此字段为必填字段。
  - **通道协议**：在列表中，单击要使用的 VPN 通道的类型。 默认值为 **L2TP**。 可用选项包括：
    - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
    - **PPTP**：点对点通道。
    - **IKEv2**：Internet 密钥交换第 2 版。
  - **身份验证方法**：在列表中，单击要使用的身份验证方法。 默认值为 **EAP**。 可用选项包括：
    - **EAP**：扩展身份验证协议。
    - **MSChapV2**：使用 Microsoft 的质询-握手身份验证相互验证身份。 选择 IKEv2 作为通道类型时，此选项不可用。 选择 MSChapV2 时，会显示**自动使用 Windows 凭据**选项；默认设置为**关**。
  - **EAP 方法**：在列表中，单击要使用的 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
  - **DNS 后缀**：键入 DNS 后缀。
  - **可信网络**：键入无需使用 VPN 连接进行访问的网络列表，用逗号隔开。 例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - **需要智能卡证书**：选择是否需要智能卡证书。 默认值为关。
  - **自动选择客户端证书**：选择是否自动选择用于身份验证的客户端证书。 默认值为关。 启用“需要智能卡证书”时此选项不可用。
  - **记住凭据**：选择是否缓存凭据。 默认值为关。 启用时，会在合适的时候缓存凭据。
  - **始终启用 VPN**：选择是否始终启用 VPN。 默认值为关。 启用后，VPN 连接保持可用，直到用户手动断开连接。
  - **跳过本地地址**：键入地址和端口号，以允许本地资源跳过代理服务器。
- **配置插件协议类型** - 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 URL、 主机名或 IP 地址。
  - **客户端应用程序 ID**：键入 VPN 插件的软件包系列名。
  - **插件配置文件 XML**：单击“浏览”并导航到要使用的自定义 VPN 插件配置文件，选择此文件。 有关格式及详细信息，请联系插件提供商。
  - **DNS 后缀**：键入 DNS 后缀。
  - **可信网络**：键入无需使用 VPN 连接进行访问的网络列表，用逗号隔开。 例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
  - **记住凭据**：选择是否缓存凭据。 默认值为关。 启用时，会在合适的时候缓存凭据。
  - **始终启用 VPN**：选择是否始终启用 VPN。 默认值为关。 启用后，VPN 连接保持可用，直到用户手动断开连接。
  - **跳过本地地址**：键入地址和端口号，以允许本地资源跳过代理服务器。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



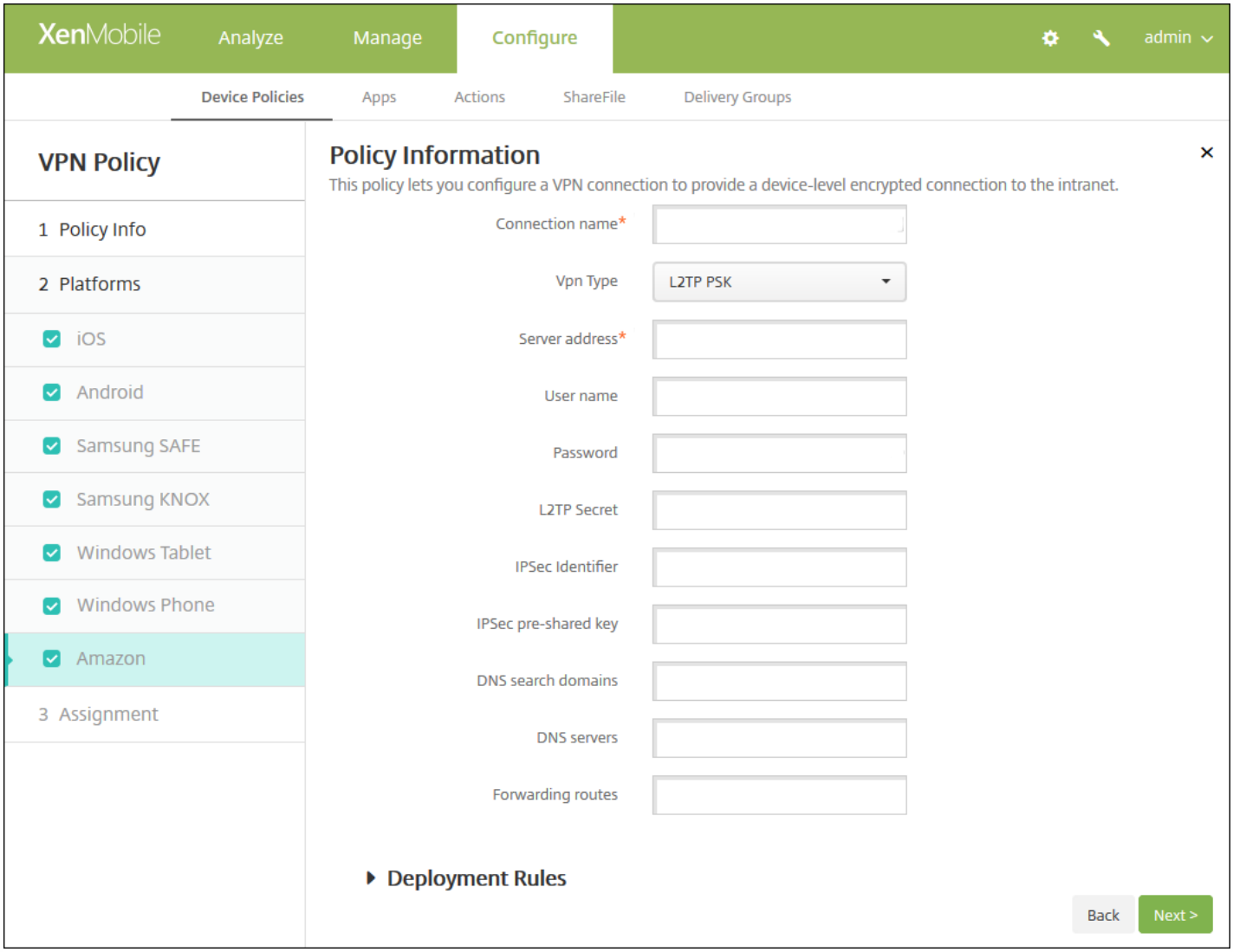
配置以下设置：

- **操作系统版本**：在列表中，单击 **8.1** 以使用 Windows 8.1 或单击 **10** 以使用 Windows 10。默认值为 **10**。

配置 Windows 10 设置

配置 Windows 8.1 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **连接名称**：输入连接的名称。
- **VPN 类型**：单击连接类型。 可用选项包括：
  - **L2TP PSK**：使用预共享密钥身份验证的第二层通道协议。 这是默认值。
  - **L2TP RSA**：使用 RSA 身份验证的第二层通道协议。
  - **IPSEC XAUTH PSK**：使用预共享密钥和扩展身份验证的 Internet 协议安全性。
  - **IPSEC HYBRID RSA**：使用混合 RSA 身份验证的 Internet 协议安全性。
  - **PPTP**：点对点通道。

以下部分列出了前面每种连接类型的配置选项。

配置 L2TP PSK 设置

配置 L2TP RSA 设置

配置 IPSEC XAUTH PSK 设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

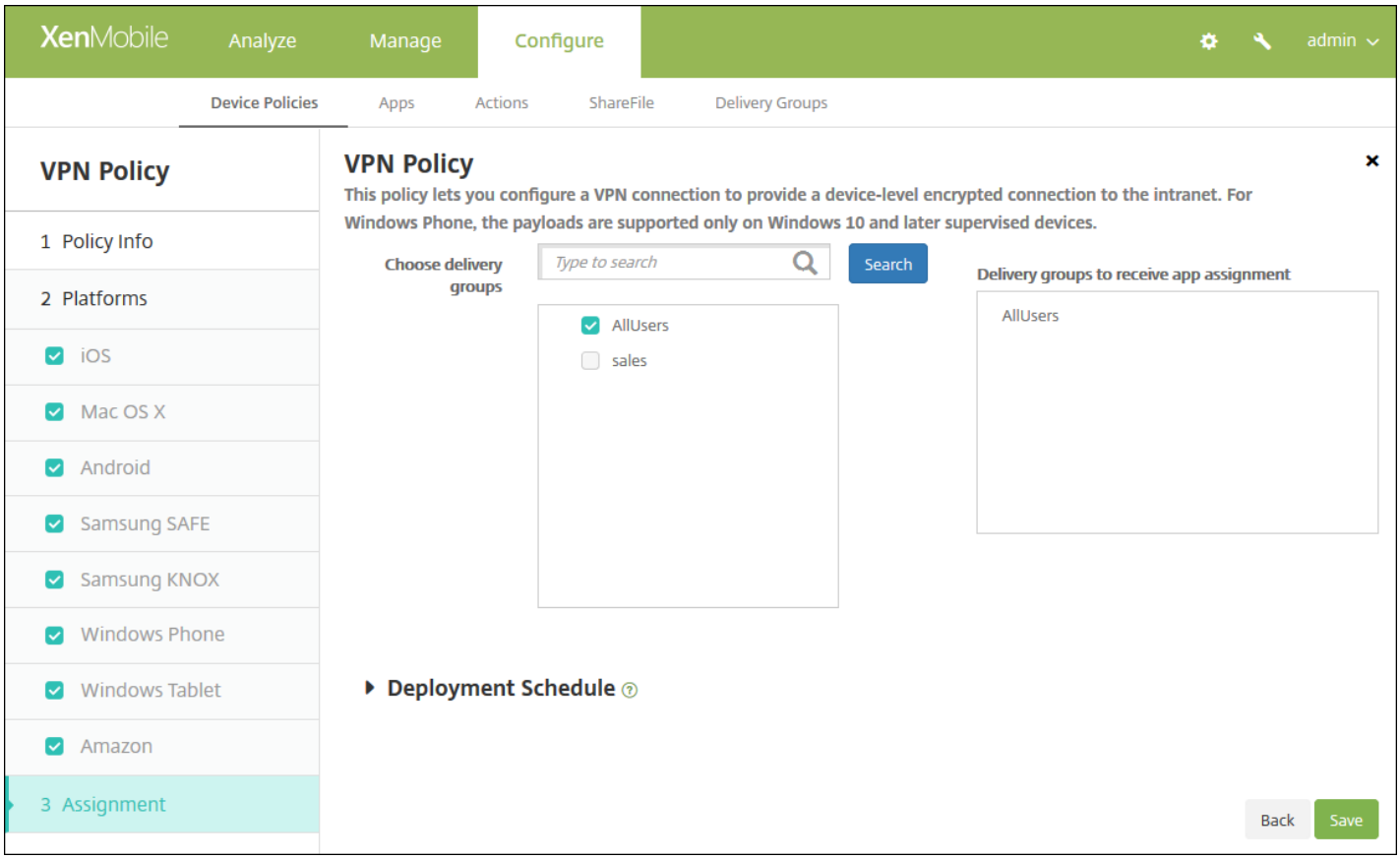
配置 IPSEC AUTH RSA 设置

配置 IPSEC HYBRID RSA 设置

配置 PPTP 设置

7. 配置部署规则

8. 单击**下一步**，将显示 **VPN 策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

墙纸设备策略

Aug 11, 2016

您可以添加 .png 或 .jpg 文件，以设置 iOS 设备锁定屏幕、主屏幕或二者的墙纸。 适用于 iOS 7.1.2 及更高版本。 要在 iPad 和 iPhone 上使用不同的墙纸，需要创建不同的墙纸策略并将其部署到相应的用户。

下表列出了 Apple 建议的用于 iOS 设备的图像尺寸。

设备		**图像尺寸（像素）**
iPhone	**iPad**	
4、4s		640 x 960
5、5c、5s		640 x 1136
6、6s		750 x 1334
6 Plus		1080 x 1920
	Air、2	1536 x 2048
	4、3	1536 x 2048
	Mini 2、3	1536 x 2048
	Mini	768 x 1024

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。

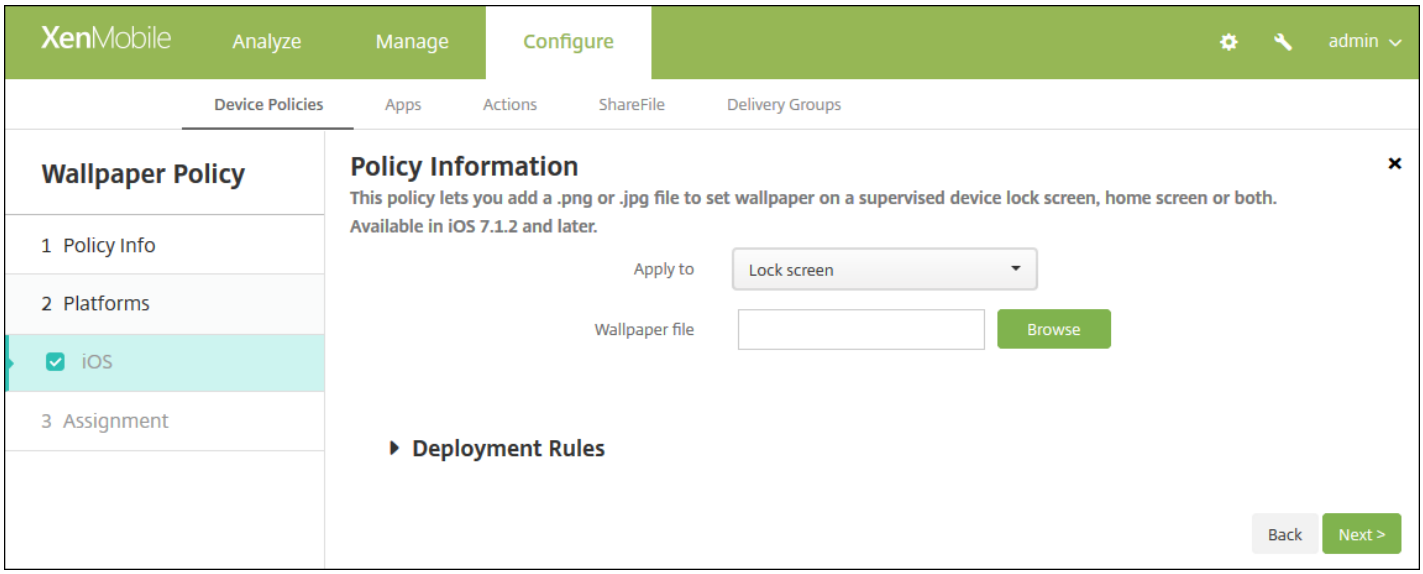
3. 展开**更多**，然后在**最终用户**下面，单击**墙纸**。 此时将显示**墙纸策略**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。



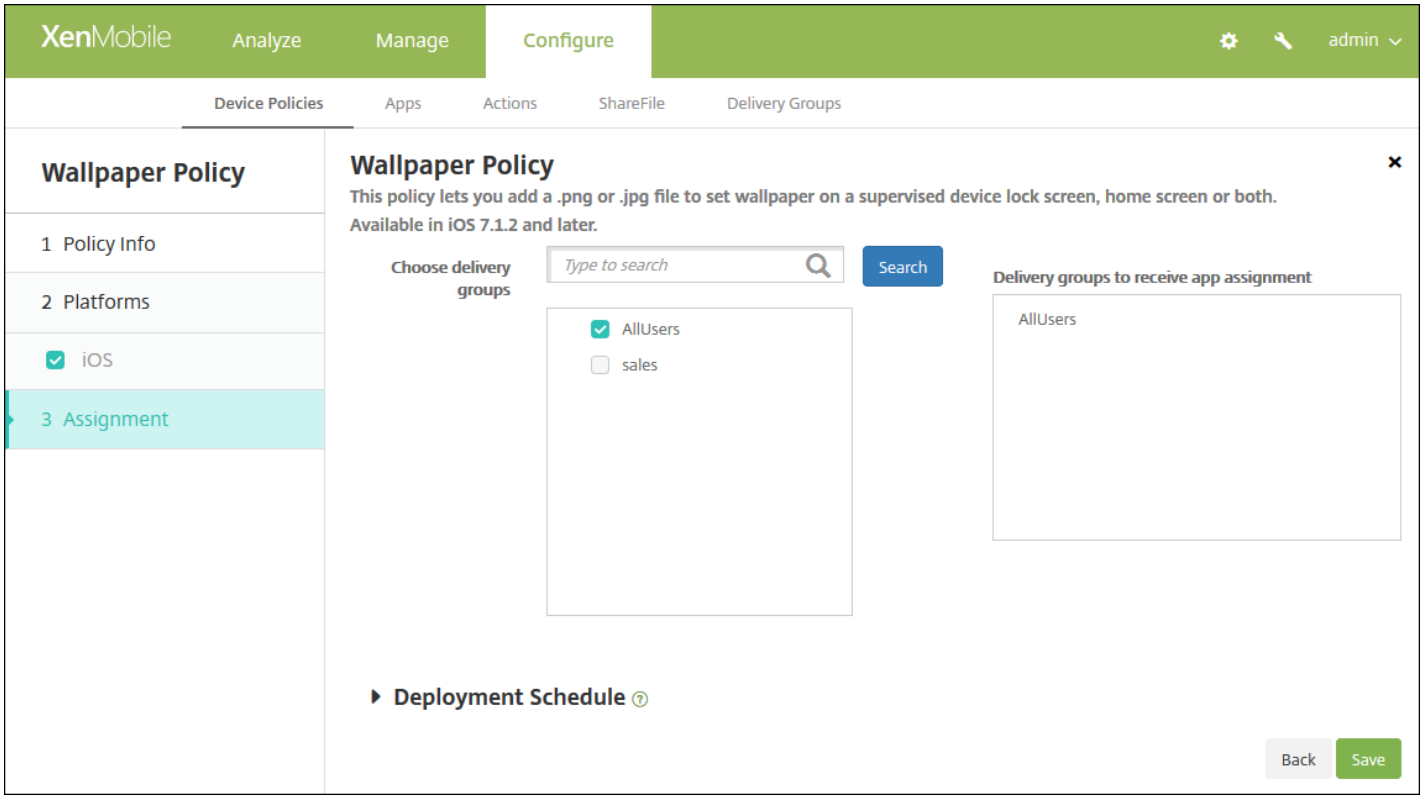
配置以下设置：

- **适用于**：在列表中，选择**锁定屏幕**、**主(图标列表)屏幕**或**锁定屏幕和主屏幕**以设置墙纸出现的位置。
- **墙纸文件**：单击**浏览**，导航到墙纸文件的位置，选择墙纸文件。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**墙纸策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Web 内容设备策略

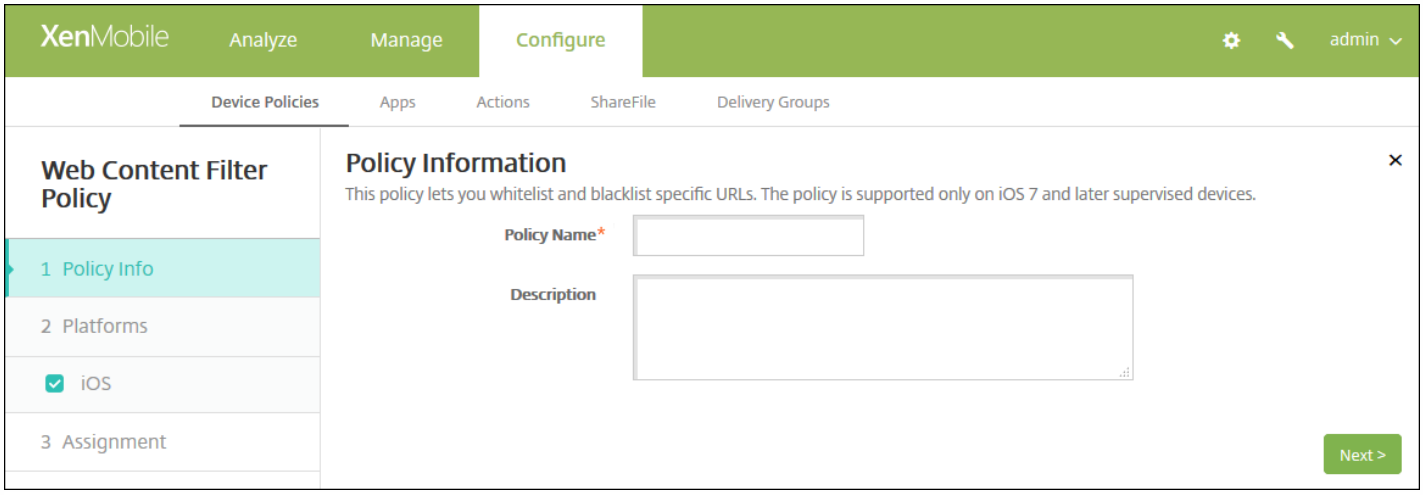
Aug 11, 2016

可以在 XenMobile 中添加一个设备策略，通过结合使用 Apple 的自动过滤功能和添加到白名单和黑名单中的特定站点，在 iOS 设备上过滤 Web 内容。 此策略仅适用于采用受监督模式的 iOS 7.0 及更高版本。 有关将 iOS 设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

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. 单击**更多**，然后在**安全性**下面，单击 **Web 内容过滤器**。 此时将显示 **Web 内容过滤策略**页面。

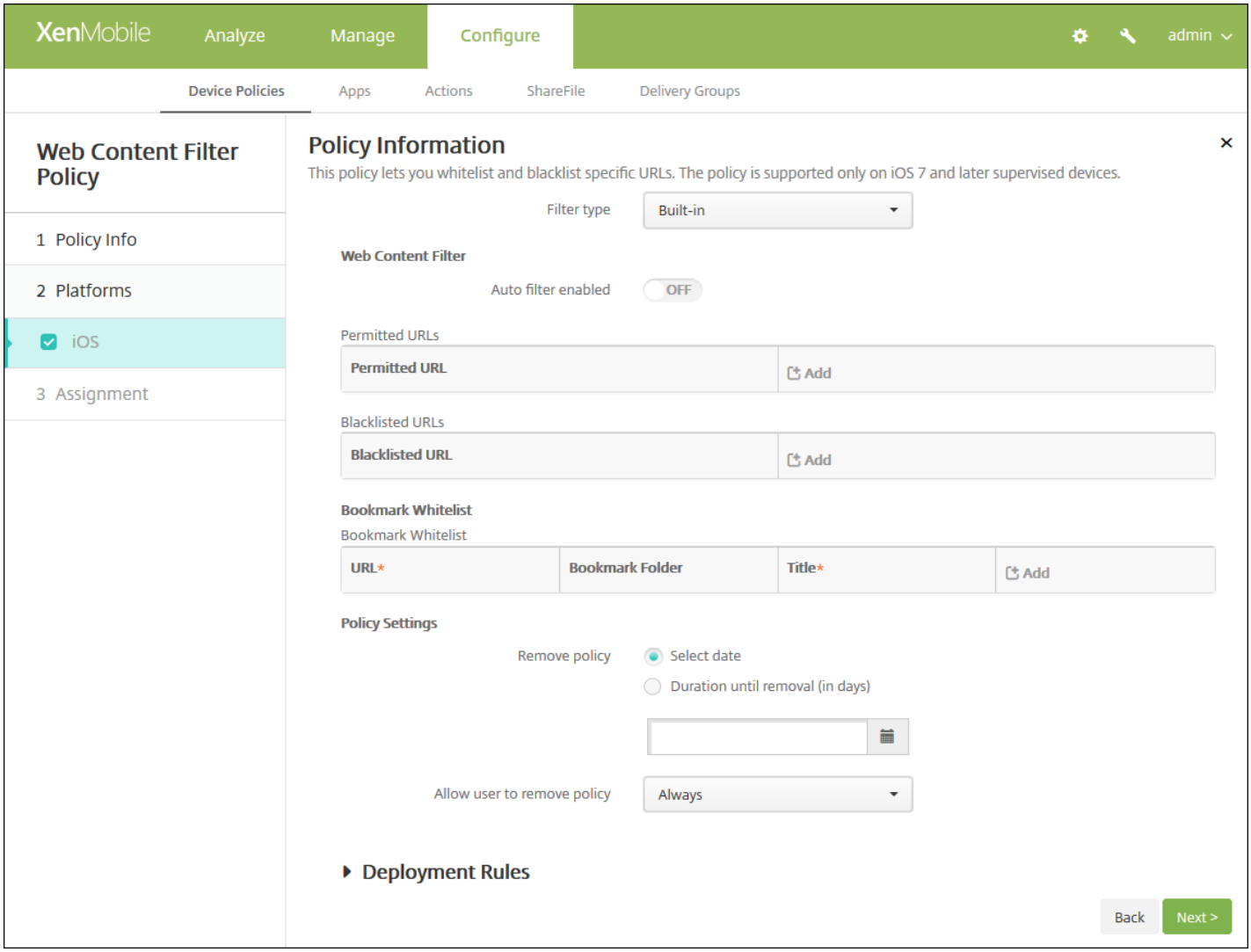


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示 **iOS 平台**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 配置以下设置：

- **过滤器类型**：在列表中，单击**内置**或**插件**，然后按照所选选项后面的步骤操作。 默认值为**内置**。

内置过滤器类型设置

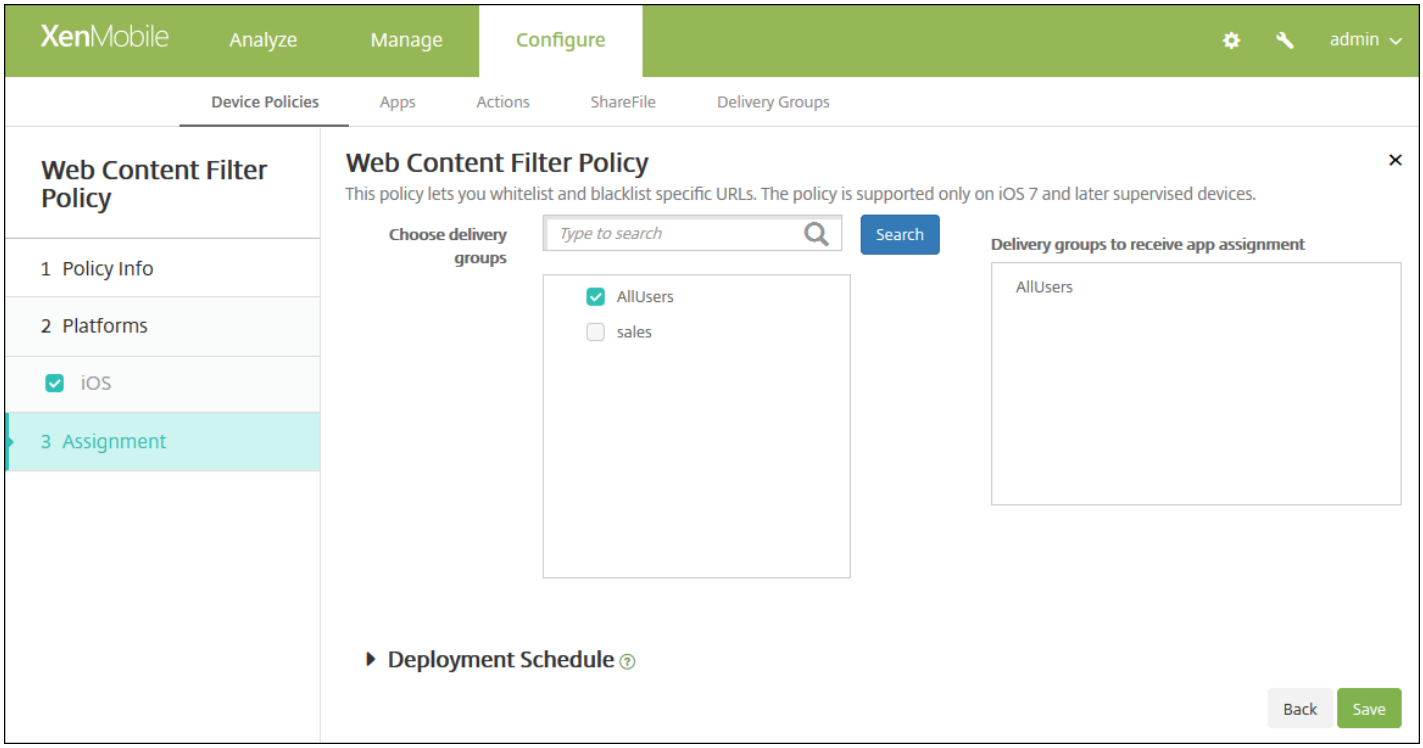
插件过滤器类型设置

- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Web 内容过滤策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- **在为始终启用的连接部署旁边，单击开或关。 默认选项为关。**

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Web 剪辑设备策略

Aug 11, 2016

可以添加网站的快捷方式或 Web 剪辑，使其随应用程序显示在用户的设备上。 可以为 iOS、Mac OS X 和 Android 设备指定您自己的图标来表示 Web 剪辑 ；Windows Tablet 仅需要一个表格和 URL。

iOS 设置

Mac OS X 设置

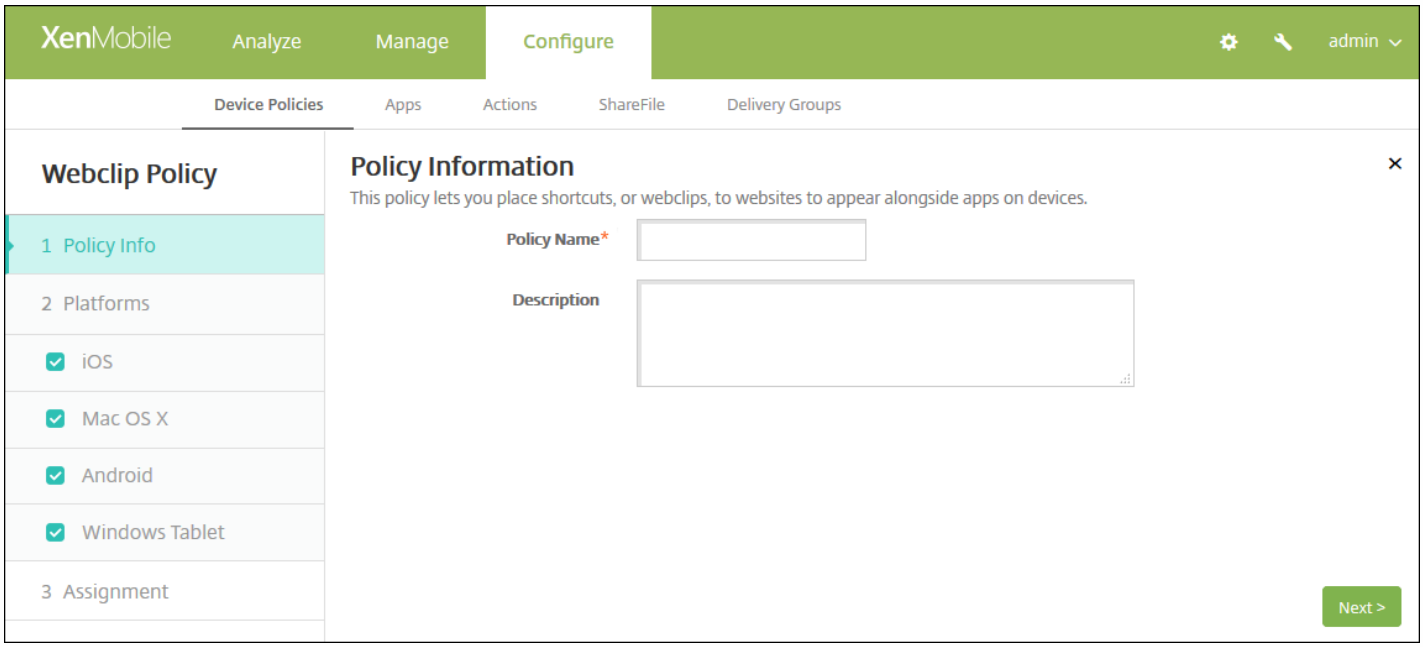
Android 设置

Windows Tablet 设置

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**应用程序**下面，单击 **Web 剪辑**。 此时将显示 **Web 剪辑 策略**页面。

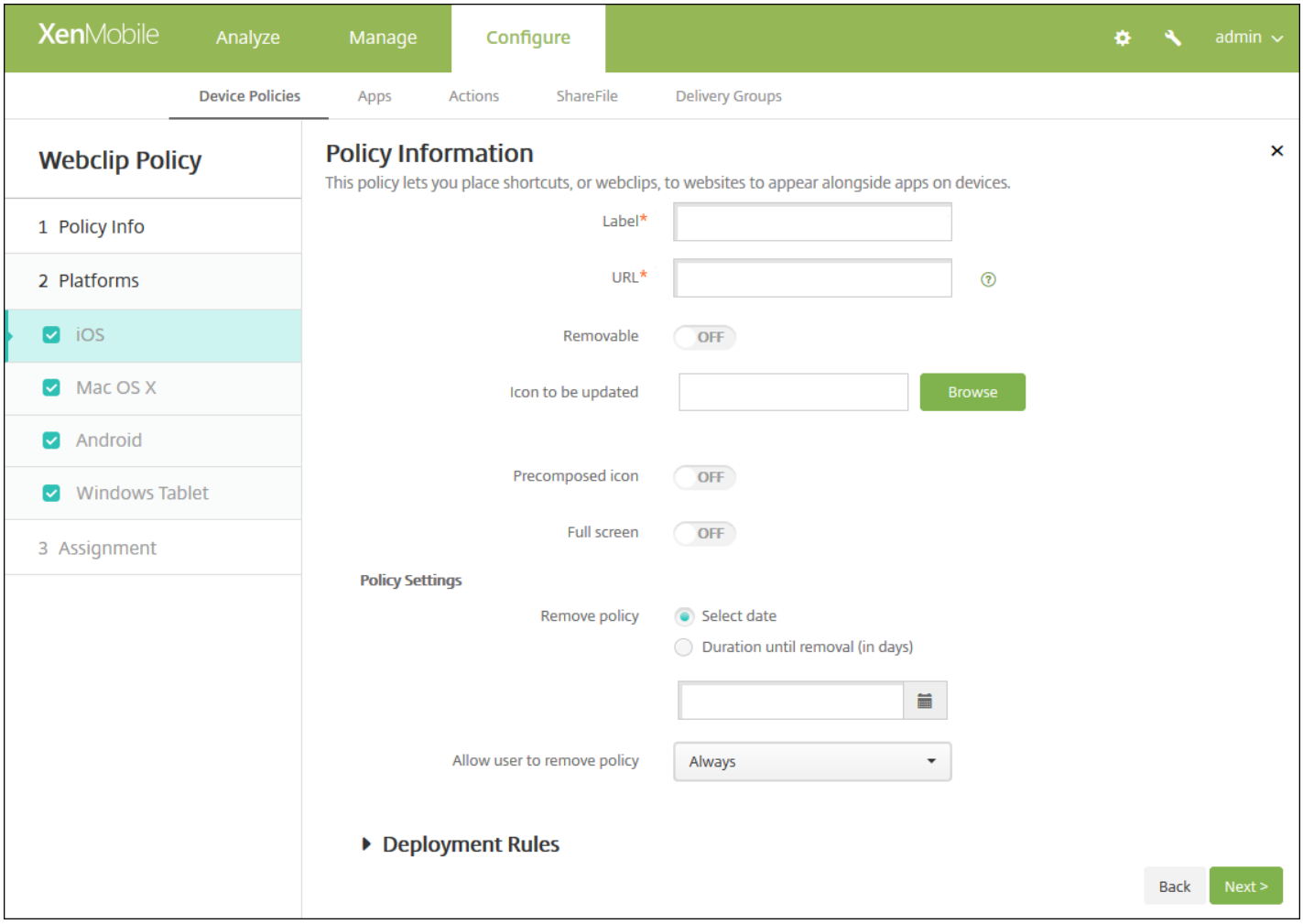


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

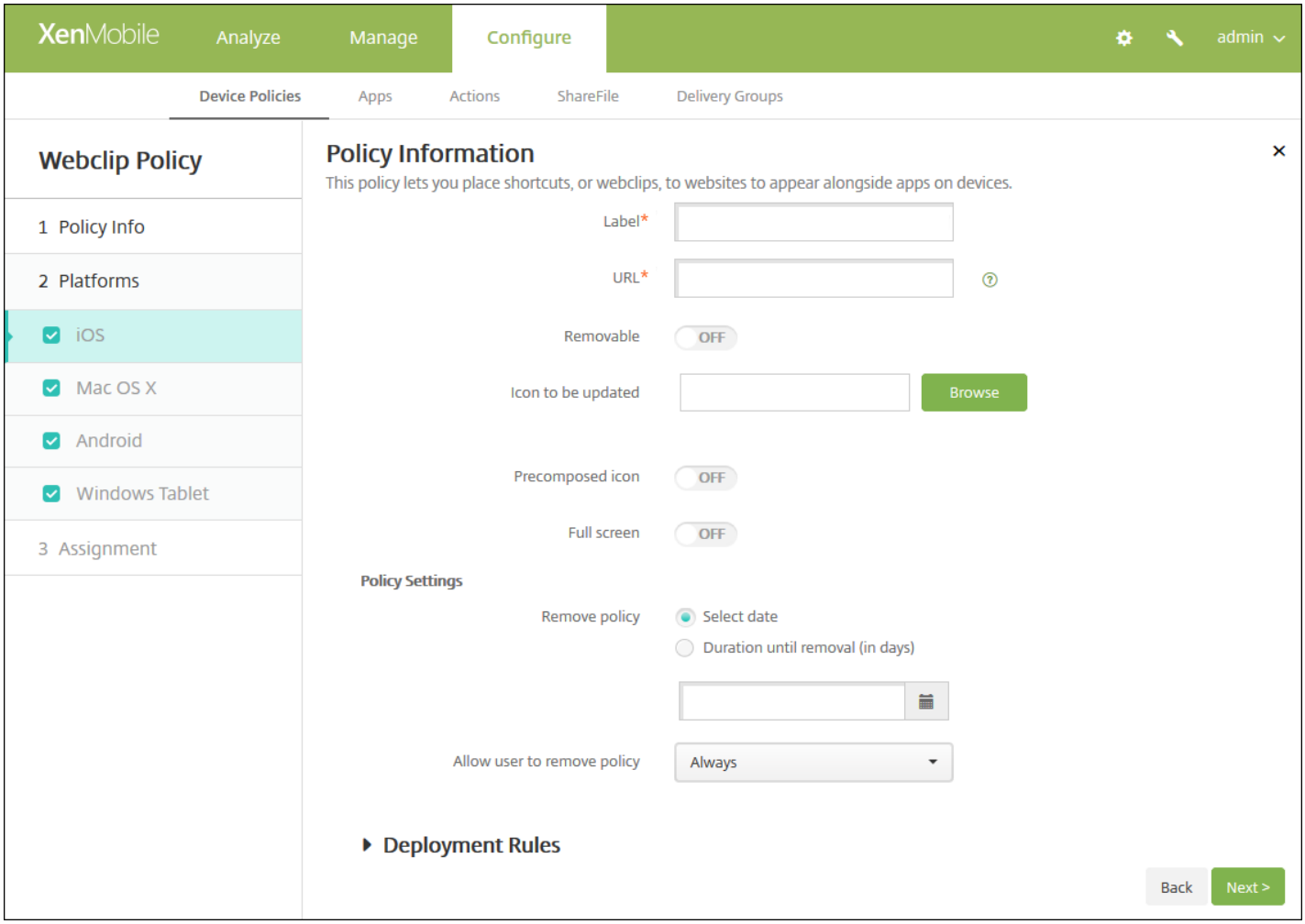
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

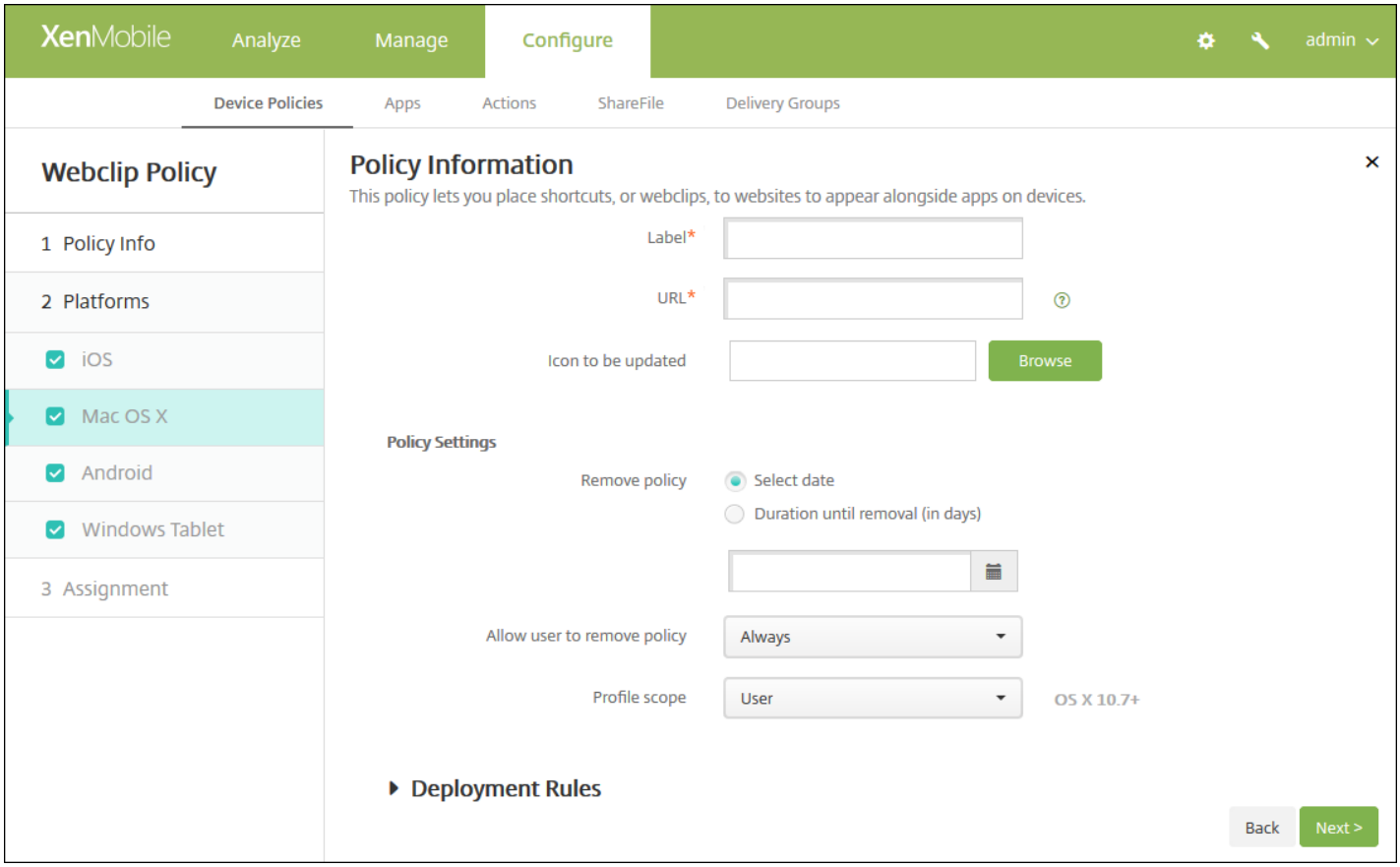
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **标签**：键入随 Web 剪辑显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。 URL 的开头必须为协议，例如 http://server。
- **可删除**：选择用户是否可以删除 Web 剪辑。 默认值为**关**。
- **待更新的图标**：选择要用于 Web 剪辑 的图标，可单击**浏览**并导航到此文件的位置。
- **复合图标**：选择此图标是否应用了某些效果（圆角、阴影和光照反射）。 默认设置为**关**，表示添加效果。
- **全屏**：选择链接的 Web 页面是否以全屏形式打开。 默认值为**关**。
- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。

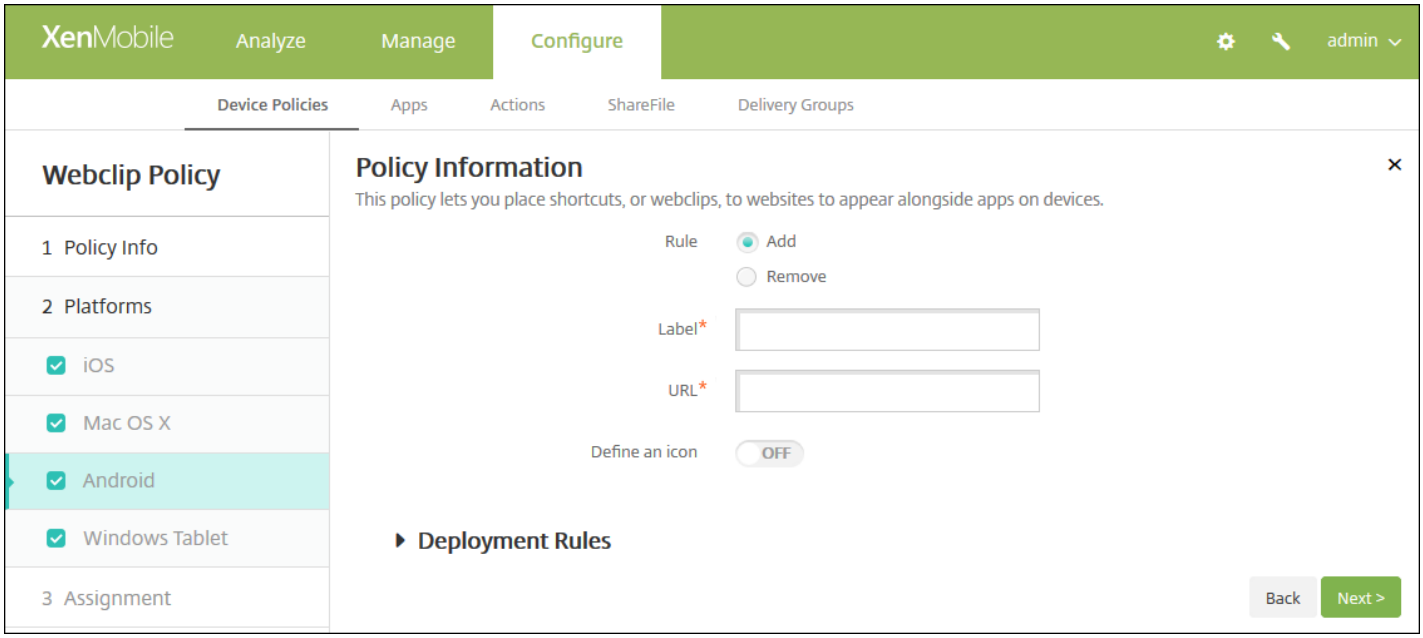
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

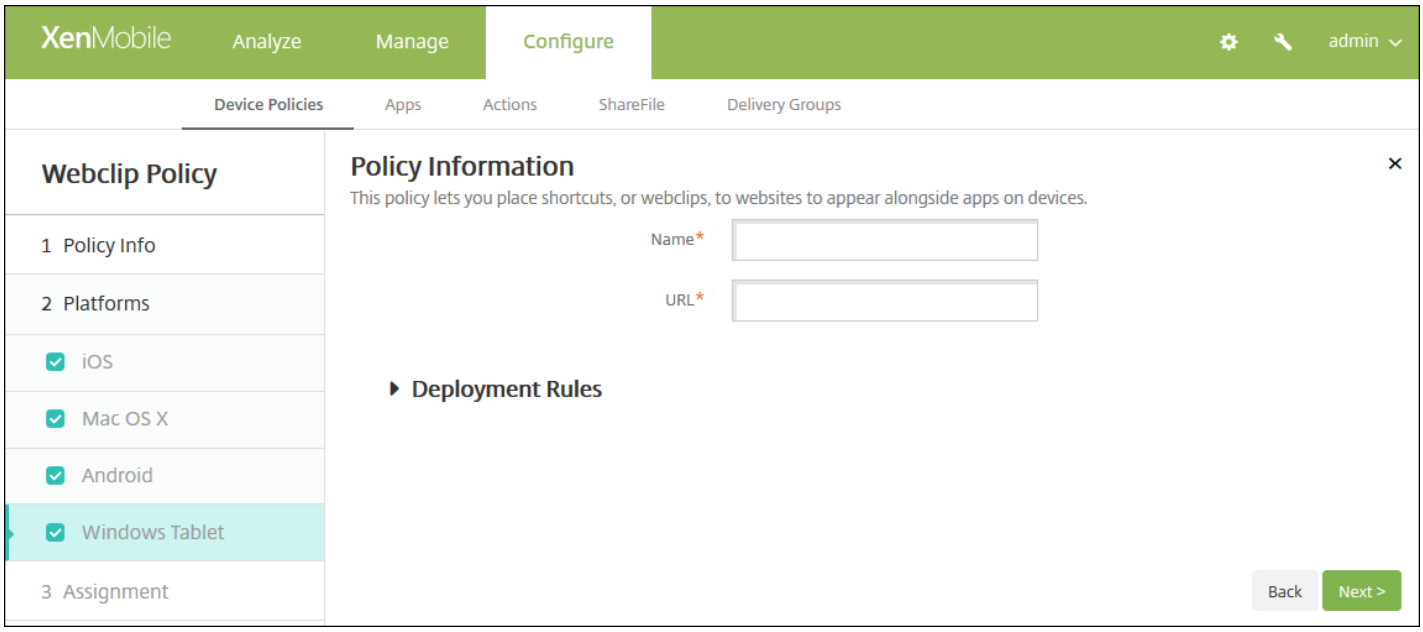
- **标签**：键入随 Web 剪辑显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。 URL 的开头必须为协议，例如 http://server。
- **待更新的图标**：选择要用于 Web 剪辑 的图标，可单击“浏览”并导航到此文件的位置。
- **策略设置**
  - 在**删除策略**旁边，单击**选择 日期** 或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**列表中，单击**用户**或**系统**。 此选项适用于 OS X 10.7 及更高版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **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**：键入随 Web 剪辑显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。
- **定义图标**：选择是否使用图标文件。 默认值为**关**。
- **图标文件**：如果**定义图标**设置为**开**，请单击**浏览**并导航到要使用的图标文件的位置，选择此文件。



配置以下设置：

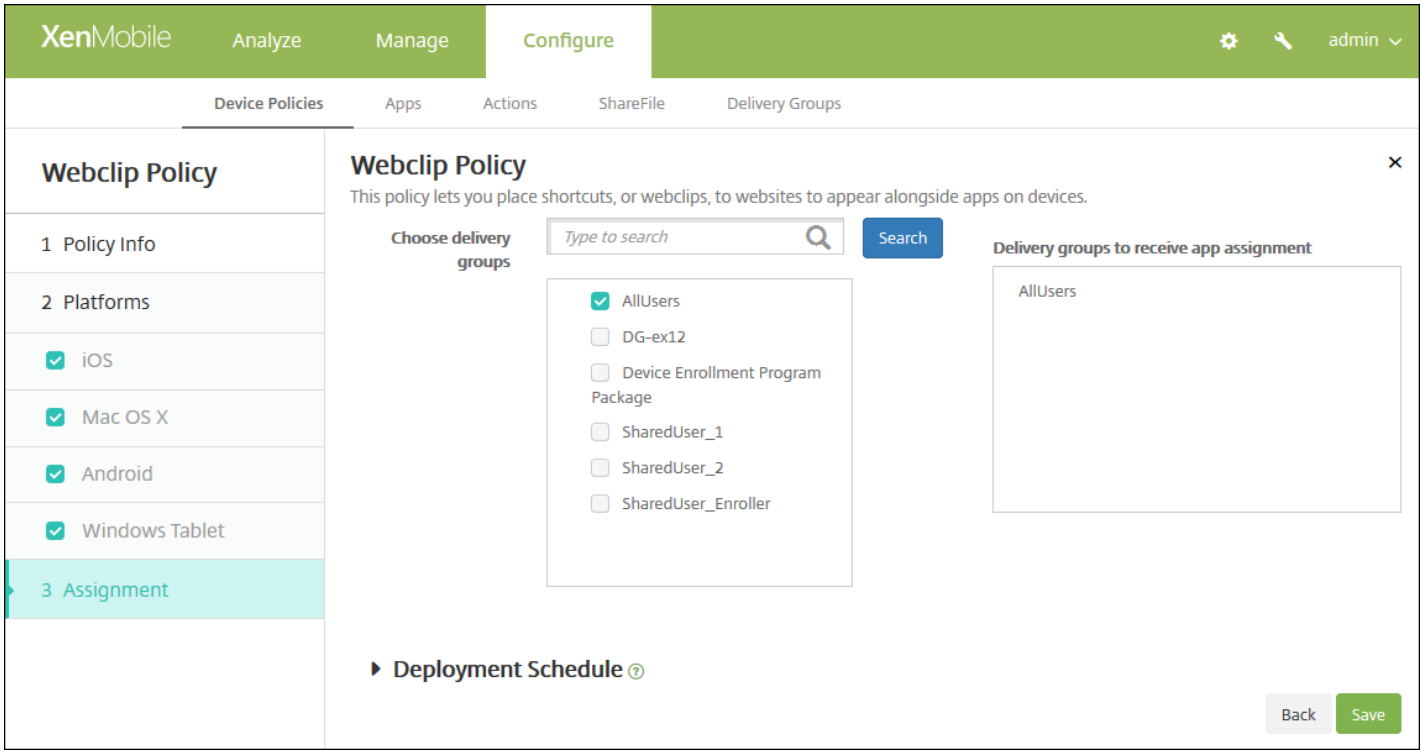
- **名称**：键入随 Web 剪辑显示的标签。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **URL**：键入与 Web 剪辑关联的 URL。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Web 剪辑策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用

11. 单击**保存**以保存此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

WiFi 设备策略

Aug 11, 2016

利用 XenMobile 控制台的"设备策略"页面，在 XenMobile 中创建或编辑现有 WiFi 设备策略。 利用 WiFi 策略，可以通过定义网络名称和类型、身份验证和安全策略、是否使用代理服务器和其他 WiFi 相关信息，使这些设置对所选设备平台上的所有用户保持一致，以管理用户将其设备连接到 WiFi 网络的方式。

可以为以下平台的用户配置 WiFi 设置：iOS、Mac OS X、Android（包括为 Android for Work 启用的设备）、Windows Phone 和 Windows Tablet。 每种平台需要一组不同的值，本文将对此进行详细介绍。

iOS 设置

Mac OS X 设置

Android 设置

Windows Phone 设置

Windows Tablet 设置

Important

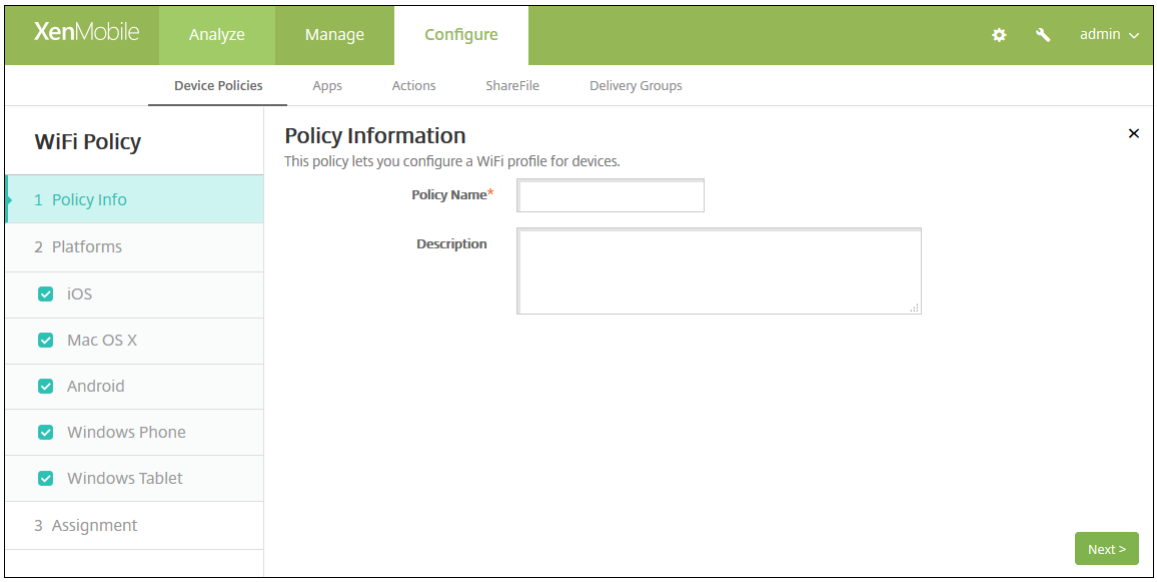
在创建新策略之前，请确保完成以下步骤：

- 创建计划使用的部署组。
- 了解网络名称和类型。
- 了解计划使用的身份验证或安全类型。
- 了解可能需要的代理服务器信息。
- 安装所有必需的 CA 证书。
- 具有所有必需共享密钥。

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. 单击 **WiFi**。 此时将显示 **WiFi 策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

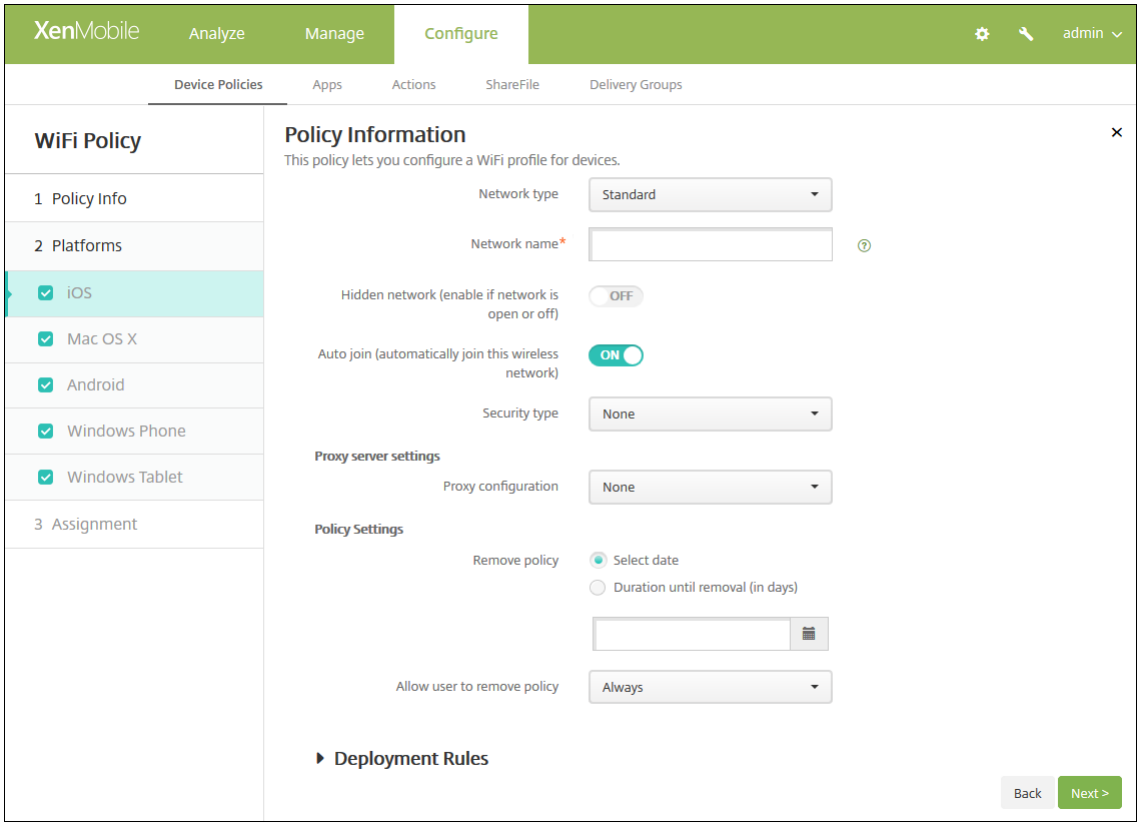
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示**平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **网络类型**：在列表中，单击**标准**、**传统热点**或 **Hotspot 2.0** 以设置您计划使用的网络类型。
- **网络名称**：键入显示在设备的可用网络列表中的 SSID。 不适用于 **Hotspot 2.0**。
- **隐藏网络(网络打开或关闭时启用)**：选择是否隐藏网络。
- **自动连接(自动连接此无线网络)**：选择是否自动连接网络。 默认值为**开**。
- **安全类型**：在列表中，单击您计划使用的安全类型。 不适用于 **Hotspot 2.0**。
  - 无 – 无需进一步配置。
  - WEP
  - WPA/WPA2 Personal
  - 任何(Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - 任何(Enterprise)

  以下部分列出了要为上述各个连接类型配置的选项。

WPA、WPA Personal、任何(Personal)

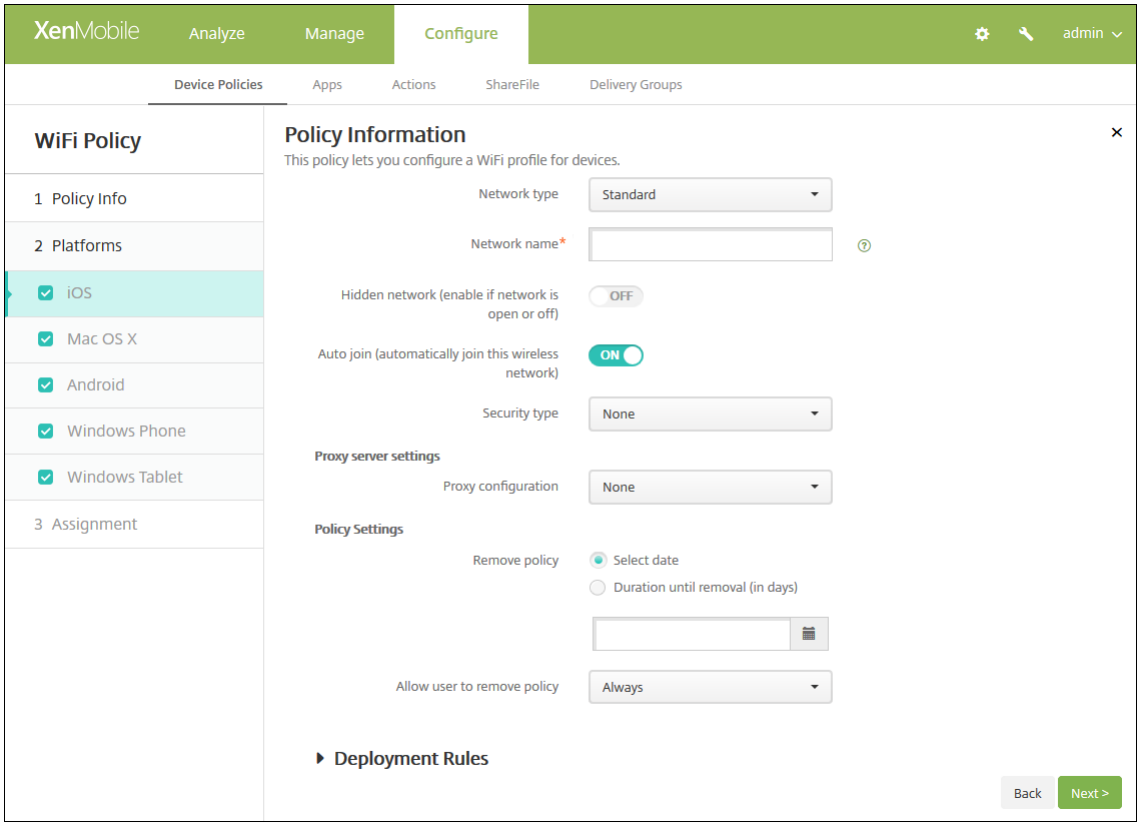
WEP Enterprise、WPA Enterprise、WPA2 Enterprise、任何(Enterprise)

- **代理服务器设置**
  - **代理配置**：在列表中，单击“无”、“手动”或“自动”以设置 VPN 连接通过代理服务器路由的方式，然后配置其他选项。 默认值为“无”，选择此项无需进一步配置。
  - 如果选择**手动**，可以配置以下设置：
    - **主机名/IP 地址**：键入代理服务器的主机名或 IP 地址。
    - **端口**：键入代理服务器端口号。
    - **用户名**：键入向代理服务器进行身份验证的可选用户名。
    - **密码**：键入向代理服务器进行身份验证的可选密码。
  - 如果单击**自动**，可以配置以下设置：
    - **服务器 URL**：键入用于定义代理配置的 PAC 文件的 URL。
    - **允许在无法访问 PAC 时直接连接**：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。 默认值为**开**。 此选项仅适用于 iOS 7.0 及更高版本。
- **Hotspot 2.0**
  - **显示的运算符名称**：键入要显示的运算符名称。 适用于 iOS 7.0 及以上版本。
  - **域名**：键入 WiFi Hotspot 2.0 协商使用的域名。 适用于 iOS 7.0 及以上版本。
  - **允许连接漫游伙伴网络**：选择是否允许设备连接到漫游合作伙伴网络。 适用于 iOS 7.0 及以上版本。
  - **漫游联盟组织标识符(OI)**：可选，添加 WiFi Hotspot 2.0 协商使用的漫游联盟组织标识符。
  - **网络访问标识符(NAI)领域名称**：可选，添加 WiFi Hotspot 2.0 协商使用的 NAI 领域名称。
  - **移动设备国家/地区代码(MCC)和移动设备网络配置(MNC)**：可选，添加 WiFi Hotspot 2.0 协商使用的 MCC 和 MNC。 每个字符串必须精确包含六位数。

  有关**协议，接受 EAP 类型**、**协议，EAP-FAST** 和 **身份验证**的信息，请参阅上述部分。
- **策略设置**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
- 如果单击**选择日期**，请单击日历以选择具体删除日期。
- 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
- 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。



配置以下设置：

- **网络类型**：在列表中，单击**标准**、**传统热点**或 **Hotspot 2.0** 以设置您计划使用的网络类型。
- **网络名称**：键入显示在设备的可用网络列表中的 SSID。 不适用于 **Hotspot 2.0**。
- **隐藏网络(网络打开或关闭时启用)**：选择是否隐藏网络。
- **自动连接(自动连接此无线网络)**：选择是否自动连接网络。 默认值为**开**。
- **安全类型**：在列表中，单击您计划使用的安全类型。 不适用于 **Hotspot 2.0**。
  - 无 – 无需进一步配置。
  - WEP
  - WPA/WPA2 Personal
  - 任何(Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - 任何(Enterprise)

  以下部分列出了要为上述各个连接类型配置的选项。

WPA、WPA Personal、WPA 2 Personal、任何(Personal)

WEP Enterprise、WPA Enterprise、WPA2 Enterprise、任何(Enterprise)

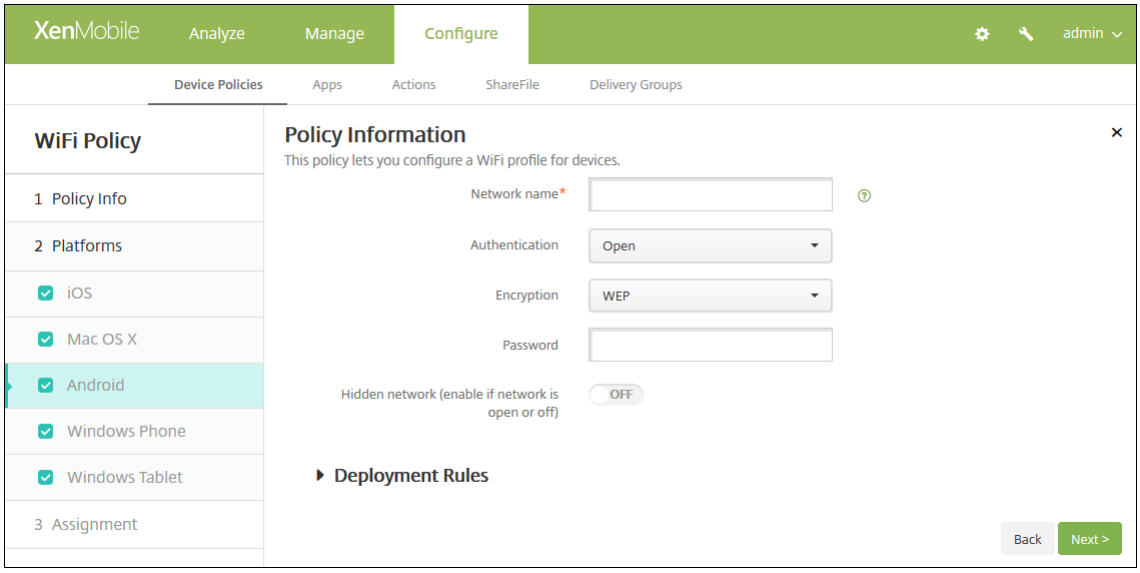
- **用作登录窗口配置**：选择是否使用在登录窗口中输入的同一凭据对用户进行身份验证。
- **代理服务器设置**
  - **代理配置**：在列表中，单击“无”、“手动”或“自动”以设置 VPN 连接通过代理服务器路由的方式，然后配置其他选项。 默认值为“无”，选择此项无需进一步配置。
  - 如果选择**手动**，可以配置以下设置：
    - **主机名/IP 地址**：键入代理服务器的主机名或 IP 地址。
    - **端口**：键入代理服务器端口号。
    - **用户名**：键入向代理服务器进行身份验证的可选用户名。
    - **密码**：键入向代理服务器进行身份验证的可选密码。
  - 如果单击**自动**，可以配置以下设置：
    - **服务器 URL**：键入用于定义代理配置的 PAC 文件的 URL。
    - **允许在无法访问 PAC 时直接连接**：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。 默认值为**开**。 此选项仅适用于 iOS 7.0 及更高版本。
- **Hotspot 2.0**
  - **显示的运算符名称**：键入要显示的运算符名称。 适用于 iOS 7.0 及以上版本。
  - **域名**：键入 WiFi Hotspot 2.0 协商使用的域名。 适用于 iOS 7.0 及以上版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **允许连接漫游伙伴网络**：选择是否允许设备连接到漫游合作伙伴网络。 适用于 iOS 7.0 及以上版本。
- **漫游联盟组织标识符(OI)**：可选，添加 WiFi Hotspot 2.0 协商使用的漫游联盟组织标识符。
- **网络访问标识符(NAI)领域名称**：可选，添加 WiFi Hotspot 2.0 协商使用的 NAI 领域名称。
- **移动设备国家/地区代码(MCC)和移动设备网络配置(MNC)**：可选，添加 WiFi Hotspot 2.0 协商使用的 MCC 和 MNC。 每个字符串必须精确包含六位数。

  有关**协议，接受 EAP 类型**、**协议，EAP-FAST** 和 **身份验证**的信息，请参阅上述部分。

- **策略设置**
  - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。
  - 在**配置文件作用域**旁边，单击**用户**或**系统**。 默认值为**用户**。 此选项仅适用于 OS X 10.7 及更高版本。



配置以下设置：

- **网络名称**：键入显示在用户设备上的可用网络列表中的 SSID。
- **身份验证**：在列表中，单击用于 WiFi 连接的安全类型。
  - 开放
  - 共享虚拟机
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

  以下部分列出了要为上述各个连接类型配置的选项。

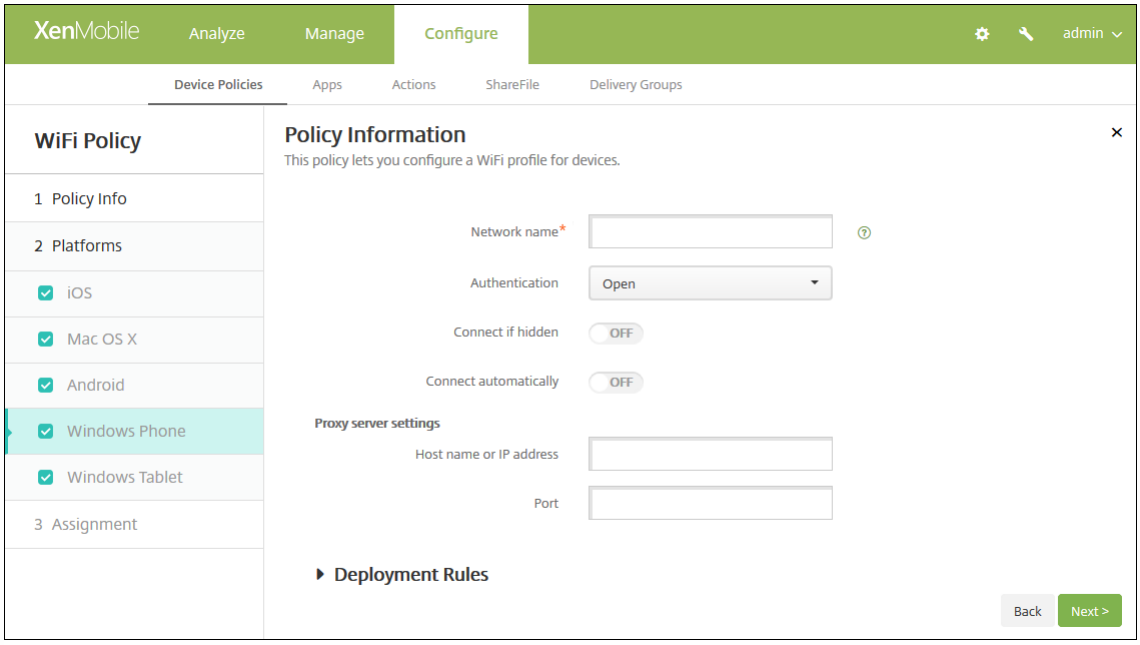
打开，共享

WPA、WPA-PSK、WPA2、WPA2-PSK

802.1x

- **隐藏网络(网络打开或关闭时启用)**：选择是否隐藏网络。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **网络名称**：键入显示在用户设备上的可用网络列表中的 SSID。
- **身份验证**：在列表中，单击用于 WiFi 连接的安全类型。
  - 开放
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise

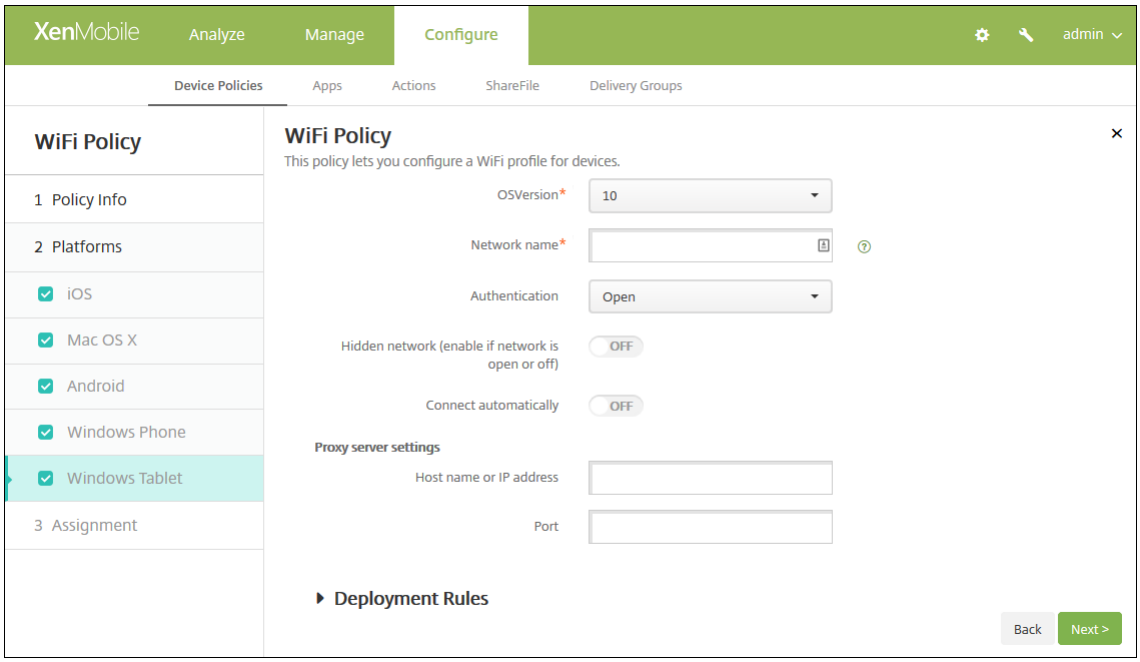
  以下部分列出了要为上述各个连接类型配置的选项。

开放

WPA Personal、WPA-2 Personal

WPA-2 Entrprise

- **代理服务器设置**
  - **主机名或 IP 地址**：键入代理服务器的名称或 IP 地址。
  - **端口**：键入代理服务器的端口号。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置以下设置：

- **操作系统版本**：在列表中，单击 **8.1** 以使用 Windows 8.1 或单击 **10** 以使用 Windows 10。 默认值为 **10**。

Windows 10 设置

- **身份验证**：在列表中，单击用于 WiFi 连接的安全类型。
  - 开放
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise

  以下部分列出了要为上述各个连接类型配置的选项。

开放

WPA Personal、WPA-2 Personal

WPA-2 Enterprise

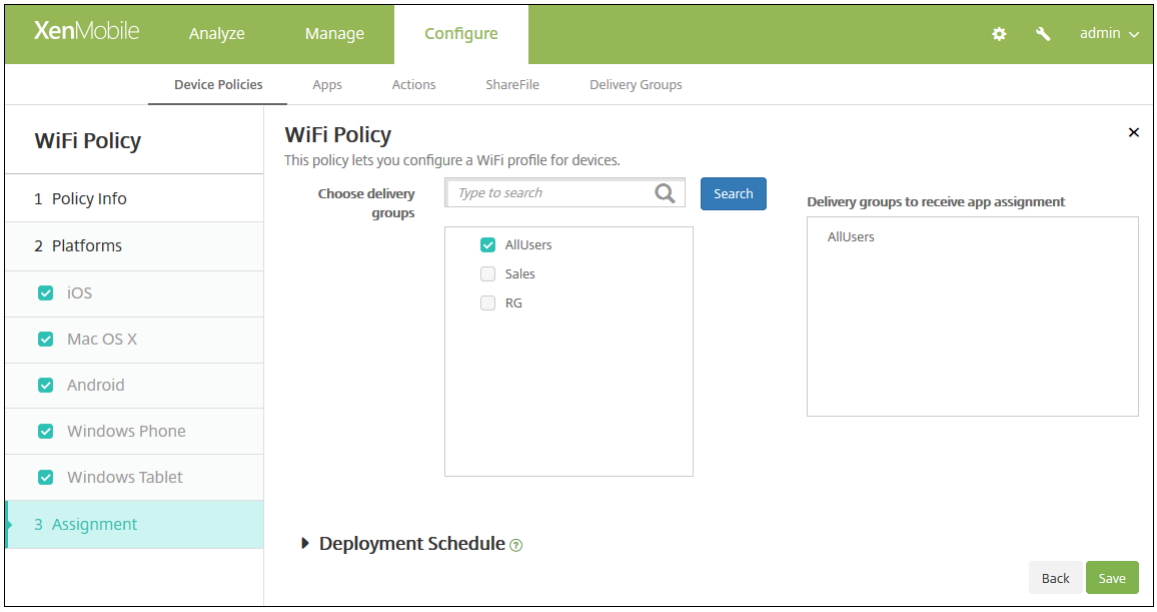
Windows 8.1 设置

- **网络名称**：键入显示在用户设备上的可用网络列表中的 SSID。
- **身份验证**：在列表中，单击用于 WiFi 连接的安全类型。
  - 开放
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise
- **隐藏网络(网络打开或关闭时启用)**：选择是否隐藏网络。
- **自动连接**：选择是否自动连接到网络。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **WiFi 策略分配**页面。

8. 单击**下一步**。 此时将显示 WiFi 策略**分配**页面。
8. 单击**下一步**。 此时将显示 WiFi 策略**分配**页面。
8. 单击**下一步**。 此时将显示 WiFi 策略**分配**页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows CE 证书设备策略

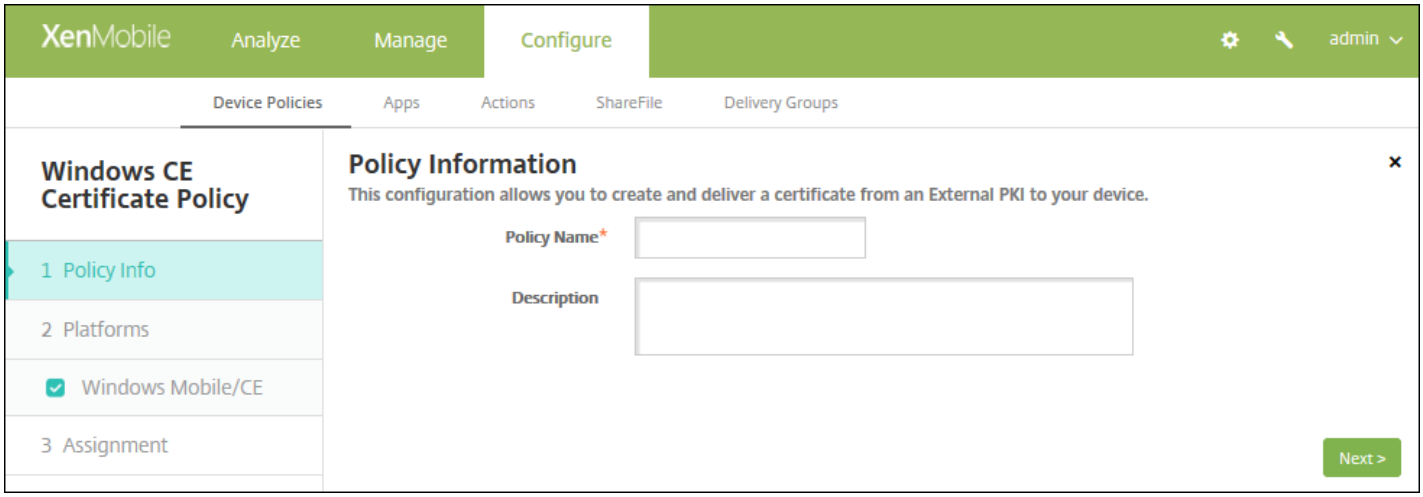
Aug 11, 2016

可以在 XenMobile 中创建一个设备策略，用于创建并向用户设备交付来自外部 PKI 的 Windows Mobile/CE 证书。 有关证书和 PKI 实体的详细信息，请参阅证书。

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**下面，单击 **Windows CE 证书**。 此时将显示 **Windows CE 证书策略**信息页面。

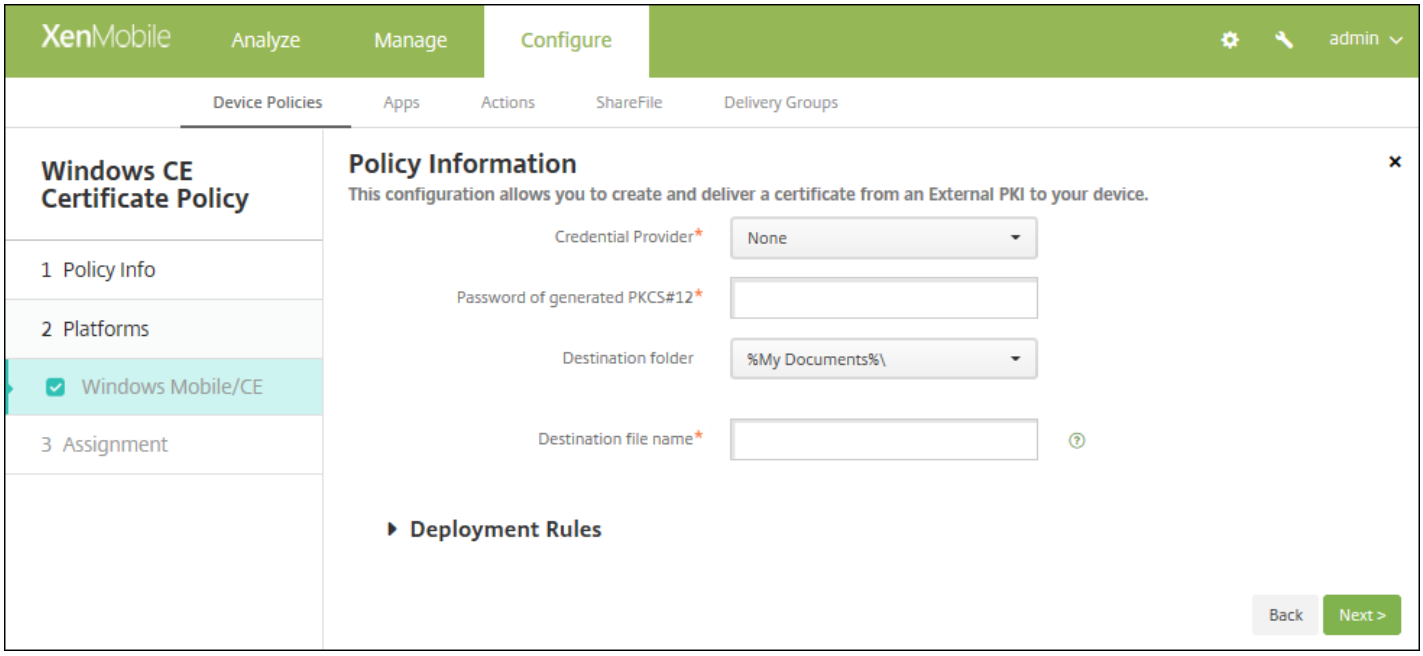


4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **Windows CE 证书策略平台**信息页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



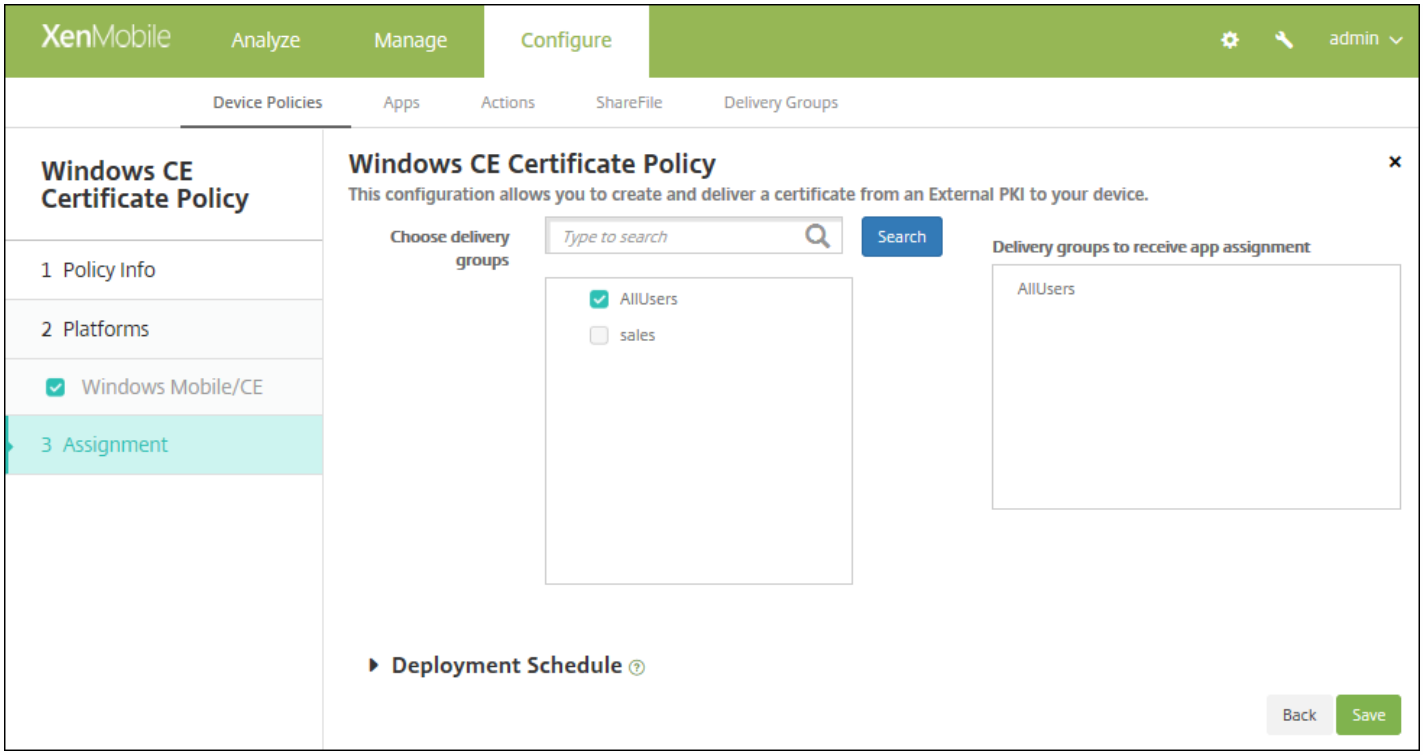
6. 配置以下设置：

- **凭据提供程序**：在列表中，单击凭据提供程序。 默认值为**无**。
- **生成的 PKCS#12 的密码**：键入用于加密凭据的密码。
- **目标文件夹**：在列表中，单击凭据的目标文件夹或单击**新增**以添加列表中尚未存在的文件夹。 预定义选项为：
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **目标文件名**：键入凭据文件的名称。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **Windows CE 证书策略**分配页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为每次连接时。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为关。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Worx Store 设备策略

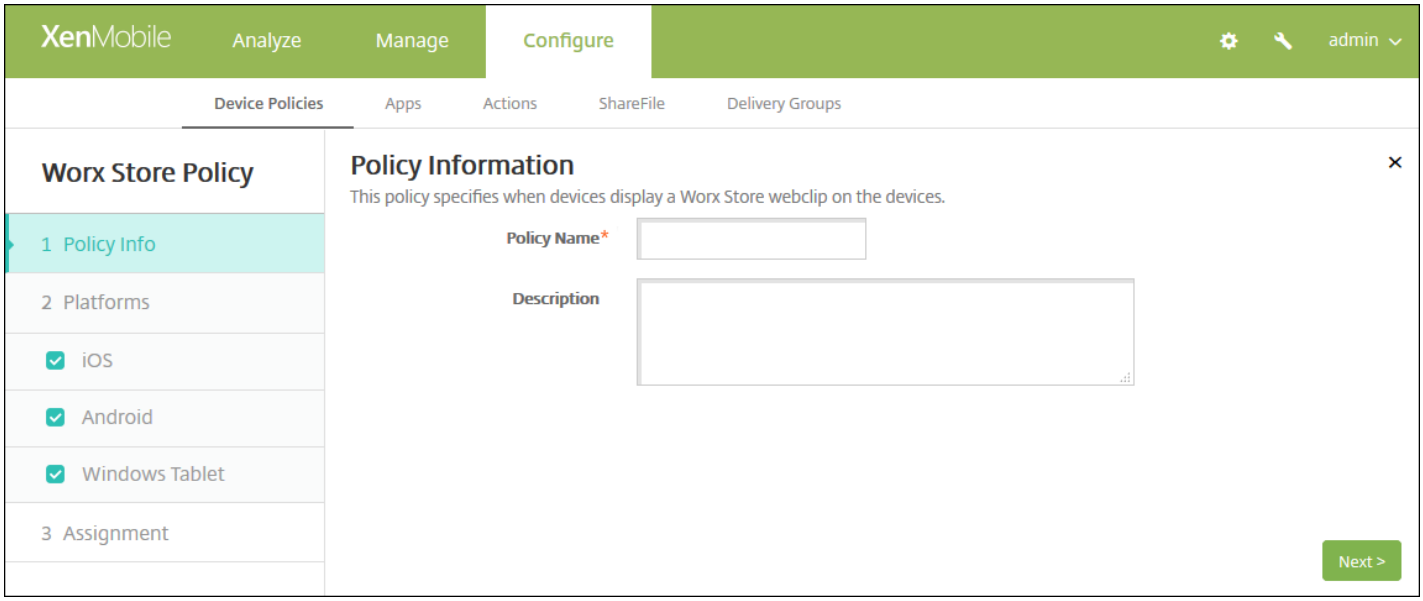
Aug 11, 2016

可以在 XenMobile 中创建一个策略，以指定 iOS、Android 或 Windows Tablet 设备是否在设备的主屏幕上显示 Worx Store Web 剪辑。

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**应用程序**下面，单击 **Worx Store**。 此时将显示 **Worx Store 策略**页面。

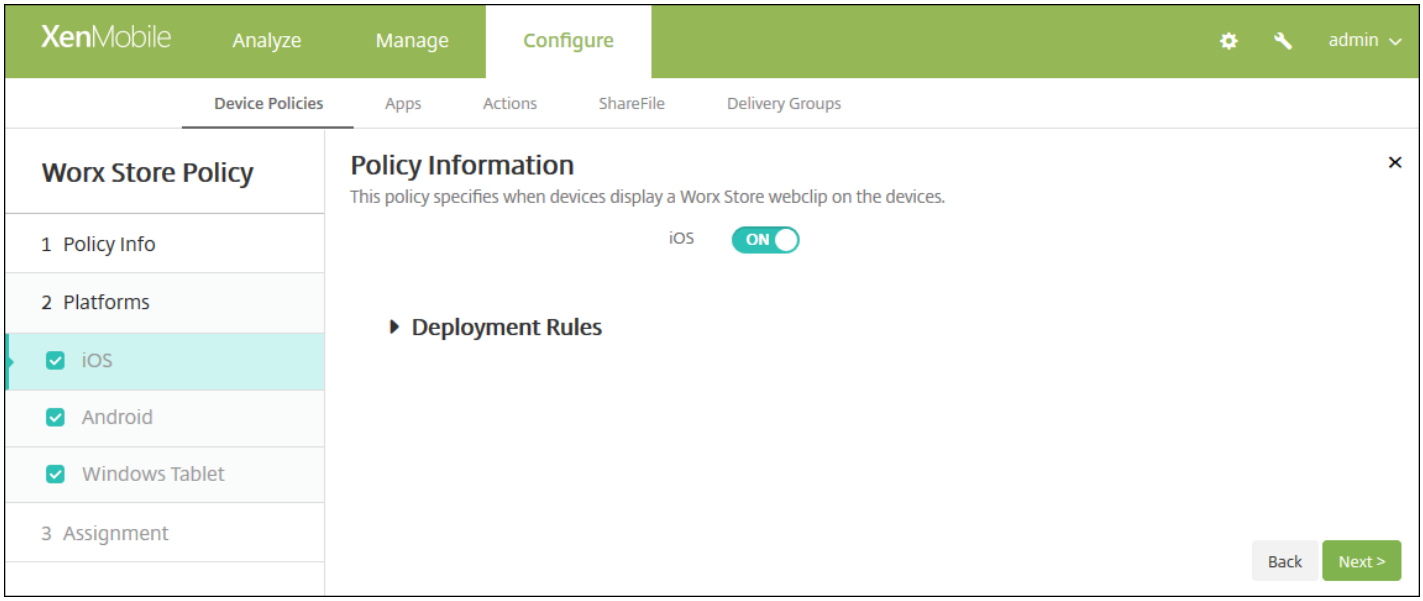


4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：如有需要，请键入策略的说明。

5. 单击**下一步**。 此时将显示**平台**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



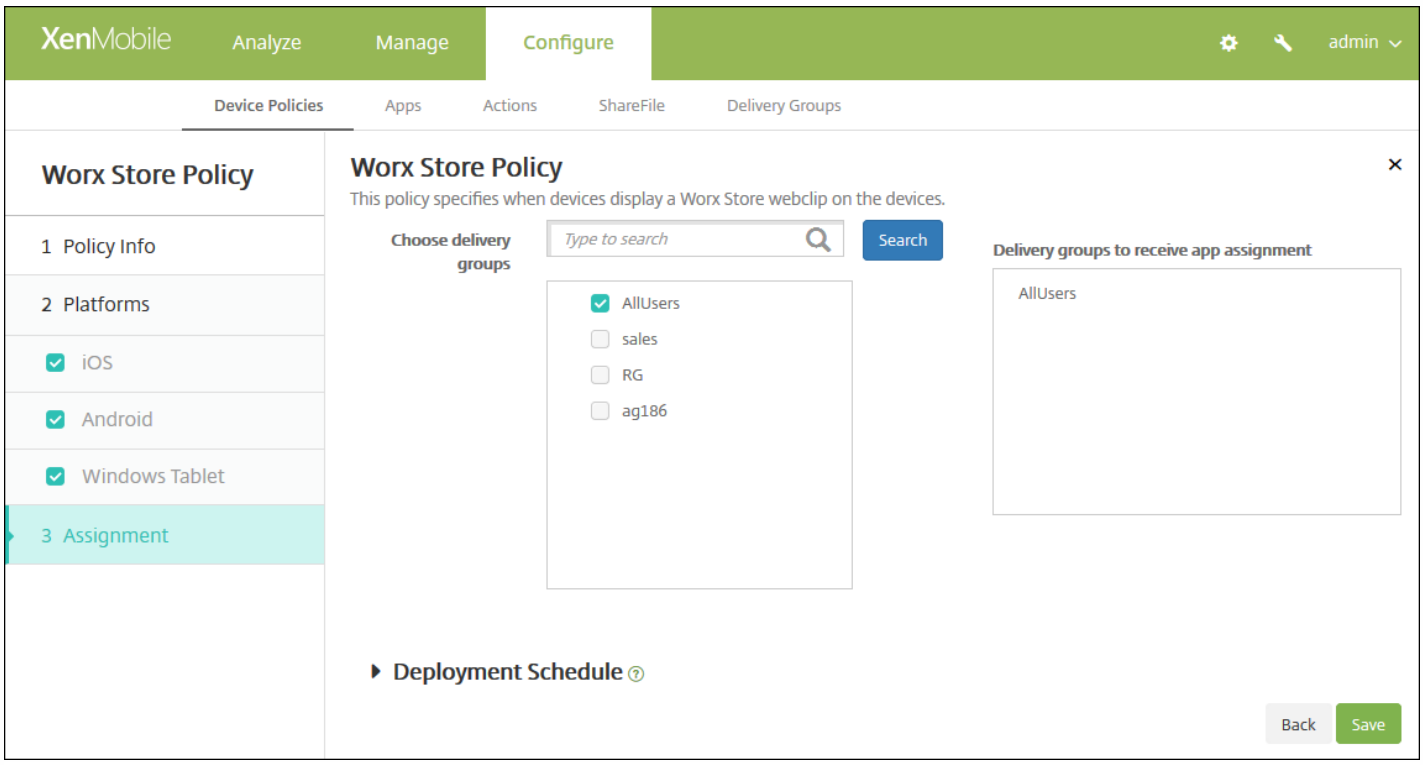
6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

7. 对于所配置的每个平台，请选择是否在用户的设备上显示 Worx Store Web 剪辑。 默认值为**开**。

配置好各个平台后，请参阅步骤 8 以了解如何设置此平台的部署规则。

8. 配置部署规则

9. 单击**下一步**，将显示**Worx Store 策略**分配页面。



10. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧**用于**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

12. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 选项设备策略

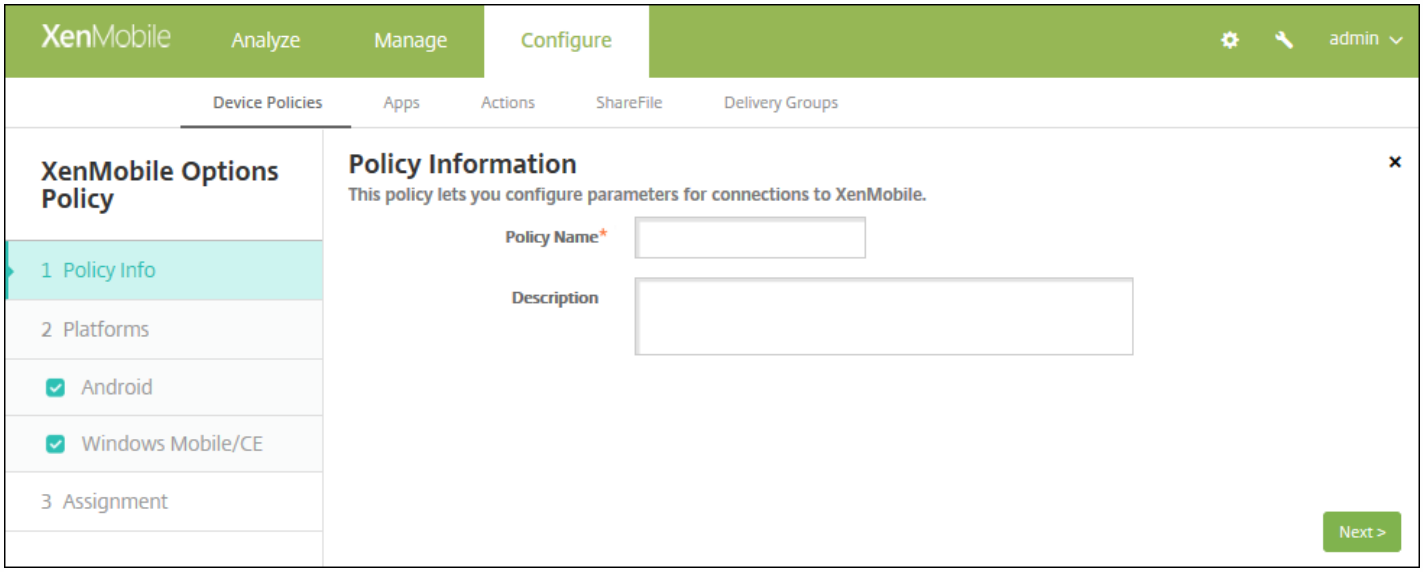
Aug 11, 2016

添加 XenMobile 选项策略，用于配置在从 Android 和 Windows Mobile/CE 设备连接到 XenMobile 时 Worx Home 的行为。

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 **XenMobile Agent** 下面，单击 **XenMobile 选项**。 此时将显示 **XenMobile Options Policy**（XenMobile 选项策略）页面。



4. 在**策略信息**窗格中，输入以下信息：

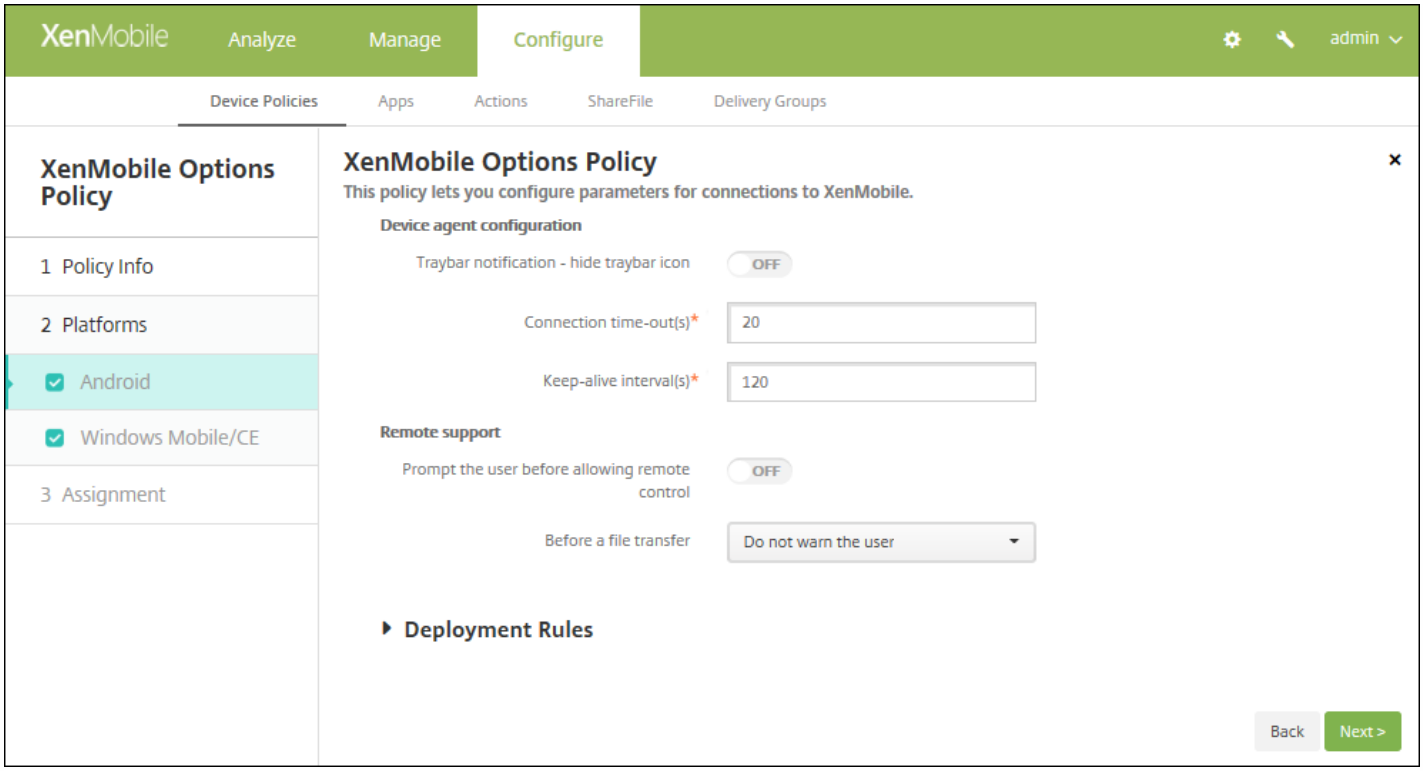
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示**策略平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

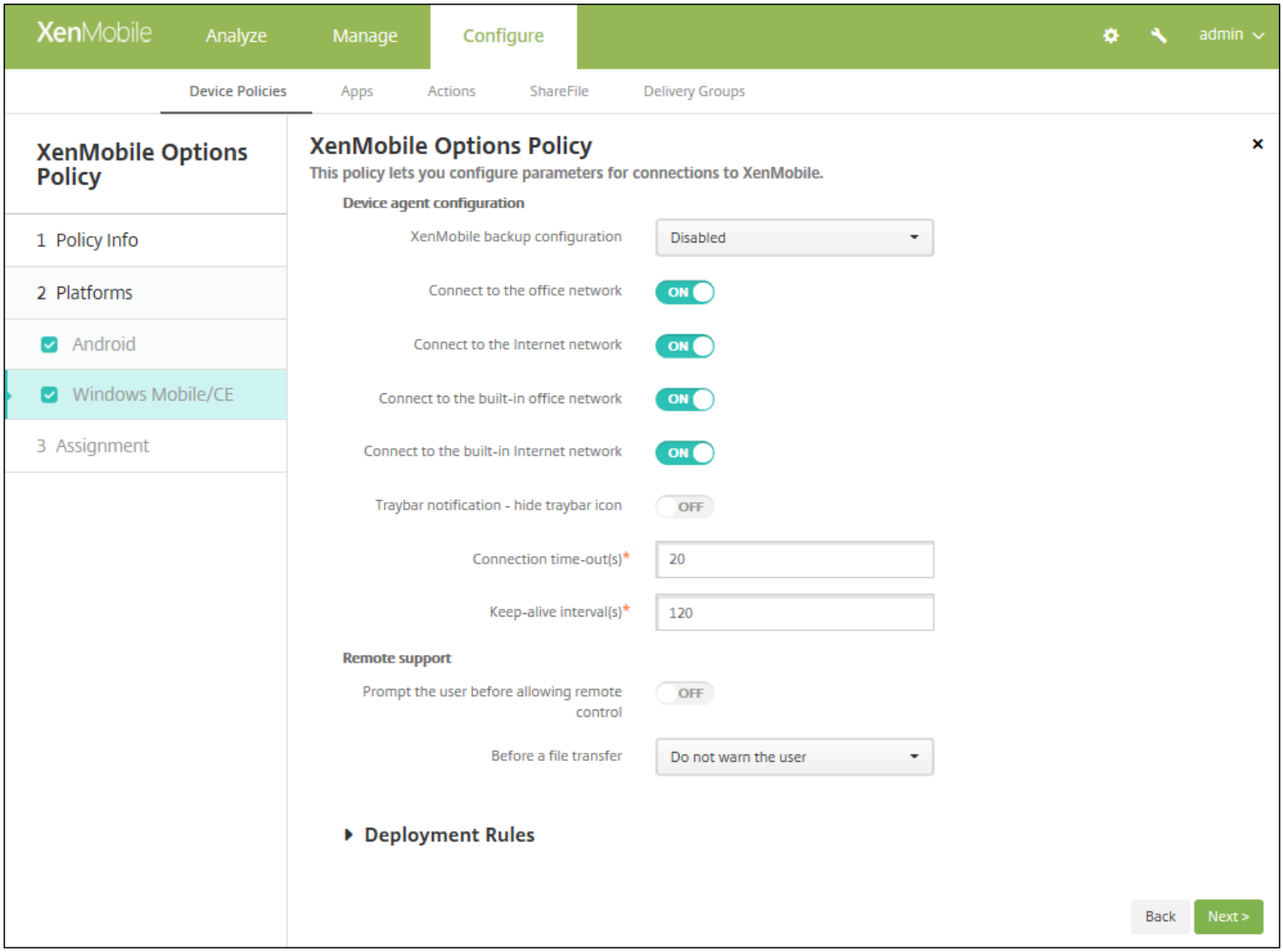
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **托盘栏通知 - 隐藏托盘栏图标**：选择是隐藏还是显示托盘栏图标。 默认值为**关**。
- **连接: 超时(秒)**：键入连接超时前连接可以空闲的时间长度，以秒为单位。 默认值为 20 秒。
- **保持活动状态时间间隔(秒)**：键入保持连接打开的时间长度，以秒为单位。 默认值为 120 秒。
- **在允许远程控制前提示用户**：选择是否在允许远程支持控制前提示用户。 默认值为**关**。
- **在文件传输前**：在列表中，单击是否就文件传输向用户发出警告，或是否请求用户允许。 可用值：**不警告用户**、**警告用户**和**要求用户权限**。 默认值为**不警告用户**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



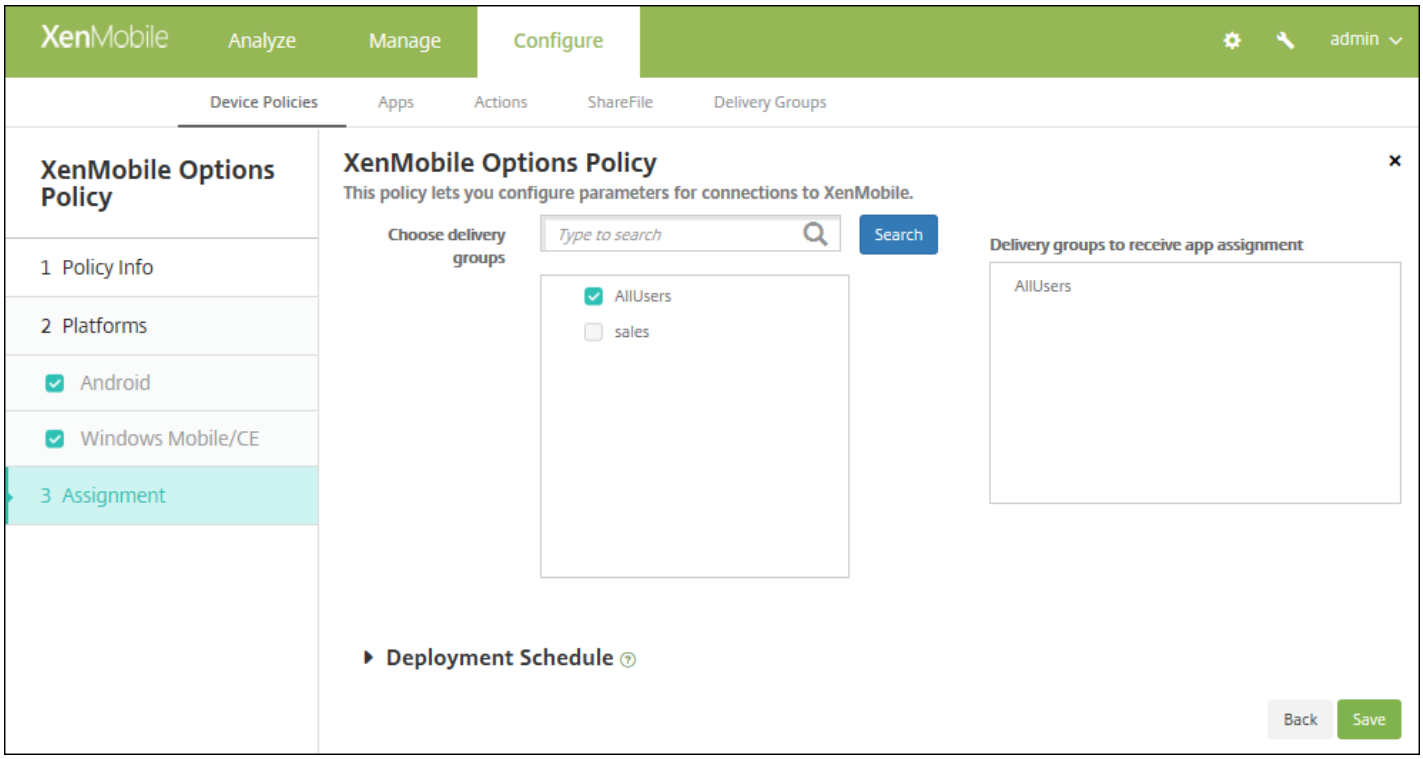
配置以下设置：

- **设备代理配置**
  - **XenMobile 备份配置**：在列表中，单击用于在用户设备上备份 XenMobile 配置的选项。 默认值为**已禁用**。 可用选项包括：
    - 已禁用
    - 安装 XenMobile 后首次连接时
    - 每次设备重新启动后首次连接时
  - **连接到办公网络**
  - **连接到 Internet 网络**
  - **连接到内置办公网络**：设置为**开**时，XenMobile 将自动检测网络。
  - **连接到内置 Internet 网络**：设置为**开**时，XenMobile 将自动检测网络。
  - **托盘栏通知 - 隐藏托盘栏图标**：选择是隐藏还是显示托盘栏图标。 默认值为**关**。
  - **连接超时(秒)**：键入连接超时前连接可以空闲的时间长度，以秒为单位。 默认值为 20 秒。
  - **保持活动状态时间间隔(秒)**：键入保持连接打开的时间长度，以秒为单位。 默认值为 120 秒。
- **远程支持**
  - **在允许远程控制前提示用户**：选择是否在允许远程支持控制前提示用户。 默认值为**关**。
  - **在文件传输前**：在列表中，单击是否就文件传输向用户发出警告，或是否请求用户允许。 可用值：**不警告用户**、**警告用户**和**要求用户权限**。 默认值为**不警告用户**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **XenMobile Options Policy**（XenMobile 选项策略）分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 卸载设备策略

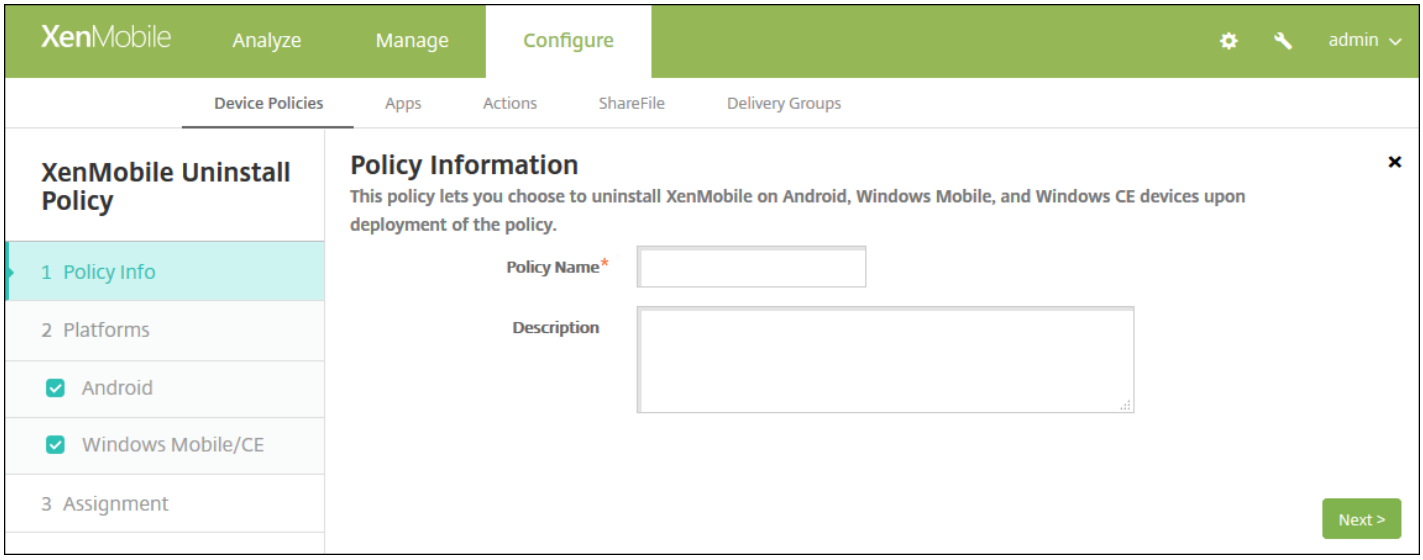
Aug 11, 2016

可以在 XenMobile 中添加一个设备策略，用于从 Android 和 Window Mobile/CE 设备卸载 XenMobile。 部署此策略时，它将从部署组中的所有设备上删除 XenMobile。

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 **XenMobile Agent** 下面，单击 **XenMobile 卸载**。 此时将显示 **XenMobile 卸载策略**页面。



4. 在**策略信息**窗格中，输入以下信息：

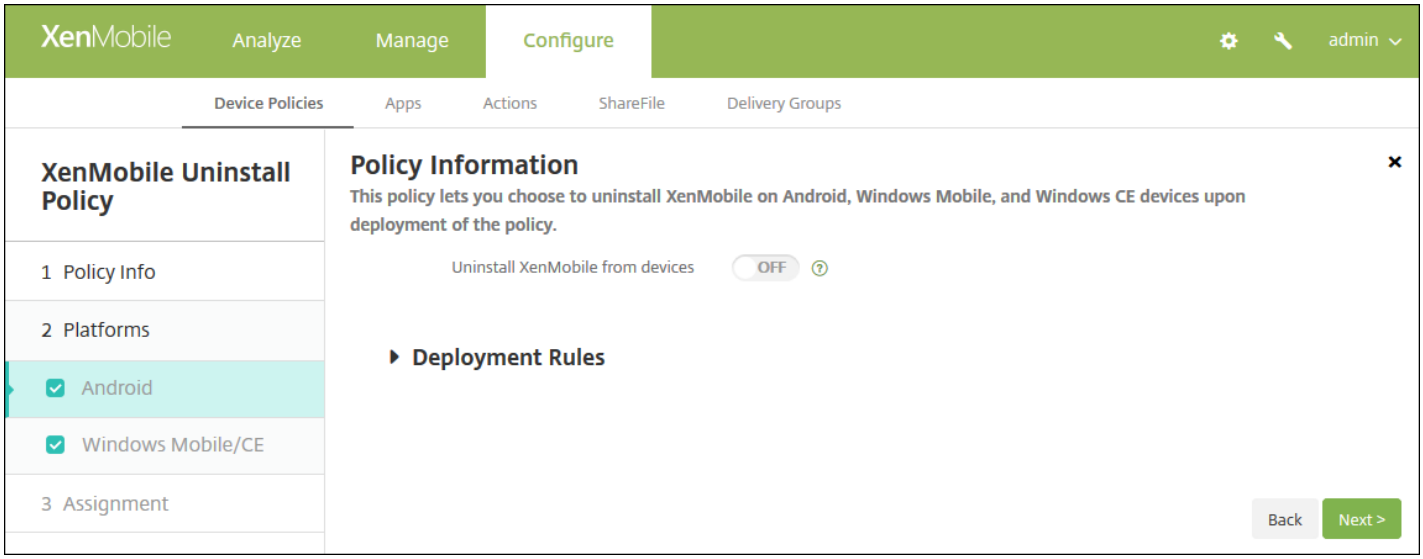
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。 此时将显示**策略平台**信息页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

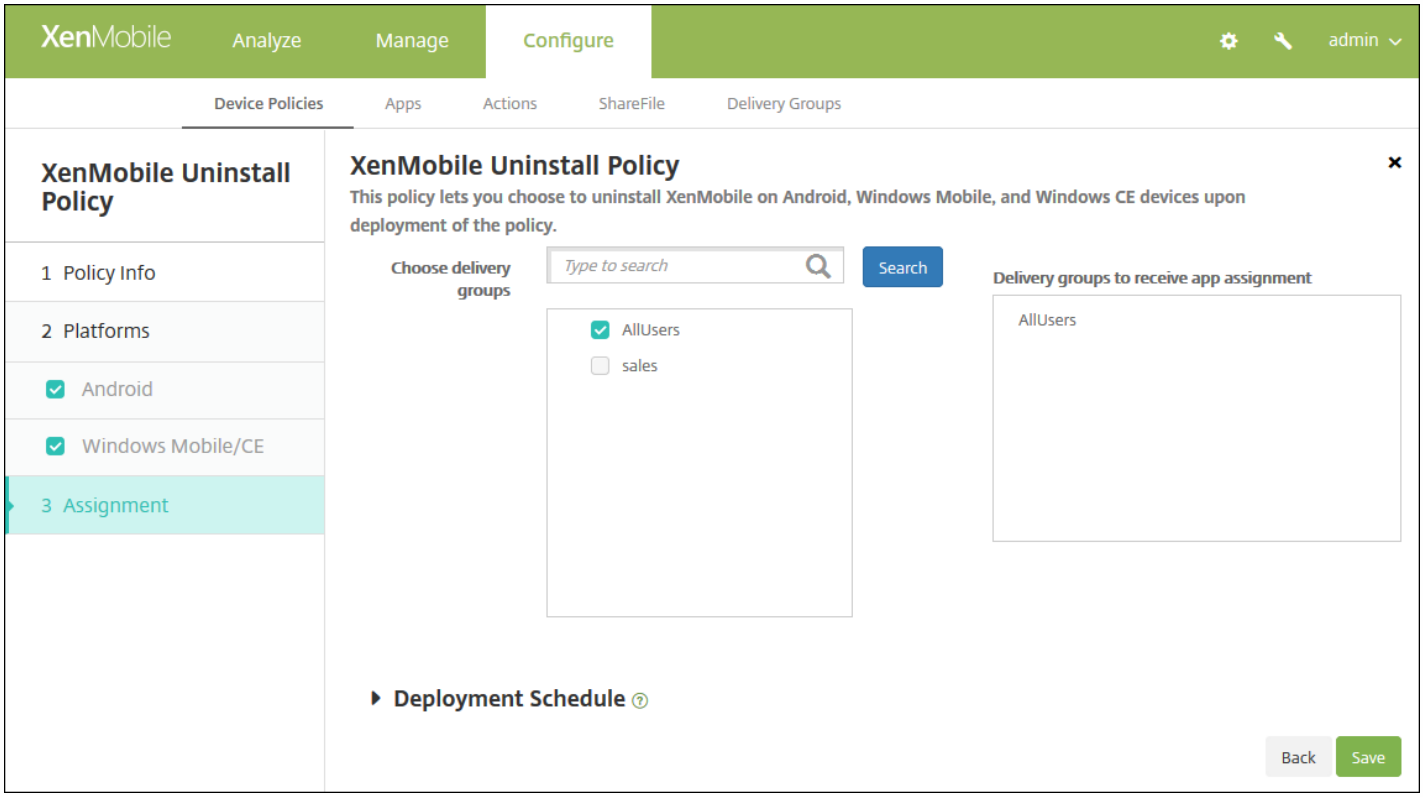


为您选择的各个平台配置此设置：

- **从设备中卸载 XenMobile**：选择是否从应用此策略的每个设备中卸载 XenMobile。 默认值为**关**。

7. 配置部署规则

8. 单击**下一步**。 此时将显示 **XenMobile 卸载策略**分配页面。



9. 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要向其分配策略的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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 之前的 部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

向 XenMobile 添加应用程序

Aug 11, 2016

可以向 XenMobile 中添加应用程序以便进行管理。 将应用程序添加到 XenMobile 控制台，然后可以在此处将应用程序分类，并将应用程序部署给用户。

可以将以下类型的应用程序添加到 XenMobile：

- **MDX**。 这些是指使用 MDX Toolkit（及相关策略）打包的应用程序。 部署从内部和公共应用商店获取的 MDX 应用程序。 例如，WorxMail。
- **公共应用商店**。 这些应用程序包括公共应用商店（如 iTunes 或 Google Play）中提供的免费或付费应用程序。 例如，GoToMeeting。 Android for Work 应用程序也属于此类别。
- **Web 和 SaaS 应用程序**。 这些应用程序包括通过内部网络（Web 应用程序）或公用网络 (SaaS) 访问的应用程序。 您可以创建自己的应用程序，或从一组用于对现有 Web 应用程序进行单点登录身份验证的应用程序连接器中选择： 例如，GoogleApps_SAML。
- **Enterprise Edition**。 这些应用程序是指未通过 MDX Toolkit 打包的本机应用程序，并且不包含与 MDX 应用程序关联的策略。
- **Web 链接**。 这是指公共或专用站点或者无需单点登录的 Web 应用程序的 Web 地址 (URL)。

> ## 注意
>
> Citrix 支持无提示安装 iOS 和 Samsung Android 应用程序。 无提示安装意味着系统不会提示用户安装您部署到设备的应用程序；应用程序将在后台无提示安装。 必须满足以下必备条件才能实施无提示安装：
>
> - 对于 iOS 应用程序，托管 iOS 设备必须处于受监督模式。 有关详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。
> - 对于 Android 应用程序，必须在设备上启用 Samsung for Enterprise (SAFE) 或 KNOX 策略。
>   为此，请设置 Samsung MDM 许可证密钥设备策略以生成 Samsung ELM 和 KNOX 许可证密钥。 有关详细信息，请参阅 Samsung MDM 许可证密钥设备策略。

XenMobile 支持 iOS、Mac OS X、Android 和 Windows 应用程序，包括 Worx 应用程序，如 Worx Home、WorxMail 和 WorxWeb 以及对 MDX 策略的使用。 使用 XenMobile 控制台可以上载应用程序，然后将应用程序交付给用户设备。 除了 Worx 应用程序，还可以添加以下类型的应用程序：

- 您为用户开发的应用程序。
- 希望在其中通过使用 MDX 策略允许或限制设备功能的应用程序。

Citrix 提供 MDX Toolkit，用于打包适用于 iOS、Mac OS X、Android 和 Windows 设备的移动应用程序与 Citrix 逻辑和策略。此工具可以安全地打包在组织内部开发的应用程序或在公司外部开发的应用程序。

XenMobile 附带一组应用程序连接器，这些连接器相当于模板，通过配置这些模板可实现对 Web 应用程序和软件即服务 (SaaS) 应用程序进行单点登录 (SSO)，在某些情况下，还可以通过配置这些连接器来创建和管理用户帐户。 XenMobile 包含安全声明标记语言 (SAML) 连接器。 SAML 连接器用于对支持 SAML 协议的 Web 应用程序实现 SSO 和用户帐户管理。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 支持 SAML 1.1 和 SAML 2.0。

您也可以构建自己的企业 SAML 连接器。

您可以在 XenMobile 中创建自己的应用程序连接器并上载 Android for Work 应用程序。 此类型的应用程序通常驻留在您的内部网络中。 用户可以使用 Worx Home 连接到应用程序。 添加企业应用程序的同时会创建应用程序连接器。

您可以配置设置以从 Apple App Store、Google Play 和 Windows 应用商店检索应用程序名称和说明。 在应用商店中检索应用程序信息时，XenMobile 会覆盖现有名称和说明。

Web 链接是指向 Internet 或 Intranet 站点的 Web 地址。 Web 链接还可以指向不需要 SSO 的 Web 应用程序。 Web 链接配置完成后，链接将以图标的形式显示在 Worx Store 中。 当用户通过 Worx Home 登录时，将显示该链接以及可用应用程序和桌面的列表。

使用控制台添加应用程序包括以下步骤：

- 添加有关应用程序的信息。
- 为每个受支持平台（如 iOS 或 Android）选择并配置应用程序。
- 定义可选批准方法。
- 设置可选交付组分配。

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。

注意：首次连接到 XenMobile 控制台时，**应用程序**表格为空；只有**添加**和**类别**选项可用。

2. 单击**添加**，然后按照以下适用于您所要添加类型的文章的主题操作：

- 向 XenMobile 中添加 MDX 应用程序
- 向 XenMobile 中添加公共应用商店应用程序
- 向 XenMobile 添加 Web 和 SaaS 应用程序
- 向 XenMobile 中添加企业应用程序
- 向 XenMobile 添加 Web 链接应用程序

添加应用程序后，应用程序将显示在**应用程序**页面上的表格中，您随时可以在这里编辑应用程序或对其进行分类。

> ## 注意
>
> 升级到 XenMobile 10.3 后，如果在 XenMobile 10.3 中更新先前在早期版本中配置的 Worx 移动应用程序，则该应用程序的设置将不再显示在 XenMobile 控制台中。 您需要重新编辑并配置这些应用程序的设置。 不需要重新安装这些应用程序。 此步骤只需执行一次；如果您将来更新应用程序或服务器，这些值将不受影响。

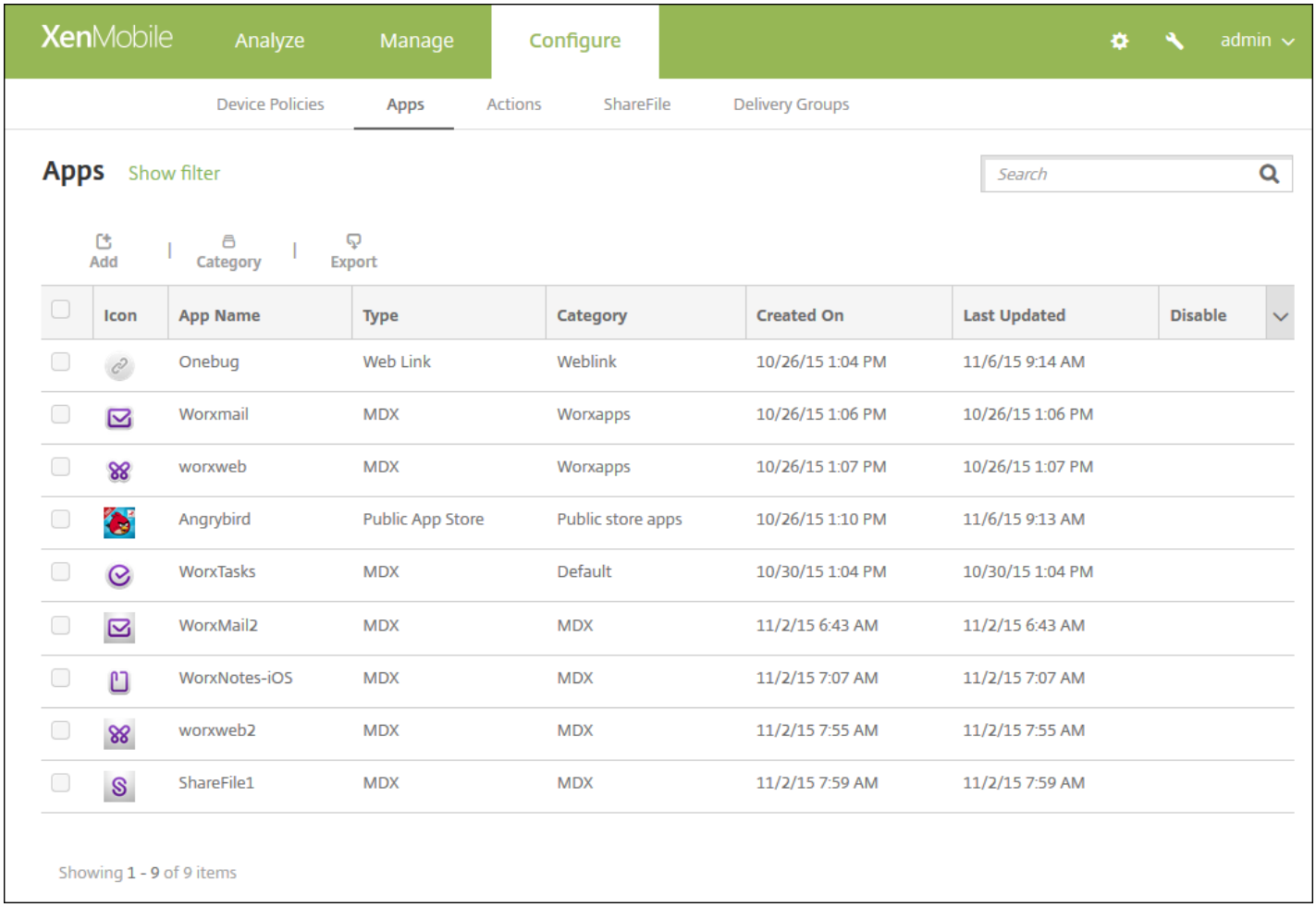
© 1999-2017 Citrix Systems, Inc. All rights reserved.

向 XenMobile 中添加 MDX 应用程序

Aug 11, 2016

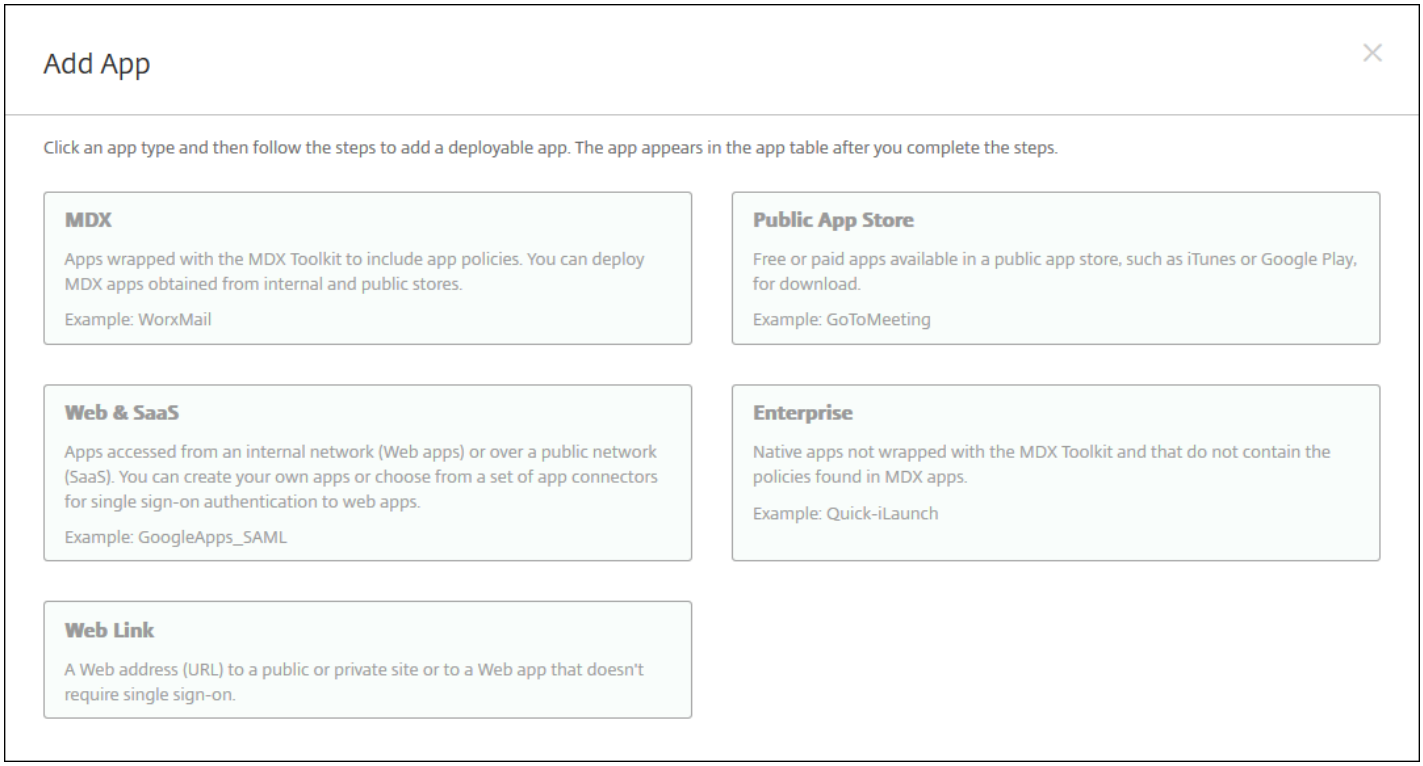
收到适用于 iOS、Android 或 Windows Phone 设备的打包 MDX 移动应用程序时，可以将应用程序上载到 XenMobile。 上载应用程序后，可以配置应用程序详细信息和策略设置。 有关每种设备平台类型可用的应用程序策略的详细信息，请参阅适用于 iOS、Android 和 Windows Phone 的 MDX 策略概览。该部分内容还详细介绍了策略的相关信息。

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。

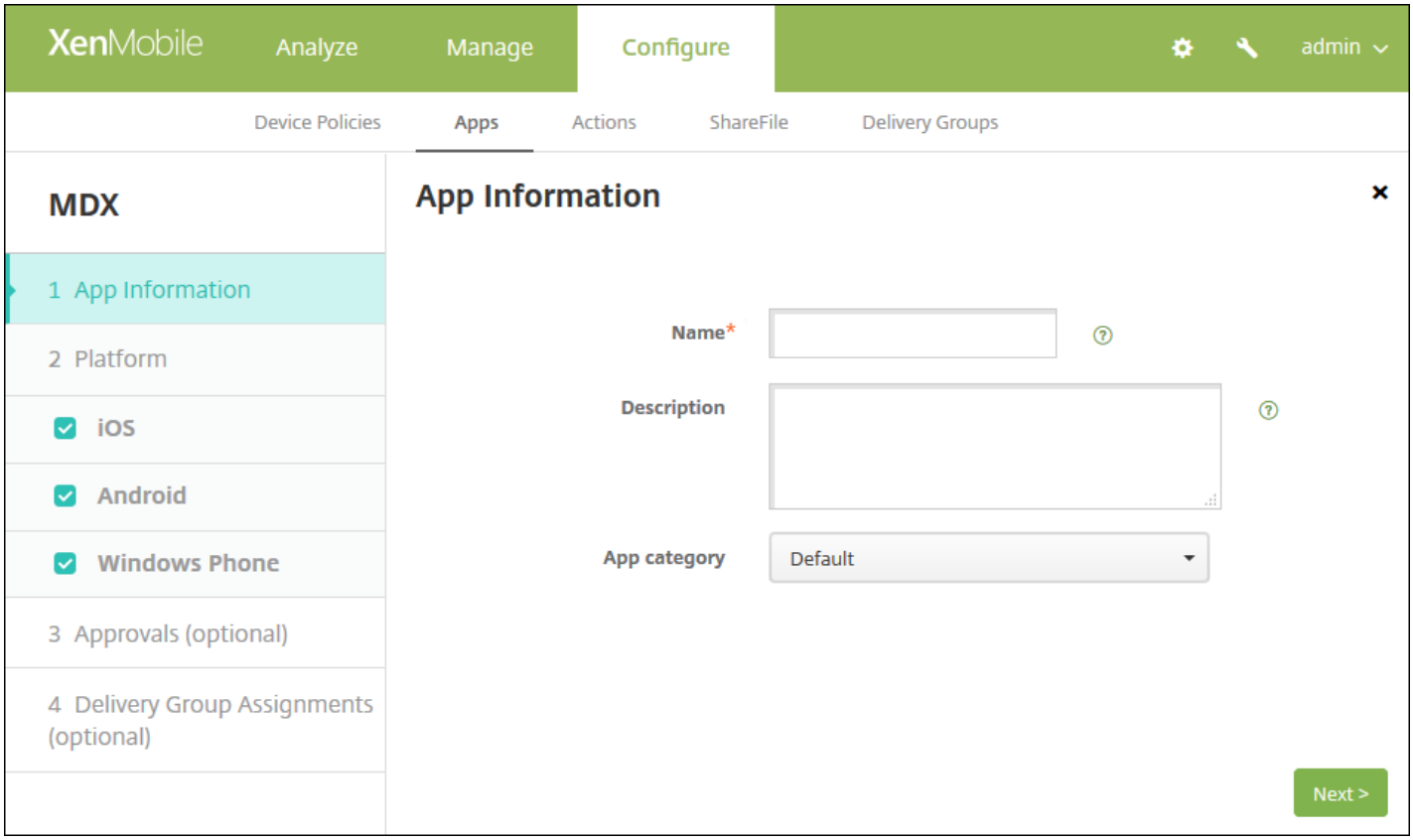


2. 单击**添加**。 此时将显示**添加应用程序**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 单击 **MDX**。 此时将显示 **MDX 应用程序信息**页面。



4. 在**应用程序信息**窗格中，键入以下信息：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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**表格上的**应用程序名称**下面。
- **说明**：键入应用程序的可选说明。
- **应用程序类别**：（可选）在列表中，单击要将应用程序添加到的类别。 有关应用程序类别的详细信息，请参阅在 XenMobile 中创建应用程序类别。

5. 单击**下一步**。 此时将显示**应用程序平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 11 以了解如何设置此平台的部署规则。

7. 通过单击**上载**并导航到要上载的 .mdx 文件的位置，选择此文件。

- 如果要添加 iOS VPP B2B 应用程序，请单击**您的应用程序是 VPP B2B 应用程序吗?** ，然后在此列表中单击要使用的 B2B VPP 帐户。

8. 单击**下一步**。 此时将显示应用程序详细信息页面。

9. 配置以下设置：

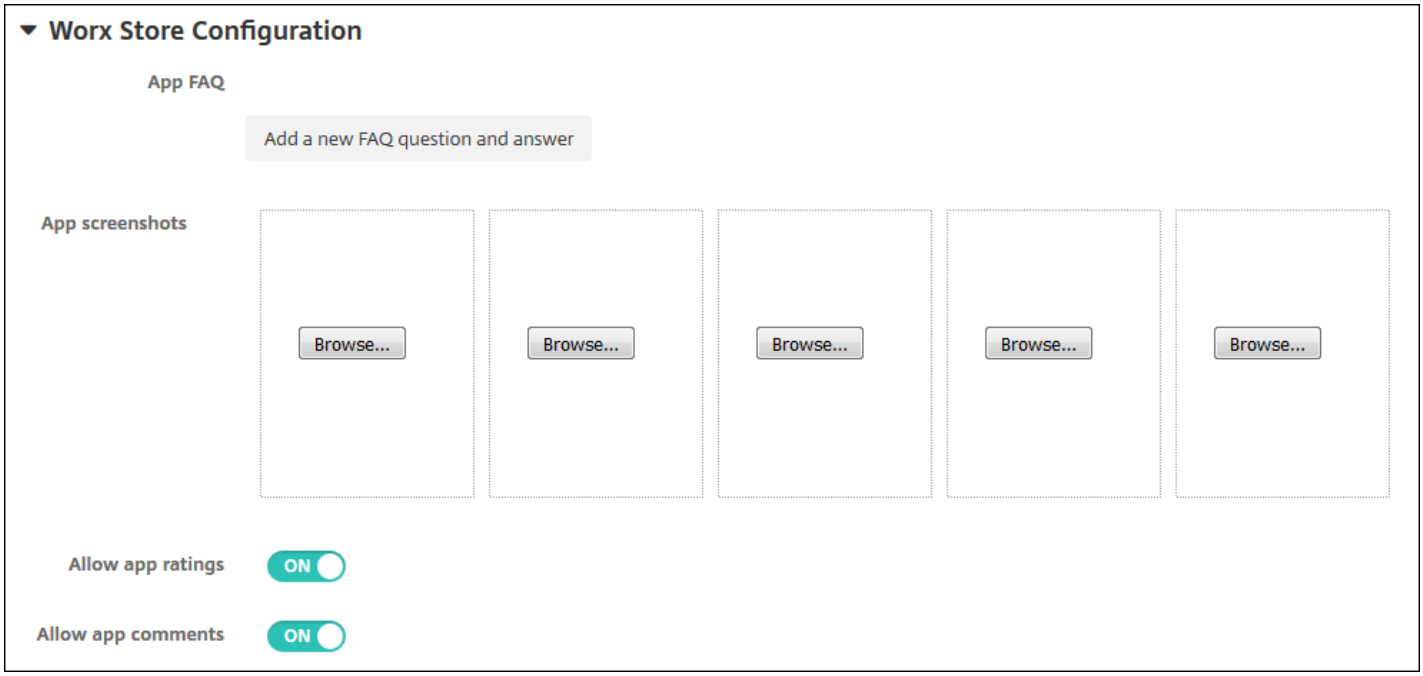
- **文件名**：键入与应用程序关联的文件名。
- **应用程序说明**：键入应用程序的说明。
- **应用程序版本**：可选，键入应用程序的版本号。
- **最低操作系统版本**：可选，键入为使用应用程序设备可以运行的最低操作系统版本。
- **最高操作系统版本**：可选，键入为使用应用程序设备必须运行的最新操作系统版本。
- **排除的设备**：可选，键入不可以运行此应用程序的设备制造商或型号。
- **删除 MDM 配置文件时也删除应用程序**：选择删除 MDM 配置文件时是否从设备删除应用程序。 默认值为 **ON**。
- **阻止备份应用程序数据**：选择是否阻止用户备份应用程序数据。 默认值为 **ON**。
- **强制管理应用程序**：选择当应用程序在未托管状态下安装时，是否提示用户允许在未受监督的设备上管理此应用程序。 默认值为 **ON**。 iOS 9.0 及以上版本支持此功能。

10. 配置 **MDX 策略**。 MDX 策略因平台而异，并包含用于身份验证、设备安全、网络要求、其他访问、加密、应用程序交互、应用程序限制、应用程序网络访问、应用程序日志和应用程序地理围栏等策略区域的选项。 在控制台中，每种策略都具有介绍此策略的提示。 有关 MDX 应用程序的应用程序策略详细信息，如显示哪些策略适用于哪些平台类型的表格，请参阅适用于 iOS、Android 和 Windows Phone 的 MDX 策略概览。

11. 配置部署规则

12. 展开 **Worx Store 配置**。

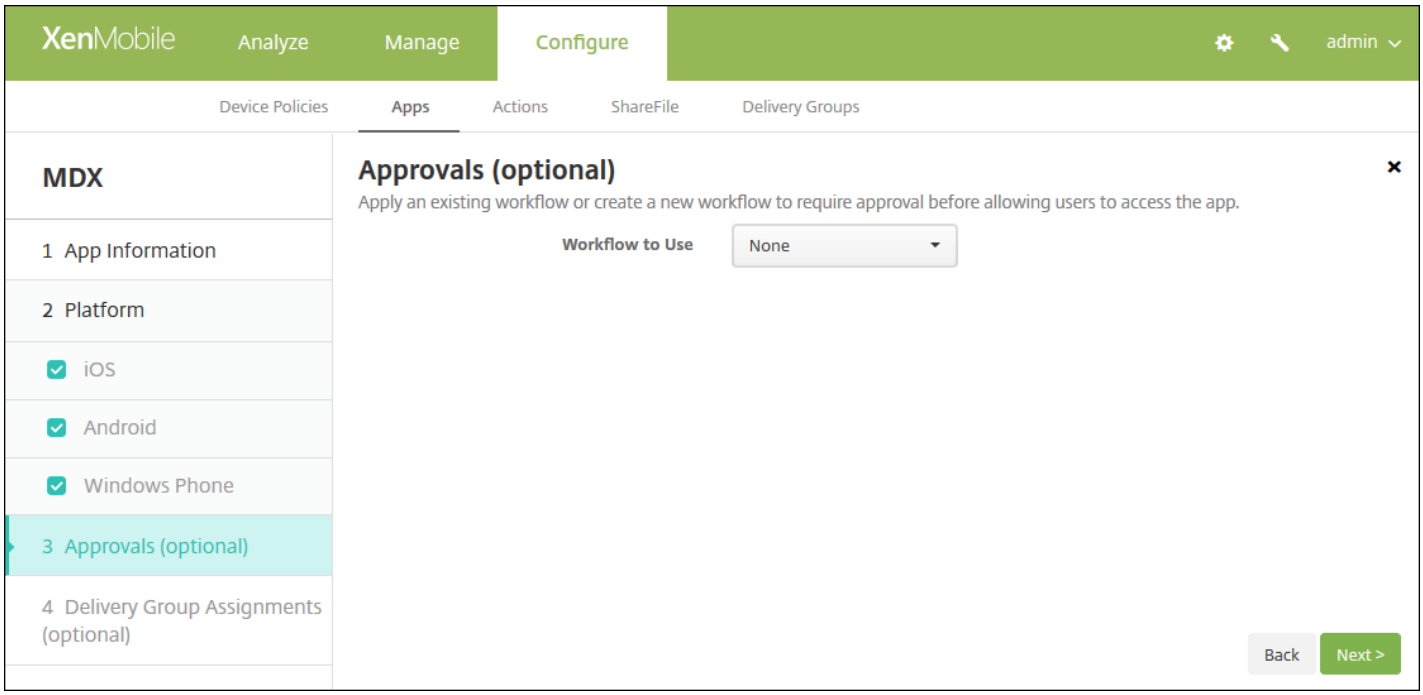
© 1999-2017 Citrix Systems, Inc. All rights reserved.



（可选）可以添加应用程序的常见问题解答或显示在 Worx Store 中的屏幕截图。 还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - **应用程序常见问题解答**：添加应用程序的常见问题和答案。
  - **应用程序屏幕截图**：添加屏幕截图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形必须为 PNG 格式。 不能上载 GIF 或 JPEG 图形。
  - 在**允许对应用程序评分**中，选择是否允许用户对应用程序进行评分。 默认值为**开**。
  - 在**允许评价应用程序**中，选择是否允许用户评价选定的应用程序。 默认值为**开**。

13. 单击**下一步**。 此时将显示**审批**页面。



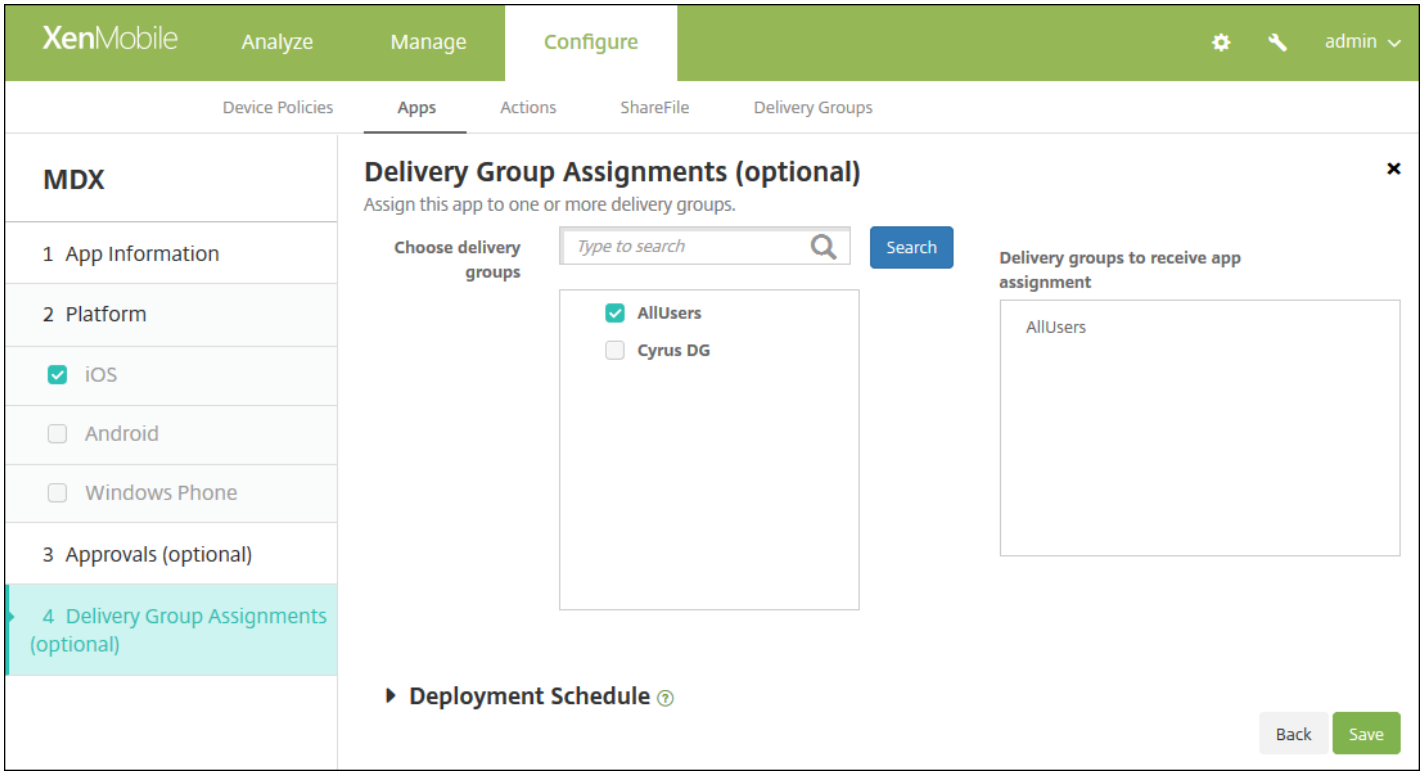
© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建用户帐户时如果需要审批则使用流程。 如果无需设置审批流程，可以跳至第 15 步。

如果需要指定或创建流程，请配置此设置：

- **要使用的流程**：在此列表中，单击现有流程或单击**创建新流程**。 默认值为**无**。
- 如果选择**创建新流程**，请配置以下设置：
  - **名称**：键入流程的唯一名称。
  - **说明**：可选，键入流程的说明。
  - **电子邮件审批模板**：在列表中，选择要指定的电子邮件审批模板。 单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
  - **经理审批级别**：在列表中，选择此流程所需的经理审批级别数。 默认值为 1 级。 可用选项包括：
    - 不需要
    - 1 级
    - 2 级
    - 3 级
  - **选择 Active Directory 域**：在列表中，选择用于流程的合适的 Active Directory 域。
  - **查找所需的其他审批者**：在搜索字段中键入其他必需人员的姓名，然后单击**搜索**。 源于 Active Directory 的姓名。
  - 人员的姓名显示在此字段中后，选中其姓名旁边的复选框。 人员的姓名和电子邮件地址显示在**选定的其他所需审批者**列表中。
    - 要从**选定的其他所需审批者**列表中删除人员，请执行以下操作：
      - 单击**搜索**以查找选定域中的所有人员列表。
      - 在搜索框中键入完整名称或部分名称，然后单击**搜索**以限制搜索结果。
      - 在搜索结果列表中，**选定的其他所需审批者**列表中的人员姓名旁边有一个复选标记。 滚动列表，并取消选中要删除的各个姓名旁边的复选框。

14. 单击**下一步**。 此时将显示**交付组分配**页面。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

15. 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要向其分配应用程序的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

16. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

17. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中创建应用程序类别

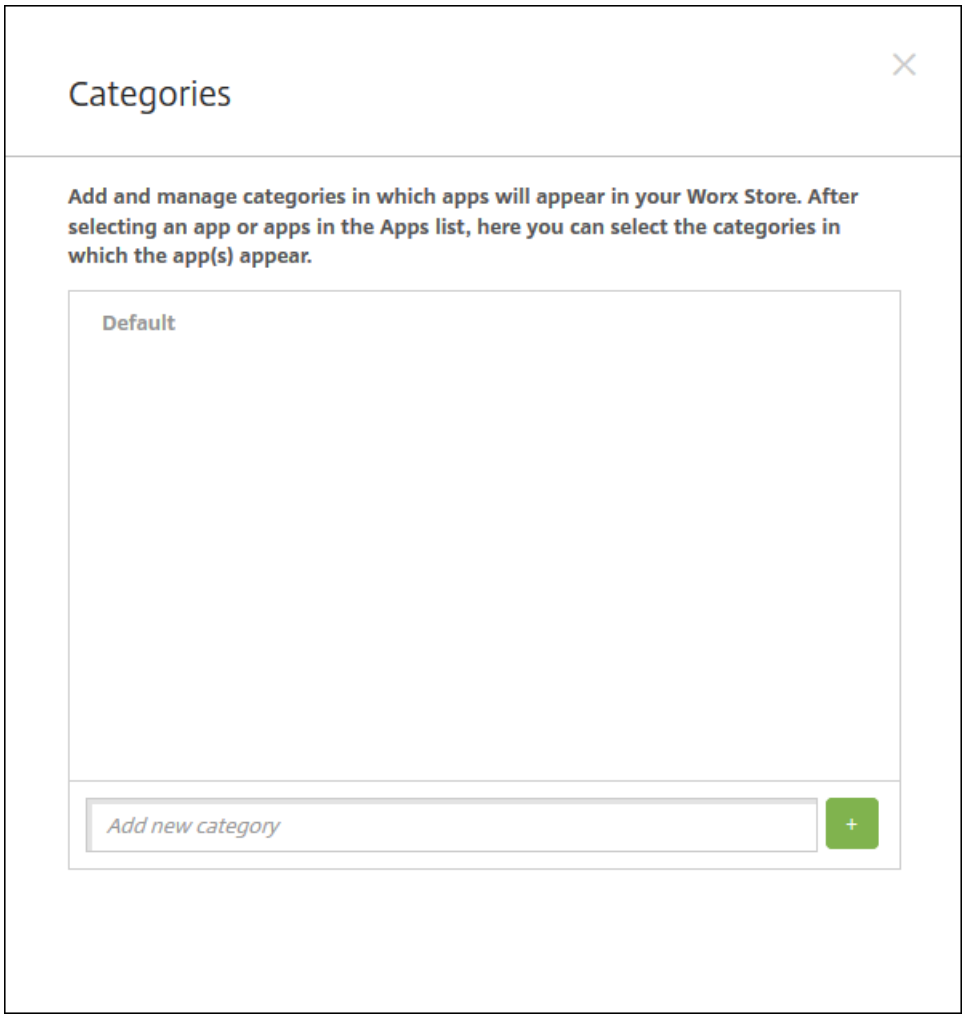
Aug 11, 2016

用户登录 Worx Home 时，会收到您已在 XenMobile 中添加并设置的应用程序、Web 链接和应用商店的列表。 您可以使用应用程序类别实现只允许用户访问您希望其访问的应用程序、应用商店或 Web 链接的目的。 例如，您可以创建“财务”类别，然后向其中添加仅与财务相关的应用程序。 您也可以配置“销售”类别，并向其分配销售应用程序。

在 XenMobile 控制台中的**应用程序**页面上配置类别。 然后，添加或编辑应用程序、Web 链接或应用商店时，可以将应用程序添加到您所配置的一个或多个类别中。

1. 在 XenMobile 控制台中，单击**配置 > 应用程序**。 此时将显示**应用程序**页面。

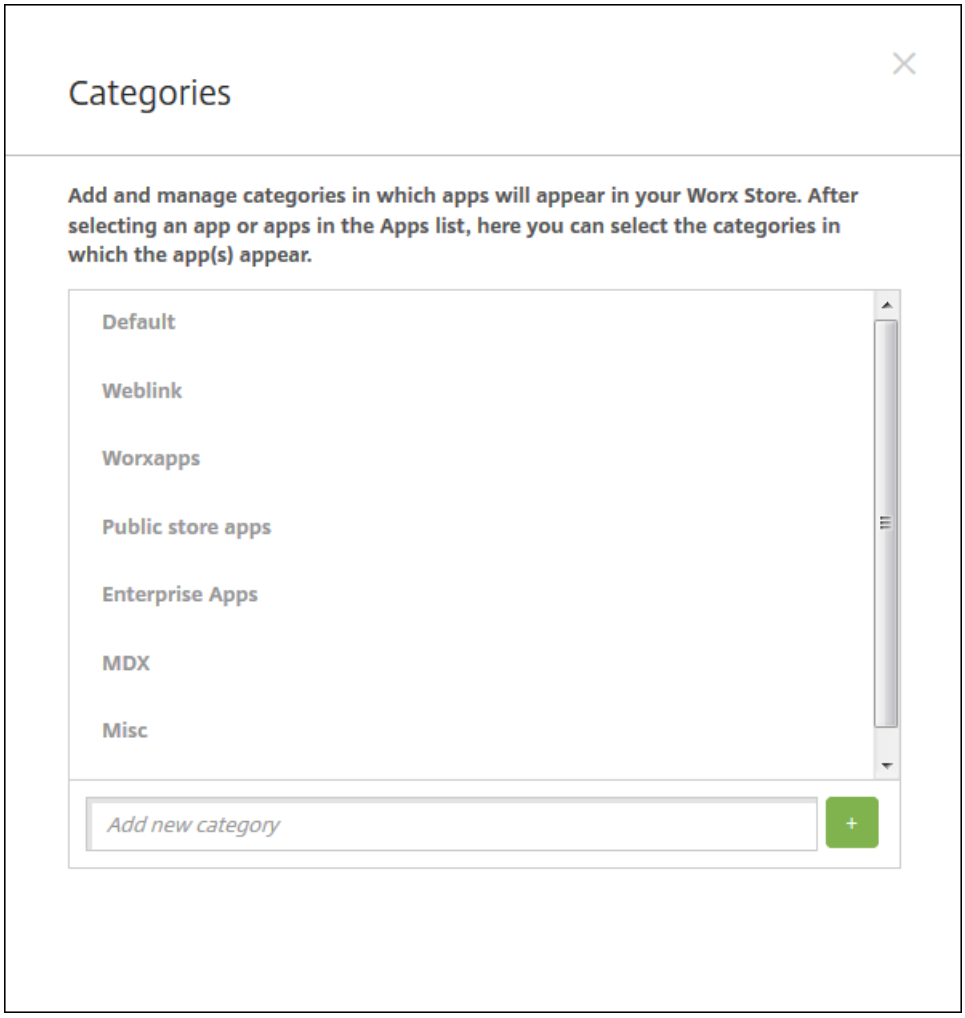
2. 单击**类别**。 将显示**类别**对话框。



3. 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，键入要添加的类别的名称。 例如，可以键入*企业应用程序*以创建企业应用程序类别。
- 单击加号 (+) 以添加类别。 此时已添加新创建的类别并显示在**类别**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 完成添加类别操作后，关闭**类别**对话框。

5. 在**应用程序**页面上，可以将现有应用程序放到新类别中。

- 选择要分类的应用程序。
- 单击**编辑**。 此时将显示**应用程序信息**页面。
- 在**应用程序类别**列表中，通过选中新类别的复选框应用新类别。 对于您不想应用到应用程序的现有类别，可以取消其对应的复选框。
- 单击**交付组分配**选项卡或单击后面各页面上的**下一步**完成剩余的应用程序设置页面。
- 单击**交付组分配**页面上的**保存**以应用新类别。 新类别将应用到应用程序并显示在**应用程序**表格中。

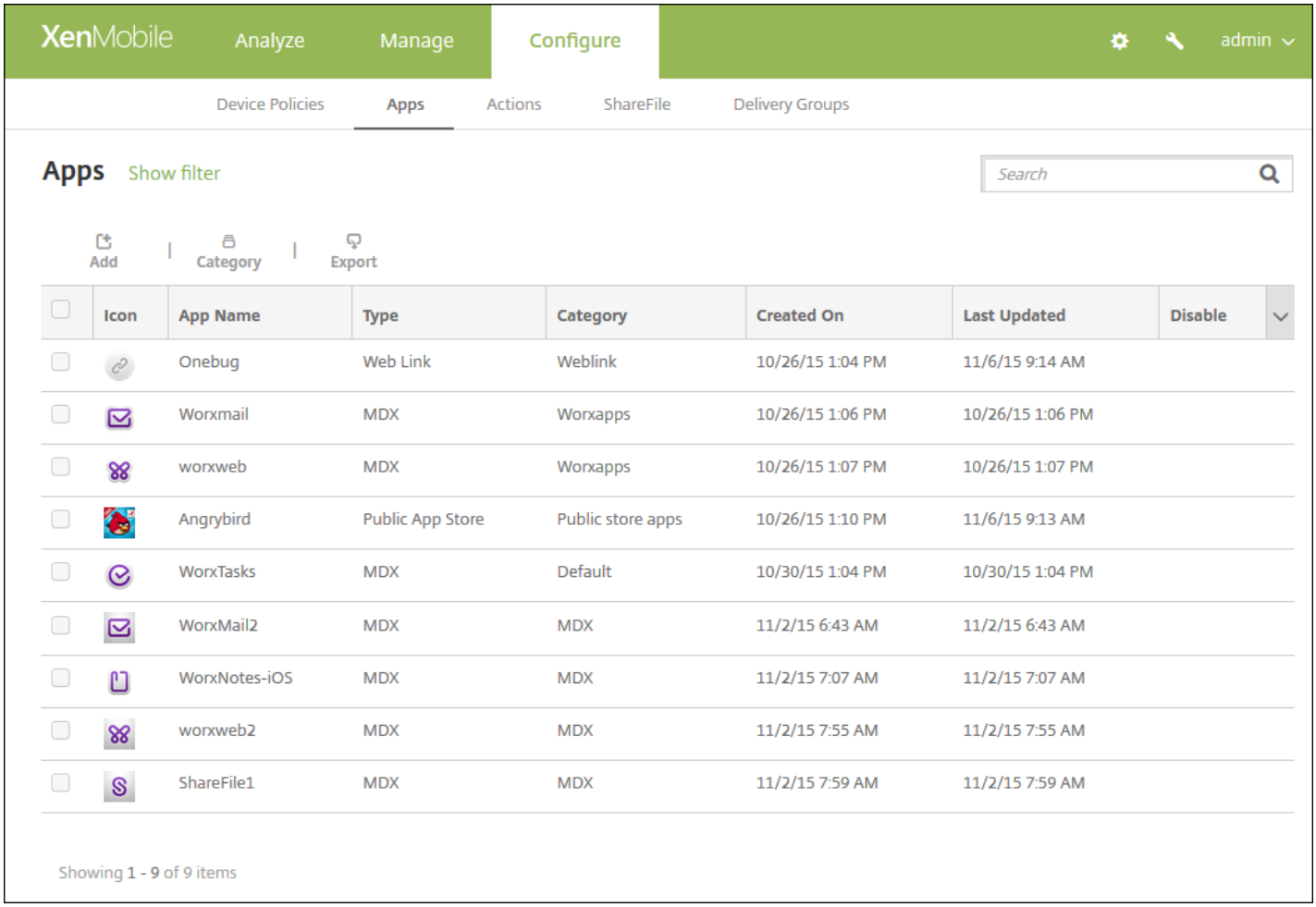
© 1999-2017 Citrix Systems, Inc. All rights reserved.

向 XenMobile 中添加公共应用商店应用程序

Oct 21, 2016

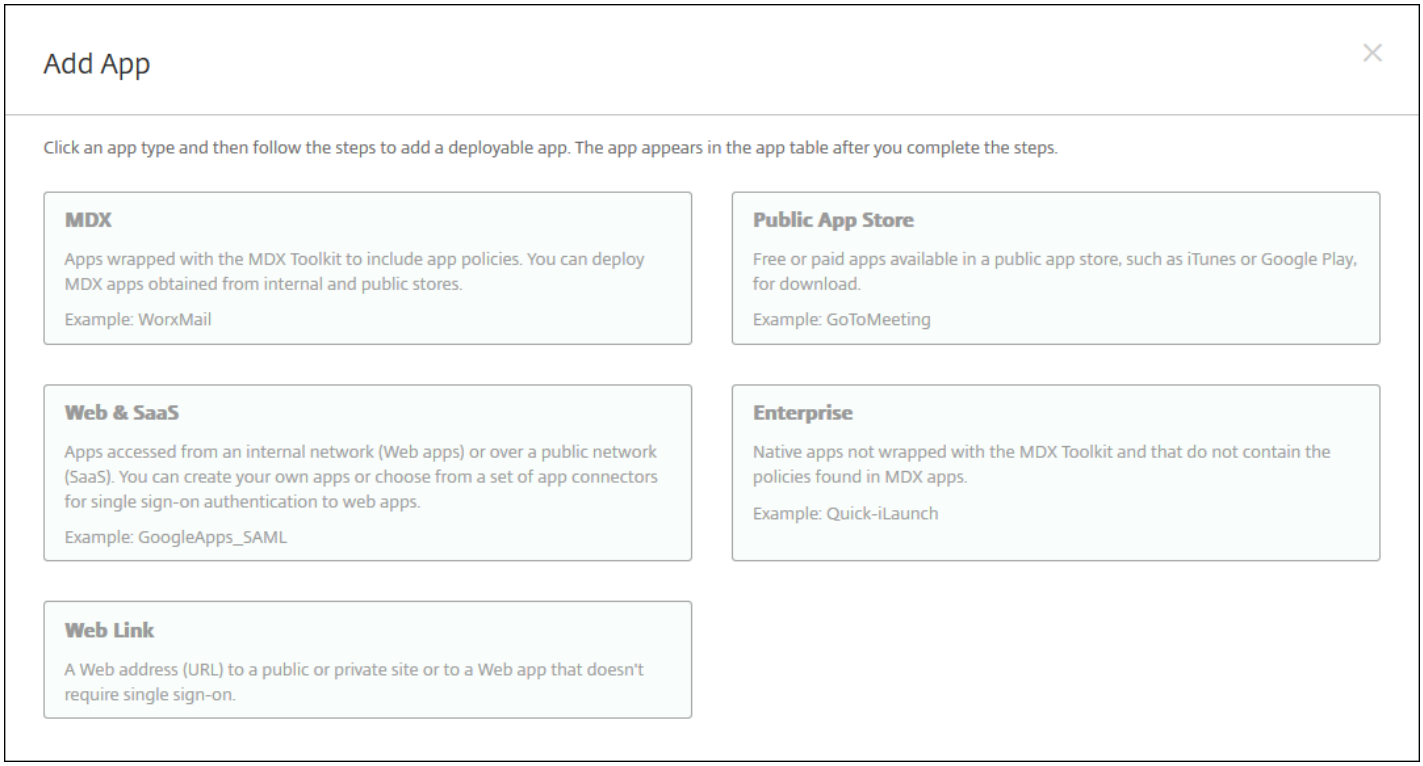
可以向 XenMobile 中添加公共应用商店（如 iTunes 或 GooglePlay）中提供的免费或付费应用程序。 例如，GoToMeeting。 此外，为 Android for Work 添加付费公共应用商店应用程序时，可以查看批量购买许可状态，即可用的许可证总数和当前正在使用的许可证数量，以及使用这些许可证的每个用户的电子邮件地址。 面向 Android for Work 的批量购买计划简化了组织批量查找、购买和分发应用程序及其他数据的过程。

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。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 单击**公共应用商店**。 此时将显示**应用程序信息**页面。

4. 在**应用程序信息**窗格中，键入以下信息：

- **名称**：键入应用程序的描述性名称。 此名称将显示在“应用程序”表格上的“应用程序名称”下面。
- **说明**：键入应用程序的可选说明。
- **应用程序类别**：（可选）在列表中，单击要将应用程序添加到的类别。 有关应用程序类别的详细信息，请参阅在 XenMobile 中创建应用程序类别。

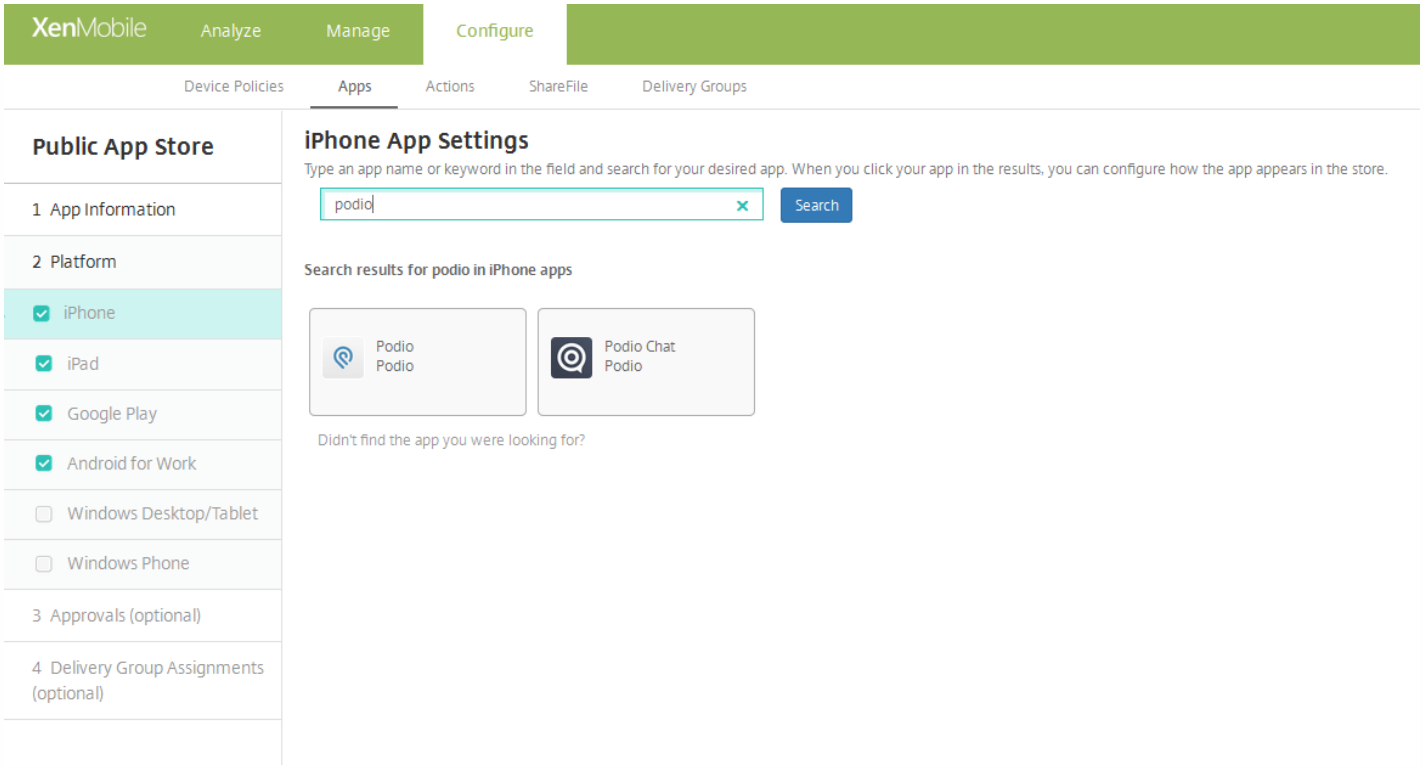
5. 单击**下一步**。 此时将显示**应用程序平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

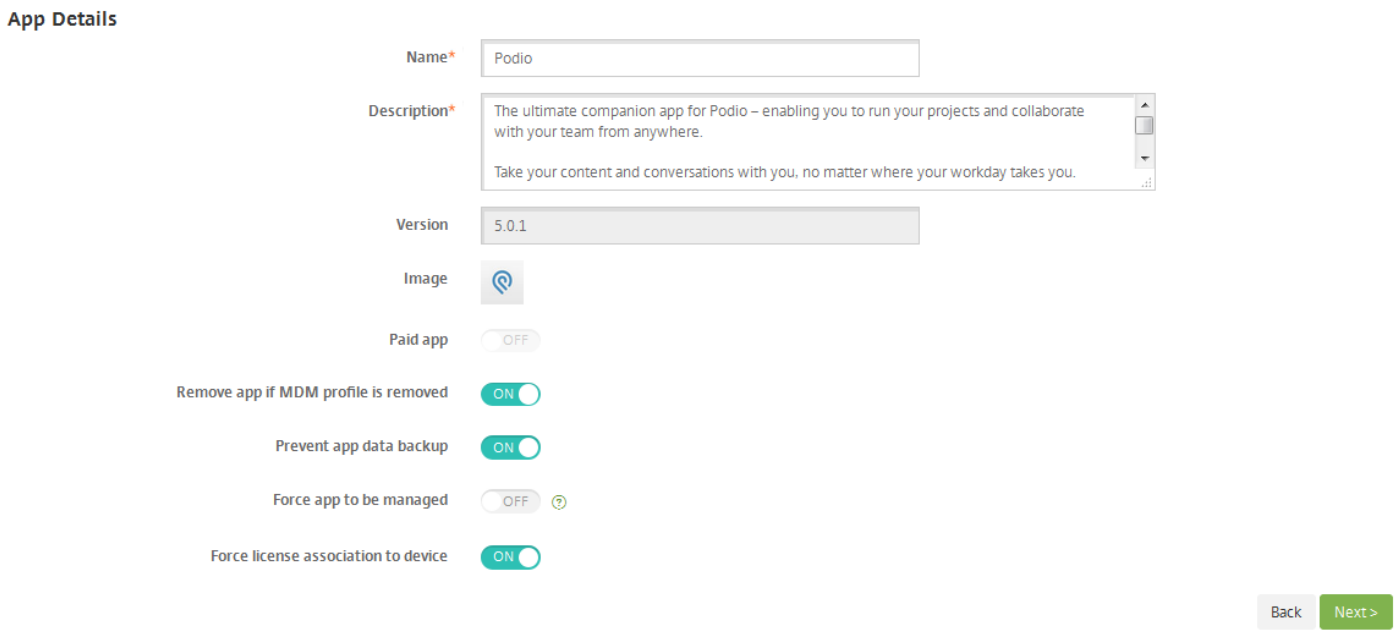
完成对平台设置的配置后，请参阅步骤 10 以了解如何设置此平台的部署规则。

7. 通过在搜索框中键入应用程序名称并单击**搜索**，选择要添加的应用程序。 此时将显示符合搜索条件的应用程序。 下图显示了 *podio* 的搜索结果。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. 单击要添加的应用程序。 **应用程序详细信息**字段已经预填充了与所选应用程序相关的信息（包括关联的名称、说明、版本号和关联的图像）。



9. 配置以下设置：

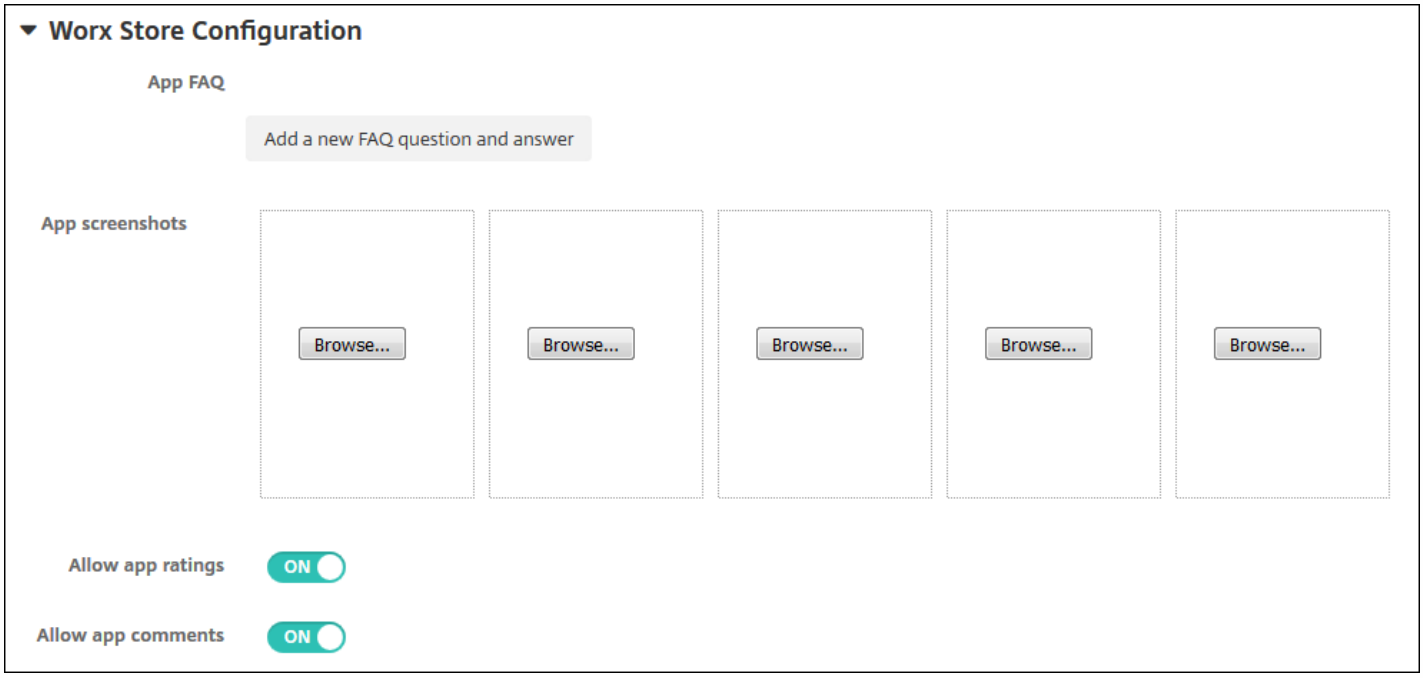
- 如有需要，可更改应用程序的名称和说明。
- **付费应用程序**：此字段已经预配置，并且无法更改。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **删除 MDM 配置文件时也删除应用程序**：选择是否在删除 MDM 配置文件时删除应用程序。 默认值为**开**。
- **阻止备份应用程序数据**：选择是否阻止应用程序备份数据。 默认值为**开**。
- **强制管理应用程序**：选择当应用程序在未托管状态下安装时，是否提示用户允许在未受监督的设备上管理此应用程序。 默认值为**关**。 iOS 9.0 及以上版本支持此功能。
- **强制与设备建立许可证关联**：选择是否将开发时启用设备关联的应用程序与设备而非用户关联。 在 iOS 9 及更高版本中可用。 如果所选应用程序不支持分配到设备，则您无法更改此字段。

10. 配置部署规则

11. 展开 **Worx Store 配置**。



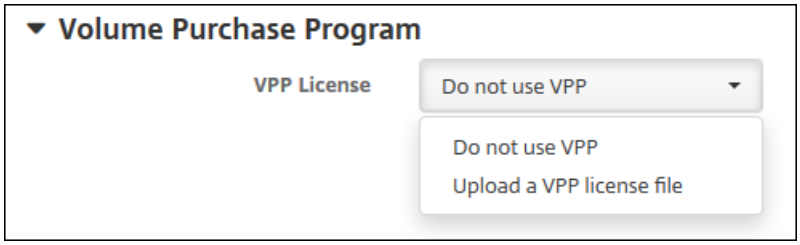
（可选）可以添加应用程序的常见问题解答或显示在 Worx Store 中的屏幕截图。 还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - **应用程序常见问题解答**：添加应用程序的常见问题和答案。
  - **应用程序屏幕截图**：添加屏幕截图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形必须为 PNG 格式。 不能上载 GIF 或 JPEG 图形。
  - 在**允许对应用程序评分**中，选择是否允许用户对应用程序进行评分。 默认值为“开”。
  - 在**允许评价应用程序**中，选择是否允许用户评价选定的应用程序。

12. 展开 **Volume Purchase Program**，或者在 Android for Work 中展开**批量购买**。

对于 Volume Purchase Program，请完成以下步骤。

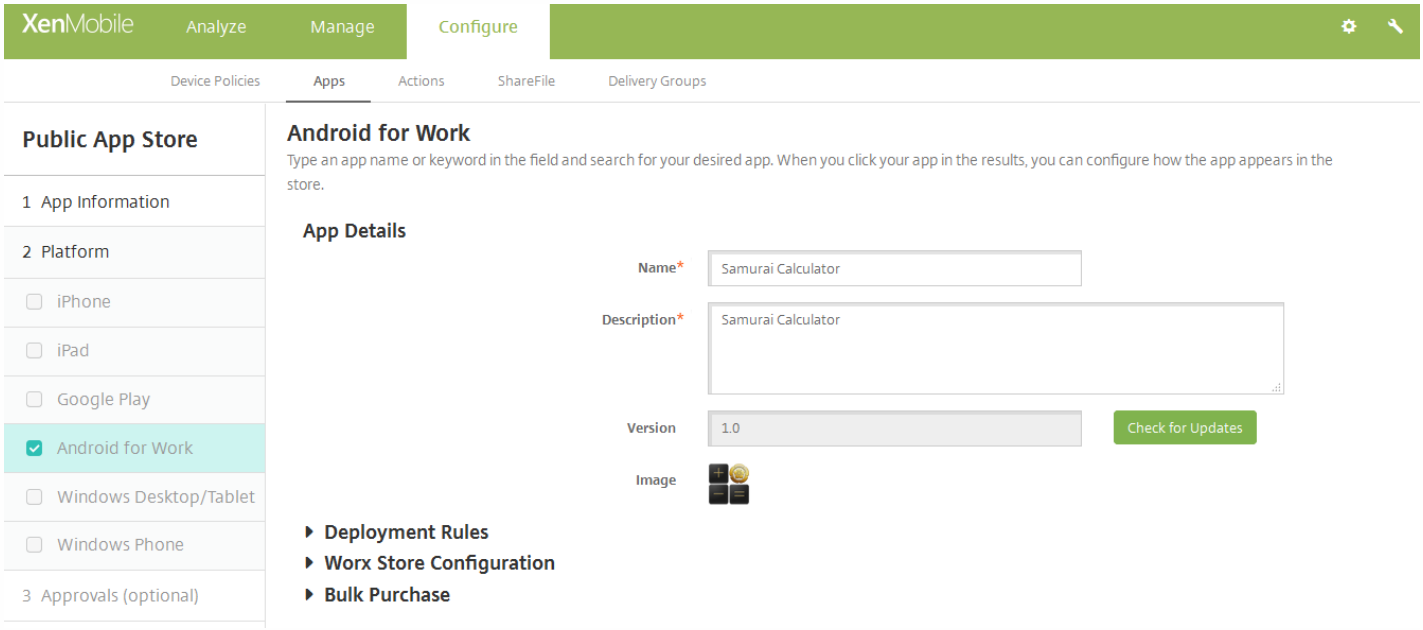
© 1999-2017 Citrix Systems, Inc. All rights reserved.



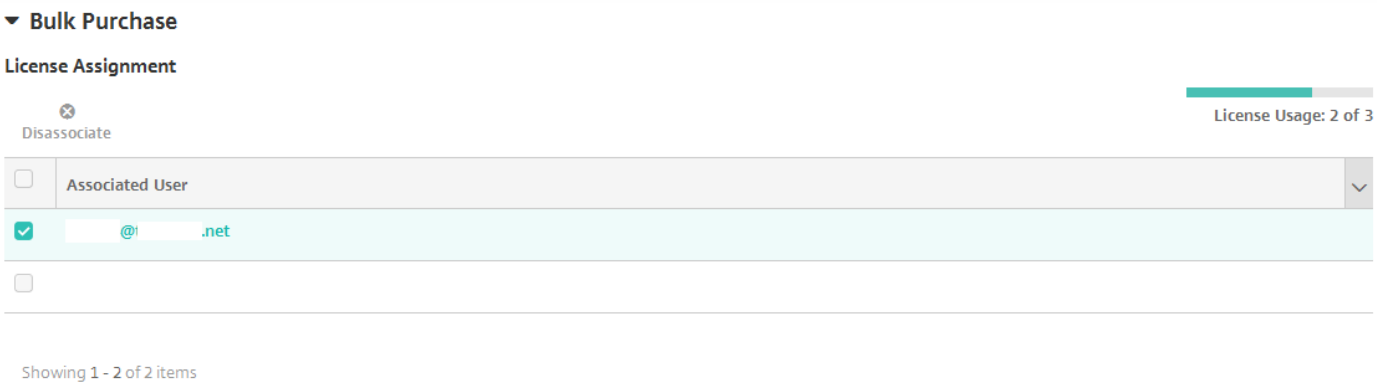
a. 如果要允许 XenMobile 为应用程序应用 VPP 许可证，请在 **VPP 许可证**列表中，单击**上载 VPP 许可证文件**。

b. 在显示的对话框中，导入许可证。

对于 Android for Work 批量购买，请展开**批量购买**部分。



在“许可证分配”表中，您将看到应用程序当前正在使用的许可证数量以及可用许可证总数。 可以选择一个用户，然后单击**解除关联**以结束其许可证分配，释放一个许可证以供其他用户使用。 但是，如果该用户不属于包含特定应用程序的交付组的一部分，您将只能解除该许可证的关联。



13. 单击**下一步**。 此时将显示审批页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建用户帐户时如果需要审批则使用流程。 如果无需设置审批流程，可以跳至下一步。

如果需要指定或创建流程，请配置此设置：

- **要使用的流程**：在此列表中，单击现有流程或单击**创建新流程**。 默认值为**无**。
- 如果选择**创建新流程**，请配置以下设置：
  - **名称**：键入流程的唯一名称。
  - **说明**：可选，键入流程的说明。
  - **电子邮件审批模板**：在列表中，选择要指定的电子邮件审批模板。 单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
  - **经理审批级别**：在列表中，选择此流程所需的经理审批级别数。 默认值为 **1 级**。 可用选项包括：
    - 不需要
    - 1 级
    - 2 级
    - 3 级
  - **选择 Active Directory 域**：在列表中，选择用于流程的合适的 Active Directory 域。
  - **查找所需的其他审批者**：在搜索字段中键入其他必需人员的姓名，然后单击**搜索**。 源于 Active Directory 的姓名。
  - 人员的姓名显示在此字段中后，选中其姓名旁边的复选框。 人员的姓名和电子邮件地址显示在**选定的其他所需审批者**列表中。
    - 要从**选定的其他所需审批者**列表中删除人员，请执行以下操作：
    - 单击**搜索**以查找选定域中的所有人员列表。
    - 在搜索框中键入完整名称或部分名称，然后单击**搜索**以限制搜索结果。
    - 在搜索结果列表中，**选定的其他所需审批者**列表中的人员姓名旁边有一个复选标记。 滚动列表，并取消选中要删除的各个姓名旁边的复选框。

14. 单击**下一步**。 此时将显示**交付组分配**页面。

15. 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要向其分配应用程序的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

16. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

17. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

向 XenMobile 添加 Web 和 SaaS 应用程序

Aug 11, 2016

使用 XenMobile 控制台，可以向用户提供对移动应用程序、企业应用程序、Web 应用程序和 SaaS 应用程序的单点登录 (SSO) 授权。 可以通过使用应用程序连接器模板，为应用程序启用 SSO。 有关 XenMobile 中可用连接器类型的列表，请参阅应用程序连接器类型列表。 您也可以在 XenMobile 中构建自己的连接器。

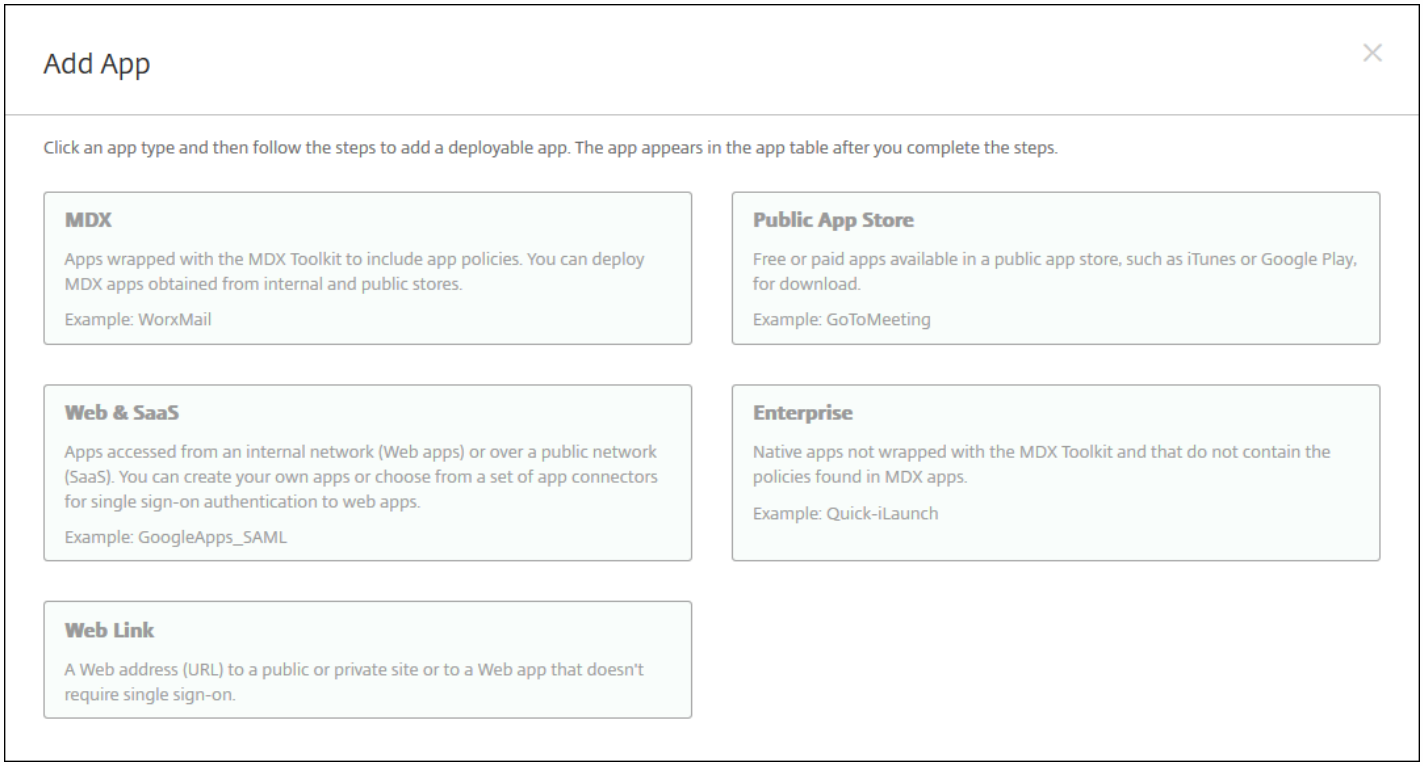
通过提供以下信息设置连接器：

- 不同的名称（可选）。 使用控制台中显示的任意应用程序连接器。 不再支持 Box 连接器。
- 应用程序的说明。
- 使用完全限定的域名 (FQDN) 提供的 Web 地址。 例如，如果要将 LinkedIn 添加到应用程序列表中，应访问 http://www.linkedin.com，然后单击“Sign in”（登录）。 显示登录页面时，使用 Web 地址 https://www.linkedin.com 配置应用程序。
- 应用程序的位置，在 Internet 上或您的内部网络上。
- SSO 的凭据。 用户可以使用应用程序凭据。
- 应用程序的类别。 利用类别可以在 Worx Home 中对应用程序分类。
- 在 XenMobile 中配置的每个应用程序的应用程序策略。
- 适用于所有应用程序的流程审批设置。 指定哪些人员可以审批您要向其分配应用程序的用户的交付组。

如果应用程序仅可进行 SSO，则在配置完前面的设置后，保存这些设置，应用程序将显示在 XenMobile 管理控制台的**应用程序**选项卡中。

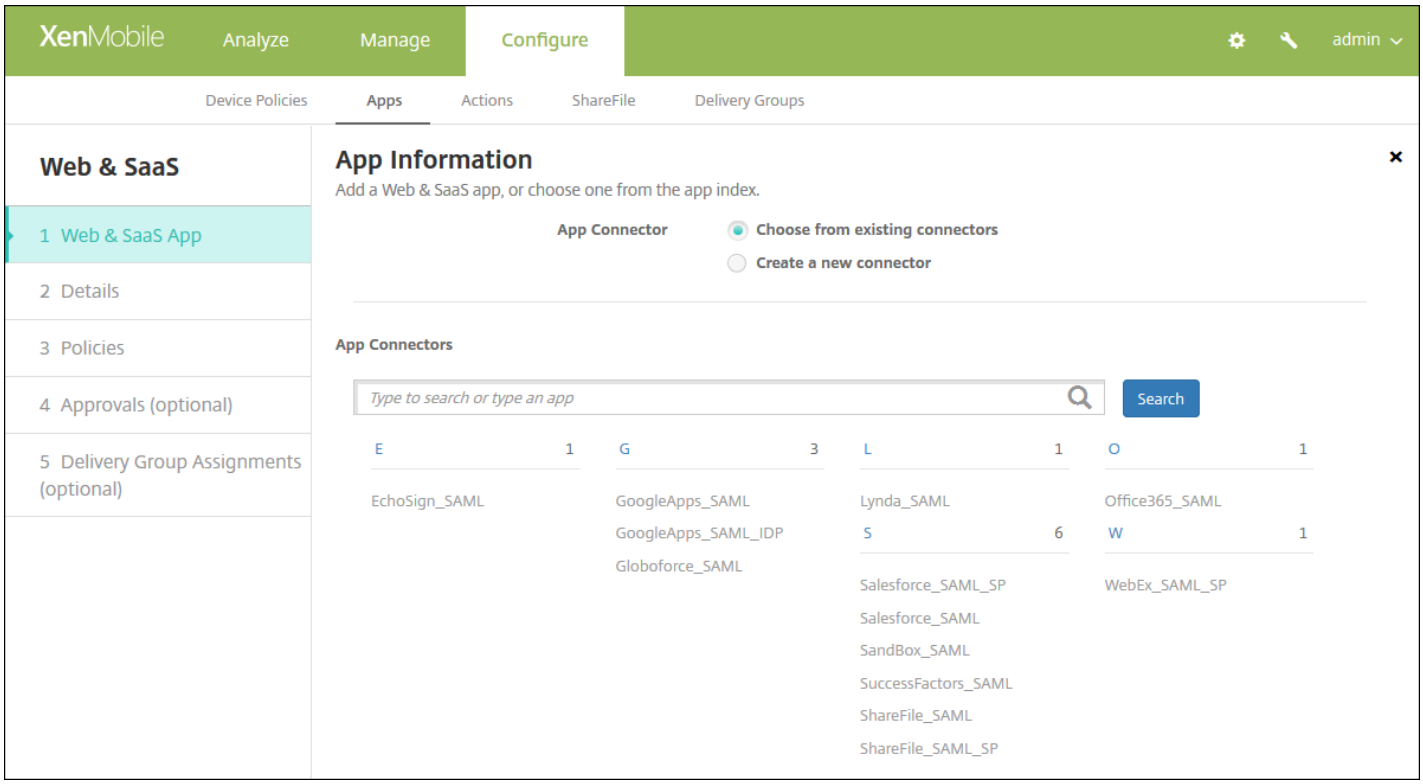
1. 在 XenMobile 控制台中，单击**配置 > 应用程序**。 将打开**应用程序**页面。

2. 单击**添加**。 此时将显示**添加应用程序**对话框。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 单击 **Web 和 SaaS**。 此时将显示**应用程序信息**页面。



4. 配置以下设置：

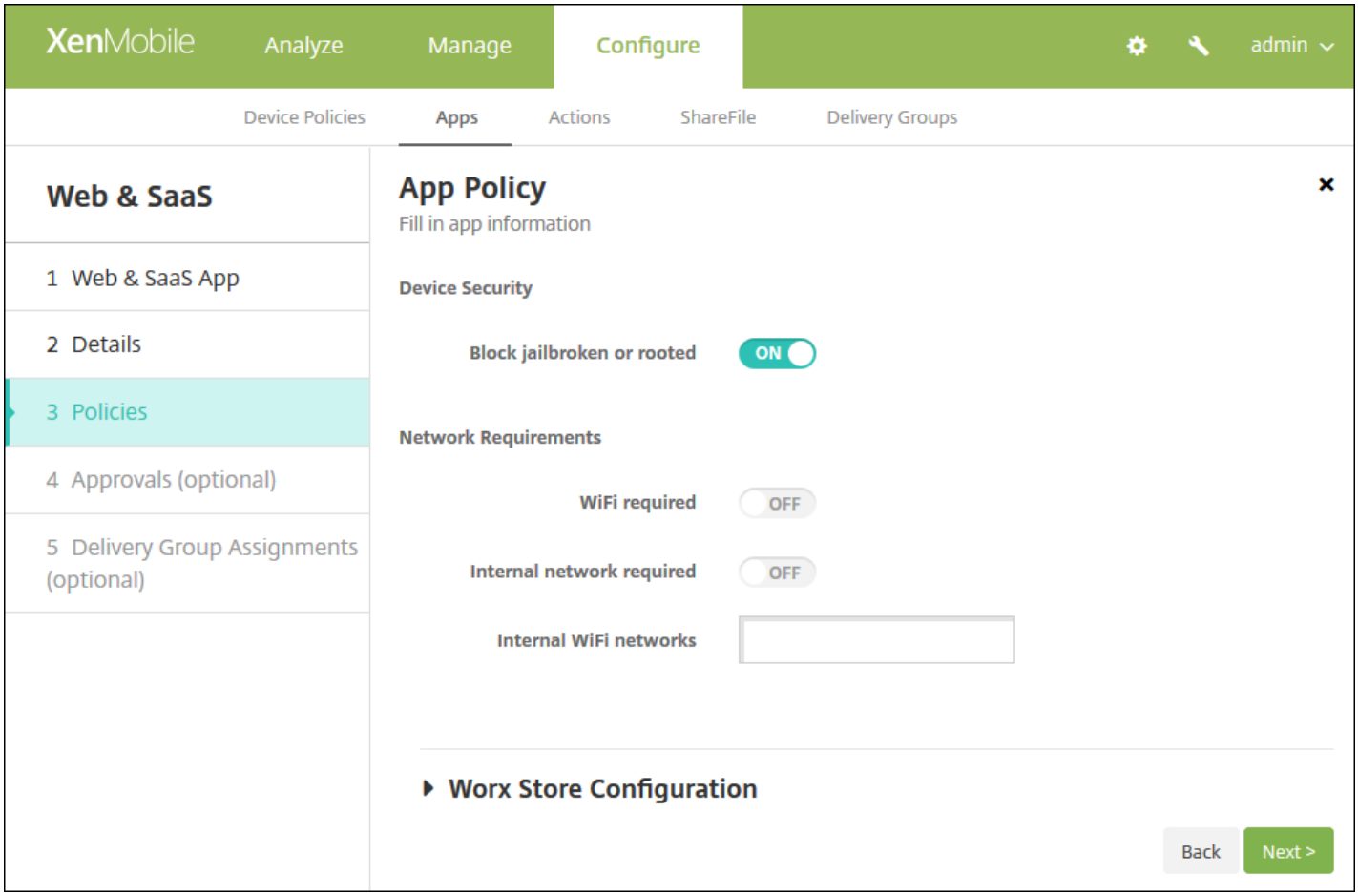
- **应用程序连接器**：单击**从现有连接器中选择**或**创建新连接器**。 默认值为**从现有连接器中选择**。
- 如果单击**创建新连接器**，将显示用于定义新连接器的字段。
  - 配置以下设置：
    - **名称**：键入连接器的名称。 此字段为必填字段。
    - **说明**：键入连接器的说明。 此字段为必填字段。
    - **登录 URL**：键入或复制并粘贴用户登录站点的 URL。 此字段为必填字段。
    - **SAML 版本**：选择 1.1 或 2.0。 默认值为 **1.1**。
    - **实体 ID**：键入 SAML 应用程序的标识。
    - **中继状态 URL**：键入 SAML 应用程序的 Web 地址。 中继状态 URL 是来自应用程序的响应 URL。
    - **名称 ID 格式**：选择“电子邮件地址”或“未指定”。 默认值为**电子邮件地址**。
    - **ACS URL**：键入身份提供商或服务提供商的声明使用者服务 URL。 ACS URL 为用户提供 SSO 功能。
    - **图片**：选择是使用默认 Citrix 图片还是上载自己的应用程序图片。 默认设置为“使用默认值”。
      - 如果希望上载自己的图片，请单击**浏览**并导航到此文件的位置，选择此文件。 此文件必须为 .PNG 文件；无法上载 JPEG 或 GIF 文件。 如果添加自定义图形，以后将无法进行更改。
  - 单击**添加**。 此时将显示**详细信息**页面。
- 如果单击**从现有连接器中选择**或在设置新连接器后单击**添加**，将显示**详细信息**页面。
- 配置以下设置：
  - **应用程序名称**：接受预先填充的名称或键入新名称。
  - **应用程序说明**：接受预先填充的说明或键入自己的说明。
  - **URL**：接受预先填充的 URL 或键入应用程序的 Web 地址。 根据您选择的连接器，此字段可能包含占位符，您必须替换占位符才能继续到下一个页面。
  - **域名**：如果适用，键入应用程序的域名。 此字段为必填字段。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **应用程序托管在内部网络中**：选择应用程序是否在内部网络中的服务器上运行。 如果用户从远程位置连接到内部应用程序，则必须通过 NetScaler Gateway 进行连接。 将此选项设置为**开**将向应用程序添加 VPN 关键字，并允许用户通过 NetScaler Gateway 连接。 默认值为**关**。
- **应用程序类别**：在此列表中，单击可选类别以应用到应用程序。
- **用户帐户置备**：选择是否为应用程序创建用户帐户。 如果使用 Globoforce_SAML 连接器，必须启用此选项以确保无缝 SSO 集成。
- 如果启用**用户帐户置备**，请配置以下设置：
  - **服务帐户**
    - **用户名**：键入应用程序管理员的名称。 此字段为必填字段。
    - **密码**：键入应用程序管理员的密码。 此字段为必填字段。
  - **用户帐户**
    - **用户授权结束时**：在列表中，单击不再允许用户访问应用程序时采取的操作。 默认设置为**禁用帐户**。 可用选项包括：
      - 禁用帐户
      - 保留帐户
      - 删除帐户
  - **用户名规则**
    - 对于要添加的每项用户名规则，请执行以下操作：
      - **用户属性**：在列表中，单击要添加到规则中的用户属性。
      - **长度(字符数)**：在列表中，单击用户属性要用于用户名规则中的字符数。 默认值为**全部**。
      - **规则**：您添加的每个用户属性自动附加到用户名规则中。
- **密码要求**
  - **长度**：键入最低用户密码长度。 默认值为 **8**。
- **密码过期时间**
  - **有效期(天)**：键入密码有效的天数。 有效值为 0 – 90。 默认值为 **90**。
  - **过期后自动重置密码**：选择是否在密码过期时自动重置密码。 默认值为**关**。 如果不启用此字段，用户的密码过期时，用户将无法打开应用程序。

5. 单击**下一步**。 将显示**应用程序策略**页面。

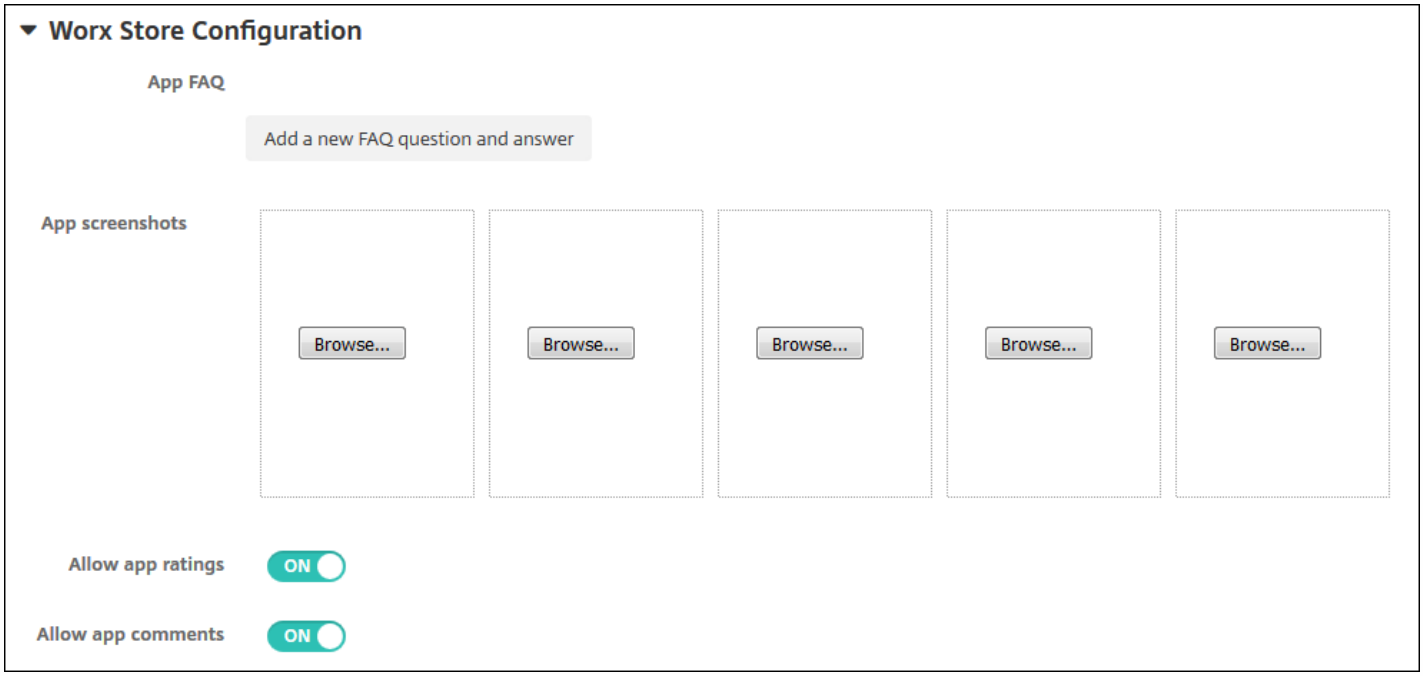
© 1999-2017 Citrix Systems, Inc. All rights reserved.



- 配置以下设置：
  - **设备安全**
    - **阻止越狱或获得 Root 权限**：选择是否阻止越狱或获得 Root 权限的设备访问应用程序。 默认值为**开**。
  - **网络要求**
    - **需要连接 WiFi**：选择运行应用程序是否需要使用 WiFi 连接。 默认值为**关**。
    - **需要连接内部网络**：选择运行应用程序是否需要使用内部网络。 默认值为**关**。
    - **内部 WiFi 网络**：如果启用**需要连接 WiFi**，请键入要使用的内部 WiFi 网络。

6. 展开 **Worx Store 配置**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

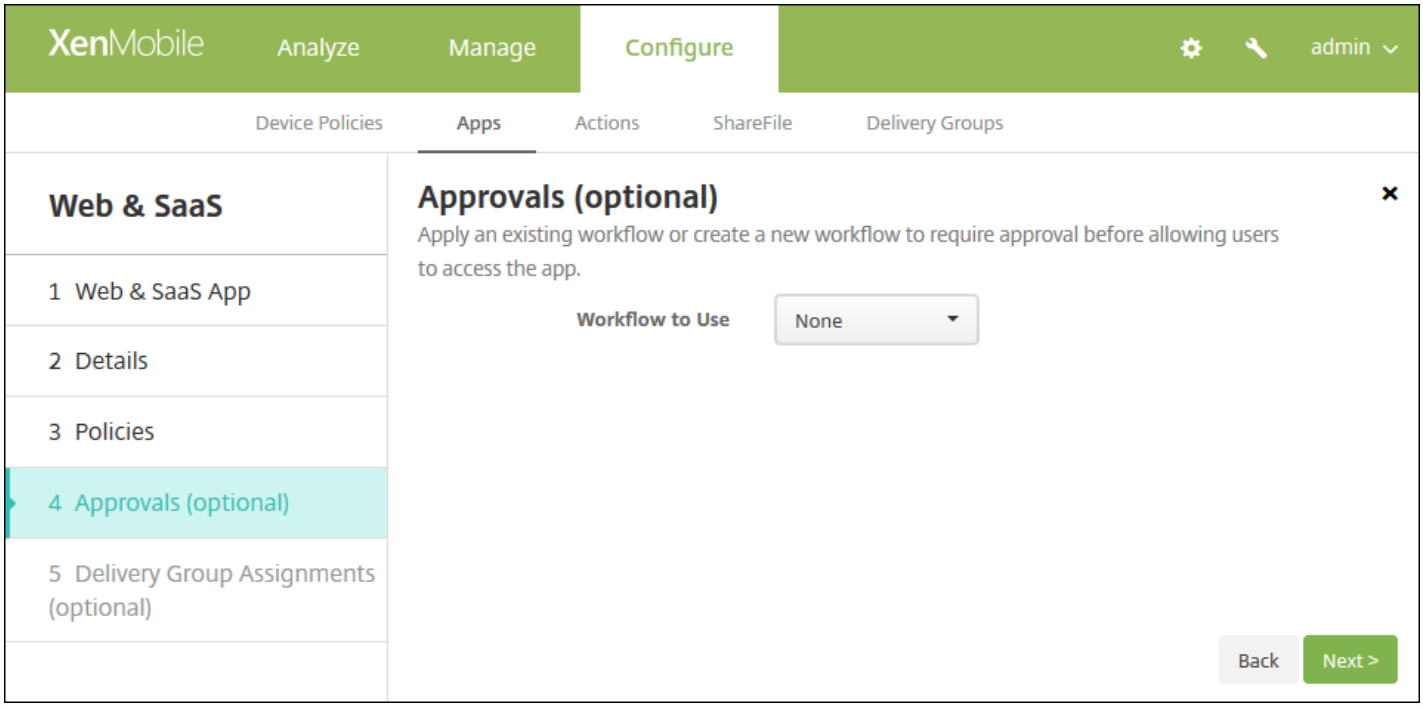


（可选）可以添加应用程序的常见问题解答或显示在 Worx Store 中的屏幕截图。 还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - **应用程序常见问题解答**：添加应用程序的常见问题和答案。
  - **应用程序屏幕截图**：添加屏幕截图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形必须为 PNG 格式。 不能上载 GIF 或 JPEG 图形。
  - 在**允许对应用程序评分**中，选择是否允许用户对应用程序进行评分。 默认值为**开**。
  - 在**允许评价应用程序**中，选择是否允许用户评价选定的应用程序。 默认值为**开**。

7. 单击**下一步**。 此时将显示**审批**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



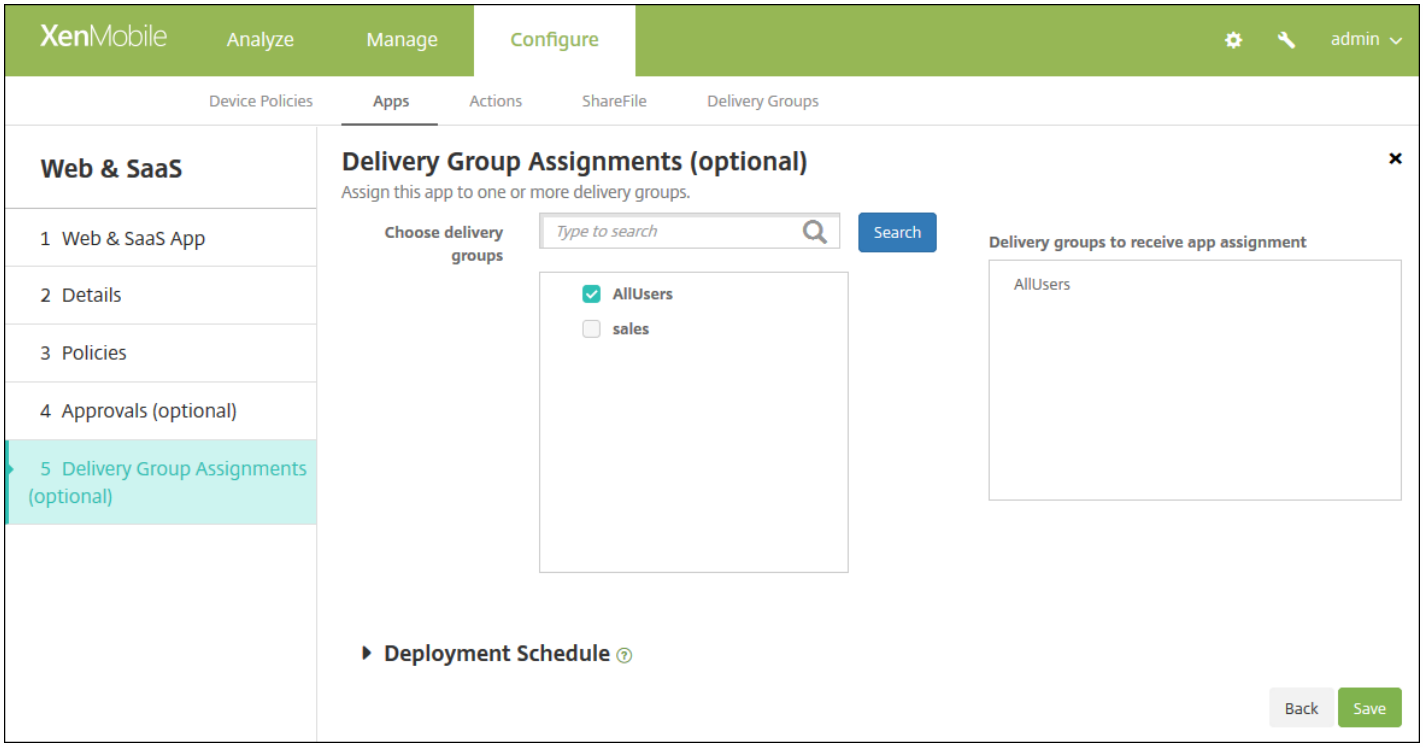
创建用户帐户时如果需要审批则使用流程。 如果无需设置审批流程，可以跳至第 8 步。

如果需要指定或创建流程，请配置此设置：

- **要使用的流程**：在此列表中，单击现有流程或单击**创建新流程**。 默认值为**无**。
- 如果选择**创建新流程**，请配置以下设置：
  - **名称**：键入流程的唯一名称。
  - **说明**：可选，键入流程的说明。
  - **电子邮件审批模板**：在列表中，选择要指定的电子邮件审批模板。 单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
  - **经理审批级别**：在列表中，选择此流程所需的经理审批级别数。 默认值为 **1 级**。 可用选项包括：
    - 不需要
    - 1 级
    - 2 级
    - 3 级
  - **选择 Active Directory 域**：在列表中，选择用于流程的合适的 Active Directory 域。
  - **查找所需的其他审批者**：在搜索字段中键入其他必需人员的姓名，然后单击**搜索**。 源于 Active Directory 的姓名。
  - 人员的姓名显示在此字段中后，选中其姓名旁边的复选框。 人员的姓名和电子邮件地址显示在**选定的其他所需审批者**列表中。
    - 要从**选定的其他所需审批者**列表中删除人员，请执行以下操作：
      - 单击**搜索**以查找选定域中的所有人员列表。
      - 在搜索框中键入完整名称或部分名称，然后单击**搜索**以限制搜索结果。
      - 在搜索结果列表中，**选定的其他所需审批者**列表中的人员姓名旁边有一个复选标记。 滚动列表，并取消选中要删除的各个姓名旁边的复选框。

8. 单击**下一步**。 此时将显示**交付组分配**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 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要向其分配应用程序的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序连接器类型列表

Aug 11, 2016

下表列出了适用于 XenMobile 的连接器及连接器类型。 表中还指出各连接器是否支持用户帐户管理。支持用户帐户管理时，您可以自动或通过工作流程创建新的帐户。

连接器名称	SSO SAML	支持用户帐户管理
EchoSign_SAML	是	是
Globoforce_SAML		注意：使用此连接器时，必须启用用户管理功能以进行置备以确保无缝 SSO 集成。
GoogleApps_SAML	是	是
GoogleApps_SAML_IDP	是	是
Lynda_SAML	是	是
Office365_SAML	是	是
Salesforce_SAML	是	是
Salesforce_SAML_SP	是	是
SandBox_SAML	是	
SuccessFactors_SAML	是	
ShareFile_SAML	是	
ShareFile_SAML_SP	是	
WebEx_SAML_SP	是	是

© 1999-2017 Citrix Systems, Inc. All rights reserved.

向 XenMobile 中添加企业应用程序

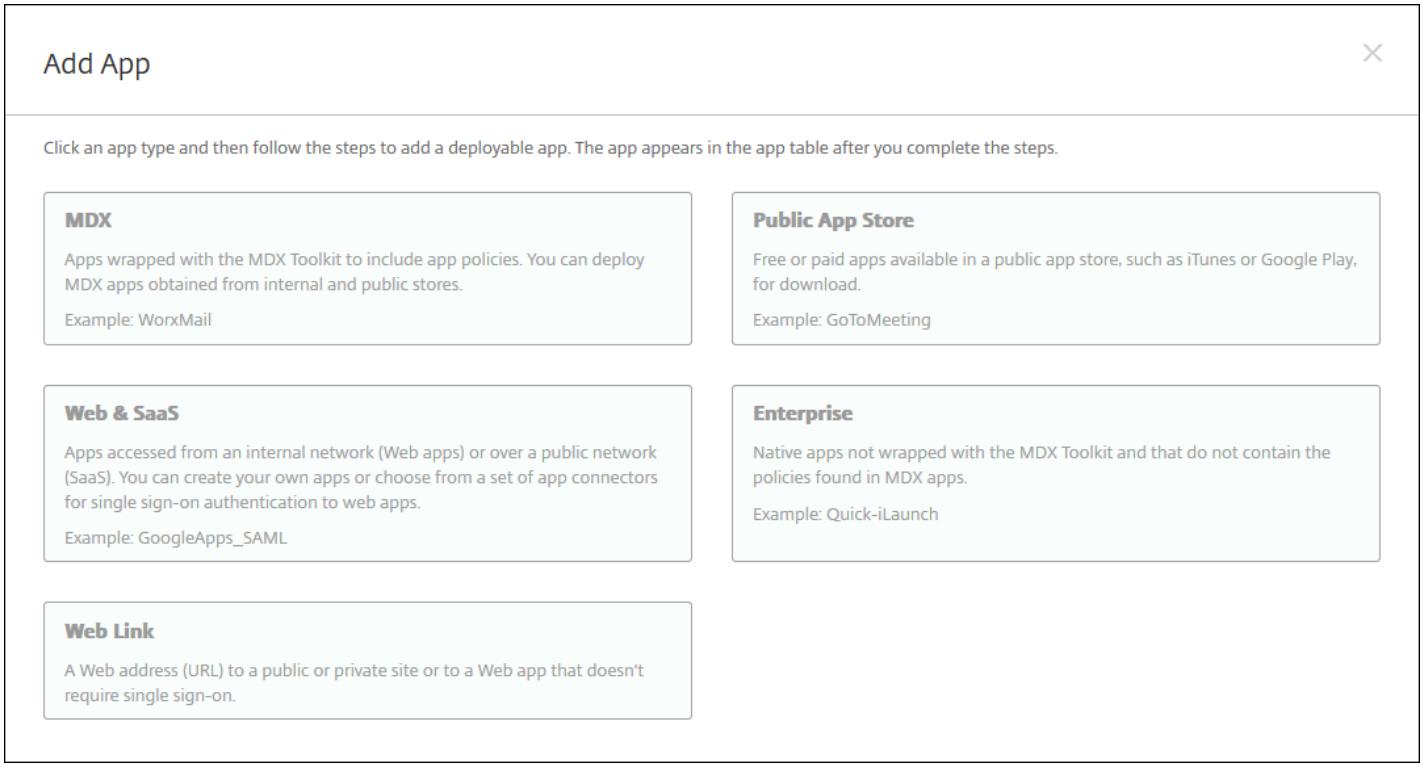
Aug 11, 2016

XenMobile 中的企业应用程序代表未通过 MDX Toolkit 打包的本机应用程序，并且不包含与 MDX 应用程序关联的策略。 可以在 XenMobile 控制台中的**应用程序**选项卡中上载企业应用程序。 企业应用程序支持以下平台（和相应的文件类型）：

- iOS（.ipa 文件）
- Android（.apk 文件）
- Samsung KNOX（.apk 文件）
- Android for Work（.apk 文件）
- Windows Phone（.xap 或 .appx 文件）
- Windows Tablet（.appx 文件）
- Windows Mobile/CE（.cab 文件）

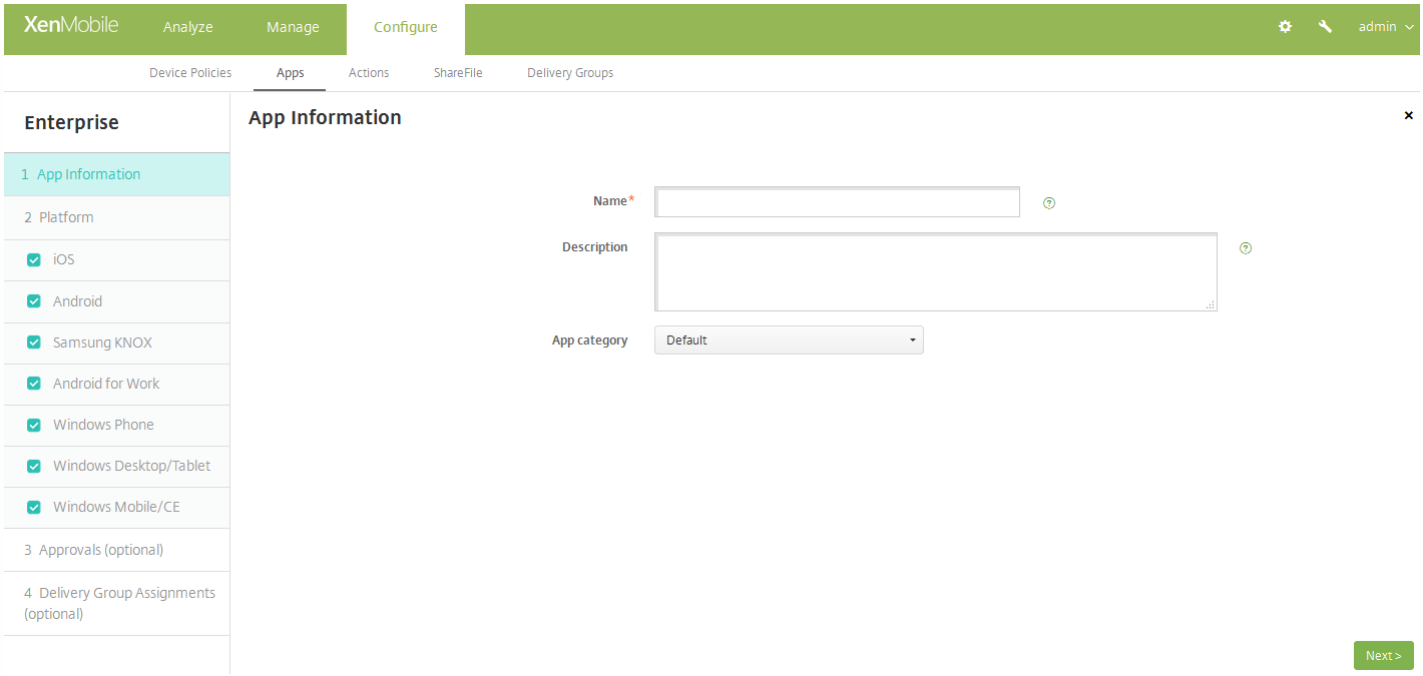
1. 在 XenMobile 控制台中，单击**配置 > 应用程序**。 将打开**应用程序**页面。

2. 单击**添加**。 此时将显示**添加应用程序**对话框。



3. 单击**企业**。 此时将显示**应用程序信息**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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。 此名称将显示在“应用程序”表格上的“应用程序名称”下面。
- **说明**：键入应用程序的可选说明。
- **应用程序类别**：（可选）在列表中，单击要将应用程序添加到的类别。 有关应用程序类别的详细信息，请参阅在 XenMobile 中创建应用程序类别。

5. 单击**下一步**。 此时将显示**应用程序平台**页面。

6. 在**平台**下面，选择要添加的平台。 如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 10 以了解如何设置此平台的部署规则。

7. 对于所选的每个平台，单击**浏览**，然后导航到文件的位置，选择要上载的文件。

8. 单击**下一步**。 此时将显示平台的应用程序信息页面。

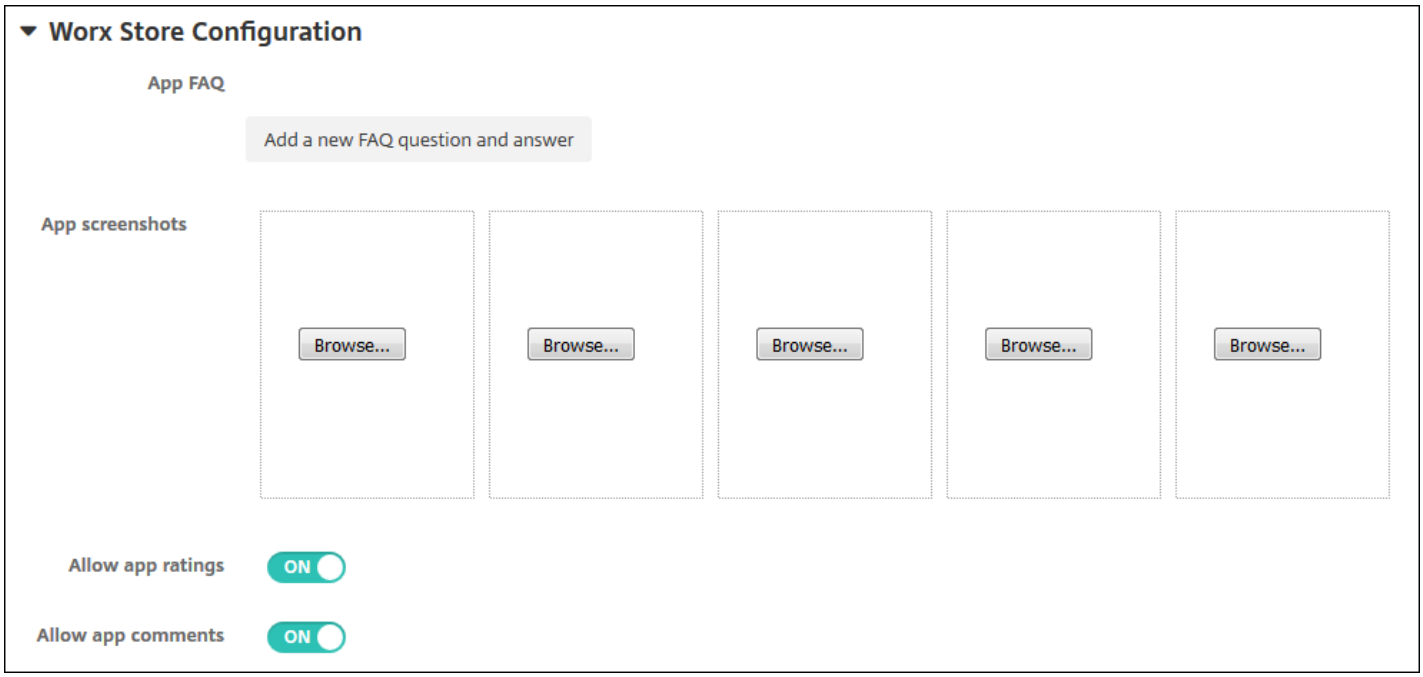
9. 配置此平台类型的设置，如：

- **文件名**：可选，键入应用程序的新名称。
- **应用程序说明**：可选，键入应用程序的新说明。
- **应用程序版本**：无法更改此字段。
- **最低操作系统版本**：
- **最高操作系统版本**：
- **排除的设备**：
- **删除 MDM 配置文件时也删除应用程序**：选择删除 MDM 配置文件时是否从设备删除应用程序。 默认值为**开**。
- **阻止备份应用程序数据**：选择是否阻止应用程序备份数据。 默认值为**开**。
- **强制管理应用程序**：安装未托管应用程序时，如果希望提示未受监督设备上的用户允许应用程序管理，请选择“开”。 如果用户接受提示，应用程序将托管。 此设置适用于 iOS 9.x 设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. 配置部署规则

11. 展开 **Worx Store 配置**。



（可选）可以添加应用程序的常见问题解答或显示在 Worx Store 中的屏幕截图。 还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - **应用程序常见问题解答**：添加应用程序的常见问题和答案。
  - **应用程序屏幕截图**：添加屏幕截图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形必须为 PNG 格式。 不能上载 GIF 或 JPEG 图形。
  - 在**允许对应用程序评分**中，选择是否允许用户对应用程序进行评分。 默认值为**开**。
  - 在**允许评价应用程序**中，选择是否允许用户评价选定的应用程序。 默认值为**开**。

12. 单击**下一步**。 此时将显示**审批**页面。

创建用户帐户时如果需要审批则使用流程。 如果无需设置审批流程，可以跳至第 13 步。

如果需要指定或创建流程，请配置此设置：

- **要使用的流程**：在此列表中，单击现有流程或单击**创建新流程**。 默认值为**无**。
- 如果选择创建新流程，请配置以下设置：
  - **名称**：键入流程的唯一名称。
  - **说明**：可选，键入流程的说明。
  - **电子邮件审批模板**：在列表中，选择要指定的电子邮件审批模板。 单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
  - **经理审批级别**：在列表中，选择此流程所需的经理审批级别数。 默认值为 **1 级**。 可用选项包括：
    - 不需要
    - 1 级
    - 2 级

© 1999-2017 Citrix Systems, Inc. All rights reserved.

    - 3 级
- **选择 Active Directory 域**：在列表中，选择用于流程的合适的 Active Directory 域。
- **查找所需的其他审批者**：在搜索字段中键入其他必需人员的姓名，然后单击**搜索**。 源于 Active Directory 的姓名。
- 人员的姓名显示在此字段中后，选中其姓名旁边的复选框。 人员的姓名和电子邮件地址显示在**选定的其他所需审批者**列表中。
    - 要从**选定的其他所需审批者**列表中删除人员，请执行以下操作：
        - 单击**搜索**以查找选定域中的所有人员列表。
        - 在搜索框中键入完整名称或部分名称，然后单击**搜索**以限制搜索结果。
        - 在搜索结果列表中，**选定的其他所需审批者**列表中的人员姓名旁边有一个复选标记。 滚动列表，并取消选中要删除的各个姓名旁边的复选框。

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要向其分配应用程序的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

15. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击关以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

16. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

向 XenMobile 添加 Web 链接应用程序

Aug 11, 2016

在 XenMobile 中，可以建立公共或专用站点或者无需单点登录 (SSO) 的 Web 应用程序的 Web 地址 (URL)。

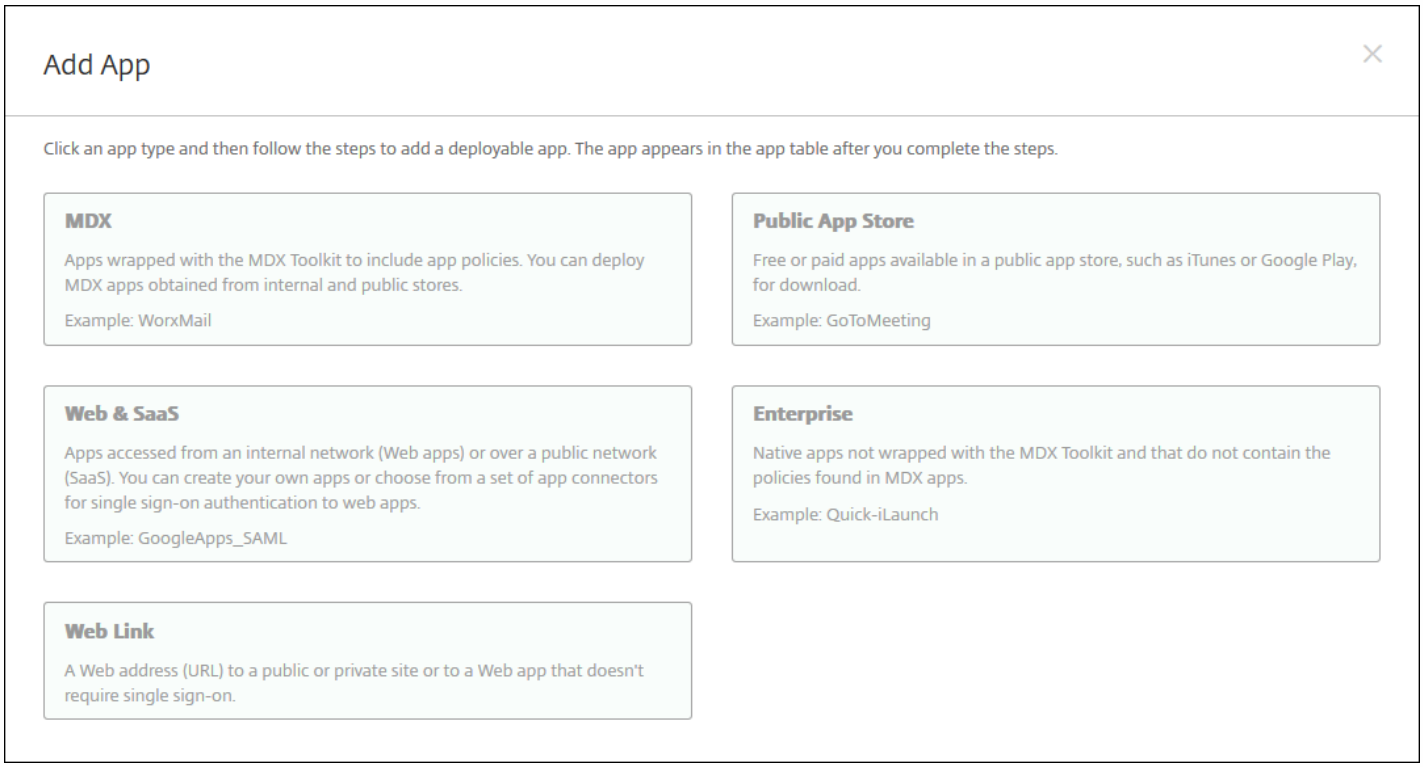
可以从 XenMobile 控制台的**应用程序**选项卡配置 Web 链接。 Web 链接配置完成后，该链接将以链接图标的形式显示在**应用程序**表格中的列表中。 当用户通过 Worx Home 登录时，将显示该链接以及可用应用程序和桌面的列表。

要添加链接，请提供以下信息：

- 链接的名称
- 链接的说明
- Web 地址 (URL)
- 类别
- 角色
- .png 格式的图像（可选）

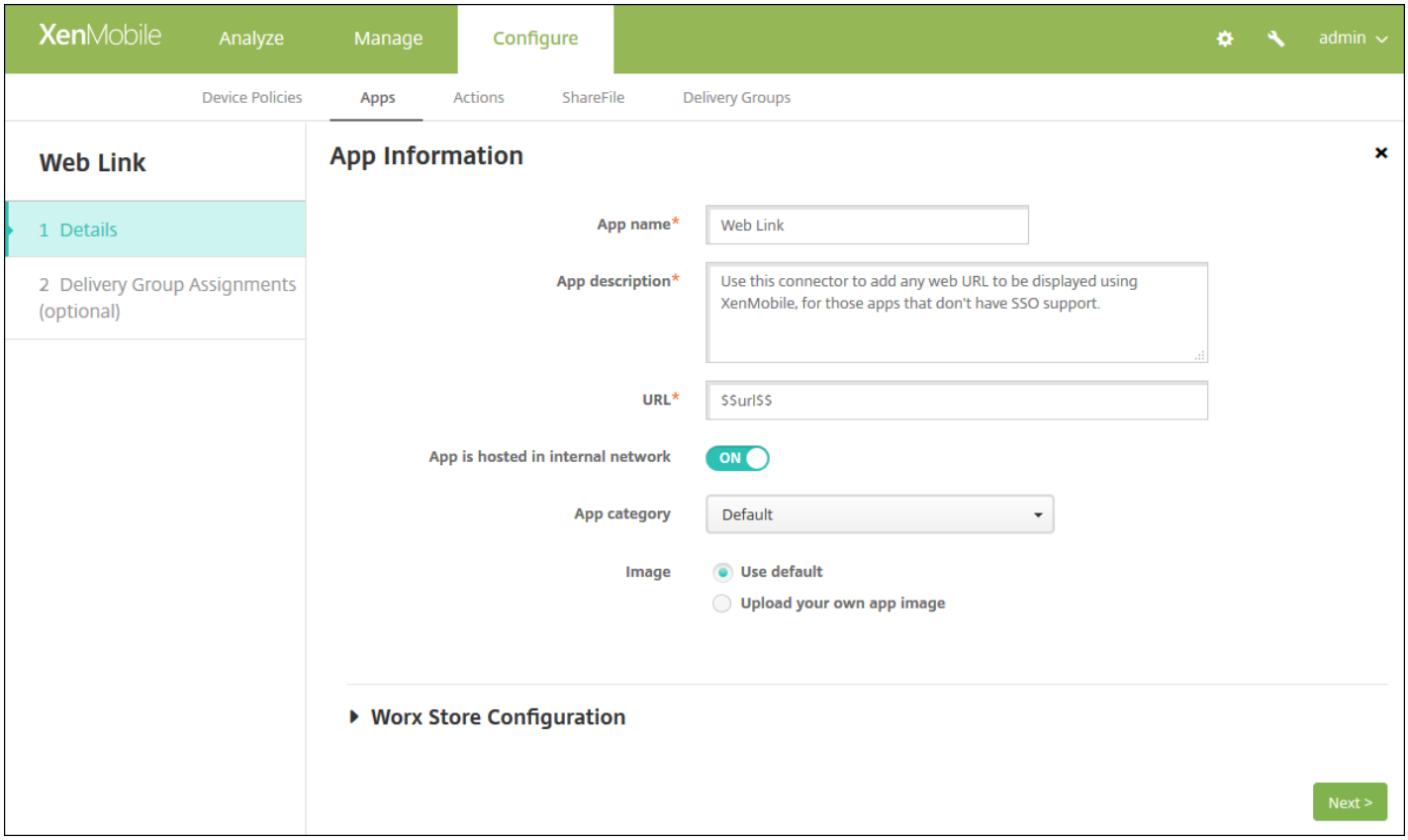
1. 在 XenMobile 控制台中，单击**配置 > 应用程序**。 此时将显示**应用程序**页面。

2. 单击**添加**。 此时将显示**添加应用程序**对话框。



3. 单击 **Web 链接**。 此时将显示**应用程序信息**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

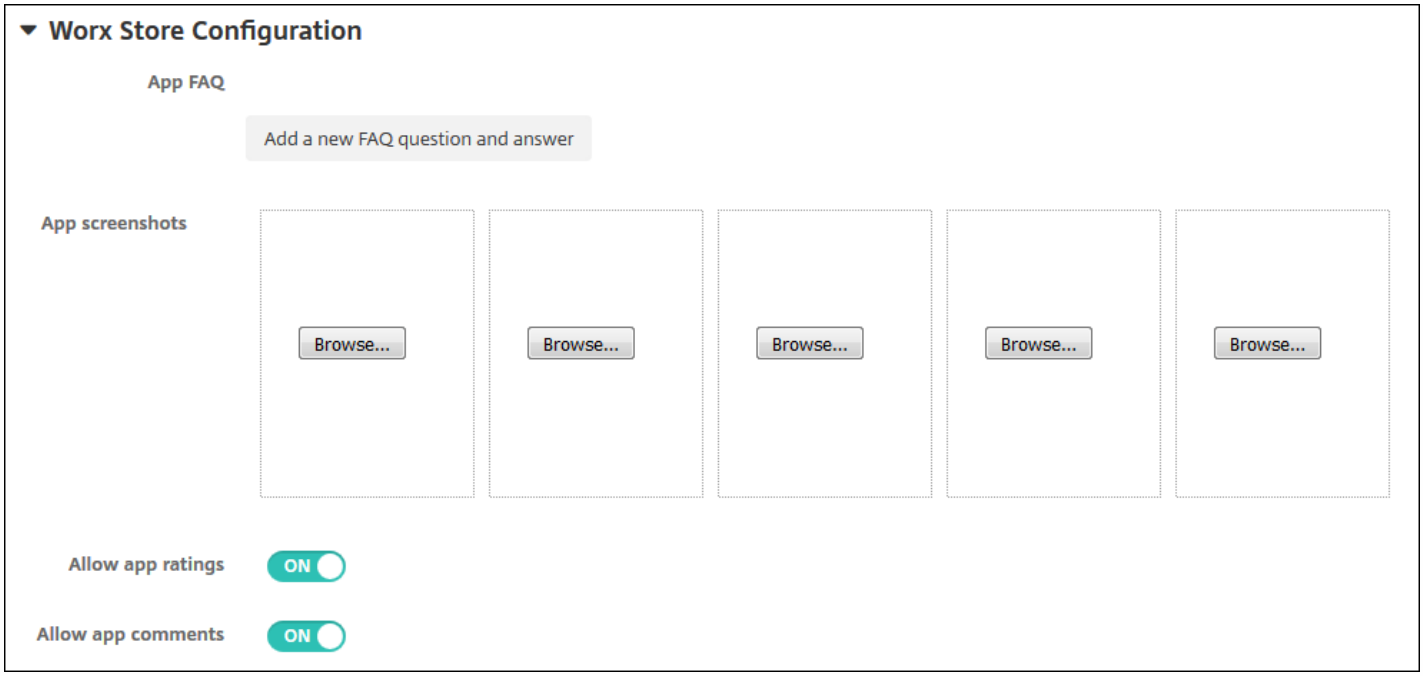


4. 配置以下设置：

- **应用程序名称**：接受预先填充的名称或键入新名称。
- **应用程序说明**：接受预先填充的说明或键入自己的说明。
- **URL**：接受预先填充的 URL 或键入应用程序的 Web 地址。 根据您选择的连接器，此字段可能包含占位符，您必须替换占位符才能继续到下一个页面。
- **应用程序托管在内部网络中**：选择应用程序是否在内部网络中的服务器上运行。 如果用户从远程位置连接到内部应用程序，则必须通过 NetScaler Gateway 进行连接。 将此选项设置为**开**将向应用程序添加 VPN 关键字，并允许用户通过 NetScaler Gateway 连接。 默认值为**关**。
- **应用程序类别**：在此列表中，单击可选类别以应用到应用程序。
- **图片**：选择是使用默认 Citrix 图片还是上载自己的应用程序图片。 默认设置为“使用默认值”。
  - 如果希望上载自己的图片，请单击**浏览**并导航到此文件的位置，选择此文件。 此文件必须为 .PNG 文件；无法上载 JPEG 或 GIF 文件。 如果添加自定义图形，以后将无法进行更改。

5. 展开 **Worx Store 配置**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

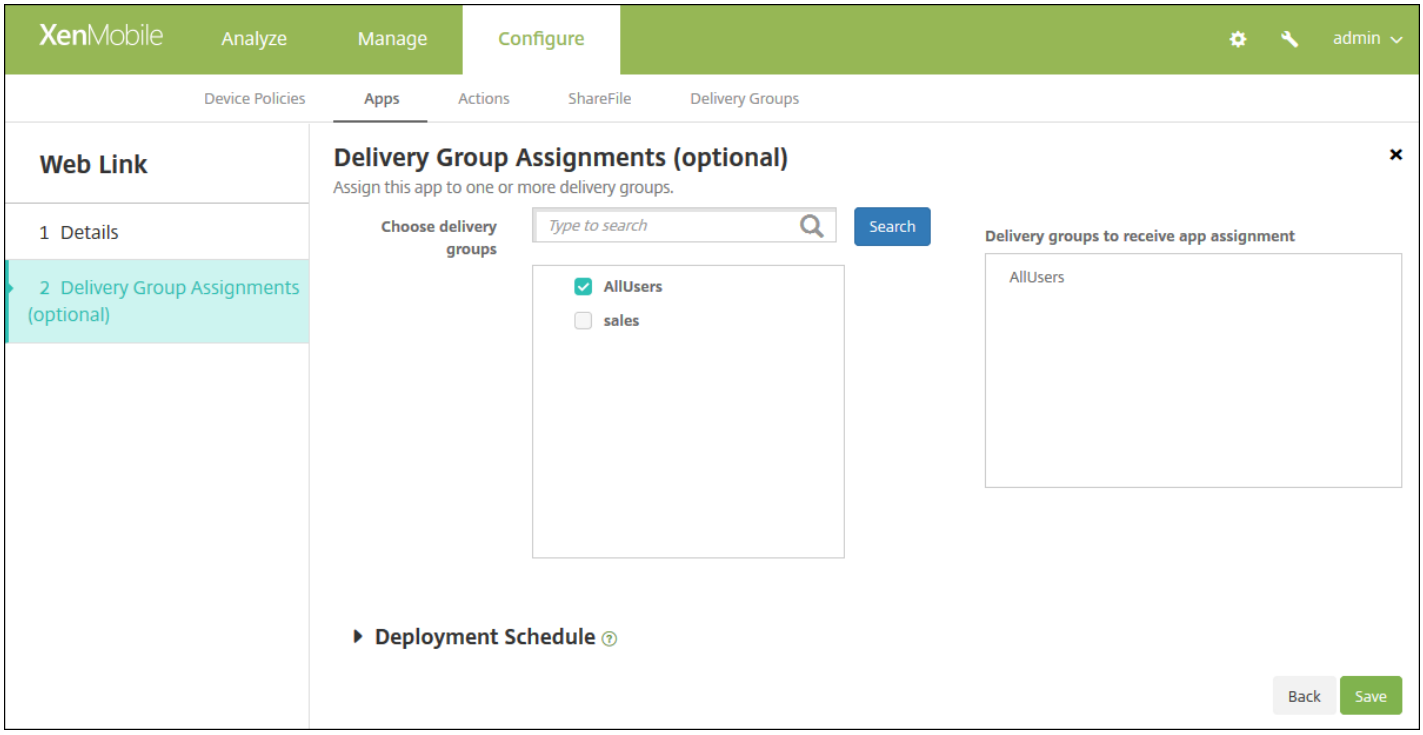


（可选）可以添加应用程序的常见问题解答或显示在 Worx Store 中的屏幕截图。 还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - **应用程序常见问题解答**：添加应用程序的常见问题和答案。
  - **应用程序屏幕截图**：添加屏幕截图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形必须为 PNG 格式。 不能上载 GIF 或 JPEG 图形。
  - 在**允许对应用程序评分**中，选择是否允许用户对应用程序进行评分。 默认值为“开”。
  - 在**允许评价应用程序**中，选择是否允许用户评价选定的应用程序。 默认值为“开”。

6. 单击**下一步**。 此时将显示**交付组分配**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



7. 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要向其分配应用程序的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

8. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

9. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中创建和管理工作流

Oct 21, 2016

可以使用工作流对用户帐户的创建和删除进行管理。 需要先确定组织中有权批准用户帐户请求的人员，然后才能使用工作流。 然后可以使用工作流模板创建和批准用户帐户请求。

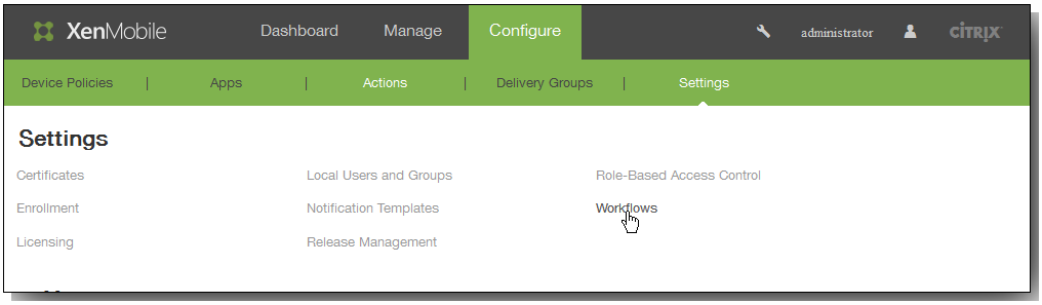
首次配置 XenMobile 时，应配置工作流电子邮件设置。 必须配置工作流电子邮件设置才能使用工作流。 随时可以更改工作流电子邮件设置。 这些设置包括电子邮件服务器、端口、电子邮件地址以及创建用户帐户的请求是否需要进行审批。

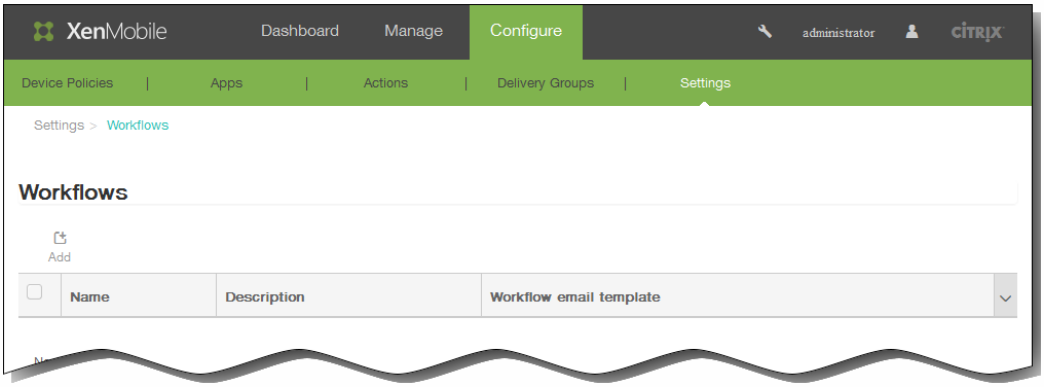
可以在 XenMobile 中的两个位置配置工作流：

- 在 XenMobile 控制台的工作流页面中。 在工作流页面上，可以配置多个用于应用程序配置的工作流。 在工作流页面上配置工作流时，可以在配置应用程序时选择工作流。
- 配置应用程序连接器时，在应用程序中提供工作流名称，然后配置可以审批用户帐户请求的人员。 请参阅向 XenMobile 添加应用程序。

可以为用户帐户分配最多三个管理者审批级别。 如果需要其他人员审批用户帐户，可以使用该人员的姓名或电子邮件地址搜索和选择其他审批者。 XenMobile 找到人员时，您可以将其添加到工作流中。 工作流中的所有人员都将收到电子邮件，以批准或拒绝新用户帐户。

1. 在 XenMobile 控制台中，单击配置 > 设置 > 工作流。

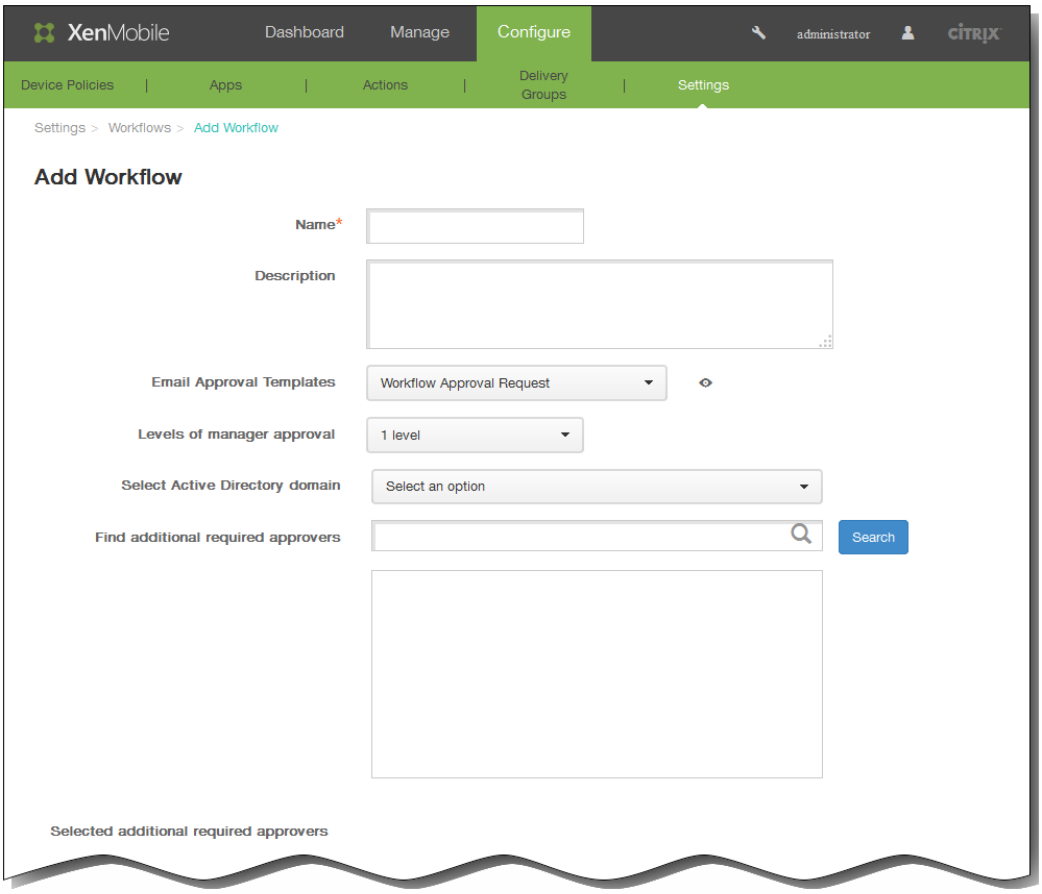




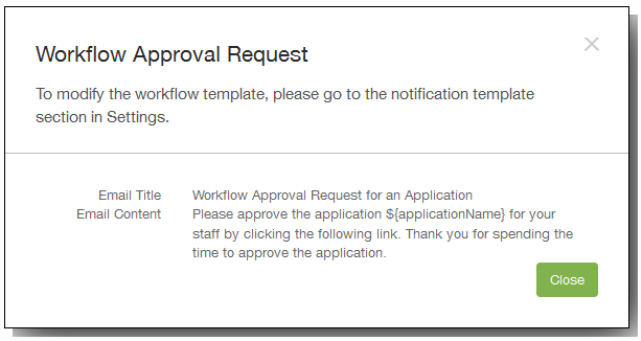
此时将显示工作流页面。

2. 在工作流页面上，单击添加。 此时将显示添加工作流页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 在添加工作流页面的名称字段中，键入工作流的唯一名称。
4. 在说明中，可以选择键入工作流的说明。
5. 在电子邮件审批模板列表中，选择要分配的电子邮件审批模板。 在 XenMobile 控制台设置下的通知模板部分创建电子邮件模板。 单击此字段右边的眼睛图标时，将显示以下提示。



6. 在 Levels of manager approval（管理员审批级别）列表中，选择此工作流所需的管理员审批的级别数。
7. 在选择 Active Directory 域列表中，选择用于工作流的合适 Active Directory 域。
8. 在查找所需的其他审批者旁边，在搜索字段中键入其他必需人员的姓名，然后单击搜索。 源于 Active Directory 的姓名。
9. 人员的姓名显示在此字段中后，选中其姓名旁边的复选框。 人员的姓名和电子邮件地址显示在选定的其他所需审批者列表中。 要从选定的其他所需审批者列表中删除人员，请执行以下操作：
   - 单击搜索以查找选定域中的所有人员列表。
   - 在搜索框中键入完整名称或部分名称，然后单击搜索以限制搜索结果。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。 滚动列表，并取消选中要删除的各个姓名旁边的复选框。

10. 单击 Save（保存）。
    已创建的工作流显示在工作流页面。

    创建工作流后，您可以查看工作流详细信息，查看与工作流相关的应用程序，或者删除工作流。 工作流创建后无法进行编辑。 如果需要使用不同审批级别或审批者的工作流，必须创建新工作流。

1. 在工作流页面的现有工作流列表中，通过单击表格中的行或选中工作流旁边的复选框，选择特定工作流。
2. 要删除工作流，请单击删除。 此时将显示确认对话框。 再次单击删除。
   重要：此操作无法撤消。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中升级 MDX 或企业应用程序

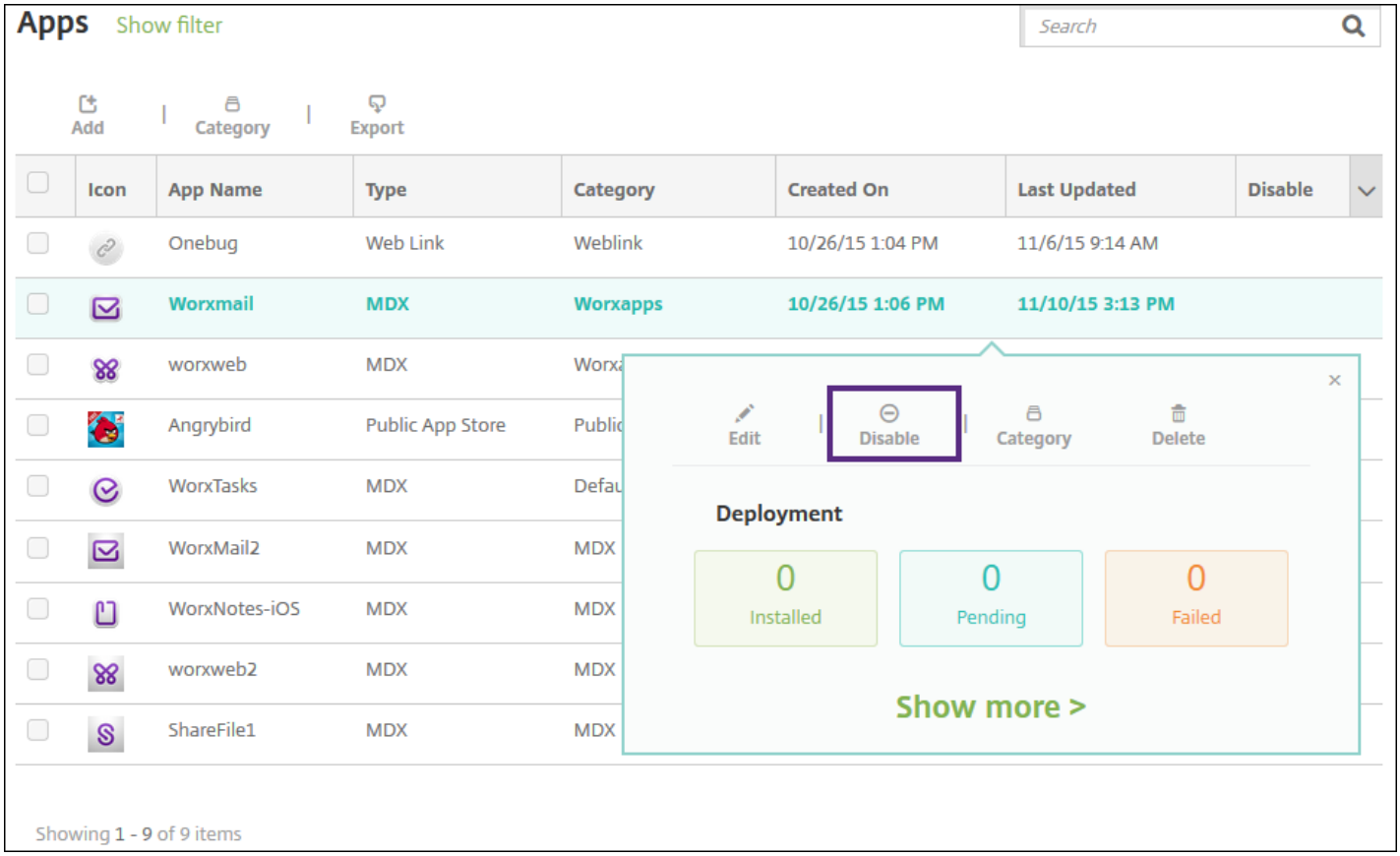
Aug 11, 2016

要在 XenMobile 中升级 MDX 或企业应用程序，您可在 XenMobile 控制台中禁用该应用程序，然后上载该应用程序的新版本。

1. 在 XenMobile 控制台中，单击**配置 > 应用程序**。 此时将显示**应用程序**页面。

2. 对于托管设备（在 XenMobile 中注册用于移动设备管理的设备），跳至步骤 4。 对于未托管设备（在 XenMobile 中注册仅用于企业版应用程序管理目的的设备），请执行以下操作：

- 在**应用程序**表格中，单击应用程序旁边的复选框或单击要更新的应用程序所在的行。
- 在显示的菜单中单击**禁用**。 此时将显示**禁用**对话框。



- 单击对话框中的**禁用**。 *已禁用*显示在应用程序的**禁用**列中。

注意：禁用应用程序会将应用程序置于维护模式。 禁用应用程序期间，用户无法在注销后重新连接到此应用程序。 禁用应用程序是可选设置，但建议禁用应用程序以避免应用程序功能出现问题。 例如，可能会由于策略更新而出现问题，或者如果用户在

© 1999-2017 Citrix Systems, Inc. All rights reserved.

您将应用程序上载到 XenMobile 的同时请求下载，也会出现问题。

4. 在**应用程序**表格中，单击应用程序旁边的复选框或单击要更新的应用程序所在的行。

5. 在显示的菜单中单击**编辑**。 此时将显示**应用程序信息**页面，其中包含最初为所选应用程序选择的平台。

6. 配置以下设置：

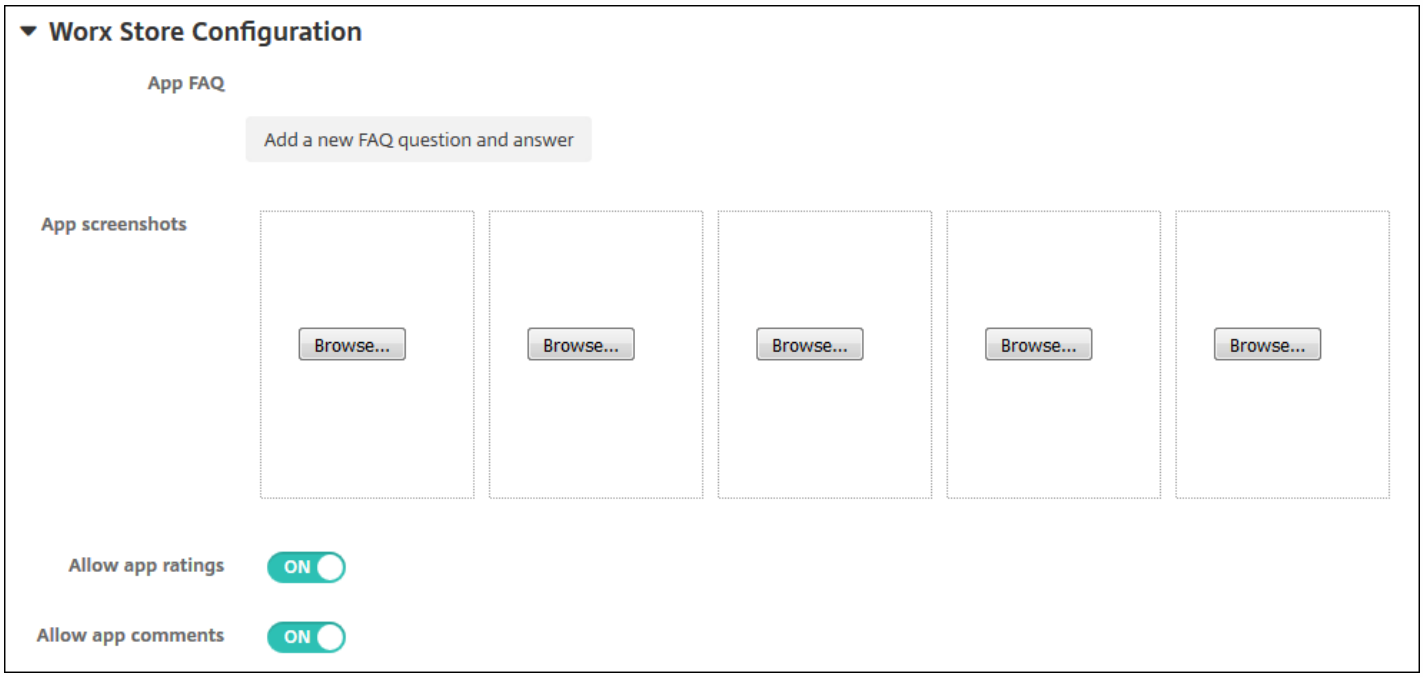
- **名称**：可选，更改应用程序名称。
- **说明**：可选，更改应用程序说明。
- **应用程序类别**：可选，更改应用程序类别。

7. 单击**下一步**。 此时将显示首先选择的平台页面。 请为选择的每个平台执行以下操作：

- 通过单击**上载**并导航到要上载的替换文件的位置，选择此文件。 应用程序即上载到 XenMobile。
- 可选，更改平台的应用程序详细信息和策略设置。
- 可选，配置部署规则（请参阅步骤 7）和 Worx Store 配置（请参阅步骤 8）。

8. 配置部署规则

9. 展开 **Worx Store 配置**。

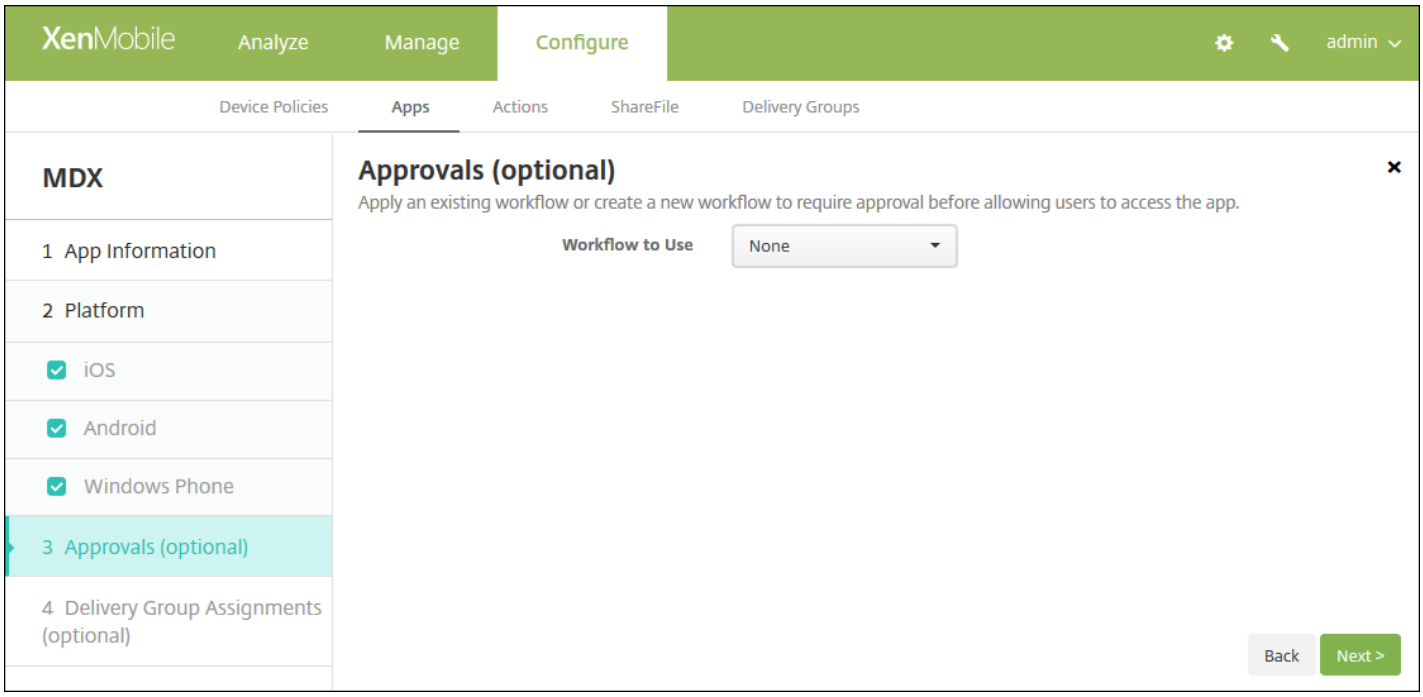


（可选）可以添加应用程序的常见问题解答或显示在 Worx Store 中的屏幕截图。 还可以设置用户是否可以对应用程序进行评分或评价。

- 配置以下设置：
  - **应用程序常见问题解答**：添加应用程序的常见问题和答案。
  - **应用程序屏幕截图**：添加屏幕截图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形必须为 PNG 格式。 不能上载 GIF 或 JPEG 图形。
  - 在**允许对应用程序评分**中，选择是否允许用户对应用程序进行评分。 默认值为**开**。
  - 在**允许评价应用程序**中，选择是否允许用户评价选定的应用程序。 默认值为**开**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. 单击**下一步**。 此时将显示**审批**页面。



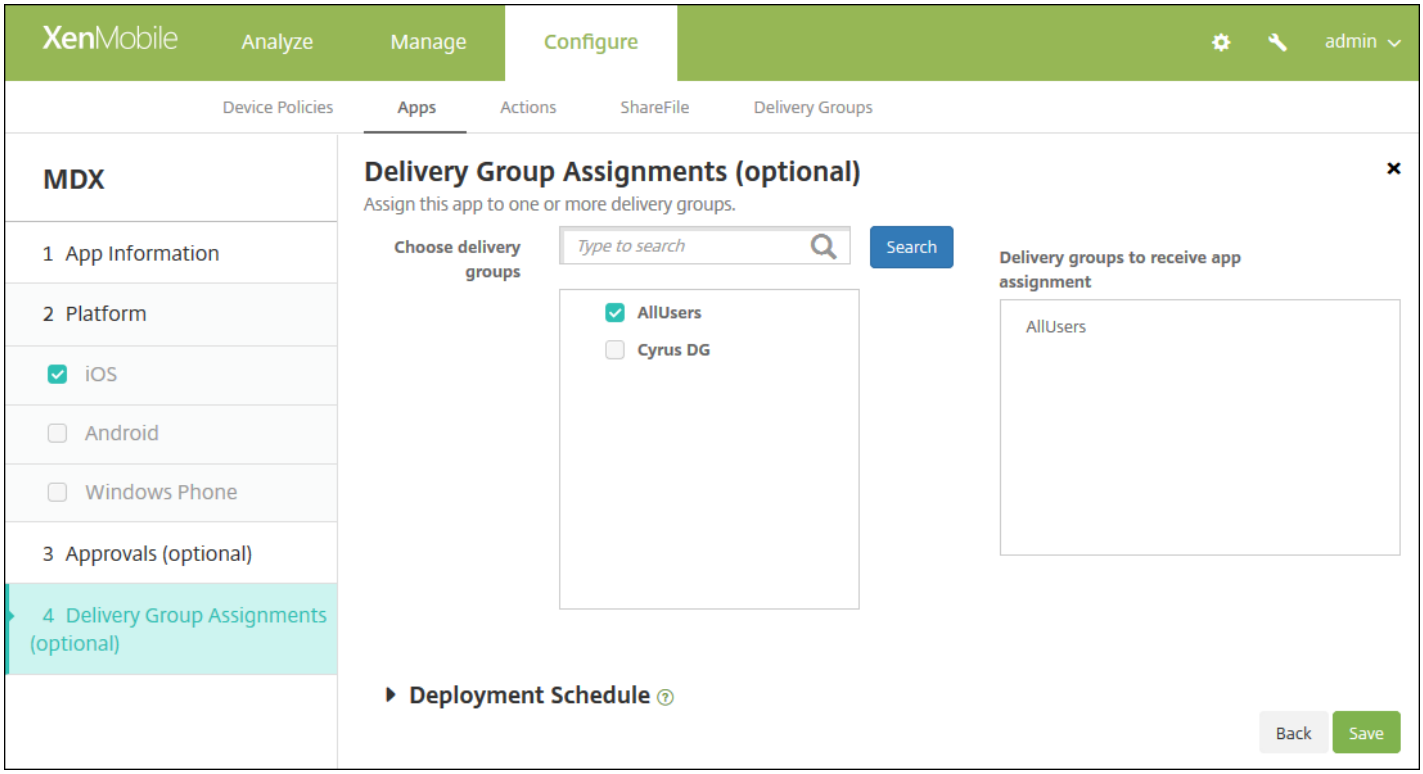
11. 创建用户帐户时如果需要审批则使用流程。 如果无需设置审批流程，可以跳至第 12 步。

如果需要指定或创建流程，请配置此设置：

- **要使用的流程**：在此列表中，单击现有流程或单击**创建新流程**。 默认值为“无”。
- 如果选择**创建新流程**，请配置以下设置：
  - **名称**：键入流程的唯一名称。
  - **说明**：可选，键入流程的说明。
  - **电子邮件审批模板**：在列表中，选择要指定的电子邮件审批模板。 单击此字段右侧的眼睛图标时，将显示一个对话框，您可以在此处预览模板。
  - **经理审批级别**：在列表中，选择此流程所需的经理审批级别数。 默认值为 **1 级**。 可用选项包括：
    - 不需要
    - 1 级
    - 2 级
    - 3 级
  - **选择 Active Directory 域**：在列表中，选择用于流程的合适的 Active Directory 域。
  - **查找所需的其他审批者**：在搜索字段中键入其他必需人员的姓名，然后单击**搜索**。 源于 Active Directory 的姓名。
  - 人员的姓名显示在此字段中后，选中其姓名旁边的复选框。 人员的姓名和电子邮件地址显示在**选定的其他所需审批者**列表中。
  - 要从选定的其他所需审批者列表中删除人员，请执行以下操作：
    - 单击**搜索**以查找选定域中的所有人员列表。
    - 在搜索框中键入完整名称或部分名称，然后单击**搜索**以限制搜索结果。
    - 在搜索结果列表中，**选定的其他所需审批者**列表中的人员姓名旁边有一个复选标记。 滚动列表，并取消选中要删除的各个姓名旁边的复选框。

12. 单击**下一步**。 此时将显示**交付组分配**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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要向其分配应用程序的交付组。 选择的组显示在**用于接收应用程序分配的交付组**列表中。

14. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在为始终启用的连接部署旁边，单击开或关。 默认选项为关。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

15. 单击**保存**。 此时将显示**应用程序**页面。

16. 如果在步骤 2 中已禁用该应用程序，请执行以下操作：

- 在**应用程序**表中，通过单击选择已更新的应用程序，然后在显示的菜单中单击**启用**。
- 在显示的确认对话框中，单击**启用**。 用户现在可以访问该应用程序并接收提示用户升级应用程序的通知。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

启用 Microsoft Office 365 应用程序

Aug 15, 2016

可以打开 MDX 容器以允许 WorxMail、WorxWeb 和 ShareFile 向 Microsoft Office 365 应用程序传输文档和数据。 有关详细信息，请参阅启用 Office 365 与 WorxMail、WorxWeb 和 ShareFile 的交互。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

MDX 应用程序策略概览

Aug 11, 2016

有关列出适用于 iOS、Android 和 Windows Phone 以及有关限制和 Citrix 建议的备注的表格，请参阅 MDX Toolkit 文档中的 MDX 应用程序策略概览。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

将 XenMobile 和 ShareFile 应用程序配置为使用 SAML 进行单点登录

Oct 21, 2016

可以将 XenMobile 和 ShareFile 配置为使用安全声明标记语言 (Security Assertion Markup Language, SAML) 提供对通过 MDX Toolkit 打包的 ShareFile 移动应用程序以及未打包的 ShareFile 客户端（例如 Web 站点、Outlook 插件或同步客户端）的单点登录 (SSO) 访问。

- **面向打包的 ShareFile 应用程序**。 通过 ShareFile 移动应用程序登录 ShareFile 的用户将被重定向到 Worx Home 进行用户身份验证以及获取 SAML 令牌。 成功进行身份验证后，ShareFile 移动应用程序会将 SAML 令牌发送到 ShareFile。 初始登录后，用户可以通过 SSO 访问 ShareFile 移动应用程序，并且可以将 ShareFile 中的文档附加到 WorxMail 电子邮件，而不需要每次都登录。
- **面向未打包的 ShareFile 客户端**。 使用 Web 浏览器或其他 ShareFile 客户端登录 ShareFile 的用户将被重定向到 XenMobile 进行用户身份验证以及获取 SAML 令牌。 成功进行身份验证后，SAML 令牌将被发送到 ShareFile。 初始登录后，用户可以通过 SSO 访问 ShareFile 客户端，而不需要每次都登录。

有关详细的参考体系结构图，请参阅《XenMobile 部署手册》文章适用于本地部署的参考体系结构。

必须先完成以下必备条件，才能对 XenMobile 和 ShareFile 应用程序配置 SSO：

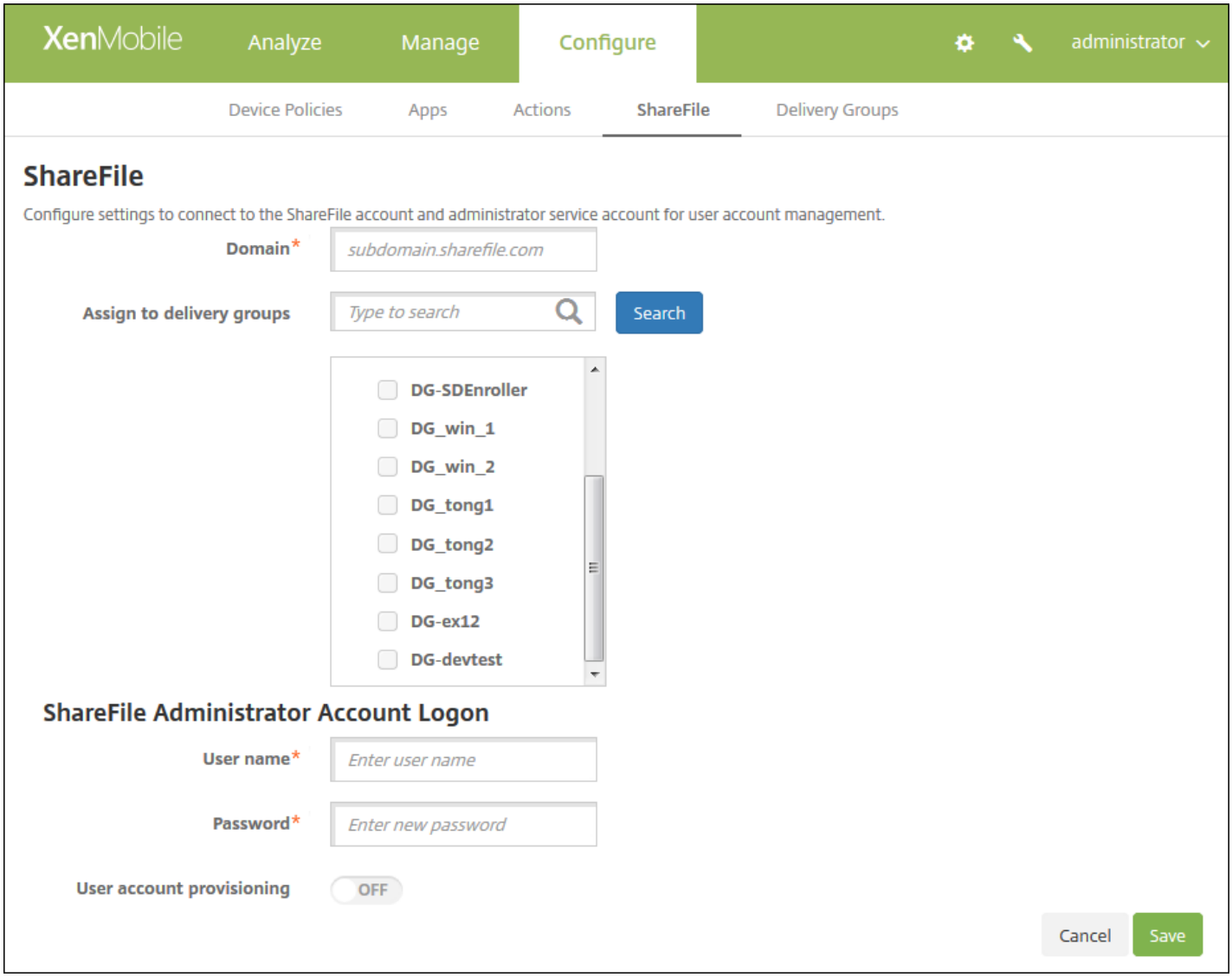
- MDX Toolkit 9.0.4 或更高版本（适用于 ShareFile 移动应用程序）
- 恰当的 ShareFile 移动应用程序：
  - ShareFile for iPhone 3.0.x
  - ShareFile for iPad 2.2.x
  - ShareFile for Android 3.2.x
- Worx Home 9.0（适用于 ShareFile 移动应用程序）- 安装合适的 iOS 或 Android 版本。
- ShareFile 管理员帐户

确保 XenMobile 和 ShareFile 能够连接。

为 ShareFile 设置 SAML 之前，请按如下所示提供 ShareFile 访问信息：

1. 在 XenMobile Web 控制台中，单击**配置 > ShareFile**。 此时将显示 **ShareFile** 配置页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 配置以下设置：

- **域**：键入 ShareFile 子域的名称，例如 example.sharefile.com。
- **分配给交付组**：选择或搜索希望能够对 ShareFile 使用 SSO 的交付组。
- **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 管理员的密码。
  - **用户帐户置备**：如果要在 XenMobile 中启用用户置备，请打开此选项；如果要使用 ShareFile 用户管理工具置备用户，请将其保留在禁用状态。

    注意：如果选定的角色中包含没有 ShareFile 帐户的用户，XenMobile 会自动为该用户置备一个 ShareFile 帐户，前提是您启用了“用户帐户置备”。 Citrix 建议您使用具有小型成员关系的角色以测试配置。 这样可以避免出现大量没有 ShareFile 帐户的用户的可能性。

3. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

以下步骤适用于 iOS 和 Android 应用程序和设备。

1. 使用 MDX Toolkit 打包 ShareFile 移动应用程序。 有关使用 MDX Toolkit 打包应用程序的详细信息，请参阅使用 MDX Toolkit 打包应用程序。

2. 在 XenMobile 控制台中，上载打包的 ShareFile 移动应用程序。 有关上载 MDX 应用程序的信息，请参阅向 XenMobile 中添加 MDX 应用程序。

3. 使用在配置 ShareFile 访问中配置的管理员用户名和密码登录 ShareFile，验证 SAML 设置。

4. 确认为 ShareFile 和 XenMobile 配置相同的时区。

注意：确保 XenMobile 显示所配置时区对应的正确时间。 如果时间不正确，SSO 可能会失败。

验证 ShareFile 移动应用程序

1. 在用户设备上，如果尚未安装和配置 Worx Home，请进行安装和配置。

2. 从 Worx Store 下载并安装 ShareFile 移动应用程序。

3. 启动 ShareFile 移动应用程序。 ShareFile 将启动，但不提示输入用户名或密码。

使用 WorxMail 进行验证

1. 在用户设备上，如果尚未安装和配置 Worx Home，请进行安装和配置。

2. 从 Worx Store 下载、安装并设置 WorxMail。

3. 打开新的电子邮件窗体，然后轻按**从 ShareFile 附加**。 此时将显示可以附加到电子邮件中的文件，但不提示输入用户名或密码。

如果要配置对未打包的 ShareFile 客户端（例如 Web 站点、Outlook 插件或同步客户端）的访问，必须将 NetScaler Gateway 配置为支持使用 XenMobile 作为 SAML 身份提供程序，如下所示：

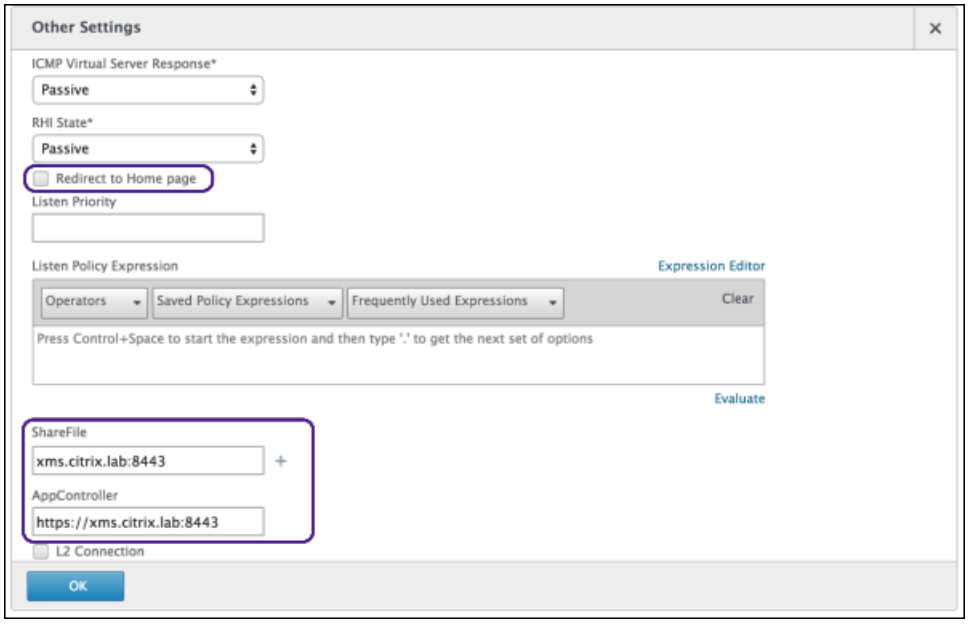
- 禁用主页重定向。
- 创建 ShareFile 会话策略和配置文件。
- 在 NetScaler Gateway 虚拟服务器上配置策略。

禁用主页重定向

必须禁用通过 /cginfra 路径发出的请求的默认行为，以便用户能够看到最初请求的内部 URL，而非配置的主页。

1. 编辑用于 XenMobile 登录的 NetScaler Gateway 虚拟服务器的设置。 在 NetScaler 10.5 中，转至 **Other Settings**（其他设置），然后取消选中标记了 **Redirect to Home Page**（重定向到主页）的复选框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 在 **ShareFile** 下，键入 XenMobile 内部服务器的名称和端口号。

3. 在 **AppController** 下，键入 XenMobile URL。

此配置授权您向通过 /cginfra 路径输入的 URL 发送请求。

创建 ShareFile 会话策略并请求配置文件

请配置以下设置以创建 ShareFile 会话策略并请求配置文件：

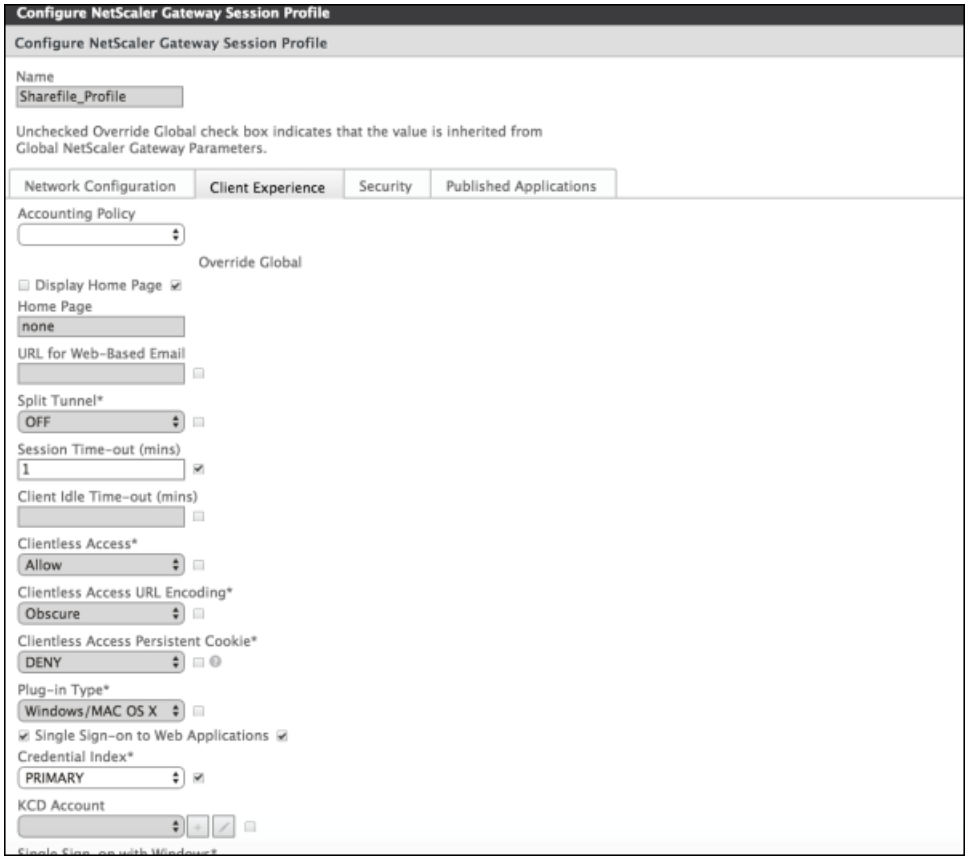
1. 在 NetScaler Gateway 配置实用程序中，在左侧导航窗格中单击 **NetScaler Gateway > Policies（策略）> Session（会话）**。

2. 创建一个新会话策略。 在 **Policies**（策略）选项卡上，单击 **Add**（添加）。

3. 在 **Name**（名称）字段中，键入 **ShareFile_Policy**。

4. 单击 **+** 按钮创建一项新操作。 此时将显示 **Create NetScaler Gateway Session Profile**（创建 NetScaler Gateway 会话配置文件）页面。

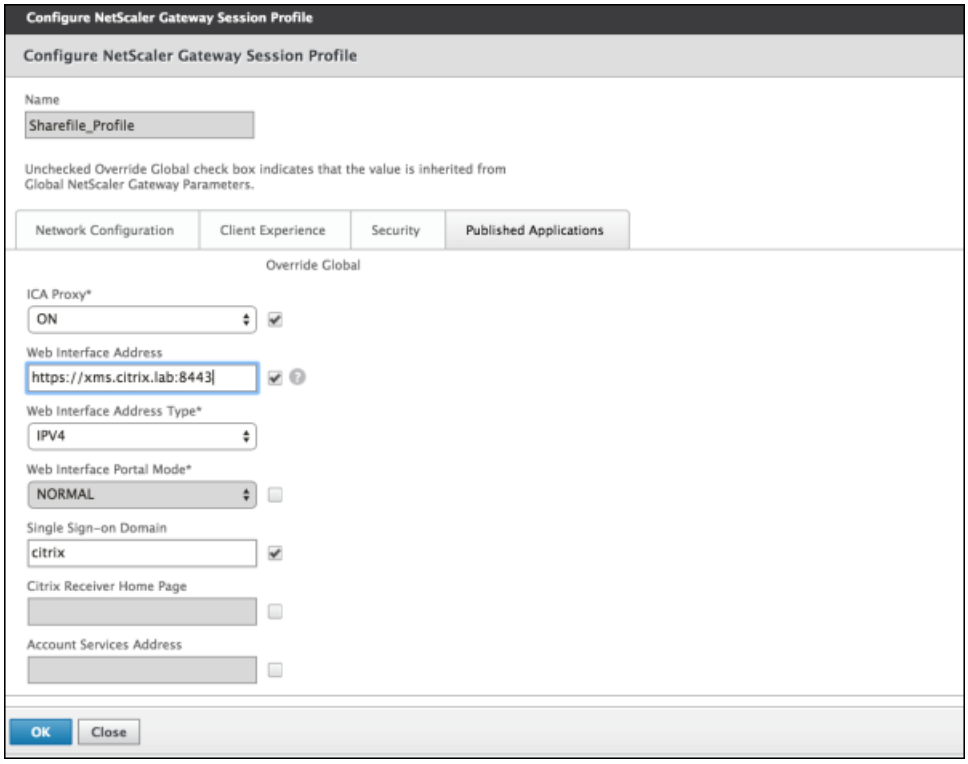
© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **Name**（名称）：键入 ShareFile_Profile。
- 单击 **Client Experience**（客户端体验）选项卡，然后配置以下设置：
  - **Home Page**（主页）：键入“none”（无）。
  - **Session Time-out (mins)**（会话超时(分钟)）：键入 1。
  - **Single Sign-on to Web Applications**（单点登录到 Web 应用程序）：选择此设置。
  - **Credential Index**（凭据索引）：在列表中，单击“PRIMARY”（主要）。
- 单击 **Published Applications**（已发布的应用程序）选项卡。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



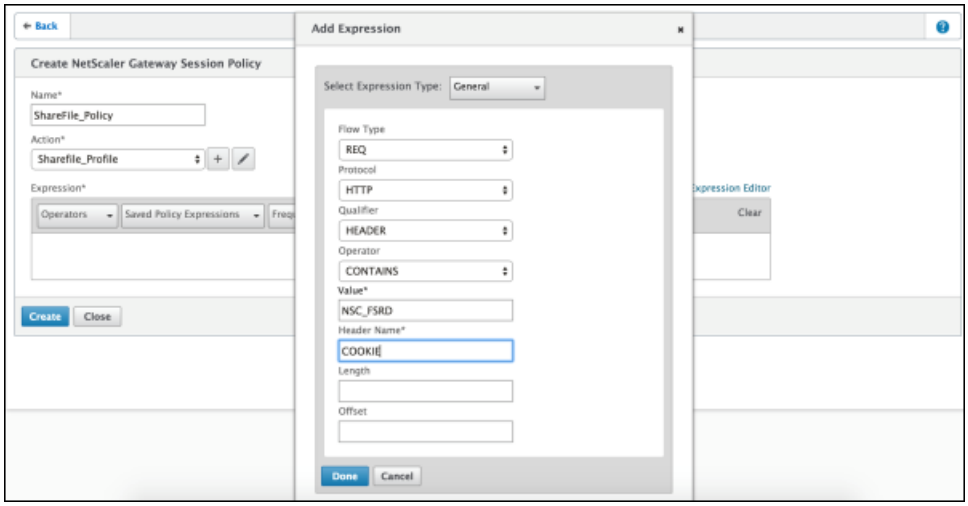
配置以下设置：

- o **ICA Proxy**（ICA 代理）：在列表中，单击 **ON**（开）。
- o **Web Interface Address**（Web Interface 地址）：键入 XenMobile 服务器的 URL。
- o **Single Sign-on Domain**（单点登录域）：键入 Active Directory 的域名。

注意：配置 NetScaler Gateway 会话配置文件时，**Single Sign-on Domain**（单点登录域）的域后缀必须与在 LDAP 中定义的 XenMobile 域别名匹配。

5. 单击 **Create**（创建）以定义会话配置文件。

6. 单击 **Expression Editor**（表达式编辑器）。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置以下设置：

- **Value**（值）：键入 NSC_FSRD。
- **Header Name**（标头名称）：键入 COOKIE。
- 单击**完成**。

7. 单击 **Create**（创建），然后单击 **Close**（关闭）。

在 NetScaler Gateway 虚拟服务器上配置策略

在 NetScaler Gateway 虚拟服务器上配置以下设置。

1. 在 NetScaler Gateway 配置实用程序中，在左侧导航窗格中单击 **NetScaler Gateway > Virtual Servers**（虚拟服务器）。

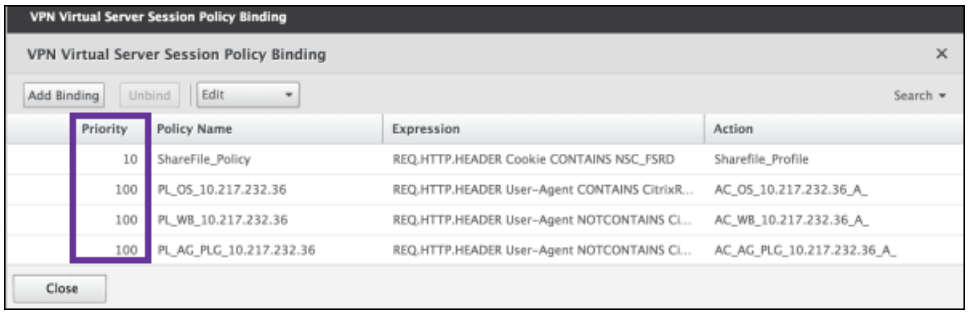
2. 在 **Details**（详细信息）窗格中，单击 NetScaler Gateway 虚拟服务器。

3. 单击**编辑**。

4. 单击 **Configured policies（已配置的策略）> Session policies（会话策略）**，然后单击 **Add binding**（添加绑定）。

5. 选择 **ShareFile_Policy**。

6. 编辑自动生成的选定策略的 **Priority**（优先级）编号，以便与列出的任何其他策略相比，其优先级最高（编号最小），如下图所示。



7. 单击 **Done**（完成），然后保存运行的 NetScaler 配置。

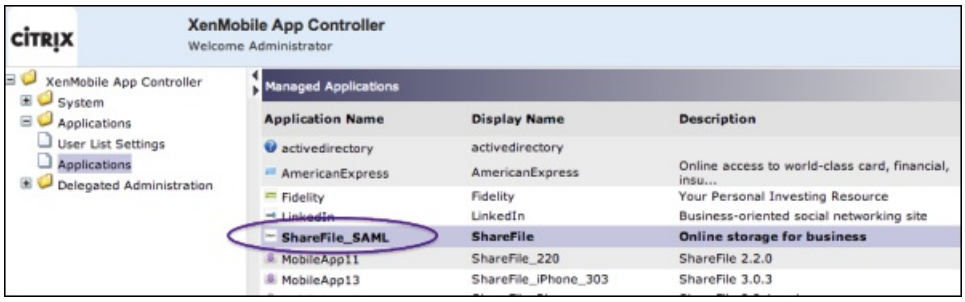
请执行以下步骤，查找 ShareFile 配置的内部应用程序名称。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 使用 URL **https://:4443/OCA/admin/** 登录 XenMobile 管理工具。 请务必使用大写字母输入 OCA。

2. 在**查看**列表中，单击**配置**。

3. 单击**应用程序 > 应用程序**，并记录**显示名称**为 ShareFile 的应用程序的**应用程序名称**。



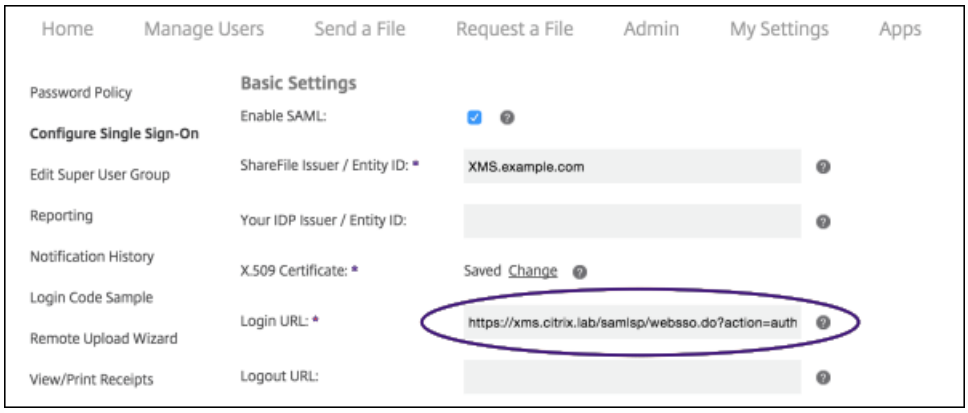
修改 ShareFile.com 的 SSO 设置

1. 以 ShareFile 管理员身份登录 ShareFile 帐户 (https://<子域>.sharefile.com)。

2. 在 ShareFile Web 界面中，单击 **Admin**（管理），然后选择 **Configure Single Sign-on**（配置单点登录）。

3. 按如下所示编辑 **Login URL**（登录 URL）：

Login URL（登录 URL）应如下所示：https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在 XenMobile 服务器的 FQDN 前面插入 NetScaler Gateway 虚拟服务器的外部 FQDN 和 /cginfra/https/，然后在 XenMobile 的 FQDN 后面添加 8443。

  登录 URL 现在应如下所示：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** 更改为为非 MDX ShareFile 应用程序配置 SAML 步骤 3 中的内部 ShareFile 应用程序名称。 内部名称默认为 **ShareFile_SAML**，但是，每次更改配置时，都会在内部名称后面附加一个数字（ShareFile_SAML_2、ShareFile_SAML_3，以此类推）。

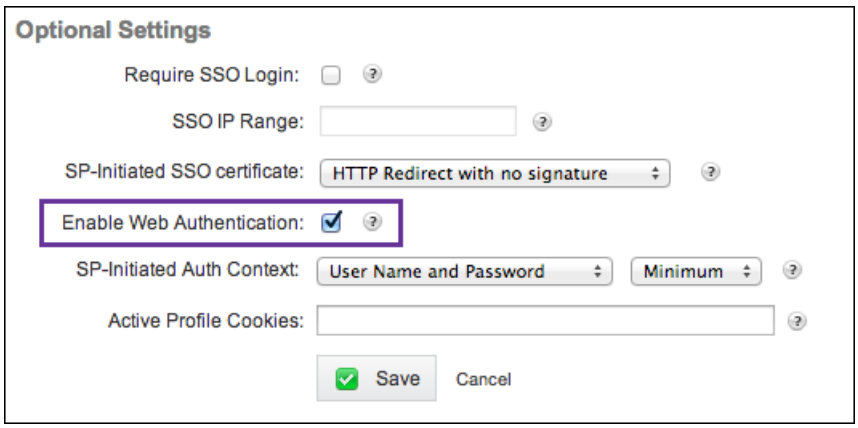
  登录 URL 现在应如下所示：https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

- 向 URL 的结尾末尾添加 &nssso=true。

  修改后的 URL 现在应如下所示：https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**。

  重要：每次在 XenMobile 控制台中编辑或重新创建 ShareFile 应用程序或更改 ShareFile 设置时，都会在内部应用程序名称后附加一个新数字，这意味着您还必须在 ShareFile Web 站点中更新登录 URL，以反映更新后的应用程序名称。

4. 在 **Optional Settings**（可选设置）下，选中 **Enable Web Authentication**（启用 Web 身份验证）复选框。



请执行以下配置以验证设置。

1. 将浏览器指向 https://<子域>sharefile.com/saml/login。

系统会将您重定向到 NetScaler Gateway 登录表单。 如果未被重定向，请验证前面的配置设置。

2. 输入所配置的 NetScaler Gateway 和 XenMobile 环境的用户名和密码。

此时将在 <子域>.sharefile.com 下显示您的 ShareFile 文件夹。 如果未显示您的 ShareFile 文件夹，请确保您输入了正确的登录凭据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

自动化操作

Oct 21, 2016

在 XenMobile 中创建自动化操作以计划对事件、用户或设备属性或者用户设备上存在应用程序做出反应。 创建自动化操作后，您可以在基于操作中的触发器连接到 XenMobile 时对用户设备建立影响。 触发事件后，您可以在采取更实质性的操作之前向用户发送通知以更正问题。

例如，如果要检测先前已加入黑名单的应用程序（如 Words with Friends），您可以指定一个触发器，设置在用户设备上检测到 Words with Friends 时不合规的用户设备。 然后，该操作会通知用户必须删除该应用程序才能使其设备重新合规。 在采取更实质性的操作（例如选择性地擦除设备）之前，您可以设置等待用户合规的时限。

设置为自动出现的影响范围如下：

- 完全或选择性地擦除设备。
- 将设备设置为不合规。
- 吊销设备。
- 在采取更严重的操作之前，向用户发送通知以更正问题。

注意：在可以通知用户之前，必须已在设置中为 SMTP 和 SMS 配置通知服务器，以便 XenMobile 可以发送消息，请参阅 XenMobile 中的通知。 此外，请在继续操作前设置打算使用的通知模板。 有关设置通知模板的详细信息，请参阅在 XenMobile 中创建或更新通知模板。

本主题介绍了如何在 XenMobile 中添加、编辑和过滤自动化操作。

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：

- 单击**添加**以添加新操作。
- 选择要编辑或删除的现有操作。 单击要使用的选项。

注意：如果选中某项操作旁边的复选框，选项菜单将显示在操作列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。

3. 此时将显示**操作信息**页面。

4. 在**操作信息**页面上，输入或修改以下信息：

- **名称**：键入一个名称来唯一地标识操作。 此字段为必填字段。
- **说明**：描述执行该操作的目的。

5. 单击**下一步**。 此时将显示**操作详细信息**页面。

注意：以下示例显示如何设置**事件**触发器。 如果选择其他触发器，生成的选项将与此处显示的选项有所不同。

6. 在**操作详细信息**页面上，输入或修改以下信息：

- 在**触发器**列表中，单击适用于此操作的事件触发器类型。 每个触发器的含义如下所示：
  - **事件**：对预定义的事件做出反应。
  - **设备属性**：检查在 MDM 模式下收集的设备上的设备属性，并对其做出反应。
  - **用户属性**：对用户属性做出反应，通常通过 Active Directory。
  - **Installed app name**（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。 默认情况下，应用程序清单策略在所有平台上均处于启用状态。 有关详细信息，请参阅添加应用程序清单设备策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. 在下一个列表中，单击对触发器的响应。

8. 在**操作**列表中，单击符合触发器条件时要执行的操作。 除**发送通知**之外，选择一个时间范围，让用户可以解决引起触发的问题。 如果在该时间范围内未解决此问题，将执行选定的操作。 可用操作如下：

- **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。
- **完全擦除设备**：擦除设备上的所有数据和应用程序，包括内存卡（如果设备具有内存卡）。
- **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，用户根本无法登录 XenMobile。 在 iOS 上，用户仍然能够登录，但无法访问应用程序。
- **应用程序擦除**：在 Android 上，此操作将删除用户的 XenMobile 帐户。 在 iOS 上，此操作将删除用户访问 XenMobile 功能所需的加密密钥。
- **将设备标记为不合规**：将设备设置为不合规。
- **发送通知**：向用户发送消息。

此过程的其余部分介绍了如何发送通知操作。

9. 在下一个列表中，选择用于通知的模板。 此时将显示与选定事件相关的通知模板。

注意：在可以通知用户之前，必须已在“设置”中为 SMTP 和 SMS 配置通知服务器，以便 XenMobile 可以发送消息，请参阅 XenMobile 中的通知。 此外，请在继续操作前设置打算使用的通知模板。 有关设置通知模板的详细信息，请参阅在 XenMobile 中创建或更新通知模板。

注意：选择模板后，可以通过单击“预览通知消息”预览通知。

10. 在以下字段中，设置延迟时间（以天、小时或分钟为单位）后再执行操作，并设置用户解决触发问题前重复操作的时间间隔。

11. 在**摘要**中，验证是否已按预期创建自动化操作。

12. 配置操作详细信息后，可以分别为每个平台配置部署规则。 为此，针对您选择的每个平台执行步骤 13。

13. 配置部署规则

14. 针对该操作完成配置平台部署规则后，单击**下一步**。 此时将显示**操分配作**页面，您可以在其中将操作分配给一个或多个交付组。 此步骤可选。

15. 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要向其分配策略的交付组。 选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。

16. 展开部署计划，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 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**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。
  注意：已在**设置** > **服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。

注意：配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

17. 单击**下一步**。 此时将显示**摘要**页面，您可以在其中验证操作配置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

18. 单击**保存**以保存操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 中的宏

Aug 11, 2016

XenMobile 提供了多个功能强大的宏，用于将用户或设备属性数据填充到配置文件、策略、通知或注册模板（用于某些操作）的文本字段中。当然，还有其他用途。 使用宏，可以配置单个策略并将其部署到较大的用户群，并为每个目标用户显示特定于用户的值。 例如，可以为涵盖数千个用户的 Exchange 配置文件中的某个用户预填充邮箱值。

此功能当前仅在适用于 iOS 和 Android 设备的配置和模板上下文中可用。

以下用户宏始终可用：

- loginname （username 加 domainname）
- username（如有，则为 loginname 去掉域）
- domainname（域名或默认域）

以下管理员定义的属性可能可用：

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename
- postalcode
- postofficebox
- telephonenumber

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname（覆盖上述属性）

此外，如果通过身份验证服务器（如 LDAP）对用户进行身份验证，该商店中与用户相关的所有属性均可用。

宏可以采用以下格式：

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

通常情况下，美元符号 ($) 后的所有语法必须以花括号 ({ }) 括起来。

- 限定的属性名称引用可以是用户属性、设备属性或自定义属性。
- 限定的属性名称包括一个前缀，后跟实际属性名称。
- 用户属性的格式为 ${user.[PROPERTYNAME] (prefix="user.")}。
- 设备属性的格式为 ${device.[PROPERTYNAME] (prefix="device.")}。

例如 ${user.username} 将在策略文本字段中填充用户名值。 这在配置由多个用户使用的 Exchange ActiveSync 配置文件和其他配置文件时非常有用。

对于自定义宏（您定义的属性），前缀为 ${custom}。 您可以忽略前缀。

注意：属性名称区分大小写。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 客户端设置

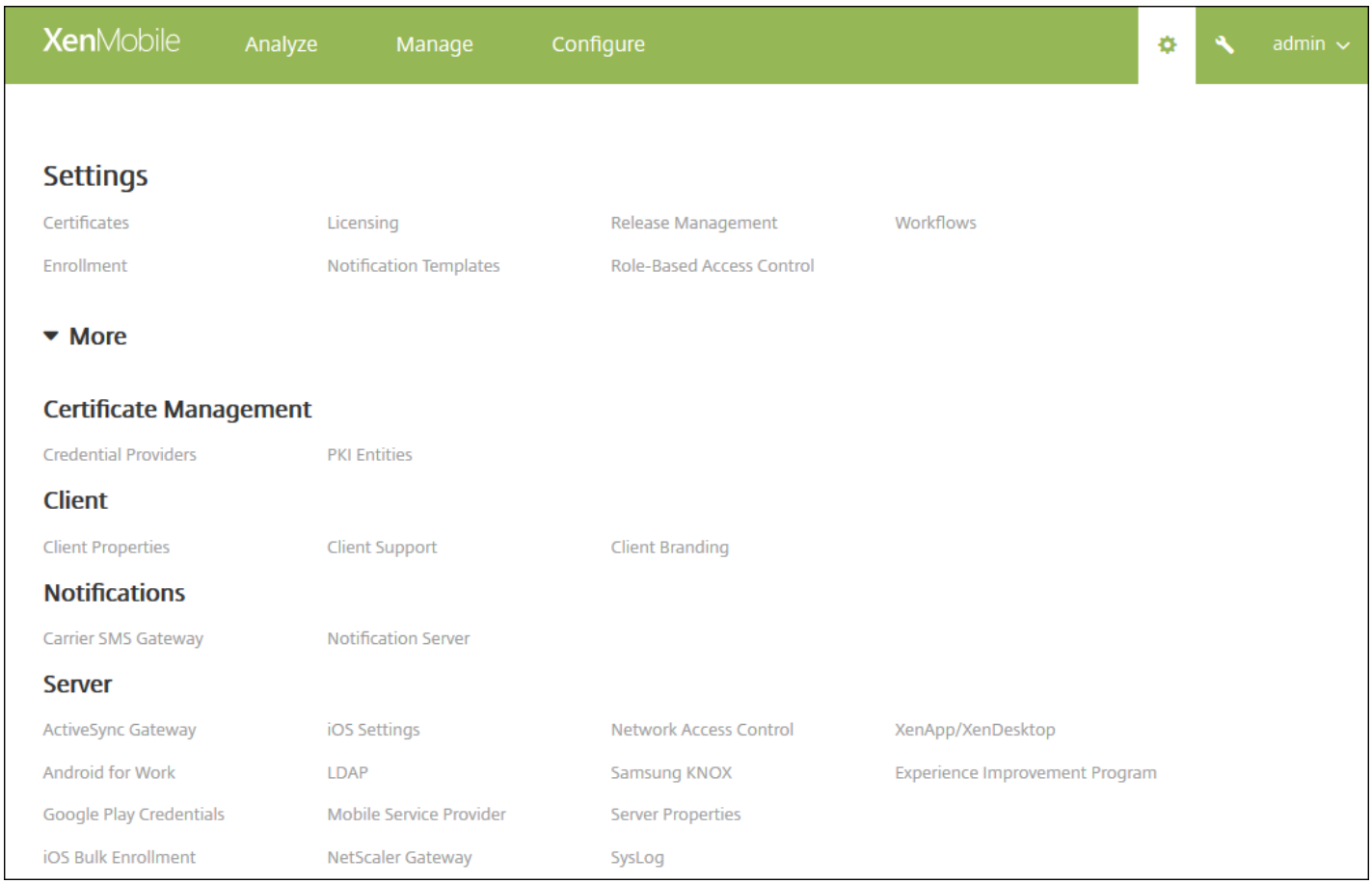
Aug 11, 2016

在 XenMobile 控制台中配置的 XenMobile 客户端设置包括：

- 客户端属性
- 客户端支持
- 客户端外观方案

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。

3. 在**客户端**下面，单击要配置的选项。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建适用于 iOS 设备的自定义 Worx Store 品牌设计

Oct 21, 2016

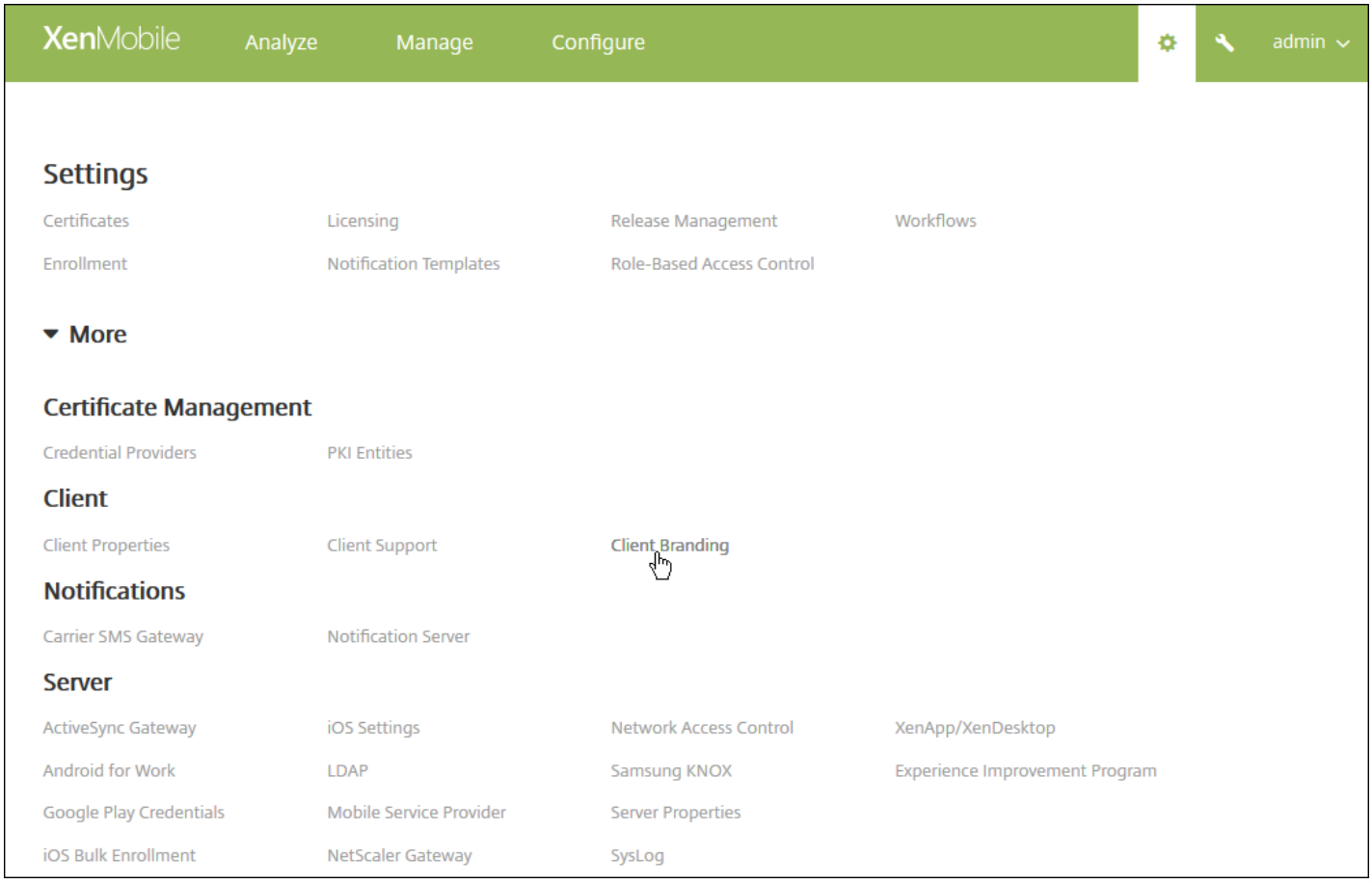
可以设置应用程序在应用商店中的显示方式，并添加徽标以在移动设备上设计适用于 iOS 和 Android 的 Secure Hub 和 XenMobile Store 外观方案。

注意：开始之前，请确保您的自定义图片已准备就绪并且可供访问。

自定义图片必须满足以下要求：

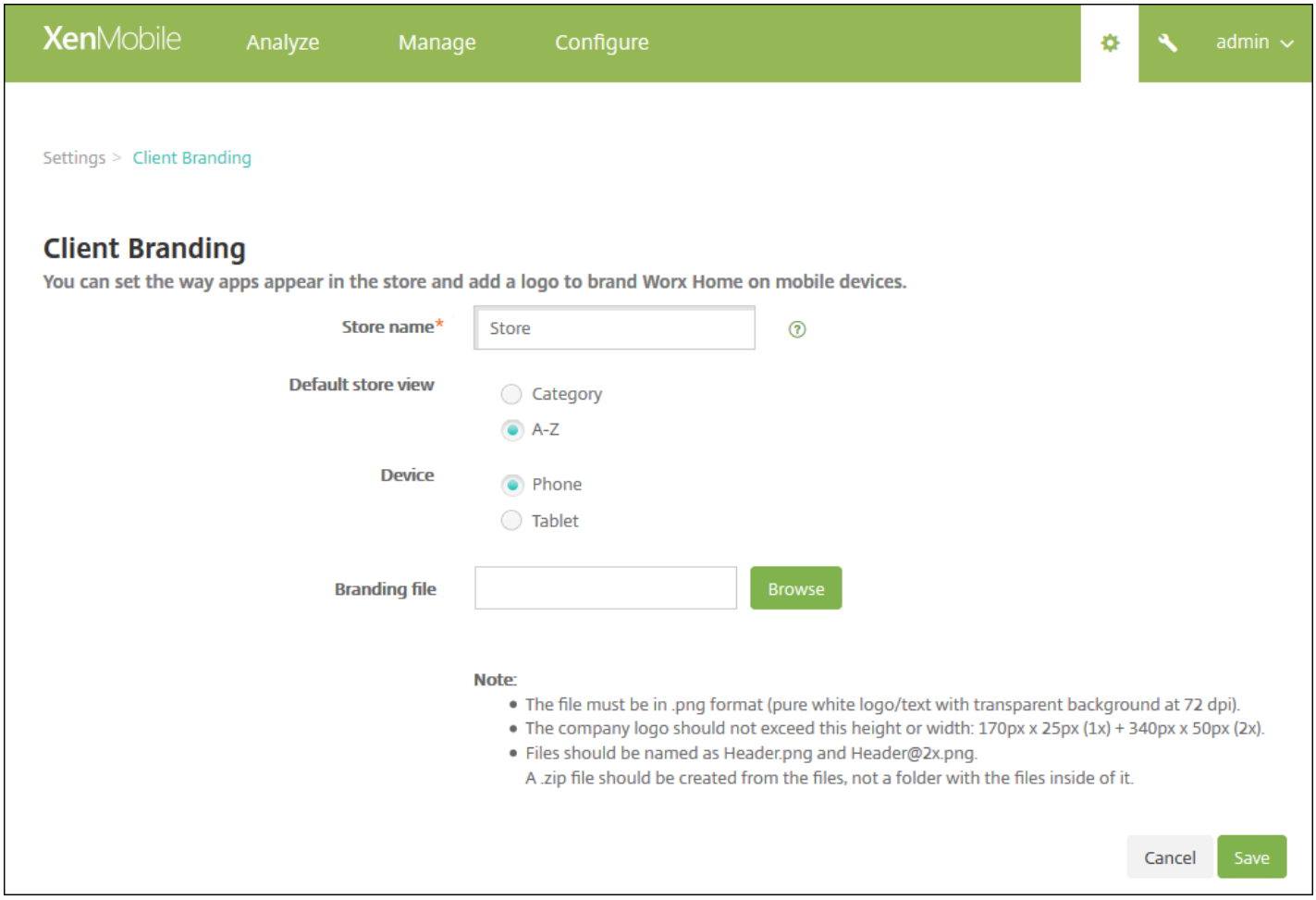
- 文件必须采用 .png 格式
- 使用纯白徽标或文本以及 72 dpi 的透明背景。
- 公司徽标不得超过此高度或宽度：170 px x 25 px (1x) 和 340 px x 50 px (2x)。
- 将文件命名为 Header.png 和 Header@2x.png。
- 从文件而不是文件所在的文件夹创建 .zip 文件。

1. 在 XenMobile 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**下面，单击**客户端外观方案**。 此时将显示**客户端外观方案**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置以下设置：

- **应用商店名称**：应用商店名称显示在用户的帐户信息中。 更改此名称也会更改用于访问应用商店服务的 URL。 通常无需更改默认名称。
- **默认应用商店视图**：选择**类别**或 **A-Z**。 默认值为 **A-Z**。
- **设备**选项：选择**电话**或**平板电脑**。 默认值为**电话**。
- **外观方案文件**：单击**浏览**并导航到要用于外观方案的图像或图像的 .zip 文件，选择此文件。

3. 单击**保存**。

要将此软件包部署到用户设备，首先需要创建一个部署软件包，然后将其部署到用户设备。

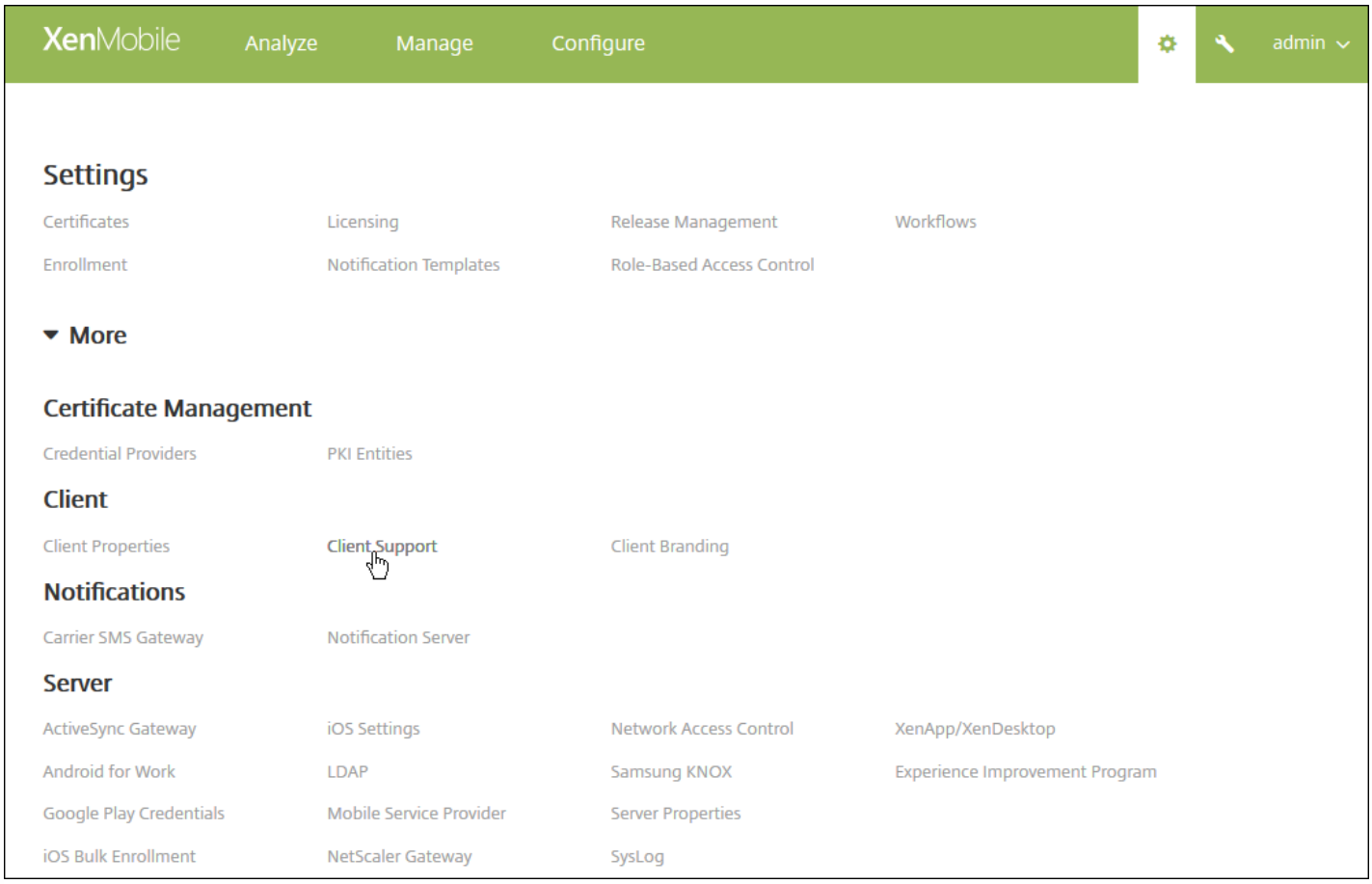
© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建 Worx Home 和 GoToAssist 支持选项

Oct 21, 2016

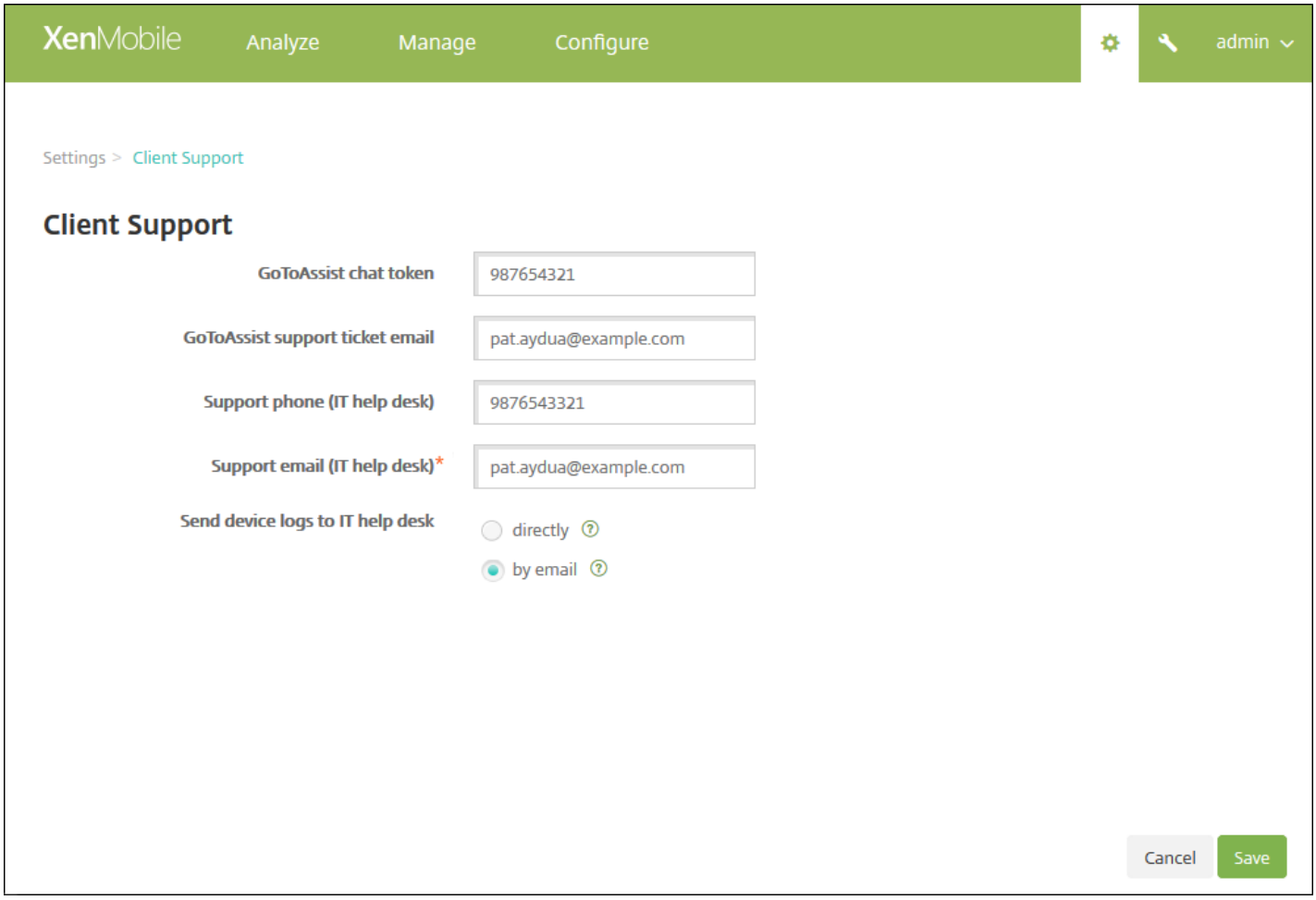
您可以通过提供电子邮件地址、电话号码和 GoToAssist 令牌，为用户提供多种联系支持员工的方式。 当用户从其设备请求帮助时，他们会看到您所设置的选项。

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**下面，单击**客户端支持**。 此时将显示**客户端支持**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 配置以下设置：

- **GoToAssist 文字消息令牌**：键入用户收到的令牌以启动 GoToAssist 会话。
- **GoToAssist 支持票证电子邮件**：键入用户用于 GoToAssist 支持票证的电子邮件地址。
- **支持电话(IT 技术支持)**：键入 IT 技术支持的电话号码。
- **支持电子邮件(IT 技术支持)**：键入 IT 技术支持联系人的电子邮件地址。
- **将设备日志发送给 IT 技术支持人员**：选择设备日志是**直接**发送还是**通过电子邮件**发送。 默认值为**通过电子邮件**。
  - 启用**直接**时，会显示“在 ShareFile 上存储日志”对应的设置。 如果启用“在 ShareFile 上存储日志”，日志将直接被发送到 ShareFile；否则，日志被发送到 XenMobile，然后再通过电子邮件发送给 IT 技术支持人员。 此外，还会显示**如果直接发送失败，请使用电子邮件**选项，默认情况下启用此选项。 如果不希望在出现服务器问题时使用客户端的电子邮件发送日志，可以禁用此选项。 但是，如果禁用此选项并出现服务器问题，将不会发送日志。
  - 启用**通过电子邮件**时，客户端的电子邮件始终用于发送日志。

4. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

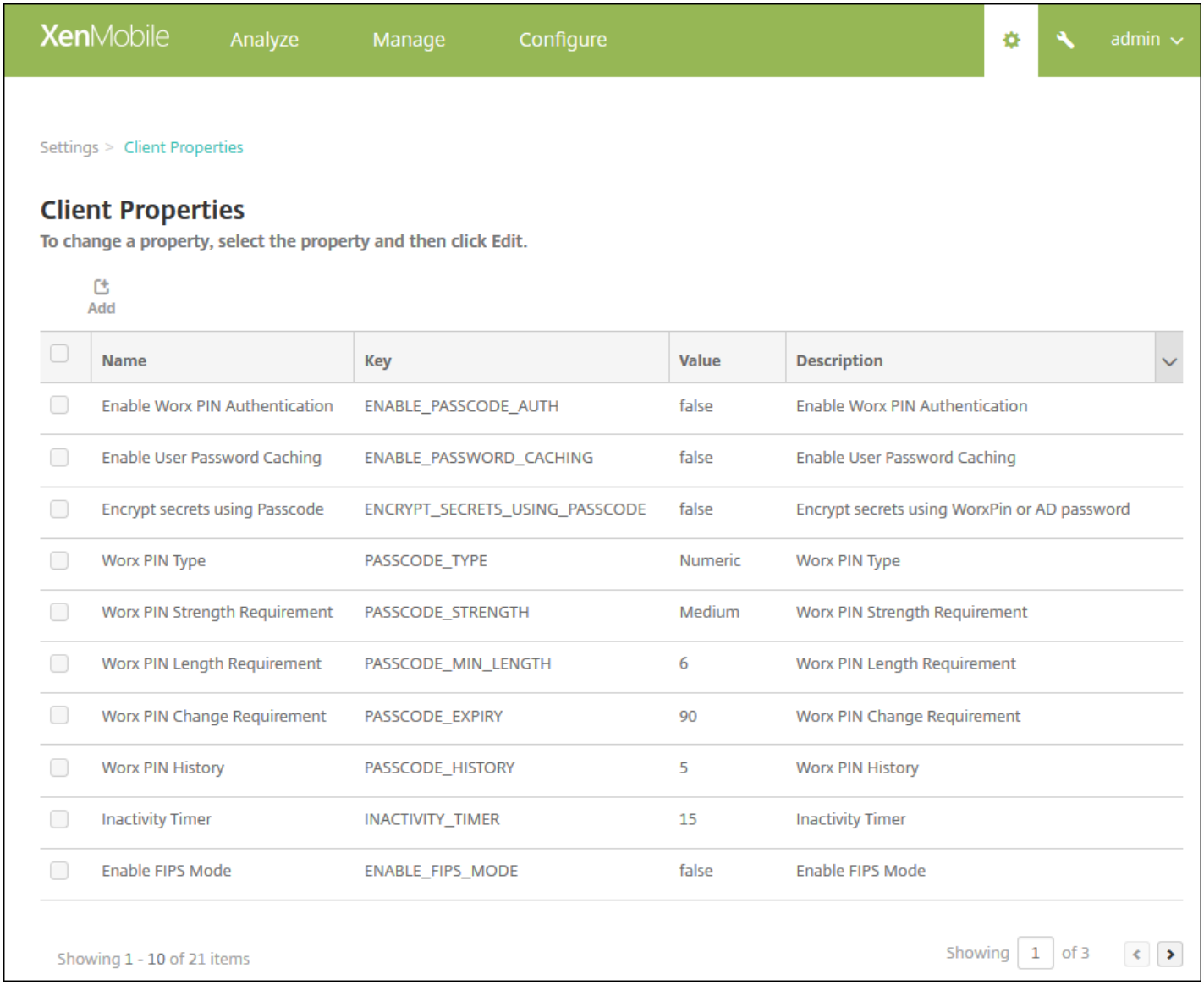
添加、编辑或删除客户端属性

Aug 11, 2016

客户端属性包含用户设备上直接提供给 Worx Home 的信息。 可以使用这些属性配置高级设置，如 Worx PIN。 从 Citrix 技术支持获取客户端属性。

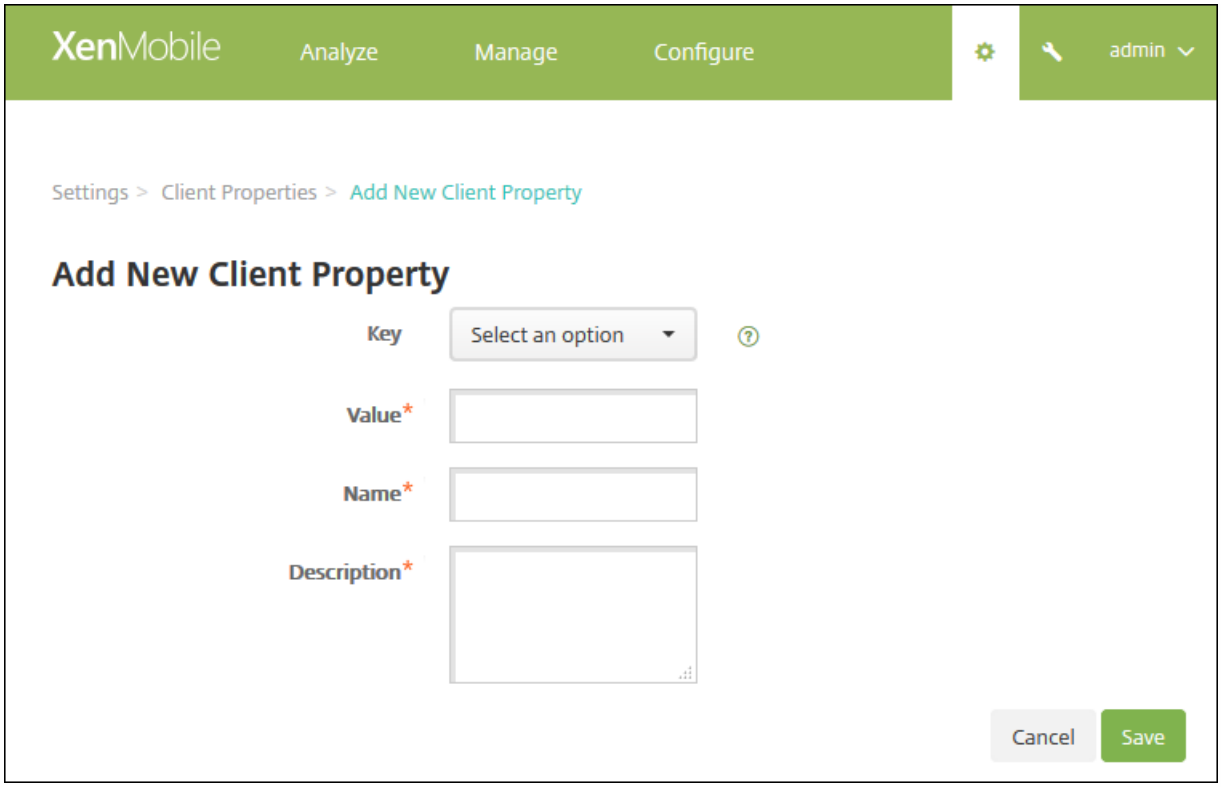
每次发布客户端应用程序（尤其是 Worx Home）时，均会更改客户端属性。 有关客户端属性的详细信息，请参阅客户端属性参考。

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**下面，单击**客户端属性**。 此时将显示**客户端属性**页面。 可以从此页面添加、编辑和删除客户端属性。



1. 单击**添加**。 此时将显示**添加新客户端属性**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 配置以下设置：

- **键**：在列表中，单击要添加的属性键。 **重要**：执行任何更改或请求特殊键以进行更改时请联系 Citrix 技术支持。
- **值**：输入选定属性的值。
- **名称**：输入属性的名称。
- **说明**：输入属性的说明。

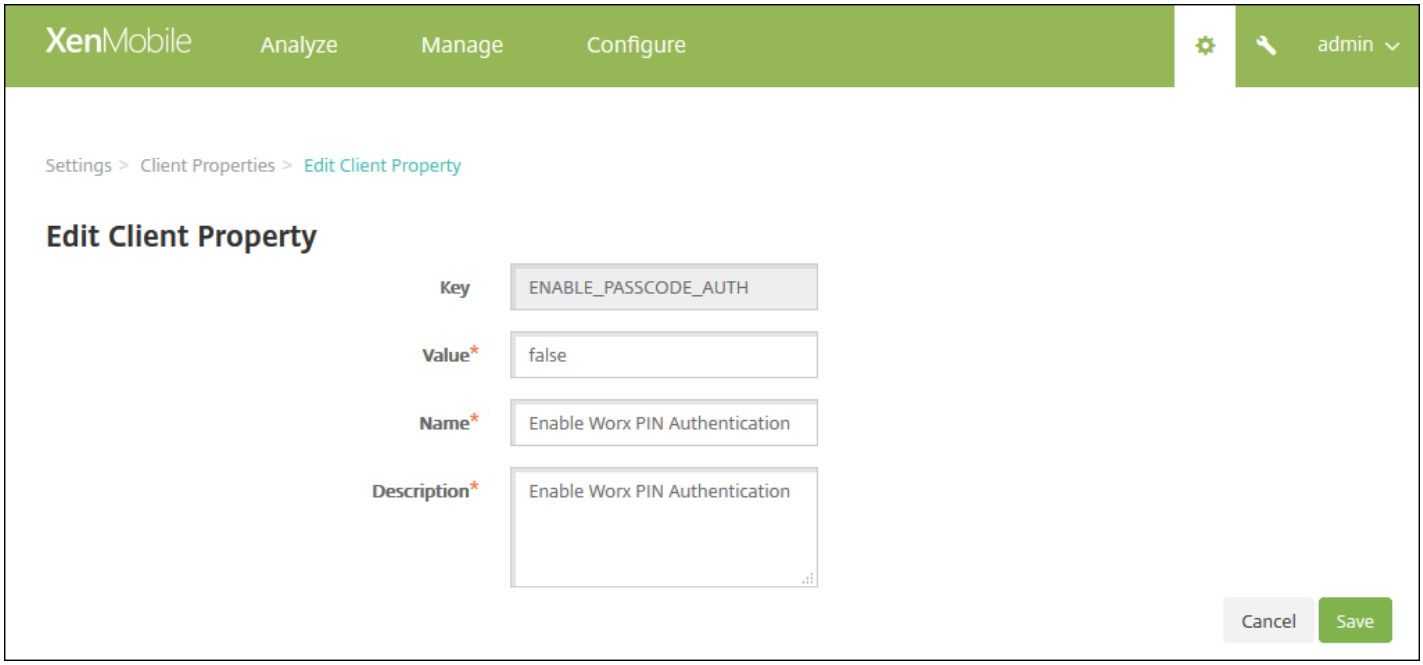
3. 单击**保存**。

1. 在**客户端属性**表格中，选择要编辑的客户端属性。

注意：如果选中某个客户端属性旁边的复选框，选项菜单将显示在客户端属性列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。

2. 单击**编辑**。 此时将显示**编辑客户端属性**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 适当更改以下信息：

- **密钥**：无法更改此字段。
- **值**：属性的值。
- **名称**：属性的名称。
- **说明**：属性的说明。

4. 单击**保存**以保存您的更改，或单击**取消**保持属性不发生更改。

1. 在**客户端属性**表格中，选择要删除的客户端属性。

   注意：可以通过选中每个属性旁边的复选框，选择要删除的多个属性。

2. 单击**删除**。 此时将显示确认对话框。 再次单击**删除**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

客户端属性参考

Aug 11, 2016

XenMobile 首选客户端属性及其默认设置如下所示。

CONTAINER_SELF_DESTRUCT_PERIOD

显示名称：自毁

自毁功能阻止在经过特定天数的非活动状态后访问 WorxHome 和托管应用程序。 超过此时间限制后，应用程序不再可用，用户设备取消从 XenMobile 服务器注册。 擦除数据包括清除已安装的各应用程序的应用程序数据，包括应用程序缓存和用户数据。 不活动时间是指在经过特定时间长度后，服务器不接收身份验证请求以验证用户。 例如，如果为此策略设置 30 天，用户不使用 Worx Home 或其他应用程序的时间超过 30 天，则此策略生效。

此全局安全性策略适用于 iOS 和 Android 平台，是对现有应用程序锁定和擦除策略的增强。

要配置此全局策略，请转至**设置 > 客户端属性**，然后添加自定义键 CONTAINER_SELF_DESTRUCT_PERIOD。

值：天数

ENABLE_WORXHOME_CEIP

显示名称：启用 Worx Home CEIP

此键将打开客户体验改善计划。 这样会定期向 Citrix 发送匿名配置和使用数据。 此数据可帮助 Citrix 改善 XenMobile 的品质、可靠性和性能。

值：true 或 false

默认值：false

ENABLE_PASSCODE_AUTH

显示名称：启用 Worx PIN 身份验证

此键允许您打开 Worx PIN 功能。 启用 Worx PIN 或通行码后，系统将提示用户定义要使用的 PIN（而非其 Active Directory 密码）。 如果启用了 ENABLE_PASSWORD_CACHING，或者如果 XenMobile 使用证书身份验证，此设置将自动启用。

如果用户执行脱机身份验证，Worx PIN 将在本地验证，并且允许用户访问所请求的应用程序或内容。 如果用户执行联机身份验证，Worx PIN 或通行码将用于解锁 Active Directory 密码或证书，随后将发送后者以通过 XenMobile 执行身份验证。

可能的值：true 或 false

默认值：false

ENABLE_PASSWORD_CACHING

显示名称：启用用户密码缓存。

此键允许您在移动设备本地缓存用户的 Active Directory 密码。 当您将此键设置为 true 时，系统将提示用户设置 Worx

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PIN 或通行码。 当您将此键设置为 true 时，必须将 ENABLE_PASSCODE_AUTH 键设置为 true。

可能的值：true 或 false

默认值：false

ENCRYPT_SECRETS_USING_PASSCODE

显示名称：使用通行码加密机密

此键允许将机密数据存储在移动设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串。 此配置键允许使用强加密的密钥，但还会添加用户熵（用户生成的只有自己知道的随机 PIN 码）。

Citrix 建议您启用此键以帮助提高用户设备的安全性。

注意：启用此键将影响用户体验，具体表现为会出现过多要求输入 Worx PIN 的身份验证提示。

可能的值：true 或 false

默认值：false

PASSCODE_TYPE

显示名称：Worx PIN 类型

此键定义用户能够定义数字型 Worx PIN 还是字母数字型 Worx 通行码。 选择“数字”时，用户只能定义数字型 Worx PIN。 选择“字母数字”时，用户可以为 Worx 通行码使用字母和数字的组合。

注意：更改此设置时，系统将在下次提示用户进行身份验证时提示其设置新 Worx PIN 或通行码。

可能的值：数字或字母数字

默认值：数字

PASSCODE_STRENGTH

显示名称：Worx PIN 强度要求

此键定义 Worx PIN 或通行码的强度。 更改此设置时，系统将在下次提示用户进行身份验证时提示其设置新 Worx PIN 或通行码。

可能的值：低、中或强

默认值：中

下表介绍了每个强度设置的密码规则，具体取决于您为 PASSCODE_TYPE 选择的设置：

通行码强度	数字通行码类型的规则	字母数字通行码类型的规则
低	所有数字，允许使用任意顺序	必须至少包含一个数字和一个字母。 不允许使用：AAAaaa、aaaaaa、abcdef 允许使用：aa11b1、Abcd1#、Ab123~、aaaa11、

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		aa11aa
中 （默认设置）	1. 所有数字不能相同。 例如，不允许使用 444444。 2. 所有数字不能连续。 例如，不允许使用 123456 或 654321。 允许使用：444333、124567、136790、555556、788888	“低”通行码强度的规则补充： 1. 字母和所有数字不能相同。 例如，不允许使用 aaaa11、aa11aa 或 aaa111。 2. 字母和数字都不能连续。 例如，不允许使用 abcd12、bcd123、123abc、xy1234、xyz345 或 cba123。 允许使用：aa11b1、aaa11b、aaa1b2、abc145、xyz135、sdf123、ab12c3、a1b2c3、Abcd1#、Ab123~
强	与“中”Worx PIN 通行码强度相同。	通行码至少应包括一个数字、一个特殊符号、一个大写字母以及一个小写字母。 不允许使用：abcd12、Abcd12、dfgh12、jkrtA2 允许使用：Abcd1#、Ab123~、xY12#3、Car12#、AAbc1#

PASSCODE_MIN_LENGTH

显示名称：Worx PIN 长度要求

此键定义 Worx 通行码可以达到的最小长度。

可能的值：1-99

默认值：6

PASSCODE_EXPIRY

显示名称：Worx PIN 到期要求

此键定义 Worx PIN 或通行码的有效时间（单位为天），超过此时间后，系统将强制用户更改其 Worx PIN 或通行码。 更改此设置时，仅当用户的当前 Worx PIN 或通行码过期时才设置新值。

可能的值：1 或更大，建议使用 1-99

默认值：90

注意：如果希望用户永远不需要重置其 PIN 码，请将该值设置为一个非常大的值（例如 100000000000）。 如果最初设置的过期期限介于 1 到 99 天之间，然后在该时间段内更改为更大的数值，PIN 在初始期限结束时仍会过期，但之后永不过期。

PASSCODE_HISTORY

© 1999-2017 Citrix Systems, Inc. All rights reserved.

显示名称：Worx PIN 历史记录

此键定义之前使用的 Worx PIN 或通行码的数量，用户在更改其 Worx PIN 或通行码时不能重用。 如果更改此设置，用户下次重置其 Worx PIN 或通行码时将设置新值。

可能的值：1-99

默认值：5

INACTIVITY_TIMER

显示名称：不活动计时器

此键定义用户可以保持其设备处于不活动状态且之后访问应用程序不会提示输入 Worx PIN 或通行码的时间（单位为分钟）。 要为 MDX 应用程序启用此设置，必须将应用程序通行码设置设为开。 如果应用程序通行码设置设为关，用户将被重定向到 Worx Home 以执行完全身份验证。 更改此设置时，该值将在系统下次提示用户进行身份验证时生效。

注意：在 iOS 上，非活动计时器也将管理对 Worx Home 的访问，而不仅仅是对 MDX 应用程序的访问。

可能的值：任意正整数

默认值：15

DISABLE_LOGGING

显示名称：禁用日志记录

此键允许您禁用用户从其设备收集并上载日志的功能。 将为 Worx Home 和安装的所有 MDX 应用程序禁用日志记录功能。 用户无法从“支持”页面发送任何应用程序的日志；即使通过显示的电子邮件撰写对话框，也无法附加日志，但会添加指出日志记录功能被禁用的消息。 除了在用户设备上产生的影响，您也无法在 XenMobile 控制台中修改 Worx Home 和 MDX 应用程序的日志设置。

将此项设置为 True 时，Worx Home 将“阻止应用程序日志”设置为 True，以确保在应用新策略时 MDX 应用程序停止记录日志。

可能的值：true 或 false

默认值：false（不禁用日志记录）

ENABLE_CRASH_REPORTING

显示名称：启用崩溃报告

此键启用或禁用使用 Worx 应用程序的 Crashlytics 的崩溃报告。

可能的值：true 或 false

默认值：true

DEVICE_LOGS_TO_IT_HELP_DESK

显示名称：向 IT 技术支持发送设备日志

此键启用或禁用向 IT 技术支持发送日志的功能。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

可能的值：true 或 false

默认值：false

ON_FAILURE_USE_EMAIL

显示名称：失败时使用电子邮件向 IT 技术支持发送设备日志。

此键启用或禁用使用电子邮件向 IT 发送设备日志的功能。

可能的值：true 或 false

默认值：true

PASSCODE_MAX_ATTEMPTS

显示名称：Worx PIN 最大尝试次数

此键定义用户可以尝试输入错误 Worx PIN 或通行码的次数，之后系统将提示用户进行完全身份验证。 用户成功执行完全身份验证后，系统将提示其创建新 Worx PIN 或通行码。

可能的值：任意正整数

默认值：15

ENABLE_TOUCH_ID_AUTH

显示名称：启用 Touch ID 身份验证

此键启用或禁用设备使用 Touch ID 身份验证的功能。 用户的设备必须启用 Worx PIN 并将“用户熵”设置为“False”，才会在启动应用程序时收到使用 Touch ID 的提示。

可能的值：true 或 false

默认值：false

ENABLE_WORXHOME_GA

显示名称：在 WorxHome 中启用 Google Analytics

此键启用或禁用在 WorxHome 中使用 Google Analytics 收集数据的功能。 更改此设置时，仅当用户下次登录 WorxHome 时才设置新值。

可能的值：true 或 false

默认值：true

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 服务器设置

Aug 11, 2016

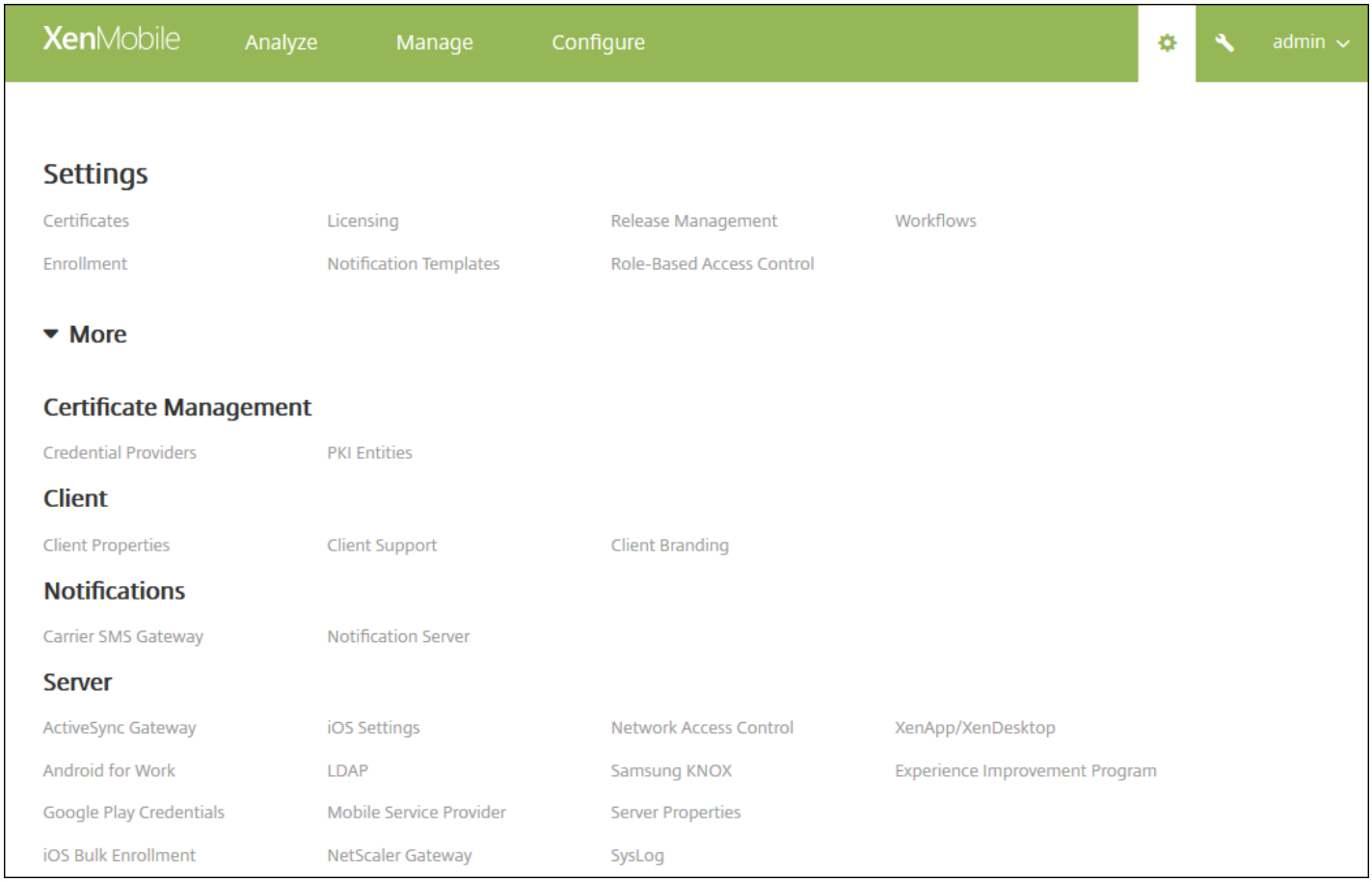
在 XenMobile 控制台中配置的 XenMobile 服务器设置包括：

- ActiveSync Gateway
- Android for Work
- 体验改善计划
- Google Play 凭据
- iOS 批量注册
- iOS 设置
- LDAP
- Microsoft Azure
- 移动服务提供商
- NetScaler Gateway
- 网络访问控制
- Samsung KNOX
- 服务器属性
- SysLog
- XenApp/XenDesktop

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**下面，单击要配置的选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 中的 ActiveSync Gateway

Aug 11, 2016

ActiveSync 是 Microsoft 开发的移动数据同步协议。 ActiveSync 与手持设备和台式（便携式）计算机同步数据。 可以在 XenMobile 中配置 ActiveSync Gateway 规则。 设备可基于这些规则，允许或拒绝访问 ActiveSync 数据。例如，如果激活了“缺少必备应用程序”规则，则 XenMobile 将检查应用程序访问策略中是否存在必备应用程序，如果缺少必备应用程序，则会拒绝对 ActiveSync 数据的访问。

XenMobile 支持以下规则：

匿名设备：检查设备是否处于匿名模式。 如果在设备尝试重新连接时 XenMobile 无法重新对用户进行身份验证，则可以执行此检查。

Samsung KNOX 认证失败：检查设备是否无法通过 Samsung KNOX 认证服务器的查询。

禁止的应用程序：检查设备是否具有应用程序访问策略中定义的禁止的应用程序。

隐式允许和拒绝：这是 ActiveSync Gateway 的默认操作，该操作会为不满足其他任何过滤器规则条件的所有设备创建一个设备列表，并根据该列表允许或拒绝连接。 如果任何规则均不匹配，则默认规则为“隐式允许”。

不活动设备：根据“服务器属性”中“Device Inactivity Days Threshold”（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。

缺少必备应用程序：检查设备是否缺少应用程序访问策略中定义的必备应用程序。

非推荐应用程序：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码：检查用户密码是否合规。 在 iOS 和 Android 设备上，XenMobile 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。 例如，在 iOS 设备上，如果 XenMobile 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。 在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规”设备属性检查设备是否不合规。 该属性通常由自动化操作进行更改，或由第三方利用 XenMobile API 进行更改。

吊销状态：检查设备证书是否已吊销。 再次授权之前，已吊销的设备无法重新注册。

已获得 root 权限的 Android 设备和已越狱的 iOS 设备：检查 Android 设备或 iOS 设备是否已越狱。

非托管设备：检查设备是否仍处于托管状态，受 XenMobile 控制。 例如，在 MAM 模式下运行的设备或已取消注册的设备为非托管设备。

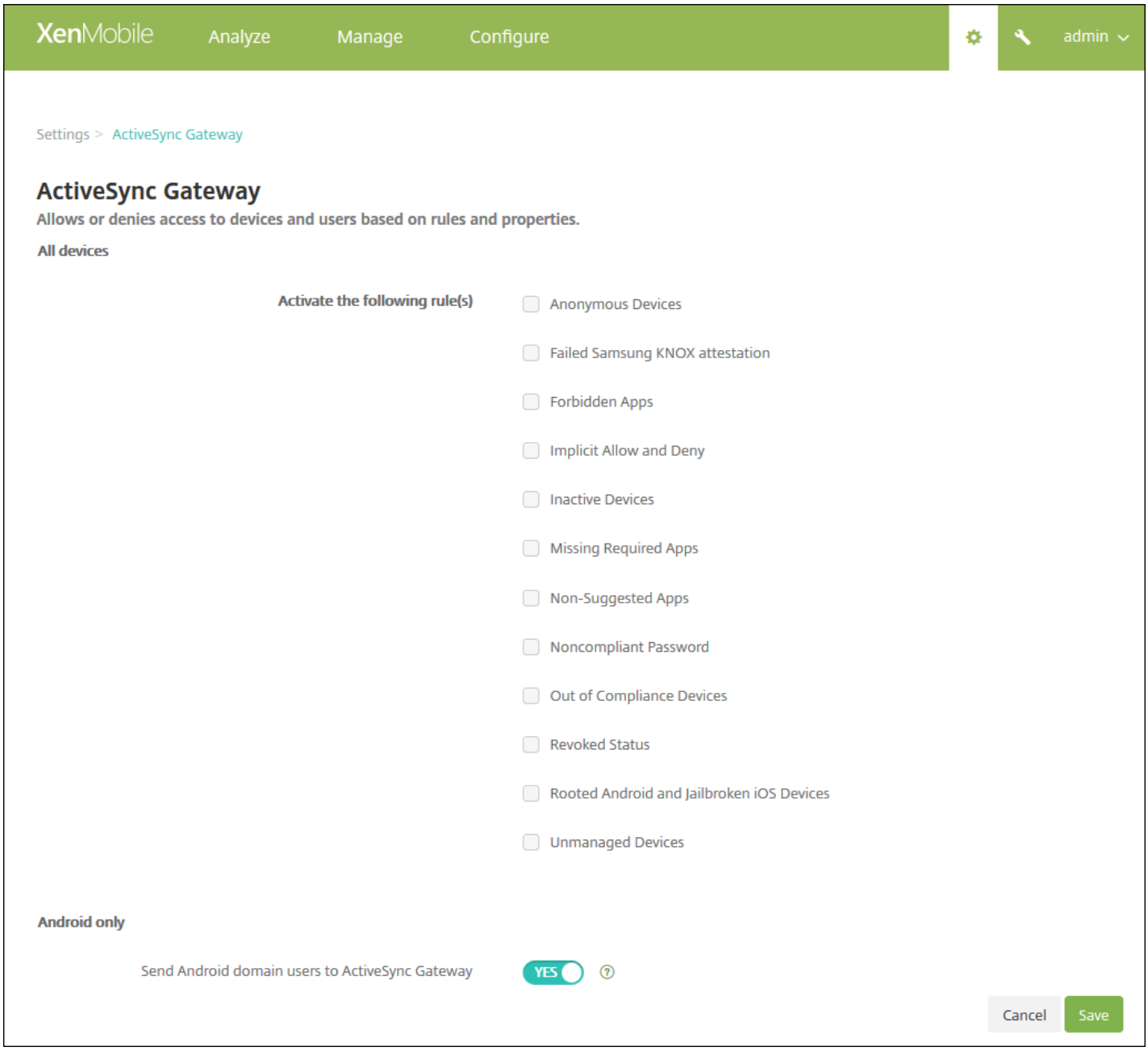
将 Android 域用户发送到 ActiveSync Gateway：单击**是**可确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。 启用此选项后，可确保在 XenMobile 不具有 Android 设备用户的 ActiveSync 标识符时，XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。

配置 ActiveSync Gateway 设置

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

2. 在**服务器**下面，单击 **ActiveSync Gateway**。 此时将显示 **ActiveSync Gateway** 页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 在**激活以下规则**下中，选择要激活的一个或多个规则。

4. 在**仅限 Android** 中的**将 Android 域用户发送到 ActiveSync Gateway** 中，单击**是**以确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。

5. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Google Play 凭据

Aug 15, 2016

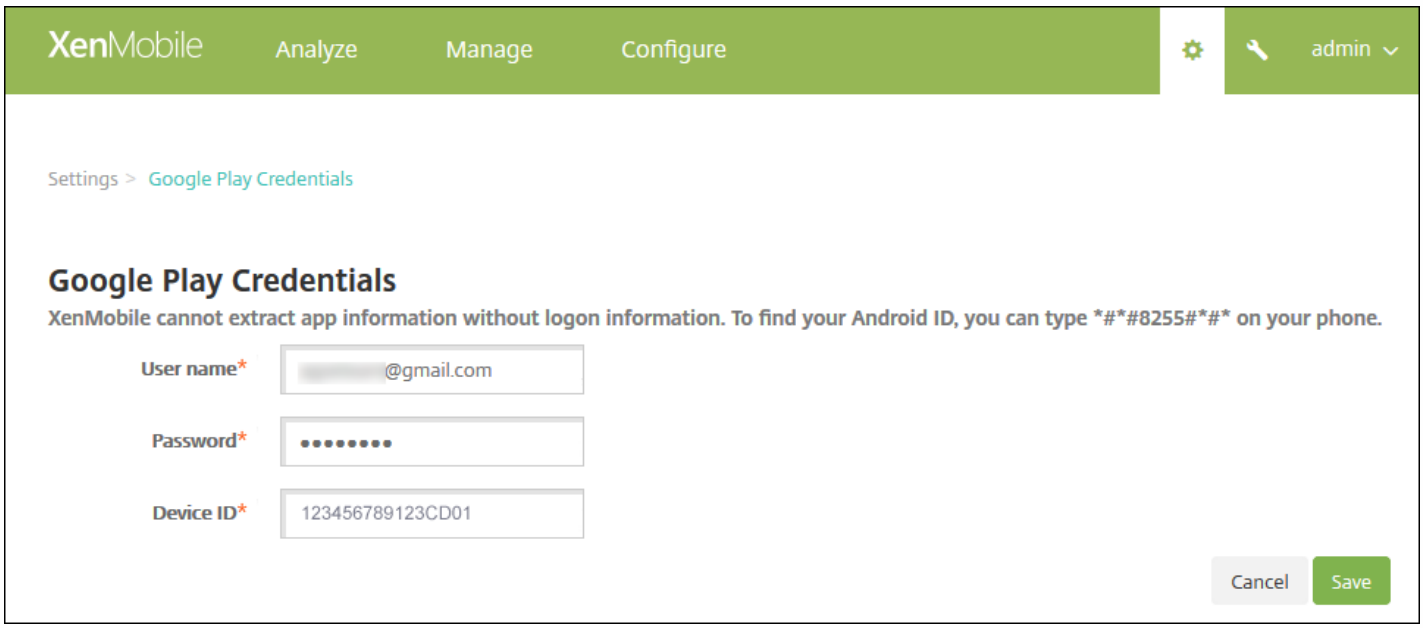
XenMobile 使用 Google Play 凭据为设备提取应用程序信息。

注意：要查找 Android ID，请在您的手机上输入 *#*#8255#*#*。 如果代码在您的设备类型中不显示设备 ID，可以使用设备 ID 第三方应用程序派生设备 ID。 需要获取的 ID 为带有 GSF ID 标签的 Google Services Framework ID。

重要：要启用 XenMobile 提取应用程序信息，您可能需要将 Gmail 帐户配置为允许不安全连接。 有关步骤，请参阅 Google 支持站点。

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 **Google Play 凭据**。 此时将显示 **Google Play 凭据**页面。



3. 配置以下设置：

- **用户名**：键入与 Google Play 帐户关联的名称。
- **密码**：键入用户密码。
- **设备 ID**：键入 Android ID。
  在电话上输入 *#*#8255#*#* 以确定 Android ID。

3. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

批量注册 iOS 设备

Aug 11, 2016

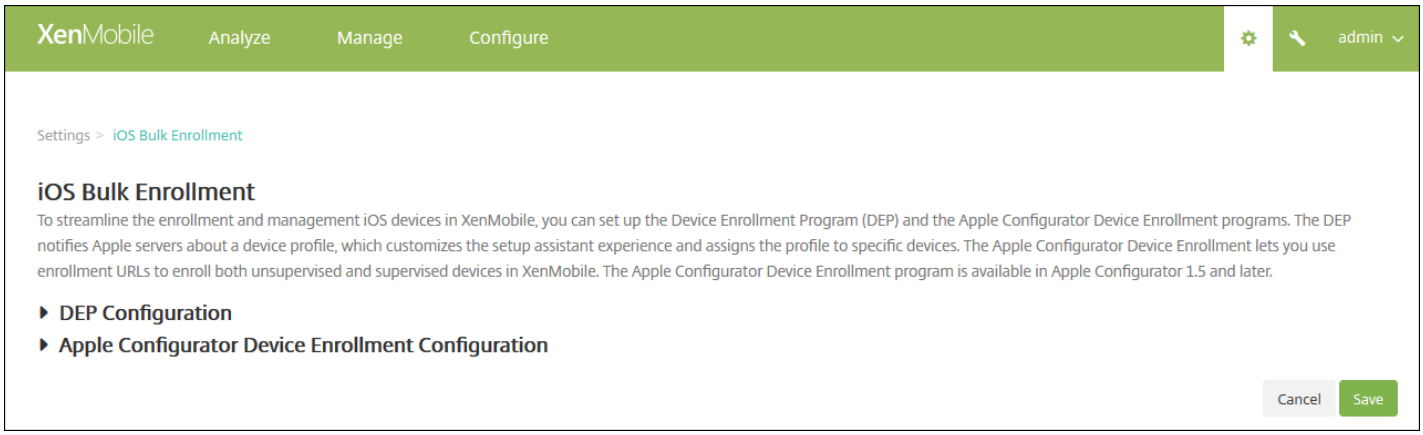
可以通过两种方式在 XenMobile 中注册大量 iOS 设备。 可以使用 Apple 的 Device Enrollment Program (DEP) 注册您直接从 Apple 或者从参与了该计划的 Apple 授权经销商或 运营商处购买的设备； 也可以使用 Apple Configurator 注册设备，无论这些设备是否直接从 Apple 购买，皆可注册。

使用 DEP 注册时，您不需要触摸或准备设备；只需通过 DEP 提交设备序列号或采购订单编号，设备即会在 XenMobile 中配置并注册。 注册设备后，可以将其提供给能够立即开箱使用这些设备的用户。 此外，通过 DEP 设置设备时，可以不执行用户在首次启动设备时需要完成的某些设置助理步骤。 有关设置 DEP 的详细信息，请参阅 Apple 的 Device Enrollment Program 页面。

使用 Apple Configurator 注册时，需要将设备连接到运行 OS X 10.7.2 或更高版本以及 Apple Configurator 应用程序的 Apple 计算机。 您通过 Apple Configurator 准备设备并配置策略。 为设备置备所需的策略后，首次将设备连接到 XenMobile 时将应用这些策略，您可以开始管理这些设备。 有关使用 Apple Configurator 的详细信息，请参阅 Apple 的 Apple Configurator 页面。

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 **iOS 批量注册**。 此时将显示 **iOS 批量注册**页面。



如果要配置 DEP 设置，请参阅配置 DEP 设置；如果要配置 Apple Configurator 设置，请参阅配置 Apple Configurator 设置。

必须在 deploy.apple.com 上创建一个 Apple DEP 帐户才能继续操作。 创建 DEP 帐户后，请设置一个虚拟 MDM 服务器以允许 XenMobile 和 Apple 进行通信。 为此，必须将 XenMobile 公钥上载到 Apple。 Apple 接受公钥后，将返回您导入到 XenMobile 中的服务器令牌。 请按照以下步骤进行操作，在 XenMobile 与 Apple 之间建立连接。

1. 要获取上载到 Apple 的公钥，请在 **iOS Device Enrollment Program** 页面上，展开 **DEP 配置**，然后单击**导出公钥**，并将该文件保存到您的计算机。

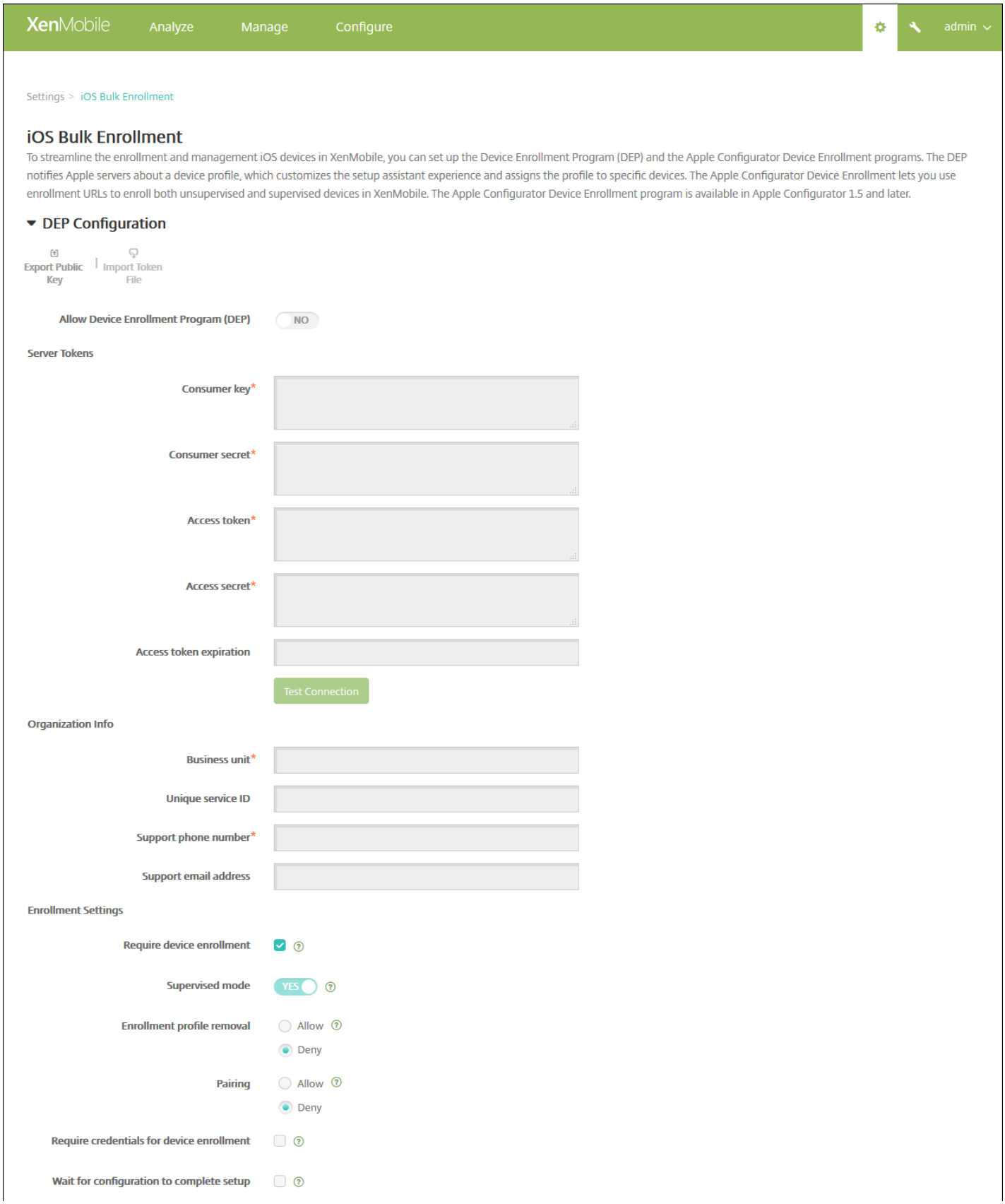
2. 转至 deploy.apple.com，登录您的 DEP 帐户，然后按照设置 MDM 服务器的说明进行操作。 在此过程中，Apple 将提供一个服务器令牌。

3. 在 **iOS 批量注册**页面上，单击**导入令牌文件**，将 Apple 服务器令牌添加到 XenMobile。

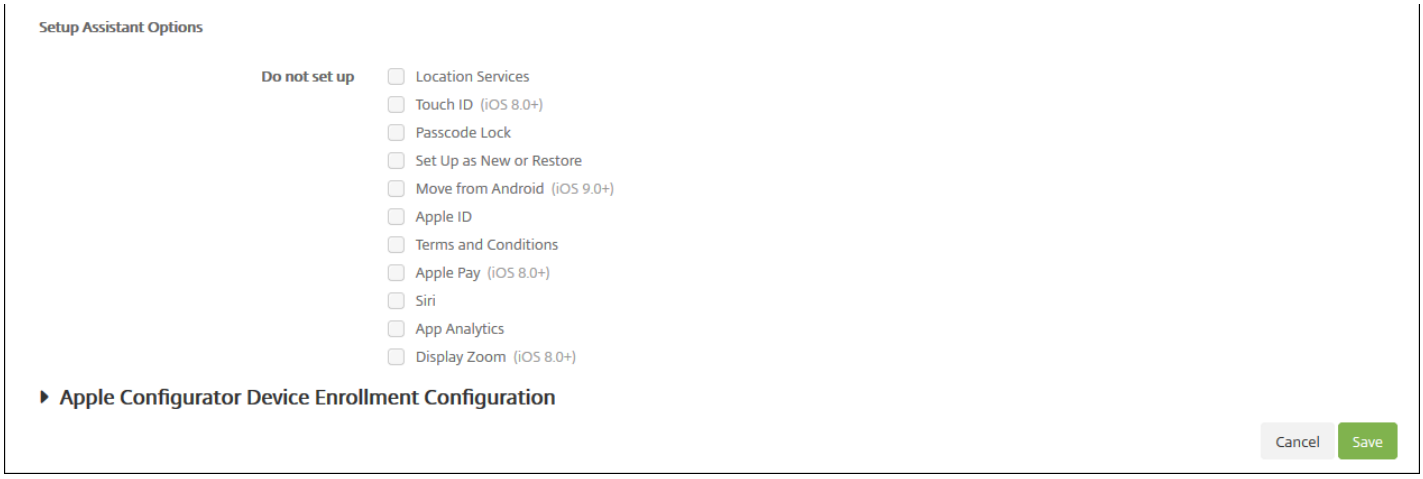
© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. 将令牌文件上载到 XenMobile 后，系统会自动填充**服务器令牌**字段。

5. 单击**测试连接**以确认 XenMobile 和 Apple 能够进行通信。 如果连接测试失败，请确认您已打开所有必需的端口，因为这是可能性最大的失败原因。 有关必须在 XenMobile 中打开的端口信息，请参阅端口要求。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 配置以下设置以完成 DEP 配置：

组织信息

- **业务部门**：输入将设备分配到的业务部门。 此字段为必填字段。
- **唯一服务 ID**：输入可选的唯一 ID。
- **支持电话号码**：输入支持电话号码，用户在设置期间可以拨打此号码寻求帮助。 此字段为必填字段。
- **支持电子邮件地址**：输入可选支持电子邮件地址。

注册设置

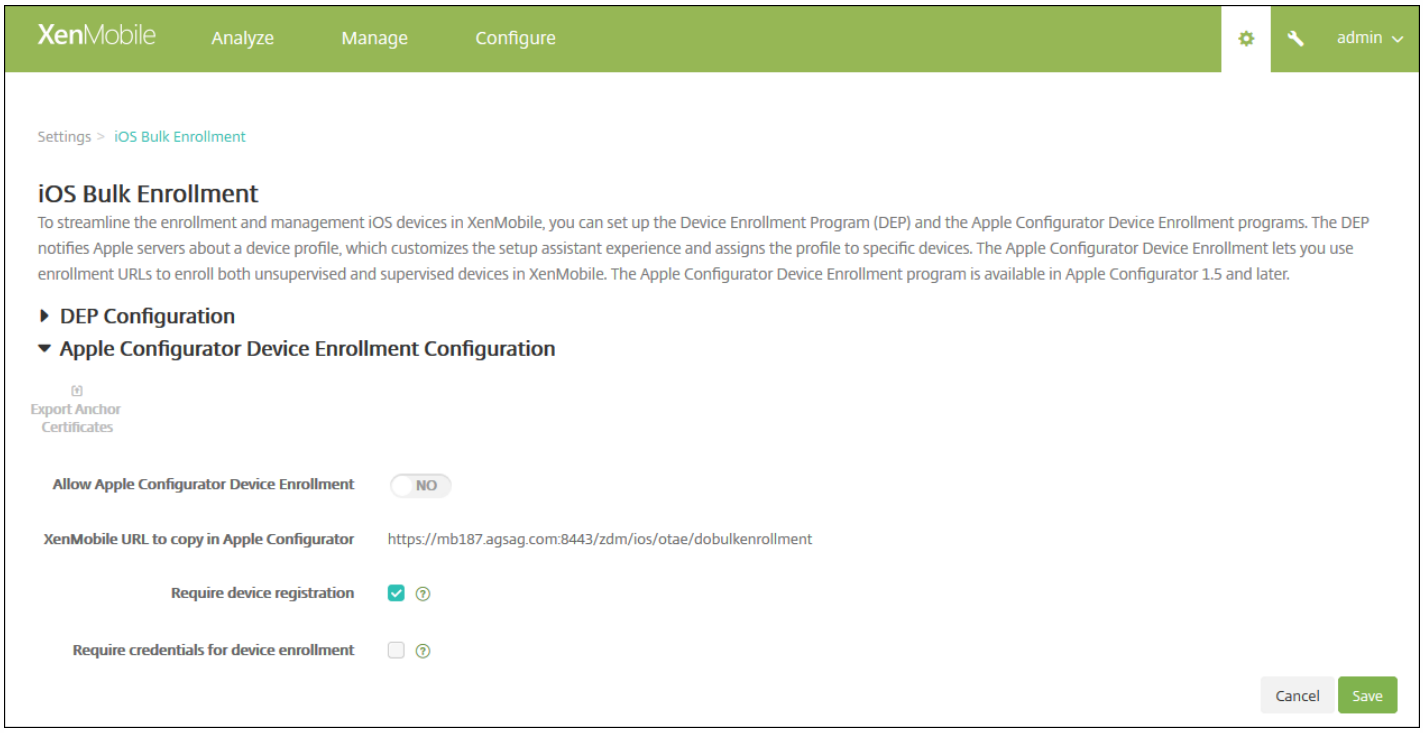
- **要求设备加密**：选择是否要求用户注册其设备。 默认要求注册。
- **受监督模式**：如果要使用 Apple Configurator管理 DEP 注册的设备或启用**等待完成配置设置**，则必须设置为**是**。 默认设置为**是**。 有关将 iOS 设备置于受监督模式的详细信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。
- **删除注册配置文件**：选择是否允许设备使用能够远程删除的配置文件。 默认设置为**拒绝**。
- **配对**：选择是否允许通过 DEP 注册的设备通过 iTunes 和 Apple Configurator 进行管理。 默认设置为**拒绝**。
- **需要提供凭据才能完成设备注册**：选择 DEP 设置过程中是否需要用户输入其凭据。 此选项适用于 iOS 7.1 及更高版本。 **注意**：当 DEP 打开以进行首次设置并且您未选中此选项时，将从头开始创建 DEP 组件（例如 DEP 用户、Worx Home、软件清单和 DEP 部署组）。 如果选择此选项，则不会创建这些组件，除非用户输入其凭据。 因此，如果您在以后清除此选项，则尚未输入其凭据的用户将无法执行 DEP 注册，因为这些 DEP 组件不存在。 在这种情况下，要添加 DEP 组件，应禁用并启用 DEP 帐户。
- **等待完成配置设置**：选择是否要求用户的设备一直保持在“设置助手”模式，直到将所有 MDM 资源部署到设备。 此选项适用于采用受监督模式的 iOS 9.0 及更高版本。
  - **注意**：Apple 文档指出，当设备处于“设置助手”模式时，以下命令可能无法使用：
    - InviteToProgram
    - InstallApplication
    - ApplyRedemptionCode
    - InstallMedia
    - RequestMirroring
    - DeviceLock

设置

选择用户在首次开始使用其设备时*不*需要执行的 iOS 设置助手步骤（即要跳过的步骤）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **定位服务**：在设备上设置定位服务。
- **Touch ID**：在 iOS 8.0 及更高版本的设备上设置 Touch ID。
- **通行码锁**：为设备创建通行码。
- **设置为新对象或还原**：将设备设置为新设备或从 iCloud 或 iTunes 备份设置设备。
- **从 Android 移动**：启用从 Android 设备向 iOS 9 或更高版本设备传递数据。 此选项仅在已选择**设置为新对象或还原**（即逃过此步骤）时可用。
- **Apple ID**：设置设备的 Apple ID 帐户。
- **条款和条件**：要求用户接受条款和条件才能使用设备。
- **Apple Pay**：在 iOS 8.0 及更高版本的设备上设置 Apple Pay。
- **Siri**：是否在设备上使用 Siri。
- **应用程序分析**：设置是否与 Apple 共享崩溃数据和使用统计信息。
- **显示缩放**：设置 iOS 8.0 或更高版本设备上的显示分辨率（标准或放大）。



1. 展开 **Apple Configurator Device Enrollment 配置**。

2. 将**启用 Apple Configurator Device Enrollment** 设置为**是**。

3. 注意并配置以下设置：

- **Apple Configurator 中要复制的 MDM 服务器 URL**：此只读字段是与 Apple 通信的 XenMobile 服务器的 URL，您需要在稍后执行的步骤中将该 URL 复制并粘贴到 Apple Configurator 中。 在 Apple Configurator 2 中，注册 URL 是 XenMobile 服务器的完全限定的域名 (FQDN) 或 IP 地址，如 mdm.server.url.com。
- **需要注册设备**：选择此设置要求您先手动或通过 CSV 文件将配置的设备添加到 XenMobile 中的**设备**选项卡，然后才能注册这些设备。 这样可确保无法注册未知设备。 默认设置为要求添加设备。
- **需要提供凭据才能完成设备注册**：注册时要求 iOS 7.1 及更高版本的设备用户输入其凭据。 默认不需要凭据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> 如果 XenMobile 服务器使用的是可信 SSL 证书，请跳过下一步。

4. 单击**导出定位证书**并将 certchain.pem 文件保存到 OS X 钥匙串（登录或系统）。

5. 启动 Apple Configurator，然后转至**准备 > 设置 > 配置设置**。

6. 在**设备注册**设置中，将步骤 4 中的 MDM 服务器 URL 粘贴到 Configurator 中的 **MDM 服务器 URL** 字段。

7. 如果 XenMobile 不使用可信 SSL 证书，请在**设备注册**设置中，将根证书颁发机构和 SSL 服务器证书颁发机构复制到**定位**证书中。

8. 使用 USB 电缆的基座接口将设备连接到运行 Apple Configurator 的 Mac，以便同时配置多达 30 台已连接的设备。 如果没有基座接口，请使用一个或多个有源 USB 2.0 高速集线器连接设备。

9. 单击**准备**。 有关通过 Apple Configurator 准备设备的详细信息，请参阅 Apple Configurator 帮助页面准备设备。

10. 在 Apple Configurator 中，配置所需的设备策略。

11. 在配置每个设备的过程中，请将其打开以启动 iOS 设置助理，以便为首次使用准备好设备。

续订 XenMobile 安全套接字层 (SSL) 证书时，请在 XenMobile 控制台的**设置** > **证书**中上载新证书。 在“导入”对话框的**用作**中，请务必单击 **SSL 侦听器**，以便将该证书用于 SSL。 重新启动服务器后，XenMobile 将使用新 SSL 证书。 有关 XenMobile 中的证书的详细信息，请参阅升级 XenMobile 中的证书。

续订或更新 SSL 证书时，不需要在 Apple DEP 与 XenMobile 之间重新建立信任关系。 但是，可以按照本文中之前的步骤随时重新配置 DEP 设置。

有关 Apple DEP 的详细信息，请参阅 Apple 文档。

有关与此配置有关的已知问题和解决方案的信息，请参阅 XenMobile 服务器 10.3 已知问题。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通过 Apple DEP 部署 iOS 设备

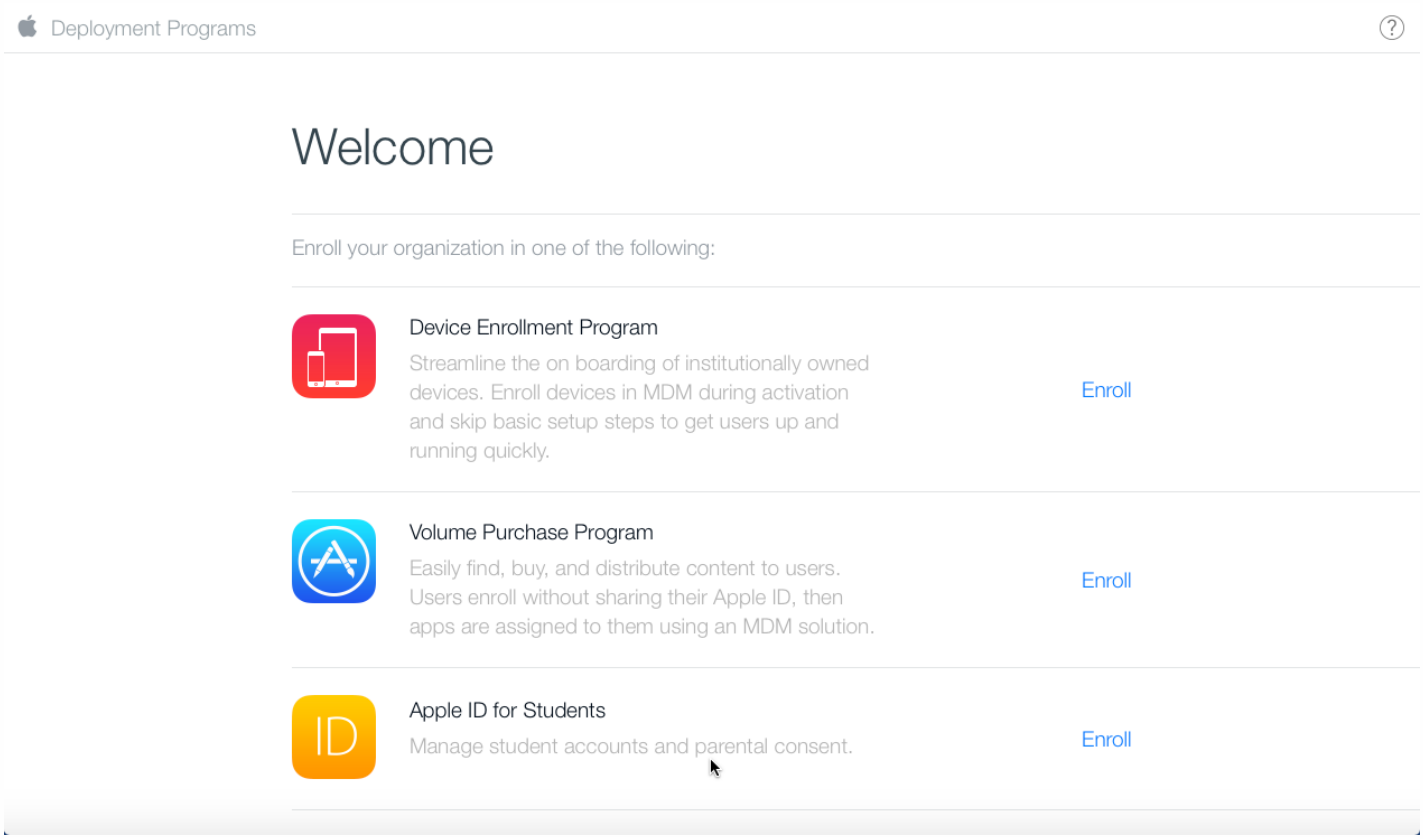
Aug 11, 2016

您需要使用 Apple Developer Enterprise Program (DEP) 帐户才能在 XenMobile 中利用 Apple DEP 进行 IOS 设备注册和管理。组织注册参加 Apple DEP 需要满足的主要要求如下。

- 工商企业或社会公共机构的电话号码和电子邮件地址
- 证明人
- 工商企业或社会公共机构的信息（DUNS/税号）
- Apple 客户编号

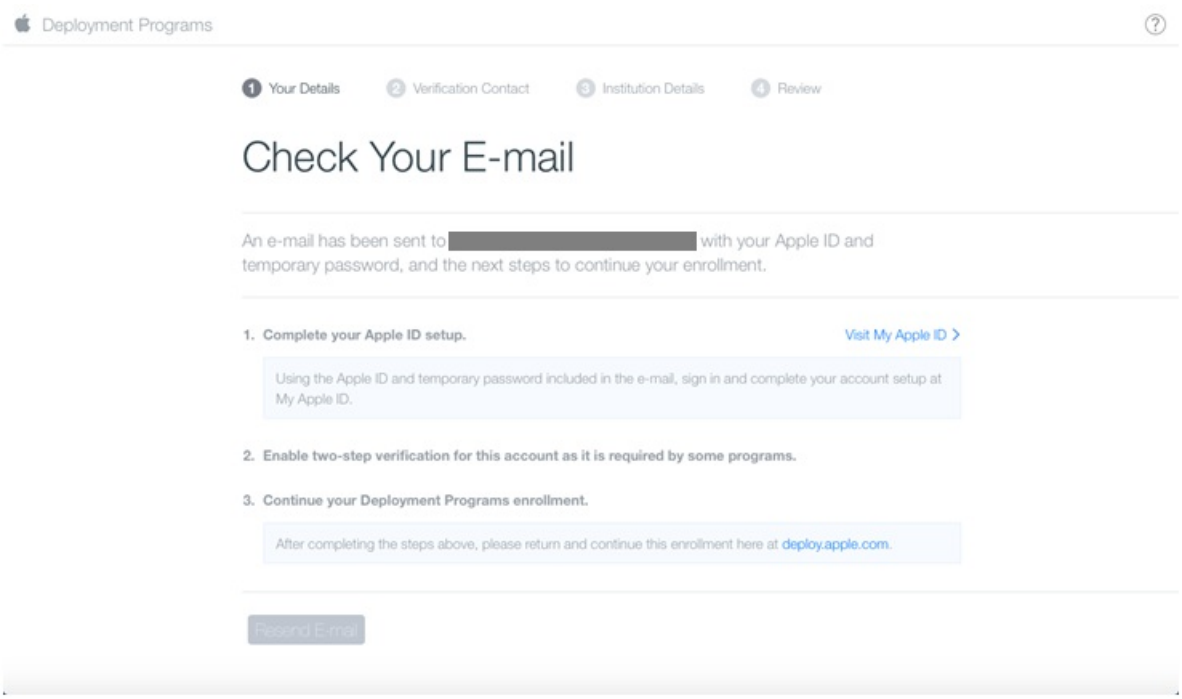
有关 Apple DEP 的详细信息，请参阅 Apple 发布的 PDF。 强调 Apple DEP 适用于组织但不适用于个人，这一点非常重要。 此外，请务必记住需要提供大量企业详细信息才能创建 Apple DEP，这一点也非常重要，这意味着客户需要花费一定的时间来申请帐户并获得批准。

申请 DEP 帐户时，最佳做法是使用与组织绑定的电子邮件地址，例如 dep@company.com。

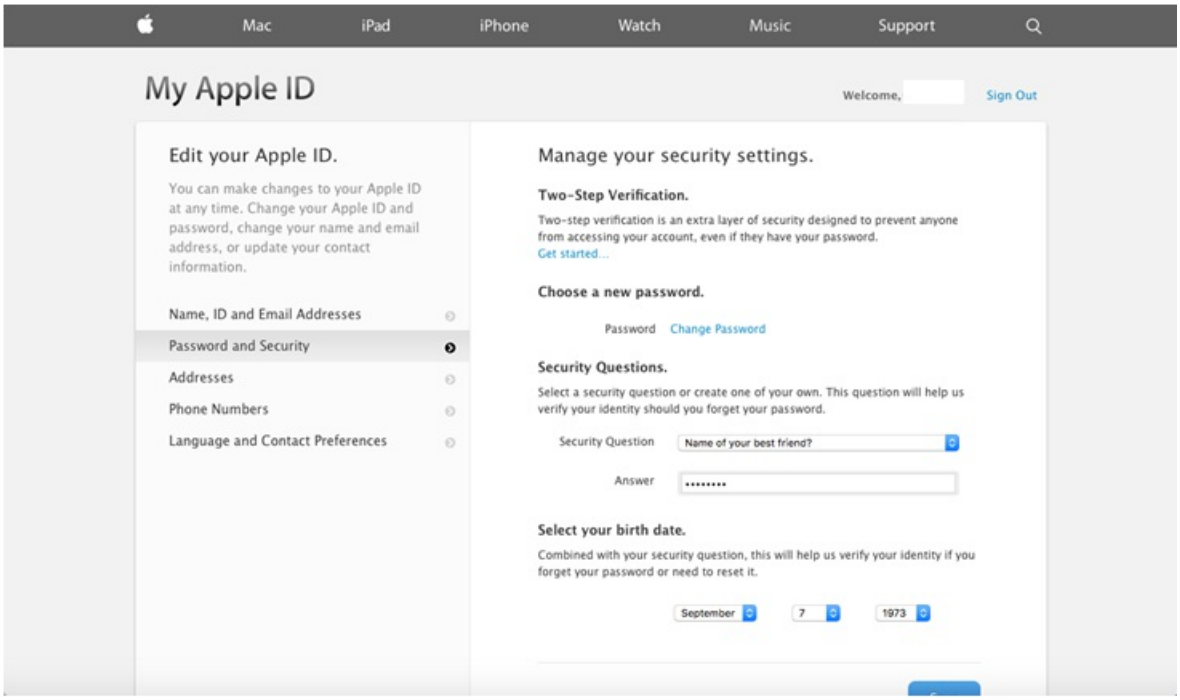


1. 输入组织信息后，应通过电子邮件收到新 Apple ID 的临时密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

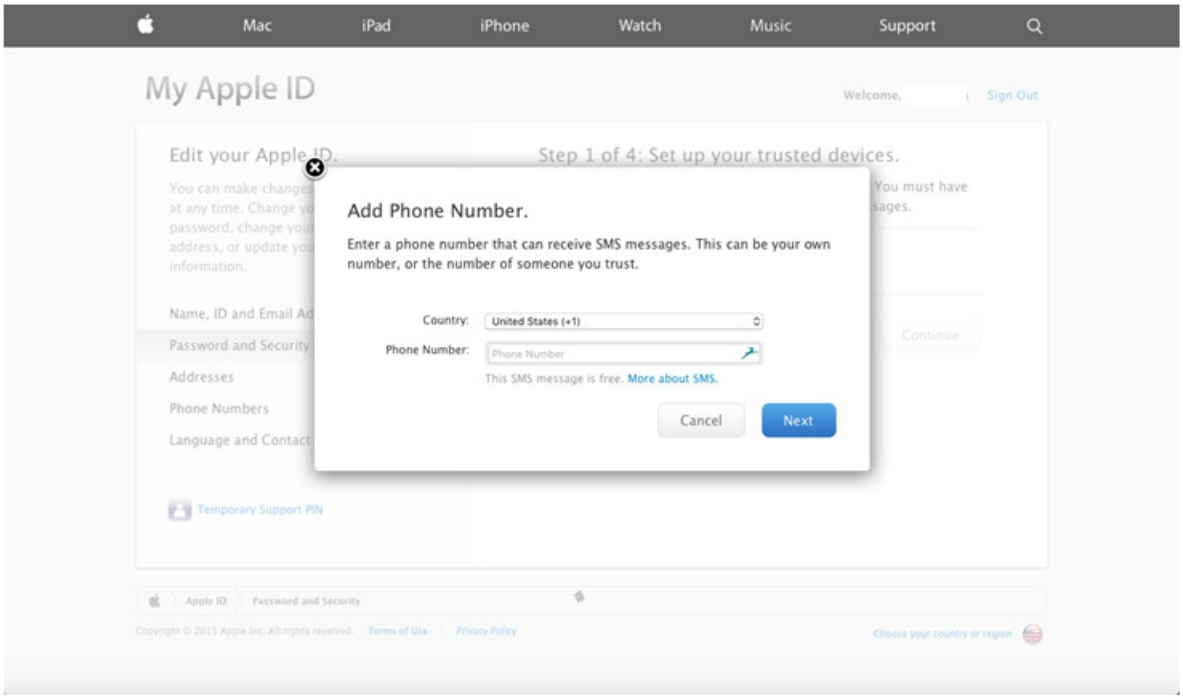


2. 随后请使用 Apple ID 进行注册并完成帐户的安全设置。

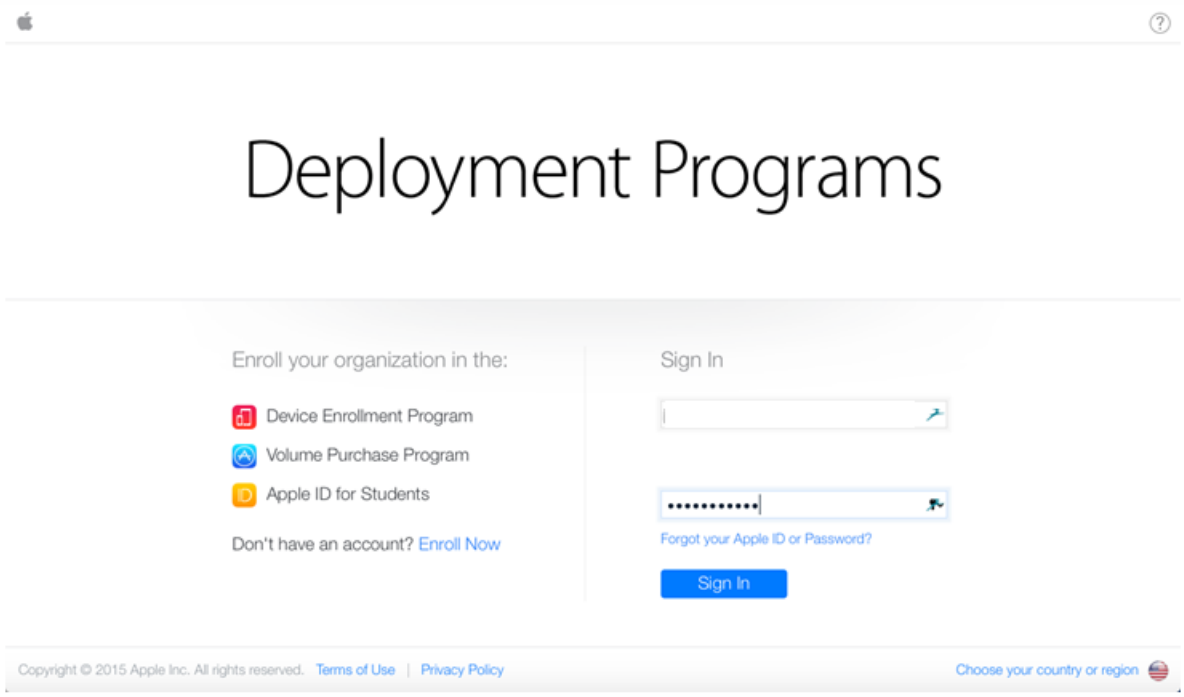


3. 配置并启用双重验证（需要对 DEP 门户使用该验证方法）。 执行这些步骤过程中，需要添加一个电话号码，您会通过该电话号码收到用于双重验证的 4 位数 PIN 码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

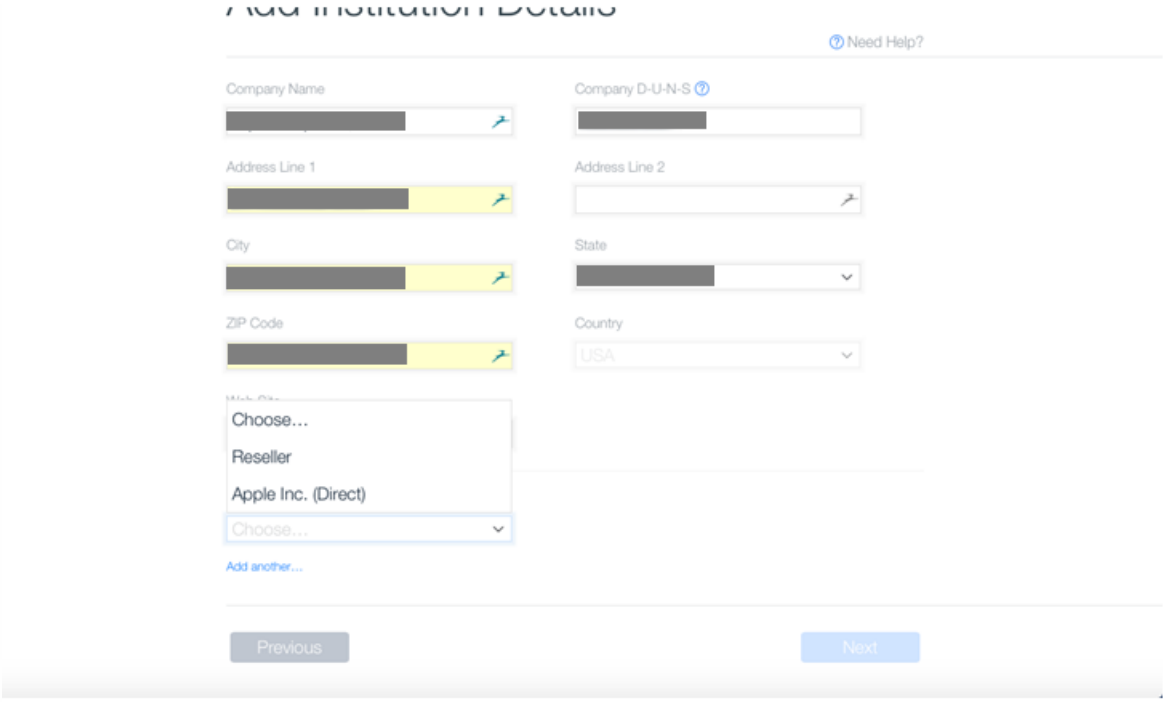


4. 登录 DEP 门户以使用刚刚设置的双重验证完成帐户配置。

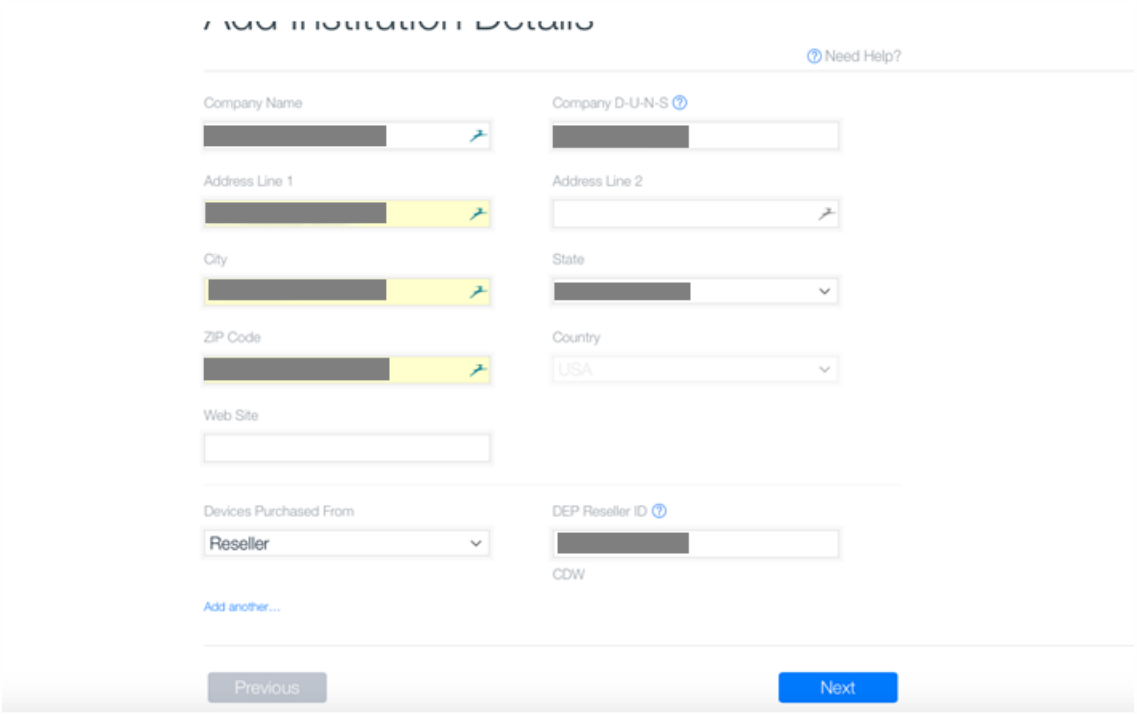


5. 添加您的公司详细信息，然后选择购买设备的地点。 有关购买选项的详细信息，请参阅下一部分内容，即订购启用了 DEP 的设备。

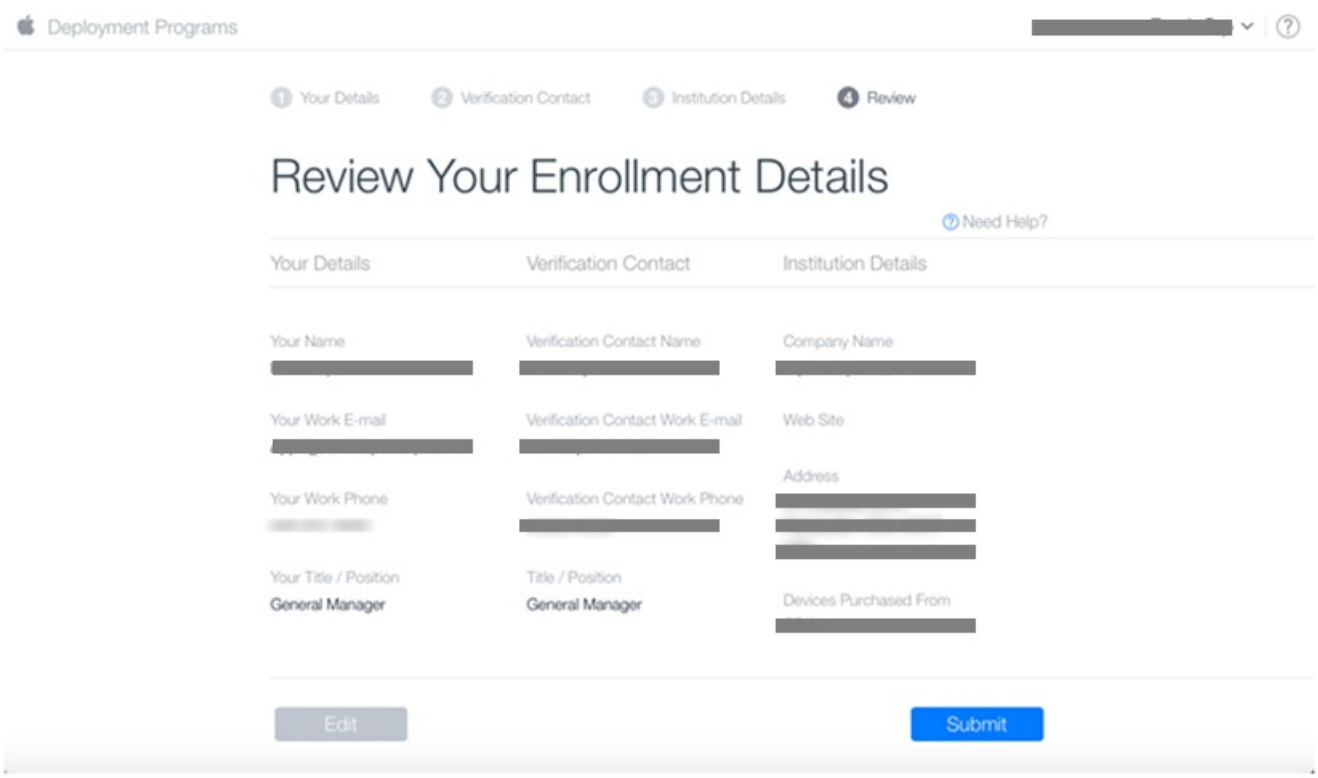
© 1999-2017 Citrix Systems, Inc. All rights reserved.



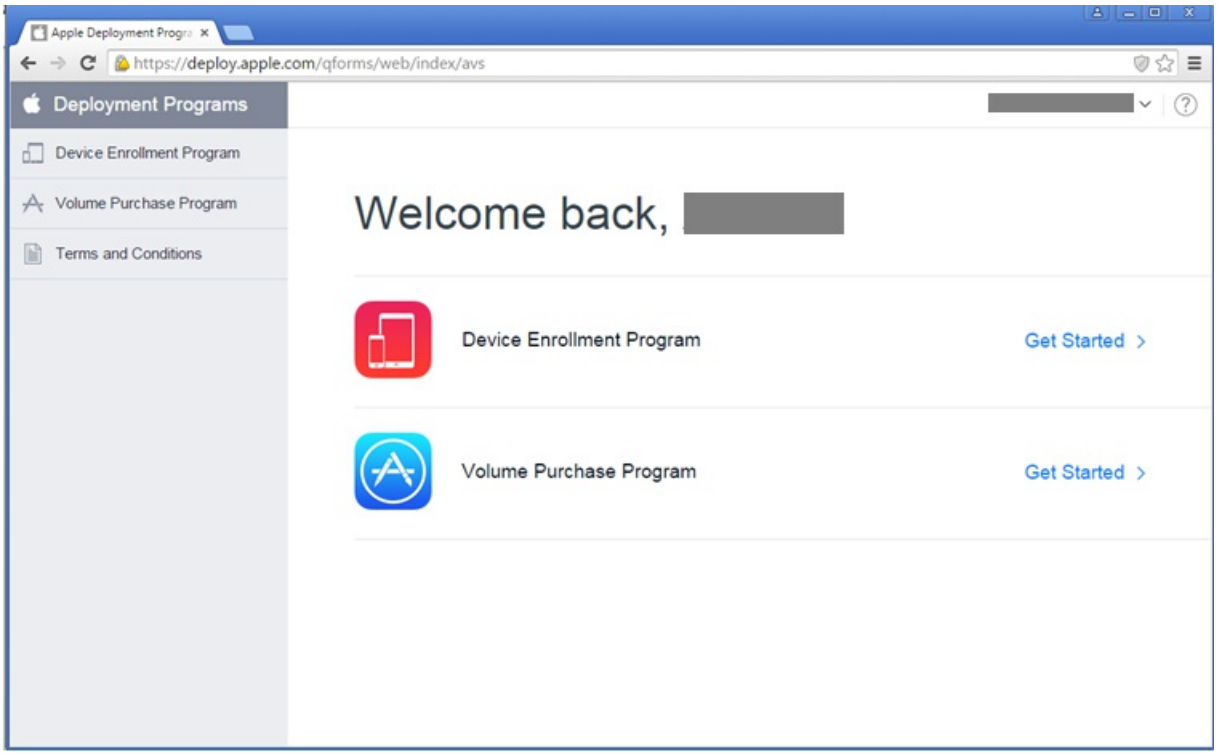
6. 添加 Apple 客户编号或 DEP 经销商 ID，然后验证注册详情并等待 Apple 审批您的帐户。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



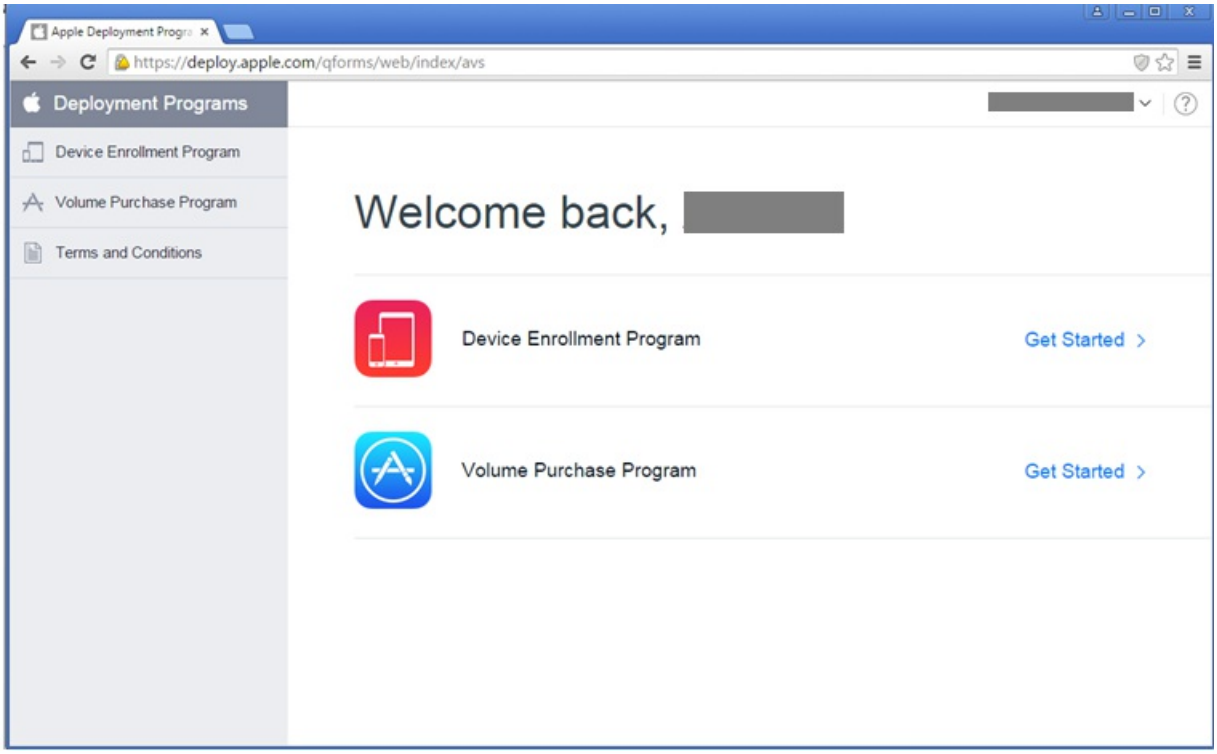
7. 收到 Apple 发送的登录凭据后，登录 Apple DEP 门户。 然后，请按照下一部分中所述的步骤将您的帐户与 XenMobile 建立连接。



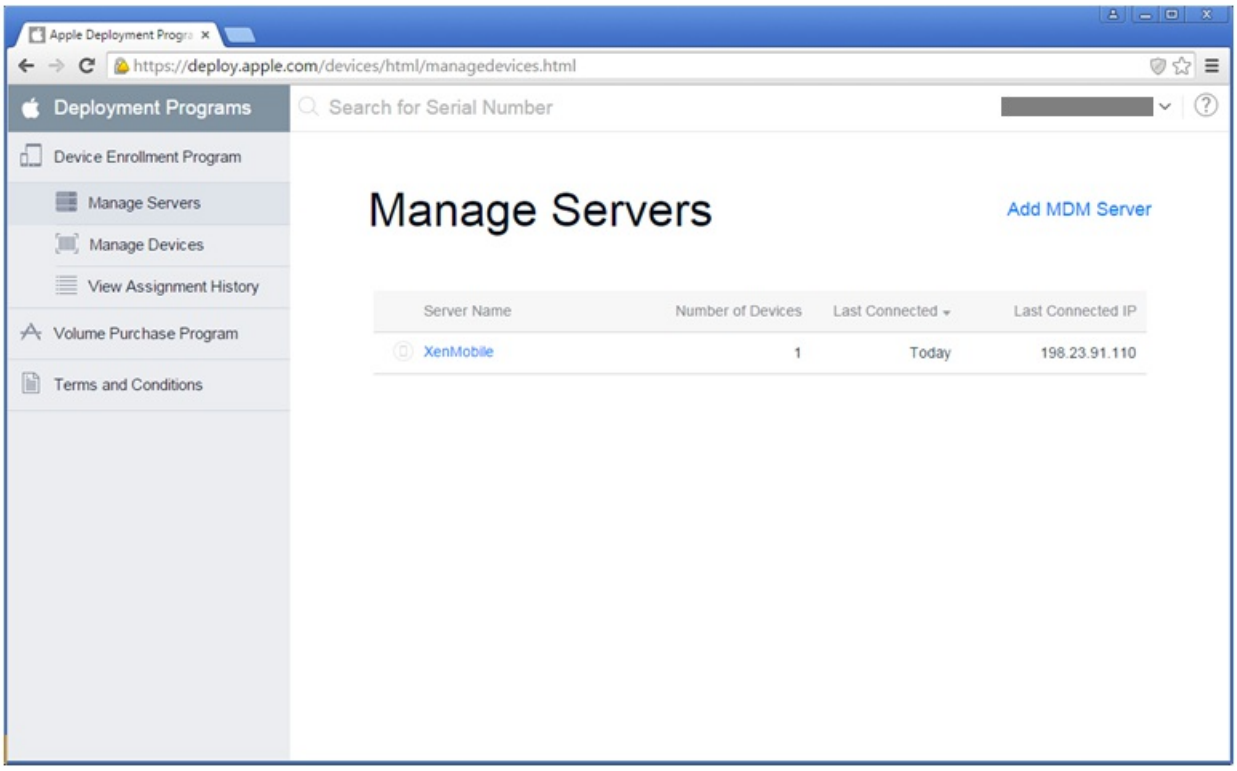
© 1999-2017 Citrix Systems, Inc. All rights reserved.

请按照本部分中所述的步骤将您的 Apple DEP 帐户与 XenMobile 服务器部署相连接。

1. 在 Apple DEP 门户的左侧，单击 **Device Enrollment Program**。

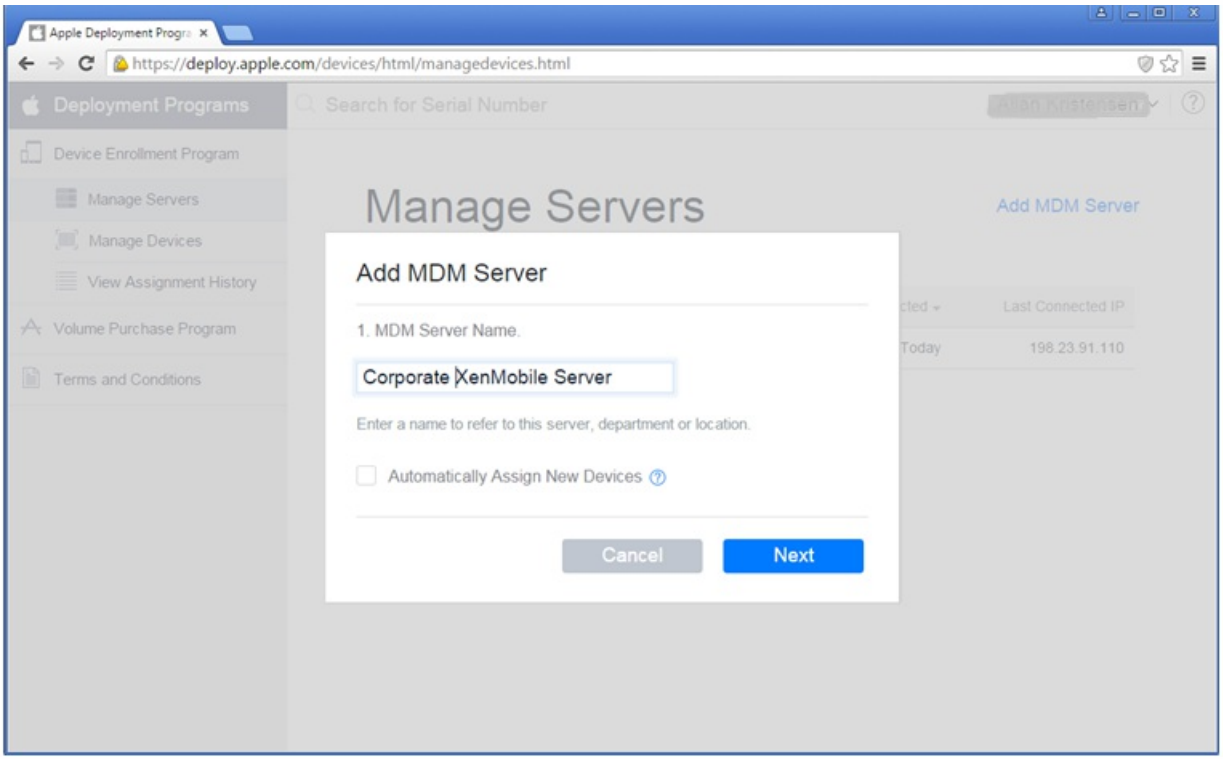


2. 单击 **Manage Servers**（管理服务器），然后单击右侧的 **Add MDM Server**（添加 MDM 服务器）。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

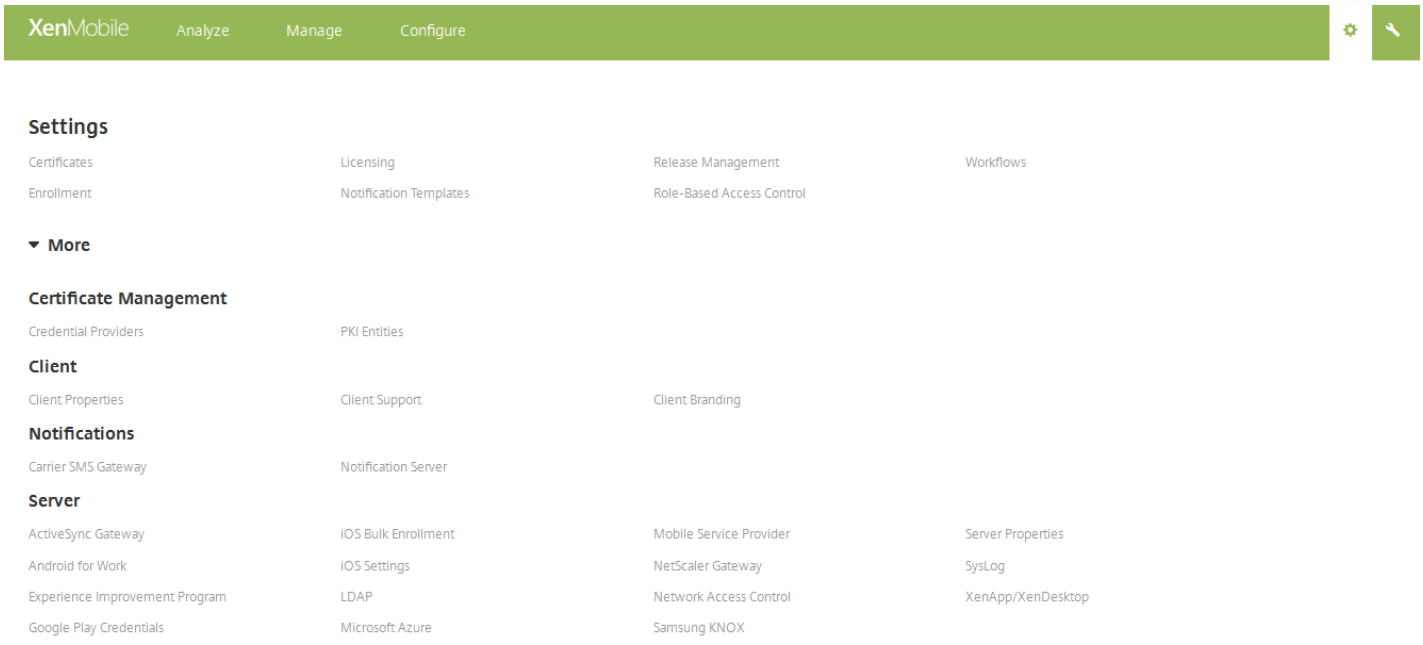
3. 在 **Add MDM Server**（添加 MDM 服务器）中，输入 XenMobile 服务器的名称，然后单击 **Next**（下一步）。



4. 从 XenMobile 服务器上载公钥。 要从 XenMobile 生成公钥，请执行以下操作：

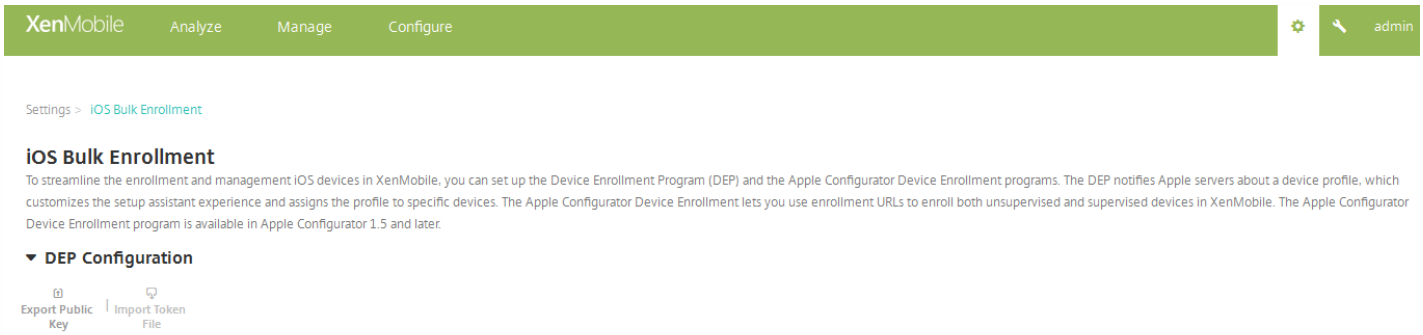
a. 在 XenMobile 控制台中，单击右上角的齿轮图标。 此时将显示**设置**页面。

b. 在**更多**下，单击 **iOS 批量注册**。

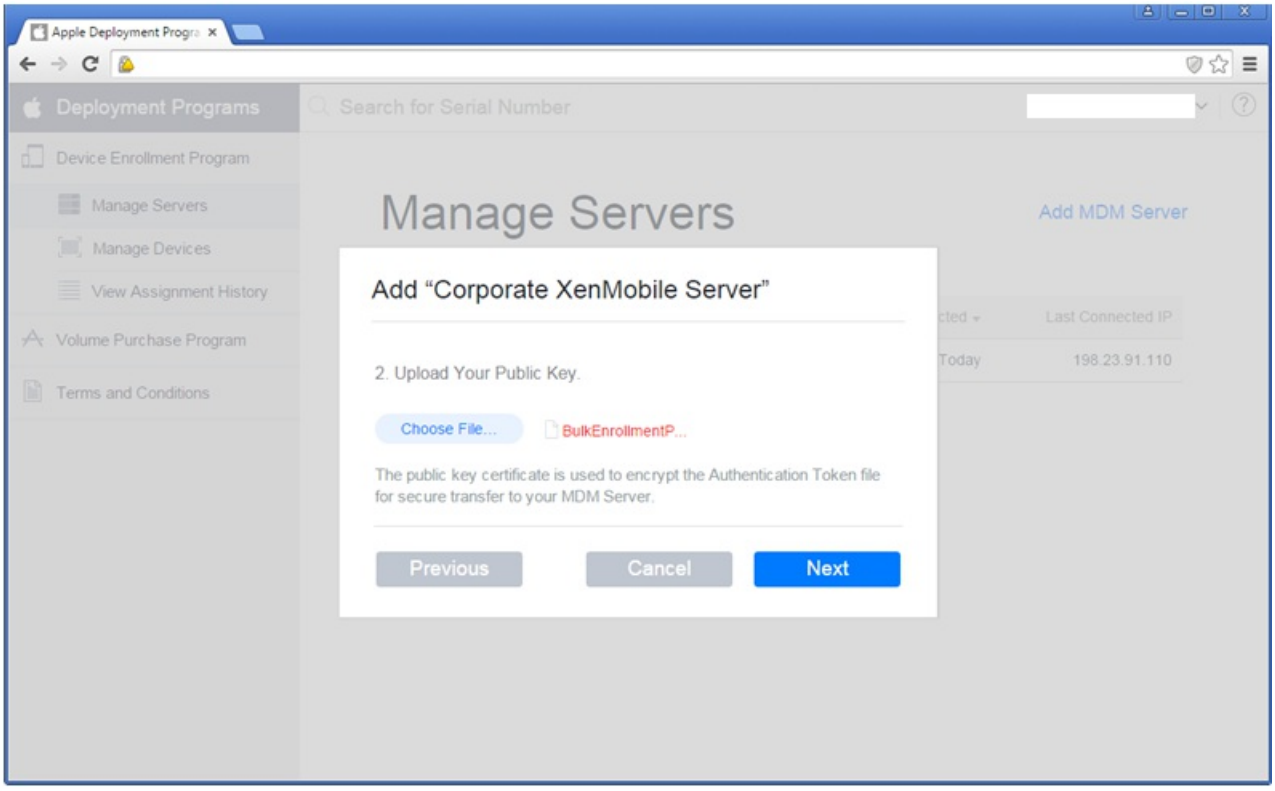


b. 在 **iOS 批量注册**页面上，展开 **DEP 配置**，然后单击**导出公钥**。 此时将下载公钥。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

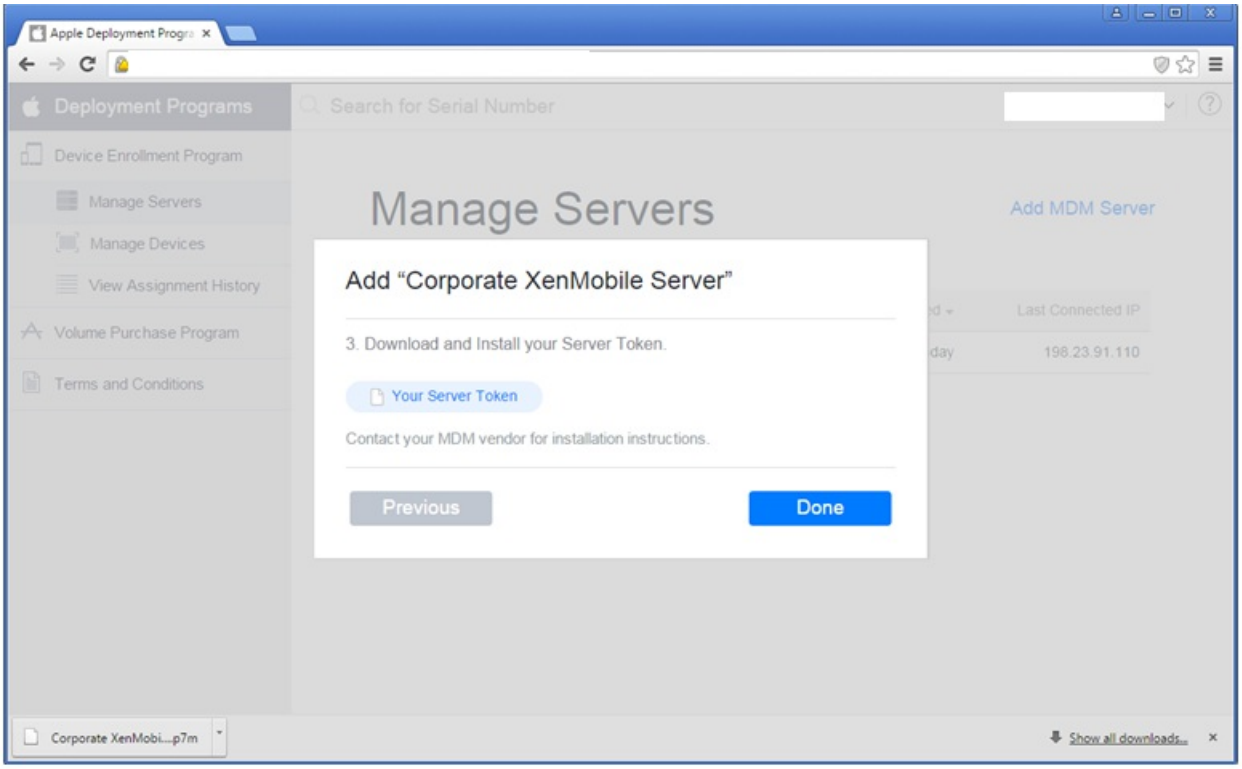


5. 在 Apple DEP 门户上，单击 **Choose file**（选择文件）选择刚刚下载的公钥，然后单击 **Next**（下一步）。

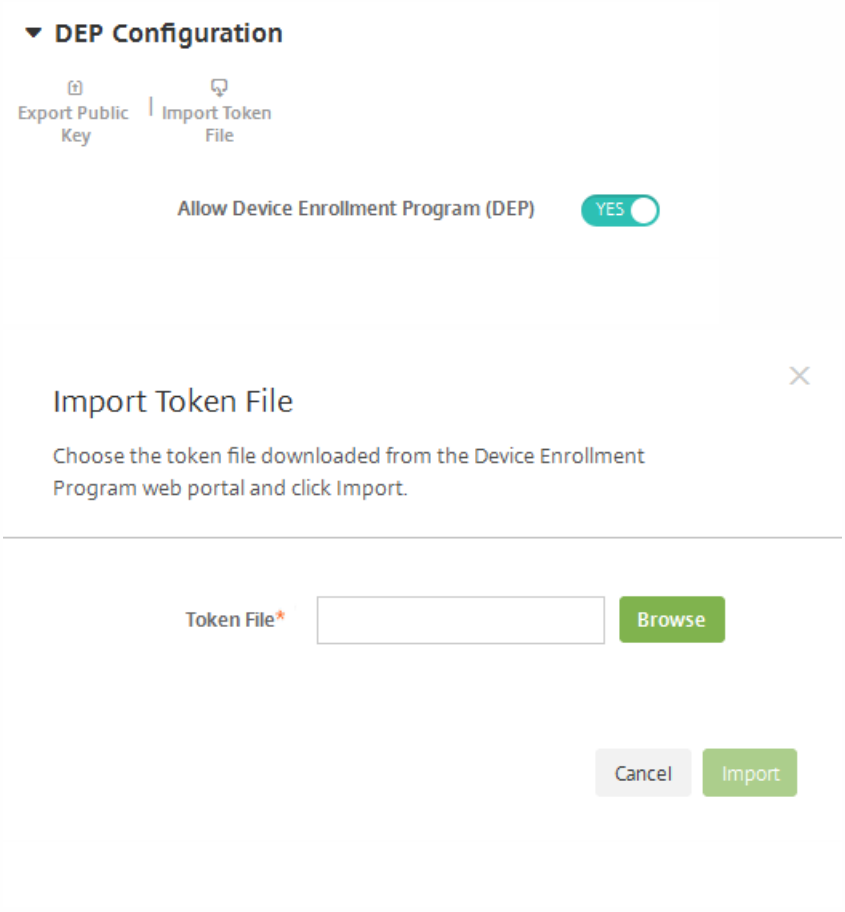


6. 单击 **Your Server Token**（您的服务器令牌）生成一个服务器令牌（可以从浏览器下载），然后单击 **Done**（完成）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



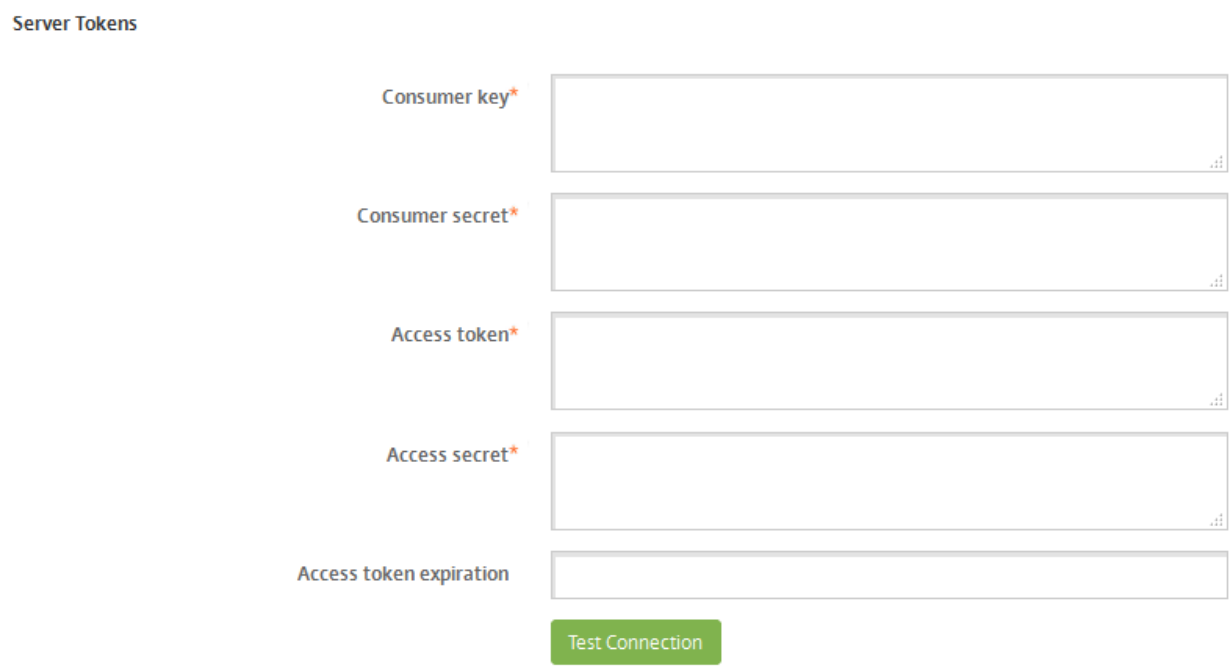
7. 在 XenMobile 控制台的 **iOS 批量注册**页面上，在**允许加入 Device Enrollment Program (DEP)** 旁边单击“是”，单击**导入令牌文件**，然后上载您在上一步中下载的令牌文件。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

导入令牌文件后，您的 Apple DEP 令牌信息将在 XenMobile 控制台中显示。

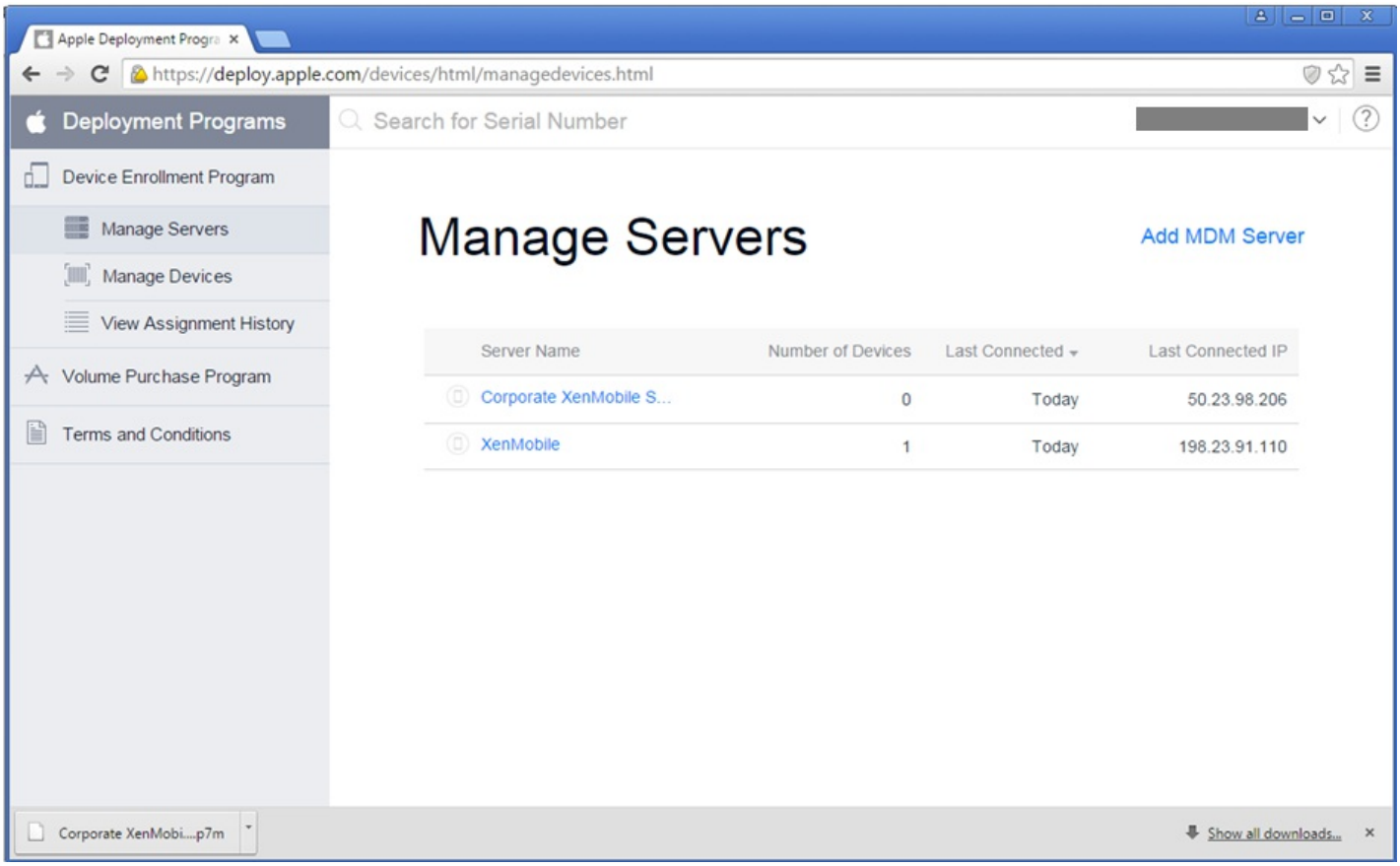
8. 单击**测试连接**验证 Apple DEP 与 XenMobile 的连接。



9. 在 **iOS 批量注册**页面上，完成其他步骤，选择要对您的 Apple DEP 设备实施的 Apple DEP 控制和策略，然后单击**保存**。

XenMobile 服务器将在 Apple DEP 门户中显示。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



可以直接从 Apple 或启用了 DEP 的授权经销商或运营商处订购启用了 DEP 的设备。 要从 Apple 订购，需要在 Apple DEP 门户内部提供 Apple 客户 ID 以允许 Apple 将您购买的设备与您的 Apple DEP 帐户相关联。

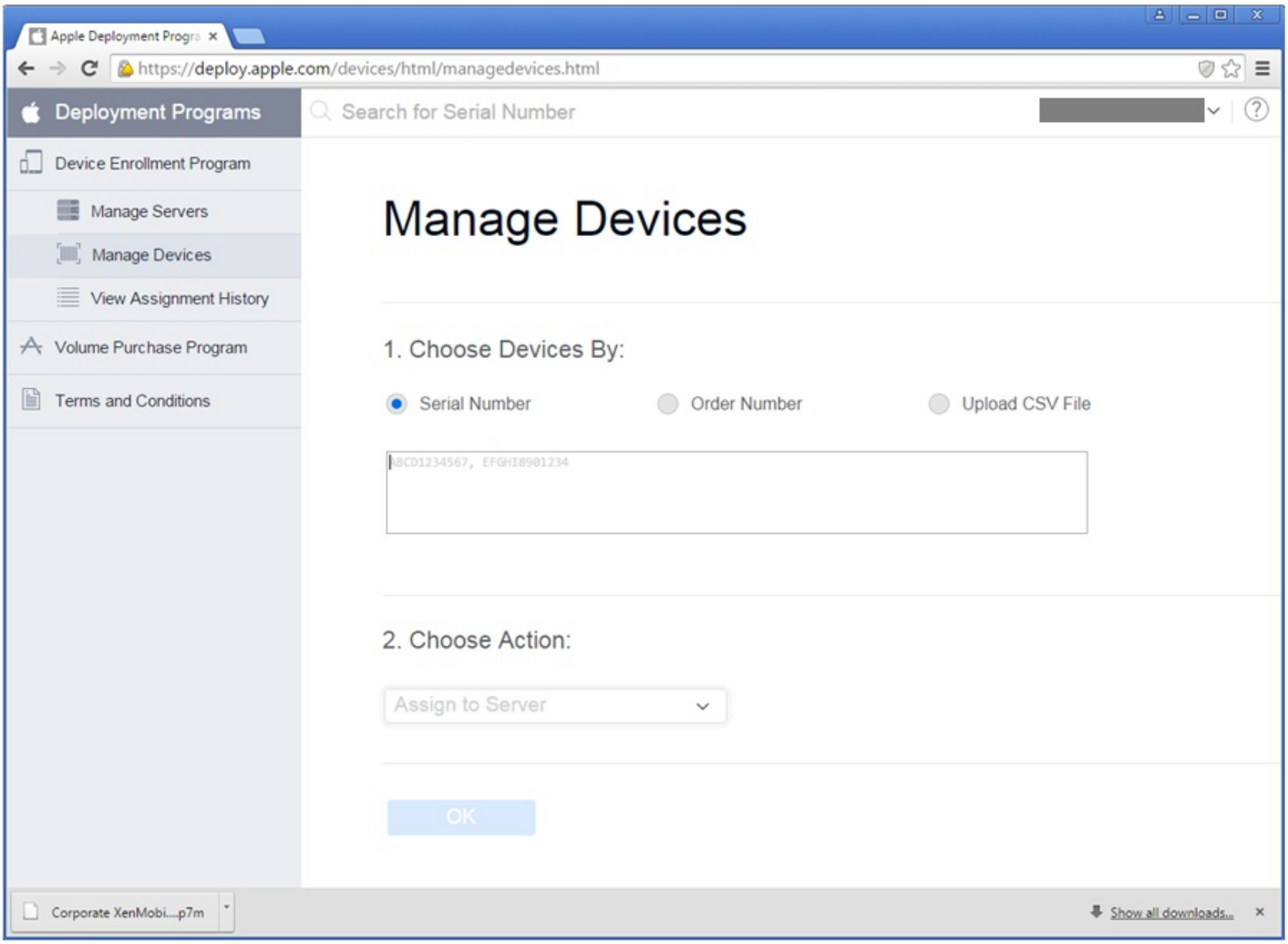
要从经销商或运营商处订购，请联系 Apple 经销商或运营商，确认其是否加入了 Apple DEP。 购买设备时，请要求经销商提供其 Apple DEP ID。 需要提供此信息才能将您的 Apple DEP 经销商添加到您的 Apple DEP 帐户。 如果已获批准，您在添加经销商的 Apple DEP ID 后会收到 DEP 客户 ID。 请向经销商提供 DEP 客户 ID，经销商将使用该 ID 将您购买的设备的相关信息提交给 Apple。 有关详细信息，请参阅 Apple Web 站点。

请按照以下步骤通过 DEP 门户在您的 Apple DEP 帐户内将设备与 XenMobile 服务器相关联。

1. 登录 Apple DEP 门户。

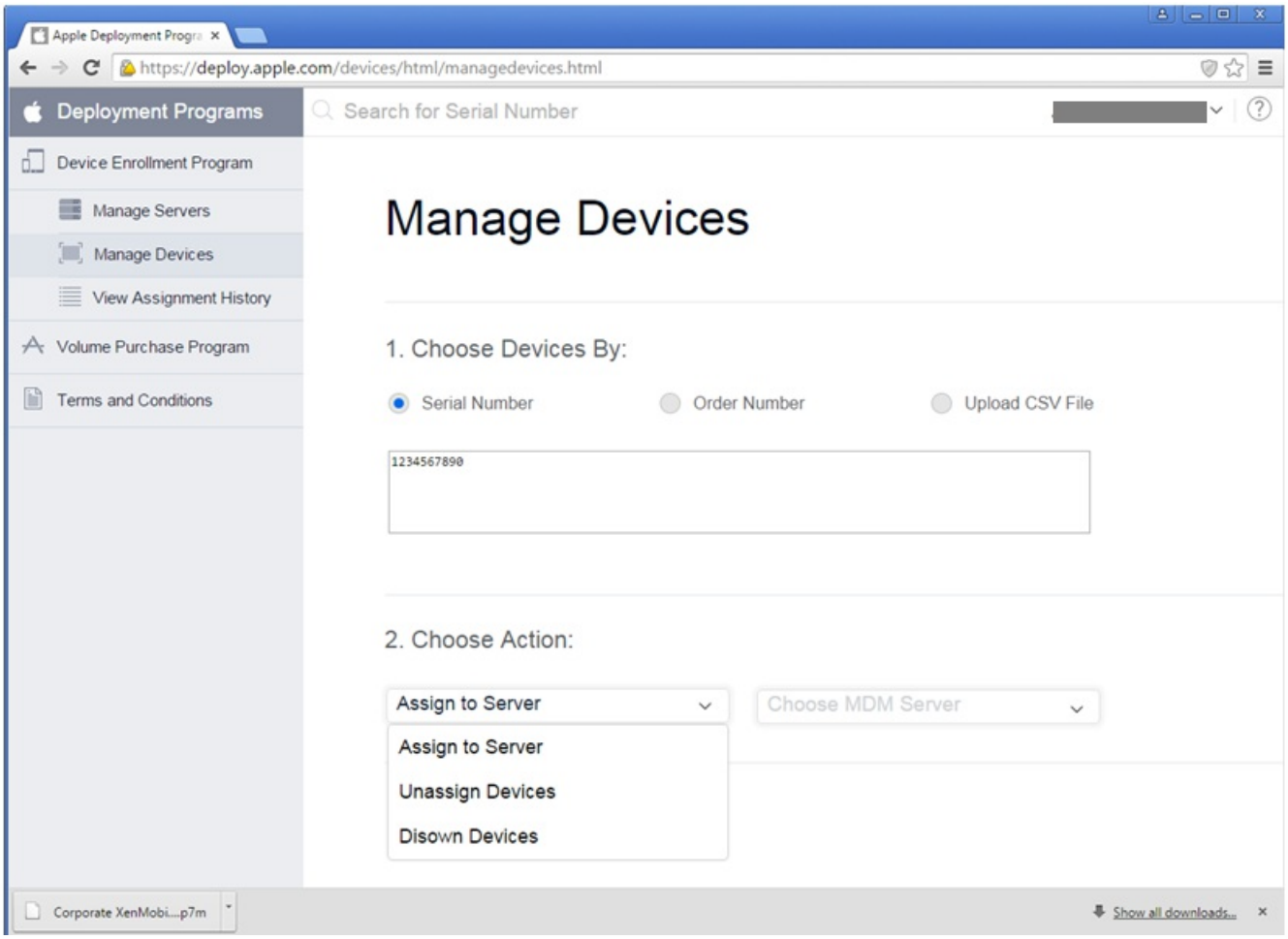
2. 单击 **Device Enrollment Program** 和 **Manage Devices**（管理设备），然后在 **Choose Devices By**（选择设备依据）中，选择上载并定义启用了 Apple DEP 的设备时使用的选项，即 **Serial Number**（序列号）、**Order Number**（订单号）或 **Upload CSV File**（上载 CSV 文件）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

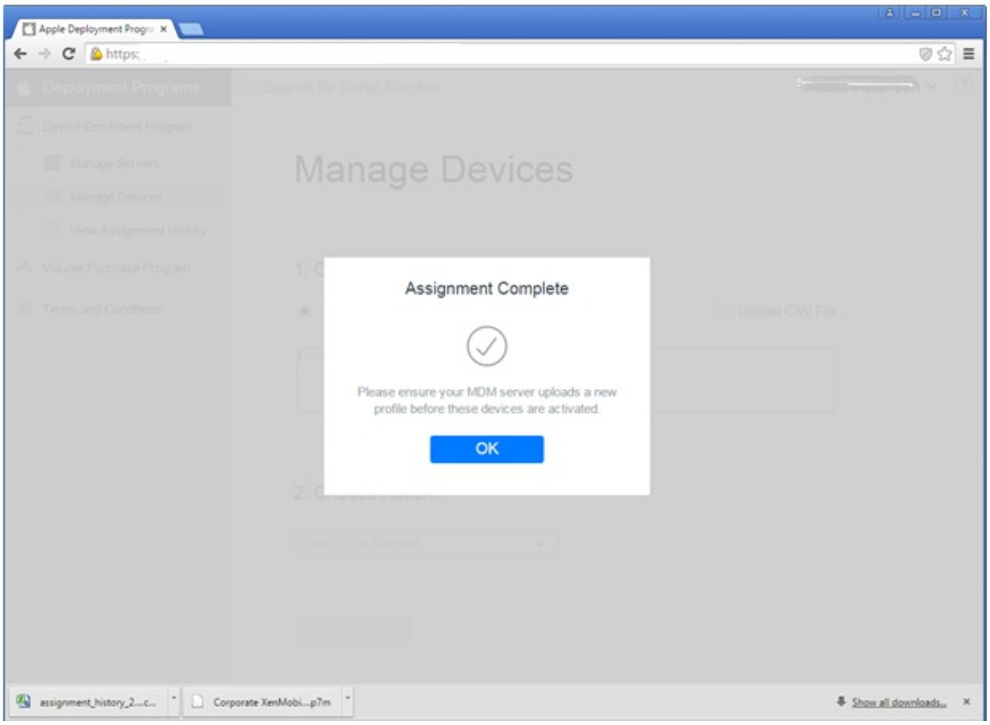


3. 在 **Choose Action**（选择操作）下，要将您的设备分配给 XenMobile 服务器，请单击 **Assign to Server**（分配给服务器），在列表中单击 XenMobile 服务器的名称，然后单击 **OK**（确定）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



您的 Apple DEP 设备现在已与选定的 XenMobile 服务器相关联。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

用户注册启用了 Apple DEP 的设备时，其体验如下。

1. 用户启动启用了 Apple DEP 的设备。

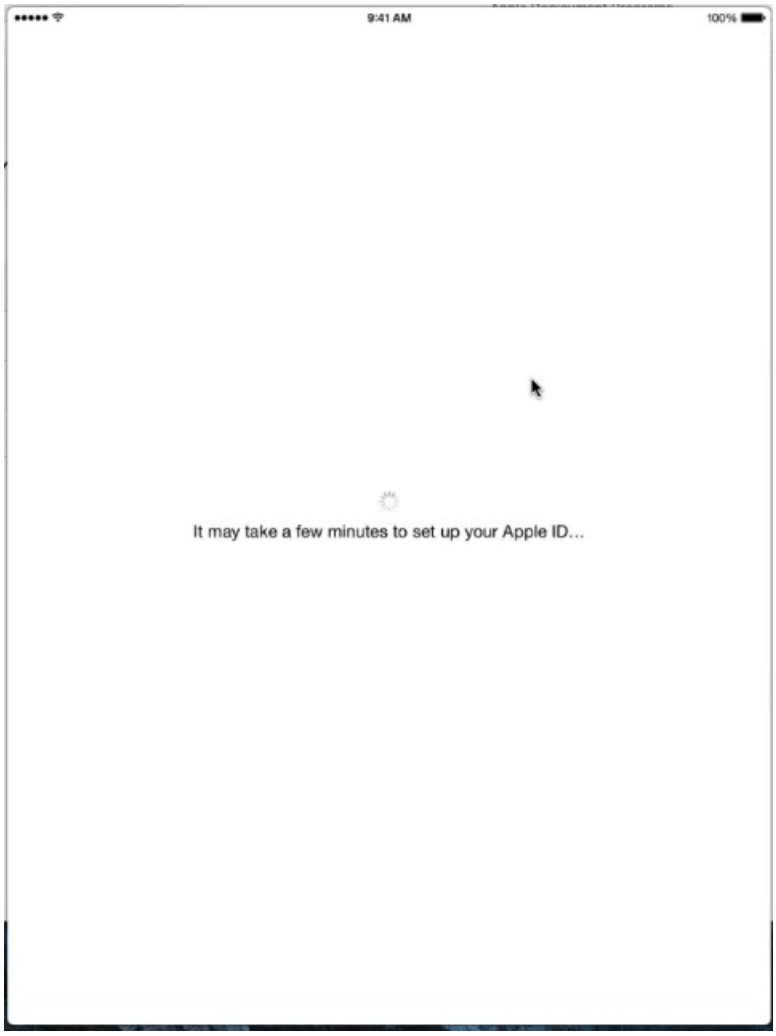
2. 使用配置向导在其 iOS 设备上配置初始设置。

3. 该设备将自动启动 XenMobile 设备注册过程。 用户按照向导进行操作，将其设备注册到与启用了 Apple DEP 的设备关联的 XenMobile 服务器。

Apple DEP 注册过程作为启用了 Apple DEP 的设备的初始 IOS 配置流程的一部分自动启动。

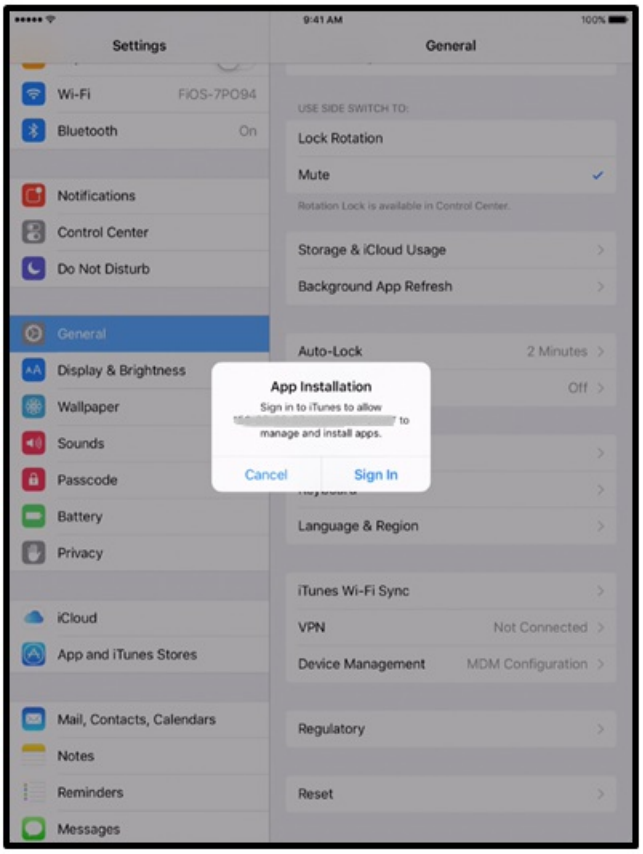
4. 您在 XenMobile 控制台中配置的 Apple DEP 配置交付给启用了 Apple DEP 的设备。 用户按照向导配置设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 系统可能会提示用户登录 iTunes 以便能够下载 Worx Home。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 用户打开 Worx Home 并输入其凭据。 如果策略要求，系统可能还会提示用户创建并验证 Worx PIN。

需要使用的其余应用程序将向下推送到设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

iOS Volume Purchase Plan 设置

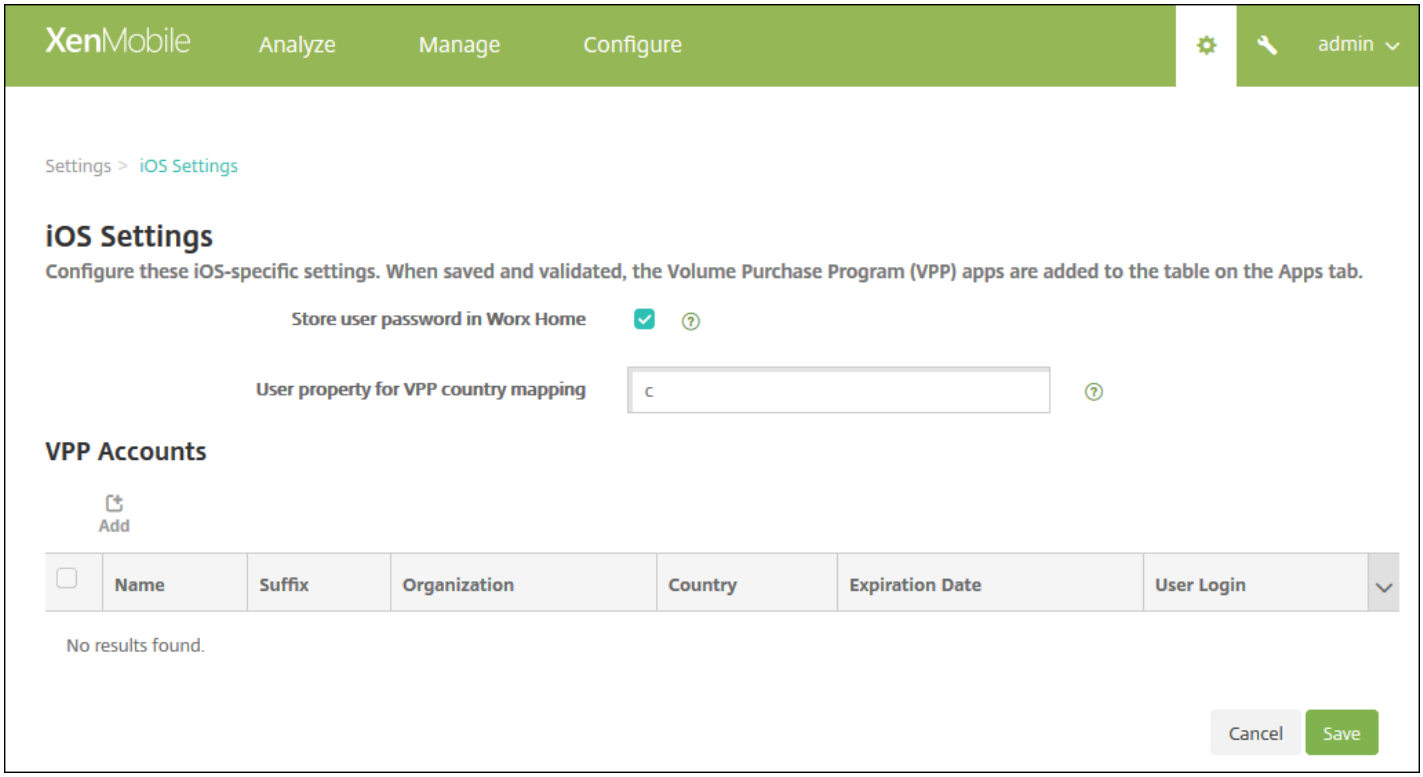
Aug 11, 2016

可以在 XenMobile 中配置特定于 iOS Volume Purchase Plan (VPP) 的设置。 iOS VPP 简化了组织批量查找、购买和分发应用程序及其他数据的过程。 VPP 为管理组织的内容需求提供可扩展的简化解决方案。

在 XenMobile 中保存并验证 iOS VPP 设置后，购买的应用程序将添加到 XenMobile 控制台“应用程序”选项卡上的表格中。

1. 在 XenMobile Web 控制台中，单击右上角的齿轮图标。 此时将显示**设置**页面。

2. 在**服务器**下面，单击 **iOS 设置**。 此时将显示 **iOS 设置**配置页面。



3. 配置以下设置：

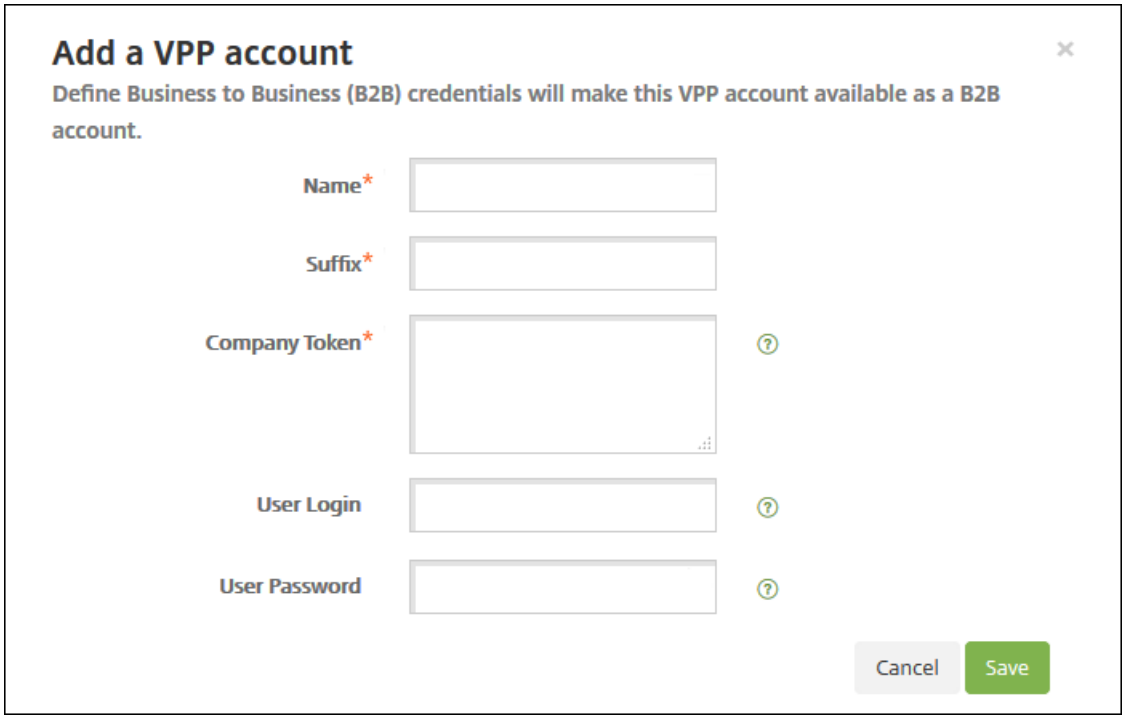
- **在 Worx Home 中存储用户密码**：选择是否将用户名和密码安全地存储在 Worx Home 中，用于 XenMobile 身份验证。 默认情况下存储此信息。
- **Volume Purchasing Program (VPP)国家/地区映射的用户属性**：键入代码以允许用户从特定于国家/地区的应用商店下载应用程序。

  此映射用于选择 VPP 的属性池。 例如，如果用户属性是美国，若应用程序的 VPP 代码分布于英国，则此用户无法下载该应用程序。 请联系您的 VPP 计划管理员，以了解关于国家/地区映射代码的更多信息。

VPP 帐户

- 对于要添加的每个 VPP 帐户 ，请单击**添加**。 此时将显示**添加 VPP 帐户**对话框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



为要添加的每个帐户配置以下设置：

- **名称**：键入 VPP 帐户名称。
- **后缀**：键入通过 VPP 帐户获取的应用程序上显示的后缀。
- **公司令牌**：键入或复制并粘贴从 Apple 获取的 VPP 服务令牌。 要获取令牌，请在 Apple VPP 门户的“Account Summary”（帐户摘要）页面中，单击“Download”（下载）按钮以生成并下载 VPP 文件。 此文件包含服务令牌及其他信息，如国家/地区代码和过期日期。 将此文件保存在安全的位置。
- **用户登录名**：键入经过授权的可选 VPP 帐户 用户名。
- **用户密码**：键入可选的 VPP 帐户用户密码。

5. 单击**保存**以关闭对话框。

6. 单击**保存**以保存 iOS 设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

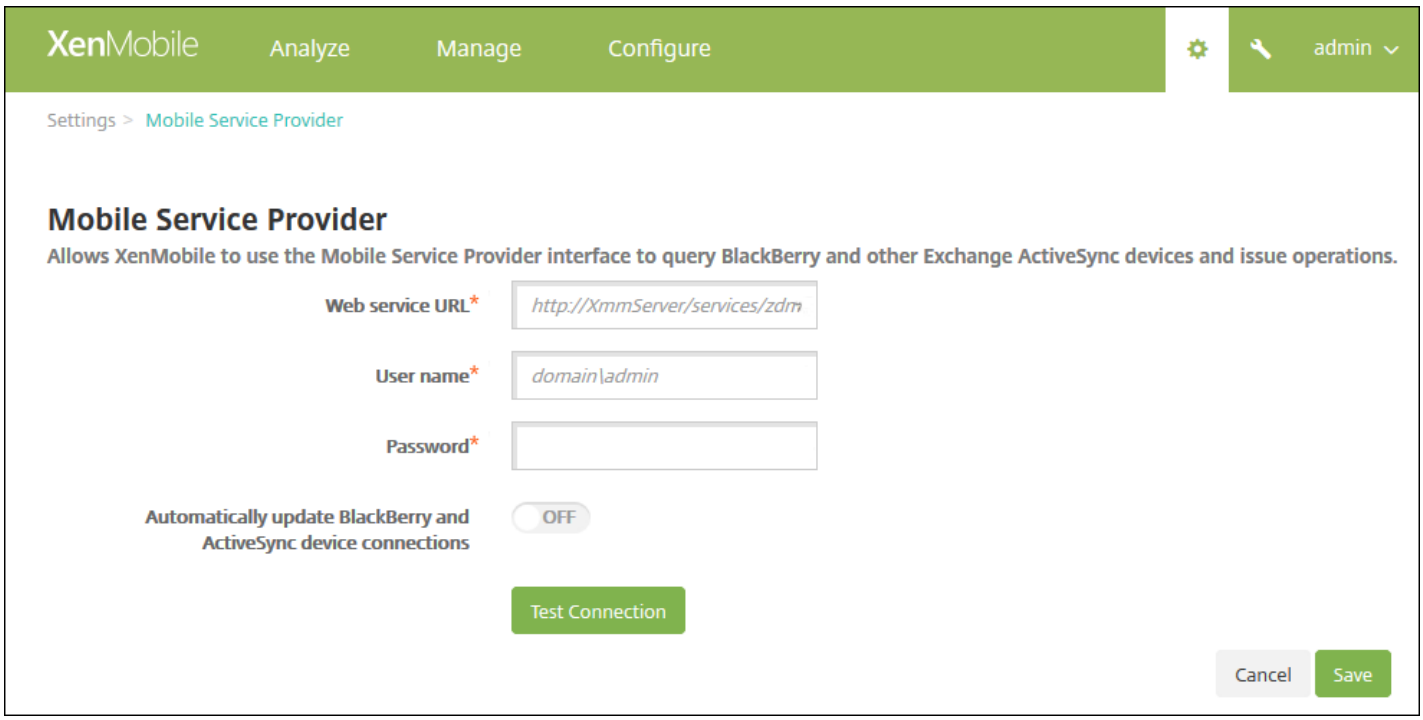
移动服务提供商

Aug 11, 2016

可以启用 XenMobile 以使用移动服务提供商界面来查询黑莓和其他 Exchange ActiveSync 设备并对设备发出操作。

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

2. 在**服务器**下，单击**移动服务提供商**。 此时将显示**移动服务提供商**页面。



3. 配置以下设置：

- **Web 服务 URL**：键入 Web 服务的 URL，例如，http://XmmServer/services/xdmservice
- 用户名：采用 domain\admin 格式键入用户名。
- **密码**：键入密码。
- **自动更新 BlackBerry 和 ActiveSync 设备连接**：选择是否自动更新设备连接。 默认值为**关**。
- 单击**测试连接**以验证连接性。

4. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

网络访问控制

Aug 11, 2016

如果已在网络中设置了网络访问控制 (NAC) 设备（如 Cisco ISE），则在 XenMobile 中，可以启用过滤器以根据规则或属性设置设备的 NAC 兼容性。 如果 XenMobile 中的托管设备不满足特定条件，并因此被标记为“不合规”，NAC 设备将在您的网络上阻止此设备。

在 XenMobile 控制台中，从列表中选择一个或多个条件，以将设备设为“不合规”。

XenMobile 支持以下 NAC 合规性过滤器：

匿名设备：检查设备是否处于匿名模式。 如果在设备尝试重新连接时 XenMobile 无法重新对用户进行身份验证，则可以执行此检查。

Samsung KNOX 认证失败：检查设备是否无法通过 Samsung KNOX 认证服务器的查询。

禁止的应用程序：检查设备是否具有应用程序访问策略中定义的禁止的应用程序。

隐式允许和拒绝：这是 ActiveSync Gateway 的默认操作，该操作会为不满足其他任何过滤器规则条件的所有设备创建一个设备列表，并根据该列表允许或拒绝连接。如果任何规则均不匹配，则默认规则为“隐式允许”。

不活动设备：根据“服务器属性”中“Device Inactivity Days Threshold”（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。

缺少必备应用程序：检查设备是否缺少应用程序访问策略中定义的必备应用程序。

非推荐应用程序：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码：检查用户密码是否合规。 在 iOS 和 Android 设备上，XenMobile 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。 例如，在 iOS 设备上，如果 XenMobile 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。 在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规”设备属性检查设备是否不合规。 该属性通常由自动化操作进行更改，或由第三方利用 XenMobile API 进行更改。

吊销状态：检查设备证书是否已吊销。 再次授权之前，已吊销的设备无法重新注册。

已获得 root 权限的 Android 设备和已越狱的 iOS 设备：检查 Android 设备或 iOS 设备是否已越狱。

非托管设备：检查设备是否仍处于托管状态，受 XenMobile 控制。 例如，在 MAM 模式下运行的设备或已取消注册的设备为非托管设备。

将 Android 域用户发送到 ActiveSync Gateway：单击**是**可确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。 启用此选项后，可确保在 XenMobile 不具有 Android 设备用户的 ActiveSync 标识符时，XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。

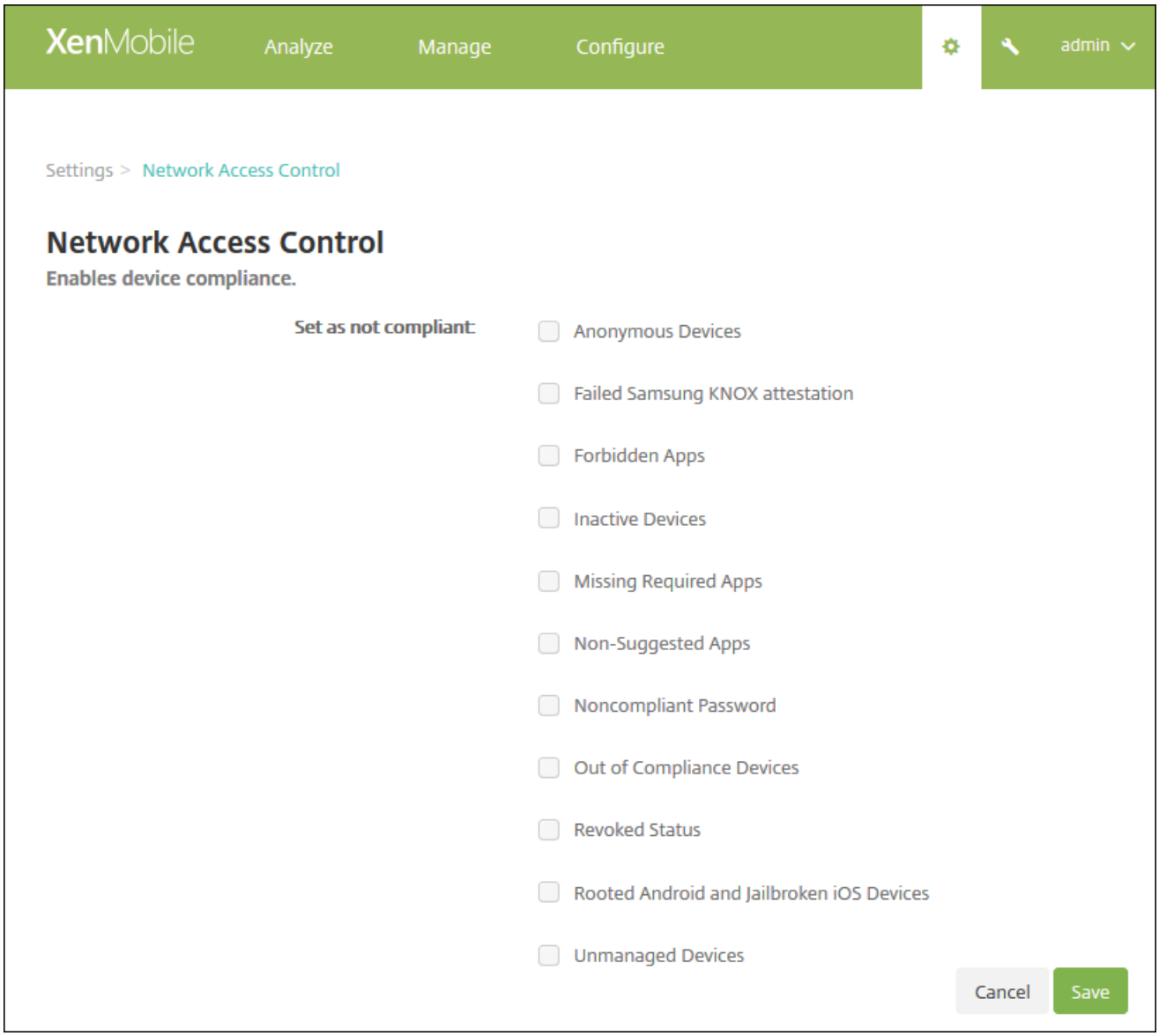
> ## 注意
>
> “隐式合规/不合规”过滤器仅在由 XenMobile 托管的设备上设置默认值。 例如，任何已安装黑名单应用程序的设备或未注册的设备都将被标记为“不合规”，并会被 NAC 设备阻止在您的网络外。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置网络访问控制

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**网络访问控制**。 此时将显示**网络访问控制**页面。



3. 选中要启用的**设为不合规**过滤器旁边的复选框。

4. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Samsung KNOX

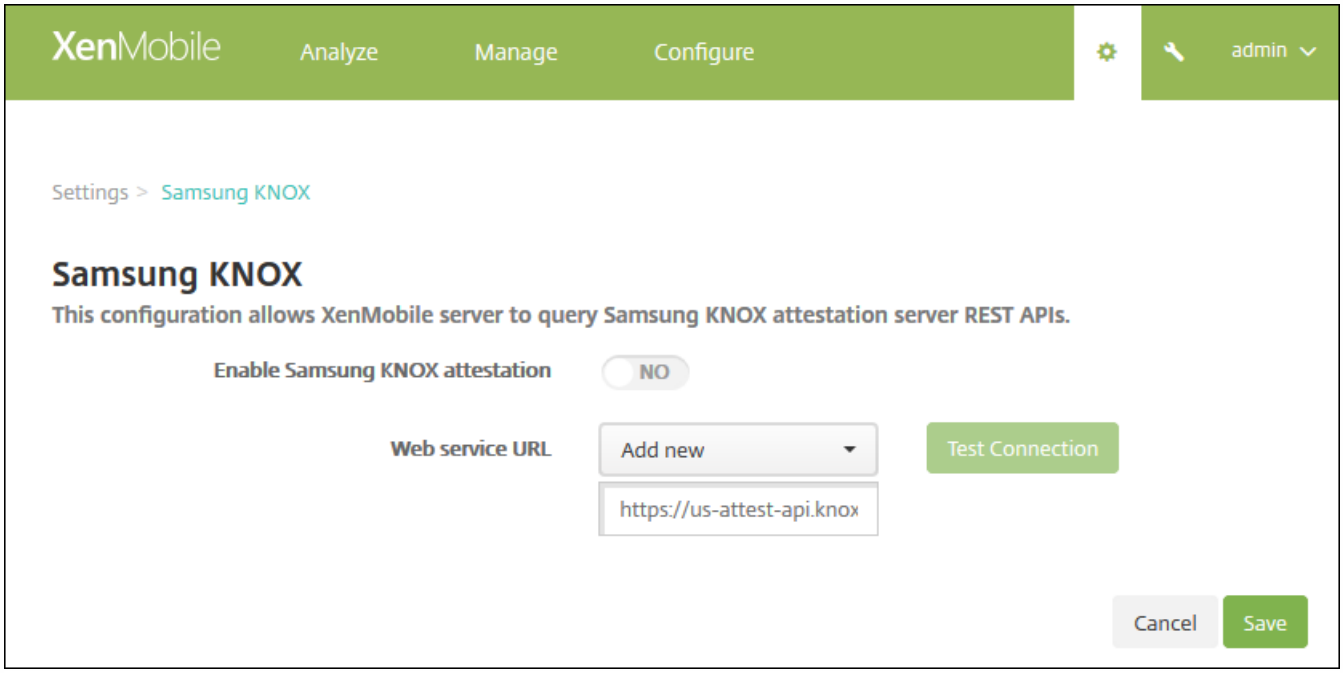
Aug 11, 2016

可以配置 XenMobile 以查询 Samsung KNOX 认证服务器 REST API。

Samsung KNOX 利用为操作系统和应用程序提供多级别保护的硬件安全功能。 其中一种安全级别驻留在通过认证的平台上。 认证服务器基于在可信引导期间收集的数据此，在运行时提供移动设备的核心系统软件（例如， 引导加载程序 和内核）验证。

1. 在 XenMobile Web 控制台中，单击右上角的齿轮图标。 此时将显示**设置**页面。

2. 在**服务器**下面，单击 **Samsung KNOX**。 此时将显示 **Samsung KNOX** 页面。



3. 配置以下设置：

- **启用 Samsung KNOX 认证**：选择是否启用 Samsung KNOX 认证。 默认值为**开**。 启用**启用 Samsung KNOX 认证**时，会启用 **Web 服务 URL** 选项。
- 在列表中，单击合适的认证服务器。

4. 单击**测试连接**以验证连接性。

5. 单击**保存**。

> **注意**
>
> 可以使用 SamSung KNOX Mobile Enrollment 将多个 Samsung KNOX 设备注册到 XenMobile（或任何 Mobile Device Manager）中，但不手动配置每个设备。 有关信息，请参阅 Samsung KNOX 批量注册。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

添加、编辑或删除服务器属性

Aug 11, 2016

XenMobile 具有 100 多个适用于服务器范围操作的属性。 本文将介绍部分较为重要的服务器属性，同时详细说明如何添加、编辑或删除服务器属性。

服务器属性定义

Audit Log Cleanup Execution Time（审核日志清理执行时间）

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

Audit Log Cleanup Interval (in Days)（审核日志清理时间间隔(天)）

XenMobile 服务器应保留审核日志的天数。 默认为 **1**。

Audit Logger（审核记录器）

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

Audit Log Retention (in Days)（审核日志保留时间(天)）

XenMobile 服务器应保留审核日志的天数。 默认为 **7**。

Deploy Log Cleanup (in Days)（部署日志清理(天)）

XenMobile 服务器应保留部署日志的天数。 默认为 **7**。

Disable SSL Server Verification（禁用 SSL 服务器验证）

如果设置为 **True**，请在满足以下所有条件时禁用 SSL 服务器证书验证：已在您的 XenMobile 服务器上启用基于证书的身份验证，Microsoft CA 服务器为证书颁发者，并且您的证书已由根证书不受 Xenmobile 服务器信任的内部 CA 签名。 默认设置为 **True**。

Inactivity Timeout in Minutes（不活动超时(分钟)）

不活动分钟数，超过此时间后，使用 XenMobile 服务器公共 API 访问 XenMobile 控制台或任何第三方应用程序的不活动管理员将被注销。 超时值 **0** 表示不活动的用户将保持登录状态。 默认为 **5**。

NetScaler Single Sign-On（NetScaler 单点登录）

如果设置为 **False**，则会在从 NetScaler 单点登录到 XenMobile 服务器时禁用 XenMobile 回调功能。 回调功能用于验证 NetScaler Gateway 会话 ID（如果 NetScaler Gateway 配置包括回调 URL）。 默认设置为 **False**。

Session Log Cleanup (in Days)（会话日志清理(天)）

XenMobile 服务器应保留会话日志的天数。 默认为 **7**。

Unauthenticated App Download for Android Devices（面向 Android 设备的未经身份验证的应用程序下载）

如果设置为 **True**，则可以将自托管应用程序下载到运行 Android for Work 的 Android 设备。 如果启用了在 Google Play

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Store 中静态提供下载 URL 的 Android for Work 选项，则需要此属性。 在这种情况下，下载 URL 不能包括带有身份验证令牌的一次性票据（由 **XAM 一次性票据服务器**属性定义）。 默认设置为 **False**。

Unauthenticated App Download for Windows Devices（面向 Windows 设备的未经身份验证的应用程序下载）

仅适用于不验证一次性票据的较旧 Worx Home 版本。 如果设置为 **False**，则可以将未经身份验证的应用程序从 XenMobile 下载到 Windows 设备。 默认设置为 **False**。

XAM One-Time Ticket（XAM 一次性票据）

一次性身份验证令牌 (OTT) 对下载应用程序有效的毫秒数。 此属性与属性 **Unauthenticated App Download for Android Devices**（面向 Android 设备的未经身份验证的应用程序下载）和 **Unauthenticated App Download for Windows Devices**（面向 Windows 设备的未经身份验证的应用程序下载）结合使用，指定是否允许下载未经身份验证的应用程序。 默认为 **3600000**。

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

不活动分钟数，超过此时间后，不活动的用户将从 XenMobile 自助服务门户注销。 超时值 **0** 表示不活动的用户将保持登录状态。 默认为 **30**。

添加、编辑或删除服务器属性

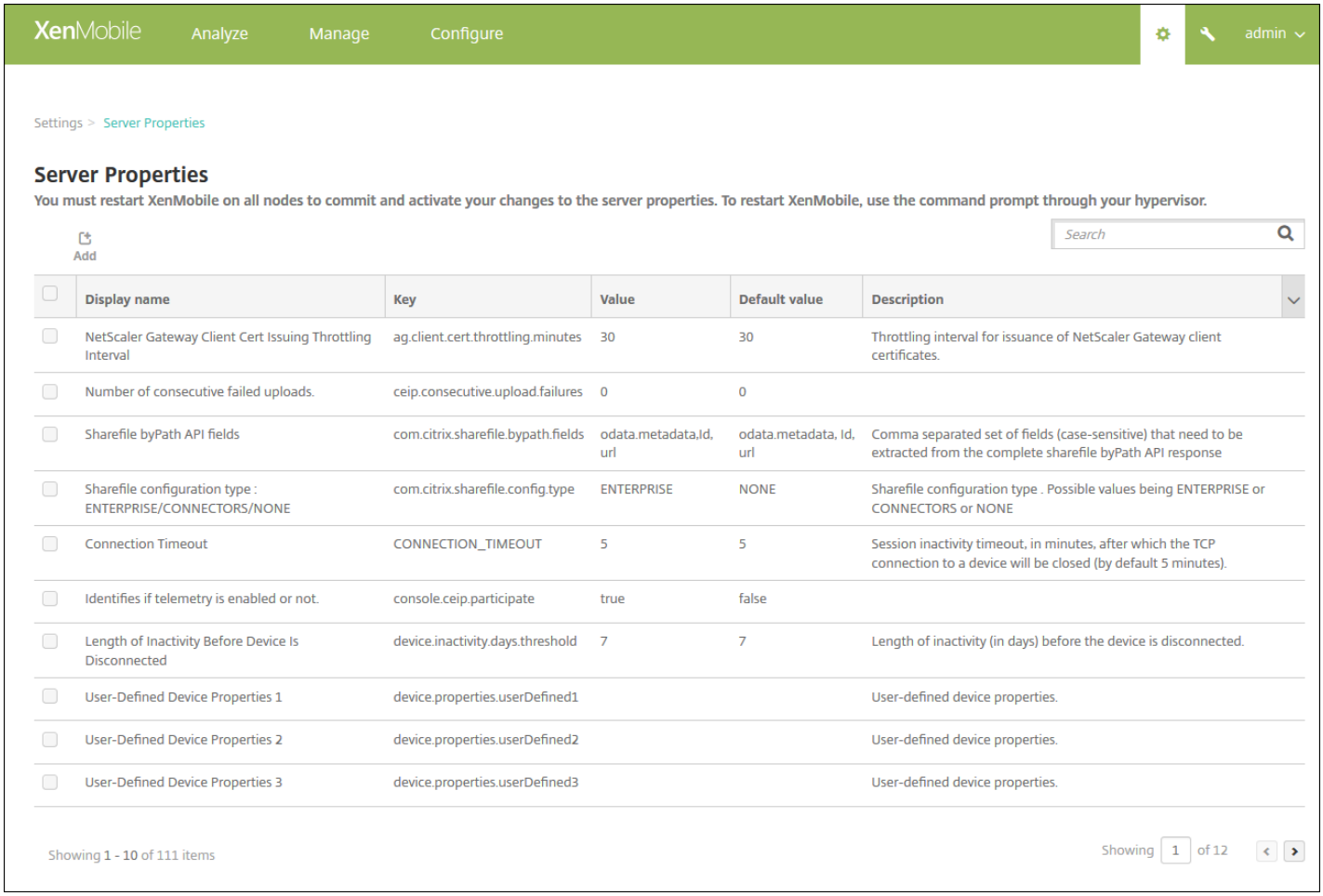
在 XenMobile 中，可以将属性应用到服务器。 更改后，在所有节点上重新启动 XenMobile 以提交并激活更改。

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

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

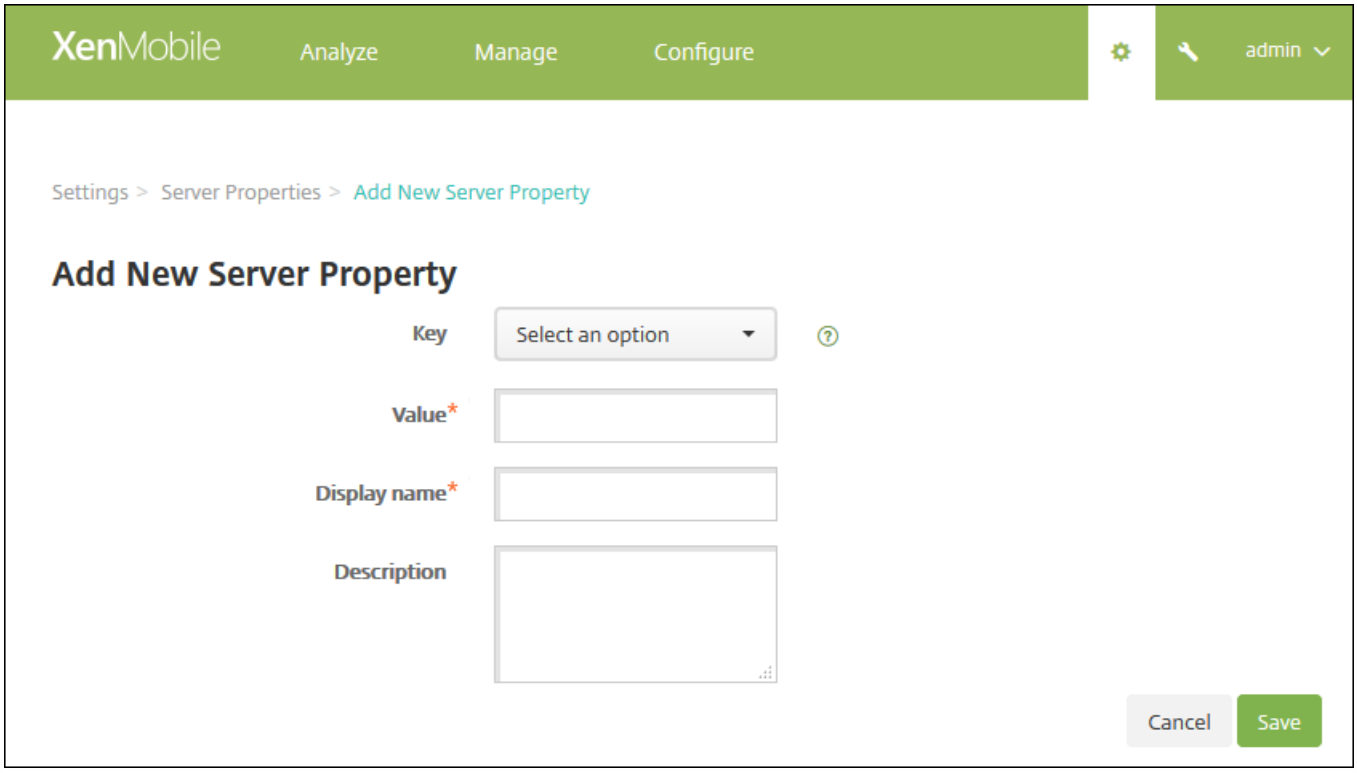
2. 在**服务器**下面，单击**服务器属性**。 此时将显示**服务器属性**页面。 可以从此页面添加、编辑和删除服务器属性。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. 单击**添加**。 此时将显示**添加新服务器属性**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 配置以下设置：

- **密钥**：在列表中，选择合适的密钥。 键区分大小写。 执行更改或请求特殊键之前必须联系 Citrix 技术支持。
- **值**：根据选择的密钥输入一个值。
- **显示名称**：输入新属性值显示在**服务器属性**表格中的名称。
- **说明**：（可选）键入新服务器属性的说明。

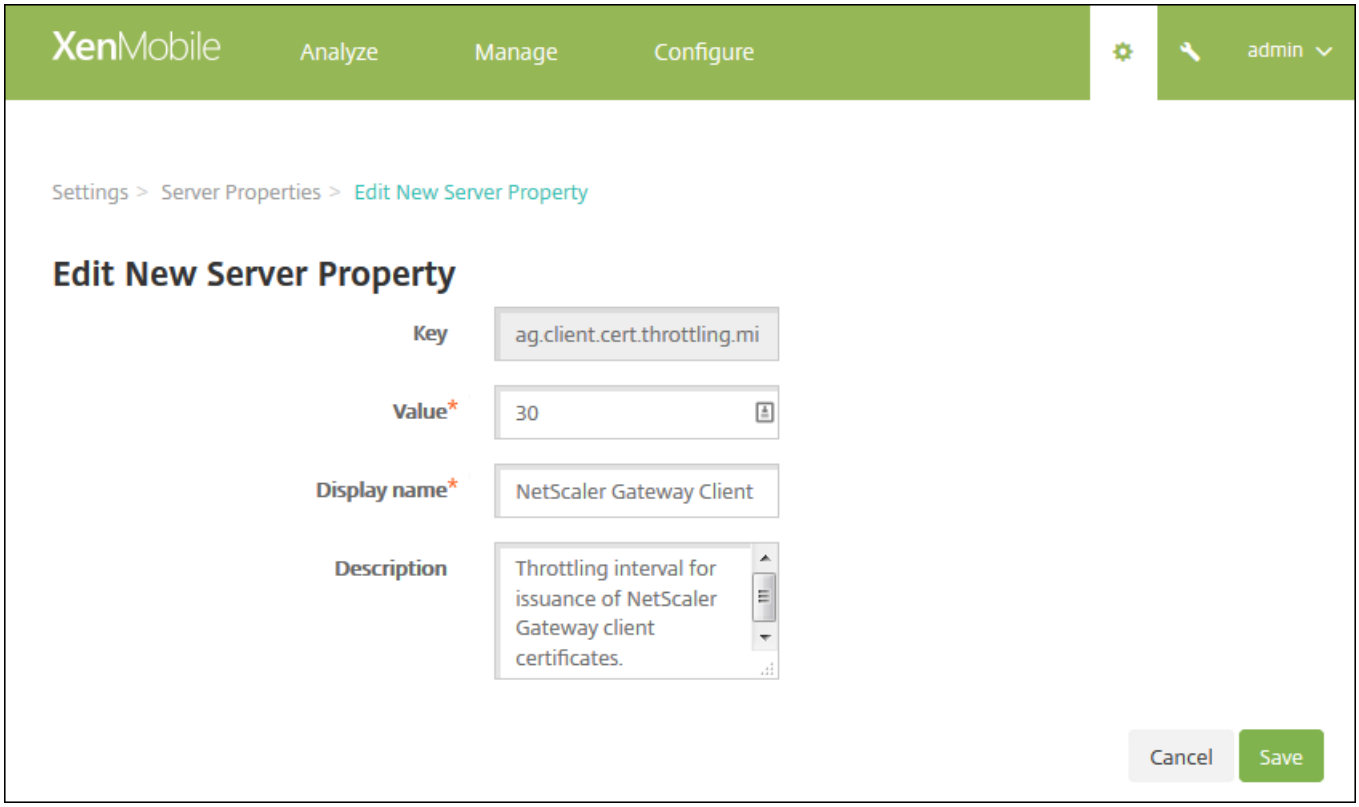
3. 单击**保存**。

1. 在**服务器属性**表格中，选择要编辑的服务器属性。

   注意：如果选中某个服务器属性旁边的复选框，选项菜单将显示在服务器属性列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。

2. 单击**编辑**。 此时将显示**编辑新服务器属性**页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 适当更改以下信息：

- **密钥**：无法更改此字段。
- **值**：属性的值。
- **显示名称**：属性的名称。
- **说明**：属性的说明。

4. 单击**保存**以保存您的更改，或单击**取消**保持属性不发生更改。

1. 在**服务器属性**表格中，选择要删除的服务器属性。

   注意：可以通过选中每个属性旁边的复选框，选择要删除的多个属性。

2. 单击**删除**。 此时将显示确认对话框。 再次单击**删除**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置 XenMobile 有效服务器模式

Aug 11, 2016

XenMobile 服务器模式是在“服务器属性”中设置的值。 可以将此值设置为 MAM、MDM 或 ENT，这三个值分别对应于应用程序管理、设备管理或应用程序和设备管理。 请根据所需的设备注册方式设置“服务器模式”属性，如下表所示。 无论许可证类型为何，“服务器模式”都默认设置为“ENT”。

有关设置服务器模式的信息，请参阅添加、编辑或删除服务器属性。

下表概述了用于特定许可证类型的“服务器模式”设置以及所需的设备模式：

您的许可证适用于此版本	您希望设备在此模式下注册	将“服务器模式”属性设置为
ENT/ADV/MDM	MDM 模式	MDM
ENT/ADV	MAM 模式（又称为“仅 MAM 模式”）	MAM
ENT/ADV	MDM+MAM 模式	ENT 选择退出设备管理的用户将在旧版 MAM 模式下操作。

*有效服务器模式*是许可证类型和服务器模式的组合。 对于 MDM 许可证，无论服务器模式的设置为何，有效服务器模式始终为 MDM。 如果您具有 MDM Edition 许可证，则无法通过将“服务器模式”设置为“MAM”或“ENT”来启用应用程序管理。 对于 Enterprise 和 Advanced 许可证，有效服务器模式与服务器模式一致。

每当激活或删除某个许可证时，以及在“服务器属性”中更改服务器模式时，都会向服务器日志中添加服务器模式。 有关创建和查看日志文件的信息，请参阅 XenMobile 支持和维护。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SysLog

Aug 11, 2016

可以将 XenMobile 配置为向系统日志 (syslog) 服务器发送日志文件。 需要服务器主机名称或 IP 地址。

Syslog 是标准日志记录协议，包含两个组件：审核模块（运行在设备上）和服务器（运行在远程系统上）。 Syslog 协议使用用户数据报协议 (UDP) 进行数据传输。 将记录管理员事件和用户事件。

可以将服务器配置为收集以下类型的信息：

- 包含 XenMobile 操作记录的系统日志。
- 包含按时间排序的 XenMobile 系统活动记录的审核日志。

syslog 服务器从设备收集的日志信息以消息的形式存储在日志文件中。 这些消息通常包含以下信息：

- 生成日志消息的设备的 IP 地址
- 时间戳
- 消息类型
- 与事件关联的日志级别（严重、错误、通知、警告、信息、调试、警报或紧急）
- 消息信息

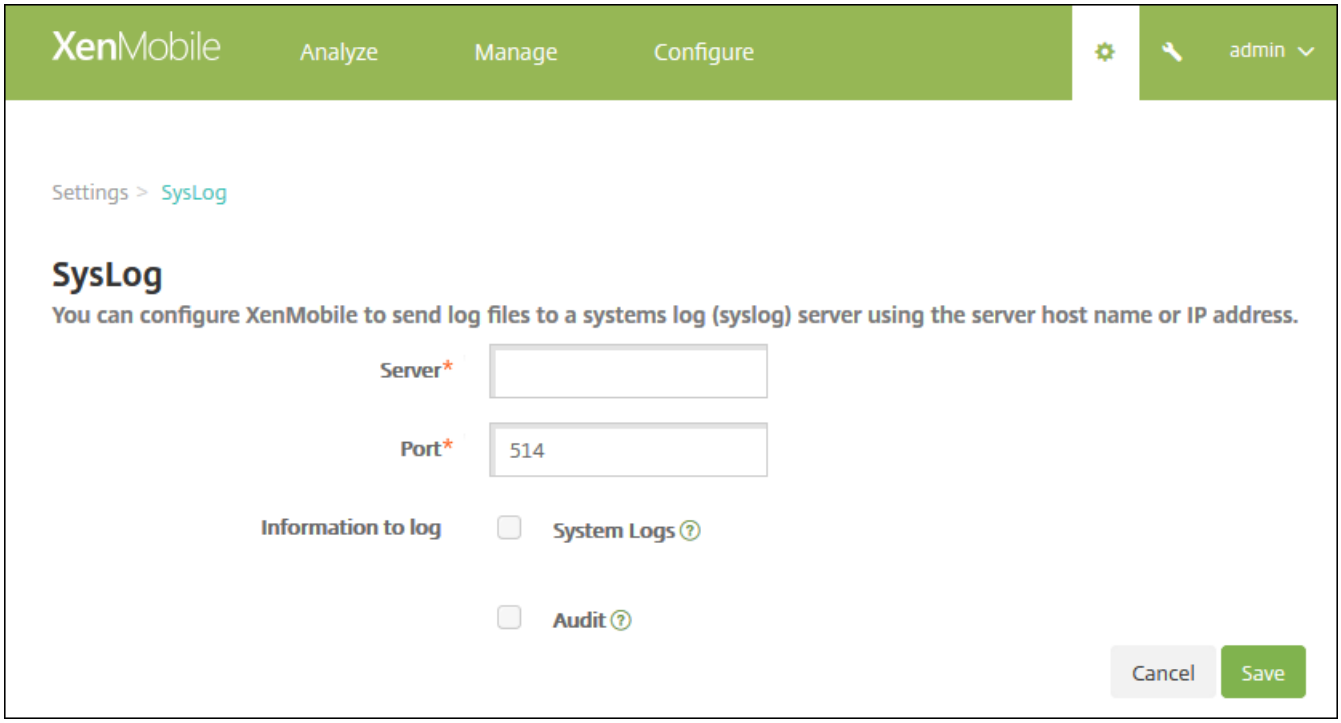
可以使用此信息分析警报来源并在需要时采用纠正措施。

> ## 注意
>
> 在 XenMobile 云部署中，Citrix 不支持 syslog 与本地 syslog 服务器相集成。 相反，可以在 XenMobile 控制台中从“支持”页面下载这些日志。 为此，必须单击**全部下载**才能获取系统日志。 有关详细信息，请参阅在 XenMobile 中查看和分析日志文件。

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

2. 单击 **Syslog**。 此时将显示 **Syslog** 页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 配置以下设置：

- **名称**：键入 syslog 服务器的 IP 地址或完全限定域名 (FQDN)。
- **端口**：键入端口号。 默认情况下，此端口设置为 514。
- **要记录的信息**：选择或取消选择**系统日志**和**审核**。
  - 系统日志包含 XenMobile 执行的操作。
  - 审核日志包含 XenMobile 的按时间排序的系统活动记录。

4. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置 XenApp 和 XenDesktop

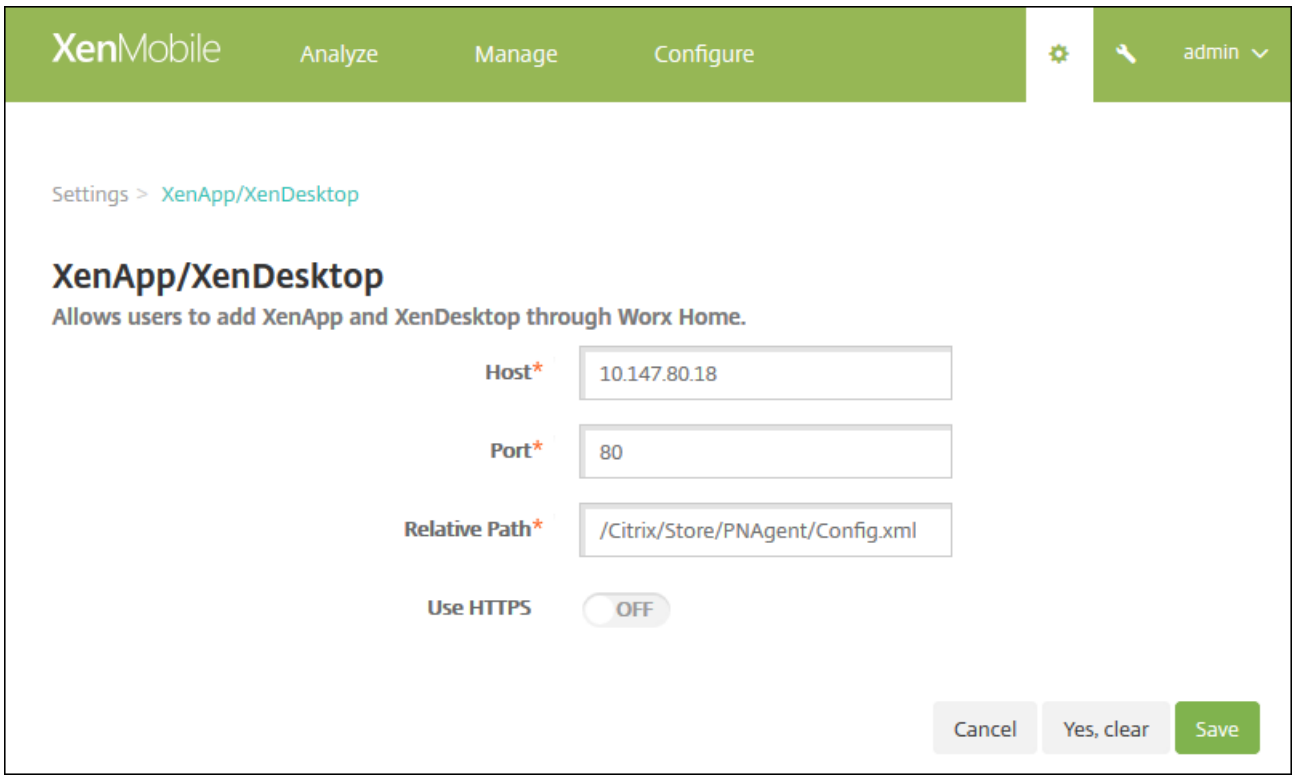
Aug 11, 2016

XenMobile 可从 XenApp 和 XenDesktop 收集应用程序，使移动设备用户可在 Worx Store 中对其进行访问。 用户可直接在 Worx Store 中订购应用程序，并从 WorxHome 启动这些应用程序。 用户 的设备上必须安装 Receiver 才能启动应用程序，但是并不需要对其进行配置。

要配置此设置，需要 Web Interface 站点或 StoreFront 的完全限定域名 (FQDN) 或 IP 地址和端口号。

1. 在 XenMobile Web 控制台中，单击右上角的齿轮图标。 此时将显示**设置**页面。

2. 单击 **XenApp/XenDesktop**。 此时将显示 **XenApp/XenDesktop** 页面。



3. 配置以下设置：

- **主机**：键入 Web Interface 站点或 StoreFront 的完全限定域名 (FQDN) 或 IP 地址。
- **端口**：加入 Web Interface 站点或 StoreFront 的端口号。 默认值为 80。
- **相对路径**：键入路径。 例如，/Citrix/PNAgent/config.xml
- **使用 HTTPS**：选择是否在 Web Interface 站点或 StoreFront 和客户端设备之间启用安全身份验证。 默认值为**关**。

4. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

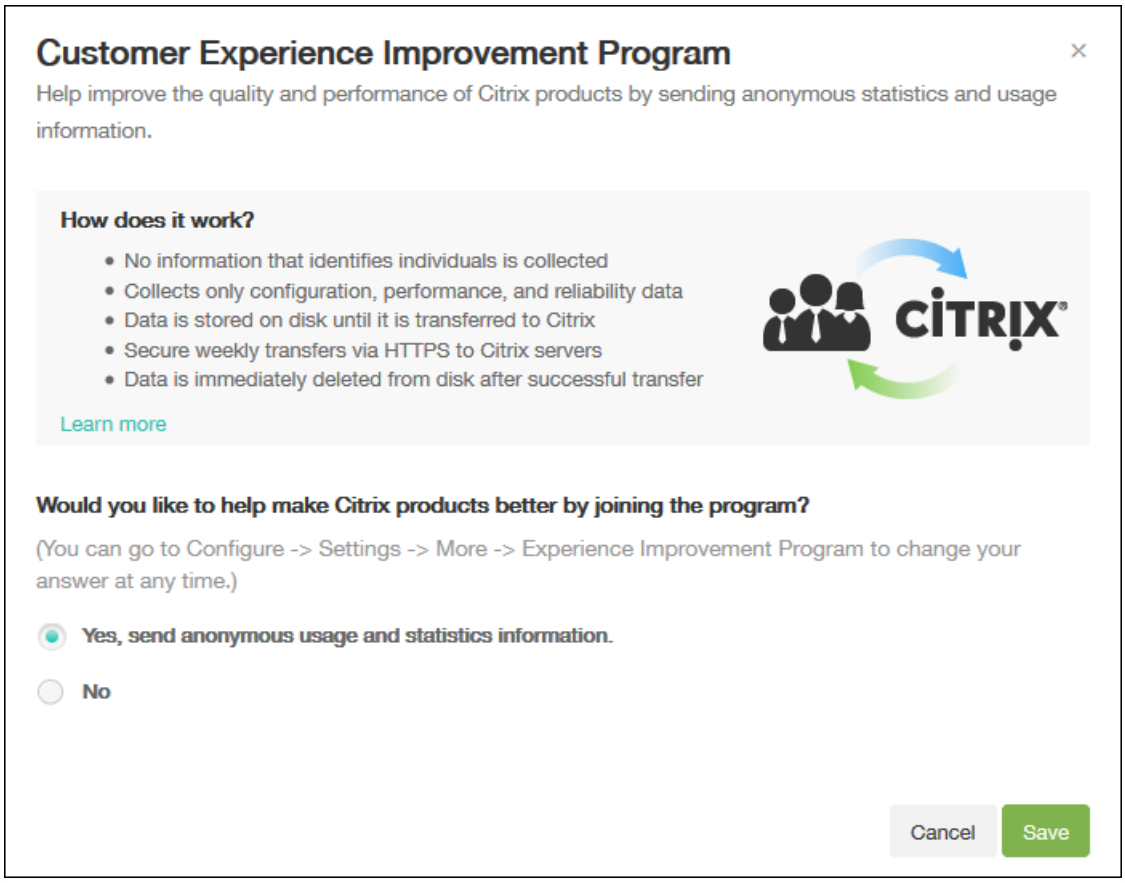
客户体验改善计划

Aug 11, 2016

Citrix 客户体验改善计划 (CEIP) 从 XenMobile 收集匿名配置和使用数据，并自动将数据发送到 Citrix。 此数据可帮助 Citrix 改善 XenMobile 的品质、可靠性和性能。 参与 CEIP 完全自愿。 首次安装 XenMobile 时或安装更新时，可以选择是否参与 CEIP。 选择参与后，通常每周收集一次数据，而性能和使用数据则每小时收集一次。 这些数据存储在磁盘上，每周一次通过 HTTPS 安全地传输给 Citrix。 您可以在 XenMobile 控制台更改是否参与 CEIP。 有关 CEIP 的详细信息，请参阅关于 Citrix 客户体验改善计划 (CEIP)。

安装或更新 XenMobile 时参与 CEIP

首次安装 XenMobile 或进行更新时，您会看到以下对话框，您可以在这里选择是否参与，然后单击**保存**。

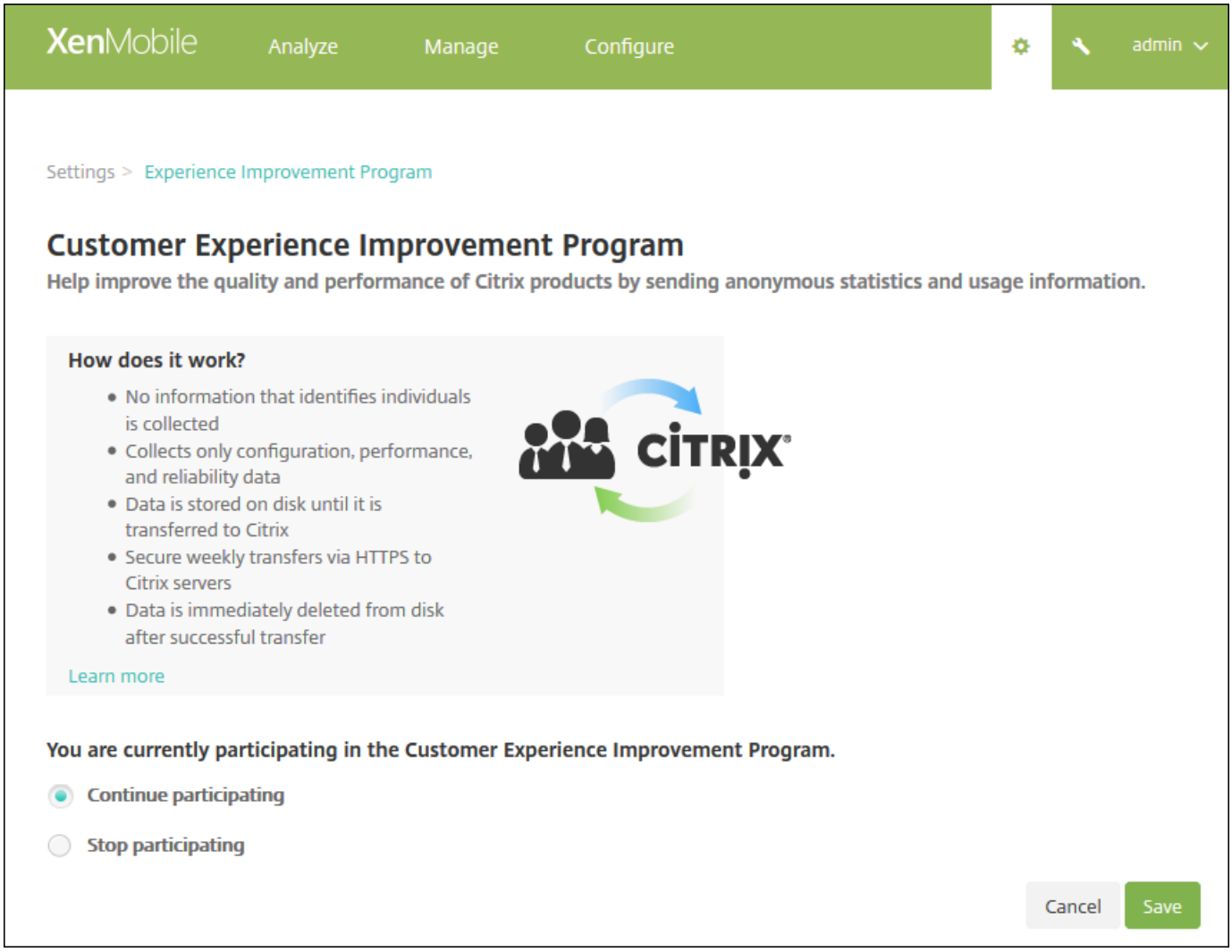


更改 CEIP 参与设置

1. 要更改 CEIP 参与设置，请在 XenMobile 控制台中，单击控制台右上角的齿轮图标以打开**设置**页面。

2. 在**服务器**下，单击**体验改善计划**。 此时将显示**客户体验改善计划**页面。 所显示的确切页面取决于您当前是否已参与 CEIP。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 如果当前已参与 CEIP 并希望停止，请单击**停止参与**。

4. 如果当前未参与 CEIP 并希望开始参与，请单击**开始参与**。

5. 单击**保存**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft Azure 设置

Aug 11, 2016

运行 Windows 10 的设备向 Azure 注册是一种联合 Active Directory 身份验证方法。 可以采用下列方法之一将 Windows 10 设备连接到 Microsoft Azure AD：

- 首次打开设备电源时在 Azure AD 联接启用过程中在 MDM 中注册。
- 配置设备后，从“Windows 设置”页面执行 Azure AD 联接过程中在 MDM 中注册。

需要具有 Microsoft Azure Active Directory 高级许可证才可以将 XenMobile 与 Microsoft Azure 集成。 启用 MDM 与 Azure AD 的集成需要许可证，以便使用 Windows 10 设备的用户可以使用 Azure AD 注册。 有关获取高级许可证的信息，请参阅 Microsoft Azure。 有关定价信息，请参阅 Azure Active Directory 定价。

必须在 XenMobile 中配置 Microsoft Azure 服务器设置，并为 Windows 设备设置“条款和条件”设备策略，Windows 设备用户才可以使用 Azure 注册。 本文介绍如何配置 Microsoft Azure 设置。 有关为 Windows 设备配置“条款和条件”设备策略的信息，请参阅条款和条件设备策略。

您需要登录到 Azure AD 门户并执行以下操作，才能在 XenMobile 中设置 Microsoft Azure 服务器设置：

1. 注册自定义域并验证域。 有关详细信息，请参阅 Add your own domain name to Azure Active Directory（将自己的域名添加到 Azure Active Directory）。

2. 使用目录集成工具，将本地目录扩展到 Azure Active Directory。 有关详细信息，请参阅目录集成。

3. 将 MDM 设为 Azure AD 的可信部分。 为此，请单击 **Azure Active Directory** > **应用程序**，然后单击**添加**。 从库中选择**添加应用程序**。 转至**移动设备管理**，选择**本地 MDM 应用程序**，然后保存设置。

4. 在应用程序中，如下所述配置 XenMobile 服务器发现、终端使用条款和 App ID URL：

- MDM 发现 URL：https://:8443/zdm/wpe
- MDM 使用条款 URL：https://:8443/zdm/wpe/tou
- 应用程序 ID URL：https://:8443/

5. 选择在第 3 步创建的本地 MDM 应用程序并启用**管理这些用户的设备**选项，以便为所有用户或任何特定用户组启用 MDM 管理。

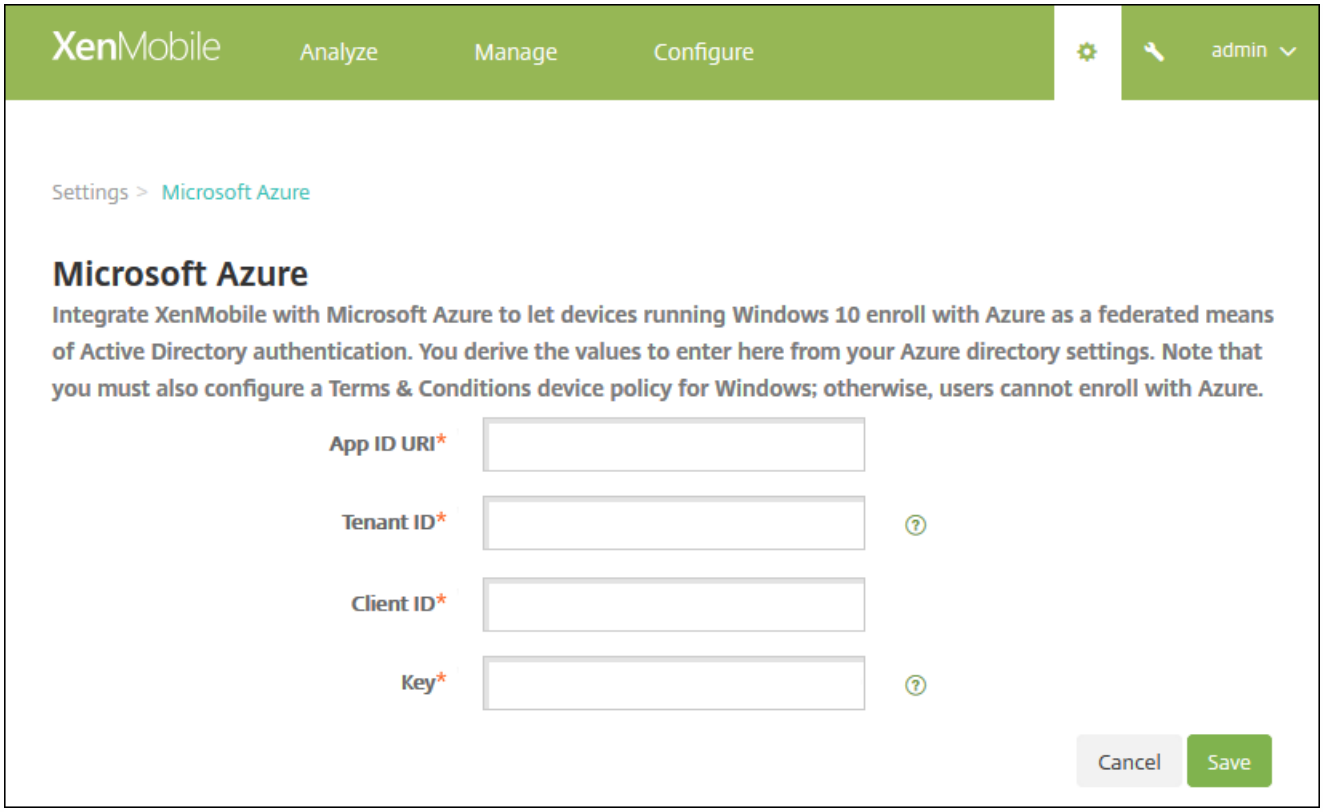
还需要记下 Microsoft Azure 帐户提供的以下信息，才能在 XenMobile 控制台中配置设置：

- 应用程序 ID URI – 运行 XenMobile 的服务器的 URL。
- 租户 ID – 来自 Azure 应用程序设置页面。
- 客户端 ID – 您的应用程序的唯一标识符。
- 密钥 – 来自 Azure 应用程序设置页面。

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**下面，单击 **Microsoft Azure**。 此时将显示 **Microsoft Azure** 页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 配置以下设置：

- **应用程序 ID URI**：键入运行 XenMobile 的服务器的 URL（在配置 Azure 设置时所输入的）。
- **租户 ID**：从 Azure 应用程序设置页面复制此值。 在浏览器地址栏中，复制由数字和字母组成的部分。 例如，在 https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem ... 中，租户 ID 为：*abc123-abc123-abc123*。
- **客户端 ID**：从“Azure 配置”页面复制并粘贴此值。 这是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**下面，从列表中选择一个持续时间并保存设置。 然后，可以复制此密钥并将其粘贴到此字段中。 应用程序在 Microsoft Azure AD 中读写数据时需要密钥。

4. 单击**保存**。

Important

用户在其 Windows 设备上加入 Azure AD 时，您在 XenMobile 中配置的 Worx Store 和 Web 链接设备策略将仅适用于 Azure AD 用户，不适用于本地用户。 对于能够使用这些设备策略的本地用户，必须执行以下操作：

1. 在 **设置** > **关于** > **加入 Azure AD** 中，代表 Azure 用户加入 Azure AD。
2. 注销 Windows，然后通过 Azure AD 帐户进行登录。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Google Cloud Messaging

Aug 11, 2016

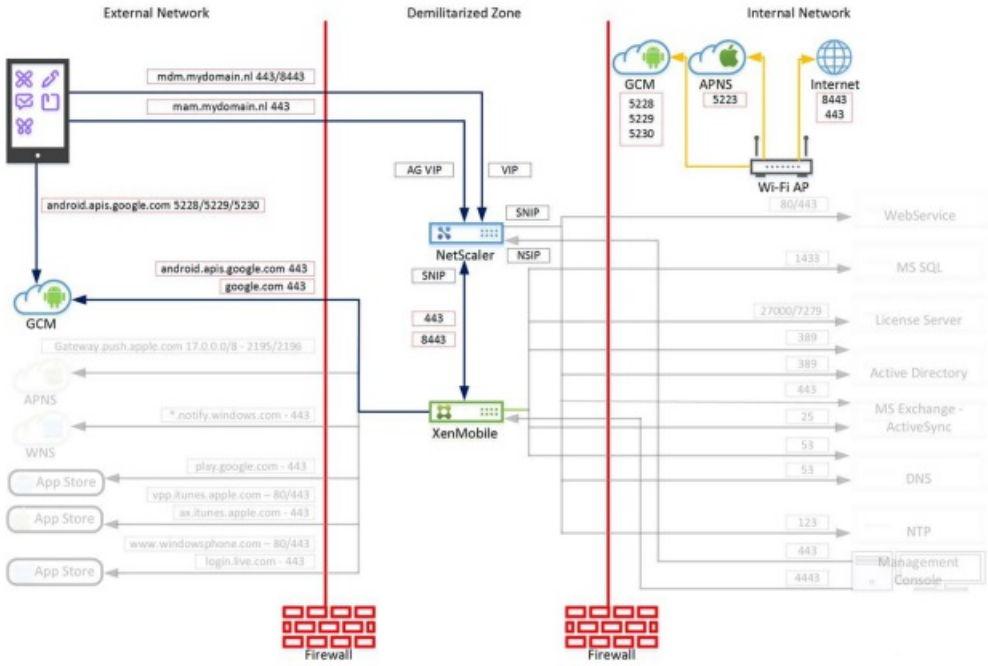
作为 MDX 策略**活动轮询期限**的备选策略，可以使用 Google Cloud Messaging (GCM) 控制 Android 设备如何以及何时需要连接到 XenMobile。 使用本文中介绍的配置，任何安全操作或部署命令都将触发向 Worx Home 推送通知，以提示用户重新连接到 XenMobile 服务器。

必备条件

- XenMobile 10.3.x
- 最新 Worx Home 客户端
- Google 开发者帐户凭据
- 在 XenMobile 上打开指向 Android.apis.google.com 和 Google.com 的端口 443

体系结构

此图显示了外部和内部网络中 GCM 的通信流程。



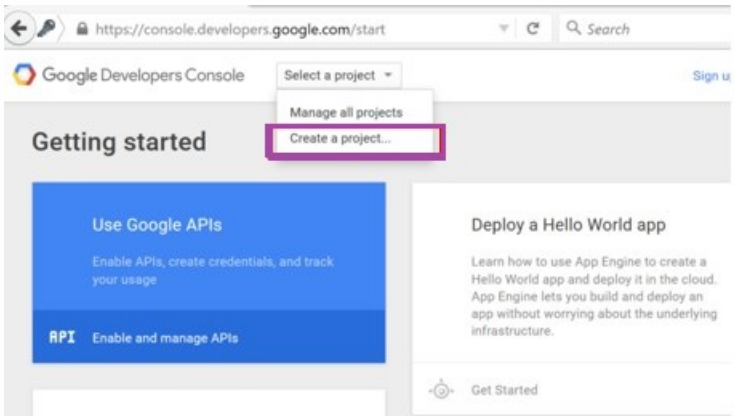
为 GCM 配置 Google 帐户

1. 使用您的 Google 开发者帐户凭据登录以下 URL：

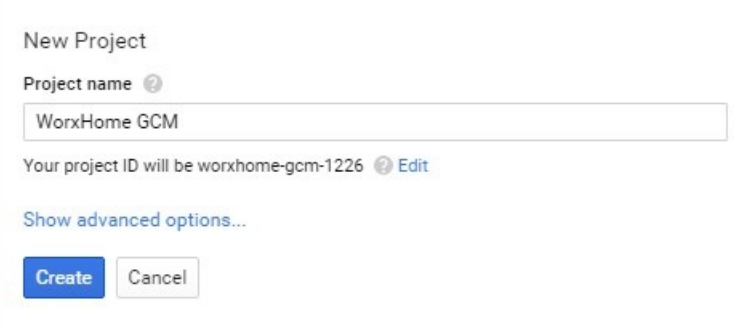
   https://console.developers.google.com

© 1999-2017 Citrix Systems, Inc. All rights reserved.

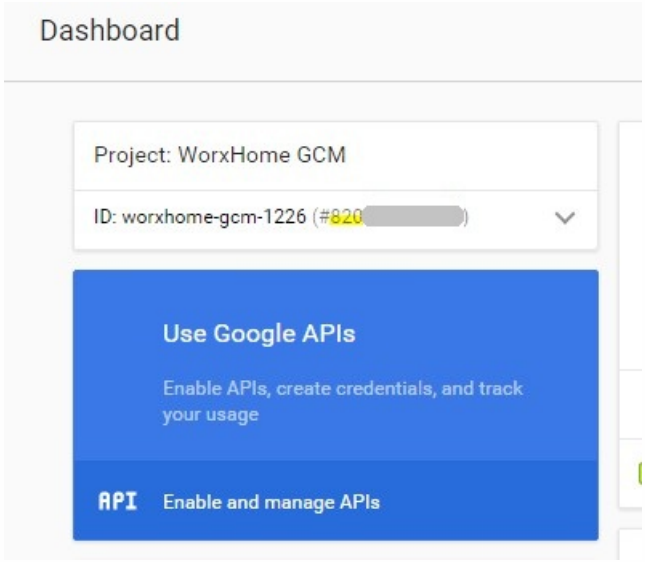
2. 在 **Select a project**（选择项目）中，选择 **Create a project**（创建项目）。



3. 输入 **Project name**（项目名称），然后单击 **Create**（创建）。

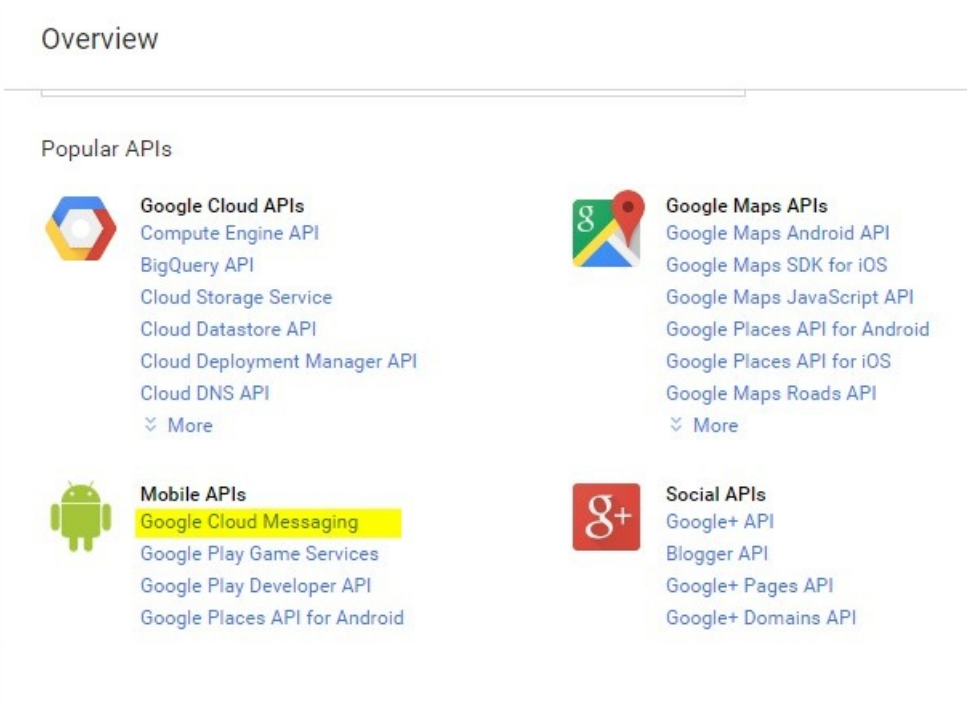


4. 在控制板中，您的发件人 ID（下面突出显示的内容）在您的项目 ID 旁边显示。 记录您的发件人 ID；必须稍后在 XenMobile 服务器设置中输入该 ID。 单击 **Use Google APIs**（使用 Google API）。

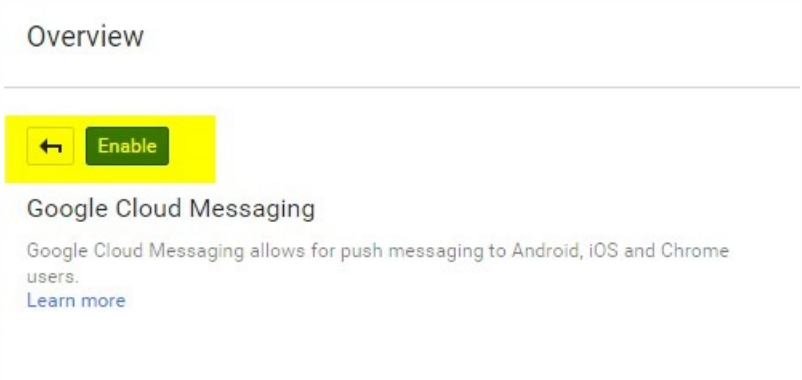


5. 在 **Mobile APIs**（移动 API）部分中，单击 **Google Cloud Messaging**。

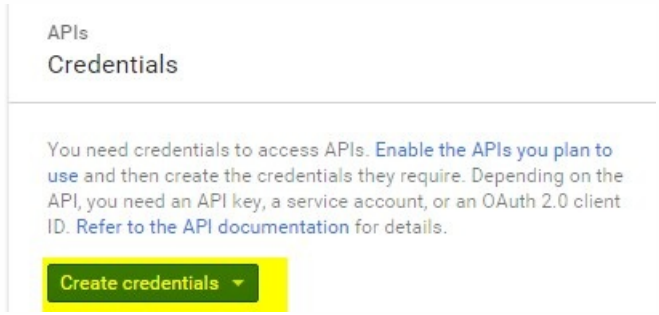
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. 单击 **Enable**（启用）。

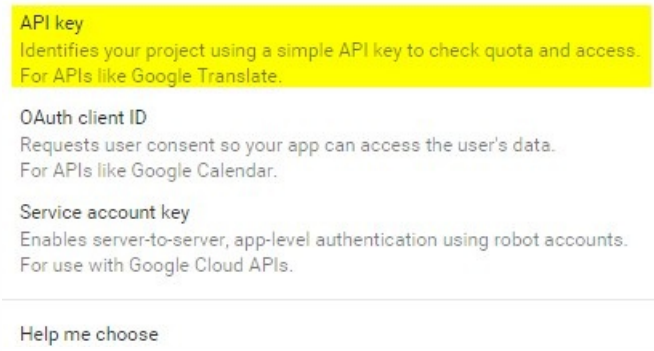


7. 在 **Credentials**（凭据）下，单击 **Create credentials**（创建凭据）。

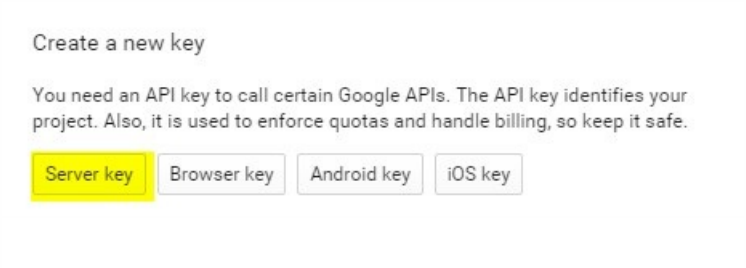


8. 单击 **API key**（API 密钥）。

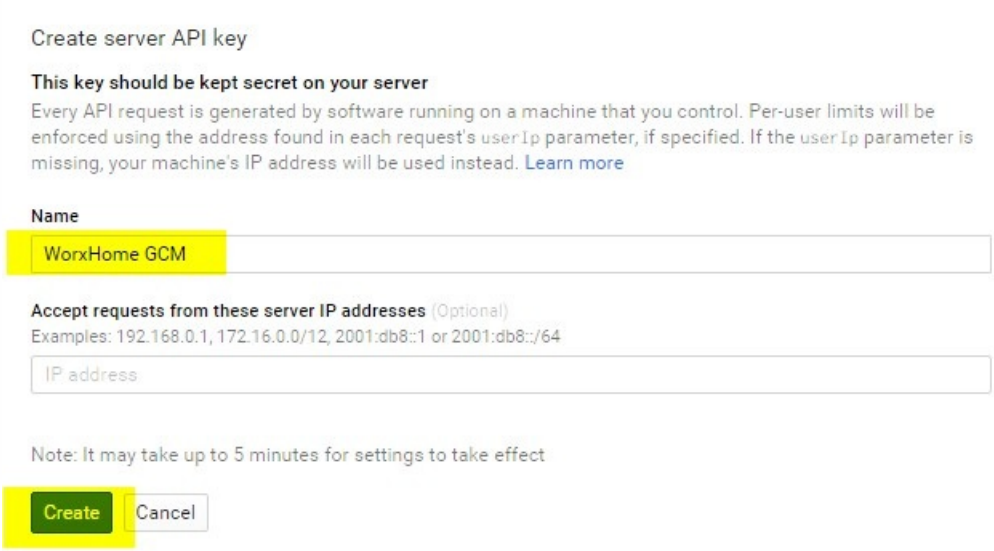
© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. 在 **Create a new key**（创建新密钥）下，单击 **Server key**（服务器密钥）。



10. 在 **Create server API key**（创建服务器 API 密钥）中，输入 **Name**（名称）（在此示例中，我们使用项目名称），然后单击 **Create**（创建）。



11. 记录 API 密钥。 您需要该密钥以配置 XenMobile。

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

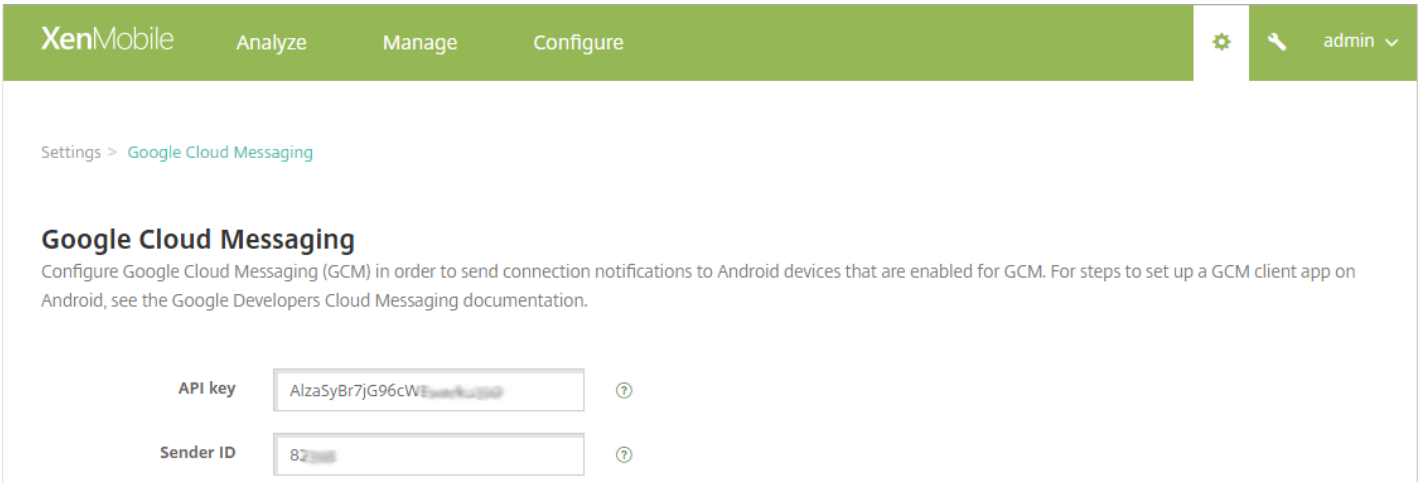
为 GCM 配置 XenMobile

1. 登录 XenMobile 管理员控制台，然后单击**设置 > Google Cloud Messaging**。

   a. 在 **API key**（API 密钥）中，输入您在上一步 GCM 配置过程中复制的 GCM API 密钥。

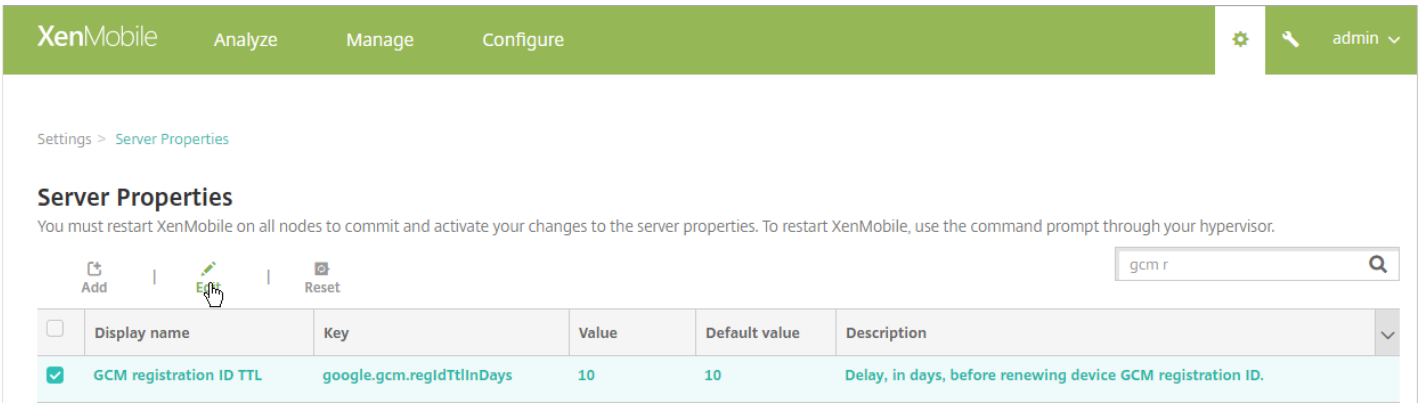
   b. 在 **Sender ID**（发件人 ID）中，复制您在前一个步骤中记录的发件人 ID 值，然后单击 **Save**（保存）。

   注意：页面**设置 > Google Cloud Messaging** 是 XenMobile 10.3.6 的新增页面。 如果您使用的不是最新版本的 XenMobile，请转至**设置 > 服务器**以升级 **API key**（API 密钥）(google.gcm.apiKey) 和 **Sender ID**（发件人 ID）(google.gcm.senderid)。



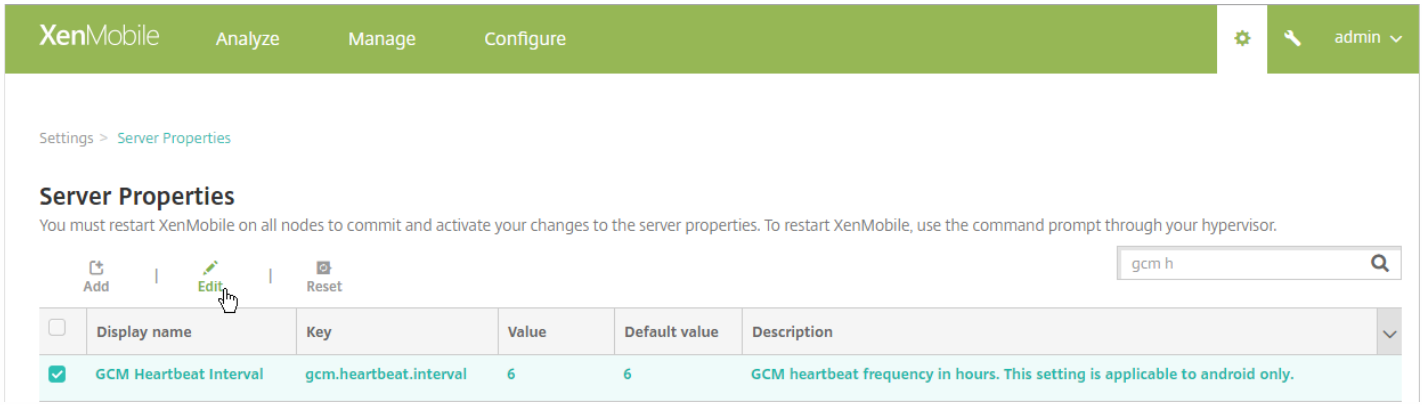
2. 如果需要更改以下任一属性的默认设置，请单击**设置 > 服务器属性**。

- **GCM Registration ID TTL**（GCM 注册 ID TTL）：续订设备 GCM 注册 ID 之前的默认延迟时间为 **10** 天。 要更改该值，请在搜索框中输入 **gcm r**，单击 **GCM Registration ID TTL**（GCM 注册 ID TTL），然后单击 **Edit**（编辑）。



- **GCM Heartbeat Interval**（GCM 检测信号时间间隔）：XenMobile 与 GCM 服务器的默认通信频率为 **6** 小时。 要更改该值，请在搜索框中输入 **gcm h**，单击 **GCM Heartbeat Interval**（GCM 检测信号时间间隔），然后单击 **Edit**（编辑）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



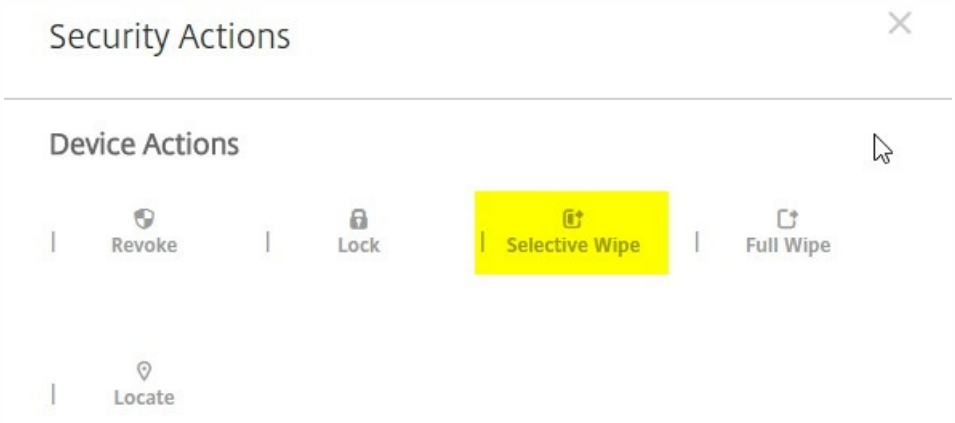
测试您的配置

1. 注册 Android 设备。

2. 保持设备在一段时间内处于空闲状态，以使其与 XenMobile 服务器断开连接。

3. 登录 XenMobile 管理员控制台，单击**管理**，选择 Android 设备，然后单击**安全**。

4. 在**设备操作**下，单击**选择性擦除**。



在成功的配置中，不需要重新连接到 XenMobile 即可在设备上执行选择性擦除。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

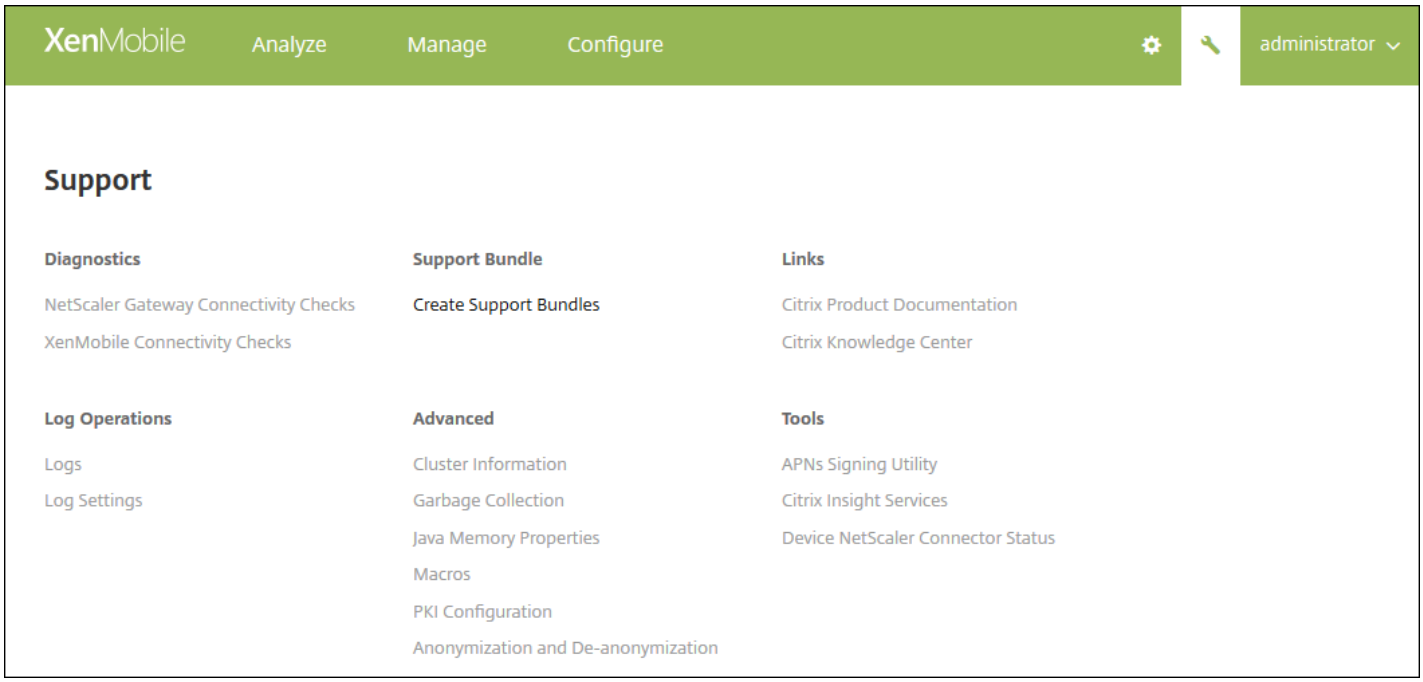
XenMobile 支持与维护

Aug 11, 2016

使用 XenMobile 的“支持”页面访问多个与支持相关的信息和工具。 也可以从命令行执行操作。 有关详细信息，请参阅 XenMobile 命令行接口选项。

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。



使用 XenMobile 的**支持**页面可以执行以下操作：

- 访问诊断。
- 创建支持包。
- 访问 Citrix 产品文档和知识中心的链接。
- 访问日志操作。
- 从高级信息和配置选项中选择。
- 访问工具和实用程序。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

执行连接检查

Aug 11, 2016

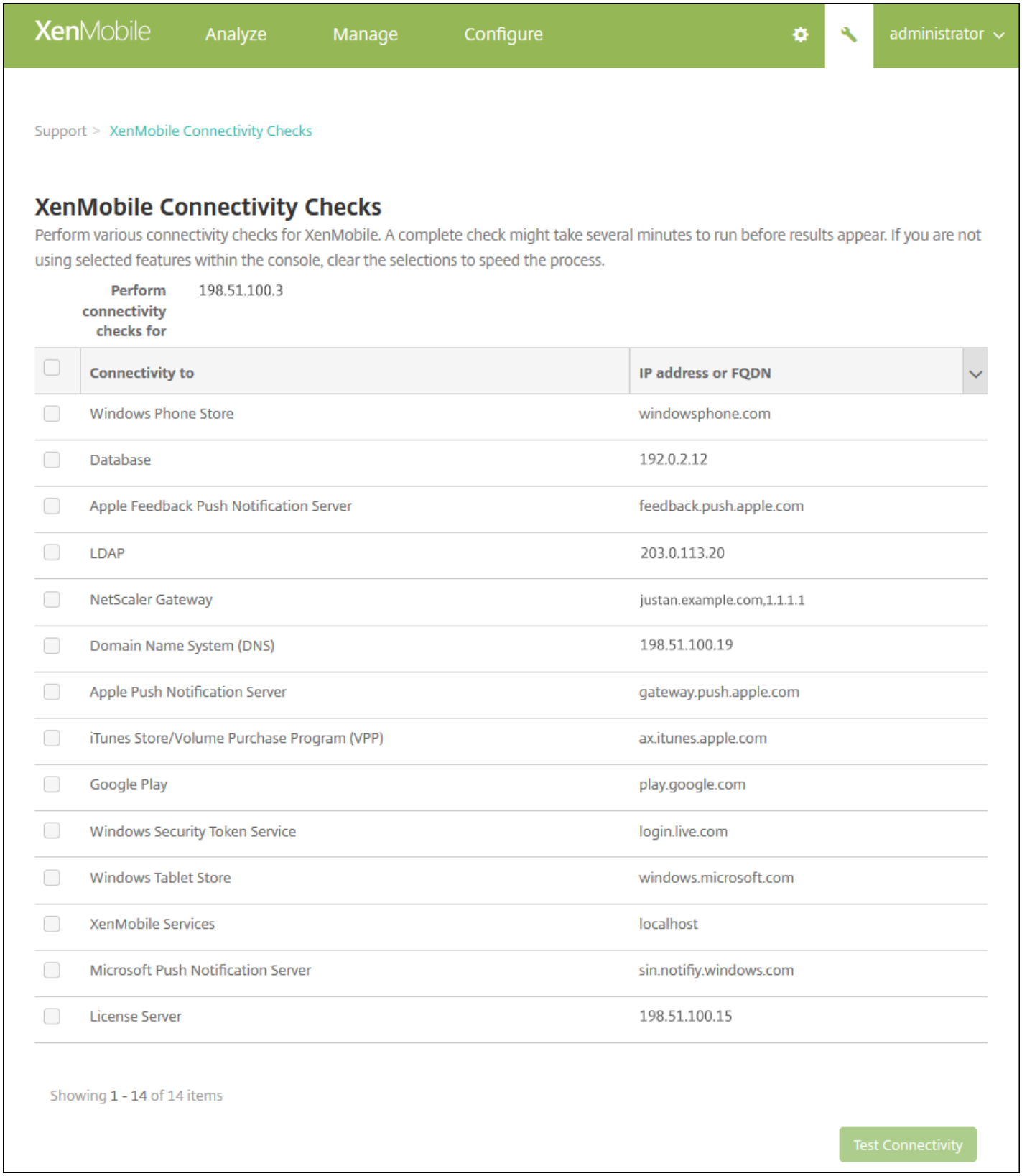
从 XenMobile 的**支持**页面，可以检查 XenMobile 与 NetScaler Gateway 及其他服务器和位置的连接性。

执行 XenMobile 连接检查

1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。 此时将显示**支持**页面。

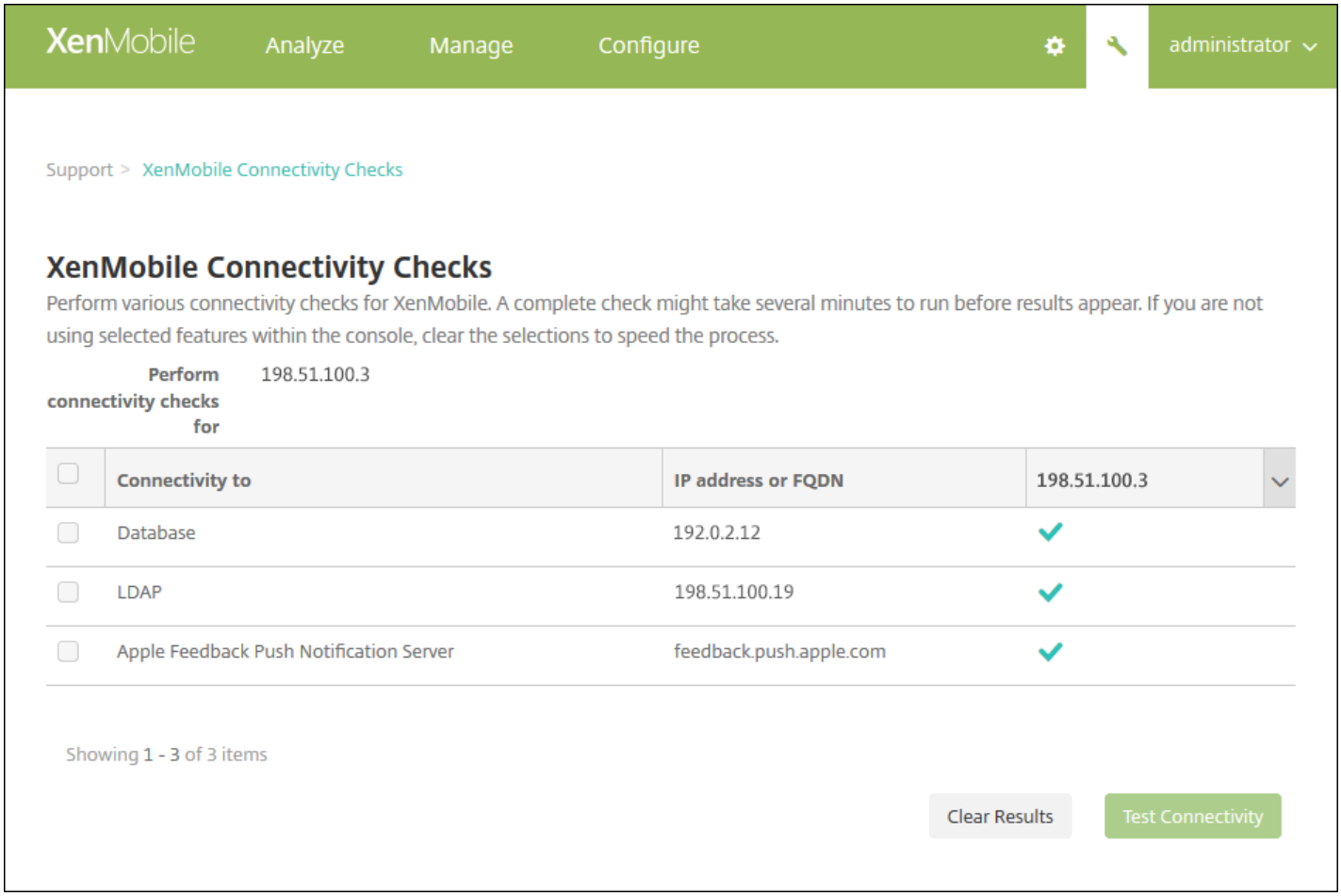
2. 在**诊断**下面，单击 **XenMobile 连接检查**。 此时将显示 **XenMobile 连接检查**页面。 如果 XenMobile 环境包含加入群集的节点，将显示所有节点。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



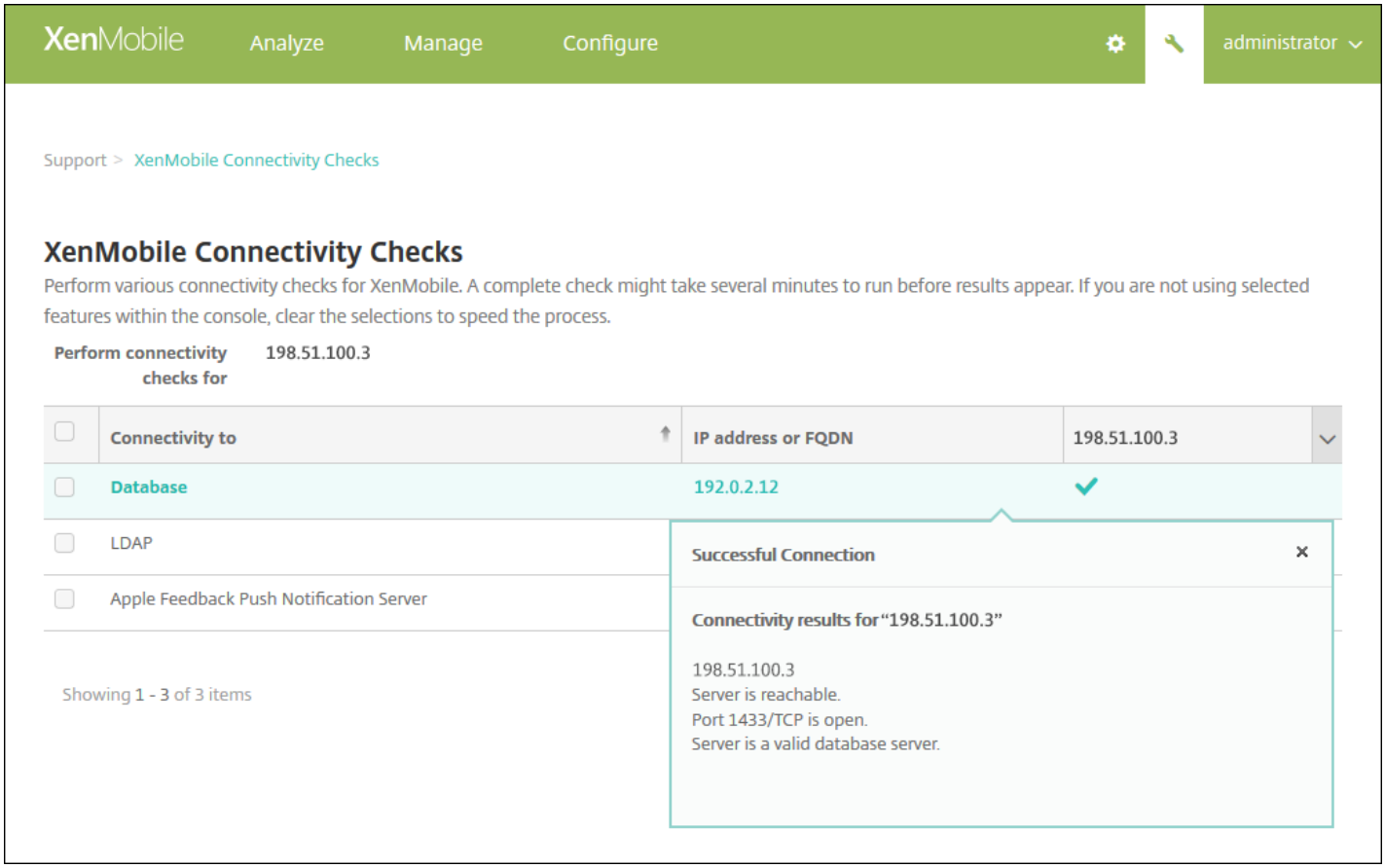
2. 选择执行连接测试时要包括的服务器，然后单击**测试连接**。 此时将显示测试结果页面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 在测试结果表格中选择一个服务器，可查看有关此服务器的详细结果。

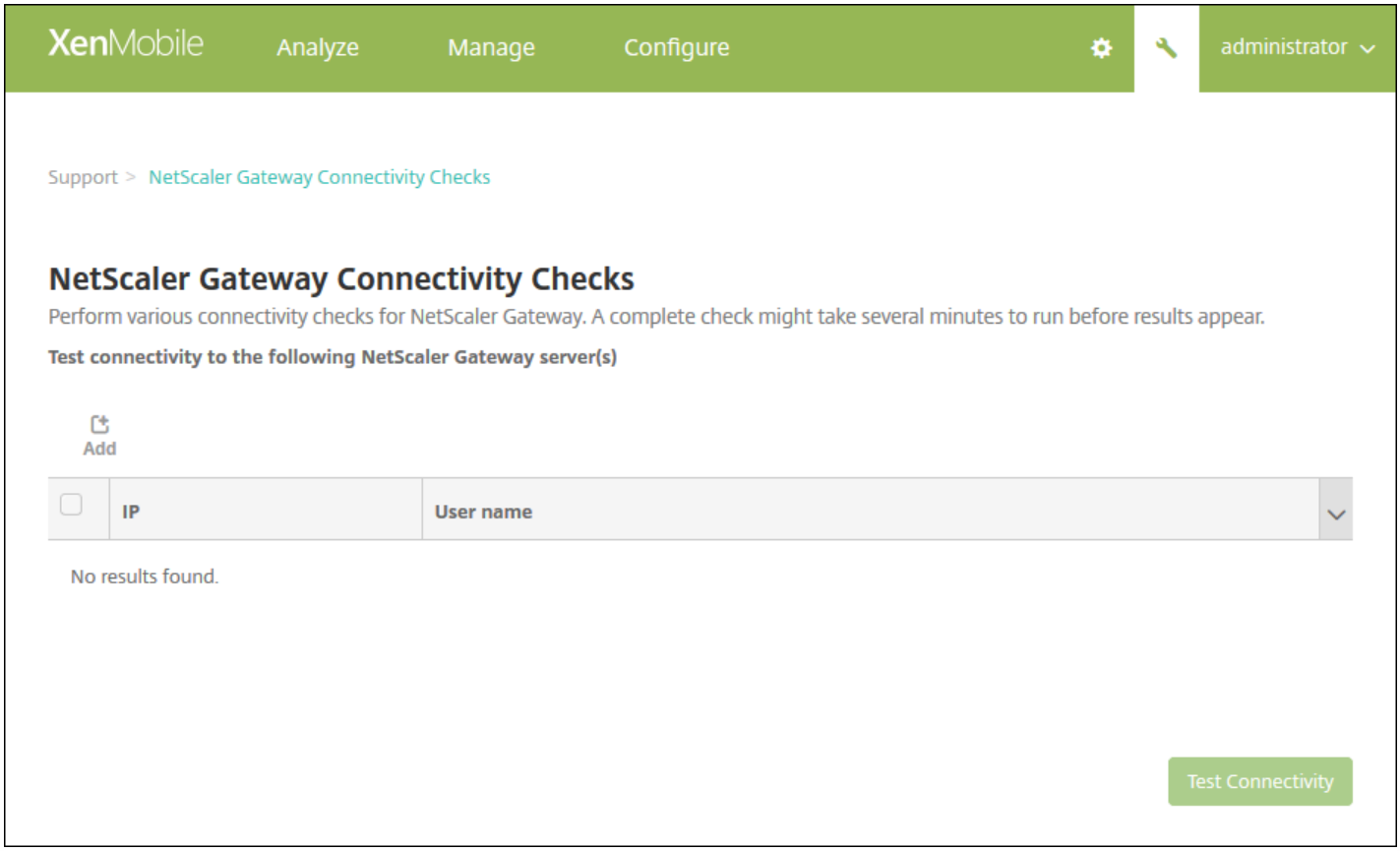
© 1999-2017 Citrix Systems, Inc. All rights reserved.



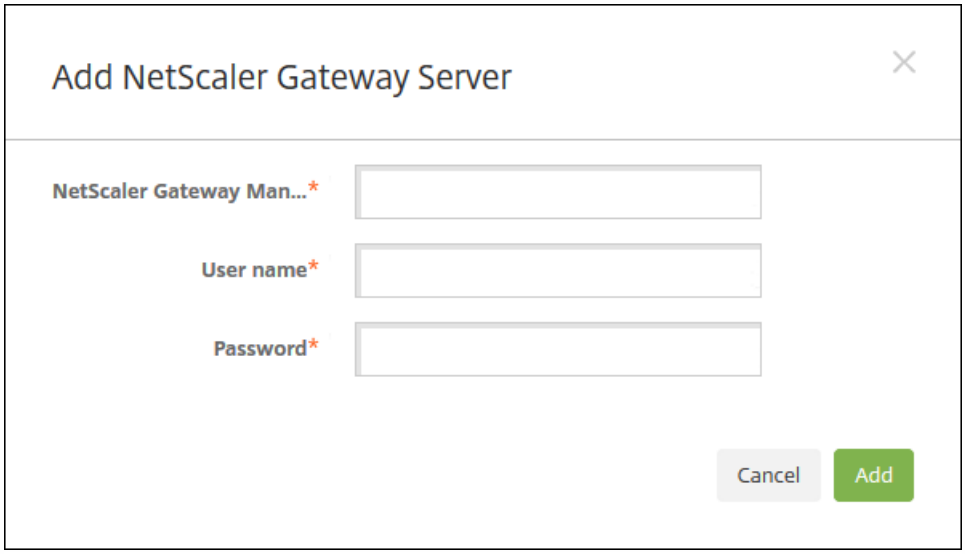
执行 NetScaler Gateway 连接检查

1. 在**支持**页面的**诊断**下面，单击 **NetScaler Gateway 连接检查**。 此时将显示 **NetScaler Gateway 连接检查**页面。 如果尚未添加任何 NetScaler Gateway 服务器，此表格为空。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 单击**添加**。 将显示**添加 NetScaler Gateway 服务器**对话框。



3. 在 **NetScaler Gateway 管理 IP** 中，键入运行要测试的 NetScaler Gateway 的服务器的 IP 地址。

注意：如果要对已经添加的 NetScaler Gateway 服务器执行连接检查，系统会提供 IP 地址。

4. 键入关于此 NetScaler Gateway 的管理员凭据。

注意：如果要对已经添加的 NetScaler Gateway 服务器执行连接检查，系统会提供用户名。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. 单击**添加**。 此 NetScaler Gateway 将添加到 **NetScaler Gateway 连接检查**页面上的表格中。

6. 单击**测试连接**。 结果将显示在测试结果表格中。

7. 在测试结果表格中选择一个服务器，可查看有关此服务器的详细结果。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

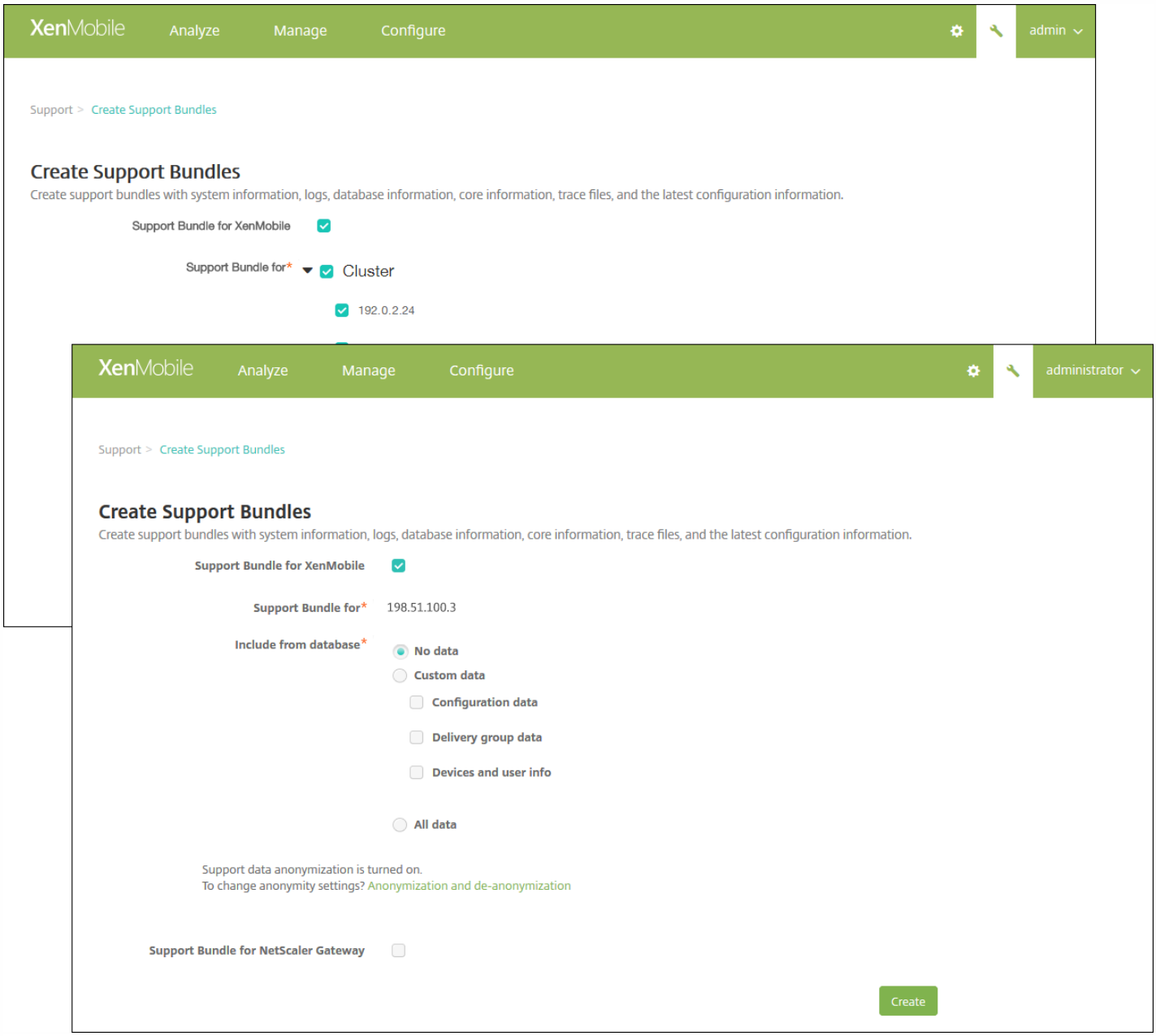
在 XenMobile 中创建支持包

Aug 11, 2016

如果要向 Citrix 报告问题或排除故障，可以创建支持包，然后将支持包上载到 Citrix Insight Services (CIS)。

1. 在 XenMobile 控制台中，单击右上角的扳手图标。 此时将显示**支持**页面。

2. 在**支持**页面上，单击**创建支持包**。 此时将显示**创建支持包**页面。 如果 XenMobile 环境包含加入群集的节点，将显示所有节点。



3. 确保选中**适用于 XenMobile 的支持包**复选框。

4. 如果 XenMobile 环境包含加入群集的节点，在**适用于此对象的支持包**中，可以选择所有节点或任何节点组合，用于从中提取

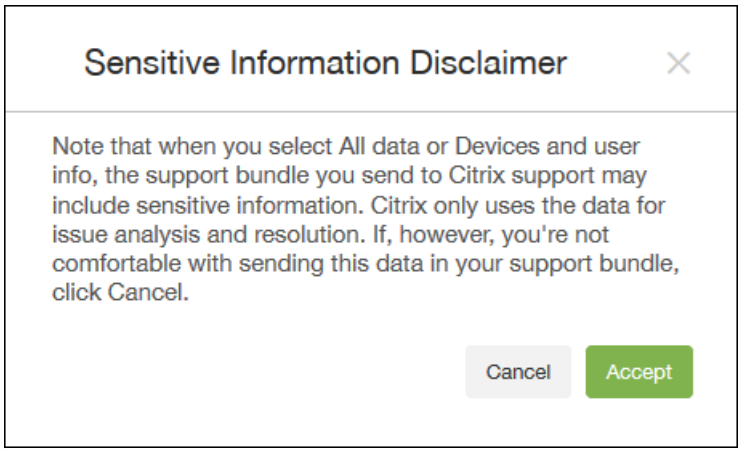
© 1999-2017 Citrix Systems, Inc. All rights reserved.

数据。

5. 在**包含的数据库内容**中，执行以下操作之一：

- 单击**无数据**。
- 单击**自定义数据**，然后选择以下任意选项或全部选项：
  - **配置数据库**：包括证书配置和设备管理器策略。
  - **交付组数据**：包括应用程序交付组信息，其中包含应用程序类型和交付策略详细信息。
  - **设备和用户信息**：包括设备策略、应用程序、操作和交付组。
- 单击**所有数据**。

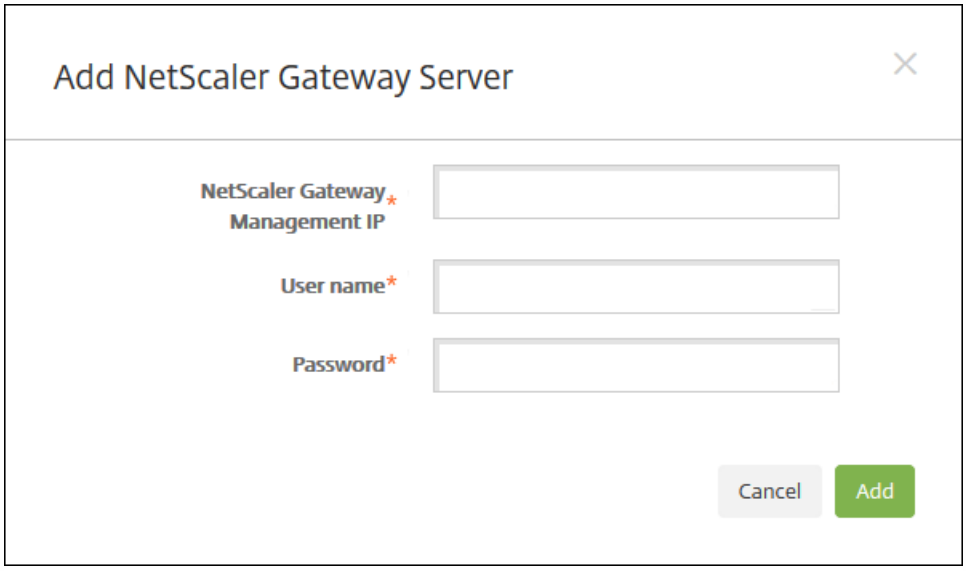
注意：如果选择**设备和用户信息**或**所有数据**，并且这是您创建的第一个支持包，则会显示**敏感信息免责声明**对话框。 阅读免责声明，然后单击**接受**或**取消**。 如果单击**取消**，支持包将无法上载到 Citrix。 如果单击**接受**，则可以将支持包上载到 Citrix，并且下次创建包含设备或用户数据的支持包时不会再出现免责声明。



6. 在**包含的数据库内容**下面，是一条关于是否在支持包中将敏感用户、服务器和网络数据设为匿名的说明。 默认设置是将数据设为匿名。 可以通过单击**匿名和取消匿名**链接更改此设置。 有关数据匿名的详细信息，请参阅匿名化支持包中的数据。

6. 如果要包含 NetScaler Gateway 中的支持包，请选择**适用于 NetScaler Gateway 的支持包**，然后执行以下操作：

- 单击**添加**。 将显示**添加 NetScaler Gateway 服务器**对话框。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在 **NetScaler Gateway 管理 IP** 中，键入要从中提取支持包数据的 NetScaler Gateway 的 NetScaler 管理 IP 地址。

  注意：如果要从已经添加的 NetScaler Gateway 服务器创建支持包，系统会提供 IP 地址。

- 在**用户名**和**密码**中，键入访问运行 NetScaler Gateway 的服务器所需的用户凭据。

  注意：如果要从已经添加的 NetScaler Gateway 服务器创建支持包，系统会提供用户名。

7. 单击**添加**。 新的 NetScaler Gateway 支持包将添加到表格中。

8. 重复步骤 7 以添加更多 NetScaler Gateway 支持包。

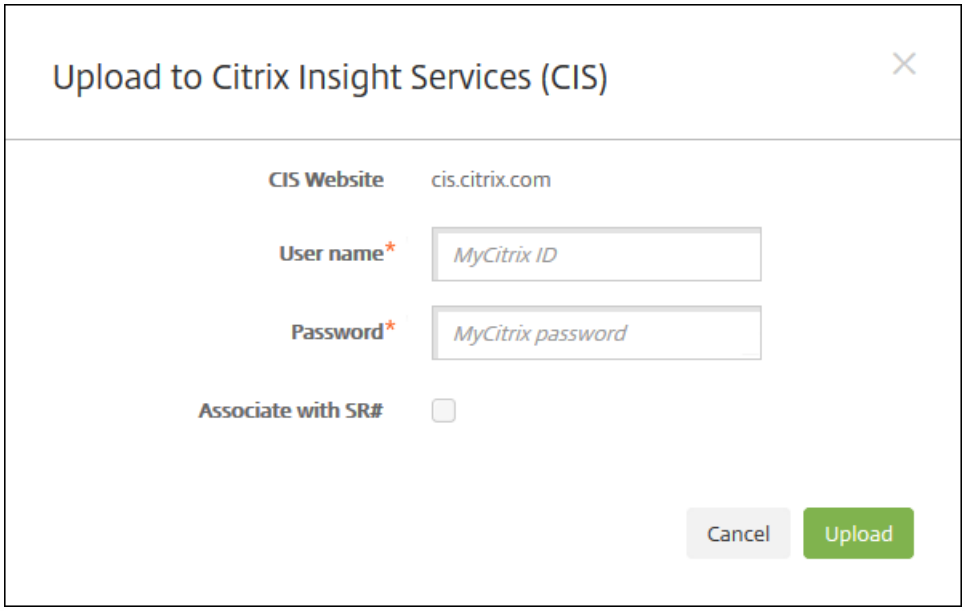
9. 单击**创建**。 将创建支持包，并显示两个新按钮：**上载到 CIS** 和**下载到客户端**。

继续执行将支持包上载到 Citrix Insight Services 或将支持包下载到客户端。

将支持包上载到 Citrix Insight Services

创建支持包后，可以将支持包上载到 Citrix Insight Services (CIS) 或将其下载到您的计算机。 下面的步骤显示如何将支持包上载到 CIS。 上载到 CIS 需要使用 MyCitrix ID 和密码。

1. 在**创建支持包**页面上，单击**上载到 CIS**。 将显示**上载到 Citrix Insight Services (CIS)** 对话框。



2. 在**用户名**中，键入 MyCitrix ID。

3. 在**密码**中，键入 MyCitrix 密码。

4. 如果要将此支持包与现有服务请求号码关联，请选中**与 SR 编号关联**复选框，并在显示的两个新字段中执行以下操作：

- 在 **SR#** 中，键入要将此包关联到的八位数服务请求号码。
- 在 **SR 说明**中，键入 SR 的说明。

5. 单击**上载**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果这是您第一次将支持包上载到 CIS，并且您尚未通过其他产品在 CIS 上创建帐户和接受“数据收集和隐私声明”协议，系统会显示以下对话框；您必须接受此协议才能开始上载操作。 如果您已经具有 CIS 帐户并且之前接受过此协议，支持包会立即开始上载。

6. 阅读协议并单击**同意并上载**。 将上载支持包。

将支持包下载到您的计算机

创建支持包之后，可以将此包上载到 CIS 或将其下载到您的计算机。 如果希望自己排除故障，可以将支持包下载到您的计算机。
在创建支持包页面上，单击下载到客户端。 支持包将下载到您的计算机。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

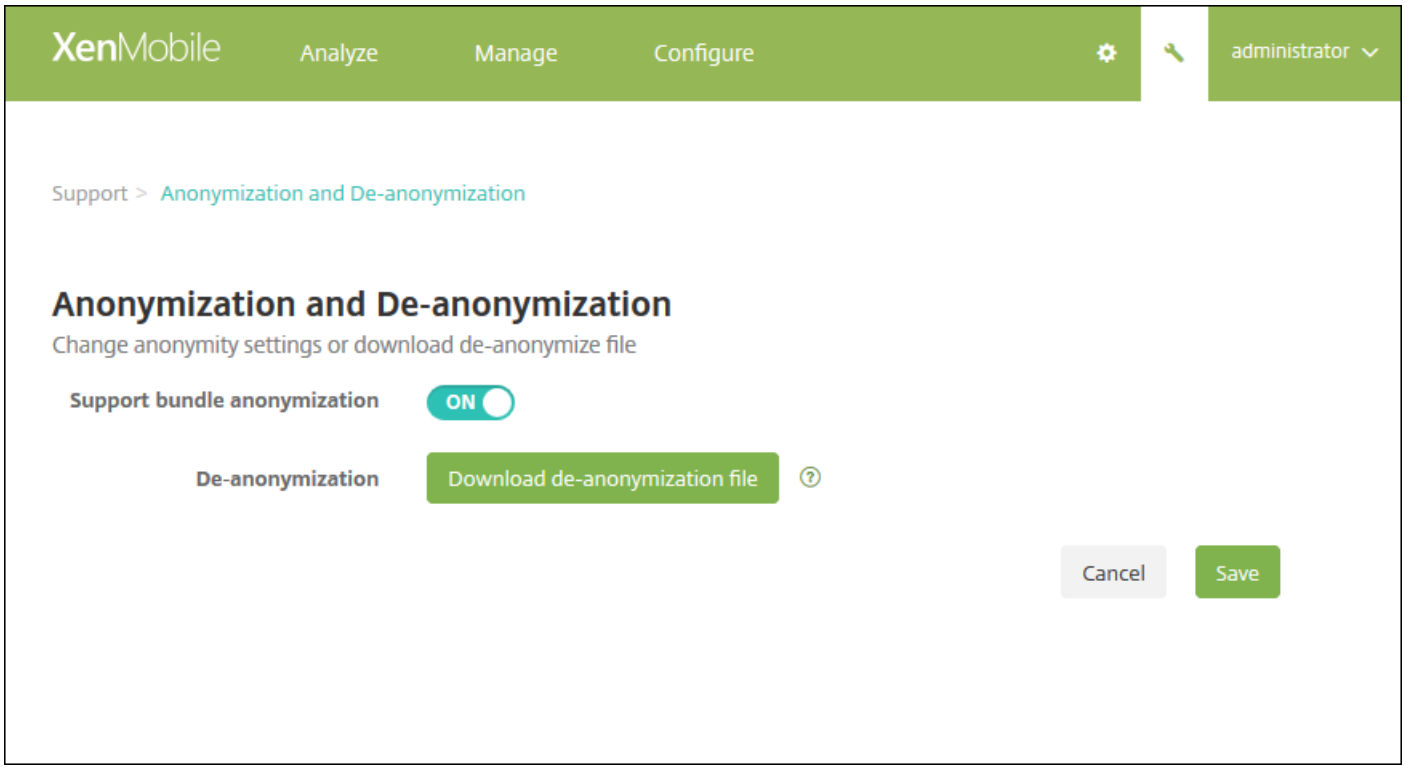
匿名化支持包中的数据

Aug 11, 2016

在 XenMobile 中创建支持包时，默认情况下会将敏感用户、服务器和网络数据设为匿名。 可以在“匿名和取消匿名”页面更改此行为。 还可以下载 XenMobile 在匿名化数据时保存的映射文件。 Citrix 支持人员可能会要求此文件对数据取消匿名，并查找特定用户和设备的问题。

1. 在 XenMobile 控制台中，单击右上角的扳手图标。 此时将显示**支持**页面。

2. 在**支持**页面的**高级**下面，单击**匿名和取消匿名**。 此时将显示**匿名和取消匿名**页面。



3. 在**支持包匿名**中，选择数据是否匿名。 默认值为**开**。

4. 在**取消匿名**旁边，单击**下载取消匿名文件**以下载映射文件，在 Citrix 支持需要特定设备或用户信息来诊断问题时，将此文件发送给他们。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

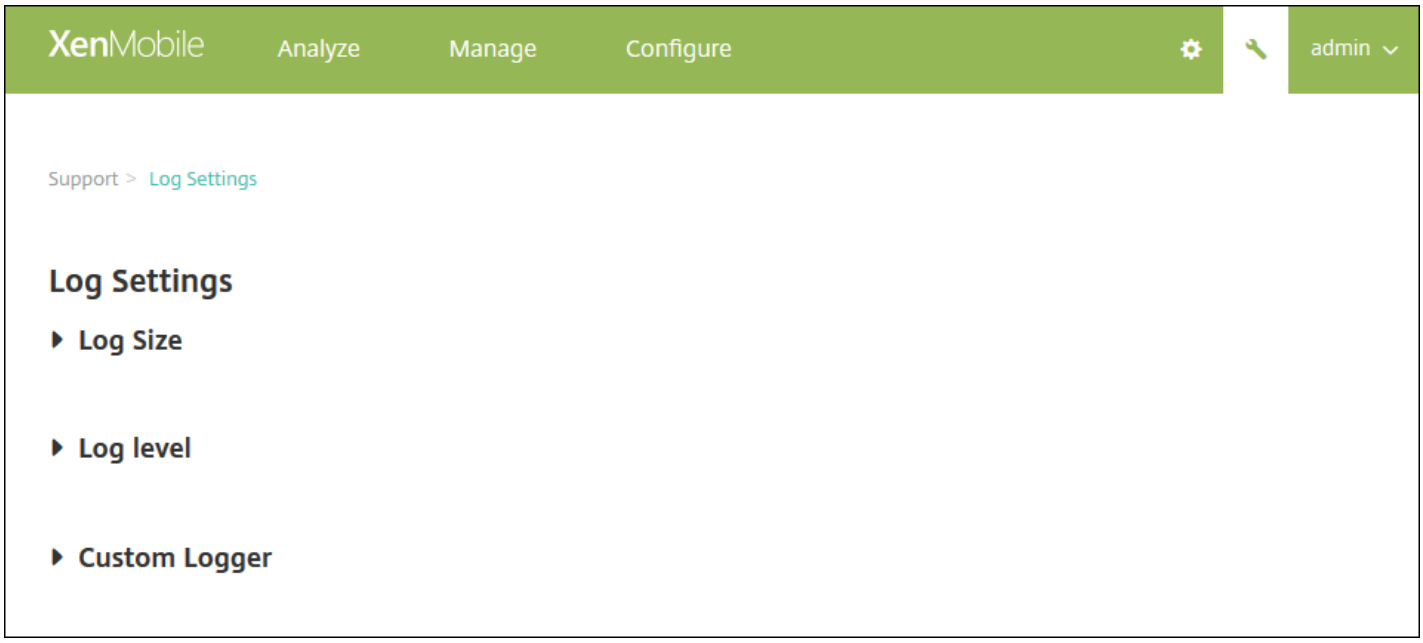
配置日志设置

Aug 11, 2016

您可以配置日志设置，以自定义 XenMobile 生成的日志的输出。 如果您的 XenMobile 服务器已加入群集，则在 XenMobile 控制台中配置日志设置时，这些设置将与群集中的所有其他服务器共享。

1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。 此时将显示**支持**页面。

2. 在**日志操作**下，单击**日志设置**。 此时将显示**日志设置**页面。



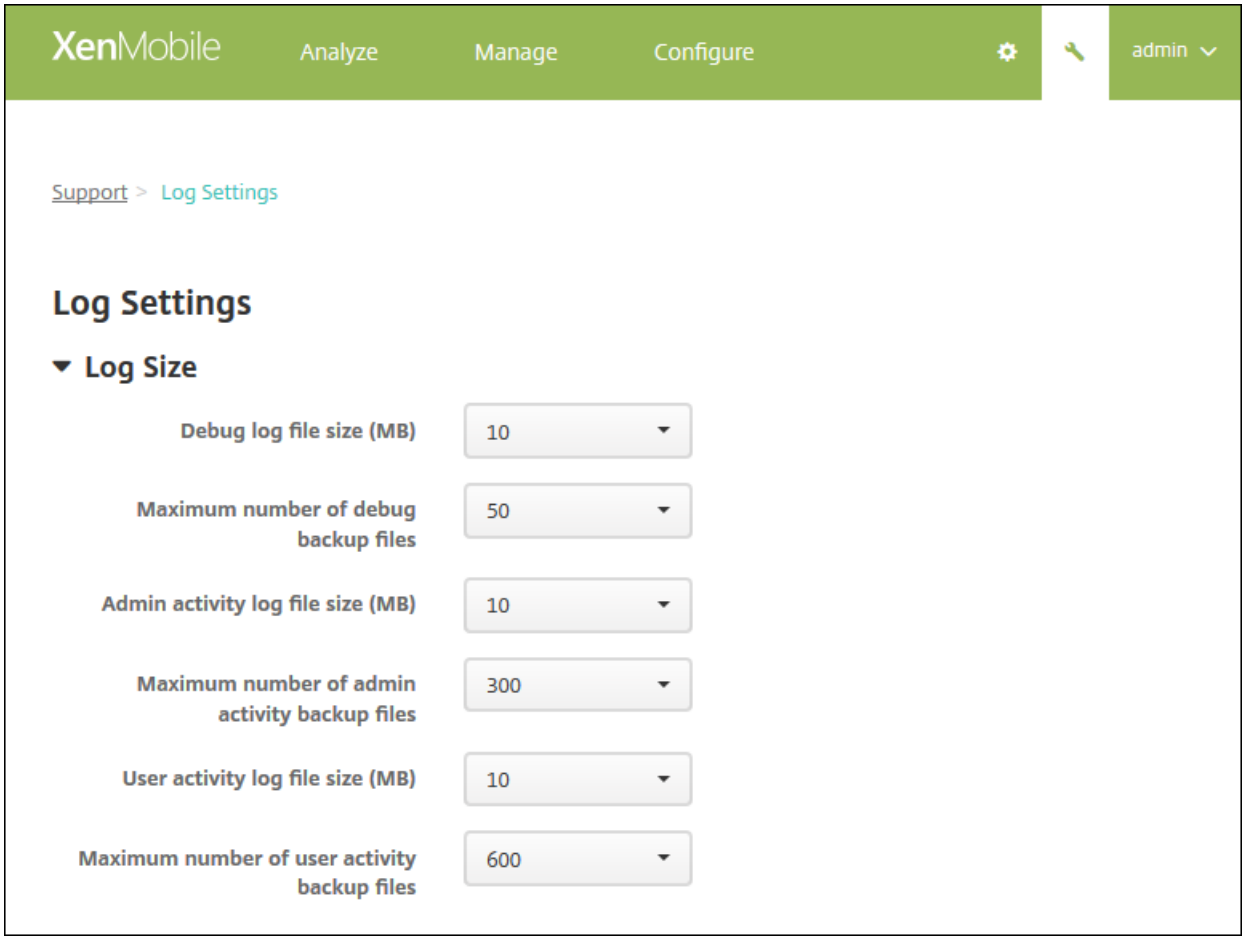
在**日志设置**页面上，您可以访问以下选项：

- **日志大小**。 使用此选项可以控制日志文件的大小和保留在数据库中的日志备份文件的最大数量。 日志大小适用于 XenMobile 支持的每个日志（调试日志、管理活动日志和用户活动日志）。
- **日志级别**。 使用此选项可将日志级别更改为静态设置。
- **自定义记录器**。 使用此选项可以创建自定义的日志记录器；自定义日志需要一个类名称和日志级别。

配置“日志大小”选项

1. 在**日志设置**页面上，展开**日志大小**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 配置以下设置：

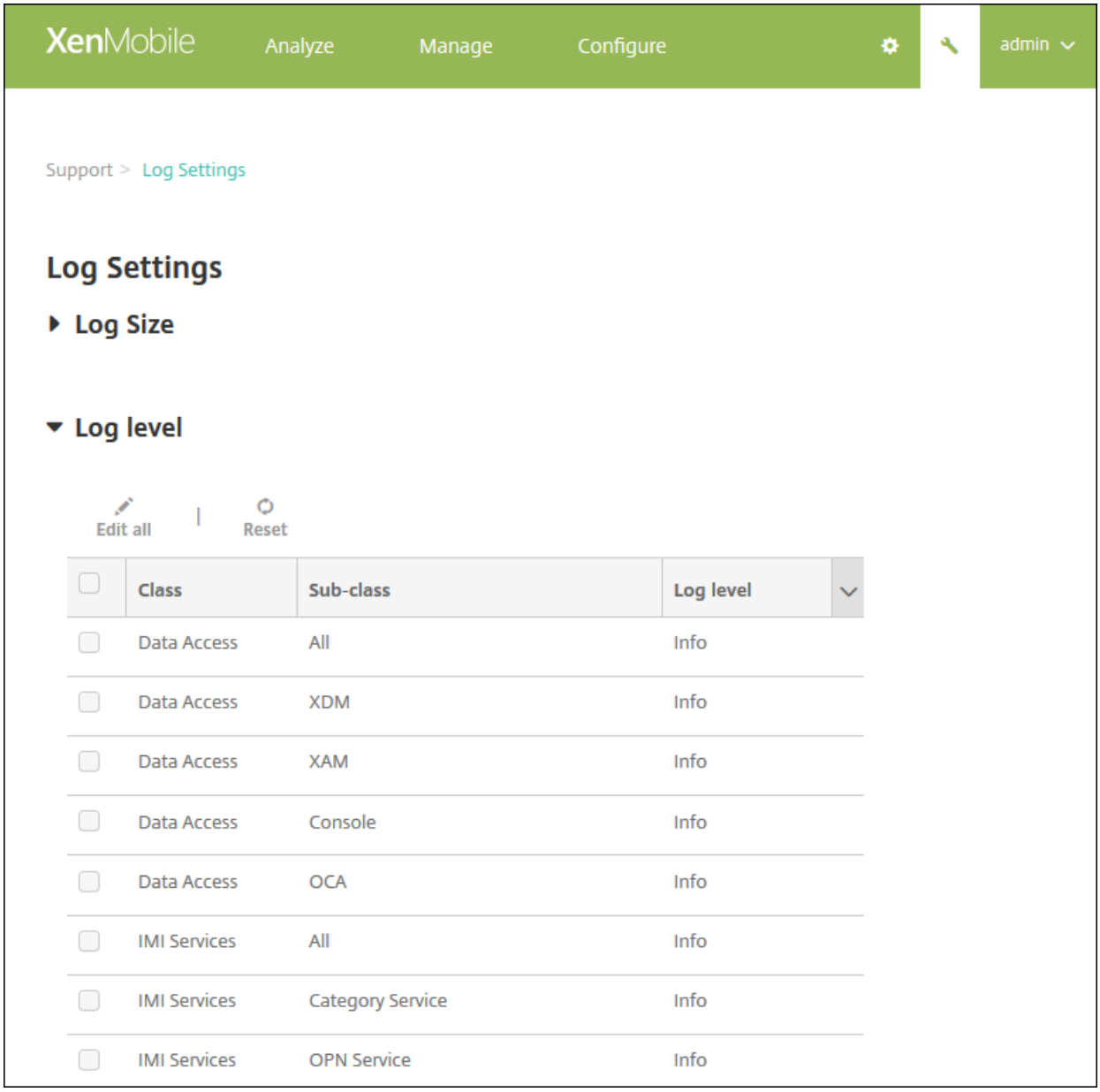
- **调试日志文件大小(MB)**：在列表中，单击一个介于 5 MB 到 20 MB 之间的大小，以更改调试文件的最大大小。 默认文件大小为 **10 MB**。
- **调试备份文件数上限**：在列表中，单击服务器保留的调试文件的最大数量。 默认情况下，XenMobile 在服务器上保留 50 个备份文件。
- **管理活动日志文件大小(MB)**：在列表中，单击一个介于 5 MB 到 20 MB 之间的大小，以更改管理活动文件的最大大小。 默认文件大小为 **10 MB**。
- **管理活动备份文件数上限**：在列表中，单击服务器保留的管理活动文件的最大数量。 默认情况下，XenMobile 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，单击一个介于 5 MB 到 20 MB 之间的大小，以更改用户活动文件的最大大小。 默认文件大小为 **10 MB**。
- **用户活动备份文件数上限**：在列表中，单击服务器保留的用户活动文件的最大数量。 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

通过日志级别，您可以指定 XenMobile 在日志中收集的信息类别。 可以为所有类别设置相同的级别，也可以将各个类别设置为特定的级别。

1. 在**日志设置**页面上，展开**日志级别**。 此时将显示一个包含所有日志类别的表格。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

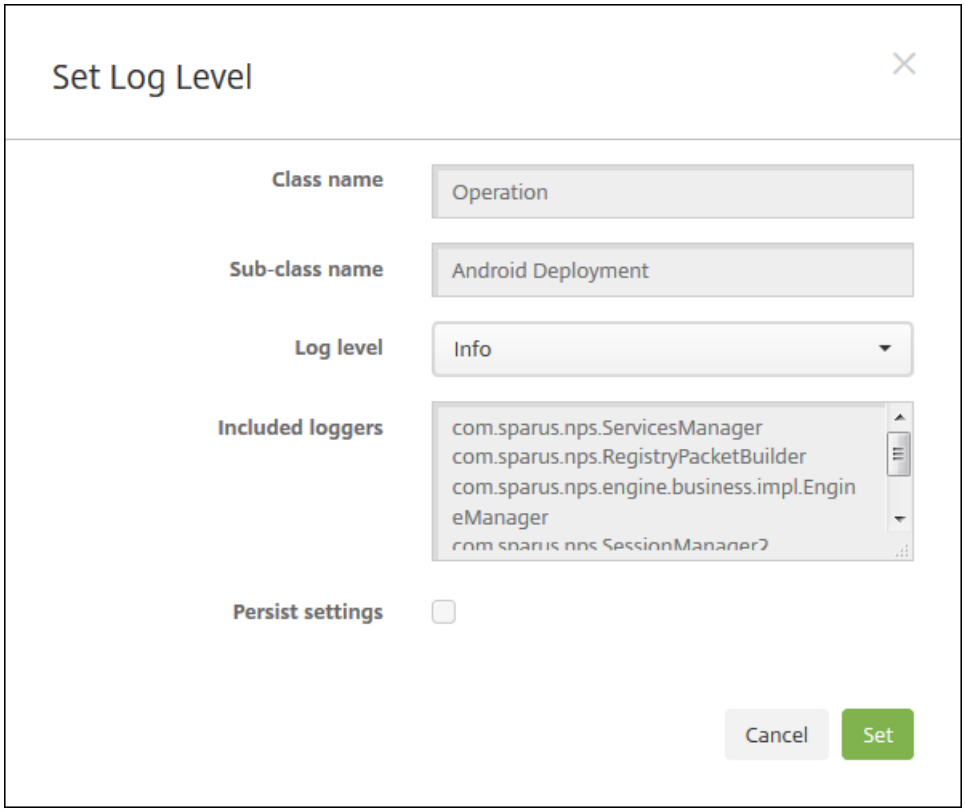


2. 执行以下操作之一：

- 单击某个“类别”旁边的复选框，然后单击**设置级别**以仅更改此类别的日志级别。
- 单击**编辑全部**以对表格中的所有类别应用日志级别更改。

此时将显示**设置日志级别**对话框，您可以在此对话框中设置日志级别并选择是否在重新启动 XenMobile 服务器时保留日志级别设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



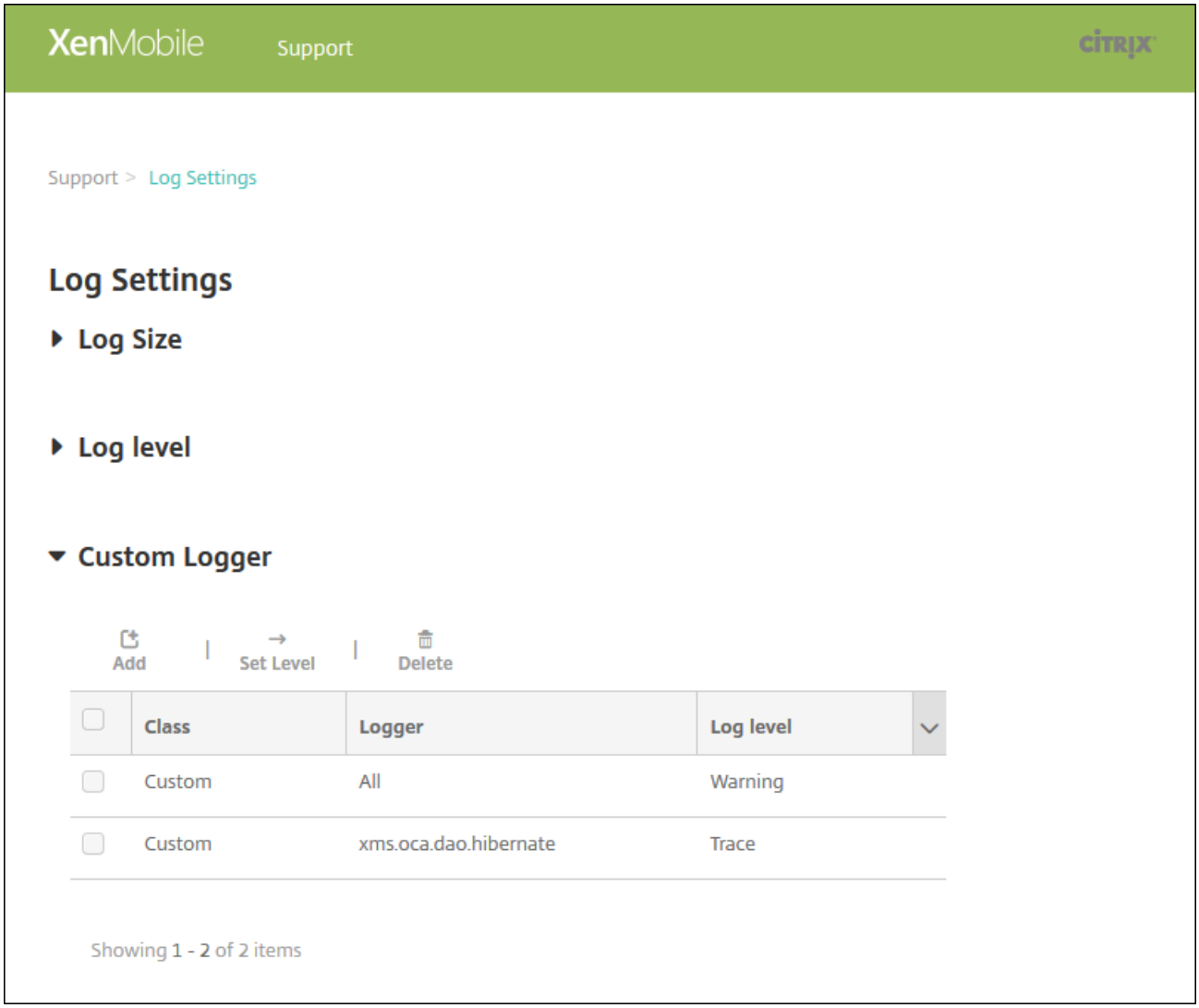
- **类别名称**：如果要更改所有类别的日志级别，此字段将显示全部，否则将显示各个类别的名称；此字段不可编辑。
- **子类别名称**：如果要更改所有类别的日志级别，此字段将显示“全部”，否则将显示单个子类别的名称；此字段不可编辑。
- **日志级别**：在列表中，单击日志级别。 支持的日志级别包括：
  - 致命
  - 错误
  - 警告
  - 信息
  - 调试
  - 跟踪
  - 关
- **Included Loggers**（包含日志记录器）：如果要更改所有类别的日志级别，此字段将为空，否则将显示各个类别的当前已配置的日志记录器；此字段不可编辑。
- **静态设置**：如果希望重新启动服务器时日志级别设置保持不变，请选中此复选框。 未选中此复选框表示当您重新启动服务器时，日志级别设置将恢复为默认值。

3. 单击**设置**提交更改。

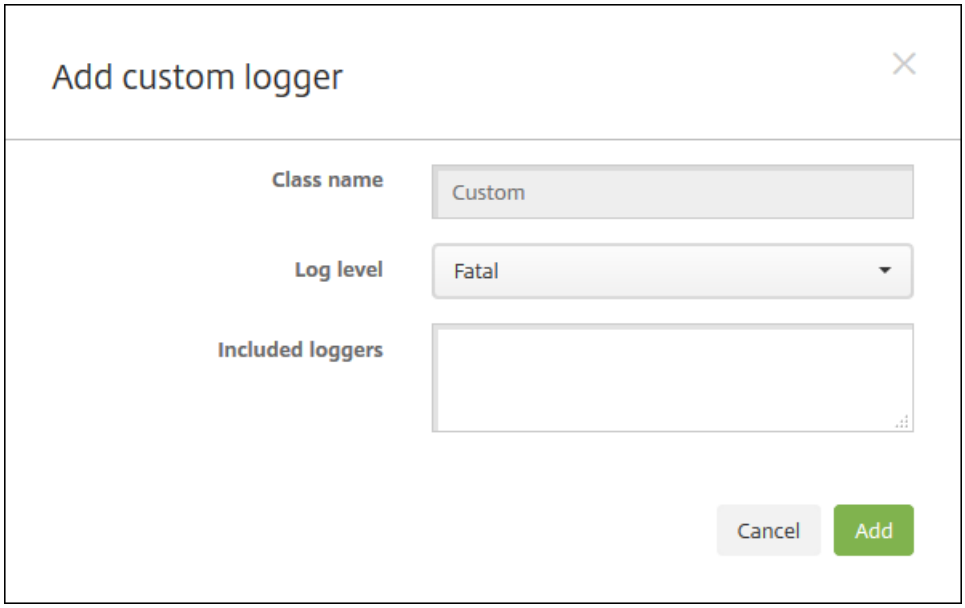
添加自定义日志记录器

1. 在**日志设置**页面上，展开**自定义记录器**。 此时将显示**自定义记录器**表格。 如果尚未添加任何自定义记录器，此表格最初为空。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 单击**添加**。 此时将显示**添加自定义记录器**对话框。

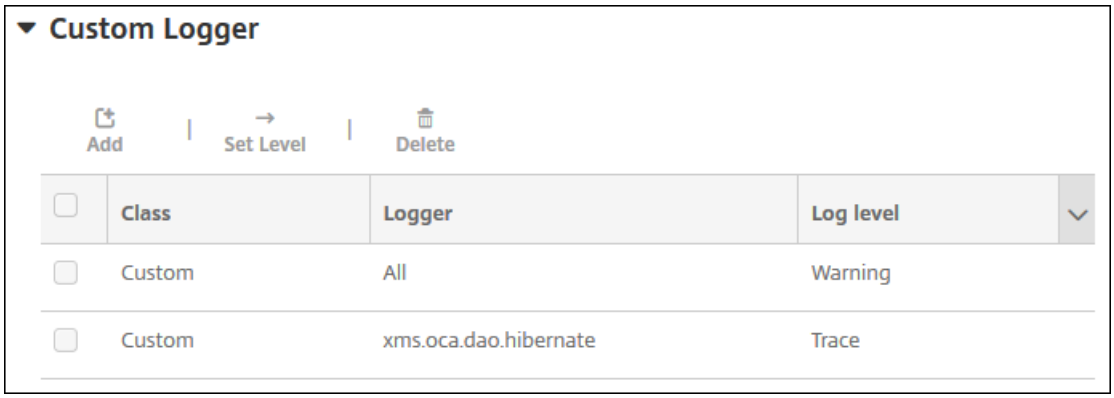


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 配置以下设置：

- **类别名称**：此字段显示**自定义**；此字段不可编辑。
- **日志级别**：在列表中，单击日志级别。 支持的日志级别包括：
  - 致命
  - 错误
  - 警告
  - 信息
  - 调试
  - 跟踪
  - 关
- **包括记录器**：键入要包含在自定义记录器中的特定记录器，或将此字段留空以包括所有记录器。

4. 单击**添加**。 自定义日志记录器将添加到 **Custom Logger**（自定义日志记录器）表格中。



删除自定义日志记录器

1. 在**日志设置**页面上，展开**自定义记录器**。

2. 选择要删除的自定义记录器。

2. 单击**删除**。 此时将显示一个对话框，询问您是否要删除该自定义日志记录器。 单击 **OK**（确定）。

重要：此操作无法撤消。

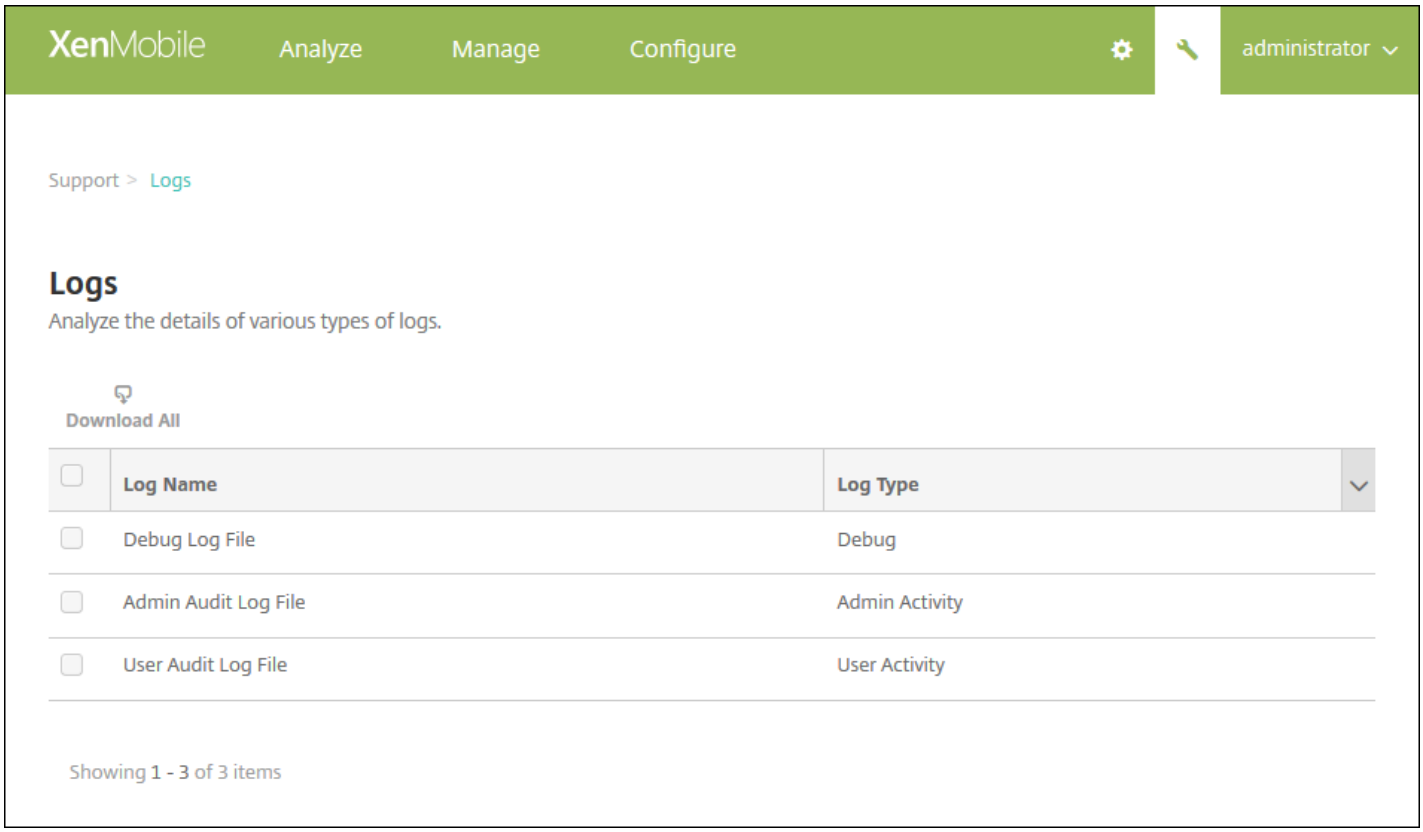
© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 XenMobile 中查看和分析日志文件

Aug 11, 2016

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。 单独的日志将显示在表格中。



3. 选择要查看的日志：

- 调试日志文件中包含对 Citrix 技术支持有用的信息，例如错误消息和服务器相关操作。
- 管理员审核日志文件中包含与 XenMobile 控制台上的活动有关的审核信息。
- 用户审核日志文件中包含与配置的用户有关的信息。

4. 使用表格顶部的操作可下载所有日志，查看、轮转或下载单个日志，或者删除选定的日志。

注意：

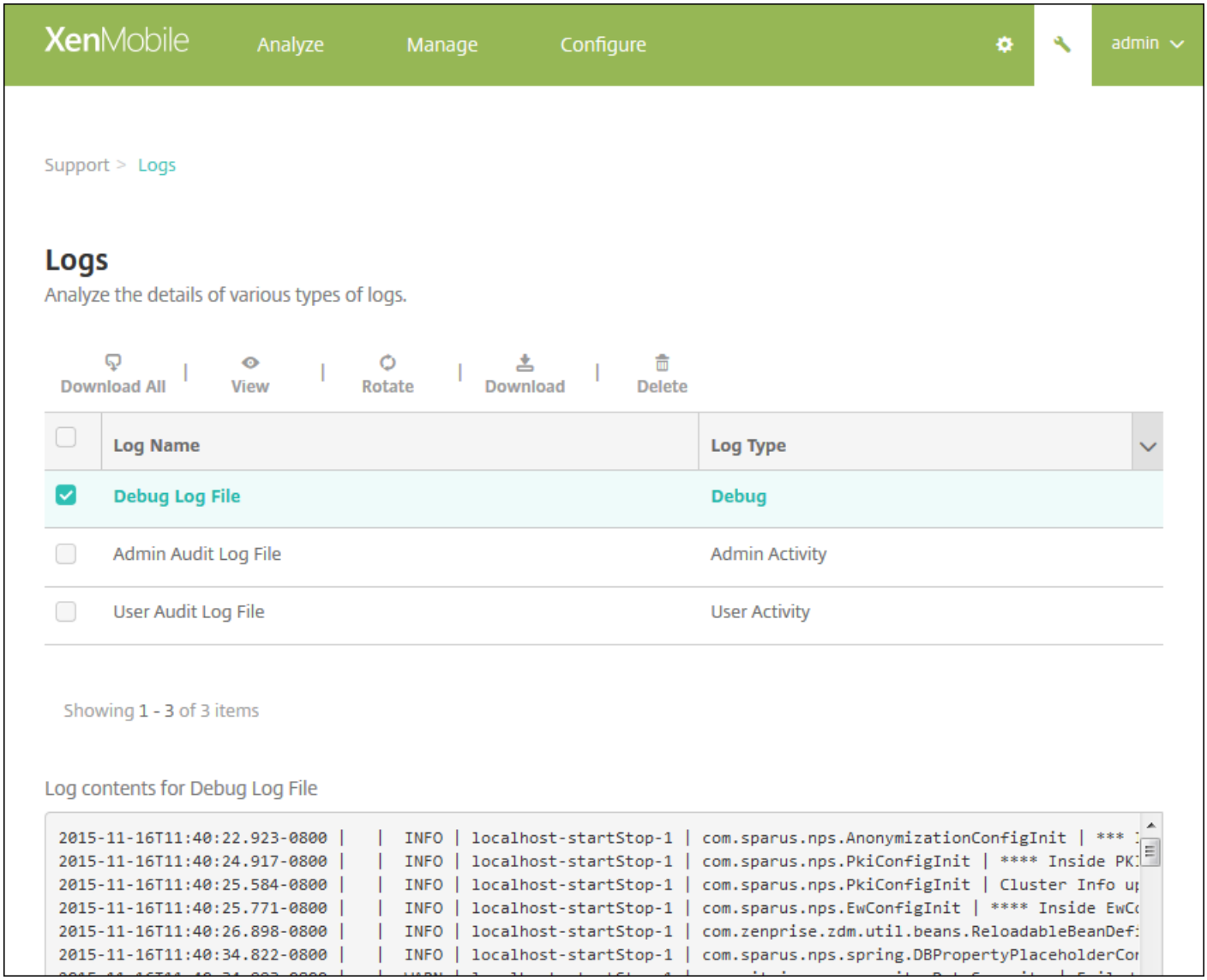
- 如果选择了多个日志文件，则只有**全部下载**和**删除**可用。
- 如果您有群集 XenMobile 服务器，只能查看所连接到的服务器的日志。 要查看其他服务器的日志，请使用以下下载选项之一。

5. 执行以下操作之一：

- **全部下载**：控制台下载系统中存在的所有日志（包括调试、管理员审核、用户审核、服务器日志等）。
- **查看**：在表格下方显示所选日志的内容。
- **轮转**：将当前日志文件存档并创建新文件以捕获日志条目。 存档日志文件时会显示一个对话框，请单击**轮转**以继续。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **下载**：控制台仅下载选定的一种日志文件类型，此外，还下载该类型对应的所有已存档的日志。
- **删除**：永久删除所选日志文件。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

远程支持

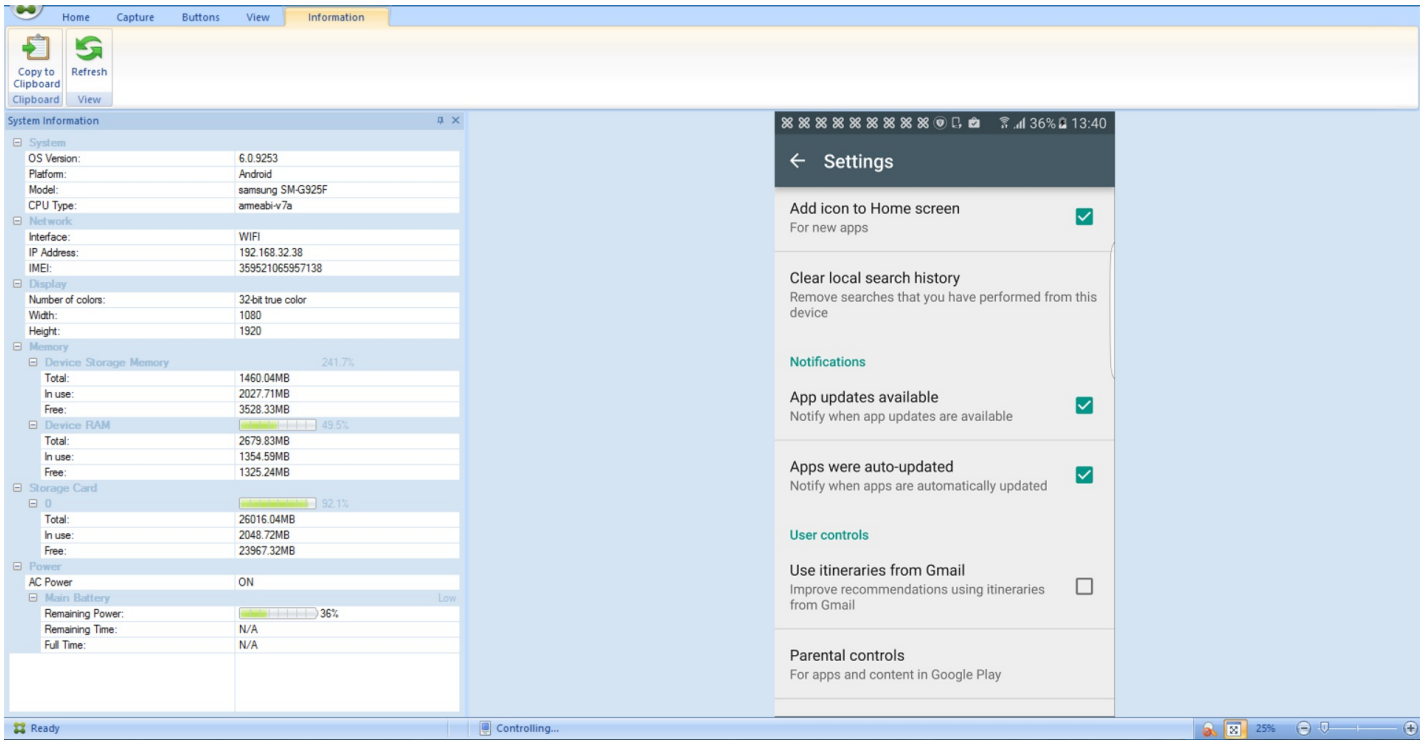
Aug 11, 2016

通过 Remote Support，您的技术支持代表能够远程控制托管的 Windows 和 Android 移动设备。 Remote Support 适用于所有 Windows 移动设备和 Android Samsung SAFE 设备。 不支持对 iOS 设备进行远程控制。

> **注意**
>
> XenMobile Remote Support 在 XenMobile Cloud 10.x 版本中不可用。

在远程控制会话期间：

- 用户会在其移动设备上看到一个图标，指示远程控制会话处于活动状态。
- Remote Support 用户会看到 Remote Support 应用程序窗口和远程控制窗口，其中显示了受控制的设备。



利用 Remote Support 可以执行以下操作：

- 远程登录到用户的移动设备并控制用户的屏幕。 用户可观看您在屏幕上的操作，这对于培训用户而言也很有帮助。
- 实时导航和修复远程设备。 您可以更改配置、解决操作系统问题、禁用或停止有问题的应用程序或进程。
- 通过远程禁用网络访问权限、停止恶意进程以及删除应用程序或恶意软件，可以隔立和遏制这些威胁，使其不会传播到其他移动设备。
- 远程启用设备响铃和拨打电话，以帮助用户找到设备。 如果用户找不到设备，可以擦除设备以确保敏感数据不会受到损害。

Remote Support 还使支持人员能够执行以下操作：

- 显示一个或多个 XenMobile 服务器中所有连接设备的列表。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 显示系统信息，包括设备型号、操作系统级别、国际移动设备标识 (IMEI) 以及序列号、内存和电池状态及连接性。
- 显示 XenMobile 服务器的用户和组。
- 运行设备任务管理器，可在其中显示并结束活动进程，并可以重新启动移动设备。
- 运行远程文件传输，包括移动设备与中央文件服务器之间的双向文件传输。
- 成批下载软件程序并安装到一个或多个移动设备上。
- 配置设备上的远程注册表项设置。
- 利用实时设备屏幕远程控制功能优化低带宽移动网络的响应时间。
- 显示大多数移动设备品牌和型号的设备外观。 显示用于添加新设备型号和映射物理键的皮肤编辑器。
- 启用设备屏幕捕获、录制和播放，并能够捕获设备上的一系列交互操作以创建视频 AVI 文件。
- 利用共享白板、VoIP 语音通信和移动用户与技术支持人员之间的聊天功能举行实时会议。

远程支持的系统要求

Remote Support 软件可安装在满足以下要求的 Windows 计算机上。 有关端口要求的信息，请参阅端口要求。

支持的平台

- Intel Xeon/Pentium 4 -1 GHz 工作站类（最低要求）
- 512 MB RAM（最低要求）
- 100 MB 可用磁盘空间（最低要求）

支持的操作系统

- Microsoft Windows 2003 Server Standard Edition 或 Enterprise Edition SP1 或更高版本
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 或更高版本
- Microsoft Windows Vista SP1 或更高版本
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

安装 Remote Support 软件

1. 要下载 Remote Support 安装程序，请转到 XenMobile 10 下载页面并登录您的帐户。
2. 展开**工具**，然后下载 XenMobile Remote Support v9。
   最新版本的 Remote Support 文件名为 XenMobileRemoteSupport-9.0.0.35265.exe。
3. 双击 Remote Support 安装程序，然后按照安装向导中的说明进行操作。

要通过命令行安装 Remote Support，请执行以下命令：

运行以下命令：

RemoteSupport.exe /S

其中，*RemoteSupport* 为安装程序的名称。 例如：

XenMobileRemoteSupport-9.0.0.35265.exe /S

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装 Remote Support 软件时，可以使用以下变量：

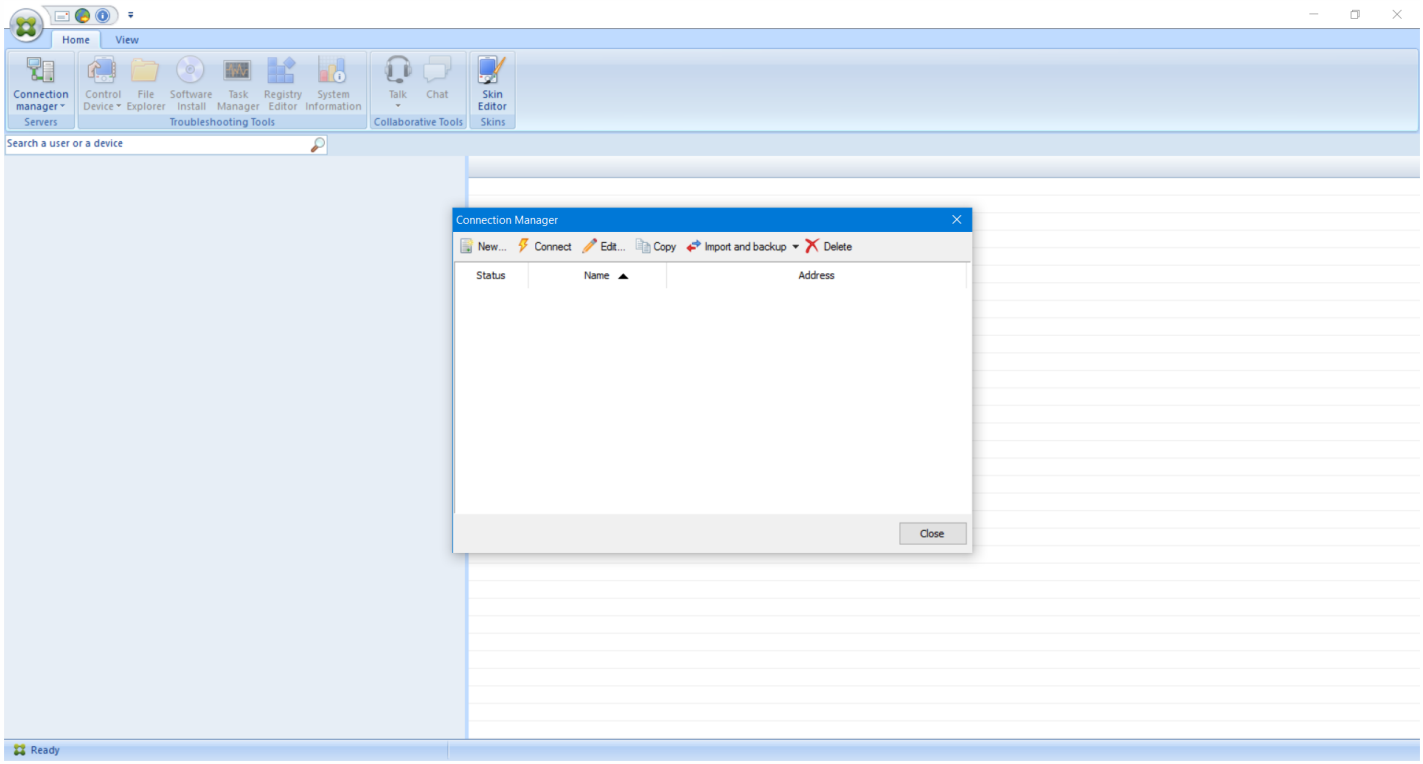
- /S: 使用默认参数无提示安装 Remote Support 软件。
- /D=dir: 指定自定义安装目录。

将 Remote Support 连接到 XenMobile

要建立与托管设备的远程支持连接，必须添加从 Remote Support 到用于管理设备的 XenMobile 服务器的连接。 该连接在“通道策略”（一项适用于 Android 和 Windows Mobile/CE 设备的设备策略）中定义的应用程序通道上运行。 必须根据应用程序通道设备策略中所述定义应用程序通道，然后才能将 Remote Support 连接到 XenMobile。

1. 启动 Remote Support 软件，并使用您的 XenMobile 凭据登录。

2. 在 **Connection Manager**（连接管理器）中，单击 **New**（新建）。



3. 在 **Connection Configuration**（连接配置）对话框中的 **Server**（服务器）选项卡上，输入以下值：

   在 **Configuration name**（配置名称）中，输入配置条目的名称。

   在 **Server IP address or name**（服务器 IP 地址或名称）中，键入 XenMobile 服务器的 IP 地址或 DNS 名称。

   在 **Port**（端口）中，键入在 XenMobile 服务器配置中定义的 TCP 端口号。

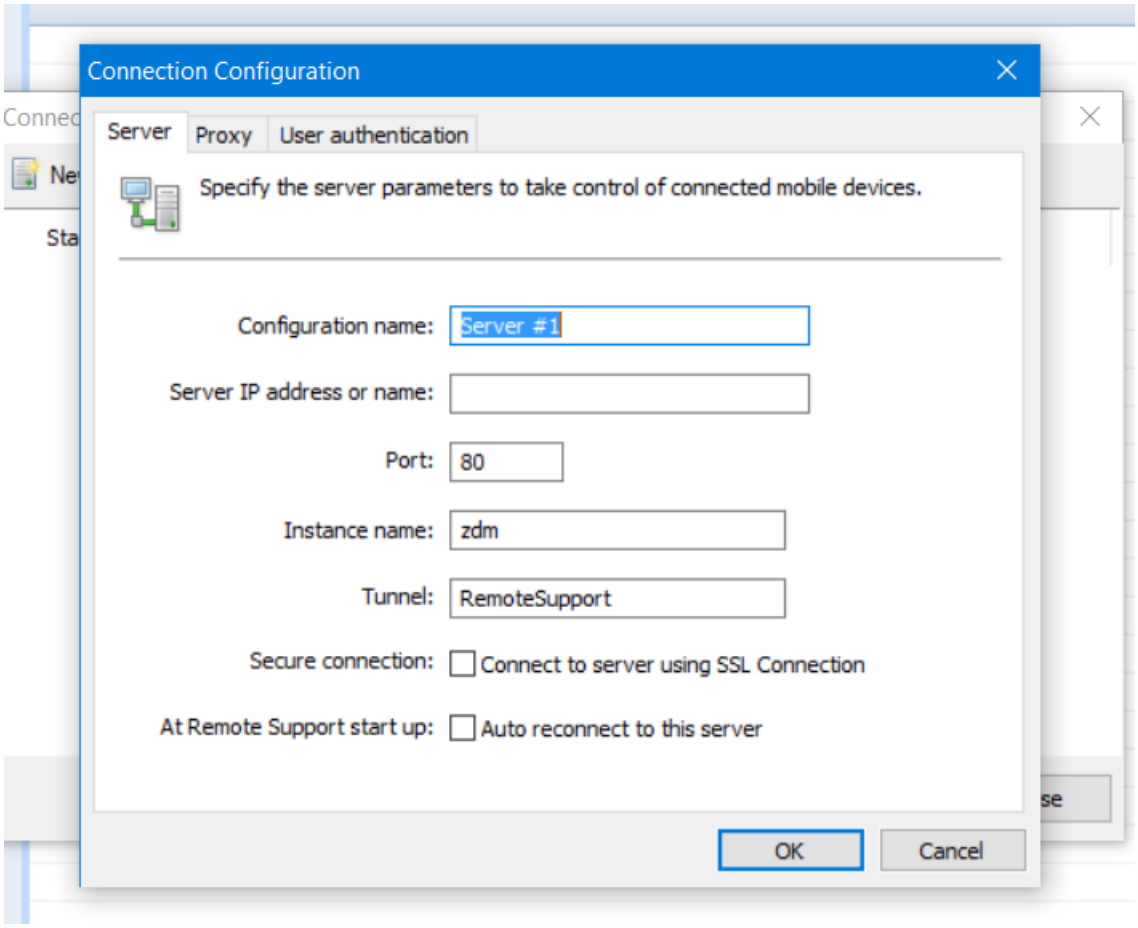
   如果 XenMobile 是多租户部署的一部分，请在 **Instance name**（实例名称）中键入实例名称。

   在 **Tunnel**（通道）中，键入通道策略的名称。

   选中 **Connect to server using SSL Connection**（使用 SSL 连接连接到服务器）复选框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

选中 **Auto reconnect to this server**（自动重新连接此服务器）复选框，在 Remote Support 应用程序每次启动时连接到所配置的 XenMobile 服务器。



4. 在 **Proxy**（代理）选项卡中，选择 **Use a http proxy server**（使用 HTTP 代理服务器），然后输入以下信息：

   在 **Proxy IP Address**（代理 IP 地址）中，键入代理服务器的 IP 地址。

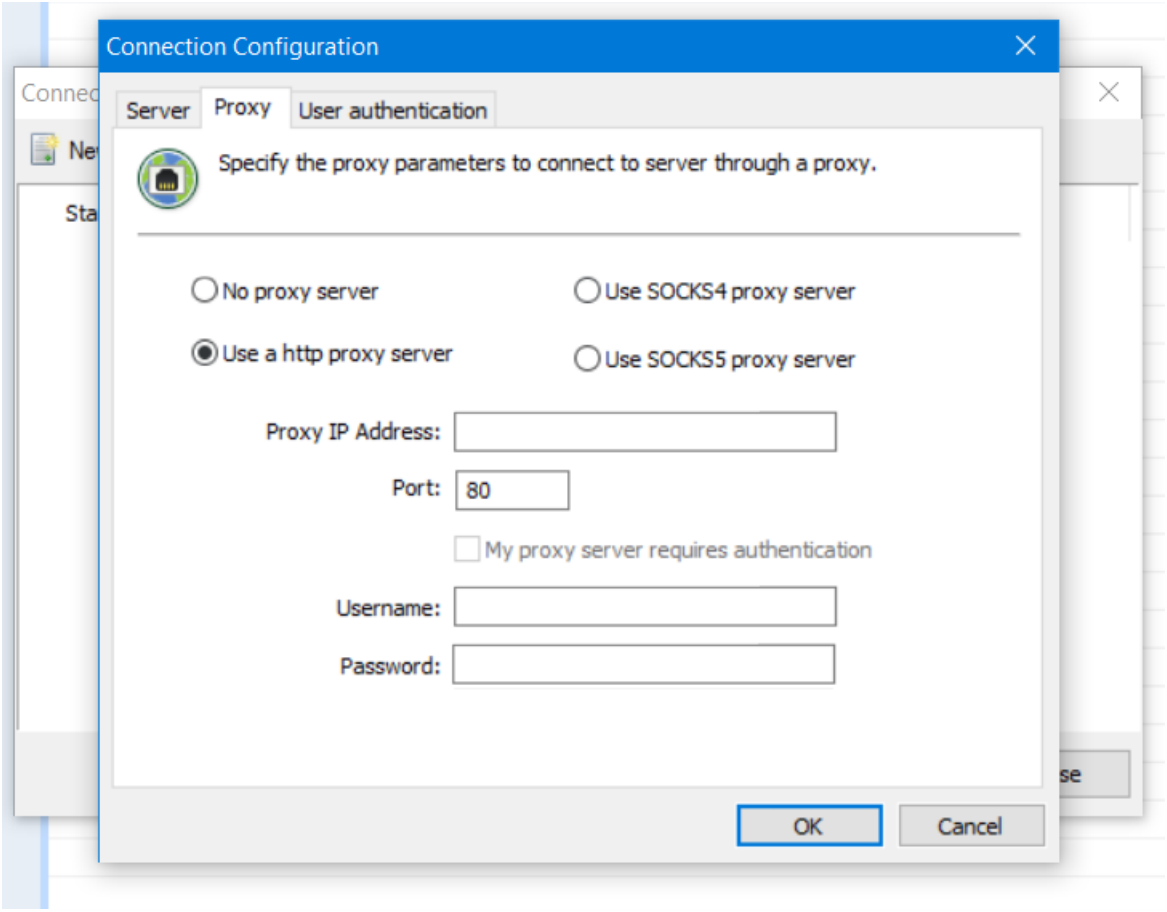
   在 **Port**（端口）中，键入代理使用的 TCP 端口号。

   如果代理服务器要求执行身份验证才能传输流量，请选中 **My proxy server requires authentication**（我的代理服务器要求执行身份验证）复选框。

   在 **Username**（用户名）中，键入在代理服务器上执行身份验证时使用的用户名。

   在 **Password**（密码）中，键入在代理服务器上执行身份验证时使用的密码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 在 **User Authentication**（用户身份验证）选项卡中，选中 **Remember my login and password**（记住我的登录名和密码）复选框，然后输入凭据。

6. 单击**确定**。

要连接到 XenMobile，请双击所创建的连接，然后输入为该连接配置的用户名和密码。

为 Samsung Knox 设备启用远程支持

可以在 XenMobile 中创建远程支持策略以授予您远程访问 Samsung KNOX

设备的权限。 可以配置两种类型的支持：

- 基本：使用此选项，您可以查看与设备有关的诊断信息（例如系统信息）、正在运行的进程、任务管理器（内存和 CPU 使用率）、已安装的软件文件夹内容等。
- 高级：此选项允许您远程控制设备的屏幕，包括控制颜色（在主窗口中或者在独立的浮动窗口中）、在技术支持人员与用户之间建立 VoIP 会话、配置设置以及在技术支持人员与用户之间建立文字消息会话的功能。

有关如何配置远程支持策略的信息，请参阅远程支持设备策略。

使用 Remote Support 会话

© 1999-2017 Citrix Systems, Inc. All rights reserved.

启动 Remote Support 后，Remote Support 应用程序窗口左侧将显示在 XenMobile 管理控制台中定义的 XenMobile 用户组。默认情况下，仅显示包含当前已连接的用户的组。 您可以在用户条目旁边看到每个用户的设备。

1. 要查看所有用户，请展开左侧列中的每个组。
   当前已连接到 XenMobile 服务器的用户用绿色图标指示。
2. 要显示所有用户（包括当前未连接的用户），请单击 **View**（视图）并选择 **Non-connected devices**（未连接的设备）。
   此时将显示未连接的用户，但不带绿色小图标。

连接到 XenMobile 服务器但未分配给用户的设备在匿名模式下显示。 （字符串 **Anonymous**（匿名）将出现在列表中。）您可以像控制登录用户的设备一样控制这些设备。

要控制某个设备，请单击该设备对应的行以将其选中，然后单击 **Control Device**（控制设备）。 该设备将出现在远程控制窗口中。 可以使用下面所示的一些方法与受控设备进行交互：

- 在主窗口或独立的浮动窗口中控制设备的屏幕，包括控制颜色。
- 建立技术支持人员与用户之间的 IP 语音会话 (VoIP)。 配置 VoIP 设置。
- 与用户建立聊天会话。
- 访问设备的任务管理器以管理项目，例如内存使用率、CPU 使用率和正在运行的应用程序。
- 浏览移动设备的本地目录。 传输文件。
- 在 Windows 移动设备中编辑设备注册表。
- 显示设备系统信息和所有已安装的软件。
- 更新移动设备与 XenMobile 服务器的连接状态。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 命令行接口选项

Aug 11, 2016

您随时可以在安装 XenMobile 的虚拟机管理程序上访问以下命令行接口 (CLI) 选项 — Citrix XenServer、Microsoft Hyper-V 或 VMware ESXi。

以下是可以从 Main（主菜单）选择的选项，以及分别为前四个选项“Configuration”（配置）、“Clustering”（群集）、System（系统）和“Troubleshooting”（故障排除）显示的菜单。

Main（主菜单）

---

[0] Configuration（配置）

[1] Clustering（群集）

[2] System（系统）

[3] Troubleshooting（故障排除）

[4] Help（帮助）

[5] Log Out（注销）

Choice: [0 - 5]（选择: [0 - 1]）

“Configuration”（配置）菜单选项

从主菜单选择“Configuration”（配置）选项时，将显示以下菜单：

[0] Back to Main Menu（返回主菜单）

[1] Network（网络）

[2] Firewall（防火墙）

[3] Database（数据库）

[4] Listener Ports（侦听器端口）

Choice: [0 - 4]（选择: [0 - 1]）

选择“Network”（网络）选项时，系统会提示您重新启动以保存更改。

选择“Firewall”（防火墙）选项时，您会收到以下提示：

Configure which services are enabled through the firewall.（配置通过防火墙启用的服务。）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Can optionally configure allow access white lists:（可以选择性配置允许访问白名单:）

- comma separated list of hosts or networks（- 逗号分隔的主机或网络列表）

- e.g. 10.20.5.3, 10.20.6.0/24（- 例如: 10.20.5.3, 10.20.6.0/24）

- an empty value means no access restriction（- 空值表示无访问限制）

- enter c as value to clear list（- 输入值 c 可清除列表）

HTTP 服务

端口：80

Enable access (y/n) [y]:（启用访问(y/n) [y]:）

Management HTTPS service（管理 HTTPS 服务）

端口：4443

Enable access (y/n) [y]:（启用访问(y/n) [y]:）

SSH 服务

Port [22]:（端口 [8081]:）

Enable access (y/n) [y]:（启用访问(y/n) [y]:）

Access white list []:（访问白名单[]:）

Management API (for initial staging) HTTPS service（管理 API (用户初始过度) HTTPS 服务）

Port [30001]:（端口 [8081]:）

Enable access (y/n) [y]:（启用访问(y/n) [y]:）

Access white list []:（访问白名单[]:）

Remote support tunnel（远程支持通道）

Port [8081]:（端口 [8081]:）

Enable access (y/n) [n]:（启用访问(y/n) [n]:）

选择“Database”（数据库）选项时，您会收到以下提示：

Type: [mi]（类型: [mi]）

Use SSL (y/n) [y]:（使用 SSL (y/n) [y]:）

Upload Root Certificate (y/n) [y]:（上载根证书 (y/n) [y]:）

Copy or Import (c/i) [c]:（复制或导入 (c/i) [c]:）

“Clustering”（群集）菜单选项

© 1999-2017 Citrix Systems, Inc. All rights reserved.

从主菜单选择“Clustering”（群集）选项时，将显示以下菜单：

[0] Back to Main Menu（返回主菜单）

[1] Show Cluster Status（显示群集状态）

[2] Enable/Disable cluster（启用/禁用群集）

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

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

[5] Display Hazelcast Cluster（显示 Hazelcast 群集）

Choice: [0 - 5]（选择: [0 - 1]）

选择启用群集时，将显示以下消息：

To enable realtime 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.（要在群集成员之间启用实时通信，请使用 CLI 菜单上的“Firewall”菜单选项打开端口 80。同时在“Firewall”设置下配置访问白名单以限制访问。）

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.（您已选择禁用群集。无需访问端口 80。请禁用此端口）。

选择群集成员白名单时，如果已禁用群集，将显示以下消息：

Cluster is disabled. Please enable it.（群集已被禁用，请将其启用。）

如果启用群集，将显示以下选项：

Current White List:（当前白名单:）

- comma separated list of hosts or network（- 逗号分隔的主机或网络列表）

- e.g. 10.20.5.3, 10.20.6.0/24（- 例如: 10.20.5.3, 10.20.6.0/24）

- an empty value means no access restriction（- 空值表示无访问限制）

Please enter hosts or networks to be white listed:（请输入要列入白名单的主机或网络:）

当选择启用或禁用 SSL 卸载时，将显示以下消息：

Enabling SSL offload will open port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.（启用 SSL 卸载将为所有人打开端口 80。请在“Firewall”设置下配置访问白名单以限制访问。）

选择显示 Hazelcast 群集时，将显示以下选项：

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Hazlecast Cluster Members:（Hazlecast 群集成员:）

[列出 IP 地址]

NOTE: If an configured node is not part of the cluseter, please reboot that node.（注意: 如果某个配置节点不属于群集，请重新启动此节点。）

“System”（系统）菜单选项

从主菜单选择“System”（系统）选项时，将显示以下菜单：

---

[0] Back to Main Menu（返回主菜单）

[1] Display System Date（显示系统日期）

[2] Set Time Zone（设置时区）

[3] Display System Disk Usage（显示系统磁盘使用情况）

[4] Update Hosts File（更新主机文件）

[5] Proxy Server（代理服务器）

[6] Admin (CLI) Password（管理(CLI)密码）

[7] Restart Server（重新启动服务器）

[8] Shutdown Server（关闭服务器）

[9] Advanced Settings（高级设置）

Choice: [0 - 9]（选择: [0 - 1]）

“Troubleshooting”（故障排除）菜单选项

从主菜单选择“Troubleshooting”（故障排除）选项时，将显示以下菜单：

---

[0] Back to Main Menu（返回主菜单）

[1] Network Utilities（网络实用程序）

[2] Logs（日志）

[3] Support Bundle（支持包）

Choice: [0 - 3]（选择: [0 - 1]）

选择“Network Utilities”（网络实用程序）选项时，将显示以下菜单：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

---

[0] Back to Troubleshooting Menu（返回故障排除菜单）

[1] Network Information（网络信息）

[2] Show Routing Table（显示路由表）

[3] Show Address Resolution Protocol (ARP) Table（显示地址解析协议(ARP)表）

[4] PING

[5] Traceroute

[6] DNS Lookup（DNS 查找）

[7] Network Trace（网络跟踪）

Choice: [0 - 7]（选择: [0 - 1]）

选择“Logs”（日志）选项时，将显示以下菜单：

Logs Menu（日志菜单）

---

[0] Back to Troubleshooting Menu（返回故障排除菜单）

[1] Display Log File（显示日志文件）

Choice: [0 - 1]（选择: [0 - 1]）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Analyzer 工具

Oct 21, 2016

XenMobile Analyzer 是一个基于云的工具，可以使用该工具诊断与 XenMobile 的安装和其他功能有关的问题并进行故障排除。该工具检查您的 XenMobile 环境中是否存在设备或用户注册和身份验证问题。

要启用检查，需要将该工具配置为指向您的 XenMobile 服务器，并且需要提供服务器部署类型、移动平台、身份验证类型以及用户的测试凭据等信息。 该工具随后将连接到服务器并扫描您的环境，检查是否存在配置问题。 如果 XenMobile Analyzer 发现问题，该工具将提供更正问题的建议。

XenMobile Analyzer 的主要功能

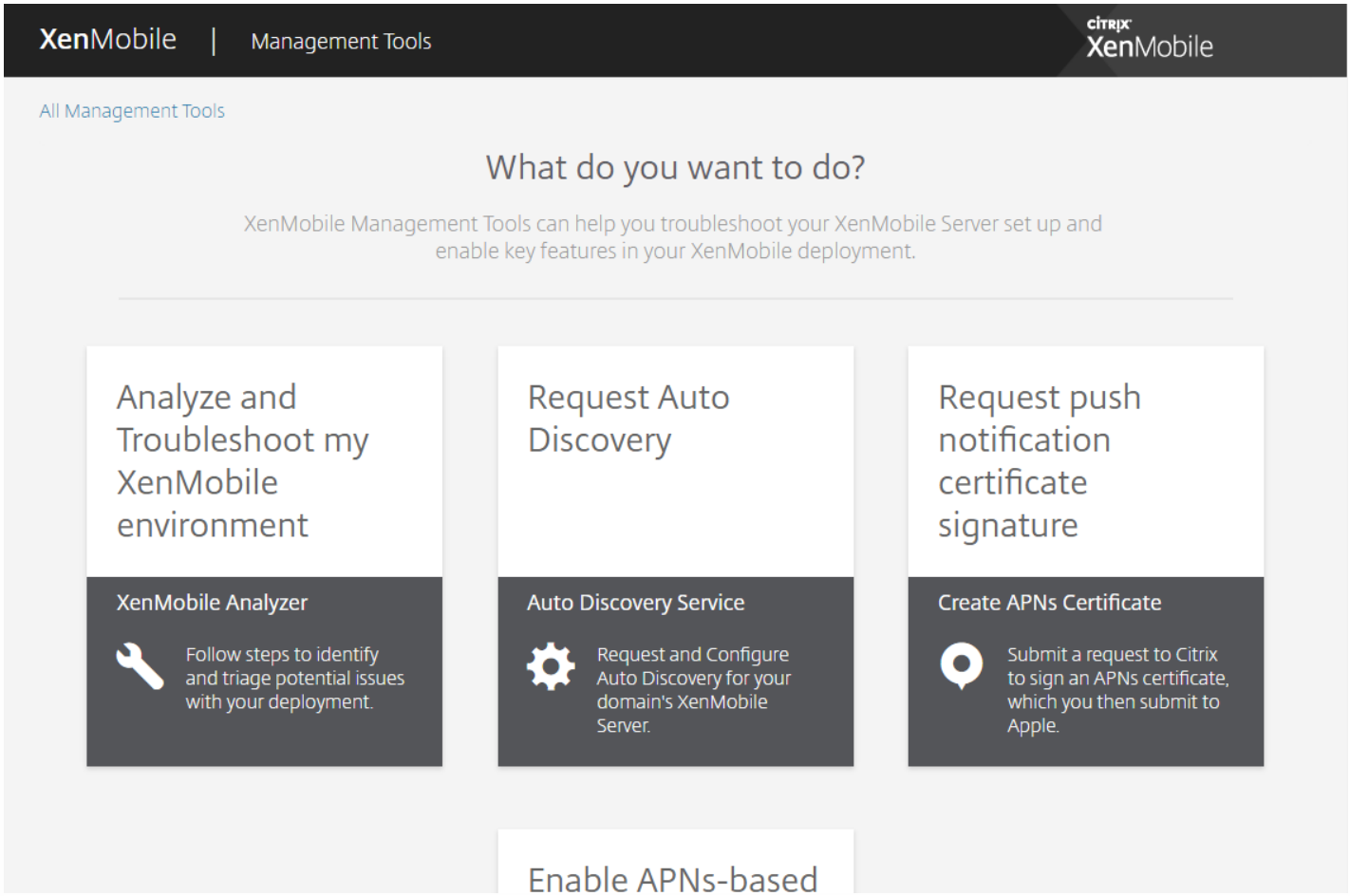
- 提供基于云的安全微服务以解决与 XenMobile 有关的所有问题。
- 存在 XenMobile 配置问题时提供准确的建议。
- 减少支持呼叫数量以及加快 XenMobile 环境的故障排除速度。
- 为 XenMobile 服务器版本提供零天支持。
- 启用 iOS 自定义注册：对 XenMobile 启用自定义端口支持（在除 8443 以外的端口上）。
- 为不受信任或不完整的服务器证书显示证书接受对话框。
- 自动检测双重身份验证场景。
- 对 Intranet 站点的可访问性执行 WorxWeb 测试。
- WorxMail Auto Discovery Service 检查。
- ShareFile 单点登录检查。
- 对 NetScaler 启用自定义端口支持。
- 支持非英语浏览器。

必备条件

产品	支持的版本
XenMobile 服务器	10.3.0 - 10.3.6
NetScaler Gateway	10.5 - 11.1
客户端注册模拟	iOS 和 Android

可以使用 MyCitrix 凭据从 https://xenmobiletools.citrix.com 访问该工具。 在打开的“XenMobile Management Tools”（XenMobile 管理工具）页面上，要启动 XenMobile Analyzer，请单击 **Analyze and Troubleshoot my XenMobile Environment**（分析我的 XenMobile 环境并进行故障排除）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

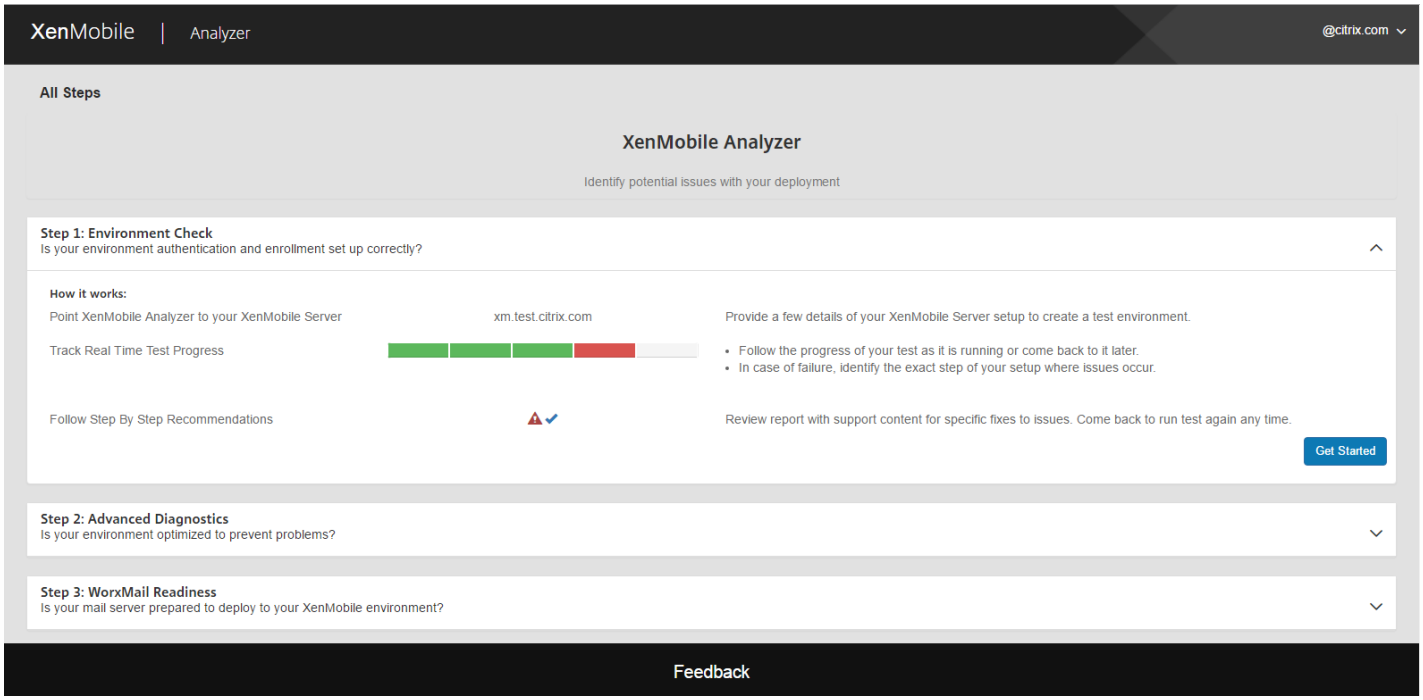


XenMobile Analyzer 包含五个设计用于引导您完成会审过程以及减少支持票据数量的主要步骤，这样可以降低所有人的成本。

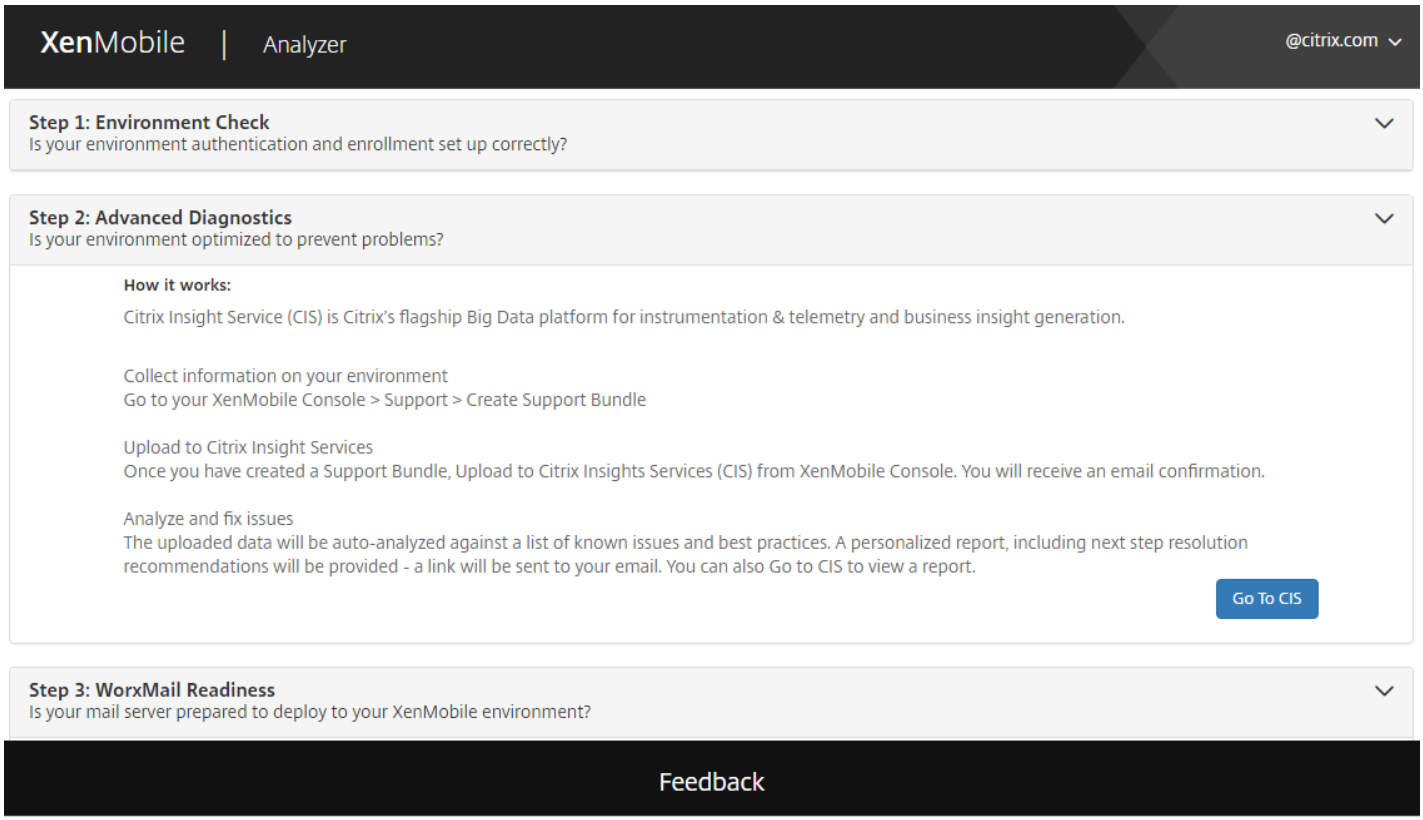
步骤如下：

1. **Environment Check**（环境检查）- 此步骤引导您设置测试以检查您的设置是否存在问题。 此步骤还提供与设备、用户注册和身份验证问题有关的建议和解决方案。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

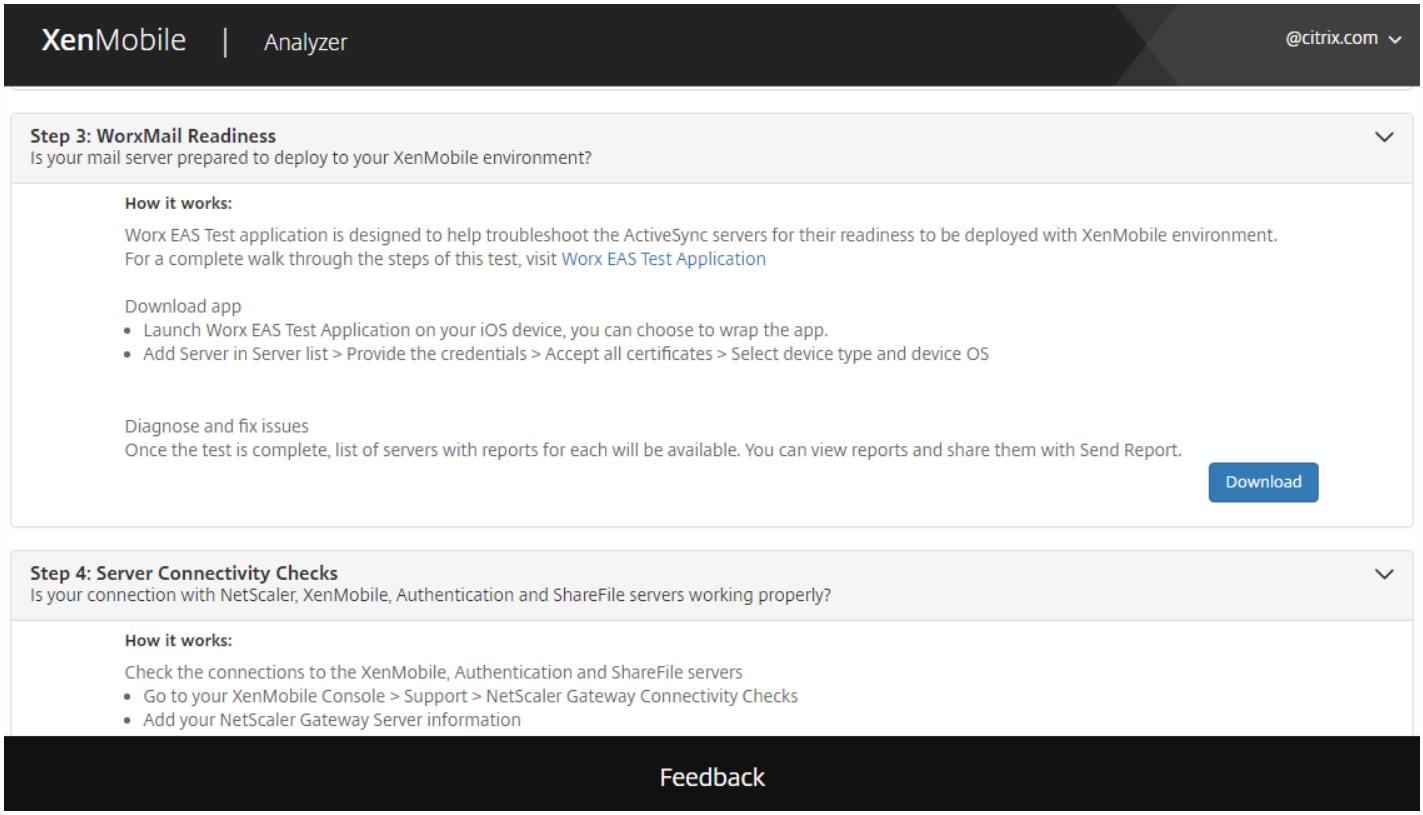


2. **Advanced Diagnostics**（高级诊断）- 此步骤提供与使用 Citrix Insight Services 进一步查找环境检查可能错过的问题有关的信息。



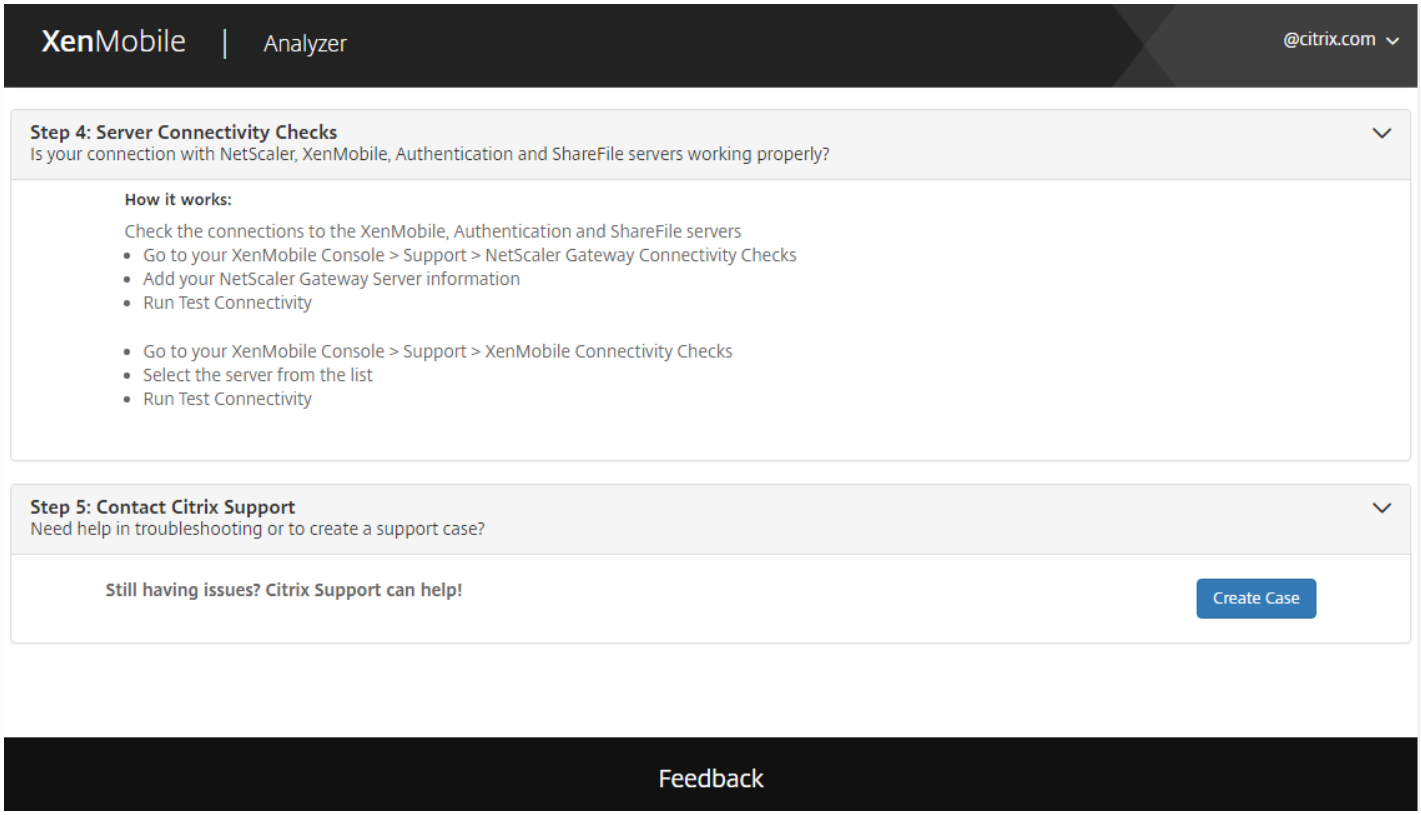
3. **WorxMail Readiness**（WorxMail 准备）- 此步骤引导您下载 Worx Exchange ActiveSync Test 应用程序，该程序可帮助您对 ActiveSync 服务器进行故障排除，以确认其是否已准备好在 XenMobile 环境中部署。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. **Server Connectivity Checks**（服务器连接检查）- 此步骤指导您测试服务器的连接。

5. **Contact Citrix Support**（联系 Citrix 技术支持）- 此步骤将您链接到能够在其中创建 Citrix 支持案例的站点（如果仍遇到问题）。

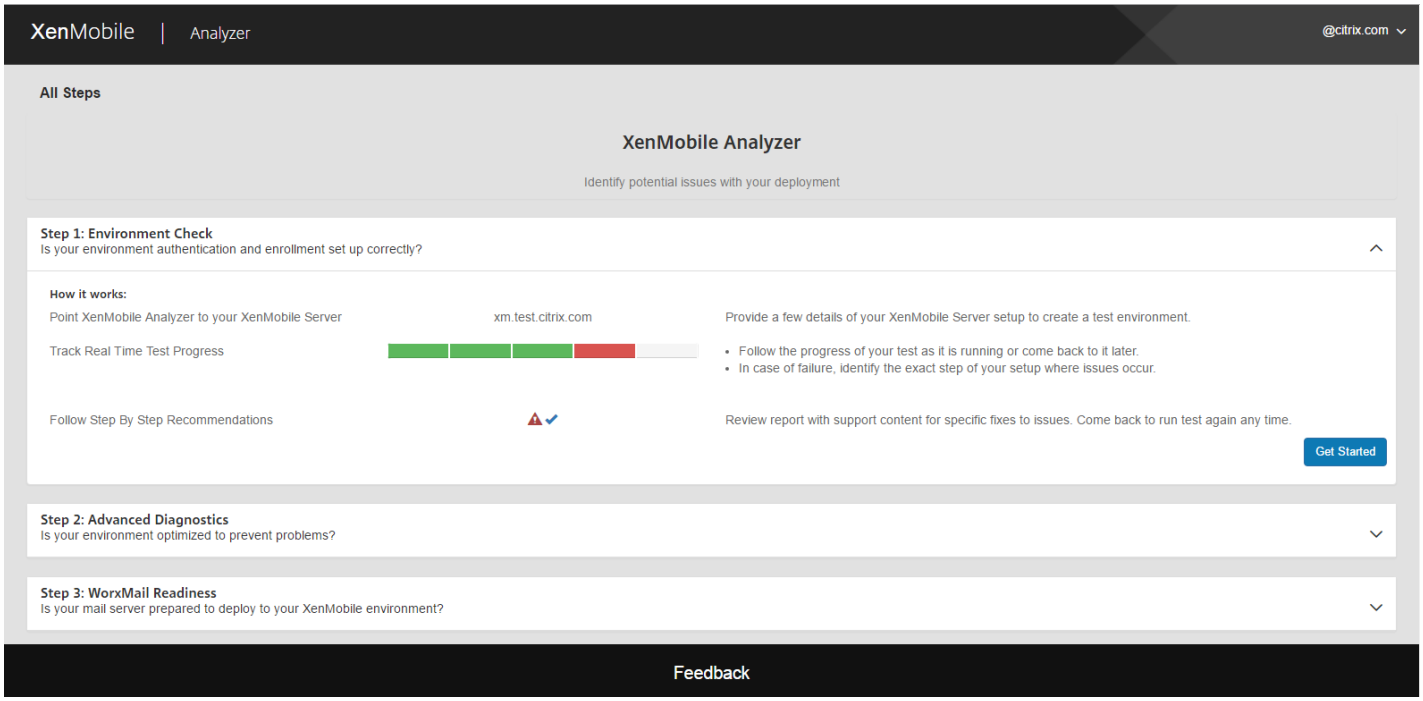


© 1999-2017 Citrix Systems, Inc. All rights reserved.

以下各部分内容更加详细地介绍了每个步骤。

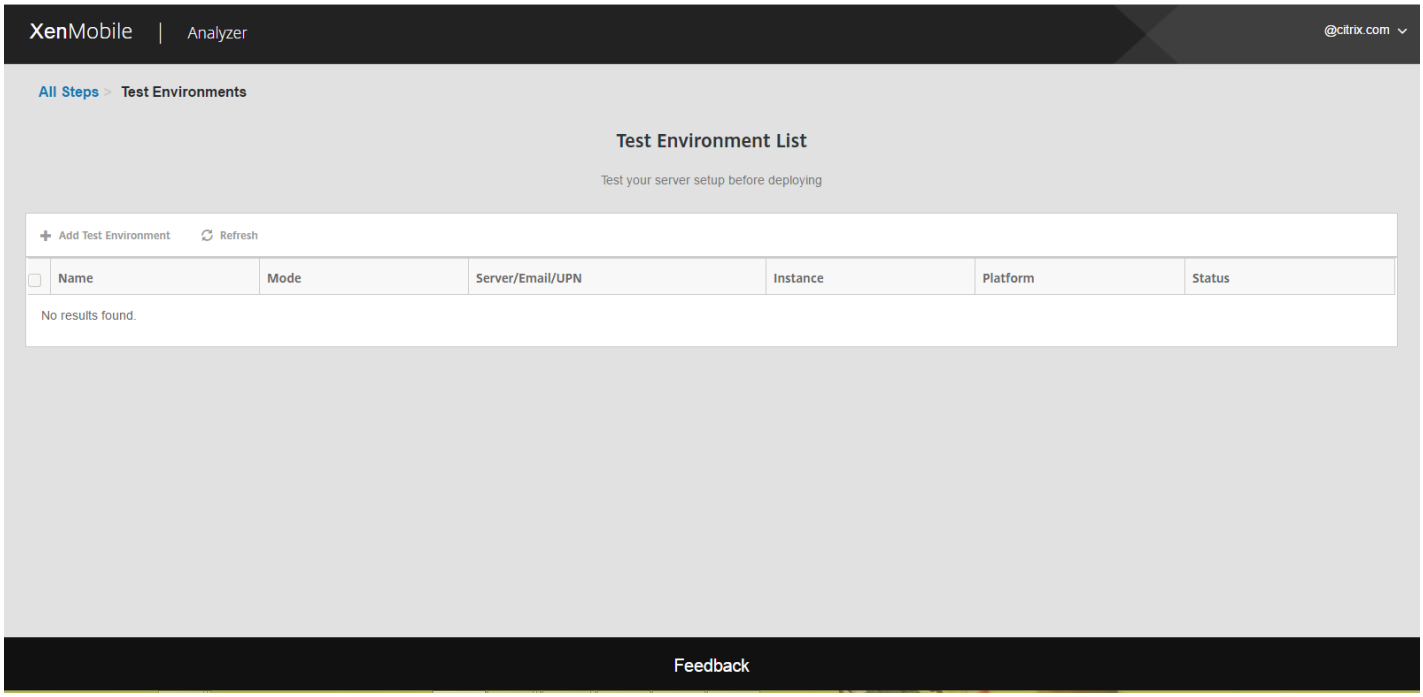
执行环境检查

1. 登录 XenMobile Analyzer，然后单击 **Step 1: Environment Checks**（步骤 1: 环境检查）。
2. 单击 **Get Started**（开始）。

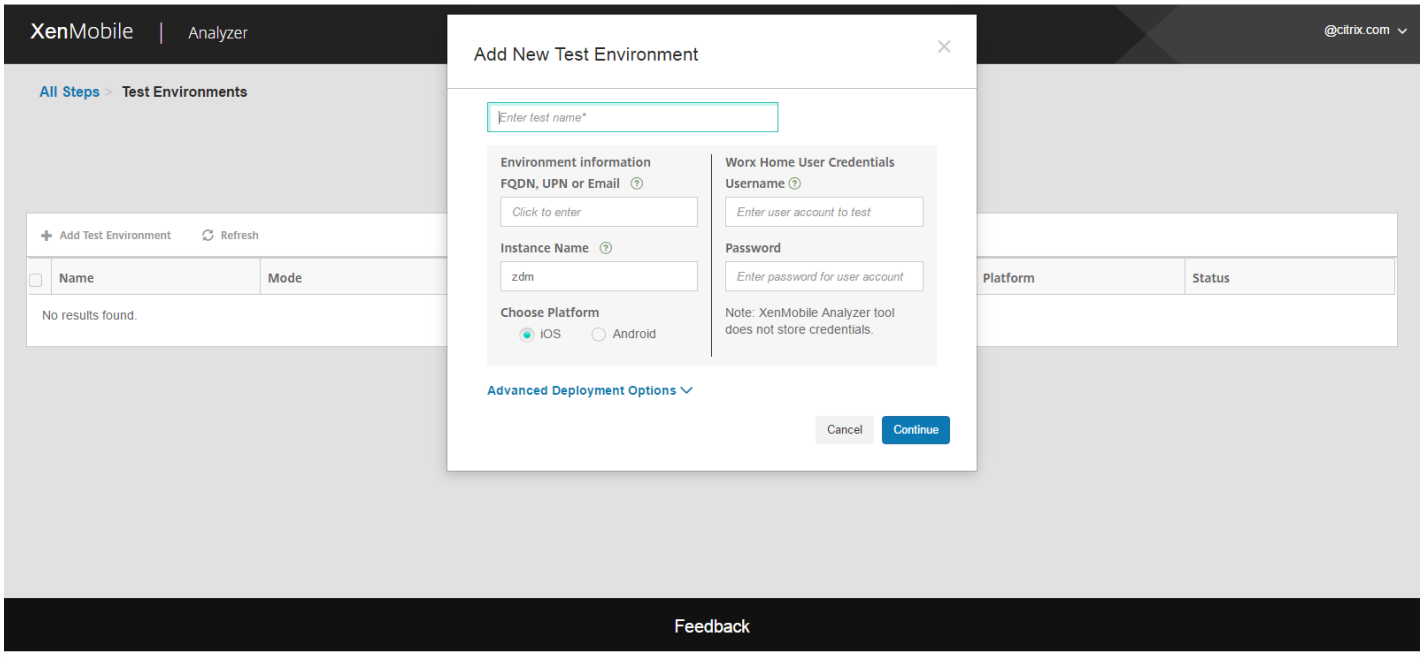


3. 单击 **Add Test Environment**（添加测试环境）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 在新的 **Add Test Environment**（添加测试环境）对话框中，执行以下操作：



a. 为测试提供将来能够帮助您识别测试的唯一名称。

b. 如果您收到用于注册的邀请 URL，请单击 **Advance Deployment Options**（高级部署选项）。 展开后，请选中 **Do you have invitation URL**（您是否有邀请 URL）复选框，然后提供此 URL。 留空该字段会导致该工具自动发现 XenMobile 服务器、用户名和其他详细信息。

c. 如果您没有邀请 URL，可以手动输入服务器信息。

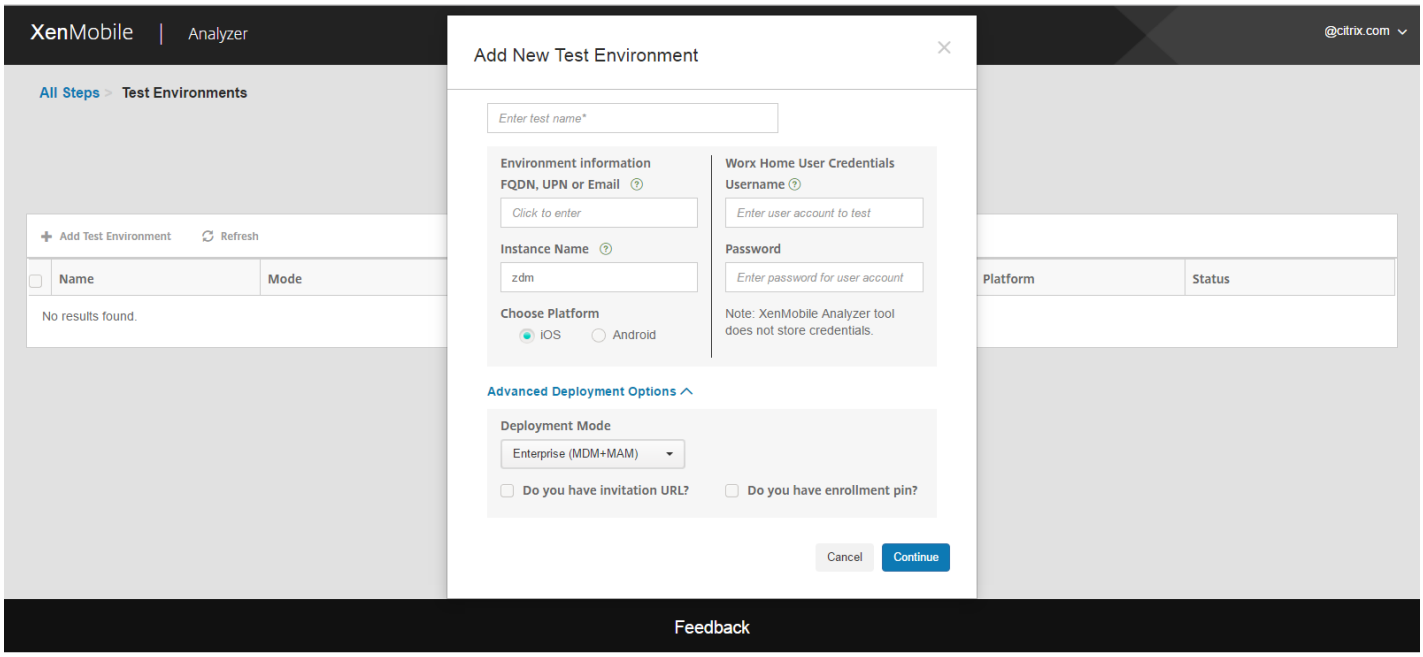
d. 在 **Deployment Mode**（部署模式）列表中，选择 XenMobile 部署模式。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

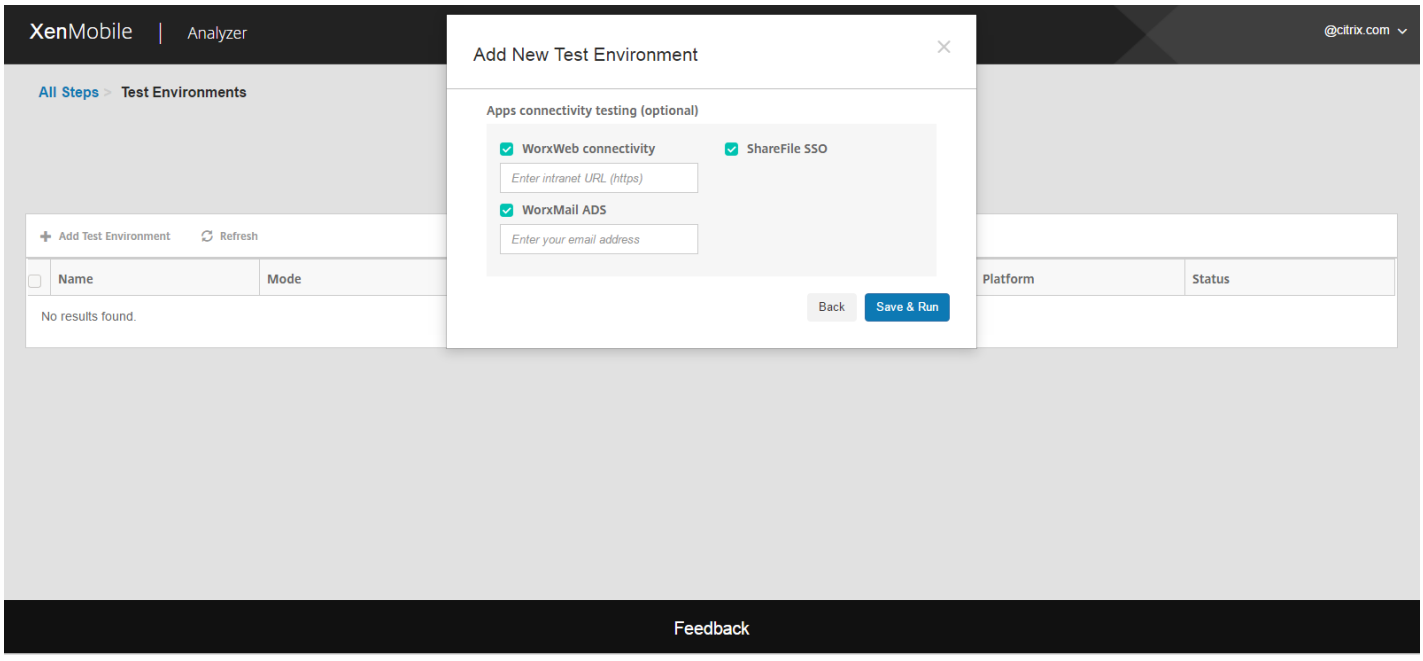
e. 在 **Instance Name**（实例名称）中，如果使用自定义实例，则可以提供该值。

f. 在 **Choose Platform**（选择平台）中，选择 **iOS** 或 **Android** 作为测试平台。

g. 在 **Username**（用户名）和 **Password**（密码）中，输入用于身份验证的用户名和密码。 如果您的环境配置为进行双重身份验证，请选中 **Two Factor Authentication**（双重身份验证）复选框，然后提供第二个密码。



5. 单击 **Continue**（继续）。



6. 您可以选择要运行的应用程序级测试。 您可以选择以下一个或多个测试：

a. WorxWeb 连接。 提供 Intranet URL。 此工具将测试此 URL 的可访问性。 此测试将检测尝试访问此 Intranet

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL 时，WorxWeb 应用程序是否可能发生任何连接问题。

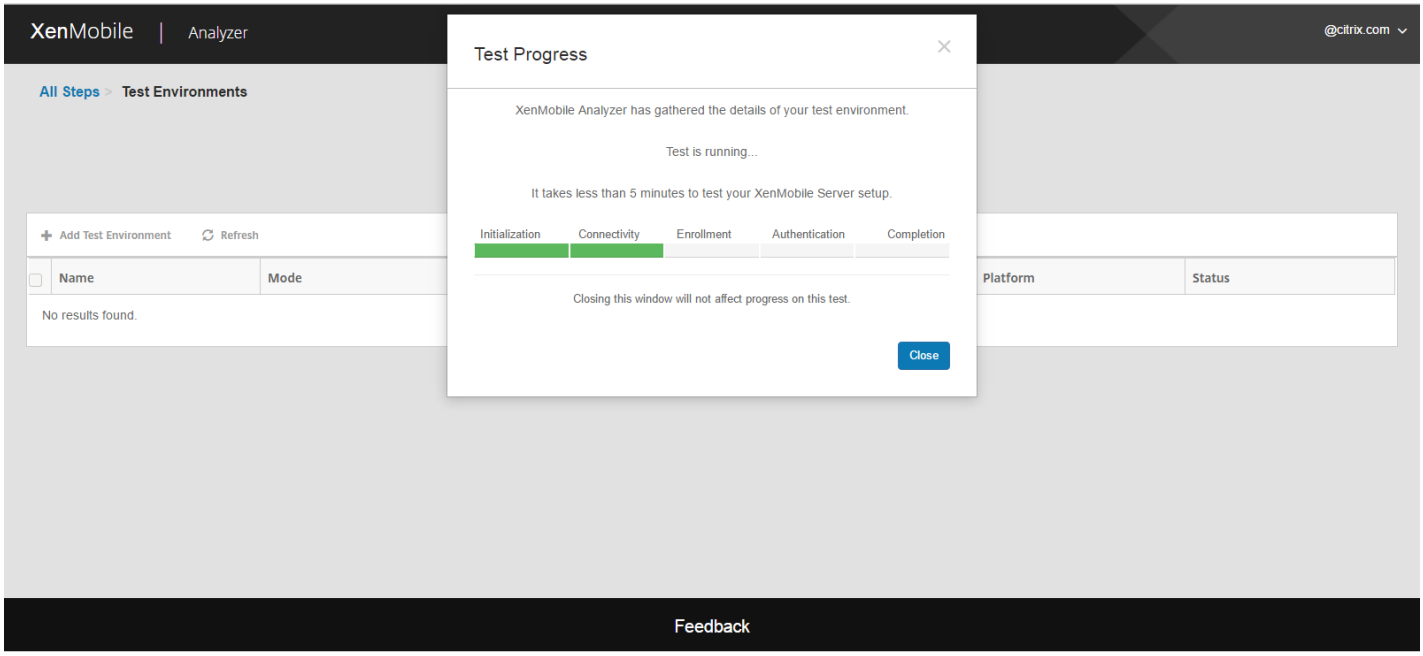
b. WorxMail ADS。 提供用户电子邮件 ID。 此测试用于测试在您的 XenMobile 环境中自动发现 Microsoft Exchange Server 的操作。 它将检测是否存在与 WorxMail Auto Discovery 有关的任何问题。

c. ShareFile SSO。 如果选择该项，XenMobile Analyzer 将测试 ShareFile DNS 解析是否成功，以及使用提供的用户凭据是否可以进行 ShareFile 单点登录 (SSO)。

7. 单击 **Save & Run**（保存并运行）开始测试。

此时将显示进度通知。 可以将进度对话框保留在打开状态，也可以关闭该对话框，测试将继续运行。

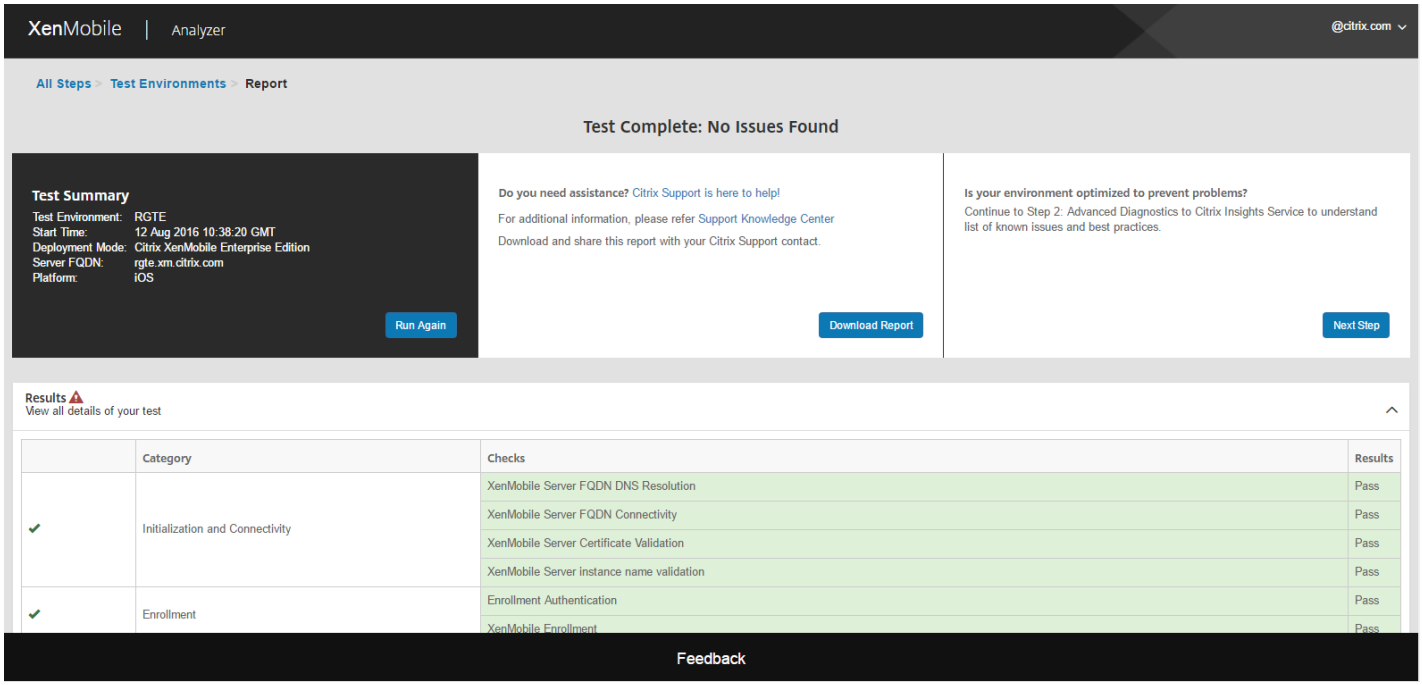
通过的测试将显示为绿色。 失败的测试将显示为红色。

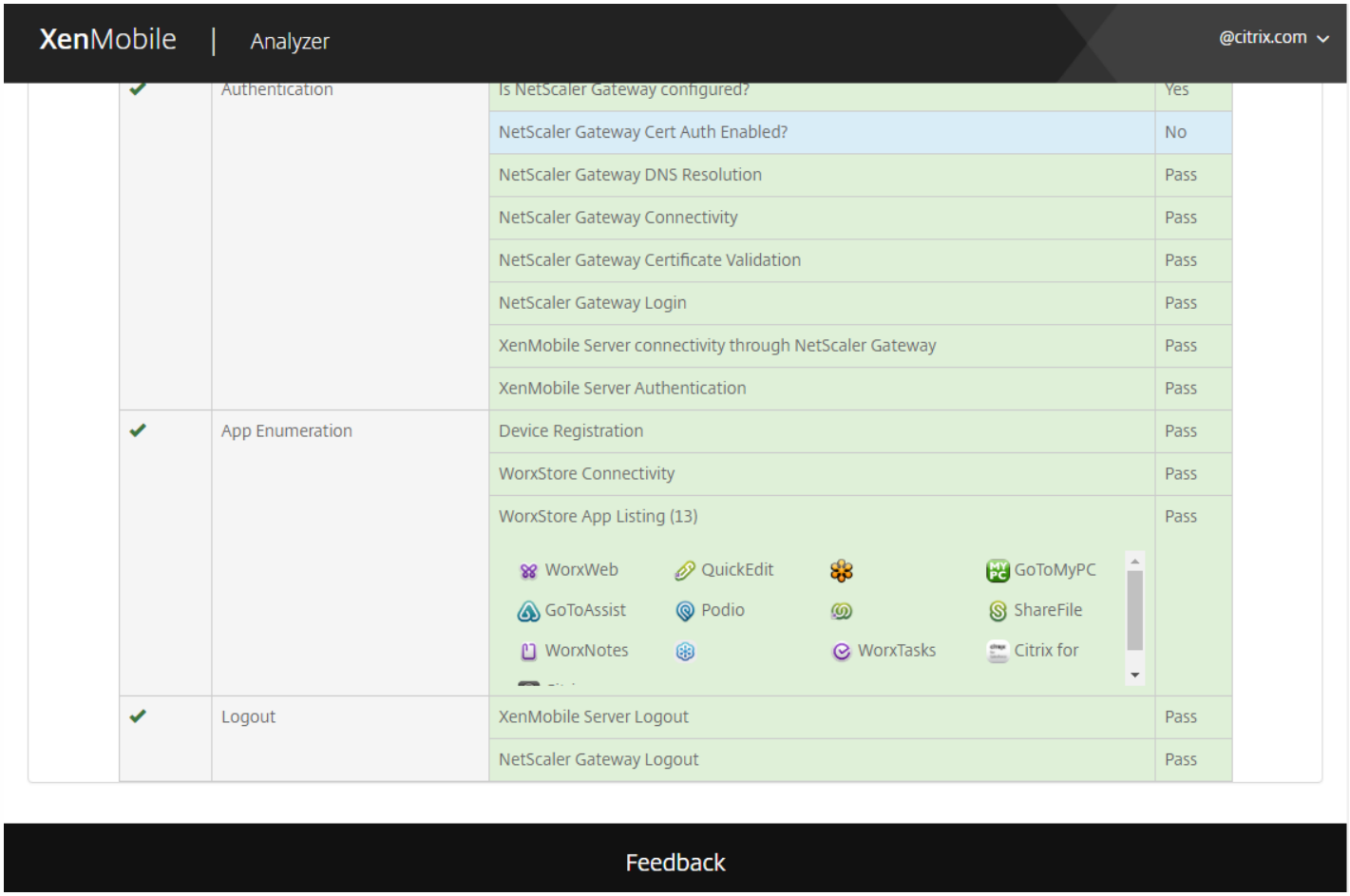


8. 在关闭进度对话框之后的任意点，可以返回到 **Test Environments List**（测试环境列表）页面，然后单击 **View Report**（查看报告）图标查看测试结果。

Results（结果）页面显示“Test Details”（测试详细信息）、“Recommendations”（建议）和“Results”（结果）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.





如果任何建议都有与之关联的 Citrix 知识库文章，相应的文章将在此页面上列出。

9. 单击 **Results**（结果）选项卡显示该工具执行的各个类别和测试及其结果。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

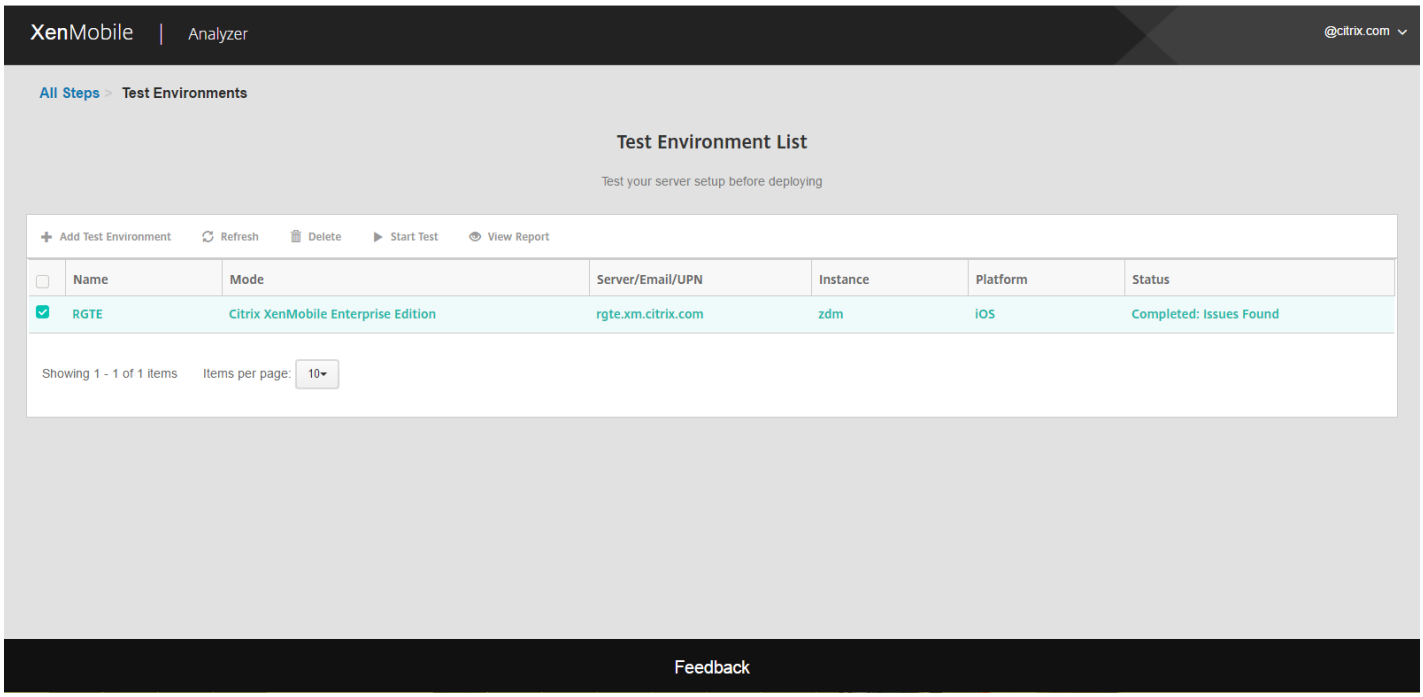
a. 要下载报告，请单击 **Download Report**（下载报告）。

b. 要返回测试环境列表，请单击 **Test Environments**（测试环境）。

c. 要重新运行相同测试，请单击 **Run Again**（重新运行）。

d. 如果您要重新运行其他测试，请返回 **Test Environments**（测试环境），选择测试并单击 **Start Test**（开始测试）。

e. 要转到 XenMobile Analyzer 的下一步，请单击 **Next Step**（下一步）。



执行 XenMobile Analyzer 步骤 2 到 5

您直接与 XenMobile Analyzer 的环境检查步骤交互以执行测试，而步骤 2 到 5 属于信息性步骤。 其中每个步骤都会提供与可用于确保正确设置 XenMobile 环境的其他支持工具有关的信息。

- **Step 2 - Advanced Diagnostics**（步骤 2 - 高级诊断）：此步骤指导您收集与环境有关的信息，然后将该信息上载到 Citrix Insight Services。 该工具分析您的数据并提供包含建议的解决方案在内的个性化报告。
- **Step 3 - WorxMail Readiness**（步骤 3 - WorxMail 准备）此步骤指导您下载并运行 Worx Exchange ActiveSync Test 应用程序。 该应用程序将对 ActiveSync 服务器进行故障排除，以确认其是否已准备好在 XenMobile 环境中部署。 该应用程序运行后，可以查看报告或将报告与其他人共享。
- **Step 4 - Server Connectivity Checks**（步骤 4 - 服务器连接检查）：此步骤向您提供检查与 XenMobile、身份验证和 ShareFile 服务器的连接的说明。
- **Step 5 - Contact Citrix Support**（步骤 5 - 联系 Citrix 技术支持）：如果所有其他步骤都失败，可以通过 Citrix 支持创建一个支持票据。

已知问题

© 1999-2017 Citrix Systems, Inc. All rights reserved.

下面是与 XenMobile Analyzer 有关的已知问题：

- 如果在 XenMobile 服务器上设置了平台限制策略，列出的应用程序数量可能会因客户端而异。
- 执行 WorxWeb Intranet 连接检查时，不支持在文本框中输入多个 URL。
- 不支持 WorxHome 的共享设备身份验证功能。

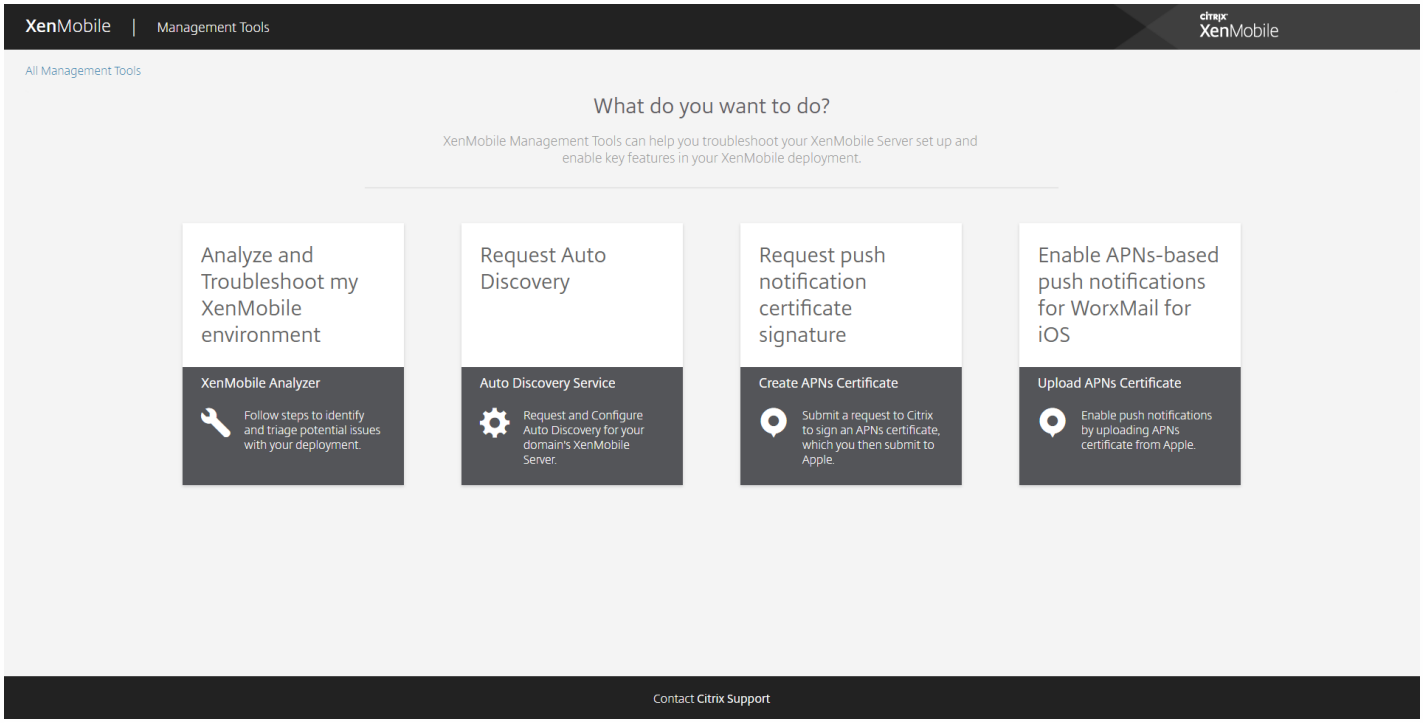
© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 自动发现服务

Aug 11, 2016

自动发现是许多 XenMobile 部署的重要部分。 自动发现可简化用户的注册流程。 用户可以使用他们的网络用户名和 Active Directory 密码注册其设备，无需再输入 XenMobile 服务器的详细信息。 用户以用户主体名称 (UPN) 格式输入其用户名，例如，user@mycompany.com。 通过 XenMobile 自动发现服务，不需要 Citrix 技术支持的帮助即可创建或编辑自动发现记录。

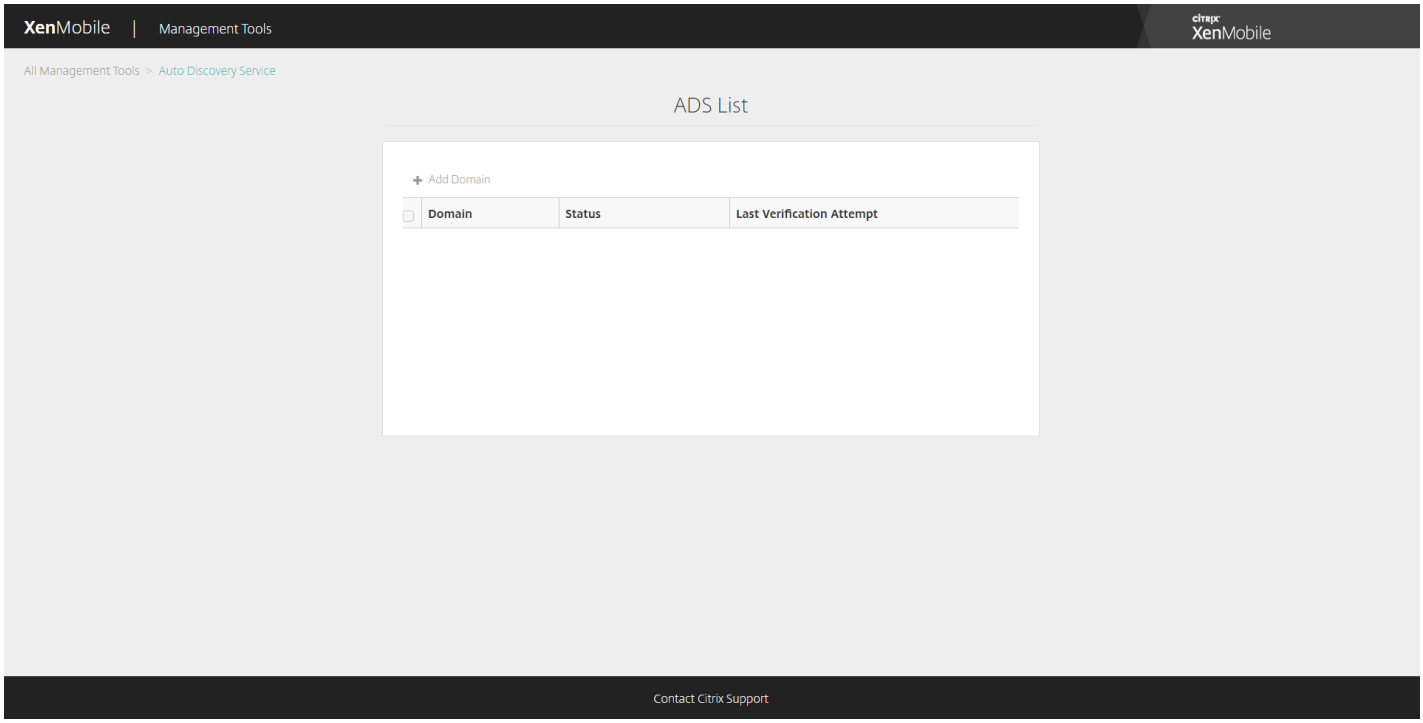
要访问 XenMobile 自动发现服务，请导航到 https://xenmobiletools.citrix.com，然后单击 **Request Auto Discovery**（申请自动发现）。



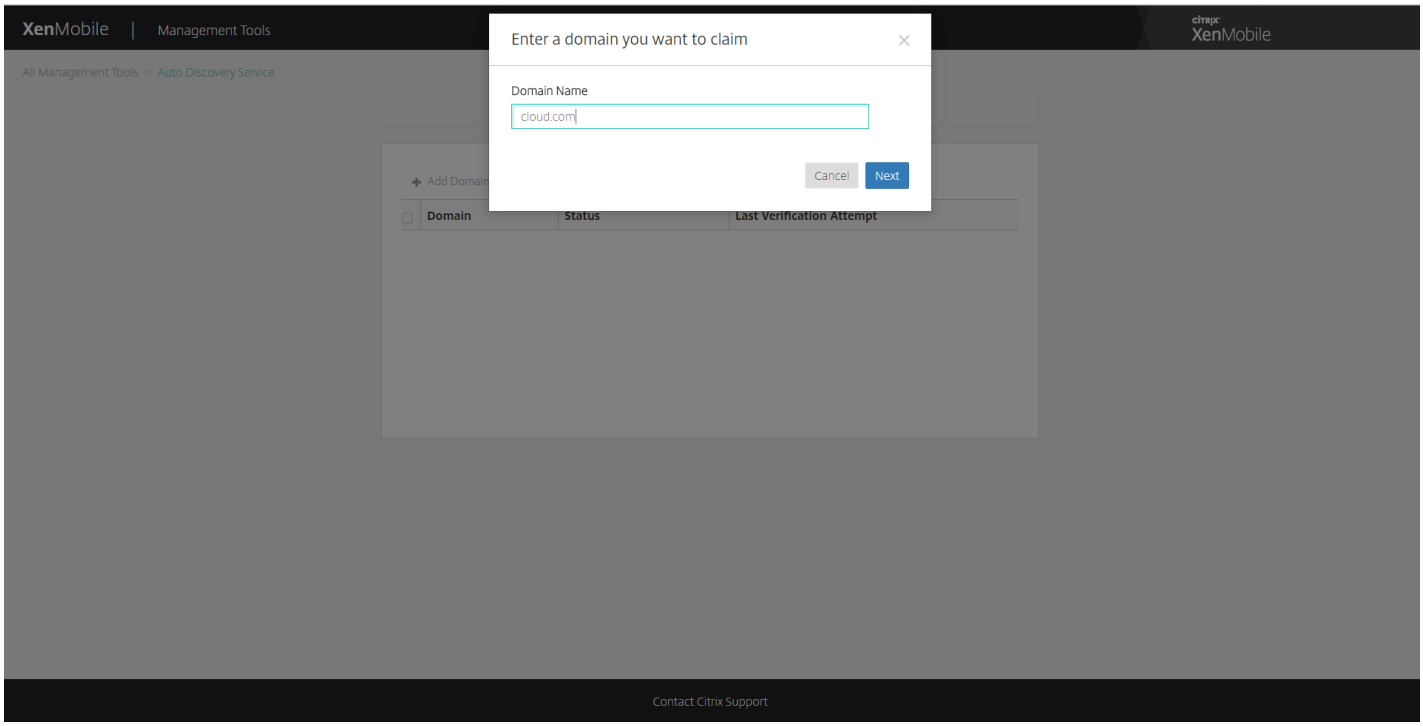
申请自动发现

1. 在“AutoDiscovery Service”（自动发现服务）页面上，需要先声明一个域。 单击 **Add Domain**（添加域）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 在打开的对话框中，输入 XenMobile 环境的域名，然后单击 **Next**（下一步）。



3. 下一步将提供与验证您自己的域有关的说明。

a. 复制在 XenMobile Tools 门户网站中提供的 DNS 令牌。

b. 在托管提供程序门户网站的域中，在您的域对应的区域文件中创建一条 DNS TXT 记录。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

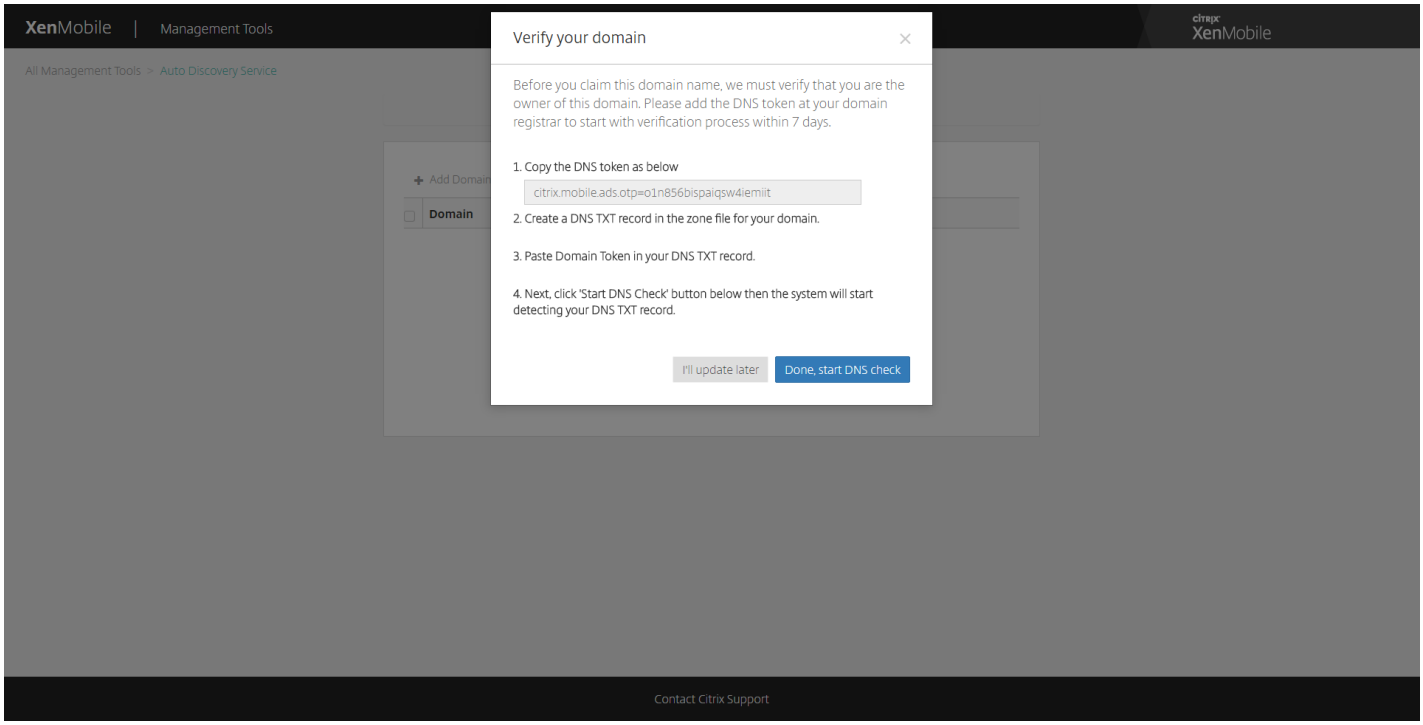
要创建 DNS TXT 记录，需要登录您在上面的步骤 2 中添加的域的域托管提供程序门户网站。 在域托管门户网站中，可以编辑您的域名服务器记录以及添加自定义 TXT 记录。 下例说明了如何在示例域 domain.com 的托管门户中添加 DNS TXT 条目。

c. 粘贴 DNS TXT 记录中的域令牌并保存您的域名服务器记录。

d. 返回 XenMobile Tools 门户，单击“Done”（完成），启动 DNS 检查。

系统将检测您的 DNS TXT 记录。 或者，可以单击“I'll update later”（我将在以后更新），记录将被保存。 DNS 检查在您选择“Waiting”（等待）记录并单击“DNS Check”（DNS 检查）后才启动。

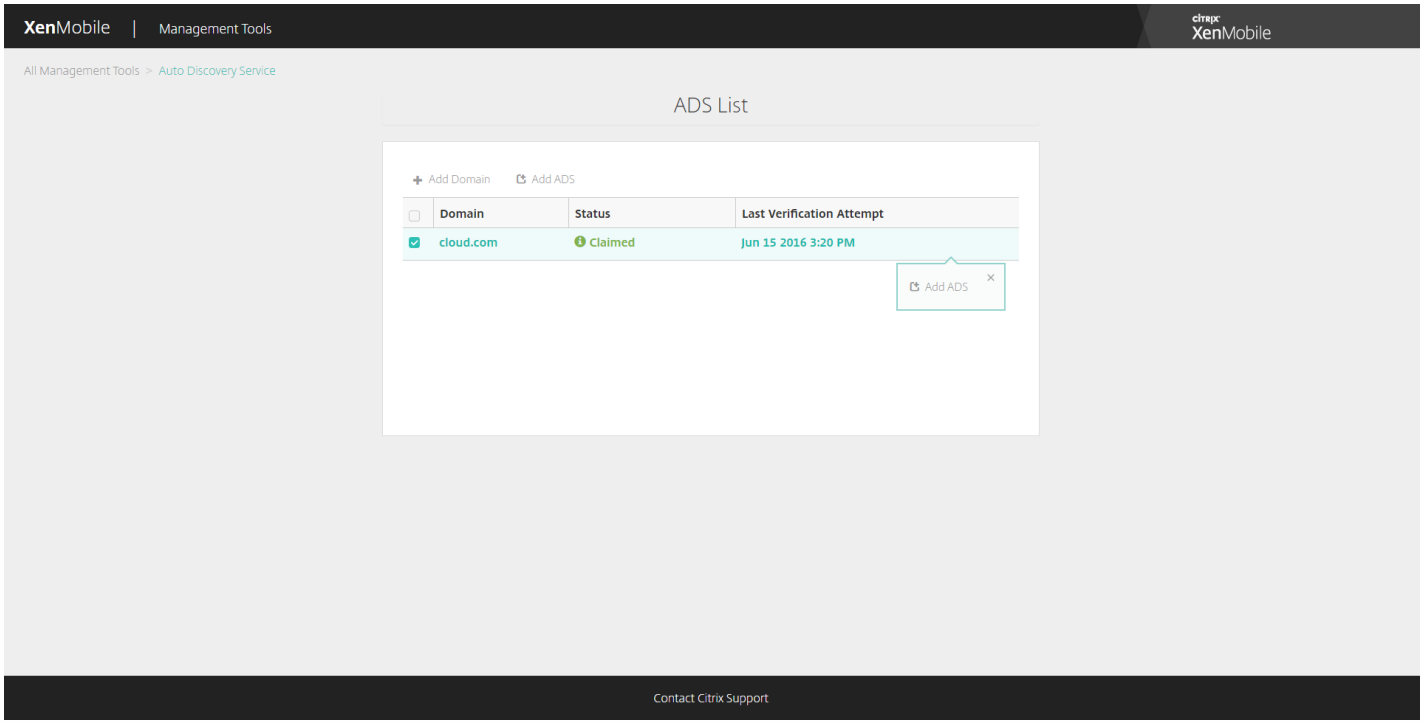
此检查的理想时间大约为一小时，但最长需要两天时间才能返回响应。 此外，您可能需要离开该门户并返回以查看状态变更。



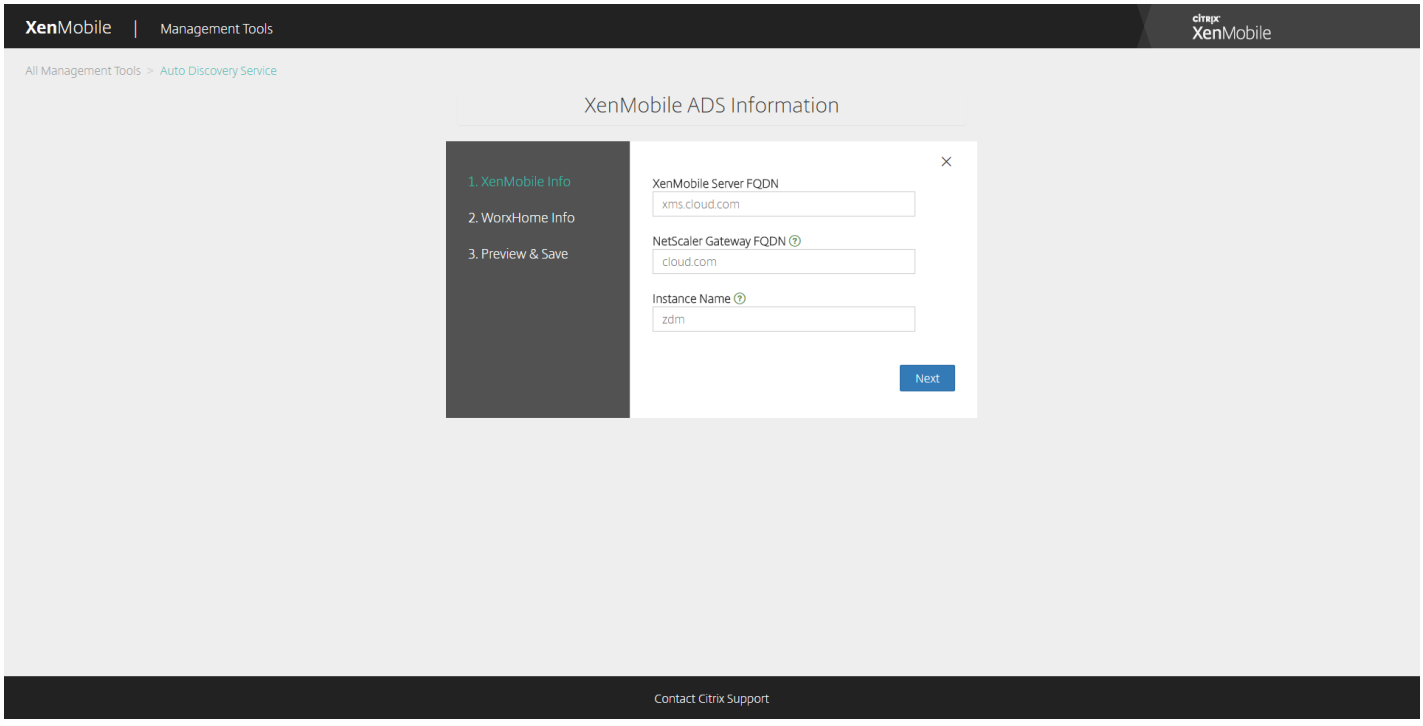
4. 声明您的域后，可以输入自动发现服务信息。 右键单击要为其申请自动发现的域记录，然后单击 **Add ADS**（添加 ADS）。

如果您的域已有自动发现记录，请通过 Citrix 技术支持记录一个案例以根据需要修改详细信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 输入 **XenMobile Server FQDN**（XenMobile 服务器 FQDN）、**NetScaler Gateway FQDN** 和 **Instance Name**（实例名称），然后单击 **Next**（下一步）。 如不确定，请添加默认实例“zdm”。



6. 输入 Worx Home 的以下信息，然后单击 **Next**（下一步）。

a. **User ID Type**（用户 ID 类型）：选择用户登录时使用的 ID 类型，即 **E-mail address**（电子邮件地址）或 **UPN**。用户的 UPN（用户主体名称）与其电子邮件地址相同时将使用 **UPN**。 这两种方法都使用输入的域来查找服务器地

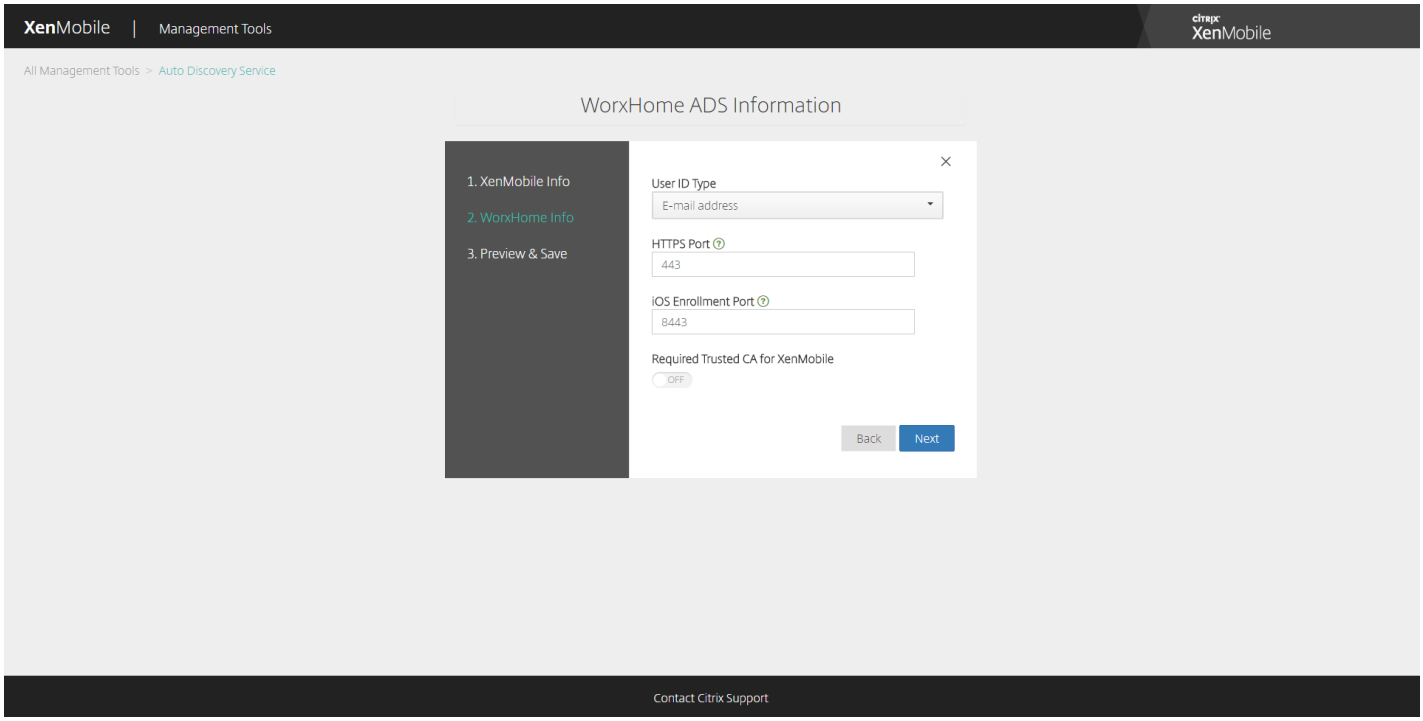
© 1999-2017 Citrix Systems, Inc. All rights reserved.

址。 使用 **E-mail address**（电子邮件地址）时，系统将要求用户输入其用户名和密码，使用 **UPN** 时，系统将要求用户输入其密码。

b. **HTTPS Port**（HTTPS 端口）：输入用于通过 HTTPS 访问 Worx Home 的端口。 通常为端口 443。

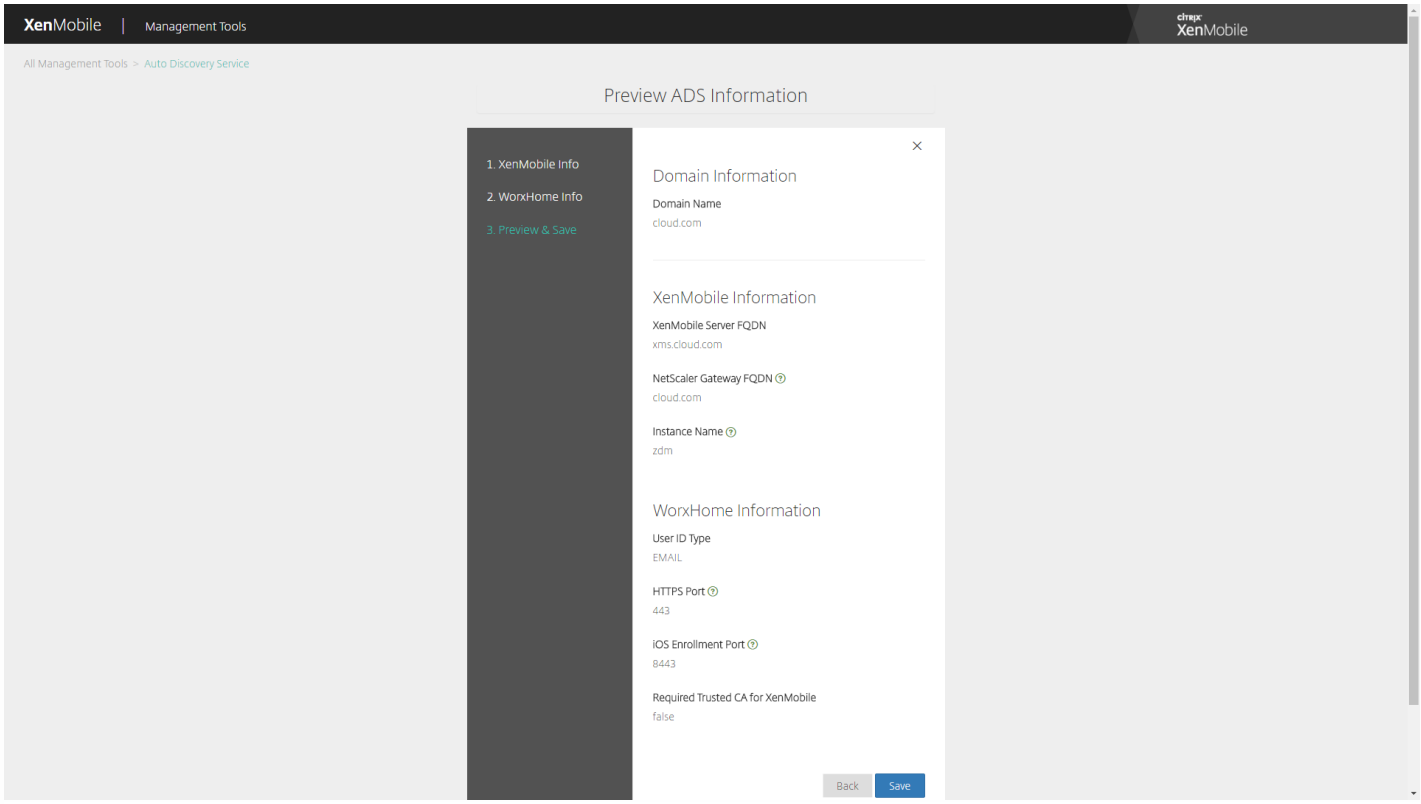
c. **iOS Enrollment Port**（iOS 注册端口）：输入用于访问 Worx Home for iOS 注册的端口。 通常为端口 8443。

d. **Required Trusted CA for XenMobile**（XenMobile 所需的可信 CA）：指示是否需要可信证书才能访问 XenMobile。 此选项可以为 **OFF**（关）或 **ON**（开）。 当前无法上载适用于此功能的证书。 如果要使用此功能，需要呼叫 Citrix 技术支持，请其设置自动发现。 要了解与证书固定有关的详细信息，请参阅 Worx Home 主题中与证书固定有关的部分。 要了解与使证书固定起作用所需的端口有关的信息，请参阅 XenMobile Port Requirements for ADS Connectivity（ADS 连接的 XenMobile 端口要求）上的技术支持文章。



7. 摘要页面将显示您在上述步骤中输入的所有信息。 验证该数据是否正确，然后单击 **Save**（保存）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile REST API 参考

Aug 11, 2016

借助 XenMobile REST API，可以通过 XenMobile 控制台调用显示的服务。 可以使用任意 REST 客户端调用 REST 服务。 API 不要求您登录 XenMobile 控制台即可调用这些服务。

有关可用 API 的最新完整集合，请下载 XenMobile REST API 参考 PDF。 本文不包括完整的 API 集合。

访问 REST API 所需的权限

您需要具有下列权限之一才能访问 REST API：

- 公共 API 访问权限，设置为基于角色的访问配置的一部分（有关设置基于角色的访问权限的详细信息，请参阅使用 RBAC 配置角色）
- 超级用户权限

调用 REST API 服务

可以使用 REST 客户端或 CURL 命令调用 REST API 服务。 以下示例使用适用于 Chrome 的高级 REST 客户端。

> **注意**
>
> 在下面的示例中，请更改主机名和端口号以匹配您的环境。

登录

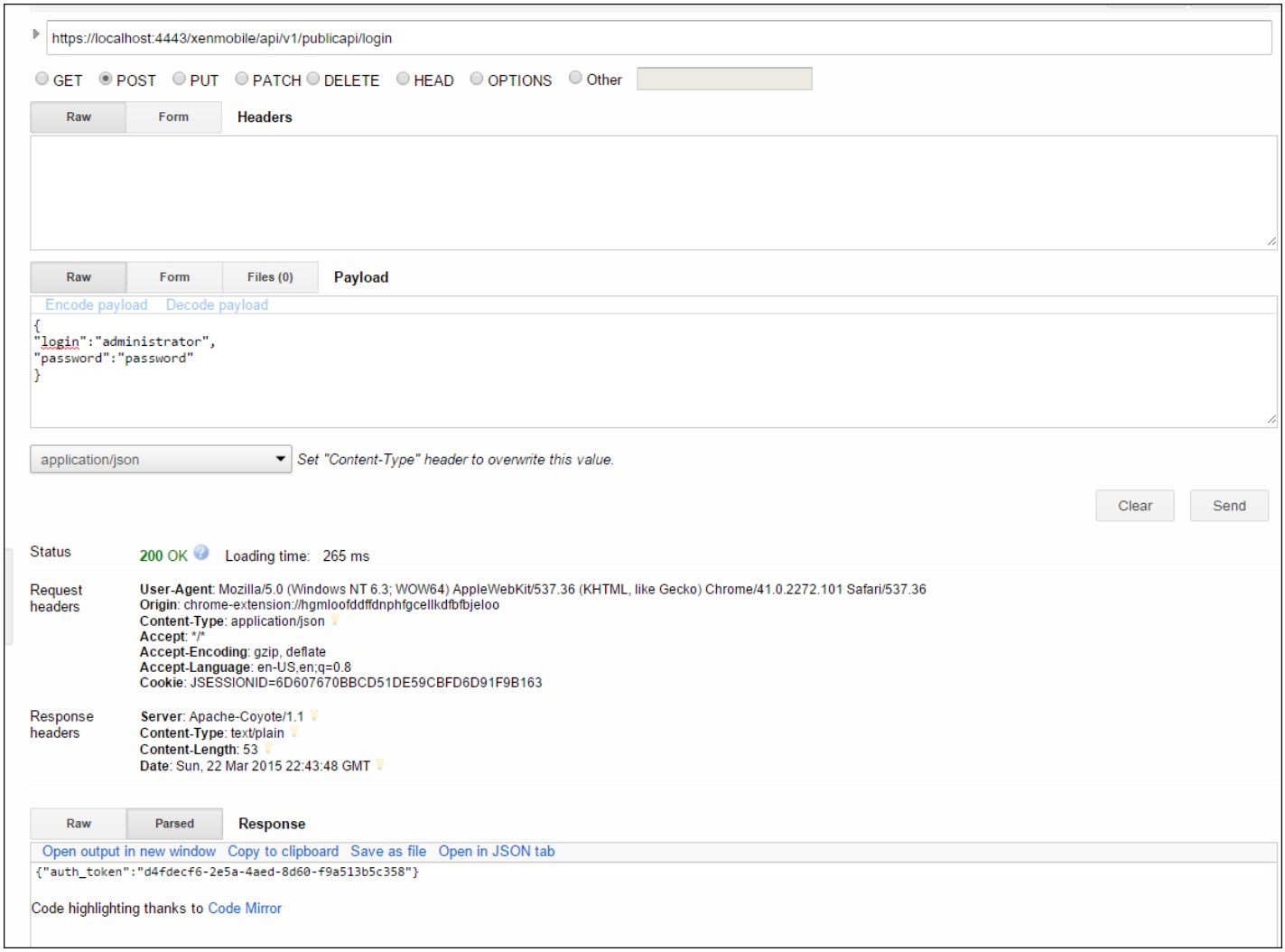
URL：https://:/xenmobile/api/v1/authentication/login

请求：{ "login":"administrator", "password":"password" }

方法类型：POST

内容类型：application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.



通过过滤获取交付组

URL：/xenmobile/api/v1/deliverygroups/filter

请求 复制

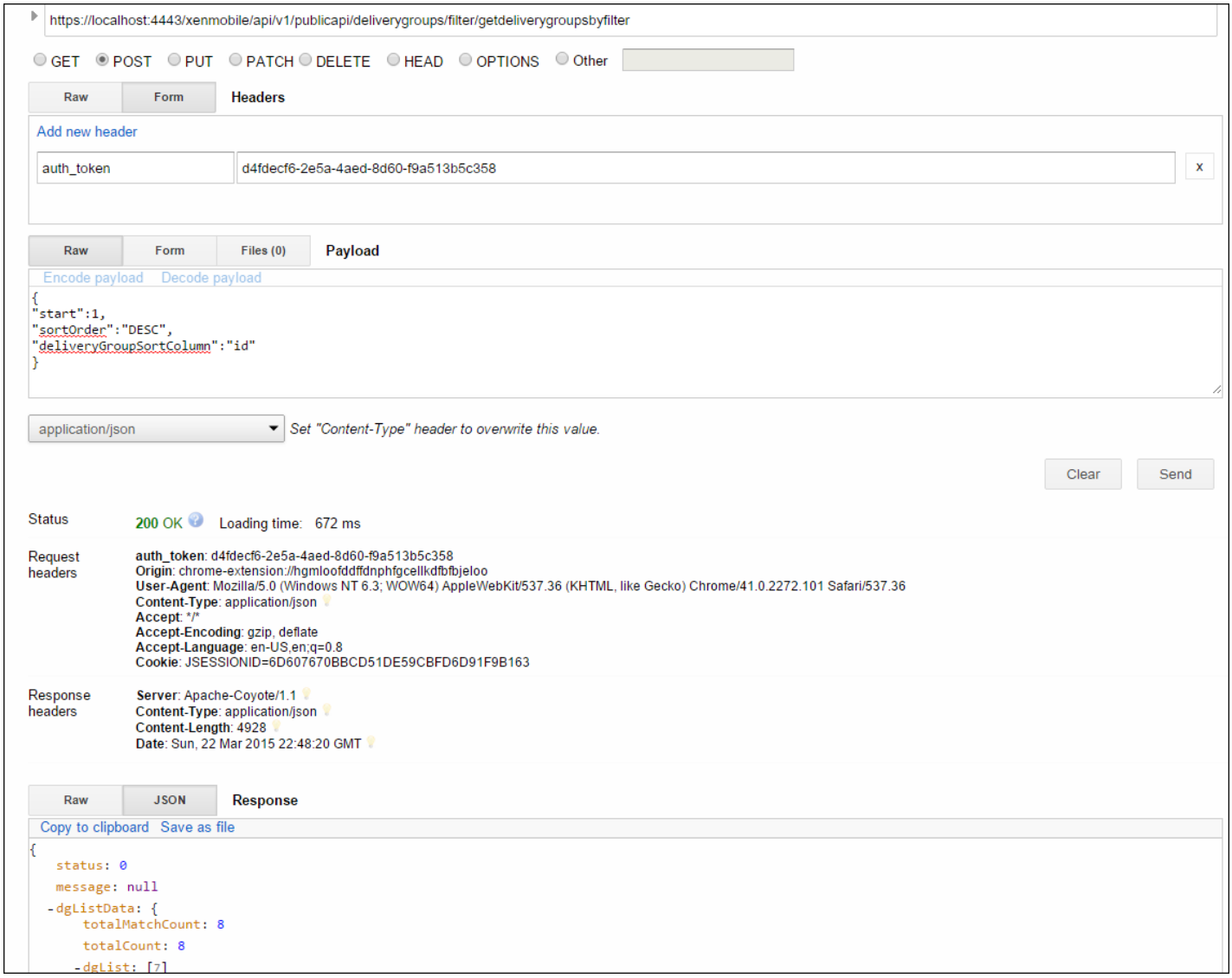
© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

    "search":"add"

}
```

方法类型：POST

内容类型：application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.



REST API 定义

以下各部分内容介绍在该 PDF 中找到的部分 API。 有关完整的 API 文档，请参阅该 PDF。

记住：在下面的示例中，请更改主机名和端口号以匹配您的环境。

登录公共 API

接受用户凭据并使用现有 AuthenticationManager 对用户进行身份验证。 AuthenticationManager 首次验证用户身份时，会生成一个身份验证令牌，放置在请求标头中。

URL：https://:4443/xenmobile/api/v1/authentication/login

请求类型：POST

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{ "login":"administrator", "password":"password" }
```

响应示例 复制

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

通过 CWC 登录公共 API

接受用户凭据并使用现有 AuthenticationManager 对用户进行身份验证。 AuthenticationManager 首次验证用户身份时，会生成一个身份验证令牌，放置在请求标头中。

URL：https://:/xenmobile/api/v1/authentication/cwclogin

请求类型：POST

请求标头：Authorization – CWSAuth service=

请求参数 复制

```
{“context”:”customer or cloud”, “customerId”:”customer ID”}
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "auth-token":"authentication token"

}
```

注销公共 API

删除用户登录时发布的身份验证令牌并注销当前用户。 请求用户名和身份验证令牌。

URL：https://:/xenmobile/api/v1/authentication/logout

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

请求参数 复制

```
{“login”:”administrator”}
```

响应示例 复制

```
{"Status":"user administrator logged out successfully."}
```

管理证书

利用证书管理操作，您可以通过公共 API 查看、删除、导入和添加证书。

获取所有证书

返回数据库中的所有证书。

URL：https://:/xenmobile/api/v1/certificates

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

请求参数：无

© 1999-2017 Citrix Systems, Inc. All rights reserved.

响应示例 复制


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
                "signatureAlgo": "SHA1WithRSAEncryption",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"version": null,

"serialNum": "348237881800118418457268346483687164l3",

"issuerName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,

    "state": null,

    "country": null,

    "description": null

},

"subjectName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                    "state": null,

                    "country": null,

                    "description": null

                }

            }

        }

    ],

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


删除证书

删除指定证书。 请求要删除的各个证书的证书 ID。

URL：https://:/xenmobile/api/v1/publicapi/certificates

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求参数 复制

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

将证书作为 SAML 证书导入

将指定证书作为 SAML 证书导入。

URL：https://:/xenmobile/api/v1/certificates/import/certificate/saml

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Multipart/form-data

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'saml',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```


将证书作为服务器证书导入

将指定证书作为服务器证书导入。

URL：https://:/xenmobile/api/v1/certificates/import/certificate/server

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Multipart/form-data

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```


将证书作为侦听器证书导入

将指定证书作为 SSL 侦听器证书导入

URL：https://:/xenmobile/api/v1/certificates/import/certificate/listener

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Multipart/form-data

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'listener',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

创建证书

创建自签名证书或需要 CA 签名的 CSR 请求。

URL：https://:/xenmobile/api/v1/certificates/csr

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Application/form_url_encoded

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求参数 复制

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```


导出证书

下载指定证书。 下表列出了此操作的参数。

参数	必选	说明
id	是	数字证书 ID

© 1999-2017 Citrix Systems, Inc. All rights reserved.

password	与要导出的证书关联的密码。
exportPrivateKey	指出是否导出私钥的标记。

URL：https://:/xenmobile/api/v1/certificates/export

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

示例响应：请求成功时显示证书字符串。

管理密钥库

您可以通过公共 API 导入密钥库。

导入服务器密钥库

导入服务器密钥库。

URL：https://:/xenmobile/api/v1/certificates/import/keystore/server

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Multipart/form-data

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```

导入 SAML 密钥库

导入 SAML 密钥库。

URL：https://:/xenmobile/api/v1/certificates/import/keystore/saml

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

© 1999-2017 Citrix Systems, Inc. All rights reserved.

内容类型 – Multipart/form-data

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
 }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```

导入 APNs 密钥库

导入 APNS 密钥库。

URL：https://:/xenmobile/api/v1/certificates/import/keystore/apns

请求类型：POST

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Multipart/form-data

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


导入 SSL 侦听器密钥库

导入 SSL 侦听器密钥库。

URL：https://:/xenmobile/api/v1/certificates/import/keystore/listener

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Multipart/form-data

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
 uploadFile = <certificate file>
 uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
"certificate": null,
"apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


管理许可证

您可以通过公共 API 管理许可证。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

获取许可证信息

列出关于所有许可证的信息。

URL：https://:/xenmobile/api/v1/licenses

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        {
            sadate: "2015.1210"
            notice: "Example Systems Inc."
            vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
            licensesInUse: 0
            licensesAvailable: 102
            overdraftLicenseCount: 2
            p_E_M: "CXM_ENTU_UD"
            serialNumber: "cxmretailent1000user"
            licenseType: "Retail"
            expirationDate: "01-DEC-2015"
        }
        licenseNotification:
        {
            id: 1
            notificationEnabled: false
            notifyFrequency: 7
            notifyNumberDaysBeforeExpire: 60
            recepientList: ""
            emailContent: "License expiry notice"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        }

    }

}
```

保存许可证信息

保存所有许可证信息。

URL：https://:/xenmobile/api/v1/licenses

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,

    "isScheduleNotificationNeeded": true,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success"
}
```

上载许可证文件

© 1999-2017 Citrix Systems, Inc. All rights reserved.

上载指定许可证文件。

URL：https://:/xenmobile/api/v1/licenses/upload

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – Multipart/form-data

请求参数：uploadFile = <要上载的许可证文件>

响应示例 复制

```
{
   "status": 0,
   "message": "Success"
}
```

激活许可证

激活指定许可证。

URL：https://:/xenmobile/api/v1/licenses/activate/{license type}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数：在激活许可证 URL 后附加许可证类型。

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "status": 0,
    "message": "Success"
    "cpLicenseServer": null
}
```

删除所有许可证

删除所有许可证。

URL：https://:/xenmobile/api/v1/licenses/remove

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "isConnected": null
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

测试许可证服务器

对许可证服务器执行连接检查。

URL：https://:/xenmobile/api/v1/licenses/testserver/

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "status": 0,

    "message": "Success",

    "isConnected": true

}
```

获取最早的过期日期

查找具有最早过期日期的许可证。

URL：https://:/xenmobile/api/v1/licenses/getexpirationdate

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "status": 0,
    "message": "Success",
    "expiredDate": 1448956800000,
    "daysBeforeExpire": 229,
    "daysInPOC": 0
}
```

管理 LDAP 配置

下表列出了 LDAP 配置操作使用的参数。

参数	必选	说明
primaryHost	是	主 LDAP 服务器 IP 地址或主机名。 采用 IP 地址或 FQDN 输入。
secondaryHost	否	辅助 LDAP 服务器 IP 地址或主机名。 采用 IP 地址或 FQDN 输入。
port	是	LDAP 服务器端口号
username	是	有效 LDAP 服务器用户名
password	是	用户名的密码
userBaseDN	是	
lockoutLimit	否	
lockoutTime	否	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

useSecure	否	
userSearchBy	是	根据 upn 或 samaccount 搜索用户
domain	是	唯一 LDAP 服务器域名
domainAlias	是	LDAP 域的别名
globalCatalogPort	否	
gcRootContext	否	
groupBaseDN	是	
isDefault	否	GET 响应的一部分，指示 LDAP 配置是否唯一。
name	否	GET 响应的一部分，是用于更新或删除 LDAP 配置的唯一标识符。

列出 LDAP 配置

列出 XenMobile 中的整个 LDAP 配置。

URL：https://:/xenmobile/api/v1/ldap

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userB

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","us

    ]

}
```

添加新的 LDAP 配置

添加新的 LDAP 配置。 域名必须唯一，并且不能与其他任何 LDAP 配置相同。

URL：https://:/xenmobile/api/v1/ldap/msactivedirectory

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "primaryHost":"192.0.2.7",
    "secondaryHost":"",
    "port":"389",
    "username":"aaa@example.com",
    "password":"1.pwd",
    "userBaseDN":"dc=example,dc=com",
    "groupBaseDN":"dc=example,dc=com",
    "lockoutLimit":"0",
    "lockoutTime":"1",
    "useSecure":"false",
    "userSearchBy":"upn",
    "domain":"example.com",
    "domainAlias":"exampleAlias",
    "globalCatalogPort":"0",
    "gcRootContext":""
}
```


响应示例 复制

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

   “status”: 0,

   “message”: “LDAP configuration created”

}
```

编辑 LDAP 配置

编辑现有 LDAP 配置，但是不能通过编辑操作更改域。

URL：https://:/xenmobile/api/v1/ldap/msactivedirectory/{name}

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

设置默认 LDAP 配置

将指定 LDAP 配置设为默认配置。

URL：https://:/xenmobile/api/v1/ldap/default/{name}

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

删除 LDAP 配置

删除指定 LDAP 配置。

URL：https://:/xenmobile/api/v1/ldap/{name}

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

管理 NetScaler Gateway 配置

管理 NetScaler Gateway 配置。 下表列出了 NetScaler Gateway 操作使用的参数。

参数	必选	说明
name	是	唯一 NetScaler Gateway 名称
alias	否	
url	是	NetScaler Gateway 的可公开访问 URL
passwordRequired	是	
logonType	是	有效值：domain-only、domain-token、domain-certificate、certificate-only、certificate-token 和 token-only
callback	否	
认情况	是	添加或编辑 NetScaler Gateway 配置时设为 True 或 False。 如果此参数未通过，默认设置为 False。
id	否	GET 响应的一部分，是用于更新或删除 NetScaler Gateway 配置的唯一标识符。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

列出所有 NetScaler Gateway 配置

列出 XenMobile 中的整个 NetScaler Gateway 配置。

URL：https://:/xenmobile/api/v1/netscaler

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false",

        "id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        }

    ]

}
```

添加新的 NetScaler Gateway 配置

添加新的 NetScaler Gateway 配置。

URL：https://:/xenmobile/api/v1/netscaler

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

编辑 NetScaler Gateway 配置

编辑指定 NetScaler Gateway 配置。

URL：https://:/xenmobile/api/v1/netscaler/{id}

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

删除 NetScaler Gateway 配置

删除指定 NetScaler Gateway 配置。

URL：https://:/xenmobile/api/v1/netscaler/{id}

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

设置默认 NetScaler Gateway 配置

将指定 NetScaler Gateway 配置设为默认配置。

URL：https://:/xenmobile/api/v1/netscaler/default/{id}

请求类型：PUT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

管理 SMS 和 SMTP 通知服务器配置

可以添加、编辑、激活（设为默认）和删除 SMS 服务器和 SMTP 服务器配置。 下表列出了 SMS 服务器和 SMTP 服务器配置操作使用的参数。

参数	必选	说明
name	是	唯一 SMS/SMTP 配置名称。
serverType	否	GET 请求中服务器发送的通知服务器类型（SMS 或 SMTP）。
active	否	指示是否将服务器用于通知。 每种类型仅可以激活一个服务器。
id	否	用于更新、删除或激活服务器的唯一标识符。
description	否	服务器的说明。
SMS 参数		
key	是	
secret	是	
virtualPhoneNumber	是	必须采用电话号码格式。
https	是	默认为 false。
country	是	
carrierGateway	是	默认为 false。
SMTP 参数		
secureChannelProtocol	是	所使用的安全协议的类型。 有效值为：None、SSL 和 TLS。 默认值为“无”。
port	是	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

authentication	是	是否使用身份验证。 有效值为 True 和 False。
username	是（当 authentication 为 True 时）	
password	是（当 authentication 为 True 时）	
msSecurePasswordAuth	是	默认为 false。
fromName	是	
fromEmail	是	
numOfRetries	否	整数。 默认值为 5。
timeout	否	整数。 默认值为 30。
maxRecipients	否	整数。 默认值为 100。

列出所有 SMS 和 SMTP 服务器

列出 XenMobile 中的所有 SMS 和 SMTP 服务器。

URL：https://:/xenmobile/api/v1/notificationserver

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

接受 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

获取服务器详细信息

根据服务器 ID 获取服务器的详细信息。

URL：https://:/xenmobile/api/v1/notificationserver/{id}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

接受 – application/json

SMS 响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

SMTP 响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

添加 SMS 服务器配置

添加 SMS 服务器配置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL：https://:/xenmobile/api/v1/notificationserver/sms

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false”,
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

编辑 SMS 服务器配置

编辑指定的 SMS 服务器配置。

URL：https://:/xenmobile/api/v1/notificationserver/sms/{id}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false",
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

添加 SMTP 服务器配置

添加 SMTP 服务器配置。

URL：https://:/xenmobile/api/v1/notificationserver/smtp

请求类型：POST

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

编辑 SMTP 配置

编辑指定的 SMTP 配置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL：https://:/xenmobile/api/v1/notificationserver/smtp/{id}

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

删除服务器配置

删除指定的 SMS 或 SMTP 服务器配置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL：https://:/xenmobile/api/v1/notificationserver/{id}

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

设置默认 SMS 配置

将指定的 SMS 服务器 配置设为默认配置。

URL：https://:/xenmobile/api/v1/notificationserver/activate/sms/{id}

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

设置默认 SMTP 配置

将指定的 SMTP 服务器 配置设为默认配置。

URL：https://:/xenmobile/api/v1/notificationserver/activate/smtp/{id}

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

管理本地用户和组

可以通过使用以下服务管理本地用户和组。

获取所有用户

获取所有本地用户。

URL：https://:/xenmobile/api/v1/localusersgroups

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    ]

}
```

获取一个用户

获取指定本地用户。

URL：https://:/xenmobile/api/v1/localusersgroups/{name}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{

    "status": 0,

    "message": "Success",

    "result": {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            company : example
        },
        "role": "ADMIN",
        "roles": null,
        "createdOn": "1/10/15 11:42 AM",
        "lastAuthenticated": "1/10/15 11:42 AM",
        "domainName": null,
        "adUser": false,
        "vppUser": false
    }
}
```

添加用户

使用指定属性添加用户。

URL：https://:/xenmobile/api/v1/localusersgroups

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

响应示例 复制

```
{
    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"message": "Success",

"user": {

    "userid": 0,

    "username": "justaname_XX",

    "password": "password",

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": null,

    "lastAuthenticated": null,

    "domainName": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "adUser": false,

        "vppUser": false

    }

}
```

更新用户

更新用户属性。

URL：https://:/xenmobile/api/v1/localusersgroups

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

响应示例 复制

```
{
    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"message": "Success",

"user": {

    "userid": 108,

    "username": "justaname_XX",

    "password": null,

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": "3/27/15 1:10 PM",

    "lastAuthenticated": "3/27/15 1:10 PM",

    "domainName": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "adUser": false,

        "vppUser": false

    }

}
```

更改用户密码

重置用户的密码；您也可以在更新本地用户调用中更改用户的密码。

URL：https://:/xenmobile/api/v1/localusersgroups/resetpassword

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

删除多个用户

删除指定用户。

URL：https://:/xenmobile/api/v1/localusersgroups/resetpassword

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{ justaname XX }
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

删除一个用户

删除指定用户。

URL：https://:/xenmobile/api/v1/localusersgroups/

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

导入置备文件

上载包含本地用户数据的文件。 要上载的文件必须采用 .csv 格式。 有关置备文件的详细信息，请参阅置备文件的格式。

URL：https://:/xenmobile/api/v1/localusersgroups/importprovisioningfile

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

响应示例 复制

```
{

   "status": 0,

   "message": "Success",

   "user": null

}
```

管理应用程序

可以使用以下服务管理应用程序。

通过过滤获取所有应用程序

© 1999-2017 Citrix Systems, Inc. All rights reserved.

根据指定的过滤器参数获取应用程序。

URL：https://:/xenmobile/api/v1/application/filter

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌
内容类型 – application/json

示例请求数据 复制

```
{
    "start": 0,
    "limit": 10,

    "applicationSortColumn": "name",
    "sortOrder": "DESC",
    "enableCount": false,
    "search": "Worx",
    "filterIds":"['application.deliverygroup#<DG_Name>@_fn_@app.dg','application.deliverygroup#<DG_Name>@_fn_@app.d
}
```

示例响应数据 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

  "status": 0,

  "message": "Success",

  "applicationListData": {

    "totalMatchCount": 2,

    "totalCount": 2,

    "appList": [{

      "id": 2,

      "name": "WorxNotes",

      "description": "Worx Notes Application",

      "createdOn": "6/7/16 3:55 PM",

      "lastUpdated": "6/7/16 5:11 PM",

      "disabled": false,

      "nbSuccess": 0,

      "nbFailure": 0,

      "nbPending": 0,

      "schedule": null,

      "permitAsRequired": true,

      "iconData": "iVBORw0KGgoAAAANSUhEUgAAAHgAAAB4CAYAAAA5ZDbSAAA.....",

      "appType": "MDX",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "categories": ["Default"],
    "roles": null,
    "workflow": null,
    "vppAccount": null
  }, {
    "id": 1,
    "name": "Angry Bird",
    "description": "",
    "createdOn": "6/7/16 3:53 PM",
    "lastUpdated": "6/7/16 3:54 PM",
    "disabled": false,
    "nbSuccess": 0,
    "nbFailure": 0,
    "nbPending": 0,
    "schedule": null,
    "permitAsRequired": true,
    "iconData": "/9j/4AAQSkZJRgABAQEAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChA...",
    "appType": "App Store App",
    "categories": ["Default"],
    "roles": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "workflow": null,
        "vppAccount": null
      }]
    }
}
```

按容器获取移动应用程序

获取指定容器内的移动应用程序。

URL：https://:/xenmobile/api/v1/application/mobile/{containerId}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "id": 14,
        "name": "testApp",
        "description": "",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"createdOn": null,

"lastUpdated": null,

"disabled": false,

"nbSuccess": 0,

"nbFailure": 0,

"nbPending": 0,

"schedule": {

    "enableDeployment": true,

    "deploySchedule": "NOW",

    "deployScheduleCondition": "EVERYTIME",

    "deployDate": null,

    "deployTime": null,

    "deployInBackground": false

},

"iconData": "",

"appType": "MDX",

"categories": [

    "Default"

],

"roles": [],
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"workflow": null,
"ios": {
    "displayName": "GoToMeeting",
    "description": "G2MW_IOS_5.3.3_075_01",
    "paid": false,
    "removeWithMdm": true,
    "preventBackup": true,
    "appVersion": "5.3.3.075",
    "minOsVersion": "",
    "maxOsVersion": "",
    "excludedDevices": "",
    "avppParams": null,
    "avppTokenParams": null,
    "rules": null,
    "appType": "mobile_ios",
    "uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",
   "id": 0,
    "store": {
        "rating": {
            "rating": 0,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "reviewerCount": 0
        },
        "screenshots": [],
        "faqs": [],
        "storeSettings": {
            "rate": true,
            "review": true
        }
    },
    "policies": [
        {
            "policyName": "ReauthenticationPeriod",
            "policyValue": "480",
            "policyType": "integer",
            "policyCategory": "Authentication",
            "title": "Reauthentication period (minutes)",
            "description": "\nDefines the period before a user is challenged to authenticate again. ",
            "units": "minutes",
            "explanation": null
        }
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
},
{
    "policyName": "BlockJailbrokenDevices",
    "policyValue": "true",
    "policyType": "boolean",
    "policyCategory": "Device Security",
    "title": "Block jailbroken or rooted",
    "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",
    "units": null,
    "explanation": null
},
{
    "policyName": "CertificateLabel",
    "policyValue": "",
    "policyType": "string",
    "policyCategory": "Network Access",
    "title": "Certificate label",
    "description": "\nThe label for the certificate.\n                                                    Default value is er
    "units": null,
    "explanation": null
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                }

            ]

        },

        "android": null,

        "android_knox": null,

        "android_work": null,

        "windows": null,

        "windows_tab": null

    }

}
```

按容器获取公共应用商店应用程序

从指定容器获取公共应用商店应用程序。

URL：https://:/xenmobile/api/v1/application/mobile/appstore/{containerId}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

删除应用程序容器

删除指定应用程序容器。

URL：https://:/xenmobile/api/v1/application/{containerId}

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

© 1999-2017 Citrix Systems, Inc. All rights reserved.

内容类型 – application/json

管理交付组配置

可以使用以下服务管理交付组配置。

通过过滤获取交付组

使用指定的过滤器参数获取交付组。

URL：https://:/xenmobile/api/v1/deliverygroups/filter

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
{

  "start": 1,

  "sortOrder": "DESC",

  "deliveryGroupSortColumn": "id",

  “limit”:10,

  "search": "add"

}
```

响应示例 复制

```
{

    "status": 0,

    "message": "Success",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"dgListData": {

    "totalMatchCount": 7,

    "totalCount": 10,

    "dgList": [

        {

            "id": null,

            "name": "add delivery group 6.0",

            "description": "testing add delivery group 6.0",

        "groups": [[{

                {

                    "id": 1null,

            "userListId": 1null,

            "name": "MSPTESTLOCALGROUP",

            "uniqueName": "MSPTESTLOCALGROUP",

            "uniqueId": "MSPTESTLOCALGROUP",

            "domainName": "local",

            "primaryToken": 0null,

                }"objectSid": null

            ],},

        {
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "id": null,
        "userListId": null,
        "name": "AC08EP61S75",
        "uniqueName": "AC08EP61S75",
        "uniqueId": "AC08EP61S75",
        "domainName": "local",
        "primaryToken": null,
        "objectSid": null
    }],
    "users": [{
        "uniqueName": null,
        "domainName": "local",
        "name": null,
        "objectId": "shankar",
        "customProperties": {
            "name": "value",
            "name1": "value1"
        },
        "uniqueId": "shankar"
    }],
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"zoneId": null,

"zoneDomain": null,

"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId

"disabled": false,

"lastUpdated": 1427144713353,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "Web Link",

        "required": false

    },

    {

        "name": "GoogleApps_SAML",

        "required": true

    }

],

"devicePolicies": [

    "test terms conditions"

]
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        ],
        "smartActions": [
            "shankar ganesh"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    },
    {
        "id": null,
        "name": "add delivery group 5.0",
        "description": "testing add delivery group 5.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                "primaryToken": 0

            }

        ],

        "zoneId": null,

        "zoneDomain": null,

        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId

        "disabled": false,

        "lastUpdated": 1426891345698,

        "anonymousUser": true,

        "roledefLangVersionId": 1,

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false

            }

        ],
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                    "devicePolicies": [

                        "test terms conditions"

                    ],

                    "smartActions": [

                        "shankar ganesh"

                    ],

                    "nbSuccess": 0,

                    "nbFailure": 0,

                    "nbPending": 0

                }

            ]

        }



}
```

根据名称获取交付组

URL：https://:/xenmobile/api/v1/deliverygroups/{name}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
        "name": "AllUsers",
        "description": "default role",
        "groups": [],
        "zoneId": null,
        "zoneDomain": null,
        "rules": null,
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": 1,
        "applications": [
            {
                "name": "test mdx",
                "required": false
            },
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        {
            "name": "test all",
            "required": false
        },
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ],
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        ],
        "smartActions": [
            "justa name"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    }
}
```

编辑交付组

URL：https://:/xenmobile/api/v1/deliverygroups

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
{
  "name": "temp3",
  "description": "temp3 desc",
  "applications": [
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

            "name": "TESTAPP",

             "priority": -1,

             "required": false

                    }     ],

    "devicePolicies": [

        {

             "name":"test terms conditions",

             "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

  "groups": [

     {

  "uniqueName": "AC08EP61S75",

       "domainName": "local",

       "name": "AC08EP61S75",

       "objectSid": "AC08EP61S75",
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"uniqueId": "AC08EP61S75",

"customProperties": {

    "gr1": "gr1",

    "gr2": "gr2"

  }

    }

  ],

  "users": [

    {

      "uniqueName": "testuser",

      "domainName": "local",

      "name": "testuser",

      "objectId": "testuser"

    }

  ],

  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"te

}
```


响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
      "status": 0,
      "message": "Success",
"role": {
            "id": null,
            "name": "temp4",
            "description": "temp4 desc",
            "zoneId": null,
            "zoneDomain": null,
            "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value
            "disabled": false,
            "lastUpdated": null,
            "anonymousUser": false,
            "roledefLangVersionId": null,
            "applications": [
                  {
                  "name": "TESTAPP2",
                  "priority": -1,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                "required": false

            },

{

                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            }

            ],

            "devicePolicies": [

                {

                "name": "TestPolicy1",

                "priority": -1

            },

{

                "name": "TestPolicy",

                "priority": -1

            }

            ],

            "smartActions": [

{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                "name": "TestAction2",

                "priority": -1

            },

{

                "name": "TestAction3",

                "priority": -1

            }

        ],

            "nbSuccess": 0,

            "nbFailure": 0,

            "nbPending": 0,

            "groups": [{

                  "uniqueName": "AC08EP61S75",

                 "domainName": "local",

                "name": "AC08EP61S75",

                 "objectSid": "AC08EP61S75",

                "uniqueId": "AC08EP61S75",

                "customProperties": {

                  "gr1": "gr1",

                    "gr2": "gr2"
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            }

        }],

        "users": [{

            "uniqueName": " tempuser ",

            "domainName": "local",

            "name": " tempuser ",

            "objectId": " tempuser ",

            "customProperties": null,

            "uniqueId": " tempuser "

        }]


    }
```

添加交付组

添加交付组。

URL：https://:/xenmobile/api/v1/deliverygroups

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

  "name": "temp3",

  "description": "temp3 desc",

  "applications": [

{

            "name": "TESTAPP",

             "priority": -1,

             "required": false

                    }     ],

    "devicePolicies": [

        {

            "name":"test terms conditions",

            "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

  "groups": [

    {

  "uniqueName": "AC08EP61S75",
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "domainName": "local",

        "name": "AC08EP61S75",

        "objectSid": "AC08EP61S75",

"uniqueId": "AC08EP61S75",

"customProperties": {

    "gr1": "gr1",

    "gr2": "gr2"

  }}

  ],

  "users": [

    {

      "uniqueName": "testuser",

      "domainName": "local",

      "name": "testuser",

      "objectId": "testuser"

    }

  ],

  "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"te

}
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

响应示例 复制


```
{
    "status": 0,
    "message": "Success",
"role": {
        "id": null,
        "name": "temp4",
        "description": "temp4 desc",
        "zoneId": null,
        "zoneDomain": null,
        "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": null,
        "applications": [
            {
            "name": "TESTAPP2",
            "priority": -1,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                "required": false

            },

{

                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            }

            ],

            "devicePolicies": [

                {

                "name": "TestPolicy1",

                "priority": -1

            },

{

                "name": "TestPolicy",

                "priority": -1

            }

            ],

            "smartActions": [

{
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
                "name": "TestAction2",
                "priority": -1
            },
{
                "name": "TestAction3",
                "priority": -1
            }
        ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "groups": [{
                  "uniqueName": "AC08EP61S75",
          "domainName": "local",
          "name": "AC08EP61S75",
          "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
      "gr1": "gr1",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
      "gr2": "gr2"

  }       }],

          "users": [{

                "uniqueName": " tempuser ",

                "domainName": "local",

                "name": " tempuser ",

                "objectId": " tempuser ",

                "customProperties": null,

                "uniqueId": " tempuser "

          }]


    }
```

删除交付组

删除指定交付组。

URL：https://:/xenmobile/api/v1/deliverygroups

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
[ "add delivery group 11.0" ]
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "roleNames": [
        "add delivery group 11.0"
    ]
}
```

启用或禁用交付组

启用和禁用指定交付组。

URL：https://:/xenmobile/api/v1/deliverygroups/{交付组名称}/{enable/disable}

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "status": 0,
    "message": "Success",
    "roleName": "AllUsers"
}
```

管理服务器属性

可以通过使用以下服务管理 XenMobile 服务器属性。

获取所有服务器属性。

获取所有当前 XenMobile 服务器属性。

URL：https://:/xenmobile/api/v1/serverproperties

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 1,
            "name": "ios.mdm.pki.ca-root.certificatefile",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",
        "displayName": "ios.mdm.pki.ca-root.certificatefile",
        "description": "",
        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",
        "displayFlag": false,
        "editFlag": true,
        "deleteFlag": false,
        "markDeleted": false
    } ,
    {
        "id": 2,
        "name": "ios.mdm.https.host",
        "value": "192.0.2.4",
        "displayName": "ios.mdm.https.host",
        "description": "",
        "defaultValue": "192.0.2.4",
        "displayFlag": false,
        "editFlag": false,
        "deleteFlag": false,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "markDeleted": false

        },

        {

            "id": 3,

            "name": "ios.mdm.enrolment.checkRemoteAddress",

            "value": "false",

            "displayName": "iOS Device Management Enrollment - Check Remote Address",

            "description": "",

            "defaultValue": "false",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": false,

            "markDeleted": false

        },

    ]

}
```


通过过滤获取服务器属性

使用指定的过滤器参数获取服务器属性。

URL：https://:/xenmobile/api/v1/serverproperties/filter

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{
    "start": 0,
    "limit": 1000,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "value": "justaserver1",
            "displayName": "justarserver display name",
            "description": "justaserver description",
            "defaultValue": "justaserver1",
            "displayFlag": true,
            "editFlag": true,
            "deleteFlag": true,
            "markDeleted": false
        }
    ]
}
```

添加服务器属性

添加指定的服务器属性。

URL：https://:/xenmobile/api/v1/serverproperties

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 1",
    "description": "Description 1"
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```

编辑服务器属性

编辑指定的服务器属性。

URL：https://:/xenmobile/api/v1/serverproperties

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

© 1999-2017 Citrix Systems, Inc. All rights reserved.

内容类型 – application/json

请求参数 复制

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

重置服务器属性

重置指定的服务器属性。

URL：https://:/xenmobile/api/v1/serverproperties/reset

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{

    "names": [,

        "justaname7"

        ]

}
```

响应示例 复制

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

删除服务器属性

URL：https://:/xenmobile/api/v1/serverproperties

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求参数 复制

```
{
    "justaname3",
    "justaname4"
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

删除设备

可以通过使用以下服务在 XenMobile 中管理设备。

通过过滤获取设备

URL：https://:/xenmobile/api/v1/device/filter

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

所有**请求参数**均为可选。

sortOrder 的有效值包括：ASC、DSC 和 DESC。

sortColumn 的有效值包括：ID、SERIAL、IMEI、ACTIVESYNCID、WIFIMAC、BLUETOOTHMAC、OSFAMILY、SYSTEM_OEM、SYSTEM_PLATFORM、SYSTEM_OS_VERSION、DEVICE_PROPERTY、LASTAUTHDATE、INACTIVITYDAYS、ISACTIVE、LASTUSER、BLCOMPLIANT、WLCOMPLIANT、RLCOMPLIANT、MANAGED、SHAREABLE 和 BULKPROFILESTATUS。

请求参数 复制


```
{
  "start": "0-999",
  "limit": "0-999",
  "sortOrder": "ASC",
  "sortColumn": "ID",
  "search": "Any search term",
  "enableCount": "false",
  "constraints": "{'constraintList':[{'constraint':'DEVICE_OS_FAMILY','parameters':[{'name':'osFamily','type':'STRING','value':'iO
  "filterIds": "['group#/group/MSP@_fn_@normal']"
}
```


响应示例 复制


```
{
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"id": "1-9999999",

"jailBroken": "true/false",

"managed": "true/false",

"gatewayBlocked": "true/false",

"deployFailed": "1-999",

"deployPending": "1-999",

"deploySuccess": "1-999",

"mdmKnown": "true/false",

"mamRegistered": "true/false",

"mamKnown": "true/false",

"userName": "user name",

"serialNumber": "serial number",

"imeiOrMeid": "IMEI/MEID",

"activeSyncId": "Active sync ID",

"wifiMacAddress": "WiFi MAC address",

"blueToothMacAccress": "Bluetoothi MAC address",

"devicePlatform": "Device platform",

"osVersion": "Operating system version of the device",

"deviceModel": "Device model information",

"lastAccess": "Timestamp when the device was last accessed",
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "inactivityDays": "Number of days device has been inactive",
    "shareable": "Flag indicating if the device is shareable",
    "sharedStatus": "Get shareable status of the device",
    "depRegistered": "Flag indicating if the device is DEP registered",
    "deviceName": "Name of the device",
    "deviceType": "Phone/Tablet",
    "productName": "Product name",
    "platform": "Platform of the device"
}
```

通过设备 ID 获取设备

URL：https://:/xenmobile/api/v1/device/{device_id}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "device": {
  "htcMdm": true,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"managedByZMSP": true,

"serialNumber": "string",

"id": 0,

"applications": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",

  "lastUpdate": 0,

  "status": "SUCCESS",

  "name": "string"

 }

],

"smartActions": [

 {

  "resourceType": "APP_NATIVE",

  "resourceTypeLabel": "string",

  "packageInfo": "string",

  "statusLabel": "string",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"platform": "string",
"osFamily": "WINDOWS",
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"deliveryGroups": [
  {
    "statusLabel": "string",
    "linkey": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"lastAuthDate": 0,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"sharedStatus": "INACTIVE",
"managed": true,
"smgStatus": "ACCESS_ALLOWED",
"mdmKnown": true,
"mamKnown": true,
"mamRegistered": true,
"lastUsername": "string",
"imei": "string",
"activesyncid": "string",
"wifimac": "string",
"bluetoothmac": "string",
"inactivityDays": 0,
"shareable": true,
"bulkProfileStatus": "NO_BULK",
"deviceType": "string",
"softwareInventory": [
 {
  "version": "string",
  "blacklistCompliant": true,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "suggestedListCompliant": true,
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"deviceActions": [
  {
    "actionType": "WIPE",
    "failedTime": 0,
    "doneTime": 0,
    "askedTime": 0
  }
],
"managedSoftwareInventory": [
  {
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "version": "string",
    "blacklistCompliant": true,
    "suggestedListCompliant": true,
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
  }
],
"policies": [
  {
    "resourceType": "APP_NATIVE",
    "resourceTypeLabel": "string",
    "packageInfo": "string",
    "statusLabel": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "name": "string"

   }

],

"active": true,

"xmlId": "string",

"deviceUsers": [

 {

  "user": {

   "displayName": "string",

   "id": 0,

   "xmlId": "string",

   "properties": [

    {

     "displayName": "string",

     "id": 0,

     "b64": true,

     "group": "string",

     "name": "string",

     "value": "string"

    }
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    ]

   },

   "lastAuthDate": 0,

   "prevAuthDate": 0,

   "userLogin": "string"

  }

 ],

 "packageStates": [

  {

   "packageName": "string",

   "packageId": 0,

   "statusLabel": "string",

   "date": 0,

   "status": "PENDING"

  }

 ],

 "pushState": "ENQUEUED",

 "pushStateLabel": "string",

 "lastPushDate": 0,

 "lastSentNotification": 0
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
 "lastSentNotification": 0,
"lastRepliedNotification": 0,
"strongId": "string",
"lastSoftwareInventoryTime": 0,
"firstConnectionDate": 0,
"lastIOSProfileInventoryTime": 0,
"lastUser": {
 "displayName": "string",
 "id": 0,
 "xmlId": "string",
 "properties": [
  {
   "displayName": "string",
   "id": 0,
   "b64": true,
   "group": "string",
   "name": "string",
   "value": "string"
  }
 ]
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
  },
  "blacklistCompliant": true,
  "suggestedListCompliant": true,
  "requiredListCompliant": true,
  "devicePropertiesTimestamp": 0,
  "revoked": true,
  "mamDeviceId": "string",
  "deviceToken": "string",
  "typeInst": 0,
  "appLock": true,
  "appWipe": true,
  "mamReady": true,
  "validCertificates": [
   {
    "credentialProviderId": "string",
    "type": "string",
    "issuerName": "string",
    "startDate": 0,
    "endDate": 0,
    "revoked": true,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "certificateNumber": "string"
  }
],
"revokedCertificates": [
  {
    "credentialProviderId": "string",
    "type": "string",
    "issuerName": "string",
    "startDate": 0,
    "endDate": 0,
    "revoked": true,
    "certificateNumber": "string"
  }
],
"authorizeEnabled": true,
"revokeEnabled": true,
"lockEnabled": true,
"cancelLockEnabled": true,
"unlockEnabled": true,
"cancelUnlockEnabled": true,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"containerLockEnabled": true,

"cancelContainerLockEnabled": true,

"containerUnlockEnabled": true,

"cancelContainerUnlockEnabled": true,

"containerPwdResetEnabled": true,

"cancelContainerPwdResetEnabled": true,

"wipeEnabled": true,

"cancelWipeEnabled": true,

"clearRestrictionsEnabled": true,

"cancelClearRestrictionsEnabled": true,

"corpWipeEnabled": true,

"cancelCorpWipeEnabled": true,

"sdCardWipeEnabled": true,

"cancelSdCardWipeEnabled": true,

"locateEnabled": true,

"cancelLocateEnabled": true,

"enableTrackingEnabled": true,

"disableTrackingEnabled": true,

"disownEnabled": true,

"activationLockBypassEnabled": true,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"ringEnabled": true,
"cancelRingEnabled": true,
"newPinCode": "string",
"oldPinCode": "string",
"lockMessage": "string",
"resetPinCode": true,
"scanTime": "string",
"screenSharingPwd": "string",
"iosprofileInventory": [
 {
  "iosConfigInventories": [
   {
    "description": "string",
    "type": "string",
    "organization": "string",
    "identifier": "string",
    "name": "string"
   }
  ],
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "description": "string",
    "organization": "string",
    "managed": true,
    "identifier": "string",
    "receivedDate": 0,
    "encrypted": true,
    "name": "string"
   }
  ],
  "iosprovisioningProfileInventory": [
   {
    "managed": true,
    "uuid": "string",
    "expiryDate": 0,
    "name": "string"
   }
  ],
  "erasedMemoryCard": true,
  "gpsCoordinates": [
   {
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "gpsTimestamp": 0

   }

],

"lastGpsCoordinate": {

  "gpsTimestamp": 0

},

"gpsFilterStartDate": 0,

"gpsFilterEndDate": 0,

"wipePinCode": "string",

"lockPhoneNumber": "string",

"dstDevIdUsed": true,

"dstValue": "string",

"smartActionsFailure": true,

"policiesFailure": true,

"applicationsFailure": true,

"touchdownProperties": [

  {

    "category": "string",

    "name": "string",

    "value": "string"
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
  }

],

"appUnwipeEnabled": true,

"requestMirroringEnabled": true,

"cancelRequestMirroringEnabled": true,

"stopMirroringEnabled": true,

"cancelStopMirroringEnabled": true,

"knownByZMSP": true,

"wipeDeviceFlag": true,

"lockDeviceFlag": true,

"appWipeEnabled": true,

"appLockEnabled": true,

"appUnlockEnabled": true,

"bulkEnrolled": true,

"nbAvailable": 0,

"hasContainer": true,

"connected": true,

"properties": [

  {

    "displayName": "string",
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
      "id": 0,
      "b64": true,
      "group": "string",
      "name": "string",
      "value": "string"
    }
   ]
  }
}
```

通过设备 ID 获取设备应用程序

URL：https://:/xenmobile/api/v1/device/{device_id}/apps

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "status": 0,
 "message": "string",
 "applications": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```

通过设备 ID 获取设备操作

URL：https://:/xenmobile/api/v1/device/{device_id}/actions

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

响应示例 复制


```
{
 "status": 0,
 "message": "string",
 "actions": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```


通过设备 ID 获取设备交付组

URL：https://:/xenmobile/api/v1/device/{device_id}/deliverygroups

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

© 1999-2017 Citrix Systems, Inc. All rights reserved.

内容类型 – application/json

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deliveryGroups": [
  {
   "statusLabel": "string",
   "linkey": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```

通过设备 ID 获取受管软件清单

URL：https://:/xenmobile/api/v1/device/{device_id}/managedswinventory

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

响应示例 复制


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

通过设备 ID 获取策略

URL：https://:/xenmobile/api/v1/device/{device_id}/policies

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "policies": [

  {

   "resourceType": "APP_NATIVE",

   "resourceTypeLabel": "string",

   "packageInfo": "string",

   "statusLabel": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```

通过设备 ID 获取软件清单

URL：https://:/xenmobile/api/v1/device/{device_id}/softwareinventory

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

响应示例 复制


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

通过设备 ID 获取 GPS 坐标

URL：https://:/xenmobile/api/v1/device/locations/{device_id}

查询参数：

startDate – 坐标过滤器的开始日期
endDate – 坐标过滤器的结束日期

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceCoordinates": {

  "deviceCoordinateList": {

   "deviceCoordinateList": [

    {

     "gpsTimestamp": 0

    }

   ],

   "startDate": 0,

   "endDate": 0

  }

}
```

向一系列设备或用户发送通知

URL：https://:/xenmobile/api/v1/device/notify

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "smtpFrom": "Test",
 "to": [
  {
   "deviceId": "1",
   "email": "user@test.com",
   "osFamily": "iOS",
   "serialNumber": "F7NLX6WDF196",
   "smsTo": "+123456676",
   "token": {
    "type": "apns",
     "value": "dfb2fb351a4fb068e40858ecad572e317e6c39b4fa7de6fb29ea1ad7e2254499"
   }
  }
 ],
 "smtpSubject": "This is test subject",
 "smtpMessage": "This is test message",
 "smsMessage": "This is test message",
 "agentMessage": "This is test message",
 "sendAsBCC": "true",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"smtp": "true",

"sms": "true",

"agent": "true",

"templateId": "-1",

"agentCustomProps": {

 "sound": "Casino.wav"

}
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "status": 0,
 "message": "string",
 "notificationRequests": {
  "smtpNotifRequestId": 0,
  "smsNotifRequestId": 0,
  "smsGatewayNotifRequestId": 0,
  "apnsAgentNotifRequestId": 0,
  "shtpAgentNotifRequestId": 0
 }
}
```

向一系列设备授权

URL：https://:/xenmobile/api/v1/device/authorize

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上应用激活锁跳过

URL：https://:/xenmobile/api/v1/device/activationLockBypass

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在一系列设备上应用应用程序锁定

URL：https://:/xenmobile/api/v1/device/appLock

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上应用应用程序擦除

URL：https://:/xenmobile/api/v1/device/appWipe

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在一系列设备上应用容器锁定

URL：https://:/xenmobile/api/v1/device/containerLock

查询参数：newPinCode – Android 容器的 PIN 代码

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上取消容器锁定

URL：https://:/xenmobile/api/v1/device/containerLock/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在一系列设备上应用容器解锁

URL：https://:/xenmobile/api/v1/device/containerUnlock

查询参数：newPinCode – Android 容器的 PIN 代码

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

在一系列设备上取消容器解锁

URL：https://:/xenmobile/api/v1/device/containerUnlock/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在一系列设备上重置容器密码

URL：https://:/xenmobile/api/v1/device/containerPwdReset

查询参数：newPinCode – Android 容器的 PIN 代码

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上取消重置容器密码

URL：https://:/xenmobile/api/v1/device/containerPwdReset/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

否认拥有一系列设备

URL：https://:/xenmobile/api/v1/device/disown

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

定位一系列设备

URL：https://:/xenmobile/api/v1/device/locate

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

取消定位一系列设备

URL：https://:/xenmobile/api/v1/device/locate/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

在一系列设备上应用 GPS 跟踪

URL：https://:/xenmobile/api/v1/device/track

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在一系列设备上取消 GPS 跟踪

URL：https://:/xenmobile/api/v1/device/track/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

锁定一系列设备

URL：https://:/xenmobile/api/v1/device/lock

查询参数：

newPinCode – Android 和 Symbian 设备的 PIN 代码必须为 4 到 16 个字符。 Windows 设备的 PIN 码必须是 4 位数字
resetPinCode – 向锁定请求中添加重置 PIN 码请求。 仅适用于 Windows phone 8.1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

lockMessage – 向锁定请求中添加消息。 仅适用于 iOS 7 及更高版本
phoneNumber – 向锁定请求中添加电话号码。 仅适用于 iOS 7 及更高版本

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

取消锁定一系列设备

URL：https://:/xenmobile/api/v1/device/lock/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

解锁一系列设备

URL：https://:/xenmobile/api/v1/device/unlock

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

取消解锁一系列设备

URL：https://:/xenmobile/api/v1/device/unlock/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

部署一系列设备

URL：https://:/xenmobile/api/v1/device/refresh

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上请求使用 AirPlay 镜像

URL：https://:/xenmobile/api/v1/device/requestMirroring

查询参数：

dstName – 目标名称，作为目标名称或目标设备 ID
dstDevId – 目标设备的 MAC 地址，作为目标名称或目标设备 ID

© 1999-2017 Citrix Systems, Inc. All rights reserved.

scanTime – 扫描秒数
screenSharingPwd – 屏幕共享的密码

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上取消请求使用 AirPlay 镜像

URL：https://:/xenmobile/api/v1/device/requestMirroring/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在一系列设备上停止使用 AirPlay 镜像

URL：https://:/xenmobile/api/v1/device/stopMirroring

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上取消停止使用 AirPlay 镜像

URL：https://:/xenmobile/api/v1/device/stopMirroring/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在一系列设备上清除所有限制

URL：https://:/xenmobile/api/v1/device/restrictions/clear

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

在一系列设备上取消清除所有限制

URL：https://:/xenmobile/api/v1/device/restrictions/clear/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

吊销一系列设备

URL：https://:/xenmobile/api/v1/device/revoke

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

使一系列设备响铃

URL：https://:/xenmobile/api/v1/device/ring

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

取消使一系列设备响铃

URL：https://:/xenmobile/api/v1/device/ring/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

擦除一系列设备

URL：https://:/xenmobile/api/v1/device/wipe

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

取消擦除一系列设备

URL：https://:/xenmobile/api/v1/device/wipe/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

选择性擦除一系列设备

URL：https://:/xenmobile/api/v1/device/selwipe

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

取消选择性擦除一系列设备

URL：https://:/xenmobile/api/v1/device/selwipe/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

擦除一系列设备上的 SD 卡

URL：https://:/xenmobile/api/v1/device/sdcardwipe

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求示例 复制

```
[1,2]
```

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

取消擦除一系列设备上的 SD 卡

URL：https://:/xenmobile/api/v1/device/sdcardwipe/cancel

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
[1,2]
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

获取设备上的所有已知属性

URL：https://:/xenmobile/api/v1/device/knownProperties

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.

响应示例 复制


```
{
 "status": 0,
 "message": "string",
 "knownProperties": {
  "knownProperties": {
   "knownPropertyList": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string",
     "group": "EVERYWAN",
     "groupLabel": "string"
    }
   ]
  }
}
```


获取设备上的所有已用属性

URL：https://:/xenmobile/api/v1/device/usedProperties

© 1999-2017 Citrix Systems, Inc. All rights reserved.

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
 "status": 0,
 "message": "string",
 "deviceUsedPropertiesList": {
  "deviceUsedProperties": {
   "deviceUsedPropertiesParameters": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string"
    }
   ]
  }
 }
}
```

通过设备 ID 获取所有设备属性

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL：https://:/xenmobile/api/v1/device/properties/{deviceId}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制


```
{
 "status": 0,
 "message": "string",
 "devicePropertiesList": {
  "deviceProperties": {
   "startIndex": 0,
   "devicePropertyParameters": [
    {
     "name": "string",
     "value": "string",
     "id": 0,
     "displayName": "string",
     "group": "string",
     "b64": true
    }
   ],
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "totalCount": 0
  }
 }
}
```

通过设备 ID 更新所有设备属性

URL：https://:/xenmobile/api/v1/device/properties/{deviceId}

请求类型：PUT

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
{
  "properties": [
    {
      "name": "ACTIVE_ITUNES",
      "value": "0"
    }
  ]
}
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "status": 0,
 "message": "string"
}
```

通过设备 ID 添加或更新设备属性

URL：https://:/xenmobile/api/v1/device/properties/{deviceId}

请求类型：POST

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

请求示例 复制

```
{
 "name": "PROPERTY_NAME",
 "value": "PROPERTY_VALUE"
}
```

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "status": 0,
 "message": "string"
}
```

通过设备 ID 删除设备属性

URL：https://:/xenmobile/api/v1/device/properties/{deviceId}

请求类型：DELETE

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

```
{
 "status": 0,
 "message": "string"
}
```

通过设备 ID 获取 iOS 设备 MDM 状态

URL：https://:/xenmobile/api/v1/device/mdmStatus/{deviceId}

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
 "status": 0,
 "message": "string",
 "deviceMdmStatus": {
  "deviceMdmStatusParameters": {
     "pushState": "ENQUEUED",
     "lastPushDate": 0,
     "lastRepliedNotification": 0,
     "lastSentNotification": 0,
     "pushStateLabel": "string"
   }
 }
}
```


生成 PIN 代码

URL：https://:/xenmobile/api/v1/device/pincode/generate

查询参数：pinCodeLength – 请求的 PIN 代码的长度

请求类型：GET

请求标头：auth_token – 用户登录时获取的身份验证令牌

内容类型 – application/json

响应示例 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

 "status": 0,

 "message": "string",

 "pinCode": {

  "answer": "string"

 }

}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile SOAP API

Aug 15, 2016

可以在 XenMobile 中使用以下 SOAP Web 服务 API 进行移动设备管理。 可以从 XenMobile Developer Community 站点下载适用于 XenMobile 的 API 和 SDK。

Web 服务定义语言 (WSDL) 名称	调用
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto

© 1999-2017 Citrix Systems, Inc. All rights reserved.

getDeviceInfo

getDeviceInformationForUser

getDeviceProperties

getLastUser

getManagedStatus

getMasterKeyList

getSoftwareInventory

getStrongID

getUserDevices

isEnforceSSL

isEnforceStrongAuthentication

locateDevice

lockDevice

putDeviceProperties

registerDeviceForUser

removeDevice

resetDeploymentState

revoke

unlockDevice

wipeDevice

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	browseOtp
	createOtp
	getAvailableEnrollmentModes
	getOtpInfo
	revokeOtp
	triggerNotification

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Mail Manager 10

Oct 21, 2016

XenMobile Mail Manager 可以采用以下方式扩展 XenMobile 的功能：

- 用于 Exchange Active Sync (EAS) 设备的动态访问控制。 可以自动允许或阻止 EAS 设备访问 Exchange 访问。
- 使 XenMobile 能够访问 Exchange 提供的 EAS 设备合作信息。
- 使 XenMobile 能够在移动设备上执行 EAS 擦除。
- 使 XenMobile 能够访问关于黑莓设备的信息以及执行控制操作，如擦除和重置密码。

要下载 XenMobile Mail Manager，请转到 Citrix.com 中 XenMobile 10 Server 下的“服务器组件”部分。

XenMobile Mail Manager 10.1 中的新增功能

访问规则

“Rule Analysis”（规则分析）窗口包含一个复选框，选中该复选框时，将仅显示冲突、替代、冗余或增补规则。

分别为在您的 XenMobile 部署中配置的每个 Microsoft Exchange 环境设置默认访问【“Allow”（允许）、“Block”（阻止）或“Unchanged”（保持不变））和 ActiveSync 命令模式（“PowerShell”或“Simulation”（模拟））】。

快照

可以配置在快照历史记录中显示的最大快照数。

可以创建主要快照期间要忽略的错误。 如果主要快照返回的错误未配置为可忽略，则将放弃快照的结果。

要将错误配置为可忽略，请使用 XML 编辑器编辑 config.xml 文件：

- 如果 Exchange Server 为 Office 365，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors 节点，并使用与现有错误子元素相同的格式添加要匹配的文本作为子元素。 支持正则表达式。
- 如果 Exchange Server 为本地服务器，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors 节点，并使用与现有错误子元素相同的格式添加要匹配的文本作为子元素。 支持正则表达式。
- 如果配置了多个 Exchange 环境，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='与所需的 Exchange 环境对应的 ID']/ExchangeServer/Specialists/PowerShell 节点 对于要忽略的每个错误，向 PowerShell 节点添加一个 IgnorableErrors 子节点。 将 Error 子节点添加到 IgnorableErrors 节点，并在 CDATA 部分包含匹配的文本。 支持正则表达式。

保存 config.xml 并重新启动 XenMobile Mail Manager 服务。

PowerShell 和 Exchange

XenMobile Mail Manager 现在根据所连接到的 Exchange 版本动态决定要使用的 cmdlet。 例如，对于 Exchange 2010，将使用 Get-ActiveSyncDevice，而对于 Exchange 2013 和 Exchange 2016，则使用 Get-MobileDevice。

Exchange 配置

无需启动 XenMobile Mail Manager 服务即可编辑和更新 Exchange Server 配置。

向 Exchange 环境的摘要选项卡中添加的两个新列显示了每个环境的命令模式【“PowerShell”或“Simulation”（模拟）】和访问模式【“Allow”（允许）、“Block”（阻止）或“Unchanged”（保持不变）】。

故障排除和诊断

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support\PowerShell 文件夹中提供了一组用于故障排除的 PowerShell 实用程序。

使用控制台的“Configuration”（配置）窗口中的“Test Connectivity”（测试连接）按钮测试与 Exchange 服务的连接将运行服务所使用的每个只读 cmdlet，针对所配置的用户的 Exchange Server 运行 RBAC 权限测试，以及使用不同颜色显示所有错误或警告（蓝色-黄色表示警告，红色-橙色表示错误）。

新的故障排除工具将对用户的邮箱和设备执行深度分析（从而检测错误条件和潜在的故障区域），并对用户执行深度 RBAC 分析。 该工具可以将所有 cdmlet 的原始输出保存到一个文本文件。

在支持场景中，可以通过选中控制台中的一个诊断复选框来保存 XenMobile Mail Manager 管理的所有设备上的所有邮箱的所有属性。

在支持场景中，现在支持跟踪级别日志记录。

身份验证

XenMobile Mail Manager 支持对本地部署进行“Basic”（基本）身份验证。 这将允许在 XenMobile Mail Manager 服务器不属于 Exchange Server 所在域的成员的情况下使用 XenMobile Mail Manager。

已修复的问题

访问规则

XenMobile Mail Manager 对 Active Directory (AD) 组中的所有用户应用本地访问控制规则，即使 AD 组包含的用户数超过 1000 也是如此。 以前，XenMobile Mail Manager 仅对 AD 组的前 1000 个用户应用本地访问控制规则。 [#548705]

XenMobile Mail Manager 控制台有时在查询包含 1000 个以上用户的 Active Directory 组时无法响应。 [CXM-11729]

“LDAP Configuration”（LDAP 配置）窗口不再显示不正确的身份验证模式。 [CXM-5556]

快照

带撇号的用户名不再导致次要快照出现故障。 [#617549]

在禁用了流水线操作的支持场景中【“Disable Pipelining”（禁用流水线操作）选项在 XenMobile Mail Manager 控制台的“Configuration”（配置）窗口中处于选中状态】，主要快照在本地 Exchange 环境中将不再出现故障。 [#586083]

在禁用了流水线操作的支持场景中【“Disable Pipelining”（禁用流水线操作）选项在 XenMobile Mail Manager 控制台的“Configuration”（配置）窗口中处于选中状态】，不再收集深层快照的数据，与环境是针对深层快照还是浅表快照配置的无关。 现在，仅当环境是针对深层快照配置的情况下，才收集深层快照的数据。 [#586092]

初始安装完成后创建的第一个主要快照有时会遇到阻止 XenMobile Mail Manager 运行另一个主要快照的错误，直至重新启动 XenMobile Mail Manager 服务。 此错误不再发生。 [CXM-5536]

关于 XenMobile Mail Manager 10

© 1999-2017 Citrix Systems, Inc. All rights reserved.

关于 XenMobile Mail Manager 10.1

Oct 21, 2016

XenMobile Mail Manager 10.1 中新增了以下功能：

访问规则

“Rule Analysis”（规则分析）窗口包含一个复选框，选中该复选框时，将仅显示冲突、替代、冗余或增补规则。

分别为在您的 XenMobile 部署中配置的每个 Microsoft Exchange 环境设置默认访问【“Allow”（允许）、“Block”（阻止）或“Unchanged”（保持不变）】和 ActiveSync 命令模式（“PowerShell”或“Simulation”（模拟）】。

快照

可以配置在快照历史记录中显示的最大快照数。

可以创建主要快照期间要忽略的错误。 如果主要快照返回的错误未配置为可忽略，则将放弃快照的结果。

要将错误配置为可忽略，请使用 XML 编辑器编辑 config.xml 文件：

- 如果 Exchange Server 为 Office 365，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors 节点，并使用与现有错误子元素相同的格式添加要匹配的文本作为子元素。 支持正则表达式。 转到步骤 7。
- 如果 Exchange Server 为本地服务器，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors 节点，并使用与现有错误子元素相同的格式添加要匹配的文本作为子元素。 支持正则表达式。 转到步骤 7。
- 如果配置了多个 Exchange 环境，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='与所需的 Exchange 环境对应的 ID']/ExchangeServer/Specialists/PowerShell 节点 对于要被忽略的每个错误，向 PowerShell 节点添加一个 IgnorableErrors 子节点，然后向 IgnorableErrors 节点添加一个 Error 子节点，并在 CDATA 部分中包含匹配的文本。 支持正则表达式。

保存 config.xml 并重新启动 XenMobile Mail Manager 服务。

PowerShell 和 Exchange

XenMobile Mail Manager 现在根据所连接到的 Exchange 版本动态决定要使用的 cmdlet。 例如，对于 Exchange 2010，将使用 **Get-ActiveSyncDevice**，而对于 Exchange 2013 和 Exchange 2016，则使用 **Get-MobileDevice**。

Exchange 配置

无需启动 XenMobile Mail Manager 服务即可编辑和更新 Exchange Server 配置。

向 Exchange 环境的摘要选项卡中添加的两个新列显示了每个环境的命令模式【“PowerShell”或“Simulation”（模拟）】和访问模式【“Allow”（允许）、“Block”（阻止）或“Unchanged”（保持不变）】。

故障排除和诊断

Support\PowerShell 文件夹中提供了一组用于故障排除的 PowerShell 实用程序。

使用控制台的“Configuration”（配置）窗口中的 **Test Connectivity**（测试连接）按钮测试与 Exchange 服务的连接将运行服务所使用的每个**只读** cmdlet，针对所配置的用户的 Exchange Server 运行 RBAC 权限测试，以及使用不同颜色显示所有错误或警告（蓝色-黄色表示警告，红色-橙色表示错误）。

新的故障排除工具将对用户的邮箱和设备执行深度分析（从而检测错误条件和潜在的故障区域），并对用户执行深度 RBAC 分析。 该工具可以将所有 cdmlet 的原始输出保存到一个文本文件。

在支持场景中，可以通过选中控制台中的一个诊断复选框来保存 XenMobile Mail Manager 管理的所有设备上的所有邮箱的所有属性。

在支持场景中，现在支持跟踪级别日志记录。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

身份验证

XenMobile Mail Manager 支持对本地部署进行“Basic”（基本）身份验证。 这将允许在 XenMobile Mail Manager 服务器不属于 Exchange Server 所在域的成员的情况下使用 XenMobile Mail Manager。

已修复的问题

访问规则

XenMobile Mail Manager 对 Active Directory 组中的所有用户应用本地访问控制规则，即使 Active Directory 组包含的用户数超过 1,000 也是如此。 以前，XenMobile Mail Manager 仅对 Active Directory 组的前 1,000 个用户应用本地访问控制规则。 [#548705]

XenMobile Mail Manager 控制台有时在查询包含 1,000 个以上用户的 Active Directory 组时无法响应。 [CXM-11729]

“LDAP Configuration”（LDAP 配置）窗口不再显示不正确的身份验证模式。 [CXM-5556]

快照

带撇号的用户名不再导致次要快照出现故障。 [#617549]

在禁用了流水线操作的支持场景中，**【Disable Pipelining**（禁用流水线操作）选项在 XenMobile Mail Manager 控制台的“Configuration”（配置）窗口中处于选中状态】，主要快照在本地 Exchange 环境中将不再出现故障。 [#586083]

在禁用了流水线操作的支持场景中，**【Disable Pipelining**（禁用流水线操作）选项在 XenMobile Mail Manager 控制台的“Configuration”（配置）窗口中处于选中状态】，不再收集深层快照的数据，与环境是针对深层快照还是浅表快照配置的无关。 现在，仅当环境是针对深层快照配置的情况下，才收集深层快照的数据。 [#586092]

初始安装完成后创建的第一个主要快照有时会遇到阻止 XenMobile Mail Manager 运行另一个主要快照的错误，直至重新启动 XenMobile Mail Manager 服务。 此错误不再发生。 [CXM-5536]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

关于 XenMobile Mail Manager 10

Oct 21, 2016

已知问题

- 在升级到 XenMobile Mail Manager 10 的过程中，已安装的 XenMobile Mail Manager 版本会始终显示为 8.5，但会进行 XenMobile Mail Manager 升级。 [#539520]
- 在次要快照中报告的“已找到设备”可能会引起混淆。 如果在启动主要快照后运行次要快照，则同一设备可能会连续在次要快照摘要中报告为“新增”。
- XenMobile Mail Manager 可能会仅对 Active Directory 组中的前 1000 个用户应用本地访问控制规则，即使该组包含的用户数超过 1000 也是如此。

已修复的问题

Power Shell/Exchange 管理

在特定的 Microsoft Exchange 环境（主要是 Office 365）中，对 XenMobile Mail Manager 设置限制可有效限制带宽，阻止应用程序发出任何 PowerShell 请求或命令。 现在可在 Exchange 配置选项卡中使用备用 PowerShell cmdlet 途径，会将 XenMobile Mail Manager 置于备用快照模式中，此模式可绕过原始数据路径。

通过一个新标志，您可以对非 Microsoft Office 365 环境公开 AllowRedirection 标志。 使用 Microsoft Exchange 配置选项卡启用此标志。

规则管理

LDAP 本地规则现在针对大型 Active Directory 环境支持任意数量的组。

XenMobile 复制 WorxMail 客户端的设备信息。 解决此问题要求您启用 XenMobile Mail Manager 的 Managed Service Provider (MSP) 部分中的正则表达式支持，这样做会过滤返回到 XenMobile 的记录集。 满足过滤条件的设备不会返回到 XenMobile。

MSP

从黑莓 Enterprise Server (BES) 数据库中删除的用户现在已从本地数据库中删除。

UI

现在可以将进度对话框类用于发生持续进程的情形。 在此类过程中，XenMobile Mail Manager 会发送用户反馈，并向他们提供取消的机会（如果适合）。

现在将新 Microsoft Exchange 实例的默认值设置为“Shallow”（浅表）。

安装程序

已更改引用 Zenprise 的组件以反映 XenMobile Mail Manager。

安装程序找不到安装路径时会挂起。

安装后，支持二进制文件和脚本现在位于“支持”文件夹中。

在 Windows 的“开始”菜单中，XenMobile Mail Manager 快捷方式现在位于 \Citrix\XenMobile Mail Manager 文件夹中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

支持

通过“支持”模型，可以通过添加 config.xml 文件启用故障排除功能。 您可以使用此文件帮助 Citrix 解决问题。 在此版本的 XenMobile Mail Manager 中，此功能仅适用于 Microsoft Exchange 配置的“Add”（添加）和“Edit”（编辑）屏幕。

注意：您还可以在打开配置实用程序时，通过按住 Shift 键来启用此故障排除功能。

日志记录

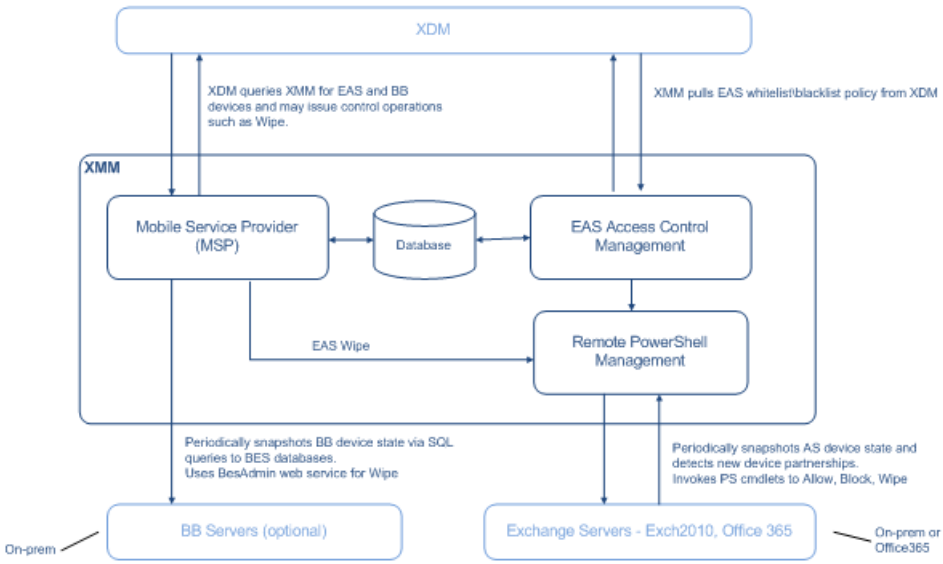
从 PowerShell 返回的错误消息现在具有与其关联的 GUID。 使用此值可控制“Snapshot History”（快照历史记录）详细信息选项卡中显示的内容。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

体系结构

Oct 21, 2016

下图显示了 XenMobile Mail Manager 的主要组件。 有关详细的参考体系结构图，请参阅《XenMobile 部署手册》文章适用于本地部署的参考体系结构。



这三个主要组件如下：

- **Exchange ActiveSync 访问控制管理**。 与 XenMobile 进行通信以从 XenMobile 中检索 Exchange ActiveSync 策略，并将此策略与所有本地定义的策略合并以确定应被允许或拒绝访问 Exchange 的 Exchange ActiveSync 设备。 本地策略允许扩展策略规则，以允许 Active Directory 组、用户、设备类型或设备用户代理（通常为移动平台版本）执行访问控制。
- **远程 Powershell 管理**。 此组件负责计划和调用远程 PowerShell 命令，以执行 Exchange ActiveSync 访问控制管理编译的策略。 此组件定期创建 Exchange ActiveSync 数据库的快照，以检测新的或已更改的 Exchange ActiveSync 设备。
- 移动服务提供商。 提供 Web 服务界面，以便 XenMobile 可以查询 Exchange ActiveSync 和/或黑莓设备以及对这些设备执行“擦除”等问题控制操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

系统要求和必备条件

Oct 21, 2016

要使用 XenMobile Mail Manager，需要满足以下最低系统要求：

- Windows Server 2008 R2（必须是基于英语的服务器）
- Microsoft SQL Server 2008、SQL Server 2012、SQL Server 2016、SQL Server Express 2008、SQL Server 2012 或 Microsoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5
- 黑莓 Enterprise Service 版本 5（可选）

Microsoft Exchange Server 的最低支持版本

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 SP2

XenMobile Mail Manager 必备条件

- 必须安装 Windows Management Framework。
  - PowerShell V5、V4 和 V3
- 必须通过 Set-ExecutionPolicy RemoteSigned 将 PowerShell 执行策略设置为 RemoteSigned。
- 必须在运行 XenMobile Mail Manager 的计算机和远程 Exchange Server 之间打开 TCP 端口 80。

运行 Exchange 的本地计算机的要求

权限。 在 Exchange 配置用户界面中指定的凭据必须能够连接到 Exchange Server，并且具有执行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：

- **针对 Exchange Server 2010 SP2**：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **对于 Exchange Server 2013 和 Exchange Server 2016**：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- 如果将 XenMobile Mail Manager 配置为查看整个林，必须授权以运行 Set-AdServerSettings -ViewEntireForest $true
- 提供的凭据必须具有通过远程 Shell 连接到 Exchange Server 的权限。 默认情况下，安装 Exchange 的用户具有此权限。
- 根据 Microsoft TechNet 文章关于远程要求，要建立远程连接并运行远程命令，凭据必须与远程计算机上的管理员用户对应。 根据此博客文章 You Don't Have to Be An Administrator to Run Remote PowerShell Commands（您不需要成为管理员即可运行远程 PowerShell 命令）， Set-PSSessionConfiguration 可以用来消除管理要求，但是对此命令的细节支持和讨论不在本文档的范围内。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 此外，Exchange Server 还必须配置为支持通过 HTTP 进行的远程 PowerShell 请求。 通常，只需要在 Exchange Server 上运行下列 PowerShell 命令的管理员： WinRM QuickConfig。
- Exchange 有许多限制策略。 其中一个策略控制每个用户允许的并发 PowerShell 连接的数目。 在 Exchange 2010 中，一个用户允许的同时连接数默认为 18。 达到连接限制后，XenMobile Mail Manager 将不能连接到 Exchange Server。 存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。 如果有兴趣，可以通过 PowerShell 来调查与远程管理相关的 Exchange 限制策略。

Office 365 Exchange 的要求

- **权限**。 在 Exchange 配置用户界面中指定的凭据必须能够连接到 Office 365，并且具有执行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- 提供的凭据必须已获得授权，可以通过远程 Shell 连接到 Office 365 服务器。 默认情况下，Office 365 联机管理员具有必备的权限。
- Exchange 有许多限制策略。 其中一个策略控制每个用户允许的并发 PowerShell 连接的数目。 在 Office 365 中，一个用户允许的同时连接数默认为三个。 达到连接限制后，XenMobile Mail Manager 将不能连接到 Exchange Server。 存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。 如果有兴趣，可以通过 PowerShell 调查与远程管理相关的 Exchange 限制策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装和配置

Oct 21, 2016

1. 单击 XmmSetup.msi 文件，然后按照安装程序中的提示安装 XenMobile Mail Manager。

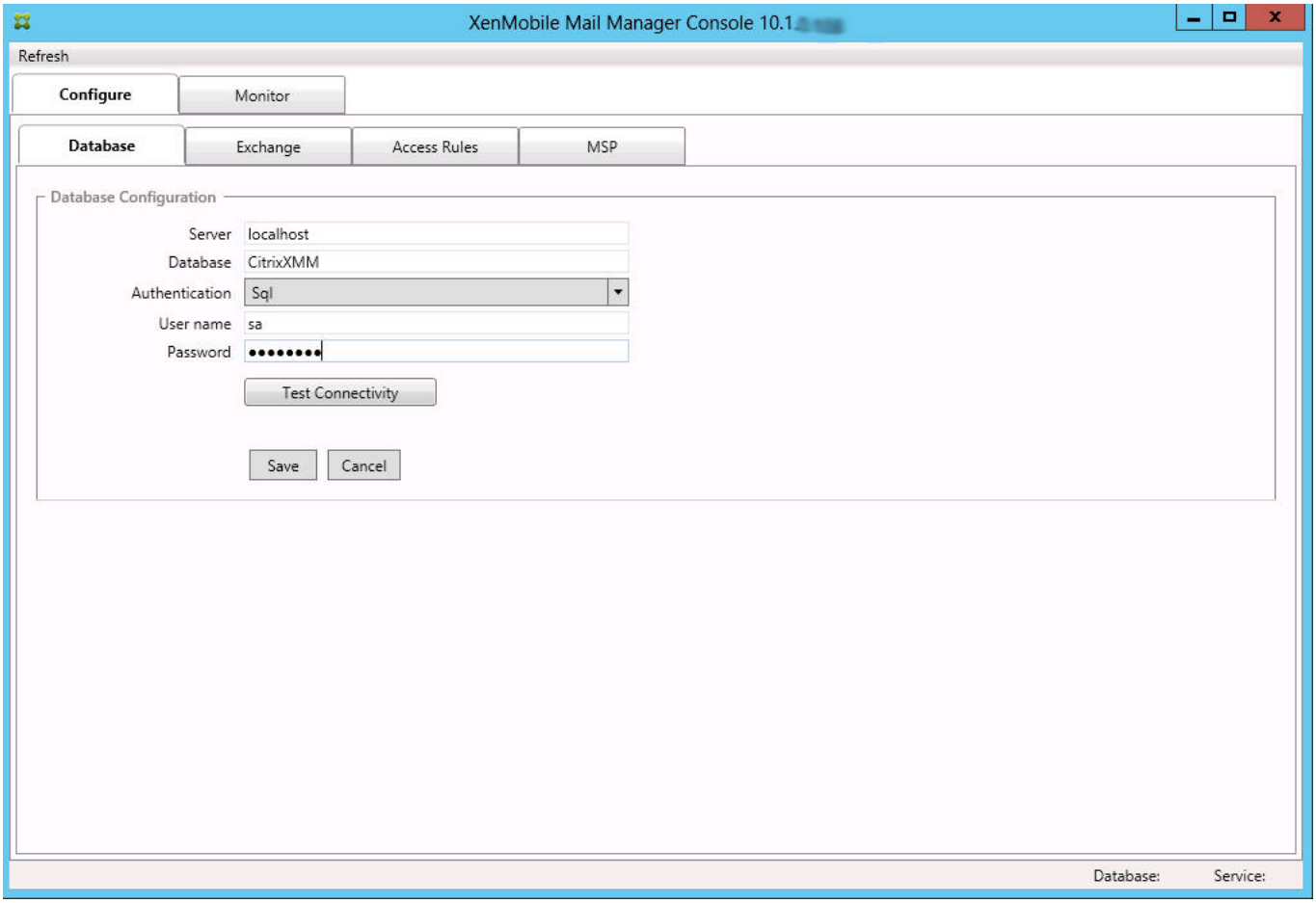
2. 保留在设置向导的最后一个屏幕中选中的 **Launch the Configure utility**（启动配置实用程序）选项。 或者，从**开始**菜单中打开 **XenMobile Mail Manager**。

3. 配置以下数据库属性：
    1. 选择 **Configure**（配置）> **Database**（数据库）选项卡。
    2. 输入 SQL Server 的服务器名称（默认为 localhost）。
    3. 将数据库保留为默认 CitrixXmm。
    4. 选择以下用于 SQL 的身份验证模式之一：
        - **Sql**。 输入有效 SQL 用户的用户名和密码。

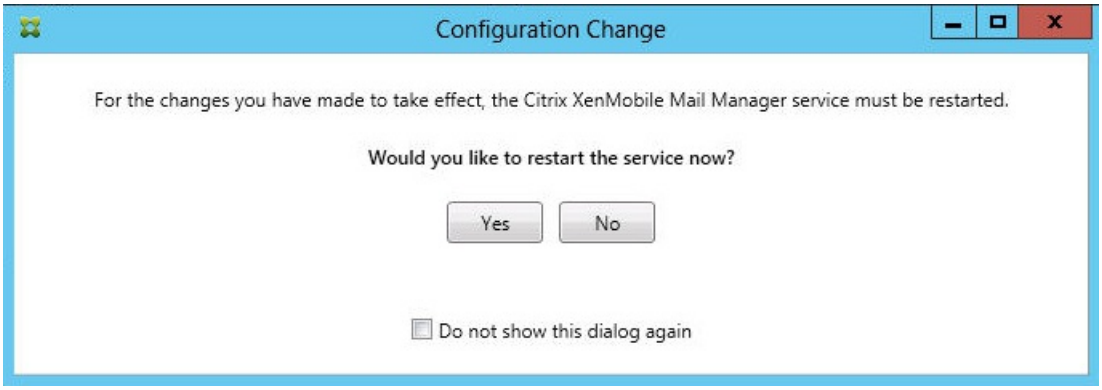
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Windows 集成**。 如果选择此选项，XenMobile Mail Manager 服务的登录凭据必须更改为具有访问 SQL Server 权限的 Windows 帐户。 为此，请打开**控制面板** > **管理工具** > **服务**，在 XenMobile Mail Manager 服务条目上单击鼠标右键，然后单击**登录**选项卡。
  注意：如果还为黑莓数据库连接选择了 Windows 集成，必须同时为此处指定的 Windows 帐户提供黑莓数据库访问权限。

5. 单击 **Test Connectivity**（测试连接）检查是否可以连接到 SQL Server，然后单击 **Save**（保存）。

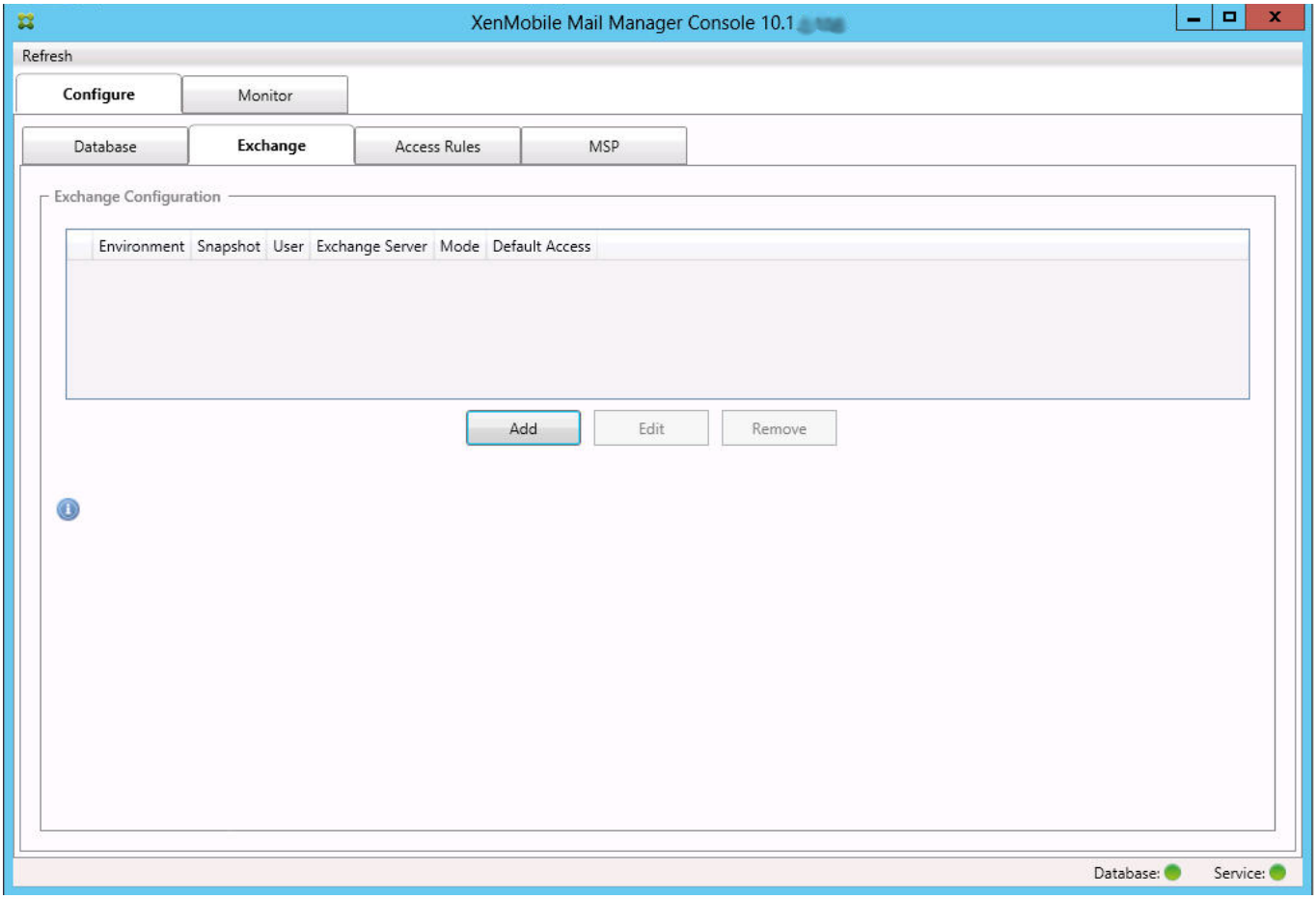


4. 此时将显示一条消息，提示您重新启动服务。 单击 **Yes**（是）。



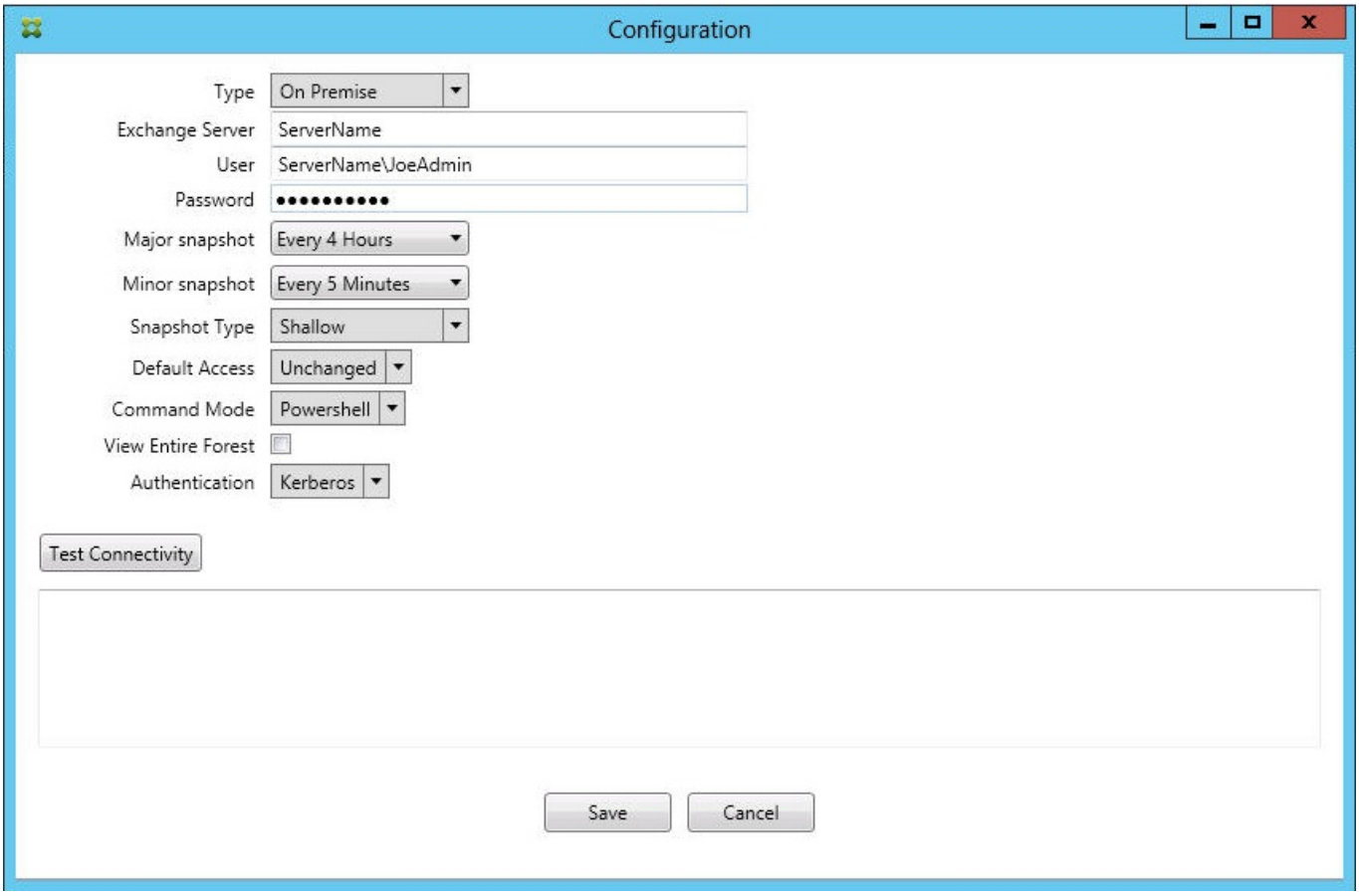
5. 配置一个或多个 Exchange Server：
   1. 如果管理单个 Exchange 环境，您仅需要指定一个服务器。 如果管理多个 Exchange 环境，您需要为每个 Exchange 环境指定一个 Exchange Server。
   2. 选择 **Configure（配置）> Exchange 选项卡**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 单击 **Add**（添加）。
4. 选择 Exchange Server 环境的类型：**On Premise**（本地）或 **Office 365**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

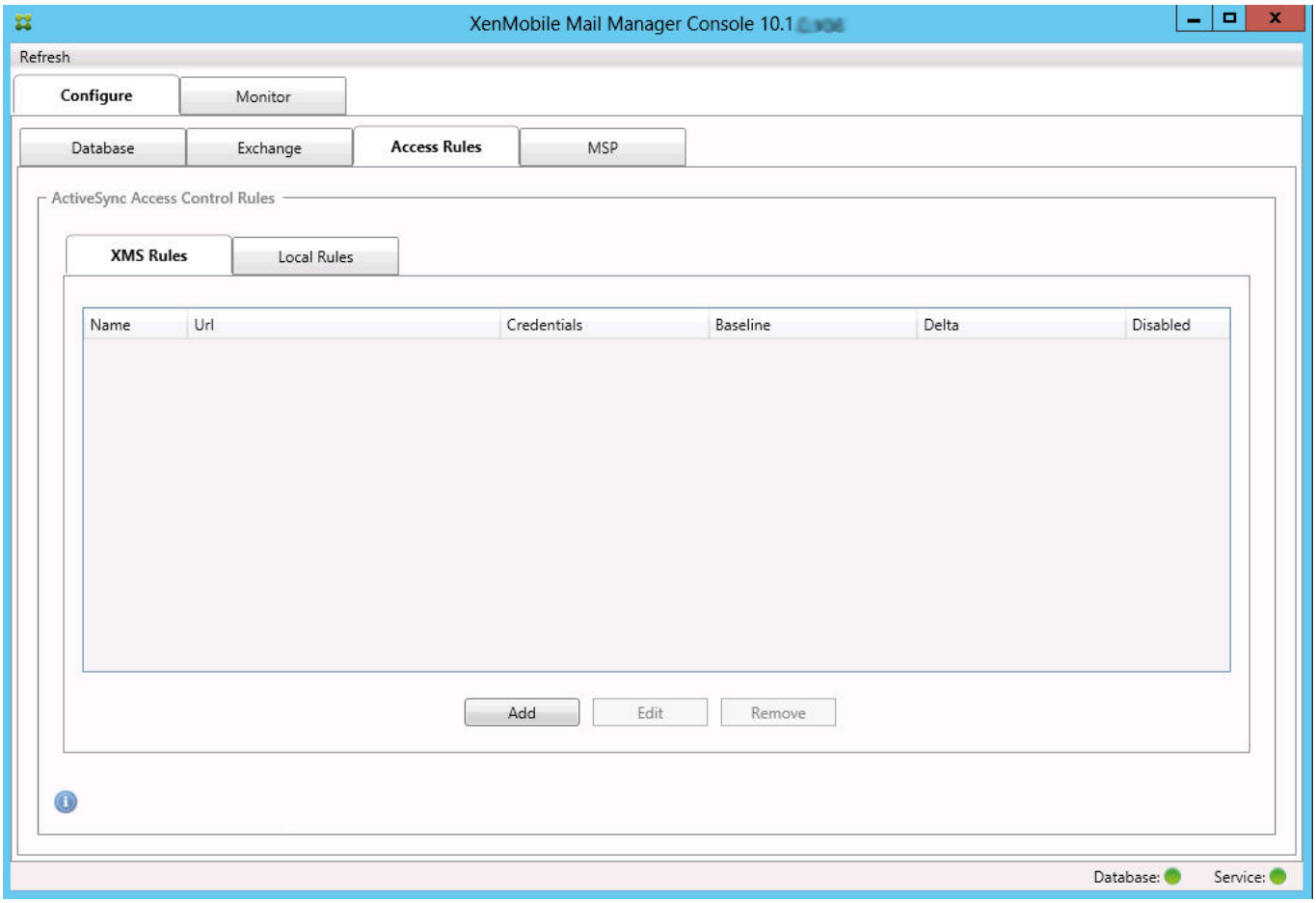


5. 如果选择 **On Premise**（本地），请输入要用于远程 PowerShell 命令的 Exchange Server 名称。
6. 输入在要求部分中指定的 Exchange Server 上具有适当权限的 Windows 身份的用户名。
7. 输入用户的 **Password**（密码）。
8. 选择运行主要快照的计划。 主要快照检测每个 Exchange ActiveSync 合作关系。
9. 选择运行次要快照的计划。 次要快照检测新创建的 Exchange ActiveSync 合作关系。
10. 选择快照类型：**Deep**（深层）或 **Shallow**（浅表）。 浅表快照通常更快并且足以执行 XenMobile Mail Manager 的所有 Exchange ActiveSync 访问控制功能。 深层快照可能需要花费更长时间，并且仅在为 ActiveSync 启用移动服务提供商（允许 XenMobile 查询未托管的设备）后才需要。
11. 选择“Default Access”（默认访问）：**Allow**（允许）、**Block**（阻止）或 **Unchanged**（不更改）。 这会控制所有设备（除了由显式 XenMobile 或本地规则确定的设备）的处理方式。 如果选择“Allow”（允许），将允许 ActiveSync 访问所有此类设备；如果选择“Block”（阻止），将拒绝访问；如果选择“Unchanged”（不更改），将不做更改。
12. 选择 ActiveSync 命令模式：**PowerShell** 或 **Simulation**（模拟）。
    - 在 PowerShell 模式下，XenMobile Mail Manager 会发出 PowerShell 命令以执行所需的访问控制。
    - 在“Simulation”（模拟）模式下，XenMobile Mail Manager 不发出 PowerShell 命令，但是会将预期命令和预期结果记录到数据库中。 在“Simulation”（模拟）模式下，用户随后可使用“Monitor”（监视）选项卡查看启用 PowerShell 模式时会发生的情况。
13. 选择 **View Entire Forest**（查看整个林）可将 XenMobile Mail Manager 配置为查看 Exchange 环境中的整个 Active Directory 林。
14. 选择身份验证协议：**Kerberos** 或 **Basic**（基本）。 XenMobile Mail Manager 支持对本地部署进行“Basic”（基本）身份验证。 这将允许在 XenMobile Mail Manager 服务器不属于 Exchange Server 所在域的成员的情况下使用 XenMobile Mail Manager。
15. 单击 **Test Connectivity**（测试连接）检查是否可以连接到 Exchange Server，然后单击 **Save**（保存）。
16. 此时将显示一条消息，提示您重新启动服务。 单击 **Yes**（是）。

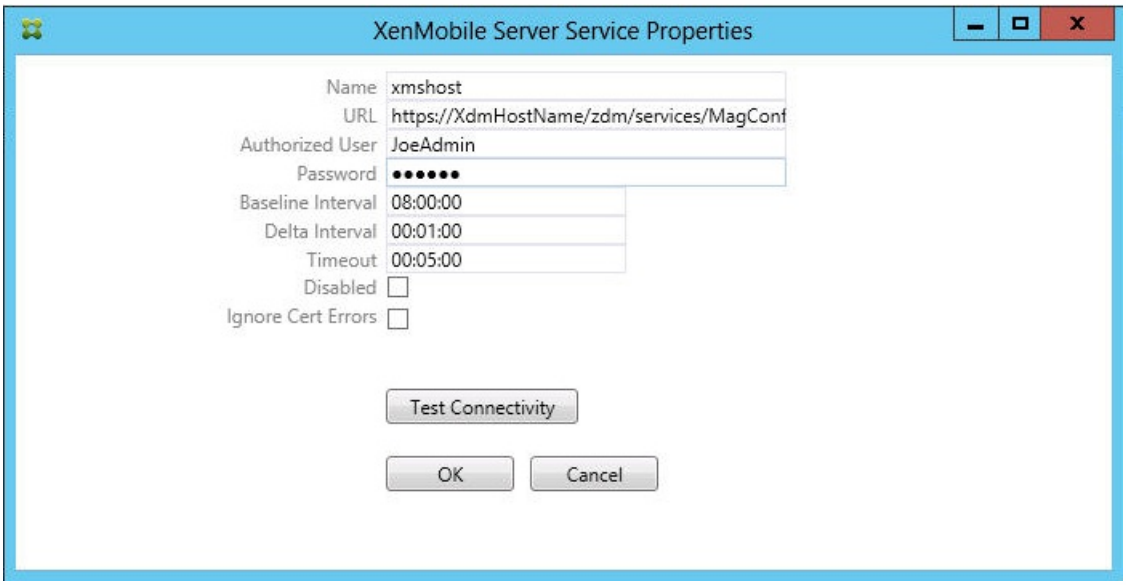
6. 配置访问规则：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 选择 **Configure**（配置）> **Access Rules**（访问规则）选项卡。
2. 单击 **XDM Rules**（XDM 规则）选项卡。



3. 单击 **Add**（添加）。

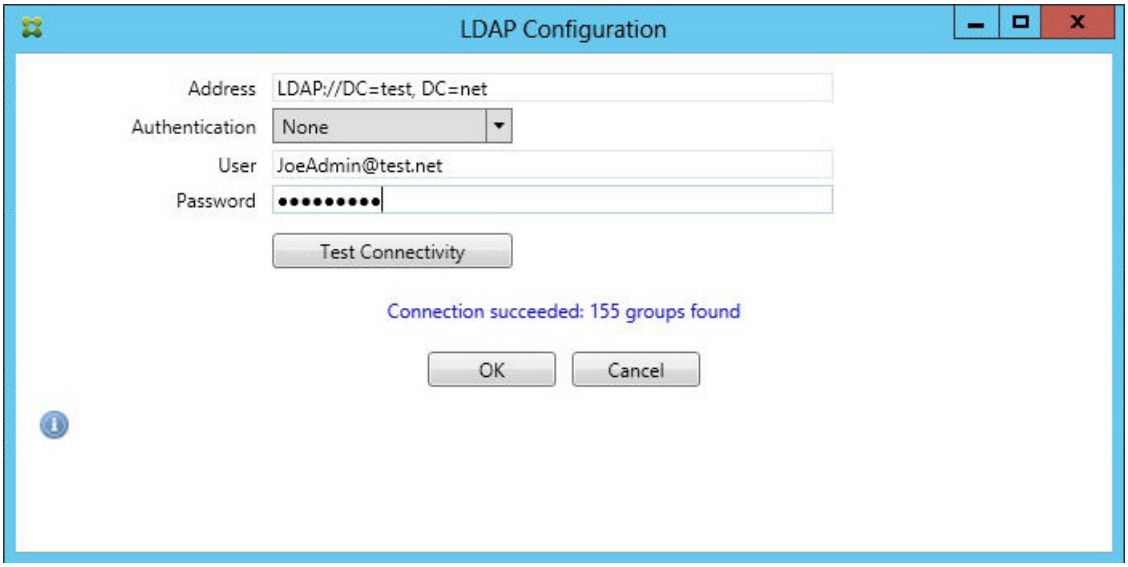


4. 输入 XenMobile 服务器规则的名称，例如 XdmHost。
5. 修改 URL 字符串以引用 XenMobile 服务器；例如，如果服务器名称为 XdmHost，输入 http://XdmHostName/zdm/services/MagConfigService。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 在该服务器上输入授权用户。
7. 输入用户密码。
8. 保留 **Baseline Interval**（基准时间间隔）、**Delta Interval**（增量时间间隔）和 **Timeout values**（超时值）的默认值。
9. 单击 **Test Connectivity**（测试连接），检查与服务器的连接。
   注意：如果选中“Disabled”（已禁用）复选框，XenMobile Mail Service 将不从 XenMobile 服务器收集策略。
10. 单击 **OK**（确定）。

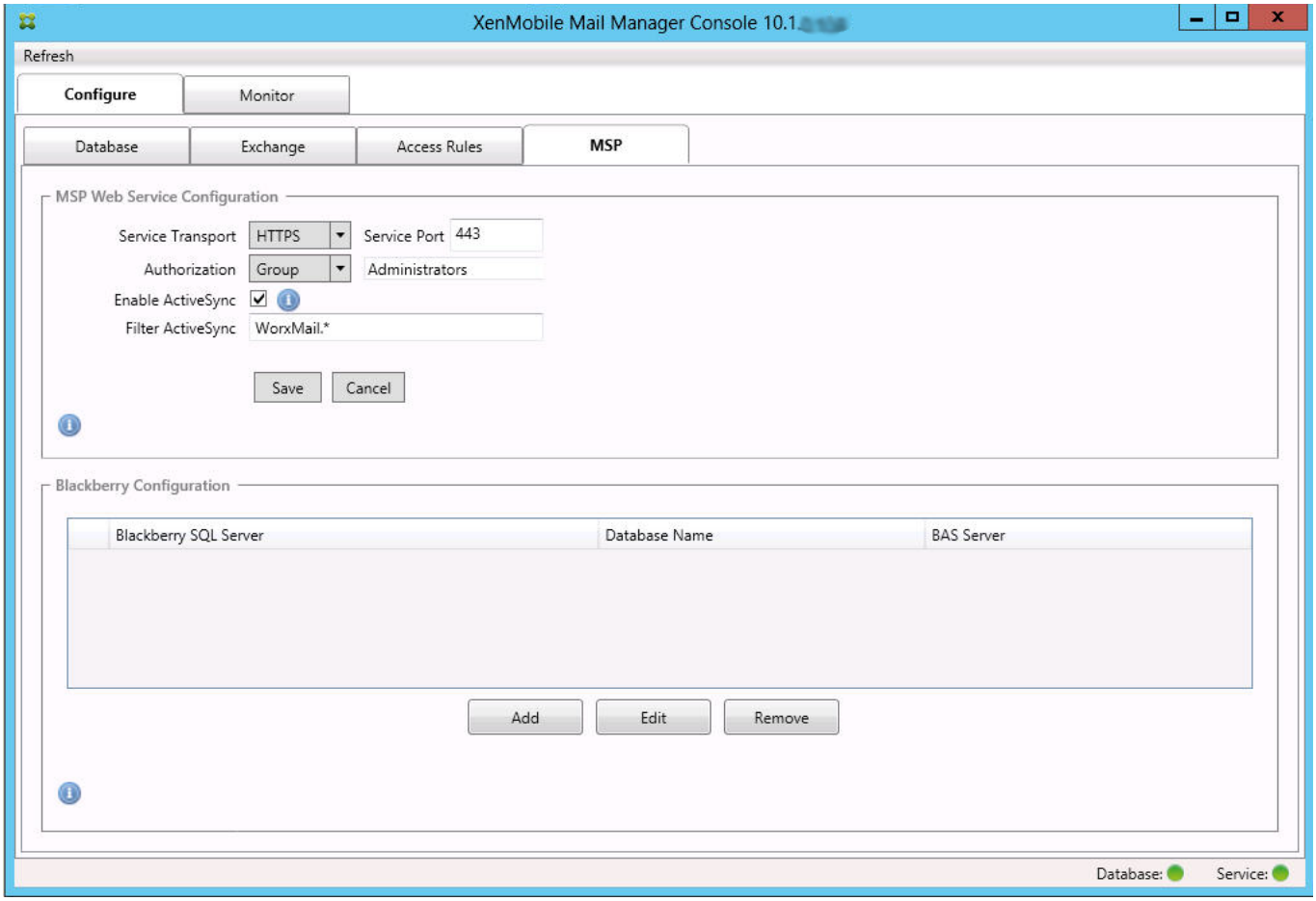
7. 单击 **Local Rules**（本地规则）选项卡。
   1. 如果要建立在 Active Directory 组中操作的本地规则，请单击 **Configure LDAP**（配置 LDAP），然后配置 LDAP 连接属性。



   2. 您可以基于 **ActiveSync Device ID**（ActiveSync 设备 ID）、**设备类型**、**AD Group**（AD 组）、**用户**或设备 **UserAgent**（用户代理）添加本地规则。 在列表中选择适当的类型。 有关详细信息，请参阅 XenMobile Mail Manager 访问控制规则。
   3. 在文本框中输入文本或文本片段。 也可单击查询按钮，查看与片段匹配的实体。
      注意：对于除 **Group**（组）以外的所有类型，系统依赖在快照中找到的设备。 因此，如果刚刚开始且尚未完成快照，则没有实体可用。
   4. 选择一个文本值，然后单击 **Allow**（允许）或 **Deny**（拒绝），将其添加到右侧的 **Rule List**（规则列表）窗格。 可以使用 **Rule List**（规则列表）窗格右侧的按钮改变规则的顺序或移除规则。 该顺序很重要，因为对于指定的用户和设备，将按照显示的顺序评估规则，并且一旦与较靠前的规则（离顶部较近）匹配，则后续的规则将失效。 例如，如果存在一条允许所有 iPad 设备的规则，而后续的规则阻止用户“Matt”，Matt 的 iPad 将仍被允许，因为“iPad”规则的有效优先级高于“Matt”规则。
   5. 要对规则列表中的规则进行分析以找到潜在的覆盖、冲突或补充结构，请单击 **Analyze**（分析）。
   6. 单击 **Save**（保存）。

8. 配置移动服务提供商。
   注意：移动服务提供商可选，仅当同时将 XenMobile 配置为使用移动服务提供商界面查询未托管的设备时必需。
   1. 选择 **Configure**（配置）> **MSP** 选项卡。

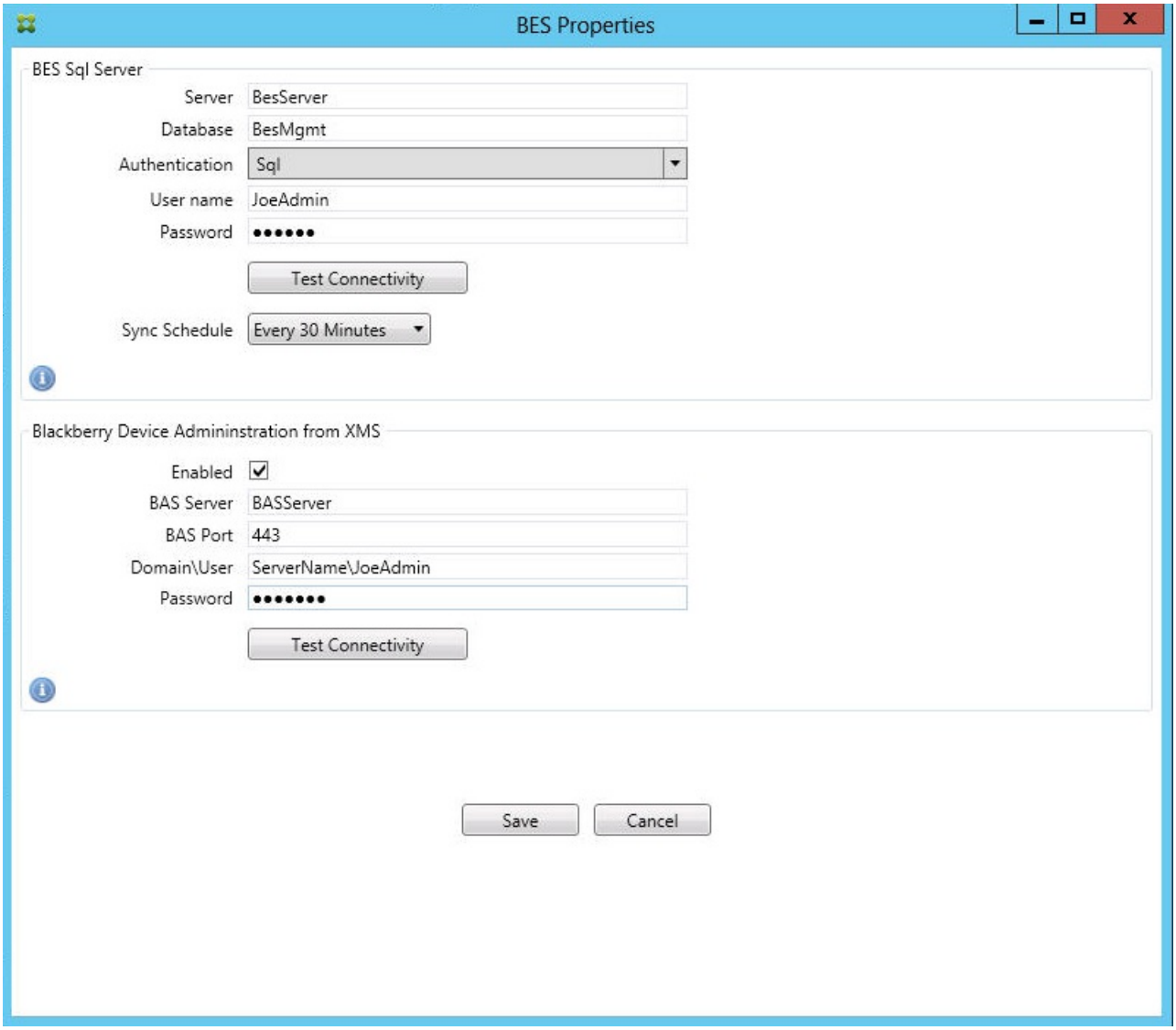
© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 将移动服务提供商服务的服务传输类型设置为 **HTTP** 或 **HTTPS**。
3. 为移动服务提供商服务设置服务端口（通常为 80 或 443）。
   注意：如果使用端口 443，该端口需要在 IIS 中绑定 SSL 证书。
4. 设置授权组或用户。 这样可以设定能够从 XenMobile 连接到移动服务提供商服务的用户或用户组。
5. 设置是否已启用 ActiveSync 查询。
   注意：如果为 XenMobile 服务器启用 ActiveSync 查询，必须将一个或多个 Exchange Server 的快照类型设置为 **Deep**（深层）；这样拍摄快照可能对性能造成很大损耗。
6. 默认情况下，不会将与正则表达式 WorxMail.* 匹配的 ActiveSync 设备发送到 XenMobile。 要更改此行为，请根据需要修改 **Filter ActiveSync**（过滤 ActiveSync）字段
   注意：空白意味着所有设备都将转发到 XenMobile。
7. 单击 **Save**（保存）。

9. 另外，可以配置一个或多个 BlackBerry Enterprise Server (BES)：
   1. 单击 **Add**（添加）。
   2. 输入 BES SQL Server 的服务器名称。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 输入 BES Management 数据库的数据库名称。
4. 选择身份验证模式。 如果选择 Windows 集成身份验证，则 XenMobile Mail Manager 服务的用户帐户就是用于连接 BES SQL Server 的帐户。
   注意：如果还为 XenMobile Mail Manager 数据库连接选择了 Windows 集成，则必须同时为此处指定的 Windows 帐户提供 XenMobile Mail Manager 数据库的访问权限。
5. 如果选择 **SQL authentication**（SQL 身份验证），请输入用户名和密码。
6. 设置 **Sync Schedule**（同步计划）。 这是用于连接到 BES SQL Server 并检查任何设备更新的计划。
7. 单击 **Test Connectivity**（测试连接），检查与 SQL 服务器的连接。
   注意：如果选择了 Windows 集成，则此测试使用当前登录的用户而非 XenMobile Mail Manager 服务用户，因此不能准确测试 SQL 身份验证。
8. 如果要支持 XenMobile 中的黑莓设备的远程擦除和/或重置密码功能，请选中 **Enabled**（已启用）复选框。
   1. 输入 BES 完全限定的域名 (FQDN)。
   2. 输入用于管理员 Web 服务的 BES 端口。
   3. 输入 BES 服务所需的完全限定用户和密码。
   4. 单击 **Test Connectivity**（测试连接），测试与 BES 的连接。
   5. 单击 **Save**（保存）。

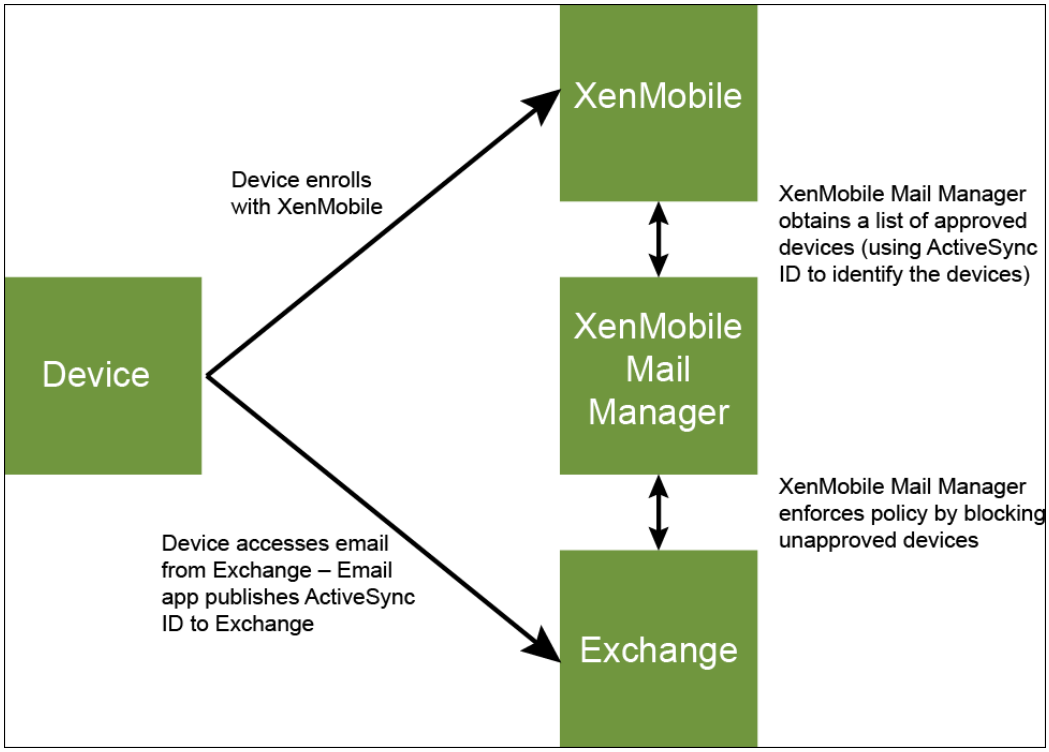
© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用 ActiveSync ID 强制执行电子邮件策略

Aug 11, 2016

您的企业电子邮件策略可以规定不批准特定设备使用企业电子邮件。 为与此策略保持一致，您希望确保员工无法通过此类设备访问企业电子邮件。 XenMobile Mail Manager 与 XenMobile 结合使用可强制实施此类电子邮件策略。 XenMobile 设置用于企业电子邮件访问的策略，当未经批准的设备向 XenMobile 注册时，XenMobile Mail Manager 会强制实施此策略。

设备上的电子邮件客户端使用设备 ID（也称为 ActiveSync ID，用于唯一标识设备）向 Exchange Server（或 Office 365）广播自己。 Worx Home 获取类似的标识符，并在注册设备时将标识符发送给 XenMobile。 通过比较两个设备 ID，XenMobile Mail Manager 可以确定特定设备是否应该获取企业电子邮件访问权限。 下图说明了此概念：



如果 XenMobile 向 XenMobile Mail Manager 发送的 ActiveSync ID 不同于设备向 Exchange 发布的 ID，XenMobile Mail Manager 无法指示 Exchange 如何处理此设备。

匹配 ActiveSync ID 可以在大多数平台上可靠地执行；但是，Citrix 已发现在某些 Android 实现上，来自设备的 ActiveSync ID 不同于邮件客户端向 Exchange 广播的 ID。 为缓解此问题，可以执行以下操作：

- 在 Samsung SAFE 平台上，从 XenMobile 推送设备 ActiveSync 配置。
- 在所有其他 Android 平台上，从 XenMobile 推送 Touchdown 应用程序和 Touchdown ActiveSync 配置。

但是，此方法不阻止员工在 Android 设备上安装除 Touchdown 之外的电子邮件客户端。 要保证正确地强制实施企业电子邮件访问策略，可以采用防御性安全措施，通过将静态策略设置为默认拒绝，将 XenMobile Mail Manager 配置为阻止电子邮件。 这意味着，如果员工确实在 Android 设备上配置了除 Touchdown 之外的电子邮件客户端，并且如果 ActiveSync ID 检测不能正常工作，将拒绝员工访问企业电子邮件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

访问控制规则

Oct 21, 2016

XenMobile Mail Manager 提供了一种基于规则的方法，为 Exchange ActiveSync 设备动态配置访问控制。 XenMobile Mail Manager 访问控制规则由两部分组成，即一个匹配的表达式和一个所需的访问状态（“允许”或“阻止”）。 规则可能会针对给定的 Exchange ActiveSync 设备进行评估，以确定该规则是否适用于该设备或是否与该设备匹配。 有多种匹配的表达式；例如，一条规则可能与给定“设备类型”（或特定 Exchange ActiveSync 设备 ID）的所有设备或者特定用户的所有设备等匹配。
在规则列表中添加、删除和重新排列规则期间，可以随时单击**取消**按钮将规则列表恢复为其首次打开时的状态。 除非单击**保存**，否则关闭配置工具时会丢失您对此窗口所做的任何更改。

XenMobile Mail Manager 有三种类型的规则，即本地规则、XenMobile 服务器规则（也称为 XDM 规则）和默认访问规则。

本地规则。 本地规则的优先级最高：如果设备与本地规则匹配，规则评估将停止。 既不查询 XenMobile 服务器规则，也不查询默认访问规则。 通过 Configure>Access Rules>Local Rules（配置>访问规则>本地规则）选项卡在本地配置 XenMobile Mail Manager 的本地规则。 支持匹配基于给定的 Active Directory 组内用户的成员身份。 支持匹配基于以下字段的正则表达式：

- Active Sync Device ID（Active Sync 设备 ID）
- ActiveSync Device Type（ActiveSync 设备类型）
- User Principal Name (UPN)（用户主体名称(UPN)）
- ActiveSync User Agent（ActiveSync 用户代理）（通常为设备平台或电子邮件客户端）

只要完成了主要快照并找到设备，您应能够添加常规或正则表达式规则。 如果尚未完成主要快照，则只能添加正则表达式规则。

XenMobile 服务器规则。 XenMobile 服务器规则是对提供托管设备相关规则的外部 XenMobile 服务器的引用。 XenMobile 服务器可通过自身的高级规则进行配置，这些规则可标识要基于 XenMobile 已知属性允许或阻止的设备（例如设备是否越狱或设备是否包含禁用的应用程序）。 XenMobile 评估高级规则并生成一组允许或阻止的 ActiveSync 设备 ID，然后将其传递到 XenMobile Mail Manager。

默认访问规则。 默认访问规则是唯一的，它可以潜在匹配每个设备，并且始终是最后一个被评估。 此规则是一条笼统的规则，这意味着如果给定的设备与本地规则或 XenMoble 服务器规则不匹配，该设备的所需访问状态将由默认访问规则的所需访问状态决定。

- Default Access – Allow（默认访问 - 允许）。 允许与本地规则或 XenMoble 服务器规则不匹配的任何设备。
- Default Access – Block（默认访问 - 阻止）。 阻止与本地规则或 XenMoble 服务器规则不匹配的任何设备。
- Default Access - Unchanged（默认访问 - 未更改）。 与本地规则或 XenMoble 服务器规则不匹配的任何设备将不会由 XenMobile Mail Manager 以任何方式修改其访问状态。 如果设备已被 Exchange 置于隔离模式，则不会采取任何措施；例如，从隔离模式删除设备的唯一方法是使用显式本地规则或 XDM 规则覆盖隔离。

关于规则评估

对于 Exchange 向 XenMobile Mail Manager 报告的每个设备，将按照优先级从最高到最低的顺序对这些规则进行评估，如下所示：

- 本地规则
- 默认访问规则
- XenMobile 服务器规则

找到匹配项时，评估将停止。 例如，如果本地规则与给定设备匹配，则不会根据任何 XenMobile 服务器规则或默认访问规则

© 1999-2017 Citrix Systems, Inc. All rights reserved.

对该设备进行评估。 这同样适用于给定的规则类型。 例如，如果某个给定设备在本地规则列表中有多个匹配项，则只要遇到第一个匹配项，评估即停止。

当设备属性发生变化、添加或删除设备或者规则本身发生变化时，XenMobile Mail Manager 会重新评估当前定义的规则集合。 主要快照以可配置的时间间隔选取设备属性更改和删除操作。 次要快照以可配置的时间间隔选取新设备。

Exchange ActiveSync 还具有控制访问的规则。 了解这些规则如何在 XenMobile Mail Manager 环境下运行非常重要。 Exchange 可能通过以下三种级别的规则进行配置：个人免除、设备规则以及组织设置。 XenMobile Mail Manager 通过以编程方式发出远程 PowerShell 请求来自动化访问控制，以影响个人免除列表。 这些是与给定邮箱关联的允许和阻止的 Exchange ActiveSync 设备 ID 列表。 部署后，XenMobile Mail Manager 有效地接替了 Exchange 中的免除列表的管理。 有关详细信息，请参阅此 Microsoft 文章。

在为相同的字段定义了多条规则的情况下，分析特别有用。 您可以对规则之间的关系进行故障排除。 请从规则字段的角度来执行分析；例如，规则是在组中基于匹配的字段进行分析的（例如 ActiveSync 设备 ID、ActiveSync 设备类型、用户、用户代理等）。

规则术语：

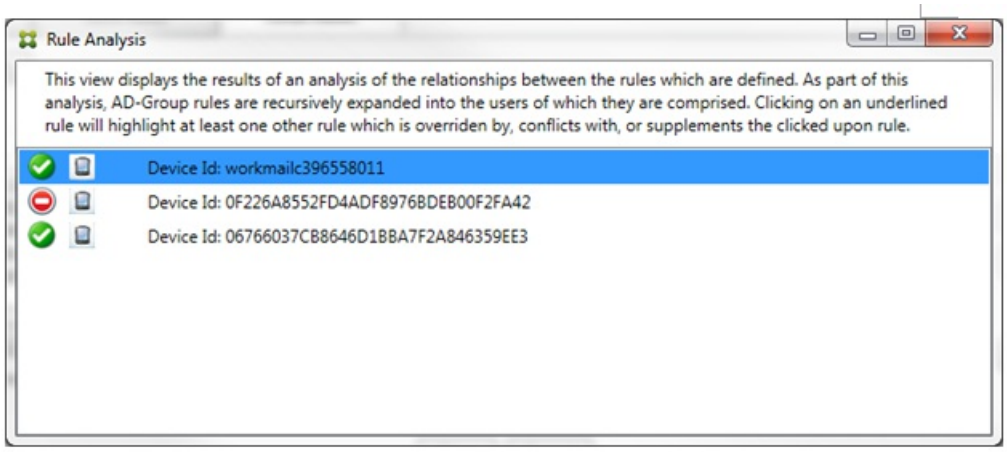
- **覆盖规则**。 当多条规则可以应用到同一设备时会发生覆盖。 因为规则是按照列表中的优先级进行评估的，可能会应用的后面的规则实例可能永远不会被评估。
- **冲突规则**。 当多条规则可以应用到同一设备但访问状态（允许/阻止）不匹配时会发生冲突。 如果冲突规则不是正则表达式规则，冲突将始终隐式包含覆盖
- **补充规则**。 当多条规则是正则表达式规则时会发生补充，因此可能需要确保两个（或多个）正则表达式可以合并为一个正则表达式，或者不复制功能。 补充规则的访问状态（允许/阻止）可能还会发生冲突。
- **主要规则**。 主要规则是已在对话框内单击的规则。 规则通过围绕它的实线框可视化地指示出来。 该规则还将具有一个或两个绿色箭头，用来指示向上或向下方向。 如果箭头指向上方，该箭头指示辅助规则在主要规则前面。 如果箭头指向下方，该箭头指示辅助规则在主要规则后面。 只有一个主要规则可以随时处于活动状态。
- **辅助规则**。 辅助规则以某种方式与主要规则相关（通过覆盖、冲突或补充关系）。 规则通过围绕它的虚线框可视化地指示出来。 对于每条主要规则，可以一条主要规则对应多条辅助规则。 单击任何带有下划线的条目时，始终从主要规则的角度突出显示一条或多条辅助规则。 例如，辅助规则将被主要规则覆盖，和/或辅助规则的访问状态将与主要规则冲突，和/或辅助规则将对主要规则进行补充。

“Rule Analysis”（规则分析）对话框中规则类型的界面外观

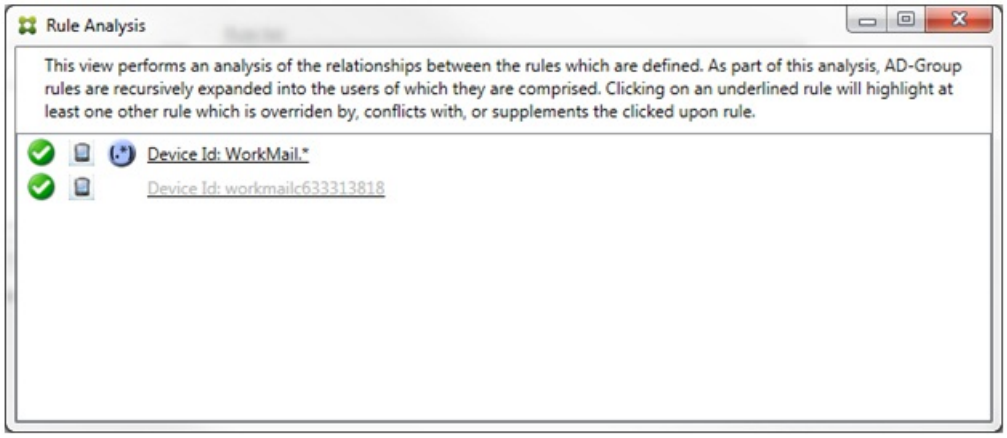
当没有冲突、覆盖或补充时，Rule Analysis （规则分析）对话框中不包含带有下划线的条目。 单击任何没有影响的项目；例如，正常选定项目的视觉效果将会出现。

“Rule Analysis”（规则分析）窗口包含一个复选框，选中该复选框时，将仅显示冲突、替代、冗余或增补规则。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

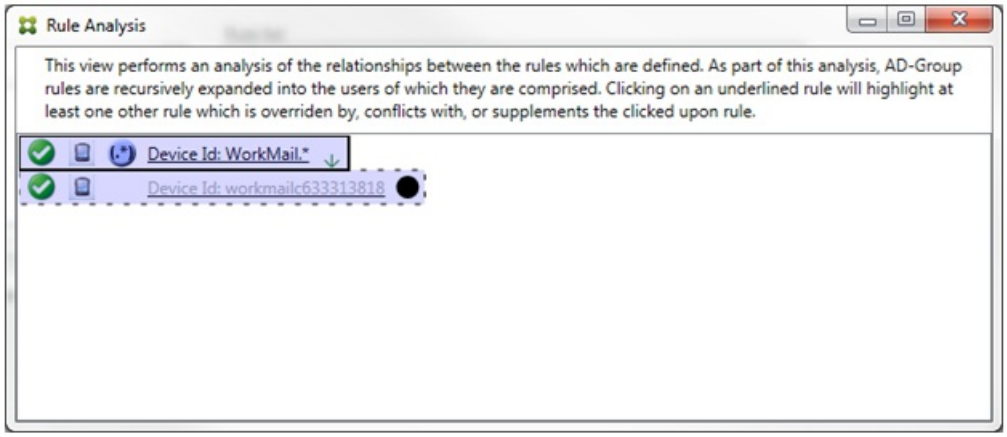


当出现覆盖时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。 至少有一条辅助规则将以较浅字体显示，指示该规则已被优先级较高的规则覆盖。 您可以单击覆盖的规则以了解覆盖该规则的一条或多条规则。 任何时间覆盖的规则都由于规则是主要规则或辅助规则而突出显示，并且将在它旁边将显示一个黑色圆圈，以进一步指示该规则处于不活动状态。 例如，在单击该规则之前，对话框显示如下：

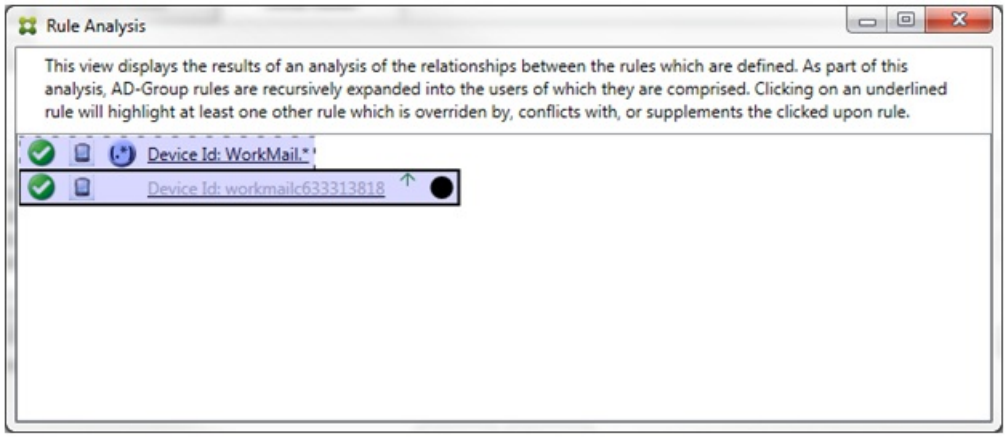


单击优先级最高的规则时，对话框显示如下：

© 1999-2017 Citrix Systems, Inc. All rights reserved.



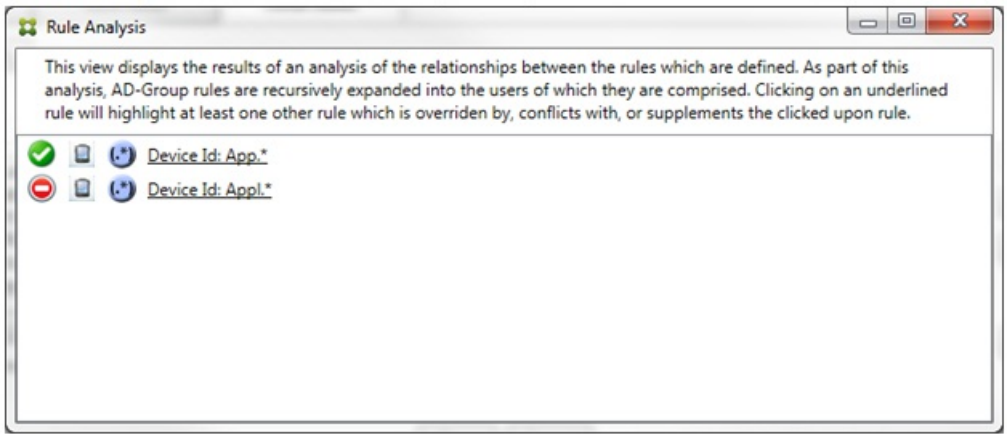
在此示例中，正则表达式规则 WorkMail.* 是主要规则（以实线框指示），常规规则 workmailc633313818 是辅助规则（以虚线框指示）。 辅助规则旁边的黑点是一个视觉提示，可进一步指示由于它的前面有较高优先级的正则表达式而处于不活动状态（永远不会被评估）。 单击覆盖的规则后，对话框显示如下：



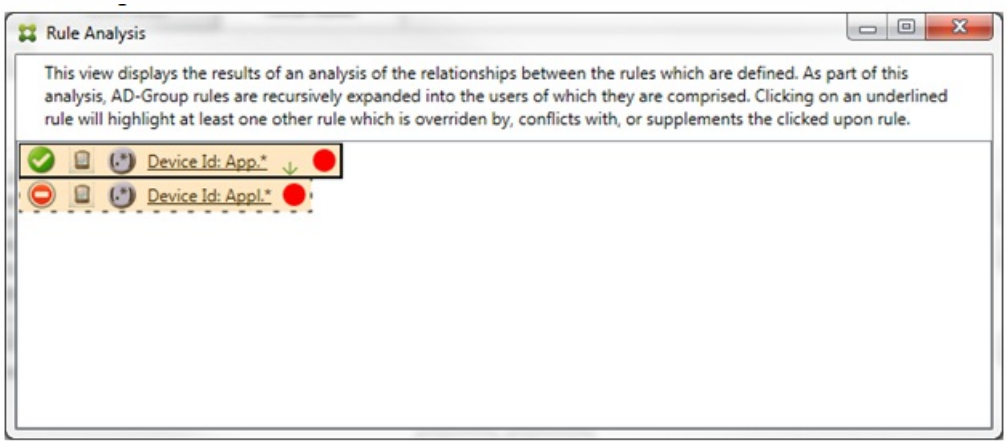
在上例中，正则表达式规则 WorkMail.* 是辅助规则（以虚线框指示），常规规则 workmailc633313818 是主要规则（以实线框指示）。 对于这一简单的示例，没有太大差异。 对于更为复杂的示例，请参阅本主题中后面所述的复杂表达式示例。 在定义了许多规则的情景中，单击覆盖的规则将快速识别已覆盖该规则的一条或多条规则。

当出现冲突时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。 发生冲突的规则用红点指示。 只有相互冲突的规则才可能定义了两条或多条正则表达式规则。 在所有其他冲突情景中，不仅将有冲突，而且还会发生覆盖。 在简单的示例中单击任一规则之前，对话框显示如下：

© 1999-2017 Citrix Systems, Inc. All rights reserved.



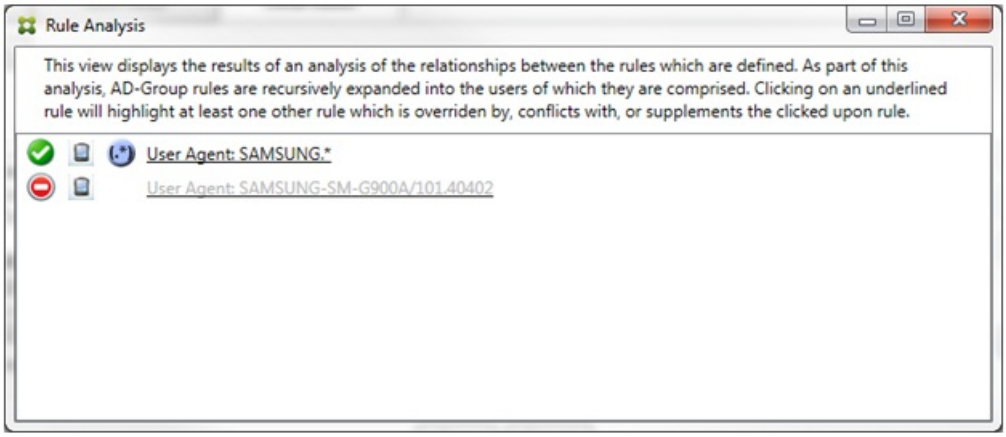
检查这两条正则表达式规则即可明显发现，第一条规则允许设备 ID 包含“App”的所有设备，第二条规则拒绝设备 ID 包含 Appl 的所有设备。 此外，即使第二条规则拒绝了设备 ID 包含 Appl 的所有设备，也不会拒绝符合条件的设备，因为允许规则的优先级较高。 单击第一条规则后，对话框显示如下：



在上述情景中，主要规则（正则表达式规则 App.*）和辅助规则（正则表达式规则 Appl.*）均以黄色突出显示。 这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

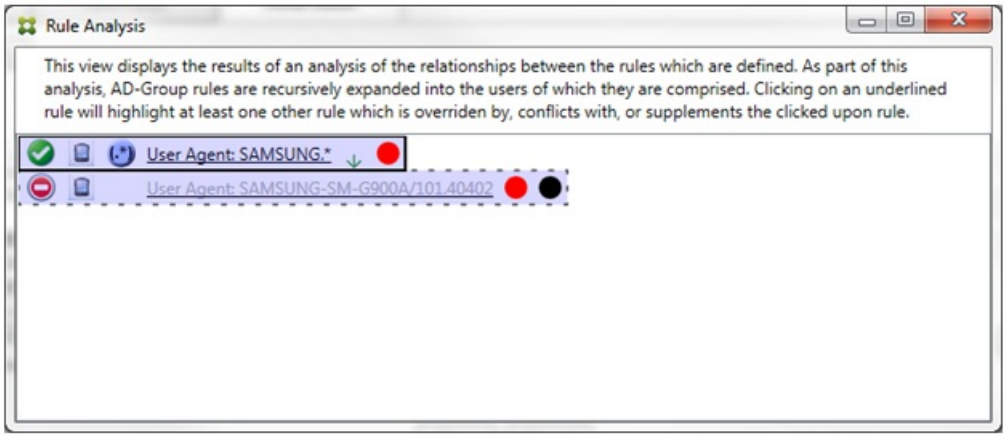
在同时存在冲突和覆盖的情景中，主要规则（正则表达式规则 App.*）和辅助规则（正则表达式规则 Appl.*）均以黄色突出显示。 这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在上例中，显而易见，第一条规则（正则表达式规则 SAMSUNG.*）不仅覆盖下一条规则（常规规则 SAMSUNG-SM-G900A/101.40402），而且这两条规则的访问状态有所不同（主要规则指定“允许”，辅助规则指定“阻止”）。 第二条规则（常规规则 SAMSUNG-SM-G900A/101.40402）以较浅文本显示，指示该规则已被覆盖，并因此处于不活动状态。

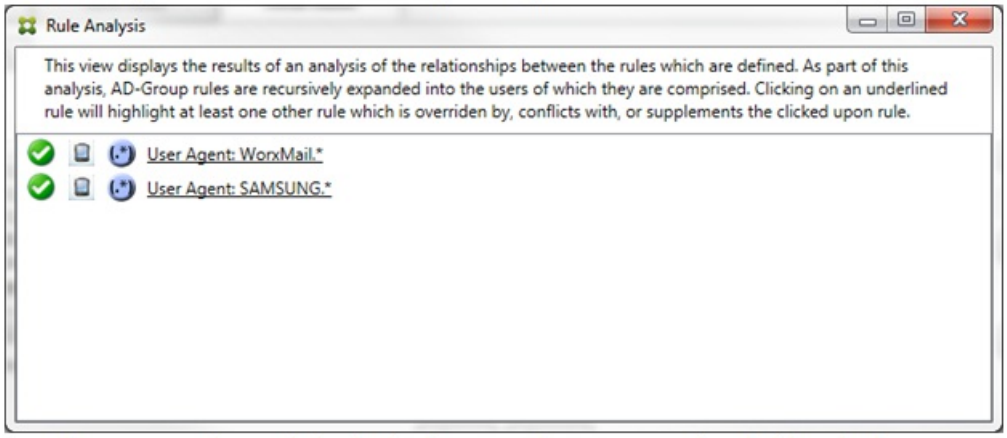
单击正则表达式规则后，对话框显示如下：



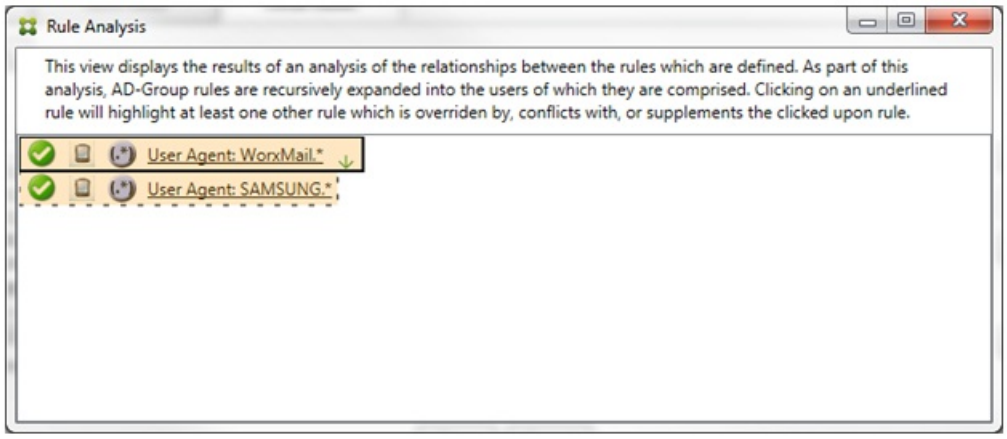
主要规则（正则表达式规则 SAMSUNG.*）后跟一个红点，指示其访问状态与一条或多条辅助规则发生冲突。 辅助规则（常规规则 SAMSUNG-SM-G900A/101.40402）后跟一个红点，指示其访问状态与主要规则发生冲突，以及如果后跟黑点，则进一步指示该规则已被覆盖，并因此处于不活动状态。

至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。 仅相互补充的规则将只涉及正则表达式规则。 当规则相互补充时，将以黄色叠加表示。 单击简单示例中的任一规则之前，对话框显示如下：

© 1999-2017 Citrix Systems, Inc. All rights reserved.



目测会很容易发现这两条规则都是正则表达式规则，都已应用到 XenMobile Mail Manager 中的 ActiveSync 设备 ID 字段。 单击第一条规则后，对话框显示如下：

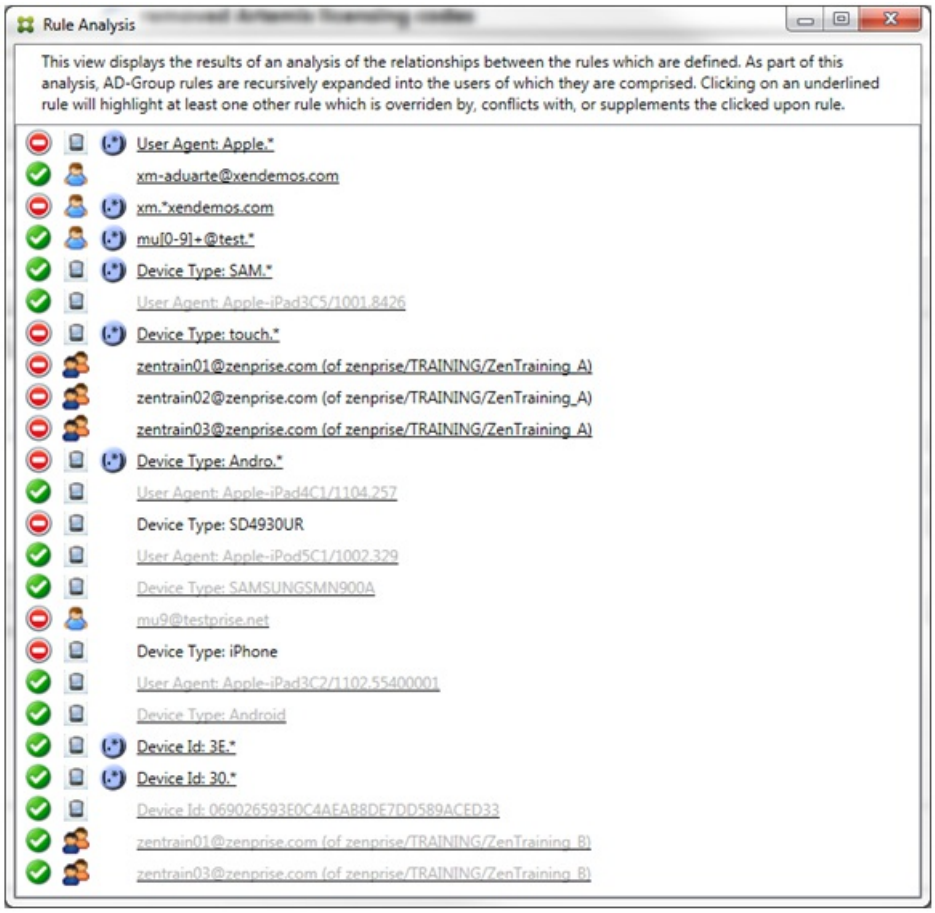


主要规则（正则表达式规则 WorxMail.*）以黄色叠加突出显示，指示至少存在一个是正则表达式的其他辅助规则。 辅助规则（正则表达式规则 SAMSUNG.*）以黄色叠加突出显示，指示辅助规则与主要规则都是要应用到 XenMobile Mail Manager 内同一字段的正则表达式规则；在此情况下，该字段为 ActiveSync 设备 ID 字段。这些正则表达式可能叠加，也可能不叠加。 是否正确制作正则表达式由您来决定。

复杂表达式示例

许多潜在的覆盖、冲突或补充都可能会发生，使其不可能举例说明所有可能的情景。 下例探讨了不会执行的操作，同时还阐明了规则分析视觉构建的强大功能。 大多数项目在下图中加了下划线。 许多项目以较浅的字体显示，指示存在问题的规则已被优先级较高的规则以某种方式覆盖。 多条正则表达式规则也包括在列表中，由 (.*) 图标指示。

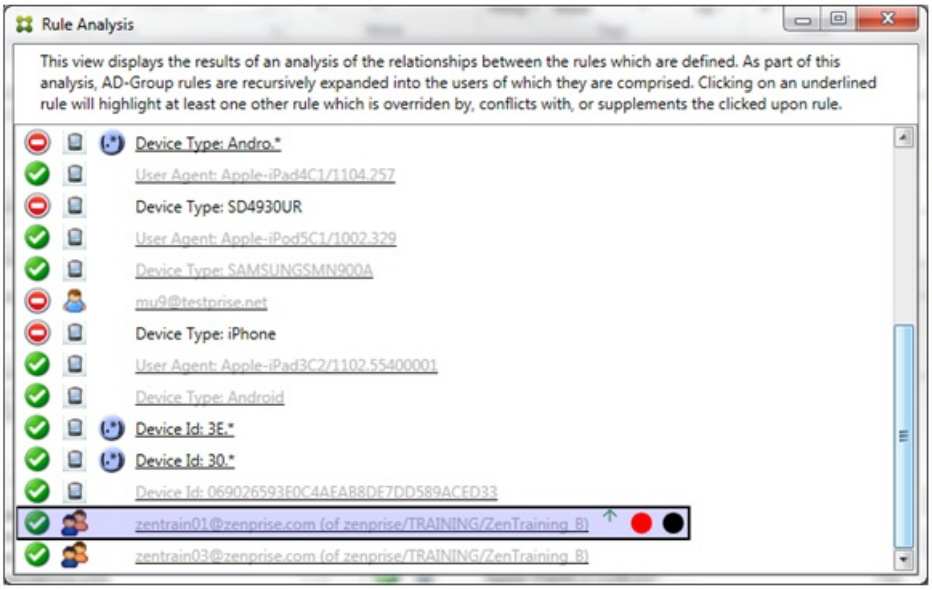
© 1999-2017 Citrix Systems, Inc. All rights reserved.



如何分析覆盖

要查看覆盖了特定规则的一条或多条规则，您可以单击该规则。

示例 1：本示例调查了覆盖 zentrain01@zenprise.com 的原因。

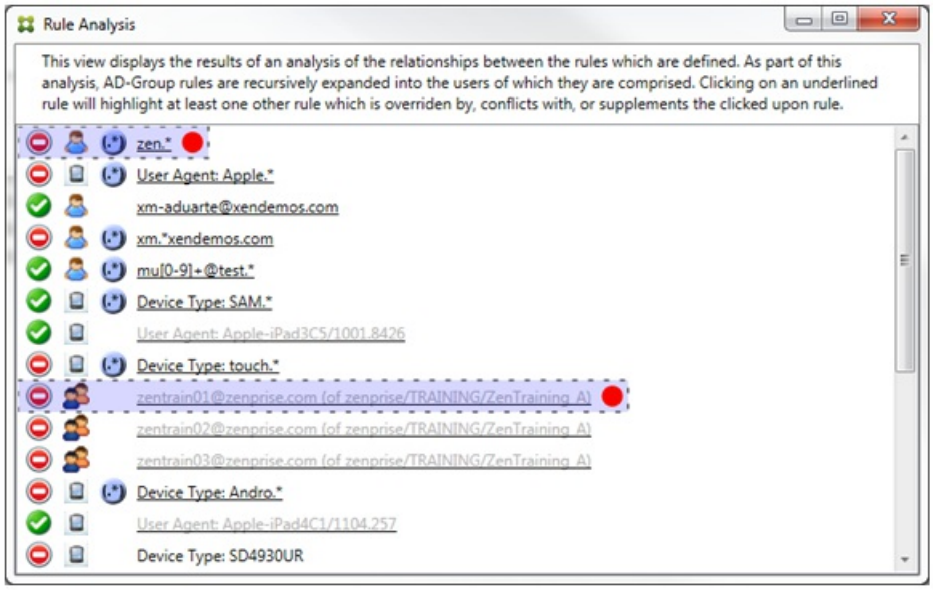


© 1999-2017 Citrix Systems, Inc. All rights reserved.

主要规则（AD-Group 规则 zenprise/TRAINING/ZenTraining B，zentrain01@zenprise.com 是其中的一个成员）具有以下特性：

- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示一条或多条辅助规则都能够在该箭头上方找到）。
- 后跟一个红色圆圈和一个黑色圆圈，分别指示一条或多条辅助规则与其访问状态存在冲突，并且主要规则已被覆盖且因此处于不活动状态。

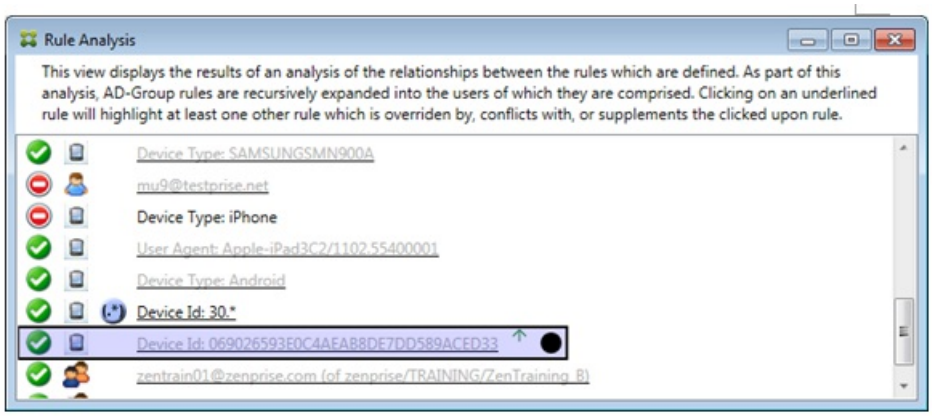
向上滚动时，您会看到以下内容：



在这种情况下，有两条辅助规则覆盖主要规则：正则表达式规则 zen.* 和常规规则 zentrain01@zenprise.com（属于 zenprise/TRAINING/ZenTraining A）。 对于后一条辅助规则，出现了以下情况：Active Directory 组规则 ZenTraining A 包含用户 zentrain01@zenprise.com，Active Directory 组规则 ZenTraining B 也包含用户 zentrain01@zenprise.com。 但是，由于辅助规则的优先级高于主要规则，因此主要规则被覆盖。 主要规则的访问状态是“允许”，并且由于这两条辅助规则的访问状态都是“阻止”，因此，后跟一个红色圆圈以进一步指示存在访问冲突。

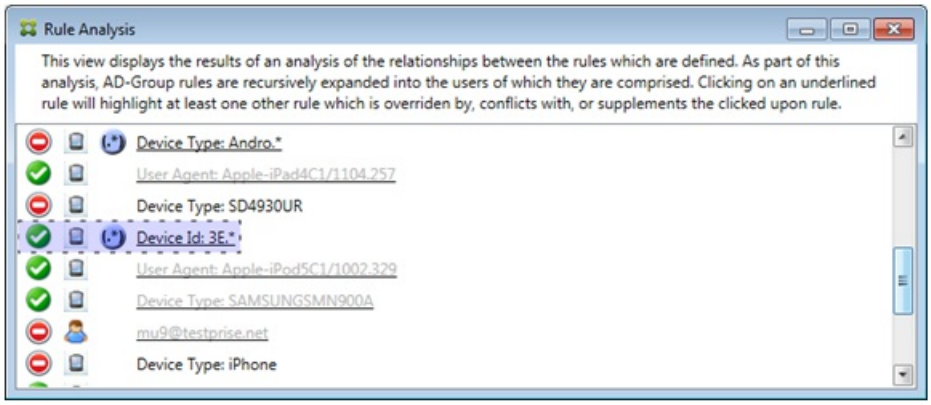
示例 2：此示例显示了覆盖 ActiveSync 设备 ID 为 069026593E0C4AEAB8DE7DD589ACED33 的设备的原因：

© 1999-2017 Citrix Systems, Inc. All rights reserved.



主要规则（常规设备 ID 规则 069026593E0C4AEAB8DE7DD589ACED33）具有以下特性：

- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示辅助规则能够在该箭头上方找到）。
- 后跟一个黑色圆圈，指示辅助规则已覆盖主要规则，并因此处于非活动状态。



在这种情况下：一条辅助规则将覆盖主要规则：正则表达式 ActiveSynce 设备 ID 规则 3E.*。由于正则表达式 3E.* 将与 069026593E0C4AEAB8DE7DD589ACED33 匹配，因此，主要规则永远不会被评估。

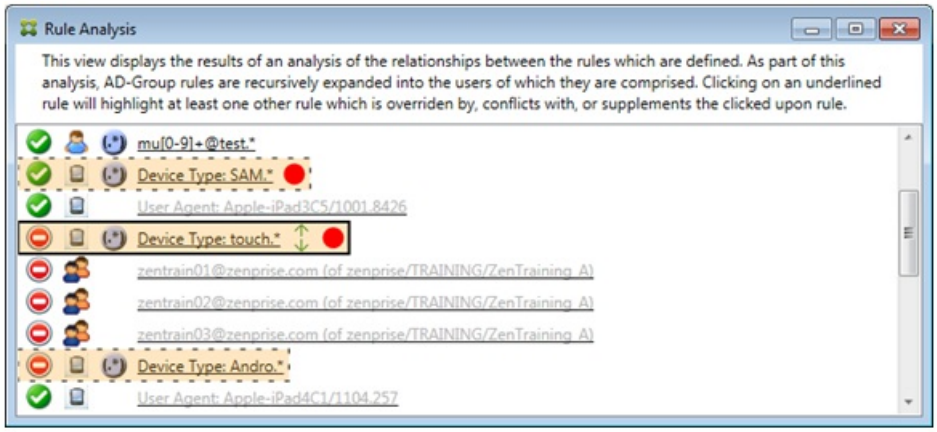
如何分析补充和冲突

在这种情况下，主要规则是正则表达式 ActiveSync 设备类型规则 touch.*。特性如下：

- 以实线框指示，并使用黄色叠加作为警告，提示正在针对特定规则字段运行多条正则表达式规则，在这种情况下为 ActiveSync 设备类型。
- 两个箭头分别指向上方和下方，指示至少存在一条具有较高优先级的辅助规则以及至少存在一条具有较低优先级的辅助规则。
- 箭头旁边的红色圆圈指示至少一条辅助规则的访问状态设置为“允许”，与主要规则的访问状态“阻止”相冲突
- 存在两条辅助规则，即正则表达式 ActiveSync 设备类型规则 SAM.* 和正则表达式 ActiveSync 设备类型规则 Andro.*
- 这两条辅助规则都加了虚线框，指示其属于辅助规则。
- 这两条辅助规则都以黄色叠加，指示其是对 ActiveSync 设备类型的规则字段的补充应用。

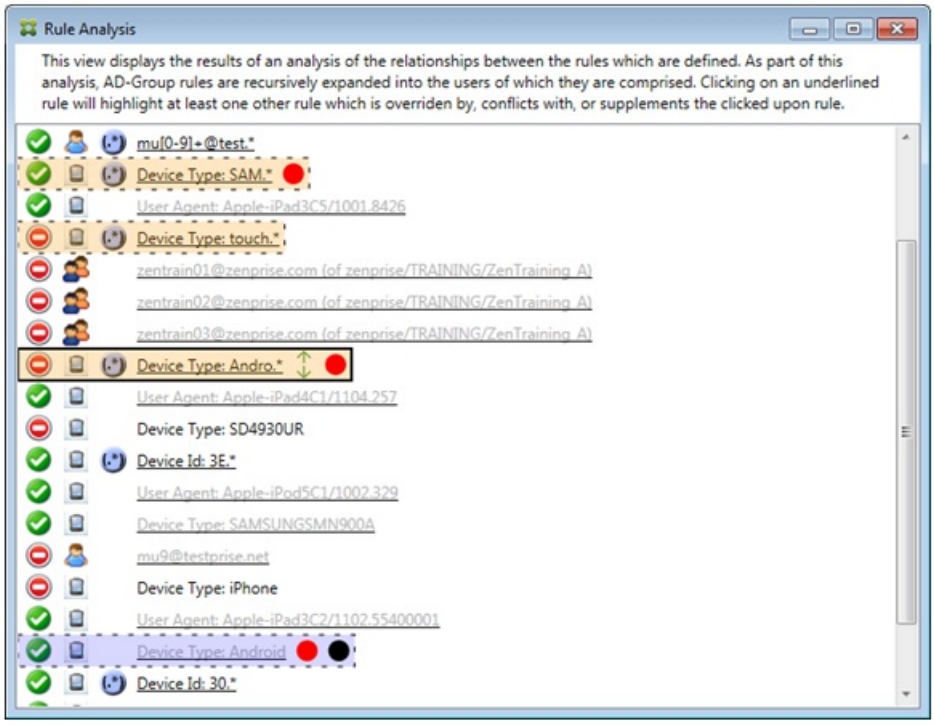
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在此类情景中，您应确保其正则表达式规则不冗余。



如何进一步分析规则

本示例探讨了规则关系如何始终从主要规则的角度建立。 上例显示了如何单击应用到设备类型值为 touch.* 的规则字段的正则表达式规则。单击辅助规则 Andro.* 将显示一组不同的辅助规则已突出显示。



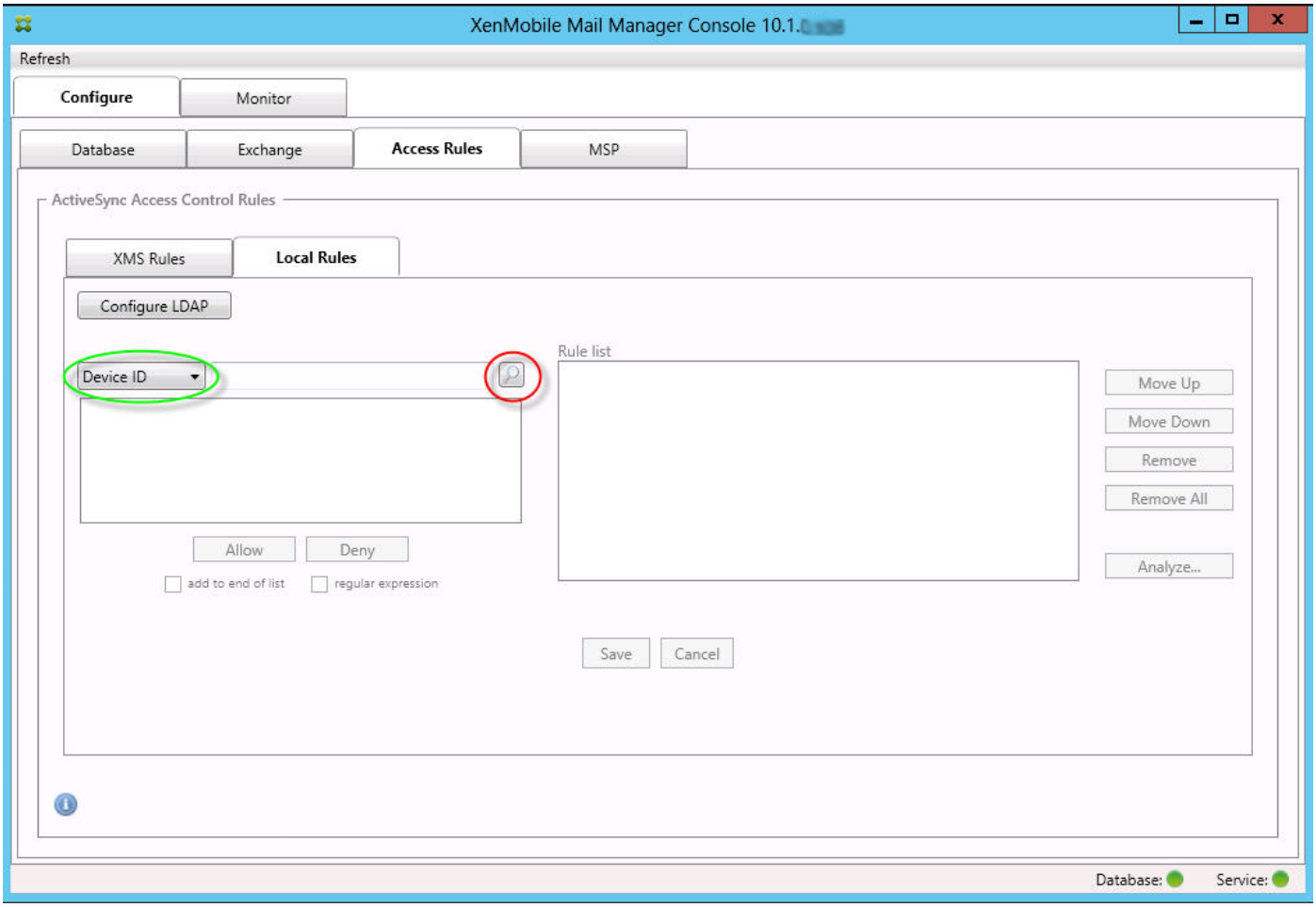
此示例显示了规则关系中包含的覆盖规则。 此规则是常规 ActiveSync 设备类型规则 Android，已被覆盖（通过旁边的浅色字体和黑色圆圈指示）并且其访问状态还与主要规则正则表达式 ActiveSync 设备类型规则 Andro.* 发生冲突；在单击该规则之前，该规则是辅助规则。 在上例中，常规 ActiveSync 设备类型规则 Android 未显示为辅助规则，因为从主要规则（正则表达式

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ActiveSync 设备类型规则 touch.*）的角度来看，该规则与主要规则不相关。

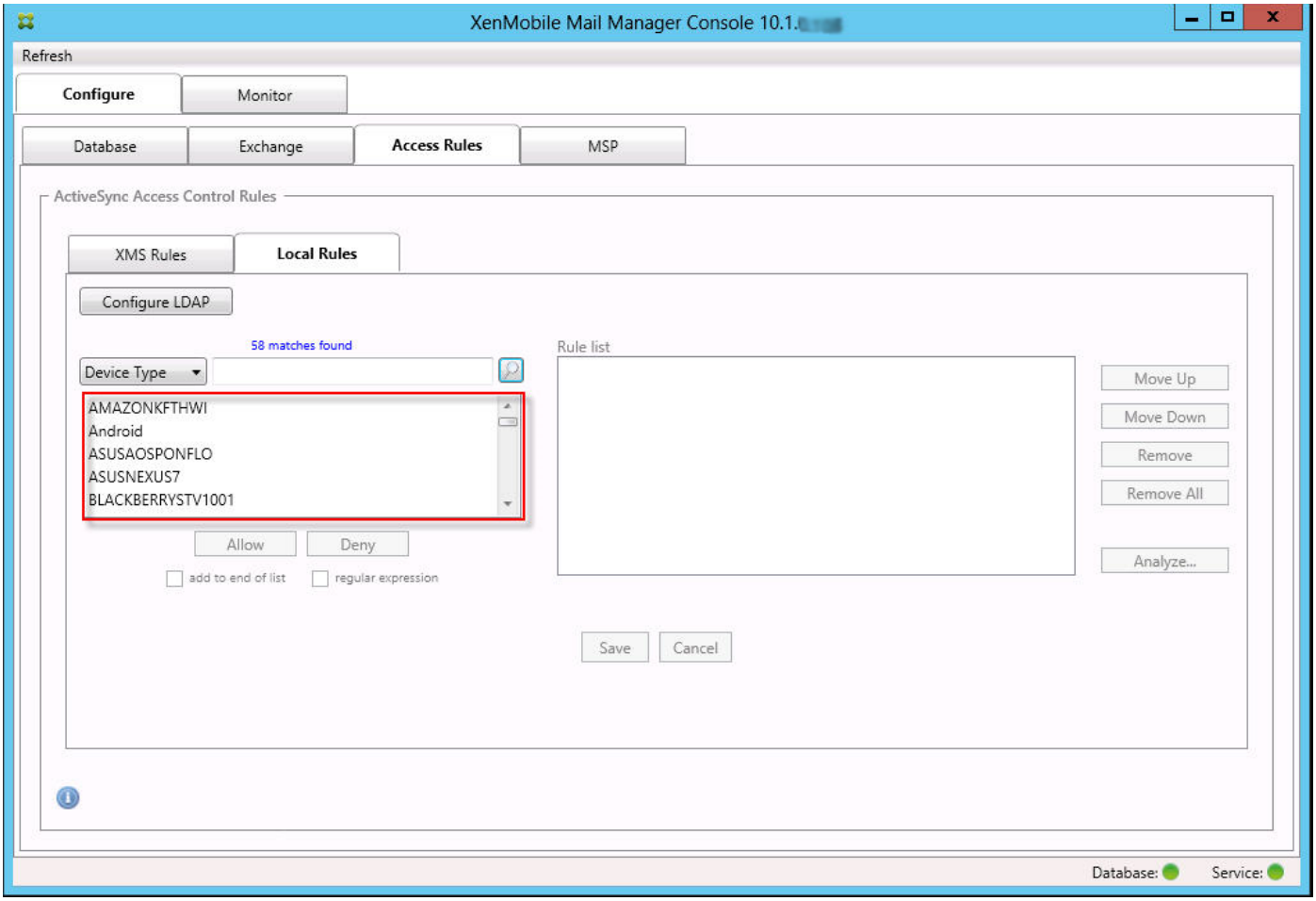
配置常规表达式本地规则

1. 单击 Access Rules（访问规则）选项卡。



2. 在设备 ID 列表中，选择要为其创建本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。 在此示例中，已选择设备类型字段，选项显示在下面的列表框中。

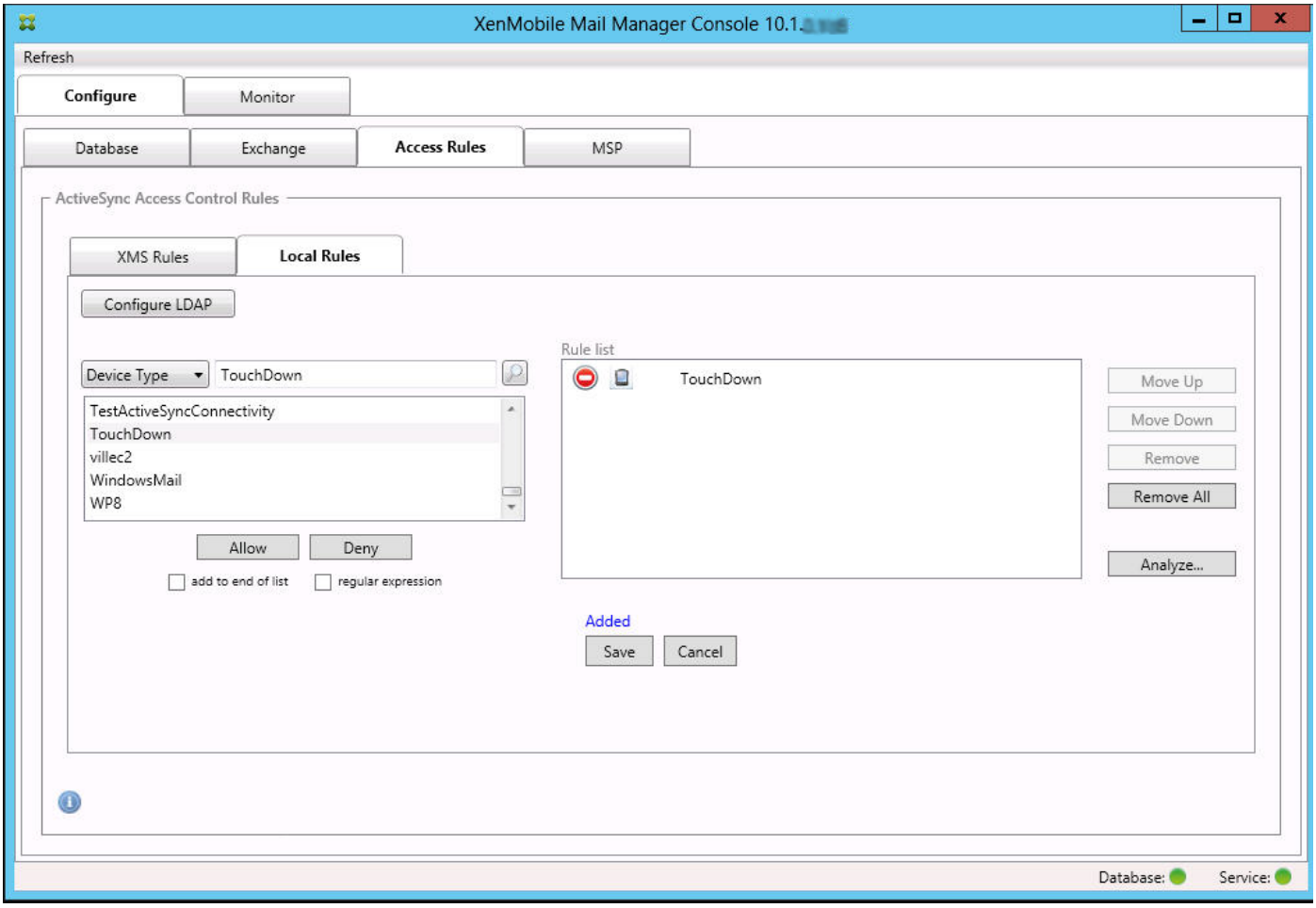
© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 在结果列表框中单击其中一个项目，然后单击以下选项之一：
   - 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 TouchDown 的所有设备将被拒绝访问。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



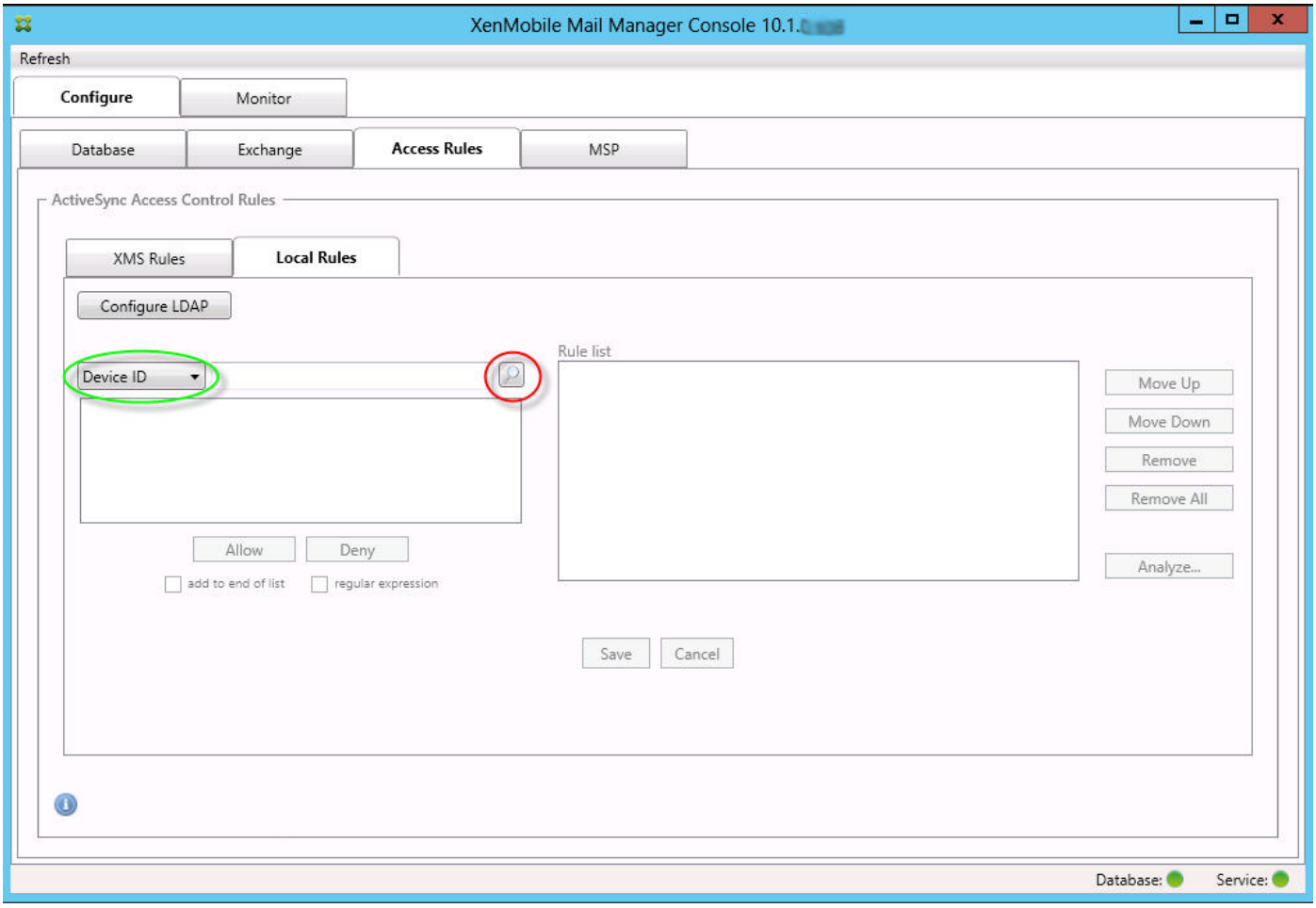
添加正则表达式

正则表达式本地规则可通过其旁边显示的图标进行区分 - (.*)。 要添加正则表达式规则，您可以通过给定字段的结果列表中的现有值来构建正则表达式规则（只要已完成主要快照），或只需键入您想要的正则表达式。

从现有字段值构建正则表达式

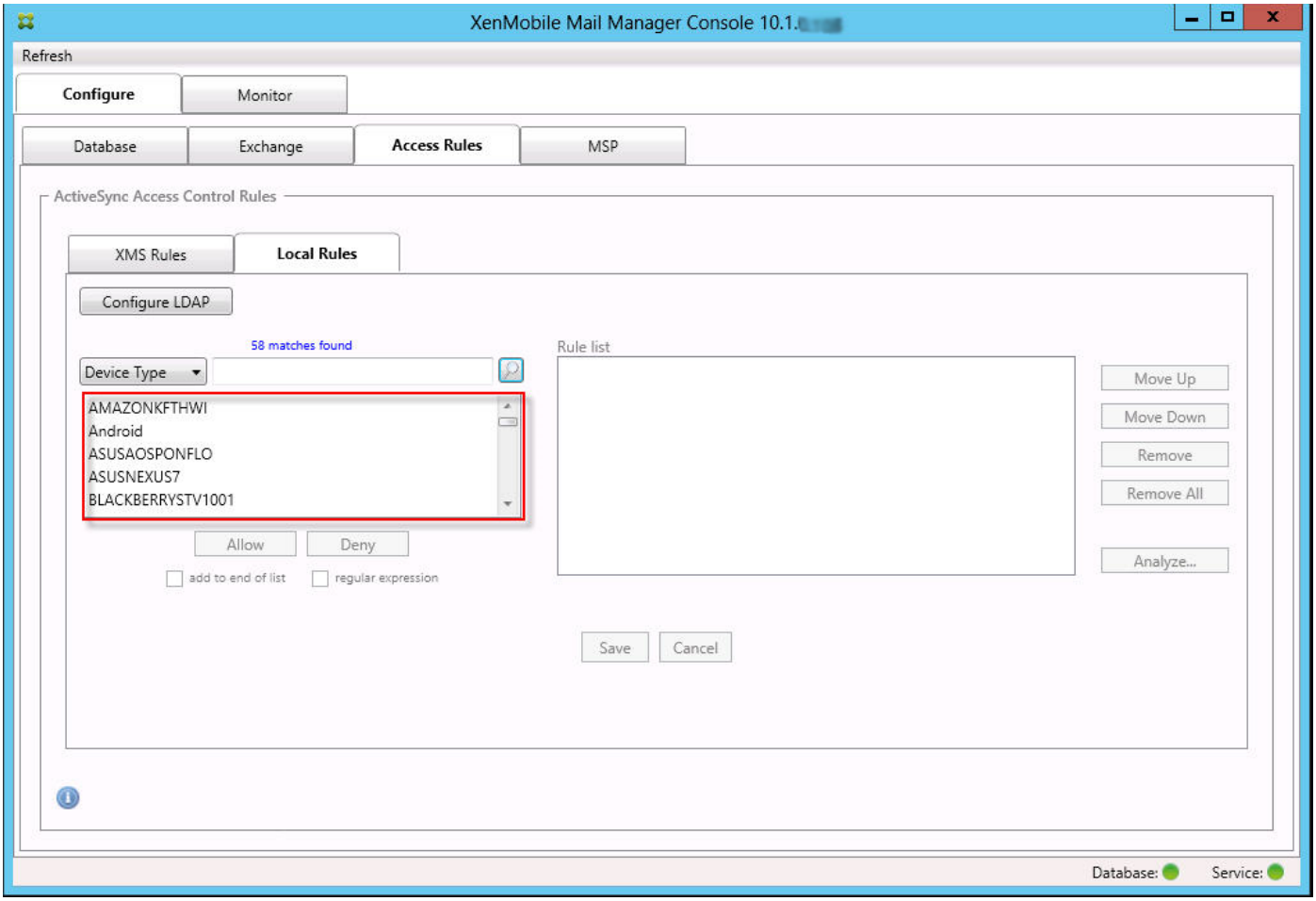
1. 单击 Access Rules（访问规则）选项卡。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



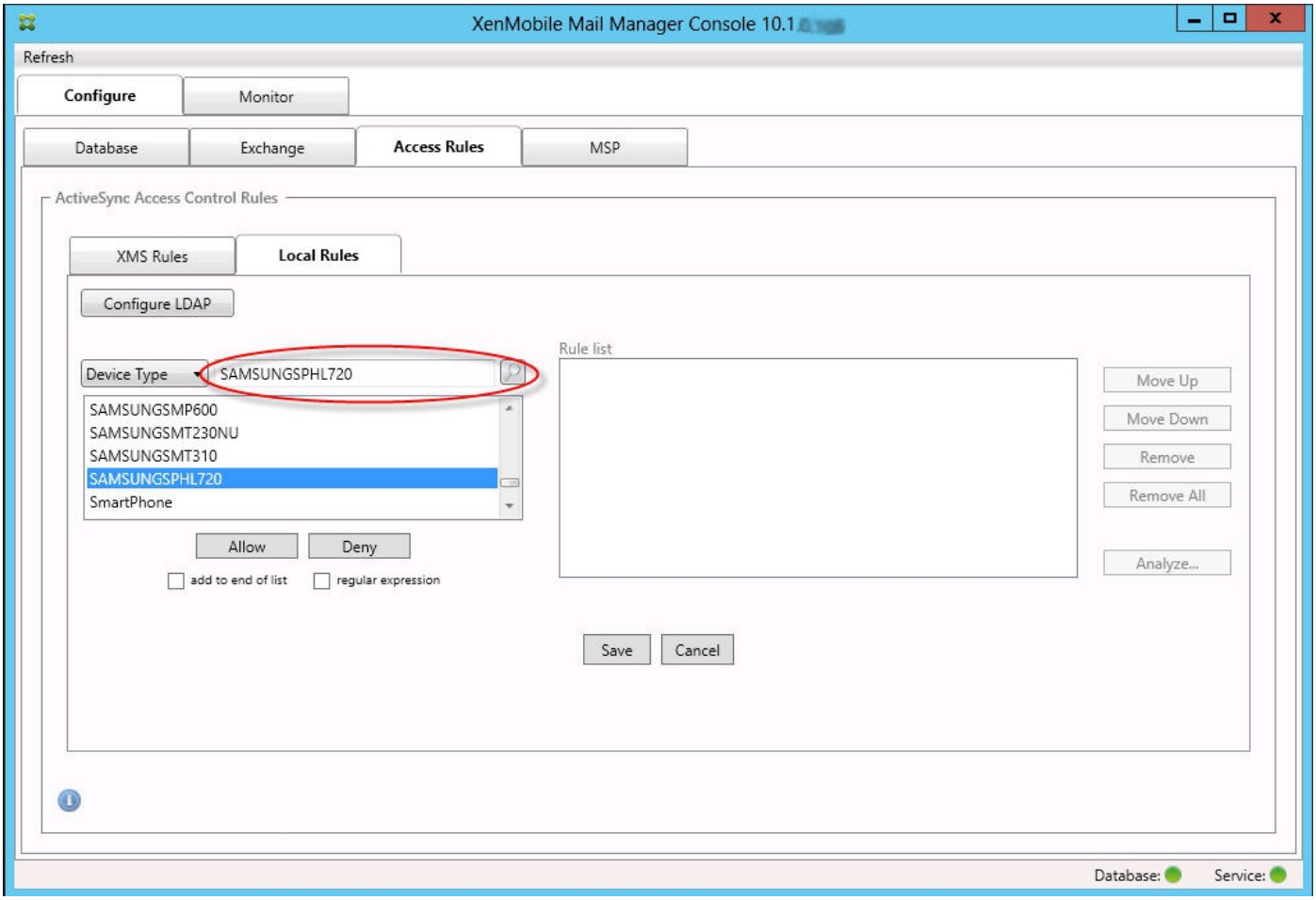
2. 在设备 ID 列表中，选择要为其创建正则表达式本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。 在此示例中，已选择设备类型字段，选项显示在下面的列表框中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



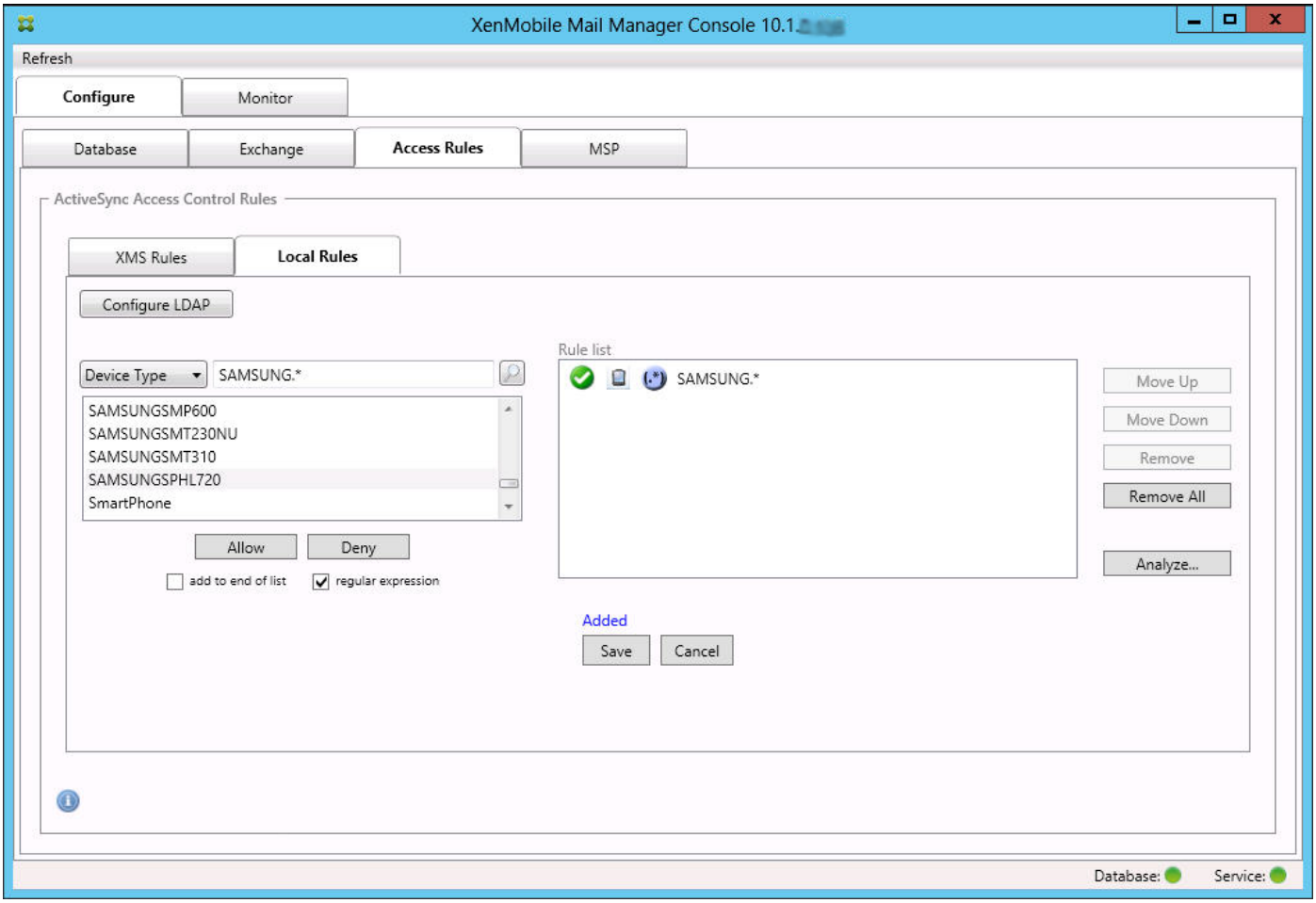
4. 单击结果列表中的其中一个项目。 在此示例中，已选择 SAMSUNGSPHL720，并显示在设备类型旁边的文本框中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 要允许设备类型值中包含“Samsung”的所有设备，请按照以下步骤添加正则表达式规则：
   1. 在所选项目文本框内单击。
   2. 将文本从 SAMSUNGSPHL720 更改为 SAMSUNG.*
   3. 确保选中正则表达式复选框。
   4. 单击允许。

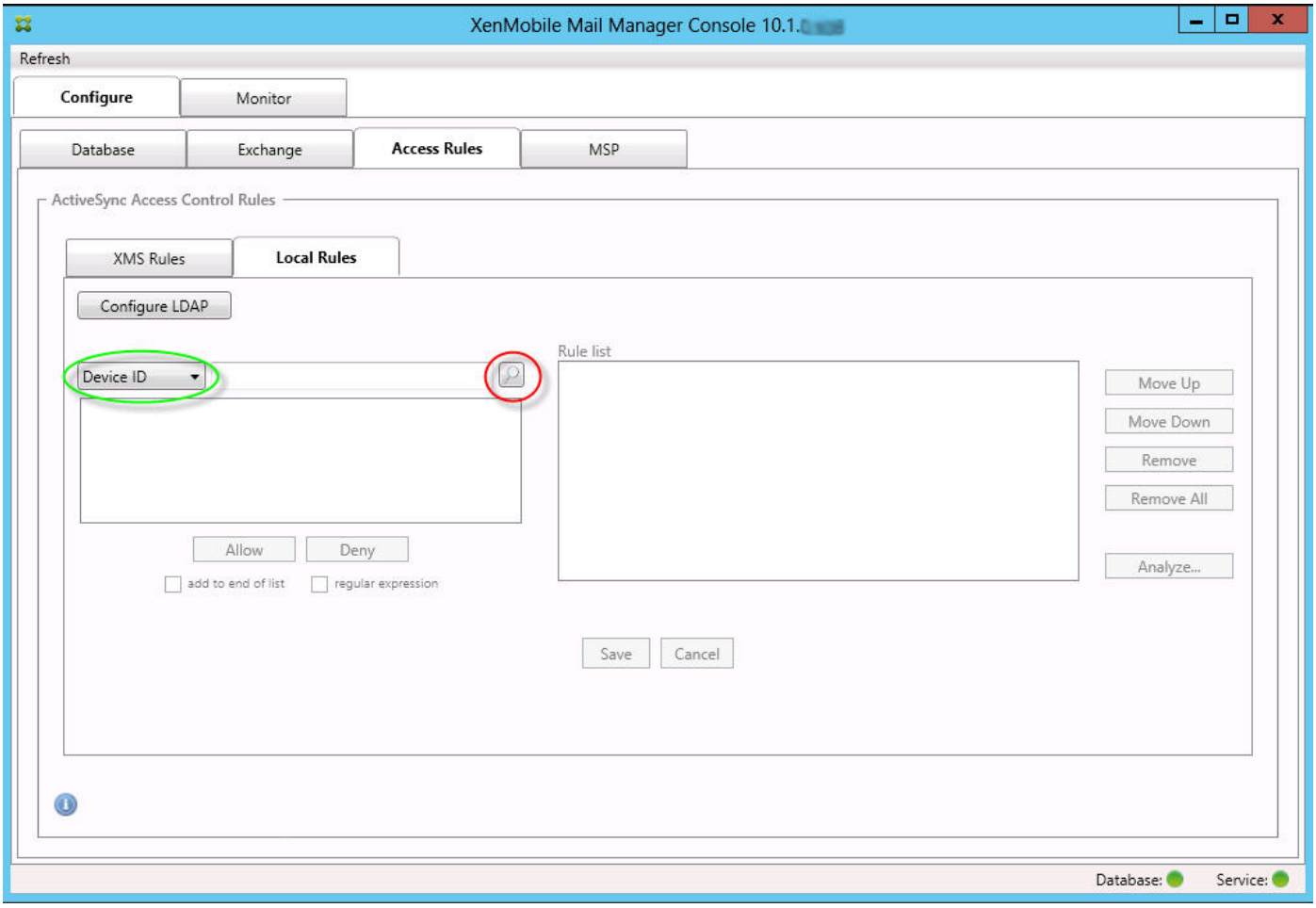
© 1999-2017 Citrix Systems, Inc. All rights reserved.



构建访问规则

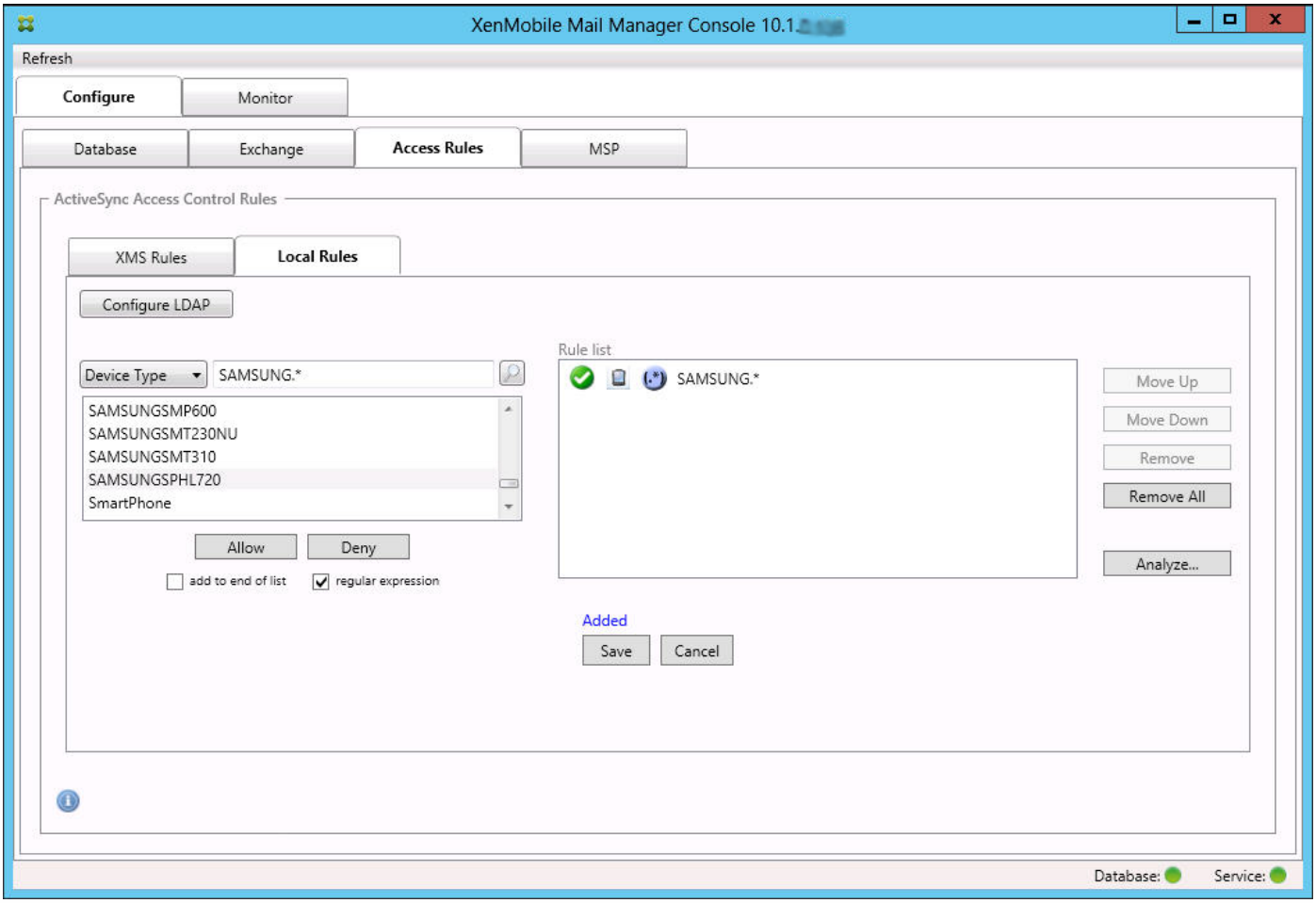
1. 单击 Local Rules（本地规则）选项卡。
2. 要输入正则表达式，需要使用“设备 ID”列表和所选项目文本框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 选择要匹配的字段。 此示例使用设备类型。
4. 键入正则表达式。 此示例使用samsung.*
5. 确保选中正则表达式复选框，然后单击允许或拒绝。 在此示例中，选择的是允许，因此最终结果如下所示：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

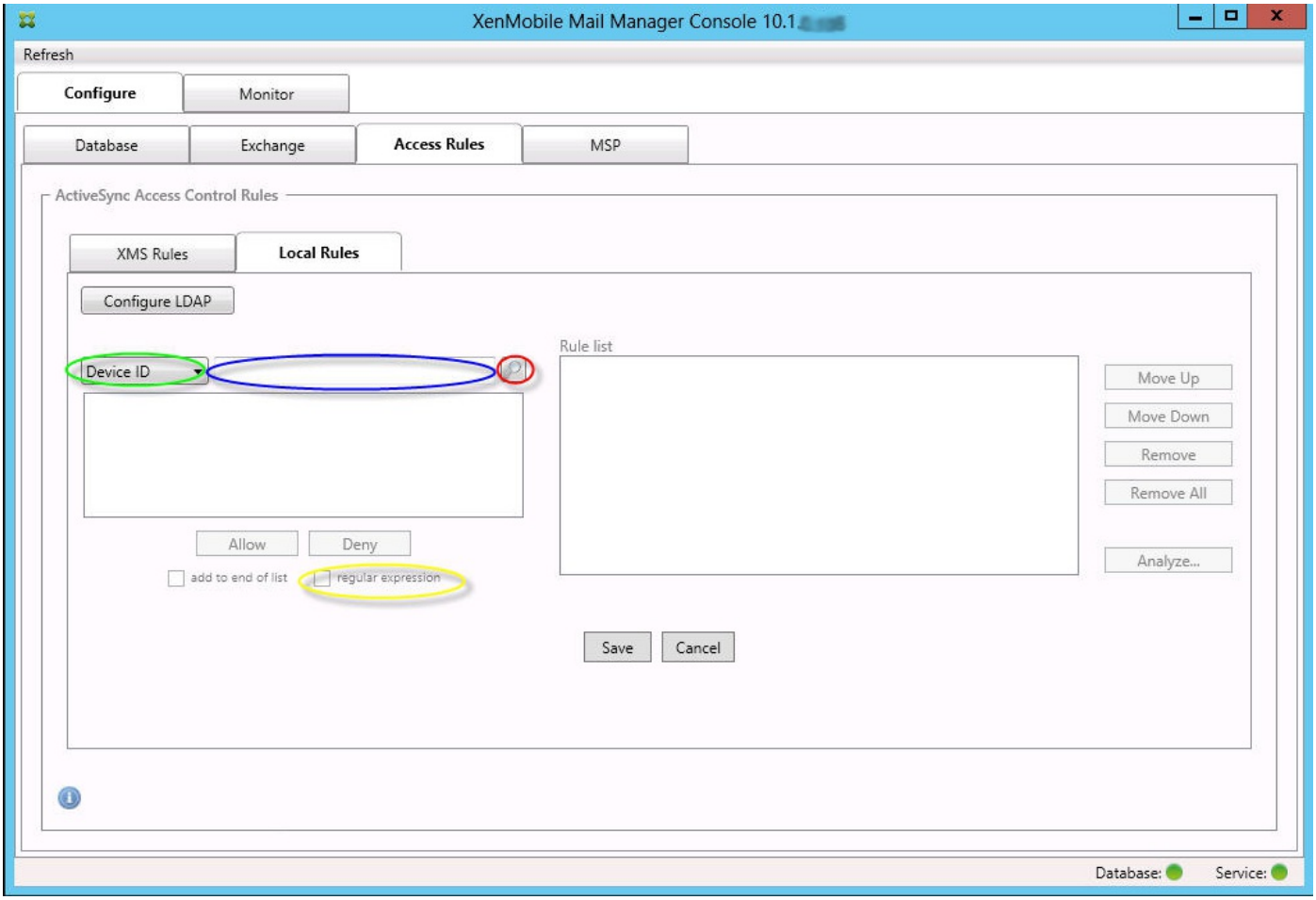


查找设备

通过选中正则表达式复选框，可以针对与给定表达式匹配的特定设备运行搜索。 此功能仅在成功完成主要快照时可用。 即使没有计划使用正则表达式规则，您也可以使用此功能。 例如，假定您要查找 ActiveSync 设备 ID 中包含文本“workmail”的所有设备。 为此，请执行以下过程。

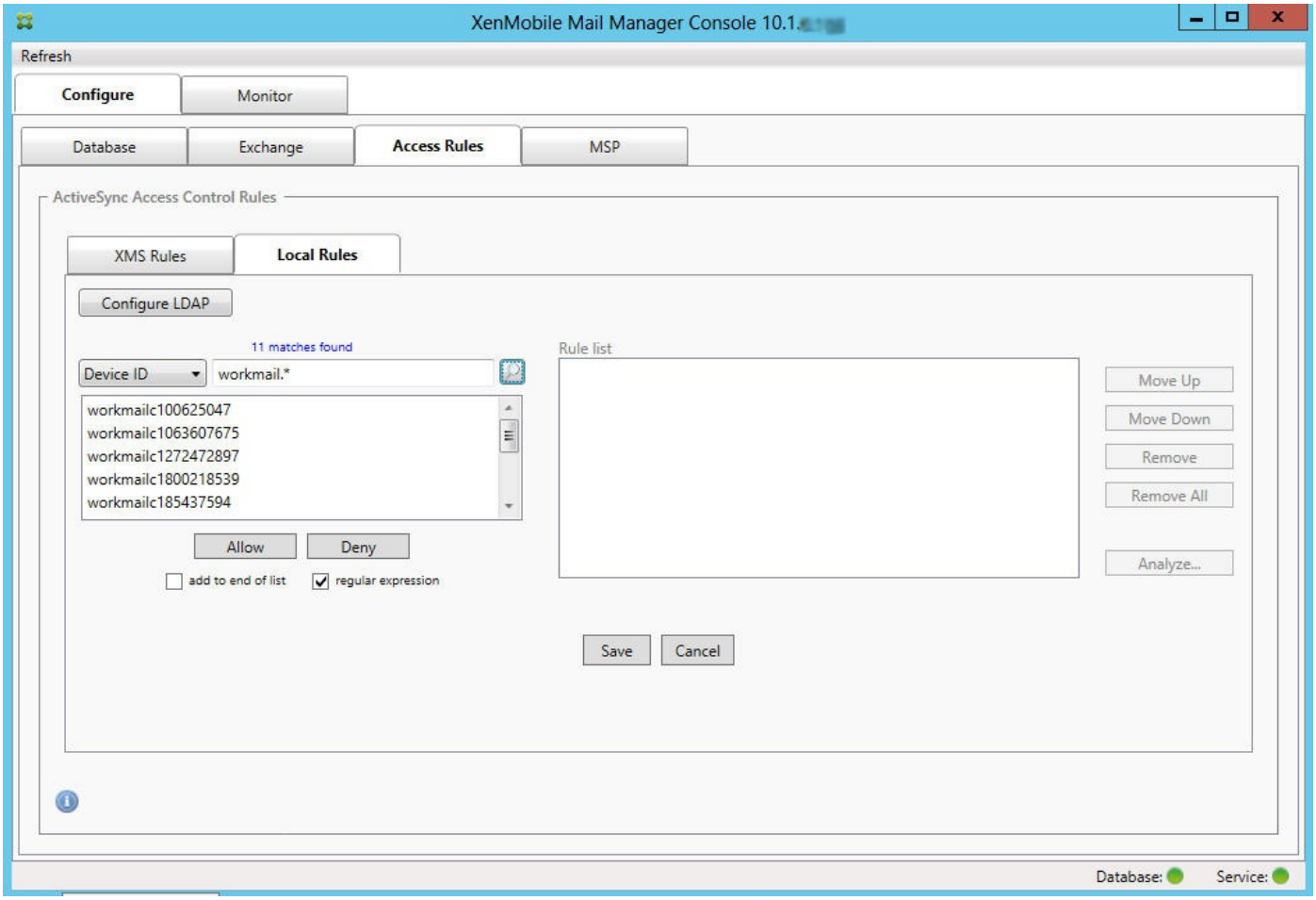
1. 单击 Access Rules（访问规则）选项卡。
2. 确保设备匹配字段选择器设置为设备 ID（默认）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 在所选项目文本框（上图中以蓝色显示的框）内单击，然后键入workmail.*。
4. 确保选中正则表达式复选框，然后单击放大镜图标显示匹配项，如下图所示。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

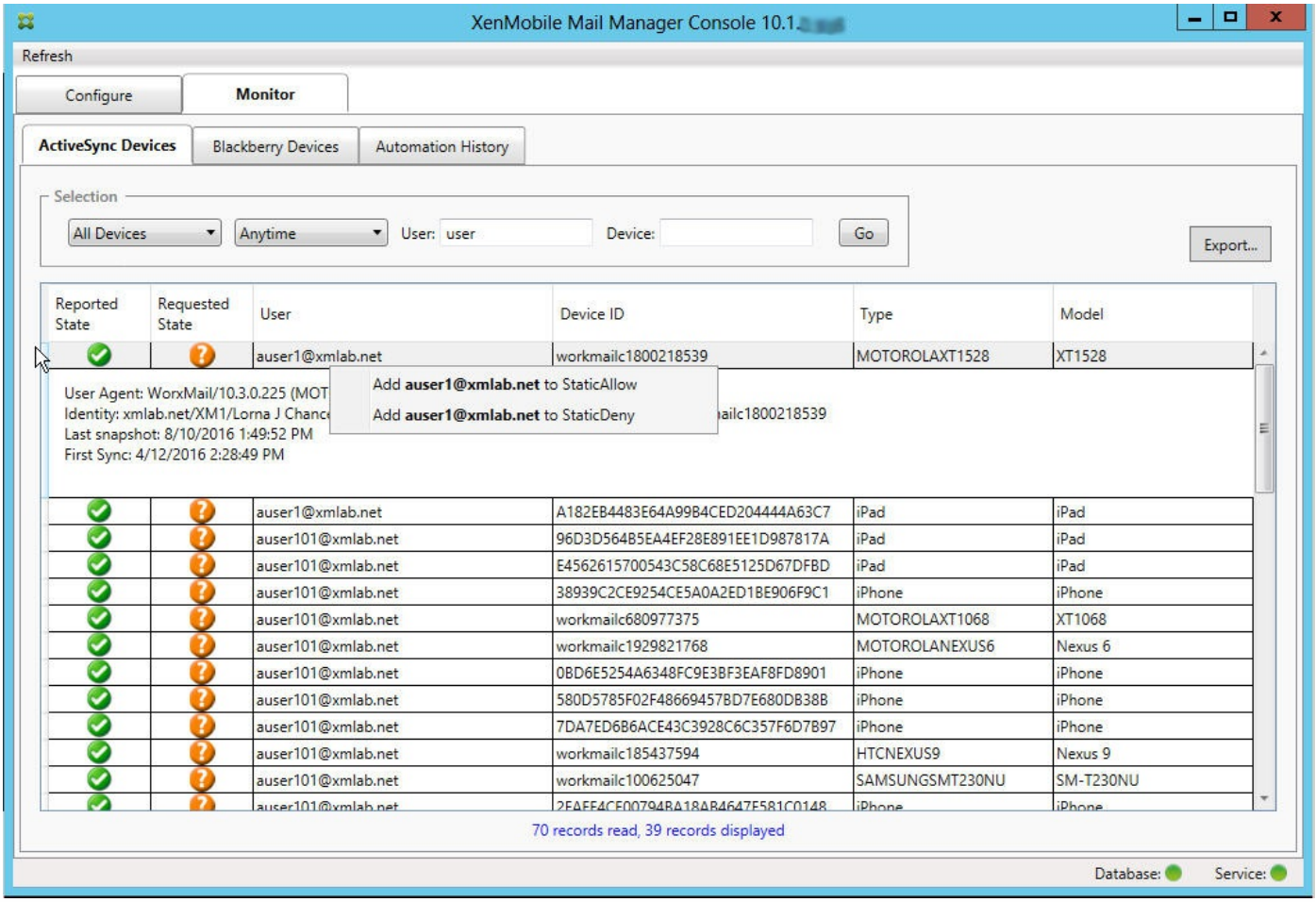


将单个用户、设备或设备类型添加到静态规则

可以基于 ActiveSync 设备选项卡上的用户、设备 ID 或设备类型添加静态规则。

1. 单击 ActiveSync 设备选项卡。
2. 在列表中，右键单击用户、设备或设备类型，然后选择是允许所选内容还是拒绝所选内容。
   下图显示了选定 user1 时的“允许”/“拒绝”选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

设备监视

Aug 11, 2016

通过 XenMobile Mail Manager 中的监视器选项卡，可以浏览已检测到的 Exchange ActiveSync 和黑莓设备以及已发出的自动化 PowerShell 命令的历史记录。 监视器选项卡有以下三个选项卡：

- ActiveSync Devices（ActiveSync 设备）：
  - 您可以通过单击导出按钮导出显示的 ActiveSync 设备合作伙伴关系。
  - 您可以通过右键单击用户、设备 ID 或类型列并选择适当的允许或阻止规则类型来添加本地（静态）规则。
  - 要折叠展开的行，请按住 Ctrl 键并单击该展开的行。
- 黑莓设备
- 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、发生了多久、检测到多少设备以及出现的任何错误。

- 在 Exchange 选项卡中，单击所需 Exchange Server 的信息图标。
- 在 MSP 选项卡中，单击所需黑莓服务器的信息图标。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

故障排除和诊断

Oct 21, 2016

XenMobile Mail Manager 将错误和其他操作信息记录到其日志文件：<安装文件夹>\log\XmmWindowsService.log。 XenMobile Mail Manager 还将重要事件记录到 Windows 事件日志。

常见错误

以下列表包括常见错误：

XenMobile Mail Manager Service 未启动

检查日志文件和 Windows 事件日志中的错误。 包括以下典型原因：

- XenMobile Mail Manager Service 无法访问 SQL Server。 以下这些问题可能导致此情况：
  - SQL Server 服务不在运行。
  - 身份验证失败。

  如果已配置 Windows 集成身份验证，必须允许 XenMobile Mail Manager Service 的用户帐户进行 SQL 登录。 XenMobile Mail Manager Service 的帐户默认设置为“Local System”（本地系统），但是可能更改为任何具有本地管理员权限的帐户。 如果已配置 SQL 身份验证，必须在 SQL 中正确配置 SQL 登录。

- 为移动服务提供商 (MSP) 配置的端口不可用。 必须选择未被系统中其他进程使用的侦听端口。

XenMobile 无法连接到 MSP

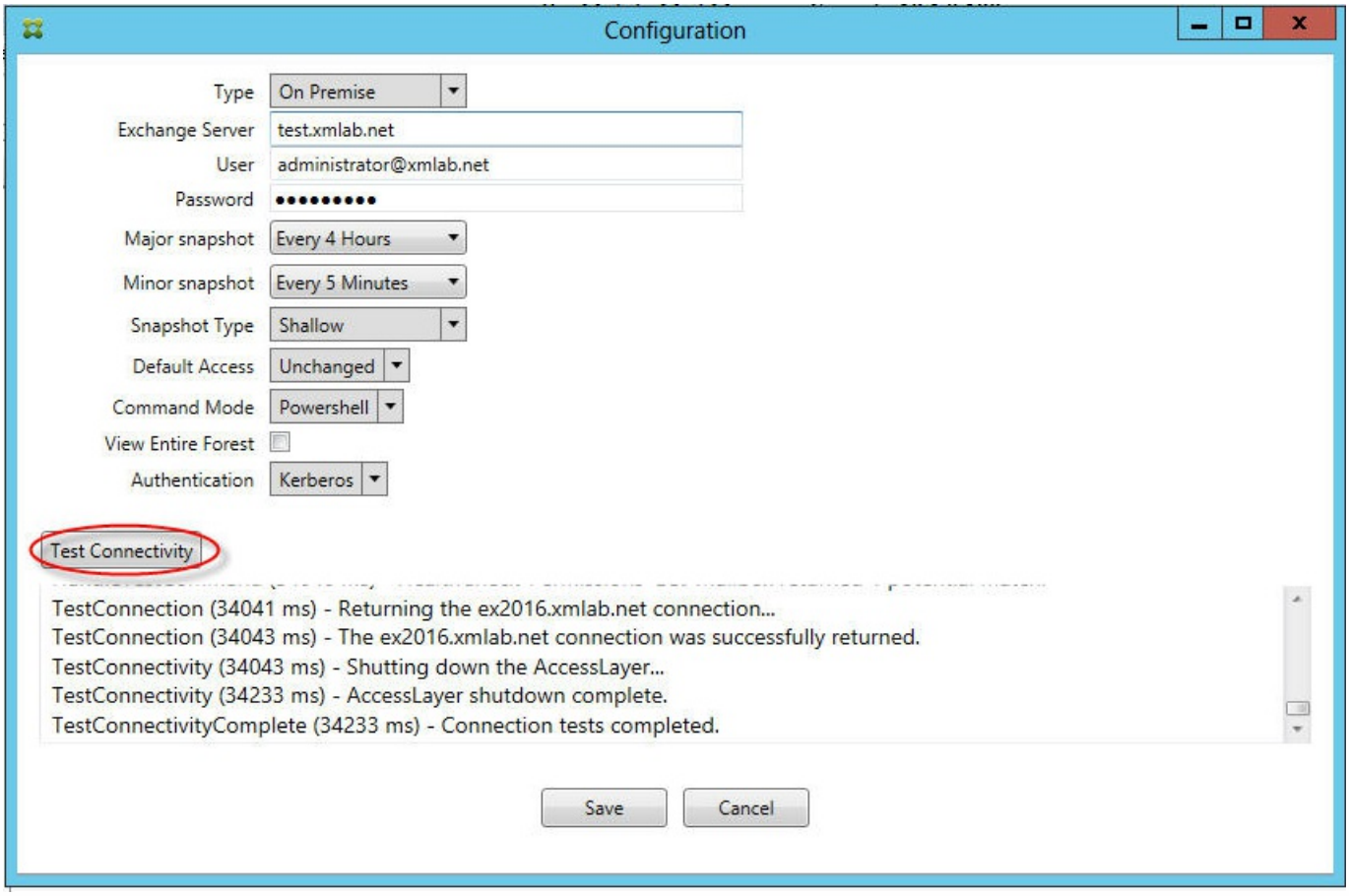
检查是否已在 XenMobile Mail Manager 控制台的配置> MSP 选项卡中正确配置 MSP 服务端口和传输。 检查是否已正确设置授权组或用户。

如果已配置 HTTPS，则必须安装有效的 SSL 服务器证书。 如果已安装 IIS，IIS Manager 可以用来安装证书。 如果未安装 IIS，有关安装证书的详细信息，请参见 http://msdn.microsoft.com/en-us/library/ms733791.aspx。

XenMobile Mail Manager 包含测试与 MSP Service 的连接的实用程序。 运行 <安装文件夹>MspTestServiceClient.exe 程序并且将 URL 和凭据设置为将在 XenMobile 中配置的 URL 和凭据，然后单击 Test Connectivity（测试连接）。 这会模拟 XenMobile Service 发出的 Web 服务请求。 注意，如果已配置 HTTPS，您必须指定服务器的实际主机名称（在 SSL 证书中指定的名称）。

注意：使用**测试连接**时，请确保至少具有一个 ActiveSyncDevice 记录，否则测试可能失败。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



故障排除工具

Support\PowerShell 文件夹中提供了一组用于故障排除的 PowerShell 实用程序。

故障排除工具将对用户的邮箱和设备执行深度分析（从而检测错误条件和潜在的故障区域）并对用户执行深度 RBAC 分析。 该工具可以将所有 cdmlet 的原始输出保存到一个文本文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile NetScaler Connector

Oct 21, 2016

XenMobile NetScaler Connector 向 NetScaler 提供 ActiveSync 客户端的设备级别授权服务，而 NetScaler 用作 Exchange ActiveSync 协议的反向代理。 授权由在 XenMobile 中定义的策略组合以及 XenMobile NetScaler Connector 本地定义的规则控制。

有关详细信息，请参阅以下文章：

- XenMobile NetScaler Connector
- XenMobile 中的 ActiveSync Gateway

有关详细的参考体系结构图，请参阅《XenMobile 部署手册》文章适用于本地部署的参考体系结构。

© 1999-2017 Citrix Systems, Inc. All rights reserved.