XenMobile Server 10

May 05, 2016

Symbian 设备

在 XenMobile 中发送注册邀请

配置部署规则

添加设备并查看设备详细信息

手动标记用户设备

设备置备文件格式

宏

设备策略

XenMobile 设备策略（按平台）

添加应用程序访问设备策略

添加应用程序清单设备策略

添加适用于 Android 的应用程序通道设备策略

自定义 XML 设备策略

应用程序卸载设备策略

添加 APN 策略

添加适用于 iOS 的手机网络设备策略

为 Windows Phone 8.1 添加企业 Hub 设备策略

Microsoft Exchange ActiveSync 设备策略

定位设备策略

连接计划设备策略

添加适用于 iOS 的 AirPlay 镜像设备策略

添加适用于 iOS 的 AirPrint 设备策略

添加适用于 iOS 的日历 (CalDav) 设备策略

添加适用于 iOS 的联系人 (CardDAV) 设备策略

凭据设备策略

为 Samsung SAFE 添加 Kiosk 设备策略

为 iOS 添加字体设备策略

为 iOS 添加组织信息设备策略

为 iOS 添加 LDAP 设备策略

添加适用于 iOS 的 Single Sign-On 帐户设备策略

添加适用于 iOS 的已订阅的日历设备策略

通行码设备策略

为 iOS 添加代理设备策略

为 Samsung KNOX 添加远程支持设备策略

限制设备策略

添加适用于 iOS 的漫游设备策略

添加适用于 iOS 的 SCEP 设备策略

Samsung MDM 许可证密钥设备策略

存储加密设备策略

添加适用于 iOS 的 Web 内容设备策略

Samsung 浏览器设备策略

添加适用于 Windows 8.1 Tablet 的旁加载密钥设备策略

添加适用于 Windows 8.1 Tablet 的签名证书设备策略

VPN 设备策略

WiFi 设备策略

添加适用于所有平台的条款和条件设备策略

添加 Worx Store 设备策略

XenMobile 选项设备策略

添加适用于 Android 的 XenMobile 卸载设备策略

使用 Apple Configurator 将 iOS 设备置于受监督模式

添加应用程序

向 XenMobile 中添加 MDX 应用程序

在 XenMobile 中创建应用程序类别

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

应用程序连接器类型列表

向 XenMobile 中添加企业应用程序

向 XenMobile 添加 Web 链接应用程序

创建和管理工作流

在 XenMobile 中升级应用程序

MDX 策略概览

自动化操作

XenMobile 客户端设置

创建适用于 iOS 设备的自定义 Worx Store 品牌设计

创建 Worx Home 和 GoToAssist 支持选项

添加、编辑或删除客户端属性

客户端属性参考

XenMobile 服务器设置

XenMobile 中的 ActiveSync Gateway

Google Play 凭据

iOS Device Enrollment Program

iOS VPP

移动服务提供商

网络访问控制

Samsung KNOX

服务器属性

SysLog

配置 XenApp 和 XenDesktop

支持与维护

执行连接检查

在 XenMobile 中创建支持包

查看调试日志文件

配置日志设置

在 XenMobile 中查看和分析日志文件

XenMobile 命令行接口选项

XenMobile 10 API

XenMobile Mail Manager 10

体系结构

系统要求和必备条件

安装和配置

使用 ActiveSync ID 强制执行电子邮件策略

访问控制规则

设备监视

关于 XenMobile 10

May 05, 2016

XenMobile 10 combines the App Controller and Device Manager components from XenMobile 9 and earlier versions into a unified management tool from which you can configure and manage user devices and apps.

Note: The Remote Support client is not available in XenMobile Cloud versions 10.x for Windows CE and Samsung Android devices.

What's New

For a list of fixed issues in this release, see http://support.citrix.com/article/CTX141722. For a list of known issues for XenMobile 10.0, see Known Issues.

- **Unified infrastructure**. Mobile device management (MDM) and mobile app management (MAM) are unified within one server infrastructure.
  - You can deploy XenMobile faster due to fewer required setup steps.
  - You can manage apps and devices from one virtual server.
- **New unified XenMobile console.**
  - Designed with an easy-to-navigate user interface that simplifies administrative tasks, such as enrolling, deploying, configuring, and troubleshooting the entire mobility environment.
  - Simplified app and device policy configuration. You can configure one policy across all available device platforms.
- **Integration with NetScaler Gateway from the same console.** You can manage automated connectivity checks for multiple systems that are part of the mobility environment.
- **Beacons support deprecated.** Beacons are not supported in XenMobile 10, even though their options appear in the XenMobile console. Citrix recommends that you either connect to the XenMobile Server through NetScaler Gateway or, from within your firewall, directly to XenMobile Server.
- **Enhanced support for app authentication.** Helps to secure encryption between devices and the internal network, between the internal network and the XenMobile server, and for XenMobile console connections.
  - RSA Adaptive Authentication
  - Support for FIPS 140.2 advanced encryption

XenMobile 10 入门

首先在虚拟机管理程序（如 XenServer、VMware ESXi 或 Hyper-V）上下载并安装 XenMobile 10.0 Edition 的虚拟映像，然后在虚拟机管理程序命令行控制台上完成 XenMobile 初始配置。 有关详细信息，请参阅系统要求、预安装核对表以及安装 XenMobile。

接下来，使用您在初始配置期间设置的管理员帐户打开基于 Web 的 XenMobile 控制台。

为了帮助您决定在控制台中接下来要访问的位置，请参阅控制台入门。 第一组建议介绍了您可能在安装步骤中跳过的初始设置。

体系结构概述

May 05, 2016

您部署的 XenMobile 组件取决于贵组织的设备或应用程序管理要求。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。

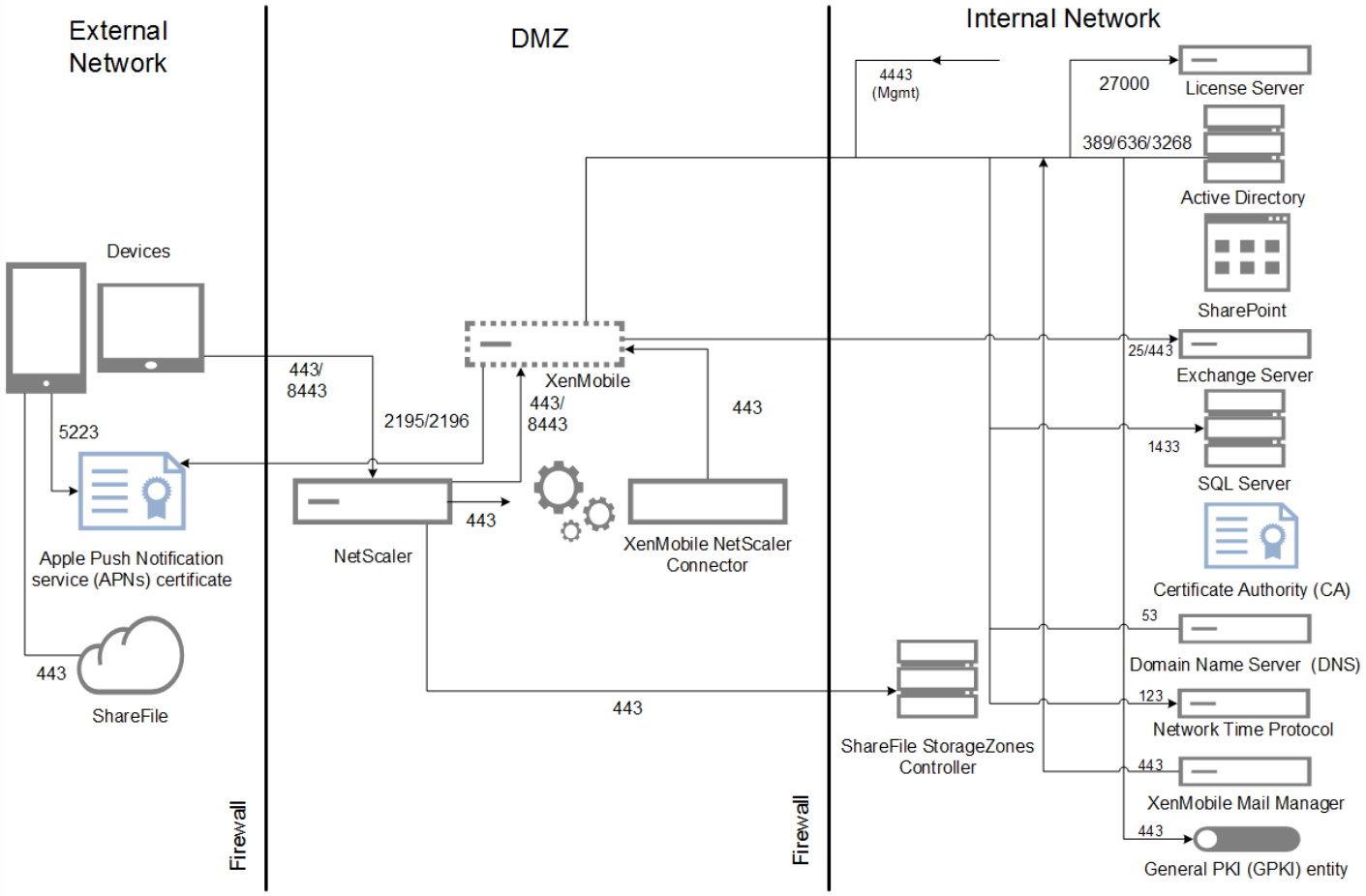
要实现部分或全部功能，Citrix 建议按以下顺序部署 XenMobile 组件：

- NetScaler Gateway。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。
  有关策略、设置、注册和应用程序的详细信息，请参阅以下 eDocs。
  - 设备策略
  - 配置 XenMobile 客户端设置
  - 配置 XenMobile 服务器设置
  - 在 XenMobile 中注册用户和设备
  - 向 XenMobile 添加应用程序
- 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。请参阅使用 MDX Toolkit 10.0 打包应用程序。
- 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。

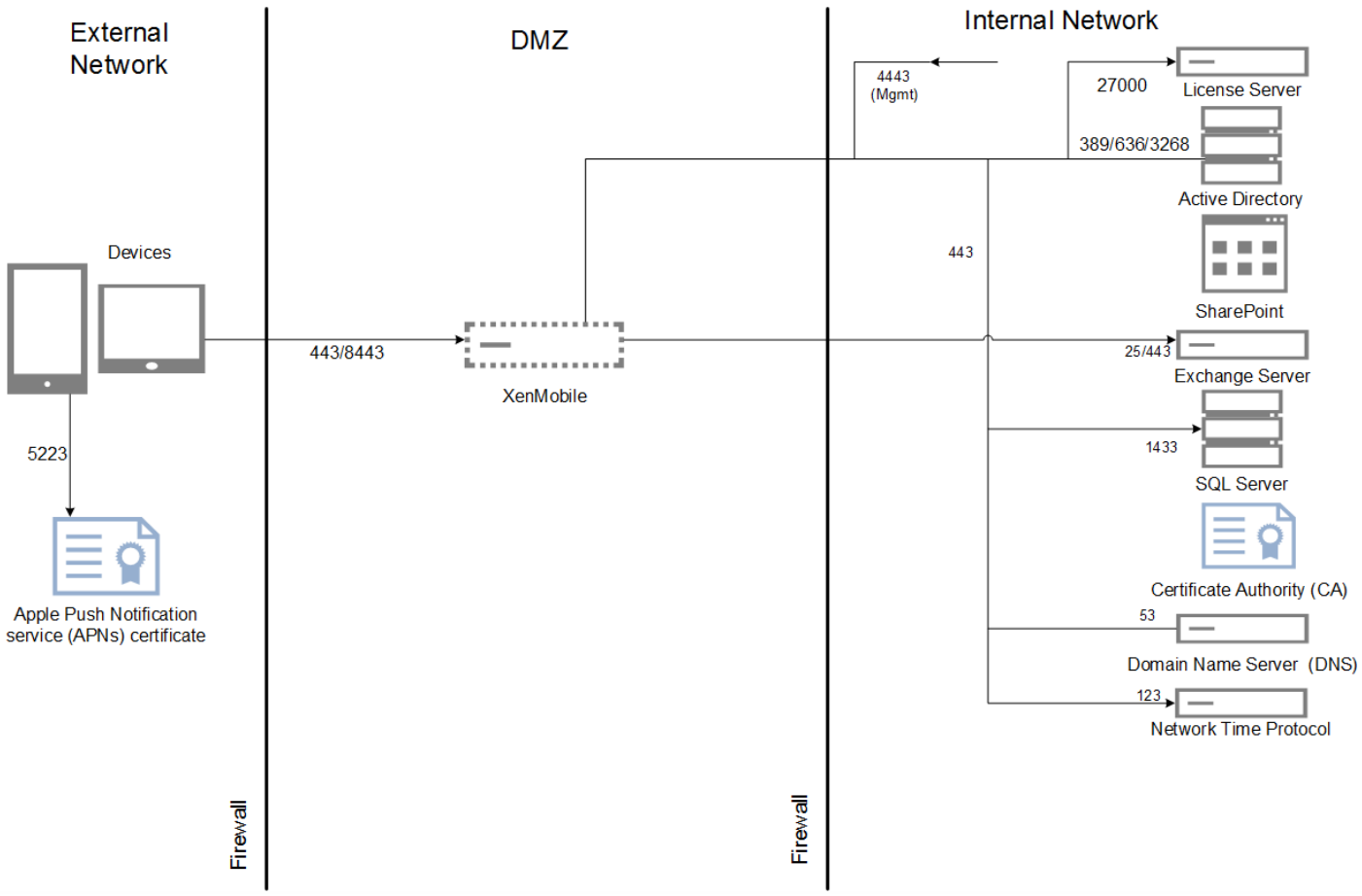
XenMobile 支持通过 XenMobile 控制台提供设备管理以及应用程序管理的集成解决方案。此部分介绍 XenMobile 部署的参考体系结构。

下图说明了 XenMobile 部署的不同参考体系结构。在图表中，连接器上面的号码表示要允许组件之间进行通信必须打开的端口。有关完整端口列表，请参阅 XenMobile 端口要求。

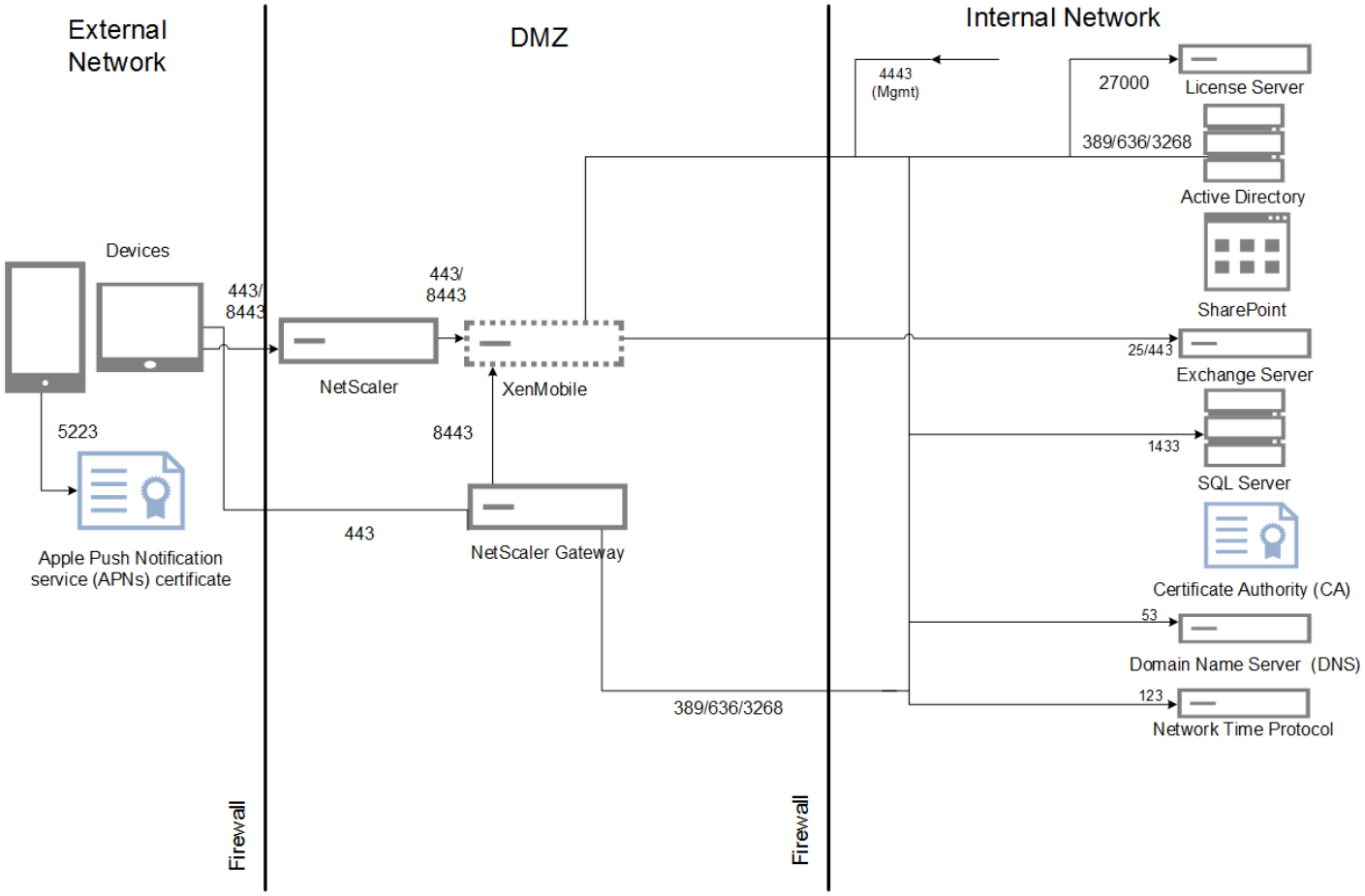
移动设备管理 (MDM) 模式 – XenMobile MDM Edition 为 iOS、Android、Amazon 和 Windows Phone 提供移动设备管理（请参阅 XenMobile 10 支持的设备平台）。在建议的模型中，XenMobile 服务器位于 DMZ 中，可选 NetScaler 位于前端，后者为 XenMobile 提供额外的保护。



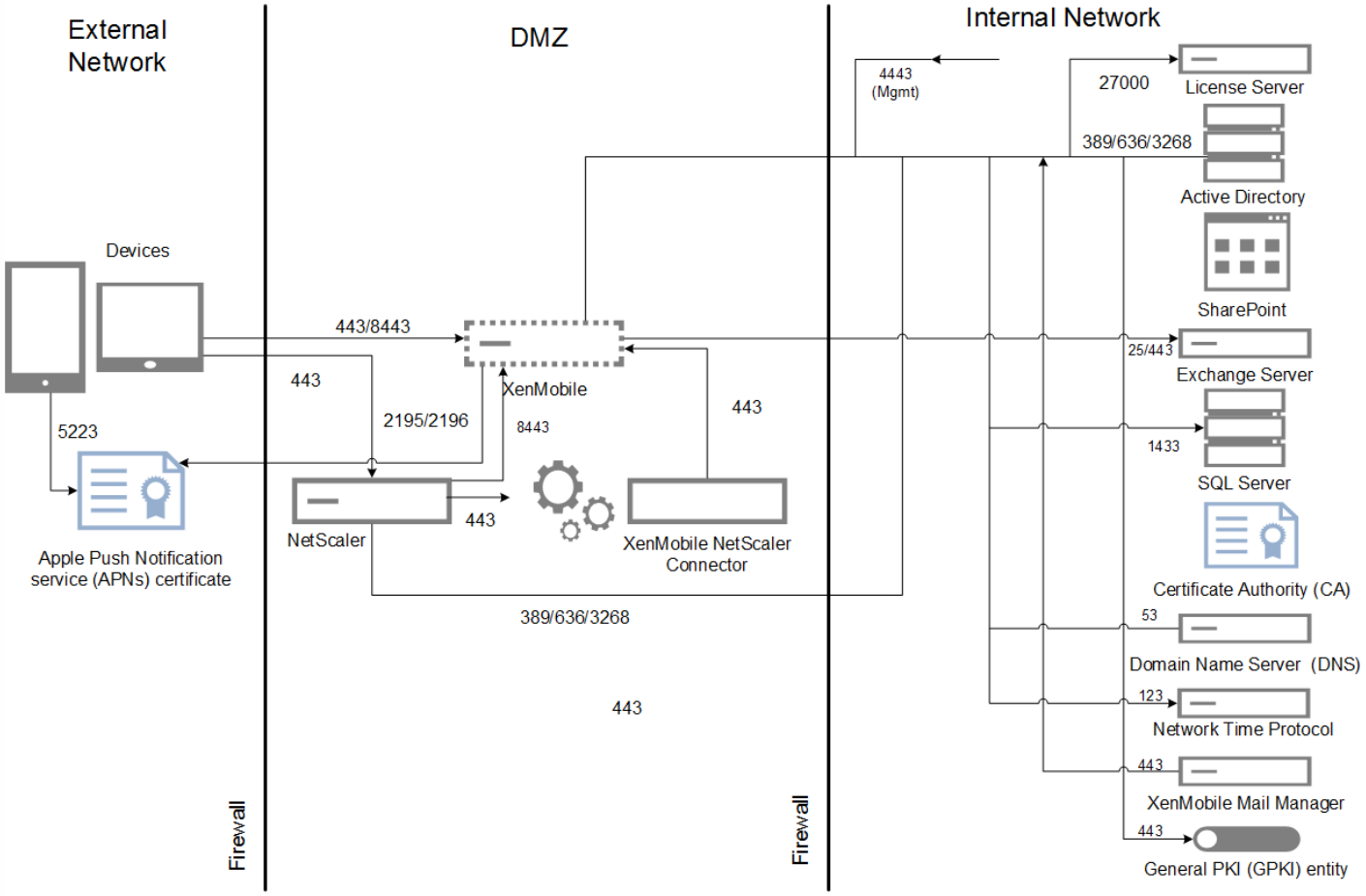
移动应用程序管理 (MAM) 模式 – 移动应用程序管理 (MAM) 支持 iOS 和 Android 设备，但是不支持 Windows Phone 设备（请参阅 XenMobile 10 支持的设备平台）。在建议的部署模型中，XenMobile 服务器与 NetScaler Gateway 位于前端，后者为 XenMobile 提供额外的保护。



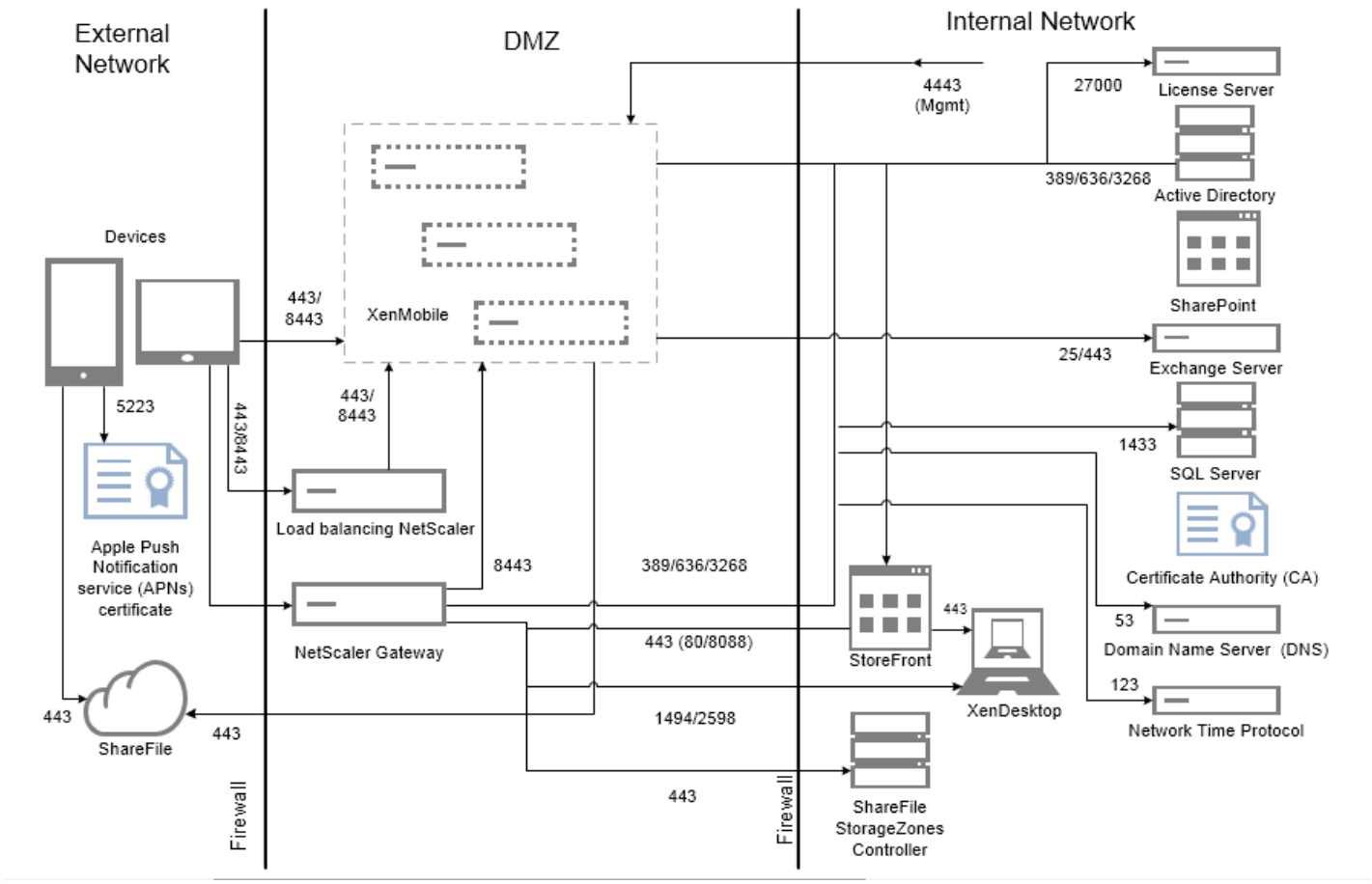
MAM 与 NetScaler Gateway（推荐的部署）



MDM 和 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（请参见 XenMobile 10 支持的设备平台）。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。



群集部署 – 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。



扩展 XenMobile 10

May 05, 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 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。

表 1.带注册的 XenMobile Enterprise

可扩展性	最多 100000 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 Server 10 节点群集
	数据库	Microsoft SQL Server 外部数据库

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：

- 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。
- 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

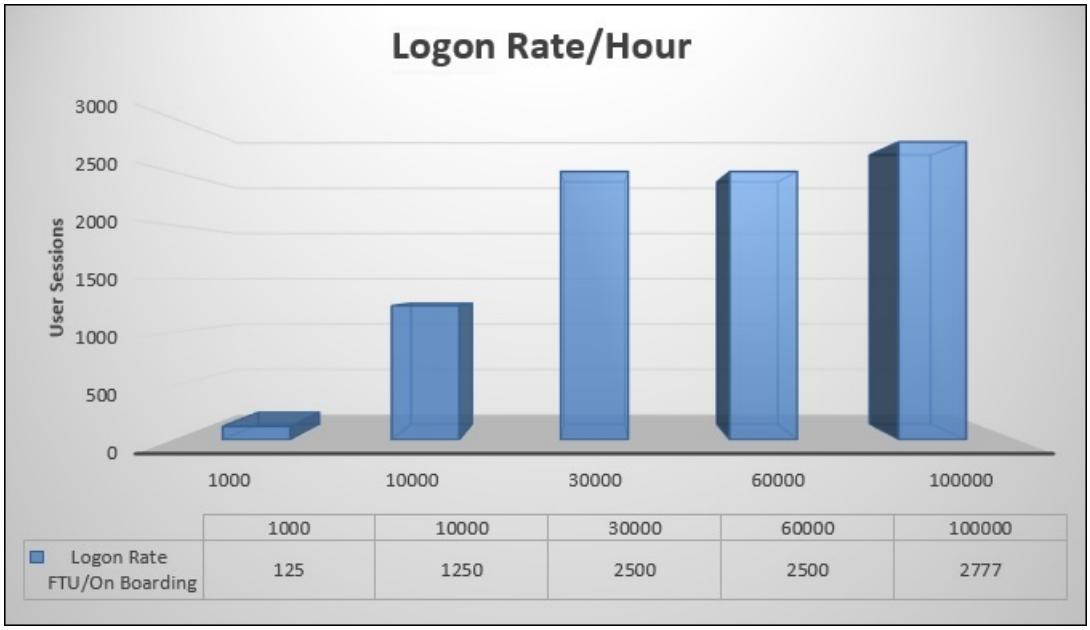
配置。

- 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。

表 2. 带注册的 XenMobile Enterprise 的可扩展性结果

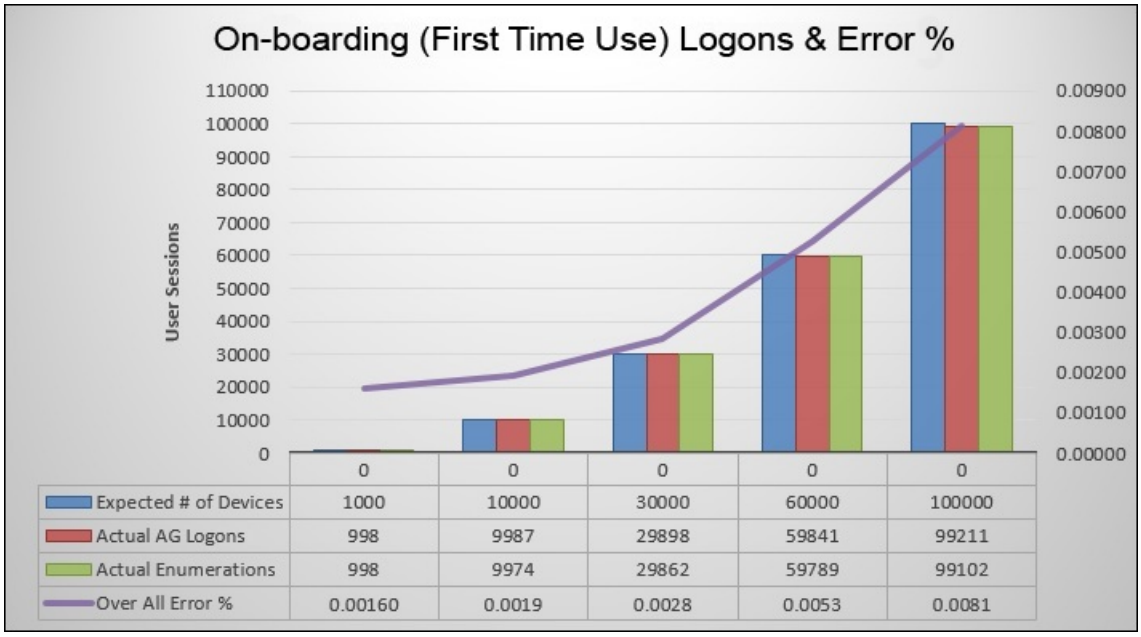
设备数量	1,000	10,000	30,000	60,000	100,000
登录率					
加入率 (FTU)	125	1250	2,500	2,500	2,777
现有用户数	1,000	2,500	7,500	15,000	16667
配置					
参考环境	VPX-XenMobile 独立模式	MPX-XenMobile 独立模式	MPX-XenMobile 群集 (3)	MPX-XenMobile 群集 (6)	MPX-XenMobile 群集 (10)
NetScaler Gateway	VPX，带 2 GB RAM 2 个虚拟 CPU	MPX-10500		MPX-20500	
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	16 GB RAM 和 4 个虚拟 CPU			
数据库	外部				

上表显示了基于 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。



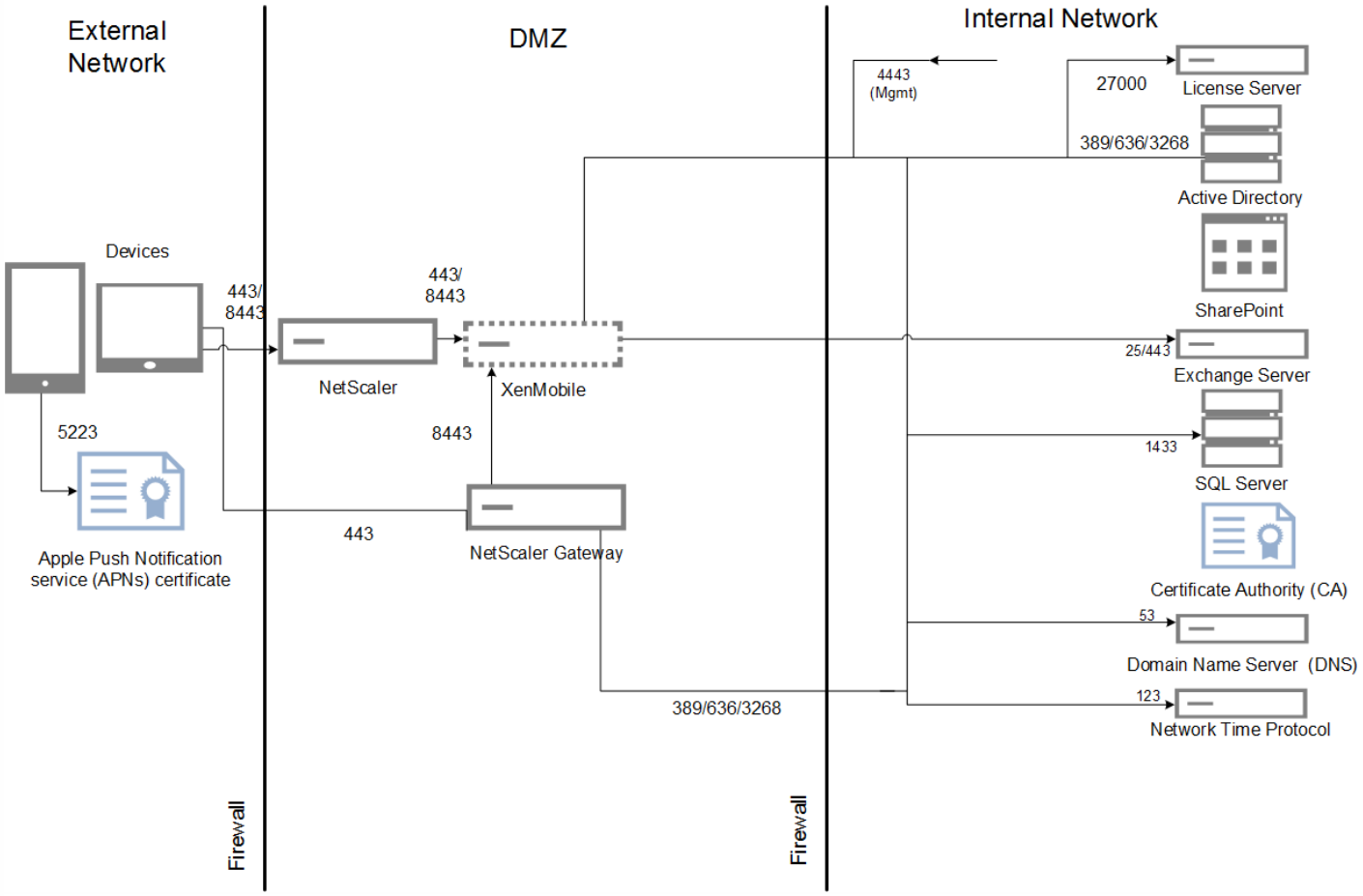
注意：调整系统时，如果超过建议的比率或硬件建议，会遇到以下问题。

- 注册或登录延迟（往返时间）
  - 平均总延迟：> 1.5 秒
  - NetScaler Gateway 登录的平均延迟：> 440 毫秒
  - Worx Store 请求的平均延迟：> 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。
  - XenMobile 控制台响应速度变慢。

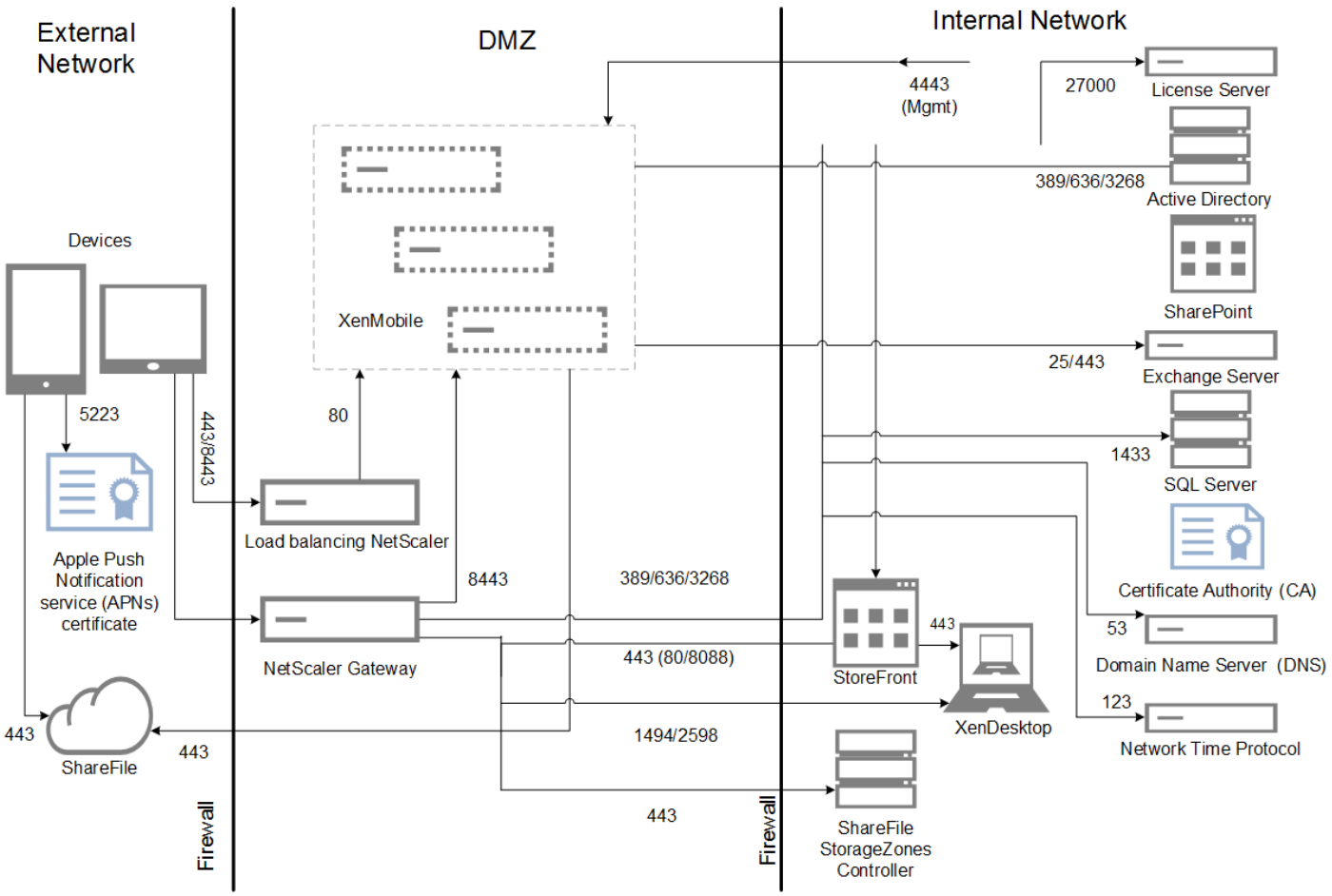


上图中的错误百分比包括遇到的总错误，考虑了每个操作对应的请求，并非仅限于登录。根据退出条件中的定义，运行的每个测试的错误百分比都在可接受的限制内。

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。



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 MDM 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 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：

表 3.用户工作负载定义

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。
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。

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）
- 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

工作负载参数包括：

- 每台设备 1 次设备注册
- 每台设备 1 次枚举
- 每台设备 14 次应用程序枚举
- 每台设备 4 次 Worx Store 启动
- 每台设备 4 次 Web/SaaS 应用程序 SSO
- 每台设备 1 次 MDX 应用程序下载
- 2 次必需的应用程序下载

现有用户工作负载

下表显示了现有用户工作负载。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 端口的可扩展性。对于 WorxWeb 应用程序，用户访问内部 Web 站点，不会触发 XenMobile 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

WorxApps 连接配置文件

下表显示了现有用户的工作负载参数。

表 4.WorxApps 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）。

注意：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

下表显示了 WorxMail 和 WorxWeb 配置文件详细信息。

表 5.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

表 6.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。
- 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。

表 7.XenMobile 基础结构组件

组件	版本
NetScaler Gateway	10.5.55.8.nc
XenMobile	10.0.0.62300

外部数据库	MS SQL Server 2008 R2 （128 GB RAM、300 GB 磁盘空间、24 个虚拟 CPU）

可扩展性测试在 XenServer 平台上运行，如下表所示。

表 8.XenServer 硬件

供应商	GenuineIntel
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）。

有关本文或此处所提及产品的其他产品信息和技术问题，请访问 Citrix.com，搜索 XenMobile 文档站点以查找最新产品文档，或联系您当地的 Citrix 代表。

关于 XenMobile 云

May 05, 2016

XenMobile Cloud is a product service that offers a XenMobile enterprise mobility management (EMM) environment for managing apps and devices as well as users or groups of users. With XenMobile Cloud, Citrix handles the configuration and maintenance of the infrastructure onsite through the Citrix Cloud Operations group. This separation lets you focus exclusively on the user experience and on managing devices, policies, and apps. XenMobile Cloud also replaces the need to purchase and manage licenses with a subscription fee.

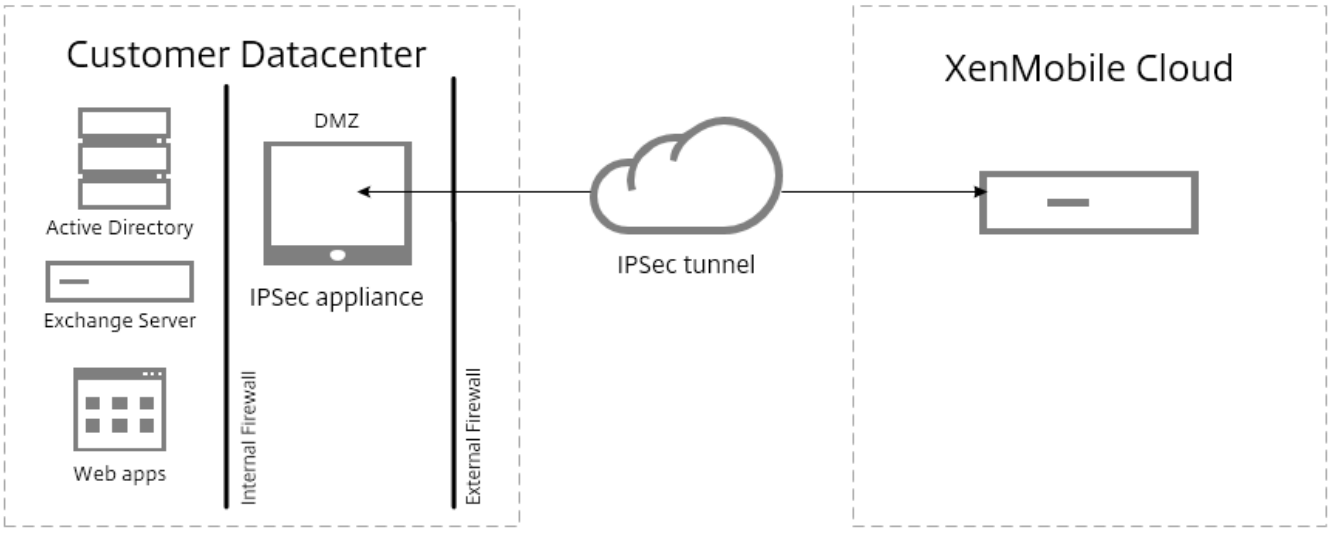
Cloud Operations administrators handle maintenance and configuration of the network connectivity, as well as the integration of Citrix products like NetScaler, XenApp, XenDesktop, StoreFront, and ShareFile. The Cloud environment is hosted in Amazon datacenters located throughout the world to deliver high performance, rapid response, and support.

To get started with XenMobile Cloud, go to https://www.citrix.com/products/xenmobile/tech-info/cloud.html

注意

- The Remote Support client is not available in XenMobile Cloud versions 10.x for Windows CE and Samsung Android devices.
- XenMobile Cloud server-side components are not FIPS 140-2 compliant.
- Citrix does not support syslog integration in XenMobile Cloud with an an on-premises syslog server. Instead, you can download the logs from the Support page in the XenMobile console. When doing so, you must click Download All in order to get system logs. For details, see Viewing and Analyzing Log Files in XenMobile.

The architecture of XenMobile Cloud is shown in the following figure:



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
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

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	高级	群集信息	Cloud 管理员和技术支持人员
支持	高级	垃圾回收	Cloud 管理员和技术支持人员
支持	高级	Java 内存属性	Cloud 管理员和技术支持人员
支持	高级	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

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	高级	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

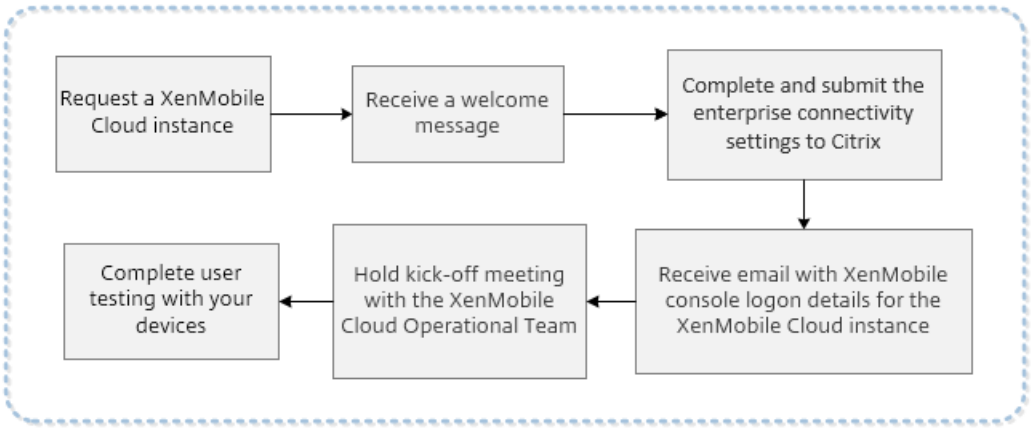
有关自定义角色的分步说明，请参谋使用 RBAC 配置角色。

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

XenMobile 云必备条件和管理

May 05, 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

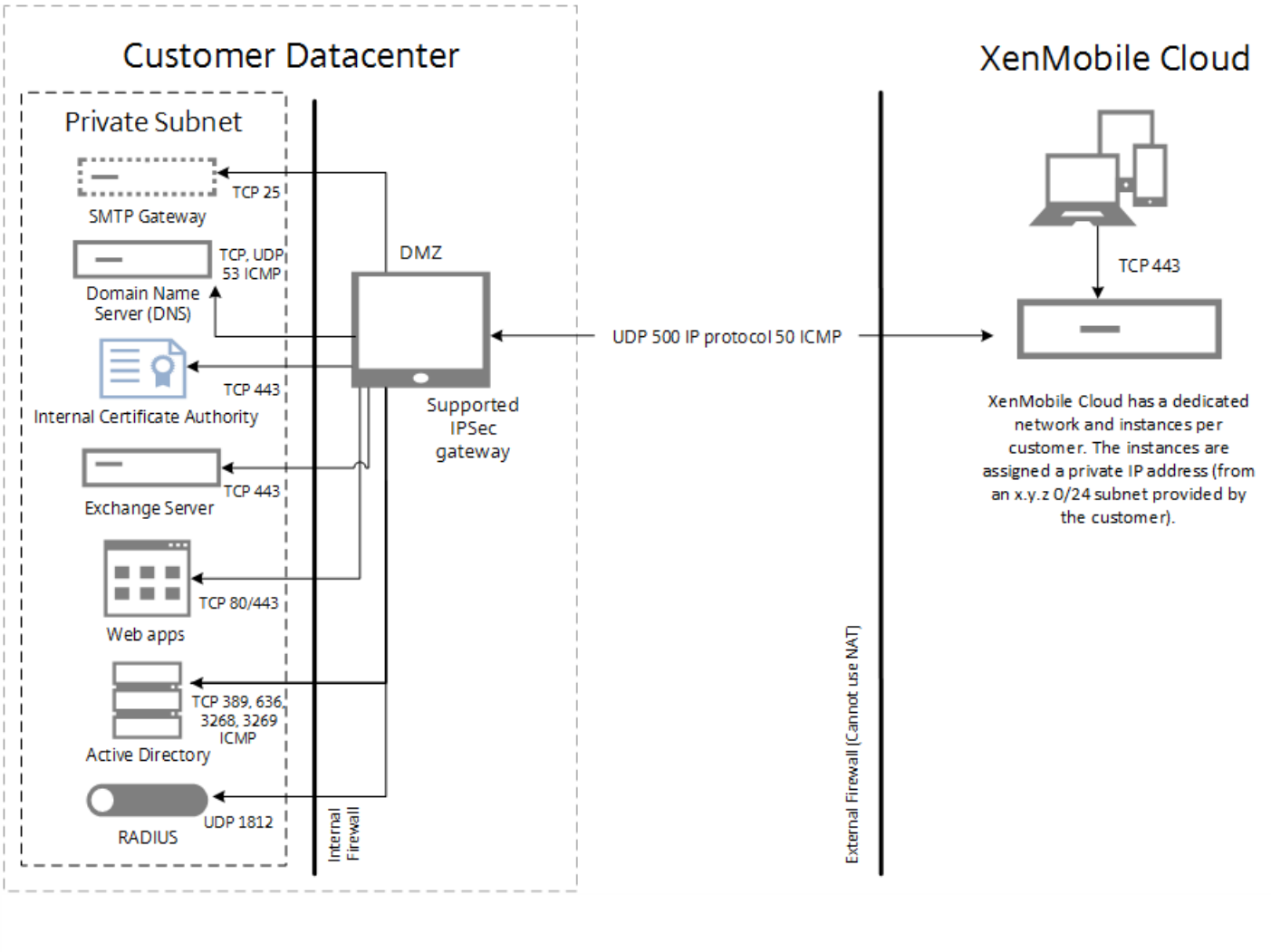
可以使用 XenMobile Enterprise Connector，这是一个 IPsec 通道，用于将 XenMobile 云基础结构与公司服务相连接，例如 Active Directory。

以下 Amazon Web 服务 Web 站点中列出的 IPsec 网关已通过官方测试，支持 XenMobile 云解决方案：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共 IP 地址，并且该地址不能使用网络地址转换 (NAT)。

下图显示了如何在 XenMobile 云解决方案中配置 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 IP 地址	客户 IPSec 设备	ICMP		适用于故障排除（可以在设置后删除）。

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

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。

XenMobile 云中支持的移动平台

May 05, 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）。

系统要求

May 05, 2016

要运行 XenMobile 10，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）；有关详细信息，请参阅 XenServer
  - VMWare（支持的版本：ESXi 4.1、ESXi 5.1 或 ESXi 5.5）；有关详细信息，请参阅 VMware
  - 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
- 两个虚拟 CPU
- 4 GB RAM
- 50 GB 磁盘空间

1 万台设备建议进行如下配置：

- 四核处理器
- 8 GB RAM

NetScaler Gateway 系统要求

要在 XenMobile 10 中运行 NetScaler Gateway，需要满足以下最低系统要求：

- XenServer、VMWare 或 Hyper-V
- 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 的数据库要求

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
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008

Citrix XenMobile 支持 SQL AlwaysOn 可用性组和 SQL 群集以实现数据库高可用性。Citrix 不支持为实现 XenMobile 数据库高可用性而进行数据库镜像。我们支持在 MS SQL 群集部署中在主动/主动或主动被动模式下使用数据库高可用性。

注意：如果数据库处于脱机状态，Device Manager 将不向来自设备的任何连接提供服务，因为 Device Manager 也处于脱机状态。

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。
注意：请确保要用于 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 开发人员网络站点上的以下页面（这些链接指向 SQL Server 2014 的相关信息。如果您使用的是其他版本，请从“其他版本”列表中选择服务器版本）：

- 服务器配置 - 服务帐户

- 配置 Windows 服务帐户和权限
- 服务器级别的角色

XenMobile 兼容性

May 05, 2016

本文概述了受支持的 XenMobile 组件的各个版本，您可以将这些组件集成在一起，包括 NetScaler Gateway 以及用于对 Worx 移动应用程序进行打包、配置和分发的 MDX Toolkit 版本。

指向本文中各部分内容的快速链接

XenMobile 10.x

支持的 NetScaler Gateway 版本：

- 11.0.64.x
- 10.5.x.e
- 10.5.x MR
- 10.1.x.e
- 10.1.x MR

XenMobile 客户端组件通常满足以下兼容性要求：

- 最新版本的 Worx Home 和 MDX Toolkit 与最新版本的 XenMobile 服务器以及该版本之前的两个最新版本兼容。
- 最新版本的 MDX Tookit 以及该版本之前的两个最新版本与最新版本的 Worx Home 和 Worx 移动应用程序兼容。

要利用新增功能、修复和策略更新，Citrix 建议您安装最新版本的 MDX Toolkit、Worx Home 和 Worx 移动应用程序以获得最佳体验。

要利用新增功能、修复和策略更新，Citrix 建议您安装最新版本的 MDX Toolkit、Worx Home 和 Worx 移动应用程序。

MDX Toolkit for iOS and Android versions	**Compatible Worx Home versions**	
	Android	**iOS**
10.3.5	10.3.5	10.3.5
10.3.1	10.3.1	10.3.1
10.3	10.3	Not applicable
10.2.1	10.2.1 10.3 10.3.1	10.2.1 10.3
10.0.7	10.0.8	10.0.8
10.0.5 - 10.0.3	10.0.3	10.0.3

MDX Toolkit for Windows Phone	**Compatible Worx Home versions**
10.0.7	10.0.3
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

> **注意**
>
> 10.0.3 之前的 Worx Home 版本兼容，但不受支持。

XenMobile 10.x 支持下表中列出的 Worx Mobile 应用程序版本：

* 表示应用程序不适用于相应平台。

App	Android	iOS	Windows Phone 8.1/10[1]
Worx Home	10.3.5 10.3.1 10.2.1 10.0.8 10.0.3 10.0.0	10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.0.3 10.0.0
WorxMail	10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7
WorxNotes	10.3.5 10.3 10.2 10.0.7 10.0.0	10.3.5 10.3 10.2 10.0.7 10.0.0	*
WorxTasks	10.3.5 10.3 10.2 10.0.7	10.3.5 10.3 10.2 10.0.7	*
WorxWeb	10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit/ WorxEdit [1]	1.2 1.1 1.0.1 1.0	5.9.3 5.9.1 5.8 5.7	*
ShareConnect/ WorxDesktop[2]	3.1 3.0	2.5 2.4	*

	2.5	2.3	
ShareFile (Worx apps)[3]	3.9.8 3.9.7 3.9.6	3.2.13 3.2.12 3.2.11	*
Citrix for Salesforce	*	10.2 10.0.7	*

[1] Windows Phone 10 在 XenMobile 服务器 10.1 上不受支持 。

[2]在早期版本中，QuickEdit 的 Worx 版本名为 WorxEdit，ShareConnect 的 Worx 版本名为 WorxDesktop。 MDX 和非 MDX 版本现在具有相同的名称：QuickEdit 和 ShareConnect。

[3] 下载页面包括一个单独的 ShareFile Worx for iOS 版本，该版本需要与受限的 StorageZones 结合使用。

浏览器支持

XenMobile 10.x 支持以下浏览器：

- Internet Explorer*
- Chrome
- Firefox
- 移动设备上安装的 Safari，用于访问自助服务门户。

XenMobile 10.x 与最新版本的浏览器以及当前版本的前一个版本兼容。

*XenMobile 10.x 不支持 Internet Explorer 9 及更低版本。

XenMobile 9

XenMobile 9 包括 Device Manager 9.0 和 App Controller 9.0。

支持的 NetScaler Gateway 版本：

- 11.0.64
- 10.5.x.e
- 10.5.x MR
- 10.1.x.e
- 10.1.x MR

XenMobile 客户端组件通常满足以下兼容性要求：

- 最新版本的 Worx Home 和 MDX Toolkit 与最后两个版本的 XenMobile 服务器兼容。
- 最新版本的 MDX Toolkit 与最新版本的 Worx 移动应用程序兼容。
- 最新版本的 MDX Toolkit 与以下版本的 Worx Home 兼容：

MDX Toolkit for iOS and Android versions	**Compatible Worx Home versions**	
	Android	**iOS**
10.3.5	10.3.5	10.3.5
10.3.1	10.3.1	10.3
10.3	10.3	Not applicable
10.2.1	10.2.1 10.3 10.3.1	10.2.1 10.3

10.0.7	10.0.8	10.0.8
10.0.5 - 10.0.3	10.0.3	10.0.3

MDX Toolkit for Windows Phone 10[1]	Compatible Worx Home versions
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2	10.2

[1]In XenMobile 9, Windows 10 requires a patch, available here.

MDX Toolkit for Windows Phone 8.1	Compatible Worx Home versions
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2.1	10.2.1
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

注意

Worx Home versions earlier than 10.0.3 are compatible but not supported.

XenMobile 9 supports the Worx Mobile Apps versions listed in the following table.

App	Android	iOS	Windows Phone 8.1
Worx Home	10.3.5 10.3.1 10.2.1 10.0.3 10.0.0	10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.3.5 10.0.3 10.0.0
WorxMail	10.3.5 10.3	10.3.5 10.3	10.3.5 10.2

	10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7 10.0.3 10.0.0	10.0.7
WorxNotes	10.3.5 10.3 10.2 10.0.0	10.3.5 10.3 10.2 10.0.7 10.0.0	Not available
WorxTasks	10.3.5 10.3 10.2	10.3.5 10.3 10.2 10.0.7	Not available
WorxWeb	10.3.5 10.3 10.2 10.0.3 10.0.0	10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit/ WorxEdit [1]	1.2 1.1 1.0.1 1.0	5.9.1 5.8 5.7 5.6.1 5.5.3	Not available
ShareConnect/ WorxDesktop[1]	3.0 2.5 2.4	2.5 2.4 2.3	Not available
ShareFile (Worx apps)[2]	3.9.8 3.9.7 3.9.6	3.2.13 3.2.12 3.2.11	Not available
Citrix for Salesforce	Not available	10.2 10.0.7	Not available

[1] 以前，QuickEdit 的 Worx 版本名为 WorxEdit，ShareConnect 的 Worx 版本名为 WorxDesktop。截至最新版本，MDX 和非 MDX 版本的名称相同，即 QuickEdit 和 ShareConnect。

[2] 下载页面包括一个单独的 ShareFile Worx for iOS 版本，该版本需要与受限的 StorageZones 结合使用。

Device Manager 8.7.1 和 App Controller 2.10

支持的 NetScaler Gateway 版本：10.1.126.1203.e 和 10.1.124.1308.e

支持的客户端版本：

MDX Toolkit	Worx Home	WorxMail、WorxWeb、WorxNotes	WorxEdit	ShareFile	WorxDesktop

10.2.1 10.0.0 9.0.4	10.2.1：iOS 和 Android 10.0.0：iOS 10.0.0：Android 9.0.1：iOS 9.0.3：Android	10.2：iOS 和 Android 10.0.0：iOS 10.0.0：Android 9.0.2：iOS 9.0.3：Android	5.5.3：iOS 1.0：Android	3.9：Android 3.2.3：iOS 3.3.2：Android	3.0：Android 1.2：iOS 1.0：Android
2.3		**WorxMail** 1.5：iOS 1.5：Android **WorxWeb** 1.3.1：iOS 1.3.3：Android	**		**
2.2.1		**WorxMail** 1.3.3：iOS 1.3.13：Android **WorxWeb** 1.3.1：iOS 1.3.3：Android	**		**

* MDX Toolkit 2.3 和 2.2.1 不支持 WorxNotes。

** 不适用

Device Manager 8.6.1 和 App Controller 2.9

支持的 NetScaler Gateway 版本：10.1.124.1308.e

支持的客户端版本：

MDX Toolkit	Worx Home	WorxMail、WorxWeb、WorxNotes*	WorxEdit	ShareFile	WorxDesktop
9.0.4	9.0.1：iOS 9.0.3：Android	9.0.2：iOS 9.0.3：Android	5.5.3：iOS 1.0：Android	3.2.3：iOS 3.3.2：Android	1.2：iOS 1.0：Android
2.2.1		1.3：iOS 1.3：Android	**		**

* MDX Toolkit 2.2.1 不支持 WorxNotes。

** 不适用

支持的设备平台

May 05, 2016

XenMobile 10.x 支持对运行以下平台的设备进行企业移动性管理，包括应用程序和设备管理。 由于平台限制和安全功能，不是所有平台都支持所有功能。

要支持旧版本的移动操作系统，例如 Android 4.1 和 iOS 7，请参阅 Citrix 支持知识中心中的文章 CTX204192。

Android

XenMobile 10.3

所有模式都支持的操作系统：Android 4.4.x、5.x、6.x

仅 MDM 模式支持的操作系统：Android 4.1.x、4.2.x、4.3

Worx Home 在基于 x86 的 Android 设备上支持 MDM 功能。 应用程序管理仅在基于 ARM 的 Android 设备上可用。 在 MDX Toolkit 10.3 中，MDX 打包的企业应用程序在基于 Android x86 的设备上不受支持 。

MDX 打包的应用程序在基于 x64 的 Android 设备上不受支持。

用于测试上面列出的操作系统中安装的 XenMobile 10.3 的某些 Android 设备如下：

- Nexus 10、7、5、9
- Samsung Galaxy S4 和 Note 3、4、5
- Galaxy Tablet 2、S3、S4、S5
- HTC One
- Samsung Tablet P750
- Samsung S6 和 S6 Edge
- OnePlus X

XenMobile 10 和 10.1

所有模式都支持的操作系统：4.4.x、5.x、6.x

仅 MDM 模式支持的操作系统：4.1.x

Android 4.2 和 4.3 不受支持。

Worx Home 在基于 x86 的 Android 设备上支持 MDM 功能。 应用程序管理仅在使用基于 ARM 的处理器的 Android 设备上可用。 MDX 打包的应用程序在基于 x86 的 Android 设备上不受支持。

用于测试上面列出的操作系统中安装的 XenMobile 10 和 10.1 的某些 Android 设备如下：

- Nexus 10、7、5、9
- Galaxy S4 和 Note 2、3
- Galaxy Tablet 2、S3、S4、S5
- Moto X
- HTC One
- HTC Desire、LG
- Samsung Tablet P750

以下设备仅受设备管理模式支持：

- Android 3.0–3.2
- Android 2.3

SAFE 和 KNOX

在兼容的 Samsung 设备上，XenMobile 10.x 可同时支持和扩展 Samsung for Enterprise (SAFE) 和 Samsung KNOX 策略。 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。

XenMobile 支持运行 Fire OS 3.0 及更早版本的 Amazon Kindle 设备，这些版本可运行基于 Android 的专有操作系统。

对于 HTC 专用策略，XenMobile 支持 HTC API 0.5.0。 对于 Sony 专用策略，XenMobile 支持 Sony Enterprise SDK 2.0。

iOS

XenMobile 10.3

- iOS 9.x
- iOS 8.4.x

Some iOS devices that XenMobile 10.3 supports:

- iPhone 5, 5s, 5c, 6, 6+
- iPad 2, 3
- iPad Pro
- Mac OS X
  - MacBook, Air, Mini, Mini Retina 10.9.5, 10.10, 10.11

XenMobile 10 and 10.1

- iOS 9.x
- iOS 8.4.x

Some iOS devices that XenMobile 10 and 10.1 support:

- iPhone 5, 5s, 5c, 6, 6+
- iPad2, 3, Mini, Air, Air2, Mini Retina

Windows Phone 和 Tablet

XenMobile 10.3

- Windows 10 Tablet
  - 当 XenMobile 处于仅 MAM 模式下时，不支持 Windows 10 Tablet。
- Windows Phone 8.1/10
  - 对于 Windows Phone 10，必须安装从 XenMobile 下载页面下载的修补程序。
  - 当 XenMobile 处于仅 MAM 模式下时，不支持 Windows Phone 8.1 和 10。
- Windows Phone 8.1 与 Worx Home 的兼容性：
  - Worx Home 10.0（当 XenMobile 处于企业模式时）。
  - Worx Home 9.1.0（当 XenMobile 处于 MDM-only 模式时）。

- Windows 8.1 Pro Edition 和 Enterprise Edition（32 位和 64 位）
- Windows RT 8.1
- Windows Mobile/CE
  - 当 XenMobile 处于仅 MAM 模式下时，不支持 Windows CE。

XenMobile 10.3 支持的部分 Windows 设备：

- Windows Tablet 10、8.1
- Windows Phone 10、8.1
- HTC (Windows Phone 8.1)
- Nokia 920、925、1020、1520 (Windows Phone 8.1)
- Windows Tablet Surface Pro 3
- Windows Tablet Surface 2
- Windows Tablet RT

XenMobile 10 和 10.1

- Windows 10 Tablet
- Windows Phone 8.1/10：
  - 当 XenMobile 处于仅 MAM 模式时，不支持 Windows Phone 8.1。
  - Windows Phone 10 在 XenMobile 10.1 上不受支持。
  - Windows Phone 10 在 XenMobile 9 上受支持，但您必须安装从 XenMobile 下载页面下载的修补程序。
- Windows Phone 8.1 与 Worx Home 的兼容性：
  - Worx Home 10.0（当 XenMobile 处于企业模式时）
  - Worx Home 9.0.3（当 XenMobile 处于 MDM-only 模式时）
- Windows 8.1 Pro Edition 和 Enterprise Edition（32 位和 64 位）
- Windows RT 8.1
- Windows Mobile：XenMobile 10.1 不支持 Windows Mobile 设备。 如果用户使用的是运行 Windows Mobile 或 Windows CE 的设备，则仍需使用 XenMobile 9。

XenMobile 10 和 10.1 支持的部分 Windows 设备：

- Windows Tablet 8.1
- HTC (Windows Phone 8.1)
- Nokia 920、925、1020、1520 (Windows Phone 8.1)
- Windows Tablet Surface Pro 3
- Windows Tablet Surface 2
- Windows Tablet RT

Windows Phone 7 通过 XenMobile Mail Manager 进行管理。 有关详细信息，请参阅安装 XenMobile Mail Manager。

Amazon

XenMobile 支持运行 Fire OS 3.0 及更早版本的 Amazon Kindle 设备，例如 Kindle Fire Phone 和 HD 8.9 (Zen561)，这些版本可运行基于 Android 的专有操作系统。 但请注意，MDX Toolkit 和 Worx 应用程序版本 10.3 不支持 Amazon Kindle 设备。

Symbian

XenMobile 10.3

XenMobile 10.3 不支持 Symbian。

XenMobile 10 和 10.1

下面是 XenMobile 10.1 和 10 支持的部分 Symbian 设备。 在 XenMobile 10 中，以下设备仅受设备管理模式支持：

- Symbian 3
- Symbian S60 5th Edition
- Symbian S60 3rd Edition, Feature Pack 2
- Symbian S60 3rd Edition, Feature Pack 1
- Symbian S60 3rd Edition
- Symbian S60 2nd Edition, Feature Pack 3
- Symbian S60 2nd Edition, Feature Pack 2

BlackBerry

BlackBerry 设备通过 XenMobile Mail Manager 进行管理。 有关详细信息，请参阅安装 XenMobile Mail Manager。

端口要求

May 05, 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。

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
443	用于回调 URL。	XenMobile	NetScaler Gateway
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 Receiver for	Internet	NetScaler Gateway

TCP 端口	说明	源	目标
	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
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
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、Worx Store 和移动应用程序管理 (MAM)。	XenMobile	XenMobile

TCP 端口	说明	源	目标
		NetScaler Gateway 设备	
4443	用于管理员通过浏览器访问 XenMobile 控制台。	访问点（浏览器）	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

打开 XenMobile 端口以管理设备

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。	XenMobile	Apple iTunes App Store (ax.itunes.apple.com) 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
443	用于到自动发现服务器的出站连接。	XenMobile	https://discovery.mdm.zenprise.com
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	用于与远程数据库服务器的连接（可选）。	XenMobile	SQL Server

TCP 端口	说明	源	目标
	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）
8443	用于 iOS 和 Windows Phone 设备注册。	Internet	XenMobile
		LAN 和 WiFi	

Auto Discovery Service 连接的端口要求

此端口配置可确保从 Worx Home for Android 10.2 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，请允许 ADS 连接跳过代理服务器。

对启用证书固定功能感兴趣的客户必须满足以下必备条件：

- **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
	54.225.219.53
	54.243.185.79
	107.22.184.230

	107.20.173.245
discovery.mdm.zenprise.com	184.72.219.144
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

FIPS 140-2 合规性

May 05, 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。

XenMobile 语言支持

May 05, 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。

Worx 应用程序语言支持

下表显示了 Worx 应用程序已翻译成的语言，X 指示语言支持。

用户界面语言	日语	简体中文	德语	法语	西班牙语	韩语	葡萄牙语	荷兰语	意大利语	丹麦语	瑞典语	希伯来语
Apple iPhone/iPad												
Worx Home	X	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X				
Android Phone/Tablet												
Worx Home	X	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X				

Windows Phone							
Worx Home	X	X	X		X	X	X
WorxMail	X	X	X		X	X	X
WorxWeb	X	X	X		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 控制台语言支持

下表概述了 XenMobile 控制台翻译状态，其中 X 指示语言可用性。

用户界面语言	**简体中文**	**德语**	**法语**	**韩语**	**葡萄牙语**
XenMobile 控制台	X	X	X	X	X

从右向左支持功能

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	

预安装核对表

May 05, 2016

可以使用此核对表记录安装 XenMobile 10 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。

基本网络连接

以下是 XenMobile 解决方案需要的网络设置。

	必备条件或设置	组件或功能	记录设置
	记录远程用户连接到的完全限定的域名 (FQDN)。	XenMobile 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	

	必备条件或设置	组件或功能	记录设置
	● 为 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	

Licensing

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，请参阅安装 NetScaler Gateway 许可证。	NetScaler Gateway	

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

证书

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	

端口

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	

数据库

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	

Active Directory 设置

	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	

	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	

XenMobile 与 NetScaler Gateway 之间的连接

	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	

用户连接：访问 XenDesktop、XenApp 和 Worx Home

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

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	

已知问题

May 05, 2016

下面是 XenMobile 10.0 的已知问题。

有关本版本中已修复问题的列表，请参阅 http://support.citrix.com/article/CTX141722。

- 将 iOS 设备从 iOS 7 更新到 iOS 8 并重新启动后，Worx Home 可能会显示灰色占位符，而非图标。这是第三方问题。[#502879]
- 注册期间，iOS 设备可能会在移动设备管理 (MDM) 配置文件安装过程中或之后遇到错误。用户可能会在运行 iOS 8.1 的设备上看到“Cocoa error 4097”（Cocoa 错误 4097），或者在运行早期版本的 iOS 的设备上看到“Profile cannot be decrypted”（配置文件无法解密）。如果发生上述情况，用户应尝试重新注册。在某些情况下，可能需要多次尝试。[#507948]
- 无法在 XenMobile 10 的 USER 组类中调用 checkUserPassword 和 addGroup SOAP。用户 API 更改会显示在数据库中，但不会显示在设备用户界面上。[#511551, #511822]
- 无法从 XenMobile Web 控制台更改交付组资源的部署顺序。如果要控制部署顺序，请按照 XenMobile 使用的部署协议重命名您的资源：数字（1、2、3、...）、大写字母（A、B、C、...）和小写字母（a、b、c、...）。系统会先部署名称以 24 开头的资源，再部署名称以 WM 开头的资源，最后部署名称以tw开头的资源。[#512566]
- 如果启用了“过滤成人内容”限制，则会在 Windows Phone 8.1 设备中禁用 SafeSearch 并将其设置为中等。[#513605]
- 部署 Windows 8.1 Tablet 设备策略时，在 XenMobile 从设备收到已执行策略的确认信息之前，您可能会在 XenMobile 控制台的设备详细信息中的部署选项卡上看到这些策略。[#514749]
- 如果用户在取消注册后很短时间内重新注册，则在重新注册设备时，注册可能会失败。[#516567]
- 有时，当用户在 Worx Home 中重新注册时，XenMobile 将显示缓存的 SSL 会话，用户会再次看到注册屏幕。此时，用户应重新注册。[#517301]
- 如果使用父域和子域中的 Active Directory 组通过 AND 运算符定义交付组，则应用程序枚举会失败。为避免这种情况，请在定义交付组时使用 OR 运算符。[#518084]
- 如果在用于上载文件（证书、PDF、字体等）的 XenMobile 控制台中配置设置或策略，并稍后查看此策略或设置的详细信息，不会显示文件名。[#519552]
- XenMobile 不支持在移动应用程序管理 (MAM) 模式下对 iOS 和 Android 设备使用 PIN 进行身份验证。如果在 XenMobile 控制台中将此模式配置为默认值，则用户必须在 Worx Home 中输入凭据两次。[#519572]
- 如果在 XenMobile 控制台中禁止将 AllUsers 组用作交付组，则不属于任何交付组的用户将无法注册设备，但可以登录到可以访问子组的门户。[#521393]
- 如果将应用程序部署为可选应用程序，适用于 Windows Phone 8.x 的 Worx Home 在移动设备管理模式下，仅支持来自公共应用商店中的这些应用程序。如果根据需要将这些应用程序添加到交付组，则它们不会显示在 Worx Home 中。[#521524]
- 系统将显示“基于角色的访问控制 (RBAC) 角色信息”页面，可使您编辑默认管理模板。尽管您对 RBAC 模板字段等内容做出了更改，但这些更改不会保存到此管理模板。此管理模板无法进行编辑。[#521540]
- 在 iOS 设备上，当用户在 Worx Home 中注册并配置其 ShareFile 帐户时，SAML 令牌的置备可能无法同步。解决方法是，用户可以注销并重新登录到 Worx Home，然后登录到 ShareFile 应用程序，以便重新触发 SAML 令牌请求。[#521934]
- 在大多数设备上，如果运行 Android 设备的用户轻按 Menu（菜单）图标，则会显示 Accept and Decline（接受和拒绝）菜单选项，从而使用户可以继续完成注册过程。但是，在一些运行 4.0 之前版本的操作系统的设备（如 Samsung Tablet GT-P7510）上，菜单图标不会显示在默认视图的“条款和条件”页面上，用户无法完成注册过程。解决方法是，您可以将设备从“条款和条件”部署中排除。[#524039]
- 如果 XenMobile 控制台上信号页面（配置 > 设置 > 更多 > 信号）中的默认应用商店名称已更改，则 iOS 设备上的 Worx Home 将无法连接到 Worx Store。默认设置为应用商店。如果更改了此设置，登录期间发现服务将失败，并且找不到 Worx Store。为了避免此问题，请将信号页面上的应用商店名称设置为应用商店。[#523306]

- 在具有负载平衡和 SSL 卸载的 XenMobile 配置中，为了在用户安装 WorxWeb 并打开服务提供商启动的应用程序时可以使用单点登录 (SSO)，在配置 SAML 应用程序时，对 XenMobile 服务器的所有引用都必须指向端口 8443，而非端口 443。[#528680]
- 创建 Samsung KNOX 通行码策略时，在配置 Lock device after (minutes of activity)（锁定设备间隔(活动分钟数)）设置后，尽管控制台中的设置会使用分钟作为单位，服务器仍会强制以秒为单位进行锁定。[#531204]
- 无法在 XenMobile 10 中配置自己的 SAML 服务和身份提供程序来对用户及其设备进行身份验证。[#530892]
- 无法在 XenMobile 控制台中添加单个黑莓或 Windows 设备。[#532844]
- 如果配置的SAML应用程序名称带有数字符号 (#)，则 Worx Home 中的单点登录 (SSO) 功能不起作用，并会显示一条错误消息。[#533078]
- 在 XenMobile 控制台中添加 Generic PKI (GPKI) 实体时，无法在配置期间测试 Web 服务描述语言 (WSDL) URL 适配器连接。[#533871]
- Windows 平板电脑密码策略不会在设备中立即生效，强制更新为最小密码长度时会出现一些不一致的情况。这是第三方问题。[#534088]
- 用户在移动设备管理 (MDM) 模式下注册 iOS 设备时，XenMobile 控制台中管理 > 设备页面上用于查找和跟踪设备的安全选项不会立即显示出来。经过短暂延迟后，此选项才会显示出来。[#534672]
- 如果配置的 StoreFront Delivery Controller 显示名称中包含特殊字符（如句点 (.)），则用户无法通过 Worx Home 使用 XenApp 订阅和打开应用程序。此时将显示错误“Cannot complete your request”（无法完成您的请求）。解决方法是，从名称中删除特殊字符。[#535497]
- 在添加和配置应用程序时，如果在 XenMobile 控制台的 Excluded devices（排除的设备）字段中键入一个值，则此应用程序不会显示在适用于 iOS 8 之前的 iOS 设备的 Worx Store 中。解决方法是，您可以配置一条部署规则，以指定可安装此应用程序的设备。[#537631]
- 如果使用 XenMobile 在非默认端口 443 上配置 NetScaler Gateway 连接，则在 iOS 设备上进行移动应用程序管理 (MAM) 注册会失败，在 Windows 设备上注册 Worx Home 也会失败。[#537368]
- $、@ 和 " 等特殊字符在安装 XenMobile 10 时使用的 CLI 的密码中以及分配给证书的密码中不被识别；特殊字符及其后面的所有字符将被忽略，登录失败。安装后，无法将 CLI 密码更改为包含特殊字符。[#541997] [#542436]
- 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。[#608213]

下面是 XenMobile Mail Manager 10.0 中的已知问题。

- 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”。

安装 XenMobile

May 05, 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，请参阅 XenMobile 10 的系统要求和 XenMobile 10 安装前核对表。

注意：请务必使用正确的时间配置虚拟机管理程序，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。

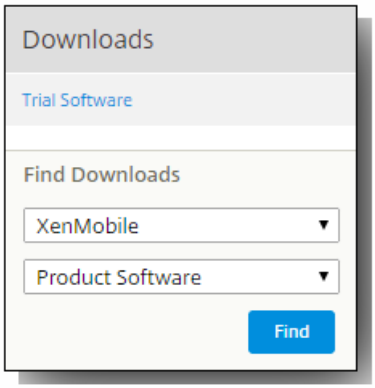
Hyper-V 必备条件：在 Hyper-V 上安装 XenMobile 之前，必须执行以下操作。有关详细信息，请参阅 Hyper-V 文档。

- 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。

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。

下载 XenMobile 产品软件

可以从 Citrix Web 站点下载产品软件。您需要登录该站点，然后单击 Citrix Web 页面上的 Downloads（下载）链接。随后可以选择要下载的产品和类型。例如，下图显示了从此列表中选择的 XenMobile 和产品软件。



单击 Find（查找），此时将显示一个列出可用下载的页面，最新版本显示在列表顶部：可以从可用选项列表中选择软件。

下载 XenMobile 的软件

1. 转至 Citrix Web 站点。
2. 单击我的帐户并登录。
3. 单击 Downloads（下载）。
4. 在 Find Downloads（查找下载资源）下，从产品列表中，单击 XenMobile。

5. 在 File Downloads（文件下载）下面，从下载类型列表中，单击 Product Software（产品软件），然后单击 Find（查找）。
6. 在 XenMobile Product Software（XenMobile 产品软件）页面上，单击要下载的 XenMobile 10.0 版。
7. 在 XenMobile 10.0 Edition 页面上，单击 Download（下载），下载相应的虚拟映像，以便在 XenServer、VMware 或 Hyper-V 上安装 XenMobile。
8. 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. 单击我的帐户并登录。
3. 单击 Downloads（下载）。
4. 在 Find Downloads（查找下载资源）下，从产品列表中，单击 NetScaler Gateway。
5. 在 File Downloads（文件下载）下面，从下载类型列表中，单击 Product Software（产品软件），然后单击 Find（查找）。
   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。
6. 在“NetScaler Gateway”页面上，展开 10.5(4)。
7. 单击要下载的设备软件版本。
8. 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。
9. 按照屏幕上的说明下载软件。

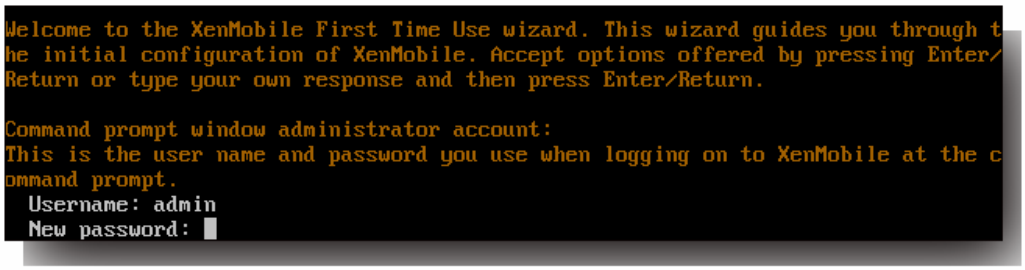
为首次使用配置 XenMobile

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、默认网关和 DNS 服务器。
2. 登录 XenMobile 管理控制台并按照初始登录屏幕上的步骤操作。

在命令提示窗口中配置 XenMobile

1. 将 XenMobile 虚拟机导入 Citrix XenServer、Microsoft Hyper-V 或 VMware ESXi。 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，在命令提示窗口中创建 XenMobile 的管理员帐户。



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. 请提供以下信息：
   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：此图片中显示的地址并不可用，仅作为示例提供。

5. 类型y以通过生成随机密码增强安全性，或者键入n提供自己的密码。Citrix 建议键入y以生成随机密码。密码是加密密钥（用于保护敏感数据）保护措施的一部分。密码哈希存储在服务器文件系统中，用于在加密数据和解密数据过程中提取密钥。条目密码。

注意：如果打算扩展环境并配置额外的服务器，应提供您自己的密码。如果选择随机密码，将无法查看密码。

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。

7. 配置数据库连接。 数据库可以是本地数据库或远程数据库。 被询问 Local or remote（本地还是远程）时，键入r 或l。
   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。

```
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:
```

重要：PostgreSQL 的默认端口为 5432。

```
Database connection:
  Local or remote [l/r]: l
```

注意：此图片中显示的地址并不可用，仅作为示例提供。

8. 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。

重要：除非完全重新安装服务器，否则无法更改 FQDN。

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

9. 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。

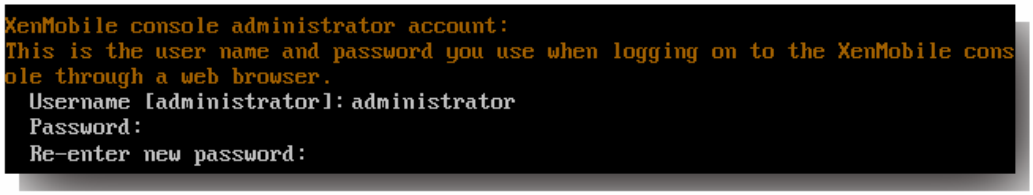
```
  HTTP [80]: 80
  HTTPS with certificate authentication [443]: 443
  HTTPS with no certificate authentication [8443]: 8443
  HTTPS for management [4443]: 4443
```

10. 系统会要求您为所有公钥基础结构 (PKI) 服务器证书提供密码，并向您提供为每个证书使用相同密码的选项。 有关 XenMobile PKI 功能的详细信息，请参阅在 XenMobile 中上载证书。
    重要：如果打算将 XenMobile 的节点或实例群集在一起，需要为后续节点提供相同的密码。

```
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:
```

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。

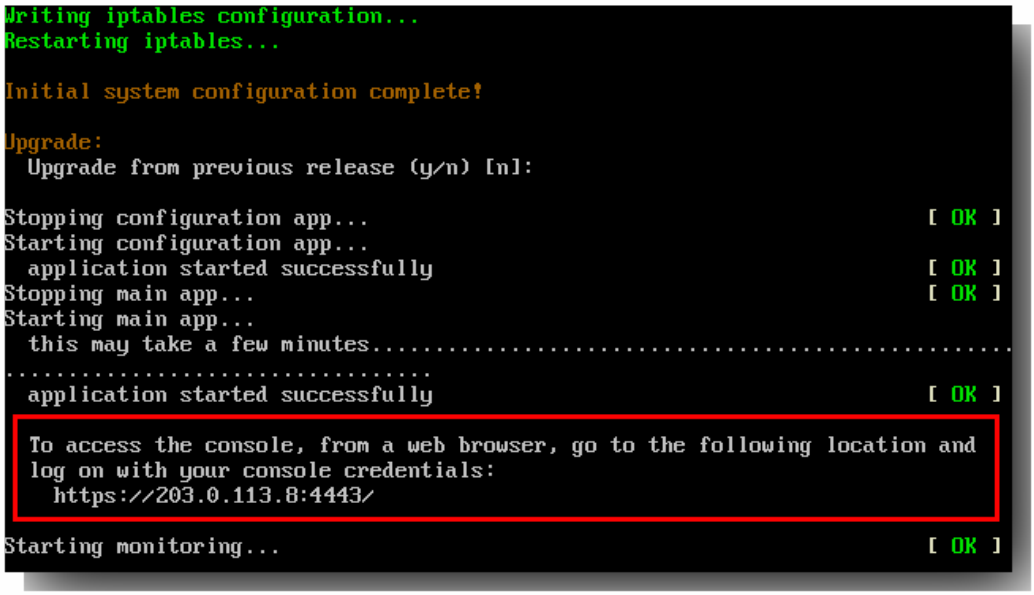
11. 创建管理员帐户以便使用 Web 浏览器登录 XenMobile 控制台。 请务必记住这些凭据，供稍后使用。



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。

12. 当询问是否为升级时，请键入n，因为这是全新安装。

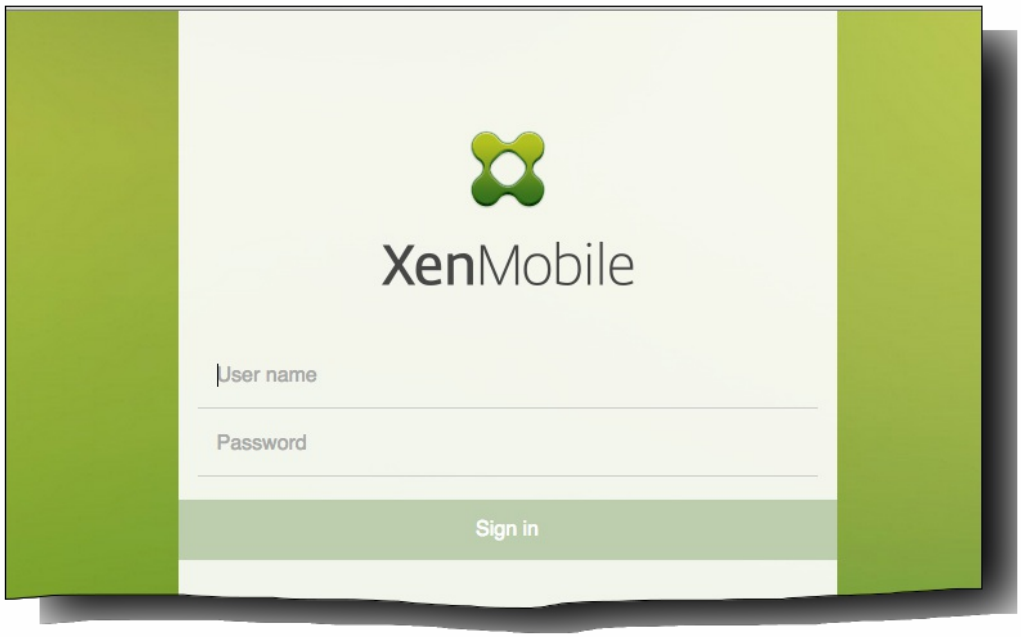
13. 完整复制屏幕上显示的 URL，并在 Web 浏览器中继续此初始 XenMobile 配置。



在 Web 浏览器中配置 XenMobile

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

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“许可”页面。
4. 配置许可证。 XenMobile 附带的是评估许可证，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，请参阅许可使用 XenMobile。
   重要：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。
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：SSL 侦听器证书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 Gateway 的详细信息，请参阅 NetScaler Gateway 和 XenMobile。
   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。
   注意：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。

在 XenMobile 中配置 FIPS

May 05, 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。

配置 FIPS 模式

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）。

导入证书

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

SQL 必备条件

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

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

    a.复制用于 SQL Server 服务的登录帐户信息。

    b.在 SQL Server 上打开 MMC.exe。

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

    d.单击**确定**。

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

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

    g.在**组或用户名**下，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。

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。

在初始 FIPS 配置过程中导入根证书

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

- 启用 FIPS：是
- 上载根证书：是
- 复制 (c) 或导入 (i)：i
- 输入 HTTP URL 以导入：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。

XenMobile 10 MDM 升级工具

May 05, 2016

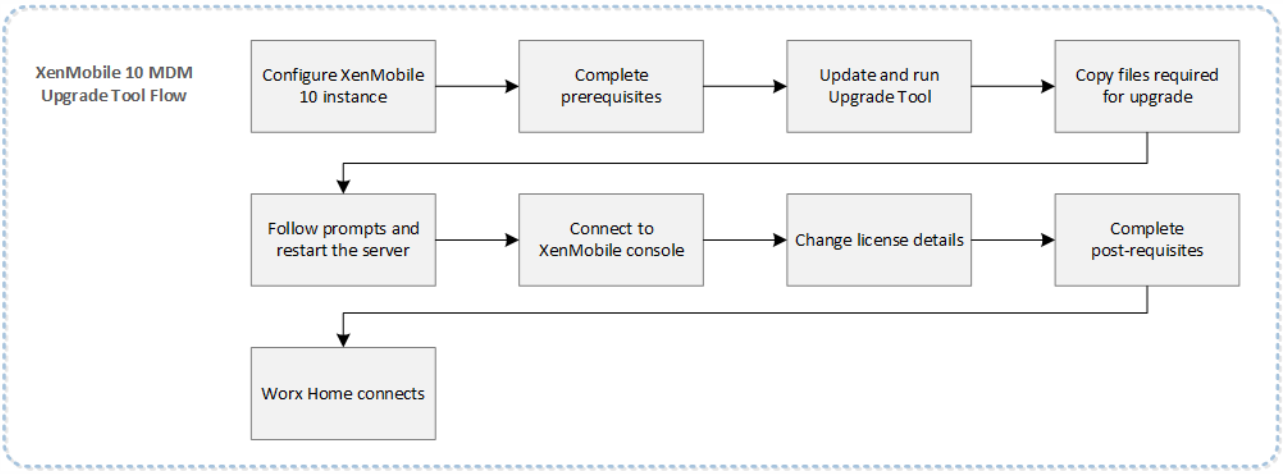
> **注意**
>
> Citrix 建议您使用最新版本的升级工具。可用的最新版本允许您在一个工具中更新 XenMobile 9.0 环境的 MAM、MDM 和 Enterprise 模式。您可以在 Citrix.com 下载页面找到该升级工具。

可以使用 XenMobile 10 MDM 升级工具从 XenMobile 9.0 升级到 XenMobile 10。支持使用该工具从 XenMobile MDM Edition 部署进行升级。

重要：不支持使用该工具从 XenMobile App Edition 或 XenMobile Enterprise Edition 进行升级。同样，不能使用该工具从 XenMobile 8.6 或 8.7 升级到 XenMobile 10。此外，如果 XenMobile 9.0 上启用了多租户控制台 (MTC)，则不能将 MTC 迁移到 XenMobile 10。
如果您的 XenMobile 9.0 安装基于命名 SQL 实例，则需要按照专门针对此类情况的步骤进行操作。有关详细信息，请参阅支持命名 SQL 实例。

升级工具在 XenMobile 10 虚拟机中构建。在 XenMobile 10 的初始安装过程中，可以通过命令行控制台启用一次性向导。

下图说明了从 XenMobile 9.0 升级到 XenMobile 10 所需执行的基本步骤。



开始迁移到 XenMobile 10 之前，请参阅必备条件和已知问题。

升级工具执行的操作

XenMobile 10 MDM 升级工具将配置和用户数据从 XenMobile 9.0 服务器迁移到 XenMobile 10 的新实例（具有相同的完全限定的域名 (FQDN)）。

您可以选择试用升级或执行全面的生产升级。在工具中选择 Test Drive（试用）时，仅将配置数据迁移到 XenMobile 10；不迁移任何设备或用户数据。使用此选项可以比较 XenMobile 9.0 和 XenMobile 10，而不会影响生产环境。

在工具中选择 Production Upgrade（生产升级）时，将迁移所有配置、设备和用户数据。升级后登录到 XenMobile 10 控制台

时，您会看到从 XenMobile 9 迁移的所有用户和设备数据。

注意：这不是原位迁移，所有数据在迁移过程中*复制*（而非移动）到 XenMobile 10。XenMobile 9.0 中的所有数据保持不变，直至将 XenMobile 10 服务器移动到生产环境中。当用户连接到生产环境中的 XenMobile 10 时，如果由于某种原因要恢复为 XenMobile 9.0，这些用户必须在 XenMobile 9.0 中重新注册。
生产升级成功后，要将 XenMobile 10 移动到实时生产中，必须执行以下操作：

1. 更新 DNS 条目以将 XenMobile 9.0 FQDN 映射到新的 XenMobile 10 服务器 IP。
2. 如果 NetScaler 是负载平衡的 XenMobile Device Manager 服务器，则需要将 XenMobile 9.0 Service 切换到 XenMobile 10 Service。

升级工具不执行的操作

使用升级工具时，**不**会将以下信息迁移到 XenMobile 10：

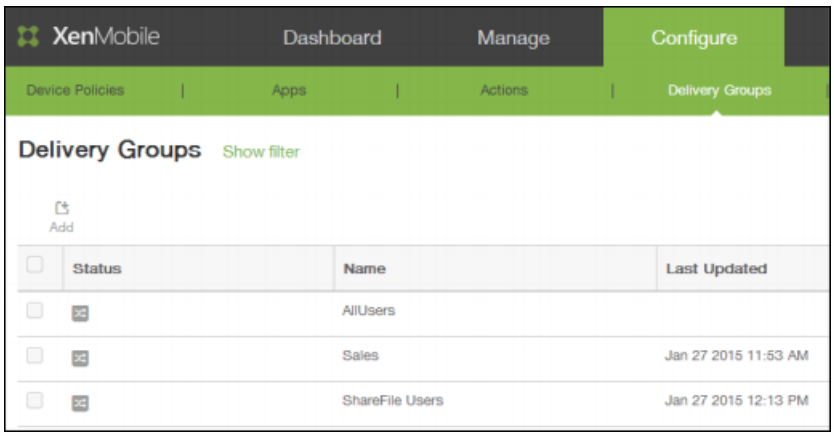
- 许可信息。
- 报告数据。
- 自动化操作。
- 服务器组策略和关联的部署。
- MSP 组。
- 与 Windows CE 和 Windows 8.0 相关的策略和软件包。
- 未使用的部署软件包；例如未将任何用户或组分配给部署软件包时。
- migration.log 文件中所述的其他任何配置或用户数据。
- CXM Web（由 Citrix WorxWeb 替代）。
- DLP 策略（由 Citrix Sharefile 替代）。
- 自定义 Active Directory 属性。
- 如果已配置多个品牌设计策略，则不会迁移品牌设计策略。XenMobile 10 支持一个品牌设计策略；您必须在 XenMobile 9.0 中保留一个品牌设计策略以成功迁移到 XenMobile 10。
- XenMobile 9.0 的 auth.jsp 文件中用于限制访问控制台的任何设置。XenMobile 10 中的控制台访问限制是可在命令行界面配置的防火墙设置。

还请注意 XenMobile 10 中的以下变更：

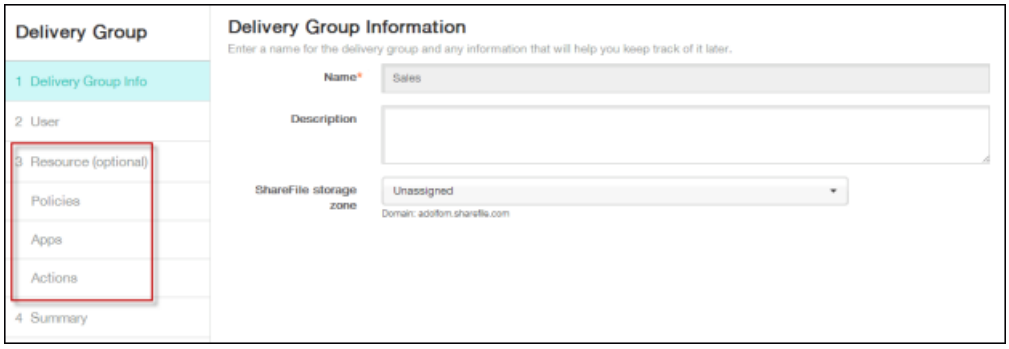
- XenMobile 10 不支持分配给本地组的 Active Directory 用户。
- 本地组层次结构已展开。

XenMobile 10 中的术语变更

请注意，升级之后，Device Manager 中的部署软件包现在称为交付组，如下图所示。有关详细信息，请参阅管理交付组。



在交付组中，您可以查看需要资源的用户组所需的 MDM 策略、操作和应用程序。

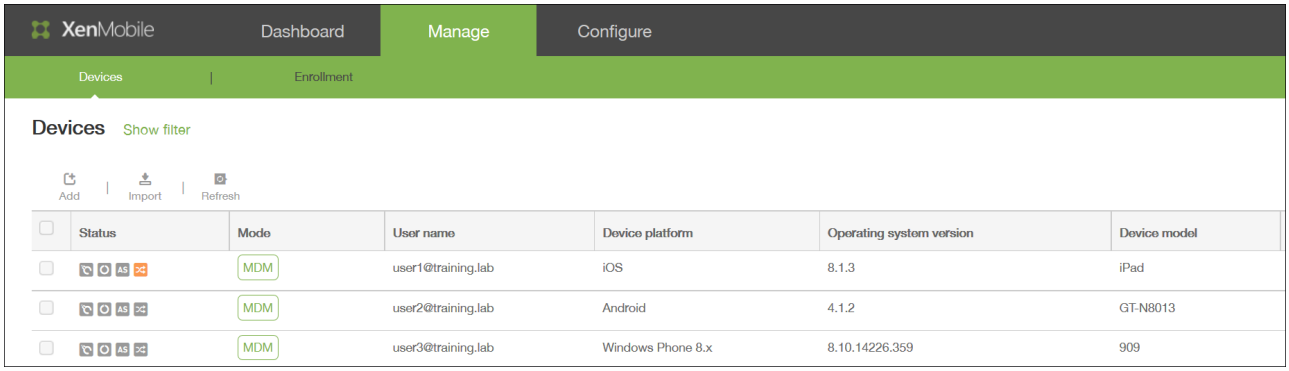


升级后的设备注册

升级到 XenMobile 10 后，用户不需要重新注册其设备。用户的设备应根据检测信号时间间隔自动连接到 XenMobile 10 服务器。

如果要立即将设备连接到 XenMobile 10，请在设备上使用 WorxHome > 设备信息 > 刷新策略。

用户设备连接后，检查以确保在 XenMobile 控制台中看到设备，如下图所示。



必备条件

May 05, 2016

您需要具备以下必备条件才能运行 XenMobile 10 MDM 升级工具。

Citrix 许可证服务器

请确保安装 11.12.1 Citrix 许可证服务器（在 Citrix Licensing 页面中提供）并使用最新的仅 V6 MDM 许可证配置该服务器。请确保许可服务器端口 27000 和 7279 对该服务器开放。此步骤至关重要，可阻止无意中将用户设备升级到 XenMobile Enterprise 模式，否则可能会导致许可违规，还会强制用户重新注册其设备。

数据库

只能在相同类型的数据库之间进行迁移。例如：

是否支持

- PostgreSQL 到 PostgreSQL
- MSSQL 到 MSSQL

不支持

- MSSQL 到 PostgreSQL
- PostgreSQL 到 MSSQL

在数据迁移过程中，XenMobile 需要能够访问在 XenMobile 9.0 Device Manager 上实施的数据库解决方案。例如，必须打开以下端口：

- 对于 Microsoft SQL Server，默认端口为 1433。
- 对于 PostgreSQL，默认端口为 5432。

要允许对 PostgreSQL 进行远程连接，必须完成以下步骤：

1. 打开文件 pg_hba.conf，找到以下行："host all all 127.0.0.1/32 md5"
2. 附加新行 hostall all[XMS address/external address]/32 md5
3. 保存该文件。
4. 停止并启动服务。
5. 找到并打开 postgresql.conf 文件，然后将此行从：
   "#listen_addresses = 'localhost'"

   更改为

   "listen_addresses = '*'"

   注意：必须取消注释该行。通过仅允许 XenMobile 9.0 和 XenMobile 10 服务器 IP 访问 PostgreSQL 数据库 (listen_addresses = '10.x.x.1,10.x.x.2') 可对此进行限制。
6. 停止并启动 PostgreSQL 服务以使更改生效。
7. 确保 XMS 和数据库能够相互通信。（此操作还将检查数据库是否能够接受远程连接。）

如果已将自定义端口分配给数据库解决方案，则必须确保允许使用该端口，并且在保护 XenMobile 9.0 Device Manager 的防火墙中处于打开状态。这样可以使 XenMobile 10 连接到数据库并迁移所需信息。

外部 SSL 证书

外部 SSL 证书必须满足如何配置外部 SSL 证书中列出的条件。请务必在开始迁移之前检查pki.xml，以确保 SSL 证书满足这些条件。

管理员帐户用户名

用于登录到 XenMobile 10 控制台的管理员帐户只能包含小写字母；如果帐户包含大写字母，迁移后您将无法登录到 XenMobile 10 控制台。全部使用小写字母创建管理员用户帐户并启用所有权限，以便您可以在迁移后使用该帐户登录到 XenMobile 10 控制台。

带有特殊字符的部署软件包名称

迁移 XenMobile 9.0 中包含特殊字符（!、$、()、#、%、+、*、~、?、|、{} 和 []）的部署软件包名称，但在迁移后不能对 XenMobile 10 中的交付组进行编辑。此外，如果在 XenMobile 9.0 中创建的本地用户和本地组包含左方括号 ([)，则会导致在 XenMobile 10 中创建注册邀请时出现问题。迁移之前，请删除部署软件包名称中的所有特殊字符以及本地用户名和本地组名称中的左方括号。

从 XenMobile 9.0 Device Manager 复制文件

假定 Device Manager 已安装在默认位置 (C:\Program Files(x86)\Citrix\XenMobile Device Manager\tomcat) 中，则将以下文件复制到临时文件夹中：

从 C:\Program Files (x86)\Citrix\XenMobile Device Manager\tomcat\conf 文件夹：

- server.xml
- https.p12
- cacerts.pem.jks
- pki-ca-root.p12
- pki-ca-devices.p12
- pki-ca-servers.p12

注意：如果在运行 Device Manager 的服务器上使用了自定义服务器 SSL 服务器证书 (.p12)，请务必将该证书（而非 https.p12）复制到临时文件夹。
从 C:\Program Files (x86)\Citrix\XenMobile Device Manager\tomcat\webapps\zdm\WEB-INF\classes\ 文件夹，将以下文件复制到同一临时文件夹中：

- ew-config.properties
- pki.xml
- variables.xml

复制上述的所有文件后，打开临时文件夹并压缩这些文件；不要压缩该文件夹，仅压缩文件。将在升级过程中上载压缩的文件。

了解已知问题并满足所有必备条件后，开始进行升级。有关详细信息，请参阅启用和运行 XenMobile 10 MDM 升级工具。

已知问题

May 05, 2016

XenMobile 10 MDM 升级工具存在以下已知问题：

- XenMobile 锁定限制值不会迁移。迁移后，需对值进行重置。[#545770]
- 基于角色的访问控制 (RBAC) 角色中的选项没有完全迁移。迁移后，需检查 RBAC 角色，并进行必要的调整。[#543183]
- 日志设置不会迁移。迁移后，需要在 XenMobile 控制台重新配置日志设置。[#541869]
- 在进行多个 LDAP 配置时，如果只迁移其中一个支持嵌套组的 LDAP 配置，则在迁移后，配置的所有 LDAP 都会启用嵌套组支持。此外，在服务器启动期间，所有 LDAP 服务器都会发生组同步。[#540713]
- 如果 Web 内容过滤器设备策略包含无 HTTP/HTTPS 的 URL，则该 URL 会在用户对其进行编辑然后取消操作时删除。迁移后，需确保所有 URL 都包含 HTTP 或 HTTPS，以防其在取消编辑操作时被删除。[#540025]
- 在多个具有不同规则的包中包含策略、应用程序或操作时，部署规则不会迁移。这种行为是有意为之。[#539517]
- 在成功迁移后，如果 XenMobile 9.0 管理员用户名包含一个大写字符，该管理员将无法登录 XenMobile 10 控制台。在迁移之前，要创建全部为小写字母的管理员用户帐户并启用所有权限，这样在迁移后才可以使用该帐户登录 XenMobile 10 控制台。[#547422]
- 如果在 XenMobile 9 上启用了多租户控制台 (MTC)，则不能将 MTC 迁移到 XenMobile 10。[#549969]
- 在 XenMobile 9.0 中创建的超级管理员角色不能在 XenMobile 10 中迁移多项设置和分配权限。迁移后，在 XenMobile 10 控制台上，转到配置 > 设置 > 基于角色的访问控制，然后重新创建具有 XenMobile 10 管理角色权限的 XenMobile 9.0 超级管理员角色。[#553079]

- 迁移后，无法编辑 XenMobile 9.0 中创建的包含特殊字符（!、$、()、#、%、+、*、~、?、|、{} 和 []）的部署包名称。此外，如果在 XenMobile 9.0 中创建的本地用户和本地组包含左方括号 ([)，则会导致在 XenMobile 10 中创建注册邀请时出现问题。迁移之前，请删除部署软件包名称中的所有特殊字符以及本地用户和本地组名称中的左方括号。[#538639]

启动和运行 XenMobile 10 MDM 升级工具

May 05, 2016

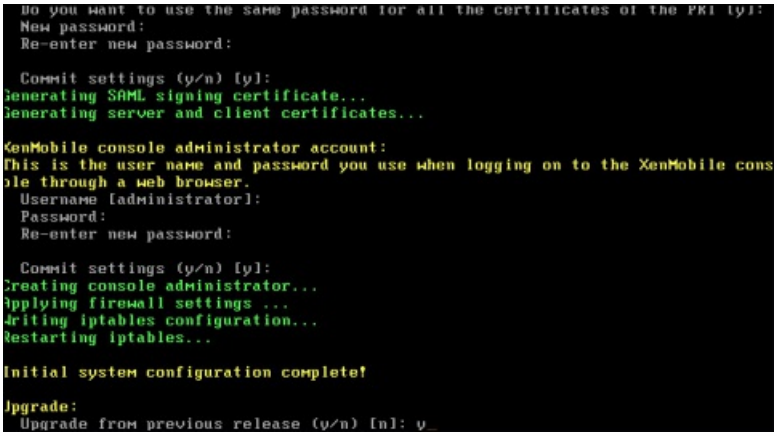
以下为从 XenMobile 9.0 升级至 XenMobile 10 需要遵循的基本步骤：

1. 使用命令行控制台配置 XenMobile 10 实例。
2. 满足所有升级工具必备条件。 有关详细信息，请参阅必备条件。
3. 将升级工具更新到最新版本。
   重要：系统重新启动后，清除浏览器缓存。
4. 在 Firefox 或 Chrome 浏览器中启动升级工具。
5. 将复制的 XenMobile 9.0 文件上载到升级工具。
6. 输入 XenMobile 9.0 证书密码。
7. 允许升级工具运行。
8. 重新启动 XenMobile 10 服务器。
9. 登录到 XenMobile 10 控制台。
10. 在 XenMobile 10 上配置许可证，以允许用户进行连接。
11. 对于生产升级，需要为 XenMobile 更改外部 DNS，以指向新的 XenMobile 10 服务器。
12. 对于生产升级，如果在使用负载平衡 NetScaler，则要删除 XenMobile 9.0 服务器的 IP，并添加 XenMobile 10 服务器的 IP。

安装 XenMobile 10 的实例并启用升级工具

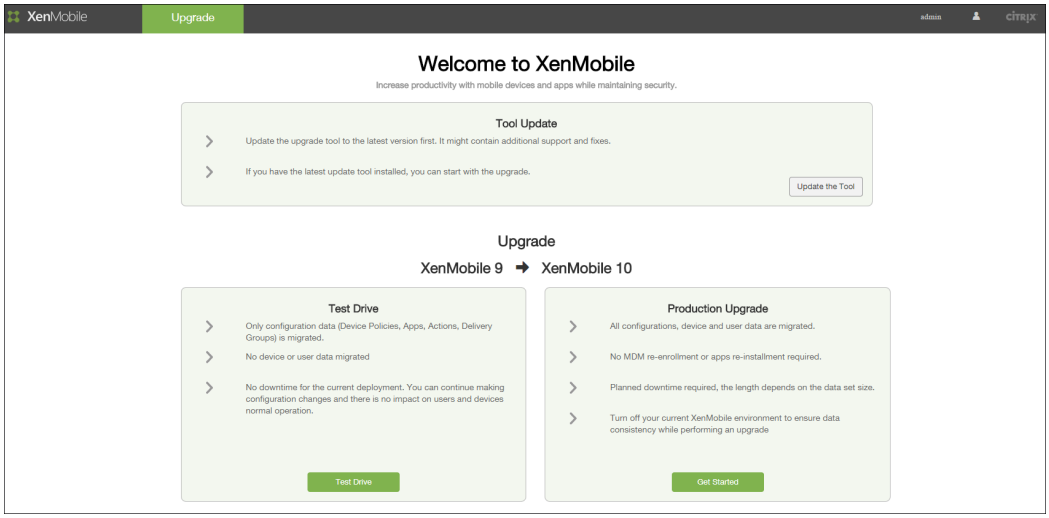
您可在 XenMobile 10 初始安装期间通过命令行控制台启用升级工具，如下图所示。

重要：如果要生成系统快照，请在 XenMobile 10 初始配置之后、访问升级工具*之前*进行。



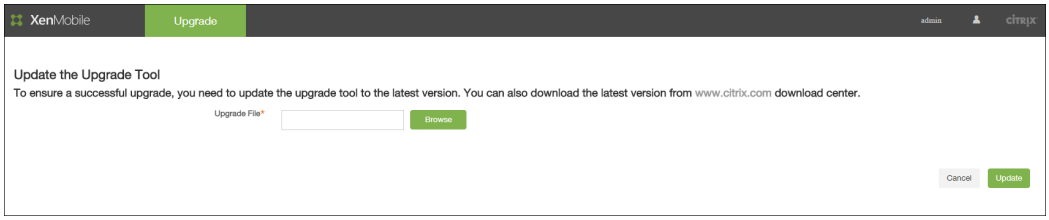
如果您键入 **y** 以进行升级，XenMobile 10 会启用一次性升级工具。然后，您可通过 https:///uw/ 访问升级工具。

提示：Citrix 建议您使用 Firefox 或 Chrome 浏览器访问升级工具；建议不要使用 Internet Explorer。
迁移到新服务器时，请确保新服务器的主机名与从其迁移的服务器的主机名匹配。此匹配可以确保 Worx Home 能够使用与 Worx Home 连接到 XenMobile 9.0 时所用的相同主机名连接到 XenMobile 10。这样，用户就不需要在 XenMobile 10 中重新注册。



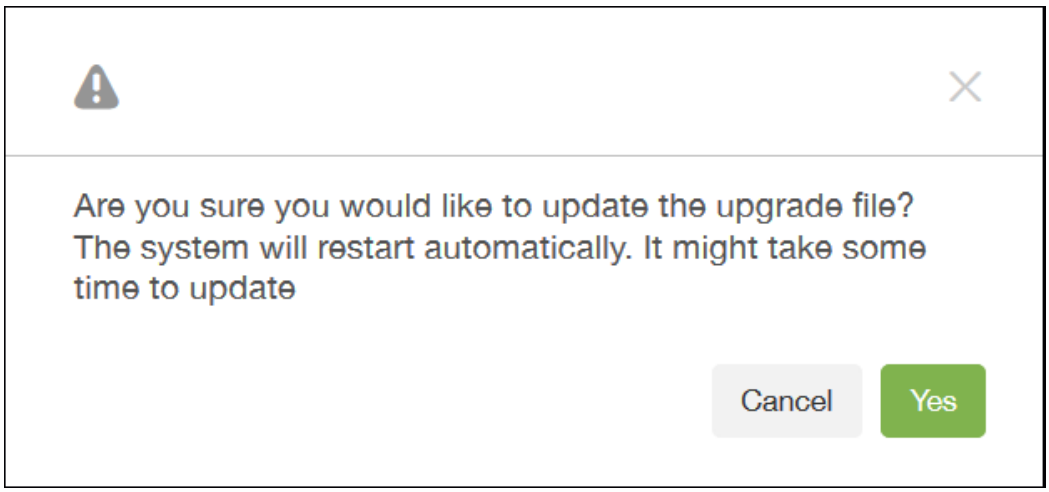
更新升级工具并启动迁移

您可在 XenMobile download（XenMobile 下载）页面找到升级工具的更新。对于 MDM 迁移，必须使用从 Citrix.com 下载的最新工具。



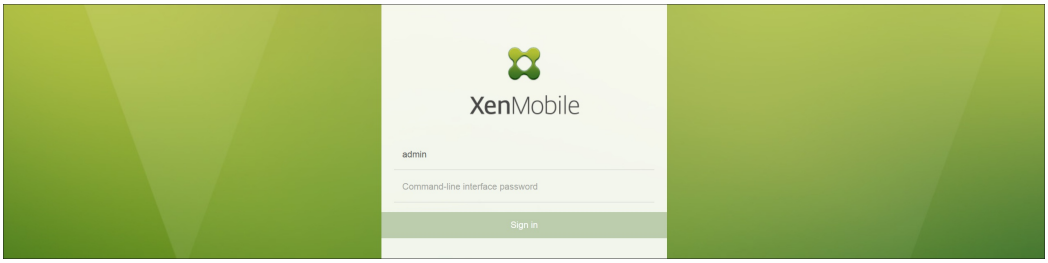
以下确认启动更新过程消息将显示。

注意：单击是后，不会出现可视化的进度指示条，但是您可以查看命令行界面，了解系统何时重新启动。更新大约需要 30 秒。

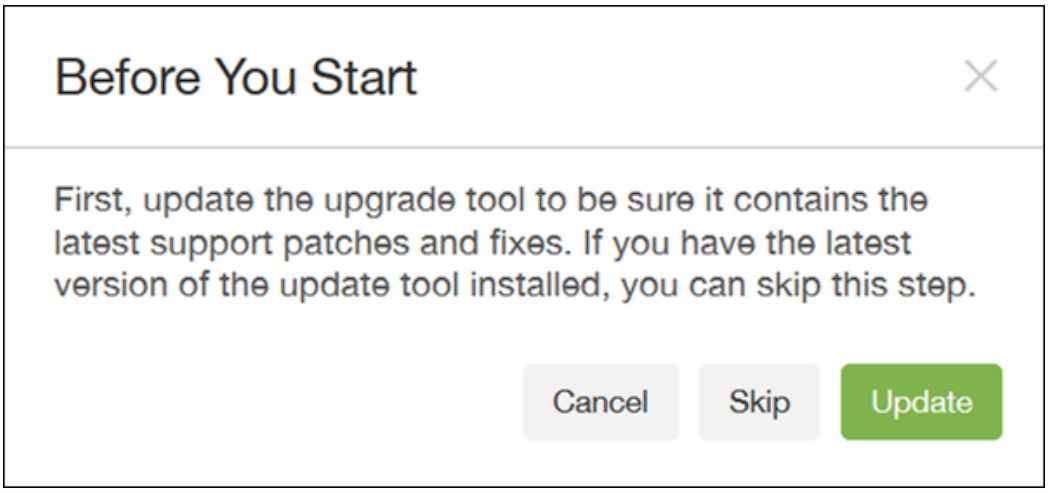


注意：

- 系统重新启动后，请在访问升级工具 URL (https:///uw) 之前再次清除浏览器缓存。
- 如果您不使用默认的 HTTPS 通信 (443) 端口，请访问升级工具 URL (https://:/uw)。

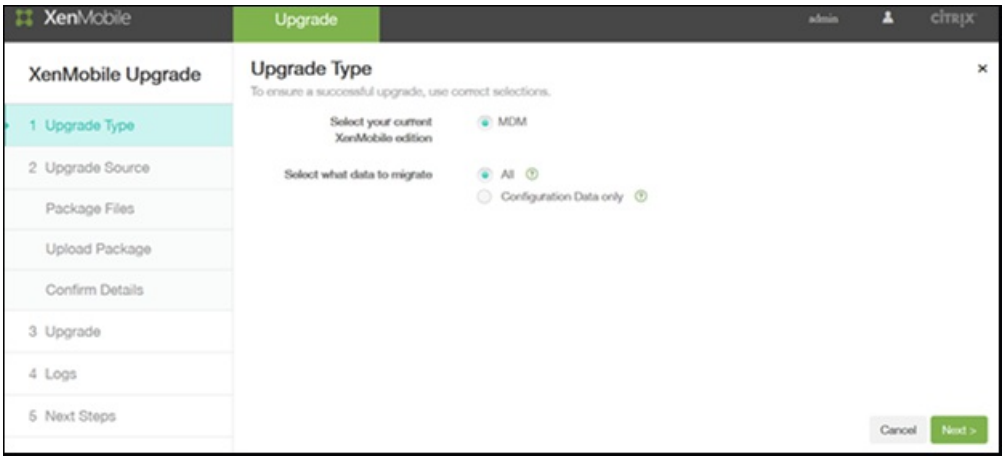


在此情况下，登录到升级工具后，由于您已经更新了升级工具，因此可以单击**跳过**。



选择 Test Drive（试用）或 Production Upgrade（生产升级），然后继续进行迁移。

在升级工具打开后，您可以选择迁移所有数据或仅迁移配置数据。如果选择 Configuration Data only（仅配置数据），用户必须重新注册其设备。单击下一步，必须将您复制并压缩的文件上载到临时文件夹中。

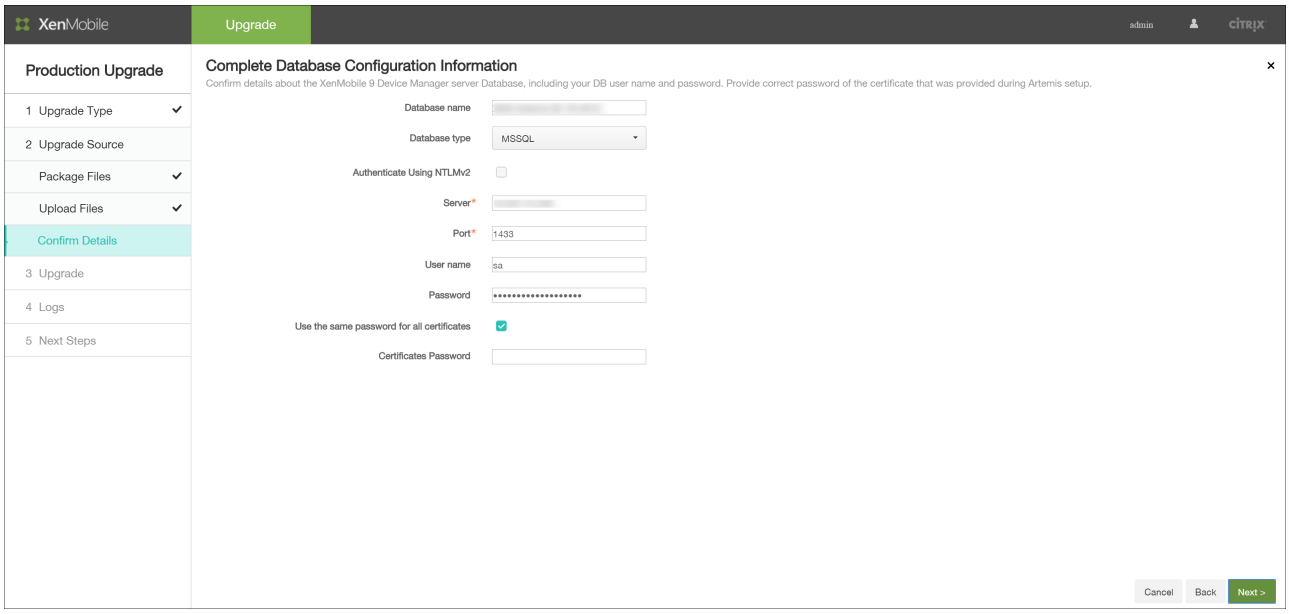


上载完成后，单击下一步。

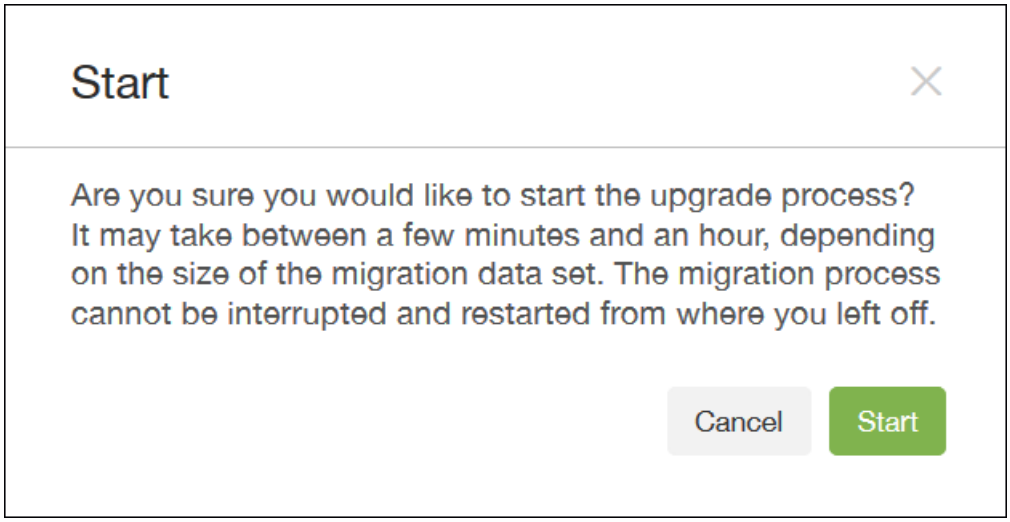
在迁移 PostgreSQL 数据库并且服务器的名称是 "localhost" 时，必须将 "localhost" 更改为服务器 IP 地址。

确认从 XenMobile 9.0 Device Manager 中收集到的信息是正确的。您还必须输入证书密码。

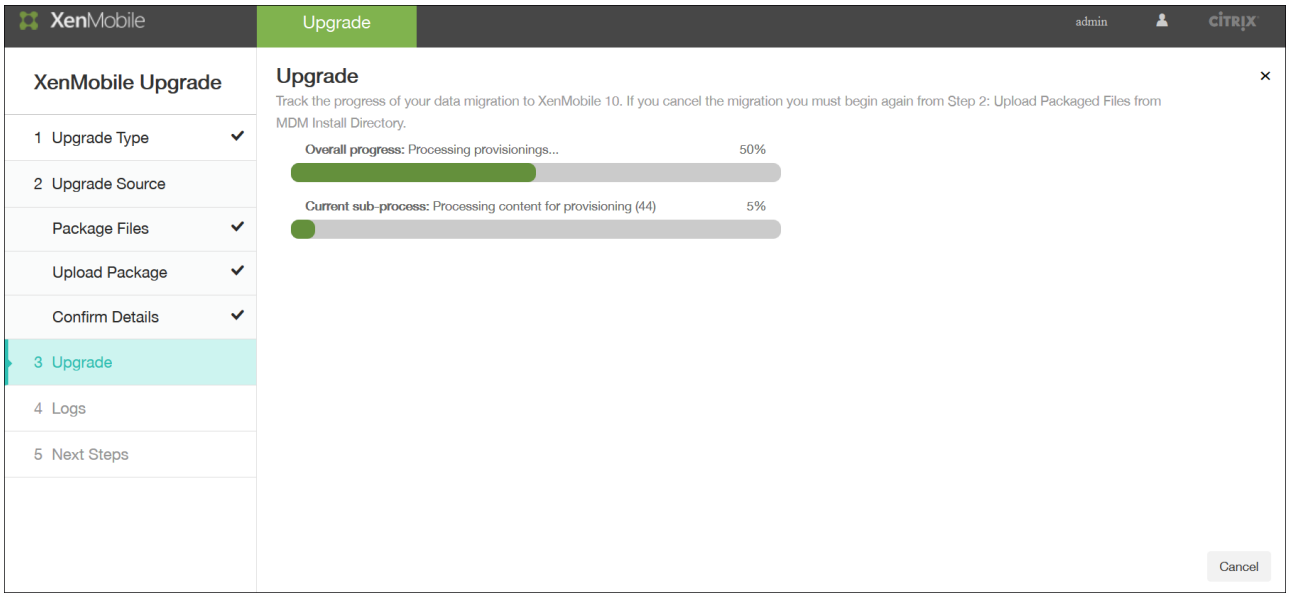
重要：必须正确输入所有证书密码，否则迁移将会失败。

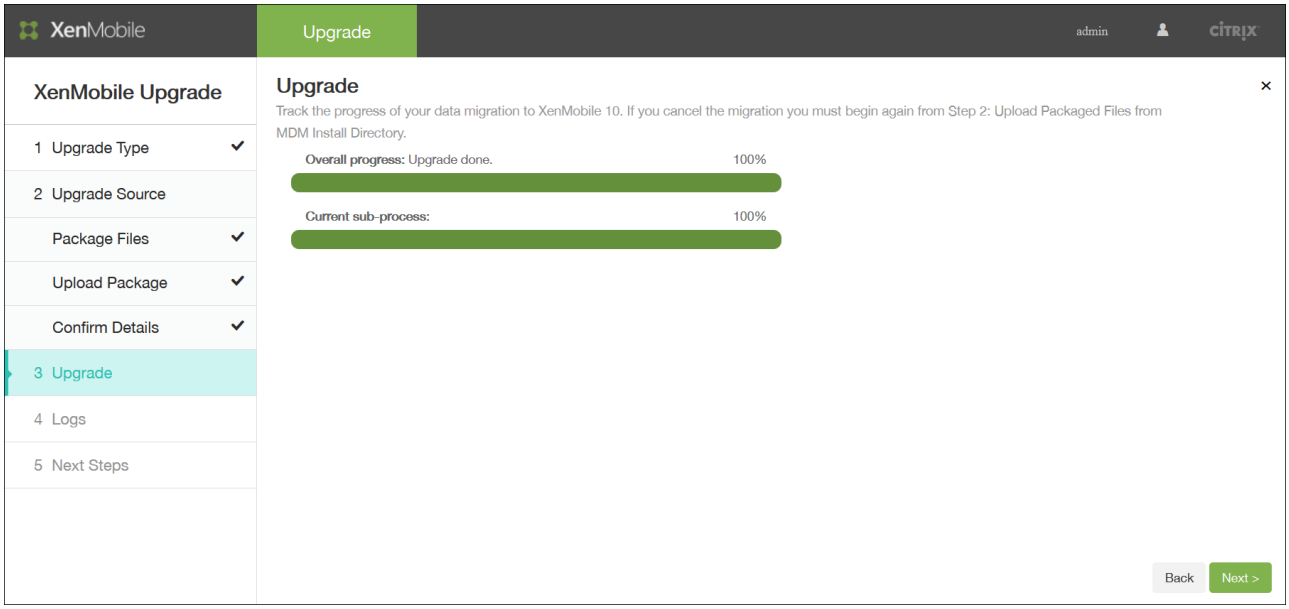


在单击下一步时，将出现以下确认消息。



然后，Upgrade（升级）页面将显示进度指示条，让您可以跟踪从 XenMobile 9.0 进行的数据迁移。



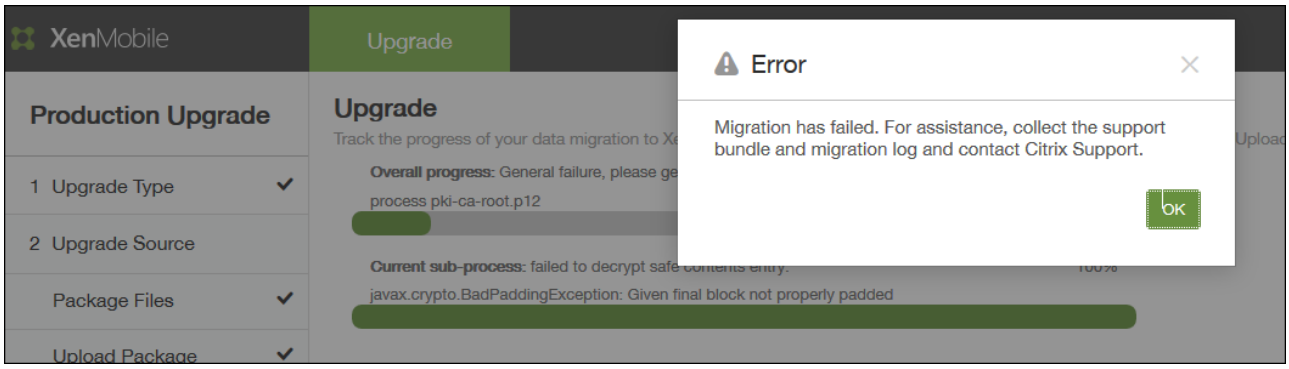


如果您未将所有必需的 Device Manager 文件复制到 .zip 文件夹，升级工具会显示丢失一个或多个文件。然后，该工具将在您添加了所需的一个或多个文件后重新启动。

如果无法解决问题，会出现错误消息，告之您生成 XenMobile 支持包、收集迁移日志，并联系 Citrix 技术支持。

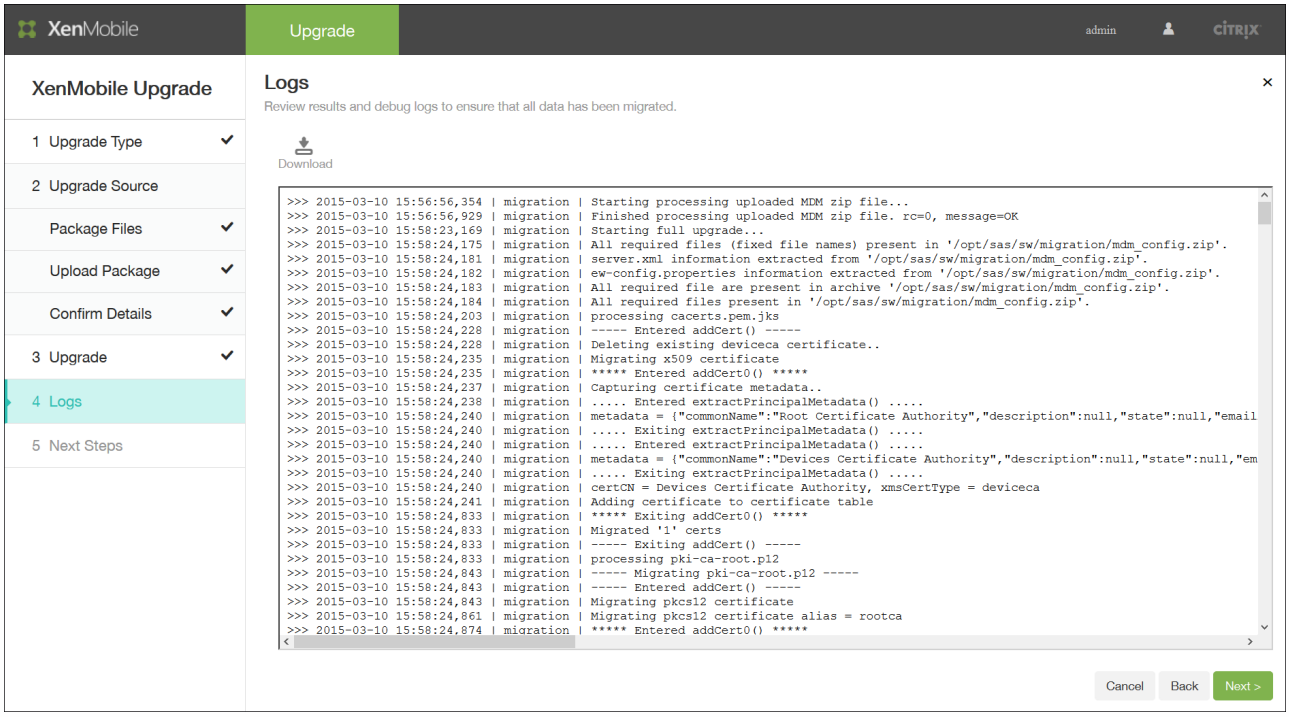
注意：

- 如果迁移失败，需要导入新的 XenMobile 10 实例，然后重新启动迁移。
- 迁移一旦完成（成功或失败），就不能再使用上一步按钮对信息进行更正。必须导入新的 XenMobile 10 实例并重新启动迁移。



查看升级工具日志

升级到 XenMobile 10 后，XenMobile 升级工具将提供日志文件 migration.log，供您下载和查看，如下图所示。Citrix 建议您查看该文件，以确定已迁移或未迁移到 XenMobile 10 的策略、设置、用户数据等信息。



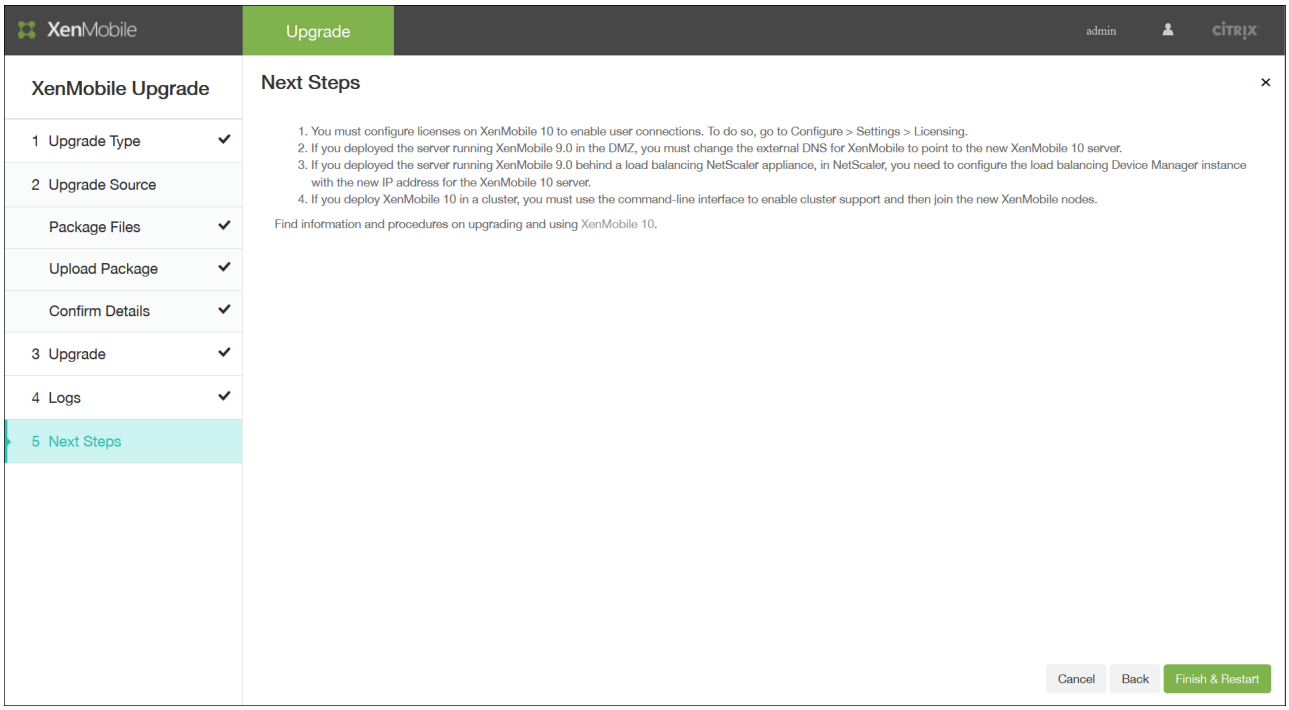
下载并查看迁移日志后，单击下一步转至 Next Steps（后续步骤）。有关详细信息，请参阅升级工具后续条件。

升级工具后续条件

May 05, 2016

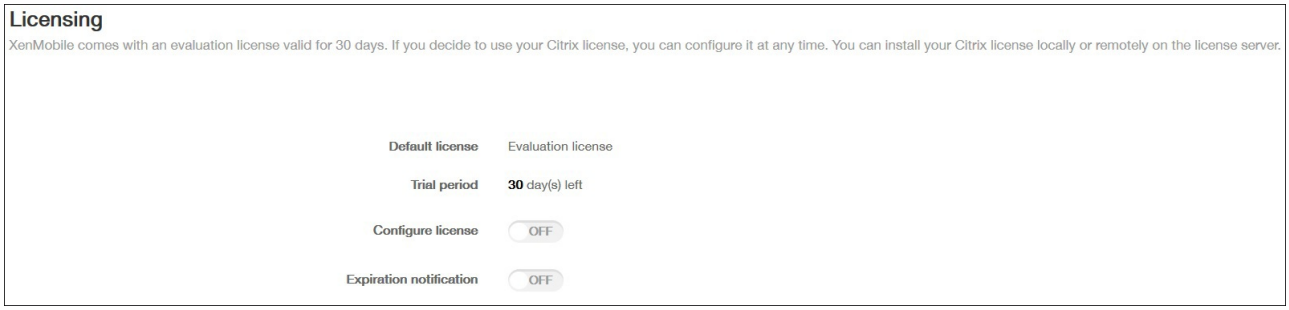
升级后，请确保完成以下后续条件，其中一些后续条件也会出现在升级工具的最后一个屏幕上。单击 Finish & Restart（结束并重新启动）时，服务器会重新启动。

注意：使用管理员凭据通过 https://:4443 登录 XenMobile 控制台。



Licensing

XenMobile 10 仅支持 Citrix V6 许可。请务必按照下图所示在 XenMobile 控制台中设置本地或远程许可证配置，并从 Citrix Licensing（Citrix 许可）下载许可证文件。有关更多详细信息，请参阅 XenMobile 许可主题。



必须在 XenMobile 10 上配置许可证，才能启用用户连接。为此，请转至**配置** > **设置** > **许可**。如果是运行 XenMobile 10 的独立服务器，您可在 XenMobile 控制台中上载仅支持 MDM 的许可证。

DNS

注意：必须满足此后续条件才能进行生产升级。如果在 DMZ 中部署运行 XenMobile 9.0 的服务器，您必须更改 XenMobile 的外部 DNS，以指向新的 XenMobile 10 服务器。

负载平衡 NetScaler IP 地址

注意：必须满足此后续条件才能进行生产升级。如果在负载平衡 NetScaler 设备之后部署运行 XenMobile 9.0 的服务器，您需要使用新的 XenMobile 10 服务器 IP 地址在 NetScaler 中配置负载平衡 Device Manager 实例。

群集

如果在群集中部署 XenMobile 10，您必须使用命令行界面启动群集支持，然后加入新的 XenMobile 节点。可以通过使用 XenMobile 9.0 的节点 IP 地址配置新的 XenMobile 10 实例，来重新使用 XenMobile 9.0 的节点 IP 地址，并将其加入到管理节点/最旧的节点。

更新未迁移的信息

根据需要进行如下更新：

- 自动化操作
- 服务器组策略和相关部署
- MSP 组
- 自定义 Active Directory 属性
- XenMobile 锁定限值
- RBAC 角色
- 日志设置
- 不含 HTTP 或 HTTPS 的 URL
- migration.log 文件中列出的所有配置或用户数据

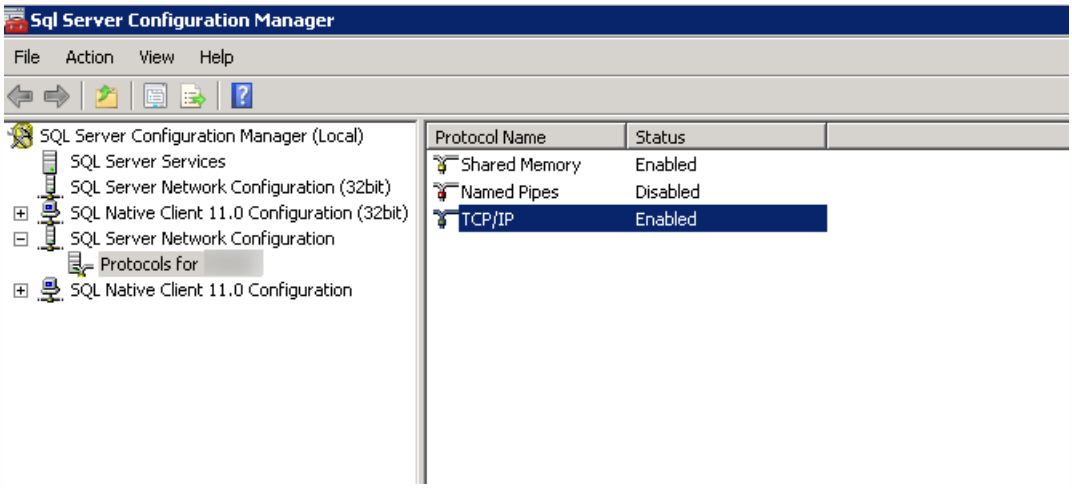
支持命名 SQL 实例

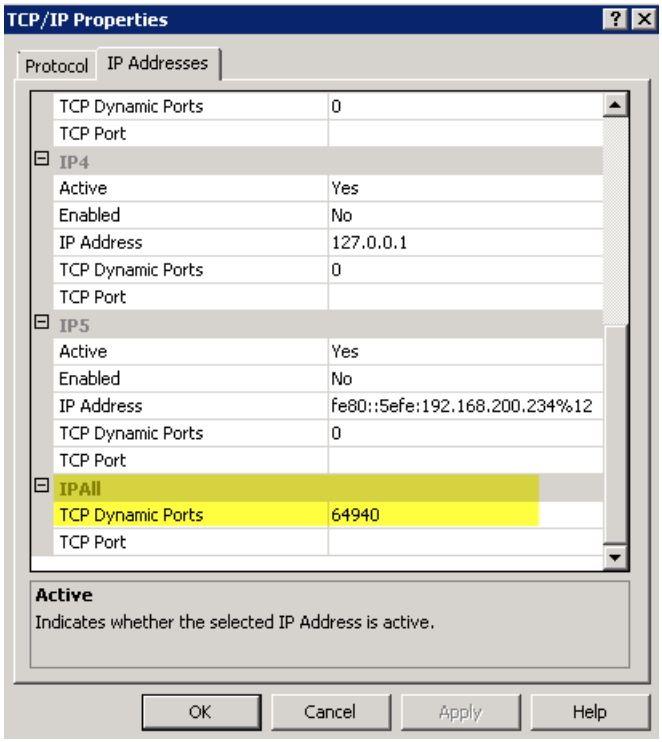
May 05, 2016

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 安装基于命名 SQL 实例，则需要按照专门针对此类情况的步骤进行操作。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。

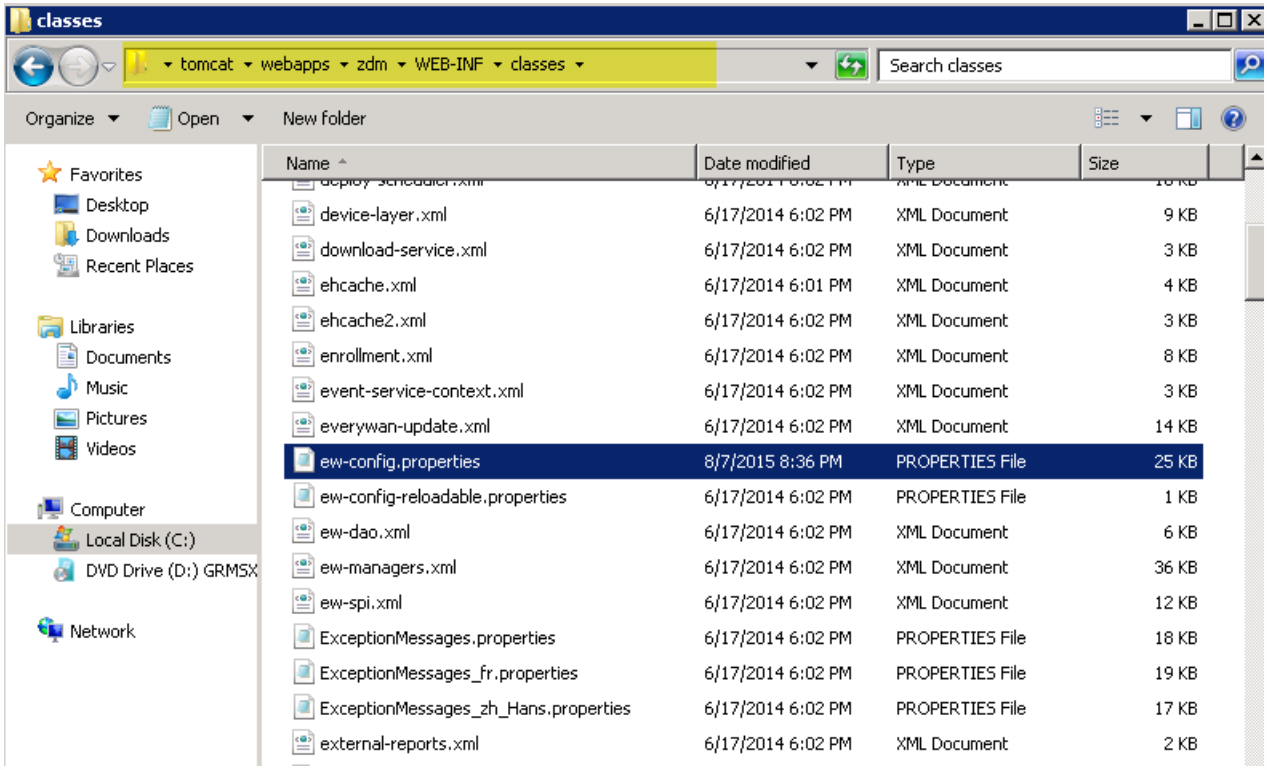
> **注意**
>
> Citrix 建议 SQL Server 数据库实例始终在静态端口上运行，因为 XenMobile 服务器需要继续访问该数据库。此连接通常通过防火墙遍历。因此，您需要在防火墙中打开恰当的端口，并且需要在静态端口上运行数据库实例。





升级包含 SQL Server 命名实例的 XenMobile 的步骤

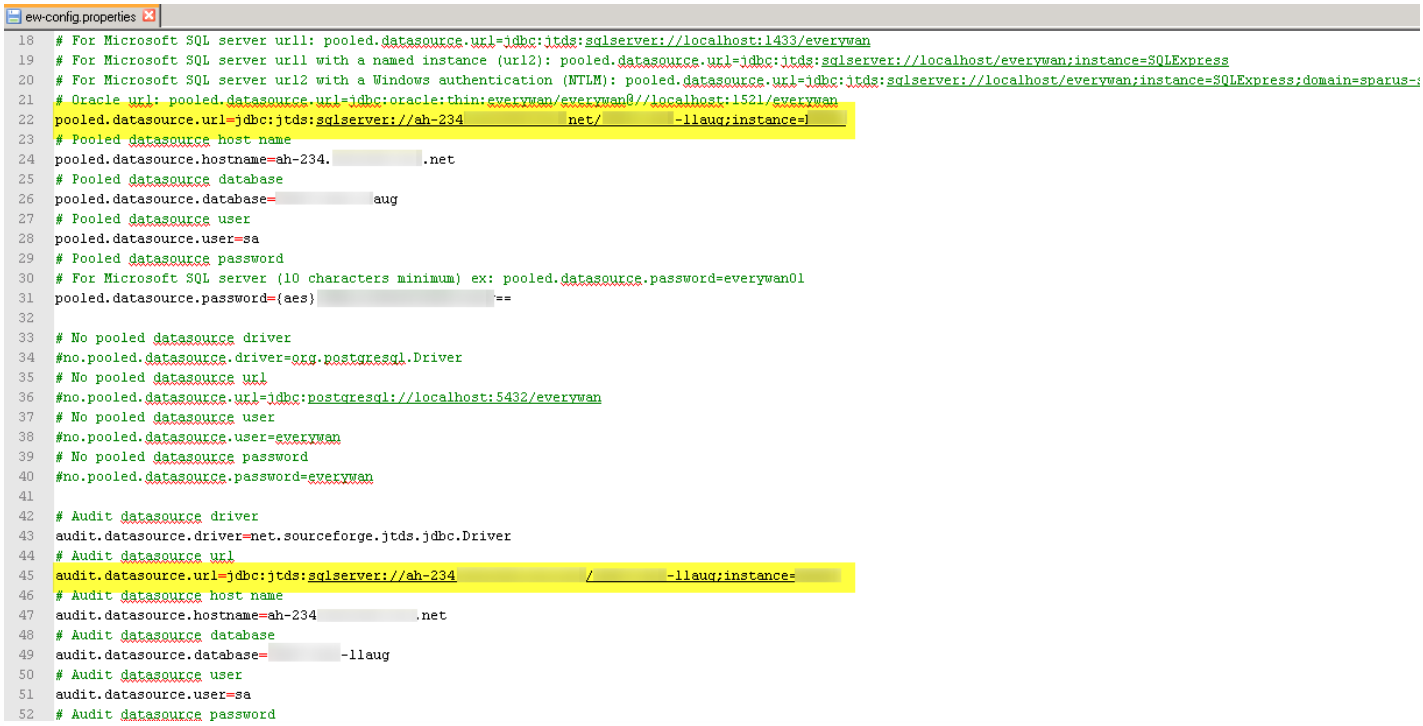
1. 转至 Device Manager 安装目录并打开 ew-config.properties 文件。此文件位于 tomcat\webapps\zdm\WEB-INF\classes 中。



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

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/

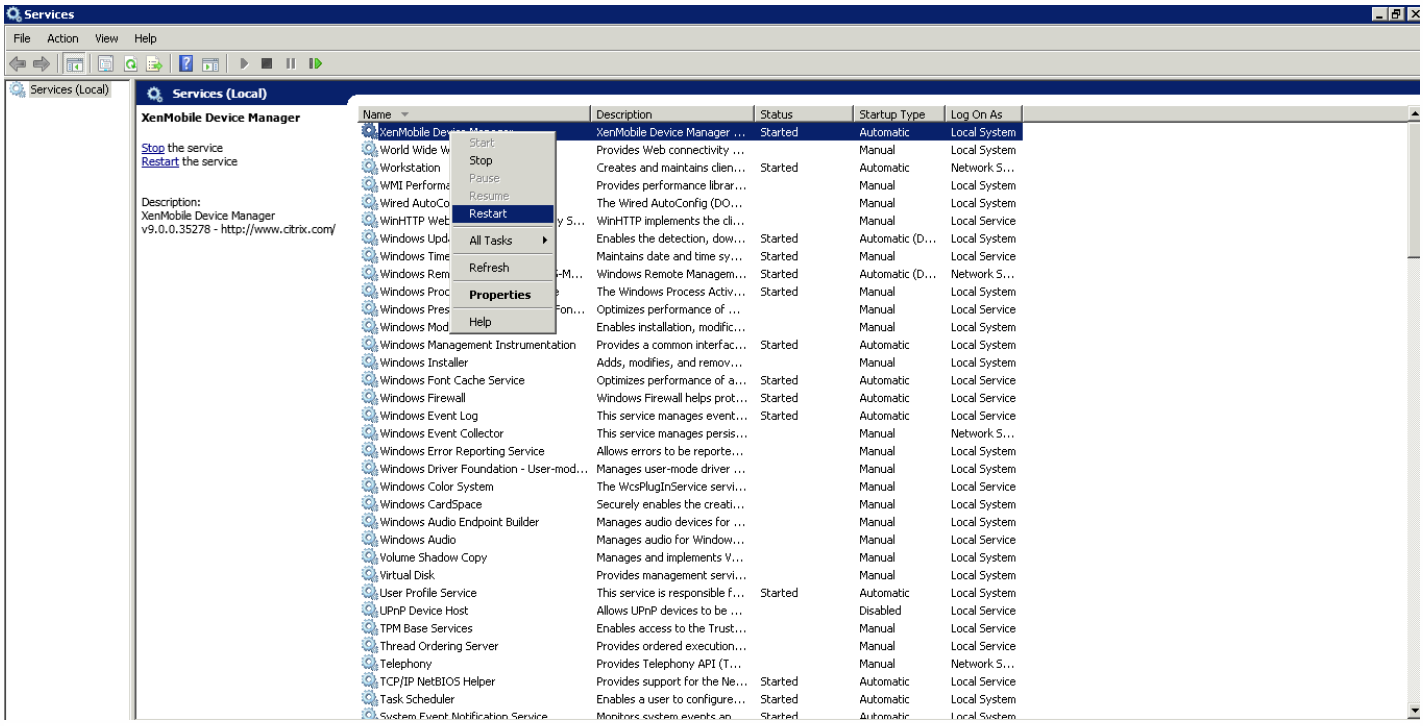
audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

> ## 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。

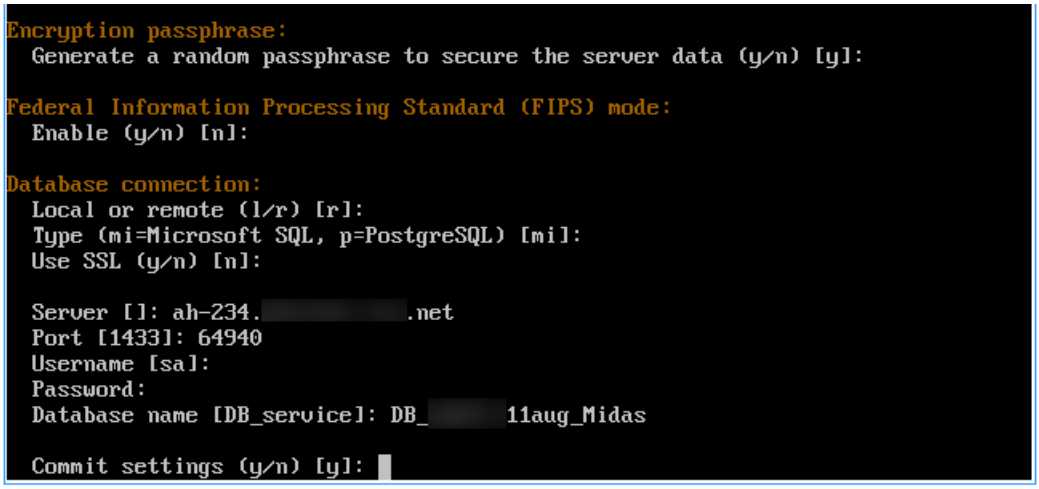
ew-config.properties

```
# 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。



6. 按照这些文件中的步骤进行操作，继续升级您的 XenMobile 环境：

- 要从 XenMobile 9.0 App Edition 或 Enterprise Edition 升级到 XenMobile 10.1，请使用 XenMobile Server App Edition 和 Enterprise Edition 升级工具。有关详细信息，请参阅启用和运行 XenMobile 10.1 升级工具。
- 要仅从 XenMobile 9.0 MDM Edition 升级到 XenMobile 10.1，请参阅 XenMobile 10 MDM 升级工具。

在 XenMobile 控制台中升级 XenMobile

May 05, 2016

XenMobile 软件的新版本可用时，可以升级到新版本。使用 XenMobile 控制台中的“Release Management”（版本管理）页面安装新版本的 XenMobile 软件、服务包和系统修补程序。

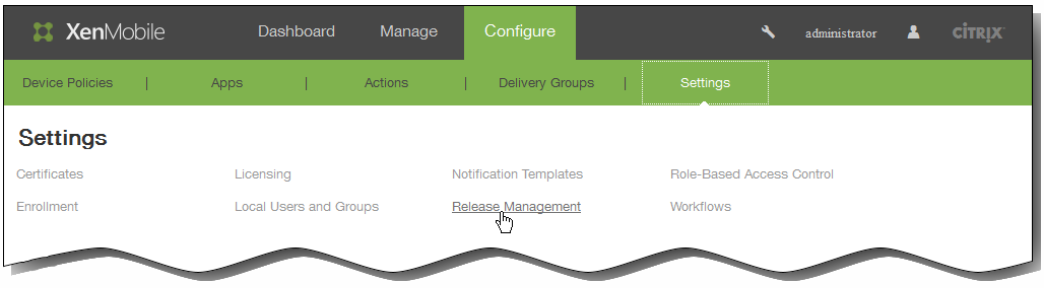
注意：当有新版本或重要更新可用时，我们会将其发布到 Citrix.com 上，并向每个客户的在案联系人发送通知。

重要提示：

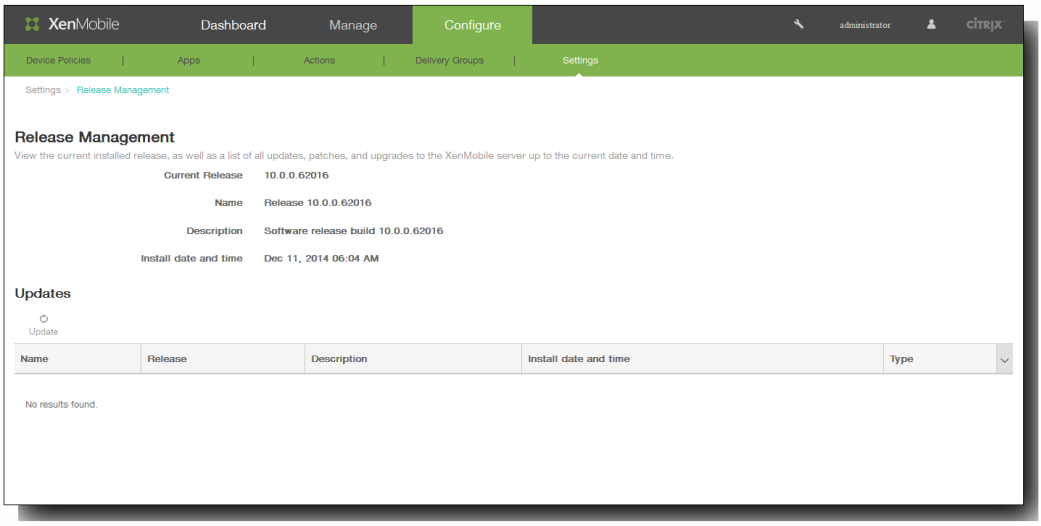
- 安装 XenMobile 更新前，请使用虚拟机 (VM) 中的设备创建系统的快照。
- 备份系统配置数据库。
- 如果已在 MDM 服务器上启用 Samsung KNOX Attestation，并计划升级到 XenMobile 10.0，您需要在升级之前添加新的自定义 KNOX Attestation 域。有关启用 Samsung KNOX Attestation 的详细信息，请参阅 Samsung KNOX。新的 Attestation 域为：
  - 中国地区 – china-attest-api.secb2b.com.cn
  - 欧洲地区 – eu-attest-api.secb2b.com
  - 美国地区 – us-attest-api.secb2b.com

升级 XenMobile

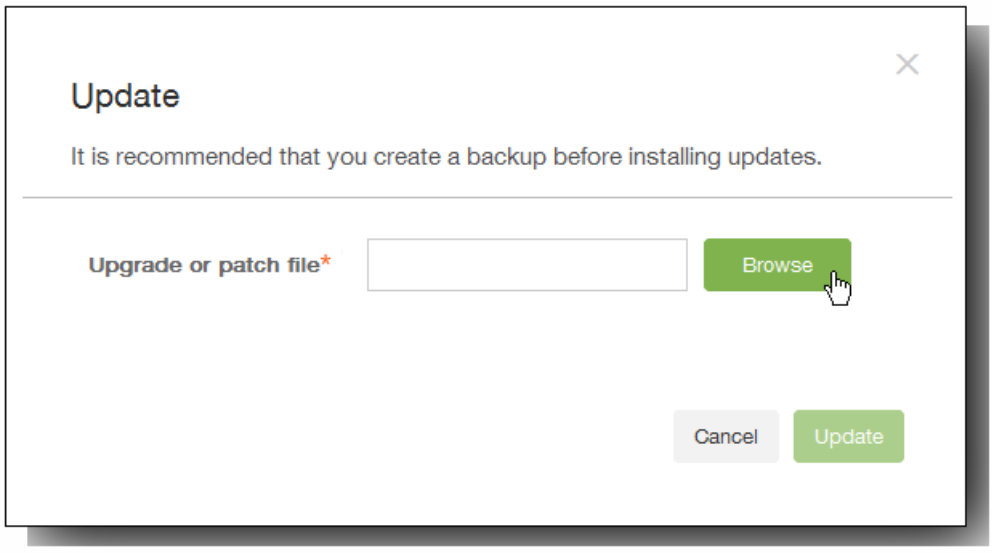
1. 在 Citrix Web 站点上登录您的帐户，然后将 XenMobile 升级 (.bin) 文件下载到合适的位置。
2. 在 XenMobile 控制台中，单击配置 > 设置 > 版本管理。



此时将出现版本管理页面，其中显示了当前已安装软件的版本，以及您已经上载的所有更新、修补程序和升级的列表。



3. 在更新下面，请单击更新。 此时将显示更新对话框。



4. 单击浏览，导航到保存您从 Citrix.com 下载的 XenMobile 升级文件的位置，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：

- 关闭除一个节点之外的所有节点。
- 更新该节点。
- 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。

为 XenMobile 10 配置群集

May 05, 2016

XenMobile 10 集成了 XenMobile 9 Device Manager 和 App Controller。在之前的 XenMobile 版本中，配置 Device Manager 作为群集，配置 App Controller 作为高可用性对。高可用性不适用于 XenMobile 10。因此，要为 XenMobile 10 配置群集，需要在 NetScaler 上配置下面两个负载平衡虚拟 IP 地址。

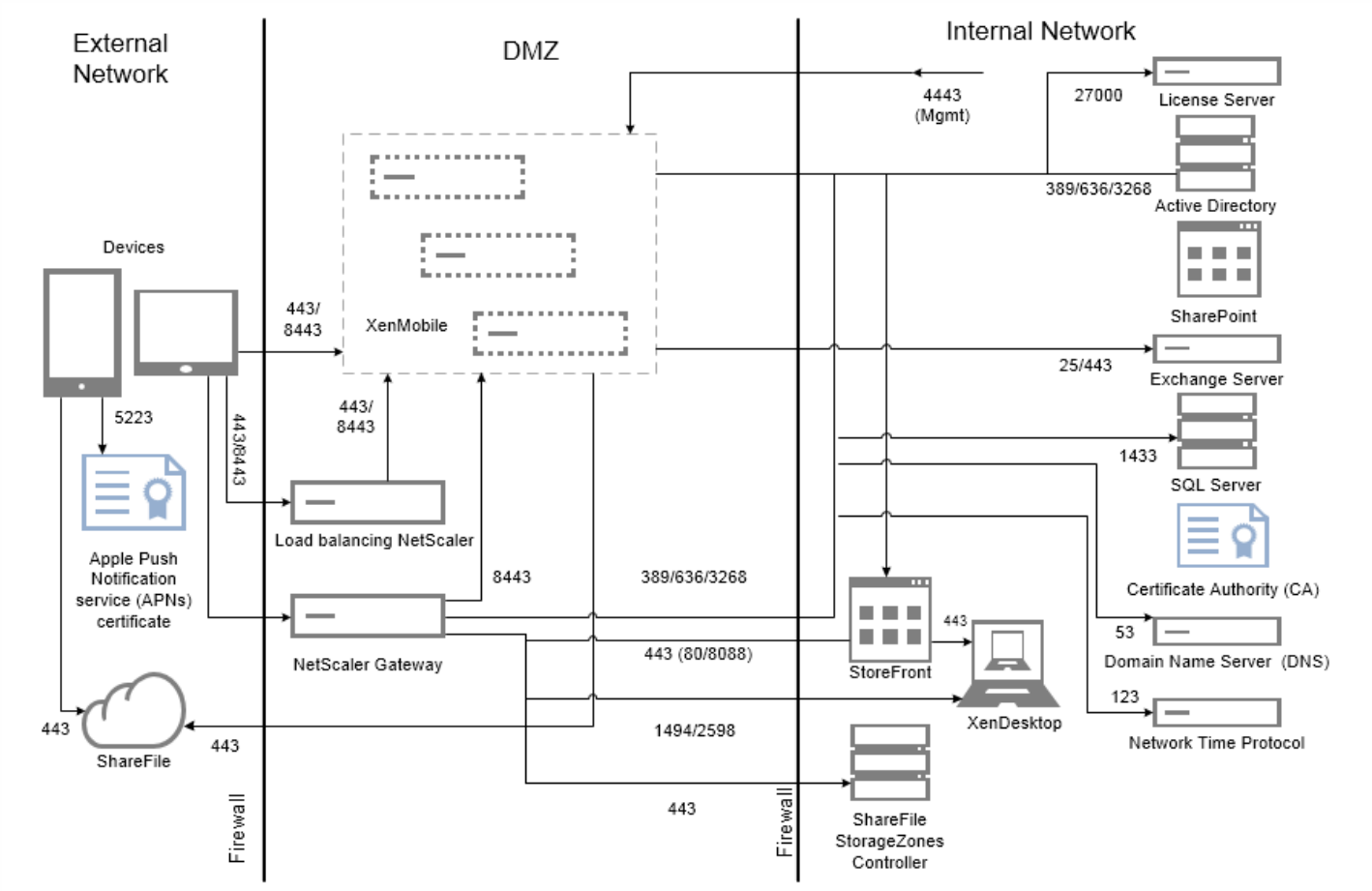
- **移动设备管理 (MDM) 负载平衡虚拟 IP 地址**：与群集中配置的 XenMobile 节点进行通信需要使用 MDM 负载平衡虚拟 IP 地址。此负载平衡在 SSL 桥接模式下完成。
- **移动应用程序管理 (MAM) 负载平衡虚拟 IP 地址**：NetScaler Gateway 与群集中配置的 XenMobile 节点进行通信需要使用 MAM 负载平衡虚拟 IP 地址。在 XenMobile 10 中，默认情况下，来自 NetScaler Gateway 的所有流量在端口 8443 上路由到负载平衡虚拟 IP 地址。

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。
- 两个用作负载平衡虚拟 IP 地址的免费 IP 地址。
- 服务器证书。
- 一个用作 NetScaler Gateway 虚拟 IP 地址的可用 IP。

理想状态下，所设置的群集环境应类似于下图：

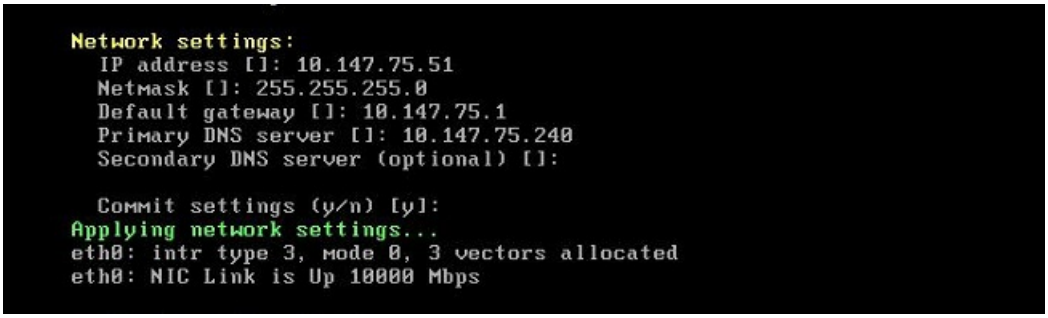


安装 XenMobile 群集节点

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。

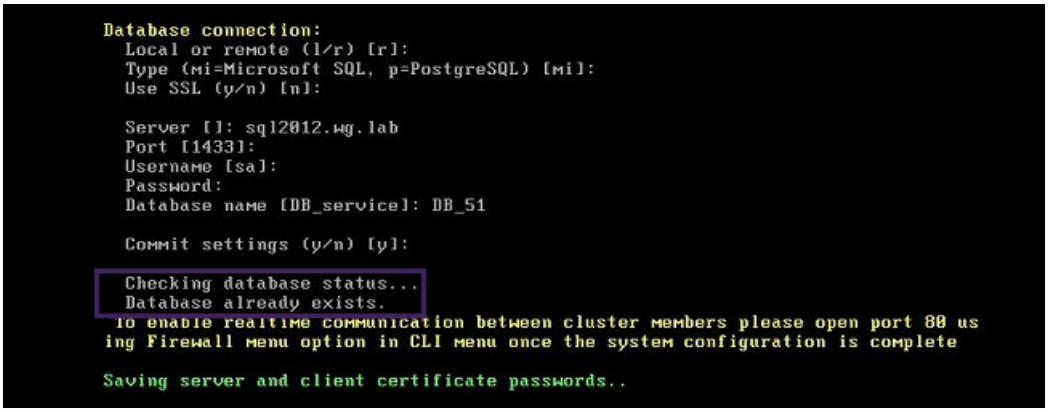
2. 提供网络配置详细信息，如下图所示。



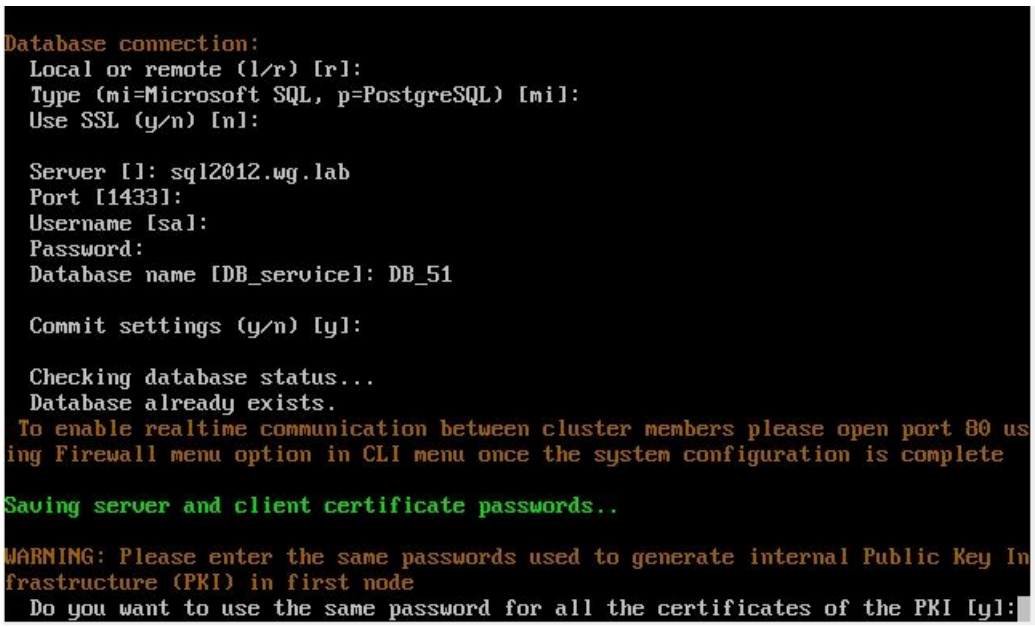
3. 如果要使用默认密码进行数据保护，请键入 **y**；否则，请键入 **n**，然后输入新密码。 **注意**：如果计划手动向群集添加其他节点，并且不打算克隆初始 XenMobile VM，必须在此处手动输入新密码。 连续节点需要相同的通行码。 如果不使用匹配的通行码，尝试加入第二个节点时，此过程会失败。 出现这种情况时可以克隆 VM，但是输入新密码可以防止失败发生。

4. 如果要使用 FIPS，请键入 **y**；否则，请键入 **n**。

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

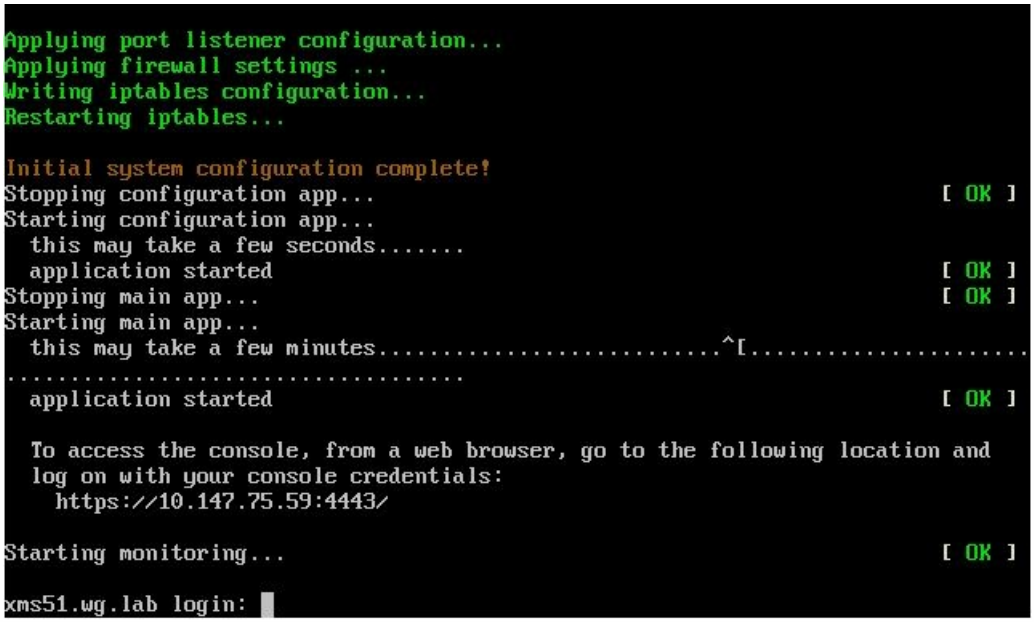


6. 输入与为第一个 VM 提供的证书相同的密码。



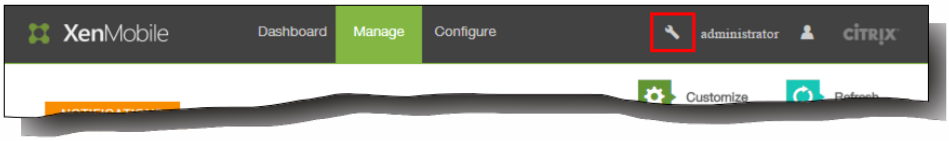
输入密码后，第二个节点上的初始配置将完成。

7. 配置完成后，服务器重新启动并显示登录对话框。

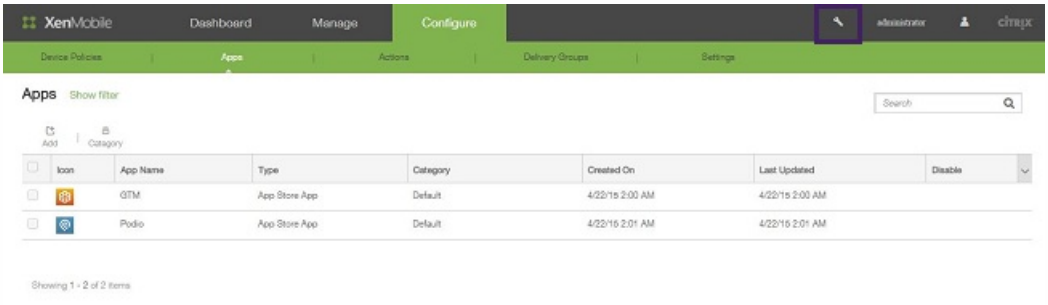


注意：登录对话框与第一个 VM 的登录对话框相同。这种相同是供您确认两个 VM 使用相同的数据库服务器的一种途径。

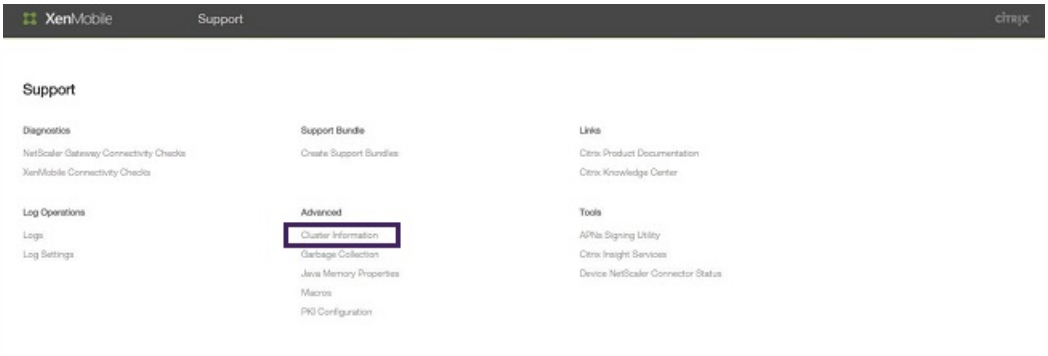
8. 使用 XenMobile 的完全限定的域名 (FQDN) 在 Web 浏览器中打开 XenMobile 控制台。
9. 在控制板上，单击屏幕右上角的工具图标。



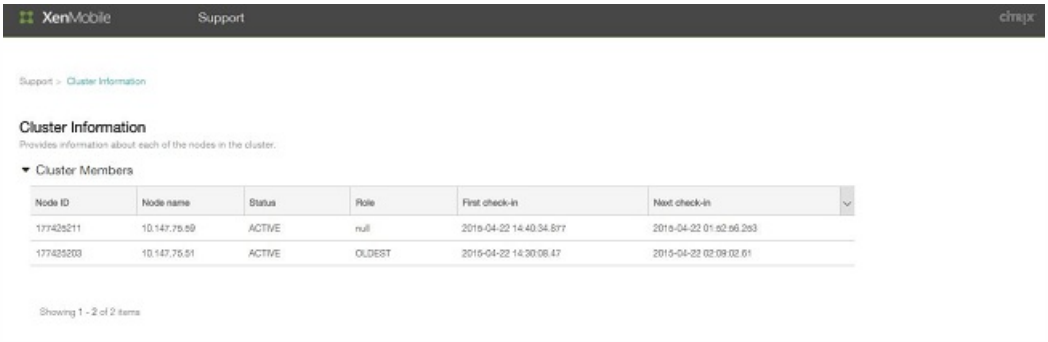
此时将打开“支持”页面。



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。



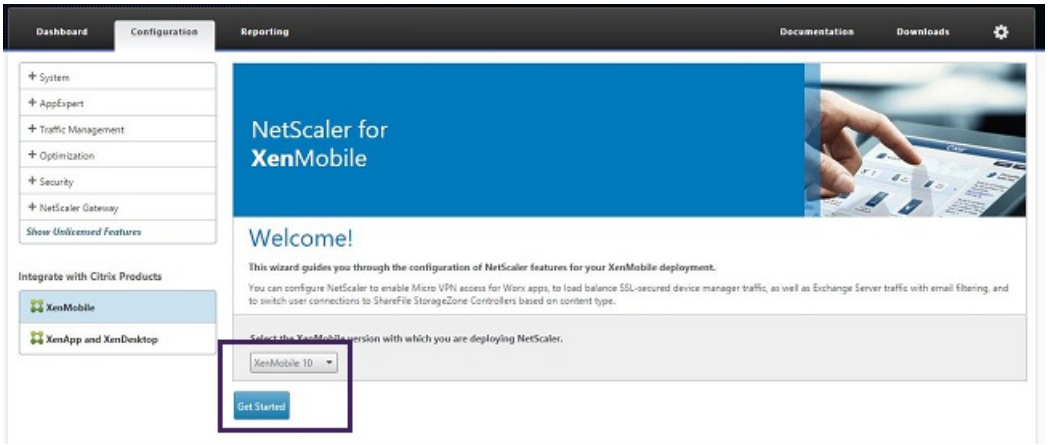
新节点现在属于群集的成员。您可以按照相同的步骤添加其他节点。

在 NetScaler 中为 XenMobile 群集配置负载平衡

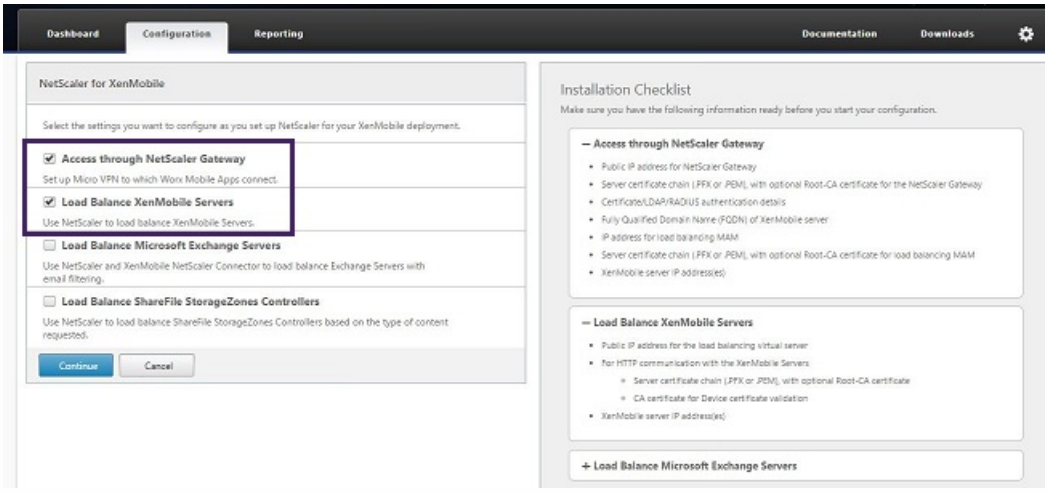
将所需的节点作为成员添加到 XenMobile 群集中后，需要对节点进行负载平衡才能访问群集。负载平衡通过运行 NetScaler 10.5.x 中提供的 XenMobile 向导完成。您可以通过运行此向导，按照本过程中的步骤对 XenMobile 进行负载平衡。

1. 登录 NetScaler。

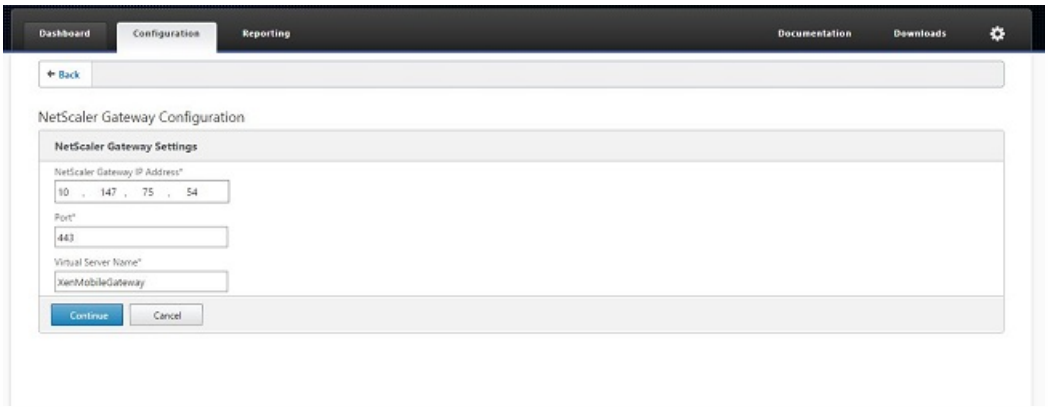
2. 在 Configuration（配置）选项卡上，单击 XenMobile，然后单击 Get Started（开始）。



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）。

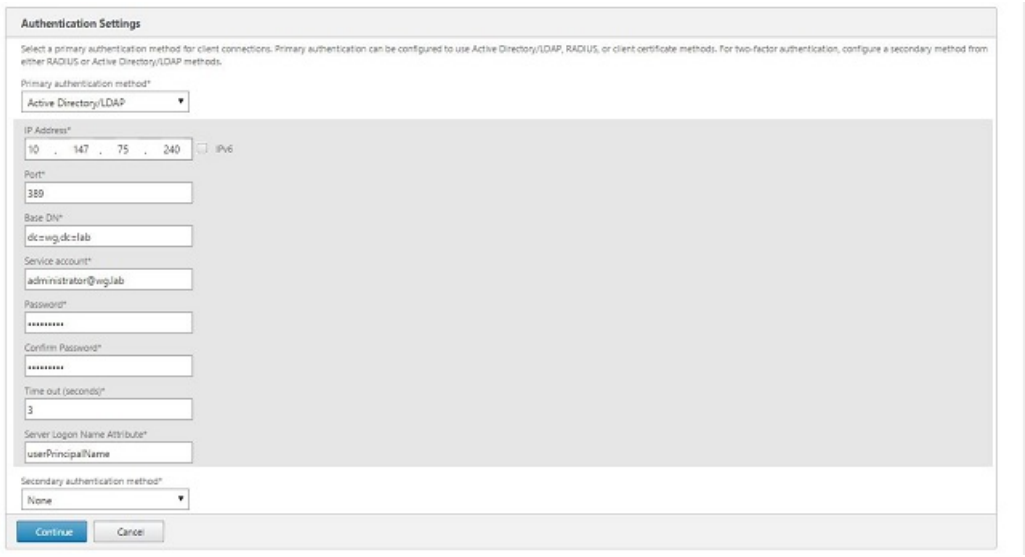


4. 输入 NetScaler Gateway 的 IP 地址，然后单击 Continue（继续）。



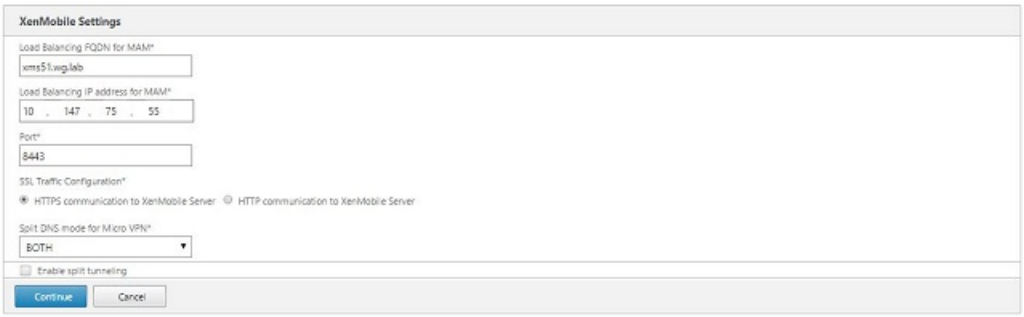
5. 通过执行以下操作将服务器证书绑定到 NetScaler Gateway 虚拟 IP 地址，然后单击 Continue（继续）。
   - 在 Use existing certificate（使用现有证书）中，从列表中选择服务器证书。
   - 单击 Install Certificate（安装证书）选项卡以上载新的服务器证书。

6. 输入身份验证服务器详细信息，然后单击 Continue（继续）。



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）。

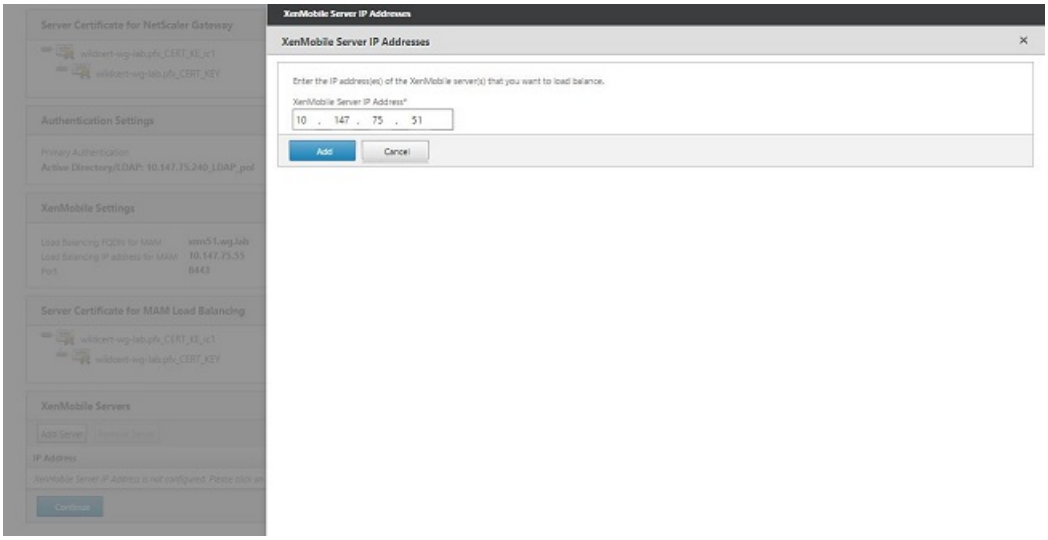


注意：确保 MAM 负载平衡虚拟 IP 地址的 FQDN 与 XenMobile 的 FQDN 相同。

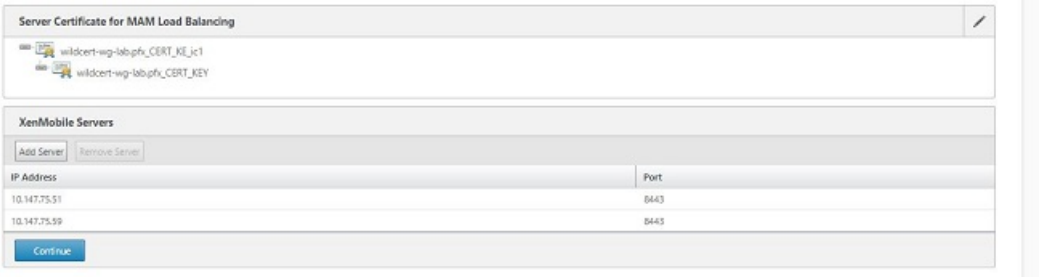
8. 如果使用 SSL 桥接模式 (HTTPS)，请选择 HTTPS communication to XenMobile Server（与 XenMobile 服务器进行 HTTPS 通信）。 但是，如果要使用 SSL 卸载，请选择 HTTP communication to XenMobile Server（与 XenMobile 服务器进行 HTTP 通信），如上图所示。为实现本文的目的，请选择 SSL 桥接模式 (HTTPS)。
9. 绑定 MAM 负载平衡虚拟 IP 地址的服务器证书，然后单击 Continue（继续）。

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。

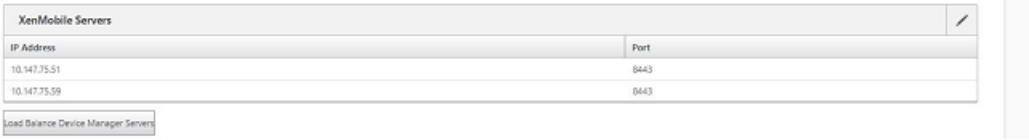
11. 输入 XenMobile 节点的 IP 地址，然后单击 Add（添加）。



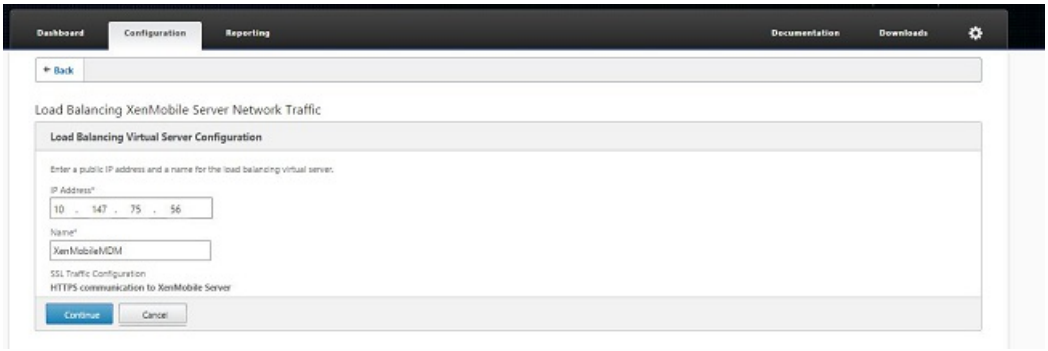
12. 重复步骤 10 和 11 以添加其他 XenMobile 节点，作为 XenMobile 群集的一部分。您将看到已添加的所有 XenMobile 节点。单击 Continue（继续）。



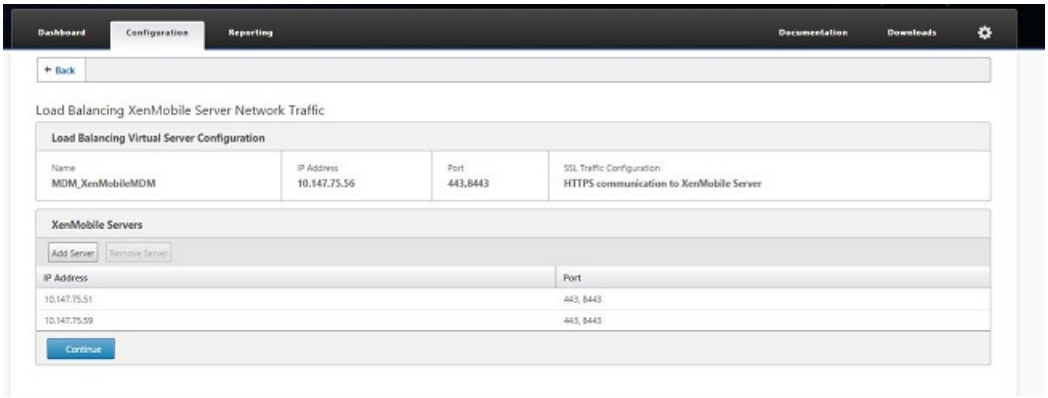
13. 单击 Load Balance Device Manager Servers（Device Manager 服务器负载平衡）以继续执行 MDM 负载平衡配置。



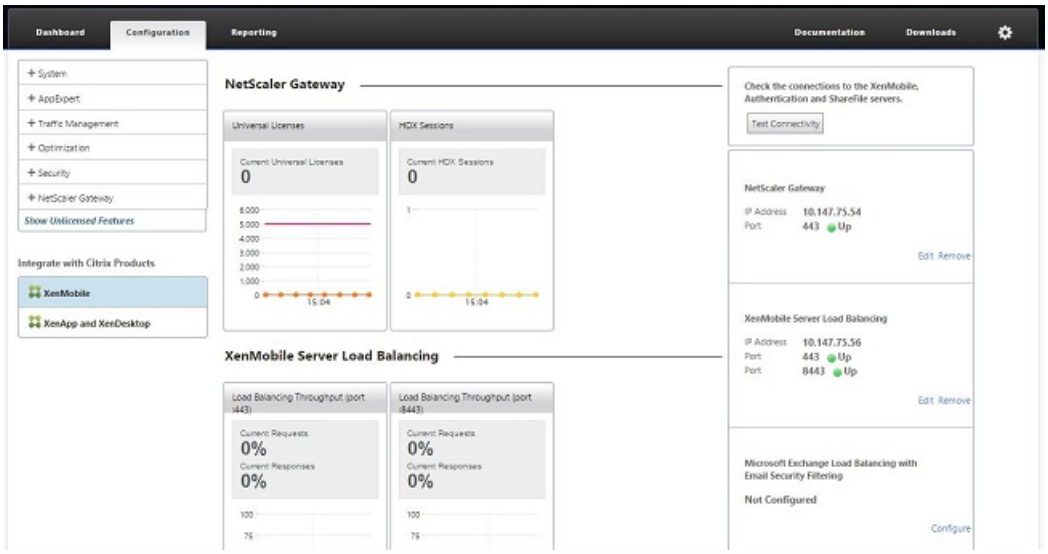
14. 输入要用作 MDM 负载平衡 IP 地址的 IP 地址，然后单击 Continue（继续）。



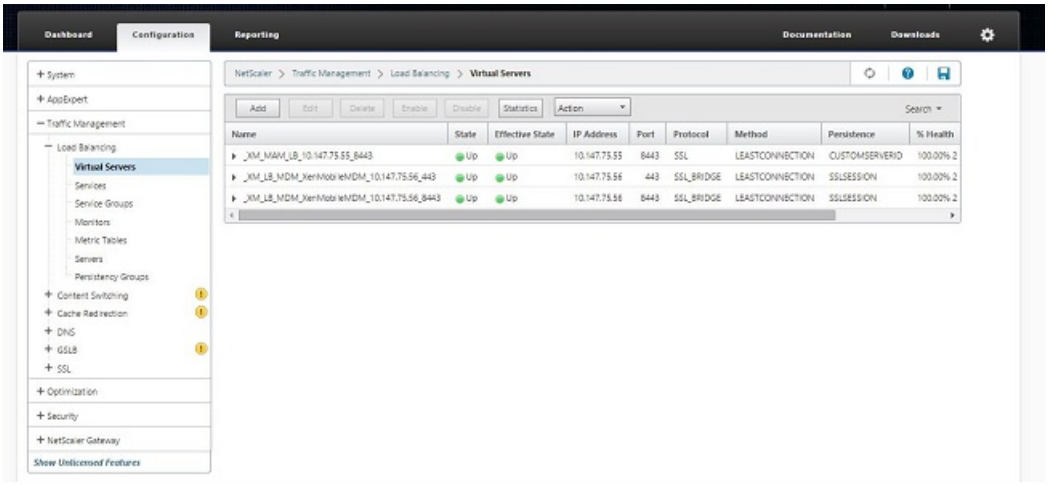
15. 列表中显示 XenMobile 节点后，单击 Continue（继续），然后单击 Done（完成）以完成此过程。



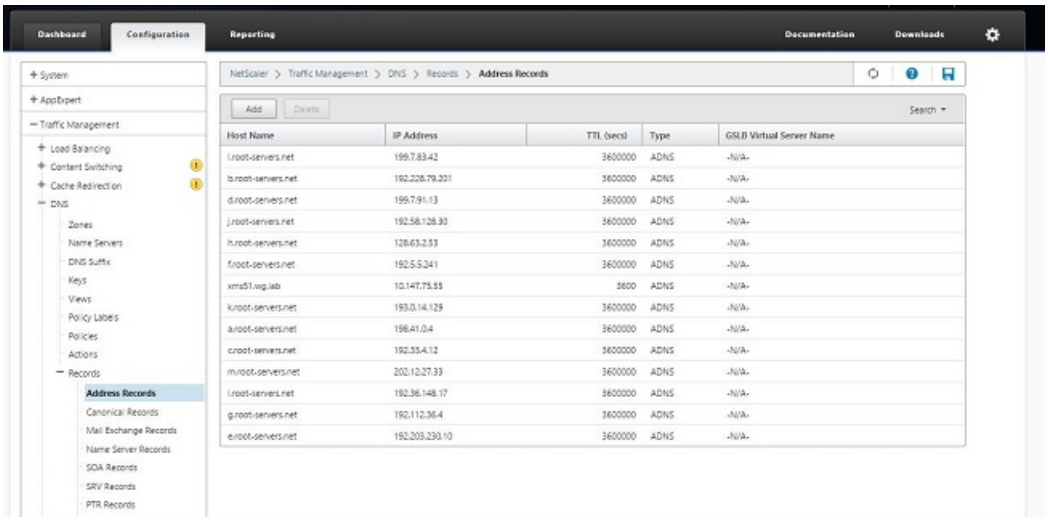
您将在 XenMobile 页面上看到虚拟 IP 地址状态。



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）。



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

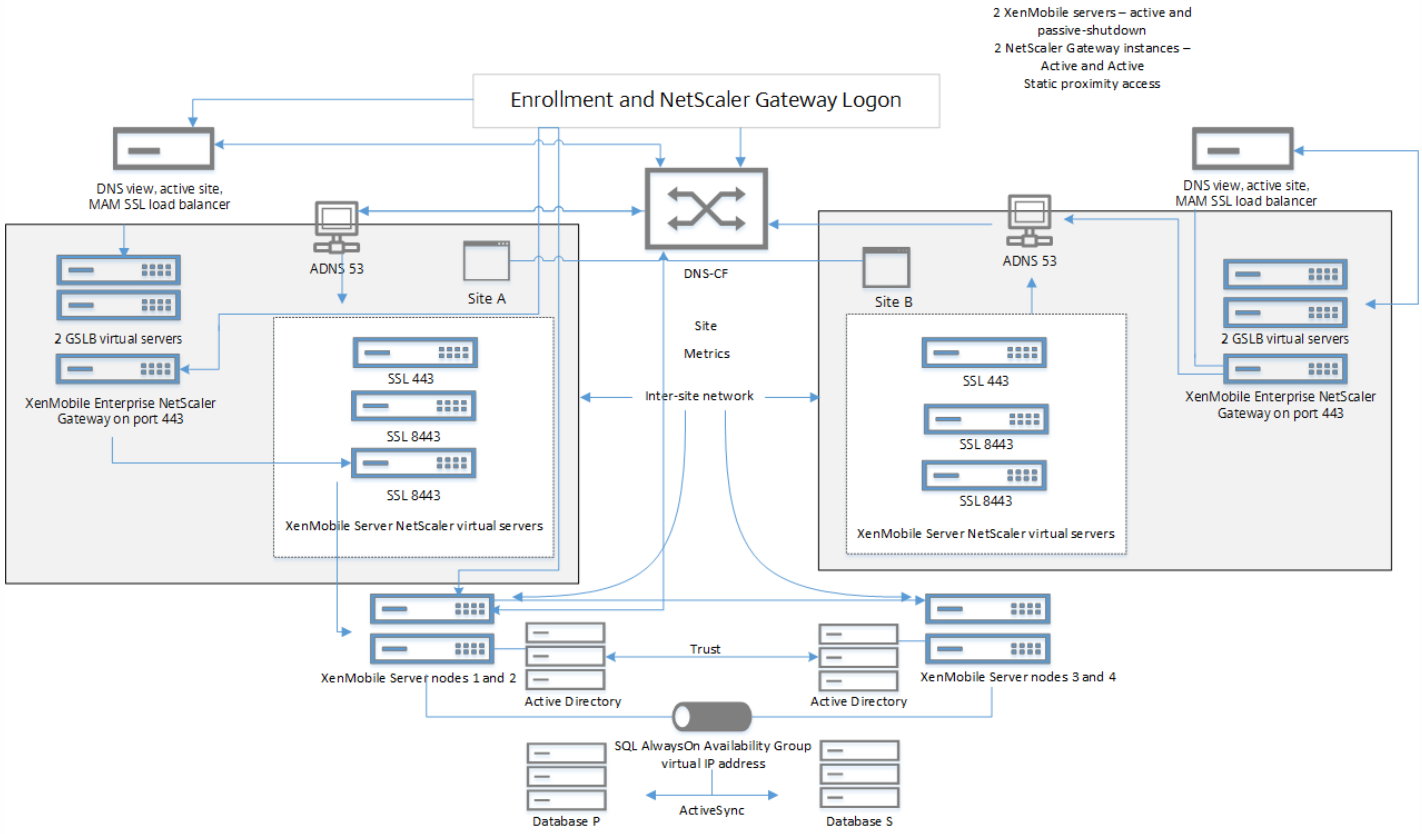


XenMobile 的灾难恢复指南

May 05, 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。



PDF XenMobile 灾难恢复指南

PDF XenMobile 灾难恢复体系结构图。

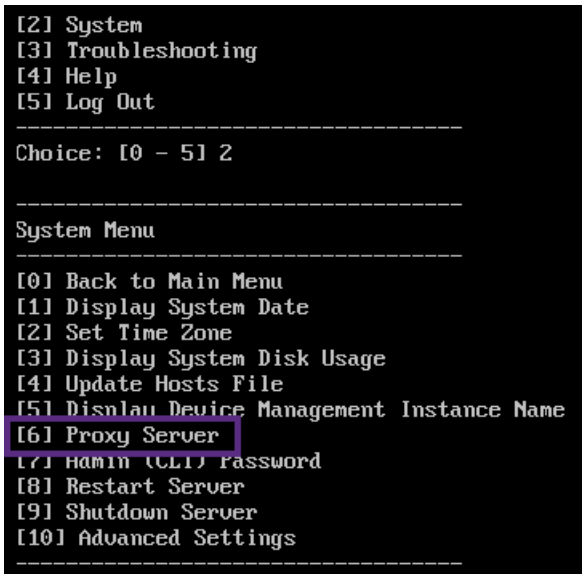
在 XenMobile 中启用代理服务器

May 05, 2016

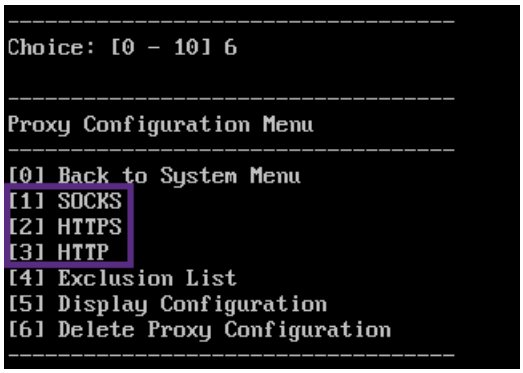
如果想要控制出站 Internet 流量，可以在 XenMobile 中设置代理服务器来承载此流量。为此，需要通过命令行接口 (CLI) 设置代理服务器。请注意，设置代理服务器需要重新启动系统。

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。



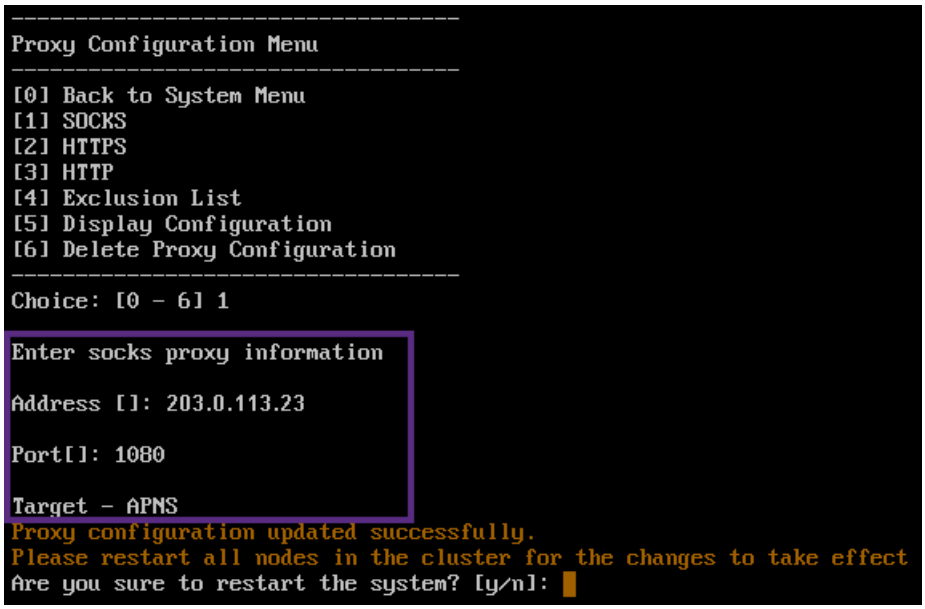
3. 在“Proxy Configuration Menu”（代理配置菜单）中，键入 **1** 以选择 SOCKS，键入 **2** 以选择 HTTPS，或键入 **3** 以选择 HTTP。



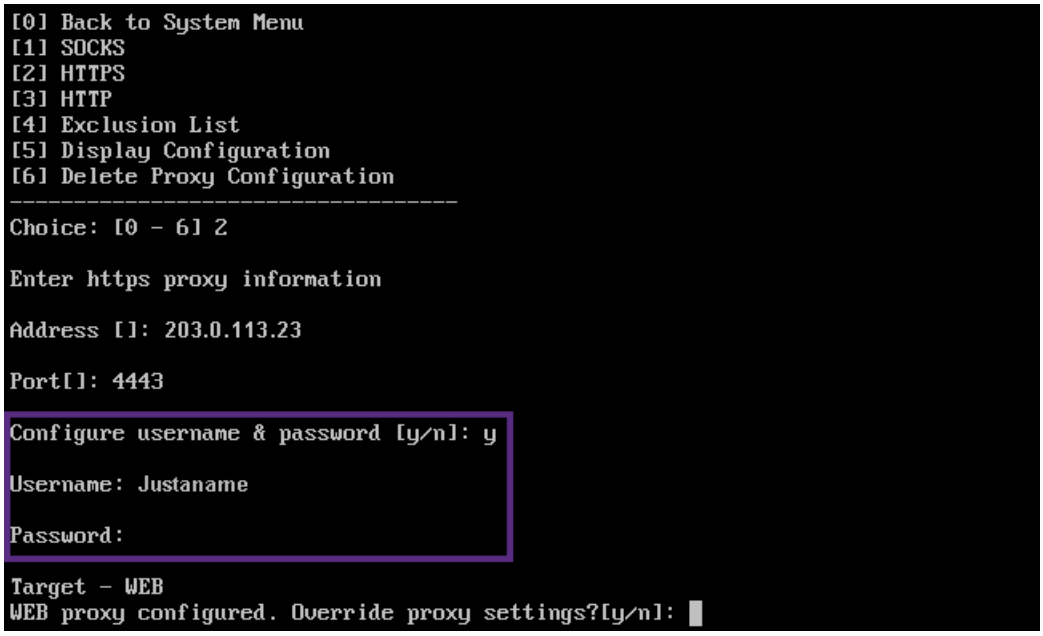
4. 键入代理服务器 IP 地址、端口号和目标。有关每种代理服务器类型支持的目标类型，请参阅下表。

代理类型	支持的目标
SOCKS	APNS

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。



6. 键入 **y** 将完成代理服务器设置。

Licensing

May 05, 2016

XenMobile 和 NetScaler Gateway 需要许可证。有关 NetScaler Gateway 许可的详细信息，请参阅在 NetScaler Gateway 上安装许可证。

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 要求使用 Citrix 许可证服务器 11.12.1 版本或更高版本；较旧的许可证服务器版本与 XenMobile 10 不兼容。

重要：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。

XenMobile 许可注意事项

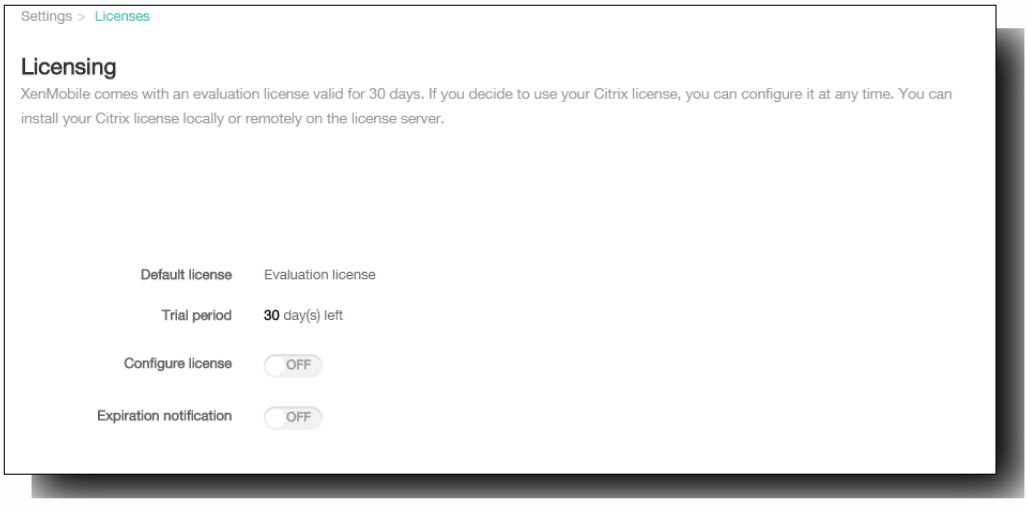
在不提供许可证的情况下，XenMobile 将在宽限期为 30 天的试用模式下运行，功能齐全。此试用模式只能使用一次，期限为从安装开始 30 天。无论是否有可用的有效 XenMobile 许可证，均不会阻止对 XenMobile Web 控制台的访问。

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，所有设备管理功能将不可用。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升级。

在 XenMobile 控制台上查找“Licensing”（许可）页面

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



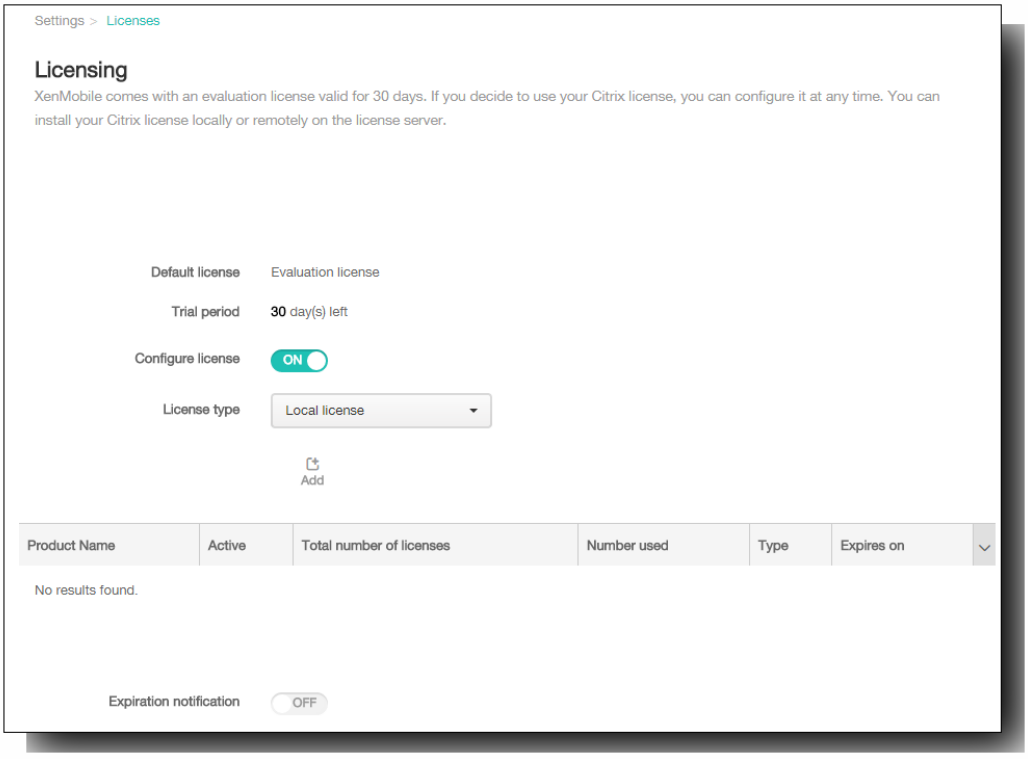
1. 在 XenMobile 控制台中，单击配置 > 设置。
2. 单击许可。 此时将显示许可页面。

添加本地许可证

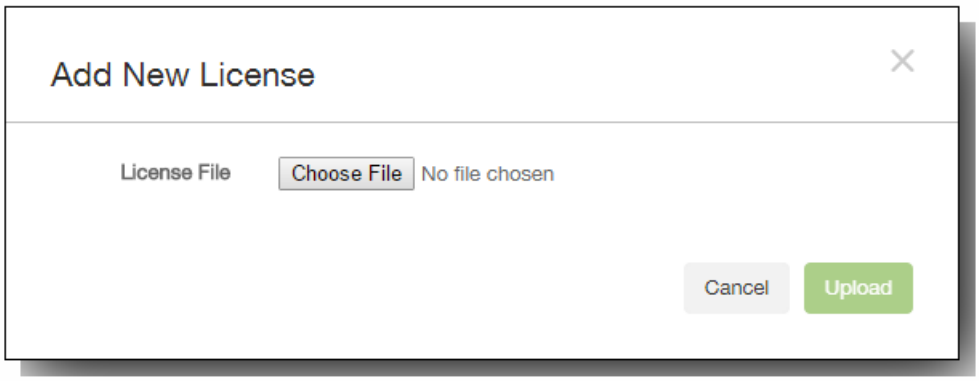
添加新许可证时，新许可证将显示在表格中。添加的第一个许可证自动被激活。如果添加同一类别（如企业）或同一类型（如设备）的多个许可证，这些许可证将显示在表格的同一行中。在这些情况下，许可证总数和使用的数量反应公共许可证的总数。过期日期显示公共许可证的最新过期日期。

通过 XenMobile 控制台管理所有本地许可证。

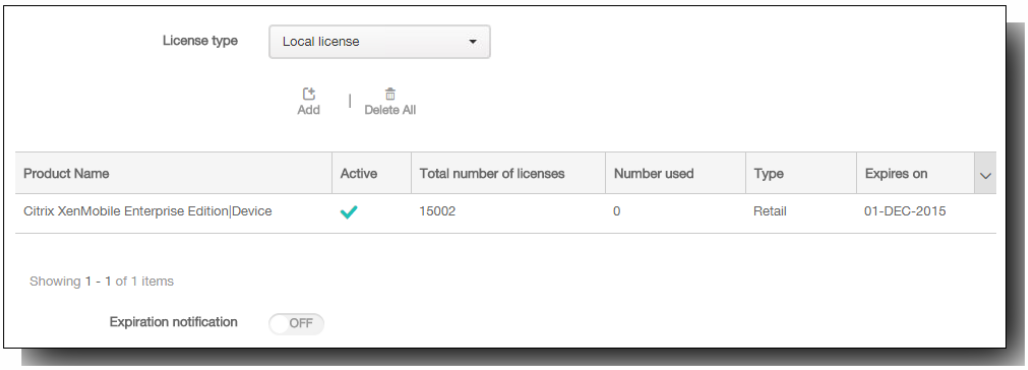
1. 从 Simple License Service 获取许可证文件，方法是通过许可证管理控制台或直接利用您在 Citrix.com 上的帐户。 有关详细信息，请参阅获取许可证文件。
2. 在控制台中，单击配置 >设置 > 许可证。 此时将显示许可页面。
3. 将配置许可证设置为开。 在许可证类型列表中，单击添加按钮，将显示许可表。许可表包含已用于 XenMobile 的许可证。如果尚未添加任何 Citrix 许可证，此表为空。



4. 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。



5. 在添加新许可证对话框中，单击选择文件，然后浏览以查找您的许可证。
6. 单击上载。 许可证将上载到本地并显示在表格中。

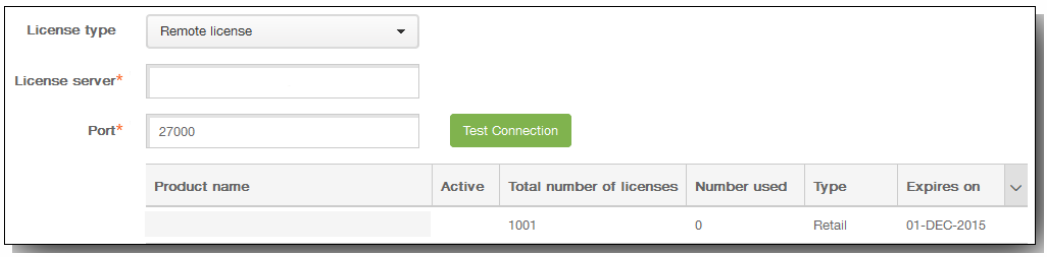


7. 许可证显示在许可证页面上的表格中以后，请将其激活。 如果此许可证是表格中的第一个许可证，此许可证会自动激活。

添加远程许可证

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的许可活动。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。
2. 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。



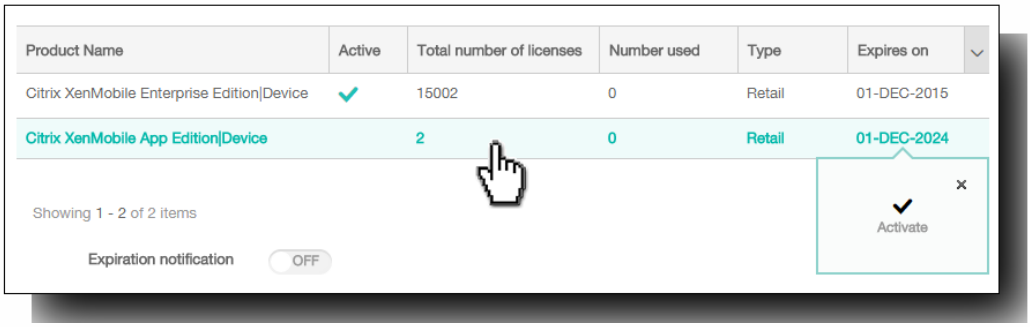
3. 在许可证服务器中，键入远程许可服务器的 IP 地址或完全限定的域名 (FQDN)。
4. 在端口字段中，接受默认端口或键入用于与许可服务器通信的端口号。

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。如果连接失败，请检查您提供的信息是否正确，以及所有连接是否激活。
   注意：如果只有一个许可证，会自动激活此许可证。

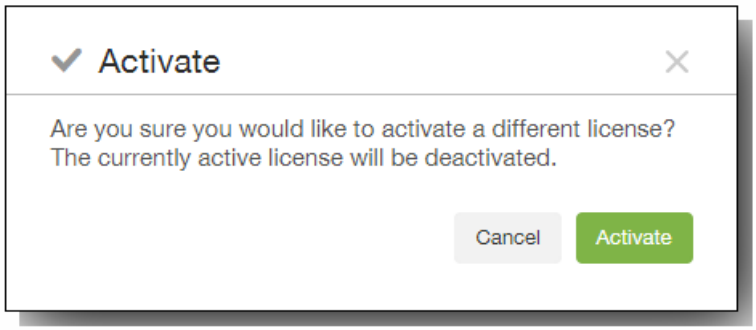
激活其他许可证

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

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



2. 单击激活。 将显示激活对话框。

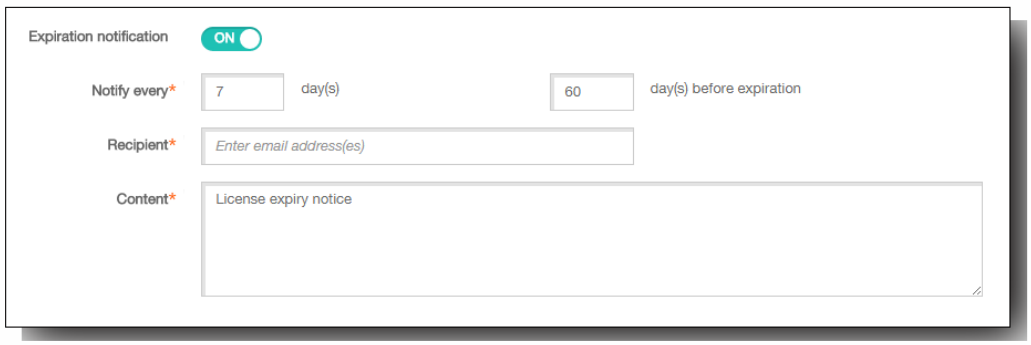


3. 单击激活。
   重要：如果激活所选许可证，当前激活的许可证将取消激活。
   所选许可证现已激活。

自动化过期通知

激活远程或本地许可证后，可以将 XenMobile 配置为在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. 在通知时间间隔中，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。
3. 在收件人字段中，键入您的电子邮件地址或许可证负责人的电子邮件地址。
4. 在内容字段中，键入收件人在通知中看到的过期通知消息。
5. 单击保存。 在过期前指定的天数时，XenMobile 开始向您标识的收件人发送电子邮件，其中包含您在此过程中提供的文本。通知按照您建立的频率重复发送。

XenMobile 控制台入门

May 05, 2016

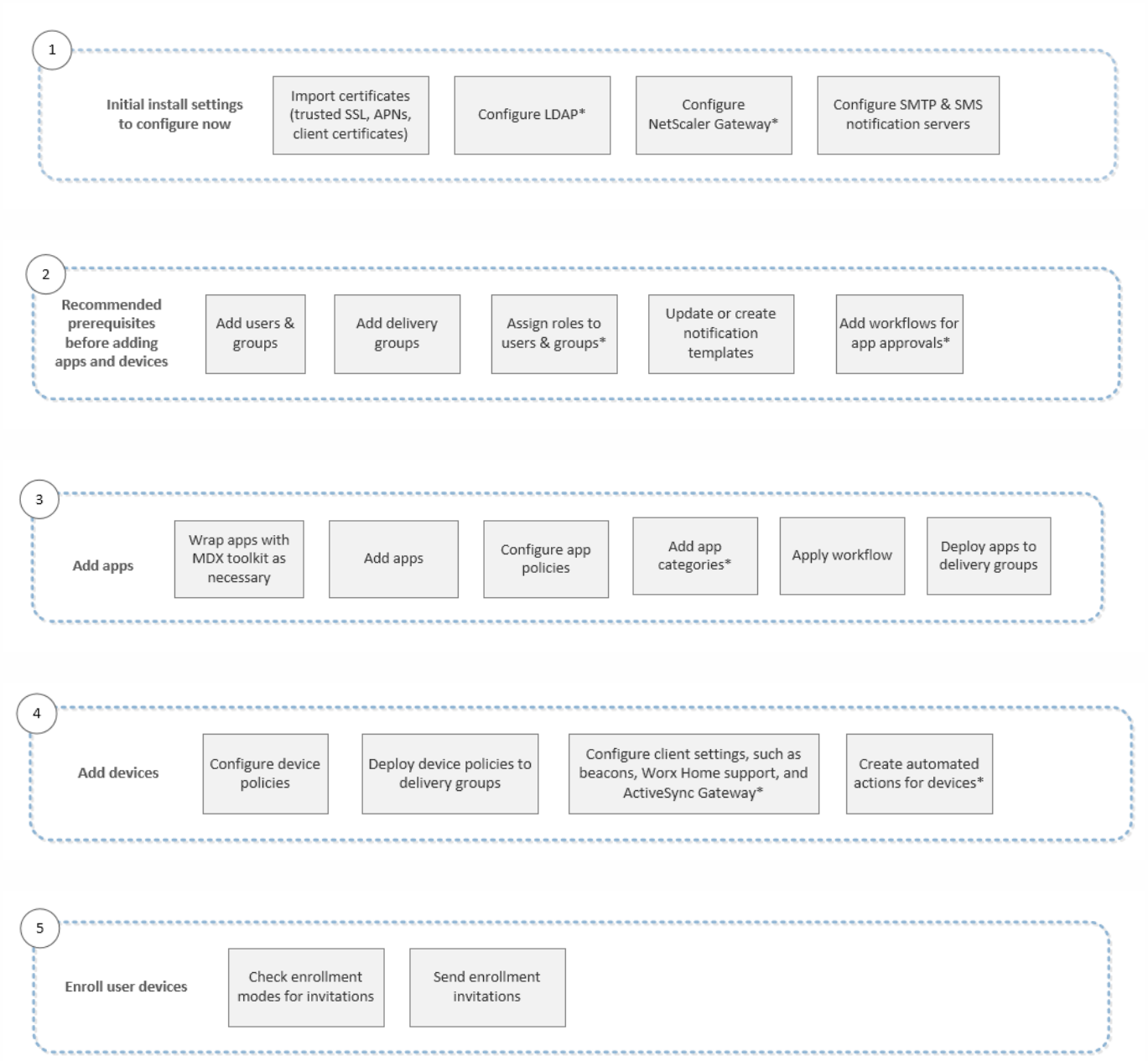
XenMobile 控制台是 XenMobile 10 中的统一管理工具，结合了 XenMobile 9 及更早版本中的 App Controller 和 Device Manager 组件。此主题假设您已安装了 XenMobile，并准备好使用此控制台。如果要安装 XenMobile，请参阅安装 XenMobile。

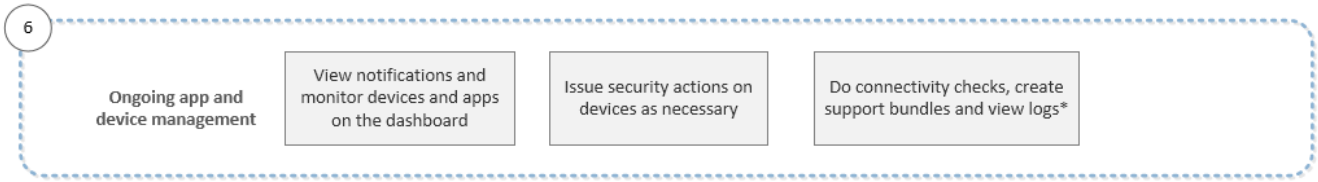
XenMobile 控制台在最近的两个 Firefox、Chrome 和 Internet Explorer 版本中受支持。

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。

提示：单击每行可打开包含详细信息和步骤链接的主题。

注意：带星号的项目为可选项目。



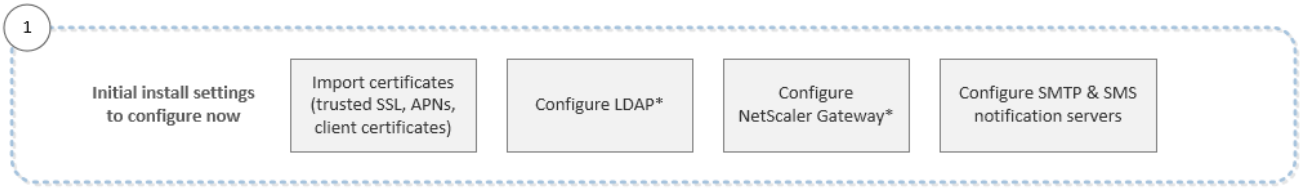


初始设置工作流

May 05, 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。要开始，请单击**配置** > **设置**。要查看整个工作流，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 eDocs 主题：

- XenMobile 中的证书
- LDAP 配置
- NetScaler Gateway 和 XenMobile
- XenMobile 中的通知

控制台必备条件工作流

May 05, 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 eDocs 主题：

- 配置用户帐户、角色和注册设置
- 在 XenMobile 中管理交付组
- 在 XenMobile 中使用 RBAC 创建或更新自定义角色
- 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

添加应用程序工作流

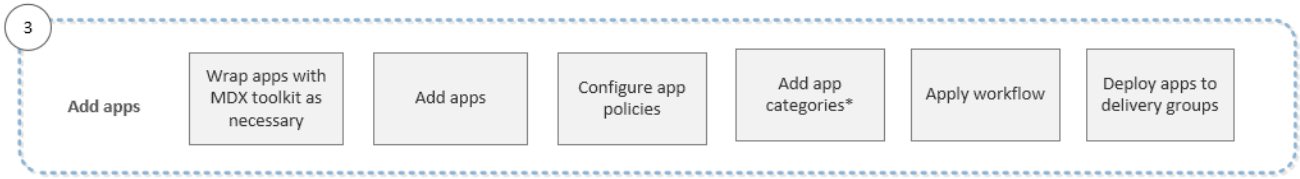
May 05, 2016

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 eDocs 主题：

- 使用 MDX Toolkit 打包应用程序
- 向 XenMobile 添加应用程序
- 适用于 iOS、Android 和 Windows Phone 8.1 的 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

添加设备工作流

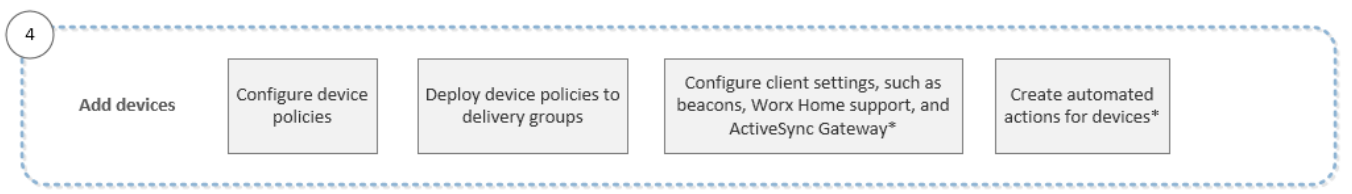
May 05, 2016

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 eDocs 主题：

- 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

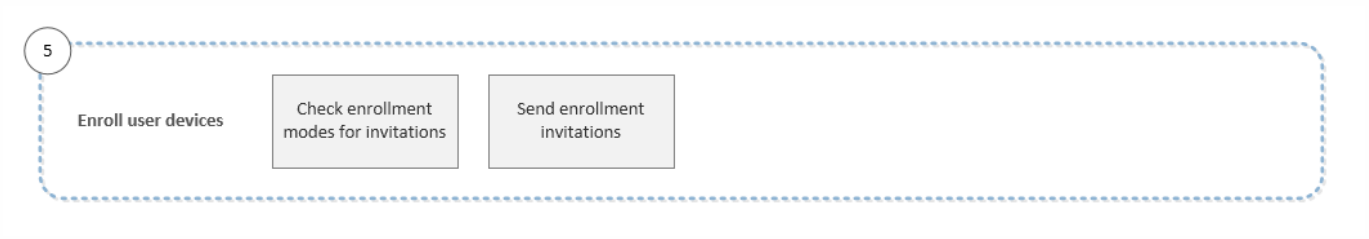
注册用户设备工作流

May 05, 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 eDocs 主题：

- 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

正在进行的应用程序和设备管理工作流

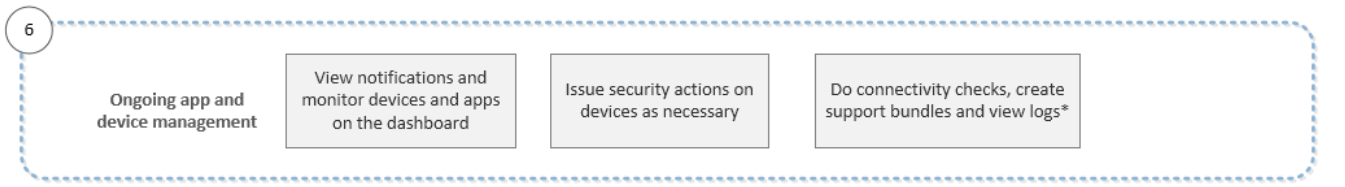
May 05, 2016

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。

XenMobile 控制台中的过滤器和表格

May 05, 2016

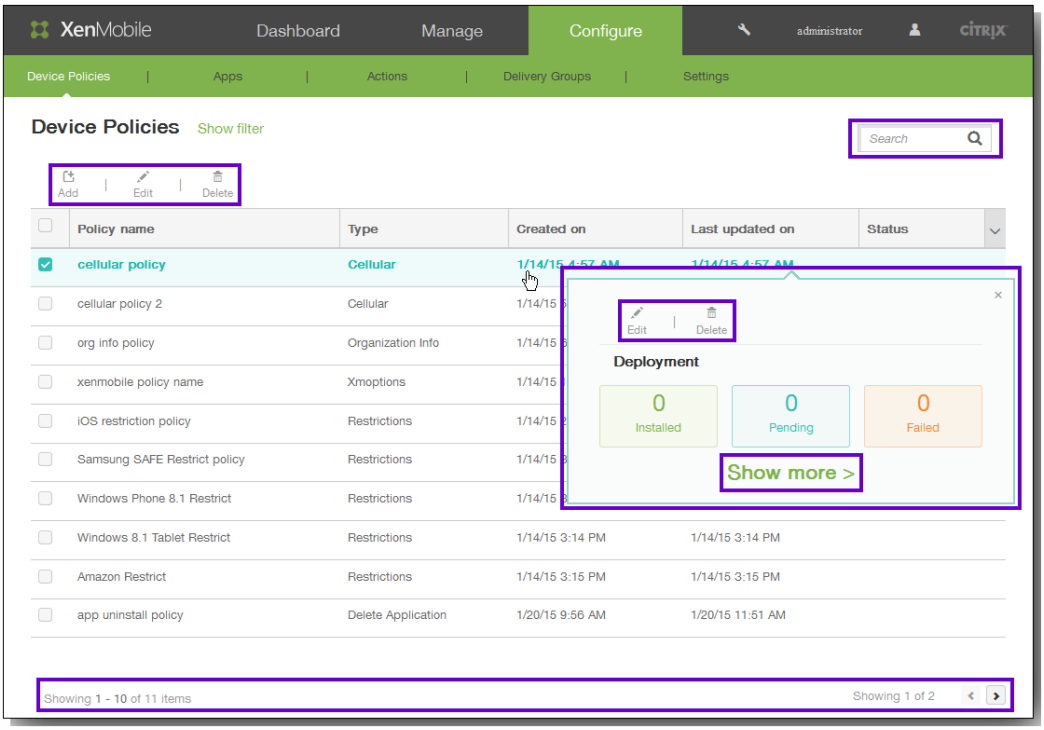
过滤器和表格存在于整个 XenMobile 控制台中，位于“Devices”（设备）、“Enrollment”（注册）、“Device Policies”（设备策略）、“Apps”（应用程序）、“Actions”（操作）和“Delivery Groups”（交付组）选项卡中。利用过滤器，可以缩小控制台上的这些区域中的信息范围，以精确查找您要查看的信息。利用表格，可以通过单击来查看用于针对在此表格中找到的信息采取操作的选项。

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：

- 可以选中策略旁边的复选框，以在策略列表的上方显示选项菜单。
- 可以选中多个策略旁边的复选框，以同时删除所有这些策略。
- 可以单击列表中的某个策略，以在此列表的右侧显示选项菜单。单击显示更多时，可以看到关于配置的详细信息列表。
- 可以在搜索框中键入完整或部分策略名称，以限制列出的策略数。

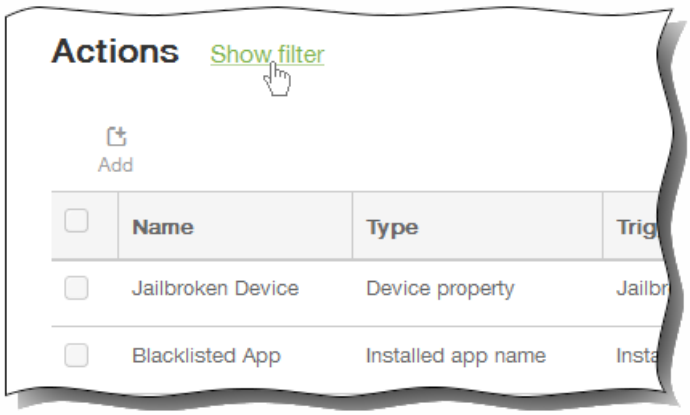
下图显示了这些选项在控制台的“设备策略”区域的显示方式。每页仅列出 10 个项目。单击页面右下角的三角形可以向前和向后移动页面。



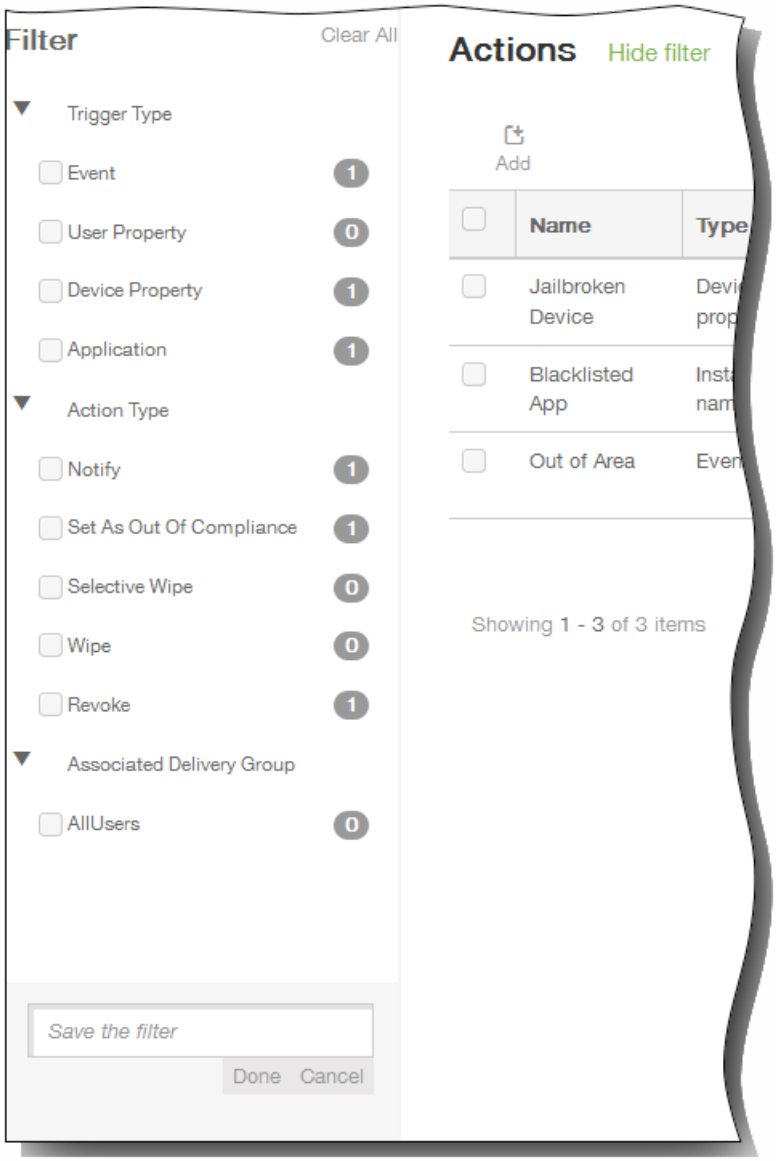
在 XenMobile 控制台中过滤信息

要在控制台的某个区域中查看信息的特定子集，如“设备”、“注册”、“设备策略”、“应用程序”、“操作”和“交付组”，可以根据您选择的条件过滤列表。此过程使用“操作”页面作为示例，但是过滤步骤在整个控制台中均相同。

1. 在操作页面中，单击显示过滤器。

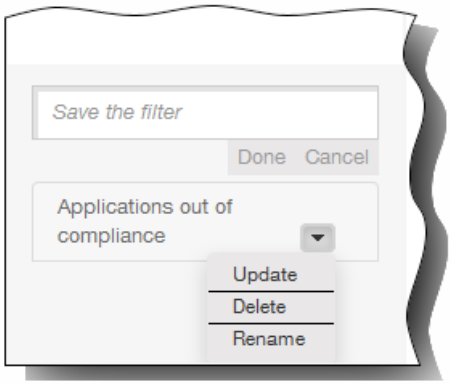


将显示过滤器面板，其中列出了过滤操作列表可以依据的条件。每个条件右侧的数字表示包含此条件的操作数。



2. 单击过滤器左侧的三角形，以显示该过滤器可以使用的选项。

3. 选择要使用的过滤条件。 操作列表中将仅包含满足所选条件的操作。
4. 执行以下操作之一：
   - 单击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。
5. 如果要将所选条件保存在自定义过滤器中，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，可以在过滤器面板的底部选择此过滤器。
   注意：如果单击过滤器名称右侧的三角形，可以使用新条件或更改后的条件更新过滤器、删除过滤器或重命名过滤器。

通知

May 05, 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，请参阅在 XenMobile 中创建自动化操作。

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。

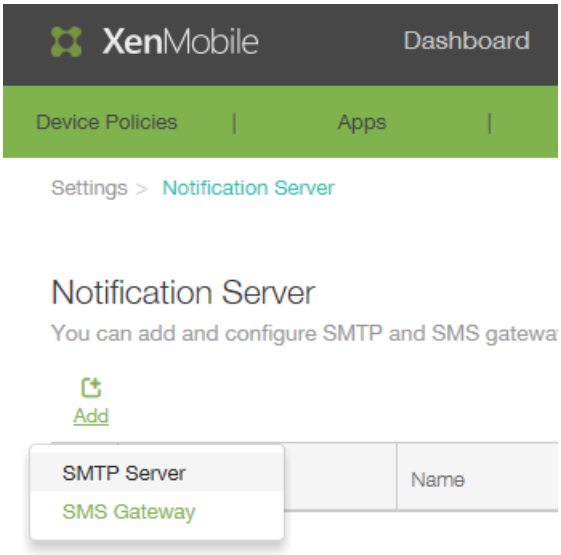
本主题中的过程讨论添加 SMTP 服务器、SMS 网关和运营商 SMS 网关的信息。

配置 SMTP 服务器和 SMS 网关

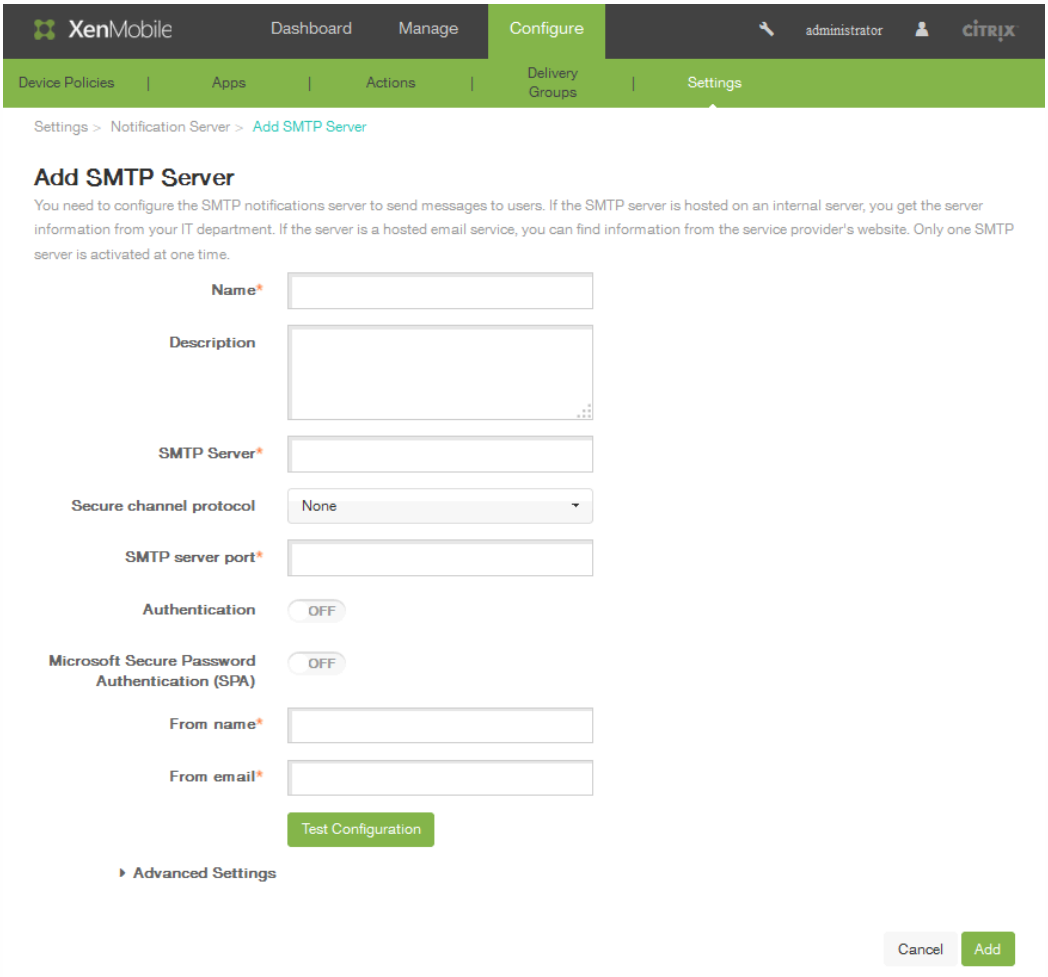
必备条件：

- 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。

1. 在 XenMobile Web 控制台中，单击配置 > 设置 > 更多 > 通知服务器。
   此时将显示通知服务器配置页面。



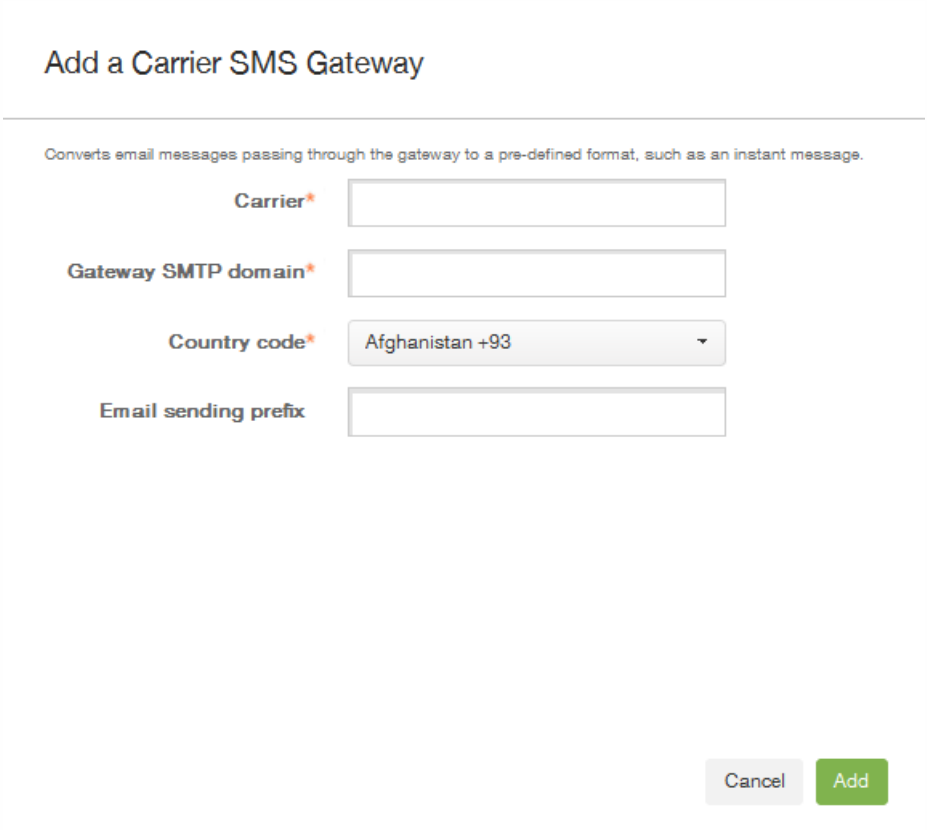
2. 单击添加，单击 SMTP 服务器或 SMS 网关，然后按照后续步骤中针对每个选项的过程操作。
   - 要添加 SMTP 服务器，请遵循步骤 3 至 6。
   - 要添加 SMS 网关，请遵循步骤 7 至 9。
3. 如果单击以添加 SMTP 服务器，将显示添加 SMTP 服务器页面。



4. 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。默认情况下，此字段设置为无。
- SMTP 服务器端口：键入 SMTP 服务器使用的端口。默认情况下，此端口设置为 25；如果 SMTP 连接使用 SSL 安全通道协议，则此端口设置为 465。
- 身份验证：选择开或关。默认情况下，此功能处于禁用状态。
- 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。默认情况下，此功能处于禁用状态。
- 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。
- 测试配置：单击以发送测试电子邮件通知。

5. 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。默认情况下，此字段设置为 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。默认情况下，此字段设置为 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。默认情况下，此值设置为 100。
6. 配置 SMTP 服务器后，单击**添加**。
7. 在通知服务器配置页面，要配置 SMS 网关，请单击添加，然后单击 SMS 网关。
   此时将显示添加 SMS 网关页面。



   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。
8. 配置以下设置：
   - 名称：标识 SMS 网关配置。
   - 说明：可选，输入配置的说明。
   - 密钥：键入系统管理员在激活帐户时提供的数字标识符。

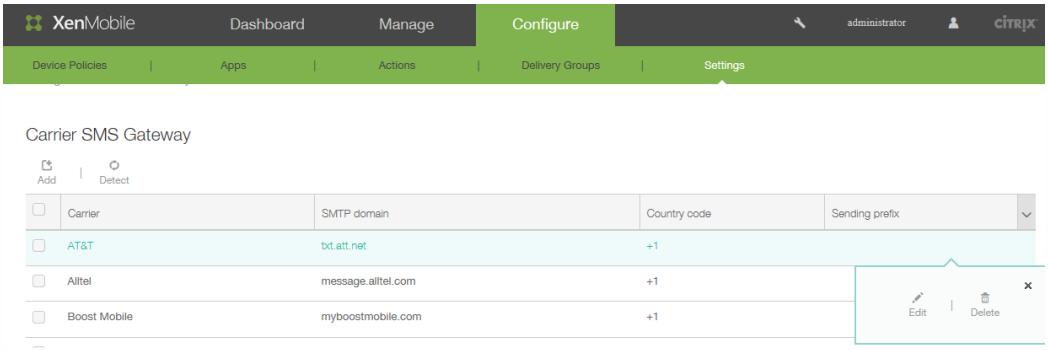
- 密码：键入系统管理员提供的密码，当密码丢失或被盗时用于访问您的帐户。
- 虚拟电话号码：向北美电话号码（前缀为 +1）发送时使用此字段。必须输入 Nexmo 虚拟电话号码；否则，请输入有意义的标签或名称。可以在 Nexmo Web 站点上购买虚拟电话号码。
- HTTPS：如果要使用 HTTPS 将 SMS 请求传输到 Nexmo，请选中此选项。
- 国家/地区代码：在此列表中，单击贵组织收件人的默认 SMS 国家/地区代码前缀。此字段始终以 + 符号开头。
- 测试配置：单击此选项将使用当前的配置发送测试消息。系统会立即检测到连接错误并将其显示出来，如身份验证或虚拟电话号码错误。接收消息的时间范围与移动电话之间发送消息的时间范围相同。

9. 单击添加。

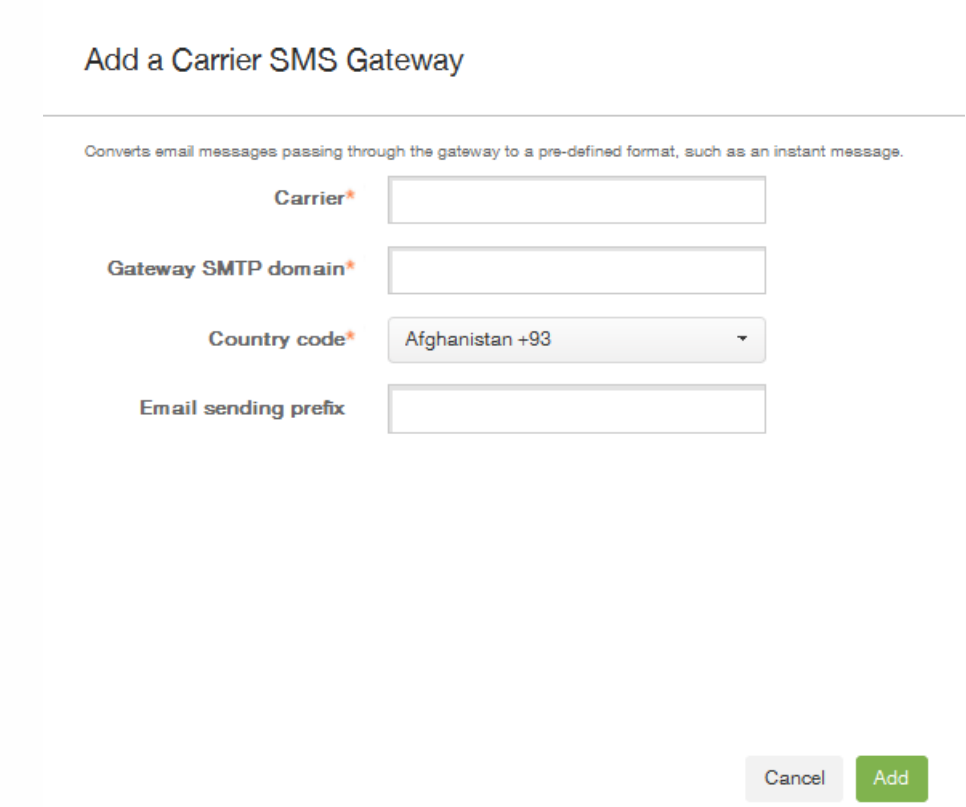
添加运营商 SMS 网关

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 Web 控制台中，单击配置 > 设置 > 更多 > 运营商 SMS 网关。 此时将显示运营商 SMS 网关配置页面。



2. 单击添加以添加新运营商。 单击检测以自动检测网关。此时将显示 添加运营商 SMS 网关对话框。



3. 键入以下信息： 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. 运营商：键入运营商的名称。
   2. 网关 SMTP 域：键入与 SMTP 网关关联的域。
   3. 国家/地区代码：在列表中，单击运营商的国家/地区代码。
   4. 电子邮件发送前缀：可选，指定电子邮件发送前缀。

证书

May 05, 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。

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 component	Certificate format	Required certificate type
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL, Root NetScaler Gateway converts PFX to PEM automatically.
XenMobile server	PEM or PFX (PKCS#12)	SSL, SAML, APNs XenMobile also generates a full PKI during the installation process.
StoreFront	PFX (PKCS#12)	SSL, Root

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。

配置用于身份验证的客户端证书

NetScaler Gateway 支持使用客户端证书进行身份验证。 登录到 NetScaler Gateway 的用户还可基于向虚拟服务器提交的客户端证书的属性进行身份验证。 客户端证书身份验证也可以与其他身份验证类型（如 LDAP 或 RADIUS）结合使用，以提供双因素身份验证。

要基于客户端证书属性对用户进行身份验证，应在虚拟服务器上启用客户端身份验证，并申请客户端证书。 必须在 NetScaler Gateway 上将根证书与虚拟服务器绑定在一起。

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。

用户登录到 NetScaler Gateway 并通过身份验证后，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。

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。

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。

在 XenMobile 中上载证书

May 05, 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，您还可以使用“证书”区域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。

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。

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。

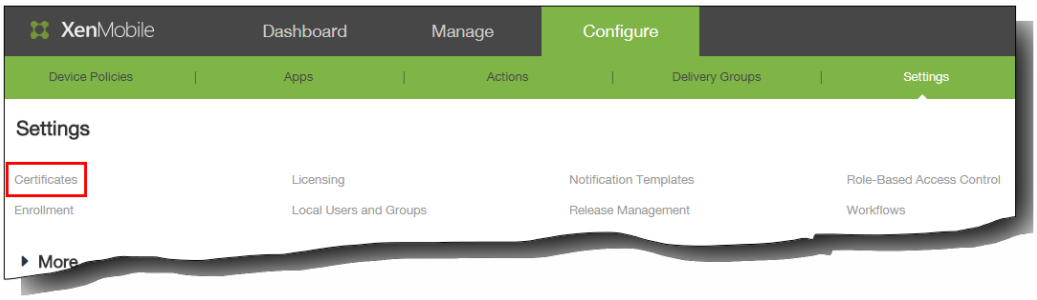
XenMobile 支持以下证书输入格式：

- 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）

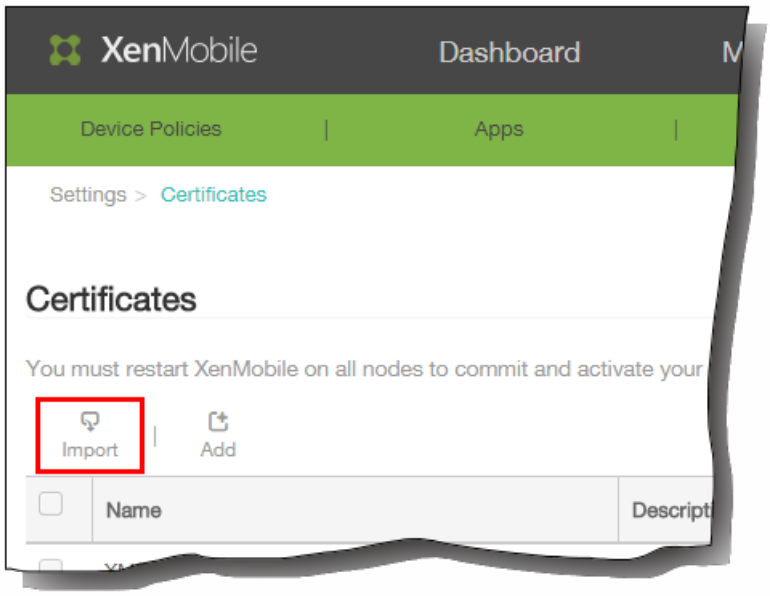
导入密钥库

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，单击配置 > 设置 > 证书。

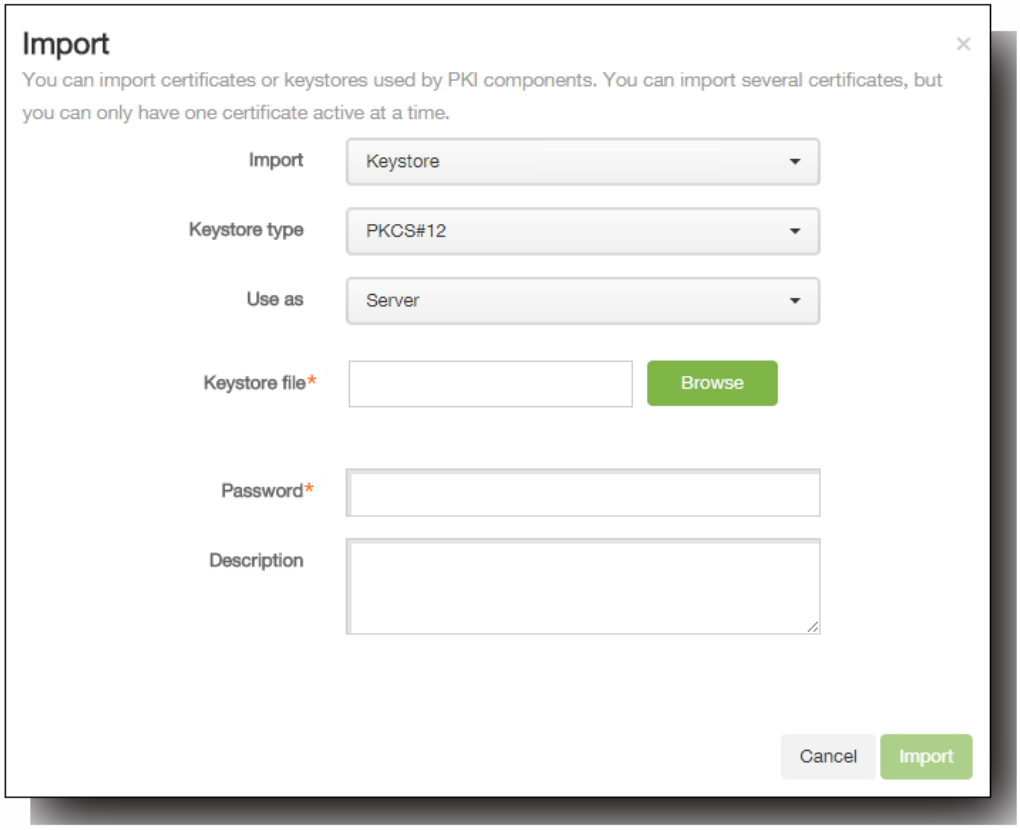


2. 在证书页面上，单击导入。



此时将显示导入对话框。

3. 在导入对话框中的导入中，单击密钥库。



导入对话框将更改，以反映可用的密钥库选项，如上图所示。

4. 在密钥库类型中，单击 PKCS#12。
5. 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。
- **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。

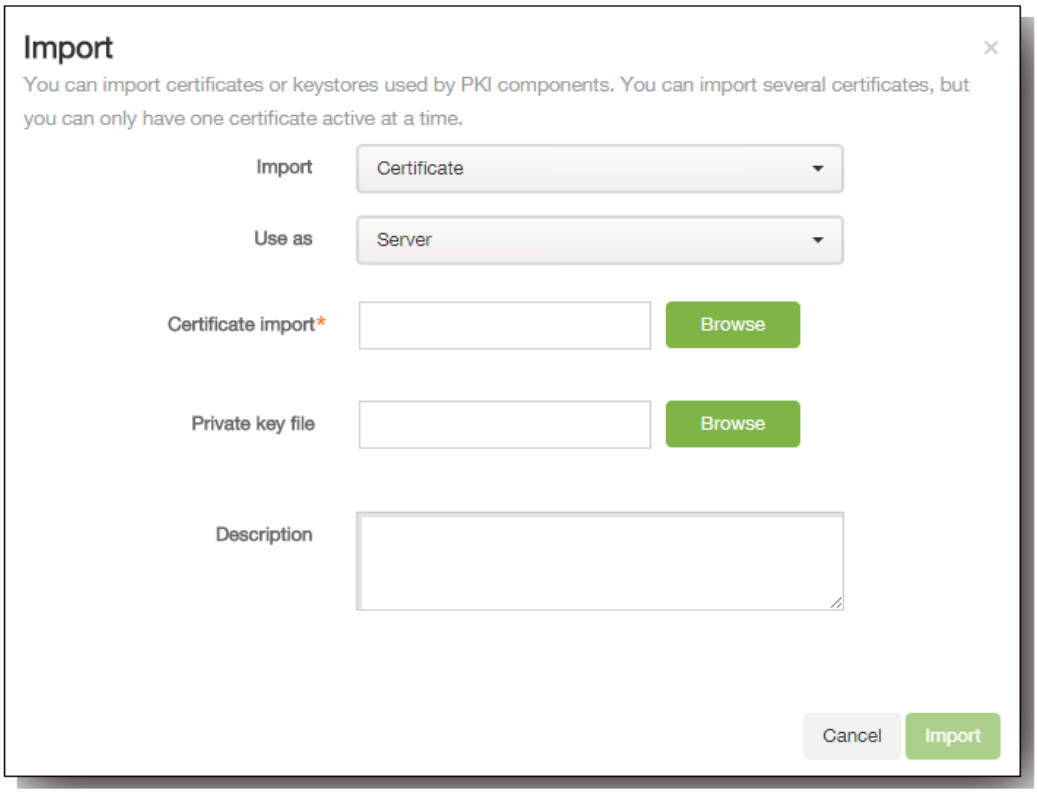
6. 浏览以查找要导入的密钥库。
7. 在密码中，键入分配给证书的密码。
8. 键入密钥库的说明（可选），以帮助您将其与其他密钥库区分开。
9. 单击 Import（导入）。密钥库将添加到证书表中。

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，单击配置 > 设置 > 证书。
2. 在证书页面上，单击导入。此时将显示导入对话框。
3. 在导入对话框的导入中，如果尚未选择，请单击证书。



导入对话框将更改以反应可用的证书选项。

4. 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 Import（导入）。证书将添加到证书表中。

更新证书

在任何时间，XenMobile 都仅允许系统中每个公钥存在一个证书。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 控制台中导入对话框的配置 > 设置 > 证书下面，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。

PKI 实体

May 05, 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。

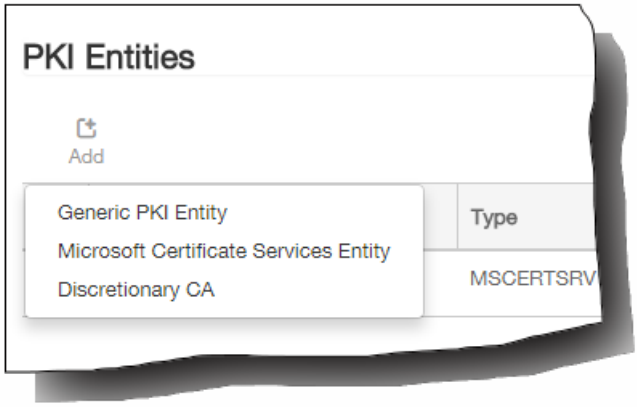
作为 SOAP Web 服务端点，GPKI 适配器可发布自我描述的 Web 服务描述语言 (WSDL) 定义。创建 GPKI PKI 实体相当于通过 URL 或上载文件本身为 XenMobile 提供该 WSDL 定义。

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。

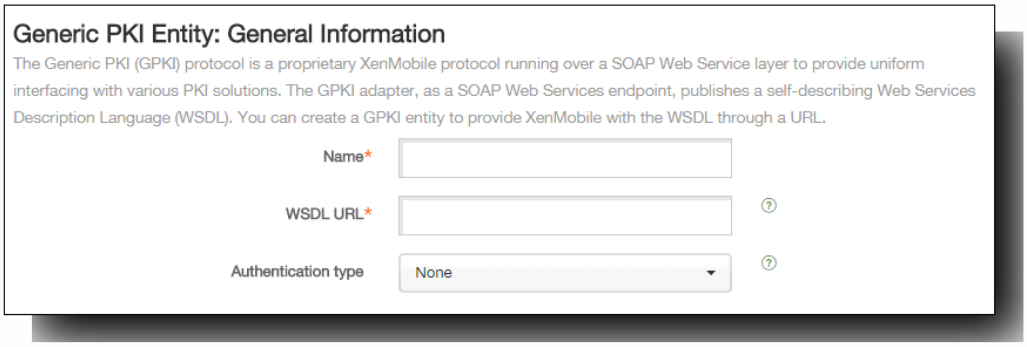
用户参数是指由 GPKI 适配器针对特定操作定义的参数，您需要为 XenMobile 提供这些参数的值。XenMobile 通过解析 WSDL 文件，决定适配器支持哪些操作（拥有哪些功能）以及适配器针对每个操作所需的参数。如果选择此项，则使用 SSL 客户端身份验证保护 XenMobile 与 GPKI 适配器之间的连接。

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 (GPKI)实体: 常规信息页面。



4. 在通用 PKI (GPKI)实体: 常规信息页面上，执行以下操作：
   1. 名称：键入 PKI 实体的描述性名称。
   2. WSDL URL：键入描述适配器的 WSDL 的位置。
   3. 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。
   4. 单击下一步。
      此时将显示通用 PKI 实体: 适配器功能页面。
5. 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。

6. 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，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。
7. 单击保存。
   实体将显示在 PKI 实体表格中。

Microsoft Certificate Services

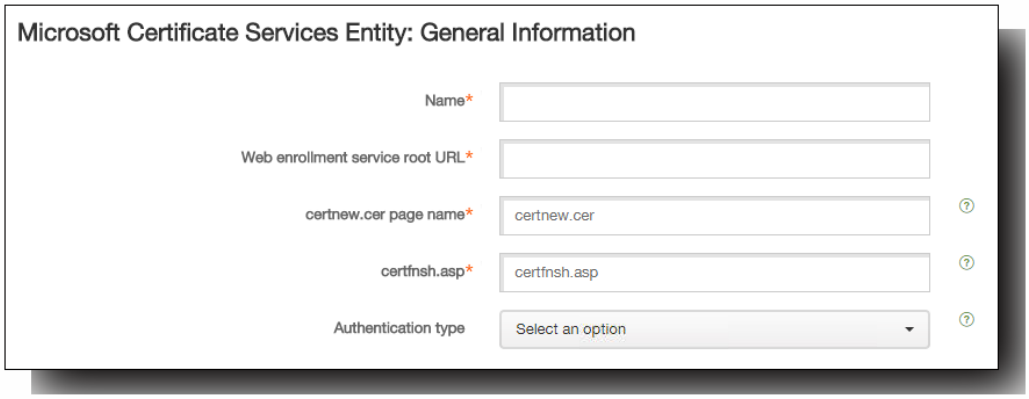
XenMobile 通过其 Web 注册界面与 Microsoft Certificate Services 交互。XenMobile 仅支持通过该界面颁发新证书（相当于 GPKI 签名功能）。

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 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：
   1. 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。
   2. 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。
   3. 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。
   4. 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。
   5. 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。
      - 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。

5. 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。
6. 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。

7. 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。

8. 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。
9. 单击保存。
   实体将显示在 PKI 实体表格中。

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：

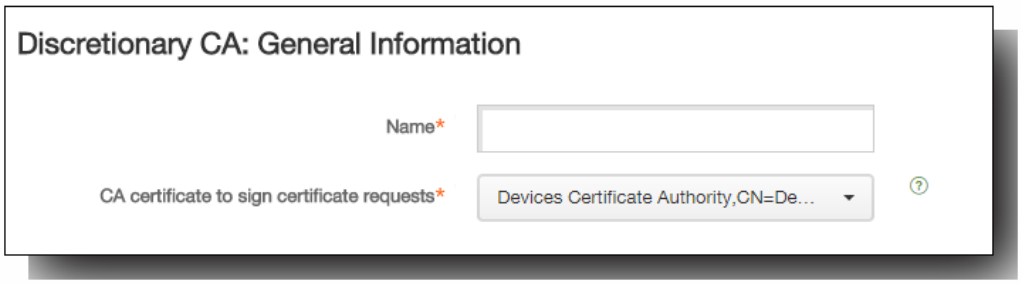
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

响应通过 SHA-256 及签名证书的密钥算法（DSA、RSA 或 ECDSA）进行签名。

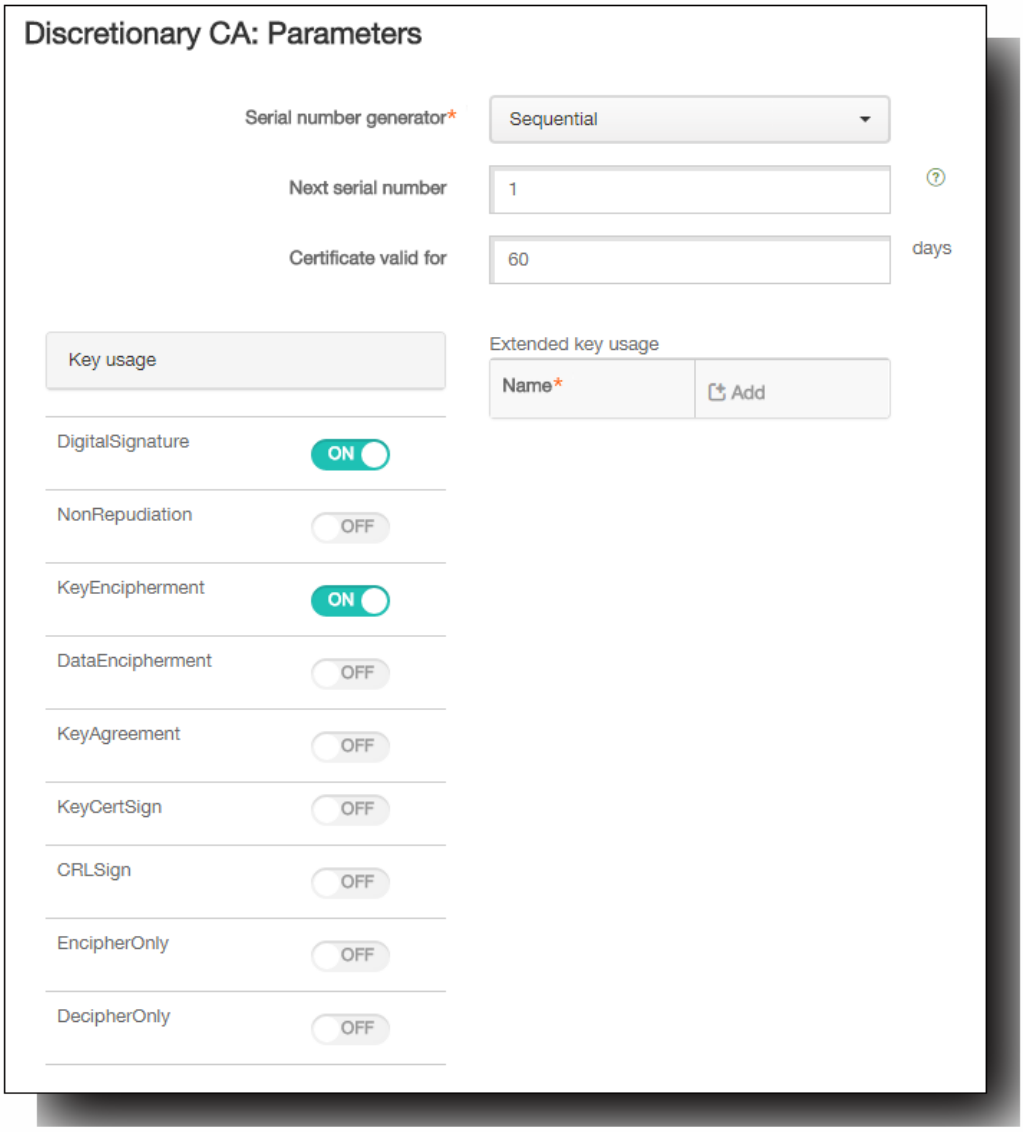
添加任意 CA

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：
   1. 名称：键入任意 CA 的描述性名称。
   2. CA certificate to sign certificate requests（为证书请求签名的 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。
   3. 单击下一步。
      此时将显示 Discretionary CA: Parameters（任意 CA: 参数）页面。



5. 在 Discretionary CA: Parameters（任意 CA: 参数）页面上，执行以下操作：
   1. 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。
   2. 下一个序列号：键入一个值，用于确定颁发的下一个号码。
   3. 证书有效期：键入证书有效的天数。
   4. 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。
   5. 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。
   6. 单击下一步。
      此时将显示 Discretionary CA: Distribution（任意 CA: 分发）页面。

6. 在 Discretionary CA: Distribution（任意 CA: 分发）页面上，选择分发模式:
   - 集中: 服务器端生成证书。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。
   - 分散: 设备端生成密钥。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。
7. 单击下一步。
   此时将显示任意 CA: 联机证书状态协议(OCSP)页面。

8. 在任意 CA: 联机证书状态协议(OCSP)页面上，执行以下操作：
   1. 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。
   2. 如果启用了 OCSP 支持，请选择 OSCP 签名 CA 证书。此证书列表使用您通过配置 > 设置 > 证书上载到 XenMobile 的 CA 证书生成。
9. 单击保存。
   任意 CA 将显示在 PKI 实体表格中。

-
-
-
-
-

-

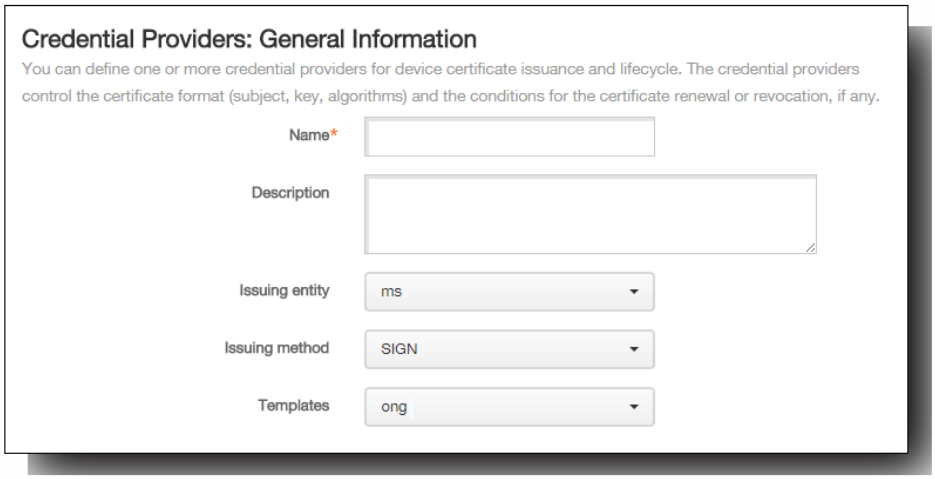
可以采用两种途径获取证书（称为颁发方法）：

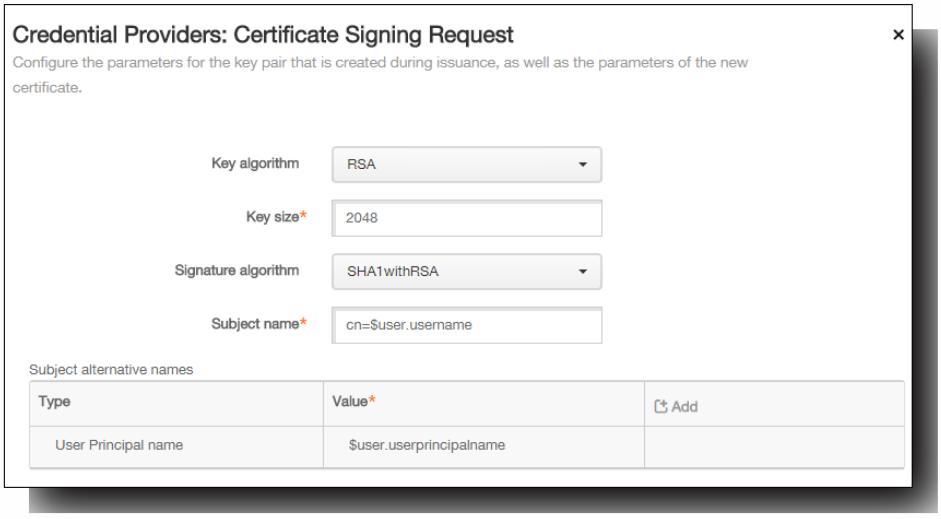
- 签名。 利用此方法，颁发包括创建新私钥、创建 CSR 和将 CSR 提交给证书颁发机构 (CA) 进行签名。 XenMobile 支持对三种 PKI 实体（Microsoft 证书服务实体、通用 PKI 和任意 CA）使用此签名方法。
- 提取。 利用此方法，用于 XenMobile 的颁发是指对现有密钥对的恢复。 XenMobile 仅支持对通用 PKI 使用提取方法。

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。

-
-

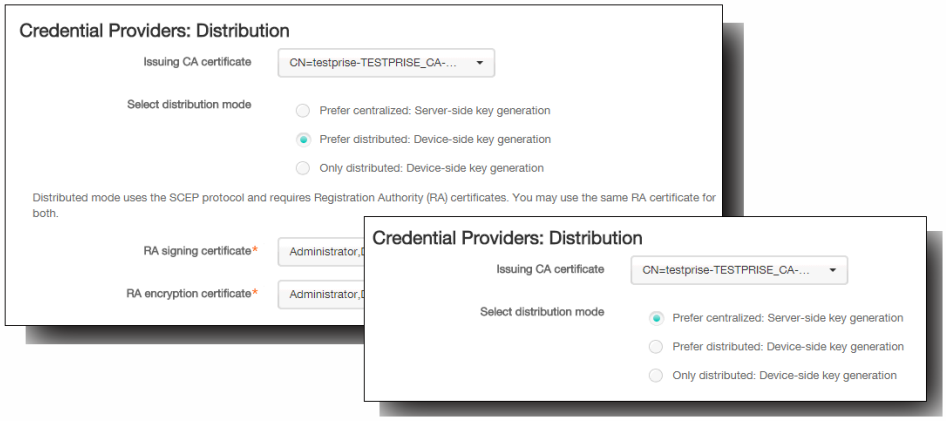
-
-
-

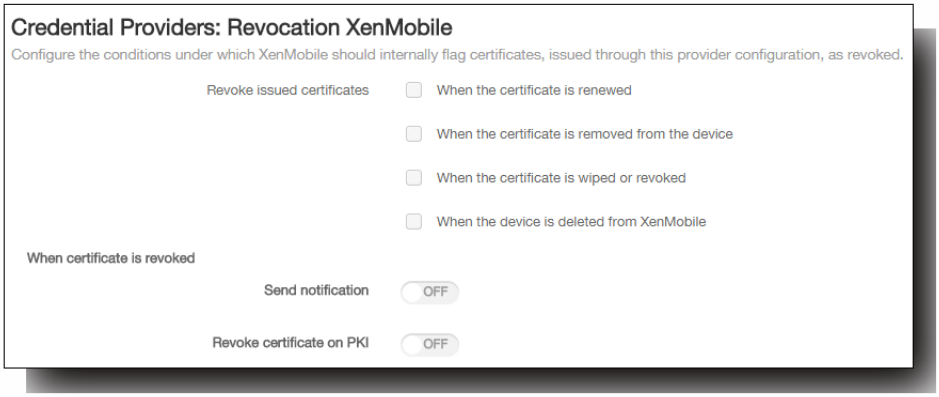


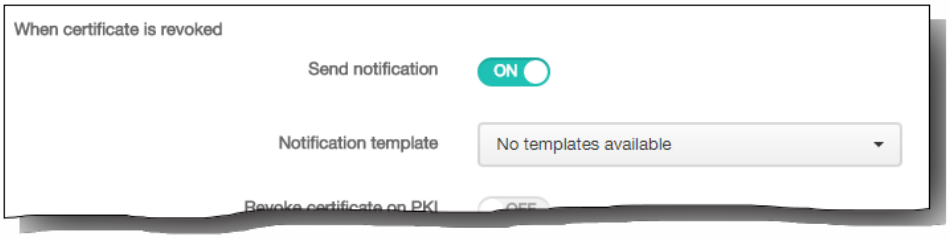


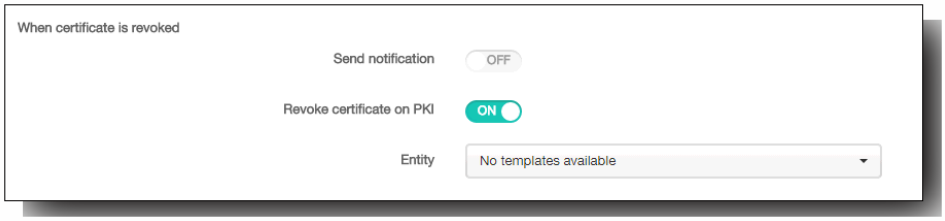
CN=${user.username} OU=${user.department} O=${user.companyname} C=${user.c}\endquotation

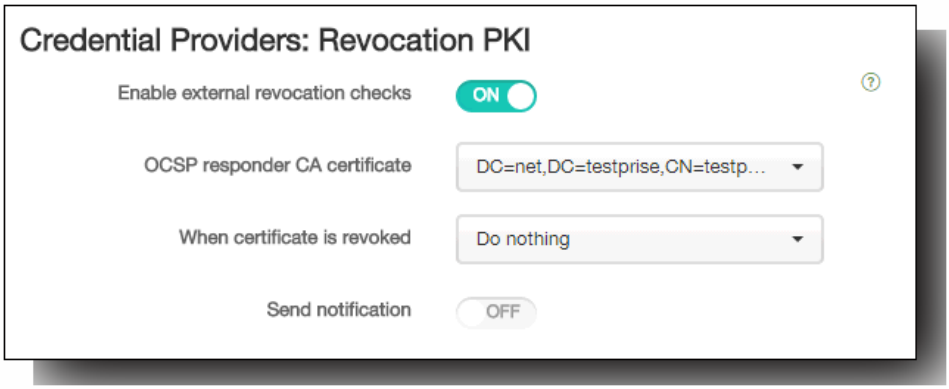
-
-
-







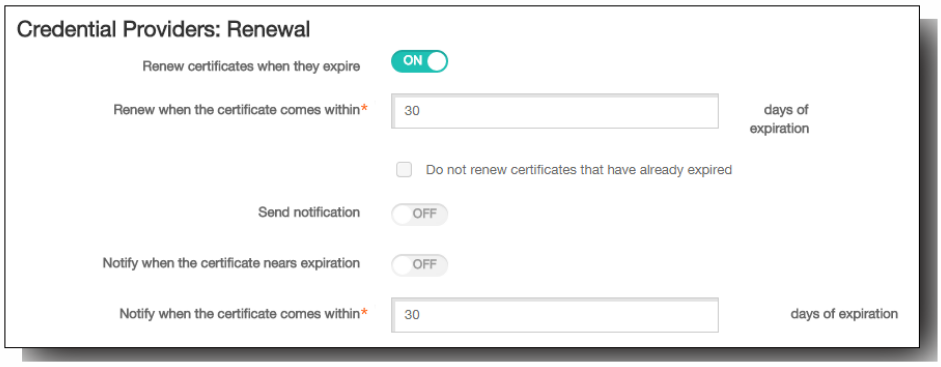




-
-
-

-
-

-
-

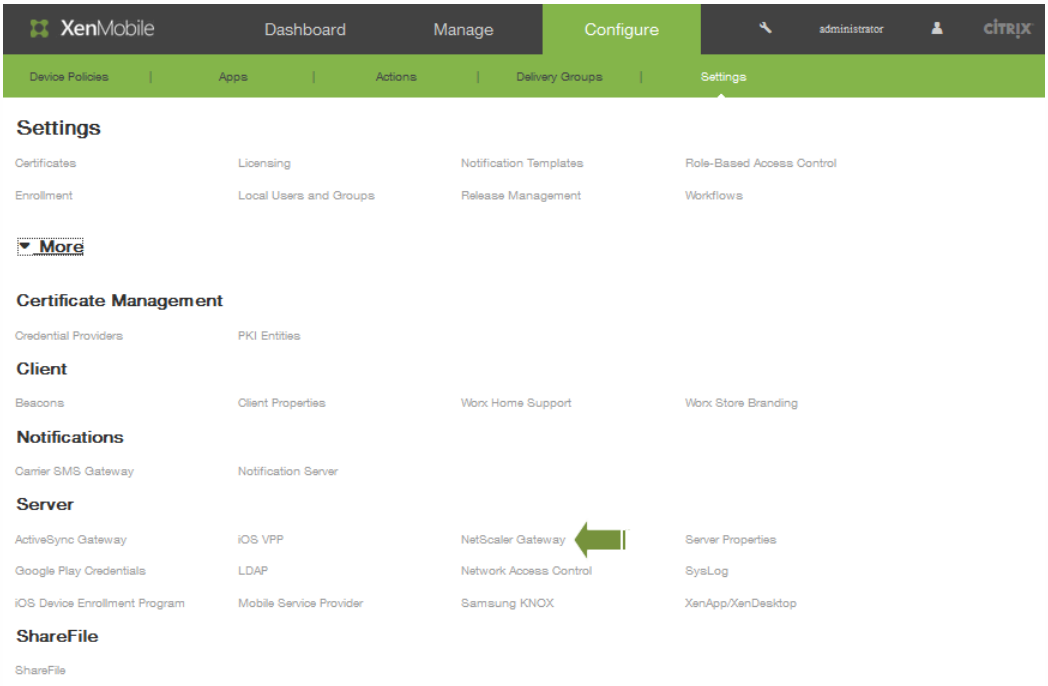


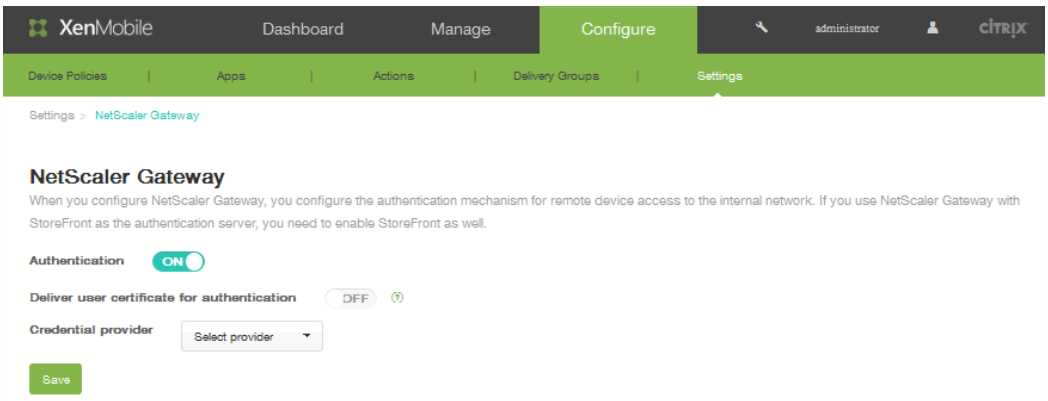
-
-

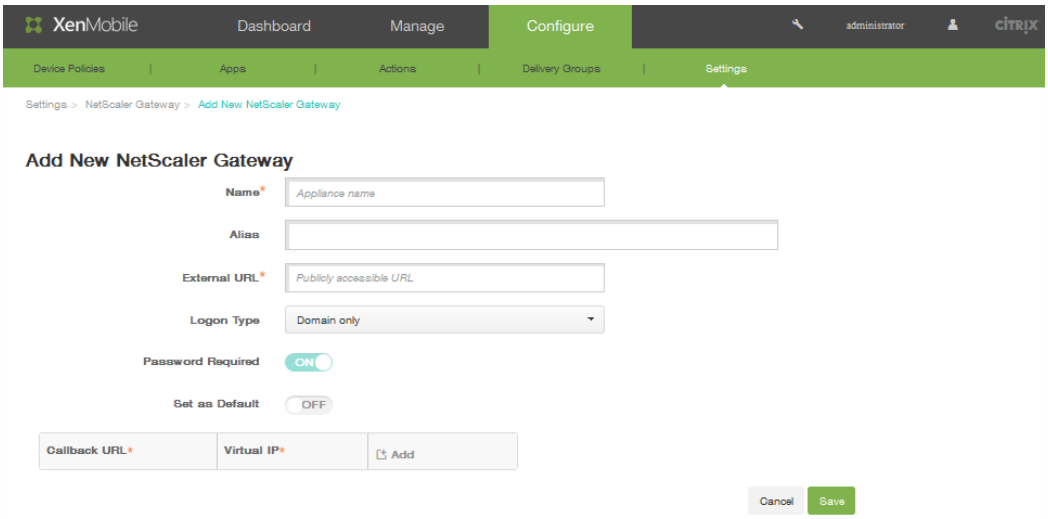
-
-

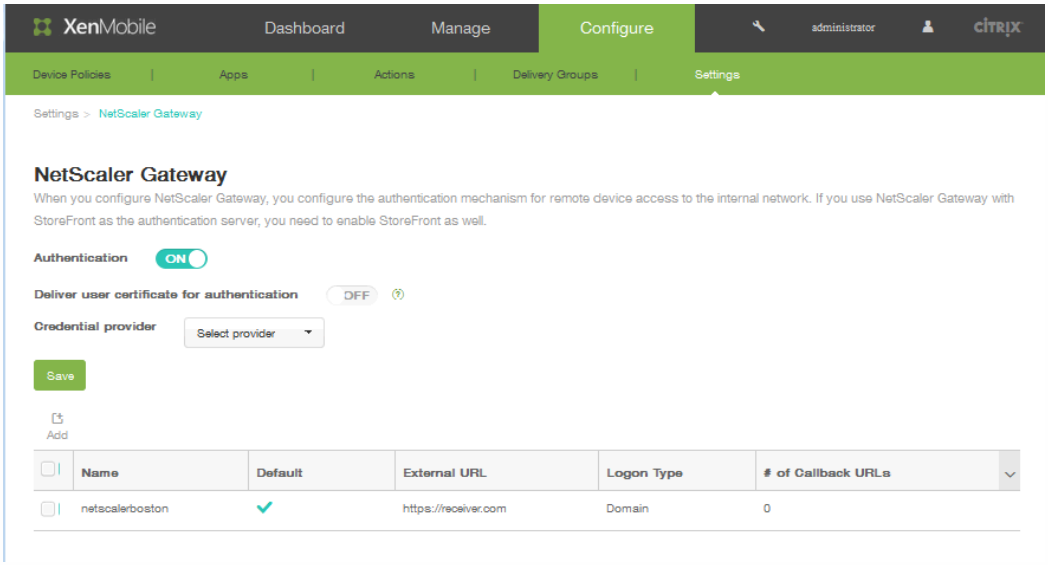
-
-
-
-
-
-

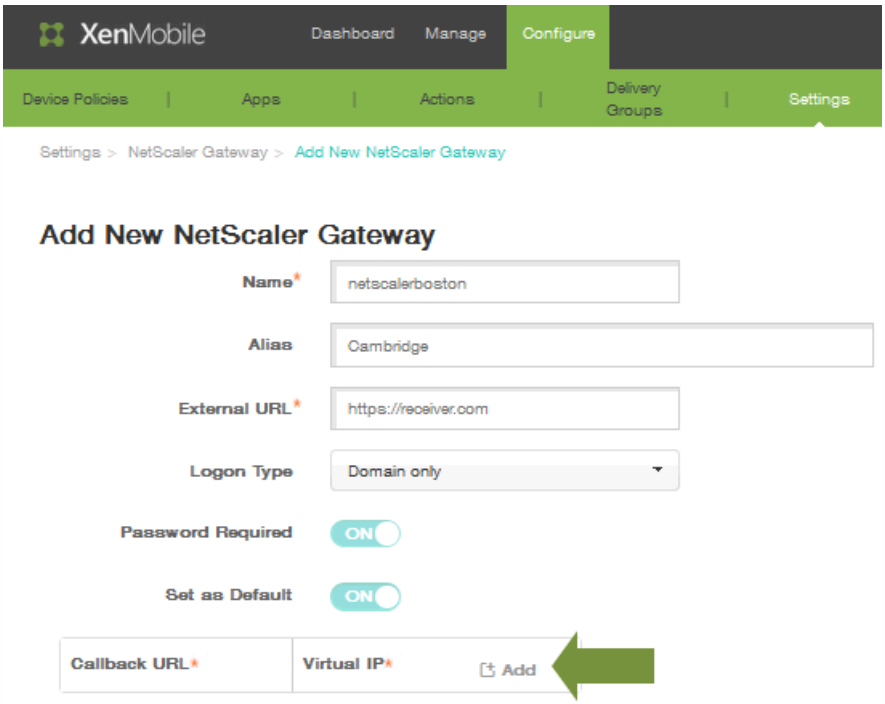
-
-
-











-
-
-
-

-
-

-

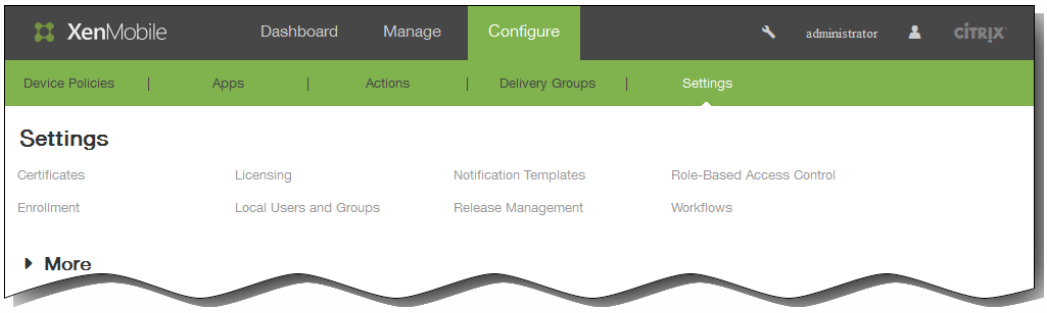
-
-
-
-

-

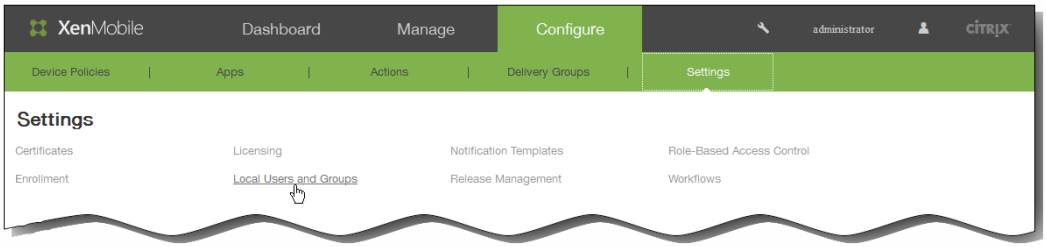
-

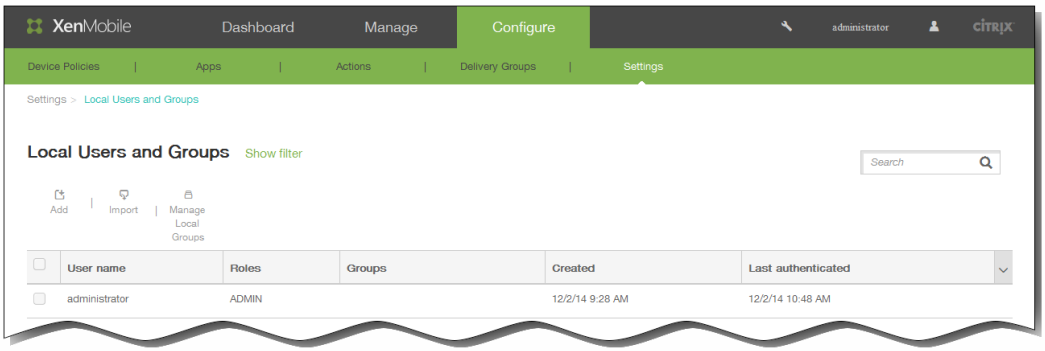
-

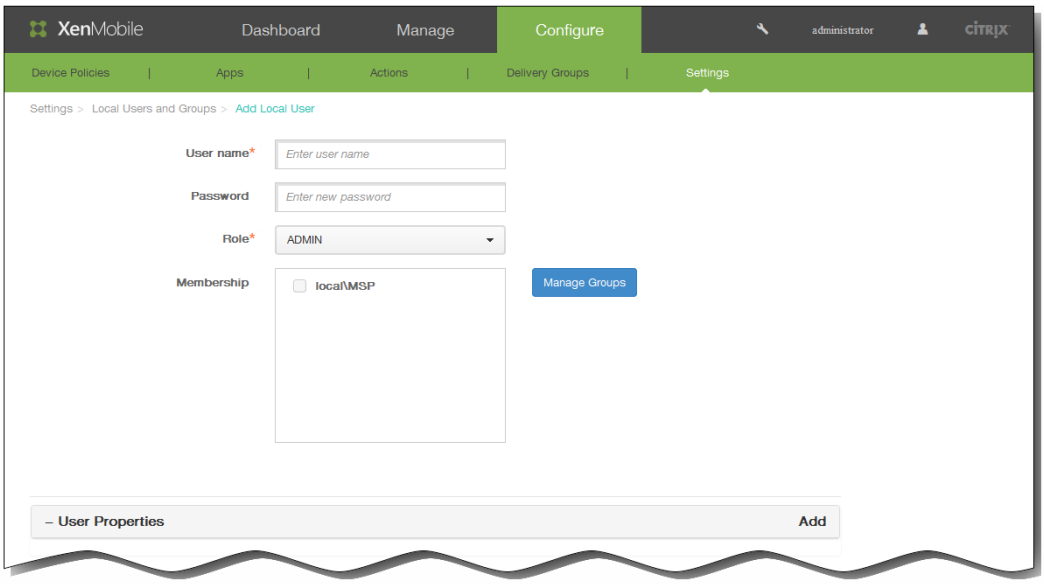
-
-

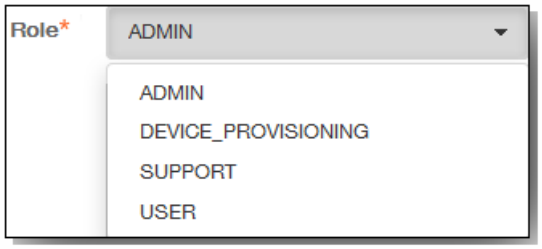


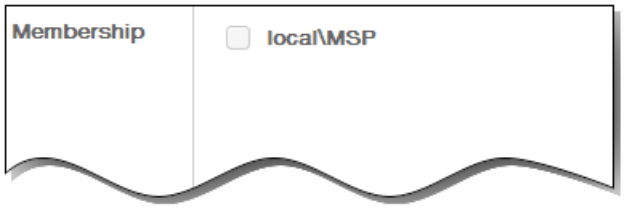
-
  -
  -
  -
-
  -
  -
-
  -
-
  -

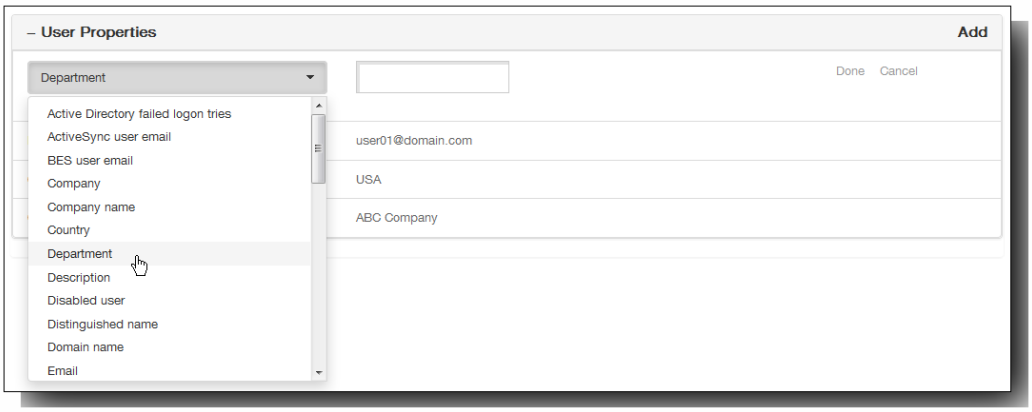


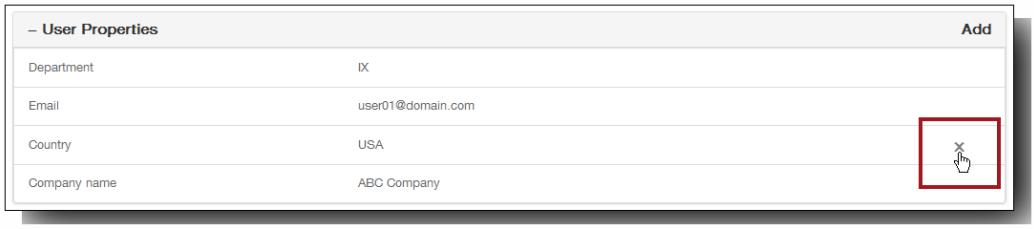


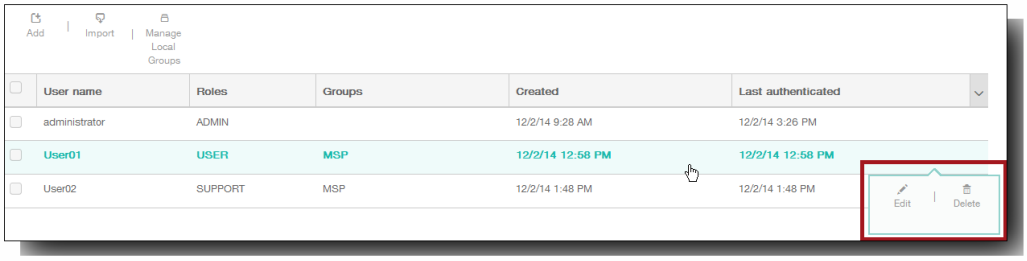


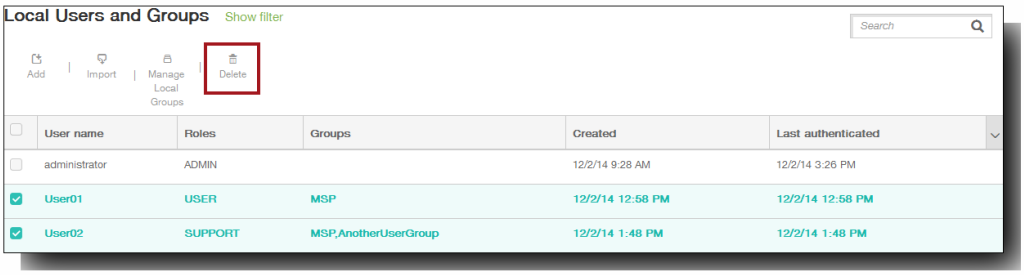


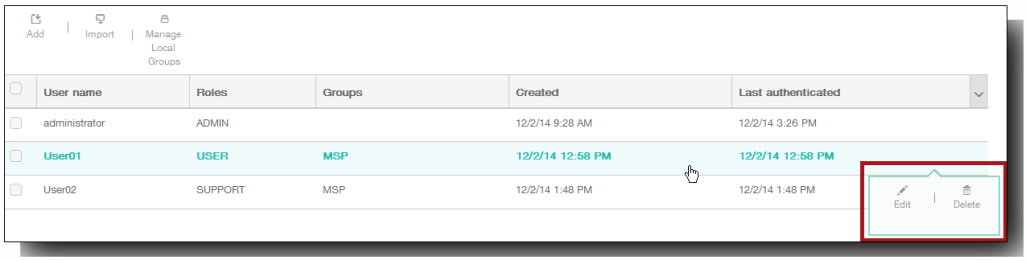




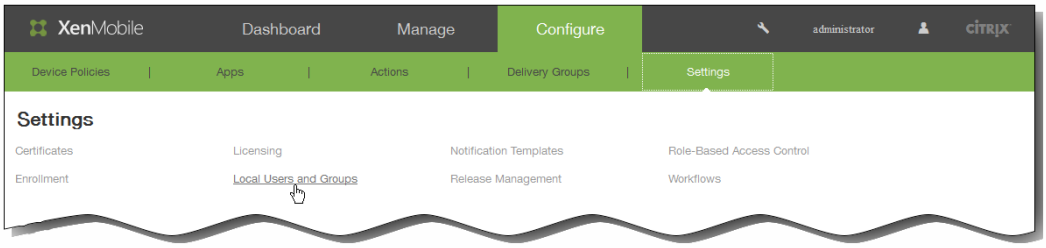


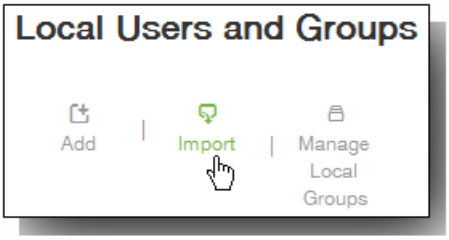


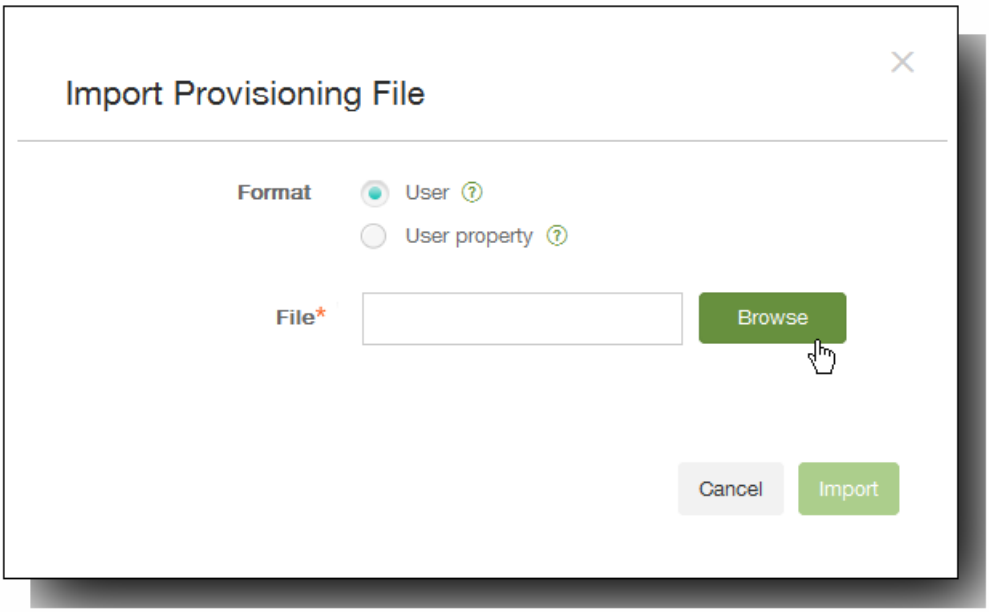
- 

- 

-
-
-







- user;password;role;group1;group2
- user;propertyName1;propertyValue1;propertyName2;propertyValue2

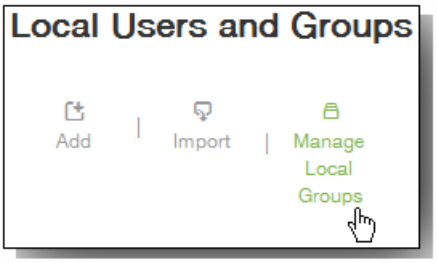
- propertyV;test;1;2 propertyV\;test\;1\;2
-
-
-

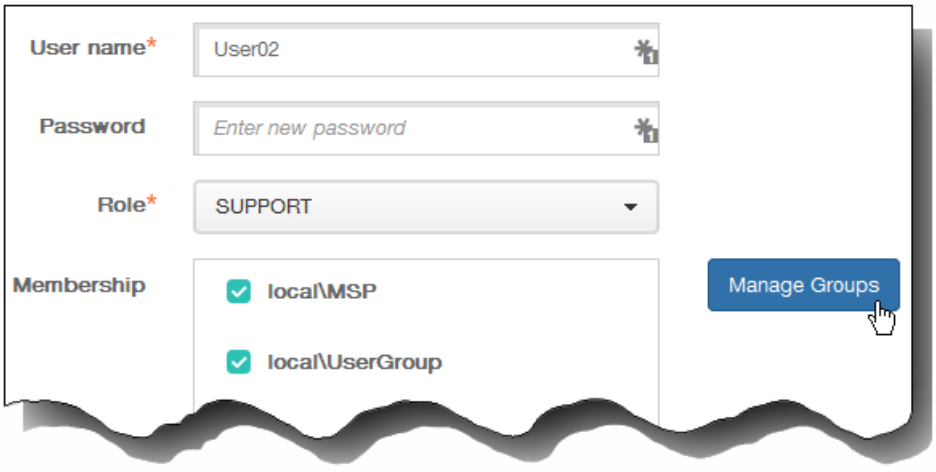
user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01

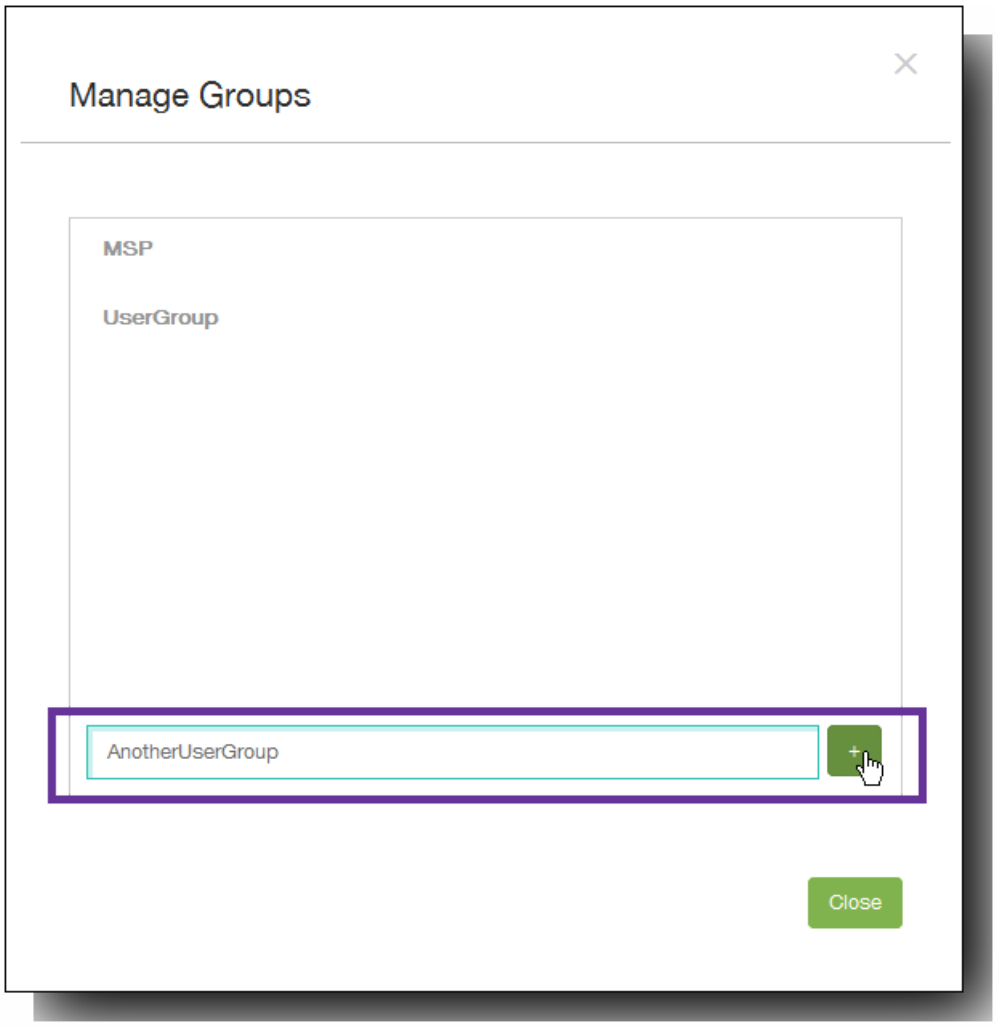
-
-
-
-
  -
  -
  -

user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value

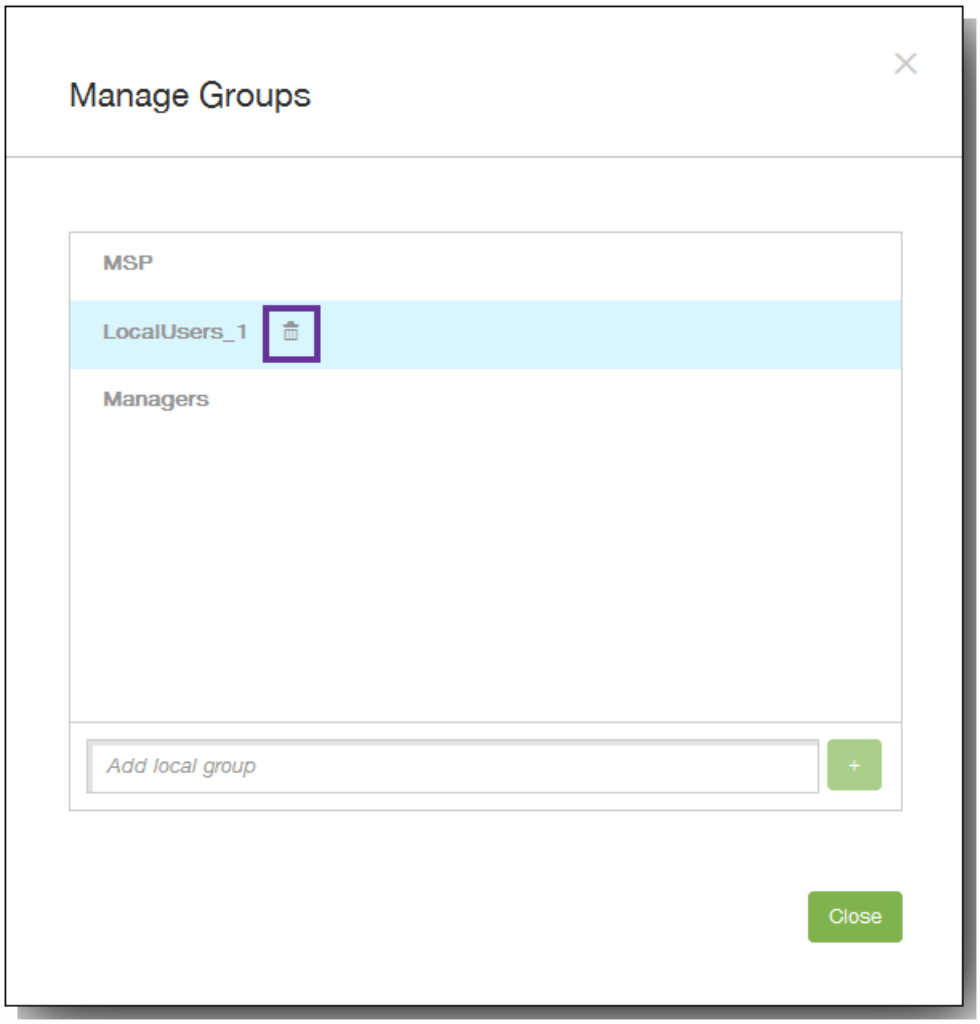
-
-
  -
  -
-
  -
  -

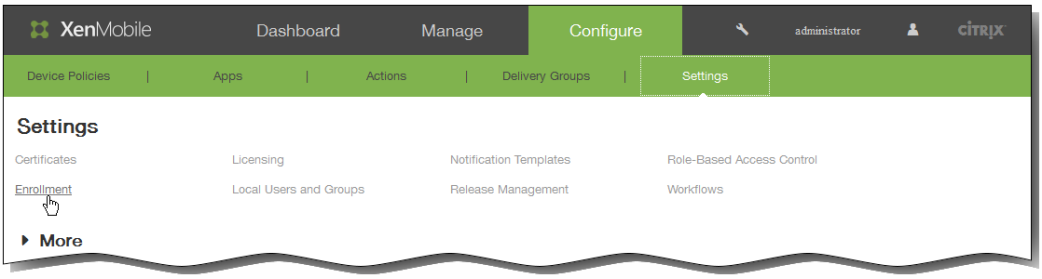
- 

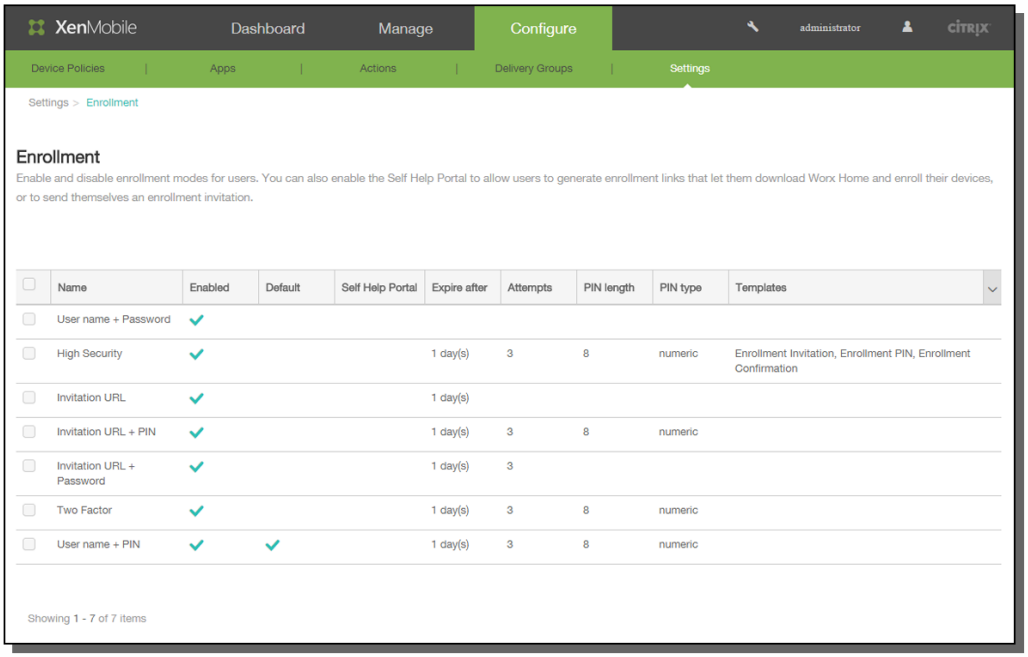
- 

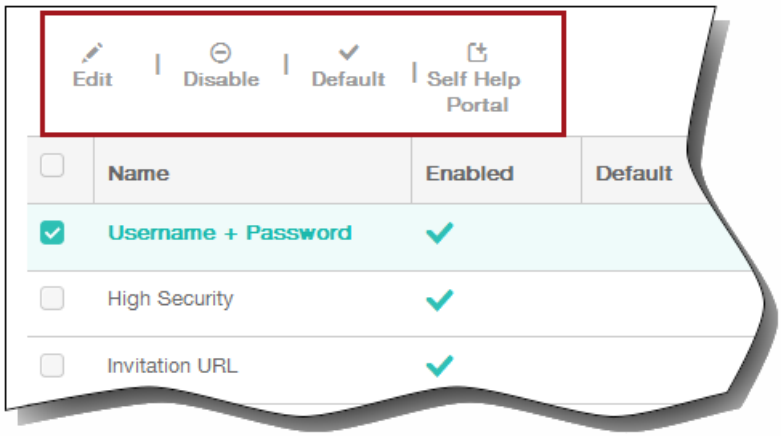


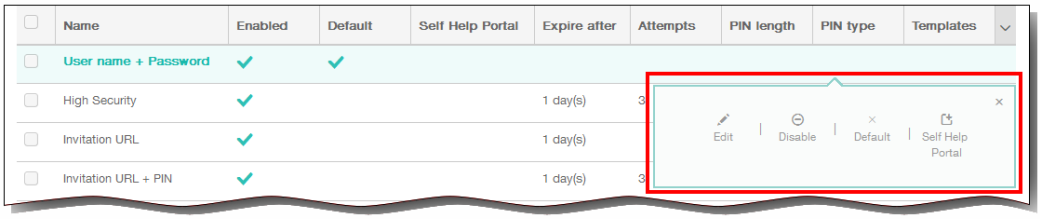
-
-

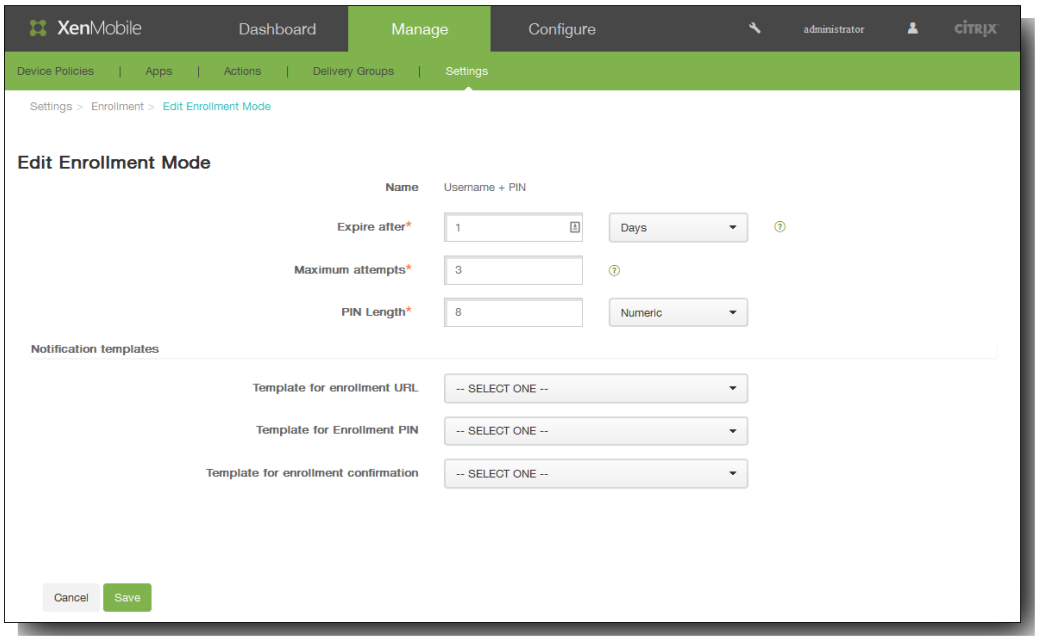


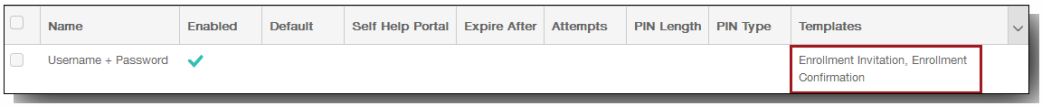




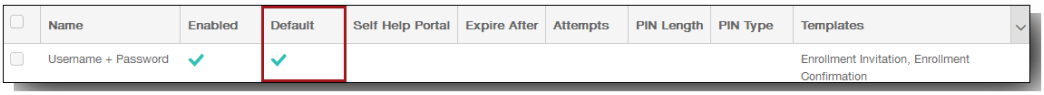




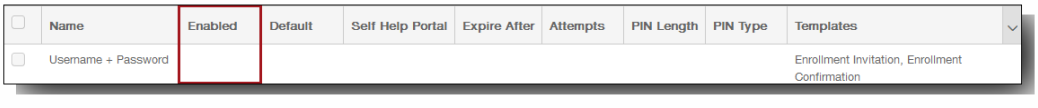




Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
Username + Password	✓							Enrollment Invitation, Enrollment Confirmation



Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
Username + Password	✓	✓						Enrollment Invitation, Enrollment Confirmation



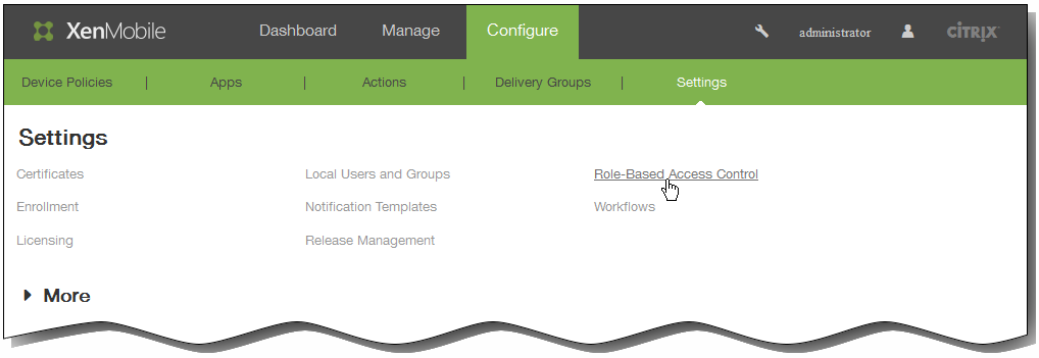
Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
Username + Password								Enrollment Invitation, Enrollment Confirmation

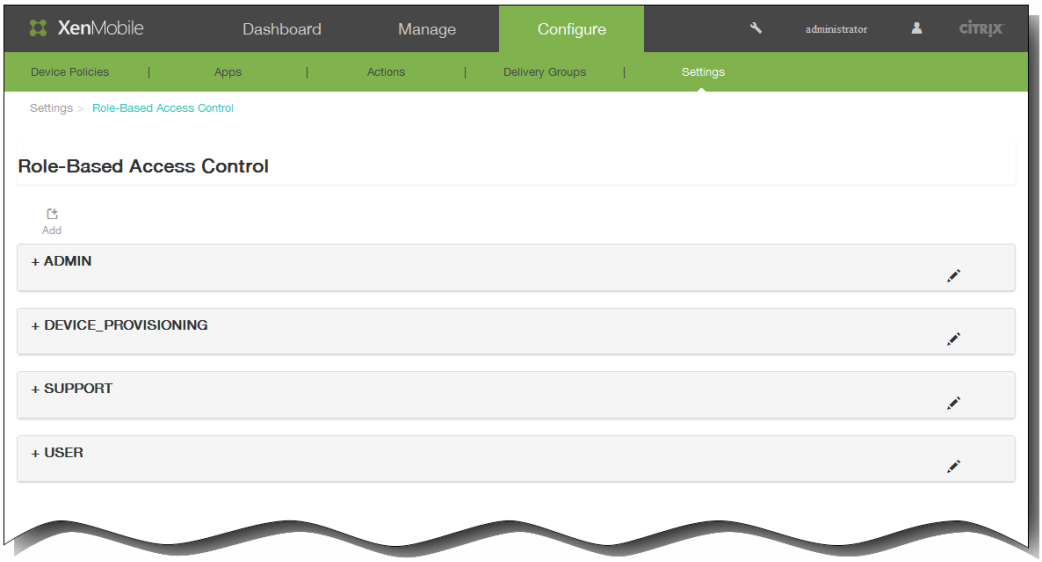
-
-

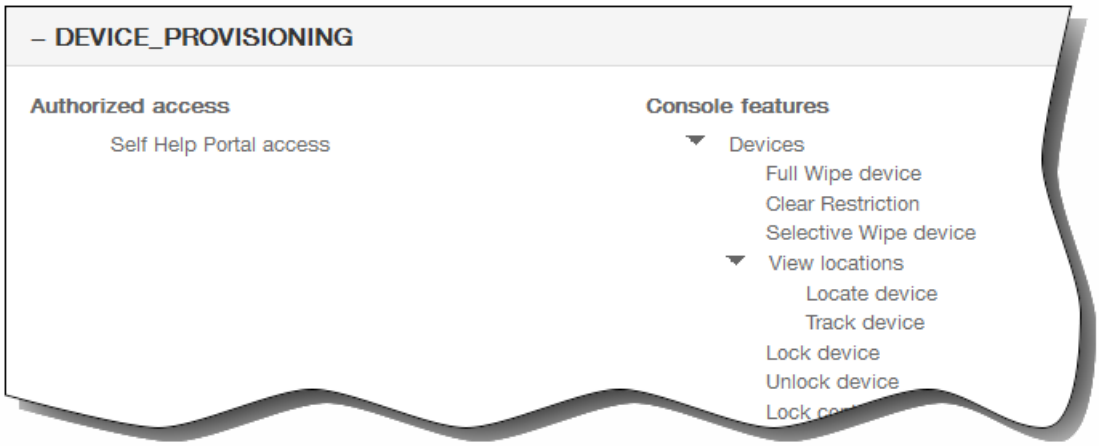
	Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
	Username + Password	✓	✓	✓					Enrollment Invitation, Enrollment Confirmation

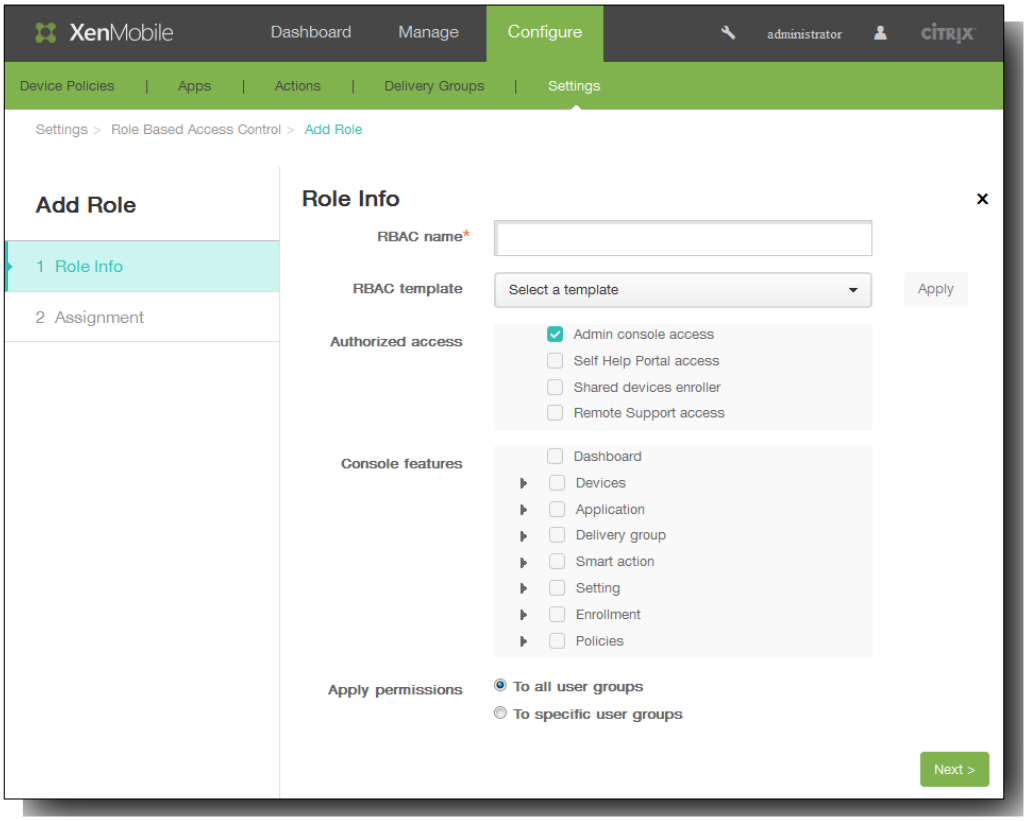
-
-
-
-

-
-
-

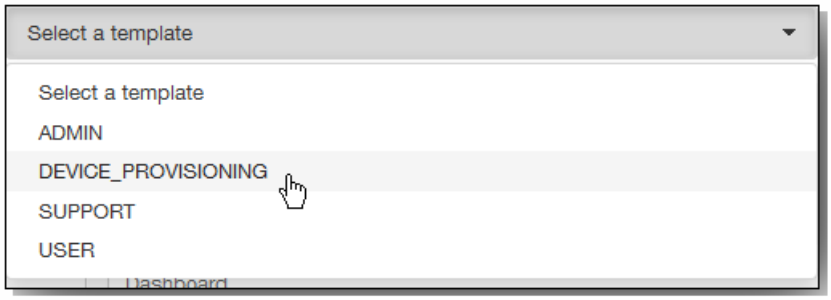




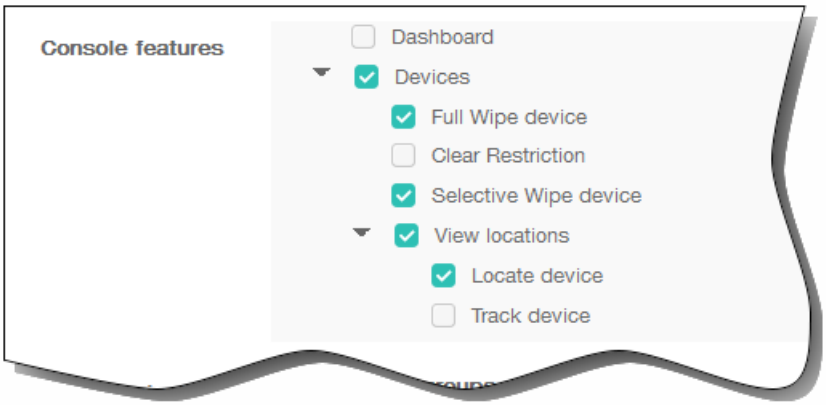


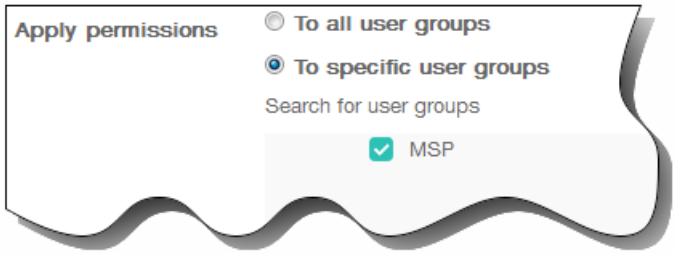


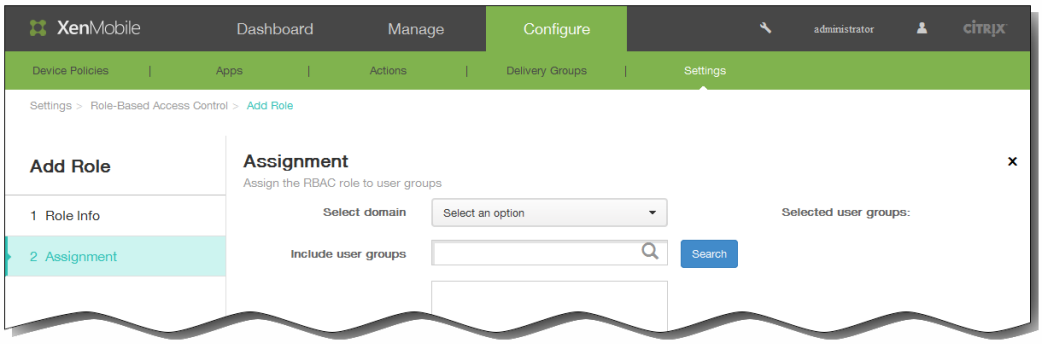
-

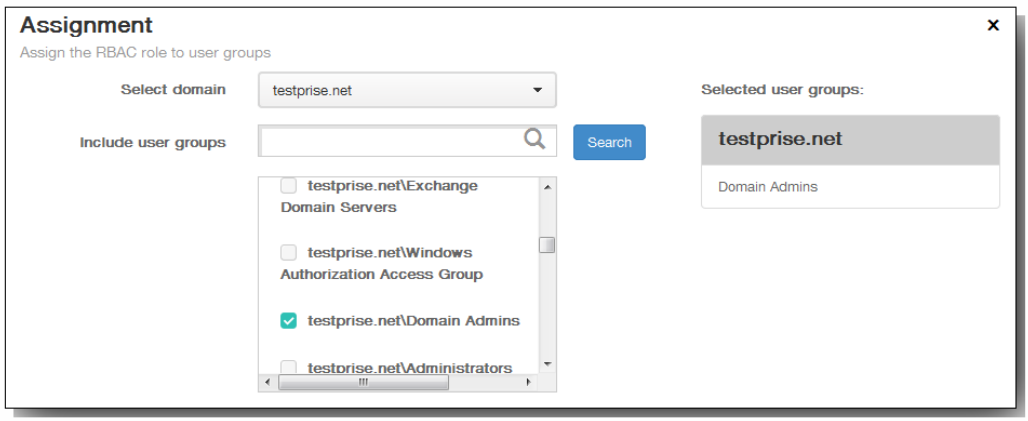


-
-





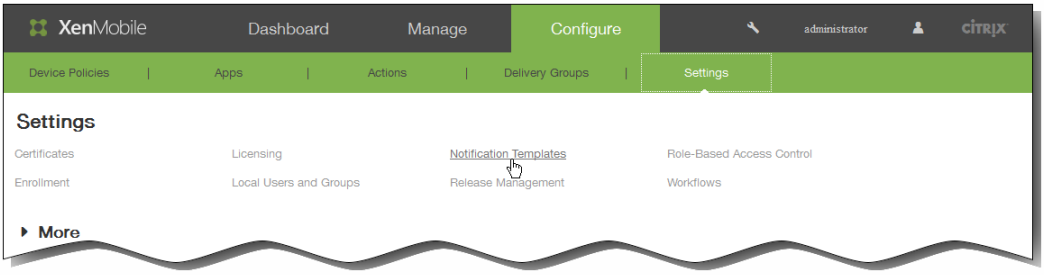




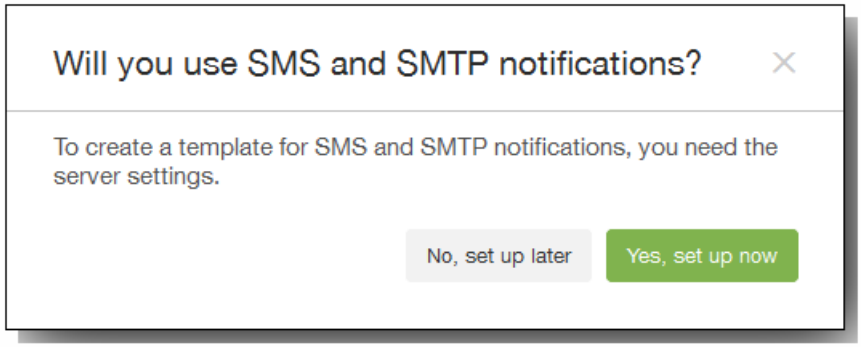
-
-

-
-
-
-
-
-
-

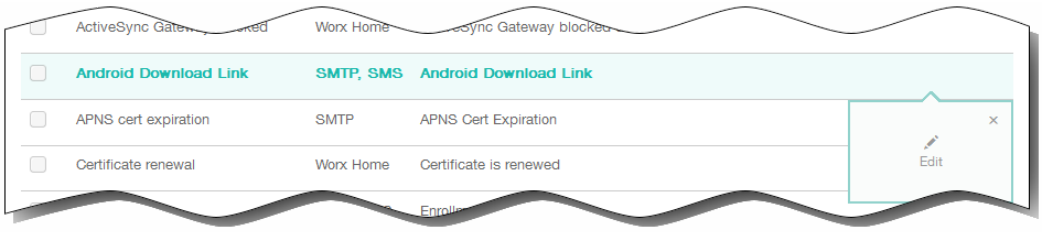
-
-

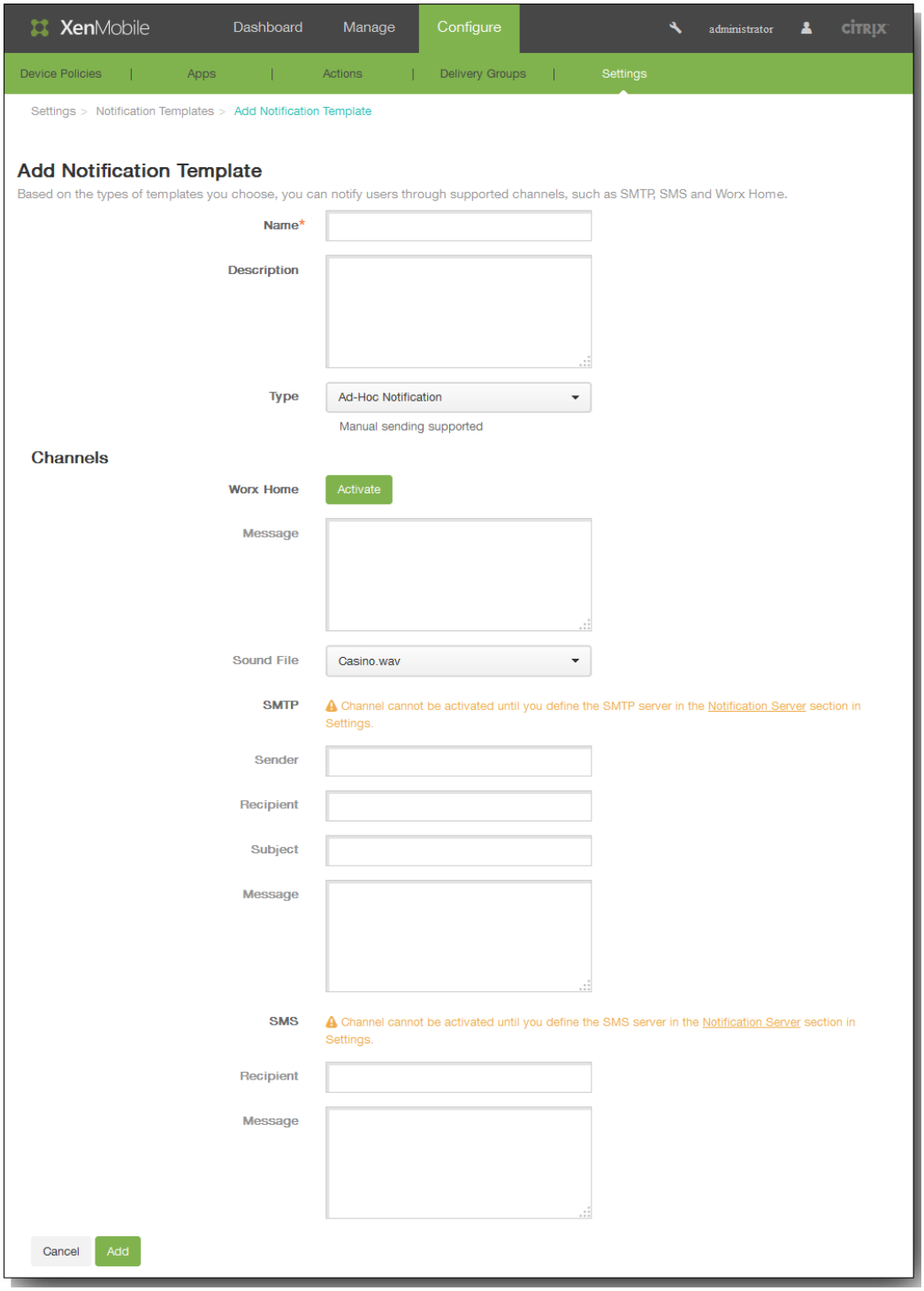


-



-
  -
  -
  -

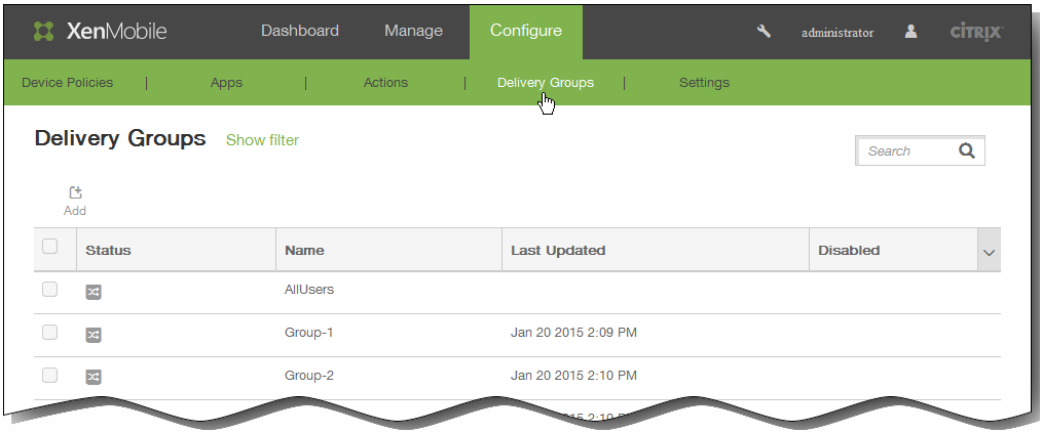


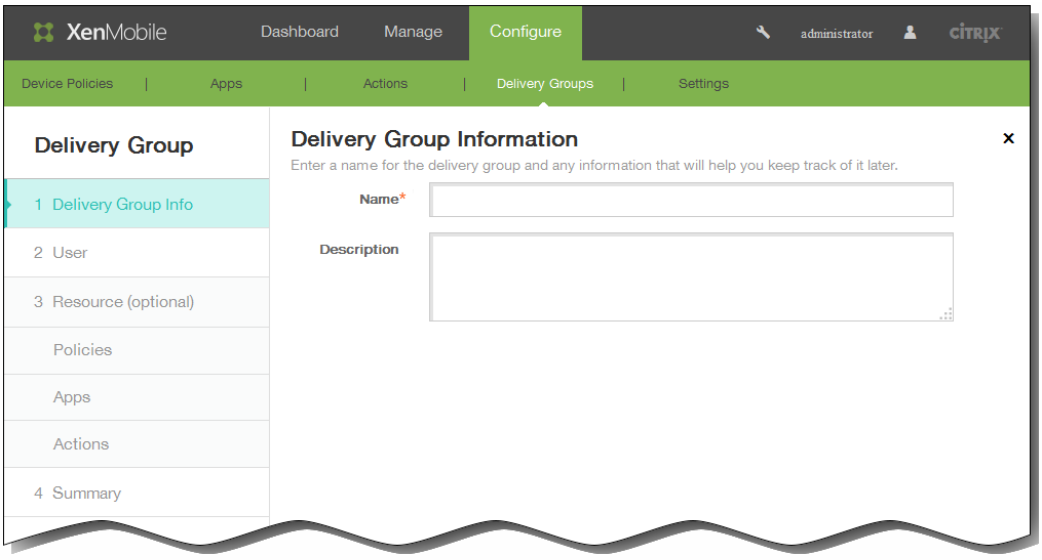


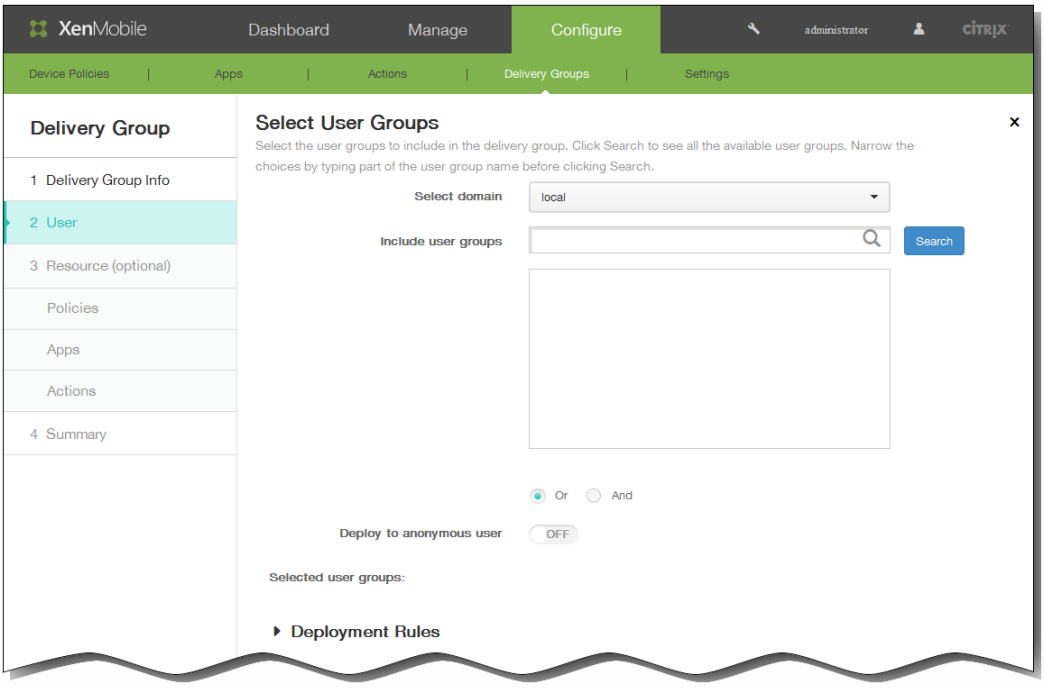
-
-

-
-
-

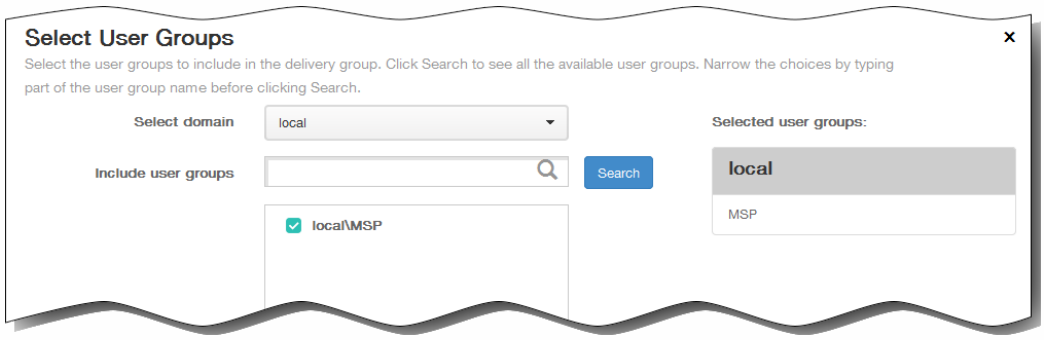
-
-
-
-
-



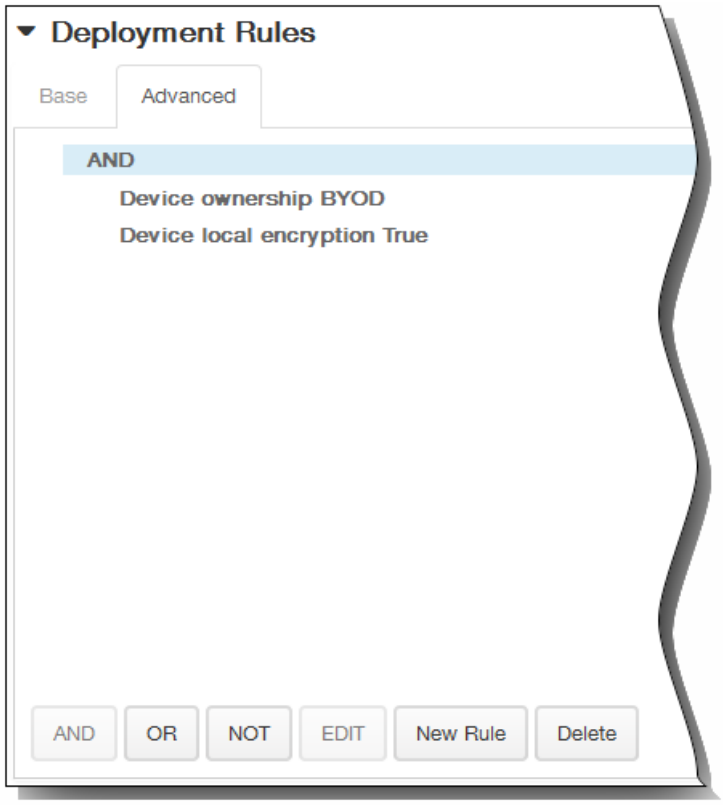


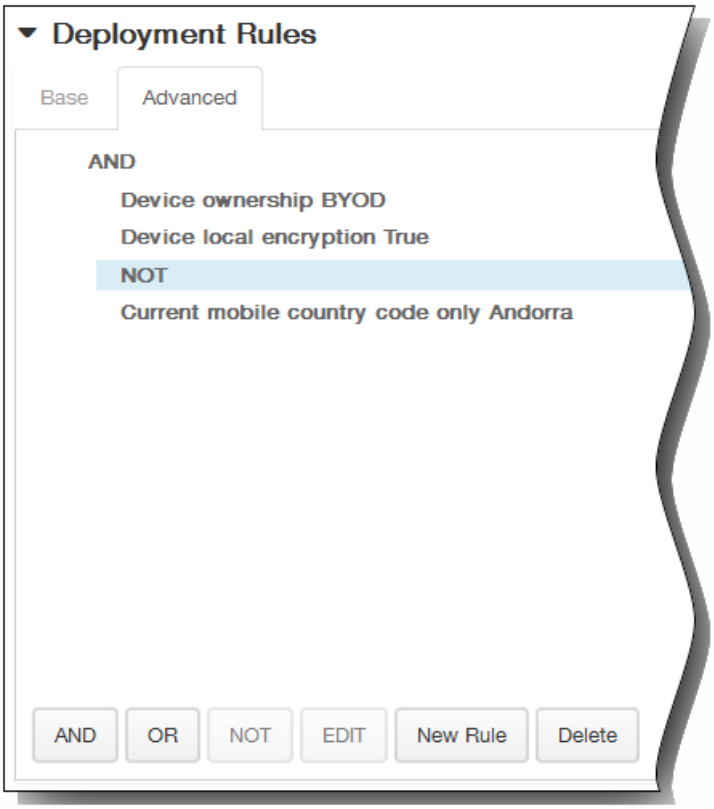


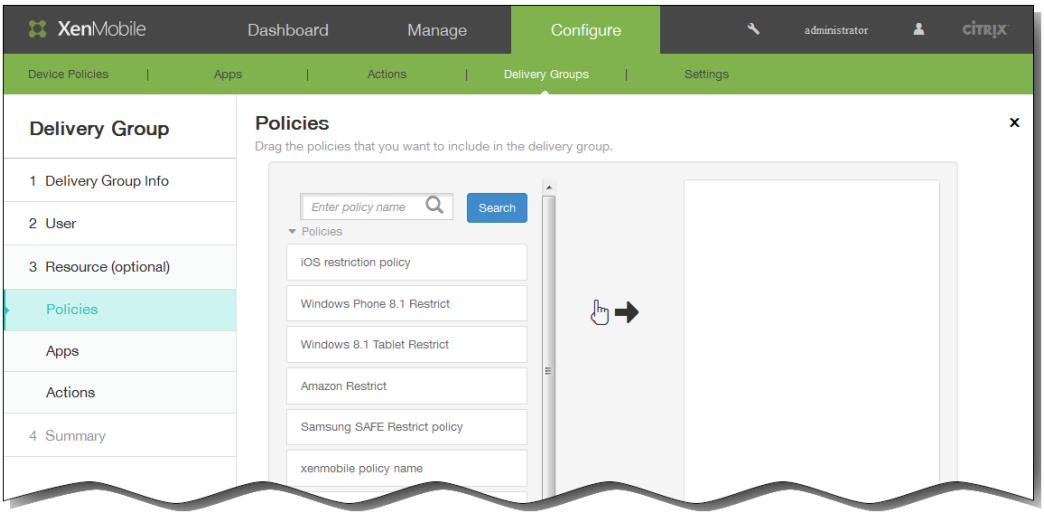
-
-

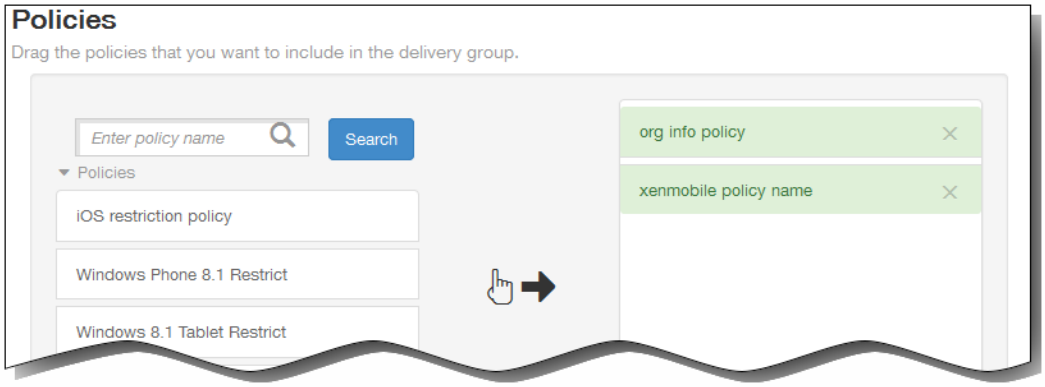


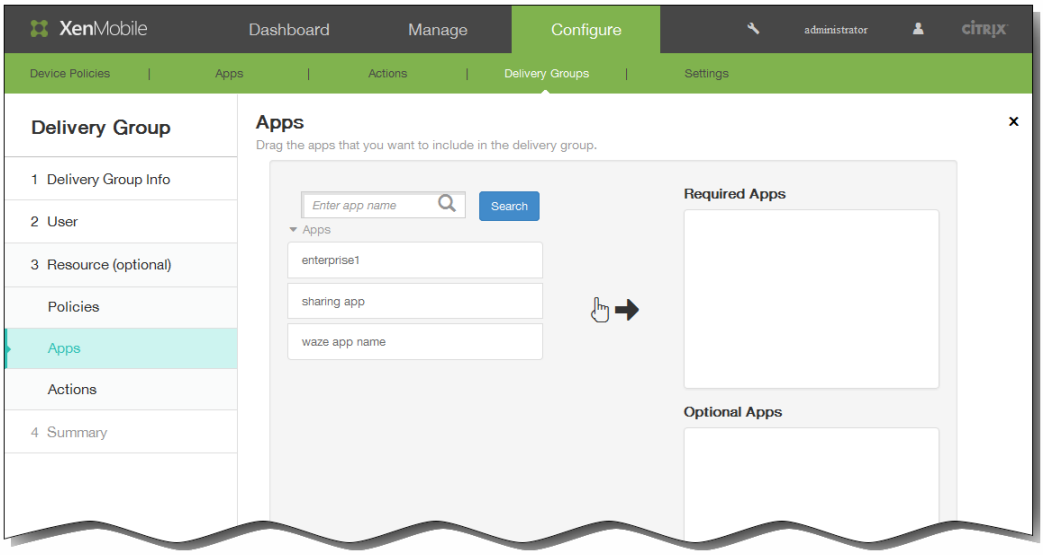
-
-

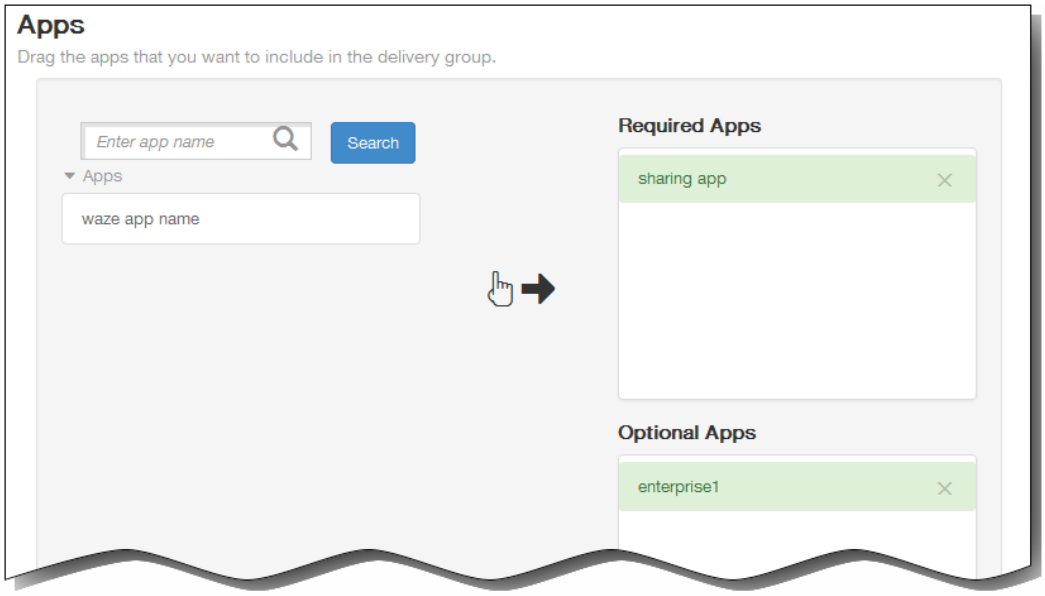


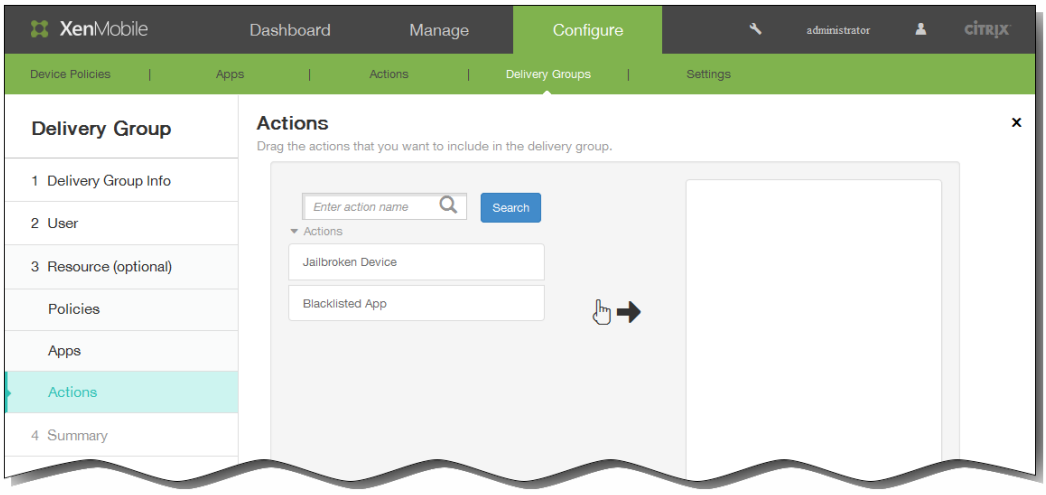


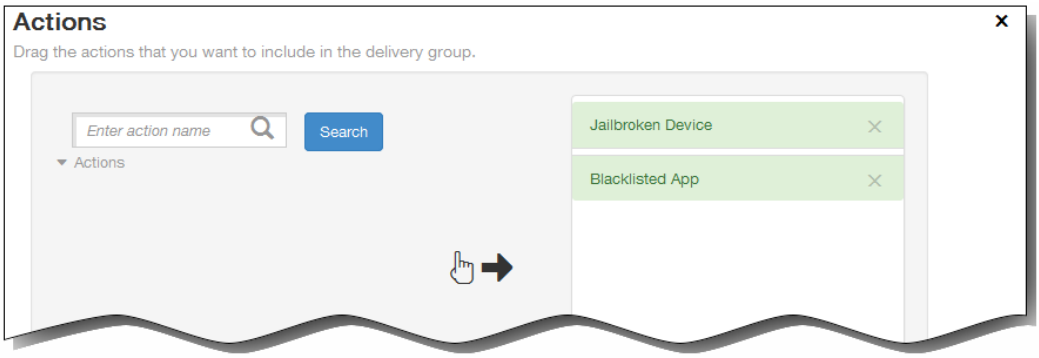


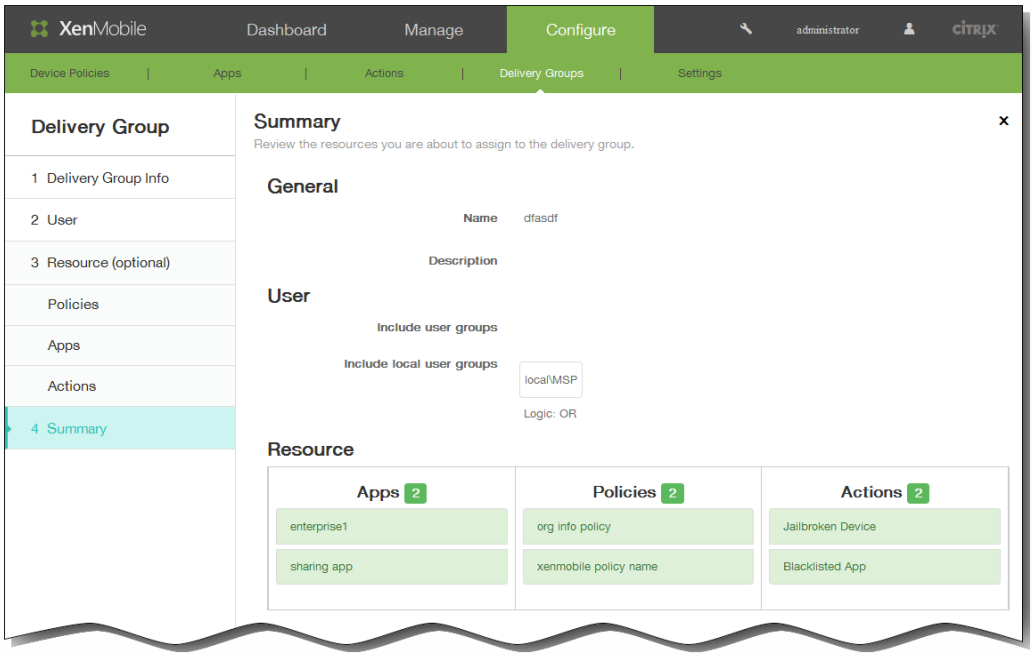


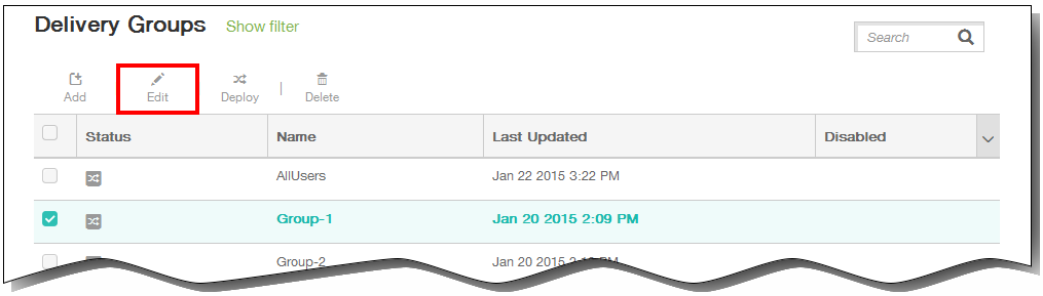


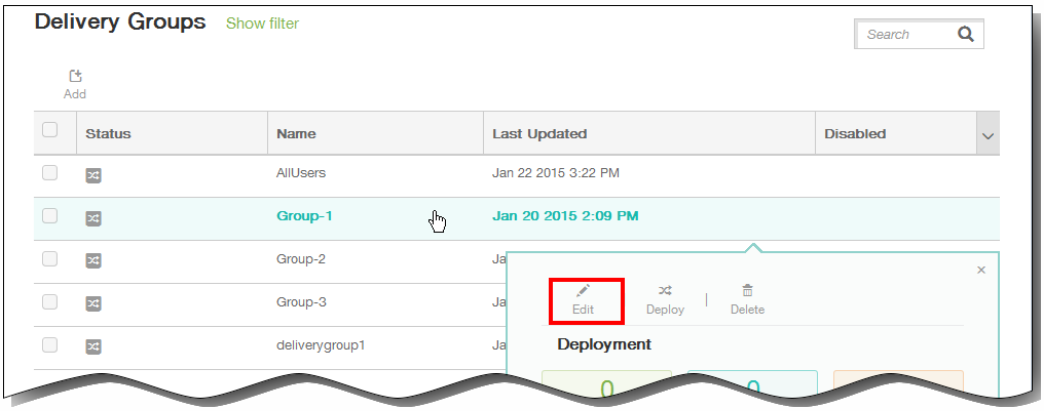


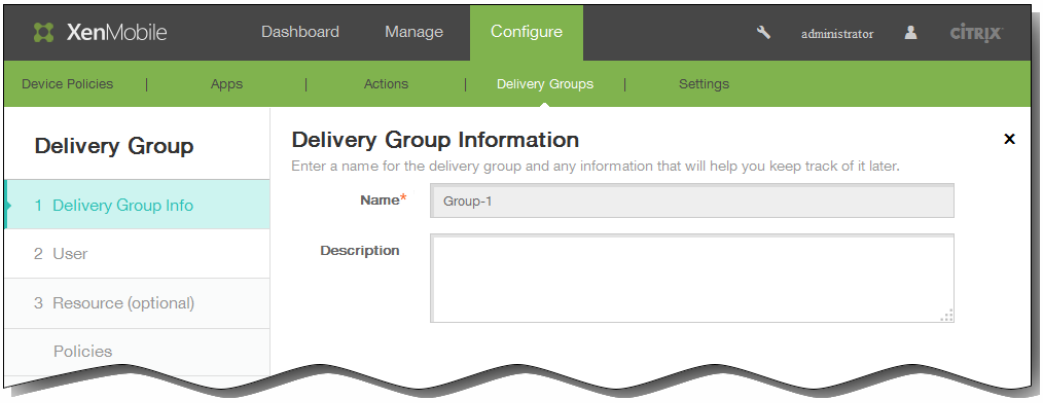


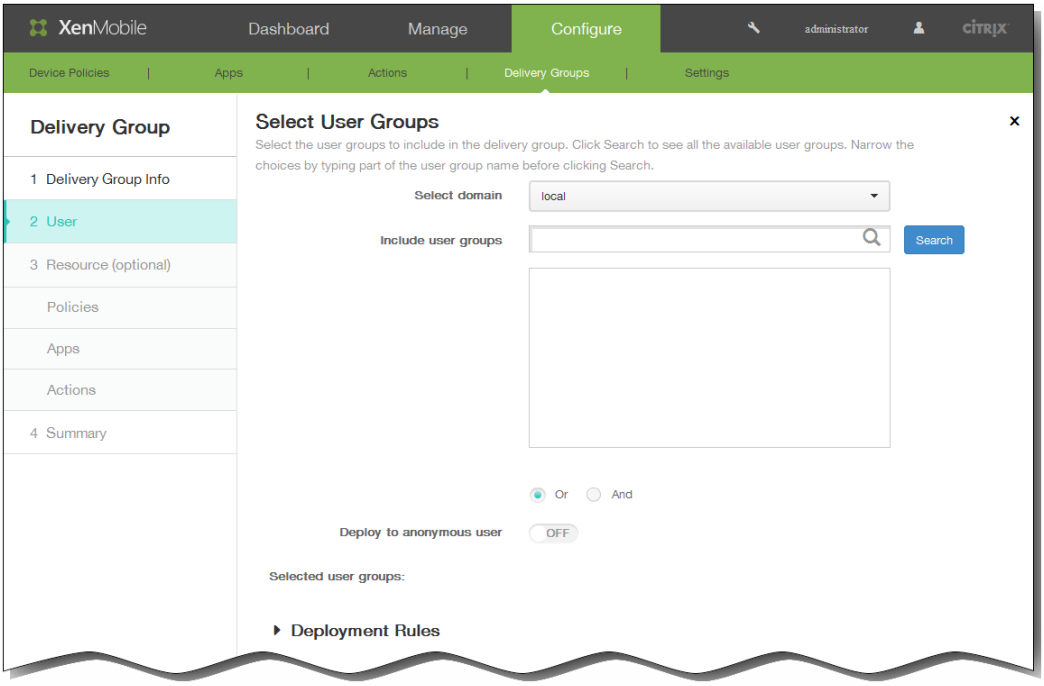




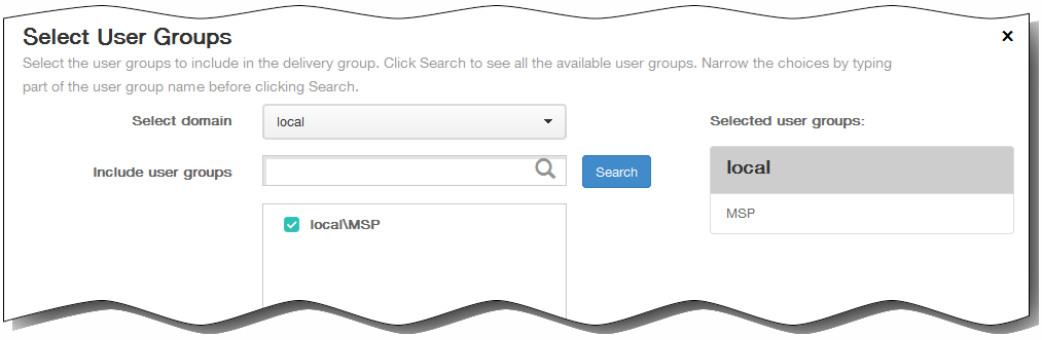


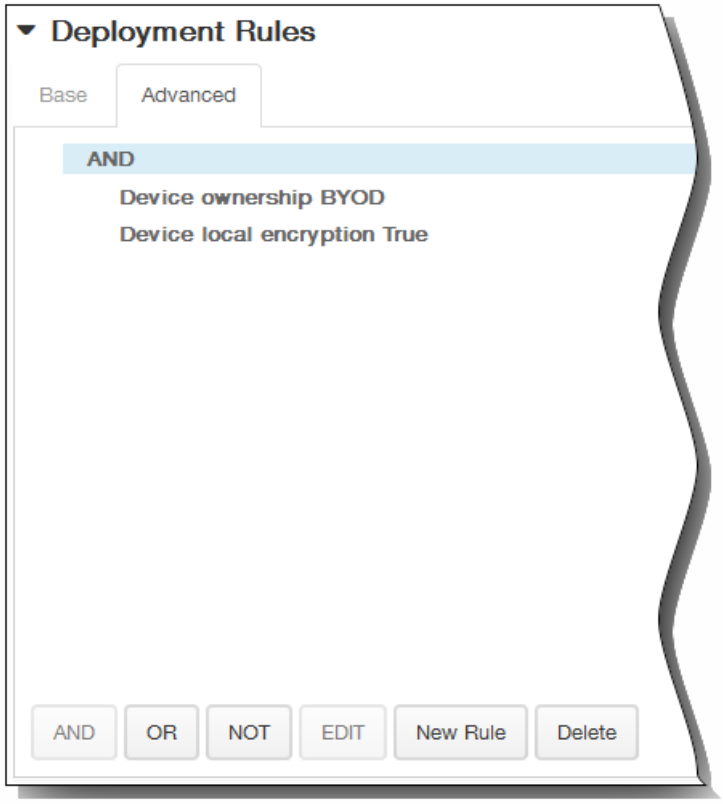


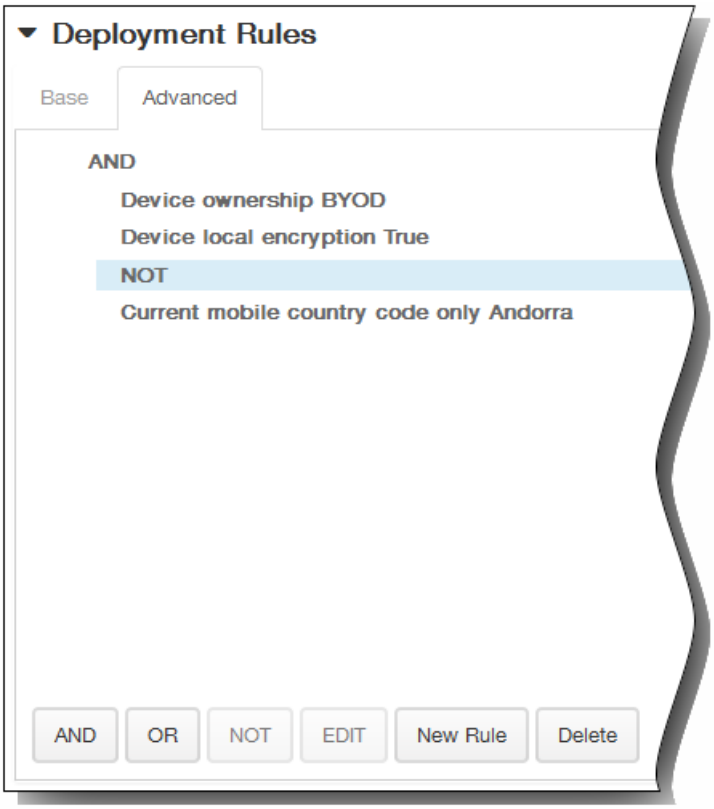


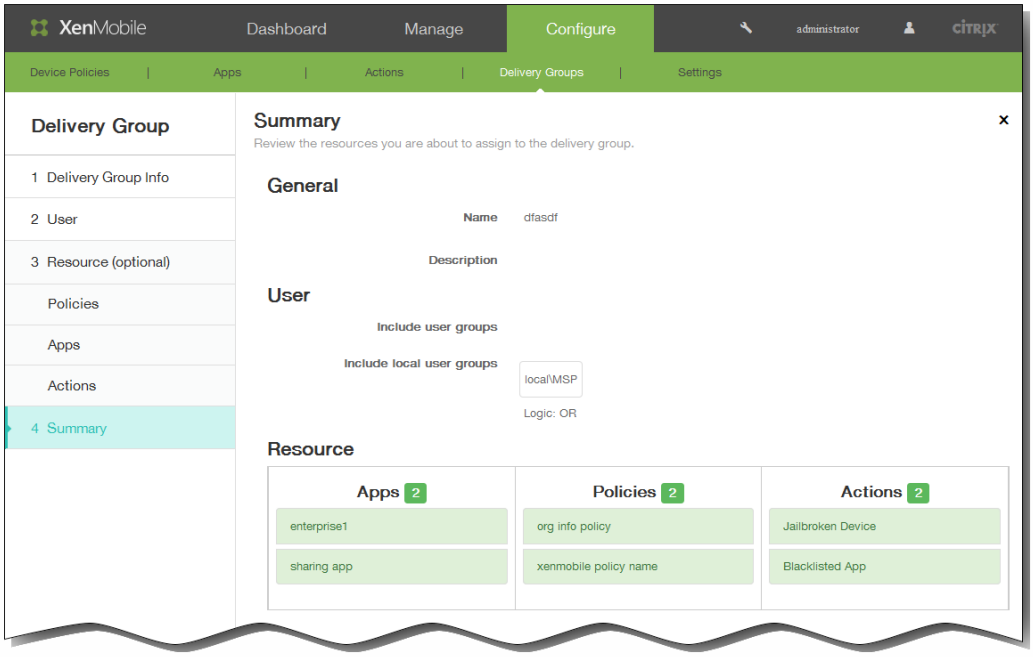


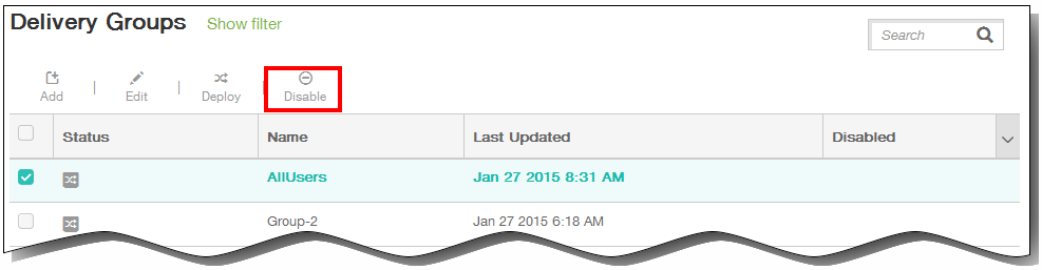
-
-

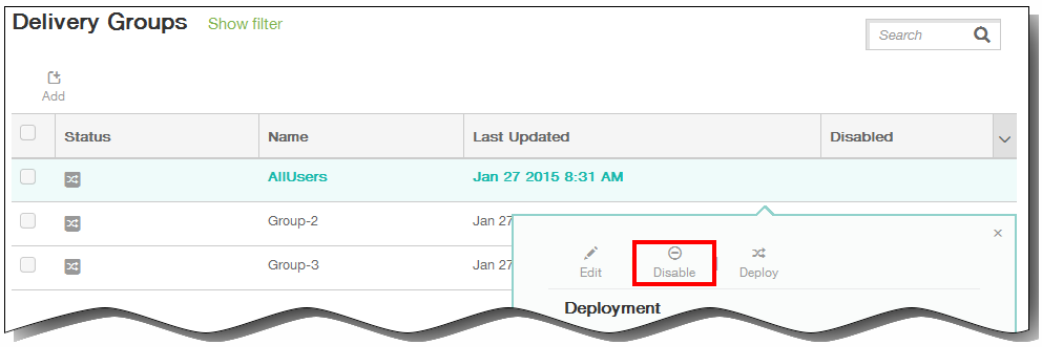




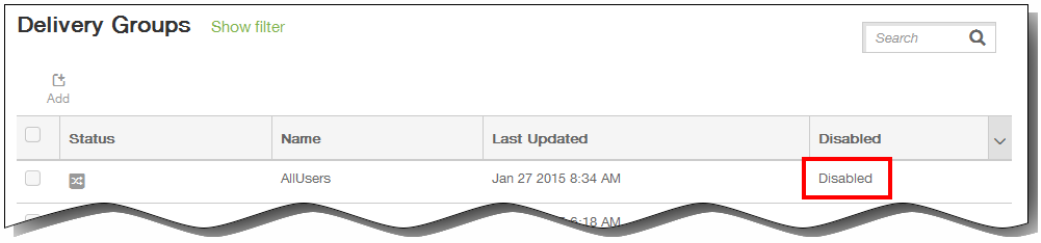






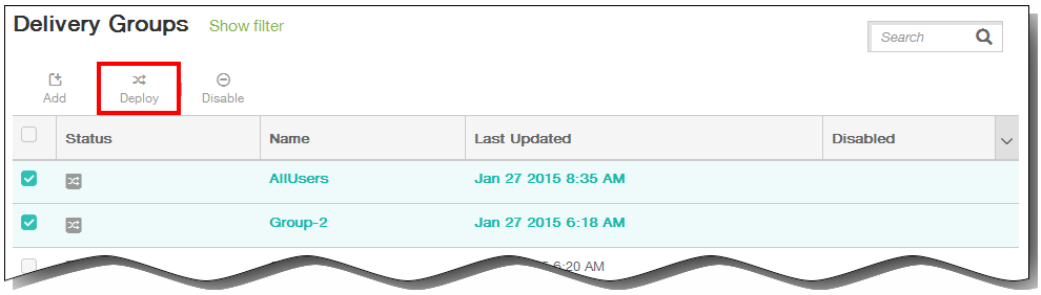


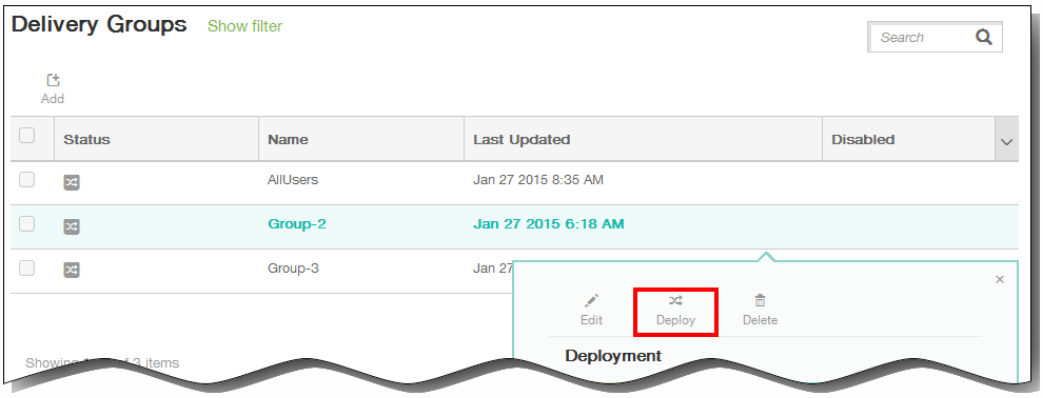
-



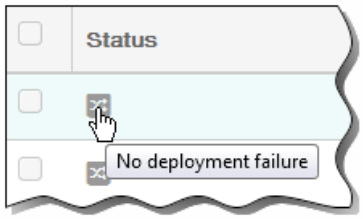
-

-
-

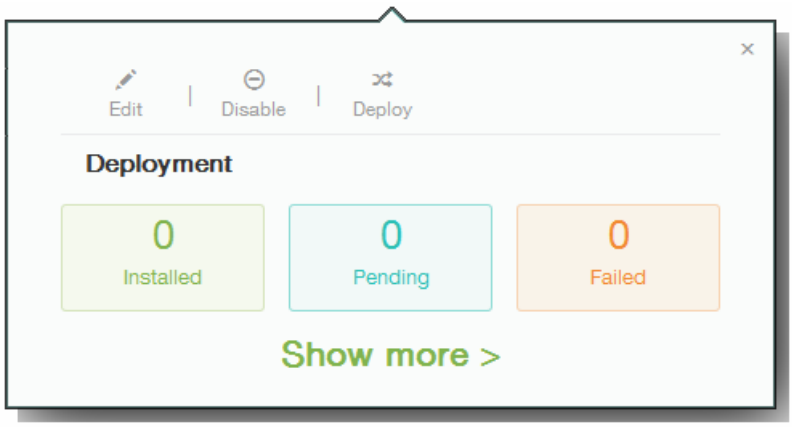




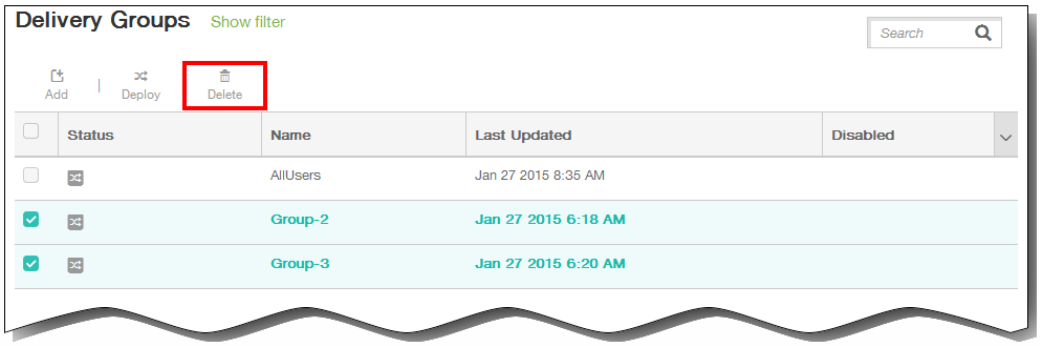
-

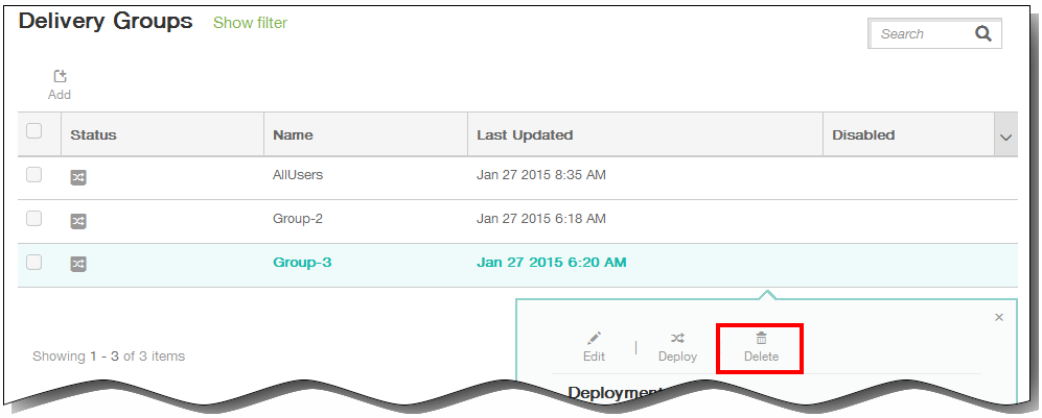


-

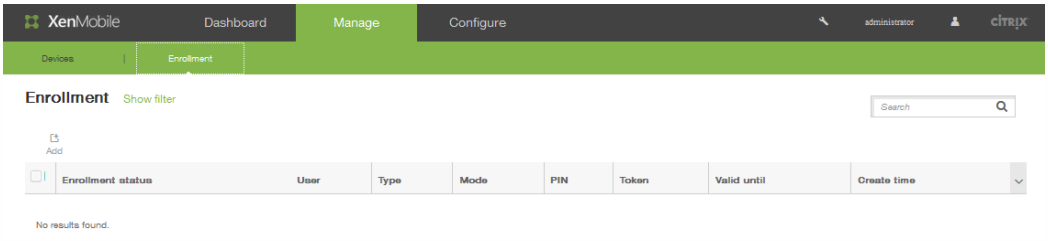


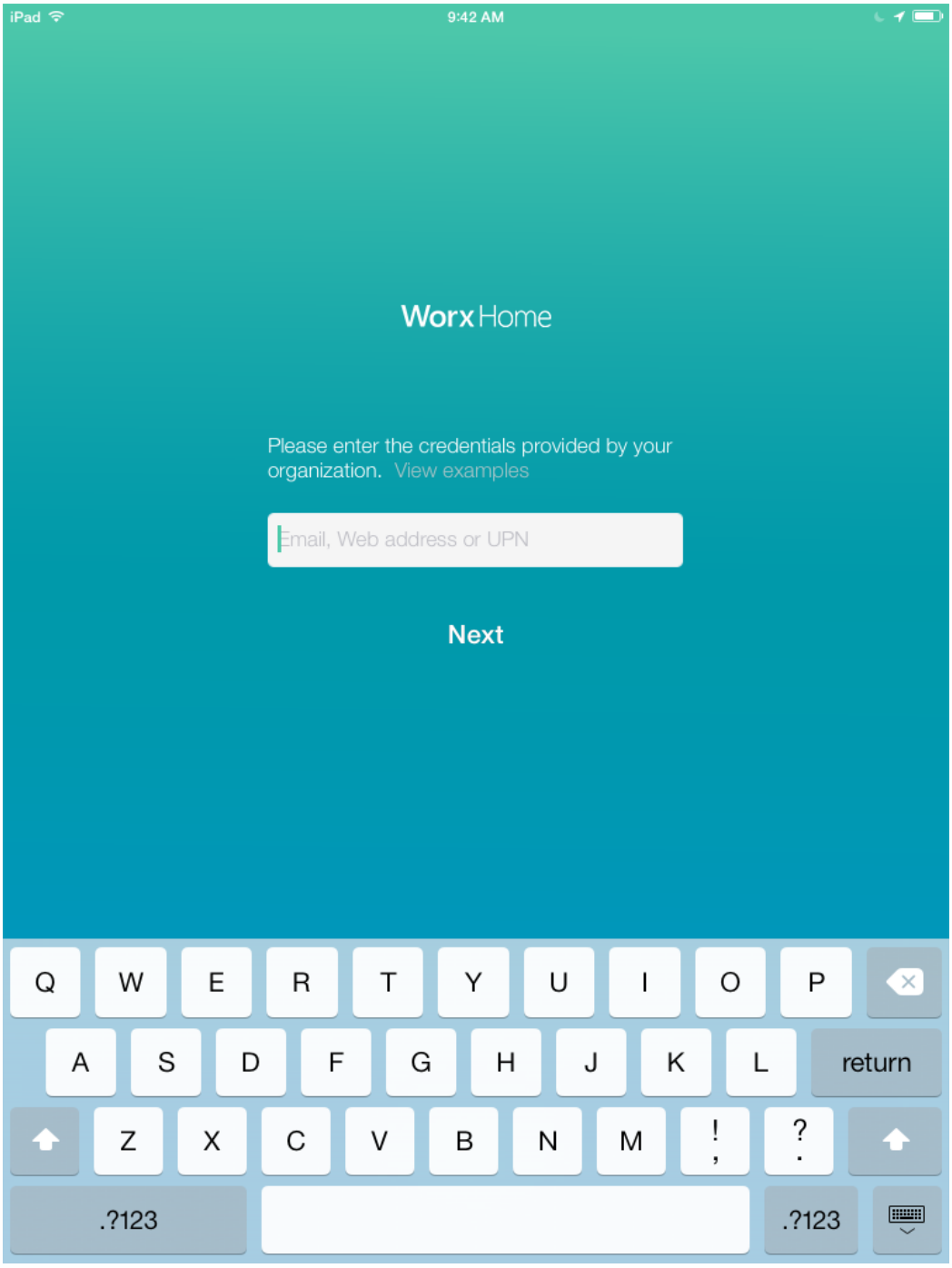
-
-

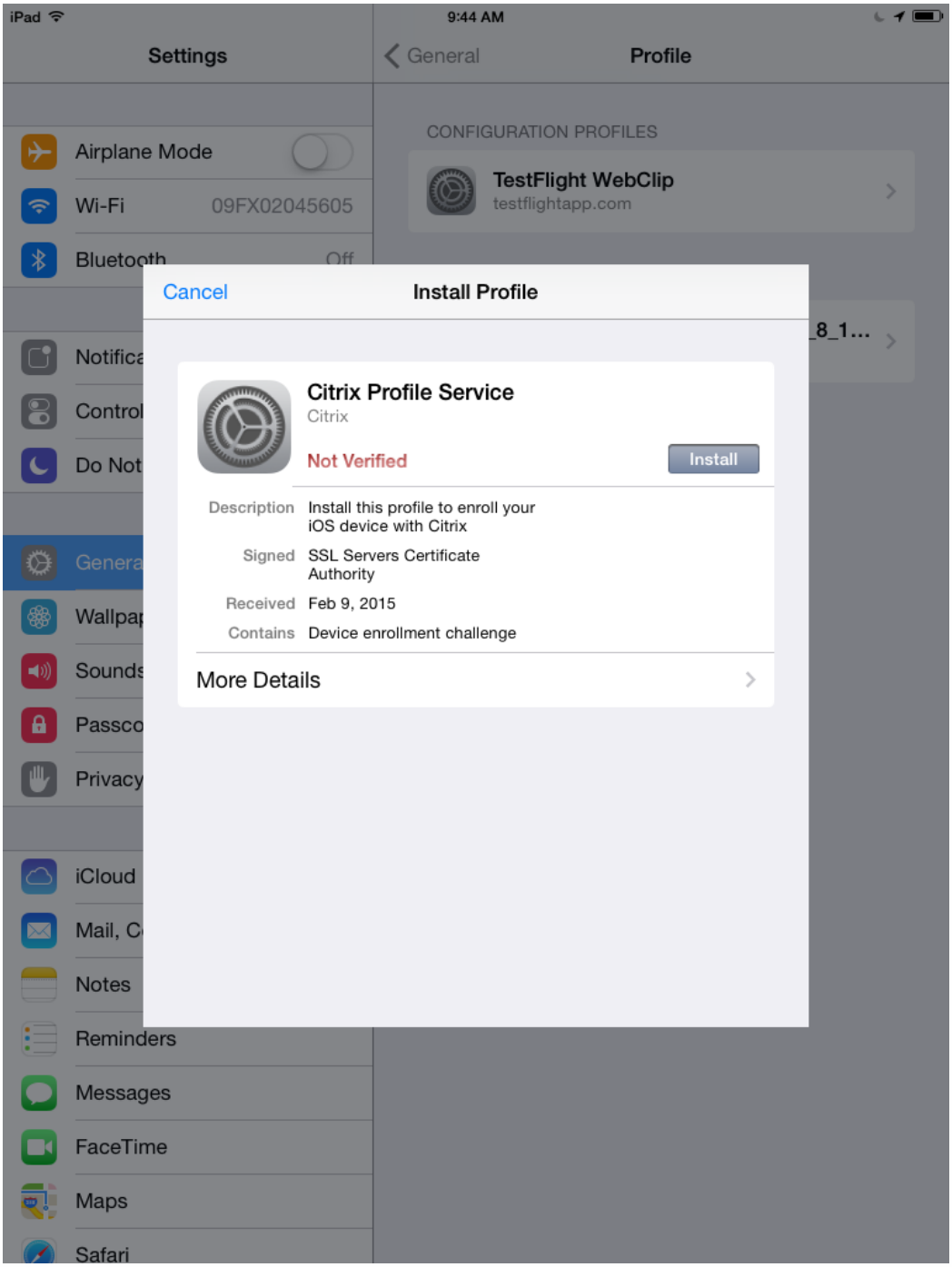


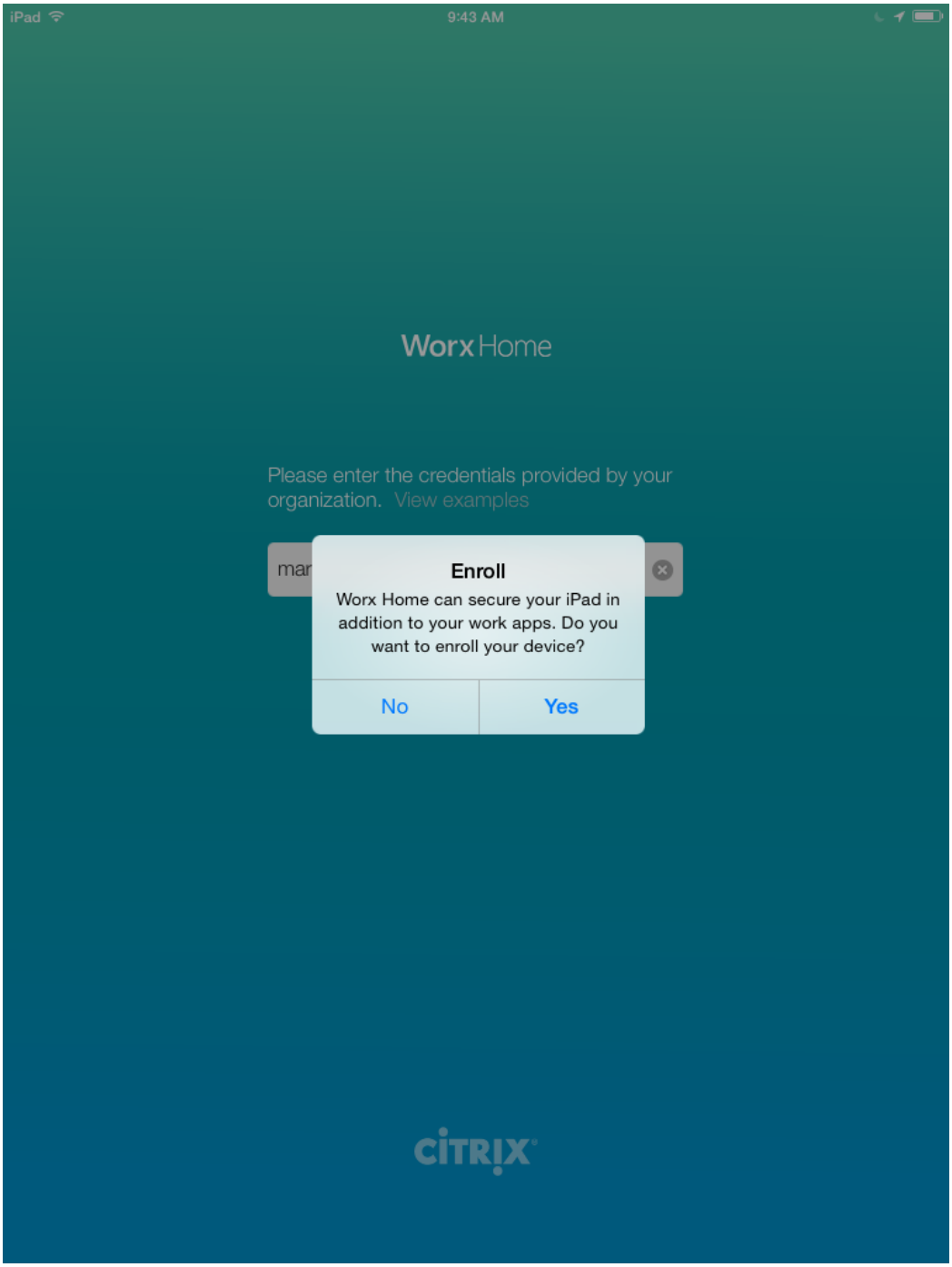


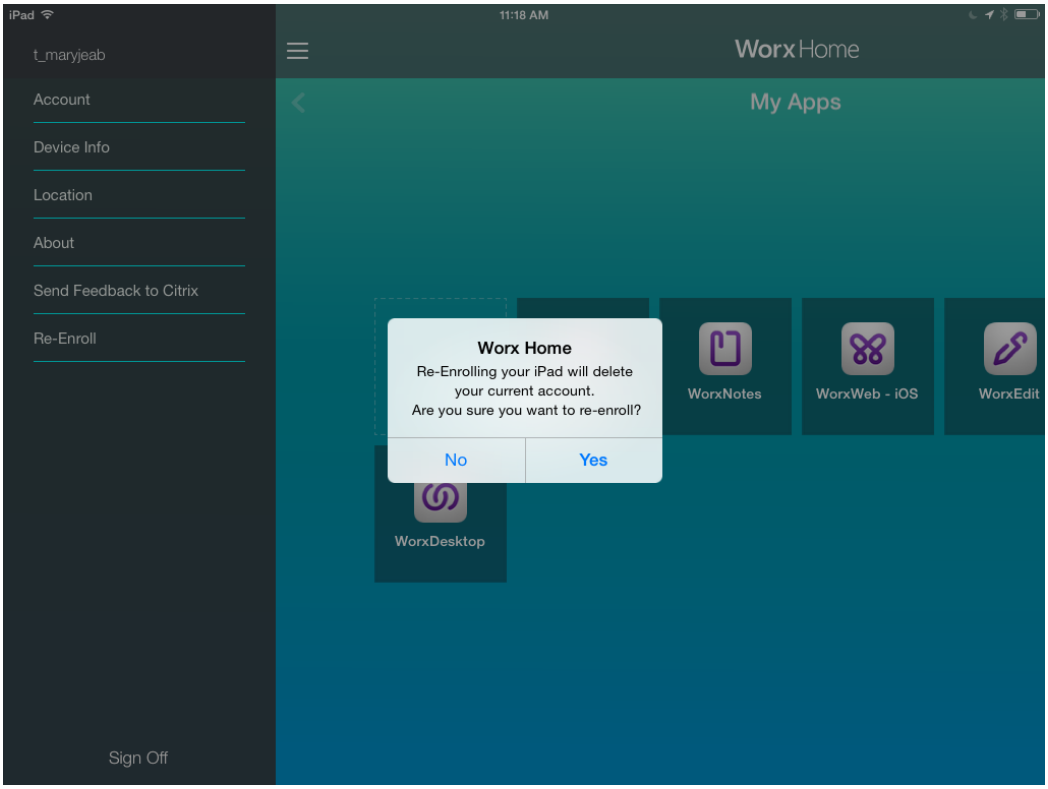
-
-
-
-



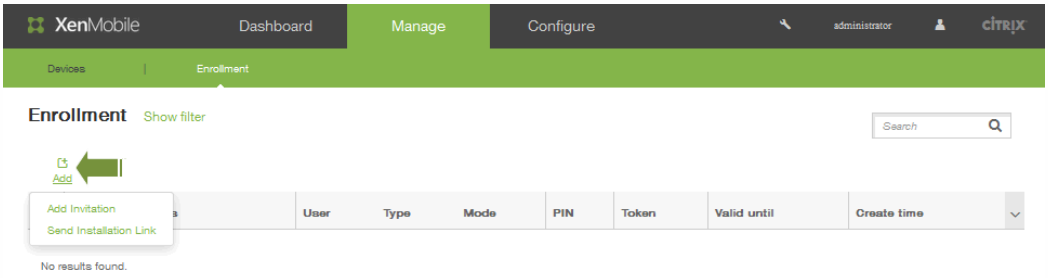


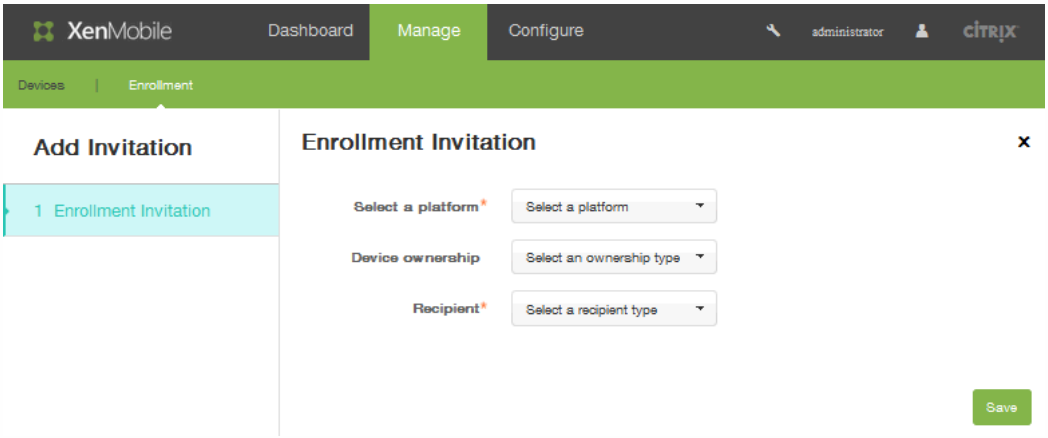


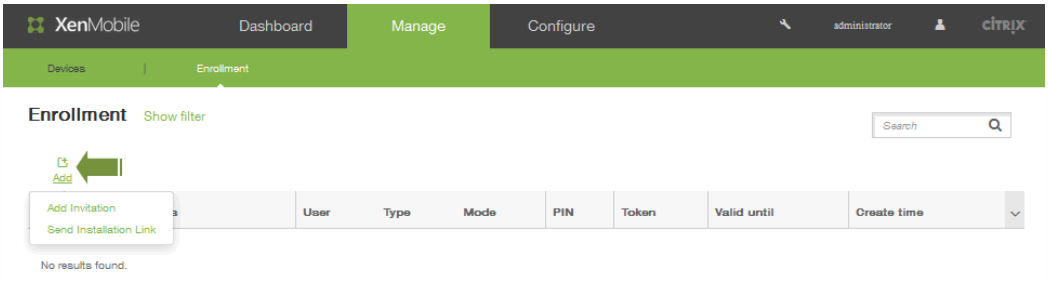


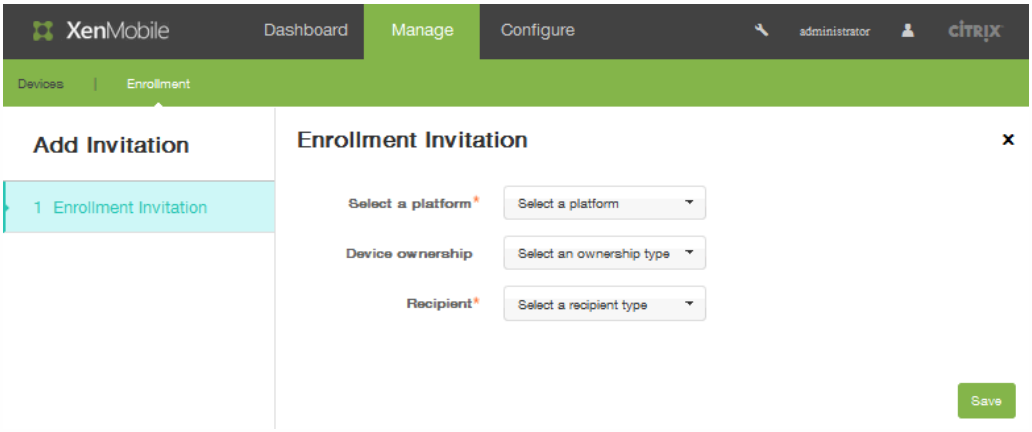


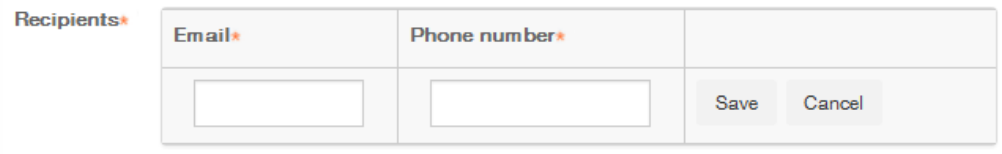
-
-

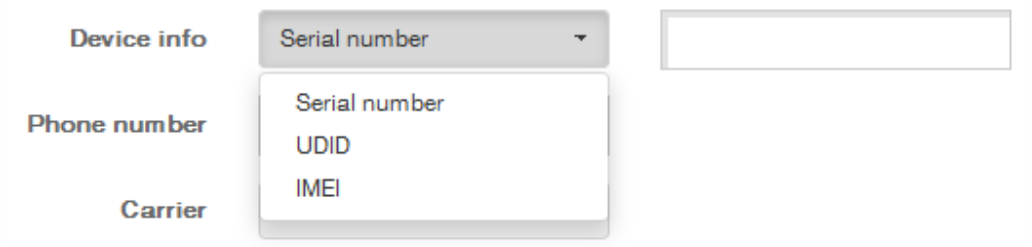


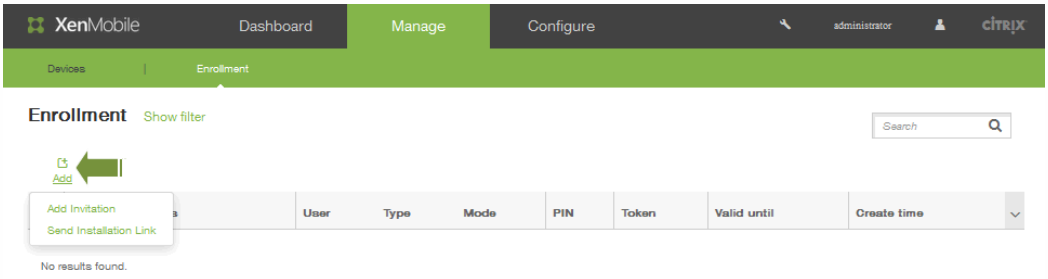


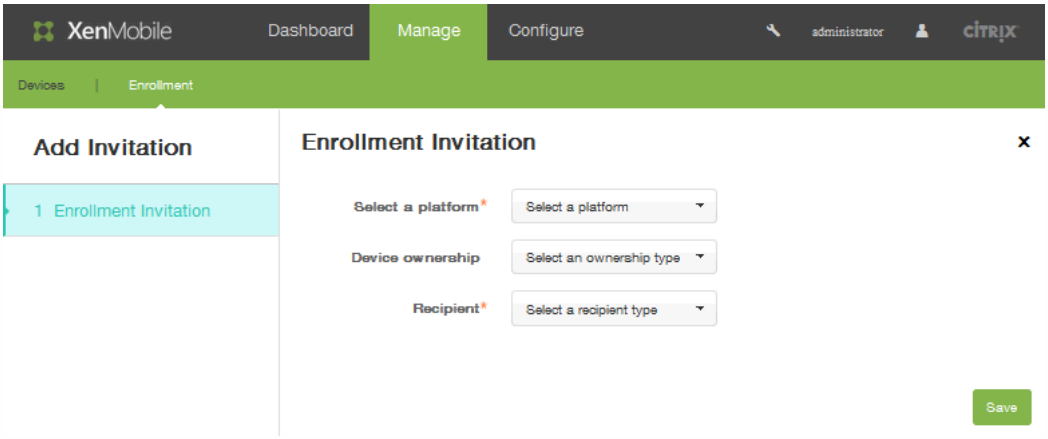


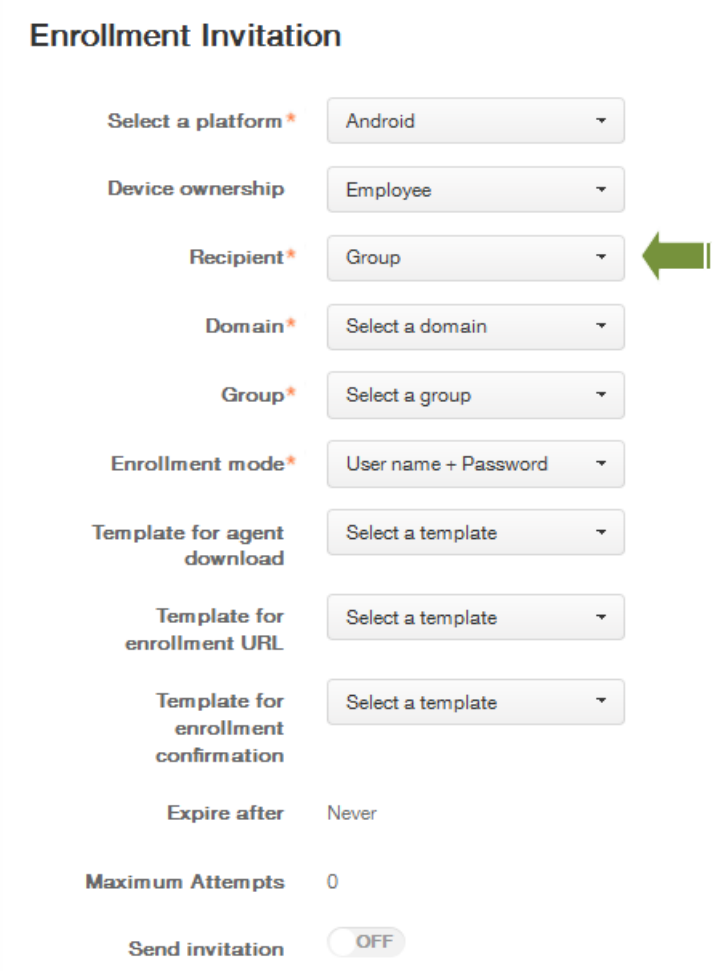


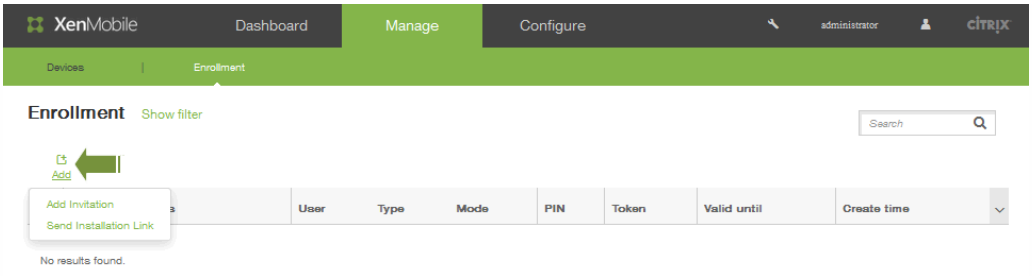


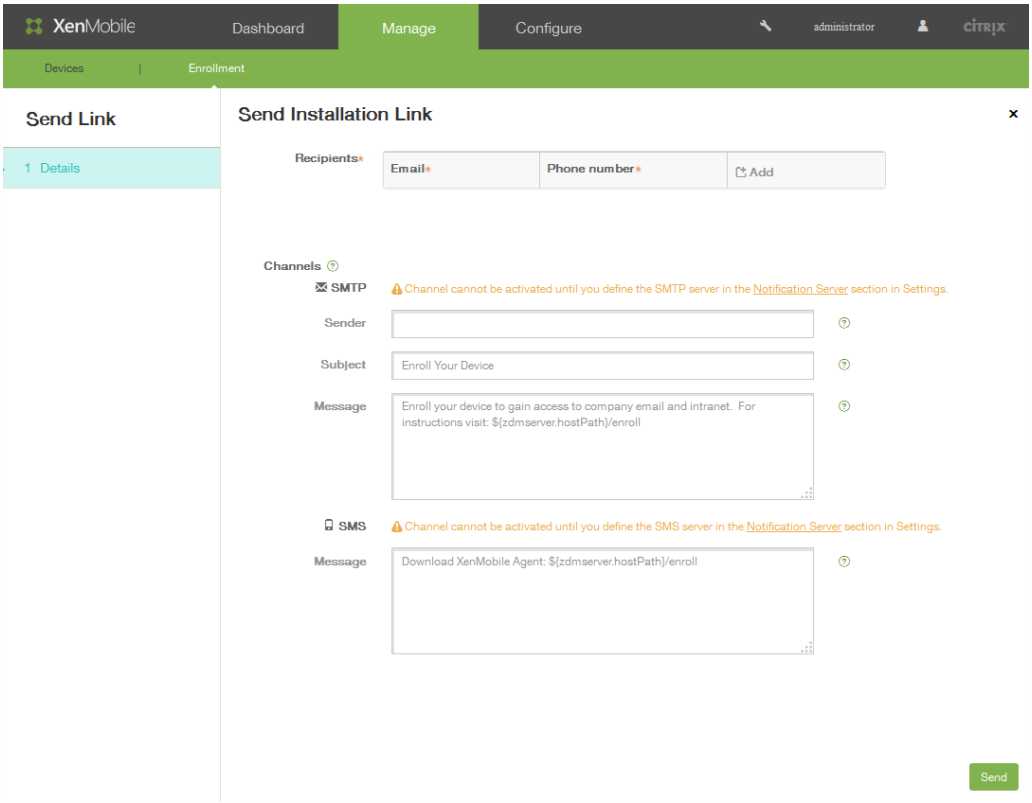










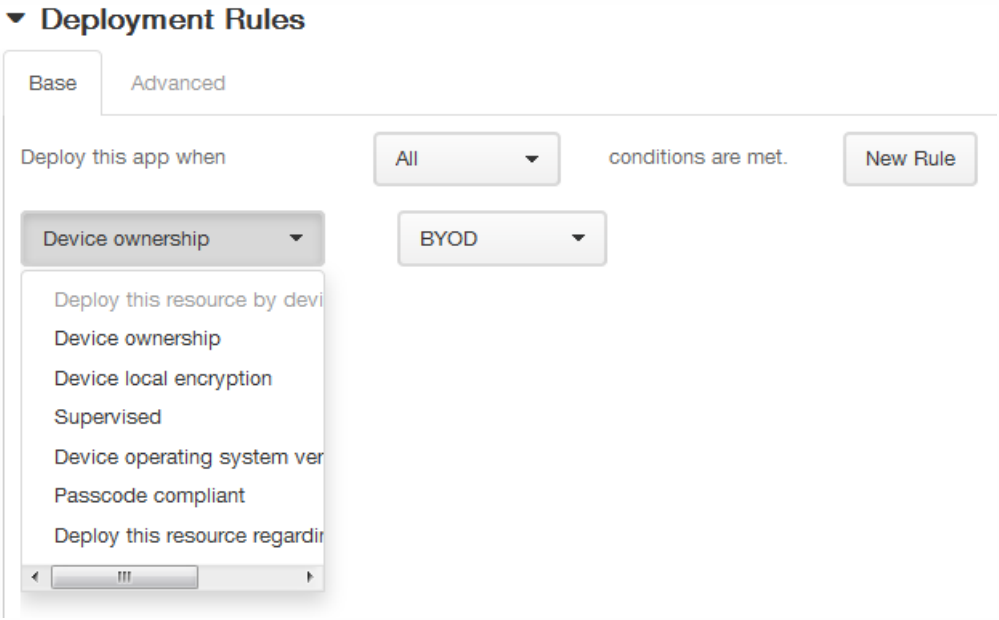


配置部署规则

May 05, 2016

您可以设置将影响软件包部署结果的任意数量的参数。

例如，软件包部署可以基于特定的操作系统版本、特定的硬件平台或一些其他组合。在此向导中，既有基础规则编辑器，也包含高级规则编辑器。“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。

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，将显示高级规则编辑器。

在此模式中，您可以指定规则之间所设置的关系。可以使用运算符 AND、OR 和 NOT。

关于 XenMobile 中的设备所有权

设备所有权包括公司拥有的设备，同时也包括用户拥有的设备，又称为自带设备 (BYOD)。您可以在 XenMobile 控制台中的两个位置控制 BYOD 设备连接到您网络的方式：在“部署规则”页面上以及通过设置选项卡上的 XenMobile 服务器属性。

通过设置服务器属性，您可以要求所有 BYOD 用户在接受公司对其设备的管理后才能访问应用程序，或者也可以在不管理用户设备的情况下直接允许其访问公司应用程序。

- 将服务器设置 wsapi.mdm.required.flag 设置为真 时，将托管所有 BYOD 设备并且任何拒绝注册的用户都将无法访问应用程序。在企业 IT 团队需要高安全性和积极用户体验（来源于在 XenMobile 中注册用户设备）的环境中，应考虑将 wsapi.mdm.required.flag 设置为真。
- 如果将 wsapi.mdm.required.flag 设置为假（默认设置），用户可以拒绝注册，但仍可以通过 Worx Store 访问其设备上的应用程序。在隐私、法律或规制不需要设备管理而仅需要企业应用程序管理的环境中，应考虑将 wsapi.mdm.required.flag 设置为假。

有关设置服务器属性的详细信息，请参阅服务器属性。

使用未托管的设备的用户可以通过 Worx Store 安装应用程序。您可以通过应用程序策略控制对应用程序的访问，而不是通过设备级控制，如选择性擦除或完全擦除。根据您设置的值，策略需要设备对 Xenmobile 服务器进行例行检查以确认仍允许运行应用程序。

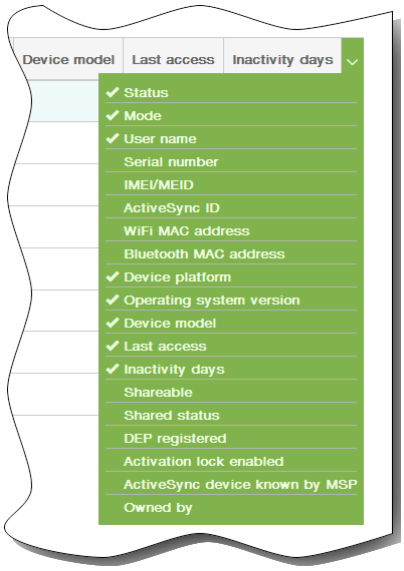
添加设备并查看设备详细信息

May 05, 2016

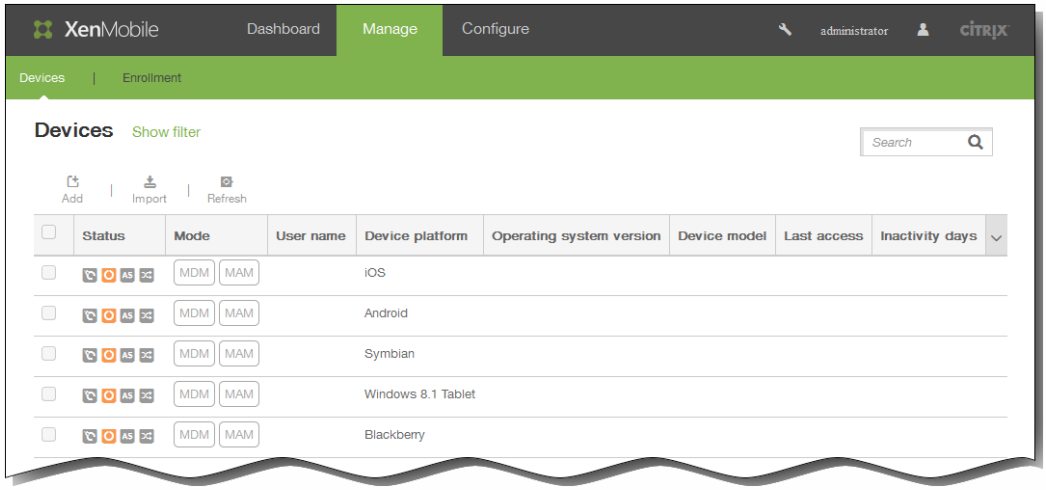
XenMobile 服务器存储库数据库中存储移动设备的列表。每个移动设备通过唯一的序列号和/或国际移动设备标识 (IMEI)/移动设备标识符 (MEID) 标识定义。要将设备填充到 XenMobile 控制台中，可以手动添加设备或从文件导入设备列表。请参阅设备置备文件格式。

在控制台中的设备页面上，可以找到列出每台设备的表格以及下列信息：状态（设备未被越狱、设备不受管理、Active Sync Gateway 不可用、无部署失败）、模式（MDM、MAM）、用户名、设备平台、操作系统版本、设备型号、上次访问时间和非活动状态天数。

注意：上述标题为默认选项。您可以自定义表格中显示的内容，方法是单击最后一个标题上的向下箭头，然后单击要查看的标题，或取消选中您不希望看到的标题。

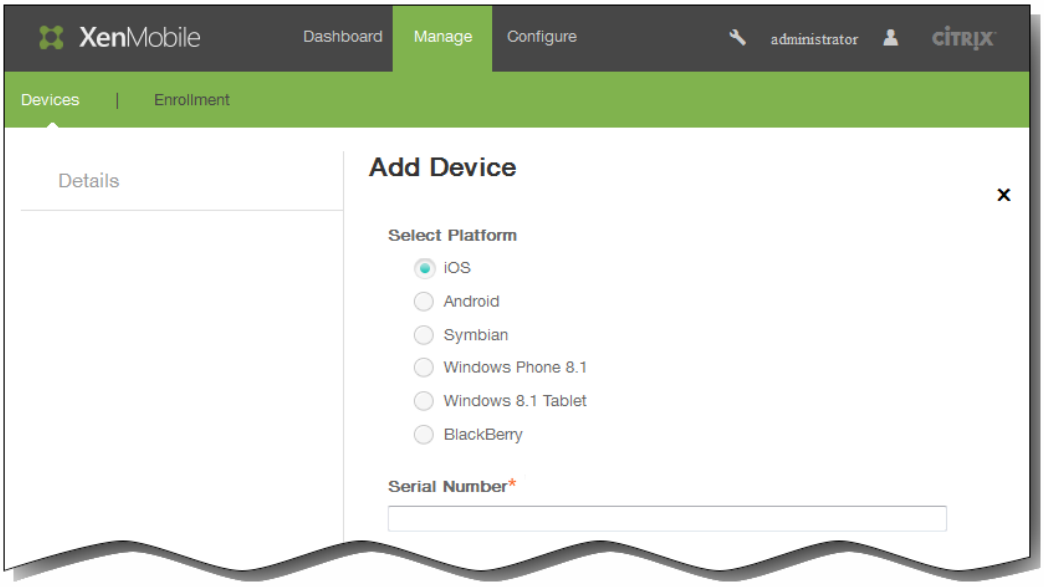


可以通过单击添加手动添加新设备，或通过单击导入导入置备文件。要更新表格，请单击刷新。

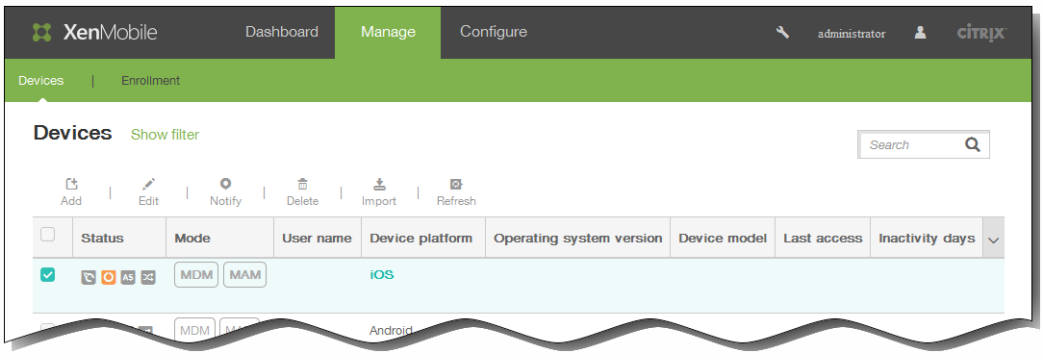


手动添加设备

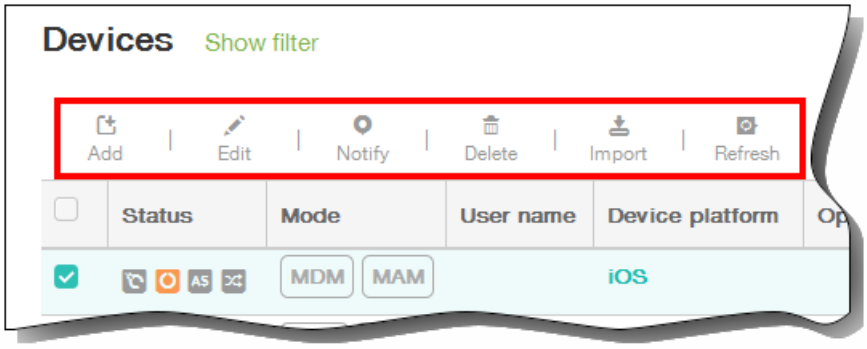
1. 在 XenMobile 控制台中，单击管理 > 设备，然后单击添加。 此时将显示添加设备页面。

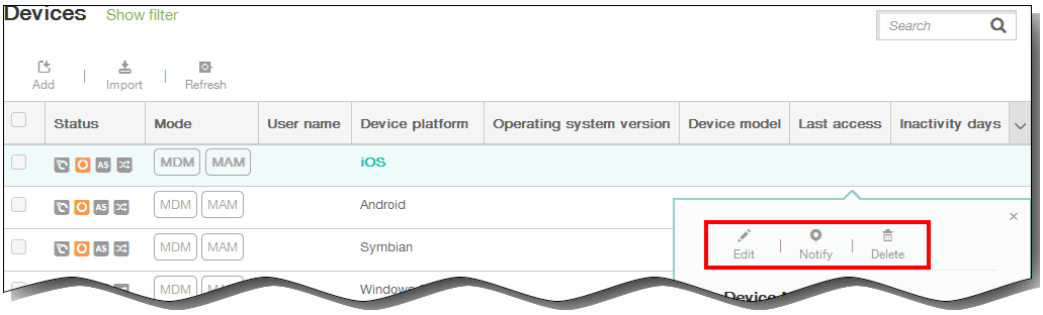


2. 在选择平台中，单击 iOS、Android、Symbian、Windows Phone 8.1、Windows 8.1 Tablet 或黑莓。
3. 输入以下信息：
   1. iOS：输入序列号。
   2. Android：输入序列号和 IMEI/MEID。
   3. Symbian：输入 IMEI/MEID。
   4. Windows Phone 8.1：输入序列号和 IMEI/MEID。
   5. Windows 8.1 Tablet：输入序列号和 IMEI/MEID。
   6. 黑莓：输入序列号和 IMEI/MEID。
4. 单击添加。 设备将添加到所显示设备表格中的列表底部。
5. 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。

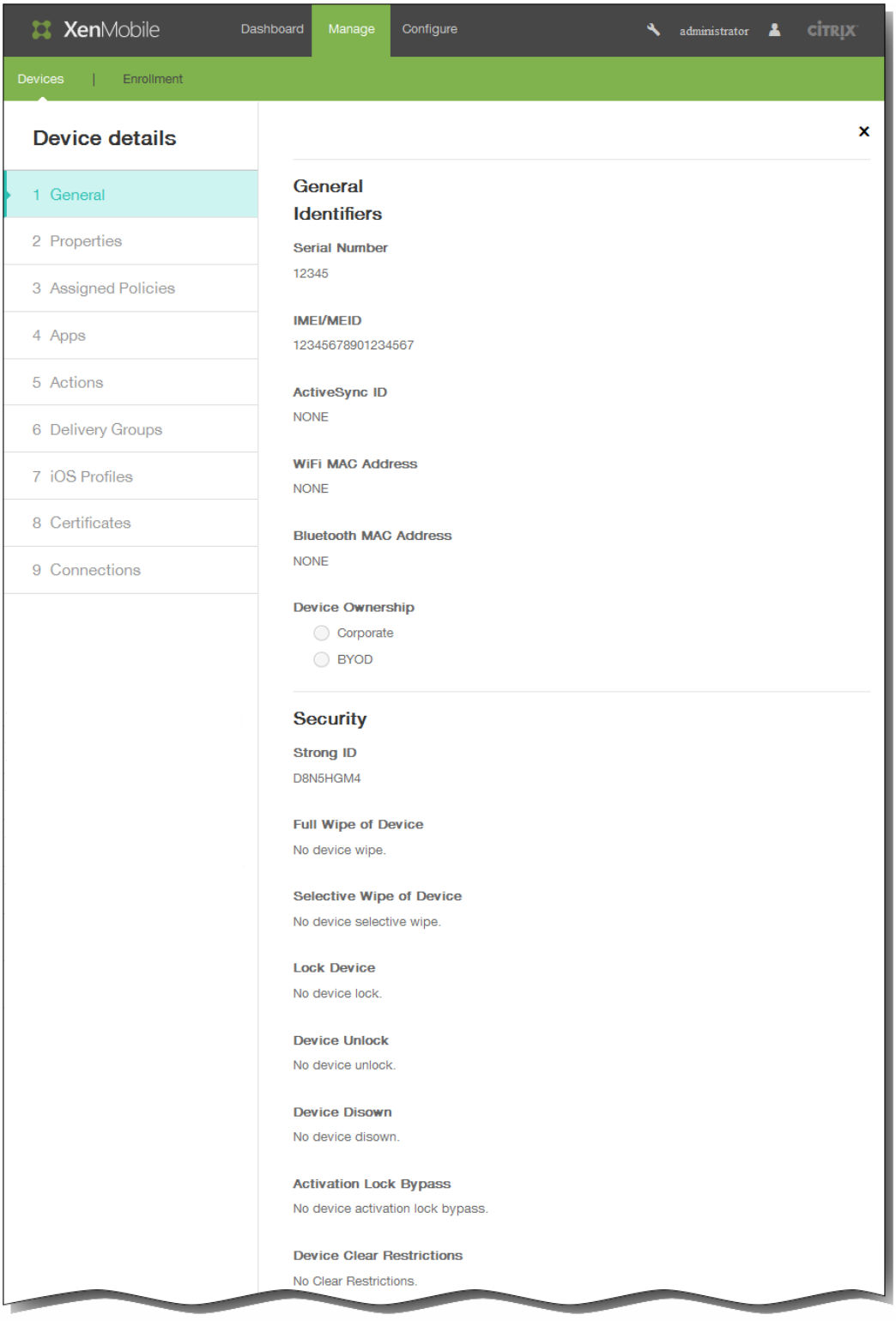


注意：如果选中某个设备旁边的复选框，选项菜单将显示在设备列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。

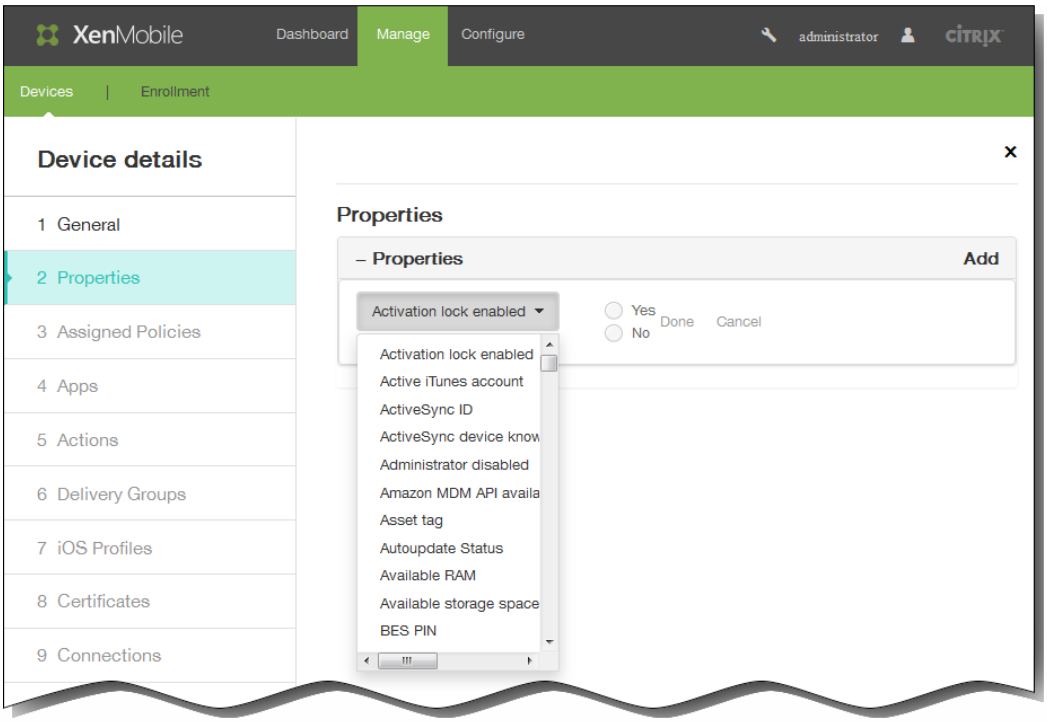




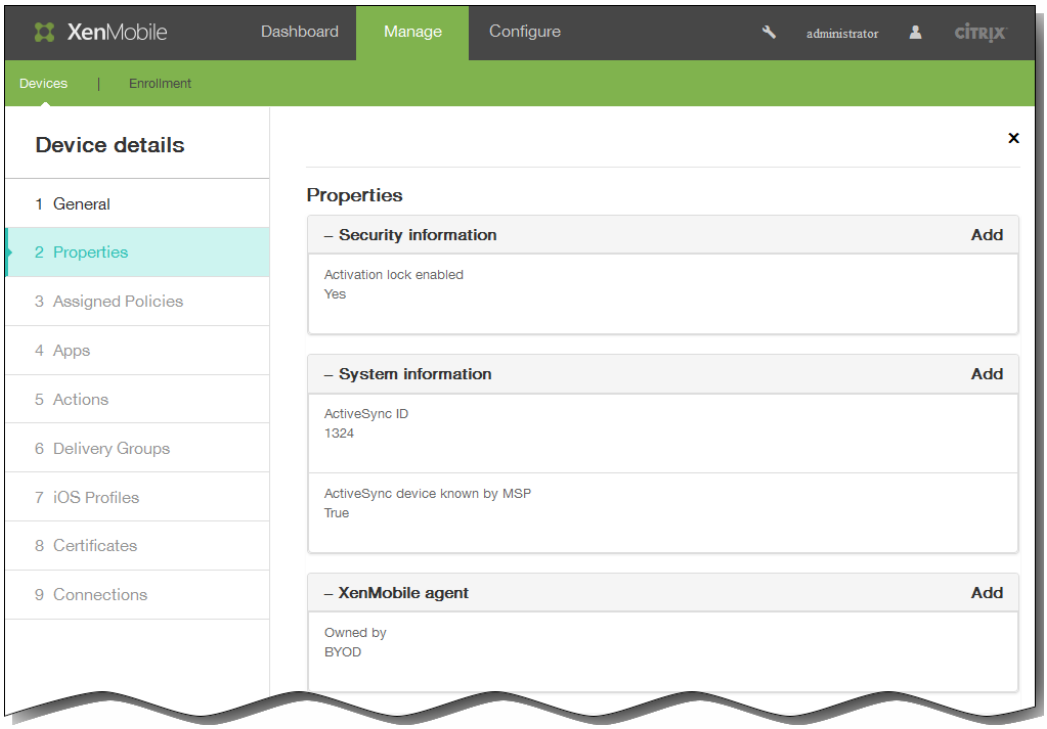
6. 在 General Identifiers（常规标识符）下面，确认显示的信息（精确的参数列表因平台类型而异）：序列号、IMEI/MEID、ActiveSync ID、WiFi MAC 地址、Bluetooth MAC 地址、设备所有权：公司或 BYOD。



7. 在安全下面，确认显示的信息（精确的参数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、否认拥有的设备、激活锁跳过、设备清除限制。
8. 单击下一步以添加属性。
9. 在属性页面上，单击添加以查看可以为设备置备的属性列表。 将显示可用属性的列表。



10. 在列表中，单击要置备的属性，然后设置其值。 例如，在前面的图片上，选择了已启用激活锁属性，您可以将其值设置为是或否。
11. 配置属性后，单击完成。
12. 为要置备的每个属性重复执行步骤 9 至 11，然后单击下一步。
    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均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。

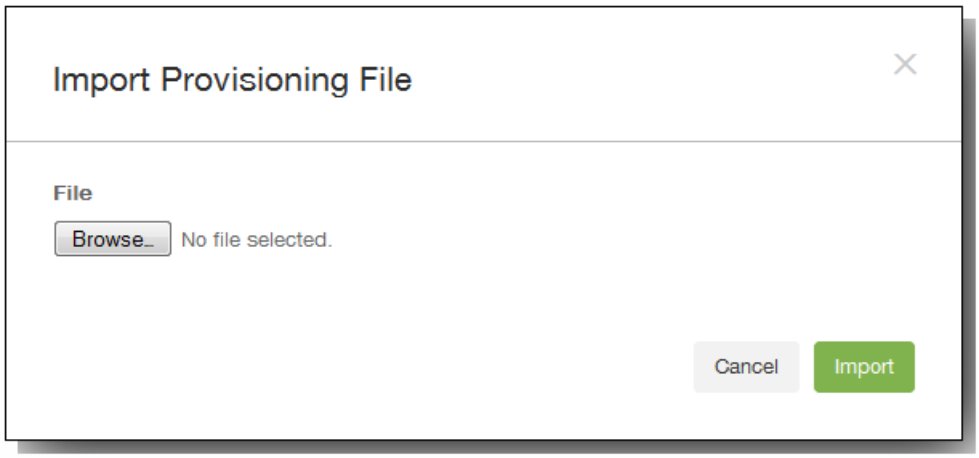
- 应用程序：以清单形式显示应用程序的数量，包括已安装的应用程序数、待定应用程序数和失败的应用程序数。
  - 对于已安装的应用程序，将显示以下信息：名称、所有权、版本、作者、大小、安装时间、标识符和类型。
  - 对于待定和失败的应用程序，将显示以下信息：名称、上次部署时间、标识符和类型。
- 操作：显示操作数，包括已部署的操作数、待定操作数和失败的操作数。每个操作显示名称和上次部署信息。
- 交付组：显示成功、待定和失败的交付组数量。为每项操作显示交付组和时间信息。此外，还显示交付组的更多详细信息，包括状态、操作、所有者和日期。
- iOS 配置文件（仅限 iOS 设备）：显示上一个 iOS 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。

13. 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。

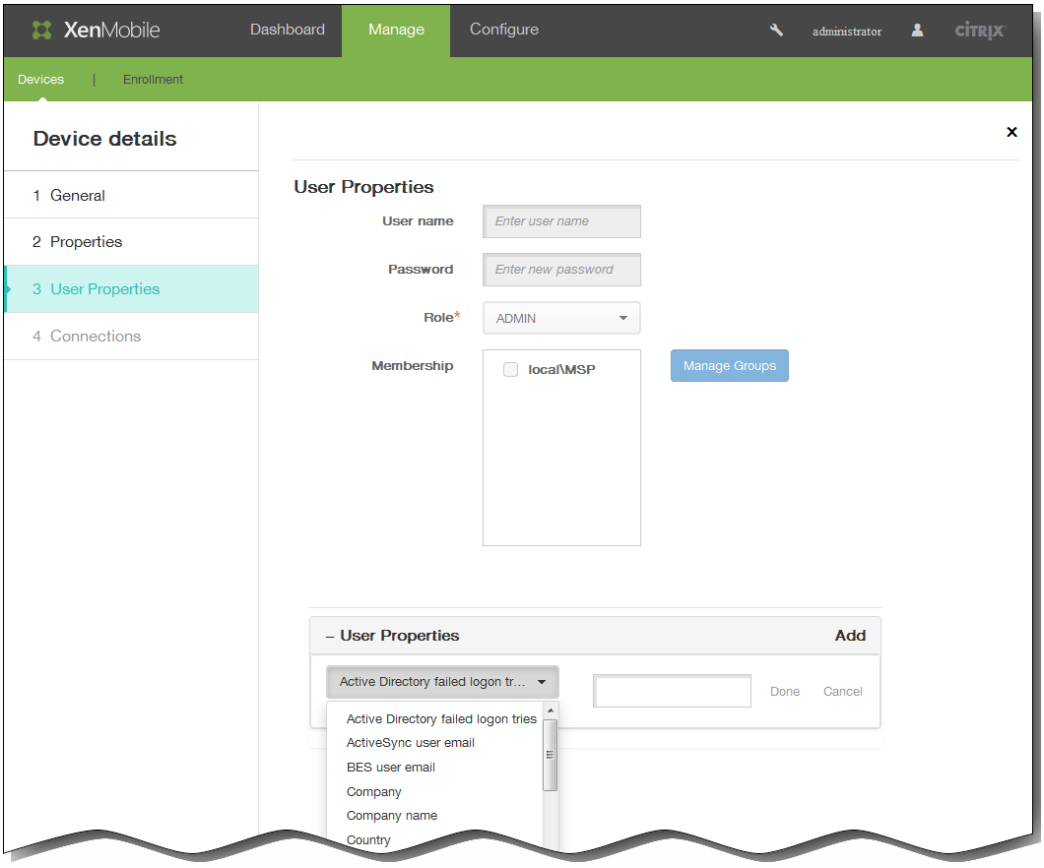
1. 在设备表格上方的菜单中，单击导入。 此时将显示导入置备文件对话框。



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）下面，您只能更改设备所有权，可以将其设置为公司或 BYOD。
3. 单击下一步。 此时将显示属性页面。
4. 在属性页面上，根据需要添加、编辑或删除属性。
   - 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，则显示已分配的属性。
6. 如果显示用户属性，请按如下所述添加、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无法编辑。

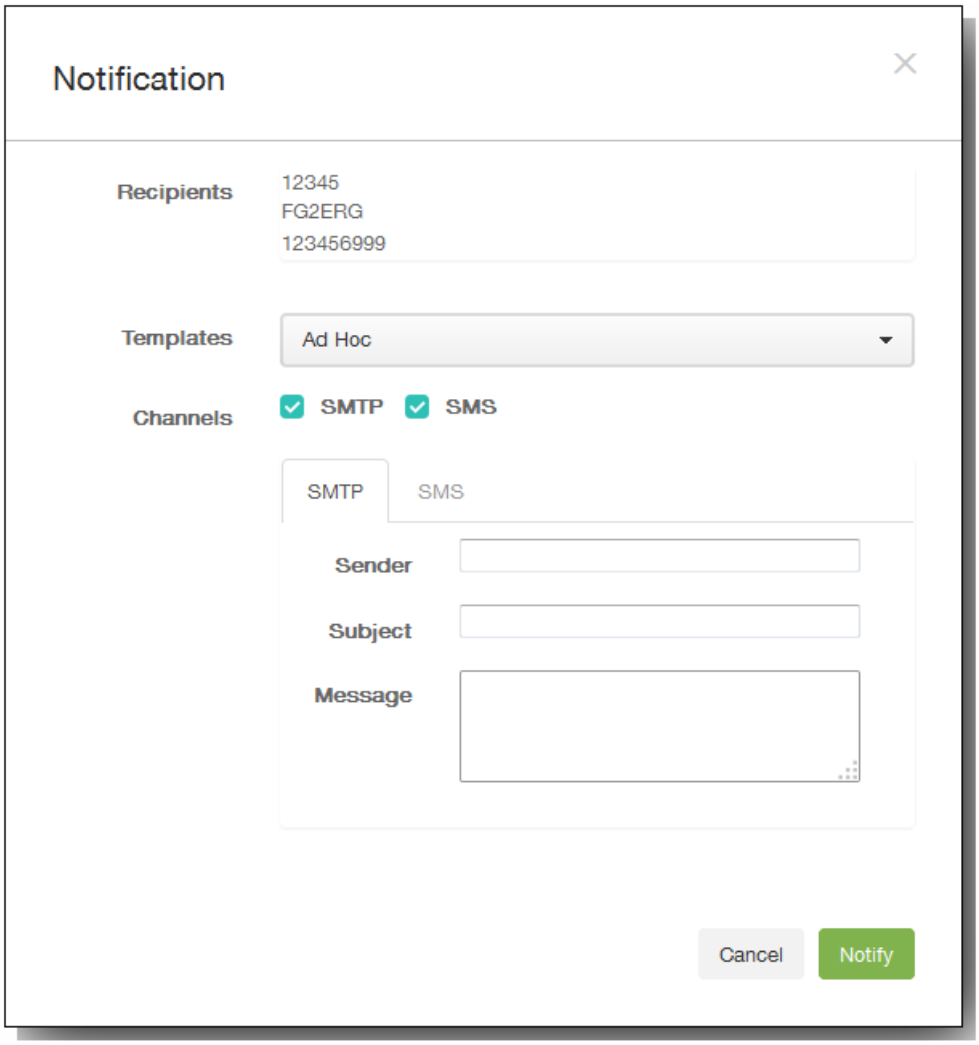
- 要添加用户属性，请单击添加。
  - 在列表中，单击要添加的属性，输入属性的值，然后单击完成或取消。为要添加的每个属性重复执行此步骤。
- 要编辑某个属性，请单击此属性，修改其设置，然后单击完成或取消。
- 要删除某个属性，请悬停在此列表的上方，然后单击右侧的 X。项目立即被删除。

7. 单击后面每个页面上的下一步以查看摘要信息。
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。 此时将显示通知对话框。收件人中列出了要接收通知的所有设备。



3. 配置以下信息：
   1. 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。
   2. 通道：选择发送消息的方式。默认值为 SMTP
      — 和
      SMS。
      可以单击 SMTP 和 SMS 选项卡以查看每种方式的消息格式。
   3. 发件人：输入可选发件人。
   4. 主题：输入临时消息的主题。
   5. 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。

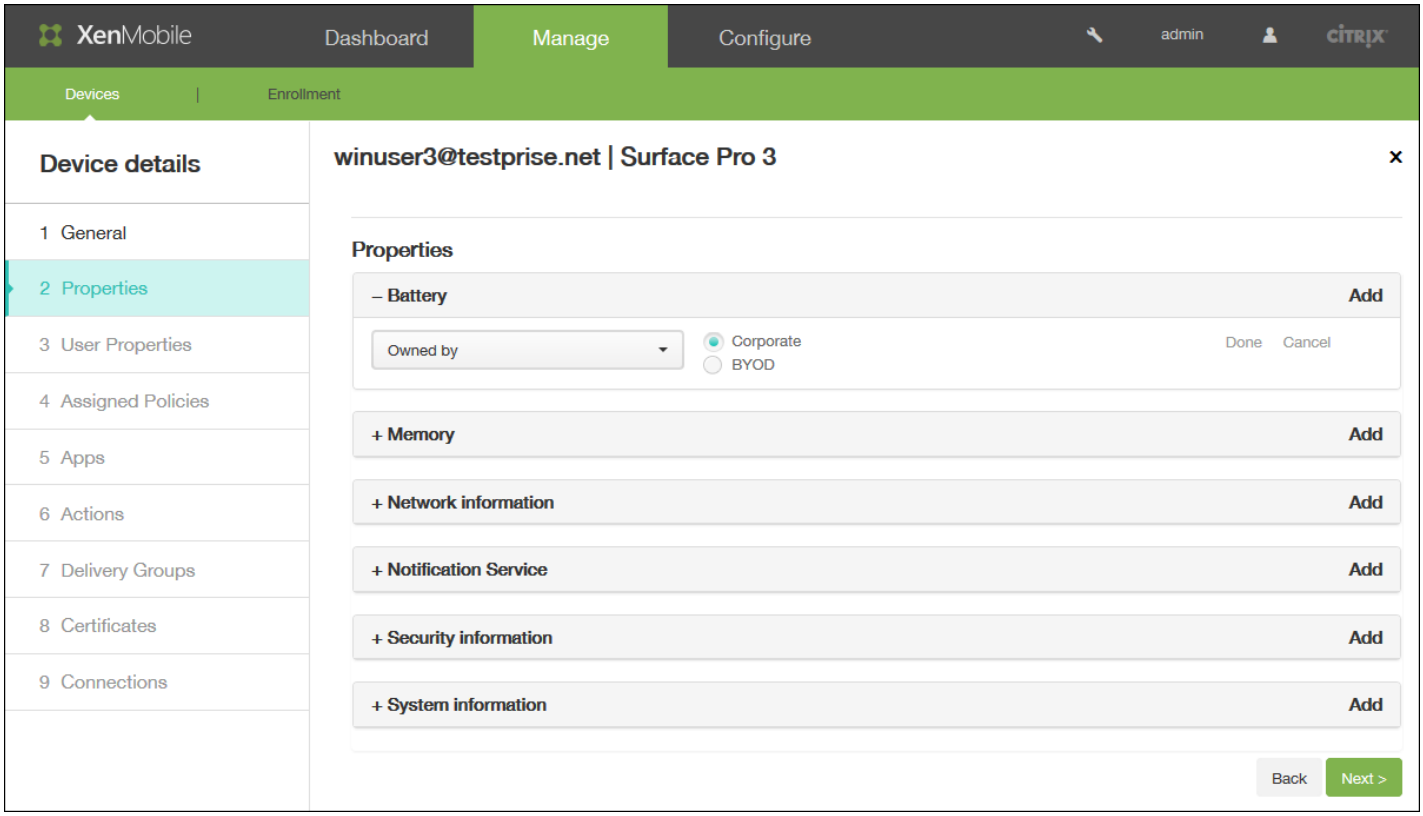
手动标记用户设备

May 05, 2016

可通过以下三种方式之一在 XenMobile 中手动标记设备：

- 在基于邀请的注册过程中标记设备。
- 在自助服务门户注册过程中标记设备。
- 通过将设备所有权添加为设备属性来标记设备。

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**选项卡将属性添加到设备，添加名为**所有者**的属性，然后选择**公司**或 **BYOD** 来手动标记设备。



设备置备文件格式

May 05, 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应该按照propertyV\;test\;1\;2这种形式键入。
- 序列号必须提供（如果未提供IMEI。
- 序列号必须提供（适用于 iOS 设备），因为序列号是 iOS 设备标识符。
- IMEI必须提供（如果未提供序列号。
- OperatingSystemFamily的有效值为：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

XenMobile 中的宏

May 05, 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。

定义用户宏

以下用户宏始终可用：

- loginname（username 以及domainname）
- username（如有，则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

- 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。

宏语法

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。

设备策略

May 05, 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。

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：

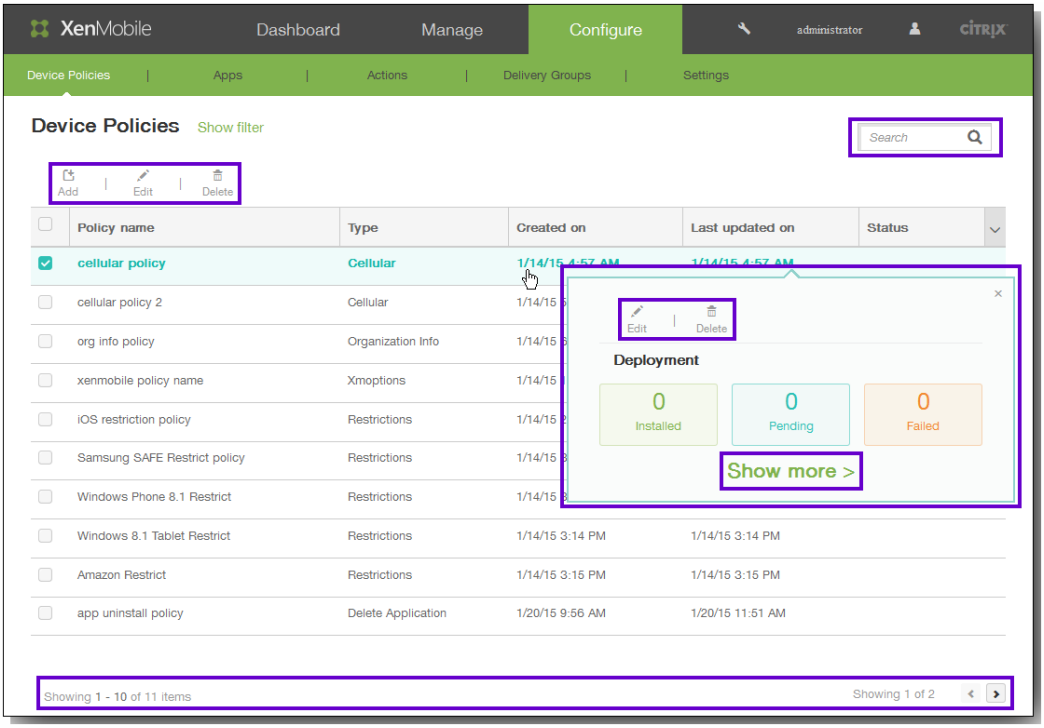
1. 为策略命名并添加说明。
2. 配置一个或多个平台。
3. 创建部署规则（可选）。
4. 将策略分配到交付组。
5. 配置部署计划（可选）。

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。

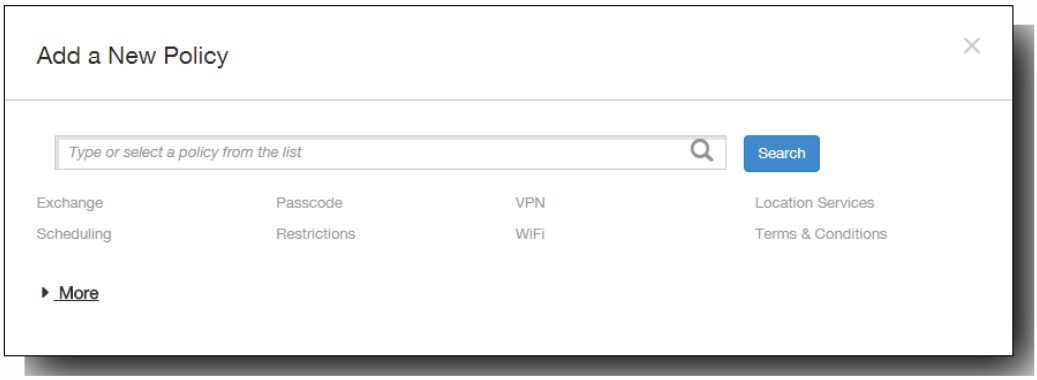
设备策略页面包含一个表格，其中显示了当前的所有策略。

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。

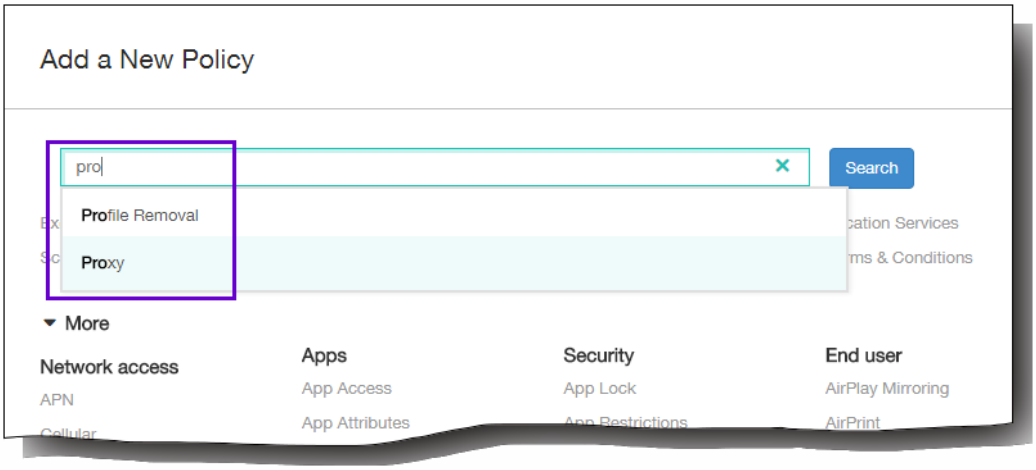


添加设备策略

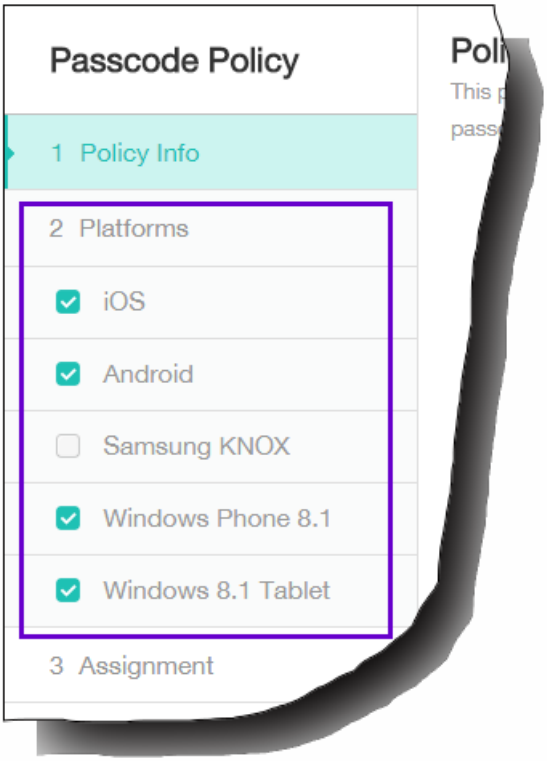
1. 在设备策略页面上，单击添加。
   此时将显示添加新策略对话框。可以展开更多以查看其它策略。



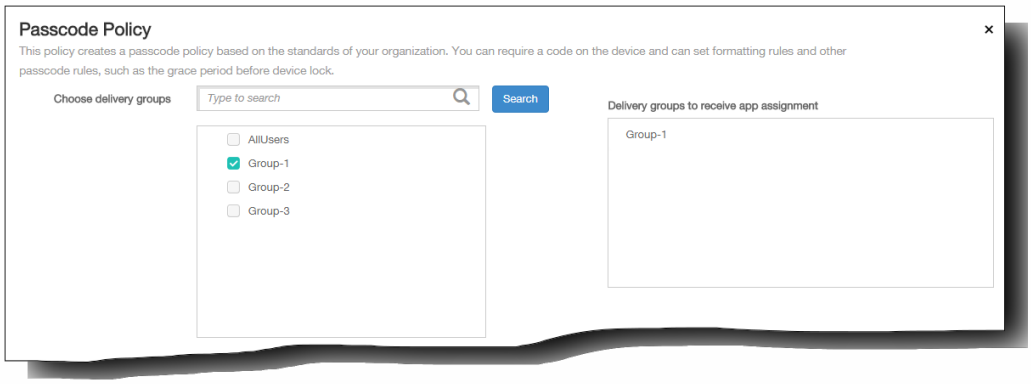
2. 查找要添加的策略，执行以下操作之一：
   - 单击策略。
     此时将显示所选策略的策略信息页面。
   - 在搜索字段中键入策略的名称。随着键入，将显示可能的匹配项。如果列表中存在您的策略，请单击此策略。只有选中的策略保留在对话框中。单击此策略以打开其策略信息页面。
     重要：如果选定的策略位于更多区域，则只有展开更多才会显示此策略。



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。



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。



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。

XenMobile 设备策略（按平台）

May 05, 2016

下表显示了您可以在 XenMobile 10.0 中为 Amazon、iOS、Android、Samsung SAFE、Samsung KNOX、Symbian、Windows Phone 8.1 和 Windows 8.1 Tablet 设备添加和配置的设备策略。在 XenMobile 控制台中，可以从配置 > 设备策略添加和配置设备策略。

注意：Android Sony 仅支持存储加密策略。Android HTC 仅支持 Exchange 策略。

设备策略	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
通用功能								
Exchange		X	X	X	X		X	
计划			X			X		
通行码		X	X		X		X	X
限制	X	X		X			X	X
VPN	X	X	X	X	X			X
WiFi		X	X				X	X
定位服务		X	X					
条款和条件	X	X	X	X	X	X	X	X
网络访问								
APN		X	X		X			
手机网络			X					
个人热点		X						
代理		X						
远程支持					X			

漫游策略	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
Samsung 防火墙				X				
通道			X					
	Amazon	**iOS**	**Android**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 Tablet**
自定义虚拟机								
自定义 XML						X	X	X
导入 iOS 配置文件		X						
删除								
配置文件删除		X						
应用程序								
应用程序访问权限		X	X			X		
应用程序属性		X						
应用程序配置		X						
应用程序清单		X	X		X	X	X	X
应用程序卸载		X	X		X			X
应用程序卸载限制	X			X				
文件			X					
Samsung 浏览器				X	X			
旁加载密钥								X

签署证书 设备策略	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	X Windows 8.1 Tablet
Web 剪辑		X	X					X
Worx Store		X	X					X
	Amazon	**iOS**	**Android**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 Tablet**
安全性								
应用程序锁定		X	X					
应用程序限制					X			
联系人 (CardDAV)		X						
凭据		X	X					X
是否需要 Kiosk				X				
托管域		X						
SCEP		X						
Samsung MDM 许可证密钥				X	X			
存储加密			X	X			X	
Web 内容过滤器		X						
XenMobile 代理								
企业 Hub							X	
XenMobile 选项			X			X		
XenMobile 卸载			X					

最终用户设备策略	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
AirPlay 镜像		X						
AirPrint		X						
日历 (CalDav)		X						
字体		X						
LDAP		X						
MDM 选项		X						
邮件		X						
组织信息		X						
SSO 帐户		X						
订阅日历		X						

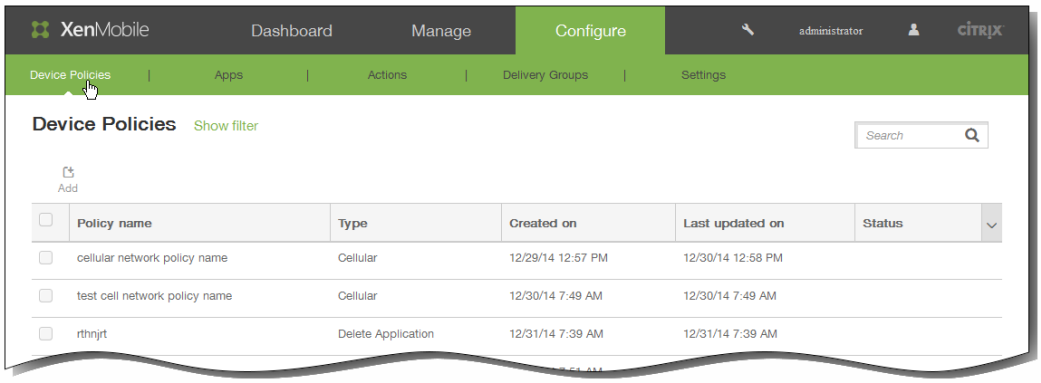
添加应用程序访问设备策略

May 05, 2016

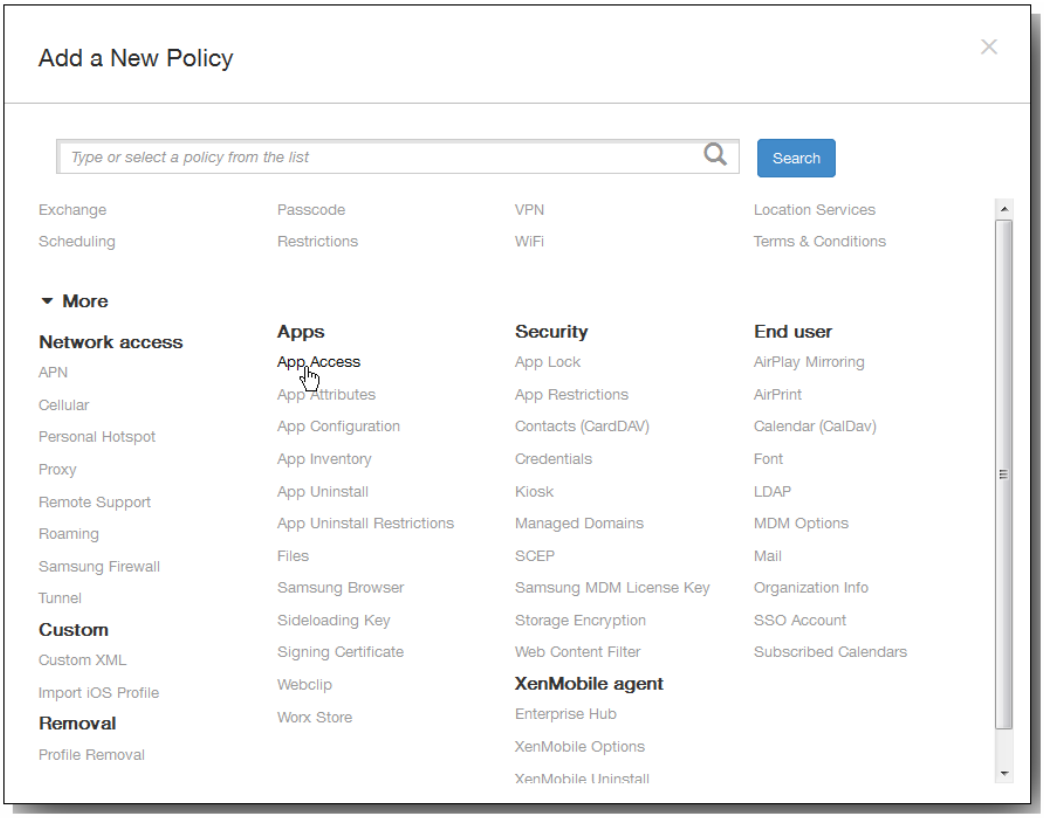
利用 XenMobile 中的应用程序访问设备策略，可以定义需要安装到设备上、可以安装到设备上或不得安装到设备上的应用程序列表。然后，可以创建自动化操作，以使设备符合此应用程序列表。可以创建适用于 iOS、Android 或 Symbian 设备的应用程序访问策略。

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。

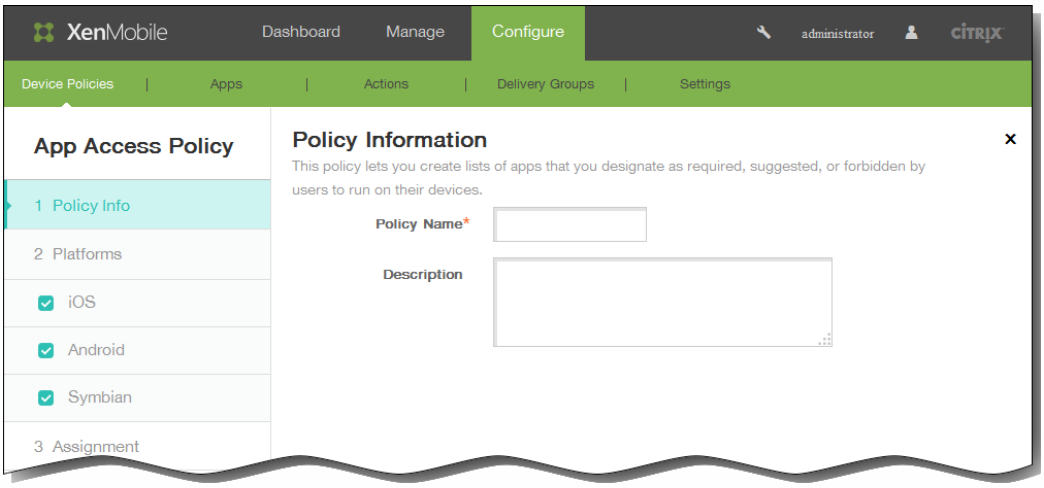
1. 在 XenMobile 控制台中，单击配置 > 设备策略。



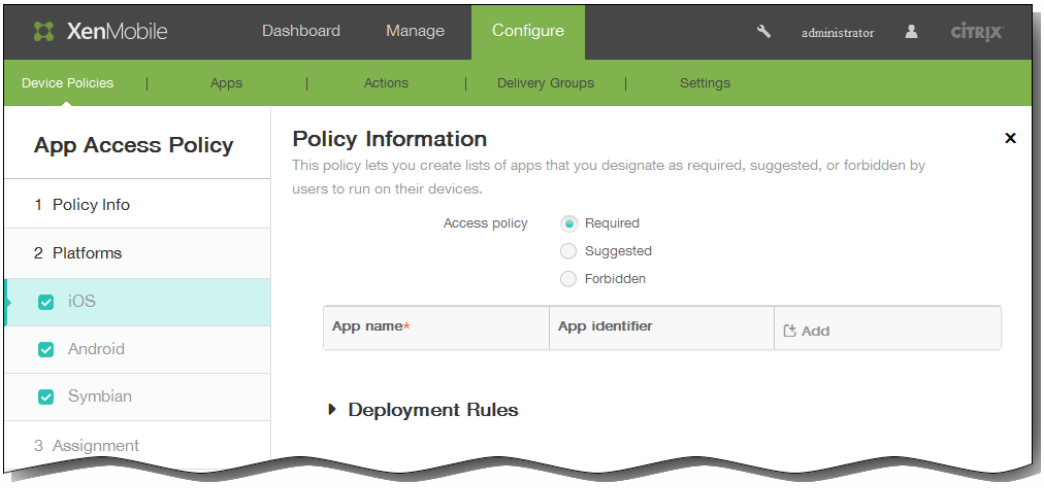
2. 单击添加。 此时将显示添加新策略对话框。



3. 单击更多 > 应用程序访问。 将显示应用程序访问策略信息页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。
   注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 iOS 平台配置页面。



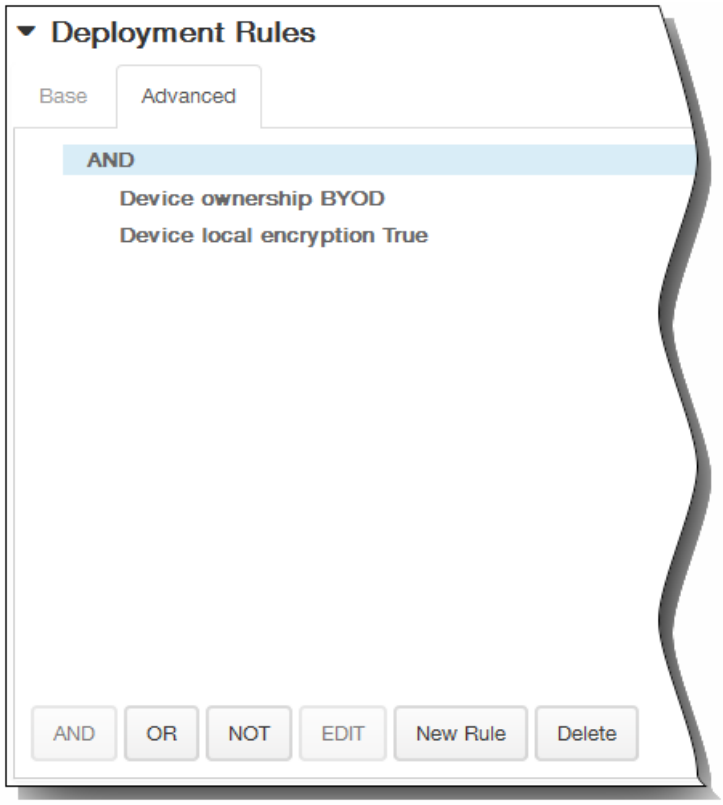
6. 在平台下面，选择要添加的一个或多个平台，然后为每个平台执行以下操作：
   1. 访问策略：单击必需、推荐或禁止。 默认设置为必需。
   2. 要向列表中添加一个或多个应用程序，请单击添加，然后执行以下操作：
      1. 应用程序名称：输入应用程序的名称。
      2. 应用程序标识符：输入可选应用程序标识符。
      3. 单击保存或取消。
      4. 为要添加的每个应用程序重复步骤 i.至步骤 iii.。

      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。

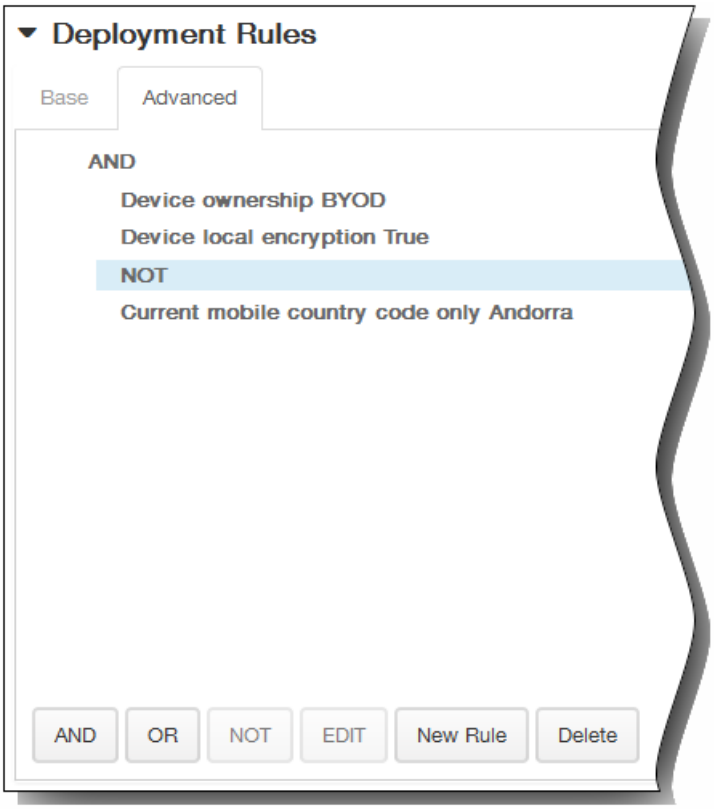
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

   1. 在此列表中，单击选项以确定部署策略的时间。
      1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
      2. 单击新建规则以定义条件。
      3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
      4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
   2. 单击高级选项卡以使用布尔选项组合规则。

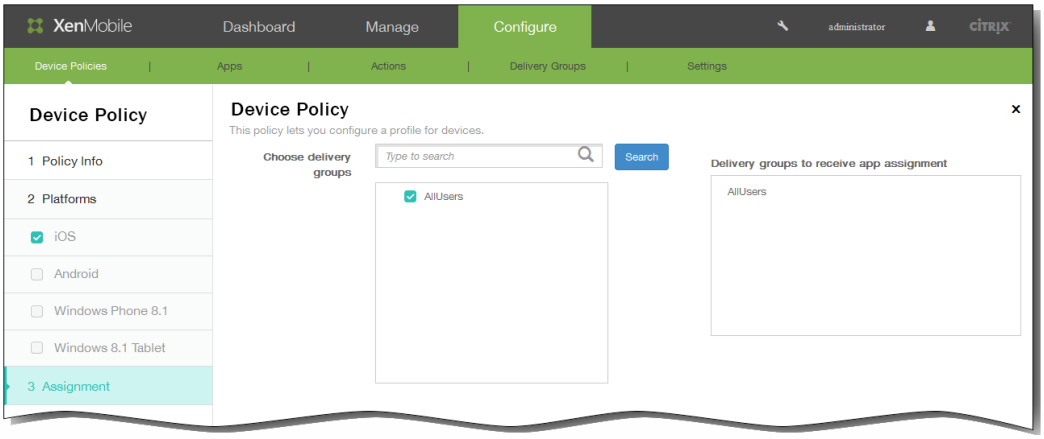


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



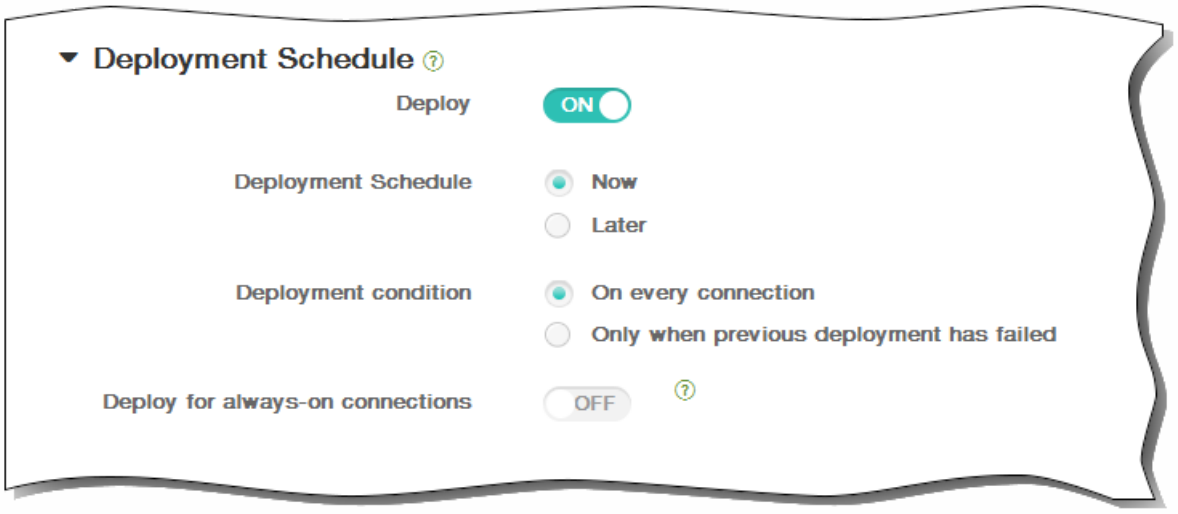
8. 单击下一步。 此时将显示下一个平台页面或分配策略页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

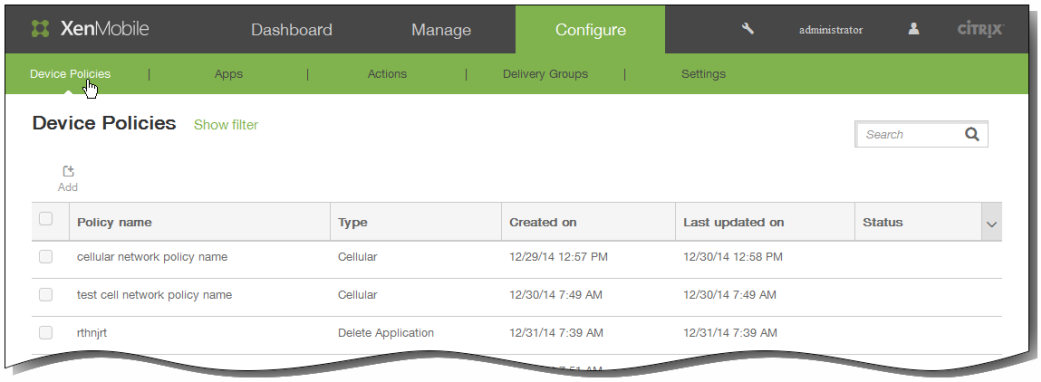
添加应用程序清单设备策略

May 05, 2016

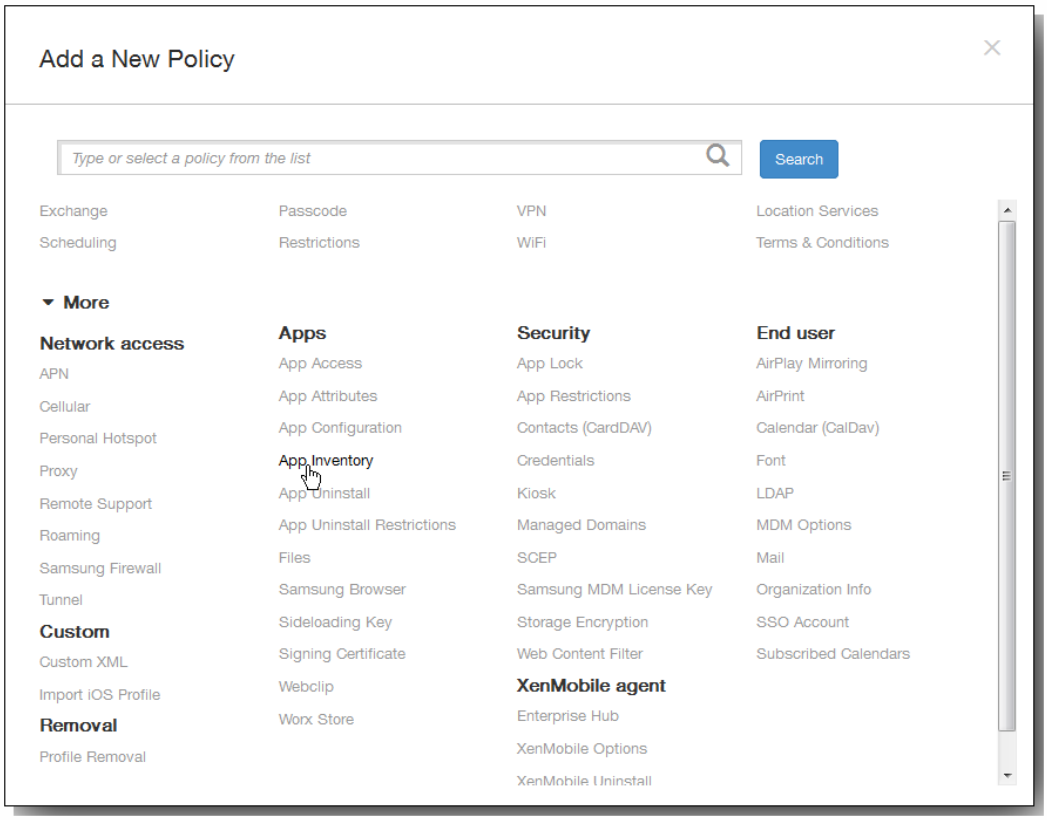
借助 XenMobile 中的应用程序清单策略，您可以收集受管理设备上应用程序的清单，然后根据该清单对比部署到这些设备上的任何应用程序访问策略。这样，您可以发现出现在应用程序黑名单（在应用程序访问策略中禁止）或白名单（在应用程序访问策略中需要）上的应用程序，并采取相应的操作。

重要：要使已更新的应用程序显示在用户 Android 设备上 Worx Store 中的“有可用更新”列表中，必须首先向用户设备部署此策略。

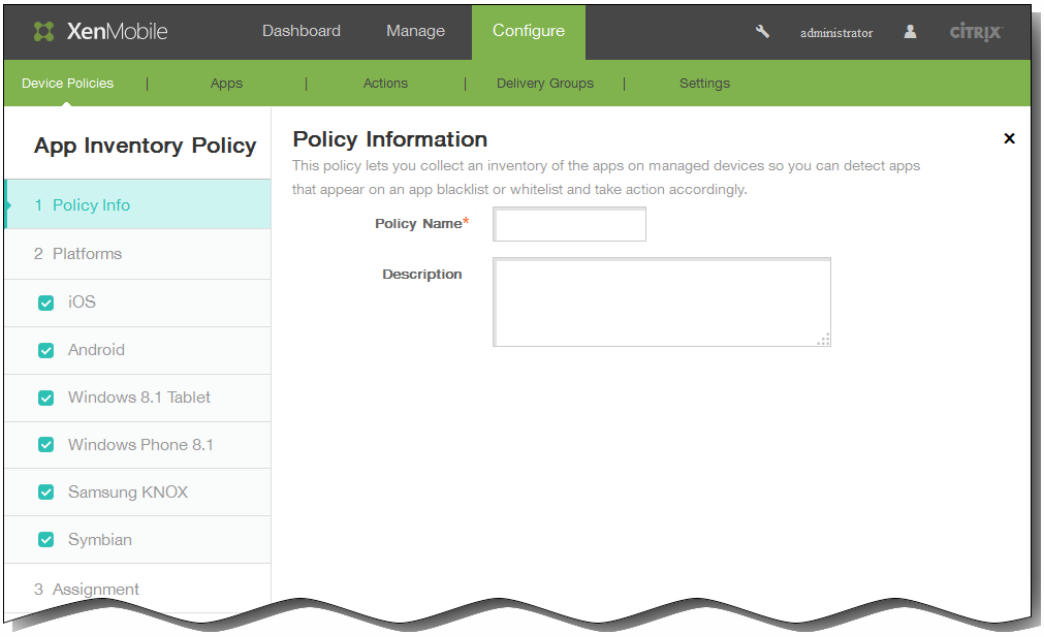
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



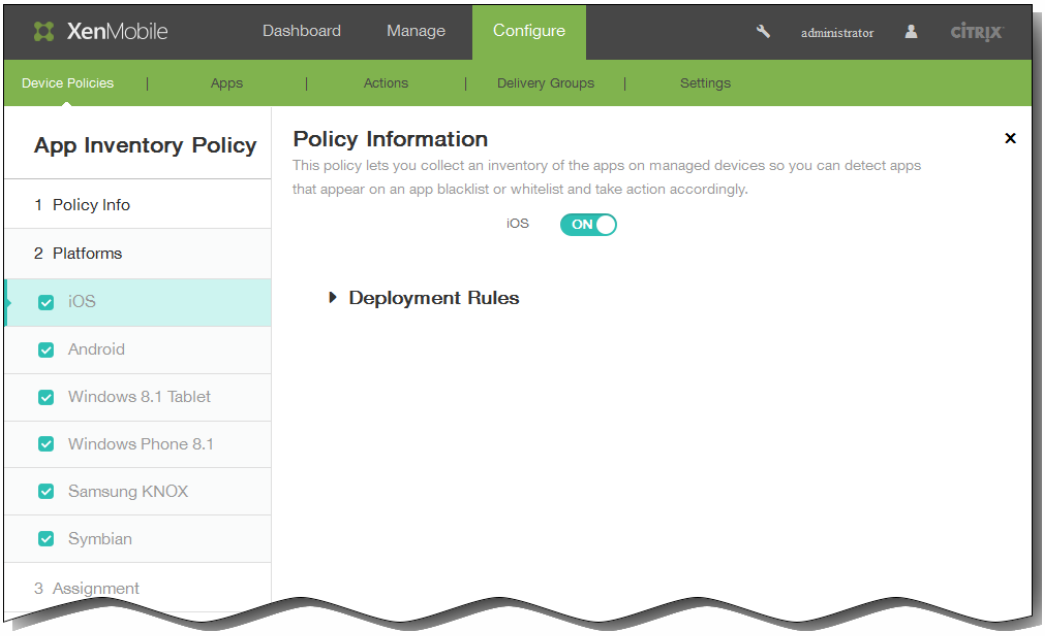
2. 单击添加。 将显示添加新策略页面。



3. 单击更多 > 应用程序清单。 将显示应用程序清单策略页面。



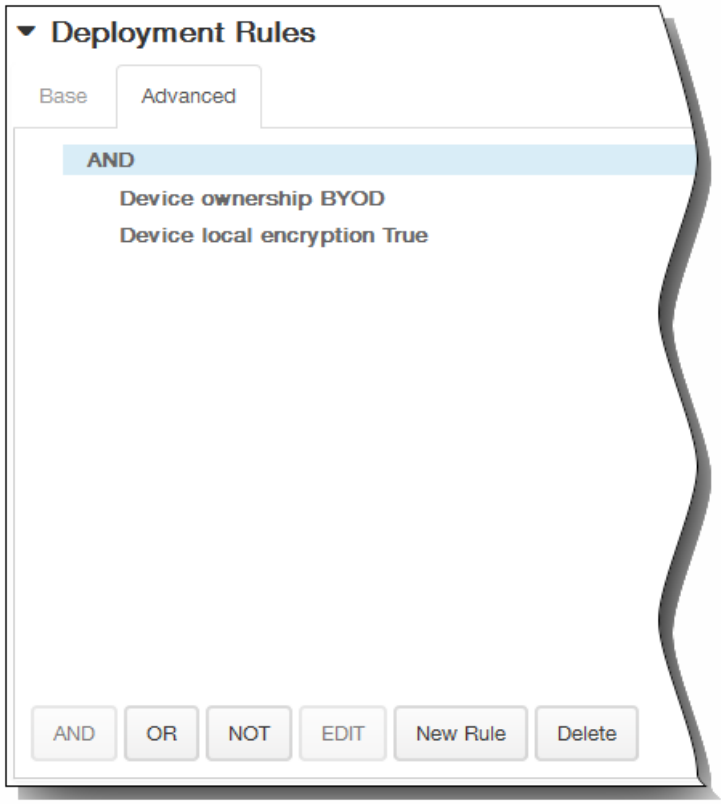
4. 在策略信息窗格中，键入以下信息：
   1. 策略名称：键入策略的名称。
   2. 说明：键入策略的可选说明。
5. 单击下一步。 此时将显示策略平台页面。
   注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 iOS 平台配置面板。



选择要添加的一个或多个平台，然后为每个平台执行以下操作：

6. 保留默认设置或将此设置更改为关。 默认值为开。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

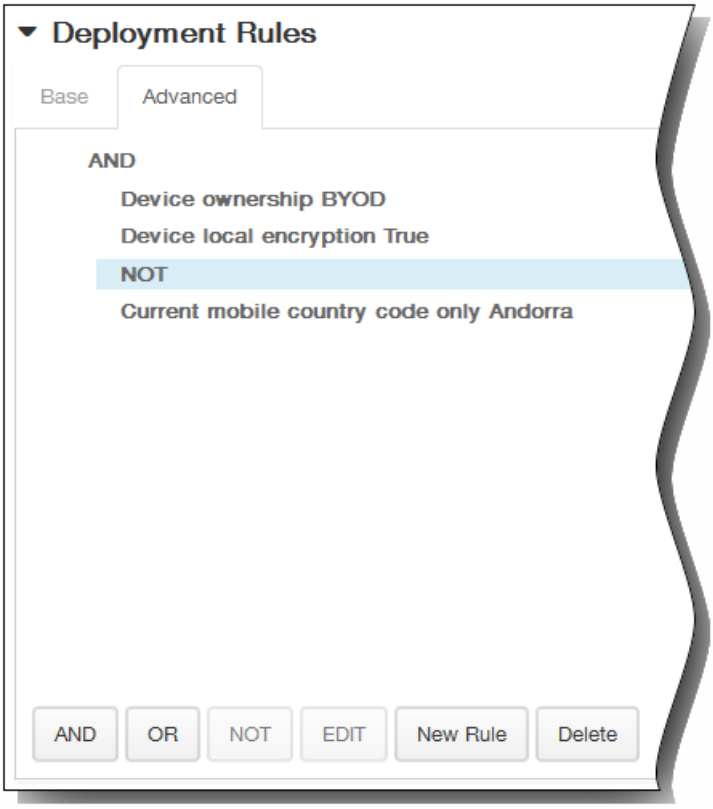
1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。



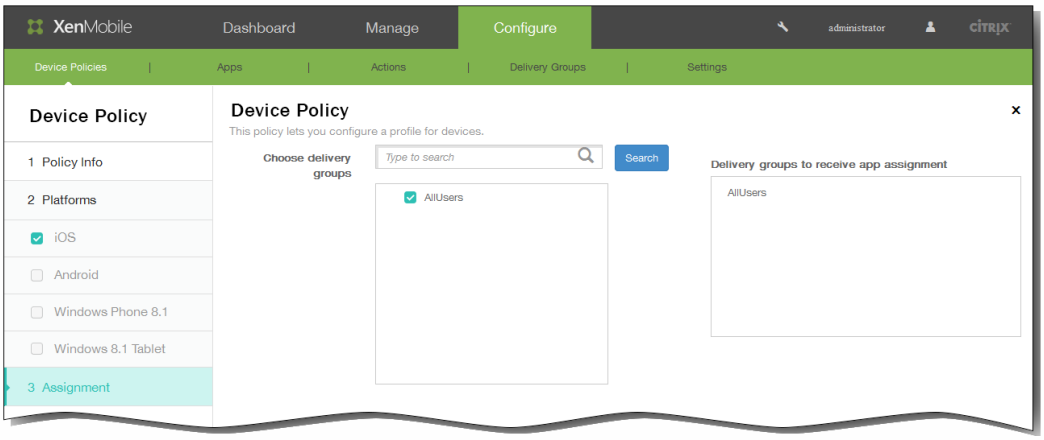
将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。

3. 如果要添加更多条件，请再次单击新建规则。
   在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



8. 单击下一步。 此时将显示下一个平台页面或分配策略页面。
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。

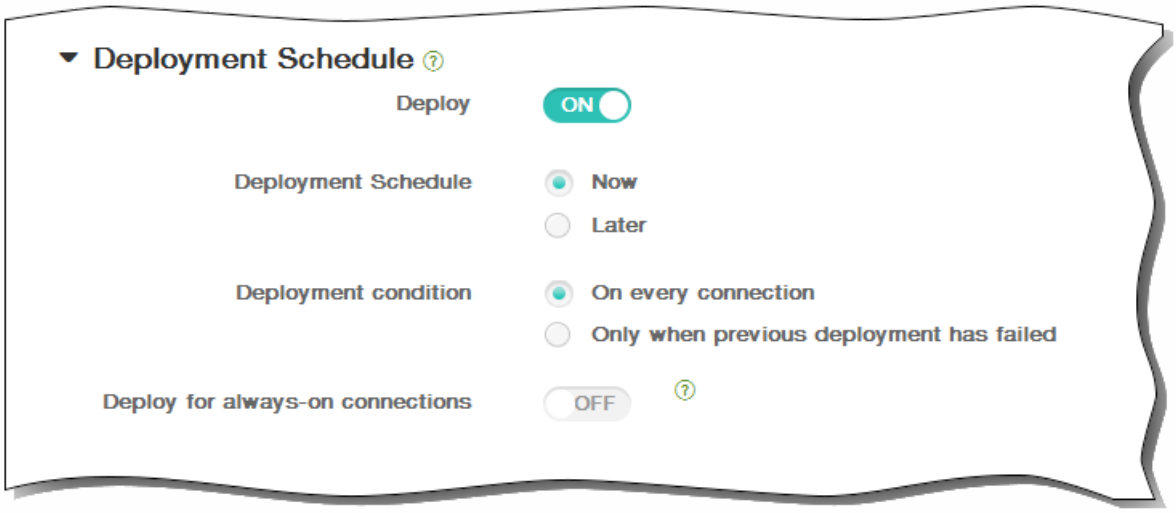


10. 展开部署计划，然后配置以下设置：
    1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。 如果选择关，无需配置其他选项。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
    4. 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。 默认选项为每次连接时。

5. 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。



11. 单击保存以保存此策略。

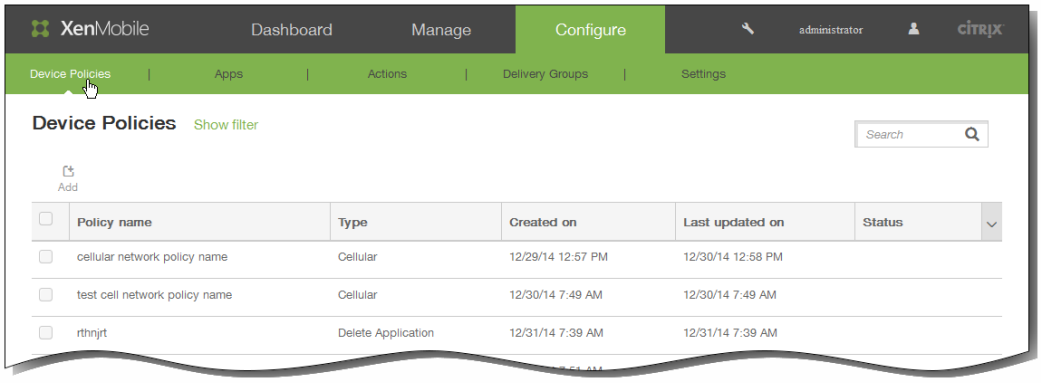
添加适用于 Android 的应用程序通道设备策略

May 05, 2016

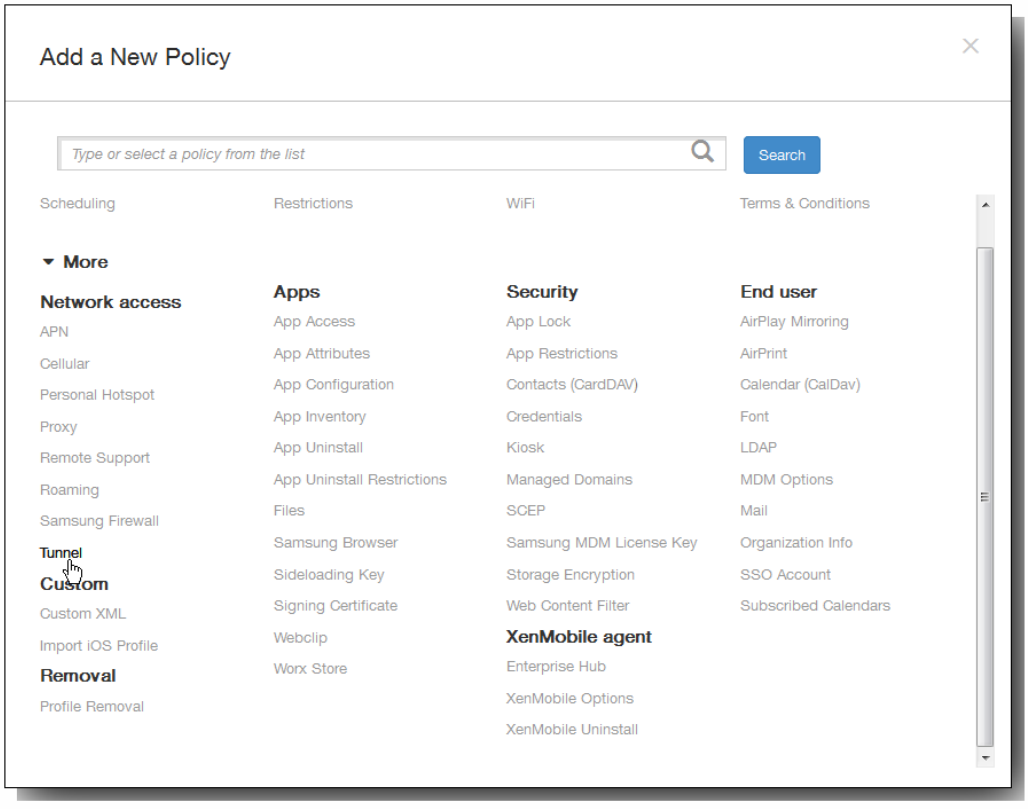
应用程序通道旨在提高移动应用程序的服务连续性及数据传输可靠性。应用程序通道定义移动设备应用程序的客户端组件与应用程序服务器组件之间的代理参数。还可以使用应用程序通道创建设备的远程支持通道以使用管理支持。

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。

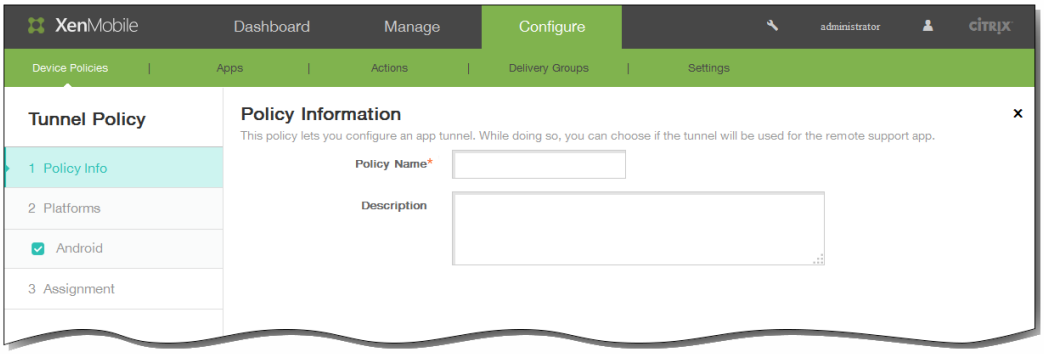
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



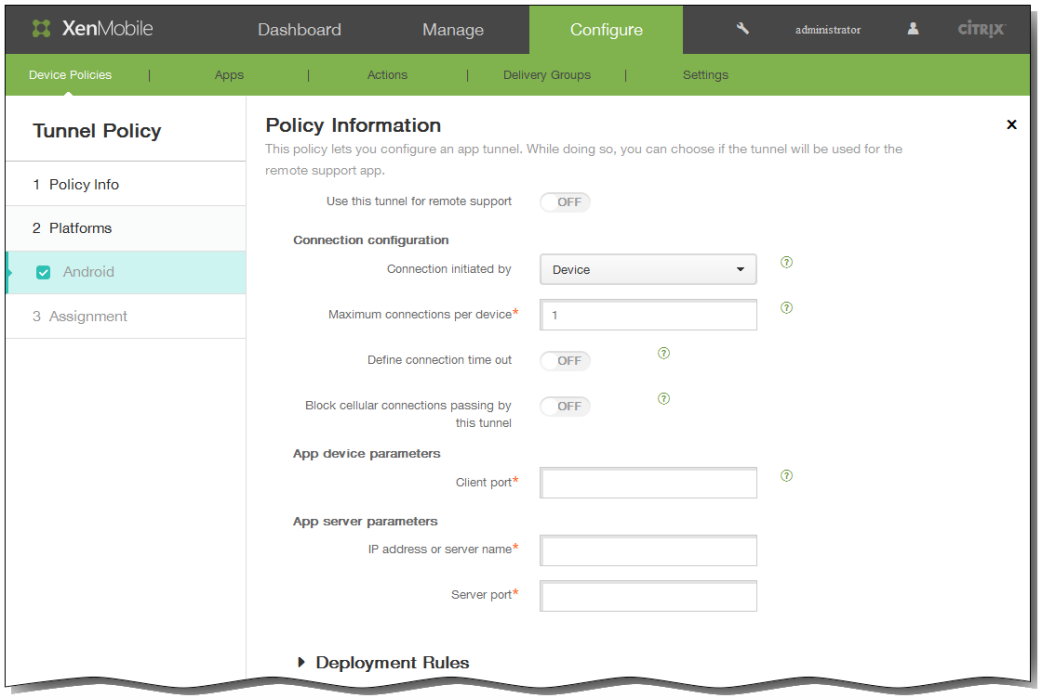
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在网络访问下面，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：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 Android 策略平台页面。



6. 在使用此通道进行远程支持中，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：
   1. 连接发起者：单击设备或服务器以指定发起连接的源。
   2. 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。
   3. 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。
   4. 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。
   5. 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。

6. 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。
7. 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。
8. 服务器端口：键入服务器端口号。

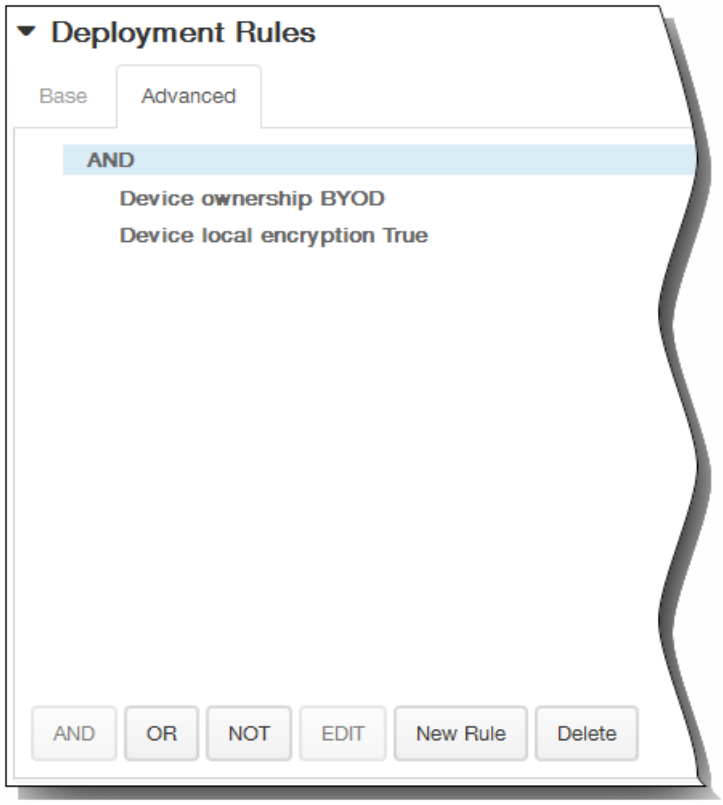
如果**选择**远程支持，请执行以下操作：

1. 使用此通道进行远程支持：设置为开。
2. 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。
3. 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。
4. 使用 SSL 连接：选择是否为此通道使用安全 SSL 连接。
5. 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。

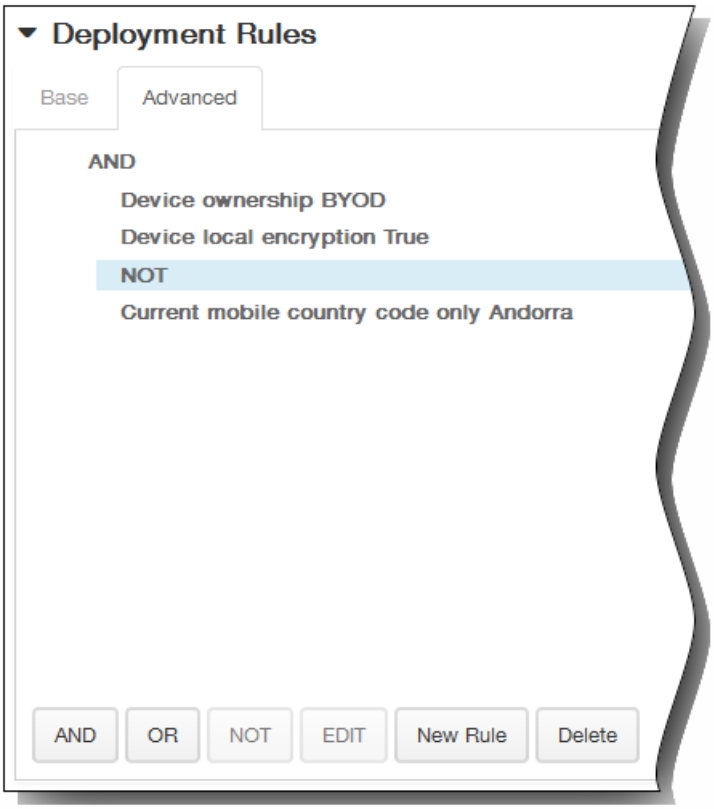
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

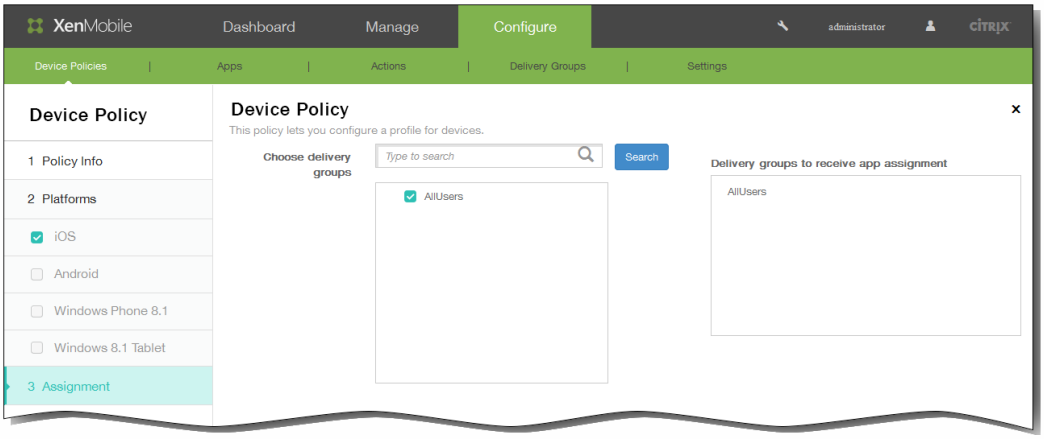


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。

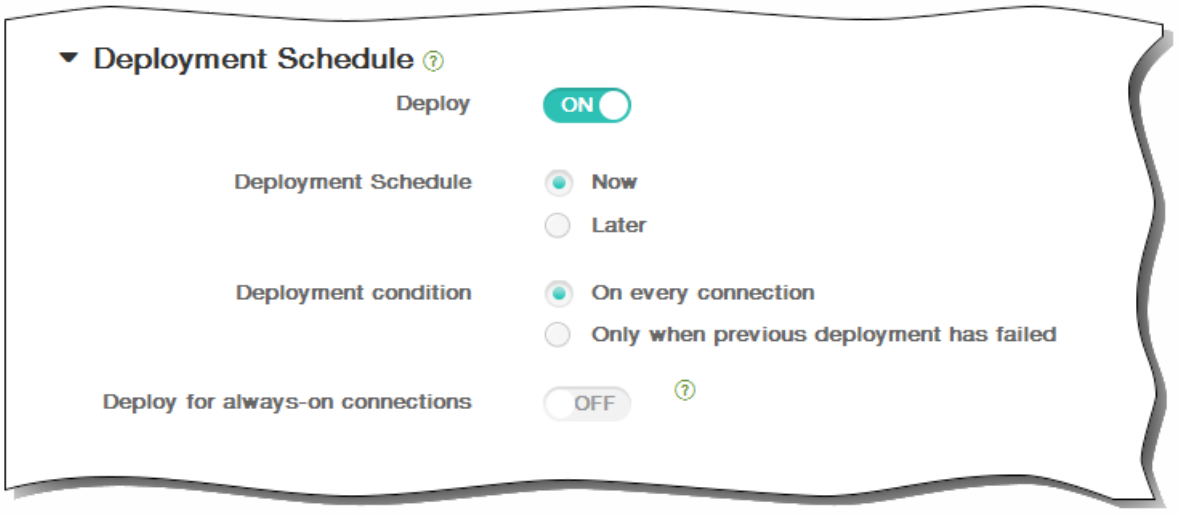


8. 单击下一步。 此时将显示通道策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

自定义 XML 设备策略

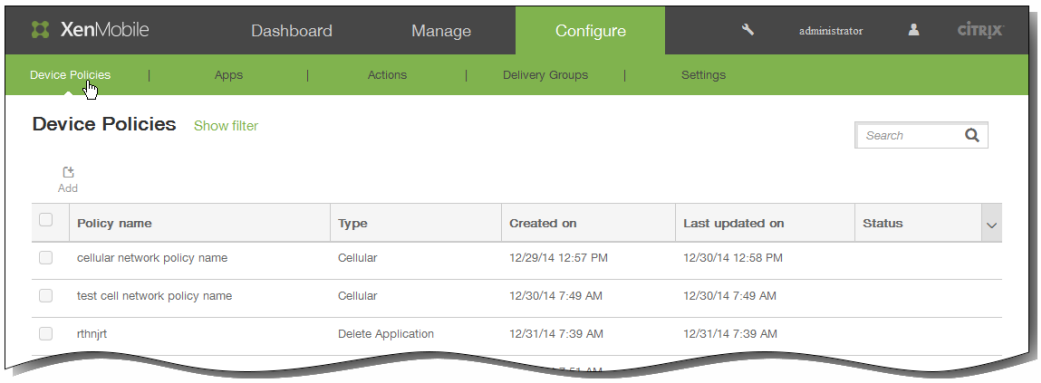
May 05, 2016

当您需要在 Windows Phone 8.1、Windows 8.1 Tablet 和 Symbian 设备上自定义以下功能时，可以在 XenMobile 中创建自定义 XML 策略：

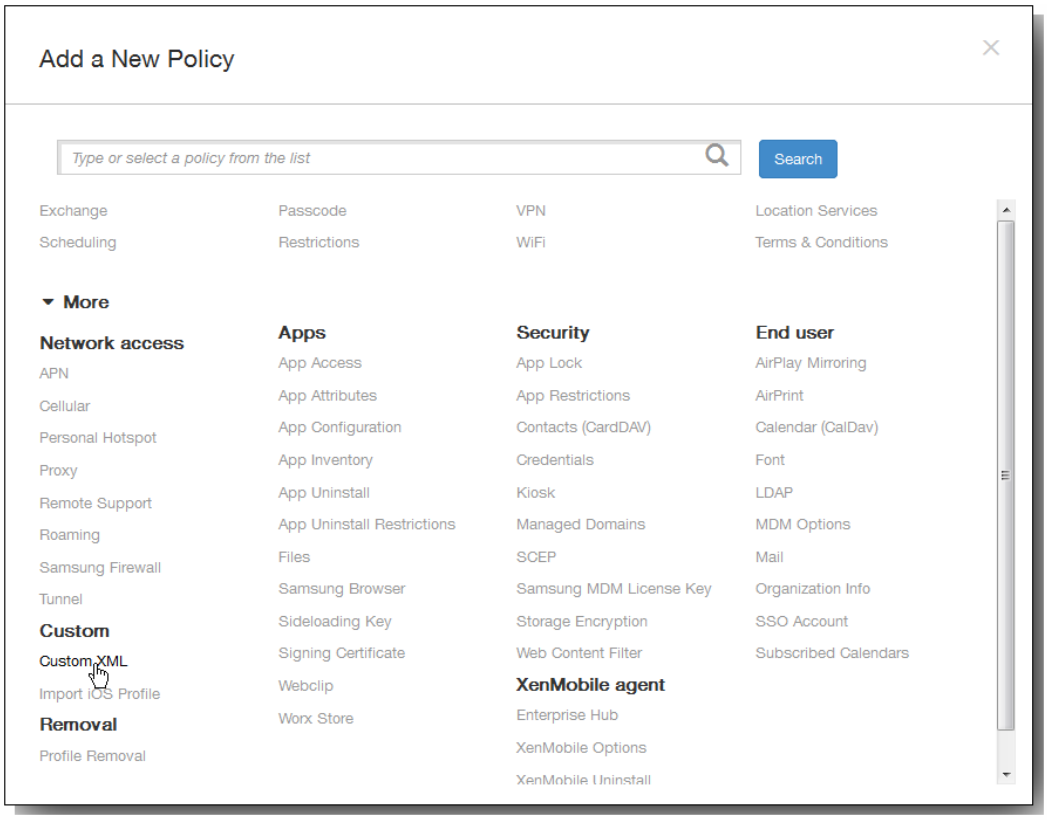
- 置备，包括配置设备以及启用或禁用功能
- 设备配置，包括允许用户更改设置和设备参数
- 软件升级，包括提供要加载到设备中的新软件或缺陷修复（包括应用程序和系统软件）
- 故障管理，包括接收来自设备的错误和状态报告

在 Windows 8.1 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。

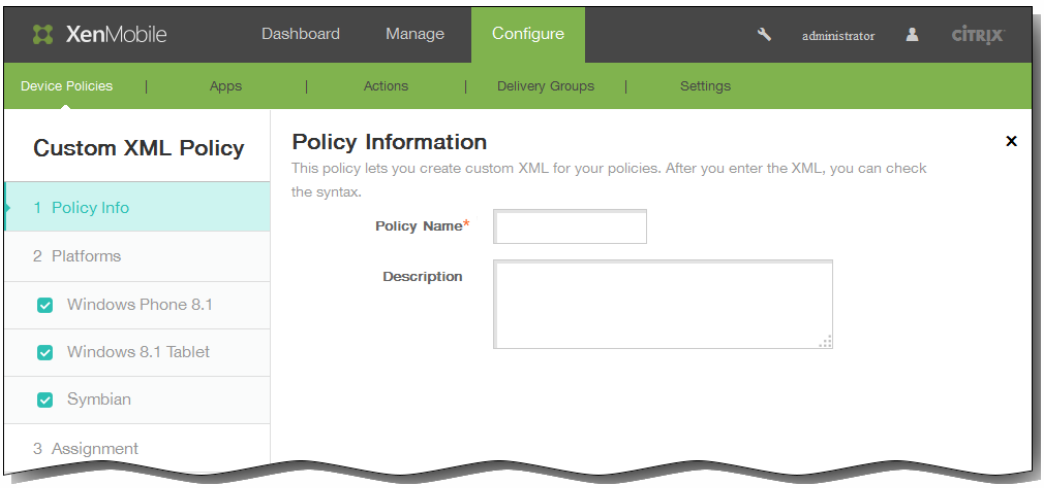
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



2. 单击添加添加新策略。 此时将显示添加新策略对话框。

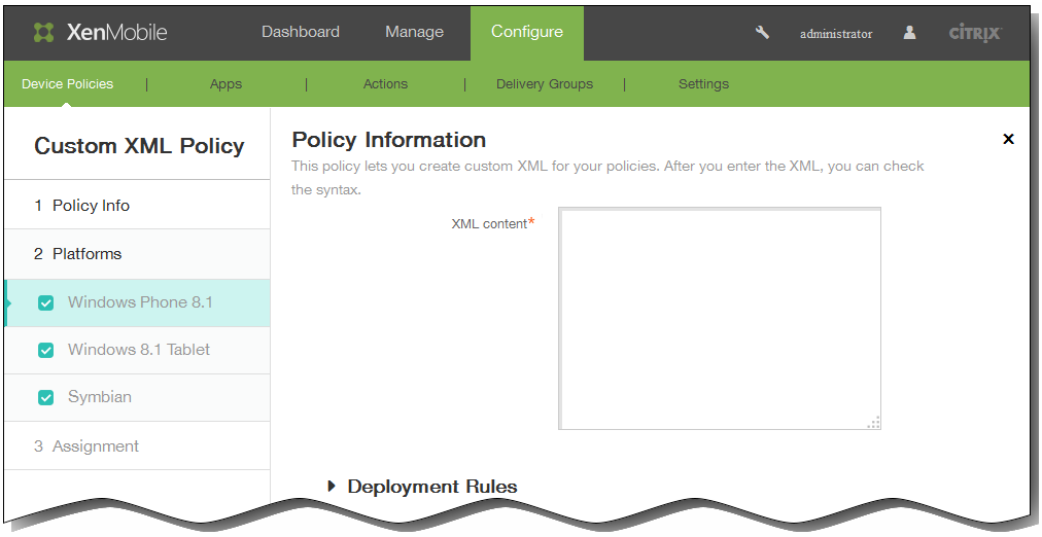


3. 单击更多，然后在自定义下单击自定义 XML。 此时将显示自定义 XML 策略信息页面。



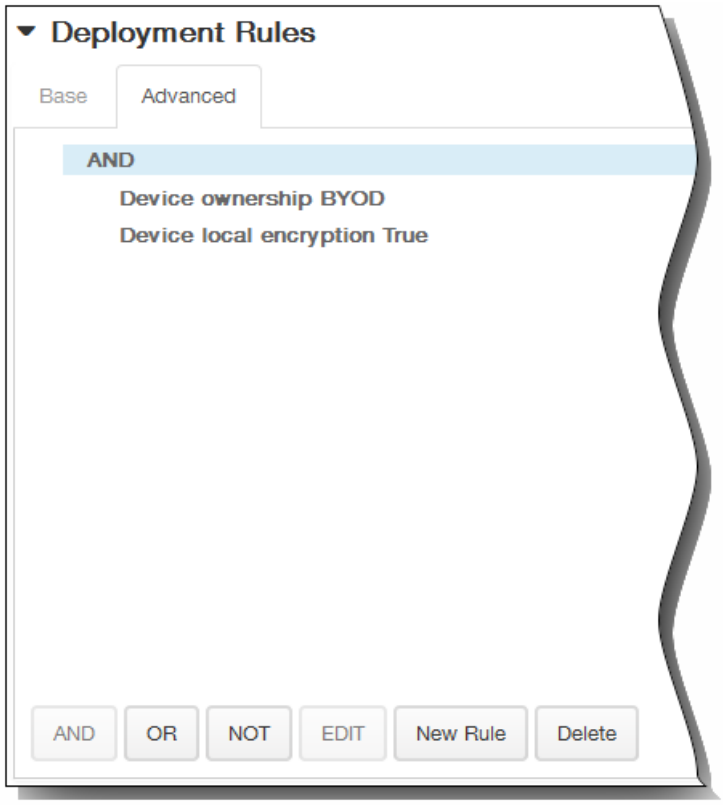
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
5. 单击下一步。 此时将显示策略平台页面。

   注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 Windows Phone 8.1 平台配置面板。



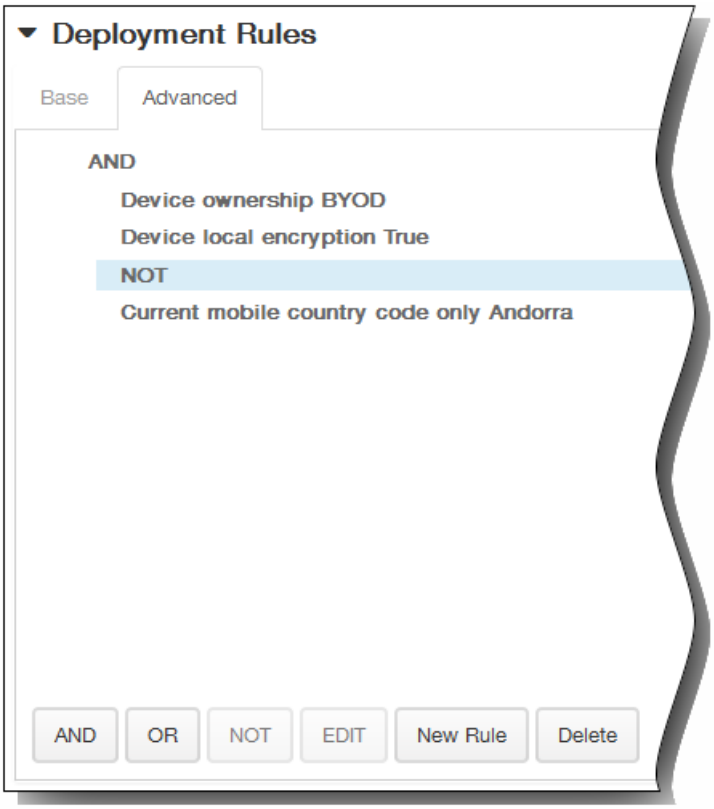
6. 在平台下面，确保只选中要添加的平台。
7. 在 XML 内容中，输入要向策略中添加的自定义 XML 代码。 如果内容太长，可以从源文件中剪切并复制该代码。
8. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。



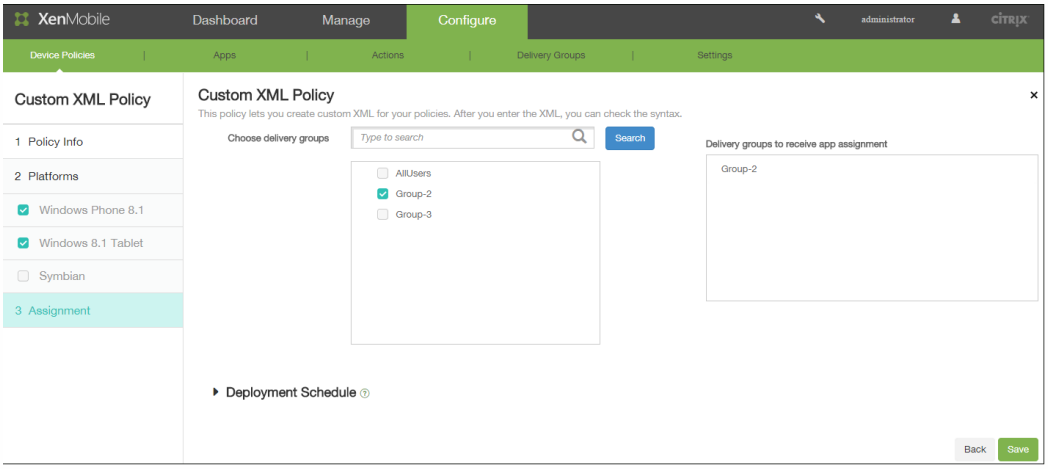
将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



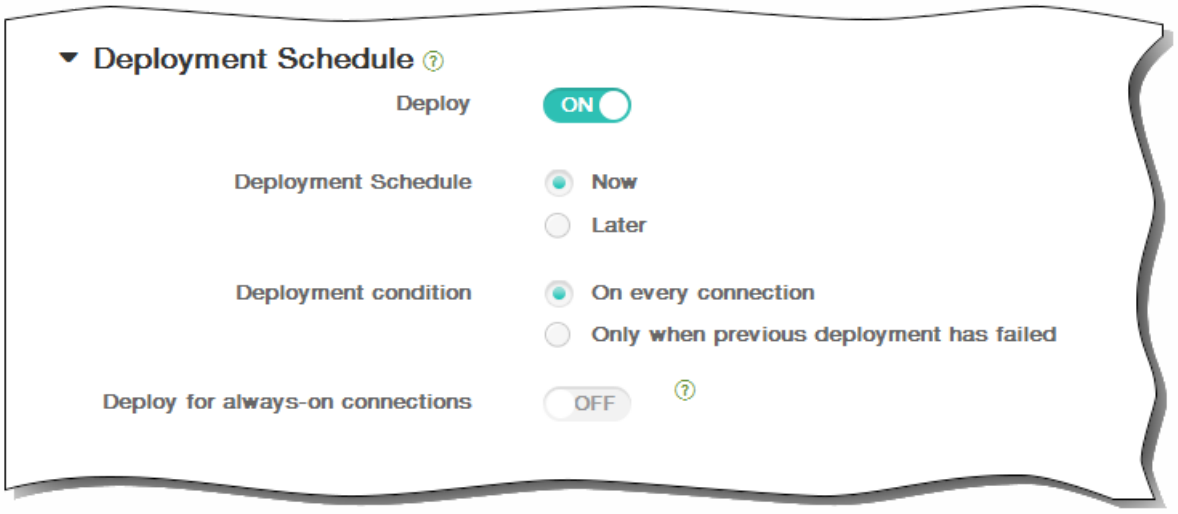
9. 单击下一步。 XenMobile 检查 XML 内容语法。内容框下将显示所有语法错误。必须先修复所有错误才能继续。
   如果没有语法错误，则将显示自定义 XML 策略分配页面。

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：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。

注意：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。



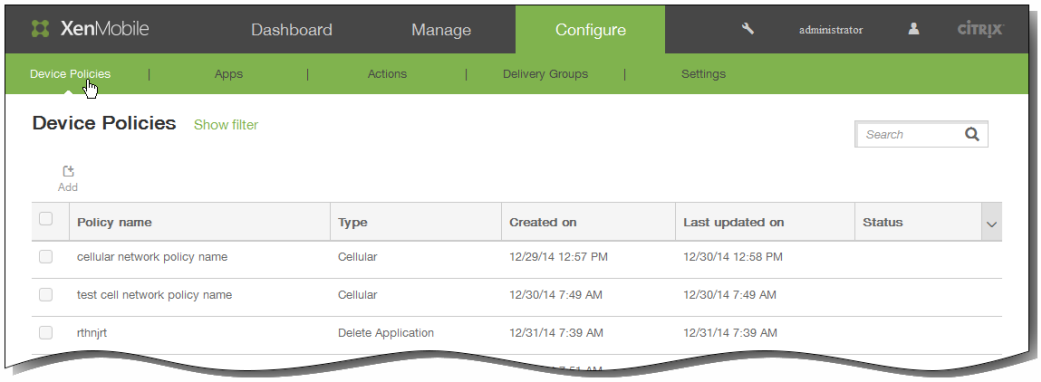
12. 单击保存以保存此策略。

应用程序卸载设备策略

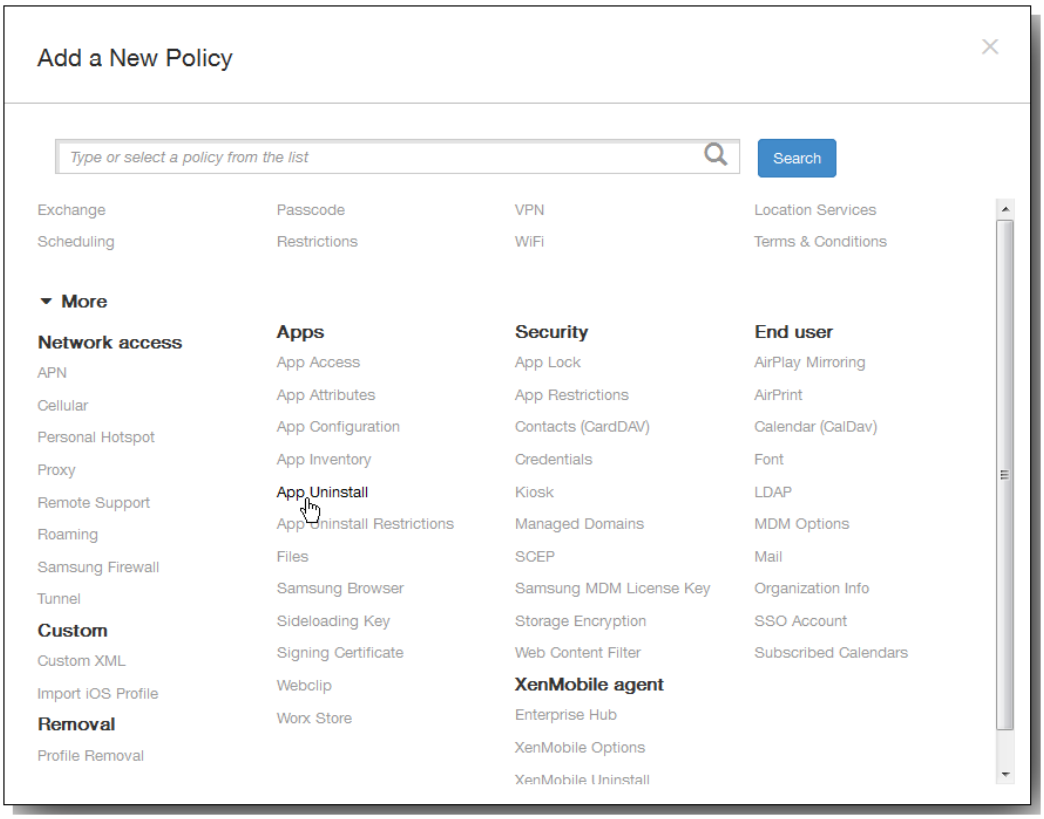
May 05, 2016

您可以为 iOS、Android、Samsung KNOX、和 Windows 8.1 Tablet 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。

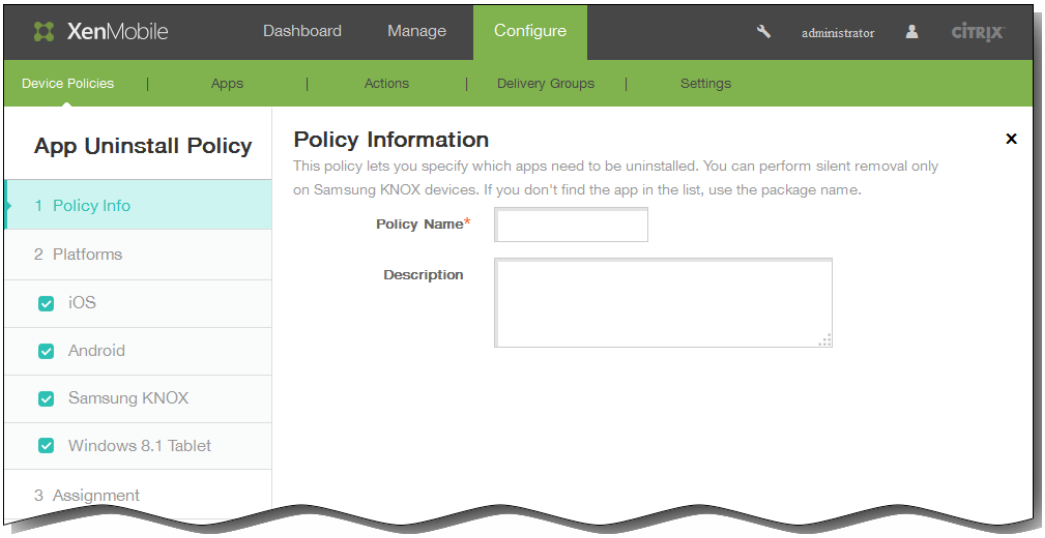
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。 在设备策略页面上，单击添加。



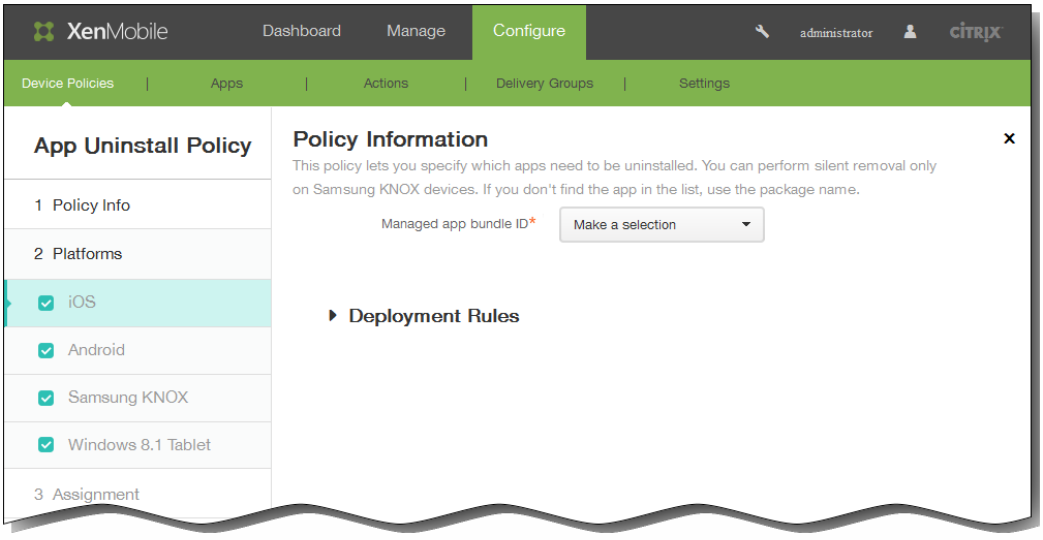
2. 在添加新策略对话框中，单击更多，然后在应用程序下面，单击应用程序卸载。



3. 在应用程序卸载策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
   3. 单击下一步。

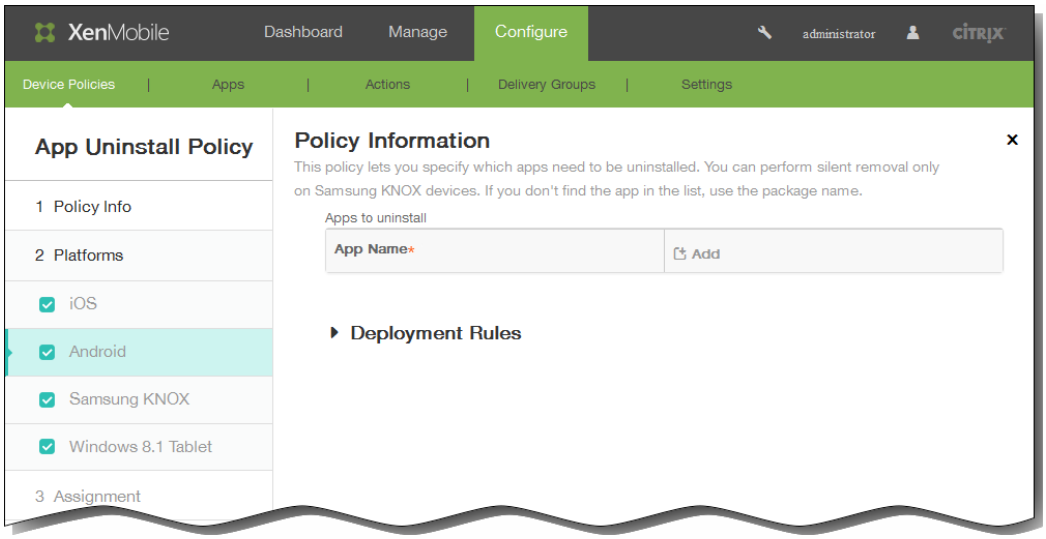


4. 策略平台页面显示时，所有平台都处于选中状态，您首先看到 iOS 平台配置面板。 在平台下面，选择要添加的一个或多个平台，并取消选择不想添加的平台。



5. 基于您选择的平台，进行以下设置配置。
   1. 如果选择了 iOS，在托管应用程序产品组合 ID 列表上，单击现有应用程序或单击新增。

      注意：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。
   2. 如果您选择 Android、Samsung KNOX 或 Windows 8.1 Tablet：

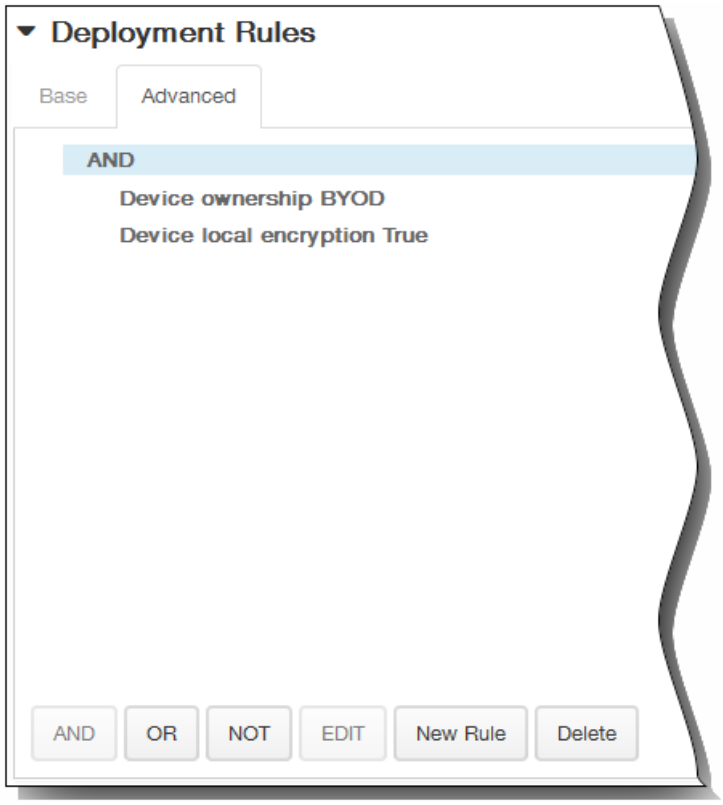


在要卸载的应用程序下面，单击添加，然后执行以下操作：

1. 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。
   注意：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。
2. 单击添加添加应用程序，或单击取消取消添加应用程序。
3. 为要添加的每个应用程序重复步骤 i.和 ii.。
   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。

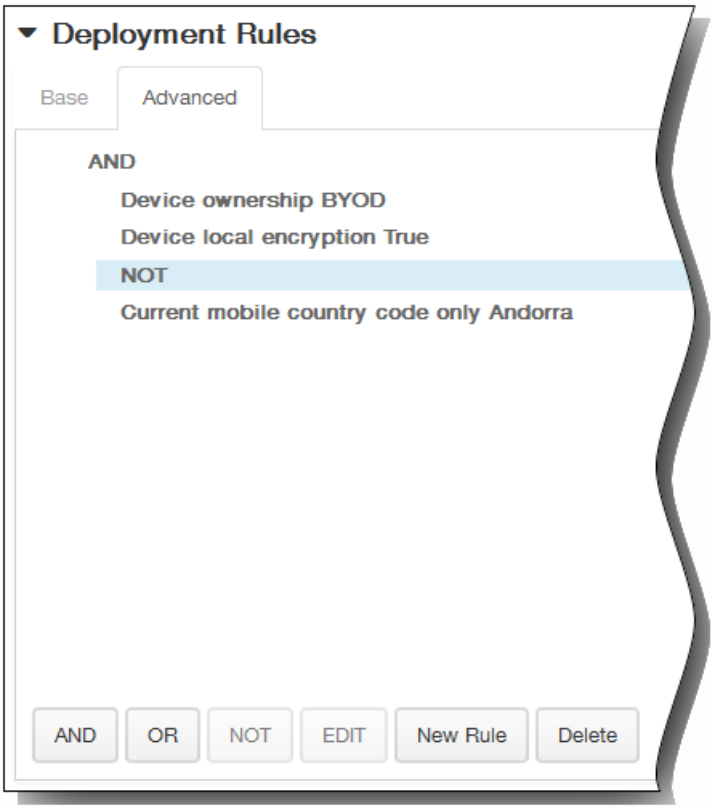
6. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

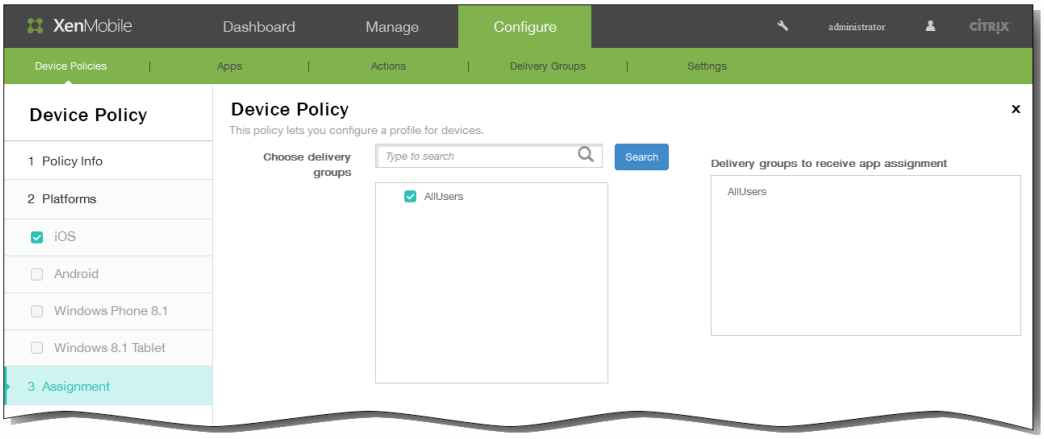


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。

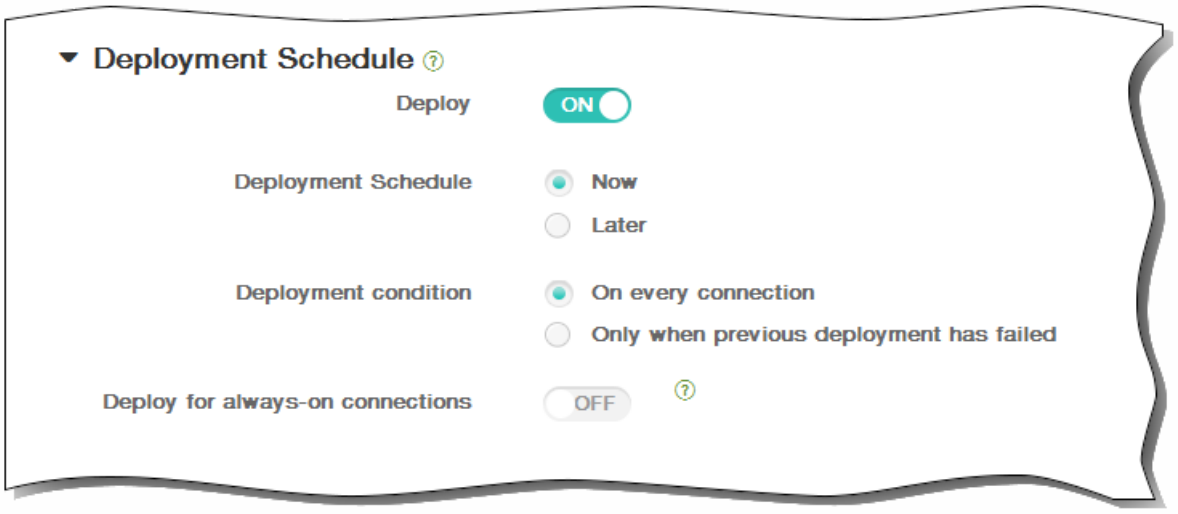


7. 单击下一步。 此时将显示应用程序卸载策略分配页面。
8. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。

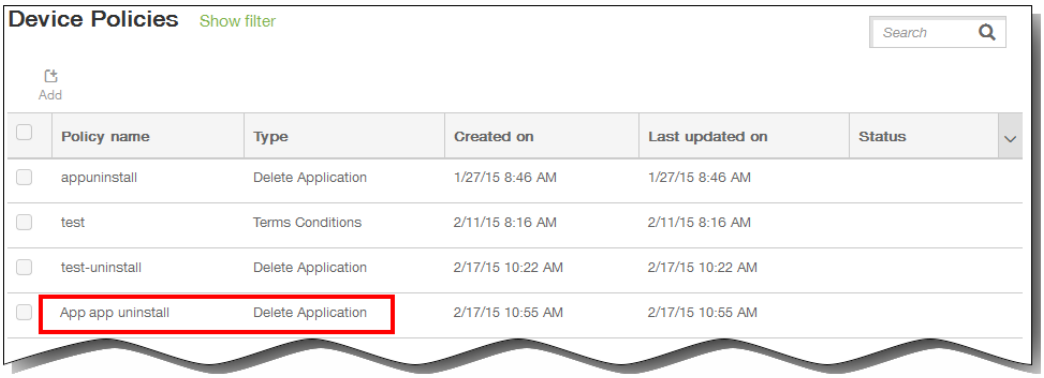


9. 展开部署计划，然后配置以下设置：
   1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。 如果选择关，无需配置其他选项。
   2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
   3. 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
   4. 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。 默认选项为每次连接时。
   5. 在为始终启用的连接部署旁边，单击开或关。 默认选项为关。
      注意：已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。

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。



10. 单击保存以保存此策略。 在设备策略页面上，类型列中列出了您已经作为“删除应用程序”类型添加的策略。

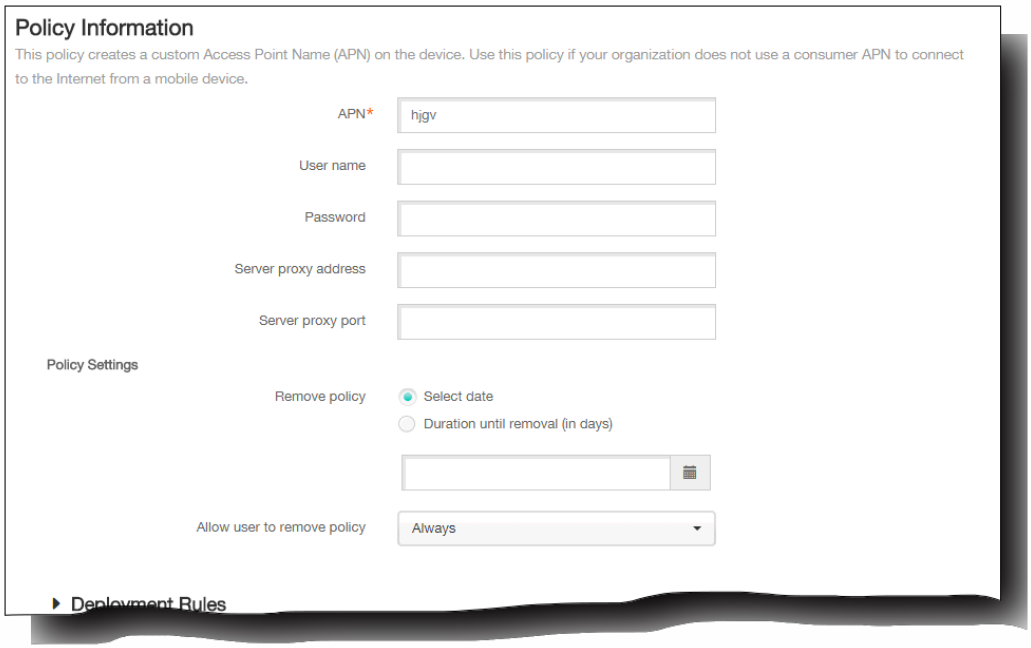


添加 APN 策略

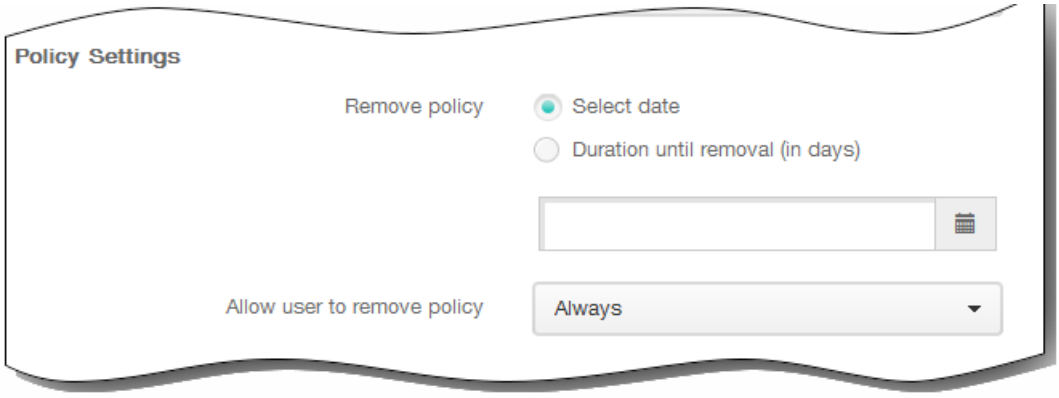
May 05, 2016

此策略允许您在 iOS、Android 或 Samsung KNOX 设备上配置自定义接入点名称 (APN)。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。

1. 在 XenMobile 控制台中，单击配置 > 设备策略 > 添加。
2. 在添加新策略页面上，单击更多，然后在网络访问权限下方，单击 APN。
3. 选择要包含在策略中的平台。 选定平台的配置页面显示在步骤 5 中。
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示首个平台信息页面。
6. 如果选择的是 iOS 平台，在“iOS 平台信息”页面上，执行以下操作：

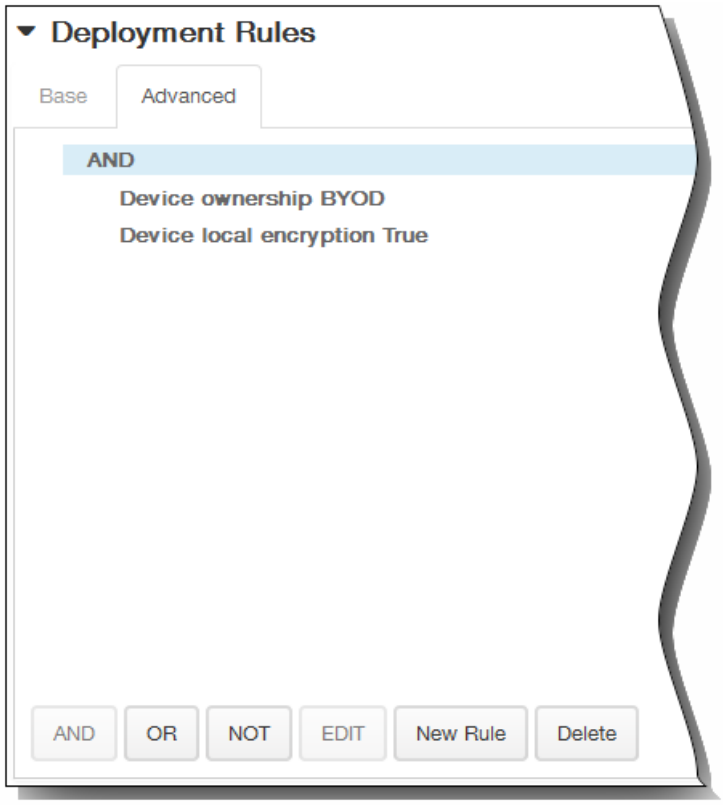


   1. APN。 输入接入点的名称。
   2. 用户名。 该字符串指定此 APN 的用户名。 如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
   3. 密码。 此 APN 的用户密码。 为进行混码处理，对密码进行了编码。 如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
   4. 服务器代理地址。 APN 代理的 IP 地址或 URL。
   5. 服务器代理端口。 APN 代理的端口号。
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



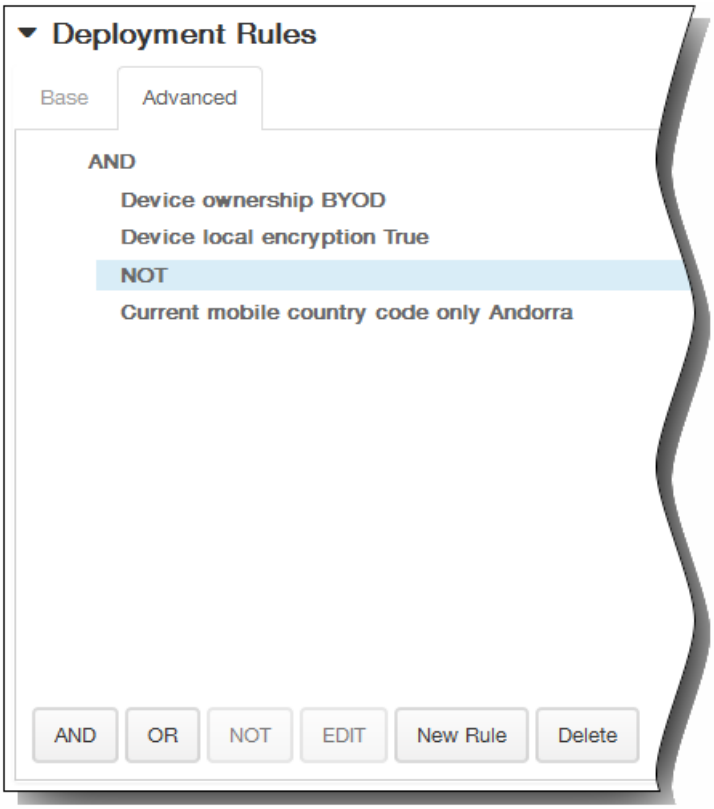
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

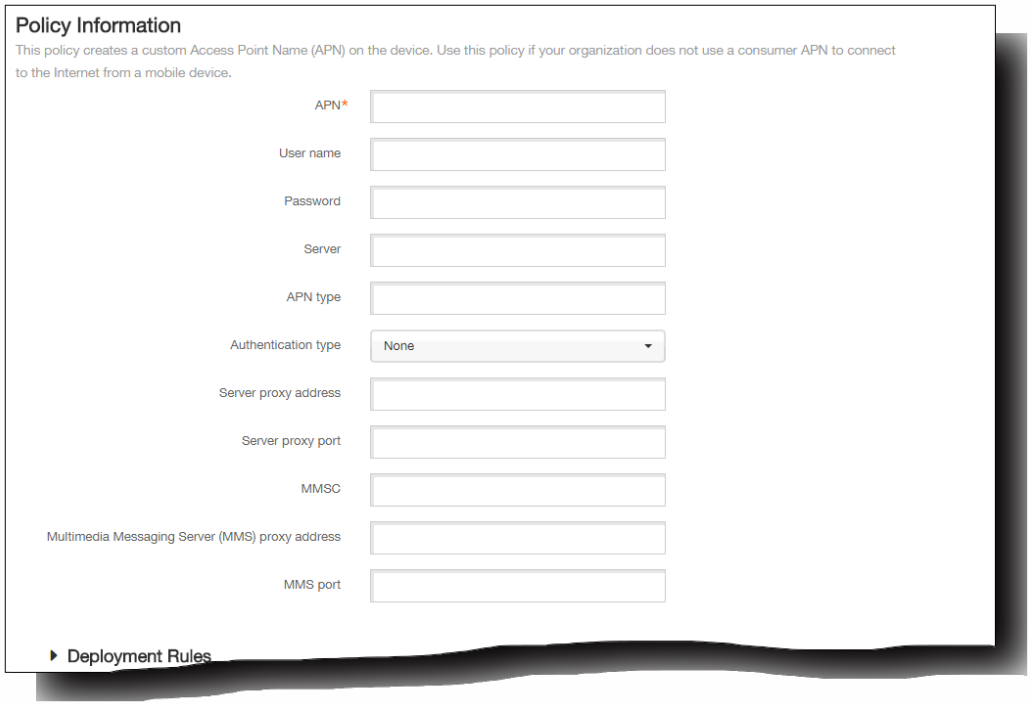


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



12. 如果选择的是 Android 或 Samsung KNOX 平台，在平台信息页面上，执行以下操作：

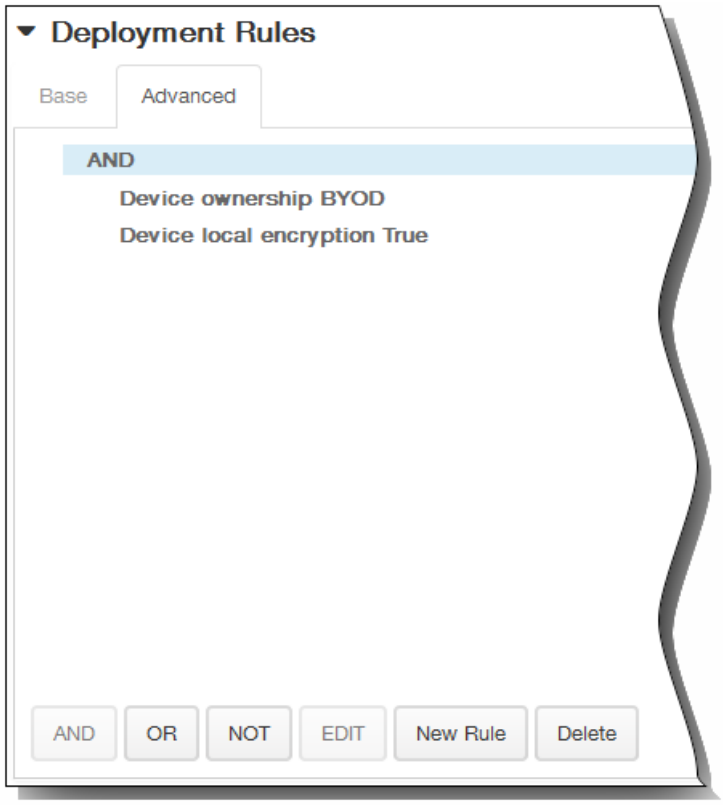


1. APN。 输入接入点的名称。
2. 用户名。 该字符串指定此 APN 的用户名。 如果用户名丢失，则在配置文件安装期间设备会提示该字符串。

3. 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。
4. 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。
5. 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。
6. 身份验证类型。 必须包含 PAP、CHAP 或 PAP 或 CHAP。 默认为无。
7. 服务器代理地址。 APN 代理的 IP 地址或 URL。
8. 服务器代理端口。 APN 代理的端口号。
9. MMSC。 用于 MMS 流量的多媒体消息服务服务器。 MMS 使得 SMS 可以发送包含多媒体内容（如图片或视频）的大型消息。 这些服务器需要特定的协议（如 MM1、... MM11）。
10. 多媒体消息服务 (MMS) 代理地址。 用于 MMS 流量的 HTTP 代理服务器。
11. MMS 端口。 MMS 代理使用的端口。

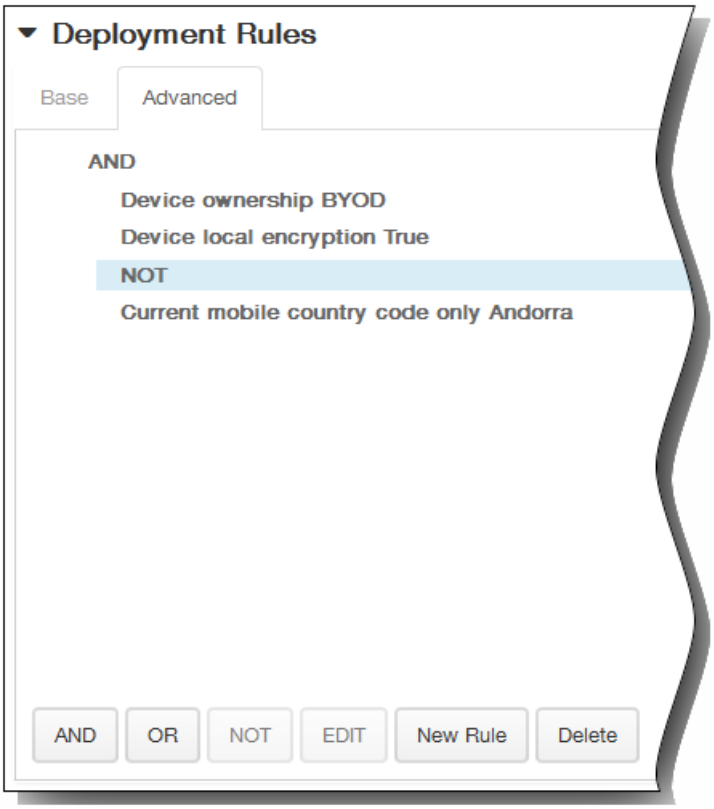
13. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

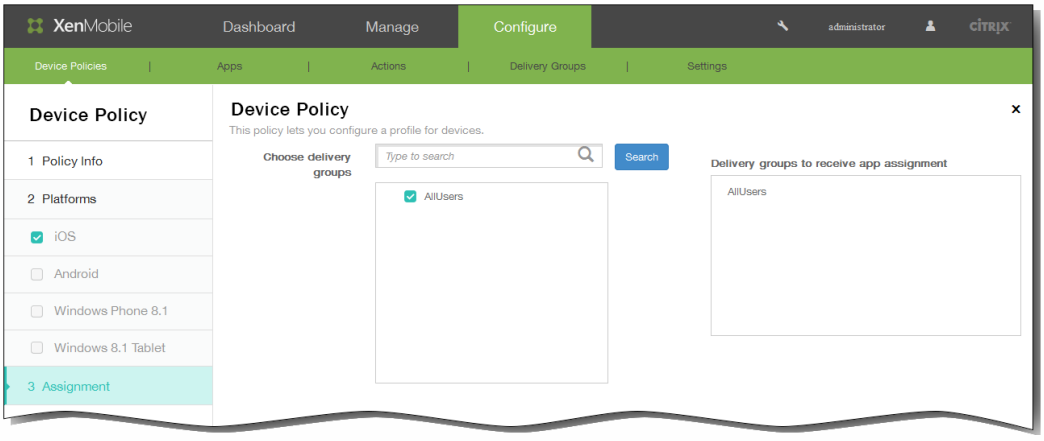


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



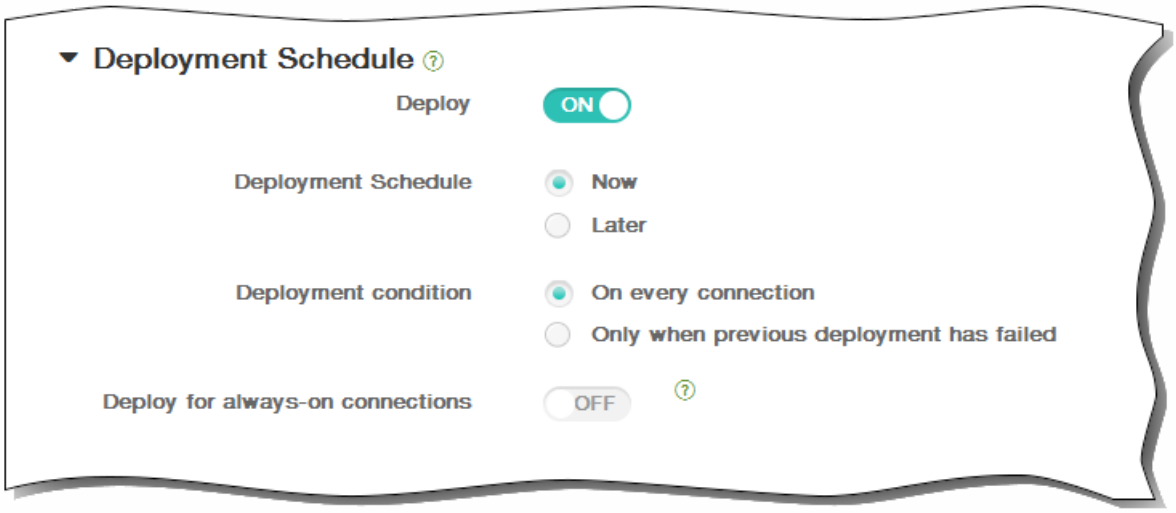
14. 如果选择 Android 或 Samsung KNOX 平台，请重复步骤 8 以完成 Samsung KNOX 平台信息页面，然后单击下一步。 此时将显示 APN 策略分配页面。
15. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



16. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



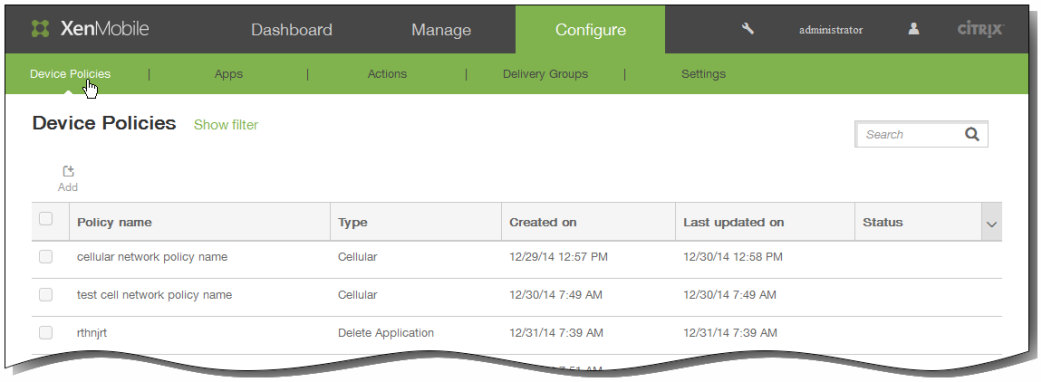
17. 单击保存以保存此策略。

添加适用于 iOS 的手机网络设备策略

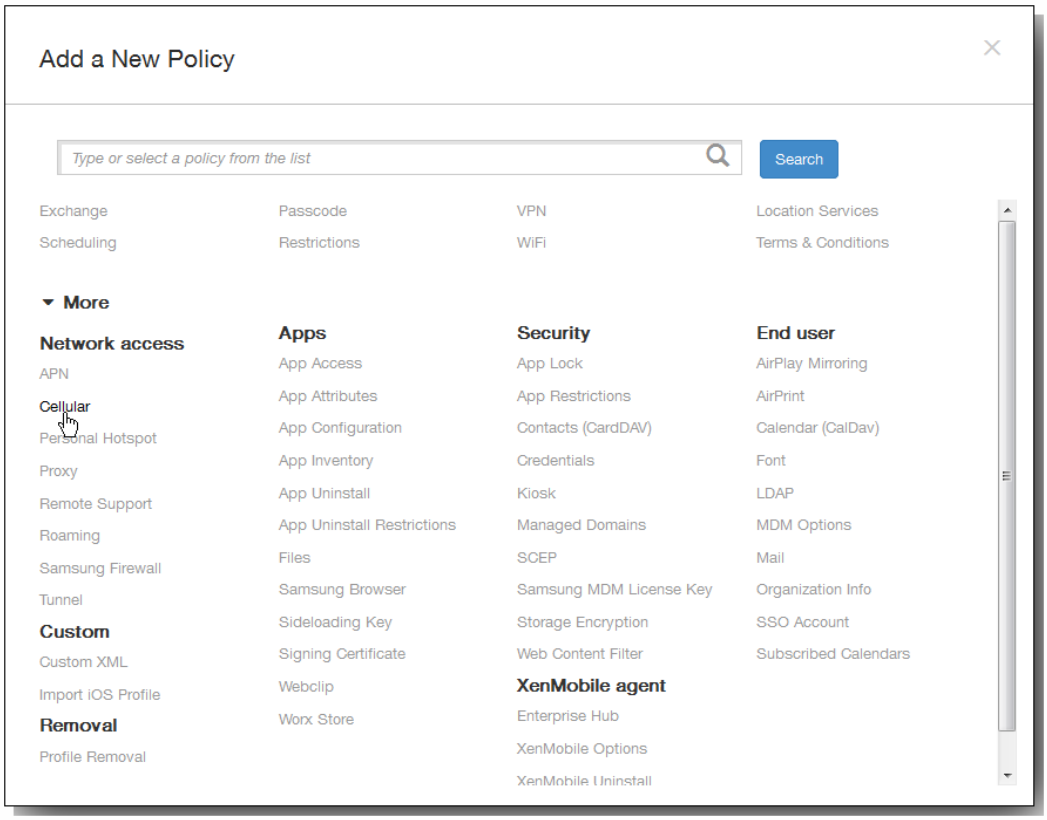
May 05, 2016

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。

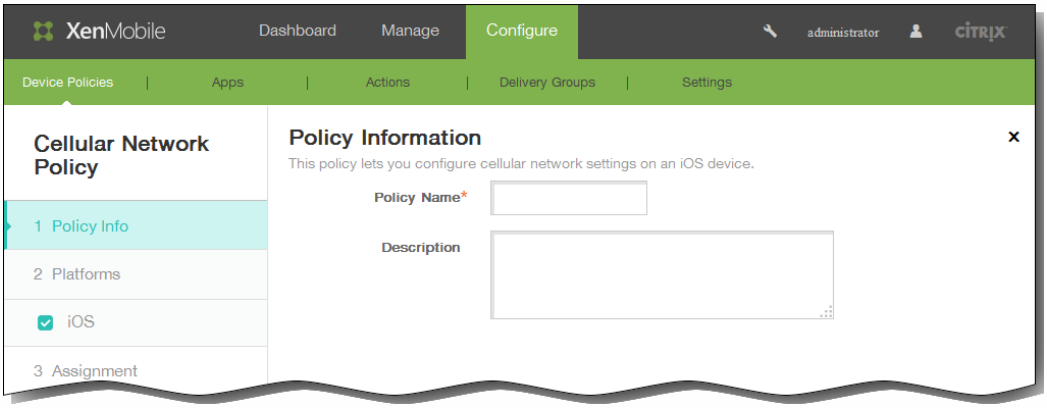


2. 单击添加。
   将显示添加新策略页面。

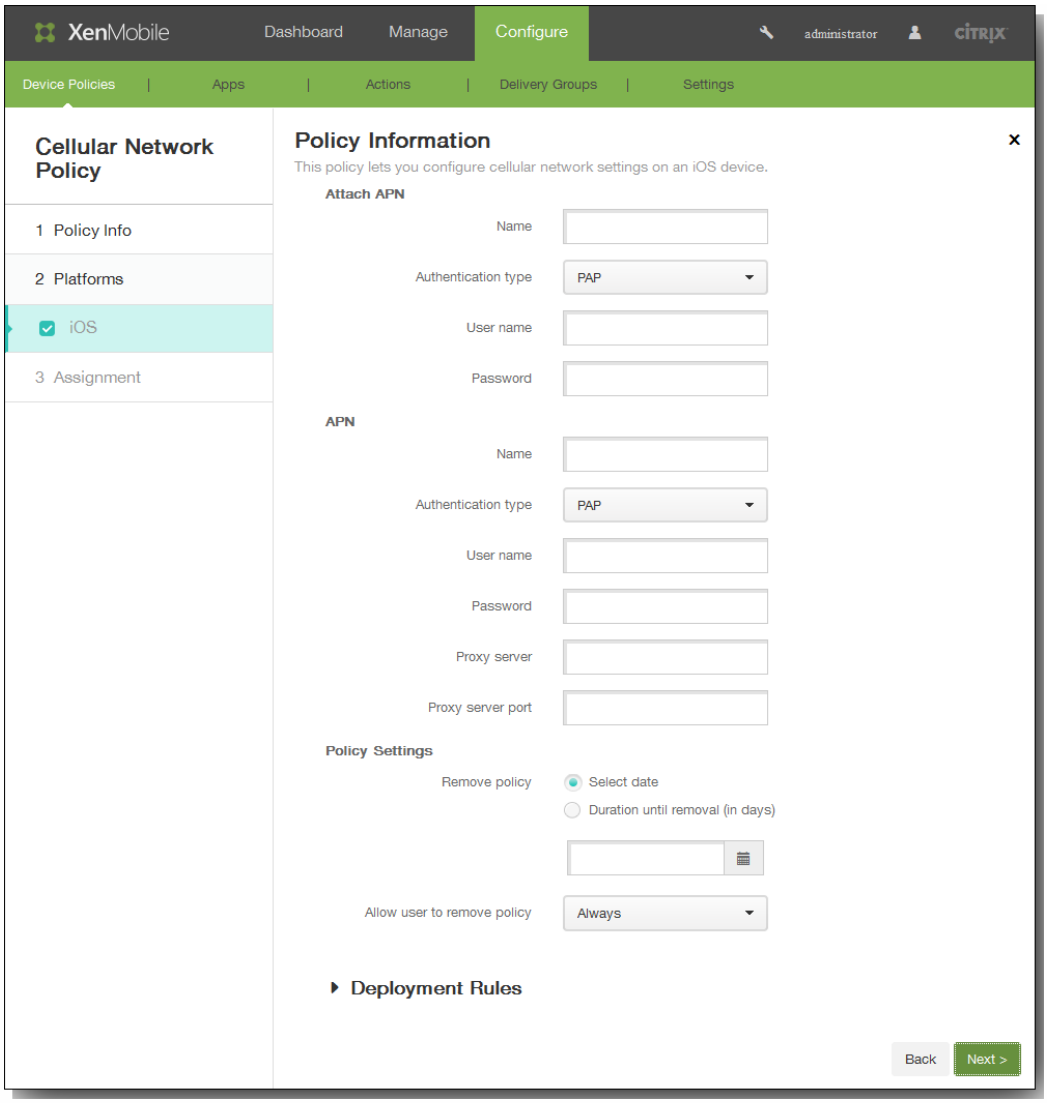


3. 在添加新策略页面上，单击更多，然后在网络访问下方，单击手机网络。

此时将显示手机网络策略信息页面出现。

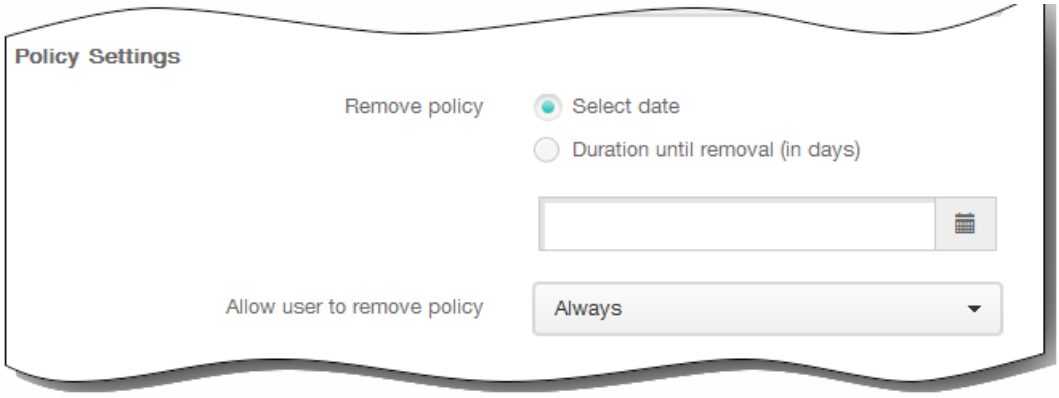


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。

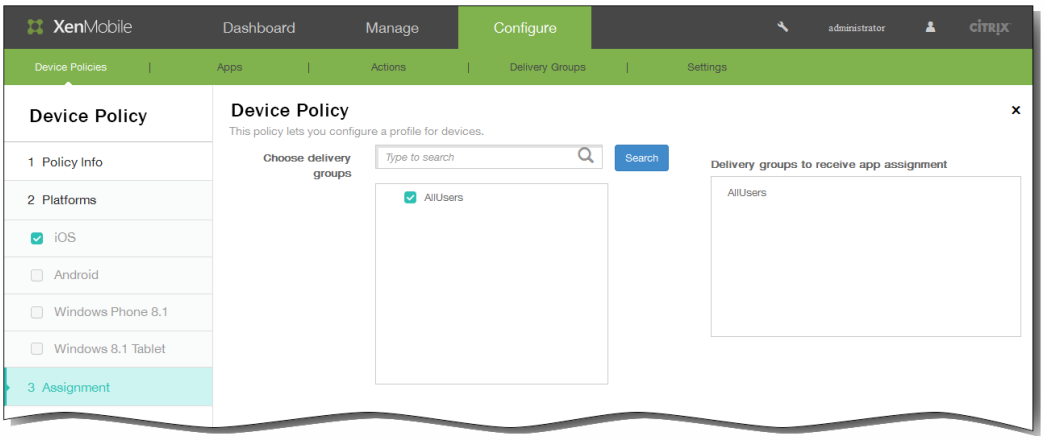


6. 在 iOS 平台信息页面上，输入以下信息：在**附加 APN** 下面：
   1. 名称：键入此配置的名称。
   2. 身份验证类型：在清单上，单击质询握手身份验证协议 (CHAP) 或密码身份验证协议 (PAP)。 默认值为 PAP。
   3. 用户名：键入用于身份验证的用户名。
   4. 密码：键入用于身份验证的密码。

   在 **APN** 下面：
   1. 名称：键入访问点名称 (APN) 配置的名称。
   2. 身份验证类型：在列表中，单击 CHAP 或 PAP。 默认值为 PAP。
   3. 用户名：键入用于身份验证的用户名。
   4. 密码：键入用于身份验证的密码。
   5. 代理服务器：键入代理服务器网络地址。
   6. 代理服务器端口：键入代理服务器端口。
7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



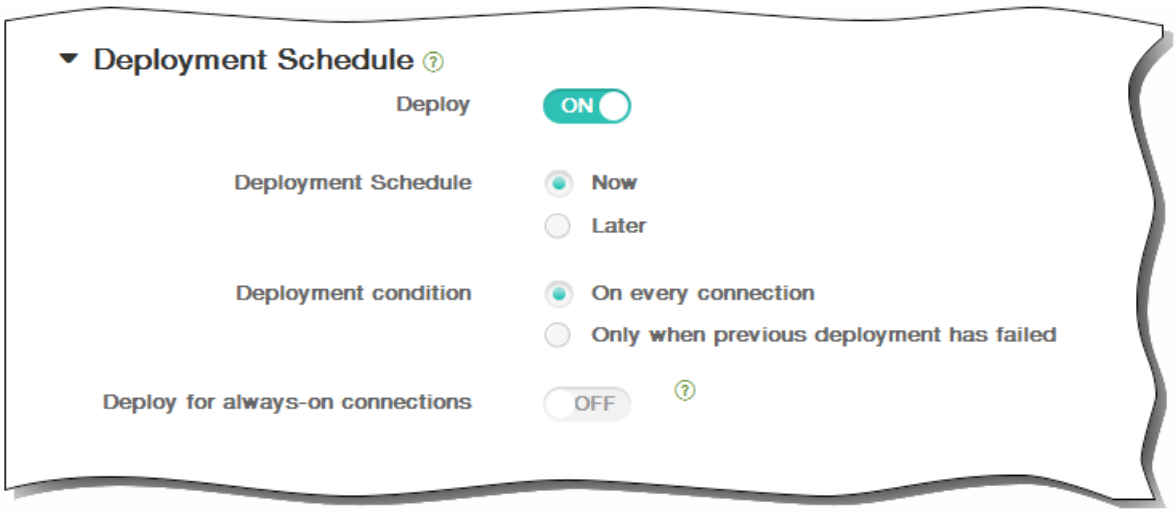
11. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



12. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



13. 单击保存以保存此策略。

为 Windows Phone 8.1 添加企业 Hub 设备策略

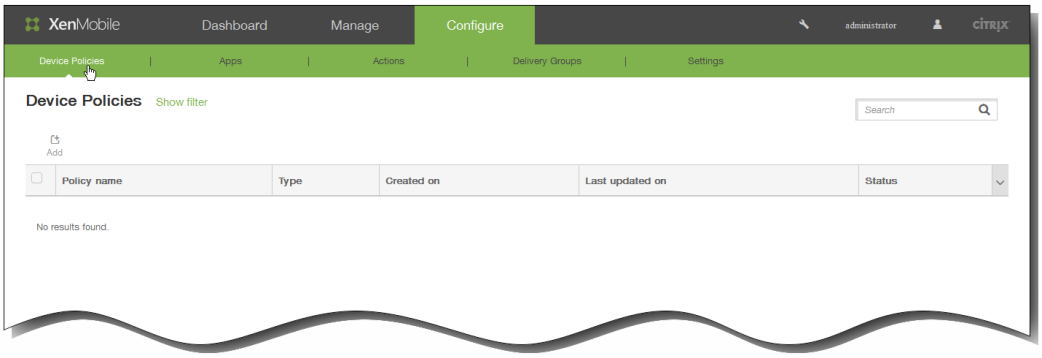
May 05, 2016

面向 Windows Phone 8.1 的企业 Hub 设备策略允许您通过企业 Hub 公司应用商店分发应用程序。

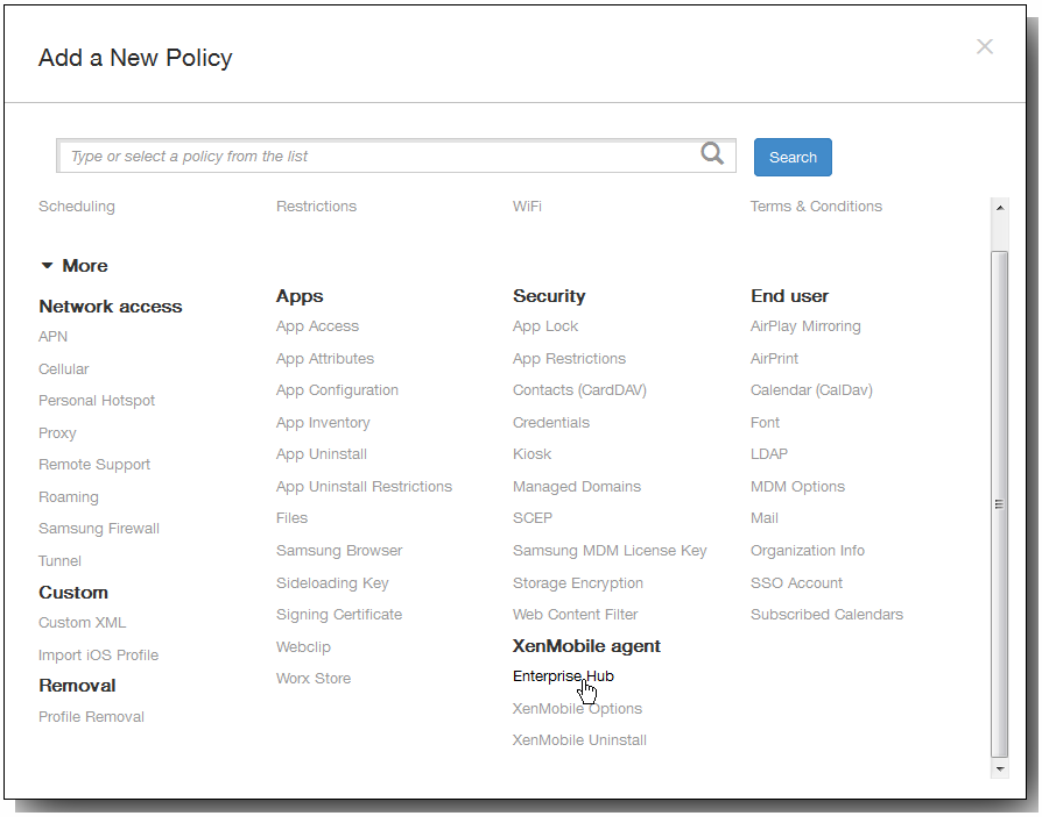
需要具备以下各项才能创建策略：

- 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

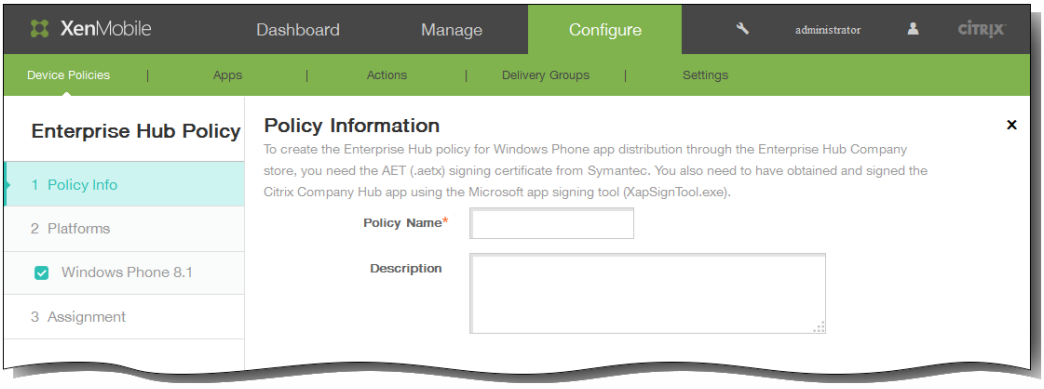
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



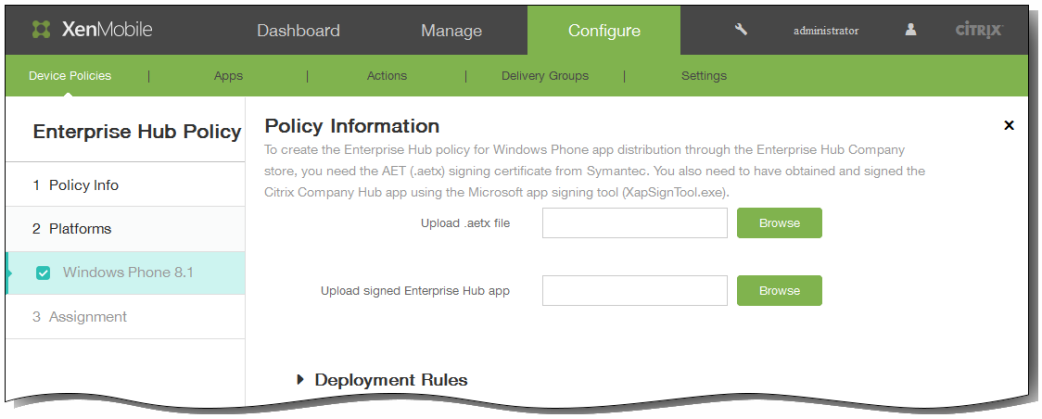
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在 XenMobile Agent 下单击企业 Hub。 此时将显示企业 Hub 策略页面。

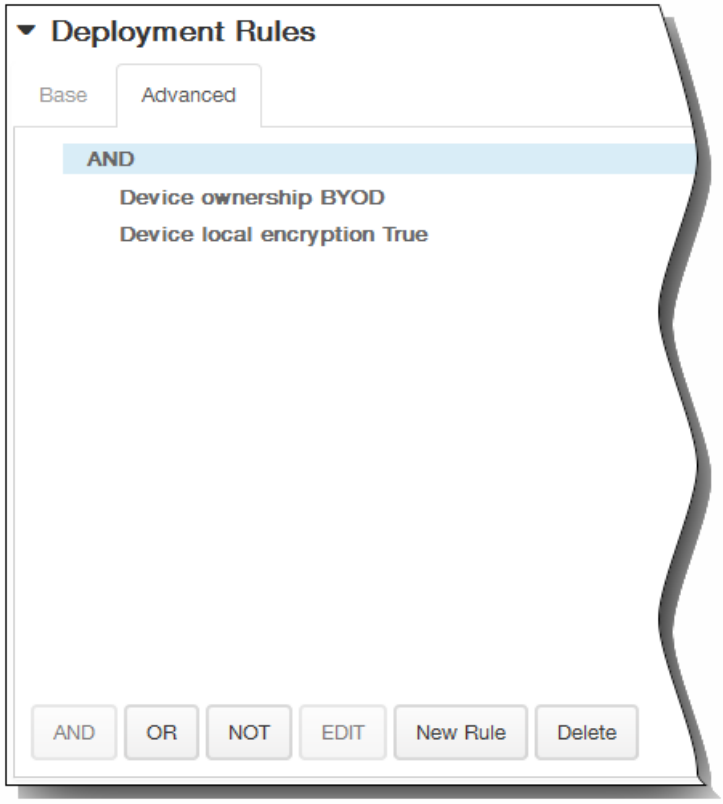


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：输入策略的描述性名称。
   2. 说明：如有需要，请输入策略的说明。
5. 单击下一步。 此时将显示 Windows Phone 8.1 平台页面。



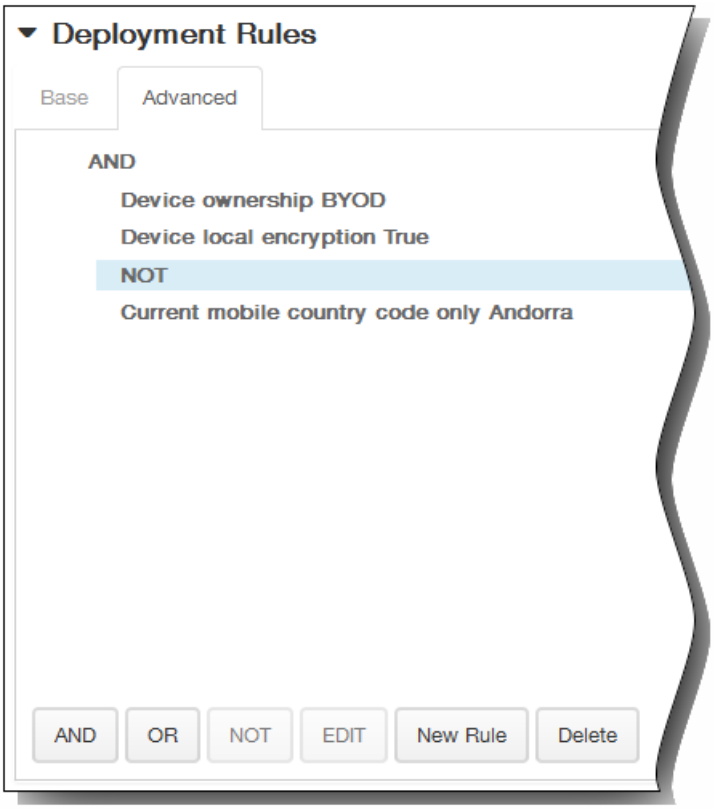
6. 配置以下设置：
   1. Upload .aetx file（上载 .aetx 文件）：浏览到 .aetx 文件所在的位置，然后选择该文件。
   2. Upload signed Enterprise Hub app（上载签名的企业 Hub 应用程序）：浏览到企业 Hub 应用程序所在的位置，然后选择该应用程序。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

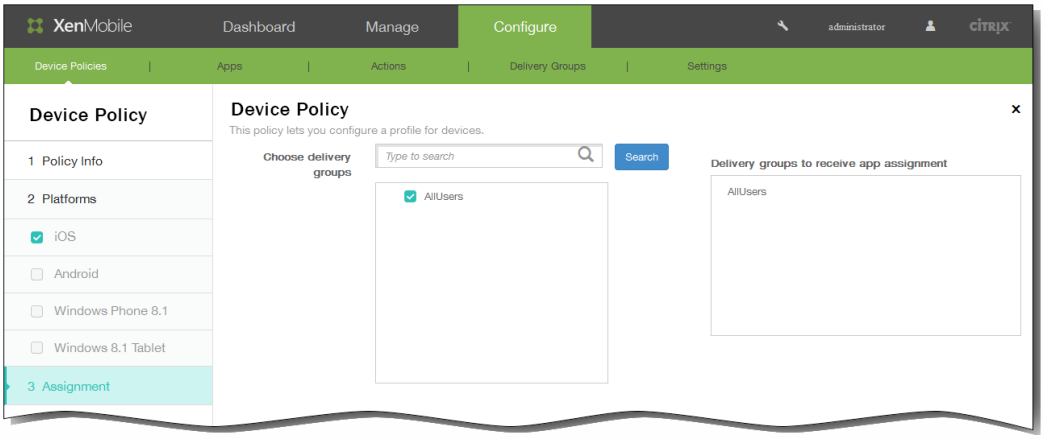


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



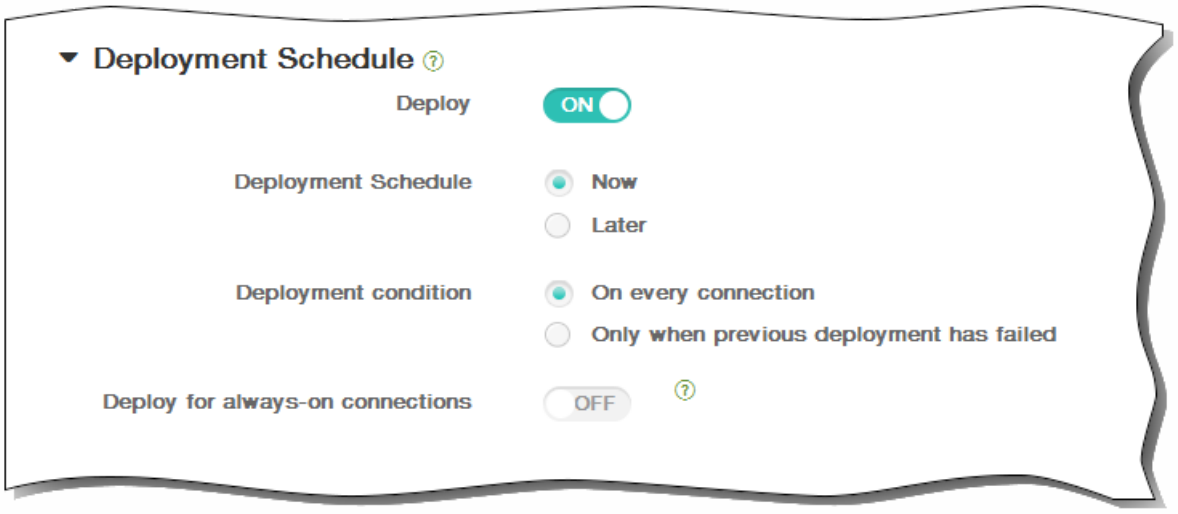
8. 单击下一步。 此时将显示 Enterprise Hub Policy（企业 Hub 策略）分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

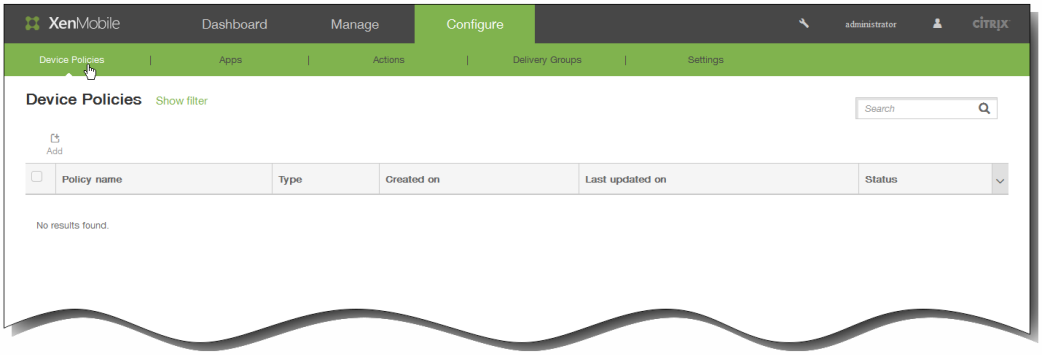
Microsoft Exchange ActiveSync 设备策略

May 05, 2016

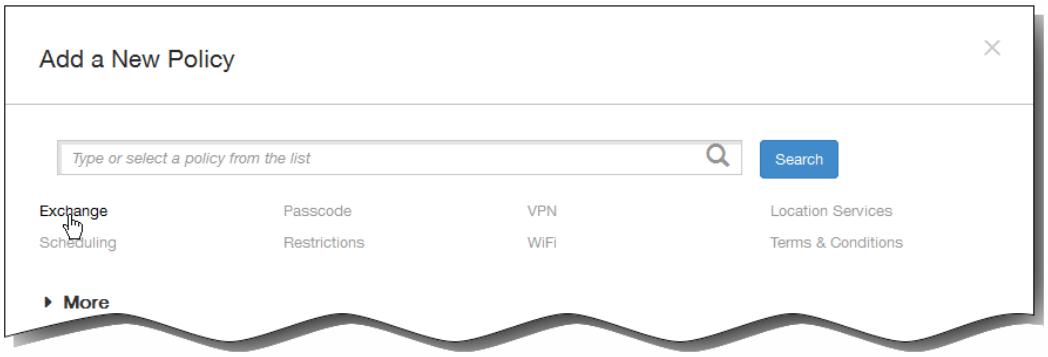
可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以允许其访问 Exchange 上托管的企业电子邮件。可以为 iOS、Android HTC、Android TouchDown、Samsung SAFE、Samsung KNOX 和 Windows Phone 8.1 创建策略。每个平台都需要一组不同的值，这些值将在以下主题中详细说明：

在可以创建此策略之前，您需要知晓 Exchange Server 的主机名或 IP 地址。

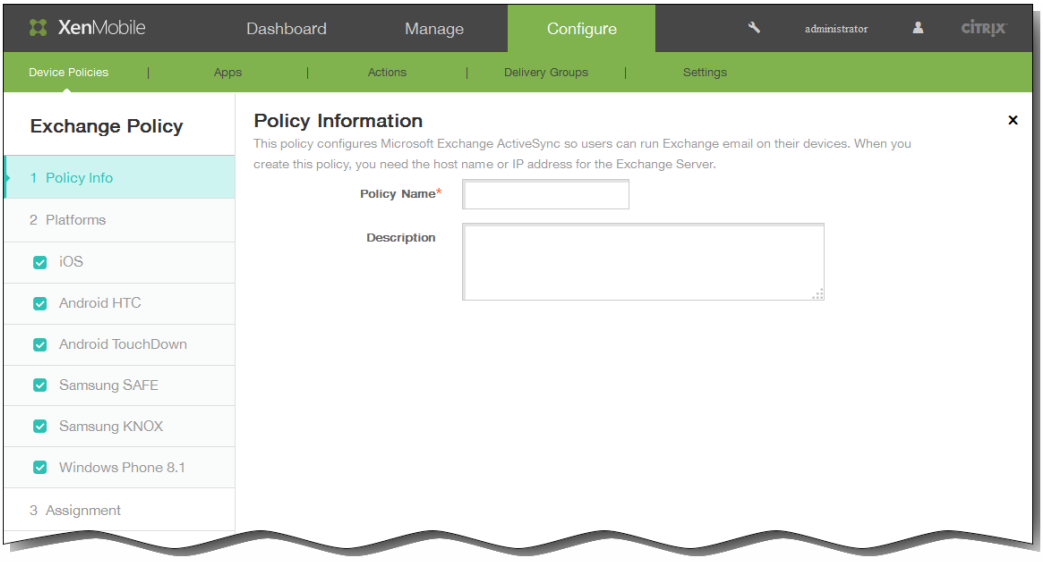
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



2. 单击添加添加新策略。 此时将显示添加新策略对话框。

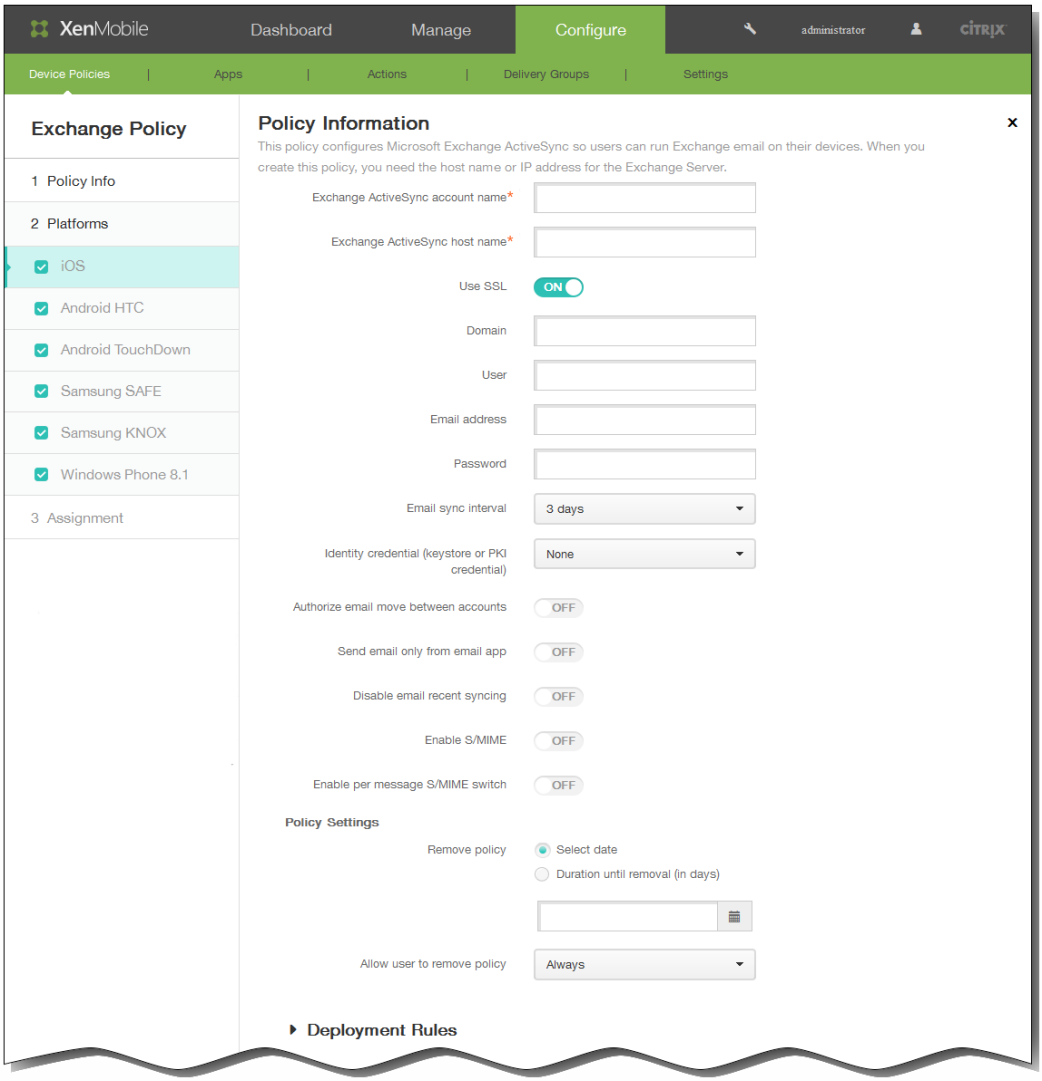


3. 单击 Exchange。 此时将显示 Exchange 策略信息页面。



4. 在策略信息窗格中，键入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。

   注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 iOS 平台配置面板。



6. 在平台下面，选择要添加的一个或多个平台。
   - 如果选择 iOS，可以配置以下设置：

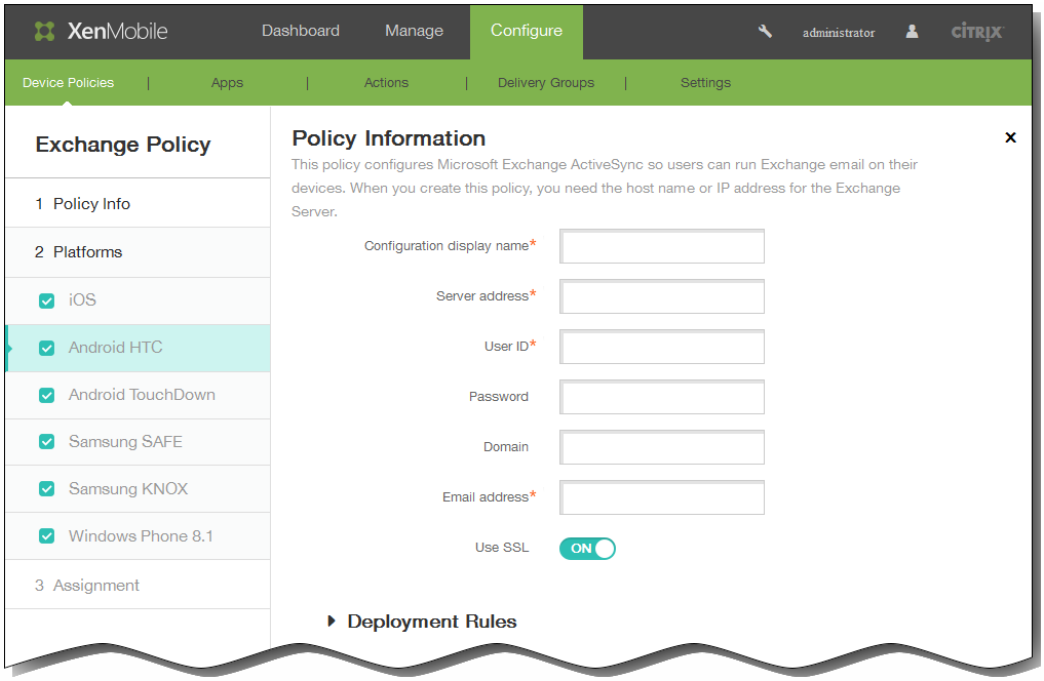
     配置显示名称：为此策略键入要在用户设备上显示的名称。

     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。
     注意：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。
     注意：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。
     注意：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。

   - 如果选择 Android HTC，可以配置以下设置：



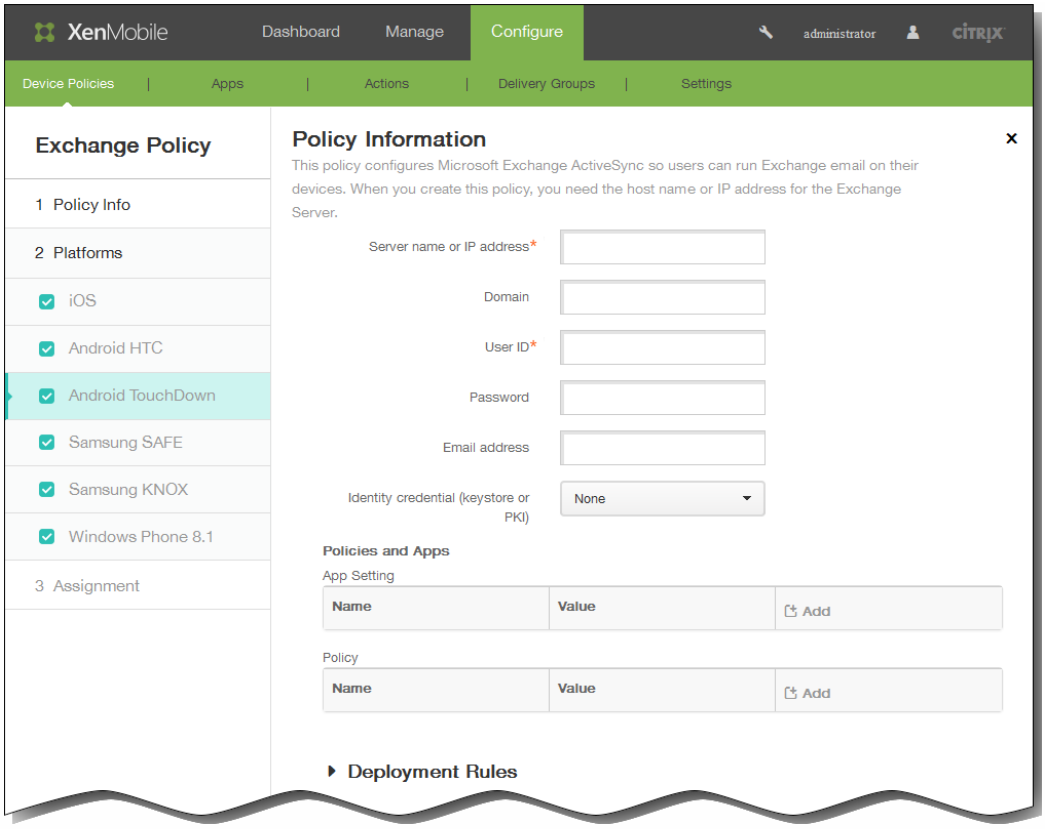
配置显示名称：为此策略键入要在用户设备上显示的名称。

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。
注意：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。
注意：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。
注意：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。

- 如果选择 Android TouchDown，可以配置以下设置：



服务器名称或 IP 地址：键入 Exchange Server 的主机名或 IP 地址。

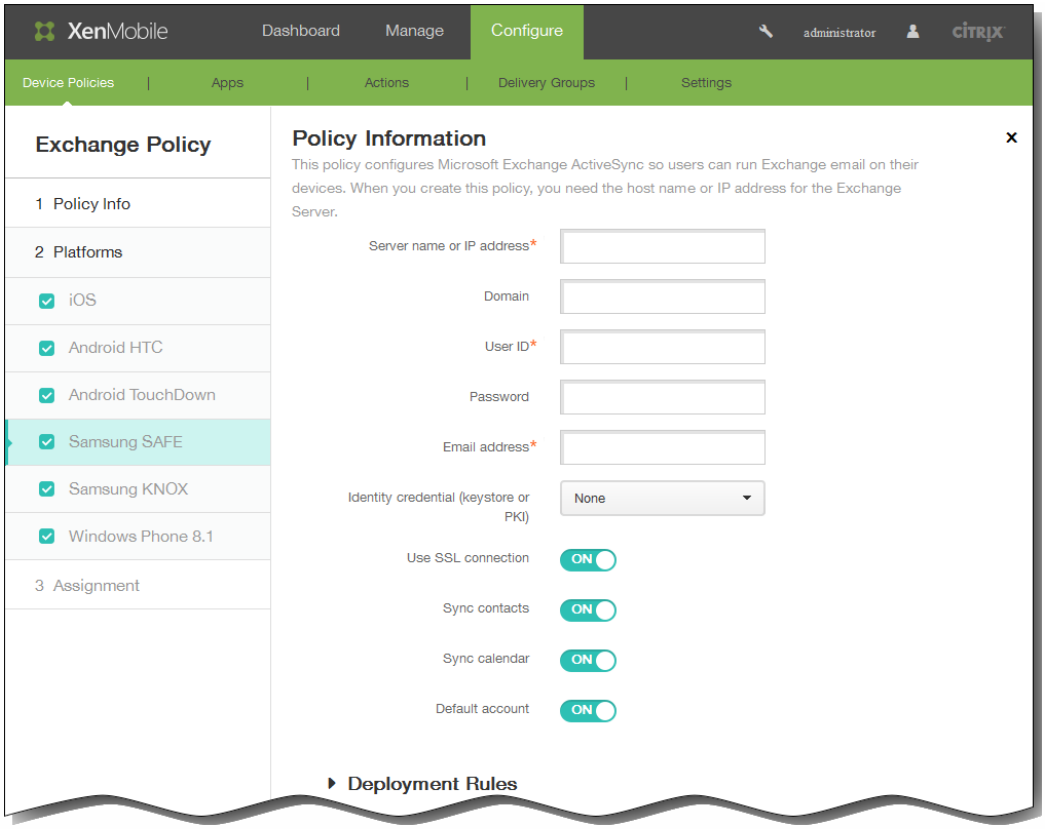
域：键入 Exchange Server 所在的域。
注意：可以在此字段中使用系统宏 ${user.domainname} 自动查找用户的域名。
用户 ID：指定 Exchange 用户帐户的用户名。
注意：可以在此字段中使用系统宏 ${user.username} 自动查找用户的名称。
密码：键入 Exchange 用户帐户的可选密码。

电子邮件地址：指定用户的完整电子邮件地址。
注意：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。

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。

- 如果选择 Samsung SAFE 或 Samsung KNOX，可以配置以下设置：



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。
注意：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。
注意：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。
注意：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。

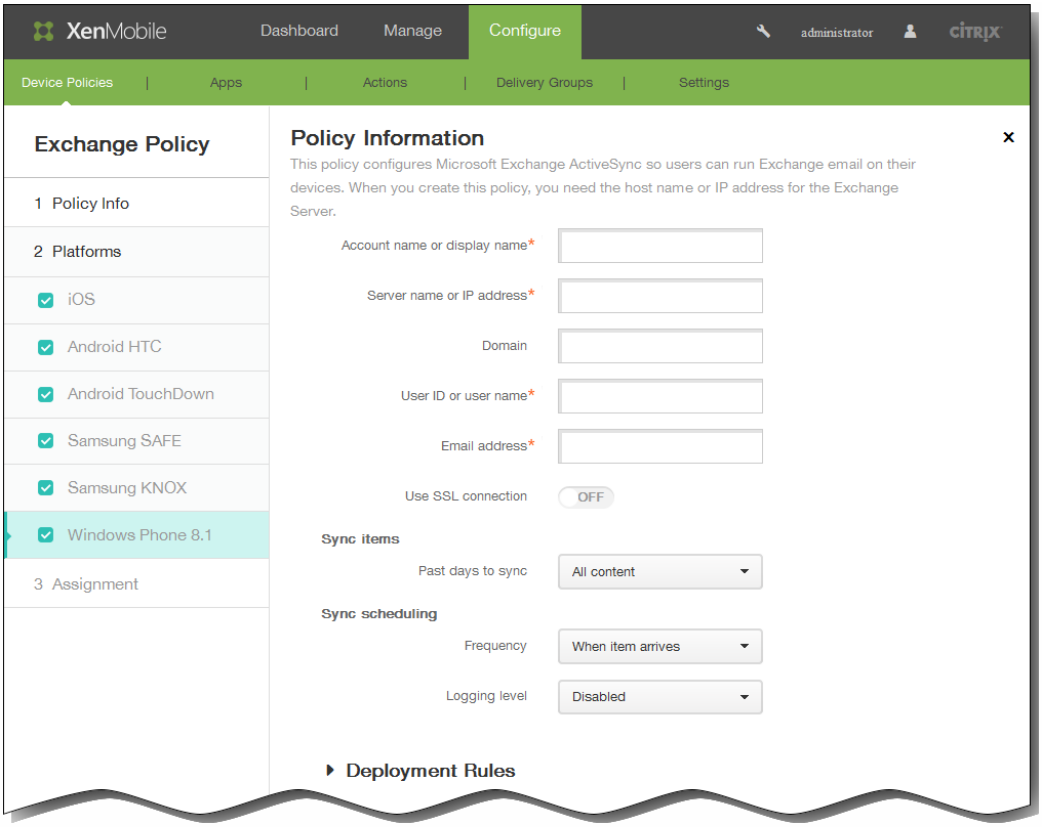
同步联系人：选择是否在用户设备与 Exchange Server 之间启用用户联系人的同步。默认值为开。

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 帐户设置为默认帐户，用于从其设备发送电子邮件。默认值为开。

- 如果选择 Windows Phone 8.1，可以配置以下设置：

  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。
注意：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。
注意：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。
注意：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。

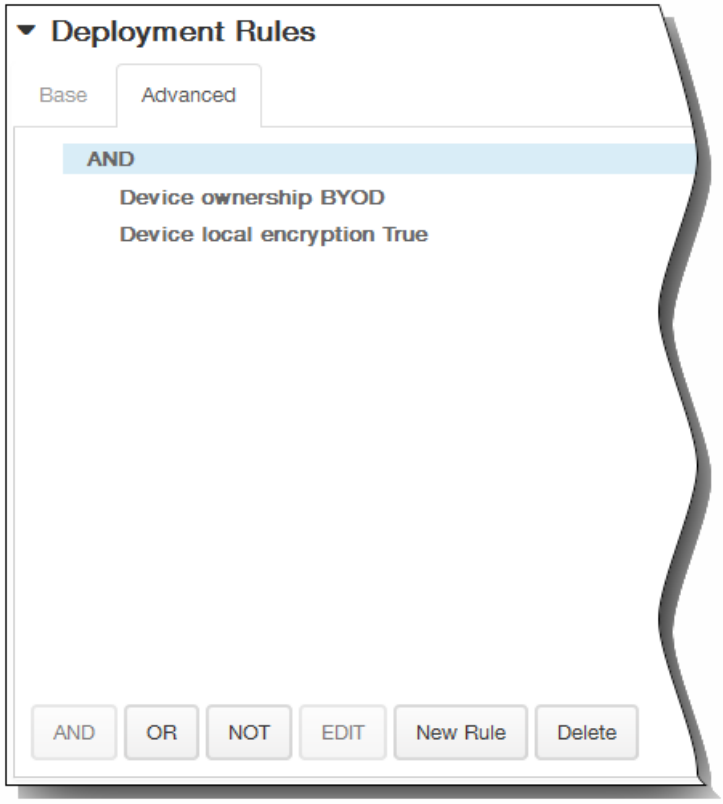
同步内容天数：在列表中，请单击要将设备上过去多少天内的所有内容与 Exchange Server 同步。

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。

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。

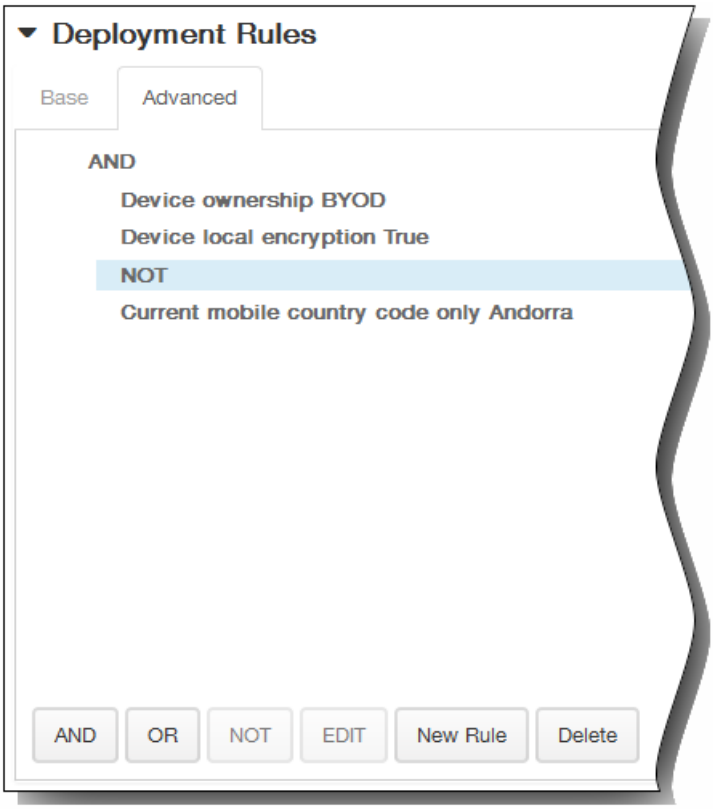
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

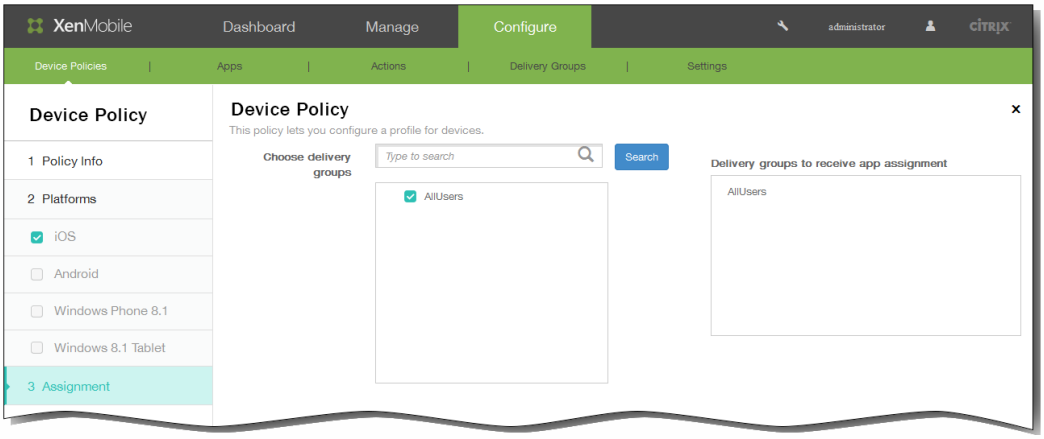


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。

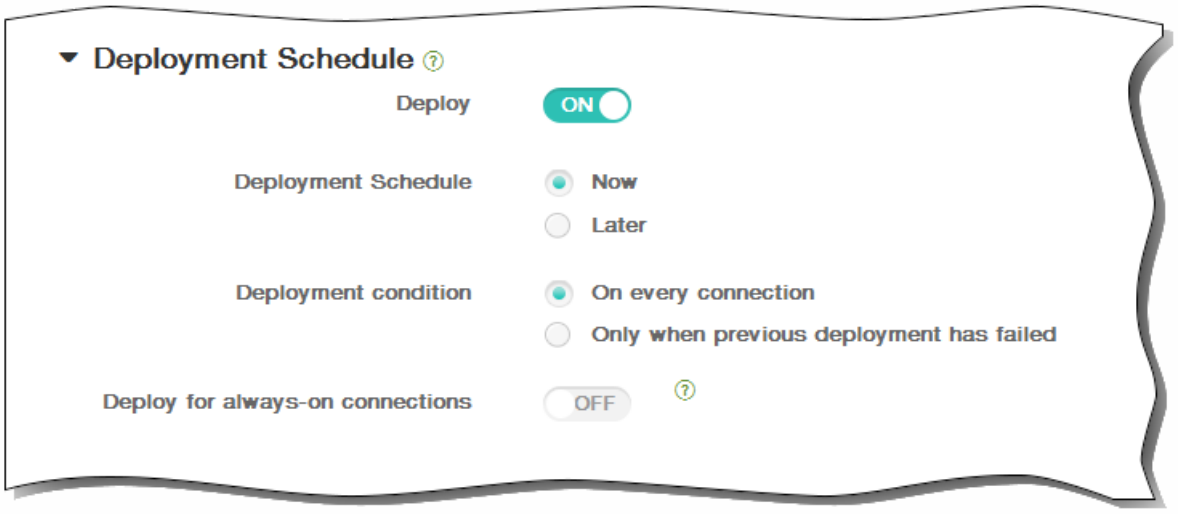


8. 单击下一步。 此时将显示 Exchange 策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存。

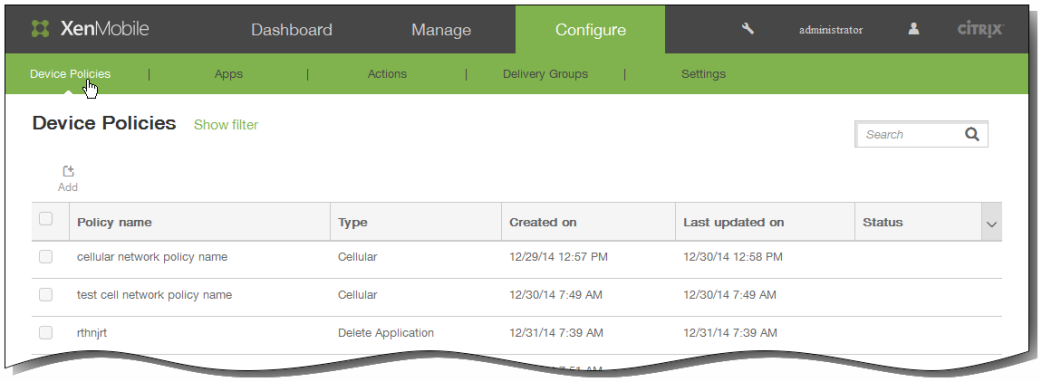
定位设备策略

May 05, 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。

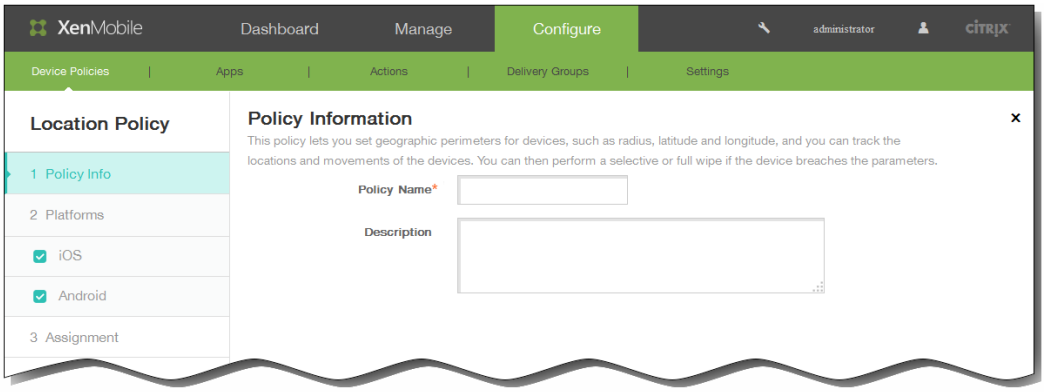
可以为 iOS 和 Android 创建定位设备策略。每种平台需要一组不同的值，本文将对此进行介绍。

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。

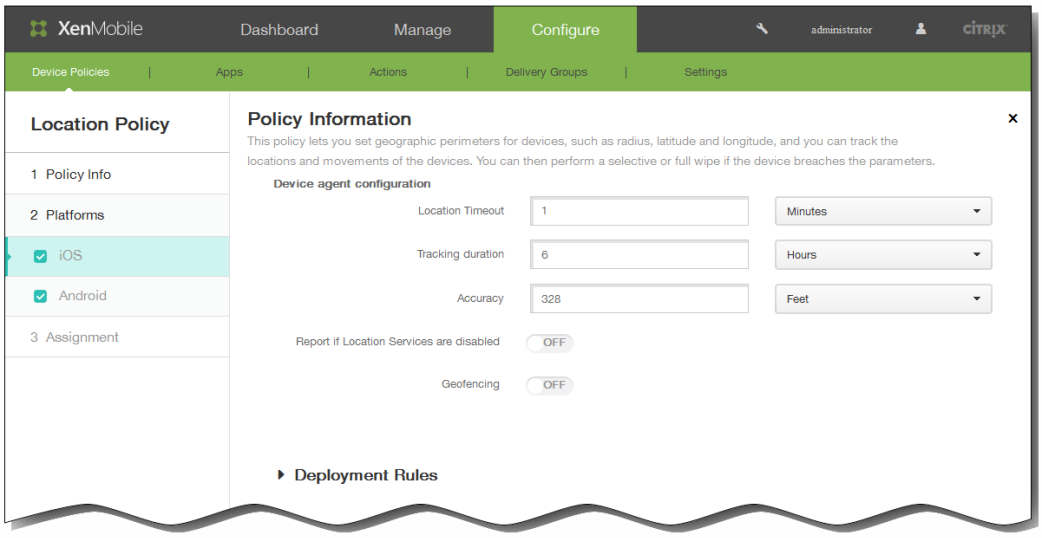


2. 单击添加添加新策略。 此时将显示添加新策略对话框。

3. 单击定位服务。 此时将显示定位策略信息页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。
   注意：策略平台页面显示时，两个平台都处于选中状态，您首先看到 iOS 平台配置面板。



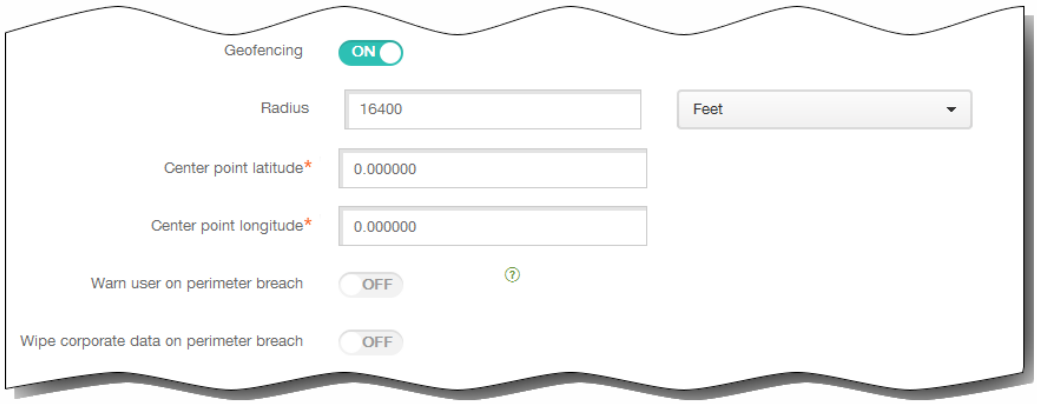
6. 在平台下面，选择要添加的平台。
   - 如果选择 iOS，可以配置以下设置：
     定位超时：键入数值，然后在列表中单击秒或分钟以设置 XenMobile 尝试修复设备位置的频率。有效值为 60–900 秒或 1–15 分钟。默认值为 1 分钟。

     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：选择此选项以配置以下设置：

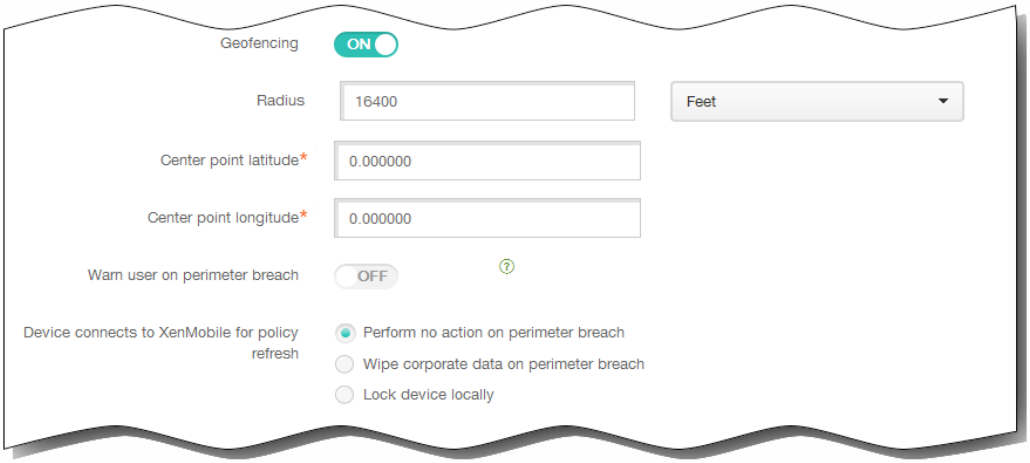


- 半径：键入数值，然后在列表中，单击要用于衡量半径的单位。默认值为 16,400 英尺。
  半径的有效值如下：
  - 164–164000 英尺
  - 1–50 千米
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- Warn user on perimeter breach（警告用户超出边界）：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 XenMobile 即可显示警告消息。
- 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。

- 如果选择 Android，可以配置以下设置：
  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。
  注意：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：选择此选项以配置以下设置：



- 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。

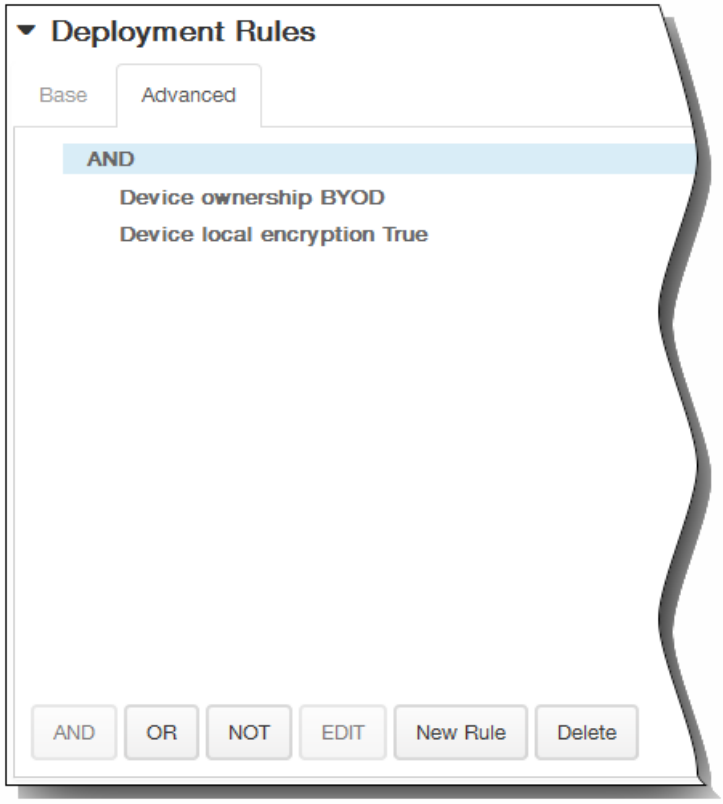
    键入数值，然后在列表中单击秒或分钟以设置从用户设备中擦除公司数据之前延迟的时间长度。这使用户有机会在 XenMobile 选择性擦除其设备之前返回到允许的位置。默认值为 0 秒。

  - 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。

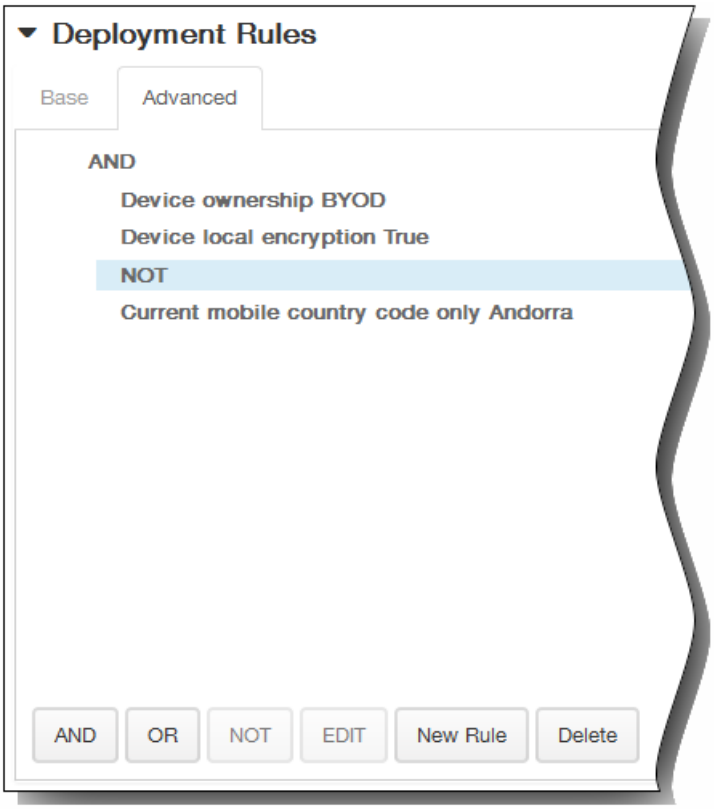
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

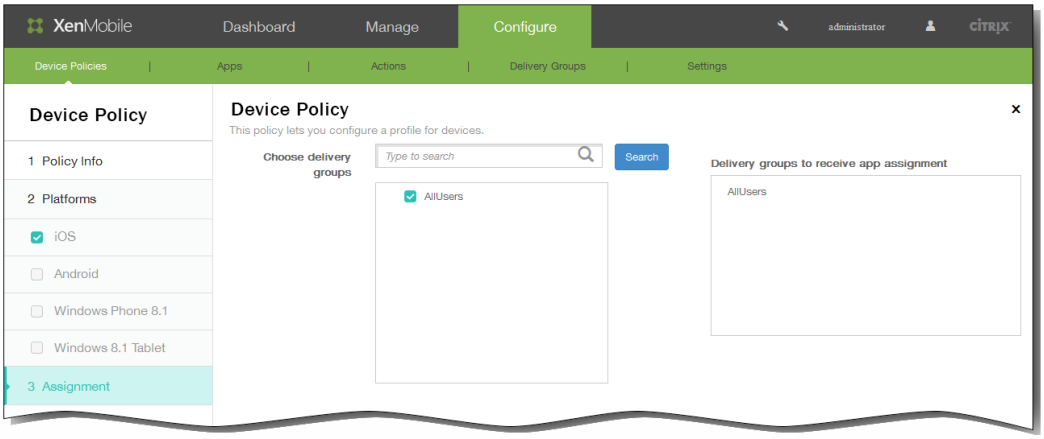


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



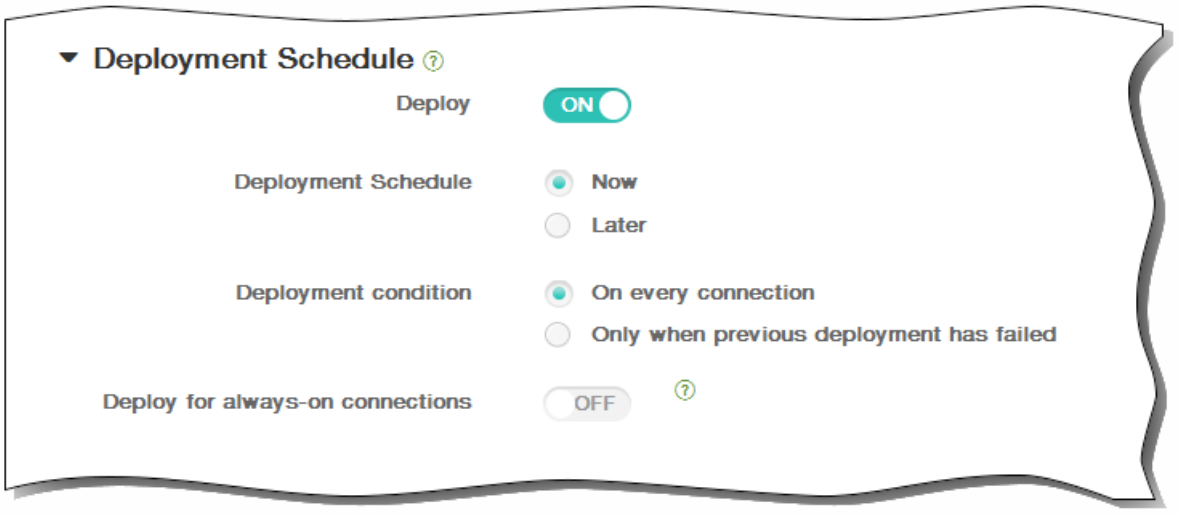
8. 单击下一步。 此时将显示定位策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



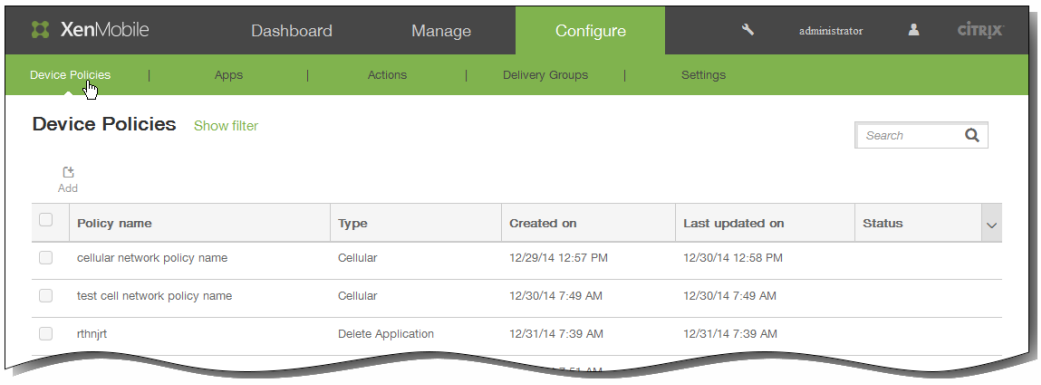
11. 单击保存以保存此策略。

连接计划设备策略

May 05, 2016

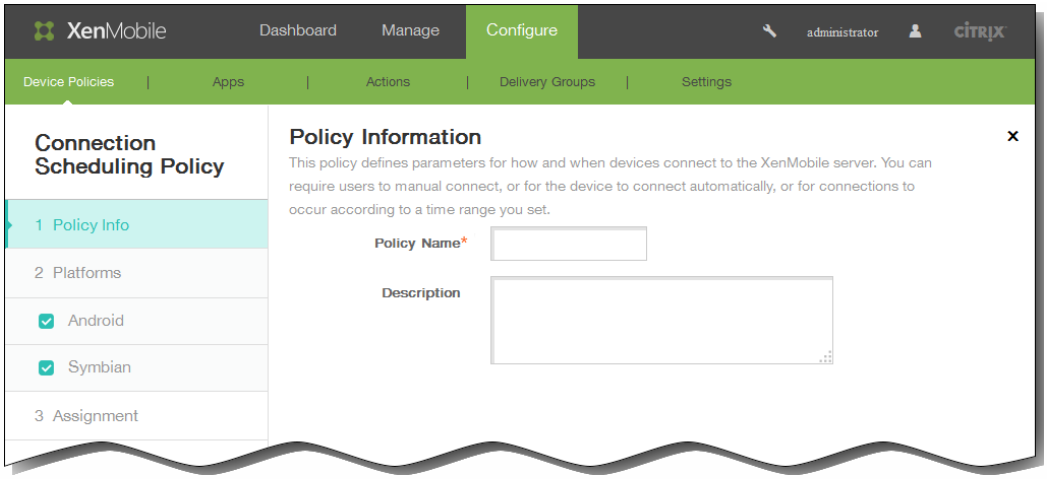
可以创建连接计划策略，用于控制用户的 Android 和 Symbian 设备连接到 XenMobile 的方式和时间。可以指定用户需要手动连接其设备、设备永久保持连接状态或设备在定义的时间范围内进行连接。

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. 单击添加添加新策略。 此时将显示添加新策略对话框。

3. 单击计划。 将显示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：
   1. 策略名称：键入策略的描述性名称。
   2. 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。
   注意：显示策略平台页面时，两个平台均会选中，您会首先看到 Android 平台配置面板。
6. 在平台下面，选择要添加的平台。
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。
   - 始终：连接永久保持活动状态。在丢失网络连接后，用户设备上的 XenMobile 尝试重新连接到 XenMobile 服务器，并通过以固定间隔传输控制数据包监视连接。
     建议不要使用此选项，因为这样会消耗电池电量并产生大量网络流量。
   - 从不：手动进行连接。用户必须从其设备上的 XenMobile 启动连接。
   - 每：按照指定间隔进行连接。经过定义的分钟数之后，设备自动连接。
     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：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。以下部分将介绍定义连接时间范围的方法。
     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。

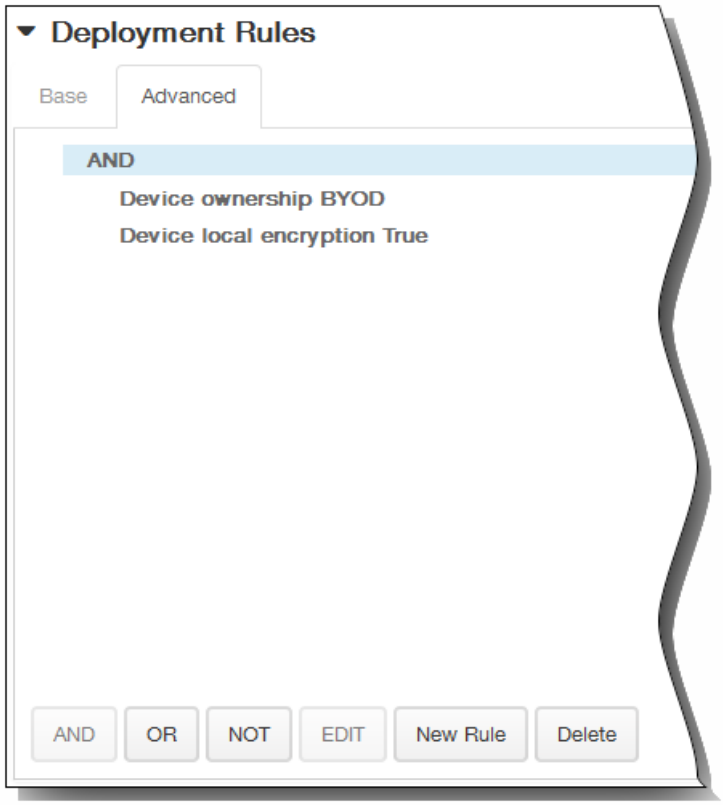
在此时段内保持永久连接：在定义的时间范围内，用户设备必须连接。

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。

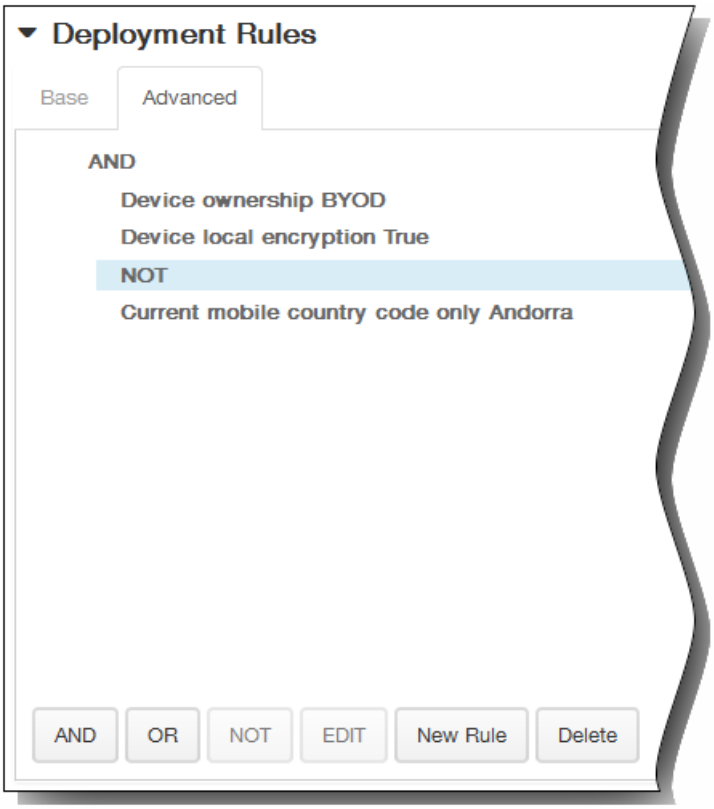
8. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

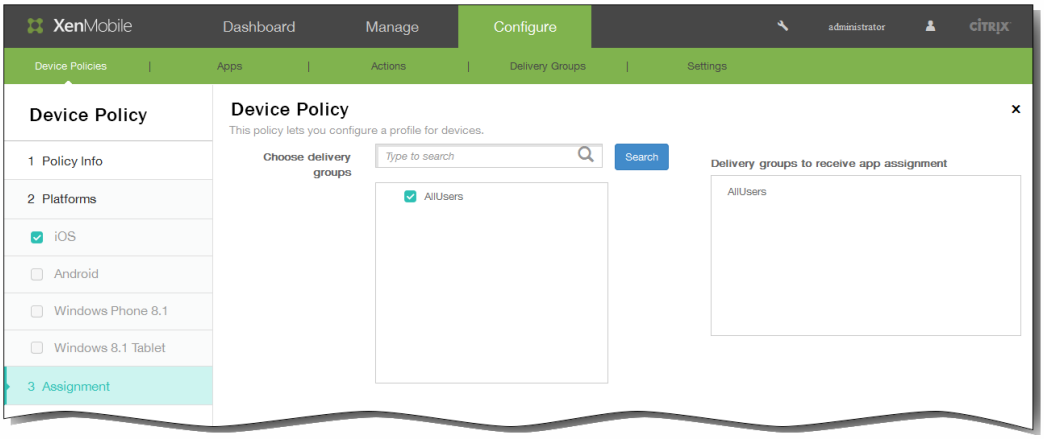


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



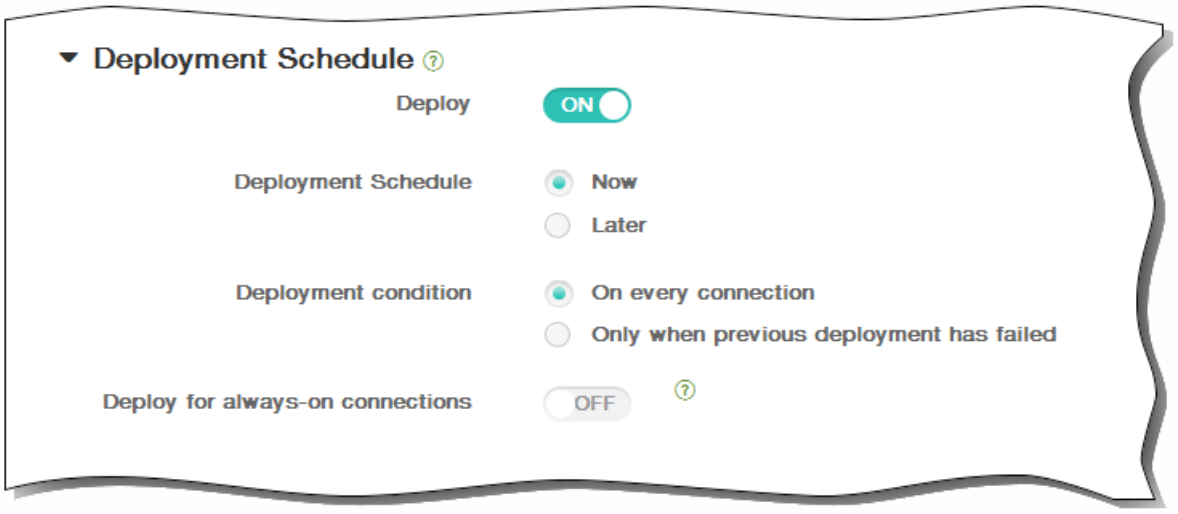
9. 单击下一步。 将显示连接计划策略分配页面。
10. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



11. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



12. 单击保存以保存此策略。

添加适用于 iOS 的 AirPlay 镜像设备策略

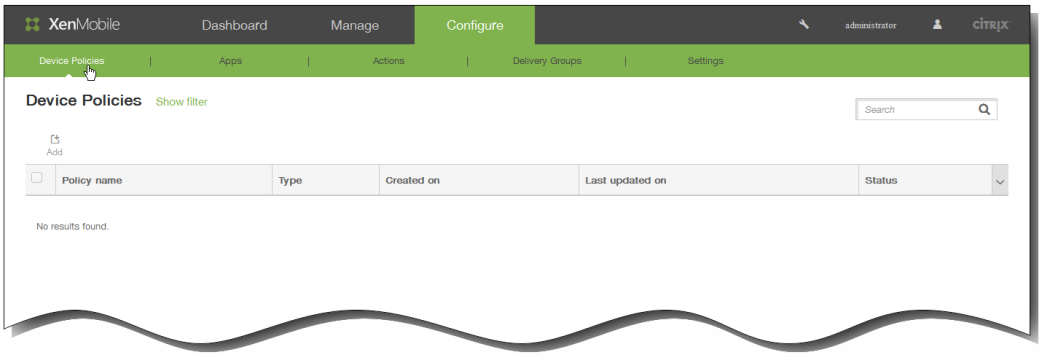
May 05, 2016

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。

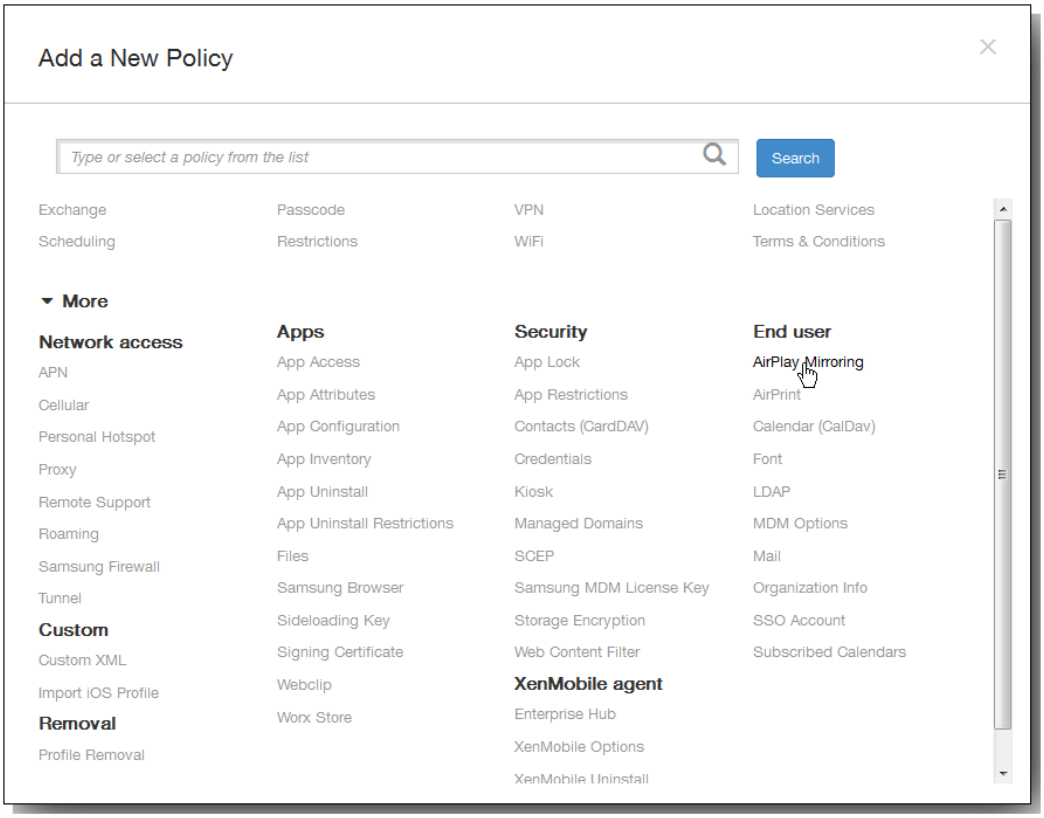
您可以在 XenMobile 中添加一个设备策略，从而将特定 AirPlay 设备（如 Apple 电视或其他 Mac 计算机）添加到用户的 iOS 设备。您还可以将设备添加到受监督设备的白名单，从而使用户仅限于白名单上的 AirPlay 设备。有关将设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

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。

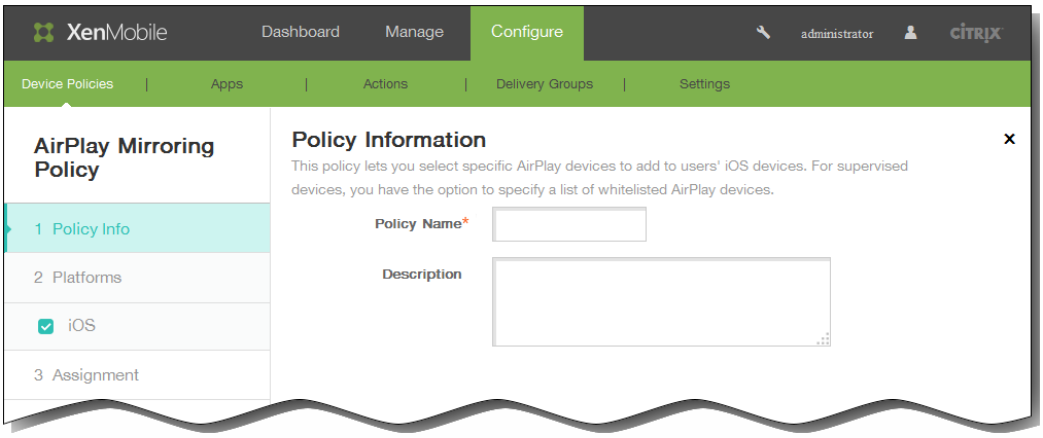
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



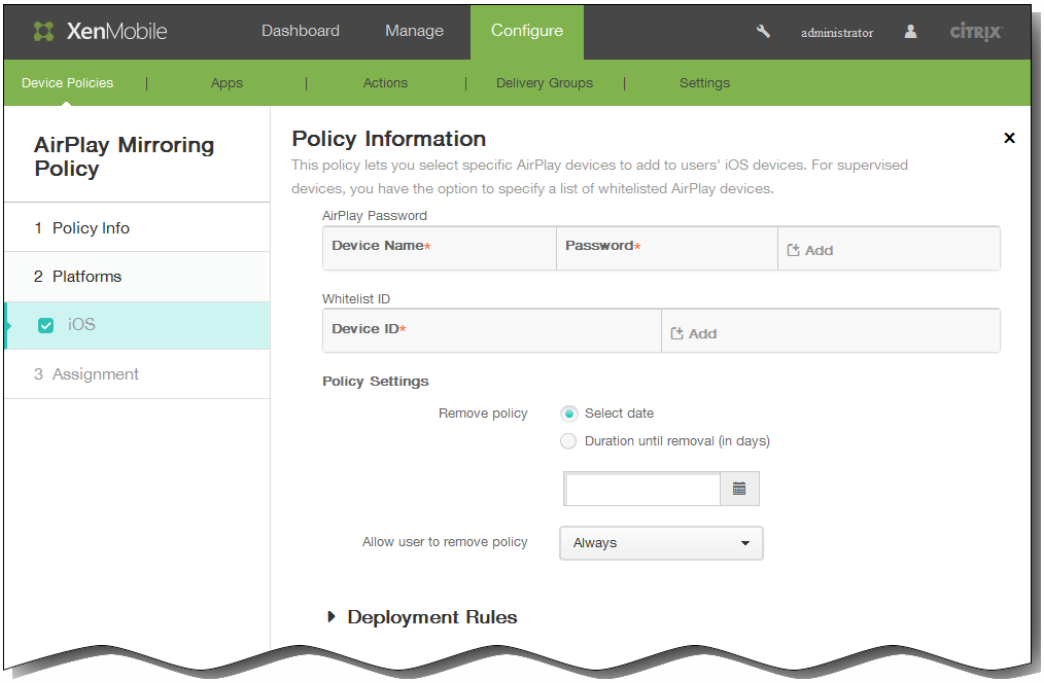
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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：
   1. 策略名称：键入策略的描述性名称。
   2. 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。

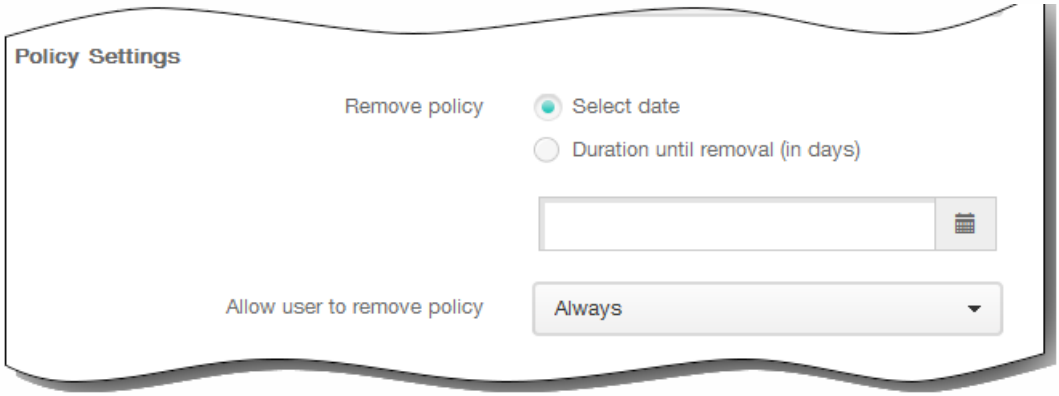


6. 在 iOS 平台信息页面上，输入以下信息：
   1. AirPlay 密码：单击添加，然后执行以下操作：
      1. 设备 ID：以 xx:xx:xx:xx:xx:xx 格式输入设备 ID。此字段不区分大小写。
      2. 密码：输入设备的可选密码。
      3. 单击添加以添加设备，或单击取消以取消添加设备。

4. 为要添加的每个应用程序重复步骤 i.至步骤 iii.。

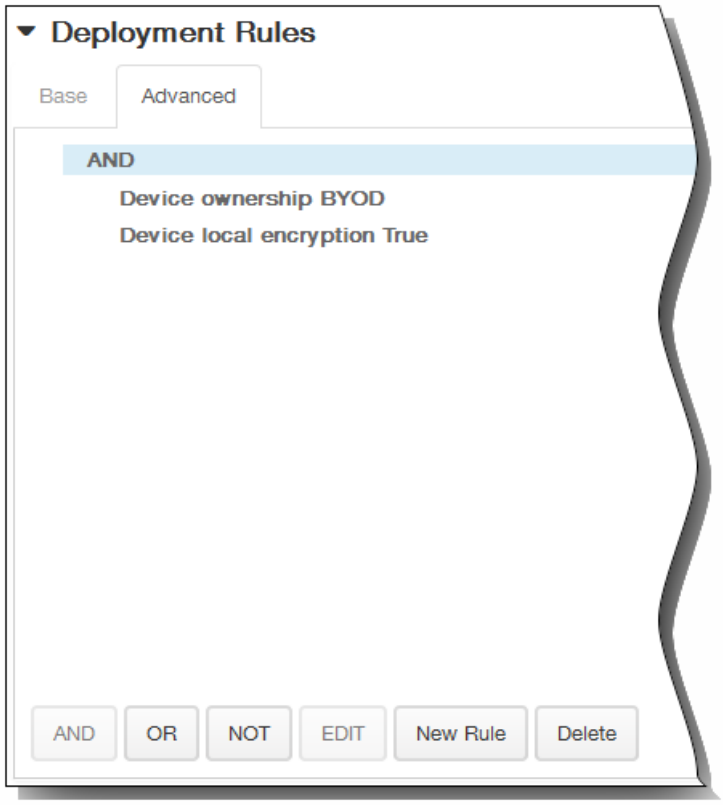
2. 白名单 ID：单击添加，然后执行以下操作，使受监督设备仅限于白名单上的这些设备 ID：
   注意：未受监督的设备请忽略此列表。
   1. 设备 ID：采用xx:xx:xx:xx:xx:xx格式输入设备 ID。此字段不区分大小写。
   2. 单击添加以添加设备，或单击取消以取消添加设备。
   3. 为要添加的每个应用程序重复步骤 i.和 ii.。
   注意：要删除现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击删除以删除列表，或单击取消以保留此列表。
   要编辑现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。更改列表，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。

7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



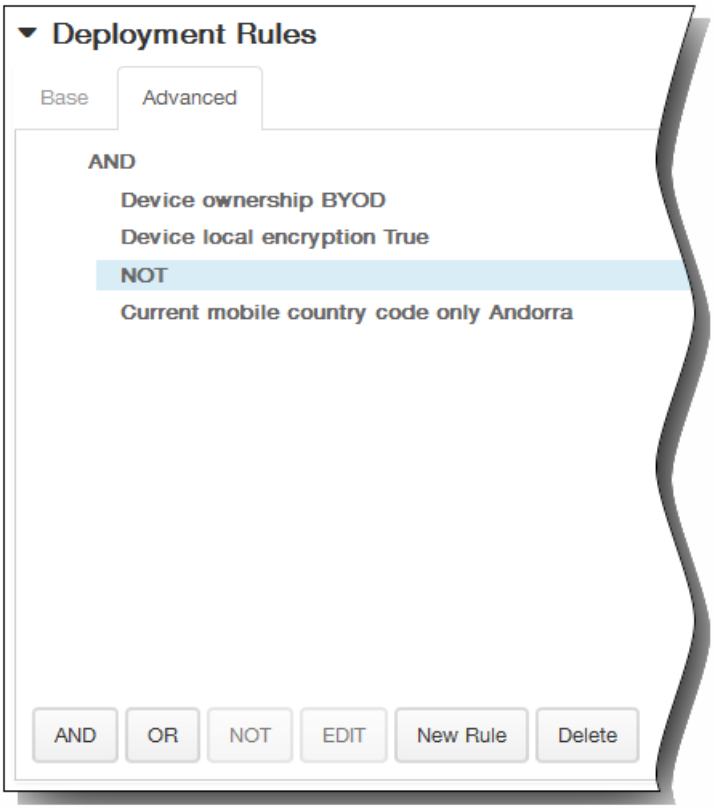
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

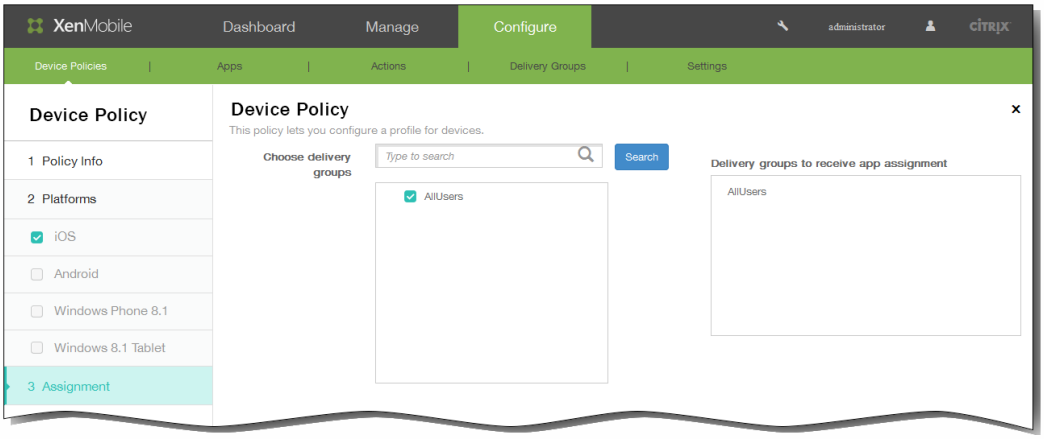


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



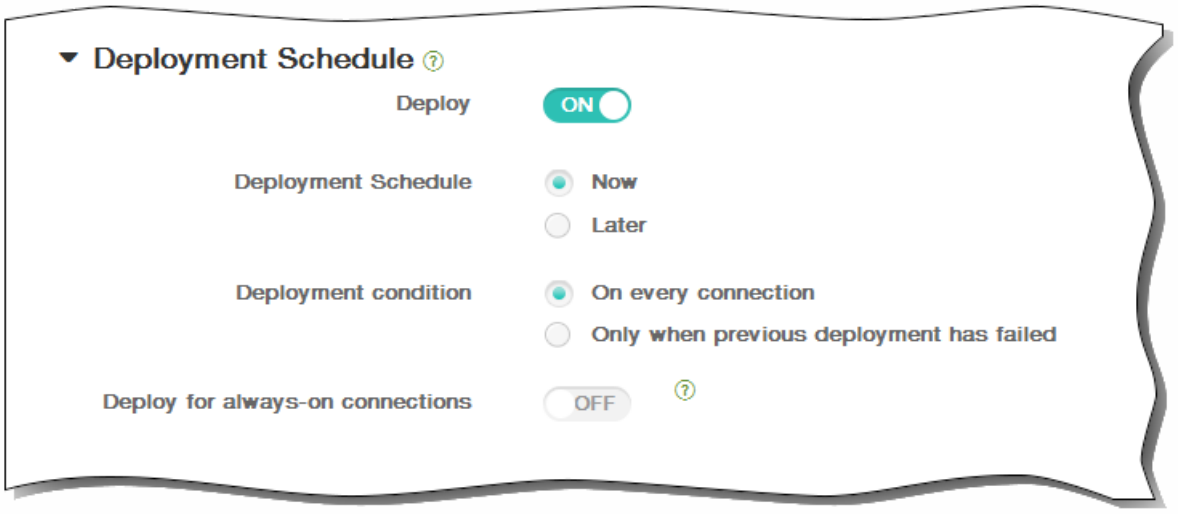
12. 单击下一步。 此时将显示 AirPlay 镜像策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



15. 单击保存以保存此策略。

添加适用于 iOS 的 AirPrint 设备策略

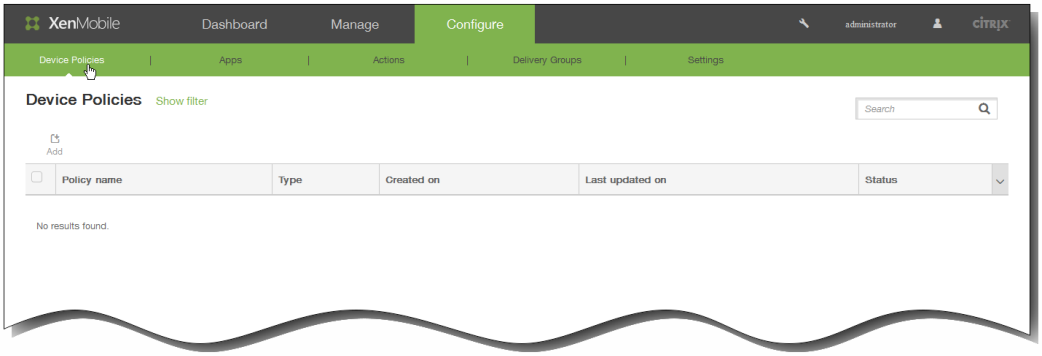
May 05, 2016

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。

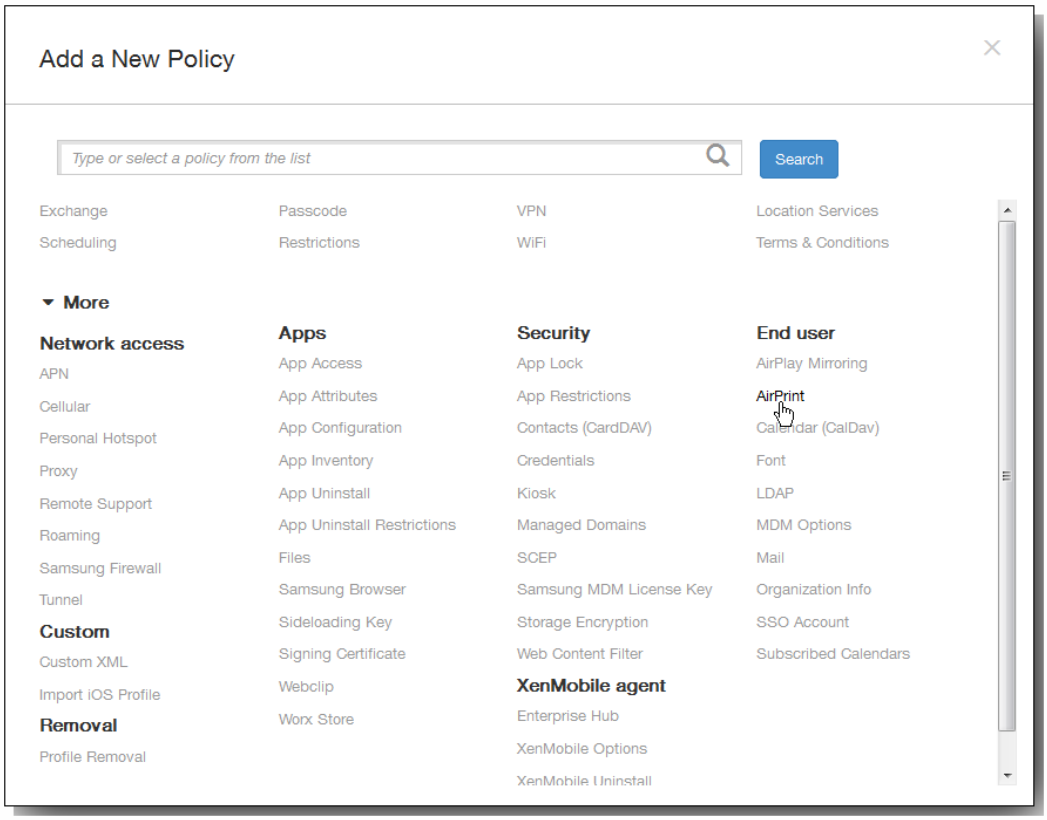
注意：

- 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。

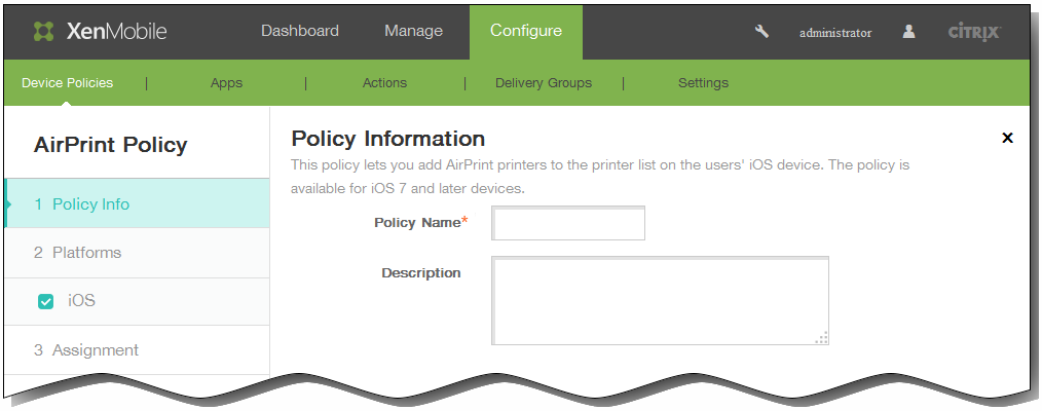
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



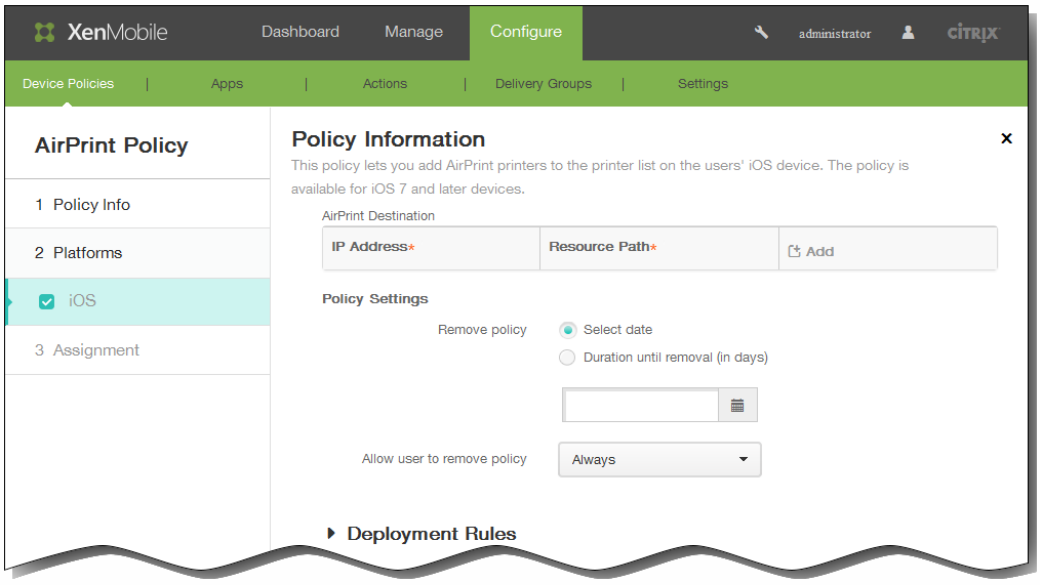
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在最终用户下面，单击 AirPrint。 此时将显示 AirPrint 策略页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。



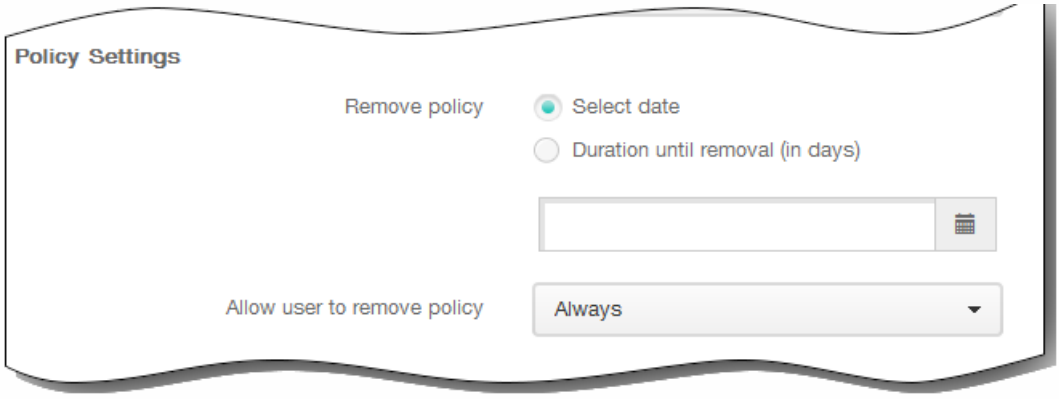
6. 在 iOS 平台信息页面上，输入以下信息：
   1. AirPrint 目标：单击添加，然后执行以下操作：
      1. IP 地址：输入 AirPrint 打印机 IP 地址。
      2. 资源路径：输入与打印机关联的资源路径。此值与 _ipps.tcp Bonjour 记录的参数相对应。例如，printers/Canon_MG5300_series 或 printers/Xerox_Phaser_7600。
      3. 单击添加以添加打印机，或单击取消以取消添加打印机。
      4. 为要添加的每个应用程序重复步骤 i.至步骤 iii.。

      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

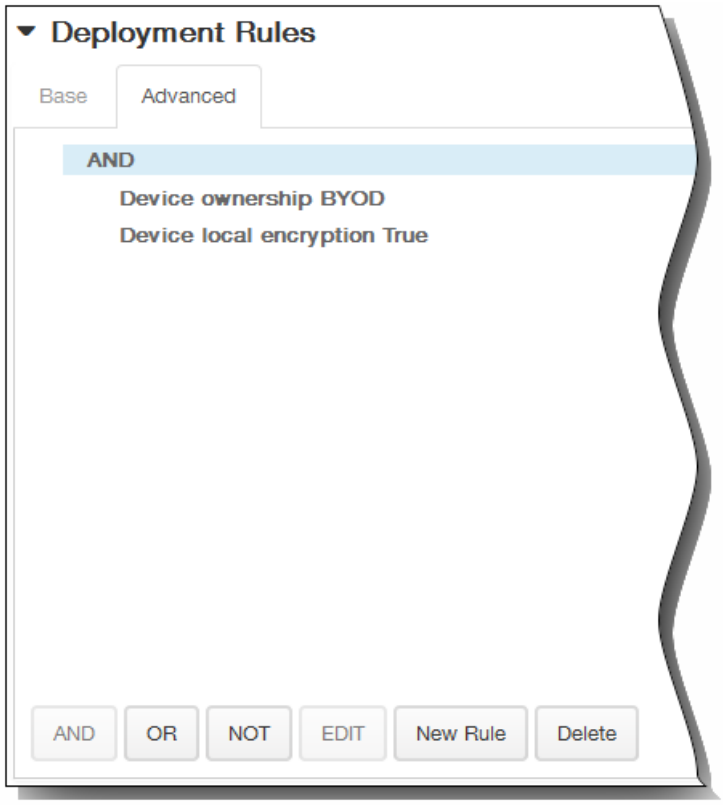
改的列表，或单击取消以保持列表不更改。

7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



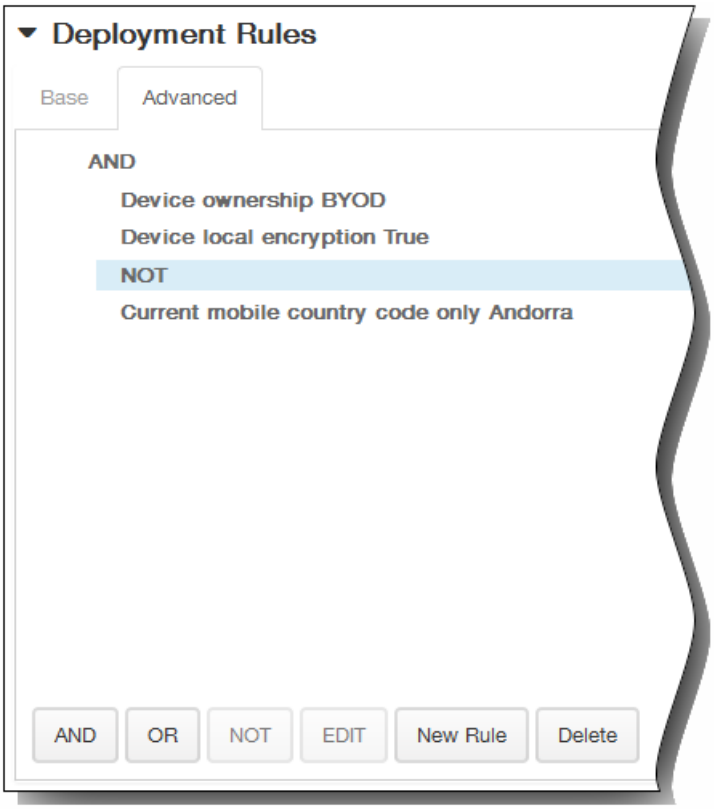
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

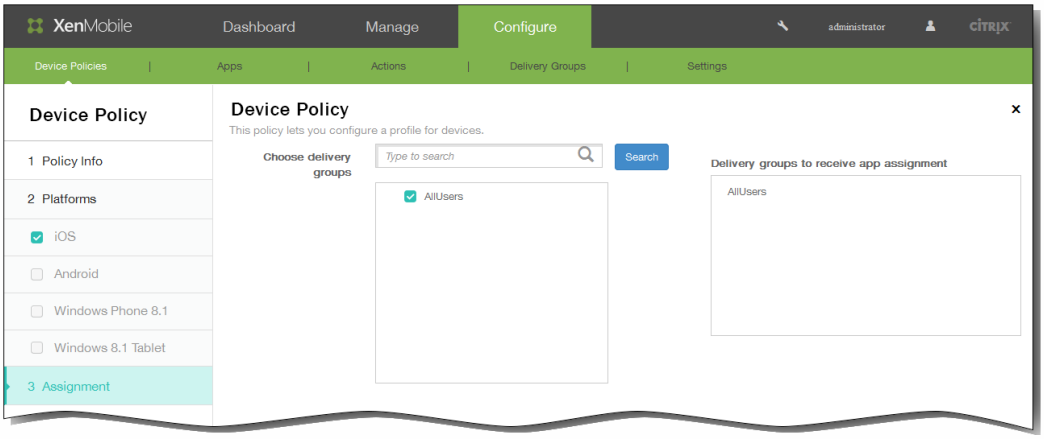


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



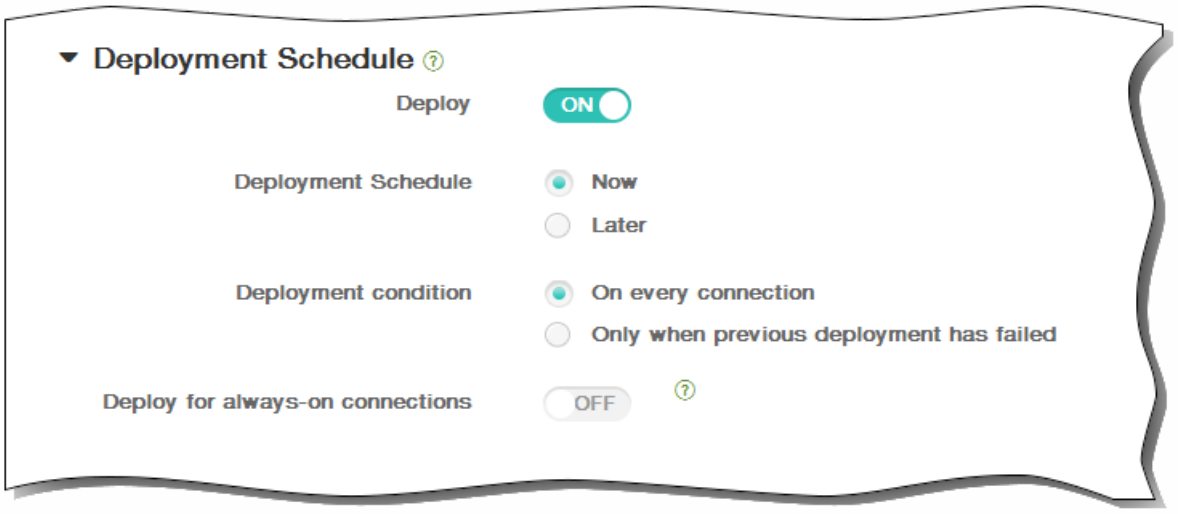
12. 单击下一步。 此时将显示 AirPrint 策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



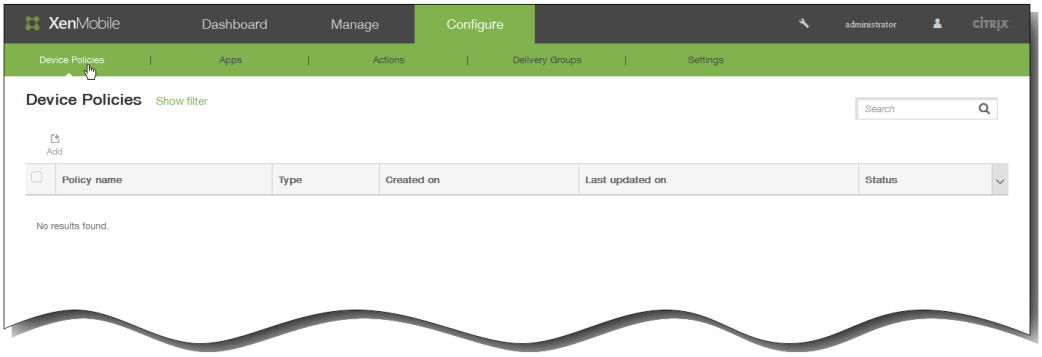
15. 单击保存以保存此策略。

添加适用于 iOS 的日历 (CalDav) 设备策略

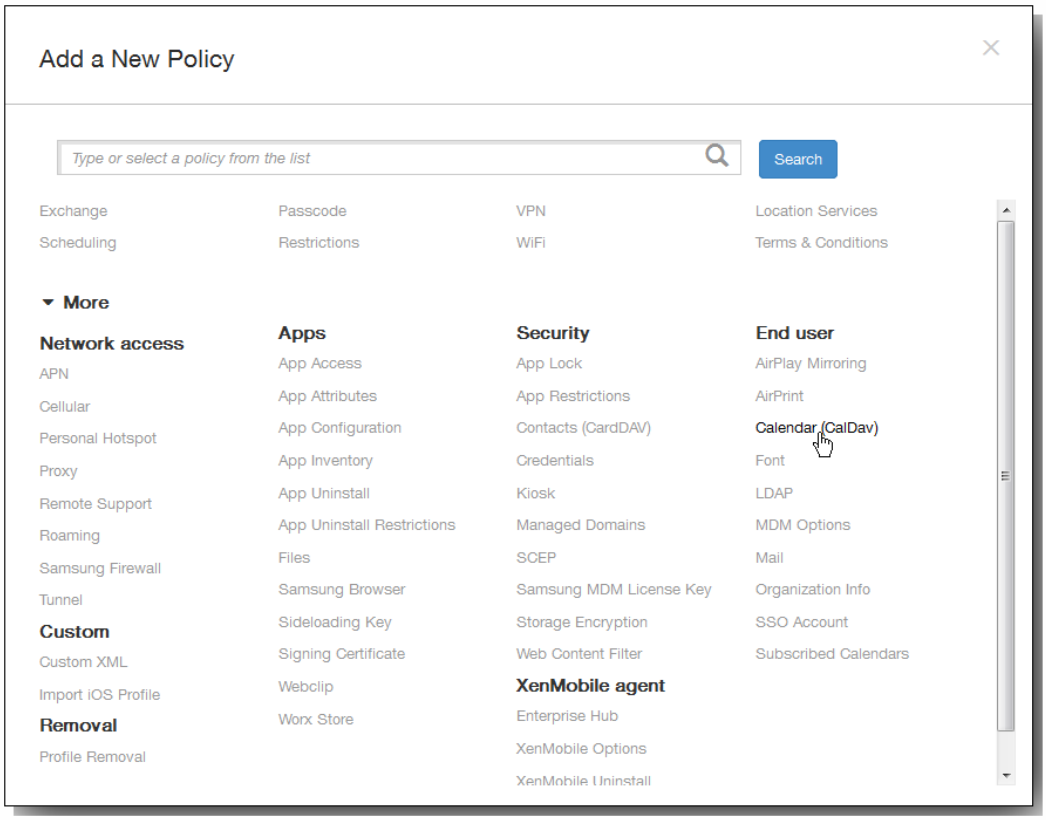
May 05, 2016

可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 设备添加 iOS 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。

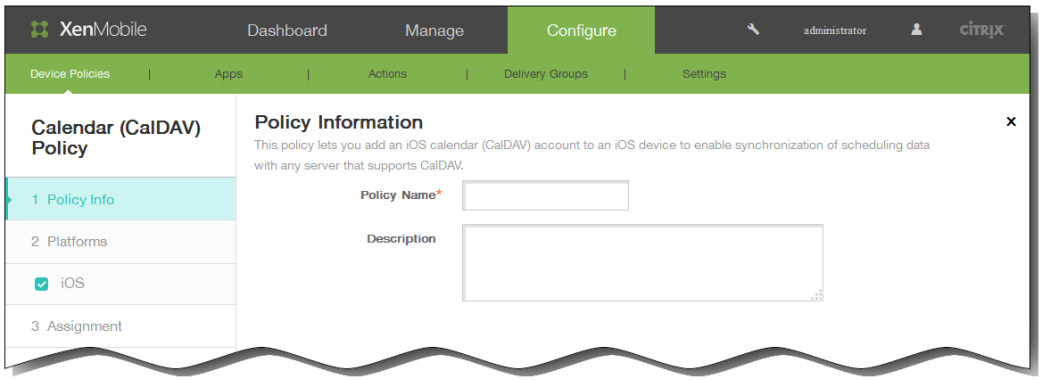
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



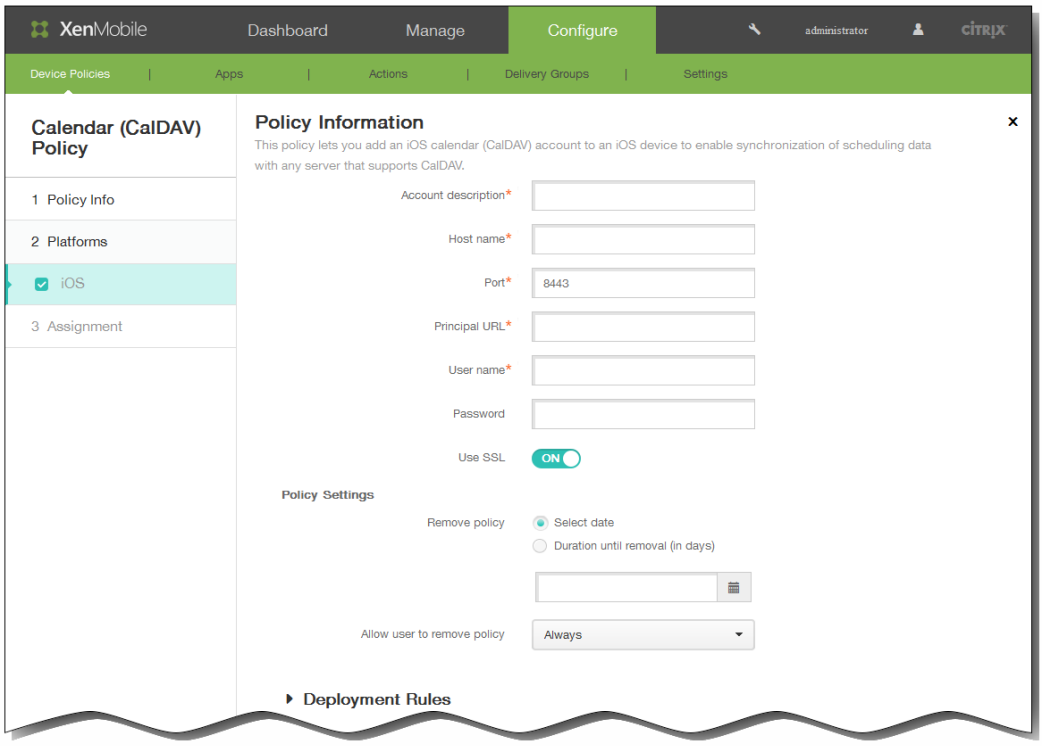
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。

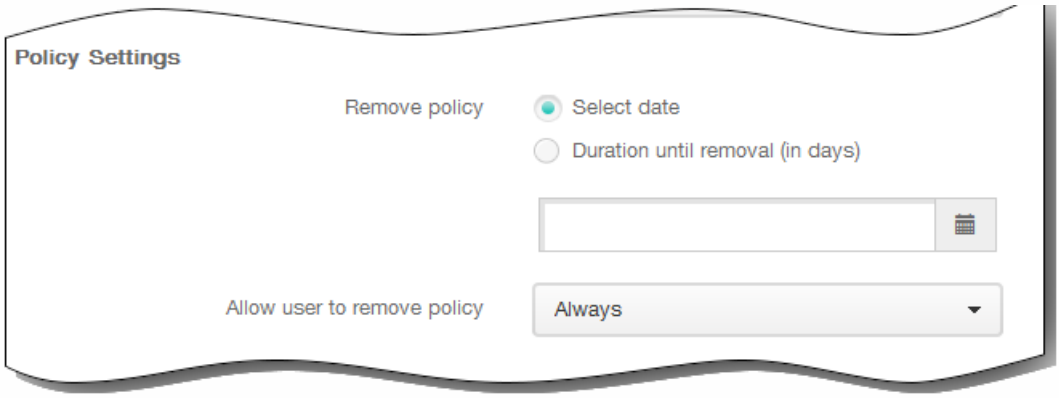


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。



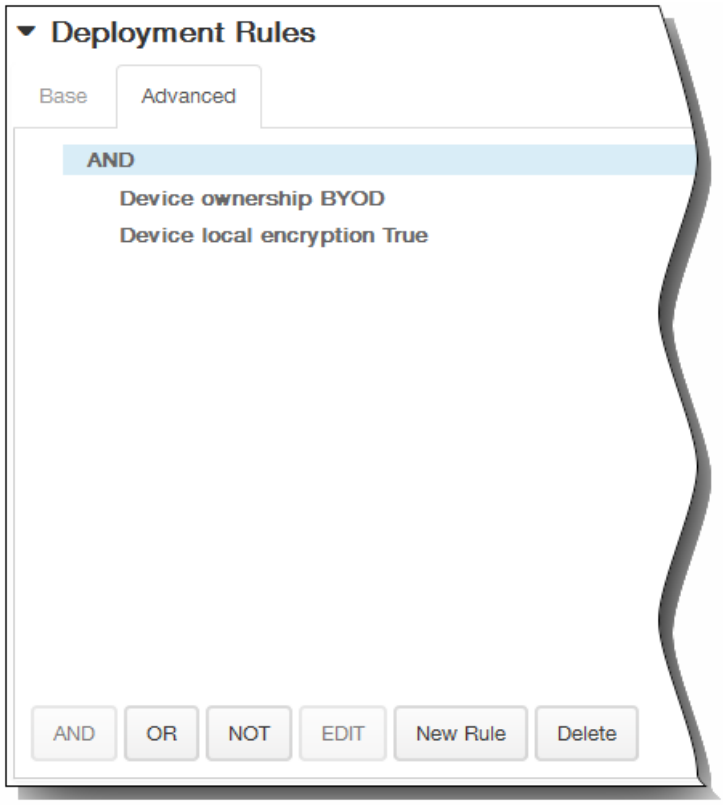
6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户说明：键入帐户说明。 此字段为必填字段。
   2. 主机名：键入 CalDAV 服务器的地址。 此字段为必填字段。
   3. 端口：键入连接到 CalDAV 服务器使用的端口。 此字段为必填字段。 默认值为 8443。
   4. 主体 URL：键入用户日历的基本 URL。
   5. 用户名：键入用户的登录名称。 此字段为必填字段。
   6. 密码：键入可选用户密码。
   7. 使用 SSL：选择是否使用安全套接字层连接到 CalDAV 服务器。 默认值为开。
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。

8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



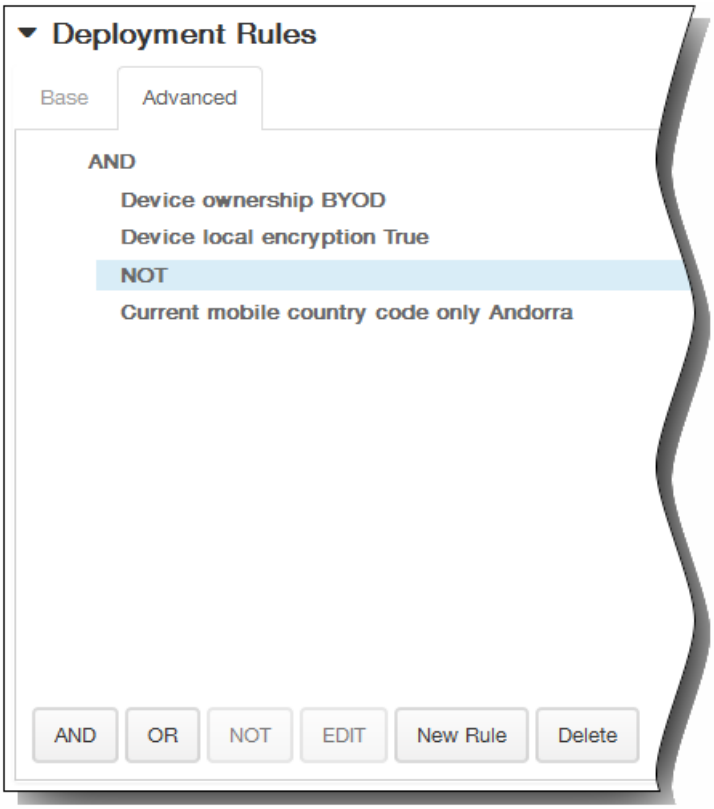
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

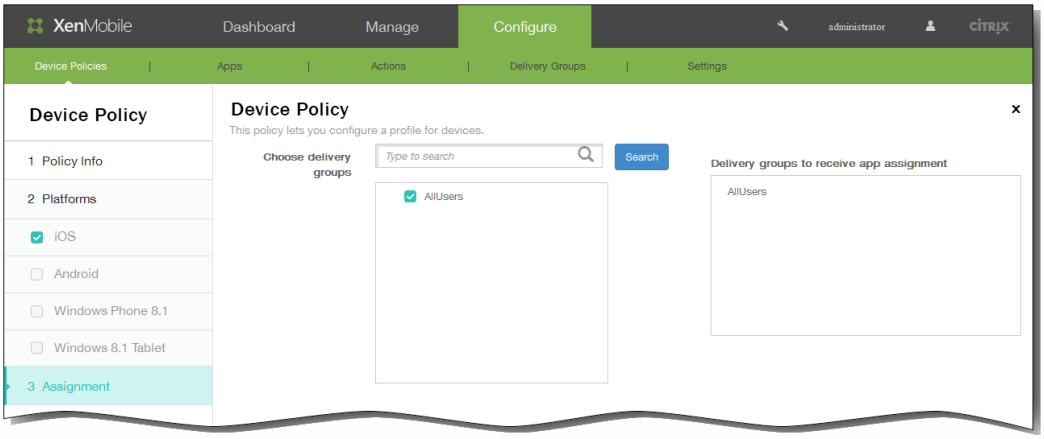


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



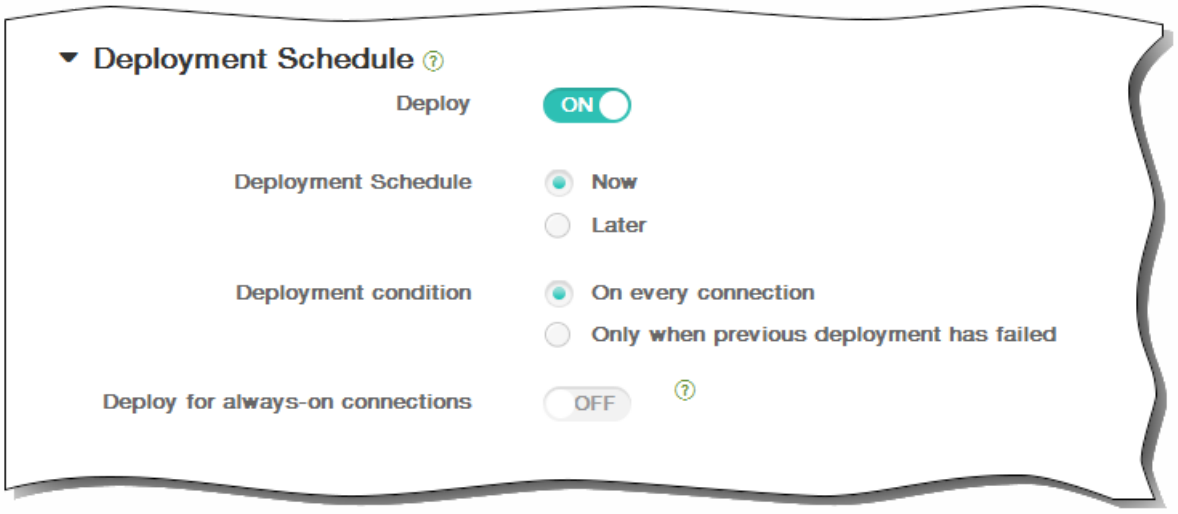
12. 单击下一步。 此时将显示日历(CalDAV)策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



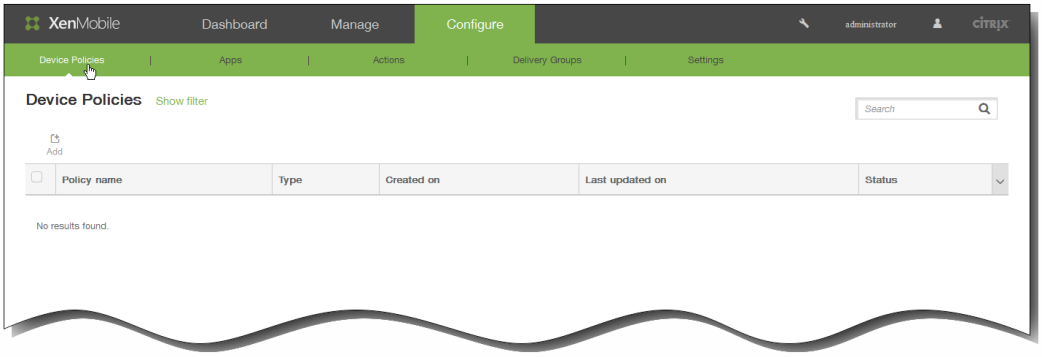
15. 单击保存以保存此策略。

添加适用于 iOS 的联系人 (CardDAV) 设备策略

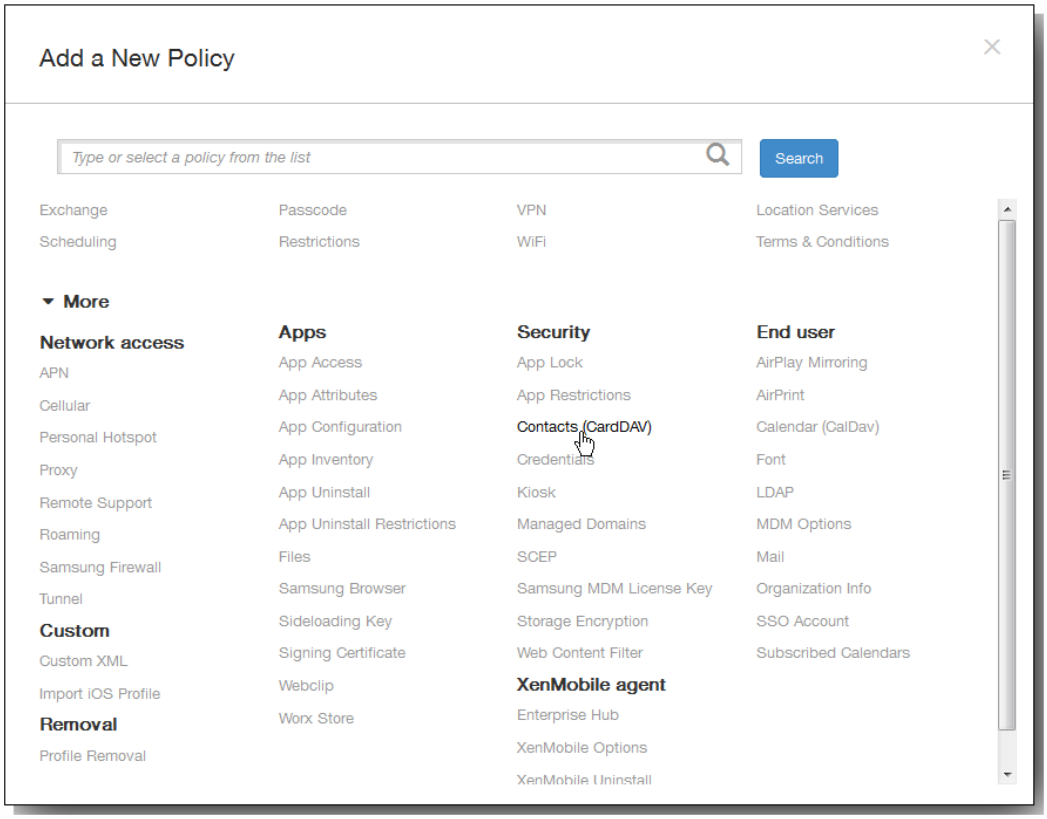
May 05, 2016

可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 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。

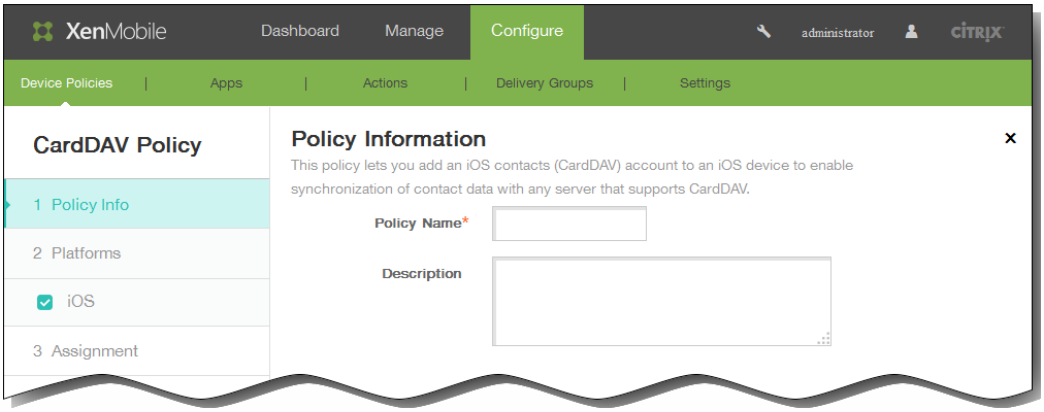
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



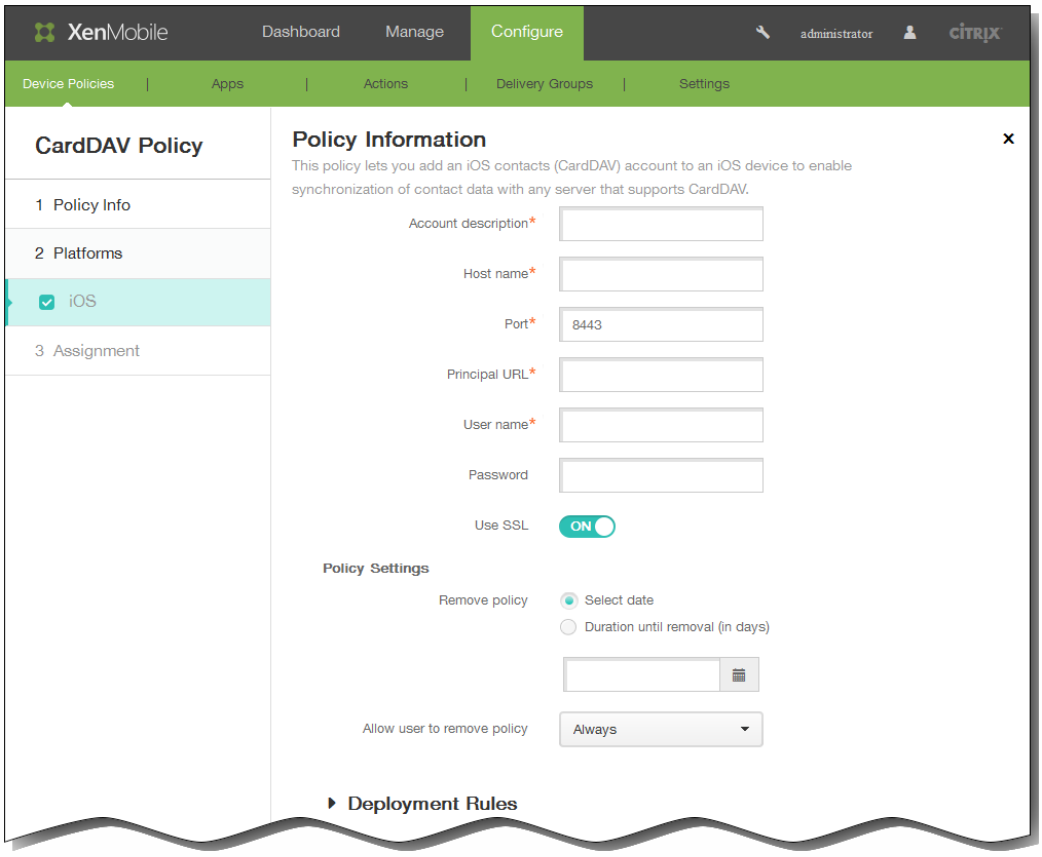
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在安全性下面，单击联系人(CardDAV)。 此时将显示 CardDAV 策略页面。



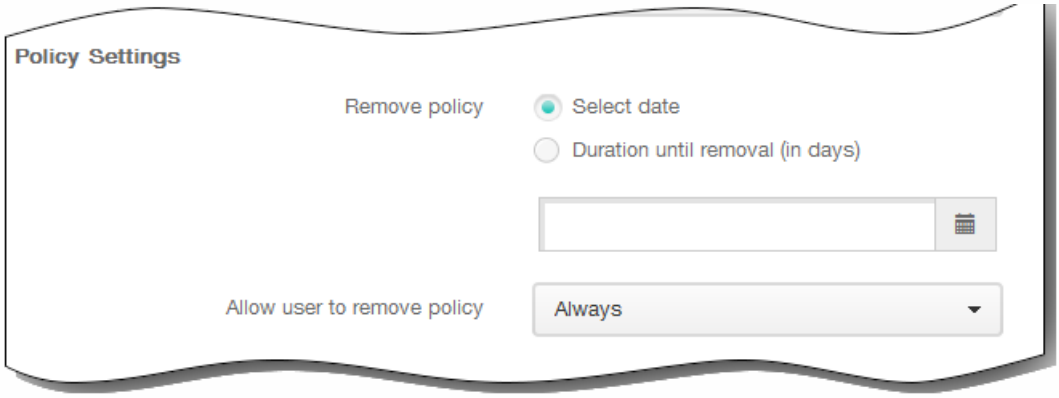
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。



6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户说明：输入帐户说明。 此字段为必填字段。
   2. 主机名：输入 CardDAV 服务器的地址。 此字段为必填字段。
   3. 端口：输入连接到 CardDAV 服务器使用的端口。 此字段为必填字段。 默认值为 8443。
   4. 主体 URL：输入用户日历的基本 URL。
   5. 用户名：输入用户的登录名称。 此字段为必填字段。

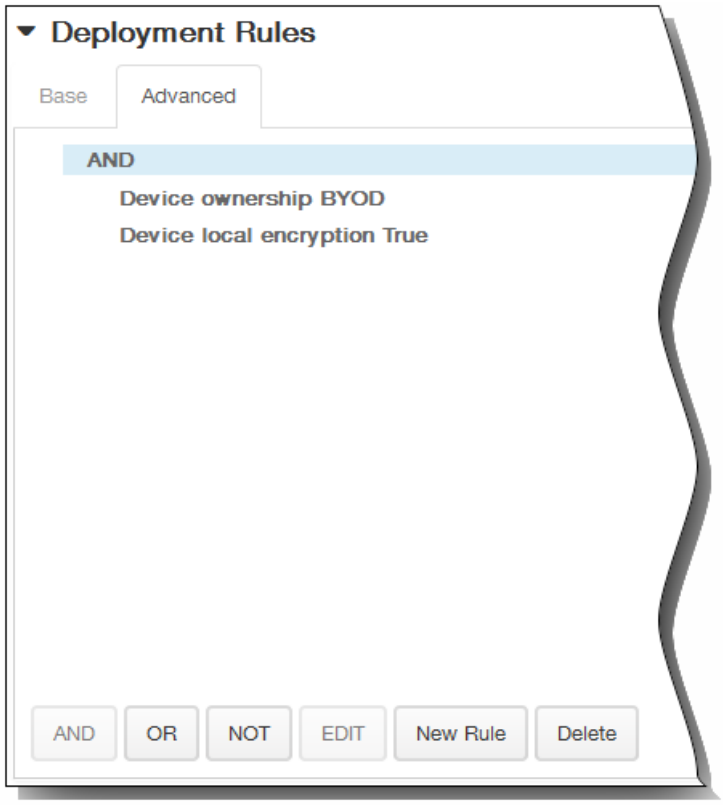
6. 密码：输入可选用户密码。
7. 使用 SSL：选择是否使用安全套接字层连接到 CardDAV 服务器。 默认值为开。

7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



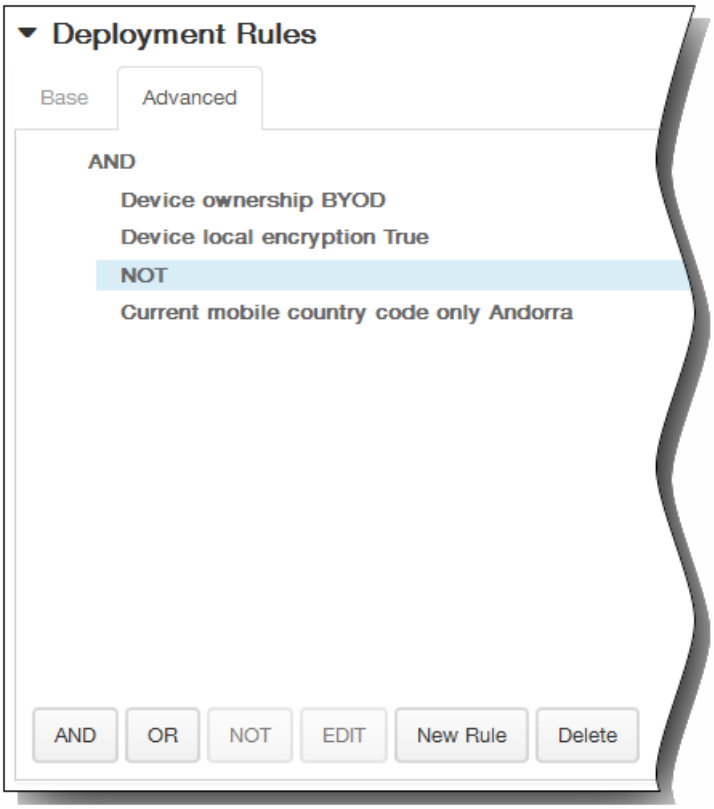
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

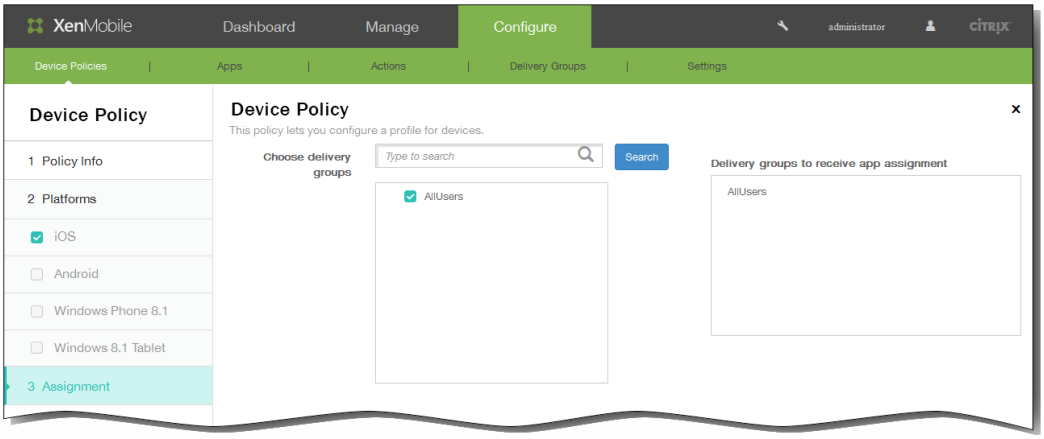


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



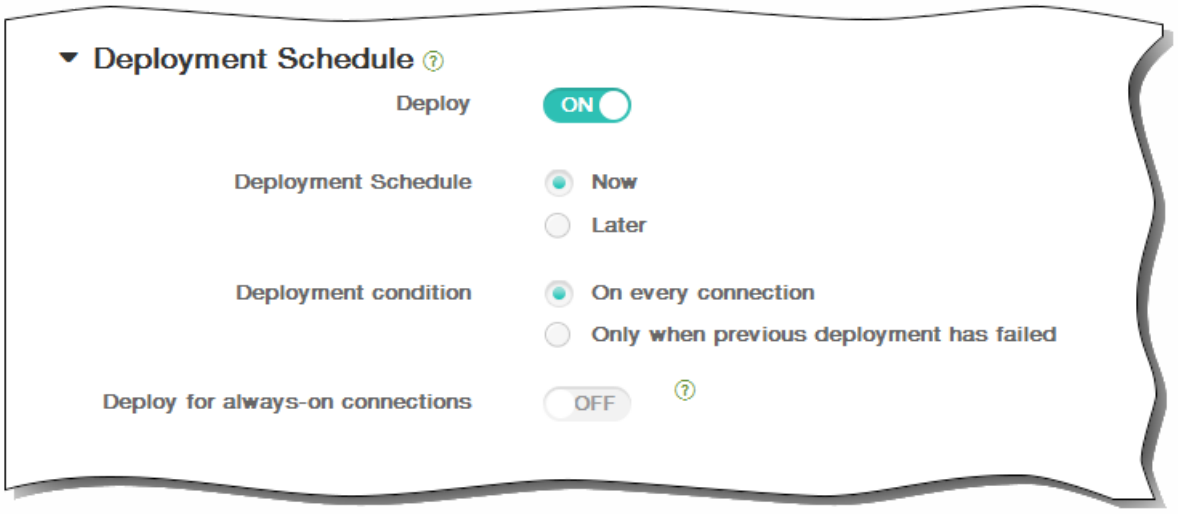
12. 单击下一步。 此时将显示 CardDAV 策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



15. 单击保存以保存此策略。

凭据设备策略

May 05, 2016

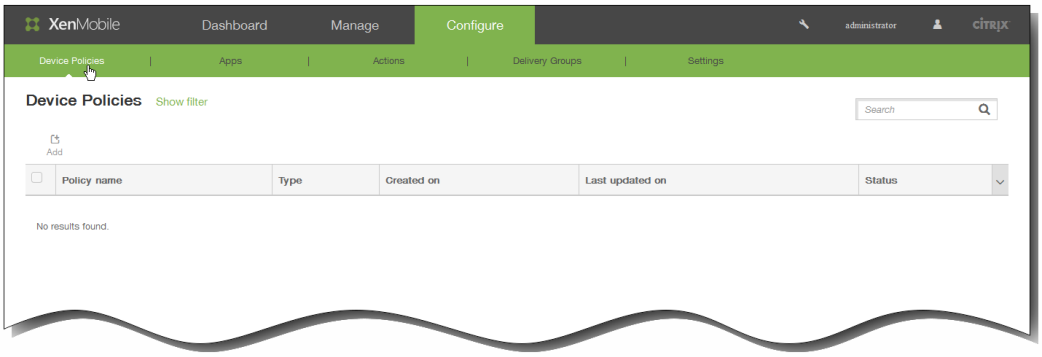
可以在 XenMobile 中创建凭据设备策略，以使用 XenMobile 中的 PKI 配置启用集成身份验证，例如 PKI 实体、密钥库、凭据提供程序或服务器证书。有关凭据的详细信息，请参阅 XenMobile 中的证书。

可以为 iOS、Android 和 Windows 8.1 Tablet 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。

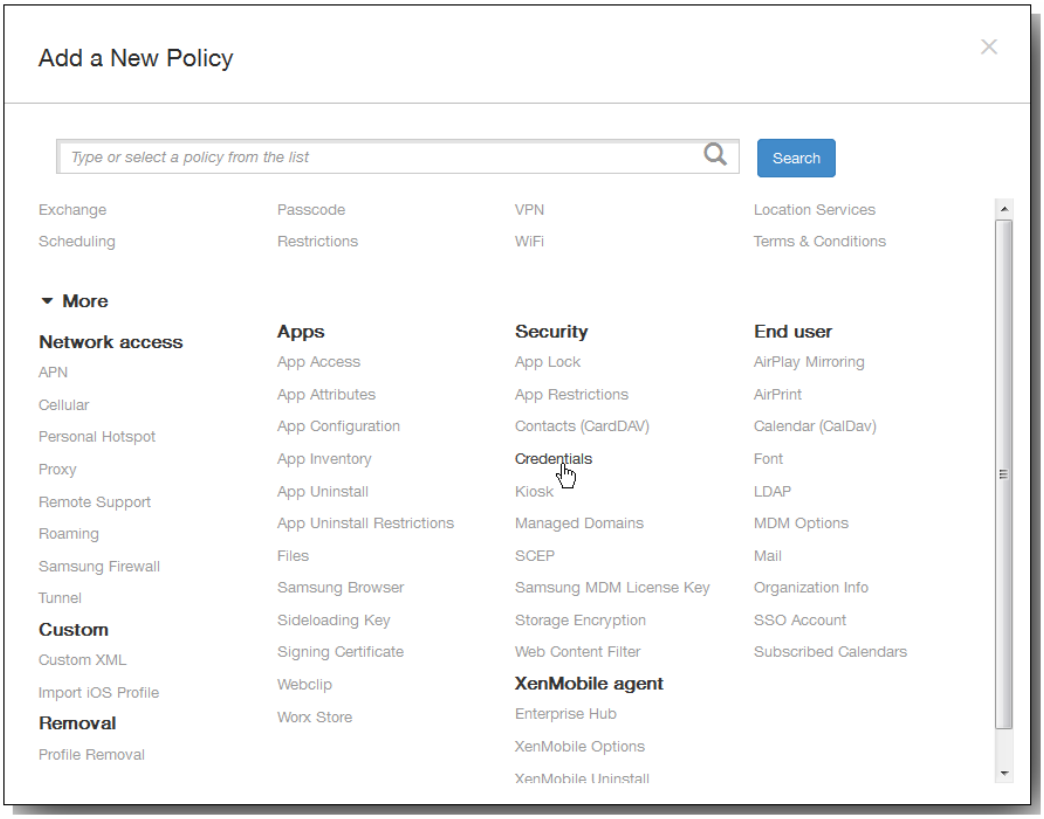
创建此策略之前，需要提供以下信息：

- 打算对每个平台使用的凭据信息以及任何证书和密码。

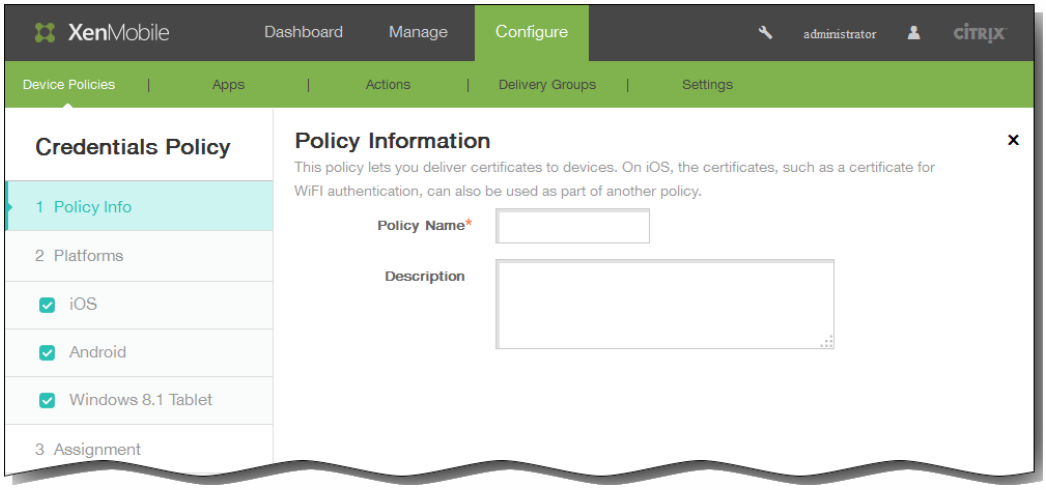
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



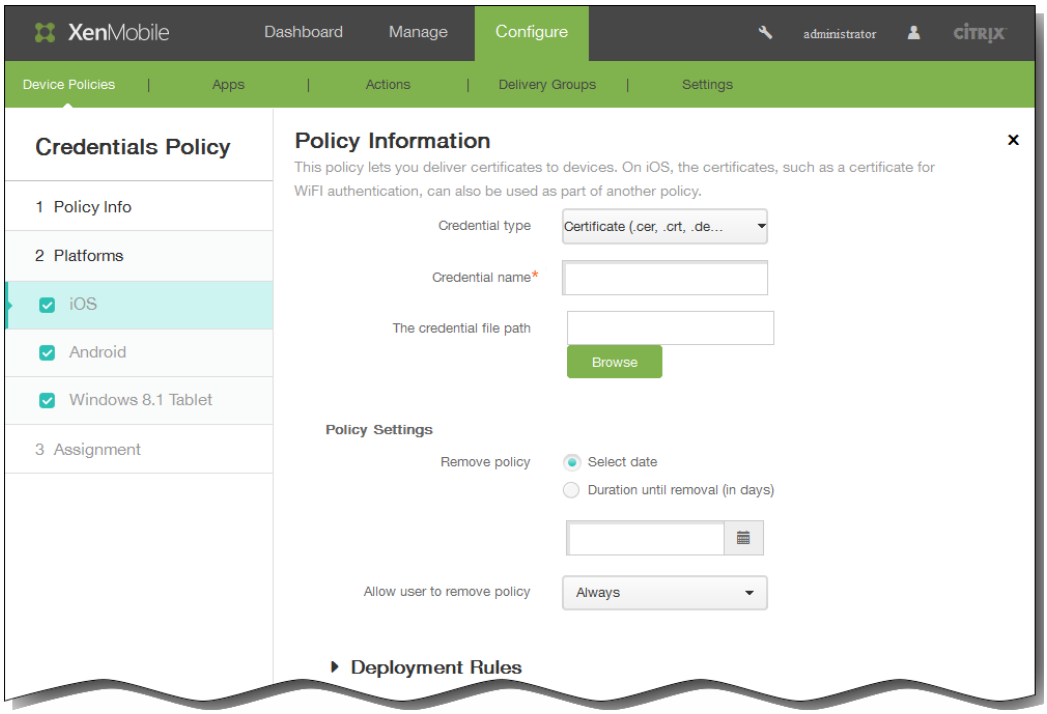
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



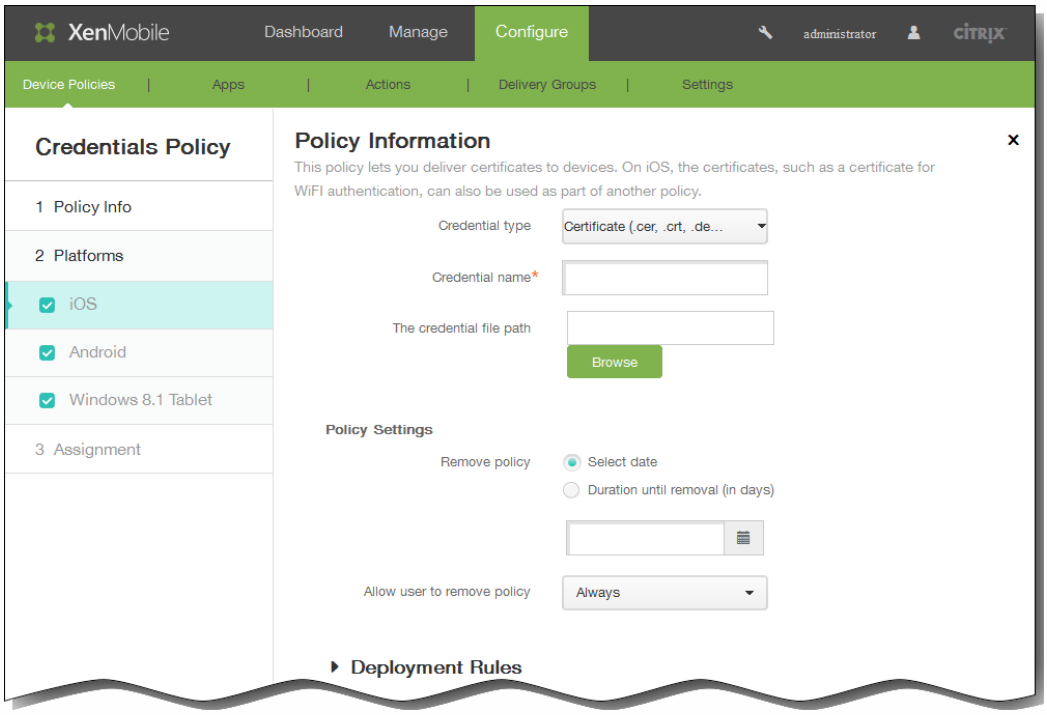
3. 单击更多，然后在安全性下面，单击凭据。 此时将显示凭据策略信息页面。



4. 在策略信息窗格中，键入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。
   注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 iOS 平台配置面板。



6. 在平台下面，选择要添加的平台。
   - 如果选择 iOS，可以配置以下设置：



凭据类型：在列表中，单击要用于此策略的凭据类型。

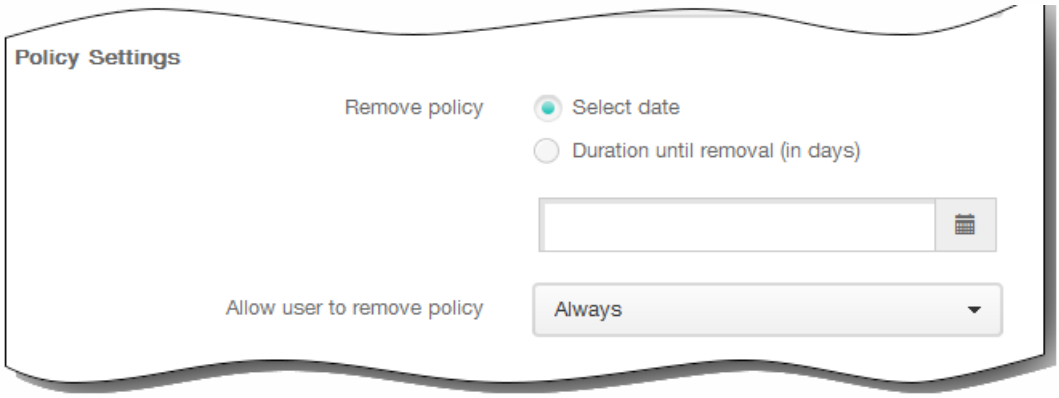
输入所选凭据的以下信息：

- **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，导航到凭据文件的位置，以选择此凭据文件。

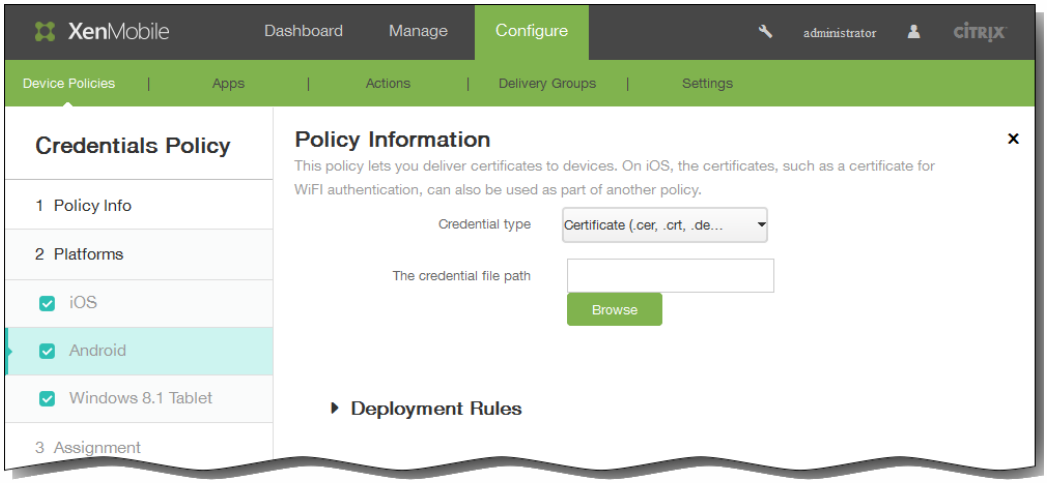
- **密钥库**
  - 凭据名称：键入凭据的唯一名称。
  - 凭据文件路径：单击浏览，导航到凭据文件的位置，以选择此凭据文件。
  - 密码：键入凭据的密钥库密码。
- **服务器证书**
  - 服务器证书：在列表中，单击要使用的证书。
- **凭据提供程序**
  - 凭据提供程序：在列表中，单击凭据提供程序的名称。

策略设置



1. 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)。
2. 如果单击选择日期，请单击日历以选择具体删除日期。
3. 在允许用户删除策略列表中，单击始终、需要密码或从不。
4. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。

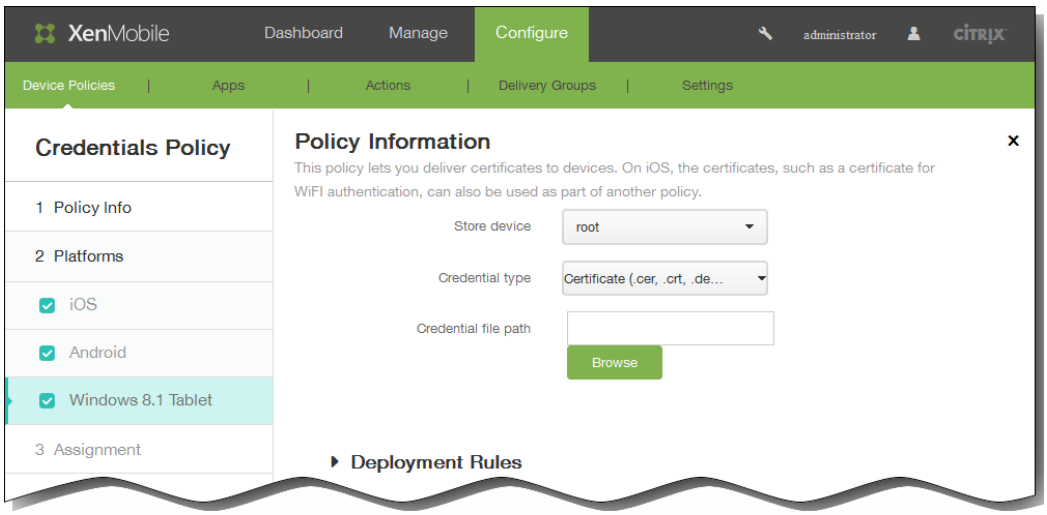
- 如果选择 Android，可以配置以下设置：



凭据类型：在列表中，单击要用于此策略的凭据类型。

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。
- 如果选择 Windows 8.1 Tablet，可以配置以下设置：



存储设备：在列表中，单击根、我的或 CA 以选择凭据的证书存储位置。我的存储用户证书存储中的证书。

凭据类型：证书是适用于 Windows 8.1 Tablet 的唯一凭据类型。

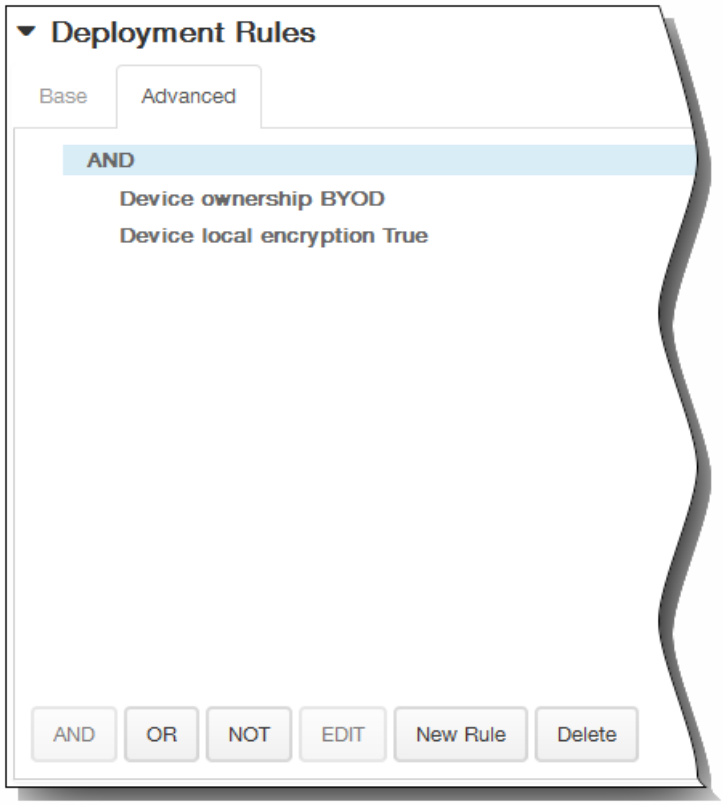
凭据文件路径：单击浏览，然后导航到凭据文件的位置，以选择此凭据文件。

7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。

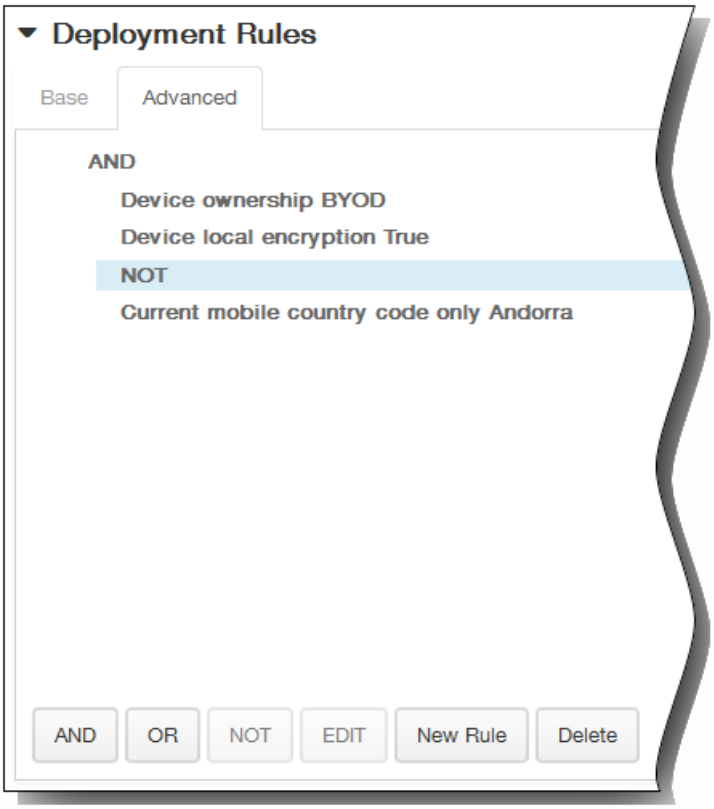
1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
2. 单击新建规则以定义条件。
3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。

2. 单击高级选项卡以使用布尔选项组合规则。

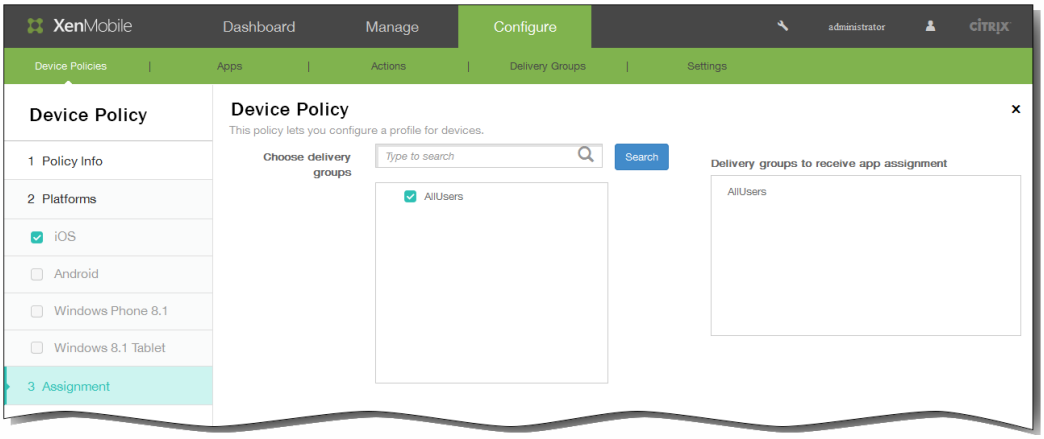


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。

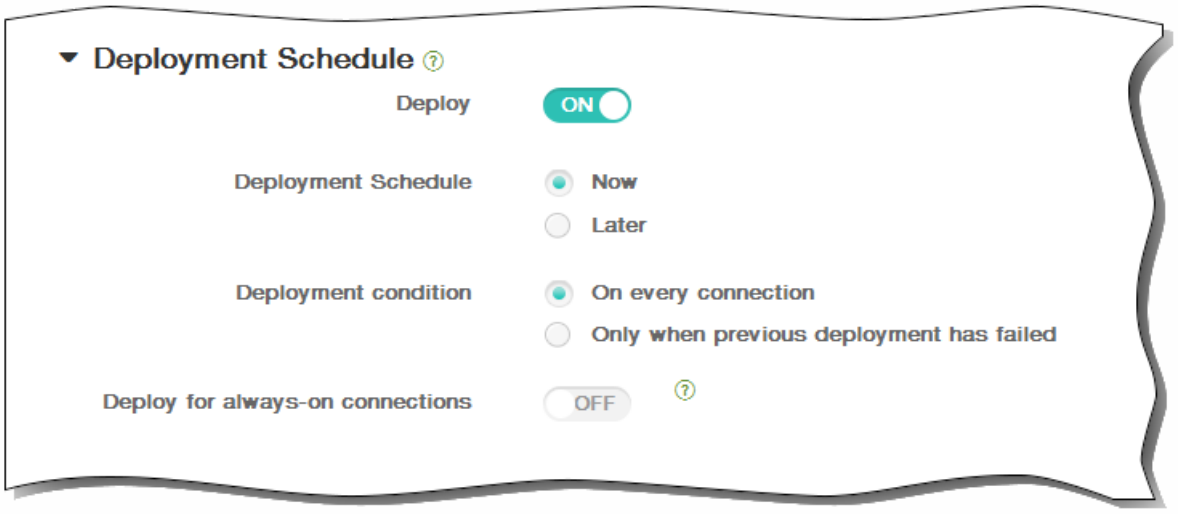


8. 单击下一步。 此时将显示凭据策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

为 Samsung SAFE 添加 Kiosk 设备策略

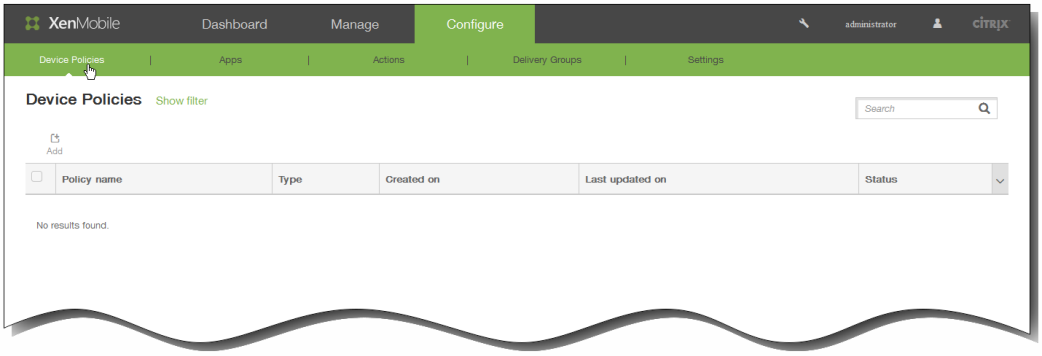
May 05, 2016

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。

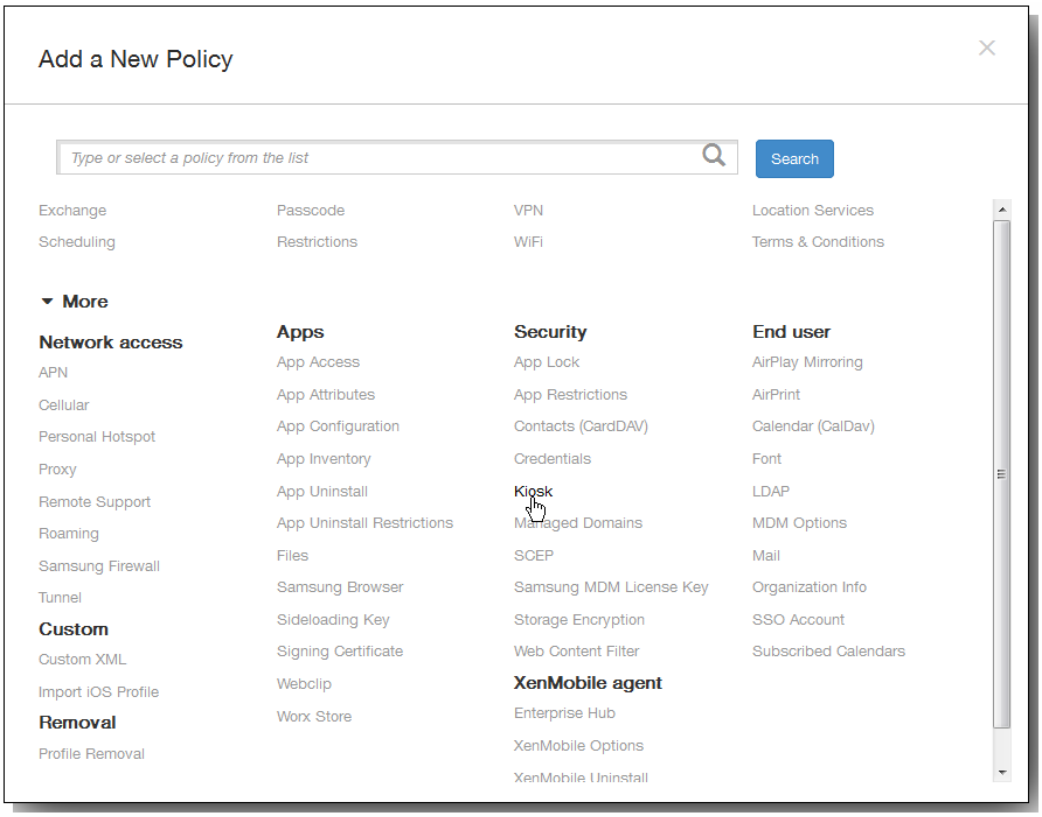
注意：

- 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 4.0 及更高版本。

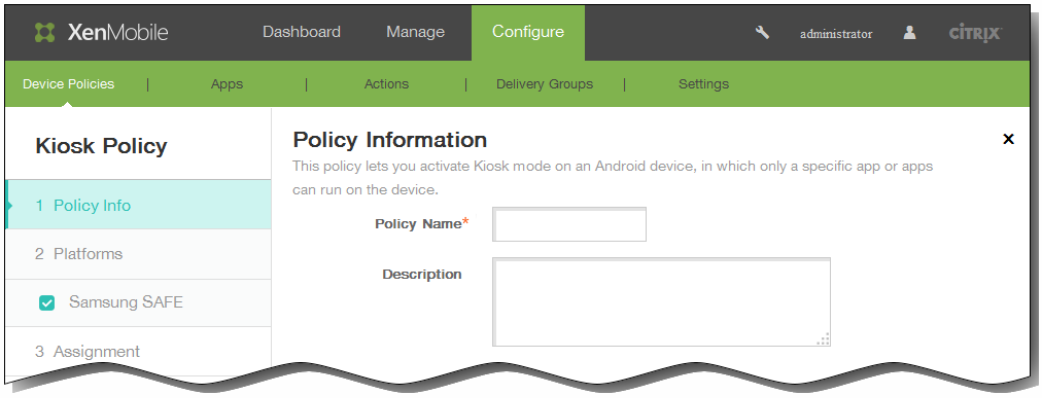
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



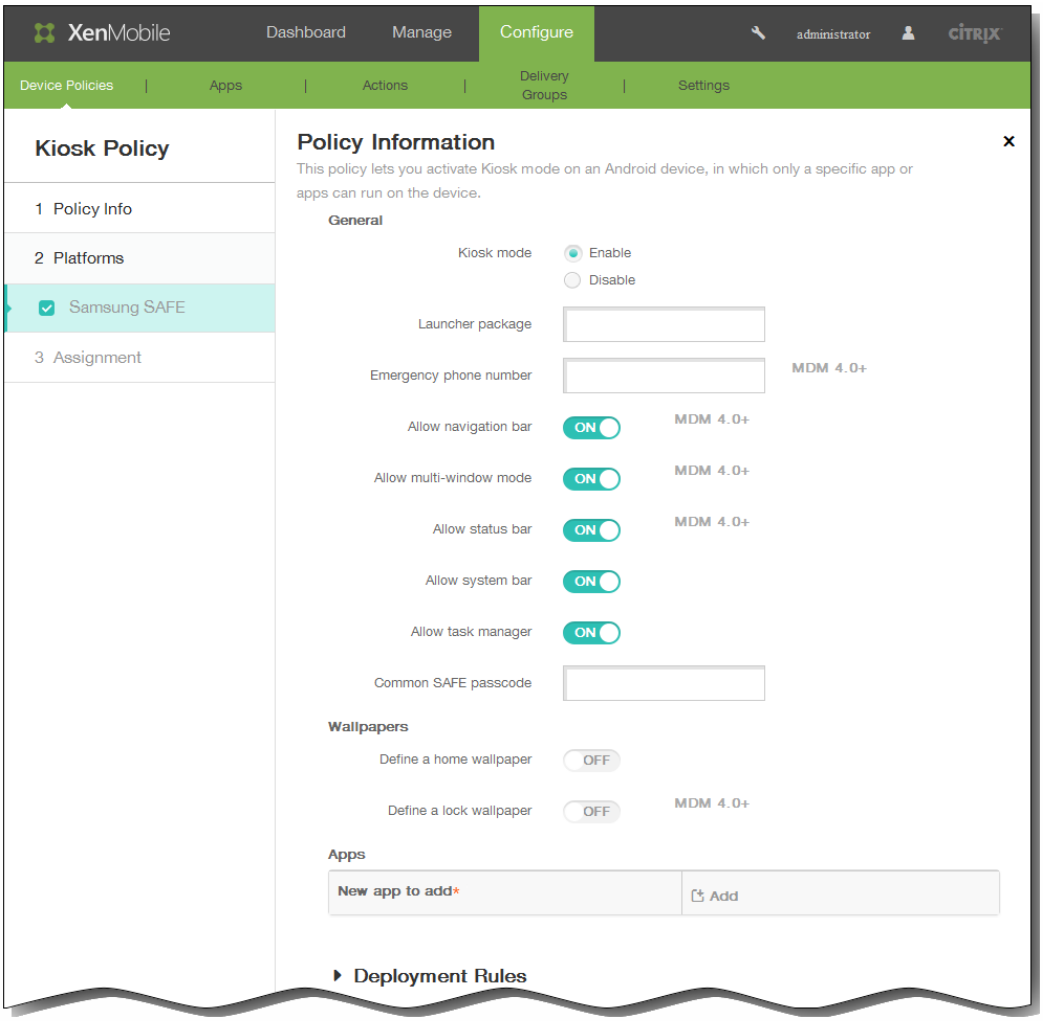
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



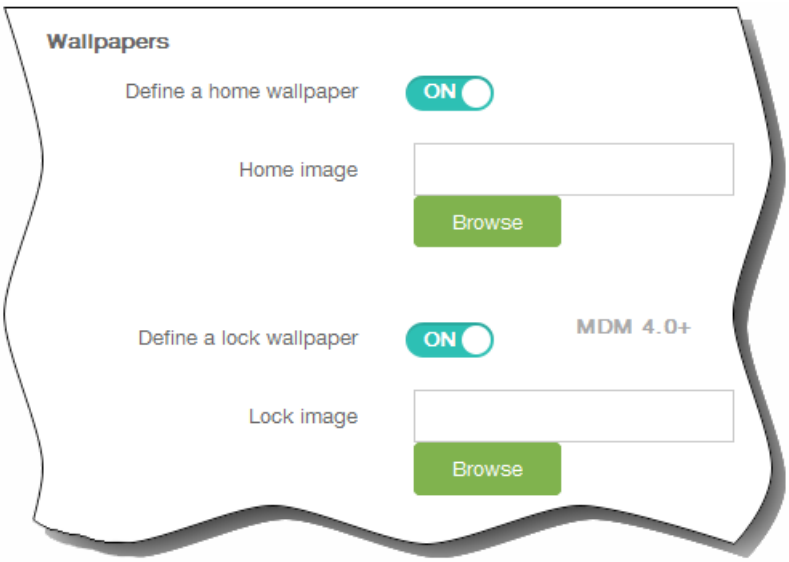
3. 单击更多，然后在安全性下，单击 Kiosk。 此时将显示 Kiosk 策略页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。



6. 在 Samsung SAFE 平台信息页面上，输入以下信息：
    1. 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。
    2. 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。
    3. 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 Samsung Mobile Device Management API 4.0 及更高版本。
    4. 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。
    5. 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。
    6. 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。
    7. 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。
    8. 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。
    9. 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。
    10. 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。
    11. 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。 如果启用了上面的任何一个选项，都会显示一个字段，以允许您通过单击浏览并导航到图片所在的位置来选择自定义图片。



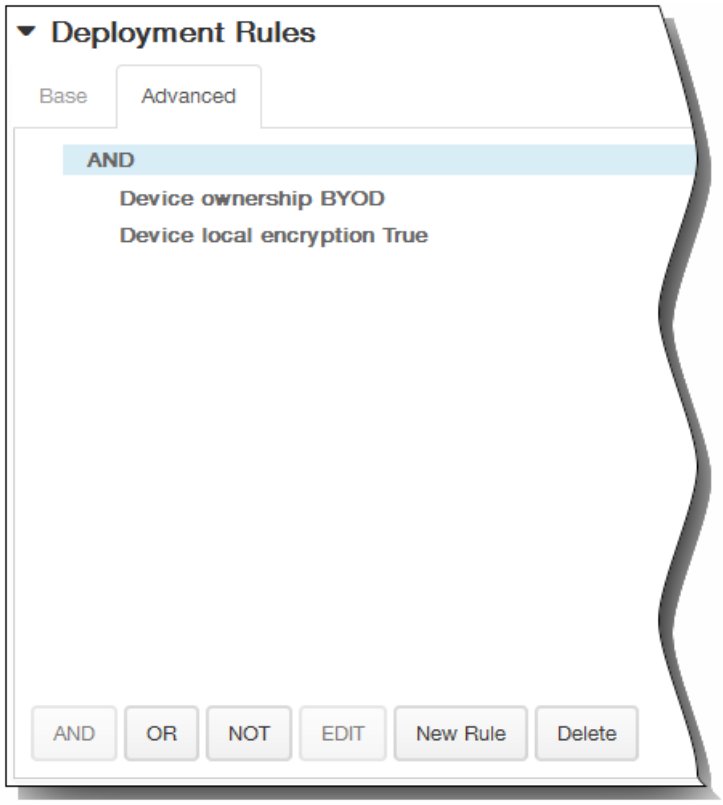
12. 应用程序：单击添加，然后执行以下操作：
    1. 新建要添加的应用程序：输入要添加的应用程序的完整名称。例如，com.android.calendar 允许用户使用 Android 日历应用程序。
    2. 单击添加添加应用程序，或单击取消取消添加应用程序。
    3. 为要添加的每个应用程序重复步骤 i.和 ii.。

    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。

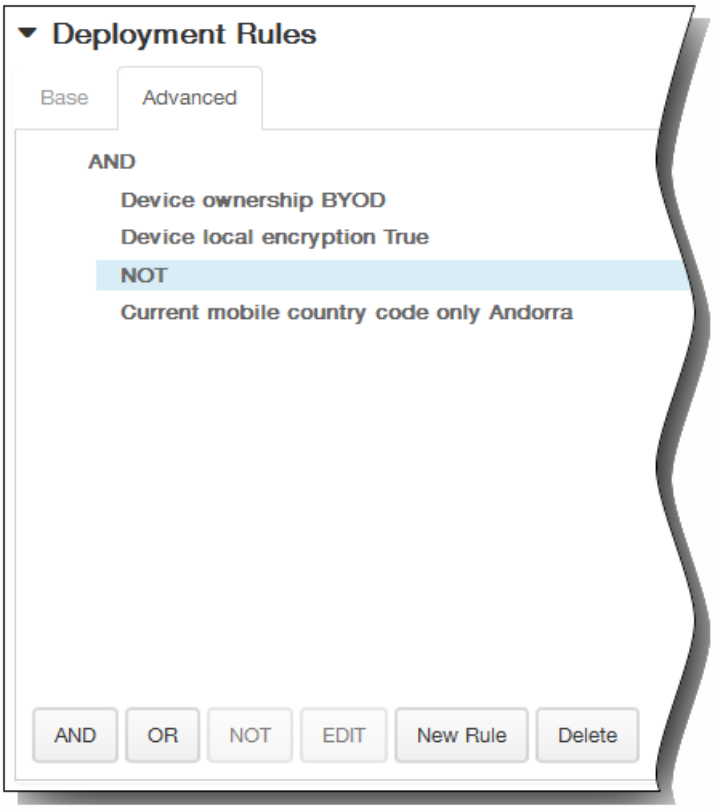
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

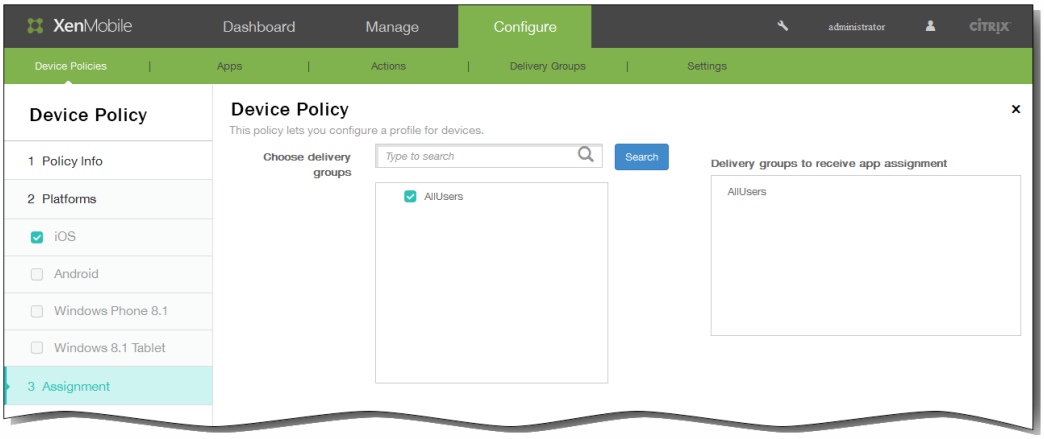


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。

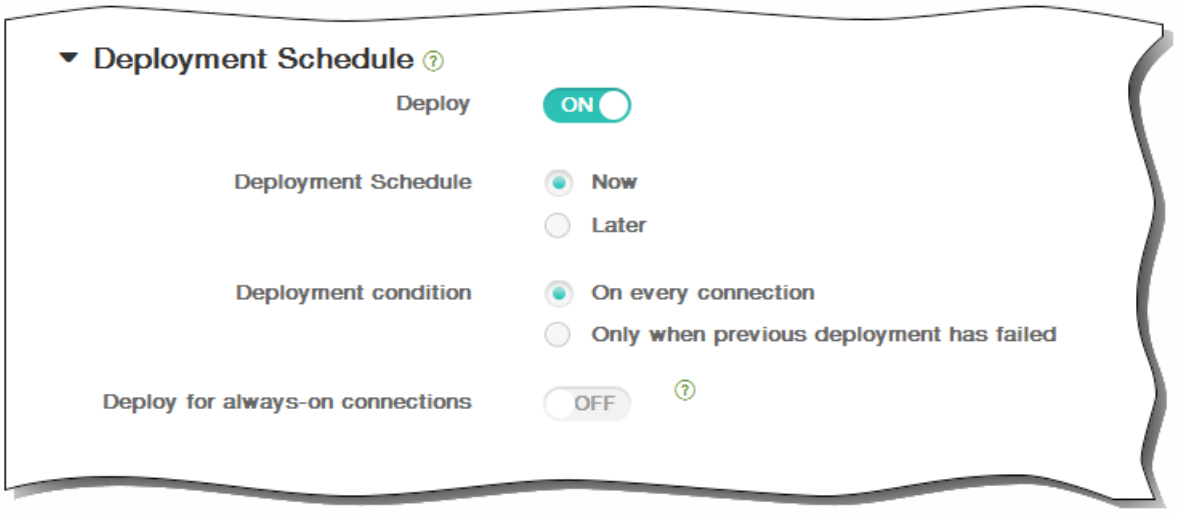


8. 单击下一步。 此时将显示 Kiosk 策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

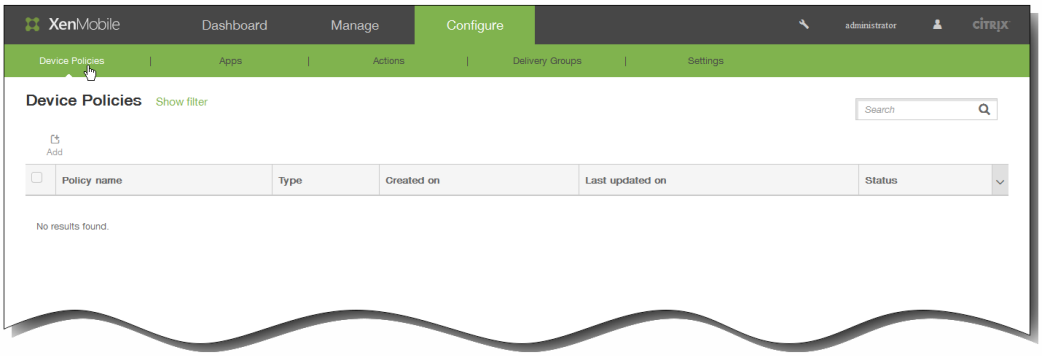
为 iOS 添加字体设备策略

May 05, 2016

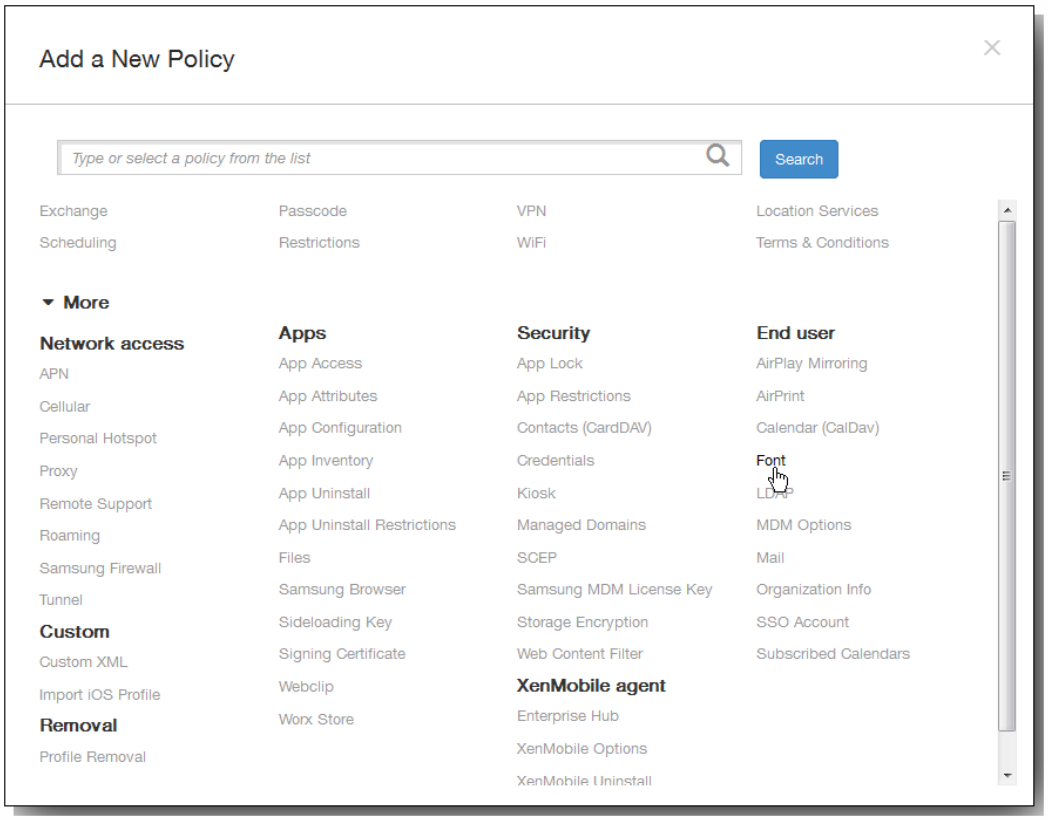
可以在 XenMobile 中添加设备策略以向用户设备添加附加字体。字体必须是 TrueType (.ttf) 或 OpenType (.oft) 字体。不支持字体集合（.ttc 或 .otc）。

注意：此策略仅适用于 iOS 7.0 及更高版本。

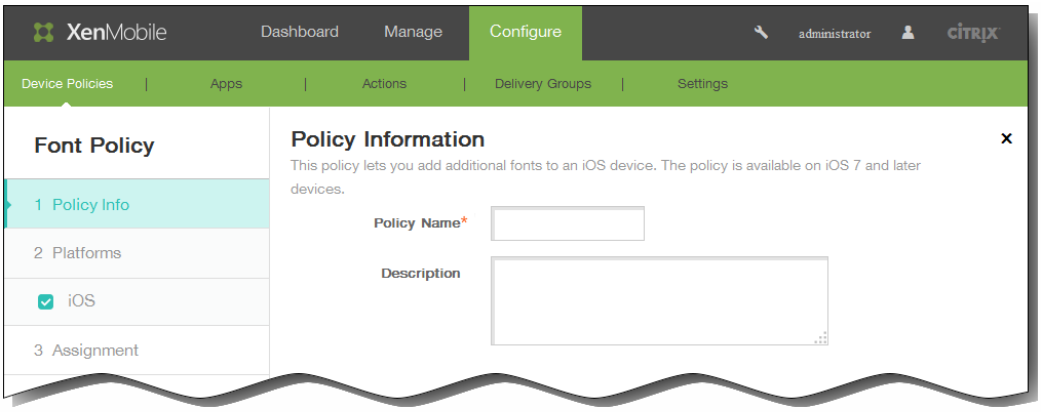
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



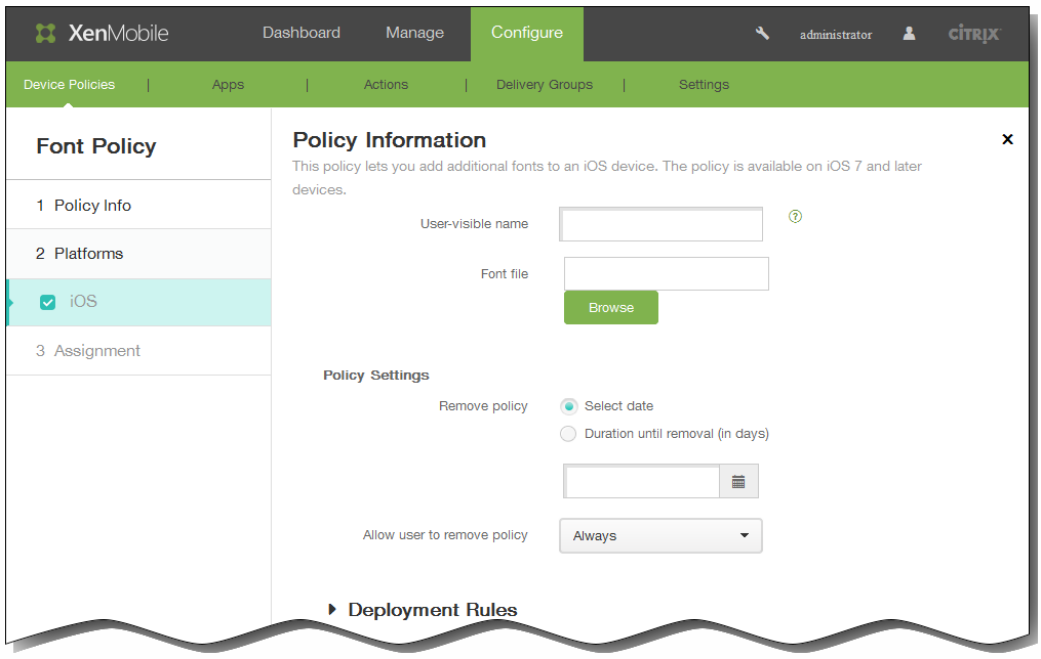
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



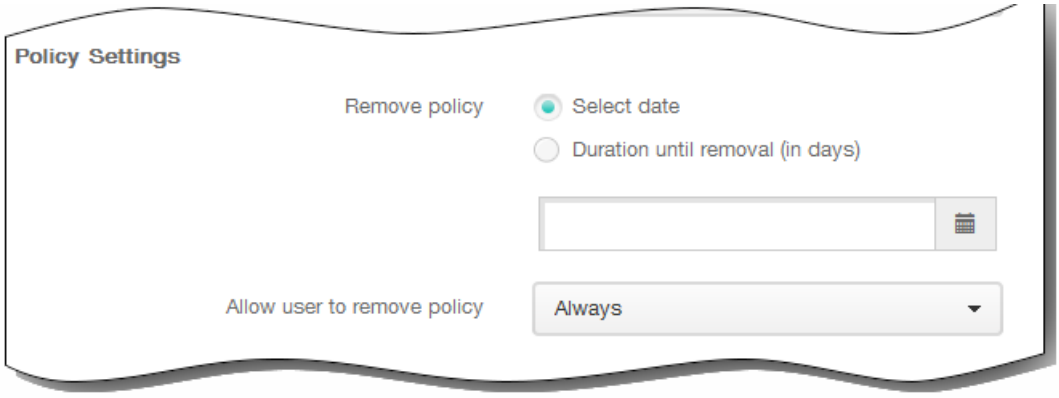
3. 单击更多，然后在最终用户下，单击字体。 此时将显示字体策略页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。

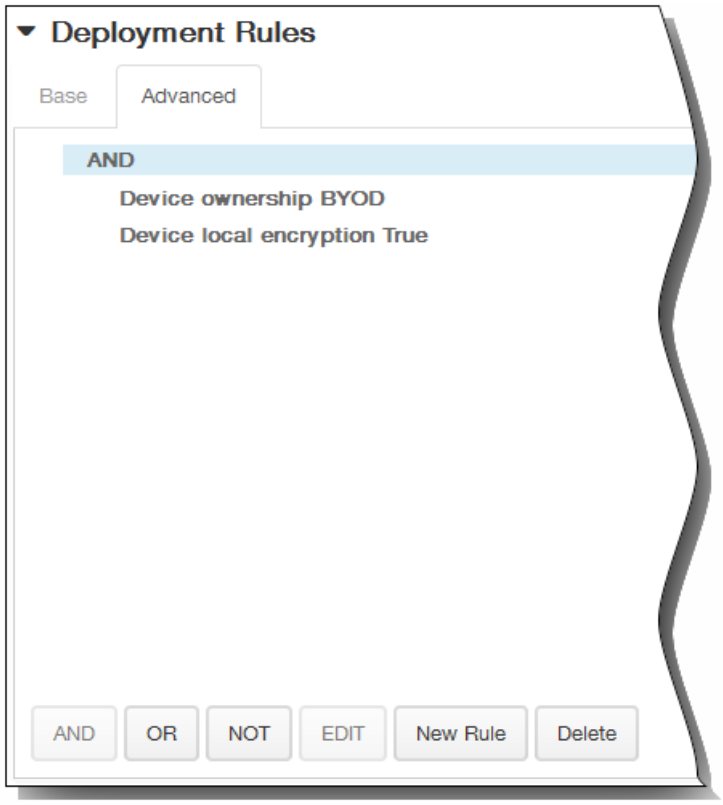


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 用户可见名称：输入用户在其字体列表中看到的名称。
   2. 字体文件：选择要添加到用户设备的字体文件，可以单击浏览，然后导航到该文件的位置。
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



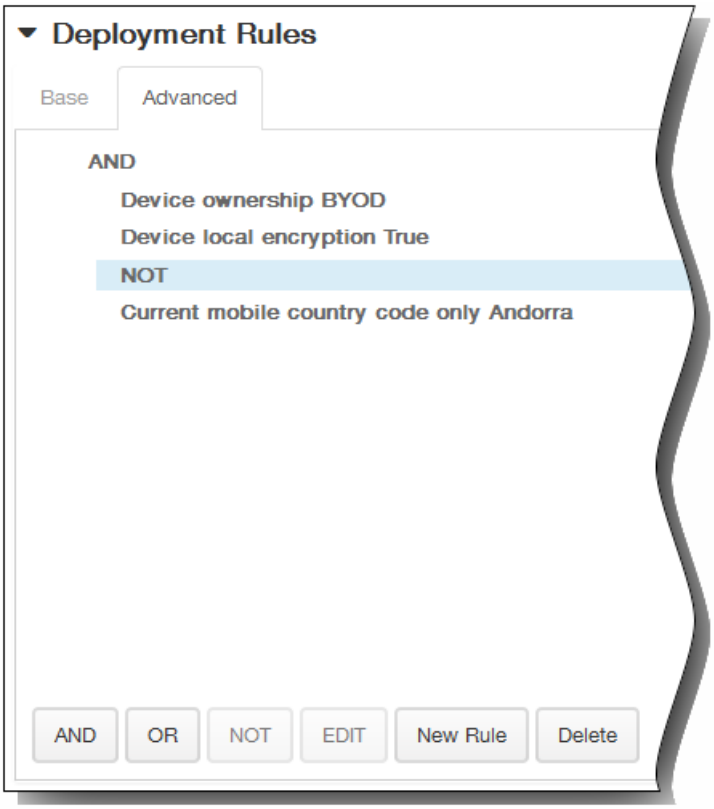
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

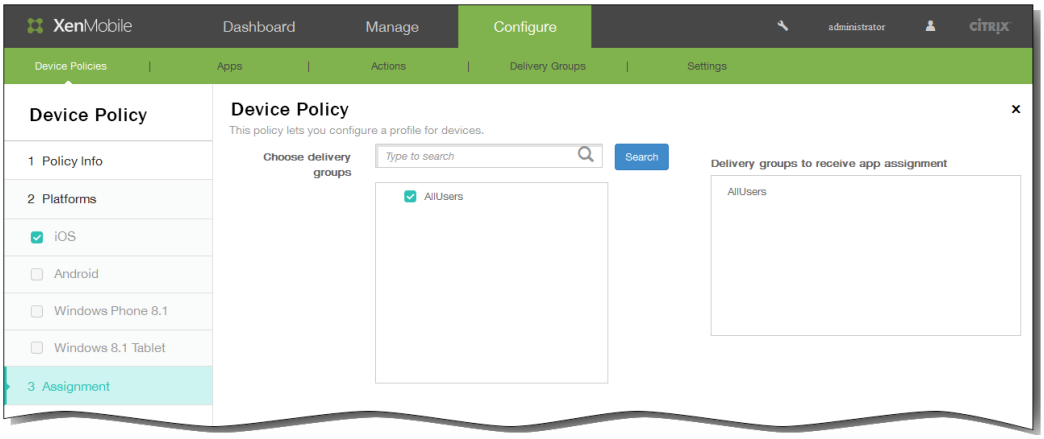


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



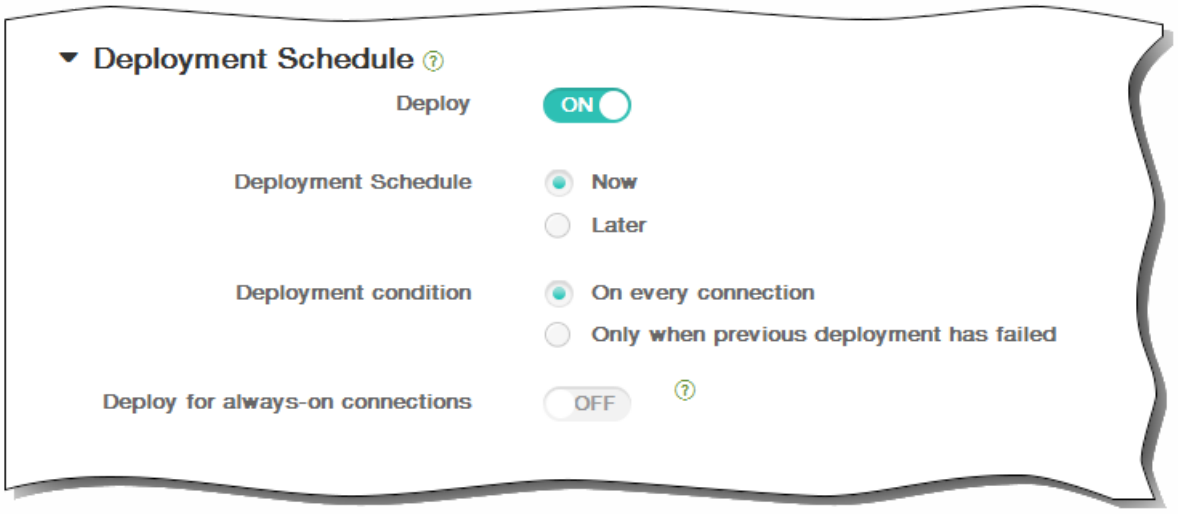
12. 单击下一步。 此时将显示字体策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



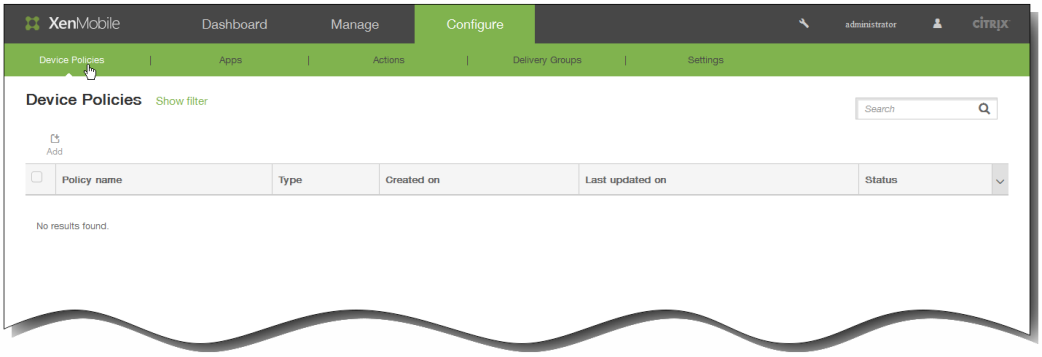
15. 单击保存以保存此策略。

为 iOS 添加组织信息设备策略

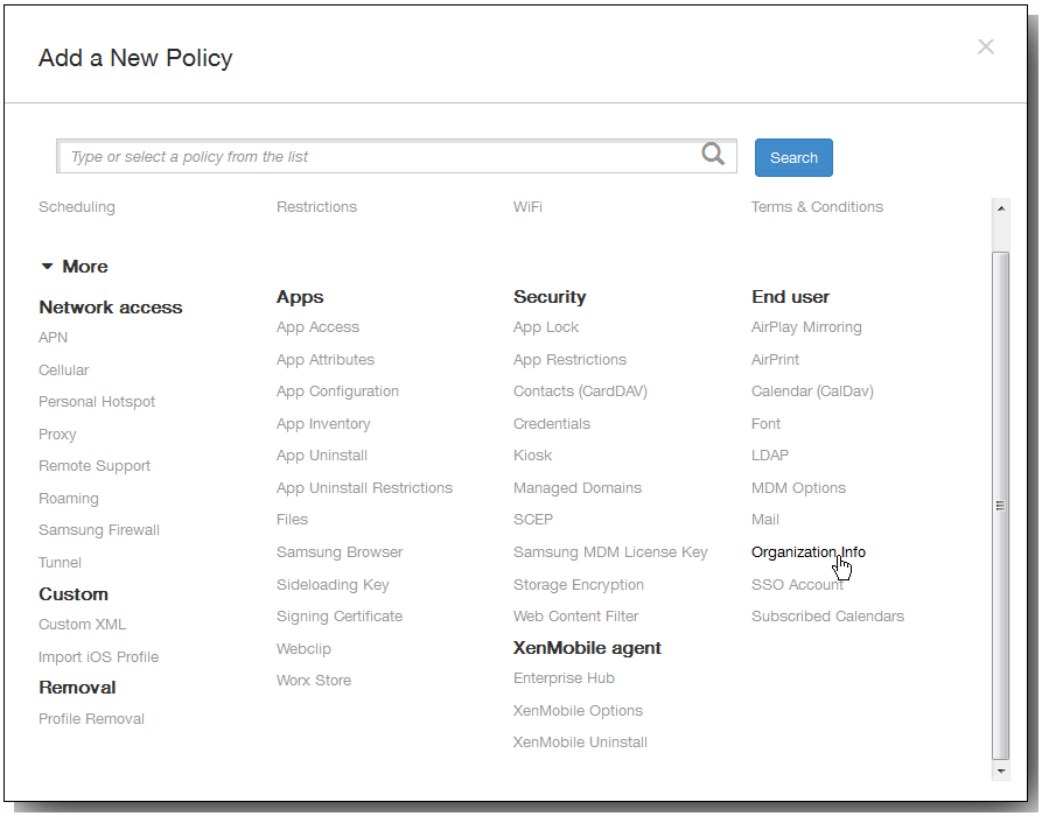
May 05, 2016

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。

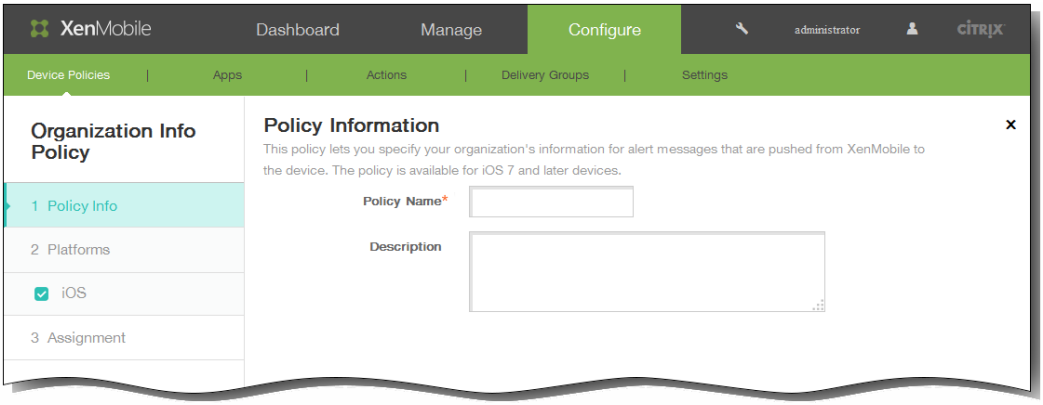
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



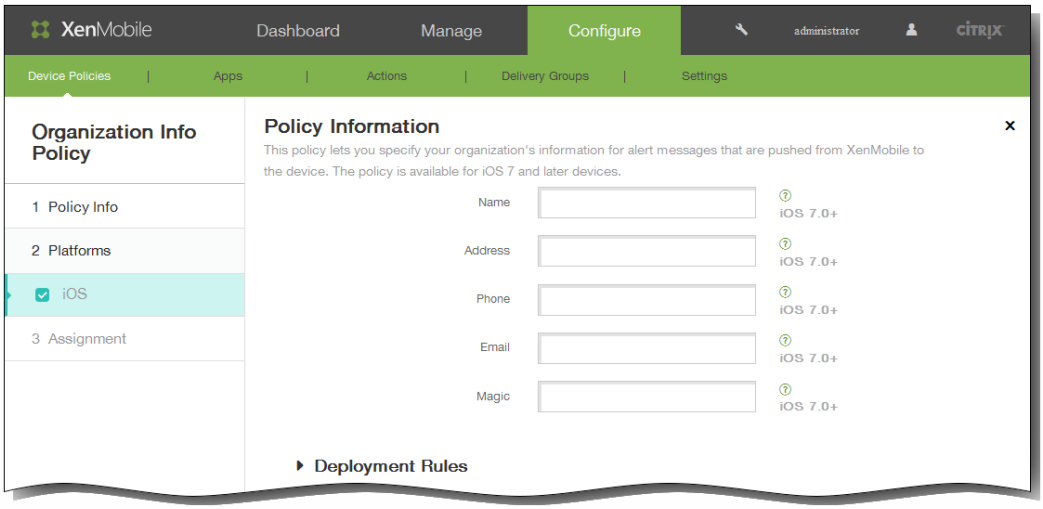
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在最终用户下，单击组织信息。 此时将显示组织信息策略页面。

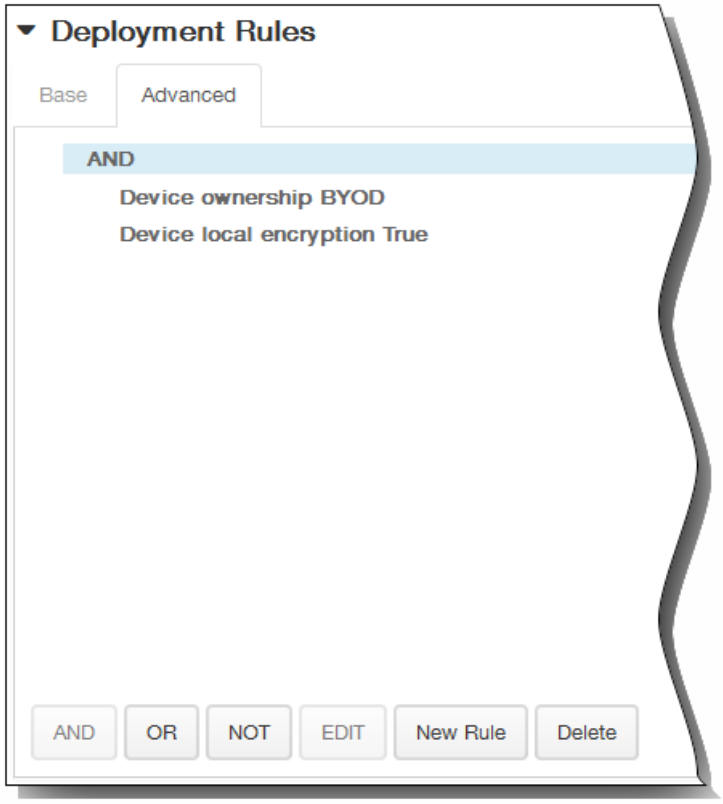


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：如有需要，请键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。



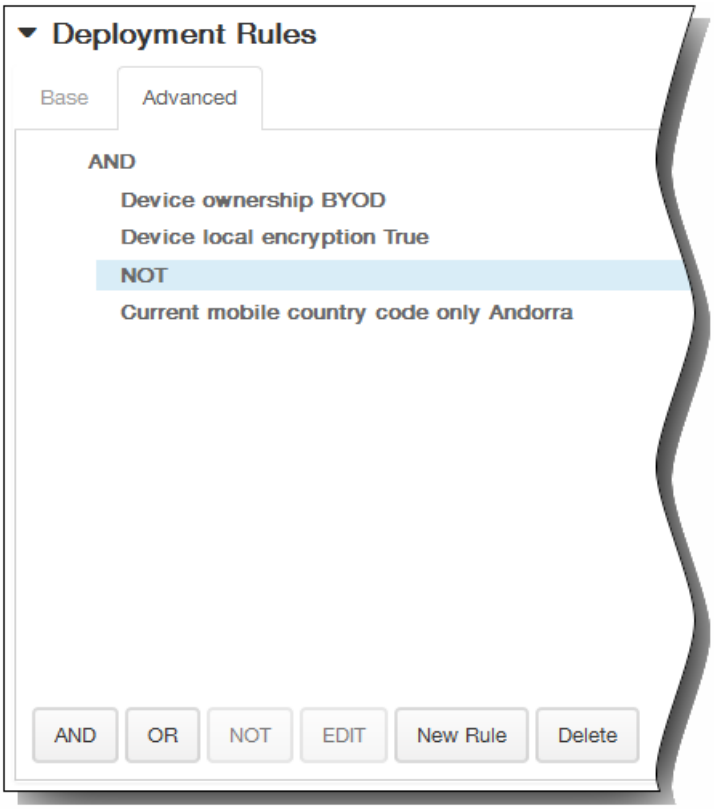
6. 在 iOS 平台信息页面上，输入以下信息：
   1. 名称：键入运行 XenMobile 的组织的名称。
   2. 地址：键入组织的地址。
   3. 电话：键入组织的技术支持电话号码。
   4. 电子邮件：键入技术支持电子邮件地址。
   5. 魔术字：键入用于描述组织托管的服务的单词或短语。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

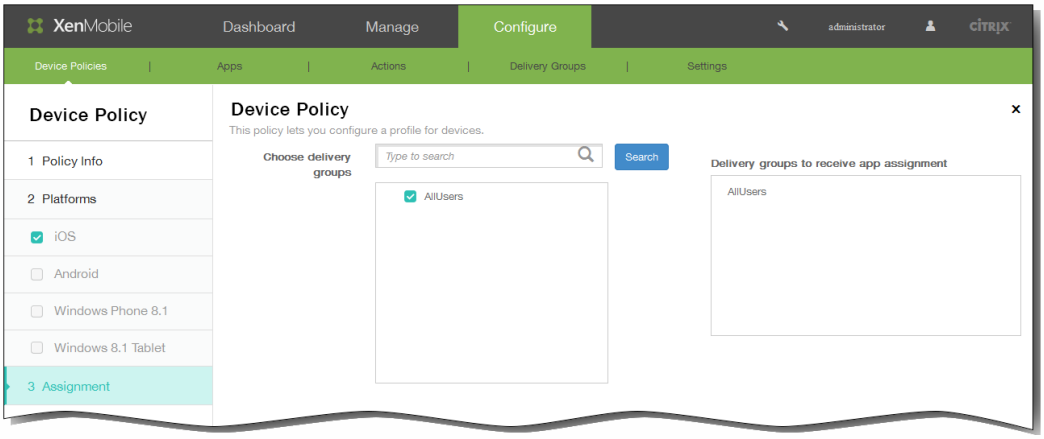


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



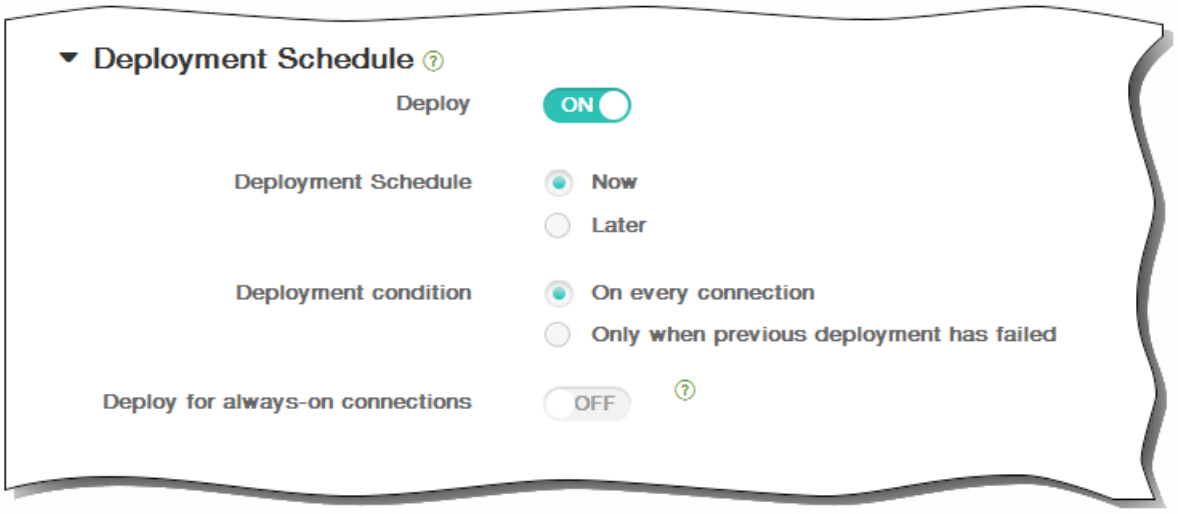
8. 单击下一步。 此时将显示组织信息策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

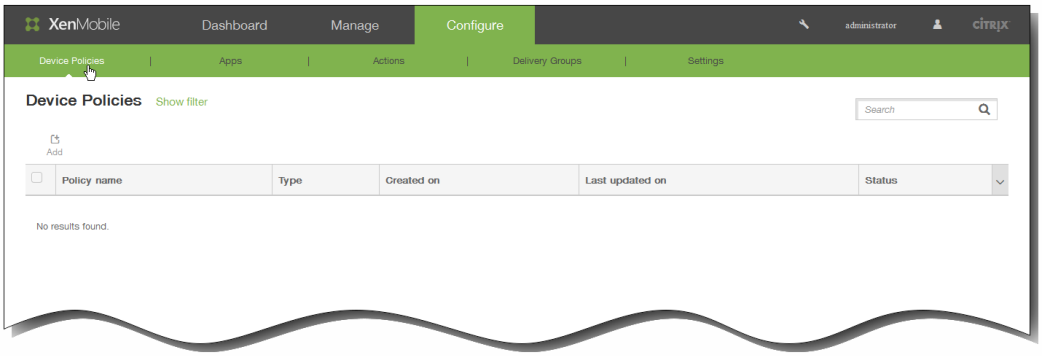
为 iOS 添加 LDAP 设备策略

May 05, 2016

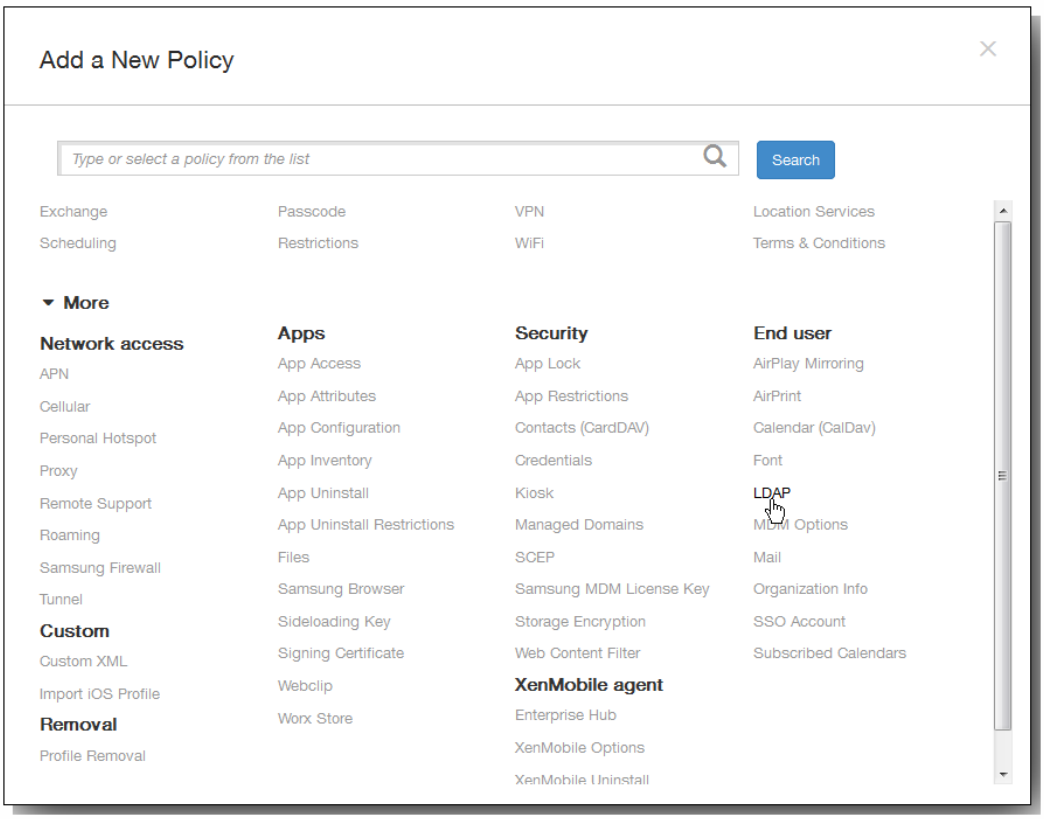
可以在 XenMobile 中为 iOS 设备创建 LDAP 策略，以提供与要使用的 LDAP 服务器有关的信息，包括任何必要的帐户信息。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。

配置此策略之前，您需要提供 LDAP 主机名。

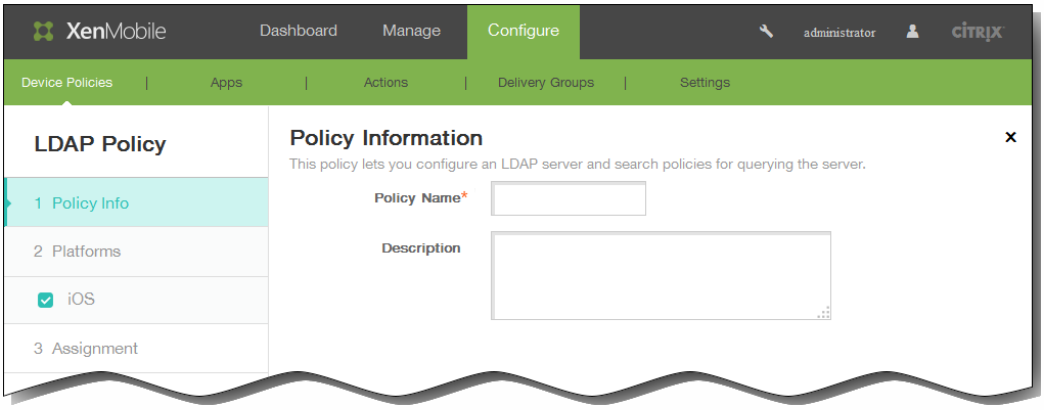
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



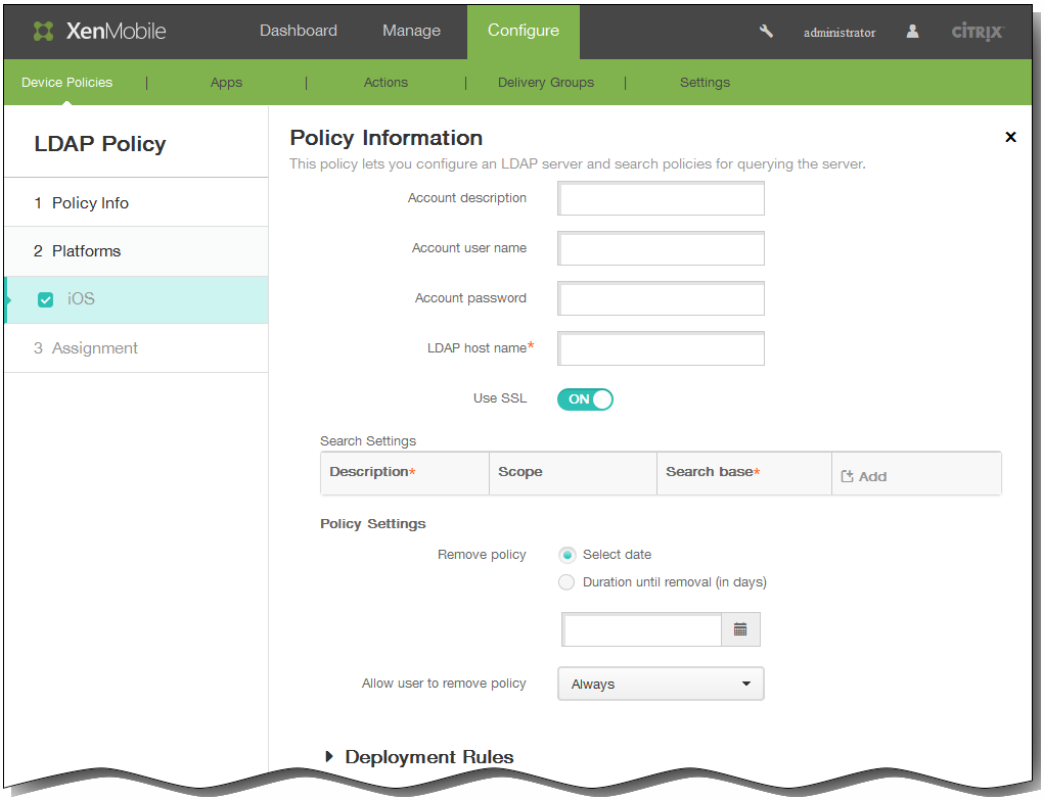
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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：
   1. 策略名称：键入策略的描述性名称。
   2. 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。

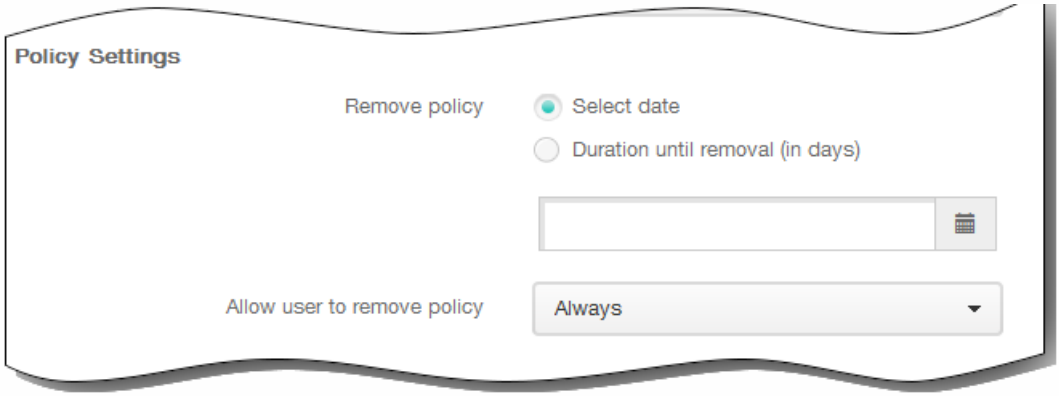


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户说明：输入可选帐户说明。
   2. 帐户用户名：输入可选用户名。
   3. 帐户密码：输入可选密码。 此选项仅适用于加密的配置文件。
   4. LDAP 主机名：输入 LDAP 服务器的主机名。 此字段为必填字段。

5. 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。
6. 搜索设置：单击添加，然后执行以下操作：
   注意：您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才能使用帐户。
   1. 说明：输入搜索设置的说明。此字段为必填字段。
   2. 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。
      - 基础搜索搜索基础指向的节点。
      - 一级搜索基础节点及其下一级节点。
      - 子树搜索基础节点及其所有子节点，而无论深度为何。
   3. 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。
   4. 单击添加添加搜索设置，或单击取消取消添加搜索设置。
   5. 为要添加的每个应用程序重复步骤 i.至步骤 iv.。

   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。
7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。

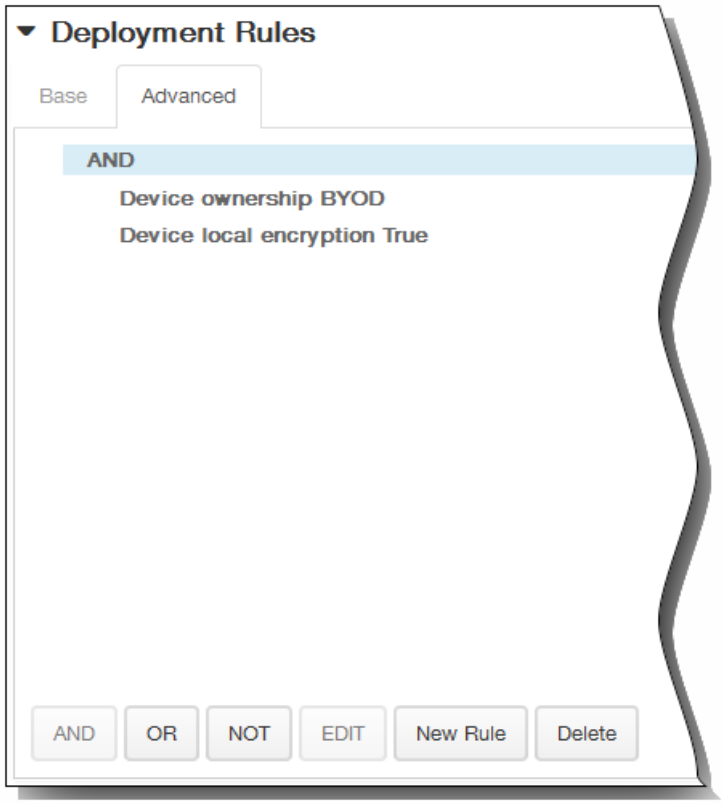


11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。

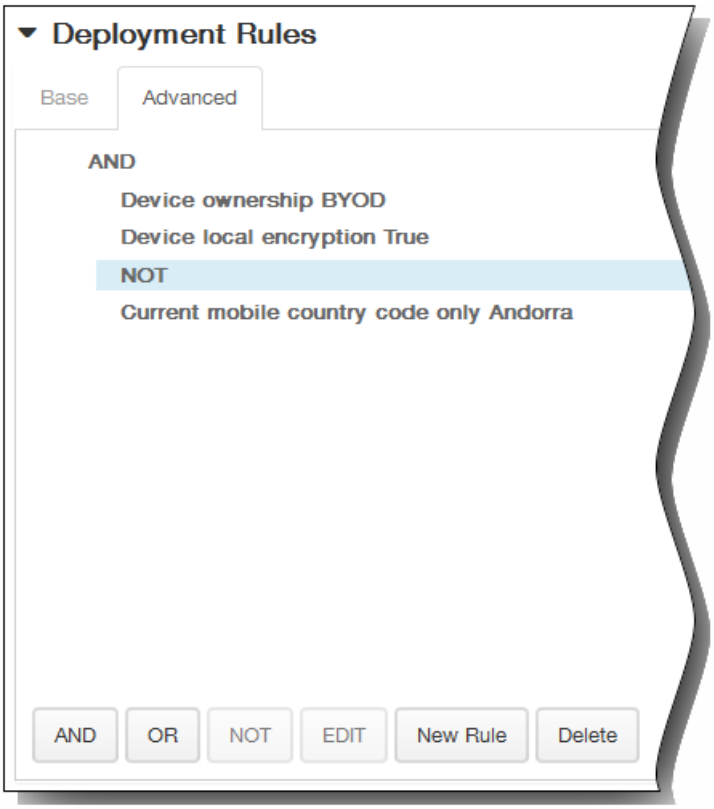
2. 单击新建规则以定义条件。
3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。

2. 单击高级选项卡以使用布尔选项组合规则。

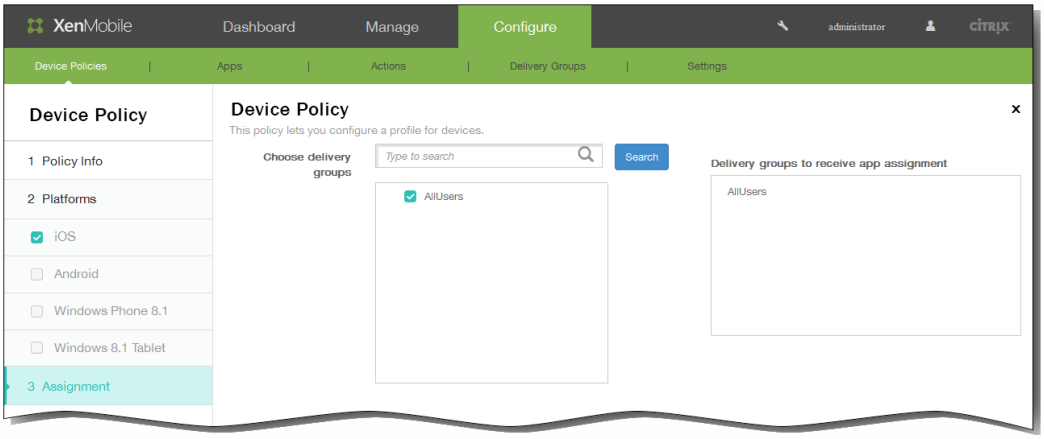


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



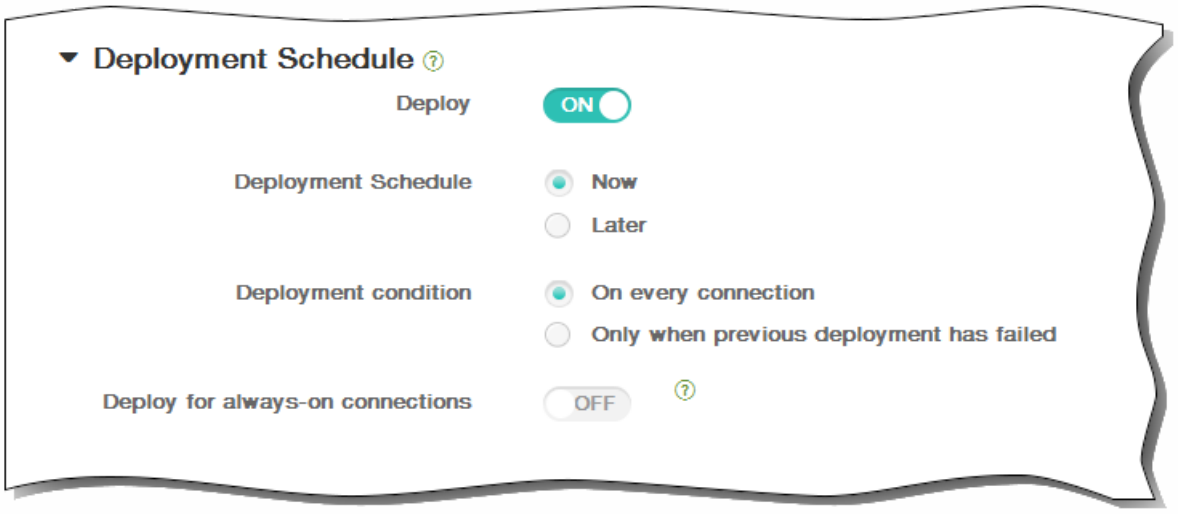
12. 单击下一步。 此时将显示 LDAP 策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



15. 单击保存以保存此策略。

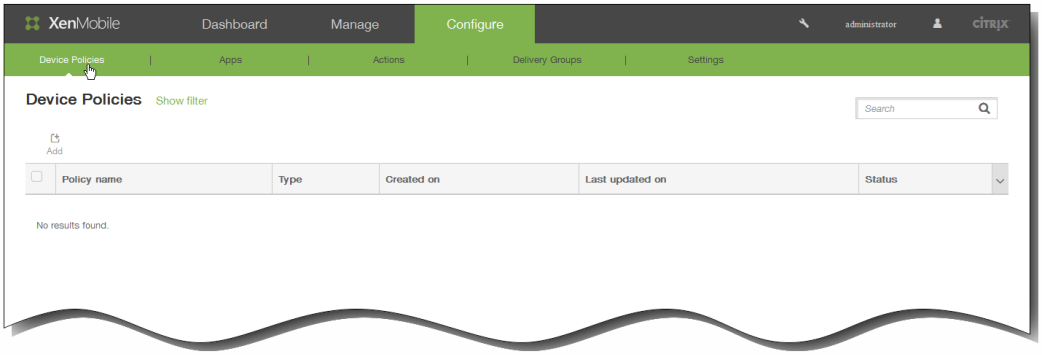
添加适用于 iOS 的 Single Sign-On 帐户设备策略

May 05, 2016

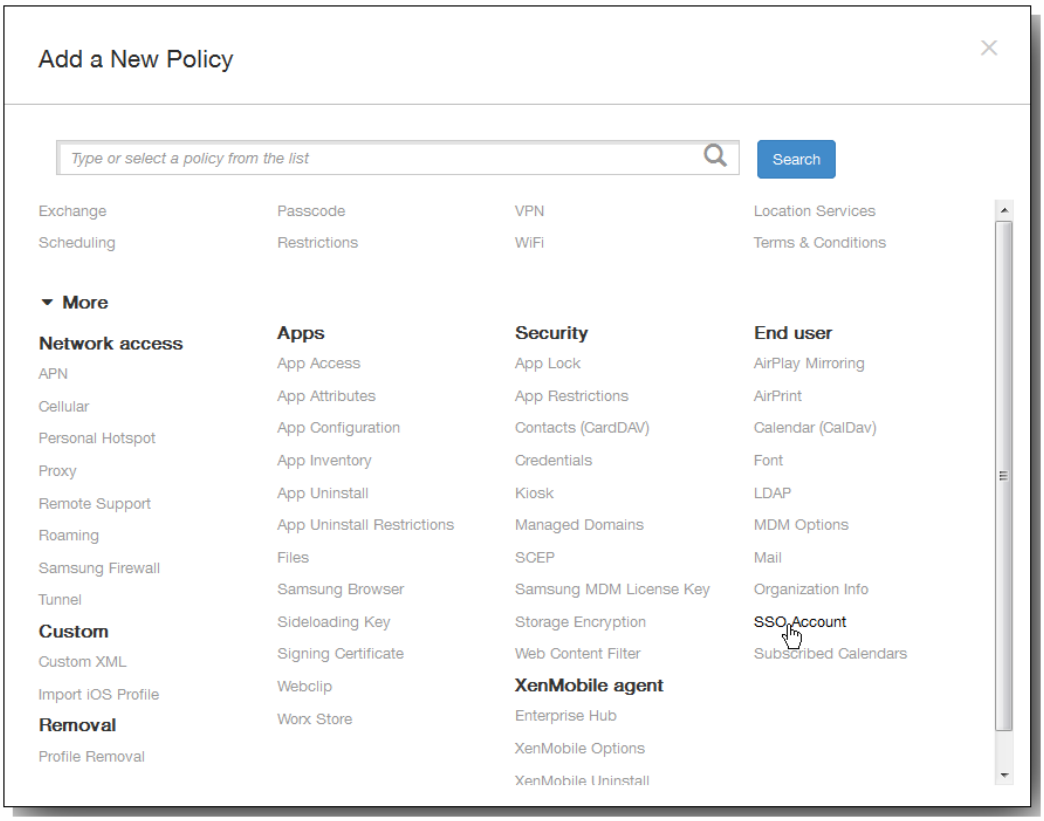
在 XenMobile 中创建 Single Sign-On (SSO) 帐户，使用户只需登录设备一次，即可从各种应用程序访问 XenMobile 和内部的公司资源。用户无需在设备上存储任何凭据。可以跨应用程序（包括 App Store 中的应用程序）使用此 SSO 帐户企业用户凭据。此策略专为 Kerberos 身份验证后端设计。

注意：此策略仅适用于 iOS 7.0 及更高版本。

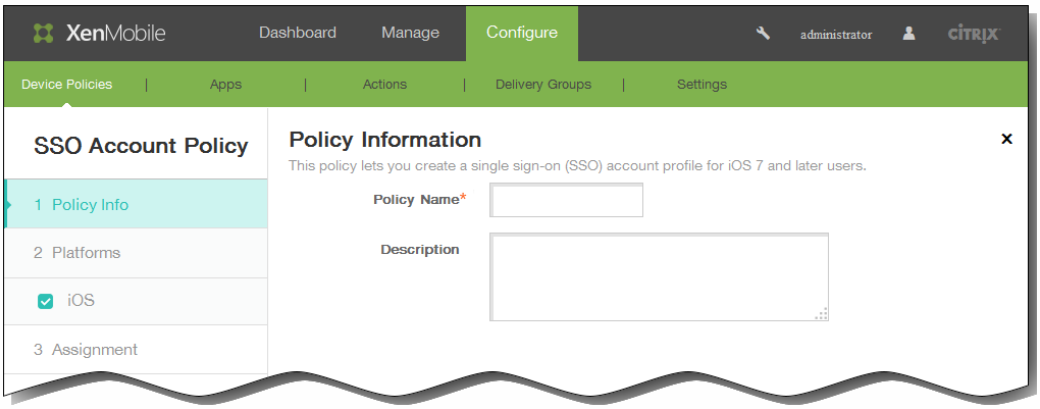
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



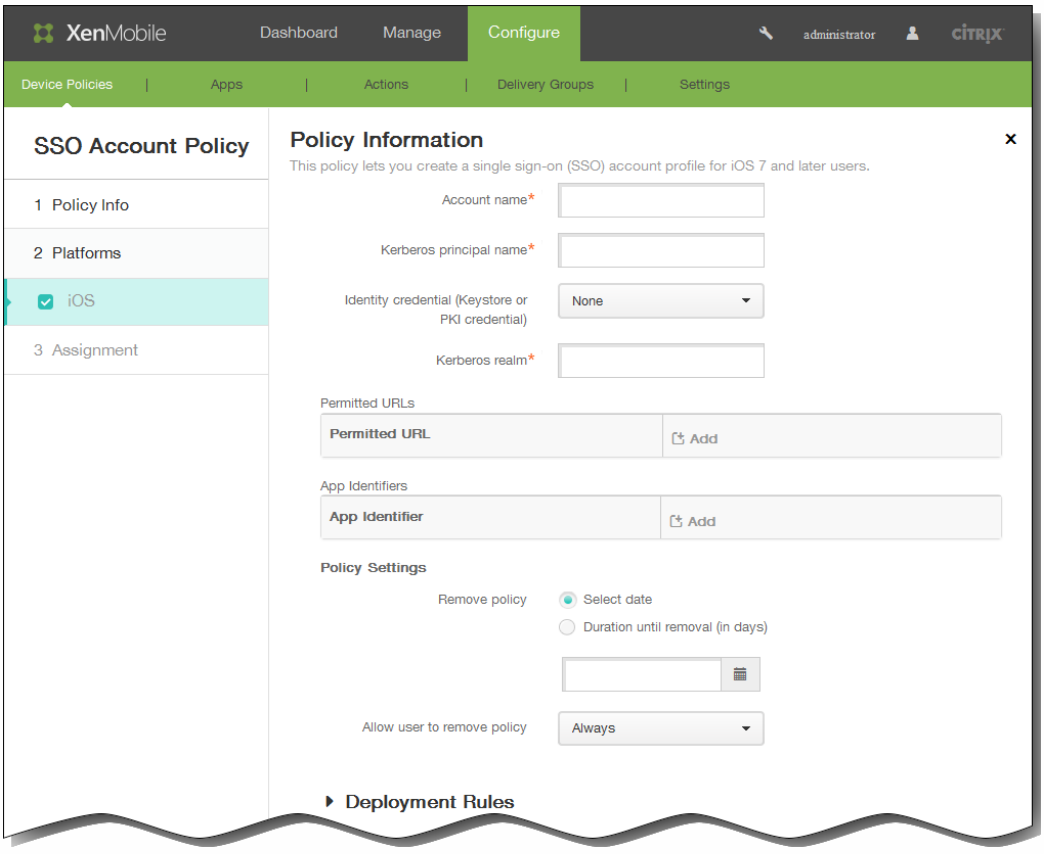
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在最终用户下面，单击 SSO 帐户。 此时将显示 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：
   1. 策略名称：键入策略的描述性名称。
   2. 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。

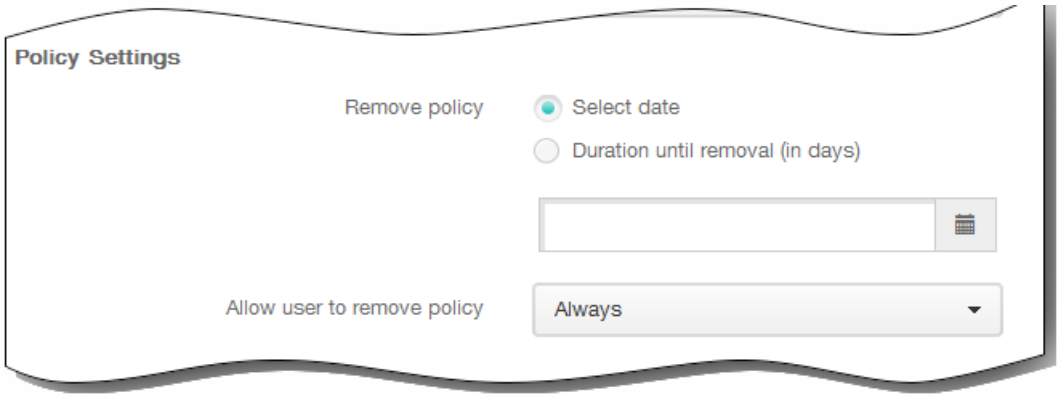


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户名称：输入显示在用户设备上的 Kerberos SSO 帐户名称。 此字段为必填字段。
   2. Kerberos 主体名称：输入 Kerberos 主体名称。 此字段为必填字段。

3. 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。
4. 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。
5. 允许访问的 URL：单击添加，然后执行以下操作：
    1. 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。
    2. 单击添加以添加 URL，或单击取消以取消添加 URL。
    3. 为要添加的每个应用程序标识符重复步骤 i.和 ii.。
6. 应用程序标识符：单击添加，然后执行以下操作：
    1. 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。
       注意：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。
    2. 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。
    3. 为要添加的每个应用程序标识符重复步骤 i.和 ii.。

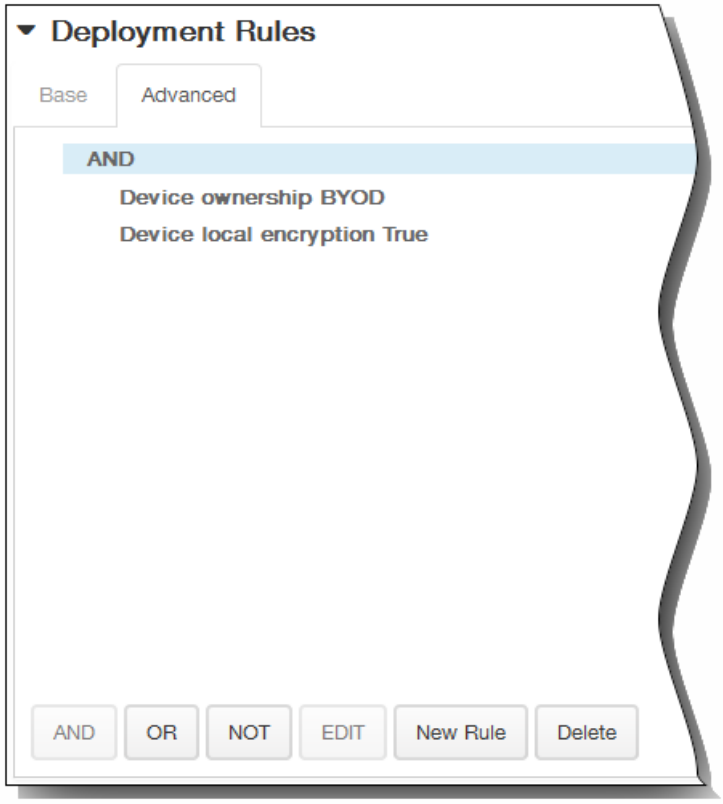
    注意：要删除现有 URL 或应用程序标识符，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击删除以删除列表，或单击取消以保留此列表。
    要编辑现有 URL 或应用程序标识符，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



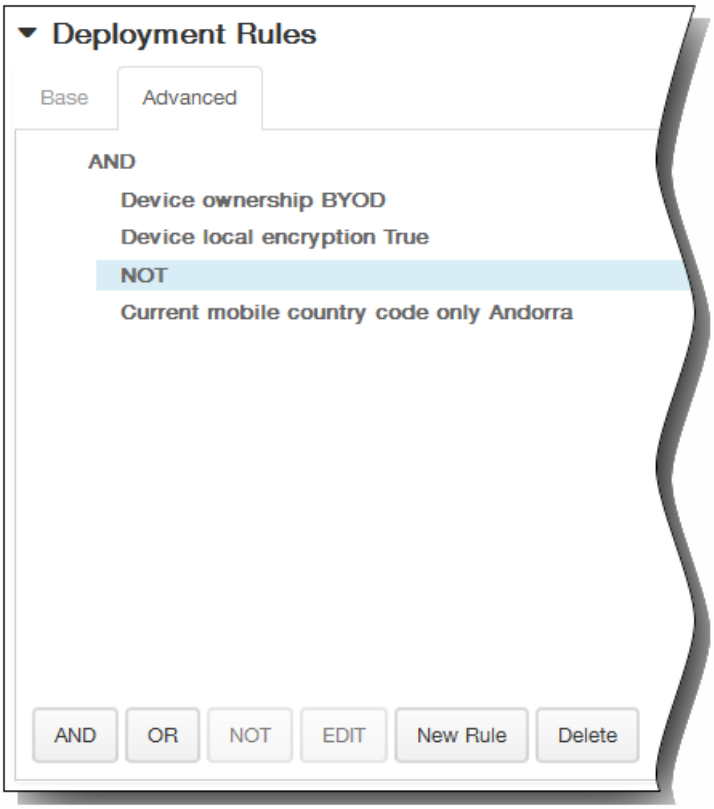
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

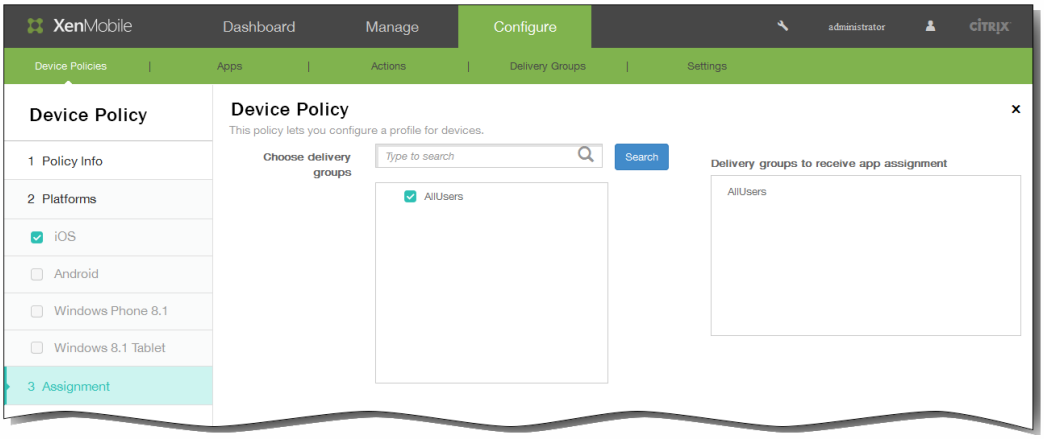


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



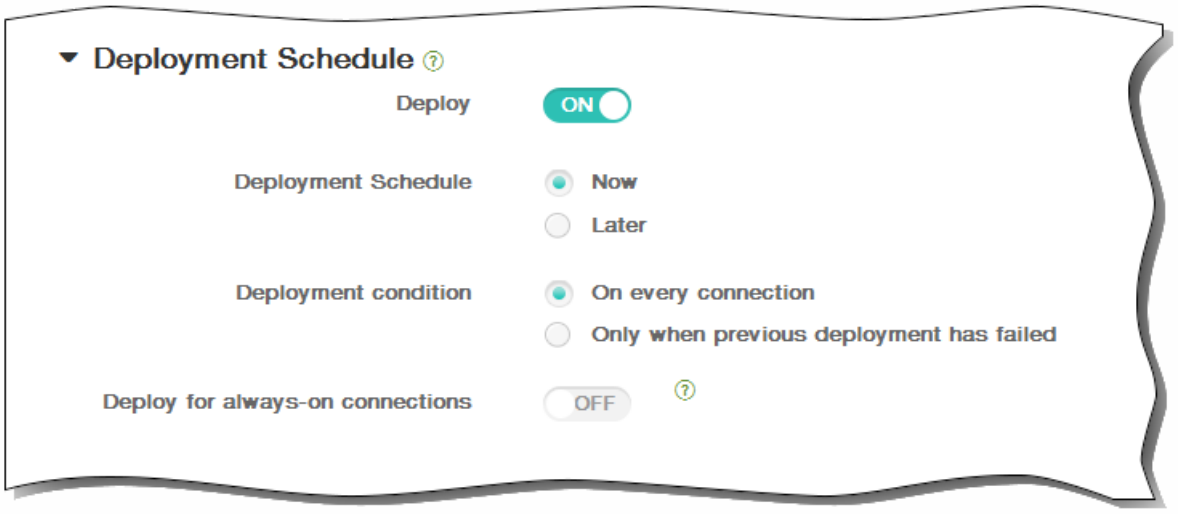
12. 单击下一步。 此时将显示 SSO 帐户策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



15. 单击保存以保存此策略。

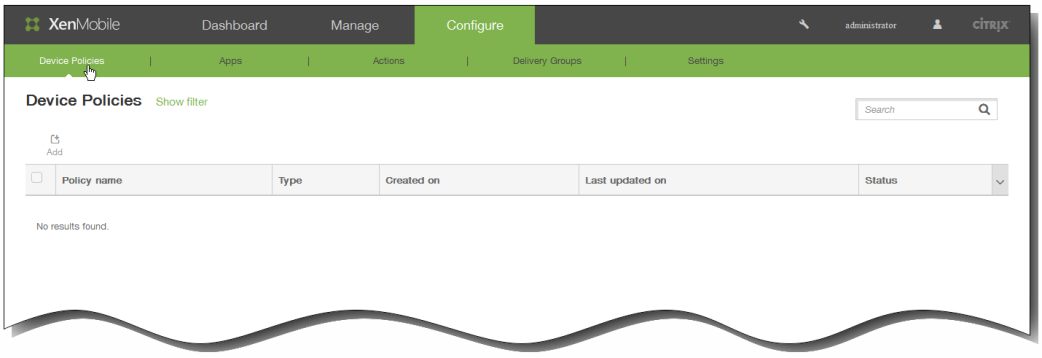
添加适用于 iOS 的已订阅的日历设备策略

May 05, 2016

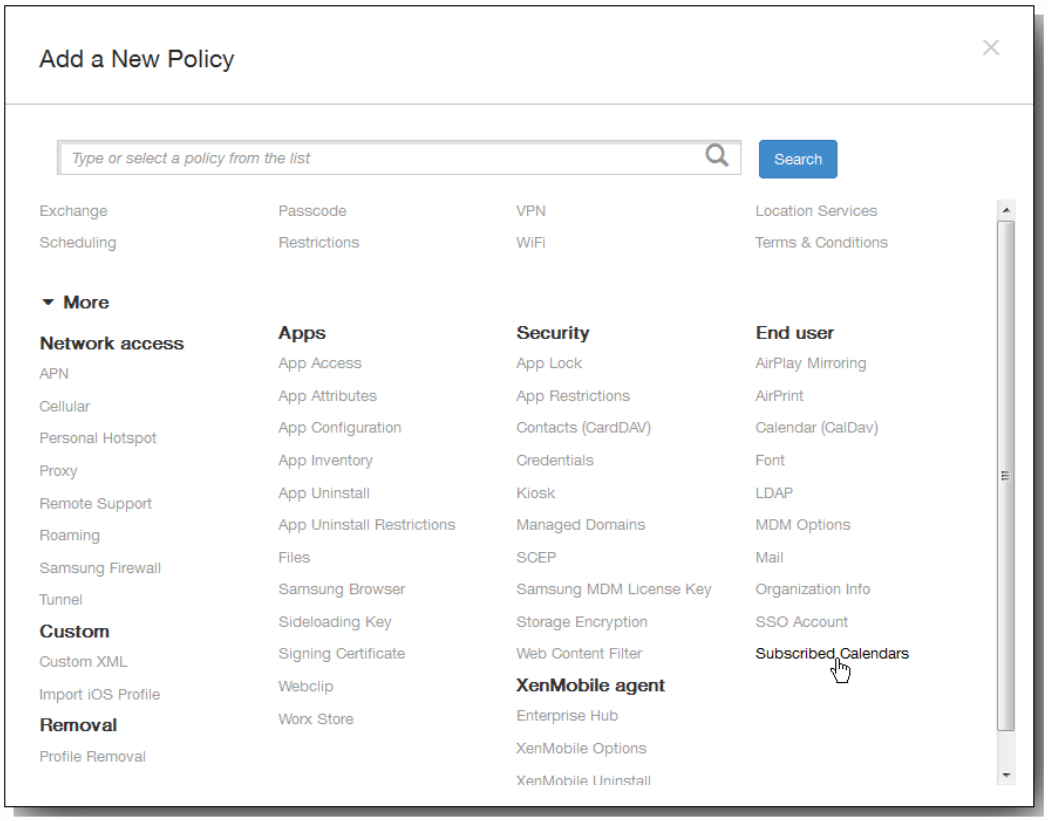
您可以在 XenMobile 中添加一个设备策略，以便在用户的 iOS 设备上向日历列表中添加已订阅的日历。www.apple.com/downloads/macosx/calendars 提供了您可以订阅的公共日历列表。

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。

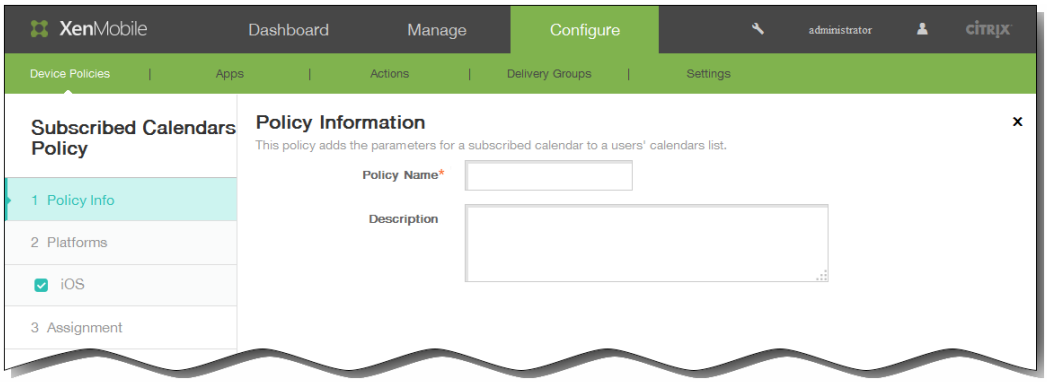
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



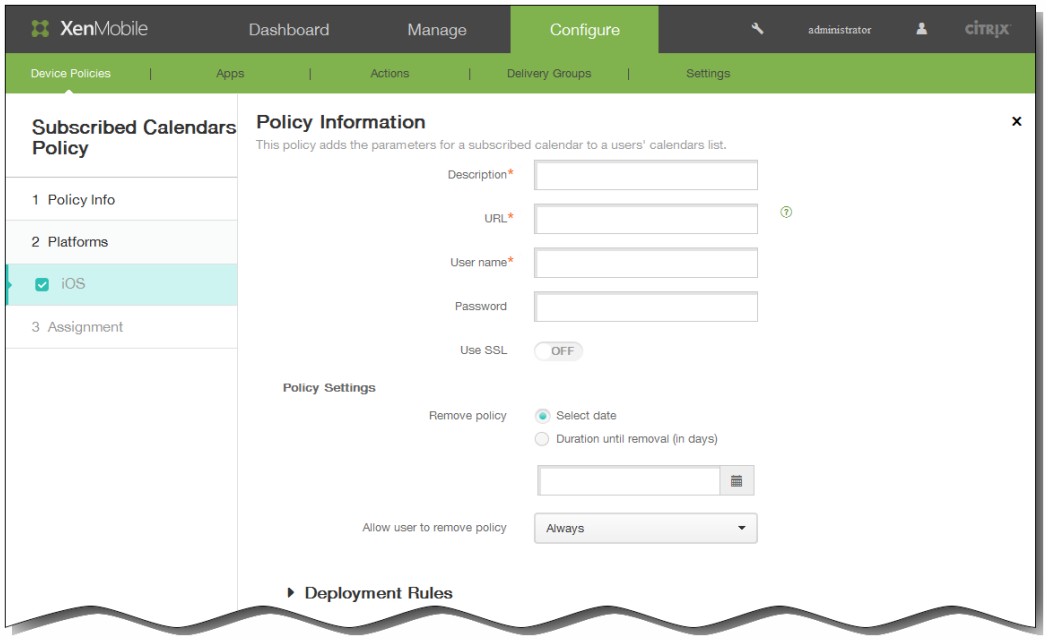
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



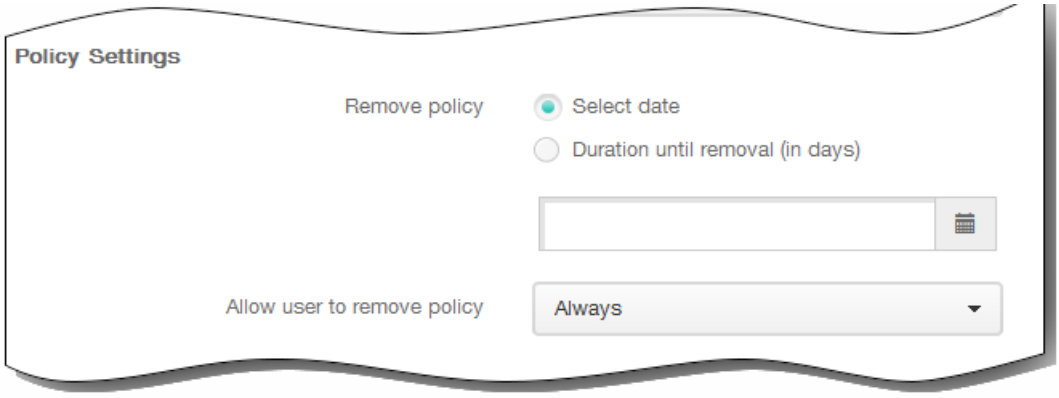
3. 单击更多，然后在最终用户下面，单击已订阅的日历。 此时将显示“已订阅的日历”策略页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。

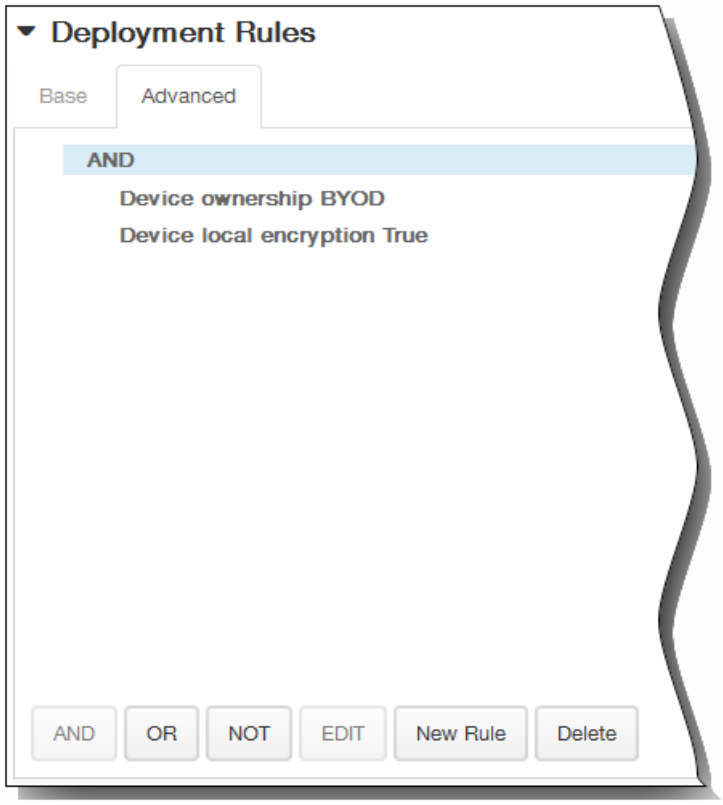


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 说明：输入日历的说明。 此字段为必填字段。
   2. URL：输入日历 URL。 可以输入 iCalendar 文件 (.ics) 的 webcal:// URL 或 http:// 链接。 此字段为必填字段。
   3. 用户名：输入用户的登录名称。 此字段为必填字段。
   4. 密码：输入可选用户密码。
   5. 使用 SSL：选择是否使用安全套接字层连接到日历。 默认设置为关
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



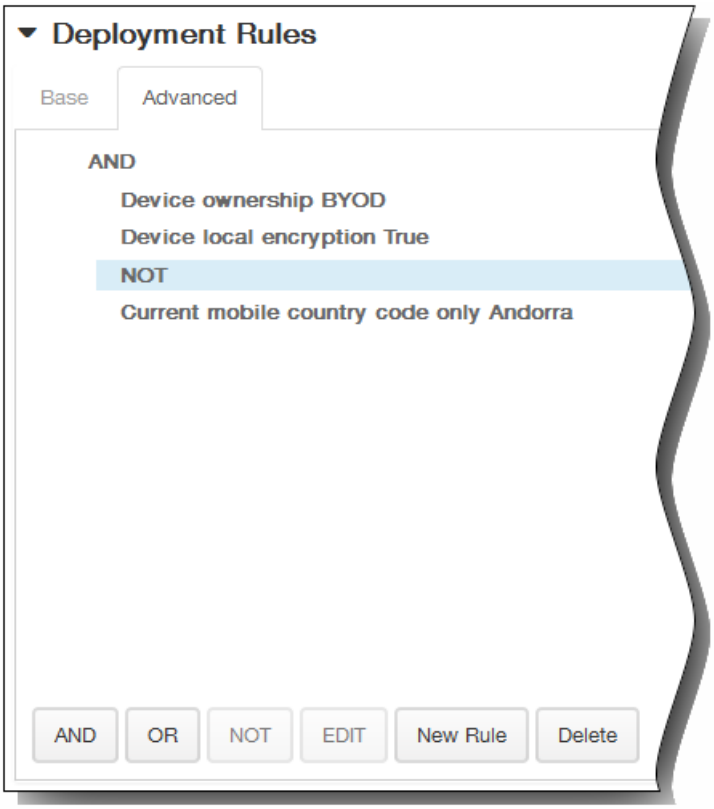
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

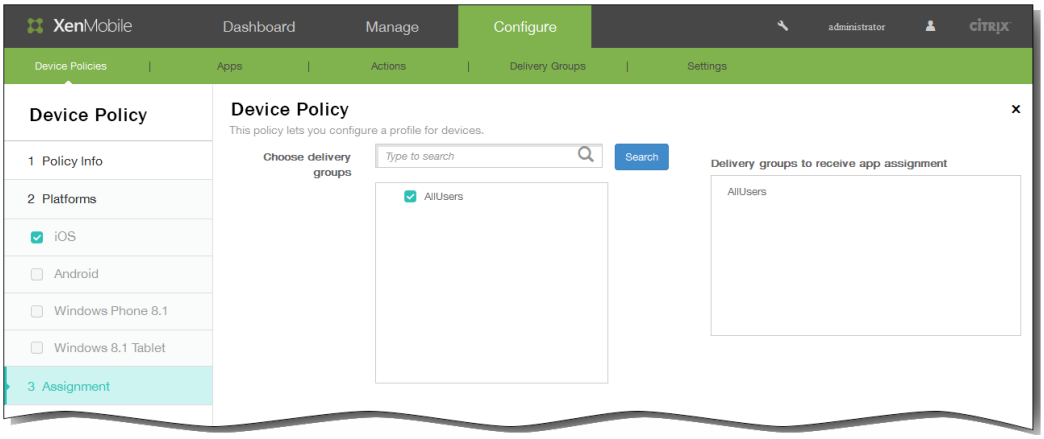


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



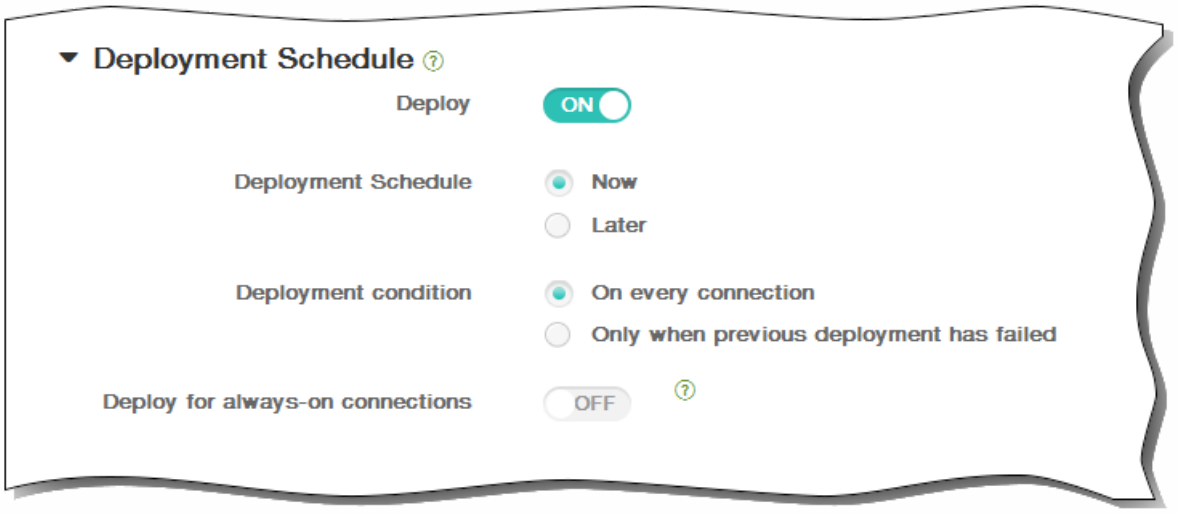
12. 单击下一步。 此时将显示“已订阅的日历”策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



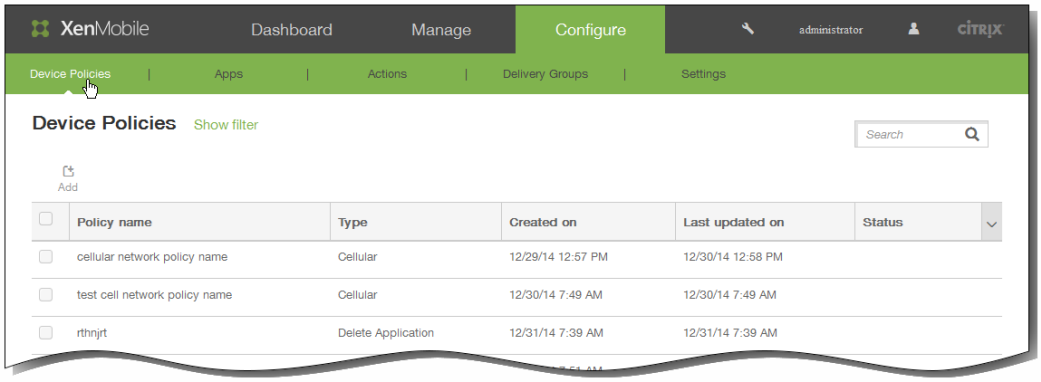
15. 单击保存以保存此策略。

通行码设备策略

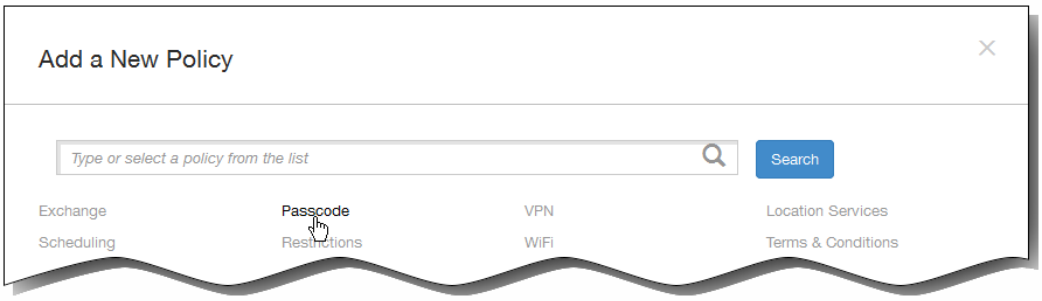
May 05, 2016

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。可以为 iOS、Android、Samsung KNOX、Windows Phone 8.1 和 Windows 8.1 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。

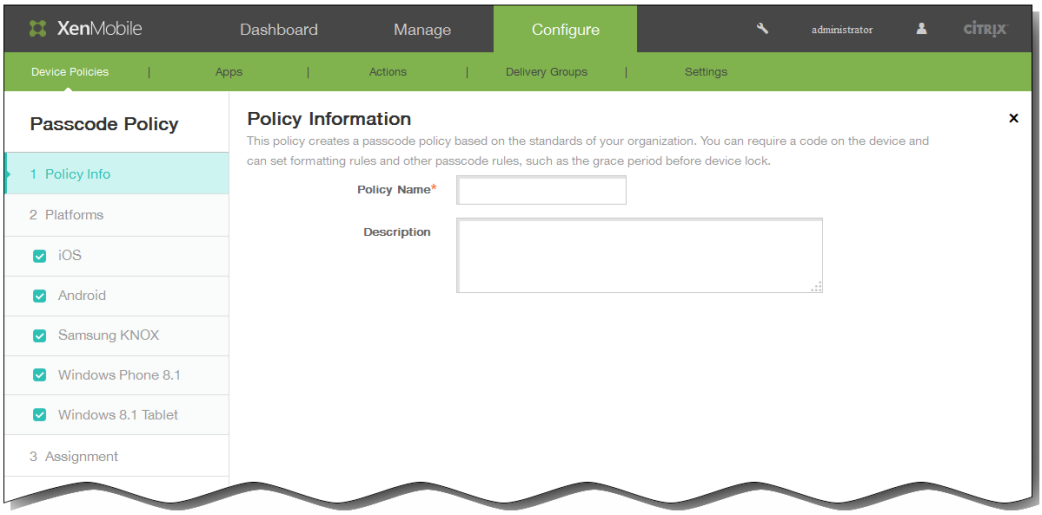
1. In the XenMobile console, click Configure > Device Policies. The Device Policies page appears. Click Add to add a new policy.



2. On the Add New Policy page, click Passcode.

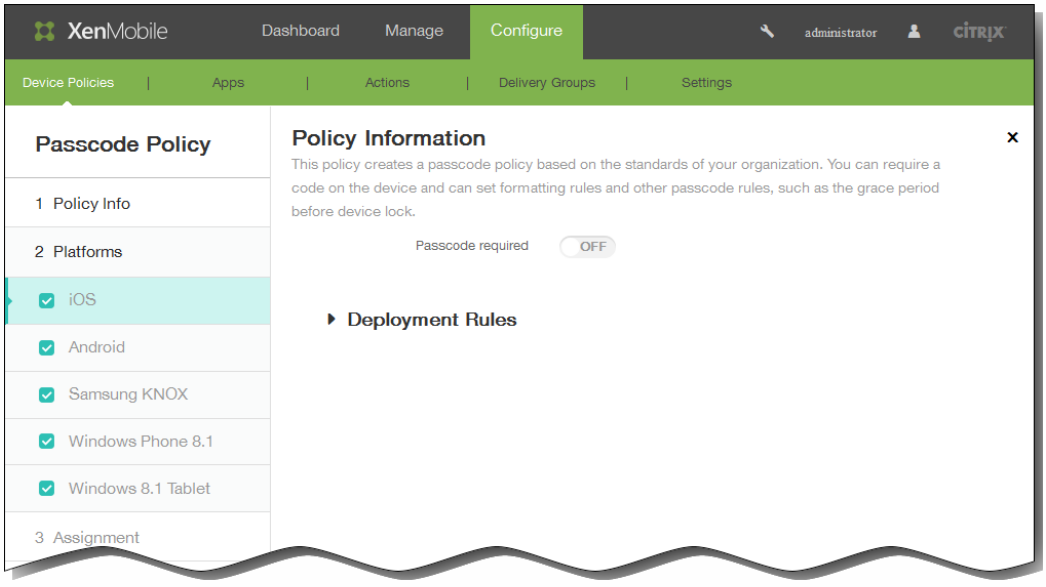


3. In the Policy Information pane, enter the following information:

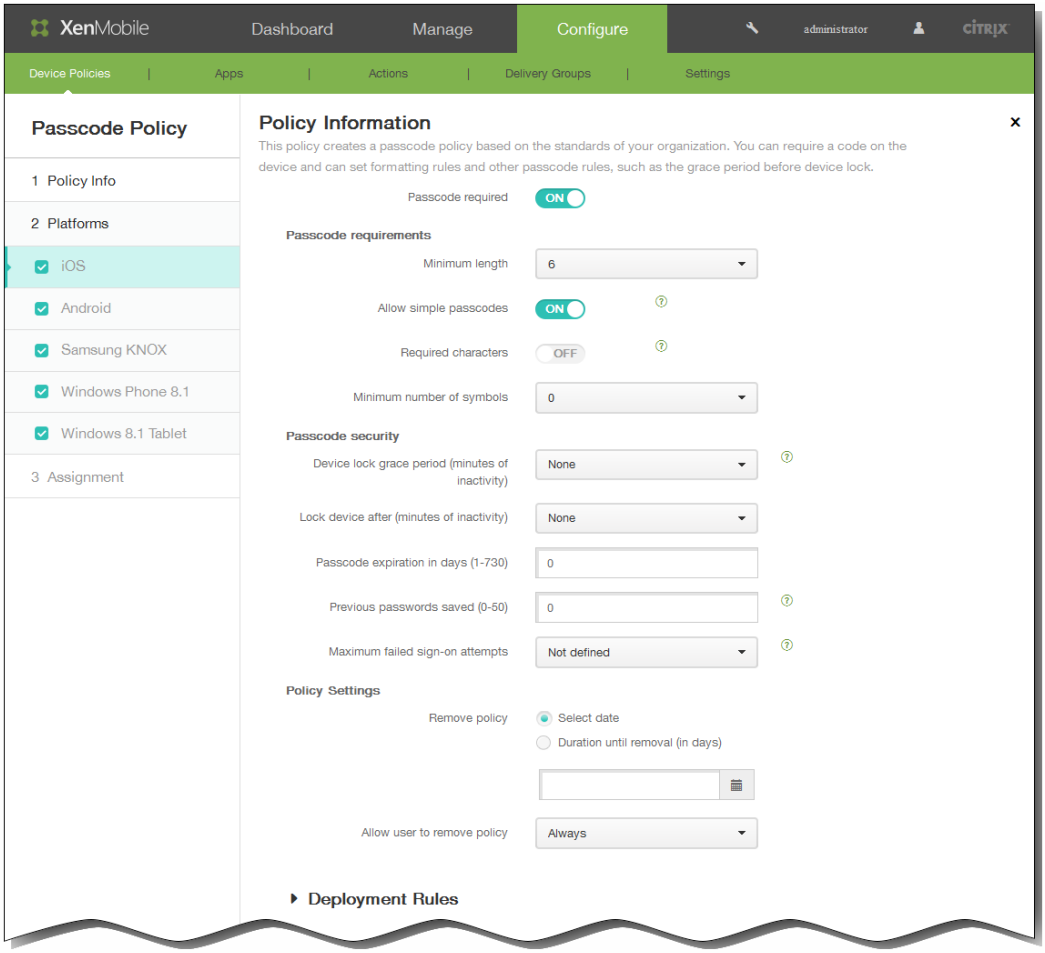


1. Policy Name: Type a descriptive name for the policy.
2. Description: Type an optional description of the policy.
3. Click Next.

4. Under Platforms, select the platforms for which you want to configure this policy.
   Note: When the Policy Platforms page appears, all platforms are selected and you see the iOS platform configuration panel first.



- If you selected iOS, configure these settings:



Passcode required: Select this option to require a passcode and to display the configuration options for an iOS passcode device policy. The page expands to let you configure settings for passcode requirements, passcode security, and policy settings.

Passcode requirements

Minimum length: In the list, click the minimum passcode length. The default is 6.

Allow simple passcodes: Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is ON.

Required characters: Select whether to require passcodes to have at least one letter. The default is OFF.

Minimum number of symbols: In the list, click the number of symbols the passcode must contain.

Passcode security

Device lock grace period (minutes of inactivity): In the list, click the length of time before users must enter a passcode to unlock a locked device. The default is None.

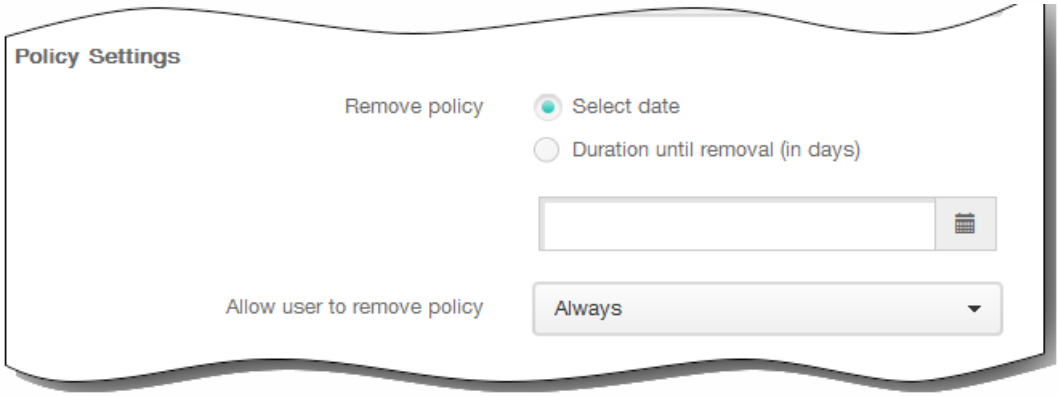
Lock device after (minutes of inactivity): In the list, click the length of time a device can be inactive before it is locked. The default is None.

Passcode expiration in days (1-730): Enter the number of days after which the passcode expires. Valid values are 1–730. The default is 0, which means the passcode never expires.

Previous passwords saved (0-50): Enter the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is 0, which means users can reuse passwords.

Maximum failed sign-on attempts: In the list, click the number of times a user can fail to sign in successfully after which the device is fully wiped. The default is Not defined.

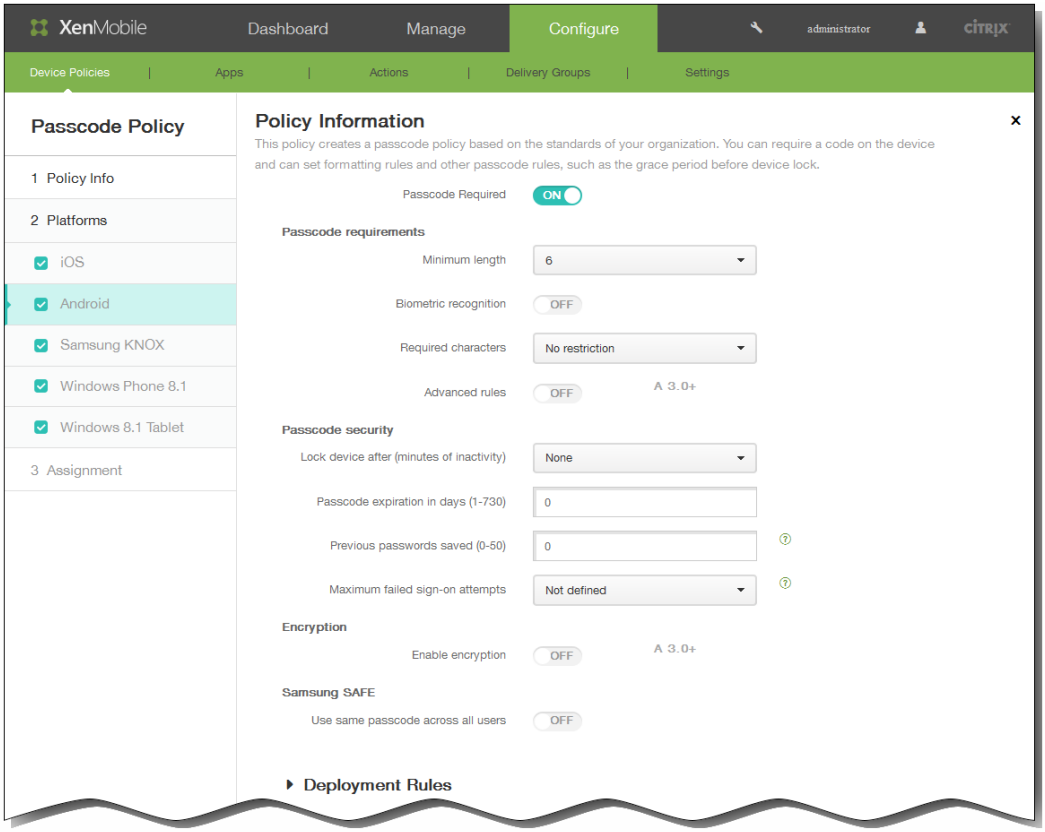
Policy Settings



1. Under Policy Settings, next to Remove policy, click either Select date or Duration until removal (in days).
2. If you click Select date, click the calendar to select the specific date for removal.
3. In the Allow user to remove policy list, click Always, Password required, or Never.
4. If you click Password required, next to Removal password, type the necessary password.

- If you selected Android, configure these settings:

  Note: The default setting for Android is OFF. The page expands to let you configure settings for passcode requirements, passcode security, encryption, and Samsung SAFE.



Passcode requirements

Minimum length: In the list, click the minimum passcode length. The default is 6.

Biometric recognition: Select whether to enable biometric recognition. If you enable this option, the Required characters field is hidden. The default is OFF.

Required characters: In the list, click No Restriction, Both numbers and letters, Numbers only, or Letters only to configure how passcodes are composed. The default is No restriction.

Advanced rules: Select whether to apply advanced passcode rules. This option is available for Android 3.0 and later. The default is OFF.

When Advanced rules is set to ON, from each of the following lists, click the minimum number of each character type that a passcode must contain:

- Symbols: The minimum number of symbols.
- Letters: The minimum number of letters.
- Lowercase letters: The minimum number of lowercase letters.
- Uppercase letters: The minimum number of uppercase letters.
- Numbers or symbols: The minimum number of numbers or symbols.
- Numbers: The minimum number of numbers.

Passcode security

Lock device after (minutes of inactivity): In the list, click the length of time a device can be inactive before it is locked. The default is None

Passcode expiration in days (1-730): Enter the number of days after which the passcode expires. Valid values are 1–730. The default is 0, which means the passcode never expires.

Previous passwords saved (0-50): Enter the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is 0, which means users can reuse passwords.

Maximum failed sign-on attempts: In the list, click the number of times a user can fail to sign in successfully after which the device is fully wiped. The default is Not defined.

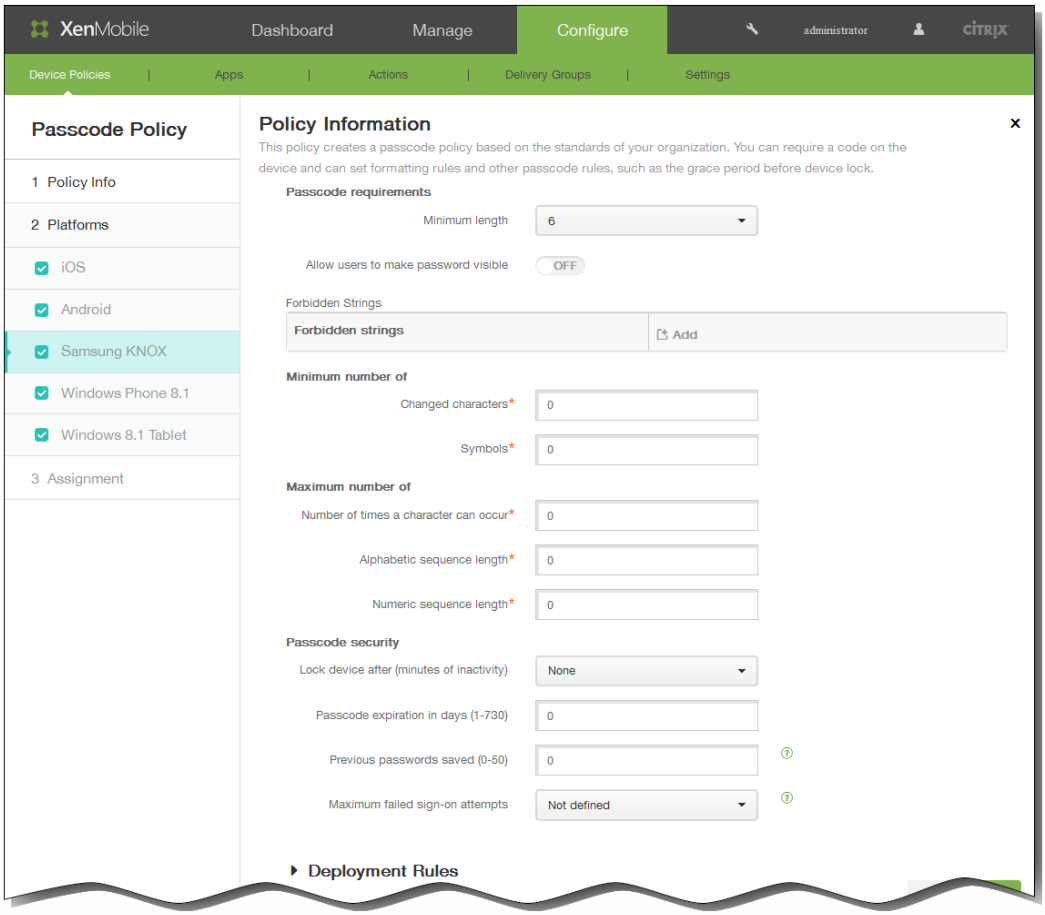
Encryption

Enable encryption: Select whether to enable encryption. This option is available for Android 3.0 and later. The option is available regardless of the Passcode required setting.

Use same passcode across all users: Select whether to use the same passcode for all users. This option applies only to Samsung SAFE devices and is available regardless of the Passcode required setting. The default is OFF.

Enter the required passcode in the field that appears when you enable this option.

- If you selected Samsung KNOX, configure these settings:



Passcode requirements

Minimum length: In the list, click the minimum passcode length.

Allow users to make password visible: Select whether to let users make the password visible.

- Forbidden strings: You create forbidden strings to prevent users from using insecure strings that are easy to guess like "password", "pwd", "welcome", "123456", "111111", and so on. Do the one of the following:
  - To add a forbidden string
    1. Click Add.
    2. Type the forbidden string.
    3. Click Save to save the string or Cancel to cancel adding the string.
    4. Repeat steps i. through iii. for each forbidden string you want to add.
  - To edit a forbidden string
    1. Previous passwords saved (0-50): Enter the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is 0, which means user can reuse passwords.
    1. Hover over the string you want to edit.
    2. Click the pen icon to the right of the listing.
    3. Make changes to the string.
    4. Click Save to save the string or Cancel to cancel changing the string.

  Minimum number of

  Changed characters: Enter the number of characters users must change from their previous passcode. The default is 0.

  Symbols: Enter the minimum number of required symbols in a passcode. The default is 0.

  Maximum number of

  Number of times a character can occur: Enter the maximum number of times a character can occur in a passcode. The default is 0.

  Alphabetic sequence length: Enter the maximum length of an alphabetic sequence in a passcode. The default is 0.

  Numeric sequence length: Enter the maximum length of a numeric sequence in a passcode. The default is 0.

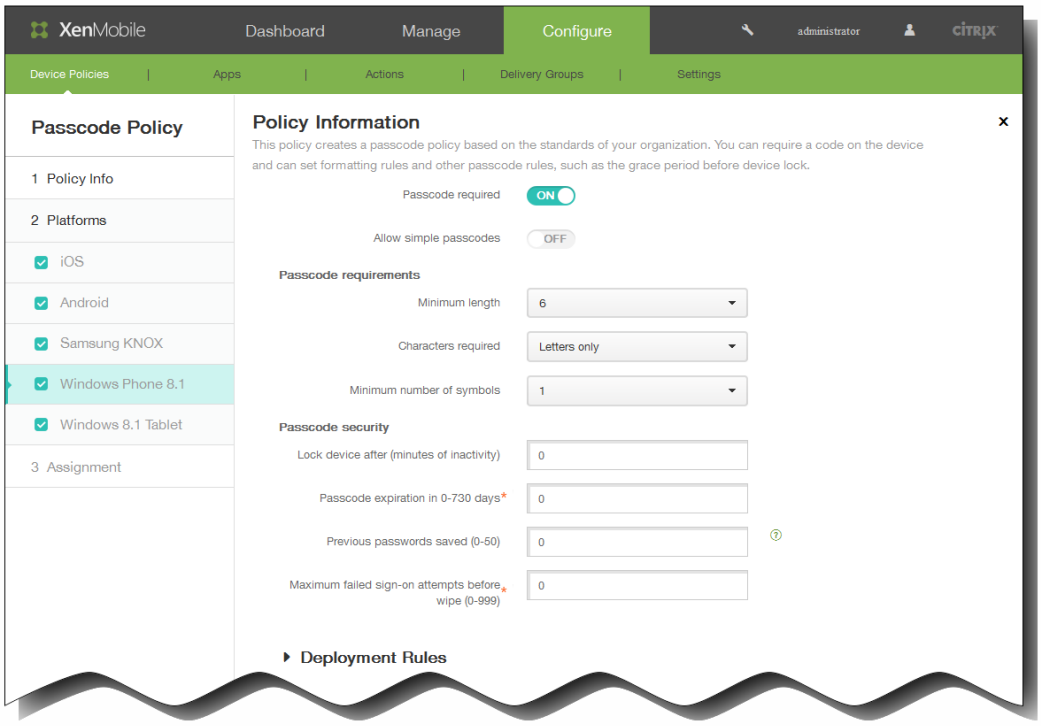
  Passcode security

  Lock device after (minutes of inactivity): In the list, click the length of time a device can be inactive before it is locked. The default is None.
  Note: Even though this field's label says "minutes of inactivity" XenMobile actually enforces the lock after the specified number of *seconds*.
  Passcode expiration in days (1-730): Enter the number of days after which the passcode expires. Valid values are 1–730. The default is 0, which means the passcode never expires.

  Previous passwords saved (0-50): Enter the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is 0, which means user can reuse passwords.

  Maximum failed sign-on attempts: In the list, click the number of times a user can fail to sign in successfully after which the device is locked. The default is Not defined.

- If you selected Windows Phone 8.1, configure these settings:



Passcode required: Select this option to not require a passcode for Windows Phone 8.1 devices. The default setting is ON, which requires a passcode. The page collapses and the following options disappear. If you do not turn off the passcode requirement, continue configuring the following settings.

Allow simple passcodes: Select whether to allow simple passcodes. Simple passcodes are a repeated or sequential set of characters. The default is OFF.

Passcode requirements

Minimum length: In the list, click the minimum passcode length. The default is 6.

Characters required: In the list, click Numeric or alphanumeric, Letters only, or Numbers only to configure how passcodes are composed. The default is Letters only.

Minimum number of symbols: In the list, click the number of symbols the passcode must contain. The default is 1.

Passcode security

Lock device after (minutes of inactivity): In the list, click the length of time a device can be inactive before it is locked. The default is 0.

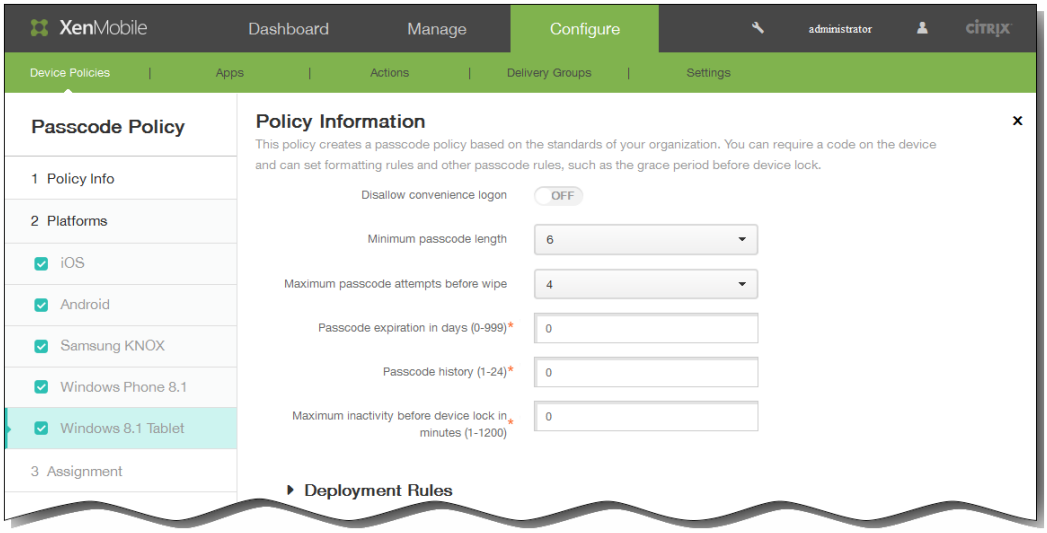
Passcode expiration in 0-730 days: Enter the number of days after which the passcode expires. Valid values are 1–730. The default is 0, which means the passcode never expires.

Previous passwords saved (0-50): Enter the number of used passwords to save. Users are unable to use any password found in this list. Valid values are 0–50. The default is 0, which means users can reuse passwords.

Maximum failed sign-on attempts before wipe (0-999): In the list, click the number of times a user can fail to sign in

successfully after which corporate data is wiped from the device. The default is 0.

- If you selected Windows 8.1 Tablet, configure these settings:



Disallow convenience logon: Select whether to allow users to access their devices with picture passwords or biometric logons. The default is OFF.

Miniumum passcode length: In the list, click the minimum passcode length. The default is 6.

Maximum passcode attempts before wipe: In the list, click the number of times a user can fail to sign in successfully after which the device is wiped. The default is 4.

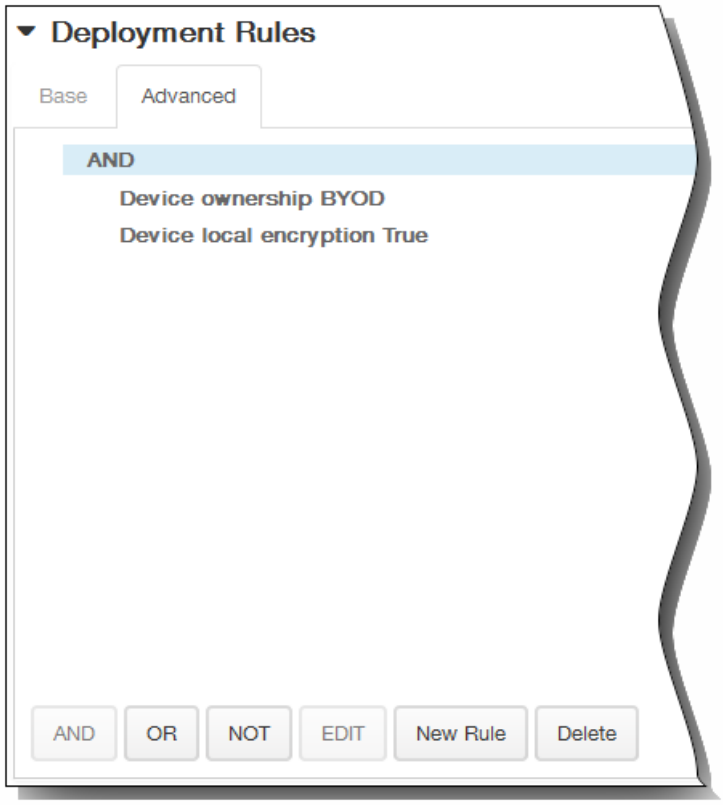
Passcode expiration in days (0-999): Enter the number of days after which the passcode expires. Valid values are 1–999. The default is 0, which means the passcode never expires.

Passcode history: (1-24): Enter the number of used passcodes to save. Users are unable to use any passcode found in this list. Valid values are 1–24. You must enter a number between 1 and 24 in this field.

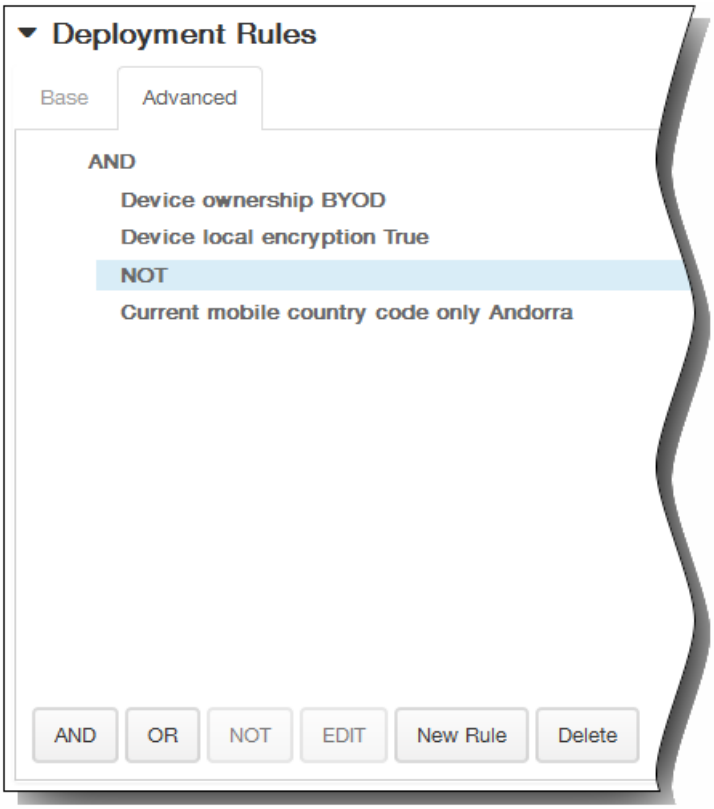
Maximum inactivity before device lock in minutes (1-1200): Enter the length of time in minutes that a device can be inactive before it is locked. Valid values are 1–1200. You must enter a number between 1 and 1200 in this field.

5. Expand Deployment Rules and then configure the following settings: The Base tab appears by default.

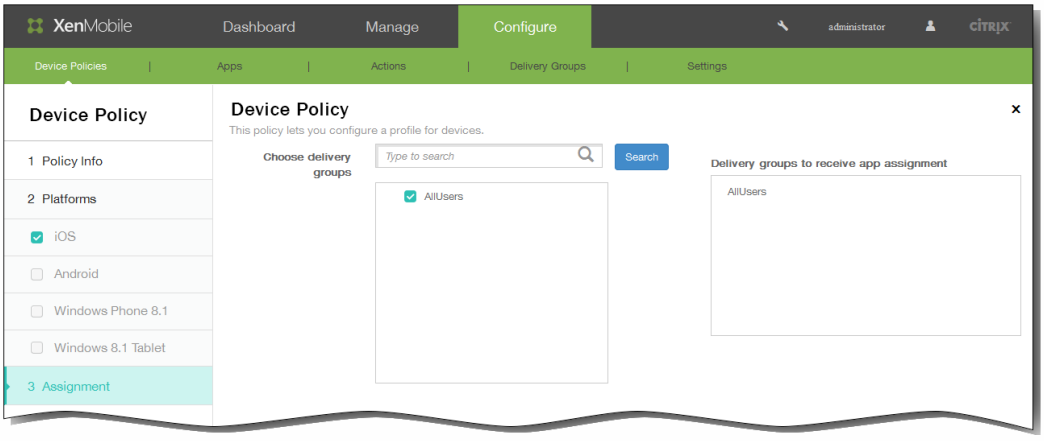
1. In the lists, click options to determine when the policy should be deployed.
    1. You can choose to deploy the policy when all conditions are met or when any conditions are met. The default option is All.
    2. Click New Rule to define the conditions.
    3. In the lists, click the conditions, such as Device ownership and BYOD, as shown in the preceding figure.
    4. Click New Rule again if you want to add more conditions. You can add as many conditions as you would like.
2. Click the Advanced tab to combine the rules with Boolean options.



   The conditions you chose on the Base tab appear.
3. You can use more advanced Boolean logic to combine, edit, or add rules.
    1. Click AND, OR, or NOT.
    2. In the lists that appear, choose the conditions that you want to add to the rule and then click the Plus sign (+) on the right-hand side to add the condition to the rule.
       At any time, you can click to select a condition and then click EDIT to change the condition or Delete to remove the condition.
    3. Click New Rule again if you want to add more conditions.
       In this example, the device ownership must be BYOD, the device local encryption must be True, and the device mobile country code cannot be only Andorra.



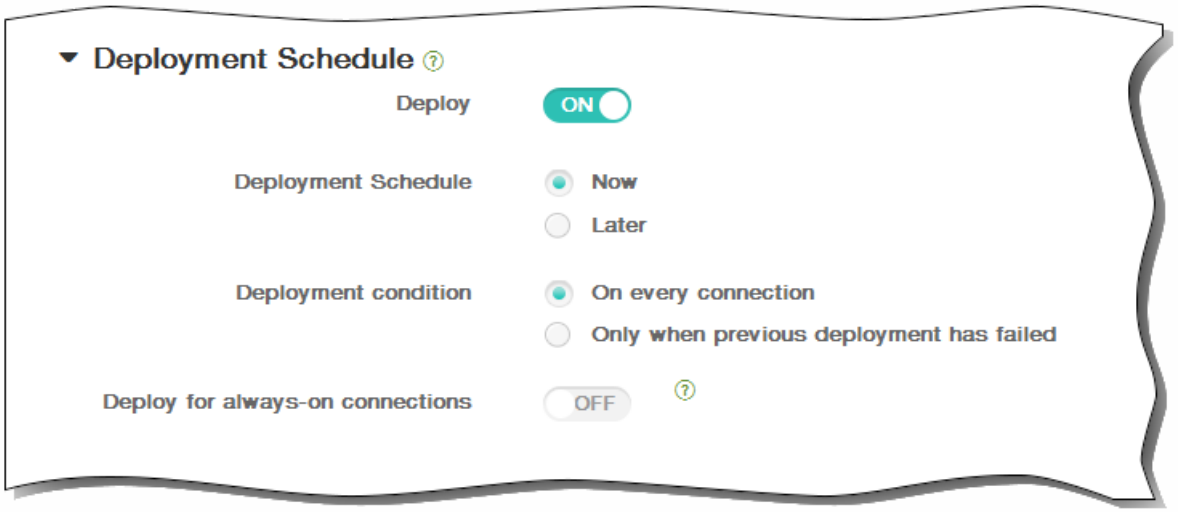
6. Click Next. The Passcode Policy assignment page appears.
7. Next to Choose delivery groups, type to find a delivery group or select a group or groups in the list to which you want to assign the policy. The groups you select appear in the right-hand Delivery groups to receive app assignment list.



8. Expand Deployment Schedule and then configure the following settings:
   1. Next to Deploy, click ON to schedule deployment or click OFF to prevent deployment. The default option is ON. If you choose OFF, no other options need to be configured.
   2. Next to Deployment schedule, click Now or Later. The default option is Now.
   3. If you click Later, click the calendar icon and then select the date and time for deployment.

4. Next to Deployment condition, click On every connection or click Only when previous deployment has failed. The default option is On every connection.
5. Next to Deploy for always-on connection, click ON or OFF. The default option is OFF.
   Note: This option applies when you have configured the scheduling background deployment key in Settings > Server Properties. The always-on option is not available for iOS devices.

Note: The deployment schedule you configure is the same for all platforms. Any changes you make apply to all platforms, except for Deploy for always on connection, which does not apply to iOS.



9. Click Save.

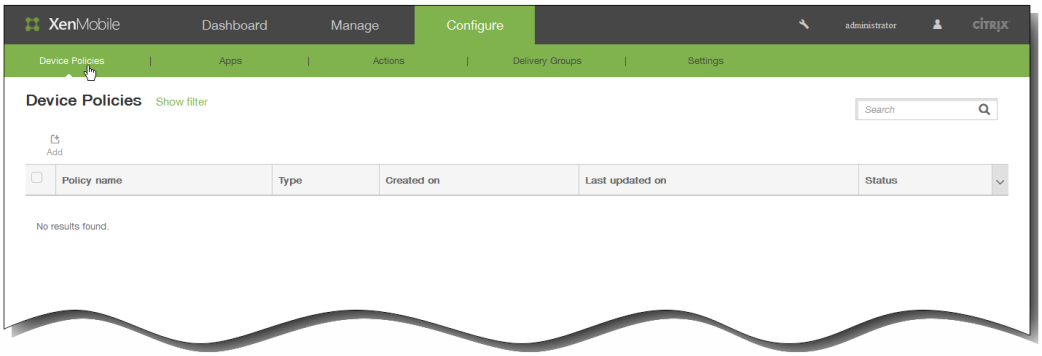
为 iOS 添加代理设备策略

May 05, 2016

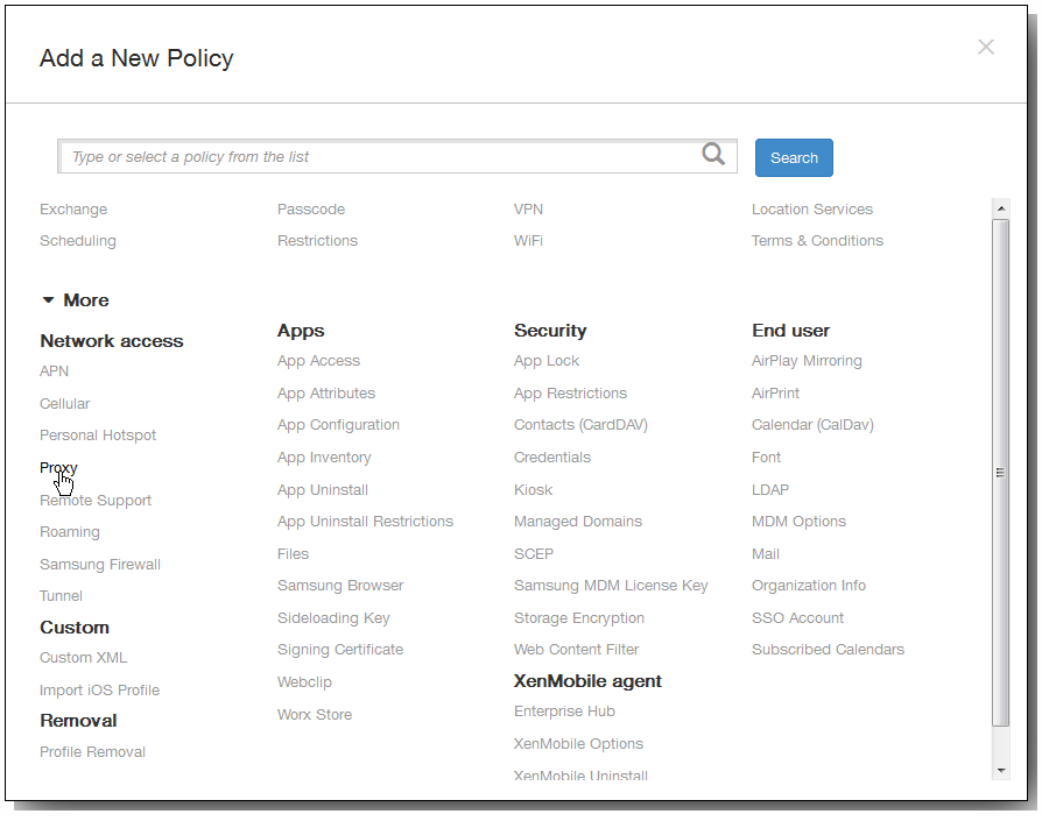
可以在 XenMobile 中添加设备策略以为运行 iOS 6.0 或更高版本的设备指定全局 HTTP 代理设置。只能为每个设备部署一个全局 HTTP 代理策略。

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。

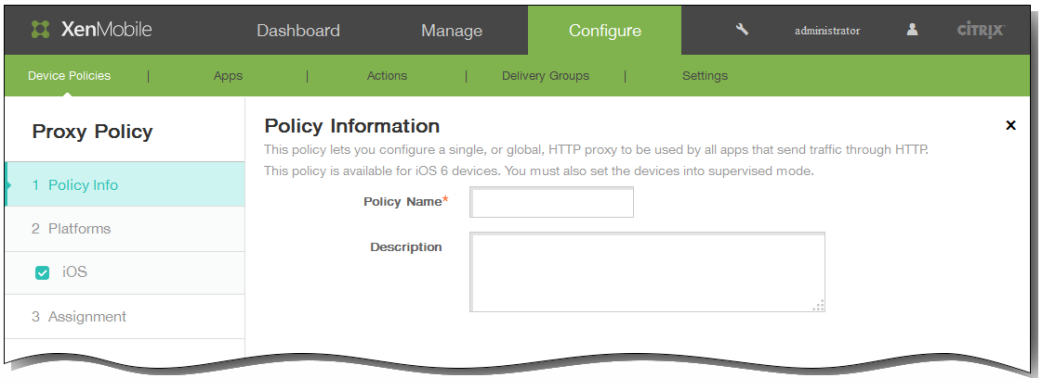
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



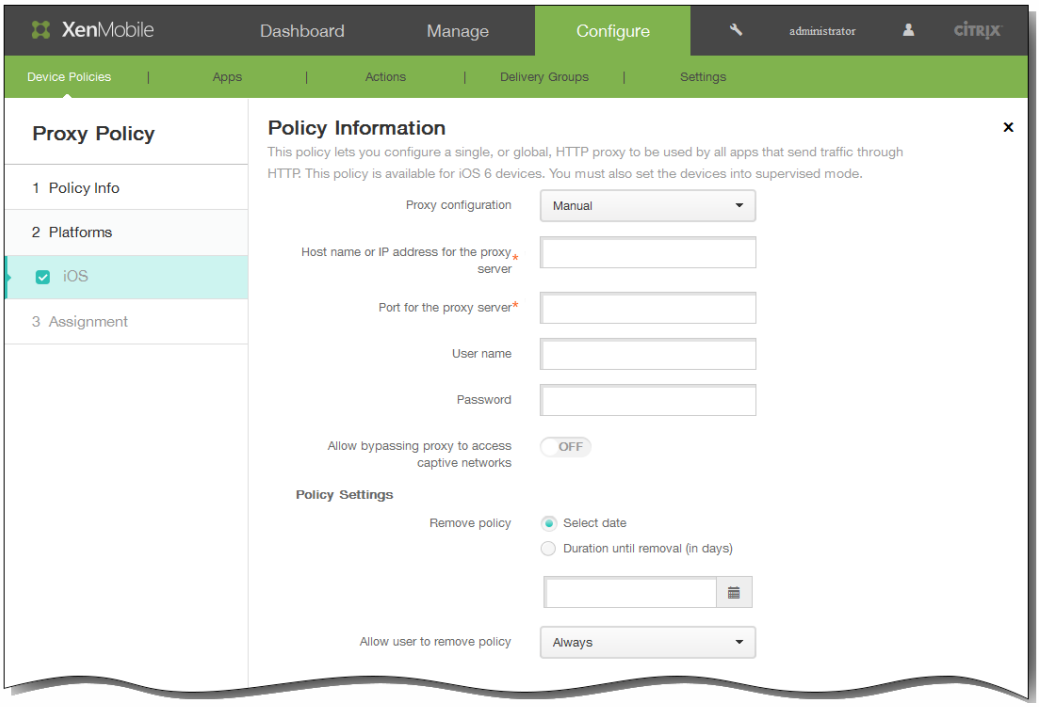
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在网络访问下，单击代理。 此时将显示代理策略页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：输入策略的描述性名称。
   2. 说明：选择性输入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。

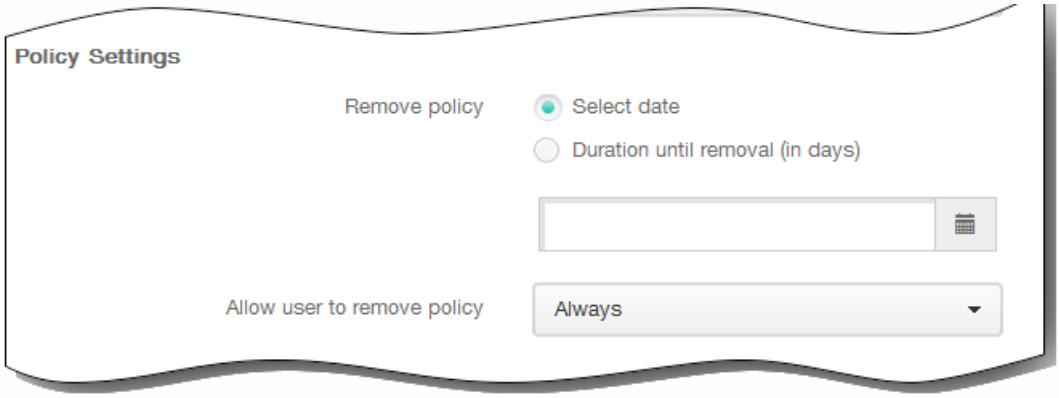


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 代理配置：单击手动或自动以设置代理在用户设备上的配置方式。 下表列出了每个代理配置可用的选项。每个单元格指示对应的选项为不适用 (-)、必选还是可选。

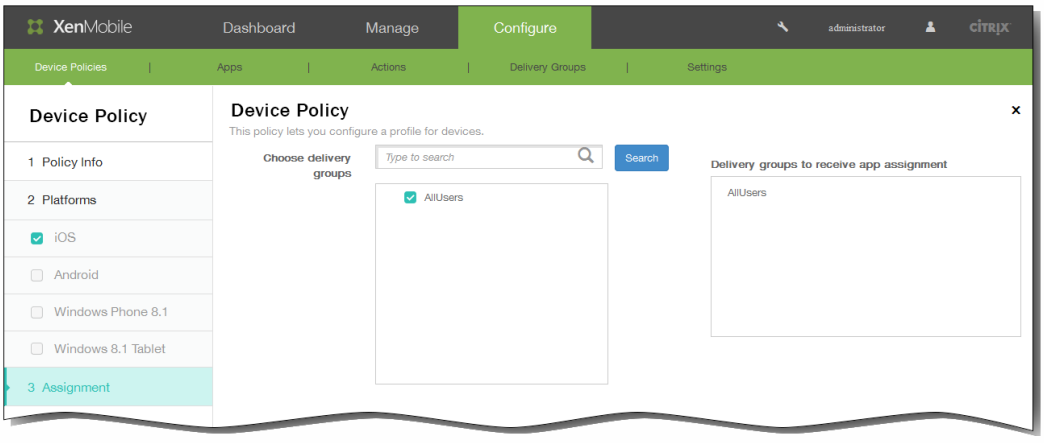
	手动	自动
代理服务器的主机名或 IP 地址	必选	–

代理服务器的端口	手动 必选	自动 –
用户名	可选	–
密码	可选	–
代理 PAC URL	_	可选
允许在无法访问 PAC 时直接连接	_	关

2. 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。
7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



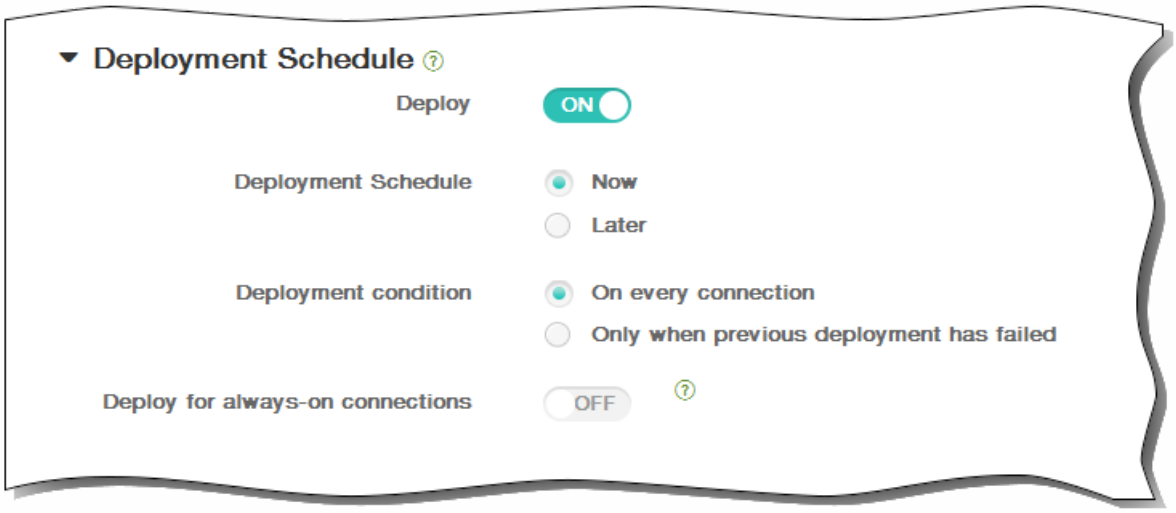
11. 单击下一步。 此时将显示代理策略分配页面。
12. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



13. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



14. 单击保存以保存此策略。

为 Samsung KNOX 添加远程支持设备策略

May 05, 2016

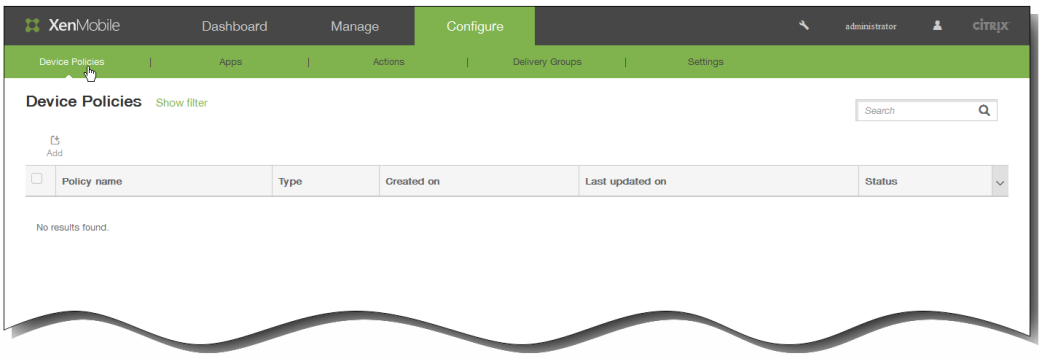
可以在 XenMobile 中创建远程支持策略以授予远程访问用户的 Samsung KNOX 设备所需的权限。可以配置两种类型的支持：

- **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。

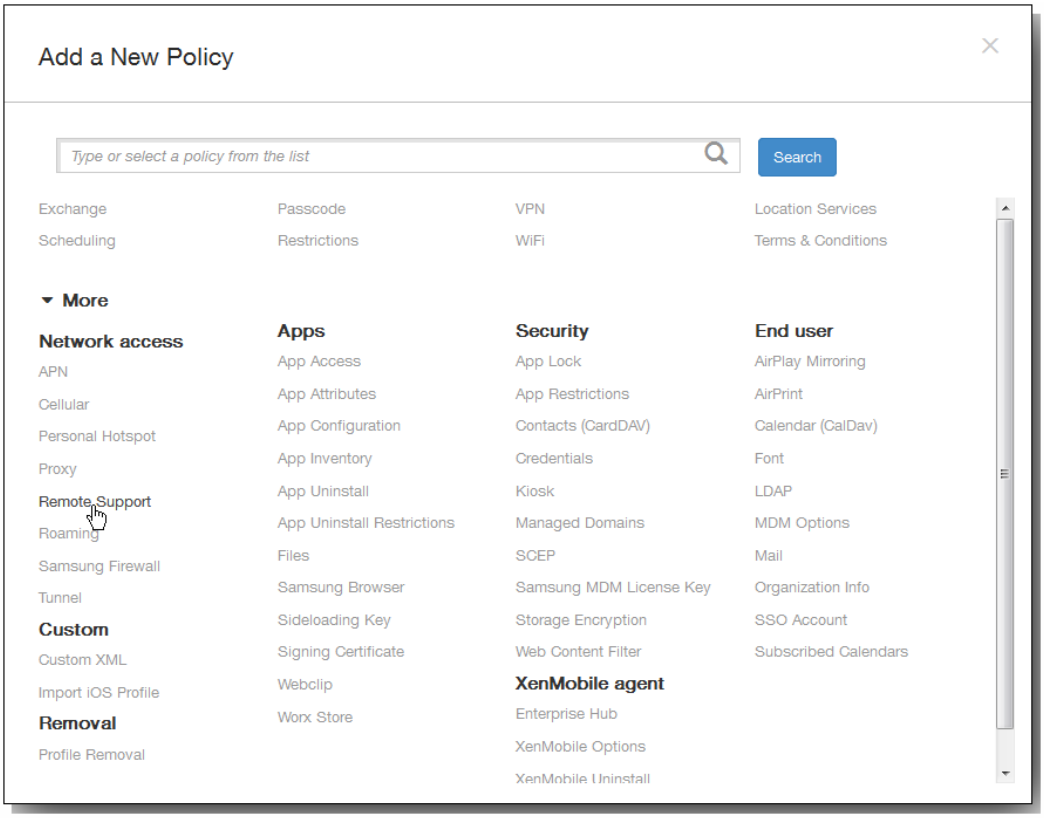
注意：要实施此策略，必须执行以下策略：

- 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，请参阅添加适用于 Android 的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。

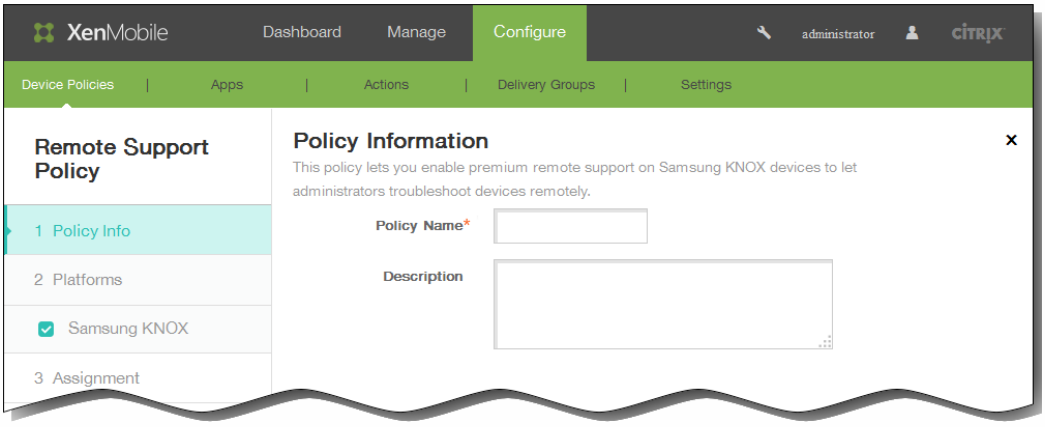
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



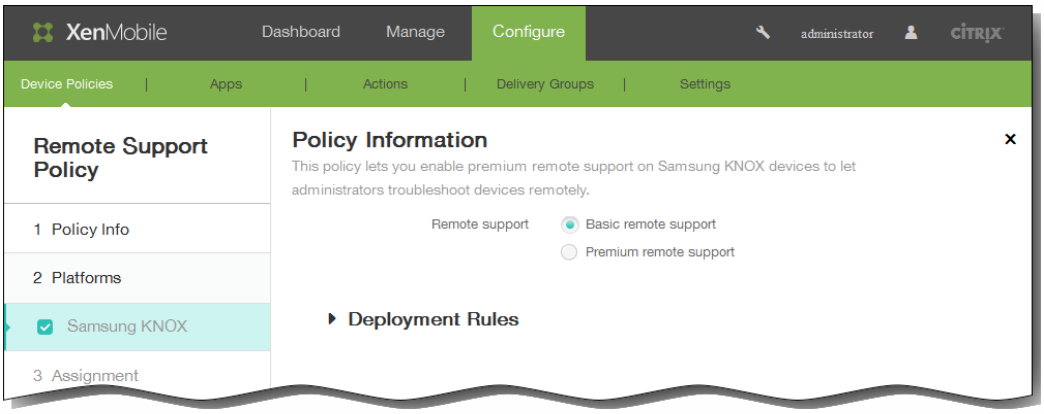
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在网络访问下，单击远程支持。 此时将显示远程支持策略页面。

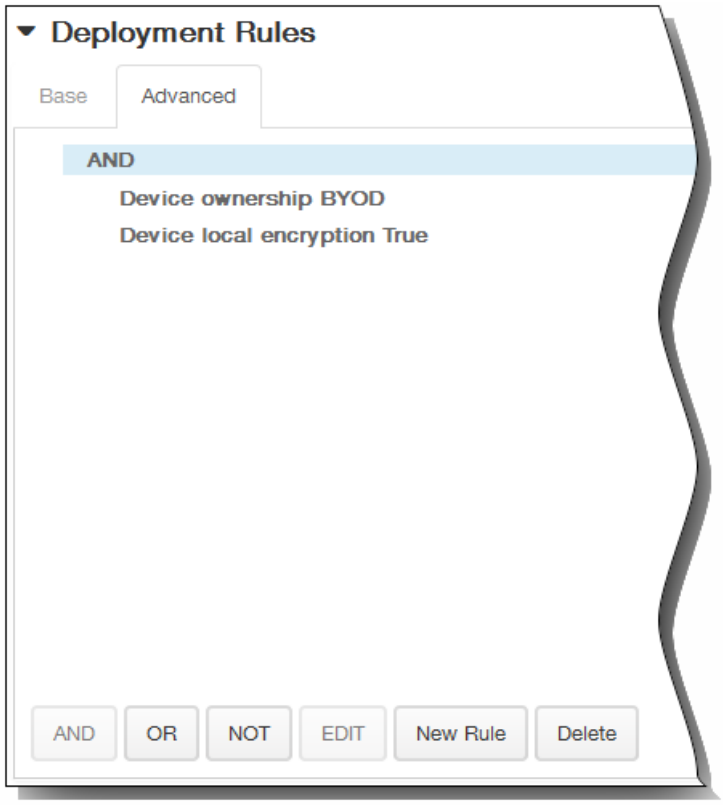


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 Samsung KNOX 平台信息页面。



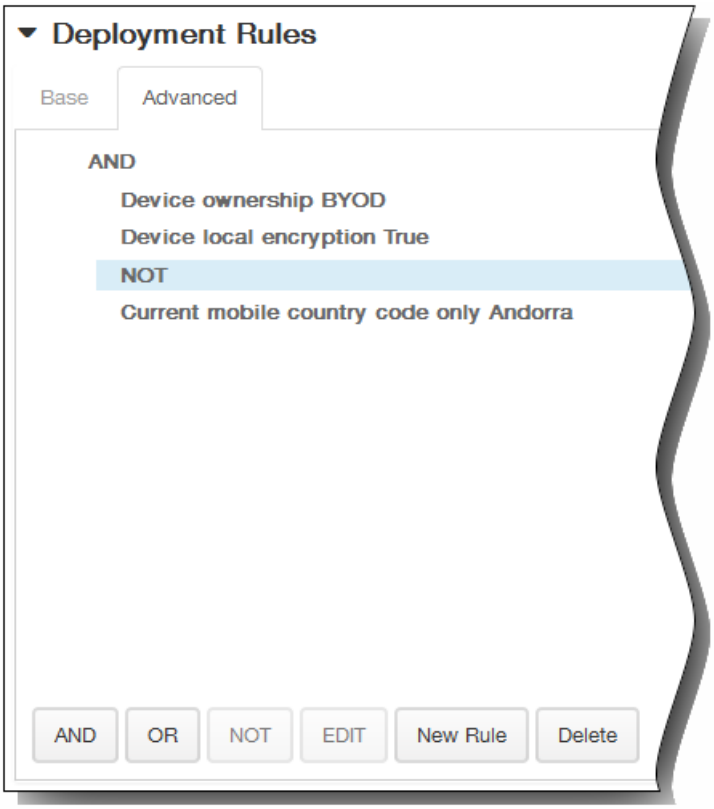
6. 在 Samsung KNOX 平台信息页面上，输入以下信息：
   1. 远程支持：选择基本远程支持或高级远程支持。 默认设置为基本远程支持。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

   1. 在此列表中，单击选项以确定部署策略的时间。
      1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
      2. 单击新建规则以定义条件。
      3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
      4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
   2. 单击高级选项卡以使用布尔选项组合规则。

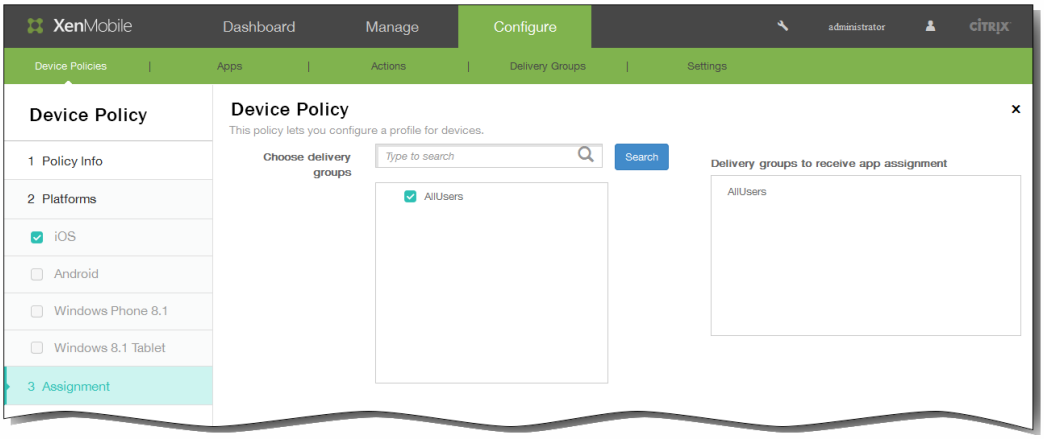


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



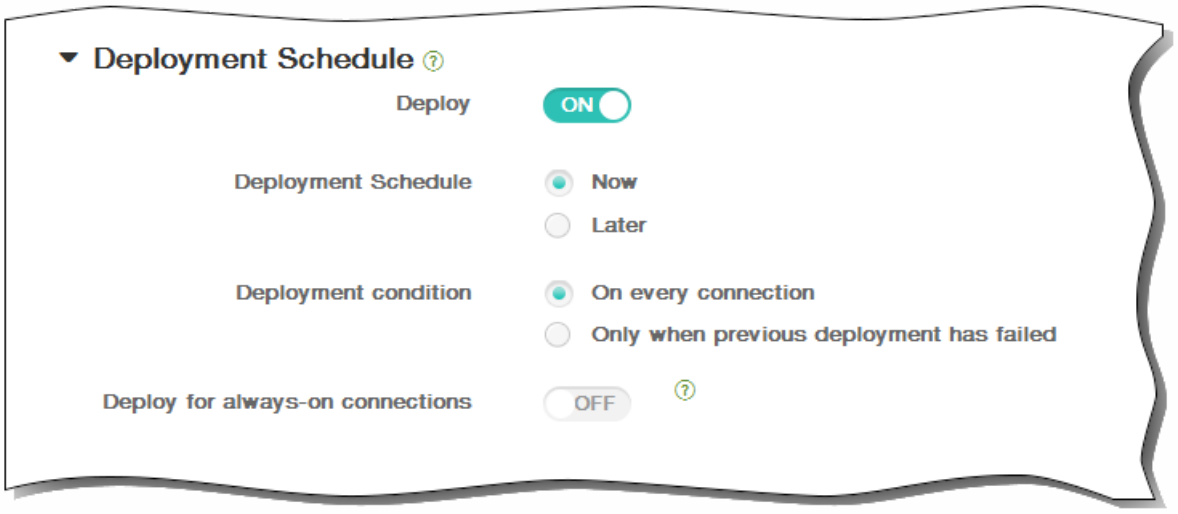
8. 单击下一步。 此时将显示远程支持策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

限制设备策略

May 05, 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、Samsung SAFE、Windows 8.1 Tablet、Windows Phone 8.1 和 Amazon。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

。主要的例外为“安全 - 强制”功能，该功能默认设置为关或

— 限制

。

提示：如果您为任何选项选择开，则意味着用户

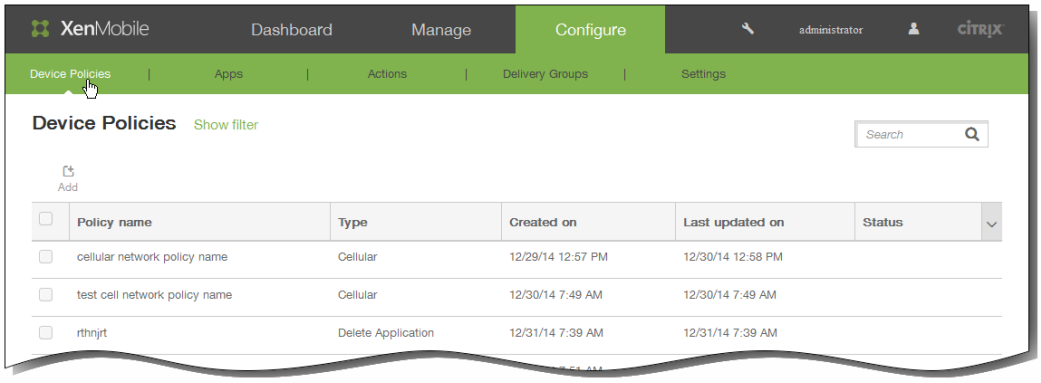
— 可以

执行该操作或使用该功能。例如：

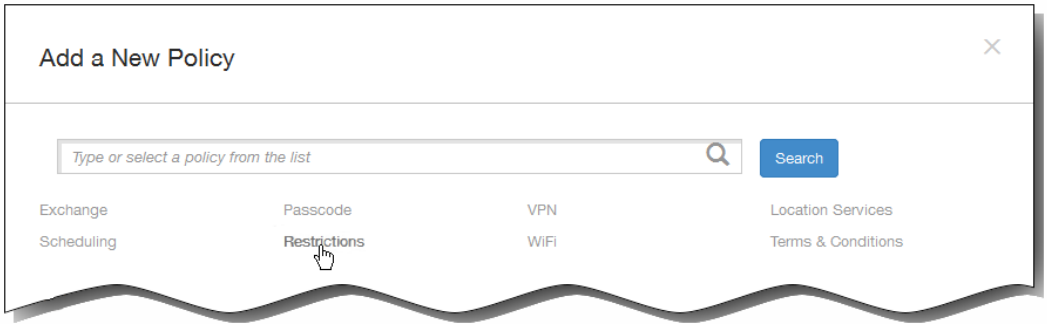
- 相机。如果选择开，用户将可以使用其设备上的相机。如果选择关，用户将无法使用其设备上的相机。
- **屏幕快照**。如果选择开，则设备用户可以在设备上创建屏幕快照。如果选择关，则设备用户无法在设备上创建屏幕快照。

注意：某些 iOS 限制选项仅适用于特定版本的 iOS（并且如果适用，这些版本将记录在 XenMobile 控制台的页面上）。此外，如果设备处于“受监督”模式，将仅有部分选项适用。例如，允许或阻止 AirDrop 的功能仅在运行 iOS 7 及更高版本的设备上受支持，而允许或阻止照片流的功能在运行 iOS 5 及更高版本的设备上受支持。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。

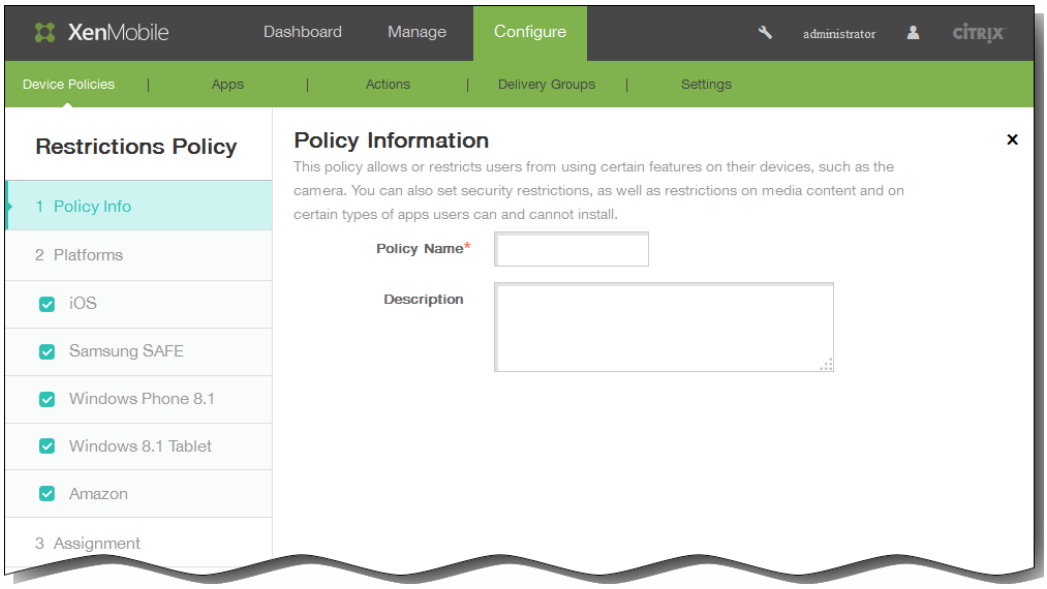
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



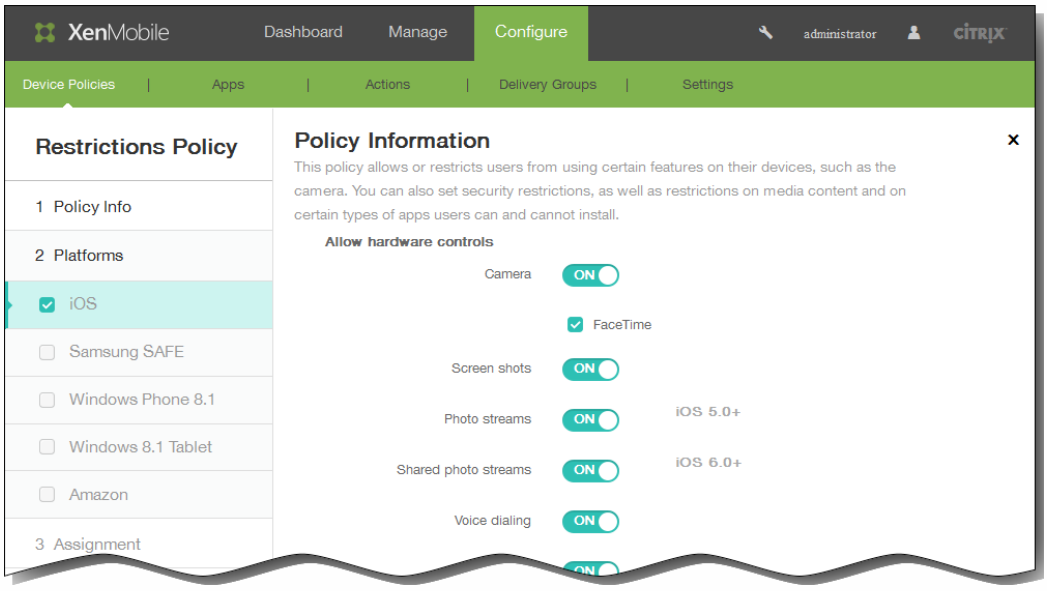
2. 单击添加。 将显示添加新策略页面。



3. 单击限制。
   将显示限制策略信息页面。



4. 在策略信息窗格中，键入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
5. 在平台下面，选择要添加的一个或多个平台。 然后，您可以更改每个选中平台的策略信息。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，可以配置以下设置：



- 在允许硬件控制中：

  相机；FaceTime

  屏幕快照

  Photo streams（照片流）（在 iOS 5.0 及更高版本中可用）。

  Shared photo streams（共享照片流）（在 iOS 6.0 及更高版本中可用）。

  语音拨号

  Siri：
  - Allow while device is locked（设备锁定时允许）：将此选项保留默认选中状态或取消选中复选框。
  - Siri profanity filter（Siri 猥亵语言过滤器）：将此选项保留默认未选中状态或选中复选框。默认设置为限制此功能。

  安装应用程序

- 在允许使用应用程序中：

  YouTube

  iTunes Store

  应用程序内购买：所有购买均需使用 iTunes 密码：保留此选项的默认不选中状态或者选中此复选框（在 iOS 5.0 及更高版本中可用）。默认设置为限制此功能。

  Safari：
  - Autofill（自动填充）：将此选项保留默认选中状态或取消选中复选框。
  - 强制显示欺诈警告：将此选项保留默认未选中状态或选中复选框。默认设置为限制此功能。
  - 启用 JavaScript：将此选项保留默认选中状态或取消选中复选框。
  - 阻止弹出窗口：将此选项保留默认未选中状态或选中复选框。默认设置为限制此功能。

  在接受 Cookie 中，单击以下选项之一：
  - 总是
  - 从不
  - 仅从访问过的站点

    默认选项为总是。

- 在 网络 - 允许执行 iCloud 操作中：

  文档和数据同步（在 iOS 5.0 及更高版本中可用）

  设备备份（在 iOS 5.0 及更高版本中可用）

  漫游时自动同步

  iCloud 钥匙链（在 iOS 7.0 及更高版本中可用）

- 在安全 - 强制中：

  加密备份默认值为关。

  有限广告跟踪（在 iOS 7.0 及更高版本中可用）默认值为关。

首次 AirPlay 配对时输入通行码（在 iOS 7.0 及更高版本中可用）默认值为关。

- 在安全 - 允许中：

  接受不可信 SSL 证书（在 iOS 5.0 及更高版本中可用）。

  自动更新证书信任设置（在 iOS 7.0 及更高版本中可用）。

  在非托管应用程序中使用托管应用程序的文档

  在托管应用程序中使用非托管应用程序的文档

  诊断结果提交到 Apple

  通过 Touch ID 解锁设备（在 iOS 7.0 及更高版本中可用）

  锁定时接收 Passbook 通知（在 iOS 6.0 及更高版本中可用）

  提交（在 iOS 8.0 及更高版本中可用）

  托管应用程序的 iCloud 同步（在 iOS 8.0 及更高版本中可用）

  企业通讯簿备份（在 iOS 8.0 及更高版本中可用）

  批注并高亮显示企业地址簿的同步（在 iOS 8.0 及更高版本中可用）

- 在仅监管设置 - 允许中：

  Spotlight 中的 Internet 结果（在 iOS 8.0 及更高版本中可用）

  擦除所有内容和设置（在 iOS 8.0 及更高版本中可用）

  配置限制（在 iOS 8.0 及更高版本中可用）

  安装配置文件（在 iOS 6.0 及更高版本中可用）

  AirDrop（在 iOS 7.0 及更高版本中可用）

  iMessage（在 iOS 6.0 及更高版本中可用）

  Siri 用户生成的内容（在 iOS 7.0 及更高版本中可用）

  iBooks（在 iOS 6.0 及更高版本中可用）

  删除应用程序（在 iOS 7.0 及更高版本中可用）

  游戏中心（在 iOS 6.0 及更高版本中可用）
  - 添加好友：将此选项保留默认选中状态或取消选中复选框。
  - 多人游戏：将此选项保留默认选中状态或取消选中复选框。

  修改帐户设置（在 iOS 7.0 及更高版本中可用）

  修改应用程序手机网络数据设置（在 iOS 7.0 及更高版本中可用）

  修改“查找我的好友”设置（在 iOS 7.0 及更高版本中可用）

  与非 Configurator 主机配对（在 iOS 7.0 及更高版本中可用）

单应用程序捆绑包 ID：在应用程序名称中，输入一个或多个应用程序。

- 安全 - 在锁定屏幕中显示：

  控制中心（在 iOS 7.0 及更高版本中可用）

  通知（在 iOS 7.0 及更高版本中可用）

  “今天”视图

- 在媒体内容 - 允许中：

  成人音乐、博客及 iTunes U 资料

  iBooks 中暴露的性内容（在 iOS 6.0 及更高版本中可用）

  评级地区：单击列表中的国家/地区。默认值为美国。

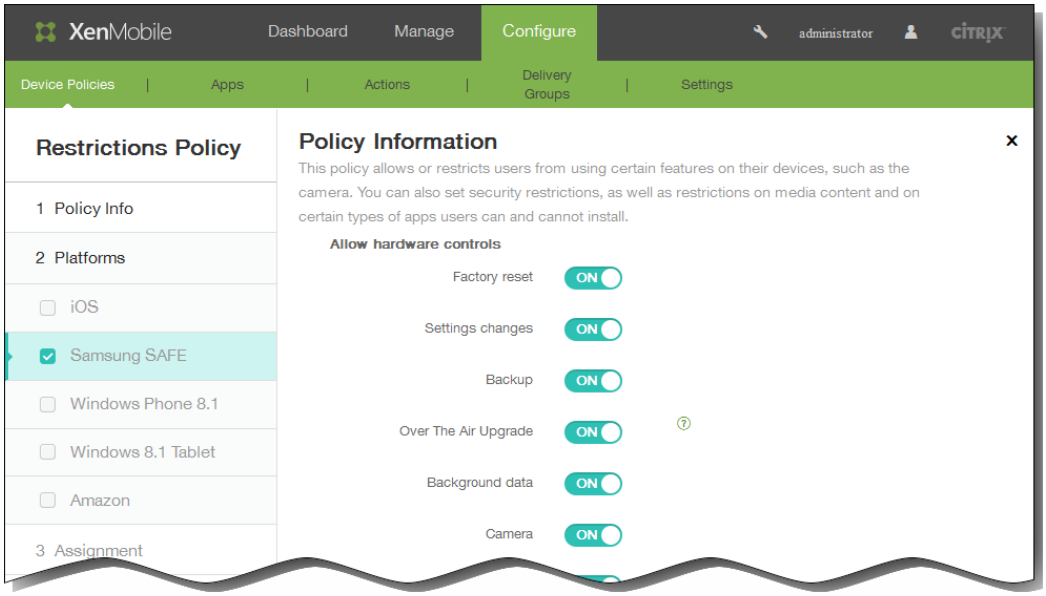
  电影：单击以下选项之一：允许所有电影、阻止电影、G、PG、PG-13、R、NC-17；默认值为允许所有电影。

  电视节目：单击以下选项之一：允许播放所有电视节目、阻止电视节目、TV-Y、TV-Y7、TV-G、TV-PG、TV-PG14、TV-MA；默认值为允许播放所有电视节目。

  应用程序：单击以下选项之一：允许所有应用程序、阻止应用程序、4+、9+、12+ 或 17+；默认值为允许所有应用程序。

- 如果选择 Samsung SAFE，可以配置以下设置：

  注意：某些选项仅适用于 Samsung Mobile Device Management API 4.0 或更高版本；这些选项标记有（MDM 4.0 及更高版本）。



- 在允许硬件控制中：

  恢复出厂设置

更改设置

备份

通过空中下载技术升级（MDM 4.0 及更高版本）

后台数据

相机

剪贴板

共享剪贴板（MDM 4.0 及更高版本）

Home 键

麦克风

伪装位置

NFC(近场通信)（MDM 4.0 及更高版本）

关闭电源（MDM 4.0 及更高版本）

屏幕快照

SD 卡

语音拨号器（MDM 4.0 及更高版本）

SBeam（MDM 4.0 及更高版本）

SVoice（MDM 4.0 及更高版本）

- 在允许使用应用程序中：

  浏览器

  YouTube

  GooglePlay/Marketplace

  允许非 Google Play 应用程序

  停止系统应用程序（MDM 4.0 及更高版本）

- 在网络中：

  Bluetooth；网络共享

  WiFi；网络共享、点对点（MDM 4.0 及更高版本）

  网络共享

  手机网络数据

允许漫游。默认值为关。

仅限安全连接

Android beam（MDM 4.0 及更高版本）

录制音频（MDM 4.0 及更高版本）

录制视频（MDM 4.0 及更高版本）

定位服务

按天限制(MB)：输入允许用户每天使用的 MB 数。默认设置为 0，表示禁用此功能。（MDM 4.0 及更高版本）

按周限制(MB)：输入允许用户每周使用的 MB 数。默认设置为 0，表示禁用此功能。（MDM 4.0 及更高版本）

按月限制(MB)：输入允许用户每月使用的 MB 数。默认设置为 0，表示禁用此功能。（MDM 4.0 及更高版本）

- 在允许执行 USB 操作中：

  调试

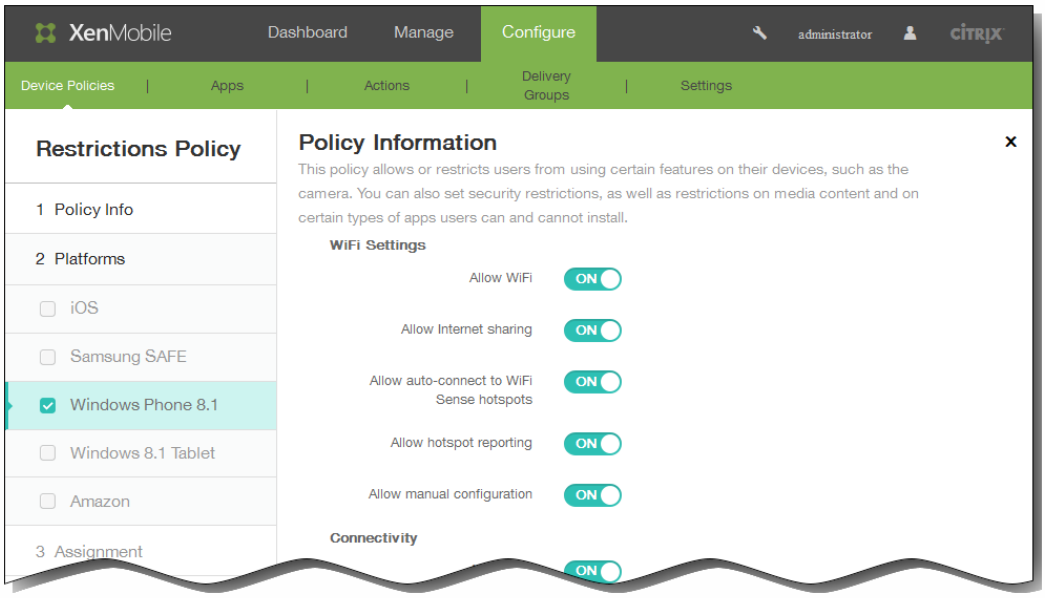
  主机存储

  大容量存储

  Kies Media Player

  网络共享

- 如果选择 Windows Phone 8.1，可以配置以下设置：



- 在 WiFi 设置中：

允许使用 WiFi

允许使用 Internet 共享

允许自动连接到 WiFi 感应热点

允许热点报告

允许手动配置

- 在连接中：

  允许使用 NFC（近场通信）

  允许使用 Bluetooth

  允许通过手机网络使用 VPN

  允许在漫游时通过手机网络使用 VPN

  允许使用 USB 连接

  允许使用手机网络数据漫游

- 在帐户中：

  允许使用 Microsoft 帐户连接

  允许非 Microsoft 电子邮件

- 在搜索中：

  允许搜索使用定位服务

  过滤成人内容（默认设置为关）。

  允许 Bing 影像存储捕获的图像

- 在 System（系统）中：

  允许使用存储卡

  允许使用定位服务

  允许使用相机

  遥测：单击以下其中一项设置：允许、不允许、允许，辅助数据请求除外。默认设置为允许。

- 在安全性中：

  允许手动安装根证书

  要求设备加密默认设置为关。

  允许复制粘贴

允许屏幕捕获

允许录制音频

允许另存为办公文件

允许显示操作中心通知

允许使用 Cortana

允许同步设备设置

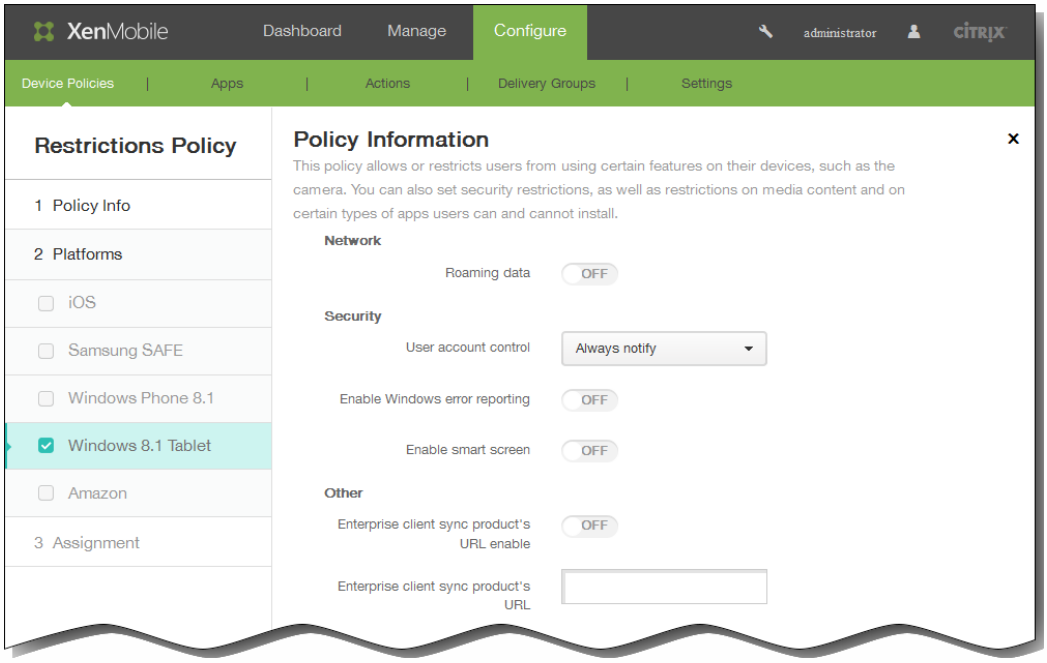
- 在应用程序中：

  允许访问应用商店

  允许开发人员解锁

  允许使用 Web 浏览器访问

- 如果选择 Windows 8.1 tablet，可以配置以下设置：



- 在网络中：

  漫游数据

- 在安全性中：

  用户帐户控制：在列表中，单击以下其中一项设置：始终通知、通知应用程序更改、通知应用程序更改(不暗显)、从不通知。默认设置为从不通知。

  启用 Windows 错误报告

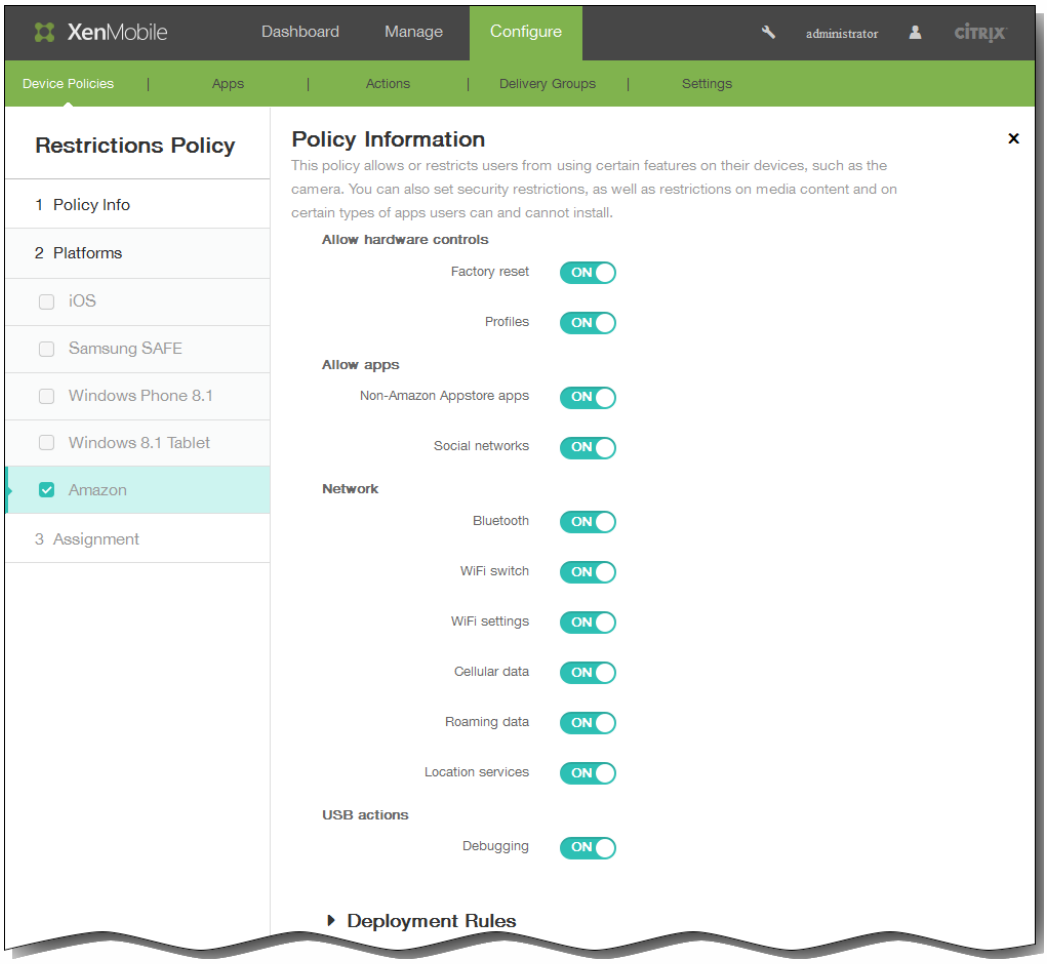
启用智能屏幕

- Other（其他）：

  企业客户端同步产品的 URL 启用

  企业客户端同步产品的 URL：键入有效的 URL 地址。

- 如果选择 Amazon，可以配置以下设置：



- 在允许硬件控制中：

  恢复出厂设置

  配置文件

- 在允许使用应用程序中：

  非 Amazon Appstore 应用程序

  社交网络

- 在网络中：

Bluetooth

WiFi 开关

WiFi 设置

手机网络数据

漫游数据

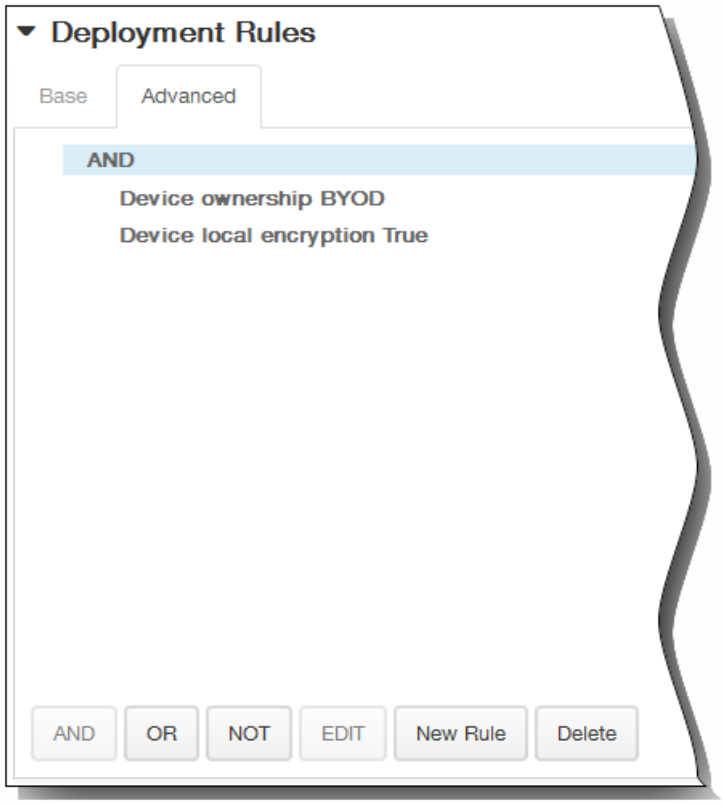
定位服务

- USB 操作：

  调试

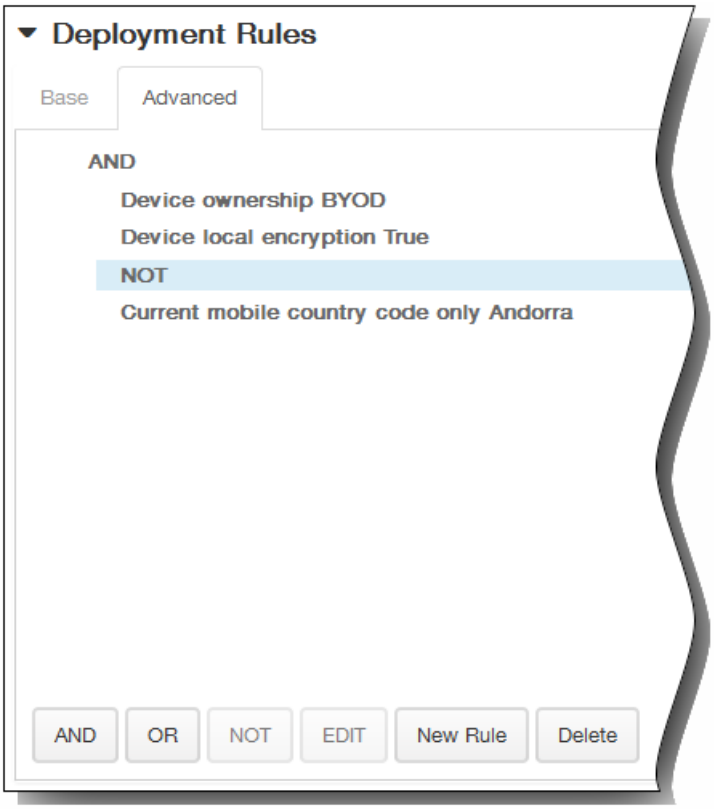
6. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

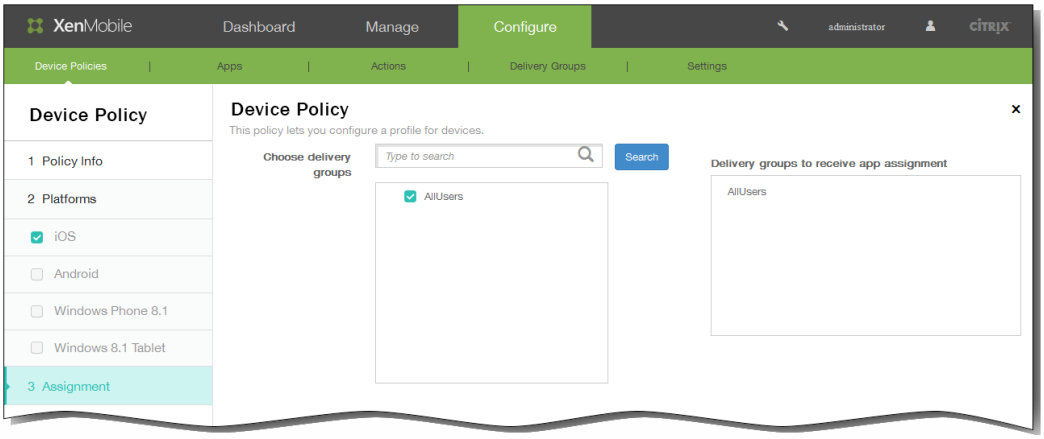


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。

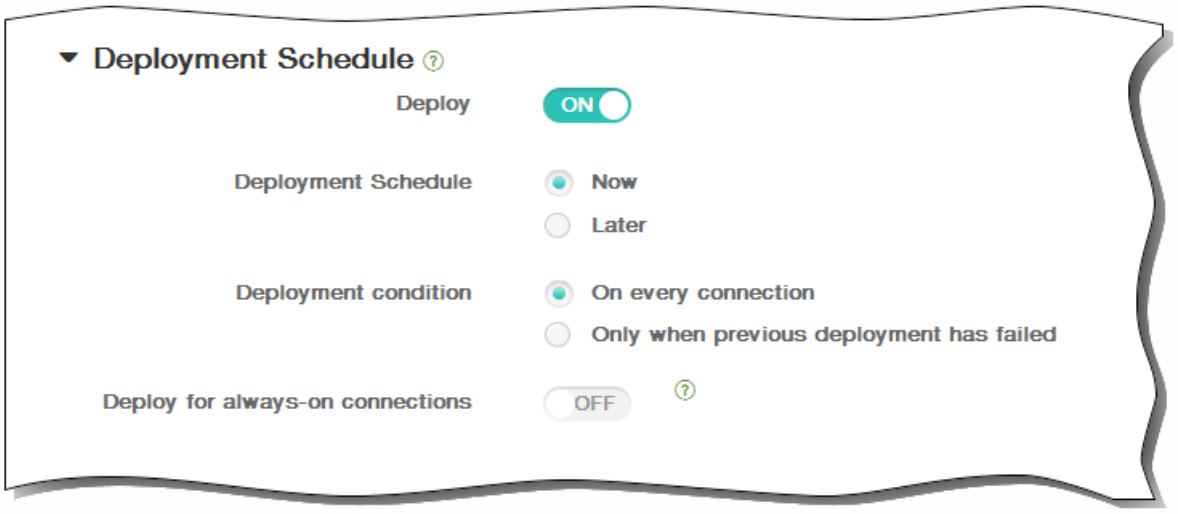


7. 配置完一个或多个平台的设置后，单击下一步，将显示分配页面。
8. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



9. 展开部署计划，然后配置以下设置：
   1. 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。
   2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
   3. 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。
   4. 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。
   5. 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。



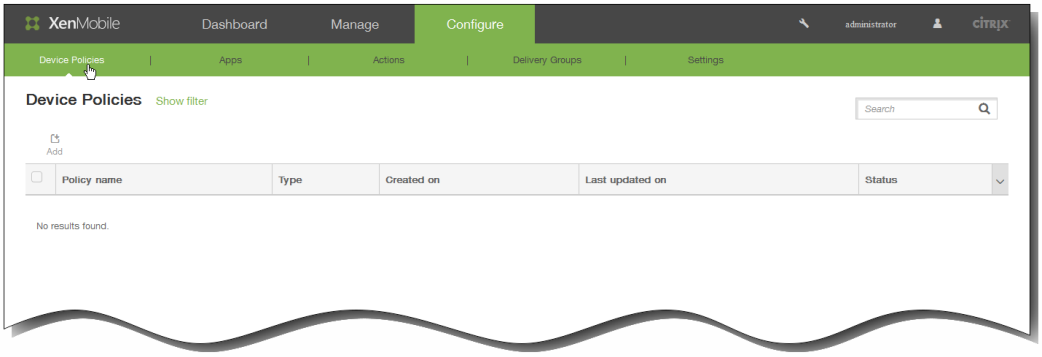
10. 单击保存以保存此策略。

添加适用于 iOS 的漫游设备策略

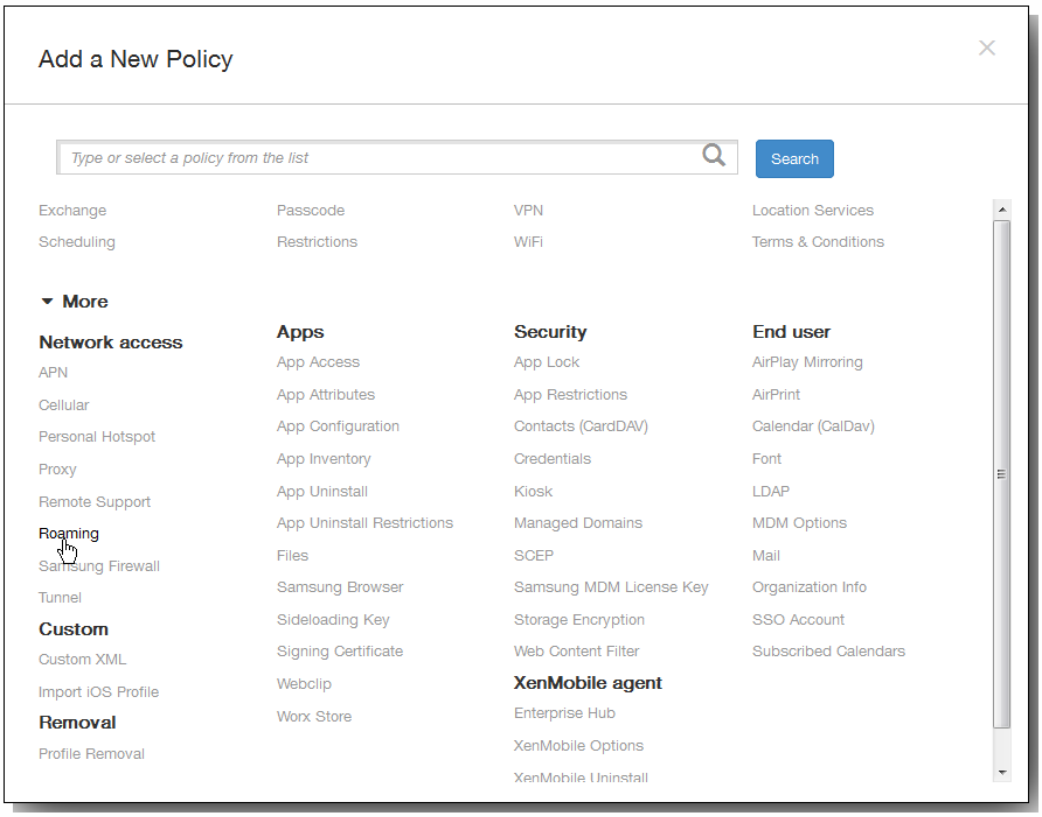
May 05, 2016

可以在 XenMobile 中添加一个设备策略，以配置在用户 iOS 设备上是否允许语音和数据漫游。禁用语音漫游时，会自动禁用数据漫游。此策略仅适用于 iOS 5.0 及更高版本的设备。

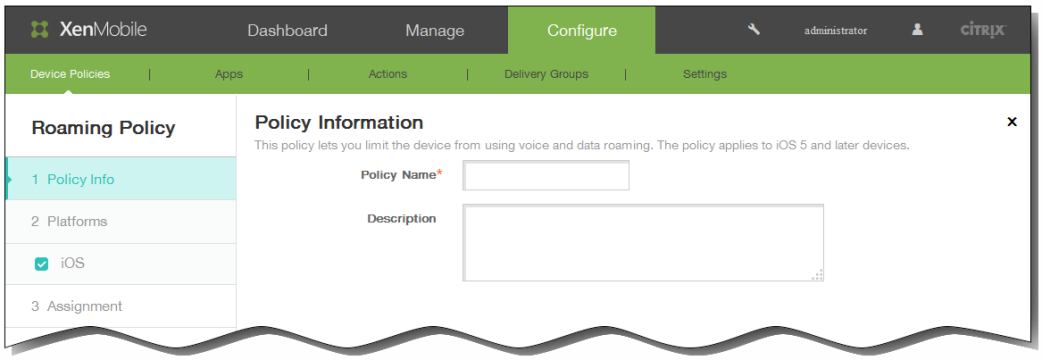
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



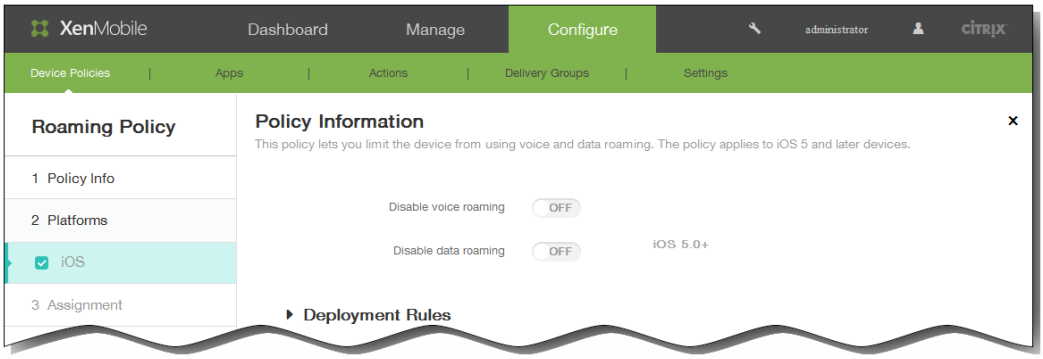
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在网络访问下面，单击漫游。 此时将显示漫游信息策略页面。



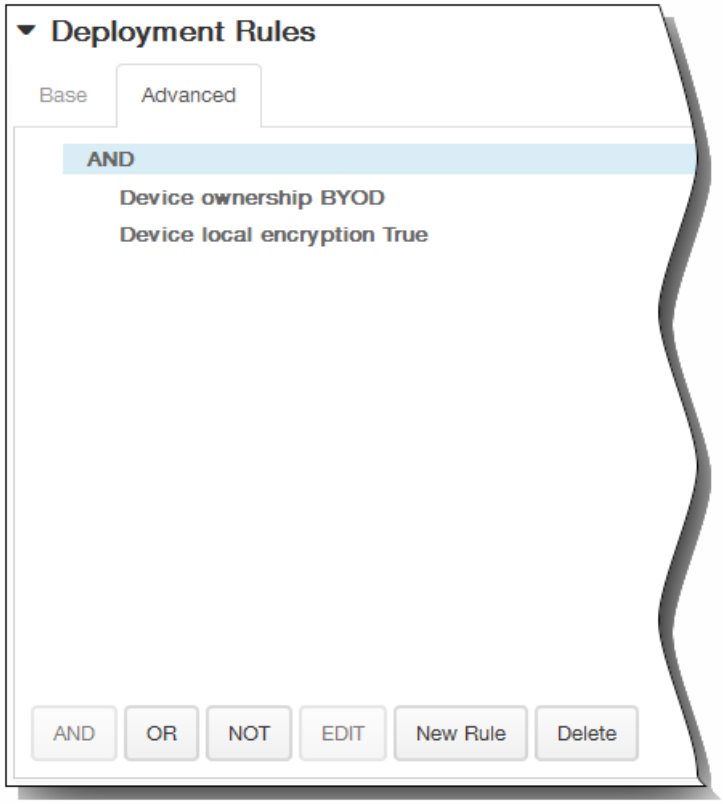
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。



6. 在 iOS 平台信息页面上，输入以下信息：
   1. 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。 默认设置为关，表示允许语音漫游。
   2. 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。 默认设置为关，表示允许数据漫游。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

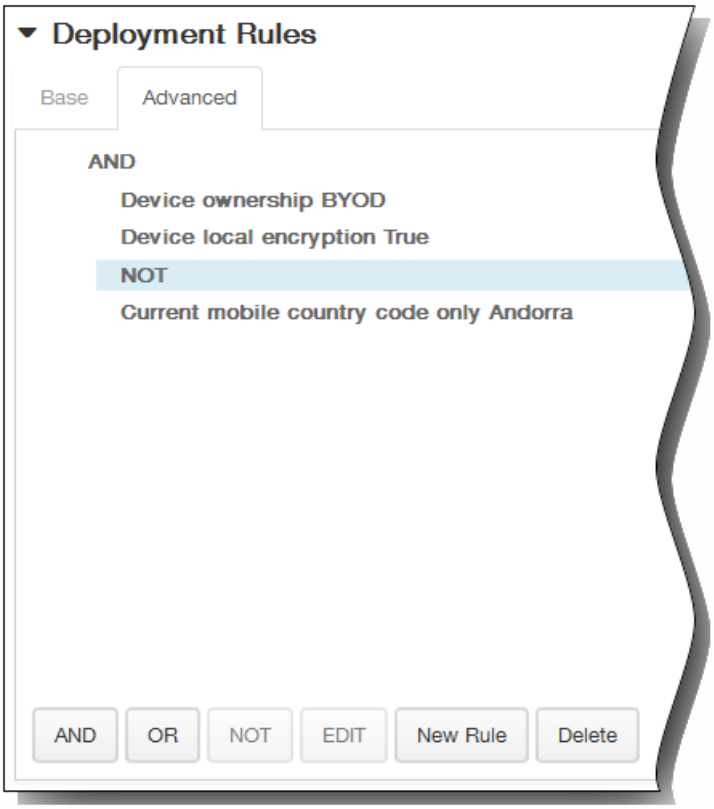
   1. 在此列表中，单击选项以确定部署策略的时间。
      1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
      2. 单击新建规则以定义条件。
      3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
      4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。

2. 单击高级选项卡以使用布尔选项组合规则。

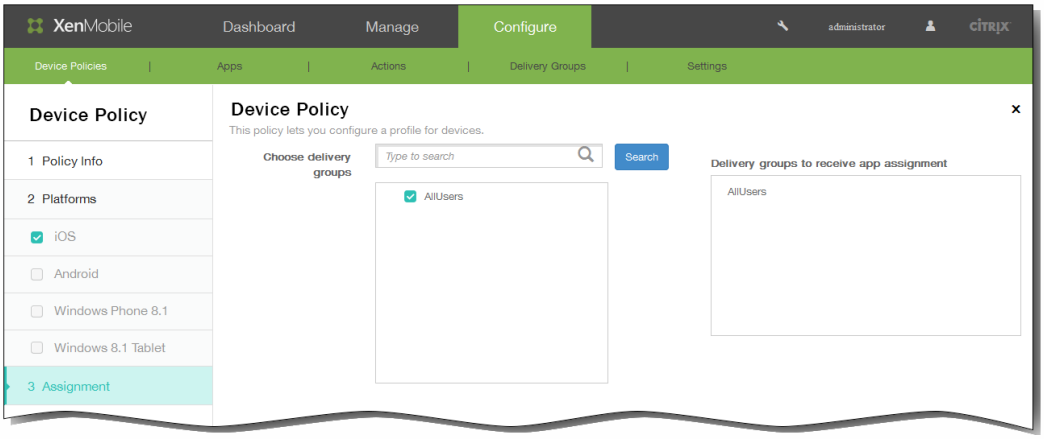


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



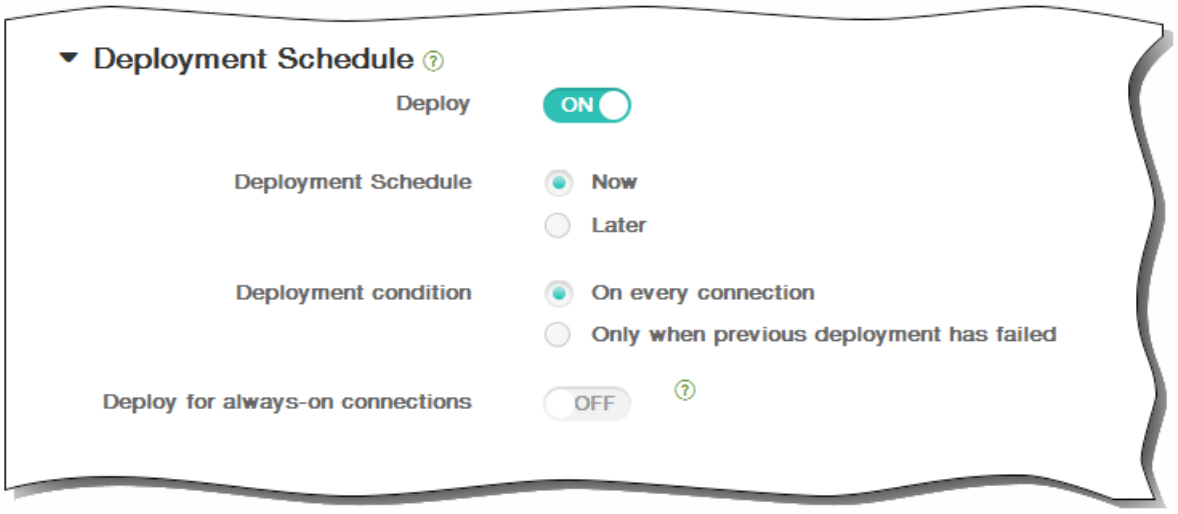
8. 单击下一步。 此时将显示漫游信息策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



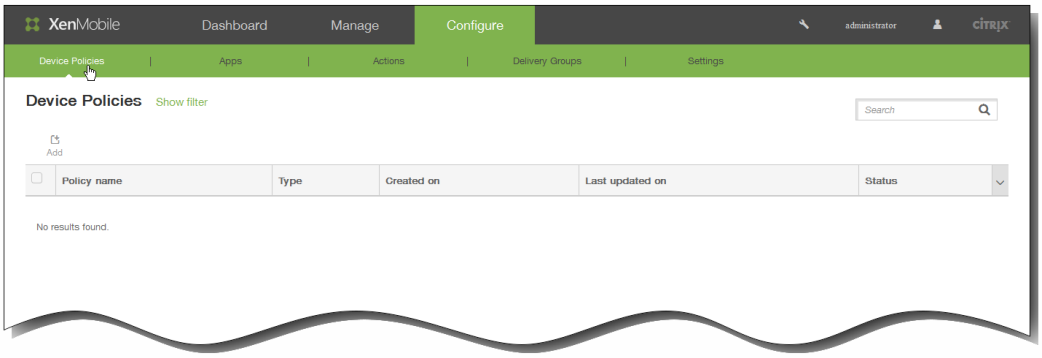
11. 单击保存以保存此策略。

添加适用于 iOS 的 SCEP 设备策略

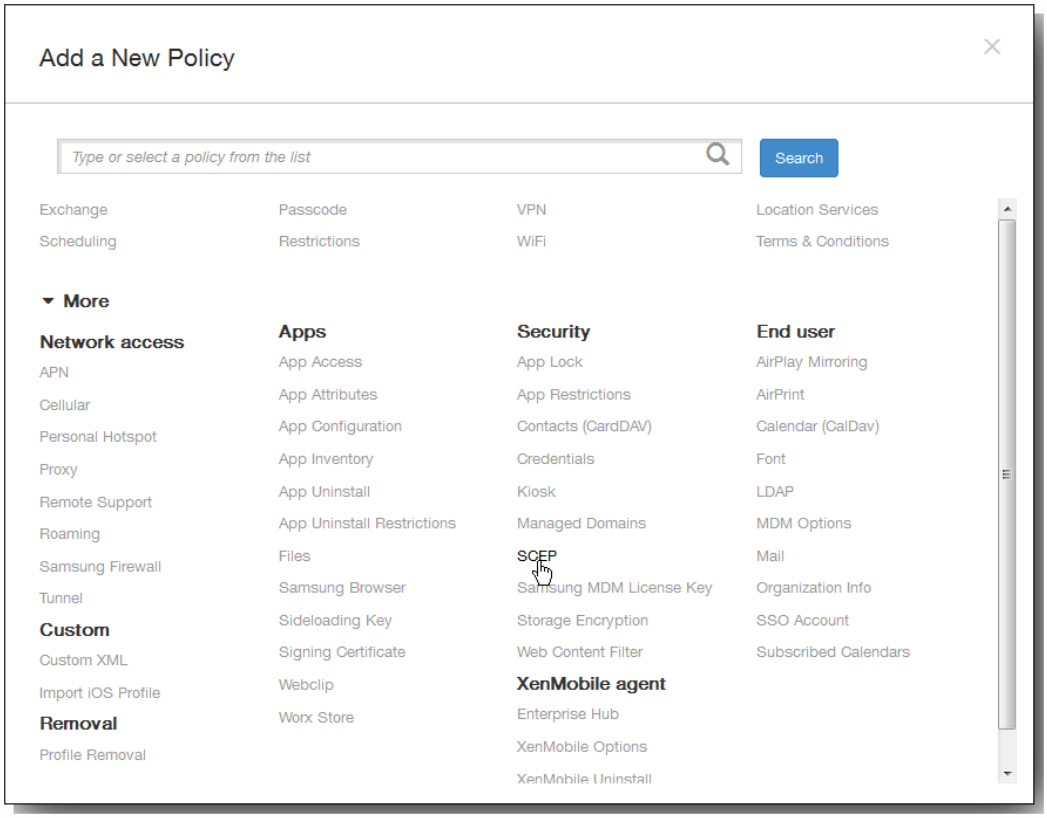
May 05, 2016

利用此策略，可以将 iOS 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。

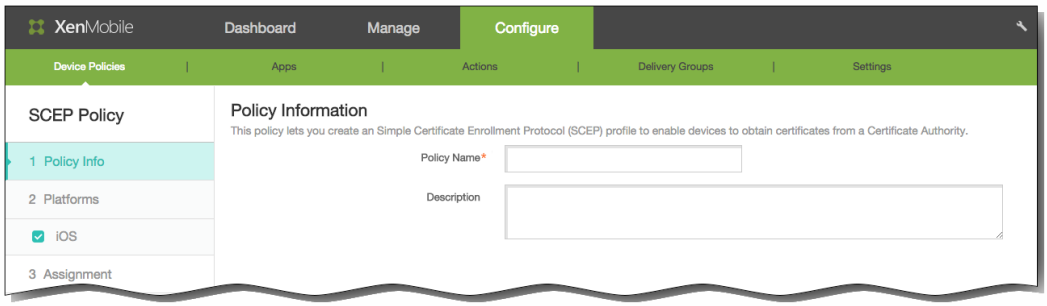
1. 在 XenMobile 控制台中，单击配置 > 设备策略。
   此时将显示设备策略页面。



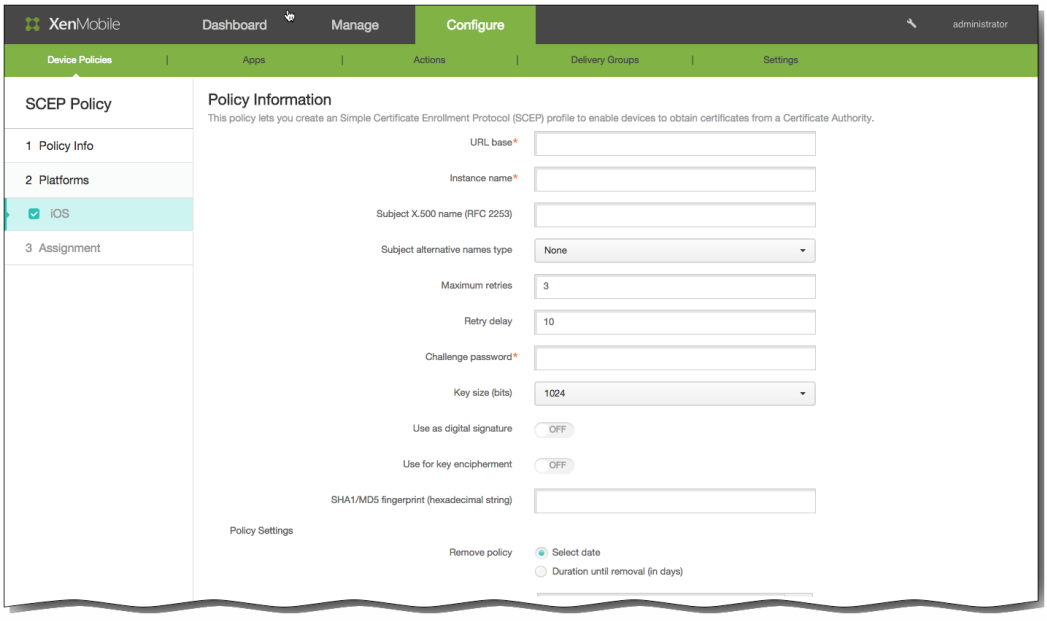
2. 单击添加。
   将显示添加新策略页面。



3. 在添加新策略页面上，单击更多，然后在安全性下方，单击 SCEP。
   此时将显示 SCEP 策略信息页面。



4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 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。

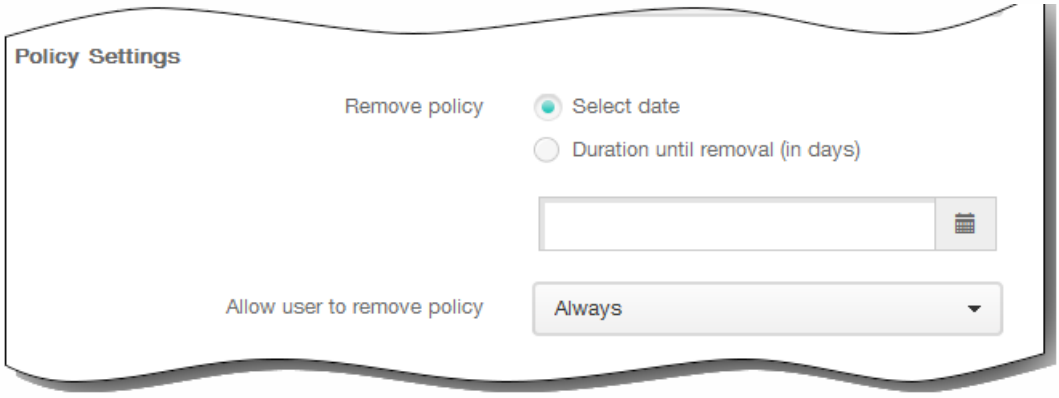


6. 在 iOS 平台信息页面上，输入以下信息：
   1. URL 库：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。 由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。 但是，如果允许重复使用一次性密码，则应该使用 HTTPS 来保护密码。 此步骤不是必需步骤。
   2. 实例名称：键入任何 SCEP 服务器可以识别的字符串。 例如，可以是类似 example.org 的域名。 如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。 此步骤不是必需步骤。
   3. 使用者 X.500 名称 (RFC 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)。

4. 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。
5. 最大重试次数：键入用户输入错误密码后允许的重试次数。 默认值为 3。
6. 重试延迟：键入用户超过最大重试次数并强制锁定的时间间隔。 默认值为 10。
7. 质询密码：输入预共享密钥。 此步骤不是必需步骤。
8. 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。
9. 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。
10. 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。
11. 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。

7. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。

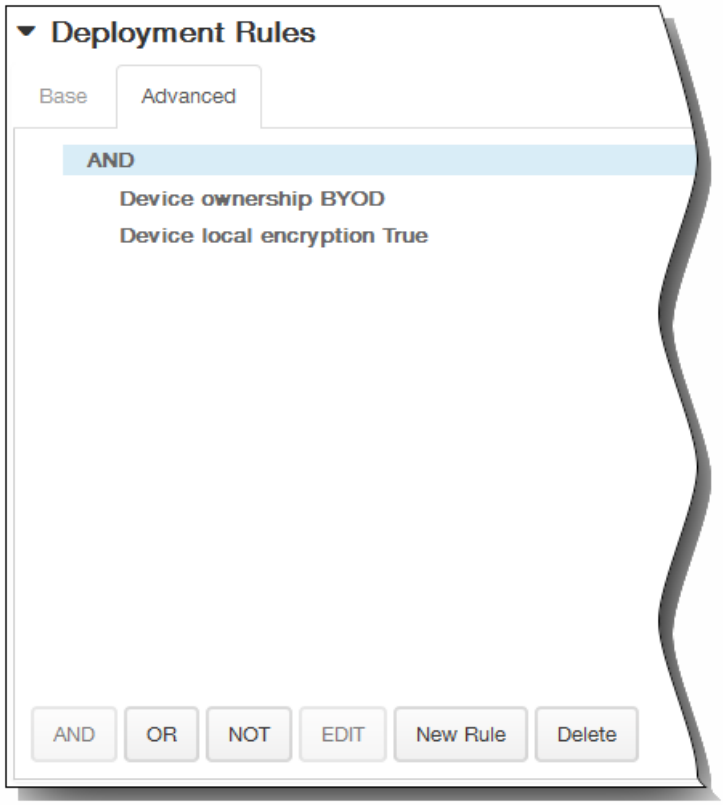


11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。

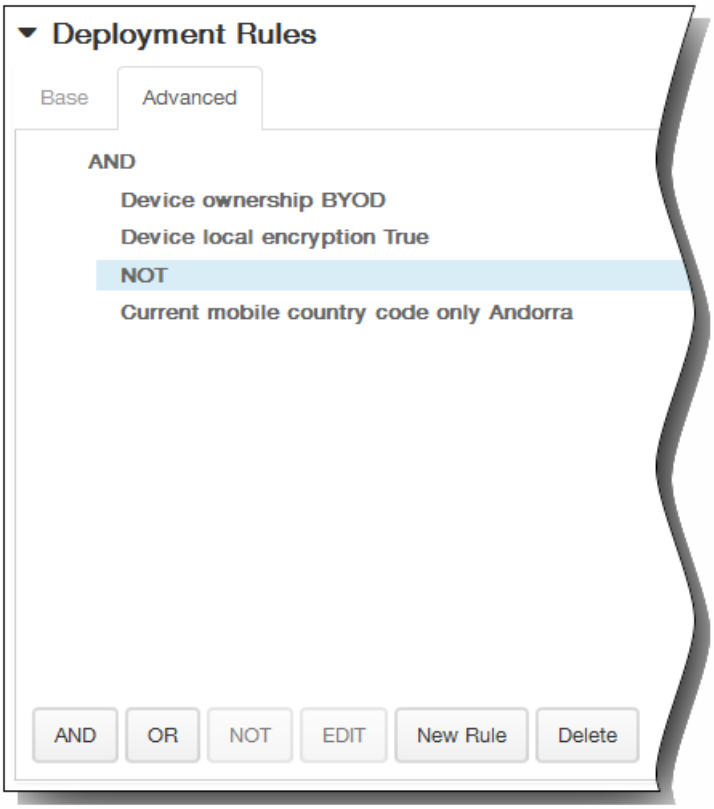
2. 单击新建规则以定义条件。
3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。

2. 单击高级选项卡以使用布尔选项组合规则。

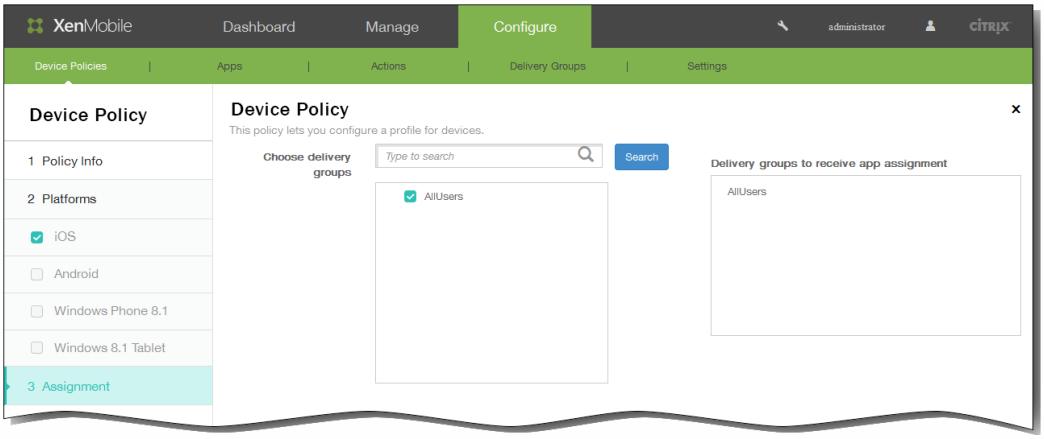


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



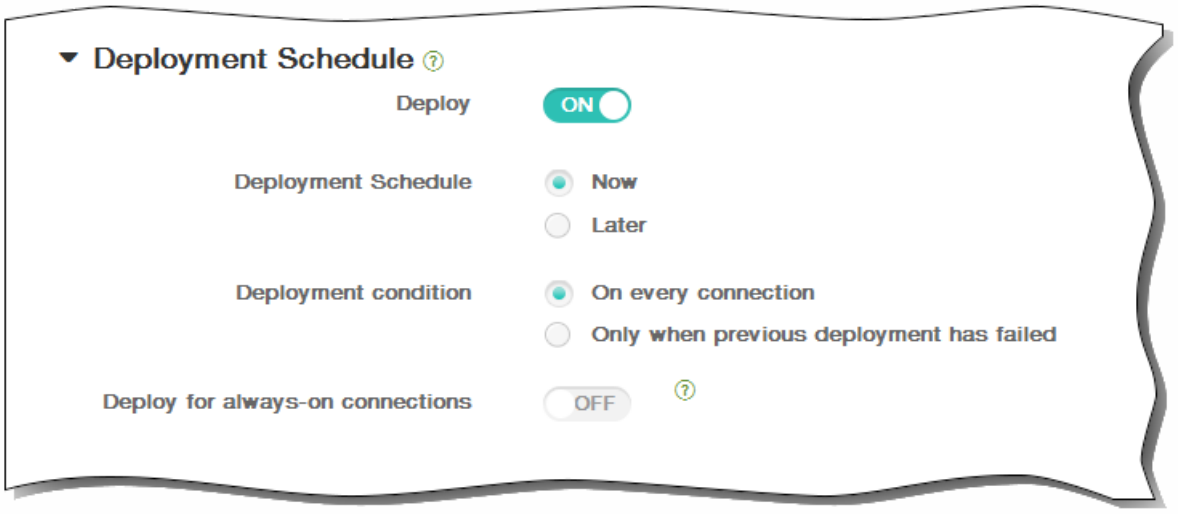
12. 单击下一步。 此时将显示 SCEP 策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



15. 单击保存以保存此策略。

Samsung MDM 许可证密钥设备策略

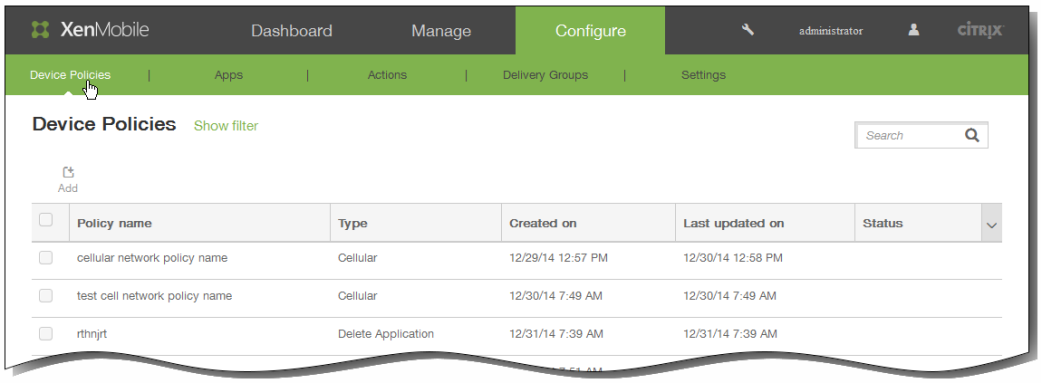
May 05, 2016

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。

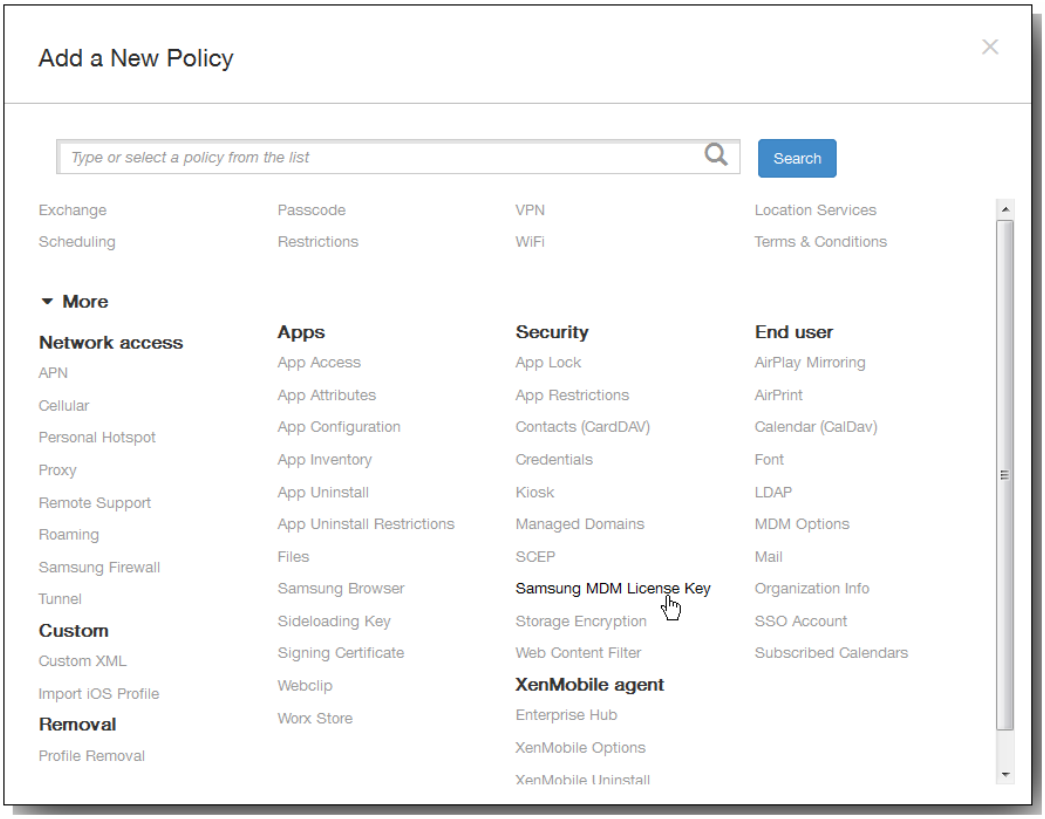
必须通过向设备部署内置 Samsung Enterprise License Management (ELM) 密钥来启用 SAFE API，才能部署 SAFE 策略和限制。要启用 Samsung KNOX API，除部署 Samsung ELM 密钥外，还需要使用 Samsung KNOX License Management System (KLMS) 购买 Samsung KNOX 许可证。Samsung KLMS 为移动设备管理解决方案提供有效的许可证，以使其能够在移动设备上激活 Samsung KNOX API。这些许可证必须从 Samsung 获取，Citrix 不提供。

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。

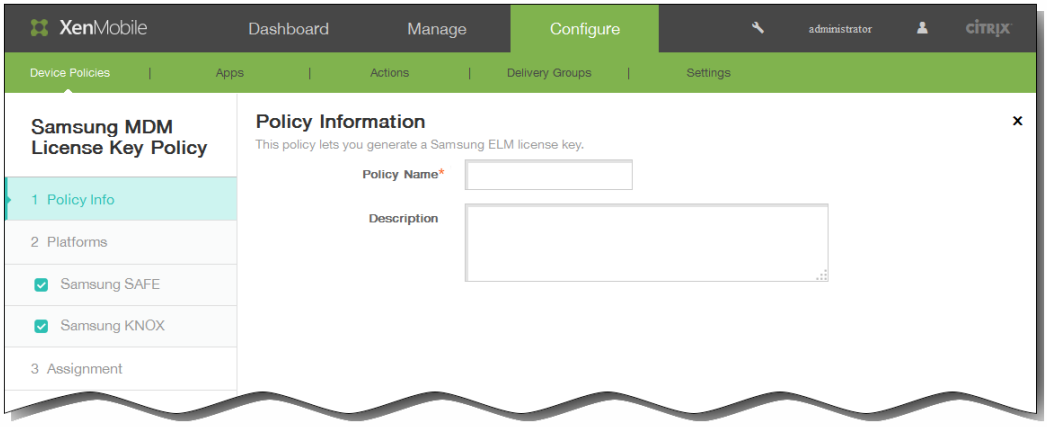
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



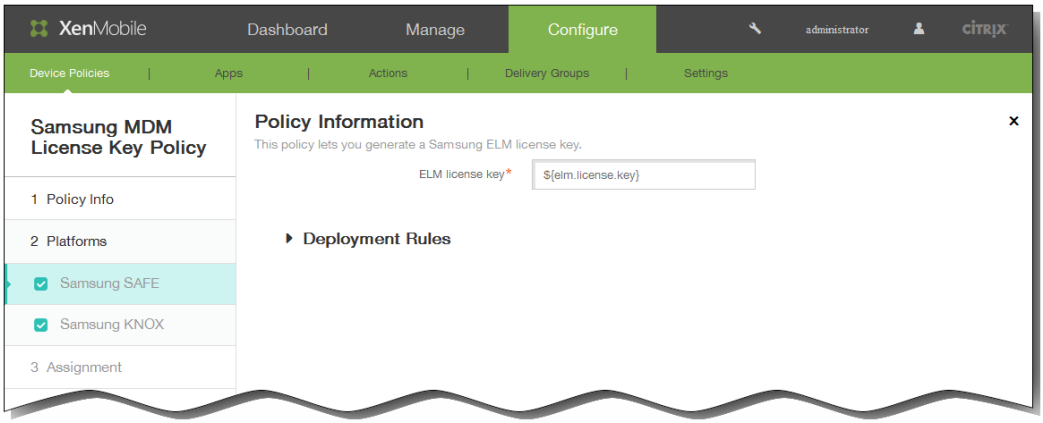
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。

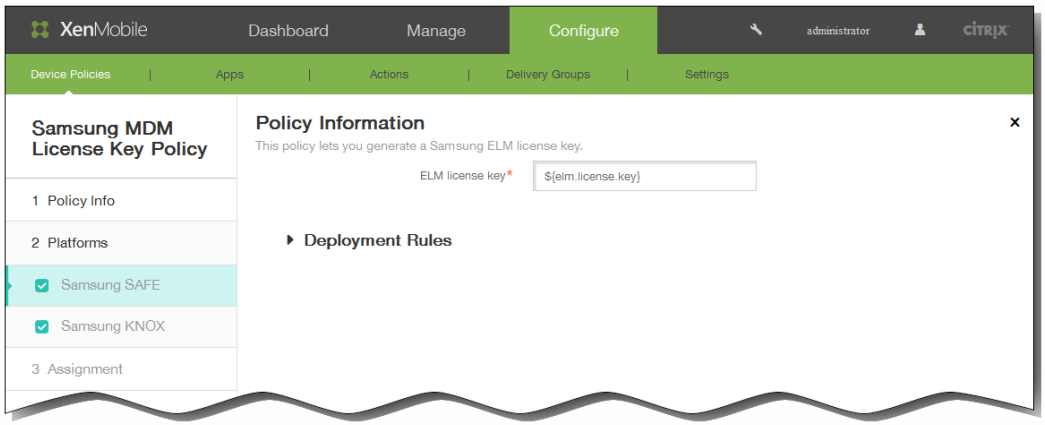


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
5. 单击下一步。 此时将显示策略平台页面。
   注意：策略平台页面显示时，两个平台都处于选中状态，您首先看到 Samsung SAFE 平台配置面板。

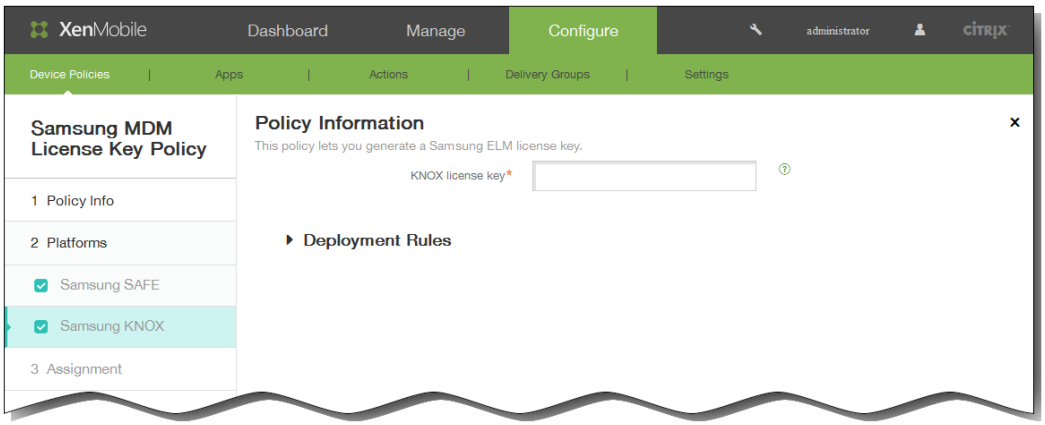


6. 在平台下面，选择要创建此策略的 Samsung 平台。 清除任何其他可能选中但又不想包含在此策略中的平台。

   - 如果选择 Samsung SAFE，对于 ELM 许可证密钥，请输入宏 ${elm.license.key} 以生成 ELM 许可证密钥。此字段应该已包含此宏：

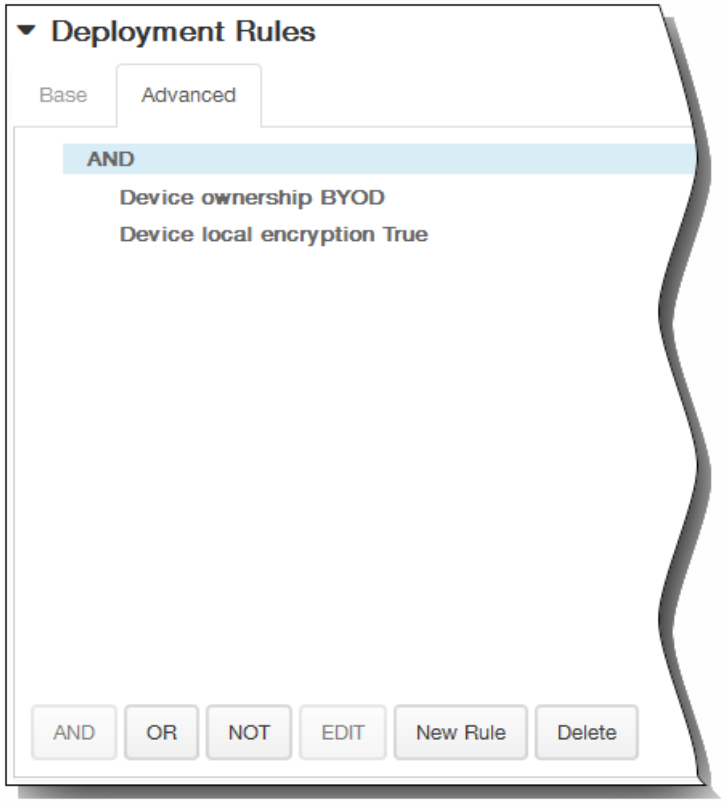


   - 如果选择 Samsung KNOX，对于 KNOX 许可证密钥，请输入 25 位 KNOX 许可证密钥：



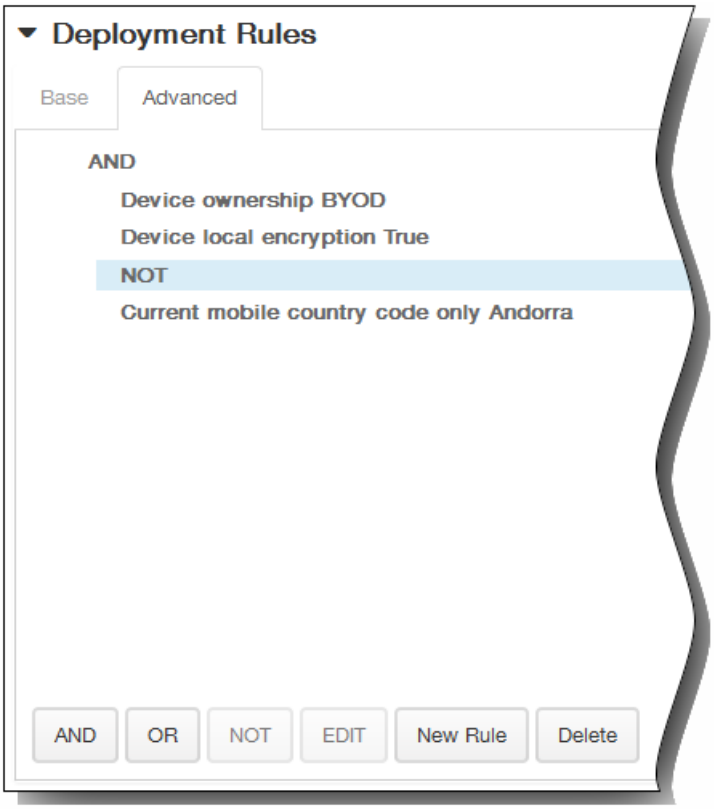
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

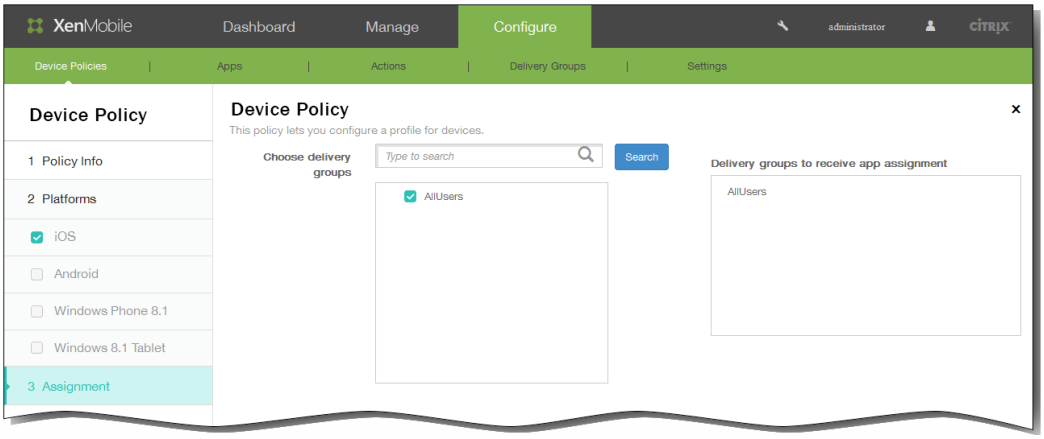


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



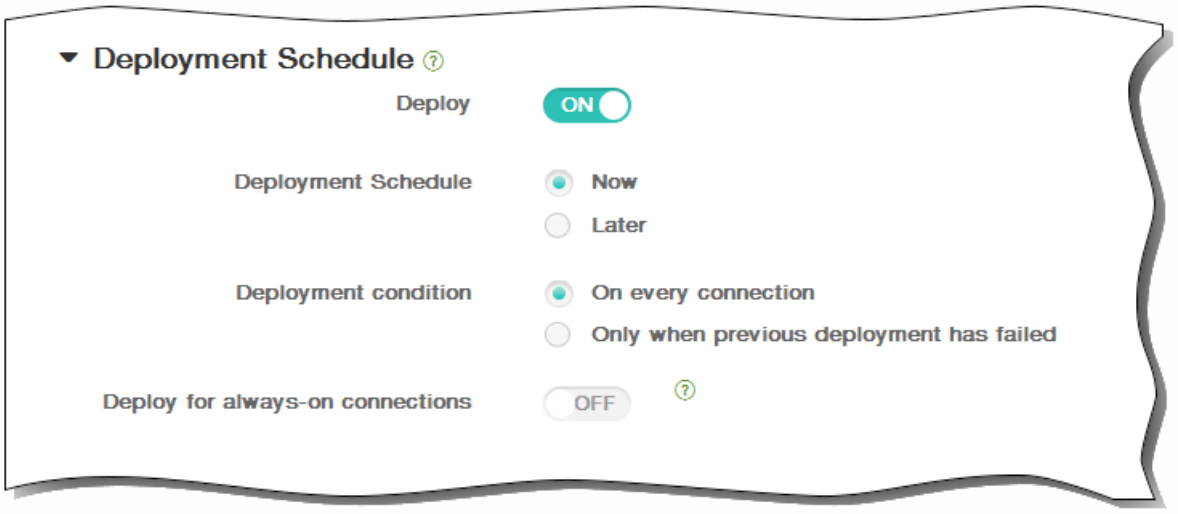
8. 单击下一步。 此时将显示 Samsung MDM 许可证密钥策略页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



11. 单击保存以保存此策略。

存储加密设备策略

May 05, 2016

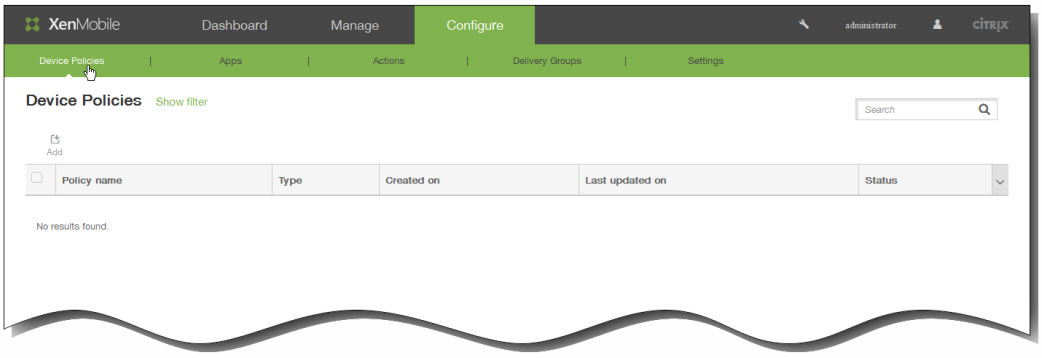
在 XenMobile 中创建存储加密设备策略，以加密内部存储和外部存储，并根据设备阻止用户在其设备上使用存储卡。

可以创建适用于 Samsung SAFE、Windows 8.1 Tablet 和 Android Sony 设备的策略。每个平台都需要一组不同的值，这些值将在以下步骤中详细说明。

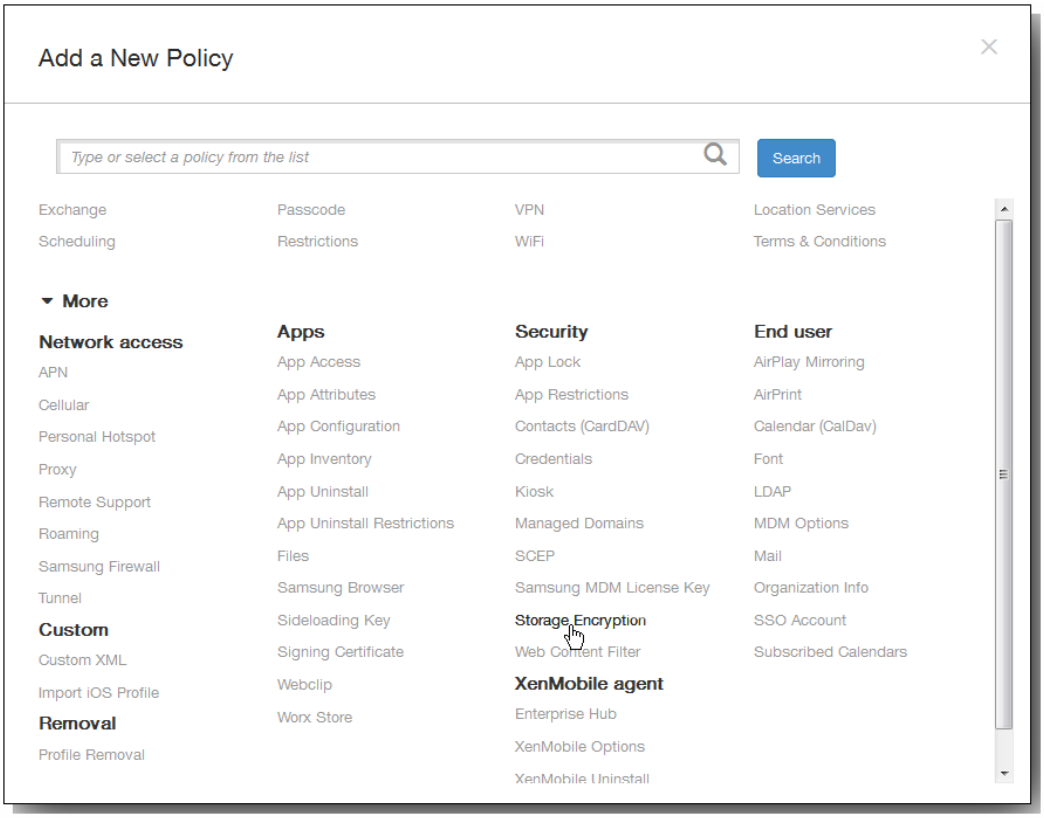
注意：对于 Samsung SAFE 设备，在配置此策略之前，请确保满足以下要求：

- 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。

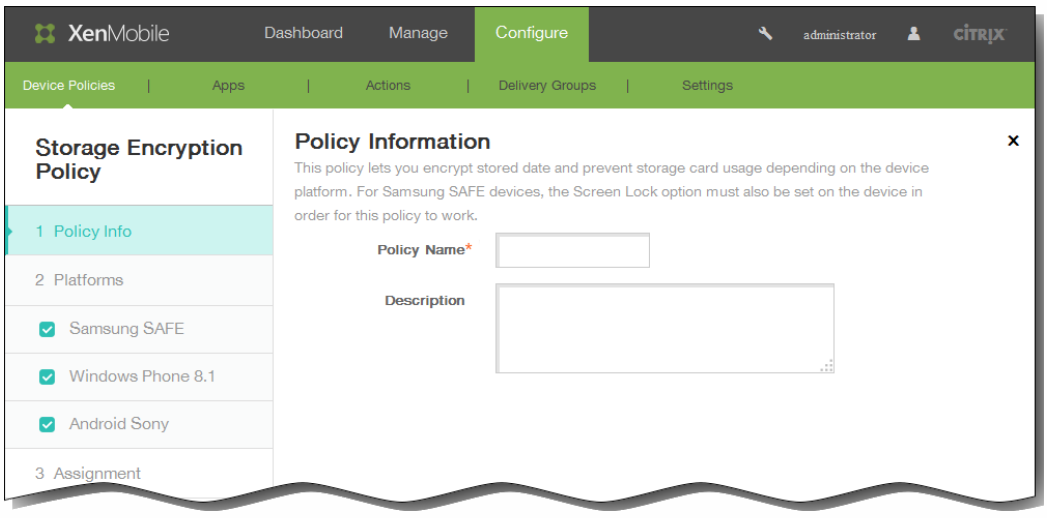
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



2. 单击添加添加新策略。 此时将显示添加新策略对话框。

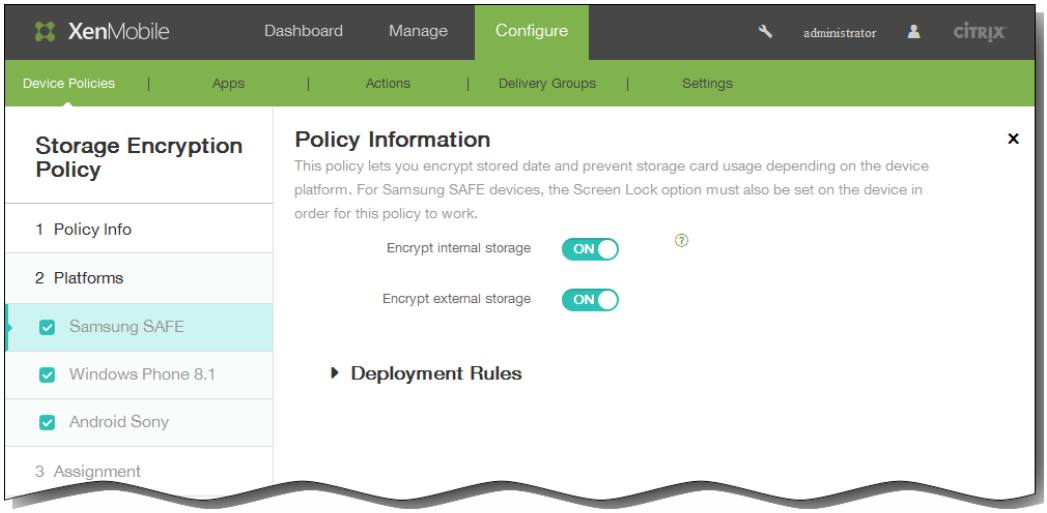


3. 单击更多，然后在安全性下面，单击存储加密。 此时将显示存储加密策略信息页面。

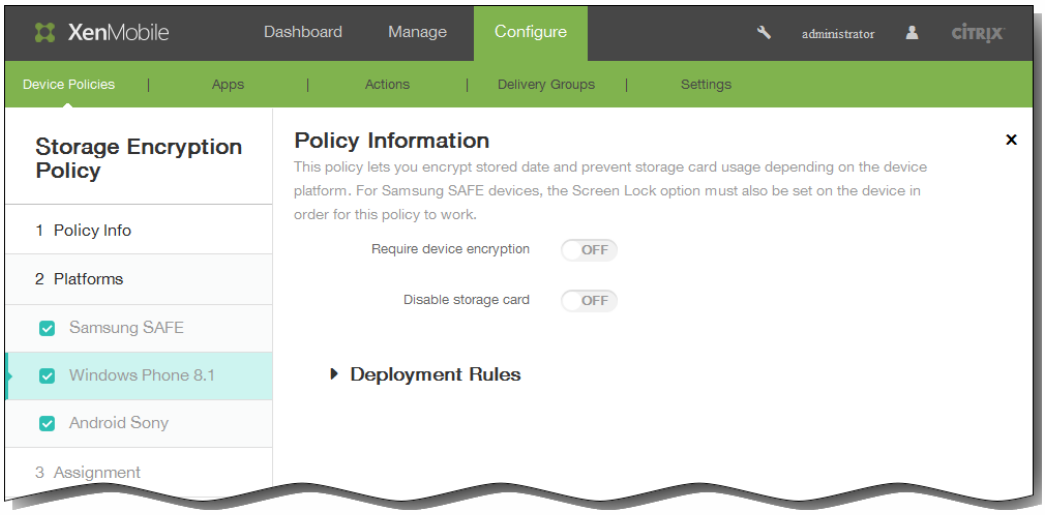


4. 在策略信息窗格中，键入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
5. 单击下一步。 此时将显示策略平台页面。
   注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 Samsung SAFE 平台配置面板。
6. 在平台下面，选择要配置此策略的平台。 如果只配置该平台，请清除可能选中的其他平台。
   - 如果选择 Samsung SAFE：

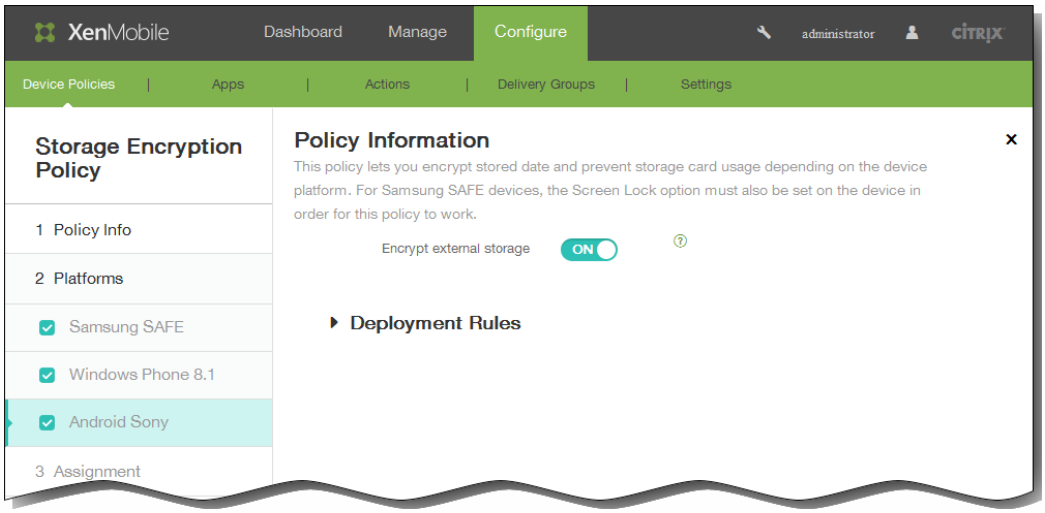
- 加密内部存储：选择是否加密用户设备上的内部存储。内部存储包括设备内存和内部存储器。默认值为开。
- 加密外部存储：选择是否加密用户设备上的外部存储。默认值为开。



- 如果选择 Windows Phone 8.1：
  - 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。

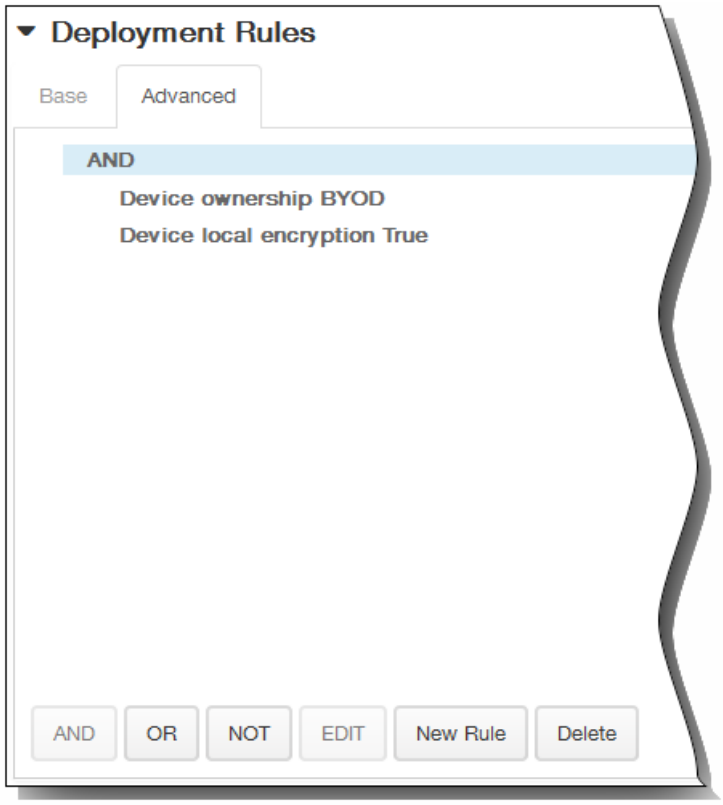


- 如果选择 Android Sony，对于加密外部存储，选择是否在用户设备上加密外部存储。设备必须使用包含数字和字母或符号的密码。默认值为开。



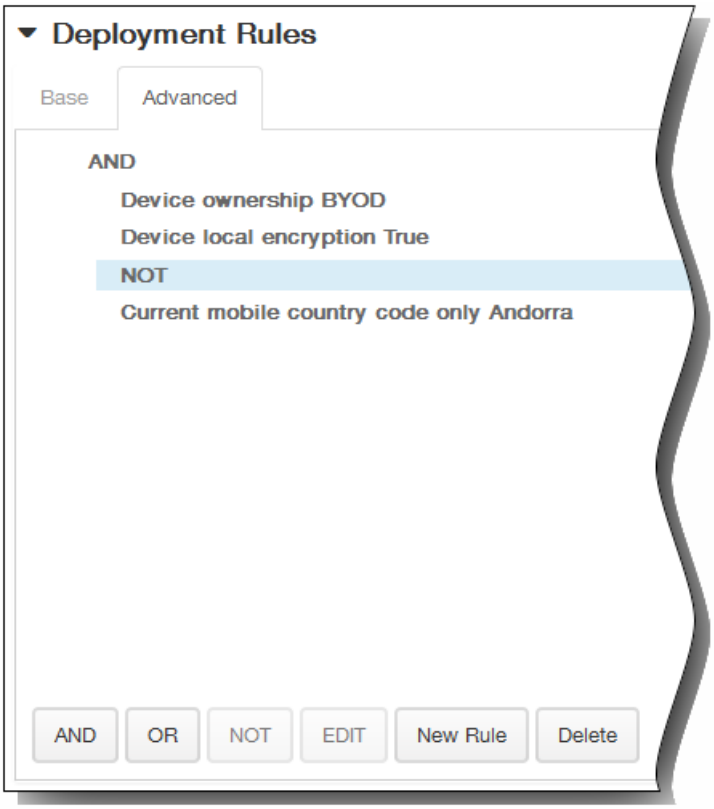
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

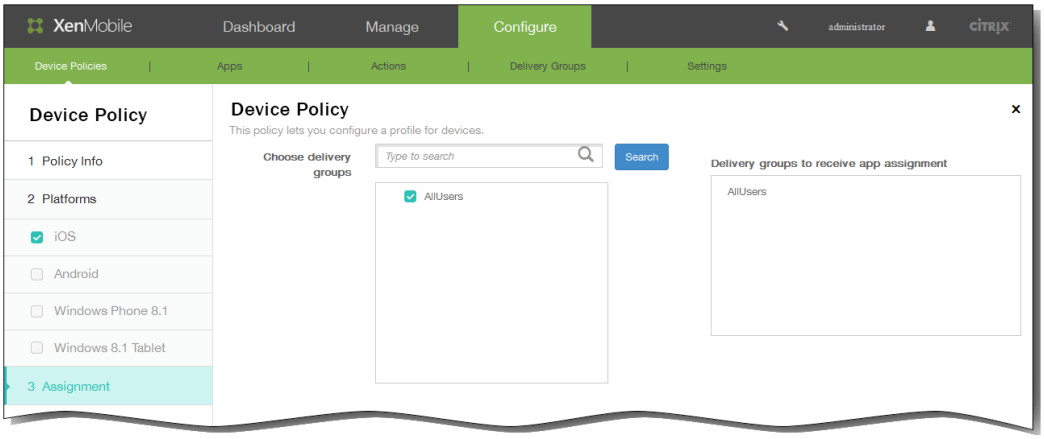


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。

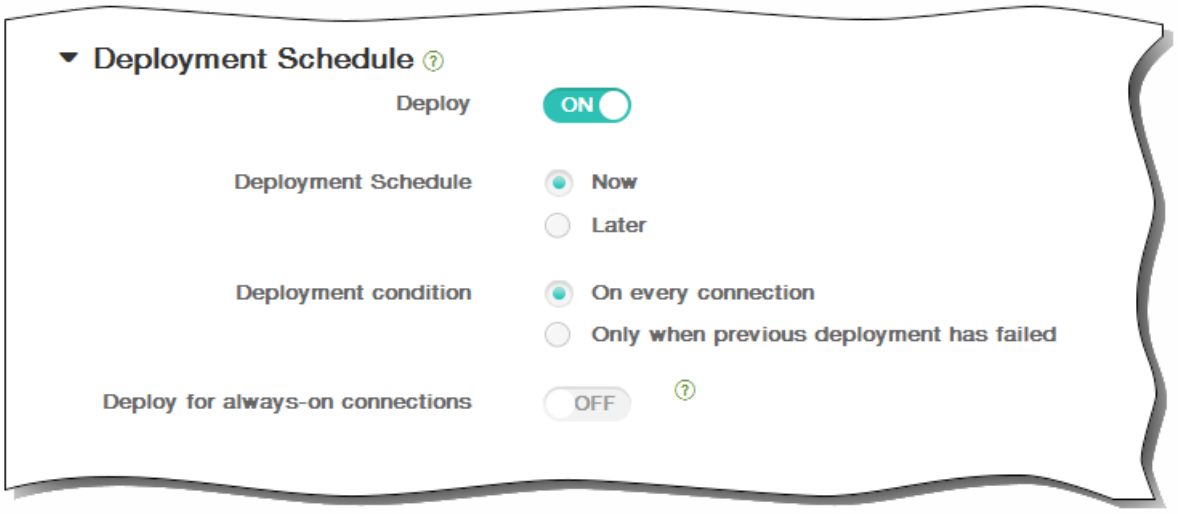


8. 单击下一步。 此时将显示 Storage Encryption Policy（存储加密策略）分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



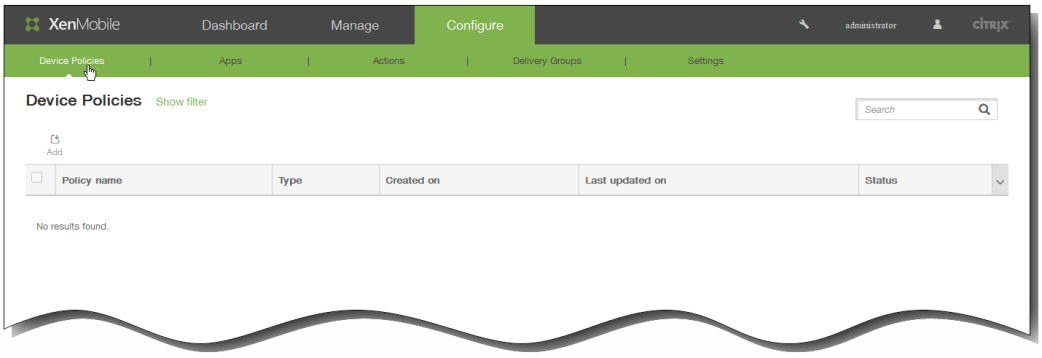
11. 单击保存以保存此策略。

添加适用于 iOS 的 Web 内容设备策略

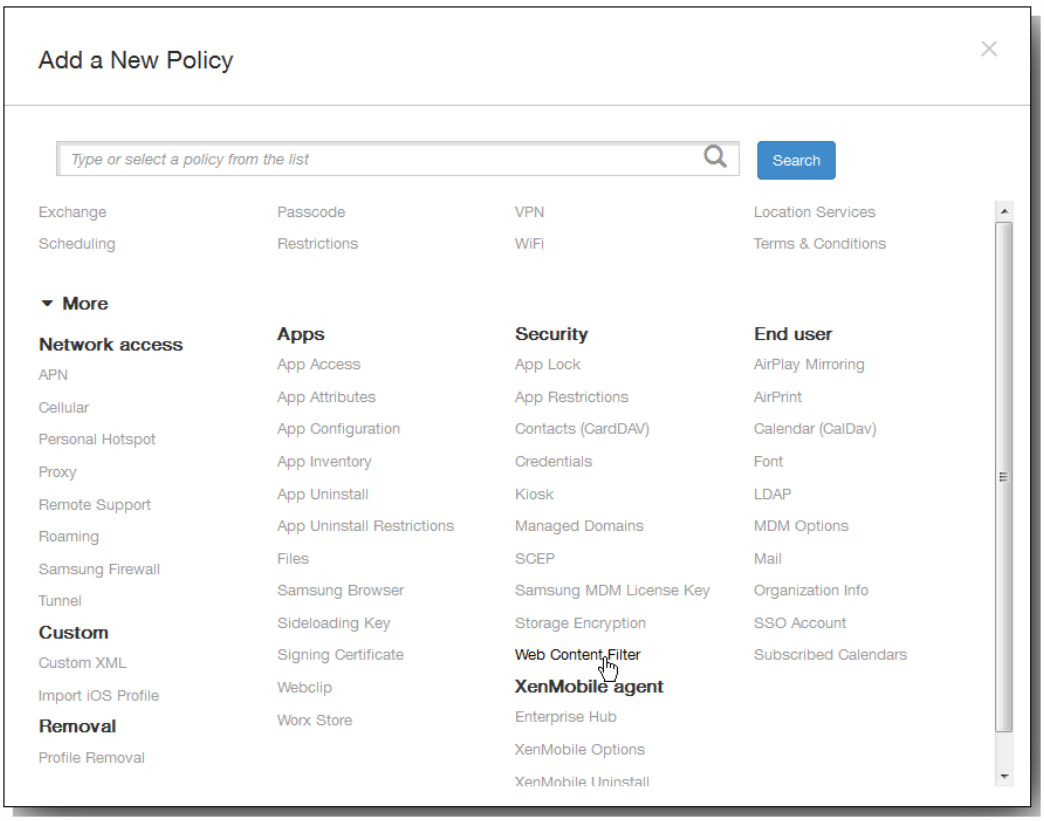
May 05, 2016

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。

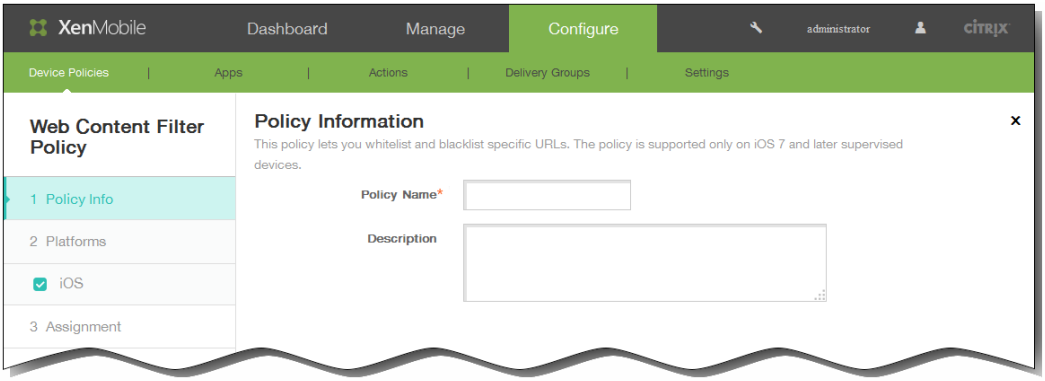
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



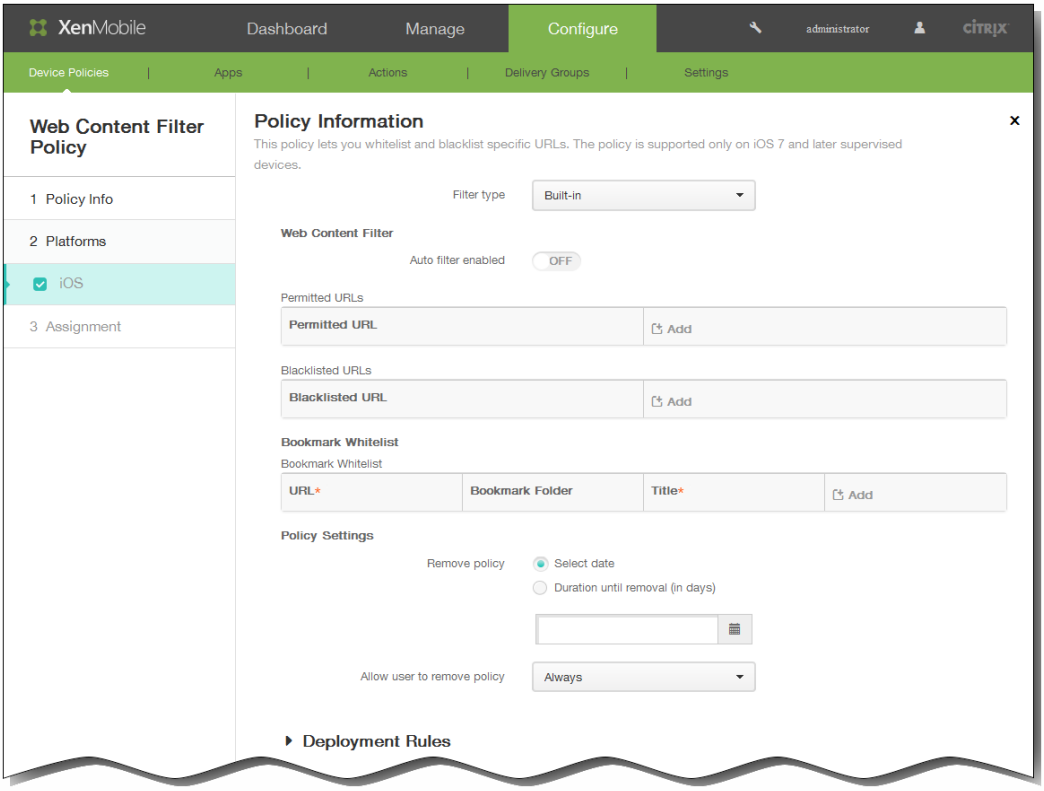
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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：
   1. 策略名称：键入策略的描述性名称。
   2. 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。



6. 在 iOS 平台信息页面中的 Filter type（过滤器类型）列表中，执行以下操作之一，然后按照本主题后面有关所选选项的过程操作。
   - 保留默认的内置过滤器类型。
   - 单击内置以配置内置过滤器类型。

   配置内置过滤器类型

   1. 已启用自动过滤：选择是否使用 Apple 的自动过滤功能来分析 Web 站点是否包含不合适的内容。 默认值为关。
   2. 允许访问的 URL：将已启用自动过滤设置为关时将忽略此列表。 将已启用自动过滤设置为开时，此列表中的项目始终可以访问，不管自动过滤器是否允许访问。

单击添加，然后执行以下操作，将 Web 站点添加到白名单中：

1. 输入允许访问的 Web 站点的 URL。必须在 Web 地址前添加 http:// 或 https://。
2. 单击保存将 Web 站点保存到白名单中，或单击取消不保存此站点。
3. 为要添加的每个应用程序重复步骤 i.和 ii.。

3. 加入黑名单的 URL：此列表中的项目始终被阻止。
   单击添加，然后执行以下操作，将 Web 站点添加到黑名单中：

   1. 输入要阻止的 Web 站点的 URL。必须在 Web 地址前添加 http:// 或 https://。
   2. 单击保存将 Web 站点保存到黑名单中，或单击取消不保存此站点。
   3. 为要添加的每个应用程序重复步骤 i.和 ii.。

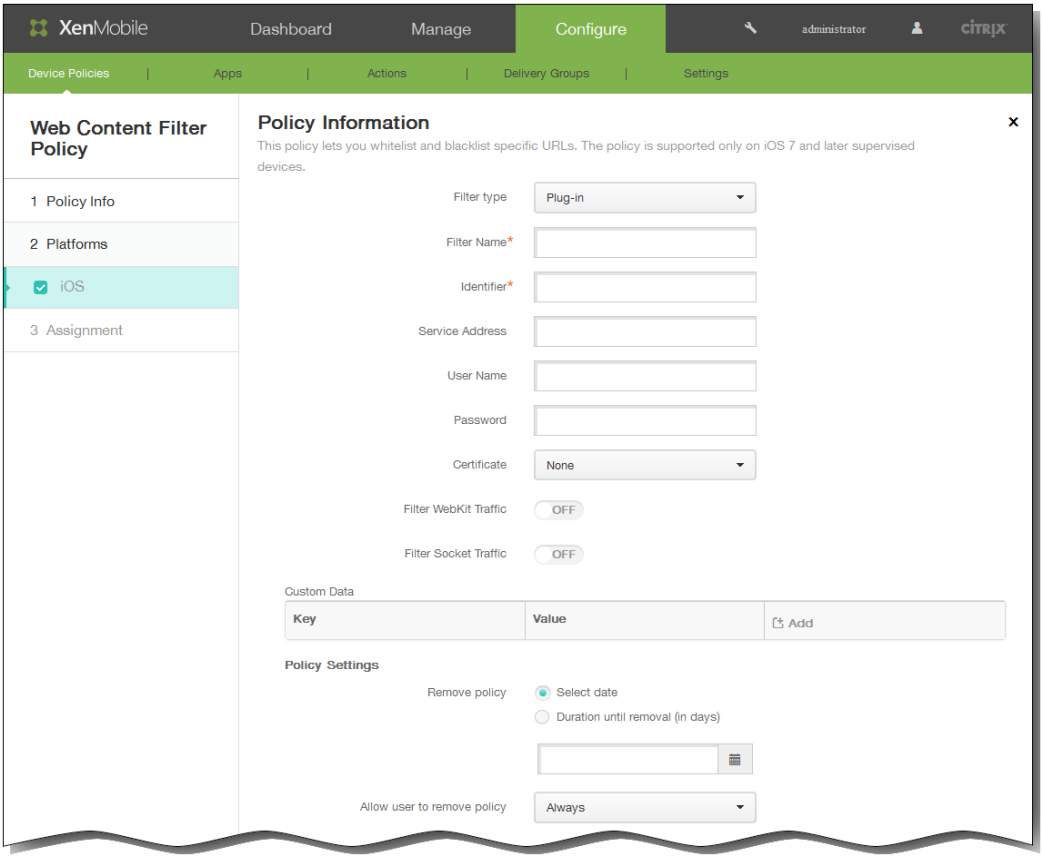
4. 书签白名单：此列表中的项目只表示用户可以访问的站点。
   单击添加，然后执行以下操作，将 Web 站点添加到书签中：

   1. URL：输入要添加到书签中的 Web 站点的 URL。必须在 Web 地址前添加 http:// 或 https://。此字段为必填字段。
   2. 书签文件夹：输入可选书签文件夹名称。如果将此字段留空，书签将添加到默认书签目录。
   3. 标题：输入 Web 站点的描述性标题。例如，为 URL http://google.com 输入“Google”。
   4. 单击保存将 Web 站点保存到黑名单中，或单击取消不保存此站点。
   5. 为要添加的每个应用程序重复步骤 i.至步骤 iv.。

   注意：要删除现有 Web 站点，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 Web 站点，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。

5. 参考步骤 7，完成内置过滤器配置。

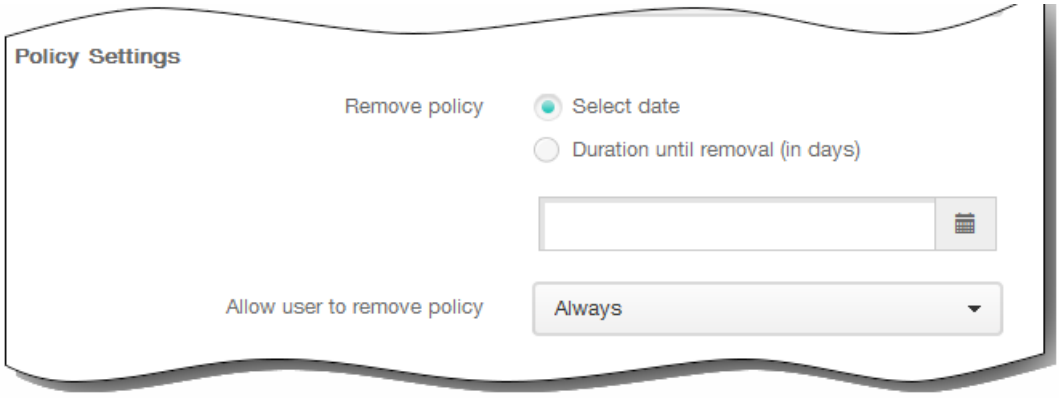
配置插件过滤器类型



1. 过滤器名称：输入过滤器的唯一名称。
2. 标识符：输入提供过滤器服务的插件的捆绑 ID。
3. 服务地址：输入可选服务器地址。 有效格式包括 IP 地址、主机名或 URL。
4. 用户名：输入服务的可选用户名。
5. 密码：输入服务的可选密码。
6. 证书：在列表中，单击用于向服务验证用户身份的身份证书。 默认值为无。
7. 过滤 WebKit 流量：选择是否过滤 WebKit 流量。
8. 过滤 Socket 流量：选择是否过滤套接字流量。
9. 自定义数据：单击添加，然后执行以下操作，向 Web 内容过滤器中添加自定义数据：
    1. 密钥：输入自定义密钥。
    2. 值：输入自定义密钥的值。
    3. 单击保存以保存自定义密钥，或单击取消不保存此自定义密钥。
    4. 为要添加的每个应用程序重复步骤 i.至步骤 iii.。

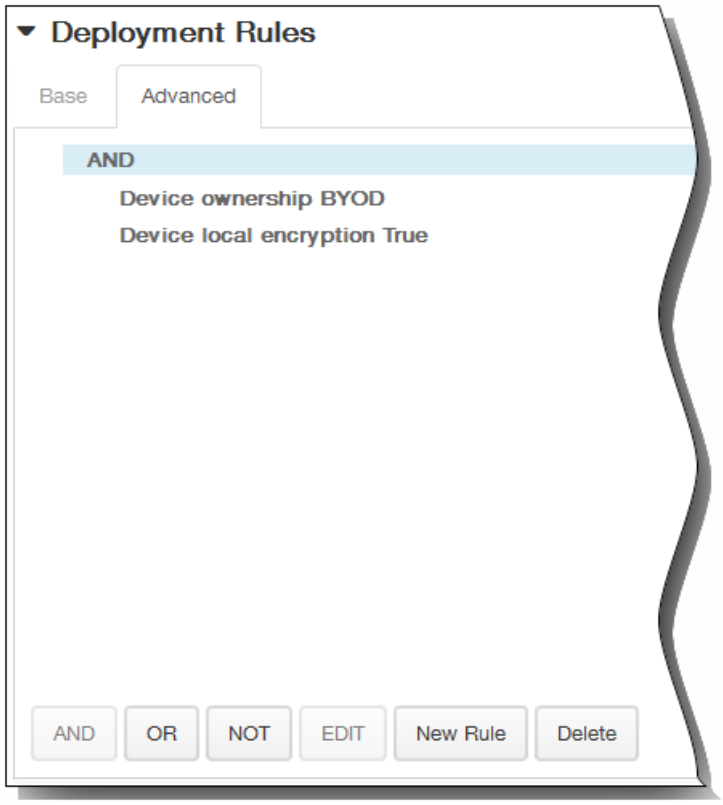
    注意：要删除现有密钥，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击删除以删除列表，或单击取消以保留此列表。

    要编辑现有密钥，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. 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)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



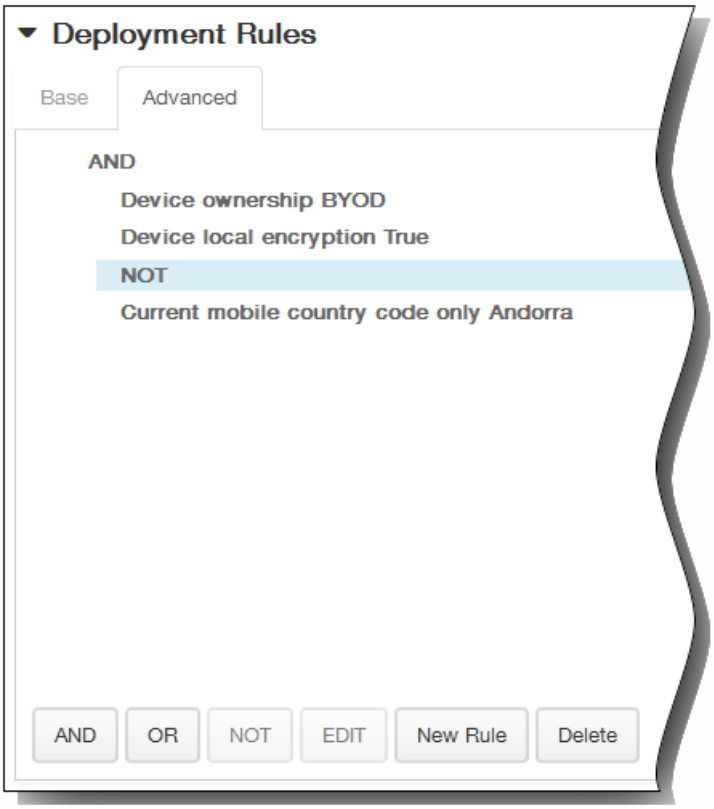
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

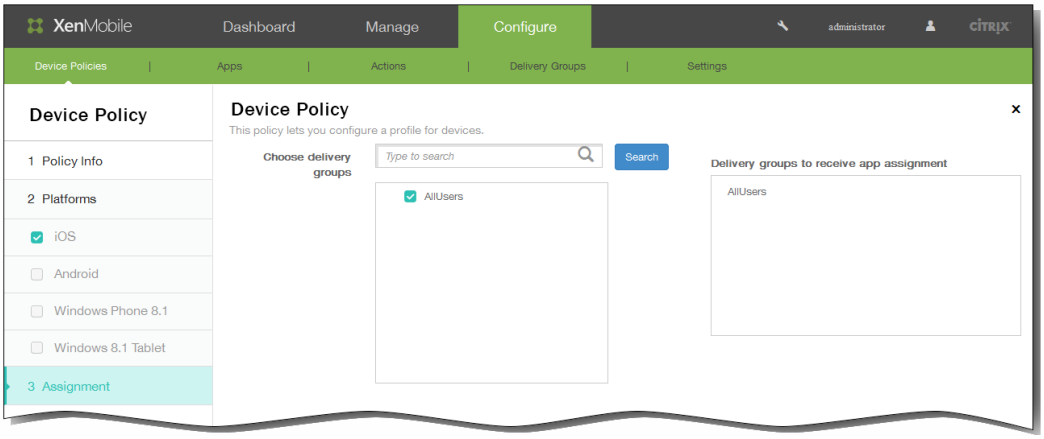


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



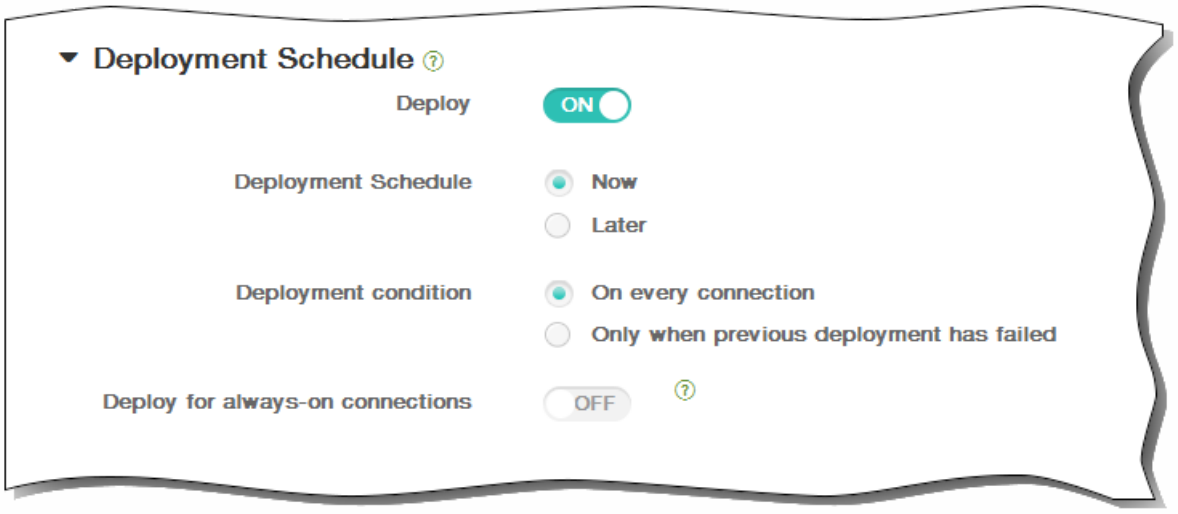
12. 单击下一步。 此时将显示 Web 内容过滤策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



14. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



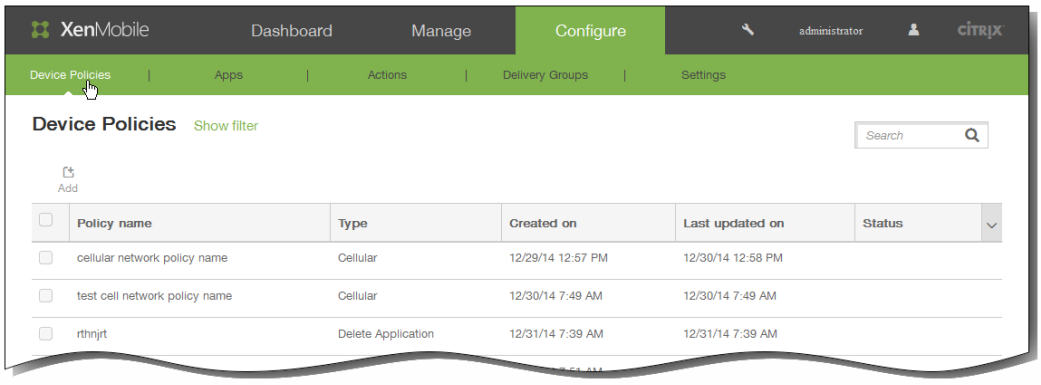
15. 单击保存以保存此策略。

Samsung 浏览器设备策略

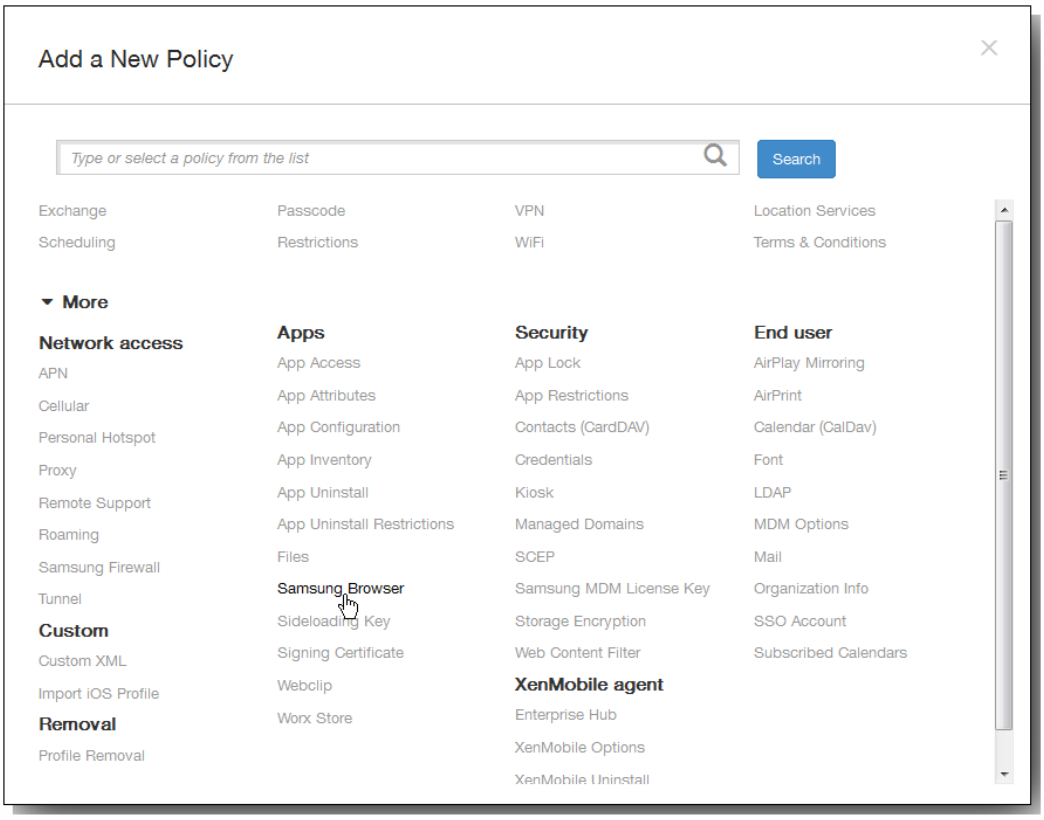
May 05, 2016

可以创建适用于 Samsung SAFE 和 Samsung KNOX 设备的 Samsung 浏览器设备策略，以定义用户的设备是否可以使用此浏览器，或限制用户的设备可以使用的浏览器功能。可以完全禁用此浏览器，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。

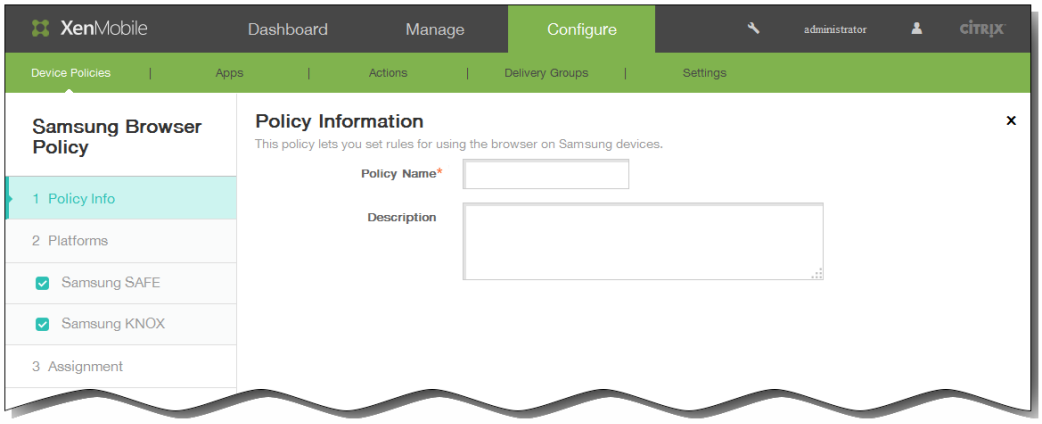
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



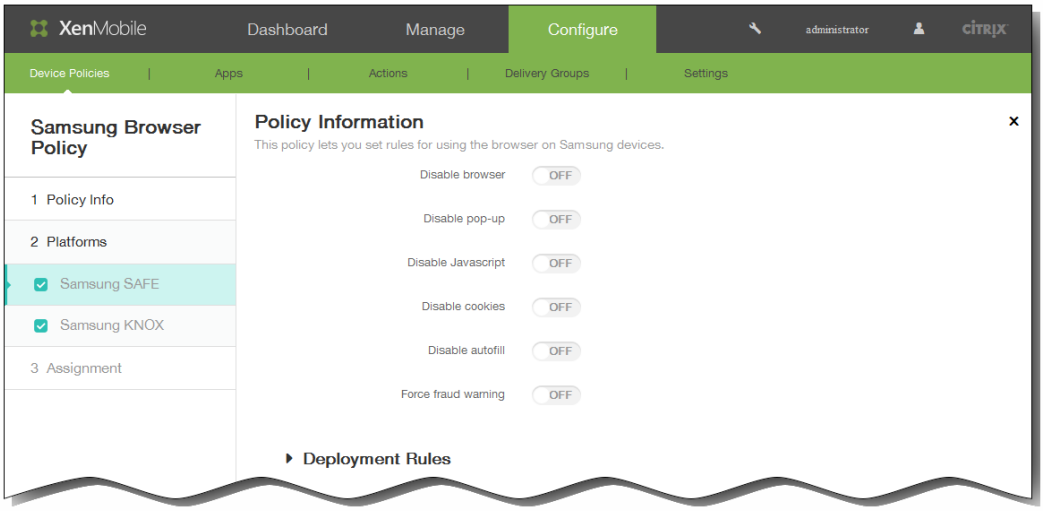
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



3. 单击更多，然后在应用程序下面，单击 Samsung 浏览器。 此时将显示 Samsung 浏览器策略信息页面。

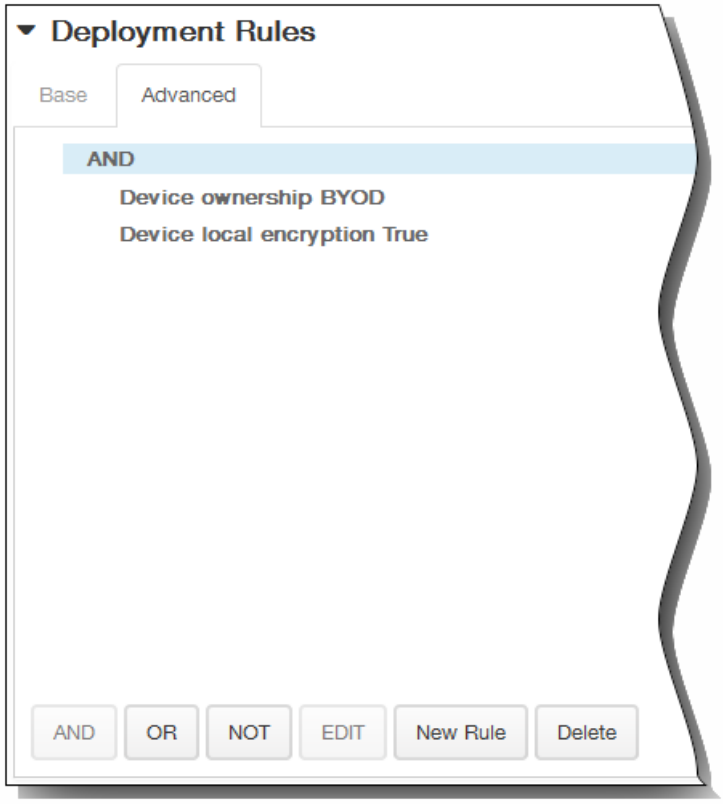


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
5. 单击下一步。 此时将显示策略平台页面。
   注意：策略平台页面显示时，两个平台都处于选中状态，您首先看到 Samsung SAFE 平台配置面板。



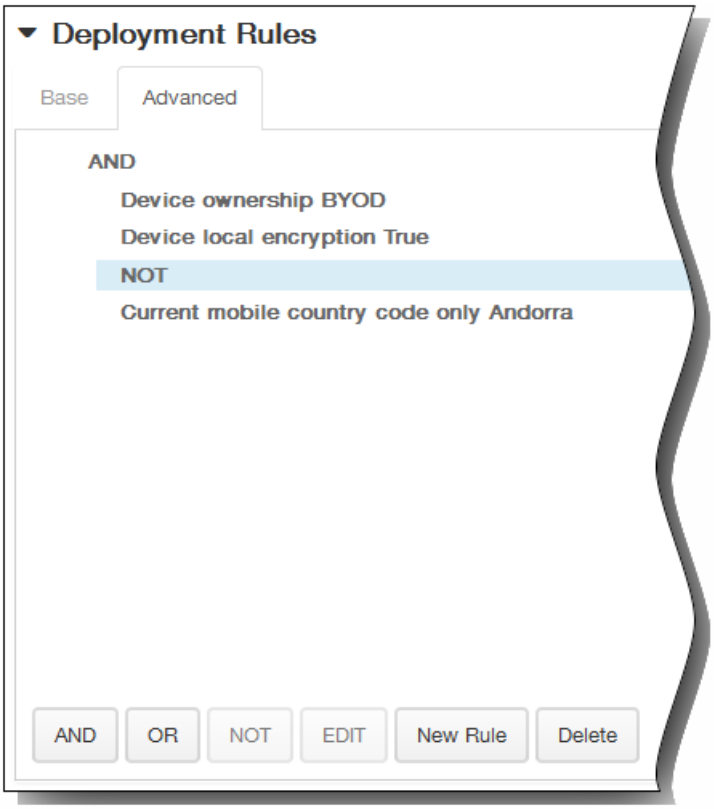
6.
7. 在平台下面，选择要添加的 Samsung 平台。 如果您只配置一个平台，清除其他平台，然后配置以下设置：
   1. 禁用浏览器：选择是否在用户设备上完全禁用 Samsung 浏览器。 默认设置为关，表示允许用户使用此浏览器。 禁用此浏览器后，将不再显示以下选项。
   2. 禁用弹出窗口：选择是否允许在此浏览器上显示弹出消息。
   3. 禁用 Javascript：选择是否允许在此浏览器上运行 Javascript。
   4. 禁用 Cookie：选择是否允许 Cookie。
   5. 禁用自动填充：选择是否允许用户启用此浏览器的自动填充功能。
   6. 强制显示欺诈警告：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。
8. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

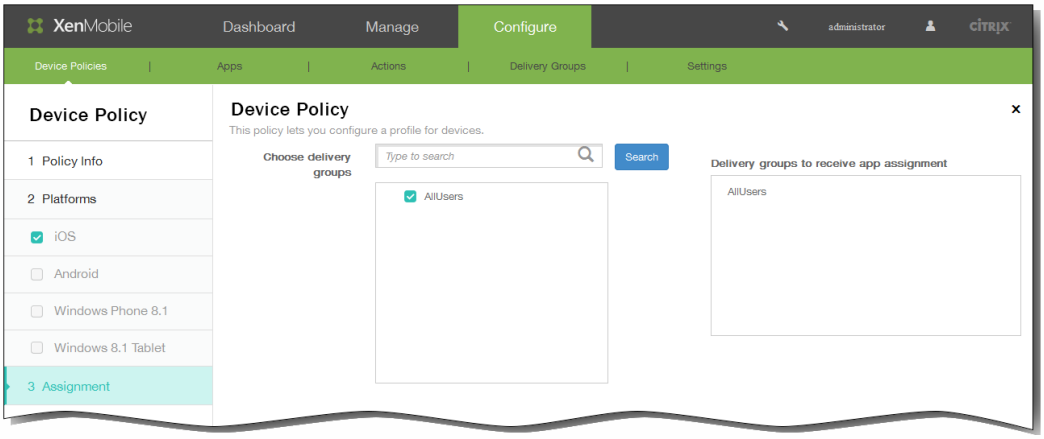


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



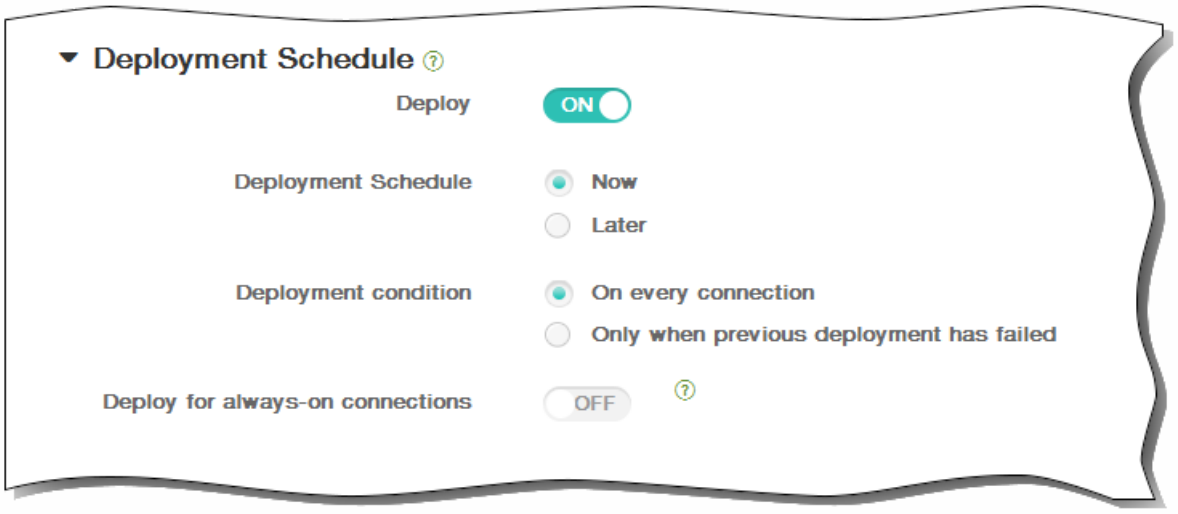
9. 单击下一步。 此时将显示 Samsung 浏览器设备策略页面。
10. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



11. 展开部署计划，然后配置以下设置：
    1. 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。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 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。
    4. 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。
    5. 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。



12. 单击保存以保存此策略。

添加适用于 Windows 8.1 Tablet 的旁加载密钥设备策略

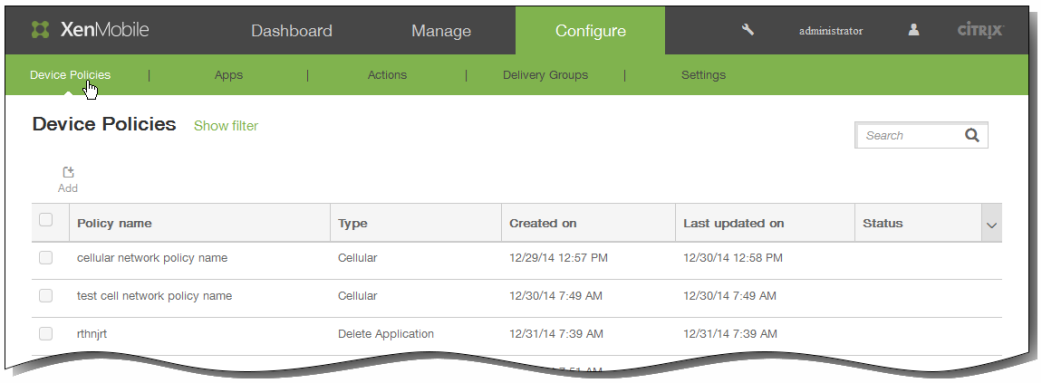
May 05, 2016

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。

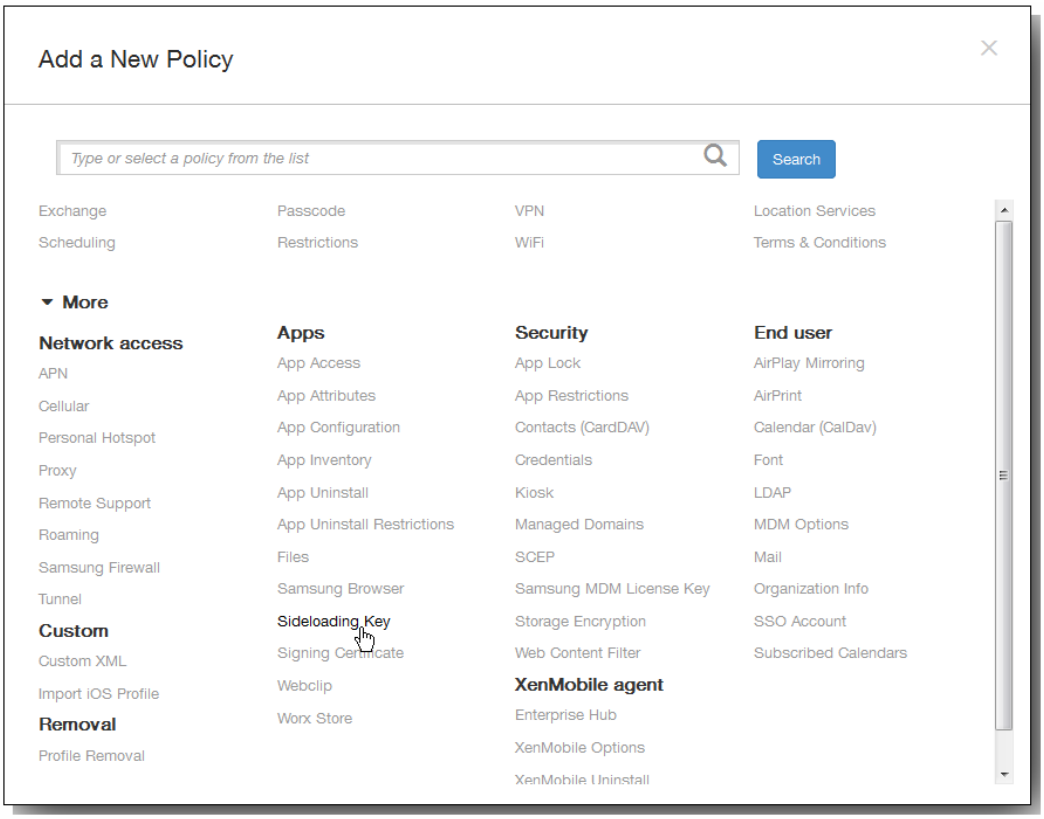
创建此策略之前，需要提供以下信息：

- 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

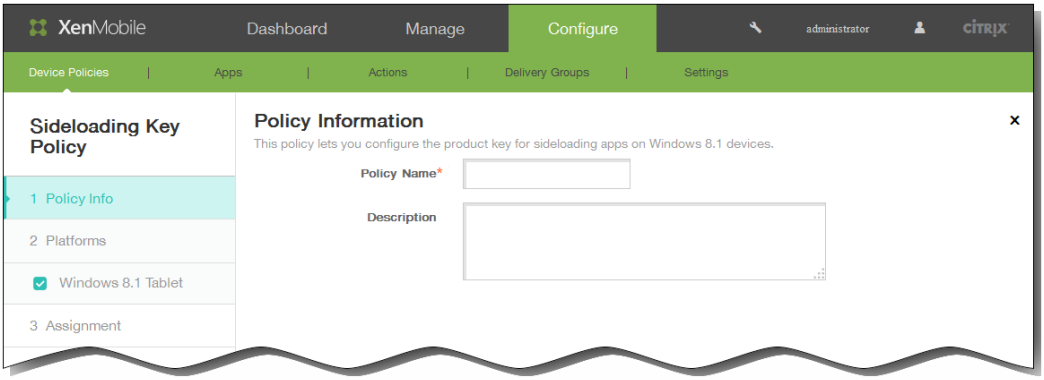
1. 在 XenMobile 控制台中，单击配置 > 设备策略将显示设备策略页面。



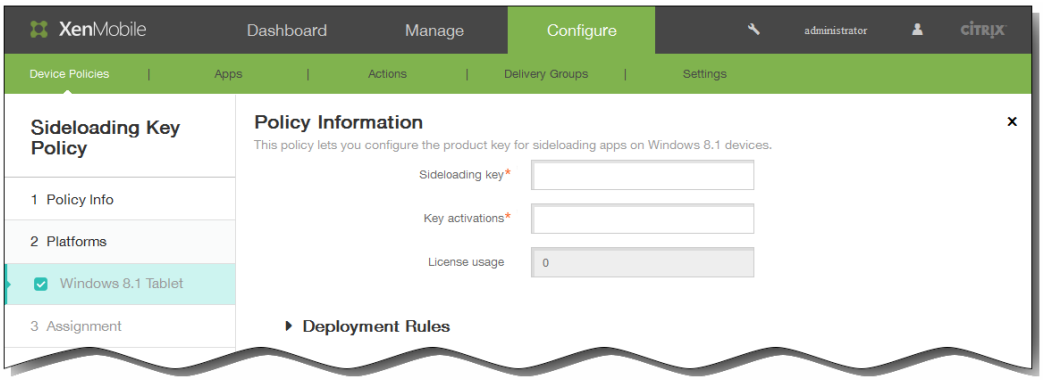
2. 单击添加。 此时将显示添加新策略对话框。



3. 单击更多，然后在应用程序下面，单击旁加载密钥。 此时将显示旁加载密钥策略页面。

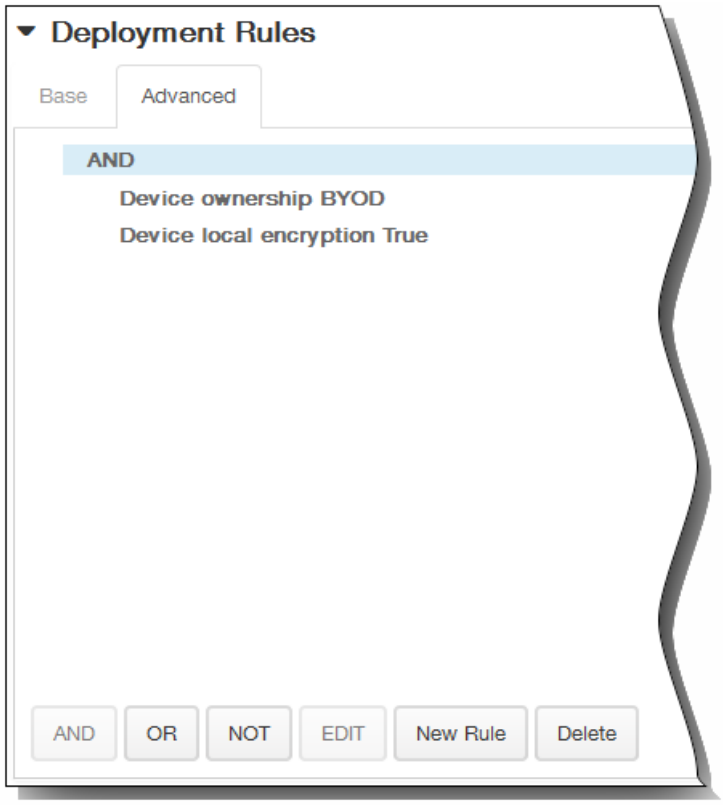


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。
   此时将显示 Windows 8.1 Tablet 平台信息页面。



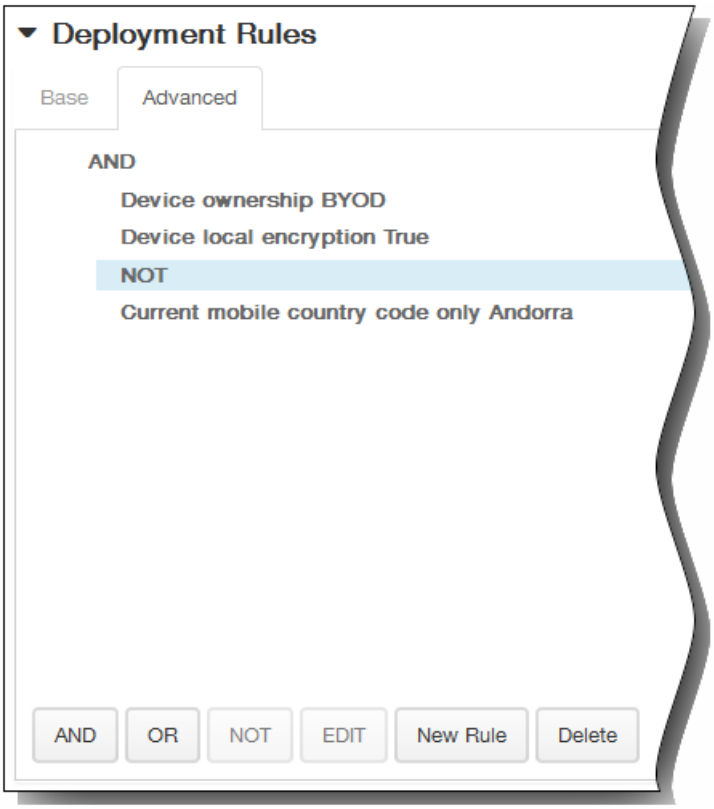
6. 配置以下设置：
   1. 旁加载密钥：键入从 Microsoft 批量许可服务中心获取的旁加载密钥。
   2. 密钥激活：键入为旁加载密钥创建的密钥激活。
   3. 许可证使用情况：XenMobile 根据注册的平板电脑数计算此值。 无法更改此字段。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

   1. 在此列表中，单击选项以确定部署策略的时间。
      1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
      2. 单击新建规则以定义条件。
      3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
      4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
   2. 单击高级选项卡以使用布尔选项组合规则。

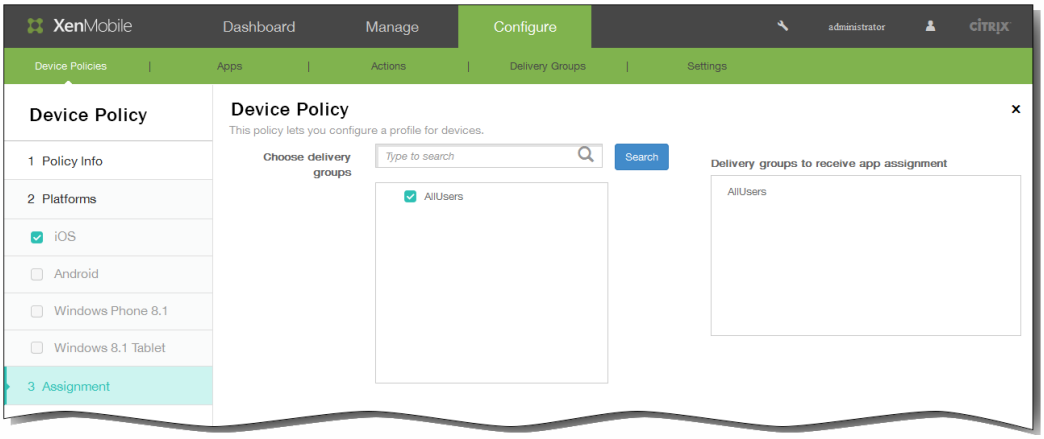


将显示您在基础选项卡上选择的条件。

3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。
   3. 如果要添加更多条件，请再次单击新建规则。
      在此示例中，设备所有权必须是 BYOD，设备本地加密必须为 True，移动设备国家/地区代码不能仅为安道尔。



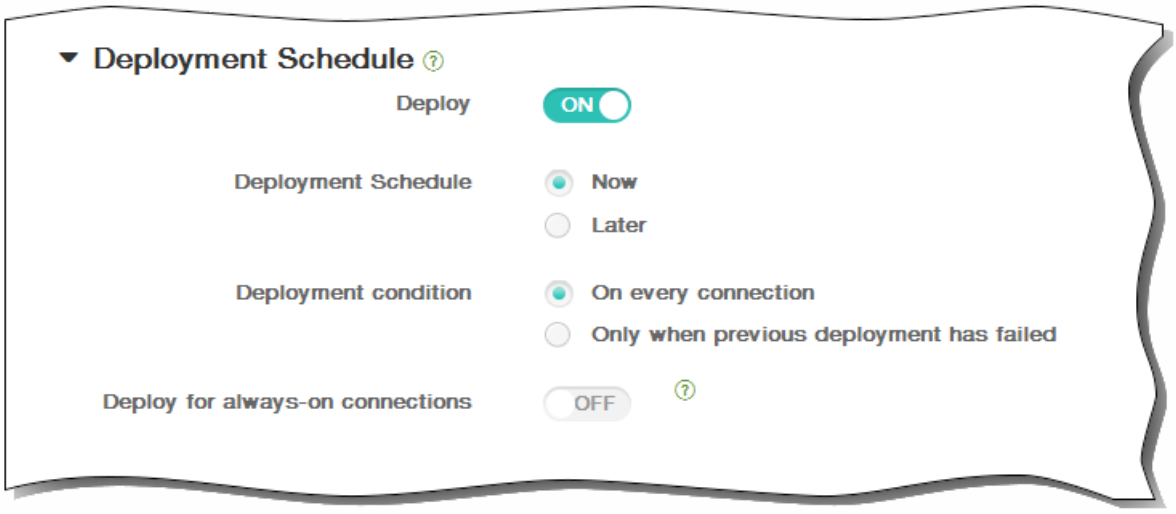
8. 单击下一步。 此时将显示旁加载密钥策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。

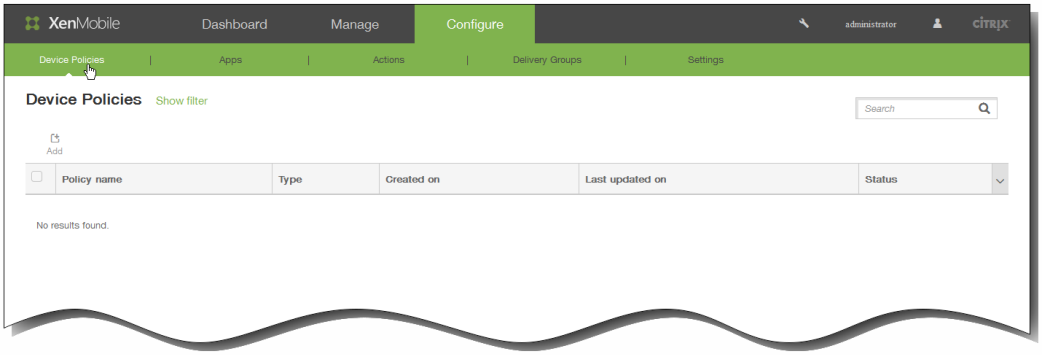


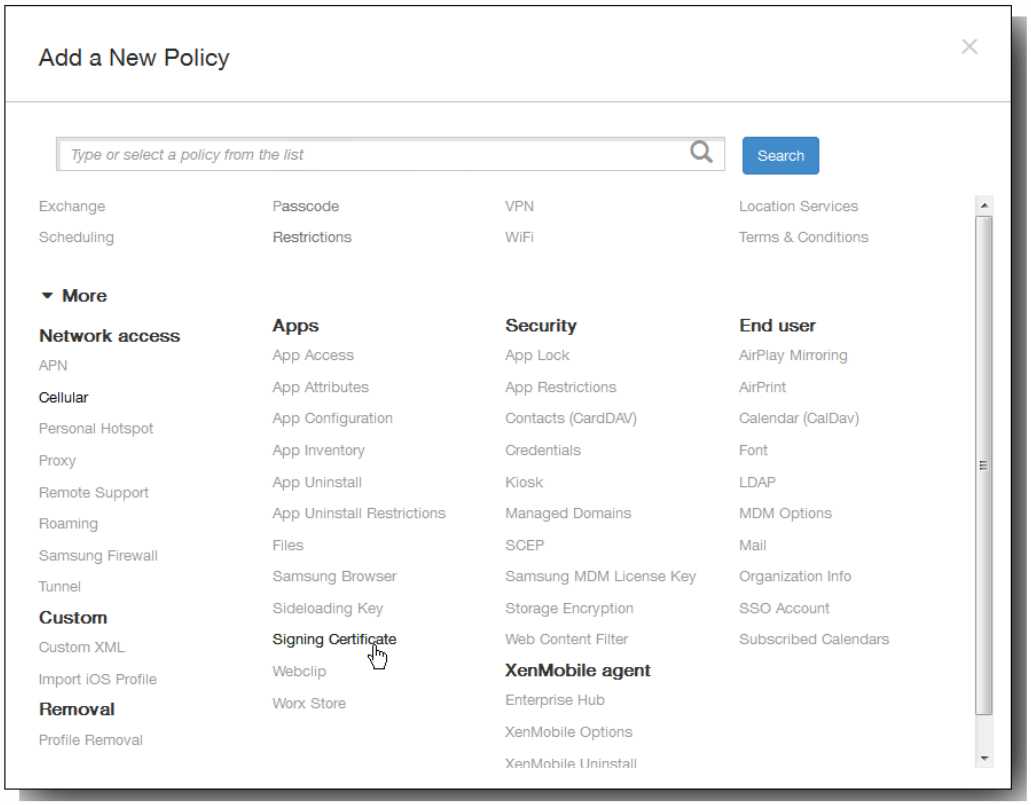
10. 展开部署计划，然后配置以下设置：
    1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。 如果选择关，无需配置其他选项。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
    4. 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。 默认选项为每次连接时。
    5. 在为始终启用的连接部署旁边，单击开或关。 默认选项为关。

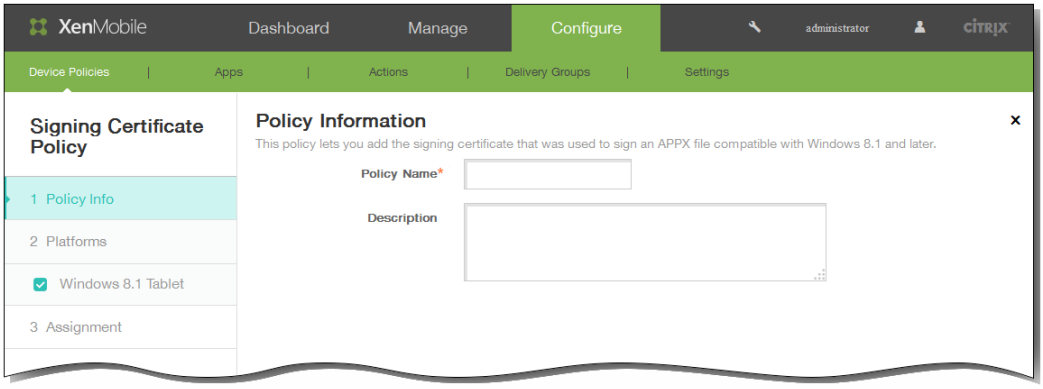
    注意：已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。

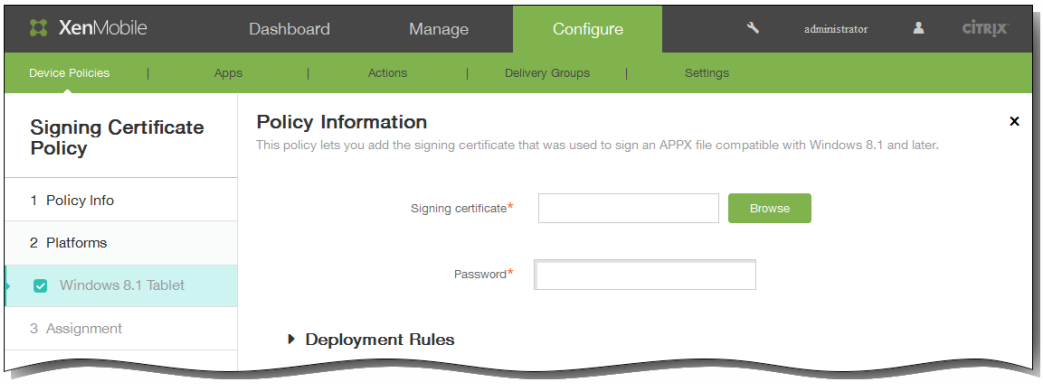
注意：配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

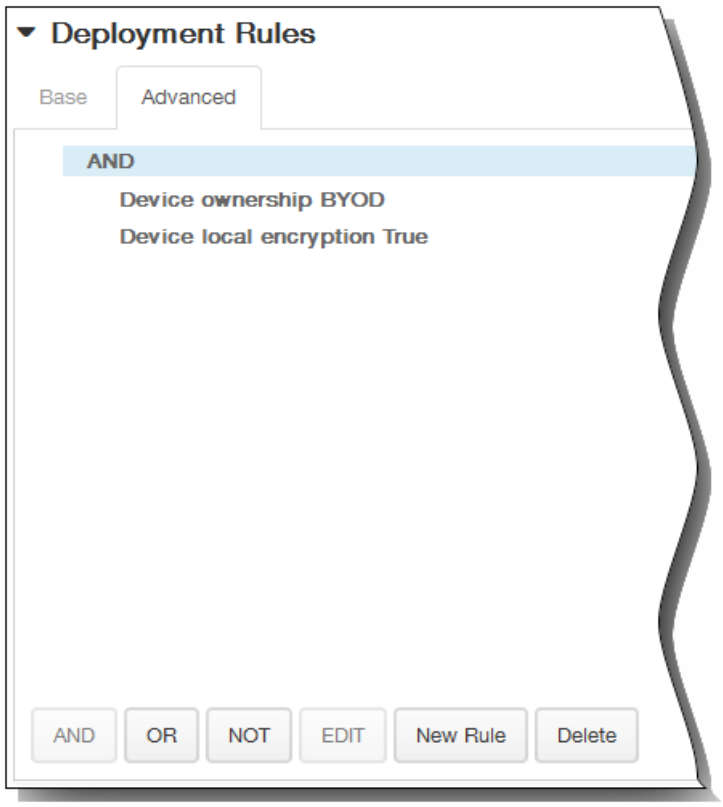


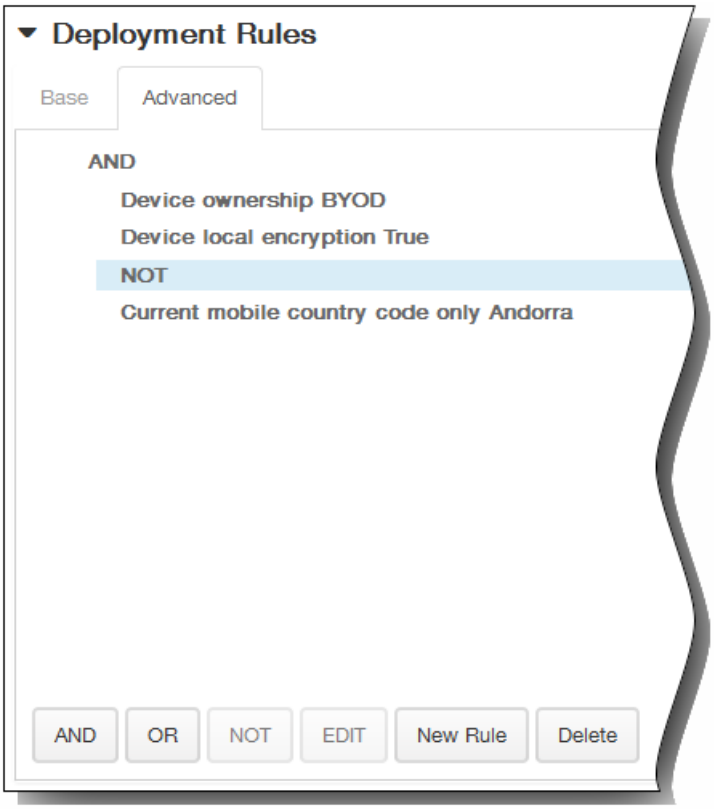


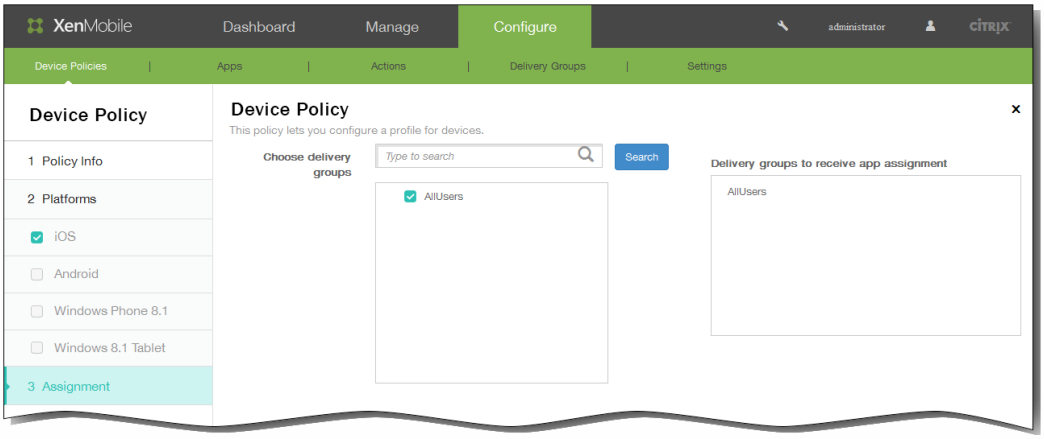


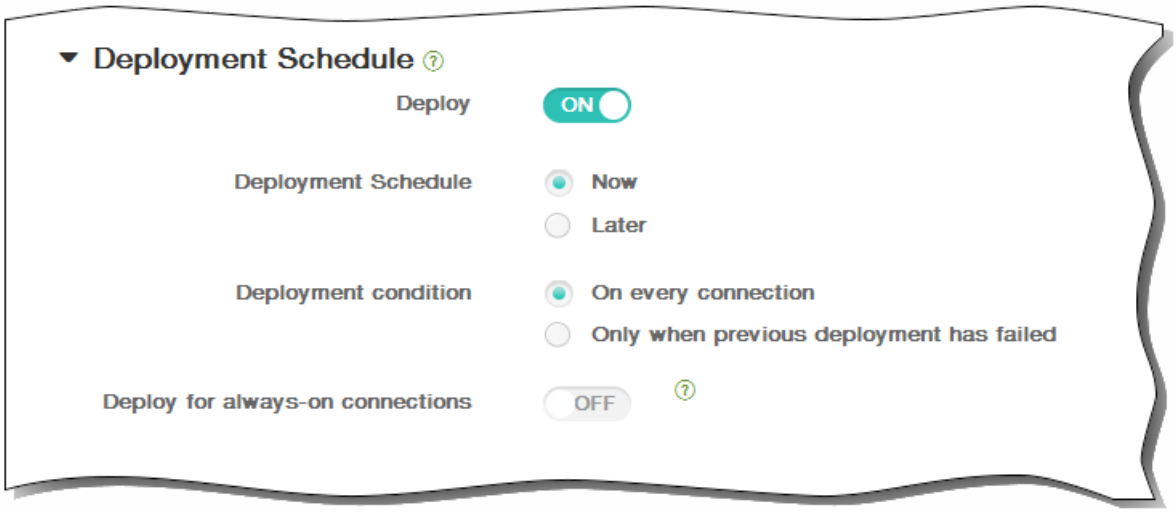


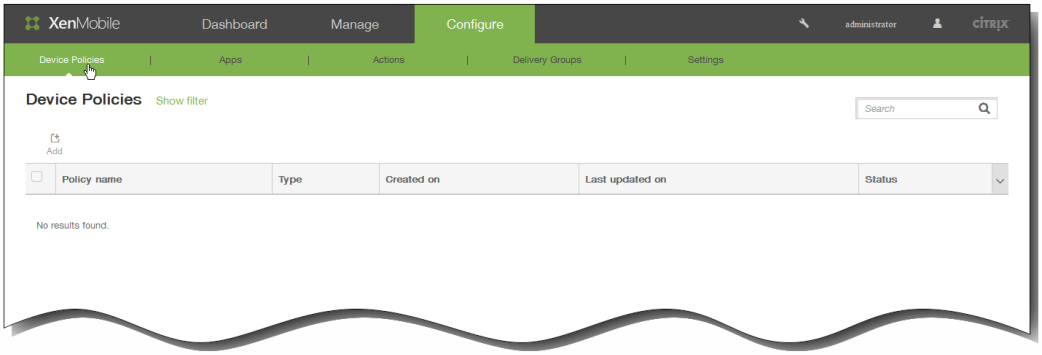


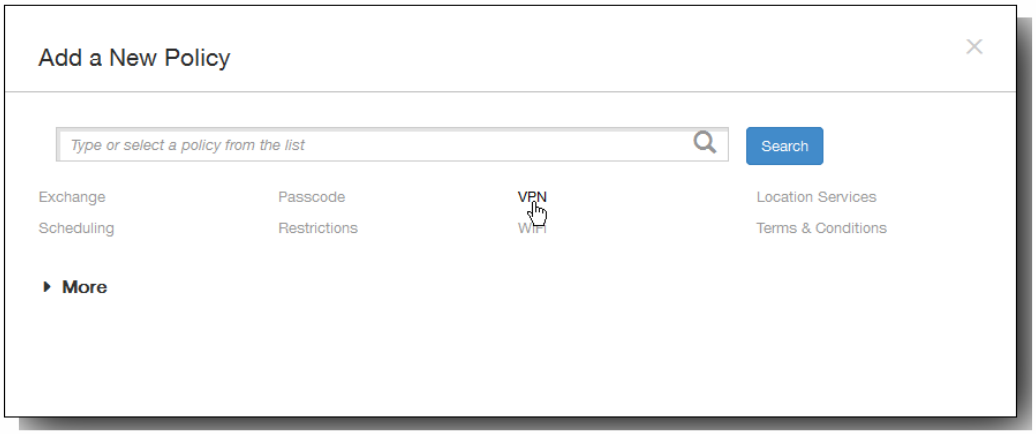


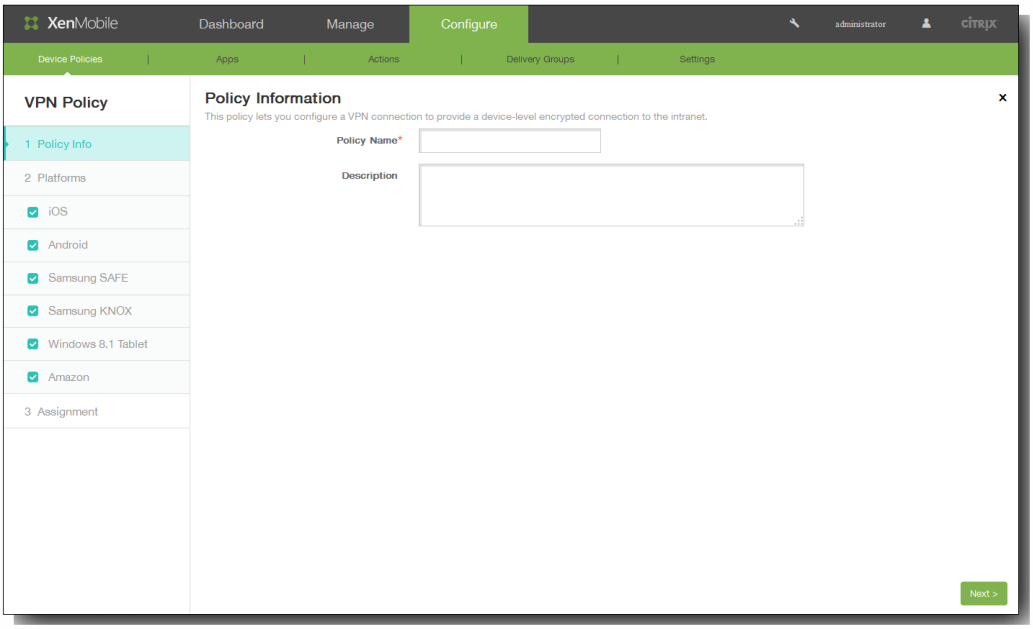


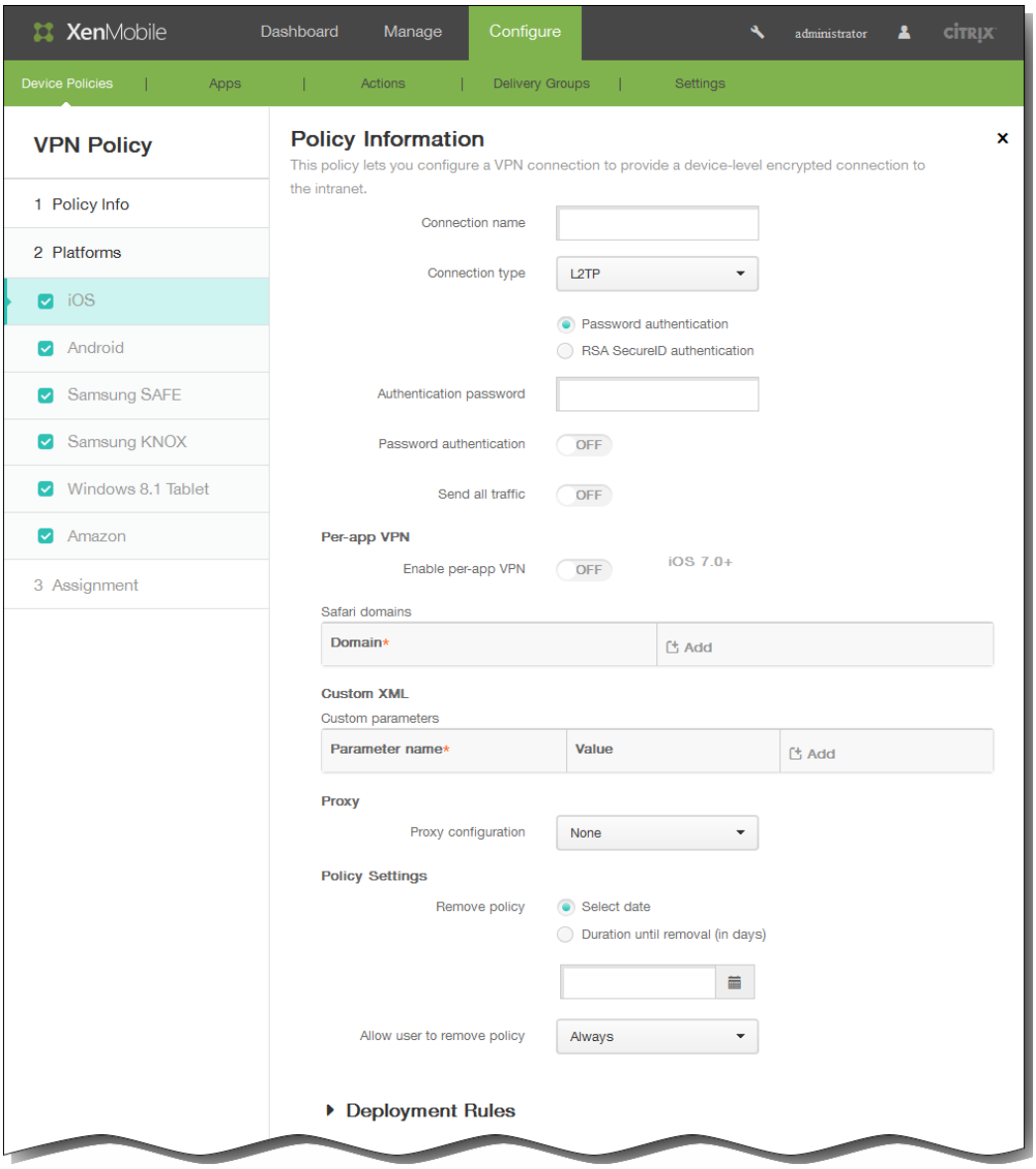




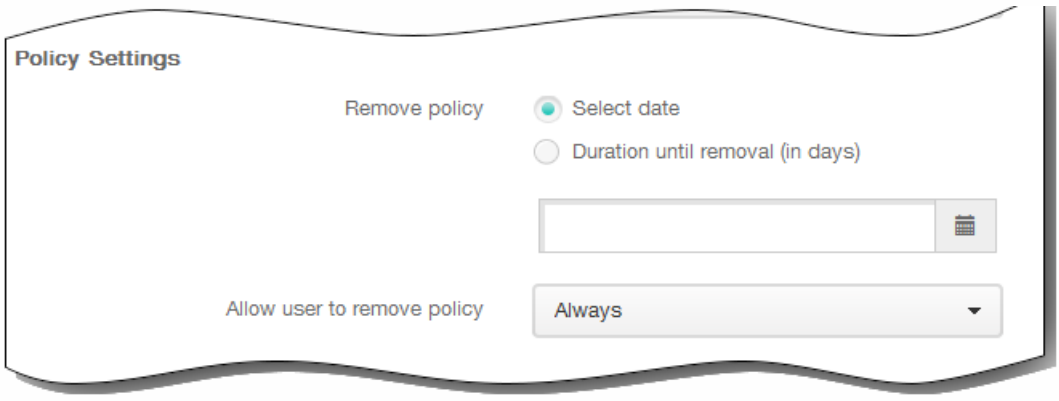


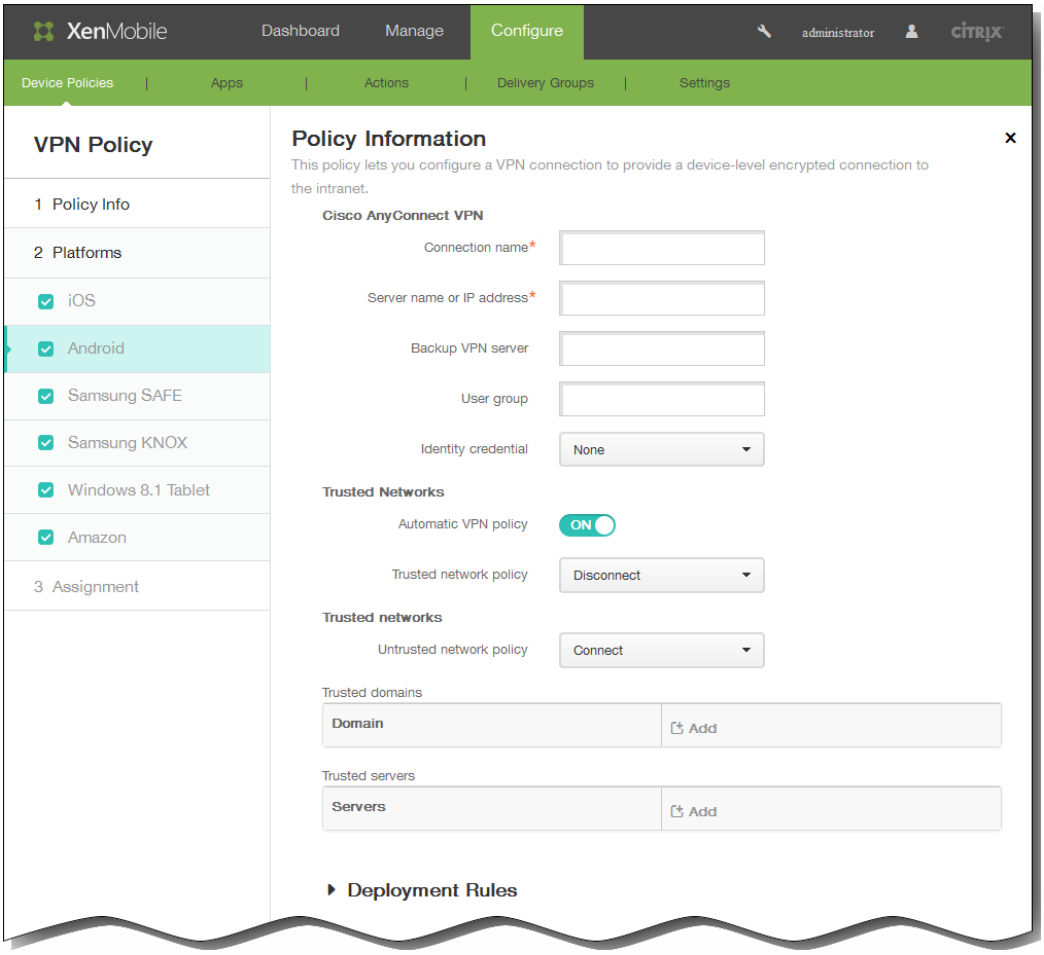




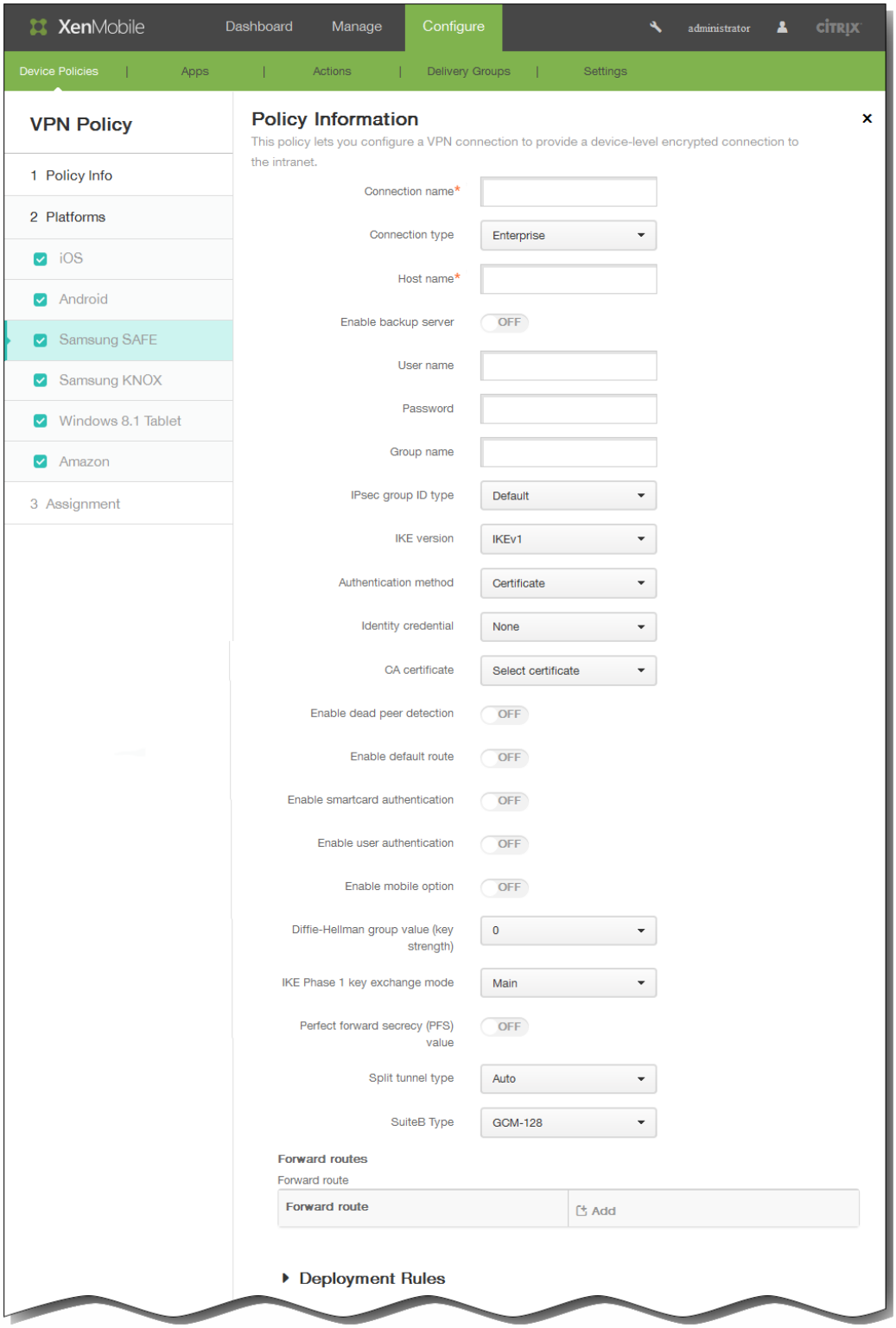


-
-
-
-
-
-
-
-
-
-

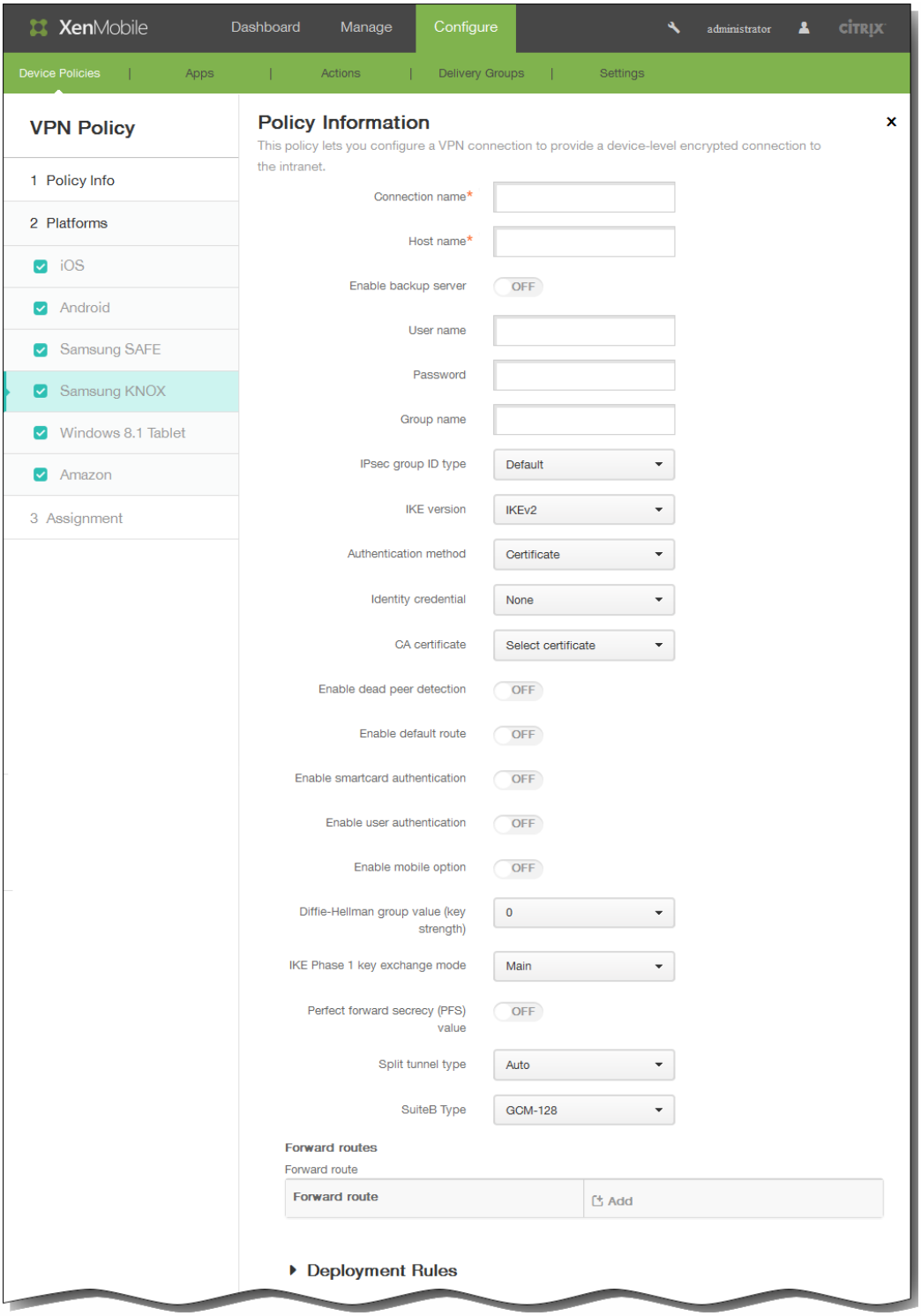




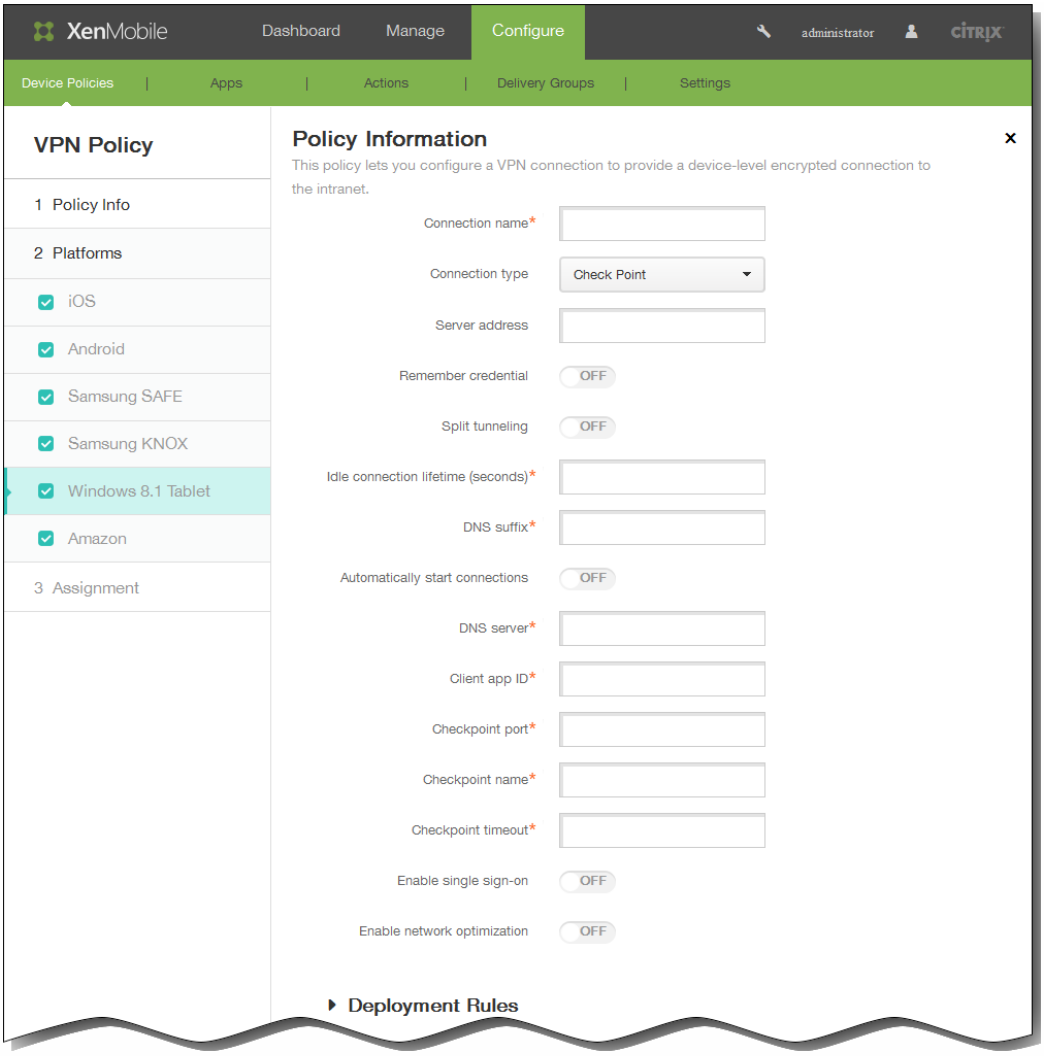
-
-



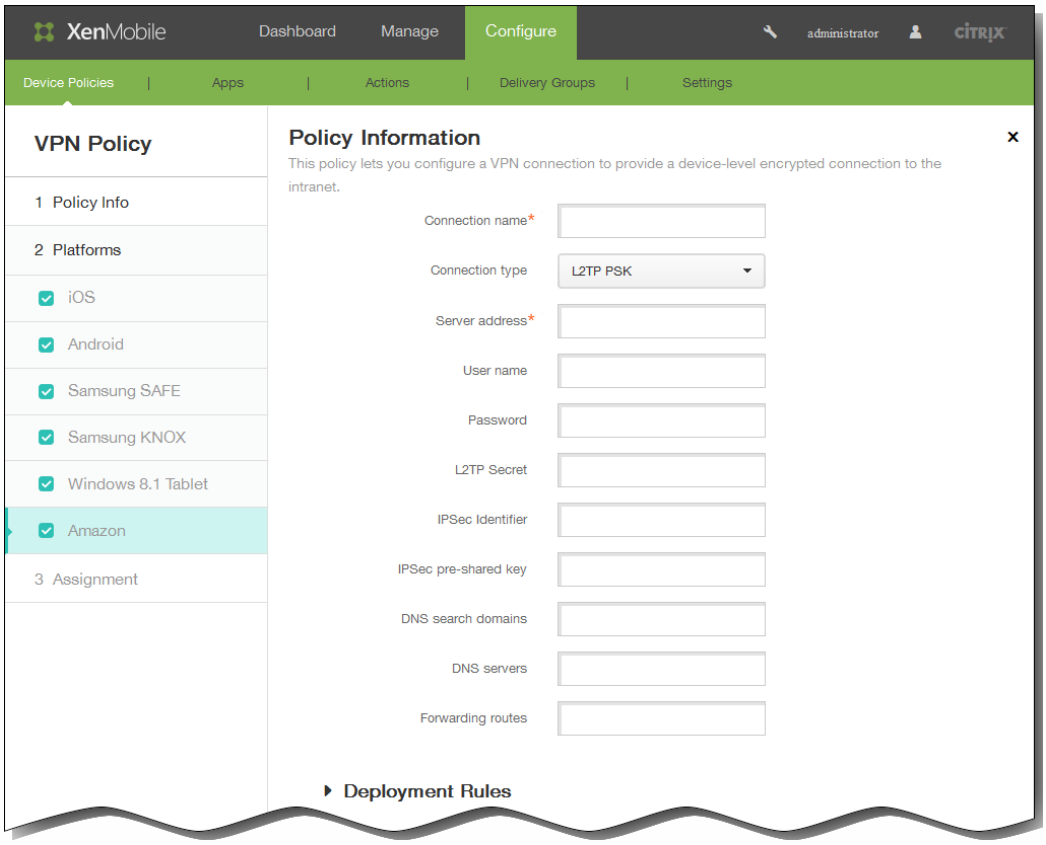
-
-
-
-



-
-
-
-
-

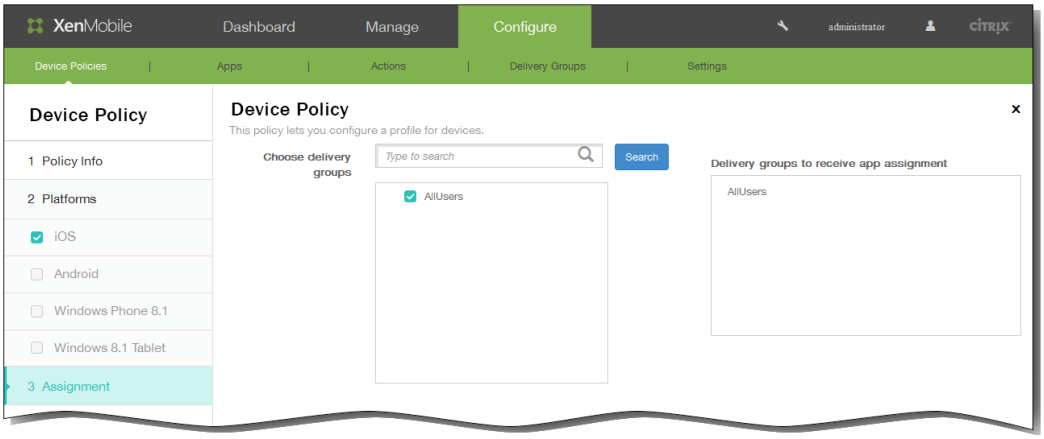


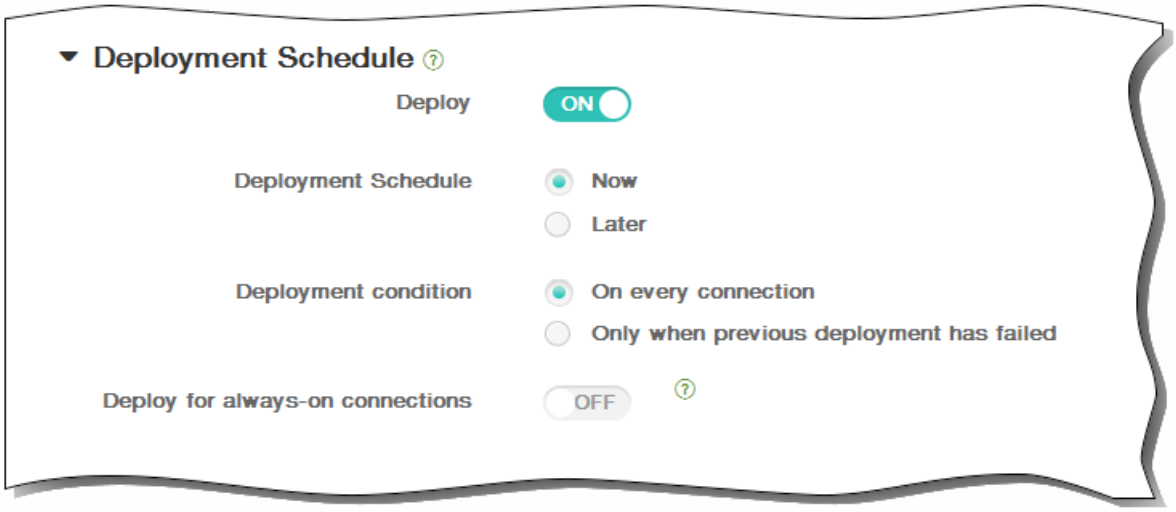
-
-
-
-
-



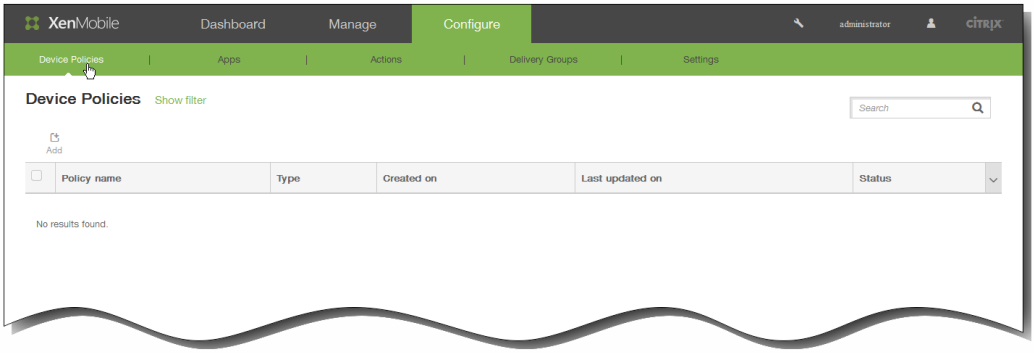
-
-
-
-
-

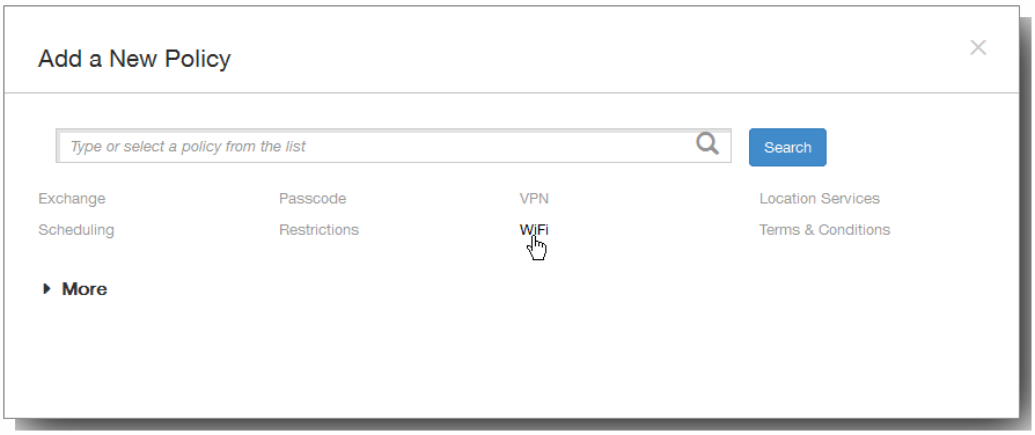
-

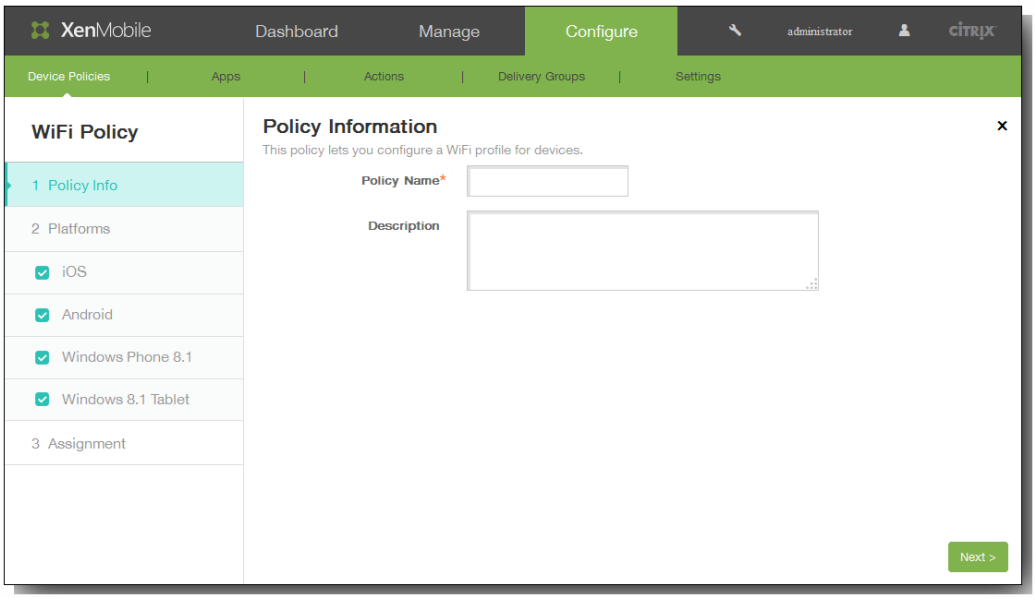


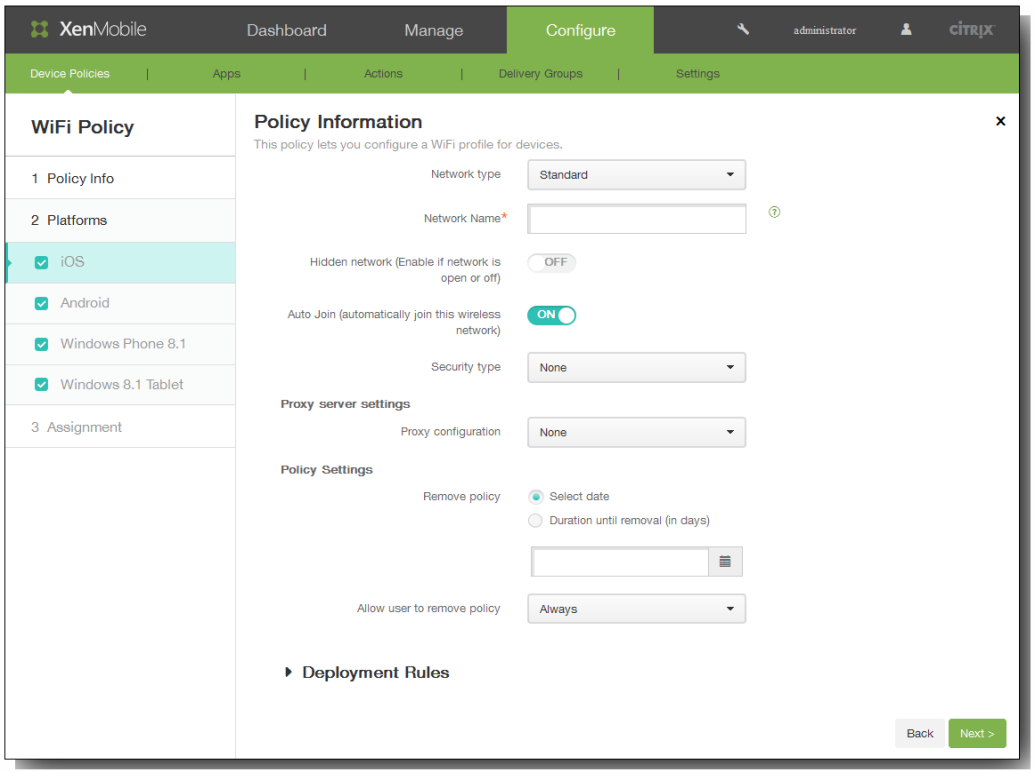


-
-
-
-
-
-

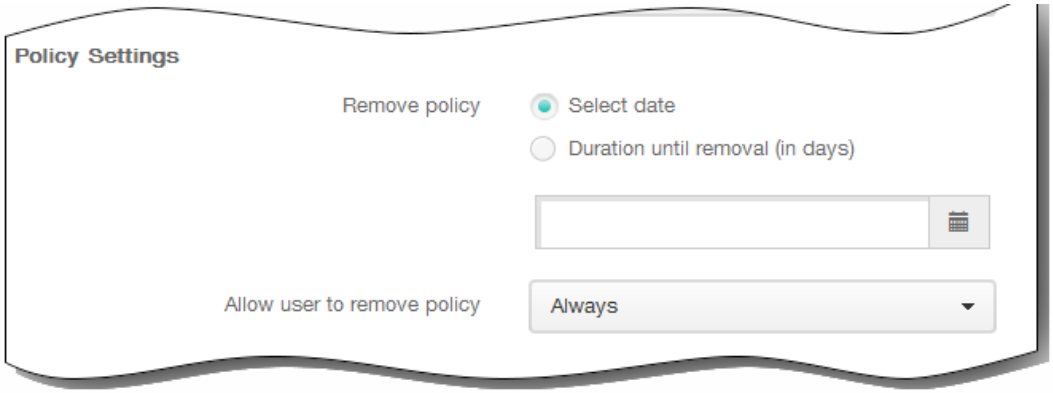


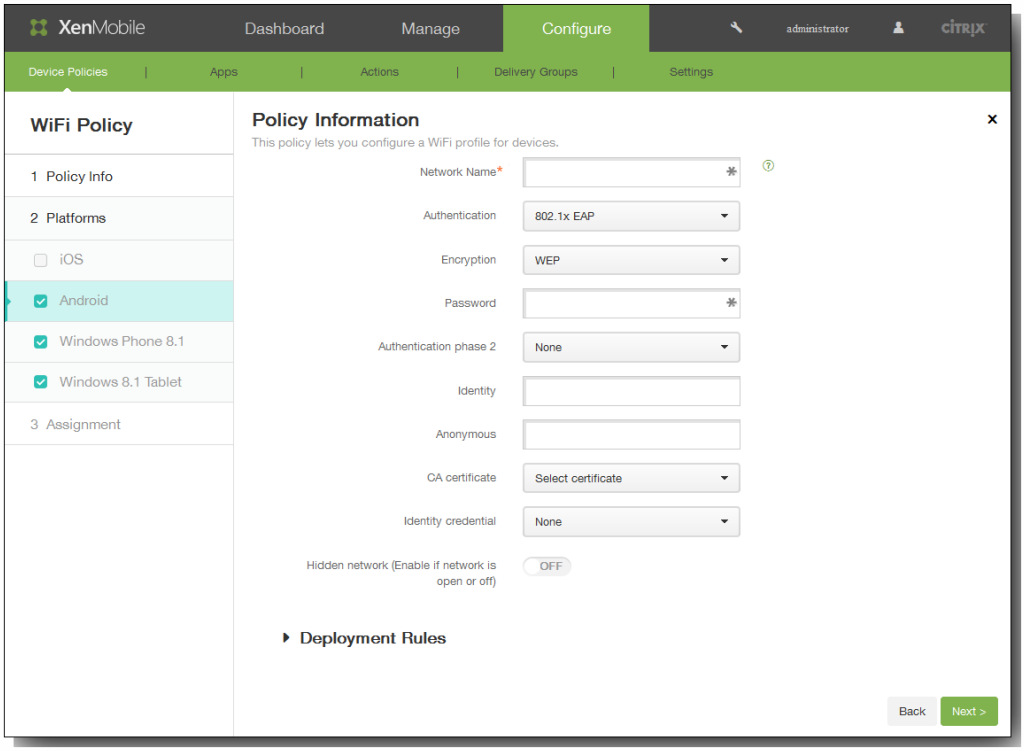






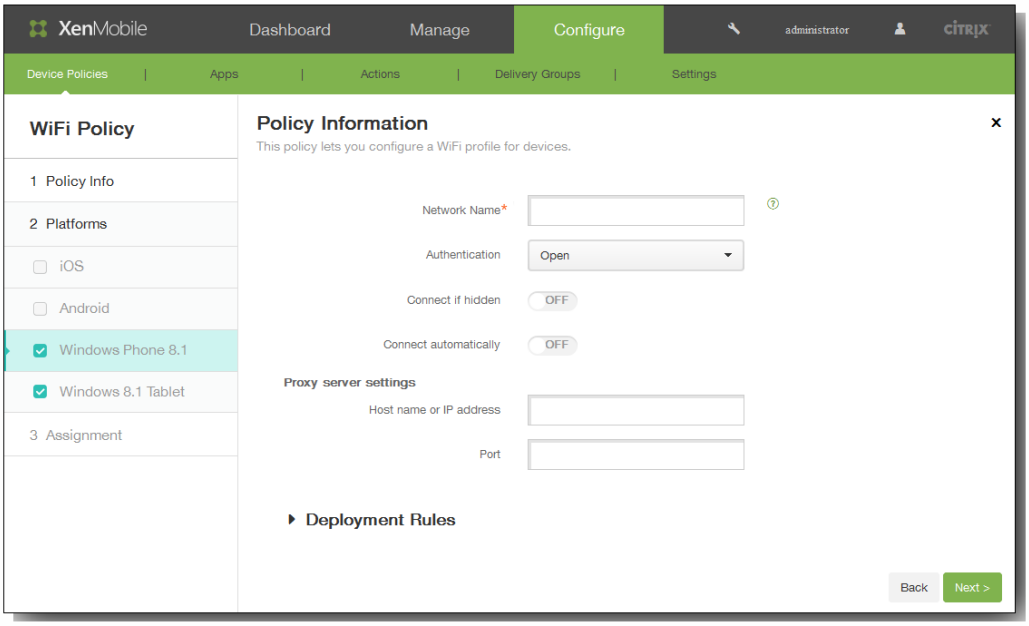
-
-
-
-
-
-
-



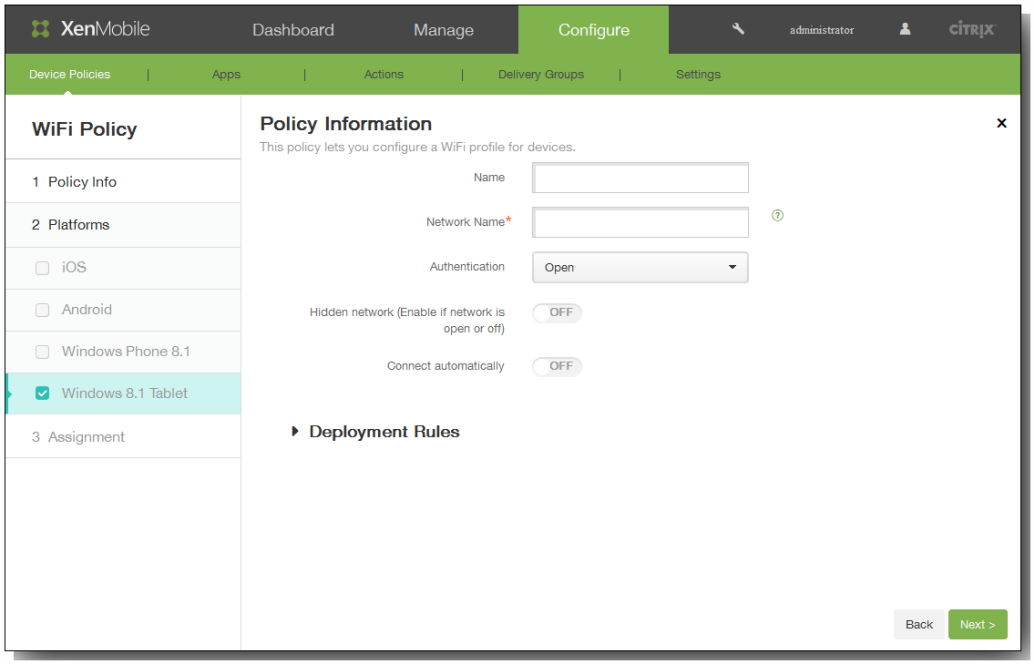


-
-
-
-
-

-
-

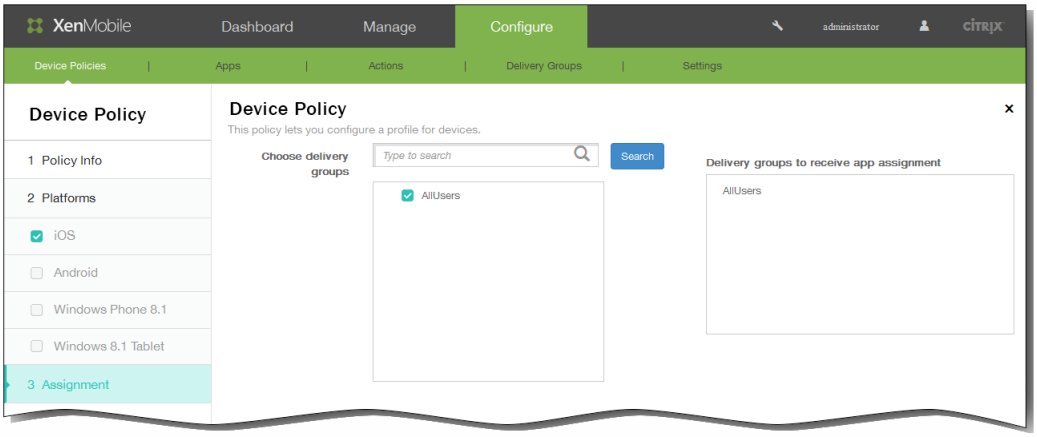


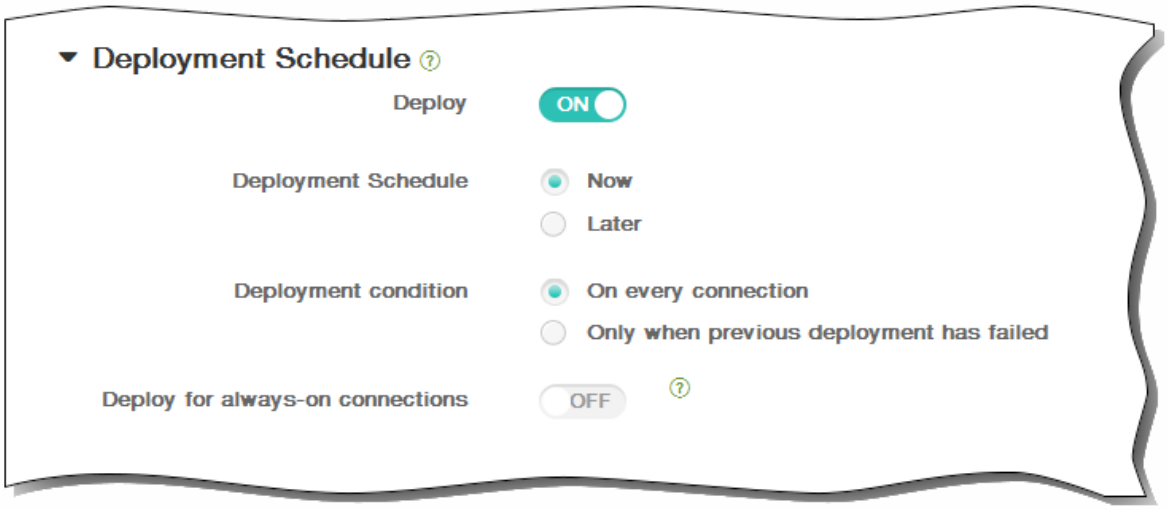
-
-
-
-

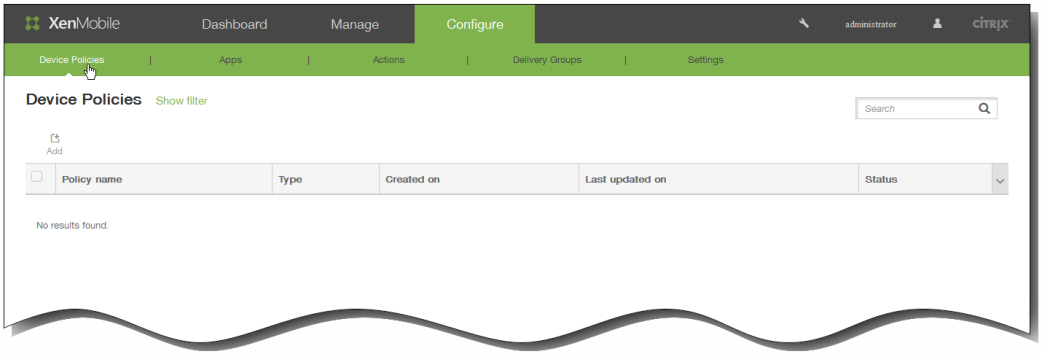


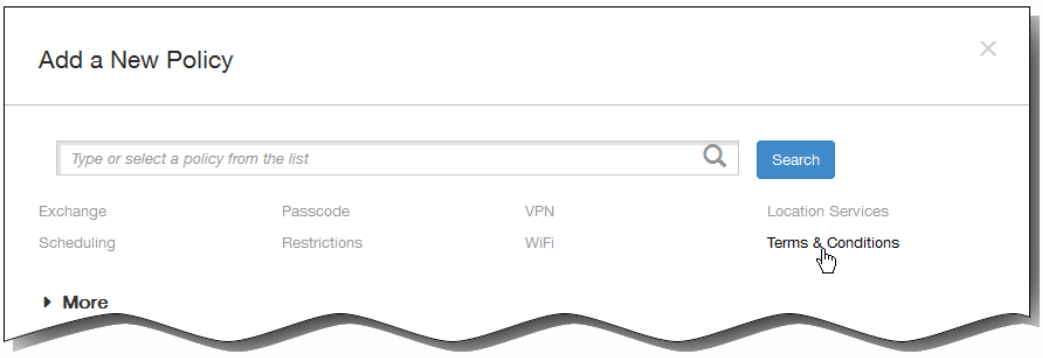
-
-
-

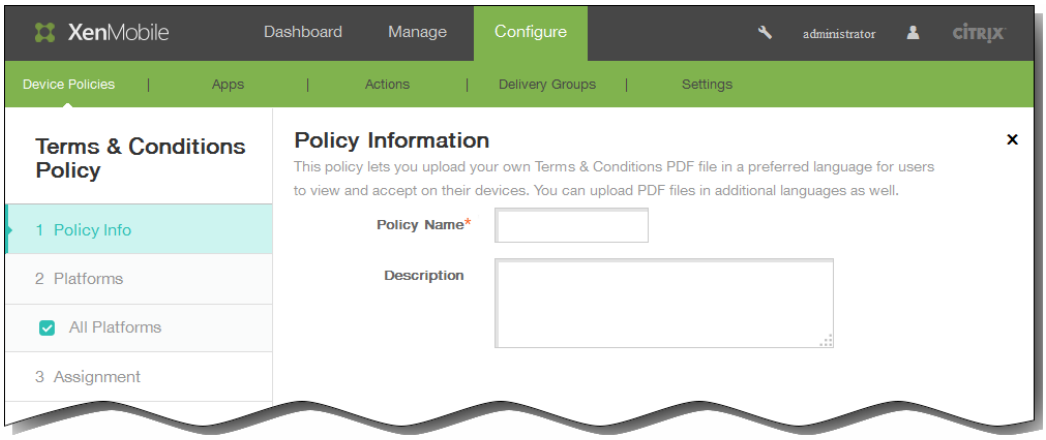
-
-

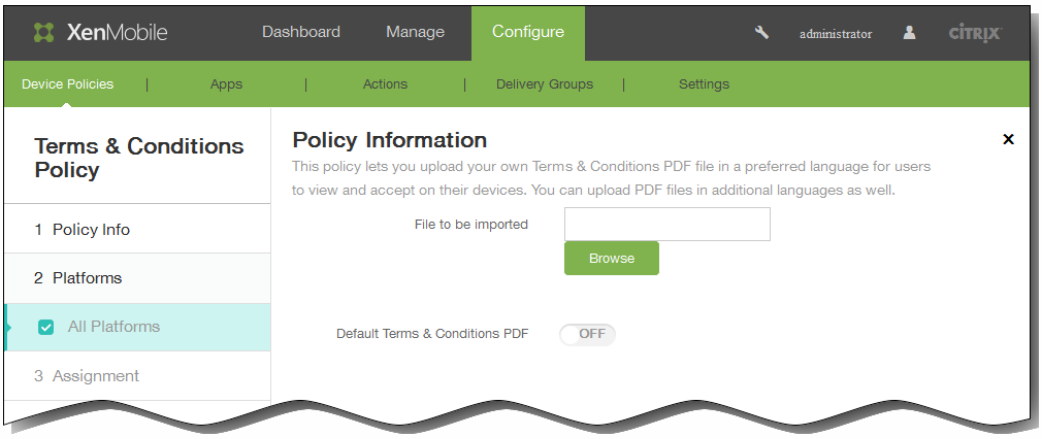


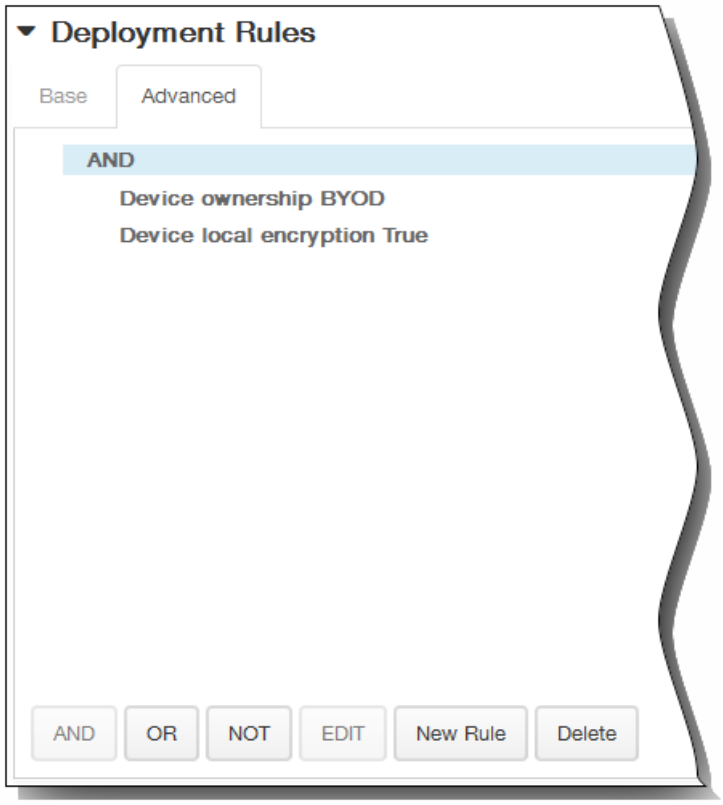


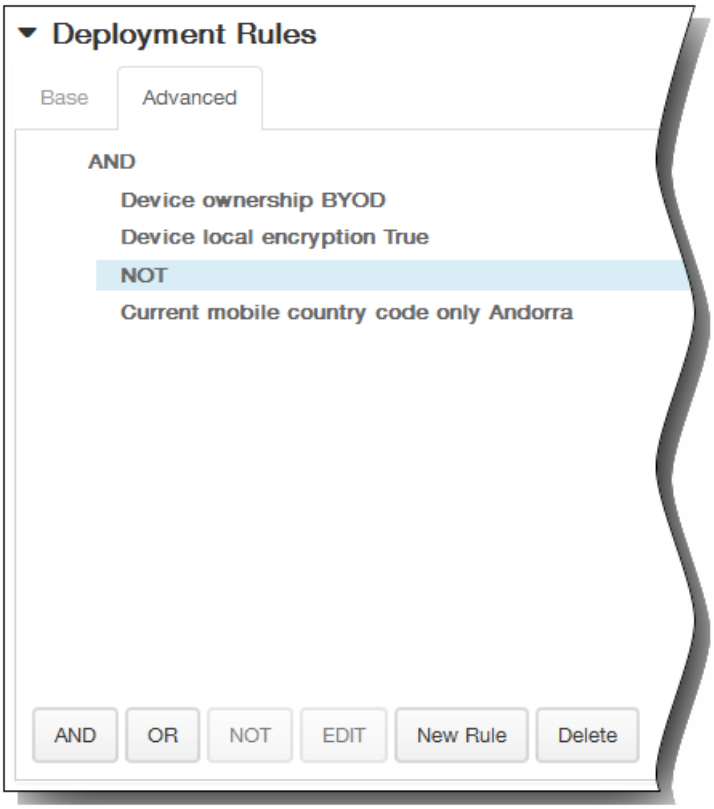


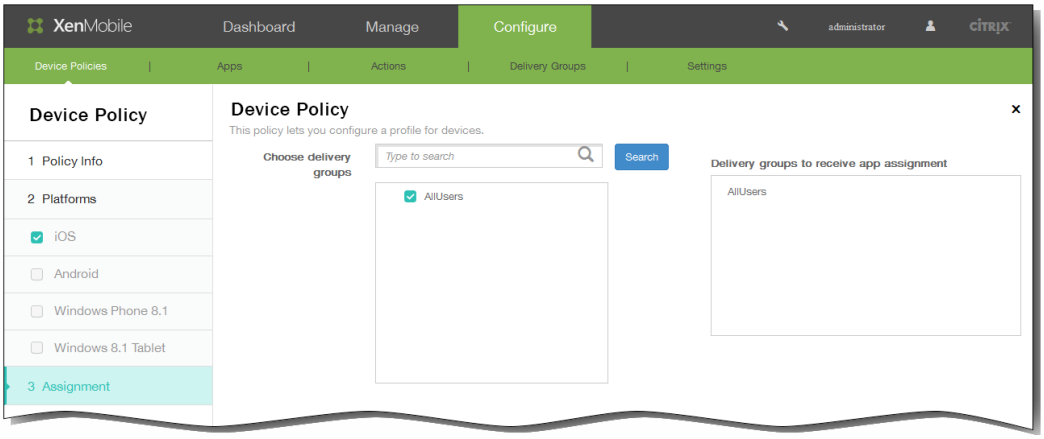


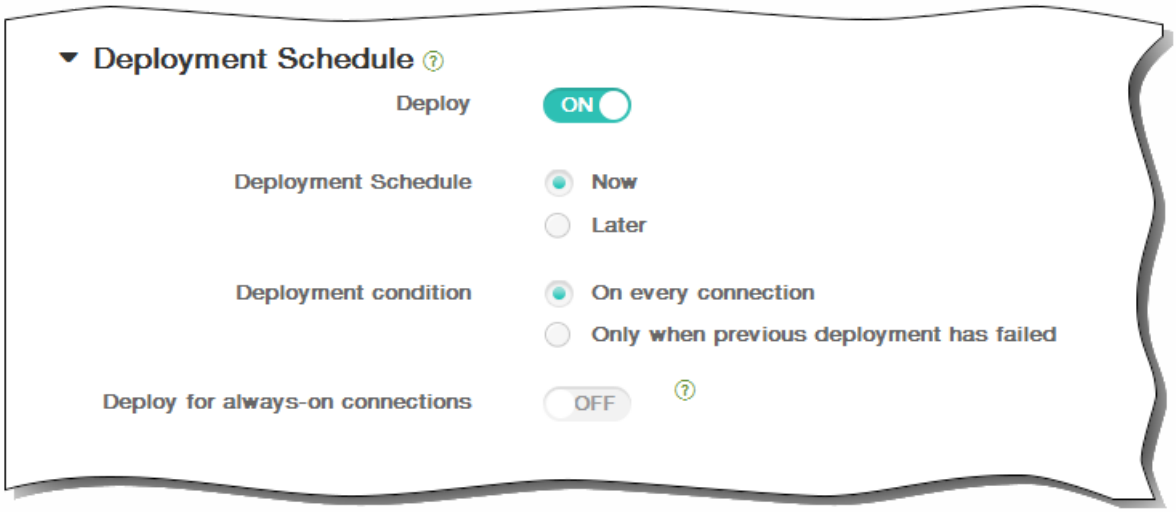


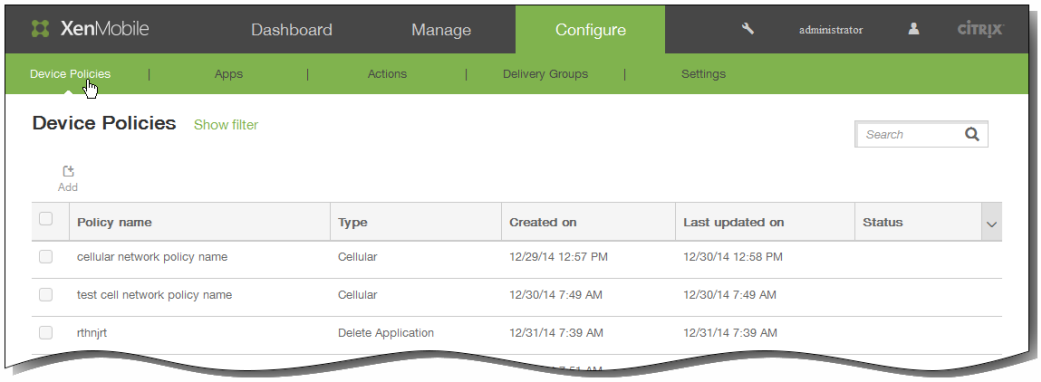


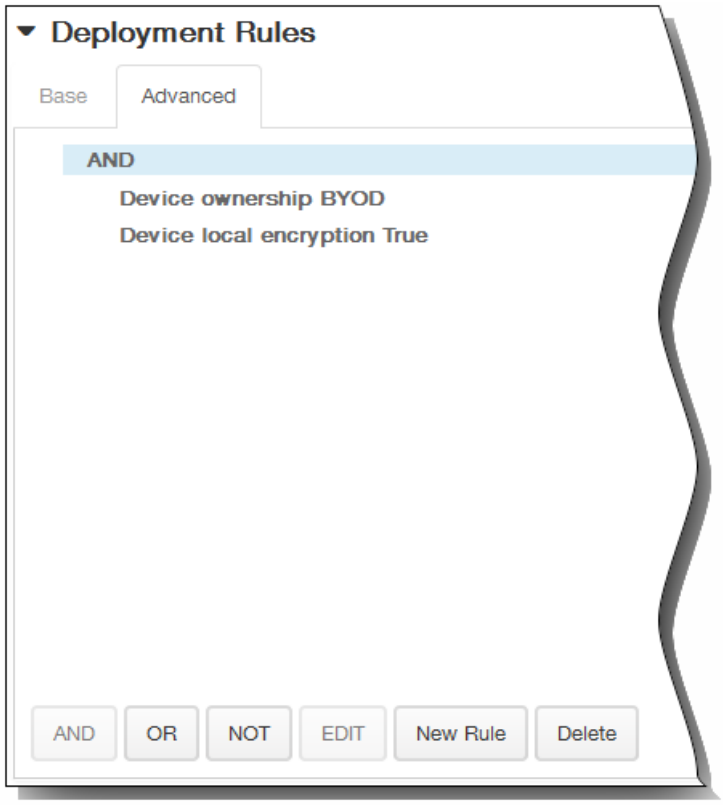


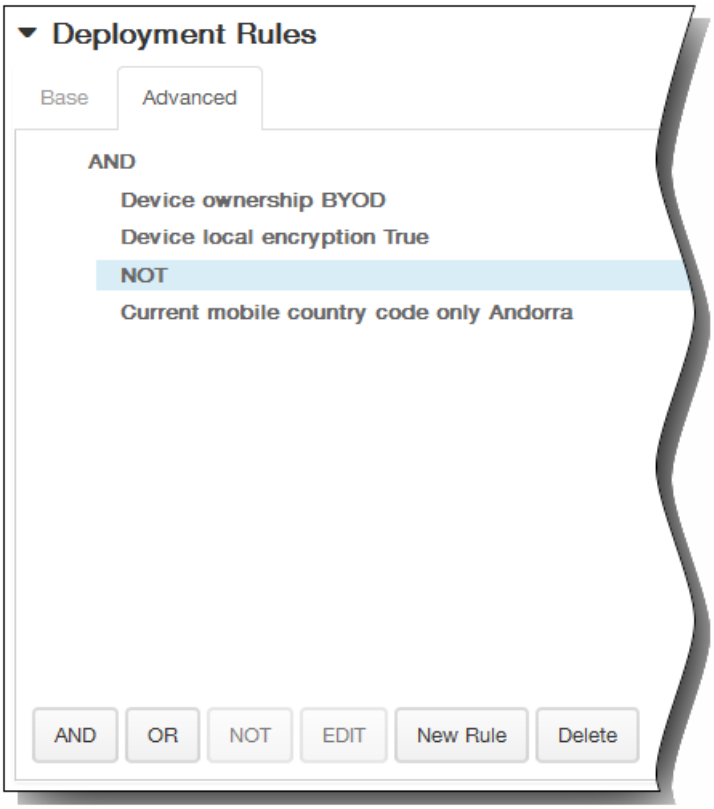


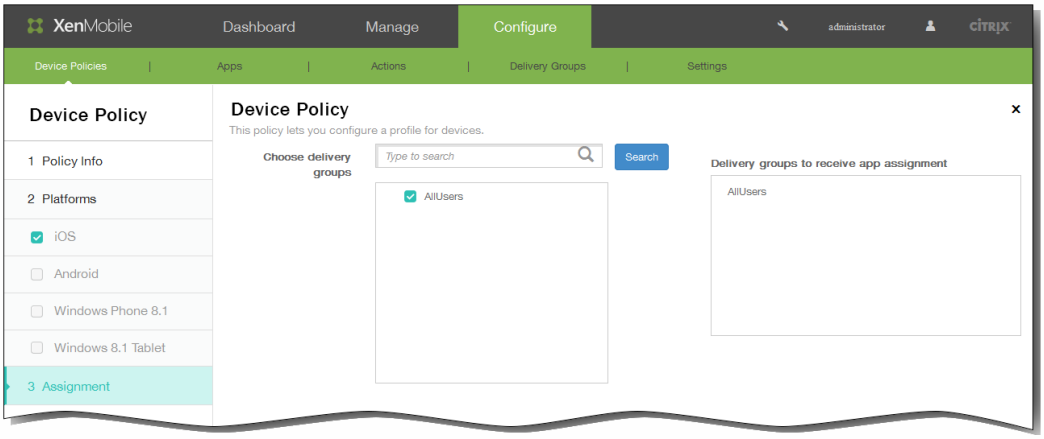


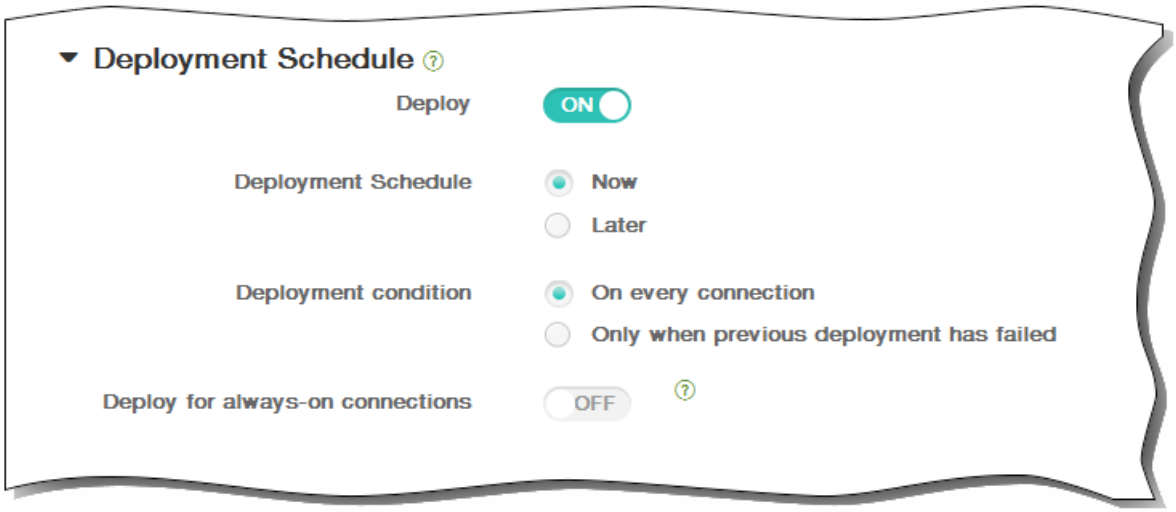


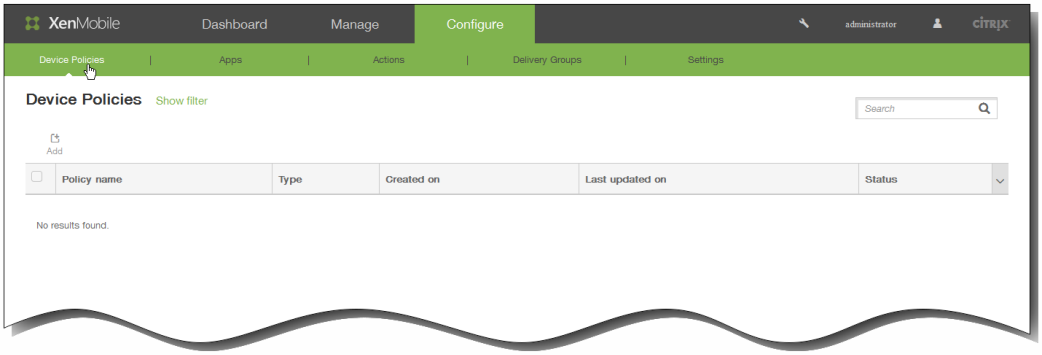


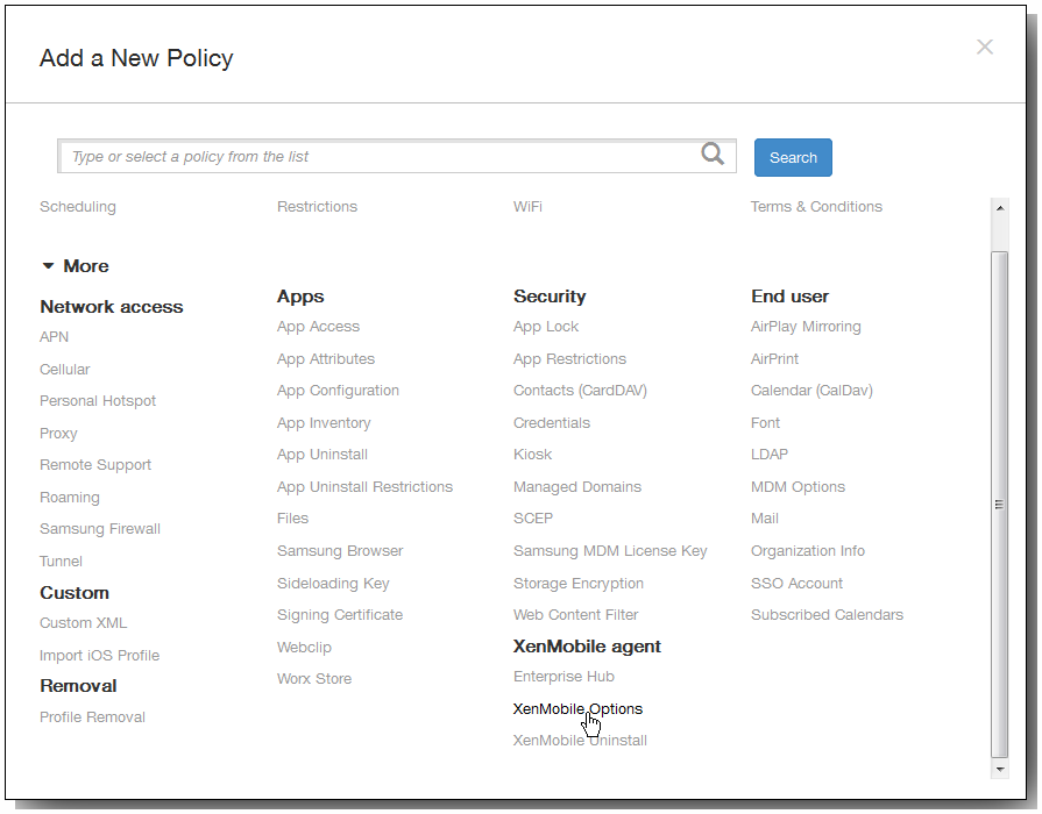


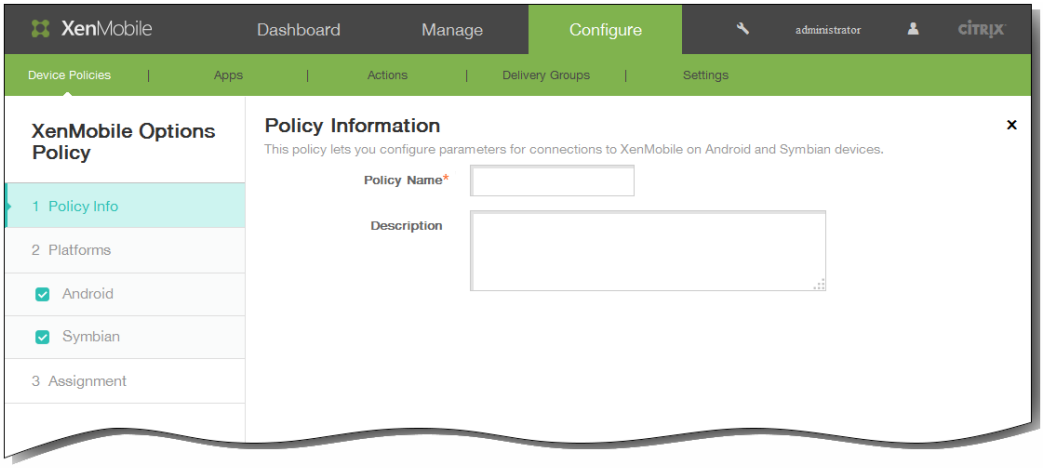


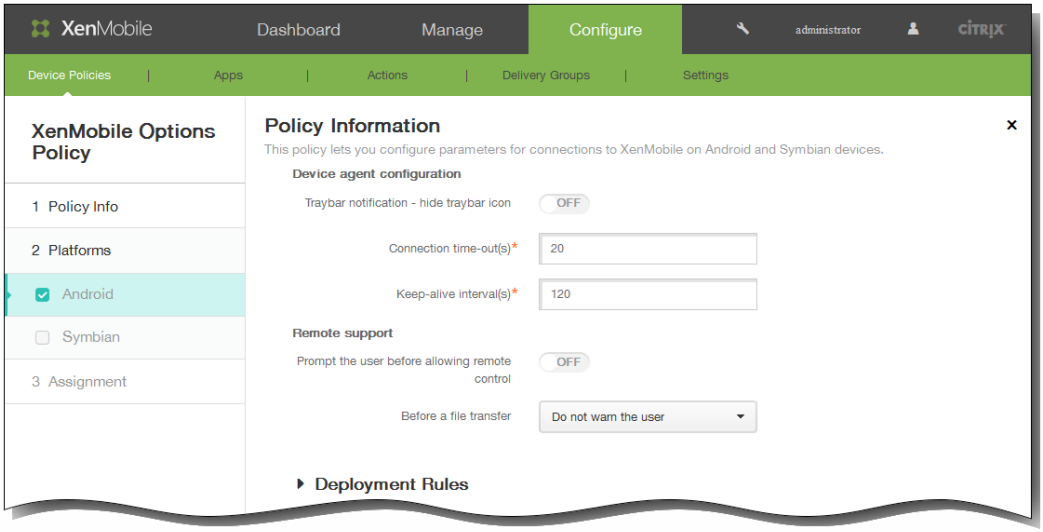


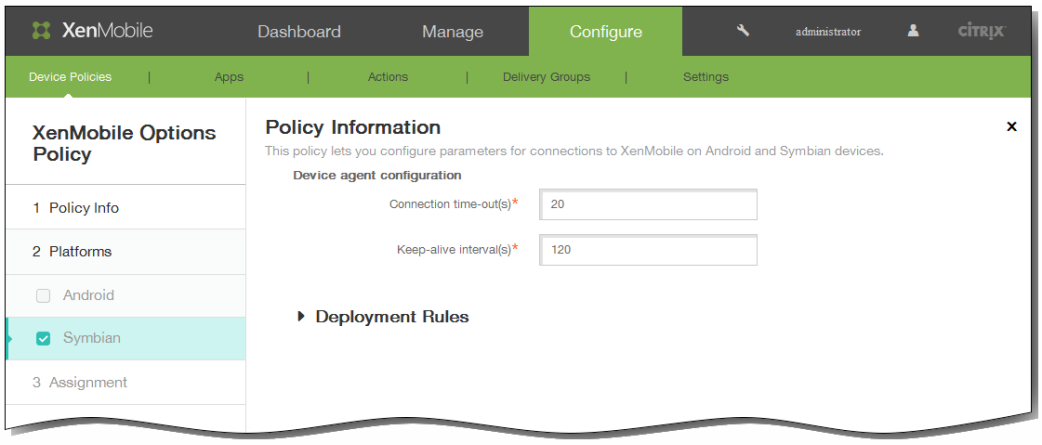


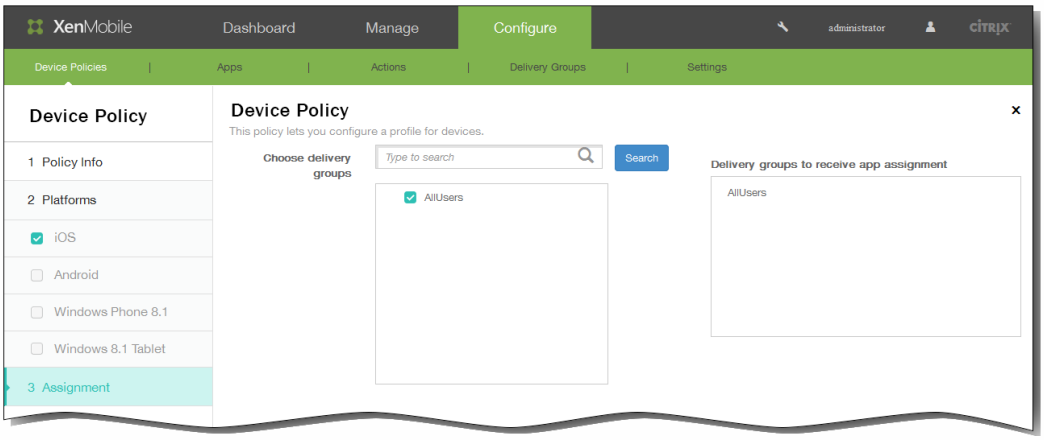


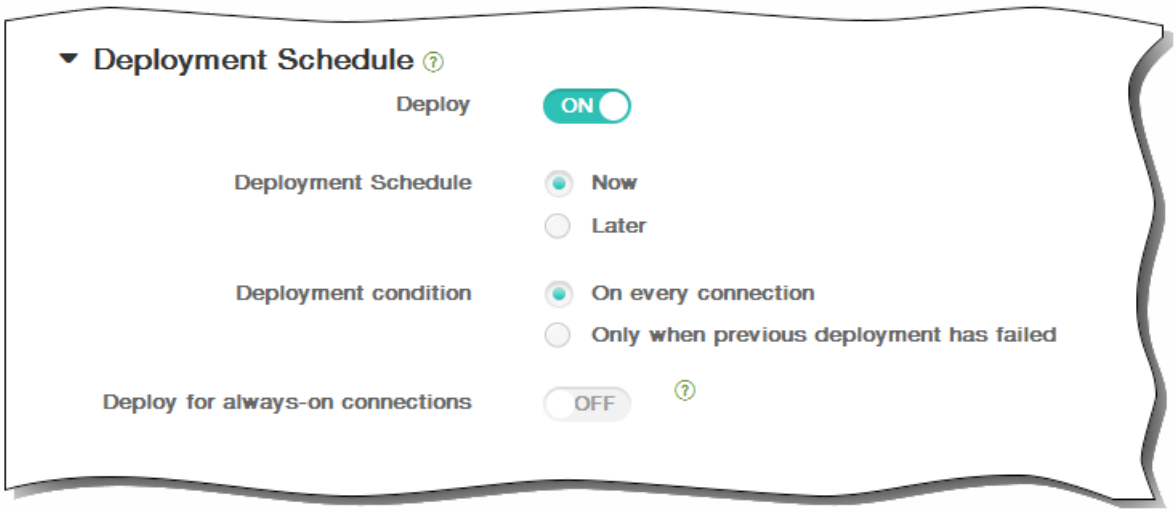


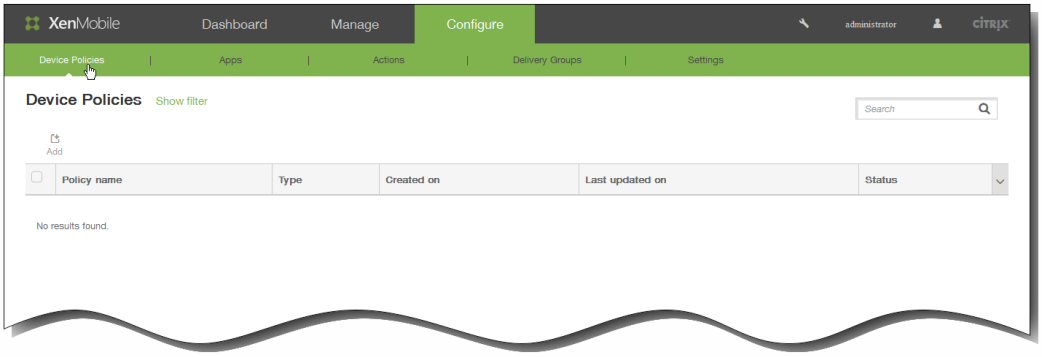


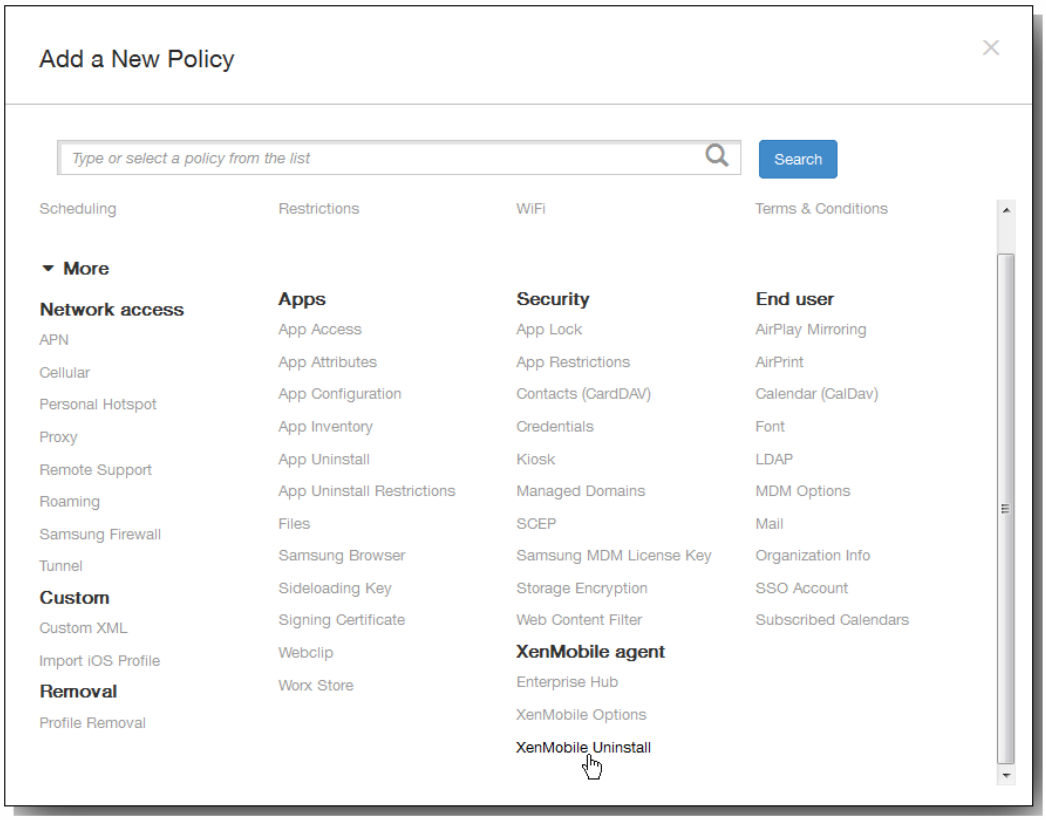


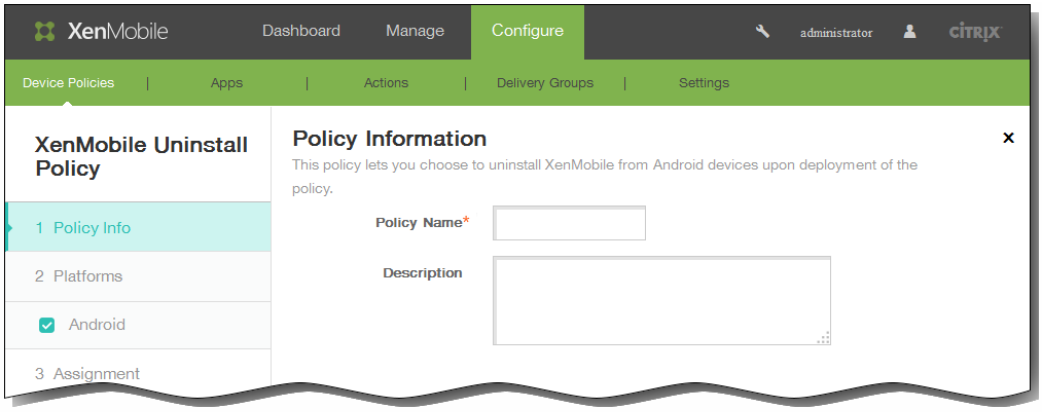


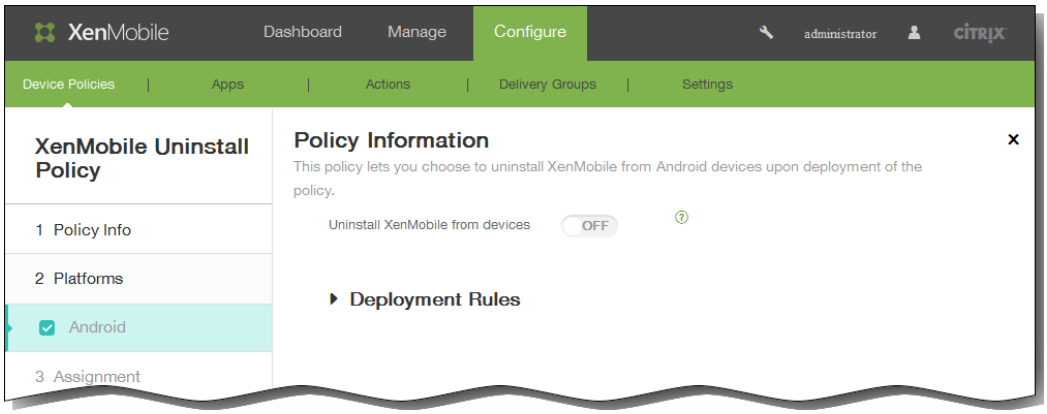


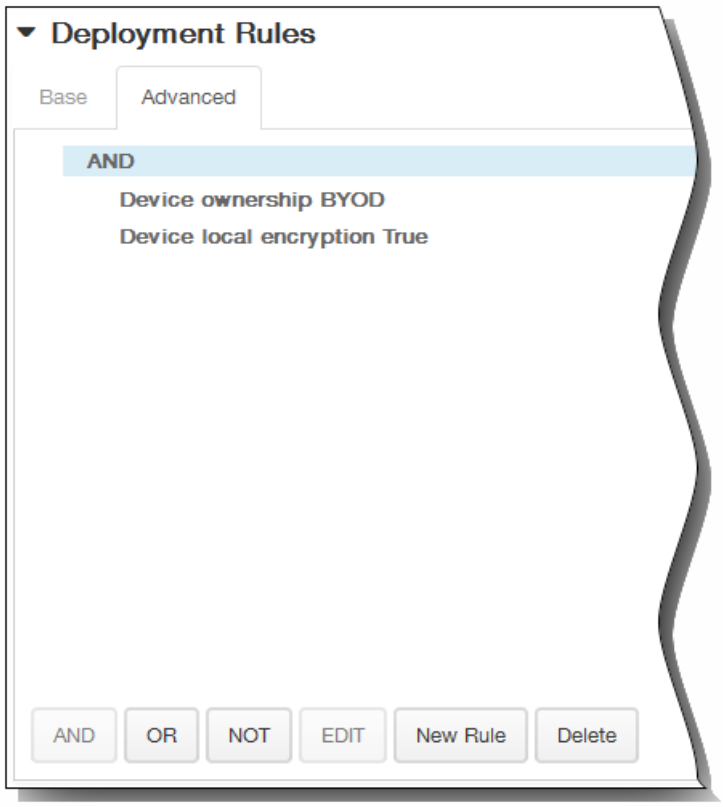


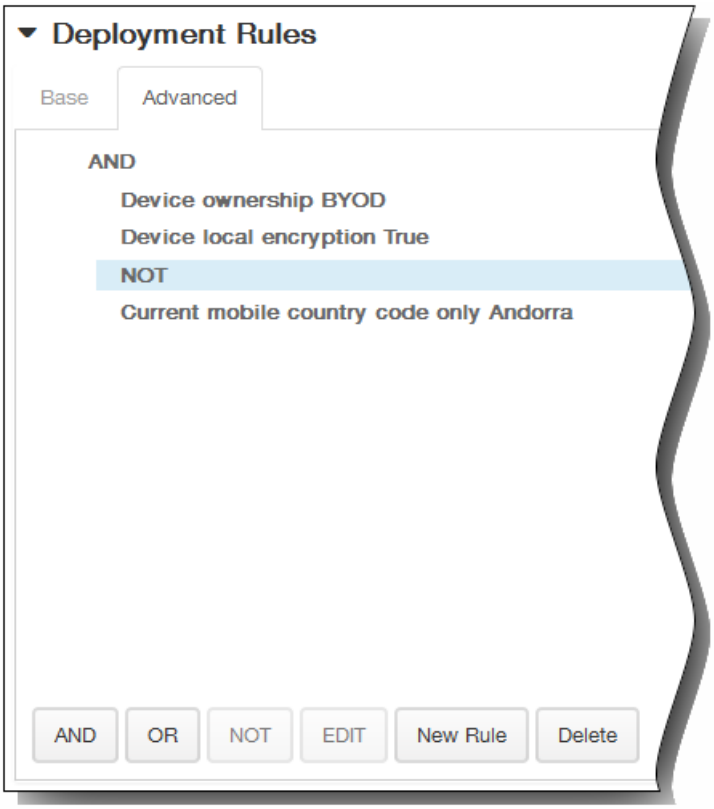


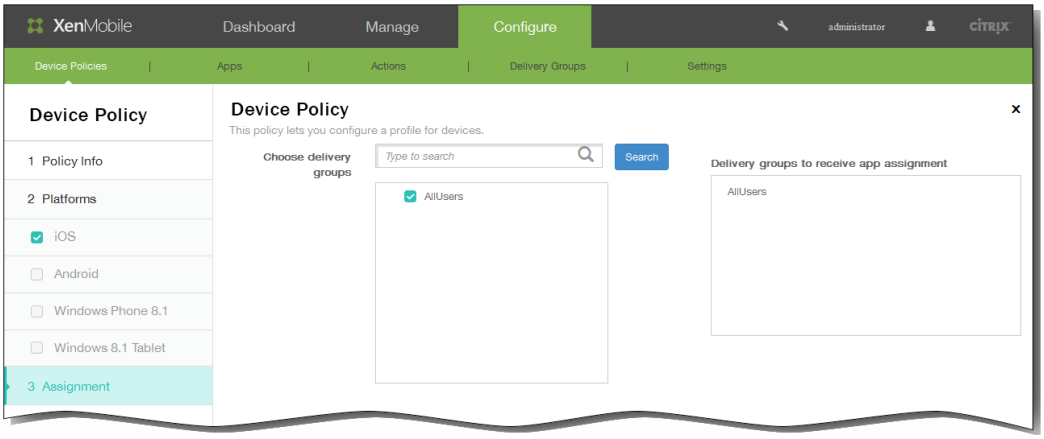


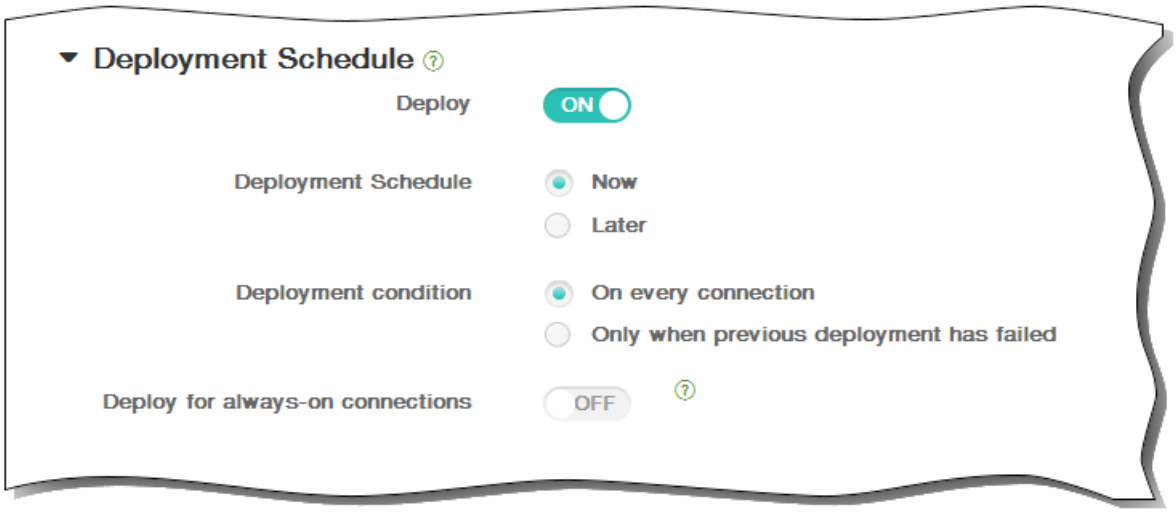






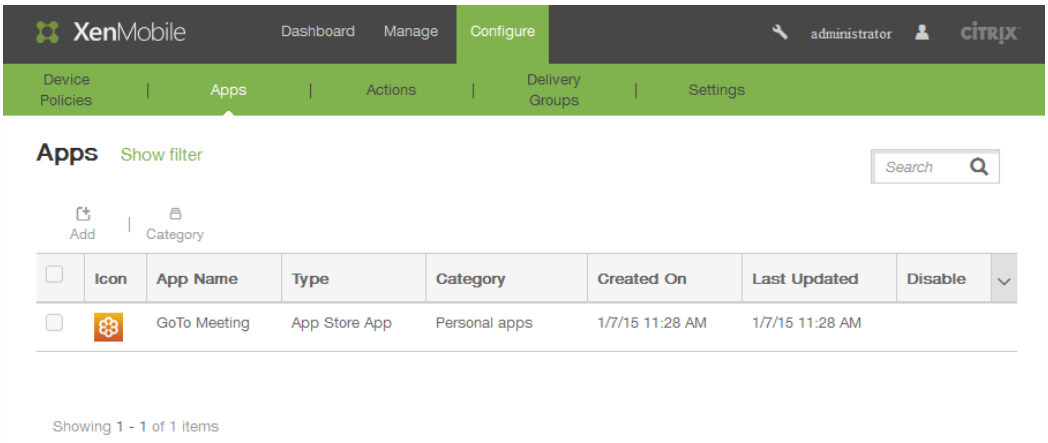






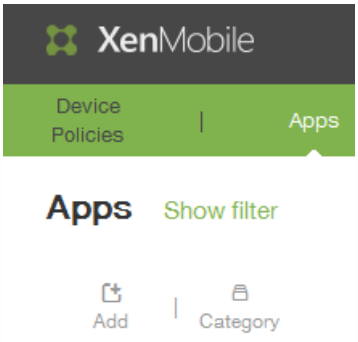
-
-
-
-
-
-
-

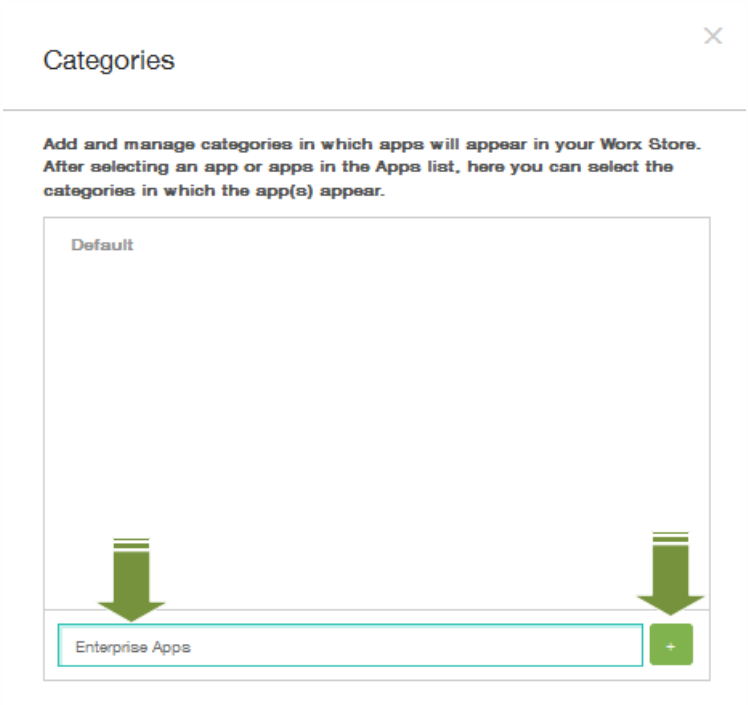
-
-
-
-

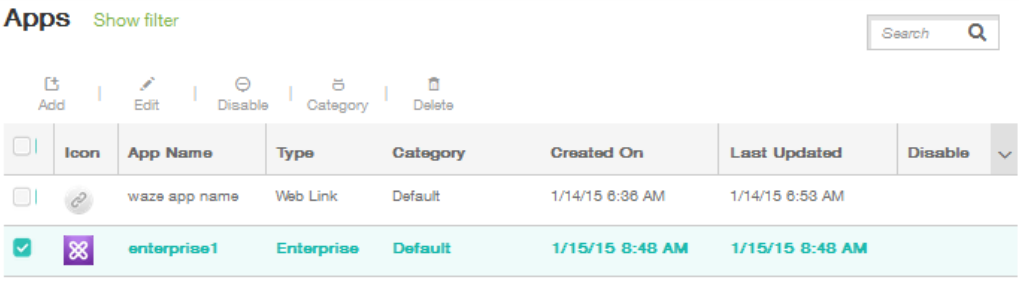


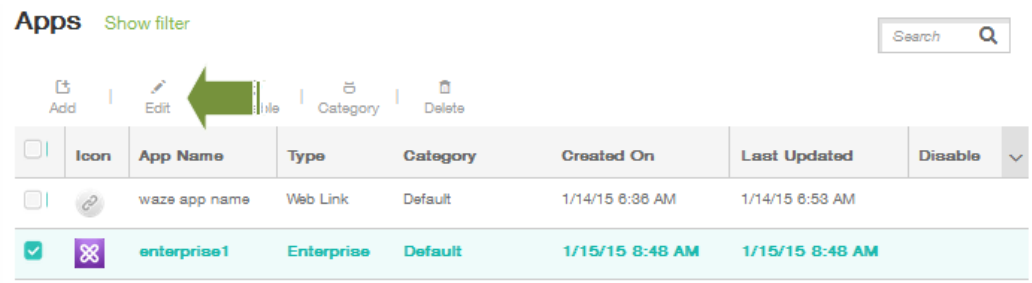
-
-
-
-
-

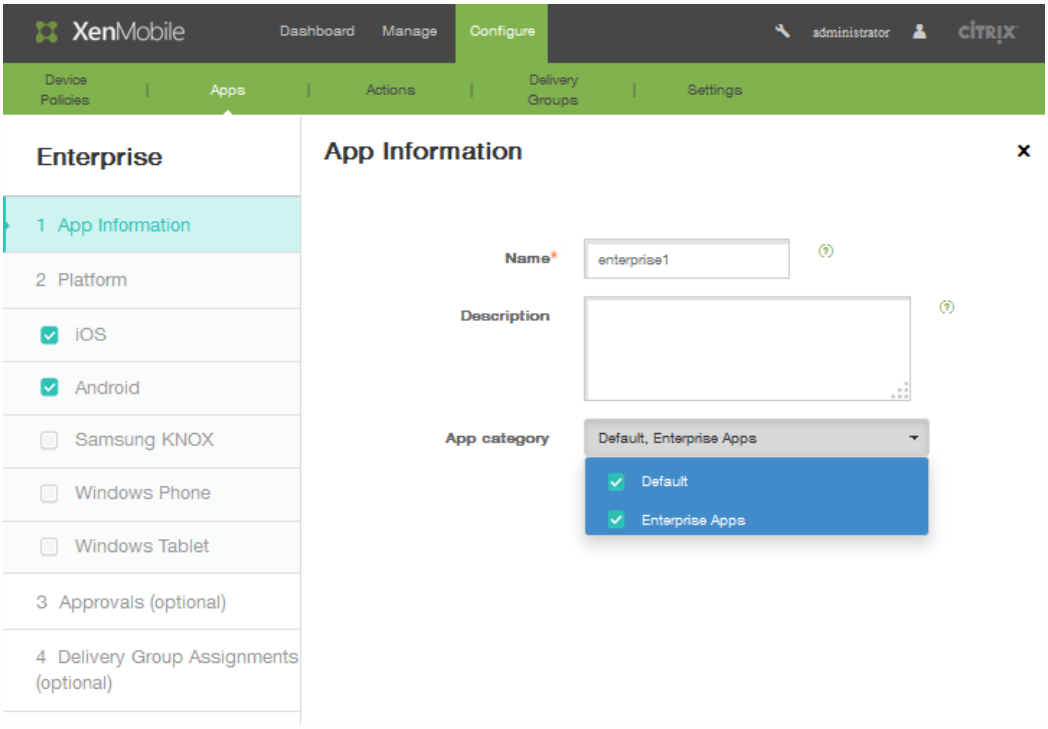
添加应用程序类别

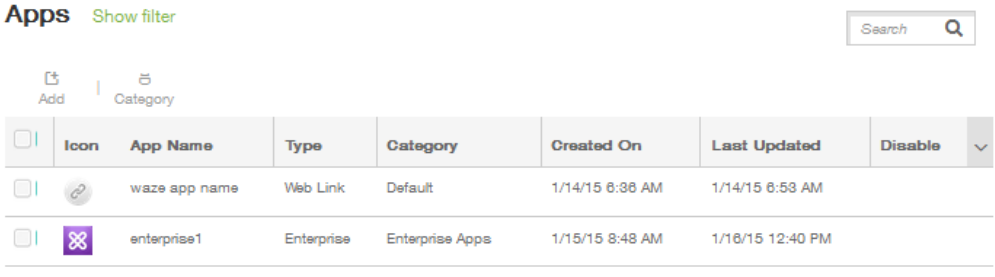


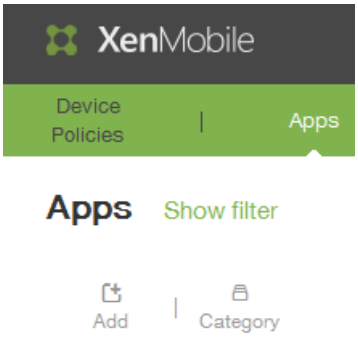


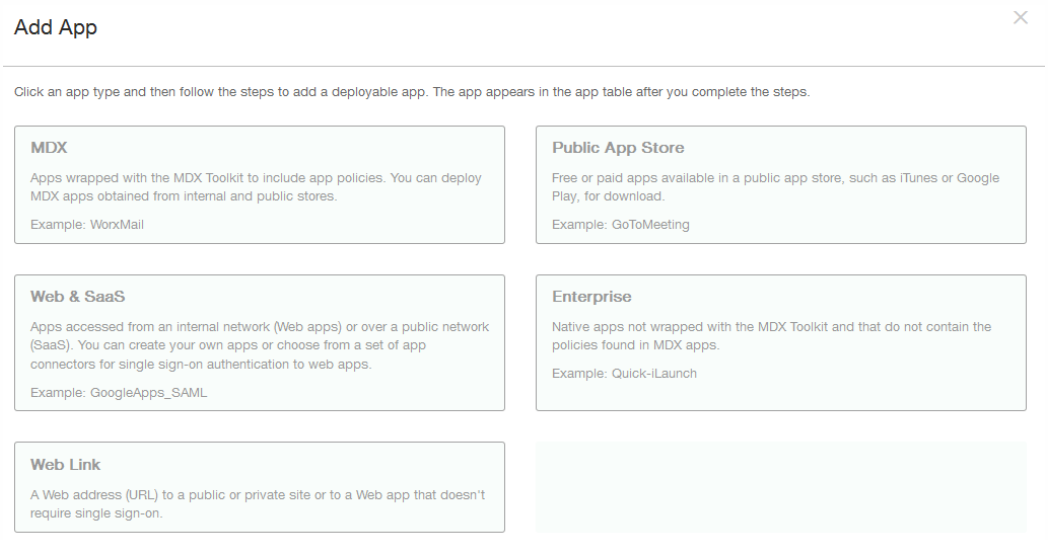


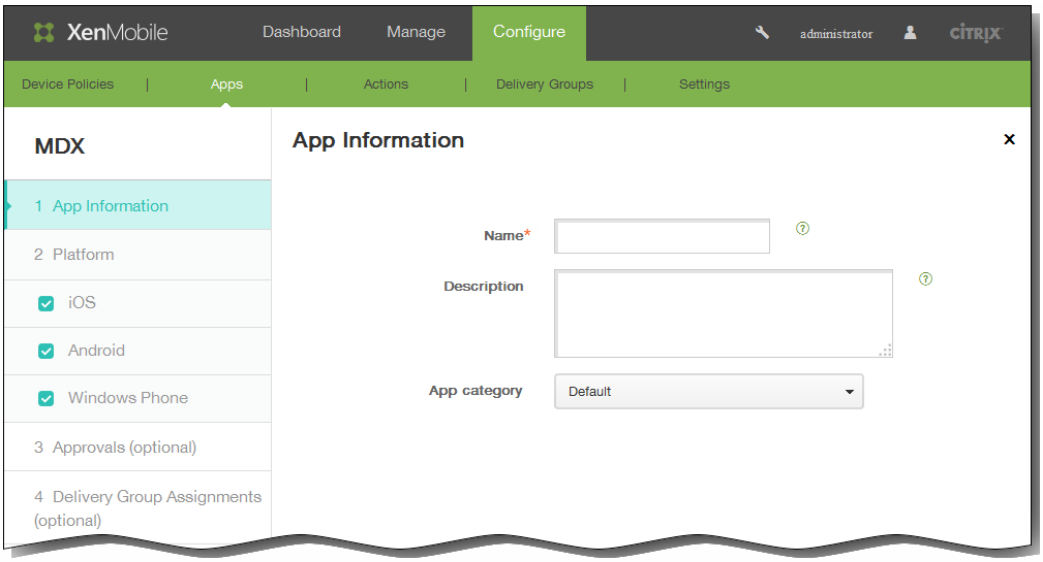


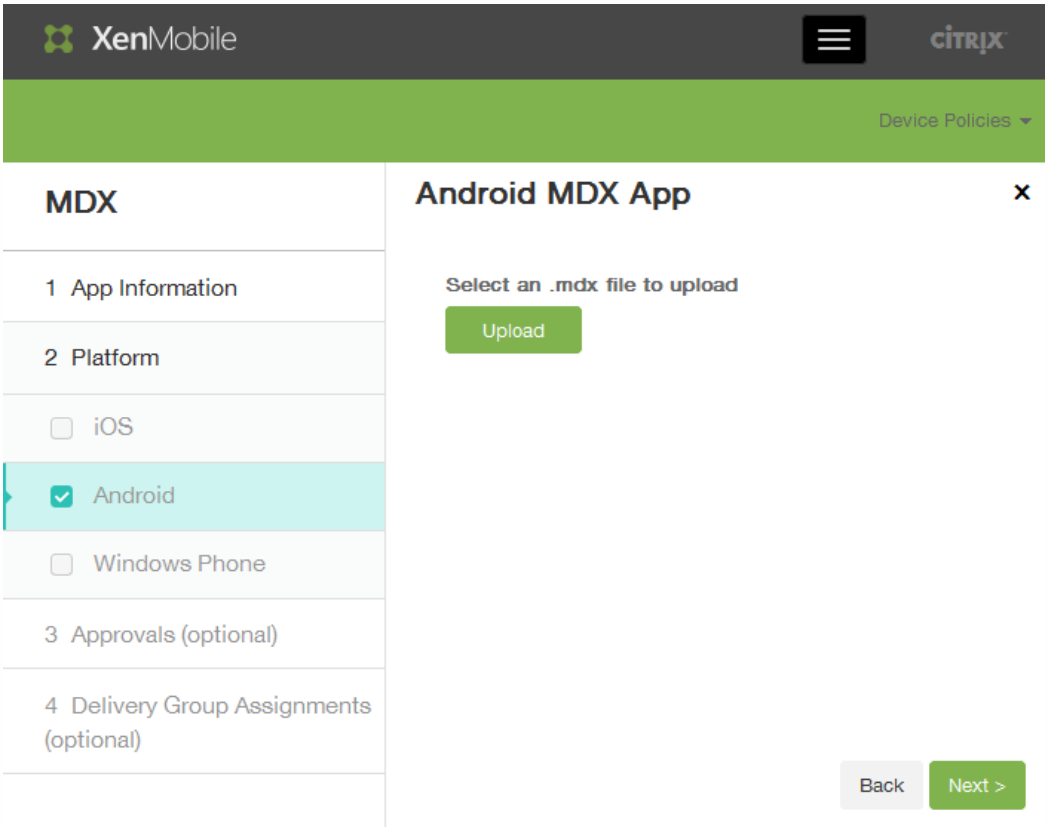


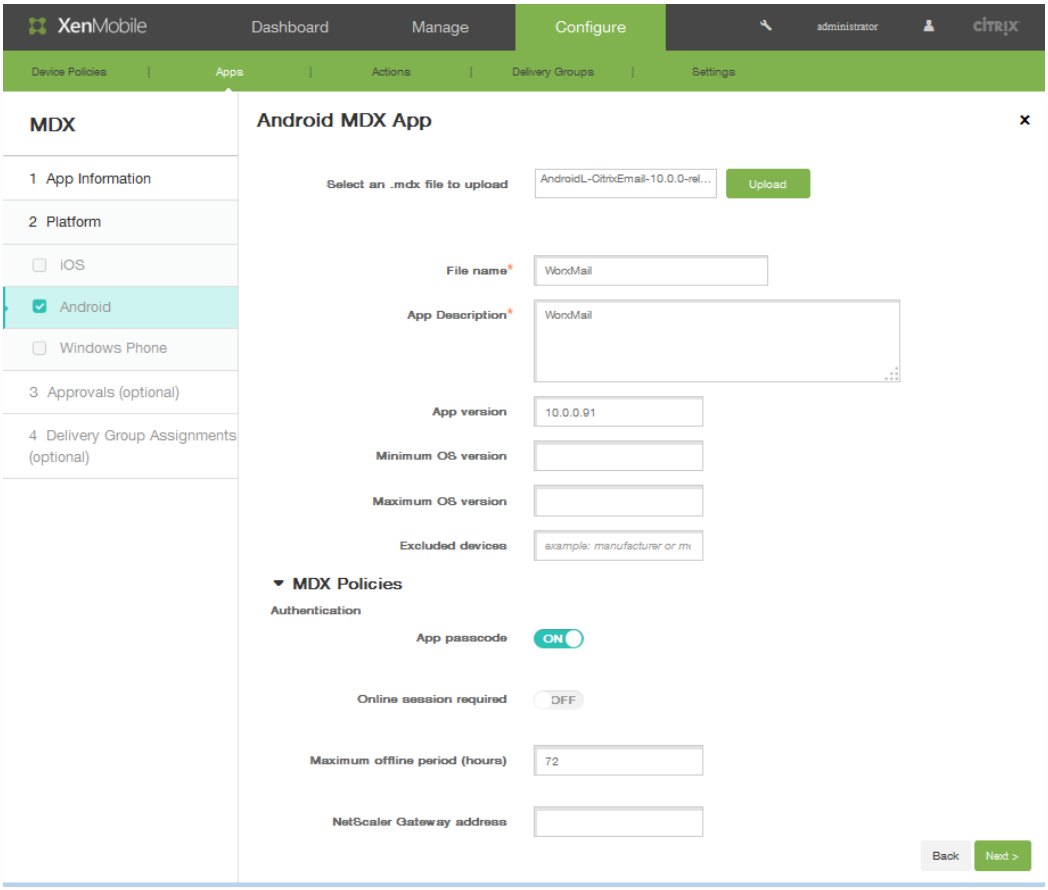


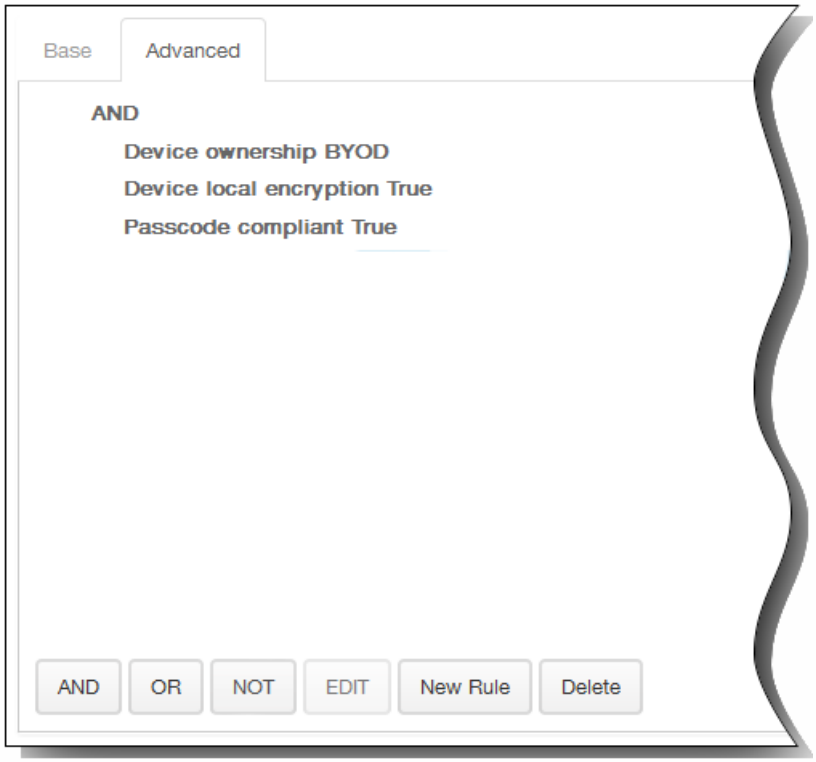


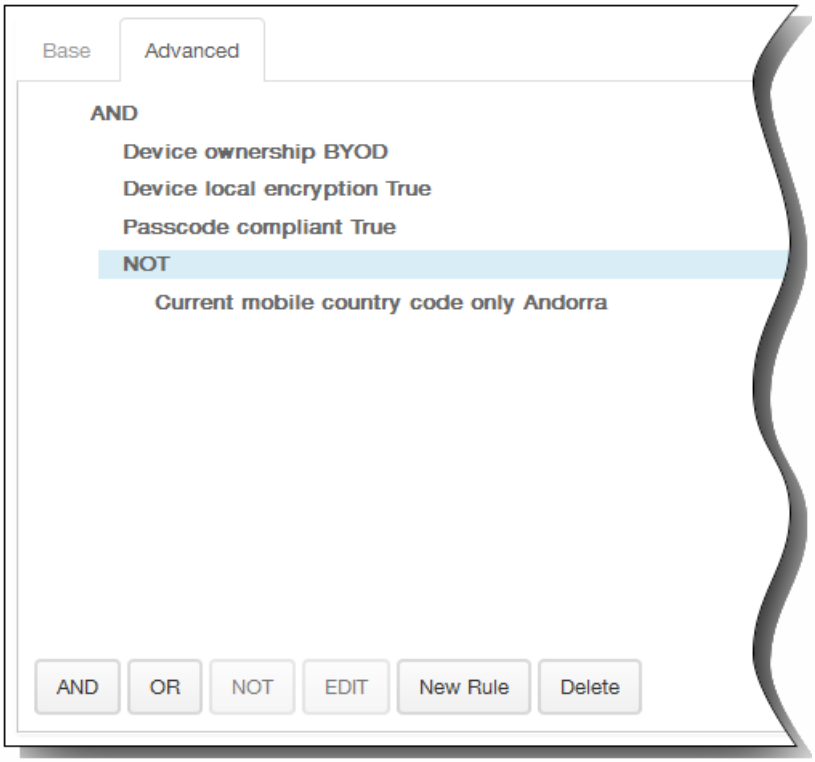


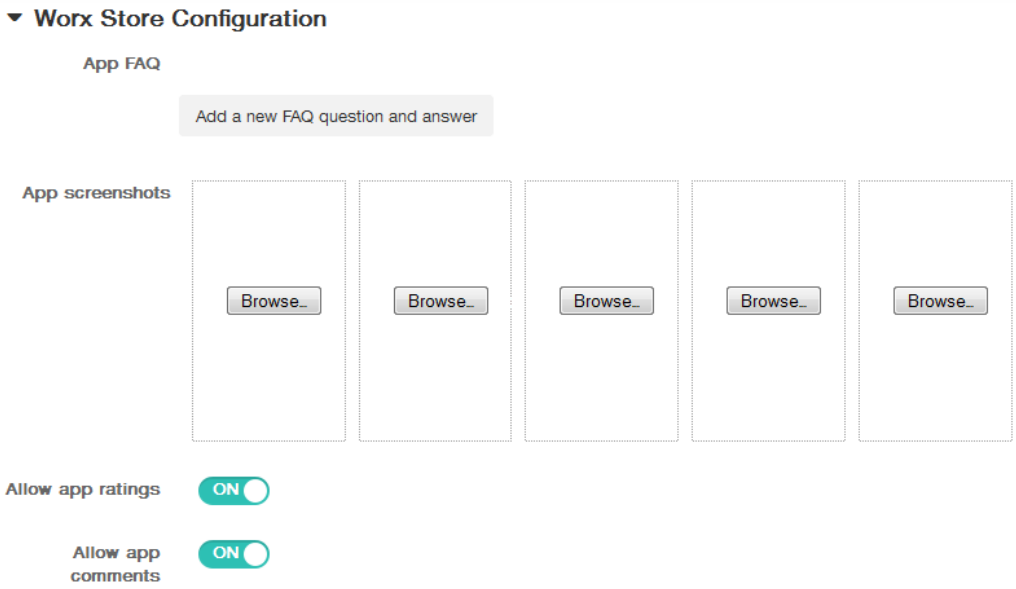


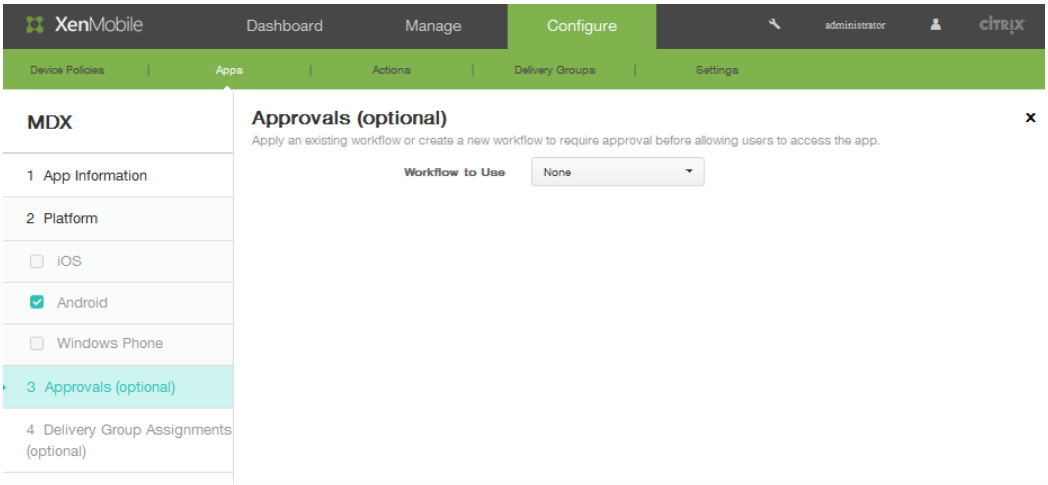


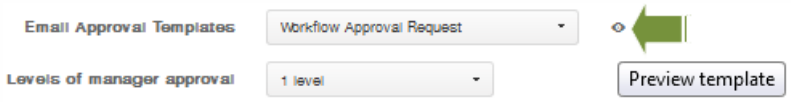


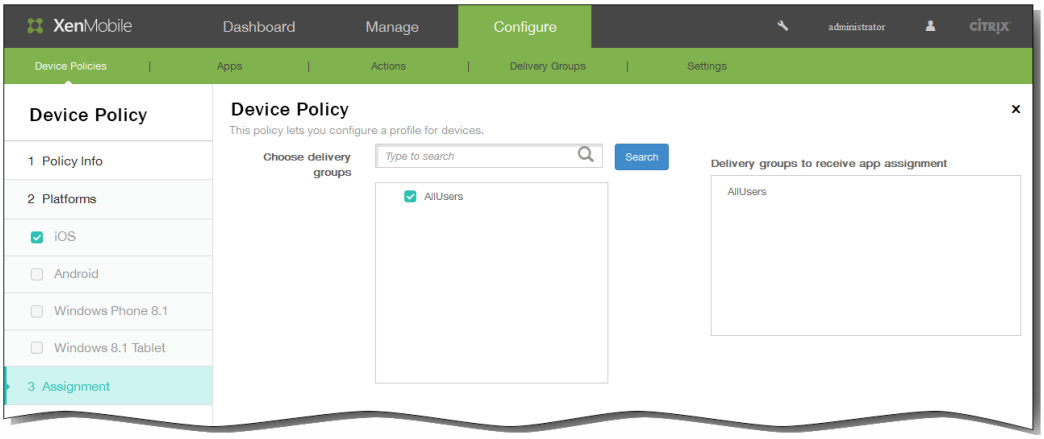


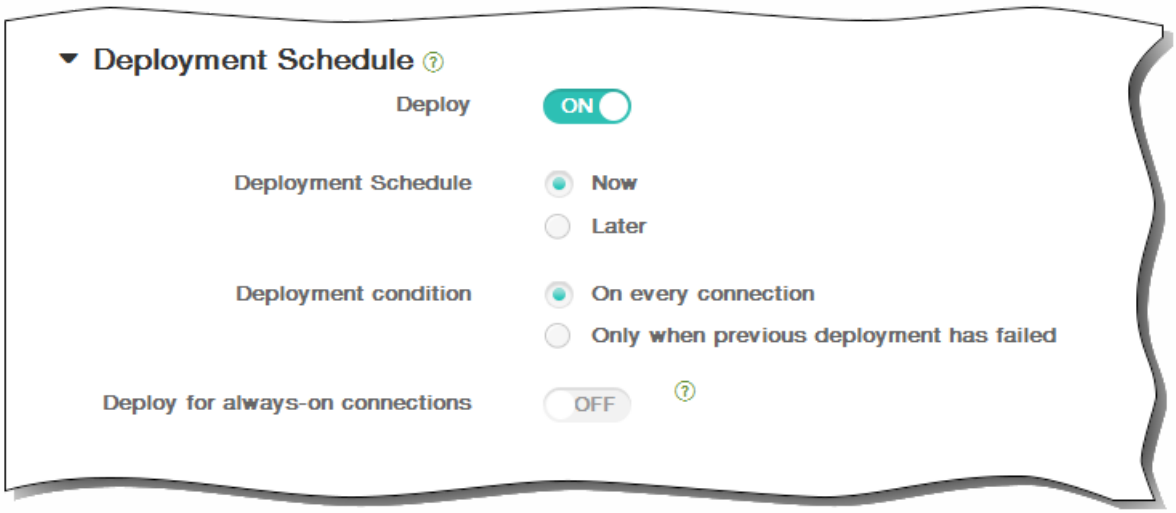


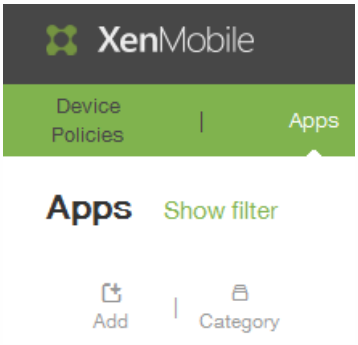


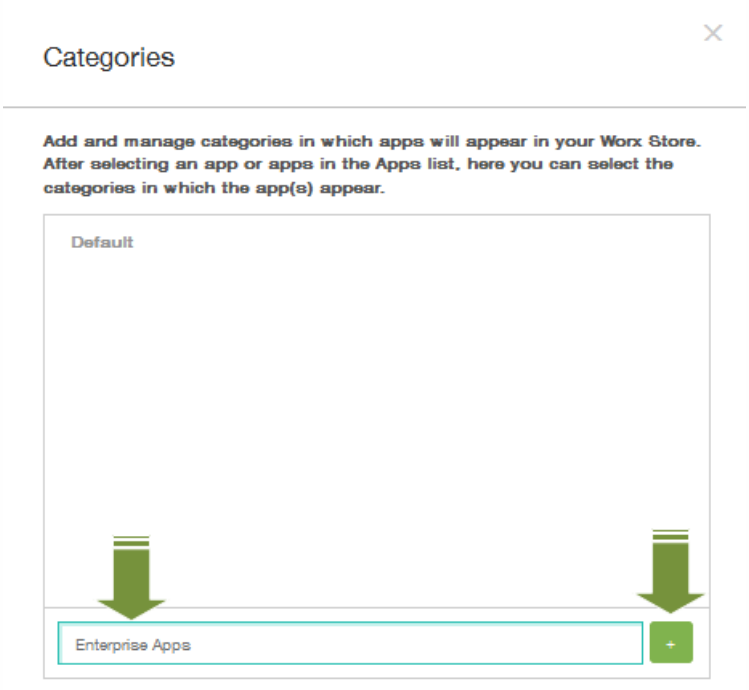


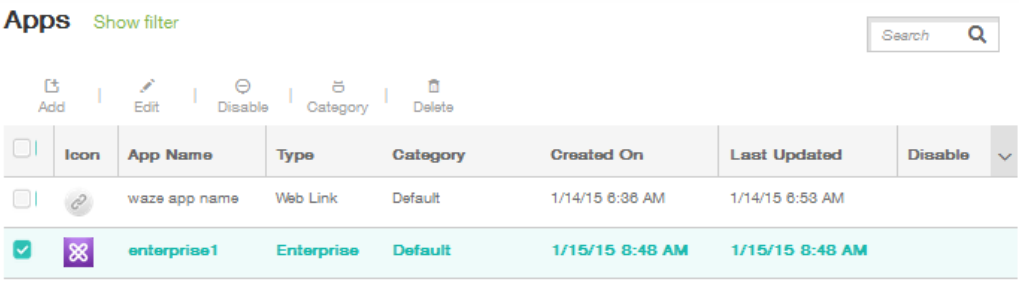


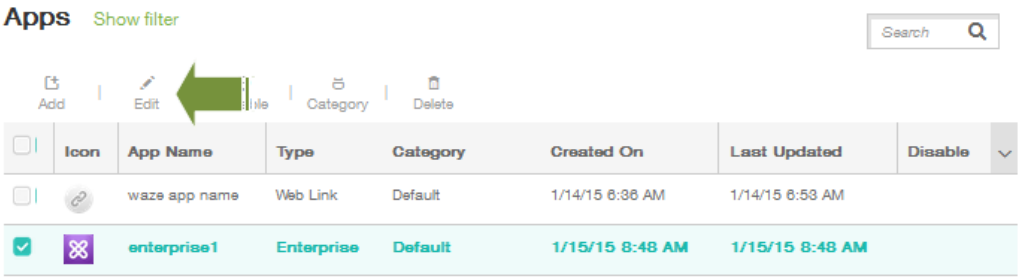


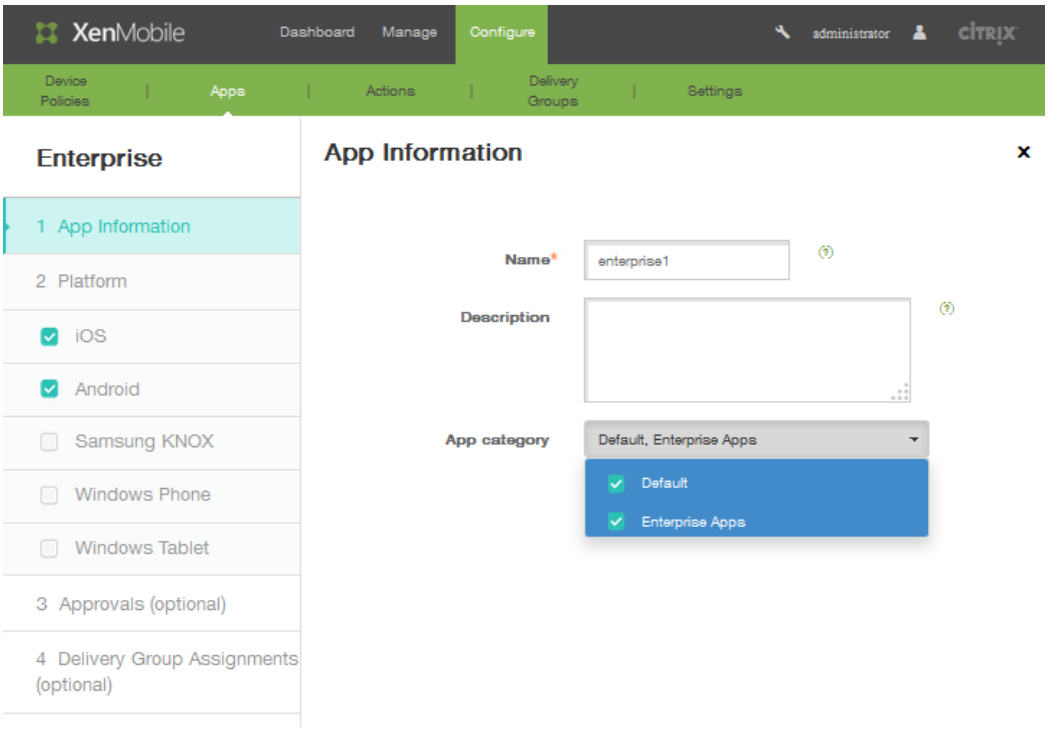


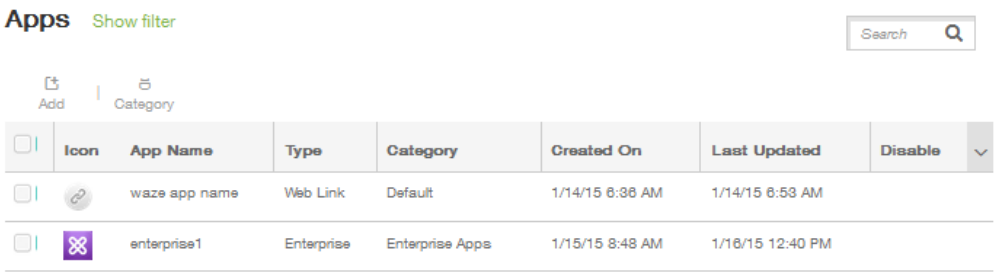


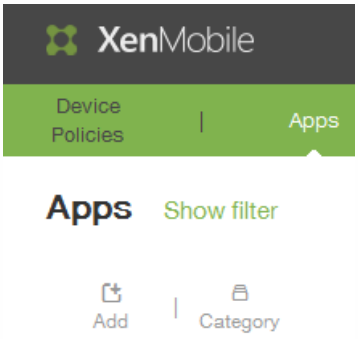


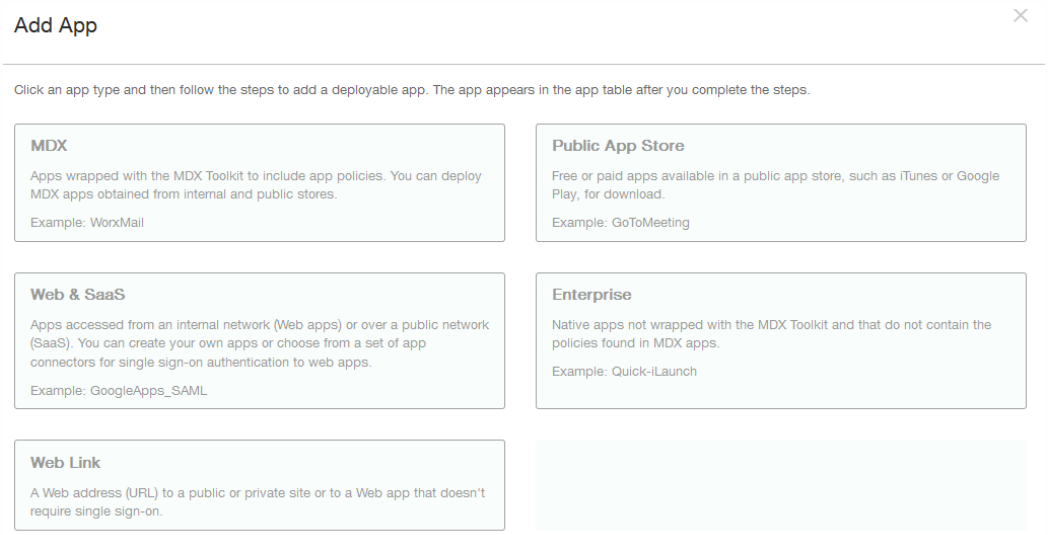


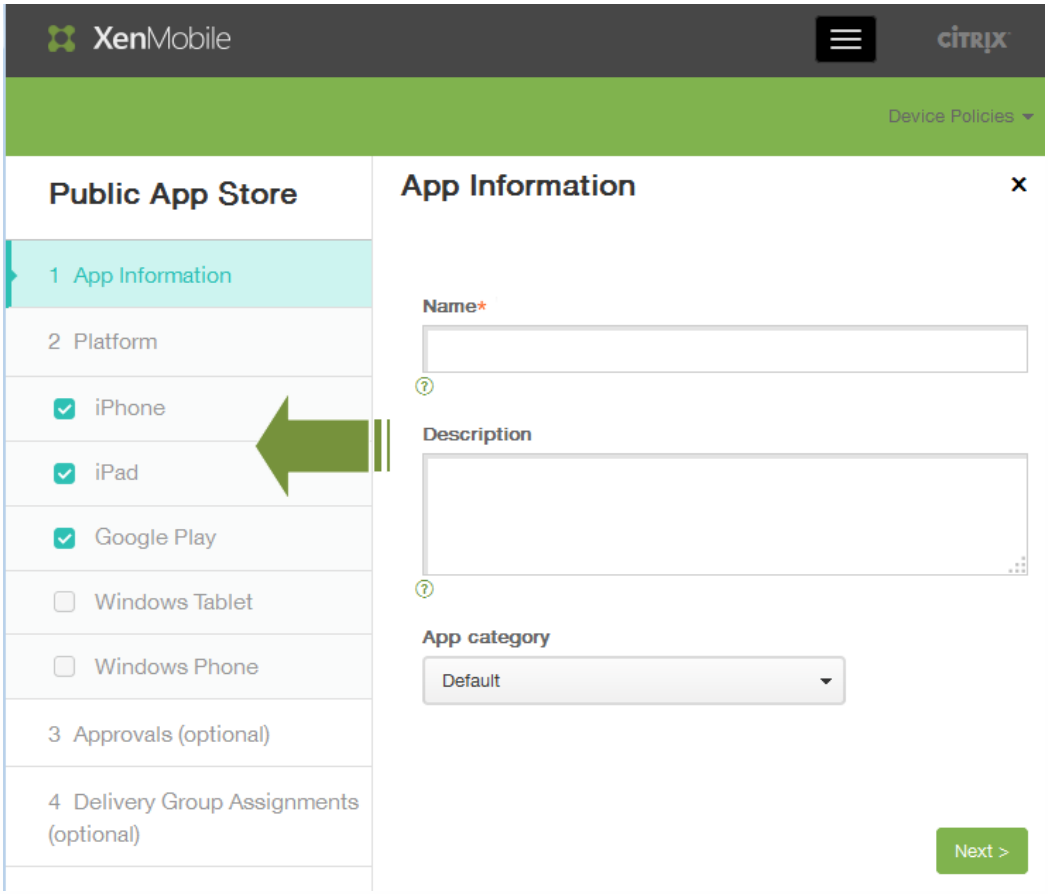


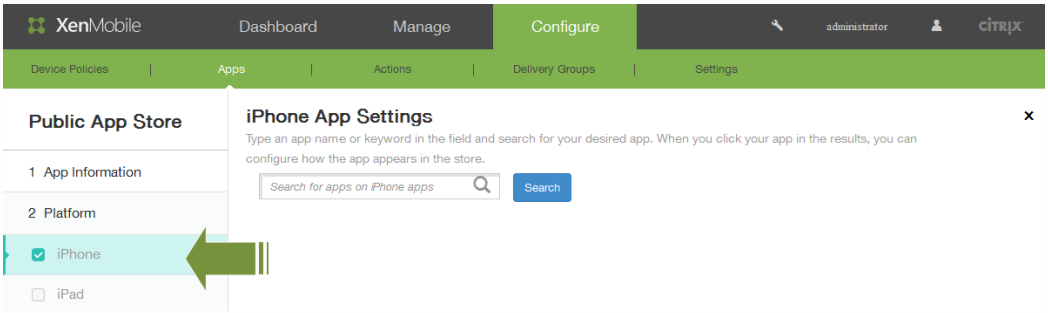


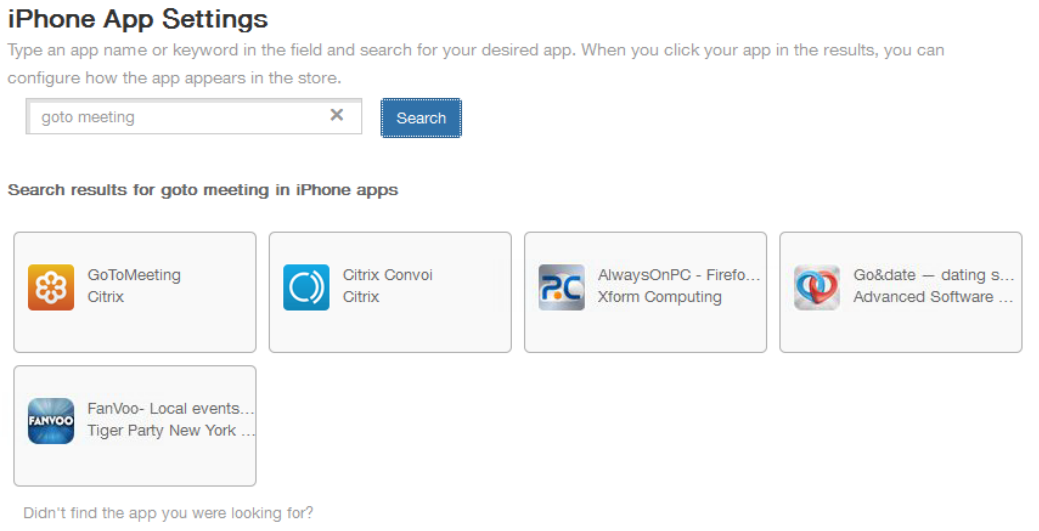


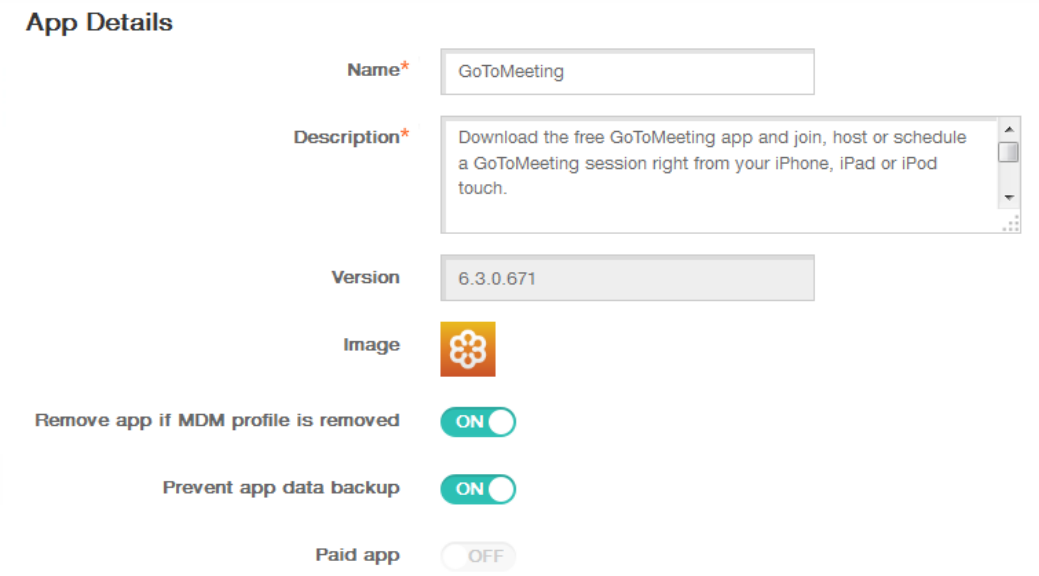


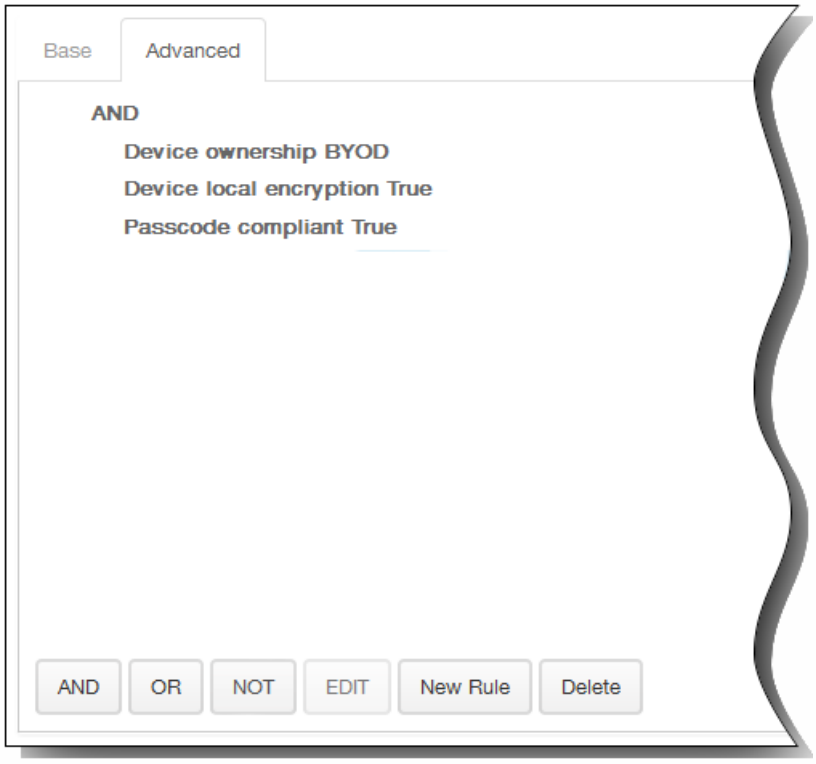


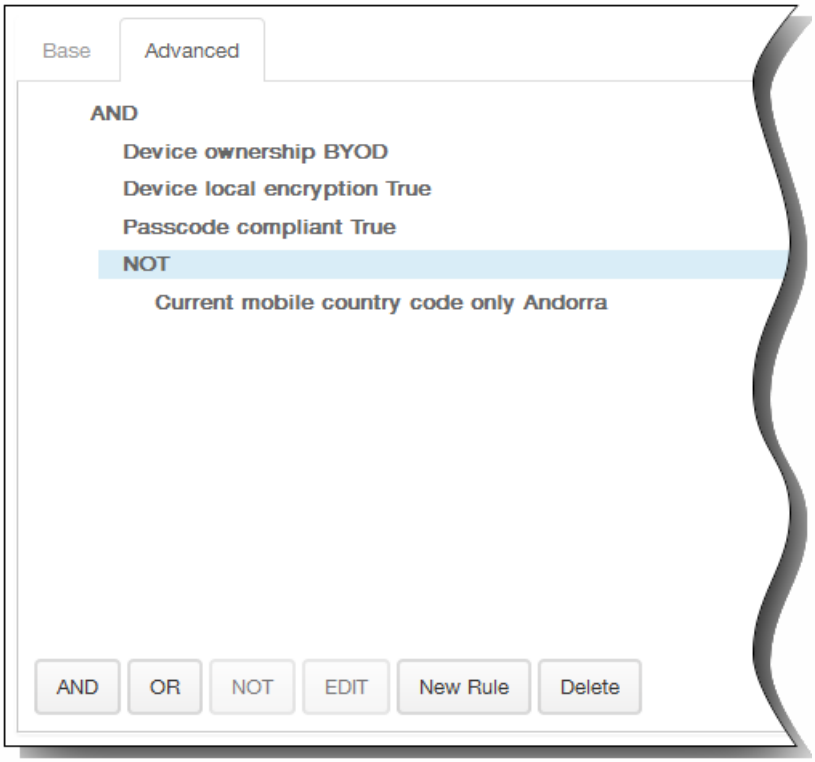


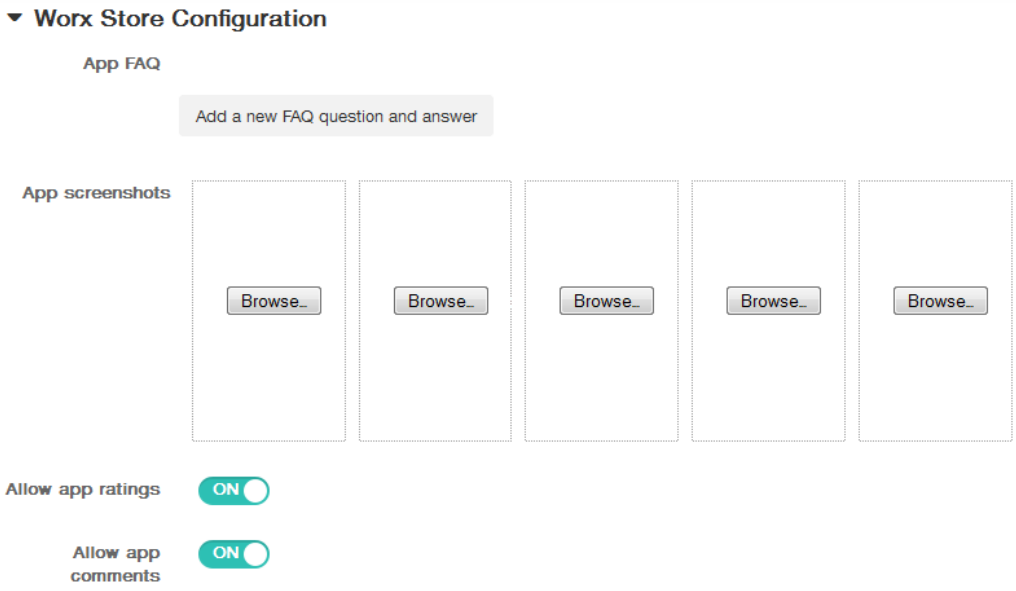


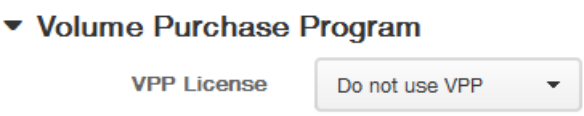


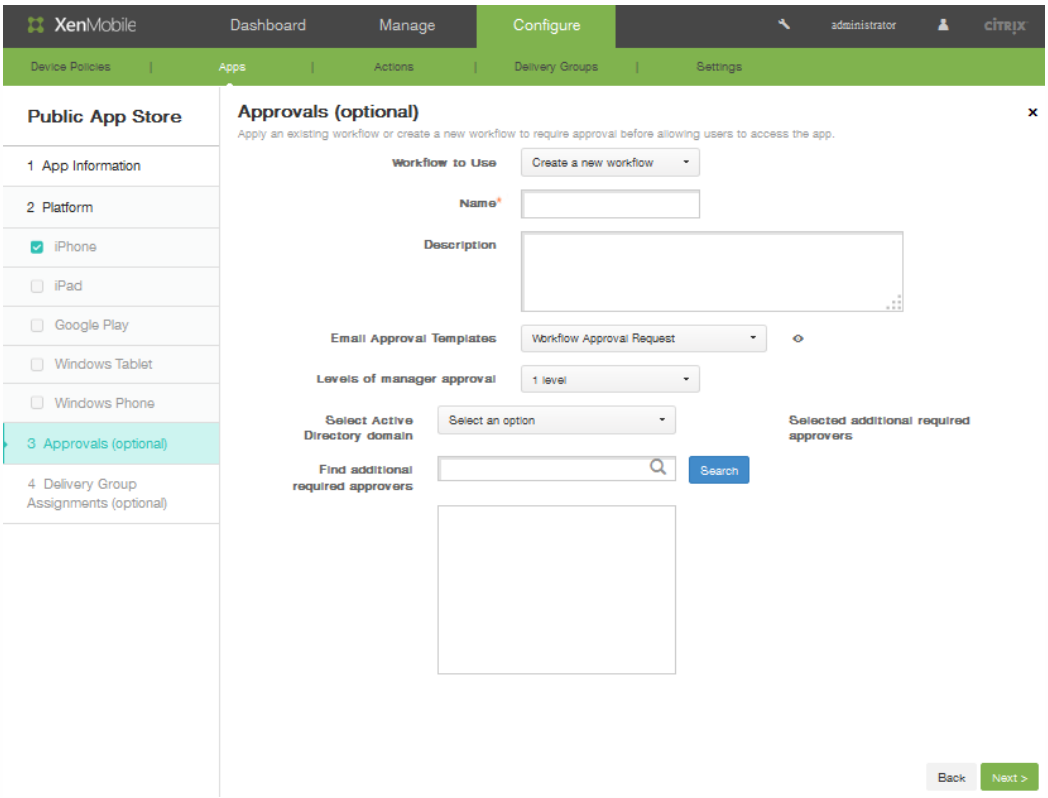


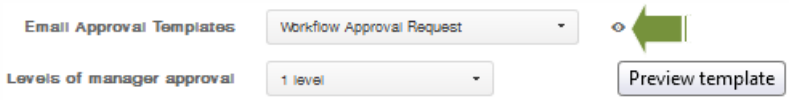


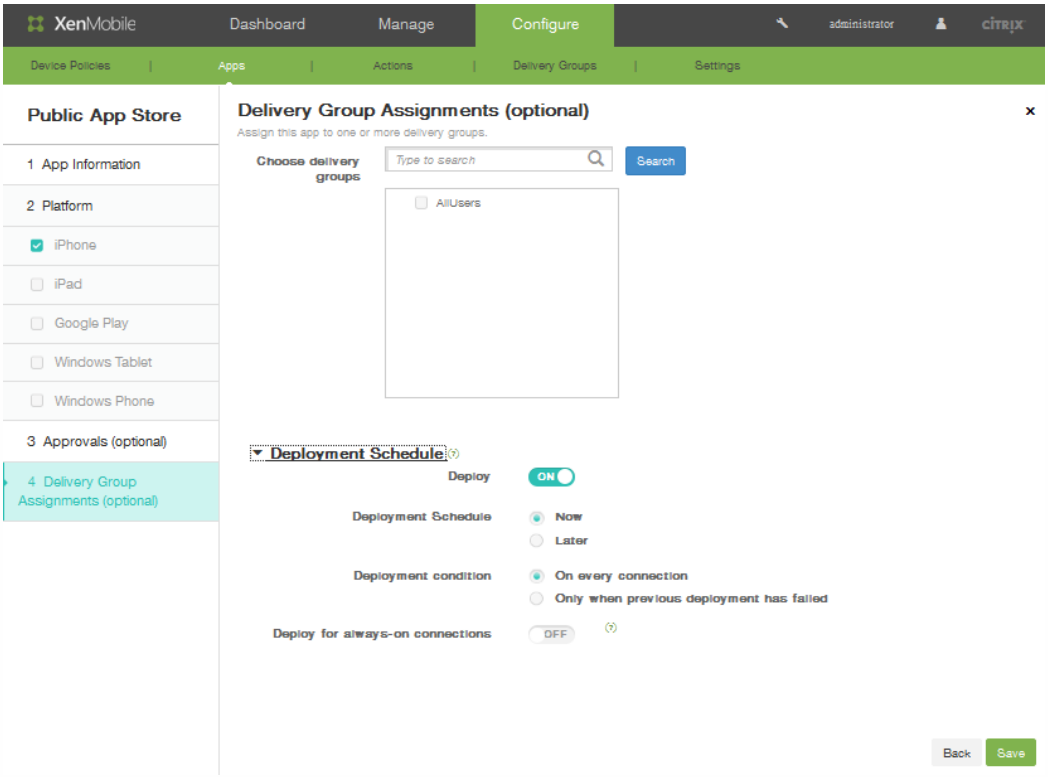








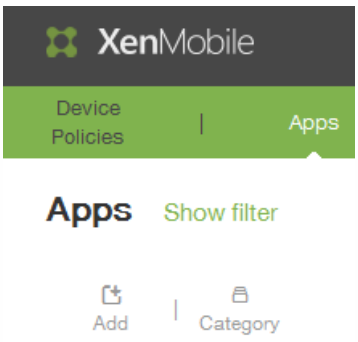


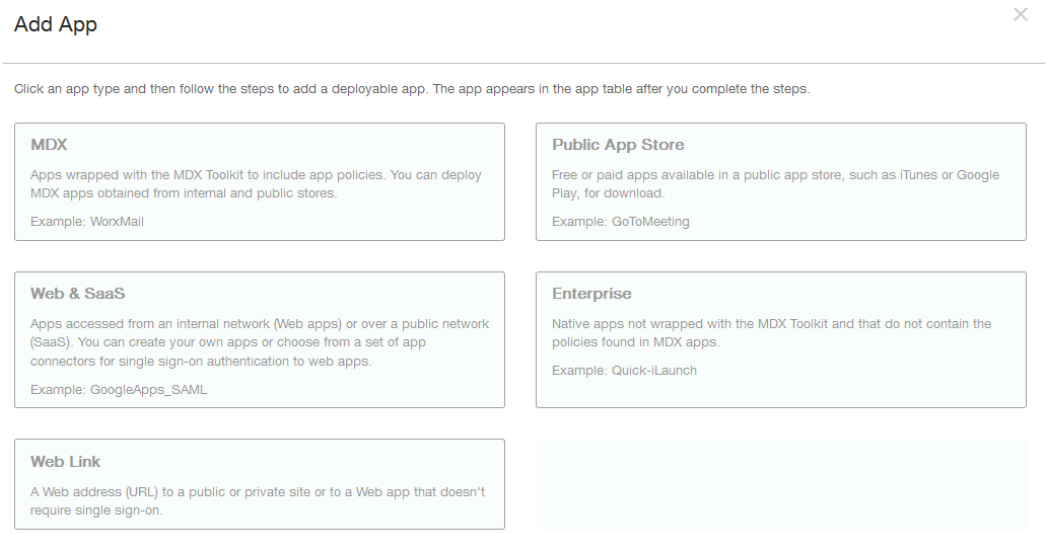


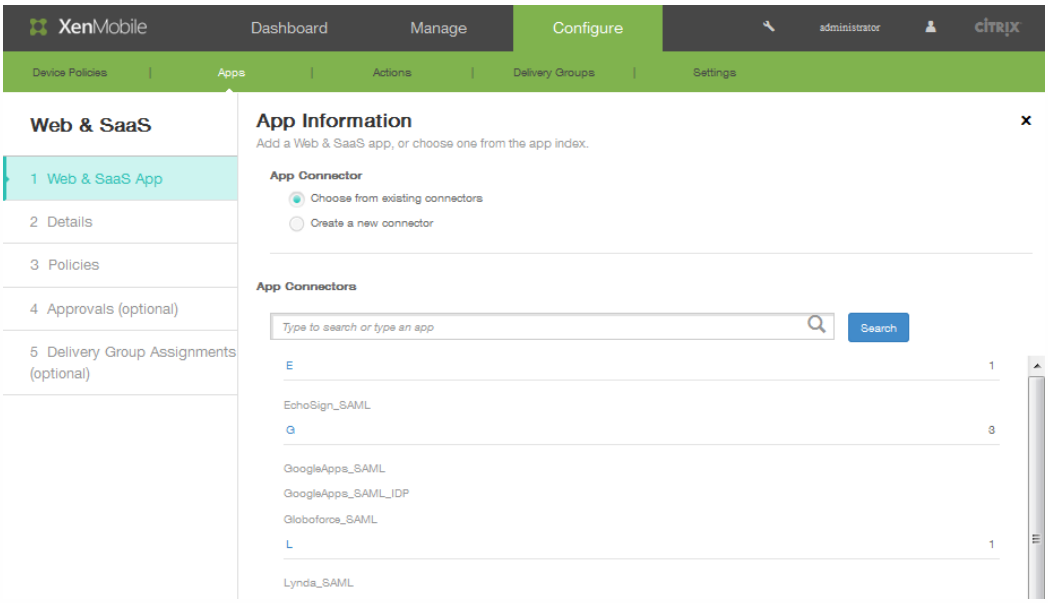
-
-
-

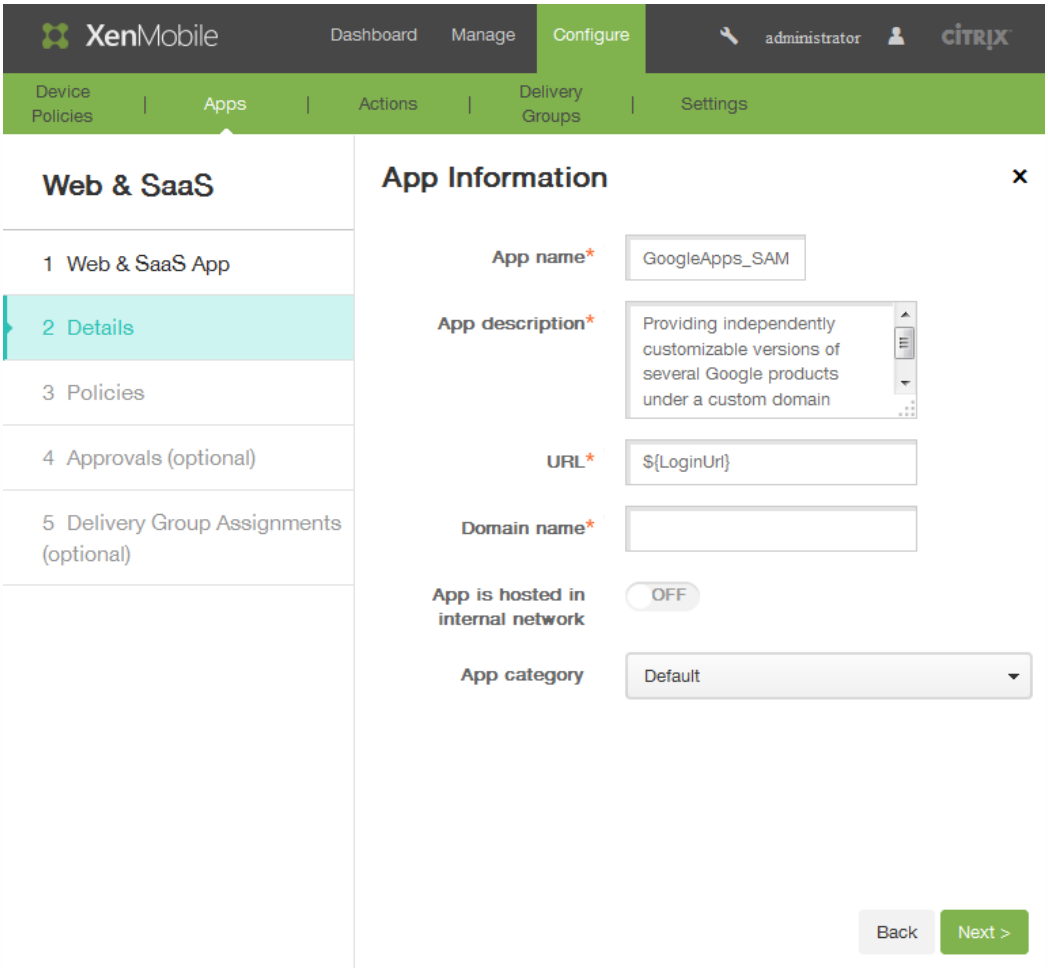
-
-
-
-
-
-

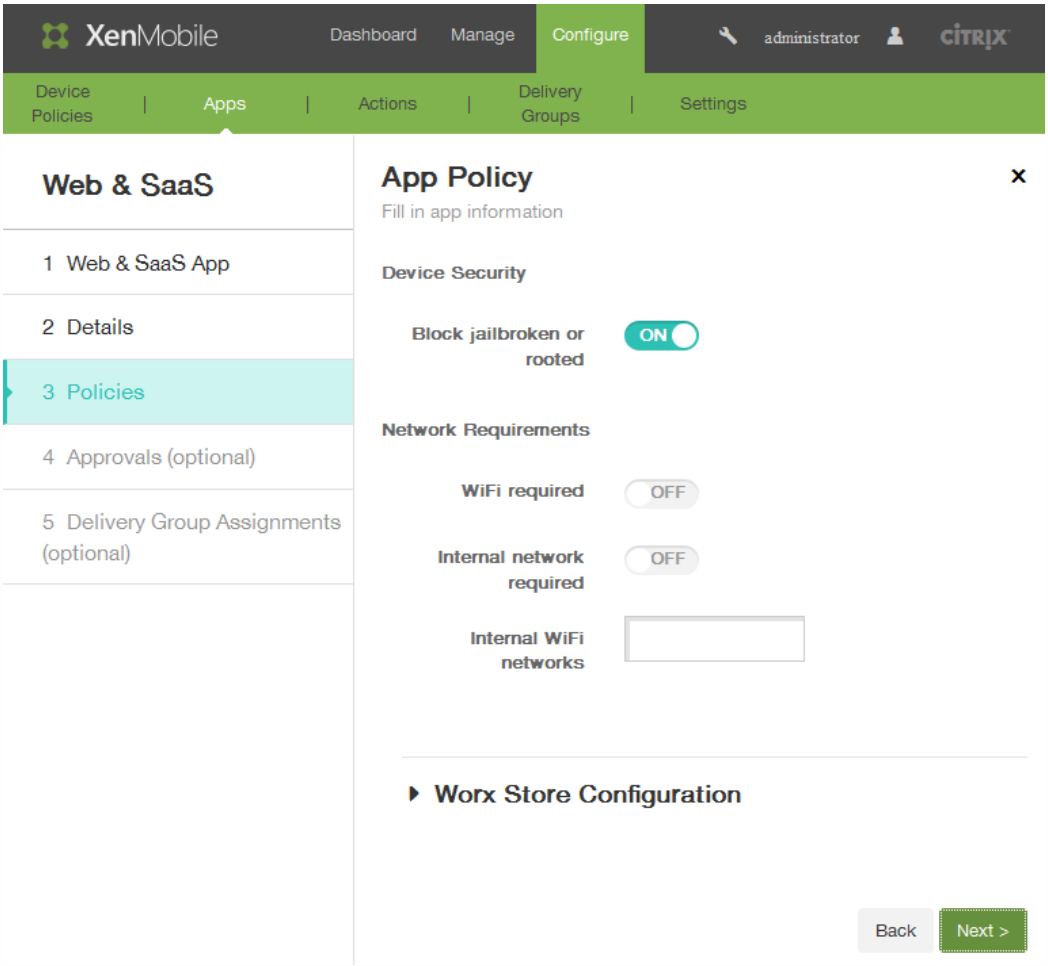
在 **XenMobile** 中添加应用程序连接器

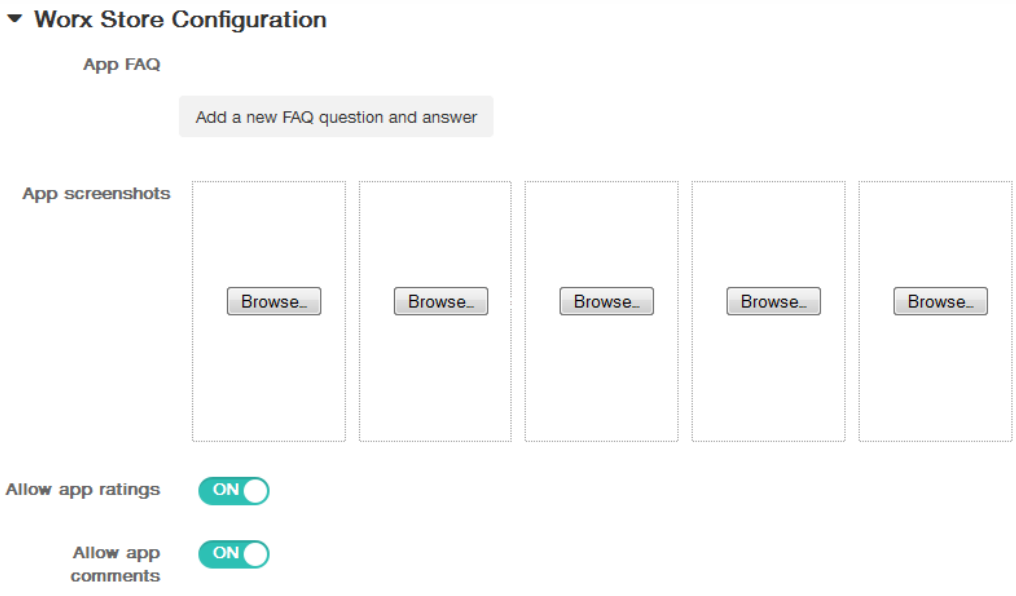


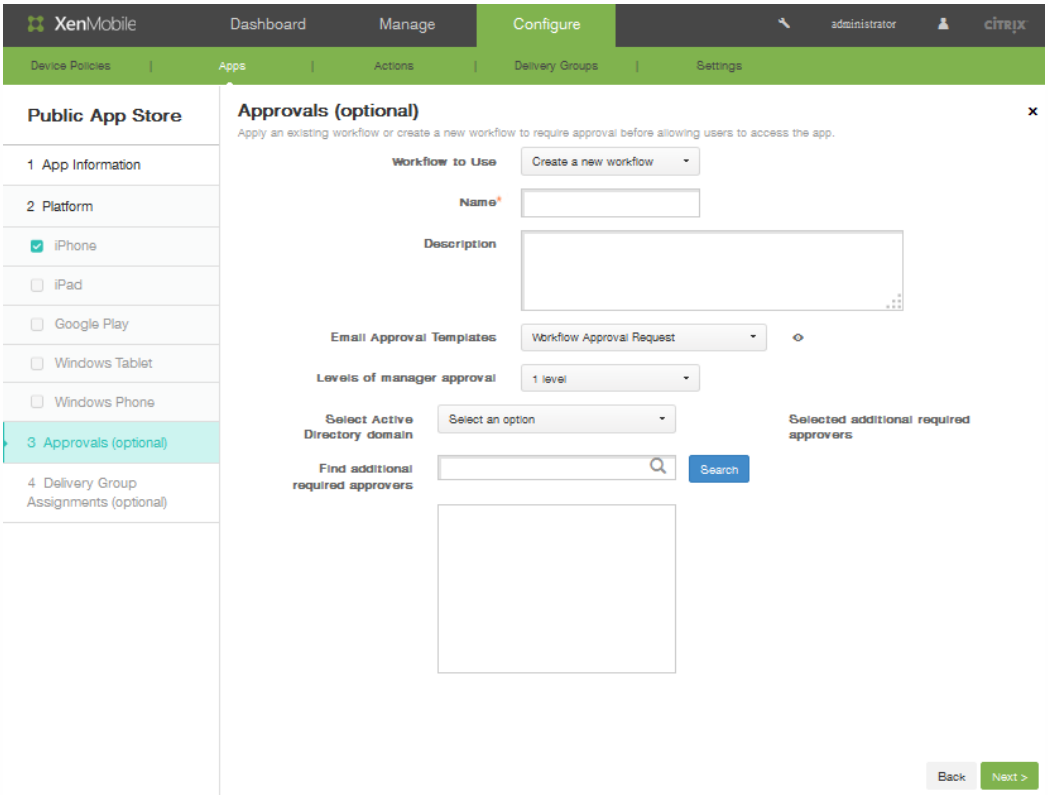


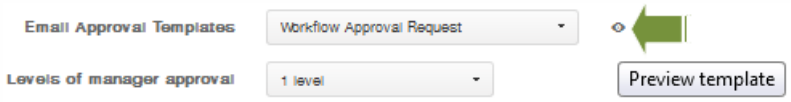


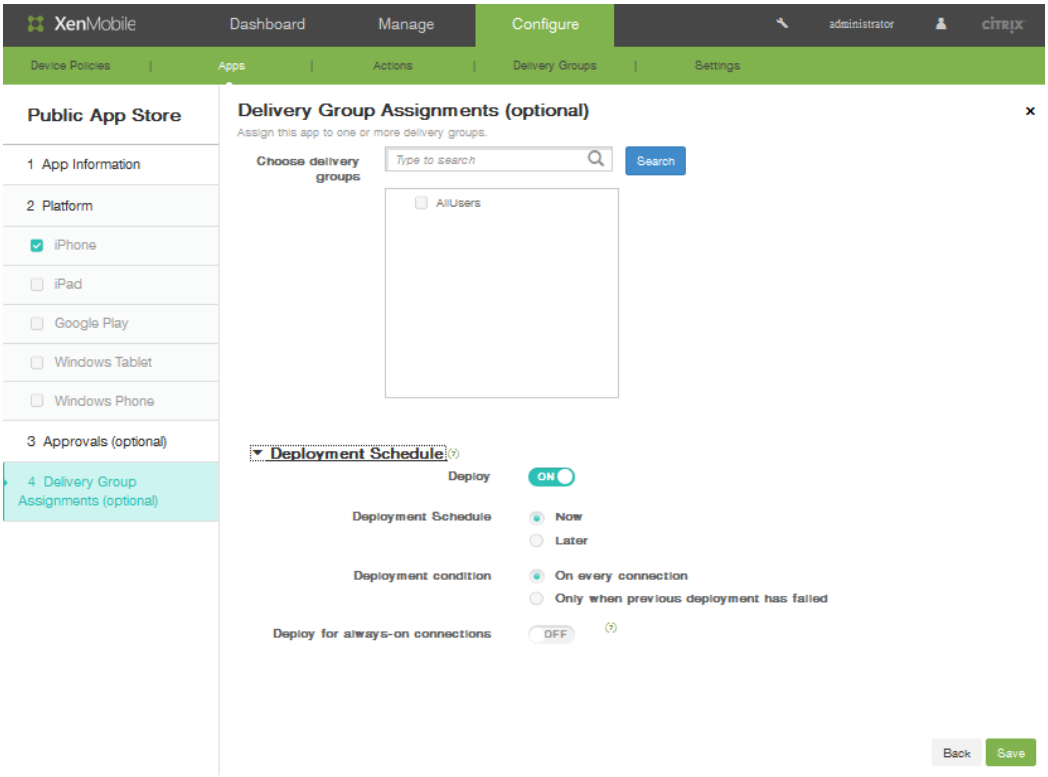


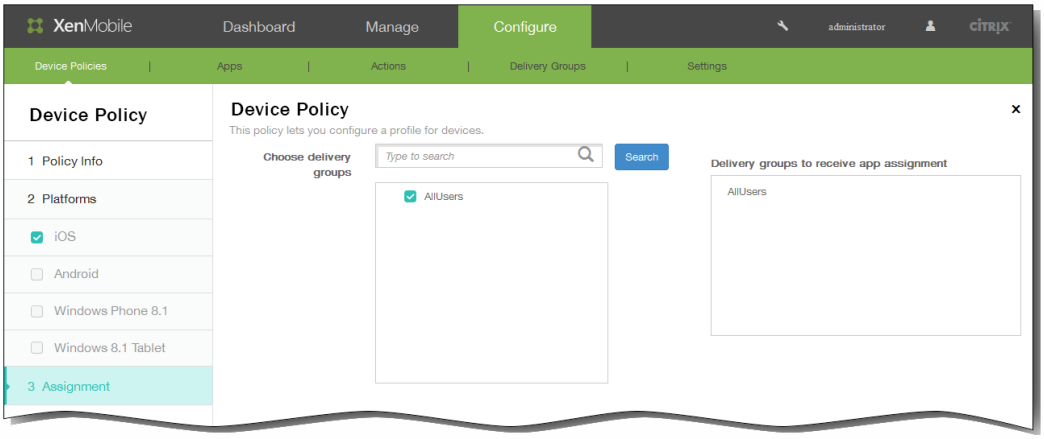


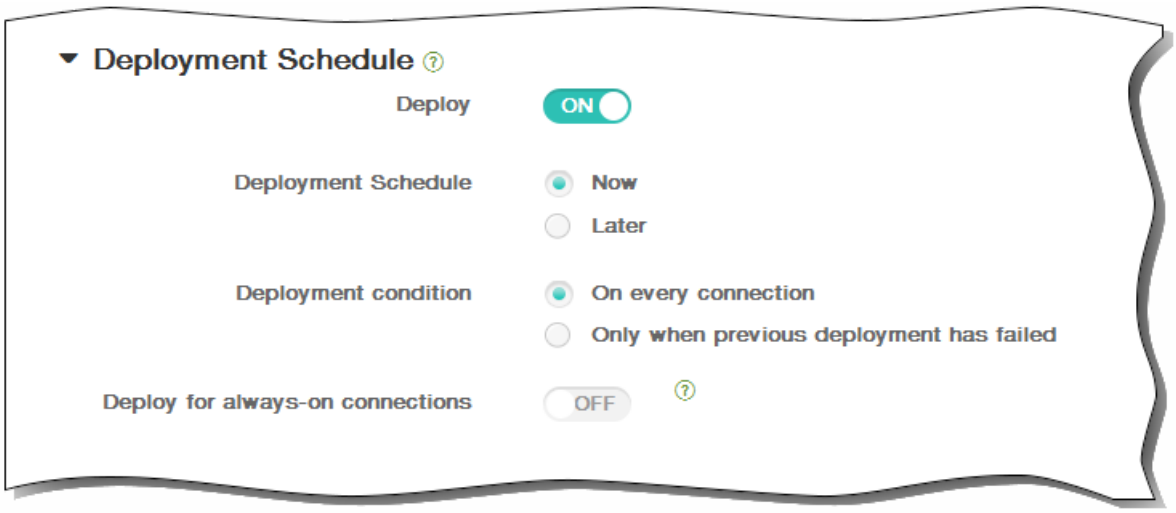






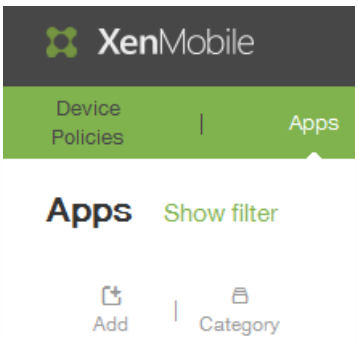


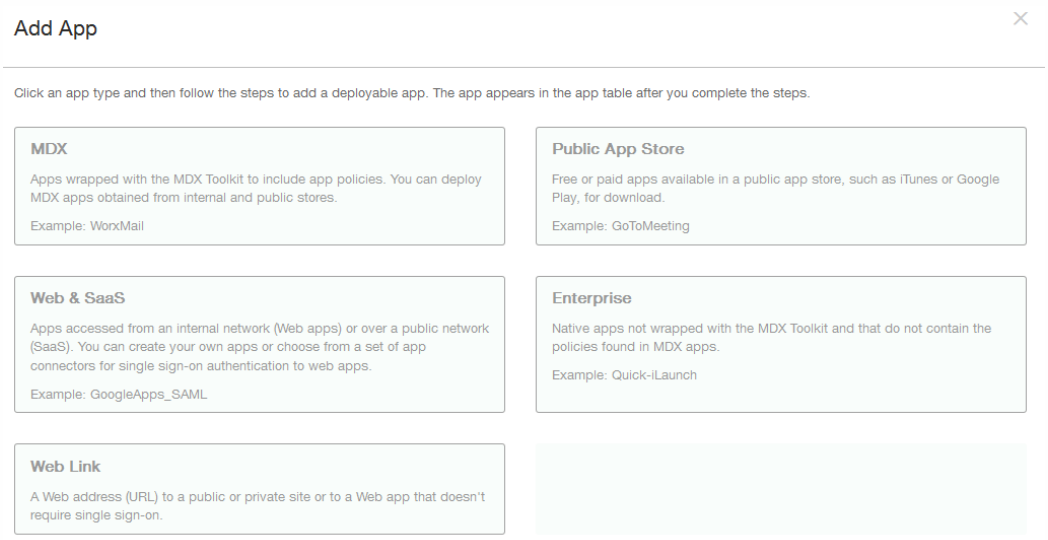


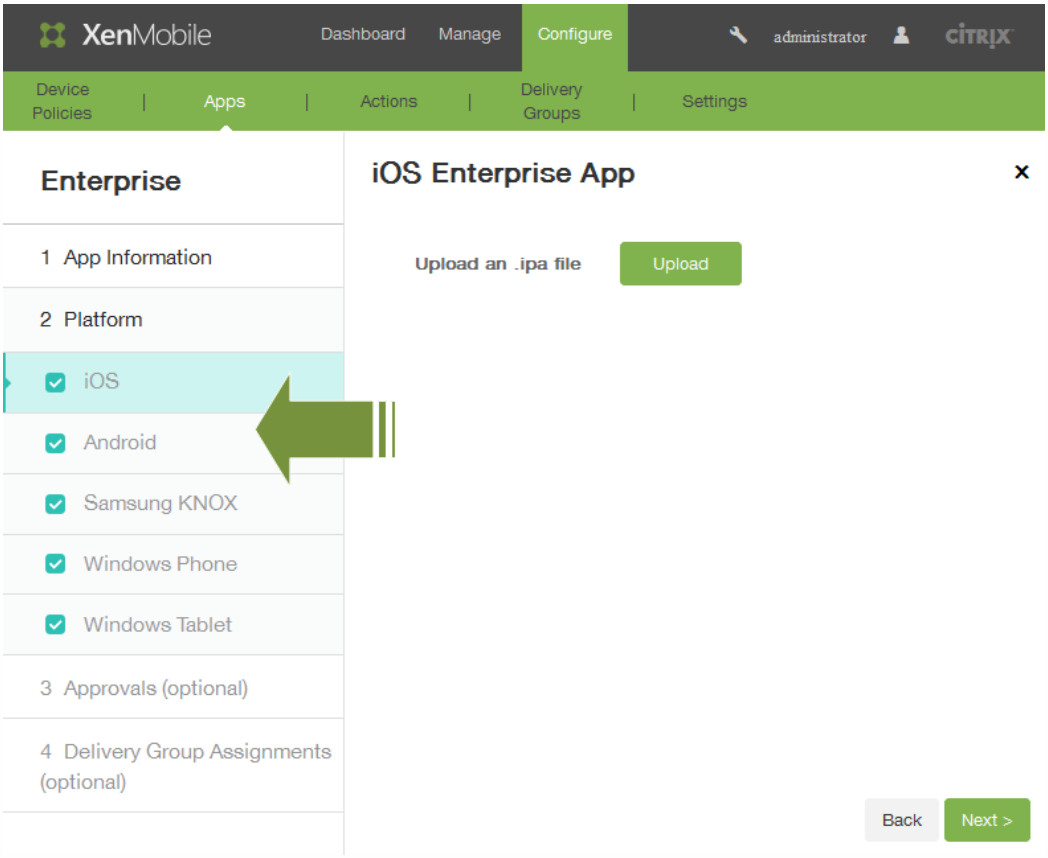


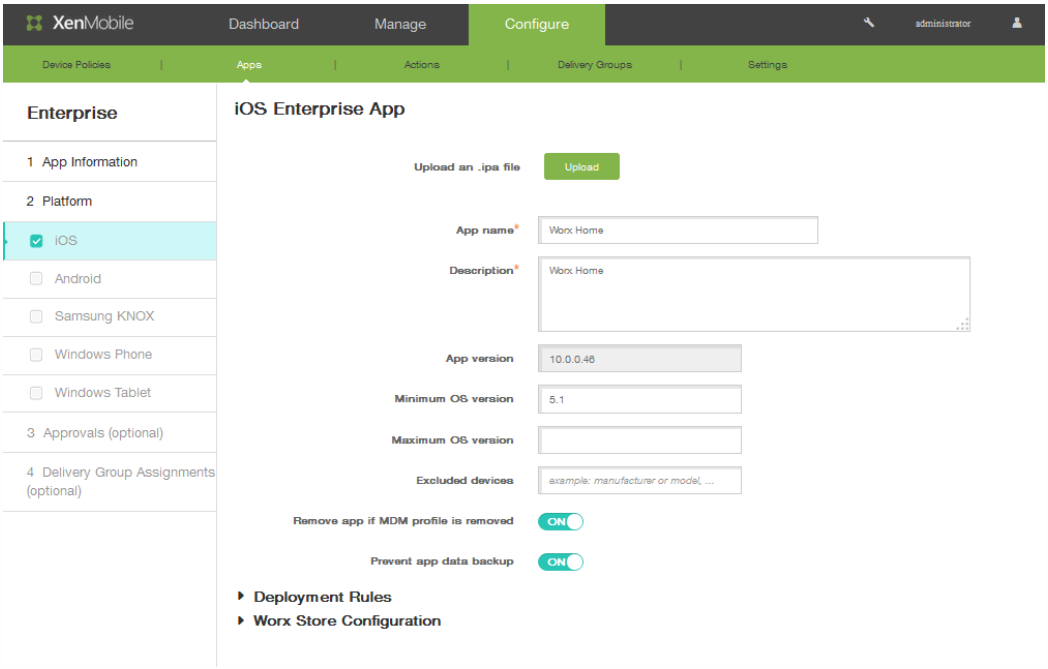
-
-
-
-
-

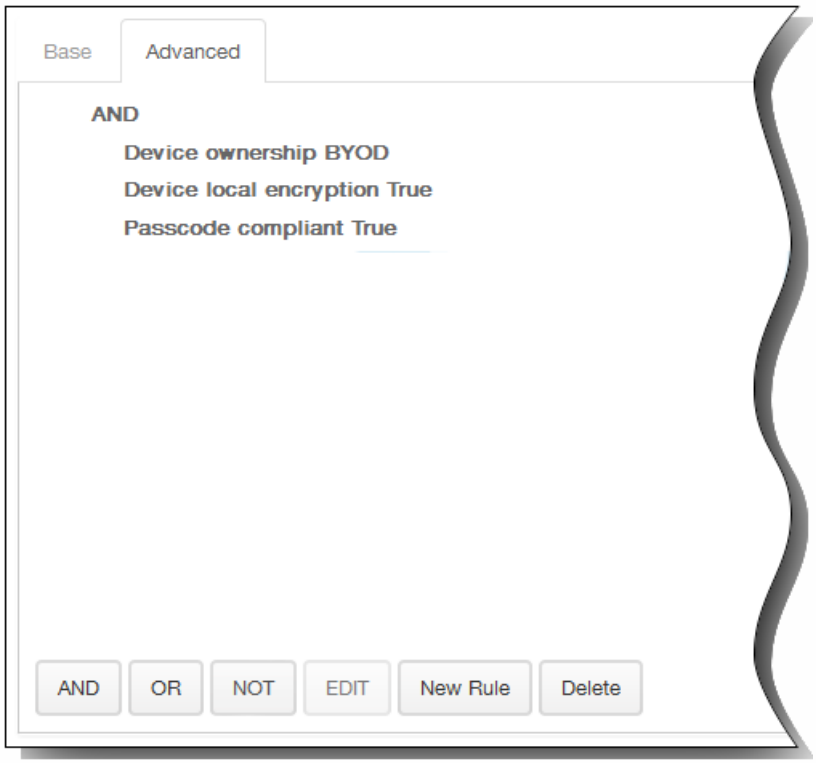
创建企业应用程序

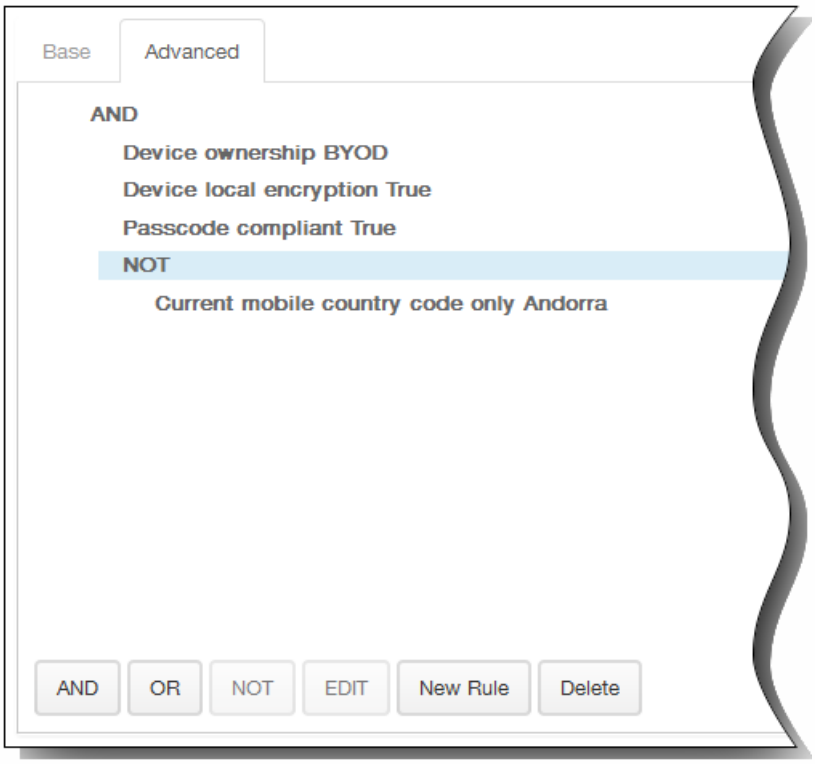


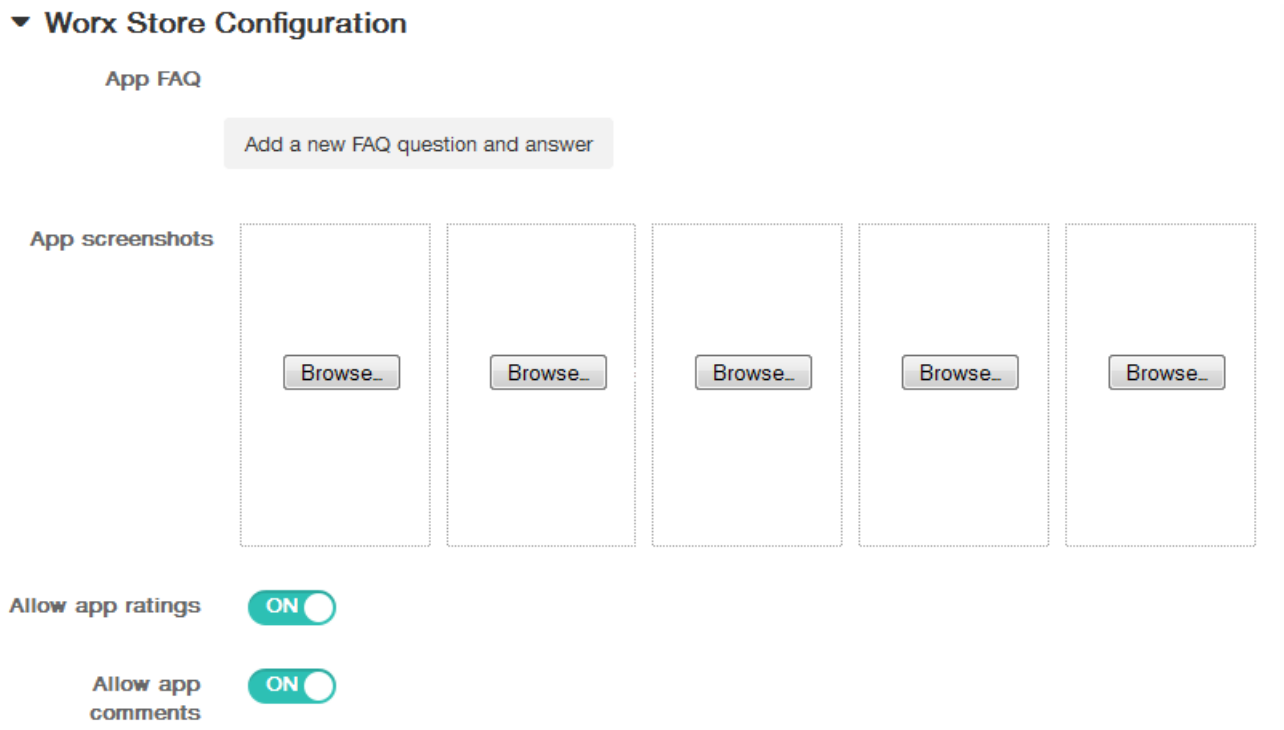


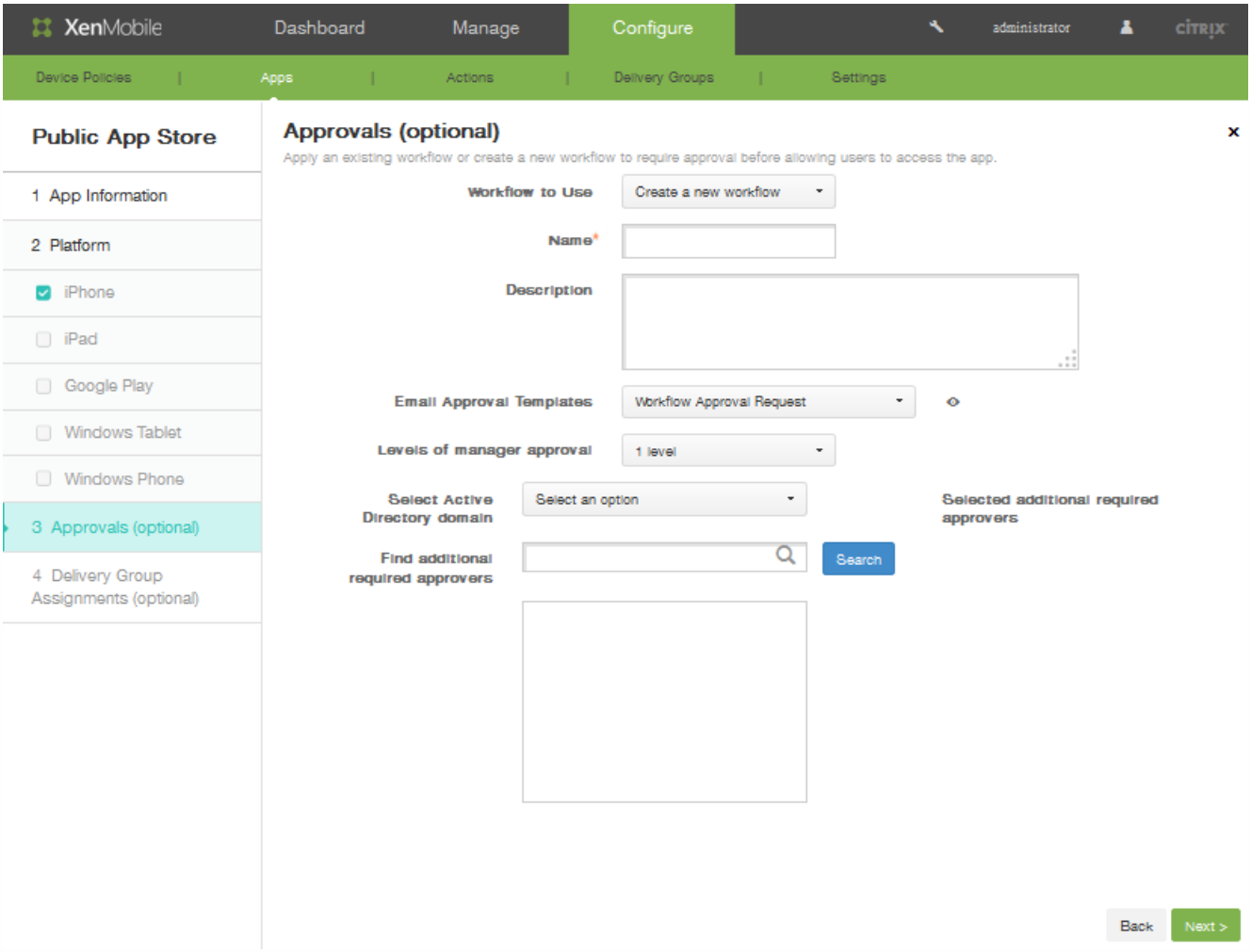


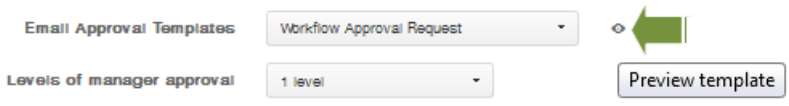


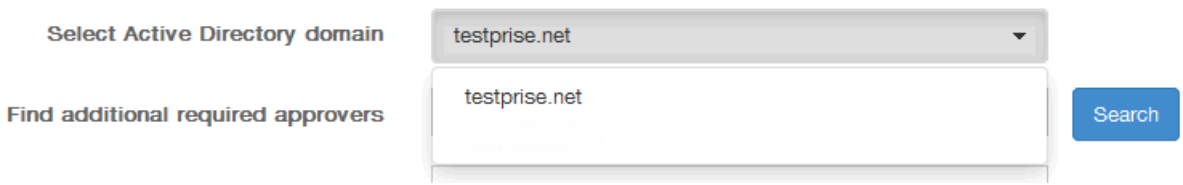


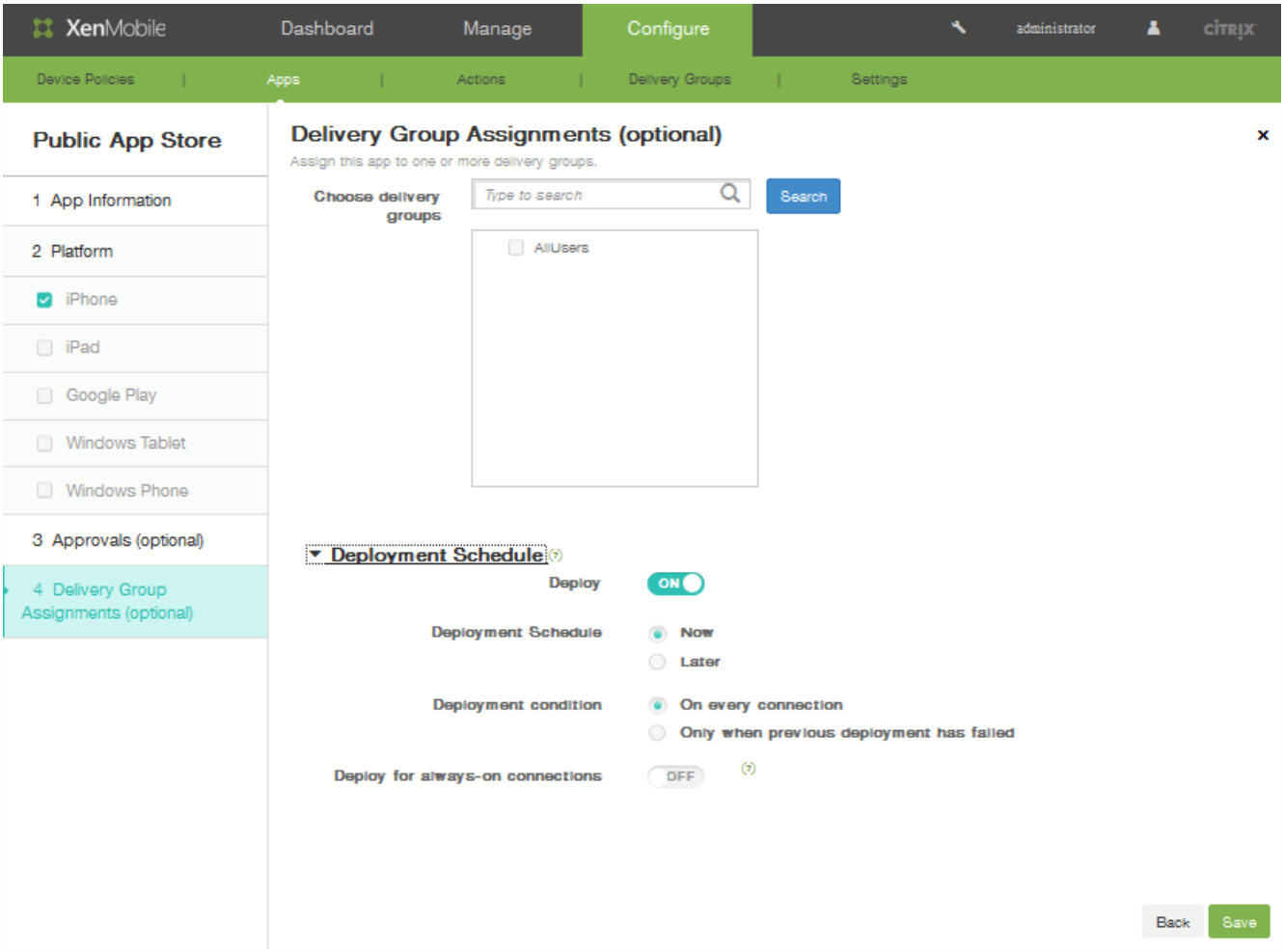




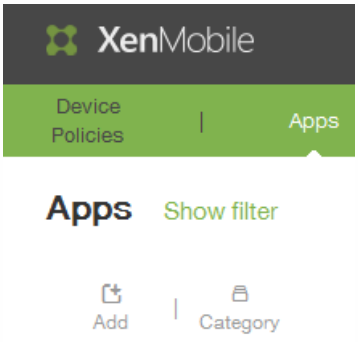


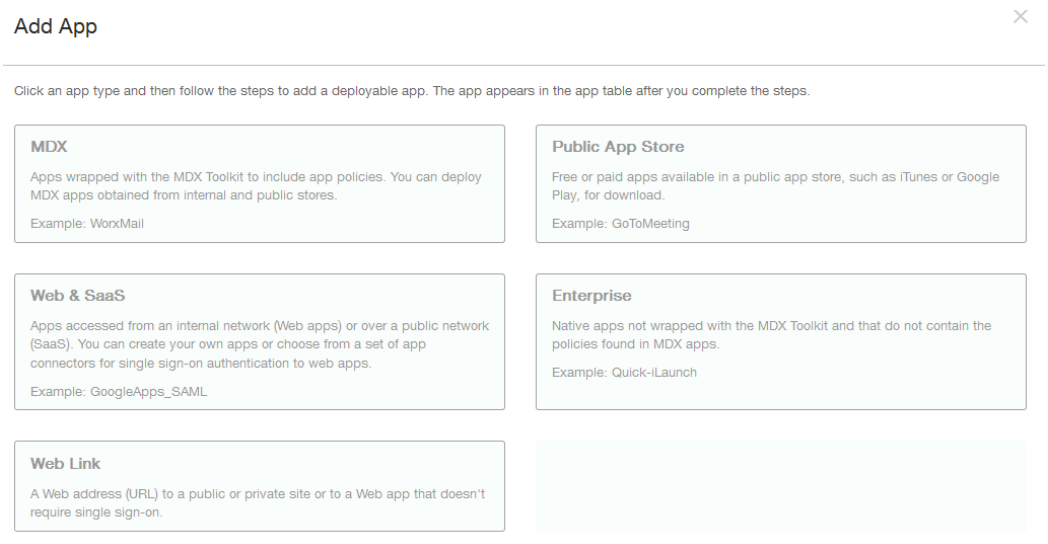


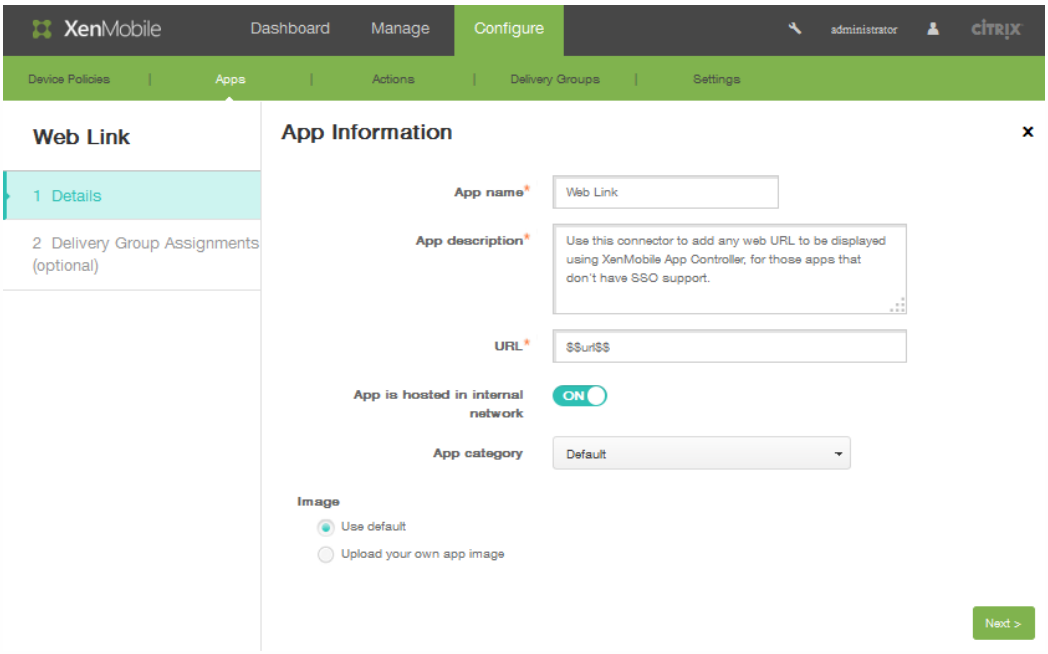


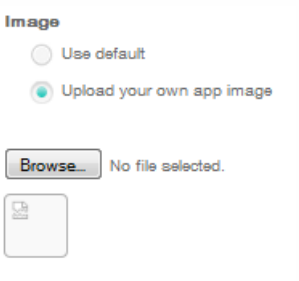


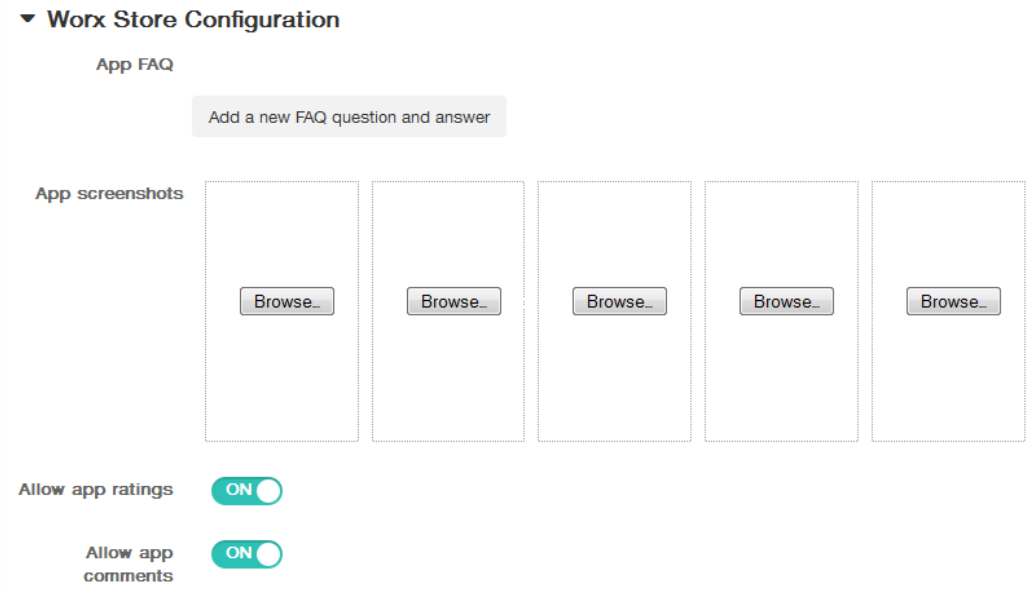
-
-
-
-
-
-

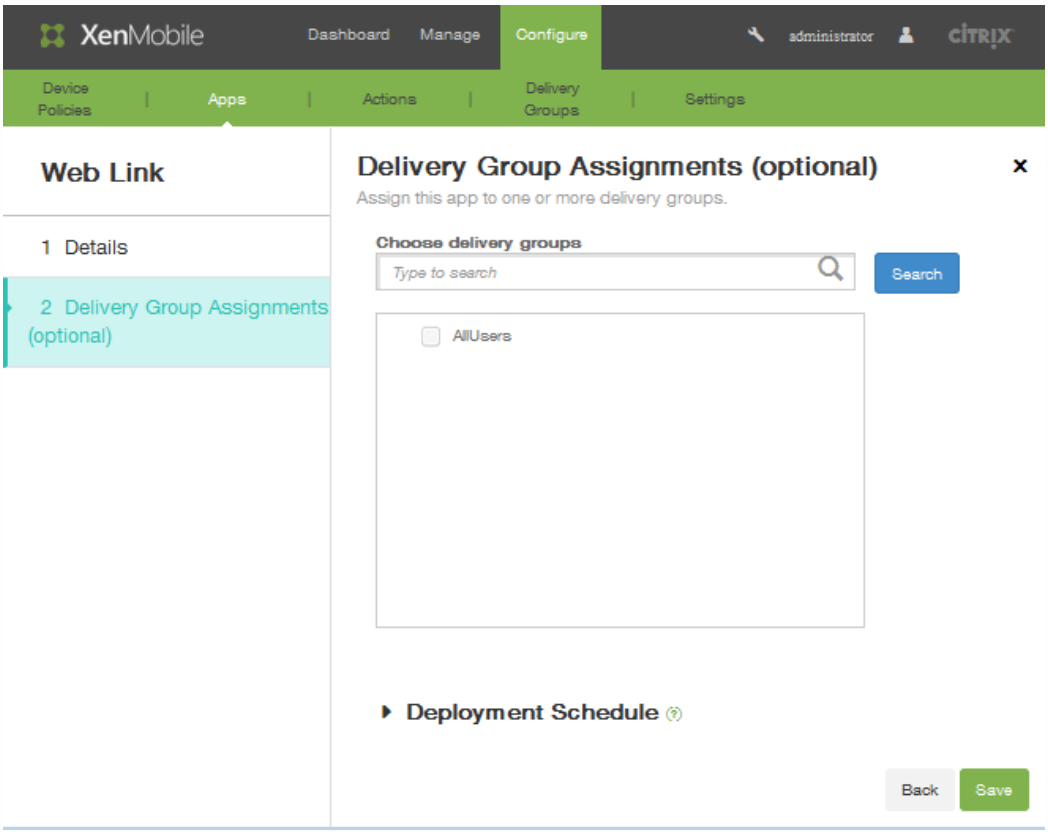


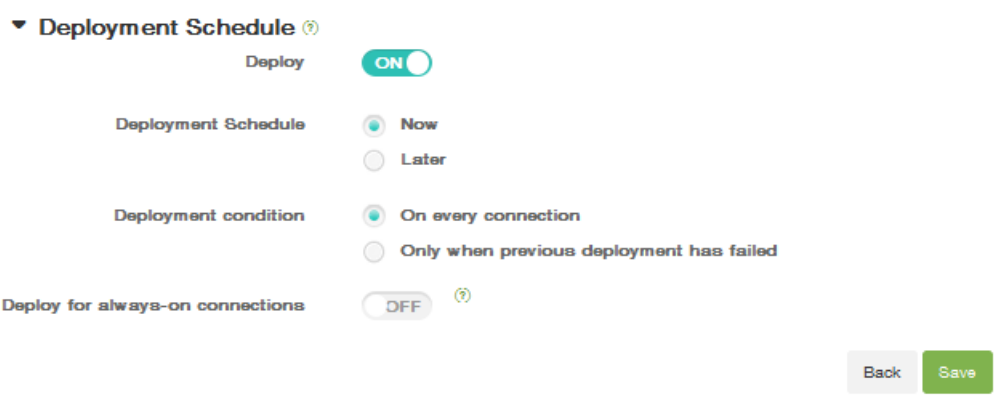




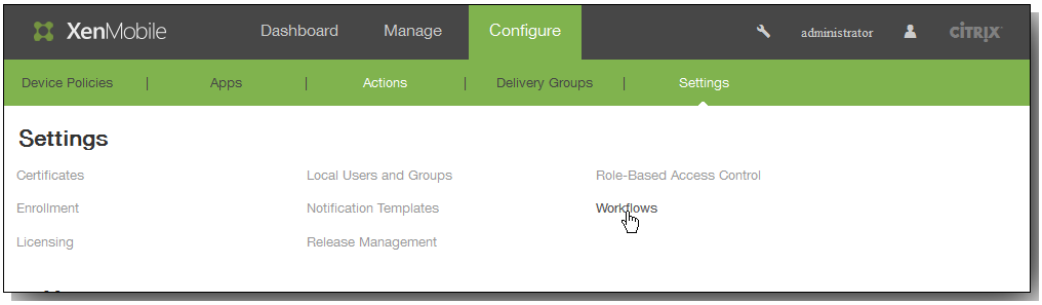


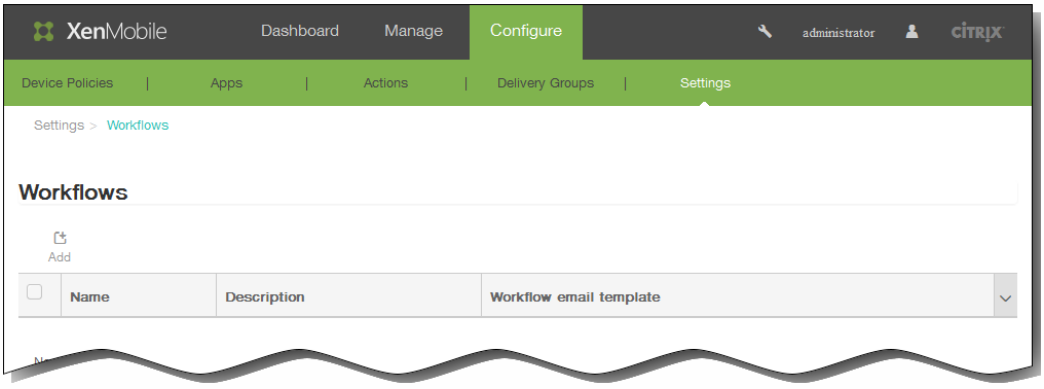


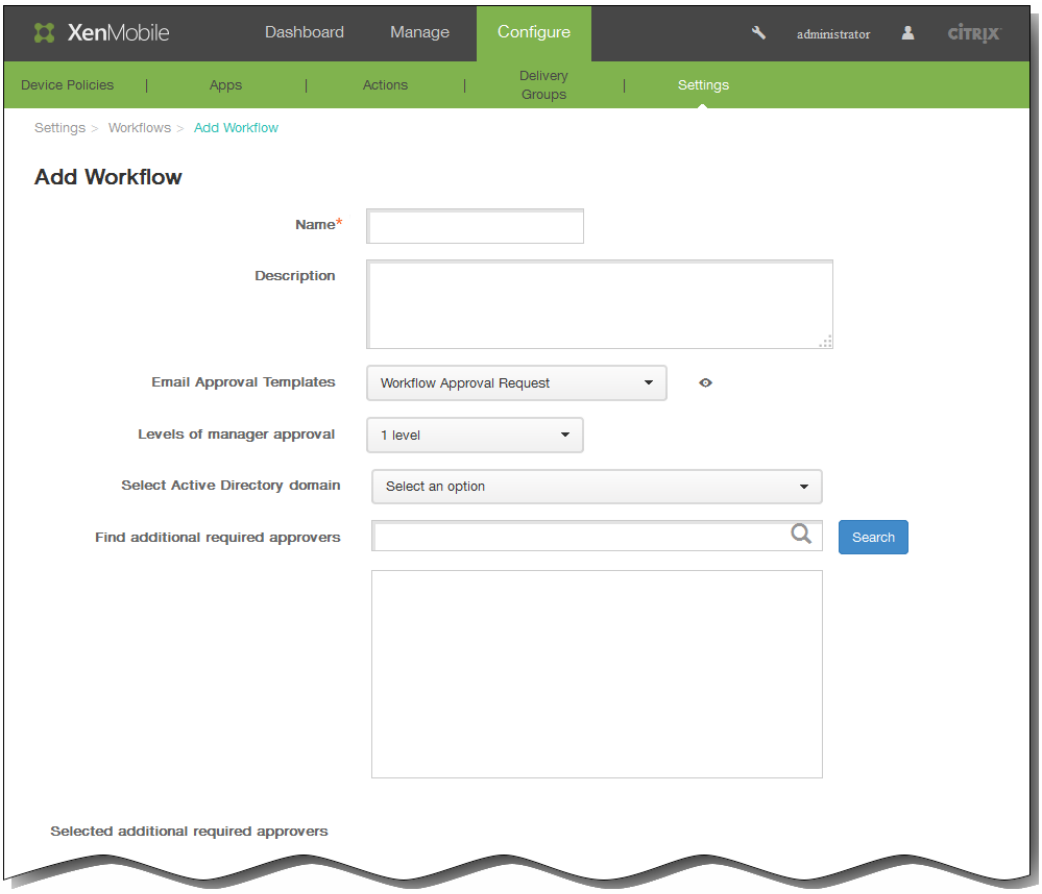


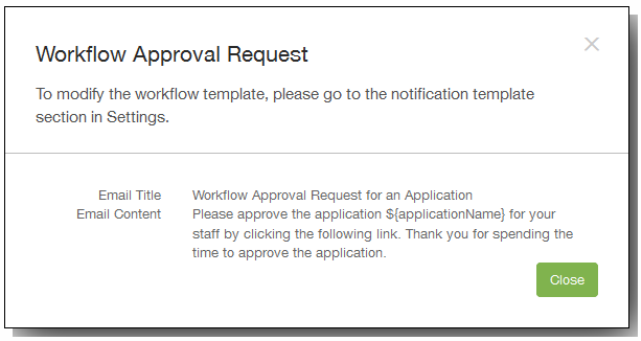


-
-



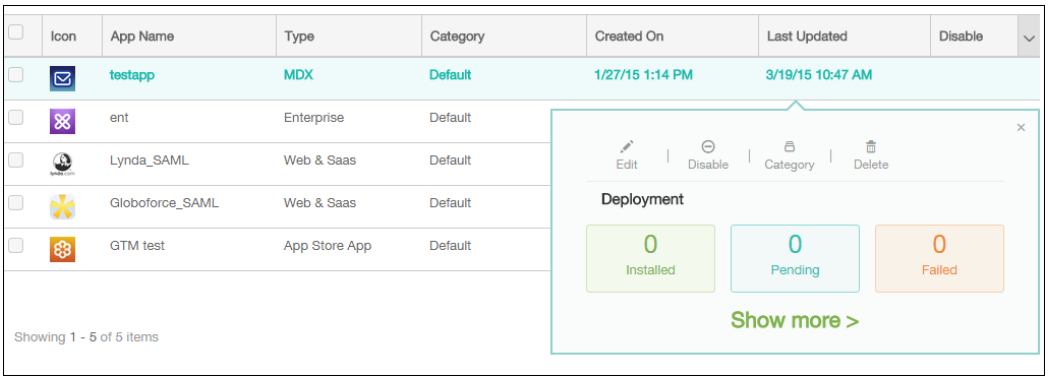


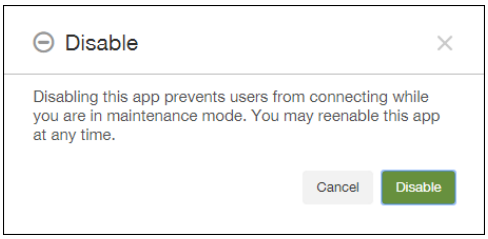


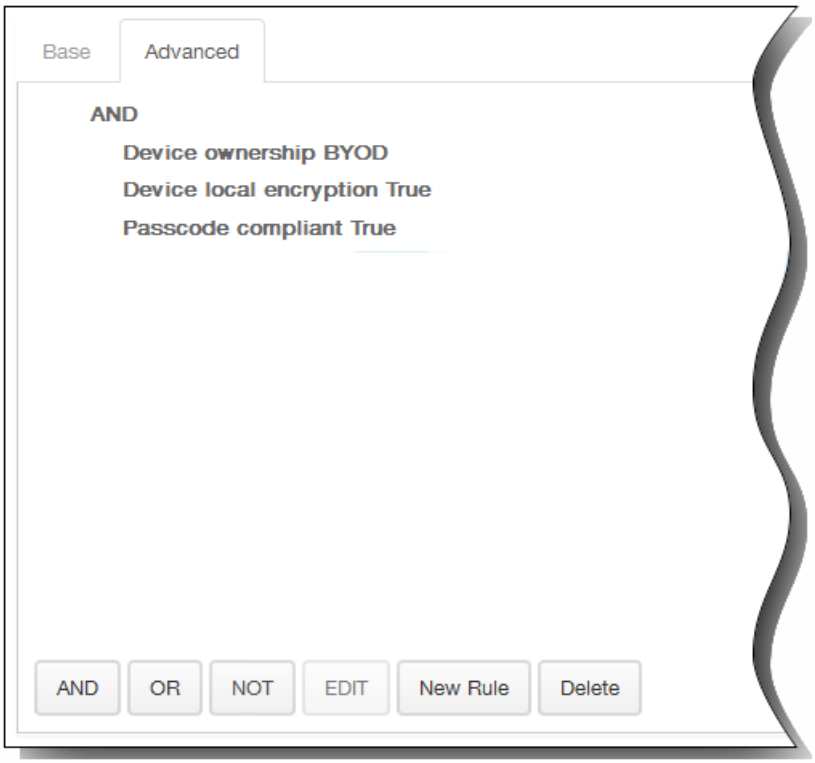


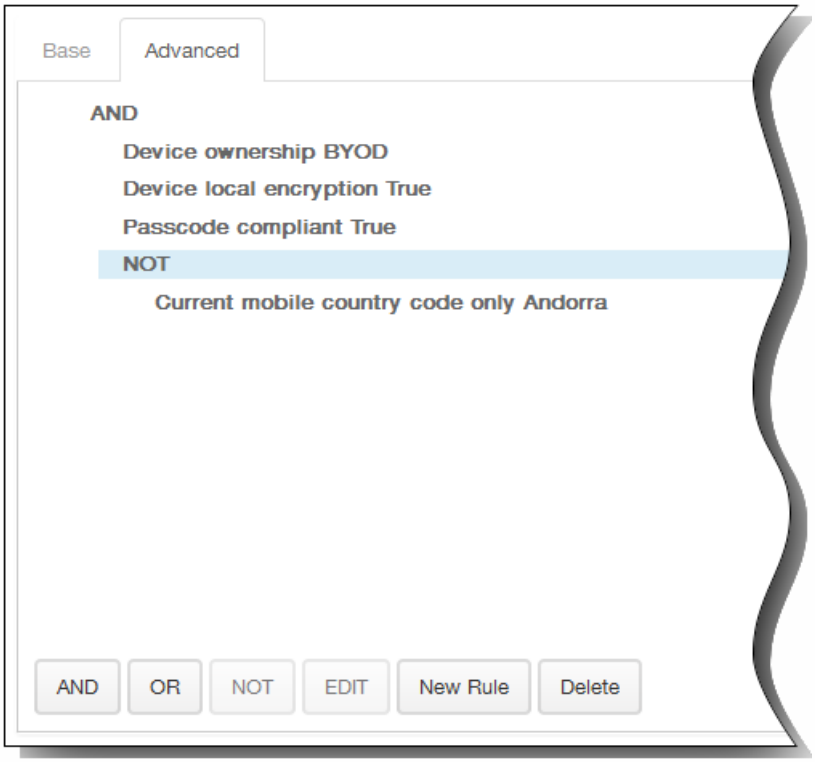
-

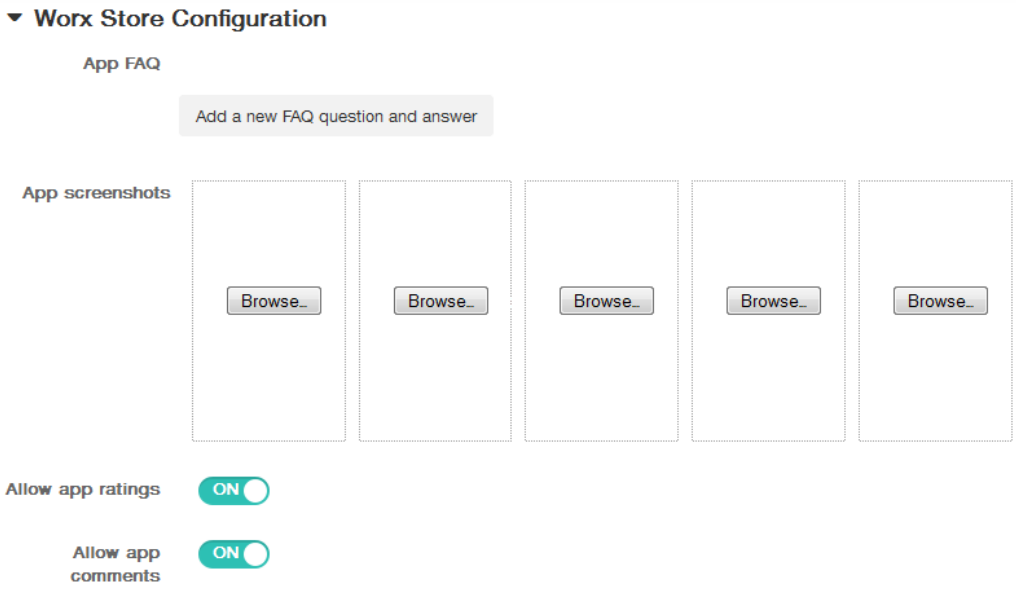
查看详细信息和删除工作流

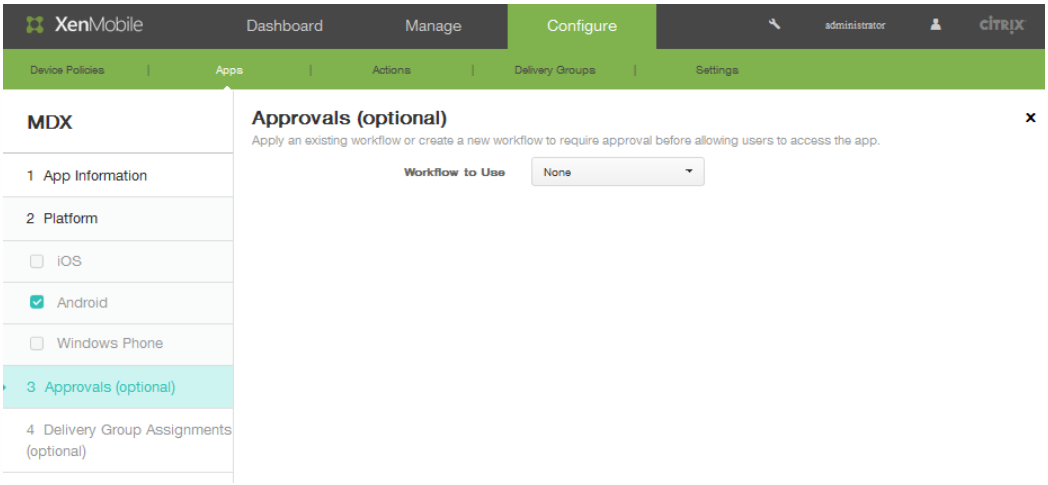


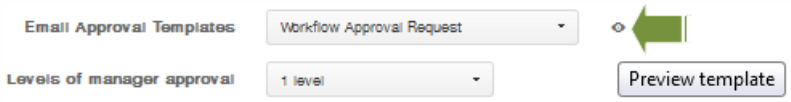


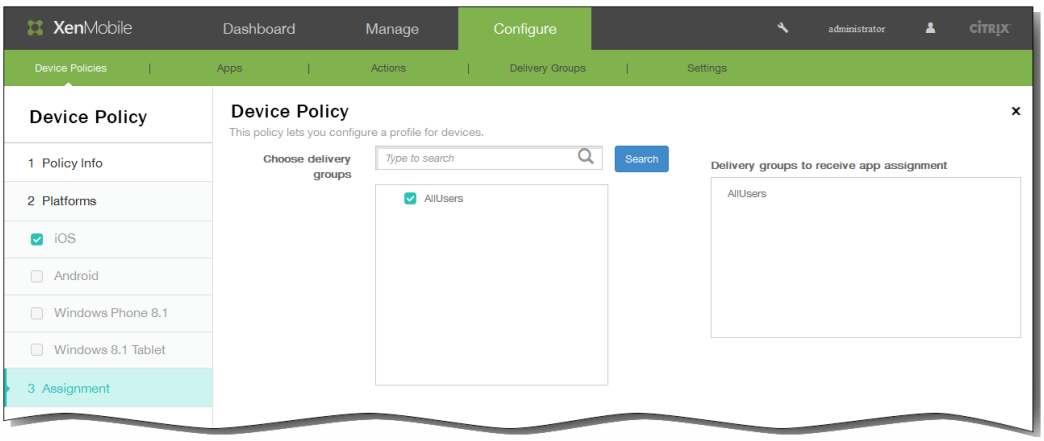


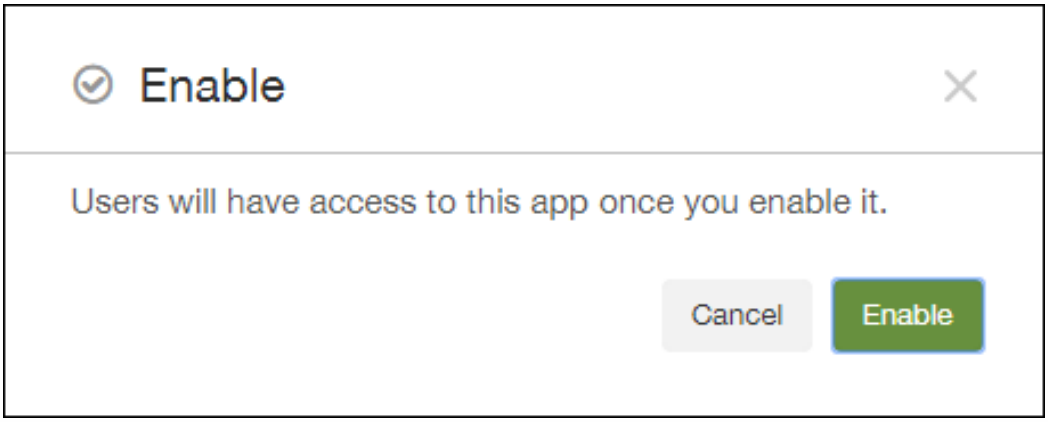




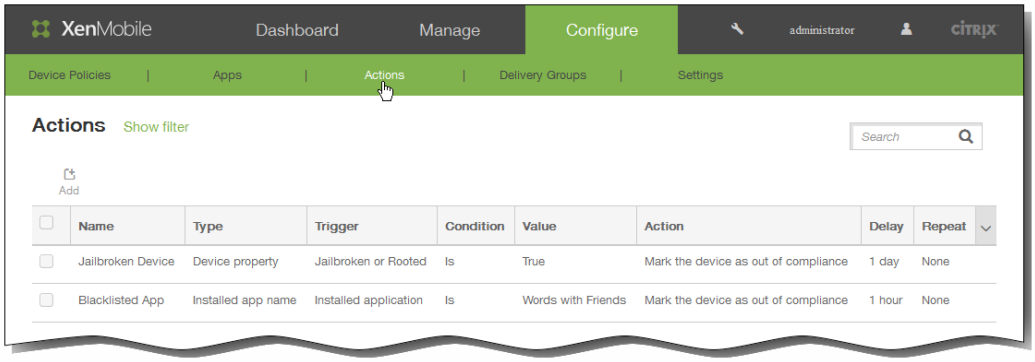




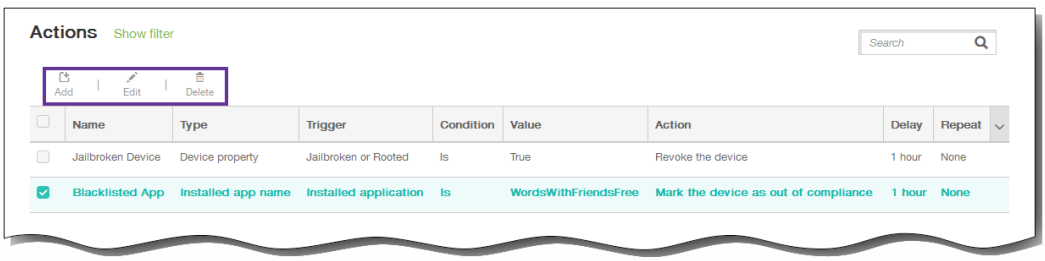


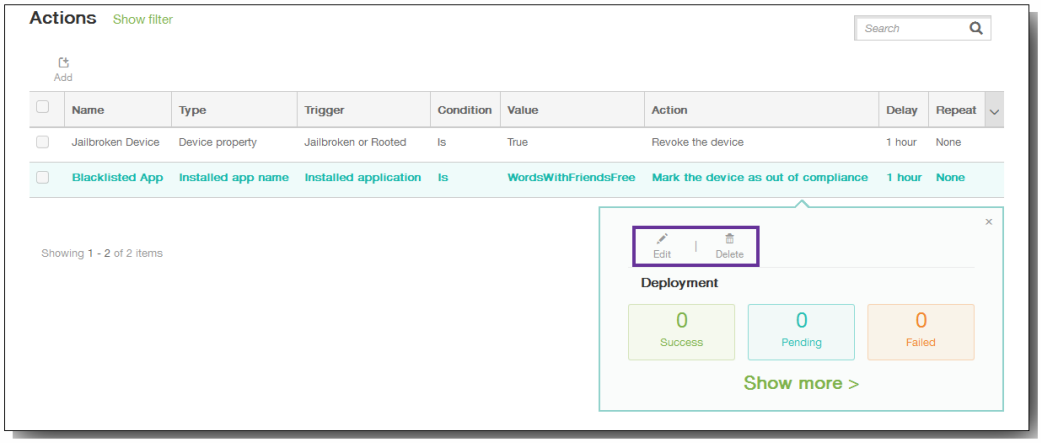


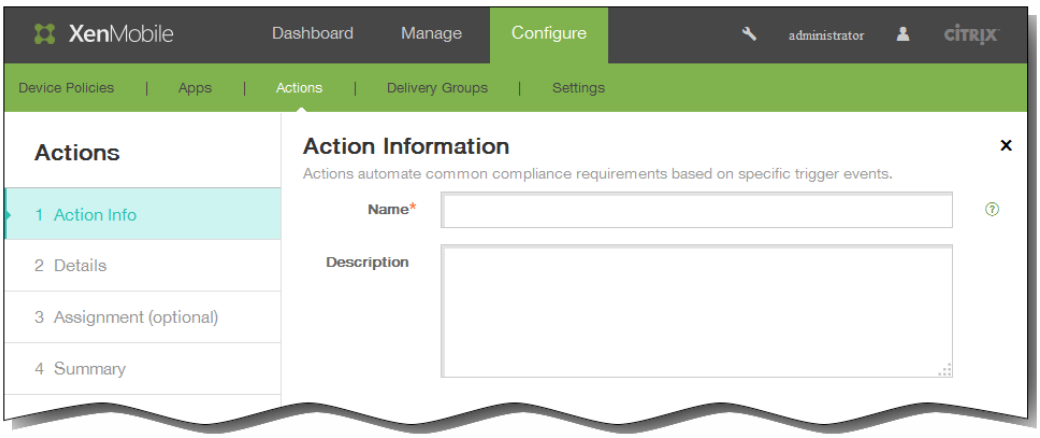
-
-
-
-

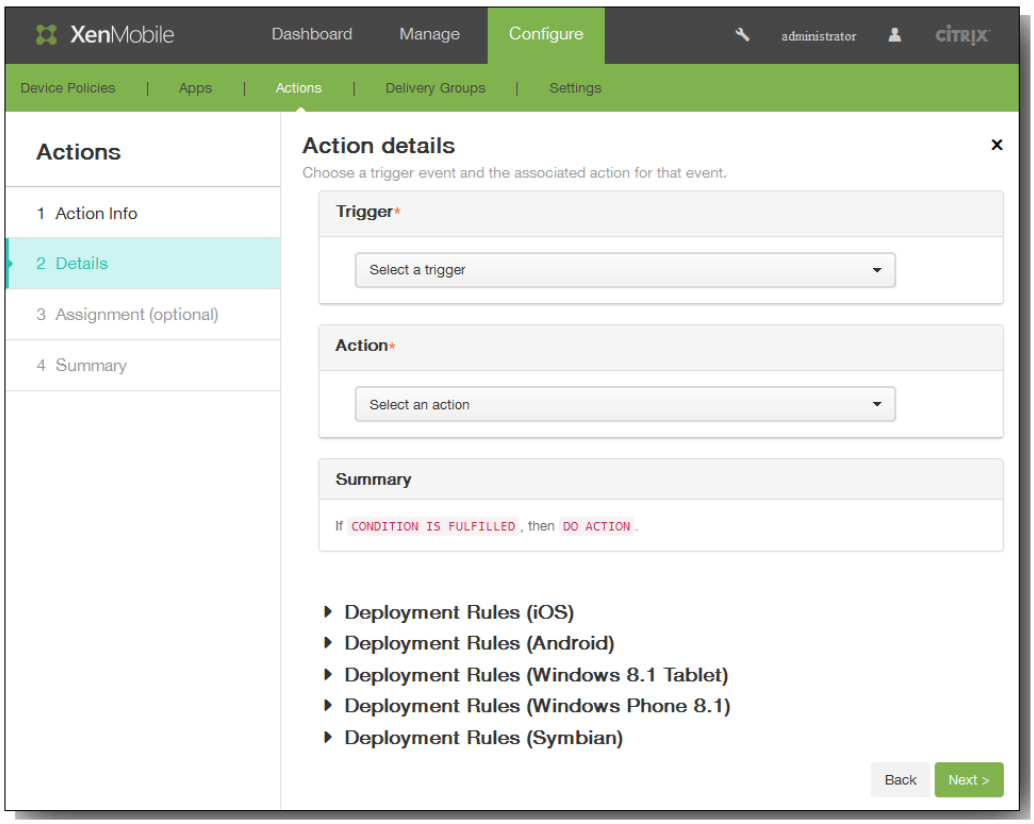


-
-

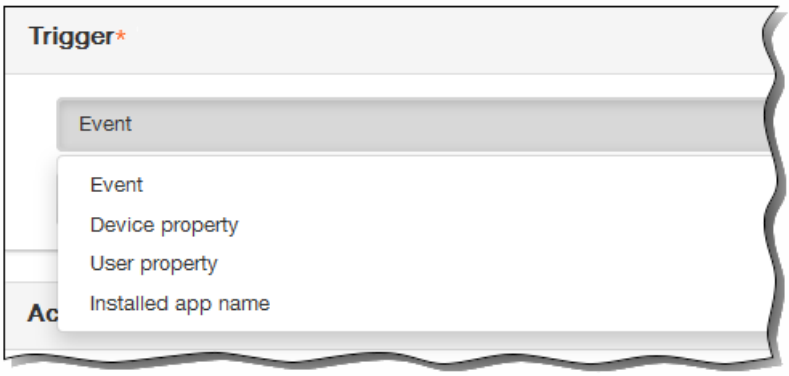


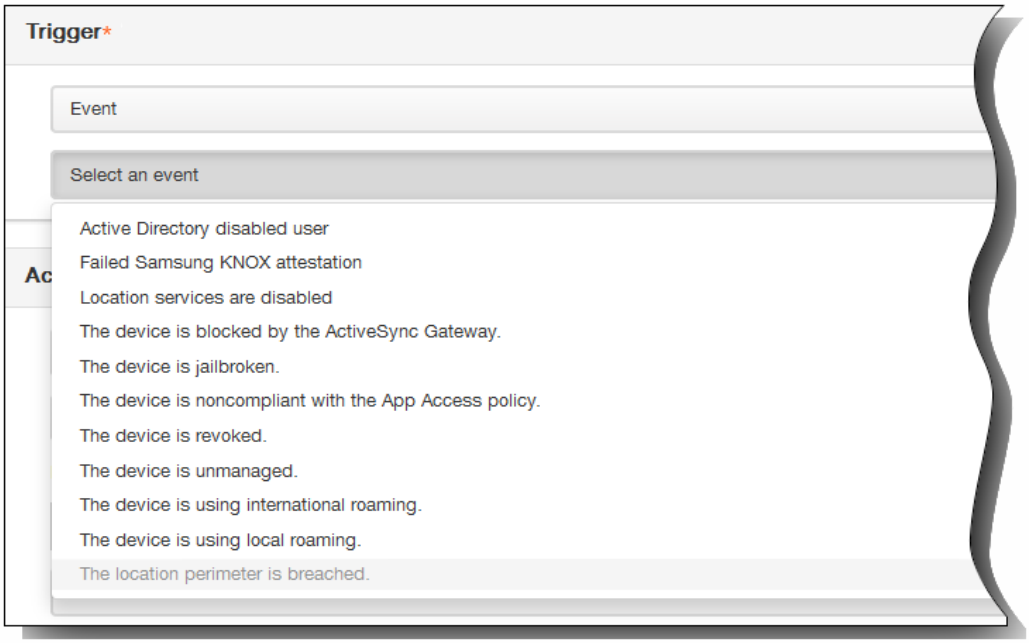


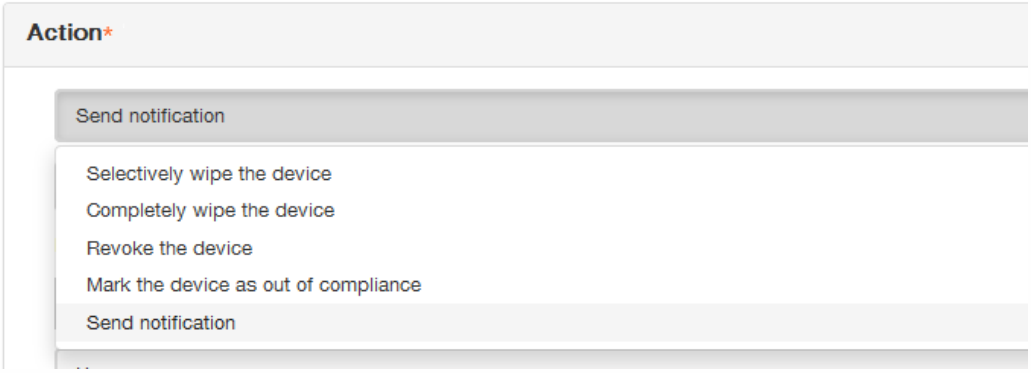


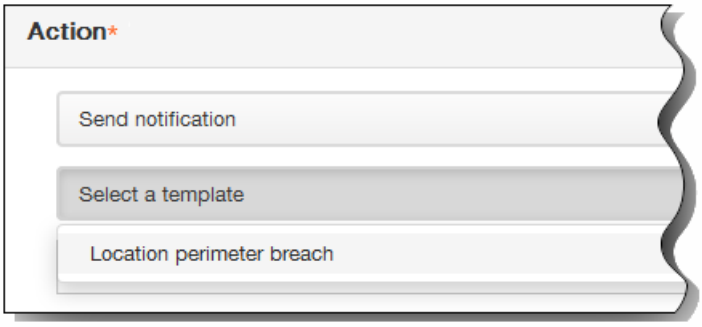


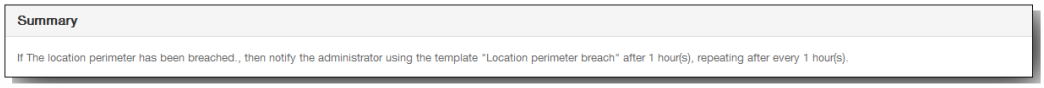
-
-
-
-

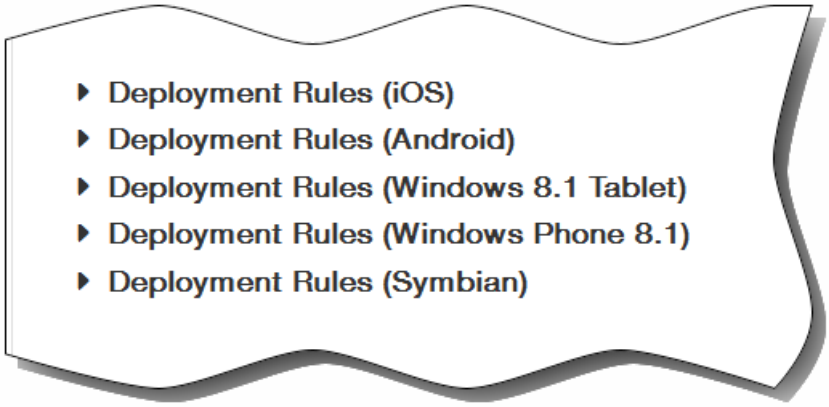


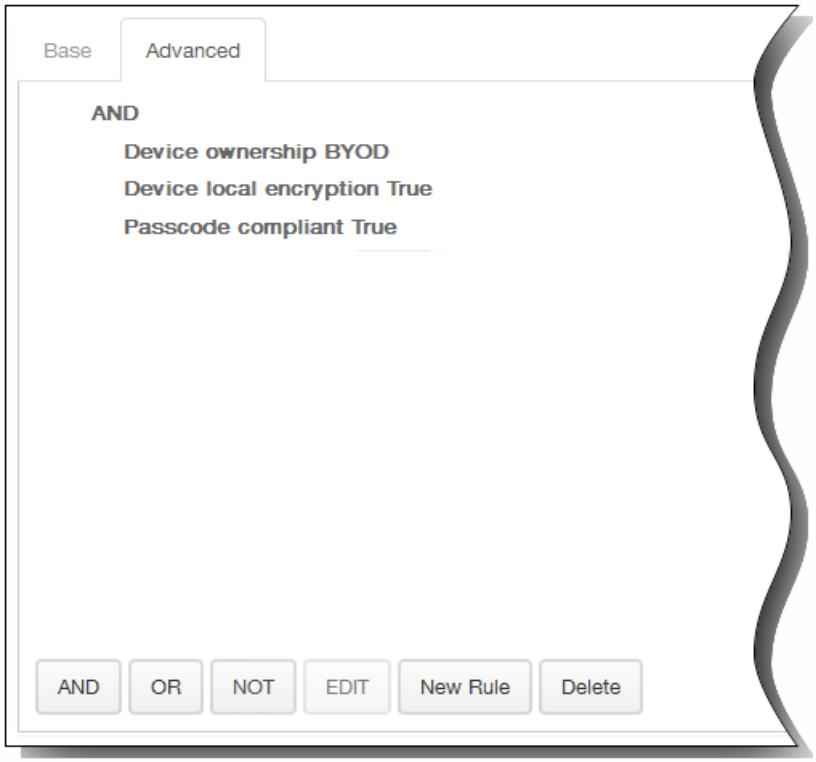


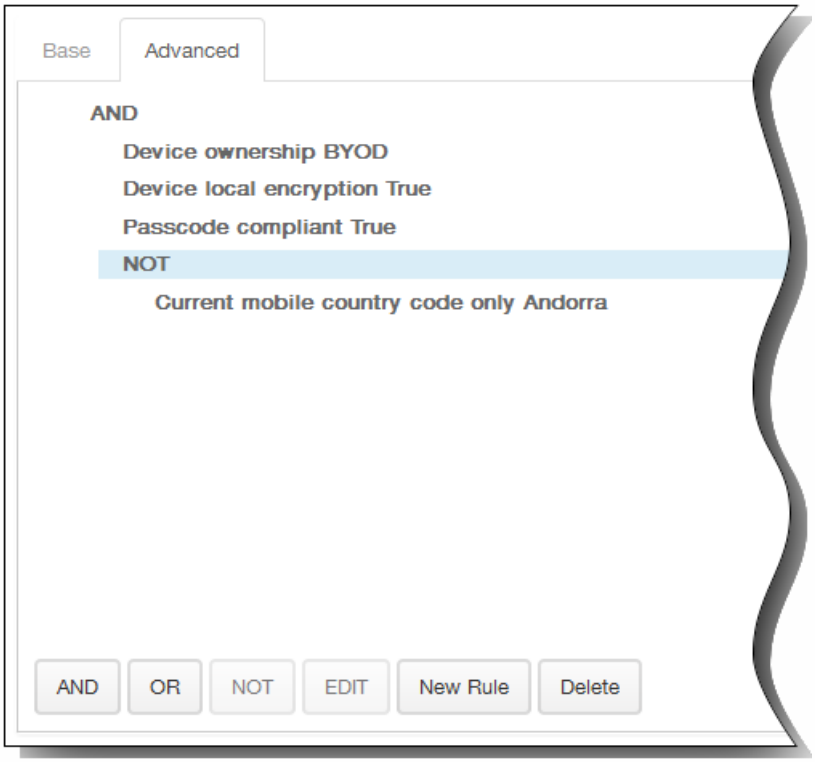


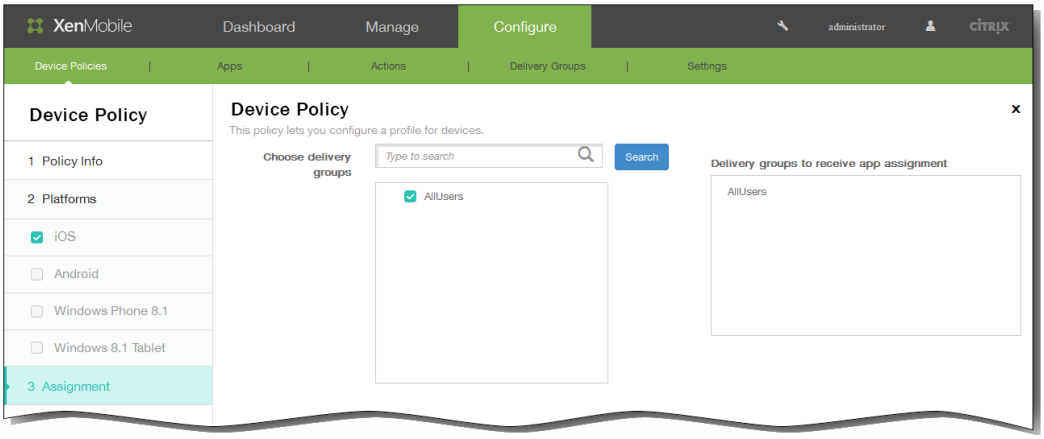


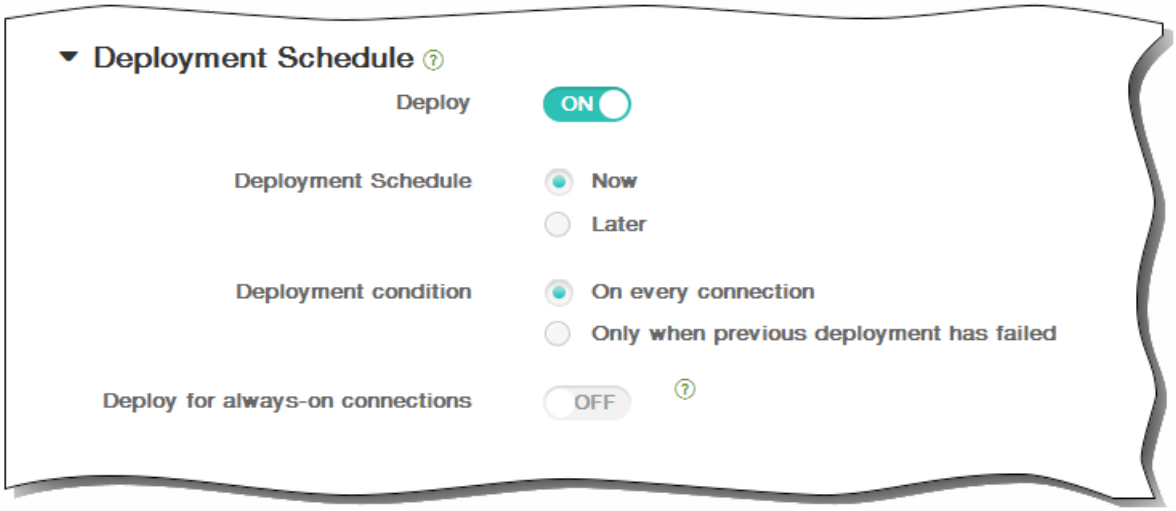


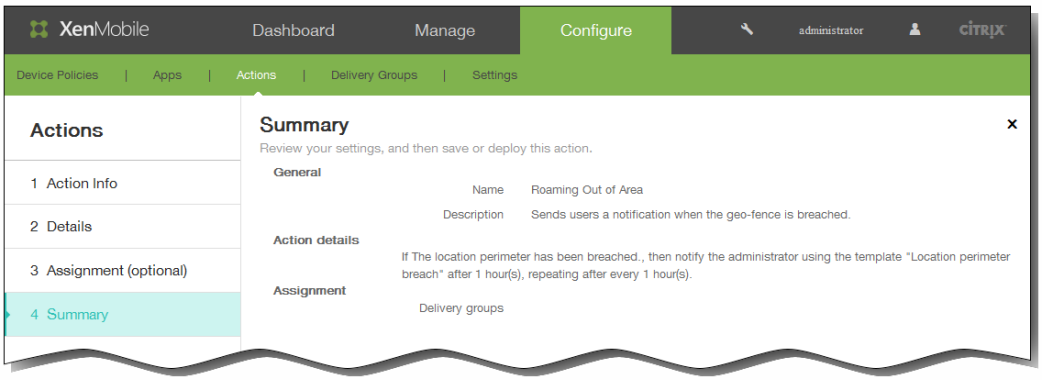












XenMobile 客户端设置

May 05, 2016

可以在 XenMobile Web 控制台中配置 XenMobile 客户端设置。

1. 在 XenMobile 控制台中，单击配置，然后单击设置。
   此时将显示设置页面。
2. 单击更多。
3. 在**客户端**下面，单击要配置的选项。

创建适用于 iOS 设备的自定义 Worx Store 品牌设计

May 05, 2016

可以为 Worx Store 创建自定义的应用商店名称和默认应用商店视图。可以在运行 Receiver for iPhone 或 Receiver for iPad 的设备上添加在 Worx Store 或 Worx Home 上显示的自定义徽标。

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。

- 文件名必须采用 .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) + 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，单击配置 > 设置 > 更多 > Worx Store 外观方案。
2. 在默认应用商店视图旁边，选择类别或 A-Z。
3. 在设备选项旁边，选择电话或平板电脑。
4. 在外观方案文件旁边，单击浏览以选择用于外观方案的图像或图像的 .zip 文件，然后单击保存。

要将此软件包部署到用户的 iOS 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。

创建 Worx Home 和 GoToAssist 支持选项

May 05, 2016

1. 在 XenMobile 控制台中，单击配置 > 设置 > 更多 > Worx Home 支持。
2. 在 Worx Home 支持页面上，键入以下字段的值：
    1. 支持电子邮件(IT 技术支持)
    2. 支持电话(IT 技术支持)
    3. GoToAssist 聊天令牌
    4. GoToAssist 支持票证电子邮件

您创建的 Worx Home 支持信息显示在 XenMobile 控制台的客户端属性列表中，与以下键关联：SUPPORT_EMAIL、SUPPORT_PHONE、GTA_CHAT 和 GTA_TICKET。

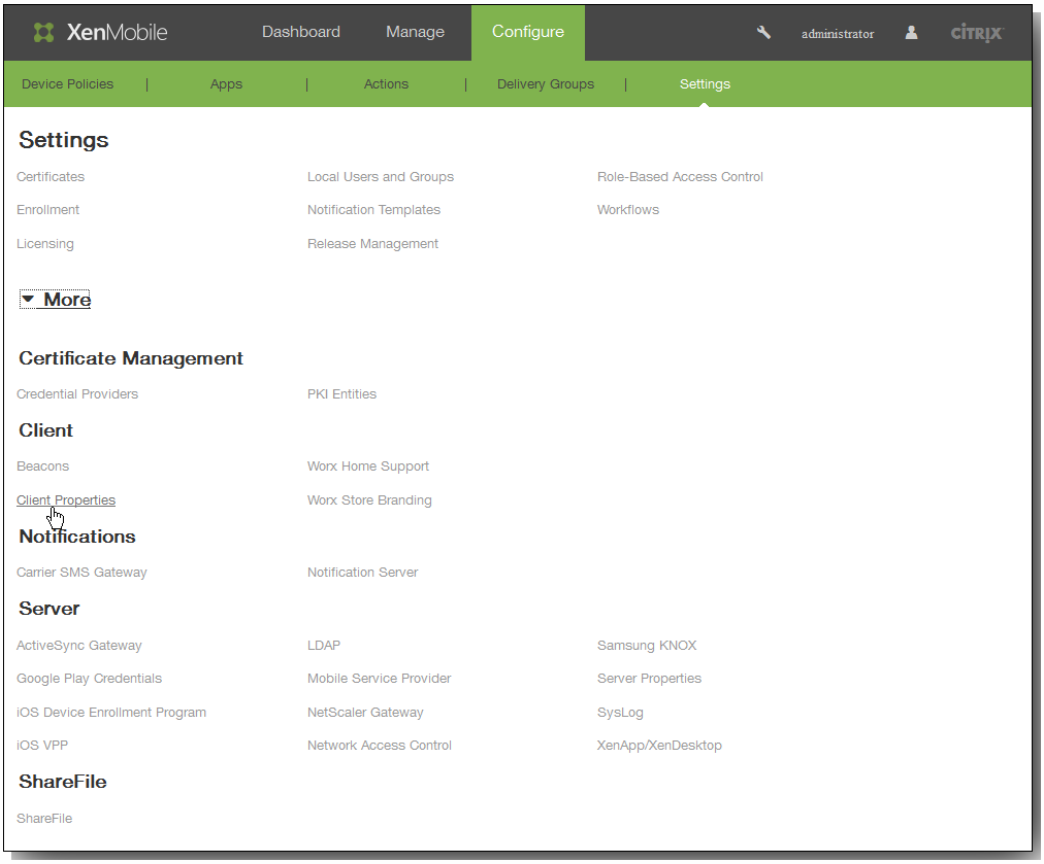
添加、编辑或删除客户端属性

May 05, 2016

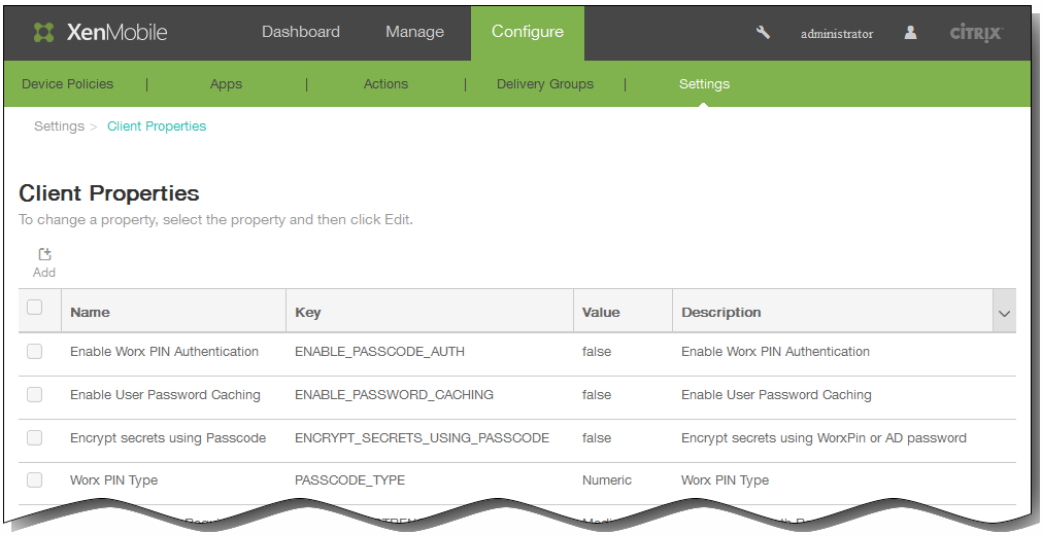
客户端属性包含用户设备上直接提供给 Worx Home 的信息。这些属性用于配置高级设置，如 Worx PIN。从 Citrix 技术支持获取客户端属性。

注意：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。

1. 在 XenMobile 控制台中，单击配置 > 设置 > 更多 > 客户端属性。

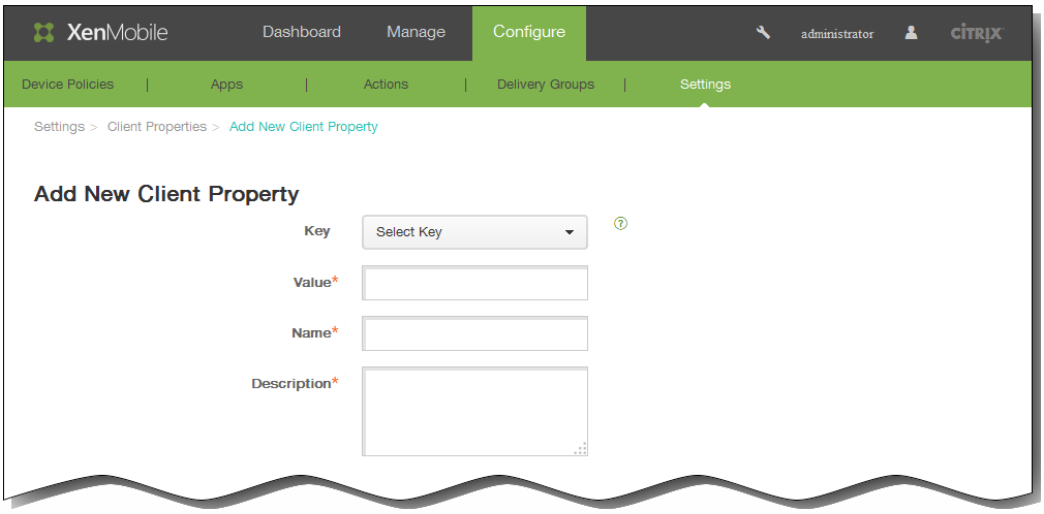


此时将显示客户端属性页面。可以从此页面添加、编辑和删除客户端属性。



添加客户端属性

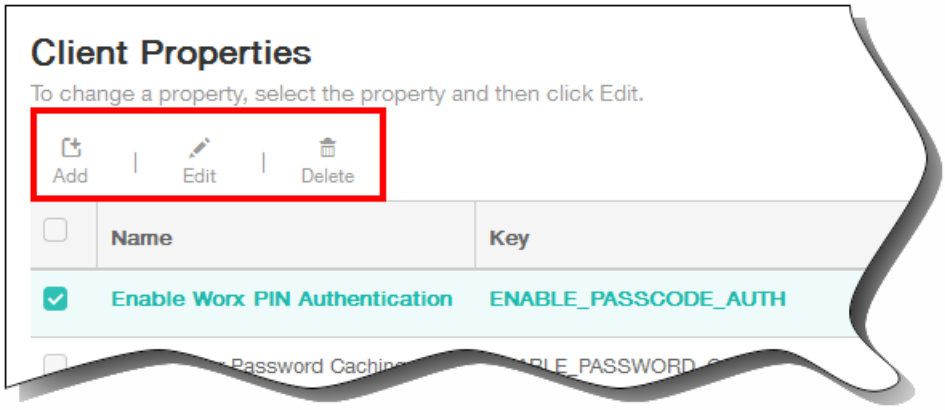
1. 在客户端属性页面中，单击添加。 此时将显示添加新客户端属性页面。

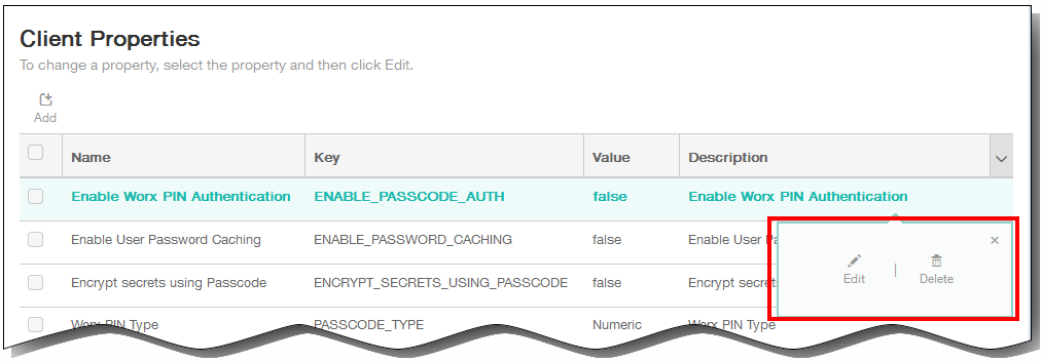


2. 在添加新客户端属性页面中，输入以下信息：
   注意：所有字段均为必填字段。
   1. 键：在列表中，单击要添加的属性键。
      重要：执行任何更改或请求特殊键以进行更改时请联系 Citrix 技术支持。
   2. 值：输入选定的属性值。
   3. 名称：输入属性的名称。
   4. 说明：输入属性的说明。

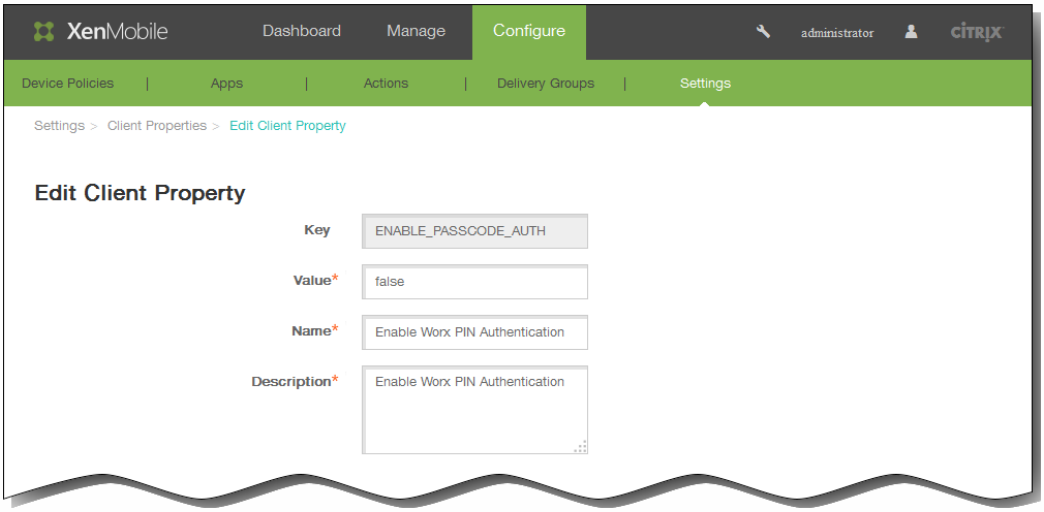
编辑客户端属性

1. 在客户端属性表格中，选择要编辑的客户端属性。
   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。



3. 适当更改以下信息：
   1. Value（值）：选定属性值。
   2. Name（名称）：属性的名称。
   3. Description（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。

删除客户端属性

1. 在编辑客户端属性表格中，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。

客户端属性参考

May 05, 2016

XenMobile 预定义的客户端属性及其默认设置如下所示。

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）。启用了 ENABLE_PASSWORD_CACHING 时或 XenMobile 使用证书身份验证时，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，解锁后，将发送该密码或证书以对 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 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

此密钥允许您将敏感数据存储在移动设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串此配置键允许对键构件执行强加密，但同时会添加用户熵（用户生成的随机 PIN 码，只有用户知晓）。

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，具体表现为更大量的身份验证将提示输入 Worx PIN。

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_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：1-99

默认值：90

PASSCODE_HISTORY

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。更改此设置时，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

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

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的时间（单位为分钟），之后用户访问应用程序时不会被提示输入 Worx PIN 或通行码。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。

可能的值：任意正整数

默认值：15

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、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#

ENABLE_CRASH_REPORTING

显示名称：启用崩溃报告

此键使用Crashlytics启用或禁用 Worx 应用程序的崩溃报告。

可能的值：true 或 false

默认值：true

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和上载日志的功能。日志记录功能对 Worx Home 和所有已安装的 MDX 应用程序禁用。用户不能从“支持”页面发送任何应用程序的日志；尽管显示了邮件撰写对话框，仍然不附加日志，但将附加一封邮件，指出日志记录功能已禁用。除对用户设备的影响外，您无法在 XenMobile 控制台中修改 Worx Home 和 MDX 应用程序的日志设置。

此键设置为 true 时，Worx Home 会将“阻止应用程序日志”设置为 true，以确保应用新策略时 MDX 应用程序停止日志记录。

可能的值：true 或 false

默认值：false（不禁用日志记录）

XenMobile 服务器设置

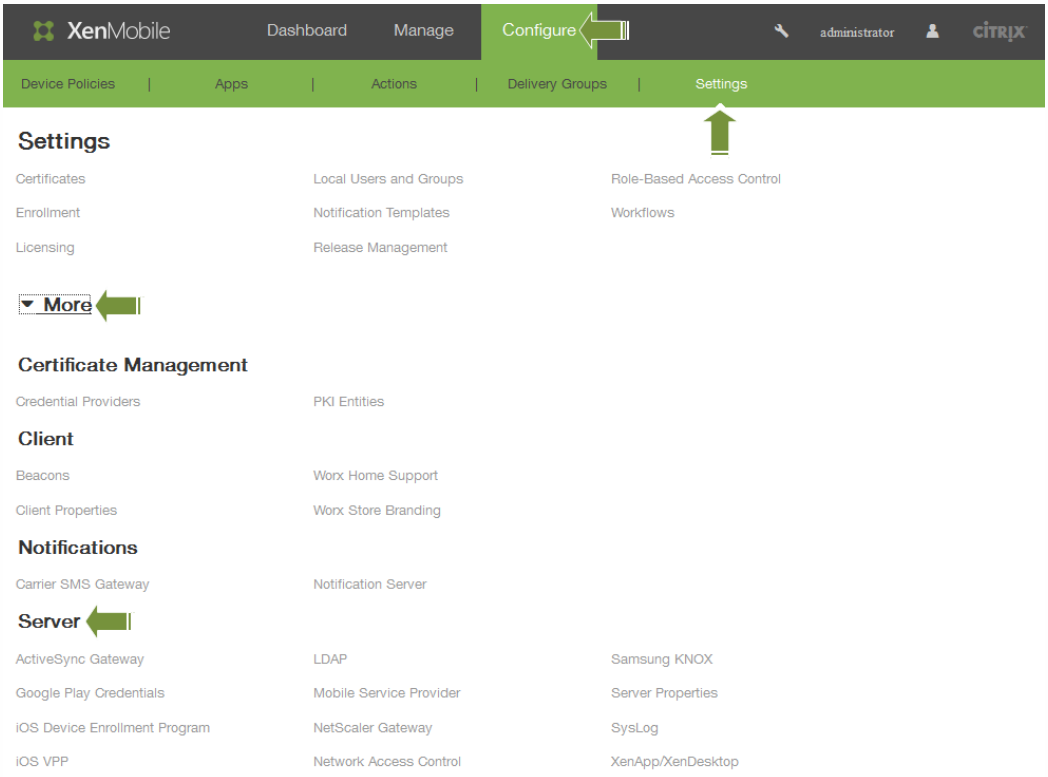
May 05, 2016

可以在 XenMobile Web 控制台中配置 XenMobile 服务器设置。

服务器配置选项包括：

ActiveSync Gateway	iOS VPP	NetScaler Gateway	服务器属性
Google Play 凭据	LDAP	网络访问控制	SysLog
iOS Device Enrollment Program	移动服务提供商	Samsung KNOX	XenApp/XenDesktop

1. 在 XenMobile 控制台中，单击配置，然后单击设置。
   此时将显示设置页面。



2. 单击更多。
3. 在**服务器**下面，单击要配置的选项。

XenMobile 中的 ActiveSync Gateway

May 05, 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。 根据这些规则，可以允许或拒绝设备访问 ActiveSync 数据。 例如，如果激活“缺少必备应用程序”规则，XenMobile 将检查应用程序访问策略中是否存在必备应用程序，如果缺少必备应用程序，则会拒绝对 ActiveSync 数据的访问。

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：检查设备是否安装了在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“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：检查设备是否缺少在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：检查设备是否具有在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。

已吊销状态：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。

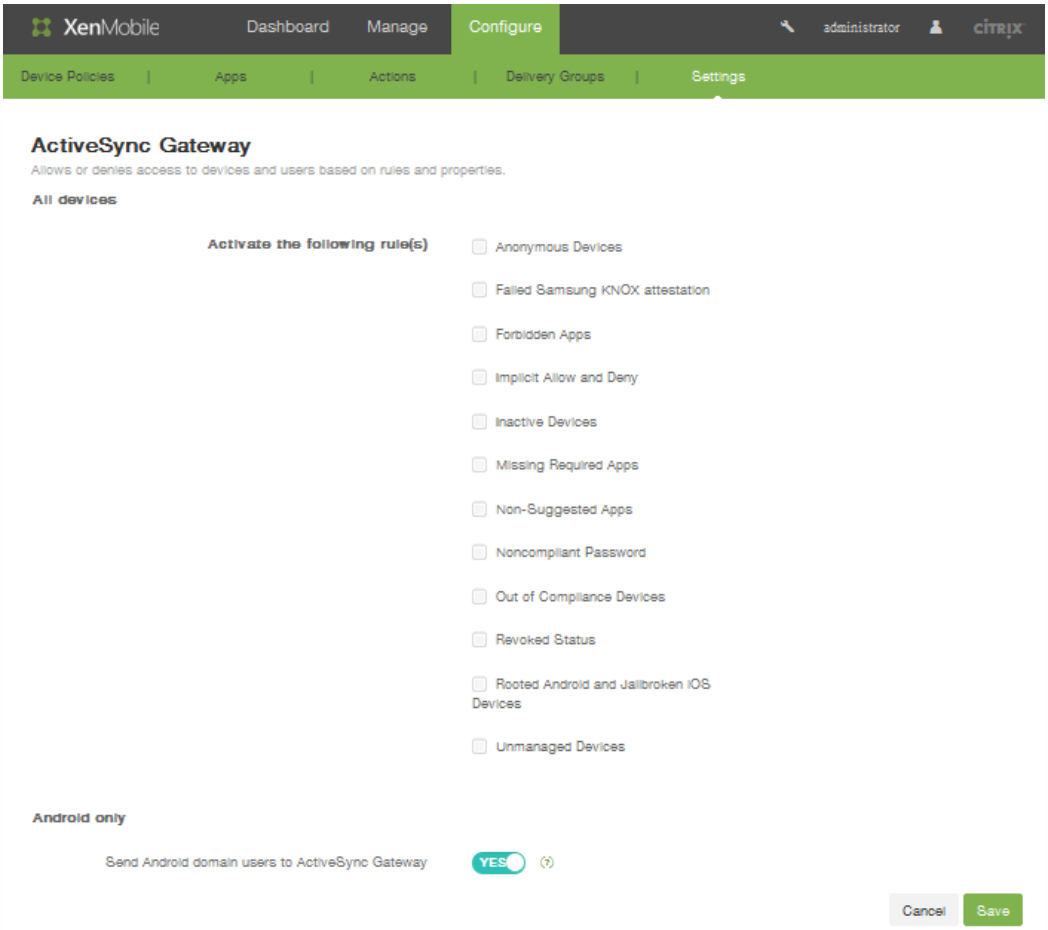
已获得 root 权限的 Android 设备和已越狱的 iOS 设备：检查 Android 设备或 iOS 设备是否已越狱。

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。

在 XenMobile 中配置 ActiveSync Gateway

1. 在 XenMobile 控制台中，单击**配置 > 设置 > 更多 > ActiveSync Gateway**。
   此时将显示 **ActiveSync Gateway** 配置页面。



2. 在**激活以下规则**中，选择要激活的一个或多个规则。
3. 在**仅限 Android**下，在**将 Android 域用户发送到 ActiveSync Gateway** 中单击**是**，以确保 XenMobile 将 Android 设备信息发送到 Secure Mobile Gateway。
4. 单击**保存**。

Google Play 凭据

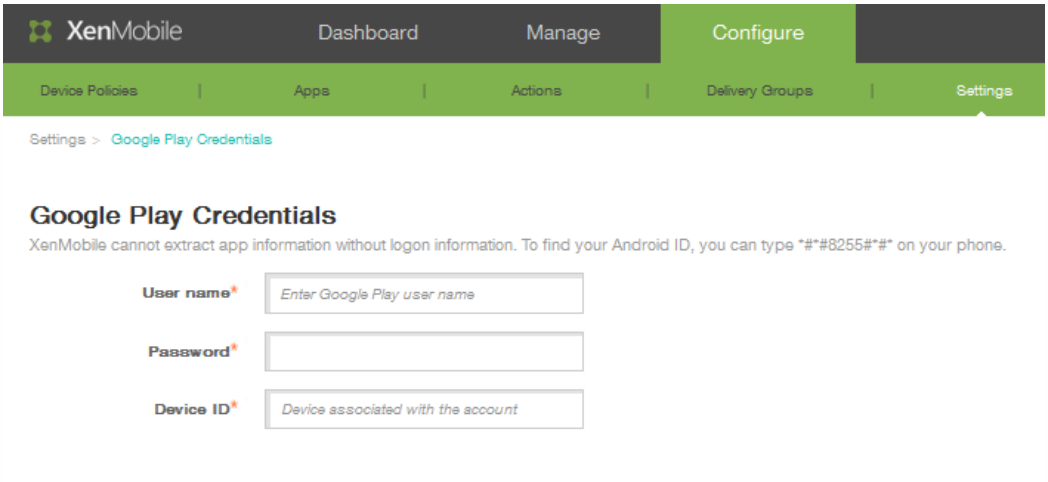
May 05, 2016

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#*#*。
重要：要启用 XenMobile 提取应用程序信息，您可能需要将 Gmail 帐户配置为允许非安全连接。有关步骤，请参阅 Google 支持站点。

配置 XenMobile 以使用 Google Play 凭据

1. 在 XenMobile Web 控制台中，单击配置 > 设置 > 更多 > Google Play 凭据。
   此时将显示 Google Play 凭据配置屏幕。



2. 在用户名中，输入与 Google Play 帐户关联的名称。
3. 在密码中，输入用户密码。
4. 在设备 ID 中，输入 Android ID。
   在电话上输入 *#*#8255#*#* 以确定 Android ID。
5. 单击保存。

iOS Device Enrollment Program

May 05, 2016

可以在 XenMobile 中为运行 iOS 的移动设备设置 iOS Device Enrollment Program。利用此功能，iOS 设备可以将自定义设备设置助理体验的配置文件告知 Apple 服务器，设备设置助理之后可以分配给特定设备。

在 XenMobile 中配置 iOS Device Enrollment Program

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。

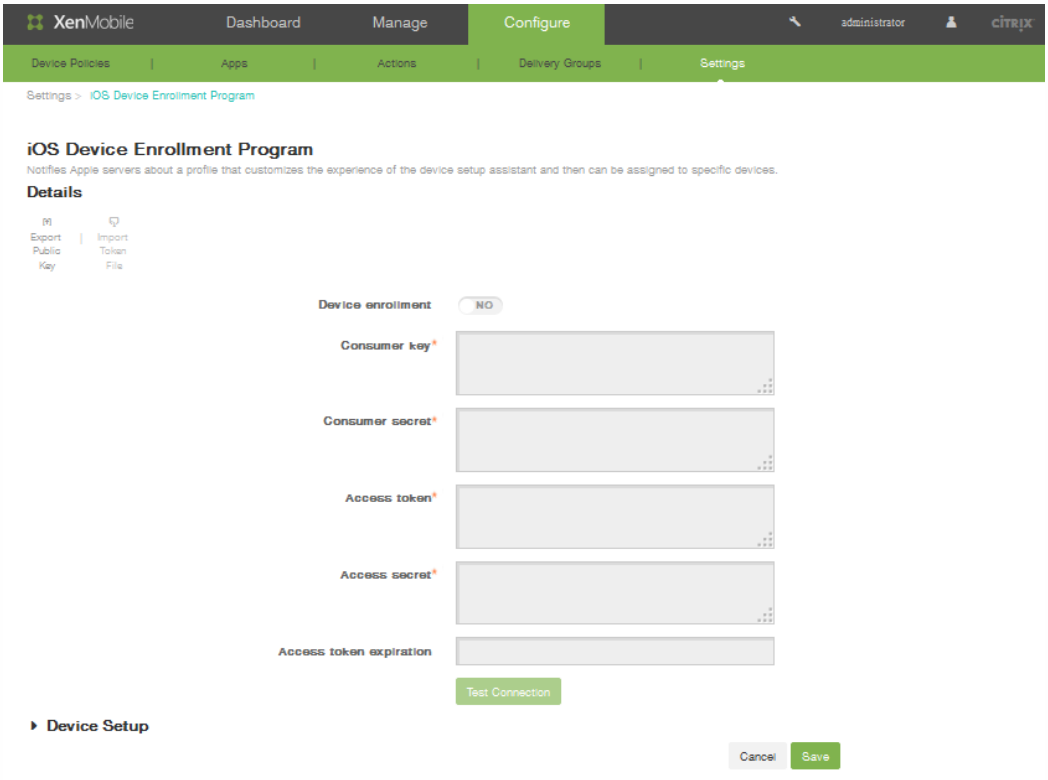
1. 要获取上载到 Apple 的公钥，请在 **iOS Device Enrollment Program** 页面上的**设置 > 更多**下，单击**导出公钥**，并将该文件保存到您的计算机。

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 Device Enrollment Program** 页面上，将**设备注册**设置为**是**，然后单击**导入令牌文件**以将 Apple 服务器令牌上载到 XenMobile。

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。



在**详细信息**中，配置以下设置以完成 DEP 配置：

- 设备注册：单击是。
- 使用者密钥：输入使用者密钥。
- 使用者机密：输入使用者机密。
- 访问令牌：指定访问令牌。
- 访问密钥：输入访问令牌的密钥。
- 访问令牌过期时间：可选，指定访问令牌过期时间。
- 单击测试连接以验证连接性。

- 展开设备设置，然后配置以下设置：
  - 业务部门：输入业务部门关联的名称。
  - 支持电话号码：输入支持电话号码。
  - 支持电子邮件地址：可选，输入支持电子邮件地址。
  - 唯一服务 ID：可选，包括一个唯一服务 ID。

- 在设备设置中，配置与 iOS Device Enrollment Program 关联的以下设备设置：
  - Allow or deny pairing（允许或拒绝配对）：单击允许，以允许通过 Apple 工具（如 iTunes 和 Apple Configurator）管理设备。

> **注意**
>
> 如果允许配对并使用 Apple Configurator，请在**受监督模式**中，选择**是**。

- - 设备配置文件删除：如果希望设备使用可以远程删除的配置文件，请单击允许。
  - 要求注册设备：选中此复选框以阻止用户跳过注册过程。

- 在设备设置步骤中，配置以下设置：
  - 定位服务：单击设置以允许设备共享位置，或单击跳过以阻止设备共享其位置。
  - 从备份还原：单击设置以允许设备从备份文件还原数据。
  - Apple 和 iCloud：如果希望设备使用 Apple ID 和 iCloud，请单击设置。
  - 条款和条件：单击设置。
  - 通行码：单击设置以使用设备注册的通行码。
  - Siri：单击设置以允许设备使用Siri。
  - Touch ID：单击设置以使用设备的 Touch ID。
  - Apple Pay：单击设置以对设备启用 Apple Pay。
  - 缩放：单击设置以启用缩放。
  - 诊断：单击设置以允许设备共享诊断。

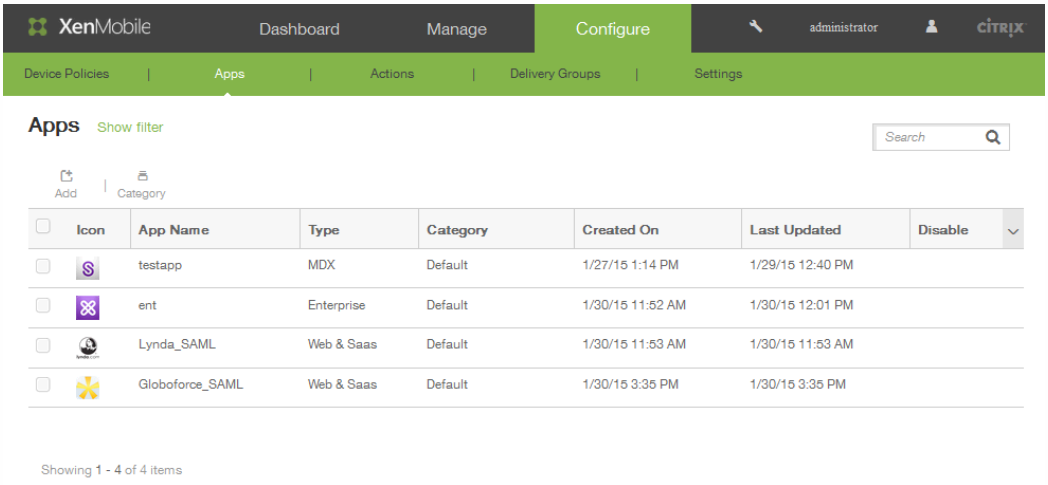
- 单击保存。

iOS VPP

May 05, 2016

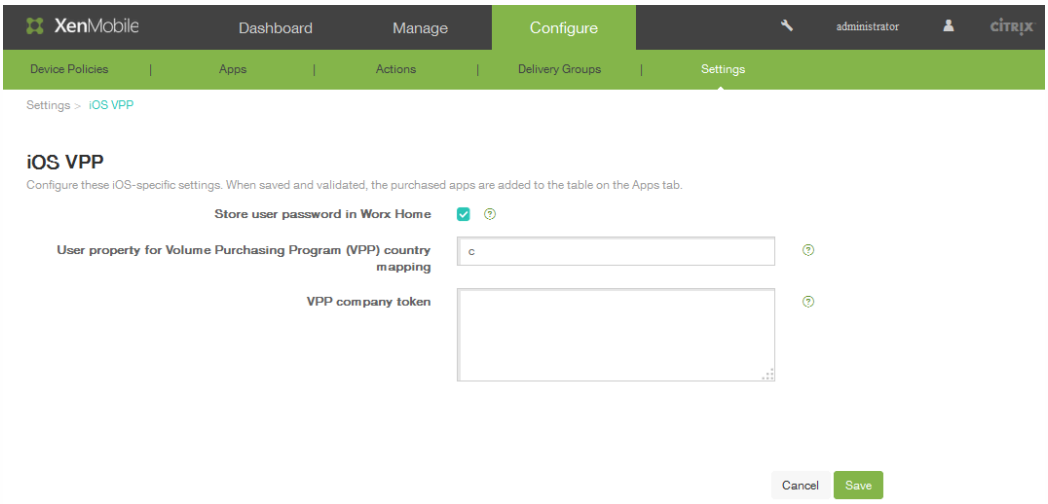
可以在 XenMobile 中配置特定于 iOS Volume Purchase Plan (VPP) 的设置。iOS VPP 简化了组织批量查找、购买和分发应用程序及其他数据的过程。VPP 为管理组织的内容需求提供可扩展的简化解决方案。

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。



在 XenMobile 中配置 iOS VPP

1. 在 XenMobile Web 控制台中，单击配置 > 设置 > 更多 > iOS VPP。
   将显示 iOS VPP 配置屏幕。

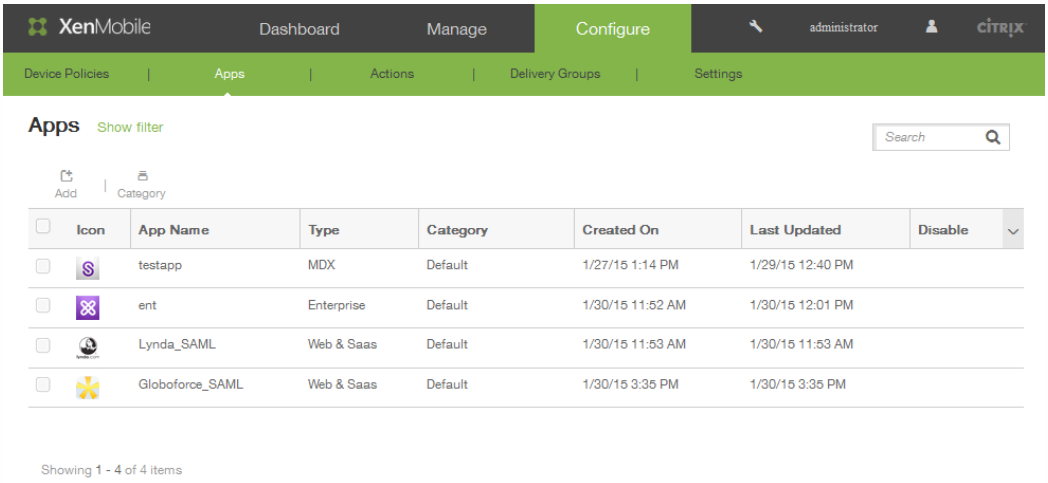


2. 在在 Worx Home 中存储用户密码中，选中复选框以将用户名和密码安全地存储在 Worx Home 中，用于 XenMobile 身份验证。
3. 在 Volume Purchasing Program (VPP)国家/地区映射的用户属性中，输入代码以允许用户从特定于国家/地区的应用商店下

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。

4. 在 VPP 公司令牌中，输入代表 VPP 服务令牌的令牌，此令牌是用户通过基于公司的帐户在 Apple App Store 中进行购买时生成的服务令牌。此令牌用于验证 VPP 许可证。例如，如果您具有 Business 的 Apple VPP 帐户，请访问 https://vpp.itunes.com，单击 **Business**（业务），并使用您的 Apple VPP 帐户凭据登录以检索相应的信息。
5. 单击保存。然后，信息将显示在应用程序表格中：



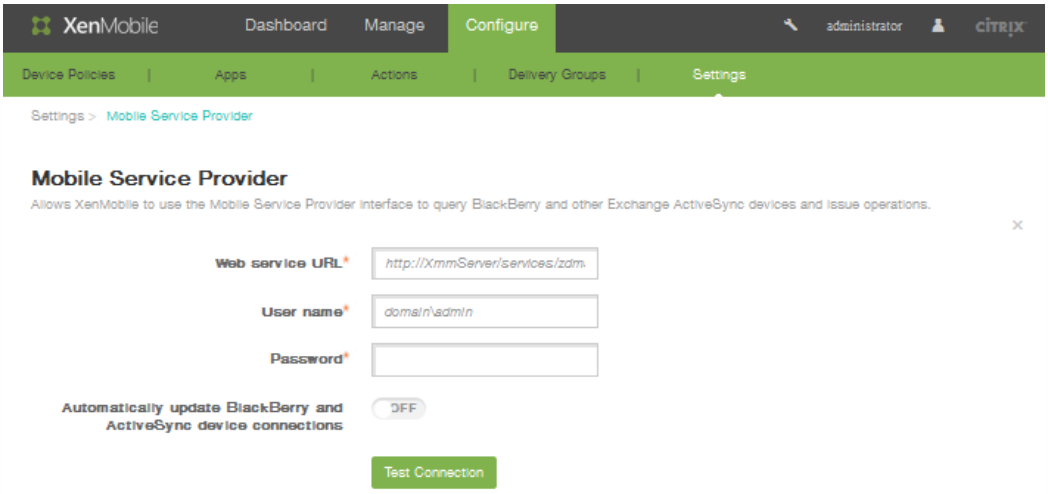
移动服务提供商

May 05, 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。

配置移动服务提供商

1. 在 XenMobile Web 控制台中，单击配置 > 设置 > 更多 > 移动服务提供商。
   此时将显示移动服务提供商配置页面。



2. 在 Web 服务 URL 中，输入 Web 服务的 URL，如 http://XmmServer/services/xdmservice
3. 在用户名中，采用 domain\admin 格式输入用户名
4. 在密码中，输入密码。
5. 在自动更新 BlackBerry 和 ActiveSync 设备连接中，如果要启用此选项，请单击“开”。默认设置为关
6. 单击测试连接以验证连接性。
7. 单击保存。

网络访问控制

May 05, 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指定条件，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：检查设备是否安装了在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“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：检查设备是否缺少在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：检查设备是否具有在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。

已吊销状态：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。

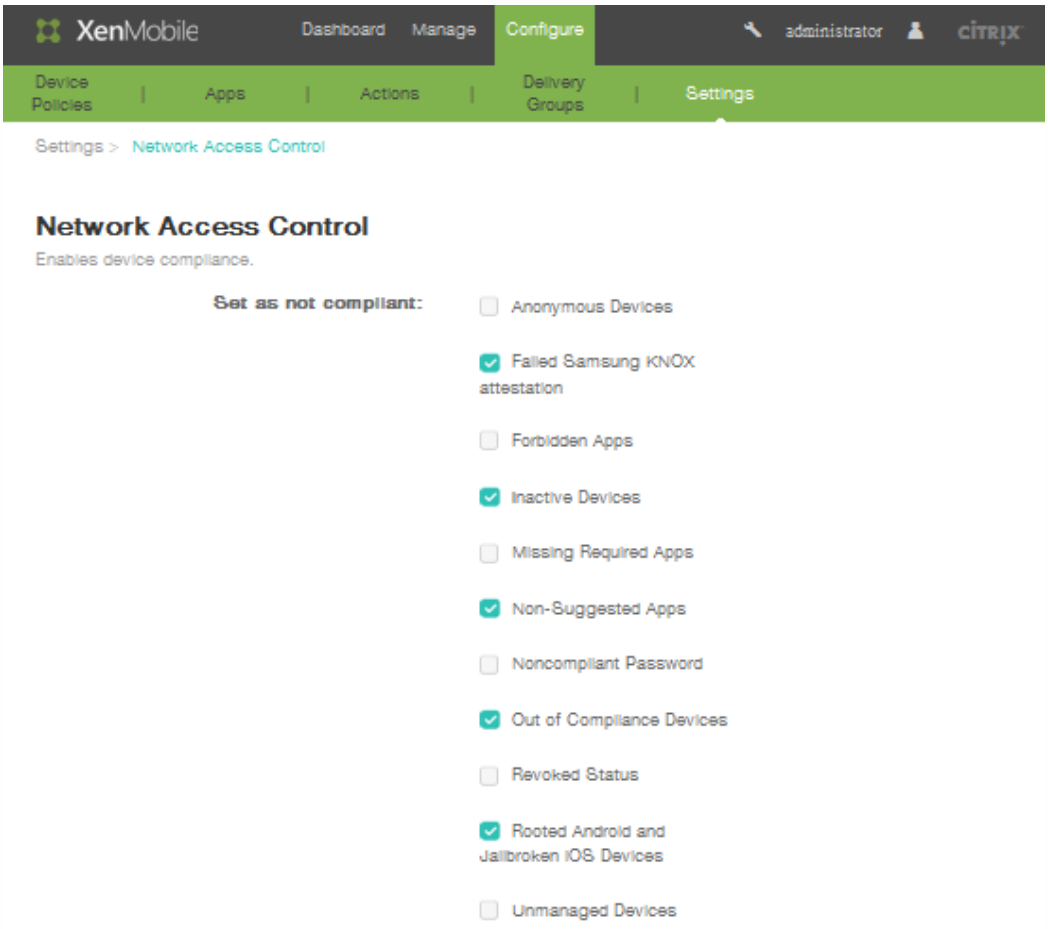
非托管设备：检查设备是否仍处于托管状态，受 XenMobile 控制。 例如，在 MAM 模式下运行的设备或已取消注册的设备为非托管设备。

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和/或未注册设备都将被标记为“不合规”，并会被 NAC 设备阻止在您的网络外。

在 XenMobile 中配置网络访问控制

1. 在 XenMobile Web 控制台中，单击**配置 > 设置 > 更多 > 网络访问控制**。
   此时将显示**网络访问控制**配置页面。



2. 选中要启用的**设为不合规**过滤器旁边的复选框。
3. 单击**保存**。

Samsung KNOX

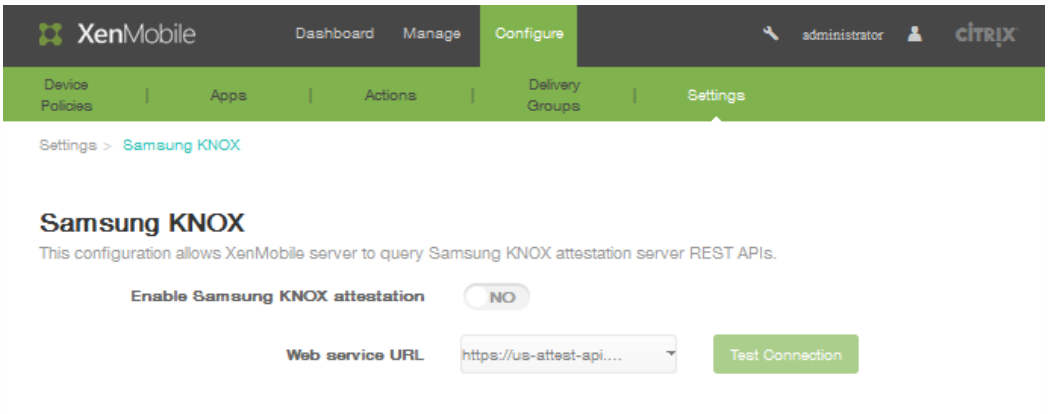
May 05, 2016

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。

启用 Samsung KNOX 认证

1. 在 XenMobile Web 控制台中，单击配置 > 设置 > 更多 > Samsung KNOX。
   此时将显示 Samsung KNOX 配置页面。



2. 在启用 Samsung KNOX 认证中，单击**是**。
3. 在步骤 2 中单击是时，将启用 **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**。

服务器属性

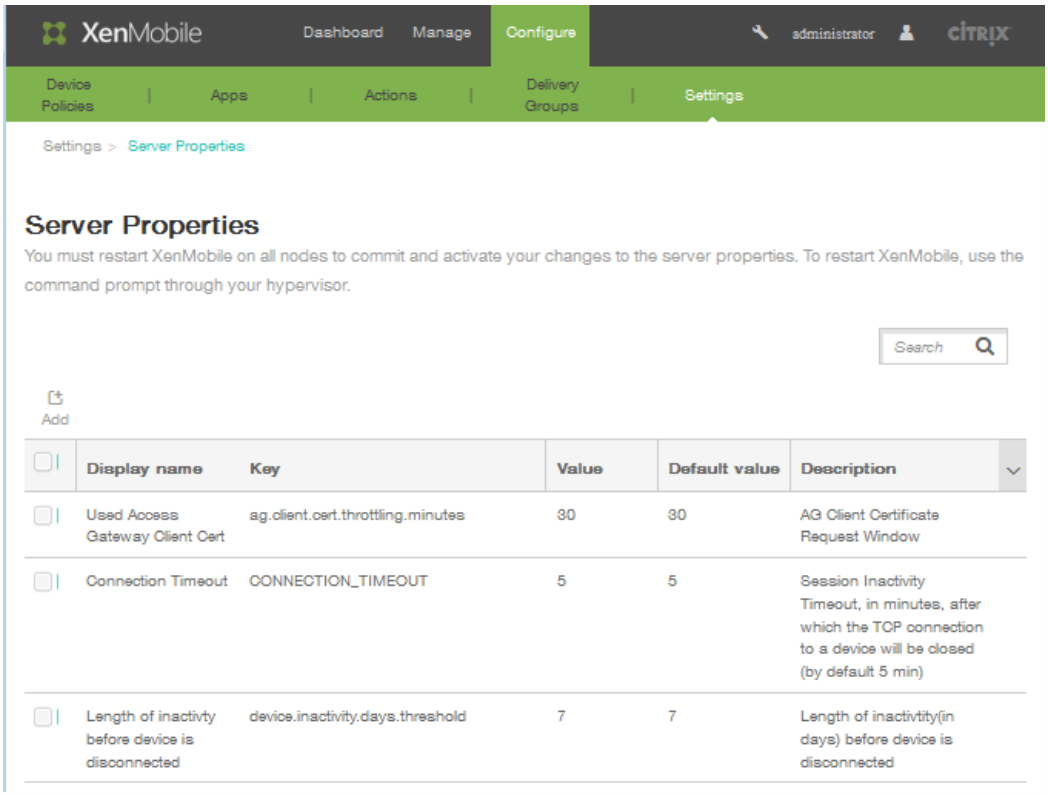
May 05, 2016

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。

在 XenMobile 中配置服务器属性

1. 在 XenMobile Web 控制台中，单击配置 > 设置 > 更多 > 服务器属性。
   此时将显示服务器属性配置页面。



2. 执行以下操作之一：
   - 单击添加以添加新服务器属性。
   - 在表格中，单击以选择现有属性，然后在显示的菜单中，单击编辑。
3. 如果在步骤 2 中单击添加，请配置以下字段：

- 键：在列表中，选择合适的键。
  注意：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**：根据选择的键输入一个值。
- **显示名称**：输入新属性值显示在服务器属性表格中的名称。
- **说明**：可以选择包含新服务器属性的说明，然后单击保存。

SysLog

May 05, 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。

可以将服务器配置为收集以下类型的信息：

- 系统日志表示 XenMobile 所执行的操作。
- 审核日志表示按时间排序的 XenMobile 系统活动记录。

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：

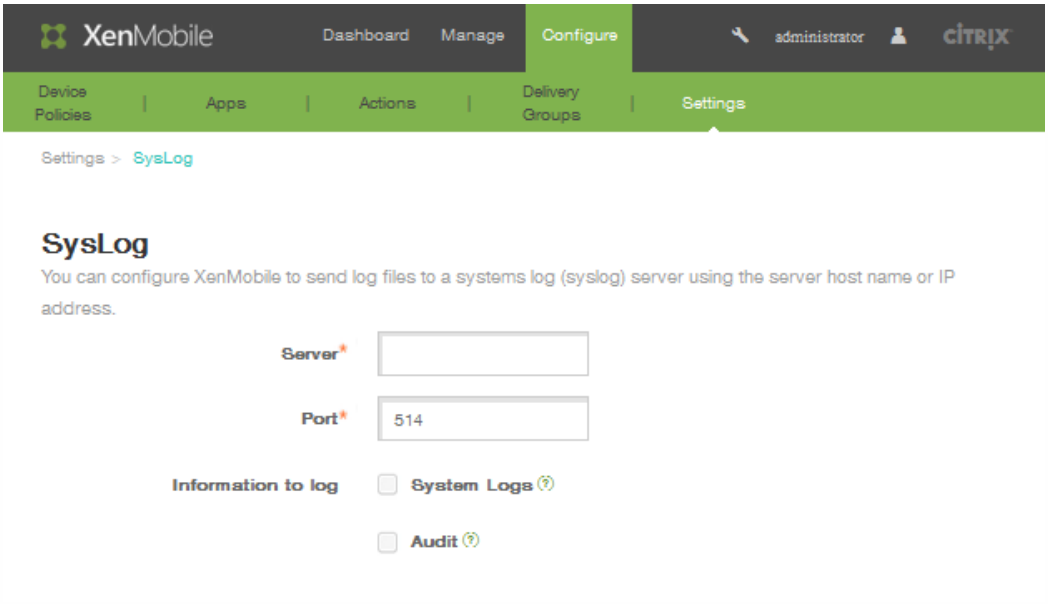
- 生成日志消息的设备的 IP 地址
- 时间戳
- 消息类型
- 与事件关联的日志级别（严重、错误、通知、警告、信息、调试、警报或紧急）
- 消息信息

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**
>
> XenMobile cloud deployments, Citrix does not support syslog integration with an an on-premises syslog server. Instead, you can download the logs from the Support page in the XenMobile console. When doing so, you must click Download All in order to get system logs. For details, see Viewing and Analyzing Log Files in XenMobile.

在 XenMobile 中配置 syslog 服务器

1. 在 XenMobile Web 控制台中，单击配置 > 设置 > 更多 > Syslog。
   此时将显示 Syslog 配置页面。



2. 在名称中，输入 Syslog 服务器的 IP 地址或完全限定的域名 (FQDN)。
3. 在端口中，输入端口号。默认情况下，此端口设置为 514。
4. 在要记录的信息中，选择或取消选择系统日志或审核。
   - 系统日志表示 XenMobile 所执行的操作。
   - 审核日志表示按时间排序的 XenMobile 系统活动记录。
5. 单击**保存**。

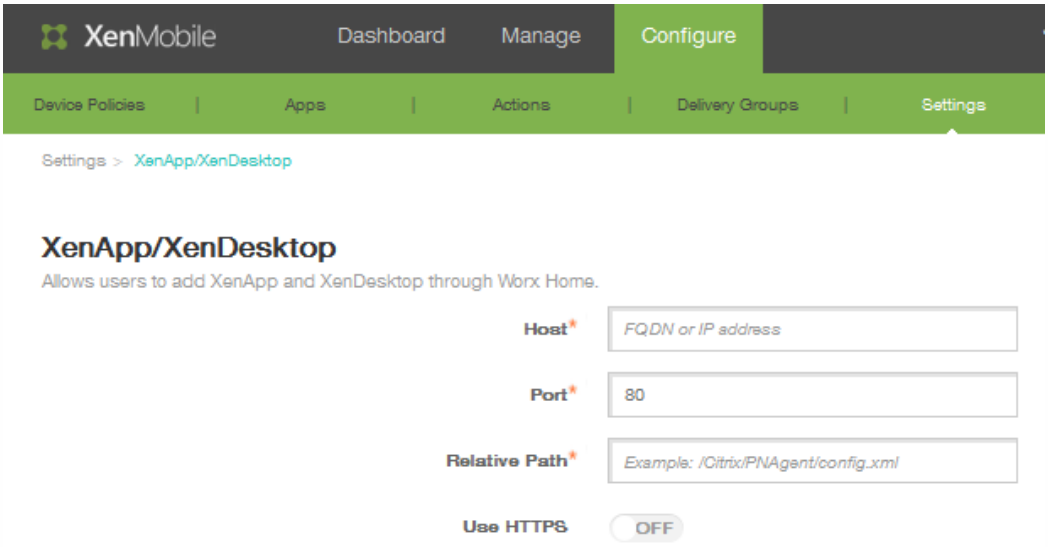
配置 XenApp 和 XenDesktop

May 05, 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 StoreFront 或 Web Interface 站点的完全限定域名 (FQDN) 或 IP 地址和端口号。

1. 在 XenMobile Web 控制台中，单击**配置 > 设置 > 更多 > XenApp/XenDesktop**。
   此时将显示 XenApp/XenDesktop 配置页面。



2. 在主机中，输入 StoreFront 或 Web Interface 站点的完全限定域名 (FQDN) 或 IP 地址。
3. 在端口中，输入 StoreFront 或 Web Interface 站点的端口号。默认值为 80。
4. 在相对路径中，输入路径。例如，/Citrix/Store/PNAgent/config.xml
5. 在使用 HTTPS 中，选择开，以在 StoreFront 或 Web Interface 站点和客户端设备之间启用安全的身份验证。默认值为关。
6. 单击**保存**。

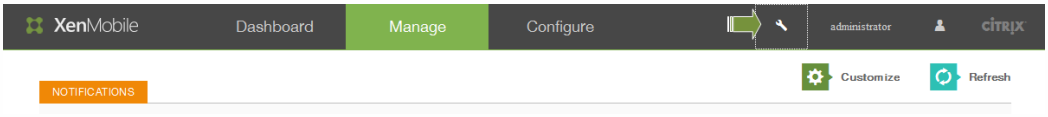
XenMobile 支持与维护

May 05, 2016

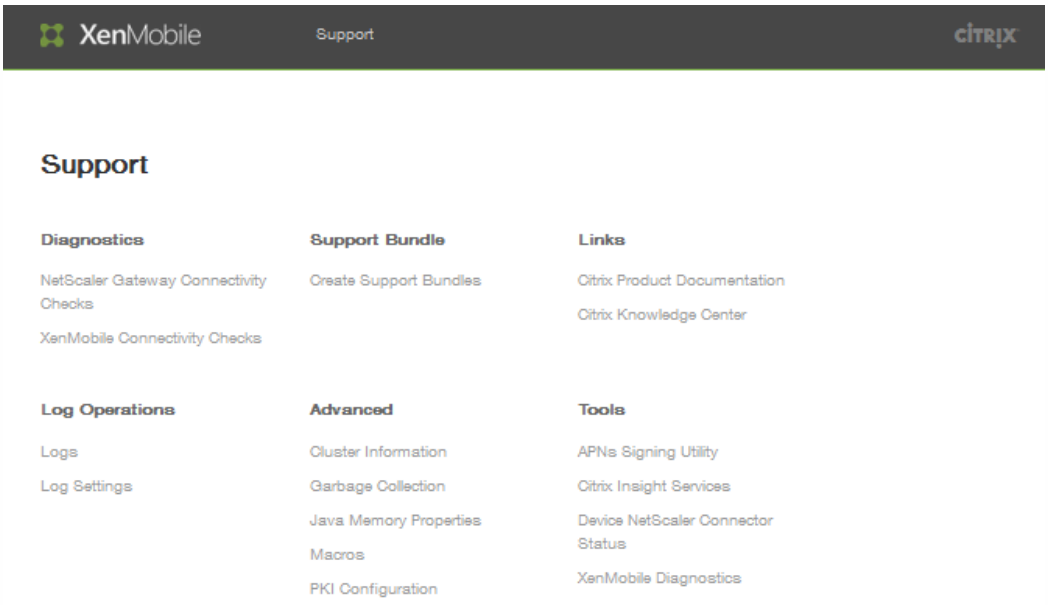
使用 XenMobile 的“支持”页面访问多个与支持相关的信息和工具。也可以从命令行执行操作。有关详细信息，请参阅 XenMobile 命令行接口选项。有关 XenMobile API 和 SDK 的详细信息，请参阅 XenMobile 10 API。

访问“支持”页面

在 XenMobile 控制台中，单击控制台右上角的扳手图标 。



支持页面将显示在单独的浏览器选项卡中：



使用 XenMobile 的“支持”页面可以执行以下操作：

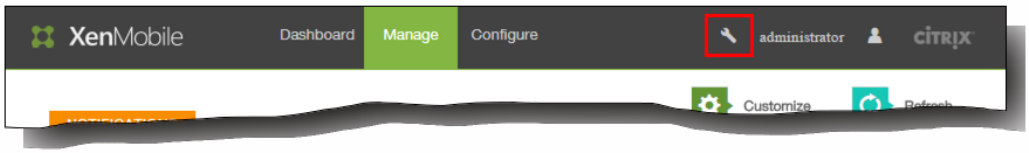
- 访问诊断。
- 创建支持包。
- 访问 Citrix 产品文档和知识中心的链接。
- 访问日志操作。
- 从高级信息和配置选项中选择。
- 访问工具和实用程序。

执行连接检查

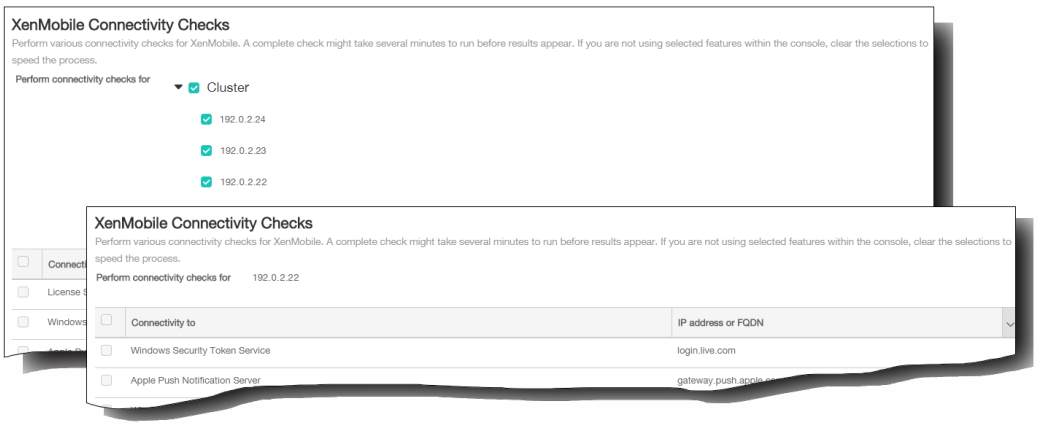
May 05, 2016

从 XenMobile 的“Support”（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。要访问“Support”（支持）页面，请执行以下操作：

1. 从 XenMobile 控制台，单击右上角的扳手图标。 XenMobile 控制台的所有页面均显示此扳手图标。系统可能会要求您提供用户名和密码。



XenMobile 的“Support”（支持）页面将在新的浏览器选项卡中打开。如果 XenMobile 环境包含加入群集的节点，将显示所有节点。



执行 XenMobile 连接检查

1. 在支持页面上，单击 XenMobile 连接检查。 此时将显示 XenMobile 连接检查页面。
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。 此时将显示结果。
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。

执行 NetScaler Gateway 连接检查

1. 在支持页面上，单击 NetScaler Gateway 连接检查。 此时将显示 NetScaler Gateway 连接检查页面。
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。
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。

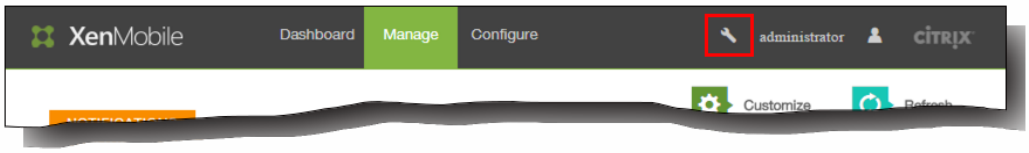
7. 在测试结果表格中选择一个服务器，可查看有关此服务器的详细结果。

在 XenMobile 中创建支持包

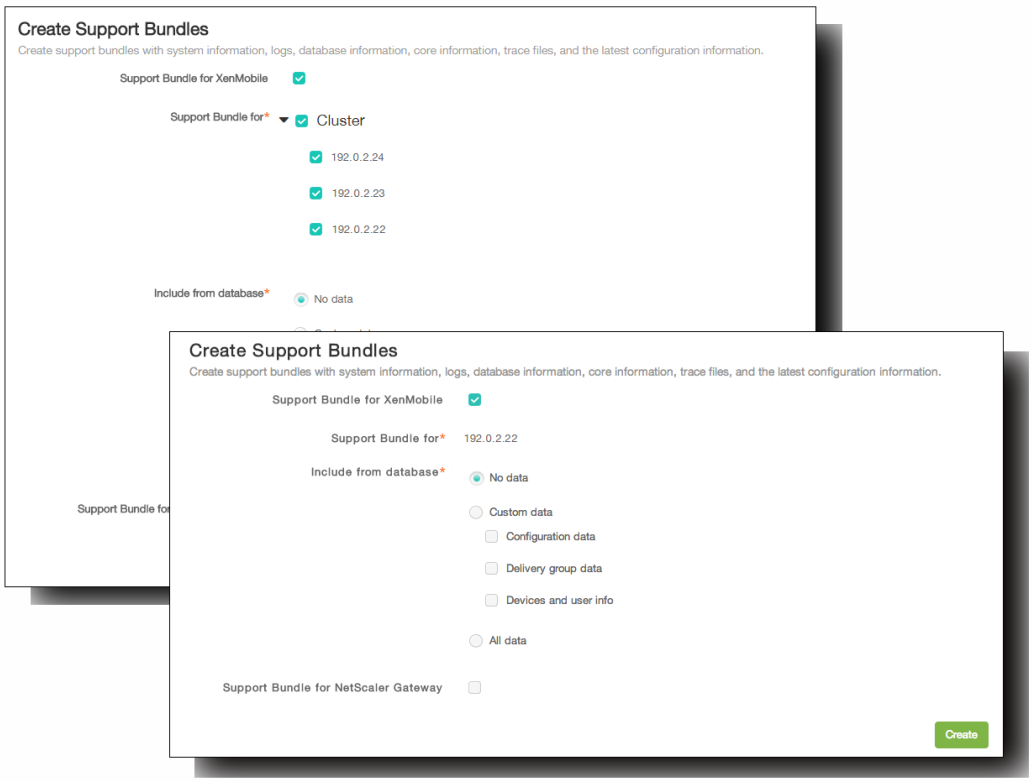
May 05, 2016

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。 XenMobile 控制台的所有页面均显示此扳手图标。
   注意：系统可能会要求您提供用户名和密码。



   此时将在新的浏览器选项卡上打开 XenMobile 支持。
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。

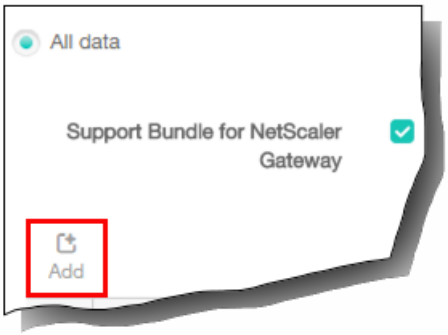


3. 确保选中适用于 XenMobile 的支持包复选框。
4. 如果 XenMobile 环境包含加入群集的节点，在适用于此对象的支持包中，可以选择所有节点或任何节点组合，以便从中提取数据。
5. 在包含在数据库中，执行以下操作之一：
   - 单击无数据。
   - 单击自定义数据，然后选择以下任意选项或全部选项：

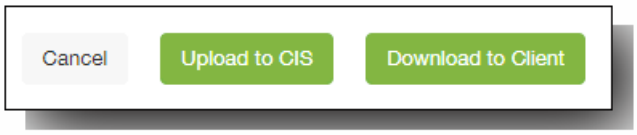
- 配置数据。包括证书配置和设备管理器策略。
- 交付组数据。包括应用程序交付组信息，其中包含应用程序类型和交付策略详细信息。
- 设备和用户信息。包括设备策略、应用程序、操作和交付组。

- 单击所有数据。

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：
   1. 单击添加。



      将显示添加 NetScaler Gateway 服务器对话框。
   2. 在 NetScaler Gateway 管理 IP 中，键入要从中提取支持包的 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。
   3. 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。
   4. 单击添加。 新的 NetScaler Gateway 支持包将添加到表格中。
   5. 根据需要，重复步骤 6 以添加其他 NetScaler Gateway 支持包。
7. 单击创建。 将创建支持包，并显示两个按钮上载到 CIS 和下载到客户端。

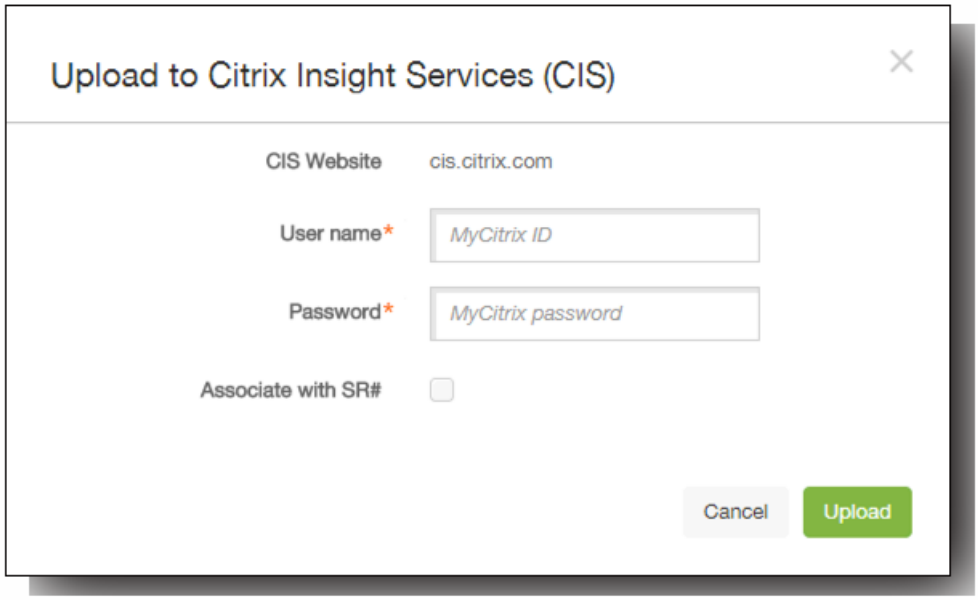


继续执行**将支持包上载到 Citrix Insight Services** 或**将支持包下载到客户端**的过程。

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。

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：
    1. 在 SR 编号中，键入要将此包关联到的八位数服务请求号码。
    2. 在说明中，键入 SR 的说明。
5. 单击上载。 支持包将上载到 CIS。

将支持包下载到您的计算机

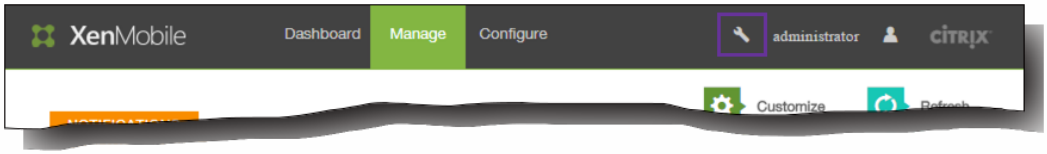
创建支持包之后，可以将此包上载到 CIS 或将其下载到您的计算机。如果希望自己排除故障，可以将支持包下载到您的计算机。
在创建支持包页面上，单击下载到客户端。支持包将下载到您的计算机。

查看调试日志文件

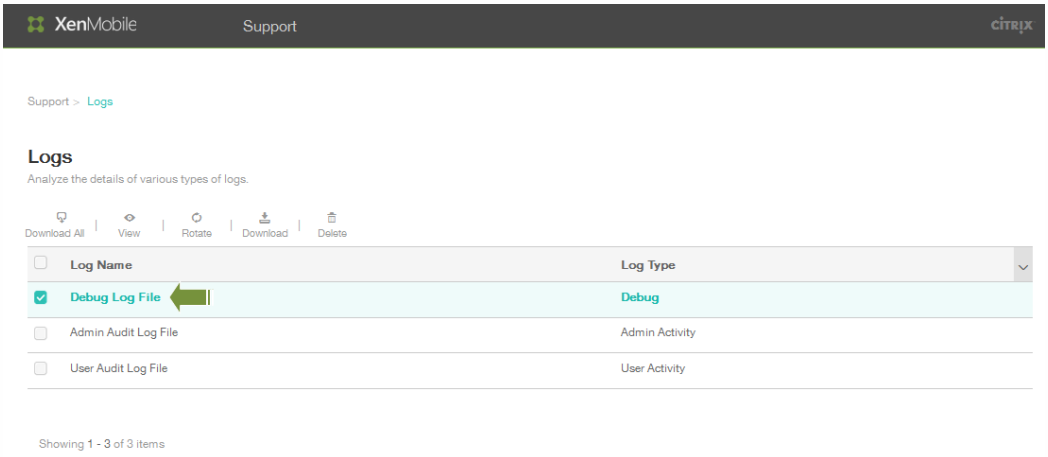
May 05, 2016

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)。

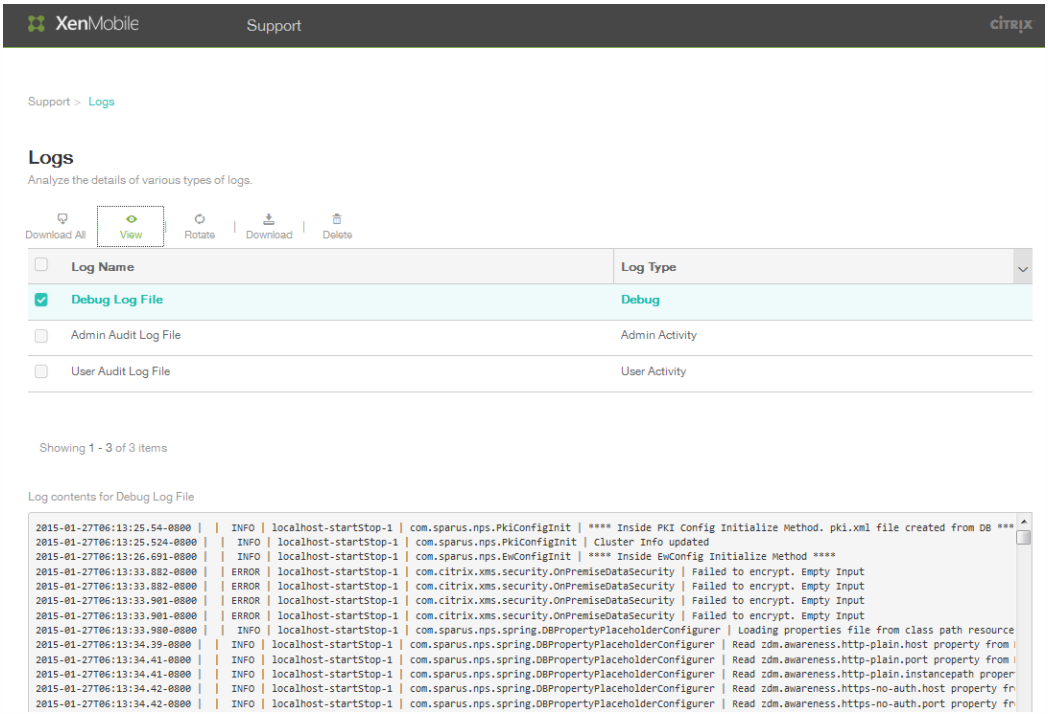
1. 在 XenMobile 控制台中，单击右上角的扳手图标。 XenMobile 控制台的所有页面均显示此扳手图标。



2. 在支持页面上，单击日志。 此时将显示“日志”屏幕。



3. 选择调试日志文件，然后单击查看，显示日志的内容。



在分析日志文件后，使用下载文件选项保存该数据，或单击删除从数据库中删除日志的内容。

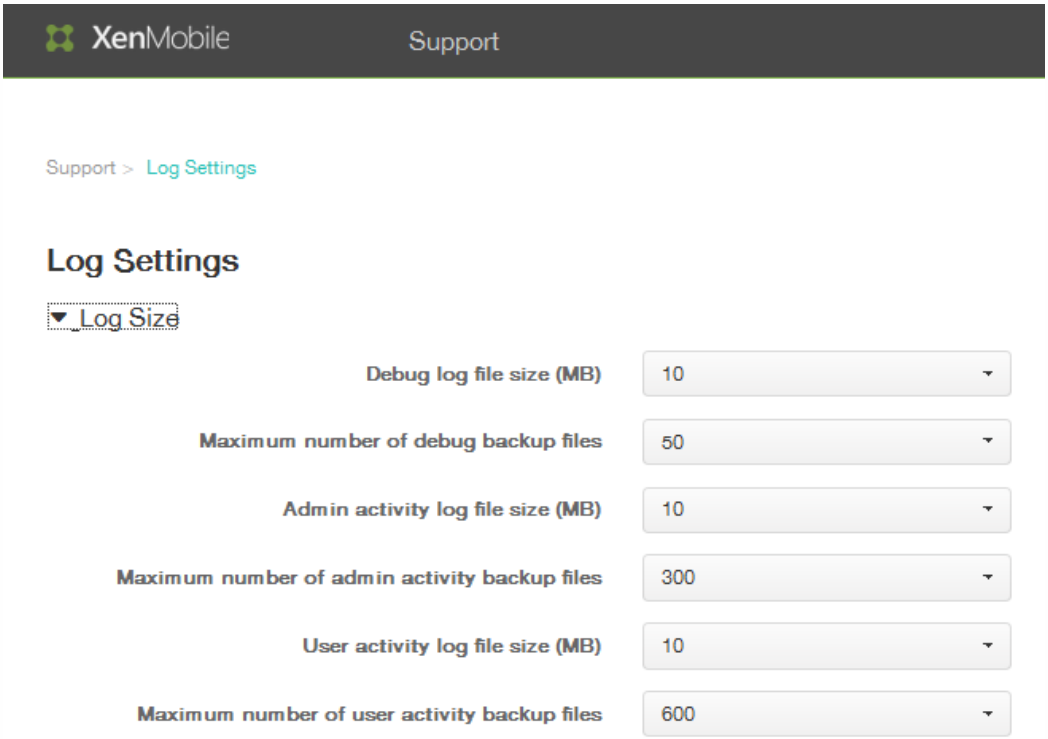
配置日志设置

May 05, 2016

您可以配置日志设置，对 XenMobile 所生成日志的输出进行自定义。在 XenMobile 控制台中，单击 Support > Log Settings（支持 > 日志设置），访问以下选项：

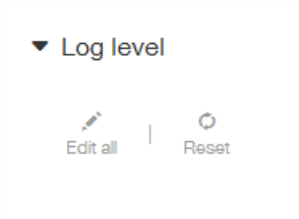
- 日志大小。使用此选项可以控制日志文件的大小和保留在数据库中的日志备份文件的最大数量。日志大小适用于 XenMobile 支持的每个日志（调试日志、管理员活动日志和用户活动日志）。
- Log Level（日志级别）。使用此选项可以更改类名称、子类名称、日志级别或者保存设置。
- 自定义记录器。使用此选项可以创建自定义的日志记录器；自定义日志需要一个类名称和日志级别。

1. 单击支持 > 日志设置，然后展开日志大小。

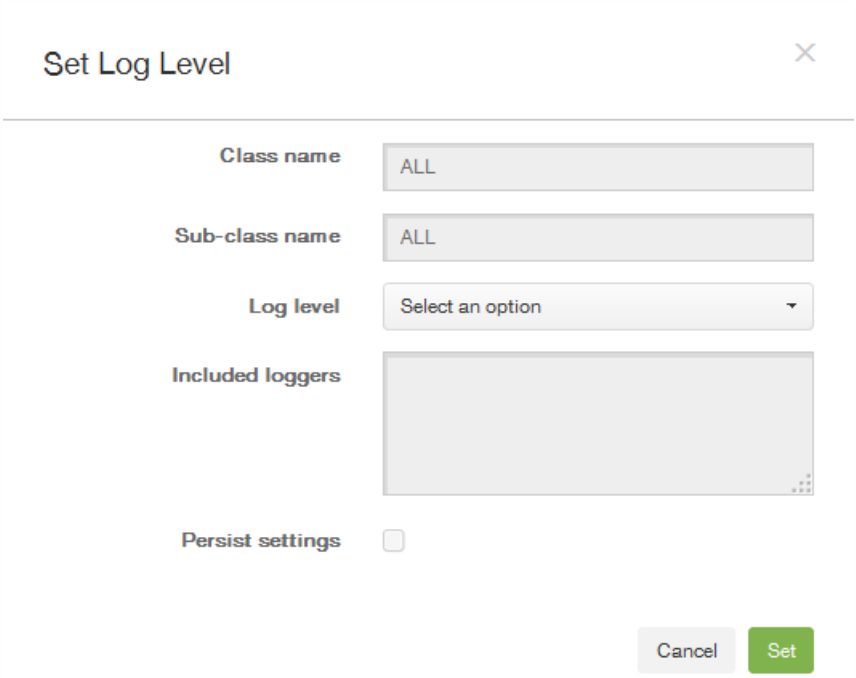


2. 在调试日志文件大小(MB) 列表中，选择一个介于 5 MB 和 20 MB 之间的大小，以更改调试文件的最大大小。 默认情况下，文件大小设置为 10 MB。
3. 在调试备份文件数上限列表中，选择 5 至 300 个调试文件，更改服务器保留的调试文件的最大数量。 默认情况下，XenMobile 在服务器上保留 50 个备份文件。
4. 在管理活动日志列表中，选择一个介于 5 MB 和 20 MB 之间的大小。 默认情况下，文件大小设置为 10 MB。
5. 在管理活动备份文件数上限列表中，选择 5 至 300 个调试文件，作为服务器保留的管理活动备份文件的最大数量。 默认情况下，XenMobile 在服务器上保留 300 个备份文件。
6. 在用户活动日志文件大小列表中，选择 5 MB 和 20 MB 之间的大小。 默认情况下，文件大小设置为 10 MB。
7. 在管理活动备份文件数上限列表中，选择 5 至 300 个调试文件，作为服务器保留的管理活动备份文件的最大数量。 默认情况下，XenMobile 在服务器上保留 300 个备份文件。

1. 单击支持 > 日志设置，然后展开日志级别，可以显示配置选项。 单击编辑全部，以配置日志级别的各项元素。

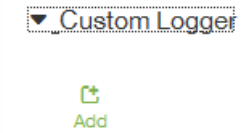


此时将显示设置日志级别屏幕。

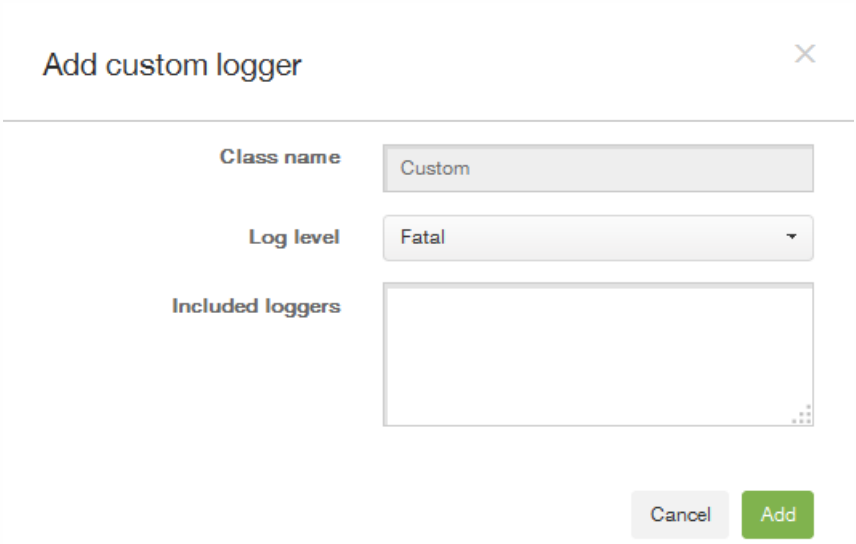


2. 输入类别名称。 默认情况下，此字段设置为全部。
3. 输入子类别名称。 默认情况下，此字段设置为全部。
4. 在日志级别列表中，选择日志级别。 支持的日志级别包括致命、错误、警告、信息、调试、跟踪或关。 包括记录器字段会显示每个配置类当前配置的日志级别。
5. 如果要保留日志级别设置，请选中静态设置复选框。
6. 单击设置提交更改。

1. 要添加自定义记录器，请单击添加。



此时将显示添加自定义记录器屏幕。

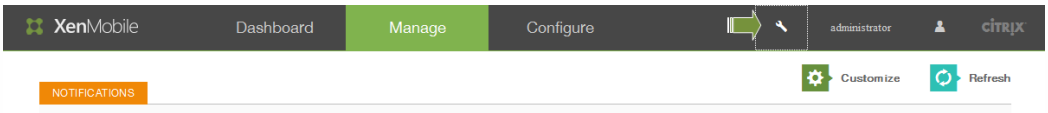


2. 指定一个类别名称。
3. 在日志级别列表中，选择日志级别。 支持的日志级别包括致命、错误、警告、信息、调试、跟踪或关。 包括记录器字段会显示每个配置类当前配置的日志级别。
4. 单击添加。

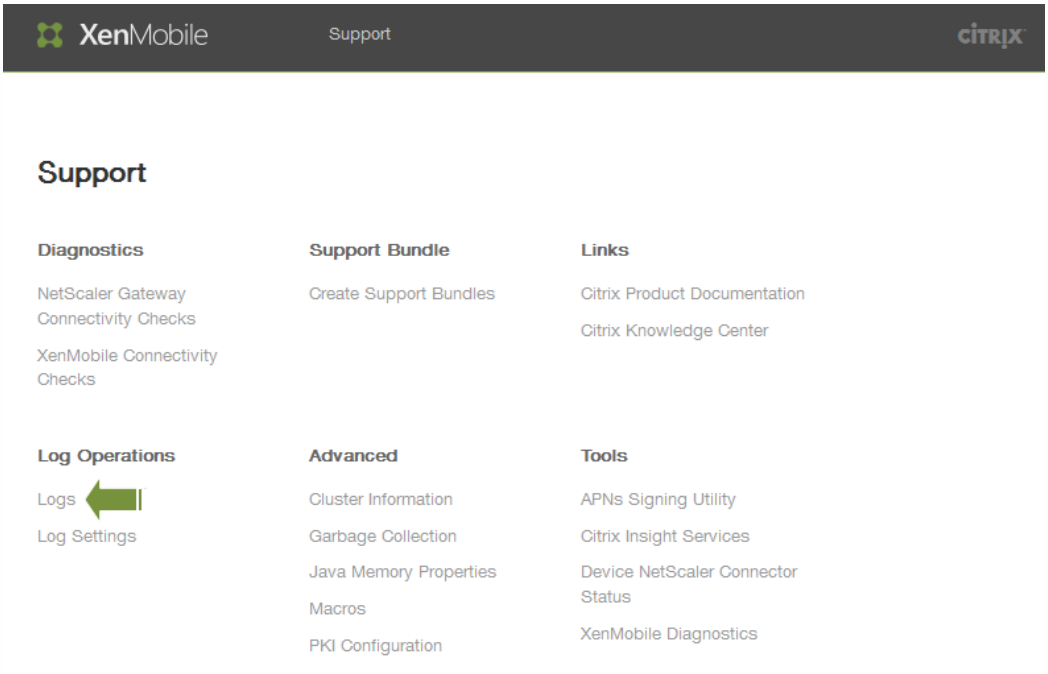
在 XenMobile 中查看和分析日志文件

May 05, 2016

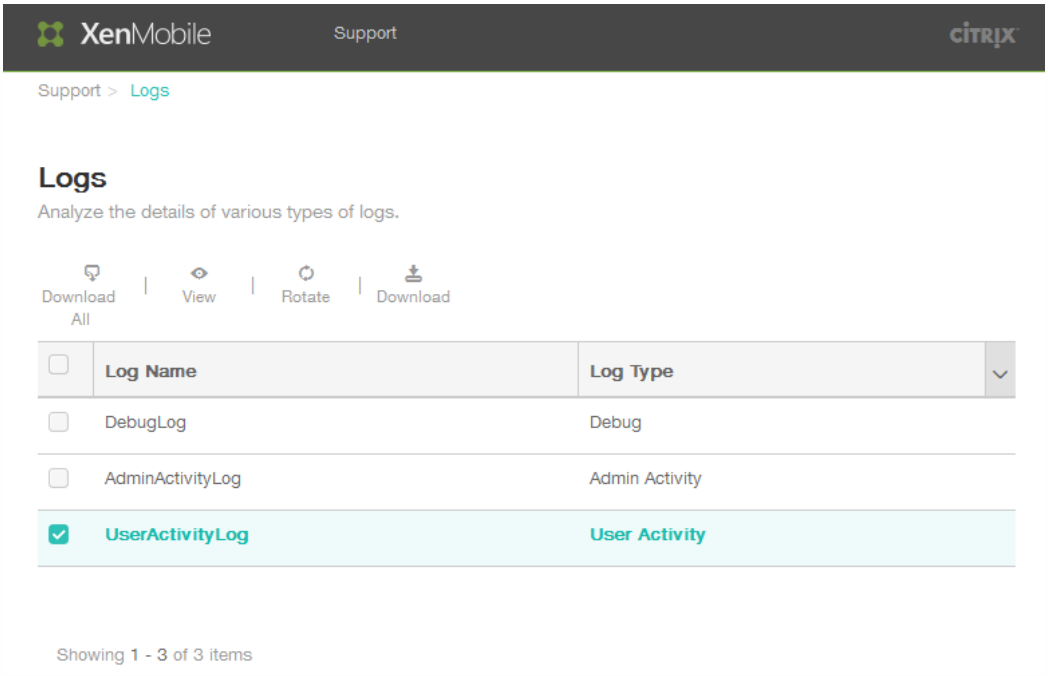
1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标 。 支持页面即在新的浏览器窗口中打开。



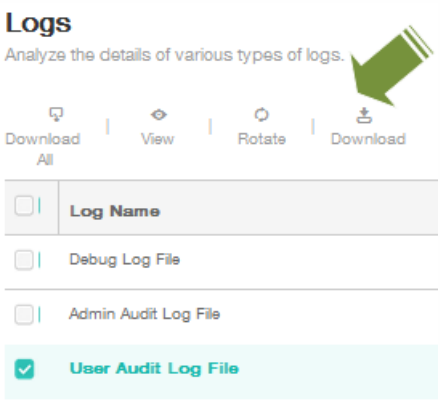
2. 在日志操作下，单击**日志**。 此时将显示**日志**屏幕。单独的日志将显示在表格中。



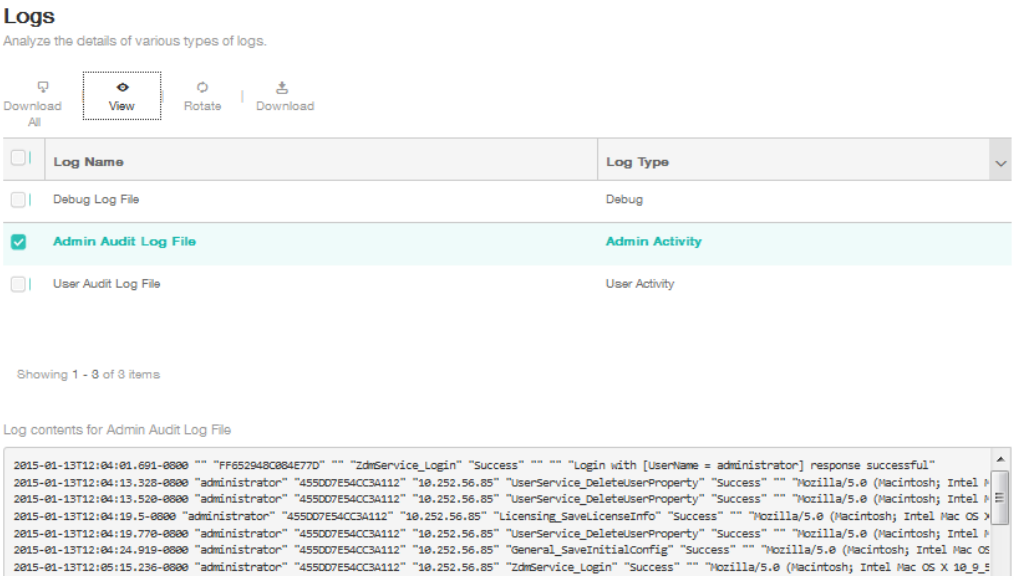
3. 选择要查看的日志。 调试日志包含对 Citrix 技术支持有用的信息；它包含错误消息以及与服务器相关的操作等有用信息。 用户活动日志显示与每个已配置用户相关的信息。 此时将显示**日志**屏幕。单独的日志将显示在表格中。



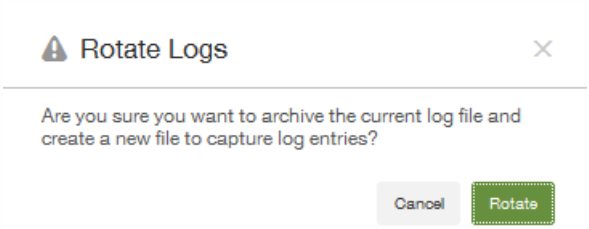
4. 使用表格顶部的操作执行以下操作：
   - 全部下载：控制台下载系统中显示的所有日志（包括调试日志、用户/管理员活动日志、服务器日志等）。单击下载可以仅保存选定的日志；也会下载存档日志。



   - 查看：在表格下方显示日志的内容。



- Delete（删除）：永久性删除所选日志文件。
- 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。



XenMobile 命令行接口选项

May 05, 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 - 5]）

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 - 4]）

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。）

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 Service（HTTP 服务）

Port（端口） : 80

Enable access (y/n) [y]:（启用访问(y/n) [y]:）

Management HTTPS service（管理 HTTPS 服务）

Port（端口） : 4443

Enable access (y/n) [y]:（启用访问(y/n) [y]:）

SSH Service（SSH 服务）

Port [22]:（端口 [22]:）

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 [30001]:）

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]:）

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 - 5]）

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：

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。）

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 - 9]）

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 - 3]）

选择“Network Utilities”（网络实用程序）选项时，将显示以下菜单：

---

[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 - 7]）

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]）

XenMobile 10 API

May 05, 2016

可以在 XenMobile 10 中使用以下 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

Web 服务定义语言 (WSDL) 名称	调用
	getDeviceInfo
	getDeviceInformationForUser
	getDeviceProperties
	getLastUser
	getManagedStatus
	getMasterKeyList
	getSoftwareInventory
	getStrongID
	getUserDevices
	isEnforceSSL
	isEnforceStrongAuthentication
	locateDevice
	lockDevice
	putDeviceProperties
	registerDeviceForUser
	removeDevice
	resetDeploymentState
	revoke
	unlockDevice

Web 服务定义语言 (WSDL) 名称	调用
	wipeDevice
	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	createOTP
	getAvailableEnrollmentModes
	getOtpInfo
	triggerNotification

XenMobile Mail Manager 10

May 05, 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。

以下是 XenMobile Mail Manager 10.0 的当前版本中的已知问题和已修复的问题。要下载 XenMobile Mail Manager，请转到 Citrix.com 中 XenMobile 10 Server 下的“服务器组件”部分。

- 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”。

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）。

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。

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 配置的添加和编辑屏幕。
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。

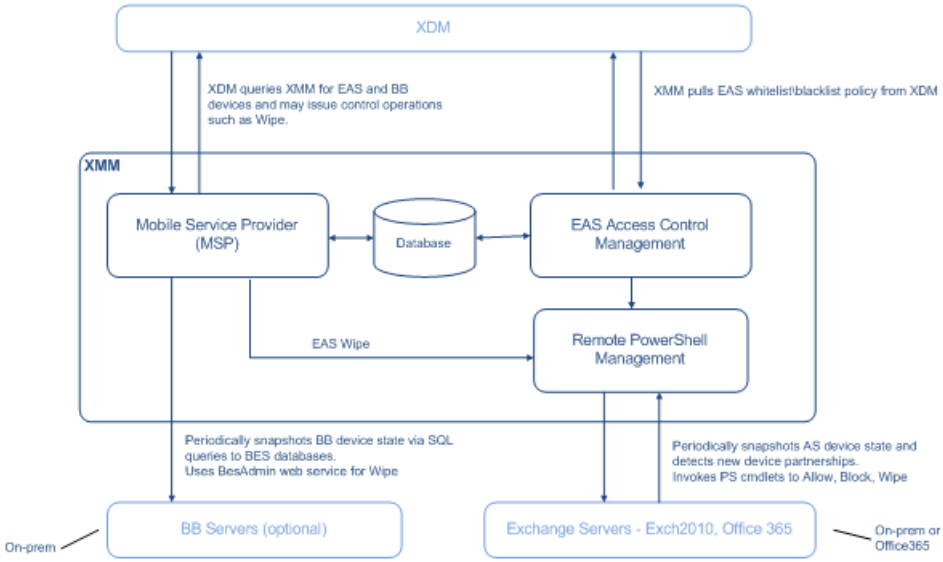
日志记录

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。

体系结构

May 05, 2016

下图显示了 XenMobile Mail Manager 的主要组件：



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。

系统要求和必备条件

May 05, 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 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 2013
- Exchange Server 2010 SP2

- 必须安装 Windows Management Framework。
  - PowerShell V4、V3 和 V2
- 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 的内部部署计算机的要求

- **权限**。Exchange 基于角色的访问控制 (RBAC) 不在本文档的范围内。话虽如此，至少，在 Exchange 配置 UI 中指定的凭据必须能够连接到 Exchange Server，并且具有执行以下指定 Exchange 的 PowerShell cmdlet 的完全权限：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- 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 http://technet.microsoft.com/en-us/library/dd315349.aspx，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。根据博客 http://blogs.msdn.com/b/powershell/archive/2009/11/23/you-don-t-have-to-be-an-administrator-to-run-remote-powershell-commands.aspx，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。
- 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 调查与远程管理相关的 Exchange 限制策略。

Office 365 Exchange 的要求

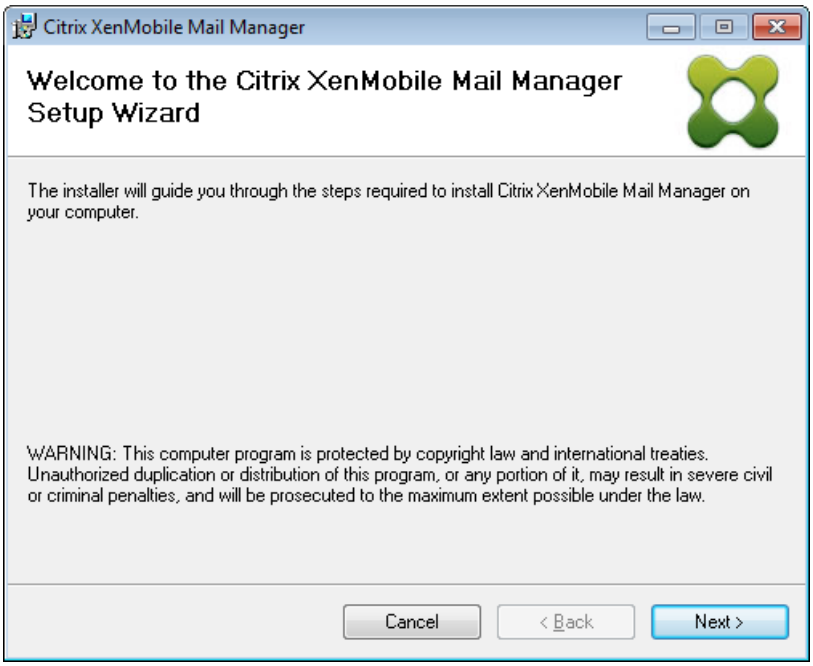
- **权限**。Exchange 基于角色的访问控制 (RBAC) 不在本文档的范围内。话虽如此，至少，在 Exchange 配置 UI 中指定的凭据必须能够连接到 Office 365，并且具有执行以下指定 Exchange 的 PowerShell cmdlet 的完全权限：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- 提供的凭据必须已获得授权，可以通过远程 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。

安装和配置

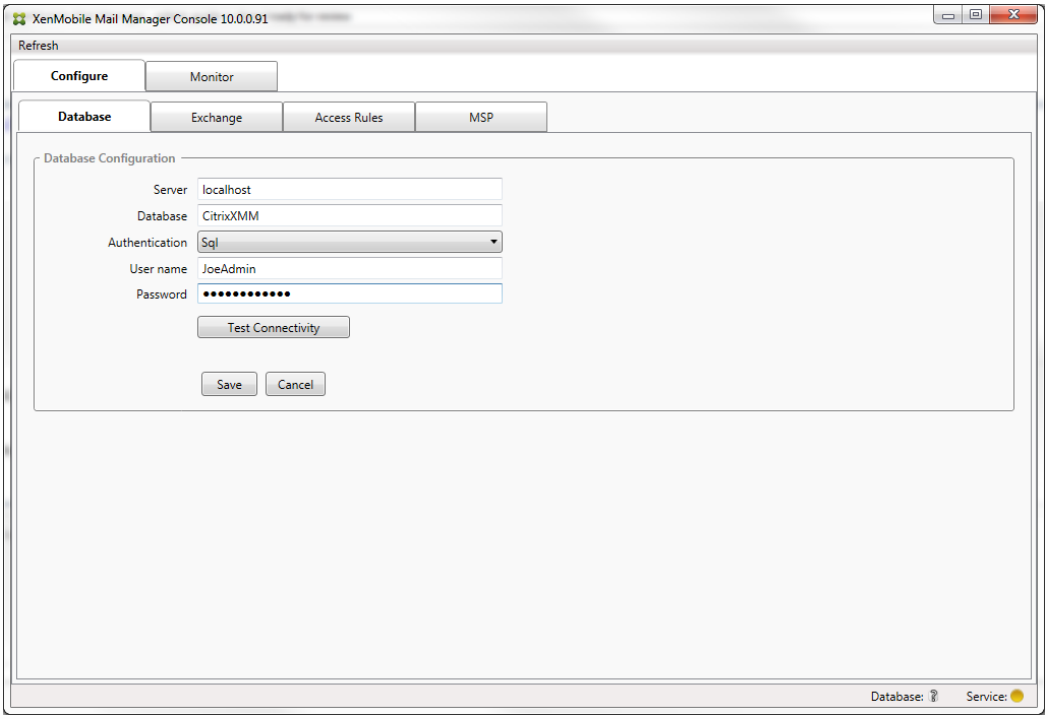
May 05, 2016

按照这些步骤安装并配置 XenMobile Mail Manager。开始前，请务必检查系统要求和必备条件。有关详细信息，请参阅XenMobile Mail Manager 系统要求和必备条件。

1. 单击 XmmSetup.msi 文件，然后按照安装程序中的提示安装 XenMobile Mail Manager。

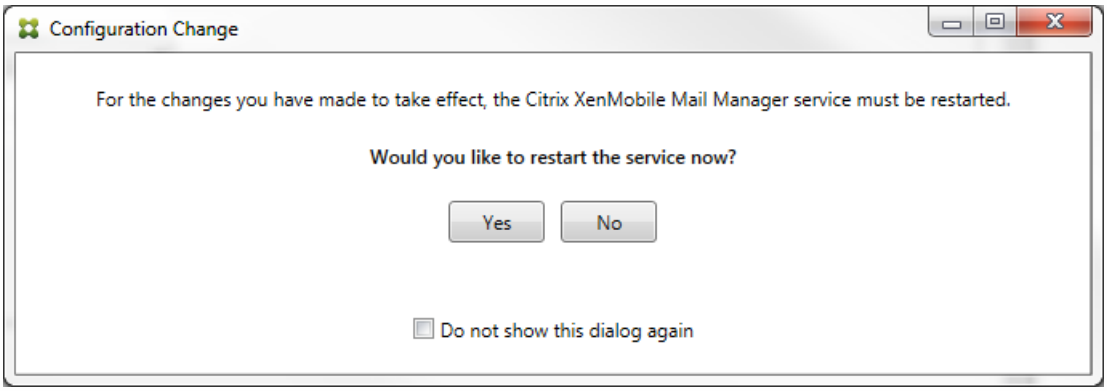


2. 从开始菜单中打开 XenMobile Mail Manager。
3. 配置以下数据库属性：
   1. 选择配置 > 数据库选项卡。
   2. 输入 SQL Server 的服务器名称（默认为 localhost）。
   3. 将数据库保留为默认 CitrixXmm。
   4. 选择以下用于 SQL 的身份验证模式之一：
      - Sql。输入有效 SQL 用户的用户名和密码。
      - Windows 集成。如果选择此选项，XenMobile Mail Manager Service 的登录凭据必须更改为具有访问 SQL Server 权限的 Windows 帐户。为此，请打开控制面板 > 管理工具 > 服务，在 XenMobile Mail Manager Service 条目上单击鼠标右键，然后单击登录选项卡。
        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。

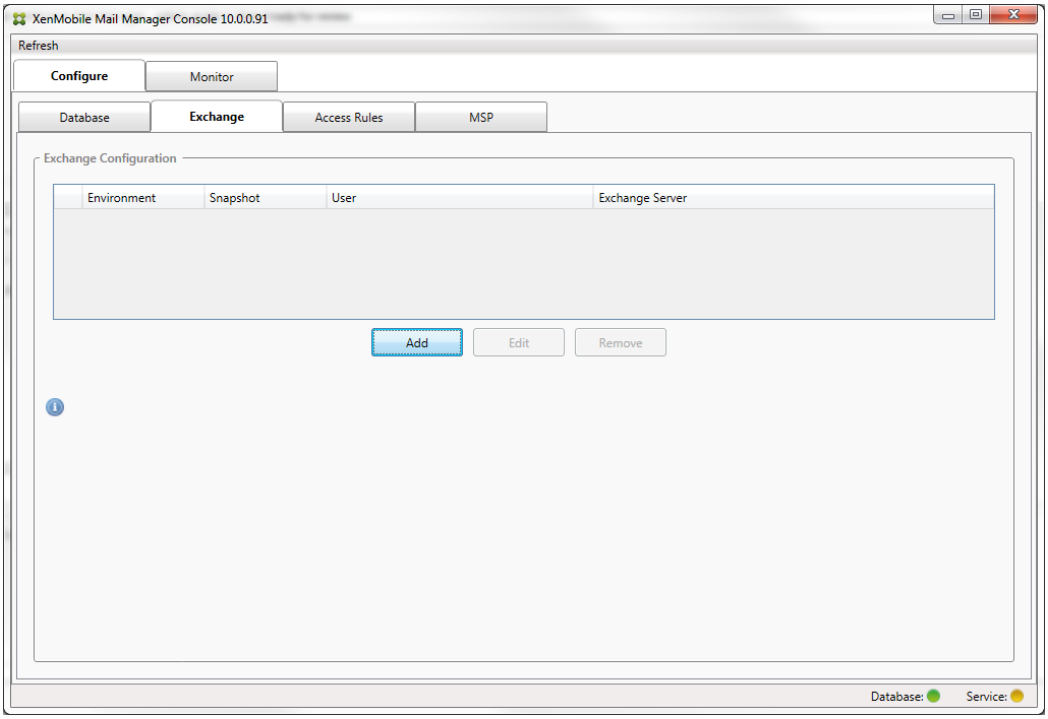


5. 单击测试连接检查是否可以连接到 SQL Server，然后单击保存。

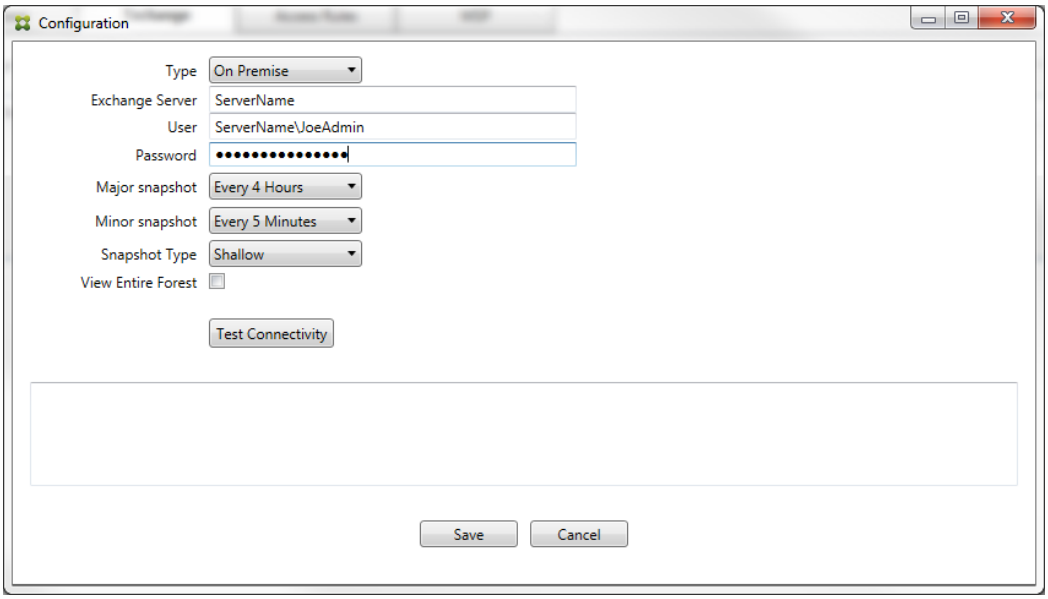
4. 此时将显示一条消息，提示您重新启动服务。 单击是。



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. 选择配置 > Exchange 选项卡。

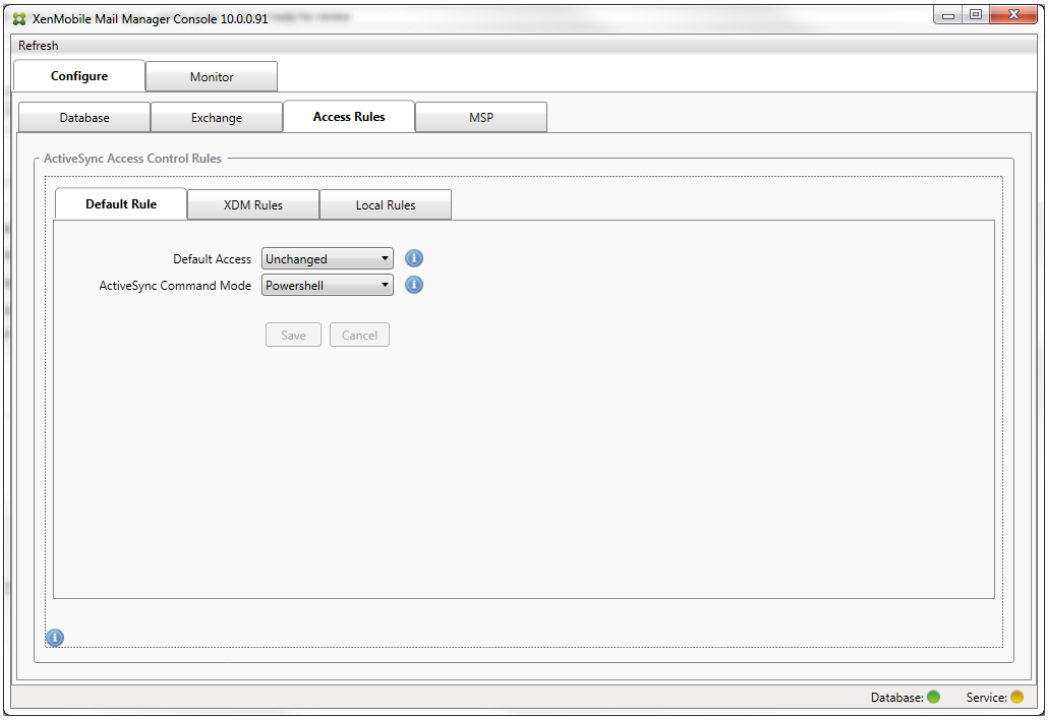


3. 单击添加。
4. 选择 Exchange Server 环境类型，On Premise（内部部署）或 Office 365。

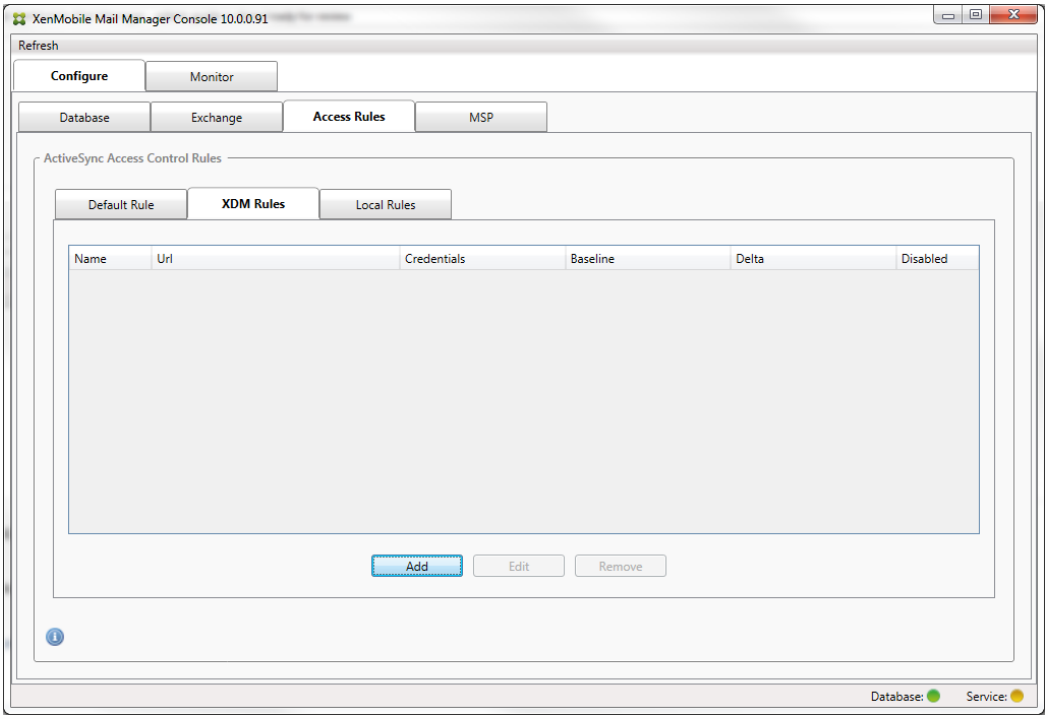


5. 如果选择 On Premise（内部部署），请输入要用于远程 Powershell 命令的 Exchange Server 的名称。
6. 输入在要求部分中指定的 Exchange Server 上具有适当权限的 Windows 身份的用户名。
7. 输入用户的密码。
8. 选择运行主要快照的计划。 主要快照检测每个 Exchange ActiveSync 合作关系。
9. 选择运行次要快照的计划。 次要快照检测新创建的 Exchange ActiveSync 合作关系。
10. 选择快照类型：Deep（深）或 Shallow（浅）。 浅快照通常更快并且足以执行 XenMobile Mail 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. 单击测试连接检查是否可以连接到 Exchange Server，然后单击保存。
12. 此时将显示一条消息，提示您重新启动服务。 单击是。

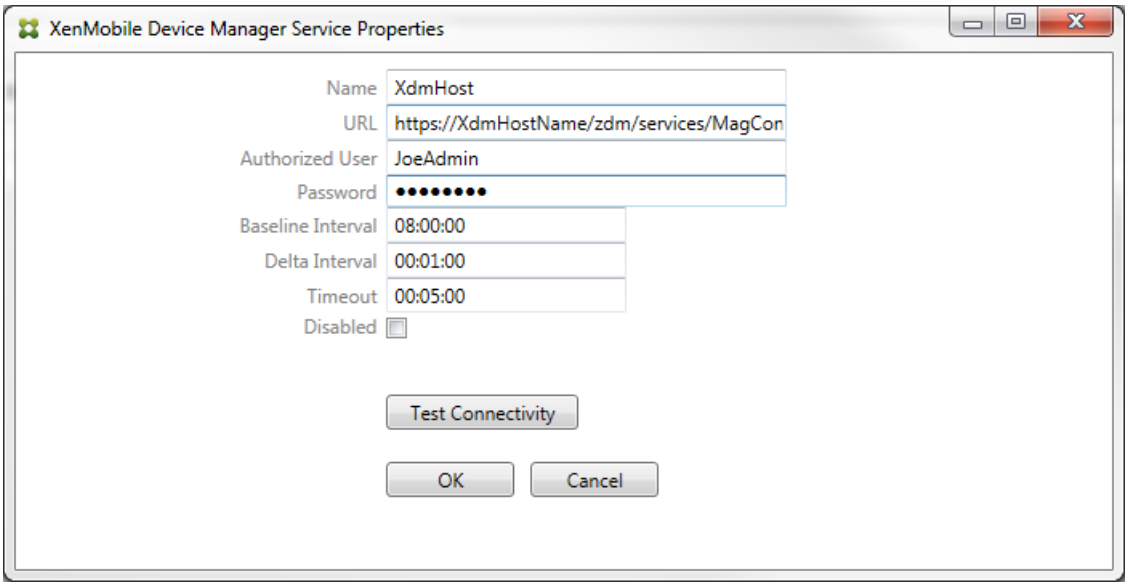
6. 配置访问规则：
    1. 选择配置 > 访问规则选项卡。



    2. 选择“Default Access”（默认访问）：允许、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。如果选择允许，将允许 ActiveSync 访问所有此类设备；如果选择阻止，将拒绝访问；如果选择 Unchanged（不更改），将不做更改。
    3. 选择 ActiveSync 命令模式：PowerShell 或 Simulation（模拟）。
        - 在 Powershell 模式中，XenMobile Mail Manager 会发出 Powershell 命令以执行所需的访问控制。
        - 在模拟模式中，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。在模拟模式中，用户随后可使用监视选项卡查看启用 Powershell 模式时会发生的情况。
    4. 单击保存。
7. 单击 XDM Rules（XDM 规则）选项卡。

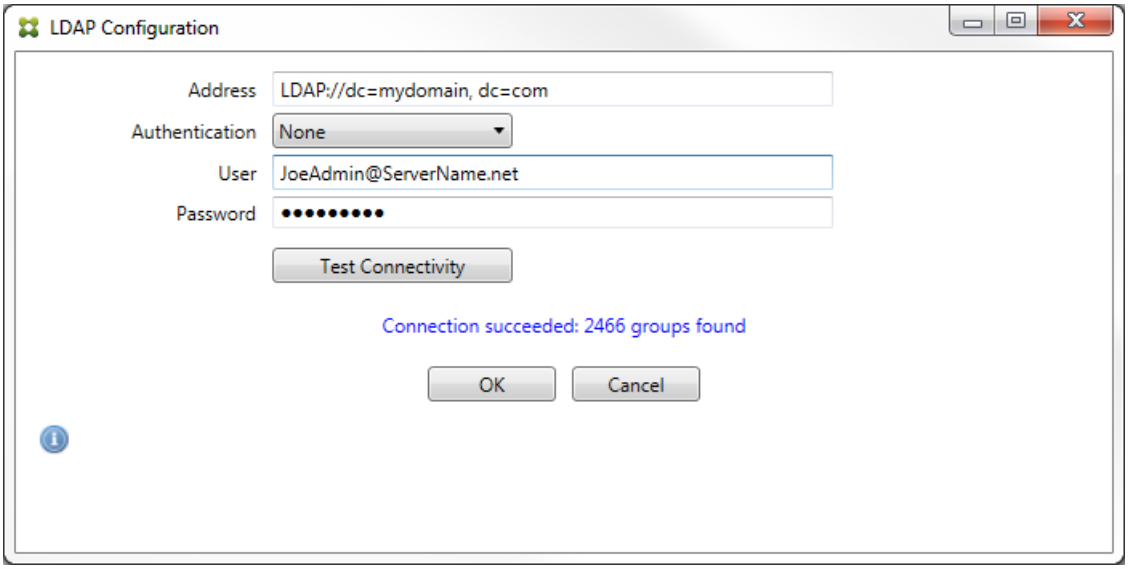


1. 单击添加。
2. 为 XDM 规则输入名称，例如 XdmHost。



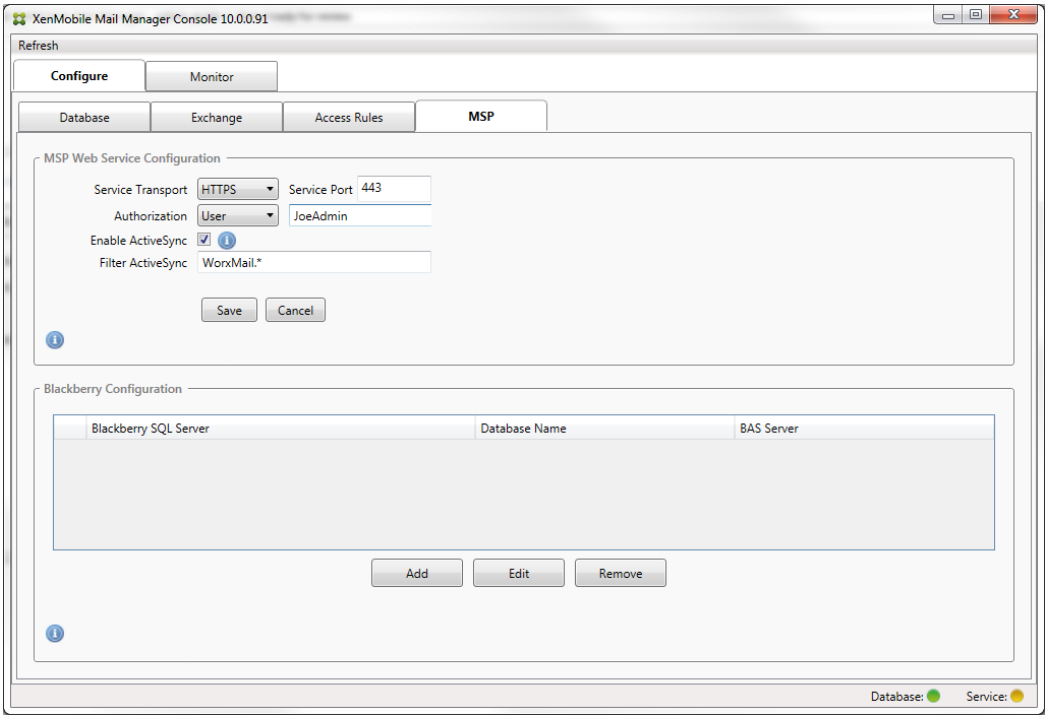
3. 修改 URL 字符串以引用 XenMobile 服务器；例如，如果服务器名称为 XdmHost，输入 http://XdmHostName/zdm/services/MagConfigService。
4. 在该服务器上输入授权用户。
5. 输入用户密码。
6. 保留 Baseline Interval（基准时间间隔）、Delta Interval（增量时间间隔）和 Timeout values（超时值）的默认值。
7. 单击测试连接，检查与服务器的连接。
   注意：如果选中“已禁用”复选框，XenMobile Mail Service 将不会从 XenMobile 服务器收集策略。
8. 单击确定。

8. 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。



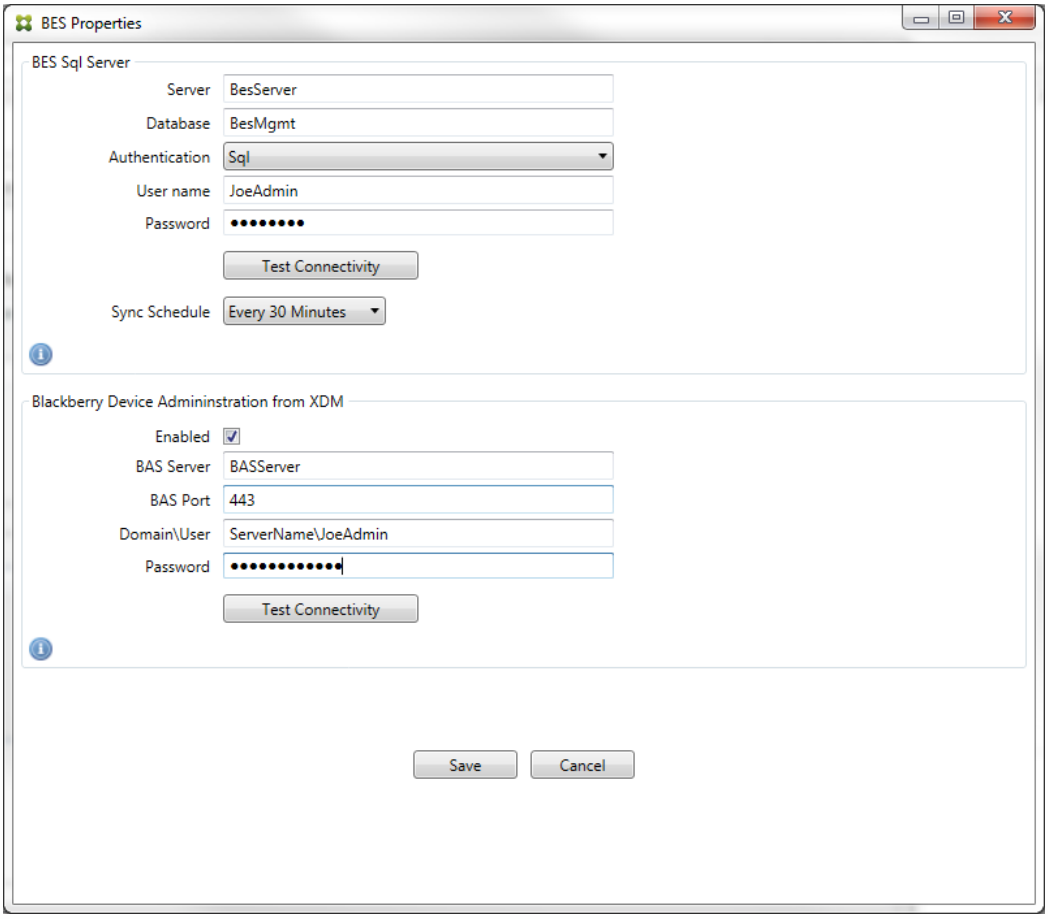
2. 您可以基于 ActiveSync Device ID（ActiveSync 设备 ID）、设备类型、AD Group（AD 组）、用户或设备 UserAgent（用户代理）添加本地规则。 在列表中选择适当的类型。 有关详细信息，请参阅 XenMobile Mail Manager 访问控制规则。
3. 在文本框中输入文本或文本片段。 也可单击查询按钮，查看与片段匹配的实体。
   注意：对于除组以外的所有类型，系统依赖在快照中找到的设备。因此，如果刚刚开始且尚未完成快照，则没有实体可用。
4. 选择一个文本值，然后单击允许或拒绝，将其添加到右侧的 Rule List（规则列表）窗格中。 可使用 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”，则 Matt 的 iPad 将仍被允许，因为“iPad”规则比“Matt”规则具有更高的有效优先级。
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，请单击分析。
6. 单击保存。

9. 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. 选择配置 > MSP 选项卡。



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）；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. 单击保存。

10. 另外，可以配置一个或多个黑莓 Enterprise Server (BES)：
    1. 单击添加。
    2. 输入 BES SQL Server 的服务器名称。



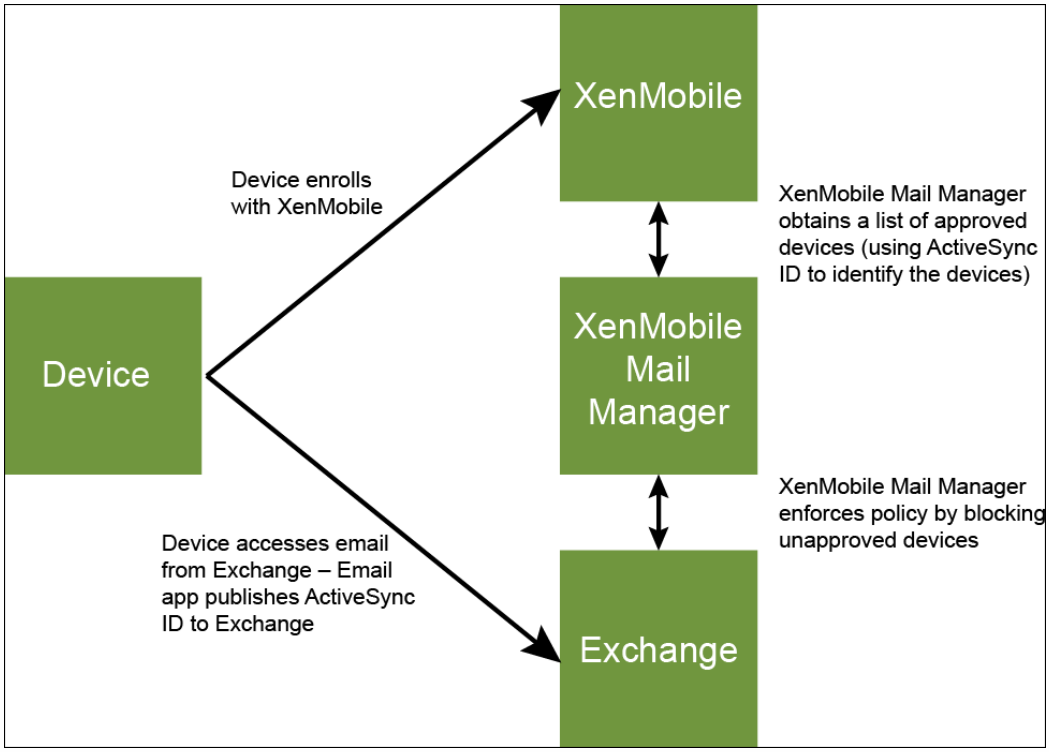
3. 输入 BES Management 数据库的数据库名称。
4. 选择身份验证模式。 如果选择 Windows 集成身份验证，则 XenMobile Mail Manager Service 的用户帐户就是用于连接 BES SQL Server 的帐户。
   注意：如果还为 XenMobile Mail Manager 数据库连接选择了 Windows 集成，则必须同时为此处指定的 Windows 帐户提供 XenMobile Mail Manager 数据库的访问权限。
5. 如果选择 SQL authentication（SQL 身份验证），请输入用户名和密码。
6. 设置 Sync 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. 单击测试连接，检查与 SQL Server 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 Service 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. 单击测试连接，测试与 BES 的连接。
   5. 单击保存。

使用 ActiveSync ID 强制执行电子邮件策略

May 05, 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。

访问控制规则

May 05, 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，任何时候单击取消按钮都会将规则列表还原回首次打开时的状态。除非单击保存，否则关闭配置工具时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、XDM 规则和默认访问规则。

Local rules（本地规则）：本地规则具有最高优先级：如果设备与本地规则匹配，规则评估将停止。既不查询 XDM 规则又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。

XDM rules（XDM 规则）：XDM 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。

Default access rule（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 XDM 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 XDM 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 XDM 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 XDM 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
- XDM 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，则不会根据任意 XDM 规则或默认访问规则对该设备进行

评估。这同样适用于给定的规则类型。例如，如果在本地规则列表中的某个给定设备有多个匹配项，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。

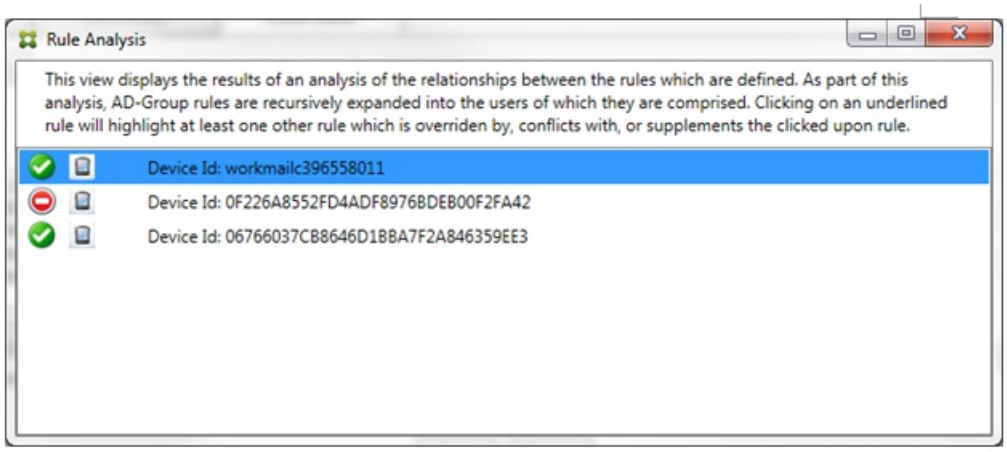
在为相同的字段定义了多条规则的情况下，分析特别有用。您可以对规则之间的关系进行故障排除。请从规则字段的角度来执行分析；例如，规则是在组中基于匹配的字段进行分析的（例如 ActiveSync 设备 ID、ActiveSync 设备类型、用户、用户代理等）。

规则术语：

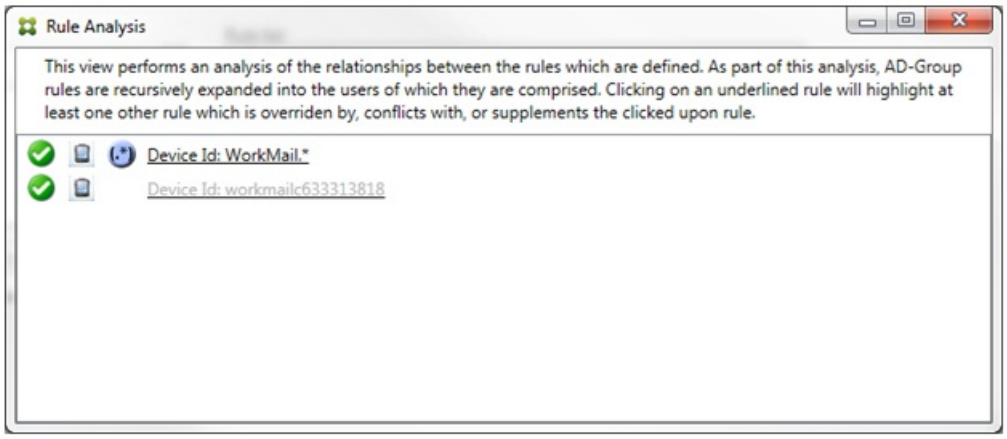
- **覆盖规则**。当多条规则可以应用到同一设备时会发生覆盖。因为规则是按照列表中的优先级进行评估的，可能会应用的后面的规则实例可能永远不会被评估。
- **冲突规则**。当多条规则可以应用到同一设备但访问状态（允许/阻止）不匹配时会发生冲突。如果冲突规则不是正则表达式规则，冲突将始终隐式包含覆盖
- **补充规则**。当多条规则是正则表达式规则时会发生补充，因此可能需要确保两个（或多个）正则表达式可以合并为一个正则表达式，或者不复制功能。补充规则的访问状态（允许/阻止）可能还会发生冲突。
- **主要规则**。主要规则是已在对话框内单击的规则。规则通过围绕它的实线框可视化地指示出来。该规则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

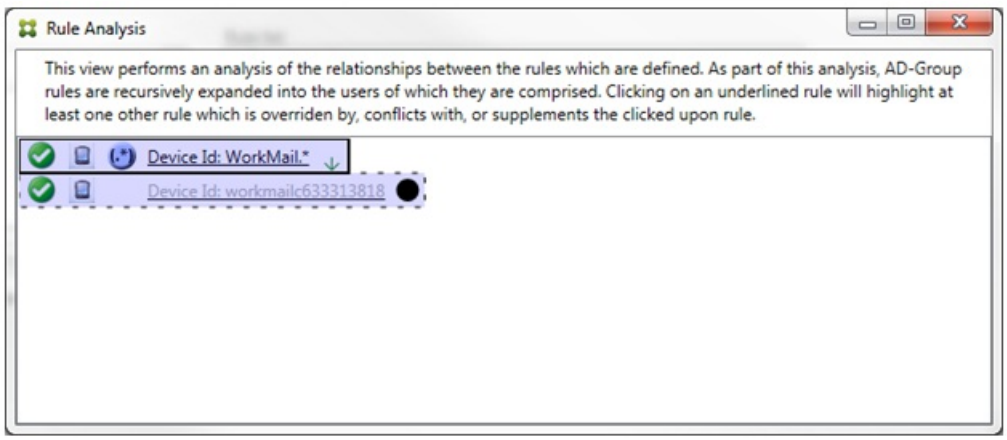
当没有冲突、覆盖或补充时，Rule Analysis （规则分析）对话框中不包含带有下划线的条目。单击任何没有影响的项目；例如，正常选定项目的视觉效果将会出现。



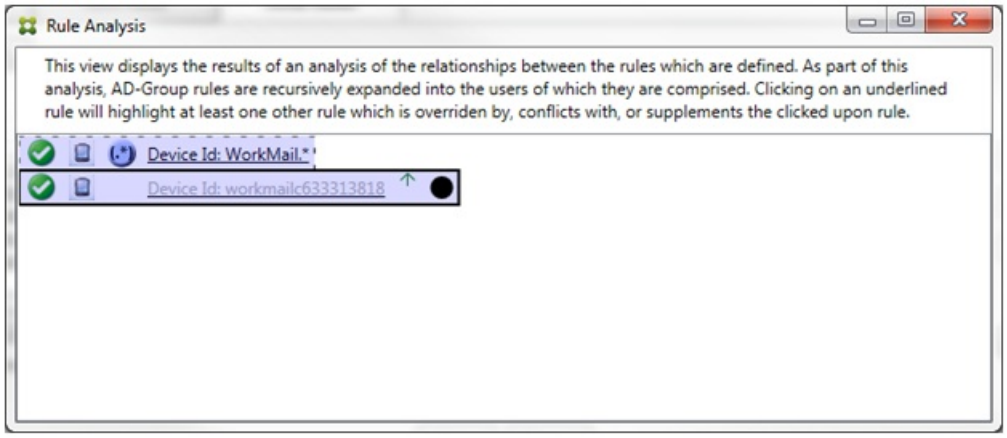
当出现覆盖时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。至少有一条辅助规则将以较浅字体显示，指示该规则已被优先级较高的规则覆盖。您可以单击覆盖的规则以了解覆盖该规则的一条或多条规则。任何时间覆盖的规则都由于规则是主要规则或辅助规则而突出显示，并且将在它旁边将显示一个黑色圆圈，以进一步指示该规则处于不活动状态。例如，在单击该规则之前，对话框显示如下：



单击优先级最高的规则时，对话框显示如下：

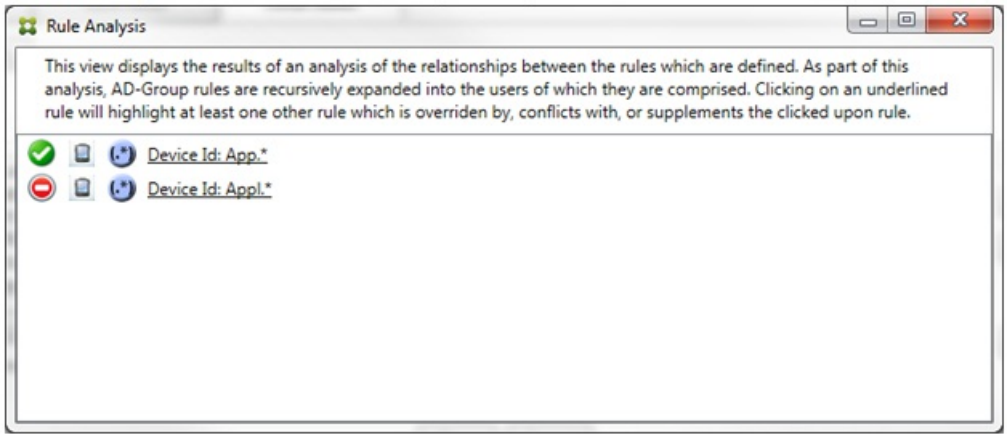


在此示例中，正则表达式规则 WorkMail.* 是主要规则（以实线框指示），常规规则 workmailc633313818 是辅助规则（以虚线框指示）。辅助规则旁边的黑点是一个视觉提示，可进一步指示由于它的前面有较高优先级的正则表达式而处于不活动状态（永远不会被评估）。单击覆盖的规则后，对话框显示如下：

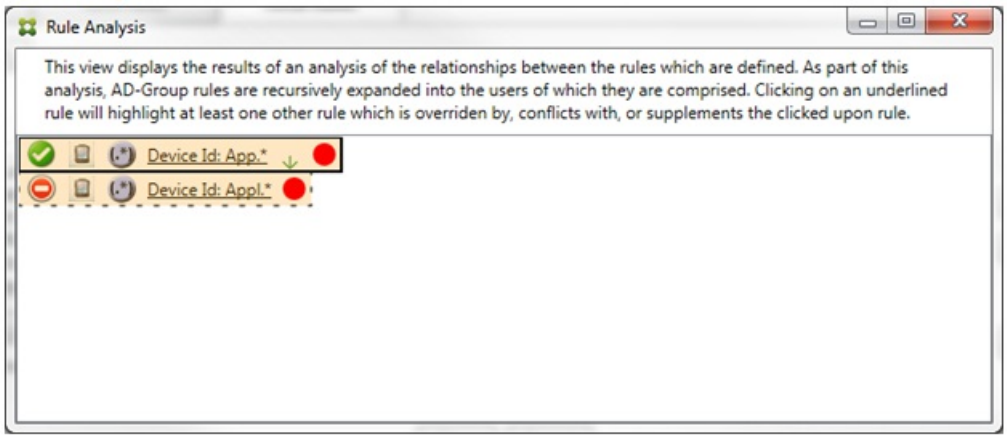


在上例中，正则表达式规则 WorkMail.* 是辅助规则（以虚线框指示），常规规则 workmailc633313818 是主要规则（以实线框指示）。对于这一简单的示例，没有太大差异。对于更为复杂的示例，请参阅本主题中后面所述的复杂表达式示例。在定义了许多规则的情景中，单击覆盖的规则将快速识别已覆盖该规则的一条或多条规则。

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：

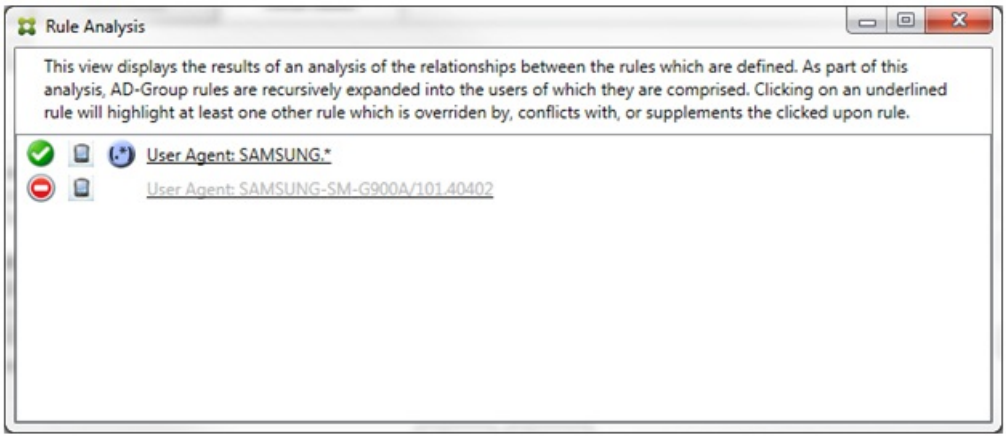


检查这两条正则表达式规则即可明显发现，第一条规则允许设备 ID 包含“App”的所有设备，第二条规则拒绝设备 ID 包含 Appl 的所有设备。此外，即使第二条规则拒绝了设备 ID 包含 Appl 的所有设备，也不会拒绝符合条件的设备，因为允许规则的优先级较高。单击第一条规则后，对话框显示如下：



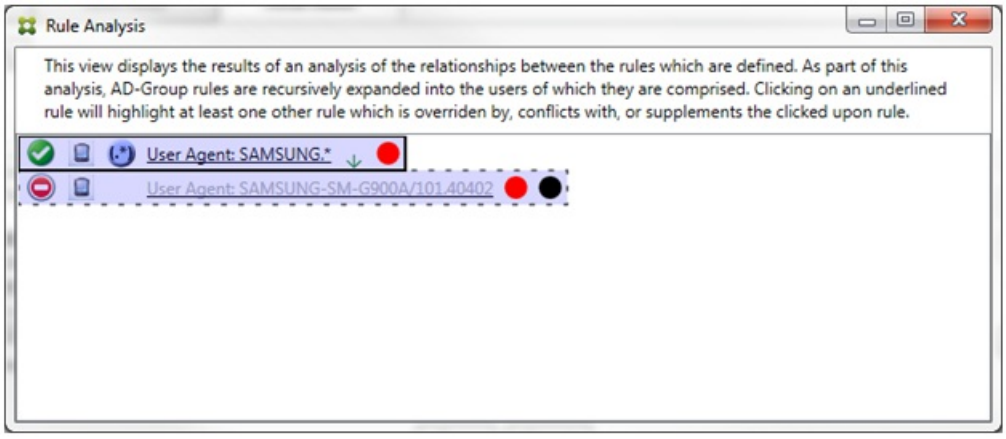
在上述情景中，主要规则（正则表达式规则 App.*）和辅助规则（正则表达式规则 Appl.*）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

在同时存在冲突和覆盖的情景中，主要规则（正则表达式规则 App.*）和辅助规则（正则表达式规则 Appl.*）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。



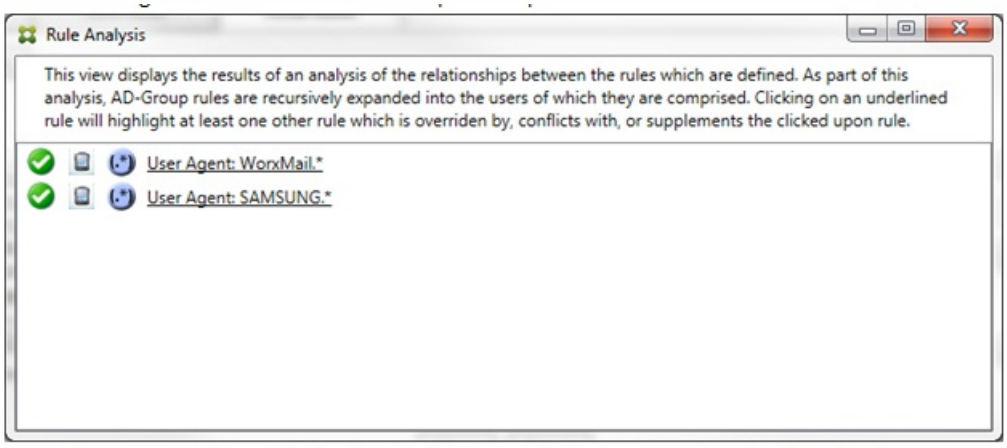
在上例中，显而易见，第一条规则（正则表达式规则 SAMSUNG.*）不仅覆盖下一条规则（常规规则 SAMSUNG-SM-G900A/101.40402），而且这两条规则的访问状态有所不同（主要规则指定“允许”，辅助规则指定“阻止”）。第二条规则（常规规则 SAMSUNG-SM-G900A/101.40402）以较浅文本显示，指示该规则已被覆盖，并因此处于不活动状态。

单击正则表达式规则后，对话框显示如下：

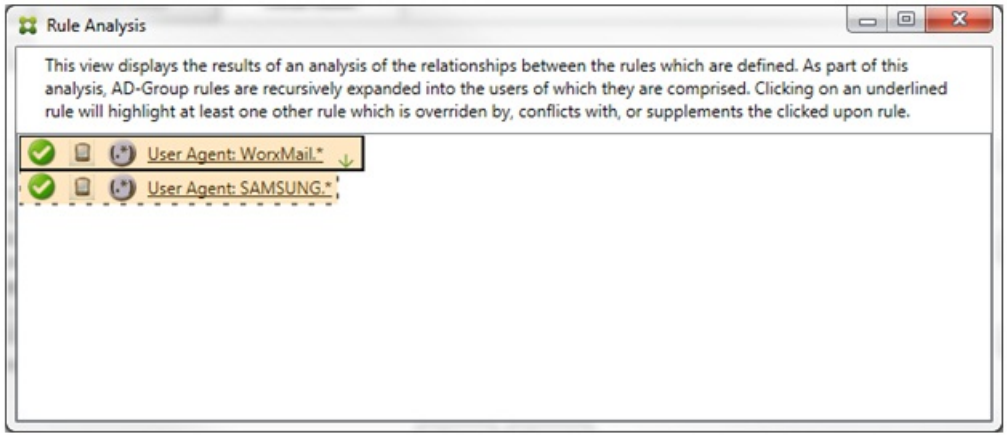


主要规则（正则表达式规则 SAMSUNG.*）后跟一个红点，指示其访问状态与一条或多条辅助规则发生冲突。辅助规则（常规规则 SAMSUNG-SM-G900A/101.40402）后跟一个红点，指示其访问状态与主要规则发生冲突，以及如果后跟黑点，则进一步指示该规则已被覆盖，并因此处于不活动状态。

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：



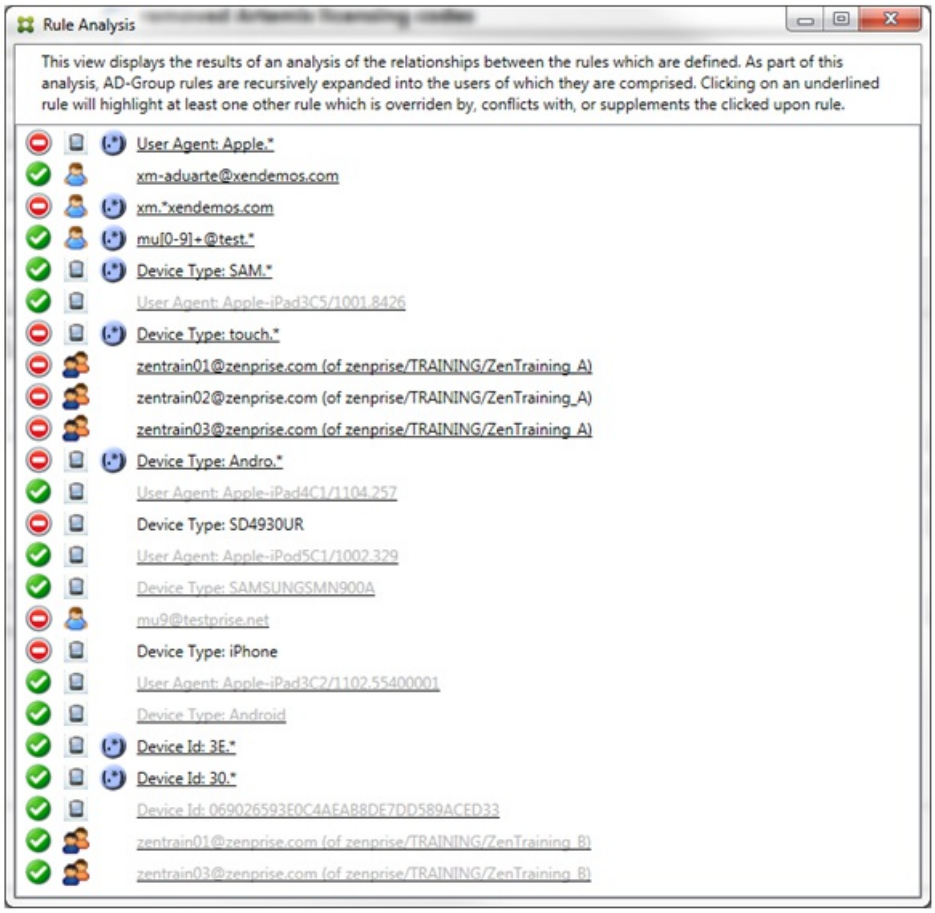
目测会很容易发现这两条规则都是正则表达式规则，都已应用到 XenMobile Mail Manager 中的 ActiveSync 设备 ID 字段。单击第一条规则后，对话框显示如下：



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

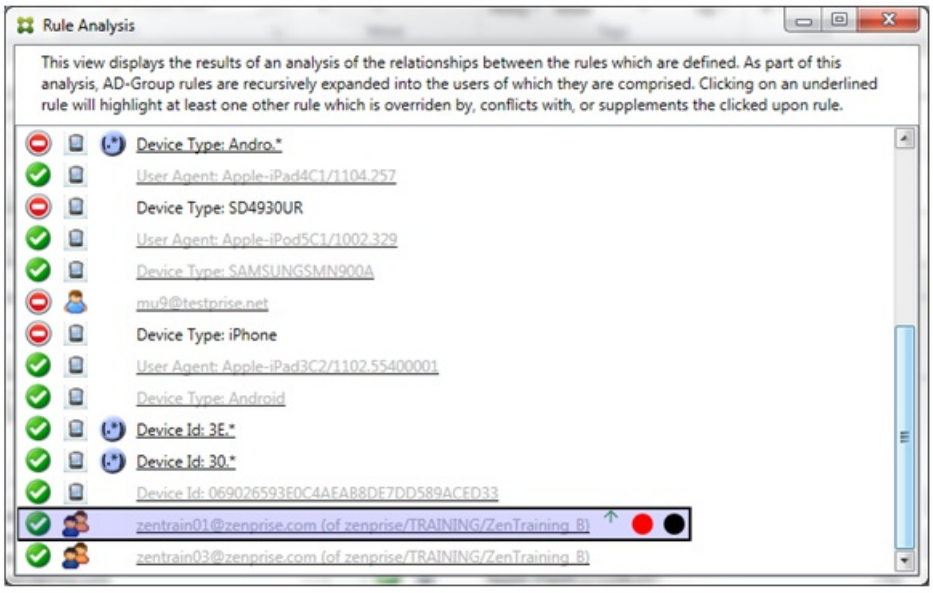
许多潜在的覆盖、冲突或补充都可能会发生，使其不可能举例说明所有可能的情景。下例探讨了不会执行的操作，同时还阐明了规则分析视觉构建的强大功能。大多数项目在下图中加了下划线。许多项目以较浅的字体显示，指示存在问题的规则已被优先级较高的规则以某种方式覆盖。多条正则表达式规则也包括在列表中，由 (.*) 图标指示。



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。

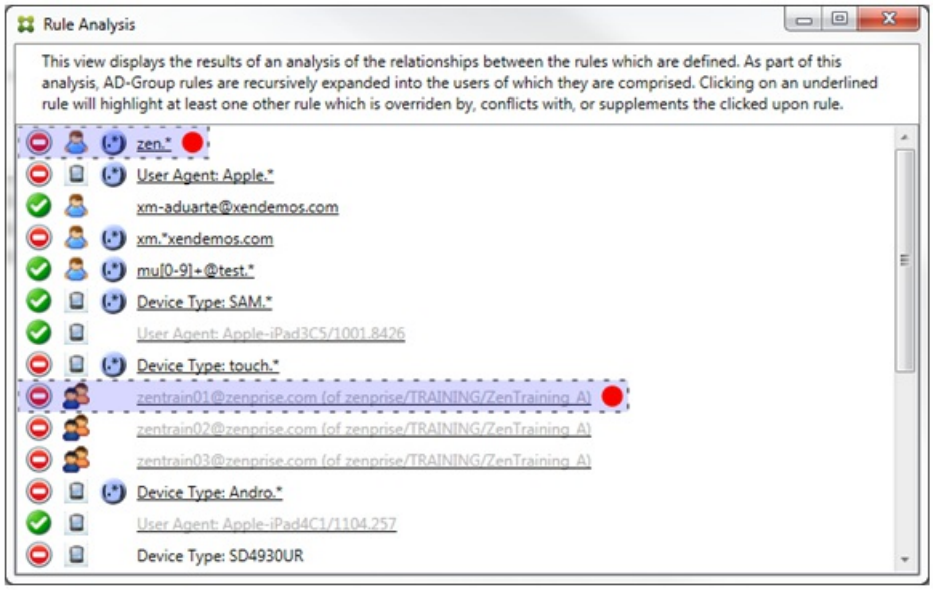
示例 1：本示例调查了覆盖 zentrain01@zenprise.com 的原因。



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：

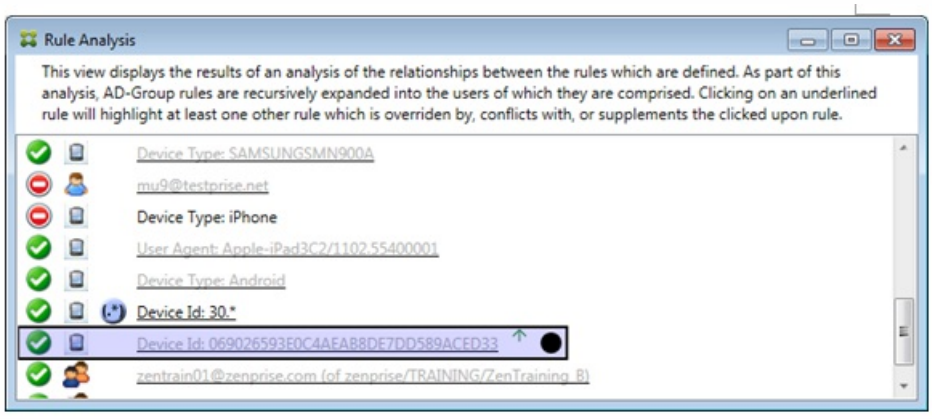
- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示一条或多条辅助规则都能够在该箭头上方找到）。
- 后跟一个红色圆圈和一个黑色圆圈，分别指示一条或多条辅助规则与其访问状态存在冲突，并且主要规则已被覆盖且因此处于不活动状态。

向上滚动时，您会看到以下内容：



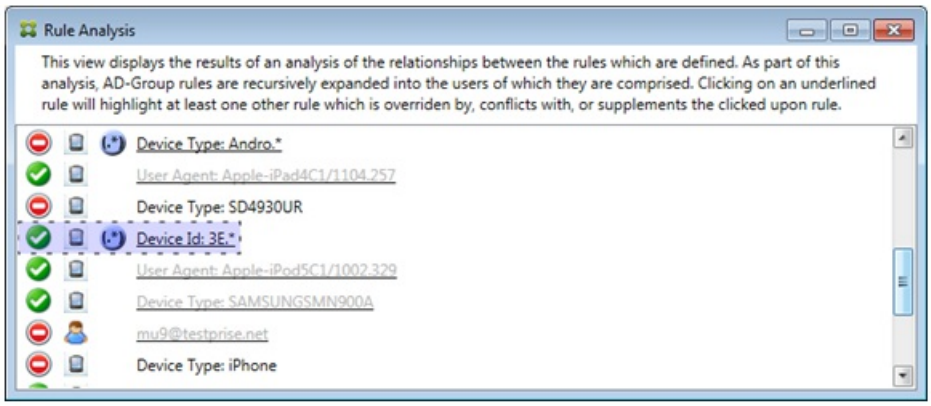
在这种情况下，有两条辅助规则覆盖主要规则：正则表达式规则 zen.* 和常规规则 zentrain01@zenprise.com（属于 zenprise/TRAINING/ZenTraining A）。对于后一条辅助规则，出现了以下情况：Active Directory 组规则 ZenTraining A 包含用户 zentrain01@zenprise.com，Active Directory 组规则 ZenTraining B 也包含用户 zentrain01@zenprise.com。但是，由于辅助规则的优先级高于主要规则，因此主要规则被覆盖。主要规则的访问状态是“允许”，并且由于这两条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访问冲突。

示例 2：此示例显示了覆盖 ActiveSync 设备 ID 为 069026593E0C4AEAB8DE7DD589ACED33 的设备的原因：



主要规则（常规设备 ID 规则 069026593E0C4AEAB8DE7DD589ACED33）具有以下特性：

- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示辅助规则能够在该箭头上方找到）。
- 后跟一个黑色圆圈，指示辅助规则已覆盖主要规则，并因此处于非活动状态。

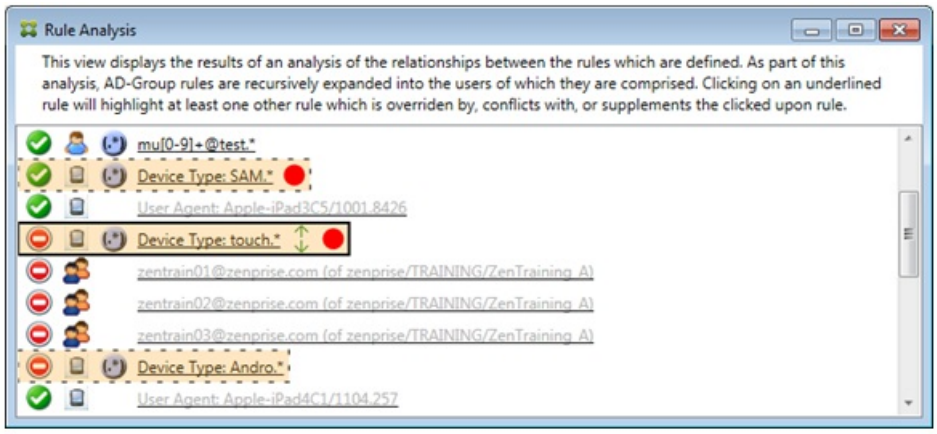


在这种情况下：一条辅助规则将覆盖主要规则：正则表达式 ActiveSynce 设备 ID 规则 3E.*。由于正则表达式 3E.* 将与 069026593E0C4AEAB8DE7DD589ACED33 匹配，因此，主要规则永远不会被评估。

如何分析补充和冲突

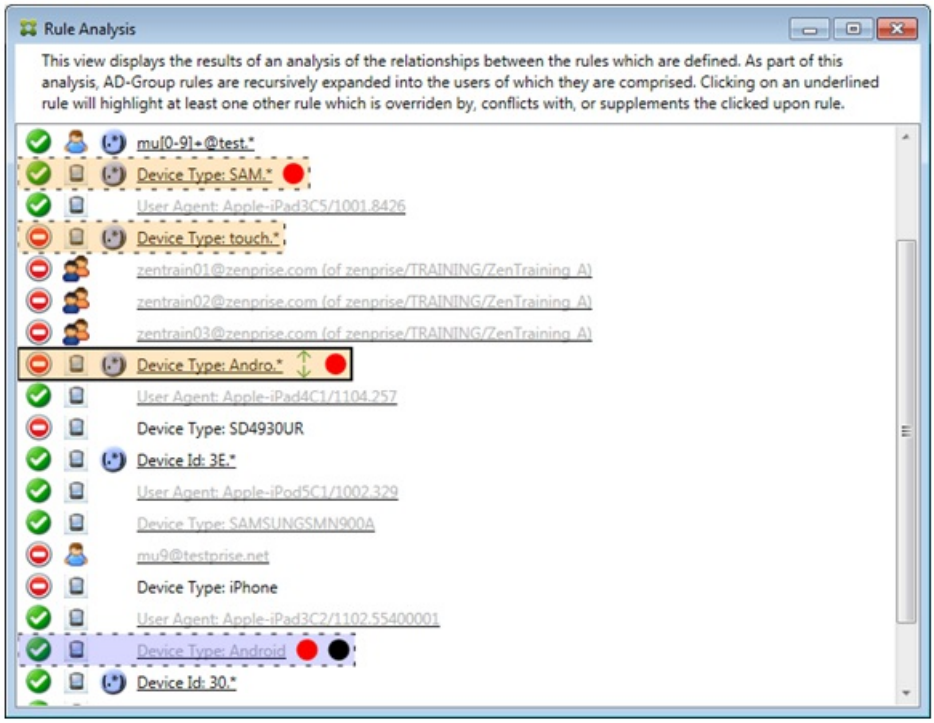
在这种情况下，主要规则是正则表达式 ActiveSync 设备类型规则 touch.*。特性如下：

- 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。
- 在此类情景中，您应确保其正则表达式规则不冗余。



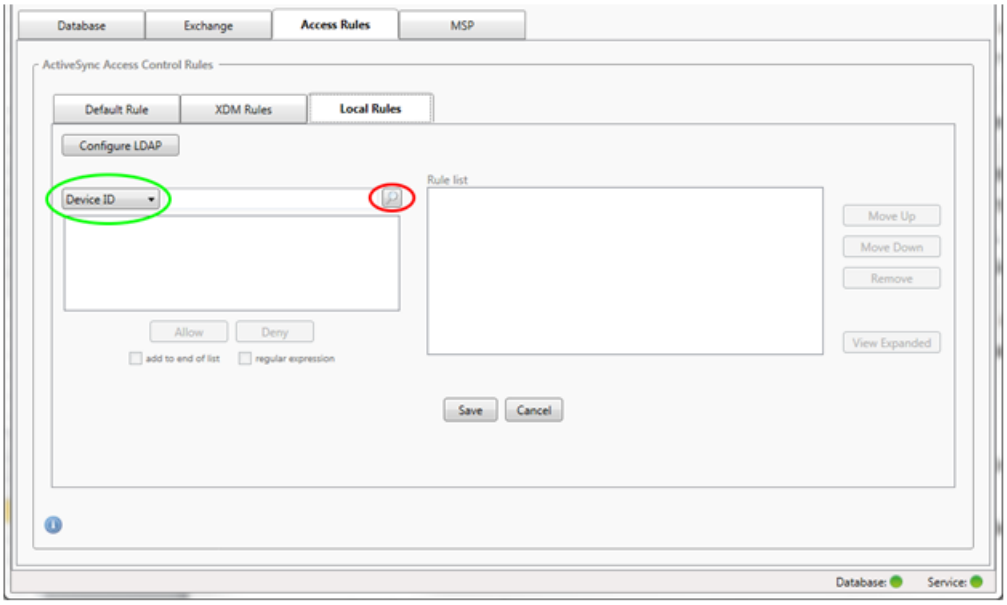
如何进一步分析规则

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。

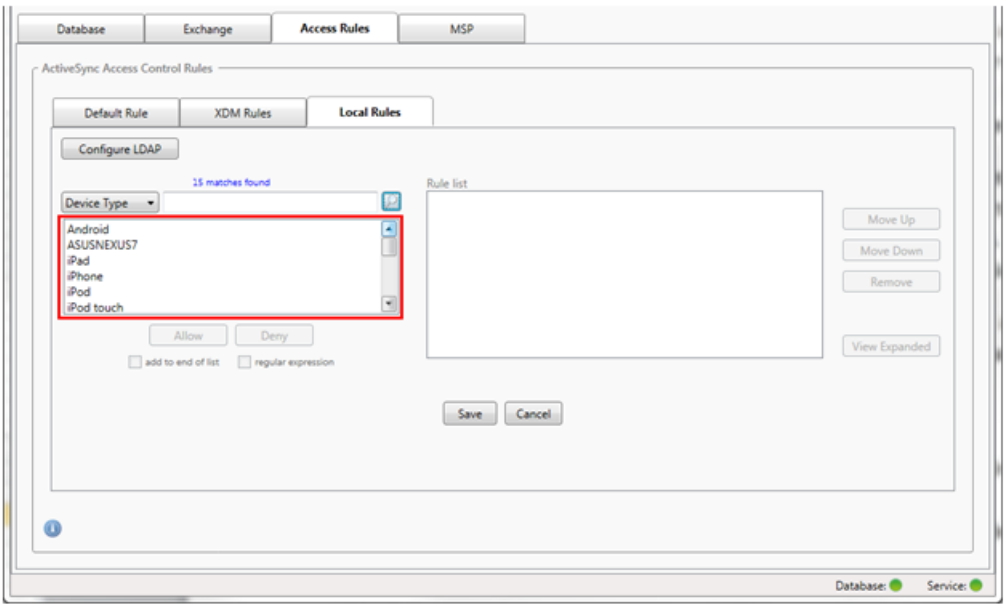


此示例显示了规则关系中包含的覆盖规则。此规则是常规 ActiveSync 设备类型规则 Android，已被覆盖（通过旁边的浅色字体和黑色圆圈指示）并且其访问状态还与主要规则正则表达式 ActiveSync 设备类型规则 Andro.* 发生冲突；在单击该规则之前，该规则是辅助规则。在上例中，常规 ActiveSync 设备类型规则 Android 未显示为辅助规则，因为从主要规则（正则表达式 ActiveSync 设备类型规则 touch.*）的角度来看，该规则与主要规则不相关。

1. 单击 Access Rules（访问规则）选项卡。

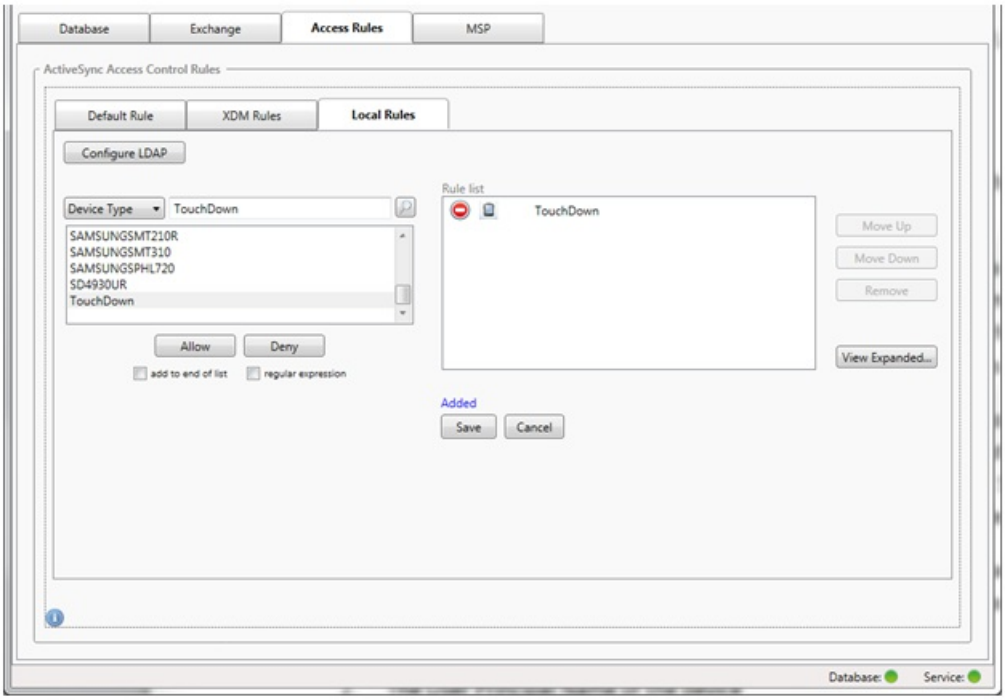


2. 在设备 ID 列表中，选择要为其创建本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。 在此示例中，已选择设备类型字段，选项显示在下面的列表框中。



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。

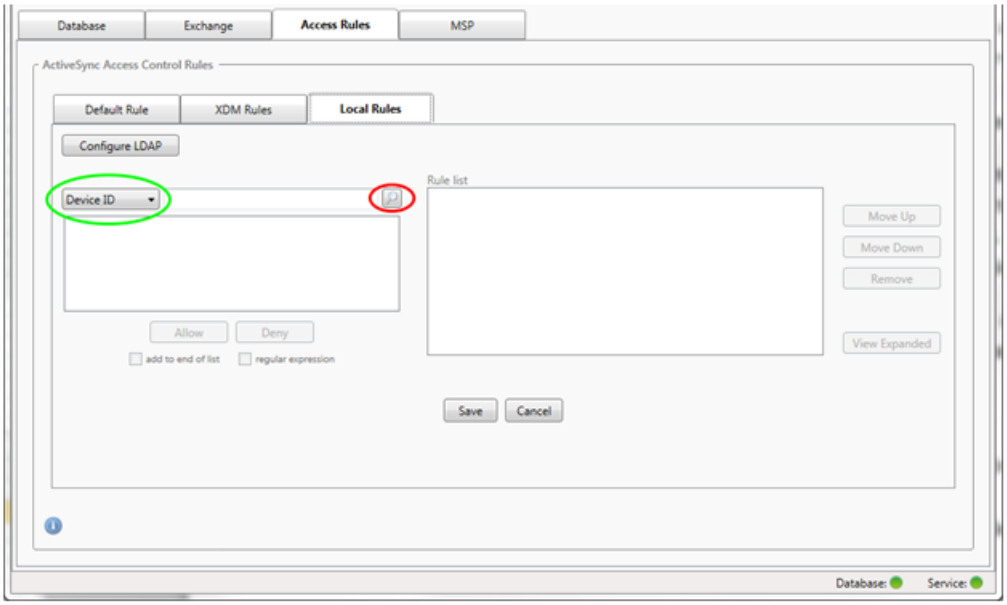
   在此示例中，设备类型为 TouchDown 的所有设备将被拒绝访问。



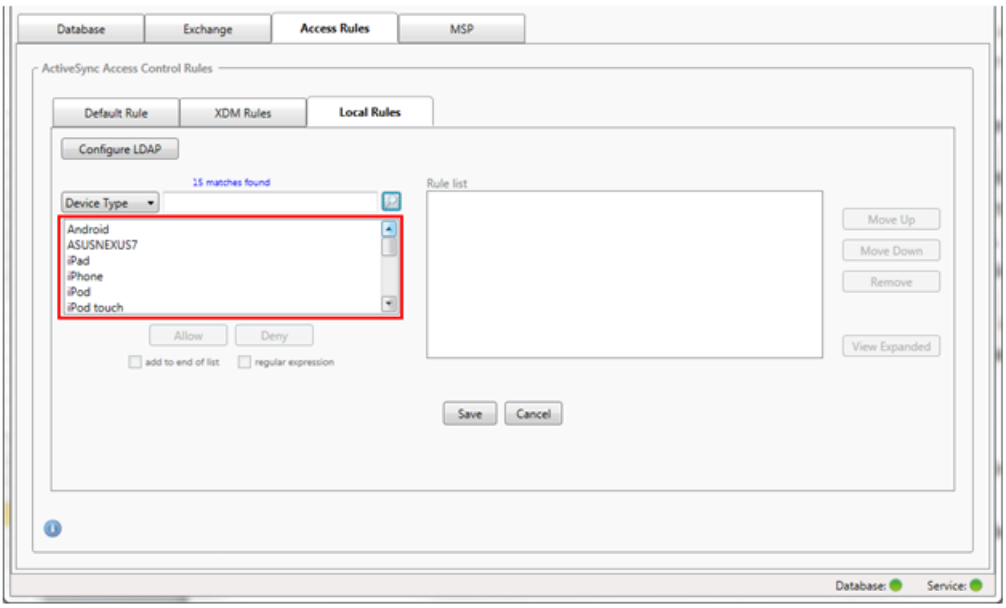
正则表达式本地规则可通过其旁边显示的图标进行区分 - (.*)。要添加正则表达式规则，您可以通过给定字段的结果列表中的现有值来构建正则表达式规则（只要已完成主要快照），或只需键入您想要的正则表达式。

从现有字段值构建正则表达式

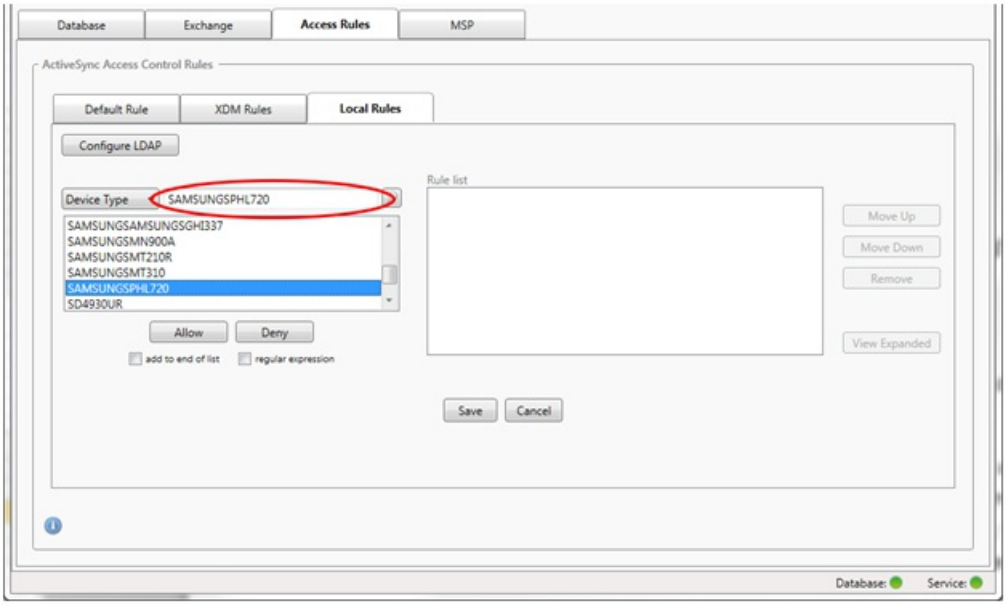
1. 单击 Access Rules（访问规则）选项卡。



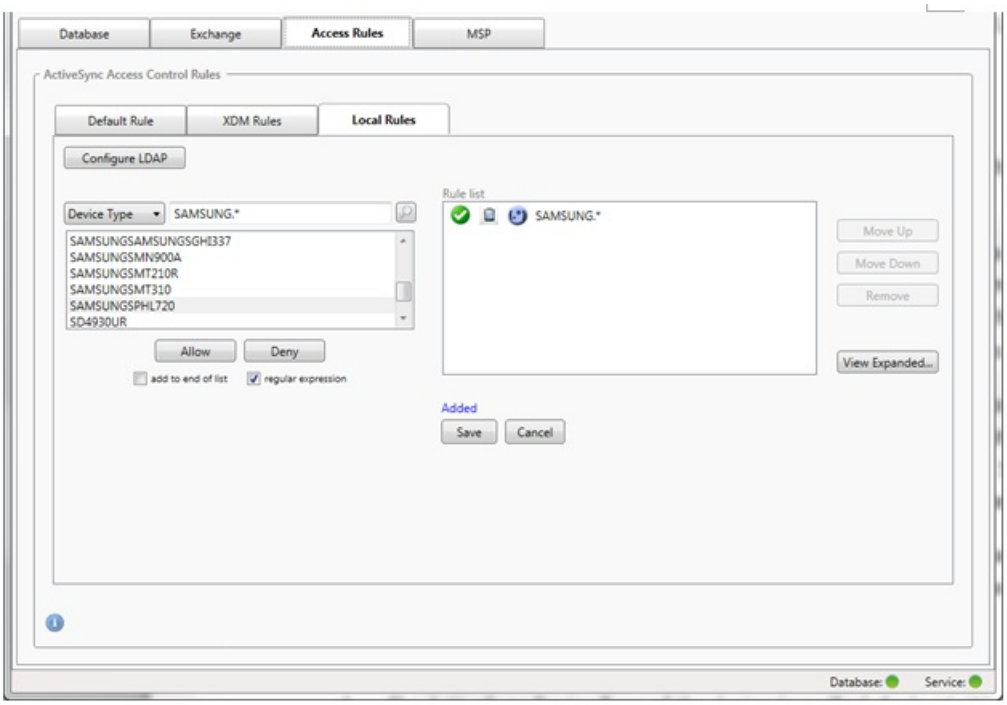
2. 在设备 ID 列表中，选择要为其创建正则表达式本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。 在此示例中，已选择设备类型字段，选项显示在下面的列表框中。



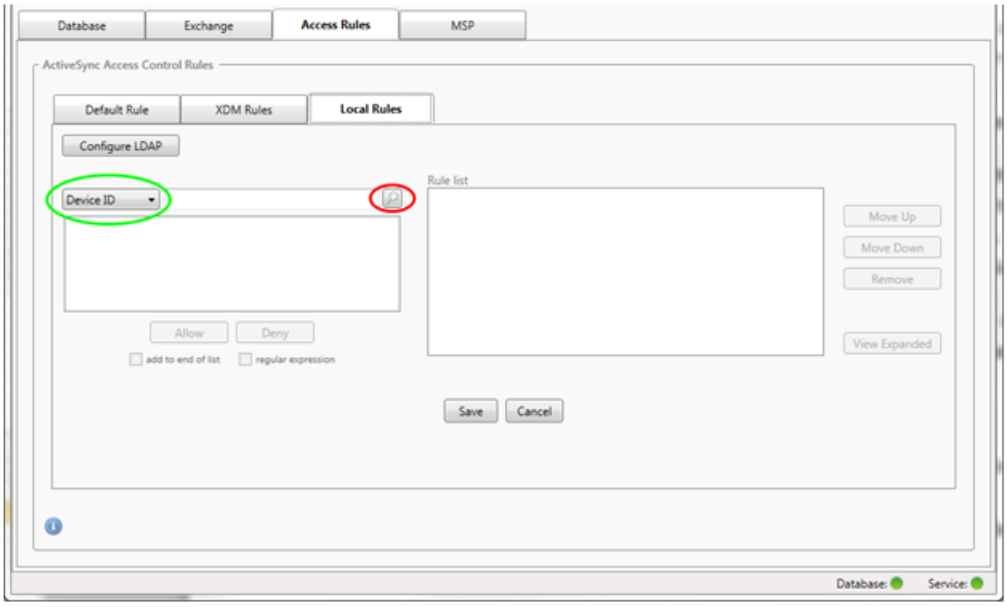
4. 单击结果列表中的其中一个项目。 在此示例中，已选择 SAMSUNGSPHL720，并显示在设备类型旁边的文本框中。



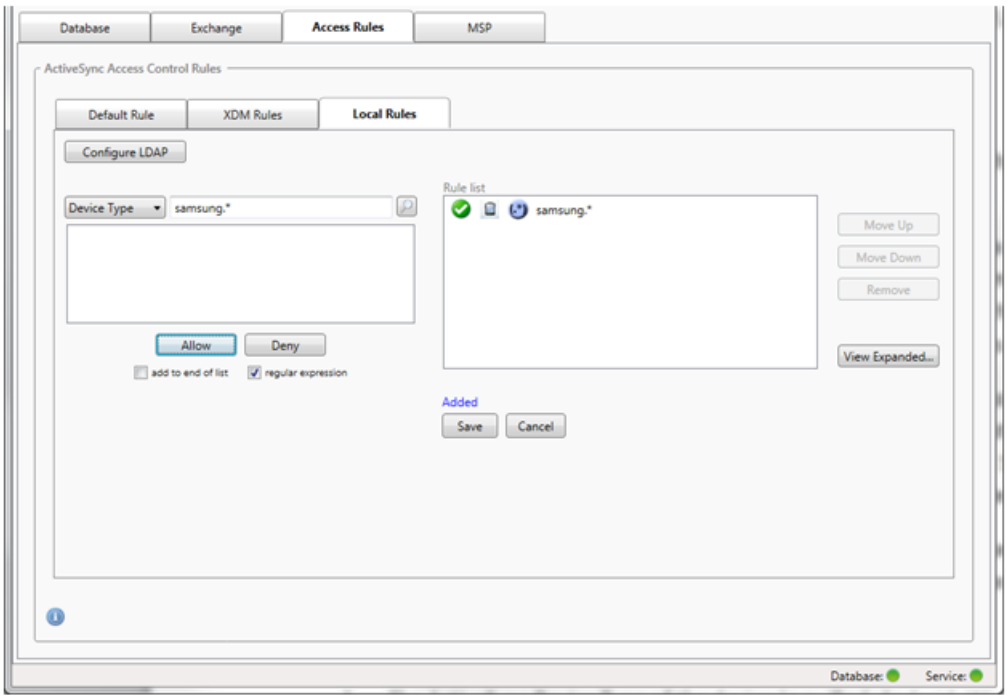
5. 要允许设备类型值中包含“Samsung”的所有设备，请按照以下步骤添加正则表达式规则：
   1. 在所选项目文本框内单击。
   2. 将文本从 SAMSUNGSPHL720 更改为 SAMSUNG.*
   3. 确保选中正则表达式复选框。
   4. 单击允许。



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。

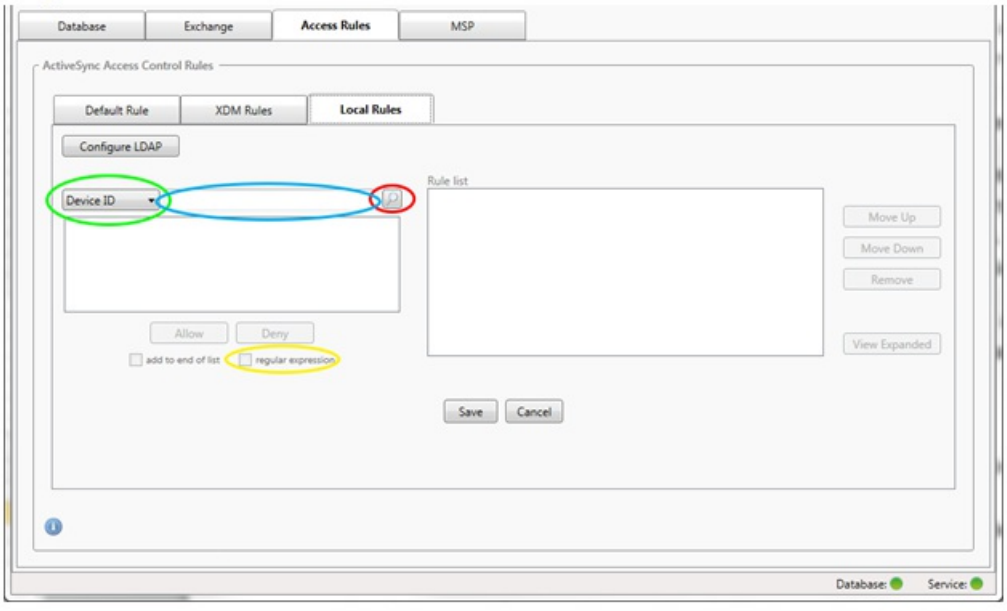


3. 选择要匹配的字段。 此示例使用设备类型。
4. 键入正则表达式。 此示例使用samsung.*
5. 确保选中正则表达式复选框，然后单击允许或拒绝。 在此示例中，选择的是允许，因此最终结果如下所示：

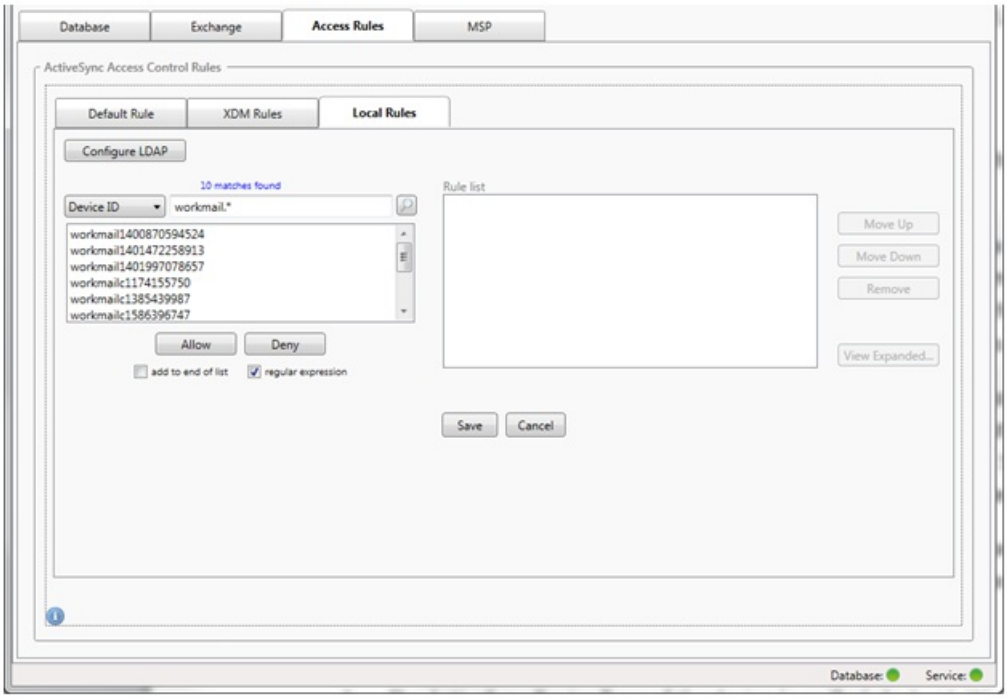


通过选中正则表达式复选框，可以针对与给定表达式匹配的特定设备运行搜索。此功能仅在成功完成主要快照时可用。即使没有计划使用正则表达式规则，您也可以使用此功能。例如，假定您要查找 ActiveSync 设备 ID 中包含文本“workmail”的所有设备。为此，请执行以下过程。

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）。

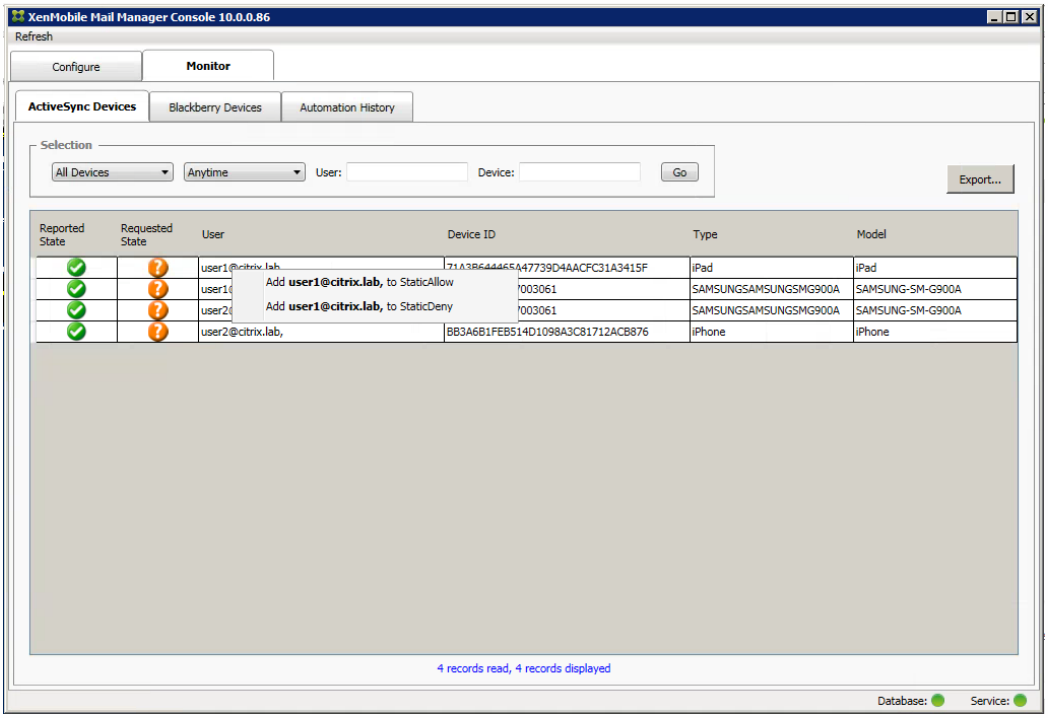


3. 在所选项目文本框（上图中以蓝色显示的框）内单击，然后键入workmail.*。
4. 确保选中正则表达式复选框，然后单击放大镜图标显示匹配项，如下图所示。



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。



设备监视

May 05, 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。

故障排除和诊断

May 05, 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。

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。

XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector 是一种解决方案，用于控制移动设备对公司电子邮件、日历和联系人的访问。 XenMobile NetScaler Connector 允许客户将兼容设备列表从 XenMobile 发送到 NetScaler，而 NetScaler 反过来控制哪些移动设备获许与公司的 Exchange Server 同步。

XenMobile 为移动应用程序、网络和数据提供全面保护，并确保端到端的安全性和合规性。 NetScaler 可以优化和控制所有企业和云服务的交付并确保交付安全。 这两种 Citrix 产品共同提供了扩展功能，确保应用程序的高可用性并保持安全性，同时降低了移动部署和管理成本。

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。

XenMobile 根据是否遵守高级别策略（例如检测已越狱的设备或检测特定应用程序）为设备提供白名单（获批准）和黑名单（被禁止）策略。 XenMobile NetScaler Connector 本地规则通常在需要特定覆盖时用于增加 XenMobile 规则，例如需要阻止使用特定版本操作系统的所有设备时。

XenMobile NetScaler Connector 的主要功能包括：

- **对 HTTP ActiveSync 请求的访问控制**。 XenMobile NetScaler Connector 可控制 Exchange Server 的移动设备发出的 HTTP ActiveSync 请求。 可在 XenMobile NetScaler Connector 中构建过滤器，以便基于指定的规则和标准允许或阻止用户设备。 在 XenMobile NetScaler Connector 中设置规则时，可在 XenMobile 中打开或关闭规则，从而管理设备访问组织内电子邮件的能力。
- **远程配置**。 XenMobile 控制 XenMobile NetScaler Connector 使用的基准和时间间隔差。
- **日志记录**。 在 XenMobile NetScaler Connector 配置实用程序的 **Log**（日志）选项卡上，可查看为给定用户设备在请求级别启用加密的时间，还可查看被允许或阻止的设备。

XenMobile NetScaler Connector 提供以下功能：

- **基于过滤器规则允许或阻止访问**。 XenMobile NetScaler Connector 根据组织的规则评估通过 NetScaler 进行路由的特定客户端请求。 最终结果是二进制*允许*状态，即允许客户端联系 Microsoft Exchange 2010 Client Access Server (CAS)，或二进制*阻止*状态，即客户端请求中断，并且不允许访问 Exchange CAS。 与 XenMobile 控制台中的设置配对后，可基于合规性准则阻止 Exchange ActiveSync 电子邮件访问设备用户，例如，如果设备已越狱，在设备上安装列入黑名单的应用程序时等等。
- **双层过滤器模型**。 第一层基于特定路径信息解析传入的 HTTP 请求。 第二层过滤器基于特定用户或特定设备的信息。 两层都可以配置。
- **过滤器规则存储在配置文件中**。 与组织内的用户帐户和设备相关的特定过滤器规则存储在网关的 XML 配置文件中。

部署 XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector 使您可以使用 NetScaler 来代理并平衡 XenMobile 服务器与 XenMobile 托管设备之间的通信负载。 XenMobile NetScaler Connector 定期与 XenMobile 通信以同步策略。 XenMobile NetScaler Connector 和 XenMobile 可以共同或单独组成群集，并能由 NetScaler 平衡负载。

XenMobile NetScaler Connector 由以下四个组件组成：

- XenMobile NetScaler Connector 服务。 提供了一个 REST Web 服务界面，NetScaler 可调用该界面确定来自设备的 ActiveSync 请求是否获得授权。
- XenMobile 配置服务。 此服务与 Device Manager 进行通信，将 Device Manager 策略更改与 XenMobile NetScaler Connector 同步。
- XenMobile 通知服务。 此服务向 Device Manager 发送未经授权的设备访问的通知，以便 Device Manager 采取相应措施，如通知用户设备被阻止的原因。
- XenMobile NetScaler 配置实用程序。 此应用程序允许管理员配置并监控 XenMobile NetScaler Connector。

要使 XenMobile NetScaler Connector 能够收到来自 NetScaler 的请求以授权 ActiveSync 通信，需要指定端口，XenMobile NetScaler Connector 可从该端口侦听 NetScaler Web 服务呼叫。

1. 从开始菜单中，选择 XenMobile NetScaler 配置实用程序。
2. 单击 Web Service（Web 服务）选项卡，然后键入 XenMobile NetScaler Connector Web 服务的侦听地址。 可以选择 HTTP 和/或 HTTPS。 如果 XenMobile NetScaler Connector 与 XenMobile 的位置相同（安装在同一服务器上），请选择与 XenMobile 不冲突的端口值。
3. 配置值后，单击 Save（保存），然后单击 Start Service（启动服务），启动 Web 服务。

要配置将应用于托管设备的访问控制策略，请执行以下操作：

1. 在 XenMobile NetScaler 配置实用程序中，单击 Path Filters（路径过滤器）选项卡。
2. 选择第一行 Microsoft-Server-ActiveSync is for ActiveSync（Microsoft-Server-ActiveSync 适用于 ActiveSync），然后单击 Edit（编辑）。
3. 从 Policy（策略）列表中选择所需的策略。 对于包含 XenMobile 策略的策略，请选择 Static + ZDM: Permit Mode（静态 + ZDM: 允许模式）或 Static + ZDM: Block Mode（静态 + ZDM: 阻止模式）。 这些策略将本地（或静态）规则与 XenMobile 的规则组合在一起。 Permit Mode（允许模式）意味着允许未被规则明确识别的所有设备访问 ActiveSync。 Block Mode（阻止模式）意味着将阻止这些设备。
4. 设置策略后，单击 Save（保存）。

在此任务中，您需要指定要与 XenMobile NetScaler Connector 和 NetScaler 结合使用的 XenMobile 服务器（又称为配置提供程序）的名称和属性。

注意：此任务假定您已安装并配置 XenMobile。

1. 在 XenMobile NetScaler Connector 配置实用程序中，单击 Config Providers（配置提供程序）选项卡，然后单击 Add（添

加）。

2. 输入您在此部署中使用的 XenMobile 服务器的名称和 URL。 如果您在多租户部署中部署了多台 XenMobile 服务器，则对每个服务器实例而言，此名称必须唯一。 例如，您可以在 Name（名称）字段中键入XMS。
3. 在 URL 中，输入 XenMobile 全局配置提供程序 (GCP) 的 Web 地址，格式通常为 https://DeviceManagerHost/zdm/services/MagConfigService。 MagConfigService 名称区分大小写。
4. 在 Password（密码）中，输入将用于 XenMobile Web 服务器的基本 HTTP 授权的密码。
5. 在 Managing Host（管理主机）中，输入安装了 XenMobile NetScaler Connector 的服务器的名称。
6. 在 Baseline Interval（基准时间间隔）中，指定从 XenMobile 提取新刷新的动态规则集的时间间隔。
7. 在 Request Timeout（请求超时）中，指定服务器请求超时的时间间隔。
8. 在 Config Provider（配置提供程序）中，选择配置提供程序服务器实例是否提供策略配置。
9. 在 Events Enabled（事件已启用）中，如果希望在设备被阻止时 Secure Mobile Gateway 通知 XenMobile，则启用此选项。 如果在任何 Device Manager 自动操作中都使用了 Secure Mobile Gateway 规则，则此选项是必需的。
10. 配置服务器后，单击 Test Connectivity（测试连接），测试与 XenMobile 服务器的连接。
11. 在建立连接后，单击 Save（保存）。

如果要扩展 XenMobile NetScaler Connector 和 XenMobile 部署，可在多个 Windows Server 上安装 XenMobile NetScaler Connector 实例，全都指向同一 XenMobile 实例，然后可使用 NetScaler 来平衡服务器的负载。

XenMobile NetScaler Connector 配置有两种模式：

- 在非共享模式中，每个 XenMobile NetScaler Connector 实例都与一个 XenMobile 服务器进行通信，并自身保持所产生的策略的私有副本。 例如，如果您有一群 XenMobile 服务器，则可在每个 XenMobile 服务器上运行 XenMobile NetScaler Connector 实例，然后 XenMobile NetScaler Connector 将从本地 XenMobile 获取策略。
- 在共享模式中，将一个 XenMobile NetScaler Connector 节点指定为主节点，它与 XenMobile 进行通信。 产生的配置通过 Windows 网络共享或 Windows（或第三方）复制功能在其他节点中共享。

整个 XenMobile NetScaler Connector 配置在一个文件夹中（由几个 XML 文件组成）。 XenMobile NetScaler Connector 进程检测此文件夹中任何文件的更改，并自动重新加载配置。 共享模式中的主节点没有故障转移功能。 但系统可容许主服务器关闭几分钟（例如，重新启动），因为上次已知的正确配置缓存在 XenMobile NetScaler Connector 进程中。

XenMobile NetScaler Connector 系统要求

May 05, 2016

XenMobile NetScaler Connector 通过 NetScaler 设备上配置的 SSL 桥接与 NetScaler 进行通信，使设备将所有安全流量直接桥接到 XenMobile。 可以将 XenMobile NetScaler Connector 安装在自己的服务器上或安装在与 XenMobile 相同的服务器上。 XenMobile NetScaler Connector 要求以下最低系统配置：

组件	要求
计算机和处理器	733 MHz 奔腾 III 或更高处理器。 2.0 GHz 奔腾 III 或更高处理器（建议）
NetScaler	NetScaler 设备，软件版本 10
内存	1 兆字节 (GB)
硬盘	具有 150 MB 可用硬盘空间的 NTFS 格式本地分区
操作系统	Microsoft Windows Server 2008 R2、Microsoft Windows Server 2008 SP2（建议）
其他设备	与主机操作系统兼容的网络适配器（用于与内部网络通信）
显示	VGA 或更高分辨率的显示器

XenMobile NetScaler Connector 的主机计算机要求以下最小可用硬盘空间：

- 应用程序。 10 -15 MB（建议 100 MB）
- 日志记录。 1 GB（建议 20 GB）

安装 XenMobile NetScaler Connector

May 05, 2016

可以将 XenMobile NetScaler Connector 安装在其自己的服务器上，或与 XenMobile 安装在相同的服务器上。

可出于以下原因考虑将 XenMobile NetScaler Connector 安装在其自己的服务器上（与 XenMobile 分开）：

- XenMobile 服务器在云端被远程托管（物理位置）。
- 不希望 XenMobile NetScaler Connector 受 XenMobile 服务器重新启动的影响（可用性）。
- 希望服务器的系统资源完全专用于 XenMobile NetScaler Connector（性能）。

XenMobile NetScaler Connector 加在服务器上的 CPU 负载取决于所管理的设备数量，一般的经验法则是，如果 XenMobile NetScaler Connector 部署在与 XenMobile 相同的服务器上，则置备一个额外的 CPU 核。 对于大量的设备（超过 50,000），如果没有群集环境，可能需要置备额外的核。 XenMobile NetScaler Connector 的内存占用量不足以保证额外的内存。

安装、升级或卸载 XenMobile NetScaler Connector

May 05, 2016

1. 用管理员帐户运行 XncInstaller.exe 以安装 XenMobile NetScaler Connector (XNC)，或者升级或删除现有的 XenMobile NetScaler Connector。
2. 按照屏幕上的说明完成安装、升级或卸载。

安装 XenMobile NetScaler Connector 后，必须手动重新启动 XenMobile 配置服务和通知服务。

卸载 XNC

May 05, 2016

1. 用管理员帐户运行 XncInstaller.exe。
2. 按照屏幕上的说明完成卸载。

管理 XenMobile NetScaler Connector

May 05, 2016

可使用 XenMobile NetScaler Connector 来构建访问控制规则，根据设备状态、应用程序黑名单或白名单以及其他合规性条件，允许或阻止托管设备发出的 ActiveSync 连接访问请求。

使用 XenMobile NetScaler Connector 配置实用程序，可构建强制执行公司电子邮件策略的动态和静态规则，从而阻止违反合规性标准的用户。 也可设置电子邮件附件加密，使通过您的 Exchange Server 到达托管设备的所有附件都被加密，且只有获得授权的用户才能在托管设备上查看。

为 XenMobile NetScaler Connector 选择安全模型

May 05, 2016

Establishing a security model is essential to a successful mobile device deployment for organizations of any size. Although it is not uncommon to use protected or quarantined network control to allow access to a user, computer, or device by default, it is not always a good practice. Every organization that manages IT security may have a slightly different or tailored approach to security for mobile devices.

The same logic applies to mobile device security. The vast numbers of mobile devices and types, quantities of mobile devices per user, and the array of operating system platforms and apps available make the very idea of using a permissive model a weak choice. In most organizations, the restrictive model will be the most logical choice.

The configuration scenarios that Citrix allows for integrating XenMobile NetScaler Connector with XenMobile are as follows:

The permissive security model operates on the premise that everything is either allowed or granted access by default. Only in the case of rules and filtering will something be blocked and a restriction applied. The permissive security model is good for organizations that have a relatively loose security concern about mobile devices and only applies restrictive controls to deny access where appropriate (when a policy rule is failed).

受限安全模型的运行前提是，默认情况下不允许或授权任何设备进行访问。 通过安全检查点的任何访问都要进行过滤和检查，并且拒绝访问，除非允许访问的规则获得通过。 受限安全模型适合对移动设备具有相对严格的安全标准的组织。 该模式仅在所有允许访问的规则都通过时，才授权访问网络服务的使用和功能。

配置 XenMobile NetScaler Connector

May 05, 2016

可以将 XenMobile NetScaler Connector 配置为基于以下属性，选择性地阻止或允许 ActiveSync 请求：Active Sync 服务 ID、设备类型、用户代理（设备操作系统）、授权用户和 ActiveSync 命令。

默认配置支持静态和动态组的组合。 通过使用 SMG Controller 配置实用程序维护静态组。 静态组可由已知类别的设备组成，如使用给定用户代理的所有设备。

动态组由称为“网关配置提供程序”的外部源维护，并由 XenMobile NetScaler Connector 定期收集。 XenMobile 可将允许和阻止设备和用户的组导出到 XenMobile NetScaler Connector。

策略是组的有序列表，其中每个组都有关联的操作（允许或阻止）和组成员列表。 一个策略可以有任何数量的组。 策略内组的排序很重要，因为找到匹配项时就会执行组的操作，不会评估后续的组。

成员定义匹配请求中属性的方式。 可以匹配单个属性，如设备 ID，或多个属性，如设备类型和用户代理。

配置 XenMobile NetScaler Connector 策略模式

May 05, 2016

XenMobile NetScaler Connector 可采用以下六种模式运行：

- Allow All（全部允许）。 此策略模式授权对通过 XenMobile NetScaler Connector 的所有流量进行访问。 不使用其他过滤规则。
- Deny All（全部拒绝）。 此策略模式阻止对通过 XenMobile NetScaler Connector 的所有流量进行访问。 不使用其他过滤规则。
- Static Rules: Block Mode（静态规则: 阻止模式）。 此策略模式执行在结尾具有隐式拒绝或阻止语句的静态规则。 不允许的设备或被其他过滤规则允许的设备被 XenMobile NetScaler Connector 阻止。
- Static Rules: Permit Mode（静态规则: 允许模式）。 此策略模式执行在结尾具有隐式许可或允许语句的静态规则。 允许未被阻止的设备或被其他过滤规则拒绝的设备通过 XenMobile NetScaler Connector。
- Static + ZDM Rules: Block Mode（静态 + ZDM 规则: 阻止模式）。 此策略模式首先执行静态规则，然后执行来自 XenMobile 的、在结尾具有隐式拒绝或阻止语句的动态规则。 将根据已定义的过滤器和 Device Manager 规则允许或拒绝设备。 与定义的过滤器和规则不匹配的任何设备都会被阻止。
- Static + ZDM Rules: Permit Mode（静态 + ZDM 规则: 允许模式）。 此策略模式首先执行静态规则，然后执行来自 XenMobile 的、在结尾具有隐式许可或允许语句的动态规则。 将根据已定义的过滤器和 XenMobile 规则允许或拒绝设备。 与定义的过滤器和规则不匹配的任何设备都会被允许。

XenMobile NetScaler Connector 根据 iOS 唯一的 ActiveSync ID 以及从 XenMobile 收到的基于 Windows 的移动设备，处理动态规则的允许或阻止。 Android 设备的特性由于制造商不同而有所不同，且有些设备没有准备好公开唯一的 ActiveSync ID。 为进行补偿，XenMobile 会发送 Android 设备的用户 ID 信息，以便做出允许或阻止决定。 因此，如果用户只有一个 Android 设备，则其允许和阻止功能正常。 如果用户具有多个 Android 设备，则所有设备都被允许，因为不能明确区别 Android 设备。 网关仍可配置为根据 ActiveSyncID（如果已知）静态阻止这些设备，也可配置为根据设备类型或用户代理进行阻止。

要指定策略模式，请在 SMG Controller 配置实用程序中执行以下操作：

1. 单击 Path Filters（路径过滤器）选项卡，然后单击添加。
2. 在 Path Properties（路径属性）对话框中，从策略下拉列表中选择策略模式，然后单击保存。

可在配置实用程序的策略选项卡中查看这些规则。 在 XenMobile NetScaler Connector 中自上而下处理这些规则。 “允许”策略显示时带有绿色选中标记。 “拒绝”策略显示为红色圆圈，中间横穿一条直线。 要刷新屏幕并查看最新更新的规则，请单击刷新。 也可在 config.xml 文件中修改规则的顺序。

要测试规则，请单击 Simulator（模拟器）选项卡。 在字段中指定值。 这些值也可从日志中获得。 将出现指定允许或阻止的结果消息。

配置静态规则

May 05, 2016

必须输入由 ActiveSync 连接 HTTP 请求的 ISAPI 过滤功能读取的静态规则的值。 静态规则使 XenMobile NetScaler Connector 能够根据下列准则允许或阻止流量：

- 用户。 XenMobile NetScaler Connector 使用在设备注册时捕获的授权用户值和名称结构。 其常见形式是“域\用户名”，由运行 XenMobile 的服务器引用，该服务器通过 LDAP 连接到 Active Directory。 如果值结构需要确定或有所不同，则 XenMobile NetScaler Connector 配置实用程序中的 Log（日志）选项卡将显示通过 XenMobile NetScaler Connector 传递的值。
- Deviceid (ActiveSyncID)。 也称为所连接设备的 ActiveSyncID。 此值通常可在 XenMobile 控制台的特定设备属性页面中找到。 此值也可从 XenMobile NetScaler Connector 配置实用程序的 Log（日志）选项卡中筛选出来。
- DeviceType。 XenMobile NetScaler Connector 可确定设备是 iPhone、iPad 还是其他设备类型，并能根据准则加以允许或阻止。 与其他值一样，XenMobile NetScaler Connector 配置实用程序可显示为 ActiveSync 连接处理的所有已连接设备的类型。
- UserAgent。 包含有关所使用的 ActiveSync 客户端的信息。 在大多数情况下，指定的值对应于移动设备平台的特定操作系统内部版本和版本。

在服务器上运行的 XenMobile NetScaler Connector 配置实用程序始终管理静态规则。

1. 在 SMG Controller 配置实用程序中，单击 Static Rules（静态规则）选项卡，然后单击 Add（添加)。
2. 在 Static Rule Properties（静态规则属性）对话框中，指定要用作条件的值。 例如，可通过输入用户名（例如 AllowedUser），然后取消选中 Disabled（禁用）复选框，输入允许访问的用户。
3. 单击 Save（保存）。 静态规则现在即生效。 此外，还可使用正则表达式来定义值，但必须在 config.xml 文件中启用规则处理模式。

配置动态规则

May 05, 2016

动态规则在 Device Manager 中通过设备策略和属性定义，并基于是否存在策略违规情况或属性设置而触发动态 XenMobile NetScaler Connector 过滤器。 XenMobile NetScaler Connector 过滤器的工作方式是针对给定策略违规情况或属性设置分析设备。 如果设备满足条件，则将设备放入设备列表中。 此设备列表既不是允许列表也不是阻止列表。 它是满足定义条件的设备的列表。 通过下列配置选项可定义是否要使用 XenMobile NetScaler Connector 允许或拒绝设备列表中的设备。

注意：必须在 XenMobile 控制台中配置这些动态规则。

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

2. 在**服务器**下面，单击 **ActiveSync Gateway**。 此时将显示 ActiveSync Gateway 页面。

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 Secure Mobile 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 XenMobile NetScaler Connector。

通过编辑 XenMobile NetScaler Connector XML 文件配置自定义策略

May 05, 2016

可在 XenMobile NetScaler Connector 配置实用程序的策略选项卡的默认配置中查看基本策略。 如果要创建自定义策略，可编辑 XenMobile NetScaler Connector XML 配置文件 (config\config.xml)。

1. 在文件中找到 PolicyList 部分，然后添加新的策略元素。
2. 如果还需要新组，如额外静态组或支持额外 GCP 的组，可将新的组元素添加到“GroupList”（组列表）部分。
3. 也可通过重新排列 GroupRef 元素，更改现有策略中组的顺序。

配置 XenMobile NetScaler Connector XML 文件

May 05, 2016

XenMobile NetScaler Connector 使用 XML 配置文件来规定 XenMobile NetScaler Connector 的操作。 此外，此文件还指定组文件和过滤器在评估 HTTP 请求时将采取的关联操作。 默认情况下，此文件命名为 config.xml 且位于：..\Program Files\Citrix\XenMobile NetScaler Connector\config\。

GroupRef 节点定义逻辑组名称 - 默认情况下为 AllowGroup 和 DenyGroup。
注意：GroupRef 节点在 GroupRefList 节点中出现的顺序很重要。
GroupRef 节点的 ID 值标识逻辑容器或用于匹配特定用户帐户或设备的成员集合。 操作属性指定过滤器处理与集合中规则匹配的成员的方式。 例如，与 AllowGroup 集中的规则匹配的用户帐户或设备将“通过”（允许访问 Exchange CAS），而与 DenyGroup 集中的规则匹配的用户帐户或设备将被“拒绝”（不允许访问 Exchange CAS）。

特定的用户帐户/设备或组合满足两个组中的规则时，会使用优先级约定来引导请求的结果。 优先级通过 GroupRef 节点在 config.xml 文件中的自上而下的顺序体现。 GroupRef 节点以优先级顺序排序。 “允许”组中针对给定条件的规则将始终优先于“拒绝”组中针对相同条件的规则。

此外，config.xml 还定义组节点。 这些节点将逻辑容器 AllowGroup 和 DenyGroup 链接到外部 XML 文件。 存储在外部文件中的条目构成过滤器规则的基础。
注意：在此版本中，仅支持外部 XML 文件。
默认安装会在配置中实施两个 XML 文件 - allow.xml 和 deny.xml。

从 XenMobile 中导入策略

May 05, 2016

1. 在 XenMobile NetScaler Configuration 配置实用程序中，单击 Config Providers（配置提供程序）选项卡，然后单击 Add（添加）。
2. 在 Config Providers（配置提供程序）对话框中，在 Name（名称）中，输入将用于 XenMobile 服务器基本 HTTP 授权以及具有管理权限的用户名。
3. 在 URL 中，输入 XenMobile 网关配置服务 (GCS) 的 Web 地址，格式通常为 https://xdmHost/xdm/services/MagConfigService。 MagConfigService 名称区分大小写。
4. 在 Password（密码）中，输入将用于 XenMobile 服务器的基本 HTTP 授权的密码。
5. 单击 Test Connectivity（测试连接），测试网关到配置提供程序的连接。 如果连接失败，请检查本地防火墙设置是否允许连接，或与管理员核查。
6. 连接成功后，取消选中 Disabled（禁用）复选框，然后单击 Save（保存）。
7. 在 Managing Host（管理主机）中，保留本地主机计算机的默认 DNS 名称。 在多个 Forefront Threat Management Gateway (TMG) 服务器配置在一个阵列中时，此设置用于协调与 XenMobile 的通信。

保存设置后，打开 GCS。

配置到 XenMobile NetScaler Connector 的连接

May 05, 2016

XenMobile NetScaler Connector 通过安全 Web 服务与 XenMobile 和其他远程配置提供程序进行通信。

1. 在 XenMobile NetScaler Connector 配置实用程序中，单击 Config Providers（配置提供程序）选项卡，然后单击 Add（添加）。
2. 在 Config Providers（配置提供程序）对话框中，在 Name（名称）中输入用户名，该用户名具有管理权限并将用于 XenMobile 服务器的基本 HTTP 授权。
3. 在 URL 中，输入 XenMobile GCS 的 Web 地址，格式通常为 https://ZdmHost/zdm/services/MagConfigService。MagConfigService 名称区分大小写。
4. 在 Password（密码）中，输入将用于 XenMobile 服务器的基本 HTTP 授权的密码。
5. 在 Managing Host（管理主机）中输入 XenMobile NetScaler Connector 服务器名称。
6. 在 Baseline Interval（基准时间间隔）中，指定从 Device Manager 提取新刷新的动态规则集的时间间隔。
7. 在 Delta interval（时间间隔差）中，指定提取到动态规则更新时的时间间隔。
8. 在 Request Timeout（请求超时）中，指定服务器请求超时的时间间隔。
9. 在 Config Provider（配置提供程序）中，选择配置提供程序服务器实例是否提供策略配置。
10. 在 Events Enabled（事件已启用）中，如果希望在设备被阻止时 XenMobile NetScaler Connector 通知 XenMobile，则启用此选项。 如果在任何 XenMobile 自动操作中都使用了 XenMobile NetScaler Connector 规则，则此选项是必需的。
11. 单击 Save（保存），然后单击 Test Connectivity（测试连接），测试“网关到配置”提供程序的连接性。 如果连接失败，请检查本地防火墙设置是否允许连接，或与管理员联系。
12. 连接成功后，取消选中 Disabled（禁用）复选框，然后单击 Save（保存）。

添加新的配置提供程序时，XenMobile NetScaler Connector 会自动创建一个或多个与提供程序关联的策略。 这些策略由模板定义进行定义，模板定义包含在 NewPolicyTemplate 部分的 config\policyTemplates.xml 中。 会为在本部分中定义的每个策略元素创建一个新策略。 操作员可添加、删除或修改策略元素，前提是策略元素符合架构定义，且不修改标准替换字符串（括在大括号中）。 接下来，为提供程序添加新组并更新策略以将新组包括在内。

为 XenMobile NetScaler Connector 选择过滤器

May 05, 2016

XenMobile NetScaler Connector 过滤器的工作方式是针对给定策略违规情况或属性设置分析设备。 如果设备满足条件，则将设备放入设备列表中。 此设备列表既不是允许列表也不是阻止列表。 它是满足定义条件的设备的列表。 在 XenMobile 中 XenMobile NetScaler Connector 可使用下列过滤器。

- 加入黑名单的应用程序。 基于由黑名单策略定义的设备列表以及是否存在加入黑名单的应用程序来允许或拒绝设备。
- 仅限加入白名单的应用程序。 基于由白名单策略定义的设备列表以及是否存在未加入白名单的应用程序来允许或拒绝设备。
- 未托管设备。 创建包括 XenMobile 数据库中所有设备的设备列表。 需要在阻止模式下部署移动应用程序网关。
- 已获得 Root 权限的 Android 设备/已越狱的 iOS 设备。 创建包括所有标记为获得 root 权限的设备的设备列表，并根据获得 root 权限的状态允许或拒绝。
- 不合规设备。 允许您拒绝或允许满足自己内部 IT 合规条件的设备。 合规是由名为不合规的设备属性定义的任意设置，它是一个可以为真或假的布尔标志。 （可以手动创建此属性并设定值，或者也可在设备满足或不满足特定条件时，使用自动操作在设备上创建此属性。）
  - 不合规 = 真。 如果设备不满足您 IT 部门设定的合规标准和策略定义，则该设备不合规。
  - 不合规 = 假。 如果设备满足您 IT 部门设定的合规标准和策略定义，则该设备合规。
- 不合规密码。 创建设备上没有通行码的所有设备的设备列表。
- 已吊销状态。 创建所有已吊销设备的设备列表，并根据吊销状态允许或拒绝。
- 非活动设备。 创建在指定时间段内与 XenMobile 没有通信（并因此视为处于非活动状态）的设备的设备列表，然后相应允许或拒绝设备。
- 匿名设备。 允许或拒绝在 XenMobile 中已注册但用户的身份未知的设备。 例如，可以是以前注册的用户，但用户的 Active Directory 密码已过期，或者是用未知凭据注册的用户。
- 隐式允许/拒绝。 创建不满足其他任何过滤器规则条件的所有设备的设备列表，并根据该列表允许或拒绝。 隐式允许/拒绝选项确保设备选项卡中的 XenMobile NetScaler Connector 状态启用，并显示设备的 XenMobile NetScaler Connector 状态。 隐式允许/拒绝选项还控制所有其他尚未被选定的 XenMobile NetScaler Connector 过滤器。 例如，加入黑名单的应用程序将被 XenMobile NetScaler Connector 拒绝（阻止），而其他所有过滤器将被允许，因为隐式允许/拒绝选项被选定为允许。

模拟与 XenMobile NetScaler Connector 之间的 ActiveSync 流量

May 05, 2016

可以使用 XenMobile NetScaler Connector 模拟启用了您的策略时 ActiveSync 流量的具体表现。 在 XenMobile NetScaler Connector 配置实用程序中，单击 Simulations（模拟）选项卡。 结果将根据您已配置的规则显示策略的应用方式。

监视 XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector 配置实用程序提供详细的日志记录，可用于查看 Secure Mobile Gateway 允许或阻止的通过 Exchange Server 的所有流量。

使用日志选项卡可查看由 NetScaler 转发到 XenMobile NetScaler Connector 以进行授权的 ActiveSync 请求的历史记录。

为确保 XenMobile NetScaler Connector Web 服务运行，还可将以下 URL 加载到 XenMobile NetScaler Connector 服务器的浏览器中：http:///services/ActiveSync/Version。 如果 URL 以字符串形式返回产品版本，则 Web 服务为可响应。