关于 XenMobile Server 10.1

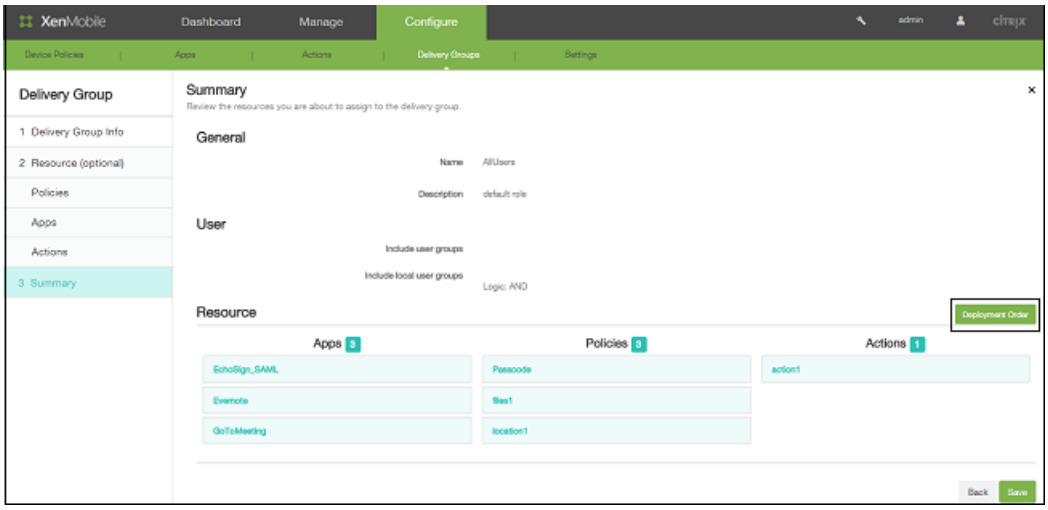
Aug 04, 2016

可以在 XenMobile 控制台上将 XenMobile 10 升级到 XenMobile 10.1。要执行升级，请使用 xms_10.1.0.62986.bin。在 XenMobile 控制台中，转至**设置** > **版本管理**。单击**升级**，然后上载 xms_10.1.0.62986.bin 文件。有关在控制台中进行升级的详细信息，请参阅升级 XenMobile。

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

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

资源部署排序。在 XenMobile MDM Edition 中，可以更改交付组中资源的部署顺序。在 XenMobile 控制台中，可以在配置 > 交付组中更改部署顺序。添加或编辑交付组时，在摘要页面上的资源旁边，单击部署顺序，则可以更改资源在列表中的显示位置，以设置首选顺序。



注意：

- 您可以设置其部署顺序的资源必须是 XenMobile 完全管理的资源，如策略和应用程序。但是，在 XenMobile MDM Edition 的本版本中，尚无法对操作排序。
- 此功能不支持 Windows Phone 和 Windows Tablet。要在这些设备上强制执行资源的部署计划，必须执行多项部署。

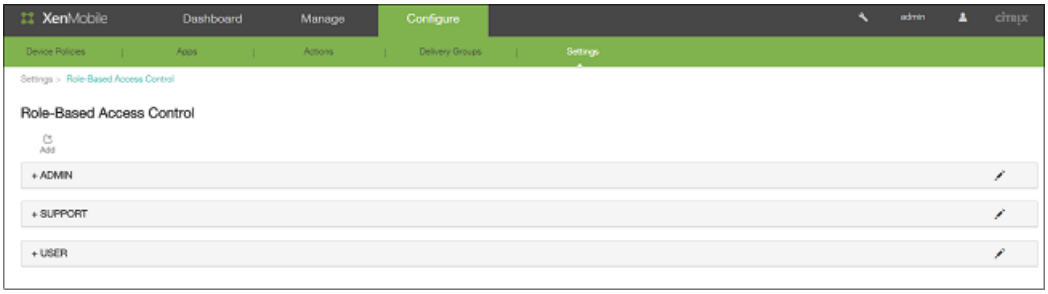
导出表格数据。对于 XenMobile 控制台中的每个表格（应用程序、策略、操作、交付组、本地用户和组、注册以及设备），可以通过单击导出来创建包含所有已显示列的 .csv 文件。

REST API。XenMobile 支持用于 REST 服务的公用 API，使您可以直接通过任意 REST 客户端调用通过 XenMobile 公开的服务。通过 XenMobile 10.1 支持的 API 可以执行以下操作：

- 在初始安装期间配置许可证、NetScaler Gateway、LDAP、证书管理。

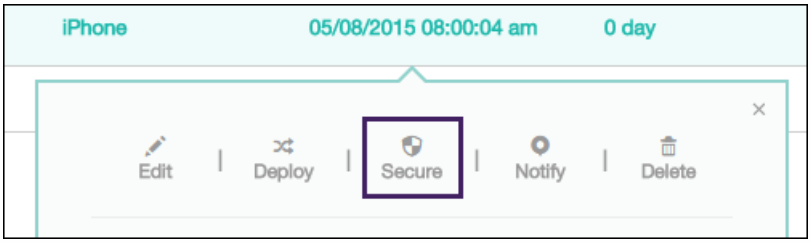
- 检索包含资源和组在内的交付组详细信息。
- 重置管理员密码。
- 导出 PKI 证书。
- 配置通知服务器设置，如添加和编辑 SMS 和 SMTP 服务器、删除服务器和激活服务器。
- 检索应用程序详细信息和删除应用程序。
- 设置主机的完全限定的域名 (FQDN)。

RBAC。DEVICE_PROVISIONING 角色已从 XenMobile 10.1 中删除，并添加了“支持”控制台功能。在 XenMobile 10 中，自动为管理员角色提供此功能；在 XenMobile 10.1 中，此功能仅在为角色选择“支持”时可用。

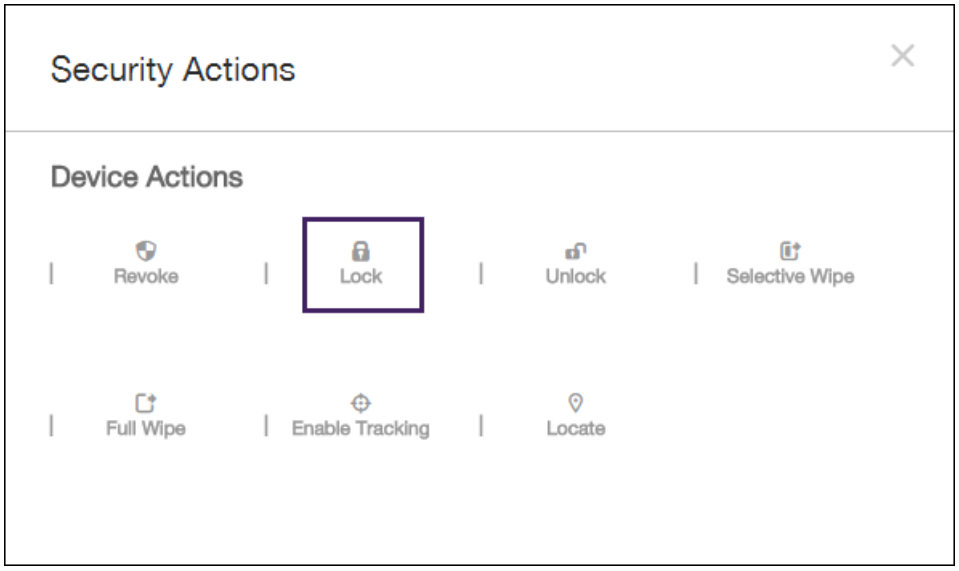


设备锁定安全操作。您可以锁定设备，同时在设备锁定屏幕上显示消息和电话号码。可以在 XenMobile 控制台的管理 > 设备中锁定设备。

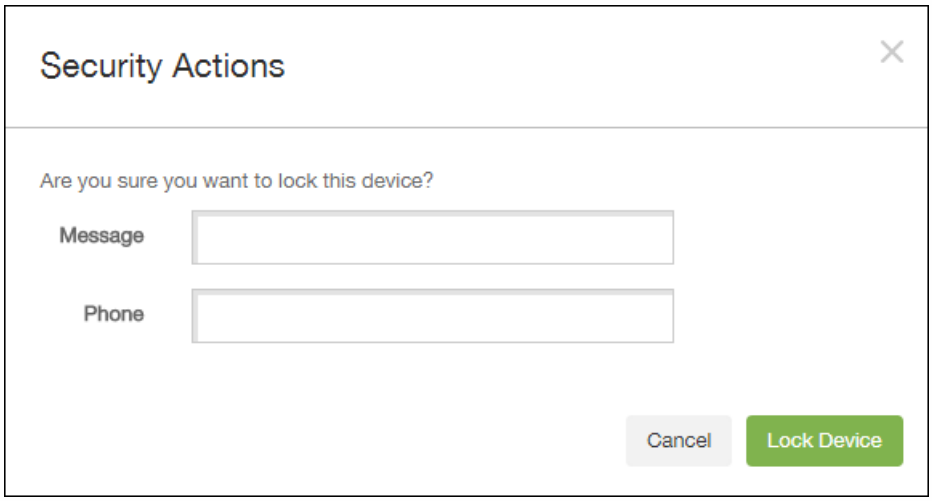
选择列表中的 iOS 设备后，在显示的对话框中，单击安全。



在安全操作对话框中，单击锁定。



然后，在确认消息中，可以选择输入消息和电话号码，然后单击锁定设备。iOS 7 和 8 设备支持此功能。

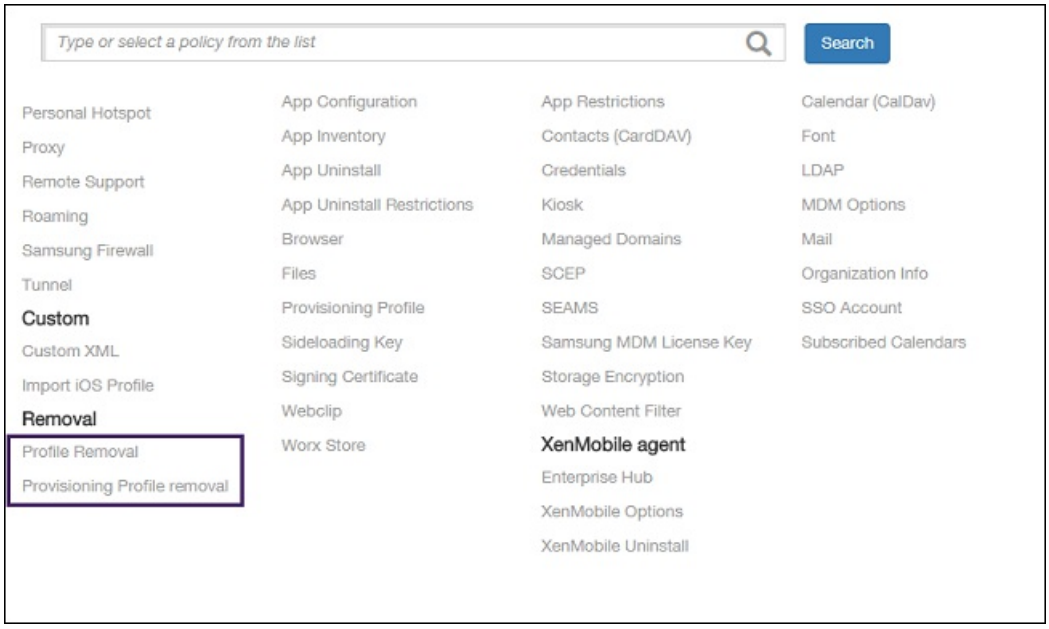


注意：如果在 XenMobile 控制台中设置了通行码策略，或者如果用户已在设备上手动启用通行码，消息和电话号码将仅显示在锁定设备上。

VPP 增强功能。以下功能扩展了 XenMobile 中的 Volume Purchasing Program (VPP) 功能。

- 允许将多个 VPP 令牌导入 XenMobile 中；例如，在多个位置购买的令牌，或者为需要不同 VPP 令牌的多个组织、业务单位或部门购买的令牌。
- 合作伙伴可以从专有企业至企业 (B2B) 应用商店向使用 iOS 设备的用户创建和部署 B2B 应用程序，方法是在 XenMobile 控制台的设置中将登录凭据添加到 VPP 配置中。
- 对于使用 XenMobile 为多个 VPP 客户和跨国公司管理应用程序和设备的组织，支持管理多个 VPP/B2B 应用程序。所有 VPP/B2B 帐户的应用程序均自动上载到 XenMobile 并自动更新。您可以在 XenMobile 控制台中将特定 VPP/B2B 应用程序分配给用户，还可在此控制台中查看应用程序所应用到的 VPP/B2B 帐户。

置备配置文件策略和设备详细信息。在 XenMobile 10 及之前的版本中，通过电子邮件附件将配置文件分发到用户设备；用户通过单击附件在其 iOS 设备上添加配置文件。XenMobile 10.1 支持以下置备配置文件策略和设备详细信息，从而易于跟踪 iOS 设备上企业应用程序的置备配置文件状态，并且不再需要用户在其设备上手动安装配置文件。



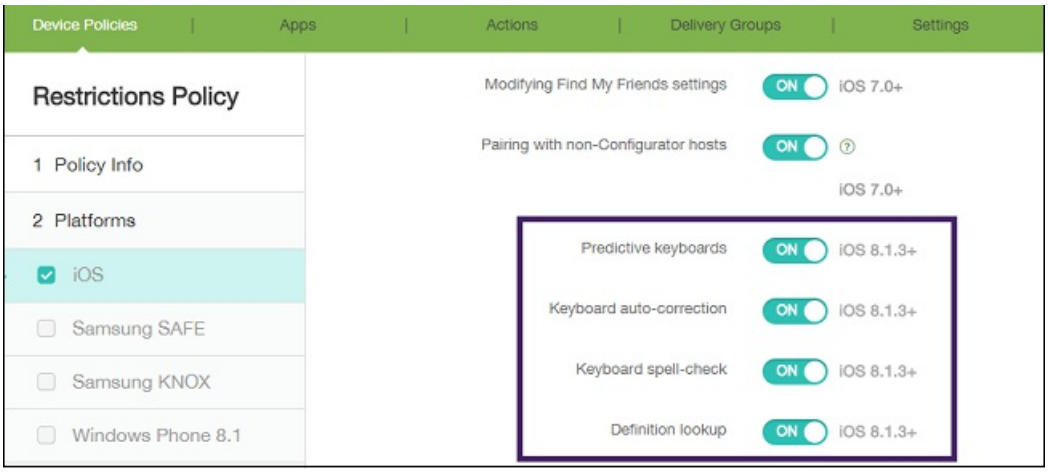
- **iOS 置备配置文件策略**。使您可以远程在 iOS 设备上安装置备配置文件。配置策略时，上载 iOS 置备配置文件，然后向用户设备部署配置文件。
- **iOS 置备配置文件删除策略**。使您可以从 iOS 设备删除置备配置文件。您可以在 XenMobile 控制台的配置 > 设备策略中配置这些设备策略。
- **iOS 置备配置文件列表**。可以查看设备的清单 iOS 配置文件以及设备上安装的置备配置文件列表，其中列出了全局唯一标识符 (UUID)、过期日期和每个配置文件的托管状态。可以在 XenMobile 控制台的管理 > 设备中查看这些详细信息。

Apple Device Enrollment Program (DEP) 预注册。使经销商可以在 DEP 中预注册设备，以便在将设备分发给用户之前在设备上安装托管应用程序。

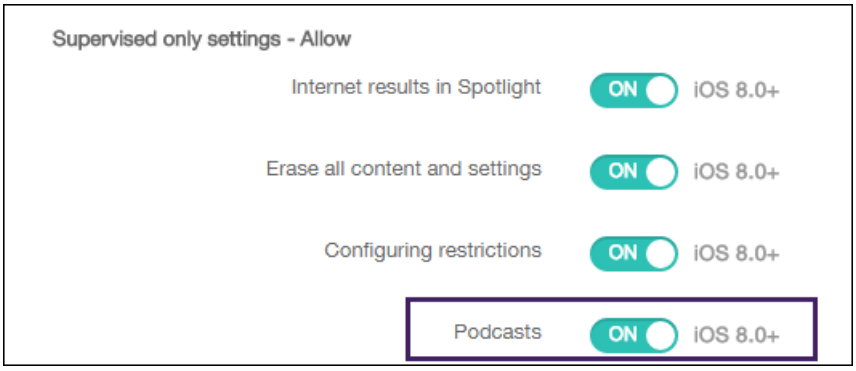
与 Apple Configurator 集成。简化了大规模企业所有设备的注册操作。设备可以连接到 Apple Configurator 并自动进行配置，以安装预生成的 XenMobile 配置文件。

适用于 iOS 受监督设备的新限制设备策略。

- 允许或阻止预测键盘、键盘自动更正、键盘拼写检查和键盘定义查找。仅适用于采用 iOS 8.1.3 的受监督设备。



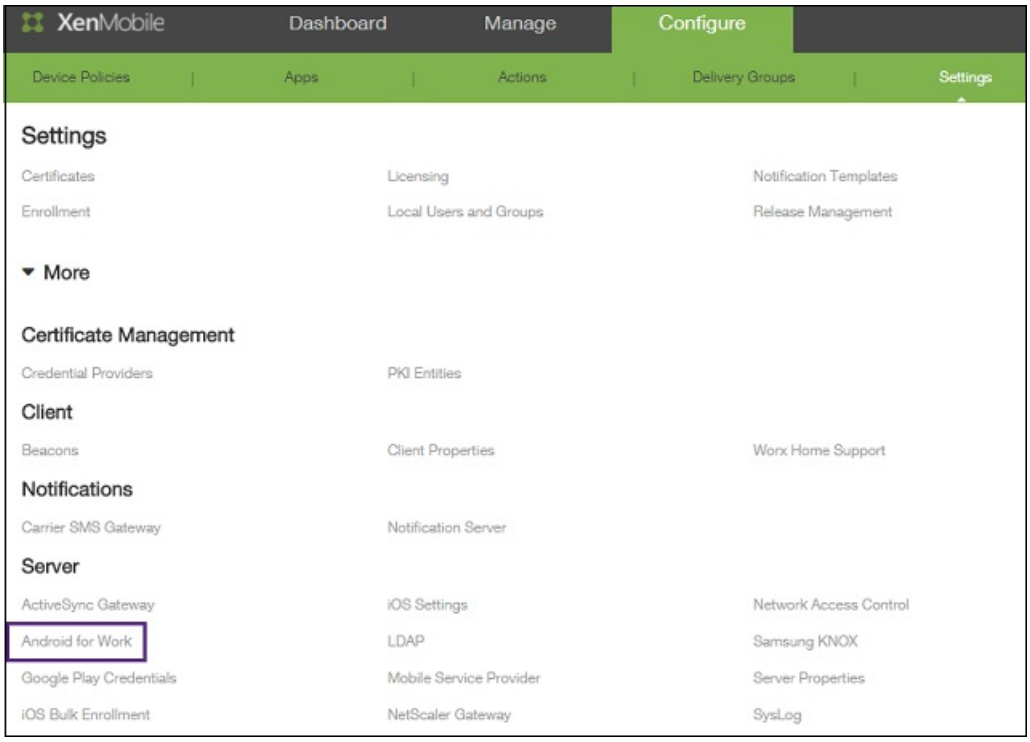
- 允许或阻止博客。仅适用于采用 iOS 8.0 及更高版本的受监督设备。

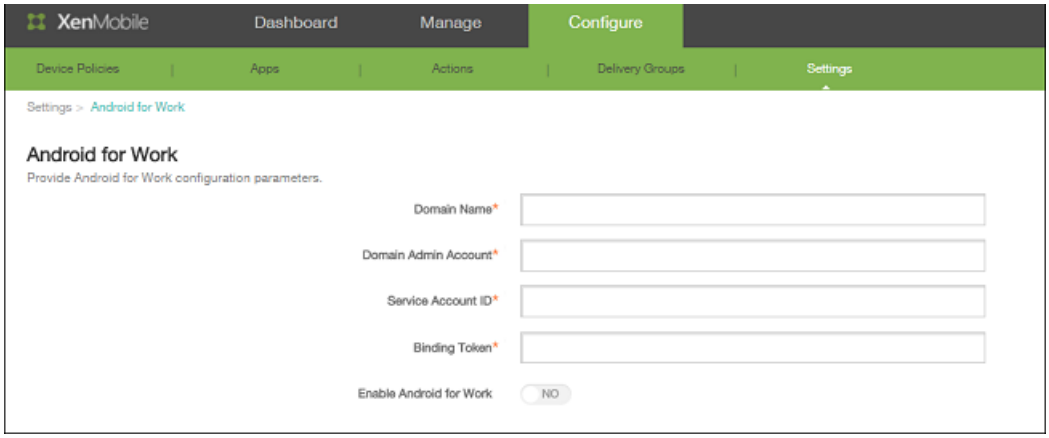


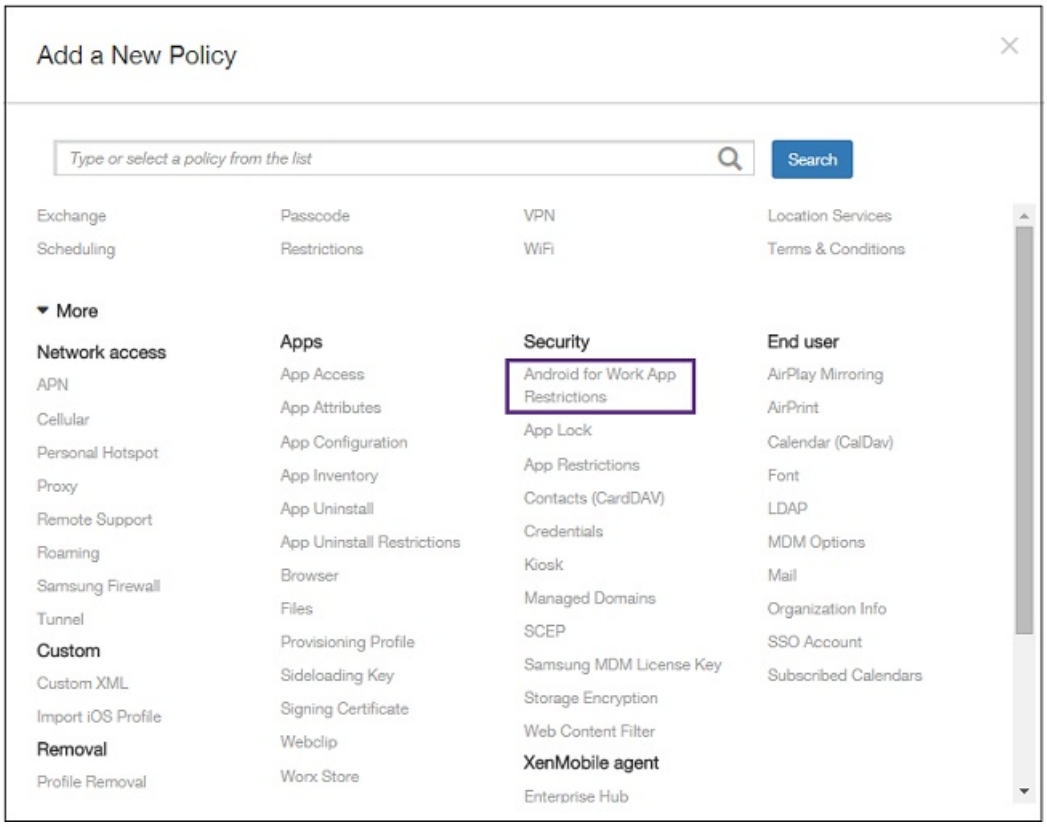
Android for Work。设备上的安全工作区将企业应用程序和数据与个人应用程序和数据区分开。组织可以使用 Google 设置 Android for Work 帐户。然后，可以将批准的应用程序从 Google Play for Work 应用商店部署到用户设备。还可以设置应用程序限制策略以控制访问权限和功能。在 XenMobile 控制台中的设置 > 服务器 > Android for Work，以及设备策略 > 安全性 > Android for Work 应用程序限制中，配置 Android for Work 设置。

注意

Android for Work 不支持打包应用程序。用户必须在其 Android 设备上安装 Worx Home，然后将 Android for Work 应用程序添加到 Worx Home。







Samsung KNOX 容器。下表列出了 Samsung KNOX 容器的 MDM 策略以及这些策略适用的操作系统。Samsung KNOX 容器是设备上的安全工作区，用于将企业应用程序和数据与个人应用程序和数据区分开。这些策略设置在 XenMobile 控制台的配置 > 设备策略 > 限制中进行配置。

策略	适用于 Samsung KNOX Standard；之前适用于 Samsung SAFE	适用于 Samsung KNOX Premium (KNOX 2.0)
允许使用 Samsung SAFE API 在 Android 设备上配置访问点名称 (APN) 和通用分组无线服务 (GPRS) 设置。	X	X
启用或禁用在 KNOX 容器中使用通用访问卡 (CAC) 身份验证（包括在容器中使用电子邮件和浏览器所需的身份验证）。		X

策略	适用于 Samsung KNOX Standard；之前适用于 Samsung SAFE	适用于 Samsung KNOX Premium (KNOX 2.0)
将解锁方法设置为组合使用指纹和密码。		X
启用或禁用用户是否可以在 KNOX 容器内移动应用程序。		X
启用或禁用在 KNOX 容器内使用非安全键盘。		X
启用或禁用在 KNOX 容器内通过列表进行共享。		X
允许或阻止用户发送或接收短信服务 (SMS) 和多媒体消息服务 (MMS) 消息	X	
允许或阻止用户手动更改日期和时间。	X	
允许用户将已安装在其个人区域的应用程序安装到 KNOX 容器中。		X
在 KNOX 容器中启用或禁用 GMS 应用程序。		X
启用或禁用将设备置于一般准则配置中。		X
启用或禁用为对称密钥提供基于 TrustZone 的安全密钥存储的 TIMA 密钥存储。		X
启用或禁用设备记录事件以用于设备的取证分析。		X

XenMobile Server 10.1 已修复的问题

Nov 10, 2015

比较对象：XenMobile 服务器 10。

XenMobile 10.1 已修复下列问题：

- 采用客户端身份验证类型添加通用 PKI 实体 (GPKI) 时，不会将 WSDL URL 发送到证书服务器以执行身份验证。

  [#501945]

- 要删除已经在交付组中配置的 Active Directory 组，请首先搜索 Active Directory 组，然后取消选中组对应的复选框。

  [#512990]

- 现在可以使用基础身份验证配置 Microsoft 证书颁发机构。

  [#526705]

- 无法在 XenMobile 控制台中添加单个黑莓或 Windows 设备。

  [#532844]

- 现在可以在 iOS 设备上安装 VPN 配置文件。

  [#533770]

- 使用主题或 SAN 宏 $user.distinguishedname 时，不再需要向导入到客户端证书中的名称添加额外的 CN=。

  [#533837]

- RBAC：仅具有查看权限的管理员现在只能查看。他们不会再看到他们不可以使用的选项。

  [#534184]

- 当 NetScaler Gateway 在非默认端口上侦听时，iOS 上的帐户创建操作失败。

  [#537368]

- 在 XenMobile 控制台 MDX 策略中的“身份验证”下，现在保存“应用程序通行码”或“要求联机会话”设置。

  [#543397]

- 适用于 iOS 的 SSO 帐户和 VPN 策略现在可用。

  [#549924]

- 现在可以发布自定义开发的 Android 应用程序。

  [#550111]

- $、@ 和 " 等特殊字符在安装 XenMobile 10 时使用的命令行接口 (CLI) 的密码中以及分配给证书的密码中无法识别；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]

- 在已注册的 Windows Phone 8.1 设备上，未托管的应用程序显示在软件清单列表中。

  [#506143]

- 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]

- 在每天的设定时间，不发生与 ShareFile 云的自动同步。结果导致最后一次成功同步之后 ShareFile 管理员在云中手动置备的所有用户均不一致。

  [#542494]

- 配置后台网络服务应用程序策略时，服务地址的 FQDN 和端口列表中不能出现字符空格。

  [#542891]

- 如果 XenMobile 安装在虚拟机管理程序上，XenMobile 服务器上的时间可能会慢几个小时。

  [#543668]

- Active Directory 用户组名称包含句点 (.) 时，无法保存交付组。

  [#547957]

- 如果用户使用备用用户主体名称 (UPN) 注册，当用户尝试通过 Worx Home 从 Worx Store 访问企业应用程序（如 XenDesktop 和 XenApp 应用程序）时，这些应用程序不显示。

  [#548339]

- 如果 Active Directory 组超过 255 个字符，列表将被截断，并且不会保存用户组成员关系。结果导致用户可能无法注册，交付组可能无法部署。

  [#548762、#557918]

- 在运行 Citrix Receiver 的 Android 或 iOS 设备上，有时用户无法从 Worx Home 打开 StoreFront 应用程序。

  [#549824]

- 在 XenMobile 控制台中使用 IPSec 连接类型配置 VPN 设备策略时，无法配置共享密钥。此外，如果将按需启用 VPN 设置为开，无法在 On Demand Domain Action（按需域操作）列表中指定一项操作。

  [#550560，#550844，#553296]

- 在 XenMobile 控制台中，配置 iOS 安全操作锁定选项时，“消息”和“电话号码”字段允许的字符串长度大于可以在设备上正常显示的长度。此外，如果单击“锁定”按钮，当“消息”字段包含问号 (?) 时，会出现错误消息。最后，配置“消息”和“电话号码”字段后，配置另一个“锁定”命令时，“消息”和“电话号码”字段有时会包含之前的配置信息。

  [#551200，#551201，#554811]

- 端口号后接服务器地址（如 mail.example.com:8443）时，无法创建和部署 Exchange ActiveSync 设备策略。

[#551313]

- 如果配置 LDAP 身份验证，且用户名和密码的长度超过 76 个字符，当您请求 CA 证书时，会出现错误。

  [#553276]

- 配置 PKI 实体时，如果在上载到 XenMobile 的证书的主题名中使用标识名，在名称中，证书名会包含“CN”，如 CN = CN=Admin, Joe。

  [#553280]

- 创建注册确认模板时，如果为收件人配置宏 ${device.imei} 以返回设备 IMEI，宏连续返回用户注册的首个设备的 IMEI，而非用户后续设备的 IMEI。当用户对每个注册设备使用相同的登录凭据时会出现此问题。

  [#553282]

- 配置新的 NetScaler Gateway 实例时，如果将登录类型设置为“仅限域”，则无法将“密码”为必填项设置为关。

  [#553628]

- 用于 WiFi 下的“允许硬件控制”和“添加配置文件”的 Samsung 限制设备策略在设备上不起作用。

  [#555938]

- 无法打包自定义开发的 .apk Android 文件。尝试将 .apk 应用程序上载到 XenMobile 时，出现软件包类型无效错误。

  [#557089]

- 在 XenMobile 控制台中，Android for Work 的过滤器在“设备策略”页面缺失。

  [#558298]

- 在 XenMobile 控制台中，在采用 Android for Work 模式注册的设备上发布锁定命令时，会看到一个使用通行码锁定设备的选项。

  [#559098]

- 使用其他用户在 Android for Work 中重新注册设备时，“Google Directory 主电子邮件”字段不会更新为新的用户信息。

  [#559161]

- 将 Google Play 应用程序推送到 Android for Work 设备失败。

  [#559174]

- 部署 Android for Work 应用程序限制策略后，XenMobile 控制台中的“设备”选项卡无法访问。此外，也无法编辑新创建的策略。

  [#560225]

- 无法在 Android for Work 平台上上载未经批准的公共应用商店。

  [#560390]

- 如果选择的部署条件为“仅当之前的部署失败时”，部署打包应用程序并将应用程序安装到已注册的设备上后，用户随后访问

Worx Store 时，应用程序不显示。应用程序图标也不再显示到设备的 Springboard 上。

[#560500]

- 在 XenMobile 控制台中，配置通用 GPKI 实体时，如果在不进行身份验证的情况下设置后端 PKI 适配器服务器，GPKI 不会连接到 HTTPS 端口。出现以下错误：Could not locate the WSDL with the URL you provided.Check the WSDL URL and try again.（找不到使用您提供的 URL 的 WSDL。请检查 WSDL URL 并重试。）

  [#560707]

- Android for Work 服务器设置不正确时，可以启用 Android for Work。

  [#561475]

- 可以将自托管的 Android for Work 应用程序作为必须的应用程序添加到交付组中。

  [#561485]

- 在 XenMobile 控制台中，配置 iOS 安全操作锁定选项时，“电话号码”字段允许输入多个加号 (+)。

  [#561792]

- 在 XenMobile 控制台中，保存 Samsung KNOX 设备限制策略时，出现错误消息。

  [#562607]

- 如果在未首先导入 Android for Work 证书时保存 Android for Work 配置，会出现配置错误。

  [#562983]

- 创建适用于 Samsung KNOX 的应用程序卸载设备策略，然后部署此策略以删除特定应用程序时，应用程序从 KNOX 容器中删除且图标从设备 Springboard 中删除，但是大约 3 到 4 秒钟以后，应用程序再次出现。

  [#562713]

- 配置 Android for Work Samsung 浏览器设备策略时，书签 URL 未验证。

  [#565379]

- 在 XenMobile 控制台中，创建 Samsung SAFE 设备限制策略时，保存策略时出现错误消息。

  [#565697]

XenMobile Server 10.1 已知问题

Aug 04, 2016

以下是 XenMobile 10.1 中的已知问题。

- 在 XenMobile 10.x 中，只能根据其预设的 Windows 2000 名称搜索组名称，因为 XenMobile 控制台显示 sAMAccountName，而非显示 CN。
- 由于在 TLS v1 实现中，运行 Windows 2008 的服务器上的 IIS 具有 SSL 握手缺陷，Java 8 会出现问题：

  [#492269]

- 利用一种解决方法，Windows 2008 R2 证书颁发机构可支持 XenMobile Server 10.1。 要启用 TLSv1.1 和 TLSv1.2 支持，请遵循 Microsoft 知识库文章 https://support.microsoft.com/zh-cn/kb/245030 中“SCHANNEL\Protocols 子键”部分的说明。
- XenMobile Server 10.1 不支持 Windows 2008“vanilla”证书颁发机构。
- 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]
- 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]
- 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]
- 创建将“禁用的用户”设置为 True 的操作时，触发问题时，不执行所配置的操作。
  [#531024]
- 如果配置 XenMobile 服务器时主机名中含有大写字母，例如 ABC.Xms.com，设备注册后，Worx Store 不会在设备上打开。
  [#545527]
- 在处于 Android for Work 模式的 Android 设备上，如果添加采用 GPKI 凭据提供程序或 Microsoft Certificate Services 的 PKI 实体并在凭据设备策略中将凭据与另一个设备关联，用户从 Worx Home 刷新设备策略时，证书被错误地吊销并重新生成。 解决方法是仅部署一次证书。
  [#547905]
- 为 Windows Phone 8.1 设备创建 Exchange 设备策略并将“日志记录级别”设置为“基本”时，部署失败。 这是第三方问题。
  [#555923]
- 在 XenMobile 控制台中，配置适用于 Android for Work 的浏览器设备策略时，对于黑名单中的 URL，强制策略实施精确匹配。 例如，如果列出 http://www.example.com，则仅阻止此 URL，不阻止 https://www.example.com or http://www.example.com.pk。
  [#560963]
- Windows Phone 8.1 设备在证书续订后无法连接到 XenMobile 服务器。 这是第三方问题。
  [#561511]
- 可以通过 Android for Work 设备的控制板，在 XenMobile 控制台中选择完全擦除操作，但是设备不支持完全擦除操作。 选

择此操作时，Android for Work 设备进行选择性擦除，并且用户无法在 XenMobile 中重新注册，除非您从 XenMobile 中删除此设备。
[#562642]

- 在 Worx Home for iOS 上，启动托管于 XenApp Delivery Controller 上配置的显示名包含特殊字符 (#%^) 的 Windows 应用程序时，可能会显示错误“Access to your company network not available”（无法访问公司网络）。
  [#564069]

- 当您创建密码设备策略并将复杂度设置为字母数字或数字时，将此策略部署到 Windows Phone 8.1 设备上之后，用户无法在小键盘上选择字母。 这是第三方问题。
  [#565682]

- 在 Windows Phone 8.1 设备上，如果用户在注册时选择不安装 Worx Home，所需的企业应用程序将错误地自动部署并安装在设备上。
  [#566166]

- 在 XenMobile 控制台上，配置 RBAC 设置时，在“授权访问”中添加角色时，必须取消选中“管理控制台访问”复选框，或在“控制台功能”中选择一个或多个选项。 如果不这样做，您仍可以添加角色，但当用户登录控制台时，将显示错误。
  [#567076]

- 未实施在 IOS 8.3+ 设备上需要 iTunes 密码。
  [#567434]

- 在 Windows Phone 8.1 上基于证书的 Worx Home 注册失败。 有关解决办法，请参阅 http://support.citrix.com/article/CTX141541。

  [#567812]

- 将数据从 XenMobile Enterprise 部署迁移到 XenMobile 10.1 后，注册后的 Windows Phone 8.1 设备出现以下问题：
  - 使用 Windows Phone 8.1 设备的用户无法登录 Worx Store。
  - 用户无法从 Worx Home 打开已安装的企业应用程序，但是可以从主菜单打开这些应用程序。
  - 用户无法打开 Worx Store。

  [#568316]

- 创建高级部署规则时，如果添加“受已知设备属性名称限制”规则并将属性值设置为 True 或 False，规则将起不到预期效果。例如，“受监督”等于 False 的规则不起作用。 解决方法是，为“受已知设备属性名称限制”规则选择的属性值应该为布尔值：0 表示 False，-1 表示 True。
  [#568964]

- 由于 APNS 中存在的延迟，注册 Worx Home 后，不会将所有必需的 iOS 应用程序发布给所有用户。
  [#569978]

- 在命令行接口中提供主机名时，如果输入无效字符，不会显示错误。 主机名的第一个字符不能是 - 并且不能包含以下字符：$? /

  [#570147]

- 在 XenMobile 控制台上，打开“设置”->“NetScaler Gateway”时，会看到以下说明：“如果 NetScaler Gateway 与 StoreFront 共同用作身份验证服务器，还需要启用 StoreFront。”这是不正确的。 您无需针对 StoreFront 执行任何操作。
  [#570820]

- 为 Android 和 Android for Work 平台配置单个设备策略时，用于 Android 设备的策略也会在 Android for Work 设备上生效。 解决方法为，为每个平台单独配置一个策略，并向每个策略分配不同的用户。 即，将使用 Android 设备的用户分配给 Android 策略，将使用 Android for Work 设备的用户分配给 Android for Work 策略。
  [#570828]

- 在 XenMobile 控制台上，配置与 ShareFile 的连接时，如果 ShareFile 管理员密码包含字符 **%** 或 **^**，将会出现错误或其他虚拟行为。 为避免这种情况，请将 ShareFile 管理员帐户密码改为不包含字符 **%** 或 **^**。。
  [#571283]

- 用户无法使用“用户名 + PIN”的注册方法注册运行 Android for Work 的设备。此设置显示在 XenMobile 控制台中的“配置”->“设置”->“注册”->“用户名 + PIN”中。

  [#571919]

- 将 sAMAccountName 作为用户搜索的方式来配置 LDAP 时，Android 设备无法在 Android for Work 模式下注册。 这是第三方问题。
  [#571927]

- 在云部署中，“支持”页面下的“NetScaler Gateway 连接检查”可能错误地将 STA 状态显示为“失败”。
  [#573564]

- 运行 Android 的设备可能存在重新注册问题。 这是第三方问题。

  [#574746]

- 如果在 SQL Server 上使用 SSL，在升级前通过 XenMobile 10.0 控制台上载可信根 CA 证书。 如果此操作失败，会导致循环重新启动。

  [#574751]

- 在“维护”模式下计划关闭群集节点，因为可能会有为期两分钟的中断。
  [#575644]

- 仅在启动群集中的第一个节点后再加入新节点。

  [#575671]

- 尝试在 XenMobile 控制台中配置 iOS Device Enrollment Program 时会出现无效配置文件错误。 这是第三方问题。

  [#607143]

- 根据 XenMobile **设置 > Google Play 凭据**页面上的说明，当前不能在您的手机上通过输入 *#*#8255#*#* 查找 Android ID。 请使用 Google Play 应用商店中的设备 ID 应用程序查找您的设备 ID。

  [#633854]

体系结构概述

Oct 13, 2016

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

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

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

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

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

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

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

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

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

移动设备管理 (MDM) 模式

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

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

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

移动应用程序管理 (MAM) 模式

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

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

MDM+MAM 模式

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

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

内部网络中的 XenMobile

可以在内部网络中（而非 DMZ 中）部署适用于 XenMobile 的体系结构，以满足下面的一个或多个要求：

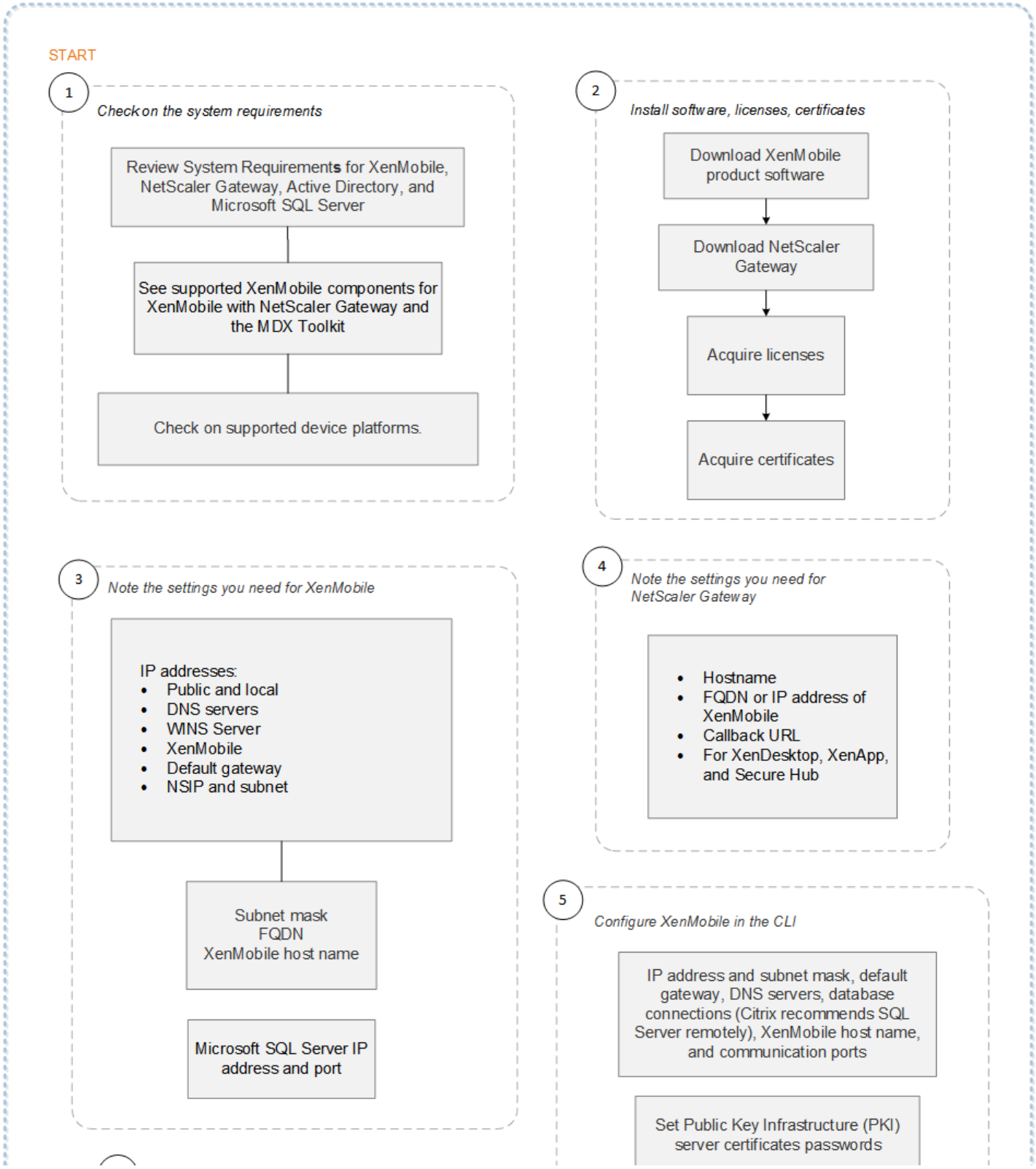
- 您在 DMZ 中未安装或不允许您安装虚拟机管理程序。
- 您的 DMZ 只能包含网络设备。

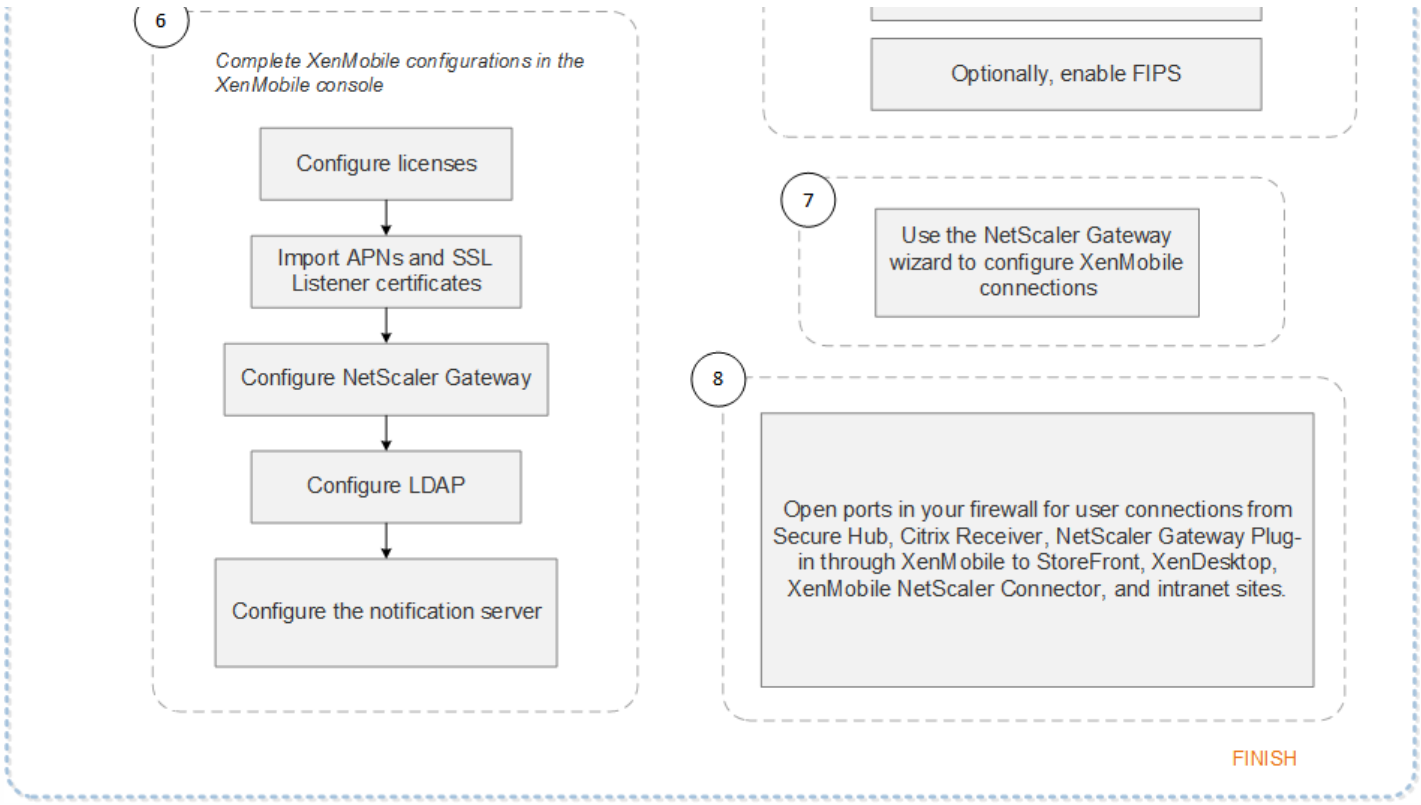
在此部署中，由于 XenMobile 服务器不在 DMZ 中，因此，您不需要在内部防火墙上打开端口即可允许从 DMZ 访问 SQL Server 和 PKI 服务器。

部署 XenMobile 与 NetScaler Gateway 的流程图

Aug 04, 2016

可以使用此流程图作为指导以完成部署 XenMobile 10.1 与 NetScaler Gateway 的主要步骤。图后面提供每个步骤的主题链接。





1

- XenMobile 10.1 的系统要求
- XenMobile 兼容性
- XenMobile 10.1 支持的设备平台

2

- 安装 XenMobile
- XenMobile 中的证书
- XenMobile 许可

3

- XenMobile 预安装核对表

4

- XenMobile 预安装核对表

5

- 在命令提示窗口中配置 XenMobile

6

- 在 Web 浏览器中配置 XenMobile

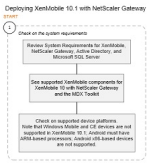
7

- 配置 XenMobile 环境的设置

8

- XenMobile 端口要求

单击缩略图可下载 PDF 格式的流程图。



扩展 XenMobile

Nov 10, 2015

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。

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 16667 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

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。

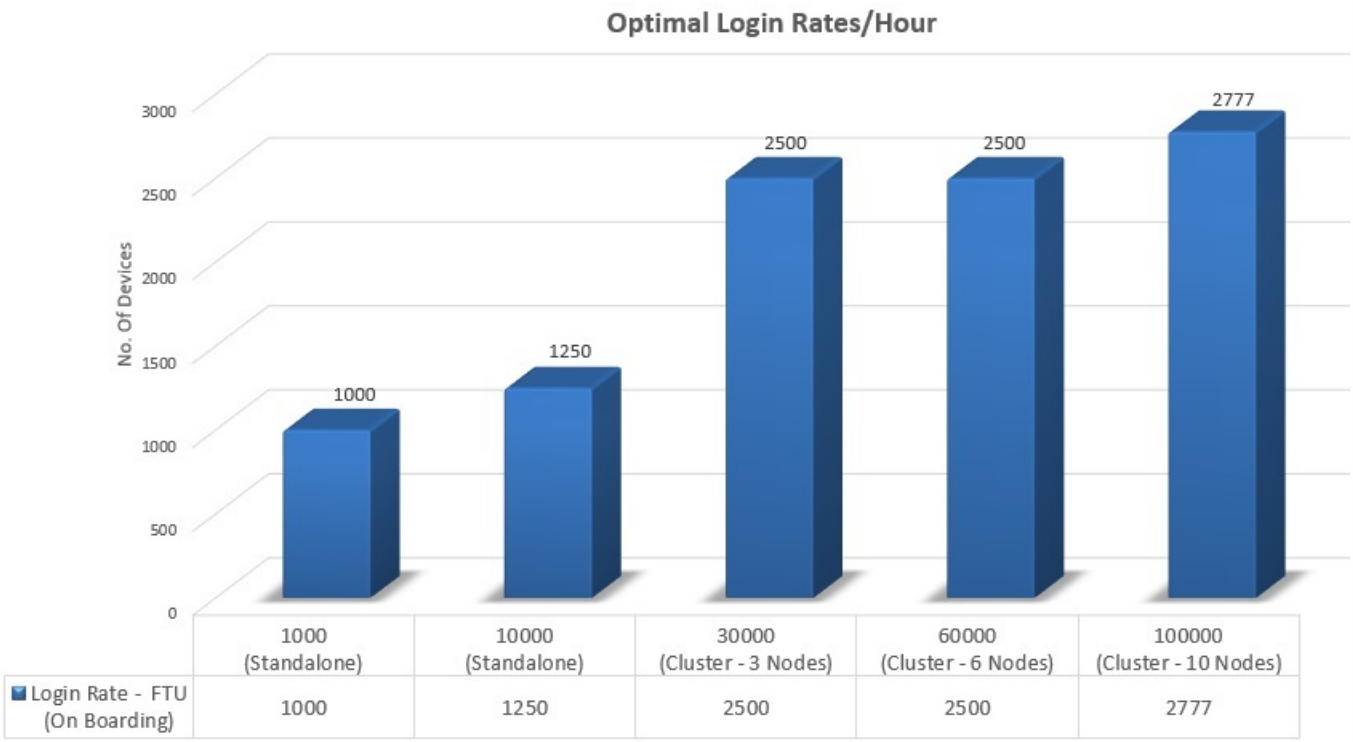
- 为实现最大可扩展性，增加了 XenMobile 上的 CPU 和 RAM 资源。
- 10 个节点的群集配置是经过验证的最大配置。扩展到大于 10 个节点需要其他 XenMobile 实现。

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**	**100000**
登录率					
加入率 (FTU)	125	1250	2,500	2,500	2,777
现有用户数	1,000	2,500	7500	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。

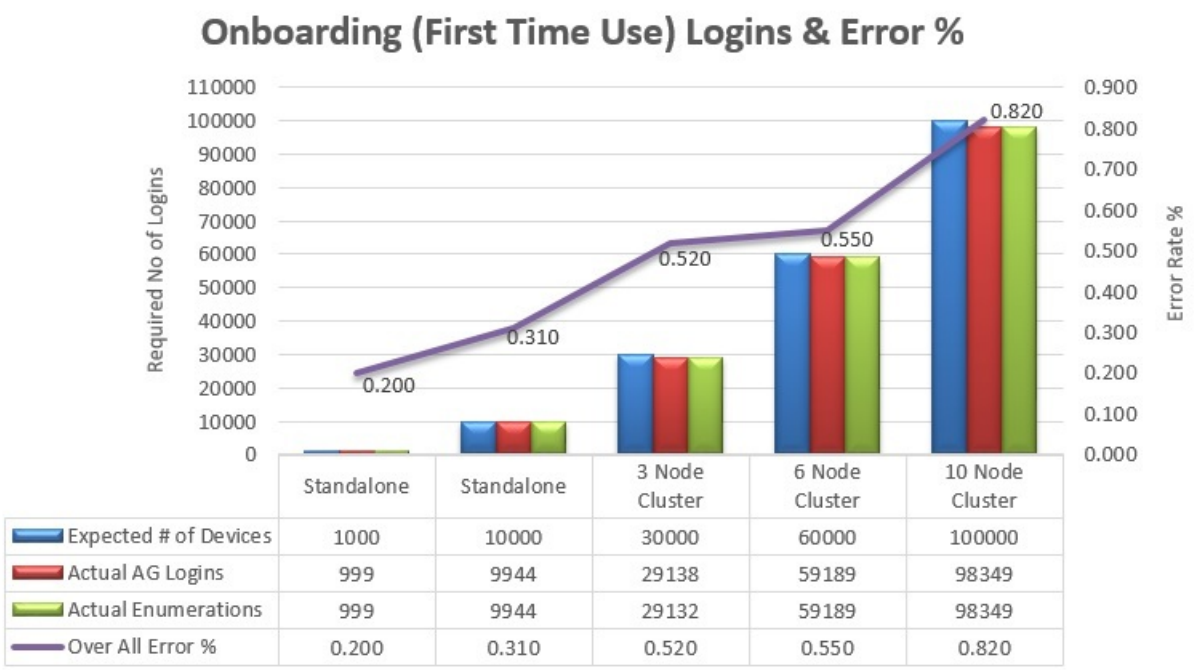
图 1. 带注册的 XenMobile Enterprise — 每小时的登录率



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。

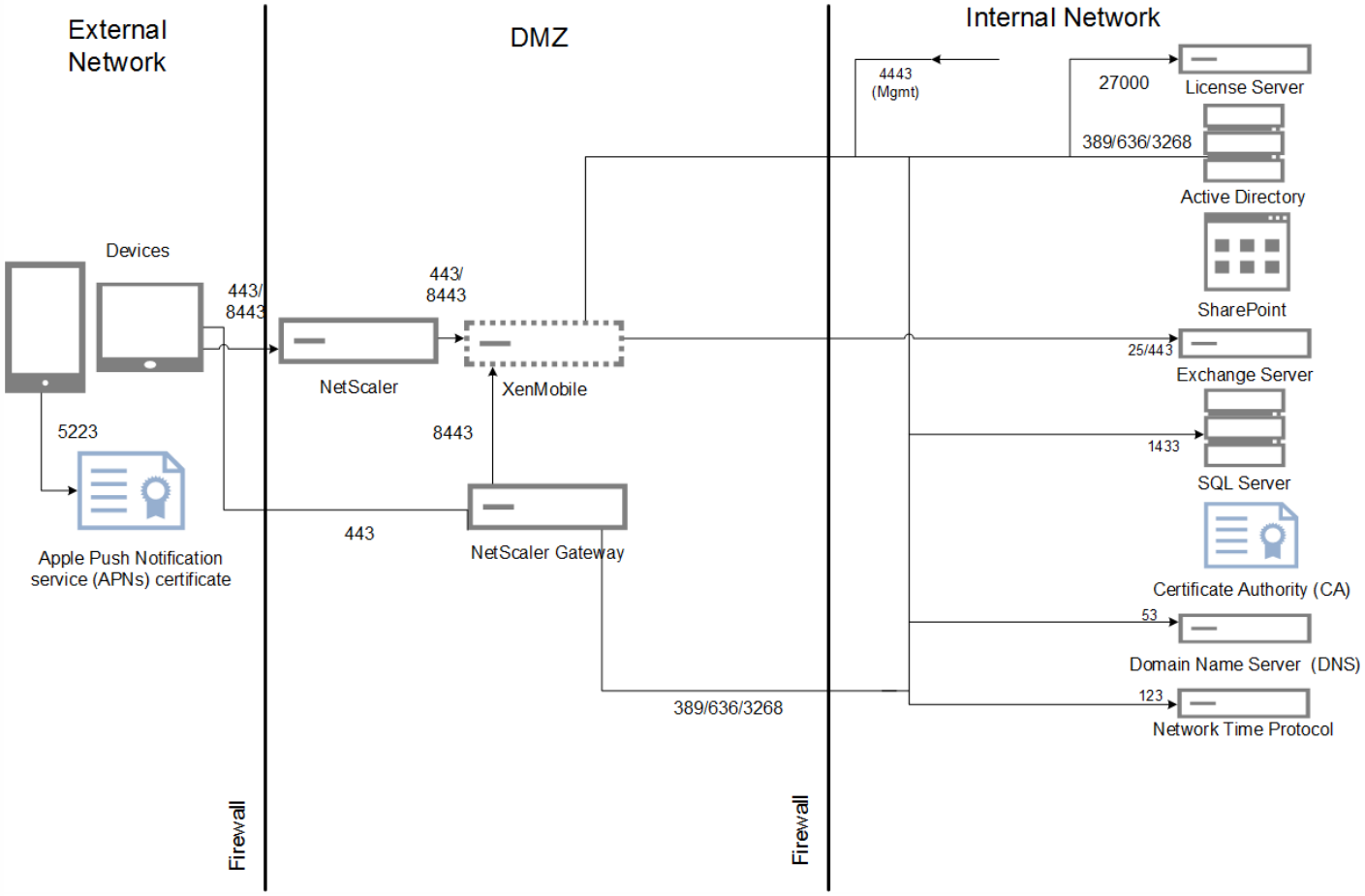
- 注册或登录延迟（往返时间）
  - 平均总延迟：> 1.5 秒
  - NetScaler Gateway 登录的平均延迟：> 440 毫秒
  - Worx Store 请求的平均延迟：> 3 秒
- 达到扩展限制时，基础结构组件上会出现物理性能下降的情况，如 CPU 和内存耗尽。
  - NetScaler Gateway 和 XenMobile 设备上出现无效响应。
  - XenMobile 控制台响应速度变慢。

图 2. 注册的加入 (FTU) 登录数和错误百分比

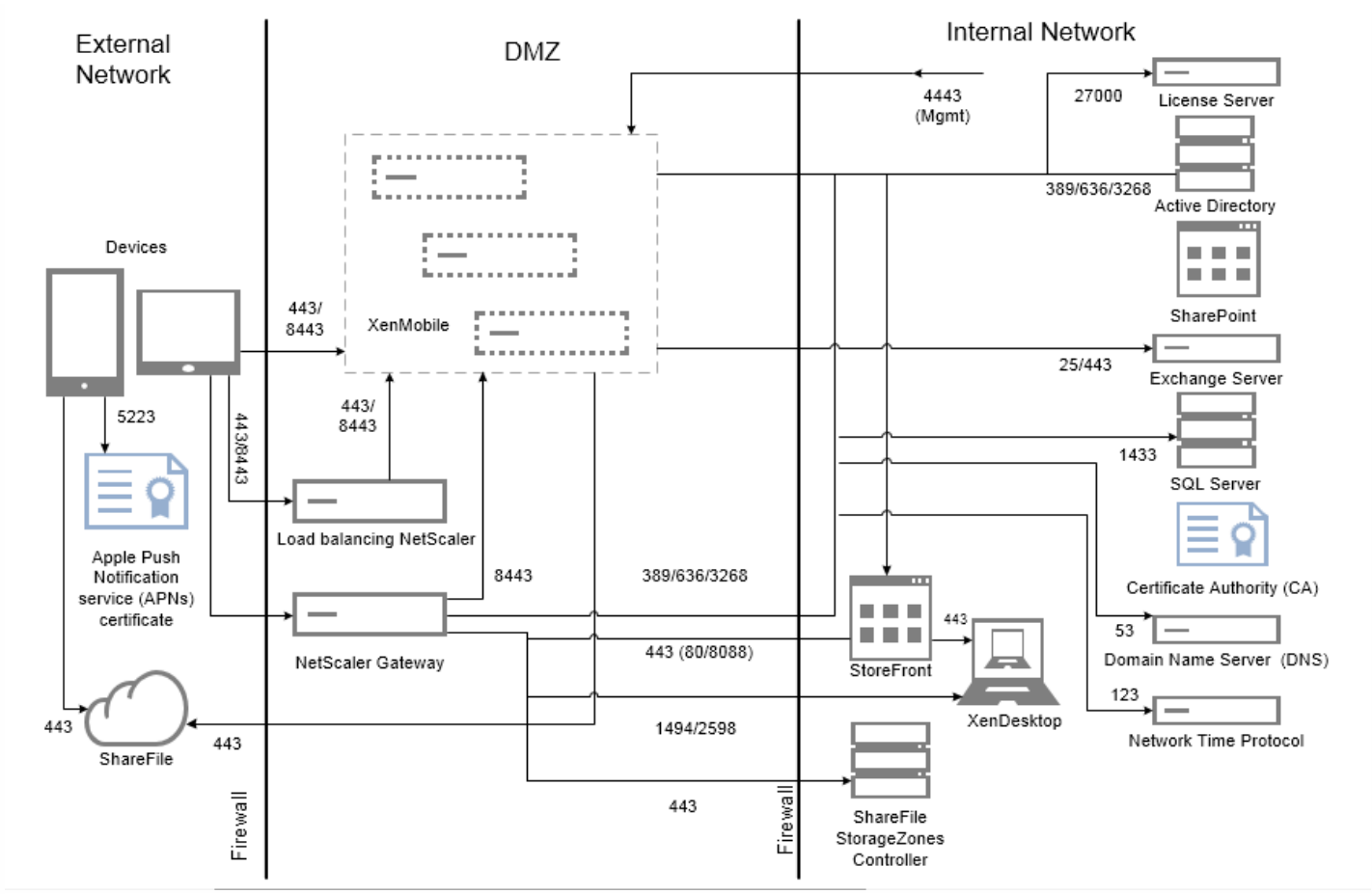


上图中的错误百分比包括遇到的总错误，考虑了每个操作对应的请求，并非仅限于登录。根据退出条件中的定义，运行的每个测试的错误百分比都在可接受的限制内。

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 MAM 功能，可支持 10,000 台或更多设备。



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。

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。

注意事项与假设

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

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

-

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

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

应在所有 XenMobile 节点上执行这些更改，然后重新启动服务器。

可扩展性测试不包括以下场景。在以后增强扩展测试功能时会考虑这些场景：

- 未测试将策略推送到设备。
- 未测试连接到 Android 的设备。
- 未测试软件包部署。
- 未测试 Windows 平台。

每个 XenMobile 最多同时支持 10000 个连接。

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

加入 (FTU) 工作负载

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

- 自动检测
- 注册
- 身份验证
- 设备注册
- 应用程序交付（web、SaaS 和移动 MDX 应用程序）
  - 应用程序订阅（包括图像和图标下载）
  - 已订阅 MDX 应用程序的安装
- 应用程序启动（web、SaaS 和移动 MDX 应用程序）
- 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。

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。

下表列出了用于这些测试的 XenMobile 基础结构软件。

表 8. XenMobile 基础结构组件

组件	版本
NetScaler Gateway	10.5-57.4.nc

XenMobile	10.1.0.63030
外部数据库	MS SQL Server 2014 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 9. XenServer 硬件

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

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

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 Cloud

Aug 04, 2016

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

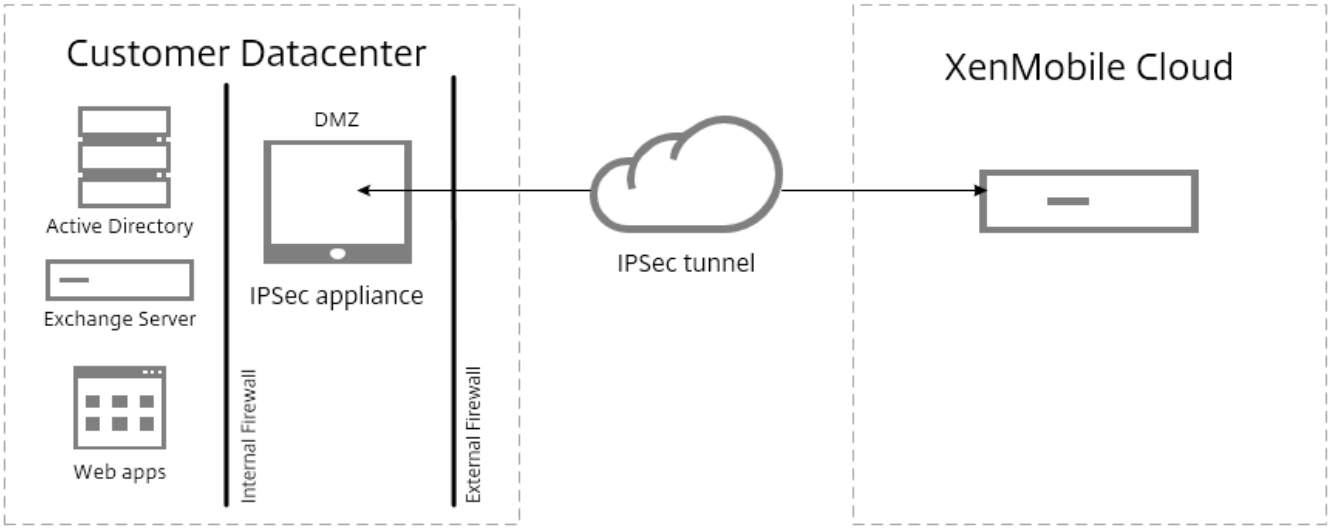
Cloud Operations 管理员处理网络连接的维护和配置，以及 Citrix 产品的集成，如 NetScaler、XenApp、XenDesktop、StoreFront 和 ShareFile。 Cloud 环境托管于遍及全球的 Amazon 数据中心内，可提供高性能、快速响应和支持。

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

注意

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

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



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

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

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	Advanced	群集信息	Cloud 管理员和技术支持人员
支持	Advanced	垃圾回收	Cloud 管理员和技术支持人员
支持	Advanced	Java 内存属性	Cloud 管理员和技术支持人员
支持	Advanced	宏	IT 管理员
FTU向导	初始配置	NetScaler Gateway	仅 Cloud 管理员或仅 IT 管理员

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

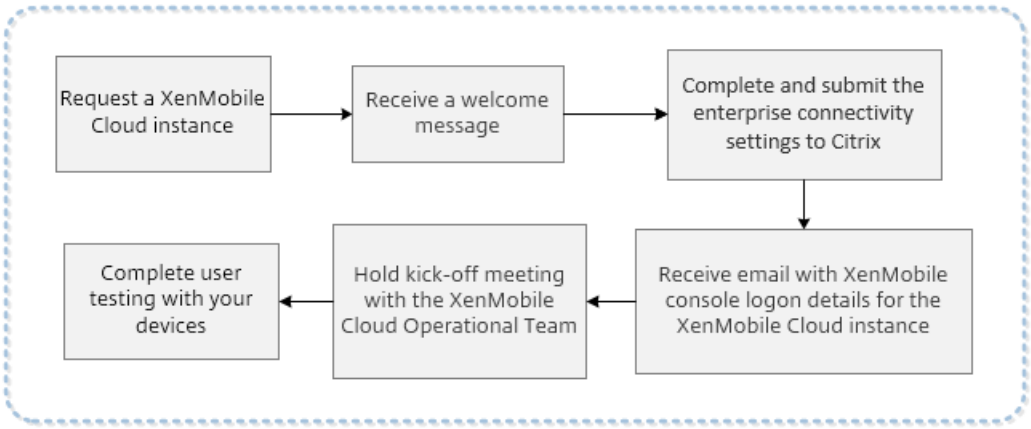
有关自定义角色的分步说明，请参谋使用 RBAC 配置角色。

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

XenMobile 云必备条件和管理

Apr 22, 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

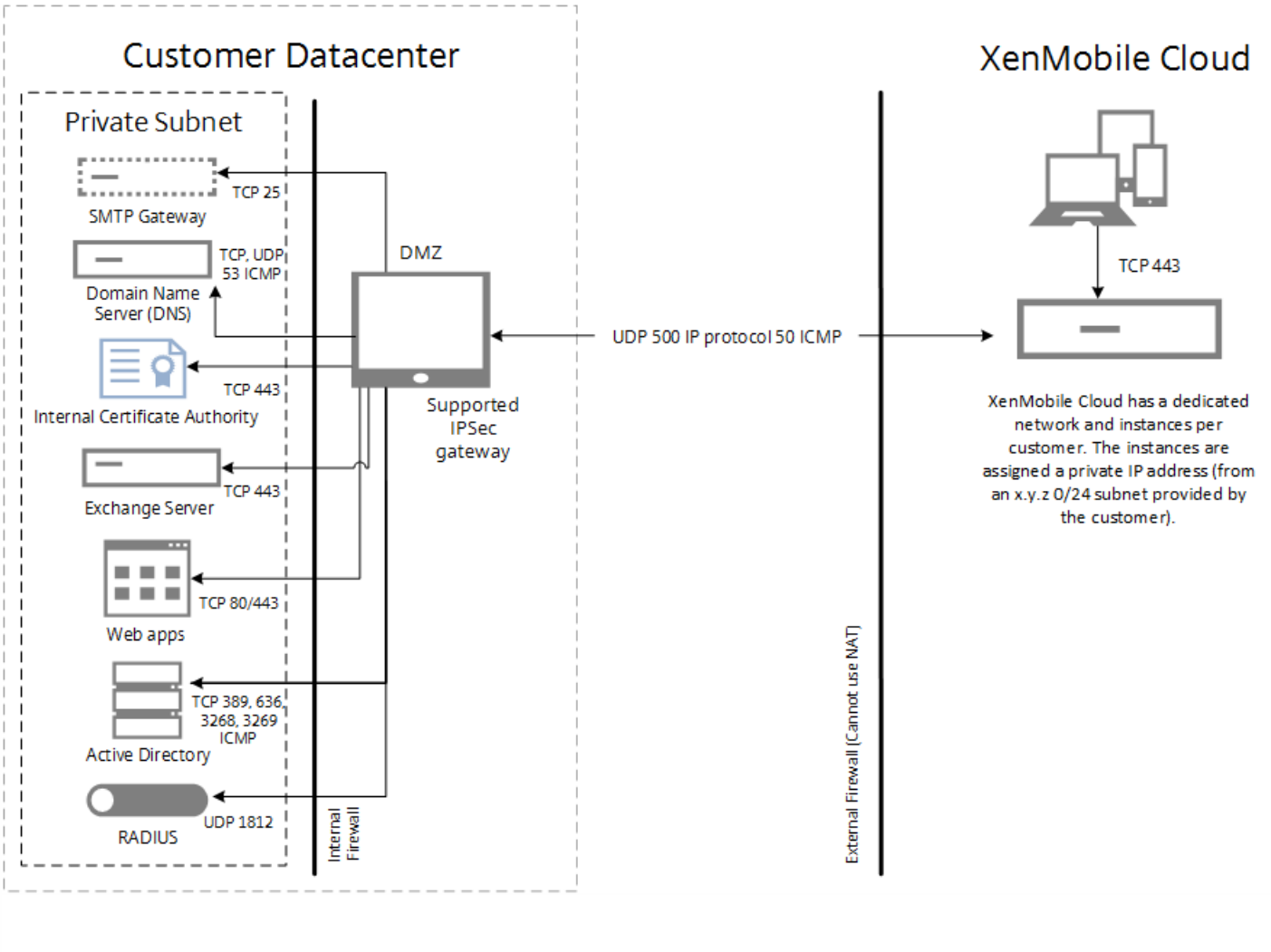
可以使用 XenMobile Enterprise Connector，这是一个 IPsec 通道，用于将 XenMobile 云基础结构与公司服务相连接，例如 Active Directory。

以下 Amazon Web ServicesWeb 站点中列出的 IPsec 网关已通过正式测试，支持 XenMobile 云解决方案：http://aws.amazon.com/cn/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

Oct 22, 2015

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。

- 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 Apps 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。

- 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。

- 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

Aug 04, 2016

要运行 XenMobile 10.1，需要满足以下最低系统要求：

- 以下其中一种：
  - XenServer（支持的版本：6.5.x、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
- 16 GB RAM

要在 XenMobile 10.1 中运行 NetScaler Gateway，需要满足以下最低系统要求：

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

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

XenMobile 需要使用以下数据库之一：

- Microsoft SQL Server

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

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

  XenMobile 10.1 支持 SQL Server AlwaysOn 可用性组。

  Citrix 建议远程使用 Microsoft SQL。

注意：请确保要在 XenMobile 上使用的 SQL Server 的服务帐户具有 DBcreator 角色权限。 有关 SQL Server 服务帐户的详细信息，请参阅 Microsoft Developer Network 站点上的以下页面（这些链接指向有关 SQL Server 2014 的信息。 如果您使用的是其他版本，请从**其他版本**列表中选择服务器版本：
Server Configuration - Service Accounts（服务器配置 - 服务帐户）

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

Server-Level 角色

- PostgreSQL

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

  注意：所有 XenMobile 版本都支持适用于 Windows 的 Remote PostgreSQL 9.3.11，但存在以下限制：

  - 最多支持 300 个设备

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

  - 不支持群集

XenMobile 10.1 支持以下邮件服务器：

- Exchange 2013
- Exchange 2010

XenMobile 兼容性

Apr 22, 2016

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

支持的设备平台

Apr 22, 2016

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

端口要求

Oct 13, 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。

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

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

	SaaS 应用程序交付。		
	用于与 XenMobile 服务器的一般设备通信	XenMobile	XenMobile
	注册时用于从移动设备到 XenMobile 的连接。	Internet	XenMobile
	用于从 XenMobile 到 XenMobile NetScaler Connector 的连接。	XenMobile	XenMobile NetScaler Connector
	用于从 XenMobile NetScaler Connector 到 XenMobile 的连接。	XenMobile NetScaler Connector	XenMobile
	用于在未进行证书身份验证的部署中的回调 URL。	XenMobile	NetScaler Gateway
514	用于 XenMobile 与 Syslog 服务器之间的连接。	XenMobile	Syslog 服务器
636	用于安全 LDAP 连接。	NetScaler Gateway XenMobile	LDAP 身份验证服务器或 Active Directory
1494	用于与内部网络中基于 Windows 应用程序的 ICA 连接。 Citrix 建议保持此端口处于打开状态。	NetScaler Gateway	XenApp 或 XenDesktop
1812	用于 RADIUS 连接。	NetScaler Gateway	RADIUS 身份验证服务器
2598	用于使用会话可靠性连接到内部网络中基于 Windows 的应用程序。 Citrix 建议保持此端口处于打开状态。	NetScaler Gateway	XenApp 或 XenDesktop
3268	用于 Microsoft Global Catalog 非安全 LDAP 连接。	NetScaler Gateway XenMobile	LDAP 身份验证服务器或 Active Directory
3269	用于 Microsoft Global Catalog 安全 LDAP 连接。	NetScaler Gateway XenMobile	LDAP 身份验证服务器或 Active Directory
9080	用于 NetScaler 和 XenMobile NetScaler Connector 之间的 HTTP 流量。	NetScaler	XenMobile NetScaler Connector

9443	用于 NetScaler 和 XenMobile NetScaler Connector 之间的 HTTPS 流量。	NetScaler	XenMobile NetScaler Connector
45000 80	用于部署在群集中的两个 XenMobile VM 之间的通信。	XenMobile	XenMobile
8443	用于注册、XenMobile Store 和移动应用程序管理 (MAM)。	XenMobile NetScaler Gateway 设备 Internet	XenMobile
4443	用于管理员通过浏览器访问 XenMobile 控制台。	访问点（浏览器）	XenMobile
	用于从一个节点为所有 XenMobile 群集节点下载日志和支持捆绑包。	XenMobile	XenMobile
27000	用于访问外部 Citrix 许可证服务器的默认端口	XenMobile	Citrix 许可证服务器
7279	用于签入和签出 Citrix 许可证的默认端口。	XenMobile	Citrix 供应商守护程序

必须打开以下端口以允许 XenMobile 在网络中通信。

TCP 端口	说明	源	目标
25	XenMobile 通知服务的默认 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 或 Windows Phone 应用商店之间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 和 *.mzstatic.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)
	用于 XenMobile 与 Nexmo SMS Notification Relay 之间的出站连接。		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
	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	
	用于 Android 和 Windows Mobile 的注册和代理安装。	Internet	XenMobile
1433	默认用于与远程数据库服务器的连接（可选）。	XenMobile	SQL Server
2195	用于 Apple 推送通知服务 (APNs) 到 gateway.push.apple.com 的出站连接，适用于 iOS 设备通知和设备策略推送。	XenMobile	Internet（使用公用 IP 地址 17.0.0.0/8 的 APNs 主机）
2196	用于到 feedback.push.apple.com 的 APNs 出站连接，适用于 iOS 设备通知和设备策略推送。		
5223	用于从 Wi-Fi 网络上的 iOS 设备到 *.push.apple.com 的 APNs 出站连接。	WiFi 网络上的 iOS 设备	Internet（使用公用 IP 地址 17.0.0.0/8 的 APNs 主机）
8443	用于 iOS 和 Windows Phone 设备注册。	Internet	XenMobile
		LAN 和 WiFi	

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

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

对启用证书固定功能感兴趣的客户必须完成以下必需操作：

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

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

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

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

FIPS 140-2 合规性

Oct 22, 2015

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。
XenMobile Device Manager 上的所有静态数据和传输中数据加密操作使用 OpenSSL 提供的加密模块，该模块经验证符合 FIPS 规范。（有关最新的开发，请参阅以下详细信息。）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通过验证的加密模块。

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

Apr 22, 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。

下表显示了 Worx 应用程序的最新版本已翻译成的语言，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
Apple iPhone/iPad											
Worx Home	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	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
WorxMail	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X			

WinPhone						
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。

下表概述了 XenMobile 控制台翻译状态，其中 X 指示语言可用性。

语言	简体中文	法语
XenMobile 控制台	X	X

预安装核对表

Nov 10, 2015

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

以下是 XenMobile 解决方案需要的网络设置。

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

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

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

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

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

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

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

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

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

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

	必备项	组件	记录设置
	Microsoft SQL Server IP 地址和端口。 确保要用于 XenMobile 的 SQL Server 服务帐户具有 DBcreator 角色权限。 在 FIPS 模式下安装 XenMobile 服务器时，需要完成 SQL Server 的必备条件。有关详细信息，请参阅 Configuring FIPS with XenMobile（在 XenMobile 中配置 FIPS）。	XenMobile	

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

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

Citrix 建议在 NetScaler 中使用快速配置向导来配置 XenMobile 与 NetScaler Gateway 之间以及 XenMobile 与 Worx Home 之

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

	必备项	组件	记录设置
	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	

安装 XenMobile

Oct 13, 2016

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

开始之前的准备工作：规划 XenMobile 部署有多个注意事项。 有关您的端到端 XenMobile 环境的建议、常见问题和用例，请参阅《XenMobile 部署手册》。 此外，还请参阅 XenMobile 10.1 的系统要求和 XenMobile 安装前核对清单。

注意：请务必为虚拟机管理程序配置正确的时间，因为 XenMobile 会使用该时间。 此外，请务必在虚拟机属性中对 XenMobile 虚拟机进行配置，使其将客户机时间与主机同步。

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。

FIPS 模式必备条件：在 FIPS 模式下安装 XenMobile 服务器时，需要完成 SQL Server 的必备条件。 有关详细信息，请参阅 Configuring FIPS with XenMobile（在 XenMobile 中配置 FIPS）。

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。
- 如果安装 Windows Server 2008 R2 或 Windows Server 2012，请执行以下操作：
  - 删除 Virtual Machines/<build-specific UUID>.xml 文件
  - 将 Legacy/<build-specific UUID>.exp 文件移到虚拟机内

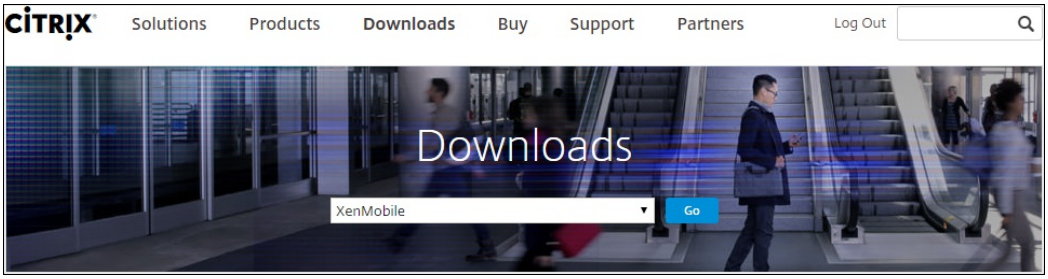
  由于有两个不同版本的 Hyper-V 清单文件可以表示 VM 配置 (.exp and .xml)，因此这些步骤十分必要。 Windows Server 2008 R2 和 Windows Server 2012 版本仅支持 .exp。 对于这些版本，您在安装前必须只具有 .exp 清单文件。

  Windows Server 2012 R2 不要求执行这些额外步骤。

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

下载 XenMobile 的软件

1. 转至 Citrix Web 站点。
2. 在“搜索”框旁边，单击登录以登录您的帐户。
3. 单击下载选项卡。
4. 在下载页面上，从“选择产品”列表中，单击 XenMobile。



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

下载 NetScaler Gateway 的软件

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

1. 转至 Citrix Web 站点。
2. 如果尚未登录 Citrix Web 站点，在“搜索”框旁边，单击登录以登录您的帐户。
3. 单击下载选项卡。
4. 在下载页面上，从选择产品列表中，单击 NetScaler Gateway。
5. 单击转到。 此时将显示 NetScaler Gateway 页面。
6. 在 NetScaler Gateway 页面上，展开 10.5。
7. 在固件下面，单击要下载的设备软件版本。
   注意：还可以单击 Virtual Appliances（虚拟设备）以下载 NetScaler VPX。选择此选项时，将显示适用于每个虚拟机管理程序所对应的虚拟机的软件列表。
8. 单击要下载的设备软件版本。
9. 在要下载版本的设备软件页面上，单击相应虚拟设备的下载。
10. 按照屏幕上的说明下载软件。

为首次使用配置 XenMobile 的过程包括两个部分。

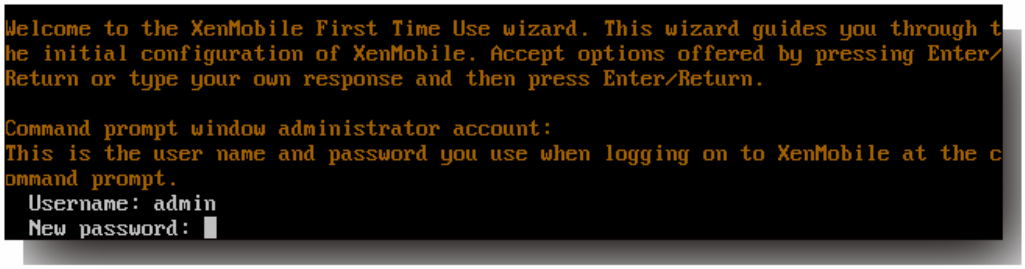
1. 通过使用 XenCenter 或 vSphere 命令行控制台，配置 XenMobile 的 IP 地址和子网掩码、默认网关、DNS 服务器等。
2. 登录 XenMobile 管理控制台并按照初始登录屏幕上的步骤操作。

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

在命令提示窗口中配置 XenMobile

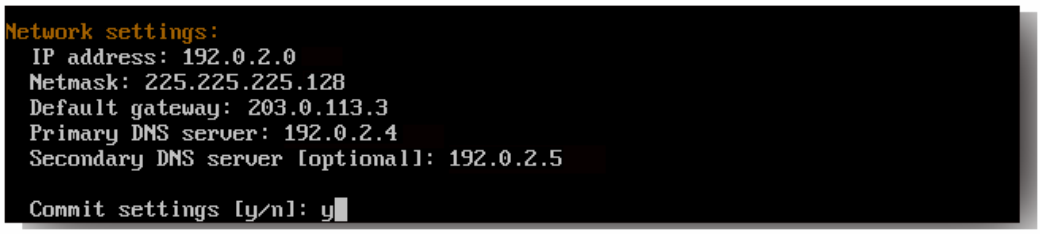
1. 将 XenMobile 虚拟机导入 Citrix XenServer、Microsoft Hyper-V 或 VMware ESXi。 有关详细信息，请参阅 XenServer、Hyper-V 或 VMware 文档。

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



   注意：键入新密码时，不会显示字符，如星号。 不会显示任何内容。

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



   注意：本图片和后面的图片中显示的地址并不可用，仅作为示例提供。

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

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

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，如在 XenMobile 中配置 FIP中所述。

7. 提供以下信息以配置数据库连接：

```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server: 198.0.2.10
  Port: 5432
  Username: postgres
  Password:
```

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

   注意：XenMobile 服务器的 FQDN 是适用于 XenMobile 注册的公共 DNS。

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

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

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

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

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

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

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

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

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

注意：键入新密码时，不会显示字符，如星号。 不会显示任何内容。

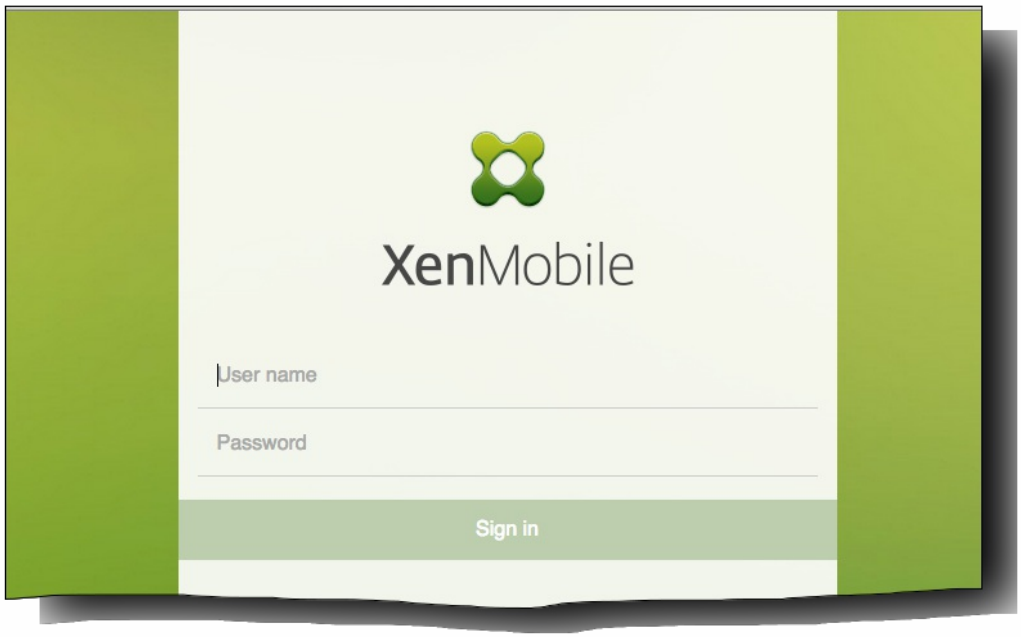
17. 按 Enter 提交设置。 此时已保存初始系统配置。
18. 当询问是否为升级时，请键入n ，因为这是全新安装。
19. 完整复制屏幕上显示的 URL，并在 Web 浏览器中继续此初始 XenMobile 配置。

```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
  Upgrade from previous release (y/n) [n]:

Stopping configuration app...                                    [ OK ]
Starting configuration app...
  application started successfully                               [ OK ]
Stopping main app...                                             [ OK ]
Starting main app...
  this may take a few minutes.....................................................
.................................
  application started successfully                               [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://203.0.113.8:4443/

Starting monitoring...                                           [ OK ]
```

在 Web 浏览器中配置 XenMobile

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

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



3. 在“入门”页面中，单击开始。 此时将显示“Licensing”（许可）页面。
4. 配置许可证。 XenMobile 附带的是评估许可证，有效期为 30 天。 有关添加和配置许可证以及配置过期通知的详细信息，请参阅 XenMobile 许可。
   重要：如果打算将 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：此步骤需要重新启动服务器。
7. 如果适用于环境，请配置 NetScaler Gateway。 有关配置 NetScaler 网关的详细信息，请参阅 NetScaler Gateway 和 XenMobile 以及配置 XenMobile 环境的设置。
   注意：
   - 可以将 NetScaler Gateway 部署在组织内部网络（或 Intranet）的外围，以提供对内部网络中服务器、应用程序和其他网络资源的安全单点访问。 在此部署中，所有远程用户必须先连接到 NetScaler Gateway，才能访问内部网络中的任何资源。
   - 尽管 NetScaler Gateway 为可选设置，但在页面上输入数据后，必须清除或完成必填字段，才能离开页面。
8. 完成 LDAP 配置，以便从 Active Directory 访问用户和组。 有关配置 LDAP 连接的详细信息，请参阅 LDAP 配置。
9. 配置能够向用户发送消息的通知服务器。 有关通知服务器配置的详细信息，请参阅 XenMobile 中的通知。

在 XenMobile 中配置 FIPS

Nov 10, 2015

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

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

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

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

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

1. 初始安装过程中，启用 **FIPS mode**（FIPS 模式）。

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

    a.复制并粘贴 CA 证书。

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

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

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

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

5. 这些步骤完成后，请继续执行 XenMobile 初始安装。

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

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

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。

升级 XenMobile

Apr 22, 2016

XenMobile 软件的新版本可用时，可以升级到新版本。您可以根据您的情况使用两个升级选项:

- 要安装新版本的 XenMobile 10.1 软件、服务包和系统修补程序，可使用 XenMobile 控制台中的“版本管理”页面，本文稍后将进行介绍。
- 要从 XenMobile 9.0（MDM Edition、App Edition 和 Enterprise Edition）升级到 XenMobile 10.1，请使用升级工具。有关详细信息，请参阅本部分中的内容。可以从 Citrix.com 下载页面下载升级工具。

注意

- Citrix 建议您使用最新版本的升级工具。此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。当有新版本或重要更新可用时，我们会将其会发布到 Citrix.com 上，并向每个客户的在案联系人发送通知。
- 如果您的 XenMobile 9.0 安装基于指定的 SQL 实例，您需要遵循特定于此情况的步骤。有关详细信息，请参阅支持指定的 SQL 实例。

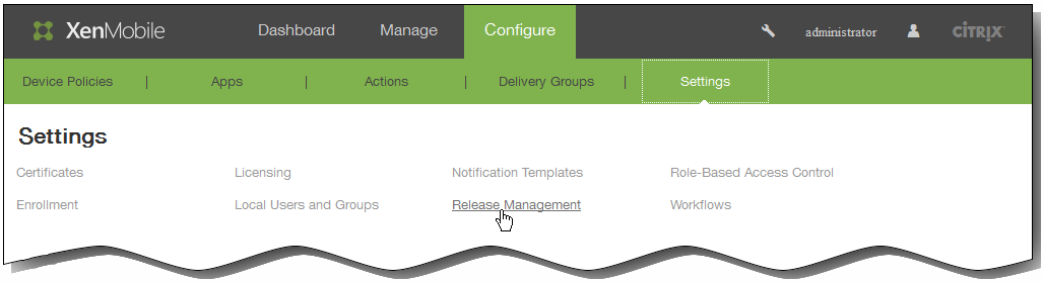
Important

- 请注意此 XenMobile 10.1 已知问题，因为您的 XenMobile 9.0 主机名称可能包含大写字母。 在此情况下，升级到 XenMobile 10.1 之后，设备无法访问 Worx Store。 如果配置 XenMobile 服务器时主机名称中含有大写字母，例如 ABC.Xms.com，则在设备注册后，Worx Store 不会在设备上打开。 [#545527]
- 升级到 XenMobile 10.1 后，如果在 XenMobile 10.1 中更新在早期版本中配置的 Worx 移动应用程序，则该应用程序的设置将不再显示在 XenMobile 控制台中。 您需要重新编辑并配置这些应用程序的设置。 不需要重新安装这些应用程序。 此步骤只需执行一次；如果您将来更新应用程序或服务器，这些值将不受影响。

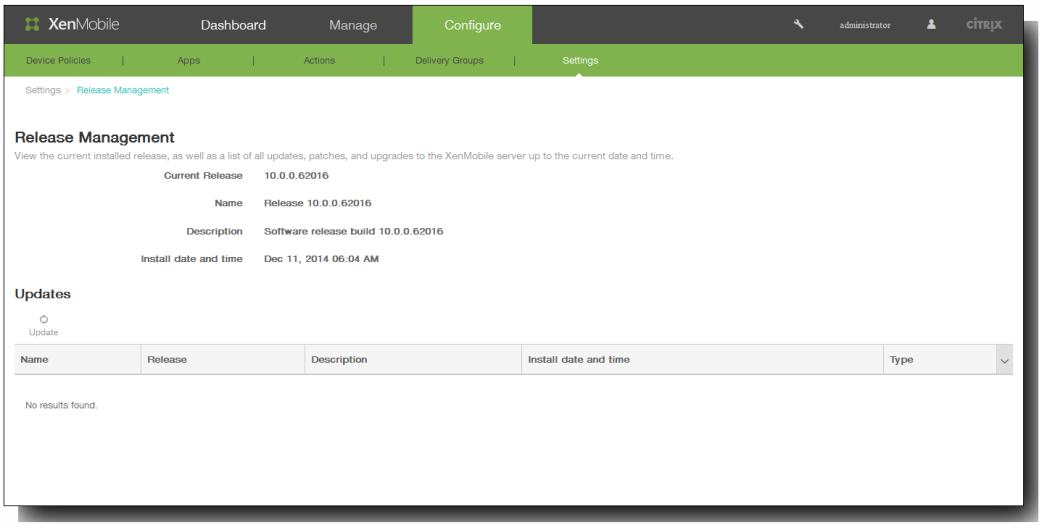
必备条件：

- 安装 XenMobile 更新前，请使用虚拟机 (VM) 中的设备创建系统的快照。
- 备份系统配置数据库。
- 检查系统要求。

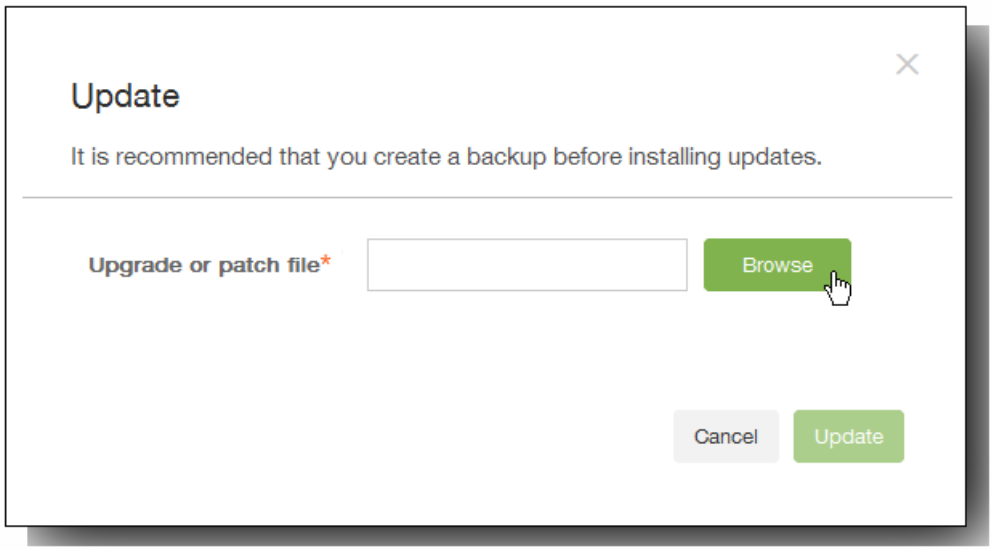
1. 在 Citrix Web 站点上登录您的帐户，然后将 XenMobile 升级 (.bin) 文件下载到合适的位置。
2. 在 XenMobile 控制台中，单击配置 > 设置 > 版本管理。



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。

关于升级工具

Aug 04, 2016

要从 XenMobile 9.0（MDM Edition、App Edition 和 Enterprise Edition）升级到 XenMobile 10.1，必须使用升级工具。该工具可以从 Citrix.com 下载页面下载。 本文稍后将列出本版本中的已修复问题和已知问题：

- 本版本的升级工具中的已修复问题
- 本版本的升级工具中的已知问题

最新版本的升级工具包括 UI 改进功能、支持远程 PostgreSQL 9.3.11 以及支持 Device Manager 9.0 RP3 和 App Controller RP7。

升级工具在 XenMobile 10.1 虚拟机中构建。 在 XenMobile 10.1 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。

升级路径

升级路径是指为确保正确迁移您的数据而建议执行的升级顺序。 本部分内容包含以下设备类型和注册模式组合的升级路径：

- iOS 和 Android 设备（所有注册模式）以及在 MDM 模式下注册的 Windows Phone 和 Windows Tablet
- 在企业模式下注册的 Windows Phone

  没有适用于在 MAM 模式下注册的 Windows Phone 或 Windows Tablet 的升级路径，也没有适用于在企业模式下注册的 Windows Tablet 的升级路径。

要升级，请从与您要升级的版本匹配的步骤开始按顺序进行操作：

1. 如果使用的是 XenMobile 8.6 或 8.7，请先升级到 XenMobile 9.0。

   不能使用升级工具从 XenMobile 8.6 或 8.7 升级到 XenMobile 10.1。

2. 使用升级工具从 XenMobile 9.0 升级到 XenMobile 10.1。

- 将 XenMobile 9 升级到 XenMobile 10.1 后，某些客户报告访问 WorxStore 、打开应用程序以及使用其他功能时会遇到问题。 虽然 Citrix 正在着力解决这些问题，但您可以暂时将升级回滚到 XenMobile 9。 有关详细信息，请参阅回滚 XenMobile 升级。
- 如果在 XenMobile 9.0 上启用了多租户控制台 (MTC)，则可以将 MTC 迁移到 XenMobile 10.1。 有关步骤，请参阅将 MTC 租户服务器升级到 XenMobile 10.1。

3. 将 XenMobile 10.1 更新到 XenMobile 10.3（或 10.3.5）。

   此更新按照从 XenMobile 9.0 升级到 10.1 的过程进行操作时，可以迁移受支持的 Android、iOS 和 Windows 设备类型的数据。

4. 将 XenMobile 10.3 更新到 XenMobile 10.3.5。

将 XenMobile 9.0 企业环境（包含在企业模式下注册的 Windows Phone 且使用 Worx Home 9.x）升级到 XenMobile 10.3 时，

建议执行以下步骤：

1. 安装适用于 Device Manager 和 App Controller 的最新修补程序。

2. 下载最新升级工具。

3. 将 Device Manager 上安装的 Worx Home 升级到 10.2，然后部署 Worx Home。

   如果用户运行的是注册了 Windows 手机的 Worx Home 9.x，我们建议您先将 Worx Home 升级到 10.2，然后再进行升级。 并且，升级到 10.1 后，必须在连接设备之前立即将 XenMobile 服务器升级到 10.3。

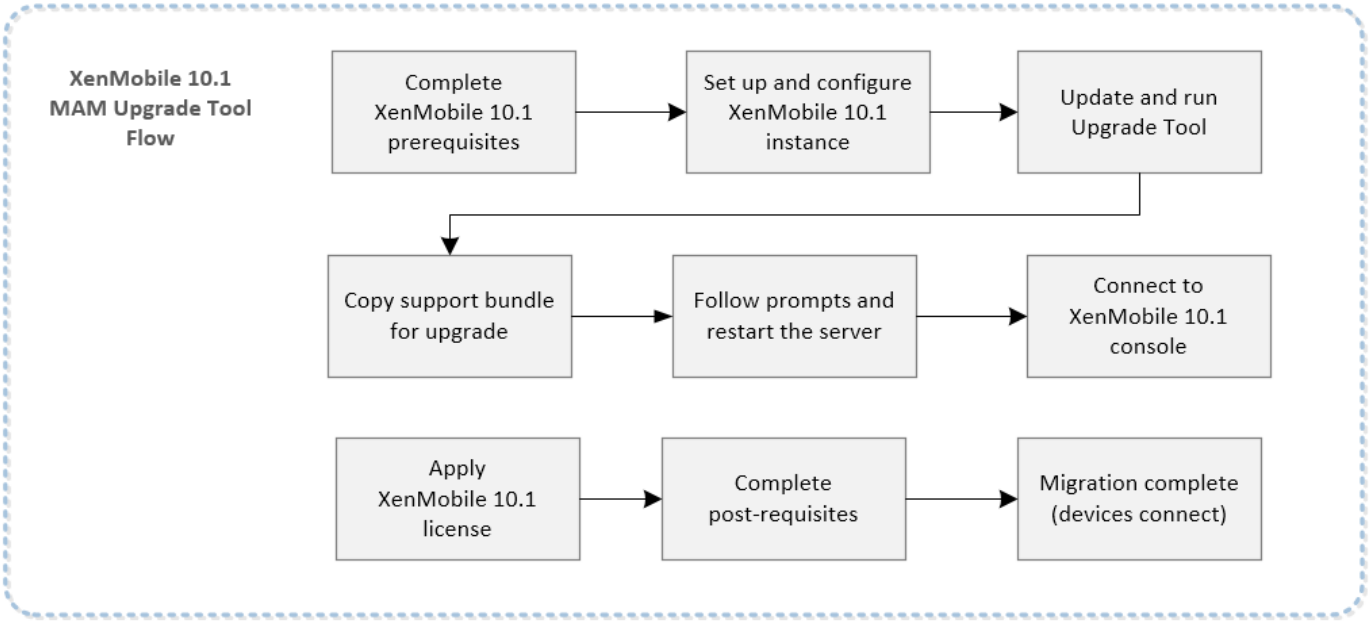
4. 从用户设备中手动卸载 Worx Home 9.x。

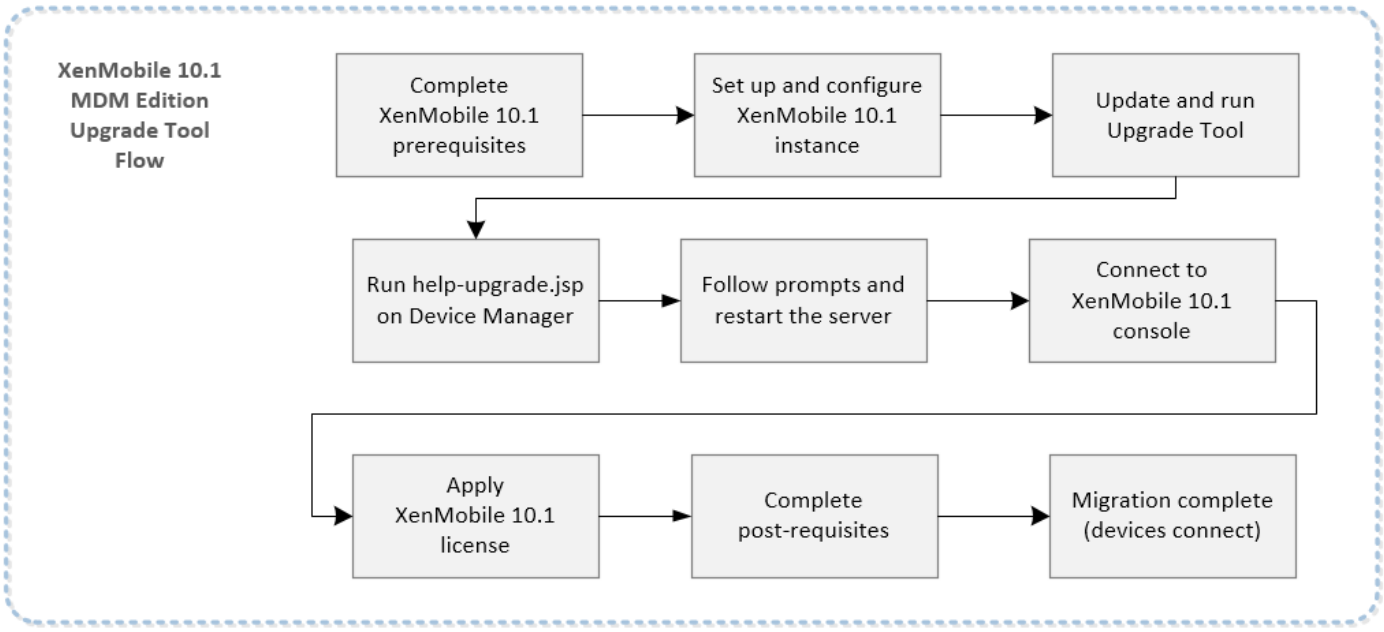
5. 指示用户转至 Windows Phone 上的下载中心以安装 Worx Home 10.2（您已从 Device Manager 中部署该版本）。

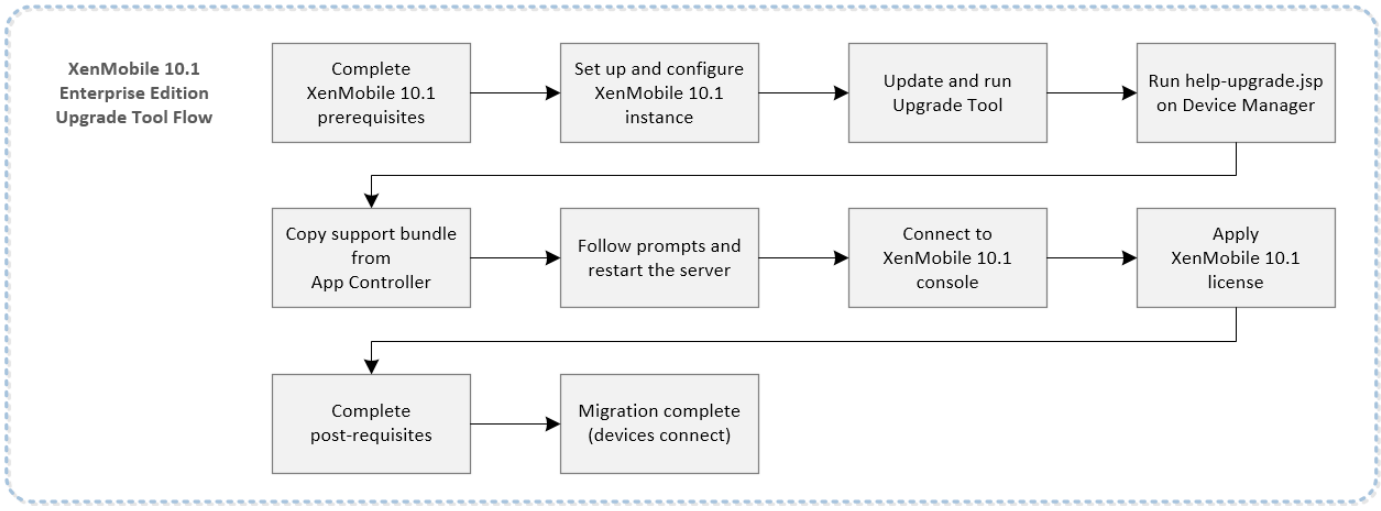
6. 在将设备连接到升级后的 XenMobile 服务器之前，请先升级到 XenMobile 10.1，然后立即升级到 XenMobile 10.3。

7. 更改 NetScaler 以便设备能够重新连接，如升级工具后续条件中所述。

下图说明了从 XenMobile 9.0 升级到 XenMobile 10.1 需要执行的基本步骤。







开始迁移到 XenMobile 10.1 之前，请参阅必备条件和 XenMobile 10.1 的已知问题和已修复的问题，以及此处列出的升级工具的已修复的问题和已知问题。

本版本的升级工具中的已修复问题

> **注意**
>
> 有关早期版本的升级工具中的已修复问题的列表，请下载此 PDF。

从 XenMobile 9 升级到 XenMobile 10.1 并更新到 XenMobile 10.3 后，Web 剪辑策略未部署到已在 XenMobile 9 中注册的

Windows 10 设备。 Web 剪辑策略会部署到新近在 XenMobile 10.3 中注册的 Windows 10 设备。 [#610101]

从 XenMobile 9 升级到 XenMobile 10.1 后，大批量 VPP 许可不起作用。 [#610418]

如果订阅信息包括大写的域名，则不迁移用户订阅。 [#620542]

如果通过 Worx App SDK 准备的应用程序包含非标准 URL（例如将 URL 中的应用商店 ID 格式化为 id*app-ID*?mt=8），则不迁移该应用程序。 [#625920]

本版本的升级工具中的已知问题

> **Important**
>
> 请注意此 XenMobile 10.1 已知问题，因为您的 XenMobile 9.0 主机名可能包含大写字母。 在这种情况下，升级到 XenMobile 10.1 之后，设备将无法访问 WorxStore。
>
> - 如果配置 XenMobile 服务器时主机名中包含大写字母，例如 ABC.Xms.com，设备注册后，WorxStore 不会在设备上打开。 [#545527]

数据和策略问题

- 升级后，syslog 服务器配置数据未迁移到 XenMobile 服务器。 [#558539]
- 如果 XenMobile 9.0 中最高或最低操作系统版本设备设置设为 10 或更高版本，并且适用于排除的设备的 MDX 和企业应用程序，则升级后，规则不会正确迁移。 应显示的应用程序不显示，不应显示的应用程序反而显示。 [#603412]
- 当用户按照支持命名 SQL 实例一文中建议的步骤从基于命名 SQL 实例的 XenMobile 9 部署中进行升级以解决 FQDN 问题时，支持包将成功上载，但出现数据库连接错误。 因此，用户无法完成升级。 [#605775]
- 部分限制策略配置在 10.1 中已弃用。 因此，从 XenMobile 9 升级到 XenMobile 10.1 并更新到 XenMobile 10.3 后，XenMobile 无法将整个限制策略成功部署到 Windows 10 手机。 但是，如果在 XenMobile 10.3 中查看并保存策略设置，策略会成功部署。 [#608541]
- 在 XenMobile 9.0 中，如果您在 LDAP 连接参数中定义了**用户组织单位** (OU)，则升级到 XenMobile 10 后，完整的根上下文将不附加到用户组织单位。 例如，OU=MDMUsers, OU=SALES 应为 OU=MDMUsers, OU=SALES, DC=citrite, DC=com。 因此，您需要在 XenMobile 10 中手动更新。 [#635981]

Google Play 应用程序

- 如果包括适用于 Android 设备的 Google Play 应用程序及默认图标，迁移后，默认图标不显示在 XenMobile 控制台中。 您必须编辑并保存应用程序或单击检查更新才能显示此图像。 [#557996]

SQL Server

- 升级工具不支持 XenMobile 9.0 SQL Server 数据库的命名实例。 此工具提供端口号，但不提供实例名称。 如果工具尝试连接到非预期实例而非默认实例，升级将失败并出现 java.sql.SQLException 错误。 要修复这些问题，请参阅支持命名 SQL 实例。 [#575679]
- 如果使用 PostgreSQL 数据库，MAM 设备在升级后将无法重新注册。 要解决此问题，请从 XenMobile 中删除设备条目，并将注册通知发送给用户。 [#632831]
- 如果您的 Device Manager 9.0 服务器设置为使用本地 PostgreSQL，并且您使用 localhost 作为数据库服务器的参考，升级将失败。 要解决此问题，请在 Device Manager 9.0 服务器上编辑 ew-config.properties，并将所有 localhost 参考替换为

Device Manager 数据库服务器的 IP 地址，然后继续完成升级必备条件。 [#635023]

RBAC

升级后 RBAC 设置出现问题：

- 如果您配置了 RBAC 角色并将访问权限限制为 LDAP 和 Active Directory 或任何子项，升级后，以管理员身份登录 XenMobile 控制台时，不会选中相同的设置。
- 如果配置了超级管理员角色，默认情况下会选中所有权限。 升级后，只会选中三个权限 - RBAC、注册和版本管理。
- 如果创建了自定义超级管理员角色，默认情况下应选中所有支持权限。 升级后，不会选中任何支持权限设置。 [#569350，#569395，#569423]

Windows CE

- XenMobile 10.1 不支持 Windows CE 设备。

Worx Home 和 WorxStore

- 将 XenMobile 10.1 更新到 XenMobile 10.3 后，当用户在 iOS 和 Android 设备上打开 Worx Home 时，WorxStore 显示空白。 解决方法为，重新启动 NetScaler 或清除 NetScaler 缓存。 [#609706]
- 从 XenMobile 9 升级到 XenMobile 10.1 之前，如果 WorxStore 具有自定义名称，则进行注册以及访问 Worx Home 和 Worx Store 时会出现问题。 解决方法为，在升级前将应用商店更改为默认设置（**应用商店**）。 [#619458]
  有关必备解决方法的详细信息，请参阅必备条件。
- 在从 XenMobile 9.0 升级到 XenMobile 10.1，并将 LDAP 选项**用户搜索依据**设置为 **sAMAccountName**，然后升级到 XenMobile 10.3.x 后，使用仅 MAM 设备的用户将无法在 Worx Home 中执行身份验证。 [#628233]

Android for Work

- 升级后，通过 SAML 身份验证登录 Android for Work 将失败，因为 SAML 证书的扩展名为 .pem，而 XenMobile 服务器不导入使用该扩展名的证书。 [#631795]

  要解决此问题，请确保 XenMobile 具有正确的 SAML 证书，如下所示：

  1. 从 XenMobile 9 App Controller 中导出带私钥的 SAML 证书 (AppController.example.com)。 该证书为 PEM 格式，扩展名为 .pem。

  2. 使用 openssl 命令基于该 PEM 文件生成一个 PFX 文件：

  ```
  openssl pkcs12 -export -out certificate.pfx  -in certificate.pem
  ```

  3. 将 PFX 文件导入到 XenMobile 10.3 中作为 SAML 密钥库。

  4. 从 XenMobile 10.3 中导出不带私钥的 SAML 证书，然后将其上载到 Android for Work 域。

升级工具执行的操作

XenMobile 10.1 升级工具将配置和用户数据从 XenMobile 9.0 服务器迁移到 XenMobile 10.1 的新实例（具有相同的完全限定域名 (FQDN)）。

- 无论使用何种 XenMobile 版本，都可以升级对生产配置数据的试用，以在不影响生产环境的情况下将 XenMobile 9.0 与 XenMobile 10.1 进行比较。

- 可以执行全面的生产升级，以将所有数据从 XenMobile 9.0 移动到 XenMobile 10.1。 但是，无法从试用移动到生产升级。相反，必须重新开始执行生产升级。

有关 XenMobile 10.1 部署的体系结构图，请参阅体系结构概述。

在工具中选择 **Test Drive**（试用）时，仅将配置数据迁移到 XenMobile 10.1，不迁移任何设备（如果是 XenMobile Enterprise Edition 部署）或用户数据。

在工具中选择 **Upgrade**（升级）时，将迁移所有配置、设备和用户数据。 升级后登录到 XenMobile 10.1 控制台时，您会看到从 XenMobile 9.0 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被*复制*（而非移动）到 XenMobile 10.1。 XenMobile 9.0 中的所有数据保持不变，直至将 XenMobile 10.1 服务器移动到生产环境中。 当用户连接到生产环境中的 XenMobile 10.1 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。

Citrix 建议您先升级试用，以大体了解进程的工作原理以及执行全面生产升级后应显示的内容。 试用后，可以对隔离环境执行全面的生产升级以进一步进行测试。 验证升级后，可以再次对您的生产环境执行生产升级。

生产升级成功后，要将 XenMobile 10.1 移动到实时生产中，必须执行以下操作：

1. 如果 NetScaler 为负载平衡的 XenMobile Device Manager 服务器，则需要：

- 创建一项新 XenMobile 10.1 负载平衡服务。
- 将 XenMobile 9.0 服务切换到 XenMobile 10.1 服务。

2. 对于独立部署，请更新 DNS 条目，以将 XenMobile 9.0 FQDN 映射到新的 XenMobile 10.1 服务器 IP。 不需要对群集环境执行此步骤。

有关详细信息，请参阅升级工具后续条件。

使用升级工具时，**不**会将以下信息迁移到 XenMobile 10.1：

- 许可信息。
- 报告数据。
- 服务器组策略以及关联的部署（在 XenMobile 10.1 中不受支持）。
- 托管服务提供程序 (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 10.1 支持一个品牌设计策略；必须在 XenMobile 9.0 中保留一个品牌设计策略，才能成功迁移到 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 10.1 中的控制台访问限制是可在命令行界面中配置的防火墙设置。
- 系统日志服务器配置。
- 在 XenMobile 9.0 上配置的表单填充连接器（在 XenMobile 10.1 中不受支持）。

还请注意 XenMobile 10.1 中的以下变更：

- XenMobile 10.1 不支持分配给本地组的 Active Directory 用户。
- 本地组层次结构已展开。

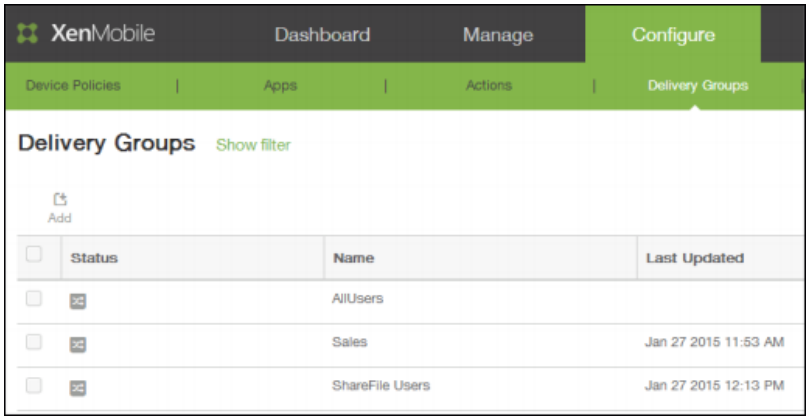
规划升级

> **Important**
>
> 对于每个阶段，请按照启用和运行升级工具和必备条件中的步骤进行操作。升级过程较为复杂；请务必在开始前完成必备条件。例如，如果输入错误的证书密码，升级将失败。如果失败，必须在命令行控制台配置新的 XenMobile 10.1 实例并重新启动升级工具。

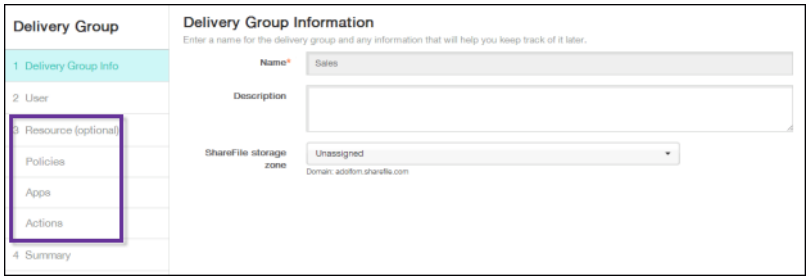
Citrix 建议您分以下阶段进行升级。

1. 在过渡环境中试用。
   1. 设置一个全新的包含 NetScaler Gateway 和 NetScaler 负载平衡虚拟服务器的 NetScaler 10.5 ，最好使用 XenMobile 10 实用程序进行设置。
   2. 恰当地更改防火墙和 DNS。
2. 在过渡环境中执行生产升级。
   1. 按照后续条件步骤调整现有 NetScaler 配置。
   2. 恰当地更改防火墙和 DNS。
3. 在生产环境中执行生产升级并使其生效。
   1. 规划迁移运行过程中停机。
   2. 按照后续条件步骤调整现有 NetScaler 配置。
   3. 恰当地更改防火墙和 DNS。

请注意，升级之后，Device Manager 中的部署软件包现在在 XenMobile 10.1 中称为交付组，如下图所示。有关详细信息，请参阅管理交付组。



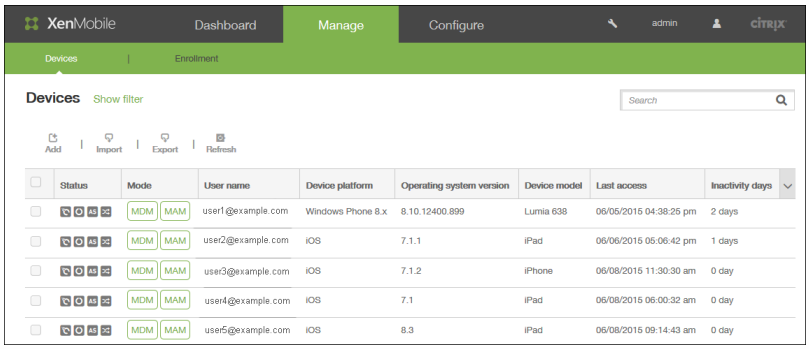
在交付组中，可以查看需要资源的用户组所需的策略、操作和应用程序。



生产升级到 XenMobile 10.1 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 10.1 服务器。但是，系统可能会要求用户重新进行身份验证，才能重新连接设备。

如果要立即将设备连接到 XenMobile 10.1，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

Aug 04, 2016

需要满足以下必备条件才能运行 XenMobile 升级工具。要查看已知问题，请参阅关于升级工具。

> ## Important
>
> 请注意此 XenMobile 10.1 已知问题，因为您的 XenMobile 9.0 主机名可能包含大写字母。在此情况下，升级到 XenMobile 10.1 之后，设备无法访问 Worx Store。
>
> - 如果配置 XenMobile 服务器时主机名中含有大写字母，如 ABC.Xms.com，设备注册后，Worx Store 不会在设备上打开。[#545527]

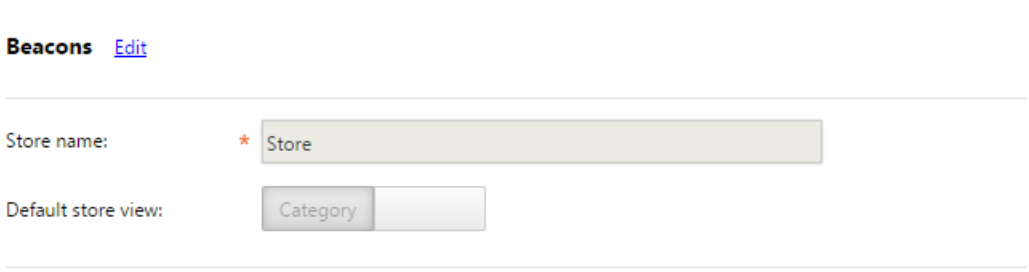
App Controller 修补程序

从 Citrix.com.cn 的“下载”页面下载 XenMobile 9.0 App Controller 的最新修补程序文件。在 App Controller 管理控制台中，转至**设置** > **版本管理**。单击**更新**，然后选择要下载的修补程序文件。单击**上载**，然后重新启动 App Controller。

应用商店名称

> ## 注意
>
> 将 XenMobile 9 升级到 XenMobile 10.1 之前，必须将自定义应用商店名称更改回其默认值，以便注册的 Windows 设备在升级后能够继续运行。 有关详细信息，请参阅 http://support.citrix.com/article/CTX214553。

在 MAM 或 Enterprise 模式下升级时，如果更改了 App Controller 上的应用商店的默认名称（**应用商店**），则在为升级生成支持包之前，请将该名称还原为默认设置（**应用商店**）。



Citrix 许可证服务器

请务必安装 Citrix 许可证服务器 11.12.1（在 Citrix Licensing 页面中提供）并使用最新的 XenMobile V6 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。 此步骤对强制用户重新注册其设备十分重要。

NetScaler 10.5 和 XenMobile 10.1

Citrix 建议您将 Netscaler 10.5 与 XenMobile 10.1 结合使用。 升级到 NetScaler 10.5 之前，请务必保存一份 Netscaler 配置

(ns.conf)。 Netscaler 10.5 发行版中包括一个易于使用的快速部署实用程序，用于引导您完成集成 NetScaler 10.5 和 XenMobile 10 的步骤。 有关详细信息，请参阅 FAQ: XenMobile 10 and NetScaler 10.5 Integration（常见问题解答：XenMobile 10 和 NetScaler 10.5 集成）。

LDAP 服务器

确保新 XenMobile 10.1 服务器连接到一个或多个 LDAP 服务器。 升级后，重新启动该服务器时，必须与 LDAP 服务器建立一个活动路由。

打开防火墙端口

为新 XenMobile 10.1 服务器 IP 打开与为 XenMobile 9.0 IP 服务器打开的端口类似的防火墙端口。

数据库迁移

下表列出了可能的数据库迁移选项。 有关系统要求，请参阅 XenMobile 10.1 数据库要求。

从 XenMobile 9.0		迁移至 XenMobile 10.1
Enterprise Edition		
App Controller	**MDM**	
本地 PostgreSQL	本地 PostgreSQL	本地 PostgreSQL
本地 PostgreSQL	MS SQL	MS SQL
本地 PostgreSQL	Remote PostgreSQL	Remote PostgreSQL
App Edition		
本地 PostgreSQL		本地 PostgreSQL
本地 PostgreSQL		Remote PostgreSQL
本地 PostgreSQL		MS SQL
MDM 版本		
本地 PostgreSQL		本地 PostgreSQL

MS SQL	MS SQL
Remote PostgreSQL	Remote PostgreSQL

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 并找到以下行："host all all 127.0.0.1/32 md5"
将此行替换为 "host all all 0.0.0.0/32 md5"

2. 保存该文件。

3. 停止并启动服务

4. 找到并打开 postgresql.conf 文件，然后将此行从：
"#listen_addresses = 'localhost'" to "listen_addresses = '*'"

> **注意**
>
> 通过仅允许 XenMobile 9.0 和 XenMobile 10.1 服务器 IP 地址访问 PostgreSQL 数据库 (listen_addresses = '10.x.x.1,10.x.x.2') 可对此进行限制。

5. 停止并启动 PostgreSQL 服务以使更改生效。

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 10.1 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查看 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 10.1 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 10.1 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 10.1 控制台。

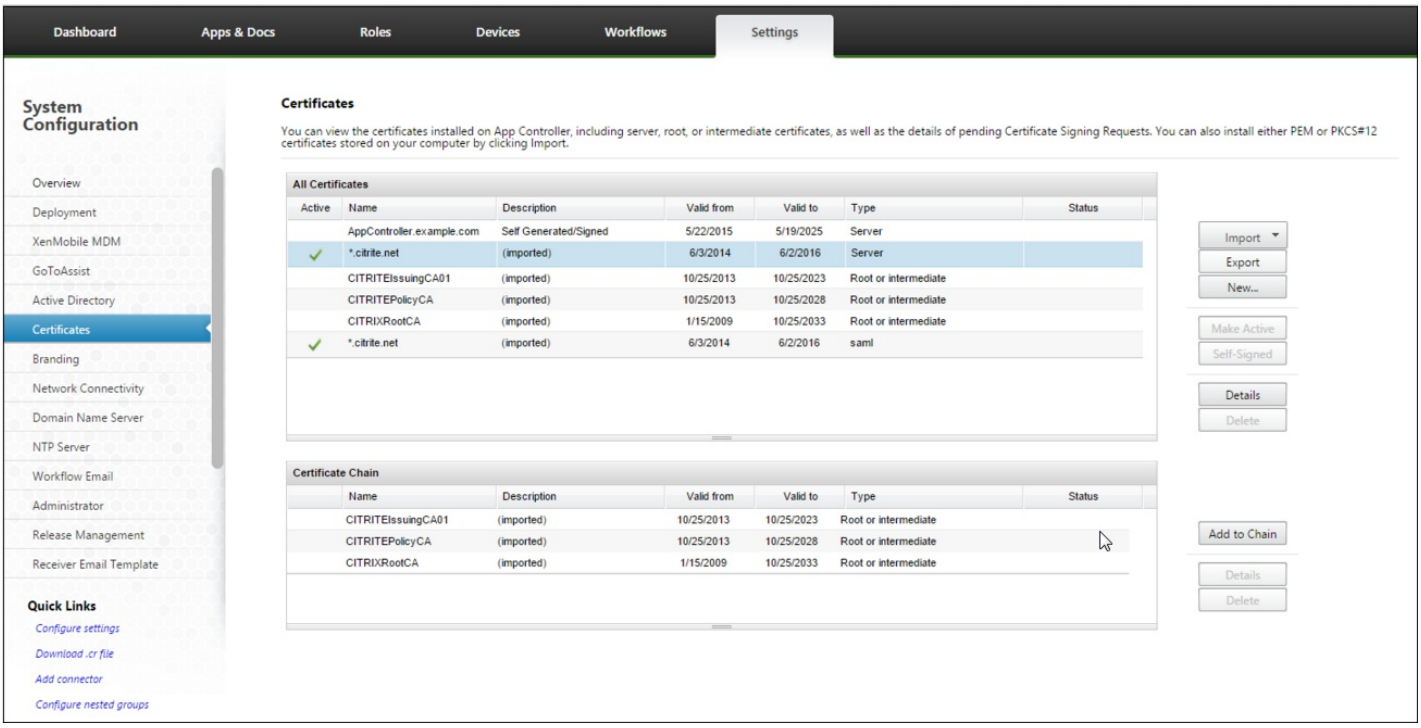
带有特殊字符的部署软件包名称

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 10.1 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 10.1 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。

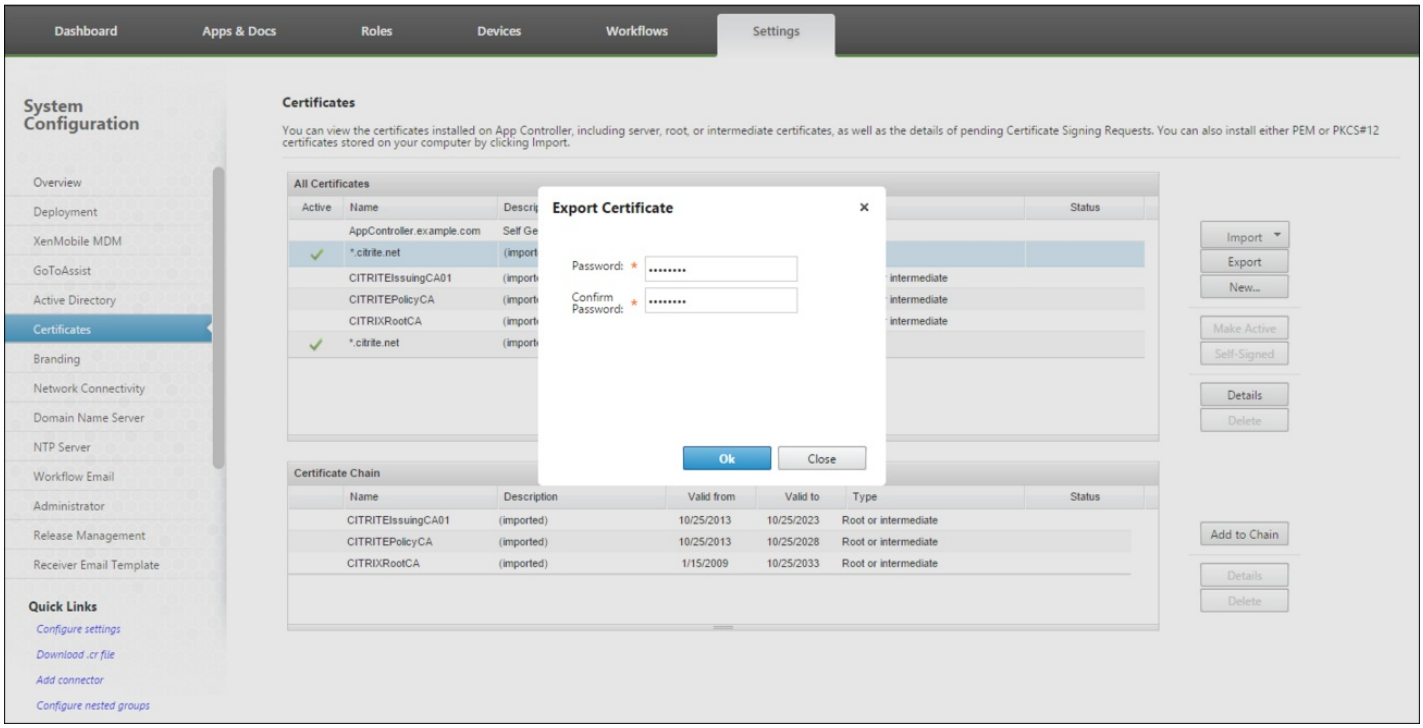
导出 XenMobile 9.0 服务器证书

如果要升级 Xenmobile 9.0 Enterprise Edition 部署，需要导出 App Controller 服务器证书并将其导入到 NetScaler Gateway 中。登录 XenMobile 9.0 App Controller 并单击 **Certificates**（证书）。请按照以下步骤进行操作以导出服务器证书：

1. 在证书列表中，单击要导出的服务器证书，然后单击 **Export**（导出）。



2. 在**导出证书**对话框的两个字段中键入证书密码，然后单击**确定**。



将服务器证书导出到 NetScaler Gateway 设备中。

用于上载加密支持包的服务器

您可以使用文件传输协议 (FTP) 或安全复制协议 (SCP) 通过命令行接口上载加密支持包的服务器。

了解已知问题并满足所有必备条件后，开始进行升级。

启用和运行 XenMobile 10.1 升级工具

Oct 13, 2016

下面是将 XenMobile Enterprise Edition 和 MAM 部署从 XenMobile 9.0 升级到 XenMobile 10.1 应执行的基本步骤：

1. 使用命令行控制台配置 XenMobile 10.1 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. 在浏览器中启动升级工具。
4. 运行 help-upgrade.jsp。 仅限 XenMobile Enterprise Edition。
5. 更新 App Controller。
6. 创建支持包。
7. 输入 XenMobile 9.0 文件的位置对应的 URL。 仅限 XenMobile Enterprise Edition。
8. 将支持包上载到升级工具中。
9. 更新数据库配置。
10. 开始升级。 **注意**：如果更新升级工具，应在启动升级前清除浏览器缓存。
11. 重新启动 XenMobile 10.1 服务器。
12. 登录到 XenMobile 10.1 控制台。
13. 应用 XenMobile 10.1 许可证以允许用户进行连接。
14. 对于 XenMobile Enterprise Edition 生产升级，如果您使用的是负载平衡的 NetScaler，请删除 XenMobile 9.0 服务器 IP 地址，并添加 XenMobile 10.1 服务器 IP 地址。
15. 对于生产升级，需要为 XenMobile 更改外部 DNS，以指向新的 XenMobile 10.1 服务器。

安装 XenMobile 10.1 的实例并启用升级工具

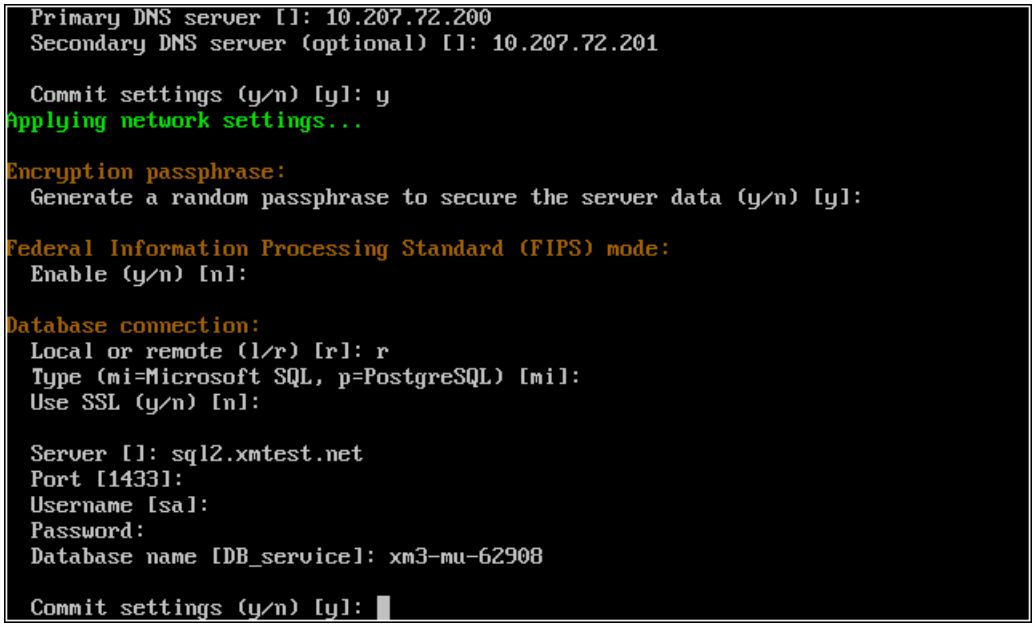
首次安装 XenMobile 10.1 时，请通过命令行界面 (CLI) 启用升级工具，如下图所示。

> **Important**
>
> 如果要生成系统快照，请在 XenMobile 10.1 初始配置之后、访问升级工具*之前*进行。

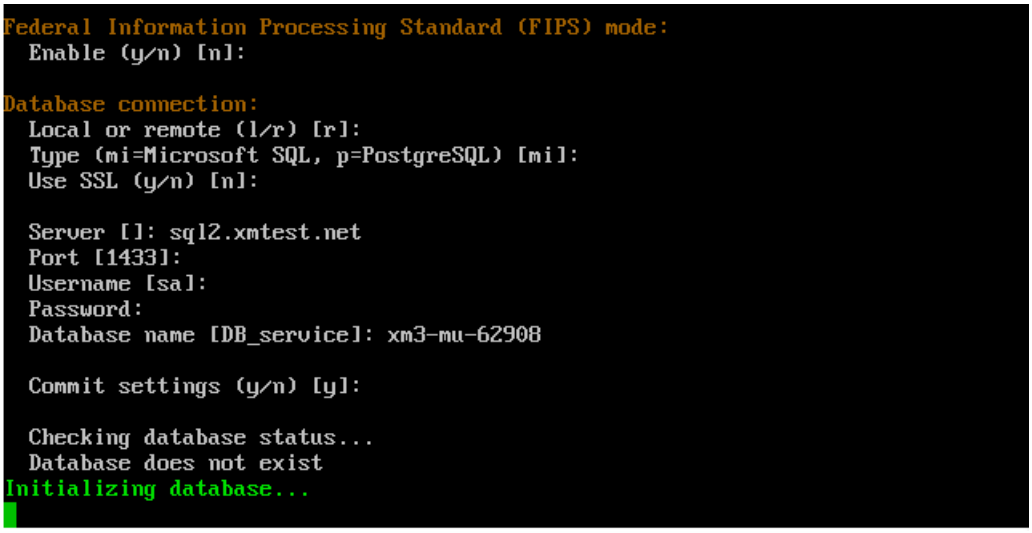
1. 在 CLI 中，键入您的管理员用户名和密码，然后输入网络设置。

2. 键入 **y** 提交设置。

3. 选择生成随机密码，以及启用 FIPS（可选）。输入数据库连接信息。



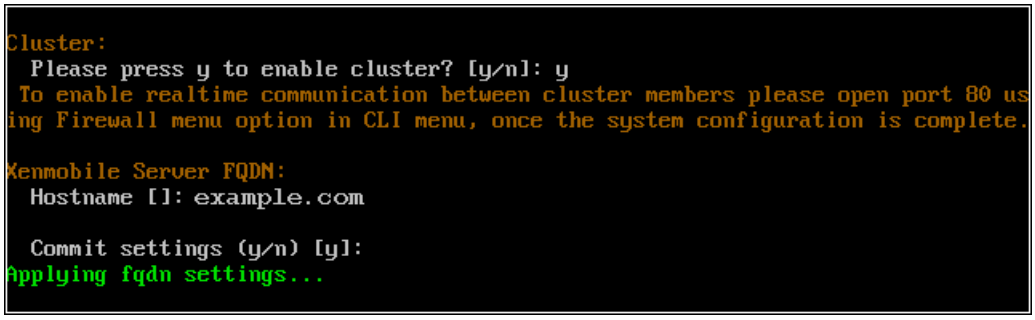
4. 键入 **y** 提交设置。XenMobile 初始化数据库。



5. 选择是否启用群集服务器。键入 XenMobile 的完全限定域名 (FQDN)。请注意以下问题：

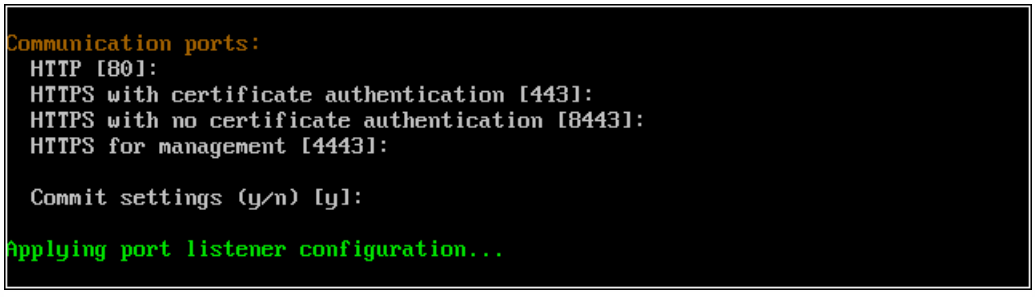
- 对于 XenMobile Enterprise Edition 部署，FQDN 与 XenMobile 9.0 MDM FQDN 相同。
- 对于 MAM 部署，FQDN 与 XenMobile 9.0 App Controller FQDN 相同。
- 对于 MDM 部署，FQDN 与 XenMobile 9.0 Device Manager FQDN 相同。

> **Important**
>
> 用于 9.0 环境和 10.1 环境的 FQDN 必须匹配。



6. 键入 **y** 提交设置。

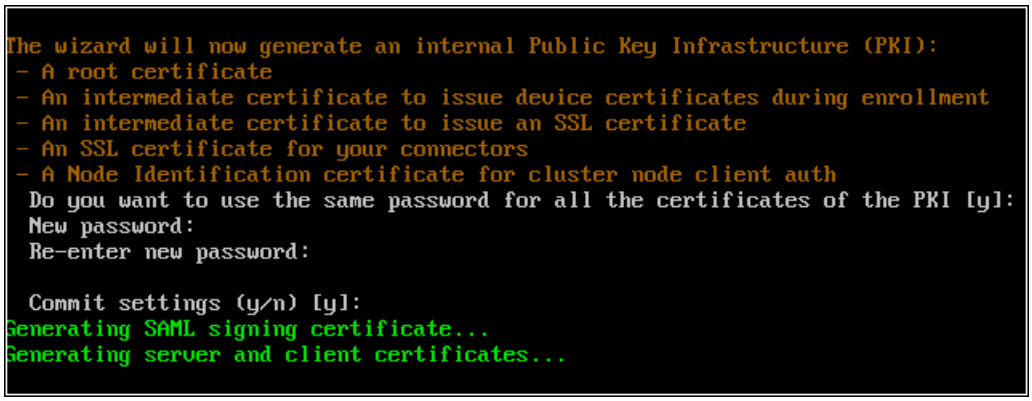
7. 设置通信端口。



设置端口后，会出现 Device Manager 实例名称提示：如果您将从上一个版本升级，此名称必须匹配上一个配置名称。请注意，默认安装使用名称 *zdm*。如果更改默认名称，必须输入更改后的名称。

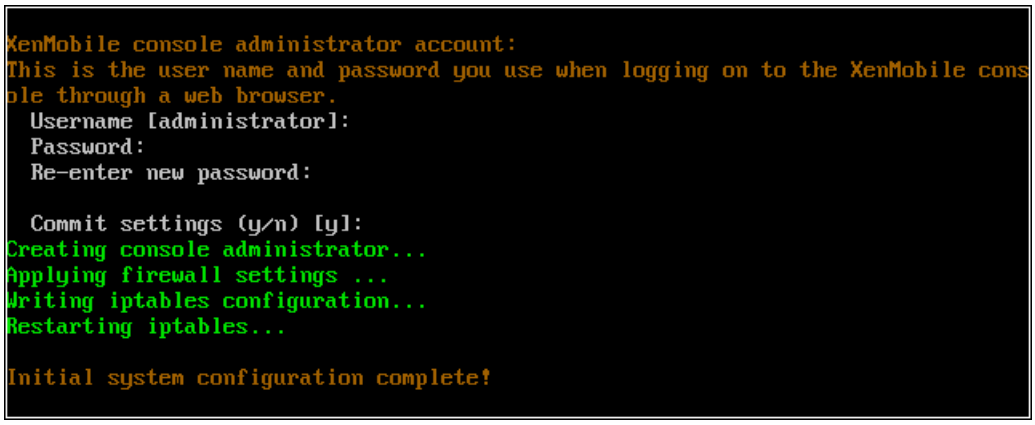
8. 键入 **y** 提交设置。

9. 键入要对证书使用的密码，然后选择是否对所有证书使用相同的密码。



10. 键入 **y** 提交设置。

11. 键入 XenMobile 控制台管理员的用户名和密码。



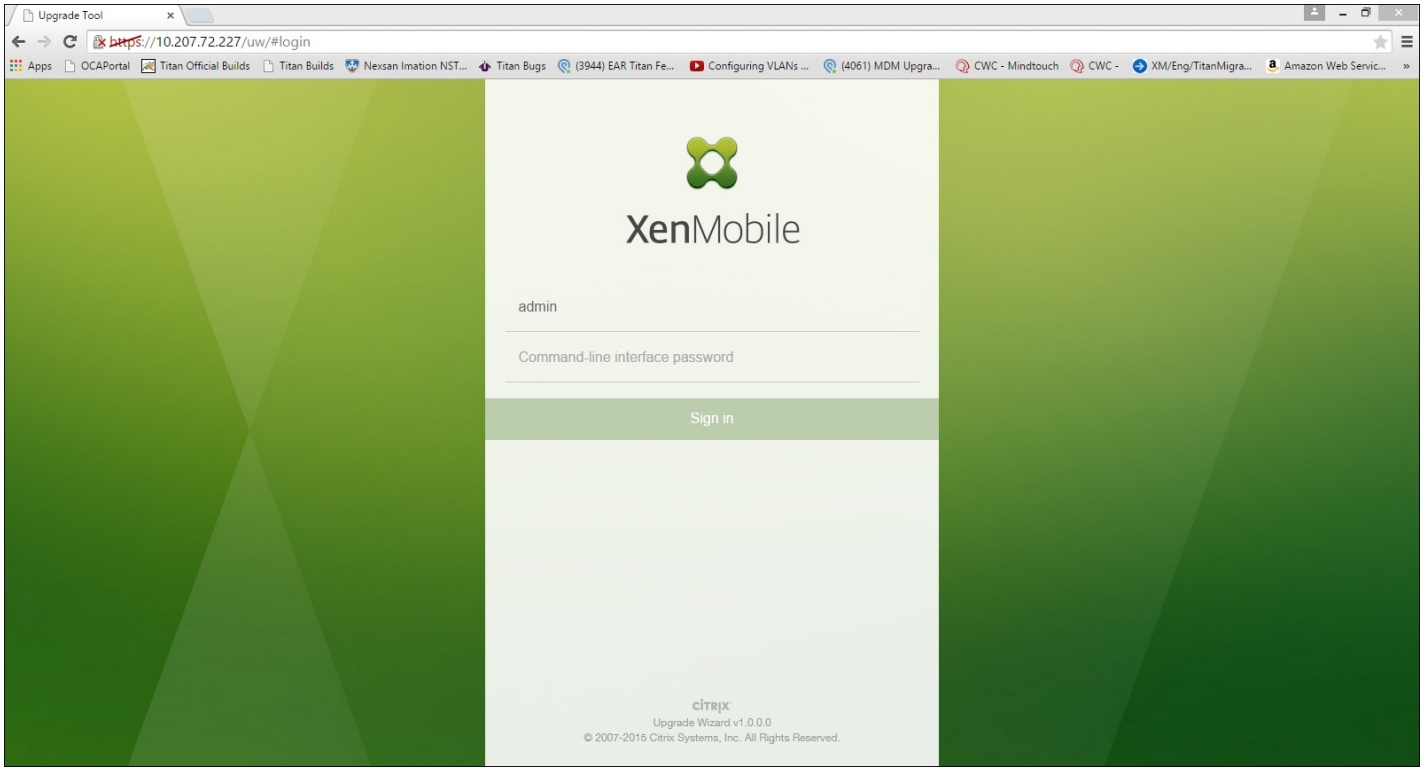
12. 键入 **y** 提交设置。

13. 键入 **y** 进行升级。**注意**：如果您不在此处选择 y，则必须在命令行控制台配置新的 XenMobile 10.1 实例并重新启动升级工具。

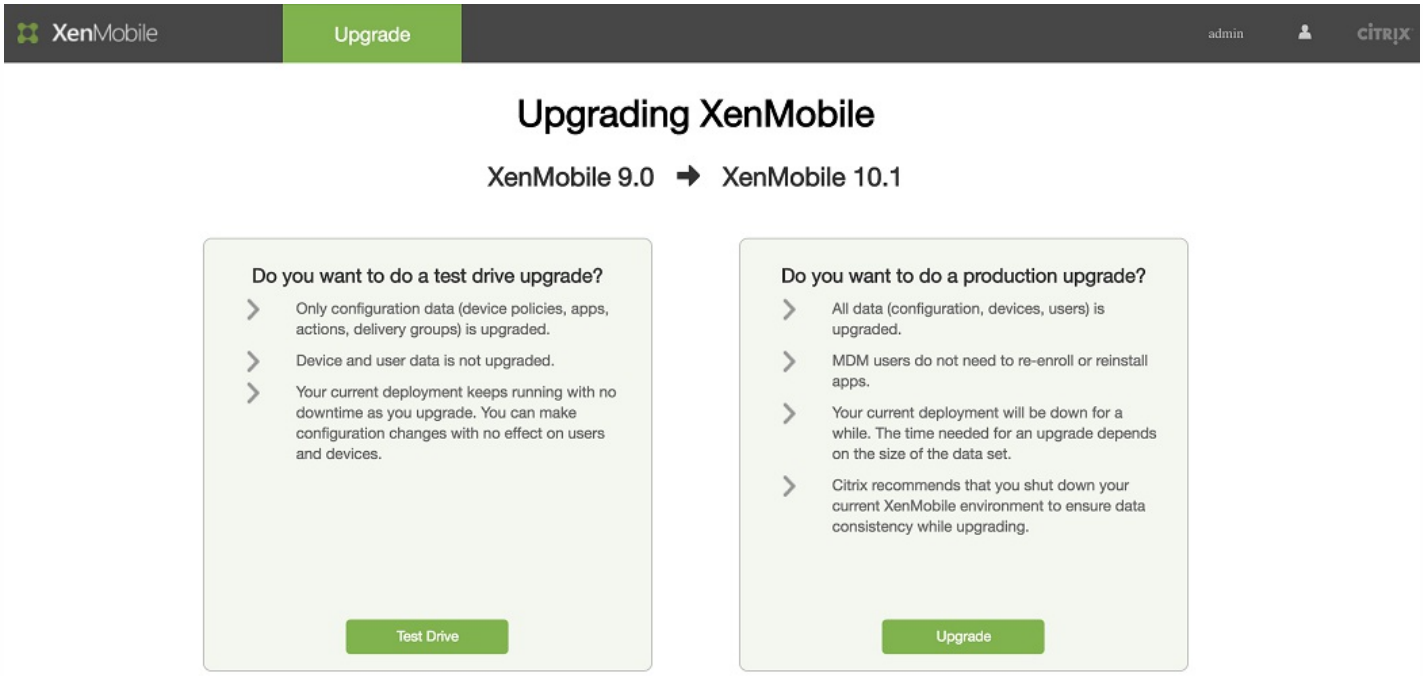
```
Upgrade:
  Upgrade from previous release (y/n) [n]: y

Stopping configuration app...                                    [ OK ]
Starting configuration app...
  this may take a few seconds........
  application started                                            [ OK ]
Stopping main app...                                             [ OK ]
Starting main app...
  not ready to start yet                                         [ OK ]

  To complete the upgrade process, from a web browser, go to the following
  location and log on with your command prompt credentials:
    https://198.51.100.1/uw/

Starting monitoring...                                           [ OK ]

enroll.example.com login:
```

XenMobile 10.1 启用一次性升级工具。

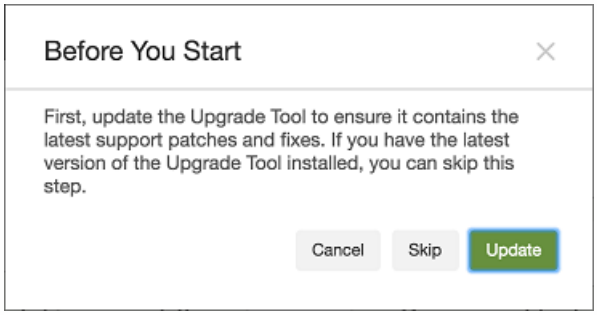
14. 在 Web 浏览器上通过 https:///uw/ 访问升级工具。

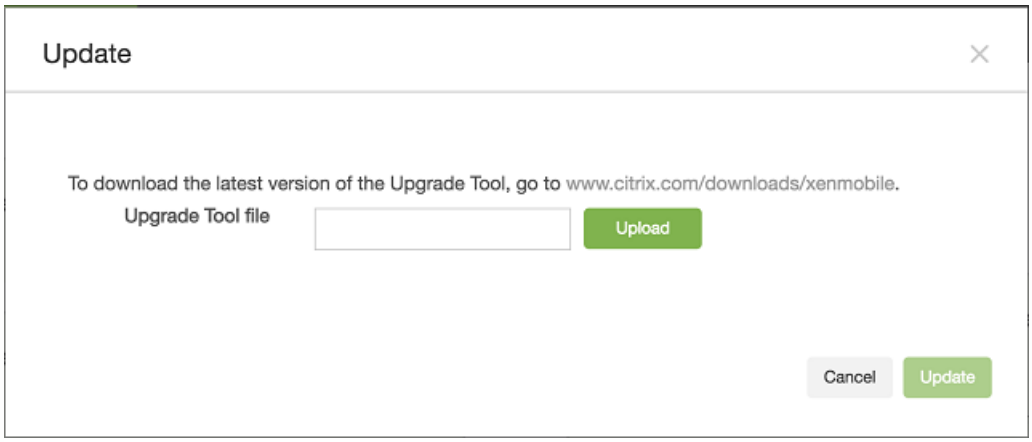


15. 现在可以在试用与生产升级之间进行选择。 这些说明适用于生产升级。 在 **Upgrading XenMobile**（升级 XenMobile）页面上，单击 **Upgrade**（升级）。



16. 在 **Before You Start**（准备工作）对话框中，单击 **Update**（更新），然后使用 **Update**（更新）对话框安装最新工具。





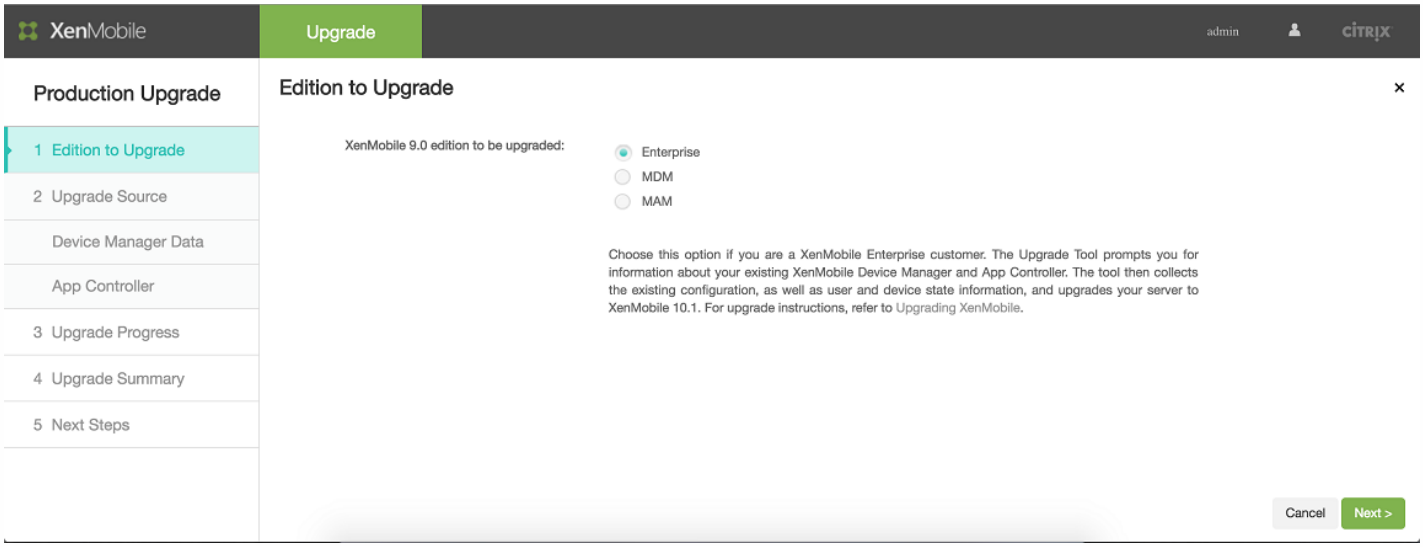
更新此工具后，此工具将重新启动您的系统。

17. 继续操作之前，清除浏览器缓存，重新输入 URL 以访问升级工具 (https:///uw/)。

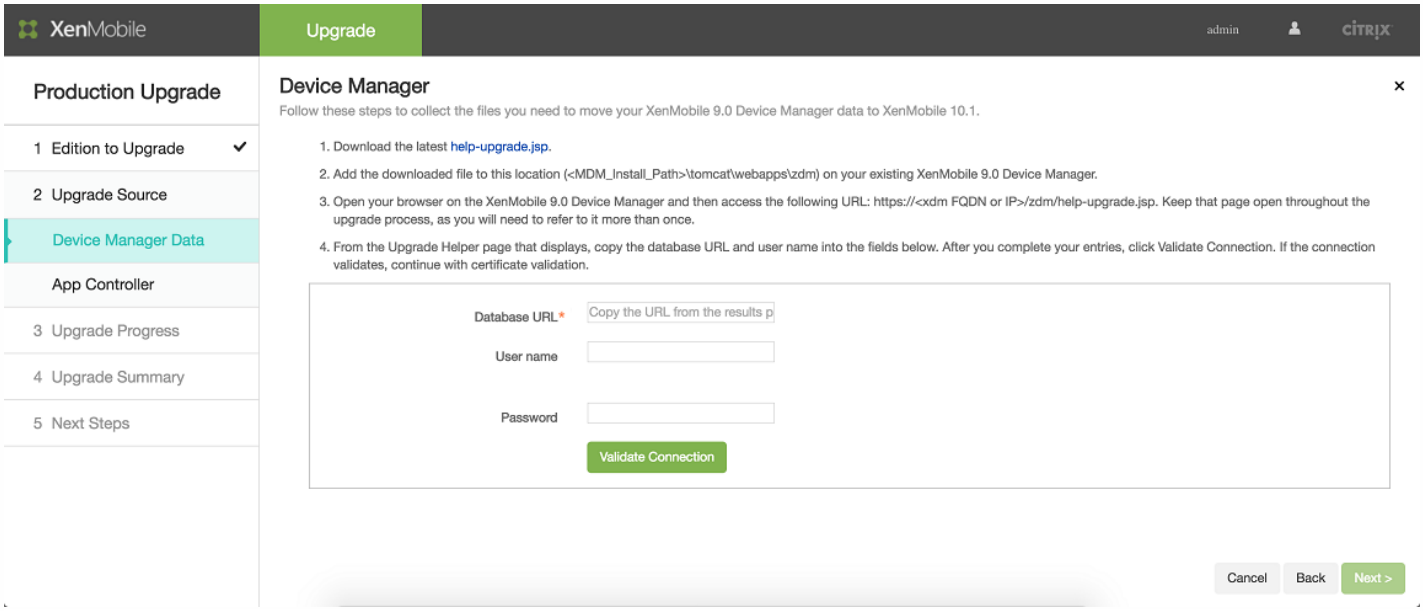
18. 在 **Upgrading XenMobile**（升级 XenMobile）页面上，单击 **Upgrade**（升级）。 在 **Before You Start**（准备工作）对话

框中，单击 **Skip**（跳过）。

19. 在 **Edition to Upgrade**（要升级的版本）页面中，选择您的版本。 在此示例中，所选版本为 **Enterprise**。



20. 单击 **Next**（下一步）。

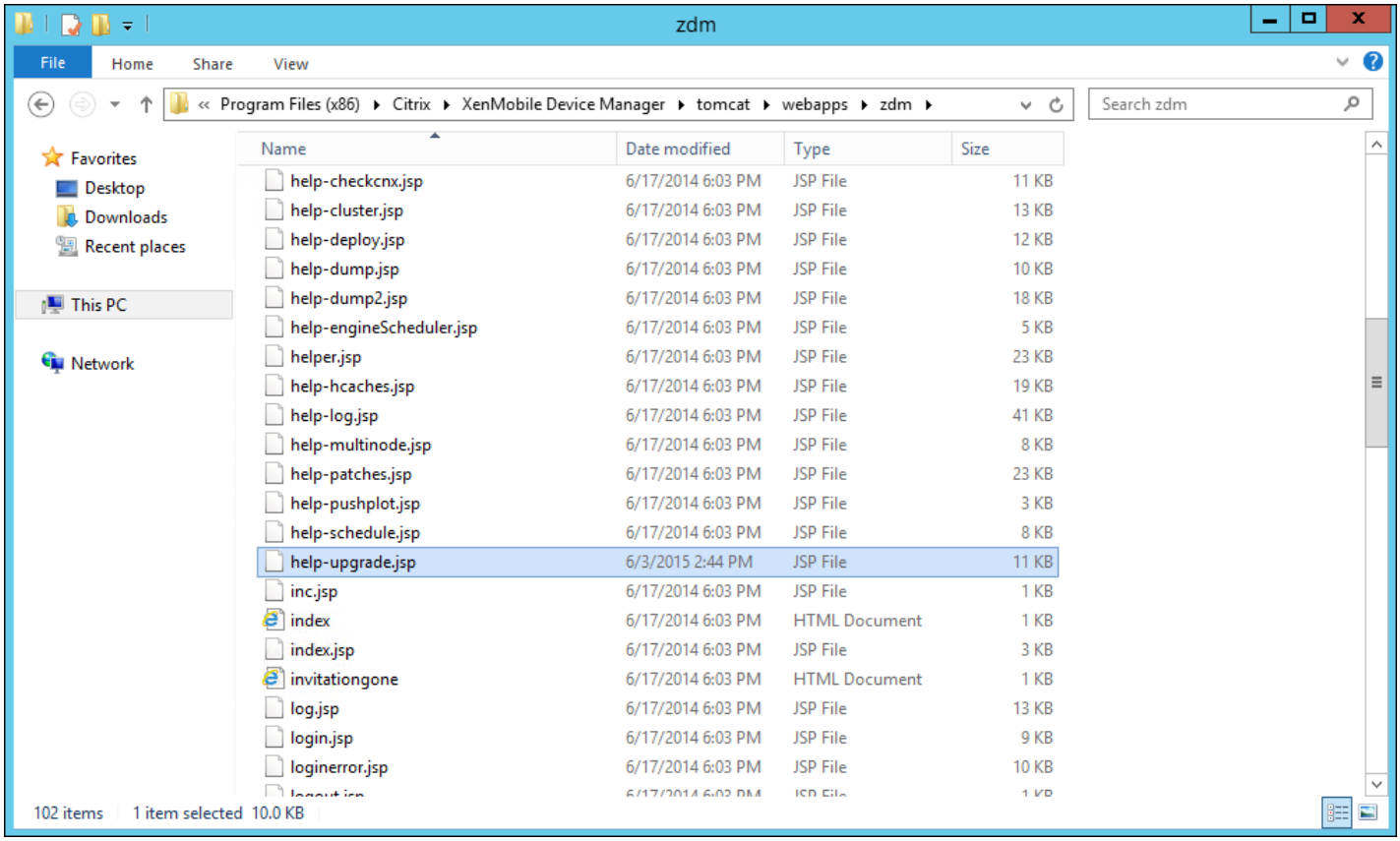


此时将显示用于 XenMobile Enterprise Edition 迁移的 **Device Manager** 页面。 此步骤不是执行 MAM 迁移必须执行的步骤。 如果要执行 MAM 迁移，将显示“Update App Controller”（更新 App Controller）页面；请跳至步骤 24 以更新 App Controller。

21. 请按照以下步骤进行操作，收集迁移现有 XenMobile 9.0 Device Manager 数据所需的文件。 您还将获得访问数据库 URL 的权限以及要复制到 **Device Manager** 页面的用户名。

a. 单击 **Device Manager** 页面的步骤 1 中的链接并保存下载的 help-upgrade.zip 文件。

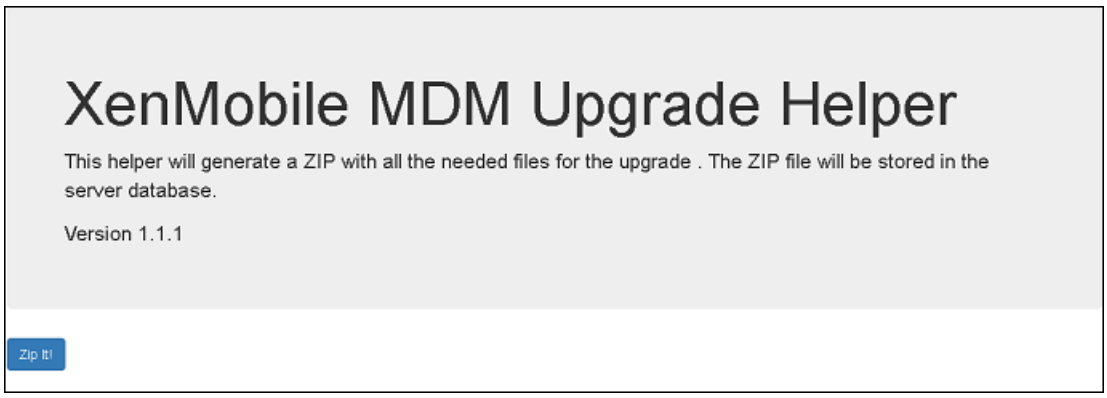
b. 将 help-upgrade.jsp 文件解压到现有 XenMobile 9.0 Device Manager 上的 \tomcat\webapps\zdm。



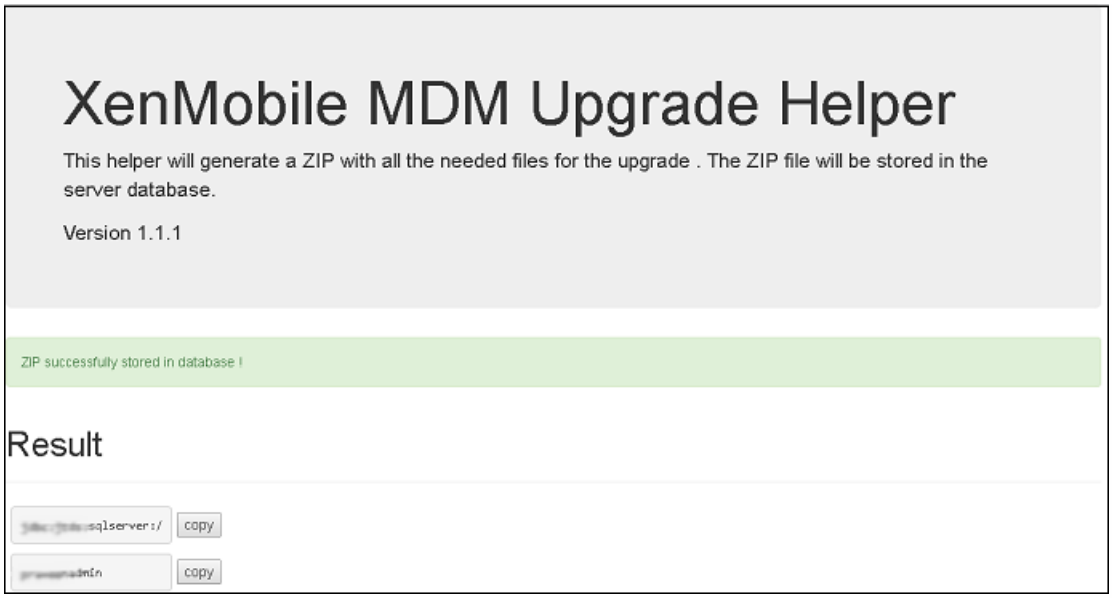
c. 在浏览器窗口中，登录到 XenMobile 9.0 服务器。

d. 在单独的浏览器选项卡中，输入以下 URL：https://localhost/zdm/help-upgrade.jsp。 此时将打开 **XenMobile MDM Upgrade Helper**（XenMobile MDM 升级帮助程序）页面，用于收集并打包 XenMobile 9.0 中升级到 XenMobile 10.1 所需的所有文件。 zip 文件随后将存储到服务器数据库中，将从该位置解压。 您可能需要登录 help-upgrade.jsp 页面。

e. 单击 **Zip it**（打包），然后按照屏幕上显示的步骤进行操作，收集升级所需的文件。



22. 在 **Result**（结果）下，复制 URL 并将其粘贴到升级工具的 **Device Manager** 页面的 **Database URL**（数据 URL）字段中。然后复制用户名并将其复制到 **Device Manager** 页面。



23. 在升级工具中：

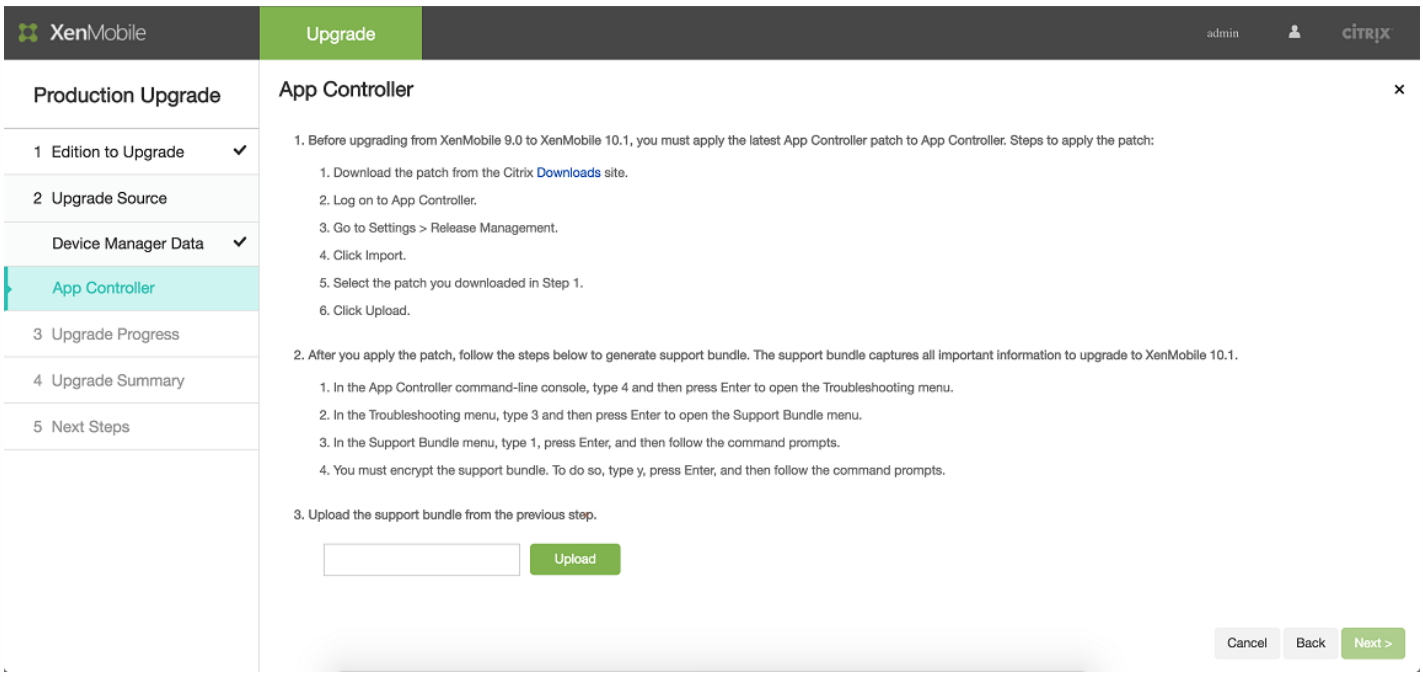
a. 输入密码，然后单击 **Validate Connection**（验证连接）。

b. 输入每个证书的密码，然后单击 **Validate Password**（验证密码）。

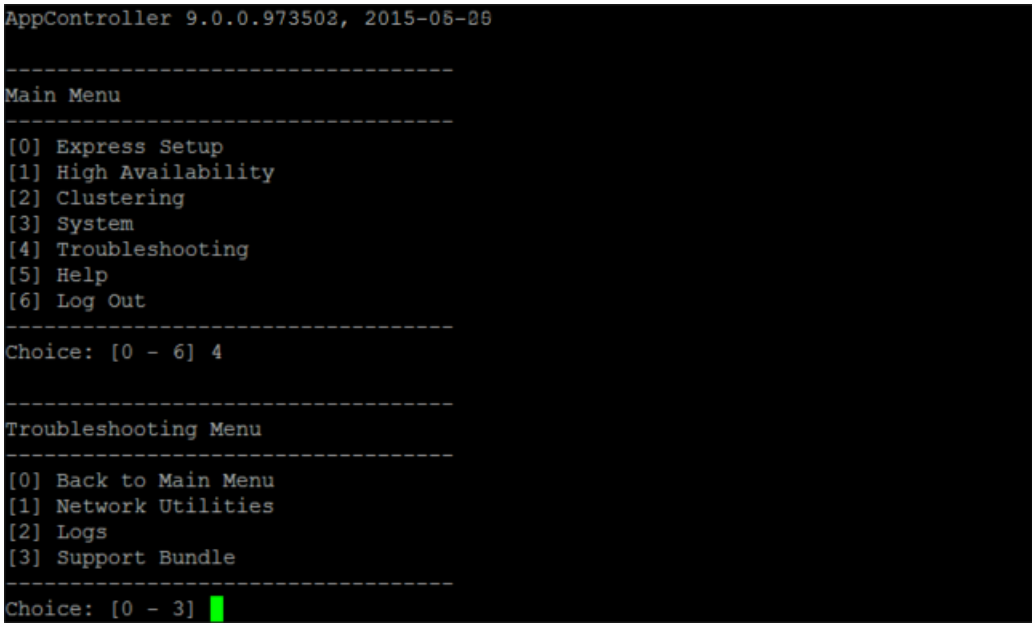
c. 单击 **Next**（下一步）。

24. 如果更改了 ew-config.properties 文件，请在 XenMobile 9 MDM 上重新启动 xdm 服务，然后访问 https://localhost/zdm/help-upgrade.jsp 以重新运行 zip。 这样会重新读取 ew-config.properties 文件，并将其保存至 XenMobile MDM 9 数据库以准备迁移。

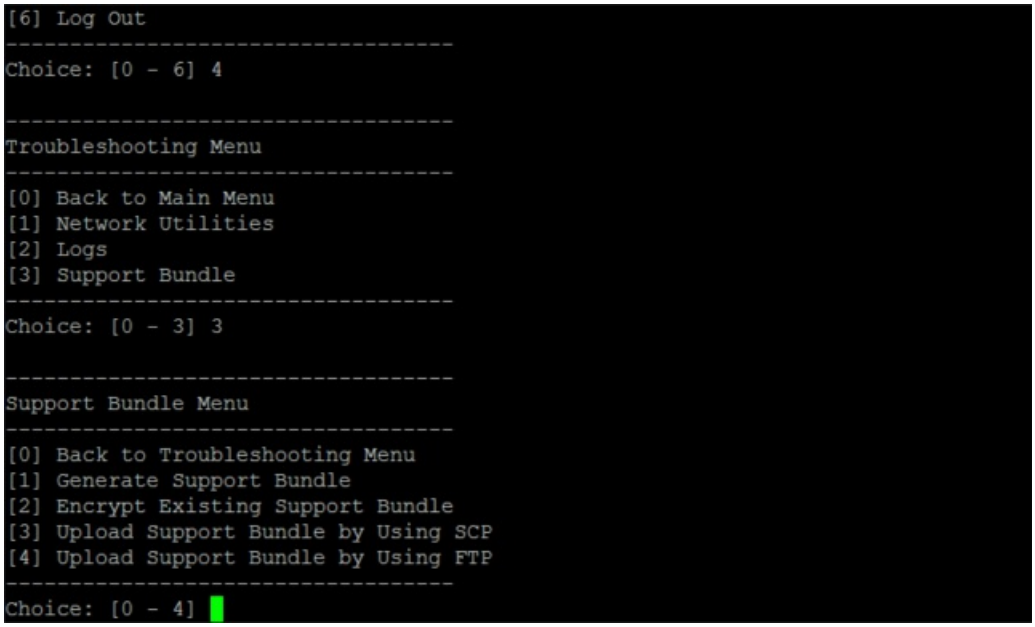
25. 下一步，您将对 App Controller 应用升级修补程序，然后生成并上载一个支持包。 首先，请按照 **App Controller** 页面中的说明升级 App Controller。 然后，请按照以下步骤创建支持包：



a. 在 App Controller 命令行控制台中，键入 **4**，然后按 Enter 键打开“Troubleshooting”（故障排除）菜单。



b.在“Troubleshooting”（故障排除）菜单中，键入 **3**，然后按 Enter 键打开“支持包”菜单。



c.在“支持包”菜单中，键入 **1**，按 Enter 键，然后按命令提示进行操作。

```
[6] Log Out
---------------------------------
Choice: [0 - 6] 4

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

---------------------------------
Support Bundle Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
---------------------------------
Choice: [0 - 4] 1
```

注意：必须加密支持包。

d.键入 **y**，按 Enter 键，然后按照命令提示进行操作。

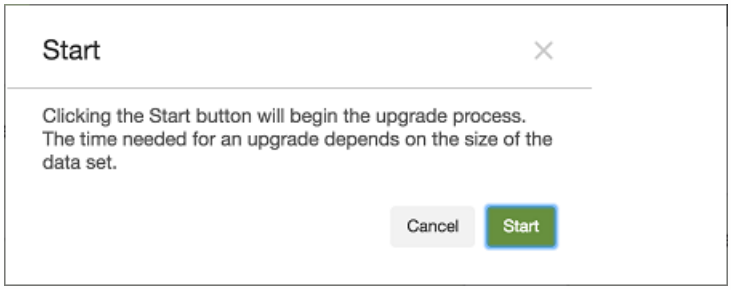
```
---------------------------------
Troubleshooting Menu
---------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
---------------------------------
Choice: [0 - 3] 3

---------------------------------
Support Bundle Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
---------------------------------
Choice: [0 - 4] 1
Do you want to encrypt the support bundle? [y/n] y

Please wait while AppController creates the support bundle.
```

e. 在“支持包”菜单中，键入 **3**，按 Enter 键，然后按命令提示进行操作。

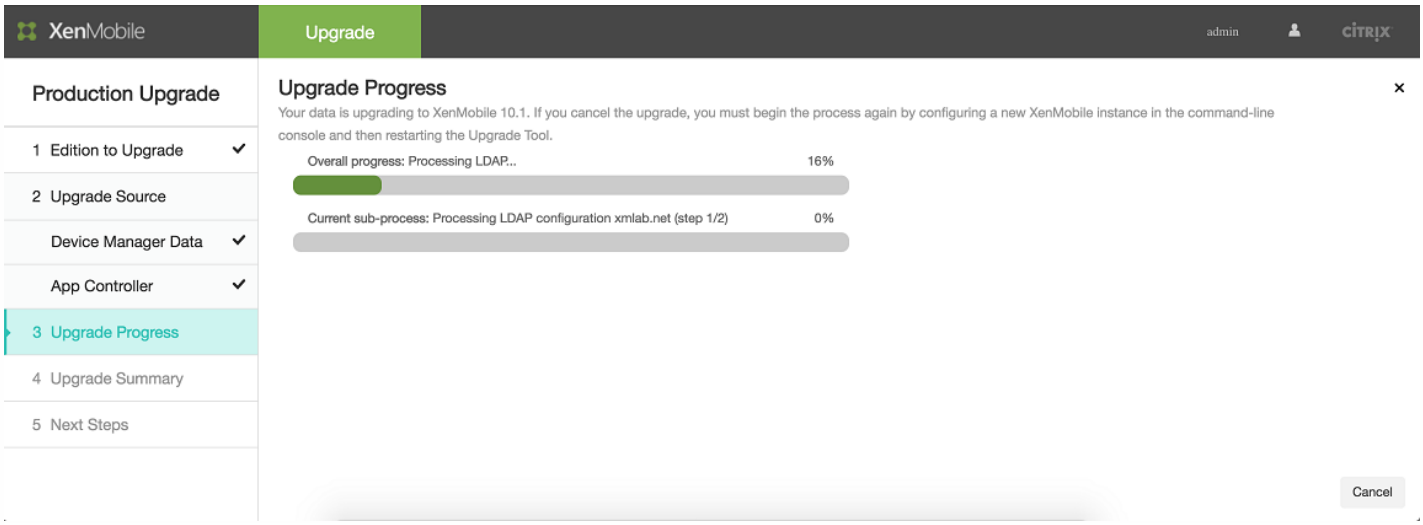
26. 在 **App Controller** 页面中，指定支持包，然后单击 **Upload**（上载）。

升级工具处理收集的文件（针对 XenMobile Enterprise Edition）和支持包。 如果要迁移大量用户，此步骤可能需要 15 分钟以上的时间。

27. 单击 **Next**（下一步）。 此时将显示 **Start**（开始）确认对话框。



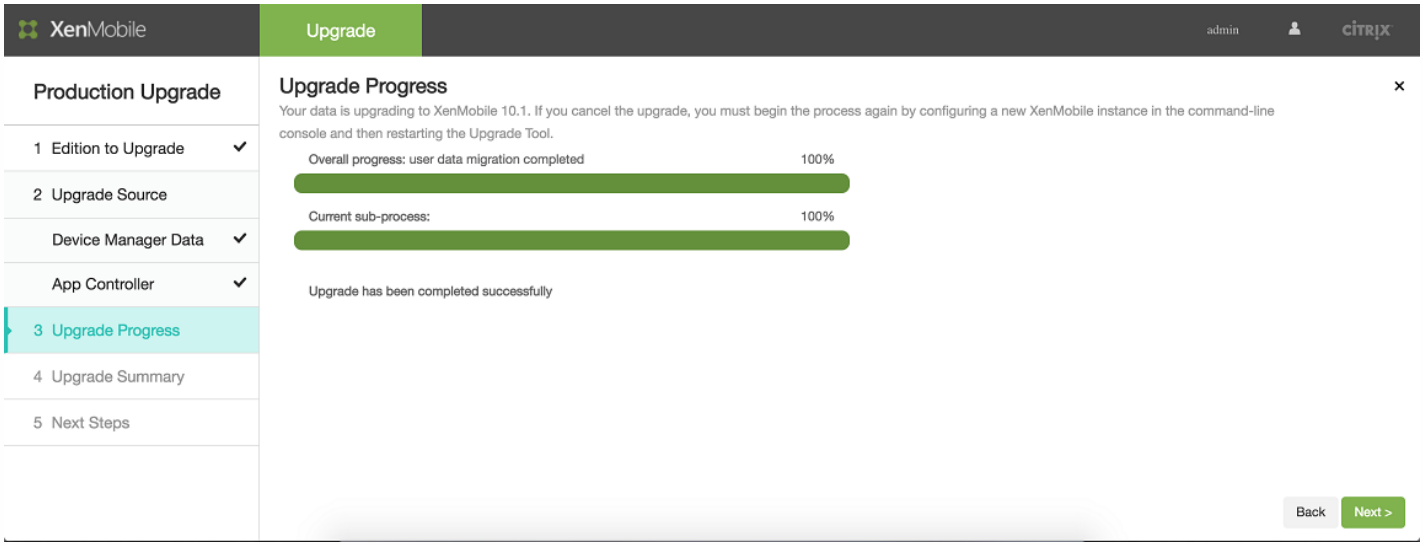
28. 单击 **Start**（开始）。 此时将显示包含进度指示条的 **Upgrade**（升级）页面，让您可以跟踪从 XenMobile 9.0 进行的数据升级。 升级完成时，进度指示器将指示 100%，并启用 **Next**（下一步）按钮。



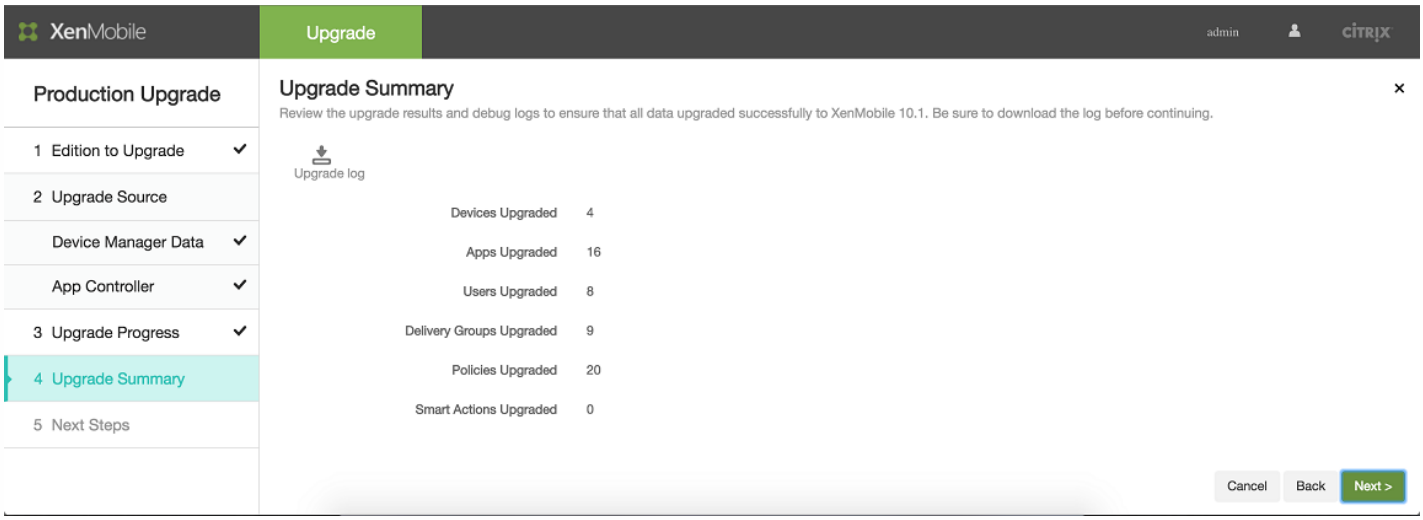
注意

如果升级失败，可以查看日志以了解失败的原因。 然后，需要导入新的 XenMobile 10.1 实例并重新启动升级过程。 不能使用浏览器的**返回**按钮返回到之前的页面并更正信息。

“Upgrade Progress”（升级进度）页面可以显示升级成功完成的时间。



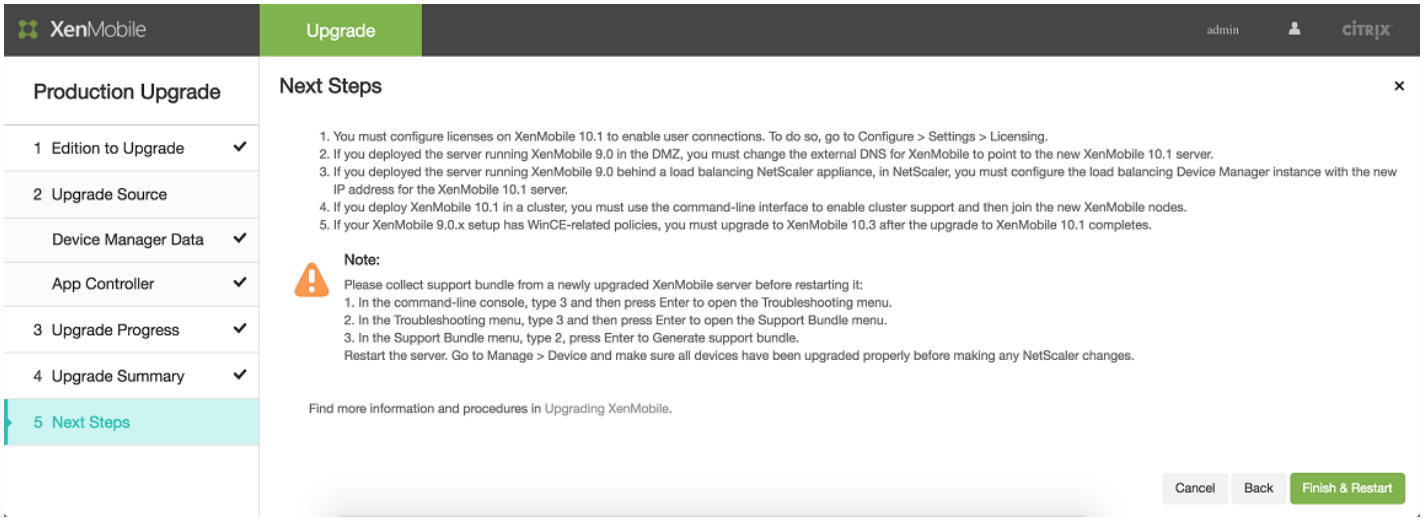
29. 单击 **Next**（下一步）。 此时将显示 **Upgrade Summary**（升级摘要）页面。



30. 单击 **Upgrade log**（升级日志）图标下载日志。 请务必在离开此页面之前下载日志。

Citrix 建议您查看日志以确定已升级或未升级到 XenMobile 10.1 的策略、设置、用户数据等信息。

31. 下载升级日志后，单击 **Next**（下一步）。 此时将显示 **Next Steps**（后续步骤）页面。



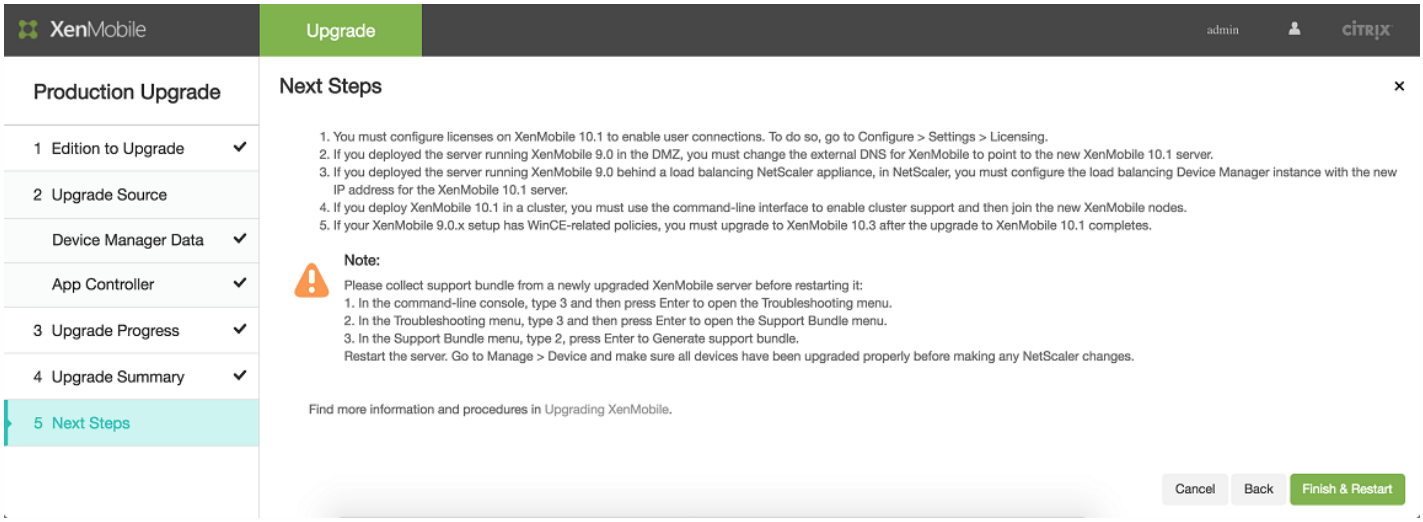
有关这些步骤的相关说明，请参阅升级工具后续条件。

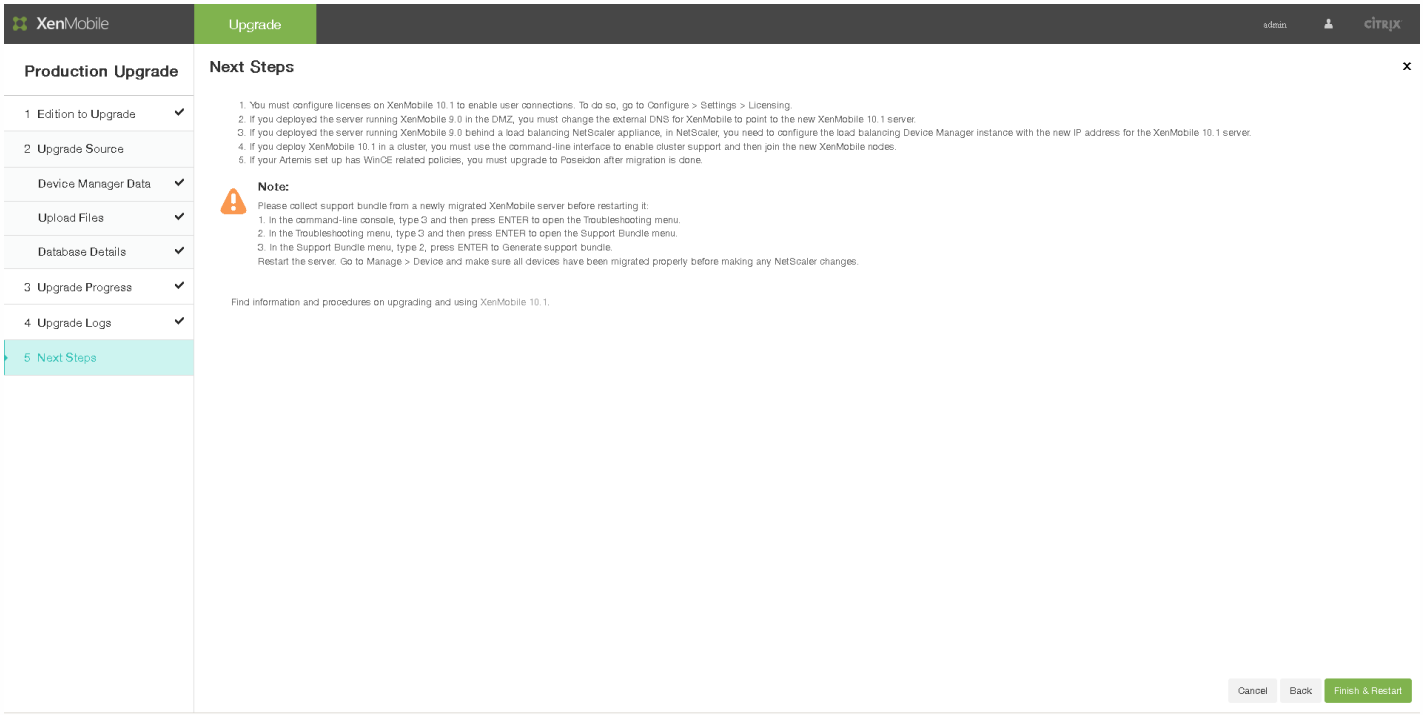
升级工具后续条件

Oct 13, 2016

升级后，请确保完成以下后续条件步骤。单击 **Finish & Restart**（结束并重新启动）时，服务器会重新启动。

注意：使用 XenMobile 9.0 Device Manager 管理员凭据通过 https://:4443 登录 XenMobile 控制台。（如果要完成 MAM 升级，则应输入 XenMobile 9.0 App Controller 管理员凭据。）





许可

XenMobile 10.1 仅支持 Citrix V6 许可。请务必按照下图所示在 XeadnMobile 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 10.1 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 10.1 的独立服务器，可以在 XenMobile 控制台中上载许可证。

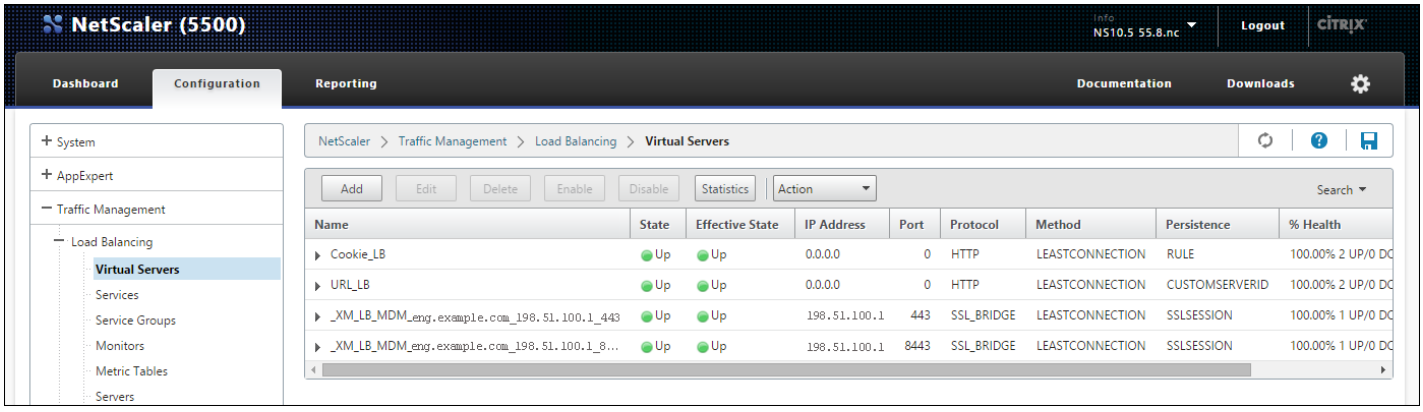
NetScaler

> ## 注意
>
> 仅当升级 XenMobile Enterprise Edition 生产升级时才需要满足此后续条件，升级 MAM 或 MDM 不需要满足此后续条件。

按照 NetScaler 中的步骤操作将导致为 XenMobile 9.0 App Controller FQDN 创建新的负载平衡虚拟服务器。遵循主要步骤包括：

1. 配置迁移负载平衡虚拟服务器。
2. 为 App Controller FQDN 创建主机条目，指向新的负载平衡虚拟服务器。
3. 将 NetScaler Gateway 改为指向 XenMobile 服务器 FQDN:8443。
4. 将 Device Manager 负载平衡虚拟服务器改为指向新的 XenMobile 服务器 IP 地址。
5. 根据 SSL 桥接或 SSL 卸载 MDM 配置创建新的 MAM 负载平衡虚拟服务器。
6. 为 XenMobile 服务器 FQDN 创建主机条目，指向新的 MAM 负载平衡虚拟服务器。

1. 登录 NetScaler，然后单击 **Traffic Management**（流量管理）> **Load Balancing**（负载平衡）> **Virtual Servers**（虚拟服务器）。

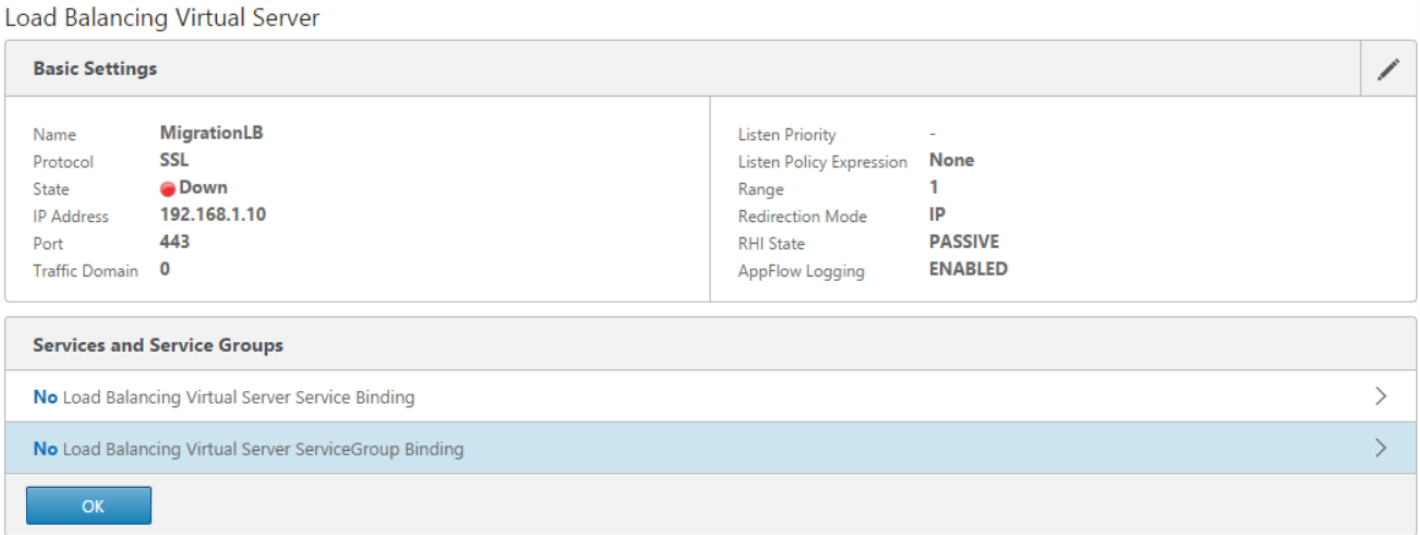


2. 单击 **Add**（添加）。

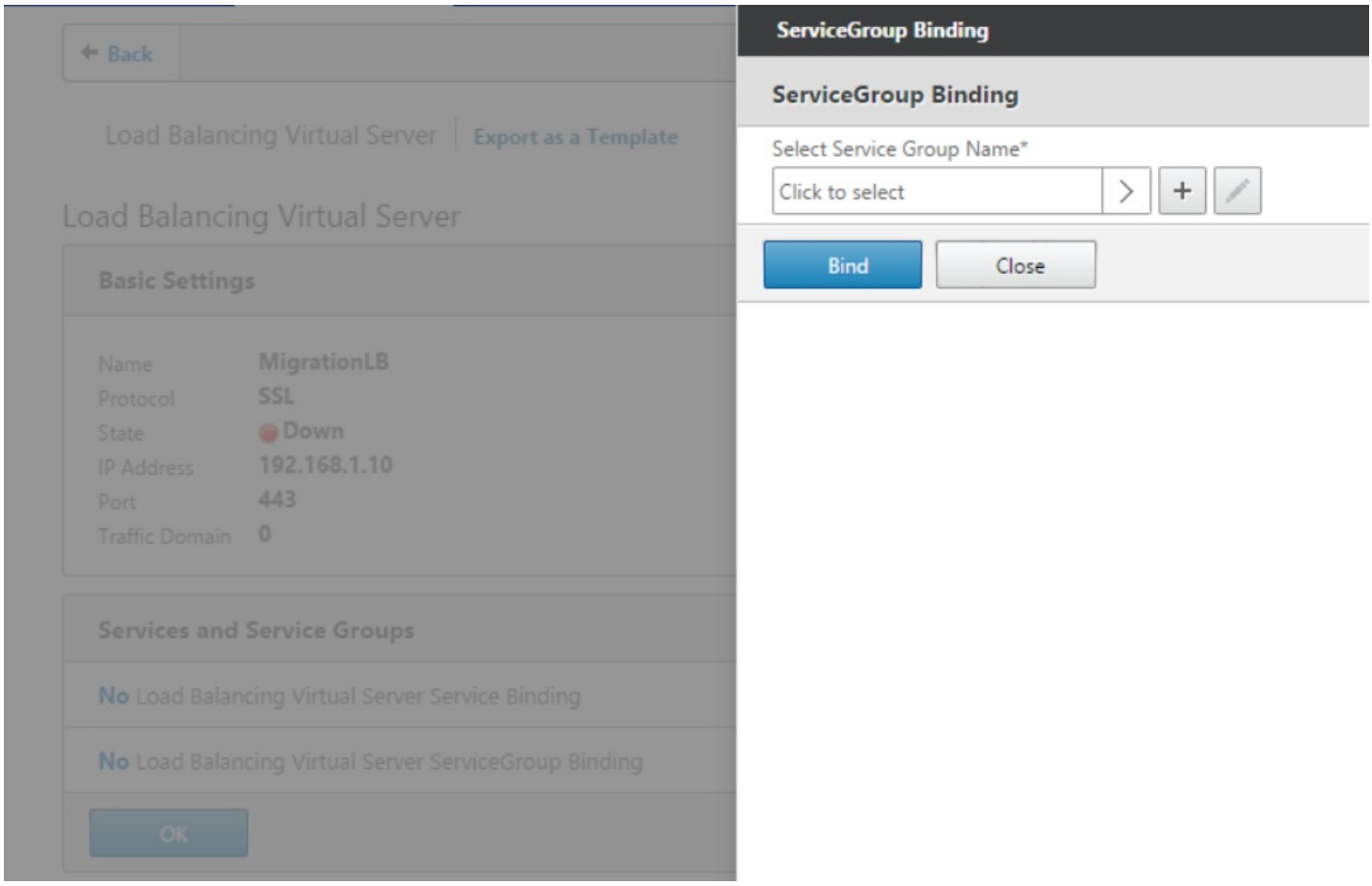
3. 在 **Load Balancing Virtual Server**（负载平衡虚拟服务器）页面上，配置以下设置，然后单击 **OK**（确定）。

- **Name**（名称）：键入新负载平衡器的名称。
- **Protocol**（协议）：确保将其设置为 SSL。默认设置为 HTTP。
- **IP Address**（IP 地址）：输入遵循 RFC 1918 的新负载平衡器 IP 地址，例如 192.168.1.10。
- **Port**（端口）：确保端口号为 443。

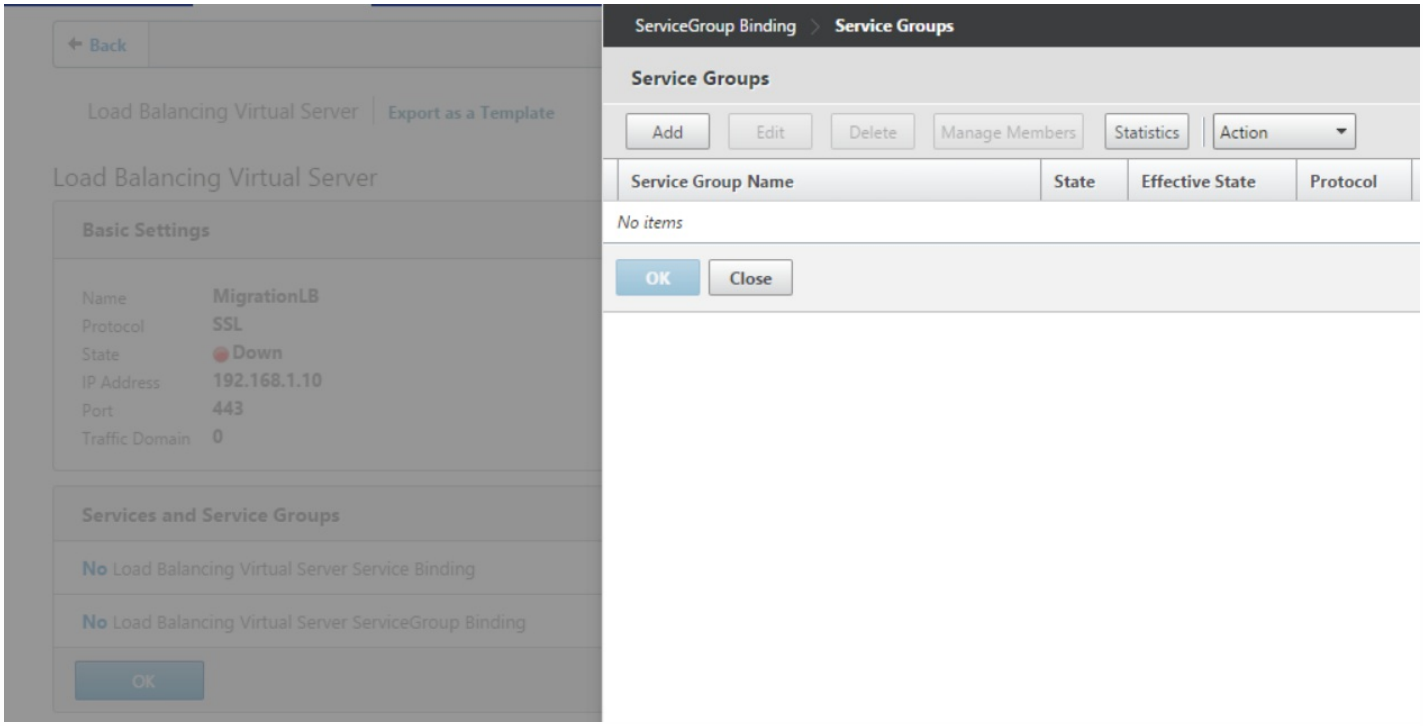
4. 在 **Services and Service Groups**（服务和服务组）下面，单击 **No Load Balancing Virtual Server Service Group Binding**（无负载平衡虚拟服务器服务组绑定）。



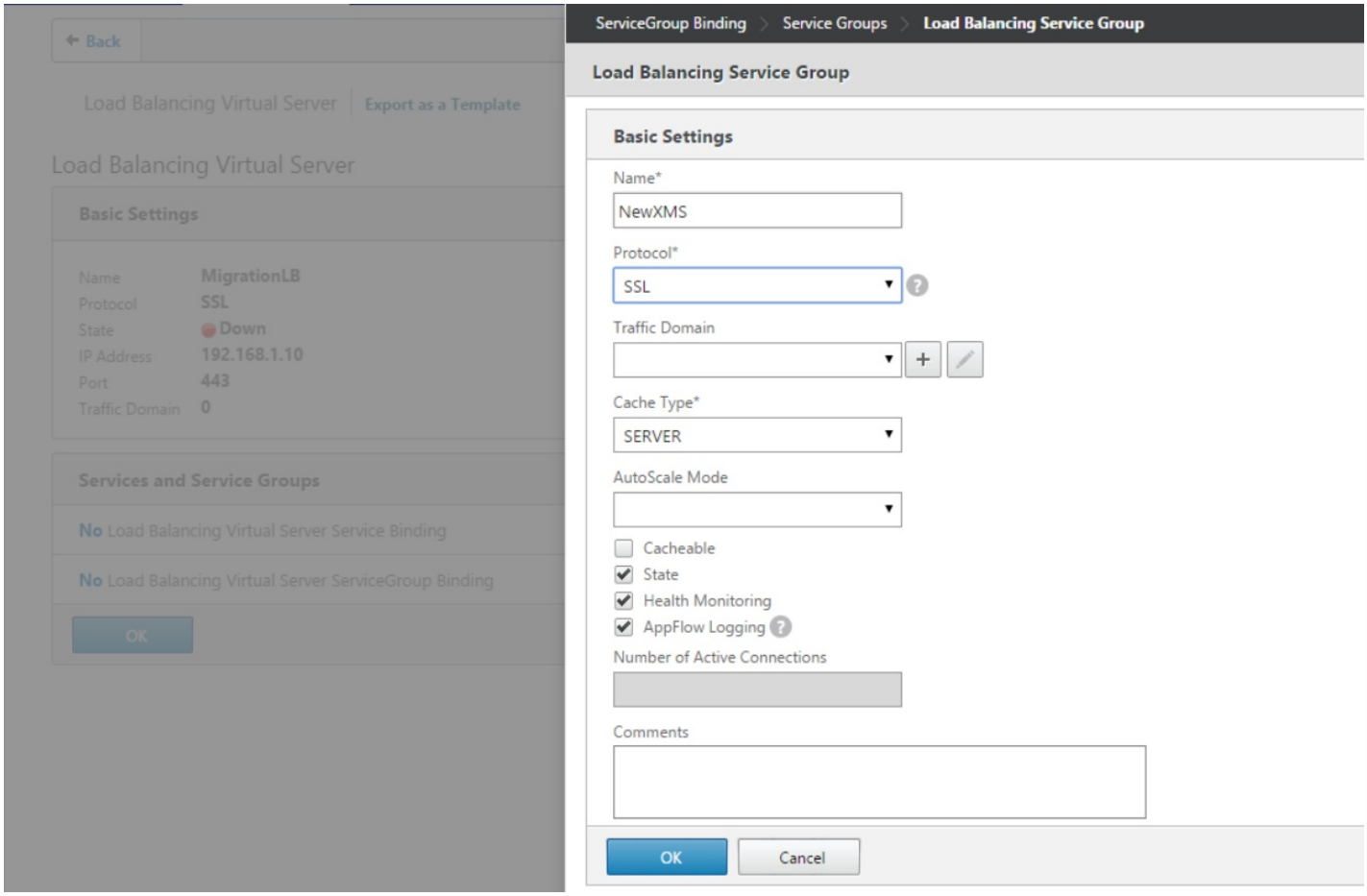
5. 在 **Select Service Group Name**（选择服务组名称）下，单击 **Click to Select**（单击以选择）。



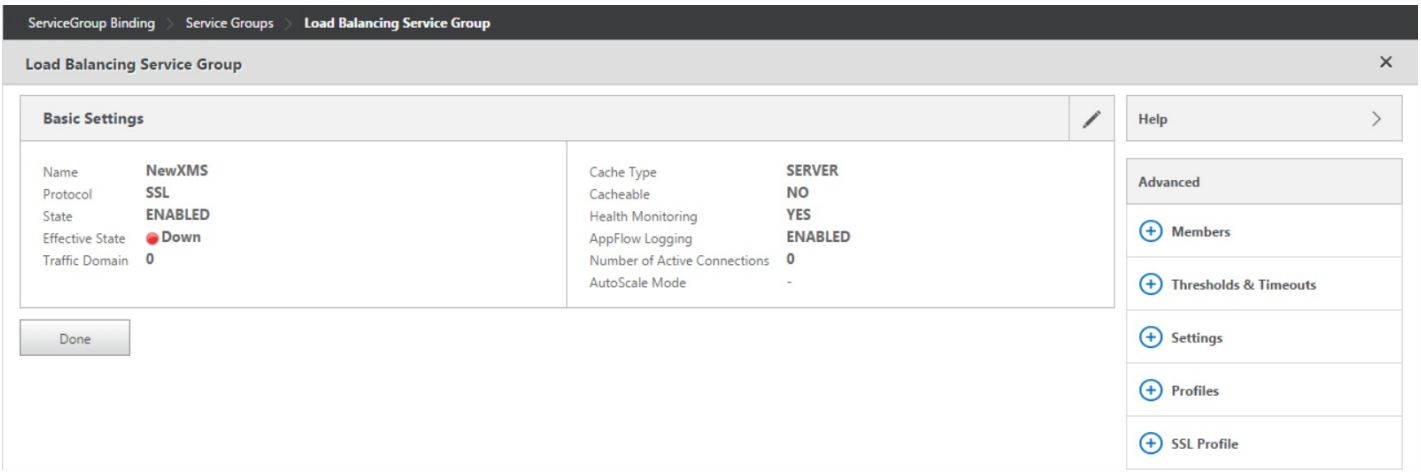
6. 单击 **Add**（添加）创建新服务组。



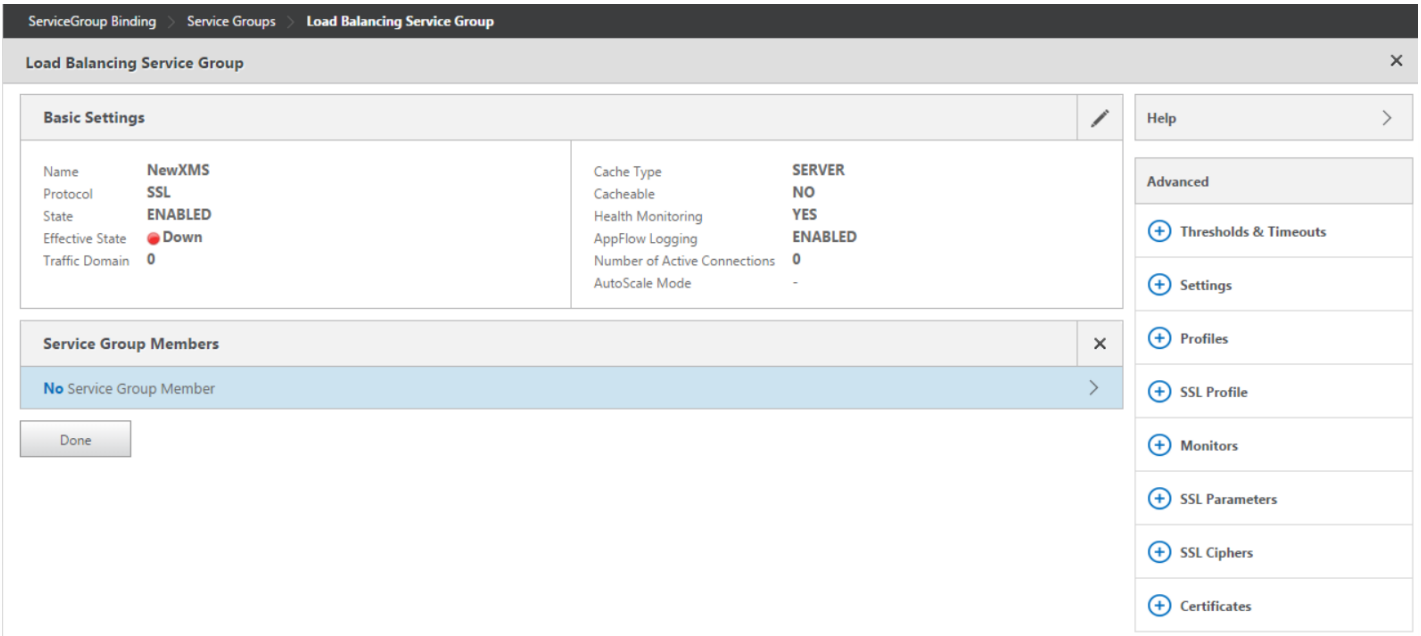
7. 在 **Load Balancing Service Group**（负载平衡服务组）页面上，键入新服务组的名称，确保将协议设为 **SSL**，然后单击 **OK**（确定）。



8. 单击 **Members**（成员）。



9. 单击突出显示的 **No Service Group Member**（无服务组成员）条目。



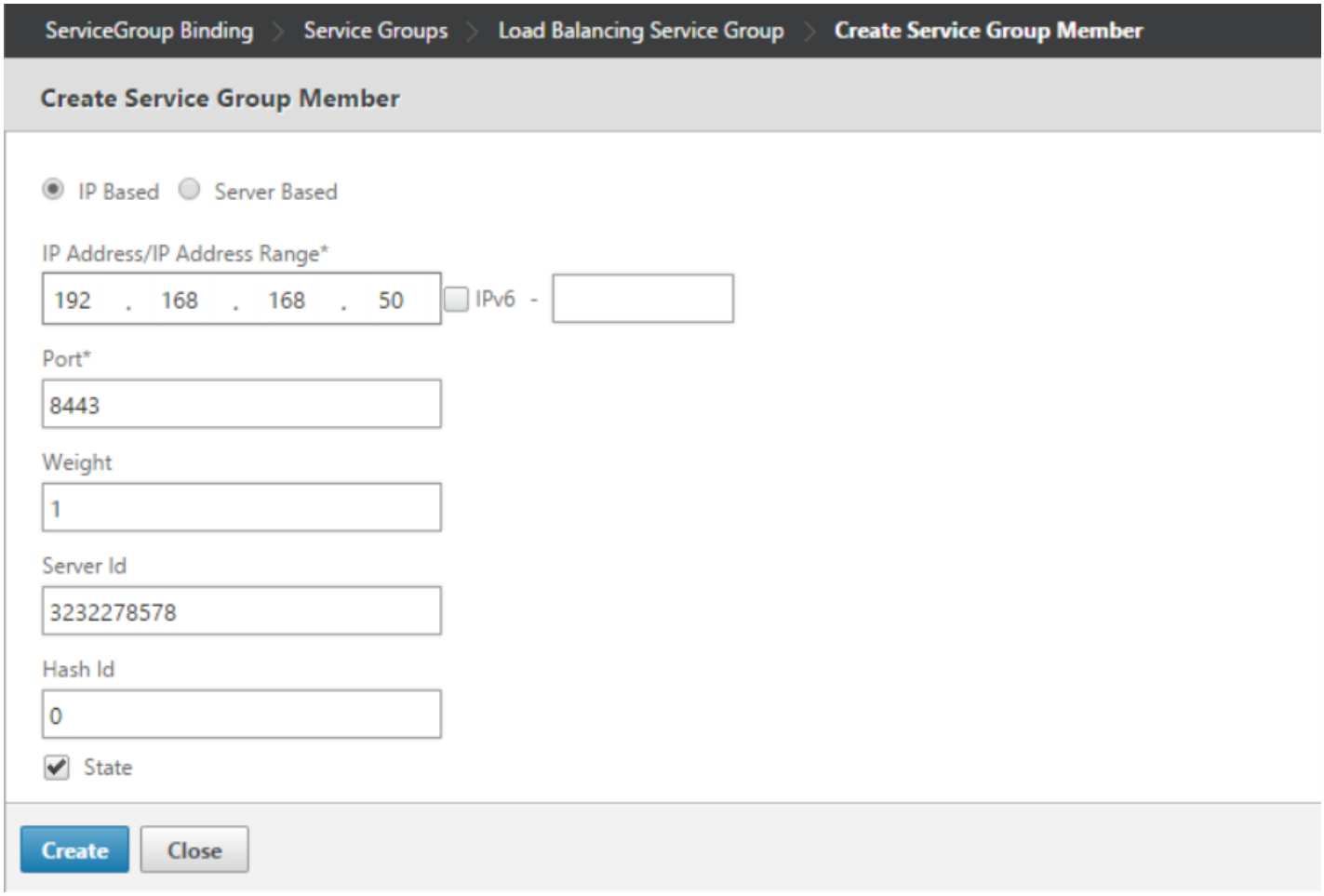
10. 在 **Create Service Group Member**（创建服务组成员）页面上，配置以下设置：

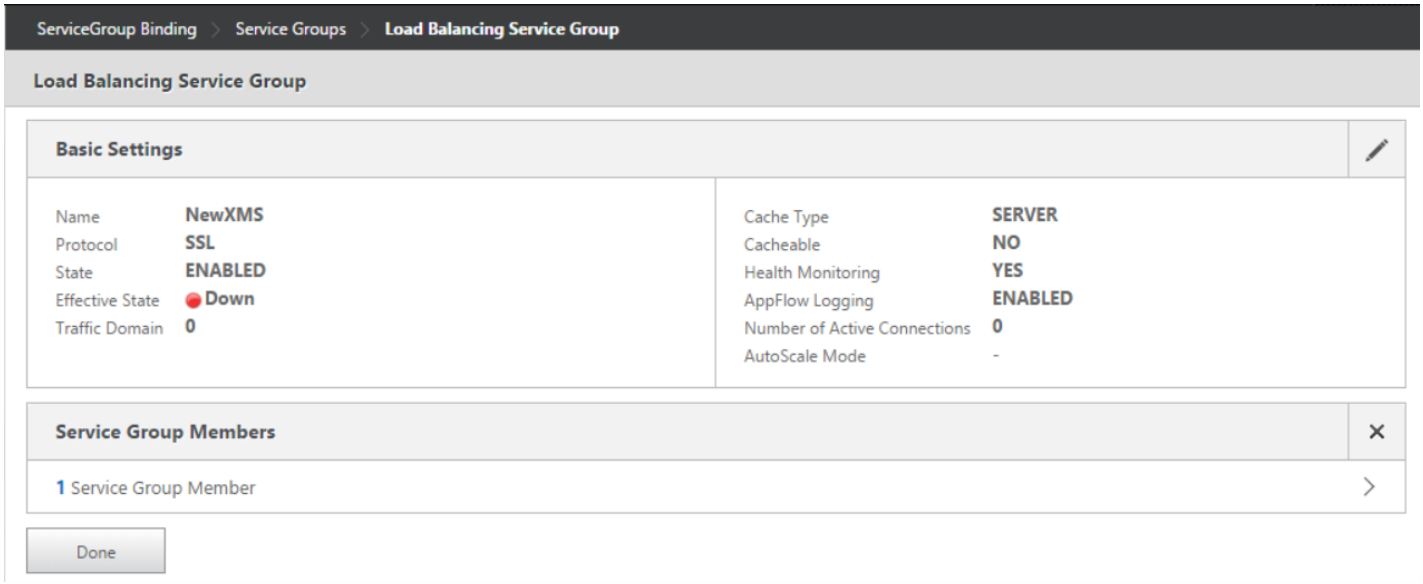
- **IP Address/IP Address Range***（IP 地址/IP 地址范围*）：输入 XenMobile 10.1 服务器的 IP 地址。
- **Port**（端口）：设置为 8443。
- **Server ID**（服务器 ID）：如果要从群集 XenMobile 9.0 环境迁移到 XenMobile 10.1 群集环境，请输入当前 XenMobile 服务器的服务器节点 ID。

> **注意**
>
> 可以登录 XenMobile 10.1 服务器命令行接口 (CLI)，然后键入 1 以转入“群集”菜单，获取服务器节点 ID。服务器节点 ID 称为当前节点 ID。

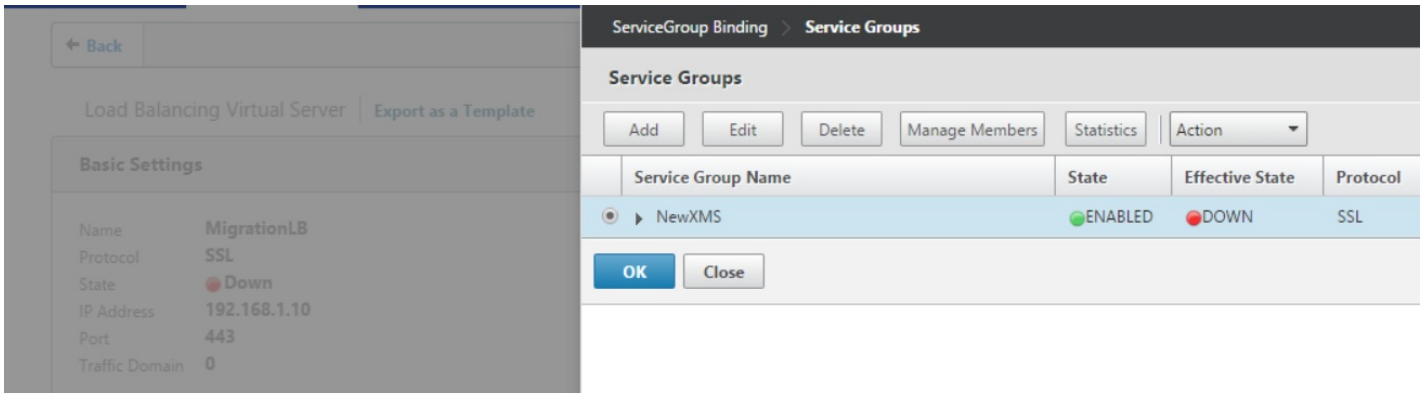
```
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
---------------------------------
Choice: [0 - 5] 1

Current Node ID: 181356771

Cluster Members:
node: 192.0.2.0 status: ACTIVE  role: OLDEST


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

11. 单击 **Create**（创建），然后单击 **Done**（完成）。

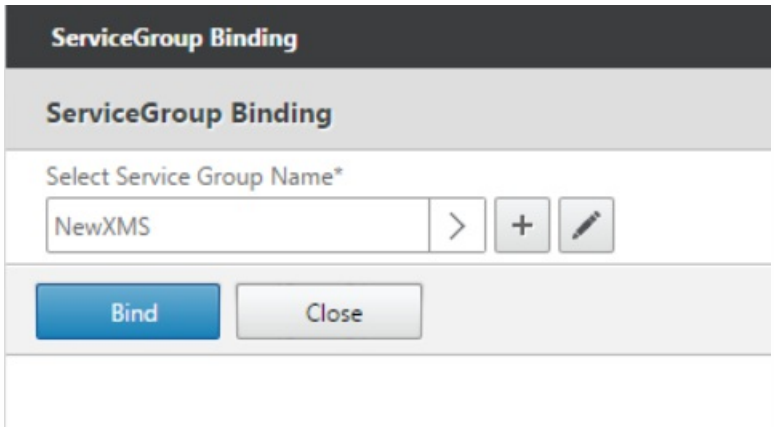


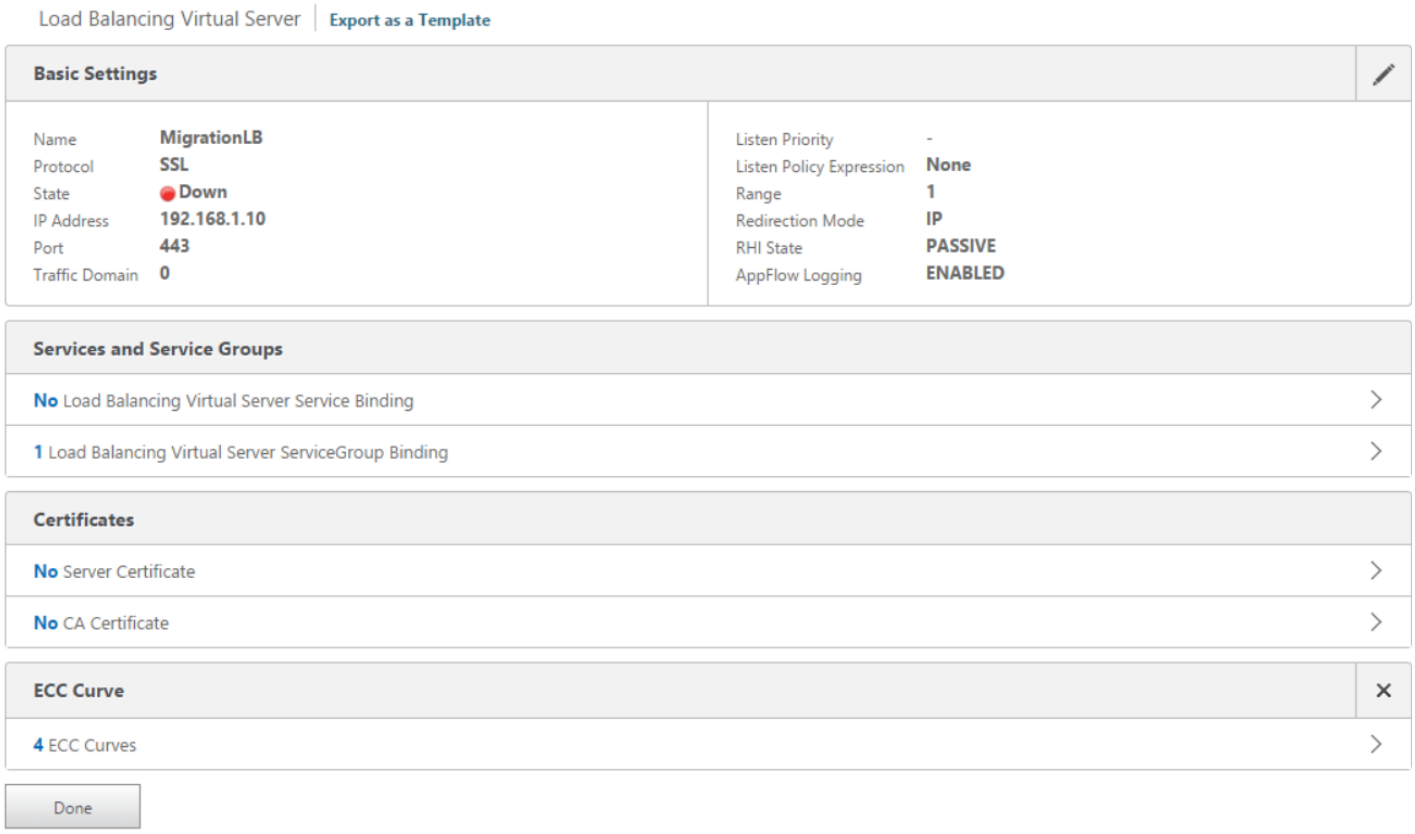


12. 单击 **OK**（确定）。

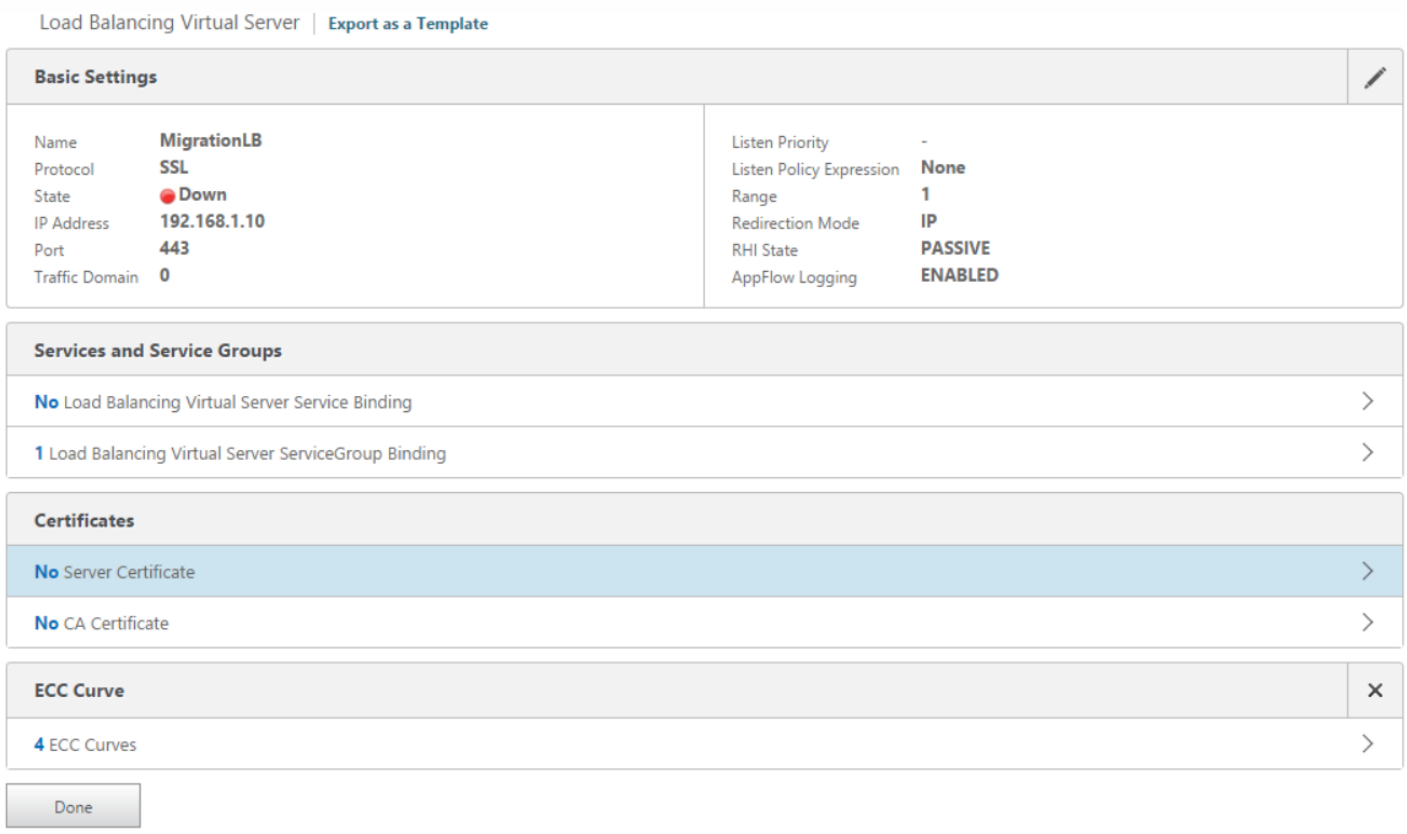


13. 单击 **Bind**（绑定），然后在下一屏幕上单击 **Done**（完成）。

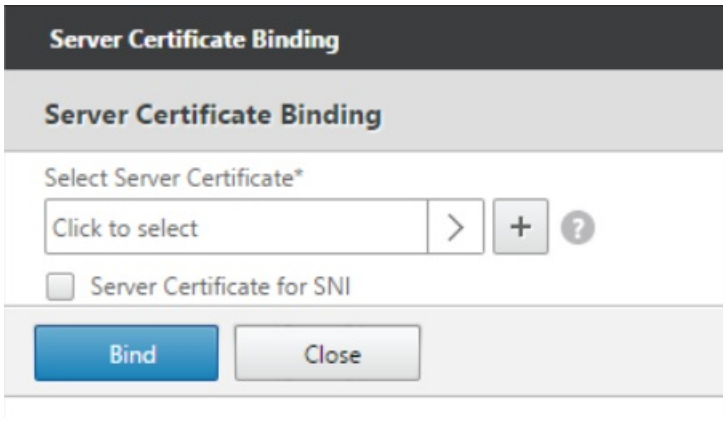




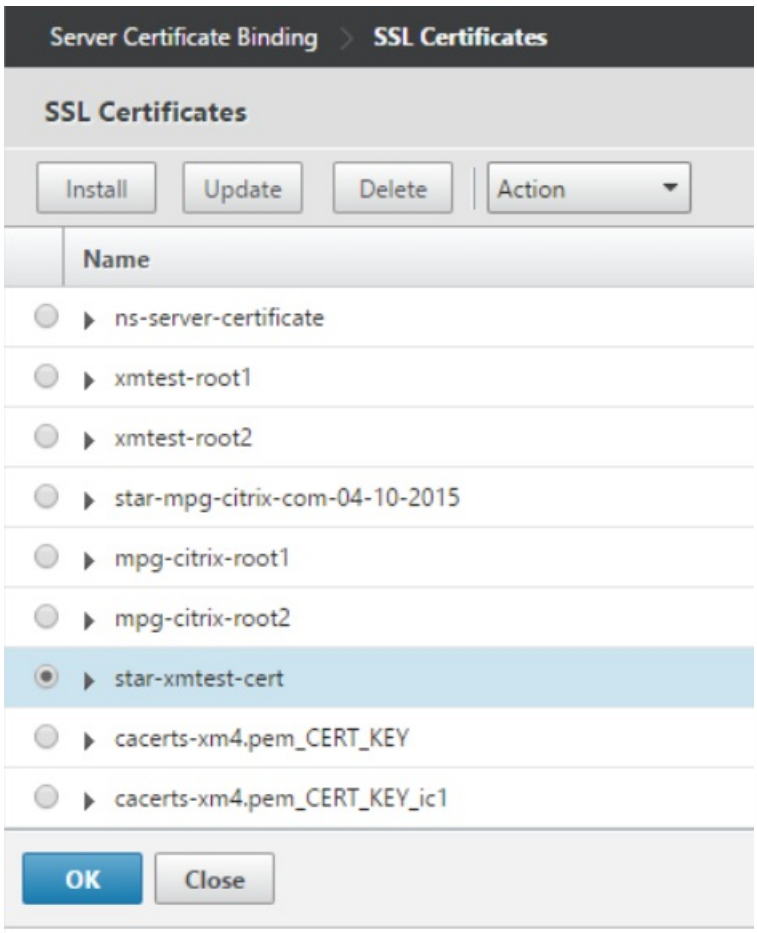
14. 在 **Certificates**（证书）下，单击 **No Server Certificate**（无服务器证书）。



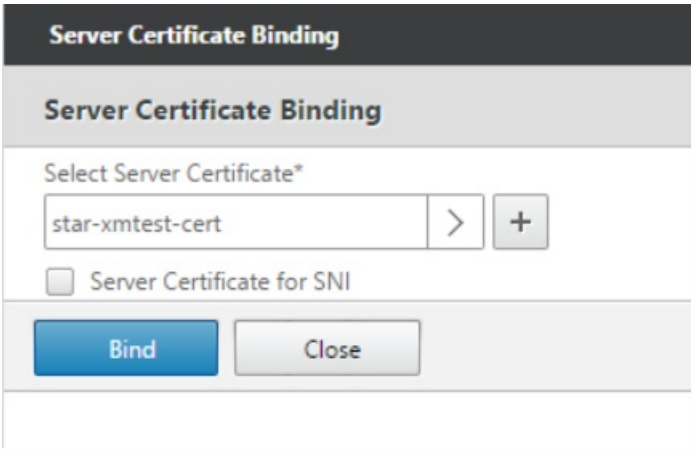
15. 在 **Server Certificate Binding**（服务器证书绑定）下，单击 **Click to Select**（单击以选择）。

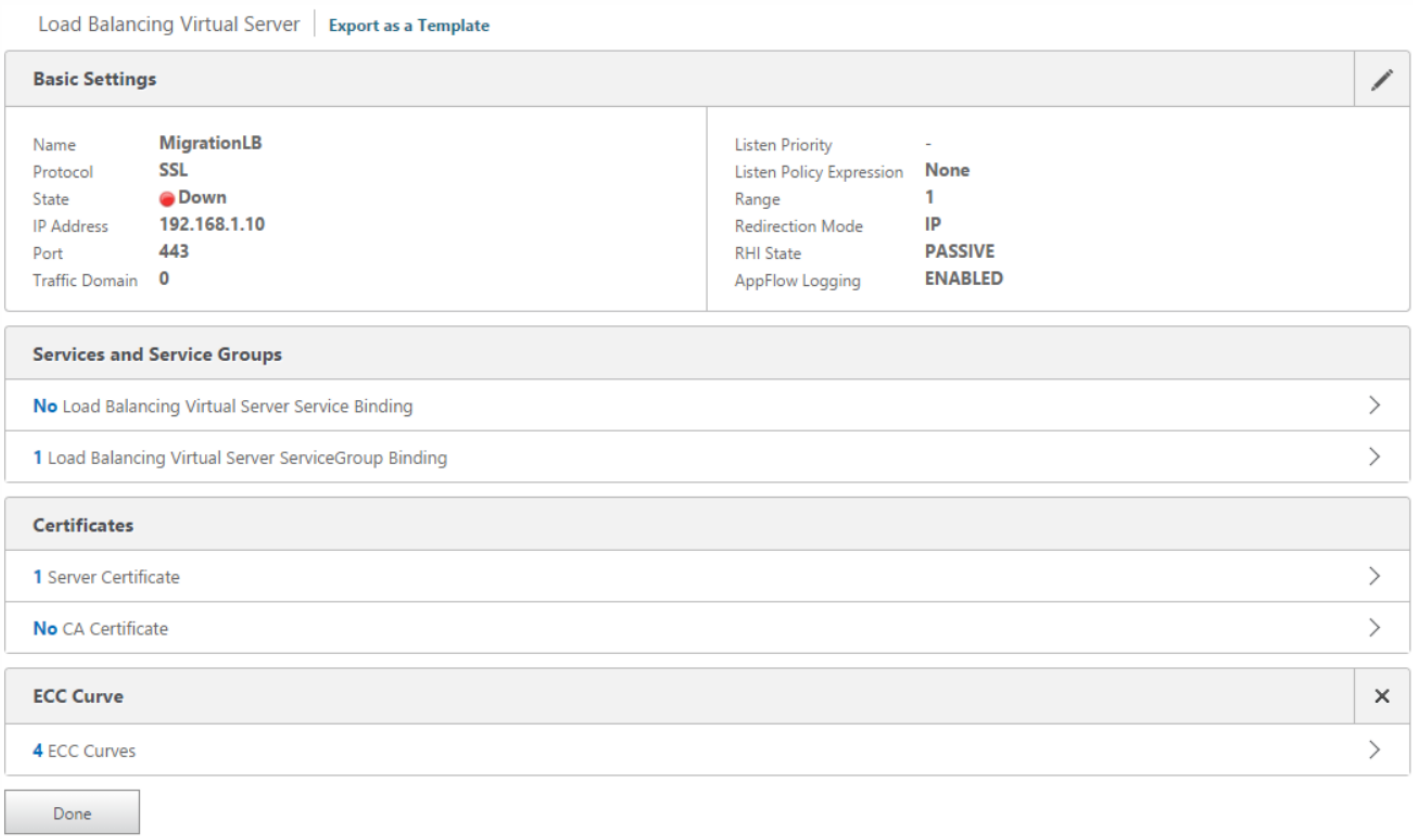


16. 在 **Certificates**（证书）下，单击在 Prerequisites（必备条件）中导出的服务器证书，单击 **OK**（确定）。

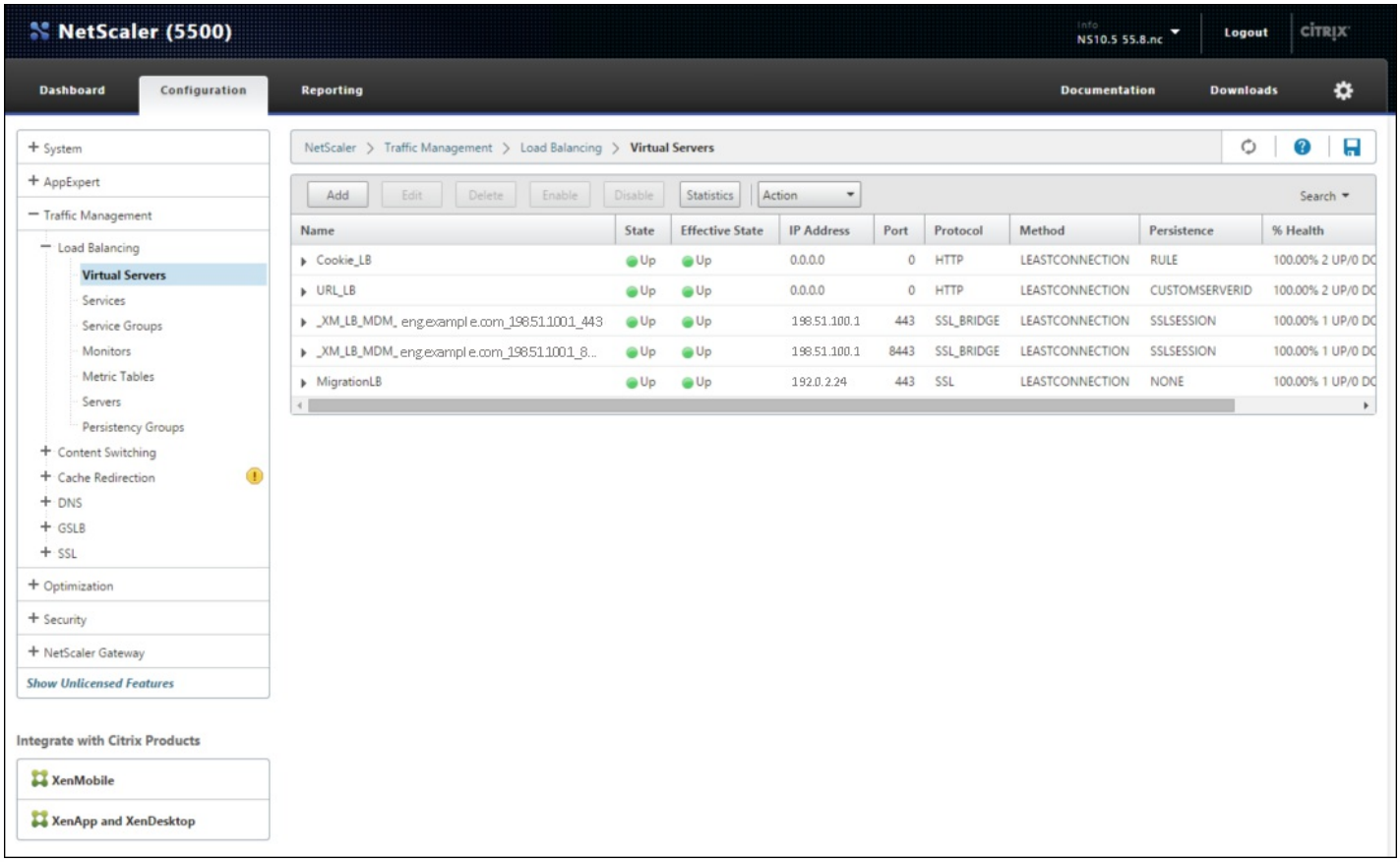


17. 单击 **Bind**（绑定），然后在下一屏幕上单击 **Done**（完成）。





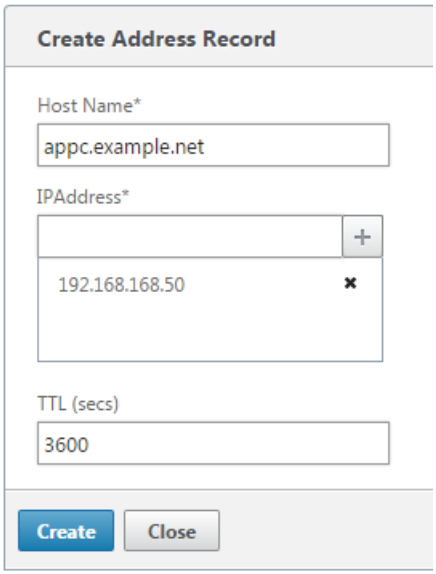
18. 单击刷新按钮以确认服务器已启动。



为 AppController 服务器 FQDN 配置指向新迁移 LB 的地址记录

单击 **Traffic Management**（流量管理）> **DNS** > **Records**（记录）> **Address Records**（地址记录），然后单击 **Add**（添加），为 AppController FQDN 创建指向新迁移负载平衡器的新地址记录。

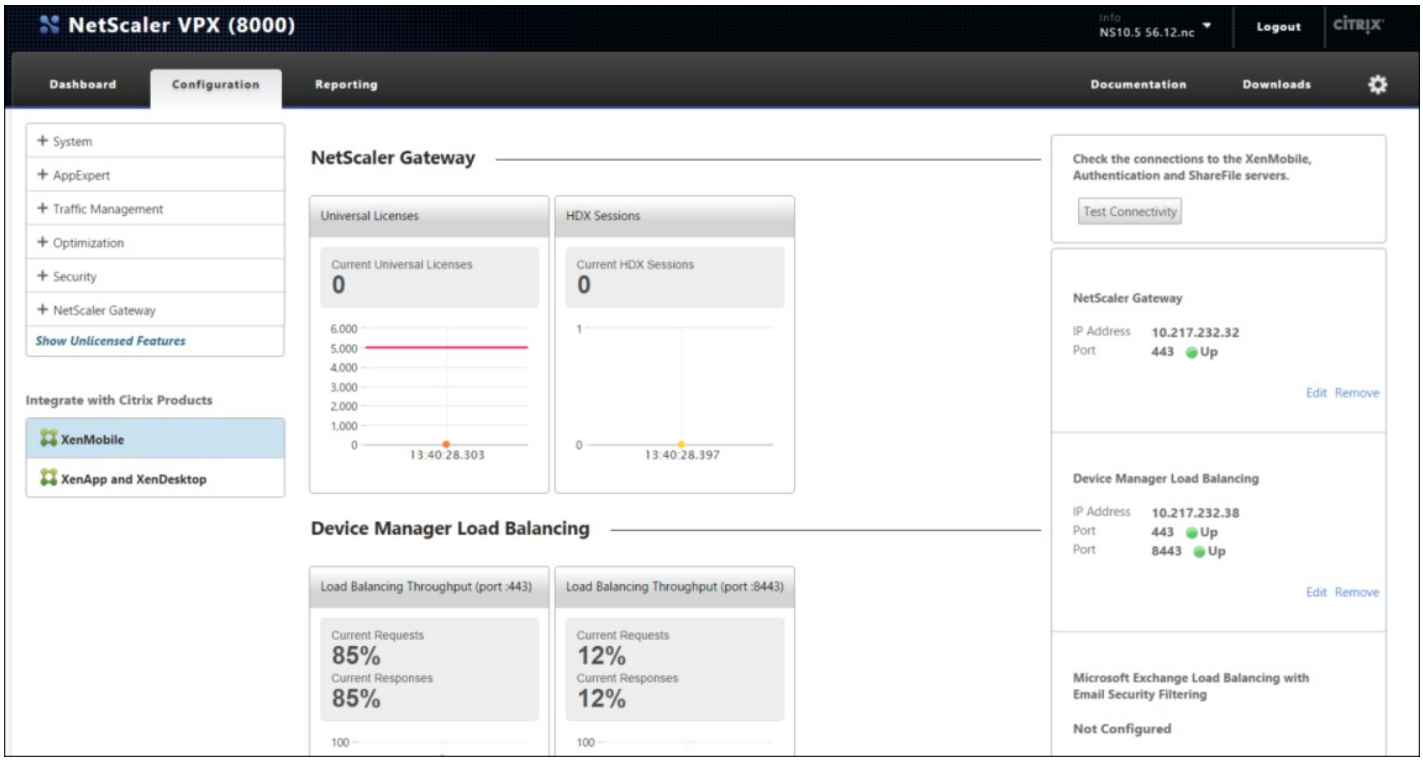
> **注意**
>
> 如果您拥有全局服务器负载平衡配置，添加地址记录会导致全局服务器负载平衡系统可靠地响应具有本地 IP 地址的服务器。



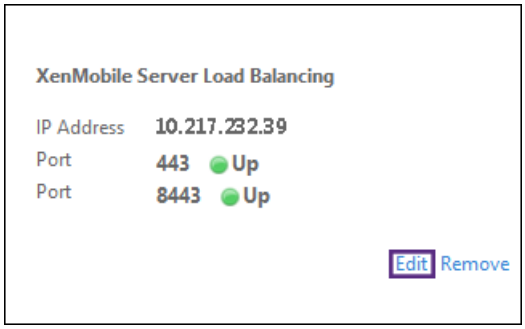
将 XenMobile 9.0 MDM 负载平衡器更新为指向新的 XenMobile 10.1 服务器 IP

如果您在负载平衡的 NetScaler 设备后面部署了运行 XenMobile 9.0 的服务器，则需要在 NetScaler 中使用 XenMobile 10.1 的新 IP 地址配置负载平衡的 XenMobile 9.0 Device Manager 实例，并将 XenMobile 9.0 服务器证书上载到 XenMobile 10.1 服务器。

1. 启动 NetScaler XenMobile 配置实用程序。

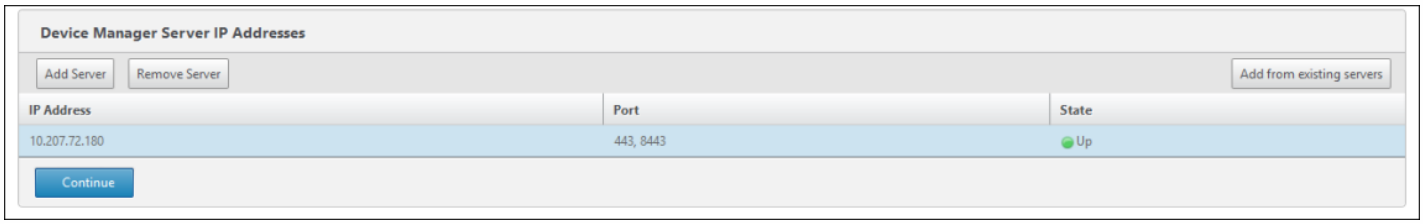


2. 在屏幕右侧的 **XenMobile Server Load Balancing**（XenMobile 服务器负载平衡）下，单击 **Edit**（编辑）。



3. 单击笔形图标以编辑 **Device Manager Server IP Addresses**（Device Manager 服务器 IP 地址）。

4. 选择 XenMobile 9.0 Device Manager 服务器 IP 地址，然后单击 **Remove Server**（删除服务器）。



5. 单击 **Add Server**（添加服务器），然后添加新的 XenMobile 10.1 服务器 IP 地址。**注意**：您无法在此处设置端口号。服务器在端口 80 上创建，并置于“Down”（关闭）状态。您必须为端口 443 和 8443 创建服务，并将这些服务与相应的负载平衡虚拟服务器绑定在一起。

在 NetScaler Gateway 上更改 App Controller FQDN

在 XenMobile 10.1 中，App Controller 组件在端口 8443（而非端口 443）上侦听。需要根据正在迁移的版本更改 App Controller FQDN。

XenMobile Enterprise Edition

将 App Controller FQDN 更改为指向新的 XenMobile 10.1 FQDN，这是后跟端口 8443 的 XenMobile 9.0 Device Manager FQDN。下表中显示了一个示例。

XenMobile 9.0 组件	组件 FQDN	XenMobile 10.1 Enterprise Edition FQDN
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	不适用
NetScaler Gateway	access.example.com	不适用

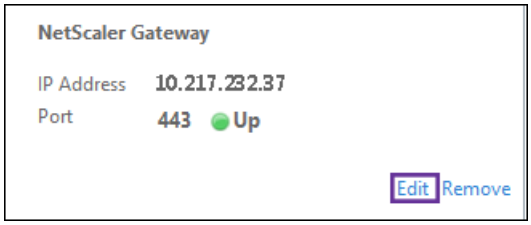
XenMobile App Edition

将 App Controller FQDN 更改为指向新的 XenMobile 10.1 FQDN，这是后跟端口 8443 的 XenMobile 9.0 App Controller FQDN。下表中显示了一个示例。

XenMobile 9.0 组件	组件 FQDN	XenMobile 10.1 Enterprise Edition FQDN
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	不适用

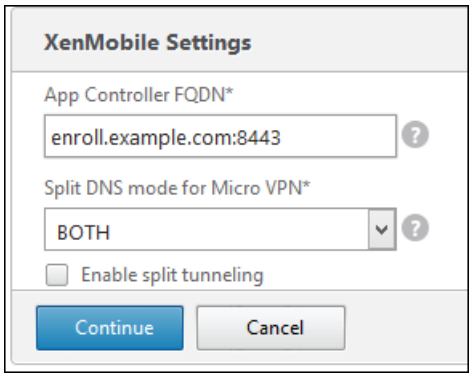
更改 App Controller FQDN

1. 在 **NetScaler Gateway** 下，单击 **Edit**（编辑）。

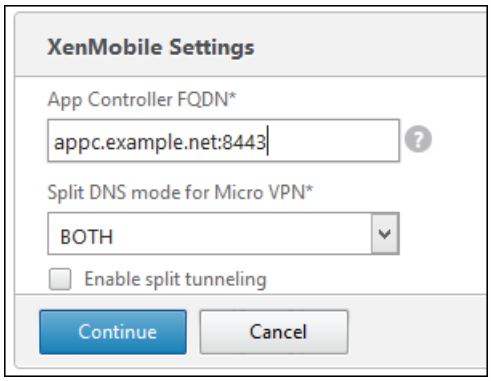


2. 单击 **XenMobile Settings**（XenMobile 设置）旁边的笔形图标。

3. 将 App Controller FQDN 改为：XenMobile Enterprise Edition：enroll.example.com:8443



XenMobile App Edition：appc.example.net:8443



4. 依次单击 **Continue**（继续）和 **Finish**（完成）。接下来，您需要更新 DNS，以便将 FQDN 解析为 XenMobile Server 10.1 的 IP 地址。

根据 SSL 桥接 MDM 配置创建新 MAM 负载平衡虚拟服务器

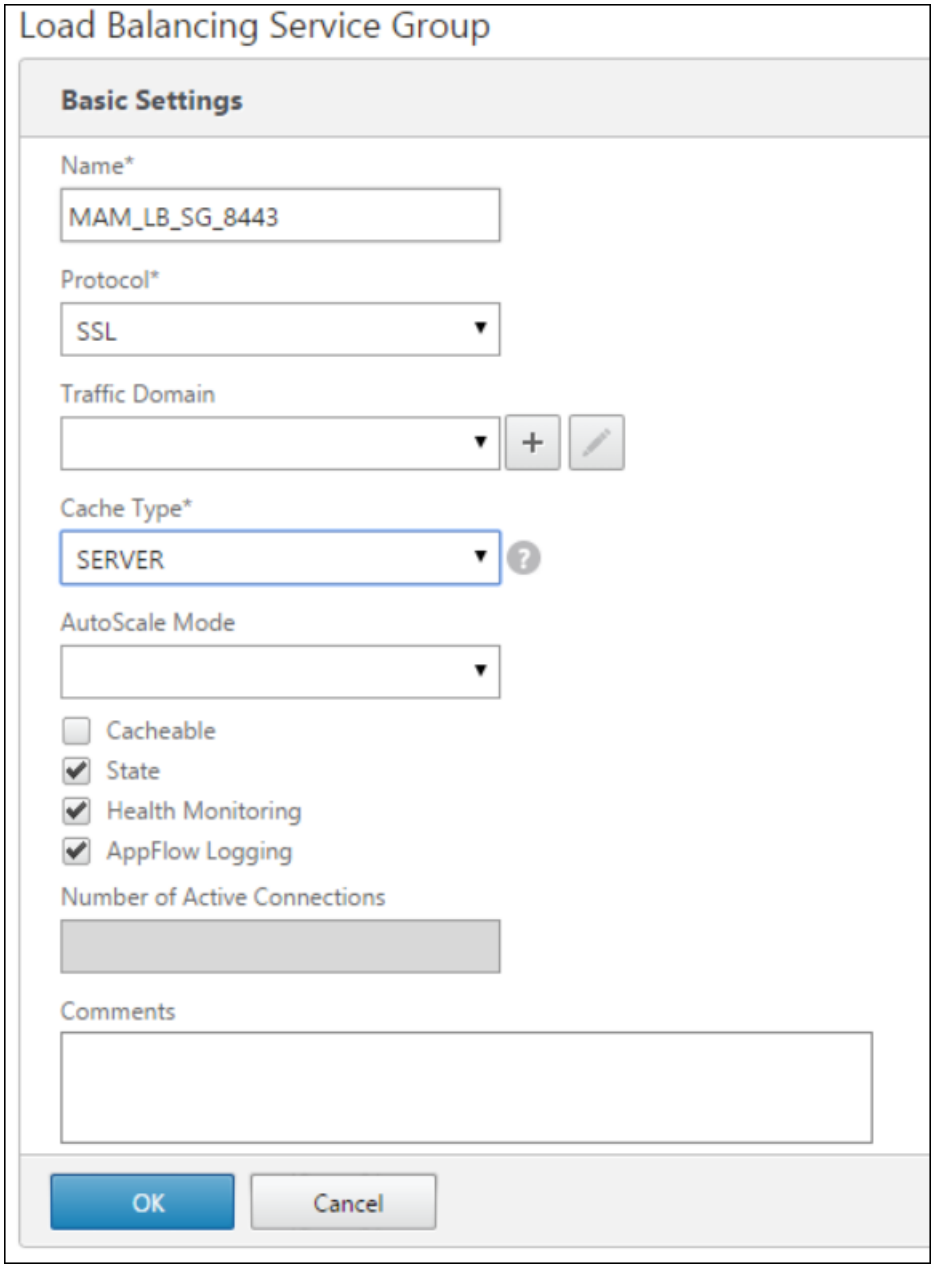
您需要创建一个新的 MAM 负载平衡虚拟服务器，才能根据现有 MDM 负载平衡虚拟服务器的配置对 MAM 流量进行负载平衡。以下过程介绍在配置了 SSL 桥接的情况下如何实现此操作。如果您的负载平衡虚拟服务器配置了 SSL 卸载，请参阅此过

程中的步骤。

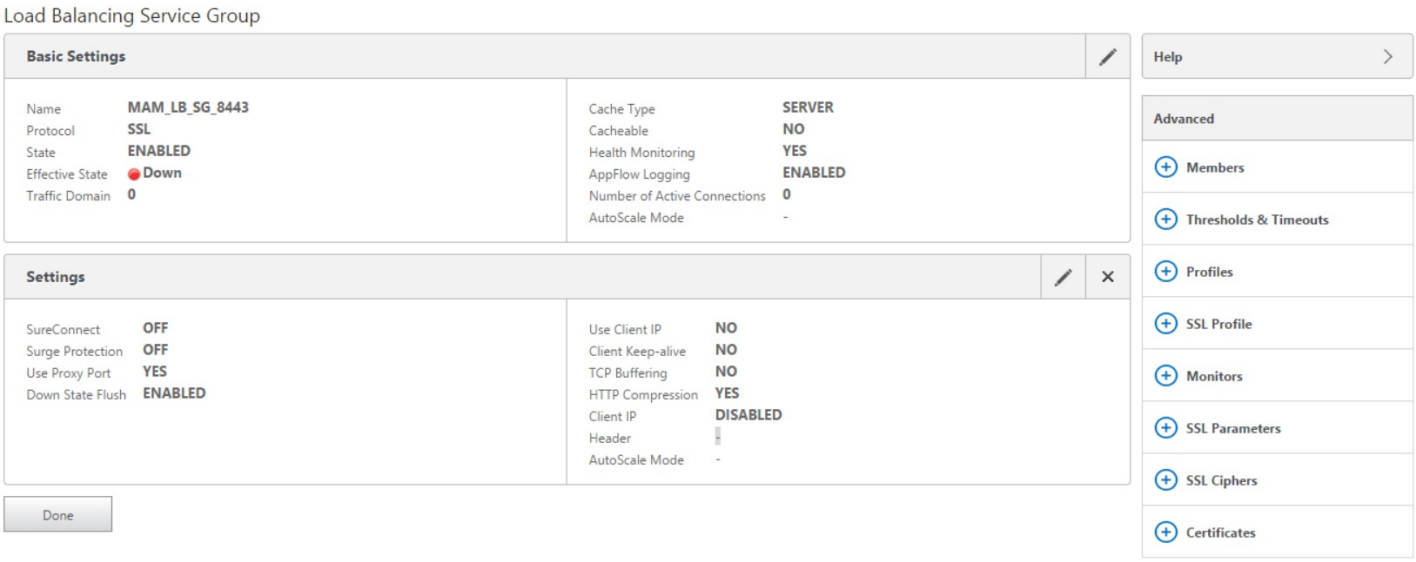
创建 MAM 负载平衡虚拟服务器并将“服务组”服务绑定到负载平衡虚拟服务器。

1. 单击 **Traffic Management**（流量管理）> **Load Balancer**（负载平衡器）> **Service Groups**（服务组）。

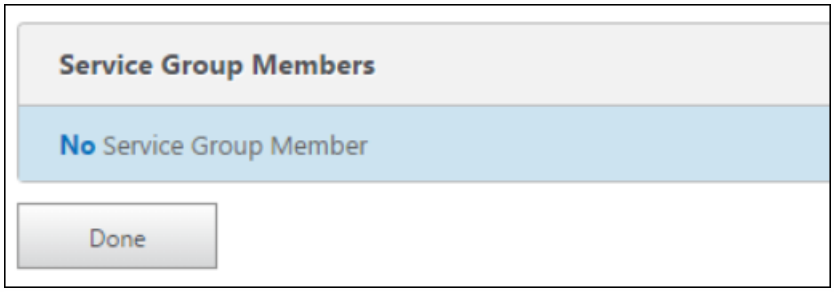
2. 单击“添加”，然后配置下图中所示的设置：



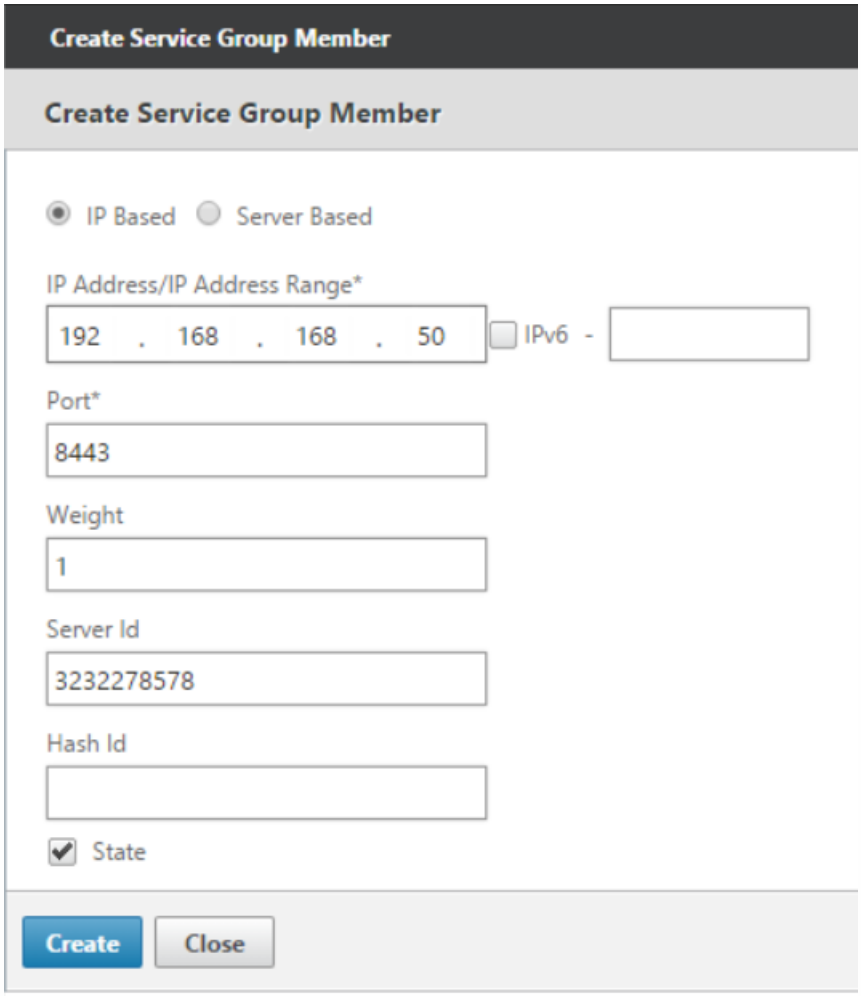
3. 单击 **OK**（确定），然后单击 **Members**（成员）。



4. 单击 **No Service Group Member**（无服务组成员）并添加新成员。



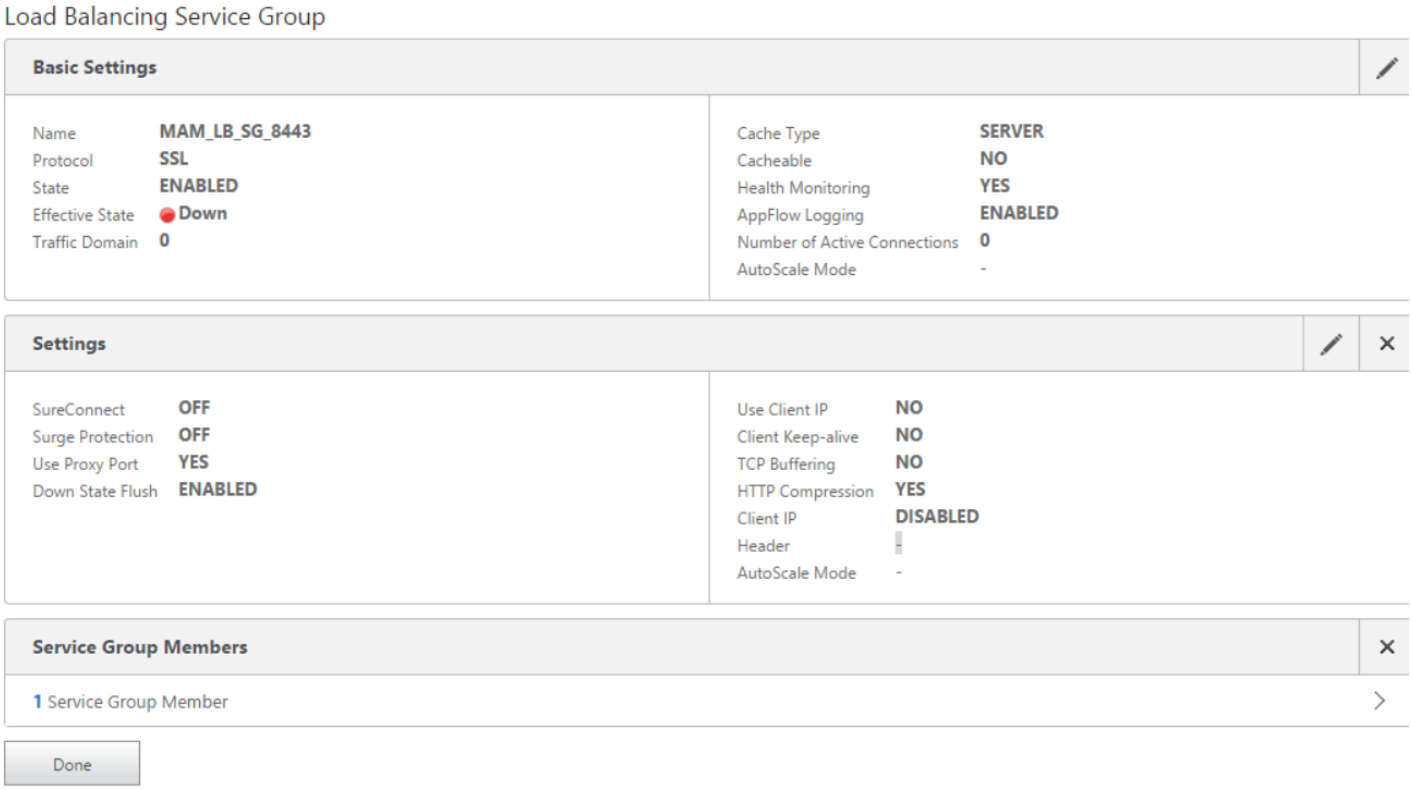
5. 输入 XenMobile 服务器 IP、端口 8443 和服务器 ID，然后单击 **Create**（创建）。



注意

- 可以在“Show Cluster Status”（显示群集状态）菜单项下从 XenMobile 10.1 CLI 获取服务器 ID。
- 如果存在多个 XenMobile 节点，请为每个节点重复此步骤，将每个节点都添加到 MAM_LB_SG_8443 服务组。

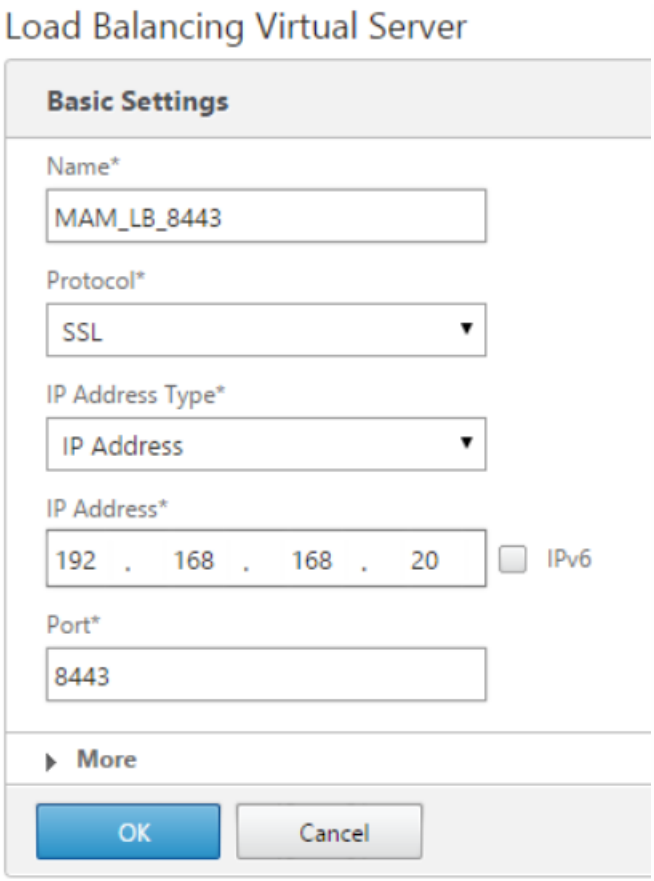
6. 单击 **Done**（完成）。



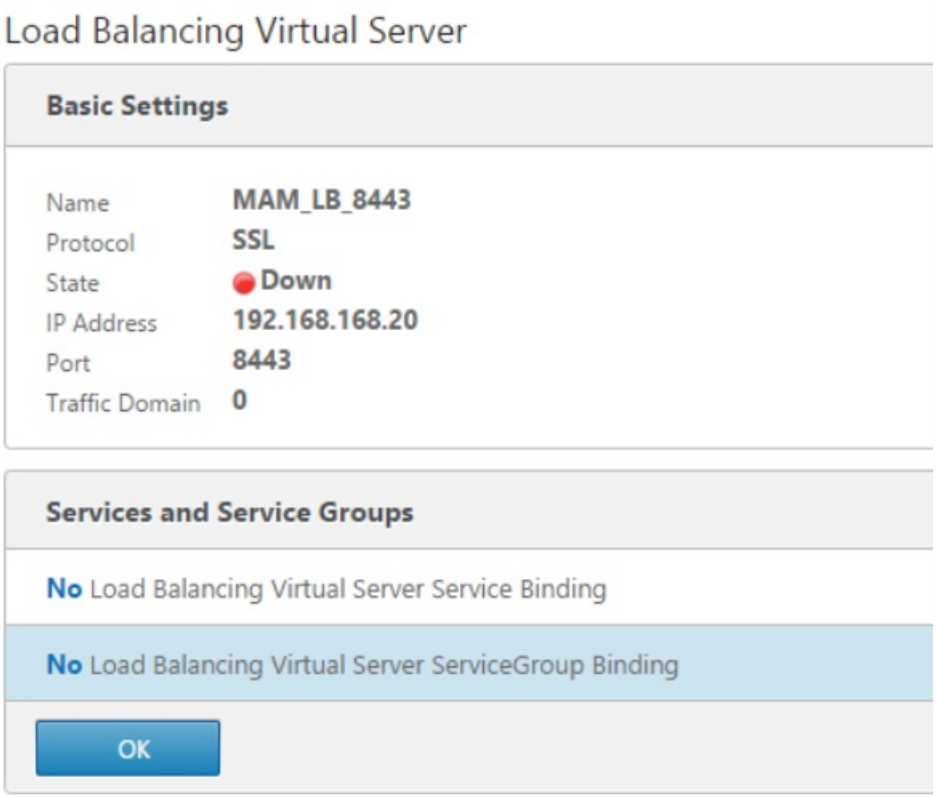
7. 单击 **Traffic Management**（流量管理）> **Load Balancer**（负载平衡器）> **Virtual Server**（虚拟服务器），然后单击 **Add**（添加）。

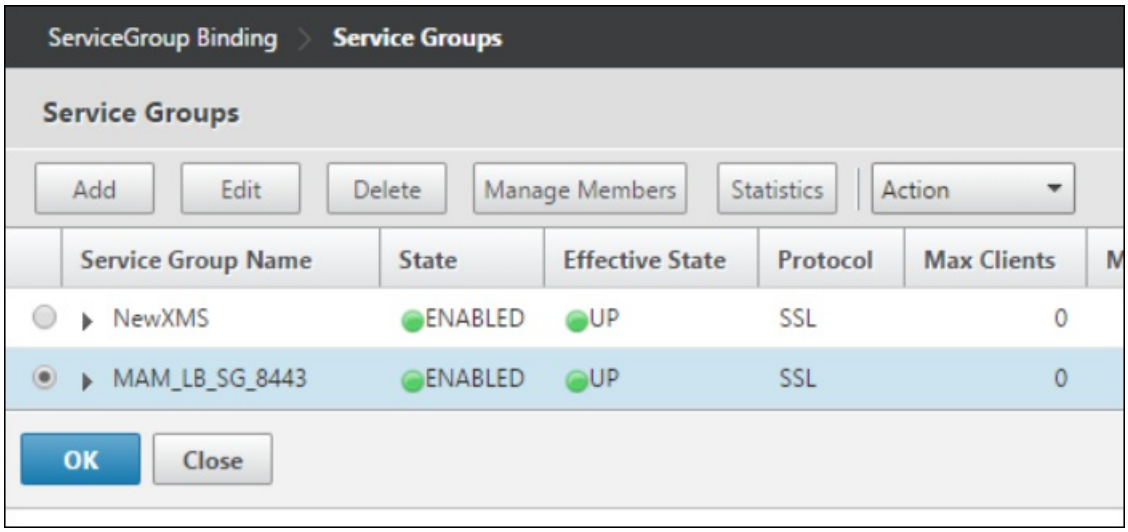
> **注意**
>
> 您创建此负载平衡器是为了将流量从 NetScaler Gateway 路由到 XenMobile 服务器节点。

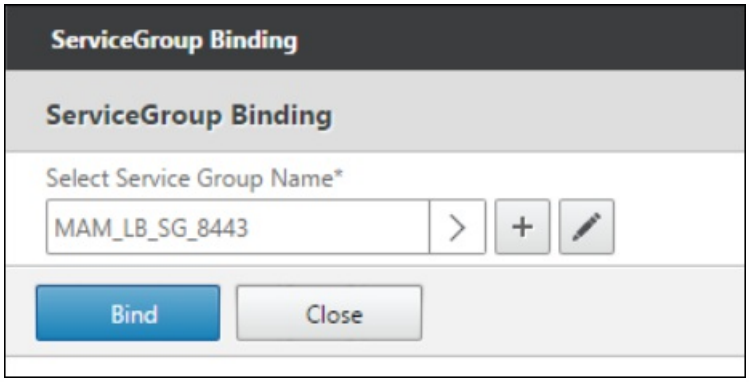
8. 键入 MAM 负载平衡器的名称、端口 8443 以及任何未使用的专用 IP 地址，如下图所示。



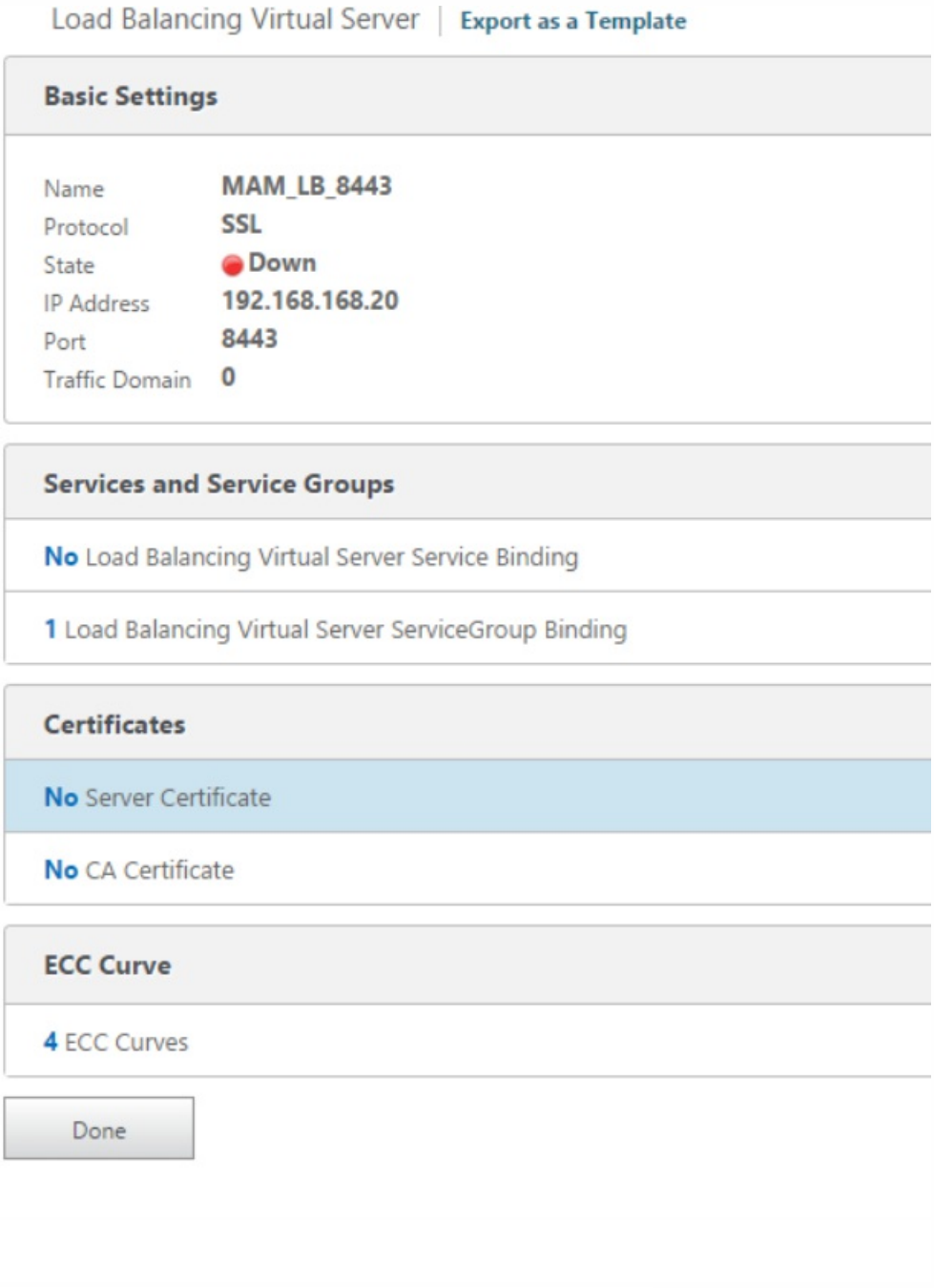
9. 单击 **No Load Balancing Virtual Server ServiceGroup Binding**（无负载平衡的虚拟服务器服务组绑定）以绑定服务组 MAM_LB_SG_8443，如下图所示。

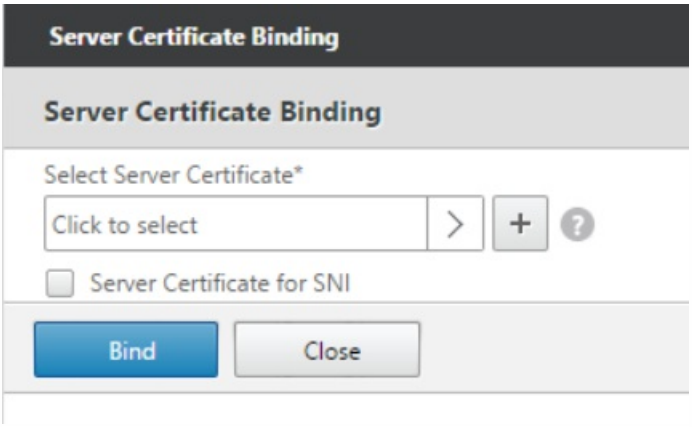


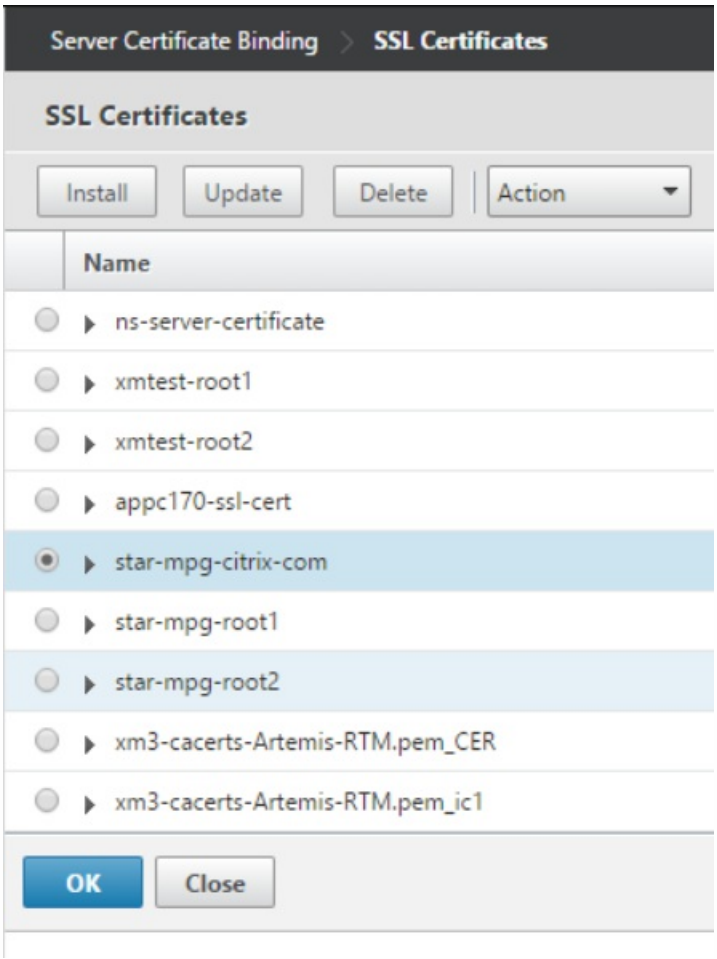


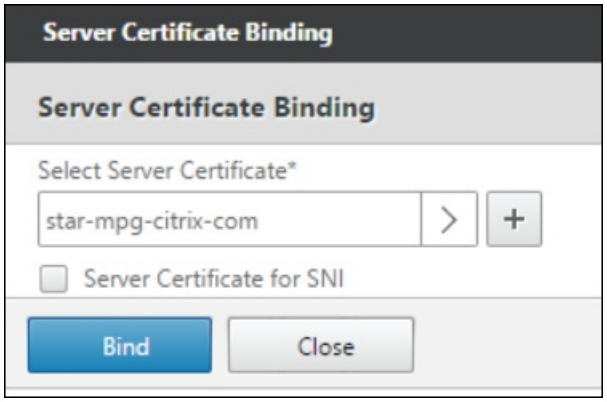


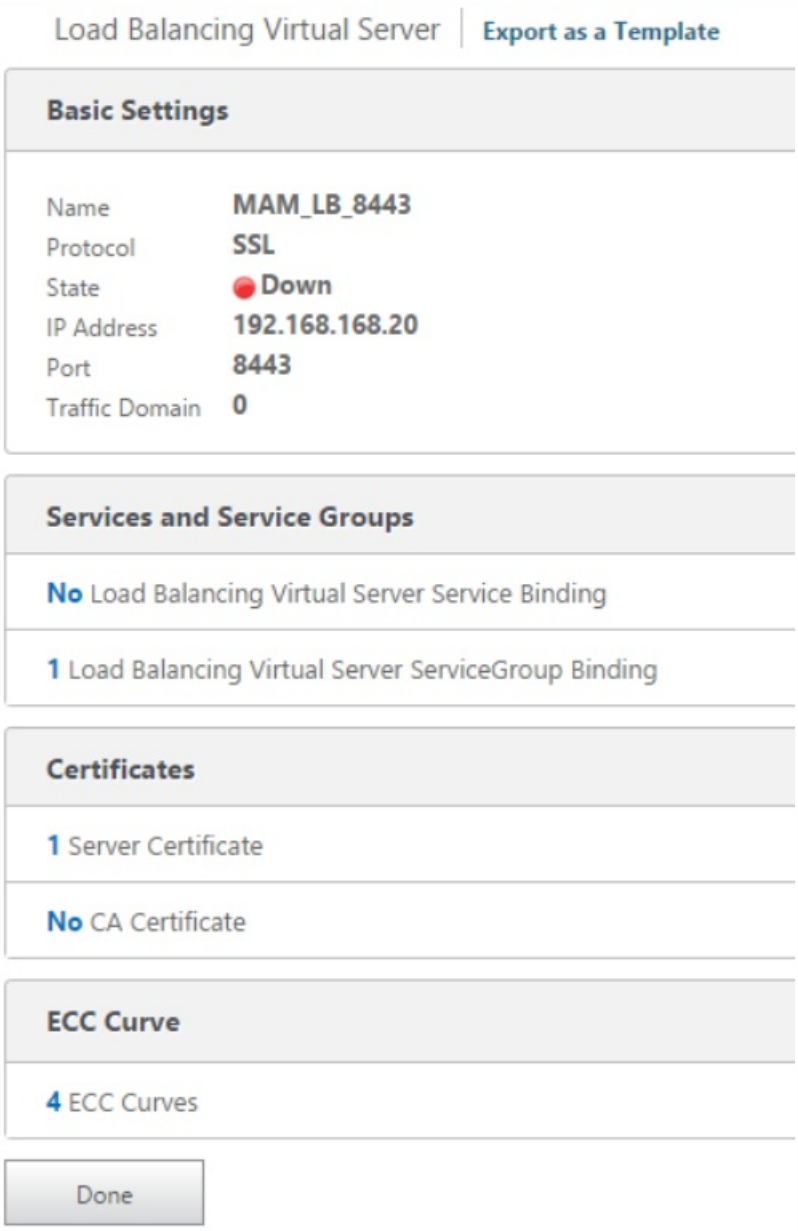
10. 将服务器证书绑定到 MAM_LB_8443 虚拟服务器，如下图所示。



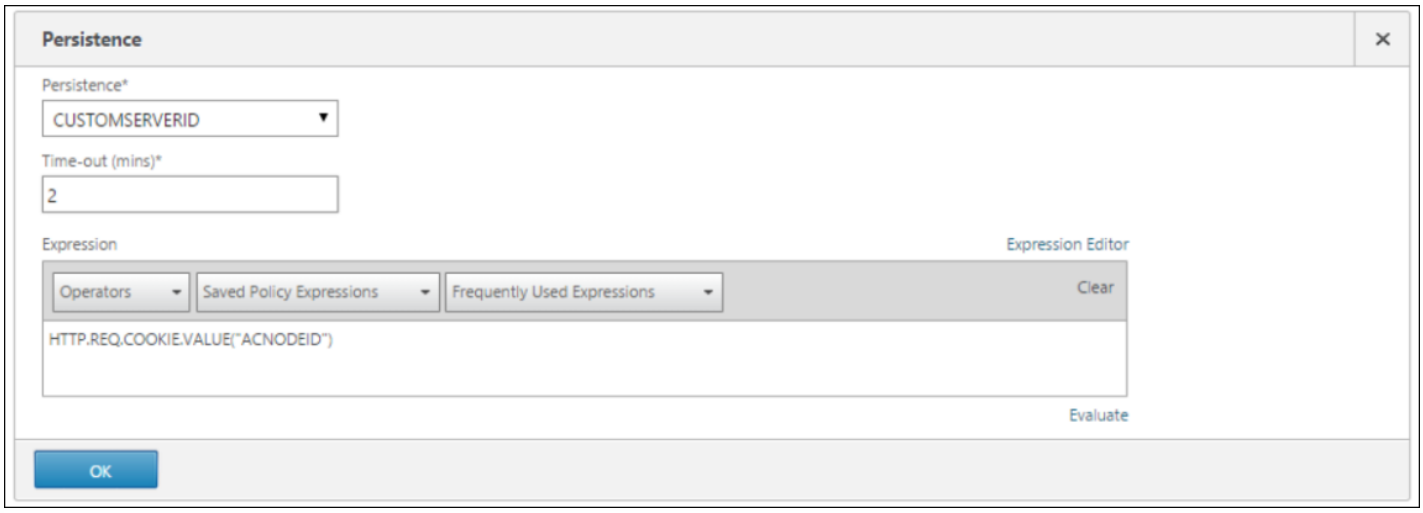






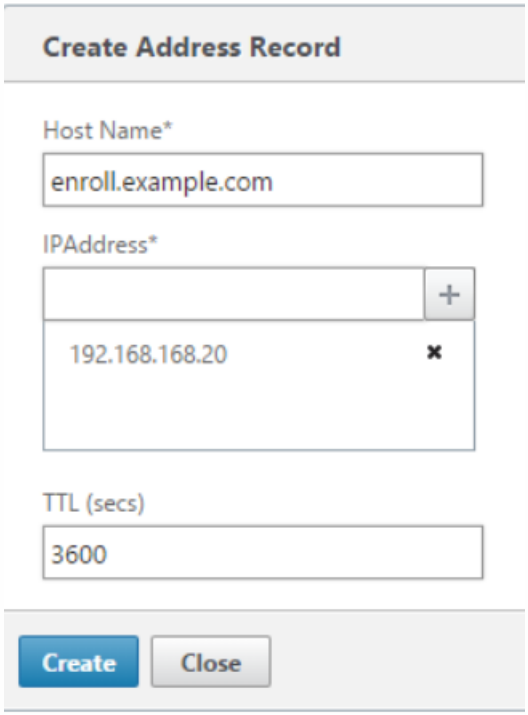


11. 在 **Persistence**（暂留）下的 **Persistence**（暂留）列表中，单击 **CUSTOMSERVERID**，然后在 **Expression**（表达式）字段中，键入 HTTP.REQ.COOKIE.VALUE("ACNODEID")，然后单击 **OK**（确定）。



12. 单击 **Traffic Management**（流量管理）> **DNS** > **Records**（记录）> **Address Records**（地址记录），为 XenMobile 10.1 服务器 FQDN 创建一条指向新 MAM_LB_8443 虚拟服务器的新地址记录。

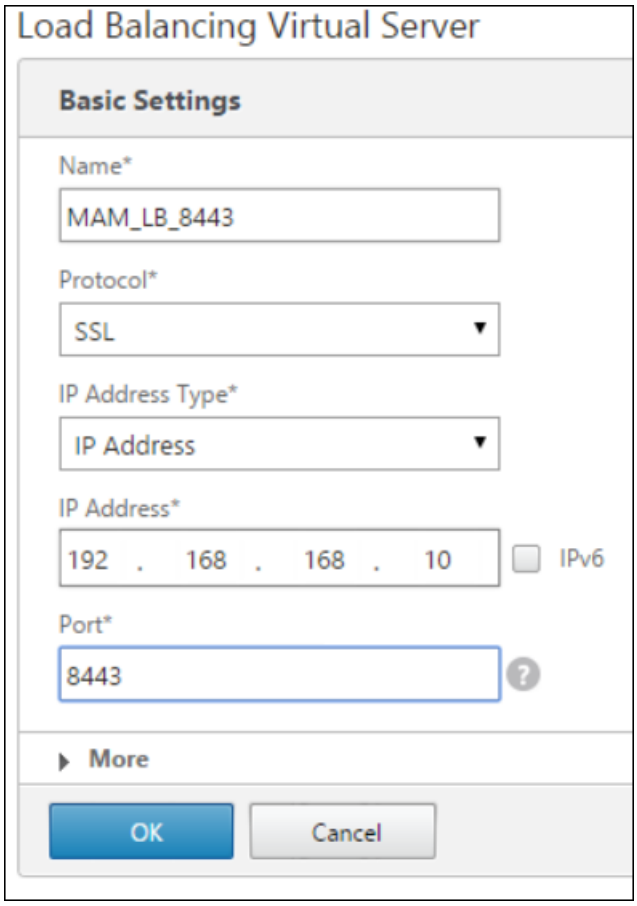
> **注意**
>
> XenMobile 10.1 服务器 FQDN为 enroll.example.com。



根据 SSL 卸载 MDM 配置创建新 MAM 负载平衡虚拟服务器

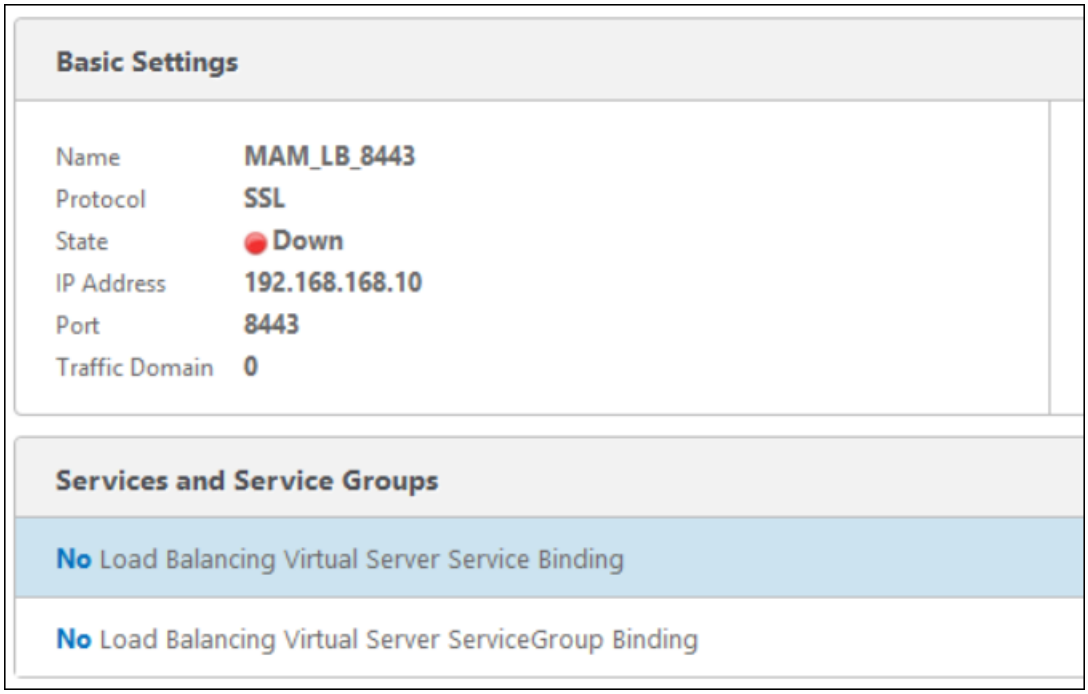
1. 单击 **Traffic Management**（流量管理）> **Load Balancer**（负载平衡器）> **Virtual Server**（虚拟服务器），然后单击 **Add**（添加）。

2. 键入 MAM 负载平衡器的名称、端口 8443 以及任何未使用的专用 IP 地址，如下图所示。



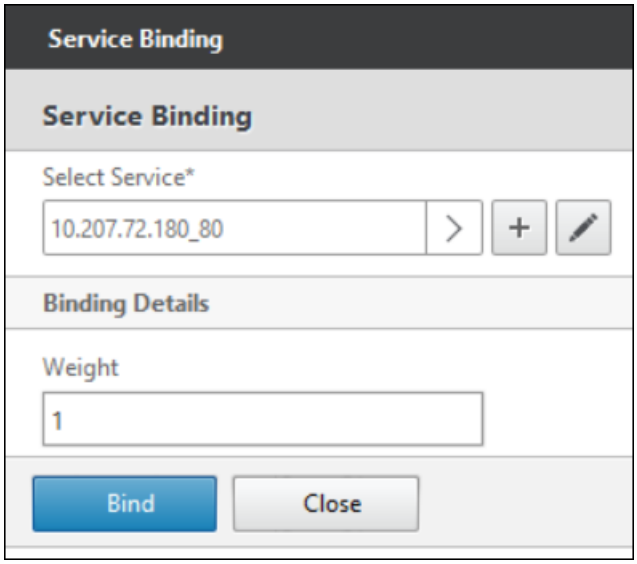
3. 单击 **OK**（确定）。

4. 单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡的虚拟服务器服务绑定）以绑定服务组 MAM_LB_8443 虚拟服务器，如下图所示。

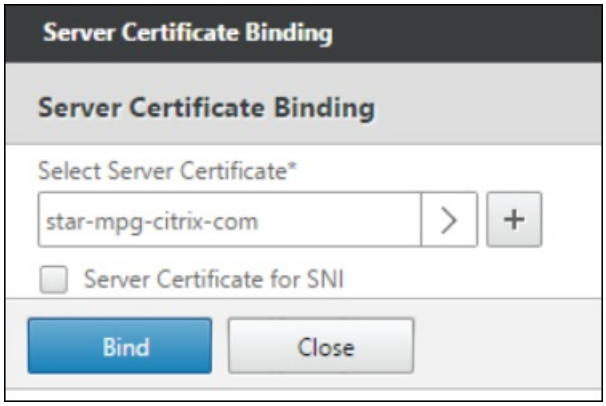


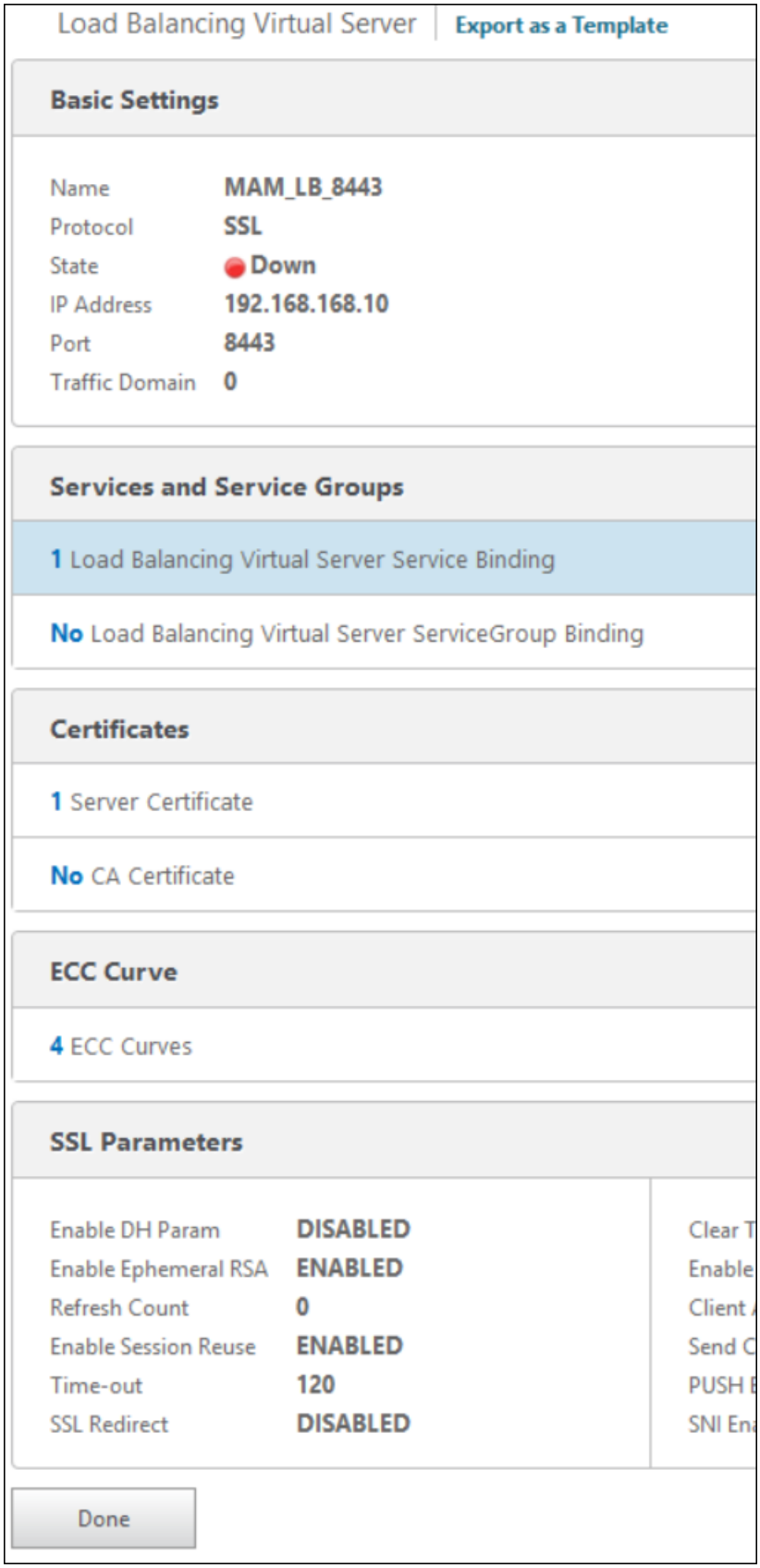
注意

由于此服务已使用 MDM 负载平衡向导配置，因此将显示此服务。

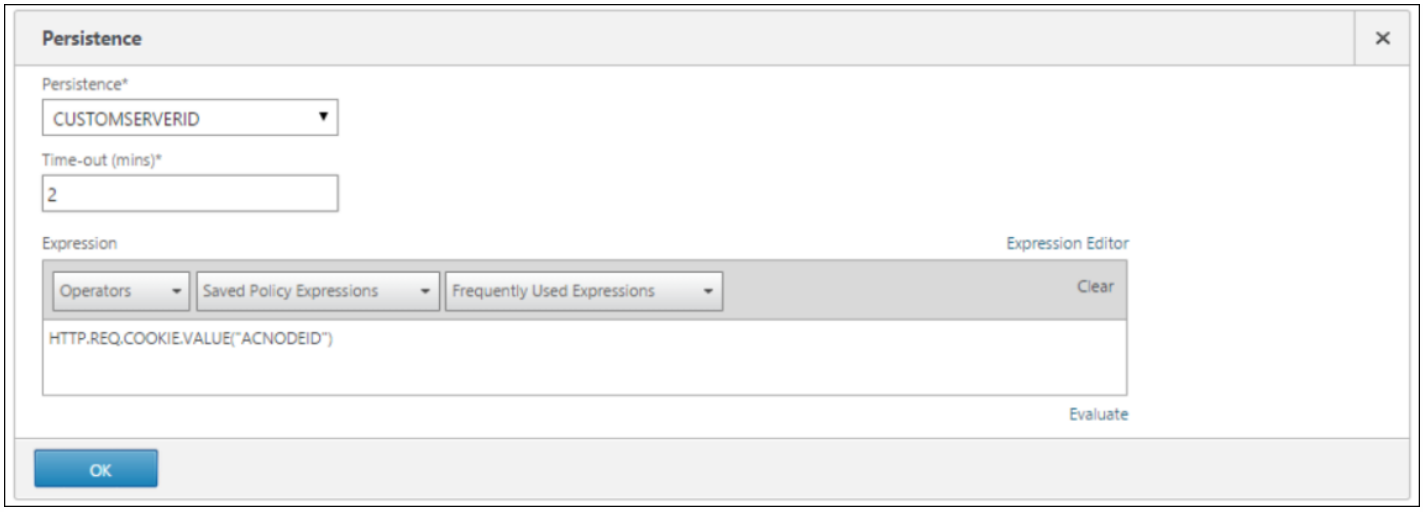


5. 将服务器证书绑定到 MAM _LB_8443 虚拟服务器（如下图所示），然后单击 **Done**（完成）。



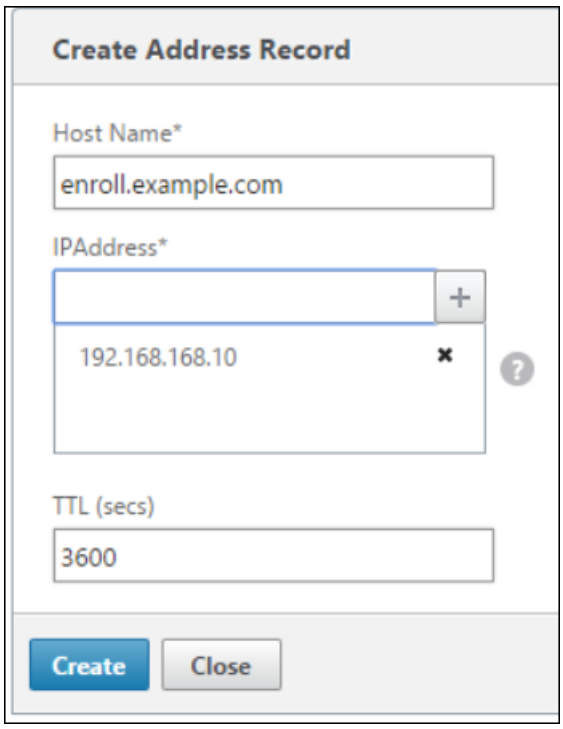


6. 在 **Persistence**（暂留）下的 **Persistence**（暂留）列表中，单击 **CUSTOMSERVERID**，然后在 **Expression**（表达式）字段中，键入 HTTP.REQ.COOKIE.VALUE(“ACNODEID”)。



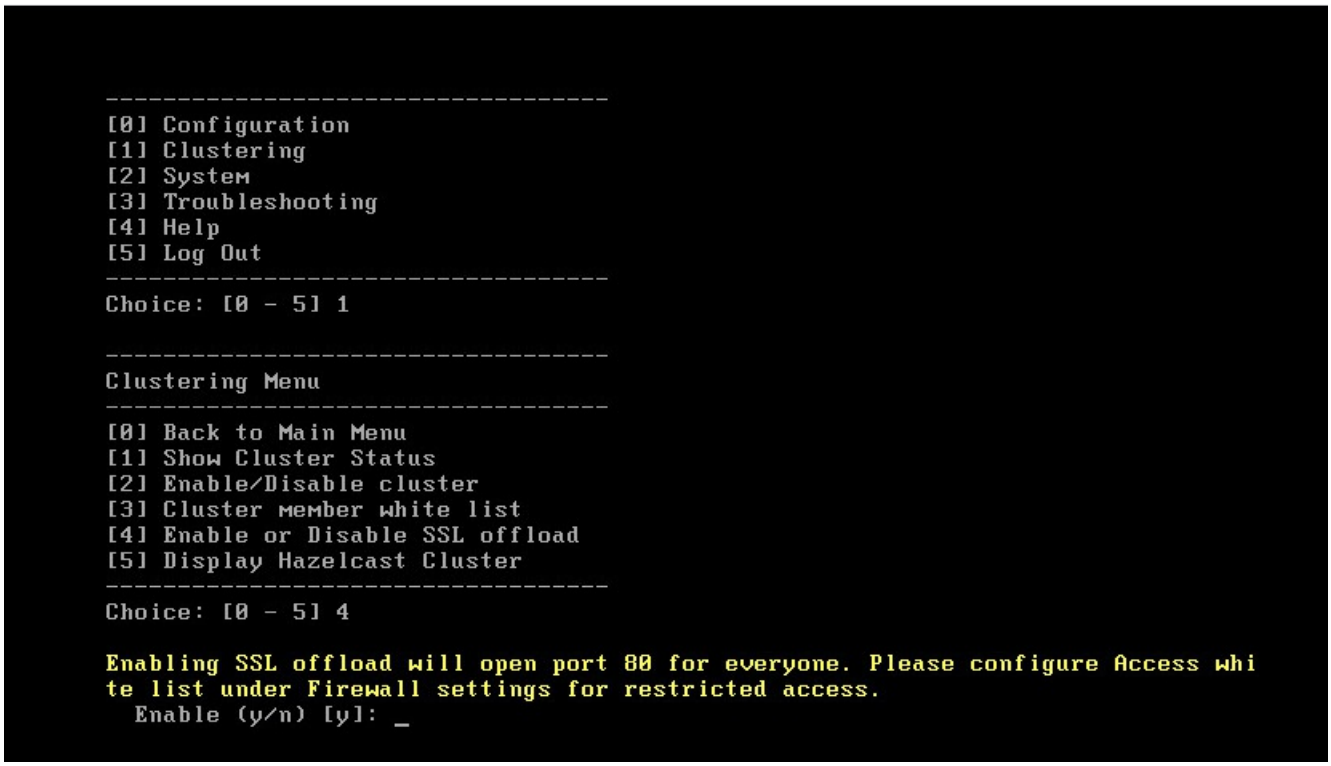
7. 为 XenMobile 服务器 FQDN 创建一条指向新 MAM 负载平衡虚拟服务器的地址记录。

8. 单击 **Traffic Management**（流量管理）> **DNS** > **Records**（记录）> **Address Records**（地址记录），然后单击 **Add**（添加），为 XenMobile 10.1 服务器 FQDN 创建一条指向新 MAM 负载平衡虚拟服务器的新地址记录。



> **注意**
>
> XenMobile 10.1 服务器 FQDN为 enroll.example.com。

9. 如果要使用 SSL 卸载，请在命令行接口中，为 SSL 卸载启用端口 80。



在 NetScaler Gateway 上重新配置 STA

在 NetScaler Gateway 中，还需要添加运行 STA 的服务器的 IP 地址或 FQDN。为此，请遵循以下步骤：

1. 单击 **Netscaler Gateway**。
2. 单击 **Virtual Servers**（虚拟服务器）。
3. 选择已配置的 Netscaler Gateway 虚拟服务器，然后单击 **Edit**（编辑）。
4. 在 **Published Applications**（已发布的应用程序）下，单击 **STA server**（STA 服务器）。
5. 记下 URL，然后从列表中选择 Secure Ticket Authority 服务器。
6. 单击 **Unbind**（取消绑定），然后单击 **Add Binding**（添加绑定）。
7. 在 **Secure Ticket Authority Server**（Secure Ticket Authority 服务器）字段中，键入在步骤 5 中记下的 URL。
8. 依次单击 **Bind**（绑定）、**Close**（关闭）和 **Done**（完成）。

NTP 设置

务必同步 NetScaler 和 XenMobile 服务器上的时间。 如有可能，请将 NetScaler 和 XenMobile 服务器指向同一个公用网络时间协议 (NTP) 服务器。

群集

如果在群集中部署了 XenMobile 10.1，则必须使用 CLI 启用群集支持，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 10.1 实例，来重新使用 XenMobile 9.0 的节点 IP 地址，并将其加入到最旧的（管理员）节点。

更新未迁移的信息

根据需要进行如下更新：

- 托管服务提供程序 (MSP) 组
- 自定义 Active Directory 属性
- RBAC 角色
- 日志设置
- migration.log 文件中列出的所有配置或用户数据
- 任意系统日志服务器配置
- 对于本地迁移，会迁移 RBAC 角色，但存在已知问题。

WorxStore 自定义应用商店名称后置条件

升级之前，其中一个必备步骤是解决此问题：

> WorxStore 已知问题：在从 XenMobile 9 升级到 XenMobile 10.1 之前，如果 WorxStore 使用的是自定义名称，则进行注册以及访问 Worx Home 和 Worx Store 时会出现问题。 解决方法为，在升级前将应用商店更改为默认设置（应用商店）。 [#619458]

如果未完成该必备操作，则必须在使用 XenMobile 服务器 10.1 之前按照以下后续必备步骤之一进行操作：

- 如果您的 Windows 设备数量庞大，请将应用商店名称更改为默认值。 之后，使用 iOS 和 Android 设备注册的最终用户必须从 WorxHome 注销，然后重新登录。
- 如果您的 Windows 设备数量少于 iOS 和 Android 设备，建议请 Windows 用户重新注册其设备。

有关此问题的详细信息，请参阅 http://support.citrix.com/article/CTX214553。

回滚 XenMobile 升级

Oct 13, 2016

将 XenMobile 9 升级到 XenMobile 10.1 后，某些客户报告访问 WorxStore 、打开应用程序以及使用其他功能时会遇到问题。 Citrix 以前提供了如何临时回滚升级的说明。 当前建议为*不*尝试回滚升级。

将 MTC 租户服务器升级到 XenMobile 10.1

Aug 04, 2016

如果在 XenMobile 9.0 上启用了多租户控制台 (MTC)，现在可以将 MTC 托管的 XenMobile 9 实例迁移到独立的 XenMobile 10 实例。 XenMobile 10 不支持 MTC，因此，必须基于各个实例管理这些升级后的实例。

1. 确保在所有 MTC 客户端的前端配置网络地址转换 (NAT)。

2. 安装 XenMobile 10 的实例。

3. 如果未对 MTC 租户启用任何端口映射，请执行下列操作：

    a. 确保允许使用证书进行 HTTPS 通信的 XenMobile 10 服务器端口（通常为端口 443）和允许不使用证书进行 HTTPS 通信的 XenMobile 10 服务器端口（端口 8443）与用于 XenMobile 实例的端口匹配。

    b. 配置新的管理端口。

    c. 启用端口映射后，请使用所映射到的端口，而非 XenMobile 服务器所侦听的端口。

4. 对于实例名称，请使用 zdm。

5. 在 XenMobile 服务器设置期间，当提示确认是否要升级时，请选择**是**。

6. 从要用于升级的服务器上的目录中复制以下文件：C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\webapps\"tenant name"\WEB-INF\classes

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

7. 从此目录中复制以下文件：C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\"tenant name"

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

8. 复制并修改此文件：C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xml

9. 在 server.xml 文件中删除其他租户正在使用的所有端口连接器。 可以保留端口 80。

10. 在使用的端口连接器上，从以下范围内的所有文件路径中删除实例名称：

keystoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\"tenant name"\https.p12

更改为：

keystoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\https.p1

11. 对以下范围内的文件路径重复步骤 10：

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\"tenant name"\cacerts.pem.jks"

更改为：

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\cacerts.pem.jks"

12. 创建一个 .zip 文件，其中包含在步骤 10 和 11 中更改的文件。

13. 打开 https://10.215.199.42:1433/uw/?cloudMode，其中 IP 地址后跟使用证书建立 HTTPS 连接所使用的端口。

14. 打开升级文件夹。

15. 安装 63110upgrade.bin 文件。

16. 选择 MDM，然后在后续屏幕中一直单击**下一步**，直至提示选择 .zip 文件。

17. 确保数据库正确无误，并输入 CA 证书的密码，然后单击两次**下一步**。

18. XenMobile 服务器重新启动后，使用 XenMobile 服务器的 IP 地址（后跟管理端口号）登录到 XenMobile 控制台。

19. 在 XenMobile 控制台中，安装新许可证。

20. 更改 NAT，以指向新的服务器。

21. 根据需要更改防火墙设置，以允许 XenMobile 服务器使用的端口。

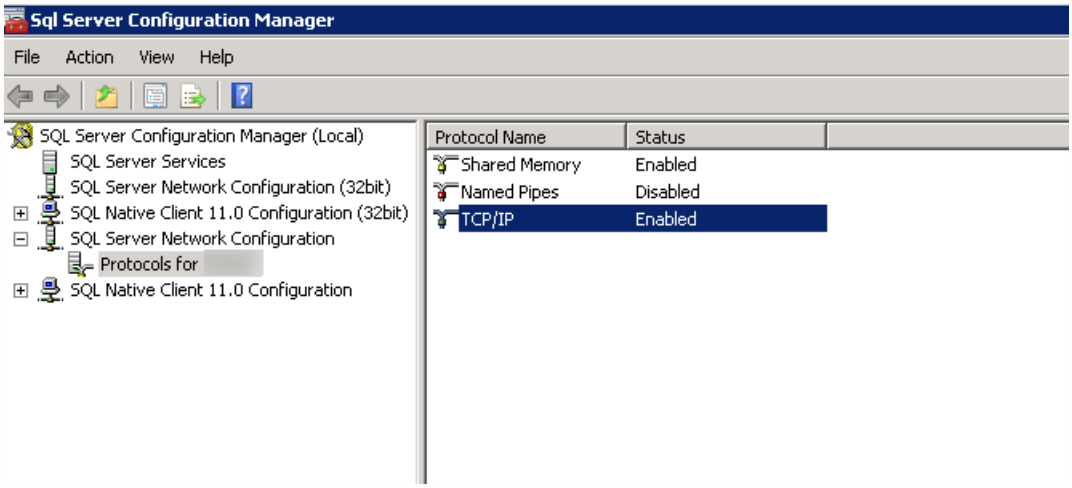
支持命名 SQL 实例

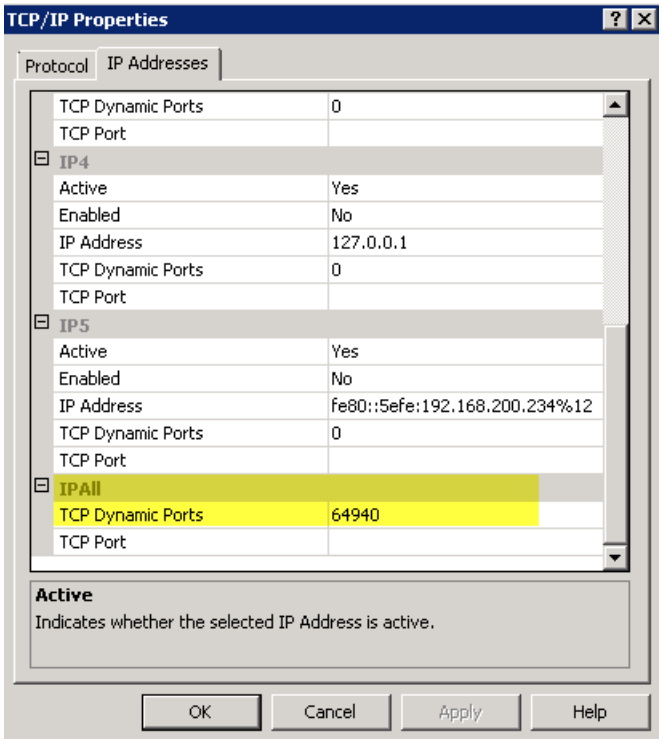
Apr 22, 2016

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

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

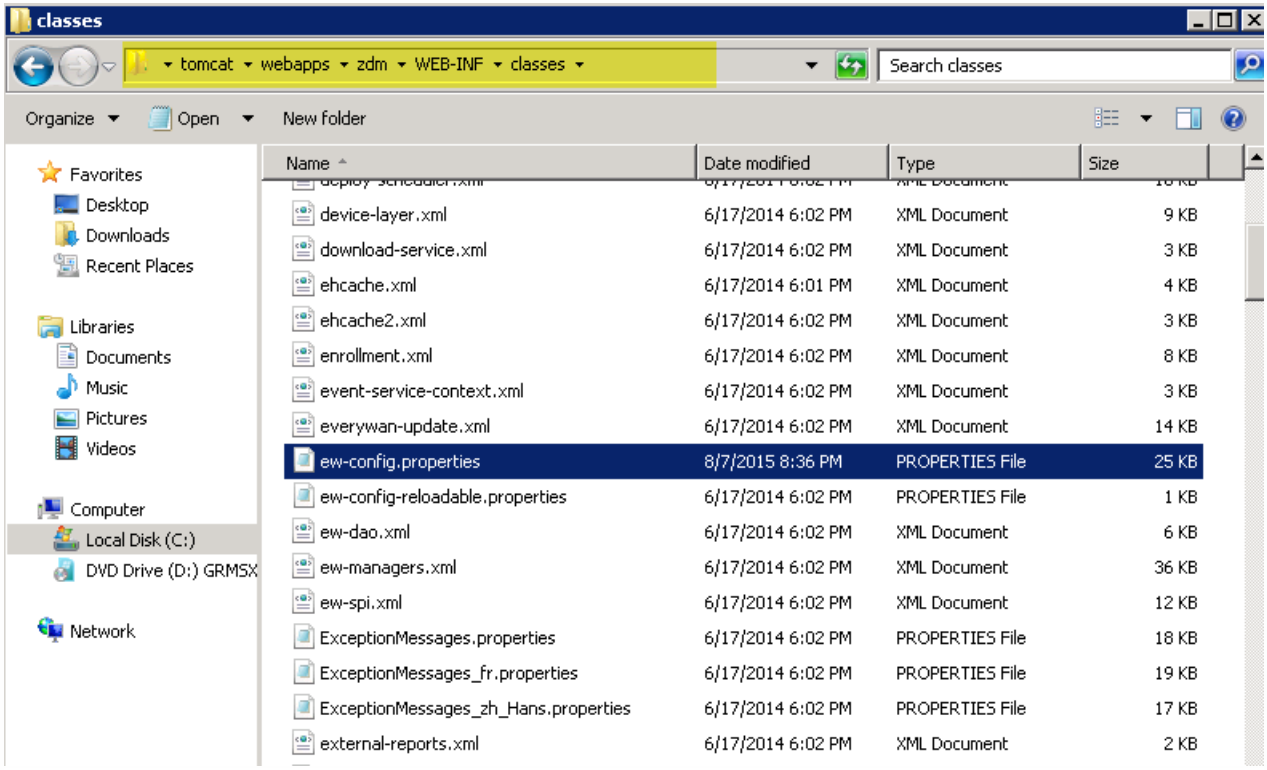
> **注意**
>
> Citrix 建议 SQL Server 数据库实例始终在静态端口上运行，因为 XenMobile 服务器需要继续访问该数据库。此连接通常通过防火墙遍历。因此，您需要在防火墙中打开恰当的端口，并且需要在静态端口上运行数据库实例。





升级包含 SQL Server 命名实例的 XenMobile 的步骤

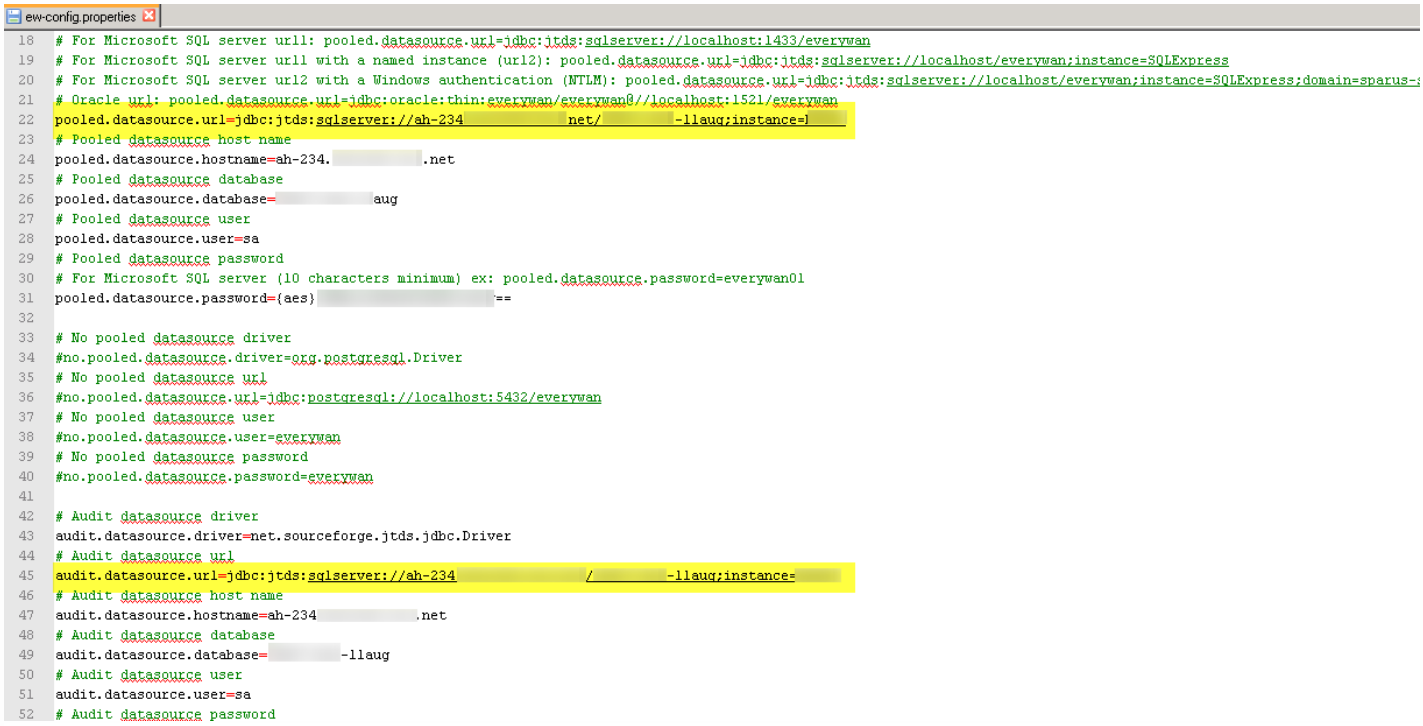
1. 转至 Device Manager 安装目录并打开 ew-config.properties 文件。此文件位于 tomcat\webapps\zdm\WEB-INF\classes 中。



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/

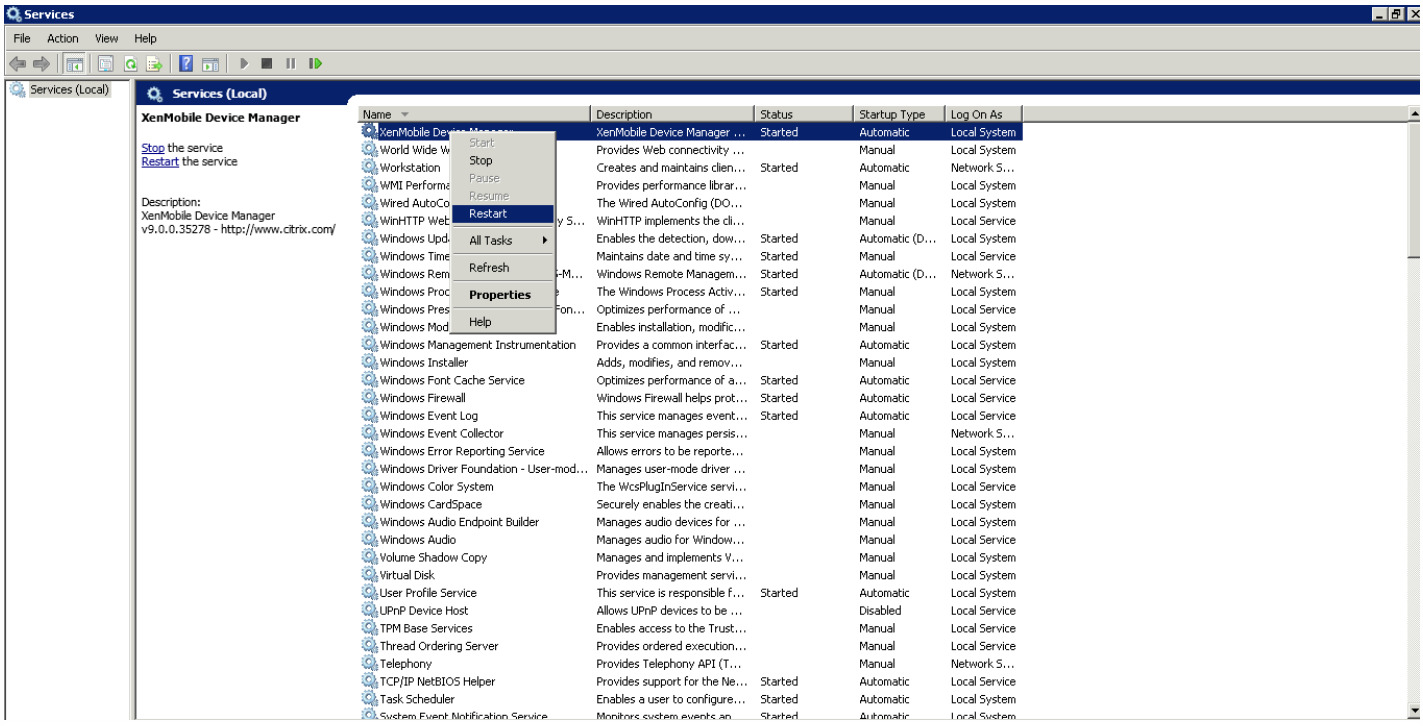
如果用户帐户属于某个域，请将“;domain=”添加到 URL 的结尾。

> ## 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。

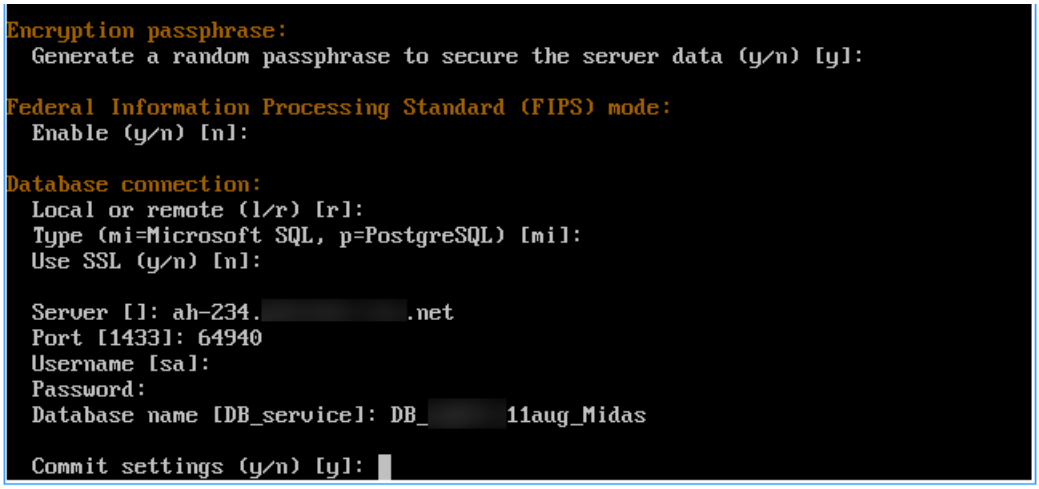
ew-config.properties

```
# 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，可使用 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。

为 XenMobile 10 配置群集

Aug 04, 2016

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

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

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

必备条件

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

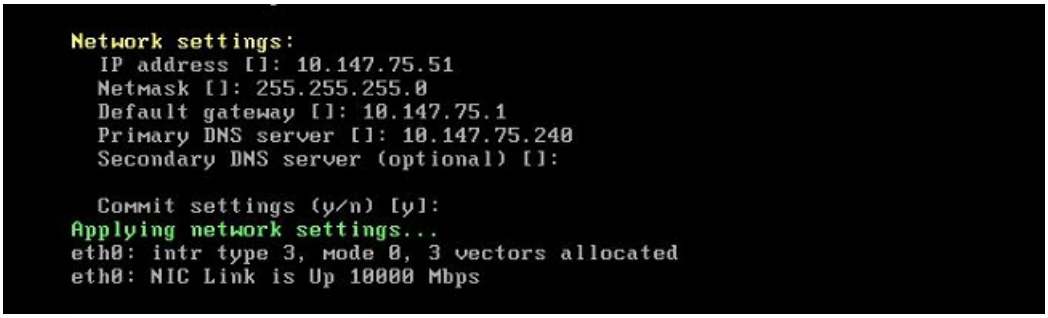
有关群集配置中 XenMobile 10.x 的参考体系结构图，请参阅体系结构概述。

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。

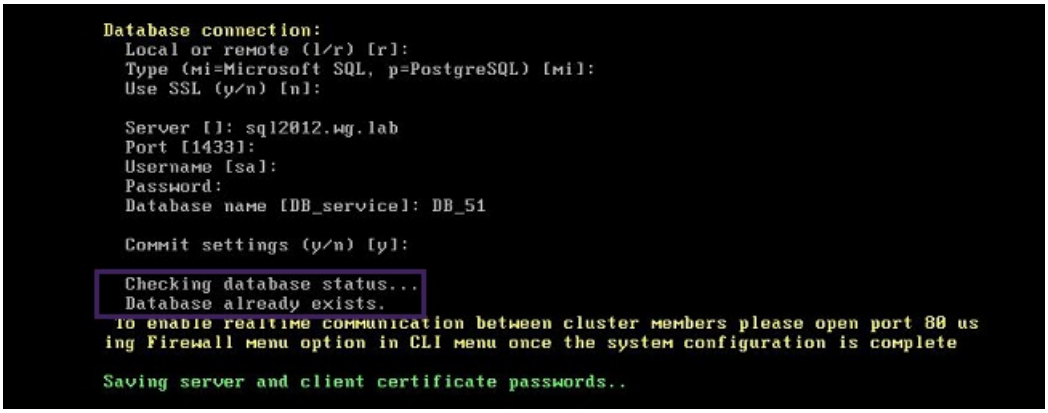
2. 提供网络配置详细信息，如下图所示。



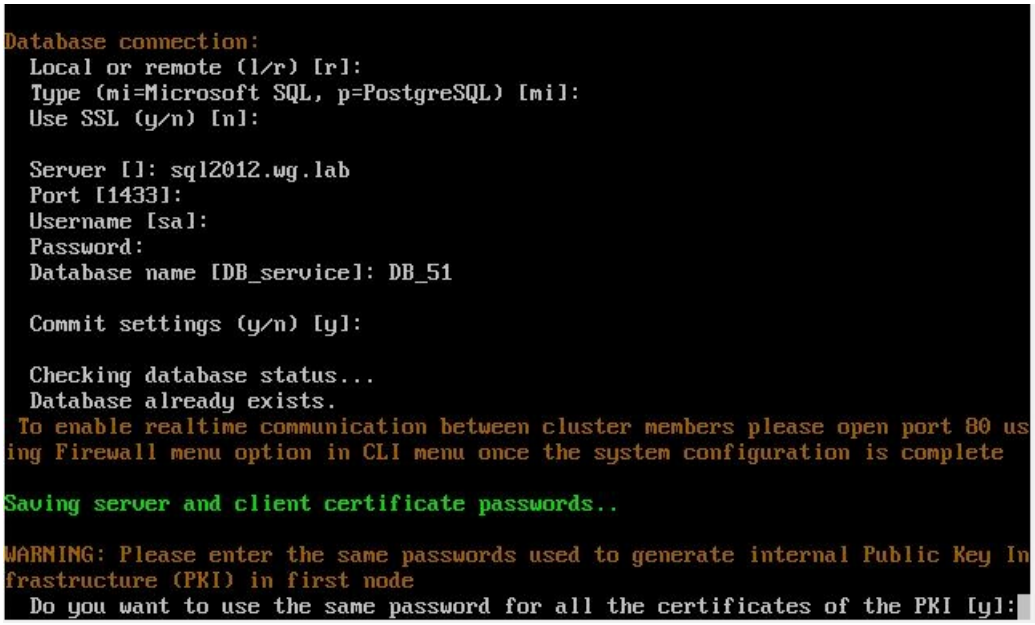
3. 如果希望使用数据保护的默认密码，请键入y；否则，请键入n 并输入新密码。

4. 如果要使用 FIPS，请键入y；否则，请键入n。

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

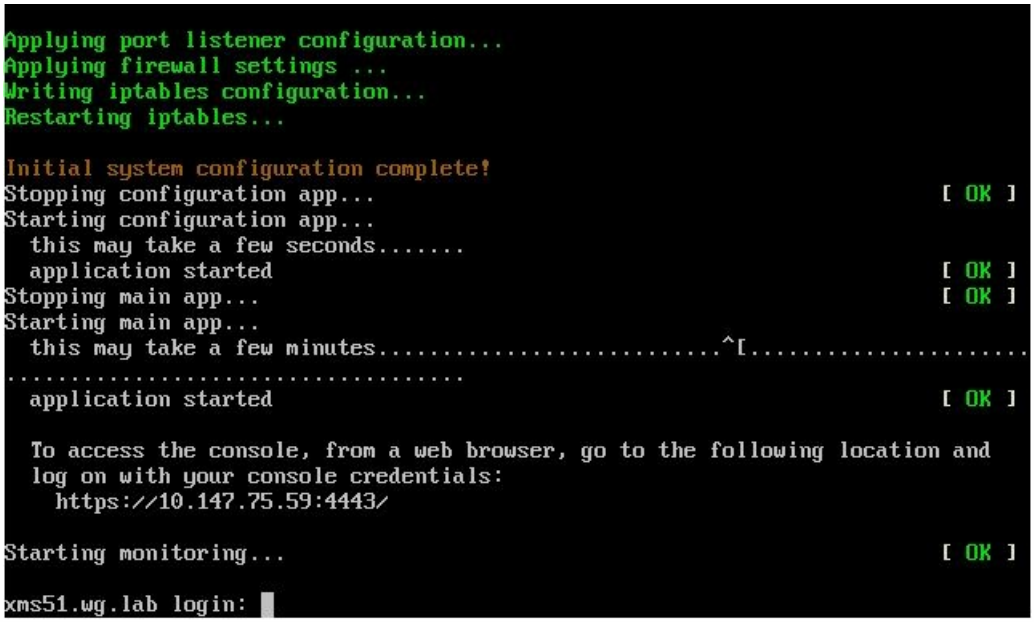


6. 输入与为第一个 VM 提供的证书相同的密码。



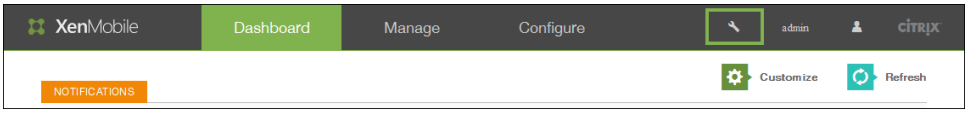
输入密码后，第二个节点上的初始配置将完成。

7. 配置完成后，服务器重新启动并显示登录对话框。

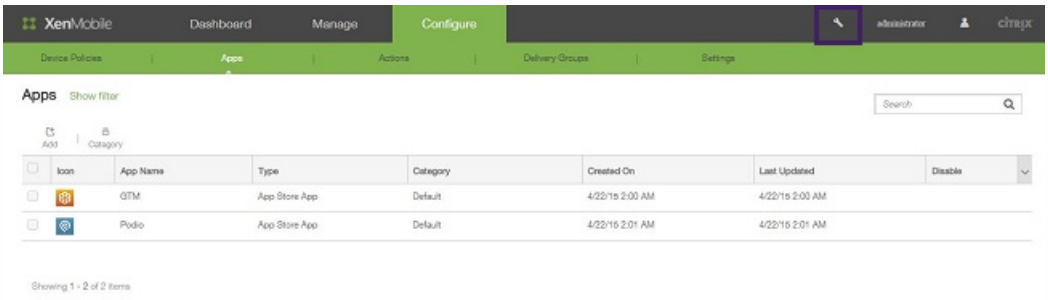


注意：登录对话框与第一个 VM 的登录对话框相同。这种相同是供您确认两个 VM 使用相同的数据库服务器的一种途径。

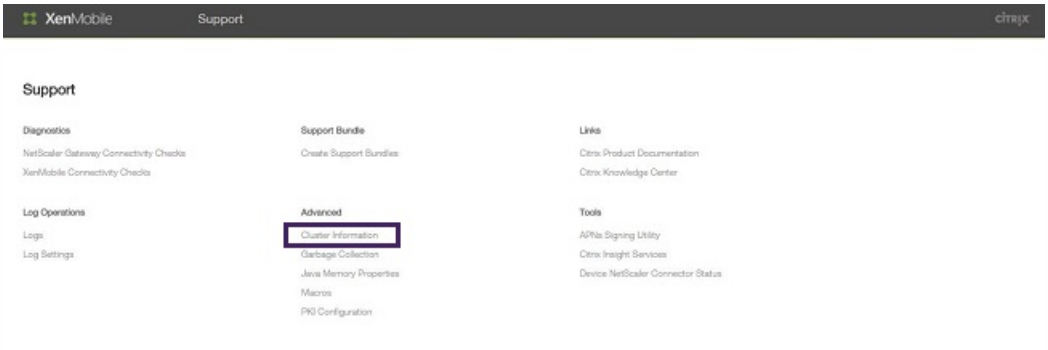
8. 使用 XenMobile 的完全限定的域名 (FQDN) 在 Web 浏览器中打开 XenMobile 控制台。
9. 在控制板上，单击屏幕右上角的工具图标。



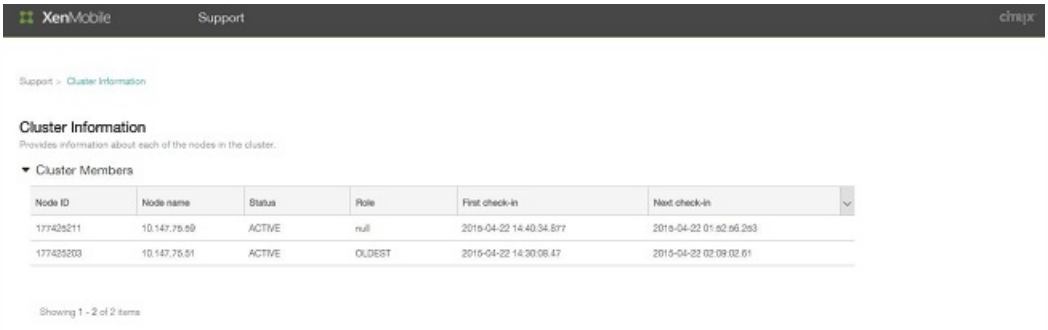
此时将打开“支持”页面。



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。



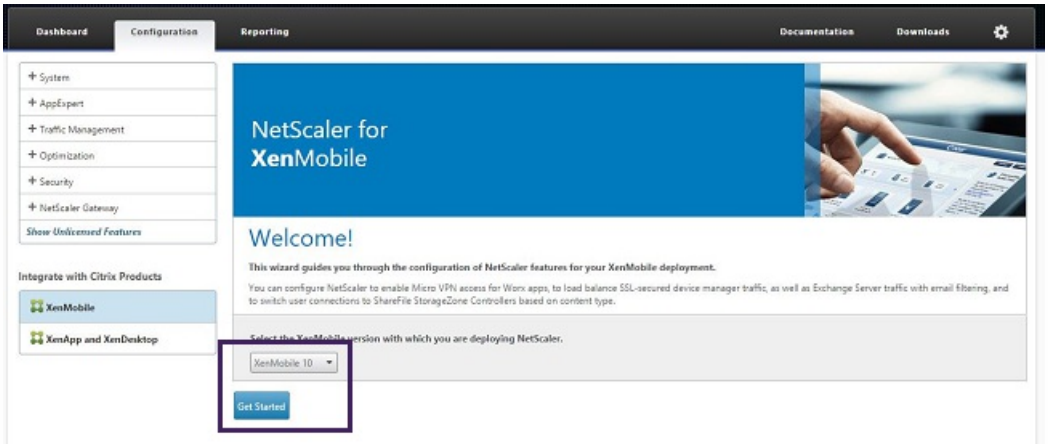
新节点现在属于群集的成员。您可以按照相同的步骤添加其他节点。

在 NetScaler 中为 XenMobile 群集配置负载平衡

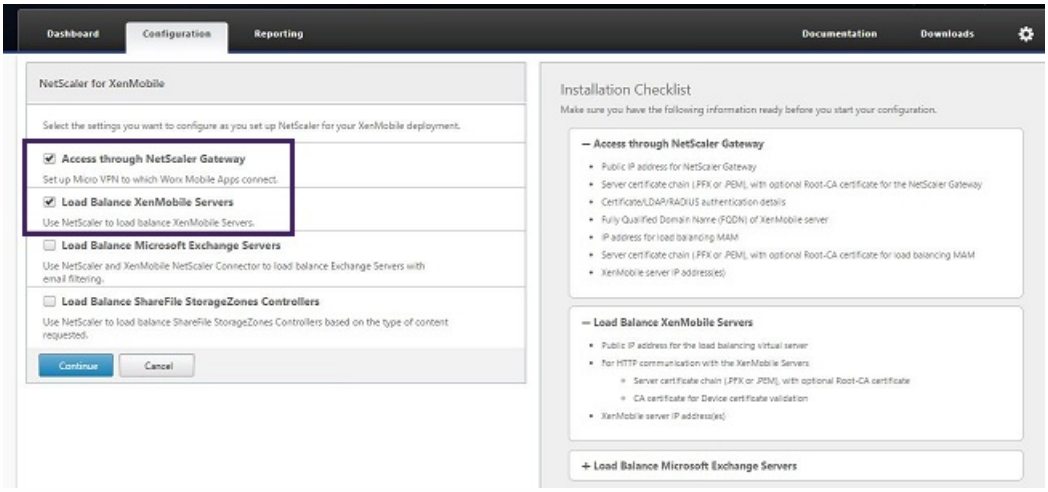
将所需的节点作为成员添加到 XenMobile 群集中后，需要对节点进行负载平衡才能访问群集。负载平衡通过运行 NetScaler 10.5.x 中提供的 XenMobile 向导完成。您可以通过运行此向导，按照本过程中的步骤对 XenMobile 进行负载平衡。

1. 登录 NetScaler。

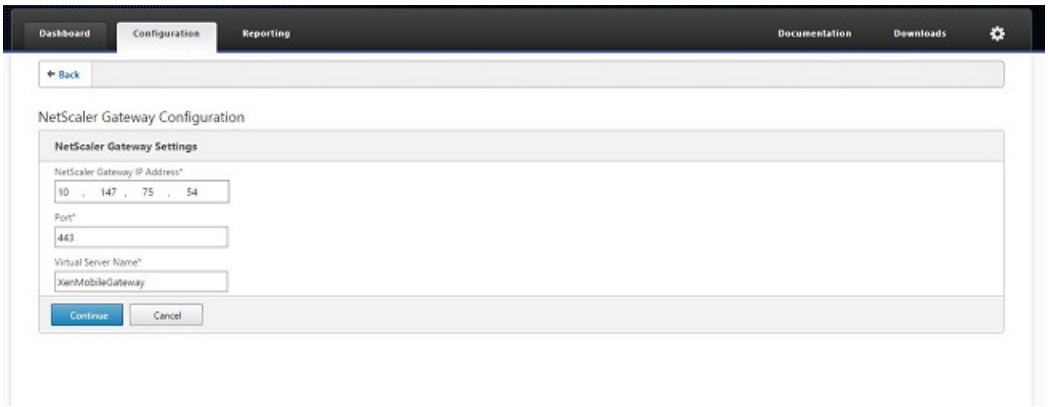
2. 在 Configuration（配置）选项卡上，单击 XenMobile，然后单击 Get Started（开始）。



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）。

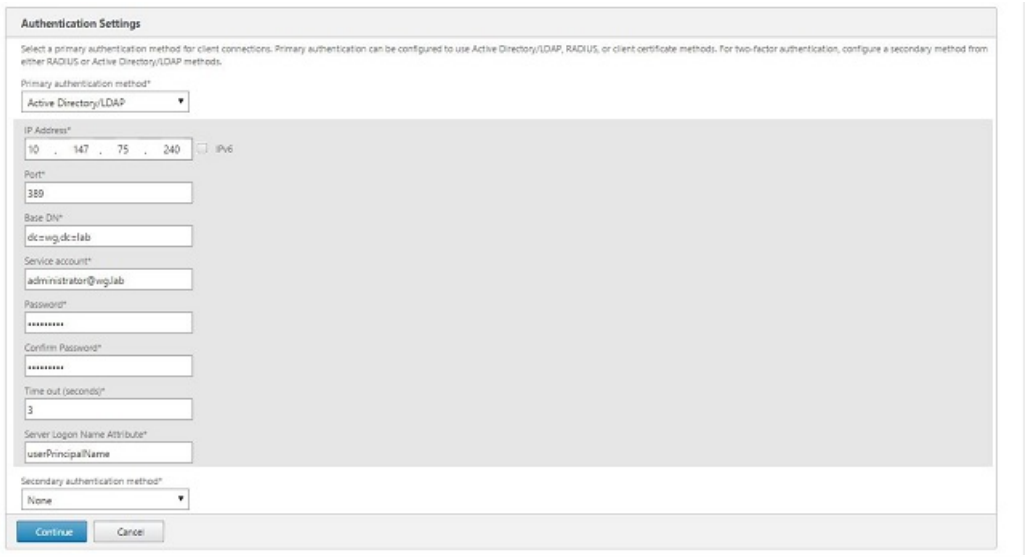


4. 输入 NetScaler Gateway 的 IP 地址，然后单击 Continue（继续）。



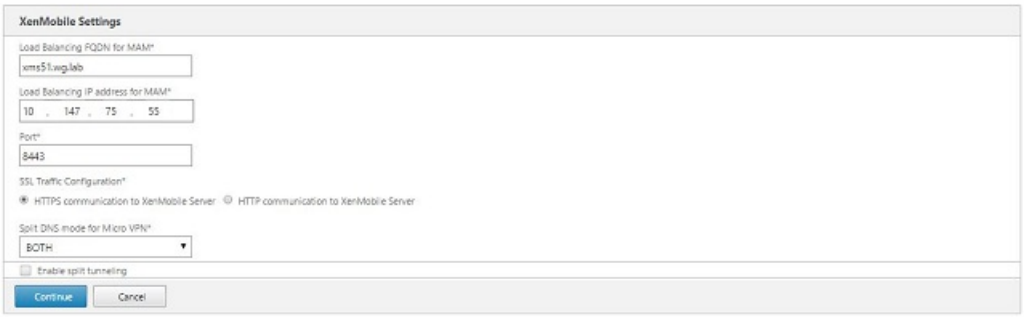
5. 通过执行以下操作将服务器证书绑定到 NetScaler Gateway 虚拟 IP 地址，然后单击 Continue（继续）。
   - 在 Use existing certificate（使用现有证书）中，从列表中选择服务器证书。
   - 单击 Install Certificate（安装证书）选项卡以上载新的服务器证书。

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）。

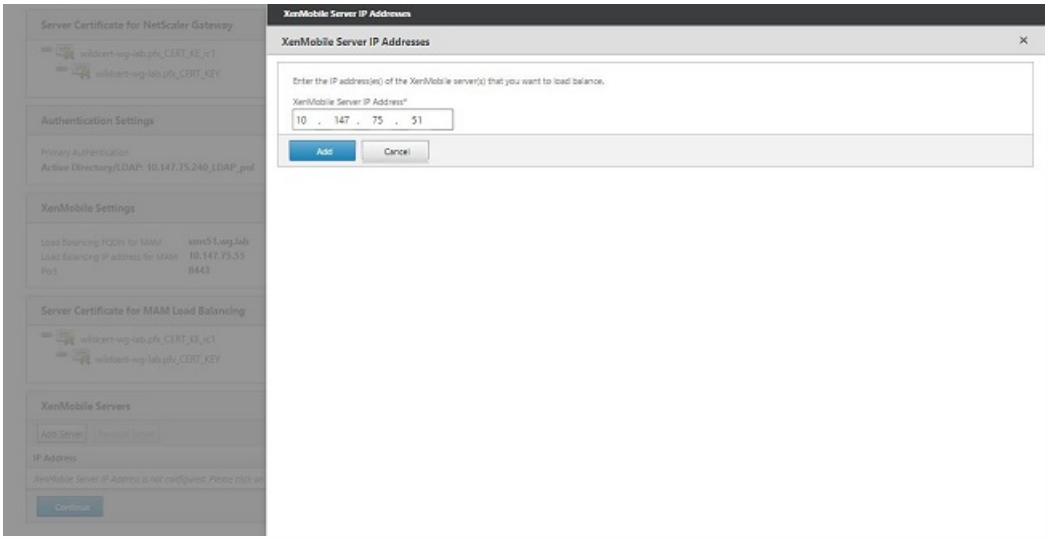


注意：确保 MAM 负载平衡虚拟 IP 地址的 FQDN 与 XenMobile 的 FQDN 相同。

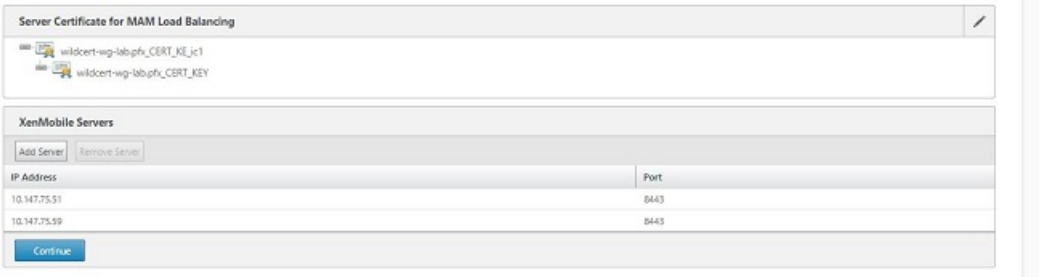
8. 如果使用 SSL 桥接模式 (HTTPS)，请选择 HTTPS communication to XenMobile Server（与 XenMobile 服务器进行 HTTPS 通信）。 但是，如果要使用 SSL 卸载，请选择 HTTP communication to XenMobile Server（与 XenMobile 服务器进行 HTTP 通信），如上图所示。为实现本文的目的，请选择 SSL 桥接模式 (HTTPS)。
9. 绑定 MAM 负载平衡虚拟 IP 地址的服务器证书，然后单击 Continue（继续）。

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。

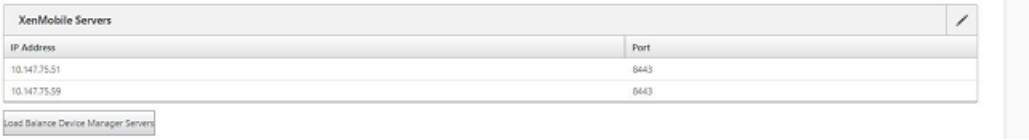
11. 输入 XenMobile 节点的 IP 地址，然后单击 Add（添加）。



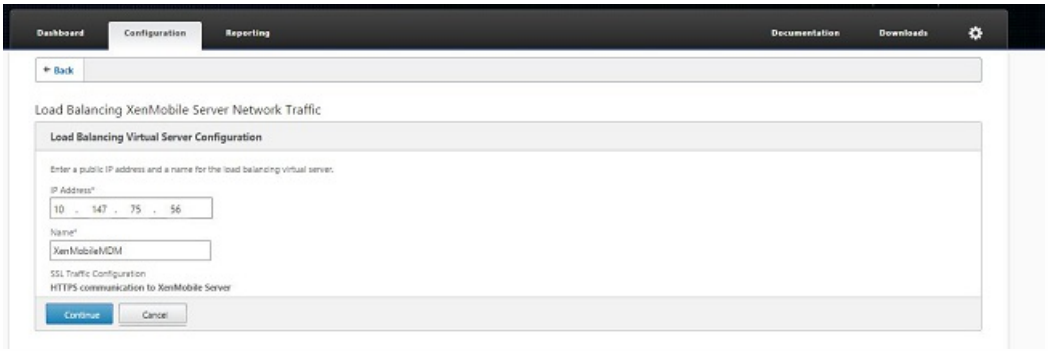
12. 重复步骤 10 和 11 以添加其他 XenMobile 节点，作为 XenMobile 群集的一部分。您将看到已添加的所有 XenMobile 节点。单击 Continue（继续）。



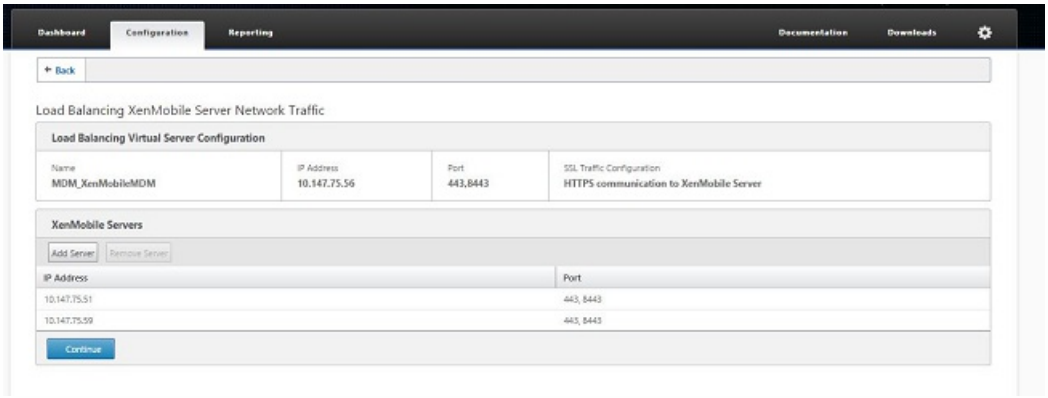
13. 单击 Load Balance Device Manager Servers（Device Manager 服务器负载平衡）以继续执行 MDM 负载平衡配置。



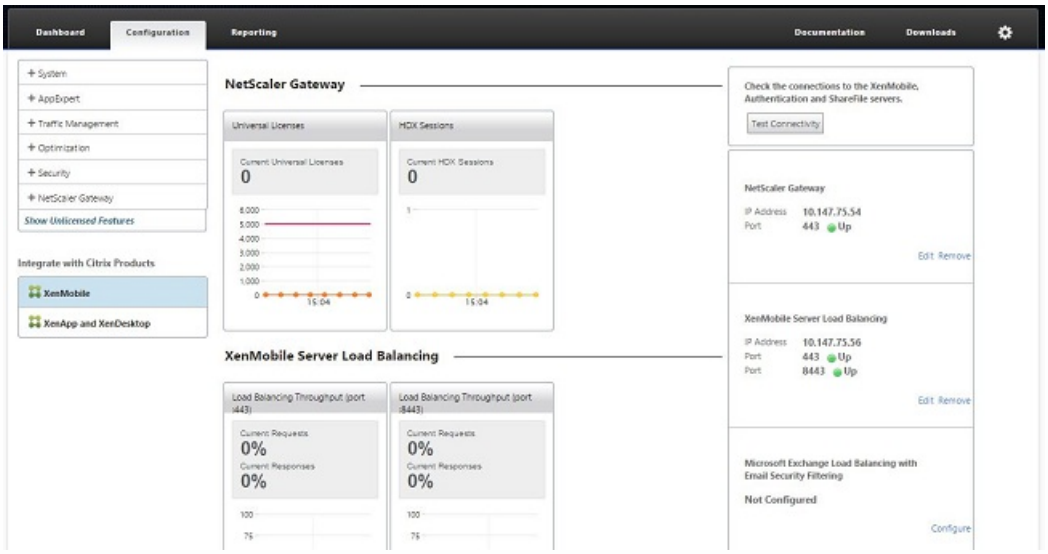
14. 输入要用作 MDM 负载平衡 IP 地址的 IP 地址，然后单击 Continue（继续）。



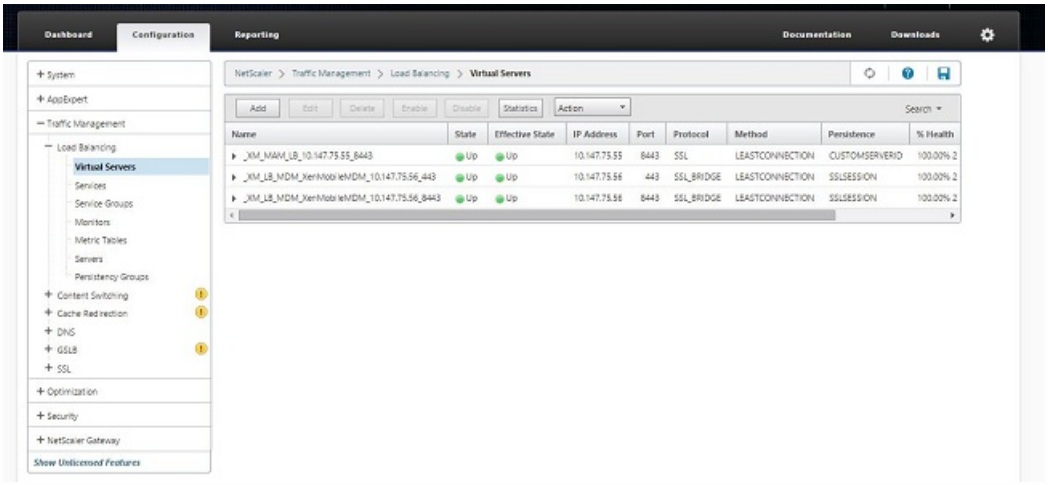
15. 列表中显示 XenMobile 节点后，单击 Continue（继续），然后单击 Done（完成）以完成此过程。



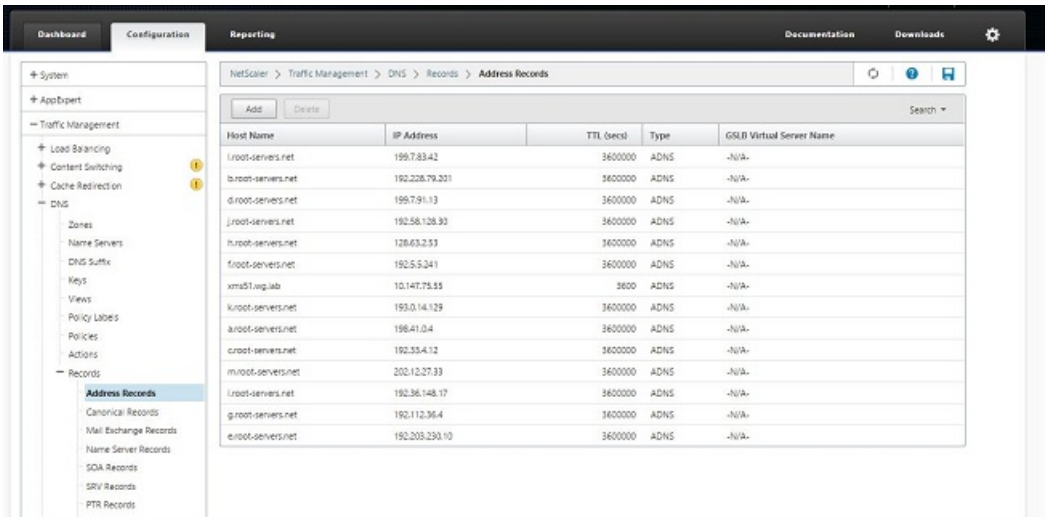
您将在 XenMobile 页面上看到虚拟 IP 地址状态。



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。



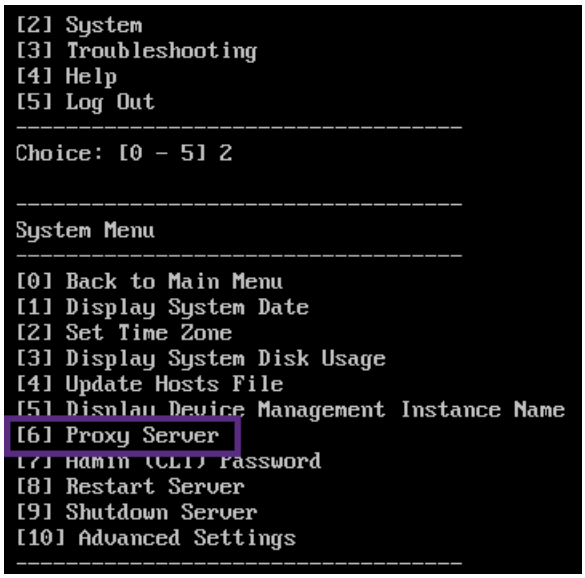
在 XenMobile 中启用代理服务器

Apr 22, 2016

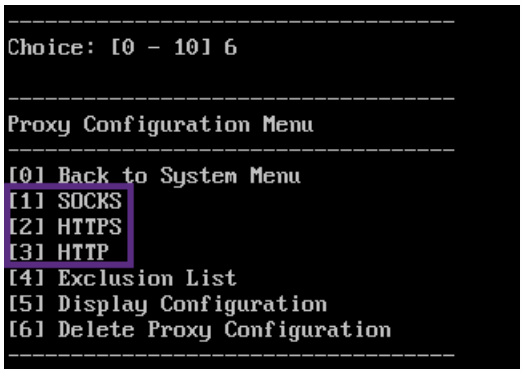
如果想要控制出站 Internet 流量，可以在 XenMobile 中设置代理服务器来承载此流量。为此，需要通过命令行接口 (CLI) 设置代理服务器。请注意，设置代理服务器需要重新启动系统。

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。



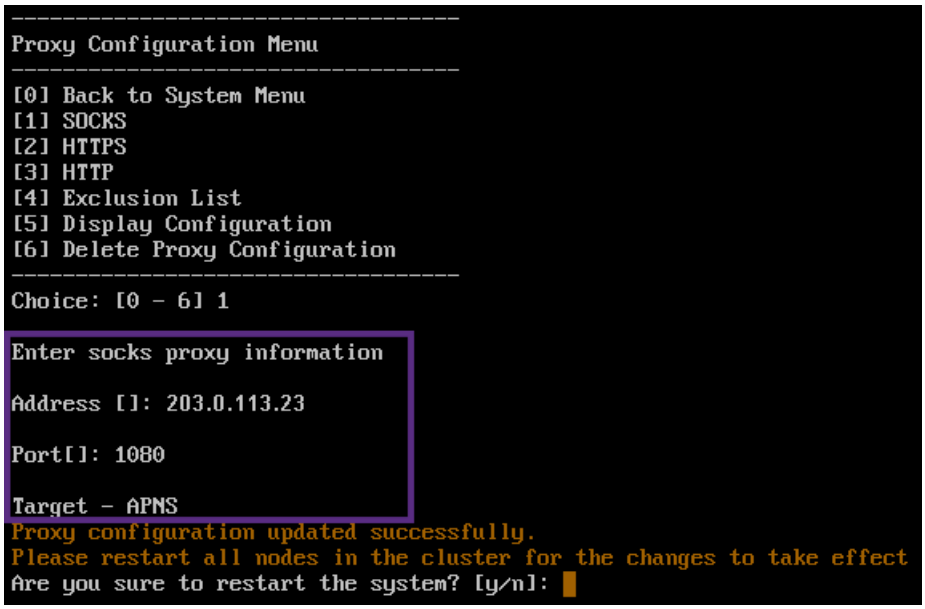
3. 在“Proxy Configuration Menu”（代理配置菜单）中，键入 **1** 以选择 SOCKS，键入 **2** 以选择 HTTPS，或键入 **3** 以选择 HTTP。



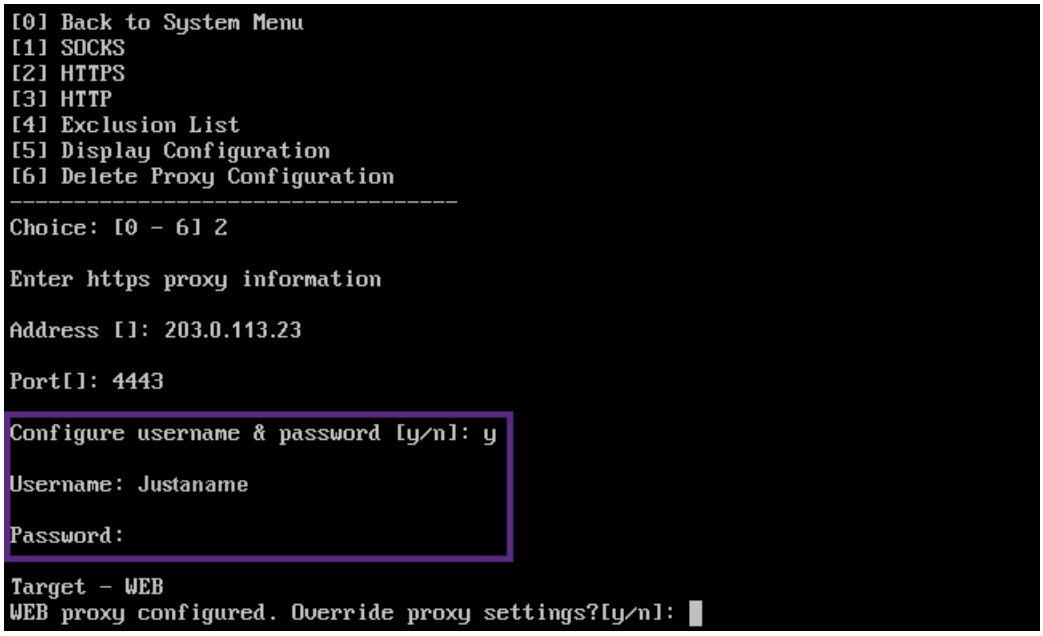
4. 键入代理服务器 IP 地址、端口号和目标。有关每种代理服务器类型支持的目标类型，请参阅下表。

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。

许可

Oct 22, 2015

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 10.1 要求 11.12.1 Citrix 许可证服务器或更高版本的许可证服务器；较旧的服务器版本与 XenMobile 10.1 不兼容。

> **Important**
>
> 如果打算将 XenMobile 的节点或实例群集在一起，需要在远程服务器上使用 Citrix Licensing。

Citrix 建议您保留收到的所有许可证文件的一份本地副本。保存配置文件的备份副本时，所有许可证文件都包含在备份中。但是，如果您在未提前备份配置文件的情况下重新安装 XenMobile，则需要使用原始许可证文件。

XenMobile 许可注意事项

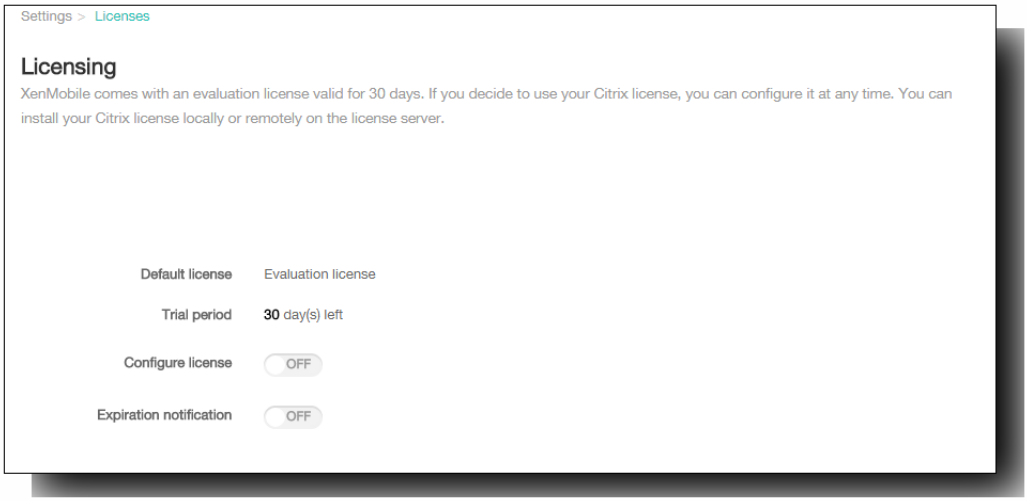
在不提供许可证的情况下，XenMobile 将在宽限期为 30 天的试用模式下运行，功能齐全。此试用模式只能使用一次，期限为从安装开始 30 天。无论是否有可用的有效 XenMobile 许可证，均不会阻止对 XenMobile Web 控制台的访问。

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。



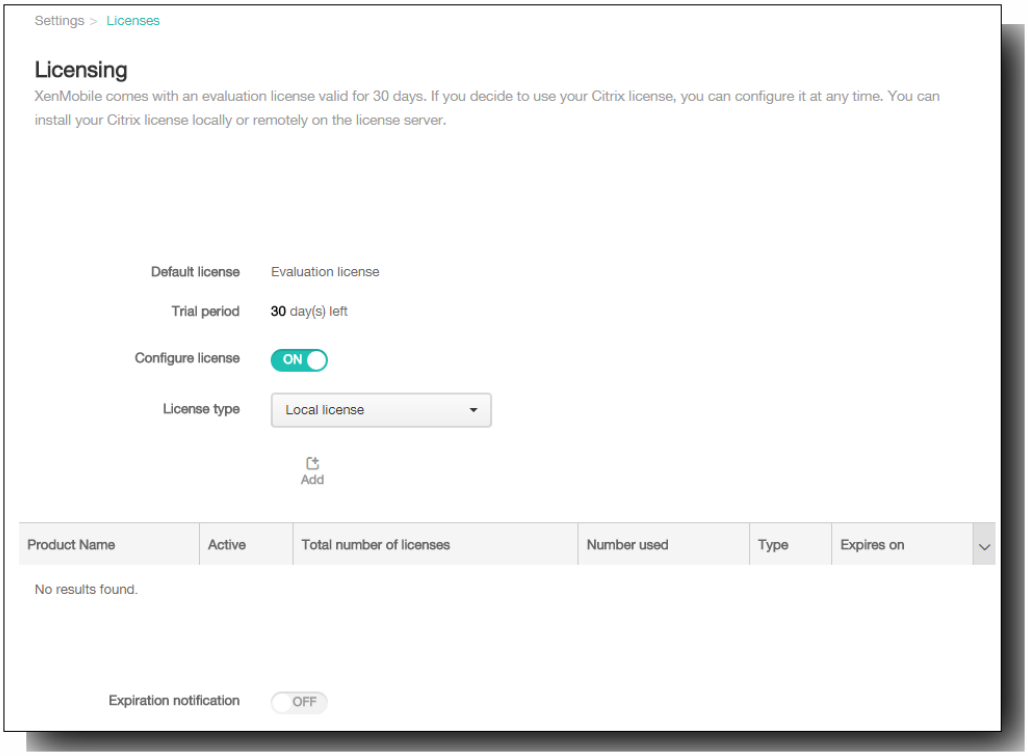
1. 在 XenMobile 控制台中，单击配置 > 设置。
2. 单击许可。 此时将显示许可页面。

添加本地许可证

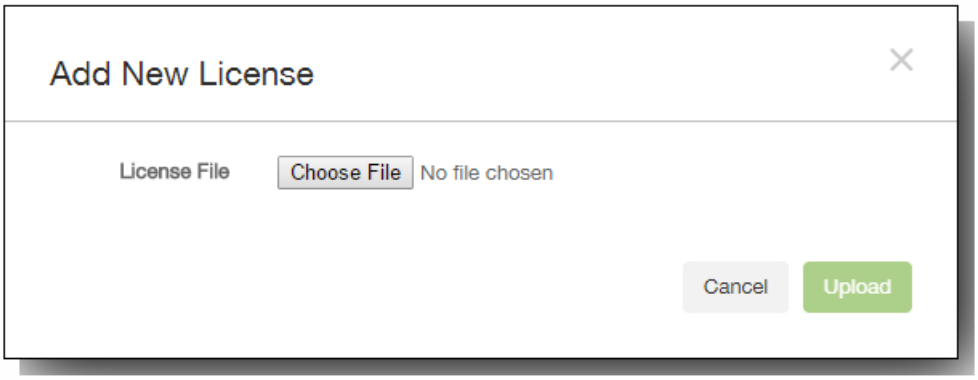
添加新许可证时，新许可证将显示在表格中。添加的第一个许可证自动被激活。如果添加同一类别（如企业）或同一类型（如设备）的多个许可证，这些许可证将显示在表格的同一行中。在这些情况下，许可证总数和使用的数量反应公共许可证的总数。过期日期显示公共许可证的最新过期日期。

通过 XenMobile 控制台管理所有本地许可证。

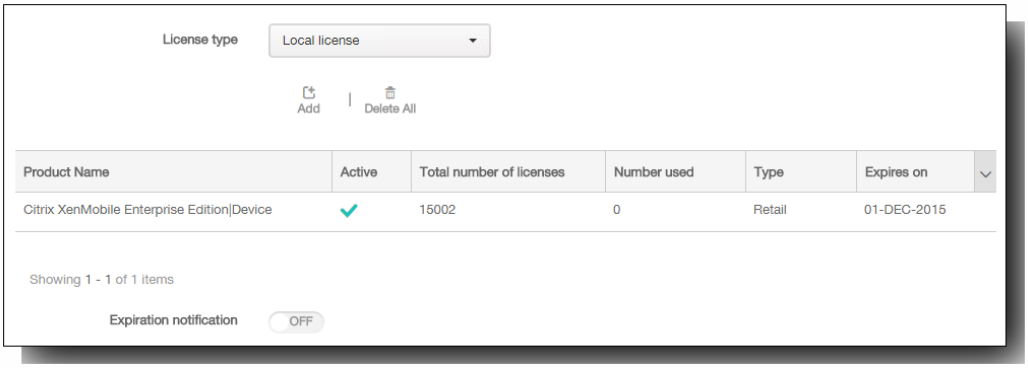
1. 从 Simple License Service 获取许可证文件，方法是通过许可证管理控制台或直接利用您在 Citrix.com 上的帐户。 有关详细信息，请参阅获取许可证文件。
2. 在控制台中，单击配置 >设置 > 许可证。 此时将显示许可页面。
3. 将配置许可证设置为开。 在许可证类型列表中，单击添加按钮，将显示许可表。许可表包含已用于 XenMobile 的许可证。如果尚未添加任何 Citrix 许可证，此表为空。



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。

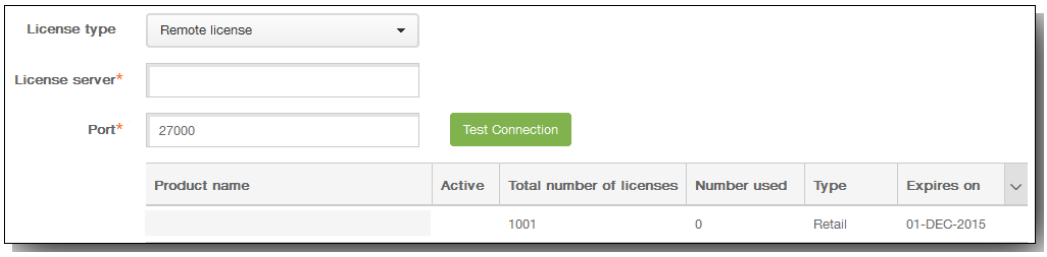


7. 许可证显示在许可证页面上的表格中以后，请将其激活。 如果此许可证是表格中的第一个许可证，此许可证会自动激活。

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。



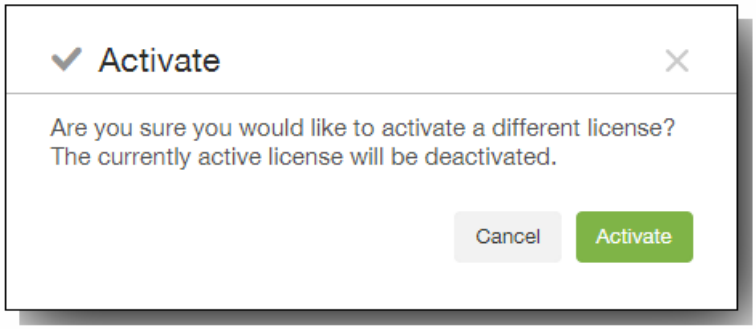
3. 在许可证服务器中，键入远程许可服务器的 IP 地址或完全限定的域名 (FQDN)。
4. 在端口字段中，接受默认端口或键入用于与许可服务器通信的端口号。
5. 单击测试连接。 如果连接成功，XenMobile 将与许可服务器连接，并且在许可表中填充可用的许可证。如果连接失败，请检查您提供的信息是否正确，以及所有连接是否激活。
   注意：如果只有一个许可证，会自动激活此许可证。

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。

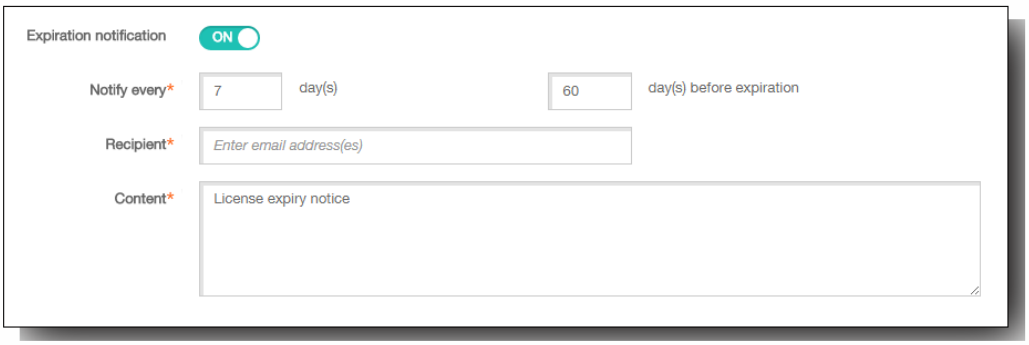


3. 单击激活。
   重要：如果激活所选许可证，当前激活的许可证将取消激活。
   所选许可证现已激活。

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

Oct 22, 2015

XenMobile 控制台是 XenMobile 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。

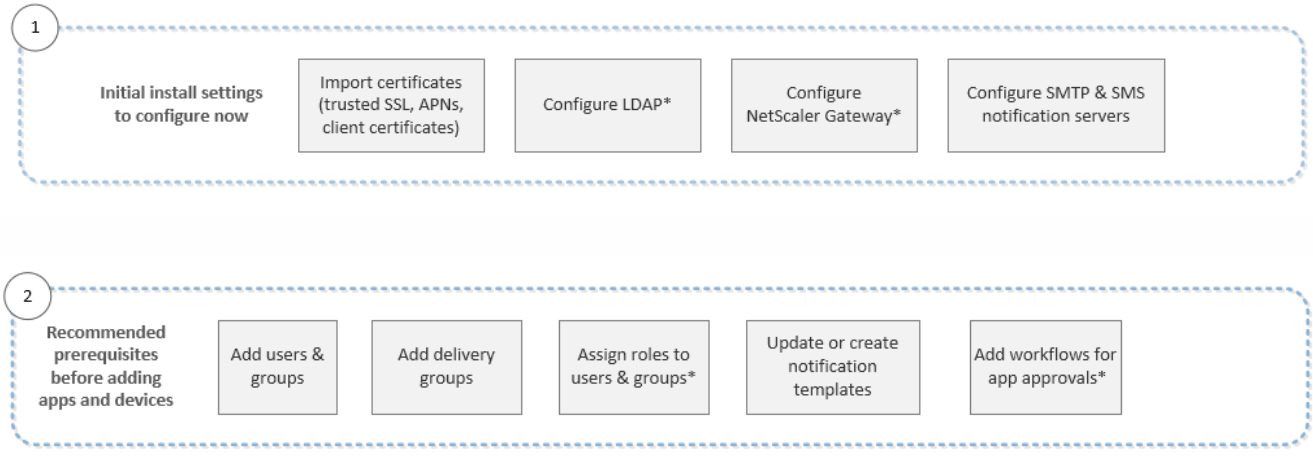
XenMobile 控制台在最近的两个 Firefox、Chrome 和 Internet Explorer 版本中受支持。

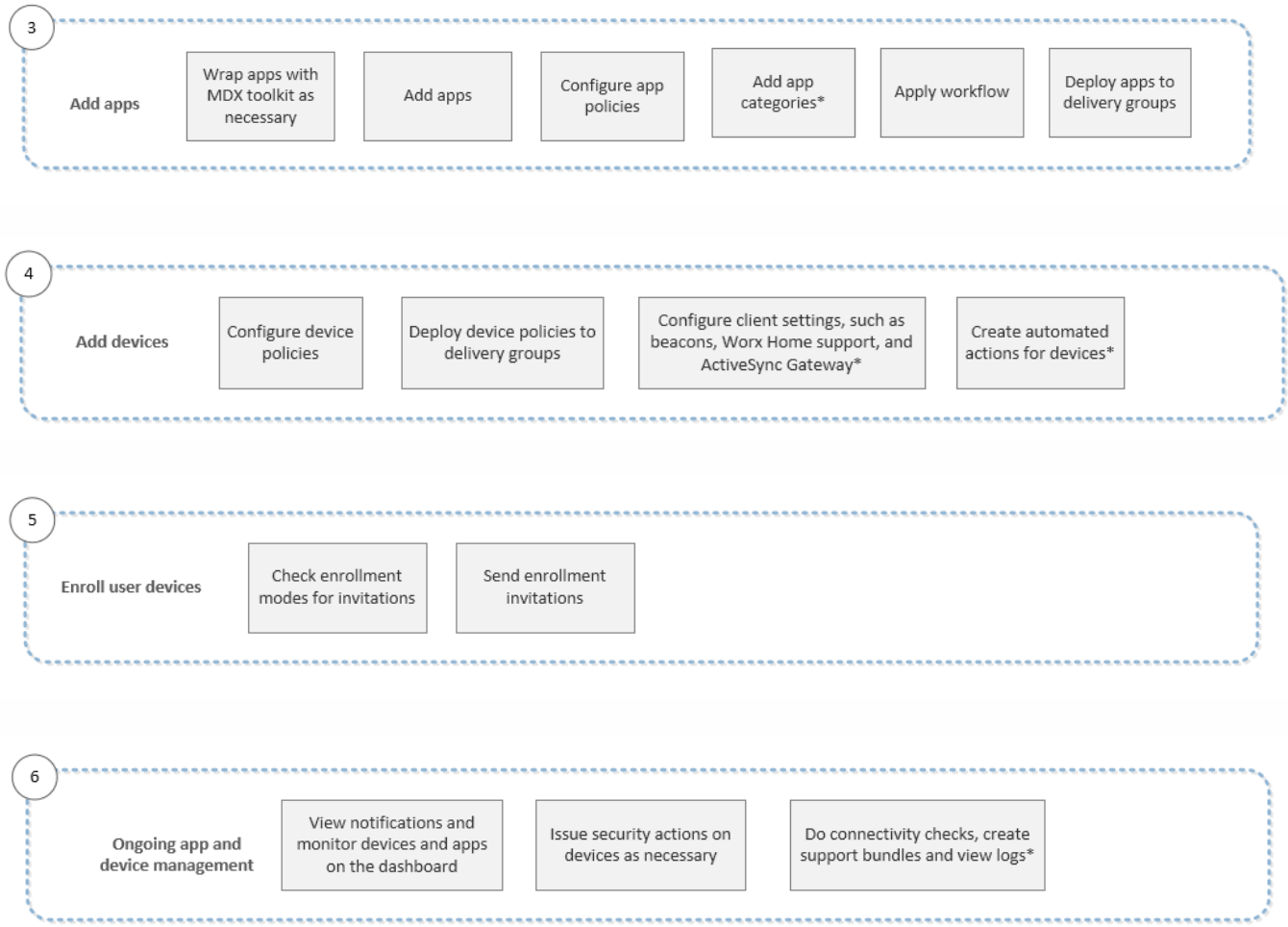
下图显示了登录基于 Web 的 XenMobile 控制台时首先出现的控制板的示例。

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。



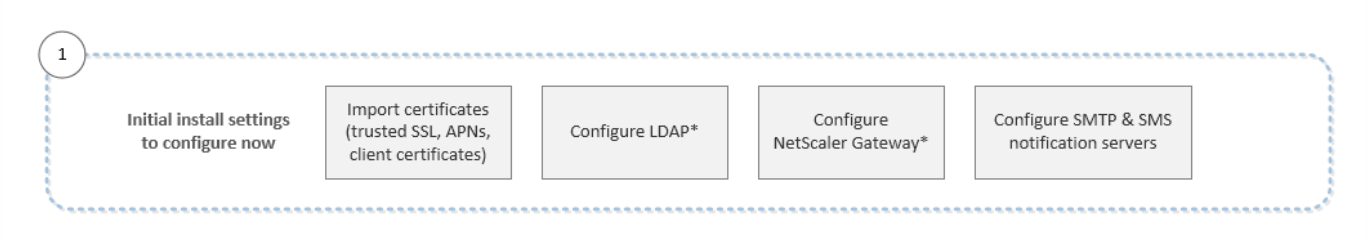


初始设置工作流

Oct 22, 2015

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 Citrix 产品文档文章：

- 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

Oct 22, 2015

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示建议在添加应用程序和设备前配置的必备条件。
注意：带星号的项目为可选项目。

有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 配置用户帐户、角色和注册设置
- 在 XenMobile 中管理交付组
- 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

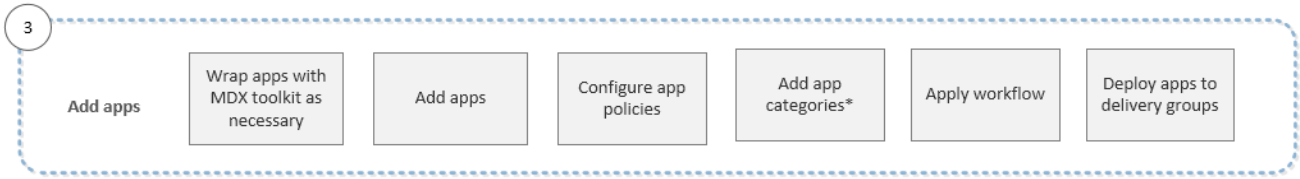
Oct 22, 2015

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。

接下来，可以按照控制台必备条件工作流中的说明，在添加应用程序和设备之前配置某些必备条件。要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示了向 XenMobile 中添加应用程序时应遵循的建议顺序。

注意：带星号的项目为可选项目。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 关于 MDX Toolkit
- 向 XenMobile 添加应用程序
- 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

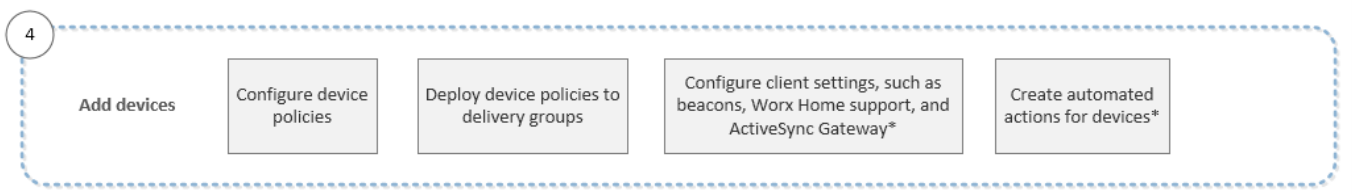
Oct 22, 2015

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。

接下来，可以按照控制台必备条件工作流中的说明，在添加应用程序和设备之前配置某些必备条件。然后，您可以按照添加应用程序工作流中的说明添加应用程序。要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示了向 XenMobile 中添加和注册设备时应遵循的建议顺序。

注意：带星号的项目为可选项目。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 在 XenMobile 中添加设备和查看设备详细信息
- XenMobile 设备策略（按平台）
- 在 XenMobile 中管理交付组
- 配置 XenMobile 客户端设置
- 在 XenMobile 中创建自动化操作

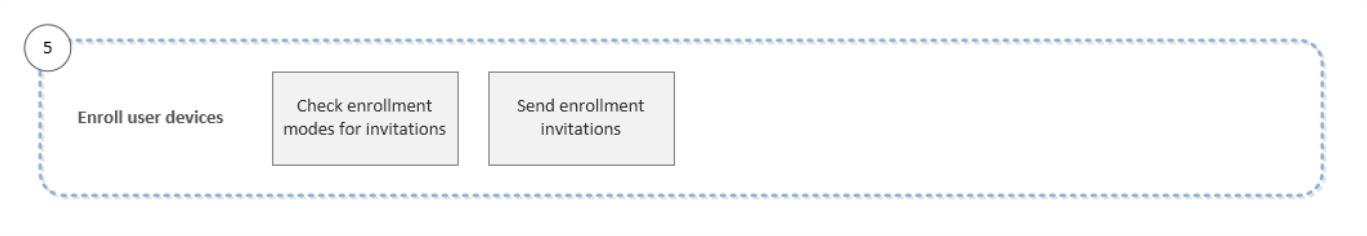
注册用户设备工作流

Oct 22, 2015

首先在命令行控制台，然后在 XenMobile 控制台中配置 XenMobile 后，控制板将打开。如果已跳过某些安装配置，可以在初始设置工作流中查看建议的初始设置。

接下来，可以按照控制台必备条件工作流中的说明，在添加应用程序和设备之前配置某些必备条件。然后，按照添加应用程序工作流中的说明添加应用程序，并按照添加设备工作流中的说明添加和注册设备。要查看整个工作流，请参阅 XenMobile 控制台入门。

此工作流显示了在 XenMobile 中注册用户设备时应遵循的建议顺序。



有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- 配置用户帐户、角色和注册设置
- 配置注册模式并启用自助服务门户

正在进行的应用程序和设备管理工作流

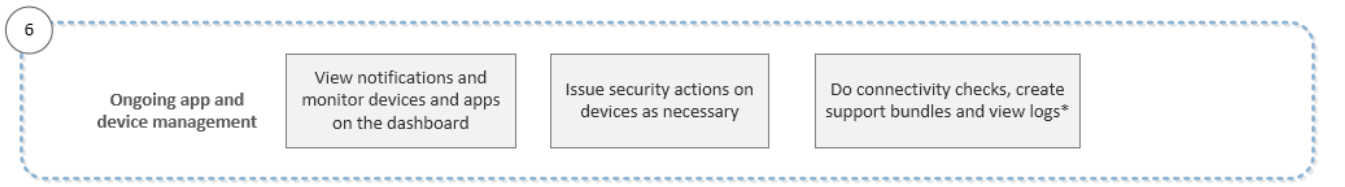
Oct 22, 2015

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

Oct 22, 2015

可以查找整个 XenMobile 控制台中的过滤器和表格。这些过滤器和表格位于主“设备”、“注册”、“设备策略”、“应用程序”、“操作”和“交付组”选项卡上以及“设备”选项卡下的多个页面上，例如“本地用户和组”。通过过滤器，您可以缩小控制台的任何区域中的信息的范围，以查找要查看或要对其执行操作的准确信息。在表格中，您可以单击一个或多个项目以查看用于对选定项目执行操作的选项。选项可能会随选定的项目数量而变化。

下表列出了某些常用选项及其所在表格。

菜单选项	操作	选项所在的表格
添加	将新项目添加到表格中。	全部
类别	添加和管理应用程序的类别。	应用程序
复制 URL	将 URL 复制到剪贴板。	注册
删除或全部删除	永久删除选定项目。	全部
部署	将资源部署到用户和设备。	设备和交付组
禁用	禁用某个应用程序或 AllUsers 交付组。	应用程序和交付组
编辑	更改现有项目。	除“注册”外的所有表格
导出	将表格的内容发送到 .csv 文件。	全部
导入	从置备文件中添加设备。	设备
	从文件中添加本地用户和组。	本地用户和组
管理本地组	添加本地组用于管理。	本地用户和组
通知	将通知发送到选定用户和设备。	“注册”和“设备”
刷新	更新表格。	设备
安全	调用选定设备上的安全选项。	设备
自助服务门户	启用自助服务门户作为注册模式。	注册

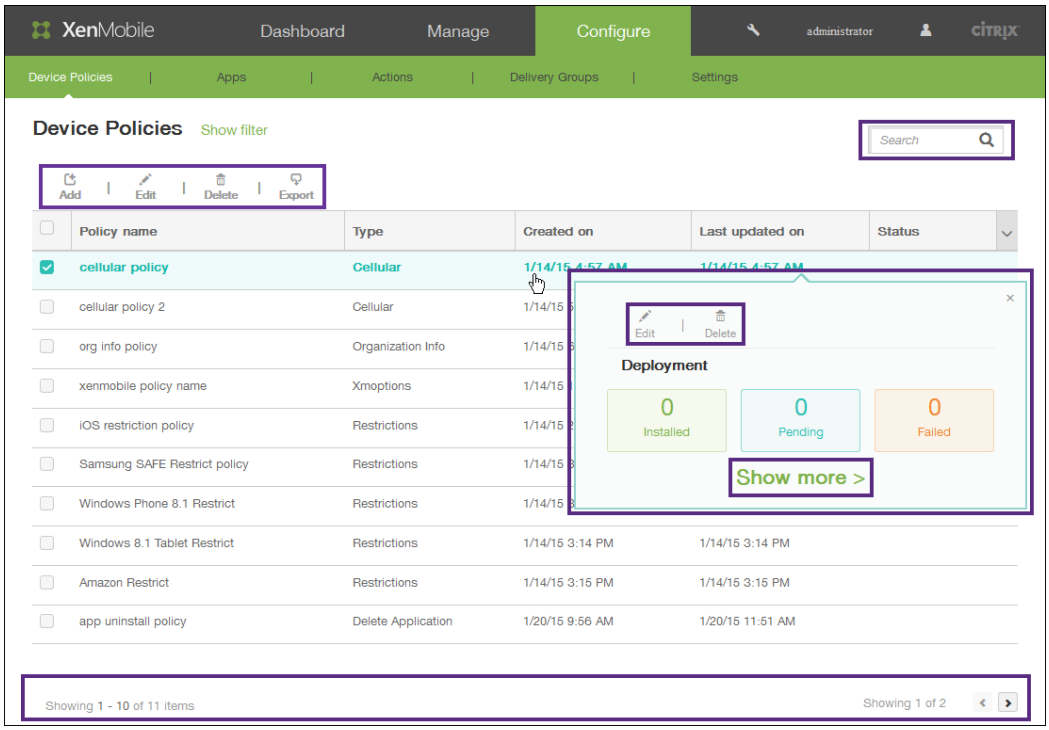
菜单选项	操作	选项所在的表格
更新	更新表格中的值。	版本管理

在 XenMobile 控制台中查看表格中的选项

要在控制台中针对表格中的信息采取操作，可以采用几种不同的方式查看各种选项：

- 可以选中某个项目旁边的复选框以在列表上方显示选项菜单。
- 可以选中多个项目旁边的复选框以同时对所有选定项目执行操作。能够对多个项目执行的操作取决于正在查看的表格。
- 可以单击列表中的某个项目以在此列表的右侧显示选项菜单。单击显示更多将显示与该项目有关的详细信息。显示的详细信息取决于正在查看的表格。
- 可以在搜索框中键入完整名称或部分名称，以限制列出的项目数。

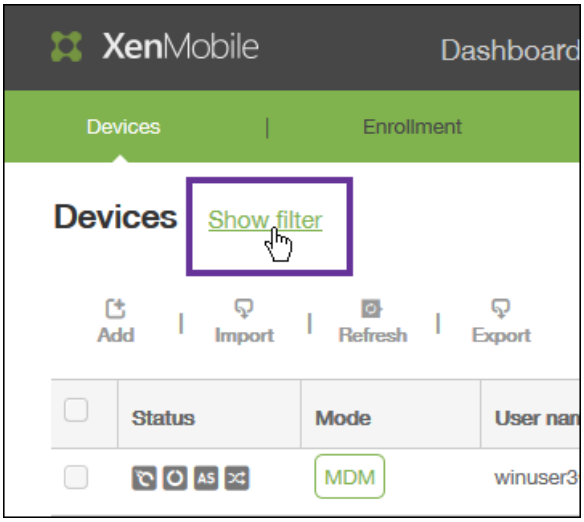
下图显示了这些选项在控制台的“设备策略”区域的显示方式。每页仅列出 10 个项目。单击页面右下角的三角形可以向前和向后移动页面。



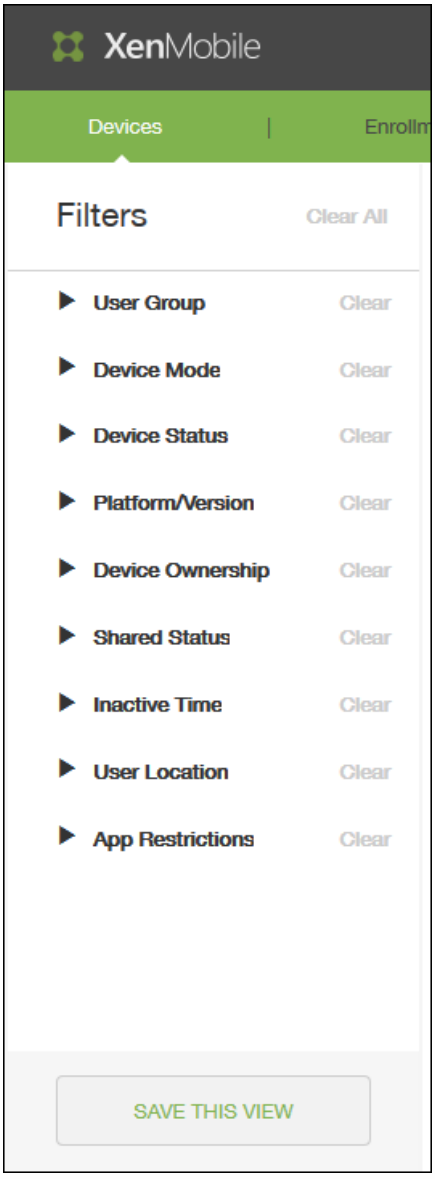
在 XenMobile 控制台中过滤信息

要在控制台的某个区域中查看信息的特定子集，例如“设备”、“注册”、“设备策略”、“应用程序”、“操作”、“交付组”和“本地用户和组”，可以根据选择的条件过滤列表。此过程以“设备”页面为例，但过滤步骤在整个控制台中均相同。

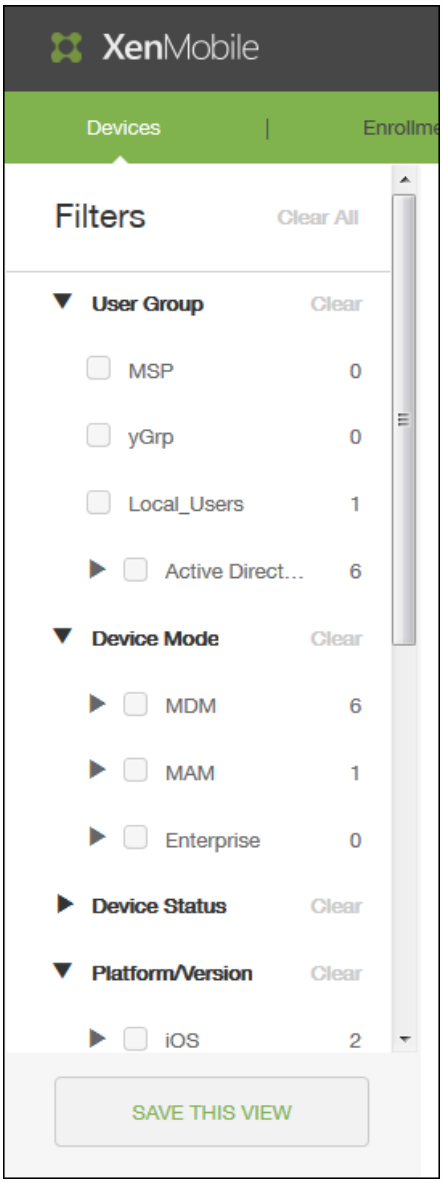
1. 在设备页面中，单击显示过滤器。



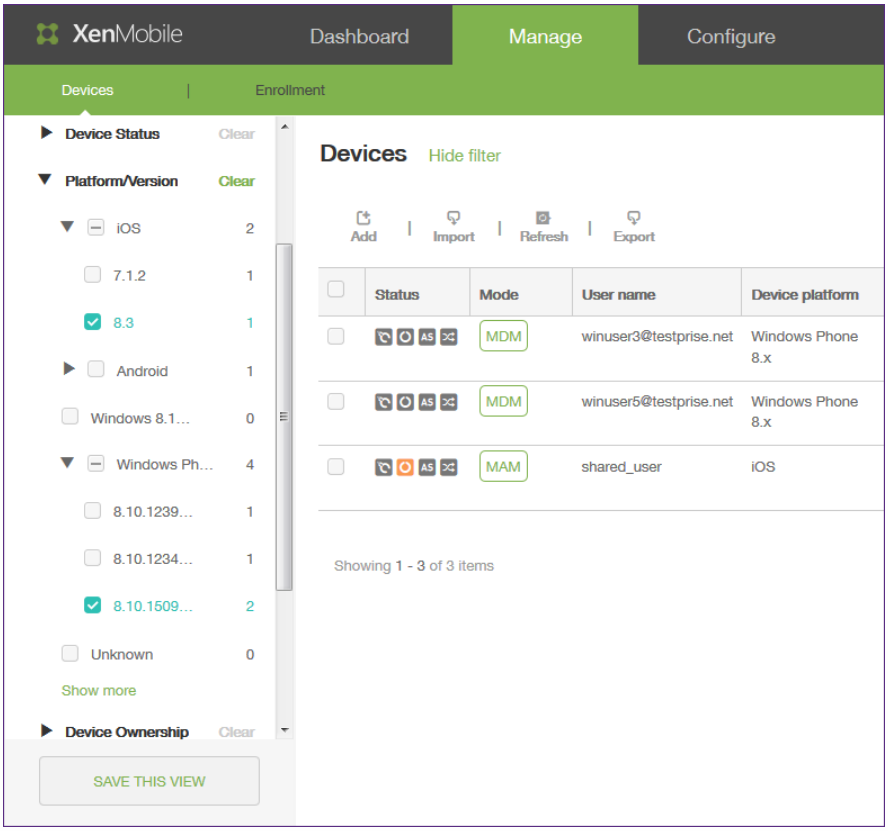
此时将显示过滤器面板，其中列出了过滤设备列表可以依据的条件。首次显示过滤器时，将折叠所有条件。



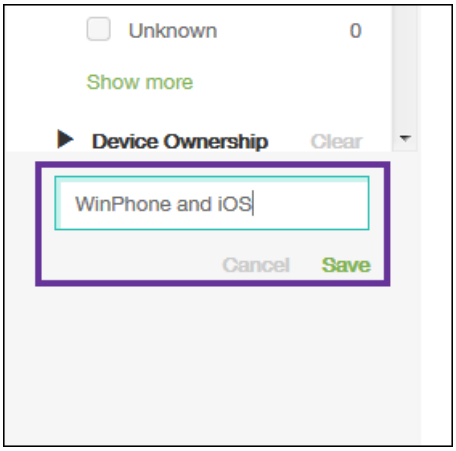
2. 单击过滤器左侧的三角形可显示该过滤器可以使用的条件。 每个条件右侧的数字表示满足该条件的设备数。



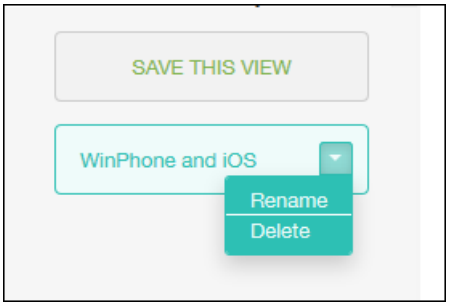
3. 选择要使用的过滤条件。 设备列表被限制到满足选定条件的设备。



4. 执行以下操作之一：
   - 单击隐藏过滤器以继续使用过滤后的列表。
   - 单击全部清除以还原到完整列表。
   - 单击特定条件旁边的清除可删除该过滤器，并从过滤后的列表中删除这些项目。
5. 如果要将所选条件另存为自定义过滤器，请在过滤器面板底部的 Save the filter（保存过滤器）字段中，键入描述性名称，然后单击保存。 如果决定不保存过滤器，请单击取消。



6. 保存过滤器后，可以在过滤器面板底部选中该过滤器以过滤表格中的信息。
   注意：如果单击过滤器名称右侧的三角形，则可以重命名或删除该过滤器。



通知

Oct 22, 2015

可以将 XenMobile 中的通知用于以下目的：

- 与选择的用户组通信以使用多个系统相关功能。您也可以将这些通知发送给特定用户，如使用 iOS 设备的所有用户、设备不合规的用户、使用员工自带设备的用户等。
- 注册用户及其设备
- 在满足某些条件时自动通知用户（使用自动化操作），例如，由于合规性问题阻止用户设备访问企业域时，或设备已被越狱或获得 Root 权限时。有关自动化操作的详细信息，请参阅自动化操作。

要使用 XenMobile 发送通知，必须配置网关和通知服务器。可以在 XenMobile 中设置通知服务器，以配置简单邮件传输协议 (SMTP) 和短信服务 (SMS) 网关服务器，以便向用户发送电子邮件和文本 (SMS) 通知。可以使用通知经两种不同的通道发送消息：SMTP 或 SMS。

- SMTP 是面向连接的文本协议，邮件发送方通常通过传输控制协议 (TCP) 发布命令字符串并提供必需的数据，从而与邮件接收方通信。SMTP 会话包括来自 SMTP 客户端（邮件发送人员）的命令和来自 SMTP 服务器的相应响应。
- SMS 是手机、Web 或移动通信系统的文本消息服务。它使用标准化通信协议，使固定线路或移动电话设备可以交换短文本消息。

您还可以在 XenMobile 中设置运营商 SMS 网关，以配置通过运营商的 SMS 网关发送的通知。运营商使用 SMS 网关发送和接受来往于电信网络的 SMS 传输。这些基于文本的消息使用标准化通信协议，允许固定线路或移动电话设备交换短文本消息。

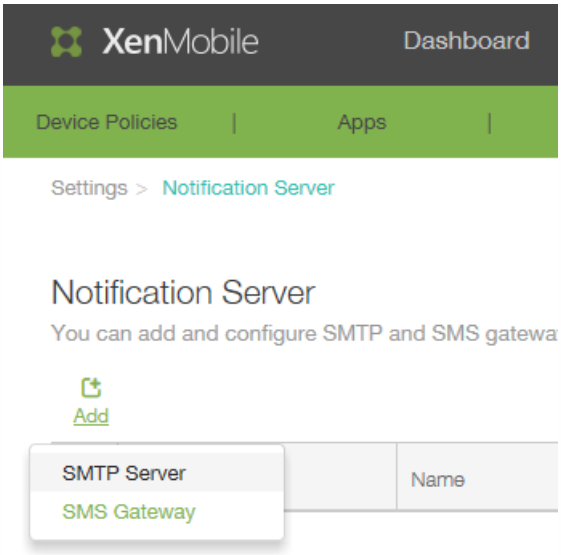
本主题中的过程讨论添加 SMTP 服务器、SMS 网关和运营商 SMS 网关的信息。

配置 SMTP 服务器和 SMS 网关

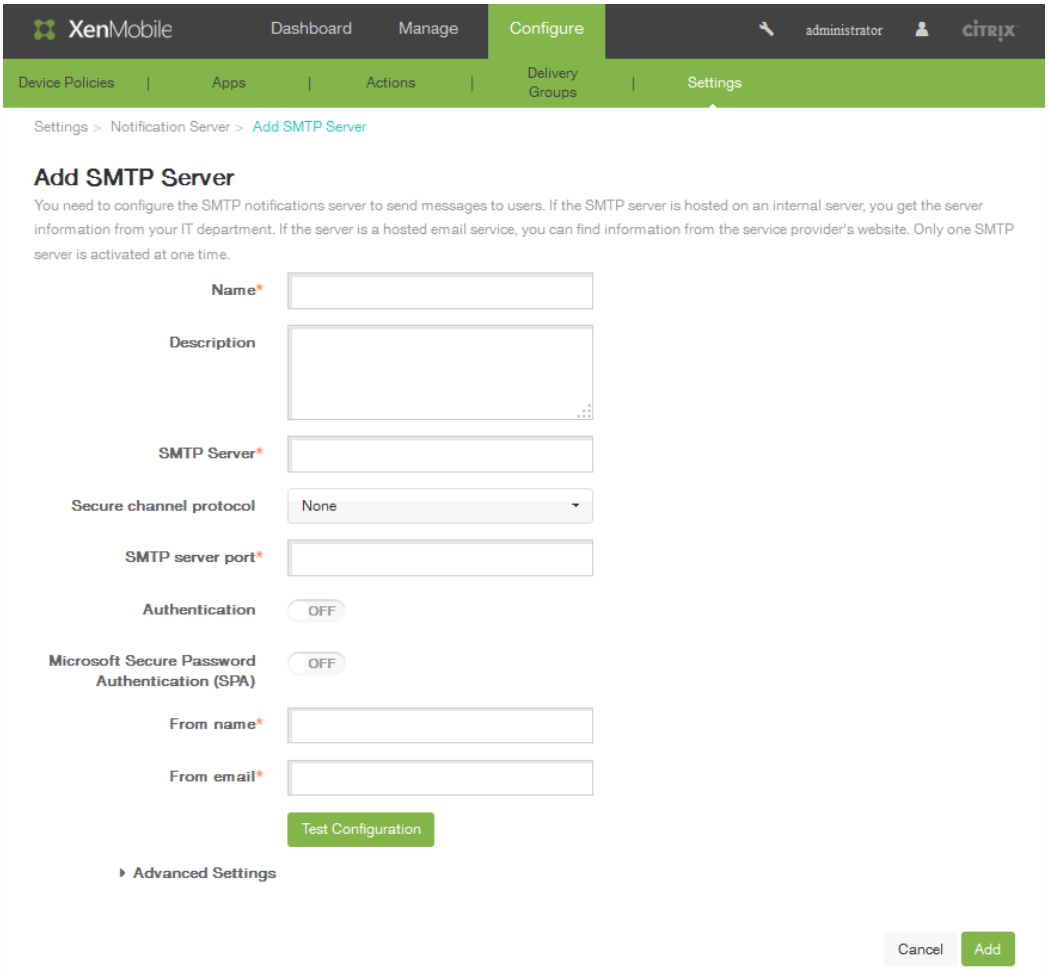
必备条件：

- 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。



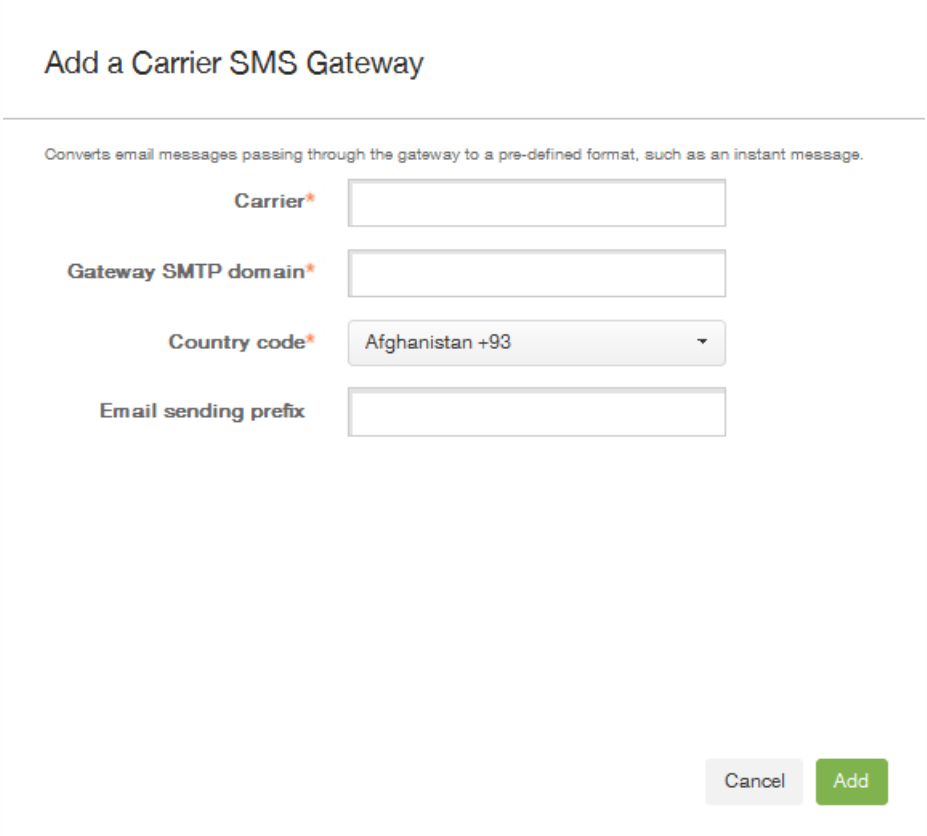
2. 单击添加，单击 SMTP 服务器或 SMS 网关，然后按照后续步骤中针对每个选项的过程操作。
   - 要添加 SMTP 服务器，请遵循步骤 3 至 6。
   - 要添加 SMS 网关，请遵循步骤 7 至 9。
3. 如果单击以添加 SMTP 服务器，将显示 Add SMTP Server（添加 SMTP 服务器）页面。



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 Advanced Settings（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 Add SMS Gateway（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。

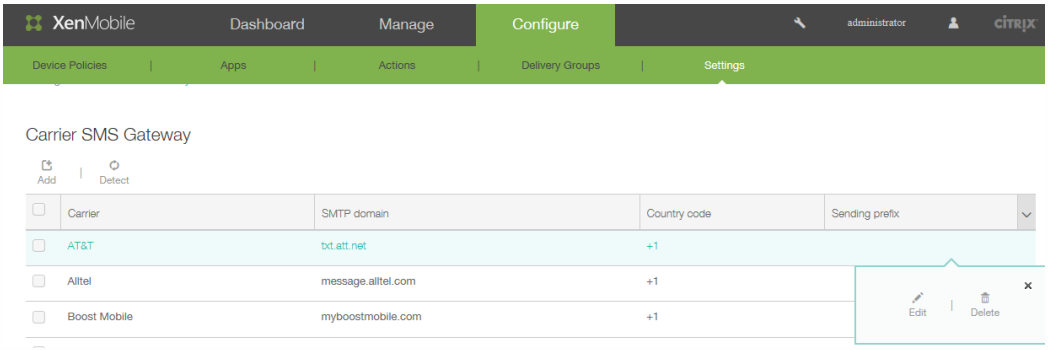
- 密码：键入系统管理员提供的密码，当密码丢失或被盗时用于访问您的帐户。
- 虚拟电话号码：向北美电话号码（前缀为 +1）发送时使用此字段。必须输入 Nexmo 虚拟电话号码；否则，请输入有意义的标签或名称。可以在 Nexmo Web 站点上购买虚拟电话号码。
- HTTPS：如果要使用 HTTPS 将 SMS 请求传输到 Nexmo，请选中此选项。
- 国家/地区代码：在此列表中，单击贵组织收件人的默认 SMS 国家/地区代码前缀。此字段始终以 + 符号开头。
- 测试配置：单击此选项将使用当前的配置发送测试消息。系统会立即检测到连接错误并将其显示出来，如身份验证或虚拟电话号码错误。接收消息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

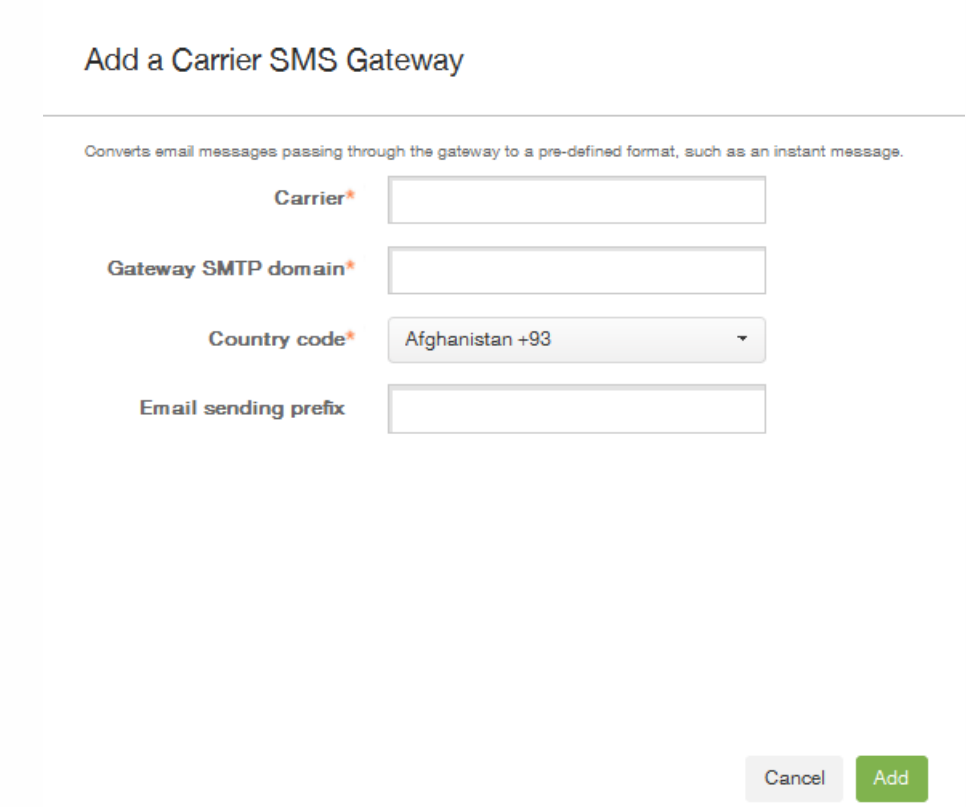
添加运营商 SMS 网关

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

Oct 13, 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 组件	证书格式	所需的证书类型
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL、根 NetScaler Gateway 自动将 PFX 转换为 PEM。
XenMobile 服务器	PEM 或 PFX (PKCS#12)	SSL、SAML、APNs XenMobile 还在安装过程中生成完全 PKI。 XenMobile 服务器不支持扩展名为 .pem 的证书。 使用 openssl 命令可从 PEM 文件生成 PFX 文件： openssl pkcs12 -export -out certificate.pfx -in certificate.pem
StoreFront	PFX (PKCS#12)	SSL、根

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

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

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。

XenMobile 证书管理

我们建议您跟踪在您的 XenMobile 部署中使用的证书，尤其是其过期日期和关联的密码。 本部分内容目的是帮助您更轻松地在 XenMobile 中进行证书管理。

您的环境中可能包含以下部分或所有证书：

XenMobile 服务器
用于 MDM FQDN 的 SSL 证书
SAML 证书（用于 ShareFile）
用于以上证书和任何其他内部资源（StoreFront/代理等）的根和中间 CA 证书
用于 iOS 设备管理的 APNS 证书
用于 XMS WorxHome 通知的内部 APNS 证书
用于与 PKI 的连接的 PKI 用户证书

MDX Toolkit
Apple 开发人员证书
Apple 置备描述文件（按应用程序）
Apple APNS 证书（用于 WorxMail）
Android 密钥库文件
Windows Phone – Symantec 证书

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

XenMobile 证书过期策略

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

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

用于 WorxMail 的 APNs 证书

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

用于 iOS 设备管理的 APNs 证书

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

可以通过登录 Apple 推送证书门户来查看 APNS 证书状态和过期日期。 请务必使用创建证书的同一用户身份登录。

在过期日期之前 30 天和 10 天，您还将收到 Apple 发送的电子邮件通知，其中包含以下信息：

The following Apple Push Notification Service certificate, created for AppleID CustomersID will expire on Date. Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

Please contact your vendor to generate a new request (a signed CSR), then visit https://identity.apple.com/pushcert to renew your Apple Push Notification Service certificate.（为 AppleID CustomersID 创建的以下 Apple 推送通知服务证书将于 Date 过期。吊销此证书或允许此证书过期需要为现有设备重新注册新的推送证书。请联系您的供应商以生成新请求（签名的 CSR），然后访问 https://identity.apple.com/pushcert 以续订您的 Apple 推送通知服务证书。）

Thank You,（顺祝商祺）

Apple Push Notification Service（Apple 推送通知服务）

MDX Toolkit（iOS 分发证书）

在物理 iOS 设备上运行的任何应用程序（Apple App Store 中的应用程序除外）必须通过置备描述文件和相应的分发证书进行签名。

请注意，现有 iOS Developer for Enterprise 证书和置备描述文件可能与 iOS 9 不兼容。 有关详细信息，请参阅“打包适用于 iOS 9 的 Worx 应用程序”。

要验证您的 iOS 分发证书是否有效，请执行以下操作：

1. 从 Apple 企业开发者门户中，为计划使用 MDX Toolkit 打包的每个应用程序创建一个显式应用程序 ID。 可接受的应用程序 ID 示例：com.CompanyName.ProductName。
2. 从 Apple 企业开发者门户中，转到 **Provisioning Profiles**（置备描述文件）> **Distribution**（分发），并创建一个内部置备描述文件。 对在上一步中创建的每个应用程序 ID 重复此步骤。
3. 下载所有置备描述文件。 有关详细信息，请参阅打包 iOS 移动应用程序。

要确认所有 Xenmobile 服务器证书是否有效，请执行以下操作：

1. 在 XenMobile 控制台中，单击**配置**，然后单击**证书**。
2. 确保包含 APNS、SSL 侦听器、根和中间证书的所有证书都有效。

Android 密钥库

密钥库是指包含用于为您的 Android 应用程序签名的证书的文件。当您的密钥有效期过期后，用户不能再无缝地升级到应用程序的新版本。

Symantec 提供的用于 Windows Phone 的企业证书

Symantec 是用于 Microsoft 应用程序中心服务的代码签名证书的独家提供商。 开发者和软件发行者加入应用程序中心来分发 Windows Phone 和 Xbox 360 应用程序，以便通过 Windows Marketplace 下载。 有关详细信息，请参阅 Symantec 文档中的 Symantec Code Signing Certificates for Windows Phone（Symantec 用于 Windows Phone 的代码签名证书）。

如果证书过期，Windows Phone 用户将无法注册和安装公司发布和签名的应用程序，也不能启动手机上安装的公司应用程序。

NetScaler

有关如果处理 NetScaler 的证书过期的详细信息，请参阅 Citrix 支持知识中心中的 How to handle certificate expiry on NetScaler （如何处理 NetScaler 的证书过期）。

如果 NetScaler 证书过期，用户将无法注册、访问 Worx Store、使用 WorxMail 时连接至 Exchange Server 以及枚举和打开 HDX 应用程序（取决于过期的证书）。

Expiry Monitor 和 Command Center 可以帮助您跟踪 NetScaler 证书，并在证书过期时通知您。 这两个工具可以协助监视以下 Netscaler 证书：

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

在 XenMobile 中上载证书

Aug 04, 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）

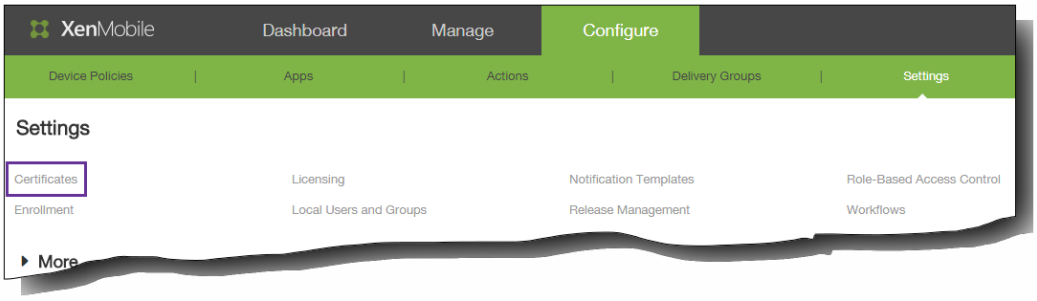
重要：XenMobile 服务器不支持扩展名为 .pem 的证书。 使用 openssl 命令可基于 PEM 文件生成 PFX 文件：

```
openssl pkcs12 -export -out certificate.pfx  -in certificate.pem
```

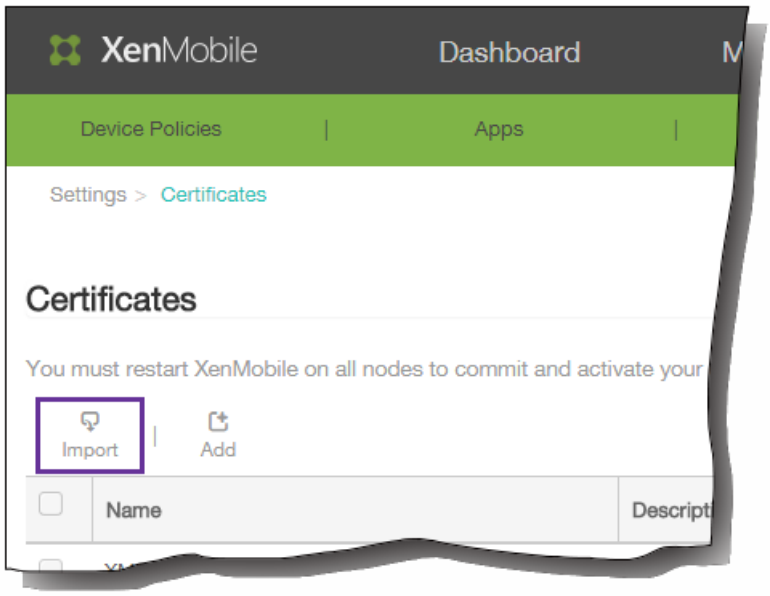
导入密钥库

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

1. 在 XenMobile 控制台中，单击配置 > 设置 > 证书。

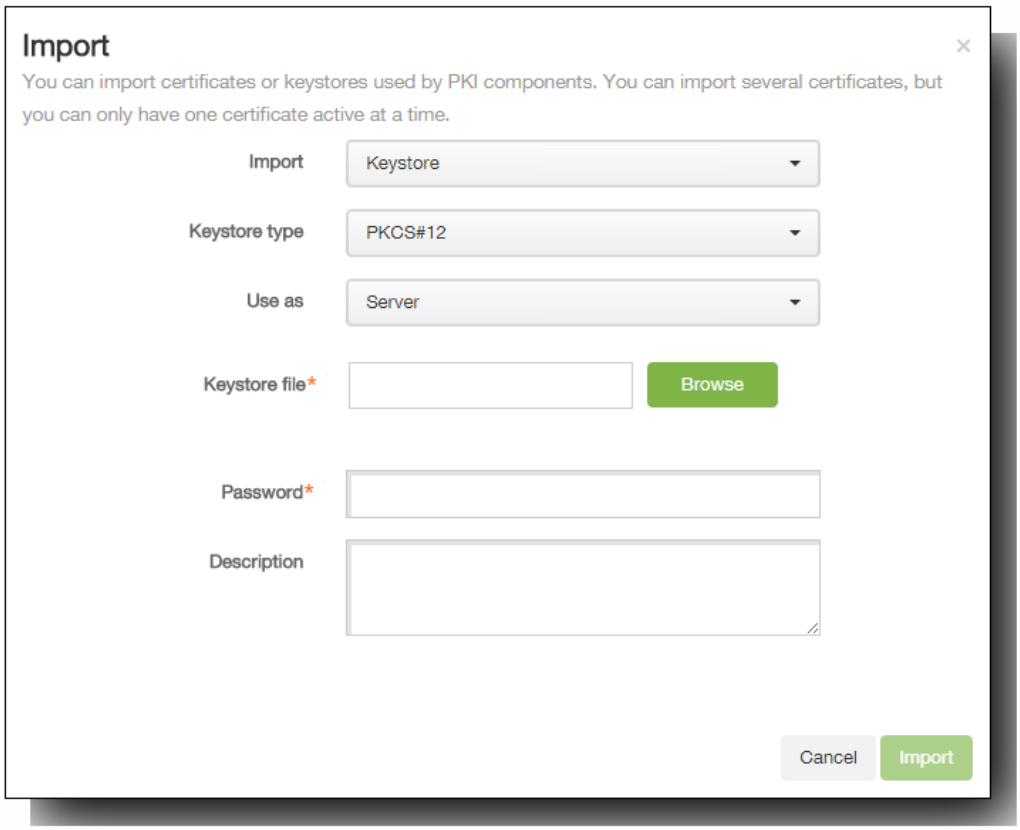


2. 在证书页面上，单击导入。



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。

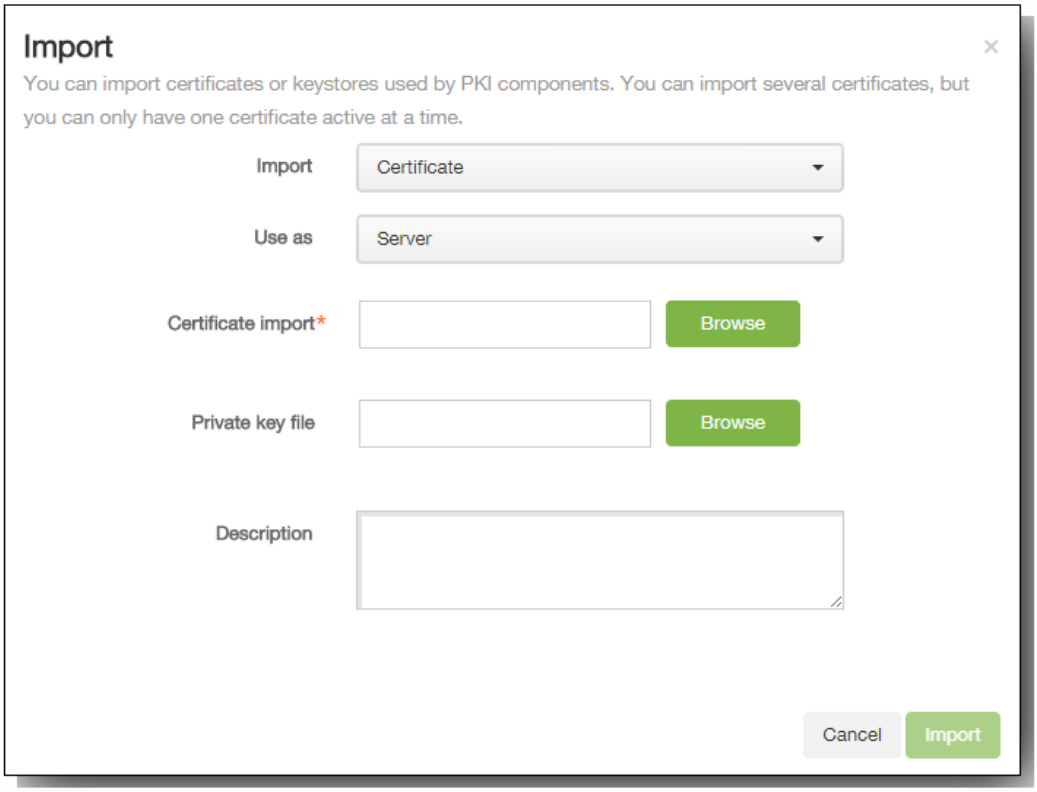
导入证书

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。

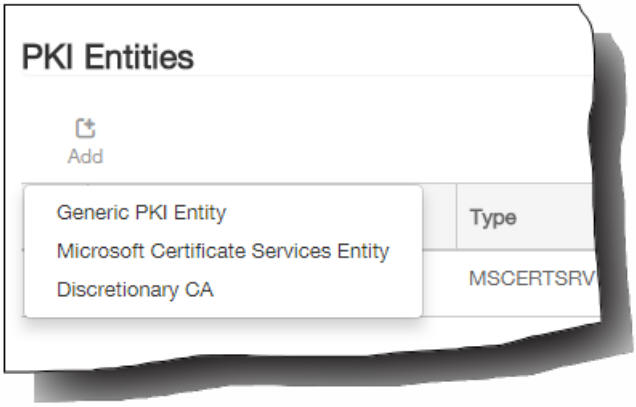
要最有效地更新证书，请在 XenMobile 控制台中导入对话框的配置 > 设置 > 证书下面，导入新证书。当更新服务器证书时，使用先前证书的组件将自动切换到使用新证书。同样，如果已经在设备上部署服务器证书，证书将在下一次部署时自动更新。

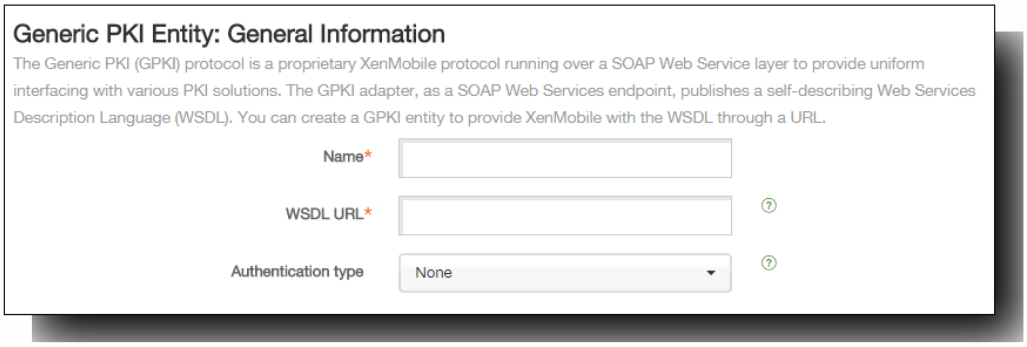
-
-
-

-
-
-

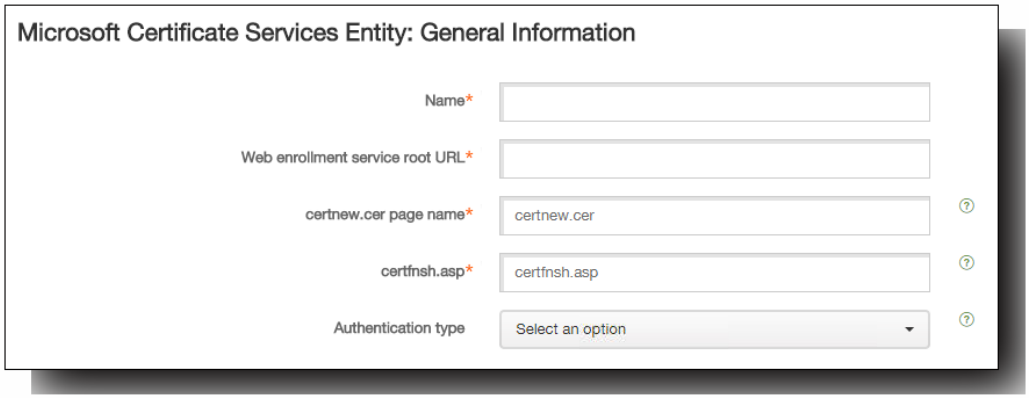
-
-
-

-
-
-





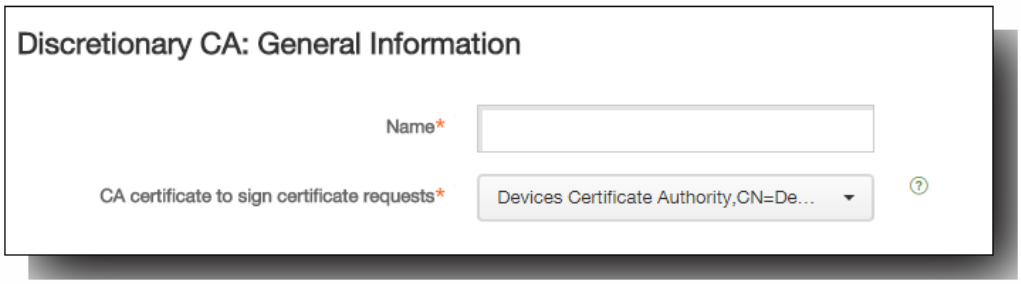
-
-
-

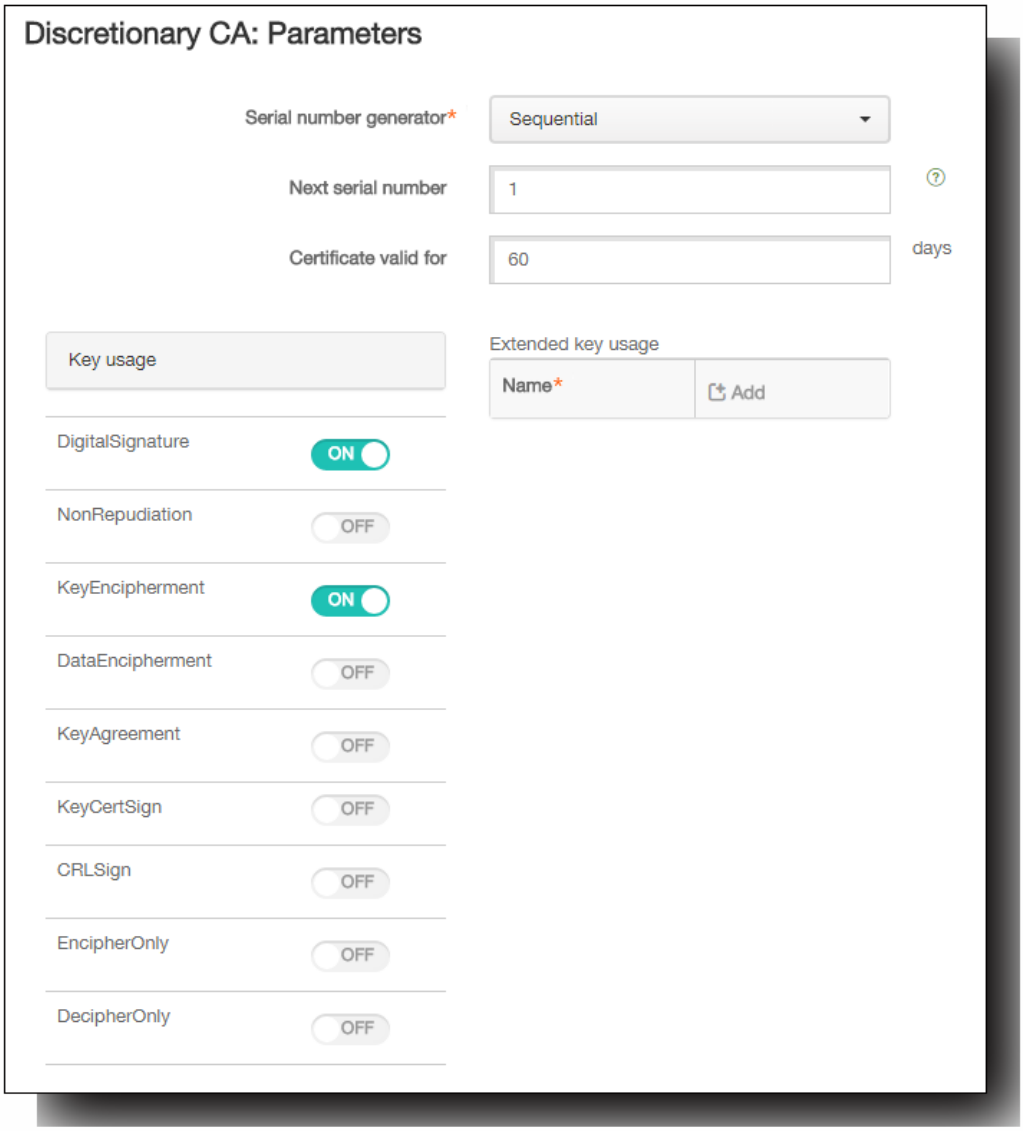


-
-
-
-

https://server/instance/ocsp

-
-
-
-
-





-
-

-
-
-
-
-

-

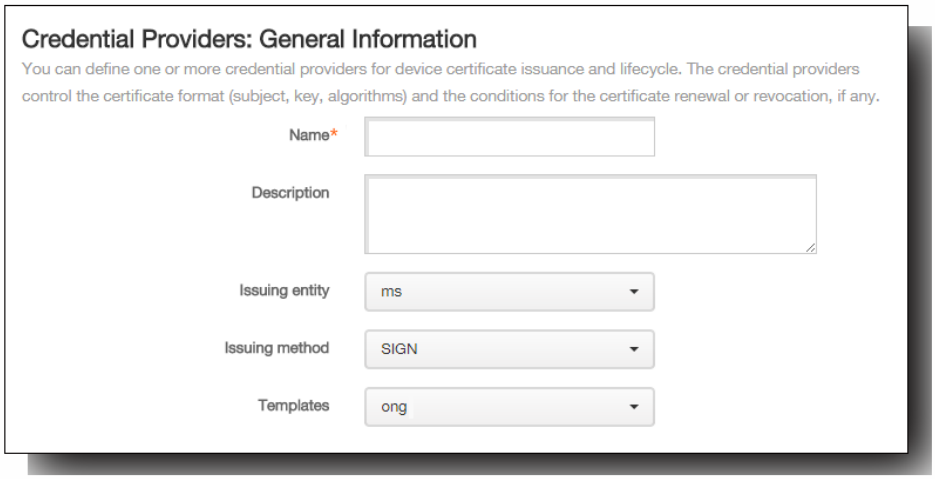
可以采用两种途径获取证书（称为颁发方法）：

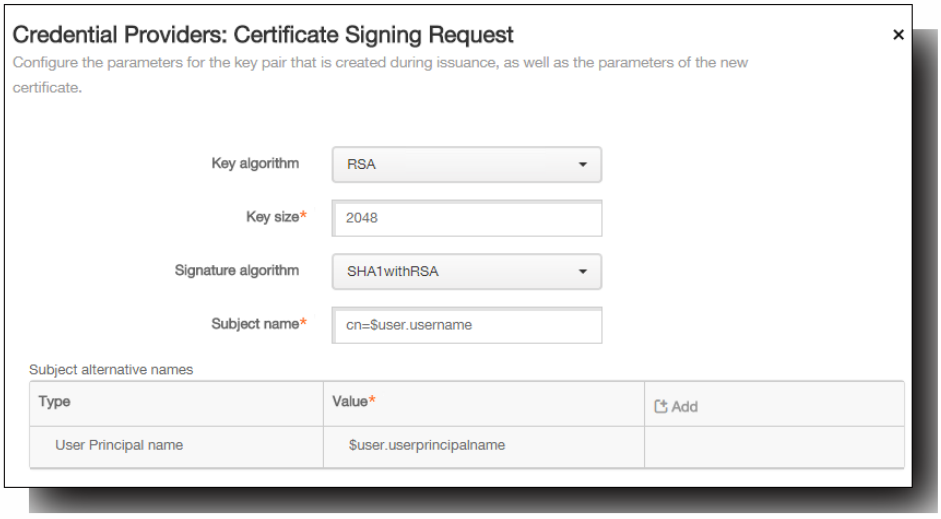
- 签名。 利用此方法，颁发包括创建新私钥、创建 CSR 和将 CSR 提交给证书颁发机构 (CA) 进行签名。 XenMobile 支持对三种 PKI 实体（Microsoft 证书服务实体、通用 PKI 和任意 CA）使用此签名方法。
- 提取。 利用此方法，用于 XenMobile 的颁发是指对现有密钥对的恢复。 XenMobile 仅支持对通用 PKI 使用提取方法。

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。

-
-

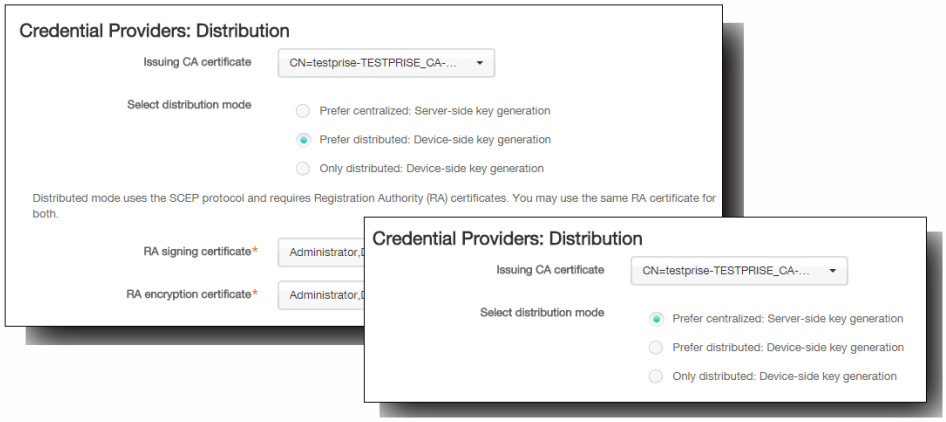
-
-
-

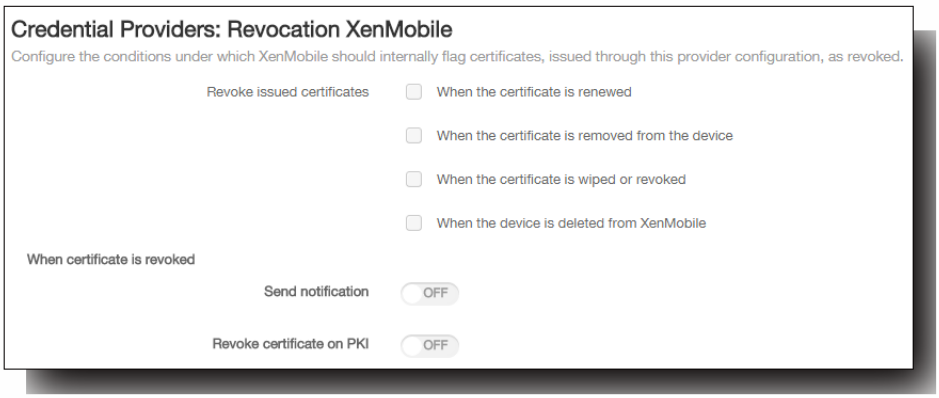


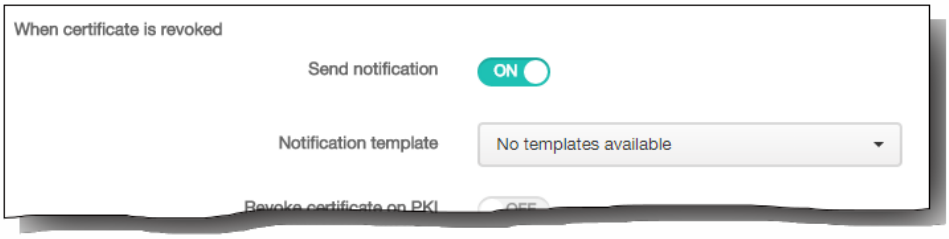


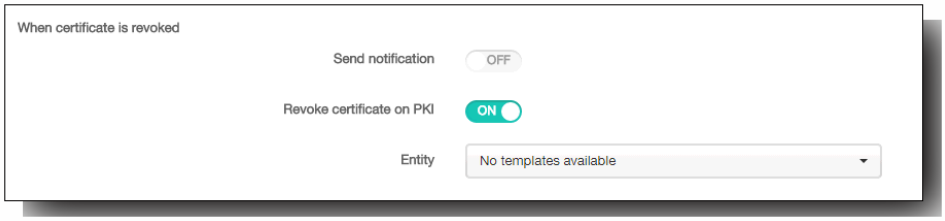
CN=${user.username} OU=${user.department} O=${user.companyname} C=${user.c}\endquotation

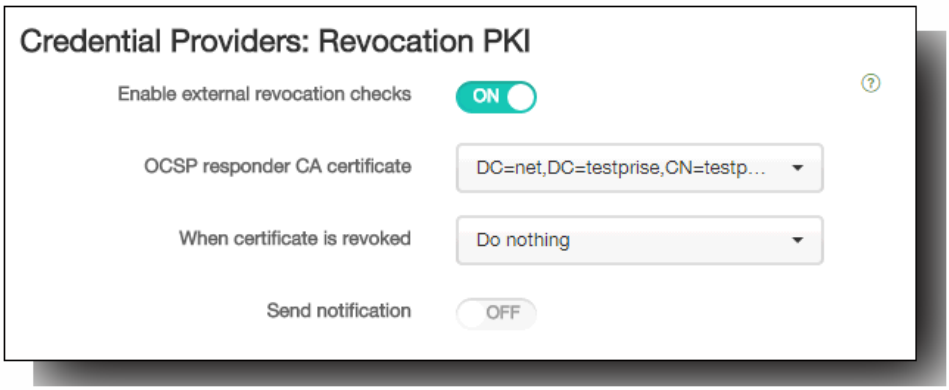
-
-
-









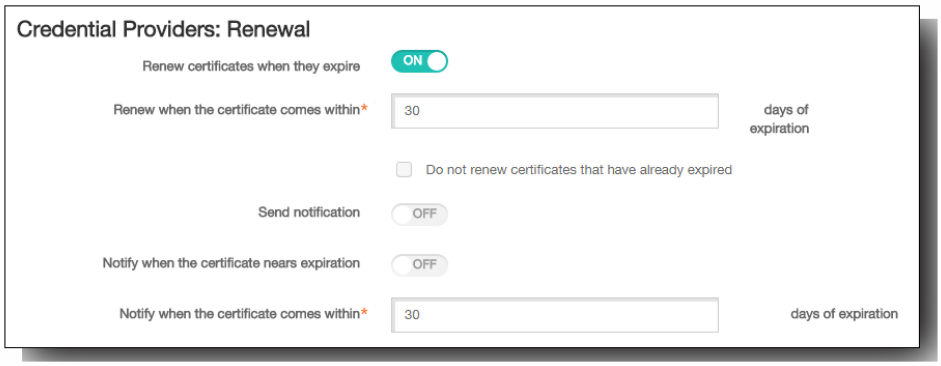


-
-
-

-

-

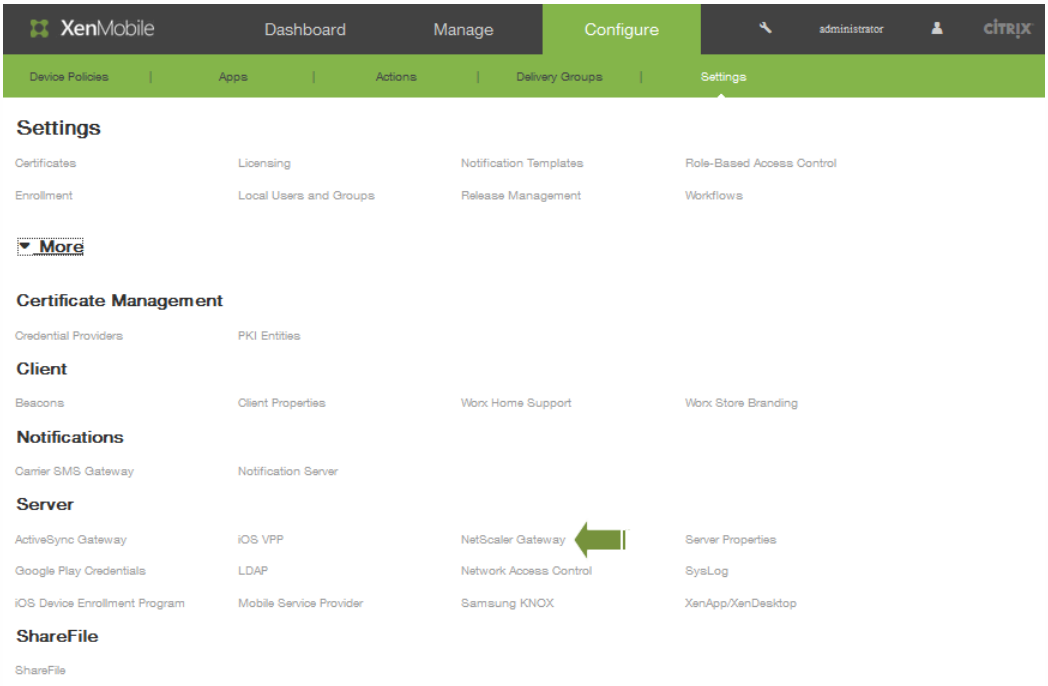
-
-

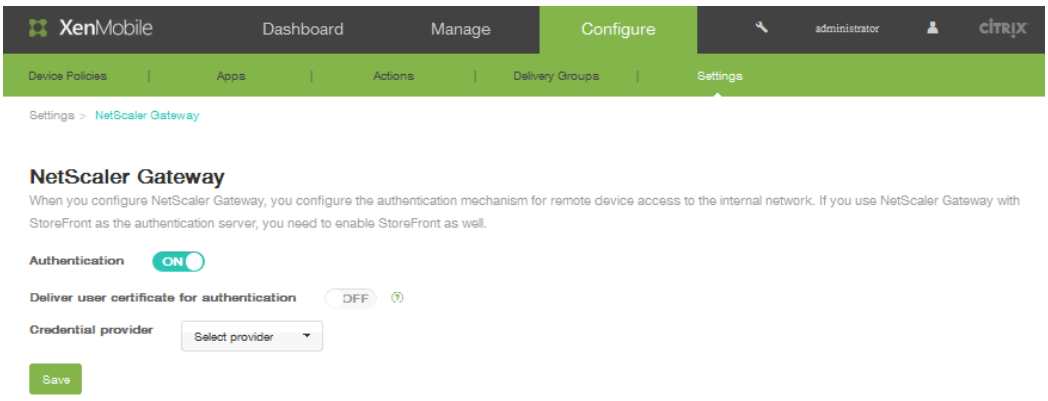


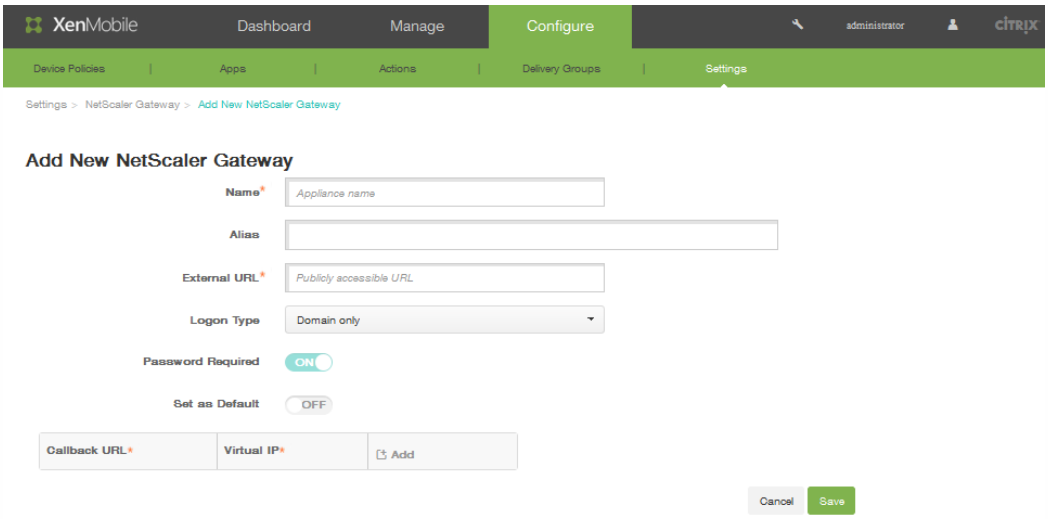
-
-
-
-

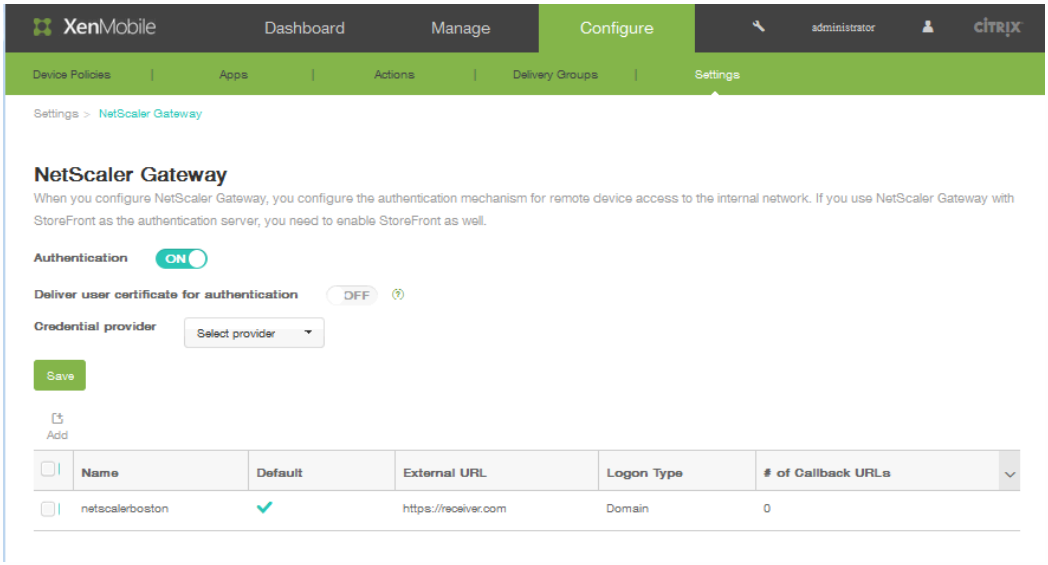
-
-
-
-
-
-

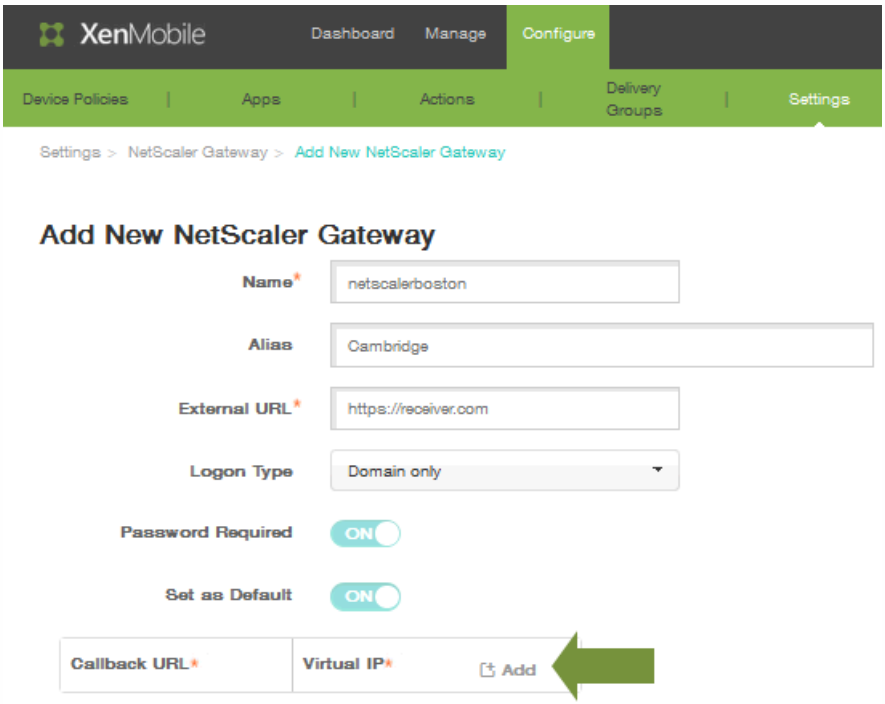
-
-
-











-
-
-
-

-
-

-

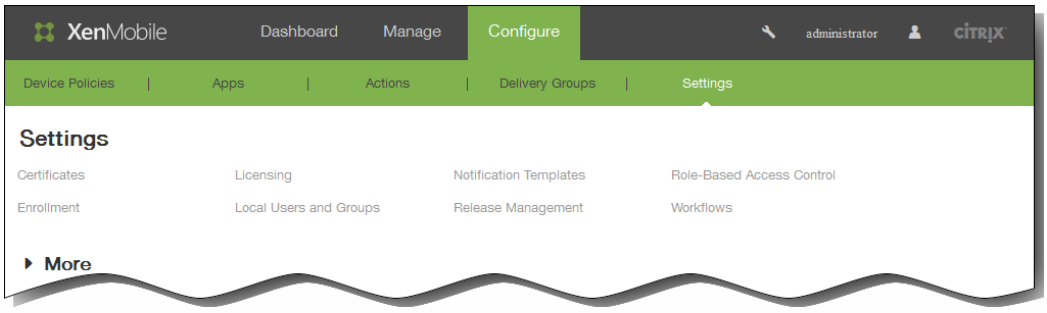
-
-
-
-

-

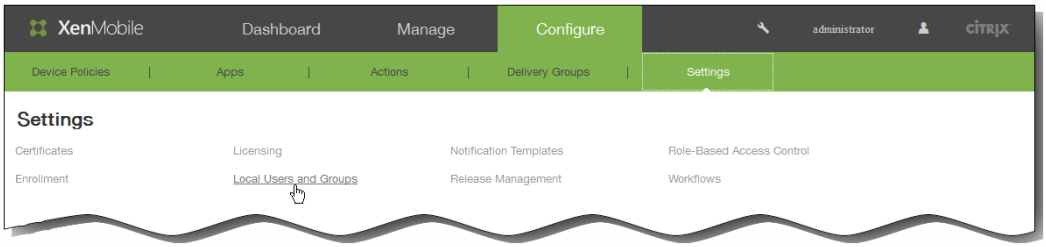
-

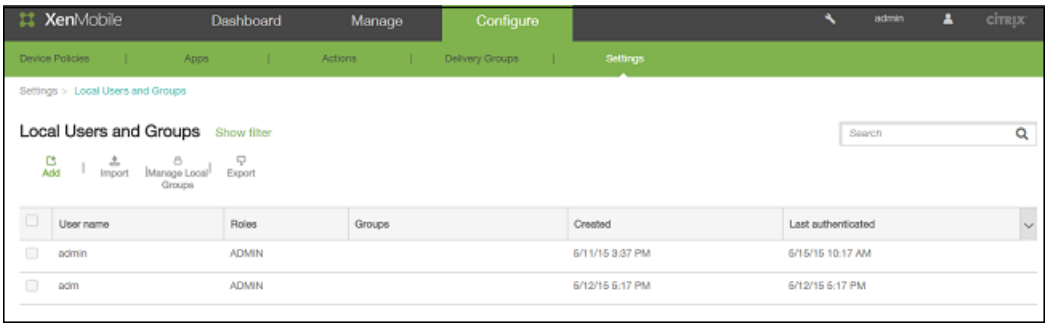
-

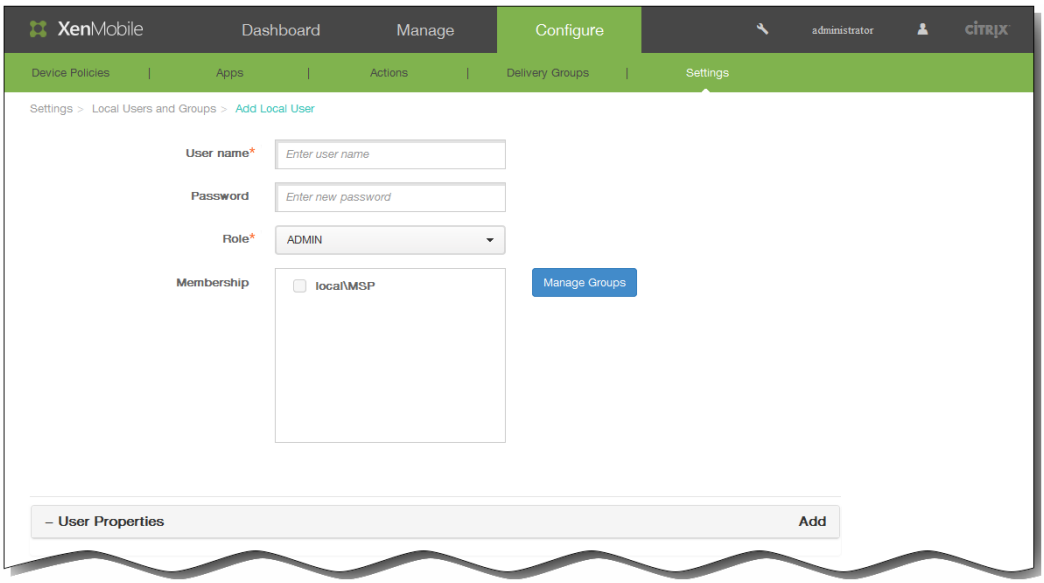
-
-

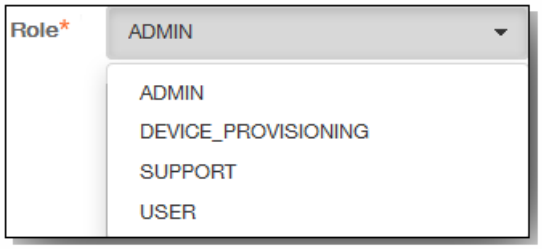


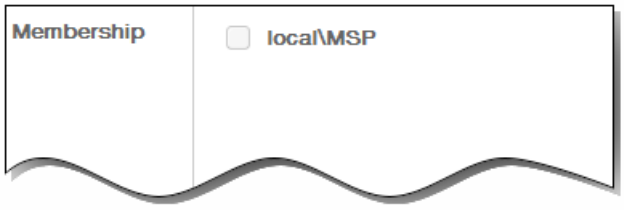
-
  -
  -
  -
-
  -
  -
-
  -
-
  -

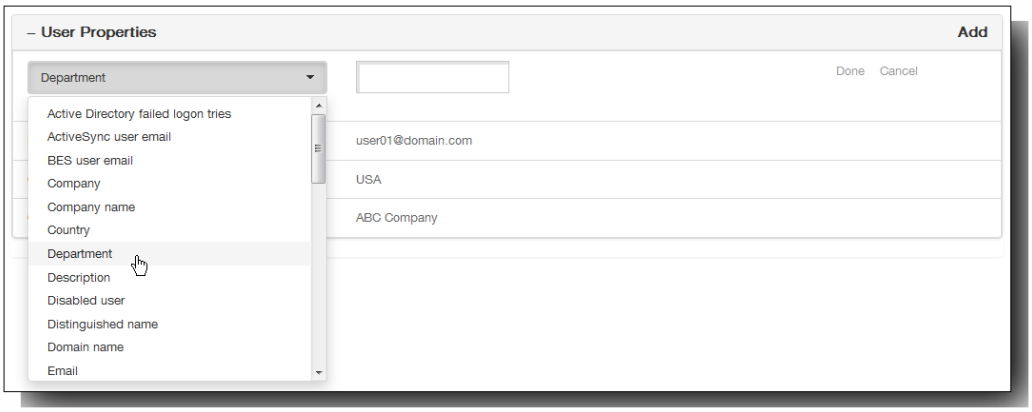


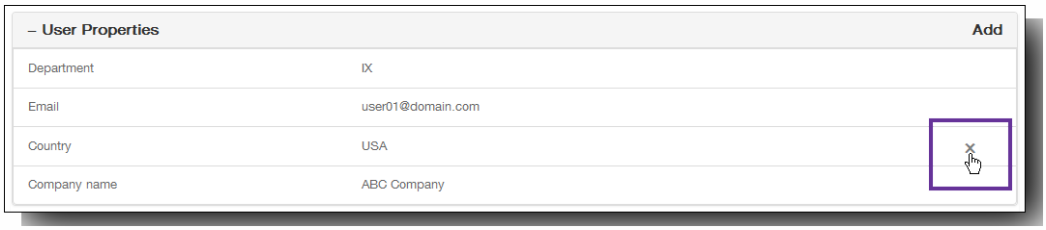


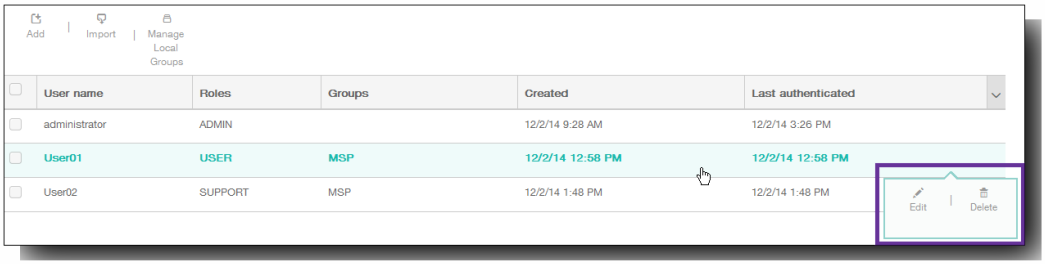


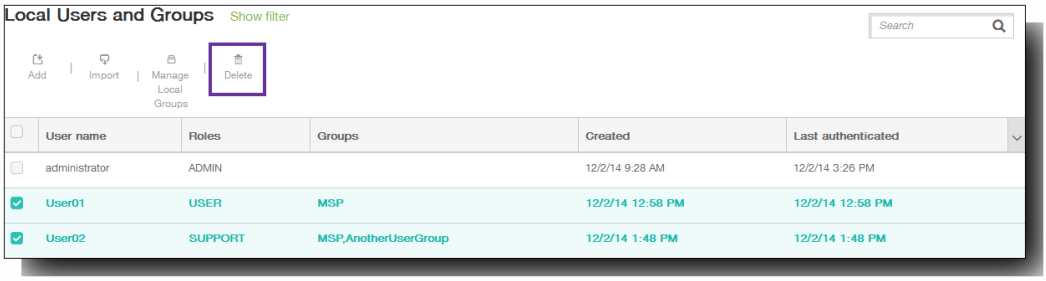


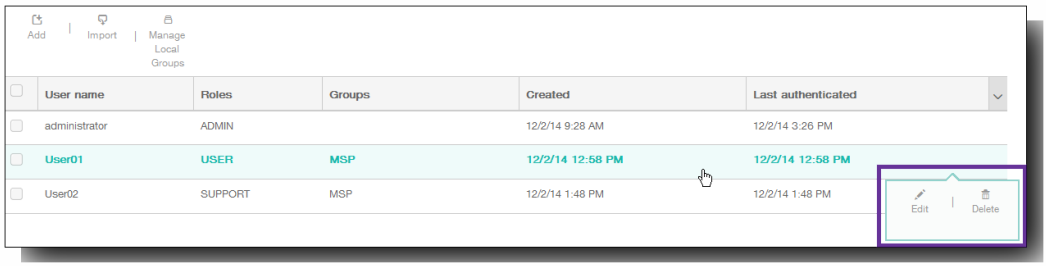




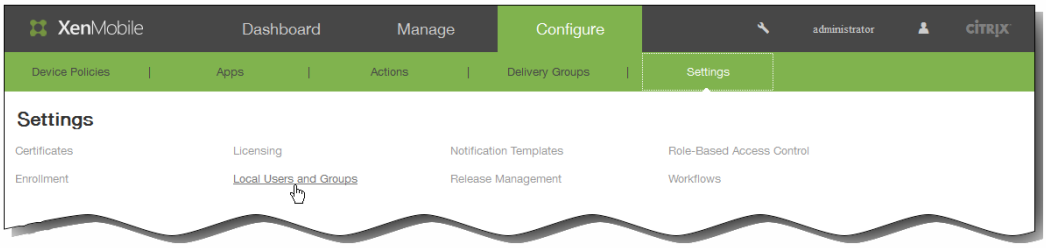


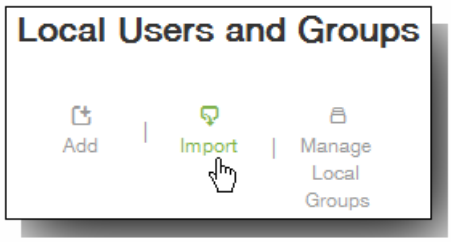


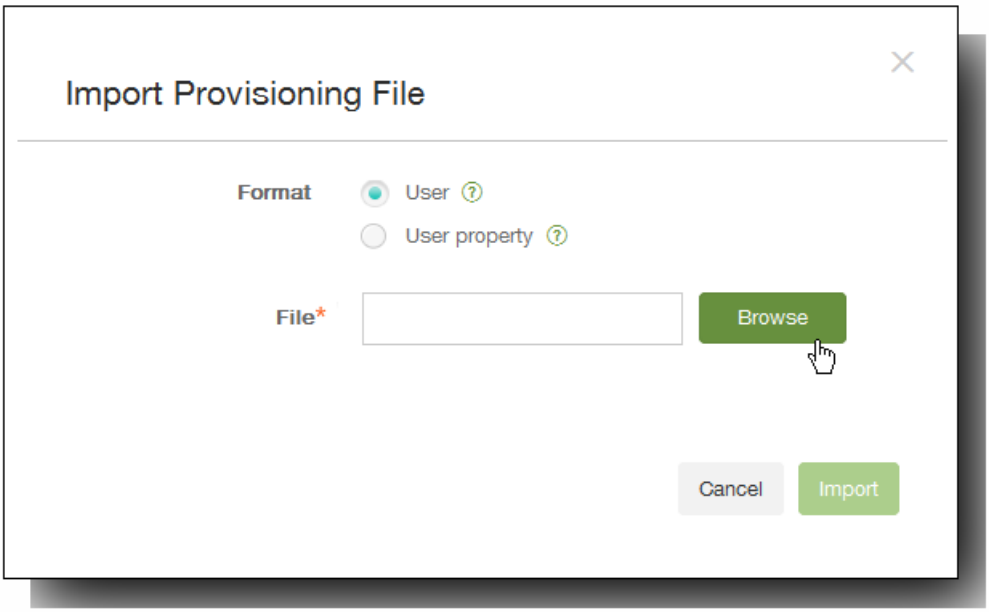
- 

- 

-
-
-







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

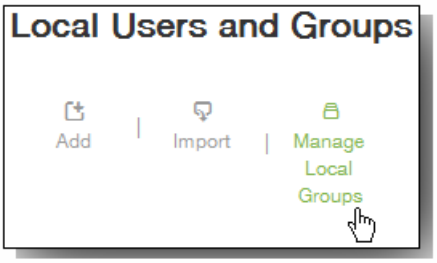
- propertyV;test;1;2 propertyV\;test\;1\;2
-
-
-

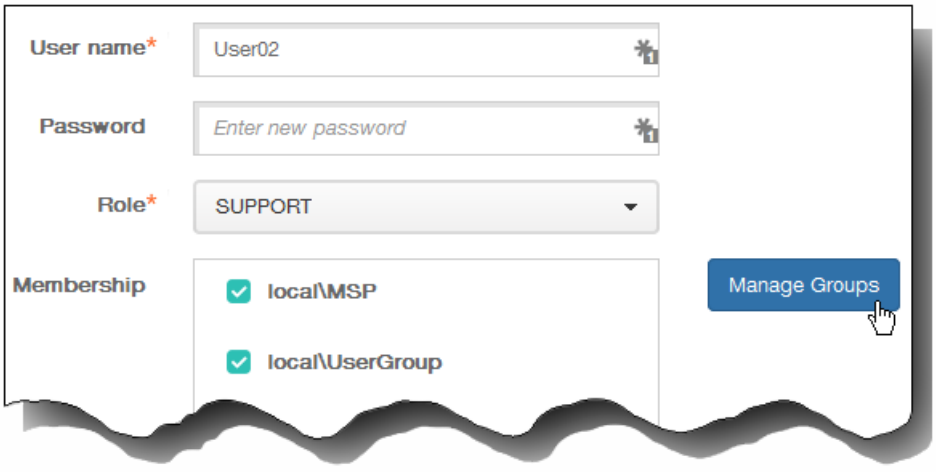
user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01

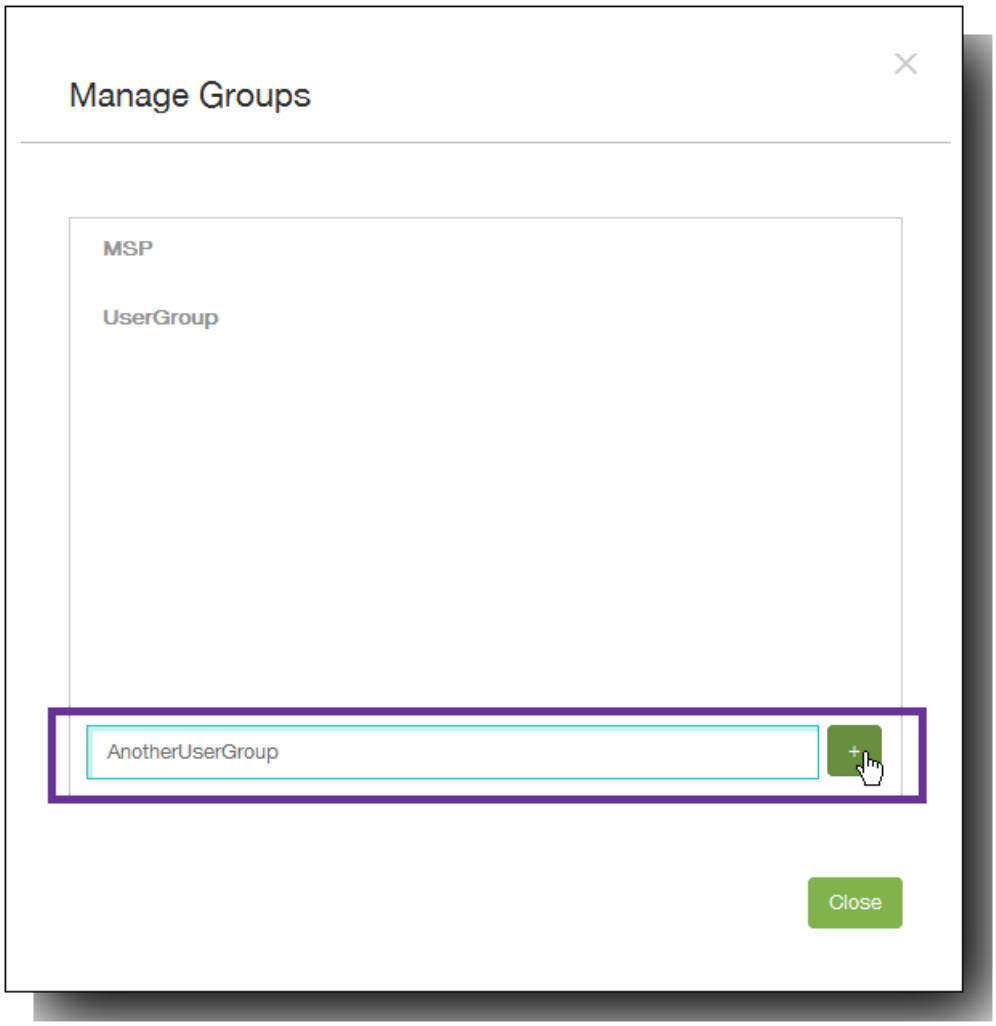
-
-
-
-
  -
  -
  -

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

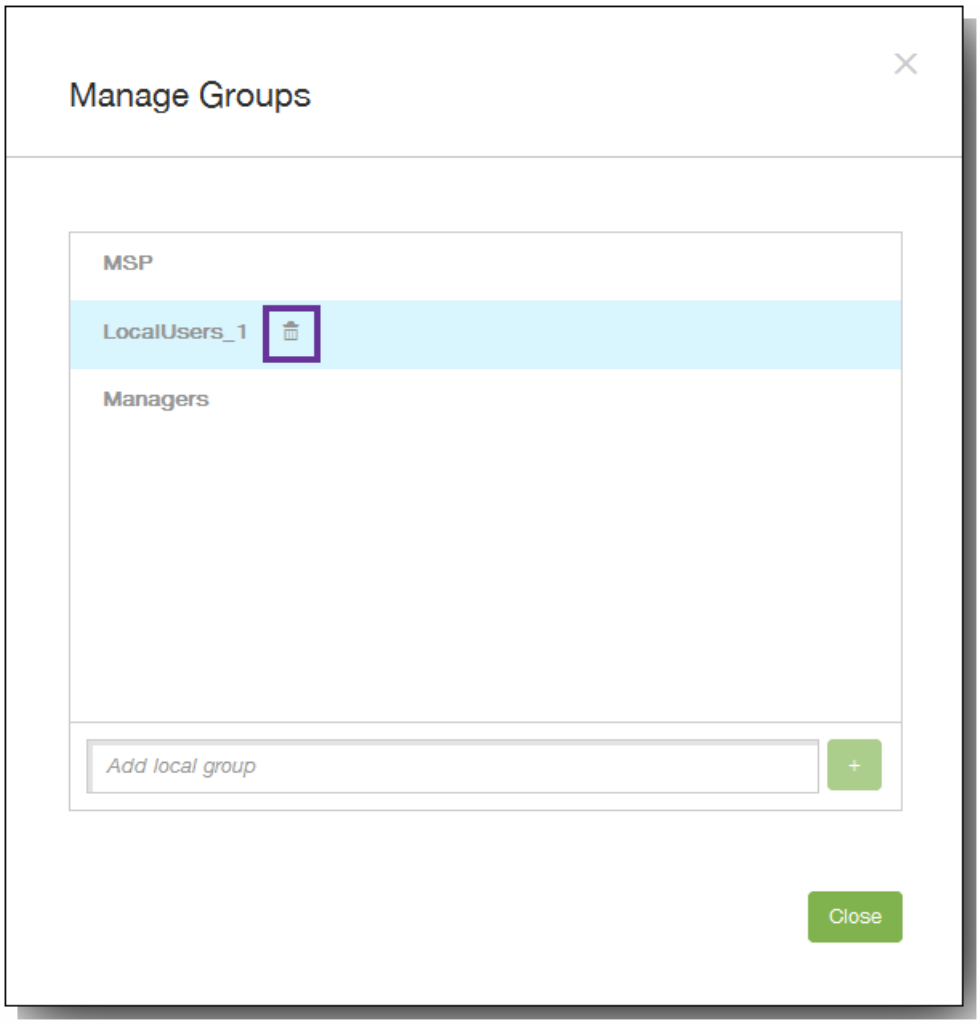
-
-
  -
  -
-
  -
  -

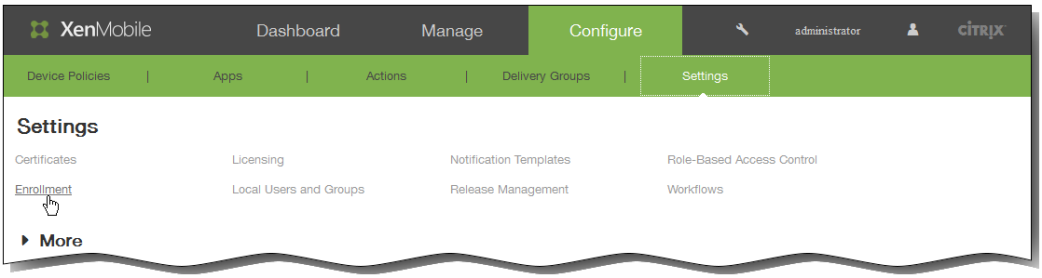
- 

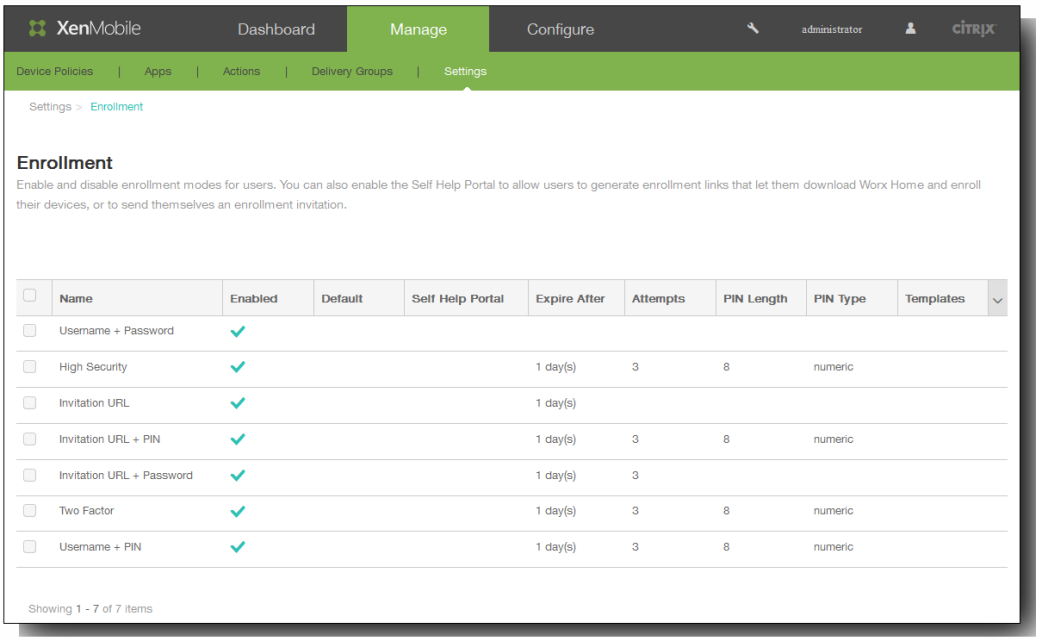
- 

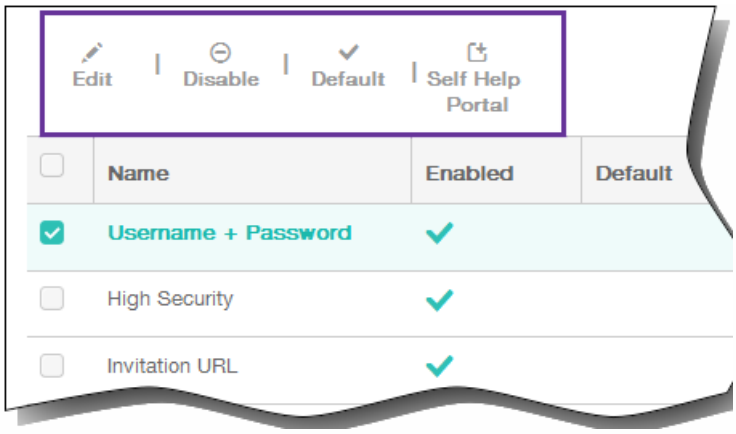


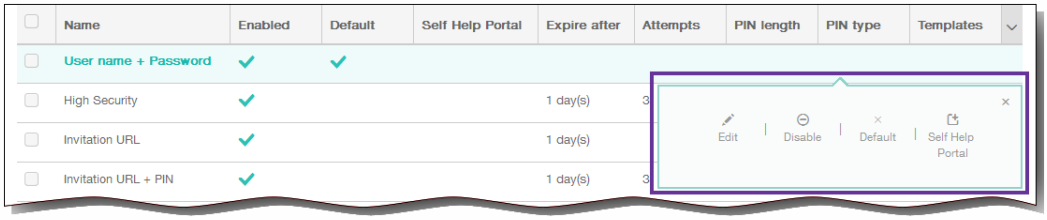
-
-

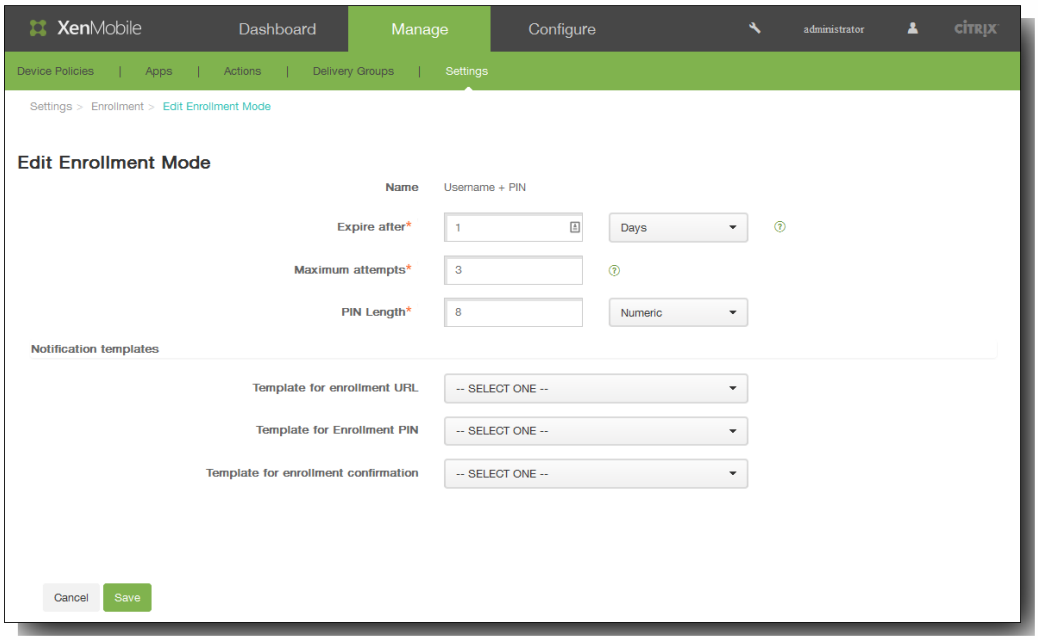


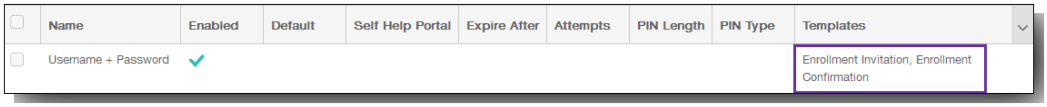




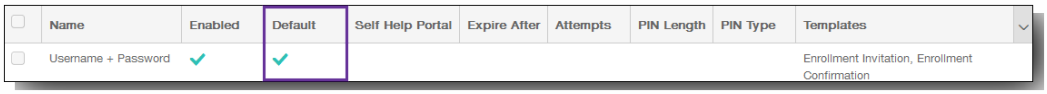




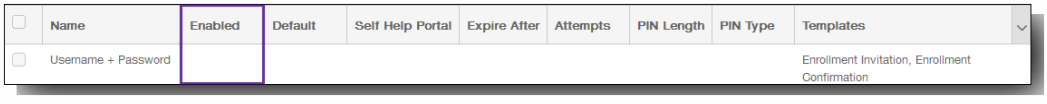




Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
Username + Password	✓							Enrollment Invitation, Enrollment Confirmation

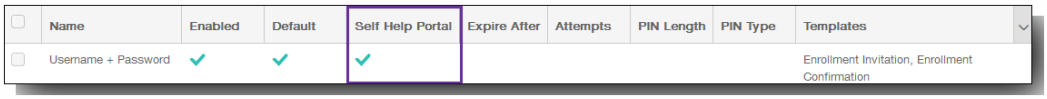


Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
Username + Password	✓	✓						Enrollment Invitation, Enrollment Confirmation



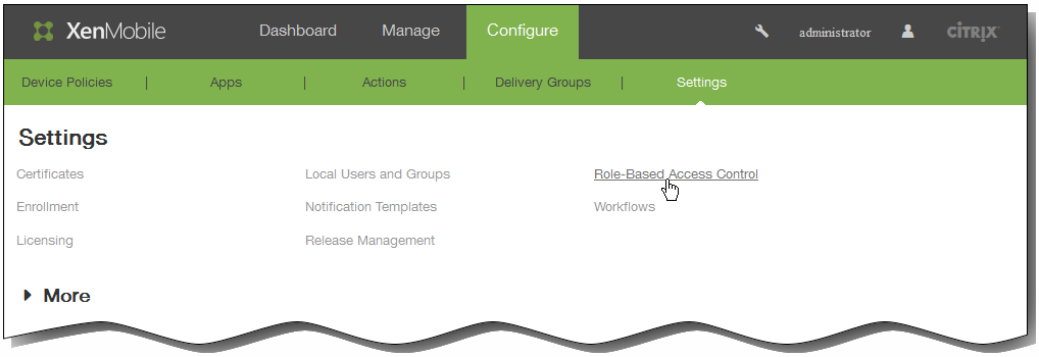
Name	Enabled	Default	Self Help Portal	Expire After	Attempts	PIN Length	PIN Type	Templates
Username + Password								Enrollment Invitation, Enrollment Confirmation

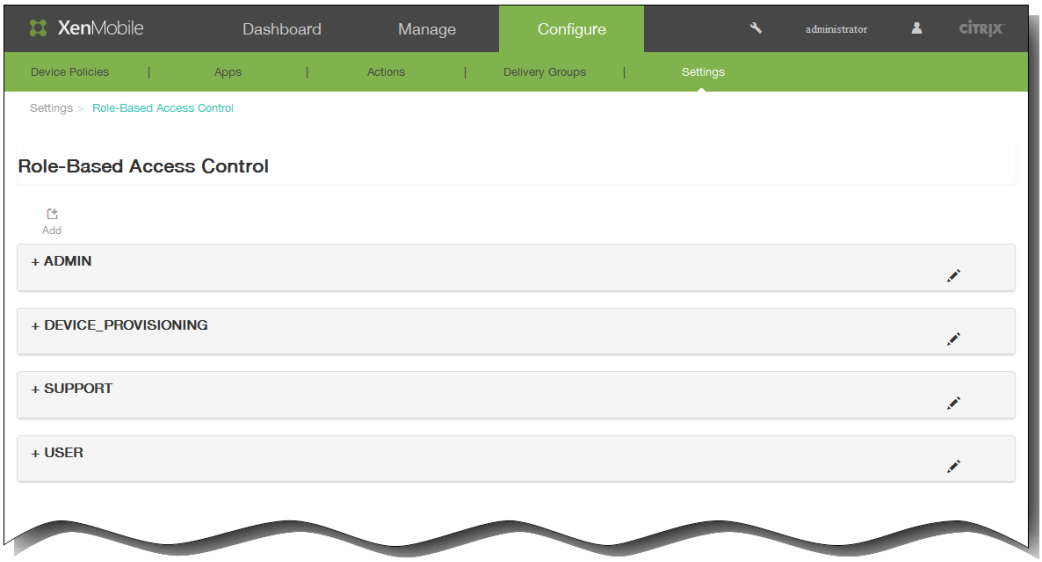
-

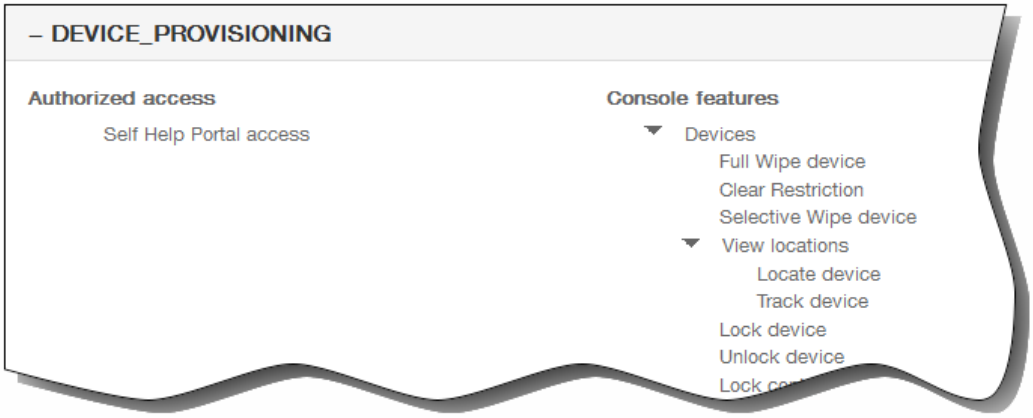
- 

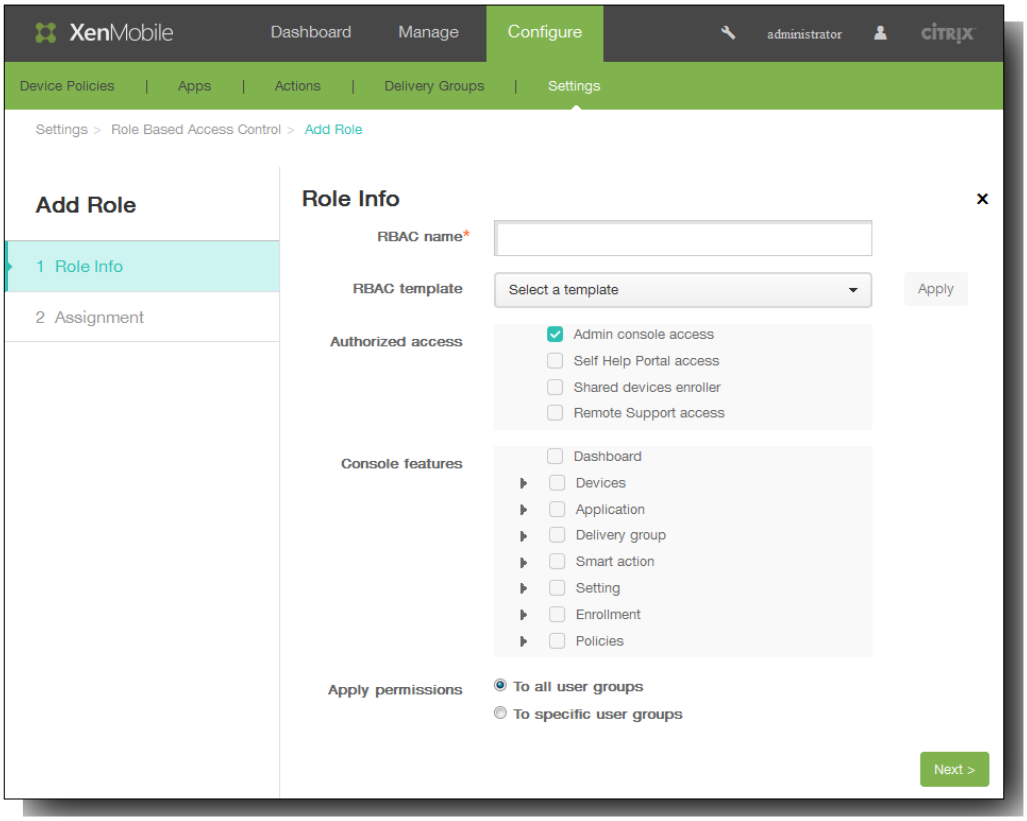
-
-
-

-
-
-

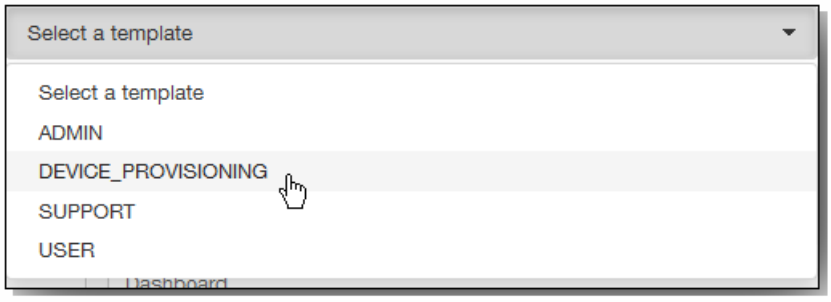




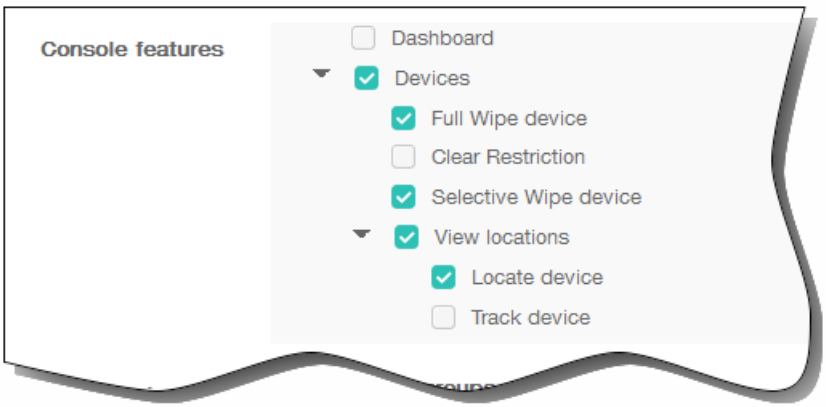


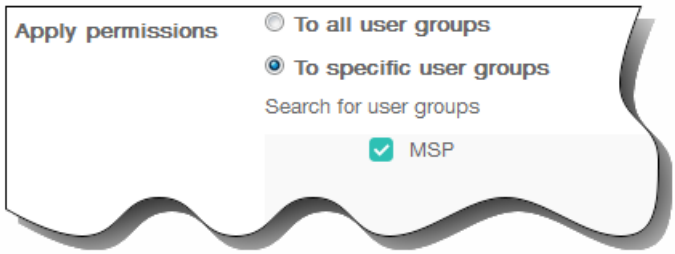


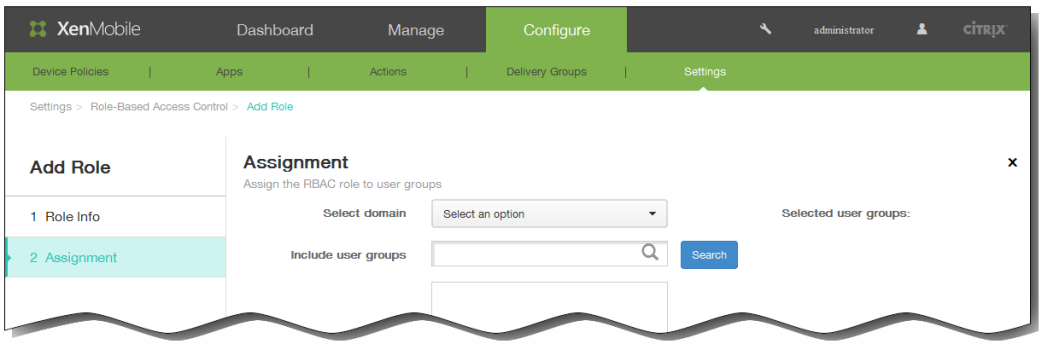
-

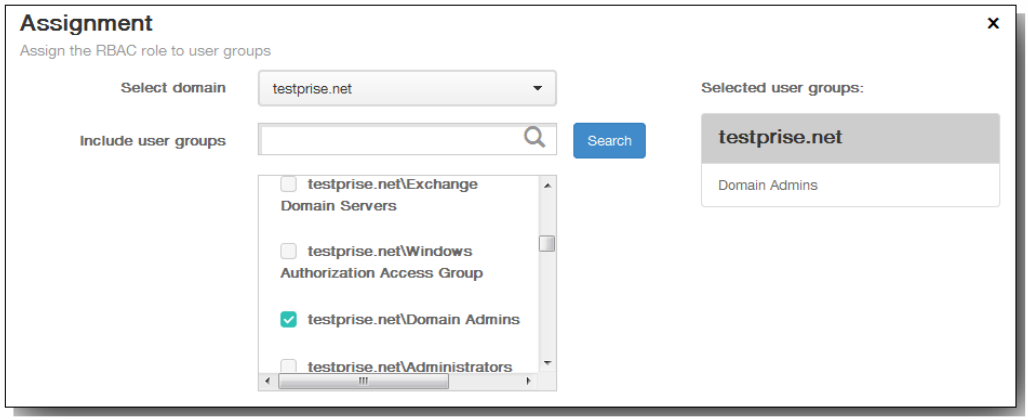


-
-





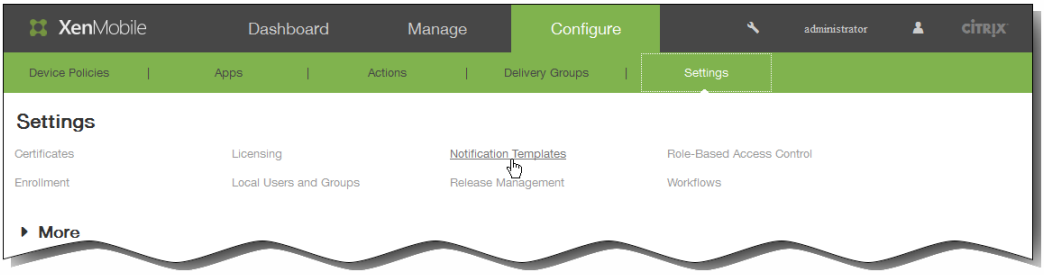




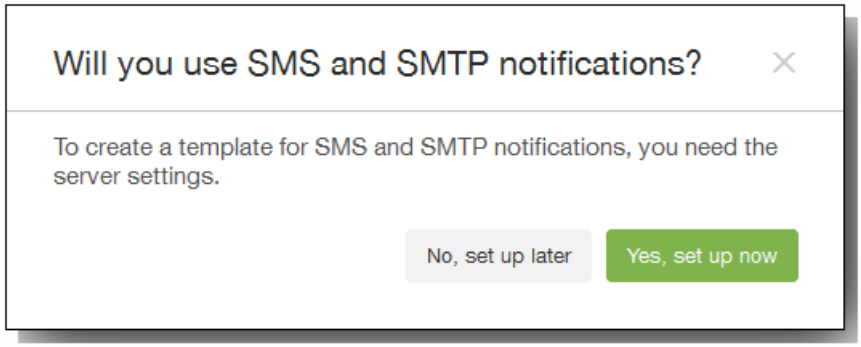
-
-

-
-
-
-
-
-
-

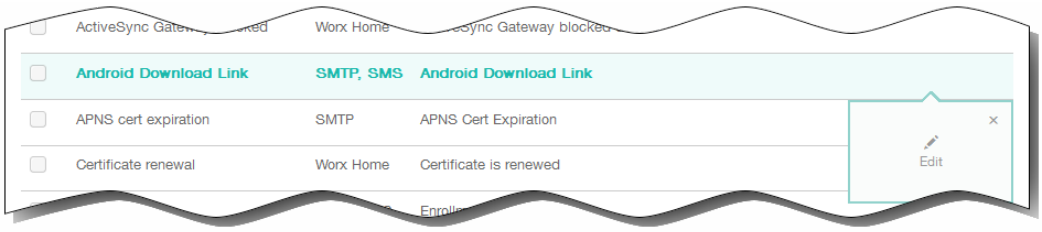
-
-

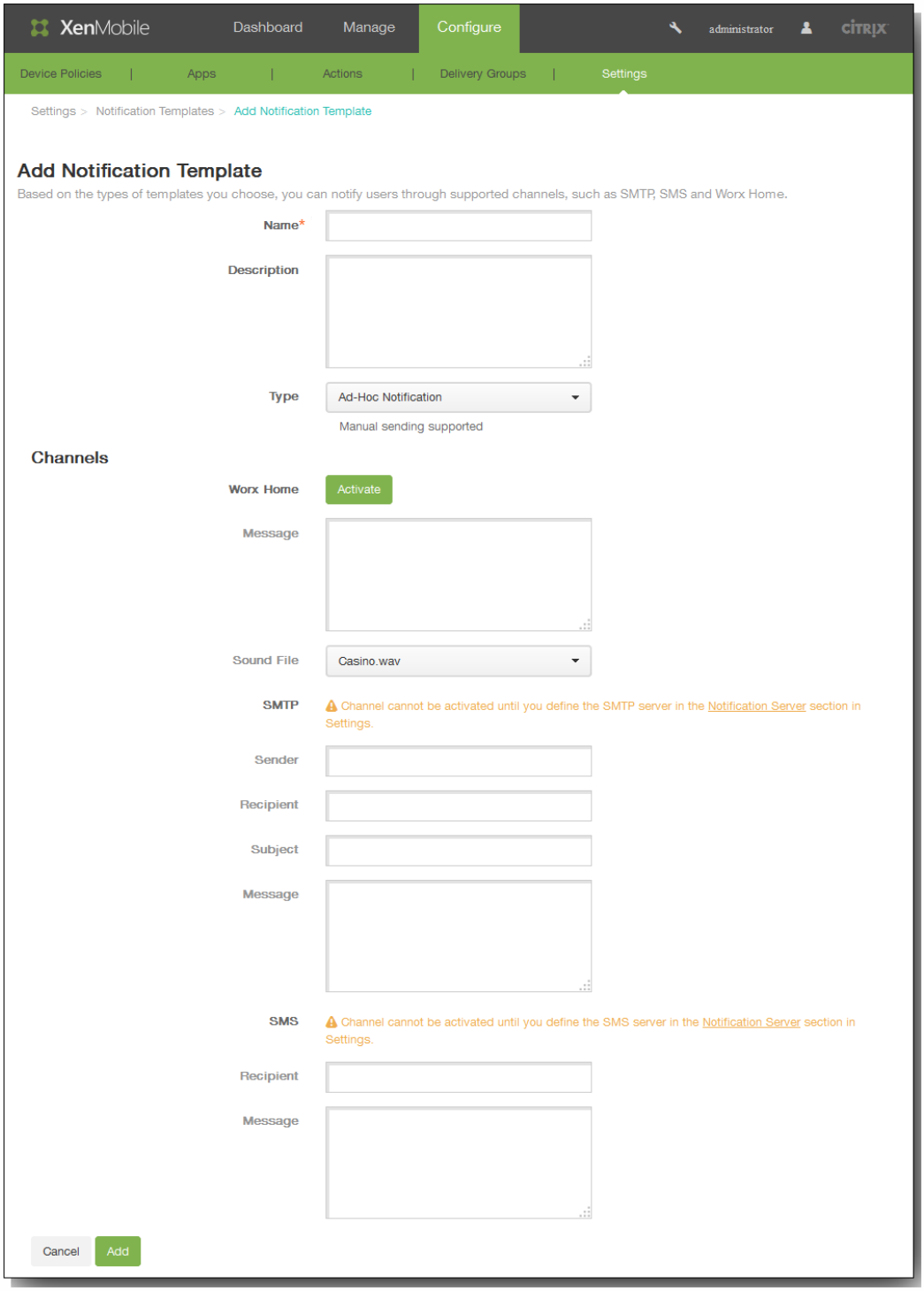


-



-
  -
  -
  -





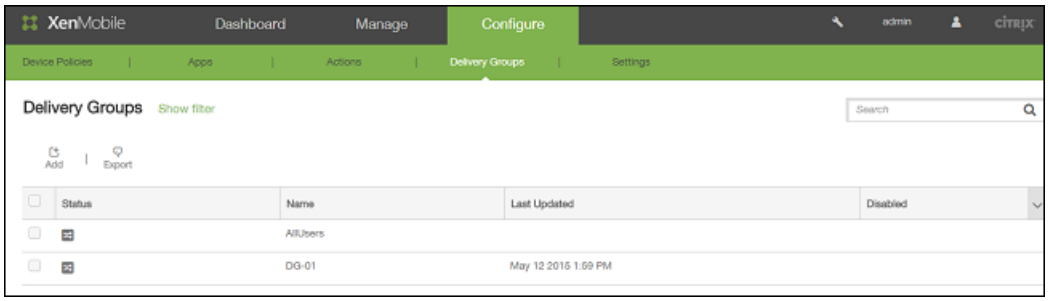
-
-

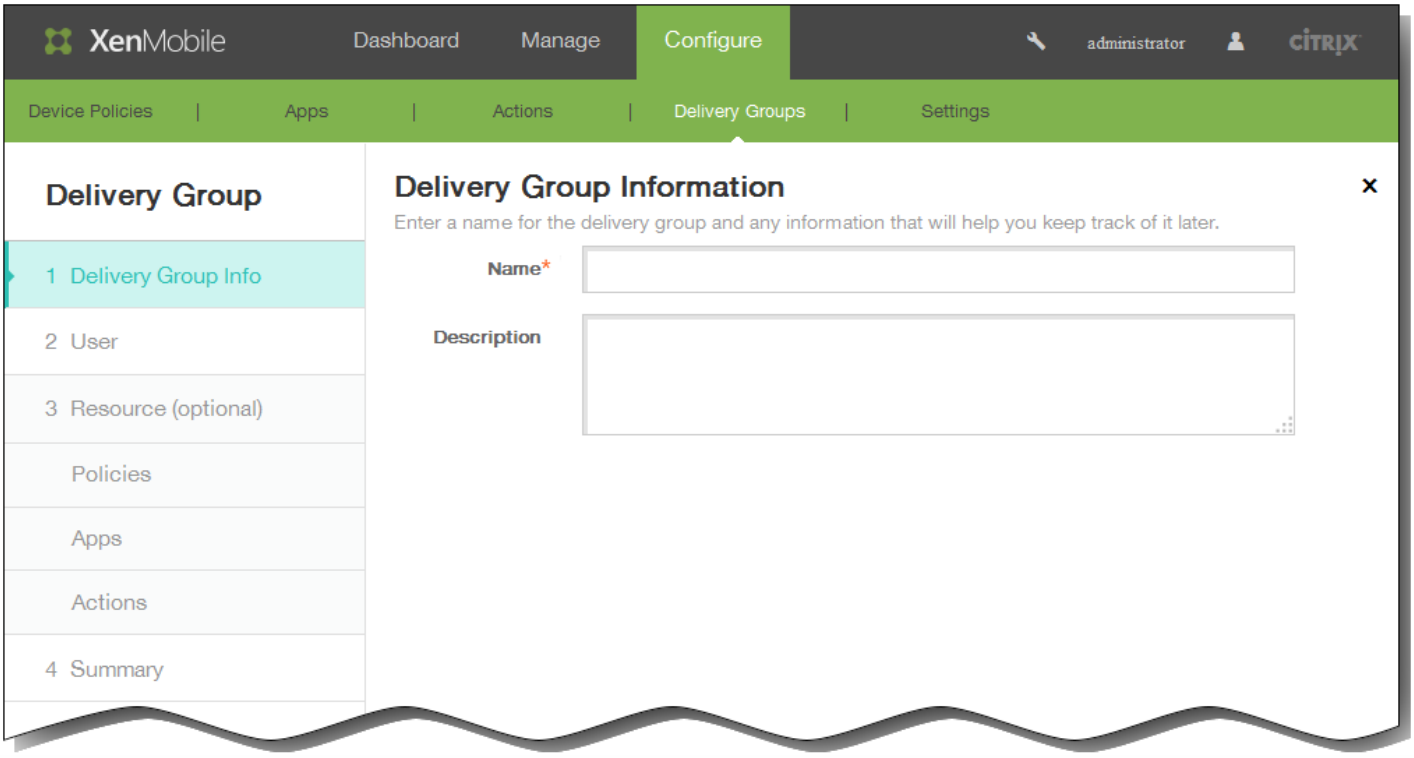
-
-
-

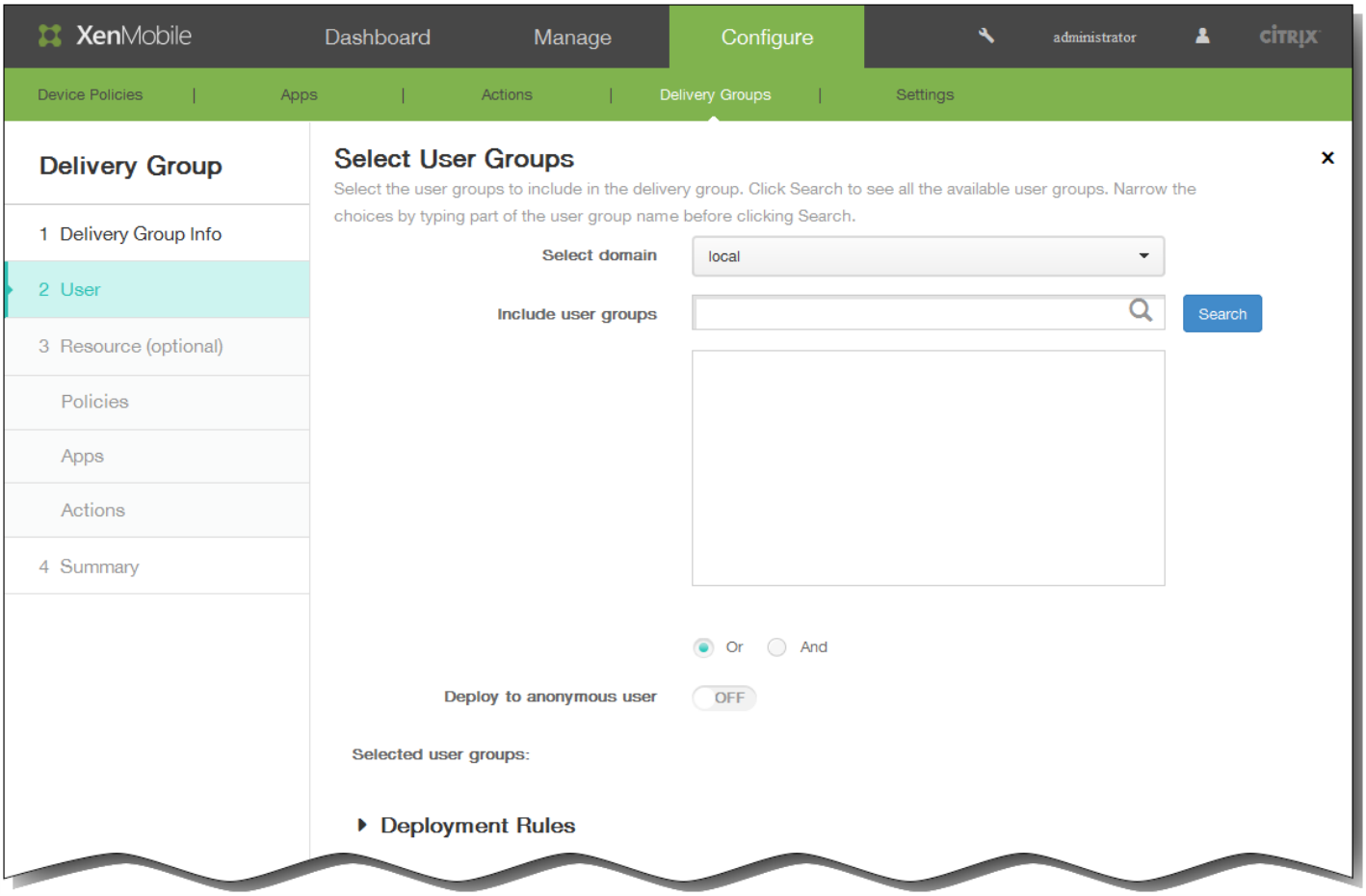
-
-
-

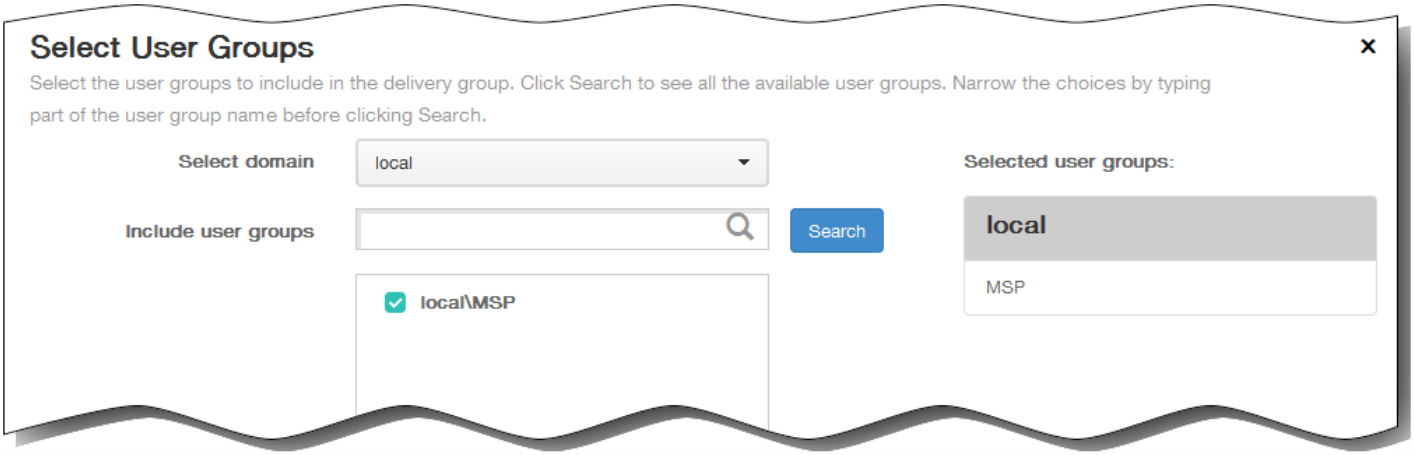
-
-

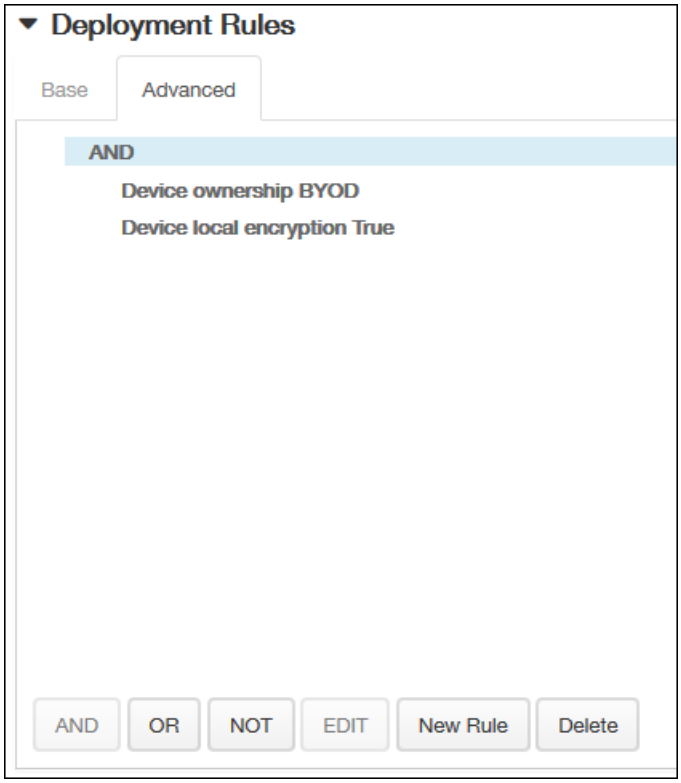
-
-

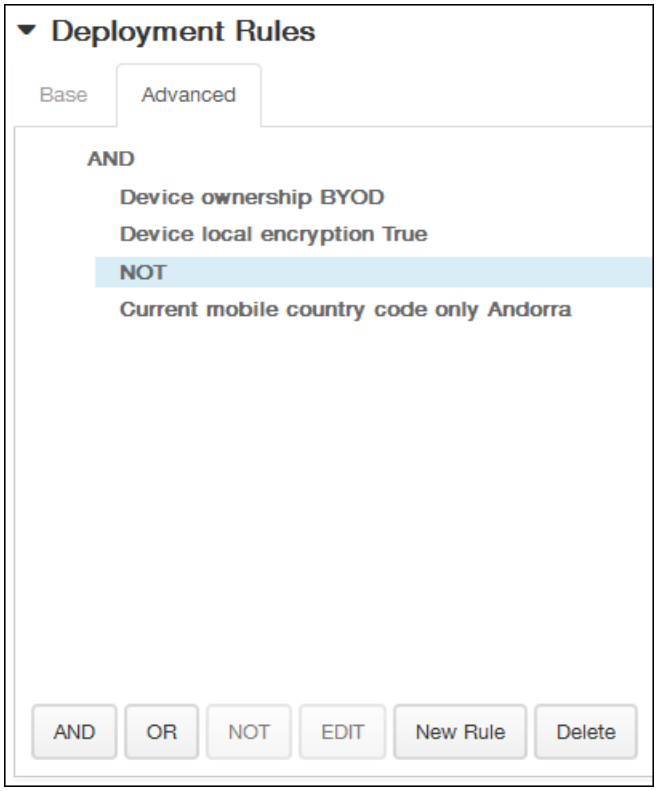


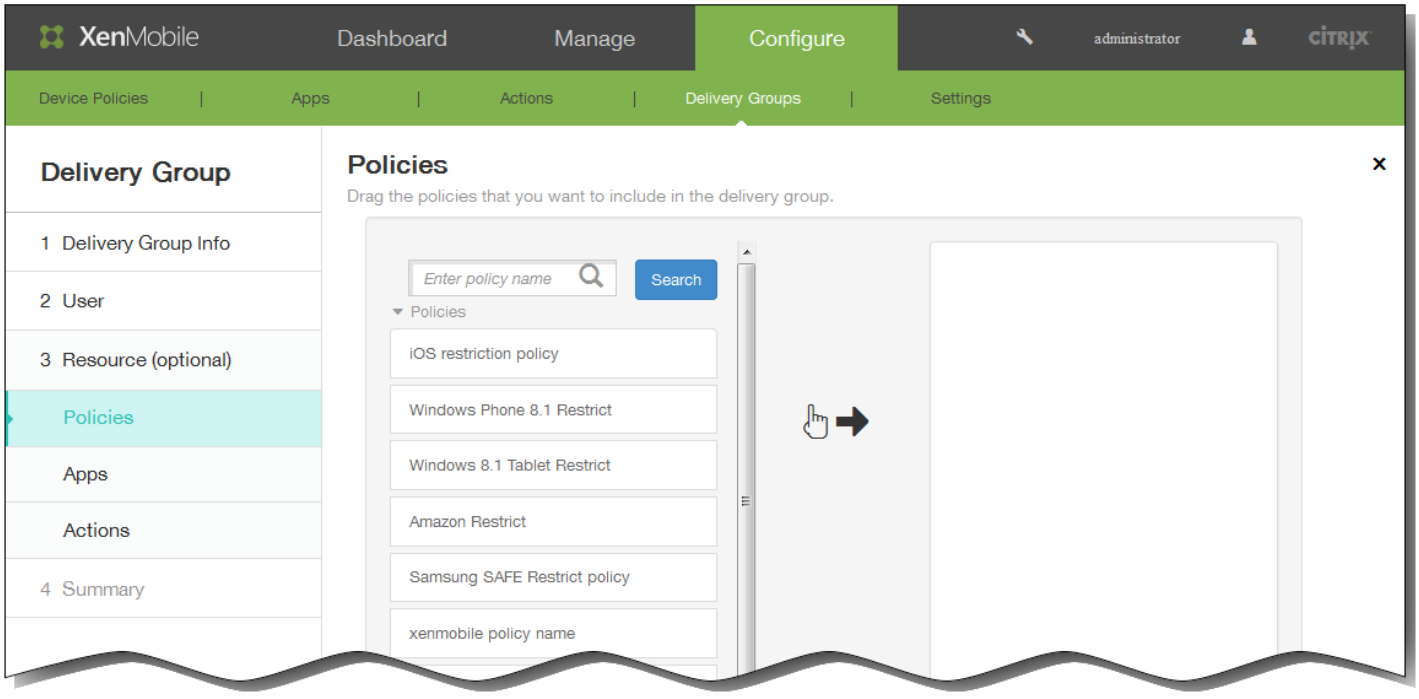


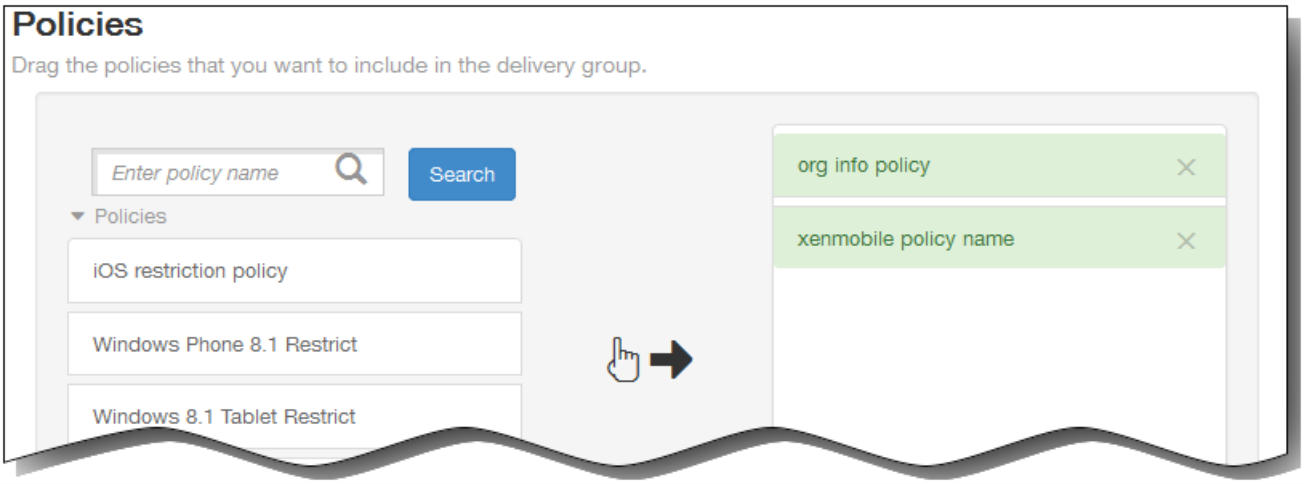


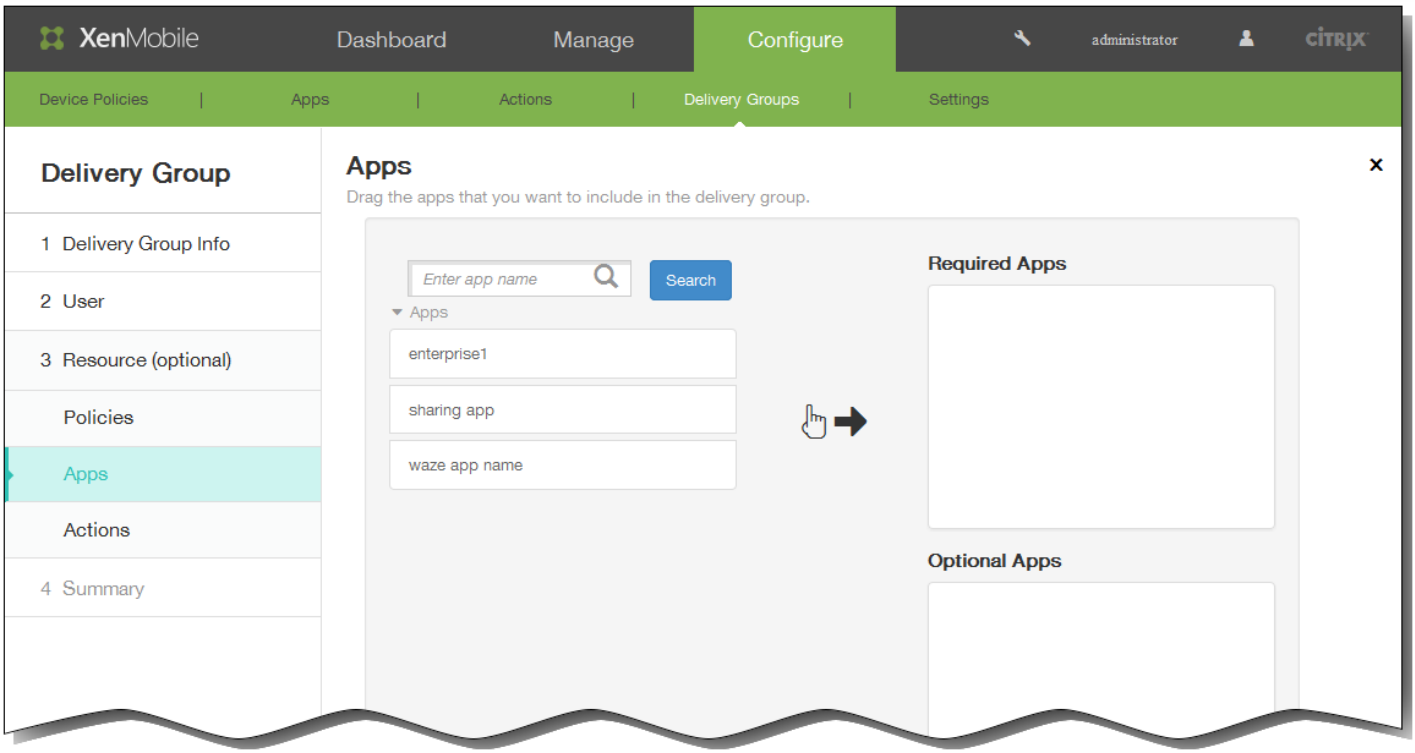


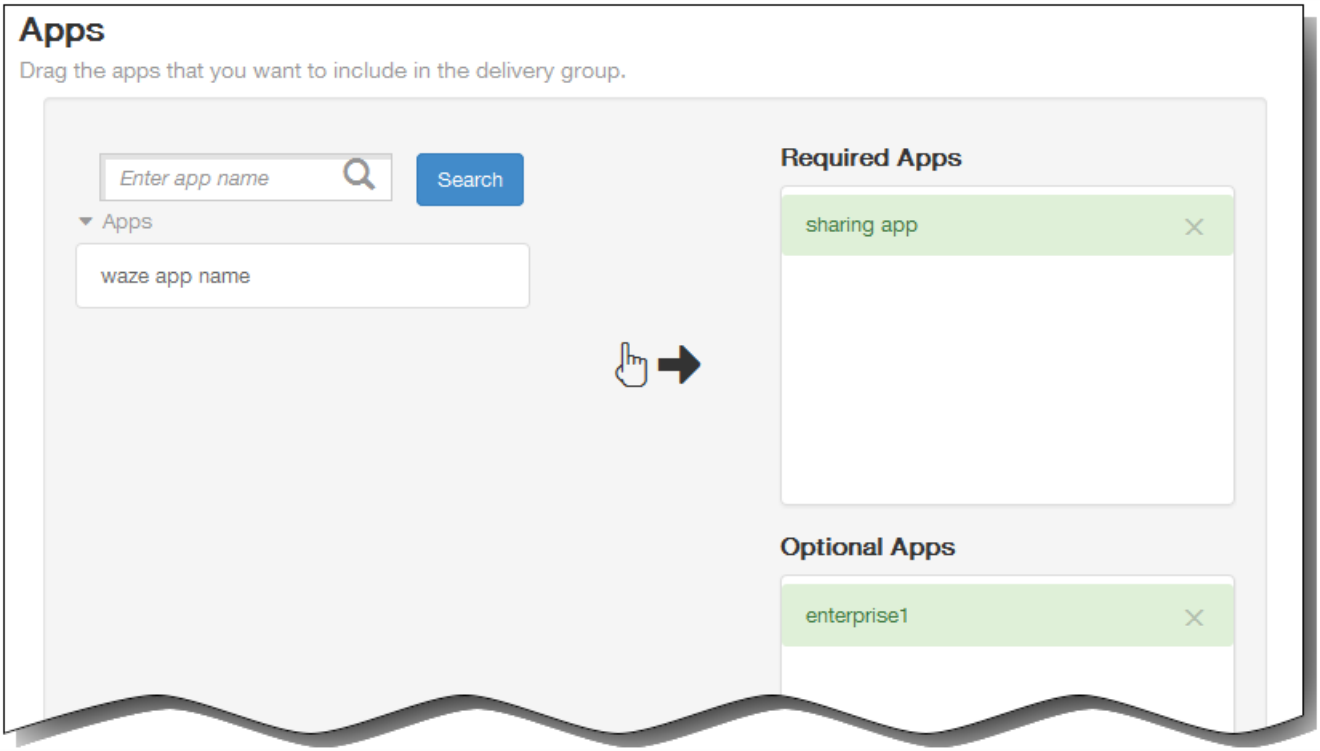


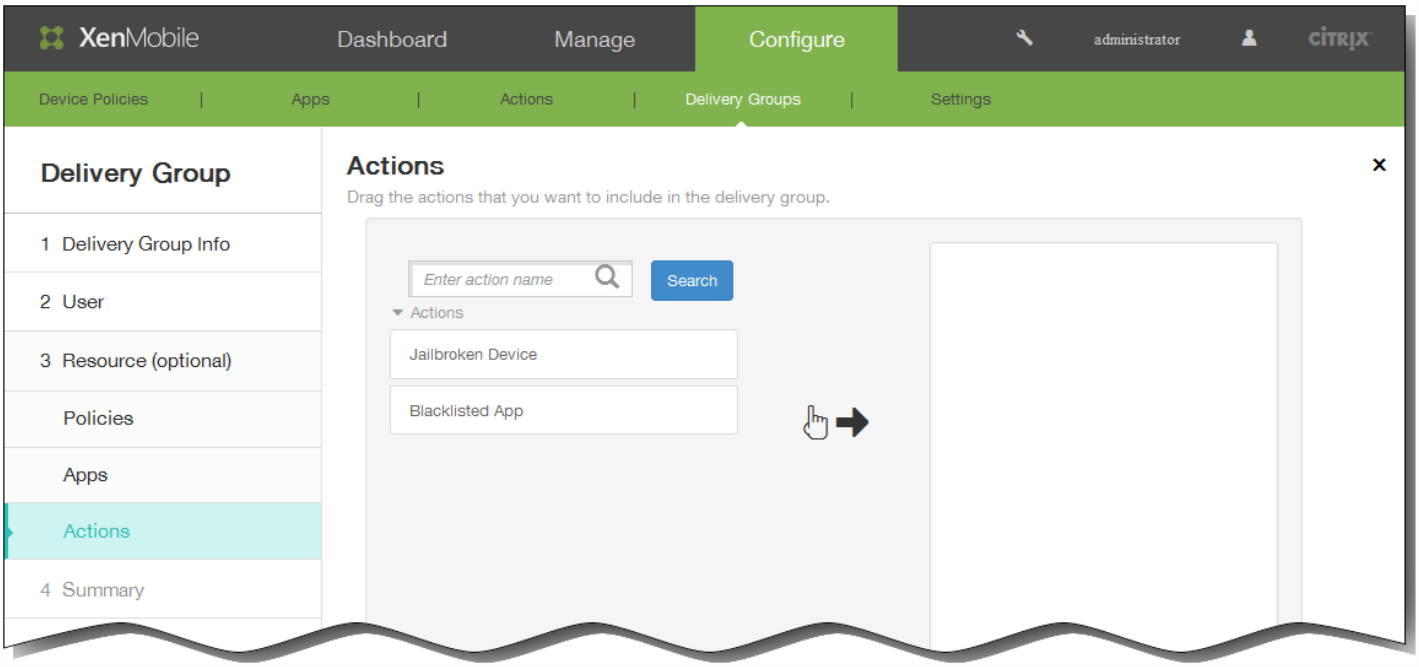


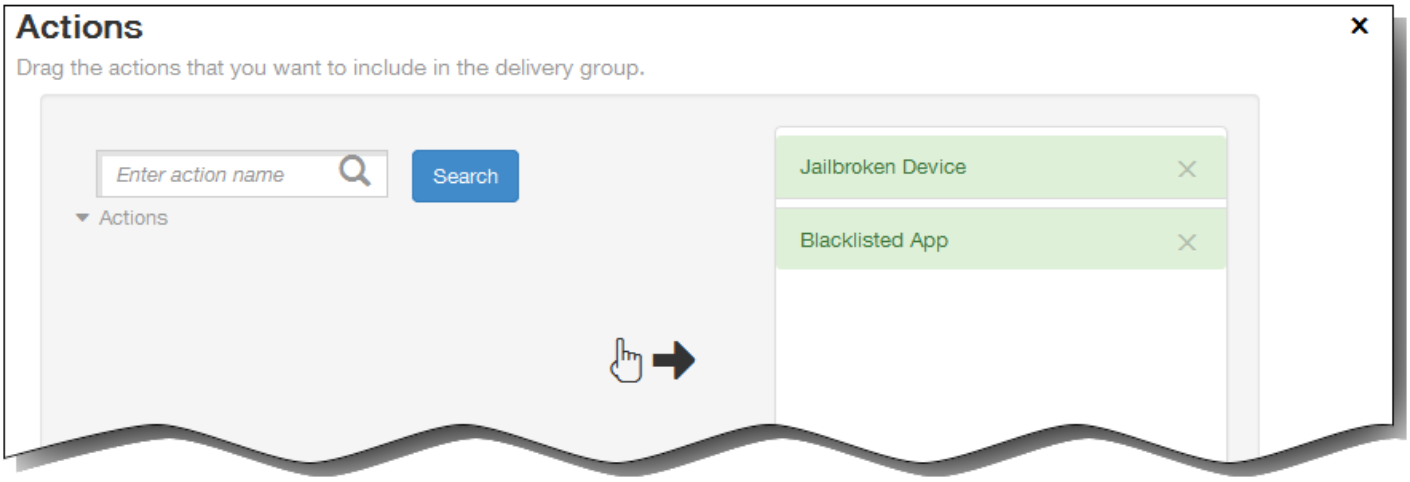


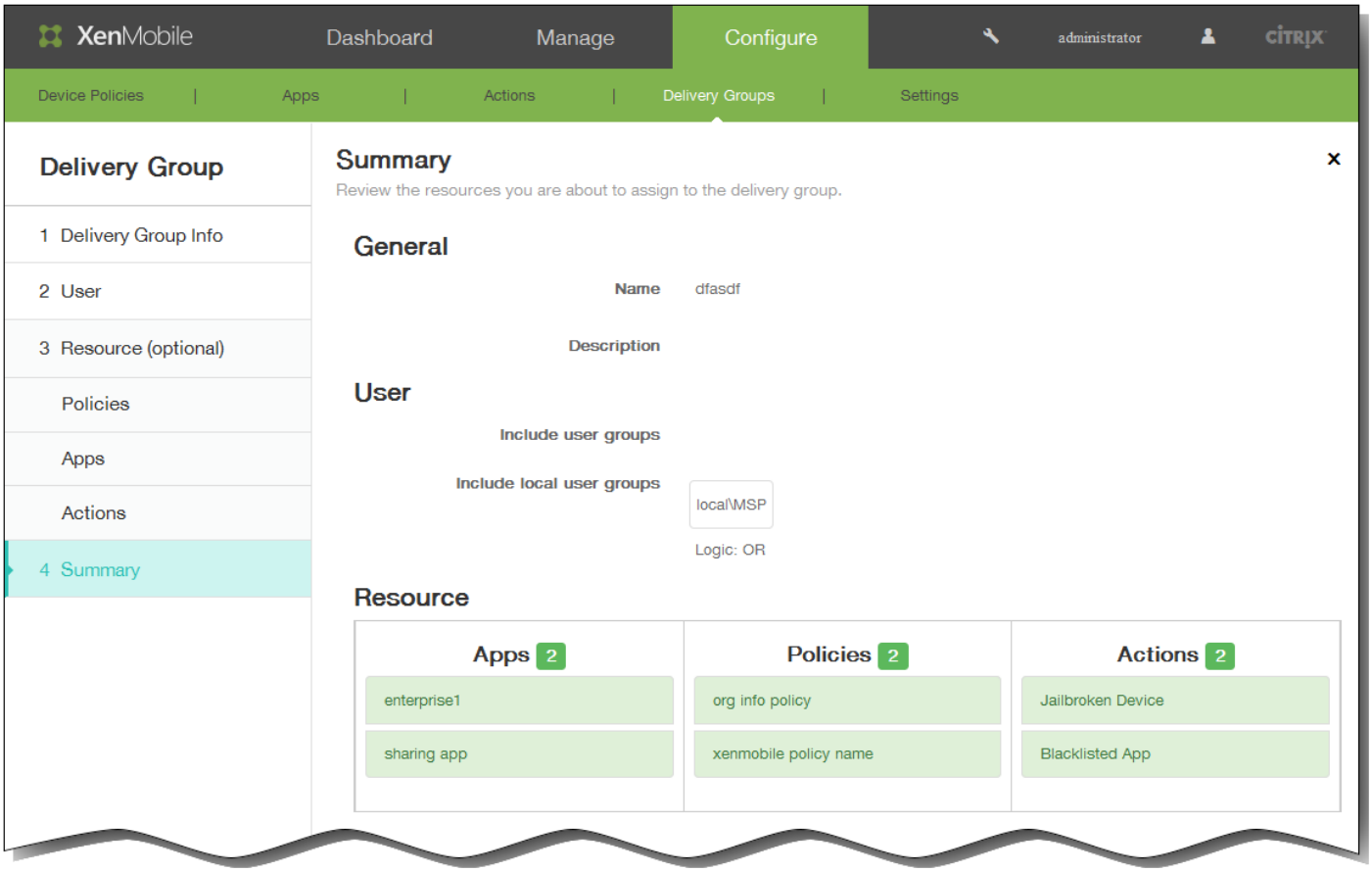


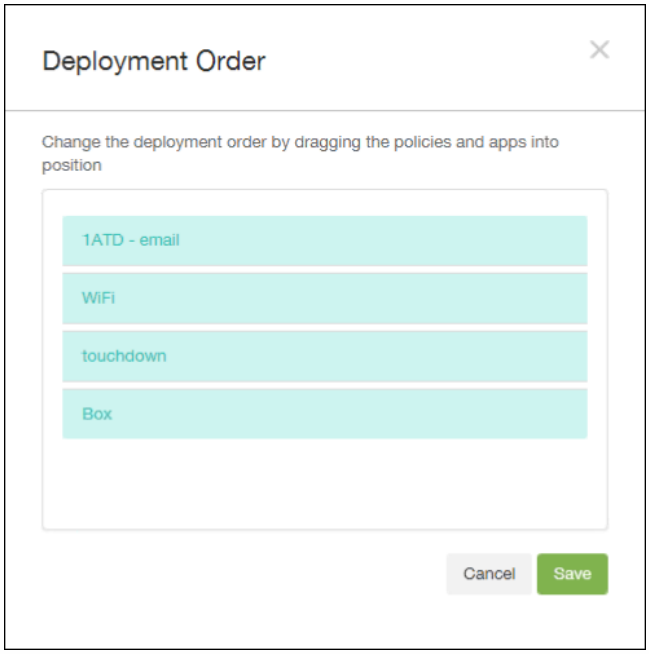


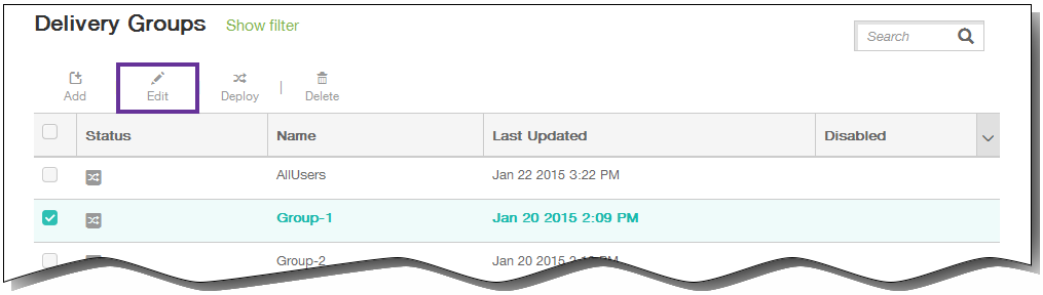


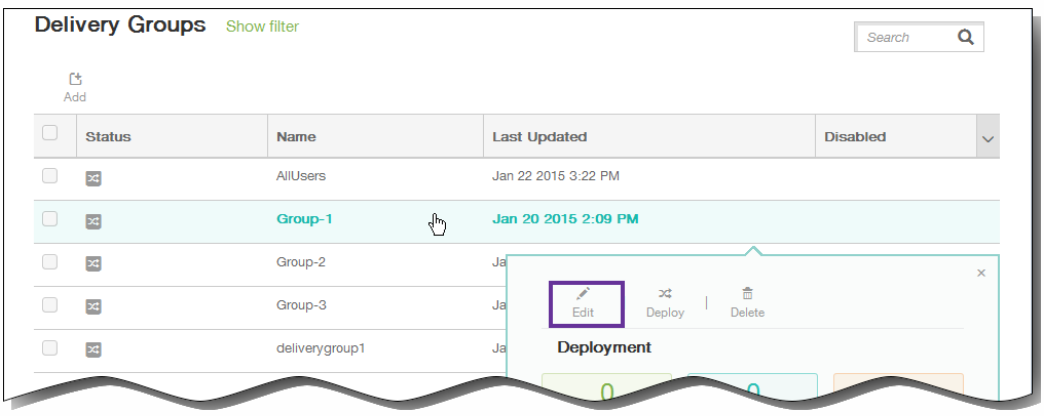


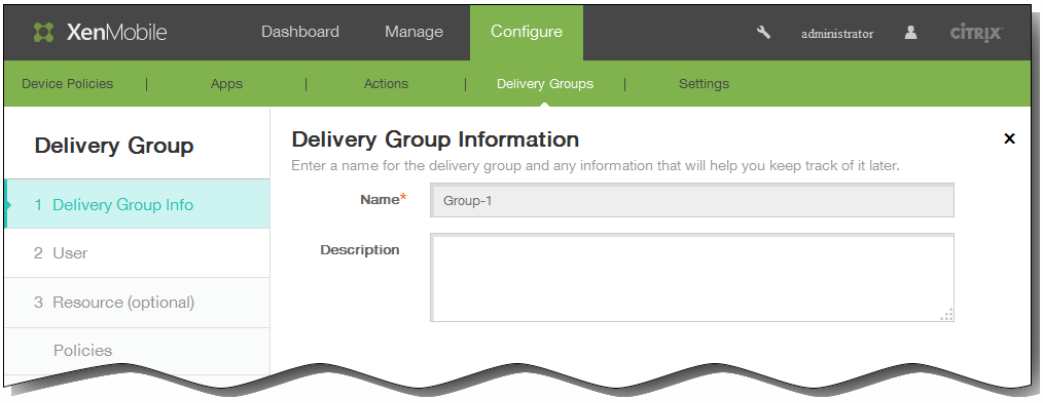


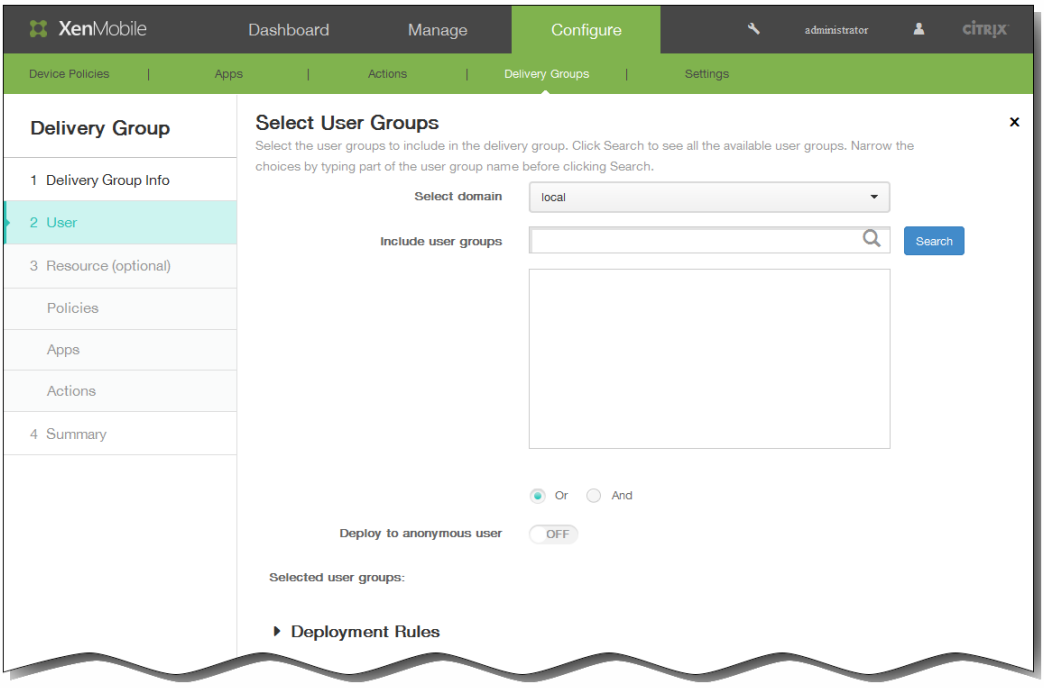




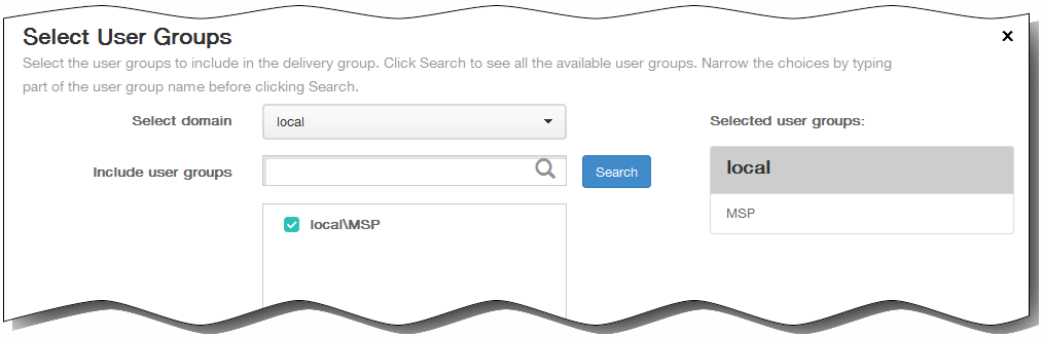


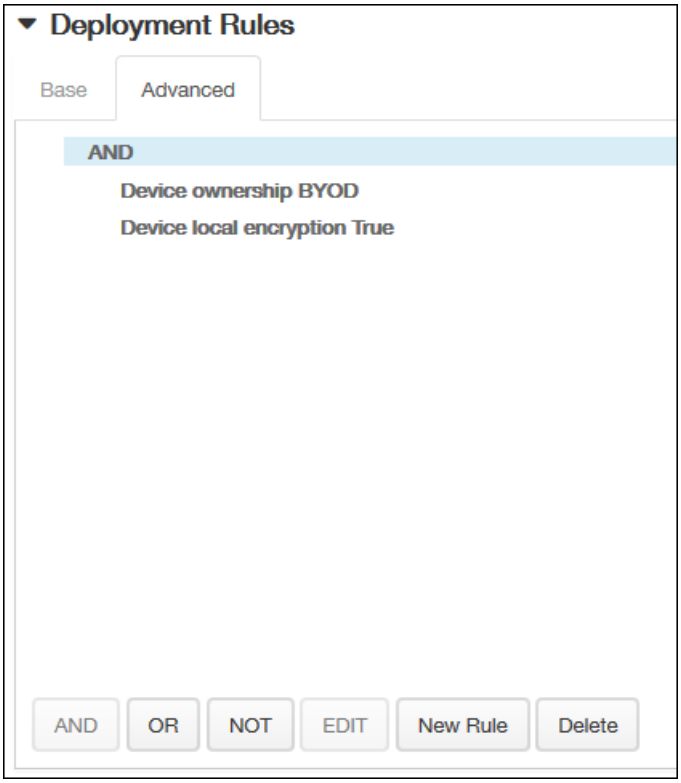


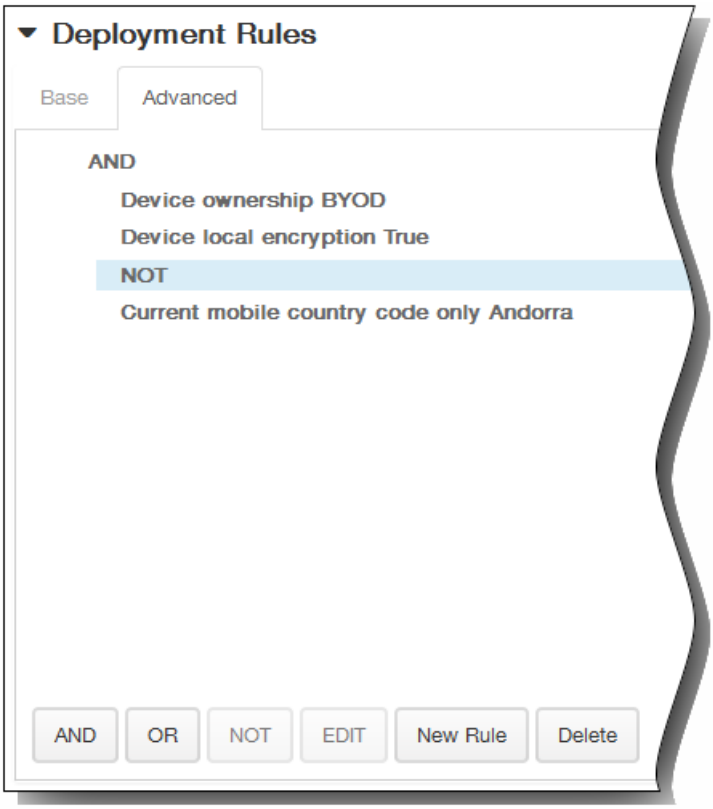


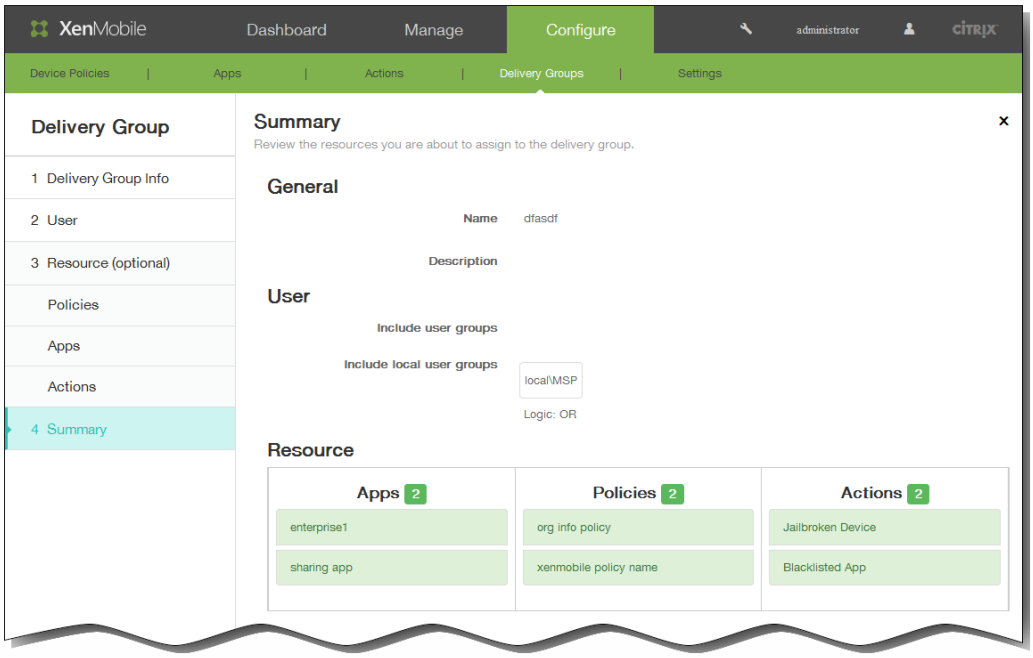


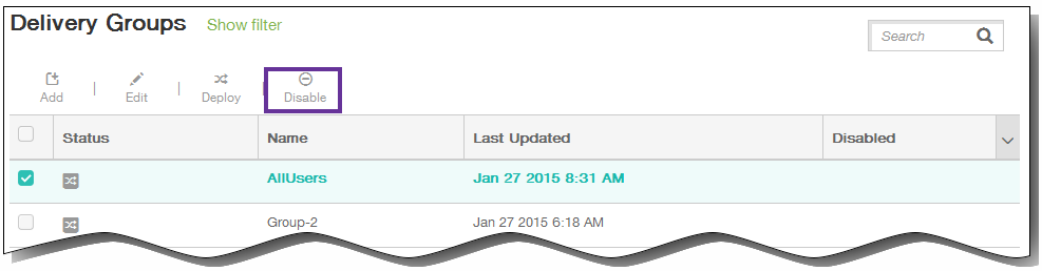
-
-

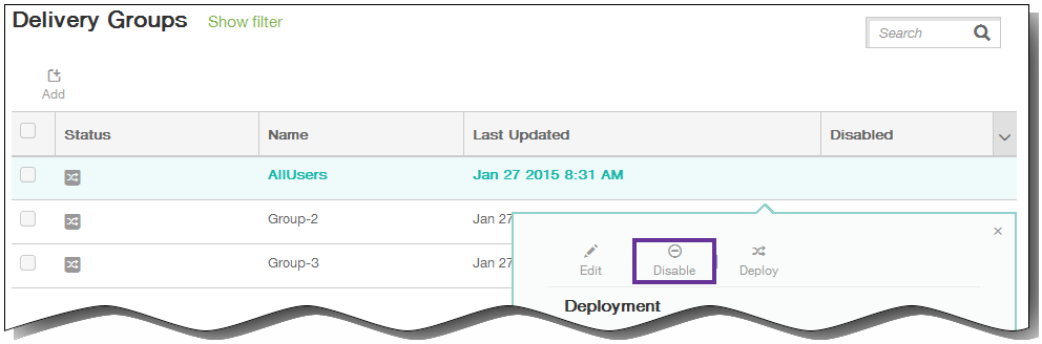




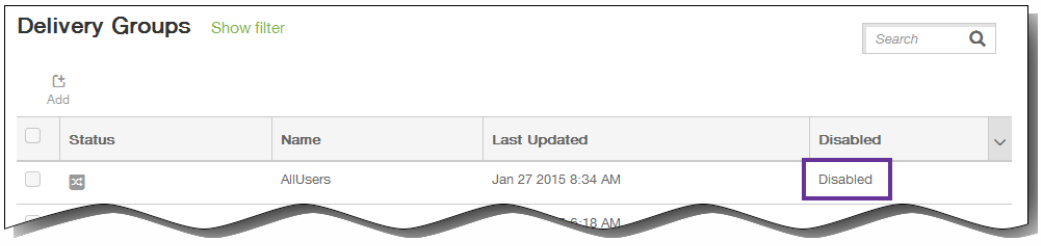






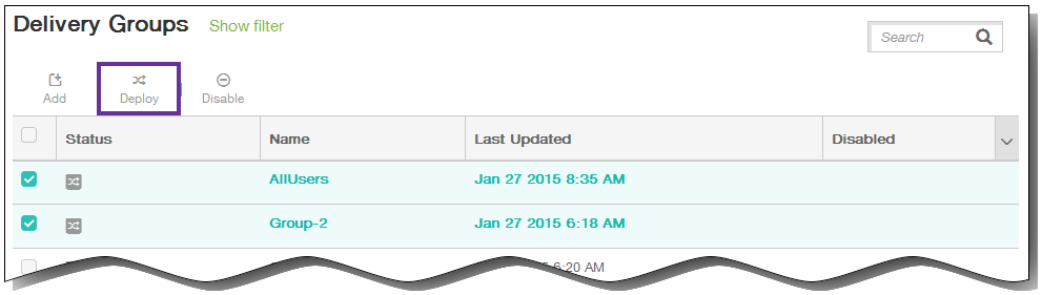


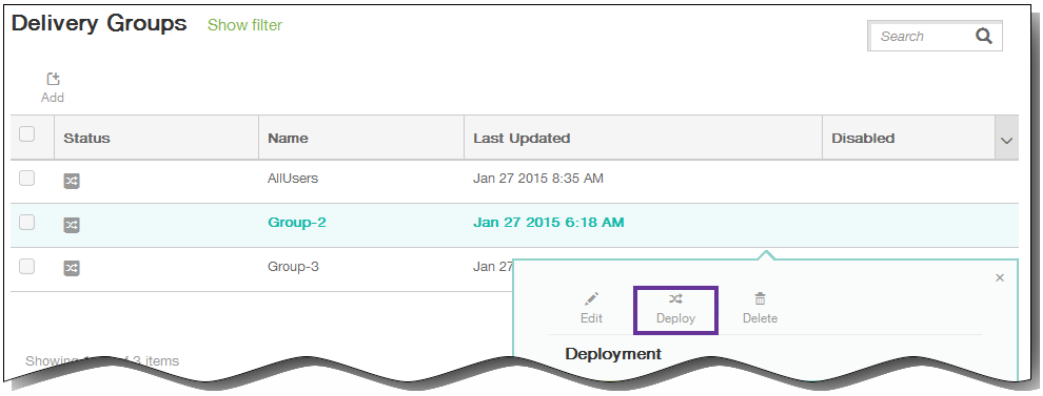
-



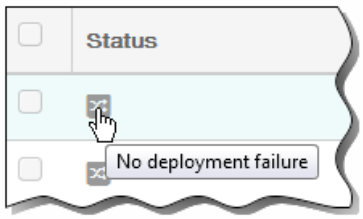
-

-
-

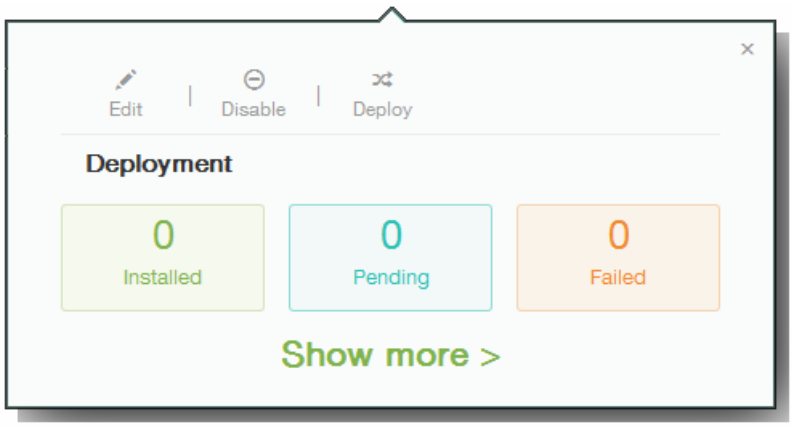




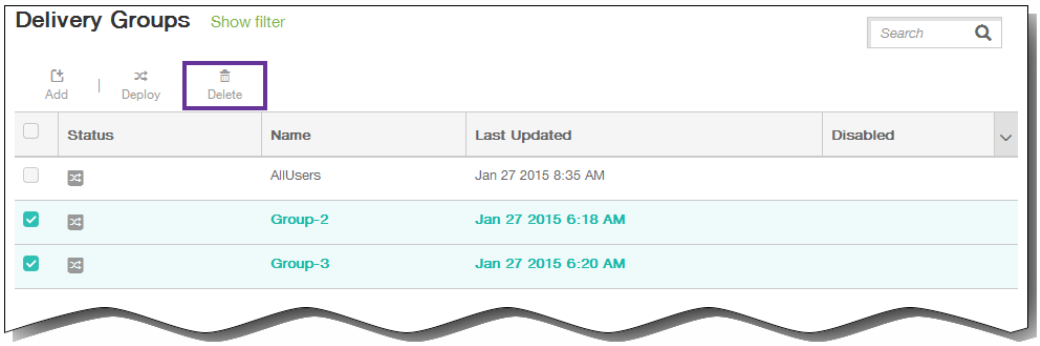
-

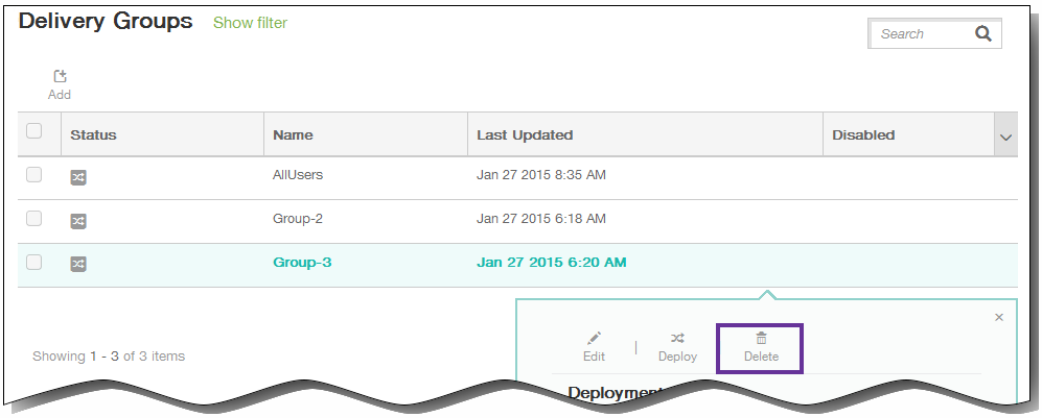


-

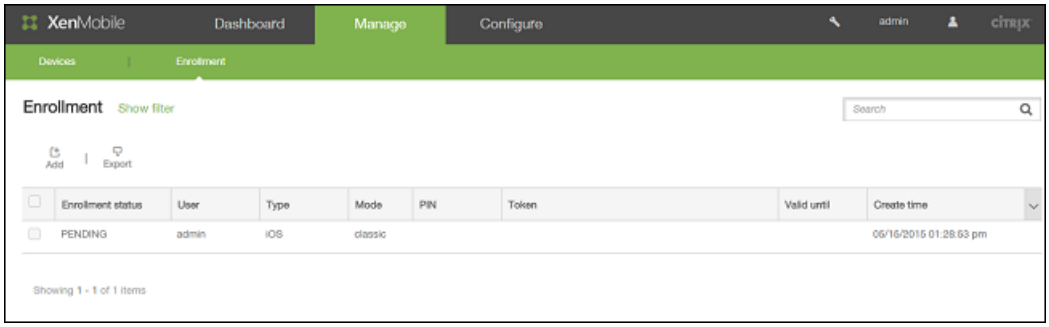


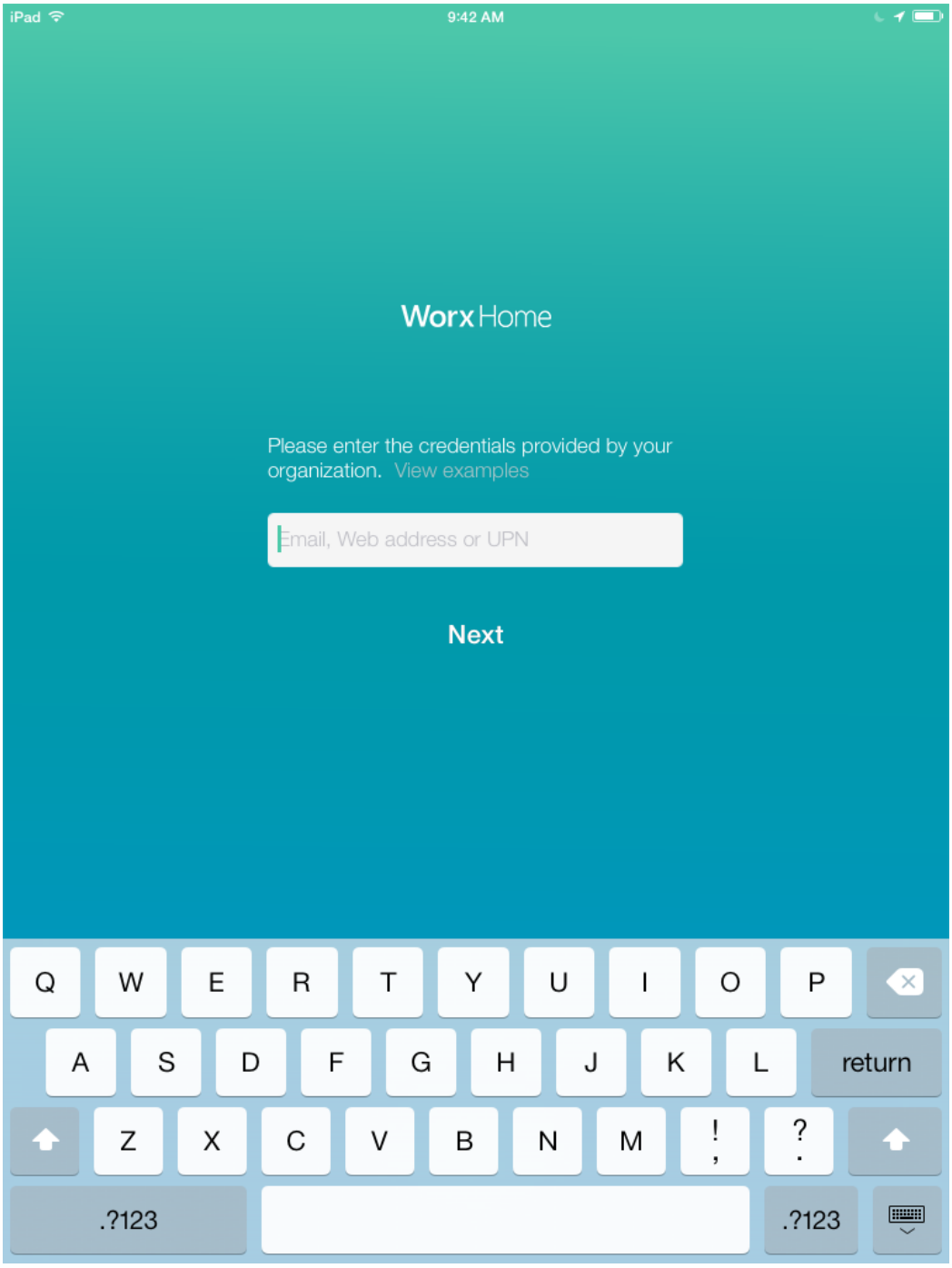
-
-

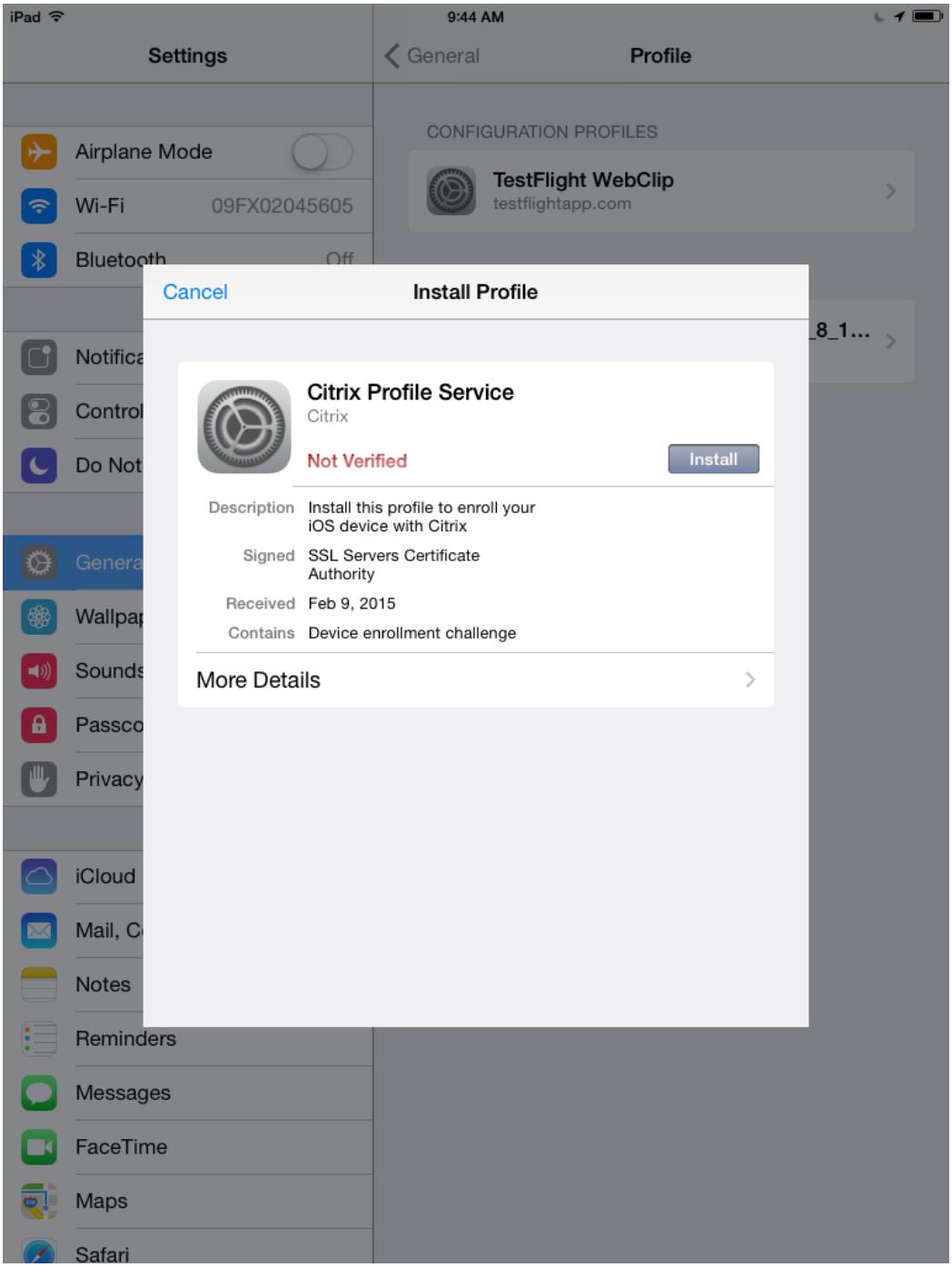


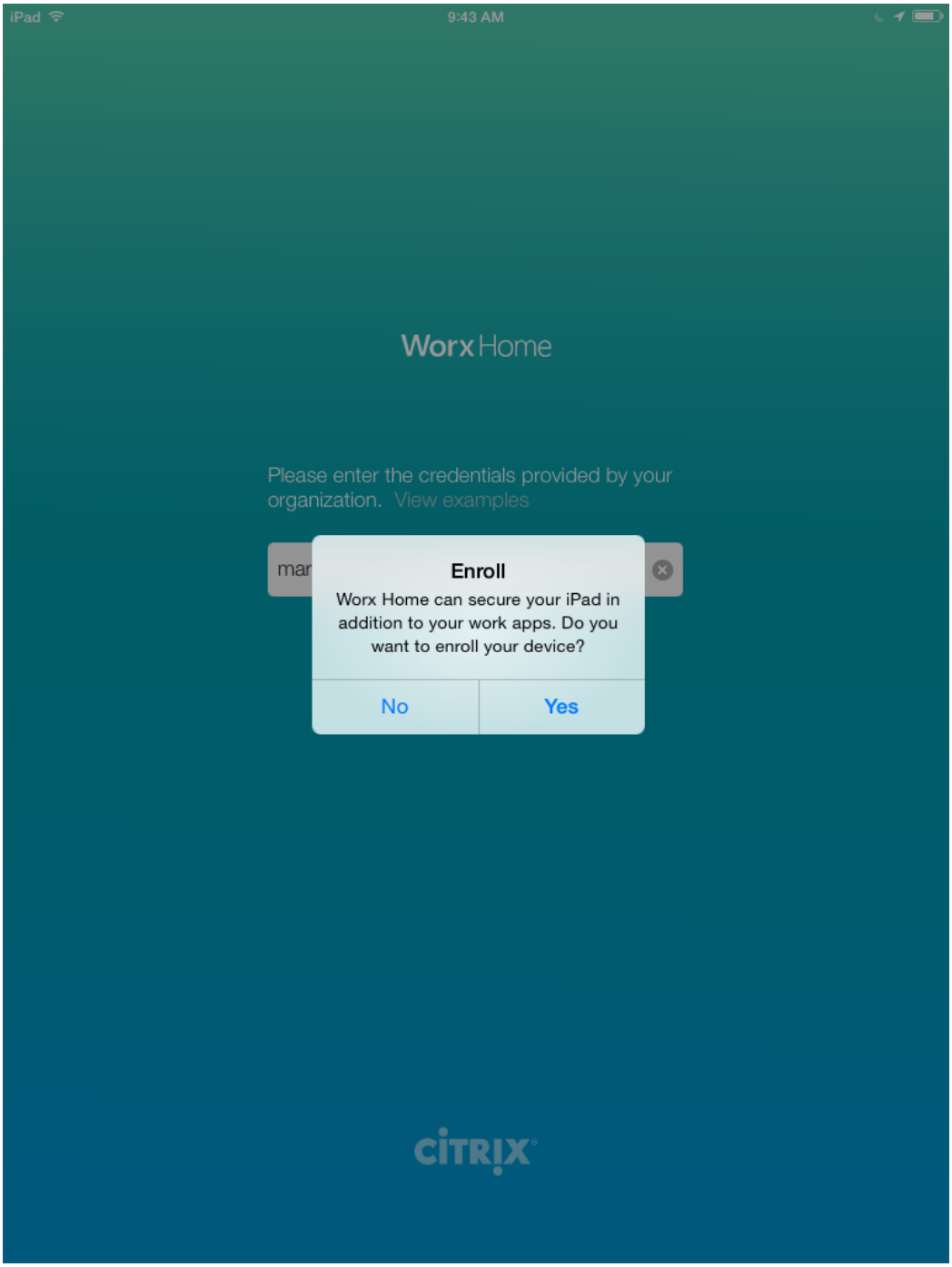


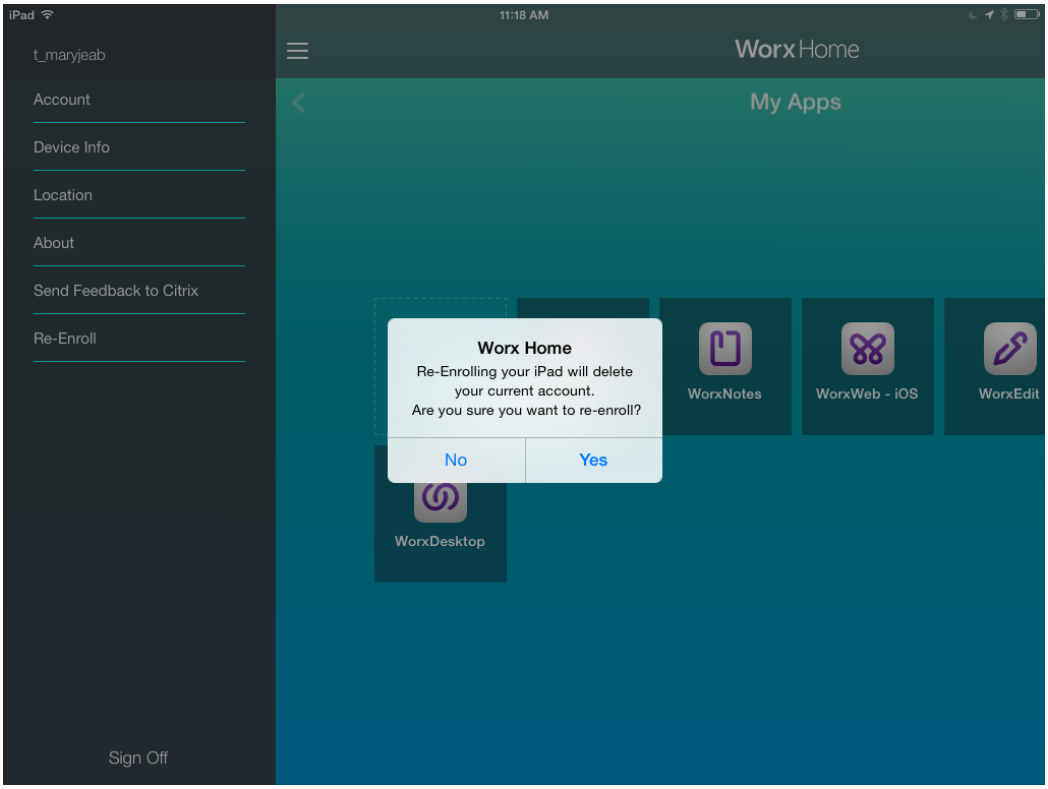
-
-
-
-











-
-

Symbian 设备

Oct 22, 2015

1. 浏览到您组织的 XenMobile Web 地址。 Web 地址的格式如下：https://.domain.com//setup
   注意：仅当您拥有可信证书机构（如 Thawte 或 VeriSign）颁发的证书时，才可以使用 HTTPS 前缀。
2. 在安装屏幕上，轻按确定。
3. 轻按 Phone Memory（电话内存），将其作为安装 XenMobile 代理的位置。
4. 安装完成后，轻按是以打开 XenMobile。
5. 在 Security Details（安全详细信息）屏幕上，轻按确定，使 XenMobile 能够访问 phone。
6. 输入服务器代码的前四位数，如 2831，然后轻按确定。
7. 在 Control Request Accepted（控制请求已接受）屏幕上，轻按确定。
8. 输入 XenMobile 服务器的用户名称和密码、服务器名称、端口和实例名称，然后轻按确定。 此时将显示连接信息。
9. 轻按选项，查看服务器连接详细信息，然后轻按关闭以完成安装。

在 XenMobile 中发送注册邀请

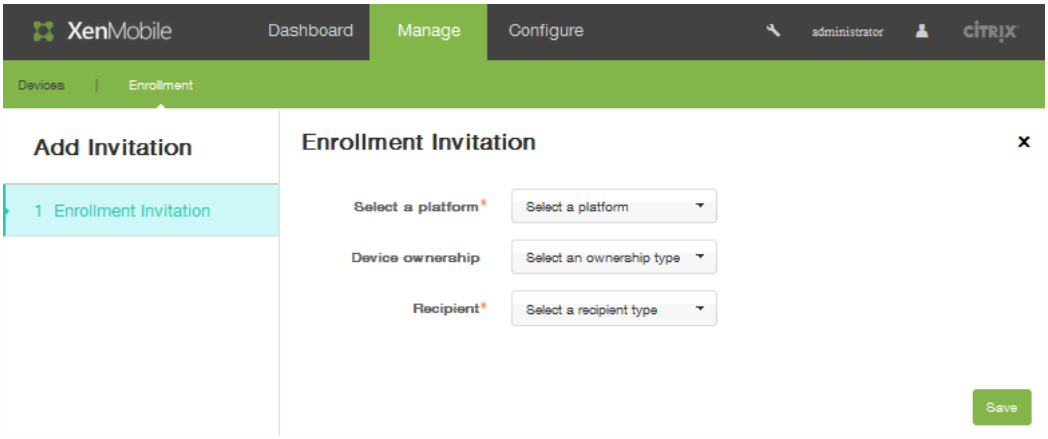
Apr 22, 2016

在 XenMobile 控制台中，向 iOS、Android 和 Windows 设备的用户发送注册邀请。

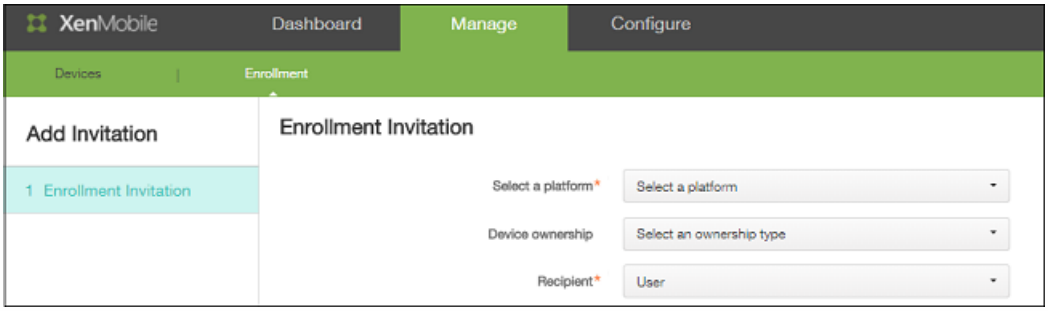
1. 在 XenMobile 控制台中，单击管理 > 注册。

2. 在注册屏幕上，单击添加。 此时将显示一个菜单，其中列出了用于添加邀请或发送邀请链接的选项。
3. 单击添加邀请。

将显示注册邀请屏幕。



4. 在选择平台列表中，单击 iOS 或 Android。
5. 在设备所有权列表中，单击公司或员工。
6. 在收件人列表中，单击用户或组。

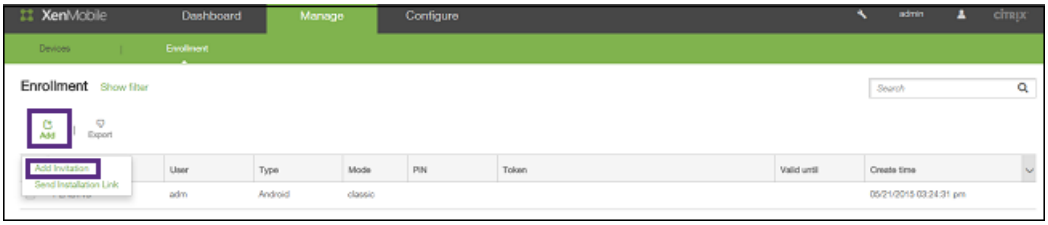


选择一个用户作为收件人时，将显示其他配置选项。请按照以下主题中的步骤，根据所选的收件人类型完成邀请设置：

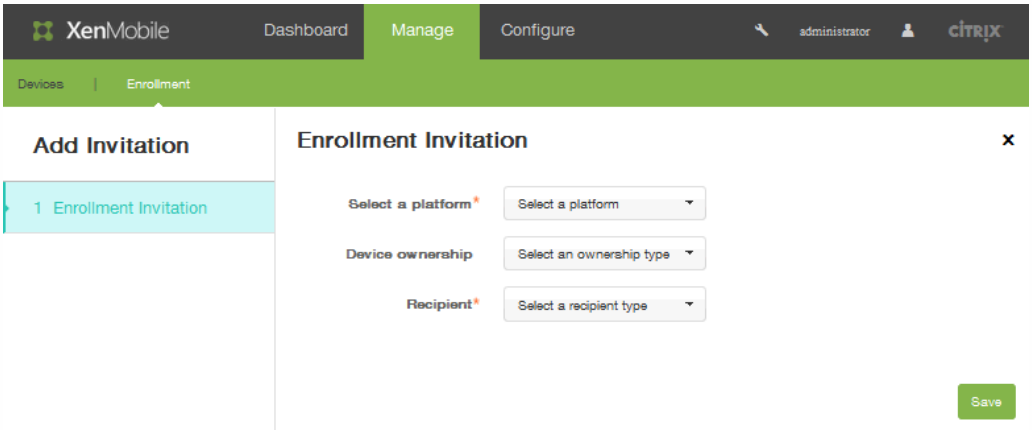
向用户发送注册邀请

1. 在 XenMobile 控制台中，单击管理 > 注册。

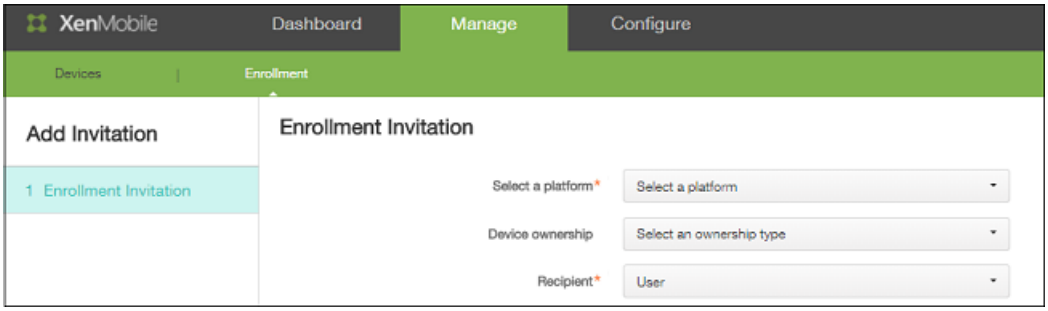
2. 在注册屏幕上，单击添加。 此时将显示一个菜单，您可以在此处选择添加邀请或发送安装链接。
3. 单击添加邀请。



将显示注册邀请屏幕。

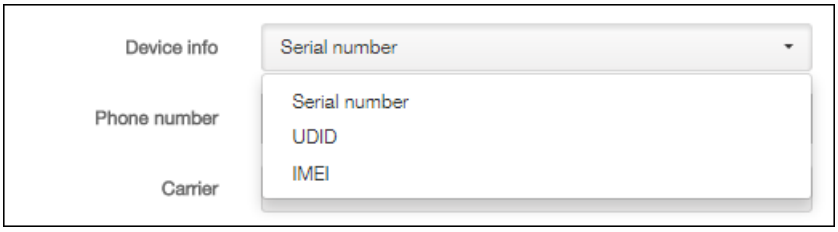


4. 在选择平台列表中，单击 iOS 或 Android。
5. 在设备所有权列表中，单击公司或员工。
6. 在收件人列表中，单击用户。



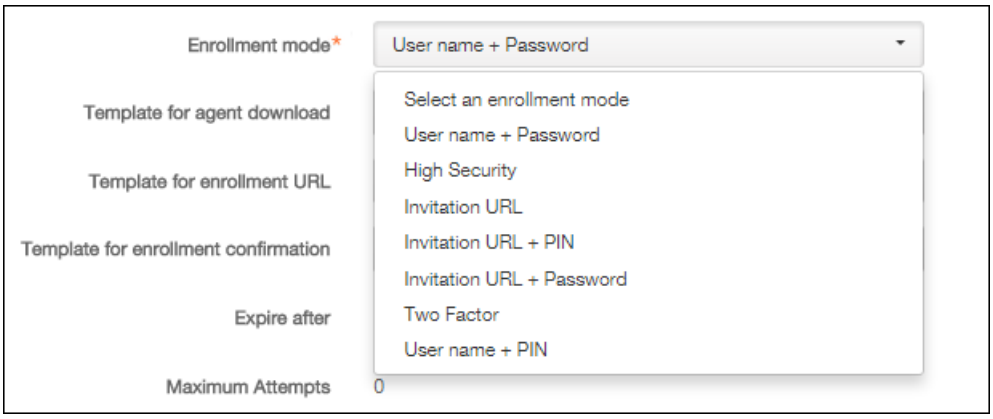
将显示与用户注册相关的其他配置选项。

7. 在用户名中，键入用户名。
   注意：用户必须作为本地用户或 Active Directory 中的用户存在于 XenMobile 服务器中。如果用户是本地用户，确保设置用户的电子邮件属性以便发送通知。如果用户是 Active Directory 中的用户，请确保配置 LDAP。
8. 在设备信息列表中，选择序列号、UDID 或 IMEI。

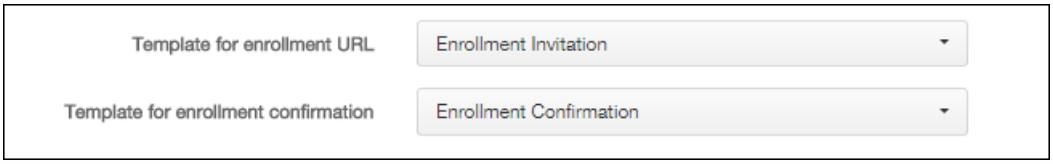


选择某个选项后，将显示一个字段，您可以在此处键入设备的相应值。

9. 在电话号码中，输入用户的电话号码（可选）。
10. 在运营商列表中，选择用户电话号码关联的运营商。
11. 在注册模式列表中，选择用户名 + 密码（默认）、高安全性、邀请 URL、邀请 URL + PIN、邀请 URL + 密码、双因素或用户名 + PIN。



12. 在代理下载模板列表中，此选项的选择项基于平台类型。 例如，如果您在步骤 1 中选择 iOS 作为平台，将显示 iOS Download Link（iOS 下载链接）选项。

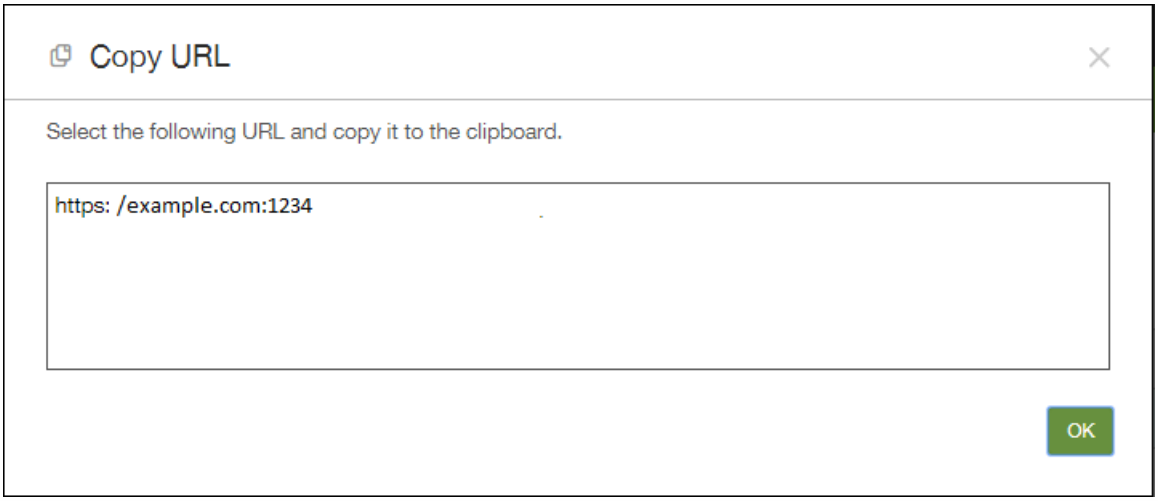


13. 在注册 URL 模板列表中，单击注册邀请。
14. 在注册确认模板列表中，单击注册确认。 注册邀请在一段时间后会过期。此时间后过期字段指示注册过期的时间。最大尝试

次数字段说明发生注册过程的最大次数。

15. 在发送邀请中，请执行以下操作：
    - 单击开，然后单击保存并发送。
    - 保留选项的值关，然后单击保存。
16. 添加的邀请将显示在“注册”页面上的表格中。 在此处，如果您单击以选择某个邀请，表格上方将显示几个新选项：通知、复制 URL 和删除。

1. 单击通知可发送待定邀请。
2. 如果您希望在电子邮件中发送邀请，单击复制 URL 可复制邀请 URL。 显示通知时，选择并复制 URL，然后单击确定。

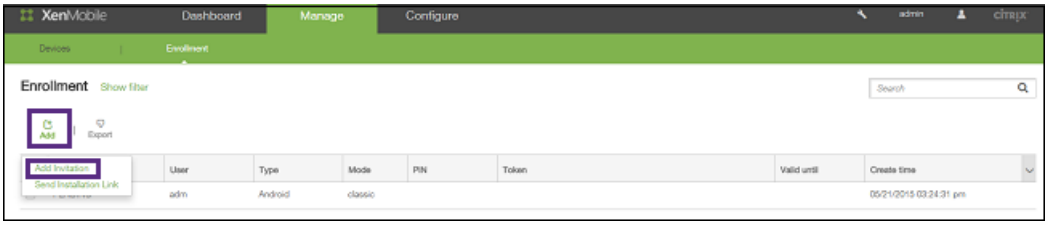


3. 单击删除可删除邀请。

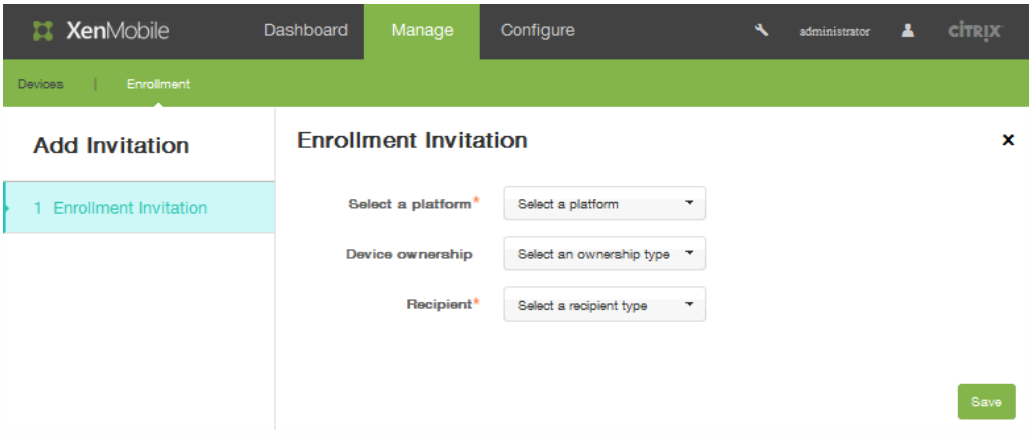
向组发送注册邀请

1. 在 XenMobile 控制台中，单击管理 > 注册。

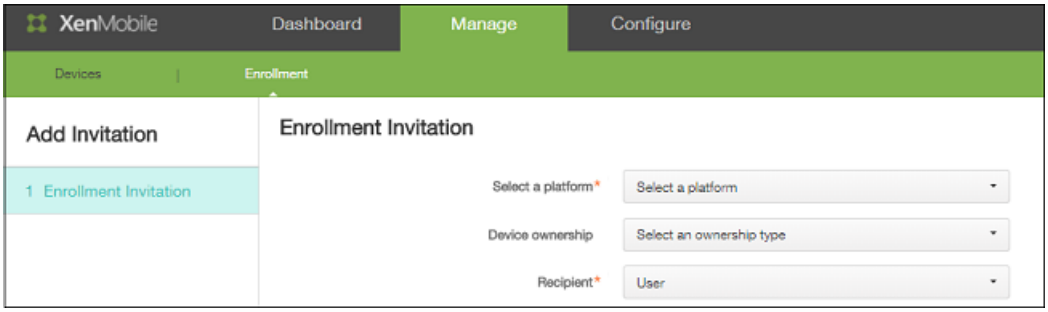
2. 在注册屏幕上，单击添加。 此时将显示一个菜单，您可以在此处选择添加邀请或发送安装链接。
3. 单击添加邀请。



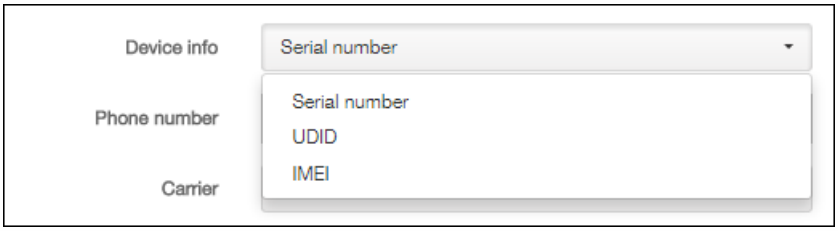
将显示注册邀请屏幕。



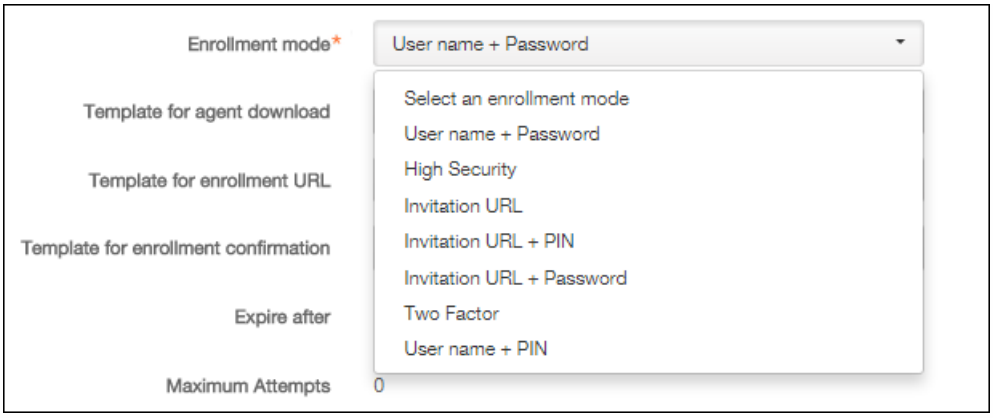
4. 在选择平台列表中，选择 iOS 或 Android。
5. 在设备所有权列表中，选择公司或员工。
6. 在收件人列表中，选择组。 将显示配置选项以便进行组注册。



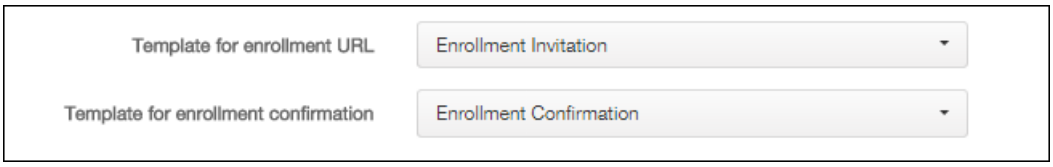
7. 在用户名中，键入用户名。
   注意：用户必须作为本地用户或 Active Directory 中的用户存在于 XenMobile 服务器中。如果用户是本地用户，确保设置用户的电子邮件属性以便发送通知。如果用户是 Active Directory 中的用户，请确保配置 LDAP。
8. 在设备信息列表中，选择序列号、UDID 或 IMEI。 选择某个选项后，将显示一个字段，您可以在此处输入设备的相应值。



9. 在电话号码中，输入用户的电话号码（可选）。
10. 在运营商列表中，选择用户电话号码关联的运营商。
11. 在注册模式中，选择用户名 + 密码（默认）、高安全性、邀请 URL + PIN、邀请 URL + 密码、双因素或用户名 + PIN。



12. 在代理下载模板列表中，此选项的选择项基于平台类型。 例如，如果您在步骤 1 中选择 iOS，将显示选项 iOS Download Link（iOS 下载链接）。



13. 在注册 URL 模板中，选择注册邀请。
14. 在注册确认模板列表中，选择注册邀请。 注册邀请在一段时间后会过期。此时间后过期字段指示注册过期的时间。最大尝试次数字段说明发生注册过程的最大次数。
15. 在发送邀请中，单击开，然后单击保存并发送。

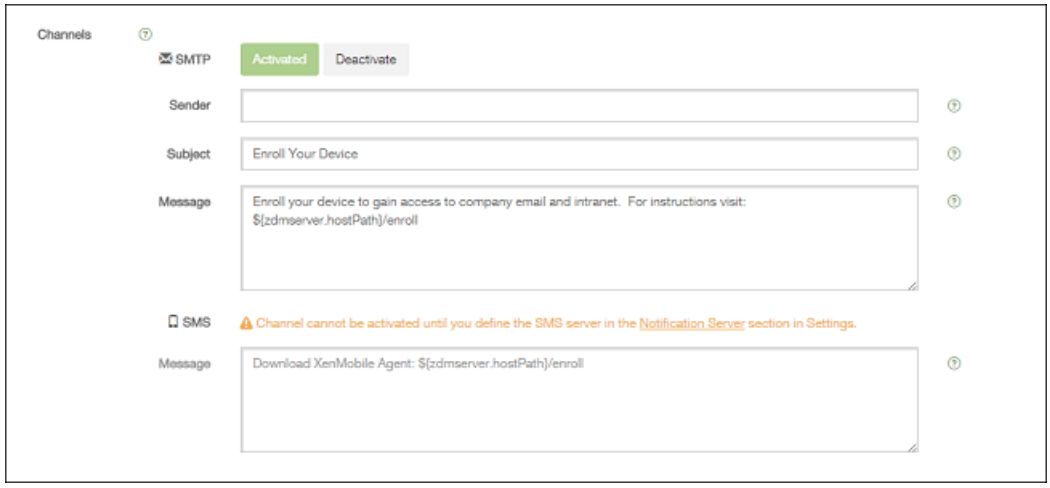
发送注册安装链接

您必须通过配置 > 设置 > 通知服务器在通知服务器上配置通道（SMTP 或 SMS），才能发送注册安装链接。有关详细信息，请参阅 XenMobile 中的通知。

1. 在 XenMobile 控制台中，单击管理 > 注册。

2. 在注册屏幕上，单击添加。 此时将显示一个菜单，您可以在此处选择添加邀请或发送安装链接。
3. 单击发送安装链接。 将显示发送安装链接选项。

4. 在收件人中，单击添加以添加要向其发送安装注册链接的收件人的电子邮件地址和电话号码，然后单击保存。 可以重复此步骤，逐个添加其他收件人。
5. 在通道中，选择合适的通道，用于发送注册安装链接。 通知通过 SMTP 或 SMS 发送。



注意：在配置 > 设置 > 通知服务器中配置服务器设置前，无法激活这些通道。有关详细信息，请参阅 XenMobile 中的通知。

6. 如果要配置 SMTP 字段，请指定发件人。 此为用于 SMTP 消息的表单字段中的可选字段。 如果不在此处指定发件人，将使用在设置 > 通知服务器字段中指定的值。
7. 对于 SMTP 通知，在主题中，可以选择性包含消息的主题。 例如，“注册您的设备”。
8. 在消息中，可以选择性添加要发送给收件人的消息内容。 例如，“注册您的设备以获取组织应用程序和电子邮件的访问权限。”
9. 要通过 SMS 发送通知，请输入发送给收件人的消息。 对于基于 SMS 的通知，此为必填字段。
   注意：在北美，超过 160 个字符的 SMS 消息将通过多条消息发送。
10. 单击发送。

> **注意**
>
> 如果您的环境使用 SAMAccountName，则当用户收到邀请并单击链接后，必须编辑用户名才能完成身份验证。 例如，用户需要从 SAMAccountName@domainname.com 中删除 domainname。

在 XenMobile 中使用 Android for Work 管理设备

Dec 03, 2015

Android for Work 是运行 Android 5.0 及更高版本的 Android 设备上的一个安全工作区，可以将企业帐户、应用程序和数据与个人帐户、应用程序和数据隔离开。在 XenMobile 10.1 中，通过让用户组合使用硬件加密和您部署的策略，在其设备上创建单独的工作配置文件，可以安全地分隔开设备的企业区域和个人区域，实现同时管理自带设备 (BYOD) 和公司拥有的 Android 设备。您可以在不影响用户个人区域的情况下，远程管理所有公司策略、应用程序和数据，并可以擦除这些策略、应用程序和数据。有关支持的 Android 设备的详细信息，请参阅 Google 的设备页面。

在 XenMobile 10.1 中，还可以通过让用户下载和安装 Android for Work 应用程序来管理运行 Android 4.0 - 4.4 的设备，这样可提供与运行 Android 5.0 及更高版本的设备中内置的安全工作区相同的功能。

使用 Google Play for Work 可添加、购买和审批应用程序，以便部署到设备的 Android for Work 工作区。您可以使用 Google Play for Work 来部署您的私有 Android 应用程序，以及公共和第三方应用程序。

Android for Work 的要求：

- 可公开访问的域
- Google 管理帐户
- 运行 Android 5.0+ Lollipop 并具有托管配置文件支持的设备，或运行 Android 4.0 - 4.4（Ice Cream Sandwich、Jelly Bean 和 KitKat）并具有 Android for Work 应用程序的设备
- 在用户的个人配置文件中安装了 Google Play 的 Google 帐户
- 用户设备上设置的工作配置文件

必须执行以下操作，才能设置 Android for Work 应用程序限制：

- 在 Google 上完成 Android for Work 设置任务。
- 创建一组 Google Play 凭据。
- 配置 Android for Work 服务器设置。
- 至少创建一个 Android for Work 设备策略。
- 在 Google Play for Work 应用商店中添加、购买和审批 Android for Work 应用程序。

管理 Android for Work 时可以使用以下链接：

- Google Admin 控制台：https://admin.google.com/AdminHome
- Play for Work 管理控制台：https://play.google.com/work/apps
- 用于专有通道和自托管应用程序的 Play 发布：https://play.google.com/apps/publish
- 用于创建服务帐户的 Google Developer Console：https://console.developers.google.com

Android for Work 必备条件

必须先执行以下操作，才能在 XenMobile 中管理 Android for Work：

- 创建一个 Android for Work 帐户
- 设置一个服务帐户
- 下载一个 Android for Work 证书
  启用并授权使用 Google Admin SDK 和 MDM API
- 授权服务帐户使用目录和 Google Play
- 获取一个绑定的令牌。

以下部分将分别介绍如何执行这些任务。完成这些任务后，可以创建一组 Google Play 凭据，配置 Android for Work 设置，并在 XenMobile 中管理 Android for Work 应用程序。

创建 Android for Work 帐户

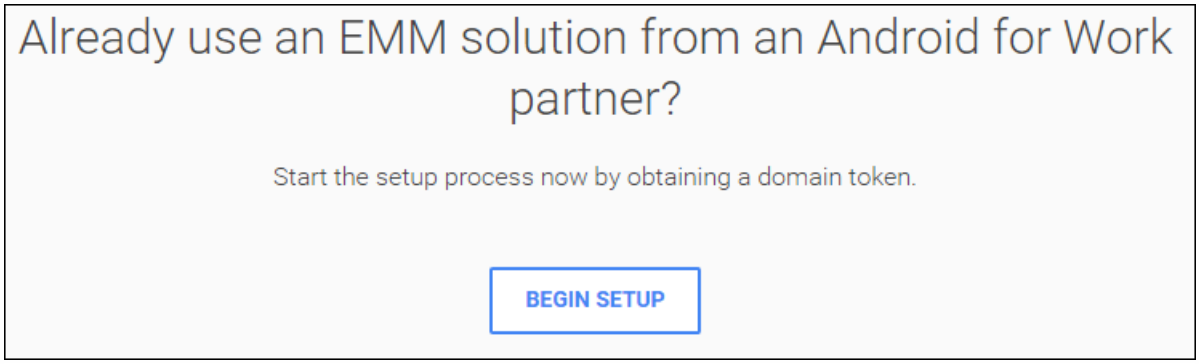
必须满足以下必备条件，才可以设置 Android for Work 帐户：

- 必须拥有域名；例如 example.com。
- 必须允许 Google 验证您是否拥有该域。
- 必须通过 Enterprise Mobility Management (EMM) 提供程序（XenMobile 10.1 或更高版本）启用和管理 Android for Work。

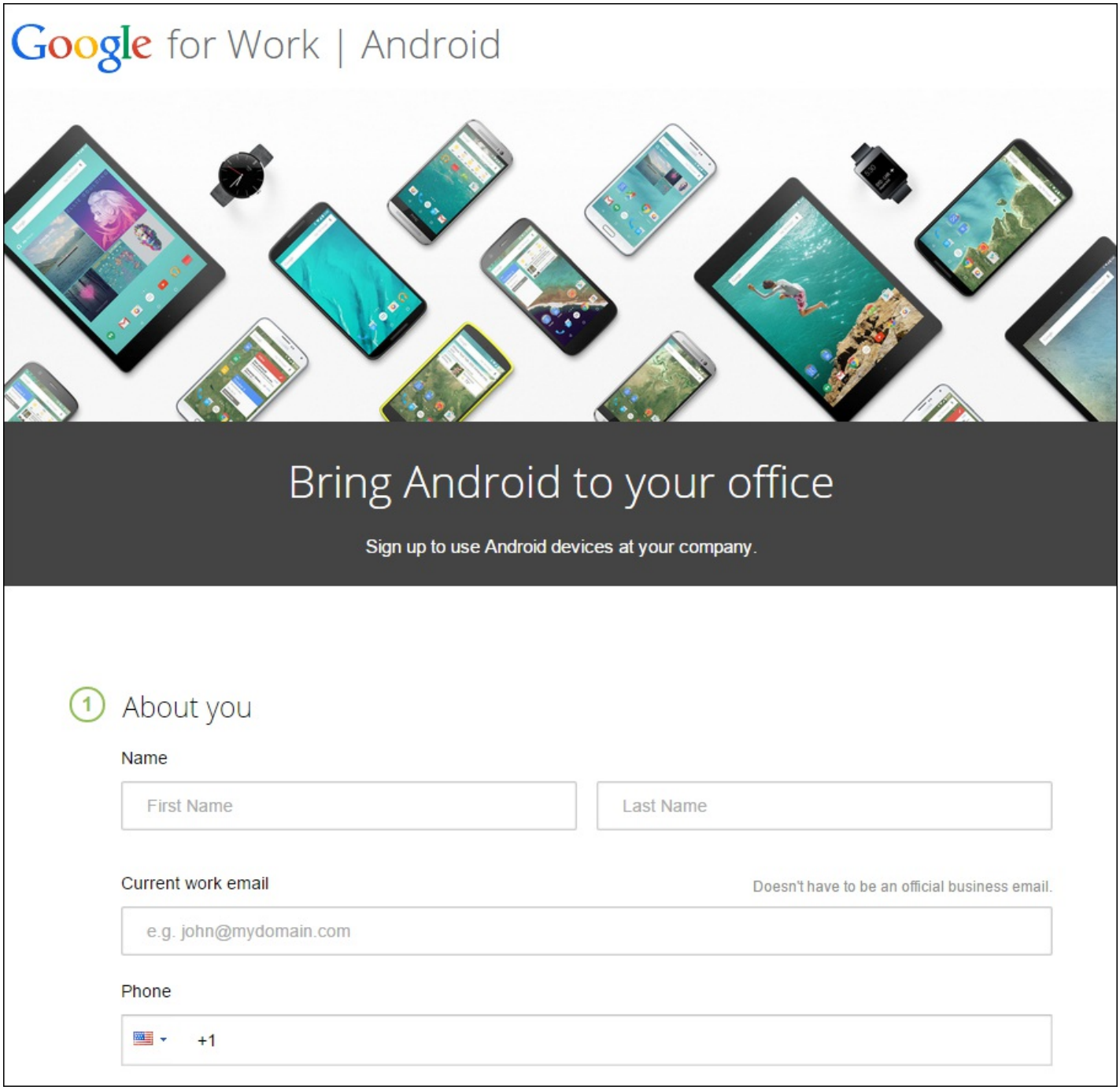
如果已向 Google 验证您的域名，可以跳至设置 Android for Work 服务帐户并下载 Android for Work 证书。

1. 转至 Google Android for Work 门户 (https://www.google.com/work/android/partners/) 并导航到 **Partners**（合作伙伴）页面。

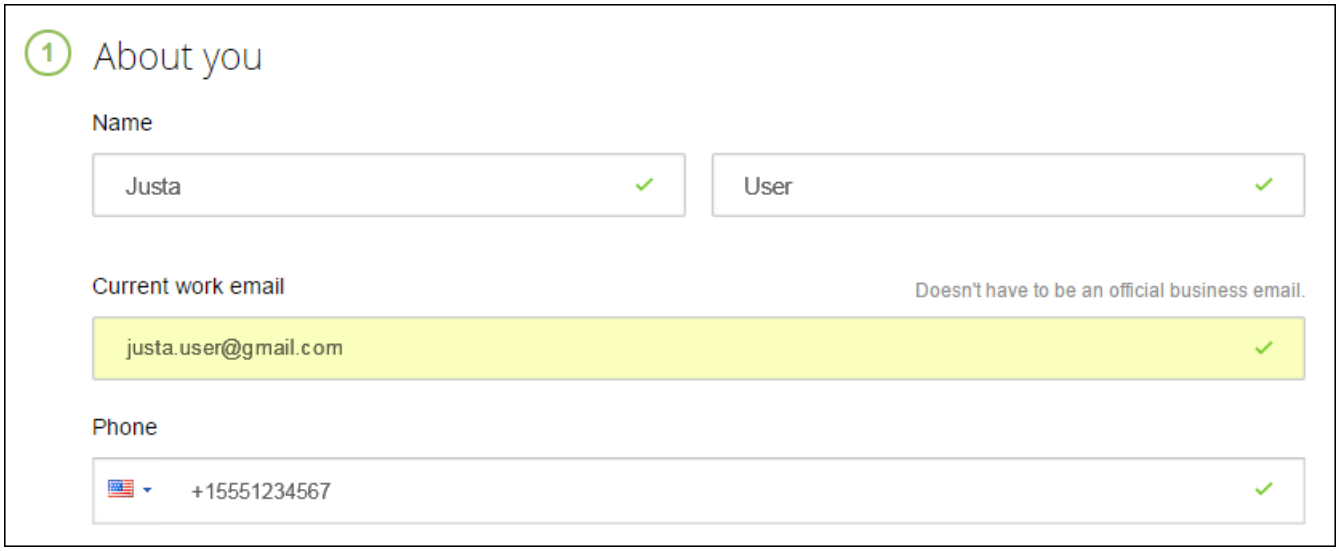
2. 单击 **Begin Setup**（开始设置）。



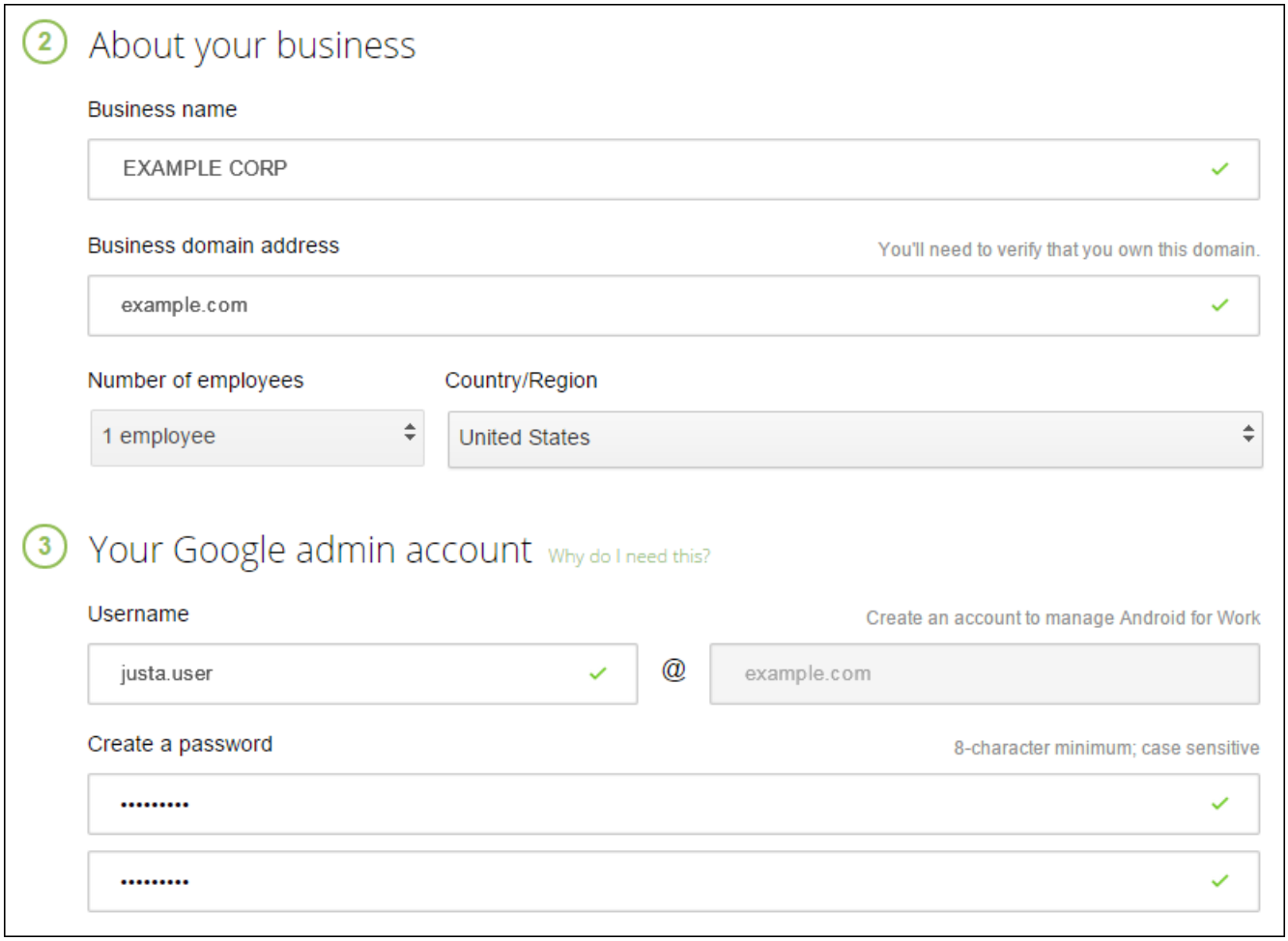
将重定向到以下页面，您可以在此页面上输入管理员信息和公司信息。



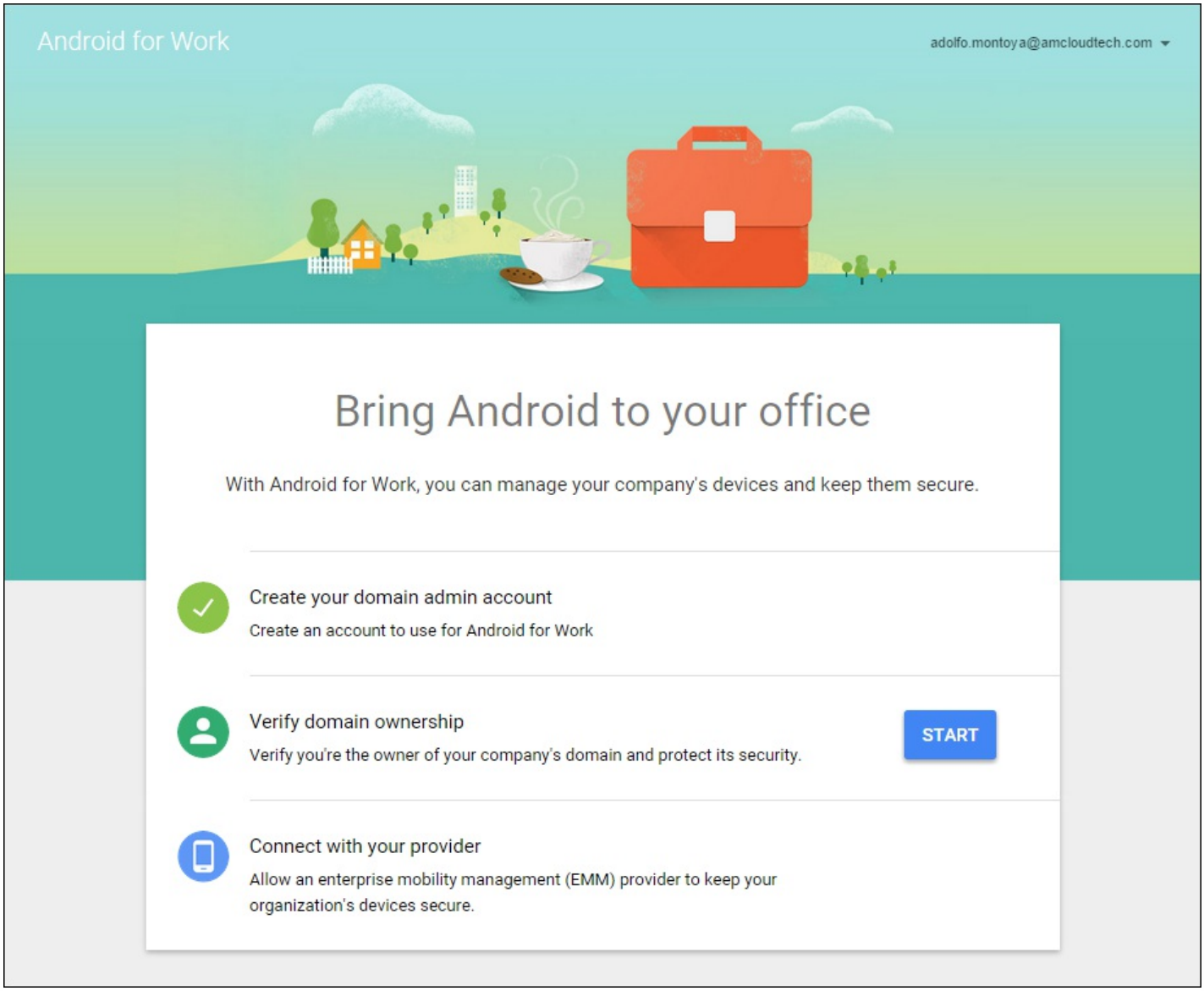
2. 输入管理员用户信息。



3. 输入公司信息，以及管理帐户信息。



此过程中的第一个步骤已完成，请继续查看下面的页面。

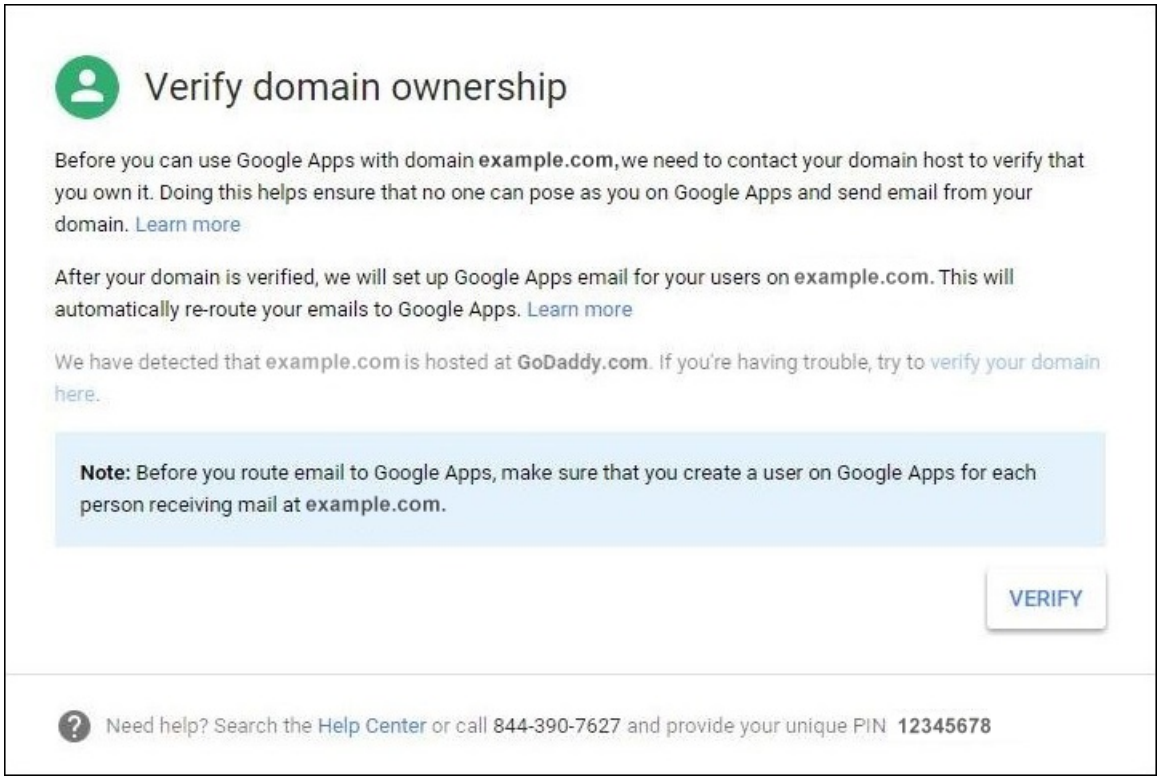


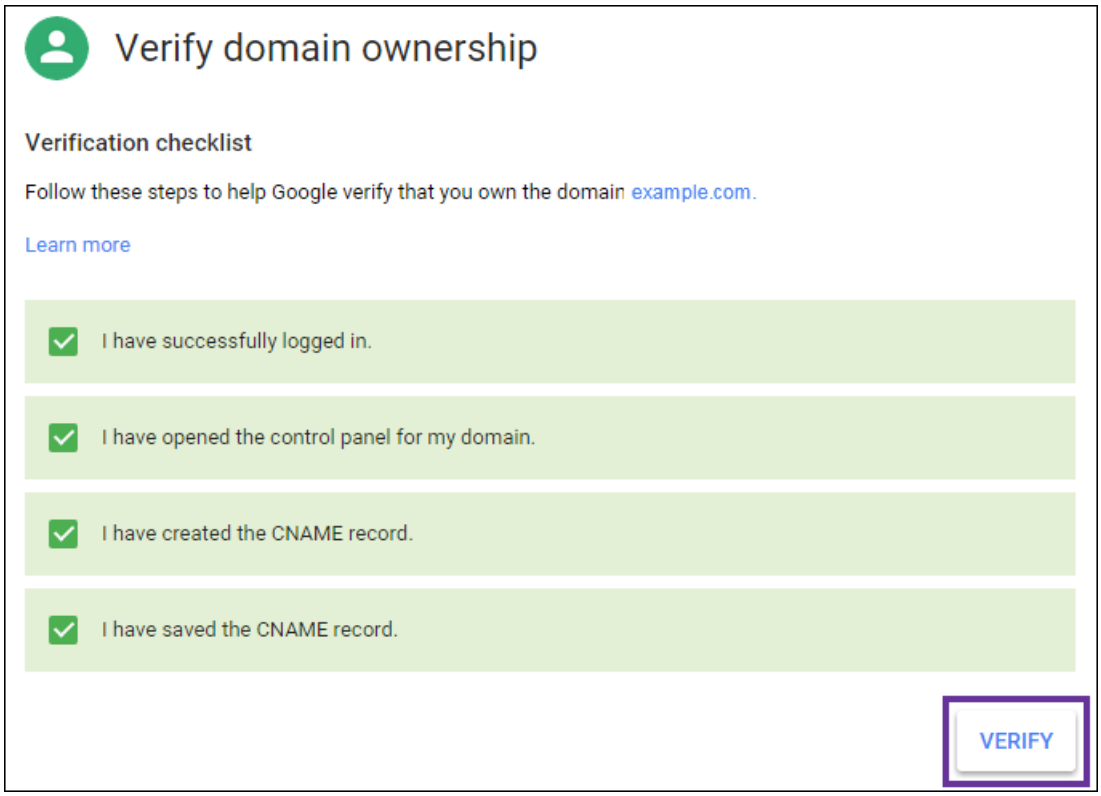
验证域所有权

您现在必须允许 Google 验证您的域。可以通过三种方法验证您的域：将 TXT 或 CNAME 记录添加到域主机的 Web 站点，将 HTML 文件上载到域的 Web 服务器，或者向主页中添加一个 标记。Google 建议使用第一种方法。本文中不包括验证域所有权的步骤，但您可以从以下网址找到所需的信息：https://support.google.com/a/answer/6095407/。

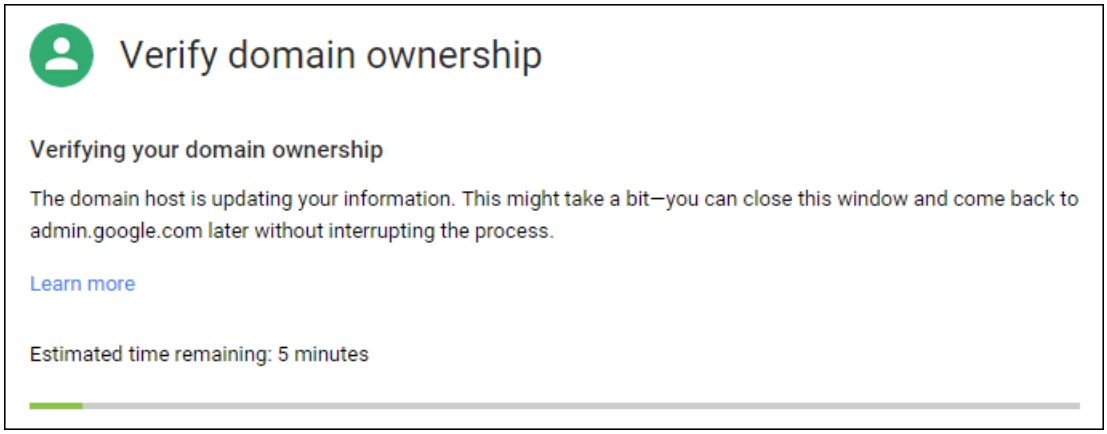
1. 单击 **Start**（开始）开始验证您的域。此时将显示 **Verify domain ownership**（验证域所有权）页面。请按照此页面上显示的说明验证您的域。

2. 操作完成后，单击 **Verify**（验证）。

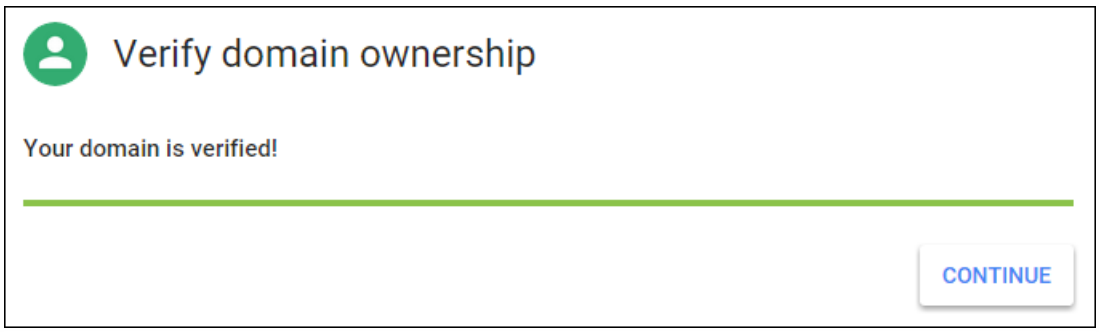




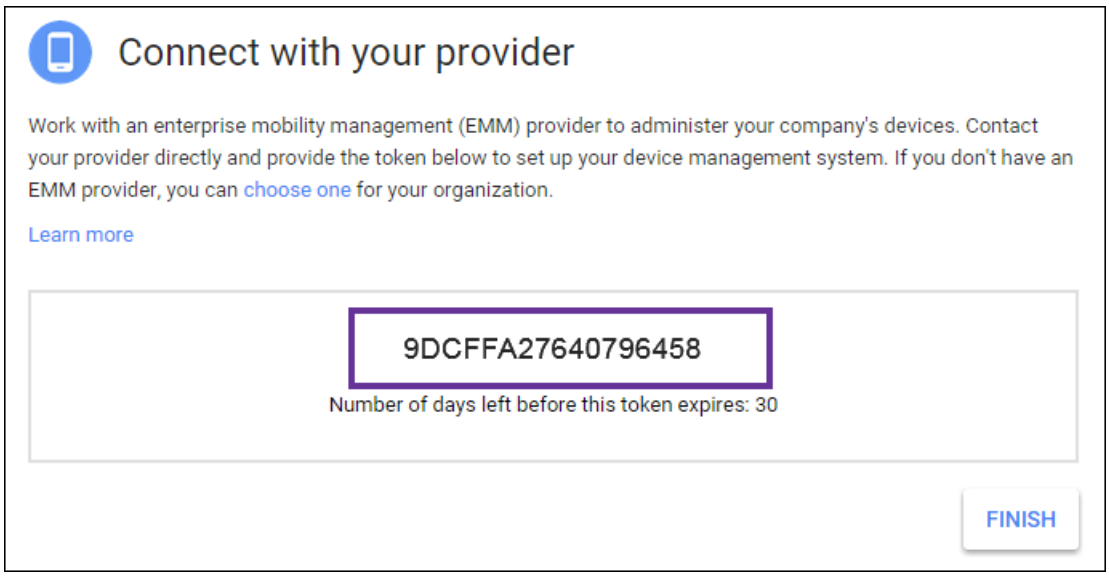
7. Google 验证您的域所有权。



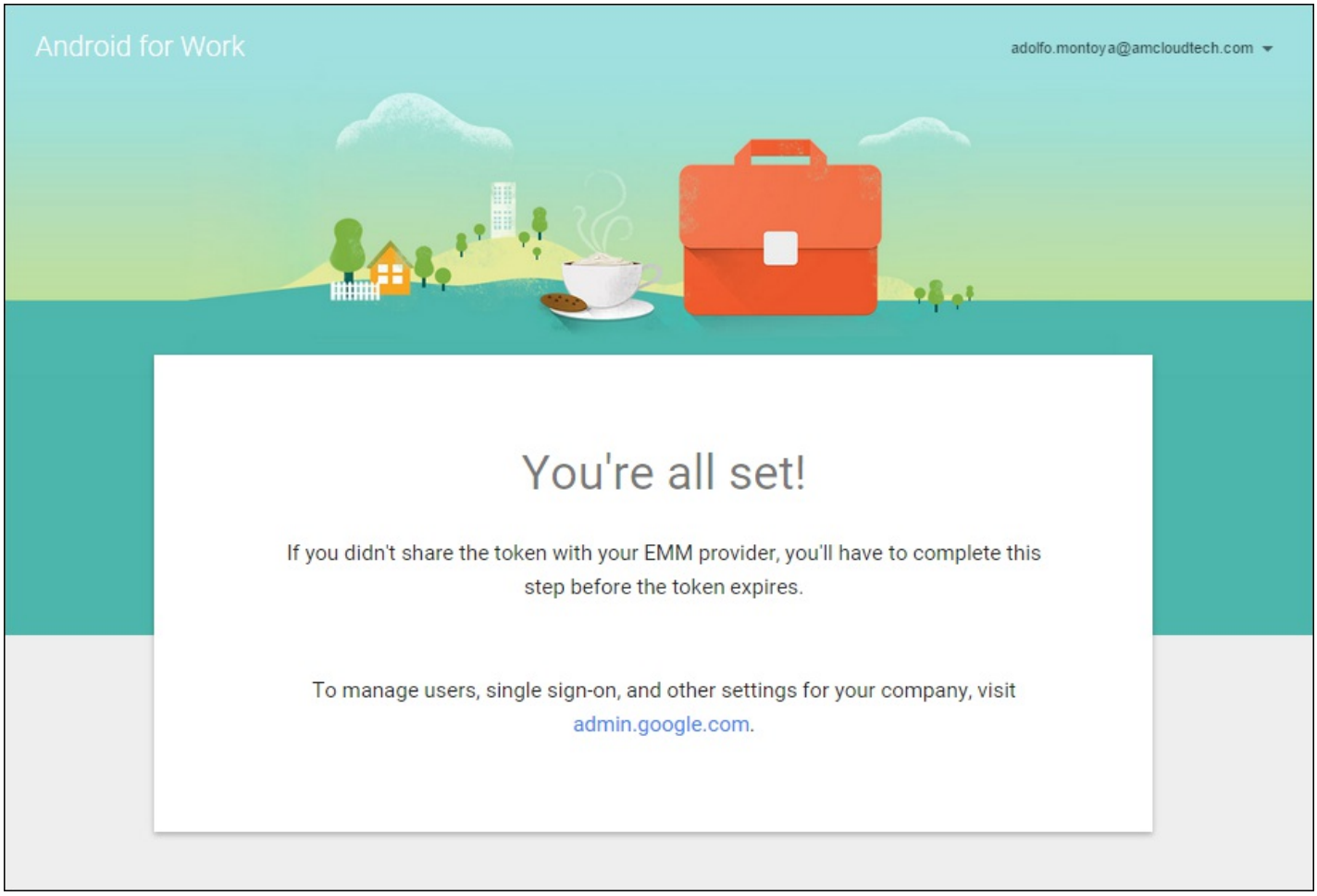
8. 成功验证后您将看到以下页面。单击 **Continue**（继续）。



9. Google 创建一个需要向 Citrix 提供的 EMM 绑定令牌，您在配置 Android for Work 设置时需要使用该令牌。复制并保存该令牌；稍后的设置过程中需要使用该令牌。



10. 单击 **Finish**（完成）以完成 Android for Work 设置。

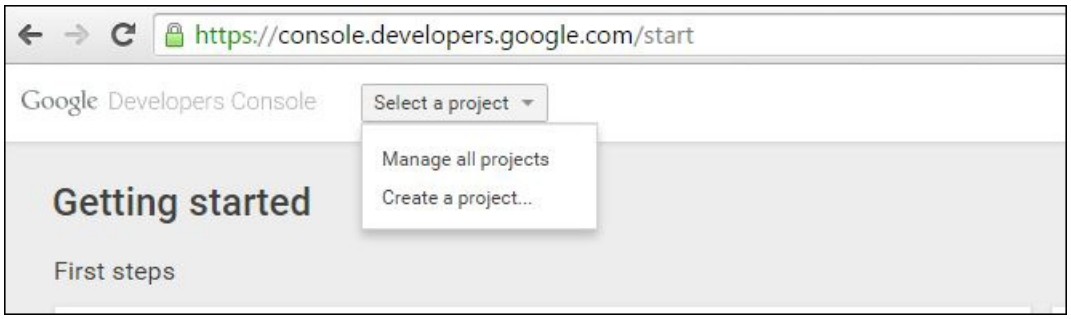


创建 Android for Work 服务帐户后，可以登录 Google Admin 控制台，以管理 Android for Work 移动性管理设置。

设置 Android for Work 服务帐户并下载 Android for Work 证书

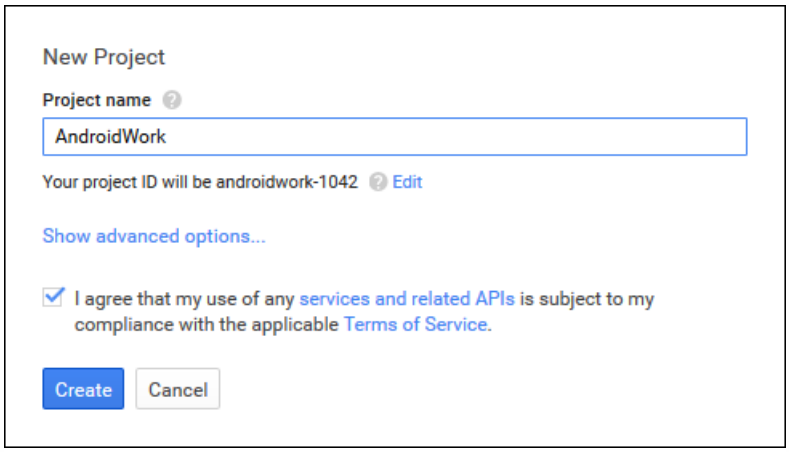
要允许 XenMobile 联系 Google Play 和 Directory 服务，必须使用 Google 的开发人员项目门户创建新的服务帐户。此服务帐户用于 XenMobile 和 Android for Work Google 服务之间的服务器至服务器通信。有关所使用的身份验证协议的详细信息，请参阅 https://developers.google.com/identity/protocols/OAuth2ServiceAccount。

1. 在 Web 浏览器中，转至 https://console.developers.google.com/project 并使用您的 Google 管理员凭据登录。

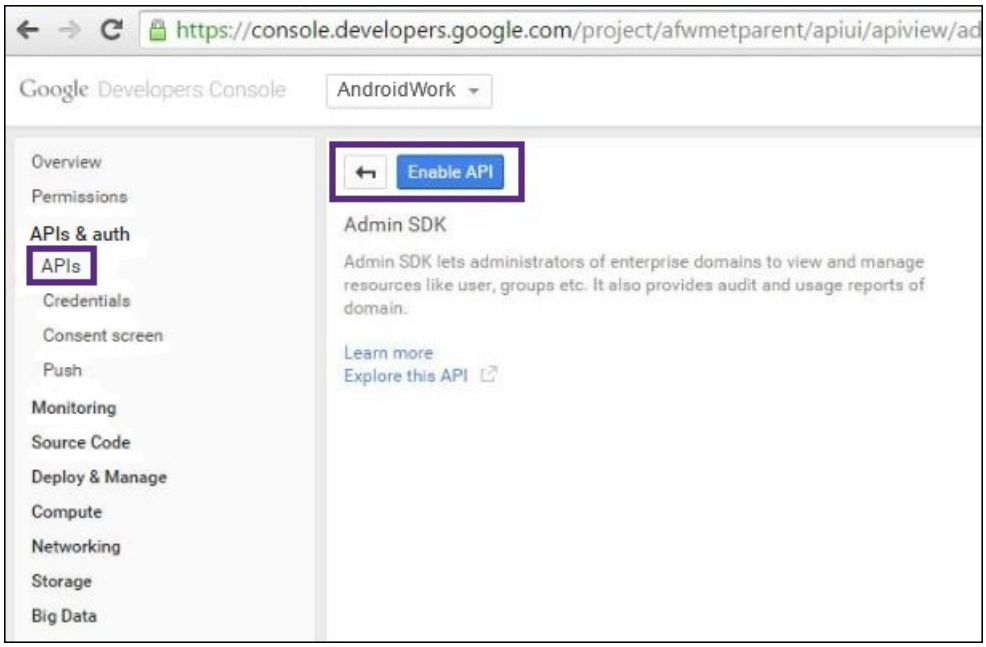


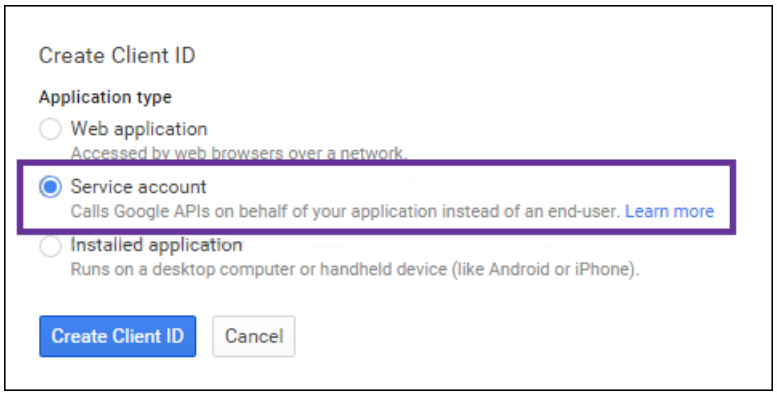
3. 在 **Select a project**（选择项目）列表中，单击**Create a Project**（创建项目）。

4. 键入项目名称，单击用于同意服务条款的复选框，然后单击 **Create**（创建）。



5. 在左侧窗格中，单击 **APIs & auth**（API 和身份验证），然后单击 **APIs**（API）。



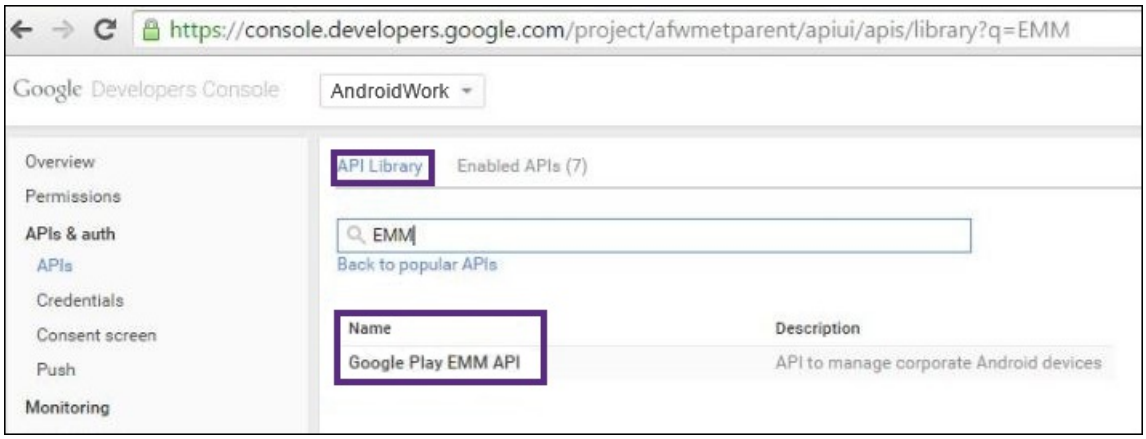


6. 在 **Google Apps APIs**（Google Apps API）下，单击 **Admin SDK**（管理 SDK）。或者，也可以在搜索字段中键入“Admin

SDK”，然后在搜索结果页面上单击 **Admin SDK**（管理 SDK）。

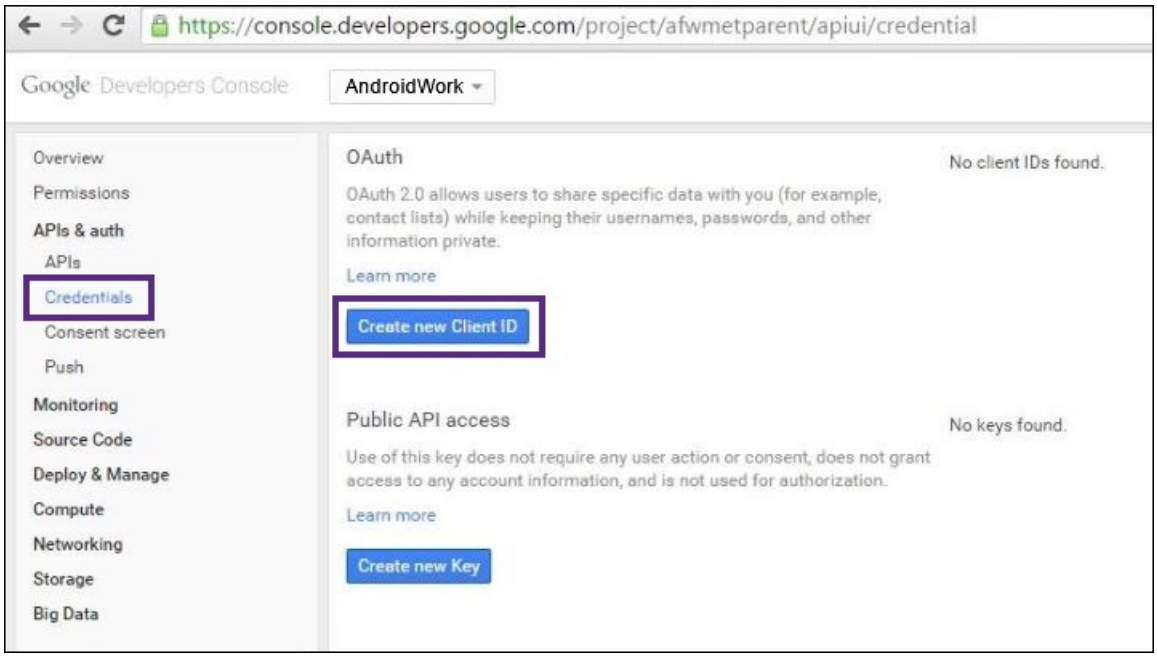
7. 单击 **Enable API**（启用 API）。

8. 在 **API Library**（API 库）下，搜索 **EMM** 并选择 **Google Play EMM API**。

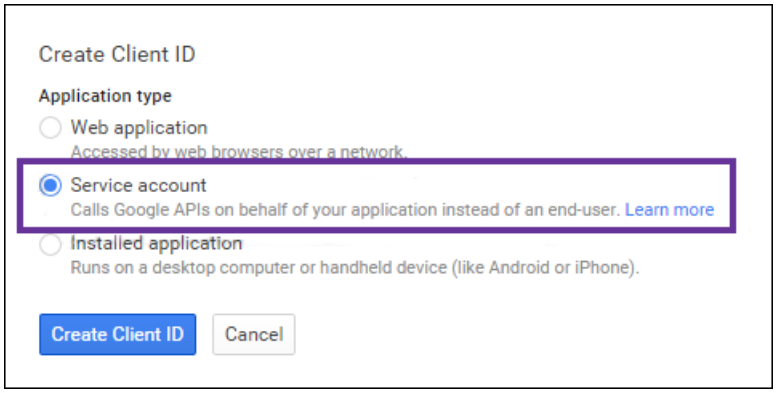


9. 单击 **Enable API**（启用 API）。

10. 在同一页面上，在左侧窗格中的 **APIs & auth**（API 和身份验证）下，单击 **Credentials**（凭据）。



11. 在右侧窗格中，单击 **Create new Client ID**（创建新客户端 ID）。此时将显示 **Create Client ID**（创建客户端 ID）对话框。



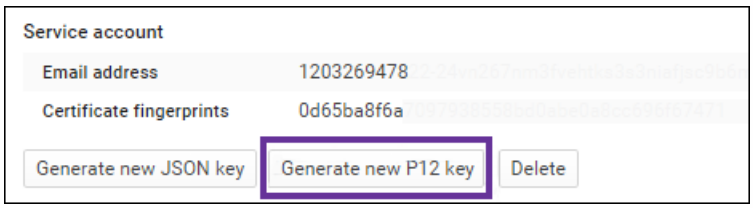
12. 选择 **Service account**（服务帐户），然后单击 **Create Client ID**（创建客户端 ID）。

13. 单击 **Okay, got it**（好的，知道了）。单击“Okay, got it”（好的，知道了）后，json文件将下载到您的计算机。请务必将该文件保存到一个安全的位置。

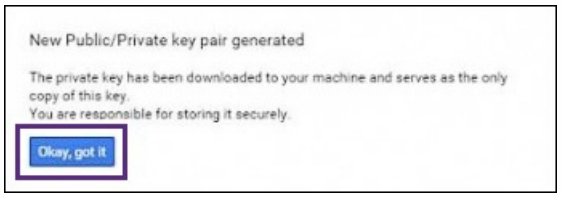
在 **Service account**（服务帐户）下，记录电子邮件地址和证书指纹（密码）。您在稍后执行的步骤中需要这两项信息。

电子邮件地址是指您在绑定 XenMobile 作为 EMM 提供程序以及启用 API 客户端访问时使用的服务帐户。

14. 在 **Service account**（服务帐户）下，单击 **Generate new P12 key**（生成新的 P12 密钥）。证书（P12 文件）将下载到您的计算机。请务必将该证书保存到一个安全的位置。

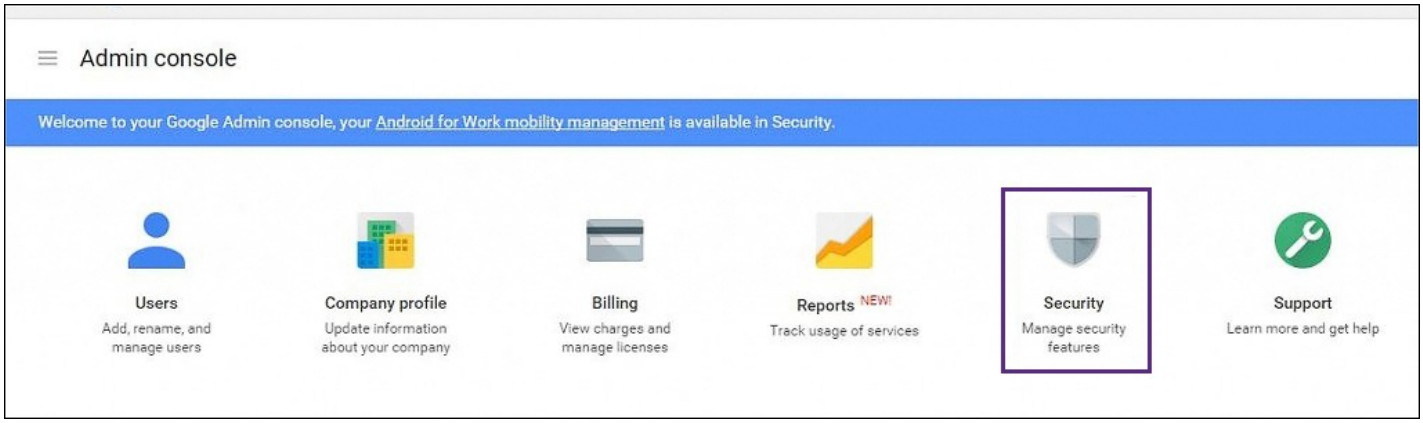


15. 单击 **Okay, got it**（好的，知道了）。

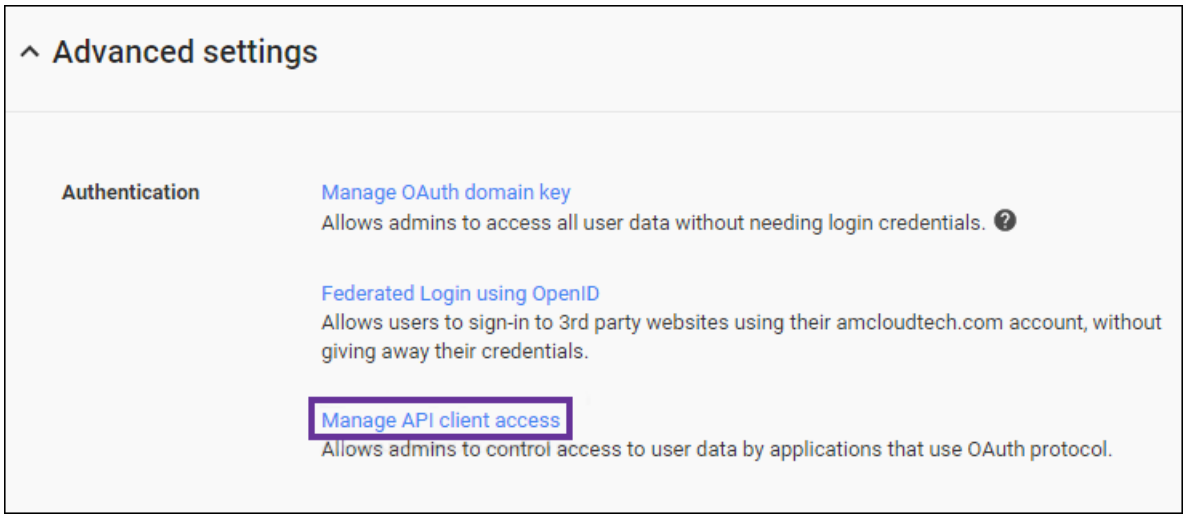


16. 使用您的 Google Android for Work 管理员凭据登录 Google 管理门户，网址为 https://admin.google.com。

17. 单击 **Security**（安全）。



18. 单击 **Advanced Settings**（高级设置），然后单击 **Manage API client access**（管理 API 客户端访问）。

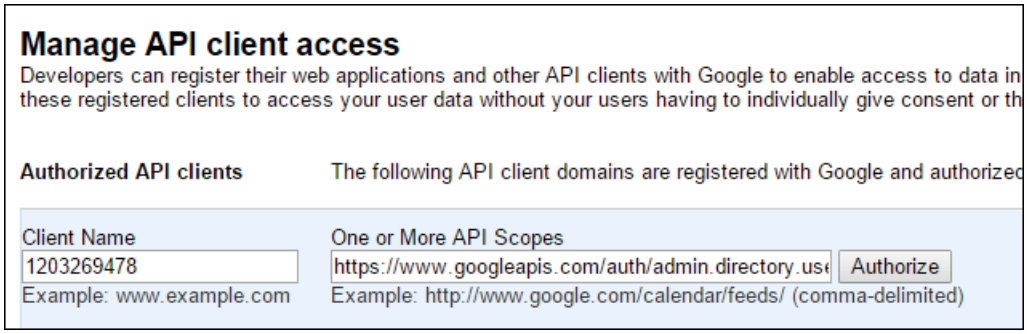


19. 单击 **Authorized API clients**（授权 API 客户端）。此时将显示 **Manage API client access**（管理 API 客户端访问）页面。

20. 在 **Client Name**（客户端名称）中，键入在步骤 14 中生成的客户端 ID。

21. 在 **One or More API Scopes**（一个或多个 API 作用域）中，输入“https://www.googleapis.com/auth/admin.directory.user”（不包括引号）。

22. 单击 **Authorize**（授权）。

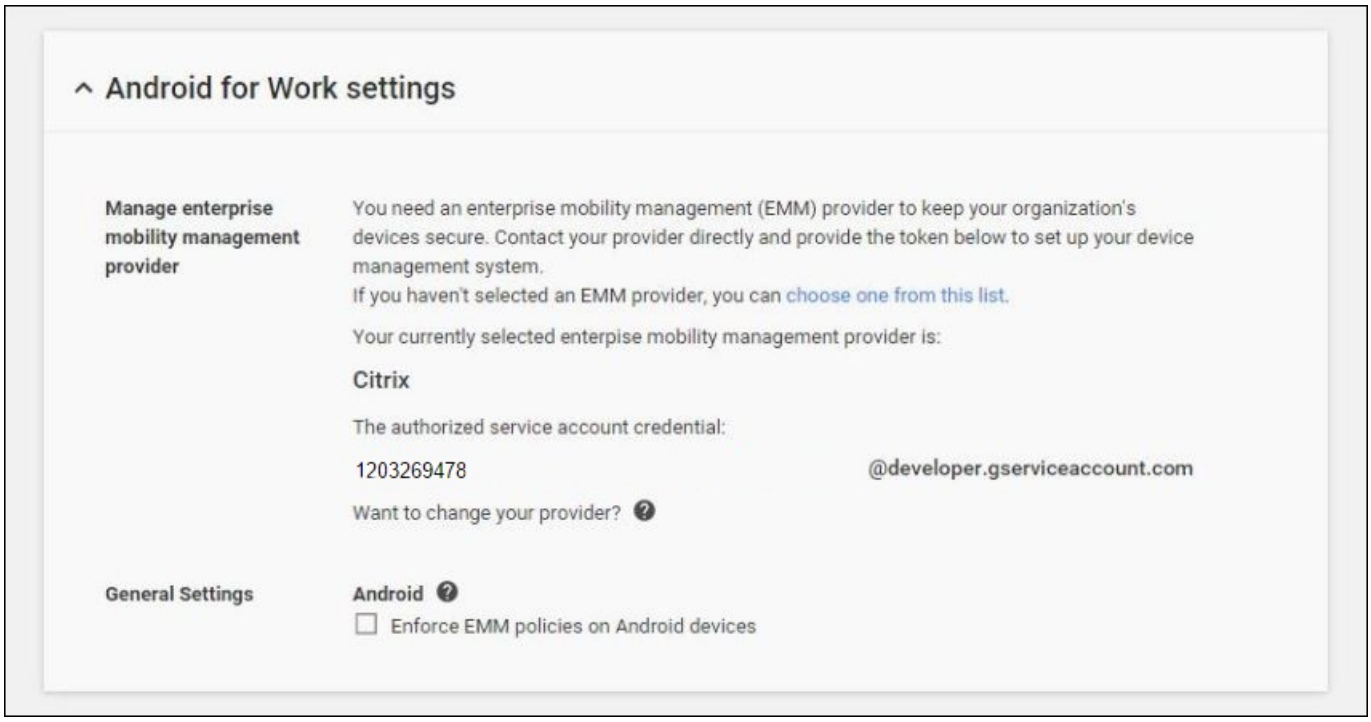


绑定到 EMM

必须先联系 Citrix 技术支持 (https://www.citrix.com/contact/technical-support.html) 并提供您的域名、服务帐户和绑定令牌，才能使用 XenMobile 管理 Android for Work 设备。Citrix 会将该令牌绑定到 XenMobile 作为 Enterprise Mobility Management (EMM) 提供程序。

1. 要确认绑定，请登录 Google 管理门户，然后单击 **Security**（安全）。

2. 单击 **Android for Work settings**（Android for Work 设置）。您将看到自己的 Google Android for Work 帐户绑定到 Citrix，用作 EMM 提供程序。



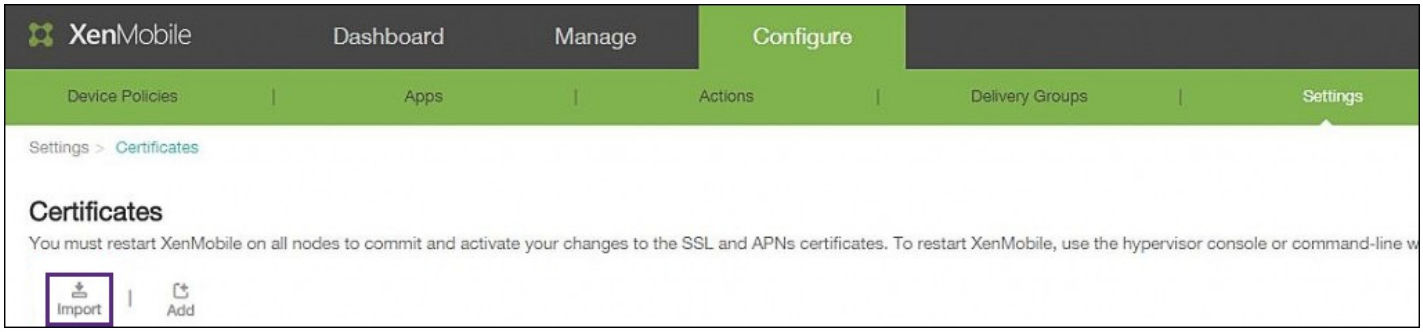
确认令牌绑定后，可以开始使用 XenMobile 管理您的 Android for Work 设备。必须导入在步骤 14 中生成的 P12 证书，设置 Android for Work 服务器设置，启用基于 SAML 的单点登录，并至少定义一条 Android for Work 设备策略。

导入 P12 证书

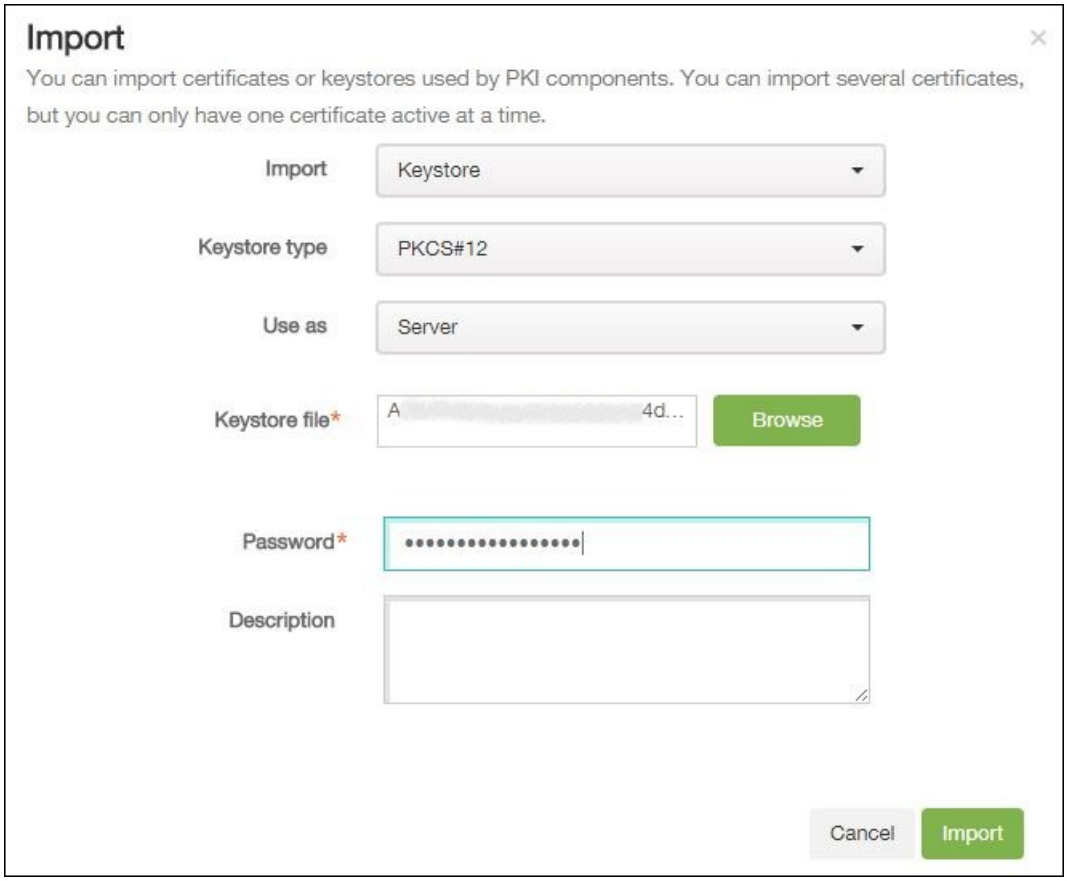
请按照以下步骤导入 Android for Work P12 证书：

1. 登录到 XenMobile 10.1 控制台。

2. 单击**配置->设置->证书**。此时将显示**证书**页面。



3. 单击**导入**。此时将显示**导入**对话框。配置以下设置：

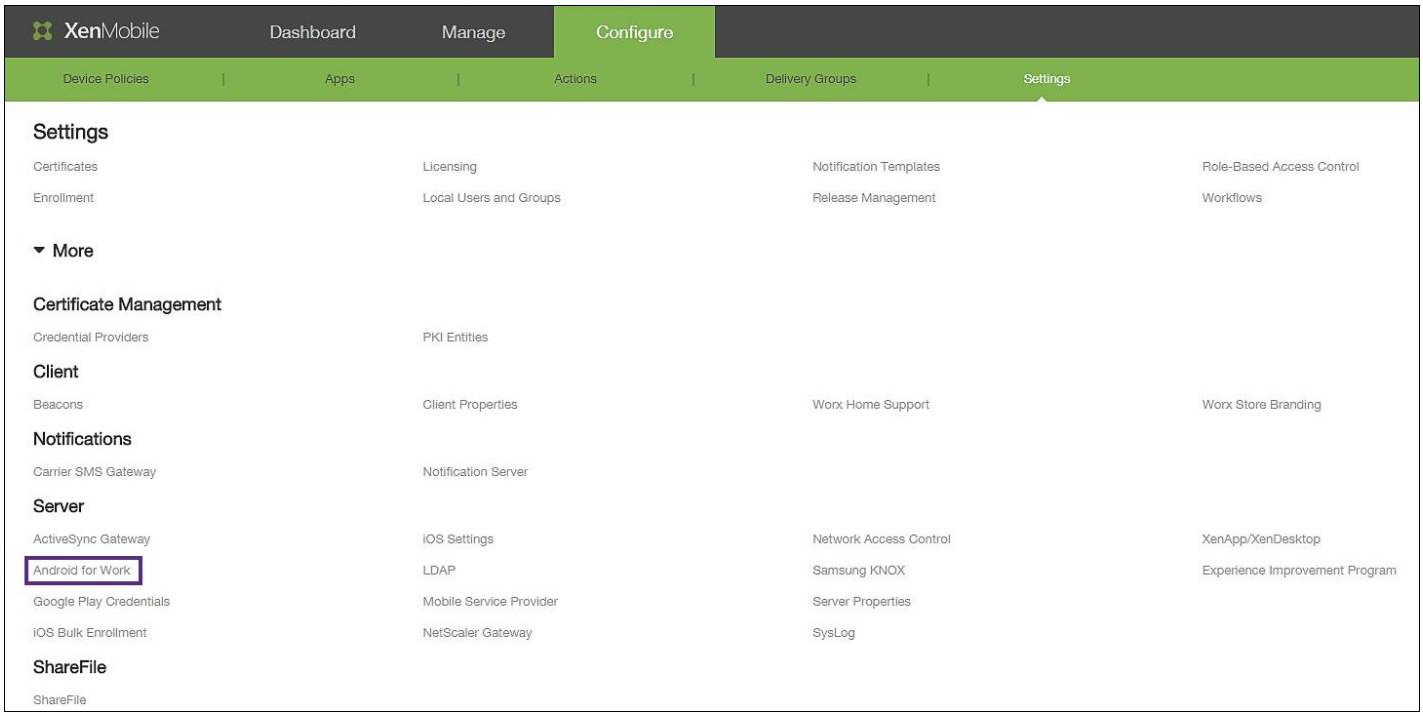


- **导入**：在列表中，单击“密钥库”。
- **密钥库类型**：在列表中，单击“PKCS#12”。
- **用作**：在列表中，单击“服务器”。
- **密钥库文件**：单击“浏览”，然后导航到 P12 证书。
- **密码**：键入密钥库密码。
- **说明**：（可选）键入证书的说明。

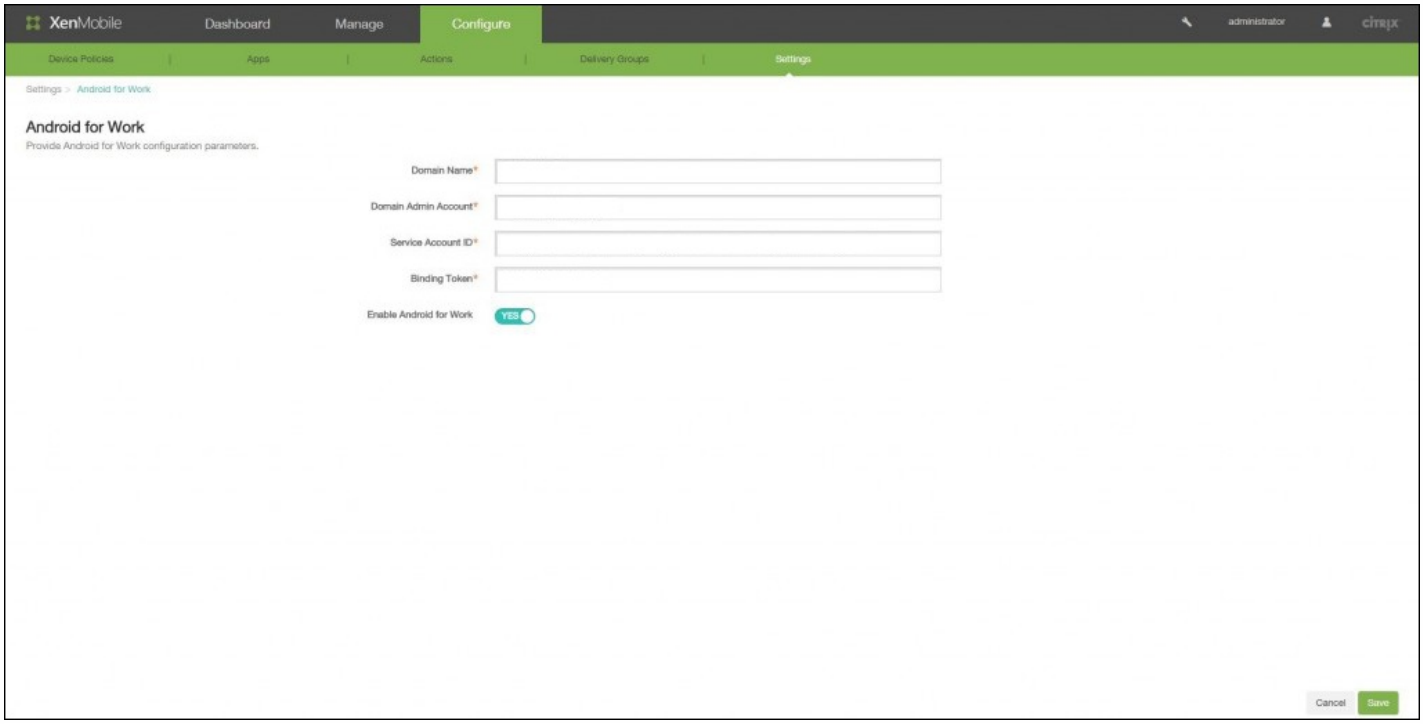
4. 单击**导入**。

设置 Android for Work 服务器设置。

1. 单击**配置->设置**，然后展开**更多**。



2. 在**服务器**下，单击 **Android for Work**。此时将显示 **Android for Work** 页面。配置以下设置：



- **域名**：键入 Android for Work 的域名。
- **域管理员帐户**：键入域管理员用户名。
- **服务帐户 ID**：键入服务帐户 ID。
- **绑定令牌**：键入或粘贴并复制绑定令牌。

- **启用 Android for Work**：单击可启用或禁用 Android for Work。

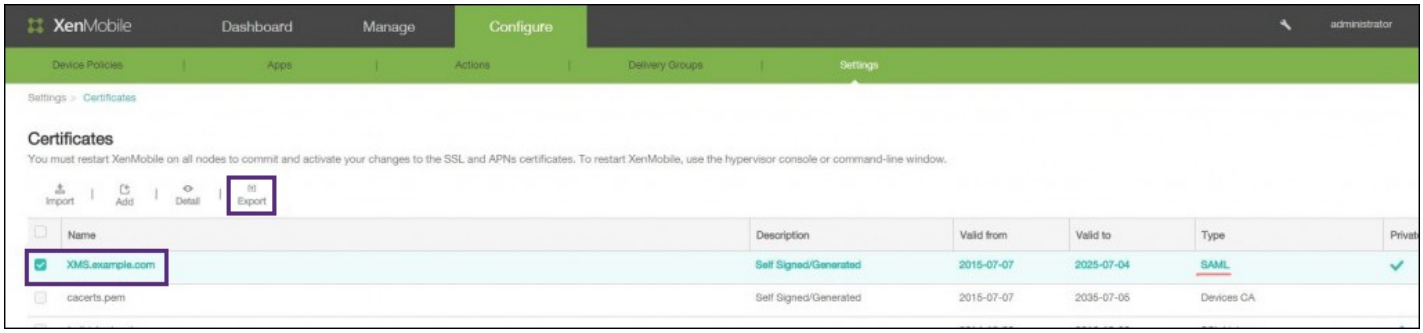
3. 单击**保存**。

启用基于 SAML 的单点登录

1. 登录到 XenMobile 10.1 控制台。

2. 单击**配置->设置->证书**。此时将显示**证书**页面。

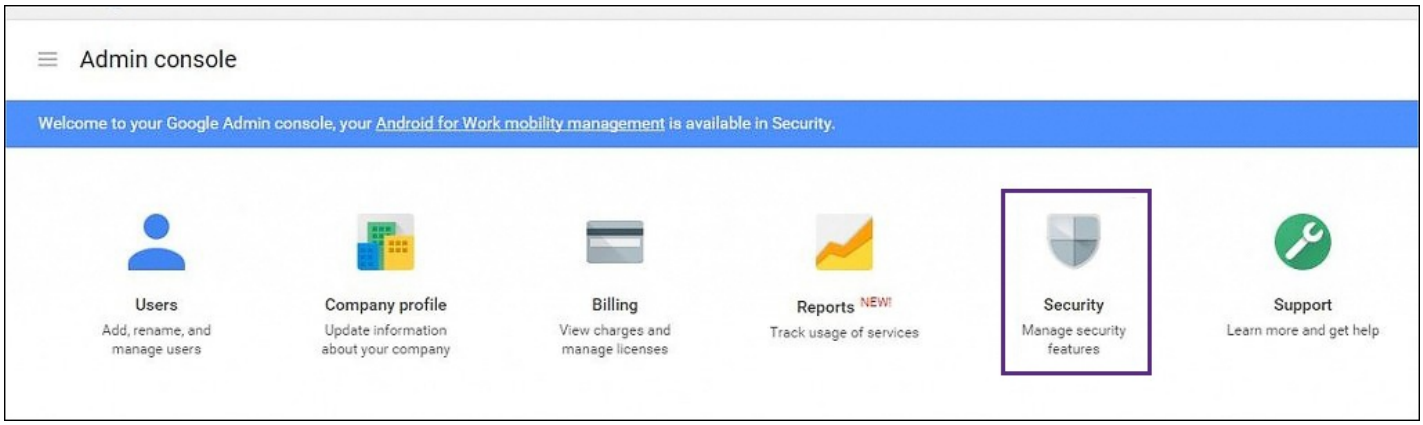
3. 在**证书**页面上的证书列表中，单击 SAML 证书。



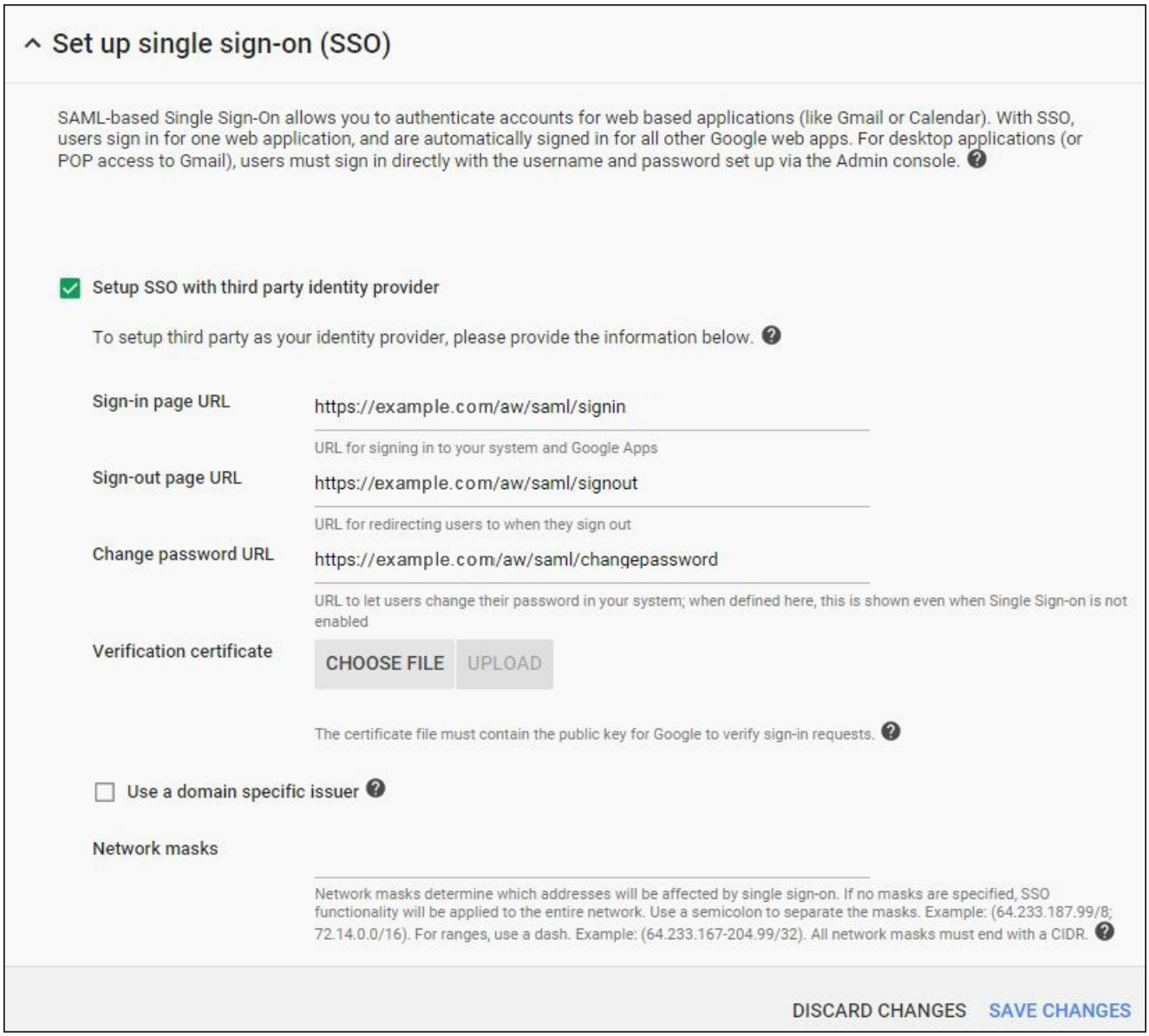
4. 单击**导出**并将证书保存到您的计算机。

5. 使用您的 Android for Work 管理员凭据登录 Google 管理门户，网址为 https://admin.google.com。

6. 单击 **Security**（安全）。



7. 在 **Security**（安全）下，单击 **Set up single sign-on (SSO)**（设置单点登录(SSO)），然后配置以下设置：

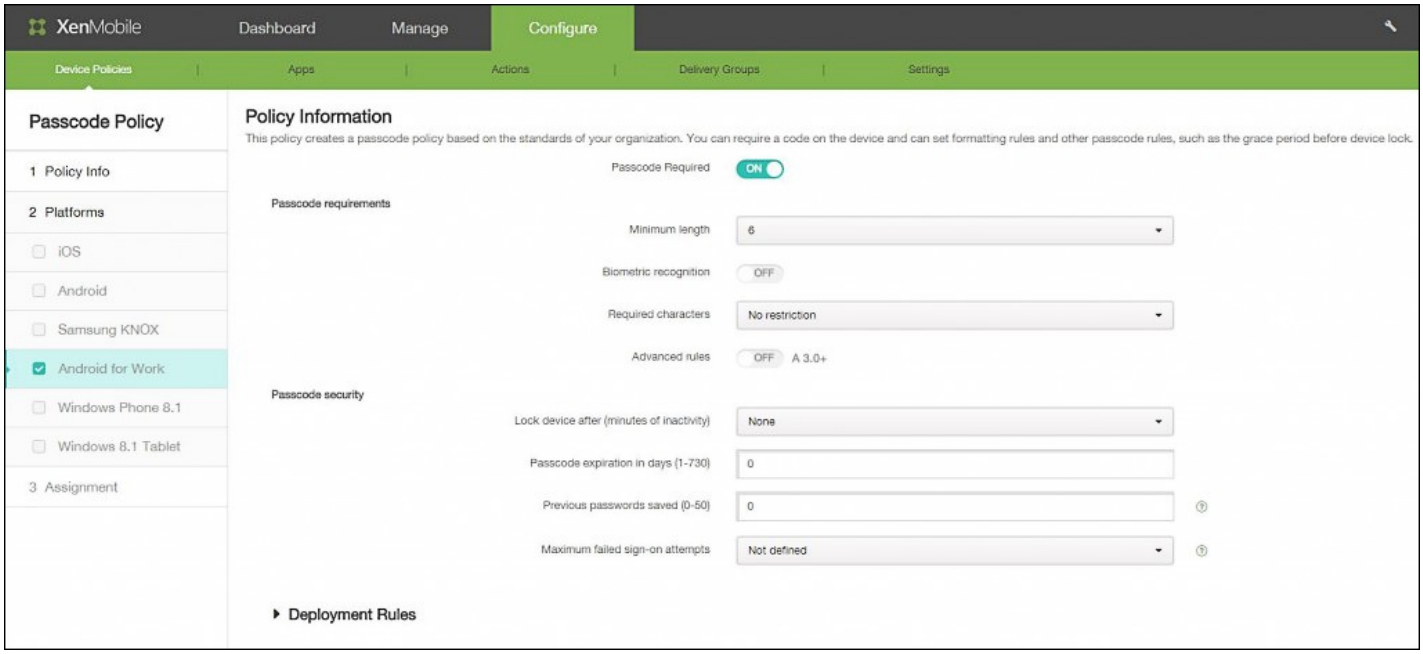


- **Sign-in page URL**（登录页面 URL）：键入用户登录到您的系统和 Google Apps 时使用的 URL。例如：https:///aw/saml/signin。
- **Sign-out page URL**（注销页面 URL）：键入注销时用户被重定向到的 URL。例如：https:///aw/saml/signout。
- **Change password URL**（更改密码 URL）：键入 URL 以允许用户更改其系统中的密码。例如：https:///aw/saml/changepassword。在此处定义时，即使 SSO 不可用，用户也可以看到此信息。
- **Verification certificate**（验证证书）：单击“CHOOSE FILE”（选择文件）并导航到从 XenMobile 导出的 SAML 证书。

8. 单击 **SAVE CHANGES**（保存证书）。

设置 Android for Work 设备策略

可以设置所需的任何设备策略，但最好设置通行码策略，以便要求用户在首次注册时在其设备上创建通行码。



设置任何设备策略的基本步骤如下：

1. 登录到 XenMobile 10.1 控制台。

2. 单击**配置->设备策略**。

3. 单击**添加**，然后选择要从**添加新策略**对话框中添加的策略（在此示例中，请单击**通行码**）。

4. 完成**策略信息**页面。

5. 单击 **Android for Work** 并配置策略设置。

6. 将策略分配到交付组。

有关设置设备策略的详细信息，请参阅设备策略。

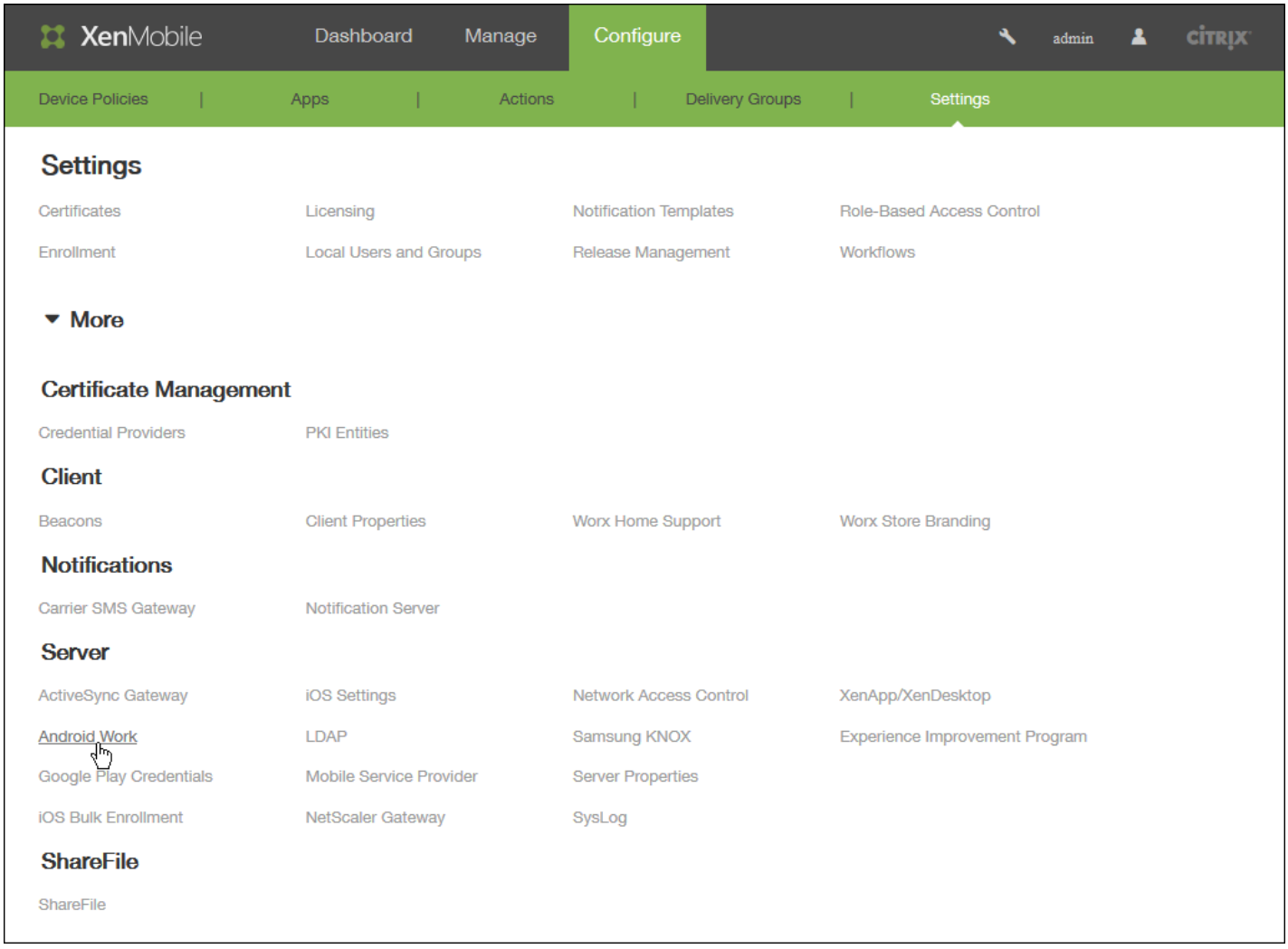
您的用户现在可以从 Google Play 应用商店下载 Worx Home 应用程序，然后在 XenMobile 中注册其设备（请务必使用用户主体名称进行注册）。设备成功注册后，Worx Home 将安装 Android for Work 配置文件，以便用户能够访问其 Android for Work 应用程序。在此过程中，系统可能会要求用户加密其设备，然后才能继续操作。

配置 Android for Work 帐户设置

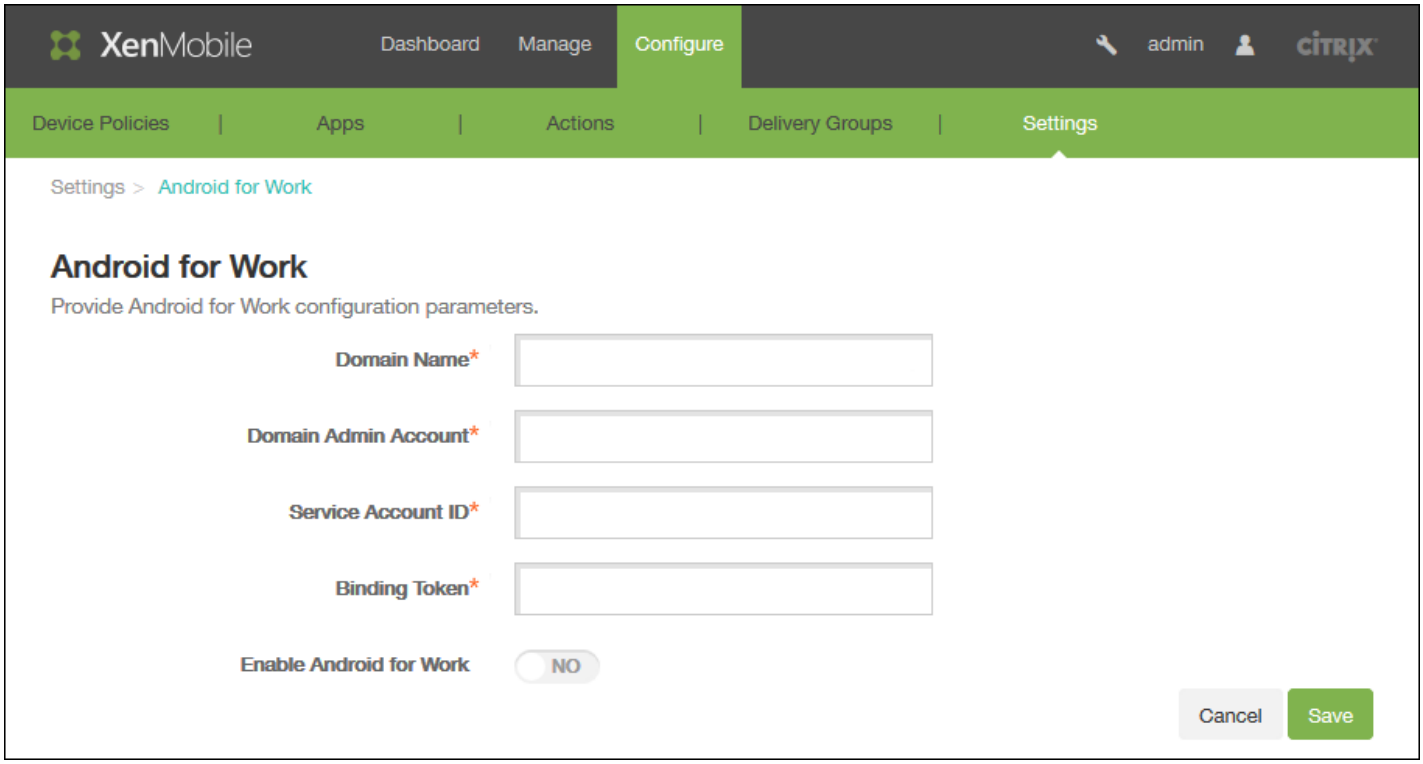
Oct 22, 2015

您必须在 XenMobile 中设置 Android for Work 域和帐户信息，才能管理用户设备上的 Android for Work 应用程序和策略。但是，执行此操作前，还必须在 Google 上完成 Android for Work 设置任务以设置域管理员，并获取服务帐户 ID 和绑定令牌。有关在 Google 上执行 Android for Work 设置任务的详细信息，请参阅使用 Android for Work 管理设备。

1. 在 XenMobile 控制台中，单击**配置 > 设置**。



2. 展开**更多**，然后在**服务器**下面，单击 **Android for Work**。此时将显示 **Android for Work** 页面。



3. 在 **Android for Work** 页面上，配置以下设置：

- **域名**：键入域名。
- **域管理员帐户**：键入域管理员用户名。
- **服务帐户 ID**：键入 Google 服务帐户 ID。
- **绑定令牌**：键入或粘贴设置 Android for Work 帐户时从 Google 收到的绑定令牌。
- **启用 Android for Work**：选择是否启用 Android for Work。

4. 单击**保存**。

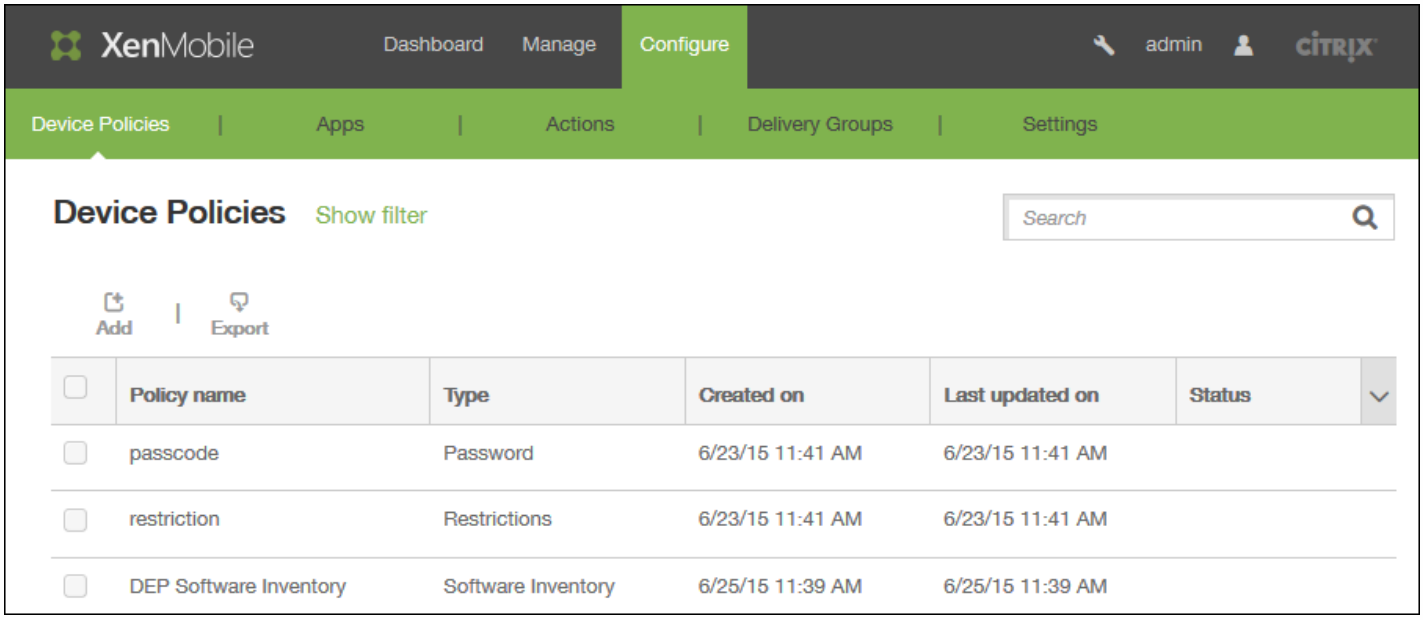
Android for Work 应用程序限制策略

Oct 22, 2015

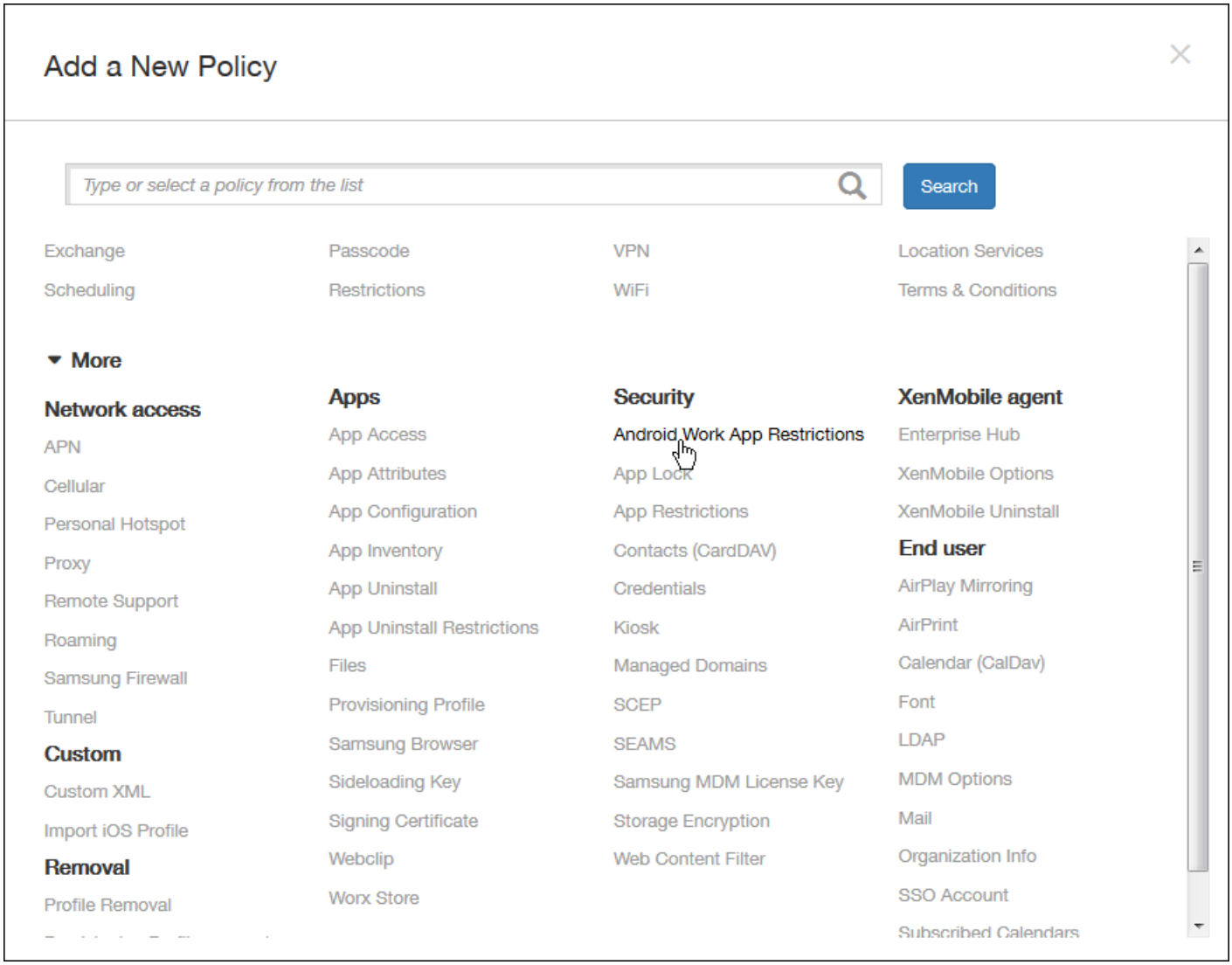
可以修改与 Android for Work 应用程序关联的限制，但是在执行此操作前，必须满足以下必备条件：

- 在 Google 上完成 Android for Work 设置任务。有关详细信息，请参阅使用 Android for Work 管理设备。
- 创建一组 Google Play 凭据。有关详细信息，请参阅 Google Play 凭据。
- 配置 Android for Work 帐户设置。有关详细信息，请参阅配置 Android for Work 帐户设置。
- 将 Android for Work 应用程序添加到 XenMobile。有关详细信息，请参阅向 XenMobile 添加应用程序。

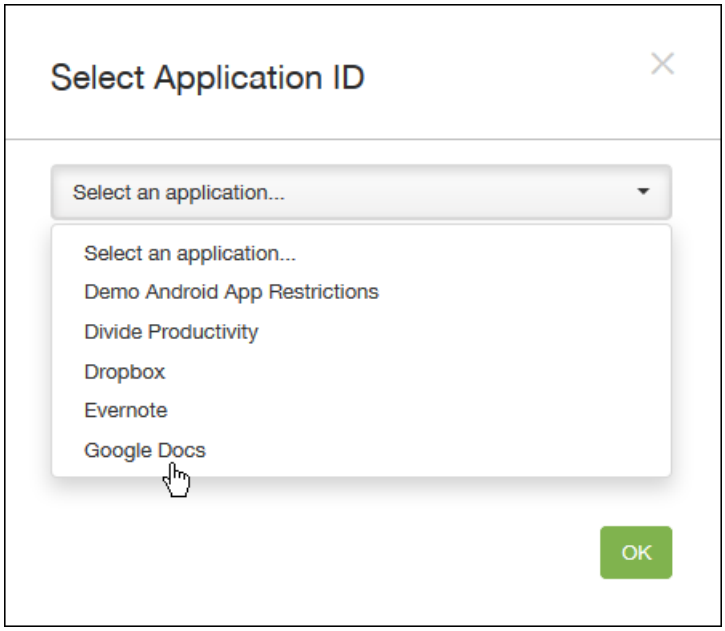
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。



2. 单击**添加**添加新策略。将显示**添加新策略**页面。

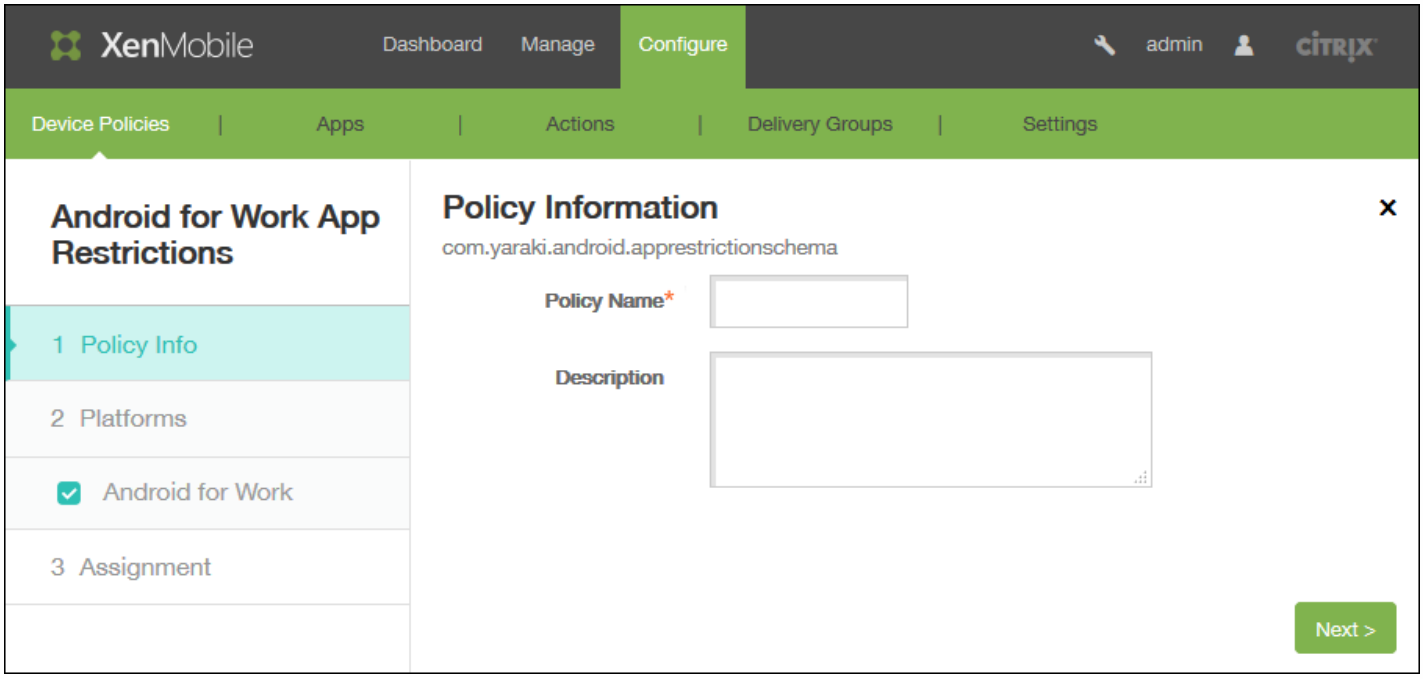


3. 在**添加新策略**页面上，单击**更多**，然后在**安全性**下方，单击 **Android for Work 应用程序限制**。此时将显示一个请求您选择应用程序的对话框。



4. 在列表中，选择要应用限制的应用程序，然后单击**确定**。

- 如果没有要添加到 XenMobile 中的 Android for Work 应用程序，将无法继续操作。有关向 XenMobile 添加应用程序的详细信息，请参阅向 XenMobile 添加应用程序。
- 如果应用程序没有关联任何限制，将显示有关相关影响的通知。单击**确定**取消对话框。
- 如果应用程序具有与之关联的限制，将显示 **Android for Work 应用程序限制策略**信息页面。

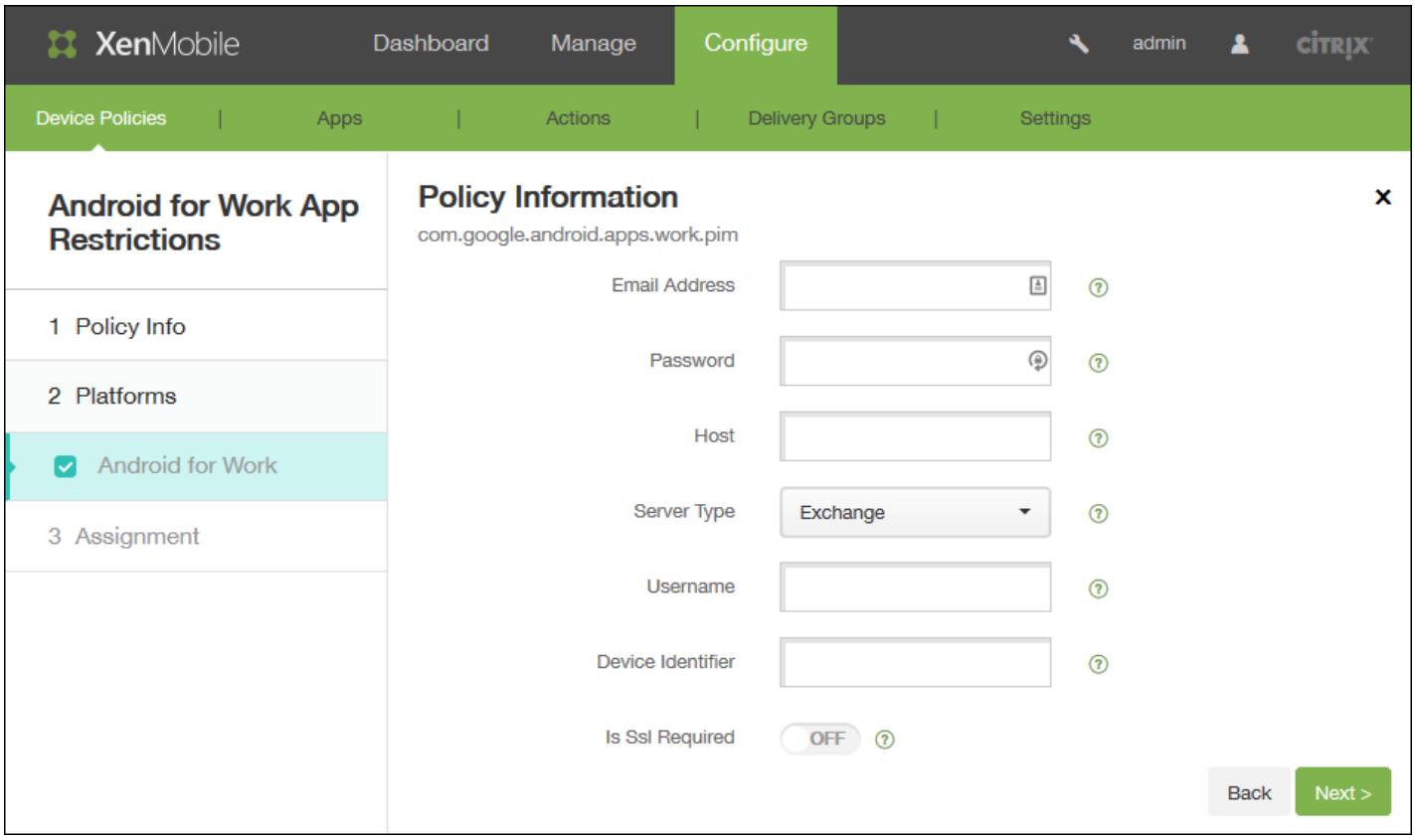


5. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

6. 单击**下一步**。此时将显示**策略平台**页面。

7. 在**平台**下面的 **Android for Work** 策略信息窗格中，为所选的应用程序配置设置。显示的设置取决于与所选应用程序关联的限制。下图显示了 Google Docs 应用程序可用的部分选项。



8. 展开**部署规则**，然后配置以下设置：

默认情况下将显示**基础**选项卡。

- 在此列表中，单击选项以确定部署策略的时间。

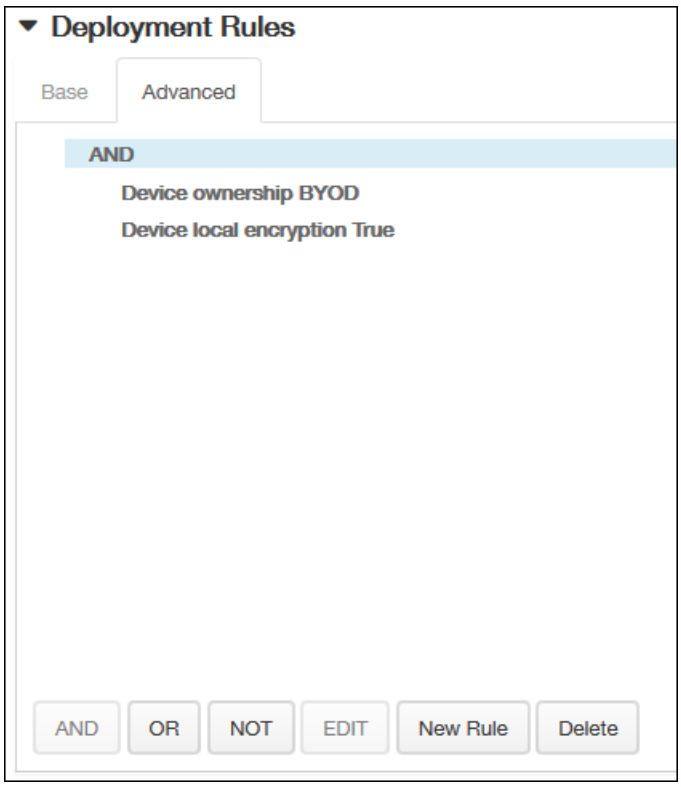
i.可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是**全部**。

ii.单击**新建规则**以定义条件。

iii.在列表中，单击条件，如**设备所有权**和 **BYOD**，如上图所示。

iv.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。

- 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。

- 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。

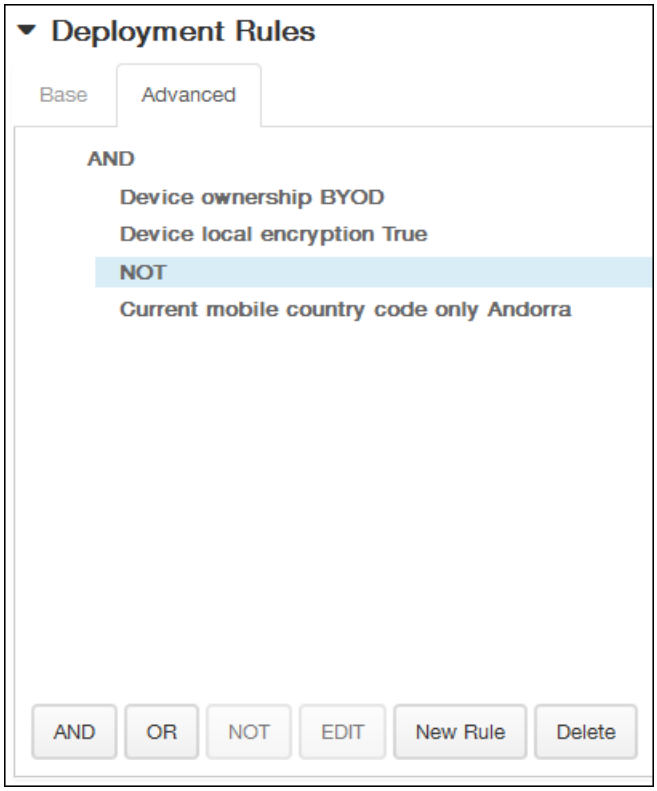
i.单击 **AND**、**OR** 或 **NOT**。

ii.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。

iii.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。

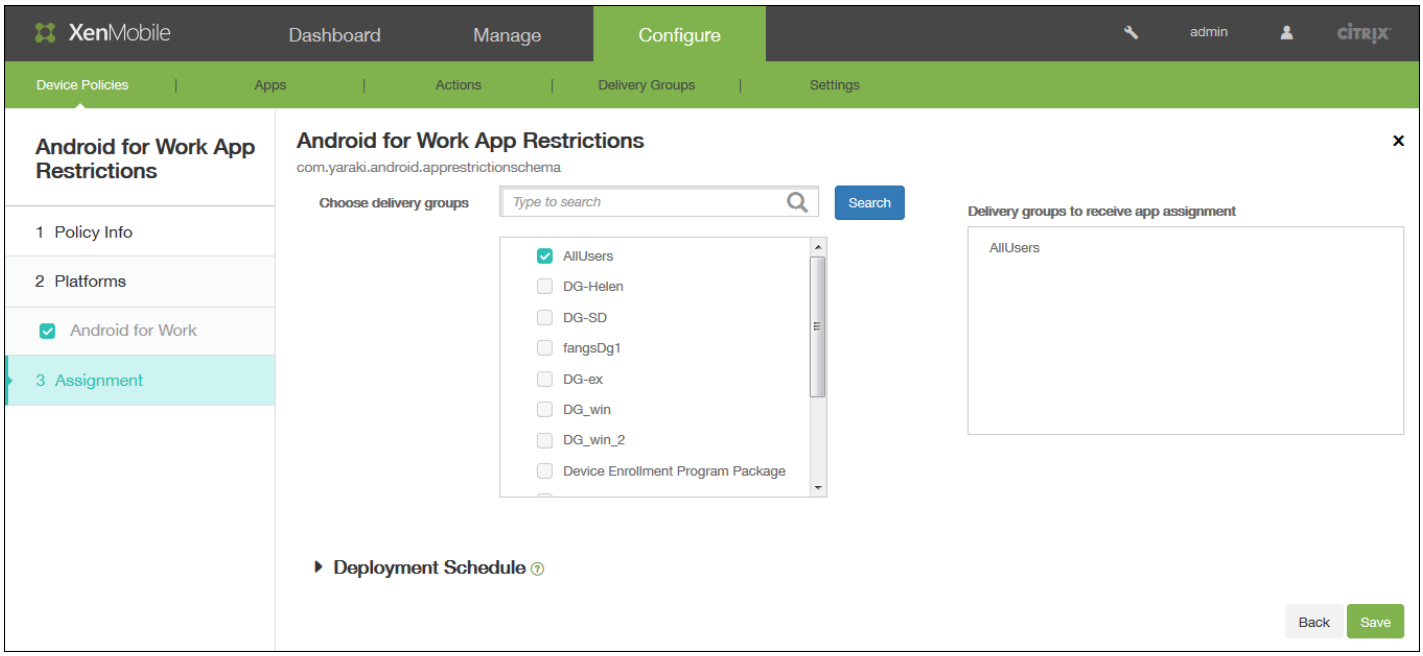


9. 单击**下一步**。

此时将显示 **Android for Work 应用程序限制策略**分配页面。

10. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。

选择的组显示在**用于接收应用程序分配的交付组**列表中。



11. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。默认选项为**开**。如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。默认选项为**立即**。
- 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
- 在**部署条件**旁边，单击**每次连接时**或单击**仅当之前的部署失败时**。默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。默认选项为**关**。

> ## 注意
>
> 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：为所有平台配置的部署计划都相同。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。

配置部署规则

Aug 04, 2016

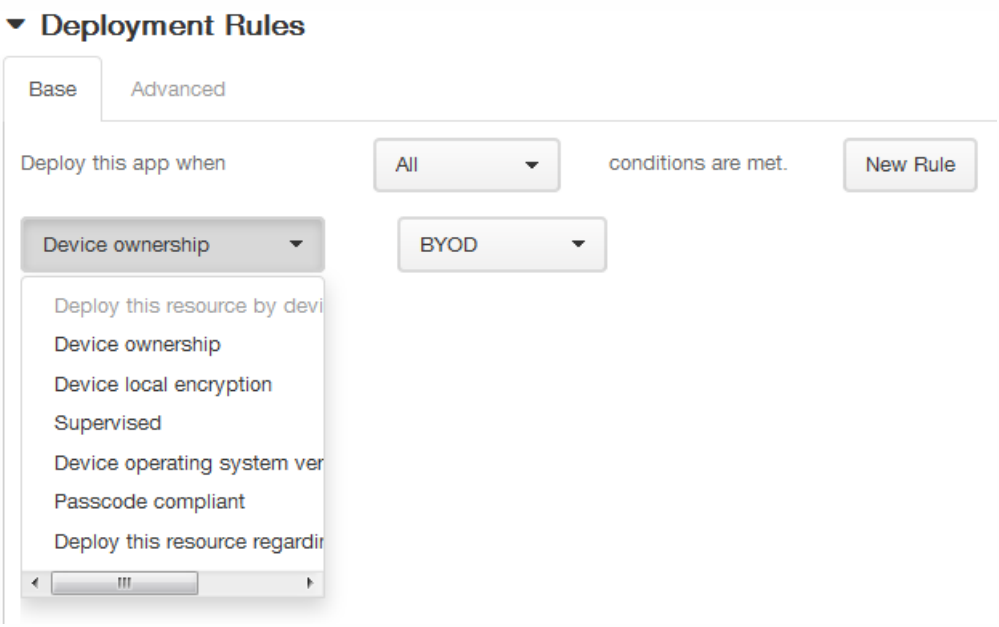
本部分介绍以下内容：

- 部署规则 - 影响软件包部署结果的参数。
- 部署计划 - 用于指定 XenMobile 何时将软件包推送到设备的选项。

配置部署规则

部署规则是一些用于控制软件包部署结果的参数。 您可以指定针对设备属性、应用程序和操作的部署规则。 在确定软件包的部署顺序时，XenMobile 将使用您为设备属性指定的部署规则来过滤策略、应用程序、操作和交付组。 有关详细信息，请参阅部署顺序。

可以基于特定操作系统版本、特定硬件平台或其他一些组合执行软件包部署。 在此用于添加和编辑设备属性、应用程序和操作的向导中，同时为“基本”和“高级”规则编辑器。 “高级”视图是一种自由形式编辑器。 下图说明了添加或编辑应用程序时显示的“部署规则”屏幕：



基础部署规则

基础部署规则由预先定义的测试和所生成的操作组成。 结果尽可能预先内置在示例测试中。 例如，基于硬件平台部署软件包时，现有的所有已知平台将填入生成的测试中，从而大大缩短规则创建时间，并限制了可能出现的错误。

单击**新建规则**以向软件包添加规则。

注意：规则生成器包含特定于每个测试的详细信息。

要创建新的规则，请选择规则模板，选择条件类型，然后自定义规则。 自定义规则涉及到修改说明。 完成对设置的配置时，将规则添加到软件包中。

您可以根据需要添加多个规则。 当所有的规则都匹配时，将部署软件包。

高级部署规则

如果单击**高级**选项卡，将出现**高级规则编辑器**。

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

配置部署计划

XenMobile 使用您为操作、应用程序和设备策略指定的部署计划来控制这些项目的部署。 可以将部署过程指定为立即执行、在特定日期和时间执行或根据部署条件执行。 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，此选项不适用于 iOS。

如果不更改部署计划选项，则将在每次连接时立即执行部署。 部署计划选项包括：

部署：默认为**开**。要阻止部署，请将此设置更改为**关**。

部署计划：默认为**立即**。 要指定部署时间，请选择**稍后**，然后选择日期并输入时间。

部署条件：默认为**每次连接时**。 要限制部署，请将此设置更改为**仅当之前的部署失败时**。

为始终启用的连接部署：默认为**关**。 对于 iOS 和 Windows 移动设备：如果将设备**连接计划策略**选项为**始终**，则必须将**为始终启用的连接部署**更改为**开**。 对于 Android 设备：XenMobile 服务器属性**后台部署**要求您将部署到 Android 设备的每个策略的**为始终启用的连接部署**设置为**开**。

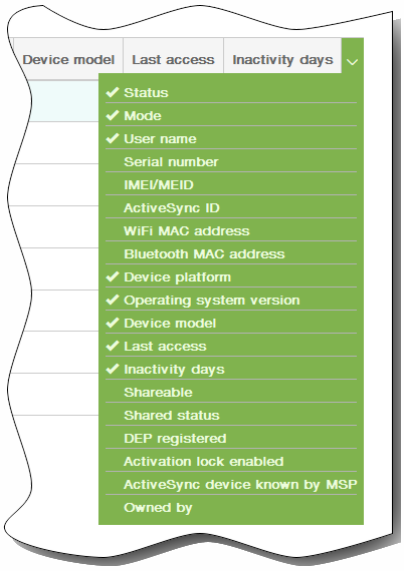
添加设备并查看设备详细信息

Oct 22, 2015

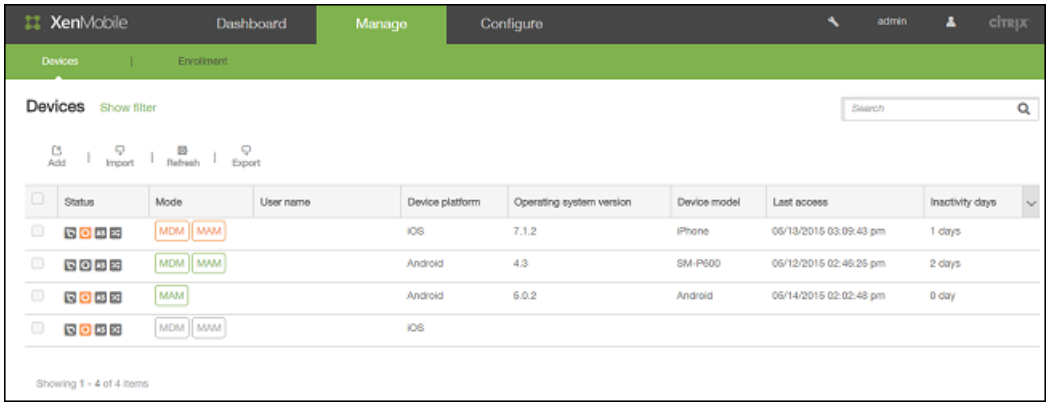
XenMobile 服务器存储库数据库中存储移动设备的列表。每个移动设备通过唯一的序列号和/或国际移动设备标识 (IMEI)/移动设备标识符 (MEID) 标识定义。要将设备填充到 XenMobile 控制台中，可以手动添加设备或从文件导入设备列表。请参阅设备置备文件格式。

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（设备未越狱、设备未托管、Active Sync Gateway 不可用、无部署故障）、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，然后在多个可用标题中，单击要在表格中查看的标题，或取消选中不希望看到的标题。



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。

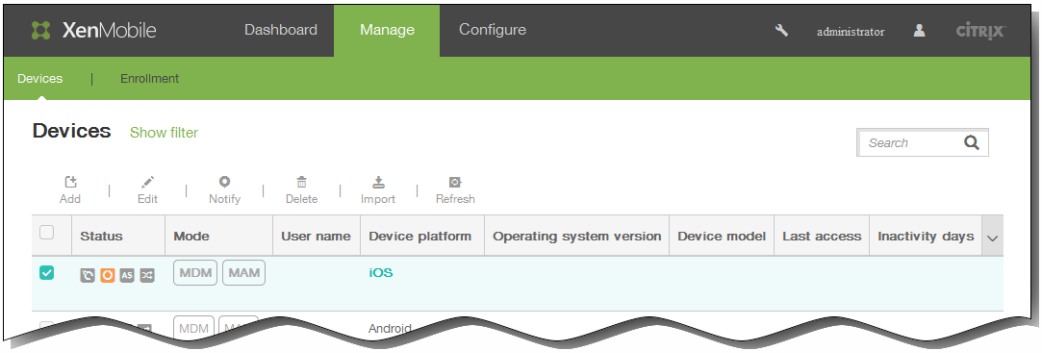


手动添加设备

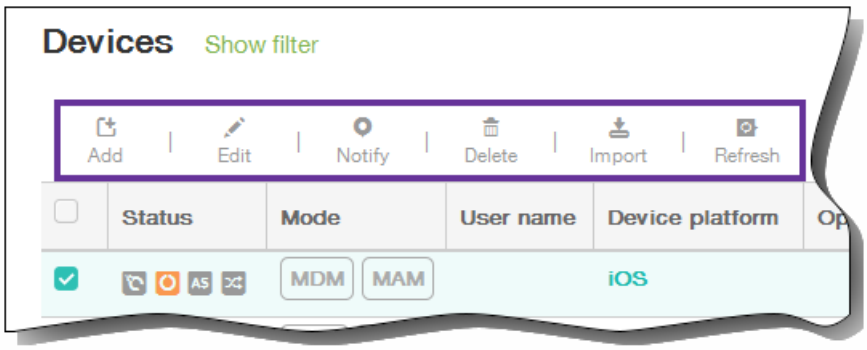
1. 在 XenMobile 控制台中，单击管理 > 设备，然后单击添加。此时将显示添加设备页面。
2. 在选择平台中，单击 iOS、Android 或 Symbian。
3. 输入以下信息：
    1. iOS：输入序列号。

2. Android：输入序列号和 IMEI/MEID。
3. Symbian：输入 IMEI/MEID。

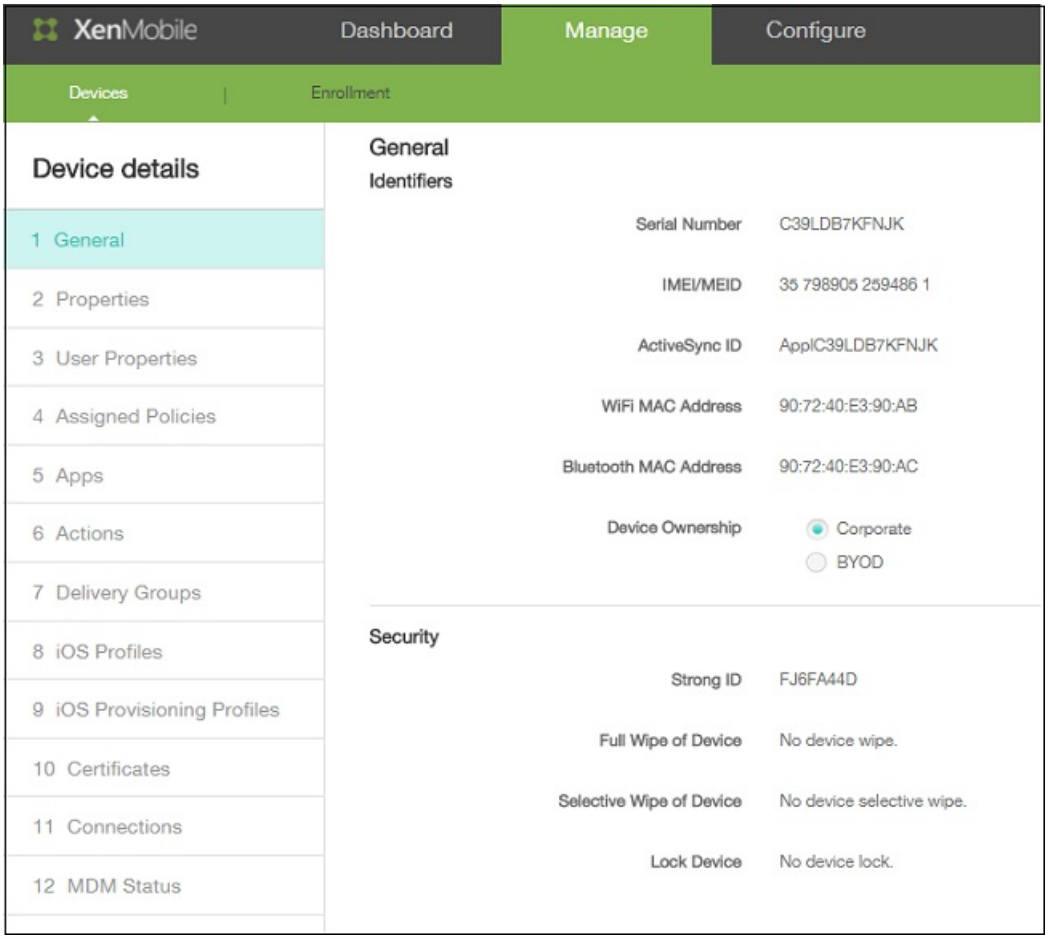
4. 单击添加。设备将添加到所显示设备表格中的列表底部。
5. 在此列表中，选择您所添加的设备，然后在显示的菜单中，单击编辑以查看并确认设备详细信息。



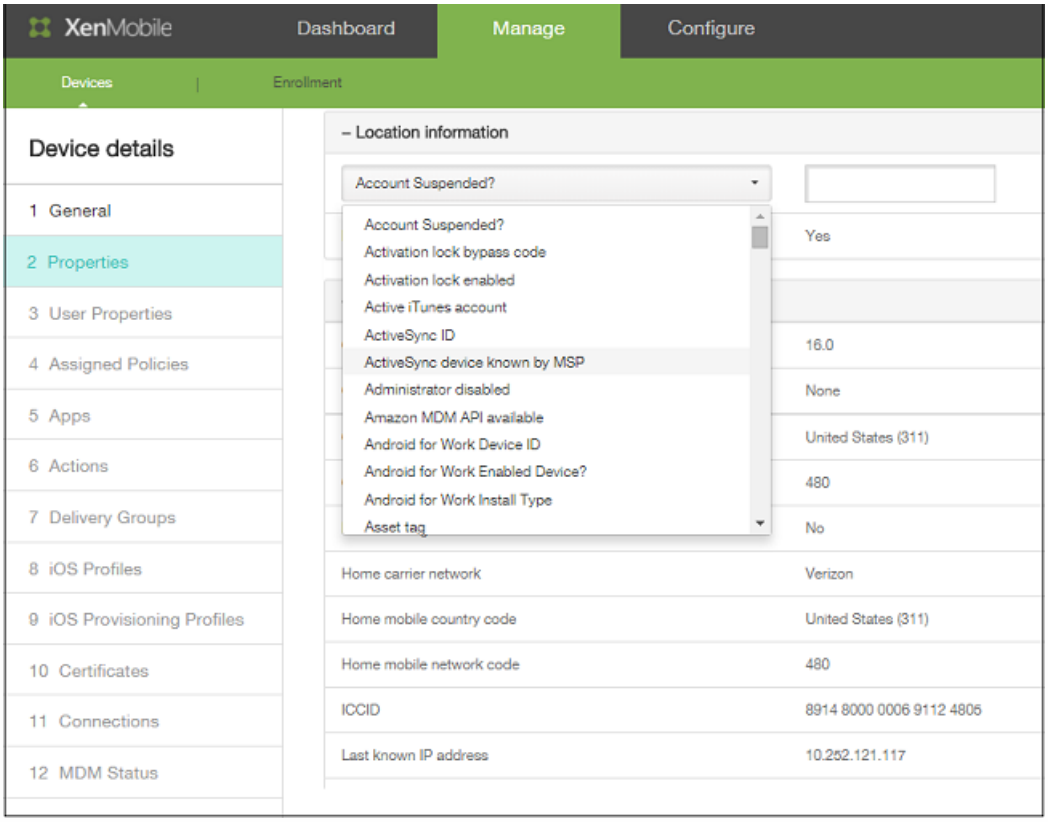
注意：如果选中某个设备旁边的复选框，选项菜单将显示在设备列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。



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。

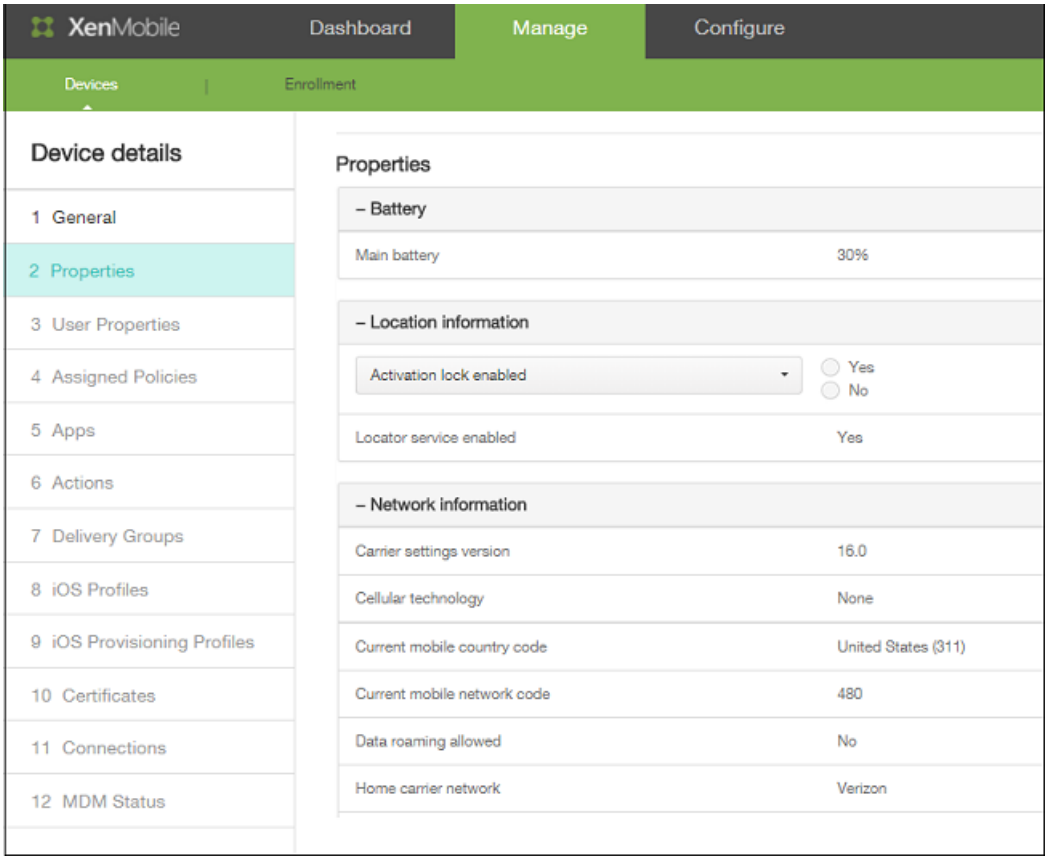


7. 在安全下面，确认显示的信息（精确的参数列表因平台类型而异）：强 ID、完全擦除设备、选择性擦除设备、锁定设备、设备解锁、否认拥有的设备、激活锁跳过、设备清除限制。
8. 单击下一步以添加属性。
9. 在属性页面上，单击添加以查看可以为设备置备的属性列表。将显示可用属性的列表。



10. 在列表中，单击要置备的属性，然后设置其值。 例如，您可以选择属性已启用激活锁并将值设置为是或否。
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。



Assigned Policies（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。

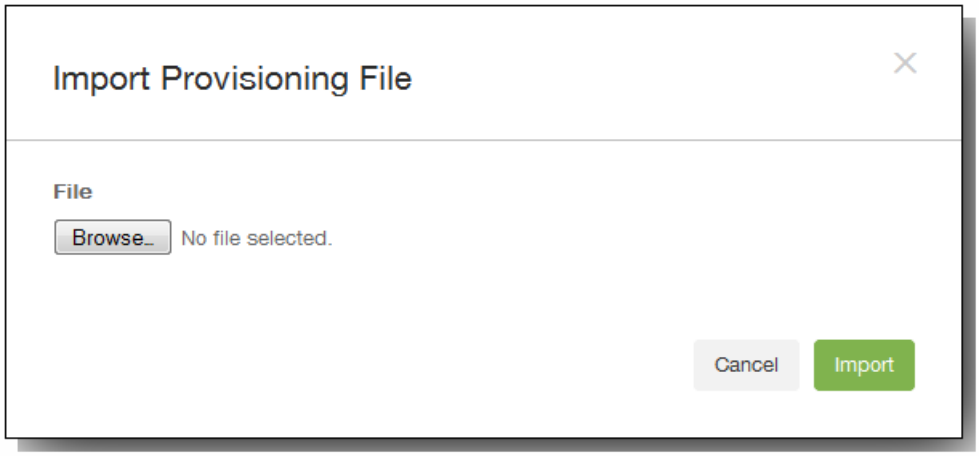
- 已分配的策略：显示已分配策略的数量，包括已部署的策略数、待定策略数和失败的策略数。也会显示每个策略的名称、类型和上次部署信息。
- 应用程序：以清单形式显示应用程序的数量，包括已安装的应用程序数、待定应用程序数和失败的应用程序数。
  - 对于已安装的应用程序，将显示以下信息：名称、所有权、版本、作者、大小、安装时间、标识符和类型。
  - 对于待定和失败的应用程序，将显示以下信息：名称、上次部署时间、标识符和类型。
- 操作：显示操作数，包括已部署的操作数、待定操作数和失败的操作数。每个操作显示名称和上次部署信息。
- Delivery Groups（交付组）：显示成功、待定和失败的交付组数量。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。

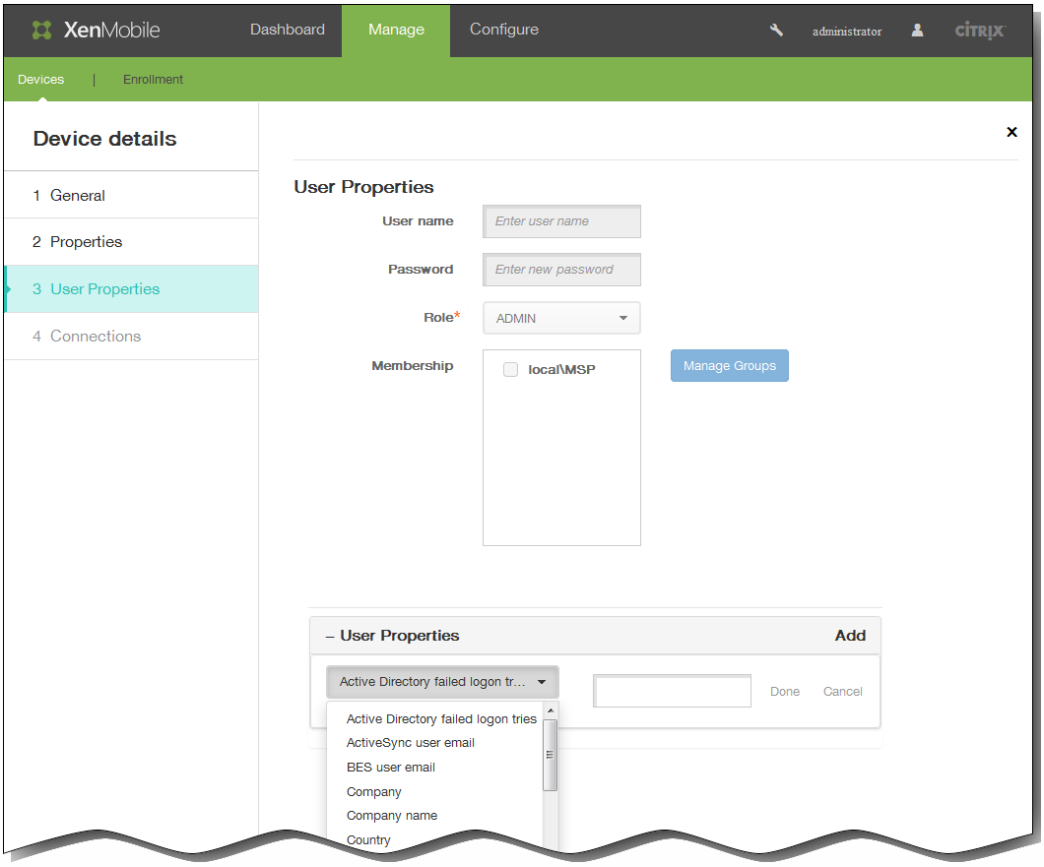
1. 在设备表格上方的菜单中，单击导入。 此时将显示导入置备文件对话框。



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。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 Assigned Properties（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。

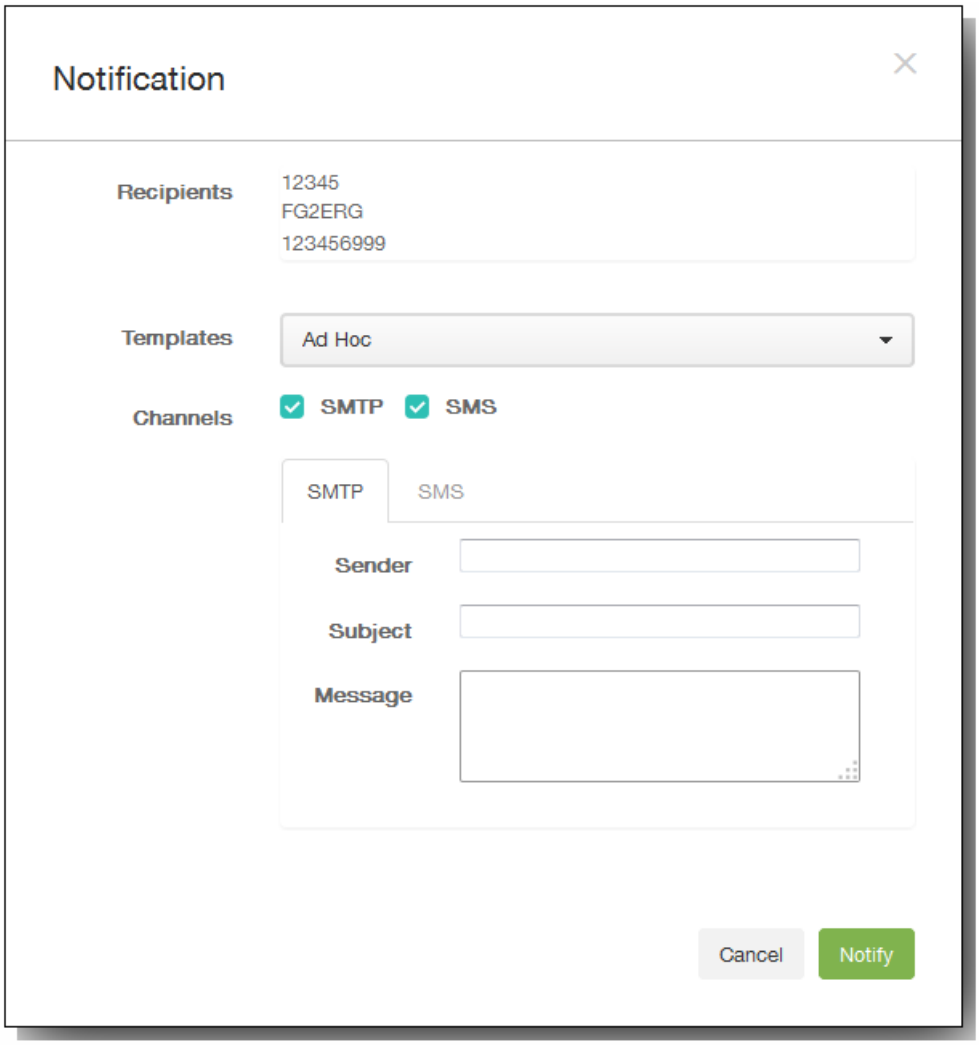
- 要添加用户属性，请单击添加。
  - 在列表中，单击要添加的属性，输入属性的值，然后单击完成或取消。为要添加的每个属性重复执行此步骤。
- 要编辑某个属性，请单击此属性，修改其设置，然后单击完成或取消。
- 要删除某个属性，请悬停在此列表的上方，然后单击右侧的 X。项目立即被删除。

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。 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。

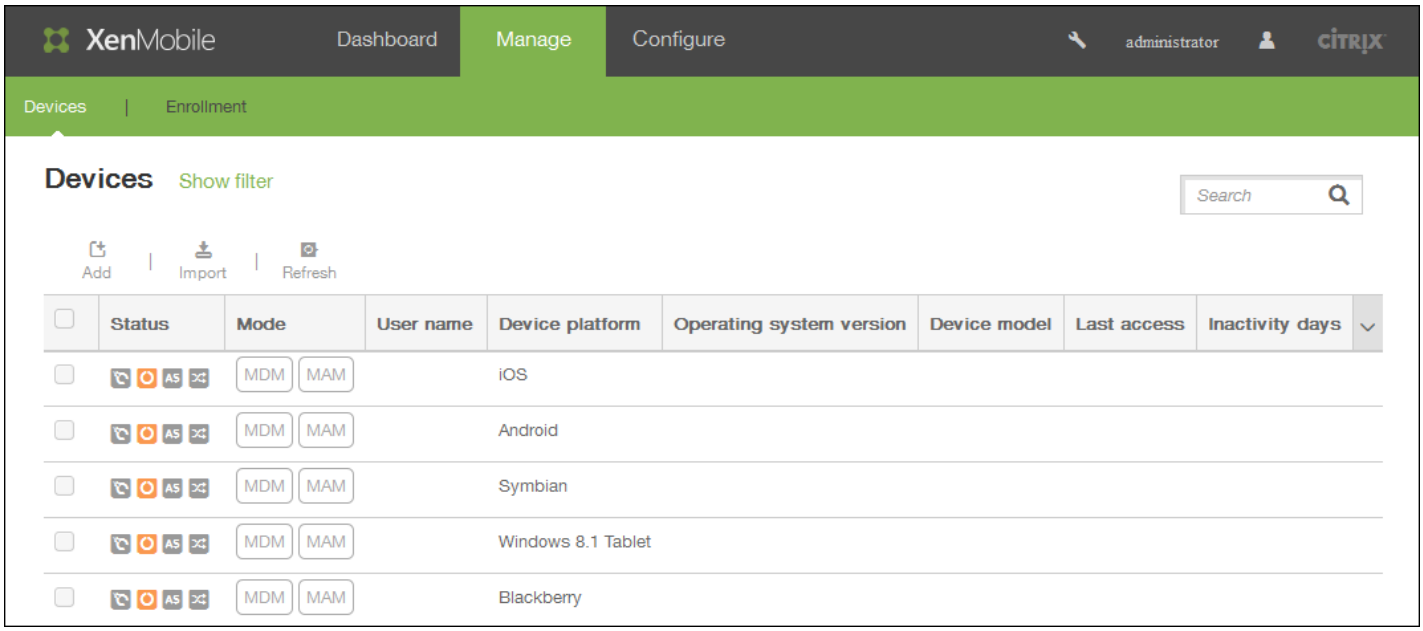
锁定 iOS 设备

Nov 20, 2015

您可以锁定 iOS 设备，同时在设备锁定屏幕上显示消息和电话号码。iOS 7 和 8 设备支持此功能。

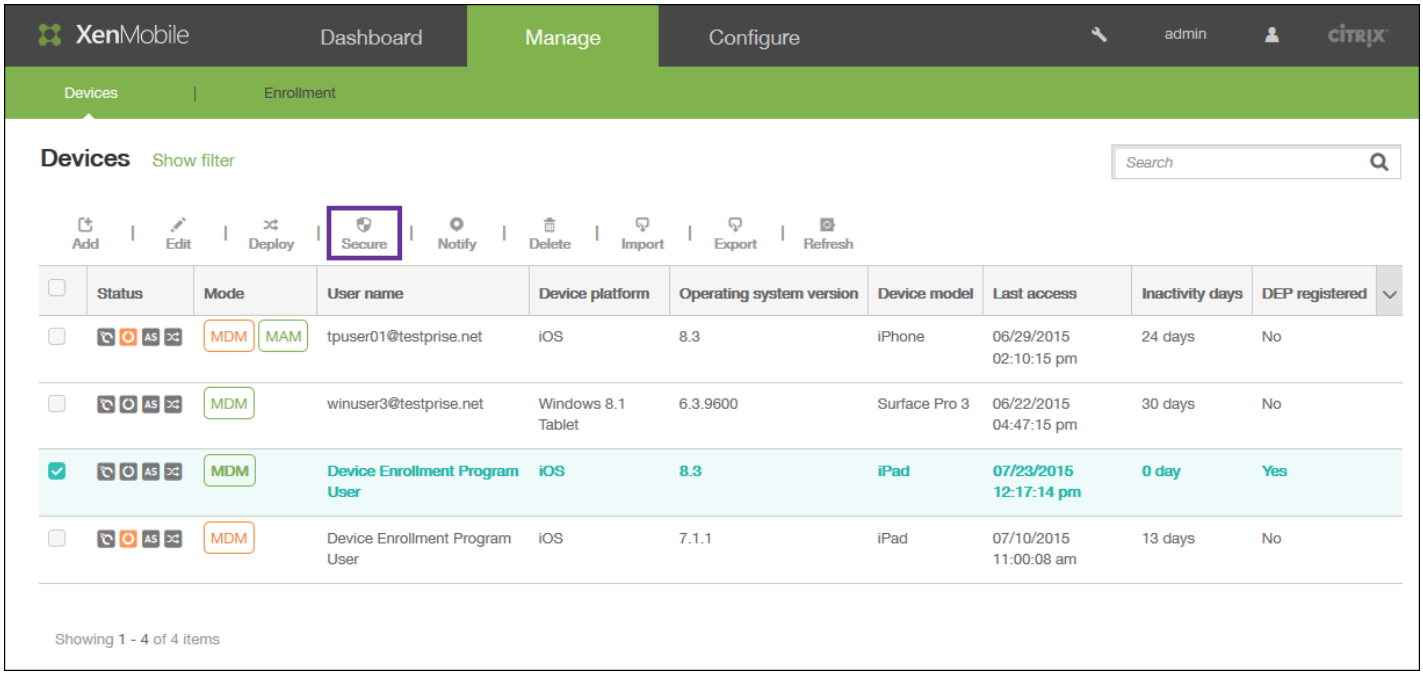
如果选择在锁定屏幕上显示消息和电话号码，同时，如果您在 XenMobile 控制台中设置了通行码策略，或者如果用户已在设备上手动启用通行码，消息和电话号码将仅显示在锁定设备上。

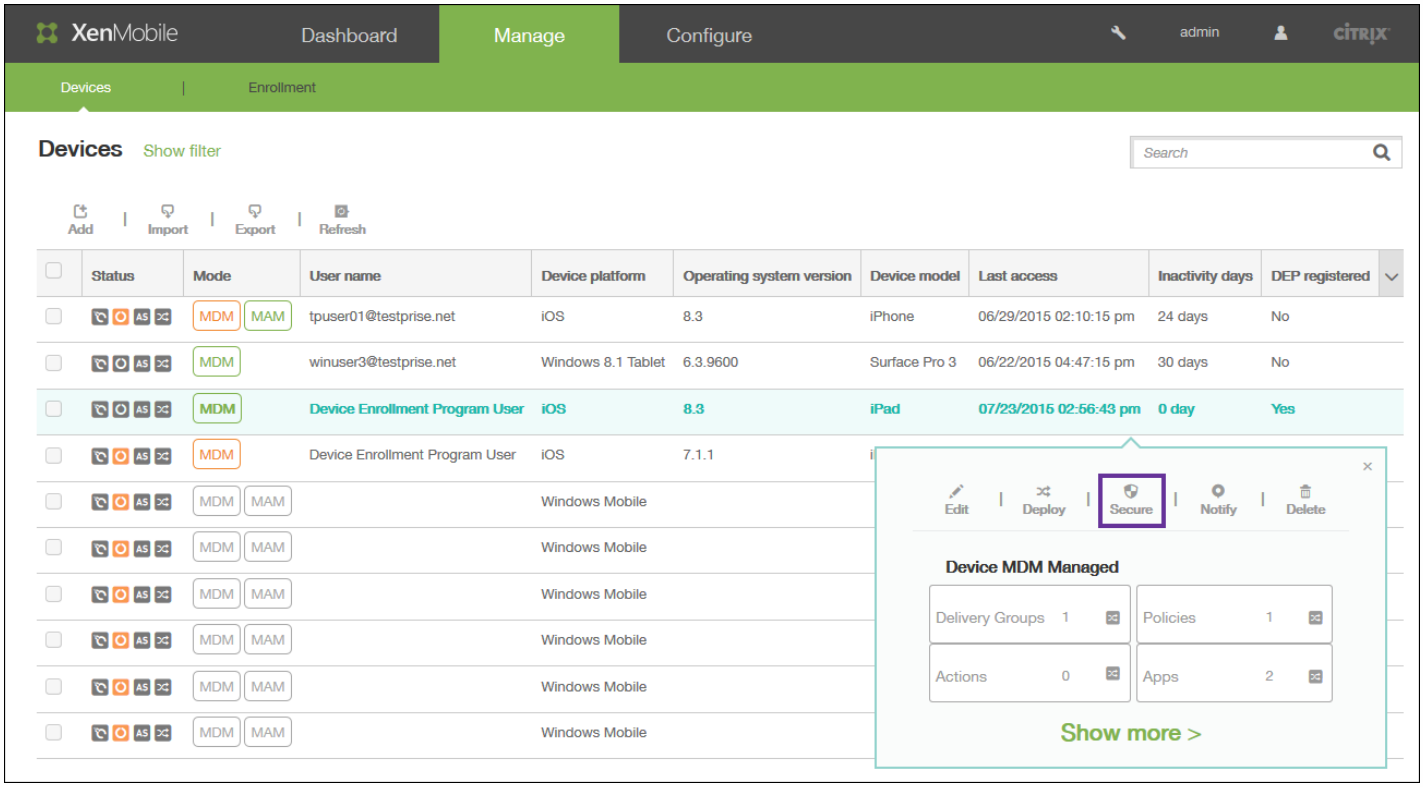
1. 在 XenMobile 控制台中，单击**管理 > 设备**。此时将显示**设备**页面。



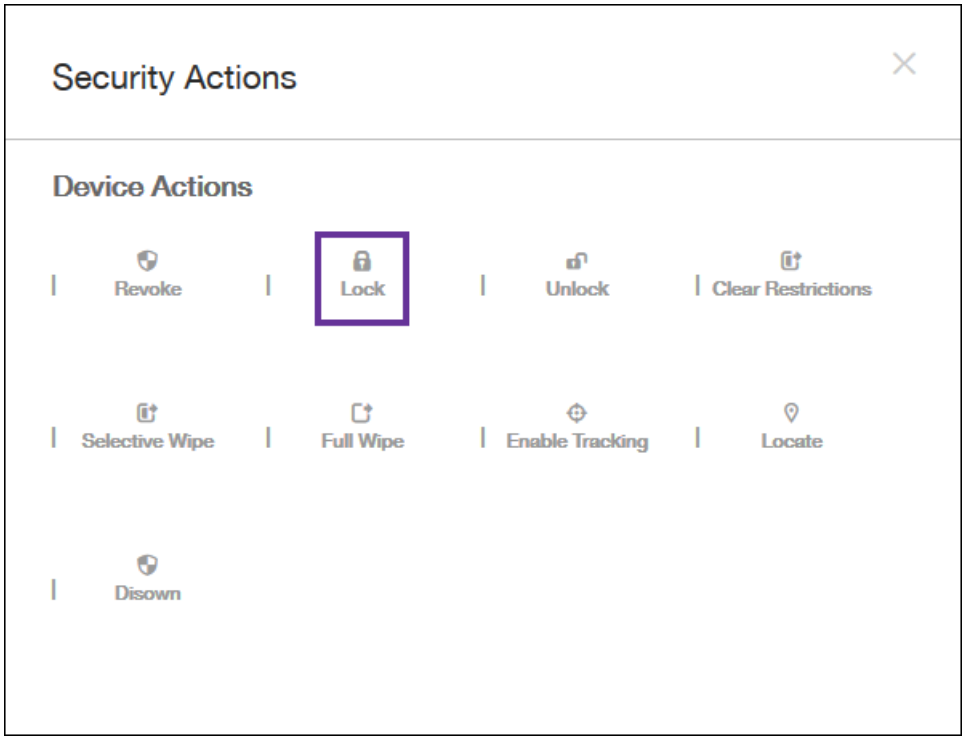
2. 选择要锁定的 iOS 设备。

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

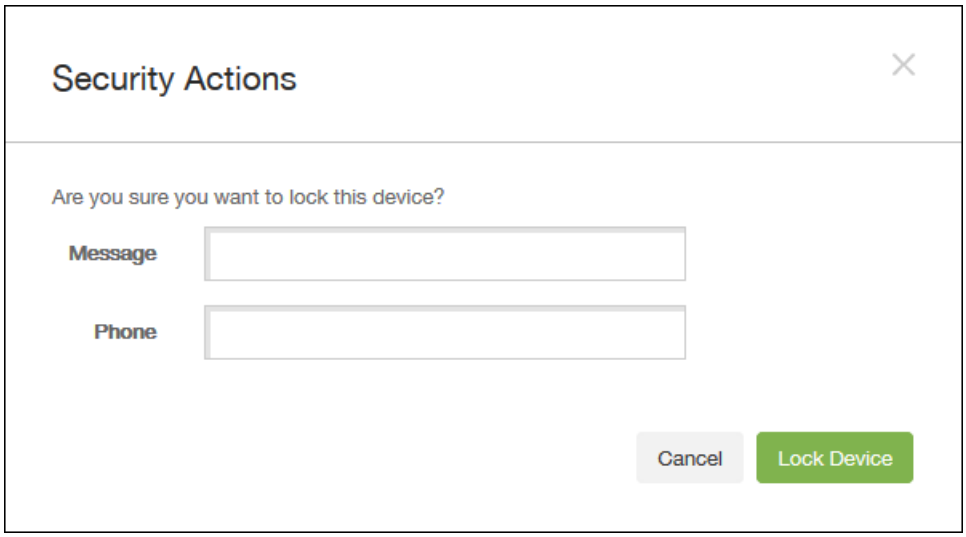




3. 在选项菜单中，选择**安全**。将显示**安全操作**对话框。



4. 选择**锁定**。此时将显示**安全操作**确认对话框。



5.（可选）输入将显示在设备锁定屏幕上的消息和电话号码。

6. 单击**锁定设备**。

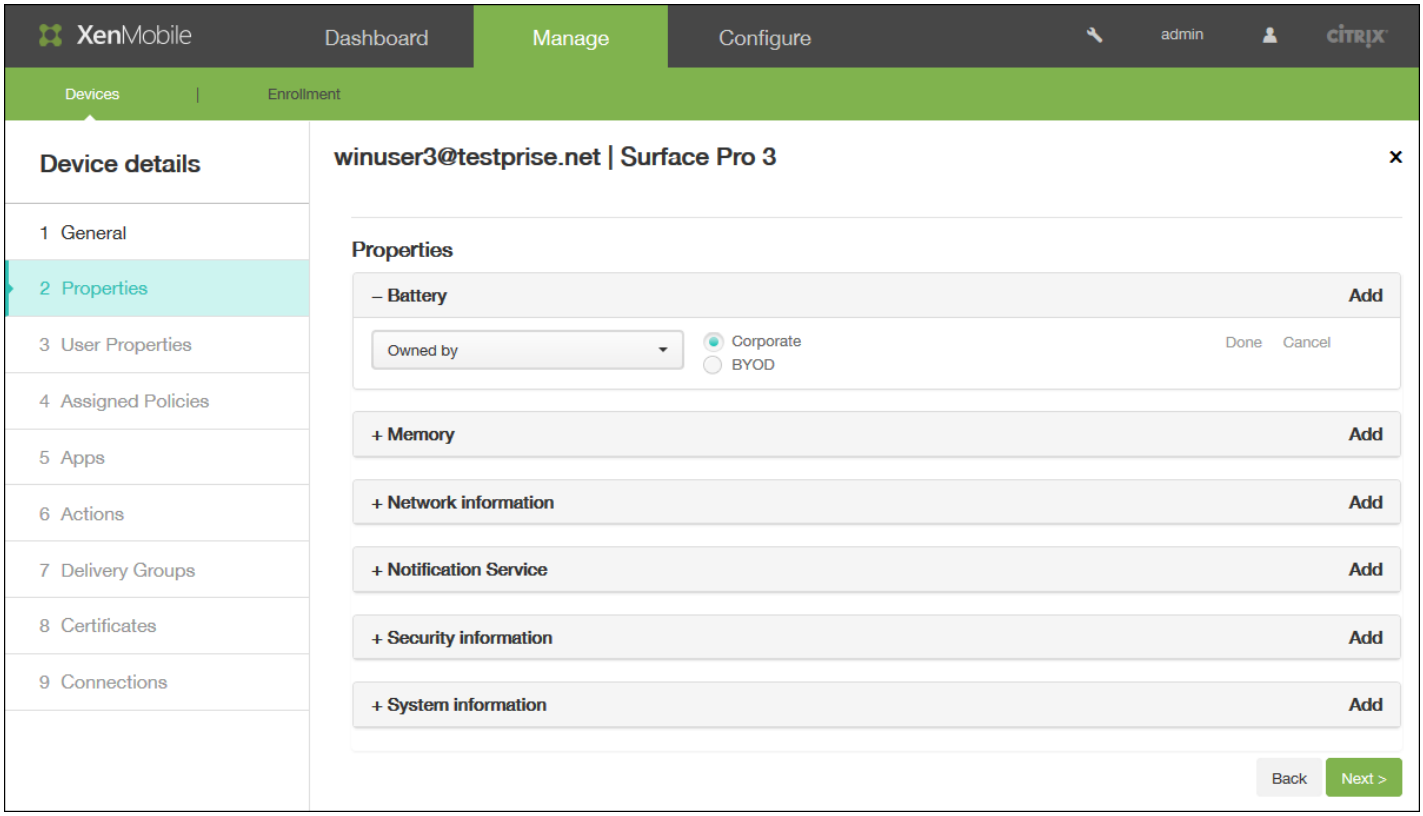
手动标记用户设备

Oct 22, 2015

可在 XenMobile 中通过以下三种方式之一手动标记设备：

- 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**选项卡向设备添加某个属性，添加名为**所有者**的属性，然后选择**公司**或**BYOD**（员工所有），来手动标记设备。



设备置备文件格式

Oct 22, 2015

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：1050BF3F5173010816100655105903 91
- 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

Apr 22, 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

Aug 04, 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：

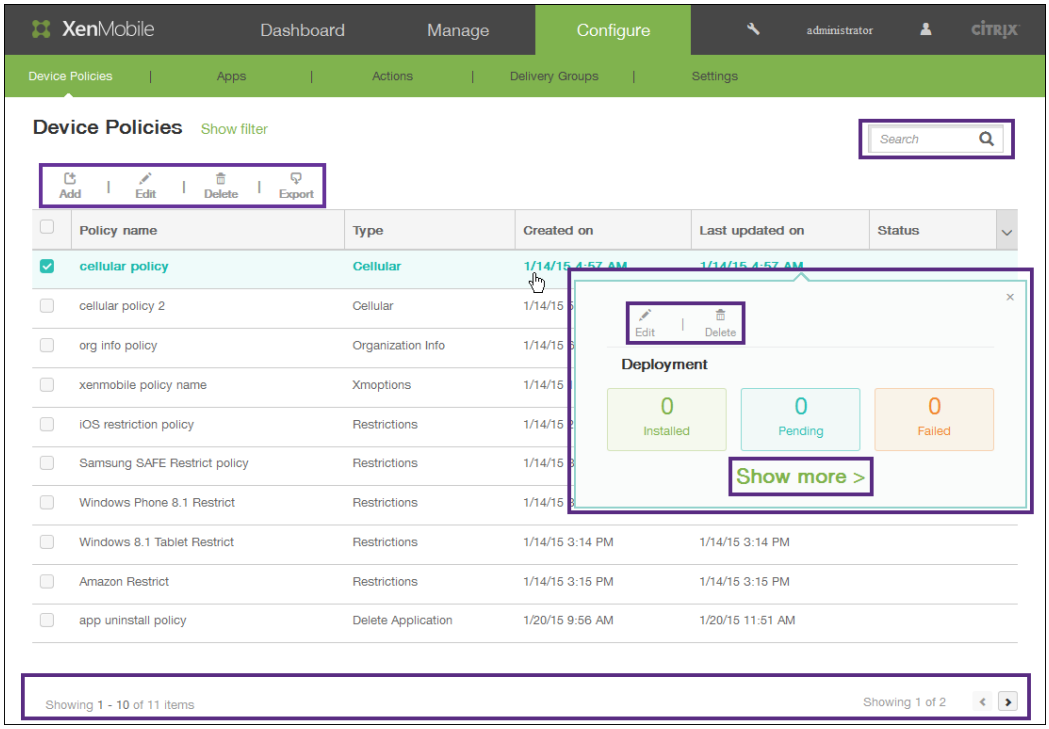
1. 为策略命名并添加说明。
2. 配置一个或多个平台。
3. 创建部署规则（可选）。
4. 将策略分配到交付组。
5. 配置部署计划（可选）。

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。

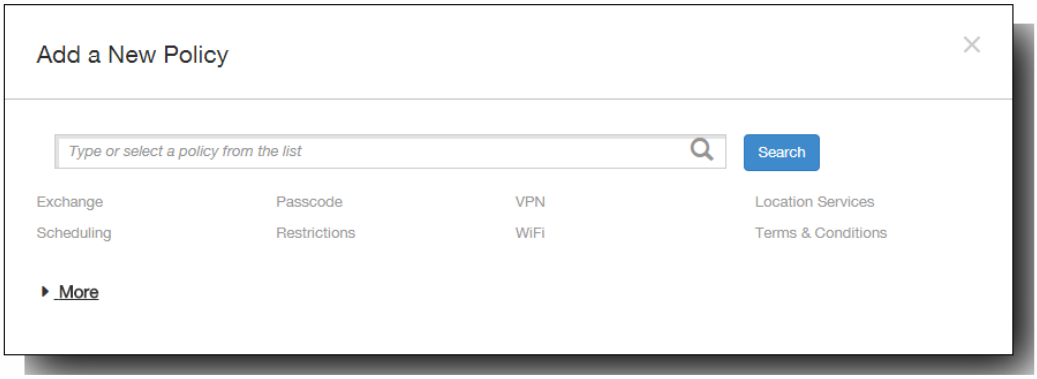
设备策略页面包含一个表格，其中显示了当前的所有策略。

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。

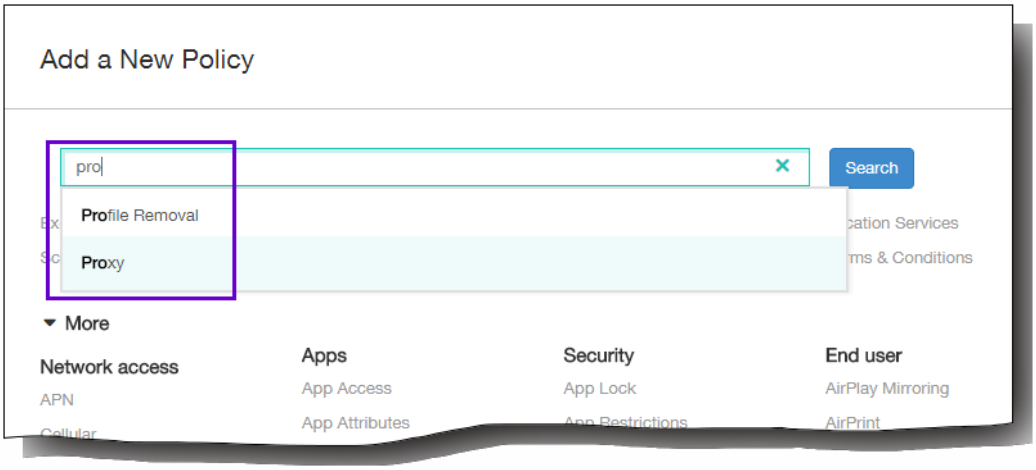


添加设备策略

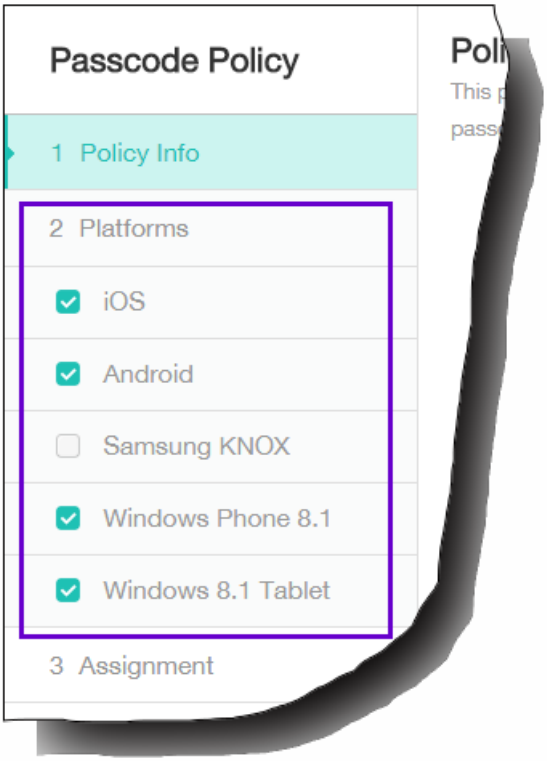
1. 在设备策略页面上，单击添加。
   此时将显示添加新策略对话框。可以展开更多以查看其它策略。



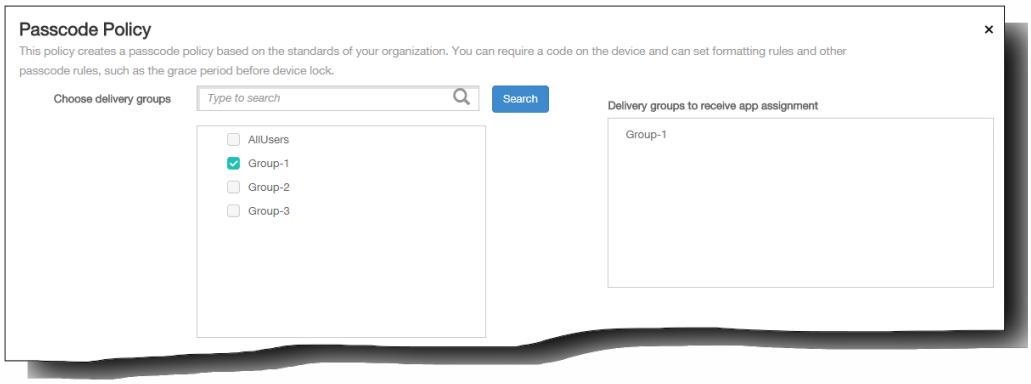
2. 查找要添加的策略，执行以下操作之一：
   - 单击策略。
     此时将显示所选策略的策略信息页面。
   - 在搜索字段中键入策略的名称。随着键入，将显示可能的匹配项。如果列表中存在您的策略，请单击此策略。只有选中的策略保留在对话框中。单击此策略以打开其策略信息页面。
     重要：如果选定的策略位于更多区域，则只有展开更多才会显示此策略。



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）

Oct 22, 2015

可以在 XenMobile 中为 Amazon、iOS、Android、Android for Work、Samsung SAFE、Samsung KNOX、Symbian、Windows Phone 8.1 和 Windows 8.1 Tablet 设备配置设备策略。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	Android for Work	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
通用功能									
Exchange		X	X	X	X	X		X	
计划			X	X			X		
通行码		X	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		
网络访问									
APN		X	X			X			
手机网络		X	X						
个人热点		X							
代理		X							

远程支持						X			
漫游		X							
Samsung 防火墙					X				
通道			X						
	Amazon	**iOS**	**Android**	**Android for Work**	**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							
删除置备配置文件		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			X
应用程序卸载限制	X				X				
文件			X						
浏览器				X	X	X			
置备配置文件		X							
旁加载密钥									X
签署证书									X
Web 剪辑		X	X						X
Worx Store		X	X						X
	Amazon	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 Tablet**
安全性									
Android for Work 应用程序限制				X					
应用程序锁定		X	X						
应用程序限						X			

制									
联系人 (CardDAV)		X							
凭据		X	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									
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							

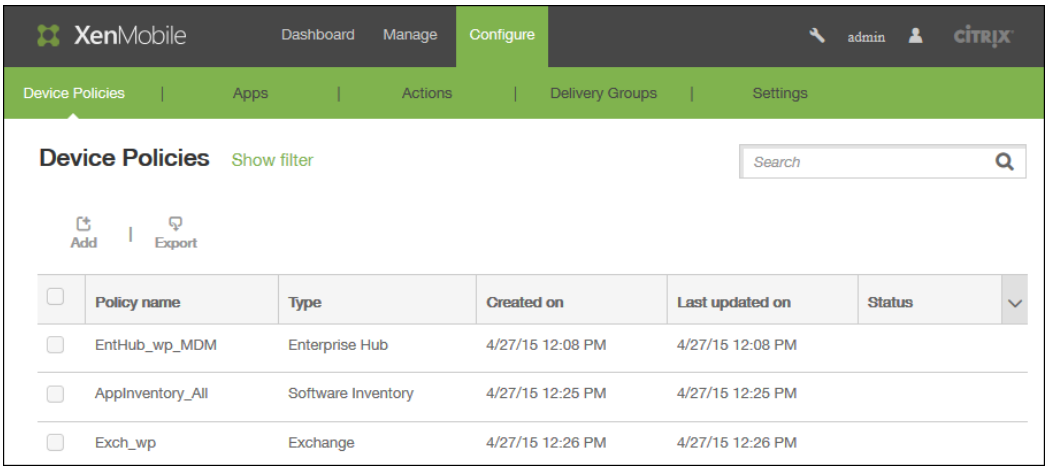
添加应用程序访问设备策略

Oct 22, 2015

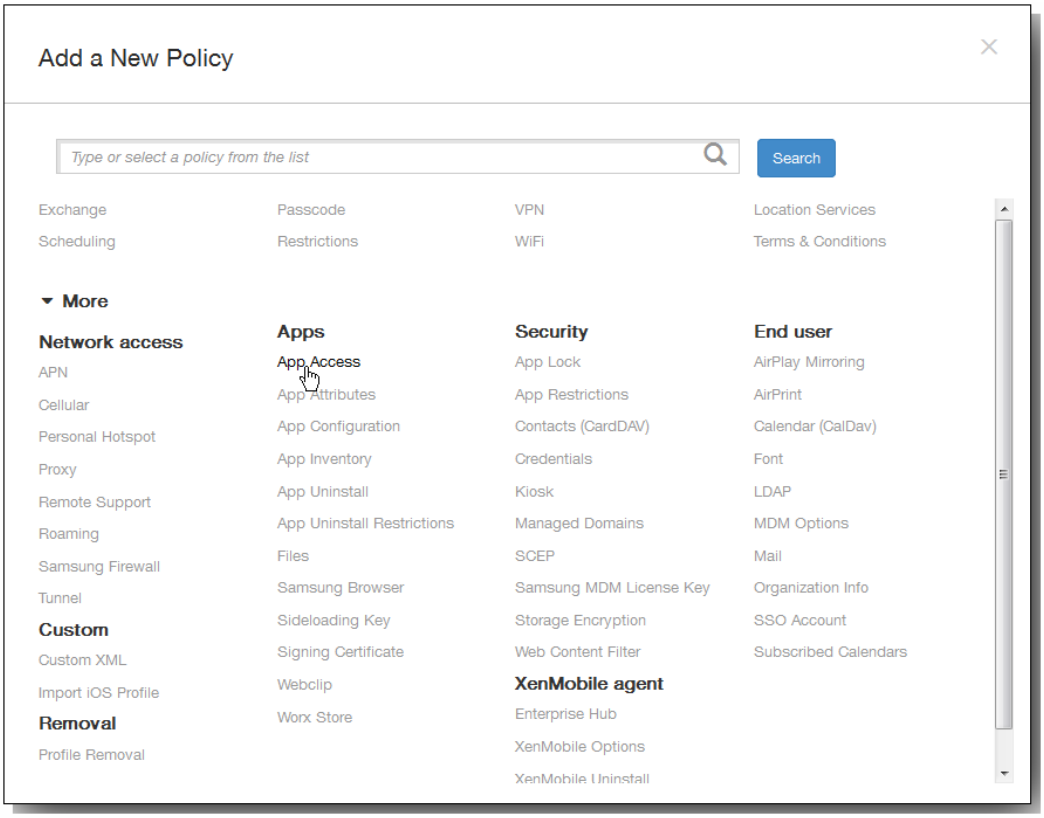
利用 XenMobile 中的应用程序访问设备策略，可以定义需要安装到设备上、可以安装到设备上或不得安装到设备上的应用程序列表。然后，可以创建自动化操作，以使设备符合此应用程序列表。可以创建适用于 iOS、Android 或 Symbian 设备的应用程序访问策略。

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。

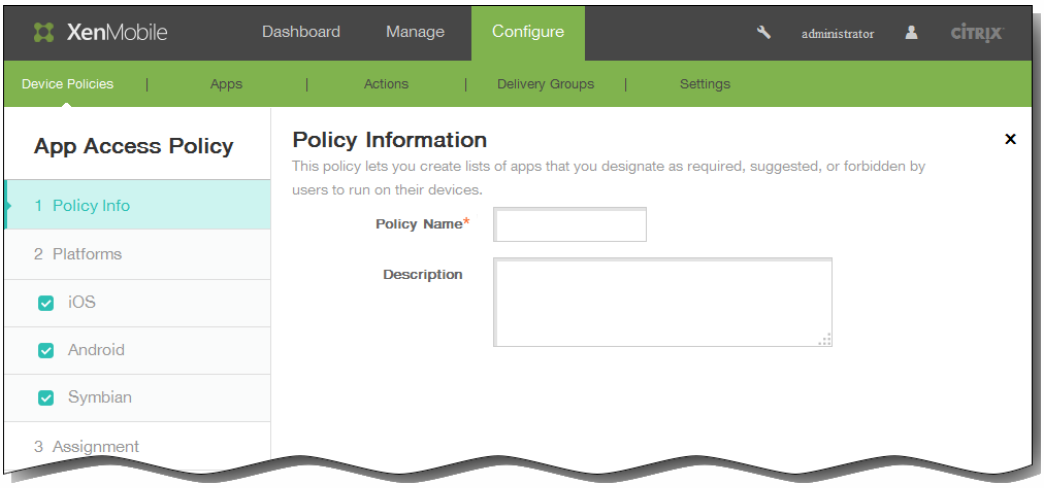
1. 在 XenMobile 控制台中，单击配置 > 设备策略。



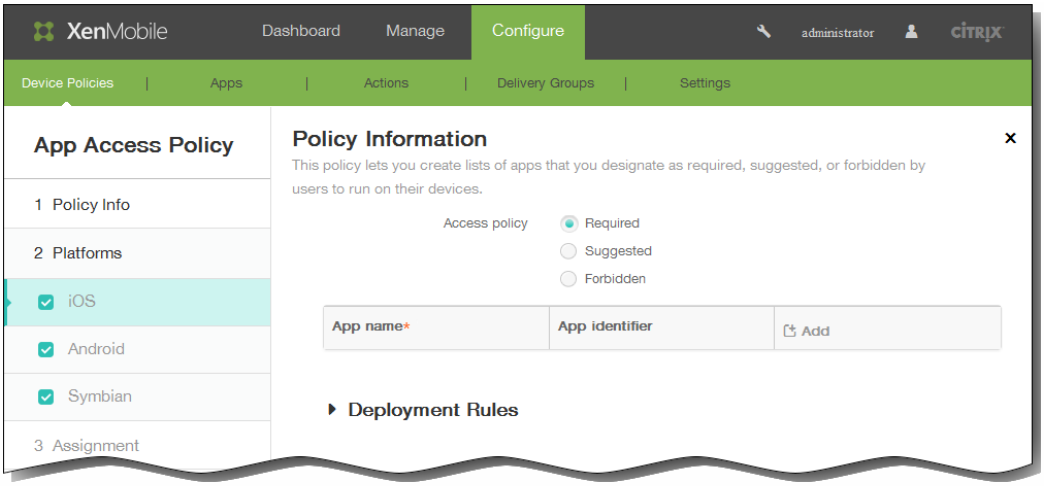
2. 单击添加。 此时将显示添加新策略对话框。



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。



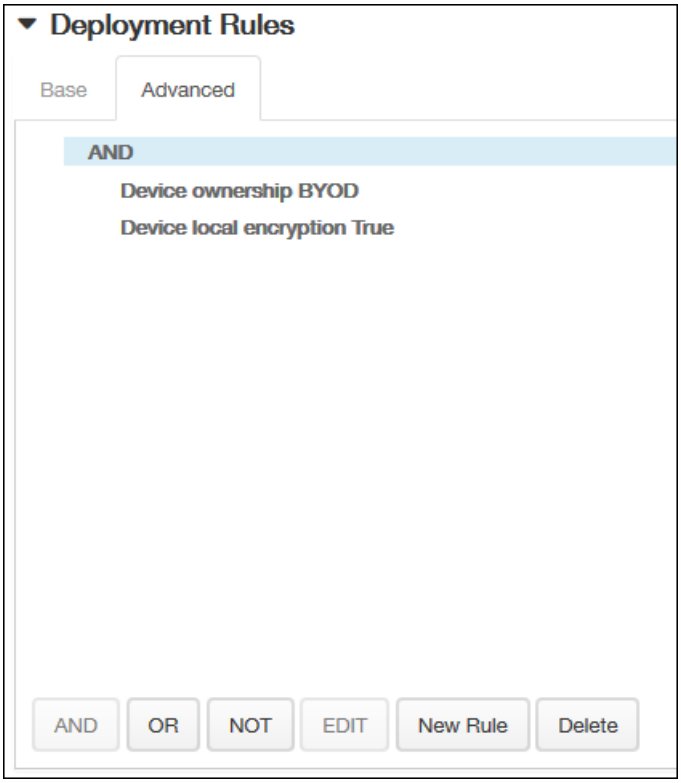
6. 在平台下面，选择要添加的一个或多个平台，然后为每个平台执行以下操作：
   1. 访问策略：单击必需、推荐或禁止。 默认设置为必需。
   2. 要向列表中添加一个或多个应用程序，请单击添加，然后执行以下操作：
      1. 应用程序名称：输入应用程序的名称。
      2. 应用程序标识符：输入可选应用程序标识符。
      3. 单击保存或取消。
      4. 为要添加的每个应用程序重复步骤 i.至步骤 iii.。

      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。

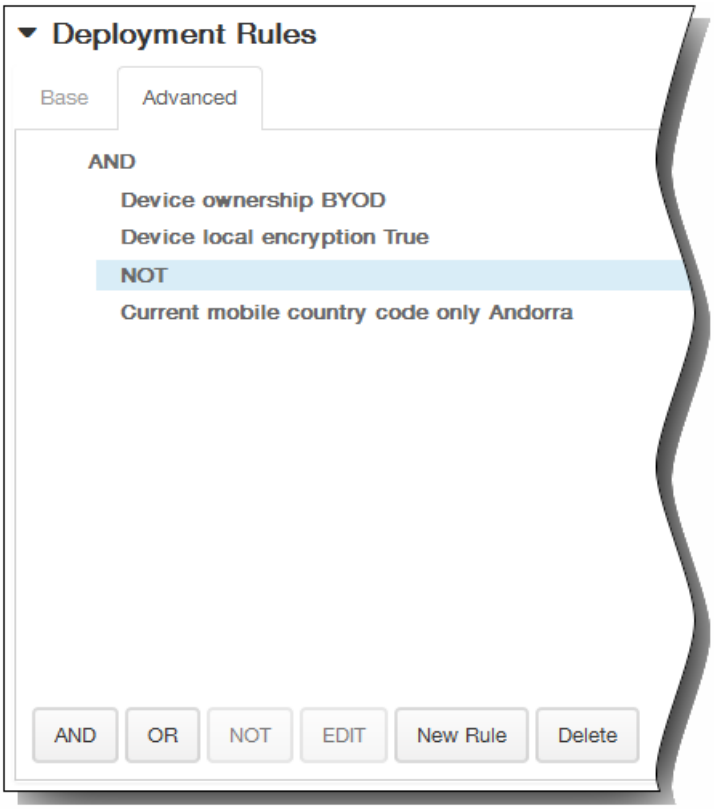
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

   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。

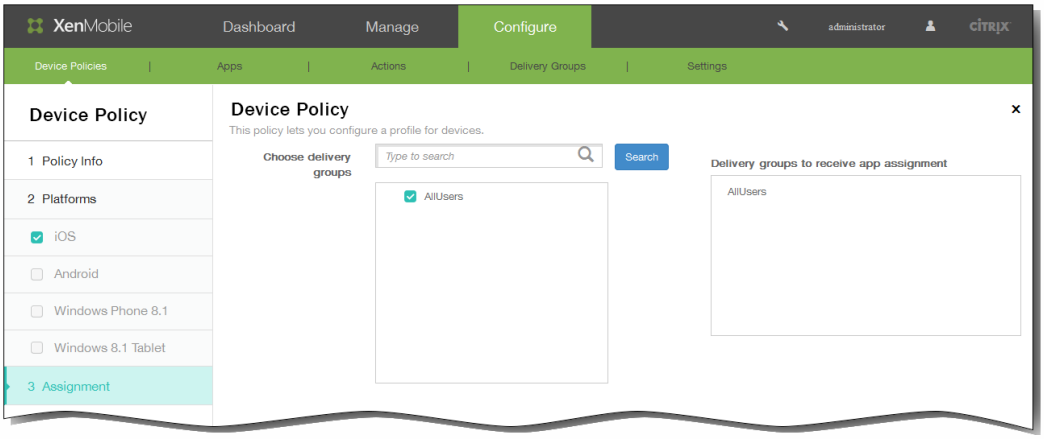


将显示您在基础选项卡上选择的条件。

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。



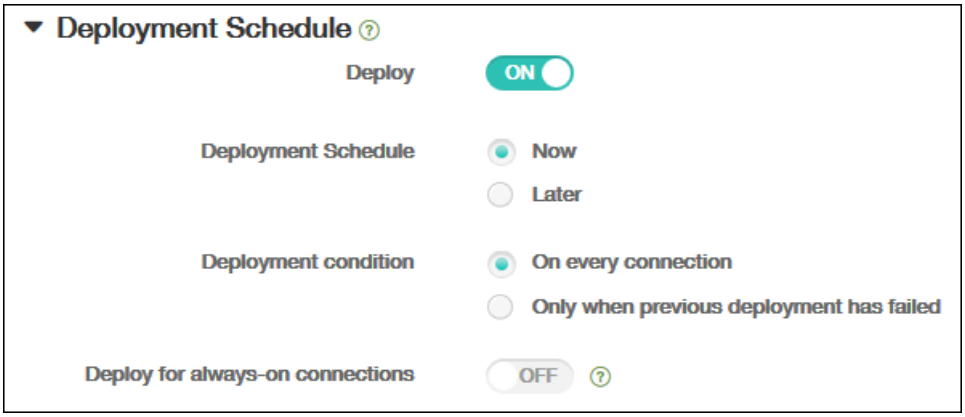
8. 单击下一步。 将显示下一个平台页面或应用程序访问策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



10. 展开部署计划，然后配置以下设置：
    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。

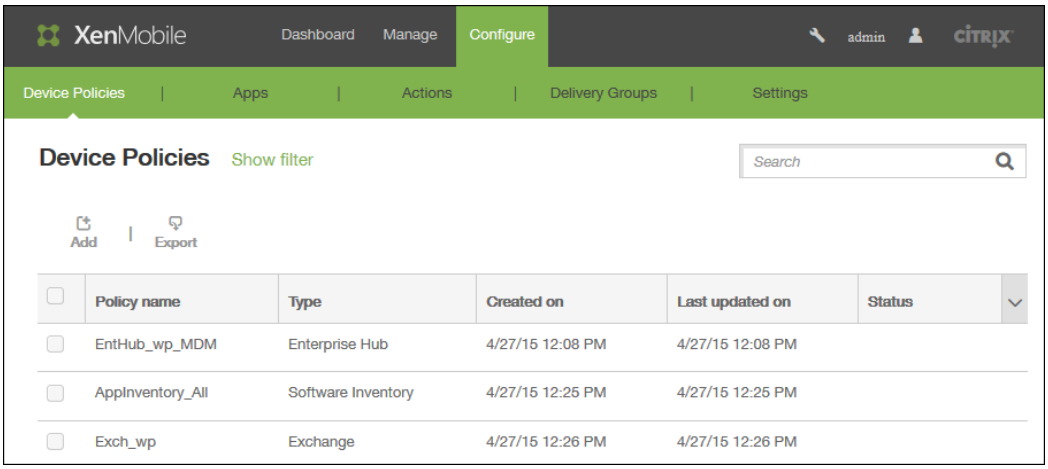
添加应用程序清单设备策略

Oct 22, 2015

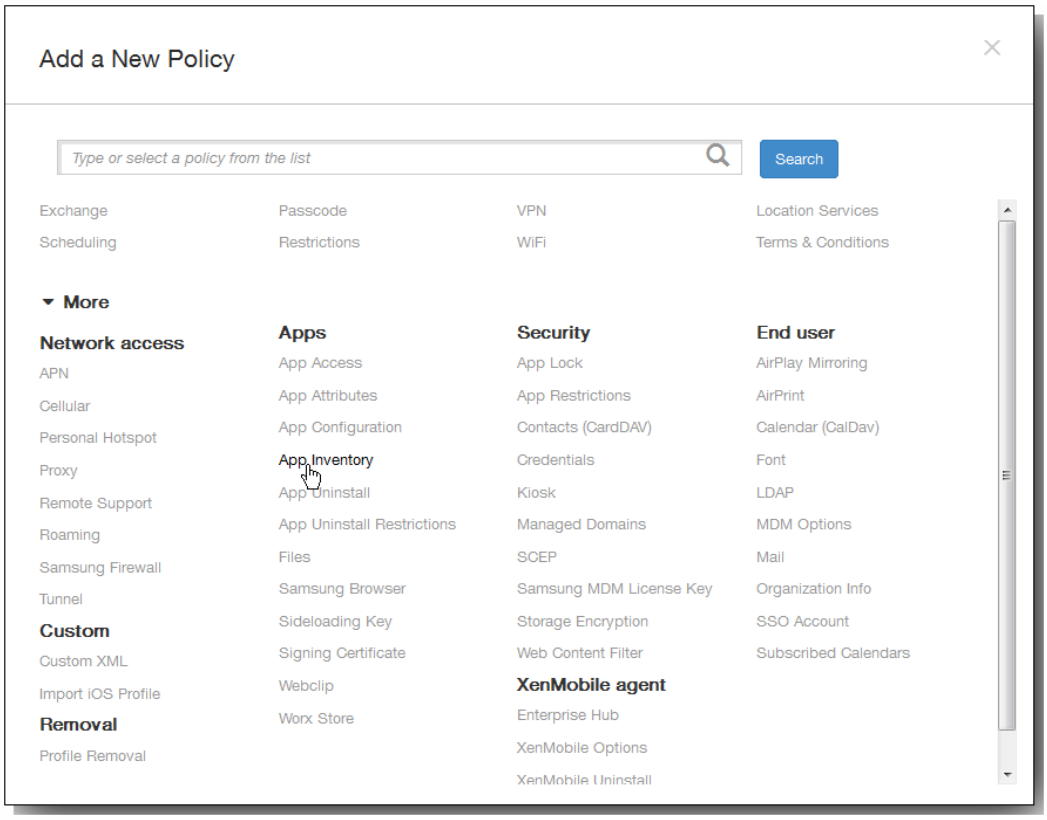
借助 XenMobile 中的应用程序清单策略，您可以收集受管理设备上应用程序的清单，然后根据该清单对比部署到这些设备上的任何应用程序访问策略。这样，您可以发现出现在应用程序黑名单（在应用程序访问策略中禁止）或白名单（在应用程序访问策略中需要）上的应用程序，并采取相应的操作。

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。

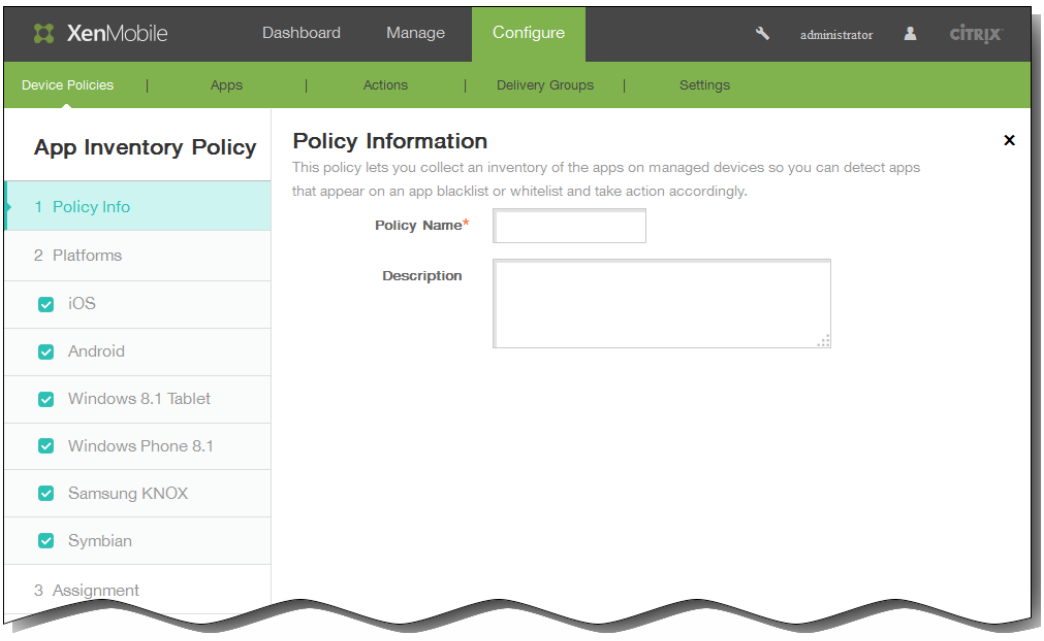
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



2. 单击添加。 将显示添加新策略页面。

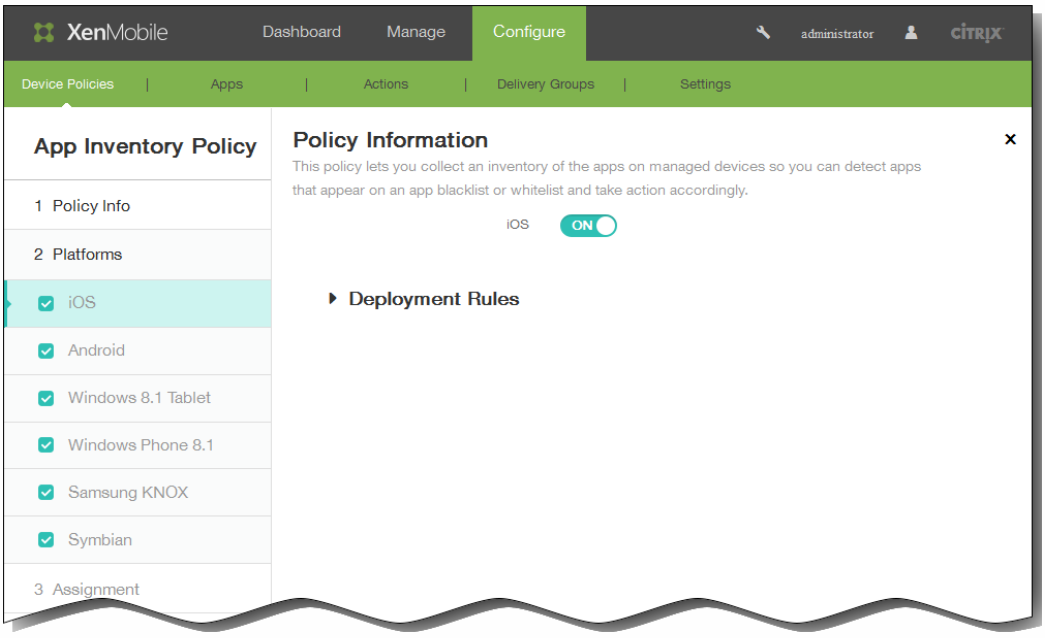


3. 单击更多 > 应用程序清单。 将显示应用程序清单策略页面。



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。

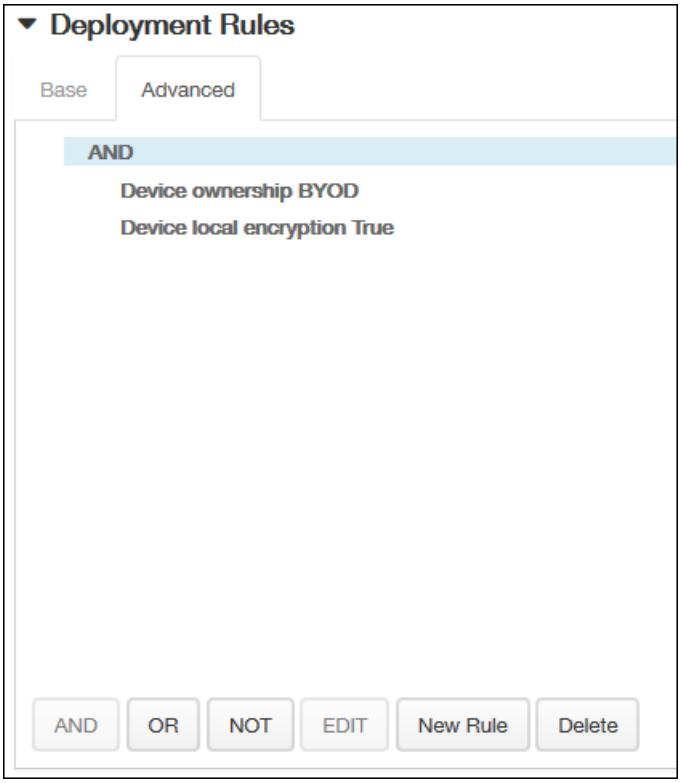
注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 iOS 平台配置面板。



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：

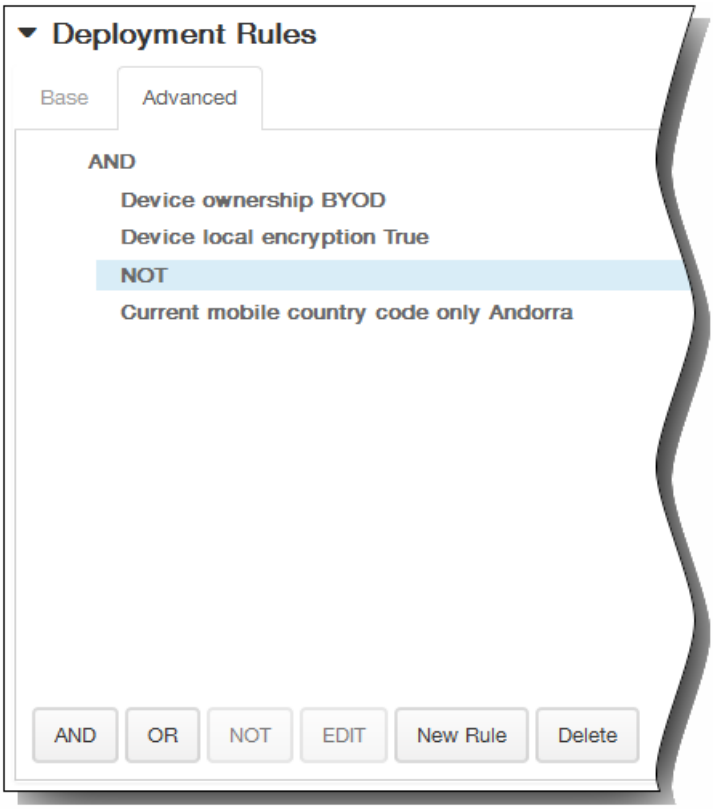
6. 保留默认设置或将此设置更改为关。 默认值为开。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

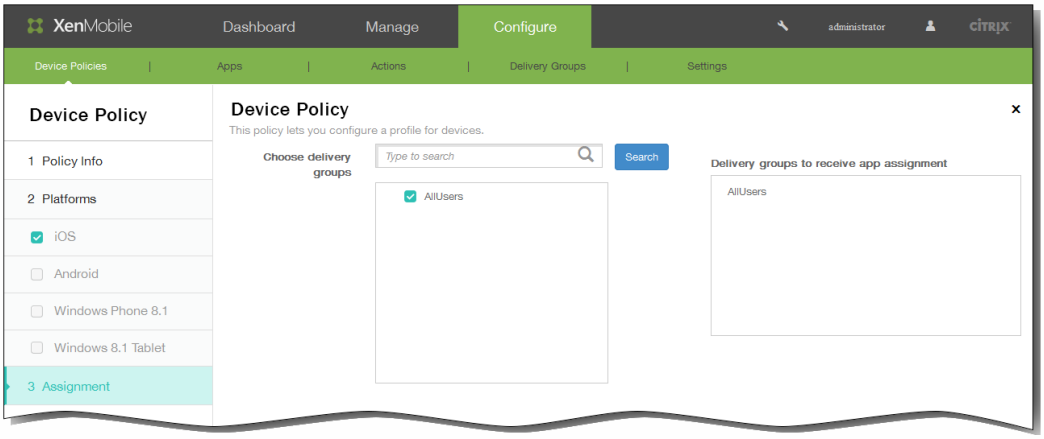


将显示您在基础选项卡上选择的条件。

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。



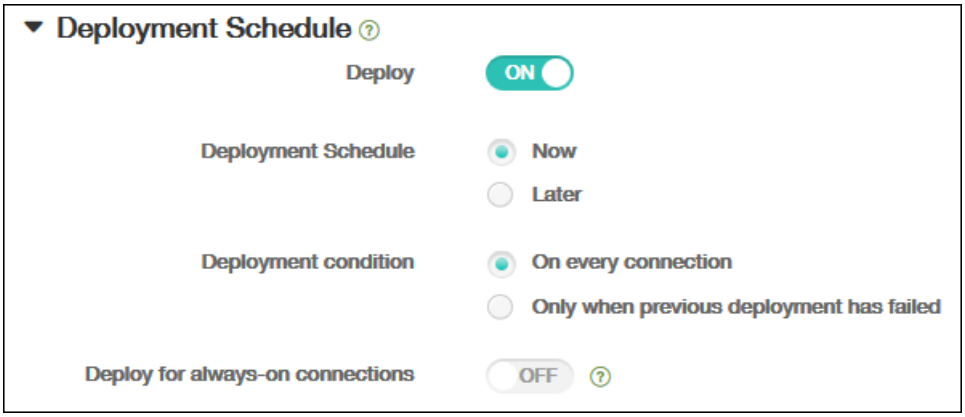
8. 单击下一步。 此时将显示下一个平台页面或分配策略页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

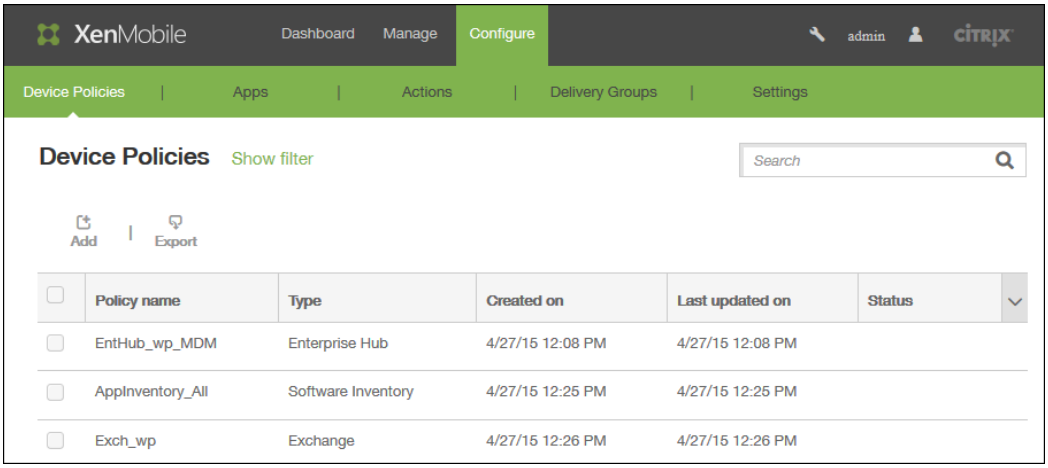
添加适用于 Android 的应用程序通道设备策略

Oct 22, 2015

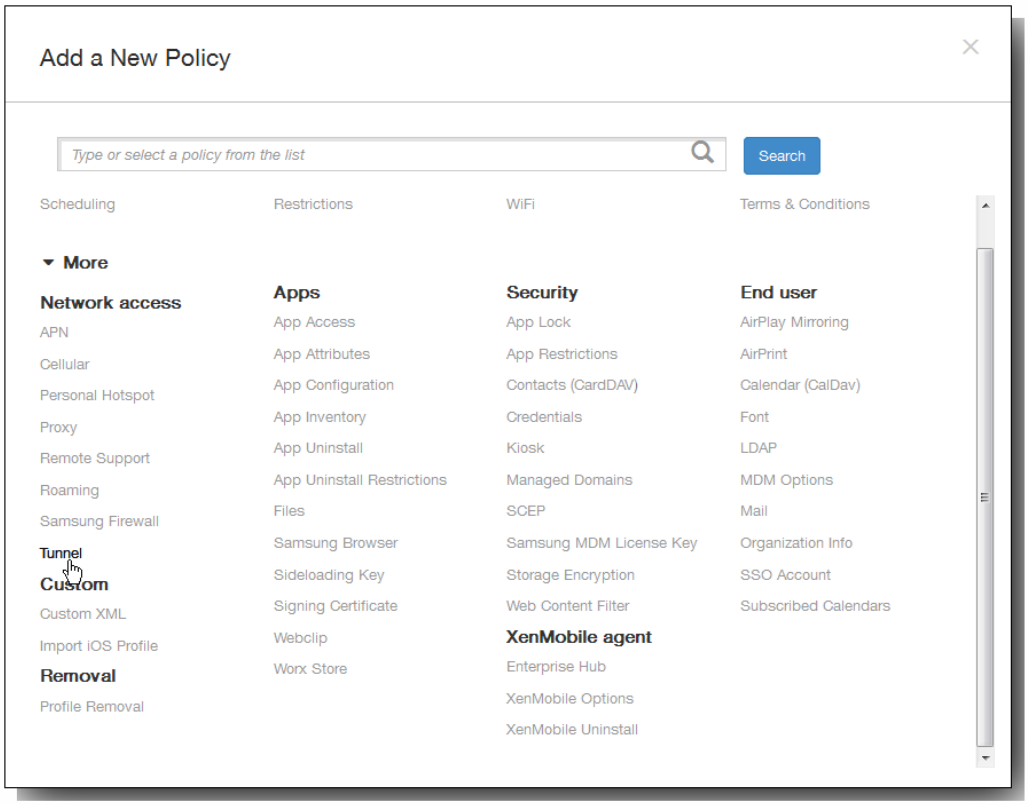
应用程序通道旨在提高移动应用程序的服务连续性及数据传输可靠性。应用程序通道定义移动设备应用程序的客户端组件与应用程序服务器组件之间的代理参数。还可以使用应用程序通道创建设备的远程支持通道以使用管理支持。

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。

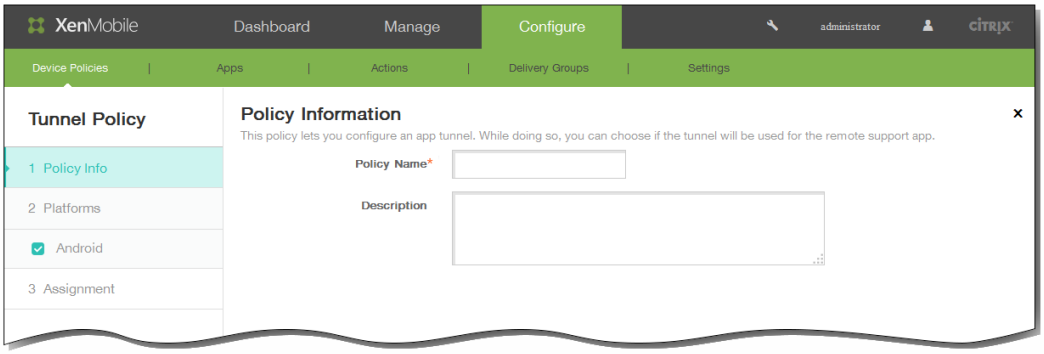
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



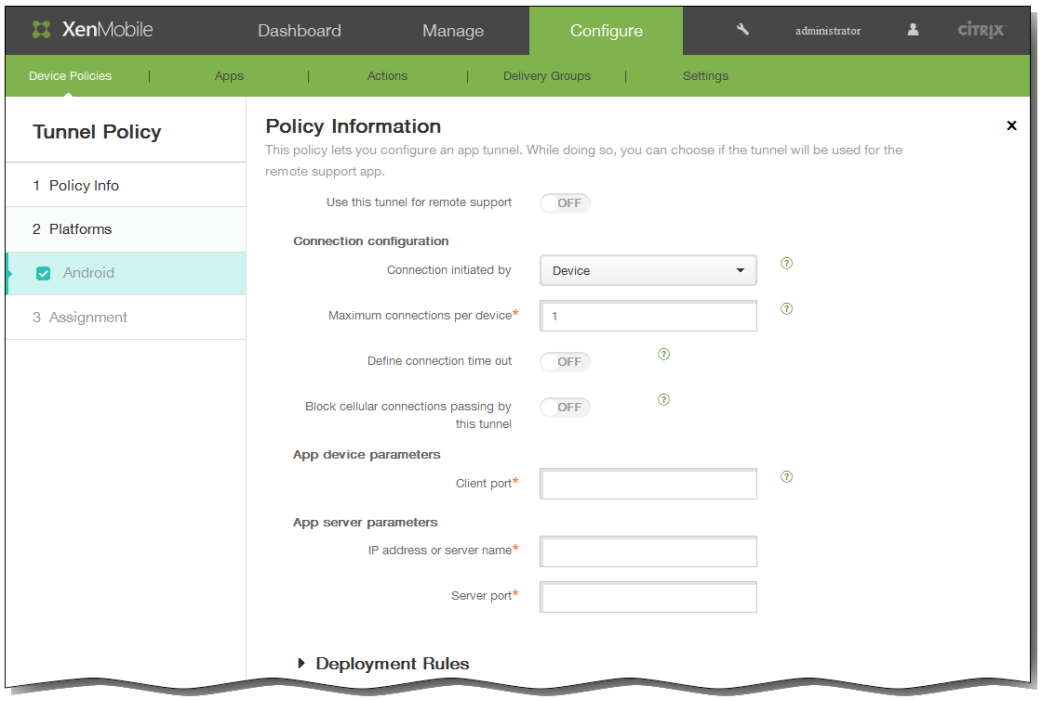
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。



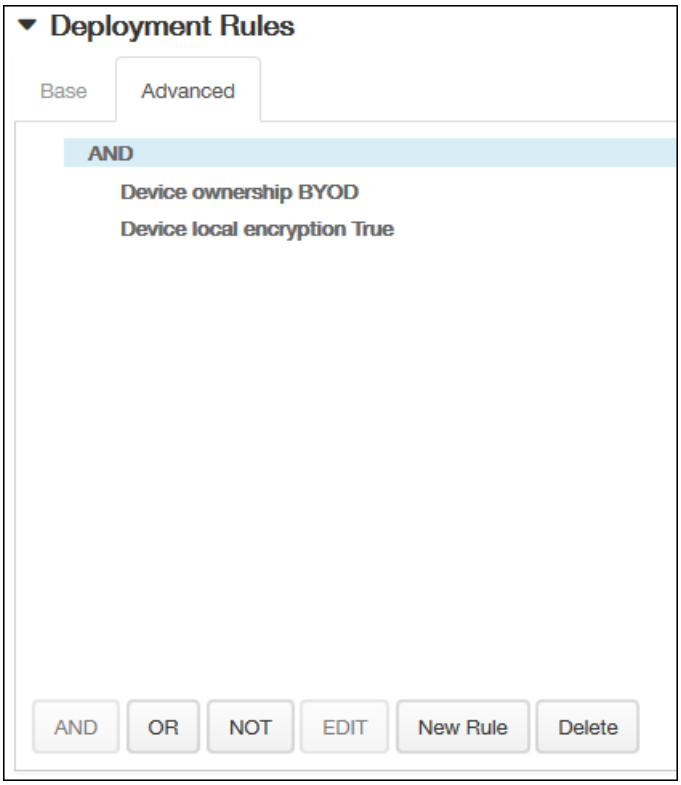
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 Android 策略平台页面。



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。

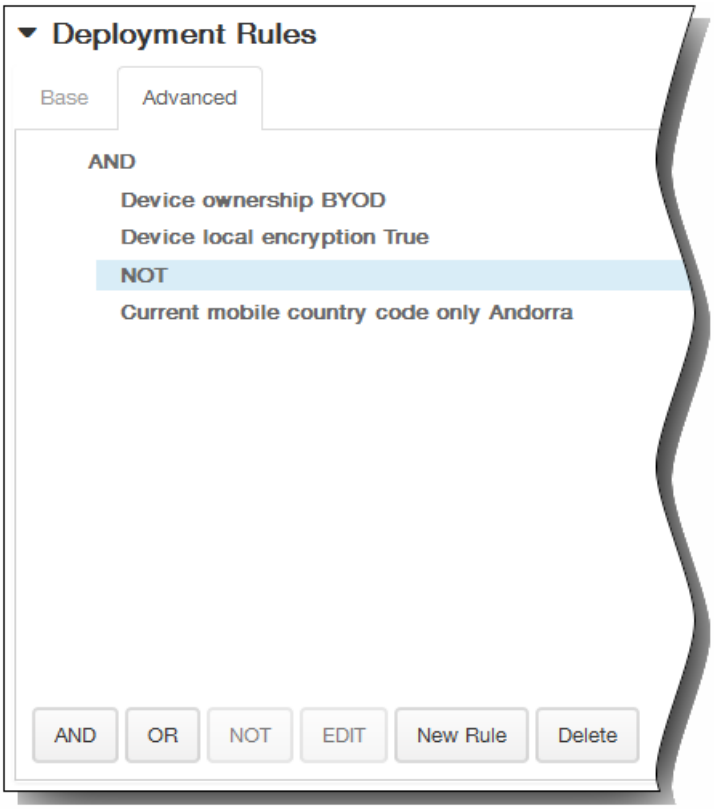
   如果**选择**远程支持，请执行以下操作：
   1. 使用此通道进行远程支持：设置为开。
   2. 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
   3. 连接超时：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度，以秒为单位。
   4. 使用 SSL 连接：选择是否为此通道使用安全 SSL 连接。
   5. 阻止手机网络连接通过此通道：选择是否在漫游时阻止此通道。
      注意：不会阻止 WiFi 和 USB 连接。
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

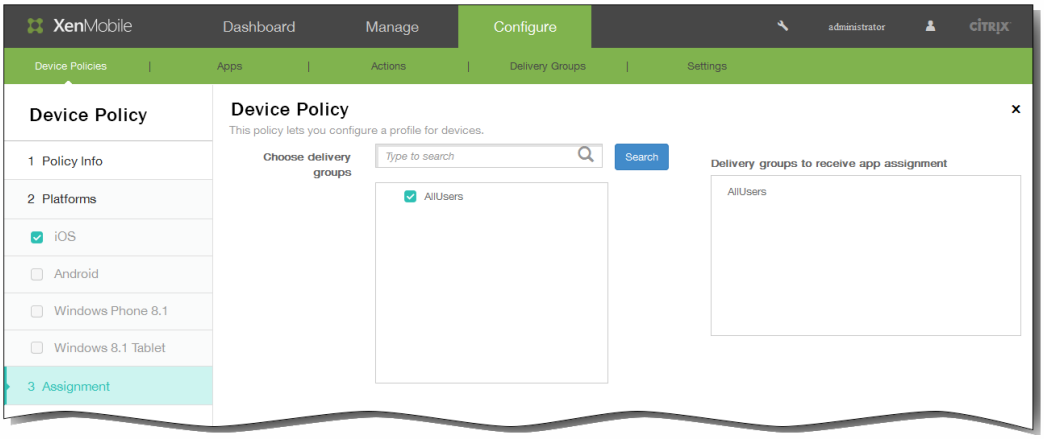


将显示您在基础选项卡上选择的条件。

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。

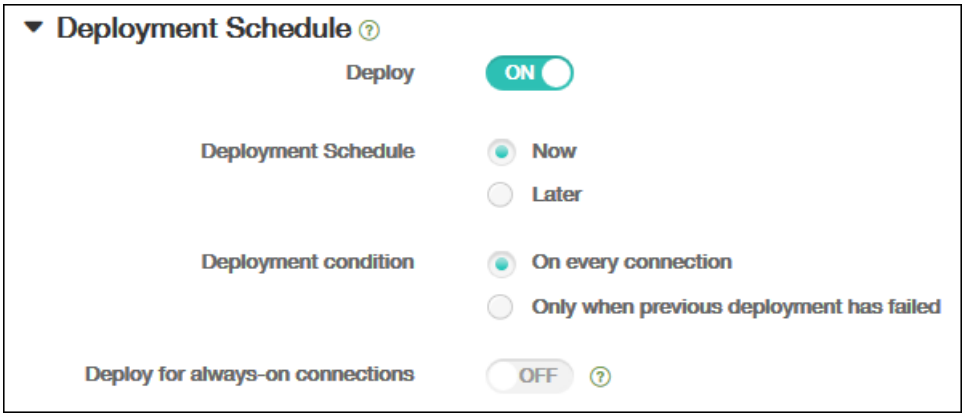


8. 单击下一步。 此时将显示通道策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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

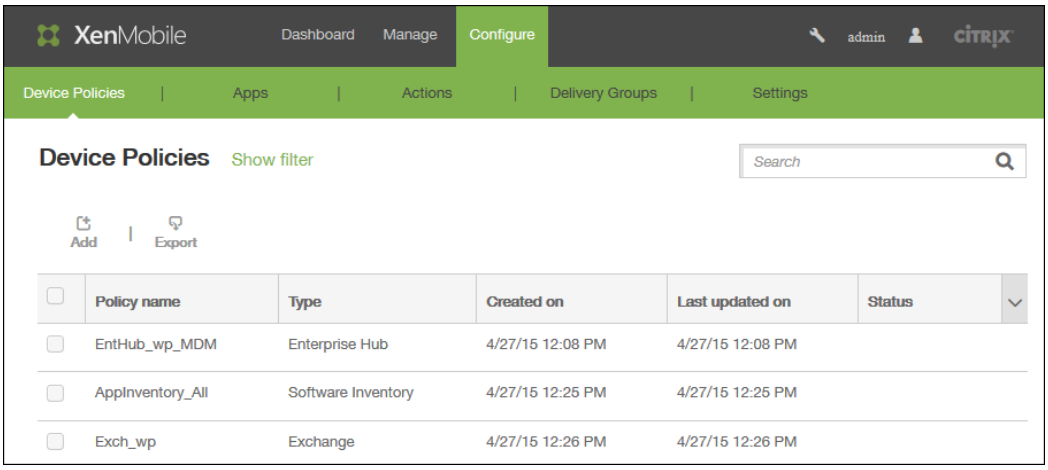
Oct 22, 2015

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：

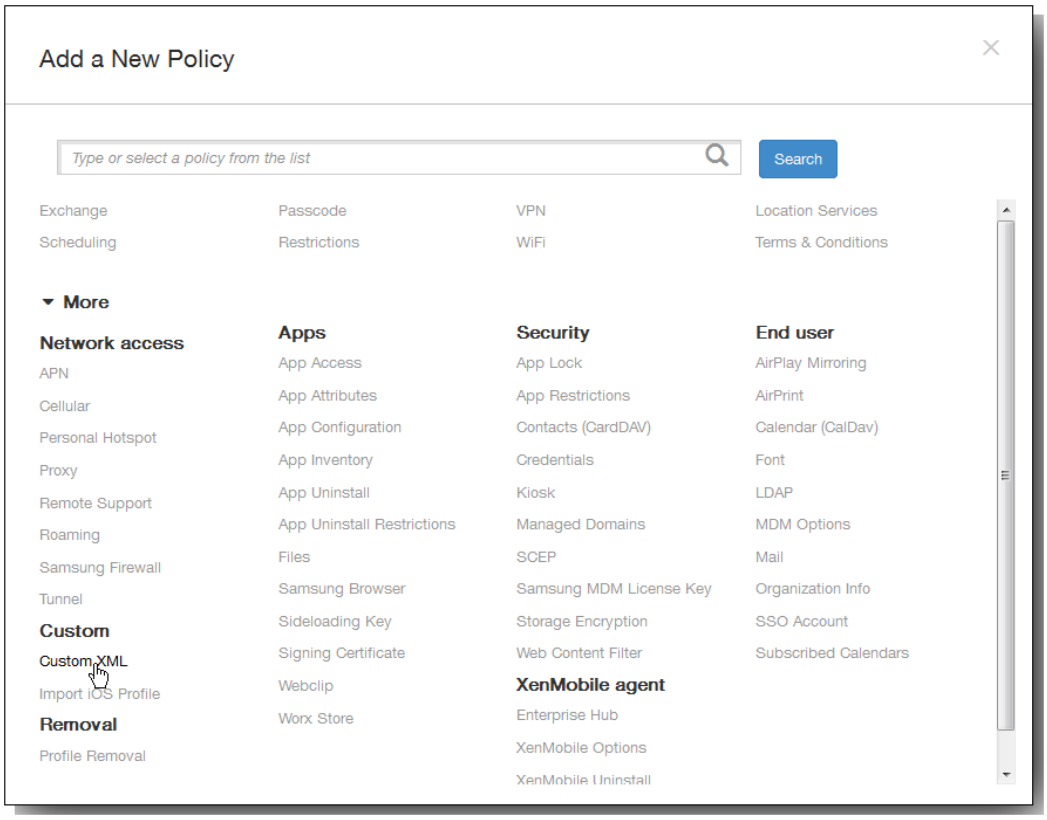
- 置备，包括配置设备以及启用或禁用功能
- 设备配置，包括允许用户更改设置和设备参数
- 软件升级，包括提供要加载到设备中的新软件或缺陷修复（包括应用程序和系统软件）
- 故障管理，包括接收来自设备的错误和状态报告

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。

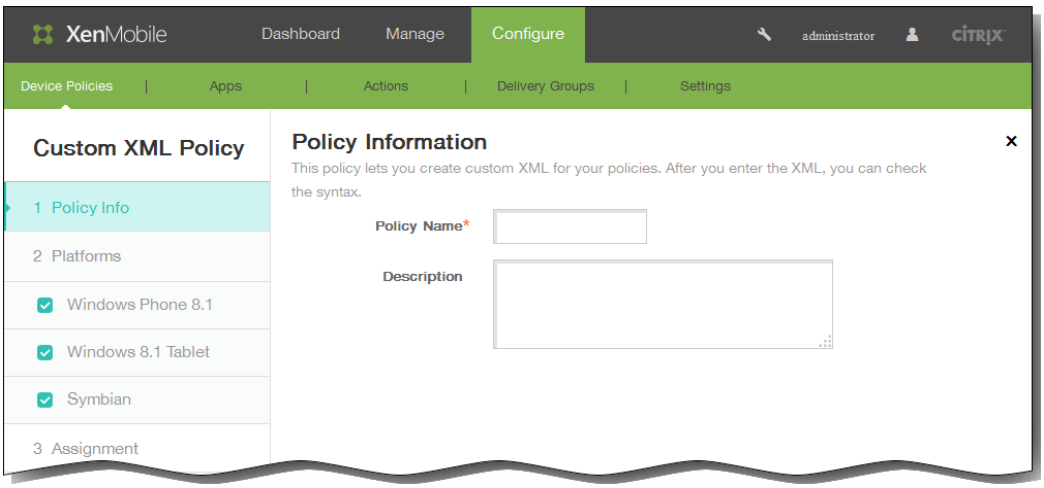
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



2. 单击添加添加新策略。 此时将显示添加新策略对话框。

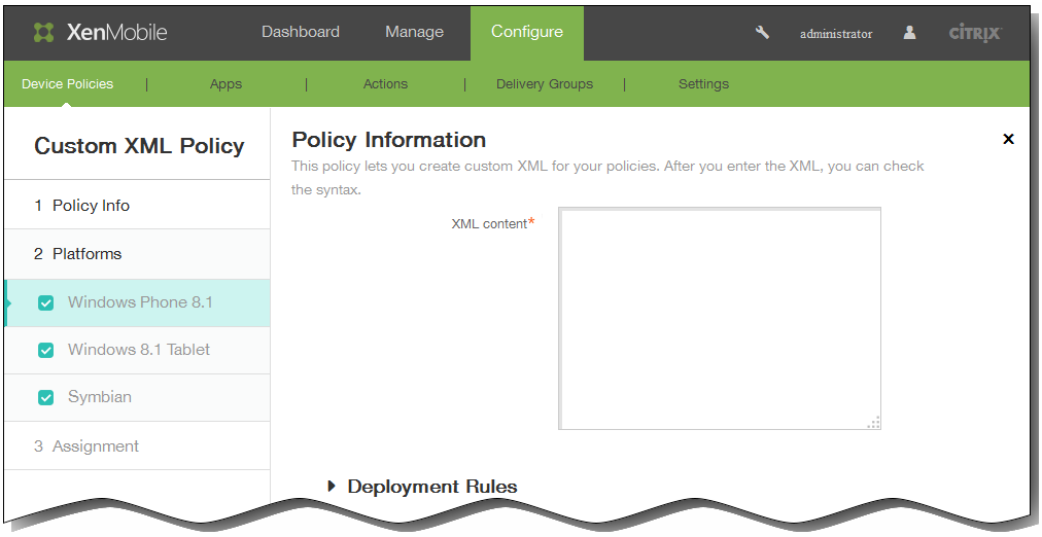


3. 单击更多，然后在自定义下单击自定义 XML。 此时将显示自定义 XML 策略信息页面。



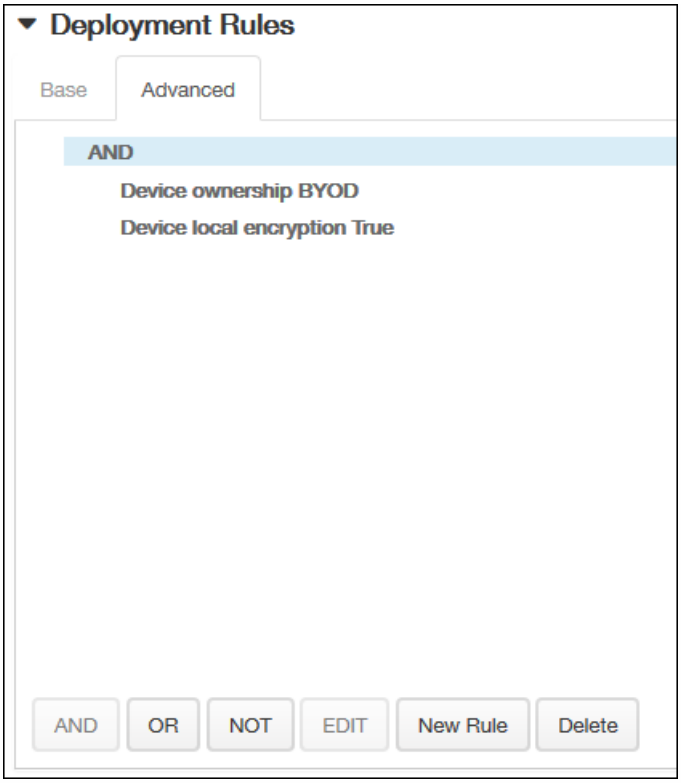
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
5. 单击下一步。 此时将显示策略平台页面。

   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。



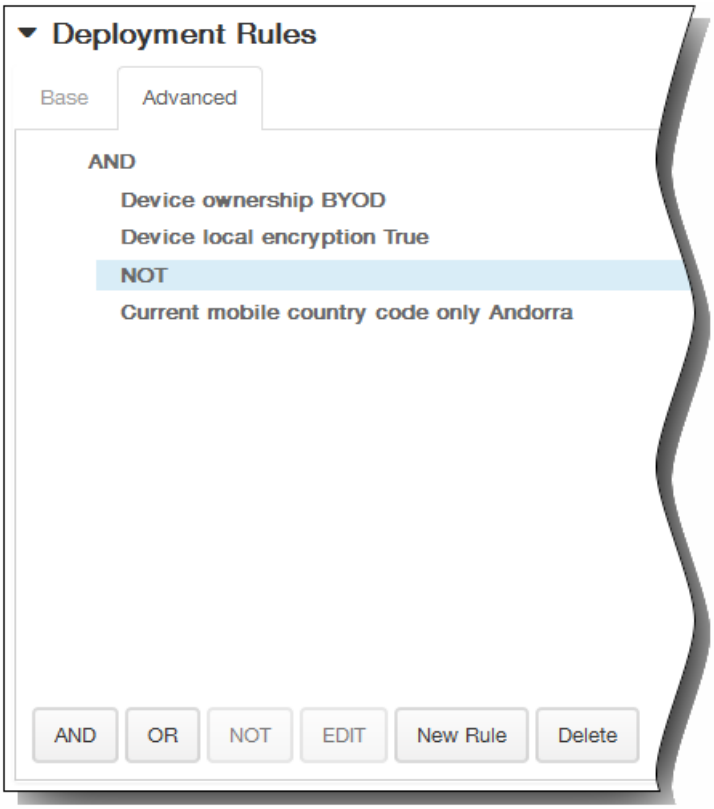
6. 在平台下面，确保只选中要添加的平台。
7. 在 XML 内容中，输入要向策略中添加的自定义 XML 代码。 如果内容太长，可以从源文件中剪切并复制该代码。
8. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。



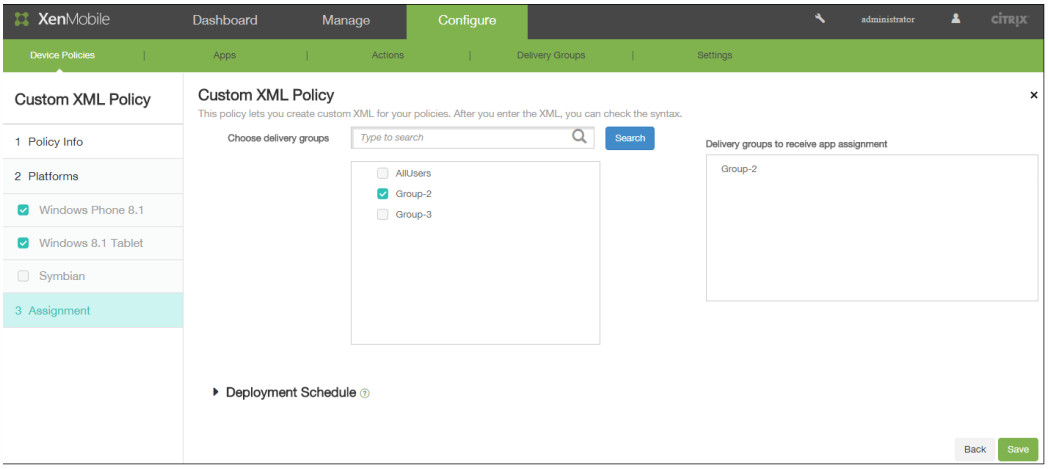
将显示您在基础选项卡上选择的条件。

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。



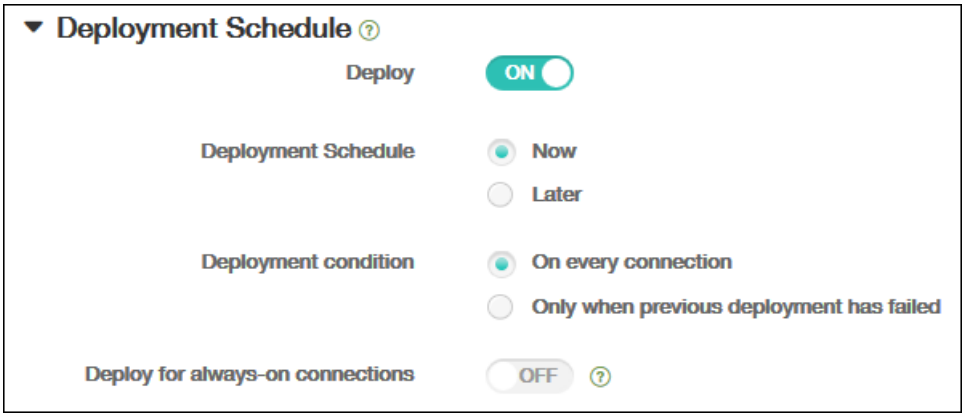
9. 单击下一步。 XenMobile 检查 XML 内容语法。内容框下将显示所有语法错误。必须先修复所有错误才能继续。
   如果没有语法错误，则将显示自定义 XML 策略分配页面。

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。



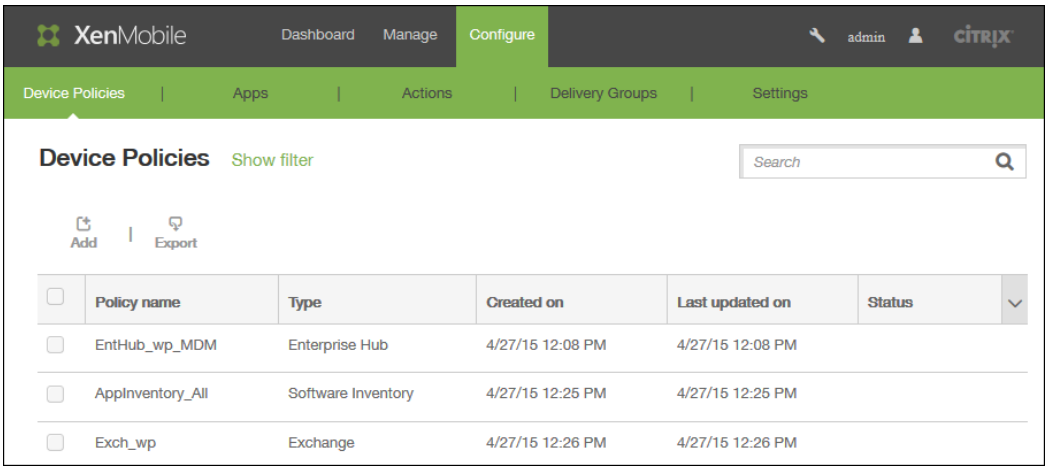
12. 单击保存以保存此策略。

应用程序卸载设备策略

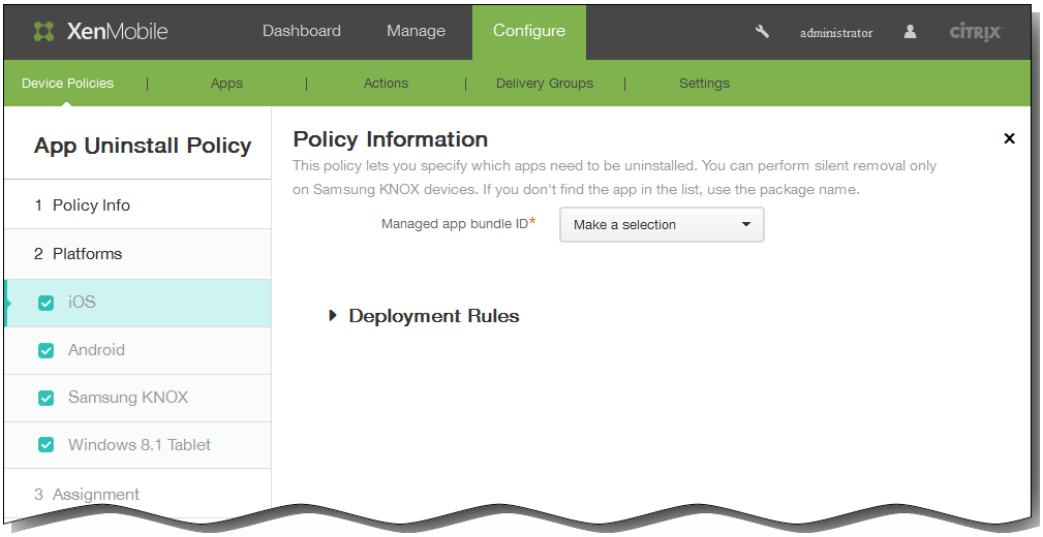
Oct 22, 2015

您可以为 iOS、Android、Samsung KNOX、Android for Work 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。

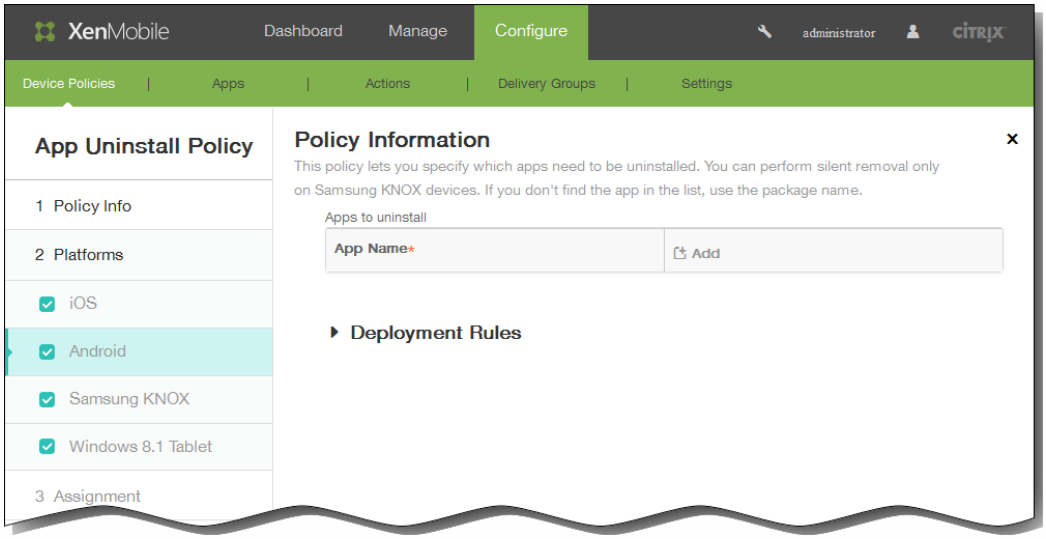
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。 在设备策略页面上，单击添加。



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 Platforms（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. 如果在托管应用程序产品组合 ID 列表上选择了 iOS，则单击现有应用程序或单击 Add new（新添）。
      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. 如果选择 Android、Samsung KNOX、Android for Work 或 Windows 8.1 Tablet：



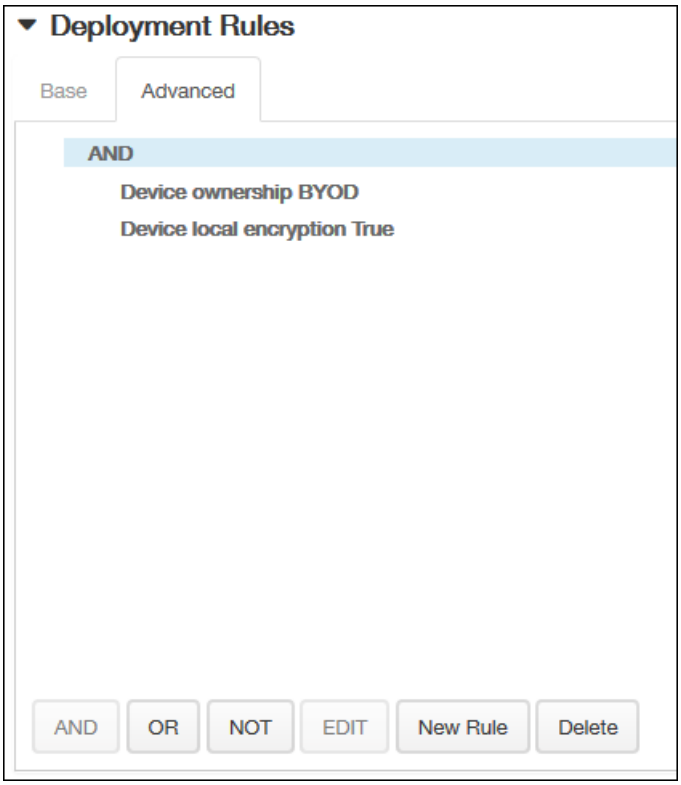
在要卸载的应用程序下面，单击 添加，然后执行以下操作：

1. 应用程序名称：在列表中，单击现有的应用程序，或单击 Add new（新添）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. 为要添加到卸载策略中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。

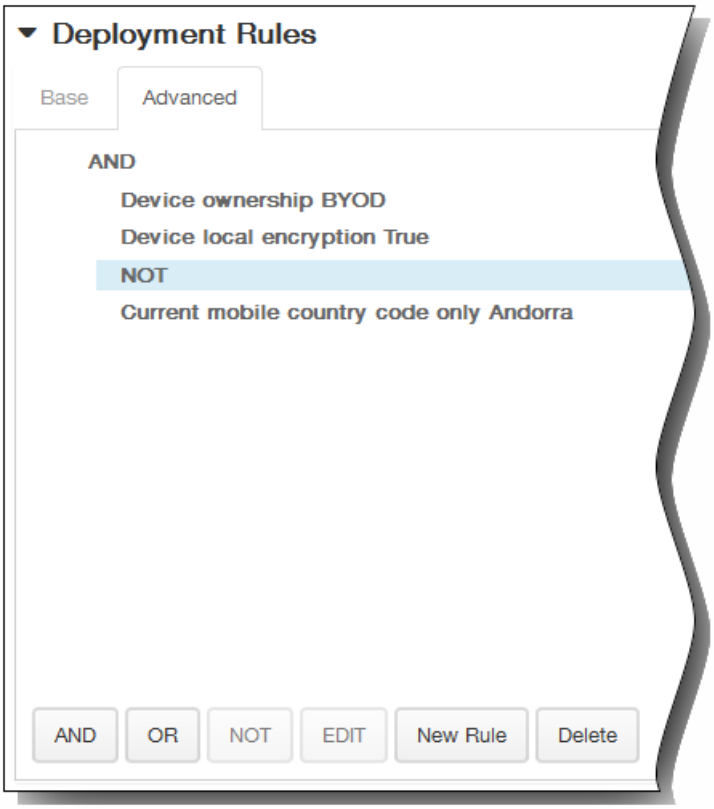


将显示您在基础选项卡上选择的条件。

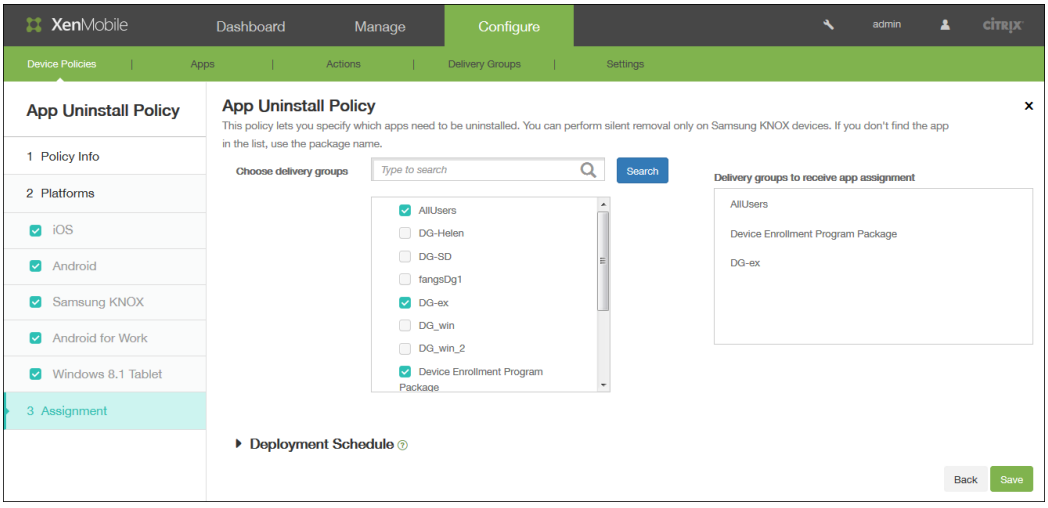
3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。

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。



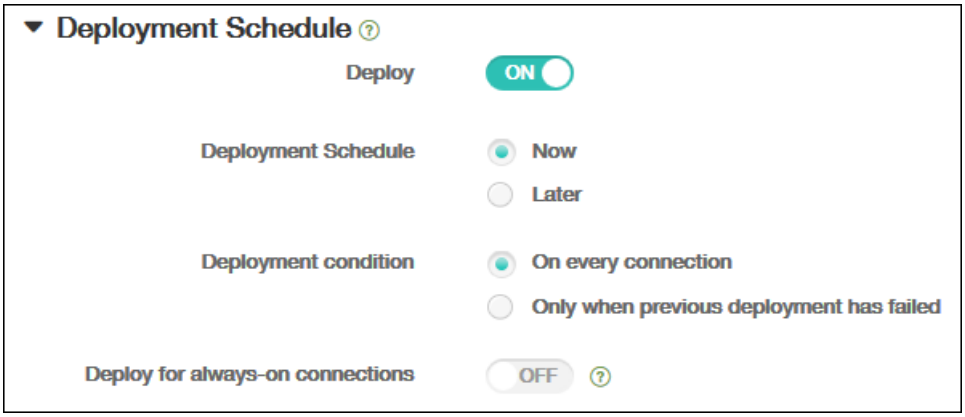
7. 单击下一步。此时将显示应用程序卸载策略分配页面。
8. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

添加适用于 Android 的文件设备策略

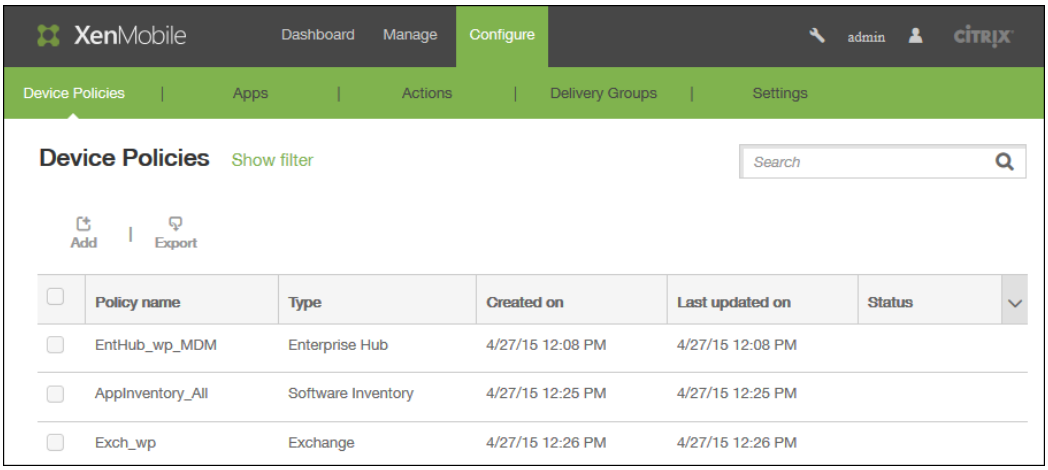
Aug 04, 2016

您可以在 XenMobile 中为用户添加执行某些功能的脚本文件，或者也可添加 Android 设备用户能够在其设备上访问的文档文件。 添加文件时，还可以指定设备上要存储该文件的目录。 例如，如果您希望 Android 用户接收公司文档或 .pdf 文件，则可以将该文件部署到设备，然后将文件位置告知用户。

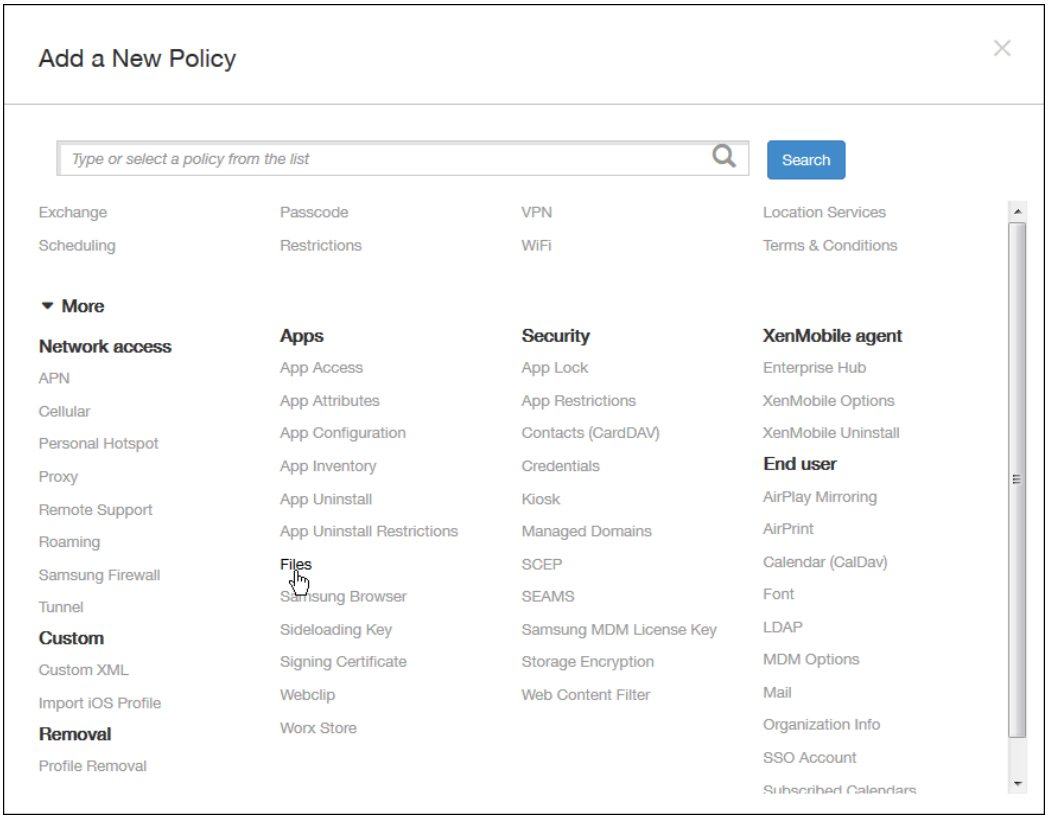
利用此策略可以添加以下文件类型：

- 文本文件（.xml、.html、.py 等）
- 其他文件，如文档、图片、电子表格或演示文稿
- 仅适用于 Windows Mobile 和 Windows CE：通过 MortScript 创建的脚本文件

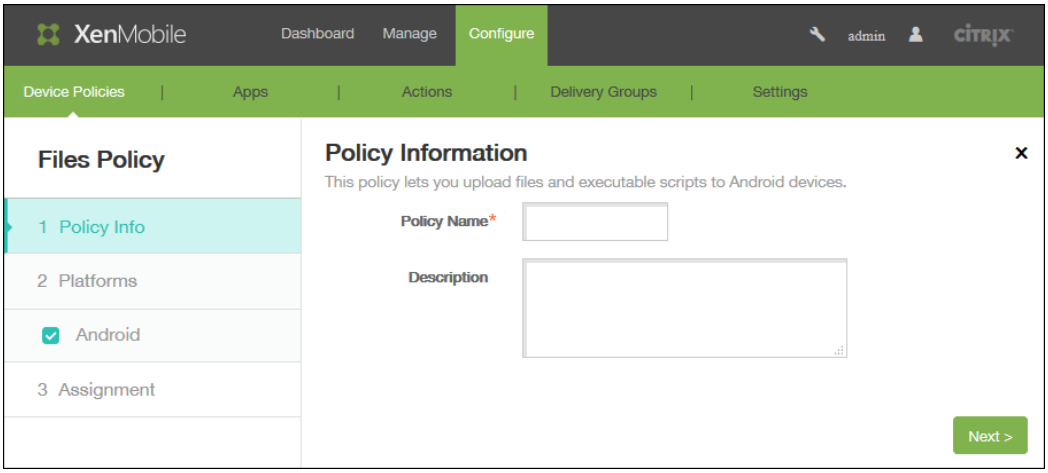
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



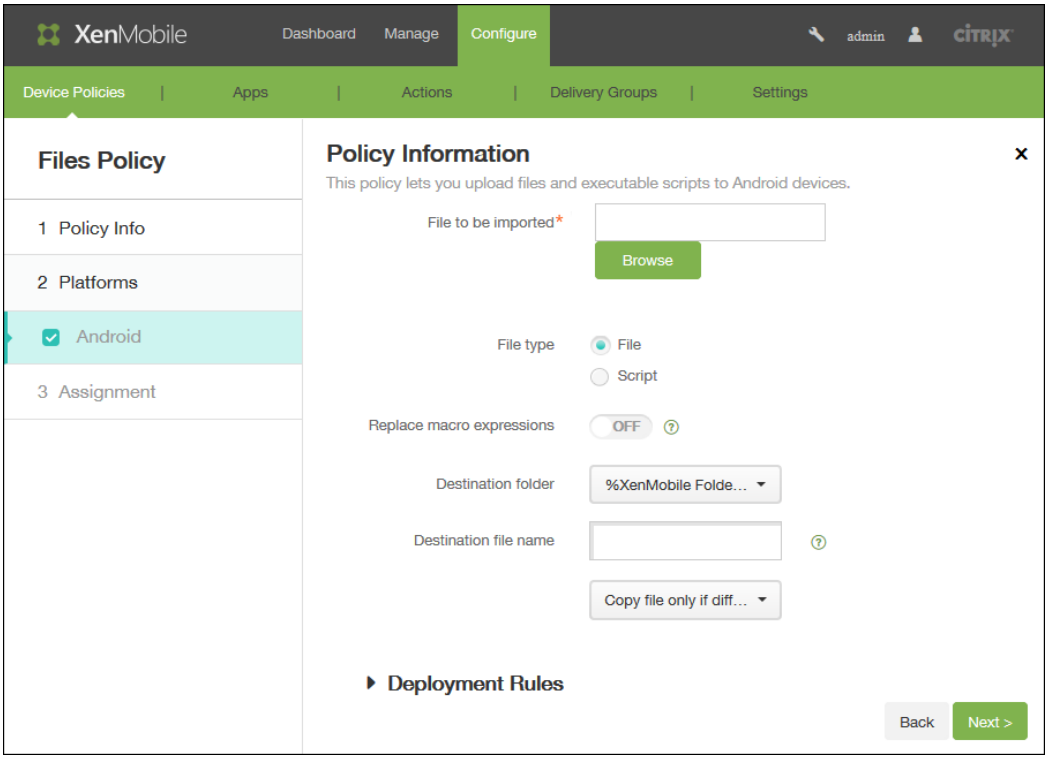
2. 单击添加。 此时将显示添加新策略对话框。



3. 单击更多，然后在应用程序下面，单击文件。 此时将显示文件策略信息页面。

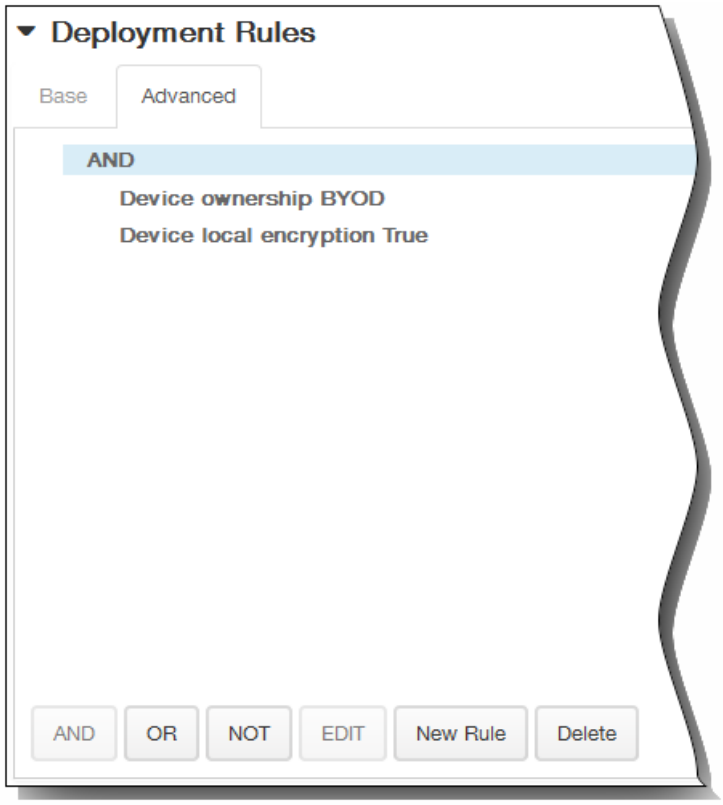


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 Android 平台信息页面。



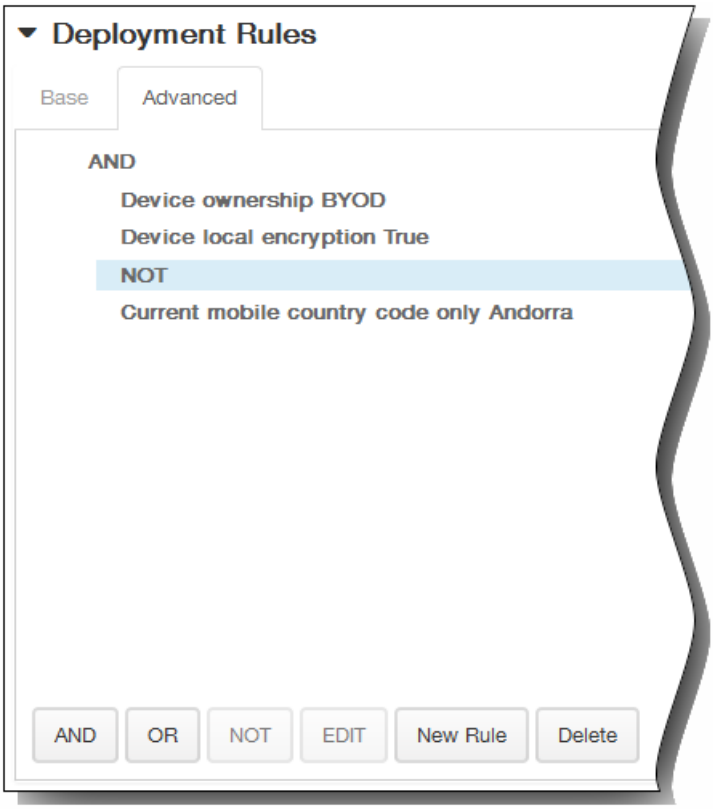
6. 在 Android 平台信息页面上，输入以下信息：
   1. 要导入的文件：单击浏览，然后导航到文件的位置，选择要导入的文件。
   2. 文件类型：选择文件或脚本。 如果选择脚本，将显示立即执行。选择是否在上载文件后立即执行脚本。默认值为关。
   3. 替换宏表达式：选择是否将脚本中的宏令牌名称替换为设备或用户属性。
   4. 目标文件夹：在列表中，选择用于存储上载文件的位置。
   5. 目标文件夹名：（可选）如果必须在部署到设备上之前更改文件名，请键入一个不同名称。
   6. 仅在不同时复制文件：在列表中，选择是仅在与现有文件存在差异时复制文件还是覆盖现有文件。
7. 展开部署规则，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。

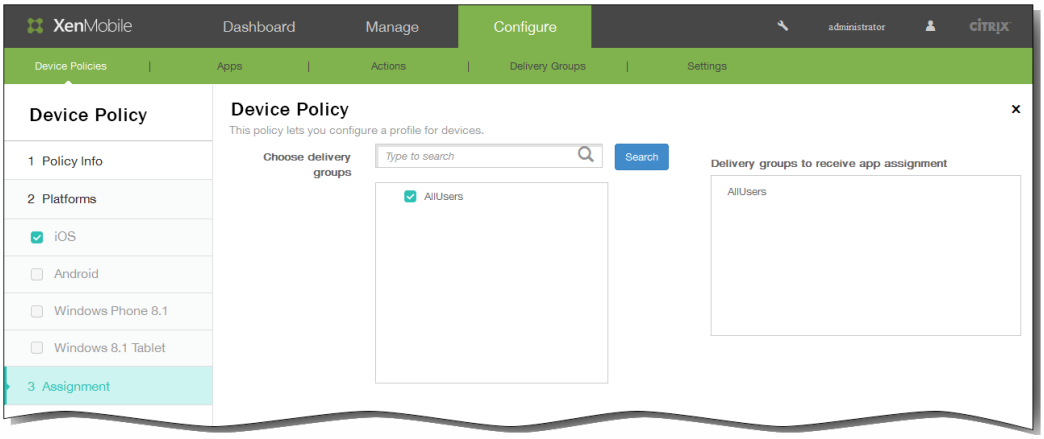


将显示您在基础选项卡上选择的条件。

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。

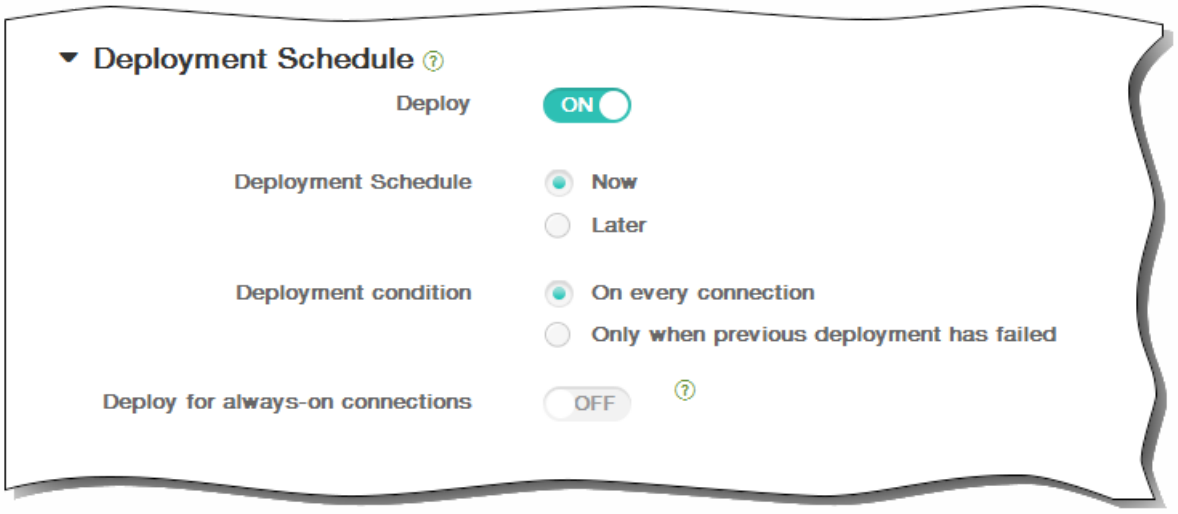


8. 单击下一步。 将显示文件策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

APN 设备策略

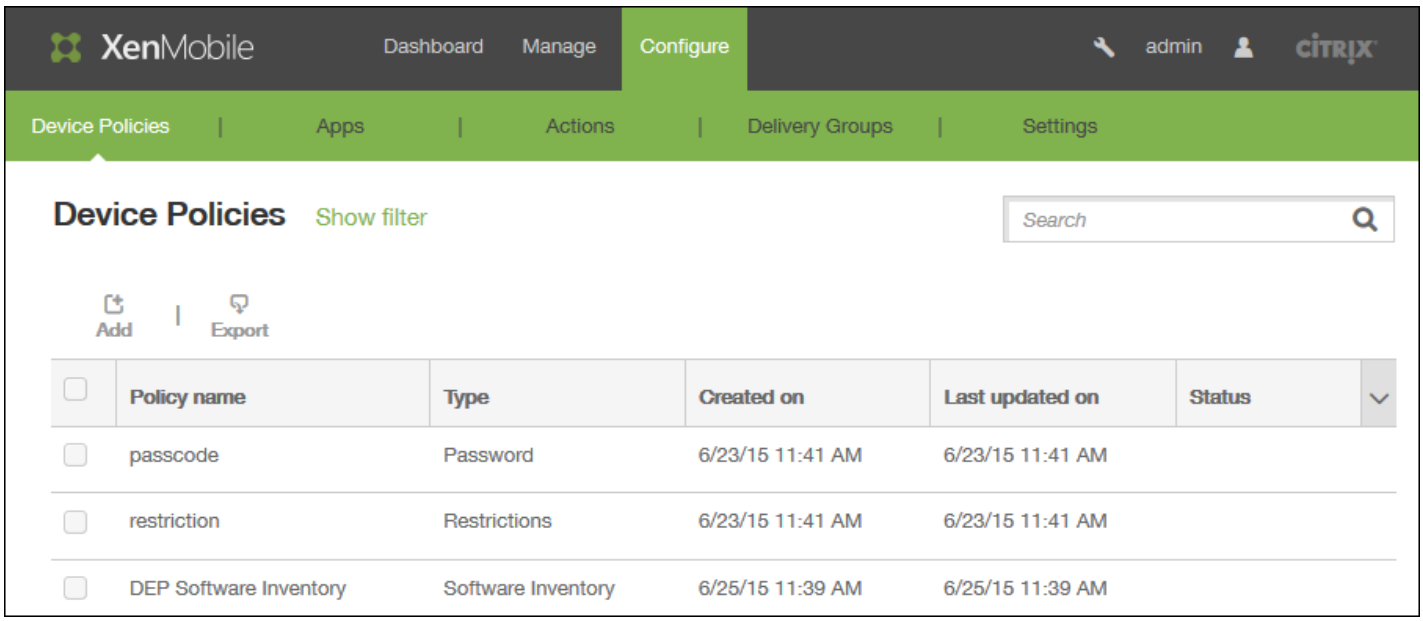
Oct 22, 2015

可以为 iOS 和 Android 设备添加接入点名称 (APN) 设备策略。如果贵组织不使用客户 APN 从移动设备连接到 Internet，可以使用此策略。APN 策略确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。大多数新式电话中已经定义此设置。

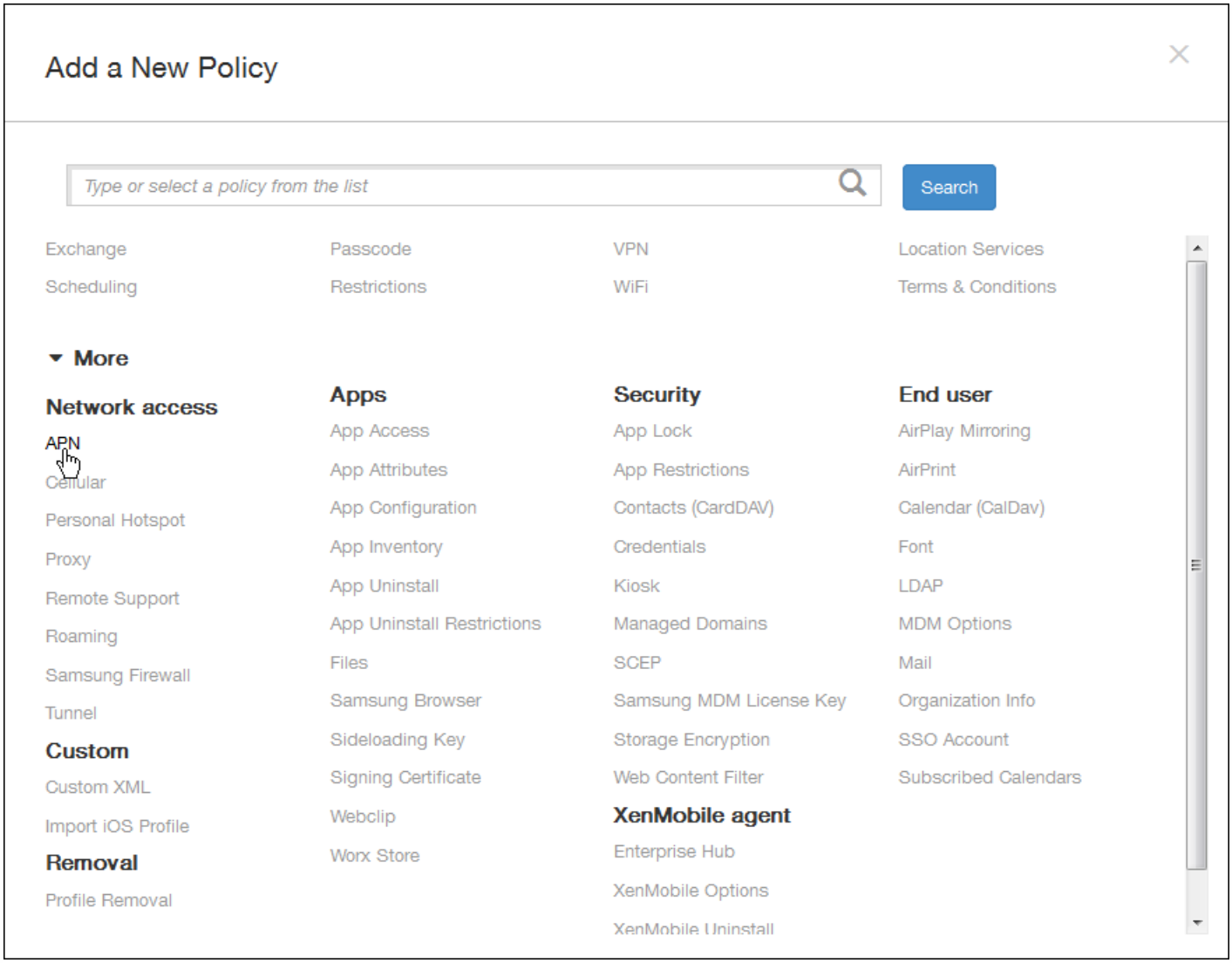
iOS 设置

Android 设置

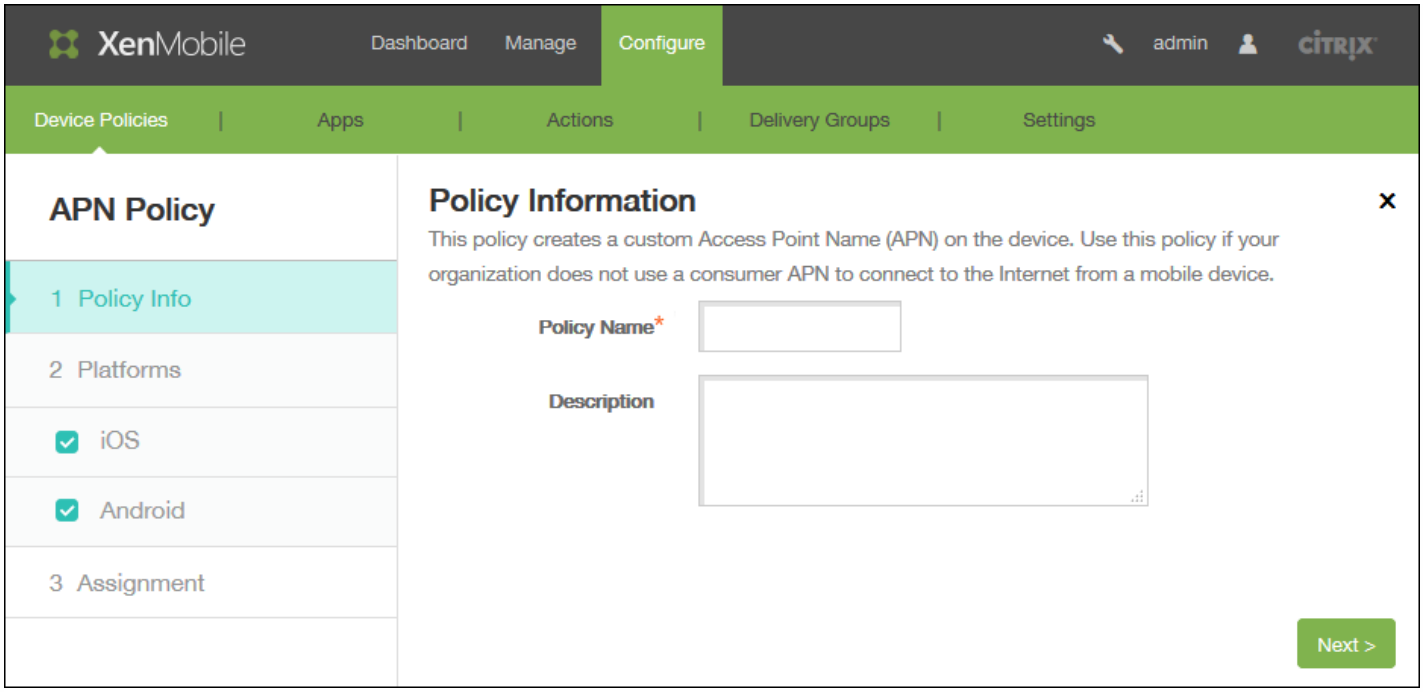
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。



2. 单击**添加**添加新策略。将显示**添加新策略**页面。



3. 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**。此时将显示 **APN 策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

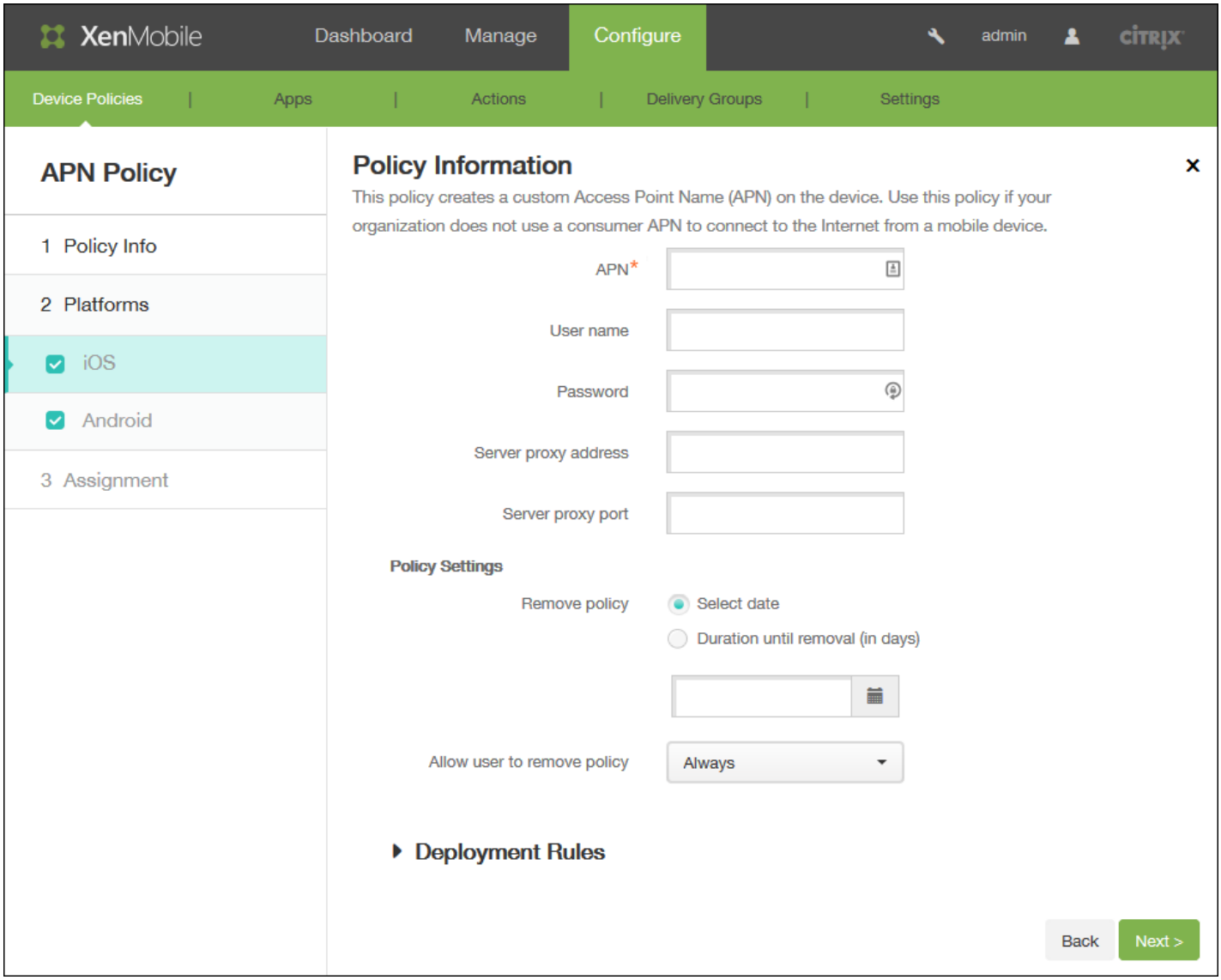
5. 单击**下一步**。此时将显示**策略平台**页面。

注意：显示**策略平台**页面时，会选中所有平台，并且首先看到 iOS 平台。

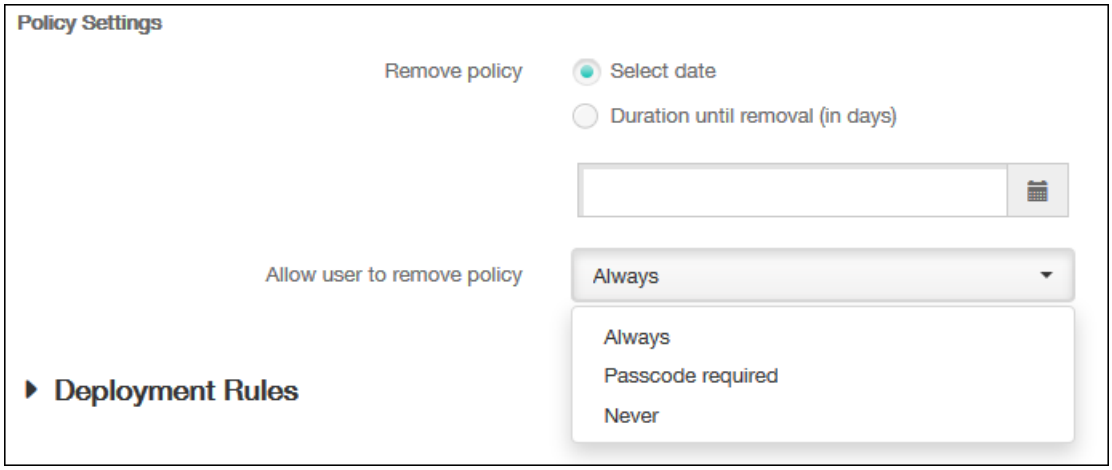
6. 在**平台**下面，选择要添加的平台。

完成对平台设置的配置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

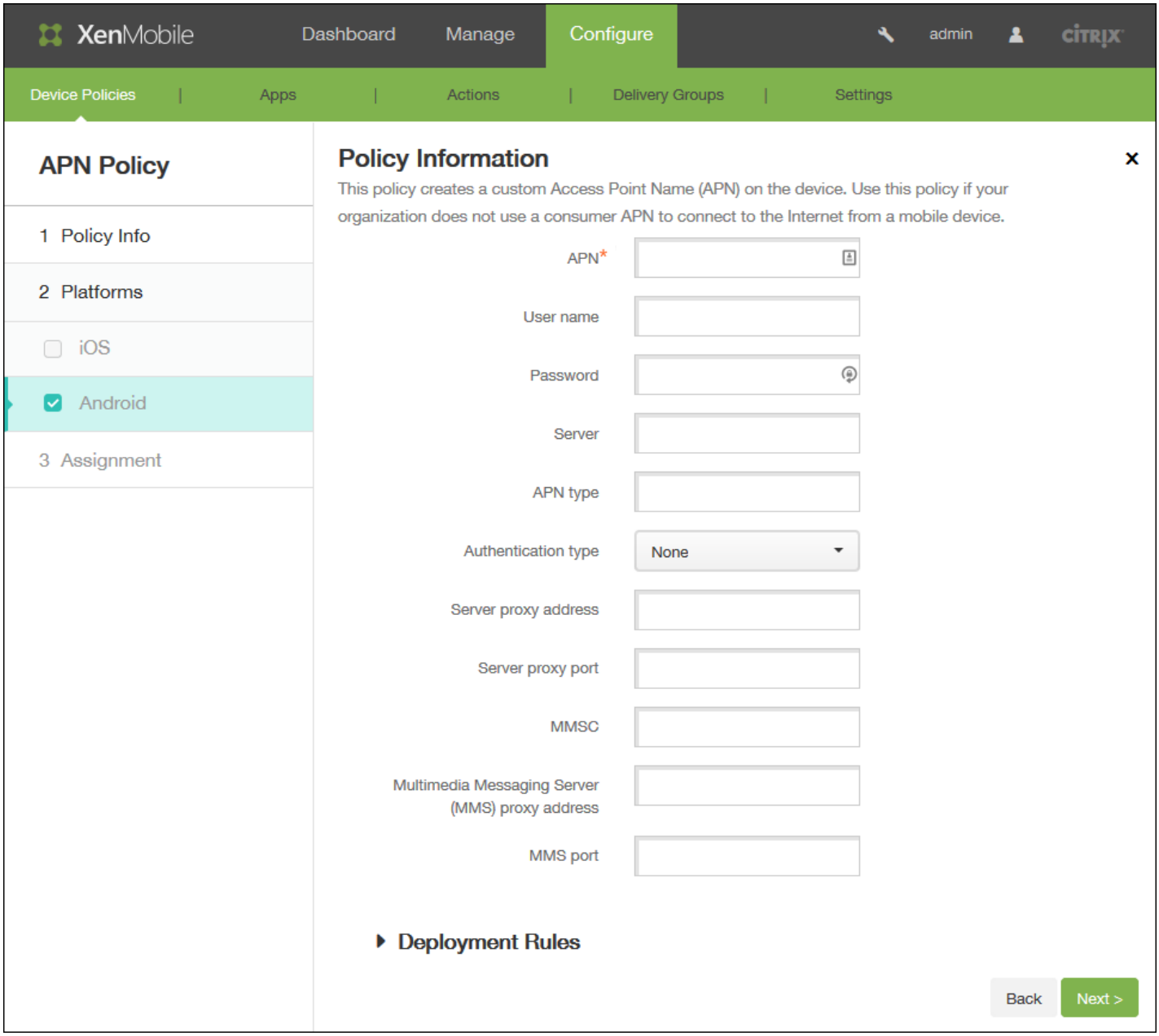
iOS 设置



- **APN**：键入接入点的名称。此值必须与某个已接受的 iOS APN 匹配，否则策略将失败。
- **用户名**：该字符串指定此 APN 的用户名。如果用户名缺失，配置文件安装期间设备会提示输入该字符串。
- **密码**：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- **服务器代理地址**：APN 代理的 IP 地址或 URL。
- **服务器代理端口**：APN 代理的端口号。如果已输入服务器代理地址，则此字段为必填字段。
- 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 **Removal password**（删除密码）旁边，键入必需的密码。



Android 设置

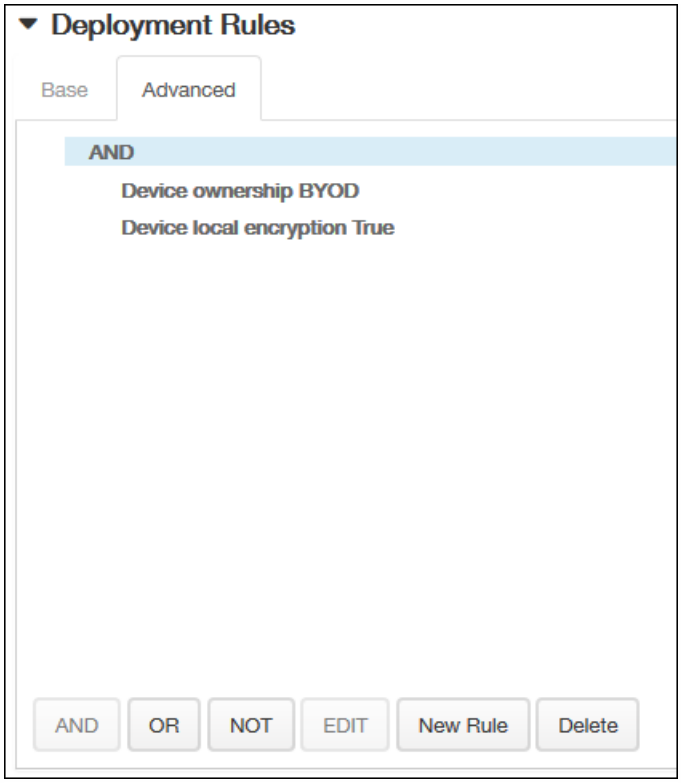


- **APN**：键入接入点的名称。此值必须与某个已接受的 Android APN 匹配，否则策略将失败。
- **用户名**：该字符串指定此 APN 的用户名。如果用户名缺失，在配置文件安装期间设备会提示输入该字符串。
- **密码**：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- **服务器**：此设置出现在智能手机出现之前，通常为空。它是指无法访问或显示标准 Web 站点的手机的无线应用协议 (WAP) 网关服务器。
- **APN 类型**：此设置必须匹配运营商的接入点用途。它是 APN 服务说明符的逗号分隔字符串，必须与无线运营商的发布定义匹配。示例包括：
  - *。所有流量均通过此接入点。
  - mms。多媒体流量通过此接入点。
  - default（默认）。包括多媒体在内的所有流量均通过此接入点。
  - supl。与 GPS 关联的安全用户层面定位 (Secure User Plane Location)
  - dun。拨号网络已经过时，很少使用。

    - hipri。高优先级网络。
    - fota。无线固件升级用于接收固件更新。
- **身份验证类型**：在列表中，单击要使用的身份验证类型。默认为“无”。
- **服务器代理地址**：运营商的 APN HTTP 代理的 IP 地址或 URL。
- **服务器代理端口**：APN 代理的端口号。如果已输入服务器代理地址，则此字段为必填字段。
- **MMSC**：运营商提供的 MMS 网关服务器地址。
- 多媒体消息服务器(MMS)代理地址：指 MMS 通信的多媒体消息服务服务器。MMS 使得 SMS 可以发送包含多媒体内容（如图片或视频）的大型消息。这些服务器需要特定的协议（如 MM1、... MM11）。
- **MMS 端口**：用于 MMS 代理的端口。

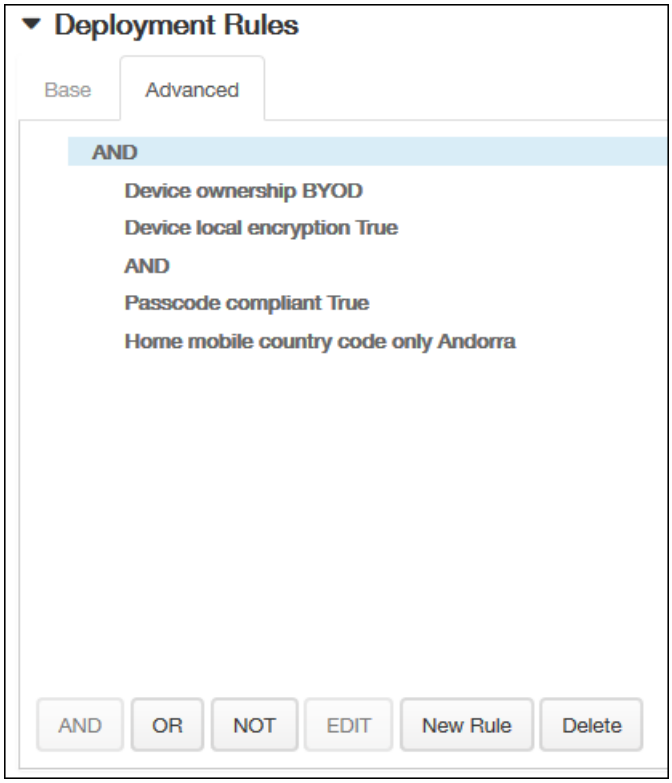
7. 展开**部署规则**，然后配置以下设置：默认情况下显示**基础**选项卡。

- 在此列表中，单击选项以确定部署策略的时间。
    - 可以选择在满足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**。
    - 单击**新建规则**以定义条件。
    - 在列表中，单击条件，如**设备所有权**和 **BYOD**，如上图所示。
    - 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。
- 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。



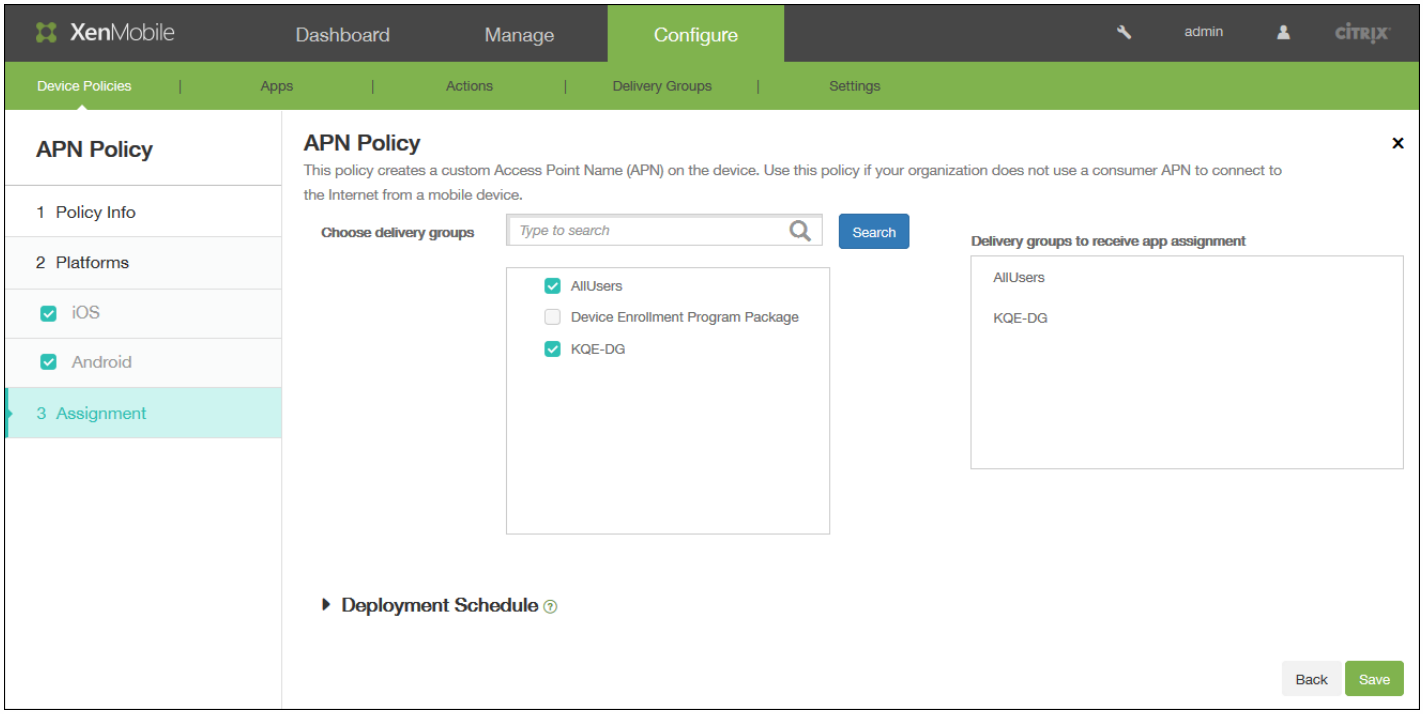
- 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
  - 单击 **AND**、**OR** 或 **NOT**。
  - 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
    您随时可以通过单击选择某个条件，然后单击**编辑**以更改此条件或单击**删除**以删除此条件。
  - 如果要添加更多条件，请再次单击**新建规则**。

    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 **APN 策略分配**页面。

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



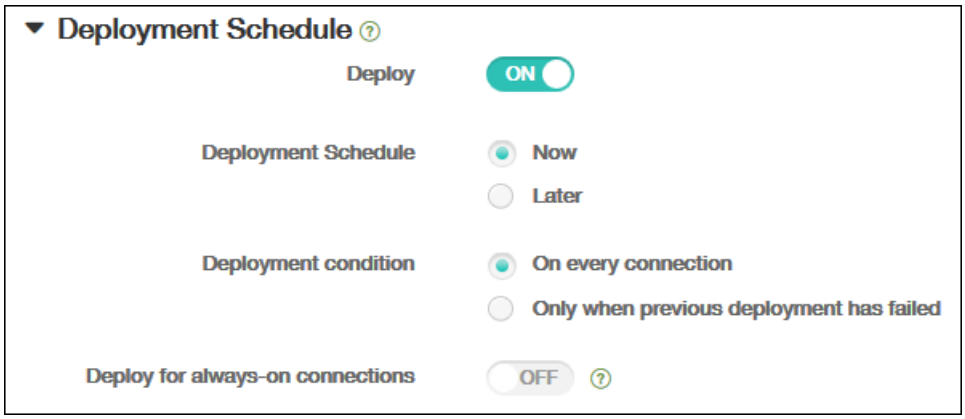
10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。默认选项为**开**。如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。默认选项为**立即**。
- 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
- 在**部署条件**旁边，单击**每次连接时**或单击**仅当之前的部署失败时**。默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。默认选项为**关**。

注意：

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

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



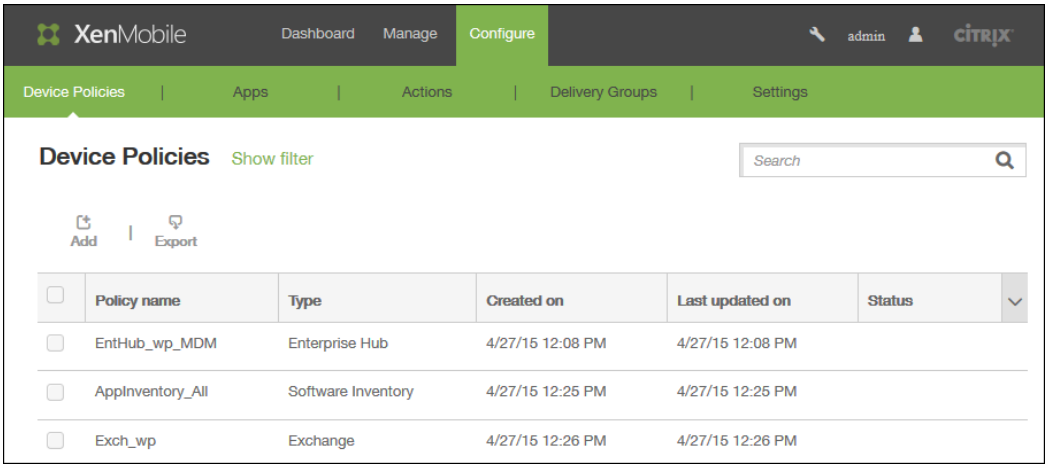
11. 单击**保存**以保存此策略。

添加适用于 iOS 的手机网络设备策略

Oct 22, 2015

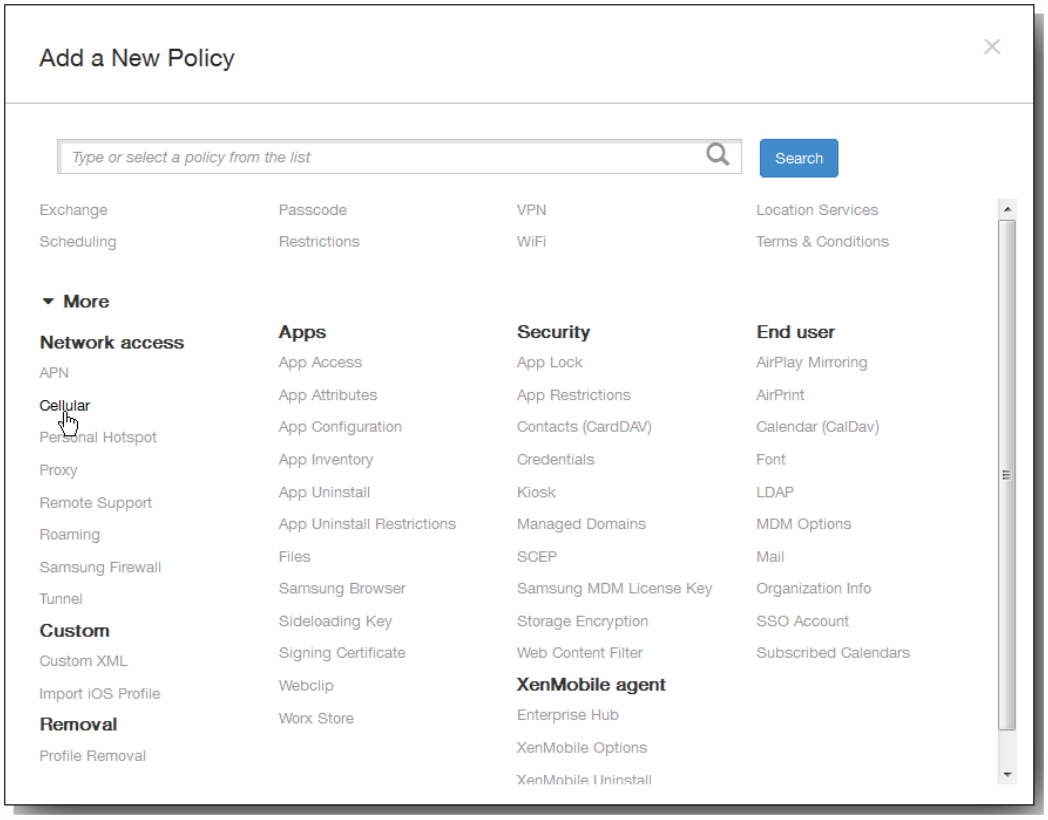
此策略允许您在 iOS 设备上配置手机网络设置。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。

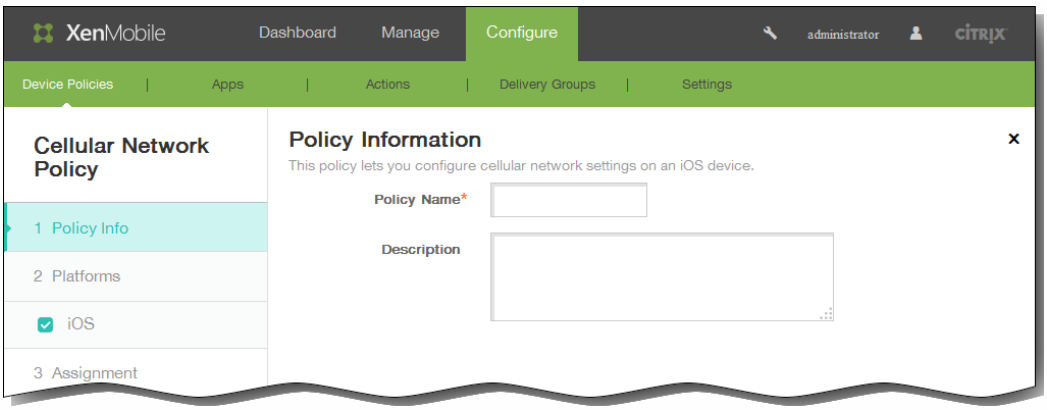


2. 单击添加。

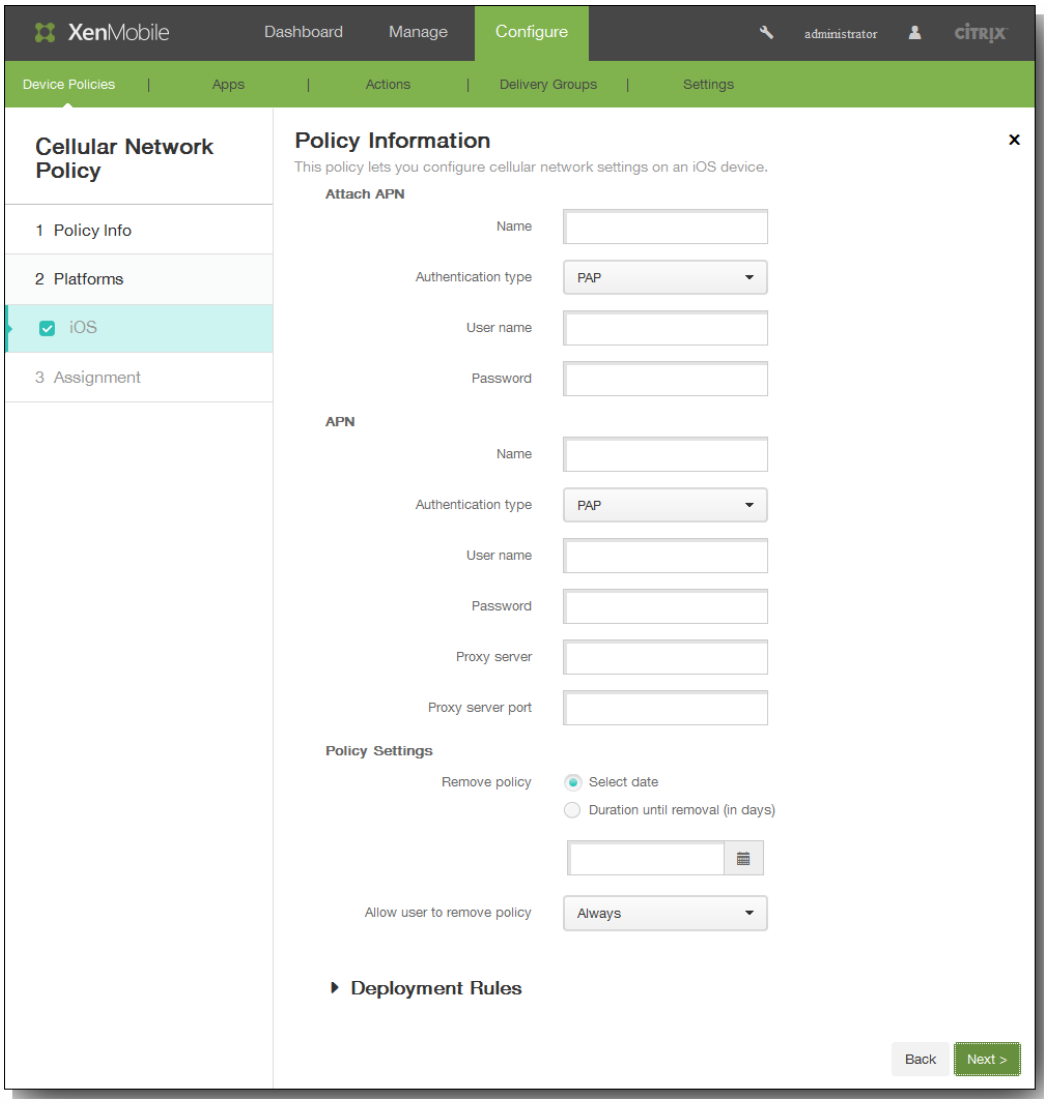
   将显示添加新策略页面。



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。

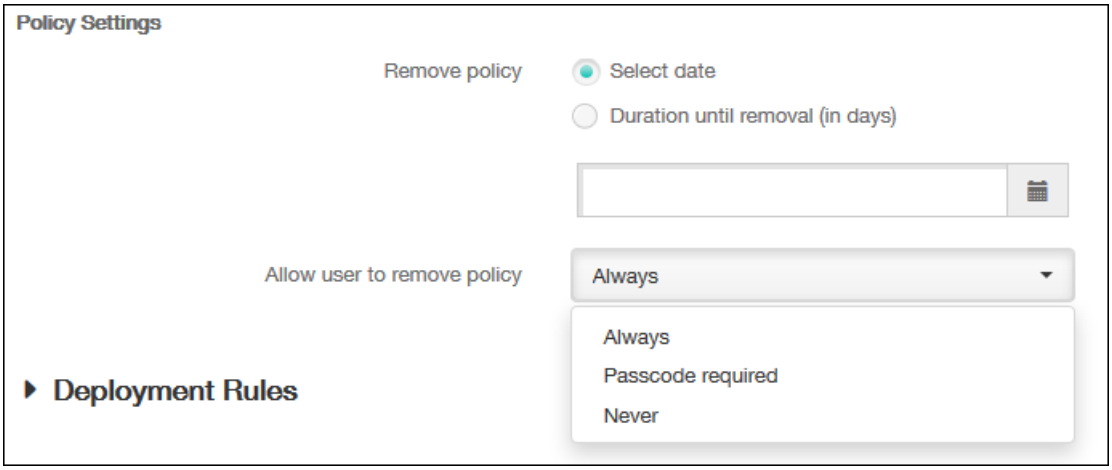


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。

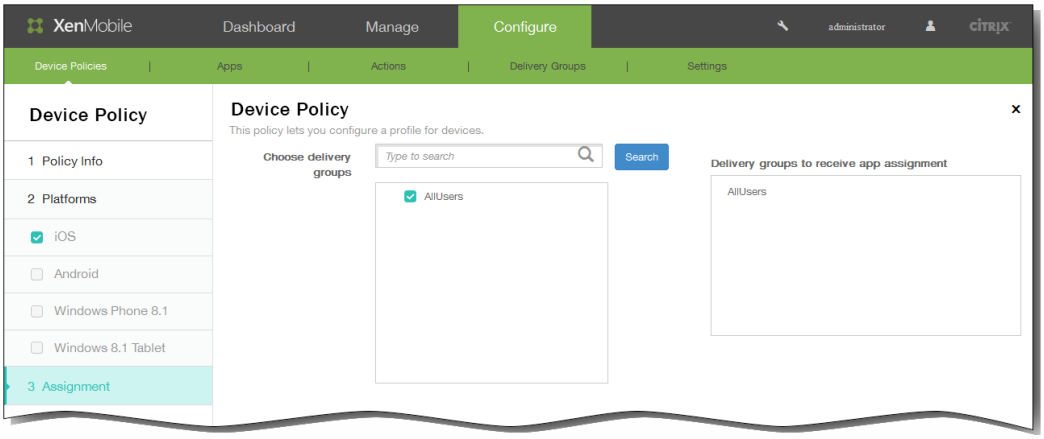


6. 在 iOS 平台信息页面上，输入以下信息：在**附加 APN** 下面：
   1. 名称：键入此配置的名称。
   2. 身份验证类型：在清单上，单击质询握手身份验证协议 (CHAP) 或密码身份验证协议 (PAP)。 默认值为 PAP。
   3. 用户名：键入用于身份验证的用户名。
   4. 密码：键入用于身份验证的密码。

   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。



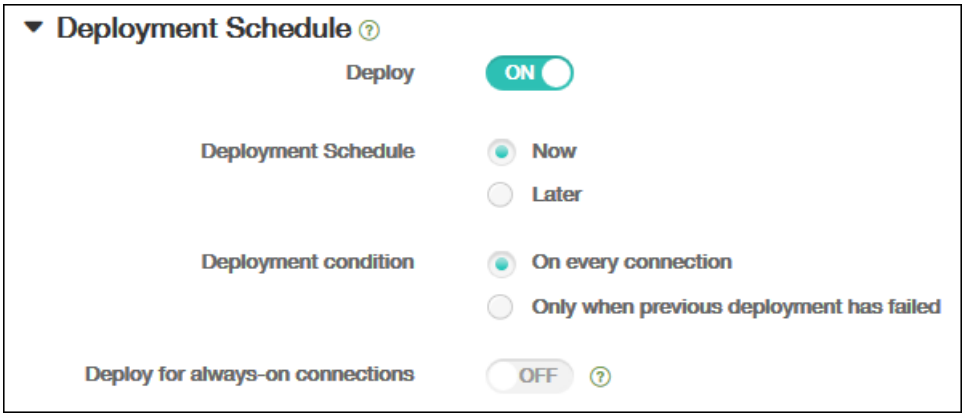
11. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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

Oct 22, 2015

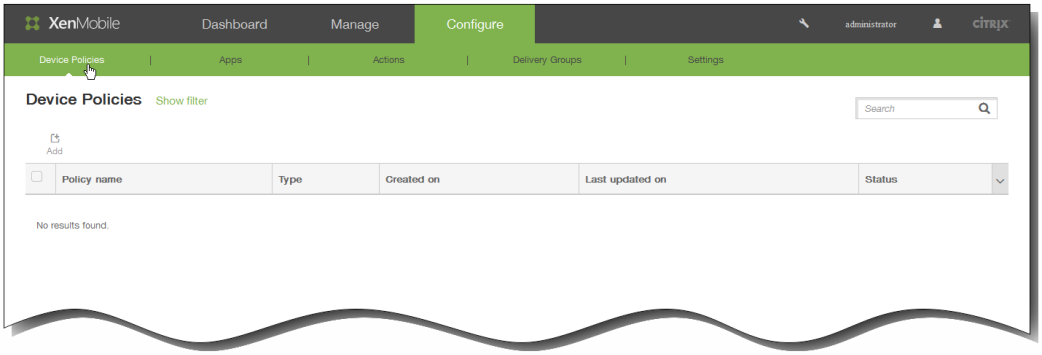
面向 Windows Phone 8.1 的企业 Hub 设备策略允许您通过企业 Hub 公司应用商店分发应用程序。

需要具备以下各项才能创建策略：

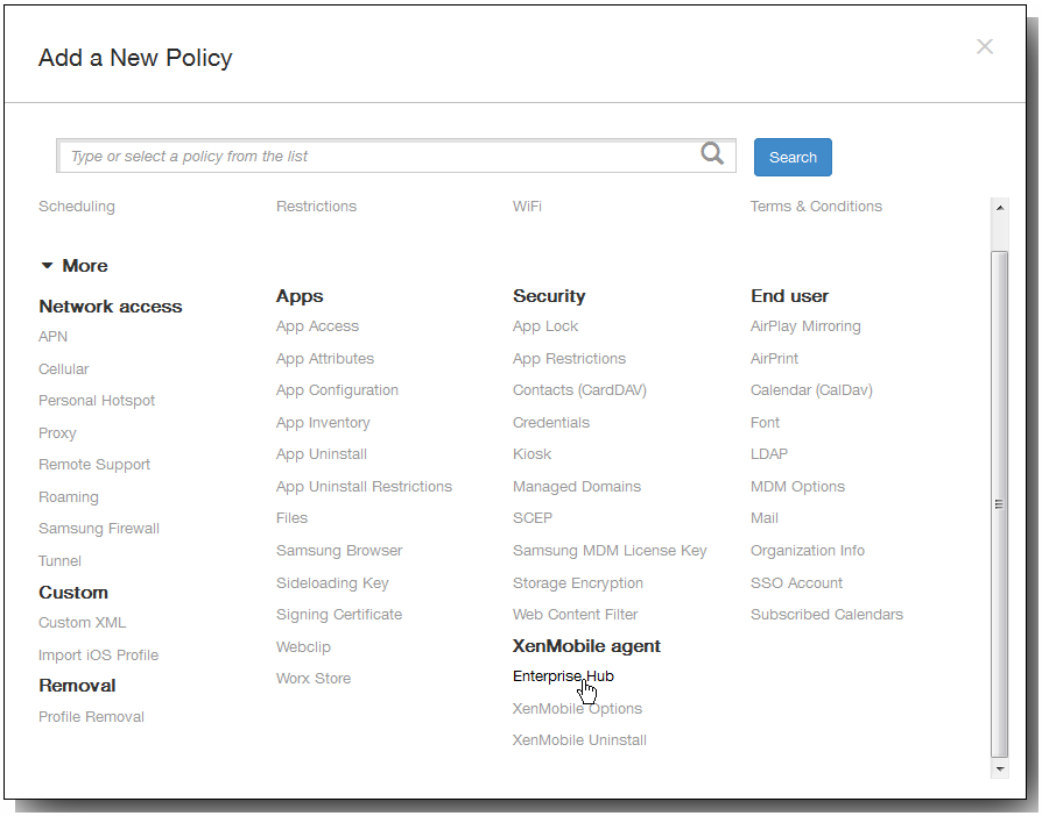
- 来自 Symantec 的 AET (.aetx) 签名证书
- 使用 Microsoft 应用程序签名工具 (XapSignTool.exe) 签名的 Citrix Company Hub 应用程序

注意：对于一种 Windows Phone 8.1 Worx Home 模式，XenMobile 仅支持一种企业 Hub 策略。例如，要上载 Windows Phone 8.1 Worx Home for XenMobile Enterprise Edition，不应该使用不同版本的 Work Home for XenMobile Enterprise Edition 创建多个企业 Hub 策略。设备注册期间只能部署初始企业 Hub 策略。

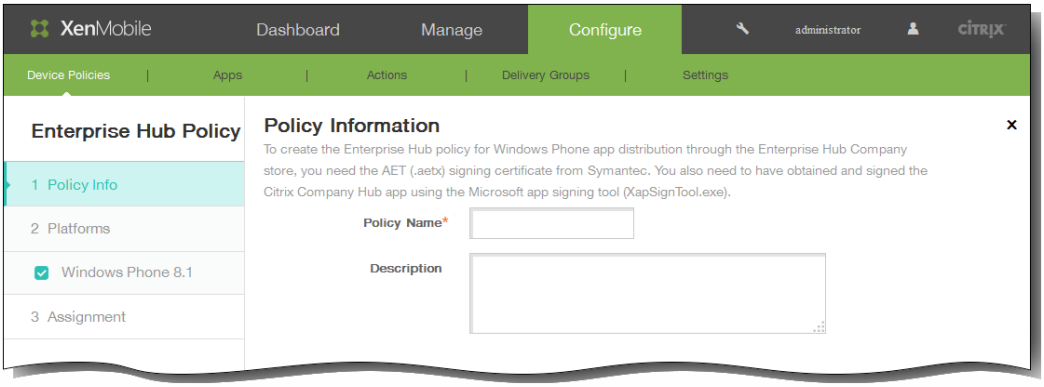
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



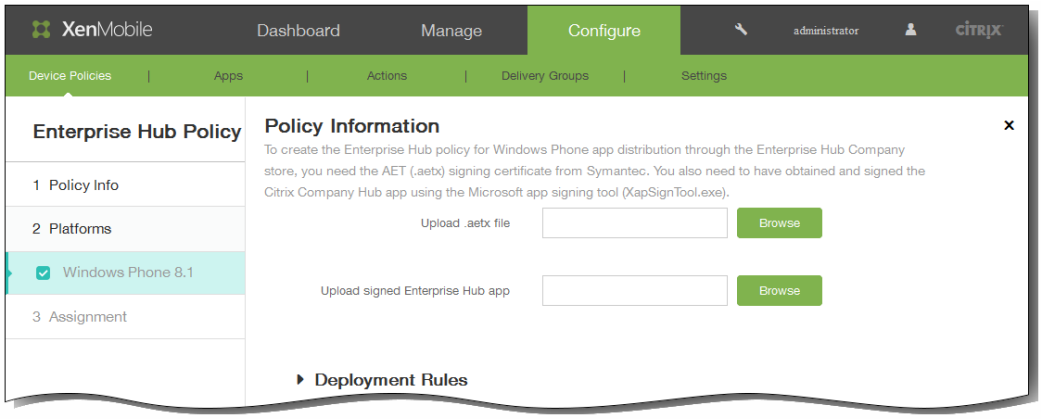
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



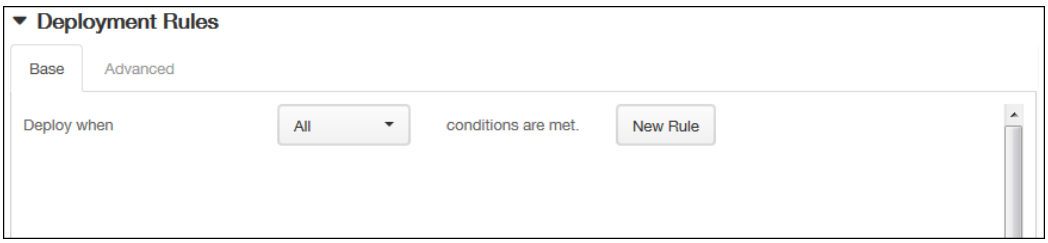
3. 单击更多，然后在 XenMobile Agent 下单击企业 Hub。 此时将显示企业 Hub 策略页面。



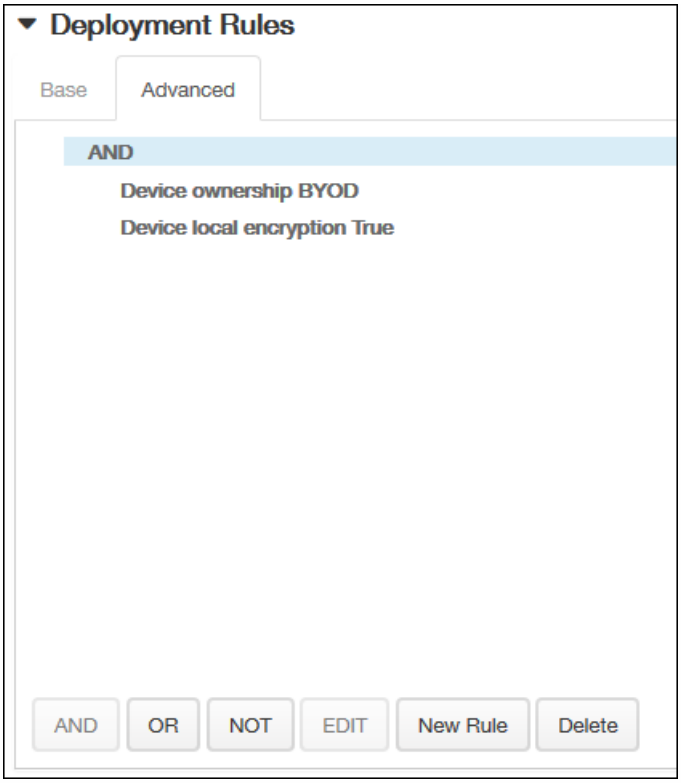
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：输入策略的描述性名称。
   2. 说明：如有需要，请输入策略的说明。
5. 单击下一步。 此时将显示 Windows Phone 8.1 平台页面。



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。

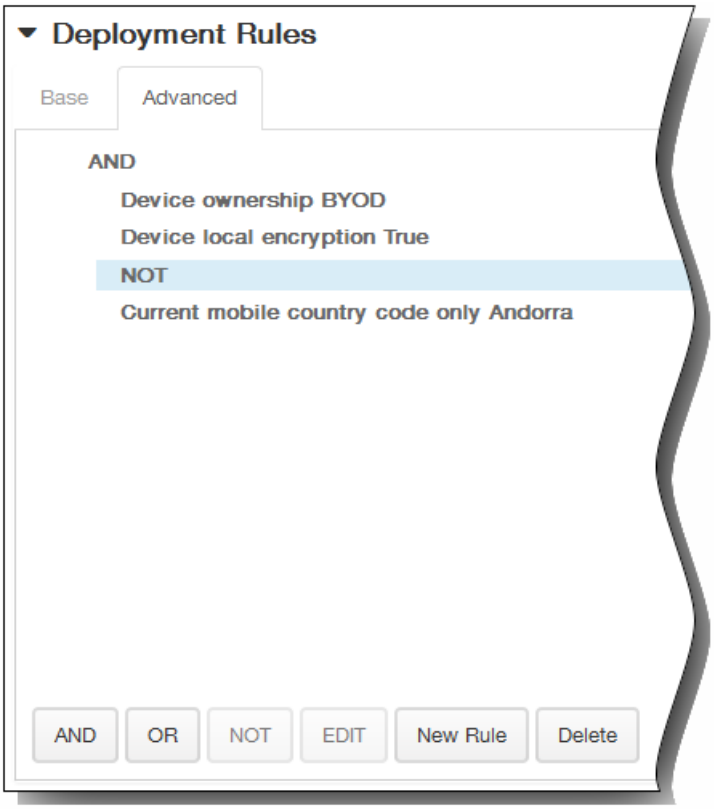


   1. 在此列表中，单击选项以确定部署策略的时间。
      1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
      2. 单击新建规则以定义条件。
      3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
      4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
   2. 单击高级选项卡以使用布尔选项组合规则。

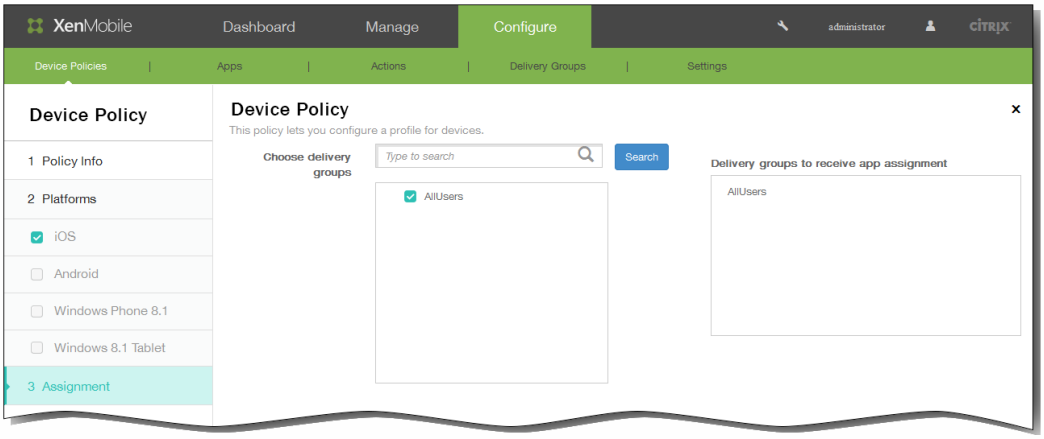


将显示您在基础选项卡上选择的条件。

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。

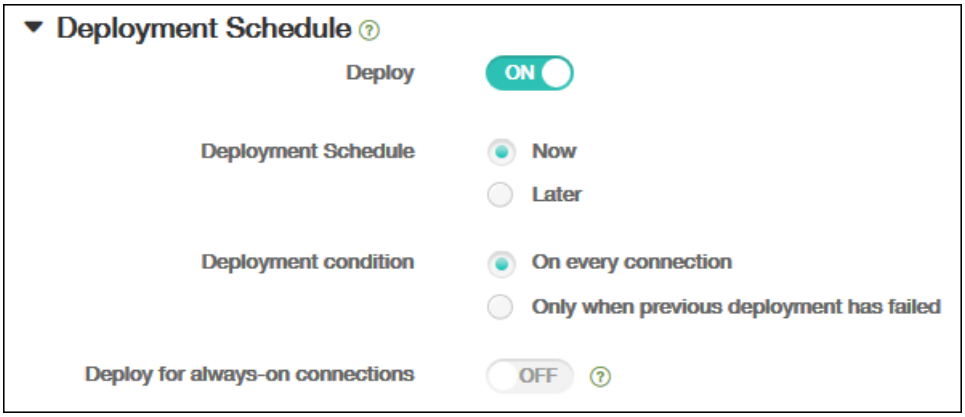


8. 单击下一步。 此时将显示 Enterprise Hub Policy（企业 Hub 策略）分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

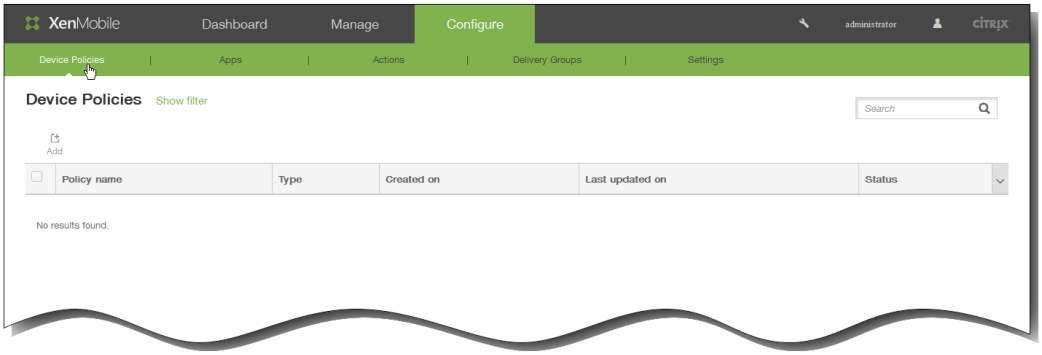
Microsoft Exchange ActiveSync 设备策略

Oct 22, 2015

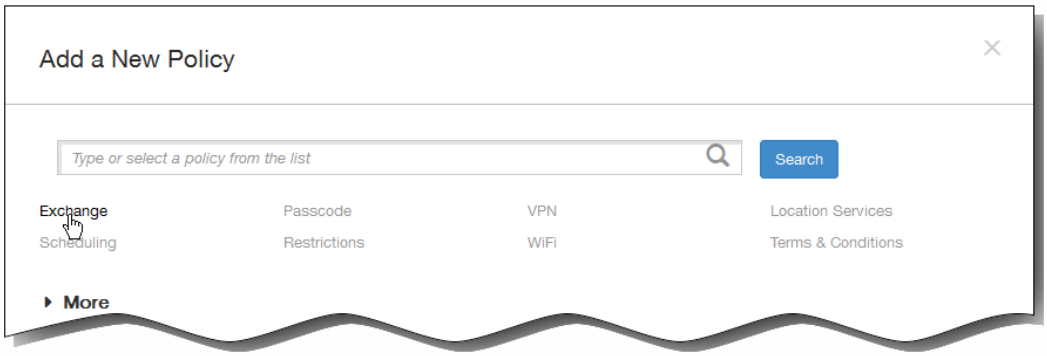
可以使用 Exchange ActiveSync 设备策略在用户设备上配置电子邮件客户端，以允许其访问 Exchange 上托管的企业电子邮件。可以为 iOS、Android HTC、Android TouchDown、Android for Work、Samsung SAFE、Samsung KNOX 和 Windows Phone 8.1 创建策略。每个平台都需要一组不同的值，这些值将在以下主题中详细说明：

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。

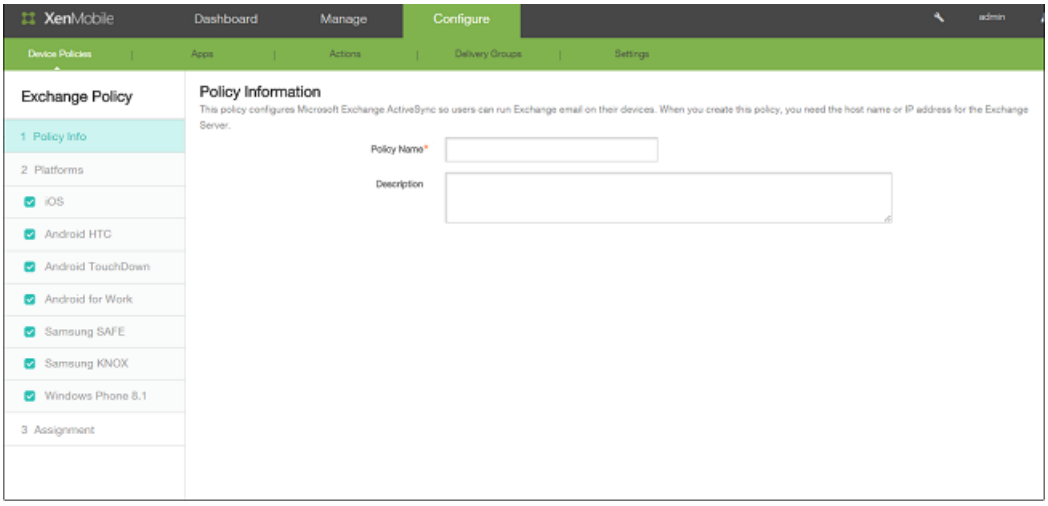
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



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：

     Exchange ActiveSync 帐户名称：键入 Exchange Server 帐户名称。

     Exchange ActiveSync主机名：键入 Exchange Server主机名或 IP 地址。

     使用 SSL：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为“开”。

     域：输入 Exchange Server 所在的域。
     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：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。

     密码：输入 Exchange 用户帐户的可选密码。

     电子邮件同步时间间隔：从下拉框中选择同步时间间隔值。

     身份凭据(密钥库或 PKI 凭据)：可选。从下拉框中选择配置的证书/PKI 凭据。

     授权电子邮件在帐户之间移动：可选。选择“开”/“关”。默认值为“关”。

     仅从电子邮件应用程序发送电子邮件：可选。选择“开”/“关”。默认值为“关”。

     禁用最新电子邮件同步：可选。选择“开”/“关”。默认值为“关”。

启用 S/MIME：可选。选择“开”/“关”。默认值为“关”。

启用“为消息单独设置 S/MIME”开关：可选。选择“开”/“关”。默认值为“关”。

- 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。默认值为“无”。

  应用程序设置：为此策略选择性添加 TouchDown 应用程序设置。

  策略：为此策略选择性添加 TouchDown 策略。

- 如果选择 **Android for Work**，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。可以添加到 doc 中，默认值为“无”。

- 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。默认值为“无”。

  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。
  Account name or display name（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。

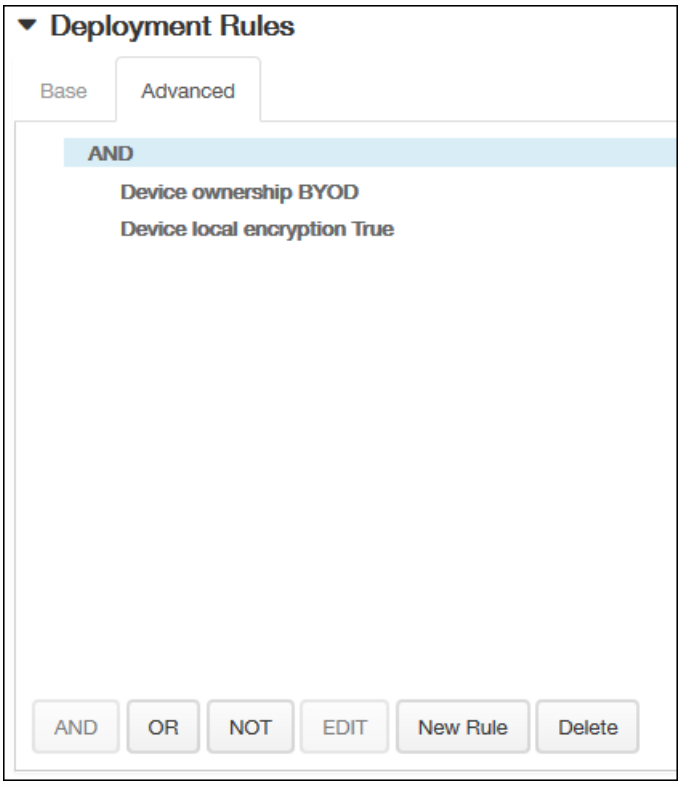
  同步内容天数：在列表中，请单击要将设备上过去多少天内的所有内容与 Exchange Server 同步。

  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。

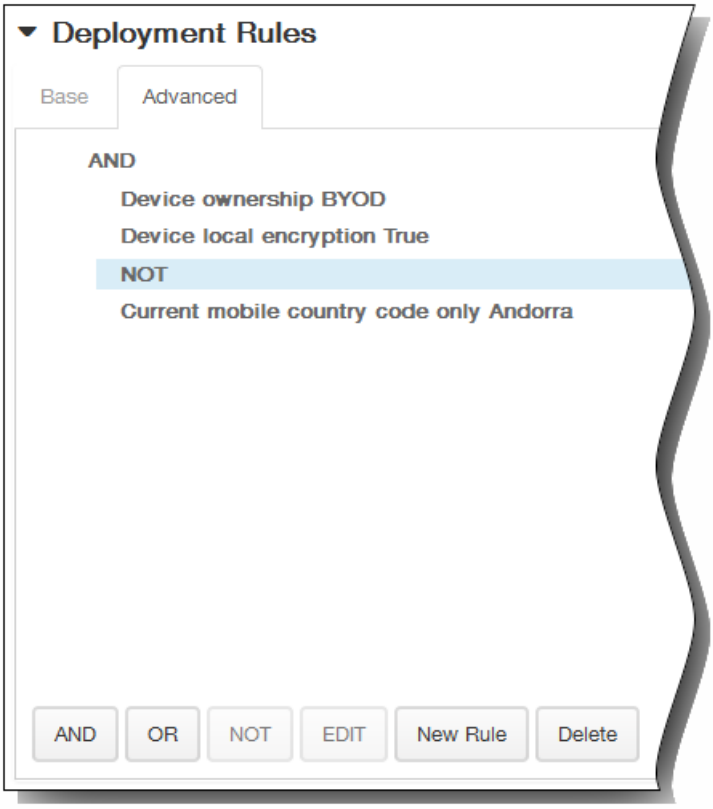
1. 在此列表中，单击选项以确定部署策略的时间。
   1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。



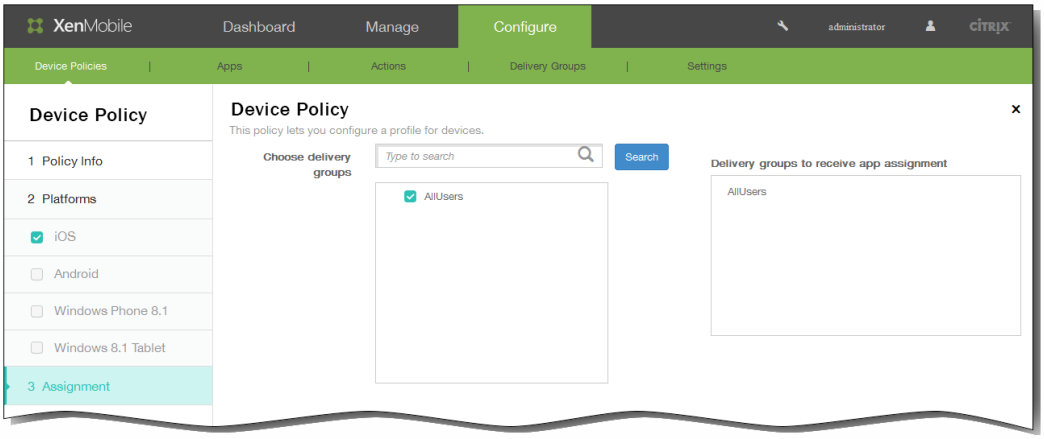
将显示您在基础选项卡上选择的条件。

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。

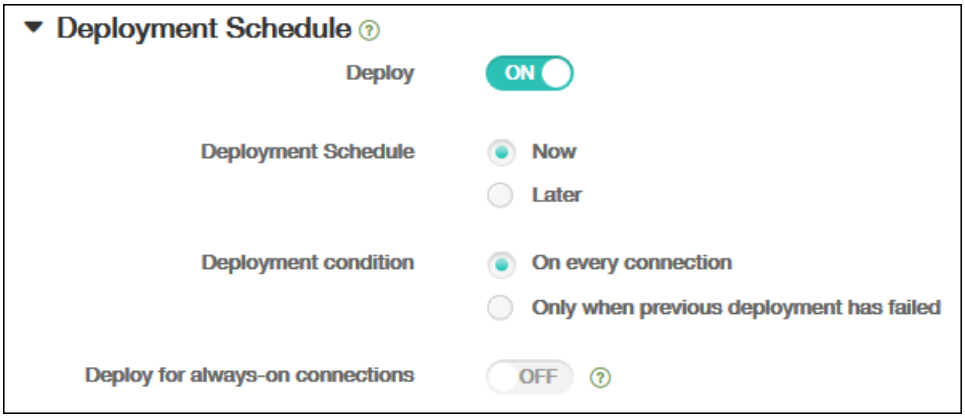


10. 展开部署计划，然后配置以下设置：
    1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。如果选择关，无需配置其他选项。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。

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。

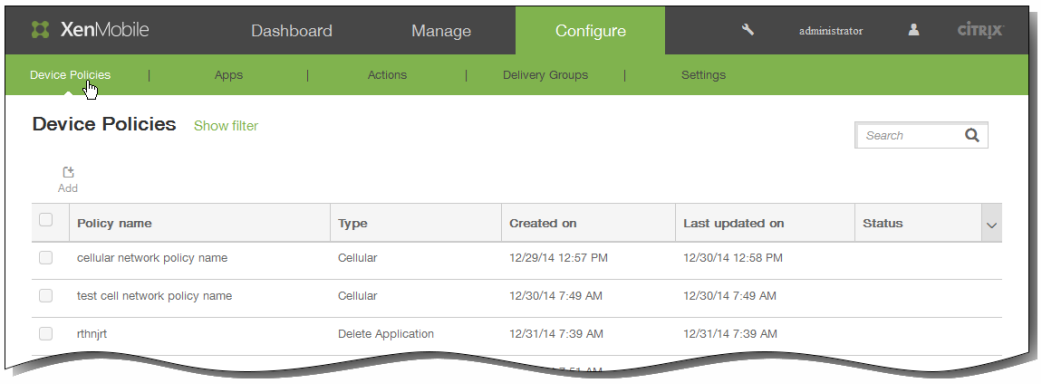
定位设备策略

Oct 22, 2015

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。

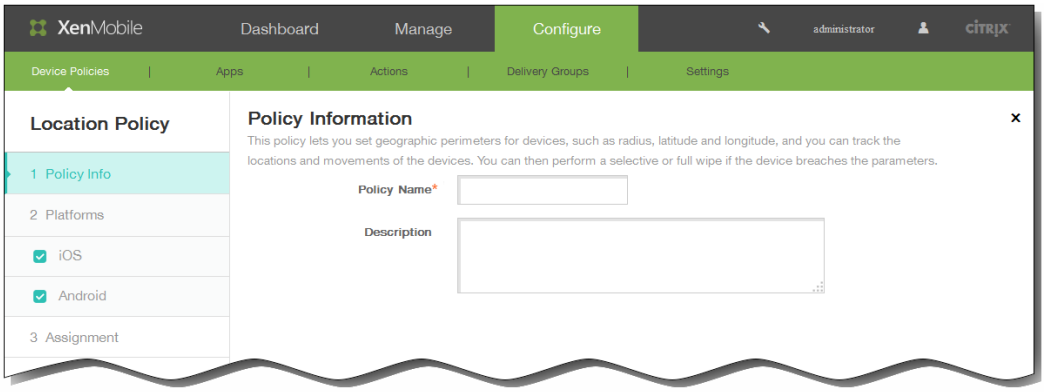
可以为 iOS 和 Android 创建定位设备策略。每种平台需要一组不同的值，本文将对此进行介绍。

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。

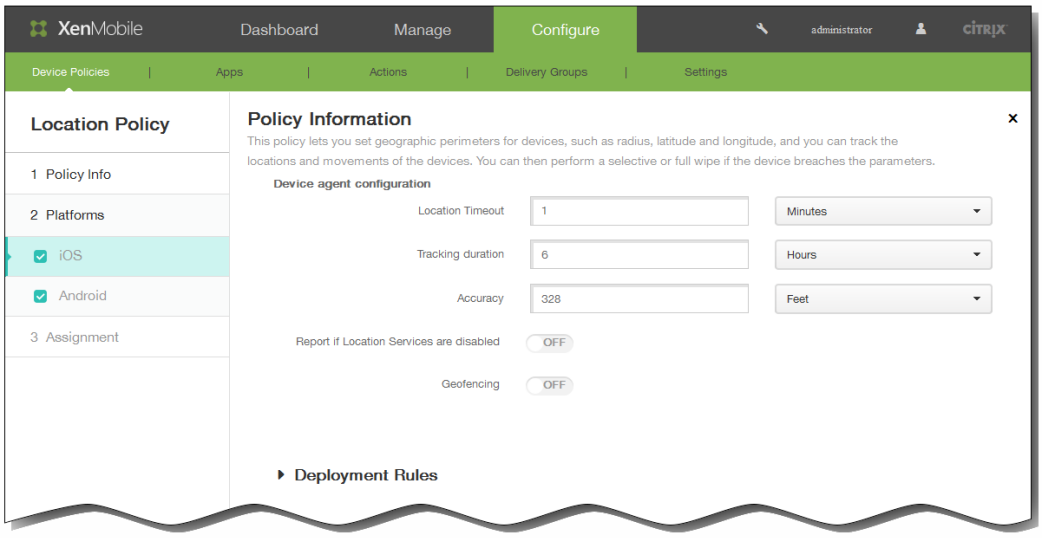


2. 单击添加添加新策略。 此时将显示添加新策略对话框。

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。



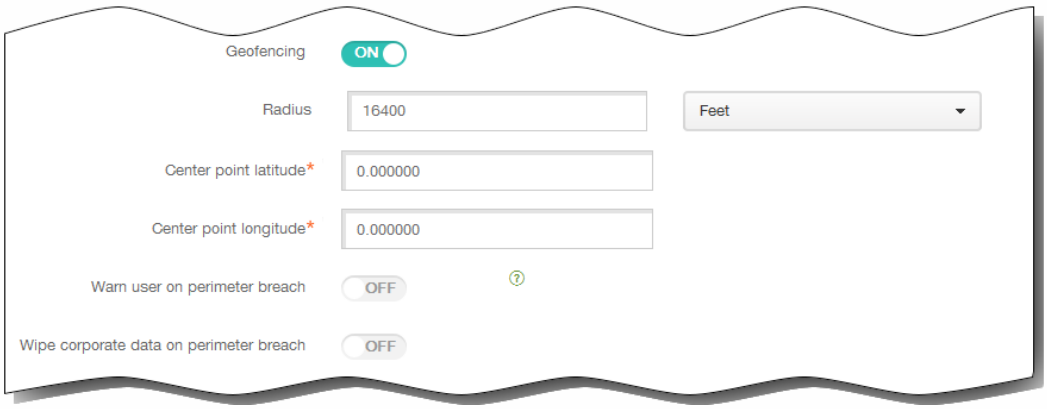
6. 在平台下面，选择要添加的平台。
   - 如果选择 iOS，可以配置以下设置：
     定位超时：键入数值，然后在列表中单击秒或分钟以设置 XenMobile 尝试修复设备位置的频率。有效值为 60–900 秒或 1–15 分钟。默认值为 1 分钟。

     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：

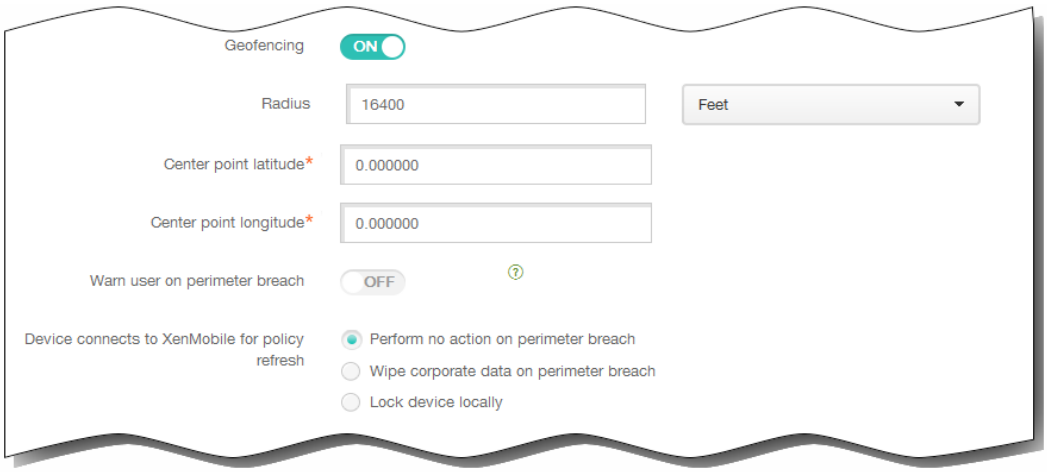


- 半径：键入数值，然后在列表中，单击要用于衡量半径的单位。默认值为 16,400 英尺。
  半径的有效值如下：
  - 164–164000 英尺
  - 1–50 千米
  - 50–50000 米
  - 54–54680 码
  - 1–31 英里
- 中心点纬度：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- 中心点经度：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- Warn user on perimeter breach（警告用户超出边界）：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 XenMobile 即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

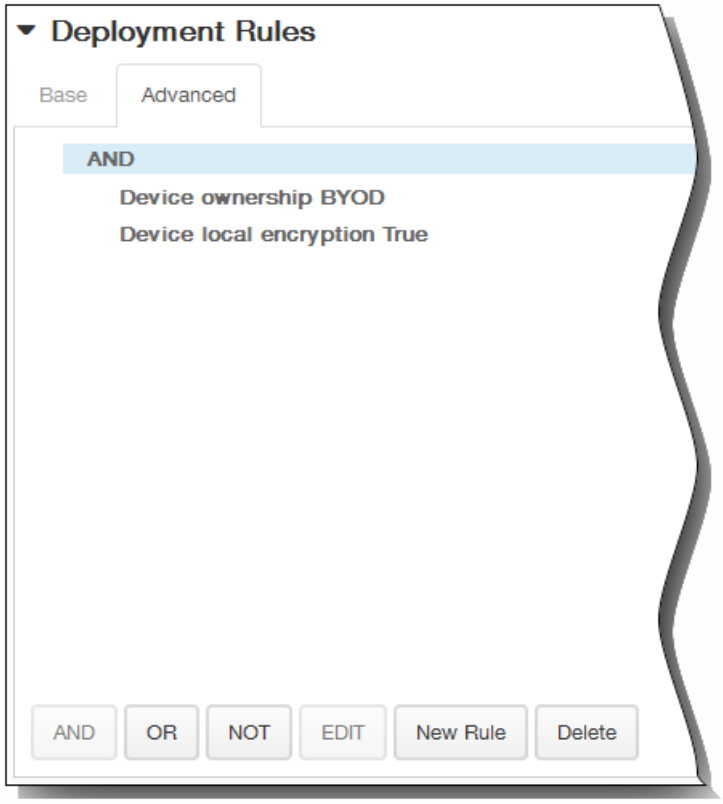
    键入数值，然后在列表中单击秒或分钟以设置从用户设备中擦除公司数据之前延迟的时间长度。这使用户有机会在 XenMobile 选择性擦除其设备之前返回到允许的位置。默认值为 0 秒。

  - 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。

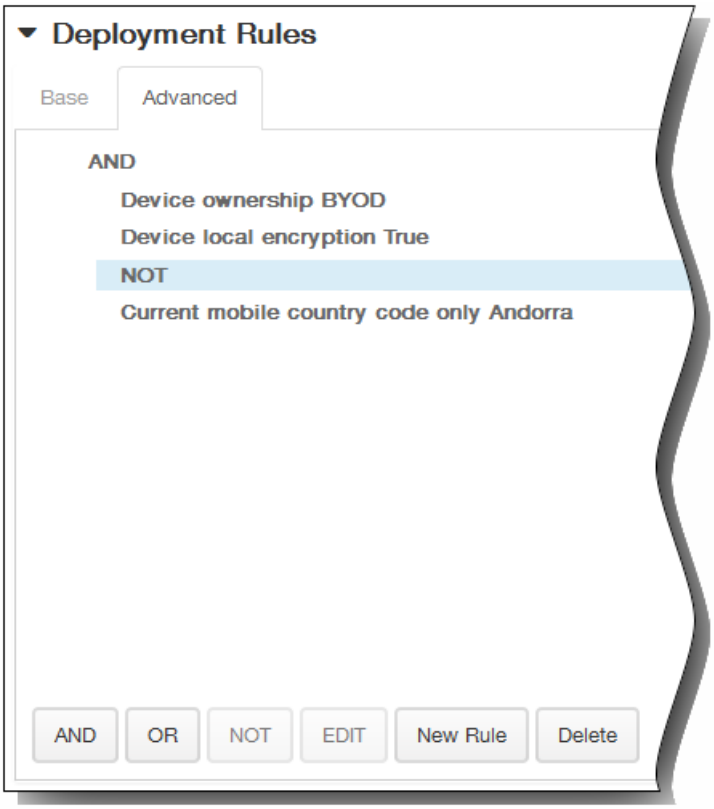
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

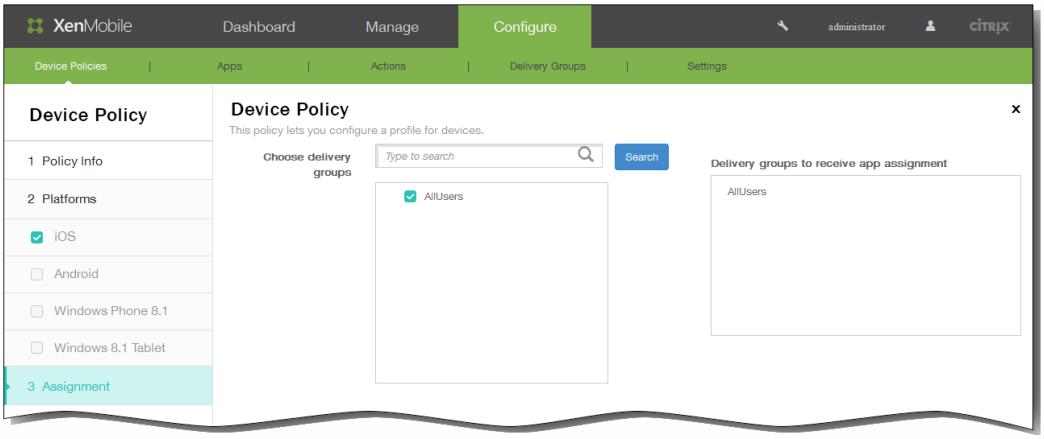


将显示您在基础选项卡上选择的条件。

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。



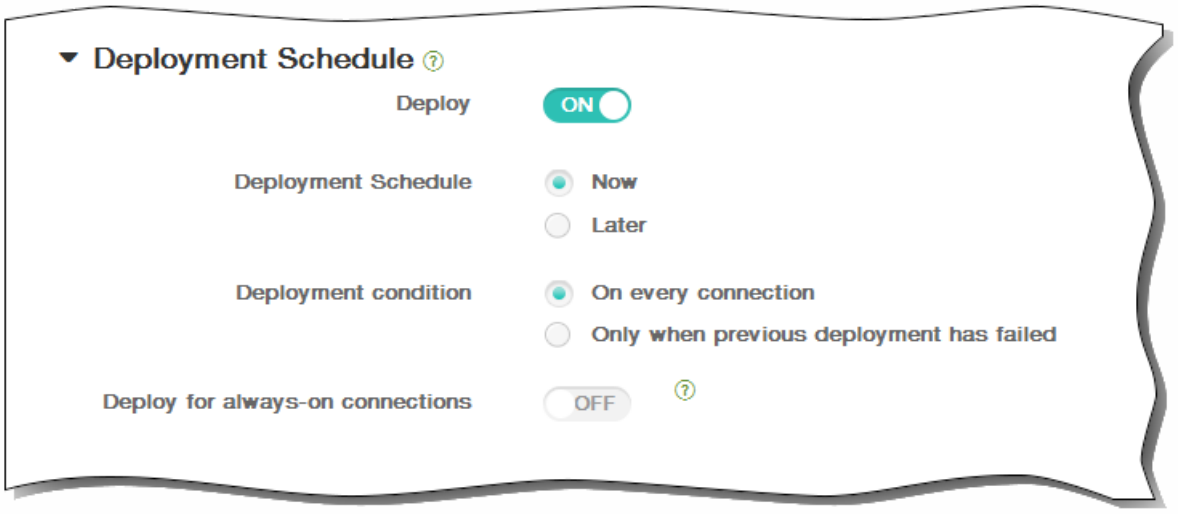
8. 单击下一步。 此时将显示定位策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。



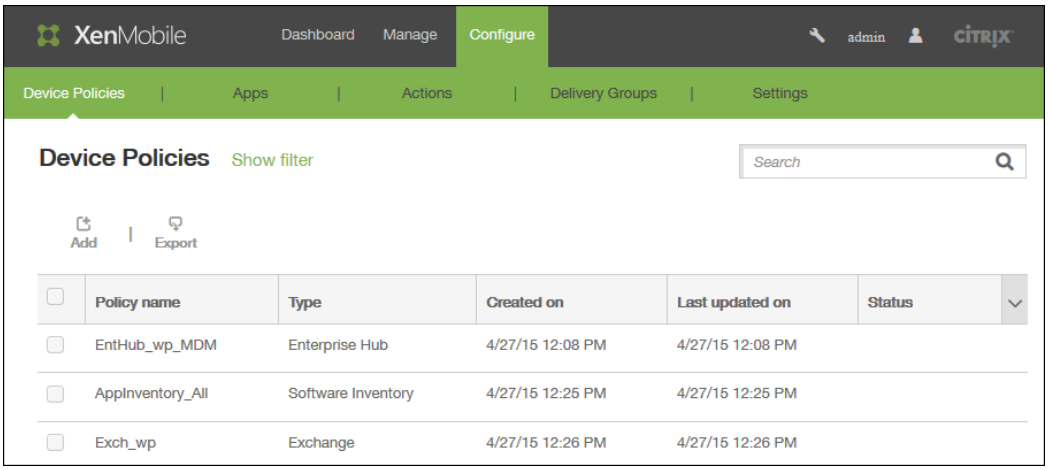
11. 单击保存以保存此策略。

连接计划设备策略

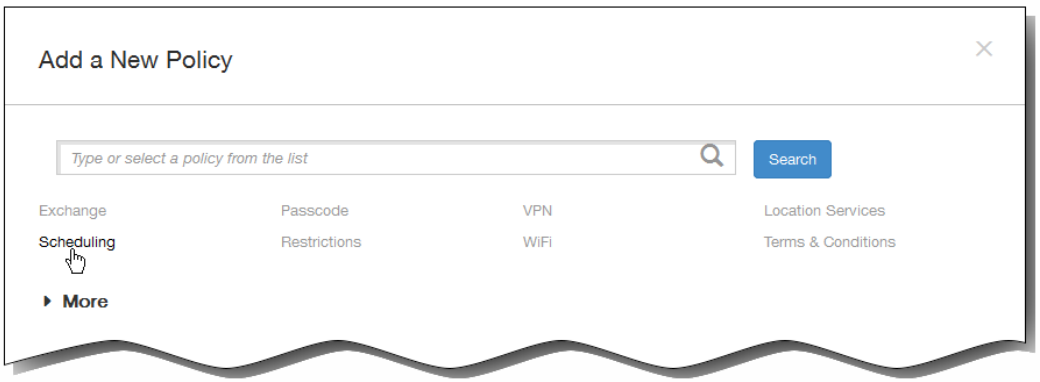
Oct 22, 2015

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。

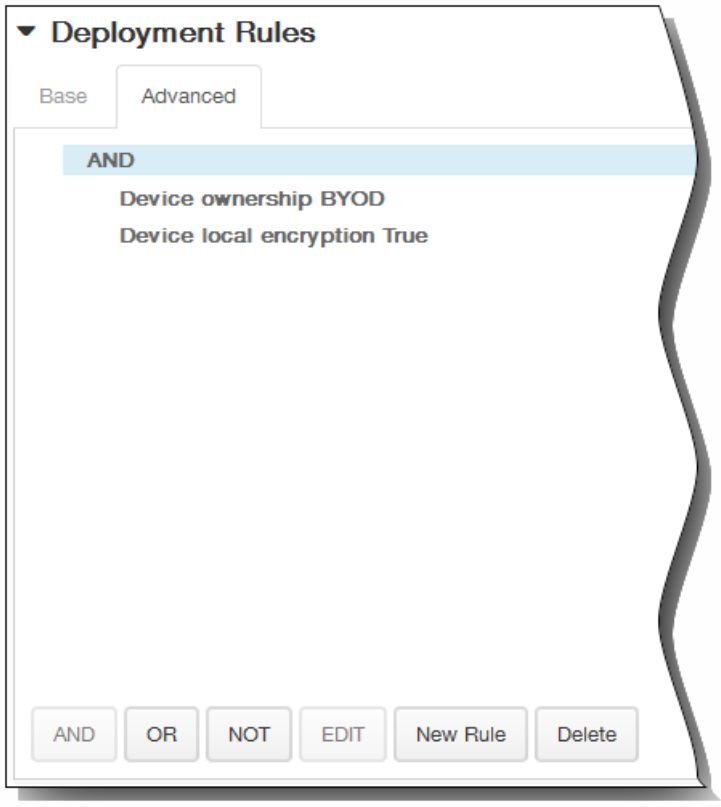
在此时段内保持永久连接：在定义的时间范围内，用户设备必须连接。

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。

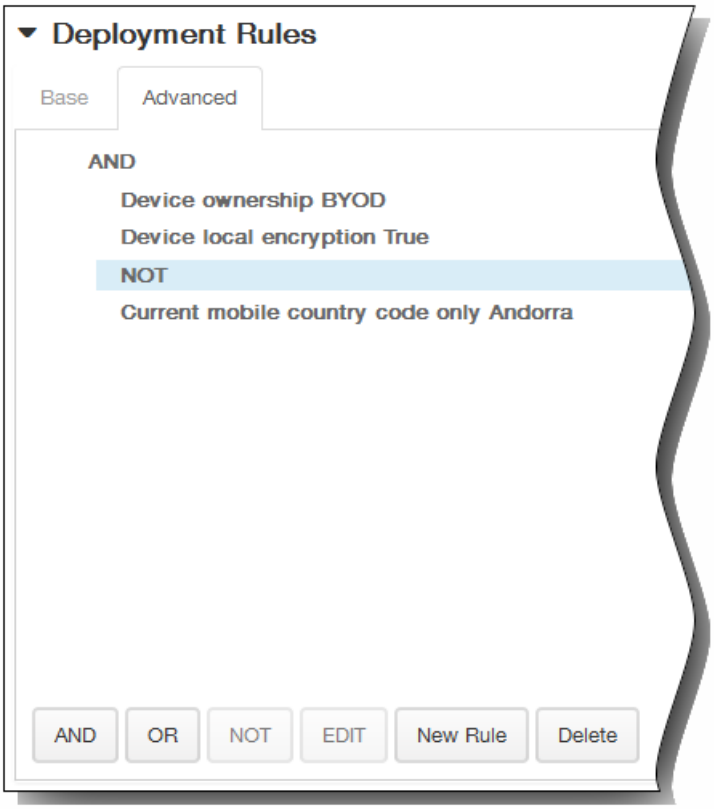


将显示您在基础选项卡上选择的条件。

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。

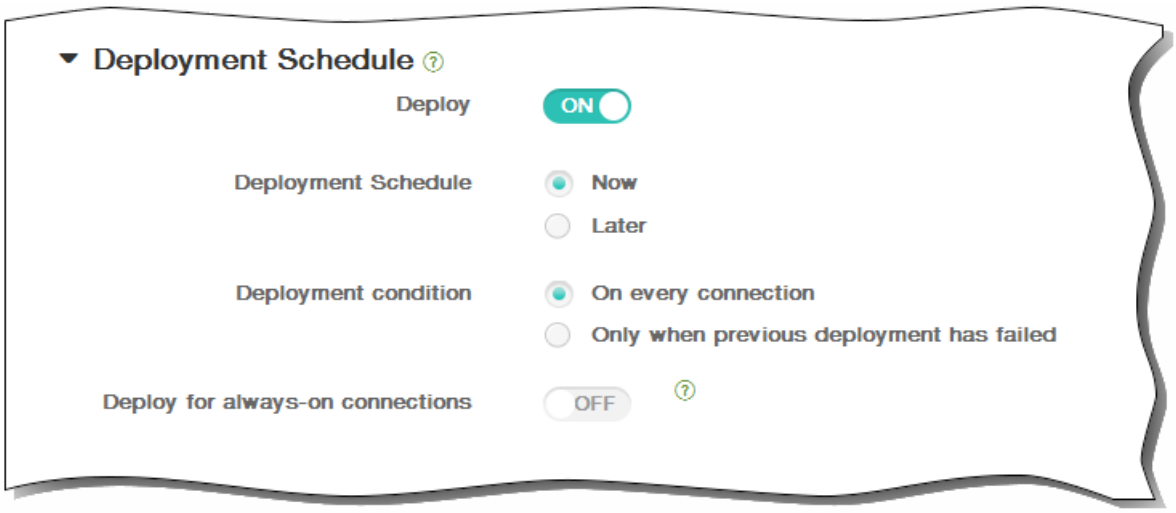
2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
   您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。

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

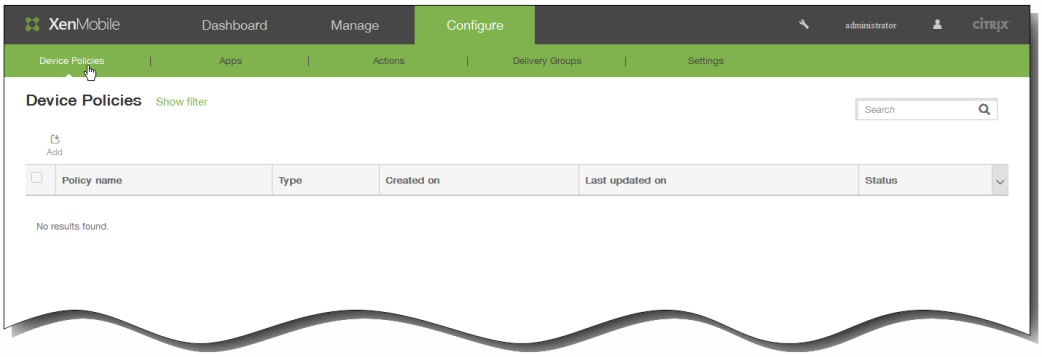
Oct 22, 2015

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。

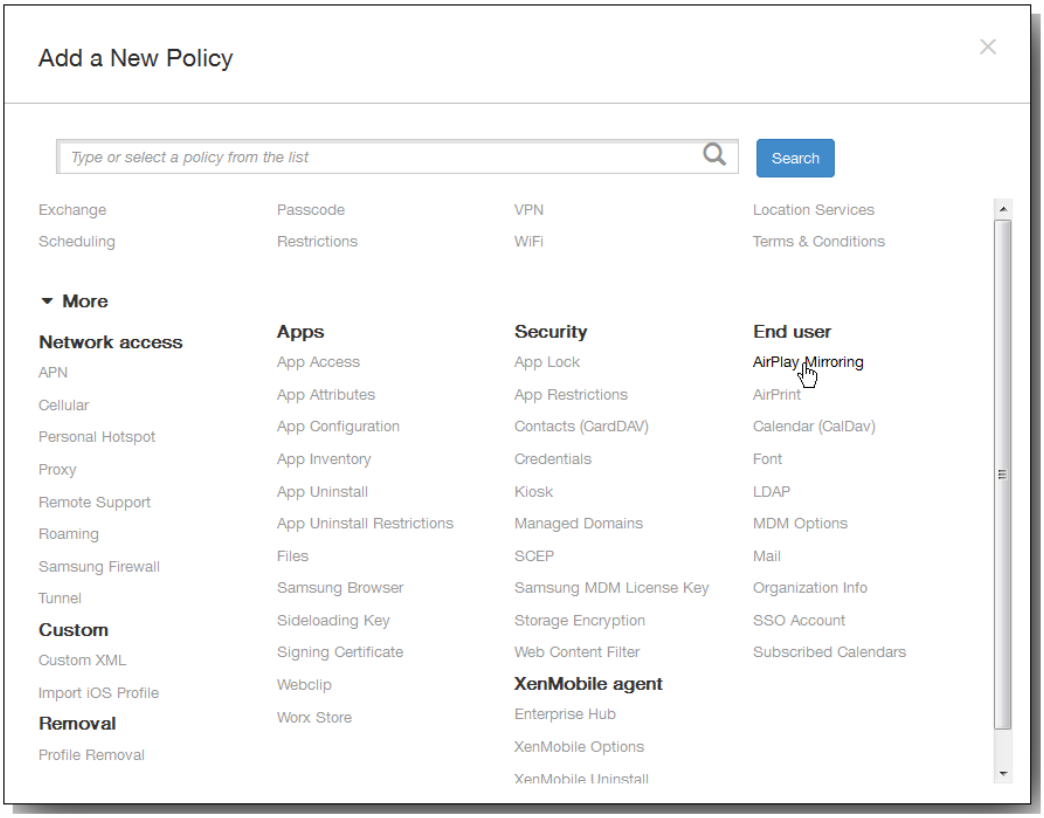
您可以在 XenMobile 中添加一个设备策略，从而将特定 AirPlay 设备（如 Apple 电视或其他 Mac 计算机）添加到用户的 iOS 设备。您还可以将设备添加到受监督设备的白名单，从而使用户仅限于白名单上的 AirPlay 设备。有关将设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

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。

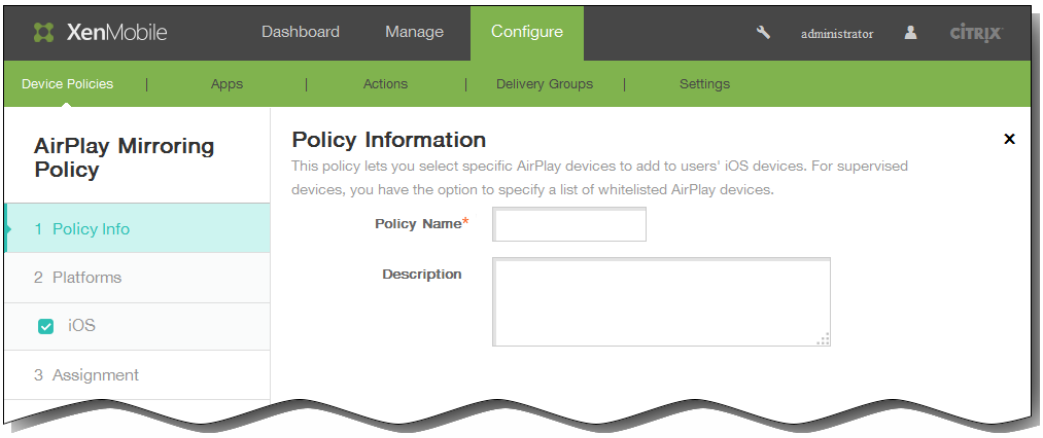
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



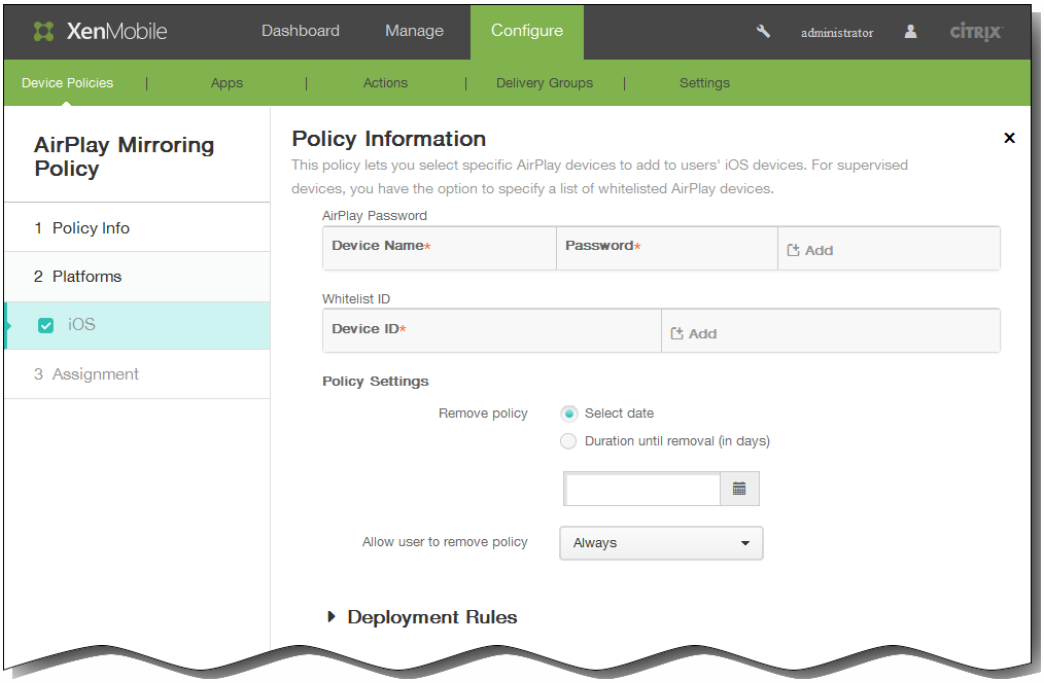
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。



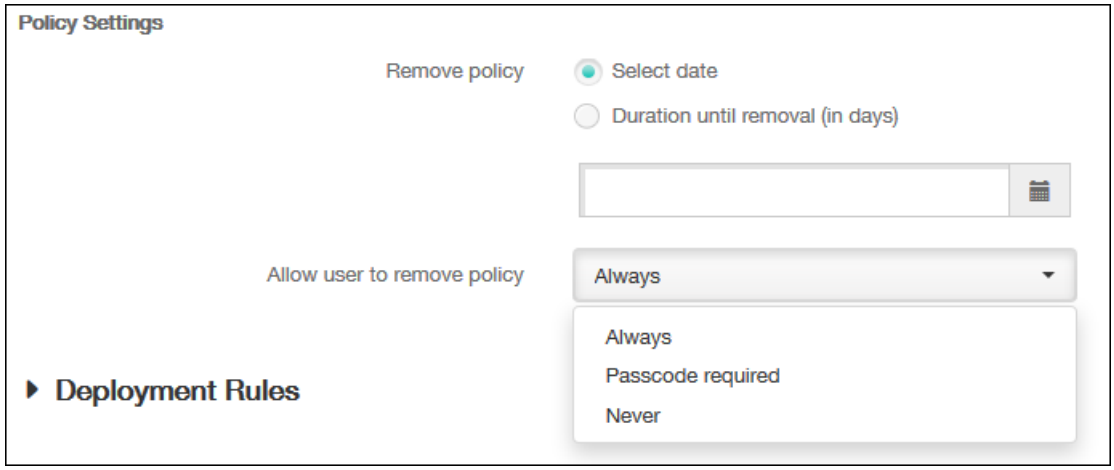
6. 在 iOS 平台信息页面上，输入以下信息：
   1. AirPlay 密码：单击添加，然后执行以下操作：
      1. 设备 ID：以 xx:xx:xx:xx:xx:xx 格式输入设备 ID。此字段不区分大小写。
      2. 密码：输入设备的可选密码。
      3. 单击添加以添加设备，或单击取消以取消添加设备。

4. 为要添加的每个设备重复步骤 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. 为要添加到白名单的每个设备重复步骤 i.和 ii.。

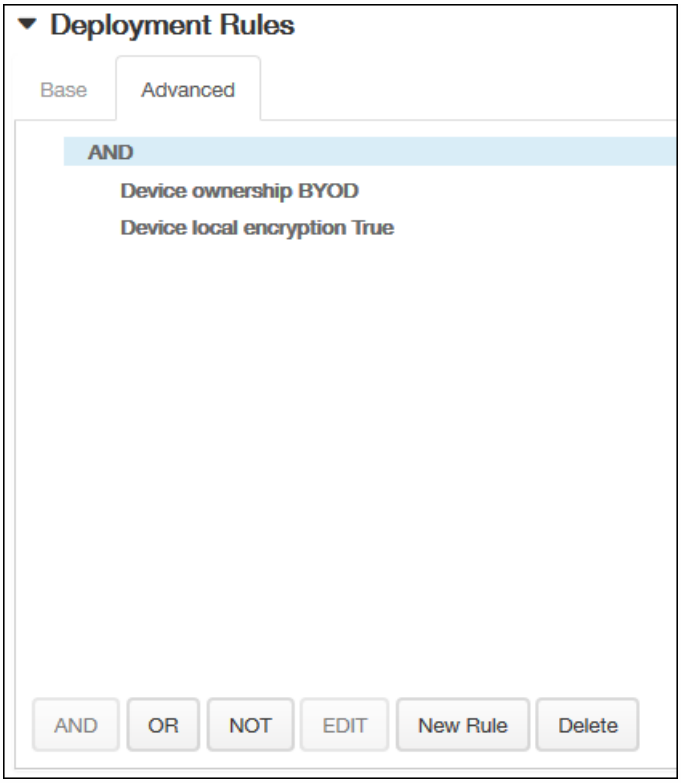
   注意：要删除现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击删除以删除列表，或单击取消以保留此列表。
   要编辑现有设备，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

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。



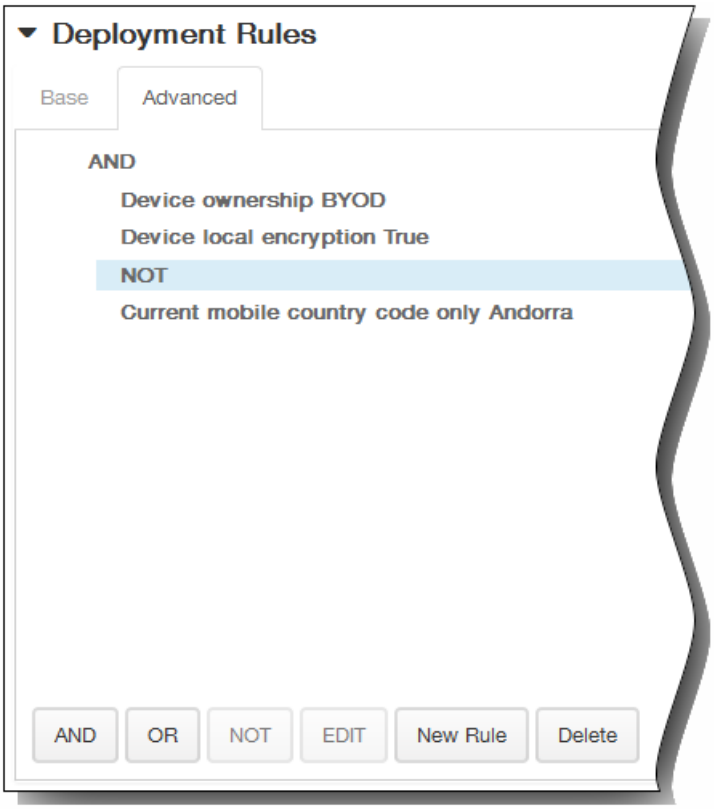
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

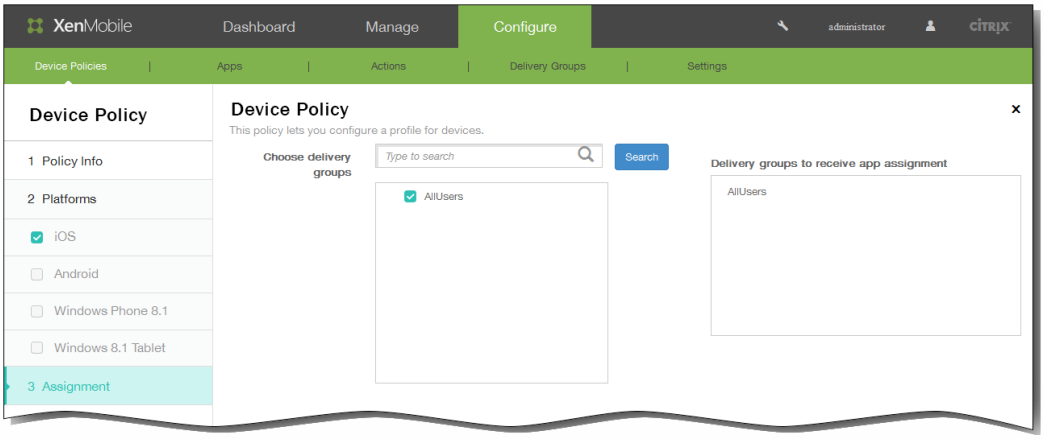


将显示您在基础选项卡上选择的条件。

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。



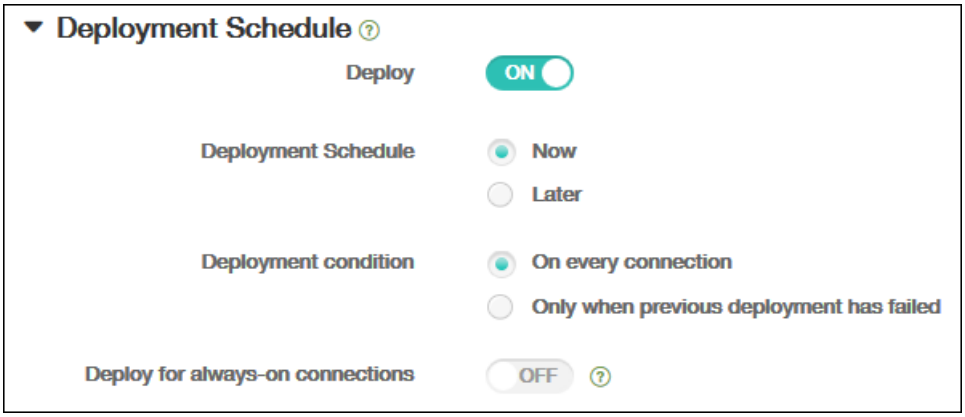
12. 单击下一步。 此时将显示 AirPlay 镜像策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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

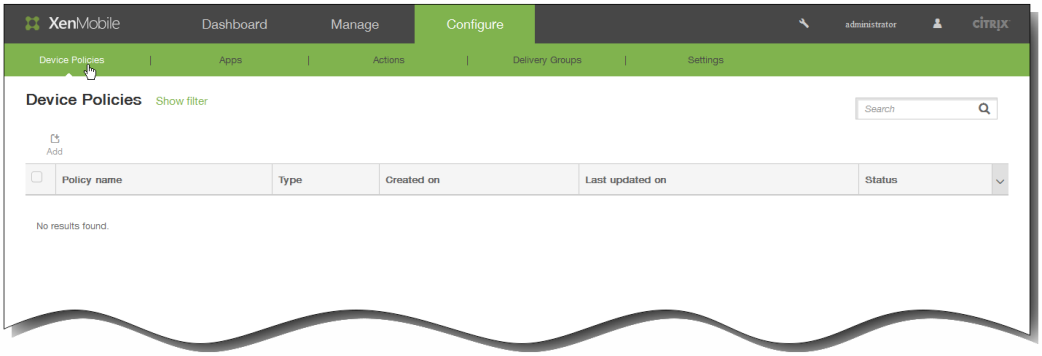
Oct 22, 2015

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。

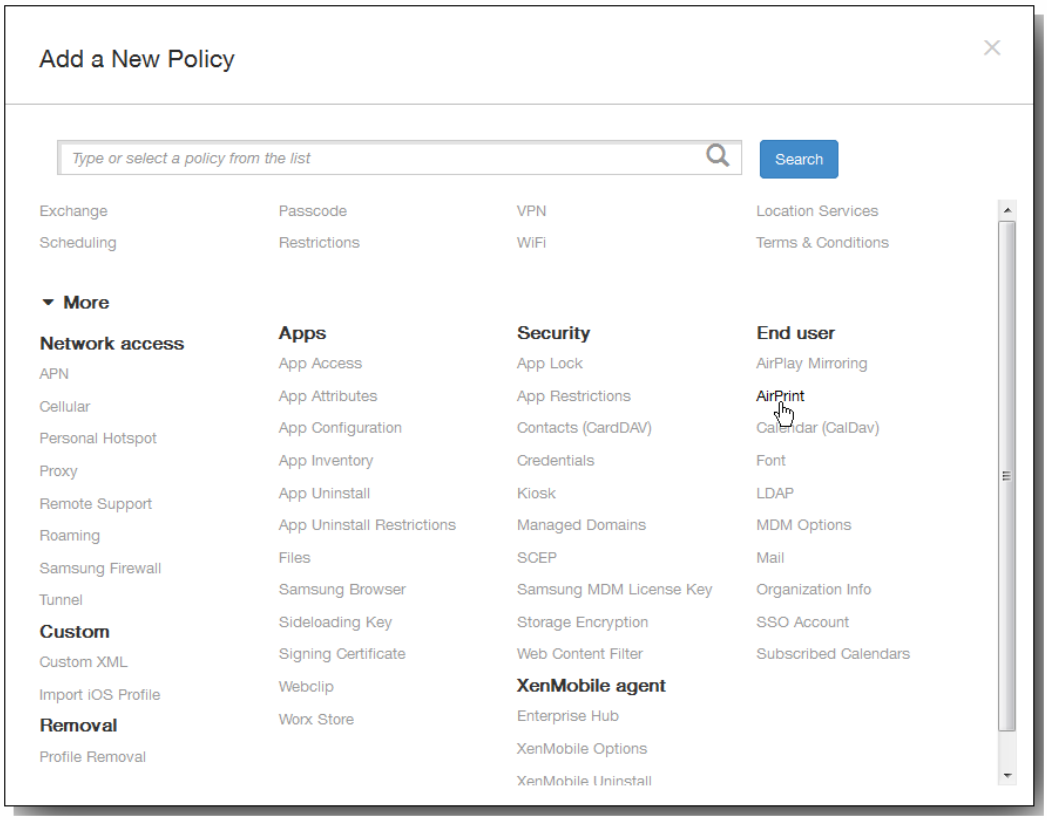
注意：

- 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。

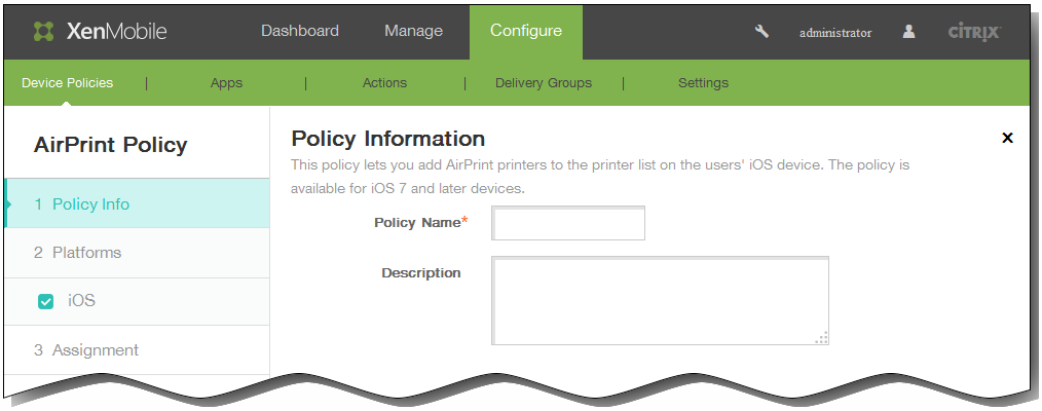
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



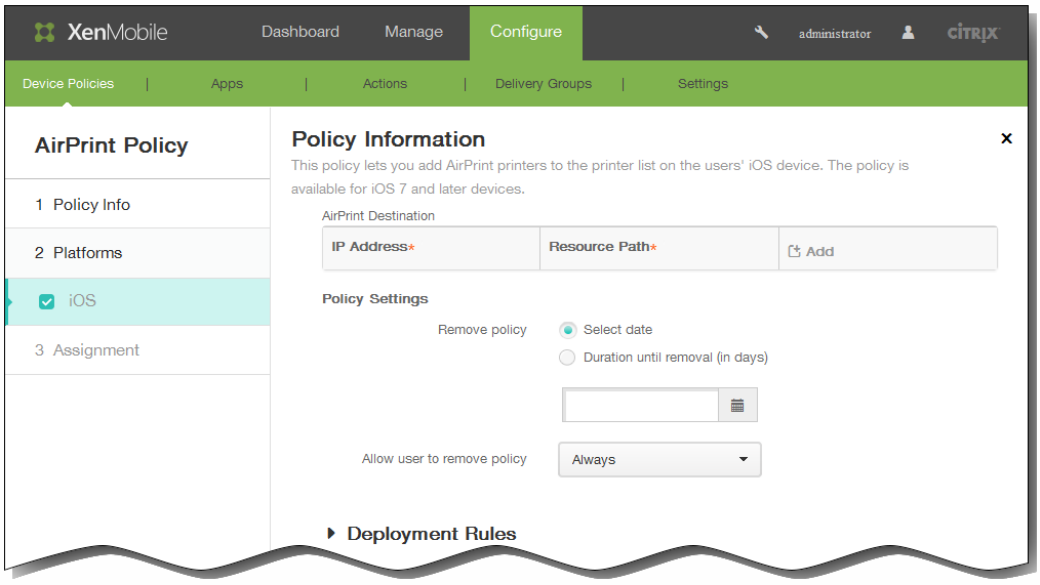
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。



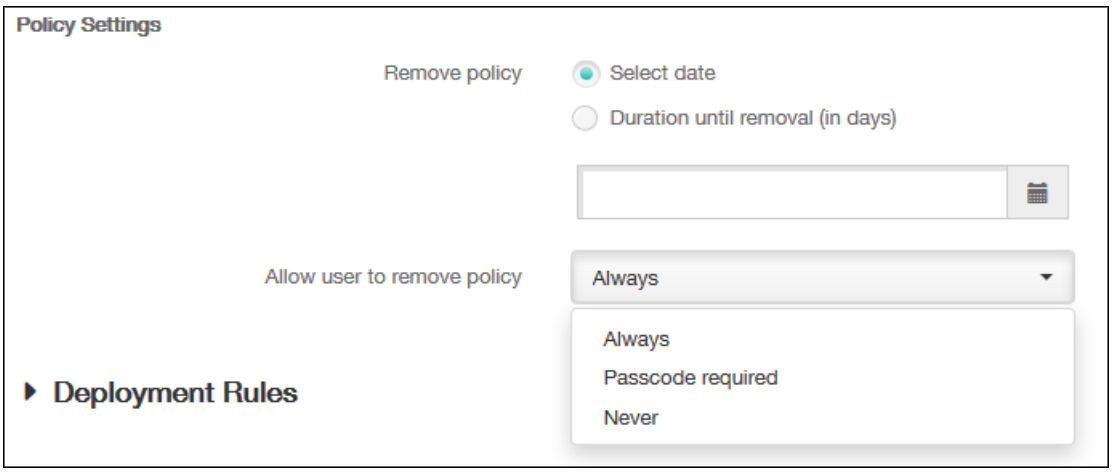
6. 在 iOS 平台信息页面上，输入以下信息：
   1. AirPrint 目标：单击添加，然后执行以下操作：
      1. IP 地址：输入 AirPrint 打印机 IP 地址。
      2. 资源路径：输入与打印机关联的资源路径。此值与 _ipps.tcp Bonjour 记录的参数相对应。例如，printers/Canon_MG5300_series 或 printers/Xerox_Phaser_7600。
      3. 单击添加以添加打印机，或单击取消以取消添加打印机。
      4. 为要添加的每个设备重复步骤 i.至步骤 iii.。

      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

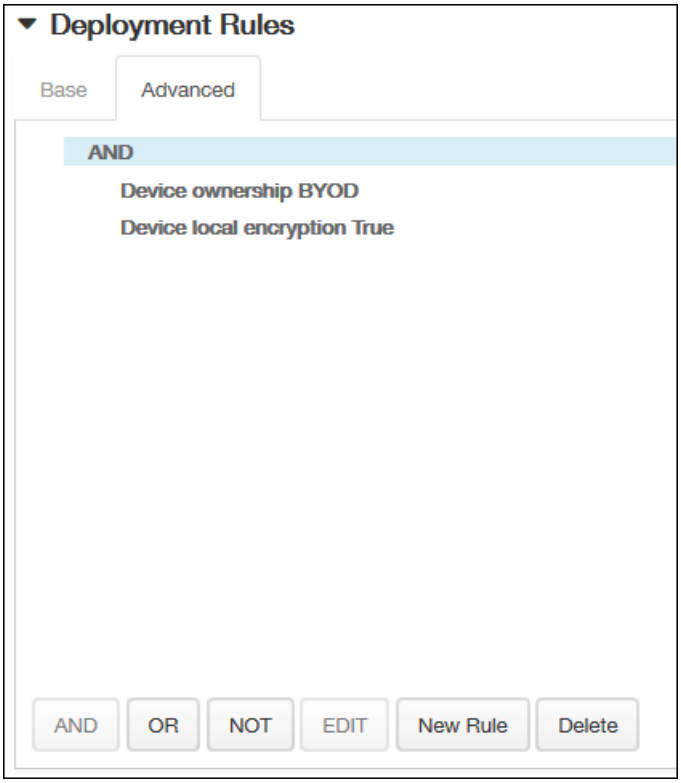
改的列表，或单击取消以保持列表不更改。

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。



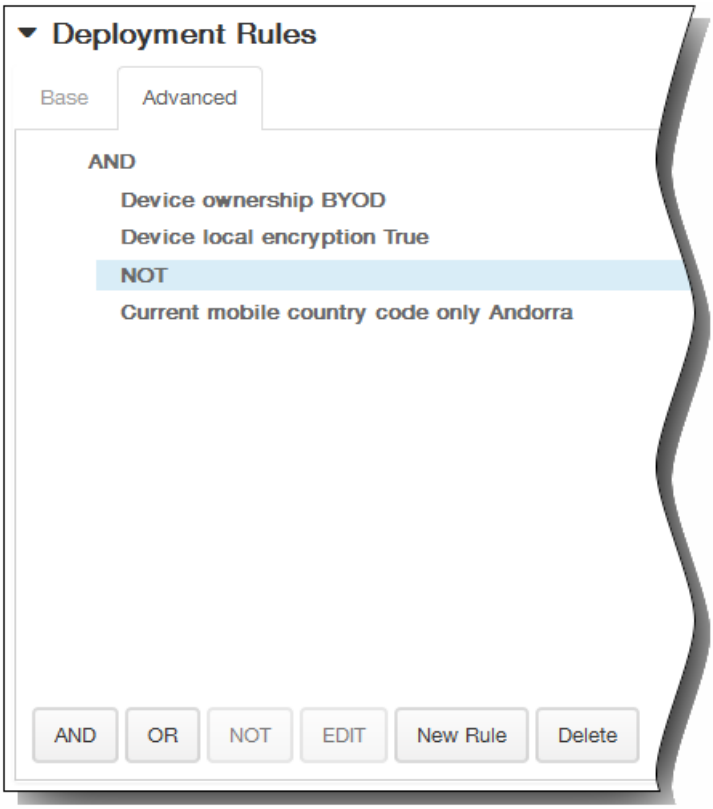
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

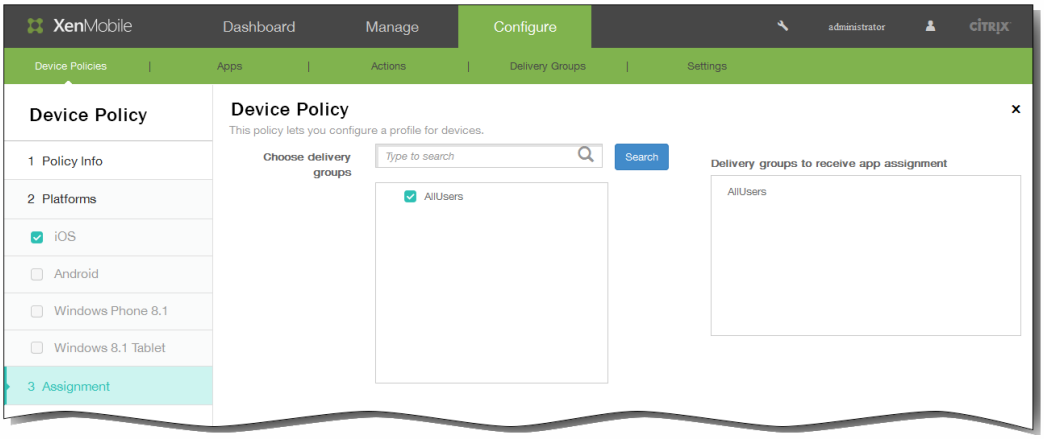


将显示您在基础选项卡上选择的条件。

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。



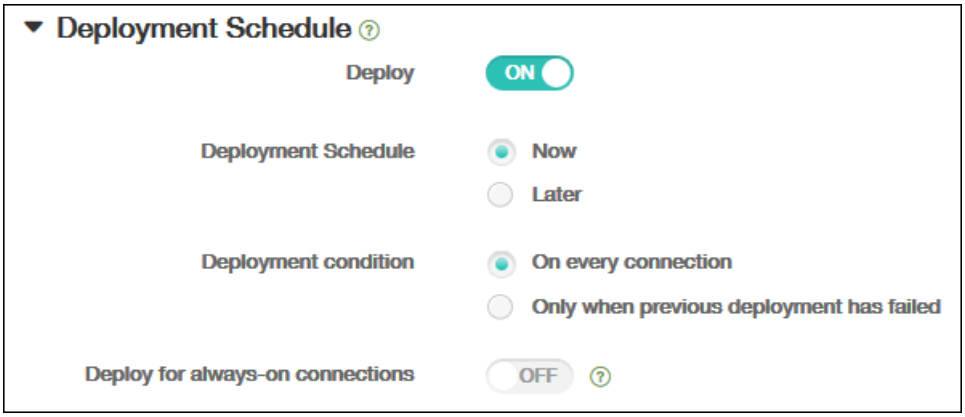
12. 单击下一步。 此时将显示 AirPrint 策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。



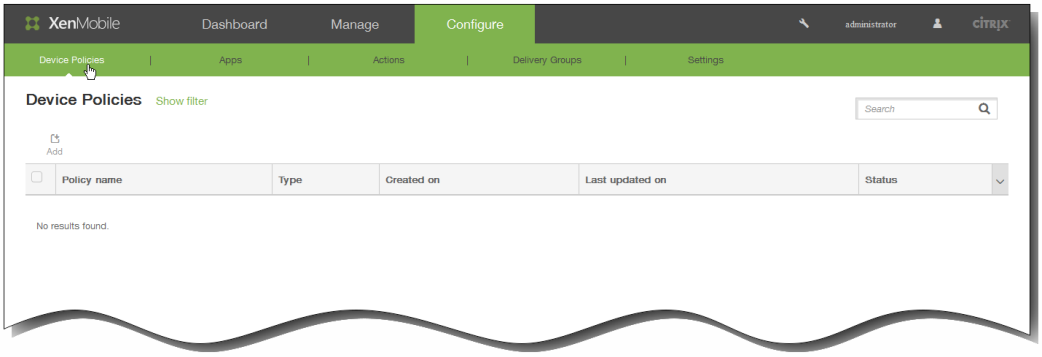
15. 单击保存以保存此策略。

添加适用于 iOS 的日历 (CalDav) 设备策略

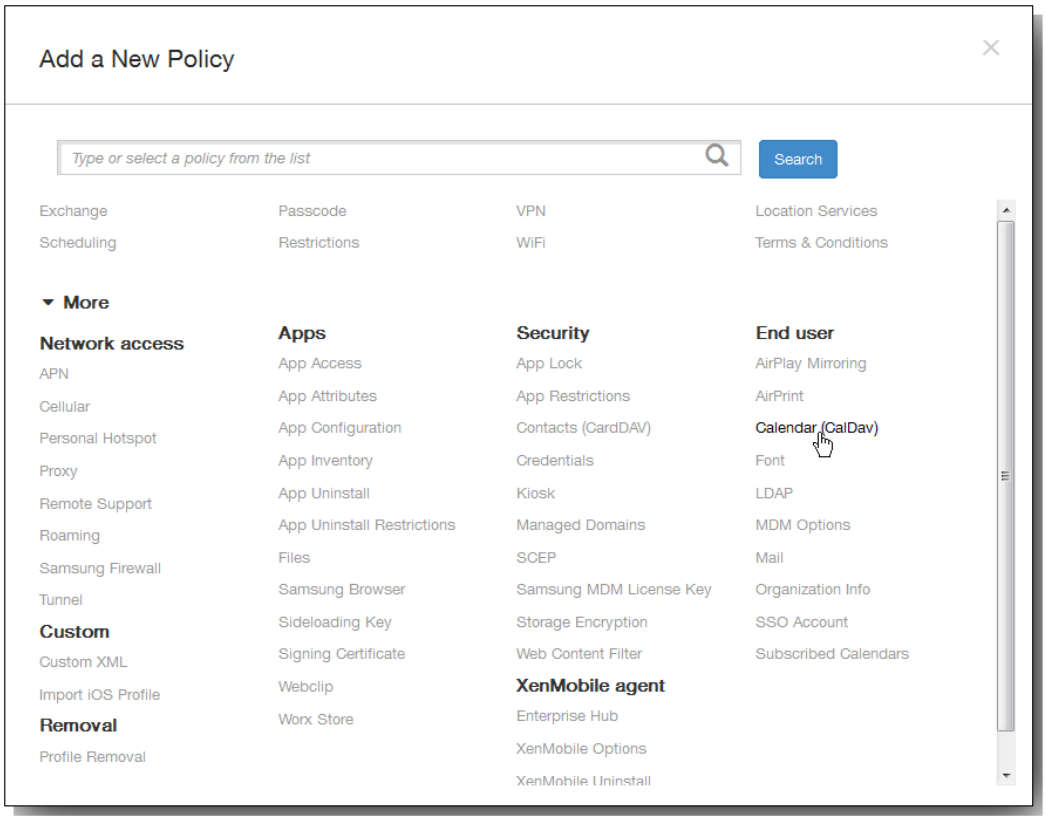
Oct 22, 2015

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。

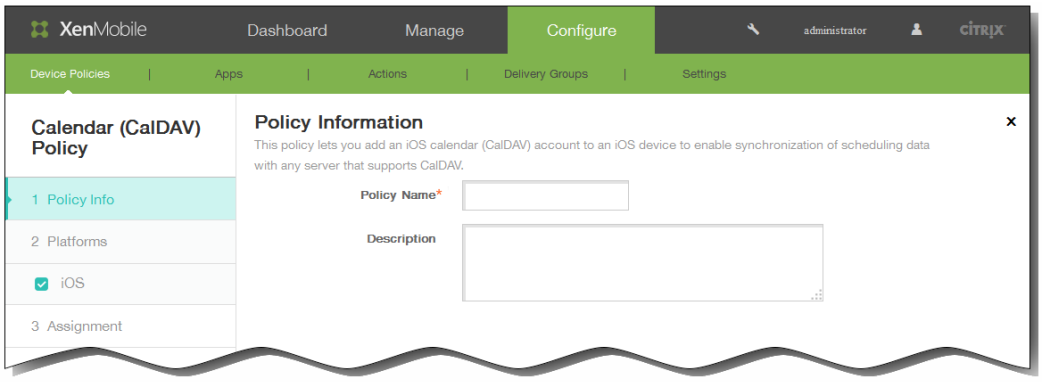
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



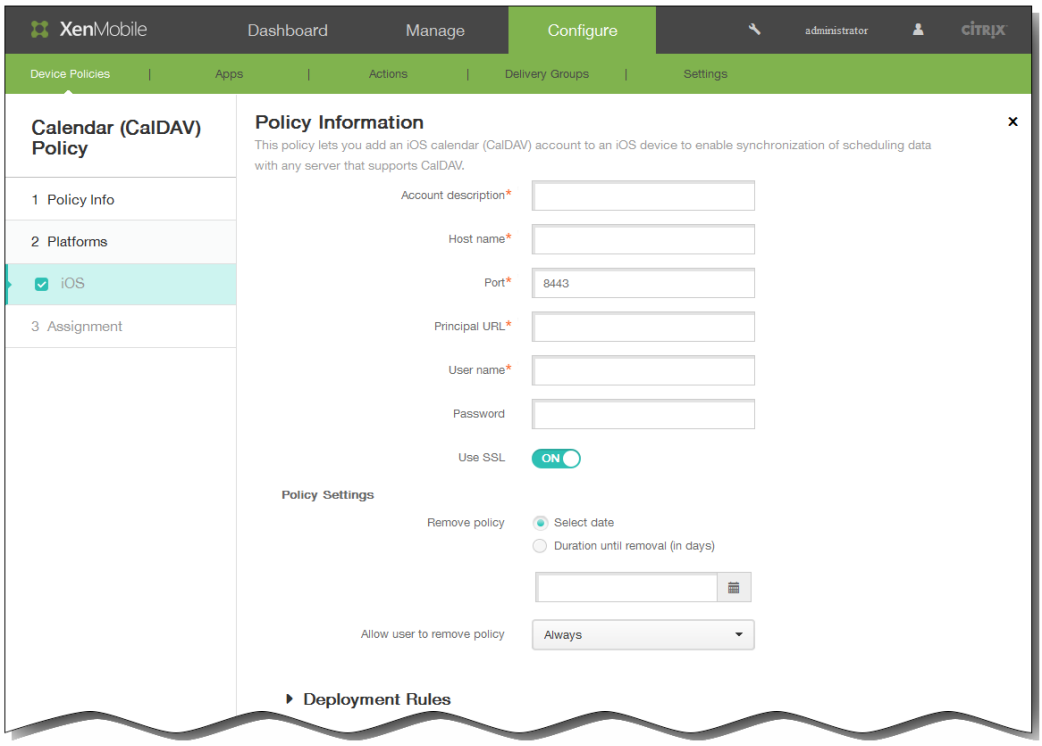
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。

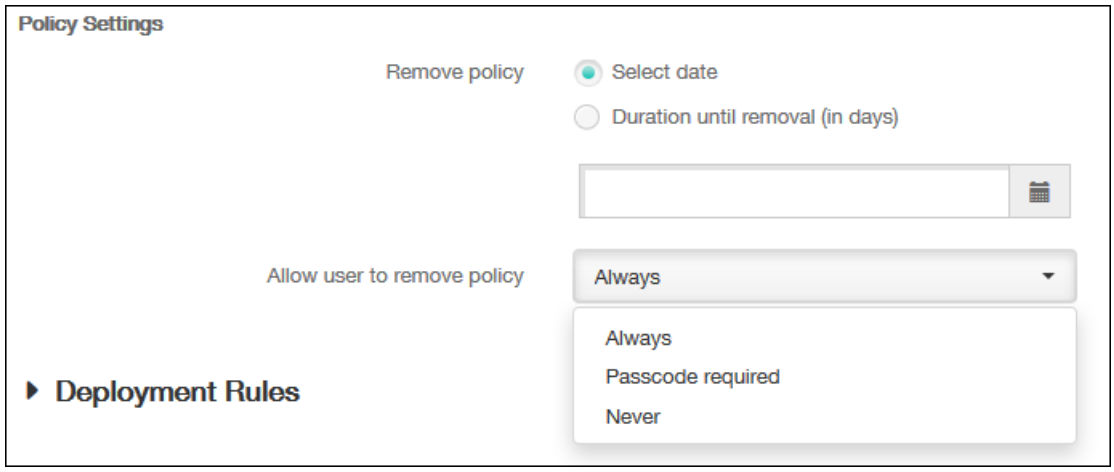


4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。



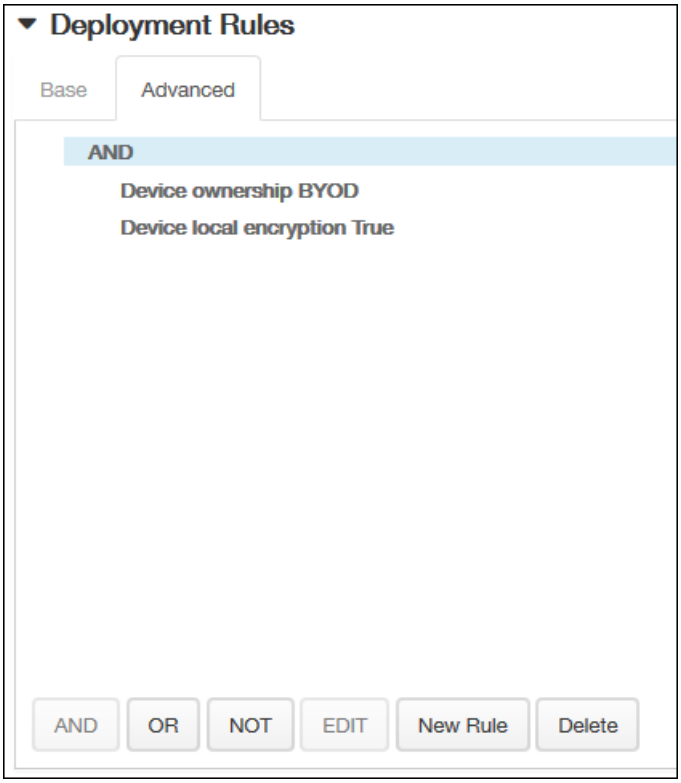
6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户说明：键入帐户说明。 此字段为必填字段。
   2. 主机名：键入 CalDAV 服务器的地址。 此字段为必填字段。
   3. 端口：键入连接到 CalDAV 服务器使用的端口。 此字段为必填字段。 默认值为 8443。
   4. 主体 URL：键入用户日历的基本 URL。
   5. 用户名：键入用户的登录名称。 此字段为必填字段。
   6. 密码：键入可选用户密码。
   7. 使用 SSL：选择是否使用安全套接字层连接到 CalDAV 服务器。 默认值为开。
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留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



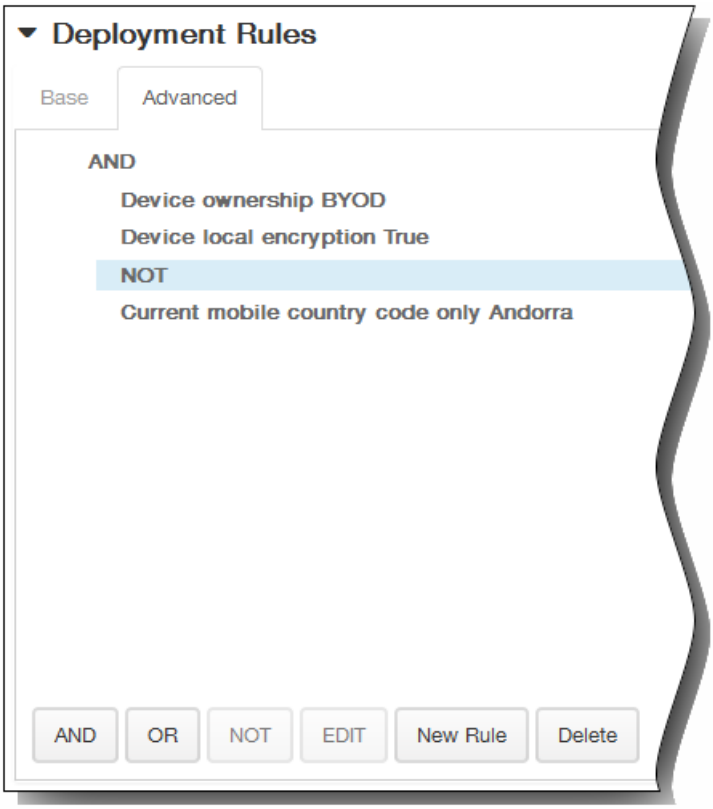
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

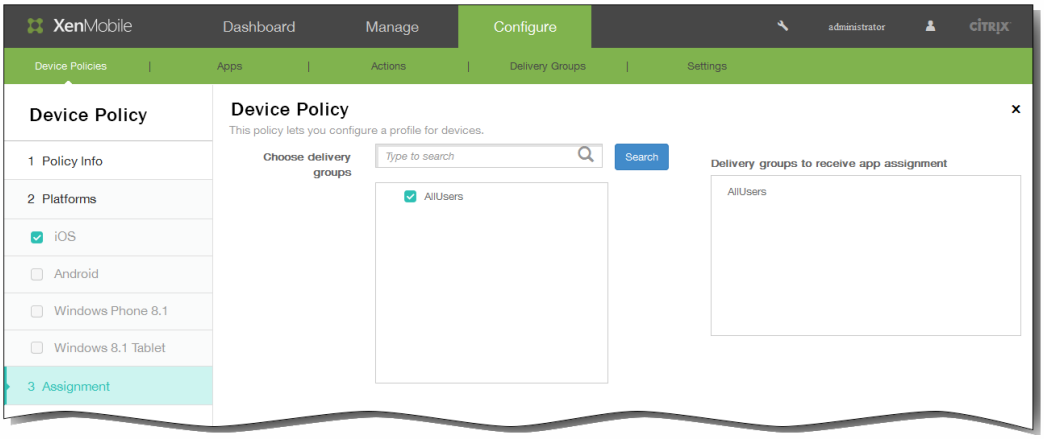


将显示您在基础选项卡上选择的条件。

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。



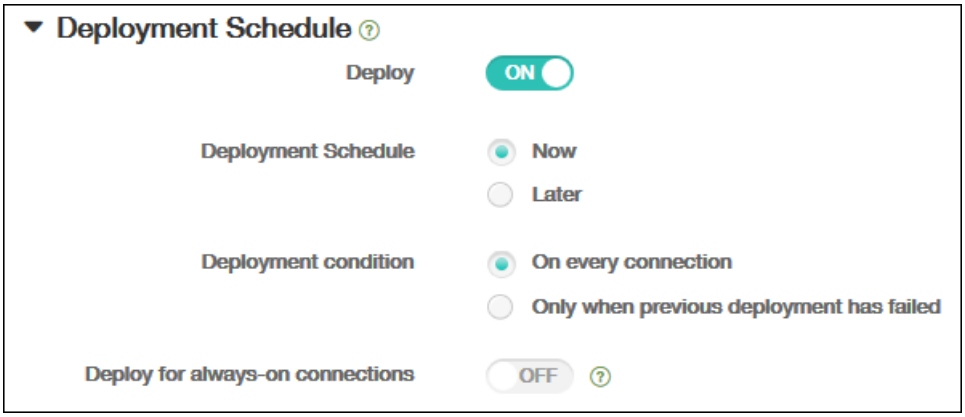
12. 单击下一步。 此时将显示日历(CalDAV)策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。



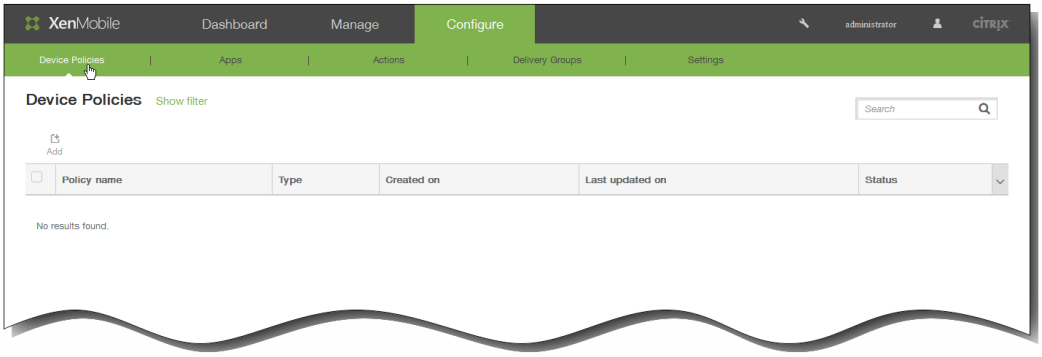
15. 单击保存以保存此策略。

添加适用于 iOS 的联系人 (CardDAV) 设备策略

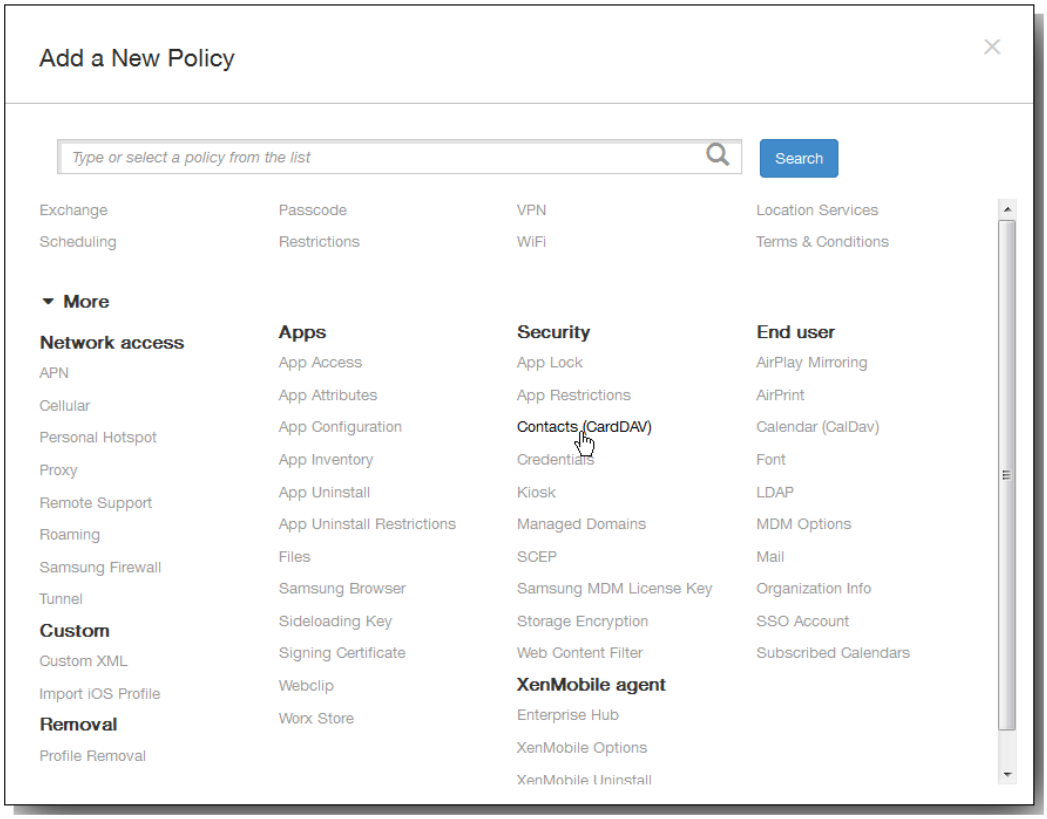
Oct 22, 2015

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。

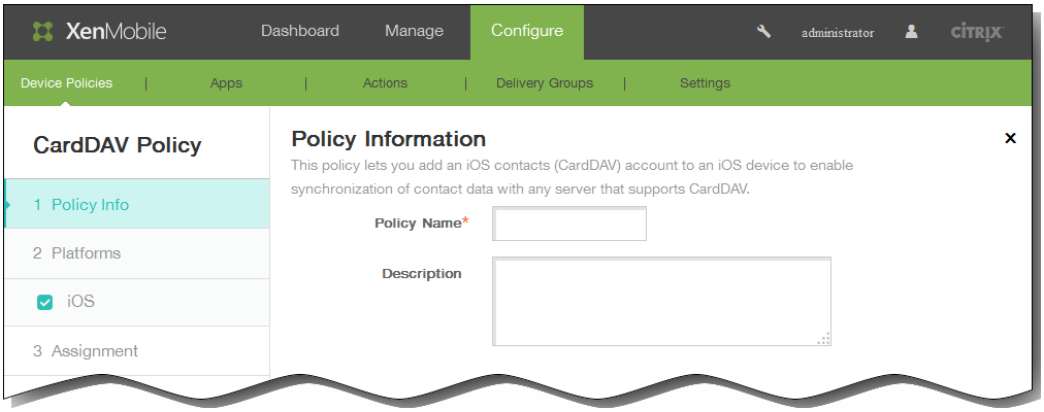
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



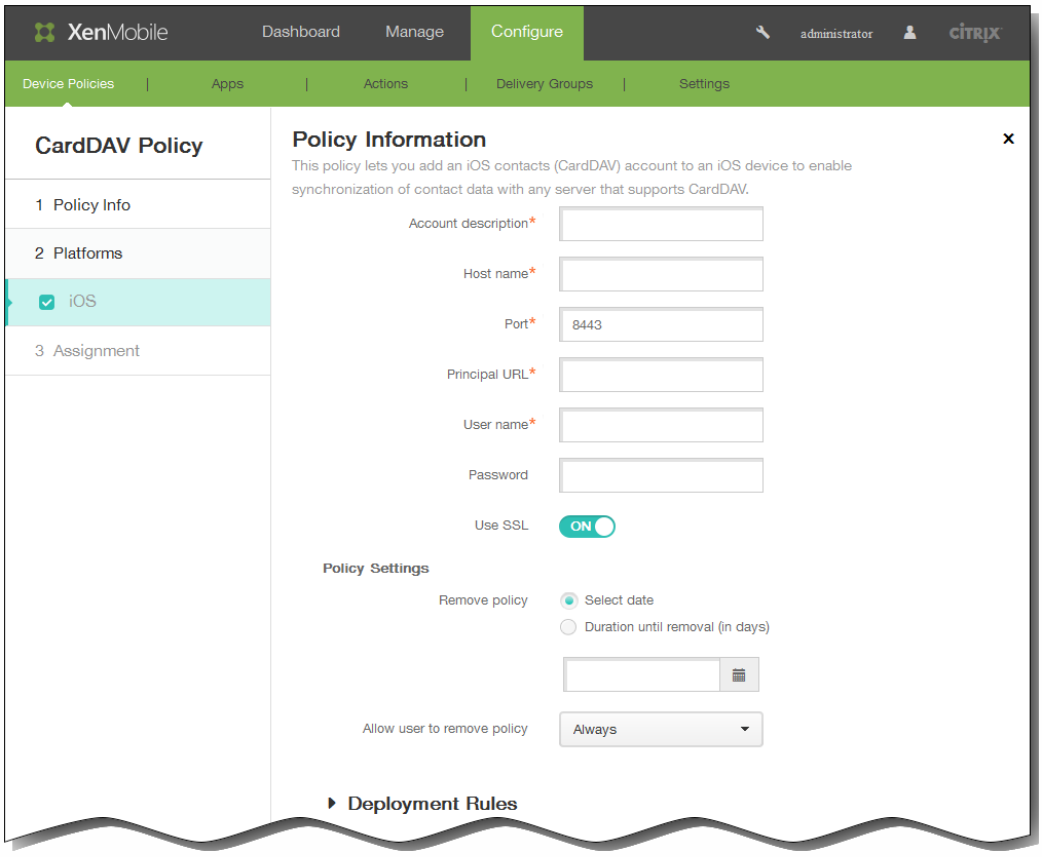
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。



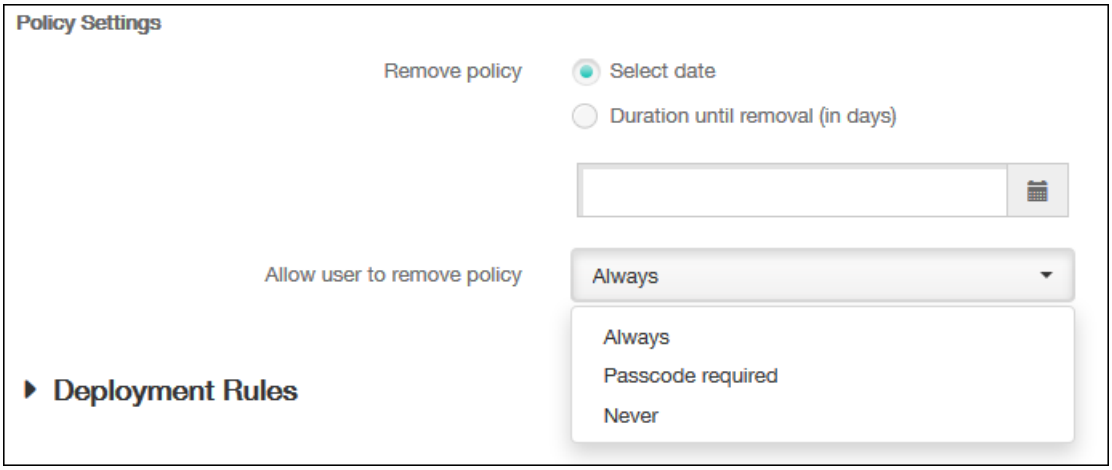
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：（可选）键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。



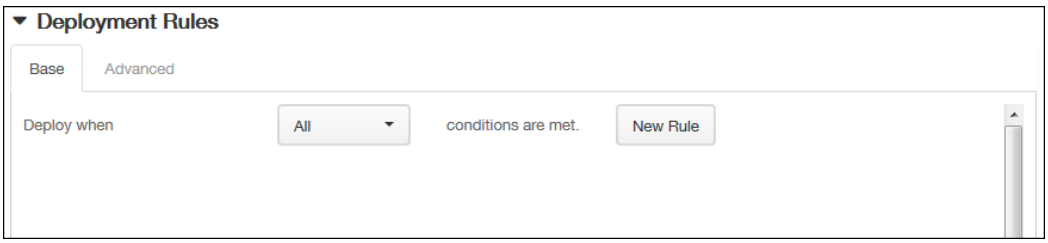
6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户说明：输入帐户说明。 此字段为必填字段。
   2. 主机名：输入 CardDAV 服务器的地址。 此字段为必填字段。
   3. 端口：输入连接到 CardDAV 服务器使用的端口。 此字段为必填字段。 默认值为 8443。
   4. 主体 URL：输入用户日历的基本 URL。
   5. 用户名：输入用户的登录名称。 此字段为必填字段。

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。

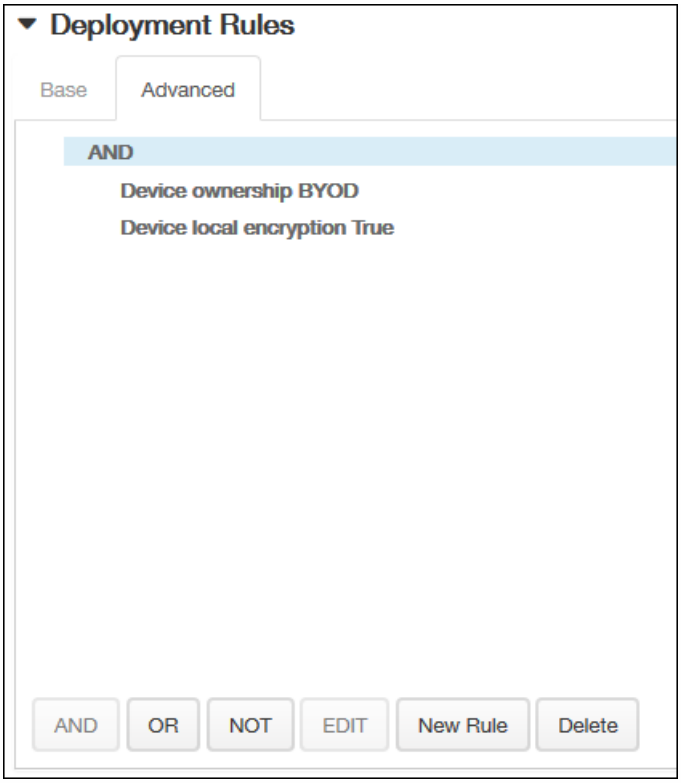
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



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。

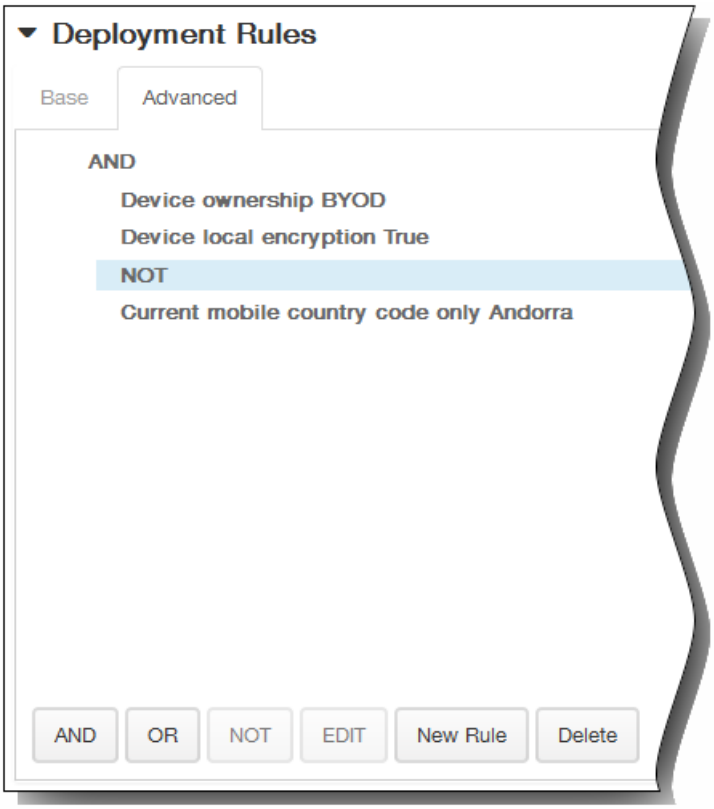


1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

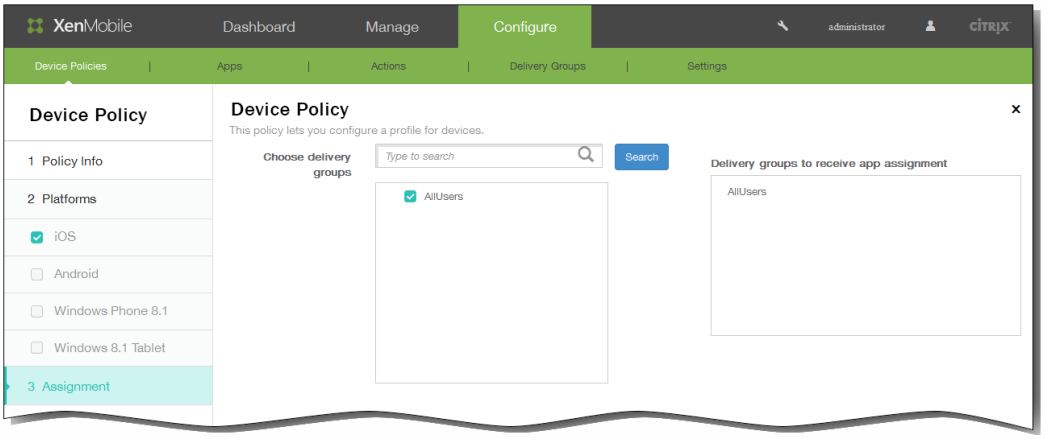


将显示您在基础选项卡上选择的条件。

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。



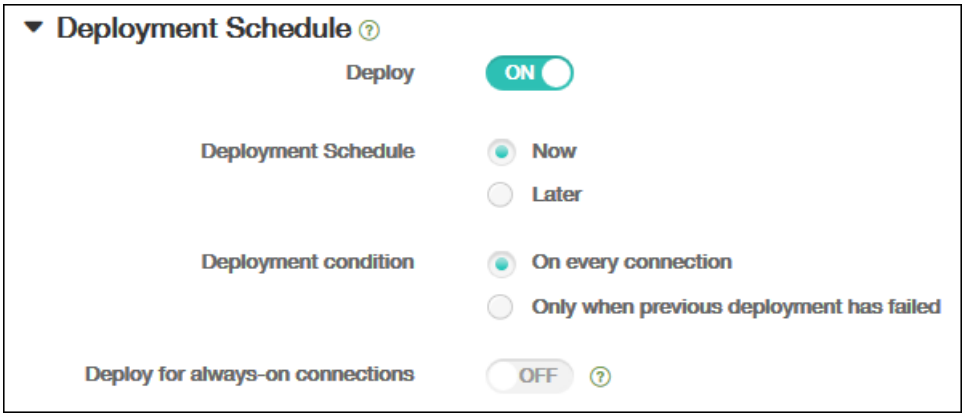
12. 单击下一步。 此时将显示 CardDAV 策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

添加适用于 iOS 的置备配置文件设备策略

Oct 22, 2015

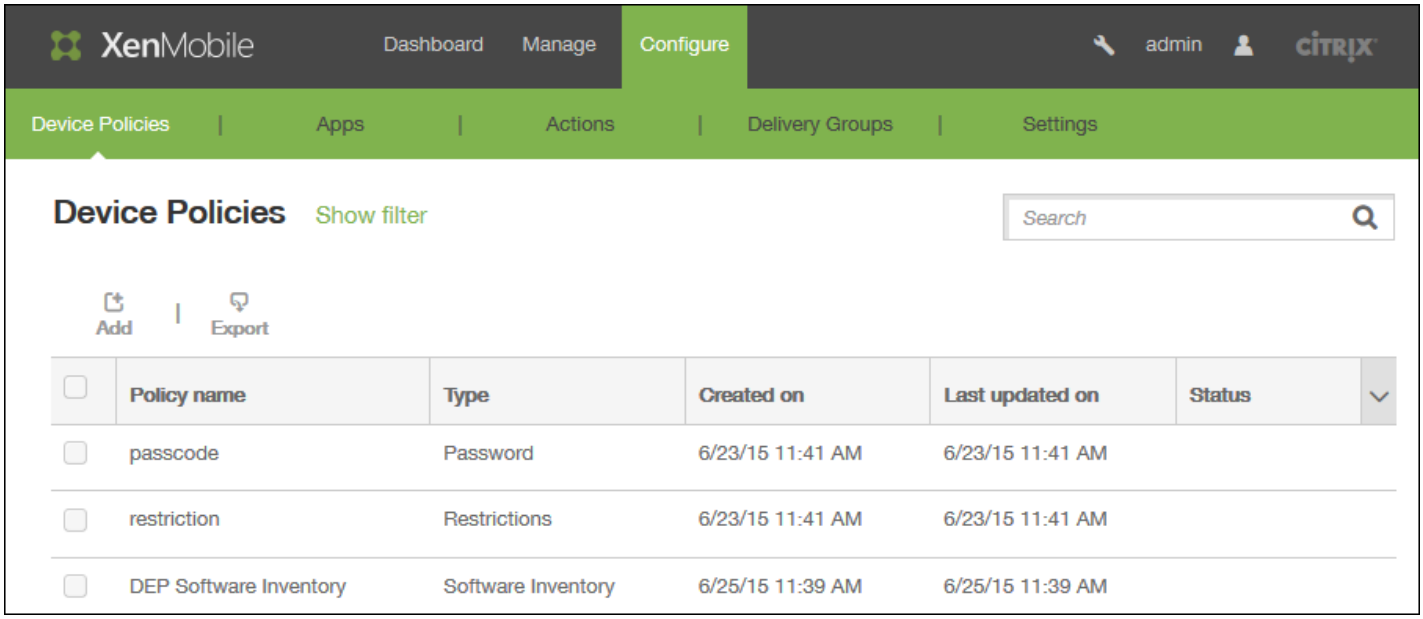
开发或代码签名 iOS 企业应用程序时，通常包含企业分发置备配置文件，Apple 需要此配置文件才能允许应用程序在 iOS 设备上运行。如果置备配置文件缺失或已过期，用户轻按应用程序以将其打开时，应用程序将崩溃。

置备配置文件的主要问题是，它们在 Apple 开发人员门户上生成一年之后将过期，您必须跟踪用户注册的所有 iOS 设备上的所有置备配置文件的过期日期。跟踪过期日期不仅涉及到跟踪实际的过期日期，还要跟踪每个用户正在使用的应用程序版本。有两个解决方案：通过电子邮件向用户发送置备配置文件，或者将其放在 Web 门户上供下载和安装。这些解决方案可行，但容易出错，因为需要用户响应电子邮件中的说明，或访问 Web 门户并下载正确的配置文件，然后再进行安装。

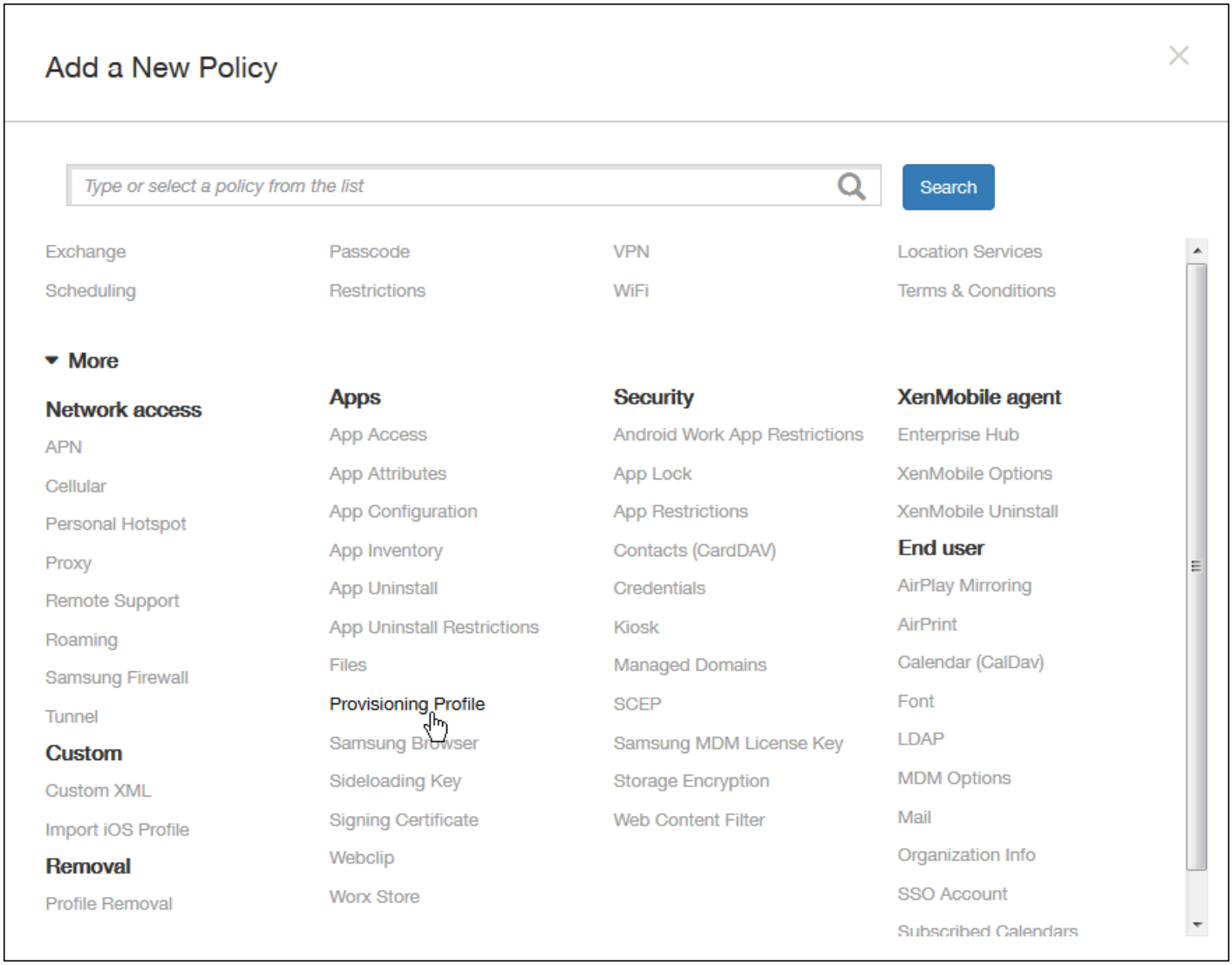
要使此过程对用户透明，您可以在 XenMobile 使用设备策略来安装和删除置备配置文件。在必要时删除缺失或过期的置备配置文件并在用户设备上安装最新的配置文件，这样一来，只需轻按应用程序，即可将其打开并使用。

创建置备配置文件策略之前，必须创建置备配置文件。有关详细信息，请参阅 Apple 开发人员站点上的 Creating Provisioning Profiles（创建置备配置文件）。

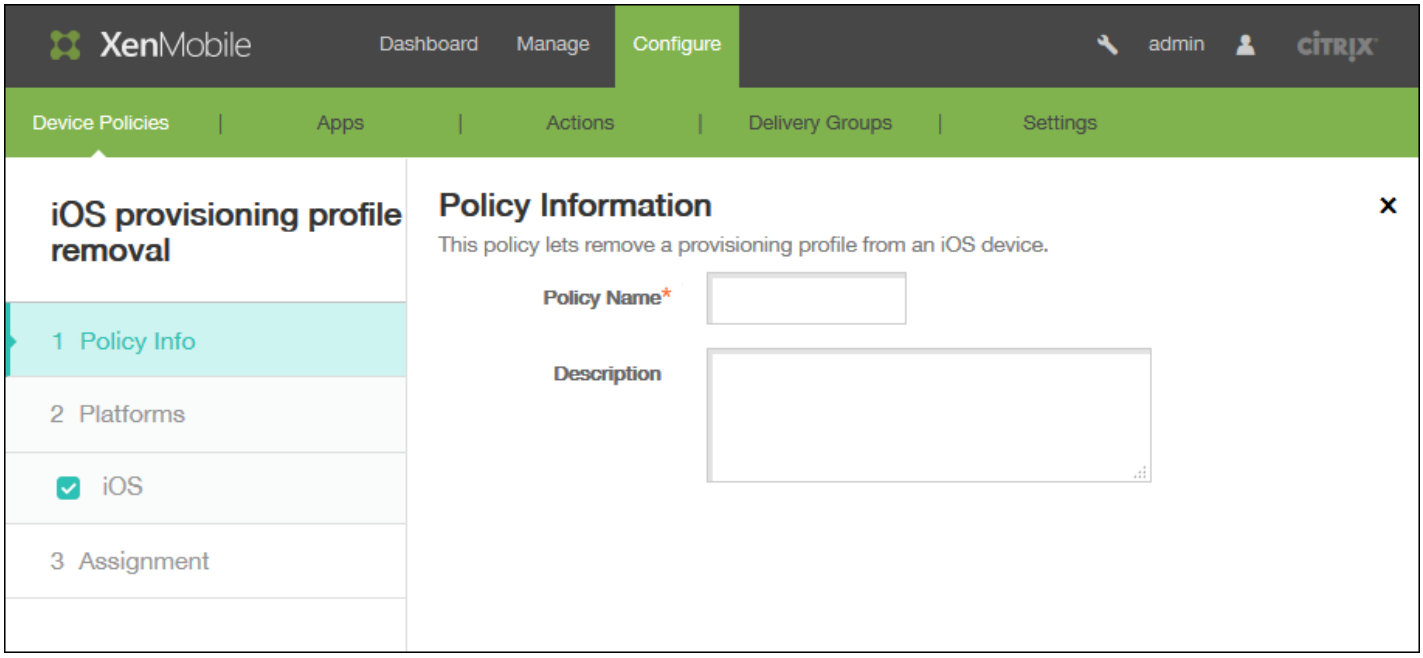
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。



2. 单击**添加**添加新策略。将显示**添加新策略**页面。



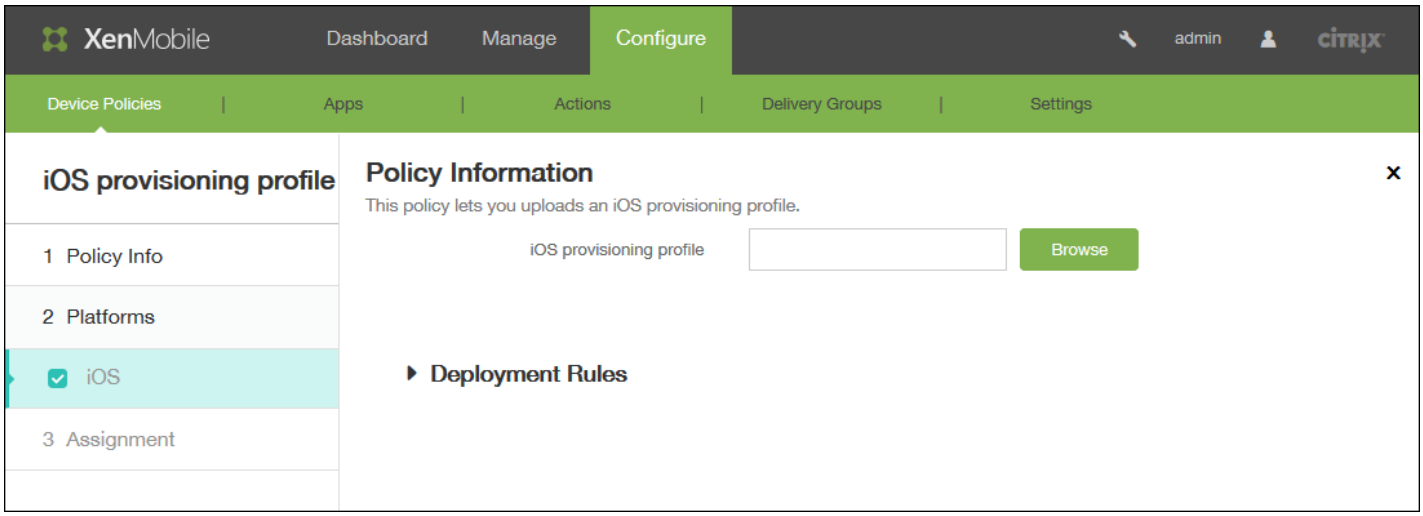
3. 在**添加新策略**页面上，单击**更多**，然后在**应用程序**下方，单击**置备配置文件**。此时将显示 **iOS 置备配置文件策略**信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。此时将显示 **iOS 平台信息**页面。



6. 在 **iOS 平台信息**页面，单击**浏览**，然后导航到要导入的置备配置文件所在的位置，选择此文件。

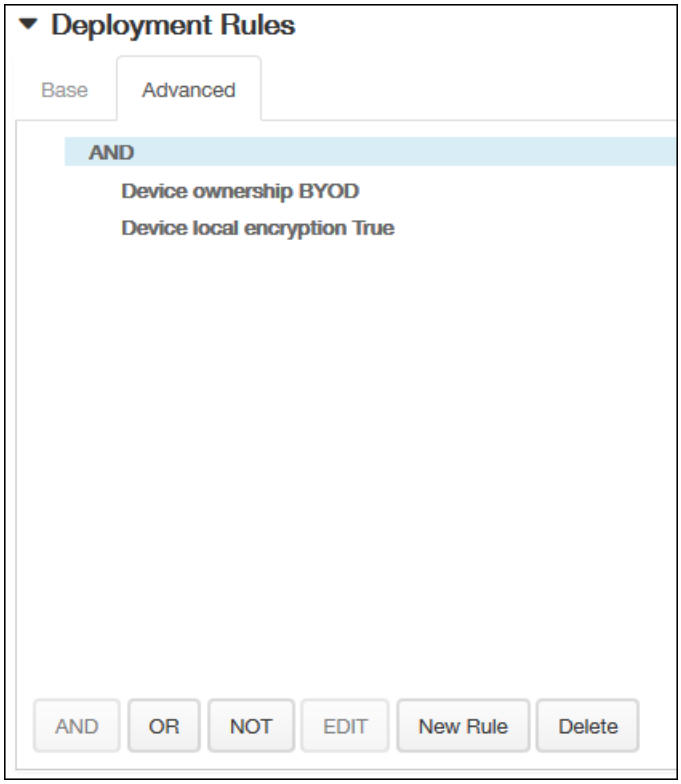
7. 展开**部署规则**，然后配置以下设置：

默认情况下将显示**基础**选项卡。

8. 在此列表中，单击选项以确定部署策略的时间。

- 可以选择在满足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**。
- 单击**新建规则**以定义条件。
- 在列表中，单击条件，如**设备所有权**和 BYOD，如上图所示。
- 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。

9. 单击**高级**选项卡以使用布尔选项组合规则。

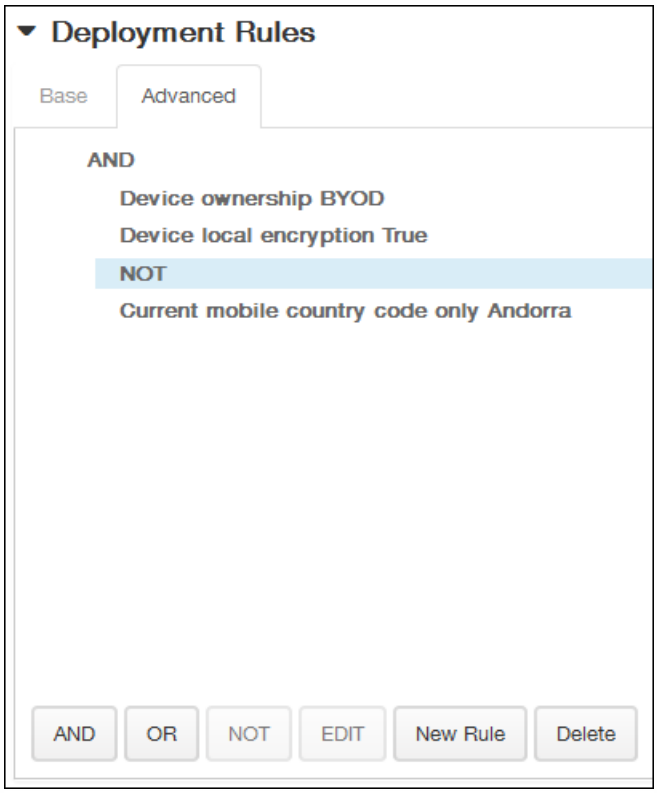


将显示您在**基础**选项卡上选择的条件。

10. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。

- 单击 AND、OR 或 NOT。
- 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。

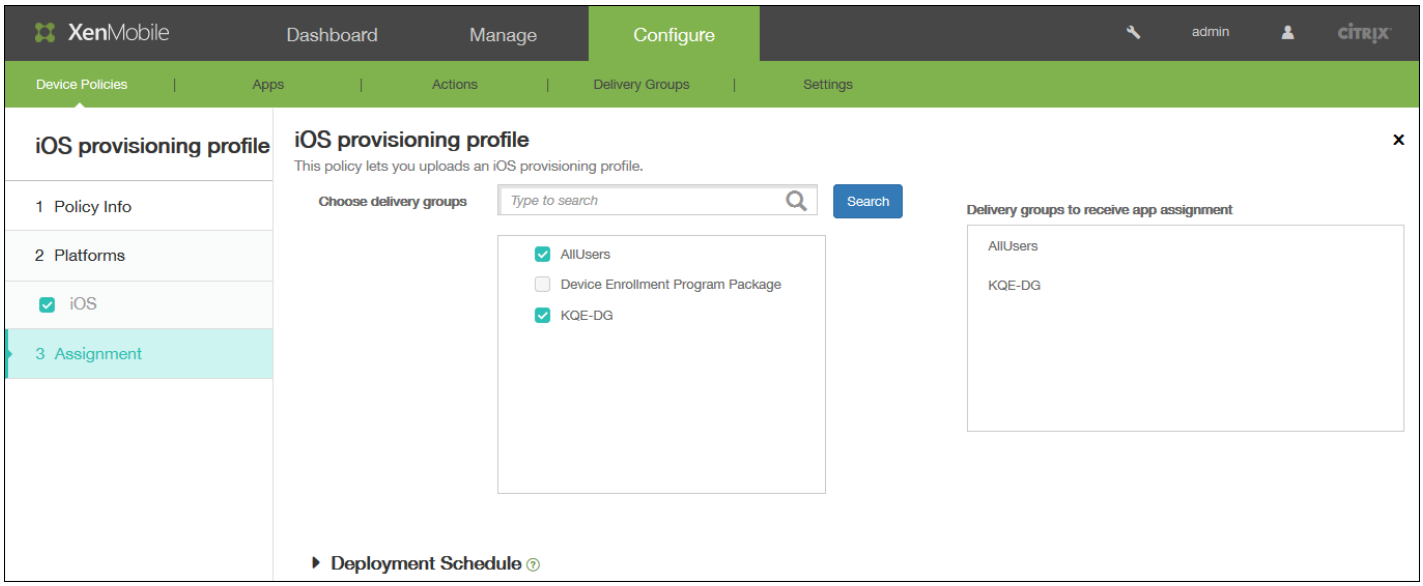
- 如果要添加更多条件，请再次单击**新建规则**。



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。

11. 单击**下一步**。此时将显示 **iOS 置备配置文件策略**分配页面。

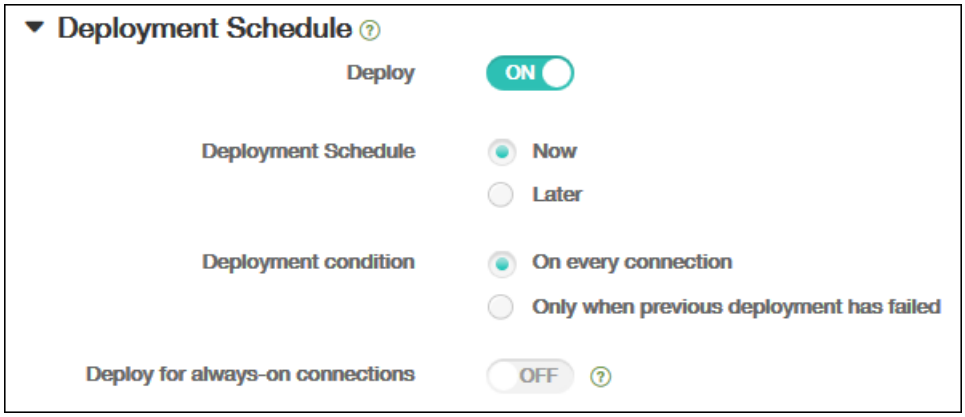
12. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。选择的组显示在**用于接收应用程序分配的交付组**列表中。



13. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。默认选项为**开**。如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。默认选项为**立即**。
- 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
- 在**部署条件**旁边，单击**每次连接时**或单击**仅当之前的部署失败时**。默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。默认选项为**关**。请注意，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。



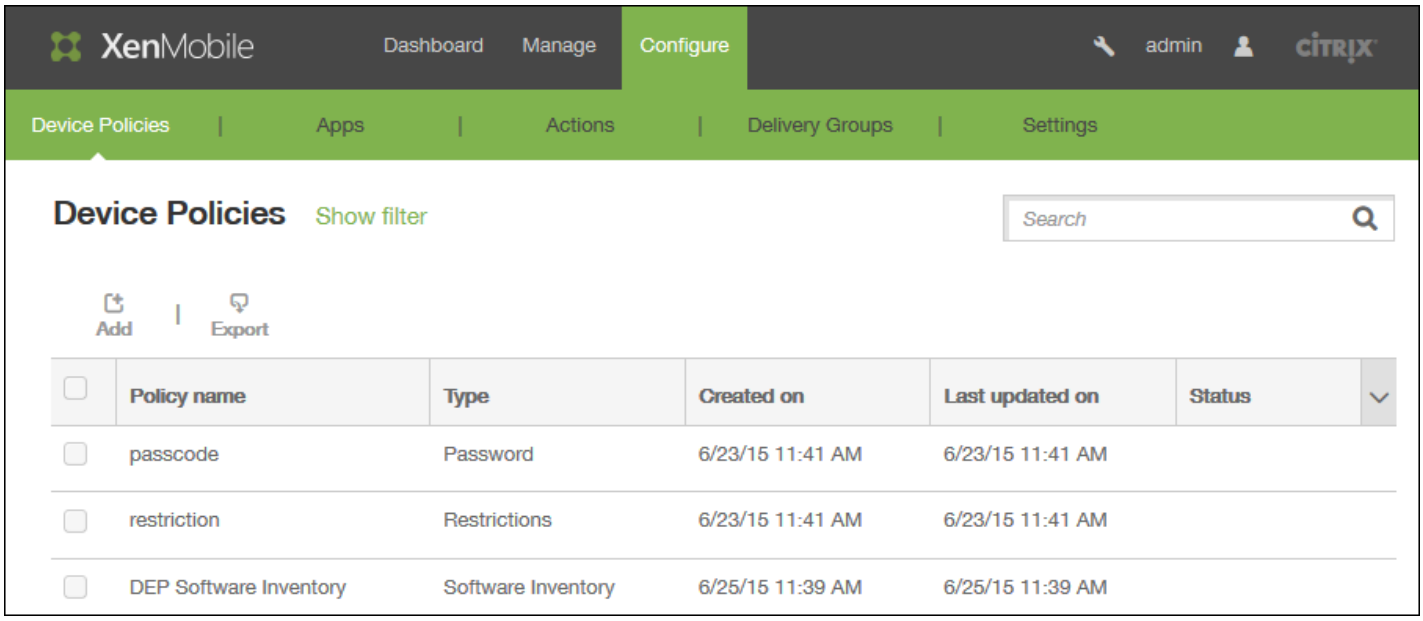
14. 单击**保存**以保存此策略。

添加适用于 iOS 的删除置备配置文件设备策略

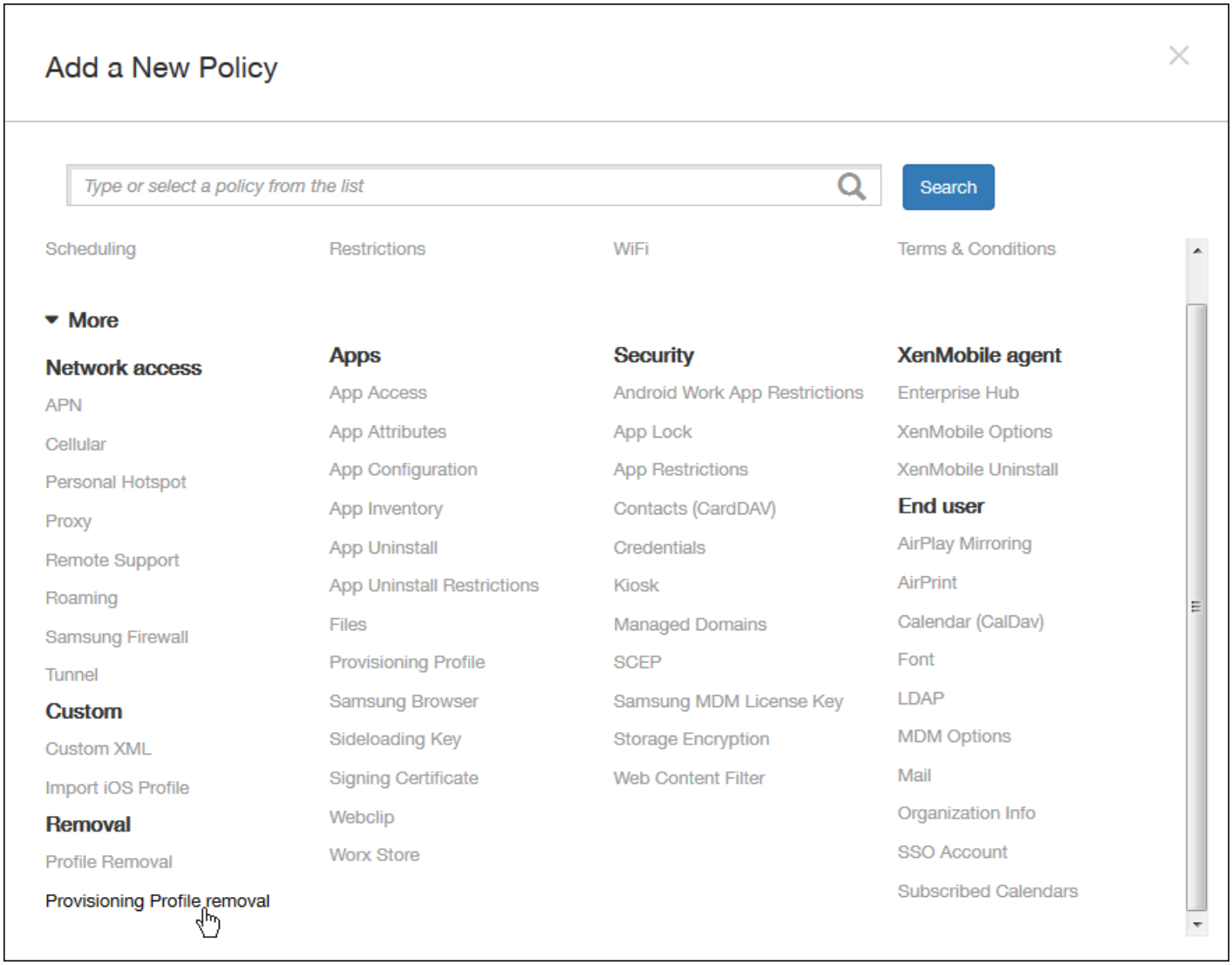
Oct 22, 2015

您可以通过设备策略删除 iOS 置备配置文件。有关置备配置文件的详细信息，请参阅添加置备配置文件。

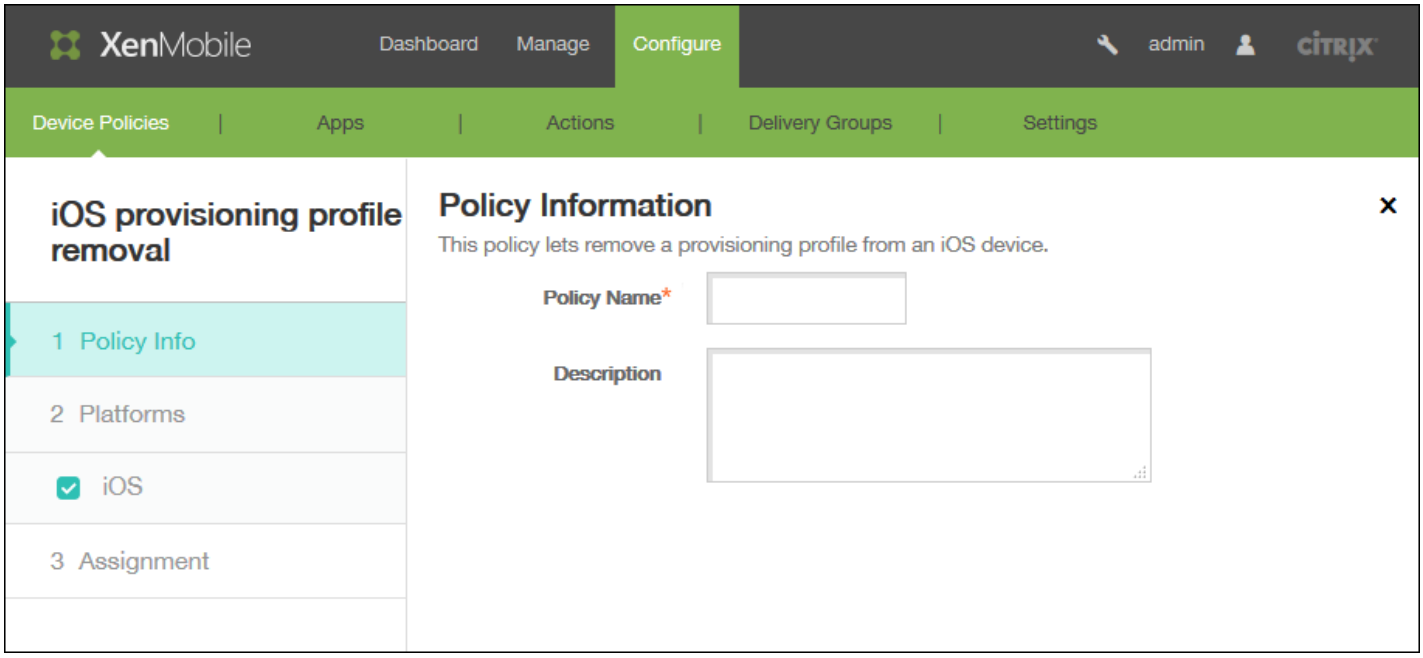
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。



2. 单击**添加**添加新策略。将显示**添加新策略**页面。



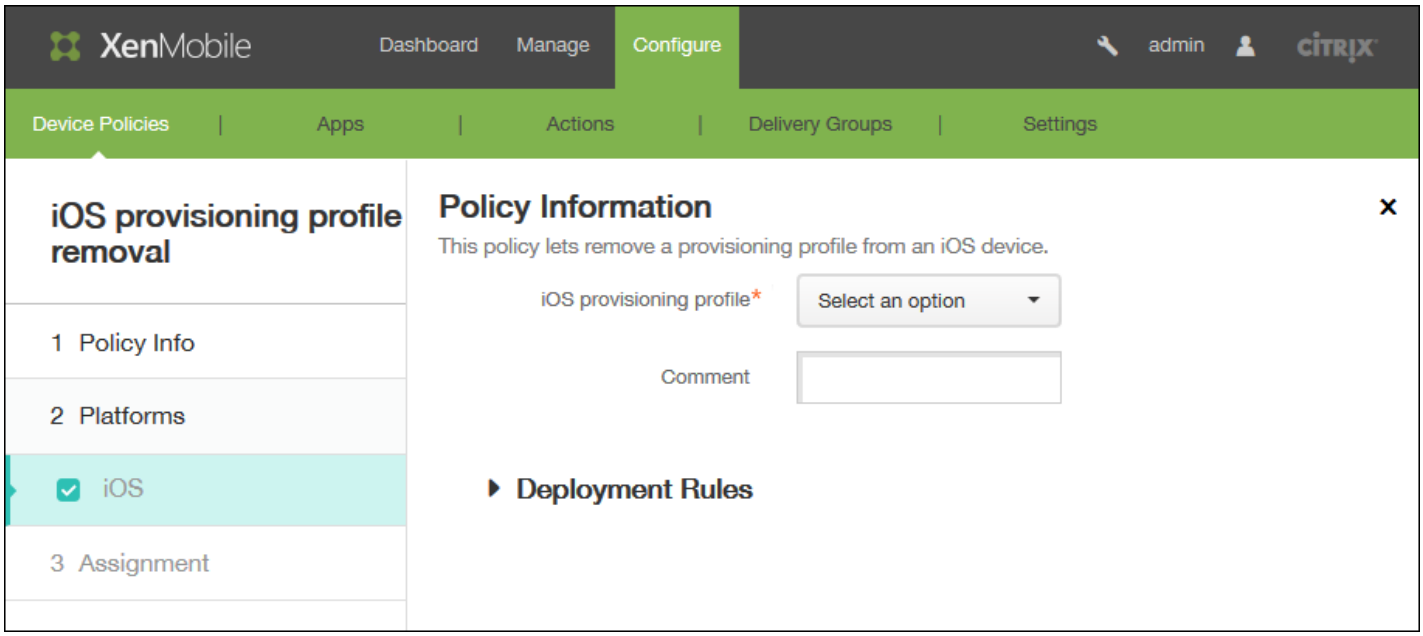
3. 在**添加新策略**页面上，单击**更多**，然后在**删除**下方，单击**删除置备配置文件**。将显示**删除 iOS 置备配置文件**策略信息页面。



4. 在**策略信息**窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。此时将显示 **iOS 平台**信息页面。



6. 在 **iOS 平台信息**页面中，配置以下设置：

- **iOS 置备配置文件**：在列表中，单击要删除的置备配置文件。
- **备注**：可选，添加备注。

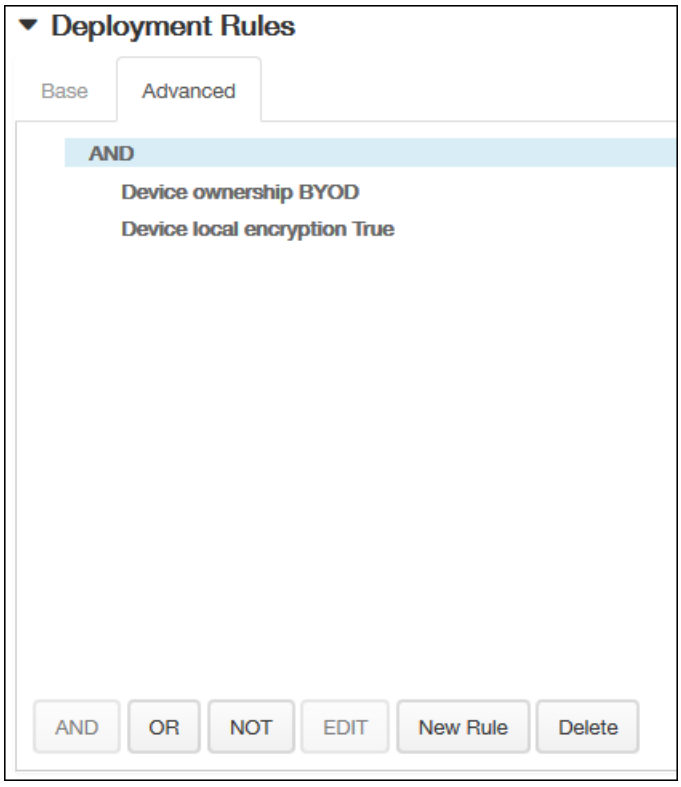
7. 展开**部署规则**，然后配置以下设置：

默认情况下将显示**基础**选项卡。

8. 在此列表中，单击选项以确定部署策略的时间。

- 可以选择在满足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**。
- 单击**新建规则**以定义条件。
- 在列表中，单击条件，如**设备所有权**和 **BYOD**，如上图所示。
- 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。

9. 单击**高级**选项卡以使用布尔选项组合规则。

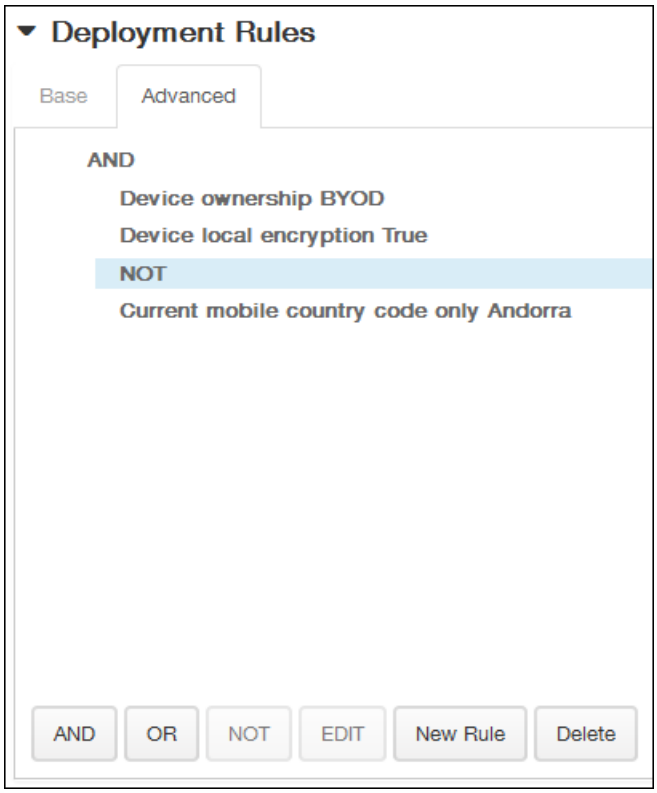


将显示您在**基础**选项卡上选择的条件。

10. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。

- 单击 **AND**、**OR** 或 **NOT**。
- 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。

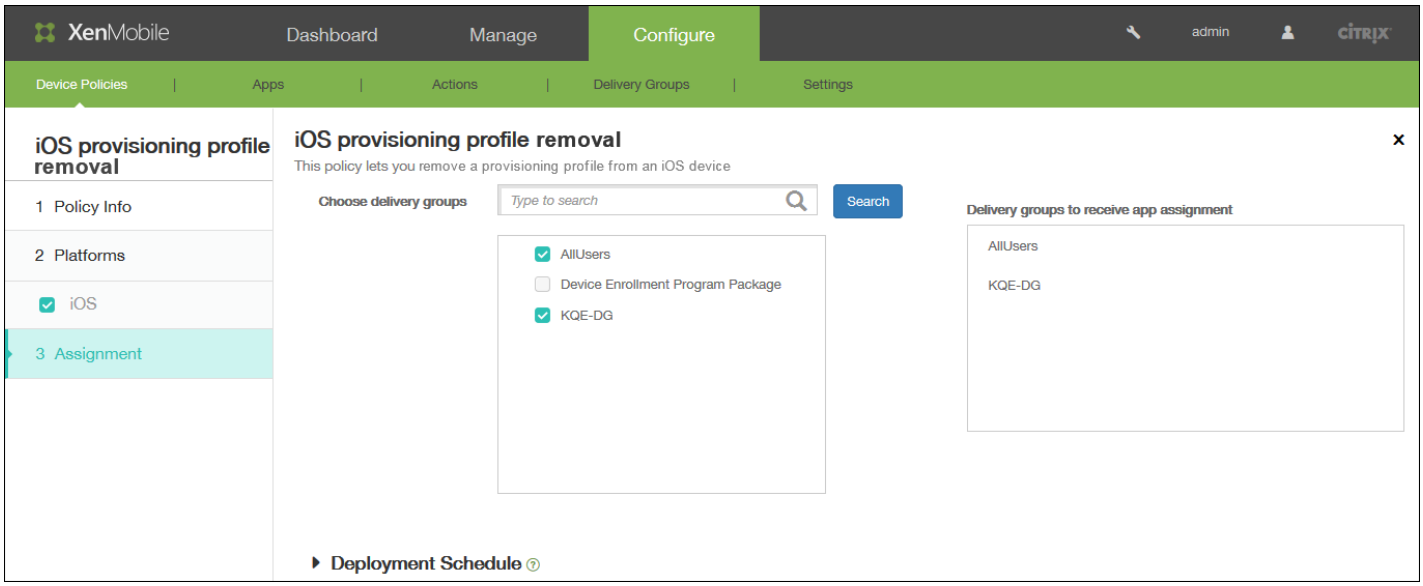
- 如果要添加更多条件，请再次单击**新建规则**。



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。

11. 单击**下一步**。此时将显示 **iOS 置备配置文件策略**分配页面。

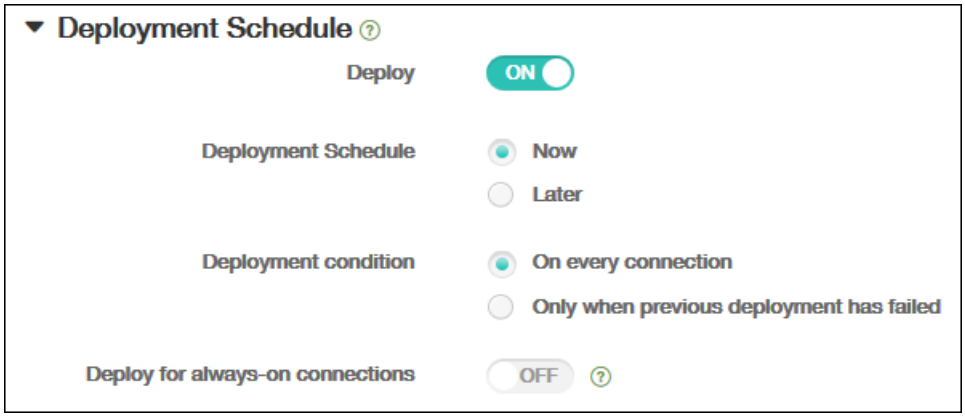
12. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。选择的组显示在**用于接收应用程序分配的交付组**列表中。



13. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。默认选项为**开**。如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。默认选项为**立即**。
- 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
- 在**部署条件**旁边，单击**每次连接时**或单击**仅当之前的部署失败时**。默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。默认选项为**关**。请注意，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。

凭据设备策略

Oct 22, 2015

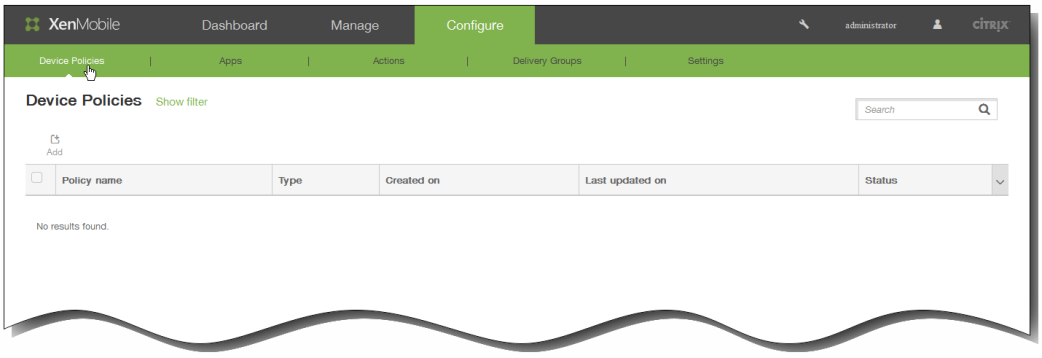
可以在 XenMobile 中创建凭据设备策略，以使用 XenMobile 中的 PKI 配置启用集成身份验证，例如 PKI 实体、密钥库、凭据提供程序或服务器证书。有关凭据的详细信息，请参阅 XenMobile 中的证书。

可以为 iOS、Android、Android for Work 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。

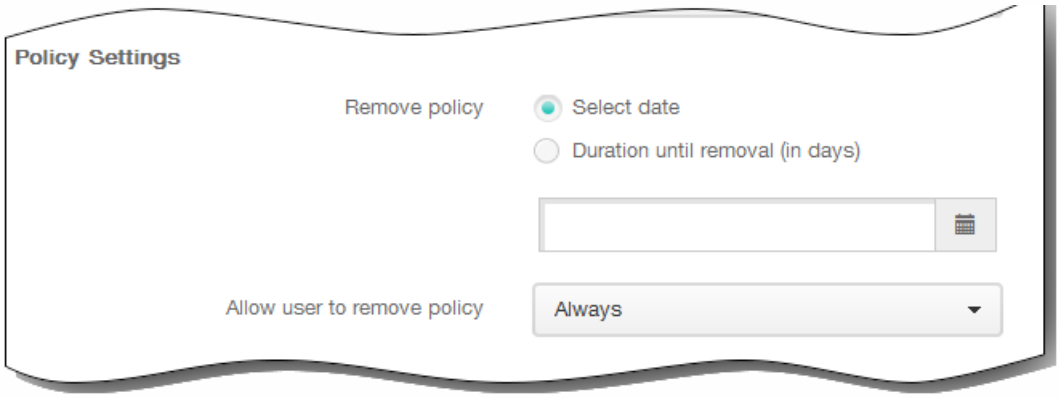


2. 单击添加添加新策略。此时将显示添加新策略对话框。
3. 单击更多，然后在安全性下面，单击凭据。此时将显示凭据策略信息页面。
4. 在策略信息窗格中，键入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：键入策略的可选说明。
5. 单击下一步。此时将显示策略平台页面。
   注意：策略平台页面显示时，所有平台都处于选中状态，您首先看到 iOS 平台配置面板。
6. 在平台下面，选择要添加的平台。
   - 如果选择 iOS，可以配置以下设置：
     凭据类型：在列表中，单击要用于此策略的凭据类型。

     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 Allow user to remove policy（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：

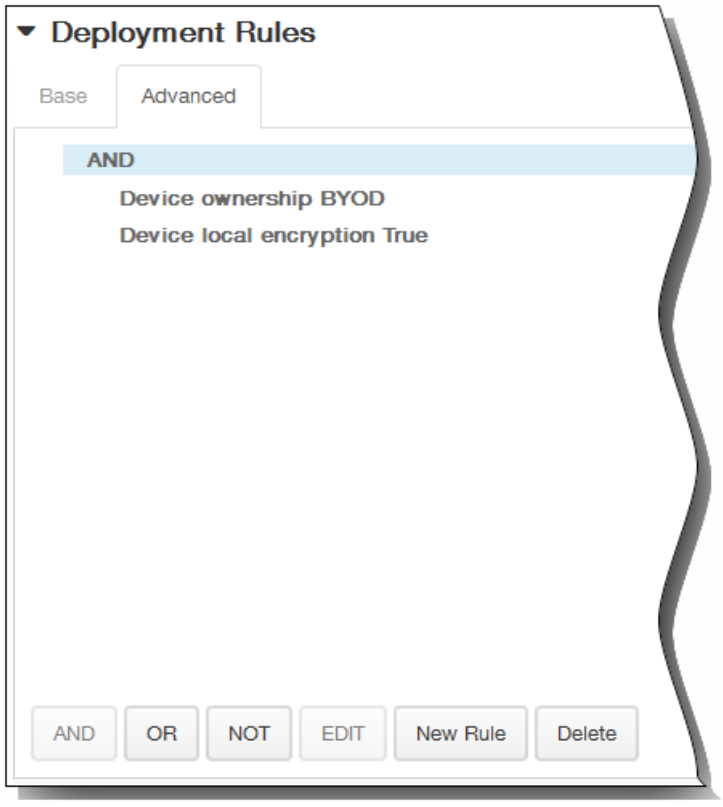
  - **证书**
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：单击浏览，然后导航到凭据文件的位置，以选择此凭据文件。
  - **密钥库**
    - 凭据名称：键入凭据的唯一名称。
    - 凭据文件路径：单击浏览，然后导航到凭据文件的位置，以选择此凭据文件。
    - 密码：键入凭据的密钥库密码。
  - **服务器证书**
    - 服务器证书：在列表中，单击要使用的证书。
  - **凭据提供程序**
    - 凭据提供程序：在列表中，单击凭据提供程序的名称。
- 如果选择 Windows 8.1 Tablet，可以配置以下设置：
  存储设备：在列表中，单击 root（根）、My（我的）或 CA 以选择凭据的证书存储位置。My（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。

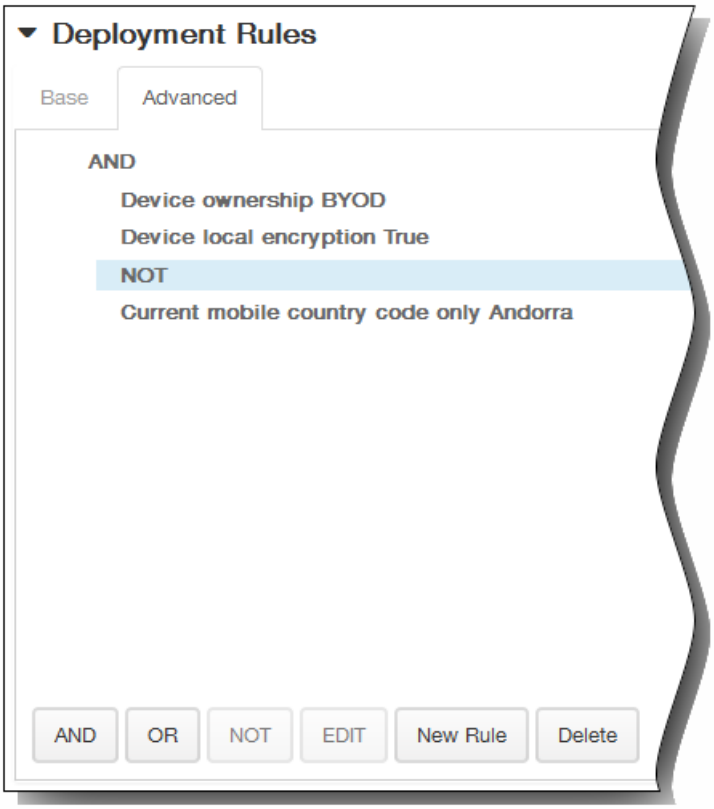


将显示您在基础选项卡上选择的条件。

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。

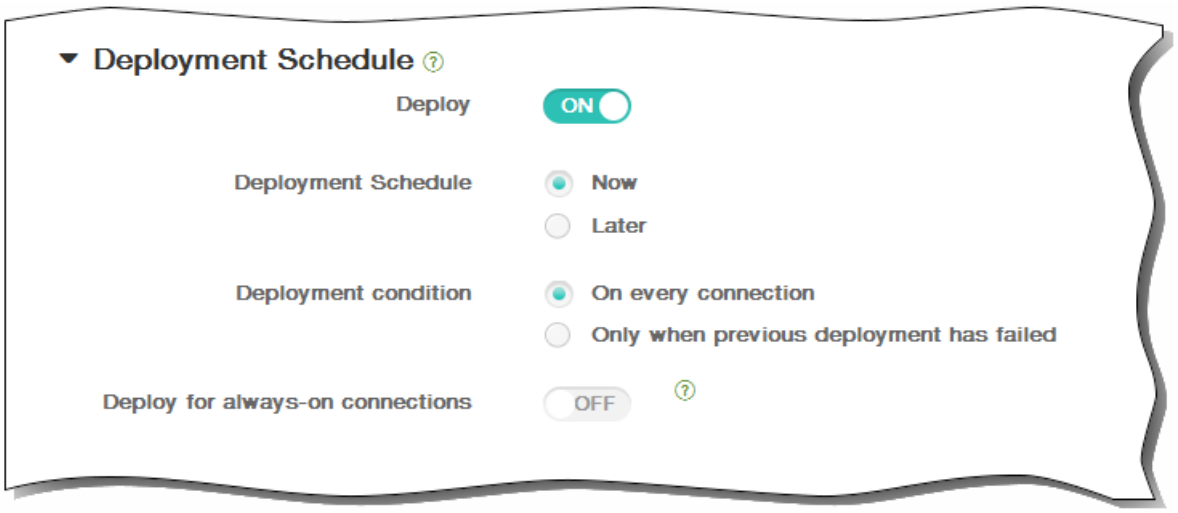
您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。

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

Aug 04, 2016

可以在 XenMobile 中创建 Kiosk 策略以便能够指定只能在 Samsung SAFE 设备上使用一个或多个特定的应用程序。 此策略对旨在仅运行特定类型或类别的应用程序的企业设备非常有用。 此策略还允许您为设备选择处于 Kiosk 模式时设备主屏幕和锁定屏幕墙纸使用的自定义图片。

将 Samsung SAFE 设备置于 Kiosk 模式

1. 在移动设备上启用 Samsung SAFE API 密钥，如 Samsung MDM 许可证密钥设备策略中所述。 此步骤允许您在 Samsung SAFE 设备上启用策略。

2. 为 Android 设备启用“连接计划策略”，如连接计划设备策略中所述。 此步骤允许 Android 设备连接回 XenMobile。

3. 添加 Kiosk 设备策略，如下一部分内容中所述。

4. 将这三条设备策略分配给恰当的交付组。 考虑是否要在这些交付组中包括其他策略，例如“应用程序清单”。

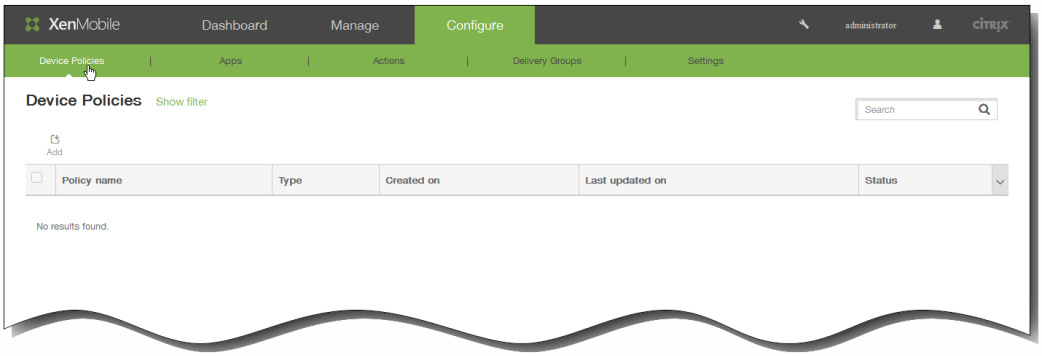
如果以后要从 Kiosk 模式中删除设备，请创建一个 **Kiosk 模式**设置为**禁用**的新 Kiosk 设备策略。 更新交付组以删除启用了 Kiosk 模式的 Kiosk 策略以及添加禁用了 Kiosk 模式的 Kiosk 策略。

添加 Kiosk 设备策略

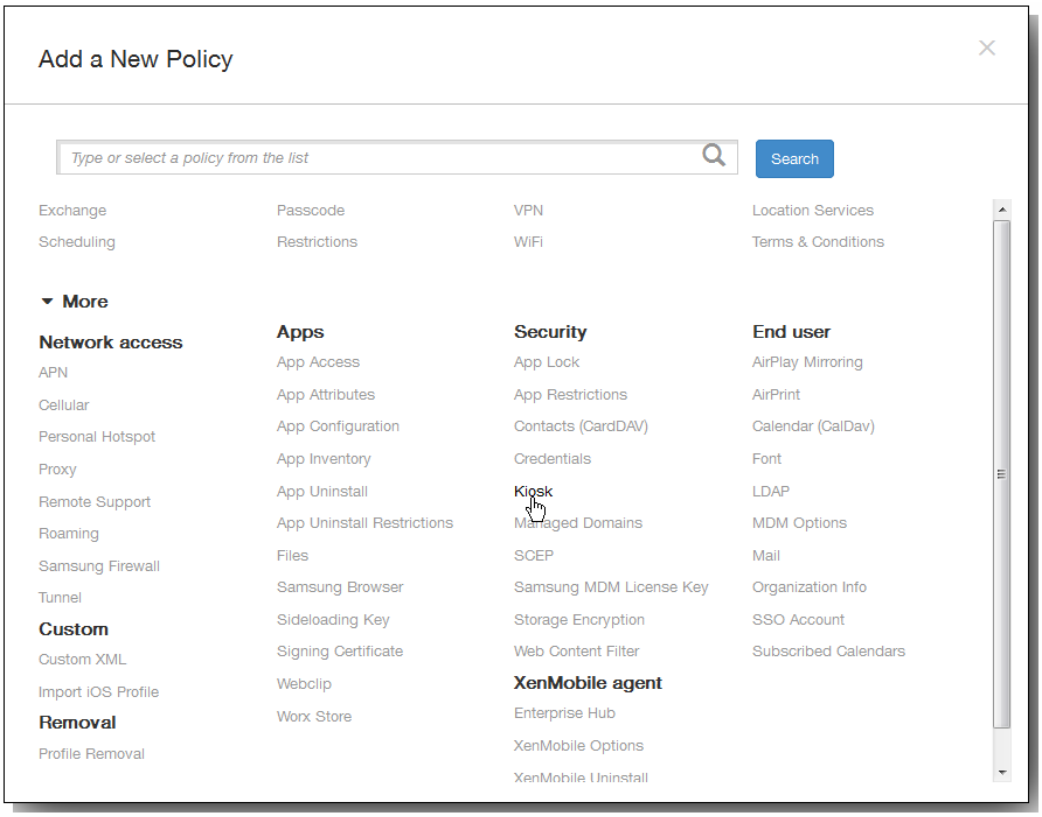
注意：

- 为 Kiosk 模式指定的所有应用程序必须已安装在用户设备上。
- 某些选项仅适用于 Samsung Mobile Device Management API 4.0 及更高版本。

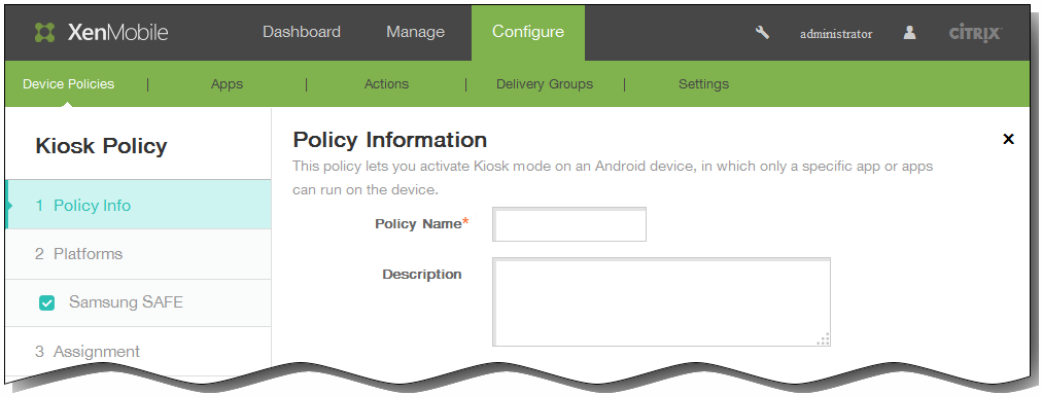
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



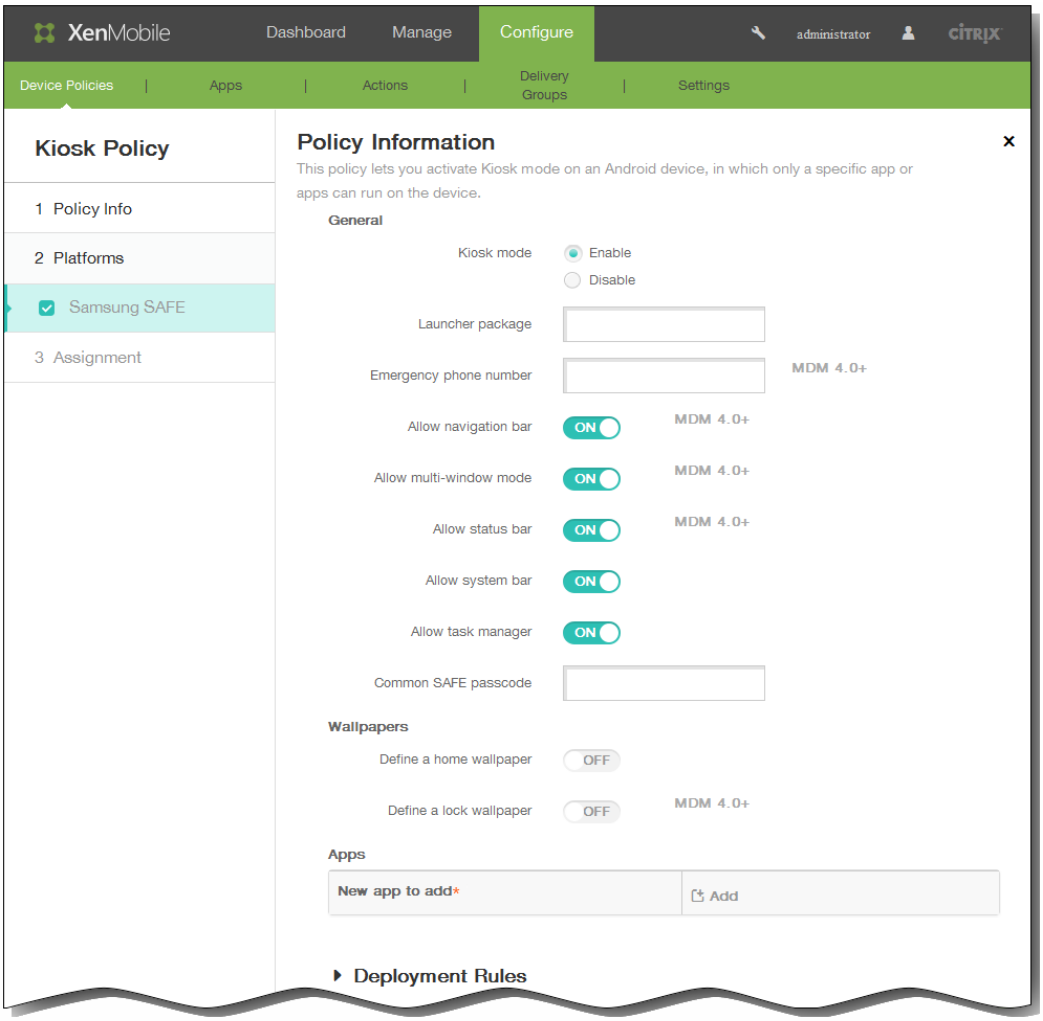
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



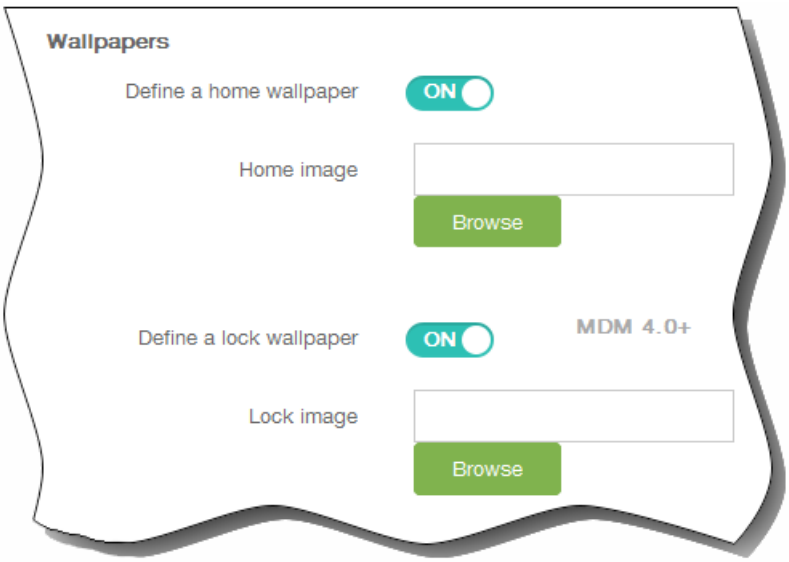
3. 单击更多，然后在安全性下，单击 Kiosk。 此时将显示 Kiosk 策略页面。



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。



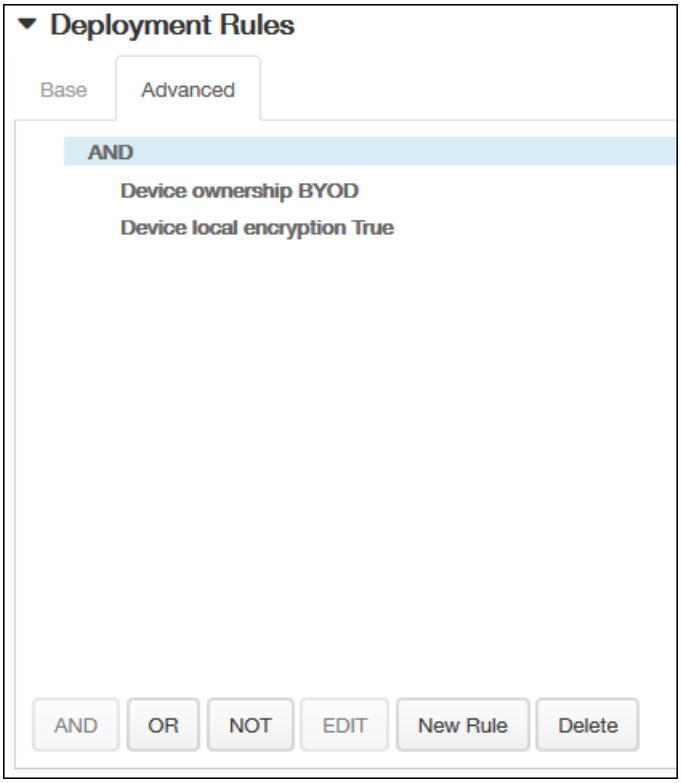
12. 应用程序：单击添加，然后执行以下操作：
    1. 新建要添加的应用程序：输入要添加的应用程序的完整名称。例如，com.android.calendar 允许用户使用 Android 日历应用程序。
    2. 单击添加添加应用程序，或单击取消取消添加应用程序。
    3. 为要添加的每个应用程序重复步骤 i.和 ii.。

    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。

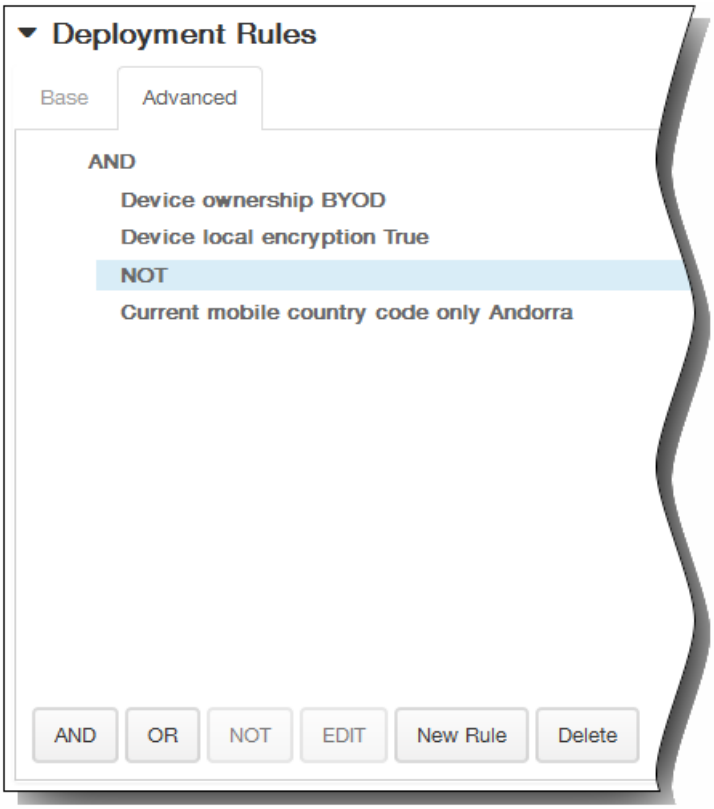
7. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

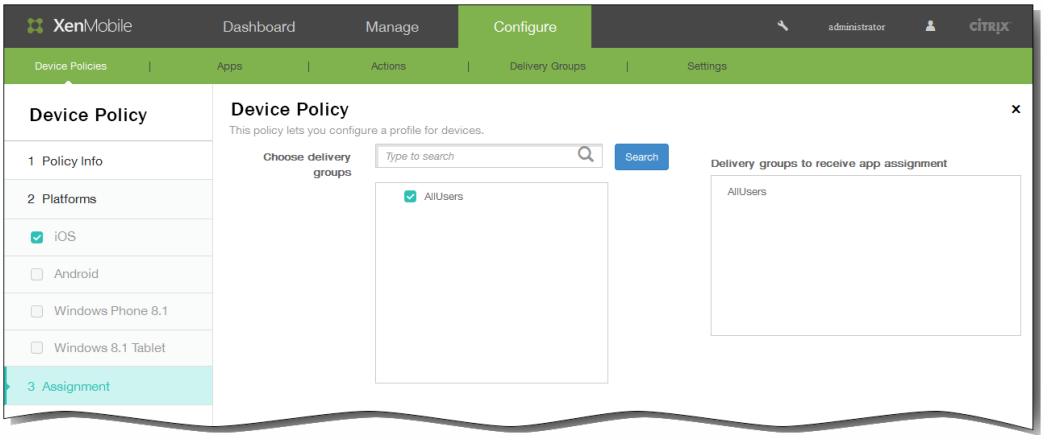


将显示您在基础选项卡上选择的条件。

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。

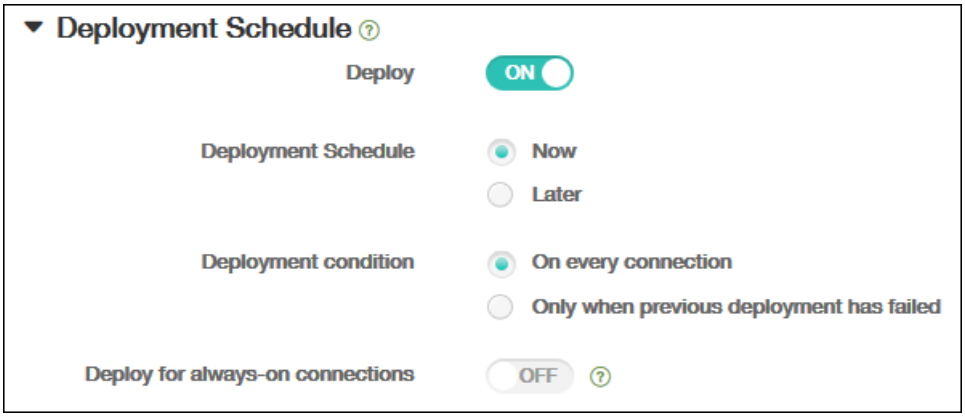


8. 单击下一步。 此时将显示 Kiosk 策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

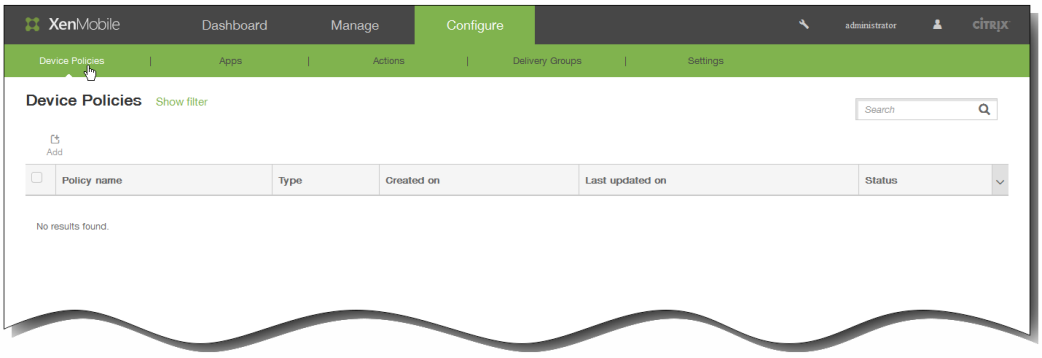
为 iOS 添加字体设备策略

Oct 22, 2015

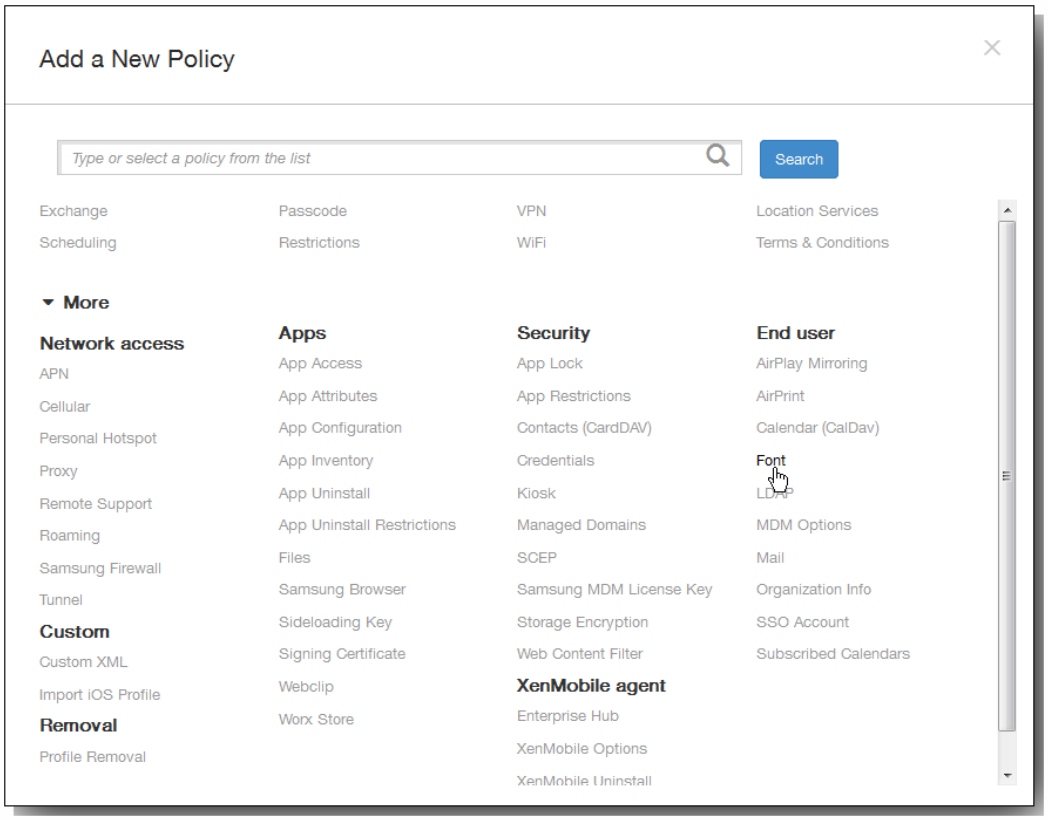
可以在 XenMobile 中添加设备策略以向用户设备添加附加字体。字体必须是 TrueType (.ttf) 或 OpenType (.oft) 字体。不支持字体集合（.ttc 或 .otc）。

注意：此策略仅适用于 iOS 7.0 及更高版本。

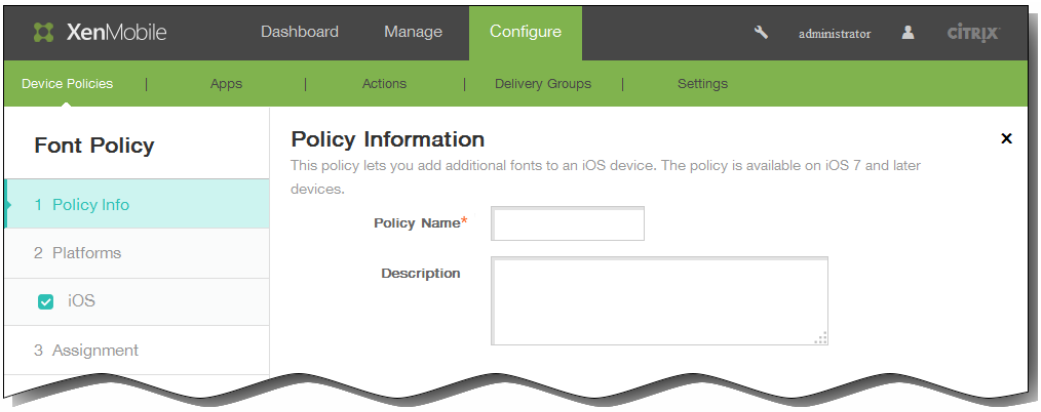
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



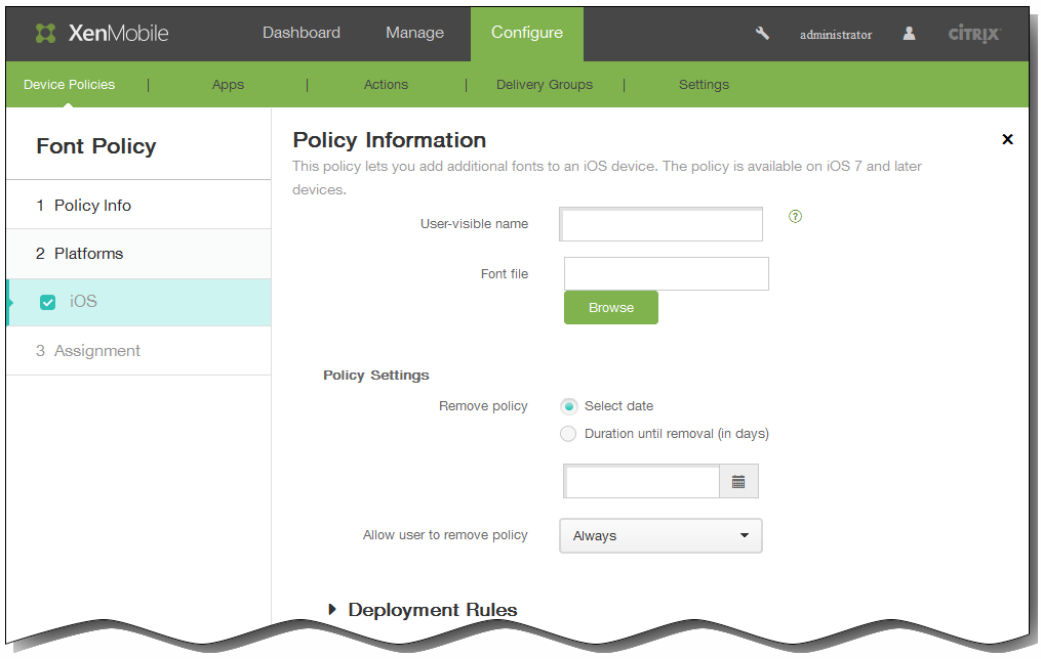
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



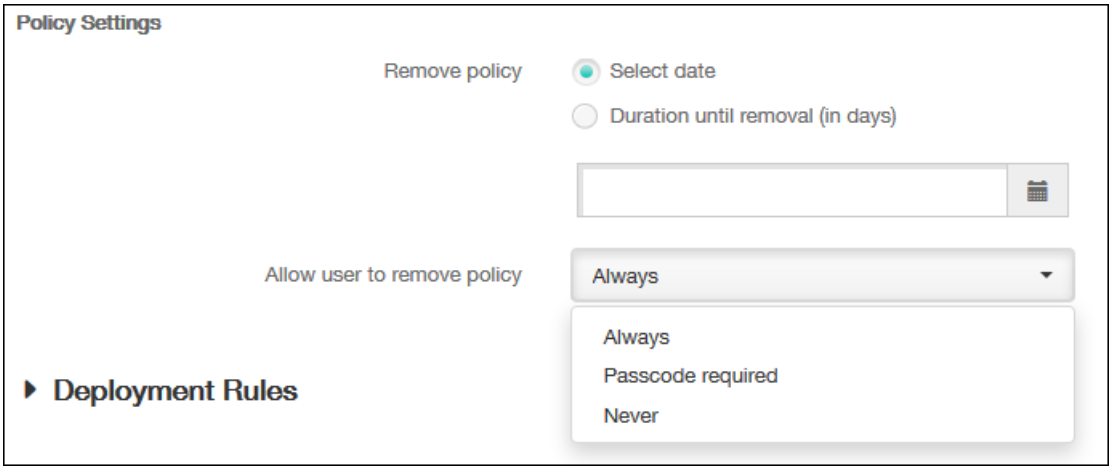
3. 单击更多，然后在最终用户下，单击字体。 此时将显示字体策略页面。



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。

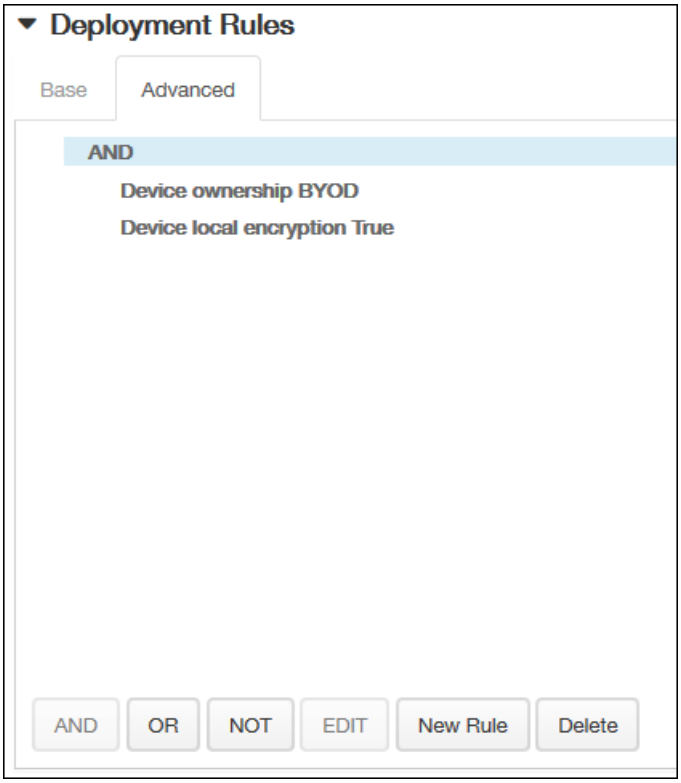


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 用户可见名称：输入用户在其字体列表中看到的名称。
   2. 字体文件：选择要添加到用户设备的字体文件，可以单击浏览，然后导航到该文件的位置。
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删除策略列表中，单击始终、需要密码或从不。
10. 如果单击需要密码，在 Removal password（删除密码）旁边，键入必需的密码。



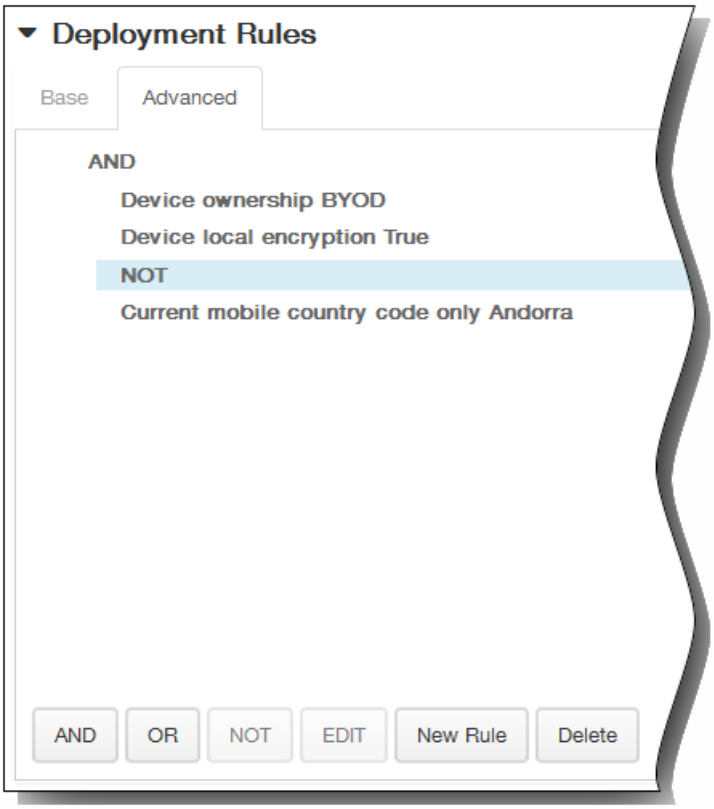
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

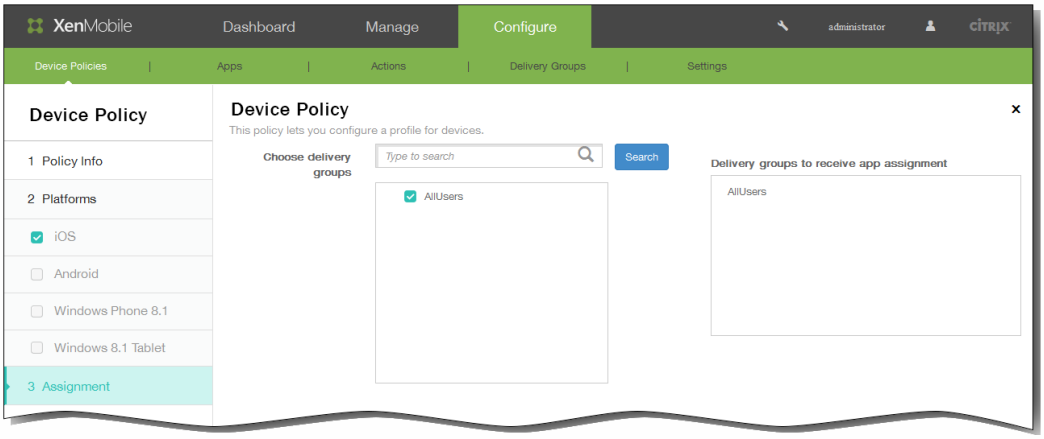


将显示您在基础选项卡上选择的条件。

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。



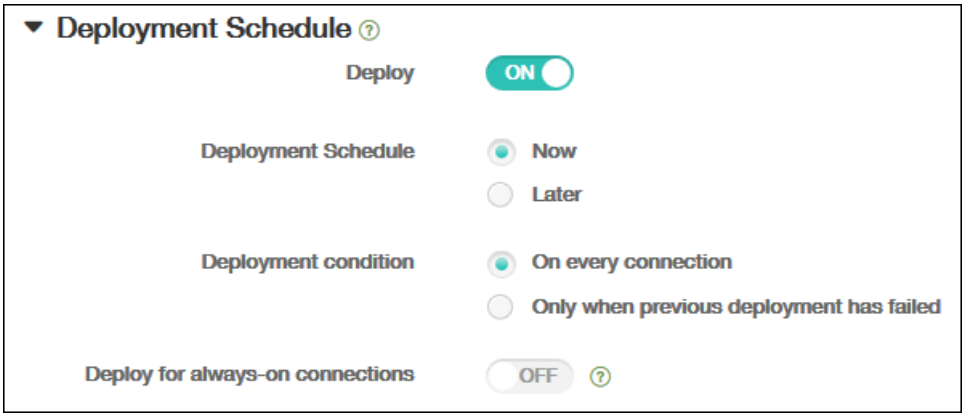
12. 单击下一步。 此时将显示字体策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。



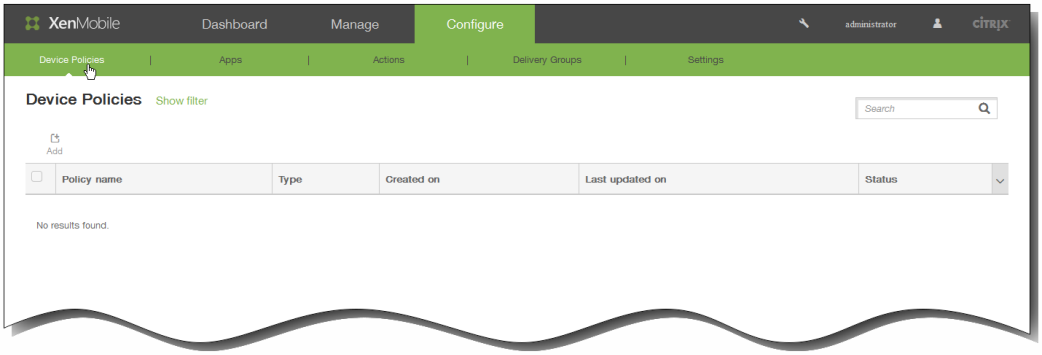
15. 单击保存以保存此策略。

为 iOS 添加邮件设备策略

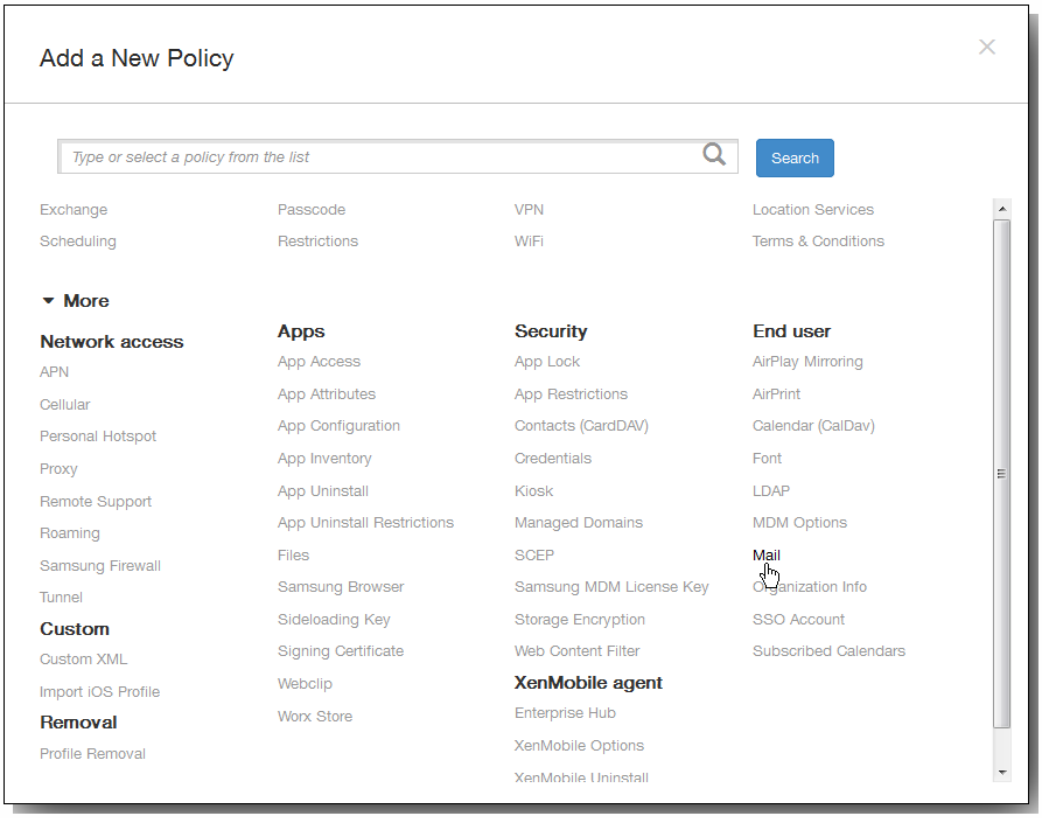
Oct 22, 2015

可以在 XenMobile 中添加邮件设备策略以在用户的 iOS 设备上配置电子邮件帐户。

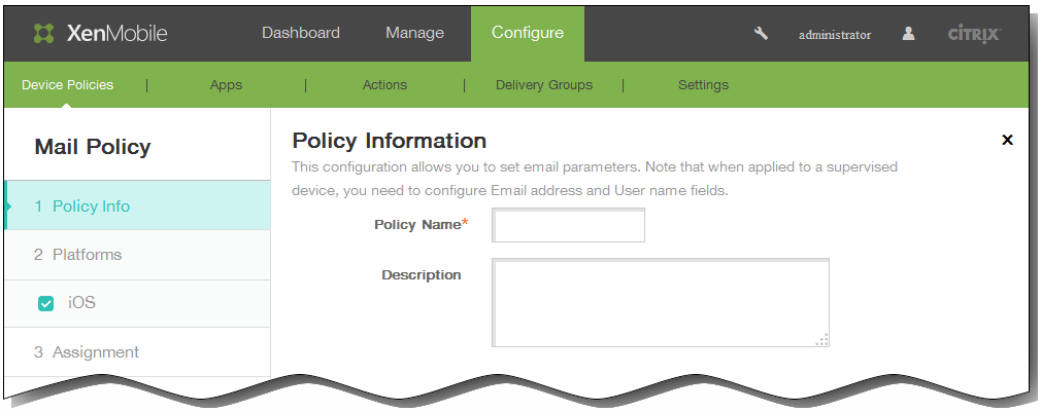
1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。



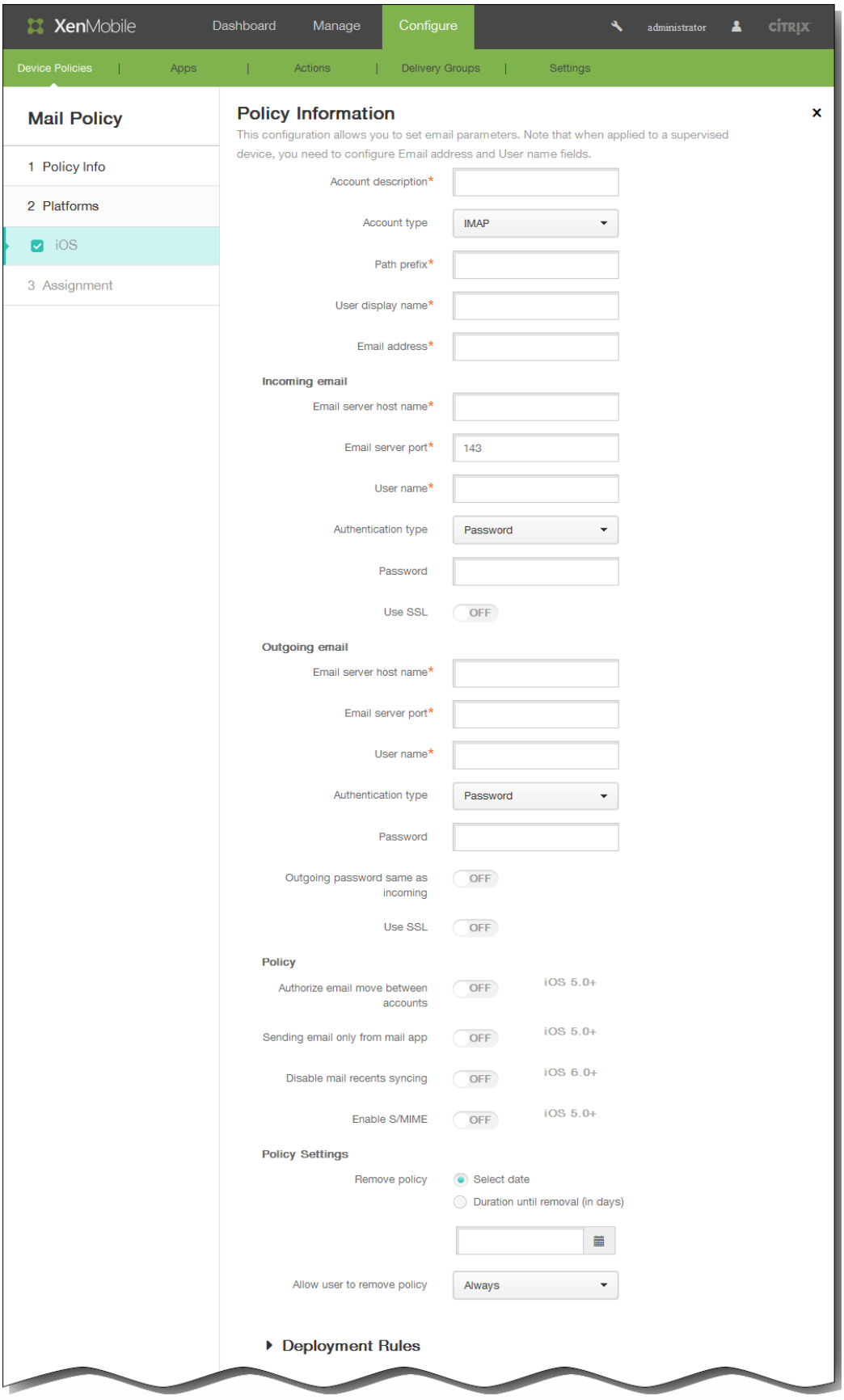
2. 单击添加添加新策略。此时将显示添加新策略对话框。



3. 单击更多，然后在最终用户下，单击邮件。此时将显示邮件策略页面。



4. 在策略信息窗格中，输入以下信息：
    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：输入在邮件和设置应用程序中显示的帐户说明。 此字段为必填字段。
2. 帐户类型：在列表中，单击 IMAP 或 POP 以选择要对用户帐户使用的协议。 默认值为 IMAP。选择“POP”时，以下路径前缀选项将消失。
3. 路径前缀：输入 INBOX 或您的 IMAP 邮件帐户路径前缀（如果不是 INBOX）。 此字段为必填字段。
4. 用户显示名称：输入要对邮件等使用的完整用户名。 此字段为必填字段。
5. 电子邮件地址：输入帐户的完整电子邮件地址。 此字段为必填字段。

传入电子邮件设置

6. 电子邮件服务器主机名：输入传入电子邮件服务器主机名或 IP 地址。 此字段为必填字段。
7. 电子邮件服务器端口：输入传入邮件服务器端口号。 默认值为 143。 此字段为必填字段。
8. 用户名：输入电子邮件帐户的用户名。 此名称通常与用户的电子邮件地址中 @ 字符前面的部分相同。 此字段为必填字段。
9. 身份验证类型：在列表中，单击以选择要使用的身份验证类型。 默认值为密码。 选中无时，以下密码字段将消失。
10. 密码：输入传入邮件服务器的可选密码。
11. 使用 SSL：选择传入邮件服务器是否使用安全套接字层身份验证。 默认值为关。

传出电子邮件设置

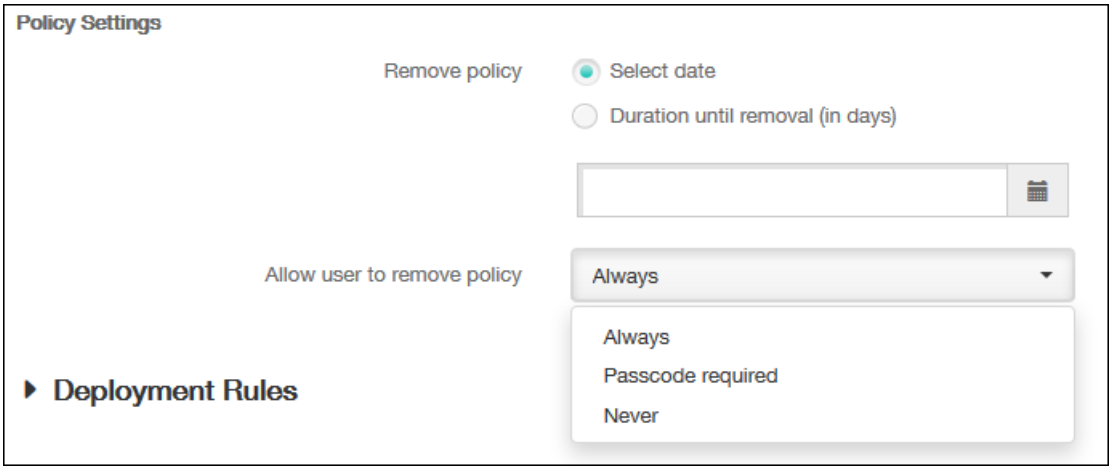
12. 电子邮件服务器主机名：输入传出电子邮件服务器主机名或 IP 地址。 此字段为必填字段。
13. 电子邮件服务器端口：输入传出邮件服务器端口号。 如果未输入端口号，则将使用指定协议的默认端口。
14. 用户名：输入电子邮件帐户的用户名。 此名称通常与用户的电子邮件地址中 @ 字符前面的部分相同。 此字段为必填字段。
15. 身份验证类型：在列表中，单击以选择要使用的身份验证类型。 默认值为密码。 选中无时，以下密码字段将消失。
16. 密码：输入传出邮件服务器的可选密码。
17. 传出密码和传入密码相同：选择传入和传出密码是否相同。 默认值为关，表示密码不相同。 设置为开时，上述密码字段将消失。
18. 使用 SSL：选择传出邮件服务器是否使用安全套接字层身份验证。 默认值为关。

策略设置

注意：这些选项仅适用于 iOS 5.0 及更高版本。

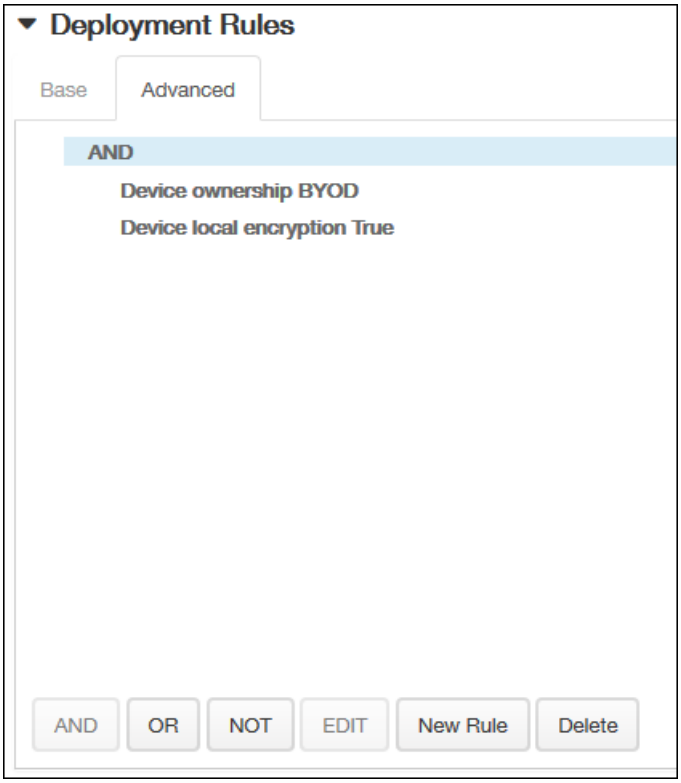
19. 授权电子邮件在帐户之间移动：选择是否允许用户将电子邮件从此帐户移出到另一个帐户以及从其他帐户转发和答复。默认值为关，此设置允许用户将电子邮件移至另一个帐户以及从其他帐户转发或答复。
20. 只从邮件应用程序发送电子邮件：选择是否将用户限制为从 iOS 邮件应用程序发送电子邮件。
21. 禁用最新邮件同步：选择是否阻止用户同步最近使用的地址。 默认值为关。 此选项仅适用于 iOS 6.0 及更高版本。
22. 启用 S/MIME：选择此帐户是否支持 S/MIME 身份验证和加密。 默认值为关。 设置为开时，将显示以下两个字段。
23. 签署身份凭据：在列表中，选择要使用的签名凭据。
24. 加密身份凭据：在列表中，选择要使用的加密凭据。

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 Allow user to remove policy（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。



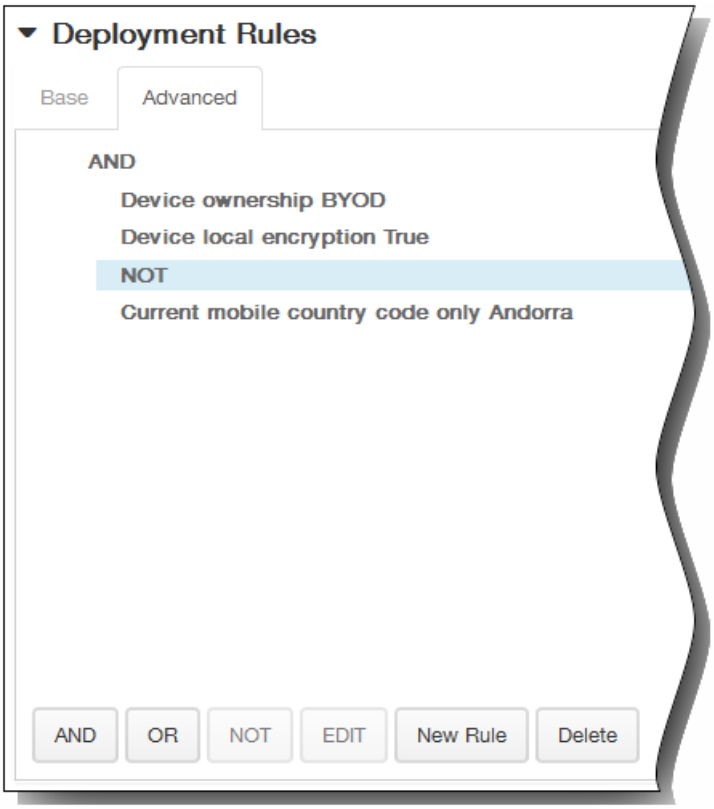
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

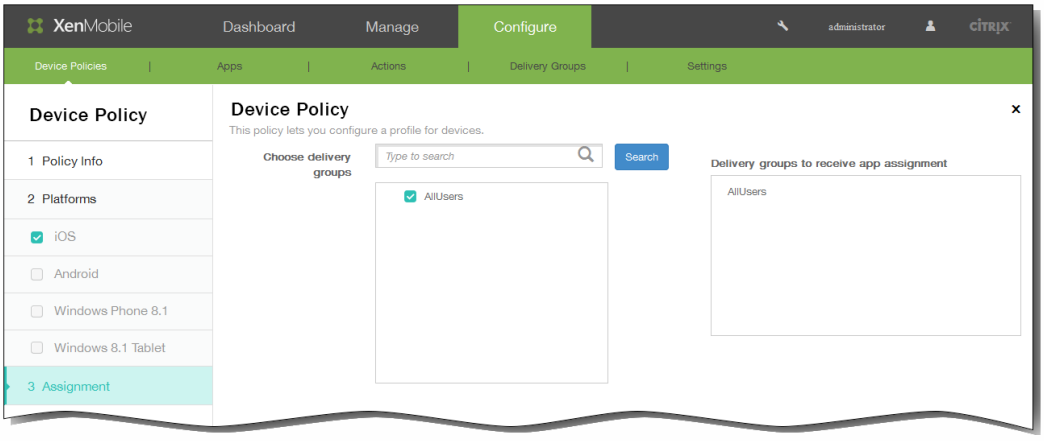


将显示您在基础选项卡上选择的条件。

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。此时将显示邮件策略分配页面。
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。

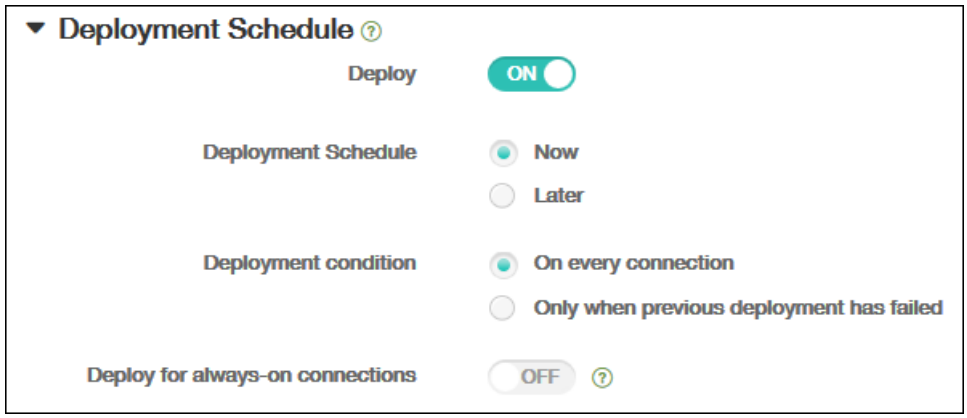


14. 展开部署计划，然后配置以下设置：
    1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。如果选择关，无需配置其他选项。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
    4. 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。 默认选项为每次连接时。

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。

托管域设备策略

Aug 04, 2016

可以定义应用到电子邮件和 Safari 浏览器的托管域。 托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护企业数据。 指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。 此策略仅在 iOS 8 及更高版本的受监督设备上可用。 有关将 iOS 设备置于受监督模式的步骤，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。

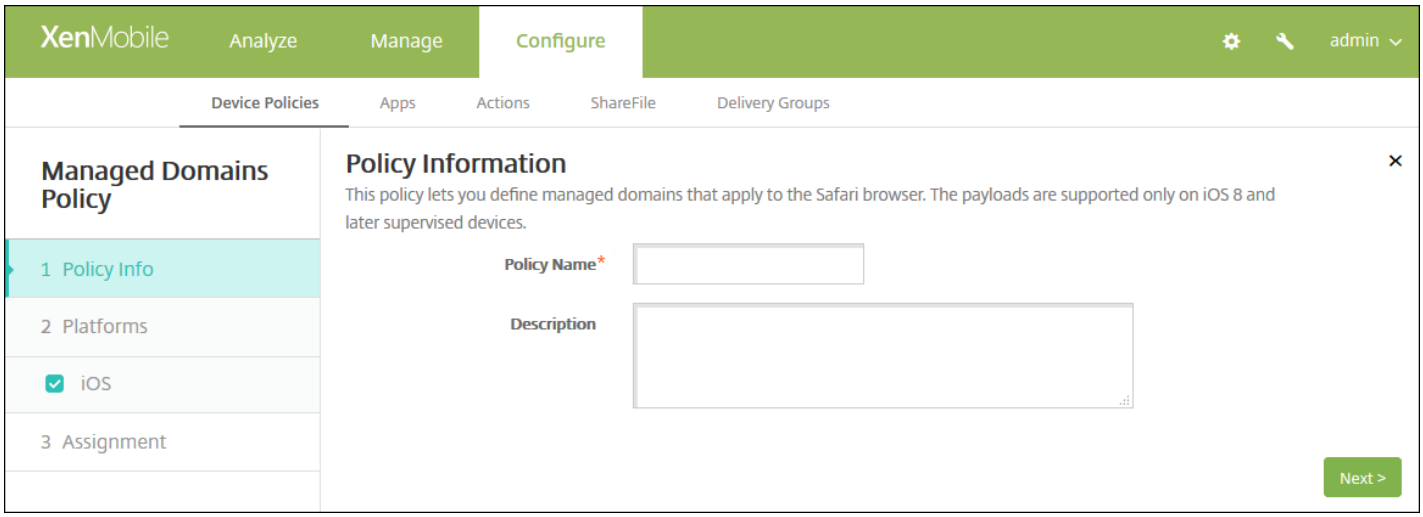
用户向域不在托管电子邮件域列表上的收件人发送电子邮件时，在用户的设备上此邮件将带有标记，以警告用户正在向企业域外部的人员发送邮件。

当用户尝试使用 Safari 从位于托管 Web 域列表上的 Web 域打开某个项目（文档、附件或下载内容）时，将由合适的企业应用程序打开此项目。 如果此项目所在的 Web 域不在托管 Web 域列表上，用户无法使用合适的企业应用程序打开此项目；他们必须使用未托管的个人应用程序。

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

2. 单击**添加**。 此时将显示**添加新策略**对话框。

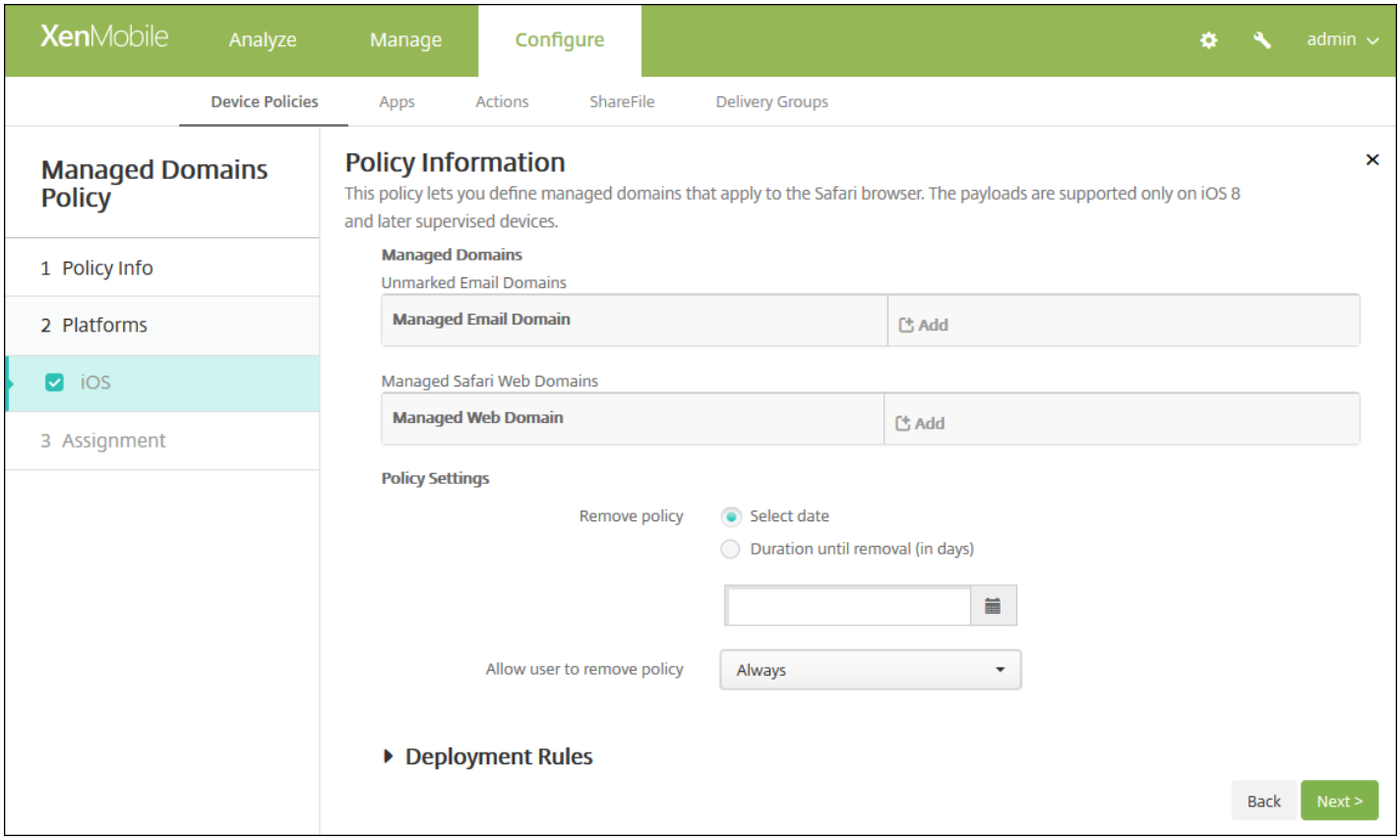
3. 展开**更多**，然后在**安全性**下面，单击**托管域**。 将显示**托管域策略**信息页面。



4. 在**策略信息**页面上，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。 此时将显示 **iOS 平台**页面。



如何指定域

6. 配置以下设置：

- **托管域**
  - **取消标记电子邮件域**：对于要包含在列表中的每个电子邮件域，请单击**添加**，然后执行以下操作：
    - **托管电子邮件域**：键入电子邮件域。
    - 单击**保存**以保存电子邮件域，或者单击**取消**不保存电子邮件域。
  - **托管 Safari Web 域**：对于要包含在列表中的每个 Web 域，请单击**添加**，然后执行以下操作：
    - **托管 Web 域**：键入 Web 域。
    - 单击**保存**以保存 Web 域，或者单击**取消**不保存 Web 域。

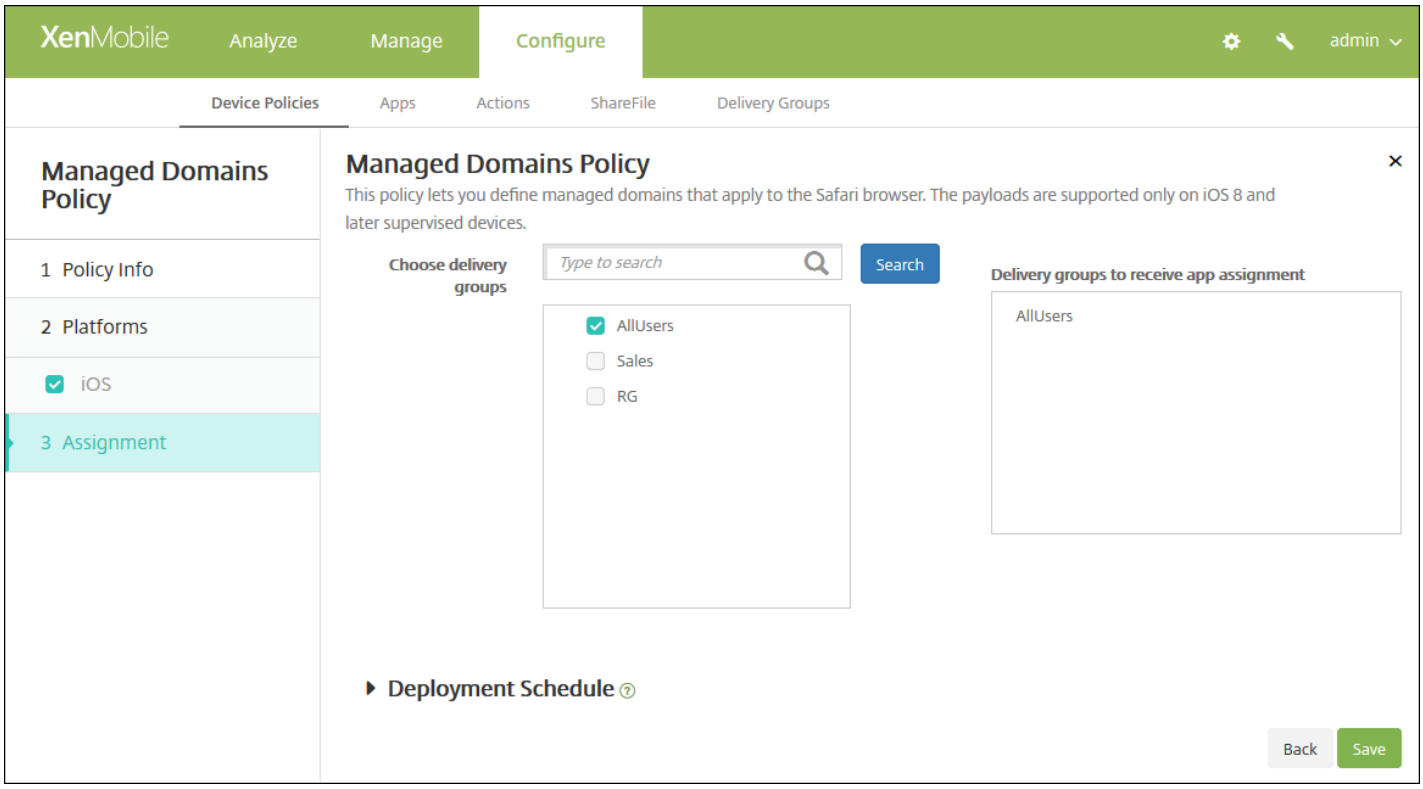
      注意：要删除现有域，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。 此时将显示确认对话框。 单击“删除”以删除列表，或单击**取消**以保留此列表。

      要编辑现有域，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。 更改列表，然后单击**保存**以保存更改的列表，或单击**取消**以保持列表不更改。

- **策略设置**
  - 在**策略设置**下，**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
  - 如果单击**选择日期**，请单击日历以选择具体删除日期。
  - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
  - 如果单击**需要密码**，在 Removal password（删除密码）旁边，键入必需的密码。

7. 配置部署规则

8. 单击**下一步**。 此时将显示**托管域策略**分配页面。



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

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。 默认选项为**开**。 如果选择**关**，无需配置其他选项。
- 在**部署计划**旁边，单击**立即**或**稍后**。 默认选项为**立即**。
- 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
- 在**部署条件**旁边，单击**每次连接时**或单击**仅当之前的部署失败时**。 默认选项为**每次连接时**。
- 在**为始终启用的连接部署**旁边，单击**开**或**关**。 默认选项为**关**。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。 始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。 您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

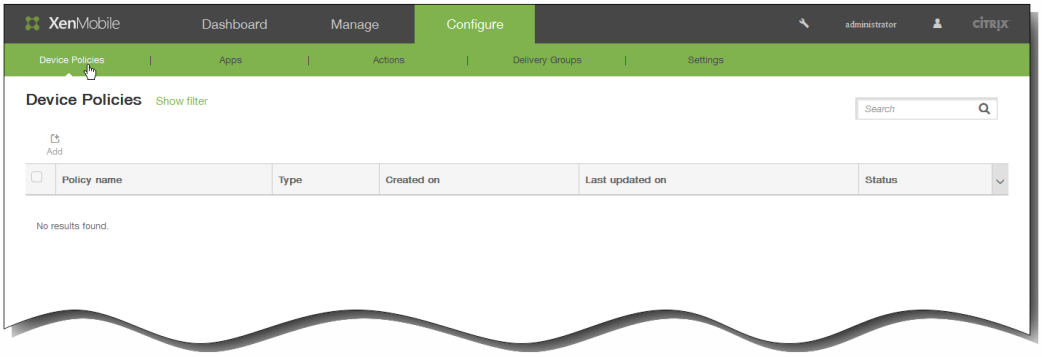
11. 单击**保存**。

为 iOS 添加组织信息设备策略

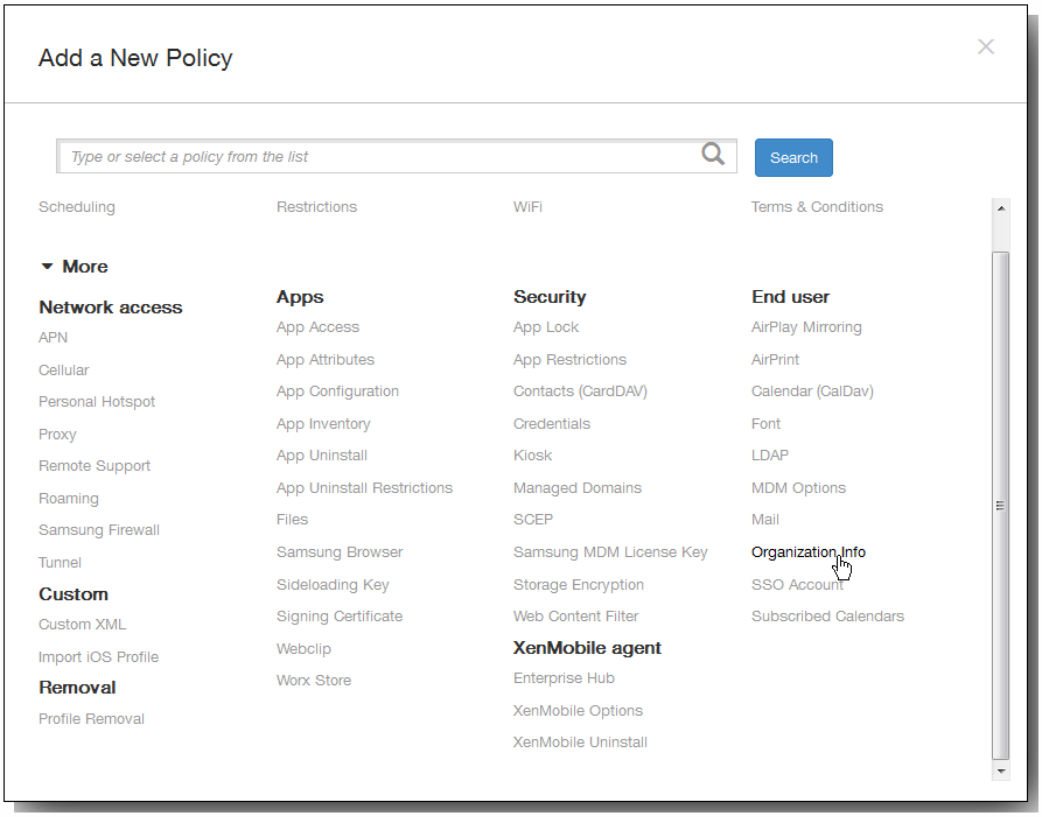
Oct 22, 2015

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。

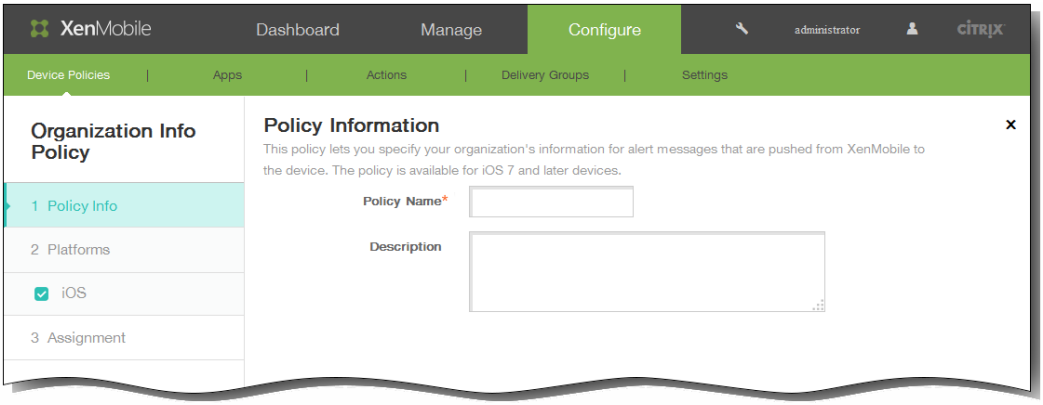
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



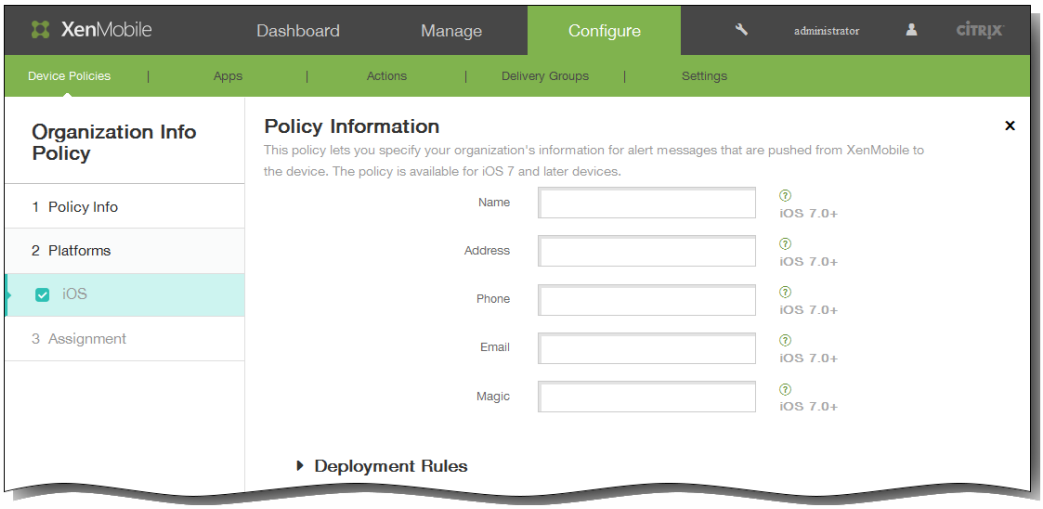
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



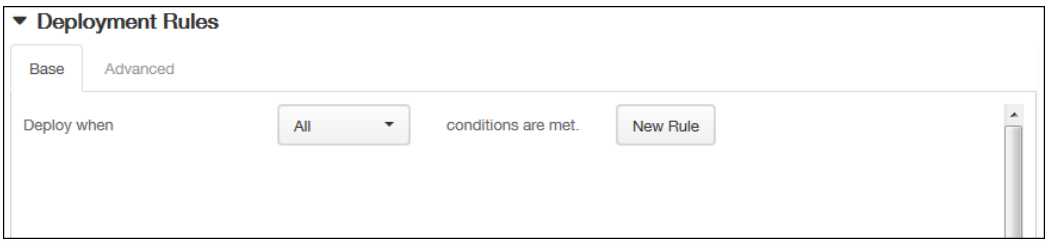
3. 单击更多，然后在最终用户下，单击组织信息。 此时将显示组织信息策略页面。



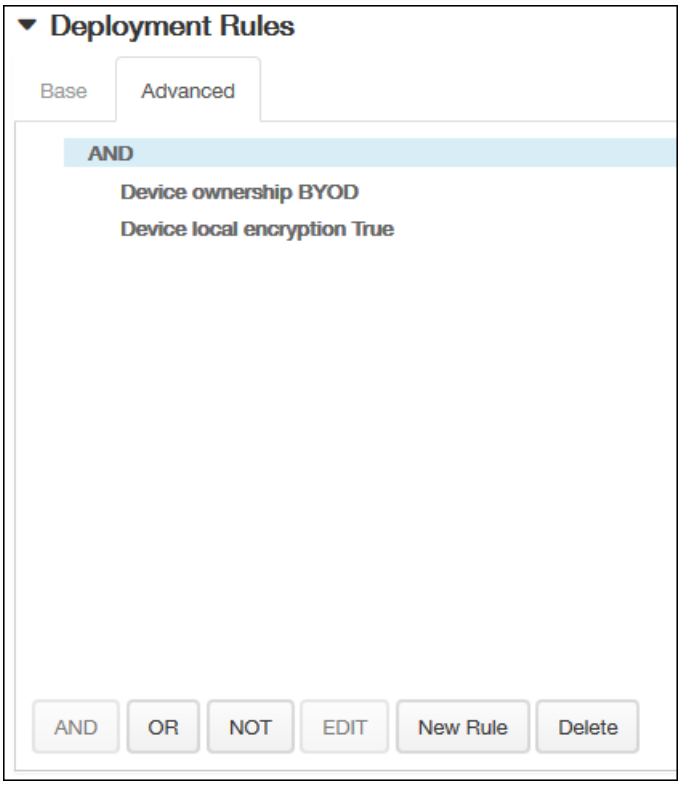
4. 在策略信息窗格中，输入以下信息：
   1. 策略名称：键入策略的描述性名称。
   2. 说明：如有需要，请键入策略的说明。
5. 单击下一步。 此时将显示 iOS 平台信息页面。



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。

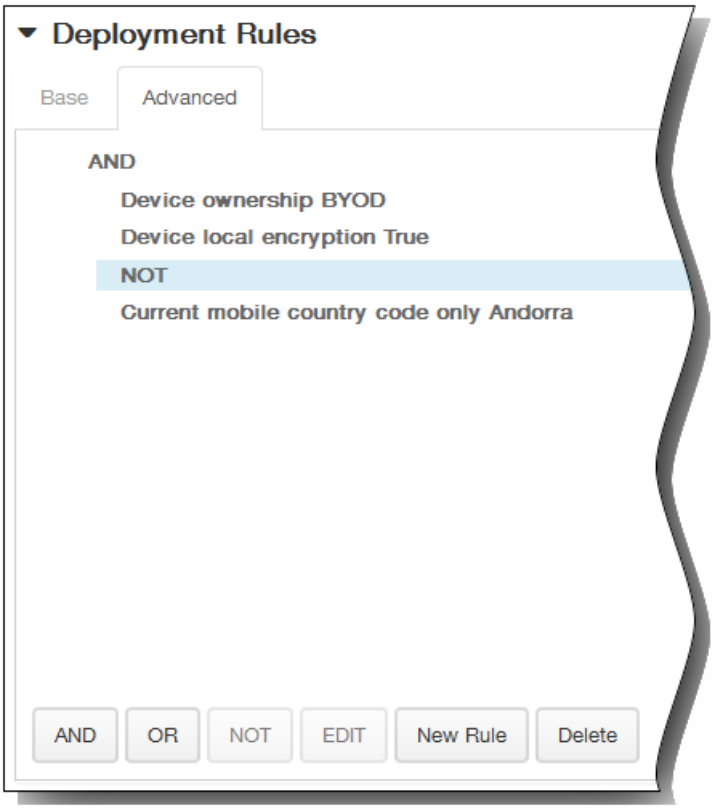


1. 在此列表中，单击选项以确定部署策略的时间。
    1. 可以选择在满足所有条件时部署策略，或在满足任意条件时部署策略。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。

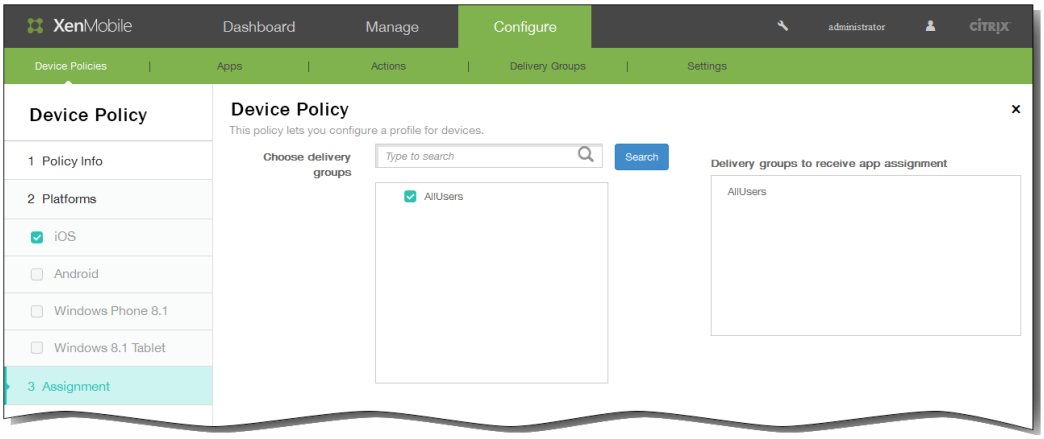


将显示您在基础选项卡上选择的条件。

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。



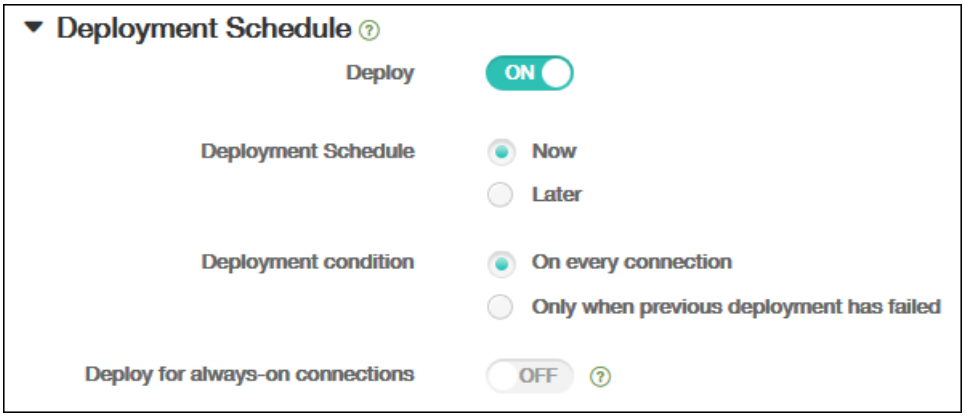
8. 单击下一步。 此时将显示组织信息策略分配页面。
9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

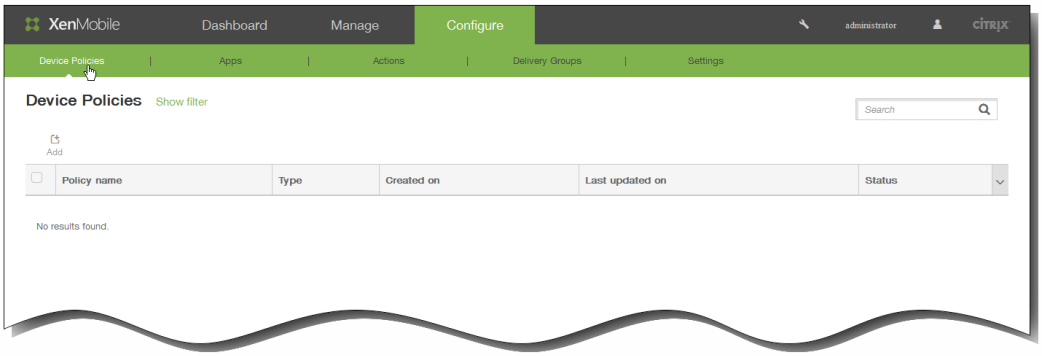
为 iOS 添加 LDAP 设备策略

Oct 22, 2015

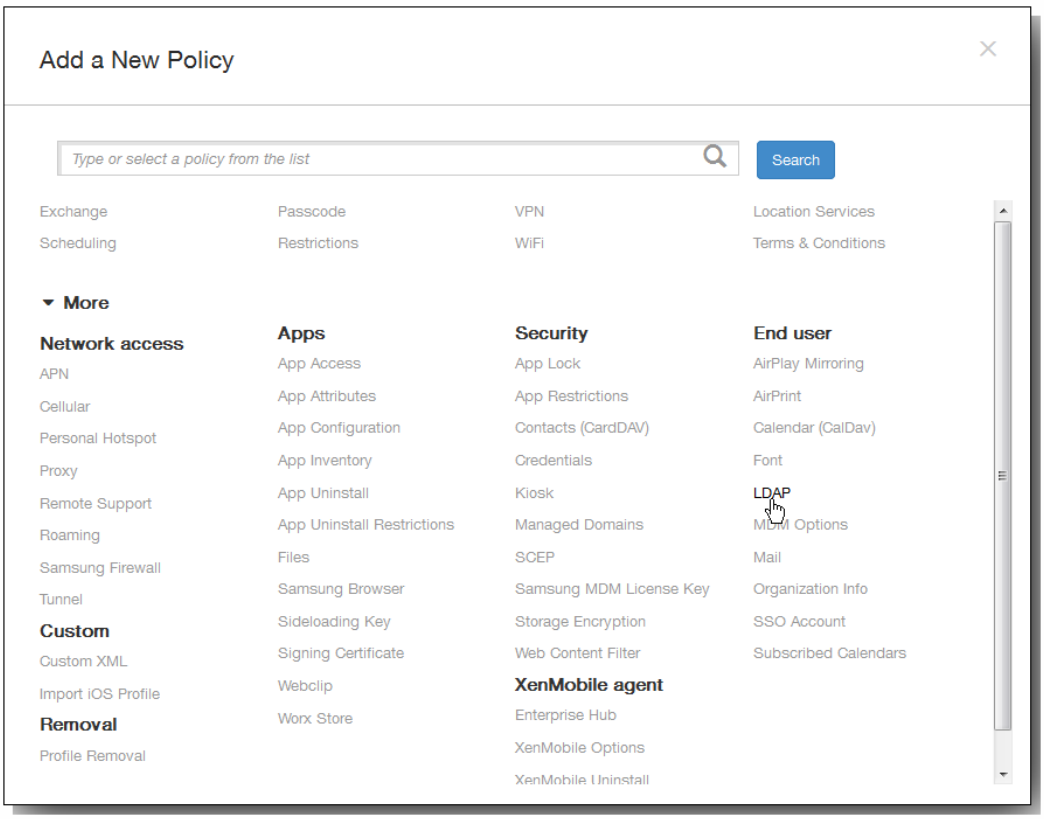
可以在 XenMobile 中为 iOS 设备创建 LDAP 策略，以提供与要使用的 LDAP 服务器有关的信息，包括任何必要的帐户信息。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。

配置此策略之前，您需要提供 LDAP 主机名。

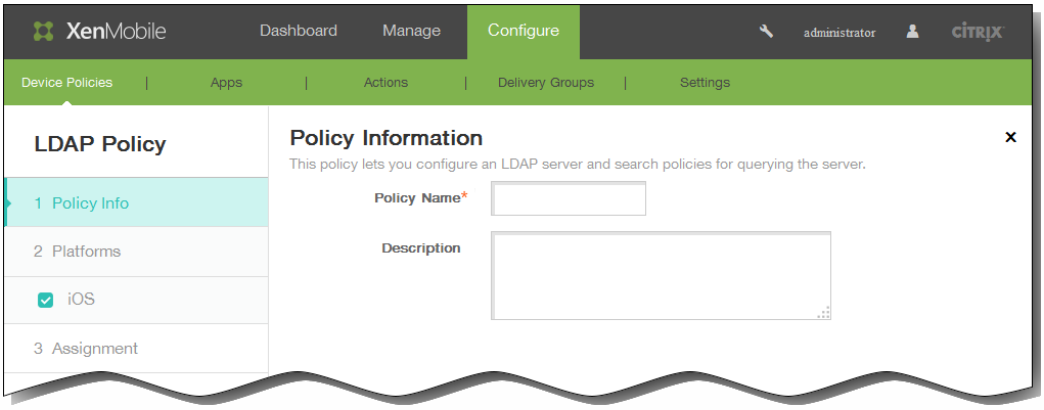
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



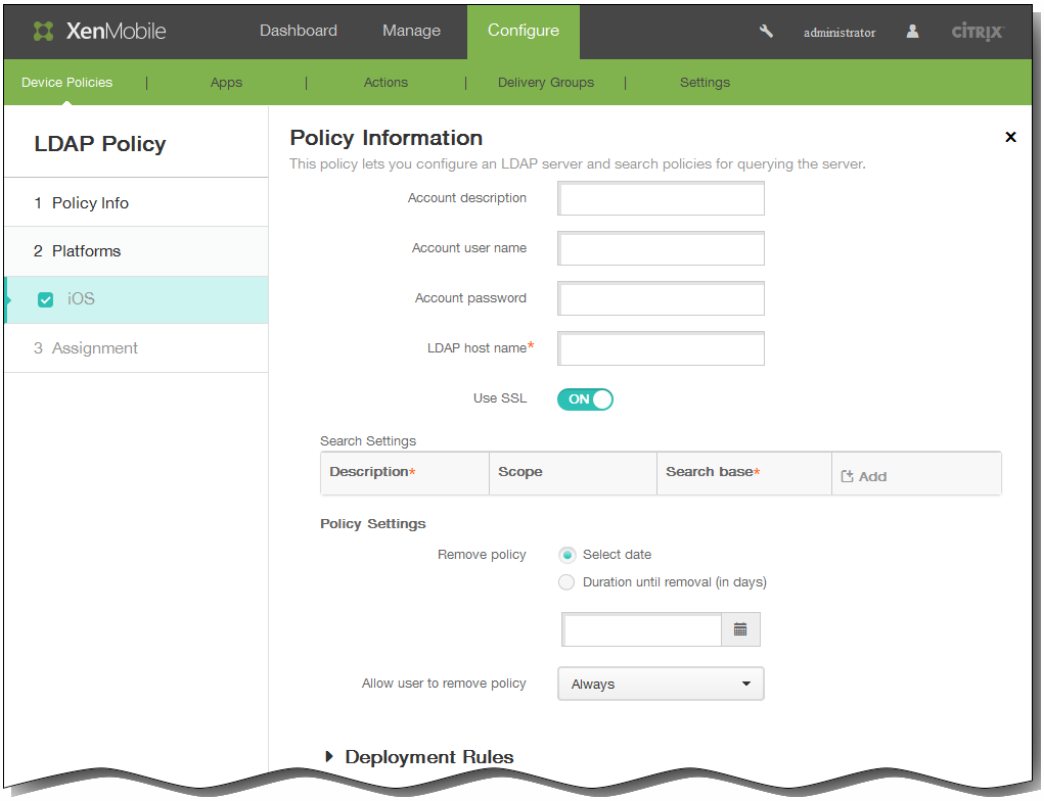
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。

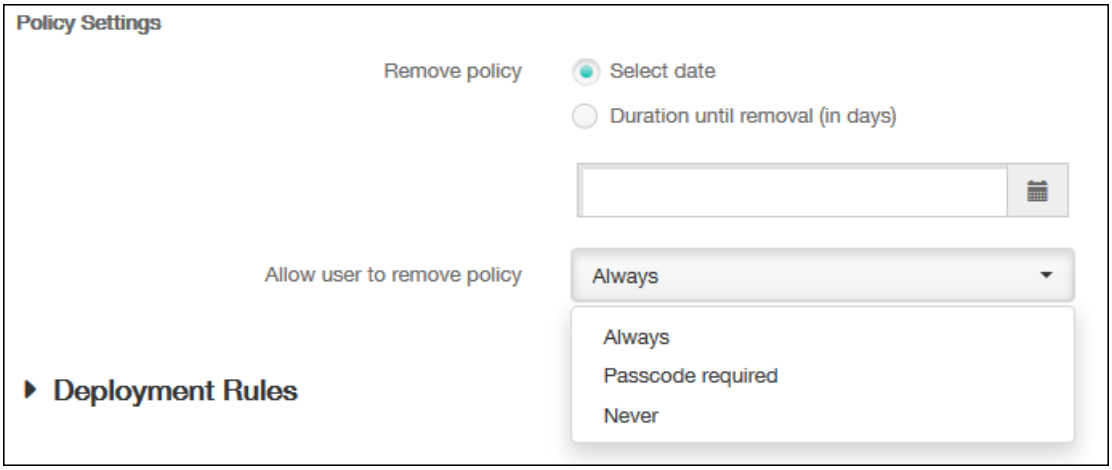


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户说明：输入可选帐户说明。
   2. 帐户用户名：输入可选用户名。
   3. 帐户密码：输入可选密码。 此选项仅适用于加密的配置文件。
   4. LDAP 主机名：输入 LDAP 服务器的主机名。 此字段为必填字段。

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. 为要添加的每个搜索设置重复步骤 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。

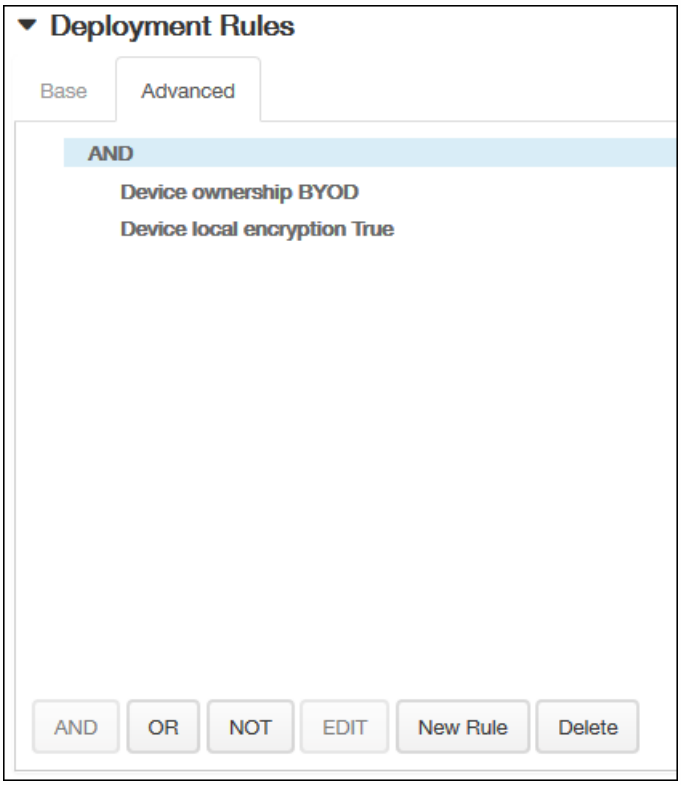


11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

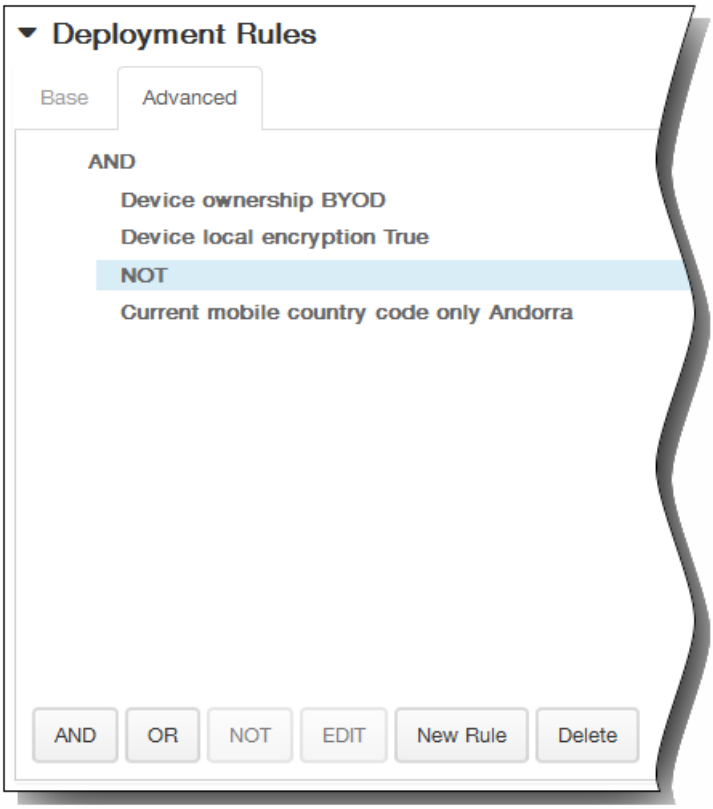
2. 单击新建规则以定义条件。
3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。

2. 单击高级选项卡以使用布尔选项组合规则。

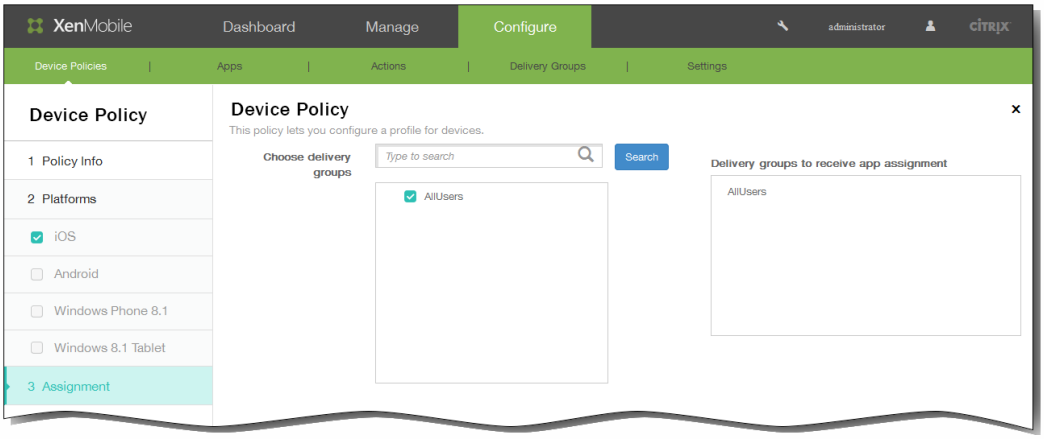


将显示您在基础选项卡上选择的条件。

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。



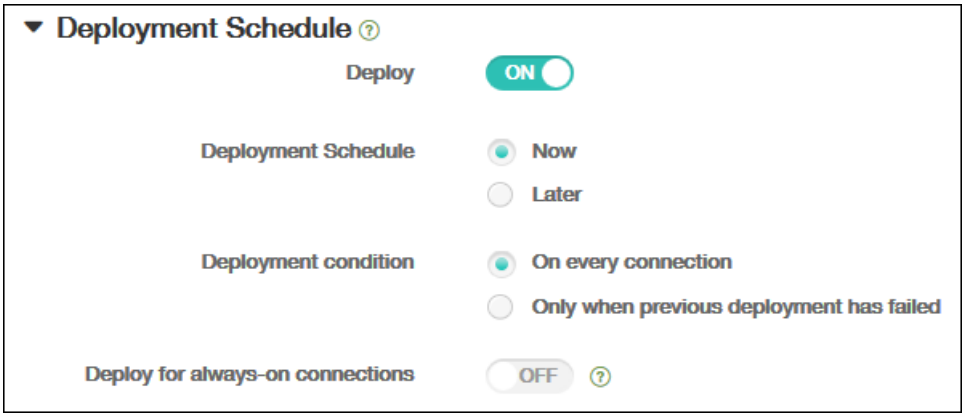
12. 单击下一步。 此时将显示 LDAP 策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

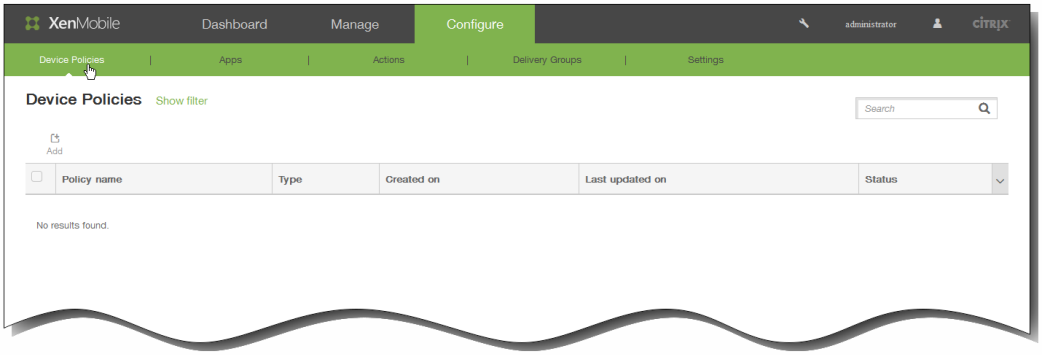
添加适用于 iOS 的 Single Sign-On 帐户设备策略

Oct 22, 2015

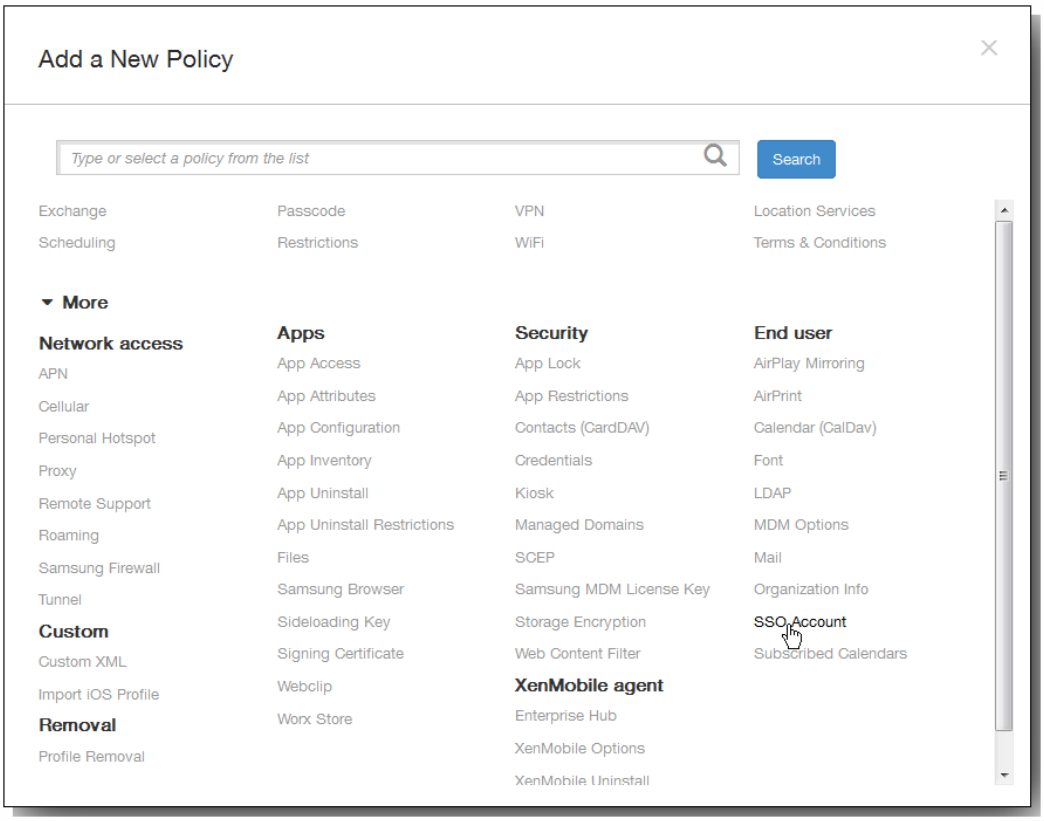
在 XenMobile 中创建 Single Sign-On (SSO) 帐户，使用户只需登录设备一次，即可从各种应用程序访问 XenMobile 和内部的公司资源。用户无需在设备上存储任何凭据。可以跨应用程序（包括 App Store 中的应用程序）使用此 SSO 帐户企业用户凭据。此策略专为 Kerberos 身份验证后端设计。

注意：此策略仅适用于 iOS 7.0 及更高版本。

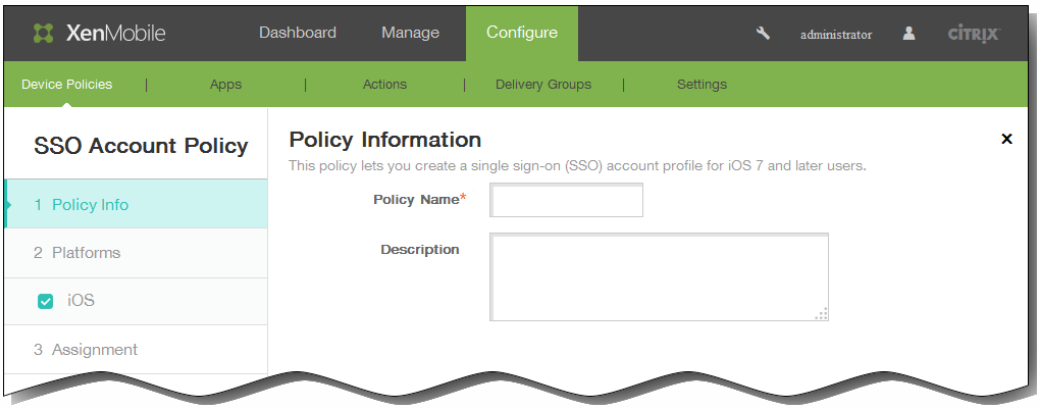
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



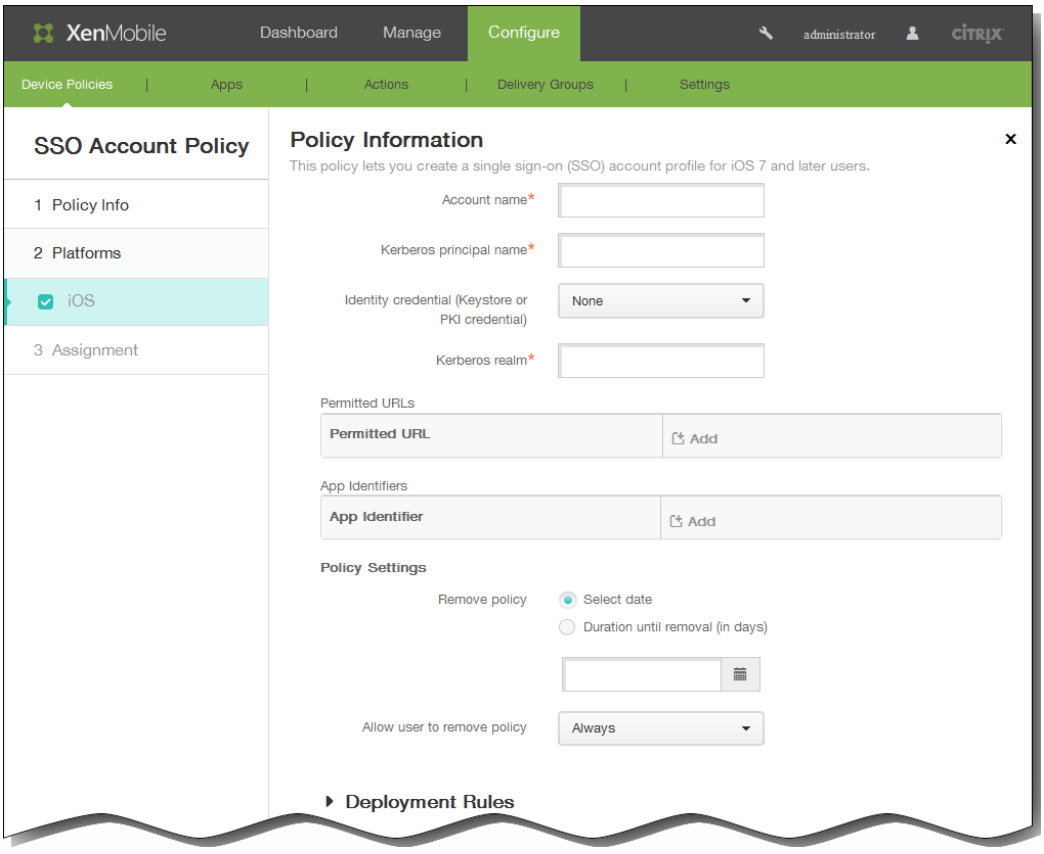
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



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。

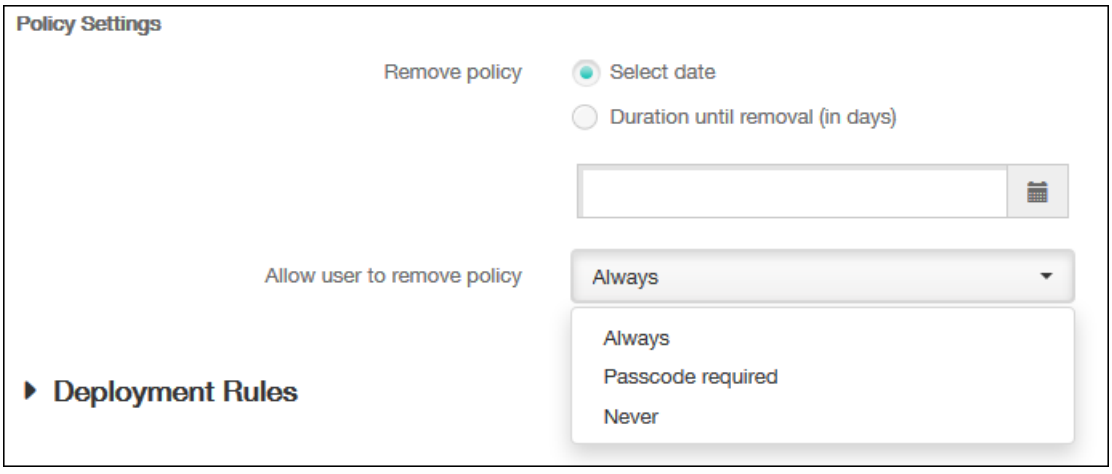


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 帐户名称：输入显示在用户设备上的 Kerberos SSO 帐户名称。 此字段为必填字段。
   2. Kerberos 主体名称：输入 Kerberos 主体名称。 此字段为必填字段。

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 URL 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.。

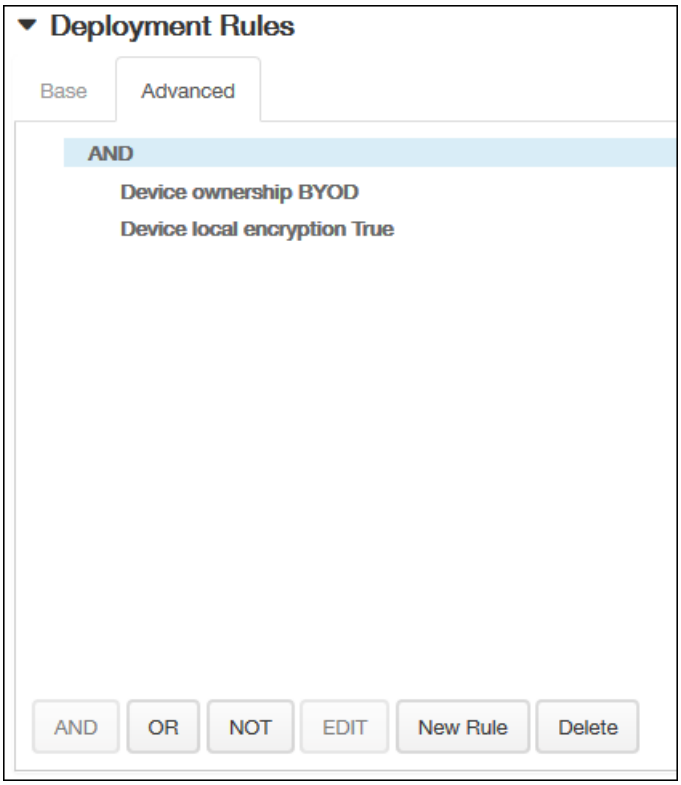
    注意：要删除现有 URL 或应用程序标识符，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击删除以删除列表，或单击取消以保留此列表。
    要编辑现有 URL 或应用程序标识符，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

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。



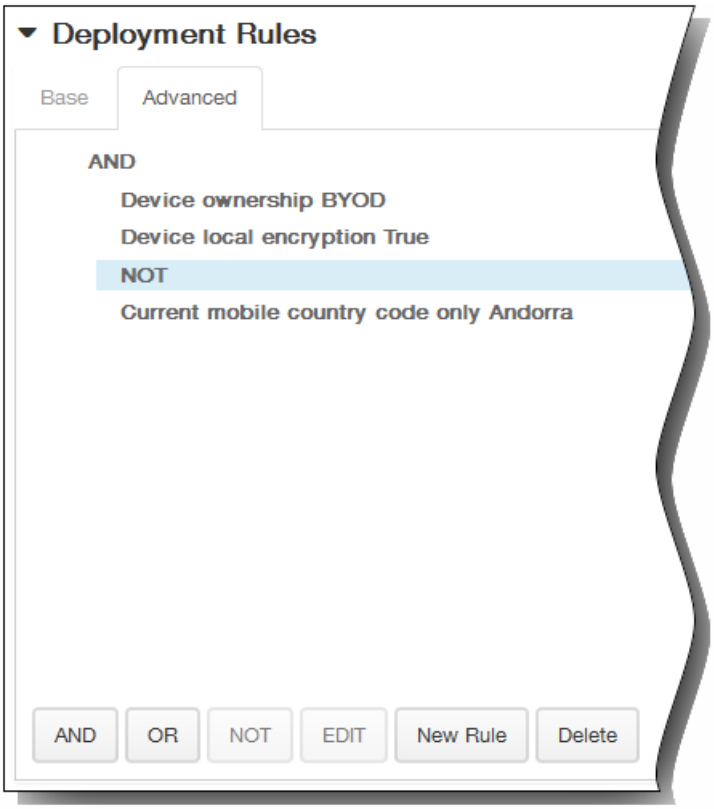
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

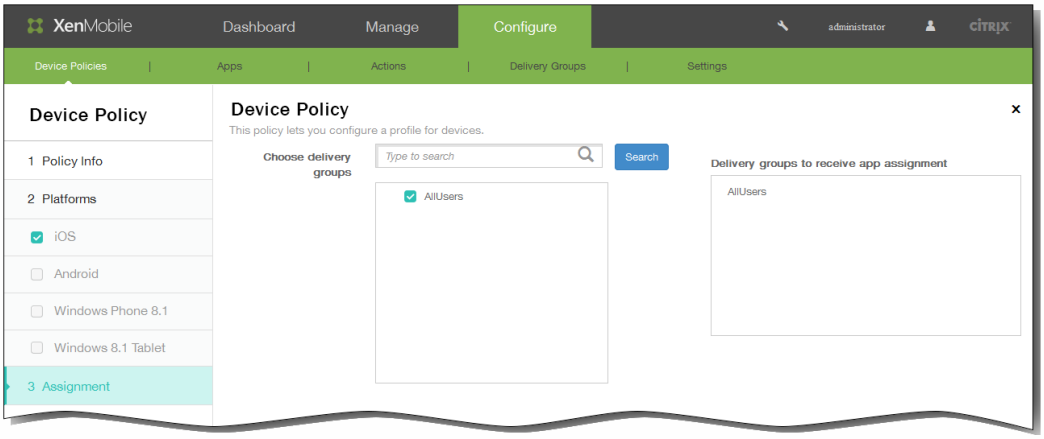


   将显示您在基础选项卡上选择的条件。
3. 您可以使用更多高级布尔逻辑来组合、编辑或添加规则。
   1. 单击 AND、OR 或 NOT。
   2. 在显示的列表中，选择要添加到规则中的条件，然后单击右侧的加号 (+) 将条件添加到规则中。
      您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。

   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。



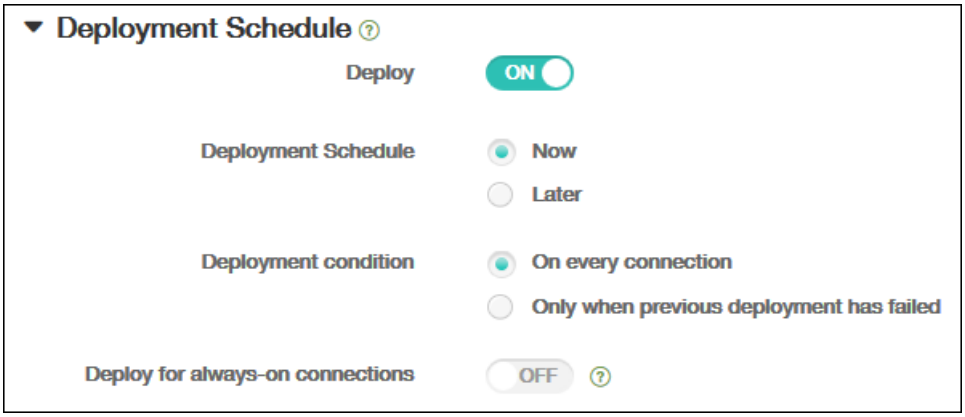
12. 单击下一步。 此时将显示 SSO 帐户策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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。

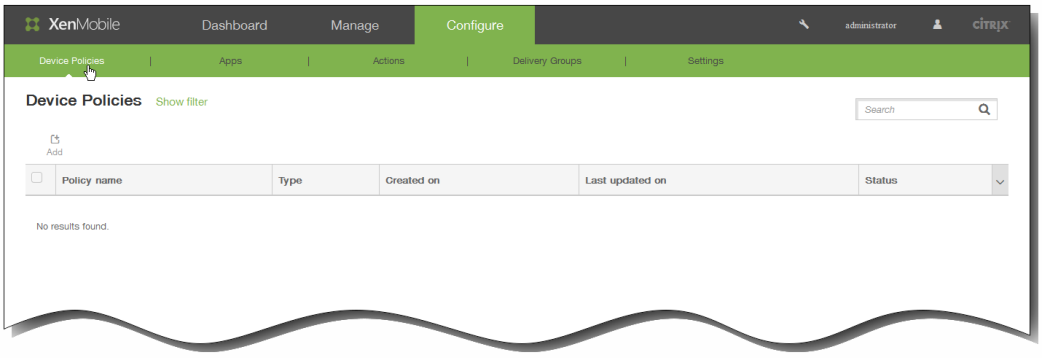
添加适用于 iOS 的已订阅的日历设备策略

Oct 22, 2015

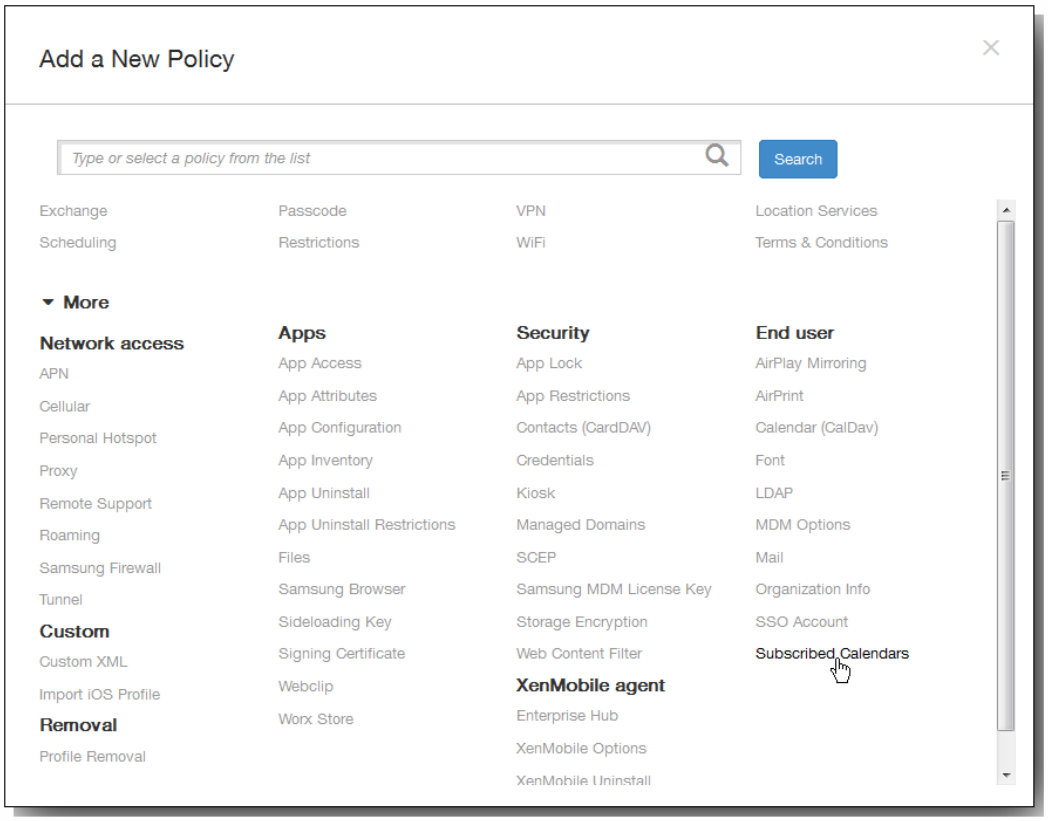
您可以在 XenMobile 中添加一个设备策略，以便在用户的 iOS 设备上向日历列表中添加已订阅的日历。www.apple.com/downloads/macosx/calendars 提供了您可以订阅的公共日历列表。

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。

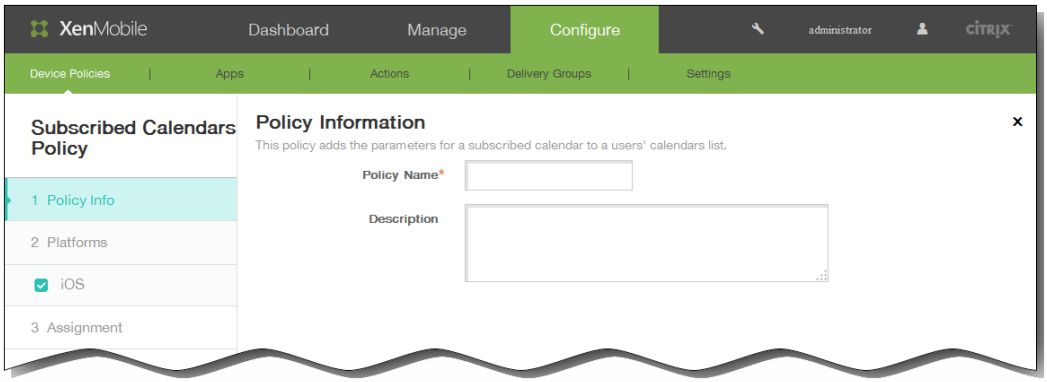
1. 在 XenMobile 控制台中，单击配置 > 设备策略。 此时将显示设备策略页面。



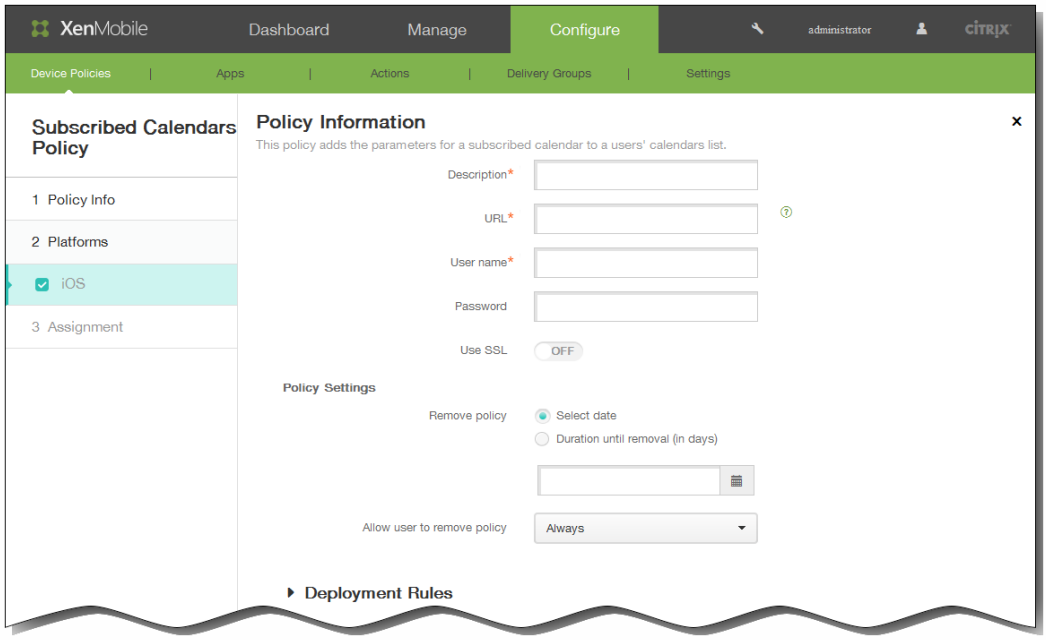
2. 单击添加添加新策略。 此时将显示添加新策略对话框。



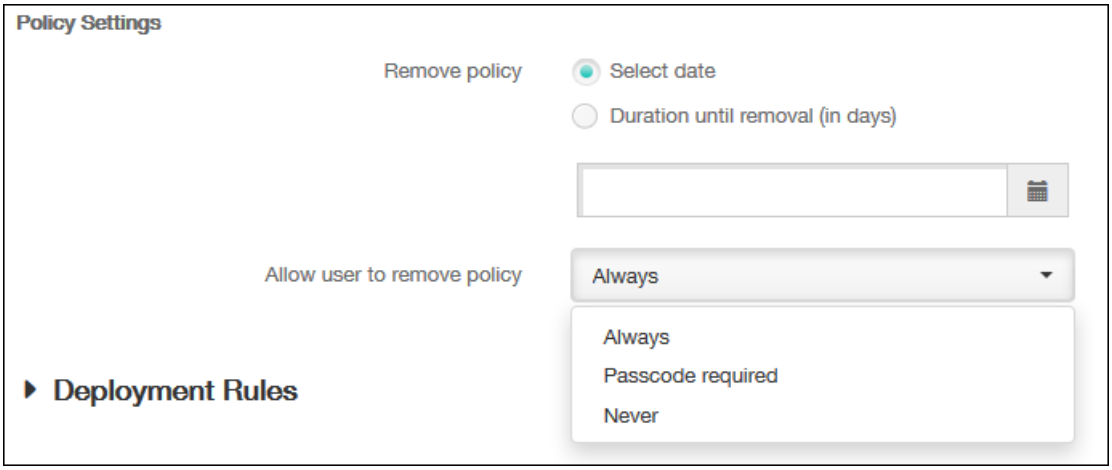
3. 单击更多，然后在最终用户下面，单击已订阅的日历。 此时将显示“已订阅的日历”策略页面。



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。

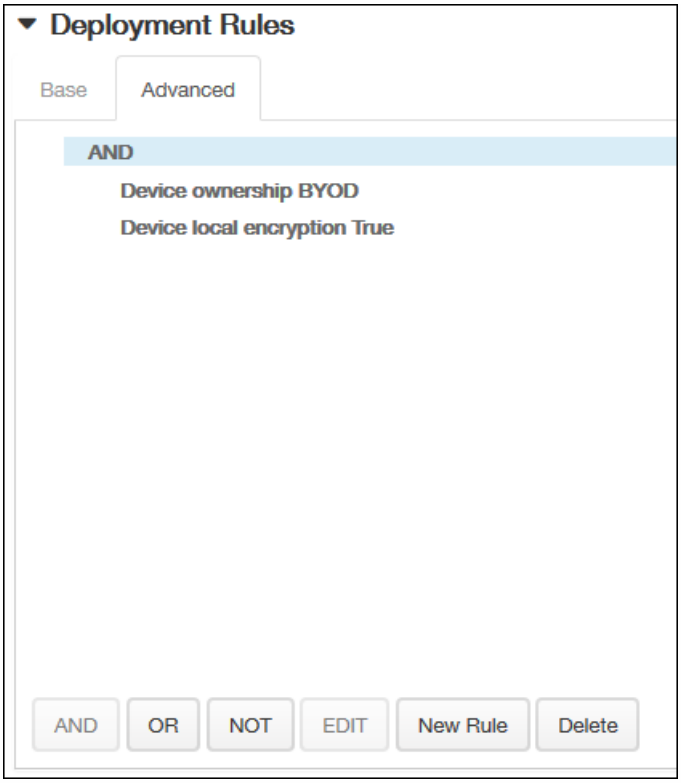


6. 在 iOS 平台信息页面上，输入以下信息：
   1. 说明：输入日历的说明。 此字段为必填字段。
   2. URL：输入日历 URL。 可以输入 iCalendar 文件 (.ics) 的 webcal:// URL 或 http:// 链接。 此字段为必填字段。
   3. 用户名：输入用户的登录名称。 此字段为必填字段。
   4. 密码：输入可选用户密码。
   5. 使用 SSL：选择是否使用安全套接字层连接到日历。 默认设置为关
7. 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
8. 如果单击选择日期，请单击日历以选择具体删除日期。
9. 在允许用户删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



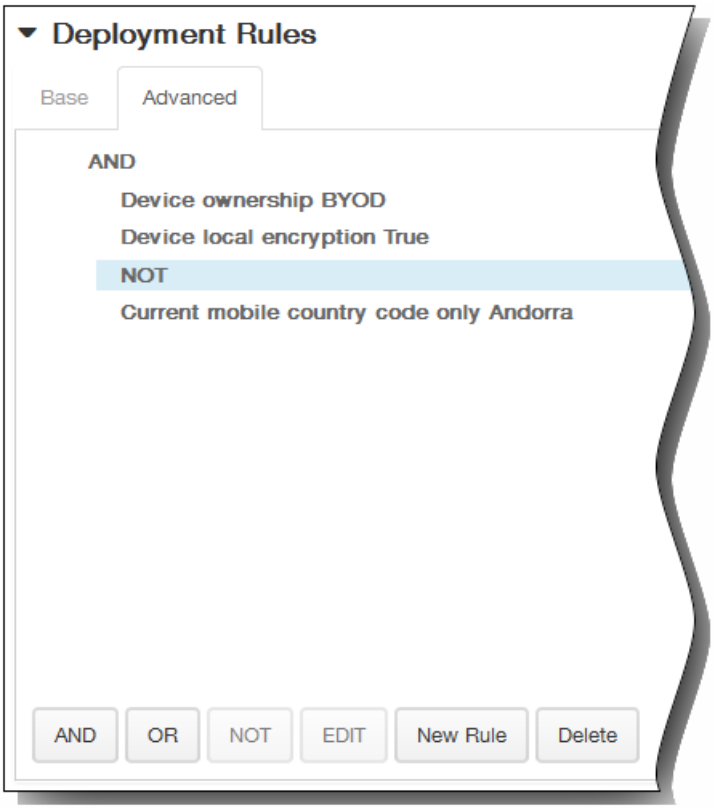
11. 展开部署规则，然后配置以下设置：默认情况下显示基础选项卡。

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。

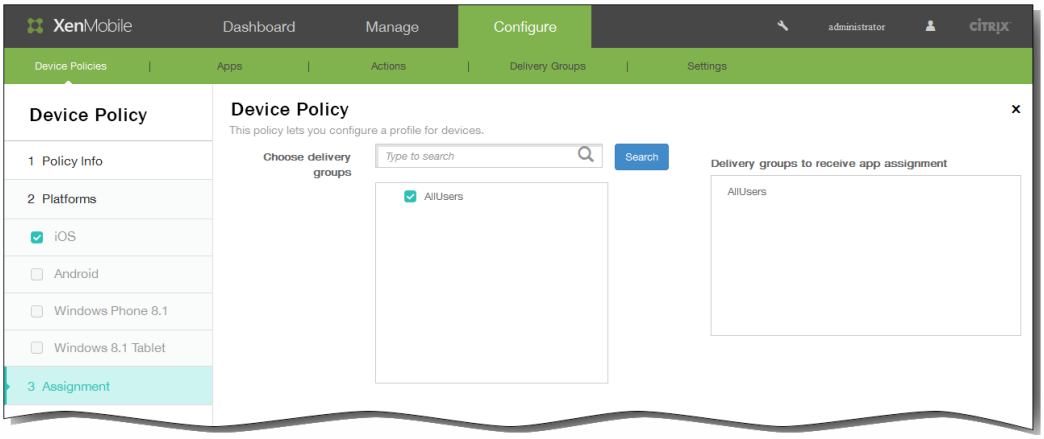


将显示您在基础选项卡上选择的条件。

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。



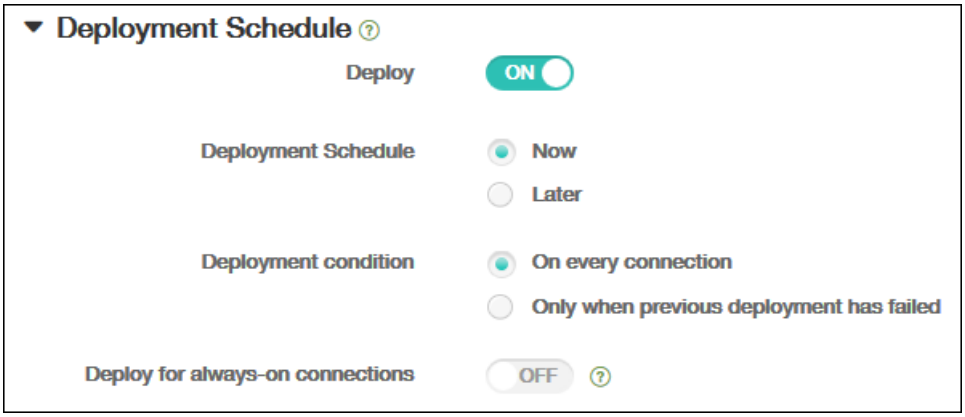
12. 单击下一步。 此时将显示“已订阅的日历”策略分配页面。
13. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。



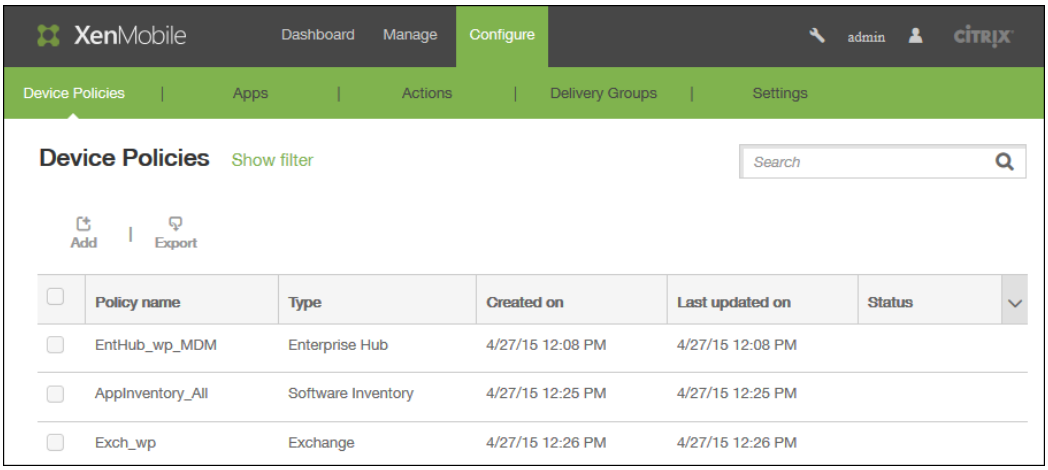
14. 展开部署计划，然后配置以下设置：
    1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。 如果选择关，无需配置其他选项。
    2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
    3. 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
    4. 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。 默认选项为每次连接时。
    5. 在为始终启用的连接部署旁边，单击开或关。 默认选项为关。

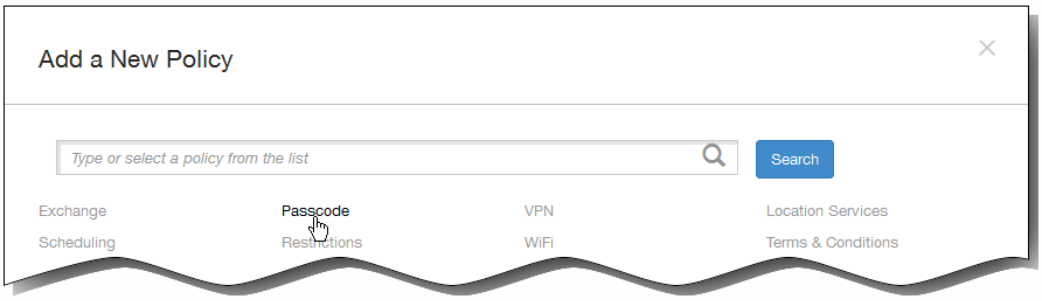
    注意：已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。

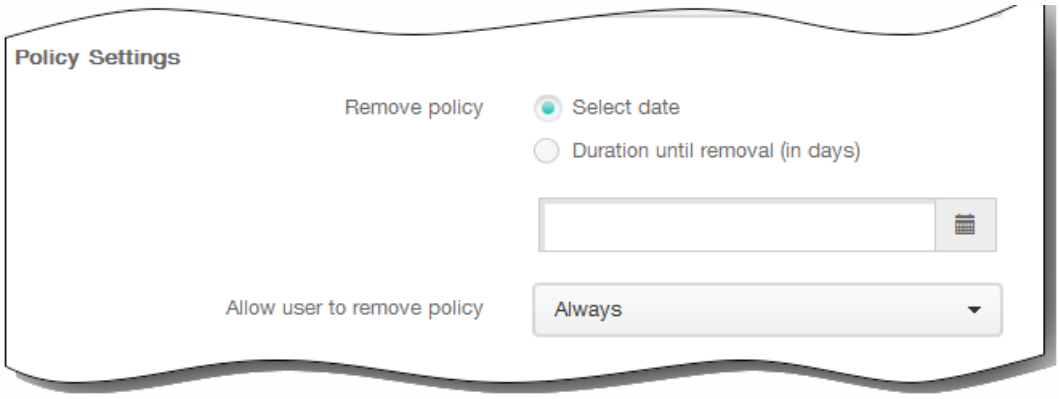
注意：配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。



15. 单击保存以保存此策略。







-
-
-
-
-
-

_____

___

-

  _____

-

-
-

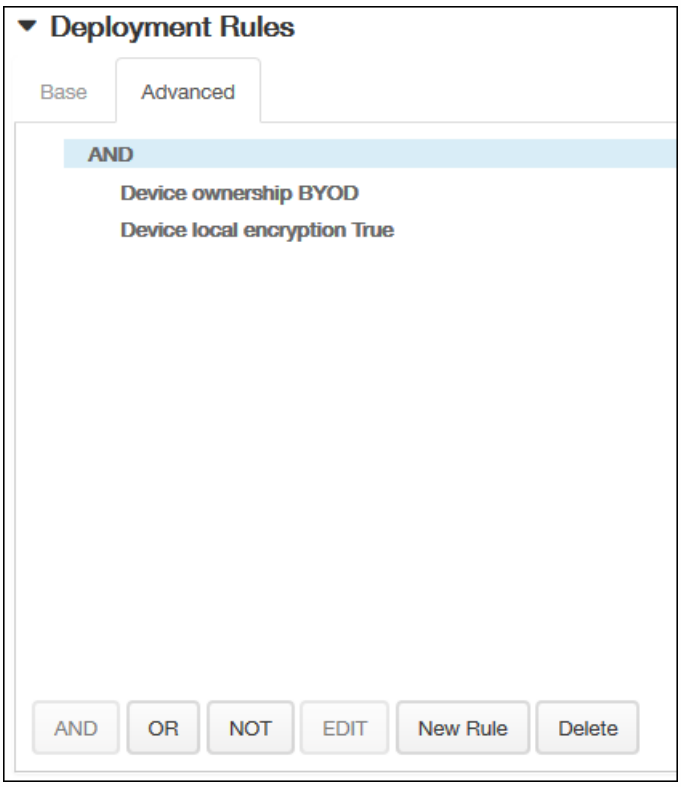
_____

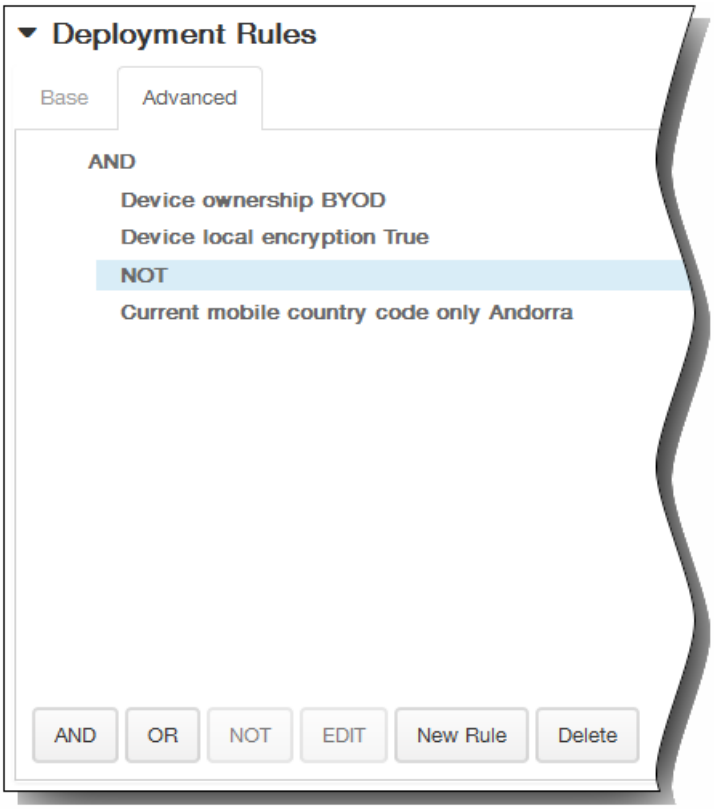
_____

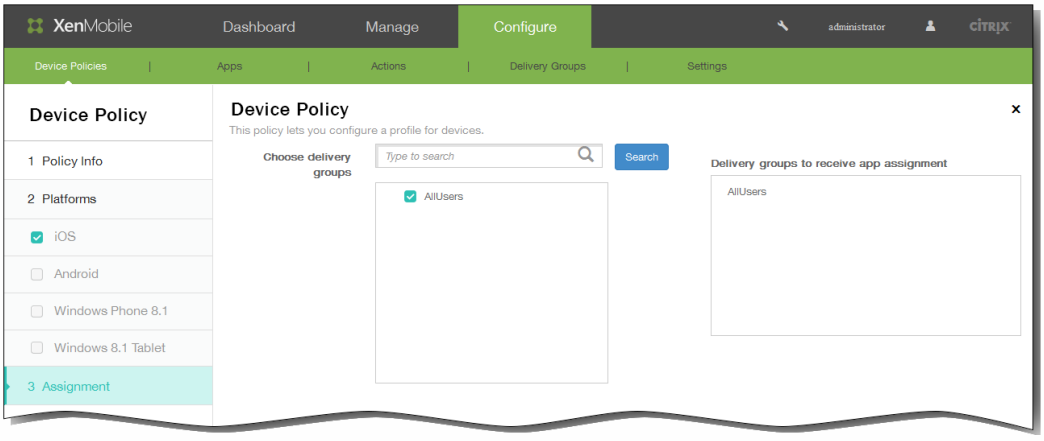
_____

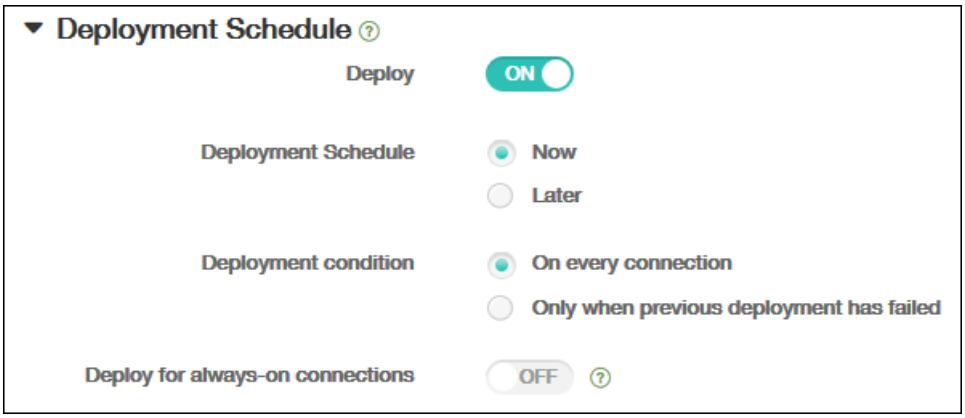
-

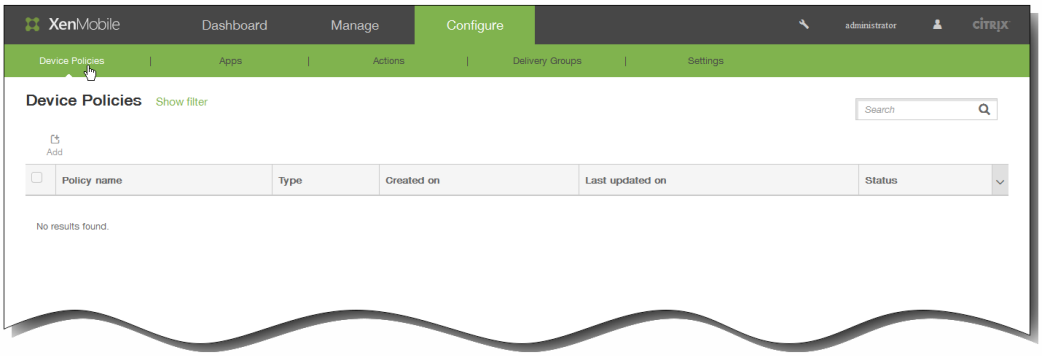
_____

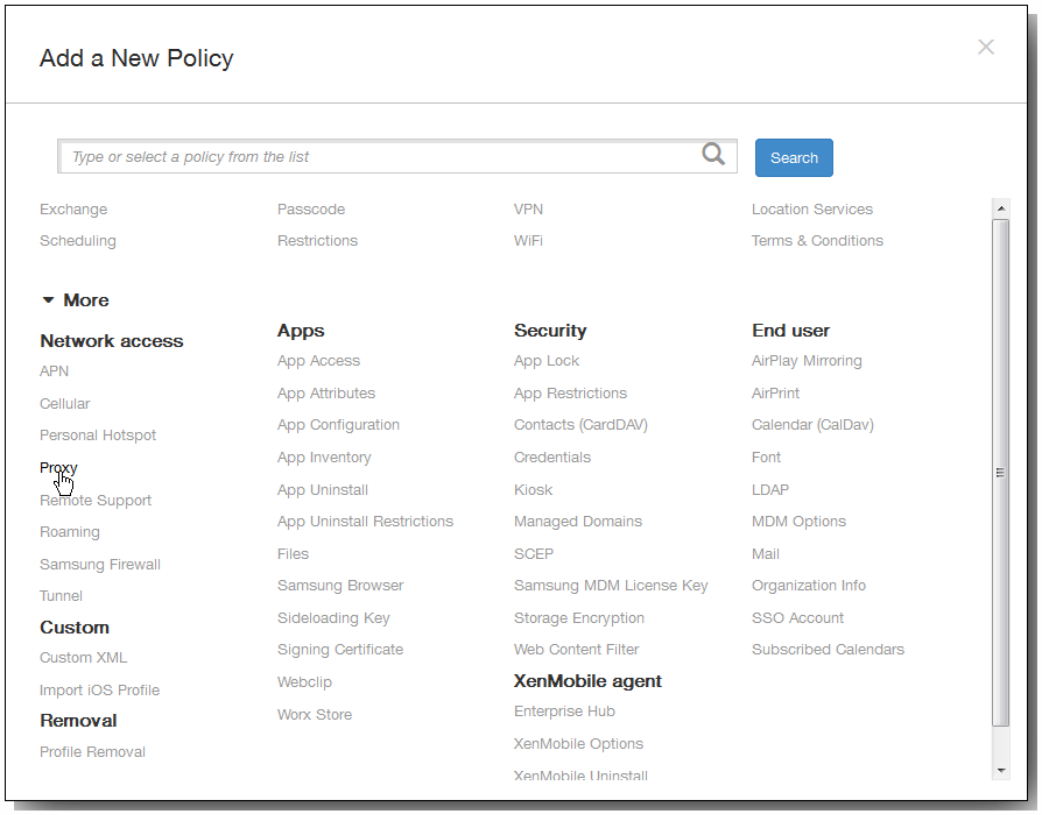


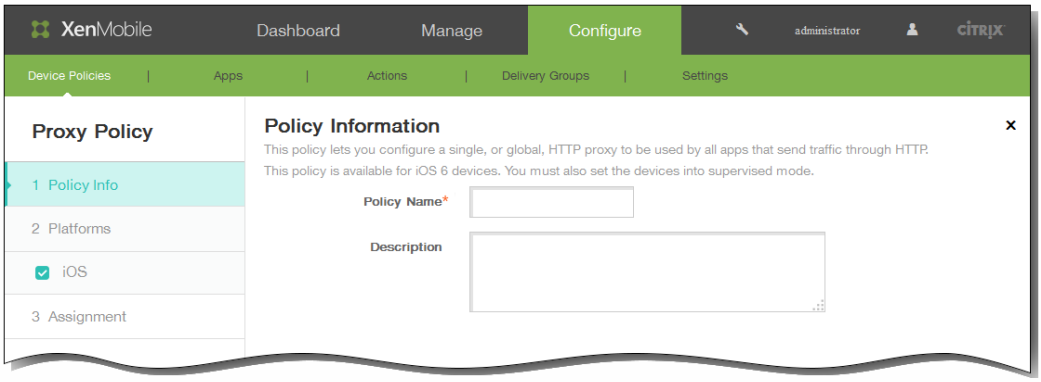


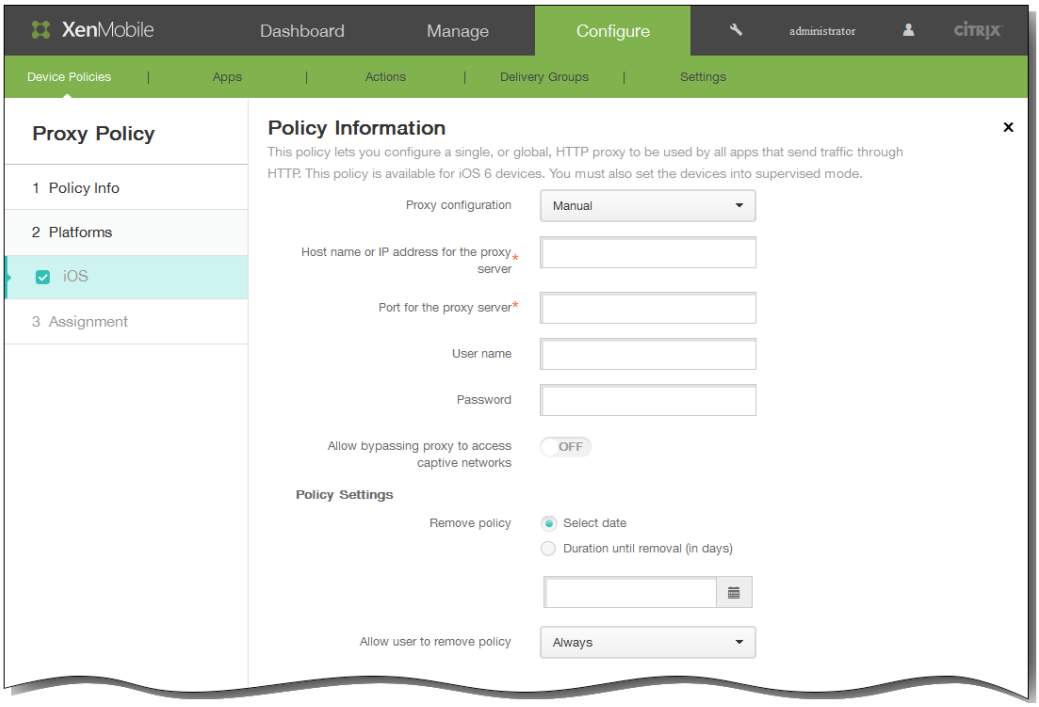


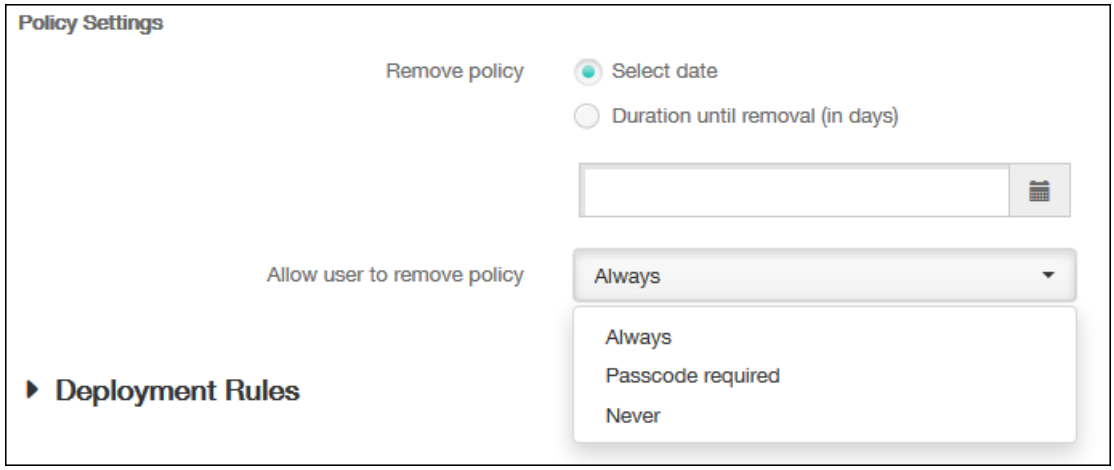


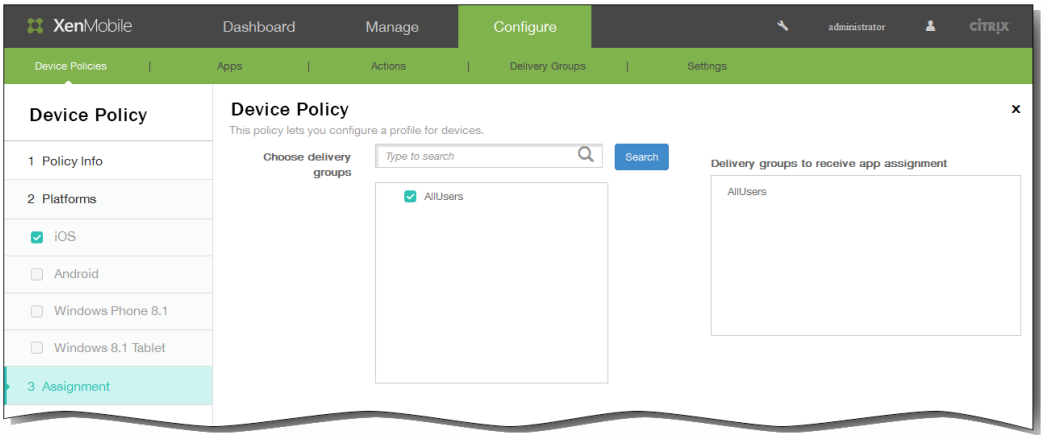


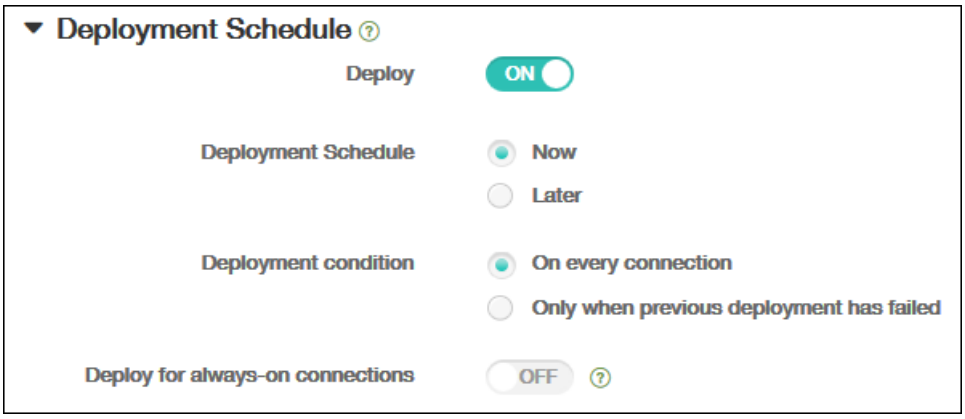




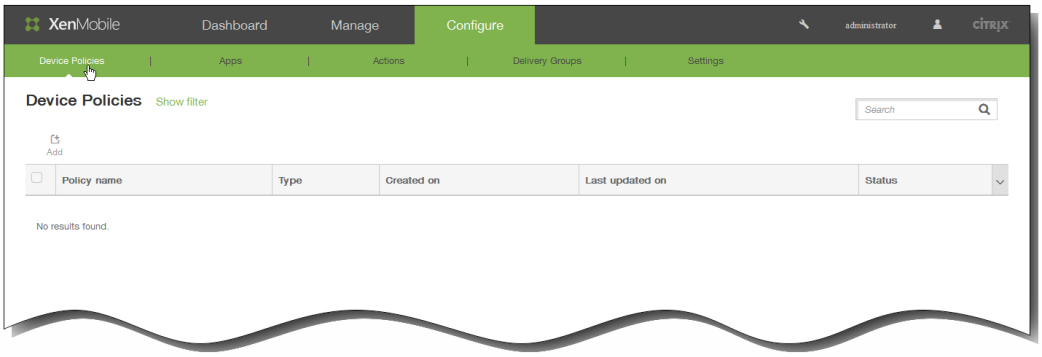


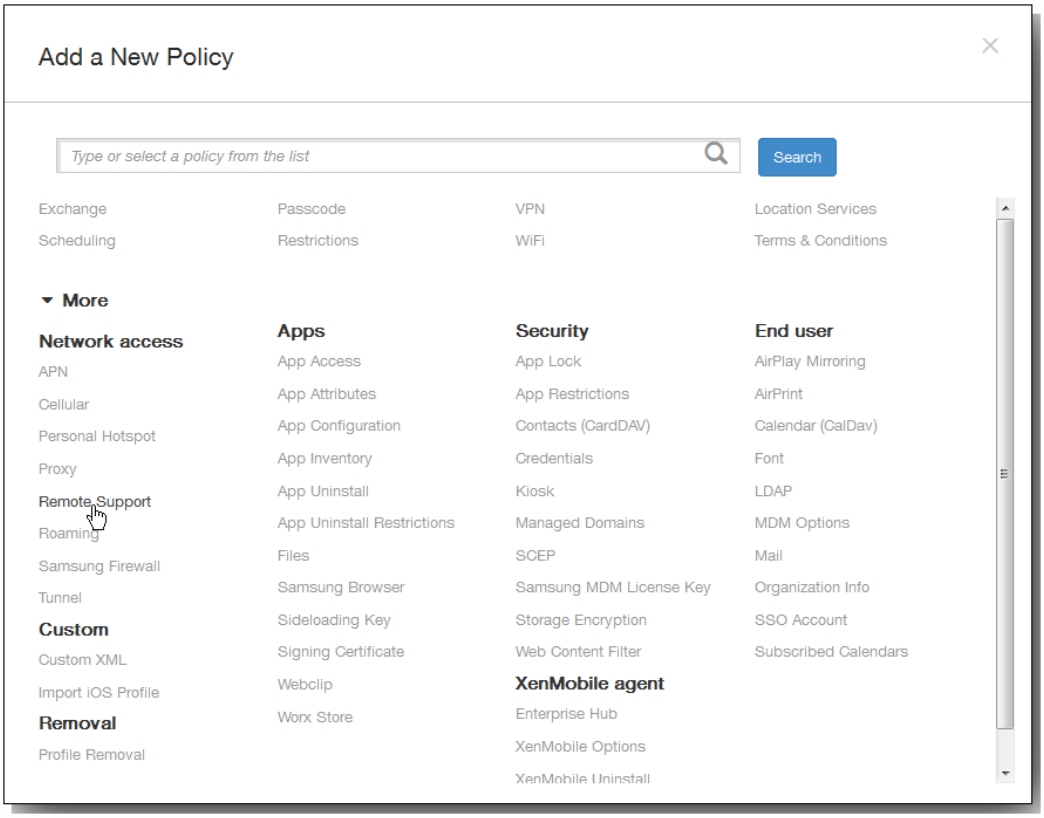


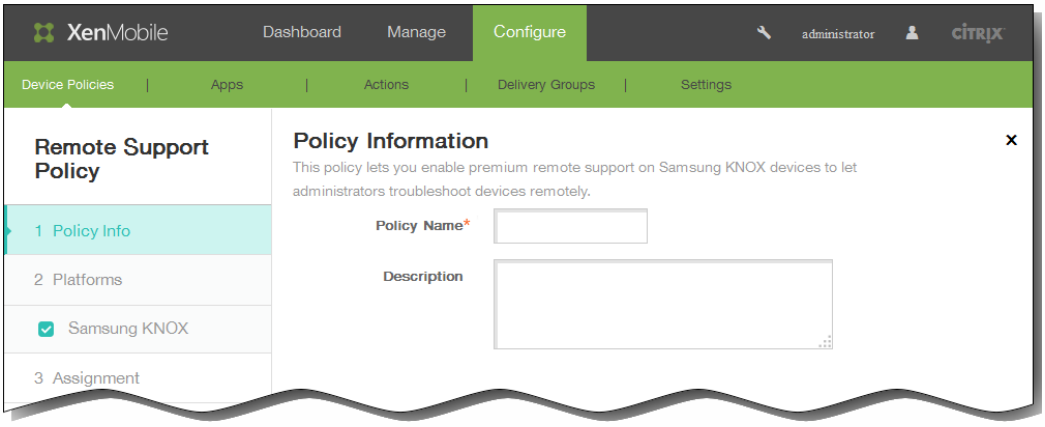


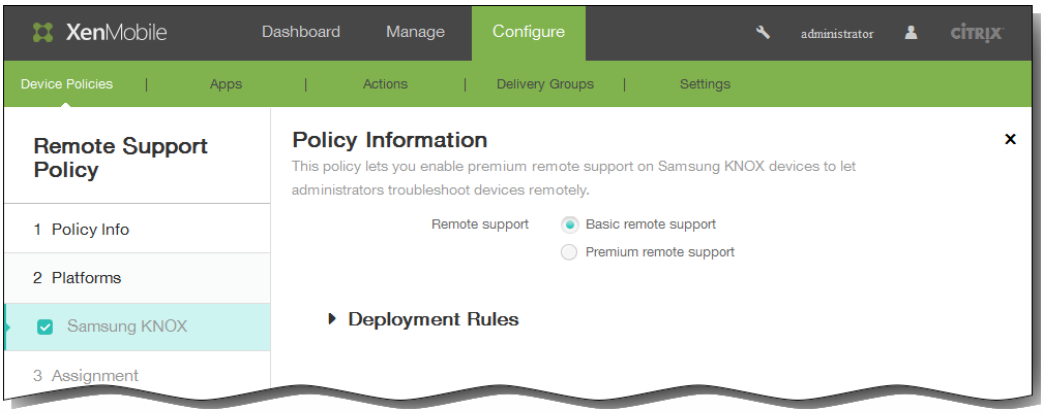


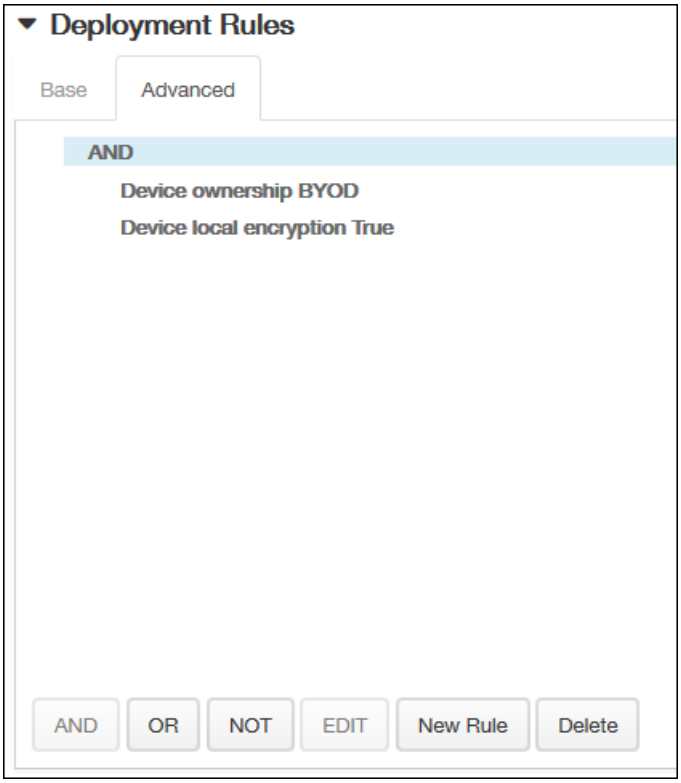
-
-
-
-
-

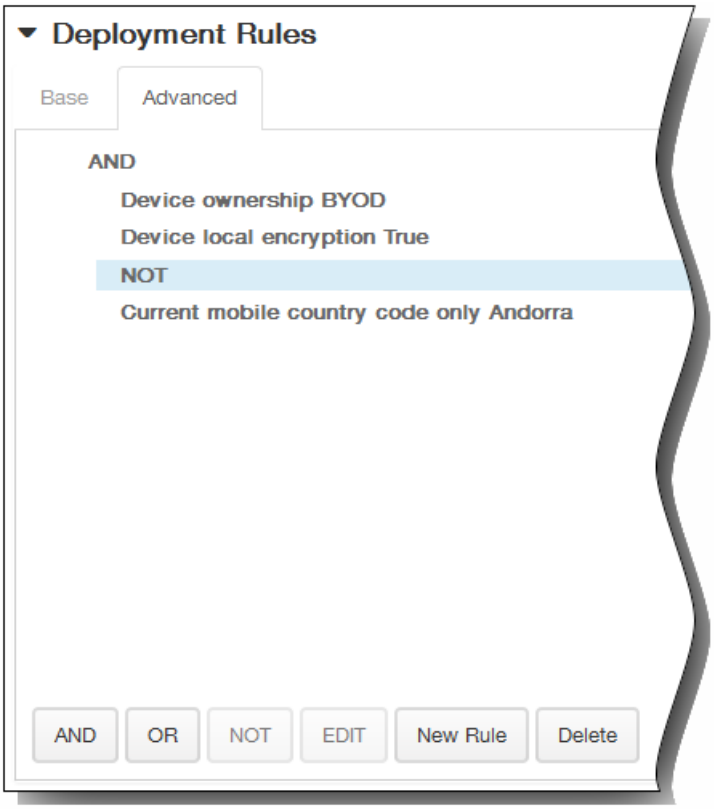


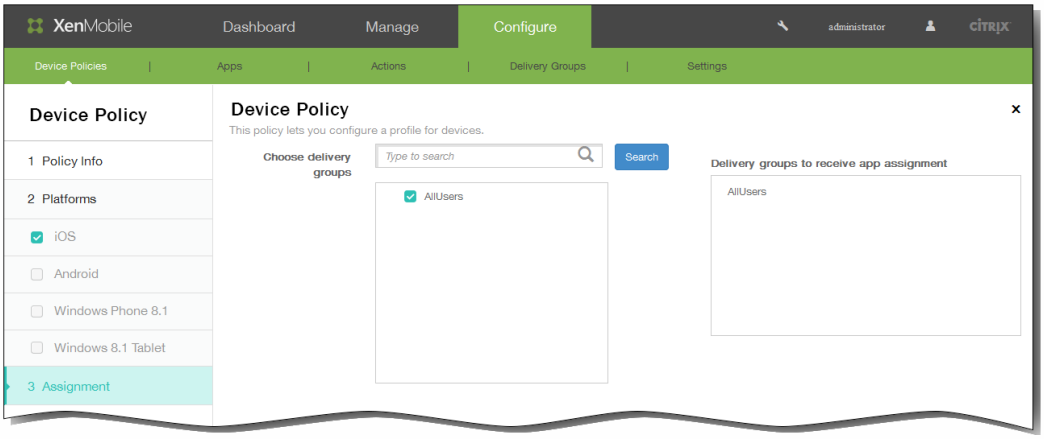


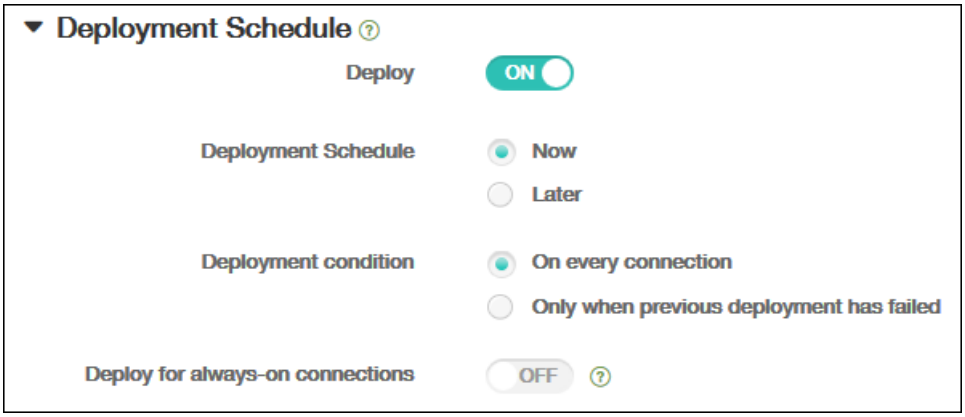




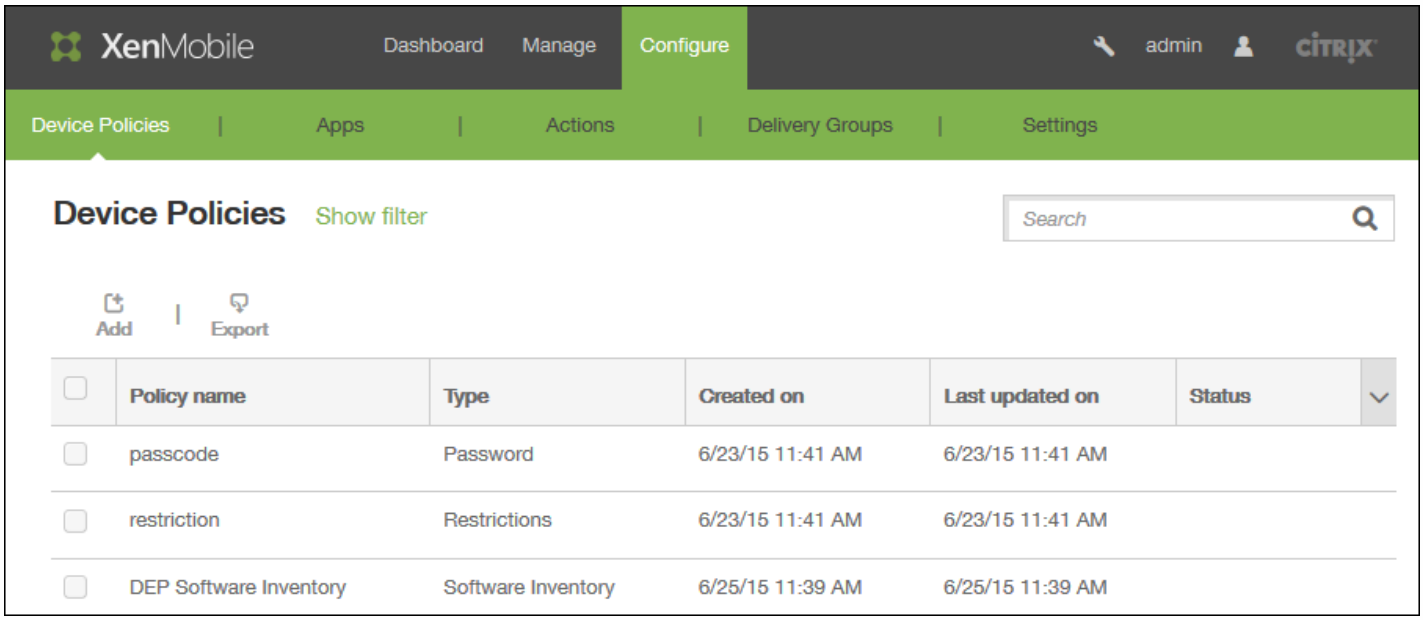


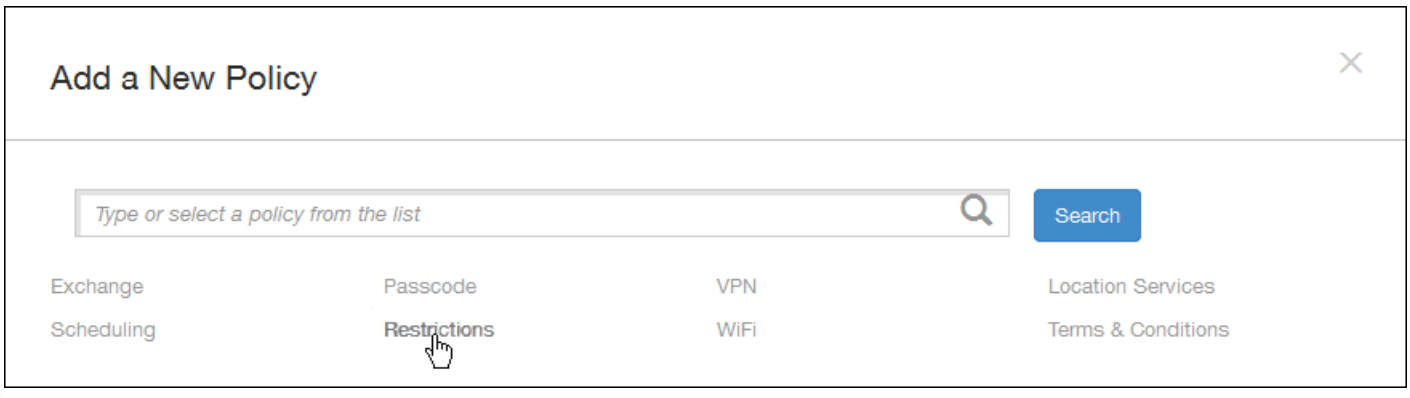


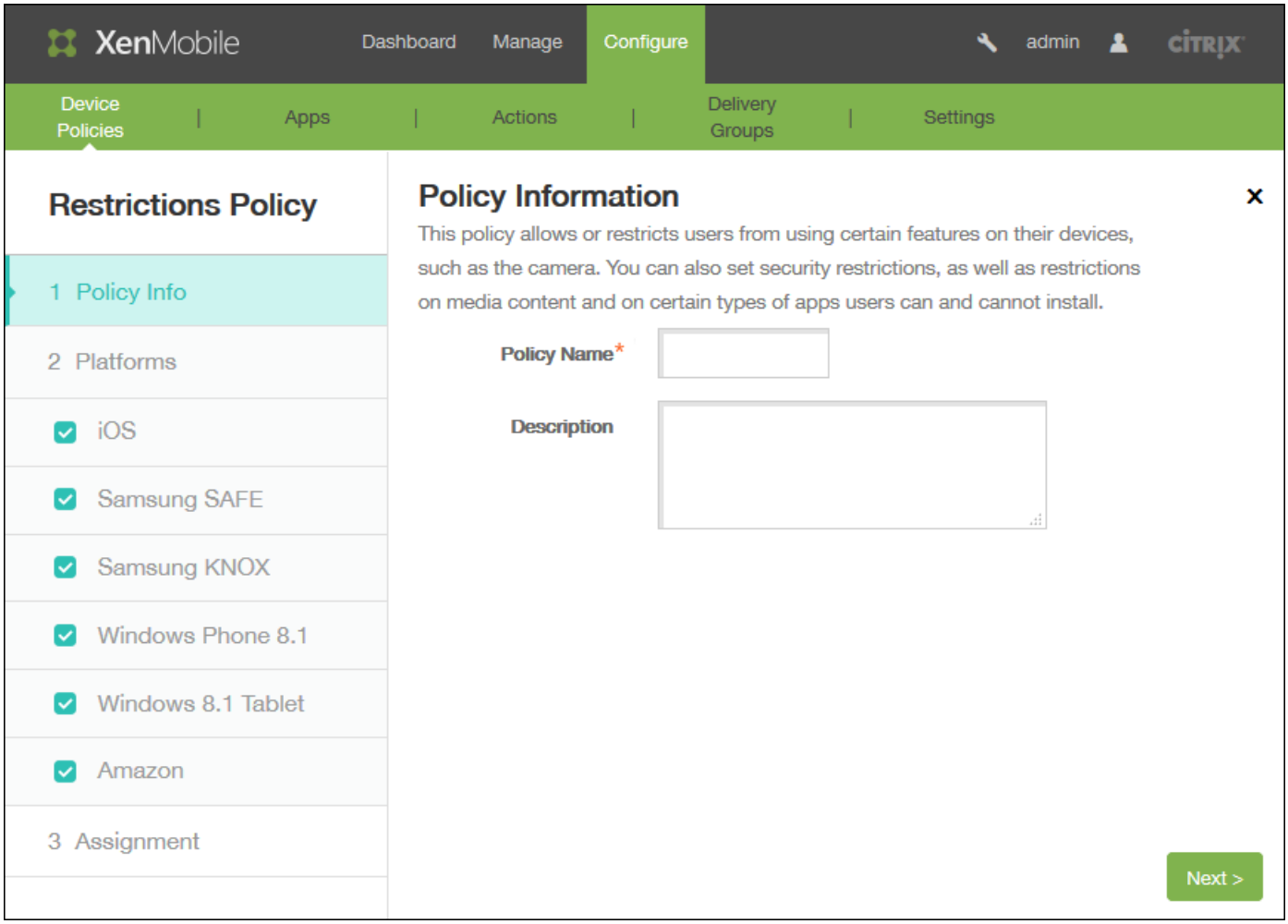




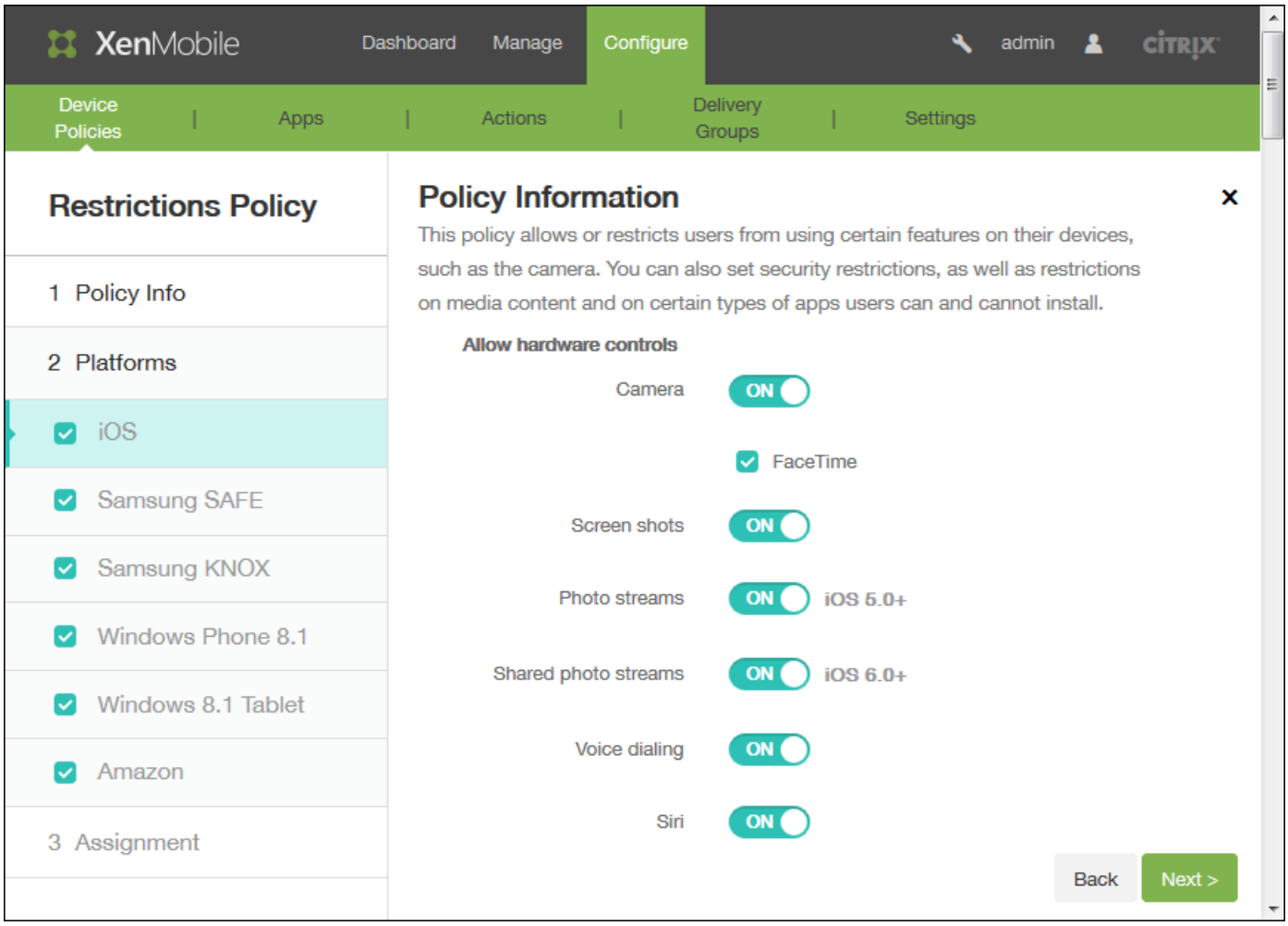
-
-



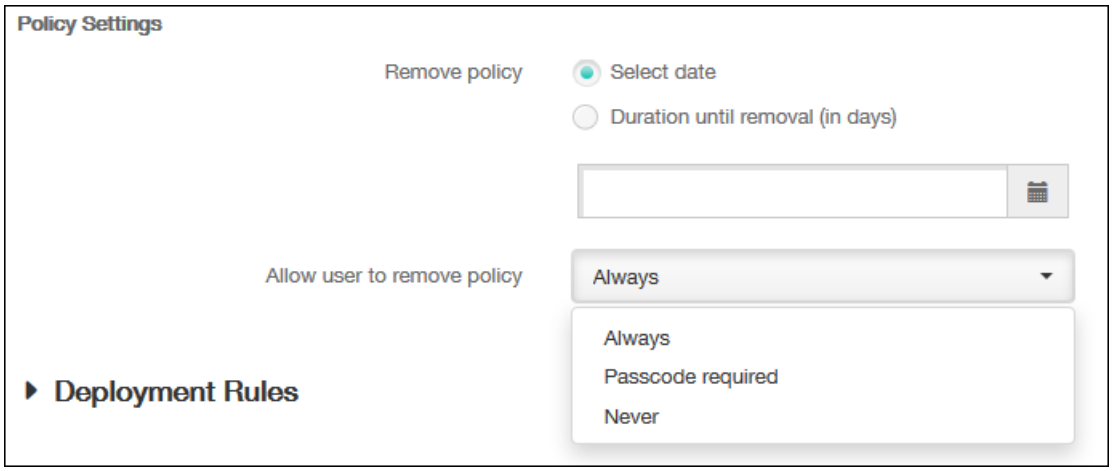


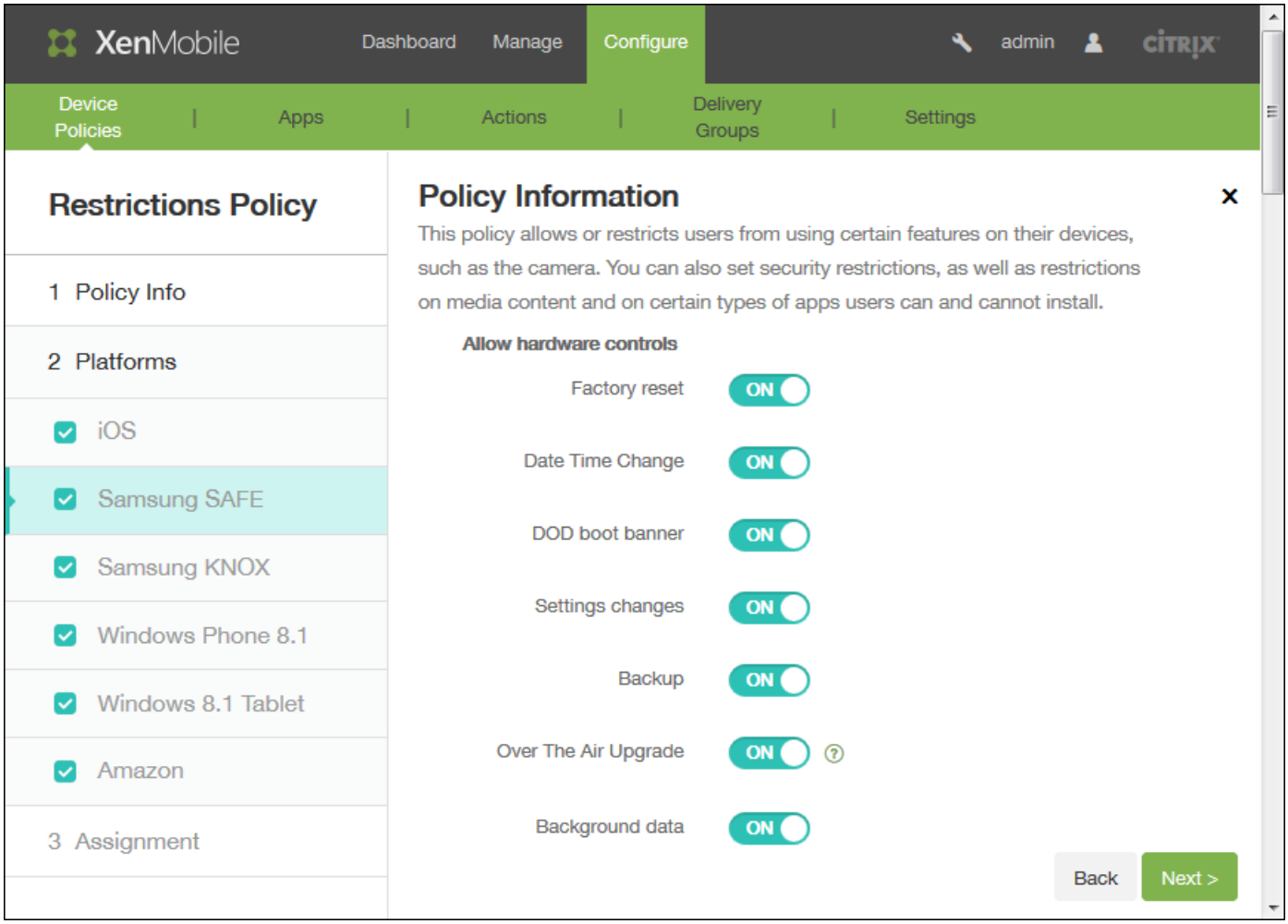


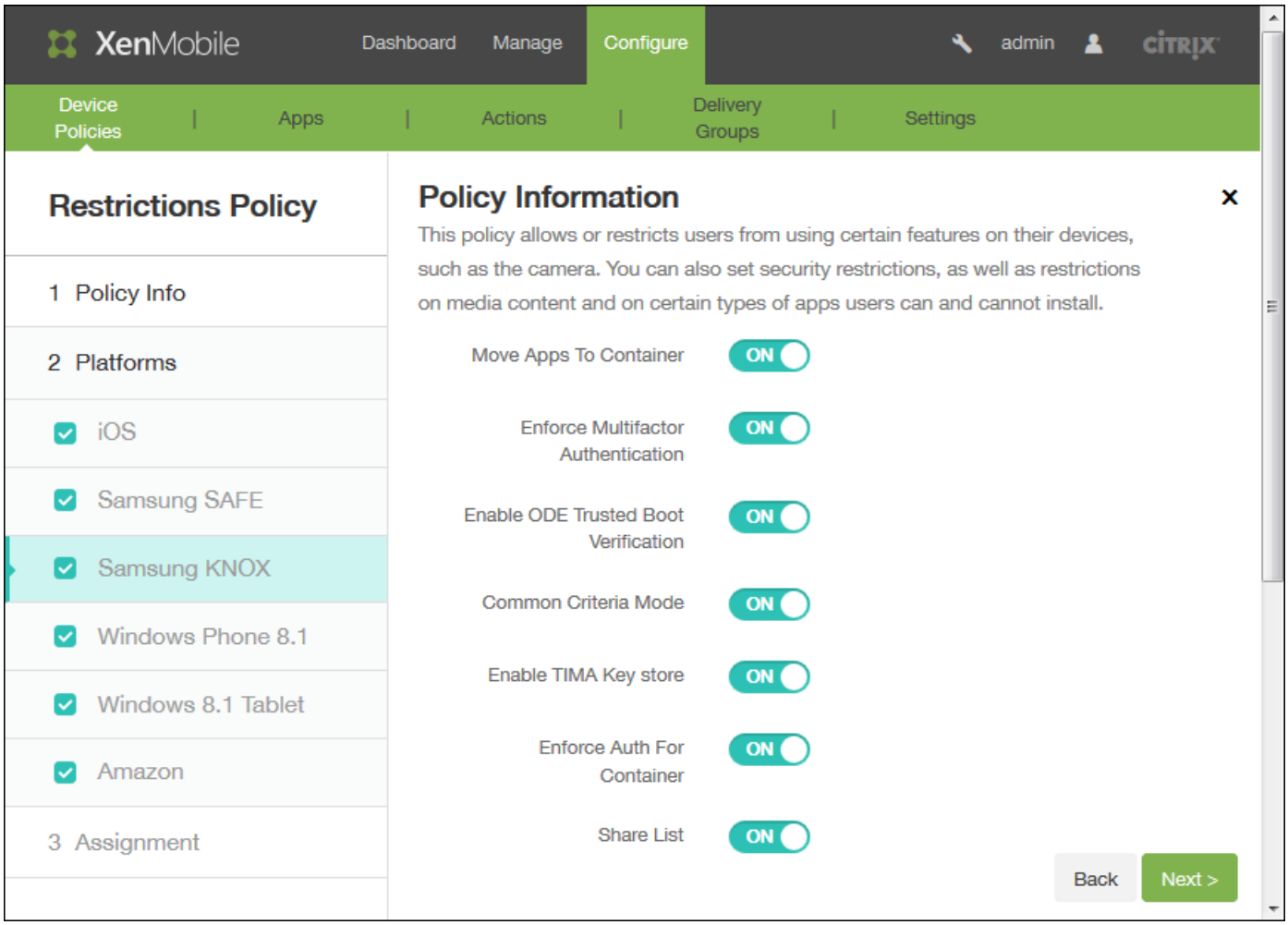
-
-



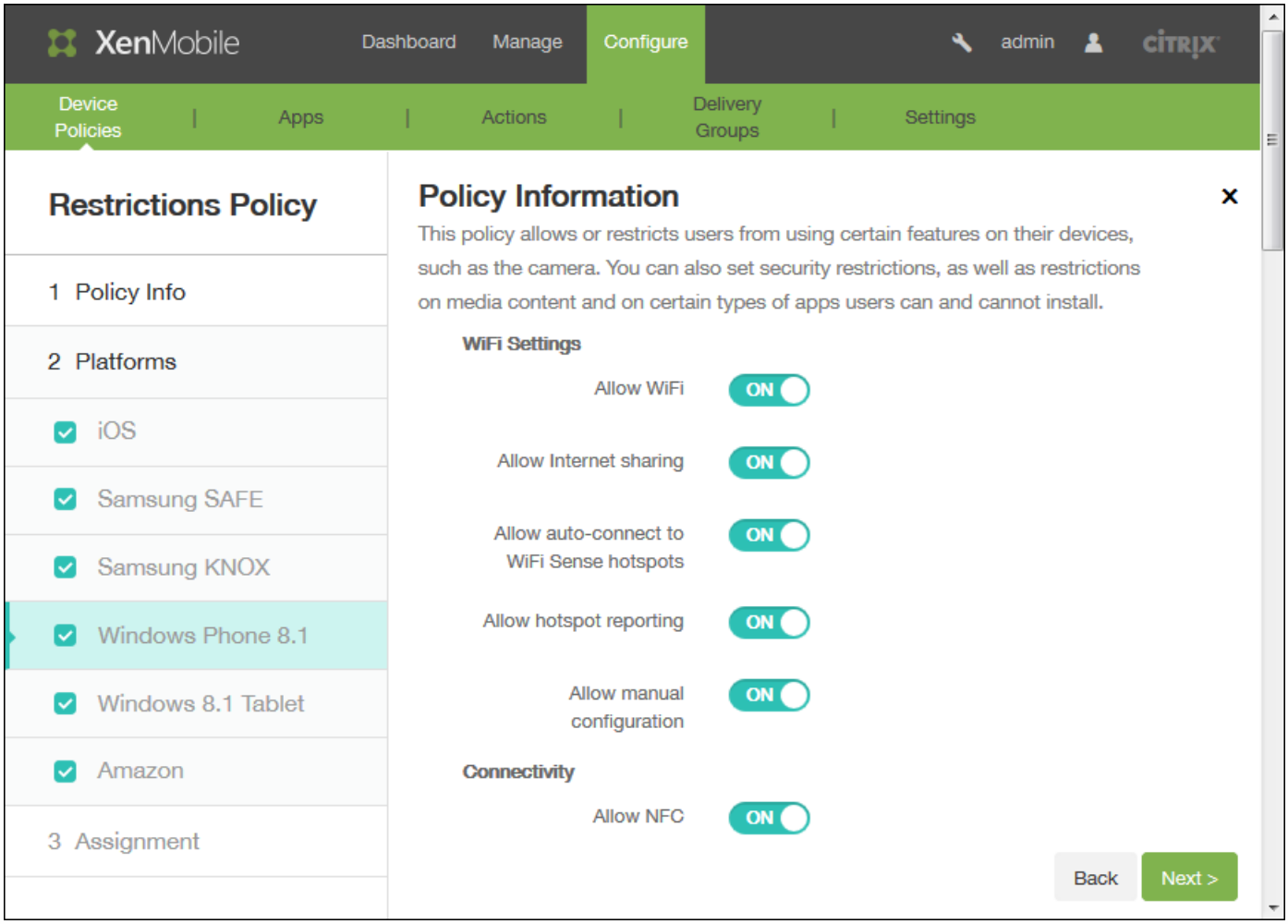
-
-
  -
  -
  -
  -
  -
  -
-



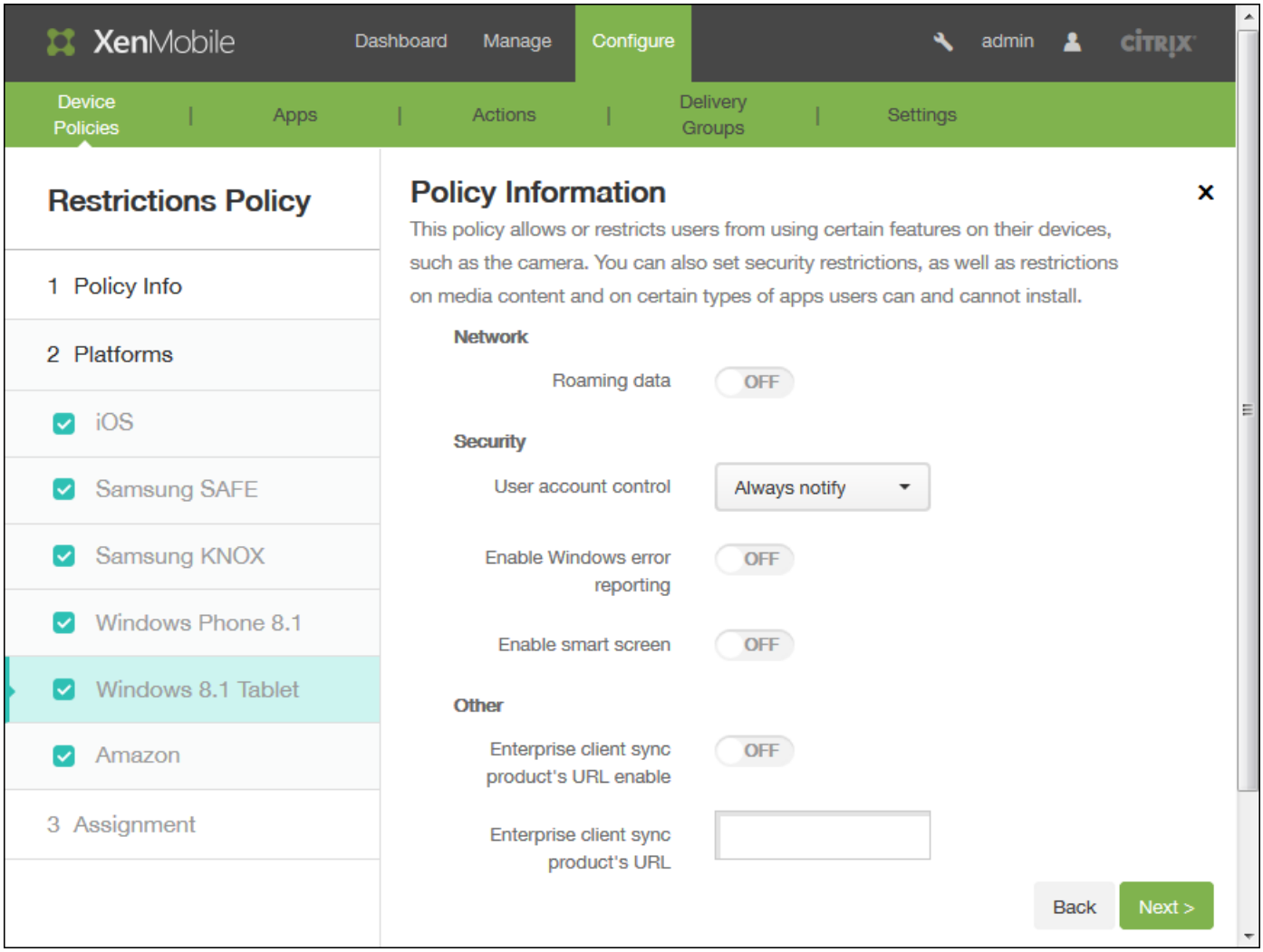


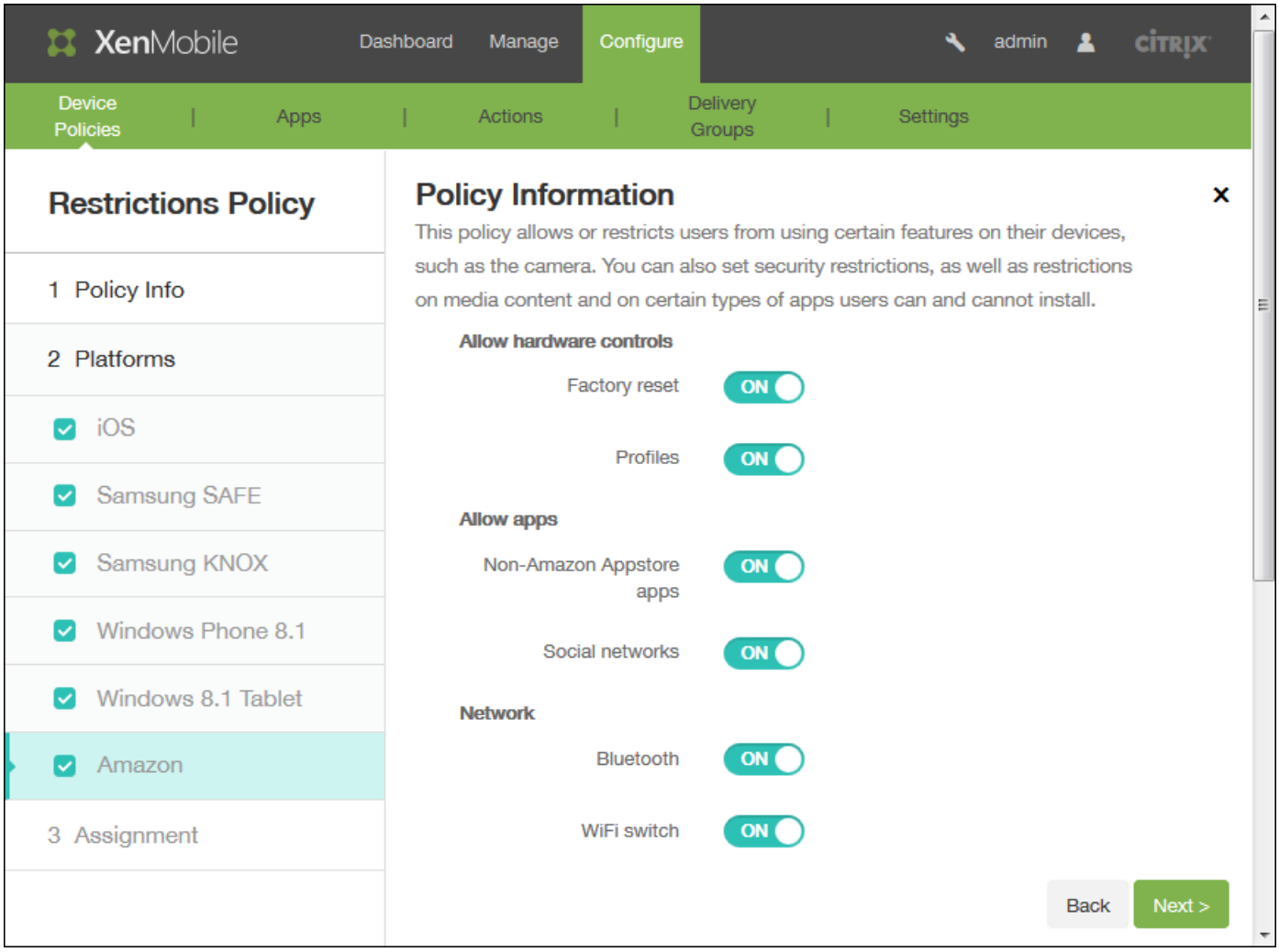


-
-
-



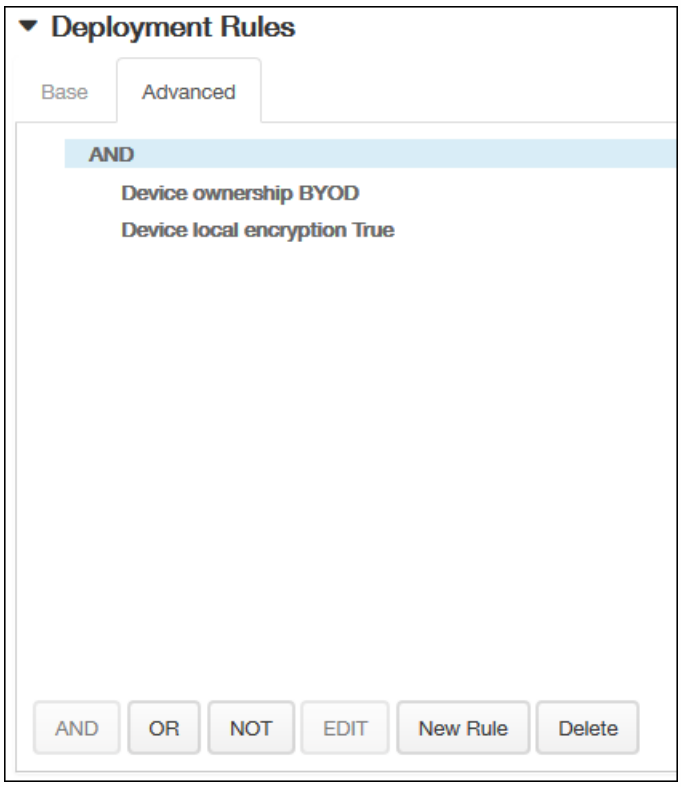
-
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
  -



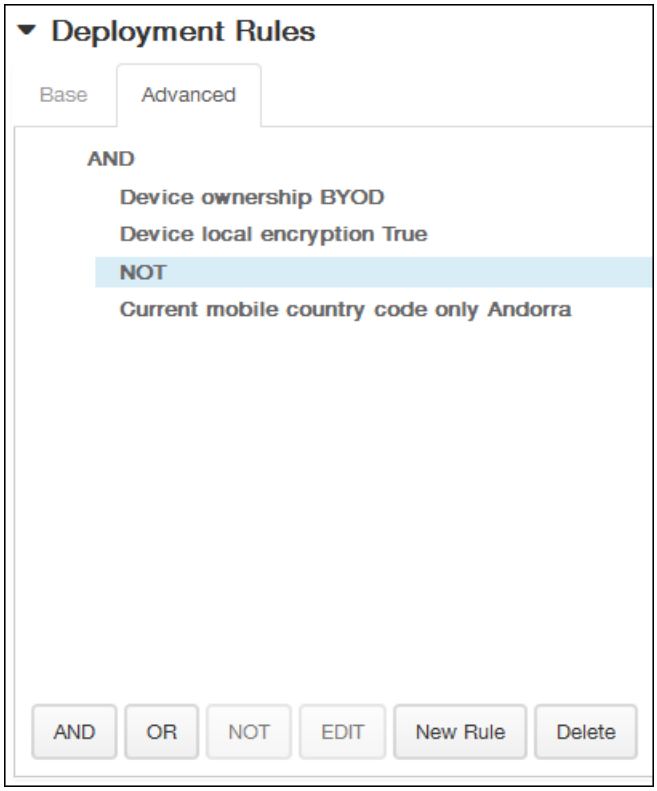


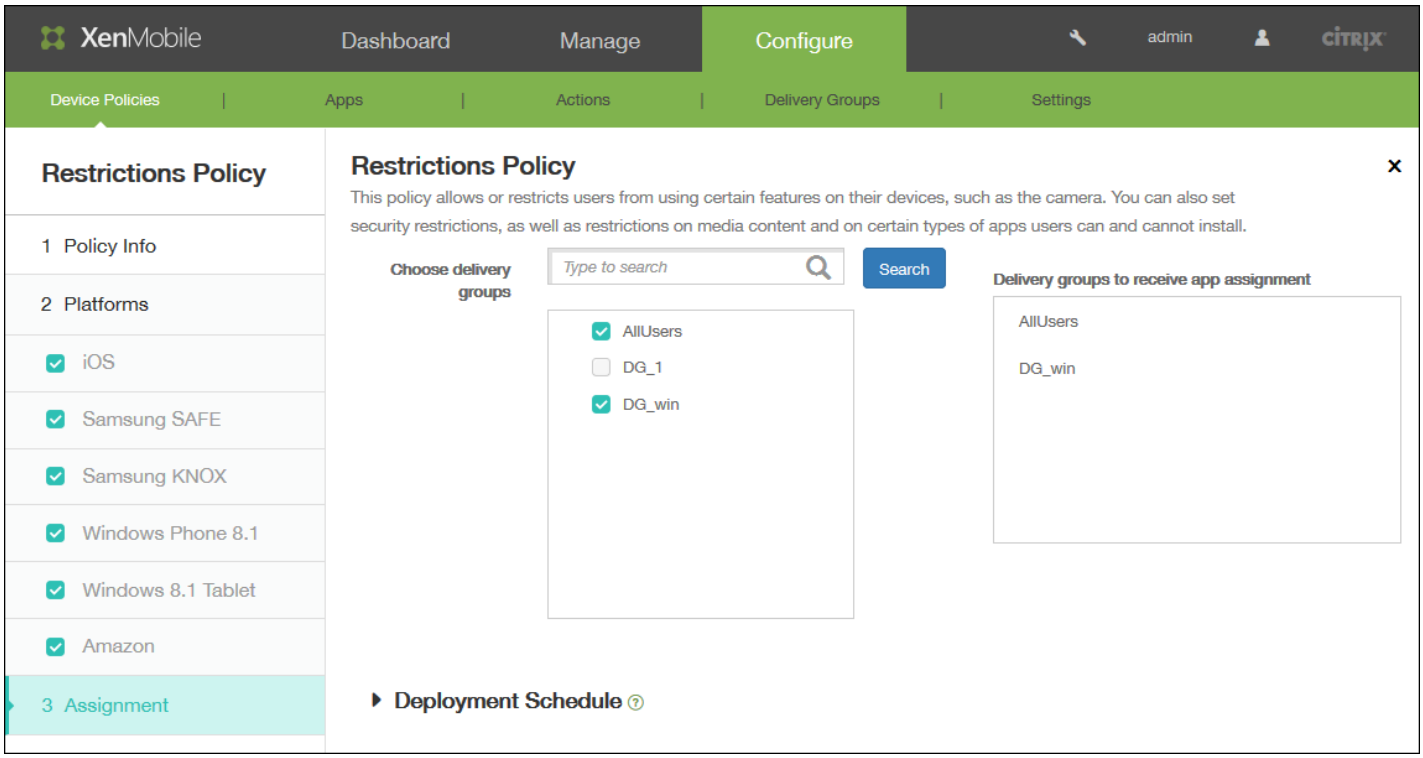
-
  -
  -
-
  -
  -
-
  -
  -
  -
  -
  -
  -
-
  -

-
  -
  -
  -
  -
  -

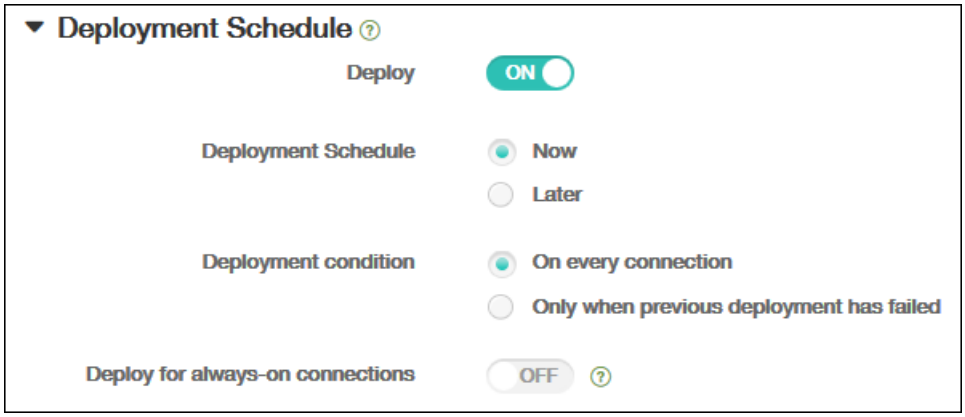


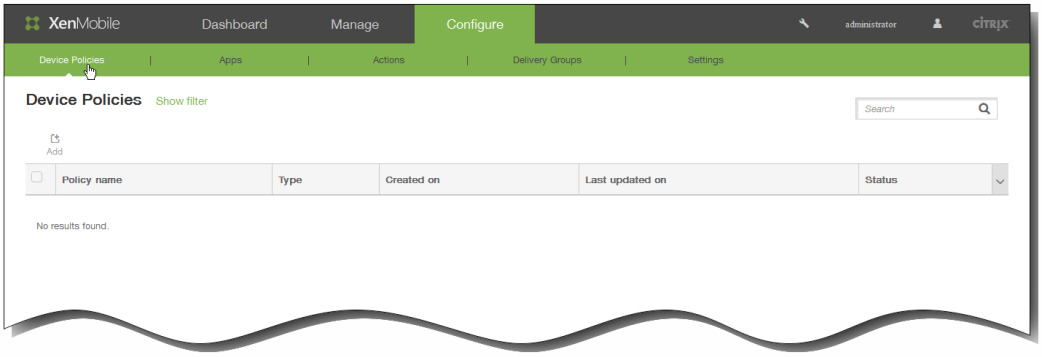
-
  -
  -
  -

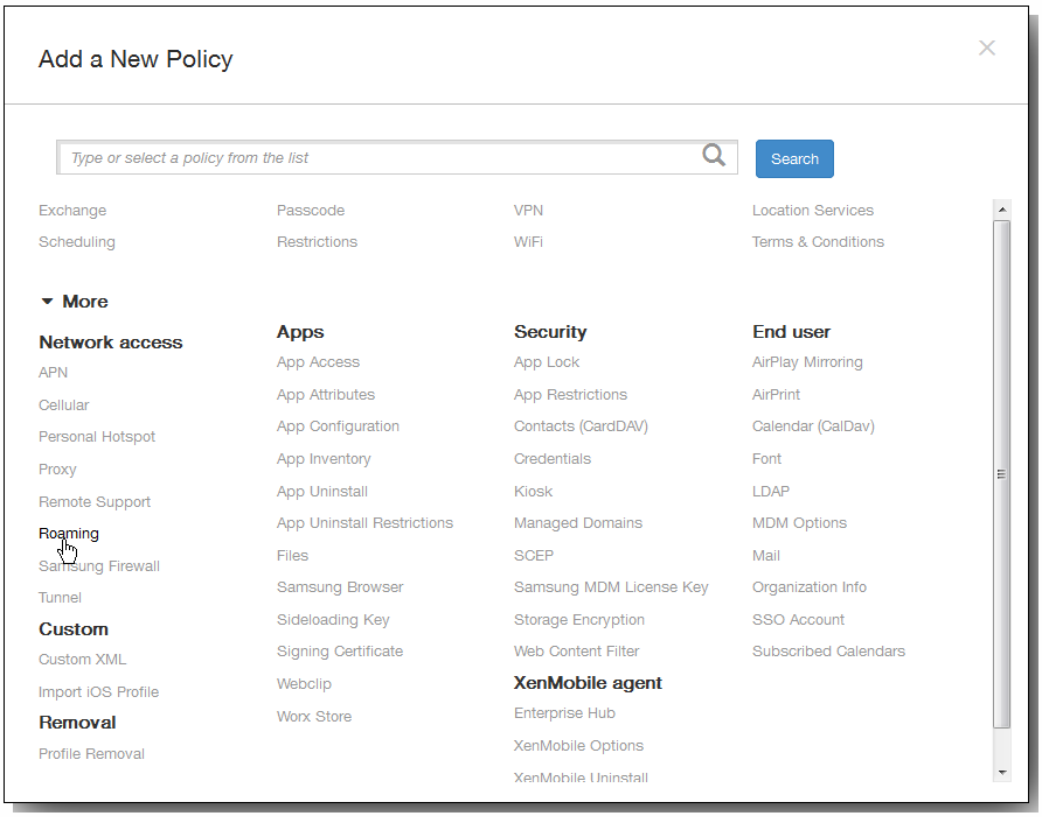


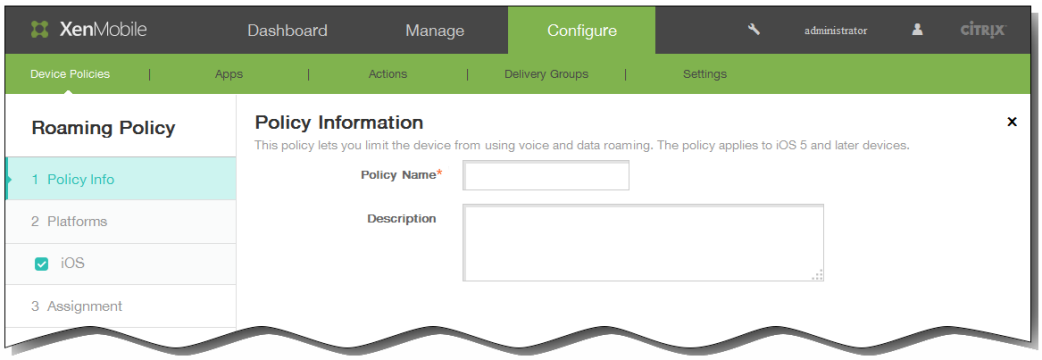


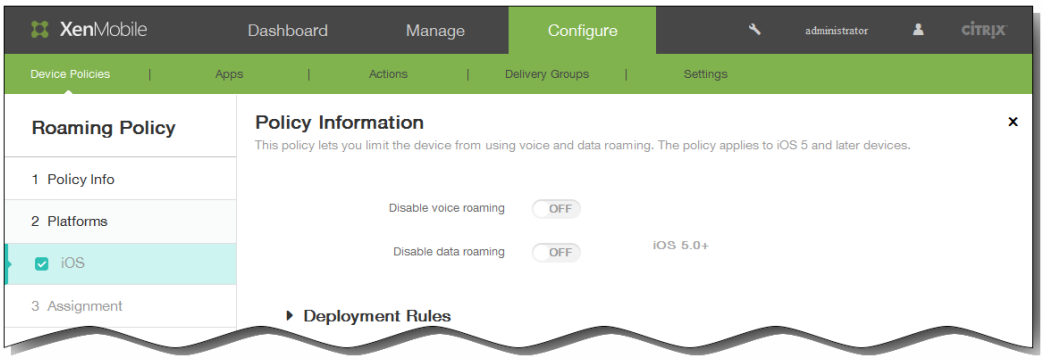
-
-
-
-
-

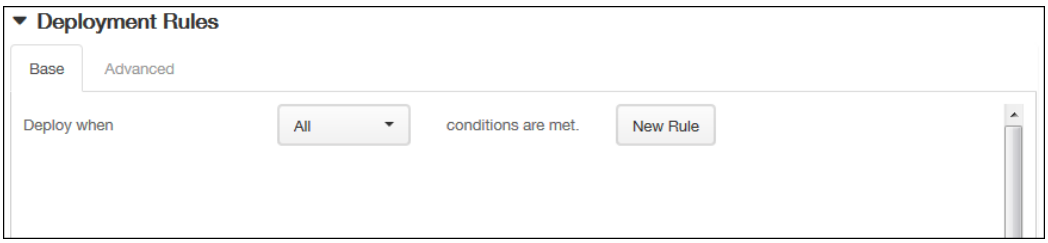


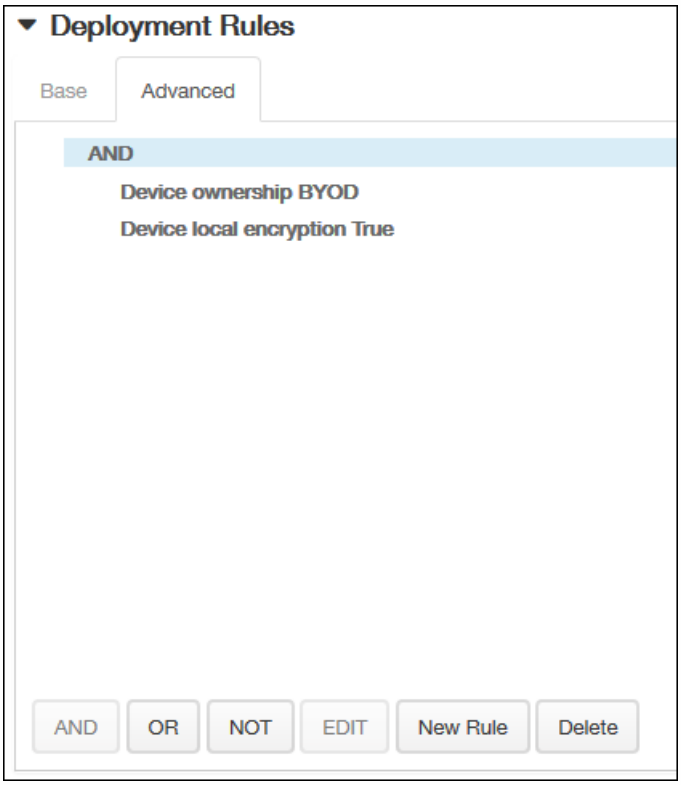


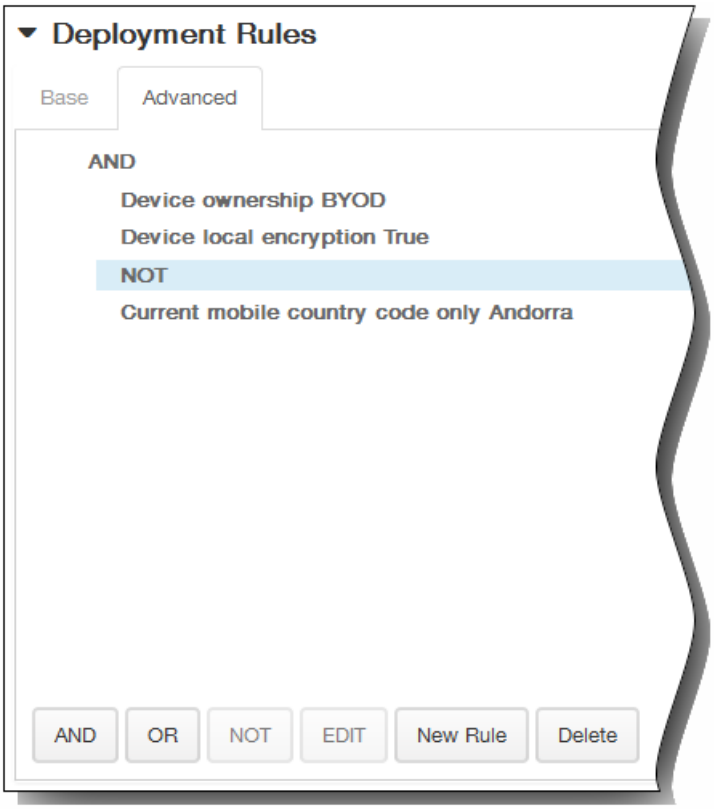


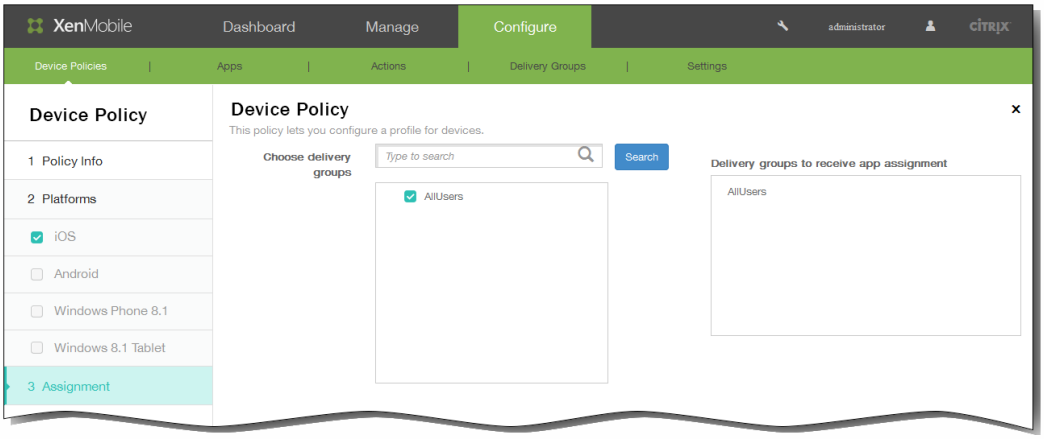


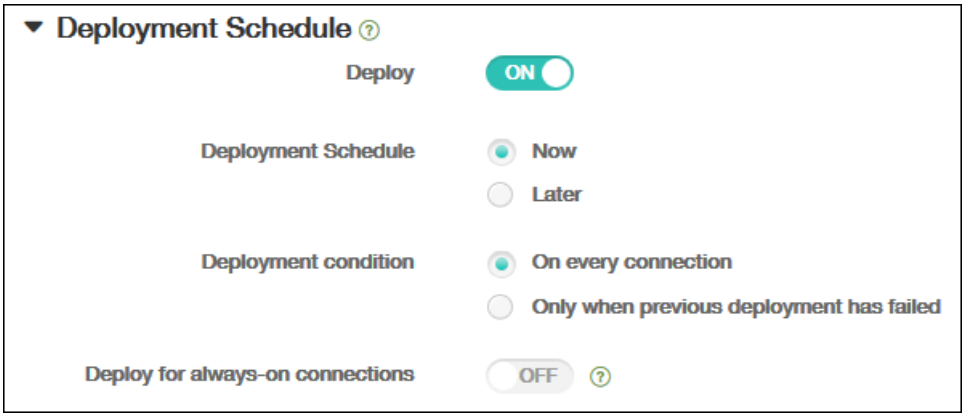


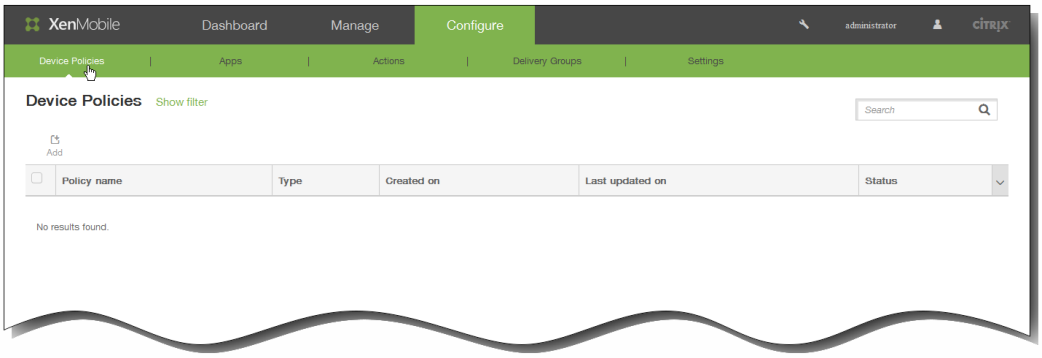


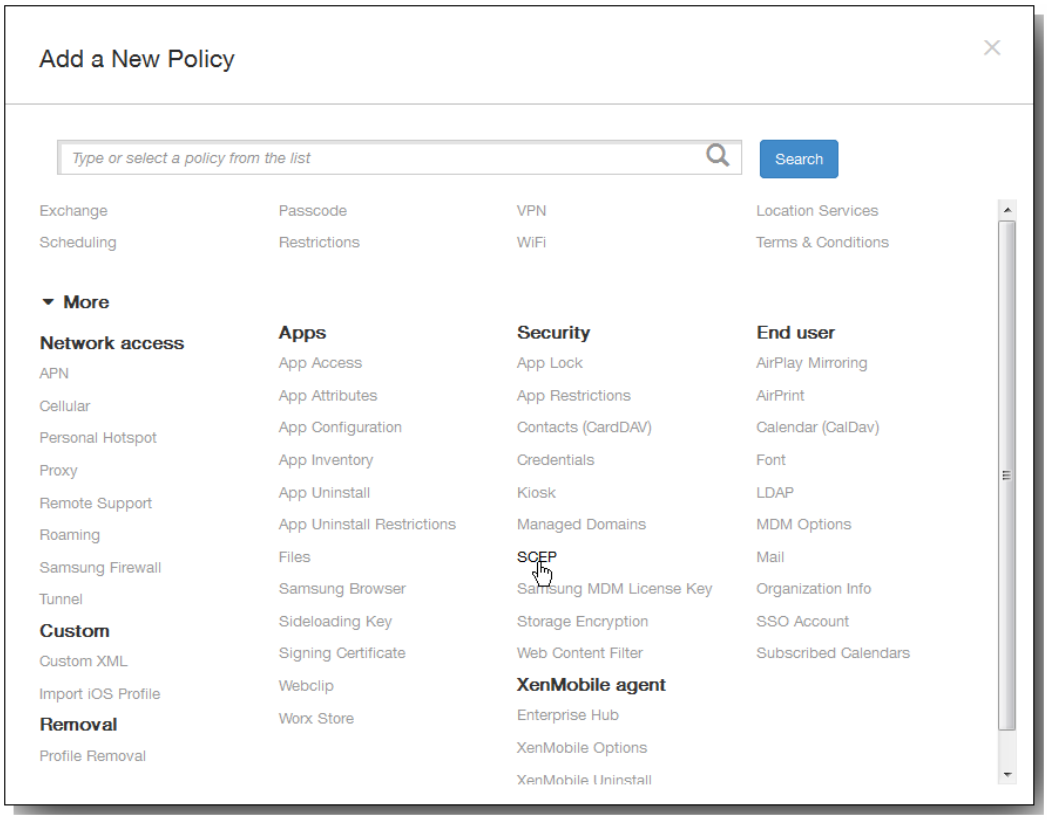


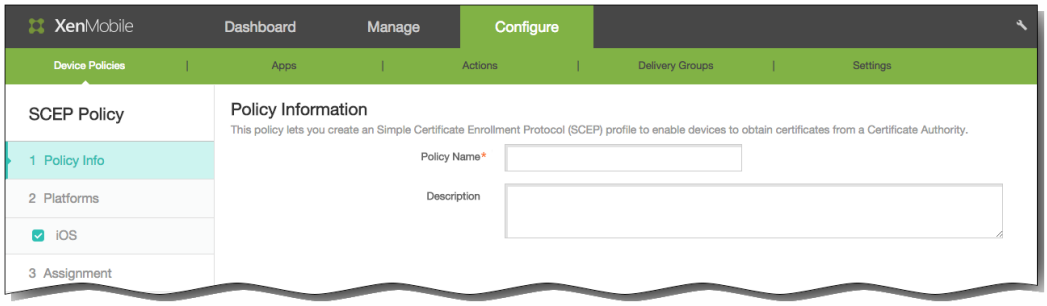


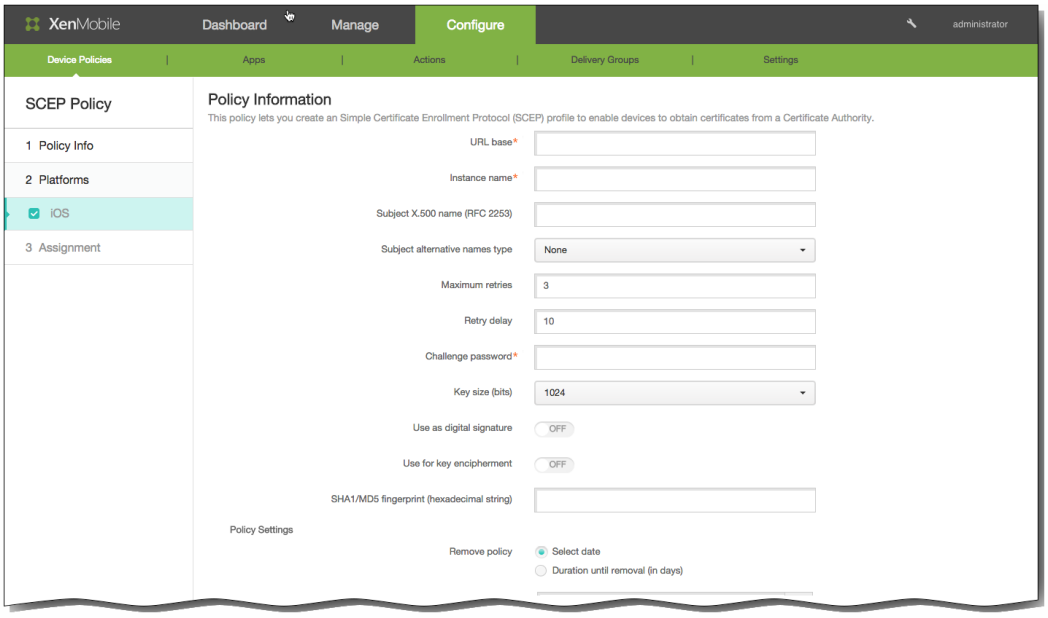


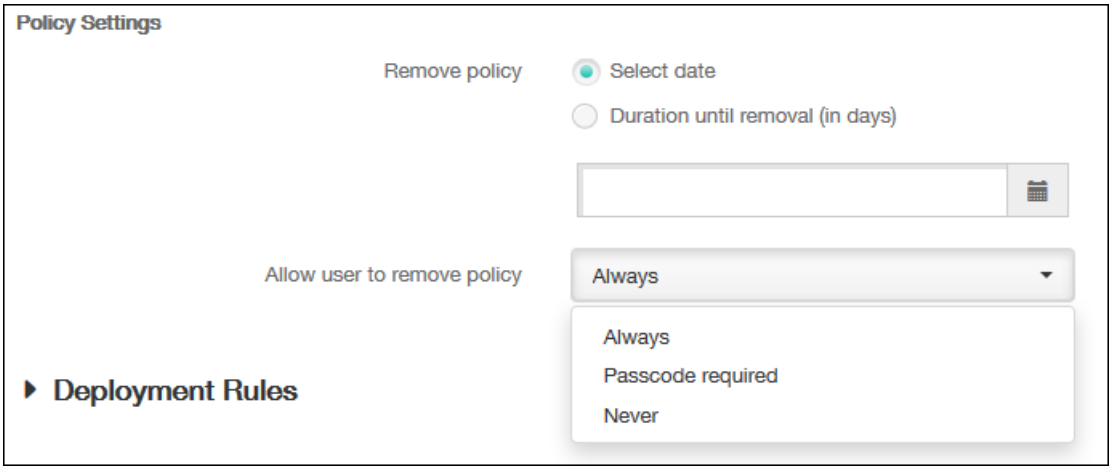


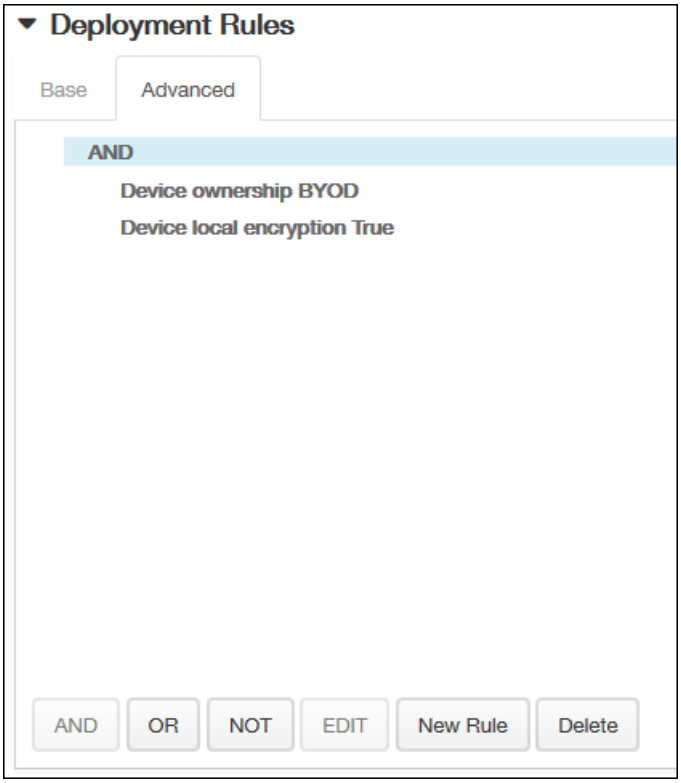


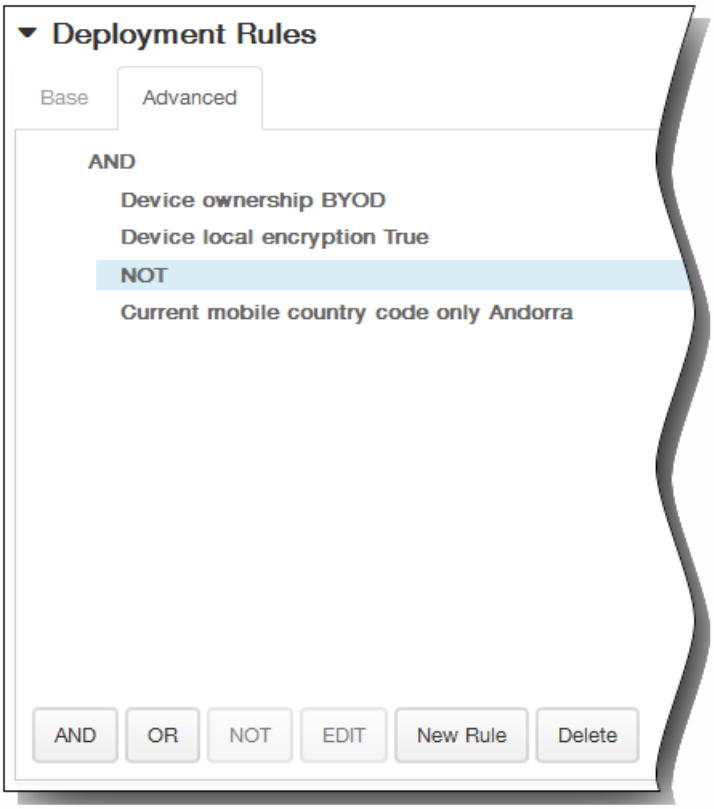


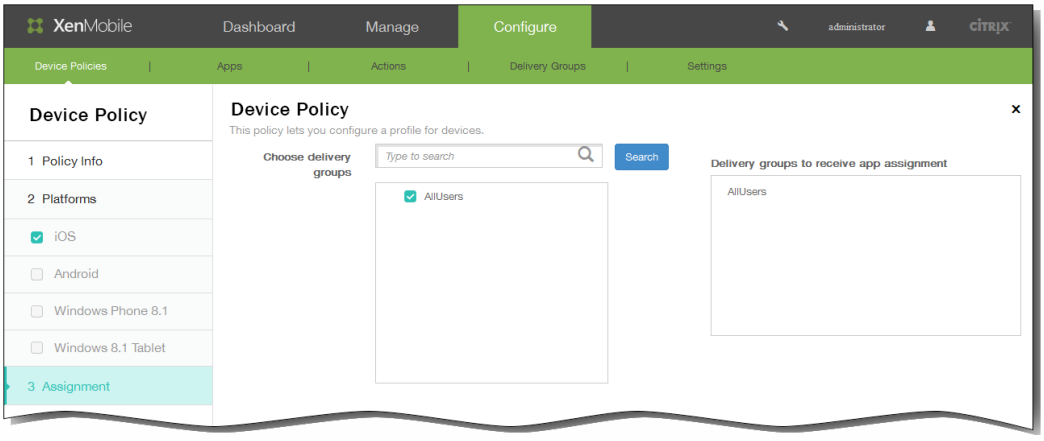


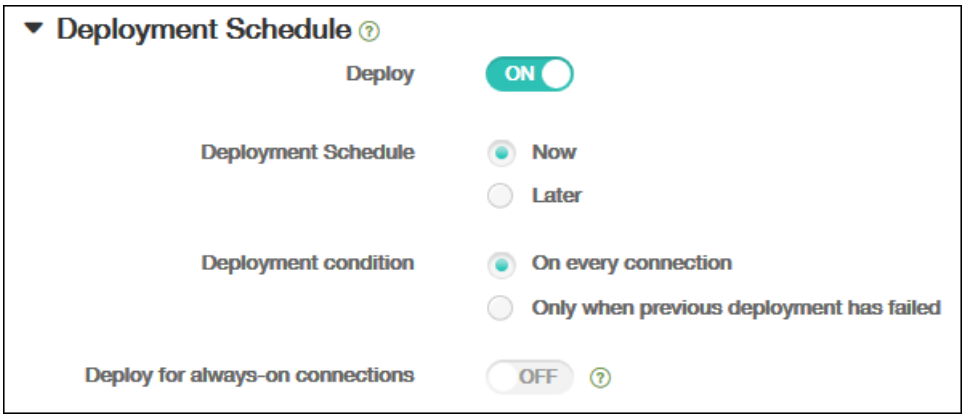


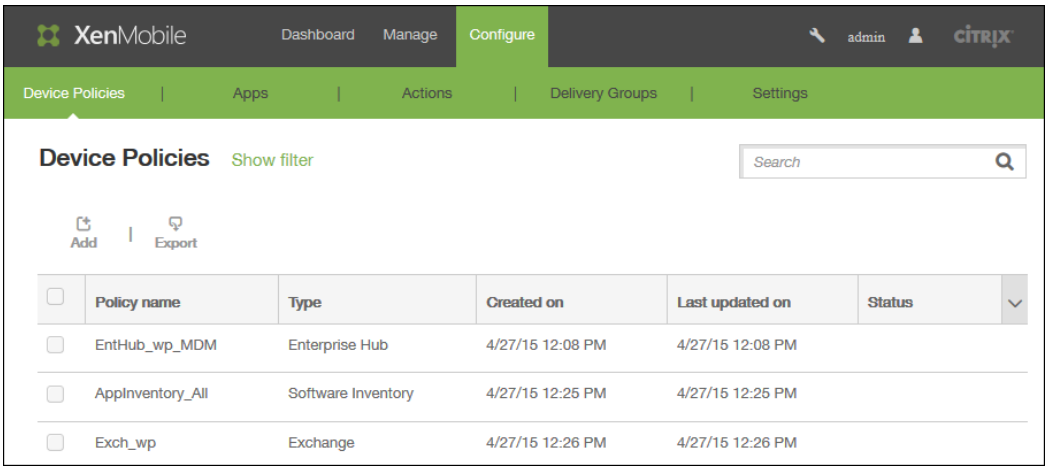


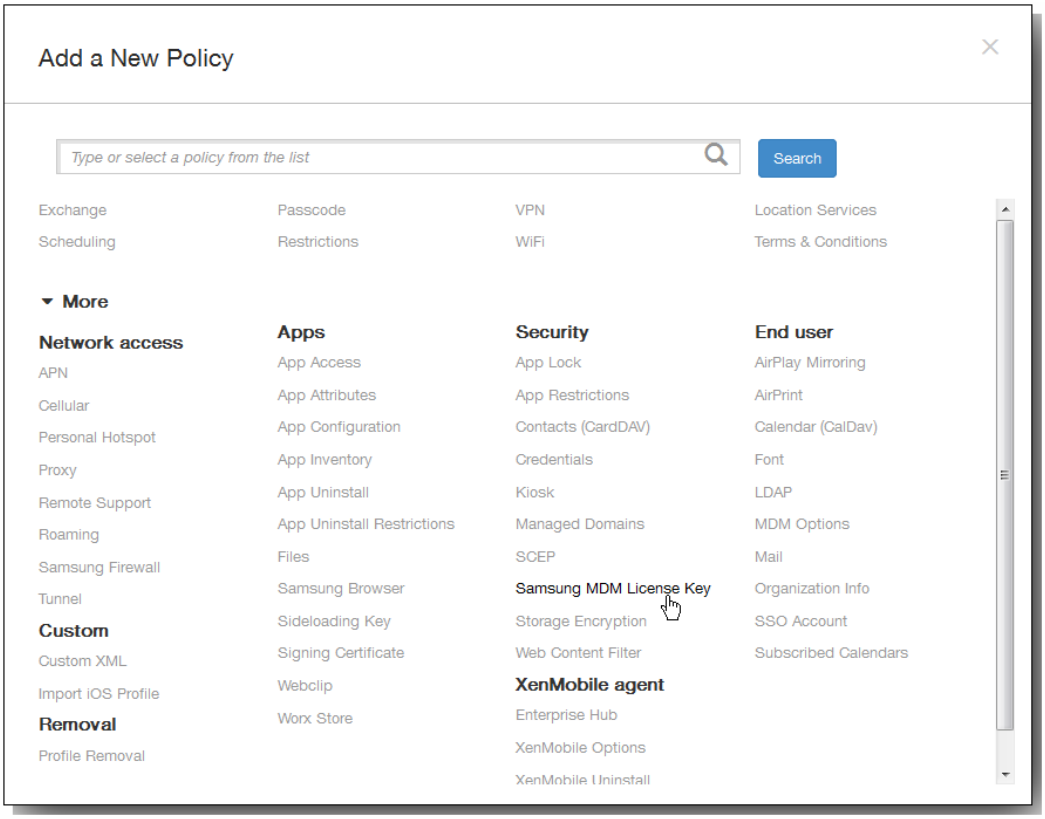


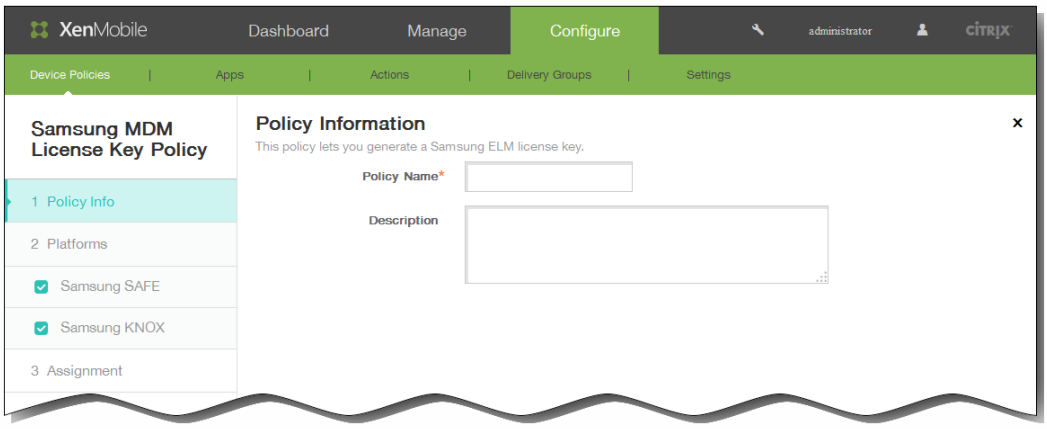


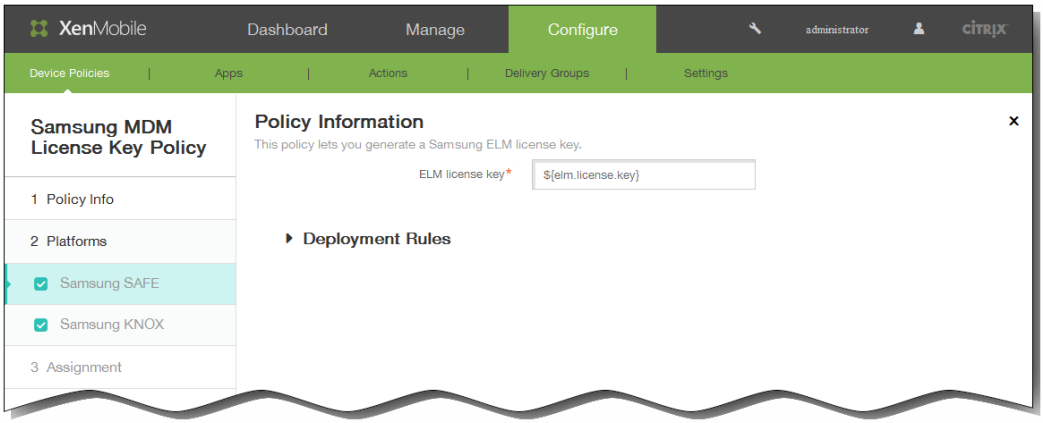




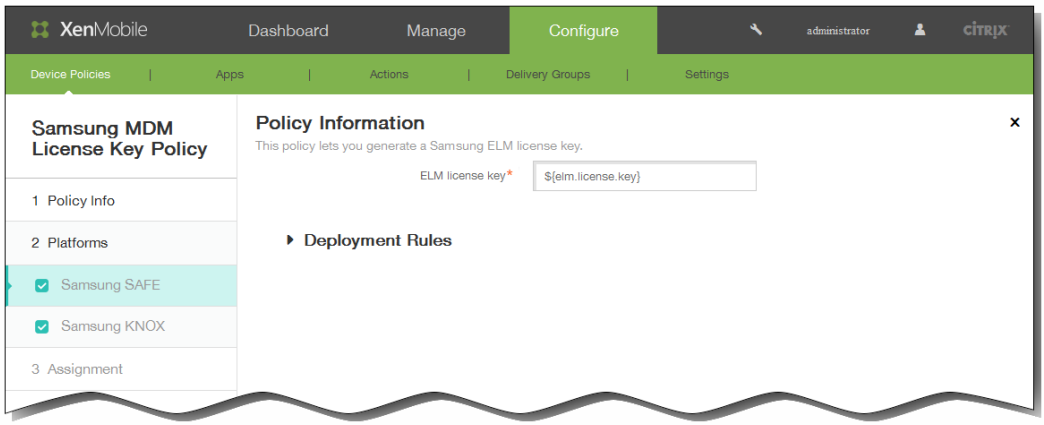




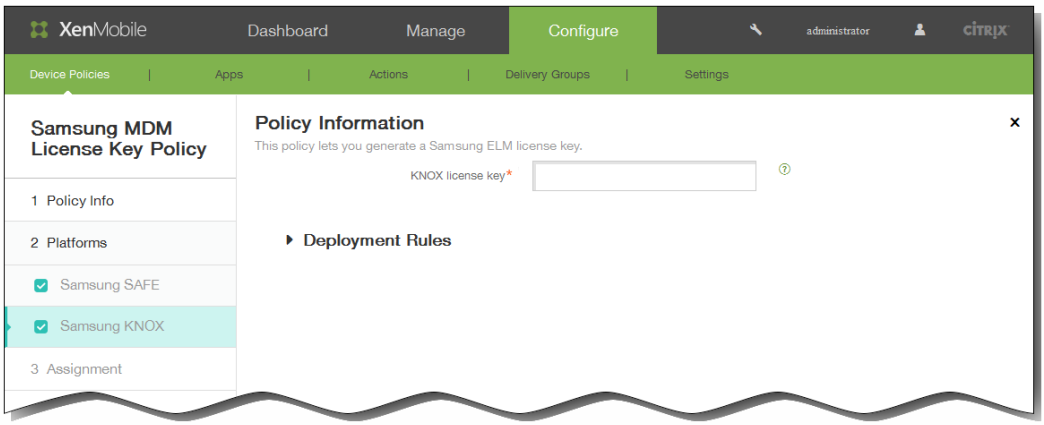


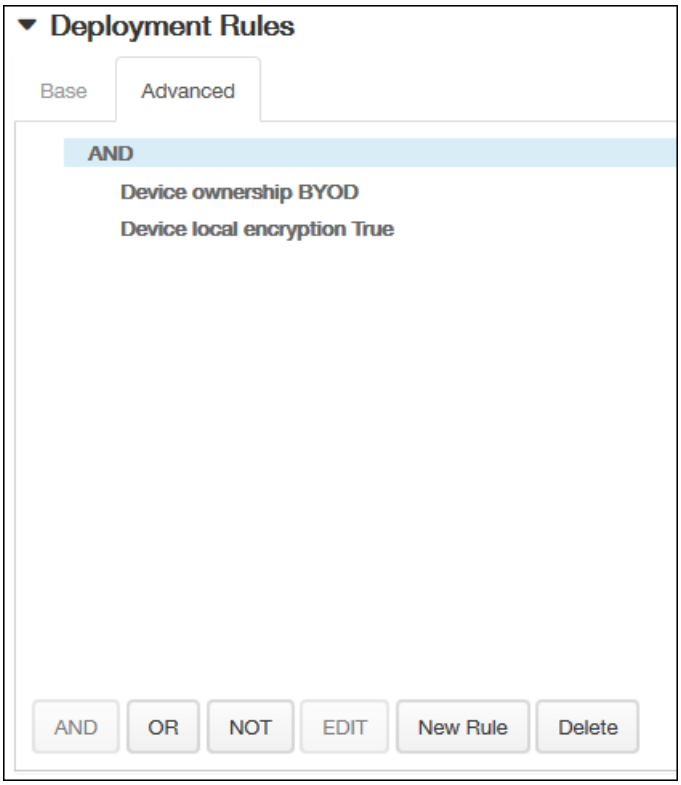


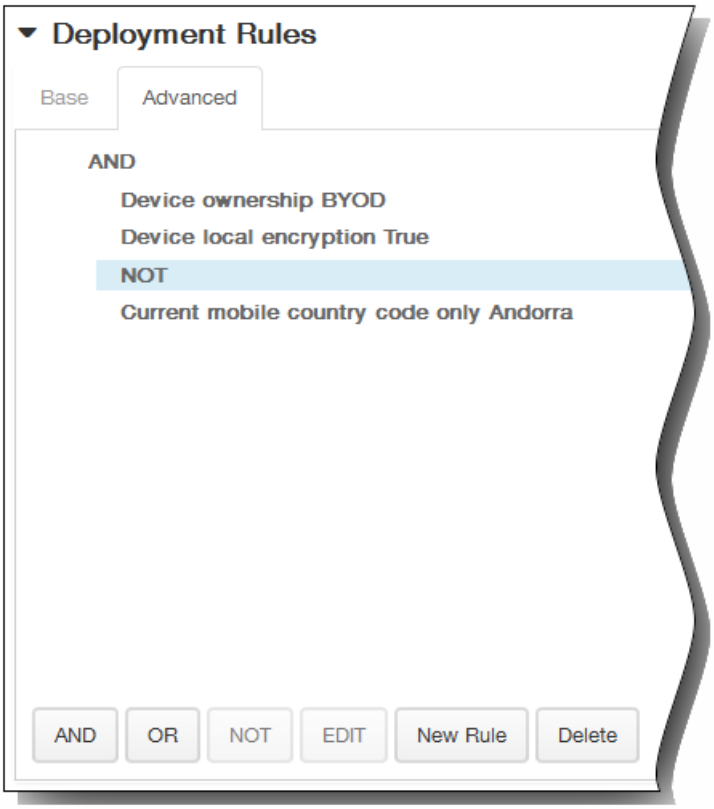
-

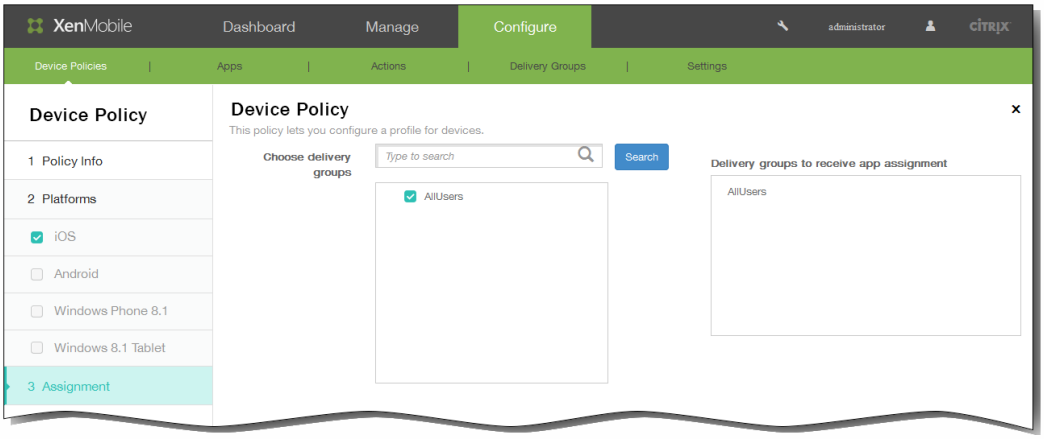


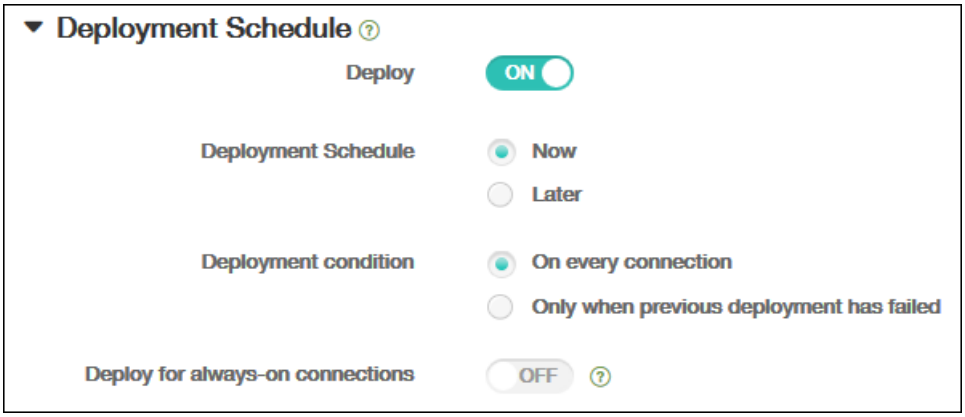
-



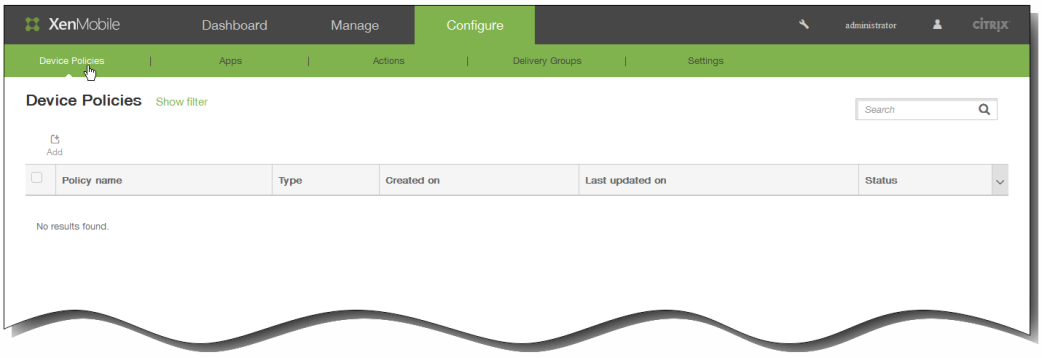


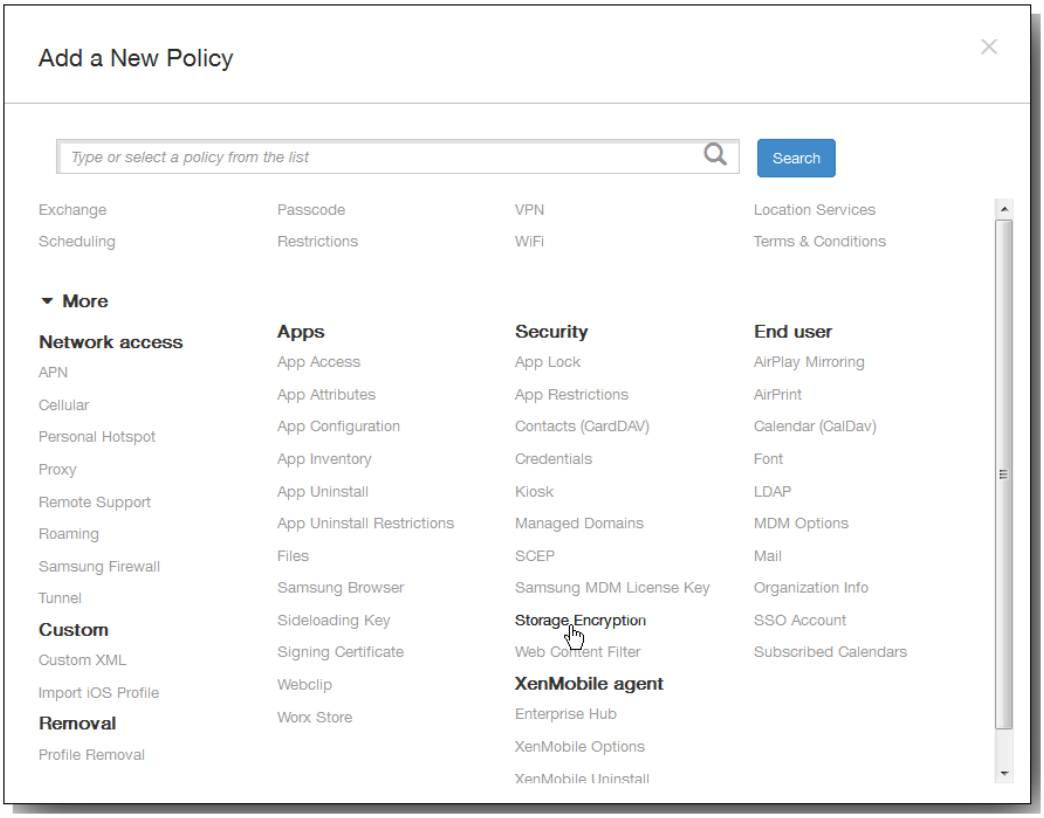


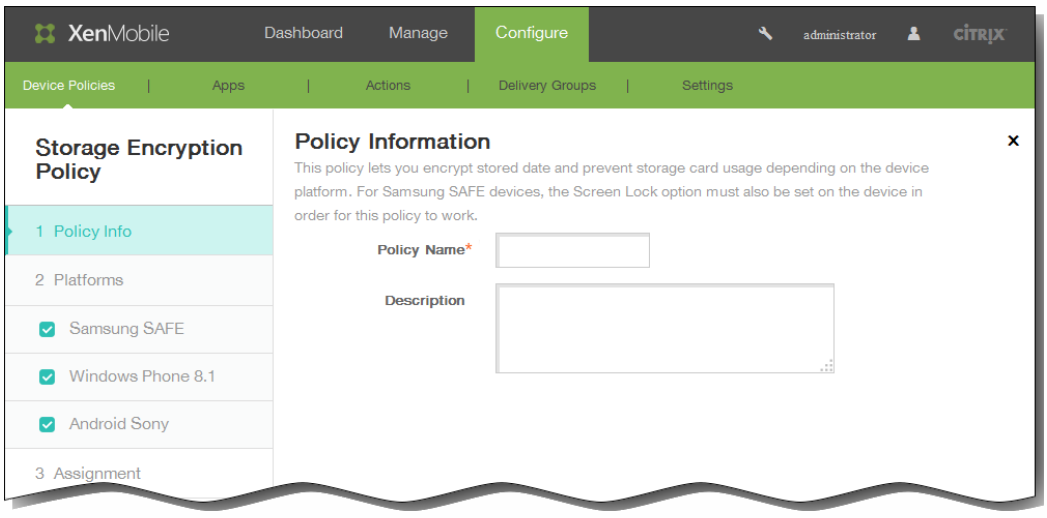




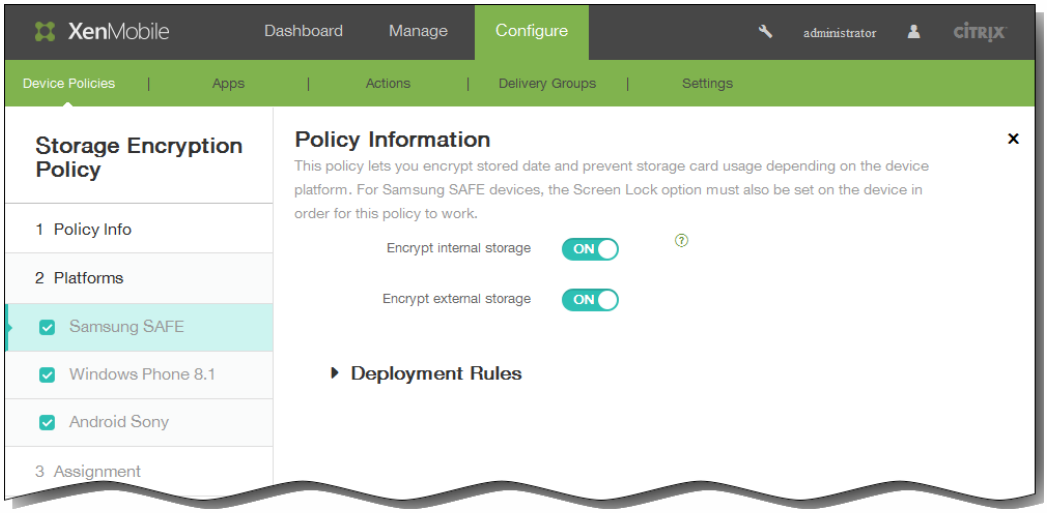
-
-
-



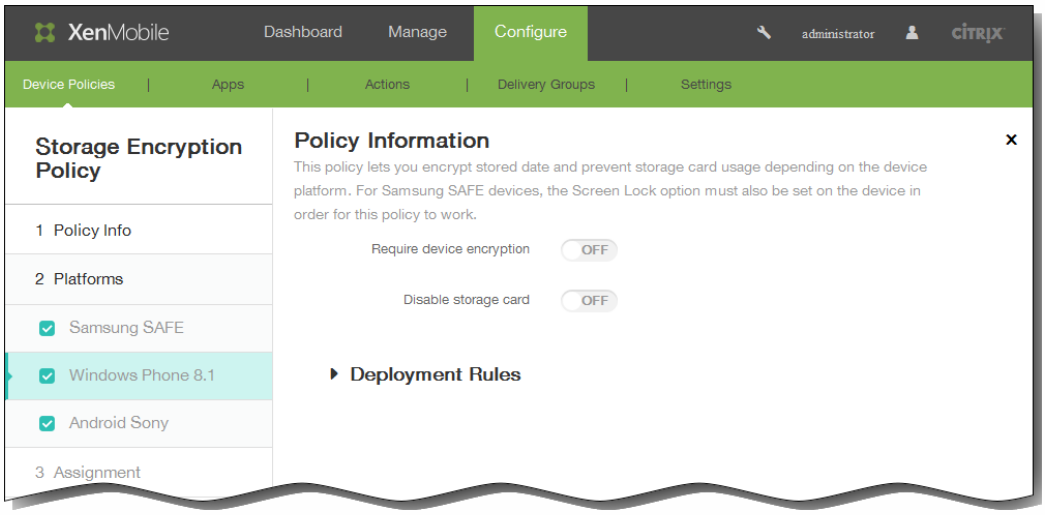




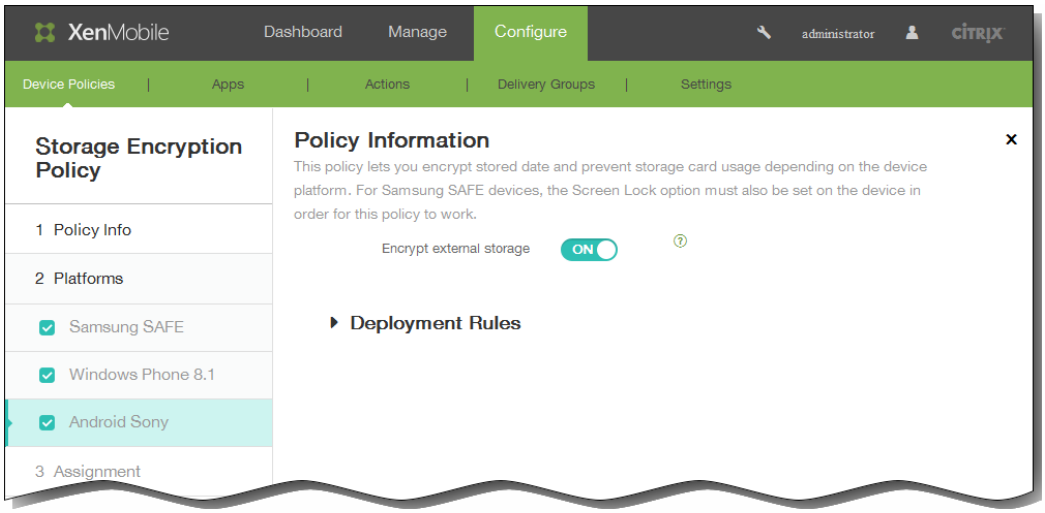
-
-

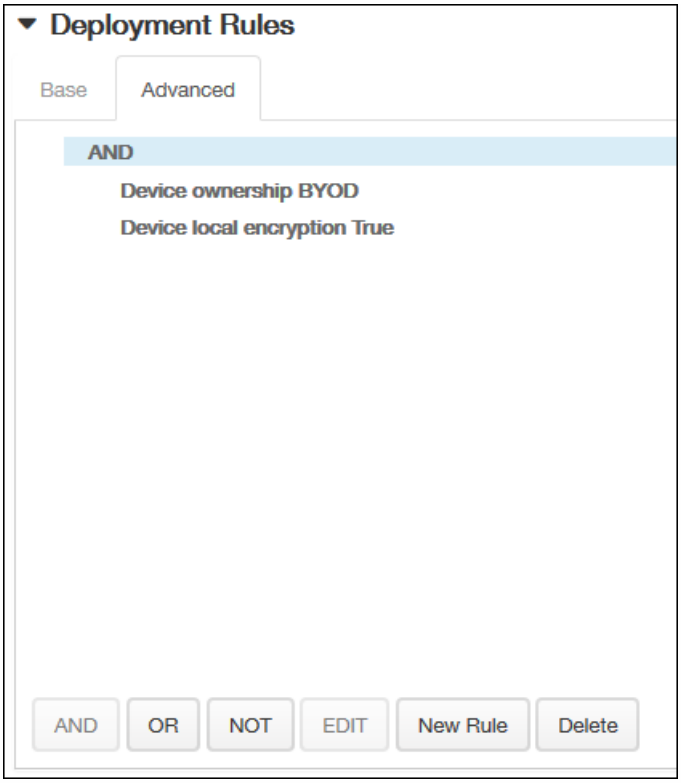


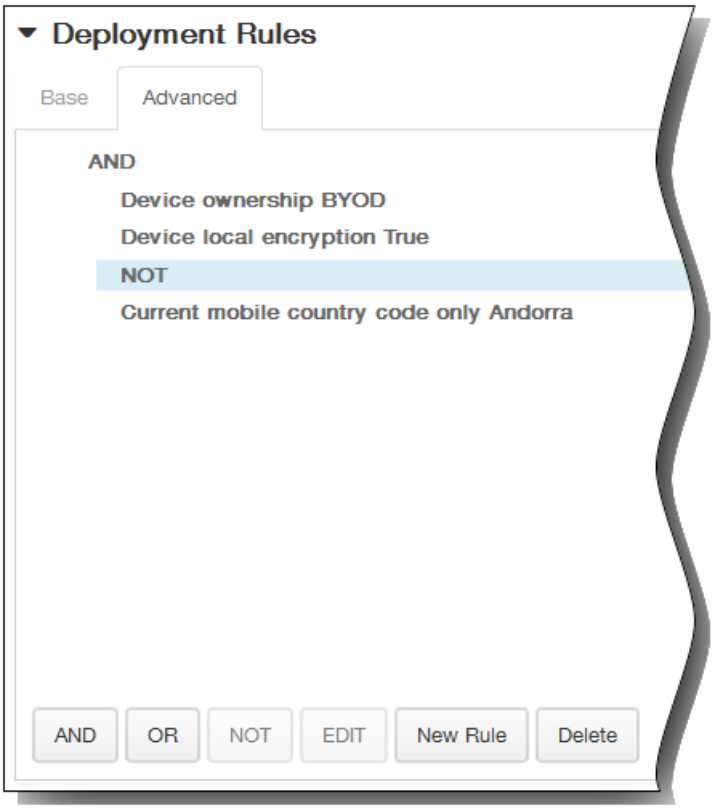
-
-

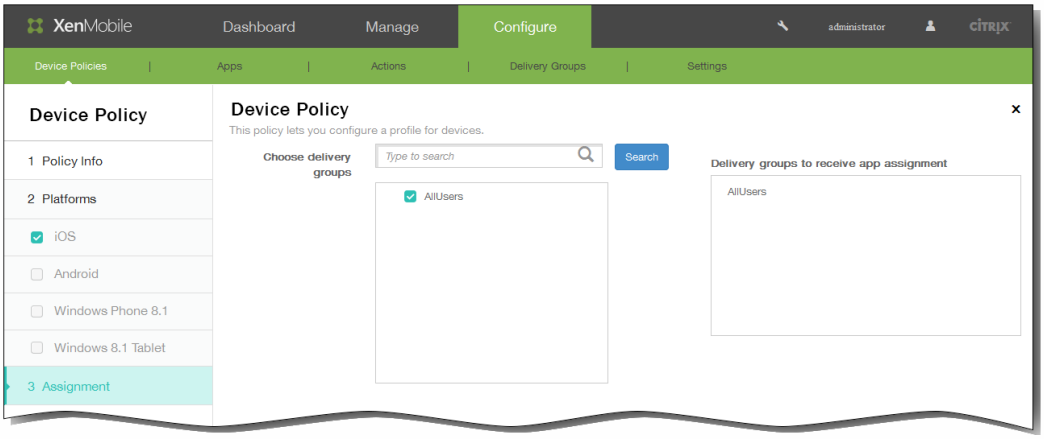


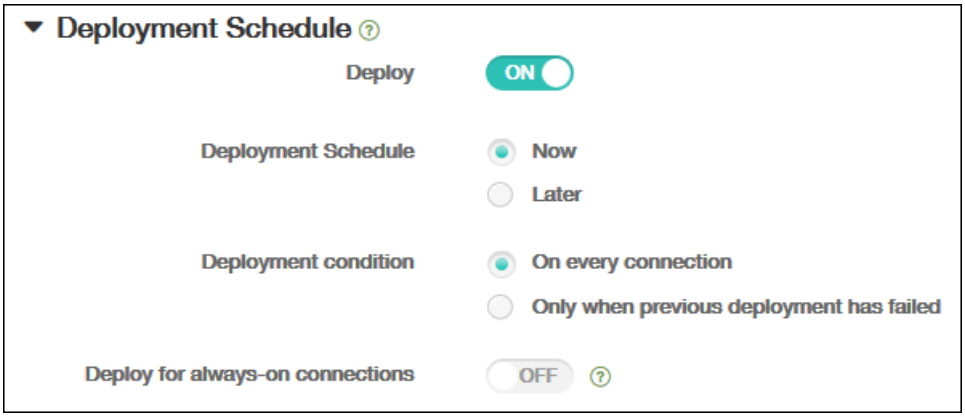
-

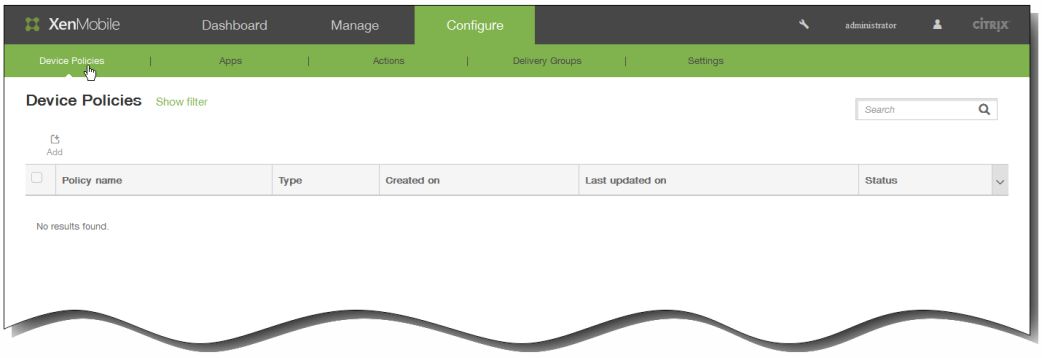


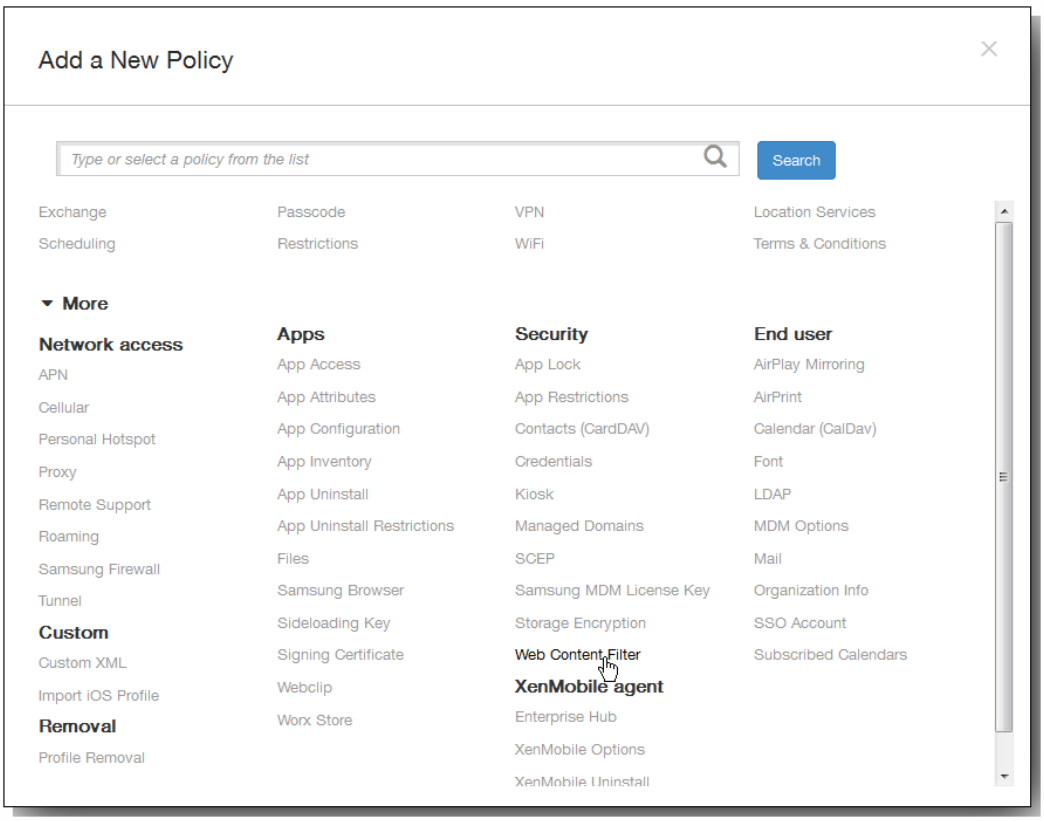


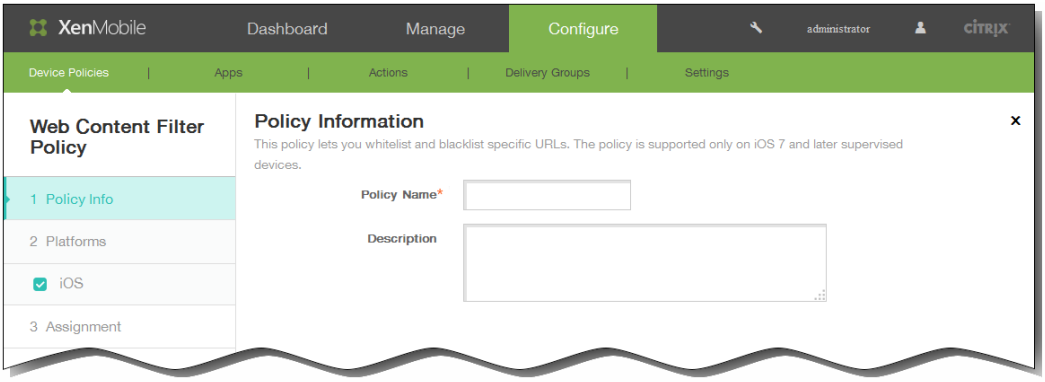


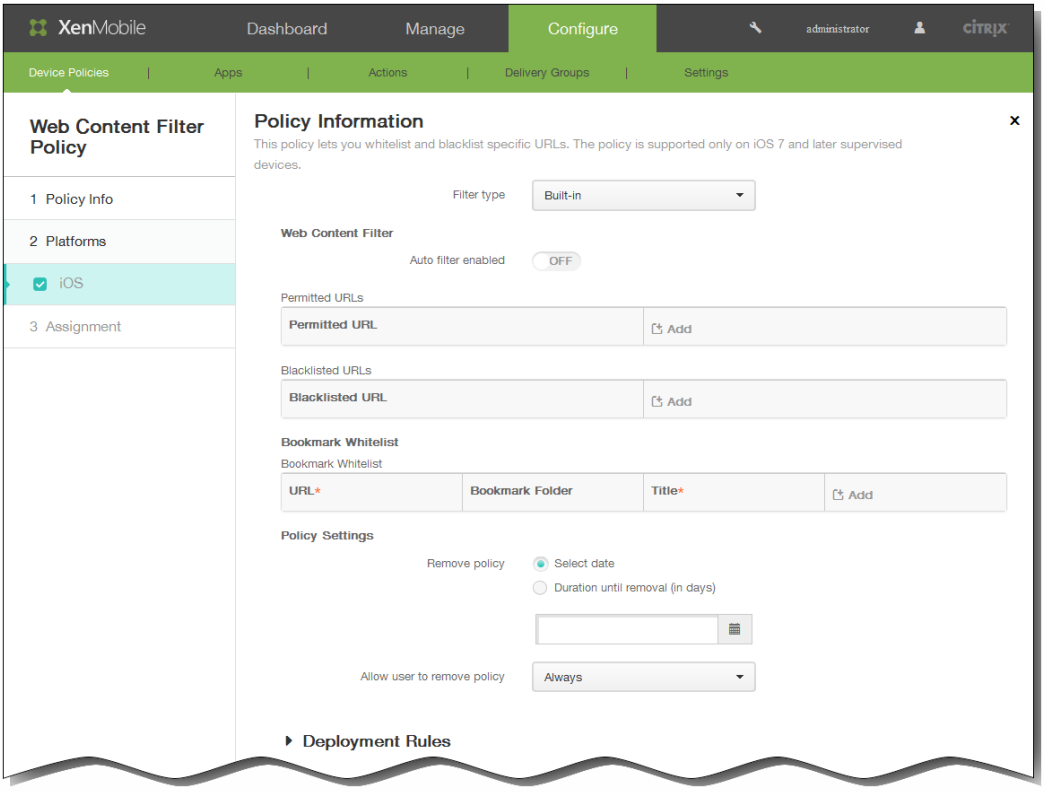




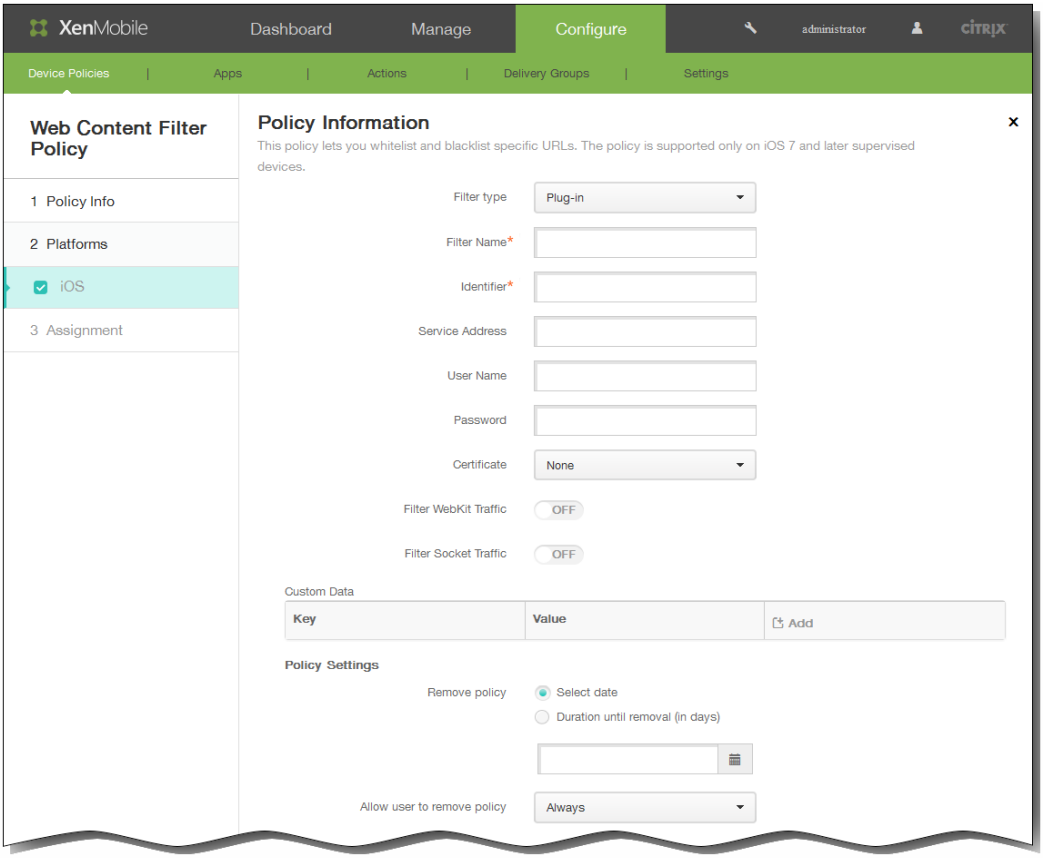


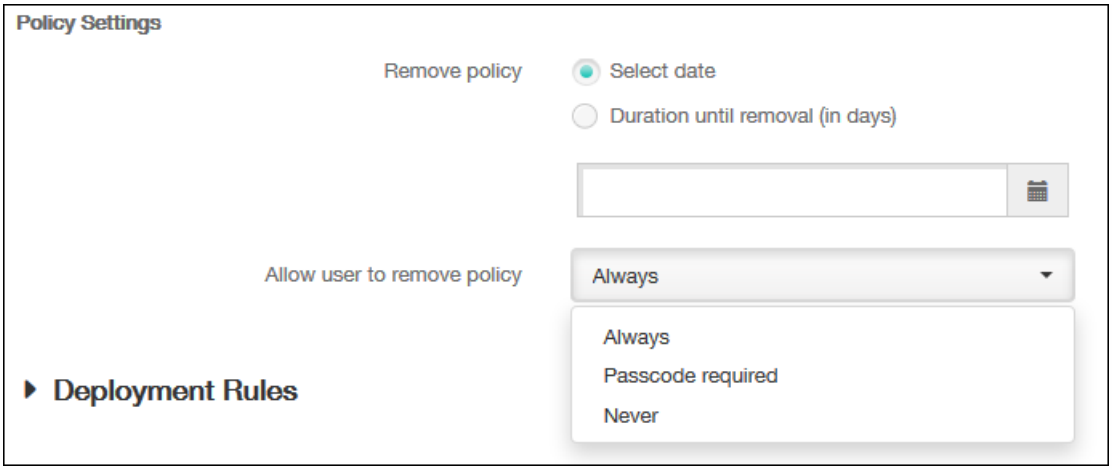


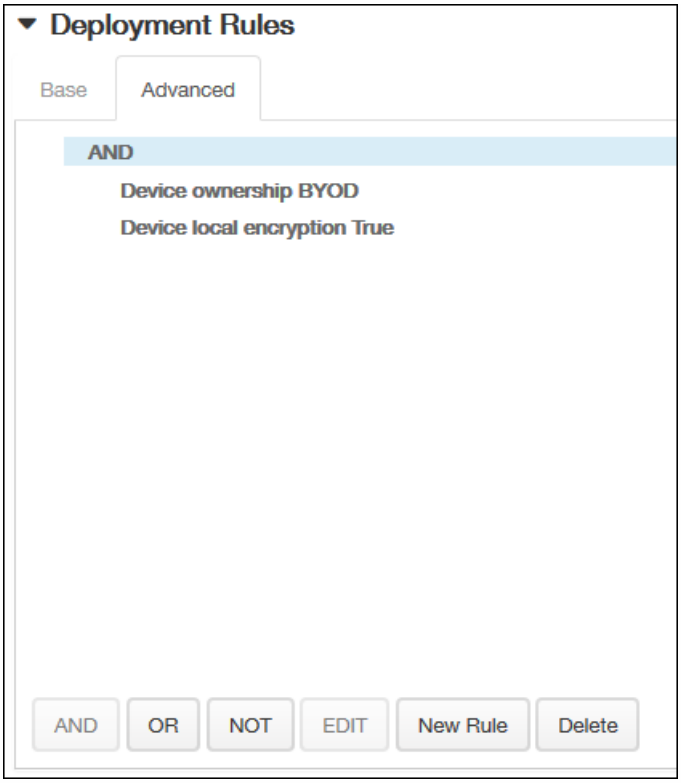


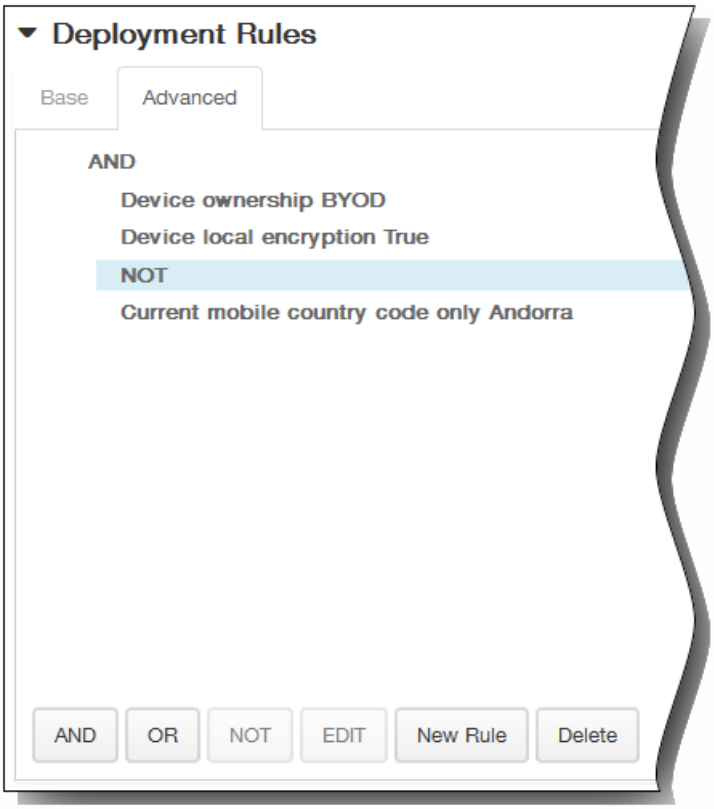


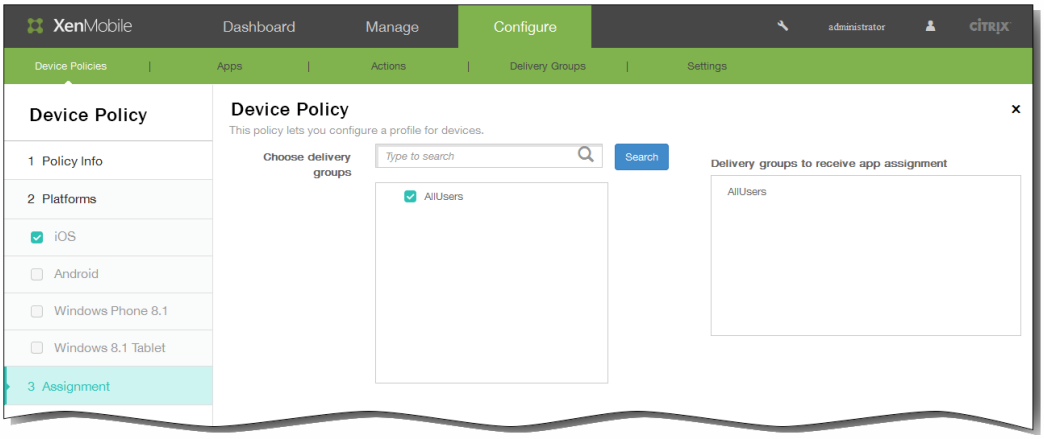
-
-

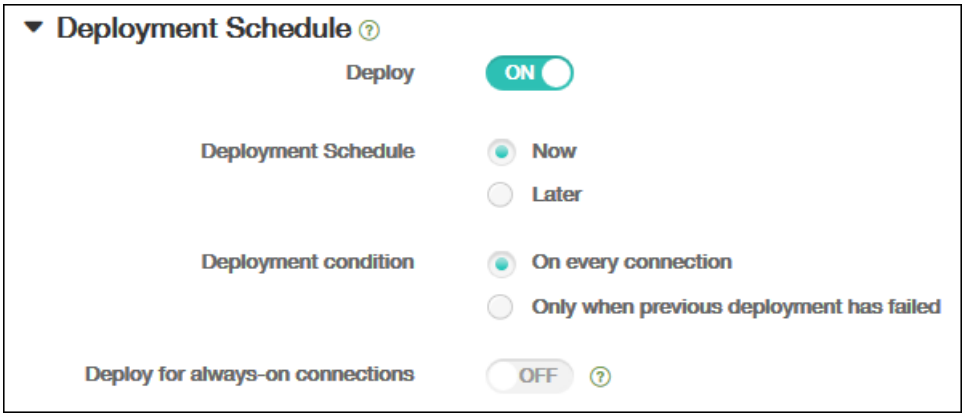


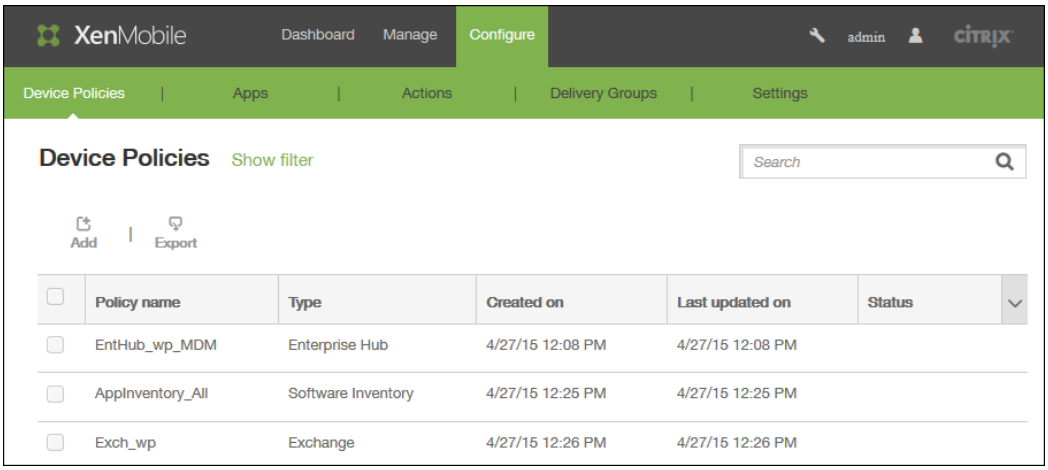


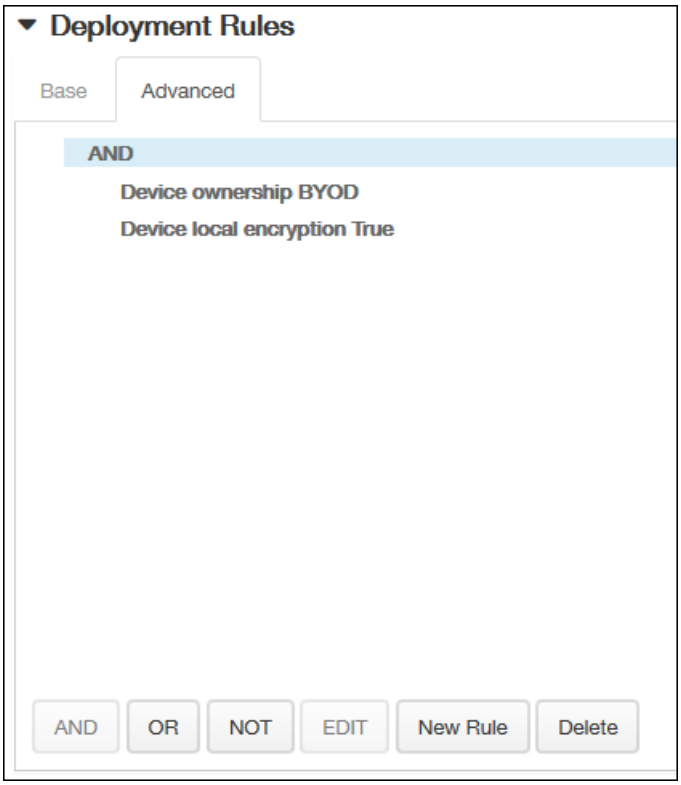


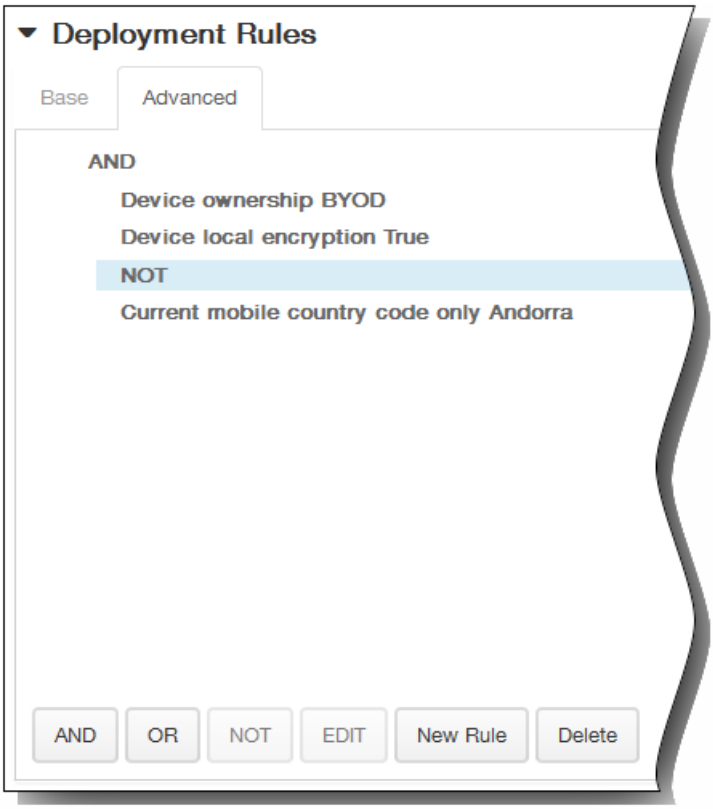


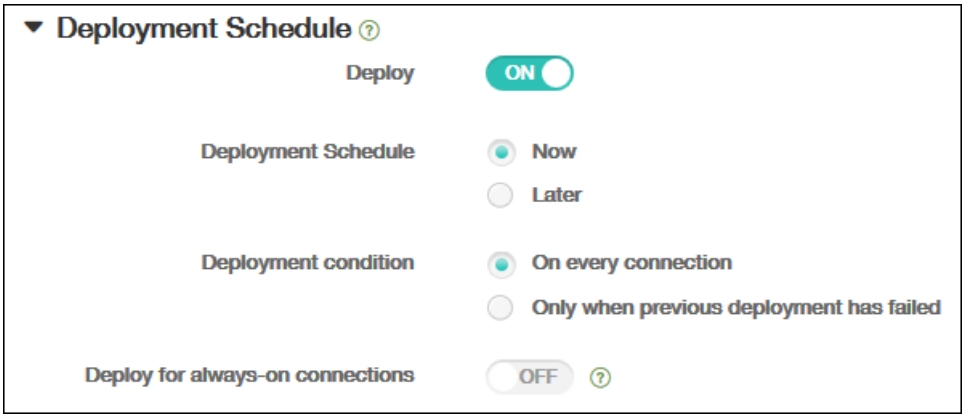




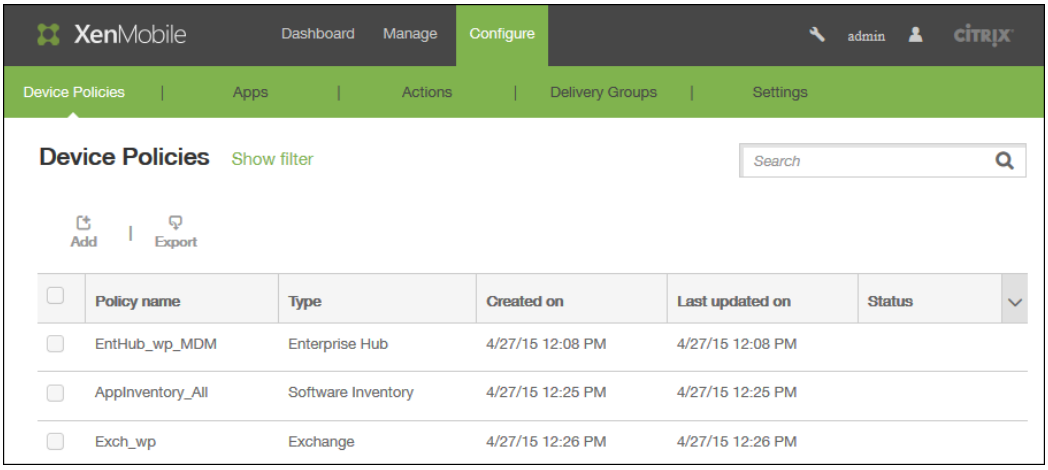


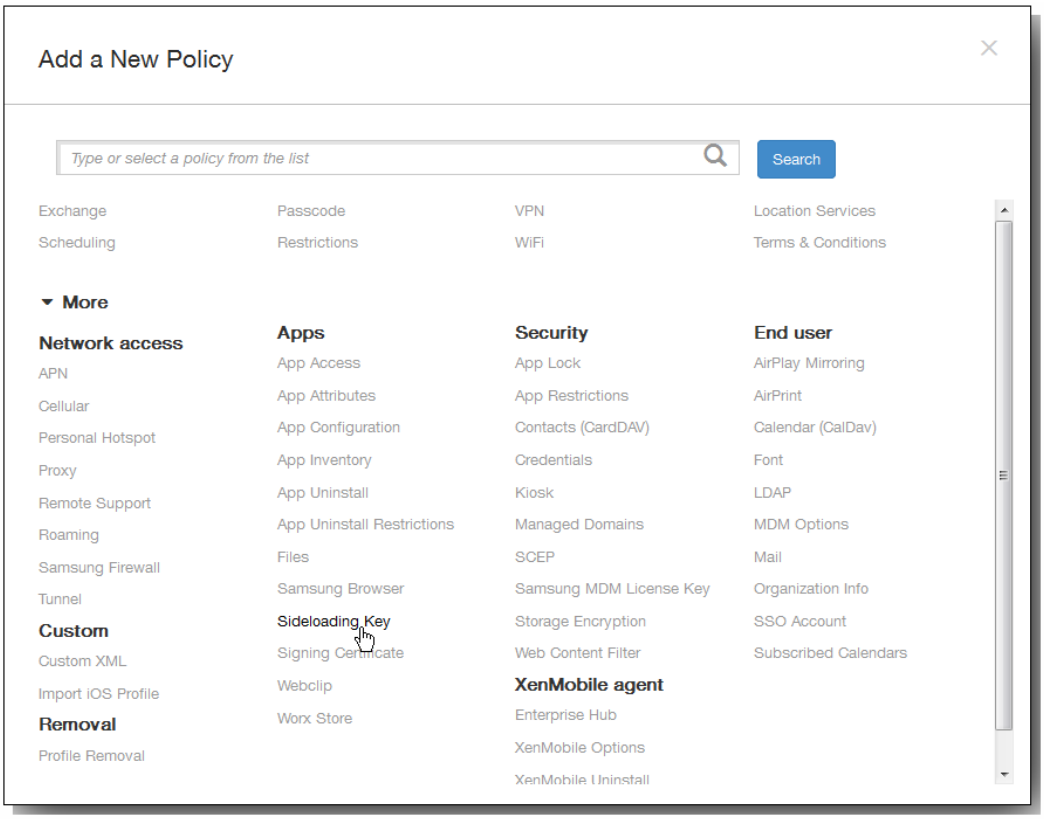


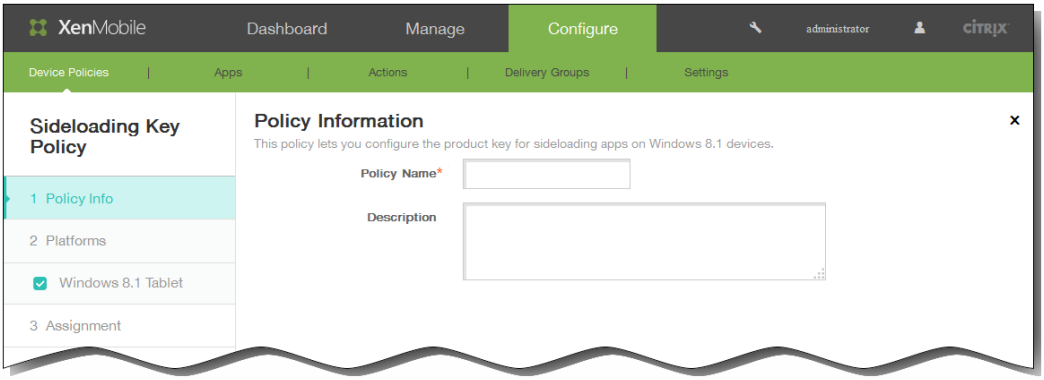


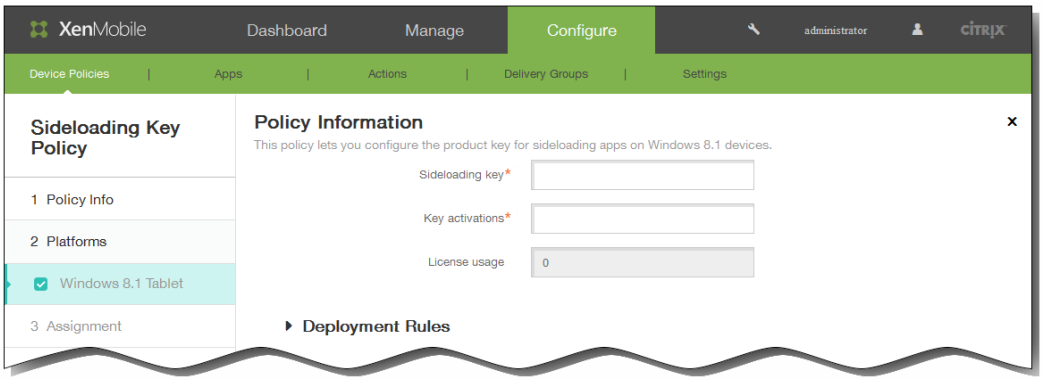


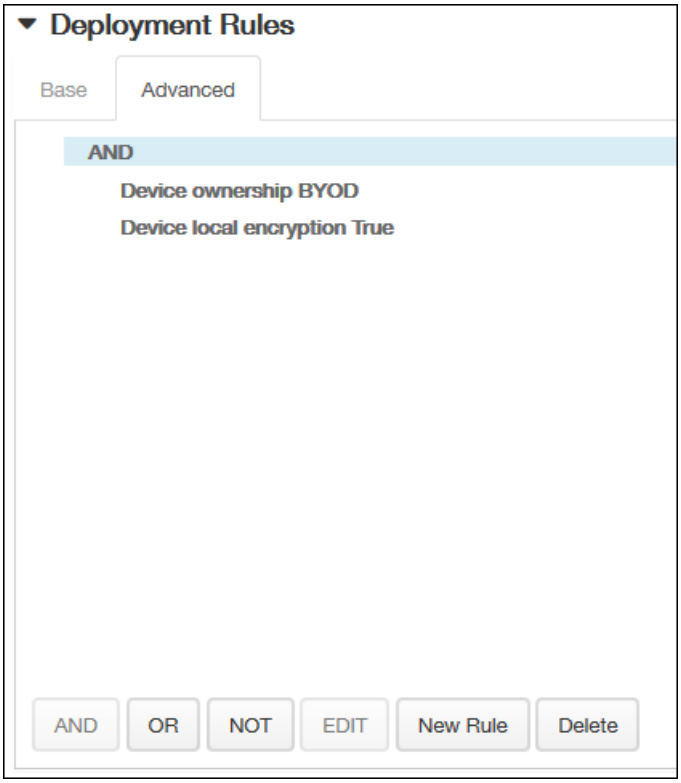
-
-

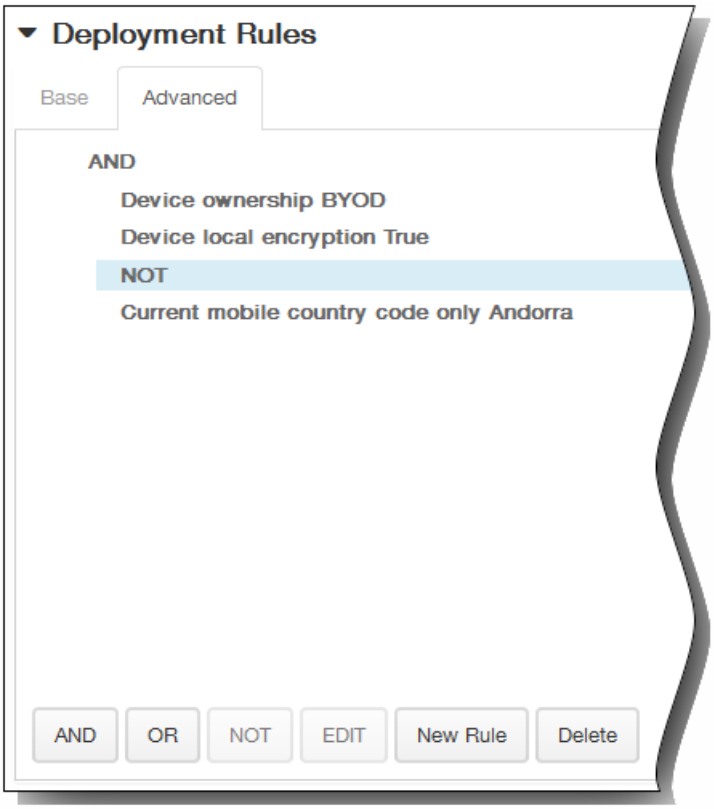


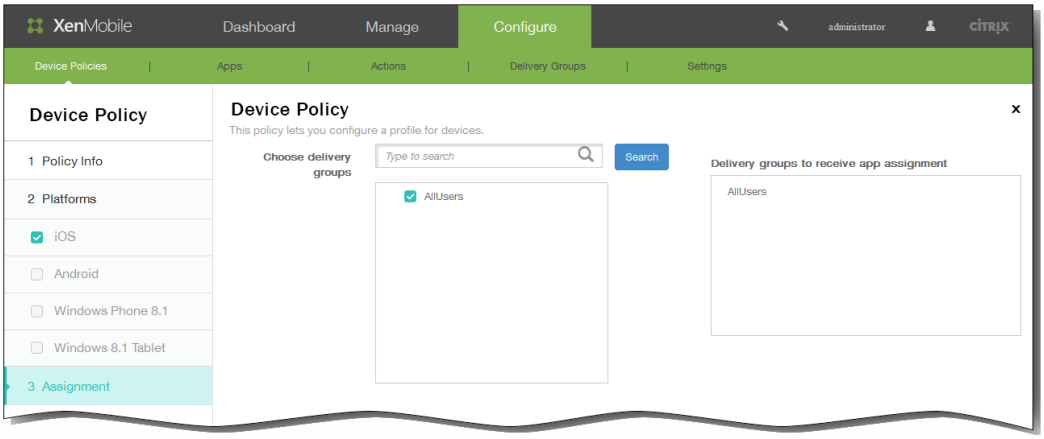


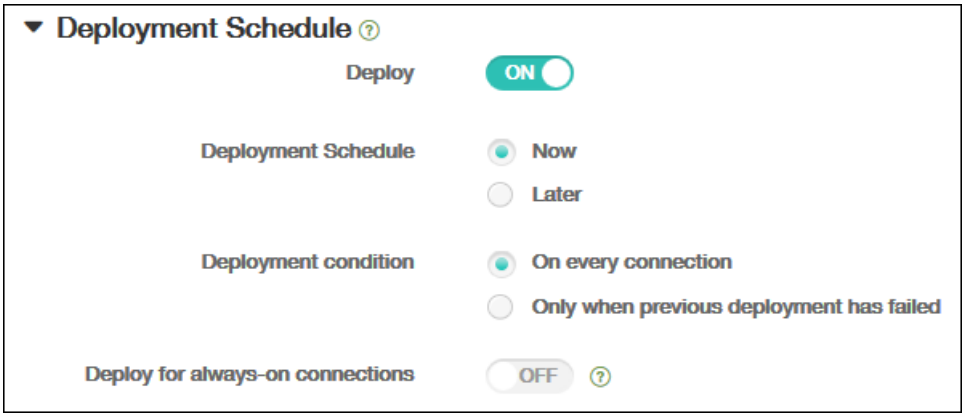


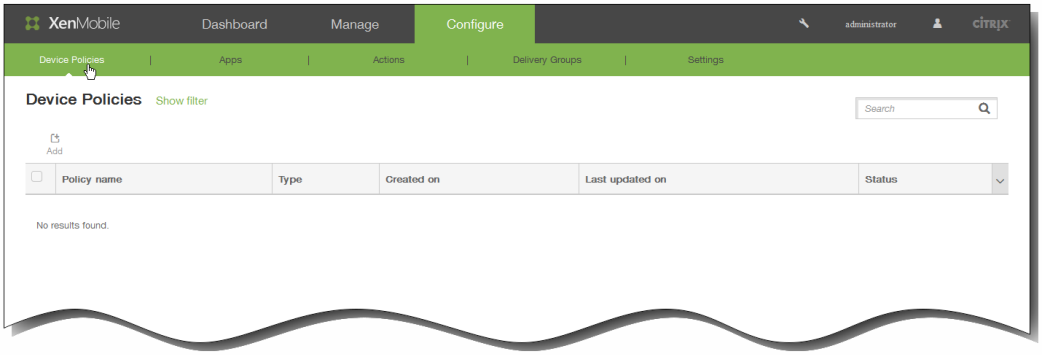


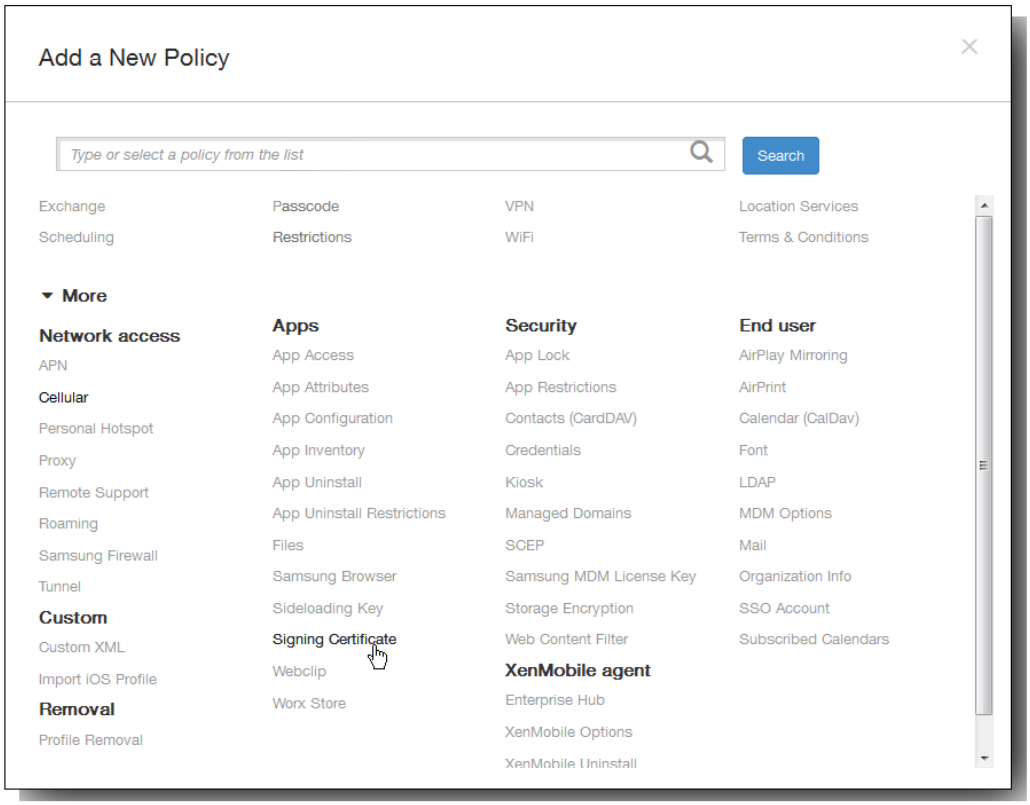


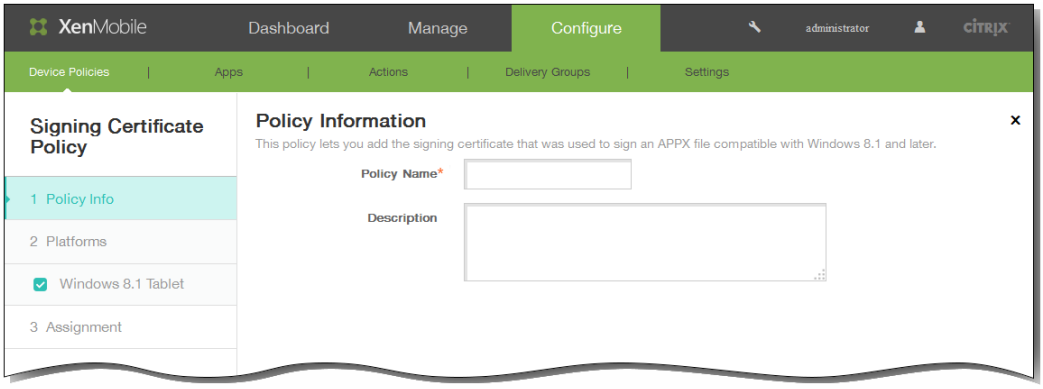


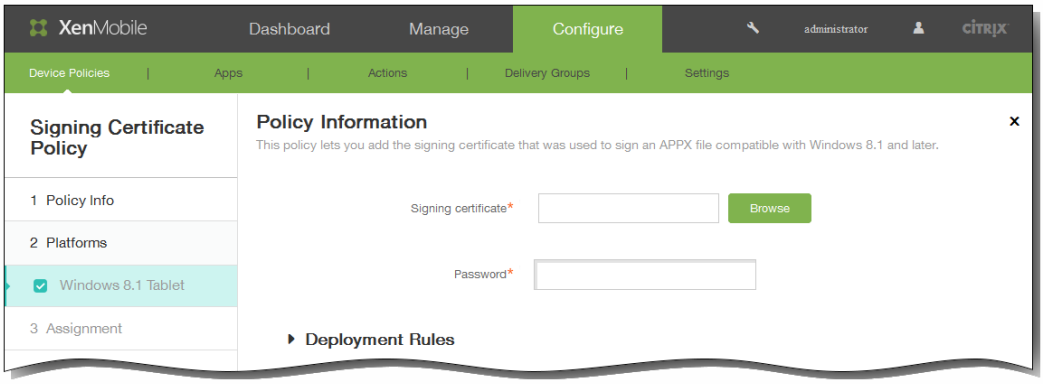


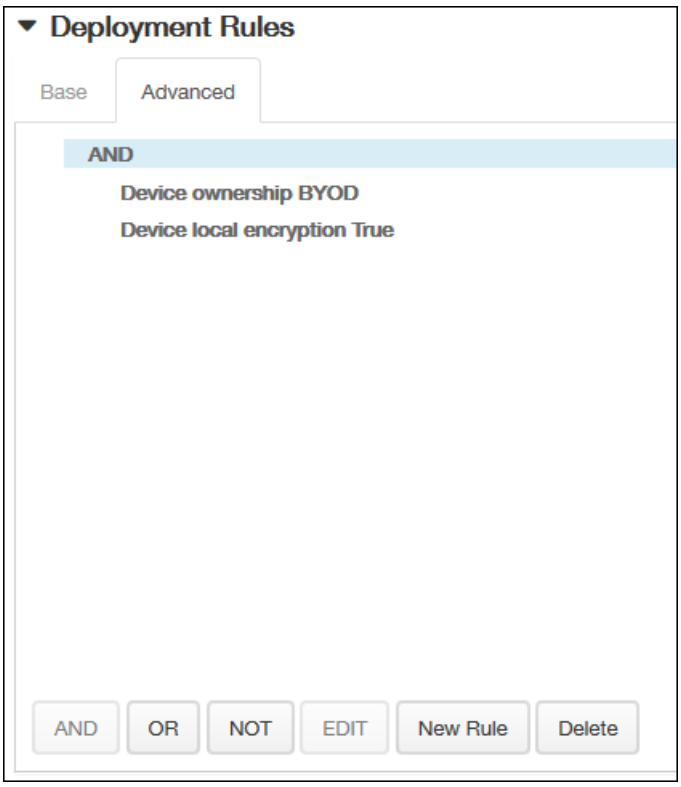


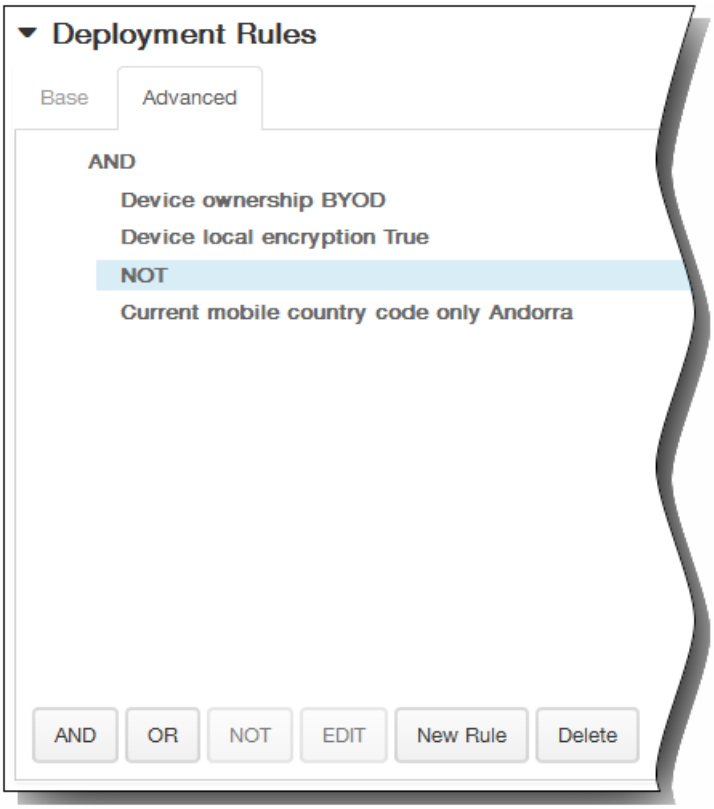


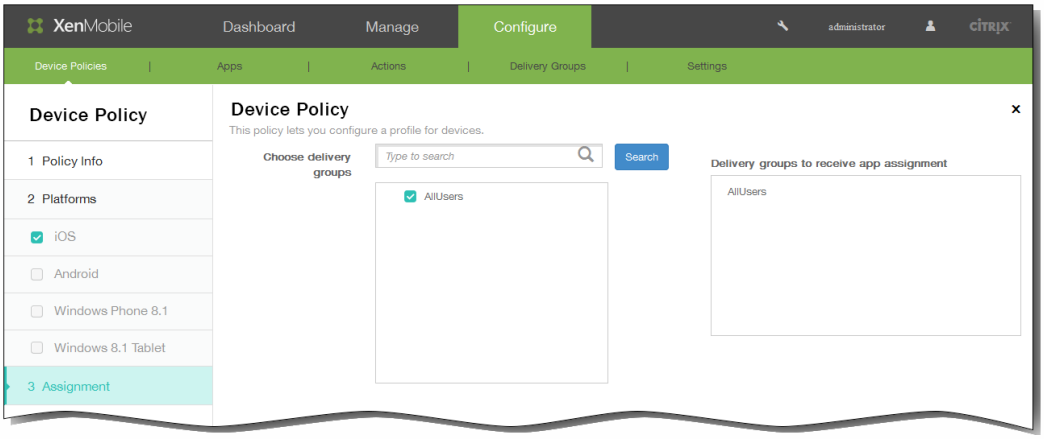


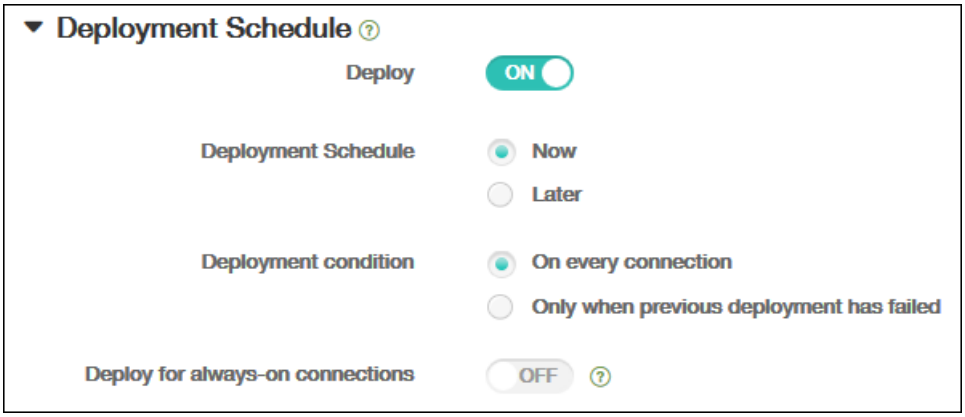


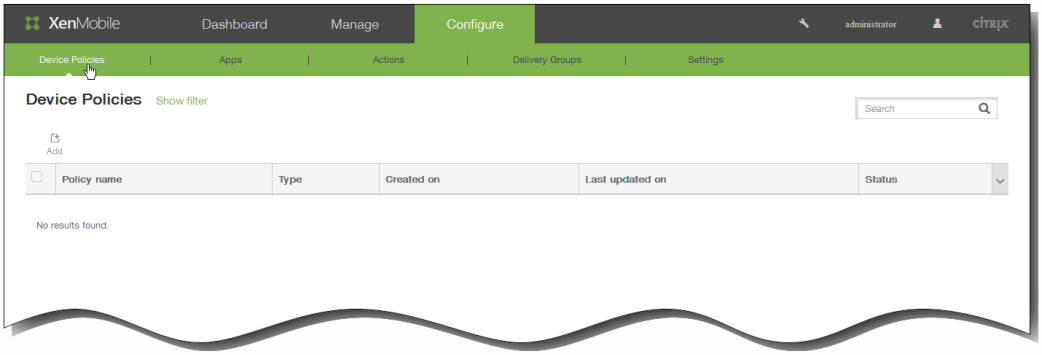


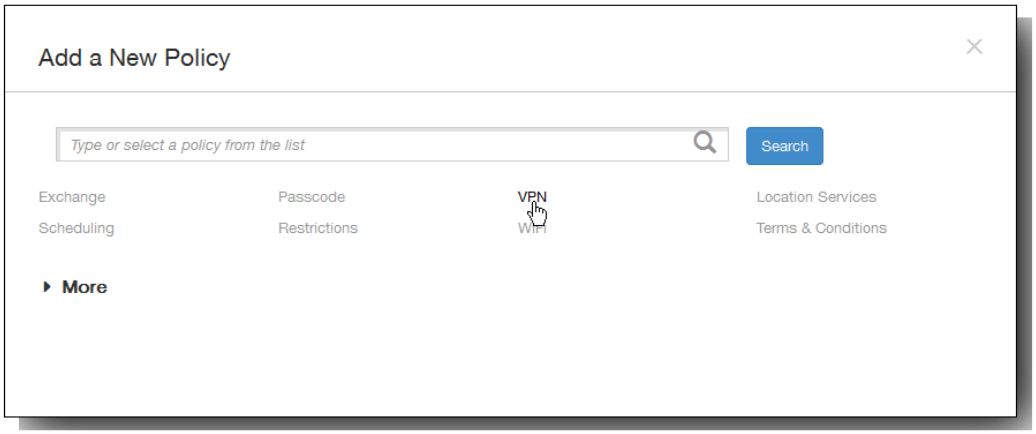


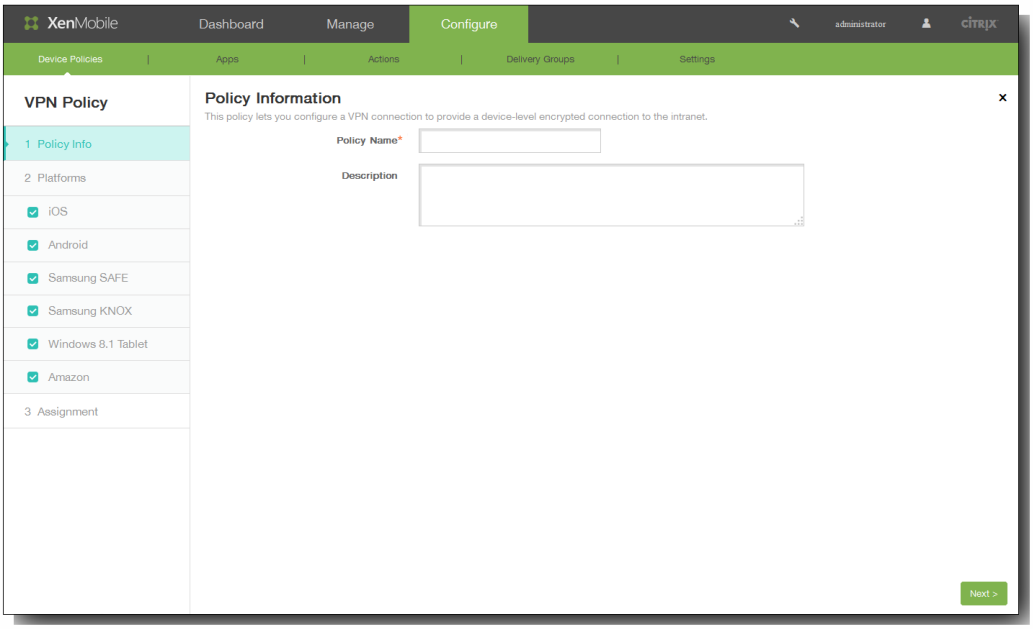


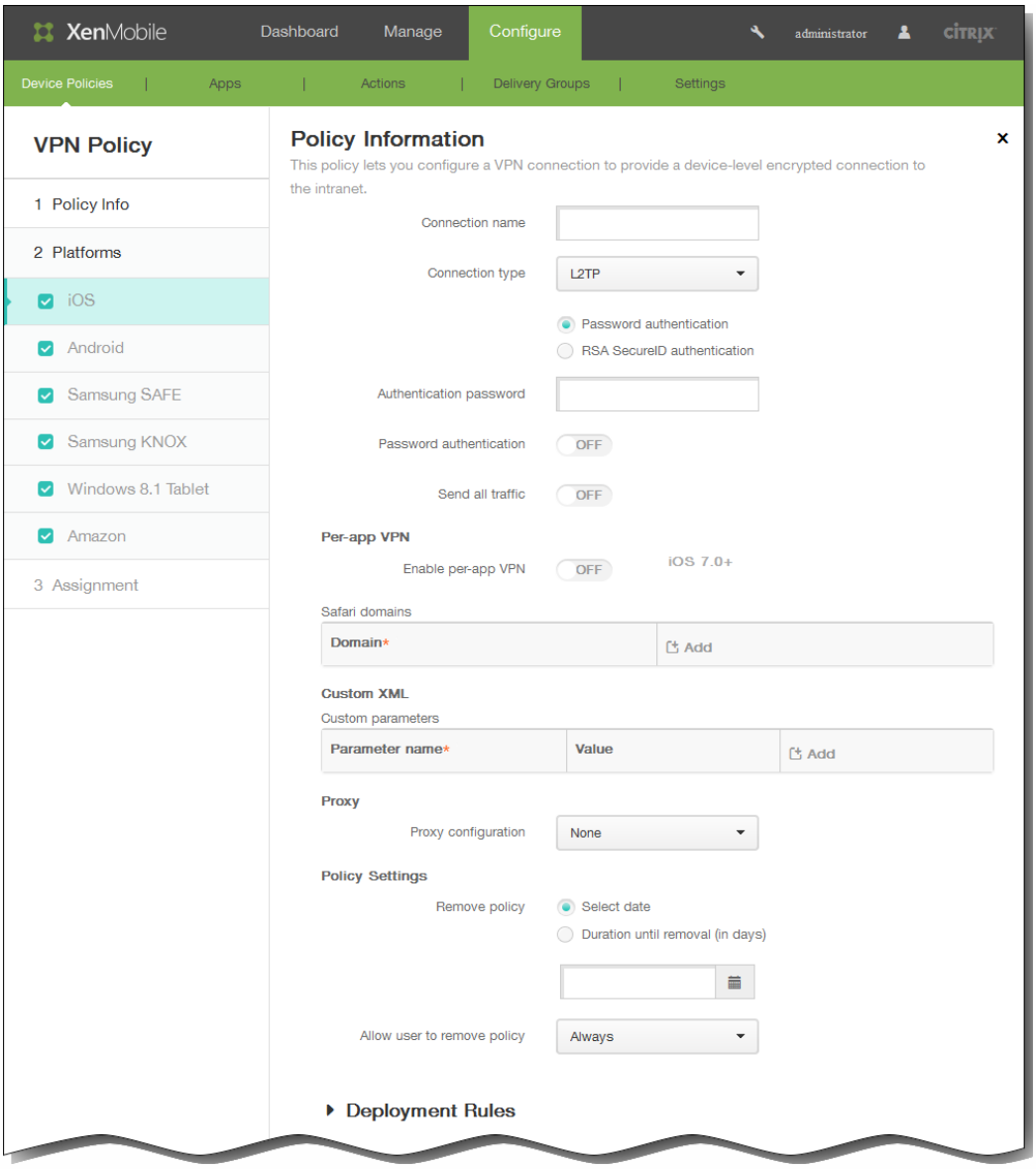




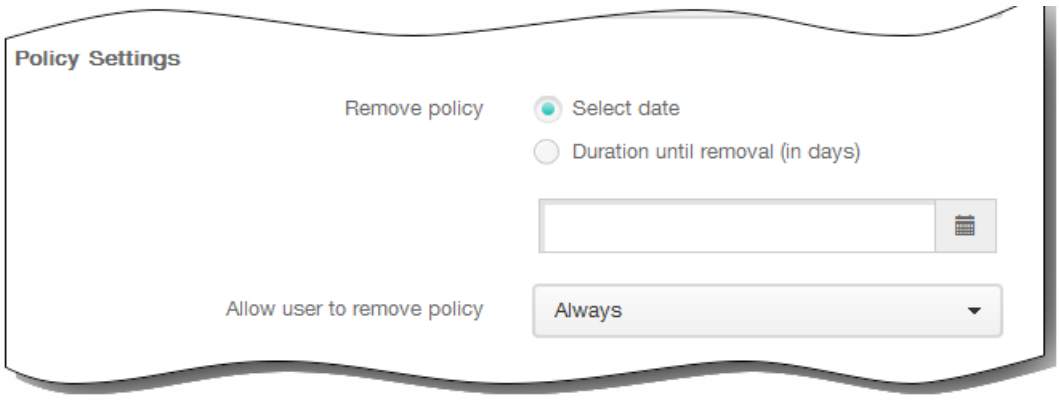


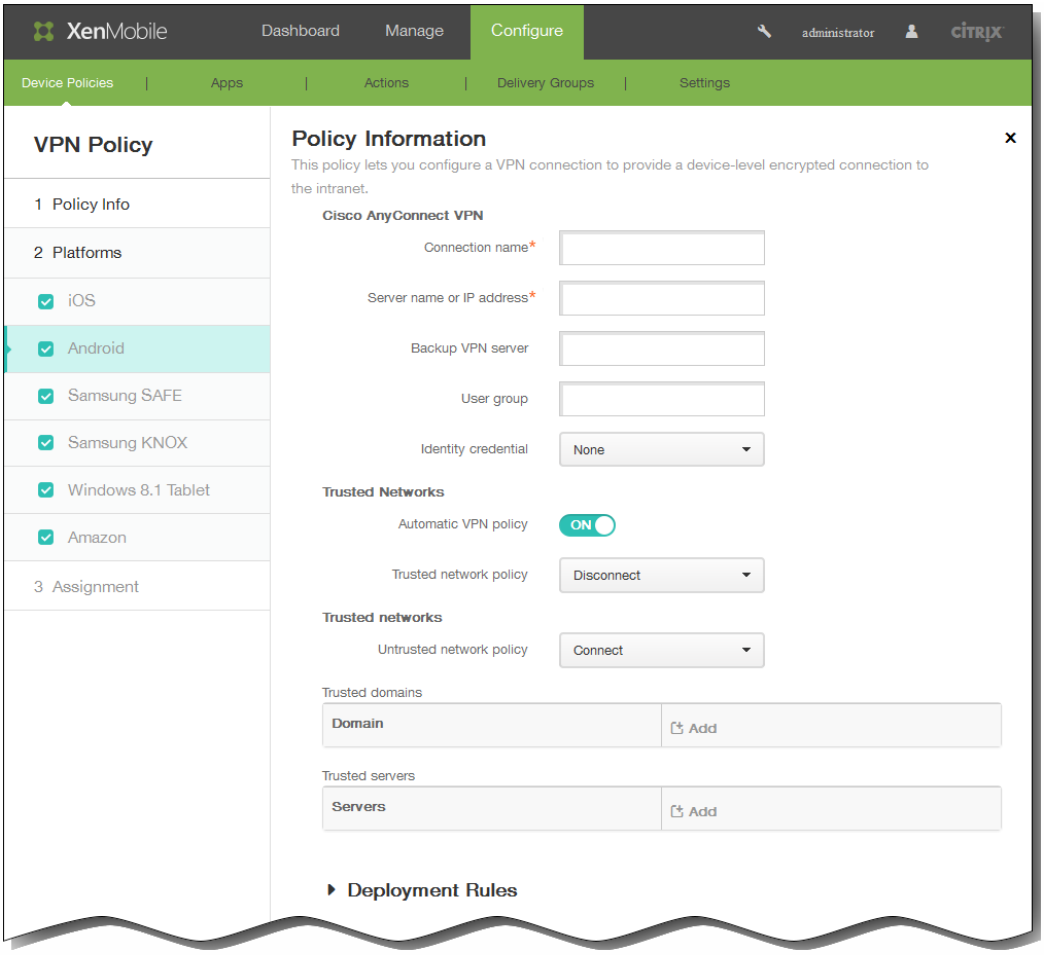




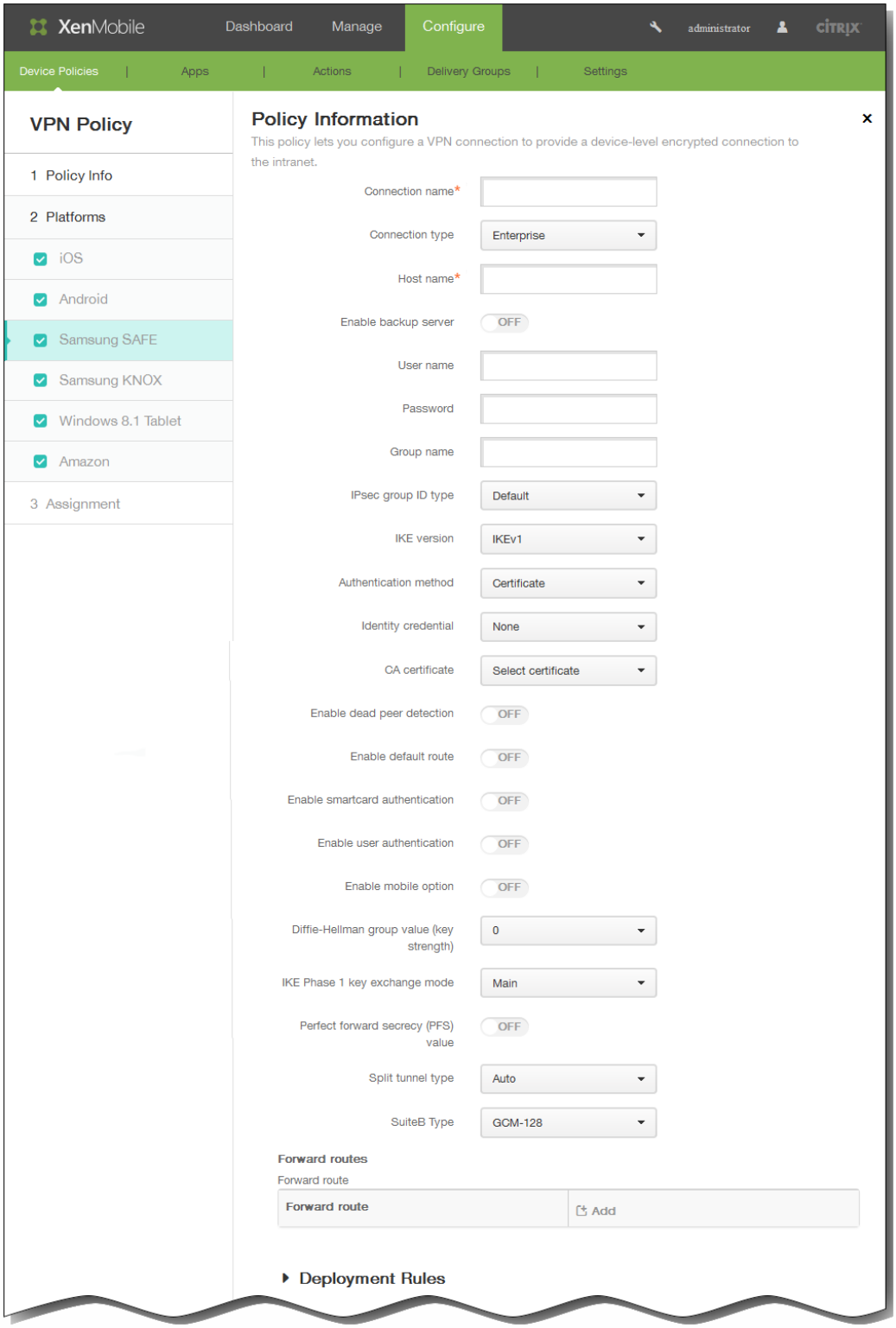


-
-
-
-
-
-
-
-
-
-

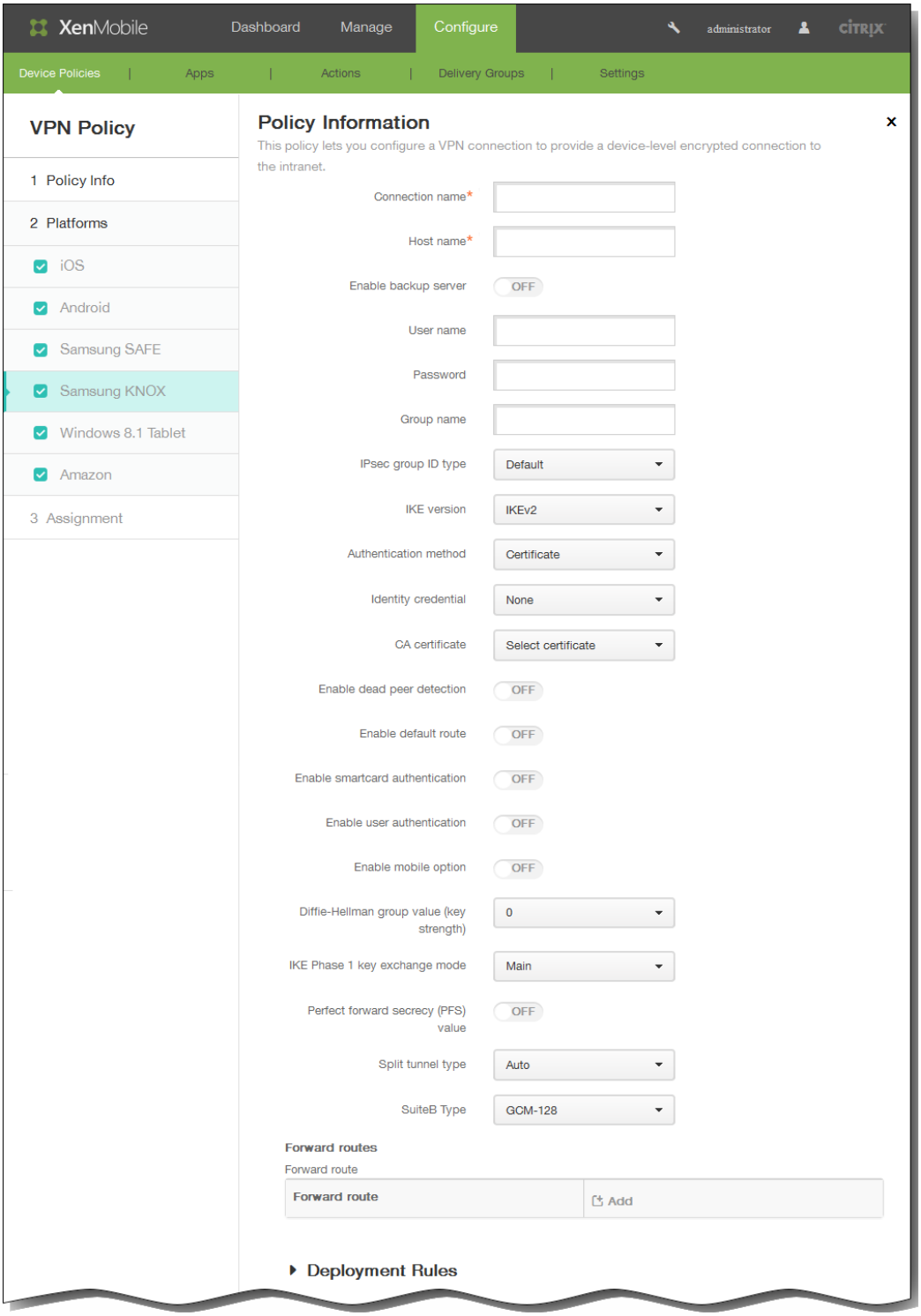




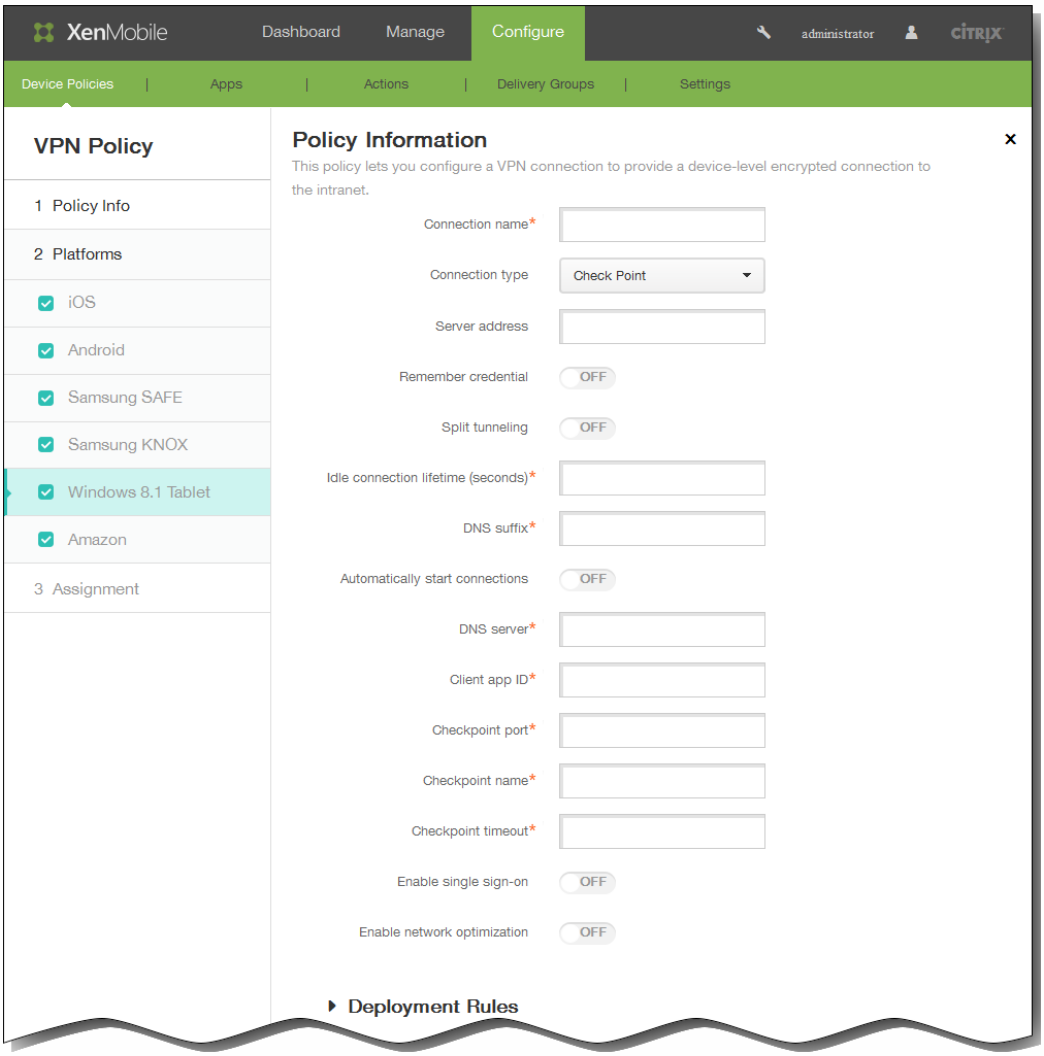
-
-



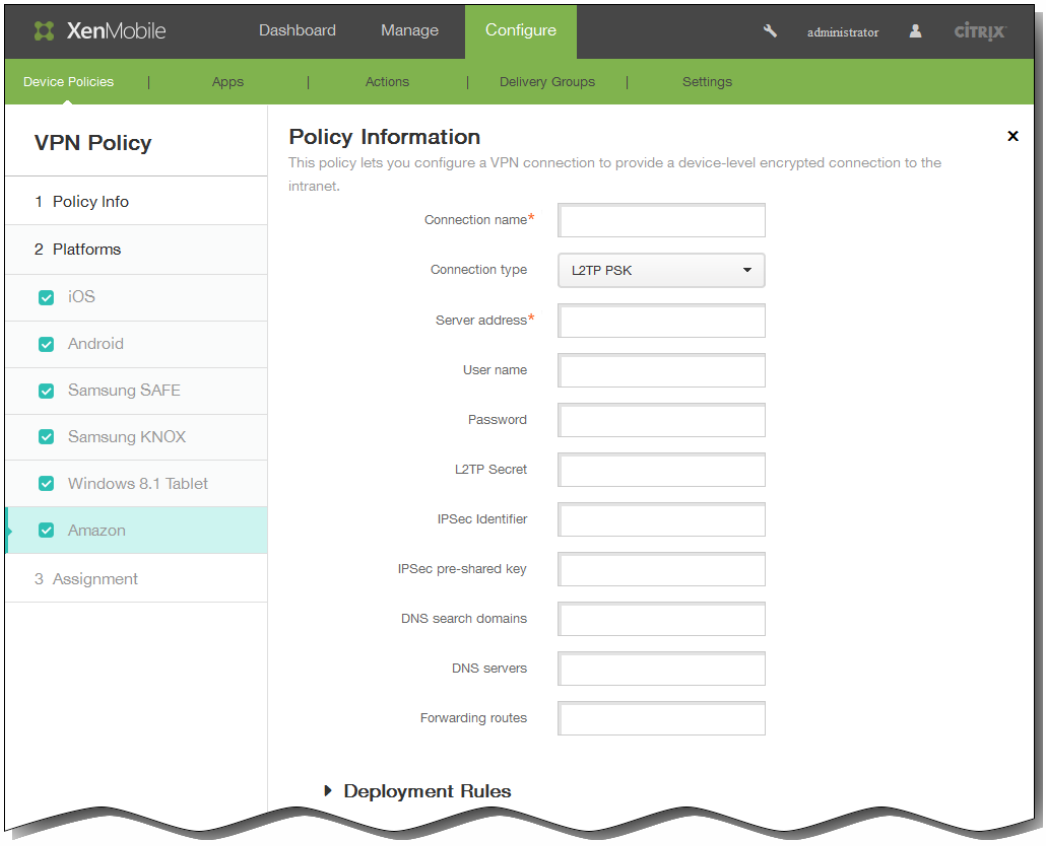
-
-
-
-



-
-
-
-
-

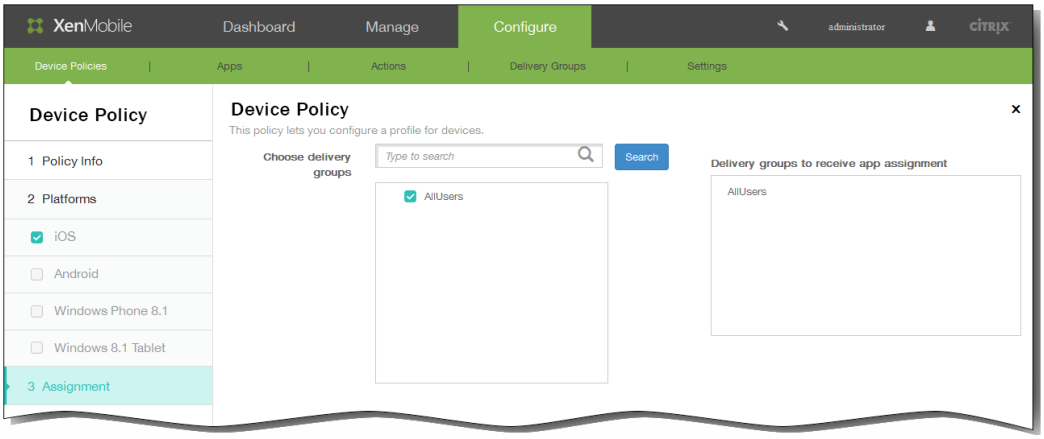


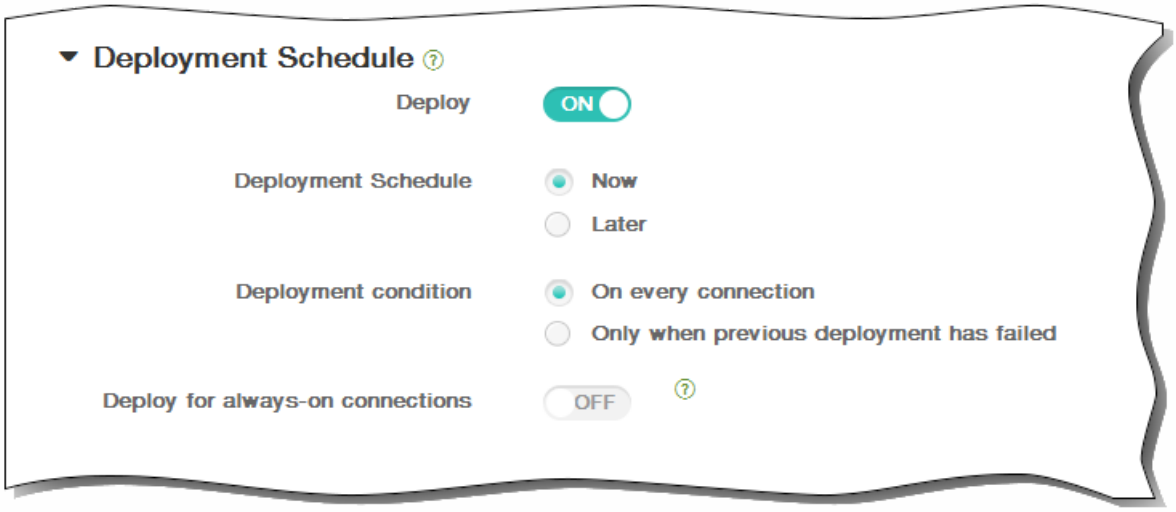
-
-
-
-
-



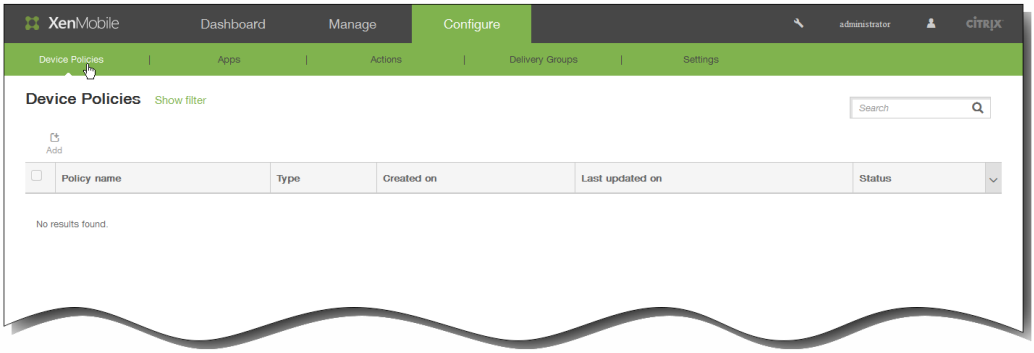
-
-

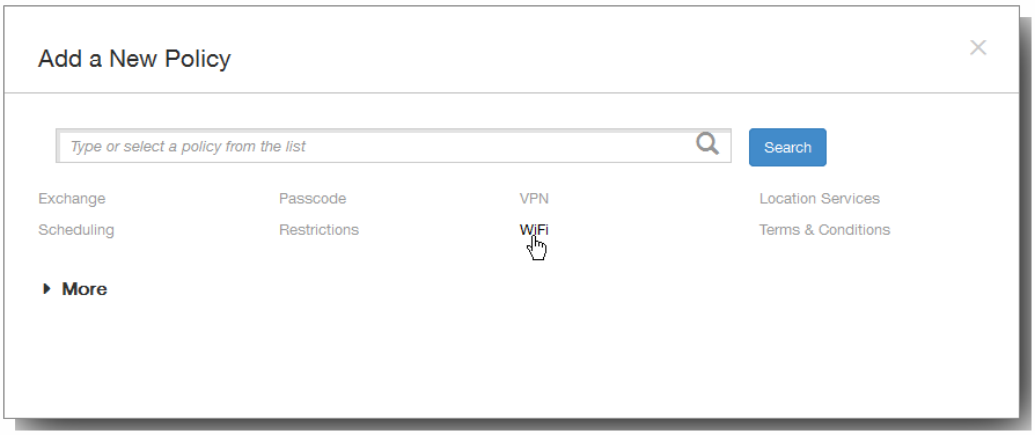
-
-
-
-

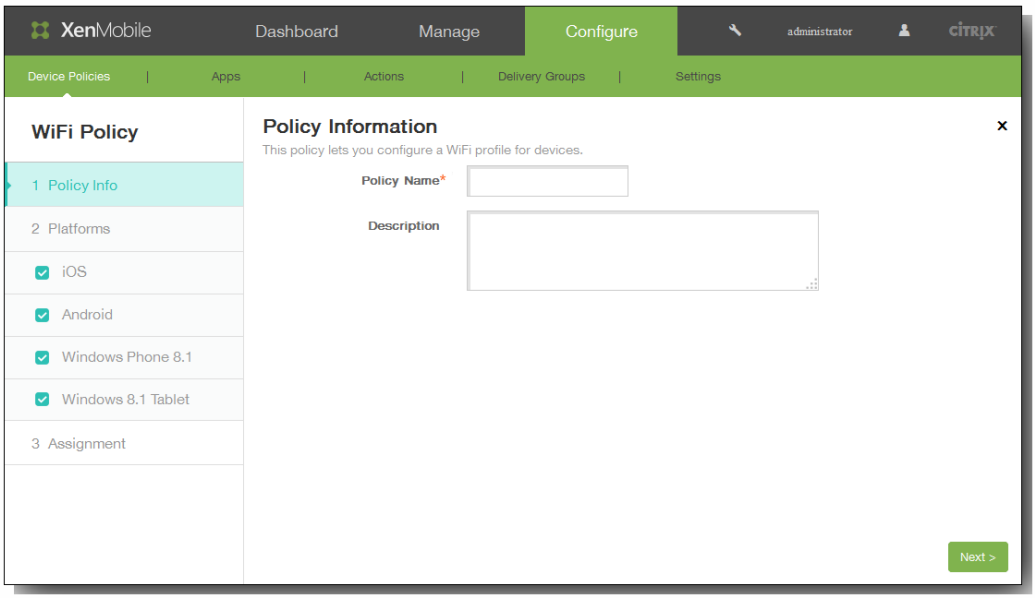


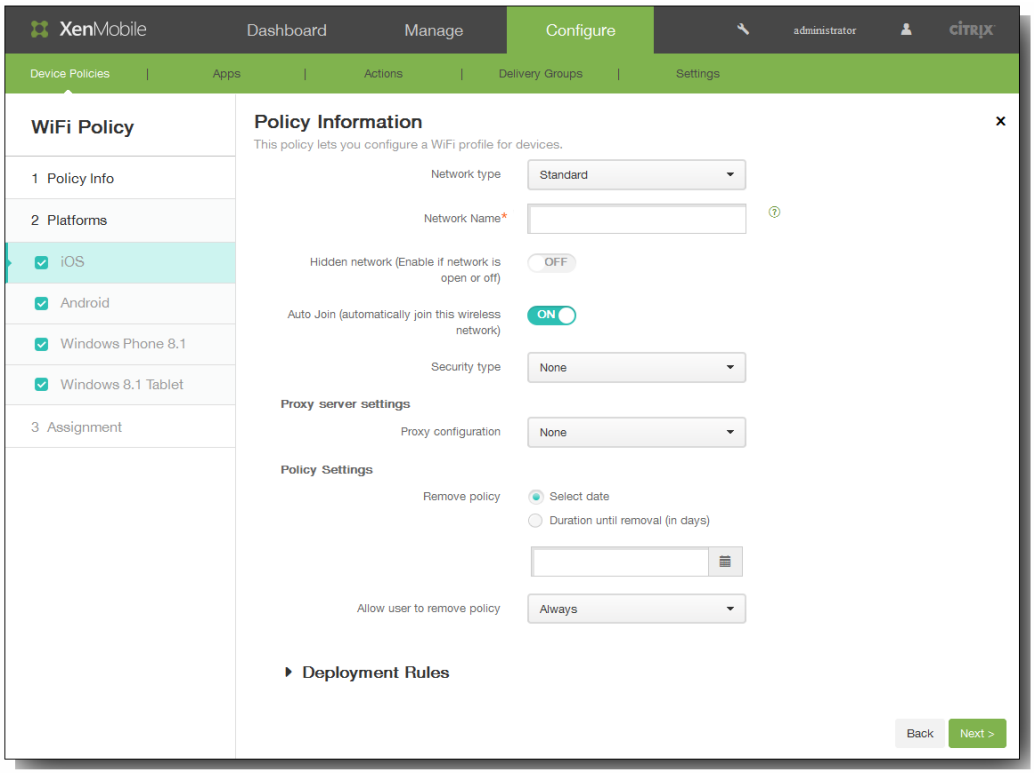


-
-
-
-
-
-

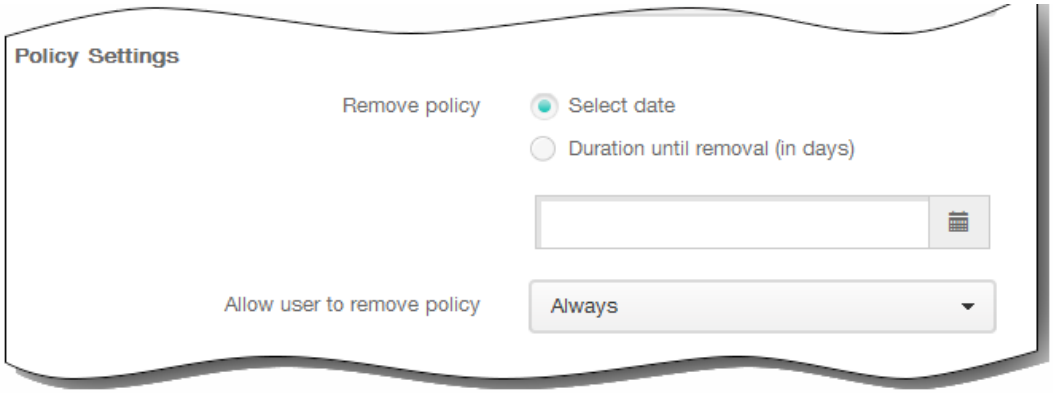


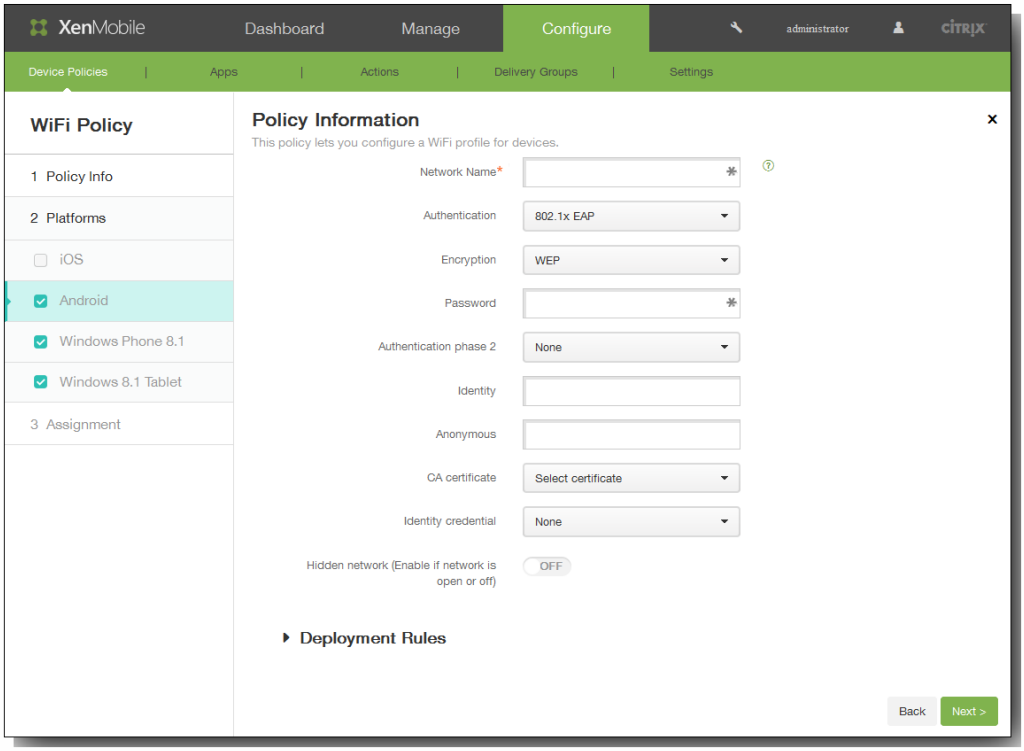






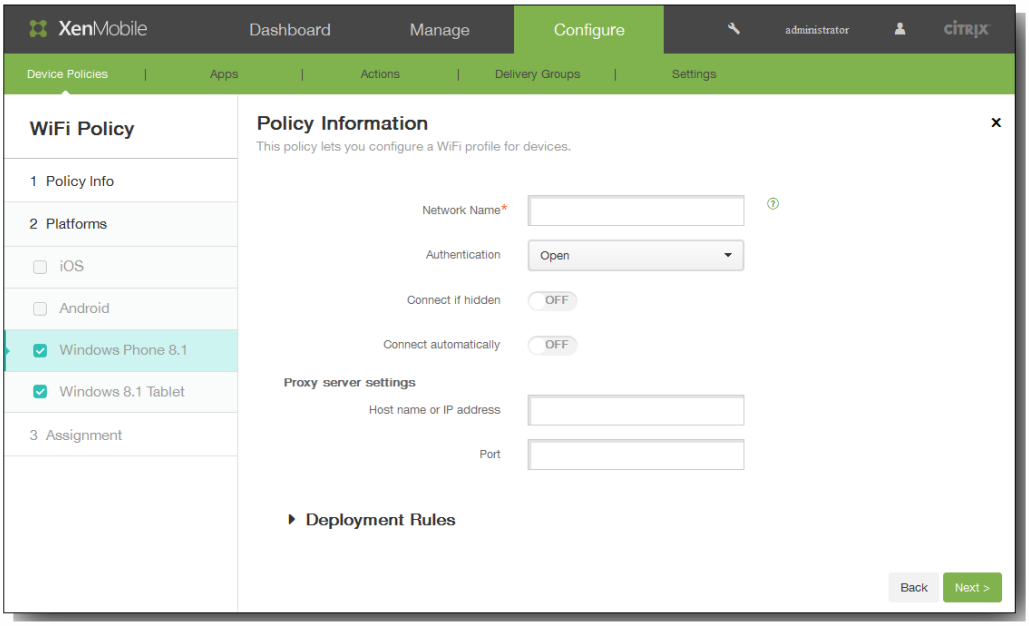
-
-
-
-
-
-
-



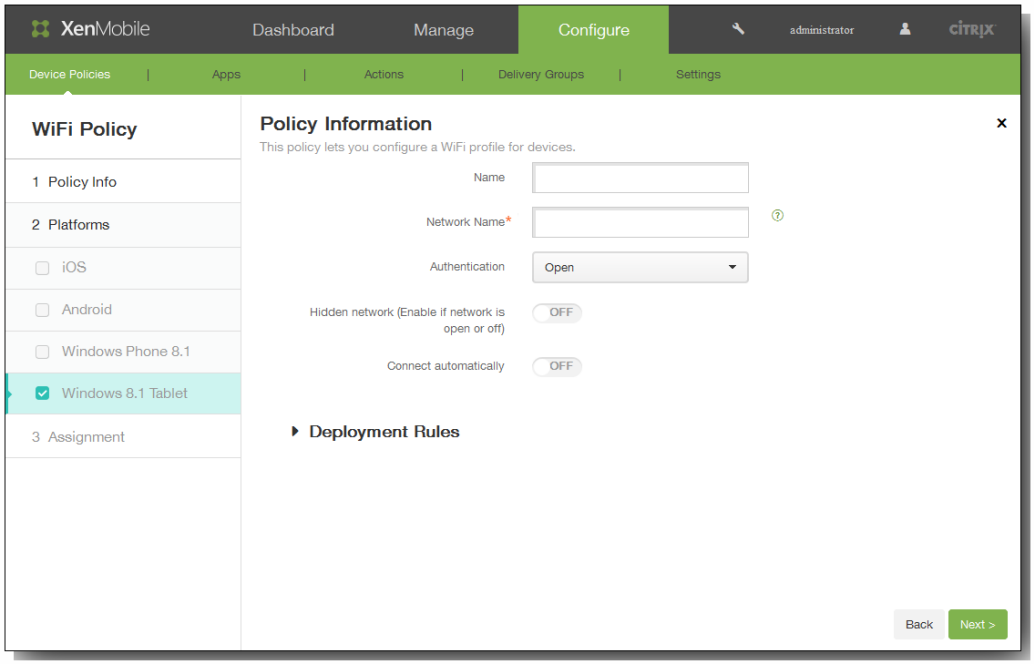


-
-
-
-
-

-
-

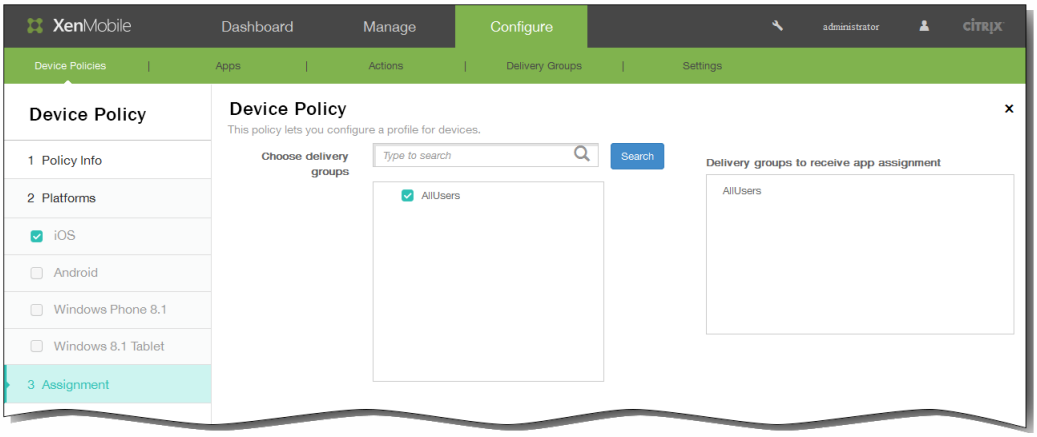


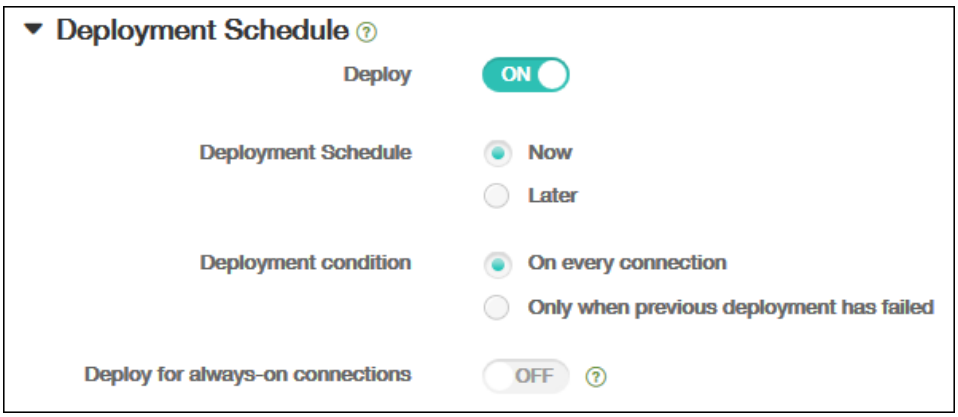
-
-
-
-

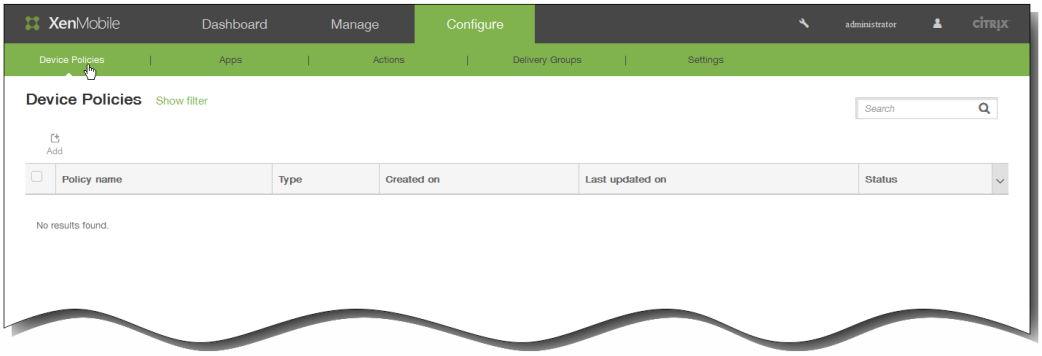


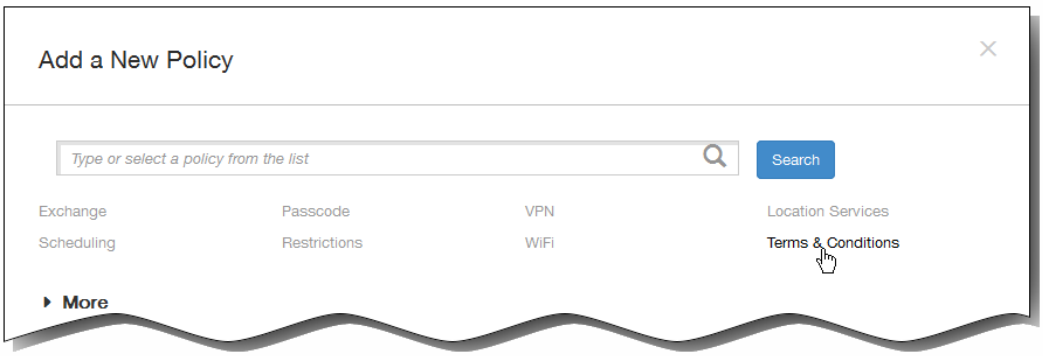
-
-
-

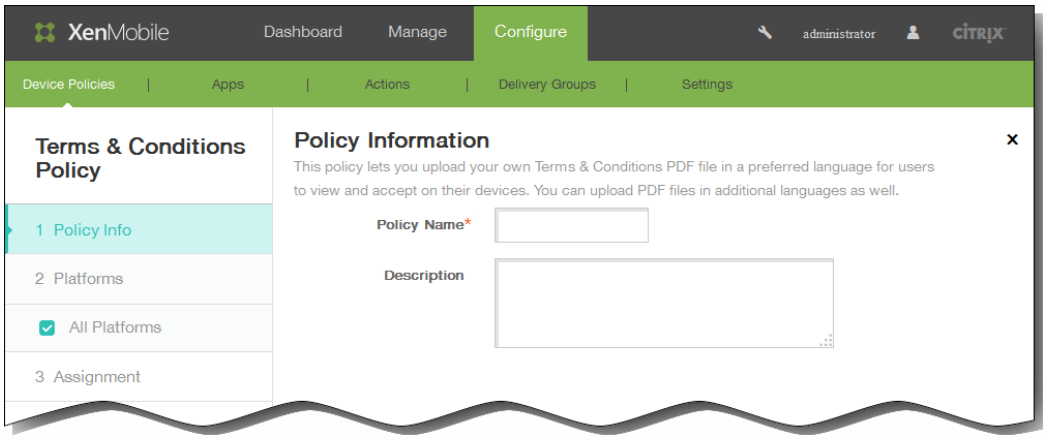
-
-

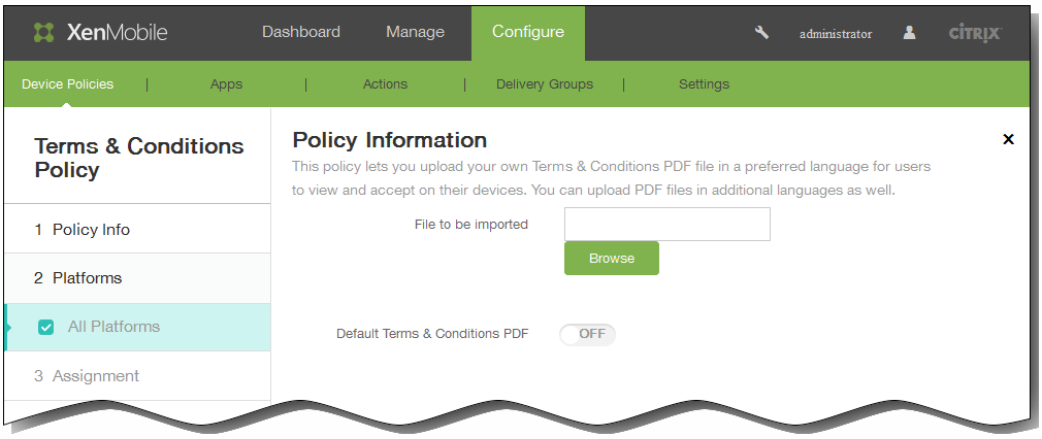


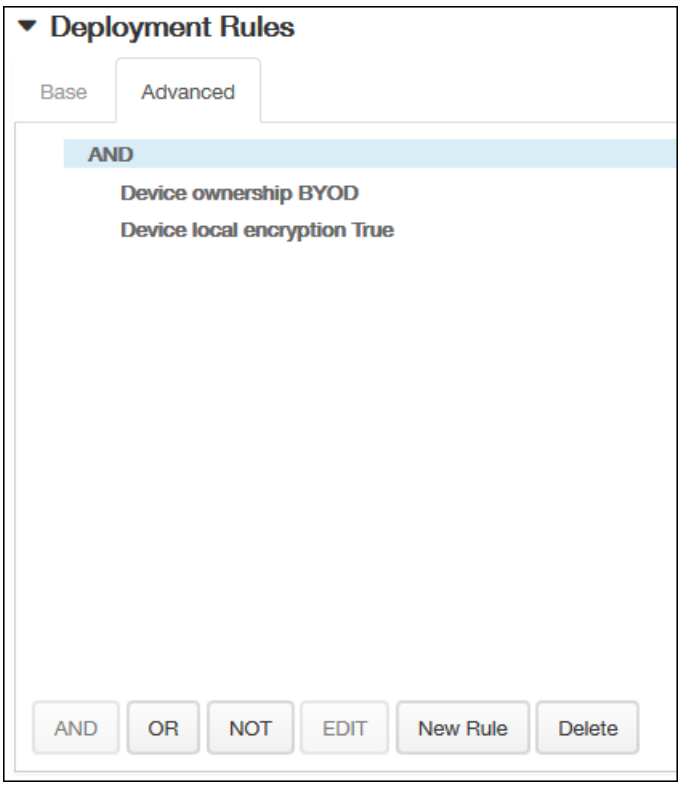


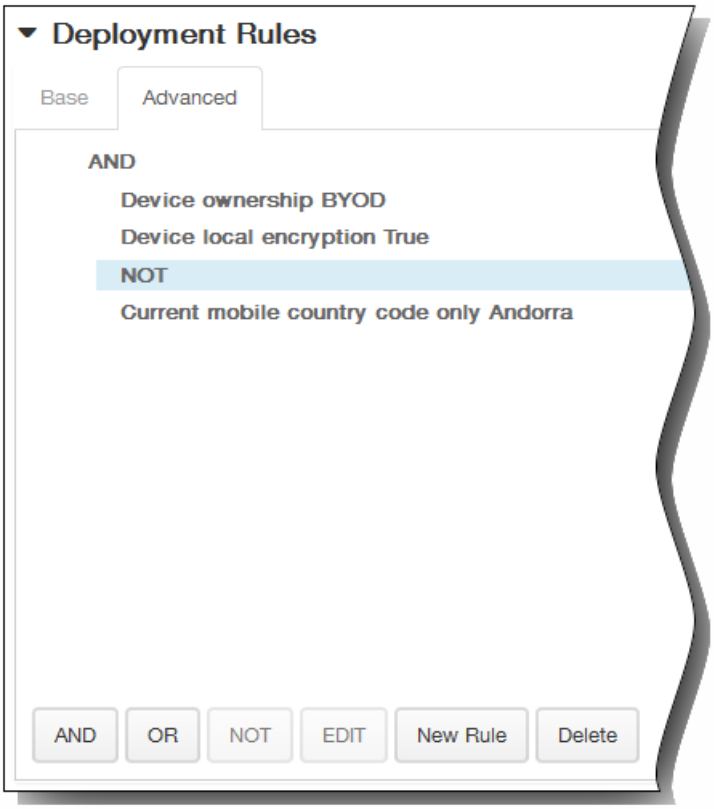


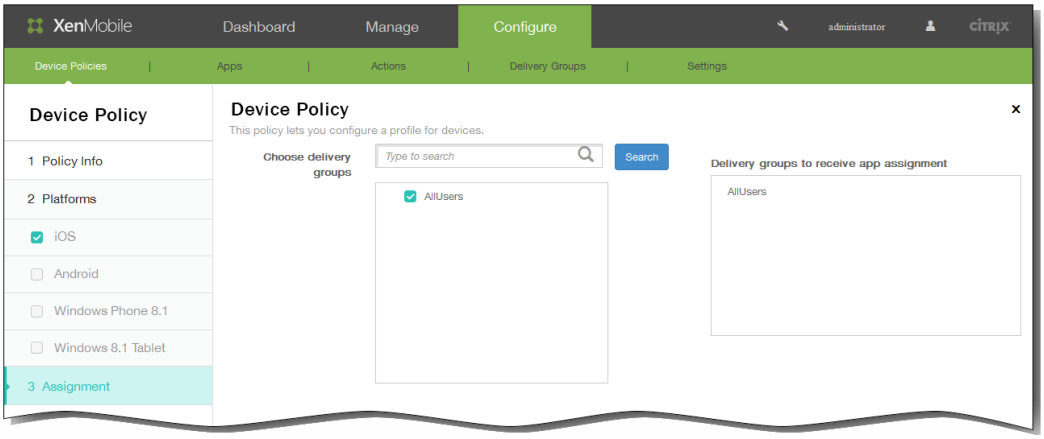


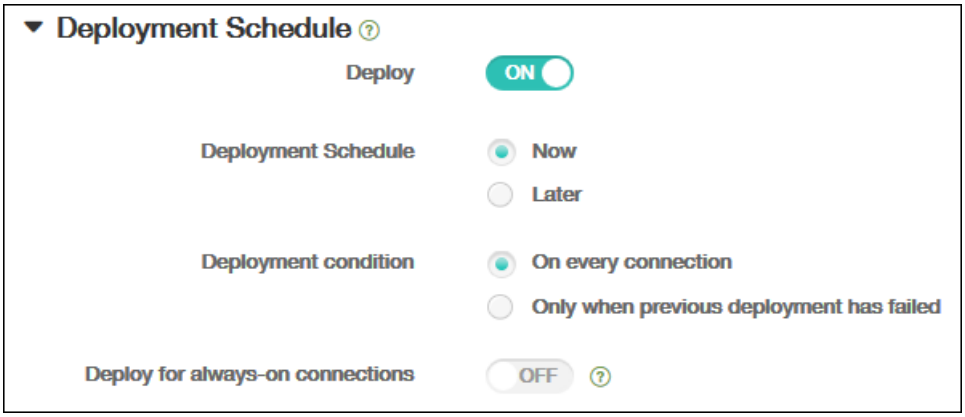


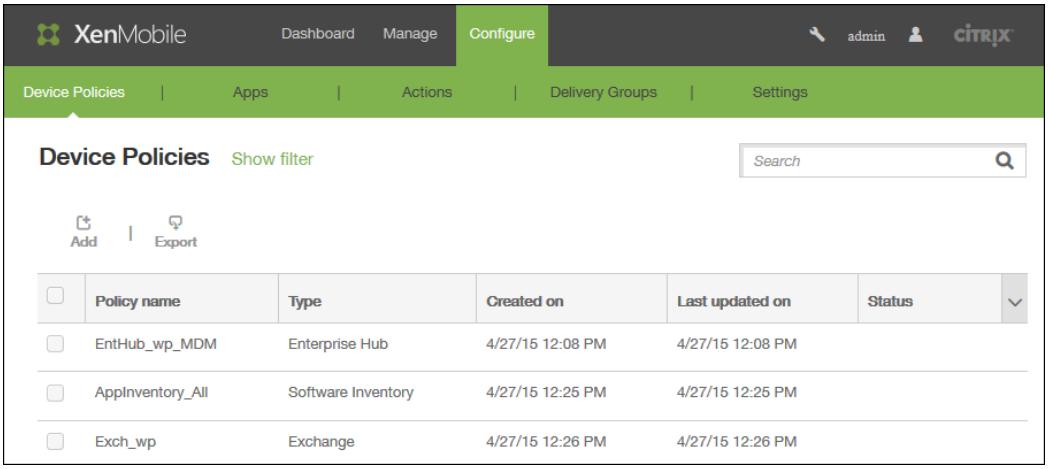


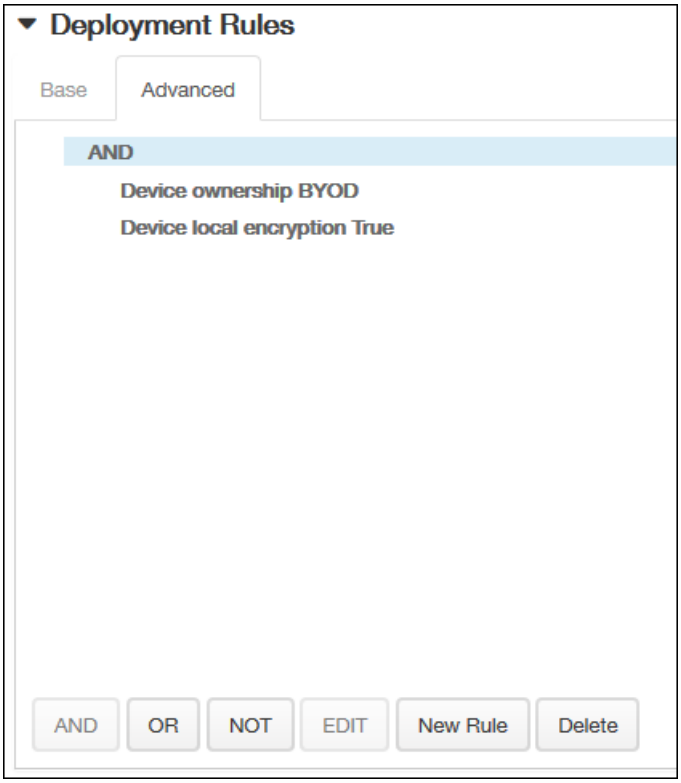


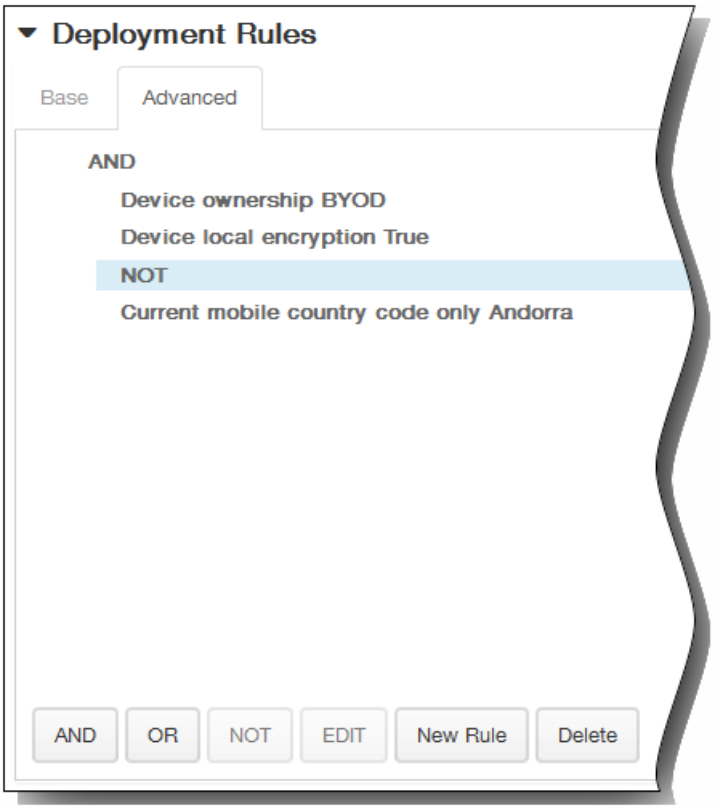


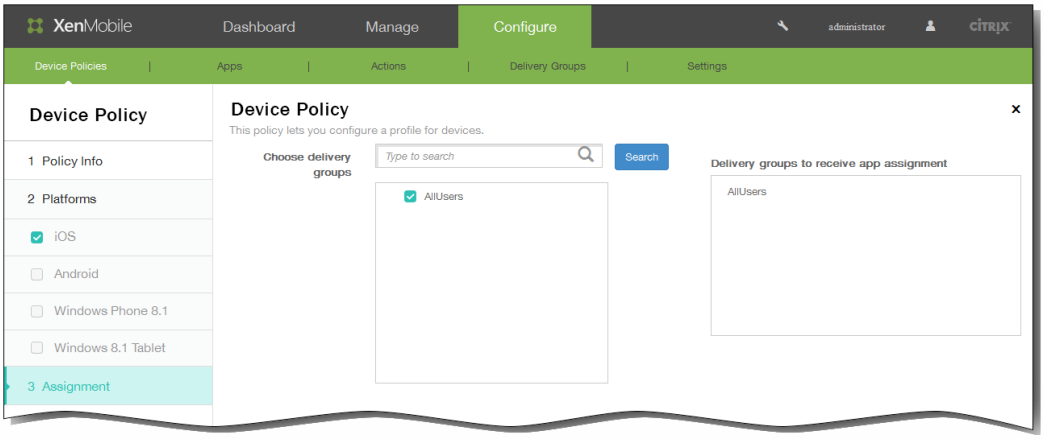


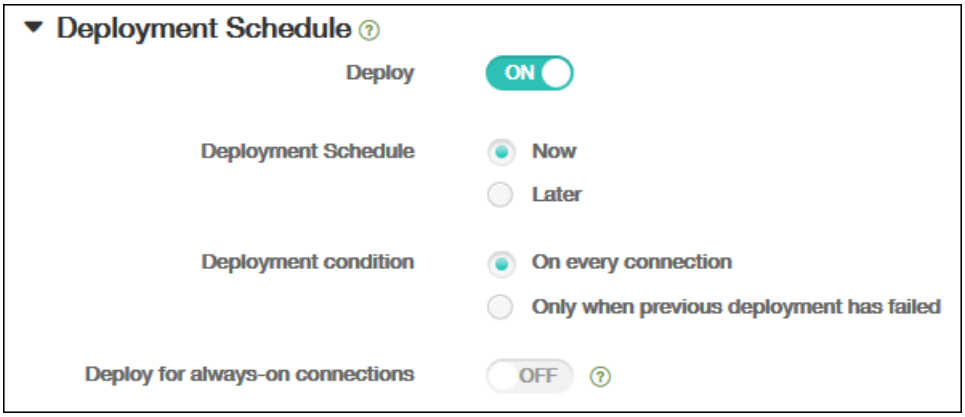


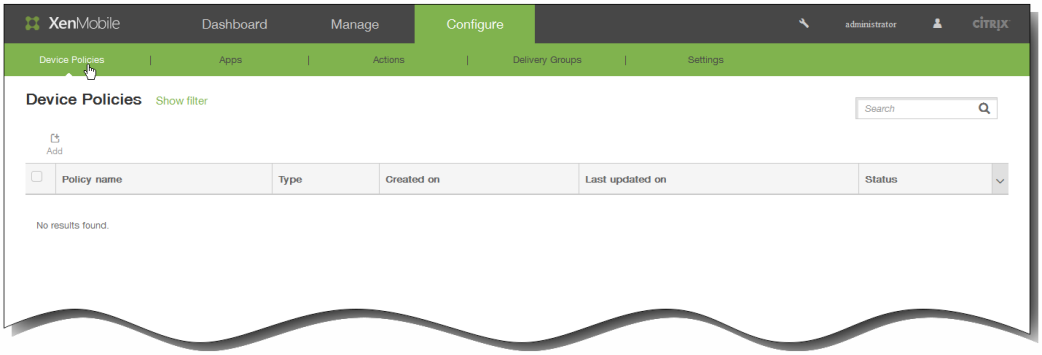


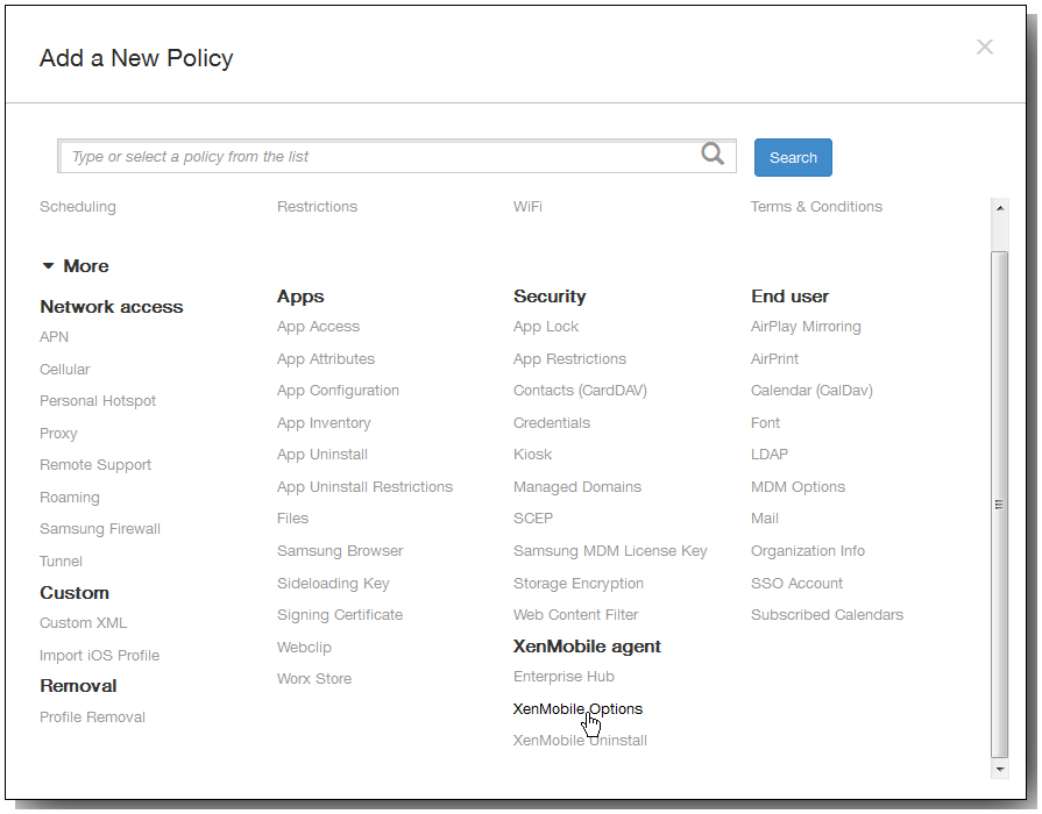


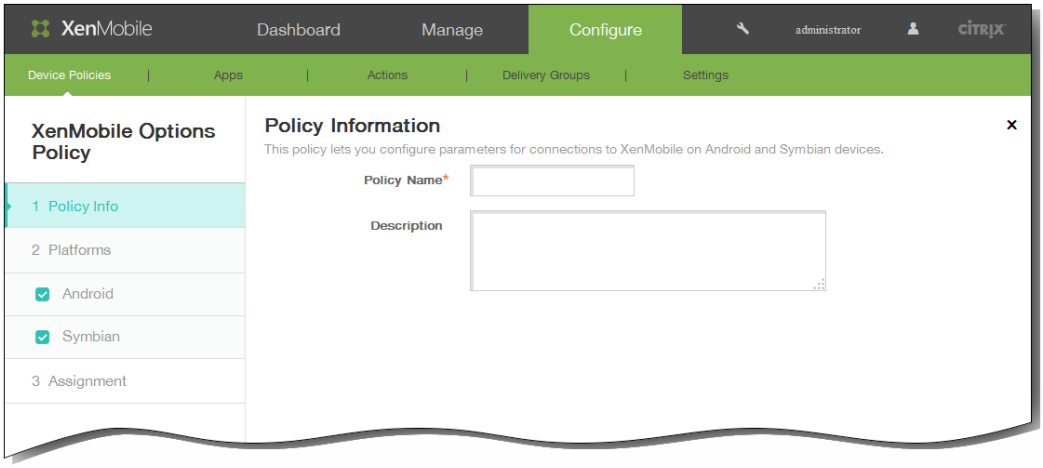


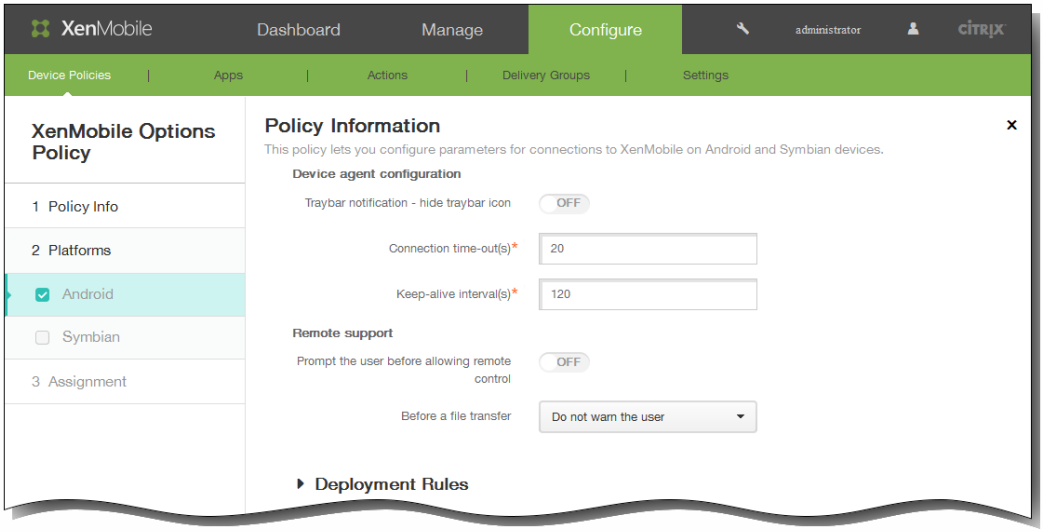


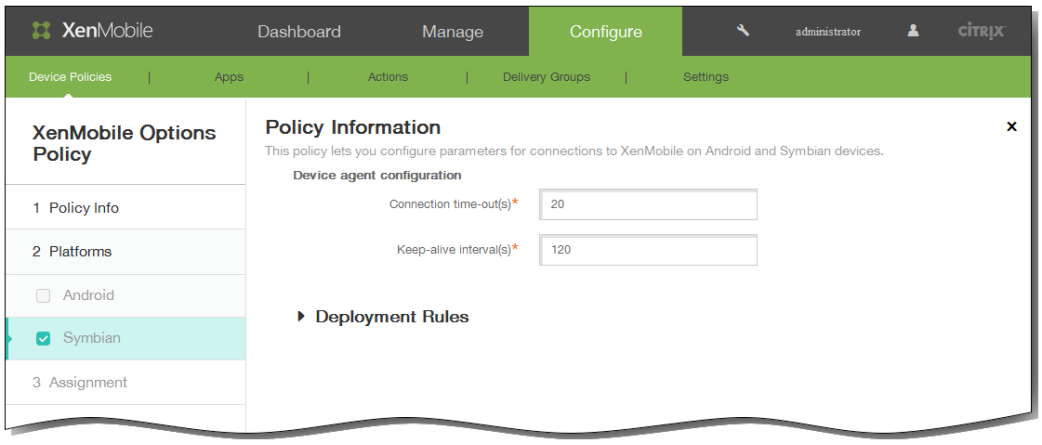


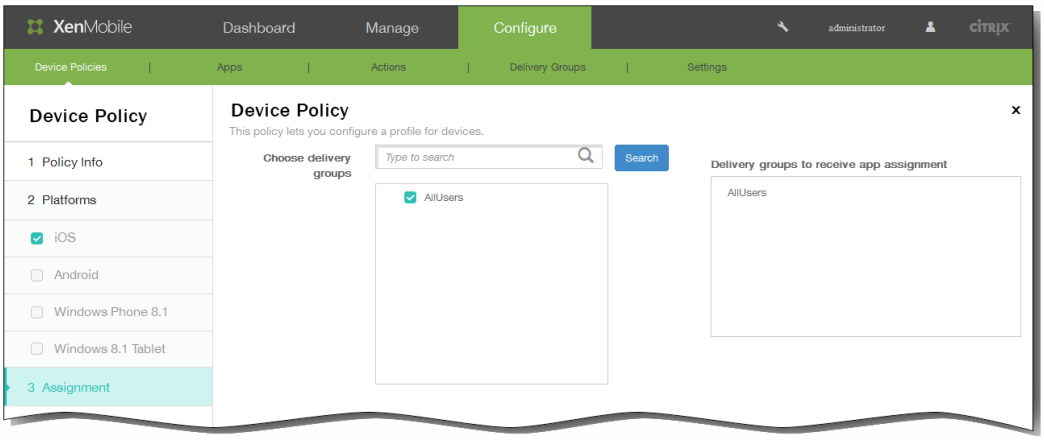


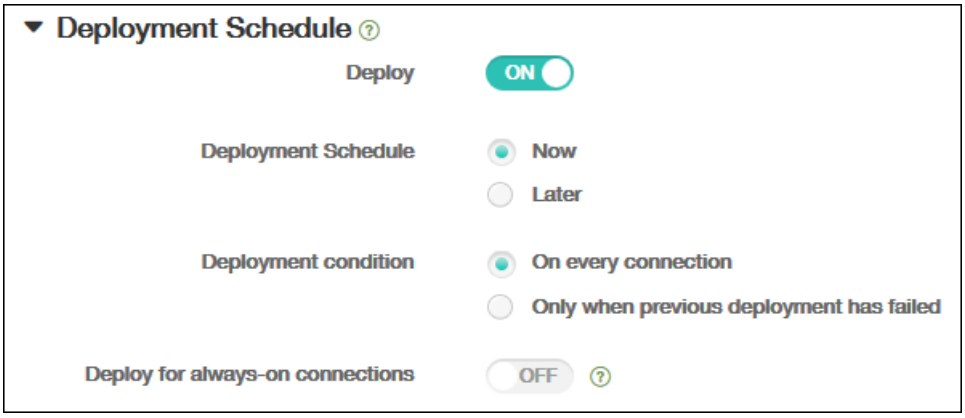


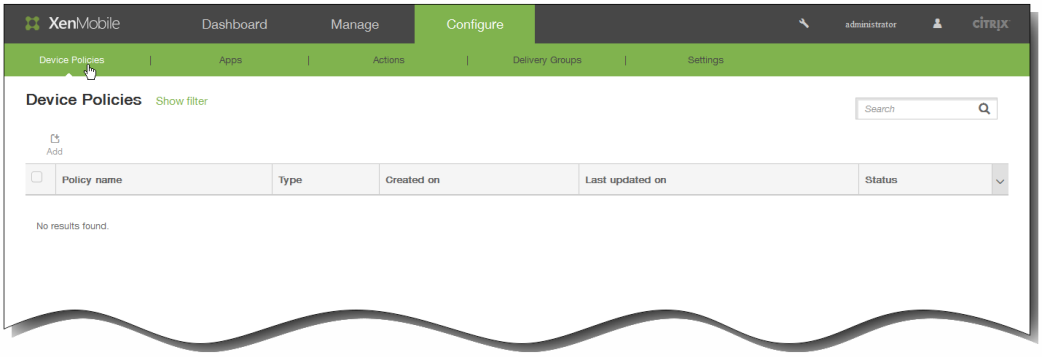


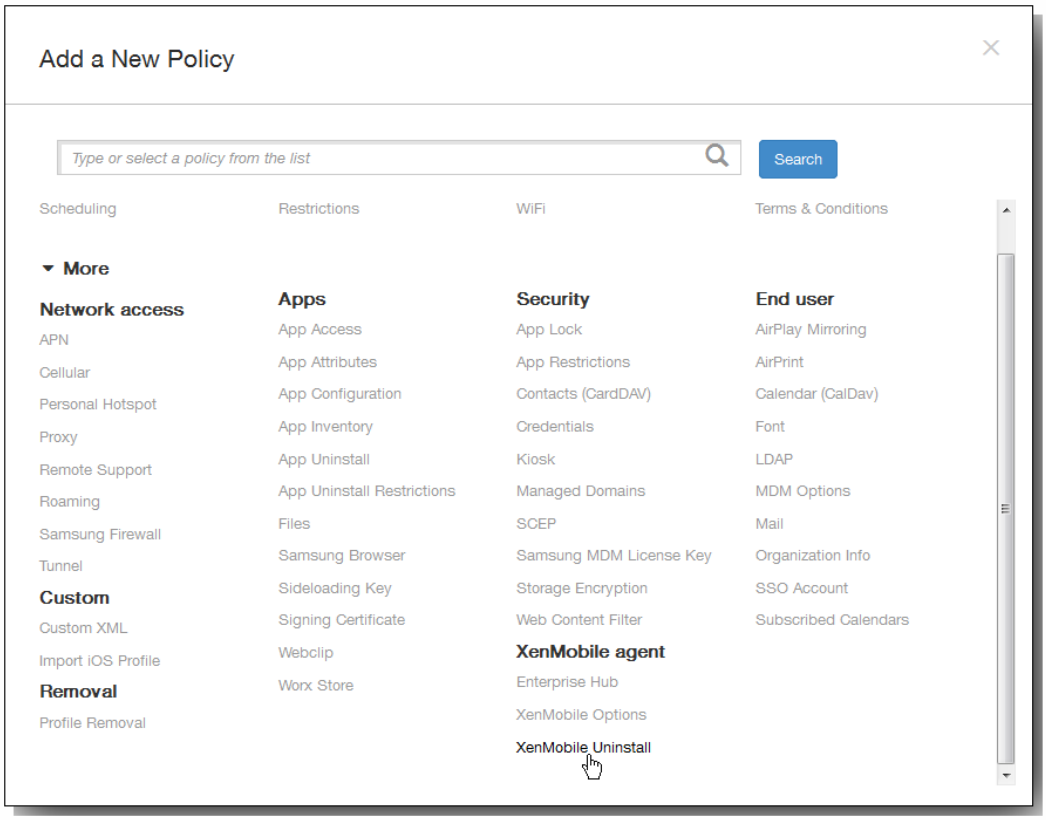


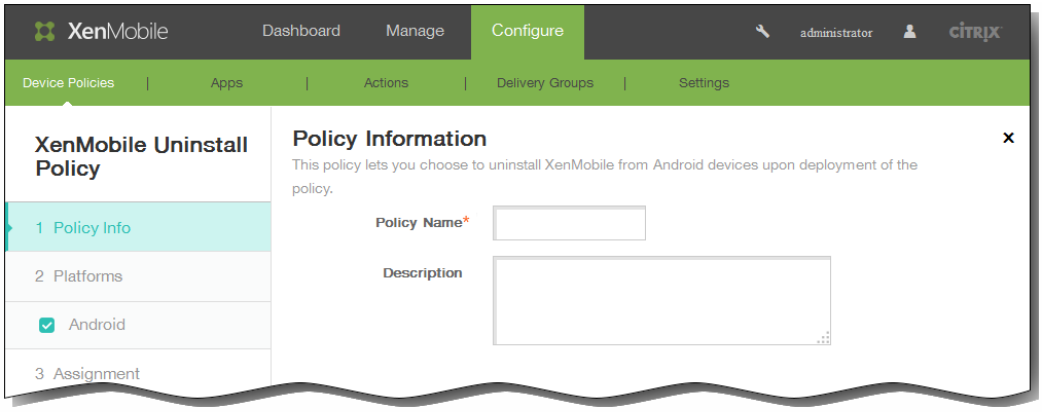


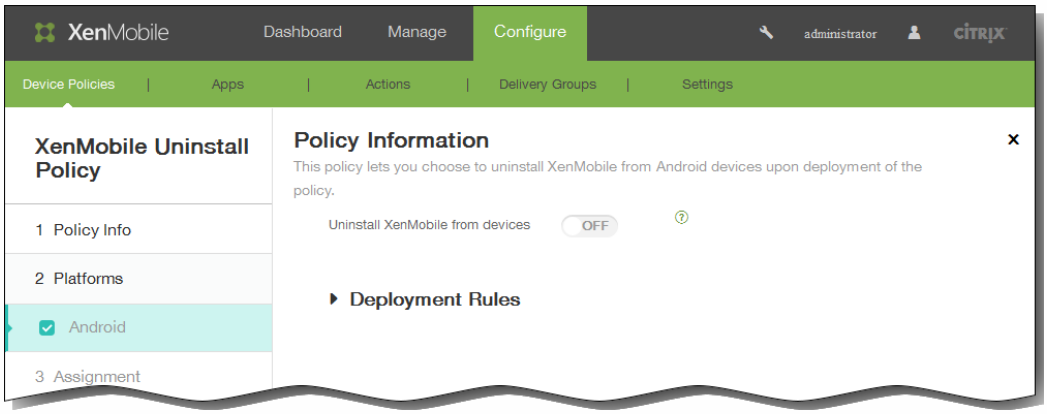


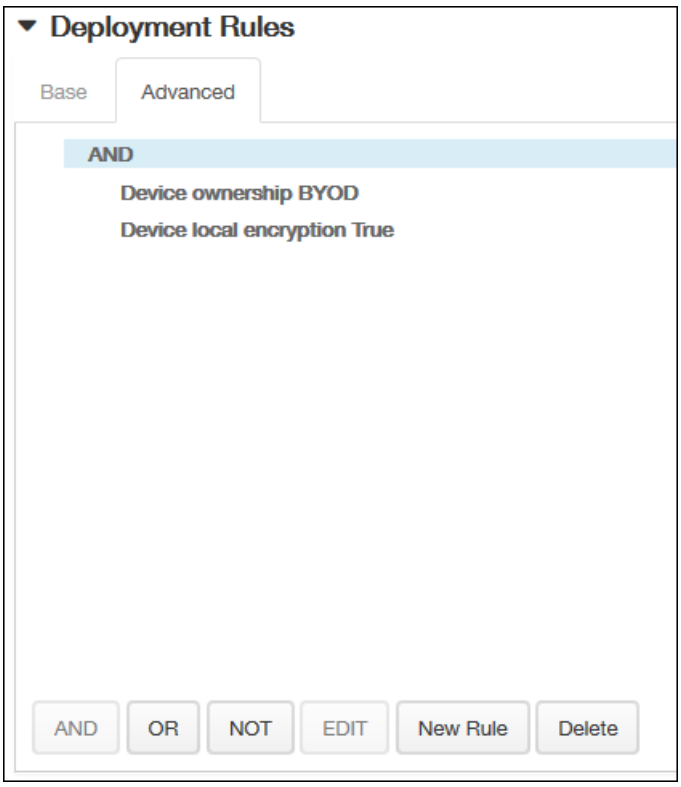


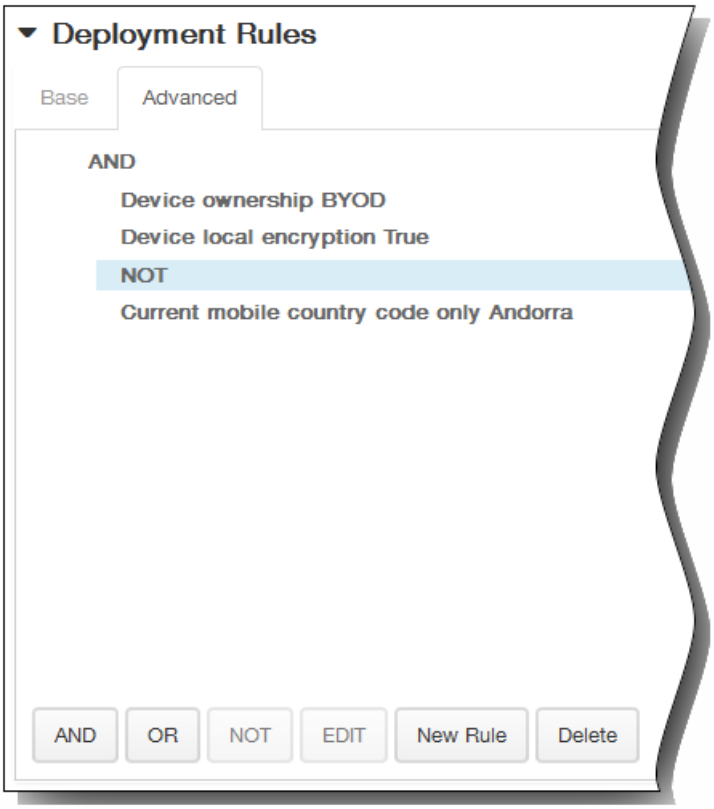


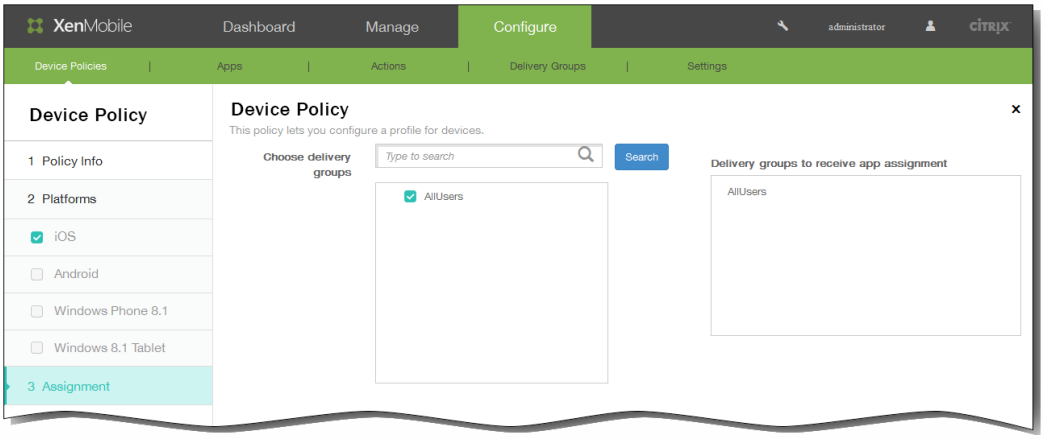


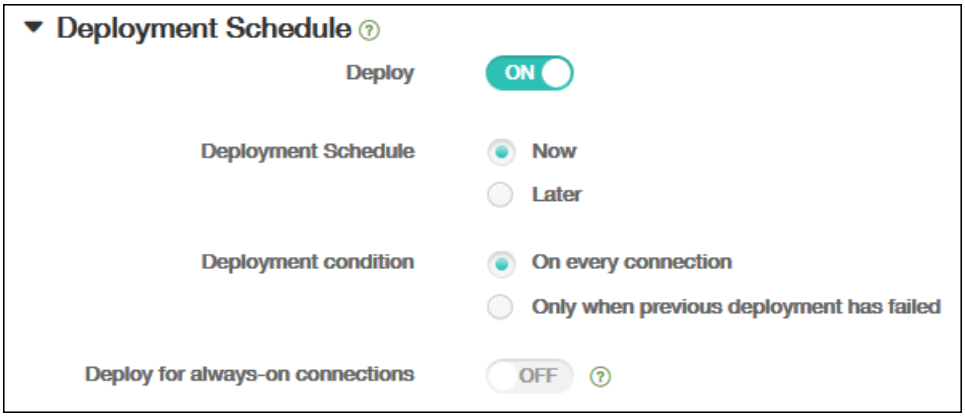






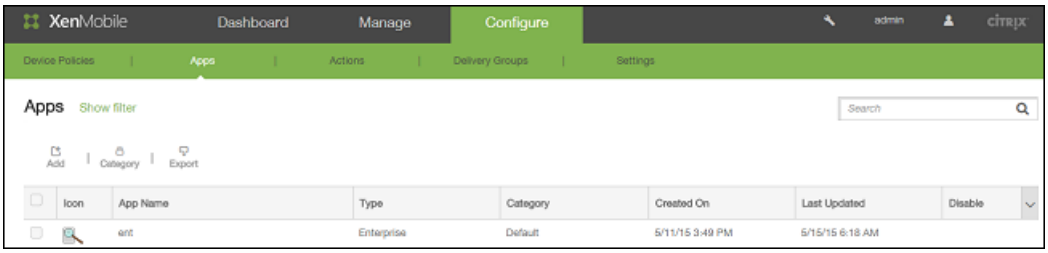






-
-
-
-
-
-
-

-
-
-
-



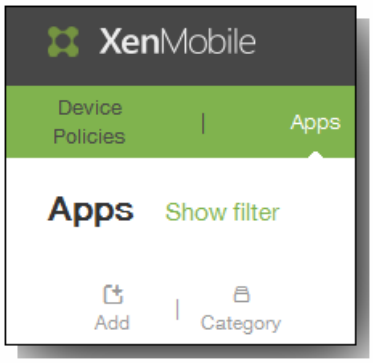
-
-
-
-
-

向 XenMobile 中添加 MDX 应用程序

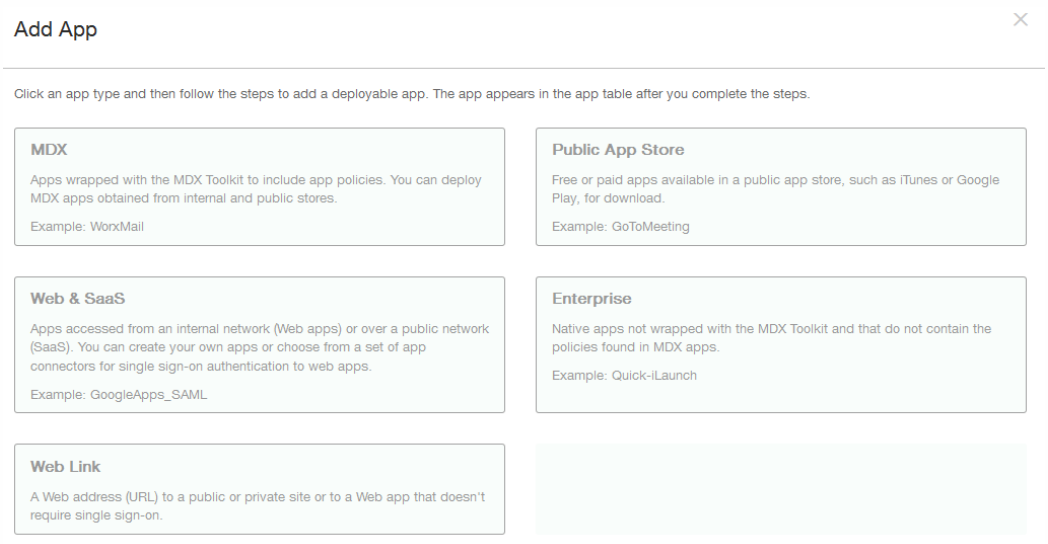
Apr 22, 2016

收到适用于 iOS、Android 或 Windows Phone 设备的打包 MDX 移动应用程序时，可以将应用程序上载到 XenMobile。 上载应用程序后，可以配置应用程序详细信息和策略设置。 有关每种设备平台类型可用的应用程序策略的详细信息，请参阅适用于 iOS、Android 和 Windows Phone 的 MDX 策略概览。 该部分内容还提供了详细的策略说明。

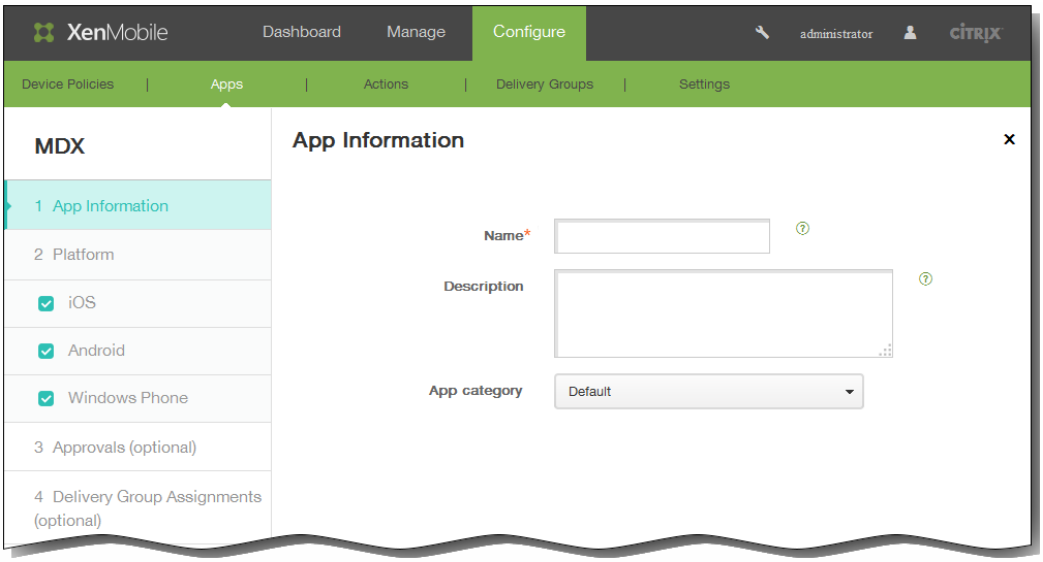
1. 在 XenMobile 控制台中，单击配置 > 应用程序。 此时将显示应用程序页面。
2. 单击添加。



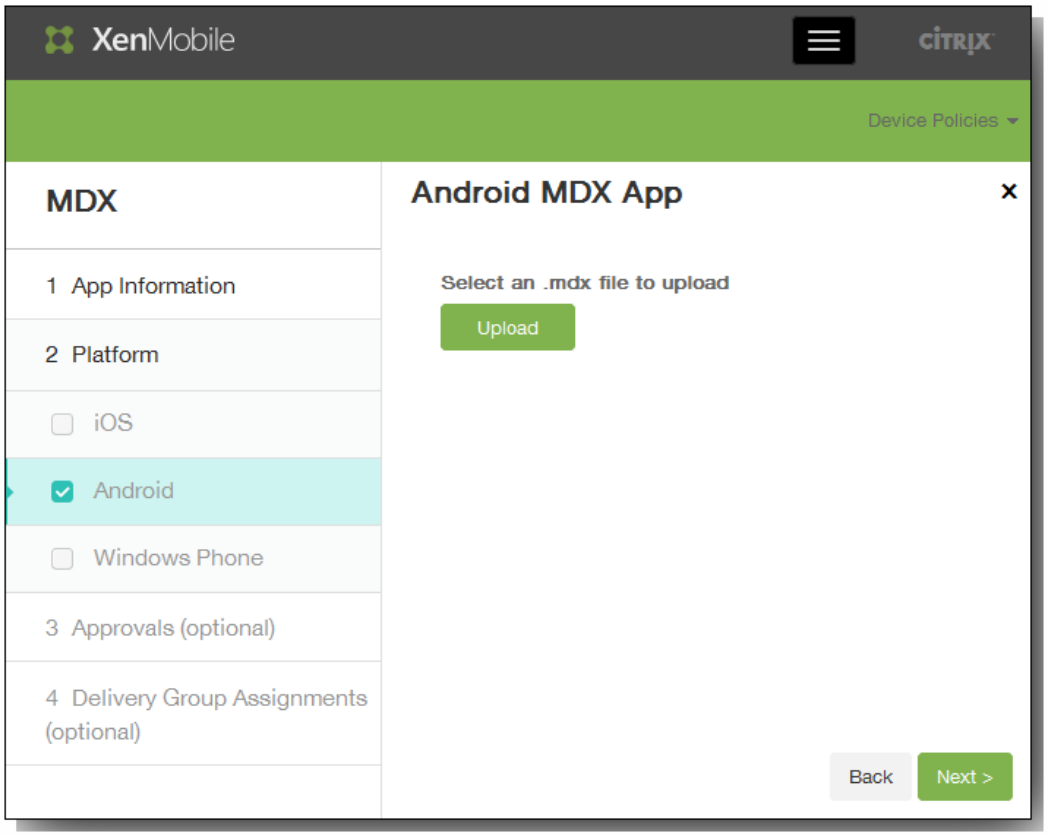
3. 在 Add App（添加应用程序）屏幕上，单击 MDX。



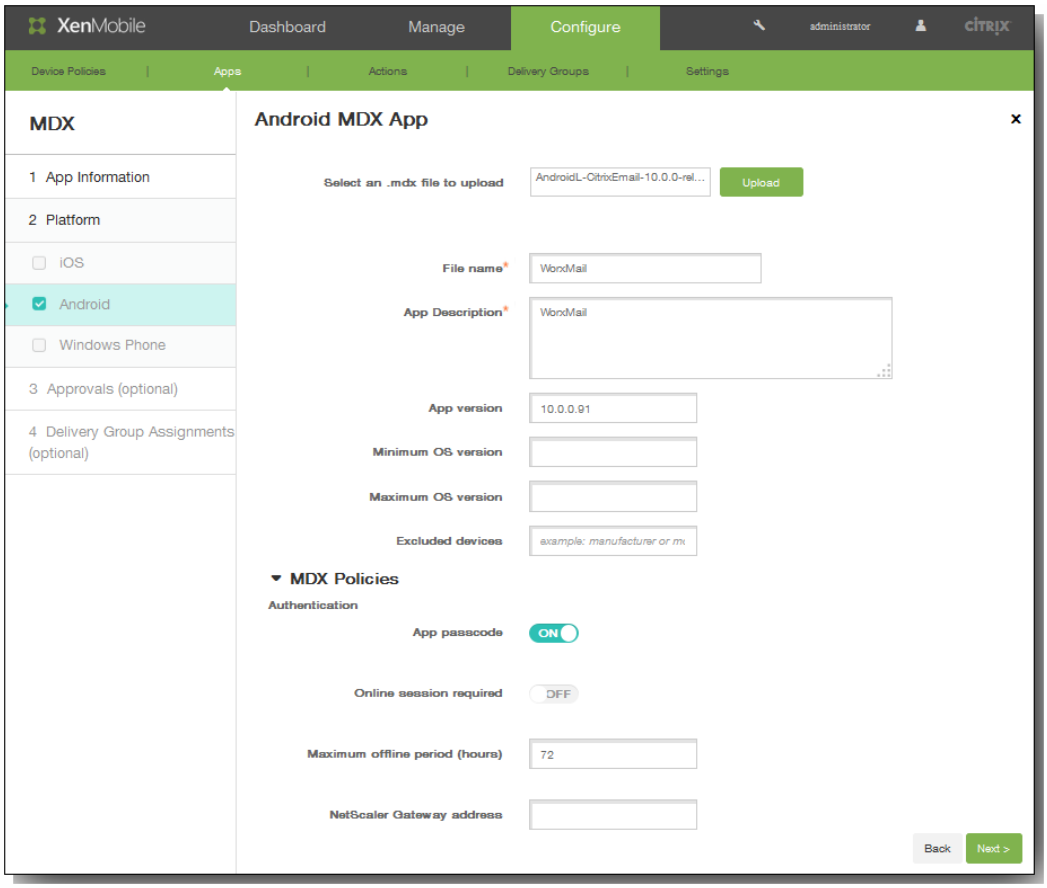
4. 在 App Information（应用程序信息）页面上，输入 Name（名称），然后提供应用程序的可选 Description（说明）。 这些字段供内部使用。 如果要添加用于多个设备的应用程序，请使用屏幕左侧部分的复选框将其选中。



5. 在应用程序类别列表中，单击应用程序类别。 有关详细信息，请参阅添加类别。
6. 单击下一步。
7. 单击上载以选择要上载的 .mdx 文件，然后单击下一步。



此时将显示应用程序详细信息和 MDX 策略字段。

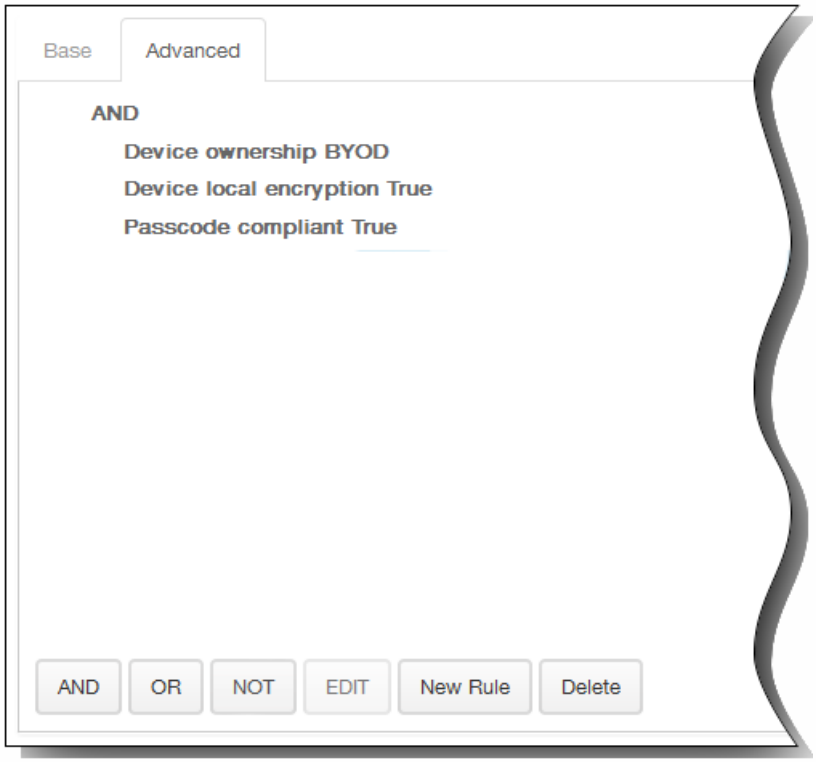


8. 配置以下设置：
   1. 文件名：输入与应用程序关联的文件名。
   2. 应用程序说明：输入应用程序的说明。
   3. 最低操作系统版本：输入为使用应用程序设备可以运行的最低操作系统版本。
   4. 最高操作系统版本：输入为使用应用程序设备必须运行的最新操作系统版本。
   5. 排除的设备：输入不可以运行此应用程序的设备制造商或型号。
9. 在 MDX Policies（MDX 策略）部分，配置 Worx Store 在身份验证、设备安全、网络要求和访问、加密、应用程序交互、应用程序限制及其他方面强制实施的策略设置。
   注意：在控制台中，可以悬停在策略名称上方以查看策略说明。 有关 MDX 应用程序的应用程序策略详细信息，如显示哪些策略适用于哪些平台类型的表格，请参阅适用于 iOS、Android 和 Windows Phone 的 MDX 策略概览。
10. 展开部署规则。 默认情况下将显示基础选项卡。

1. 在此列表中，单击选项以确定部署应用程序的时间。
   1. 可以选择在满足所有条件时部署应用程序，或在满足任意条件时部署应用程序。 默认选项是全部。
   2. 单击新建规则以定义条件。

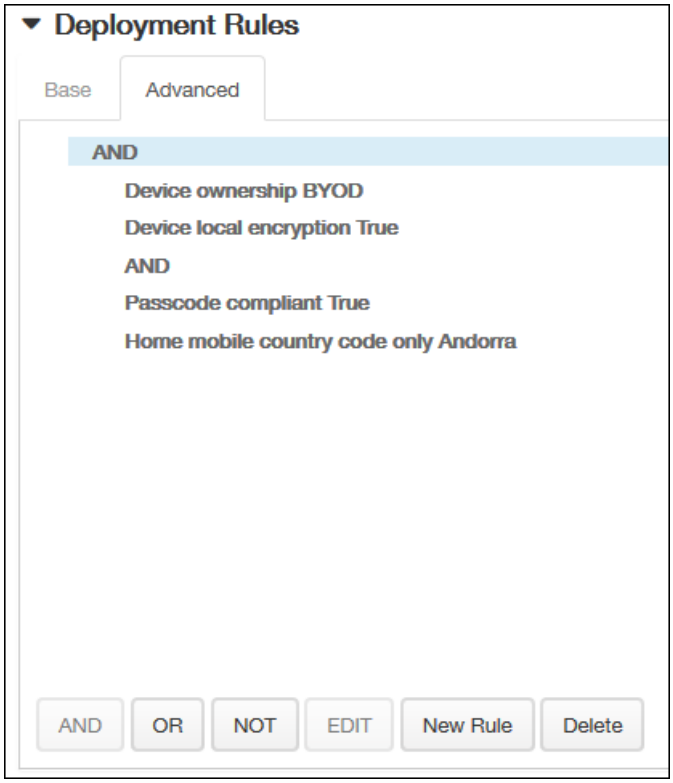
3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
4. 如果要添加更多条件，请再次单击新建规则。 您可以添加任意多项条件。

2. 单击高级选项卡以使用布尔选项组合规则。

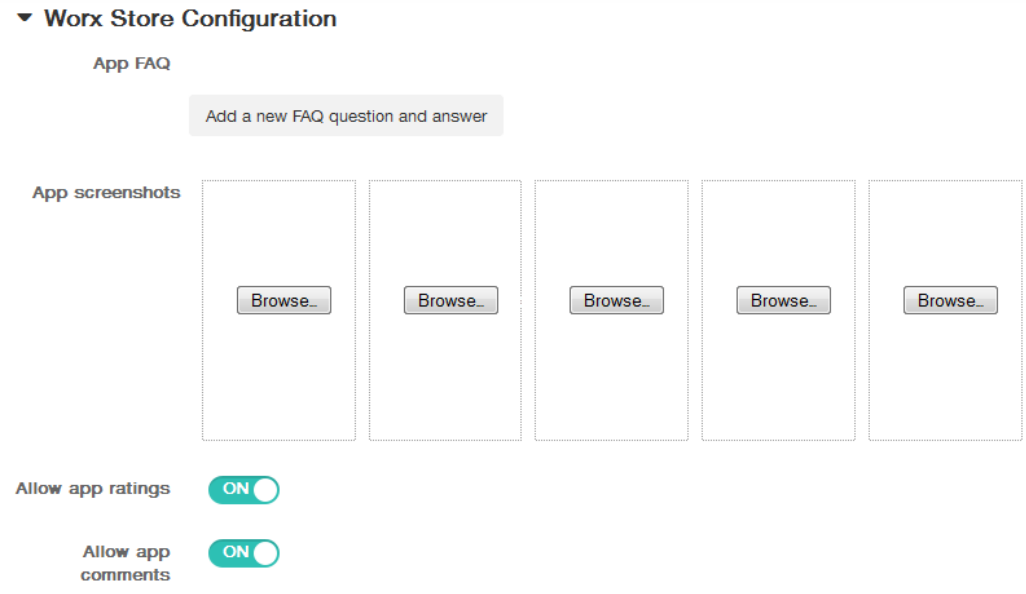


将显示您在基础选项卡上选择的条件。

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，设备必须兼容通行码，并且移动设备国家/地区代码不能仅为安道尔。

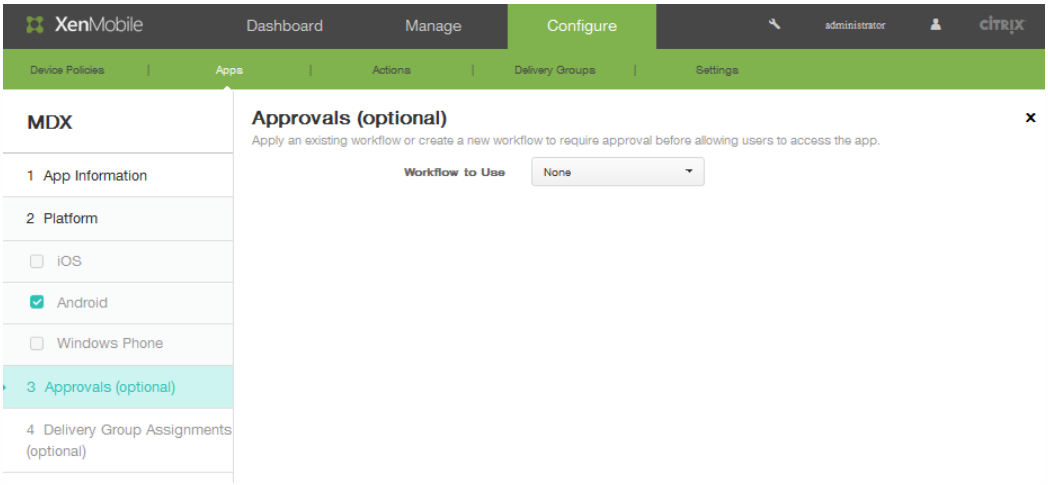


11. 展开 Worx Store Configuration（Worx Store 配置）以添加应用程序的 FAQ，或添加屏幕拍图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形类型必须为 PNG。 不能上载 GIF 或 JPEG 图形。

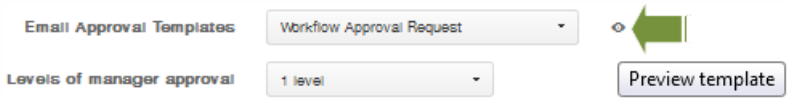


在 Allow app ratings（允许应用程序评级）中，单击 ON（启用）以允许用户对应用程序进行评级。

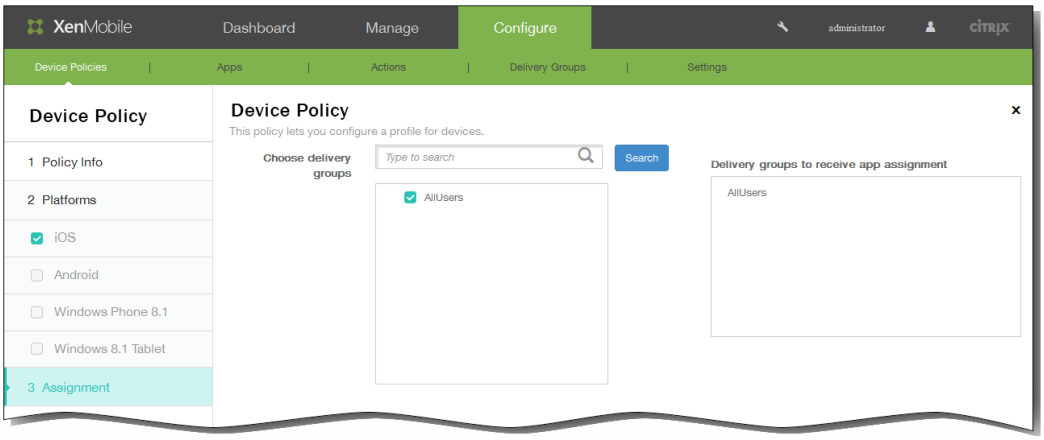
12. 在 Allow app comments（允许应用程序注释）中，单击 ON（启用）以允许用户对选定的应用程序添加注释。
13. 单击下一步。 此时将显示 Approvals（批准）屏幕。



14. 创建新工作流时，XenMobile 控制台将改为显示批准流程的配置选项。 将在下面的步骤中介绍其中的每个字段。 如果需要对创建用户帐户进行审批，请配置这些字段。
    1. 指定工作流的**名称**。
    2. 可以选择输入**说明**。
    3. 在 **Email Approval Templates**（电子邮件批准模板）字段中，单击通知选项。 单击眼睛**图标**以预览所选模板。



    4. 在 **Levels of manager approval**（管理员批准级别）中，单击 None（无）至 3 之间的级别。 .
    5. 在 **Select Active Directory domain**（选择 Active Directory 域）中，单击域。
    6. 在 Find additional required approvers（查找其他必需批准者）中，可以选择输入所需的其他批准者，然后单击 Search（搜索）。
15. 单击下一步。
16. 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。

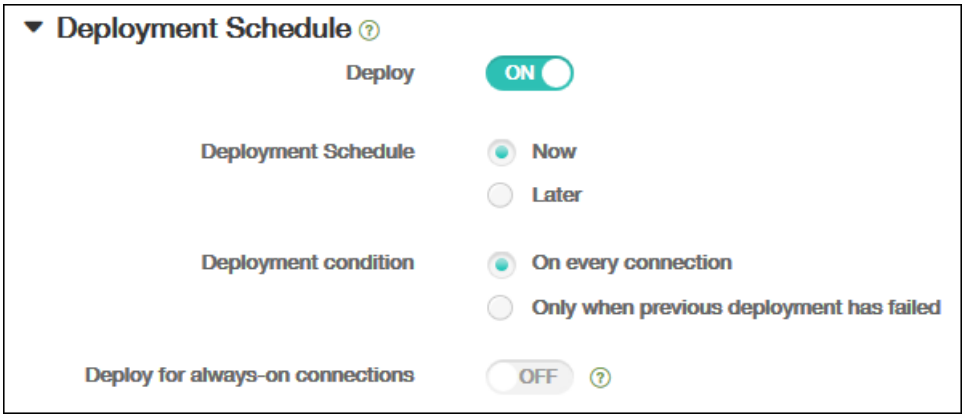


17. 展开部署计划，然后配置以下设置：
    1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。 如果选择关，无需配置其他选项。

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。



18. 单击保存。 XenMobile 控制台将应用应用程序信息。

在 XenMobile 中创建应用程序类别

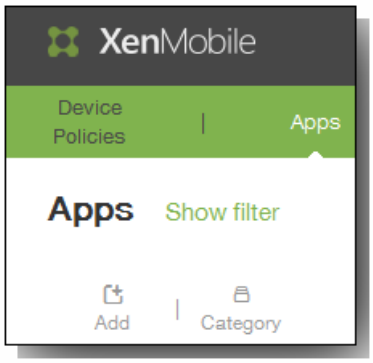
Oct 22, 2015

用户登录 Worx Home 时，会收到您已在 XenMobile 中添加并配置的应用程序、Web 链接和应用商店的列表。您可以使用应用程序类别实现只允许用户访问您希望其访问的应用程序、应用商店或 Web 链接的目的。例如，您可以创建“财务”类别，然后向其中添加仅与财务相关的应用程序。您也可以配置“销售”类别，并向其分配销售应用程序。此外，还也可以为应用程序商店配置 Apple 类别。

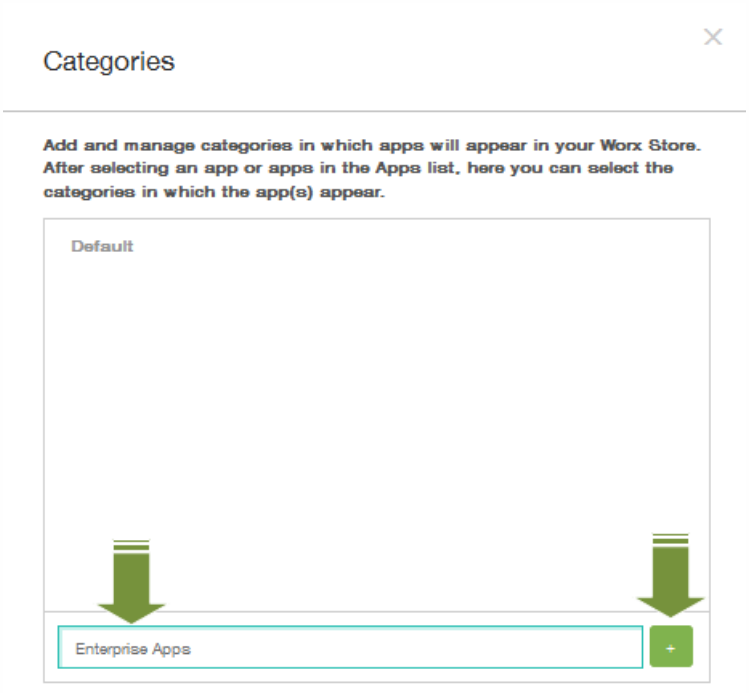
在 XenMobile 控制台中的应用程序页面上配置类别。然后，配置或编辑应用程序、Web 链接或应用商店时，将应用程序添加到您所配置的其中一个类别中。

添加类别

1. 在 XenMobile 控制台中，单击配置 > 应用程序。 此时将显示应用程序页面。
2. 在应用程序页面上，单击类别。

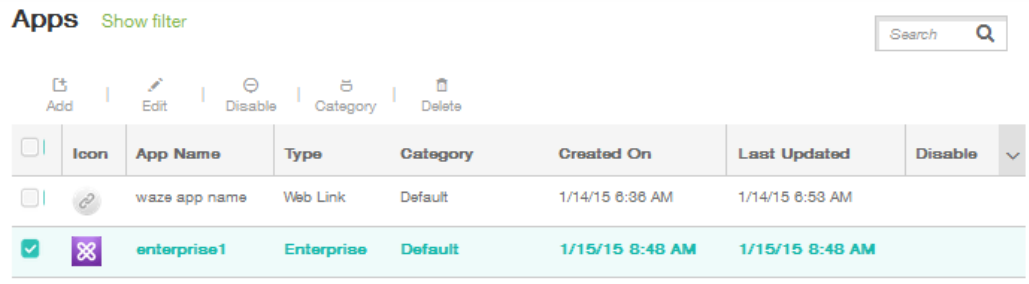


3. 在类别对话框中，输入要添加的类别的名称，然后单击加号 (+)。 例如，输入*企业应用程序*，然后单击加号 (+)。

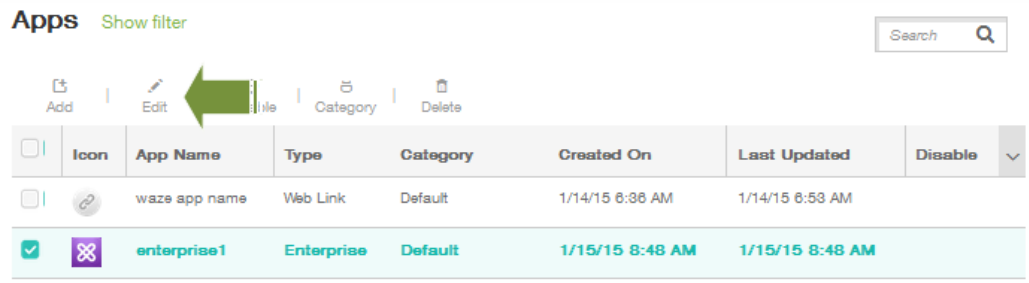


此时已添加新创建的类别并显示在同一类别对话框。如果当前未配置任何类别，将仅显示**默认**类别。

4. 如果要添加其他新类别，请重复步骤 3，然后关闭类别对话框。
5. 在应用程序页面上，可以将现有应用程序分类到新类别中。 选择要分类的应用程序。

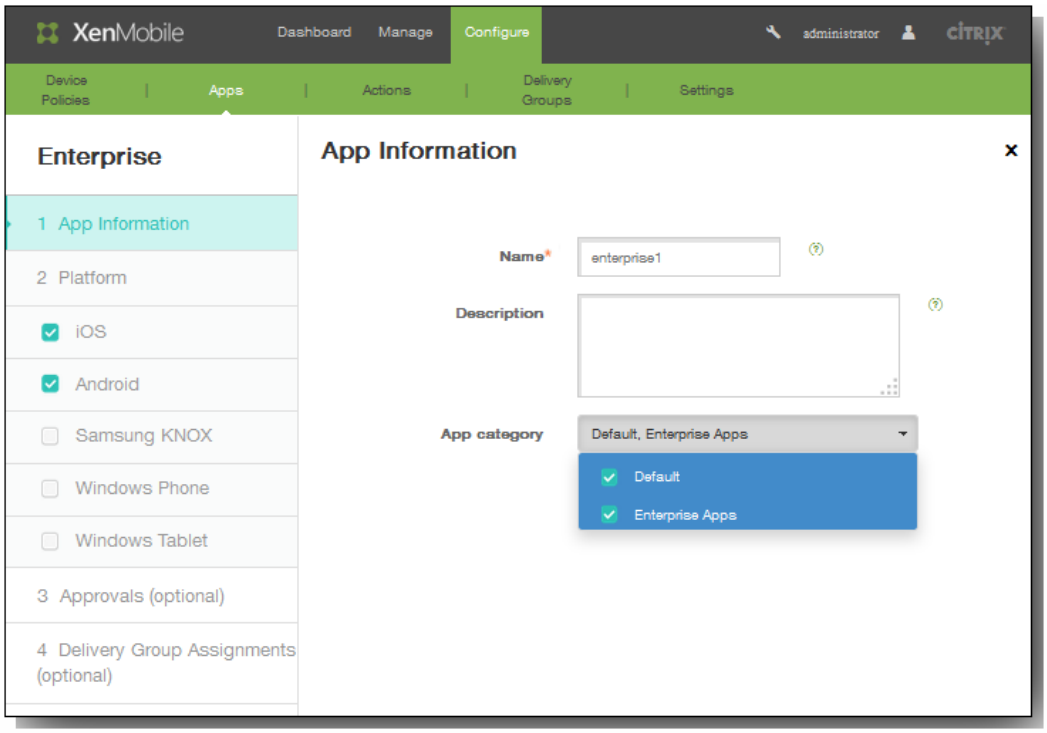


6. 单击编辑以分类应用程序。

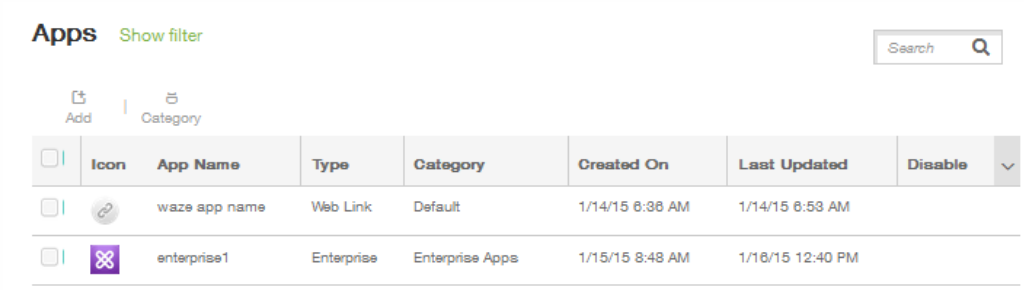


此时将显示应用程序信息页面。

7. 在应用程序类别列表中，通过选中类别复选框应用类别。



8. 单击下一步完成应用程序配置的剩余页面。
9. 单击最后一个页面上的保存以应用类别。 新创建的类别将应用到应用程序并显示在应用程序表格中。

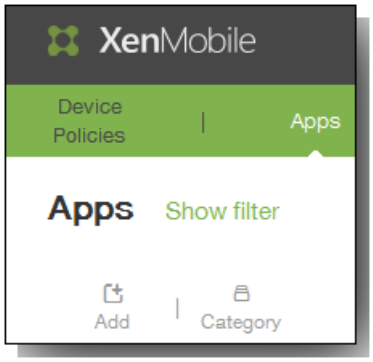


向 XenMobile 中添加公共应用商店应用程序

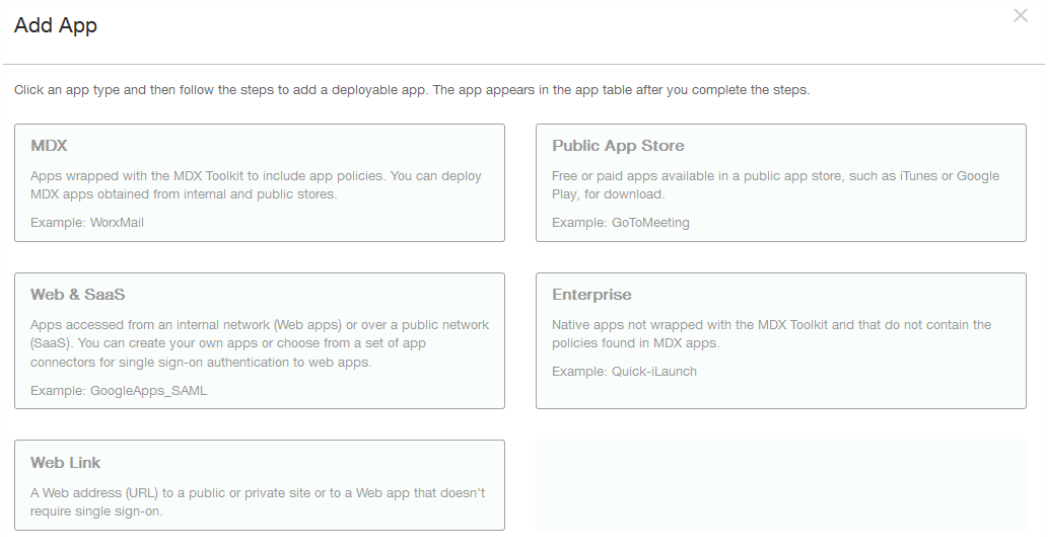
Oct 22, 2015

可以向 XenMobile 中添加公共应用商店（如 iTunes 或 GooglePlay）中提供的免费或付费应用程序。例如，GoToMeeting。

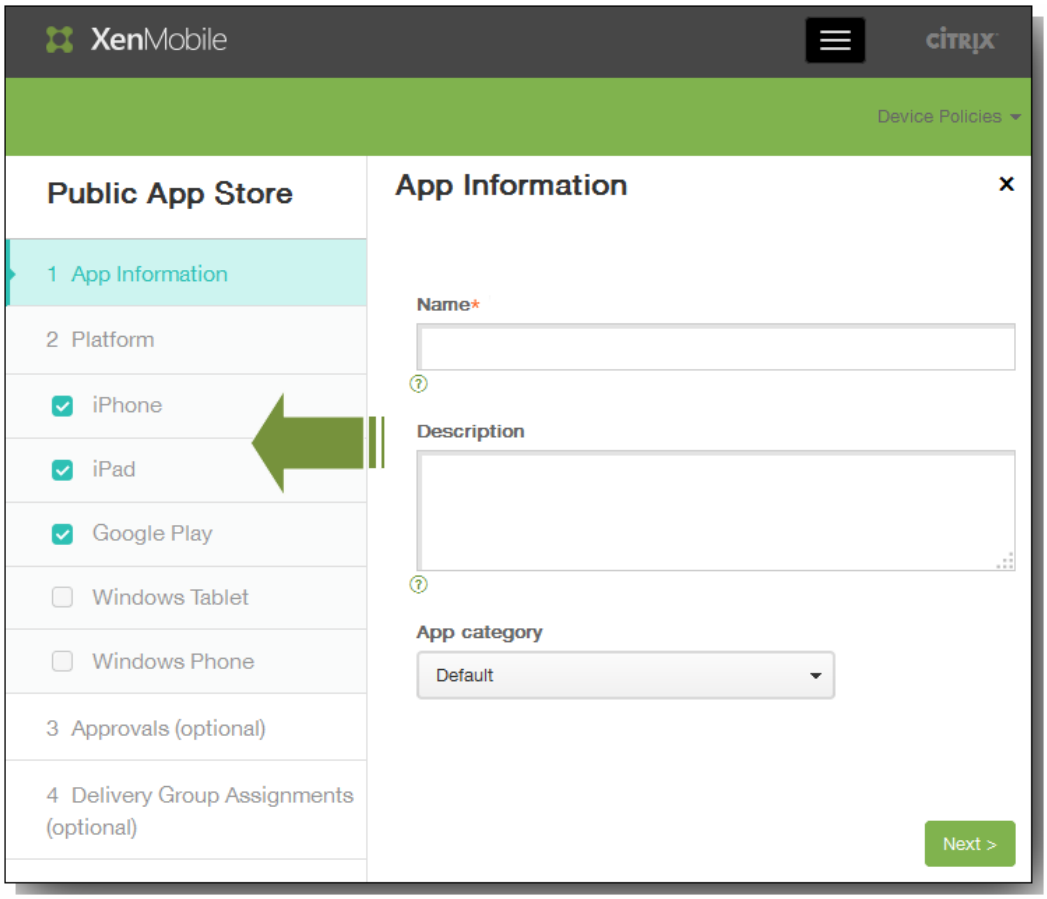
1. 在 XenMobile 控制台中，单击配置 > 应用程序。此时将显示应用程序屏幕。



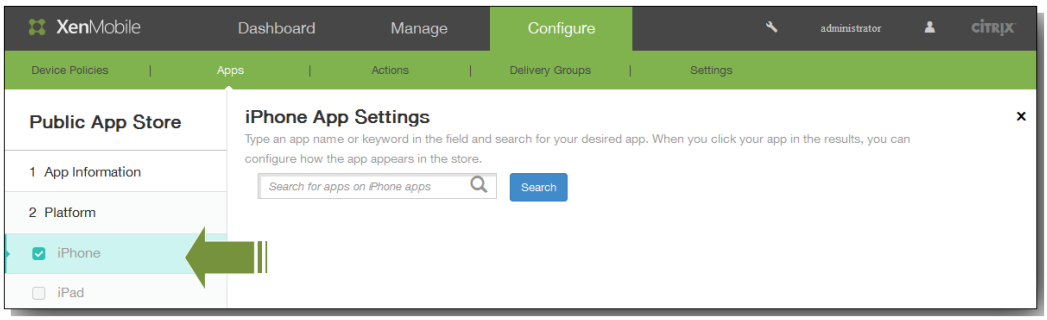
2. 单击添加。
3. 在添加应用程序屏幕中，单击公共应用商店。



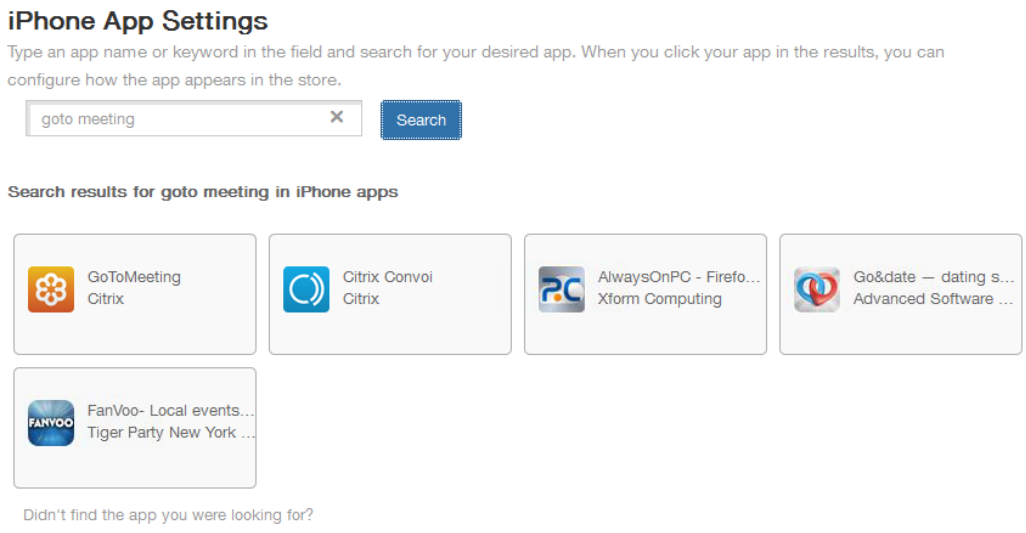
4. 在应用程序信息页面上，输入名称，然后提供应用程序的说明。 这些字段供内部使用。 如果要添加适用于多个设备（如 iPhone、iPad 和 GooglePlay）的应用程序，请使用屏幕左侧部分的复选框将其选中。



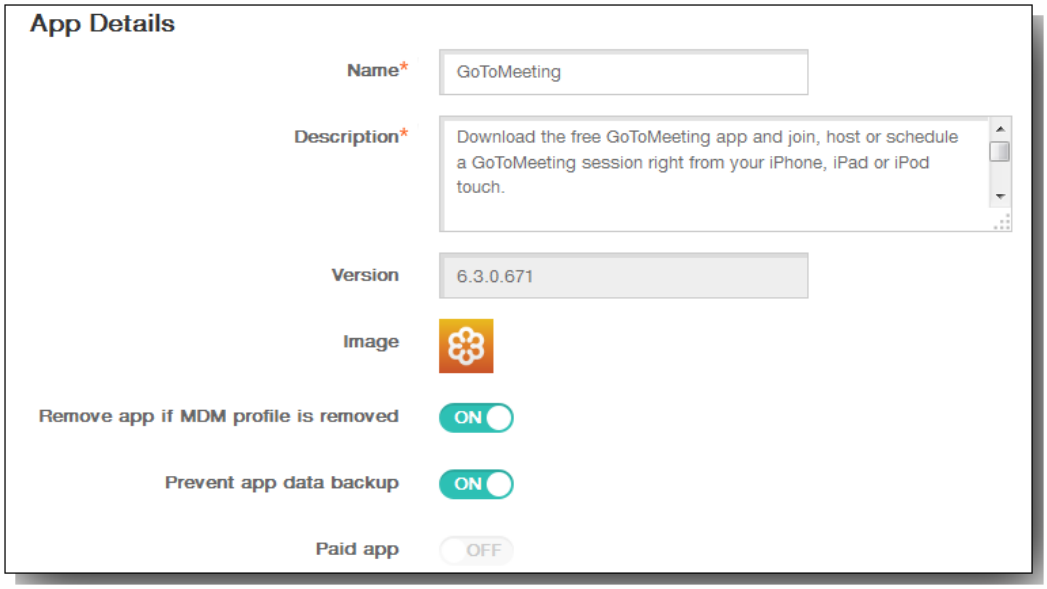
5. 在应用程序类别列表中，单击应用程序类别。
6. 单击下一步。
7. 在用于平台类型的 Platform（平台）屏幕上，在搜索字段中，键入应用程序名称或关键字以查找要添加的应用程序。例如，如果选择添加 iPhone 应用程序，XenMobile 控制台会搜索与 iPhone 设备相关的应用程序。如果选择添加适用于多个平台的应用程序，系统会显示每个平台的结果。



下图中显示了匹配搜索条件（如 GoToMeeting）的应用程序。



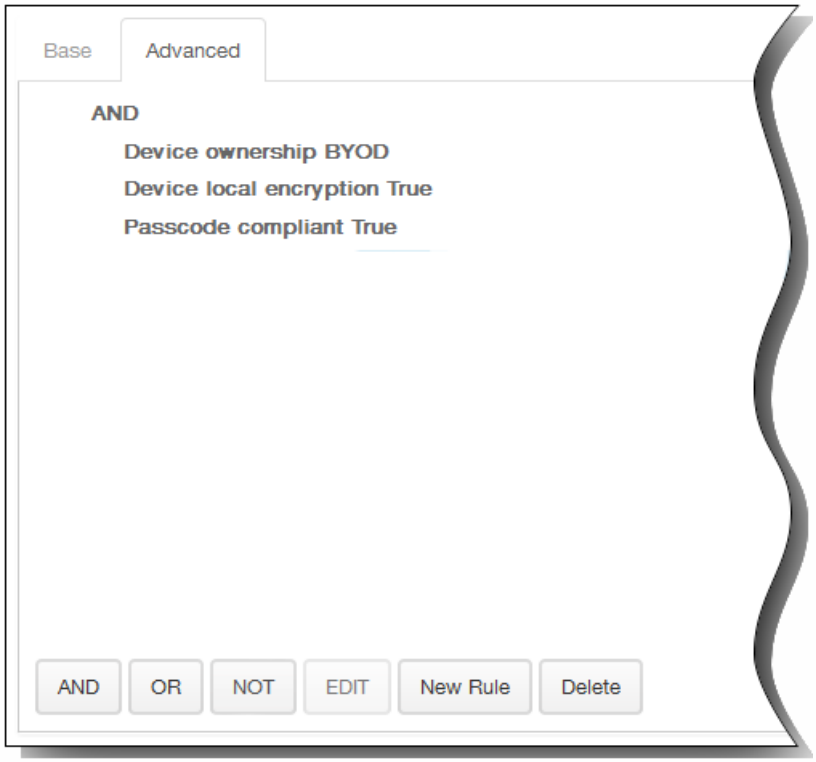
8. 单击结果中的应用程序以配置此应用程序在应用商店中的显示方式。 在 App Details（应用程序详细信息）屏幕上，字段已经预填充了与所选应用程序相关的信息（包括名称、说明、版本号和关联的图像）。 如有需要，可更改应用程序的名称和说明。



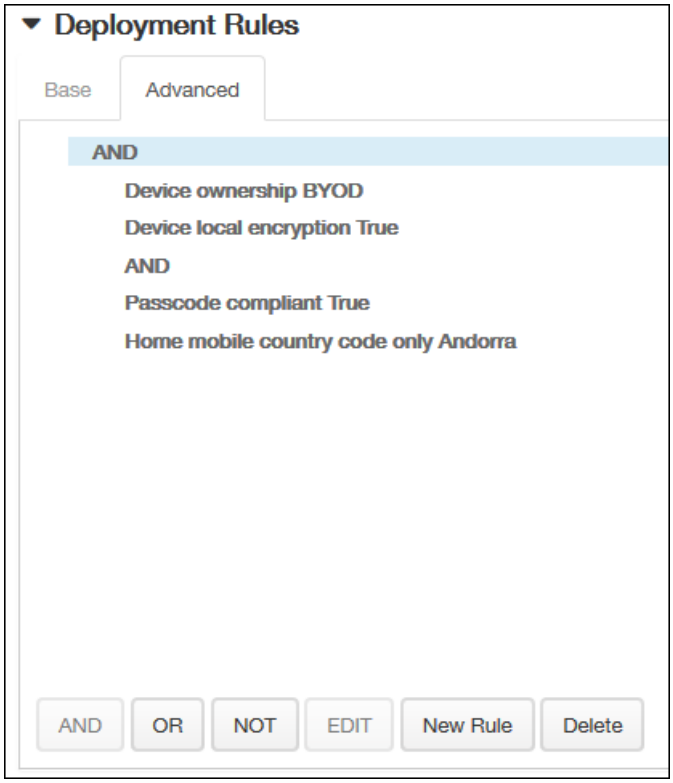
1. 如果要在删除 MDM 配置文件时删除应用程序，请在 Remove app if MDM profile is removed（删除 MDM 配置文件时删除应用程序）中，单击 ON（启用）。 默认情况下，此选项设置为 ON（启用）。
2. 如果要阻止应用程序备份数据，请在 Prevent app data backup（阻止应用程序数据备份）中，单击 ON（启用）。 默认情况下，此选项设置为 ON（启用）。
3. 在 **Paid app**（付费应用程序）中，字段已经预配置，并且无法更改。

9. 展开部署规则。默认情况下将显示基础选项卡。

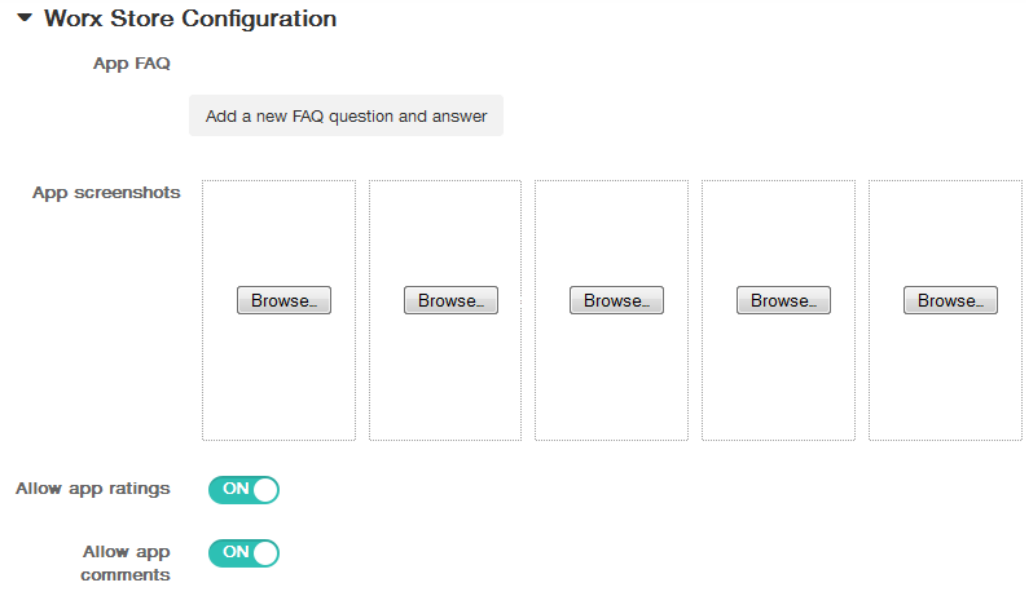
1. 在此列表中，单击选项以确定部署应用程序的时间。
   1. 可以选择在满足所有条件时部署应用程序，或在满足任意条件时部署应用程序。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。



   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，设备必须兼容通行码，并且移动设备国家/地区代码不能仅为安道尔。

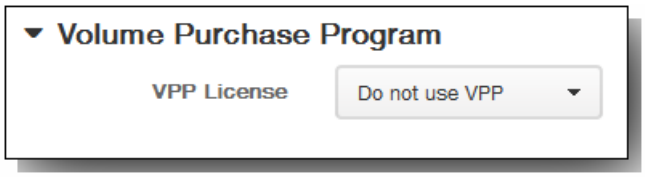


10. 展开 Worx Store Configuration（Worx Store 配置）以添加应用程序的 FAQ，或添加屏幕拍图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形类型必须为 PNG。 不能上载 GIF 或 JPEG 图形。

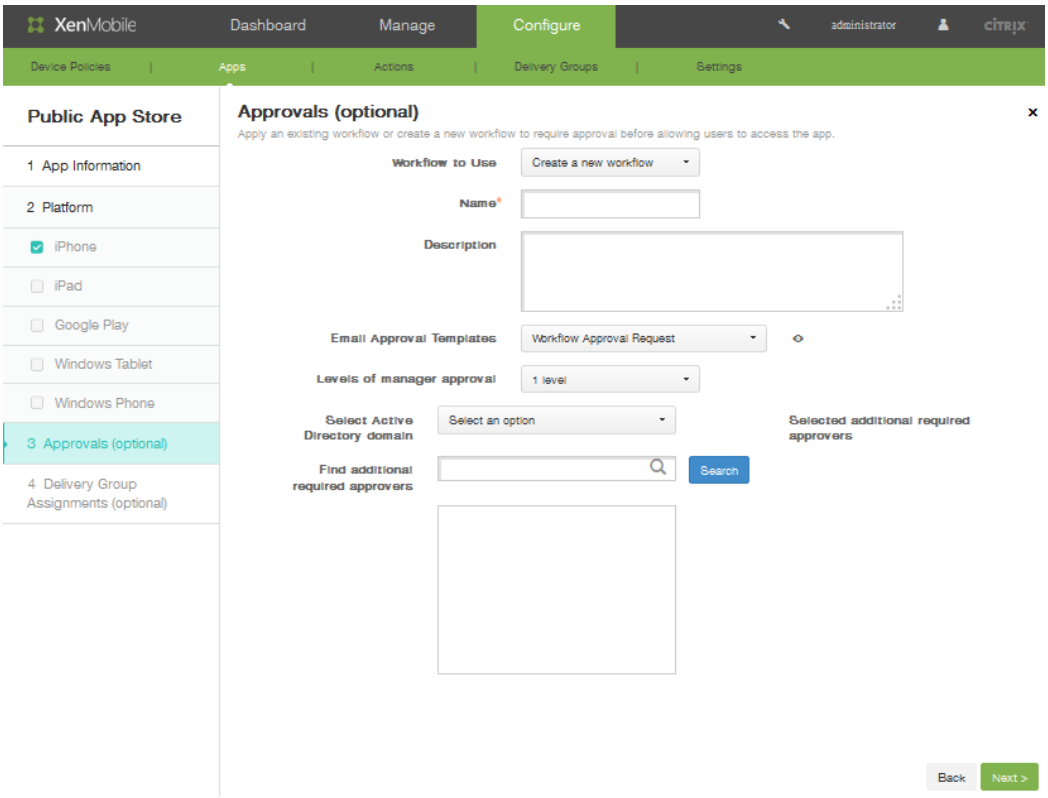


在 Allow app ratings（允许应用程序评级）中，单击 ON（启用）以允许用户对应用程序进行评级。

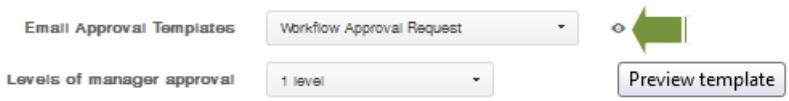
11. 在 Allow app comments（允许应用程序注释）中，单击 ON（启用）以允许用户对选定的应用程序添加注释。
12. 如果要允许 XenMobile 为应用程序应用 VPP 许可证，展开 Volume Purchase Program，然后在 VPP license list（VPP 许可证列表）中，单击 Upload a VPP license file（上载 VPP 许可证文件）。



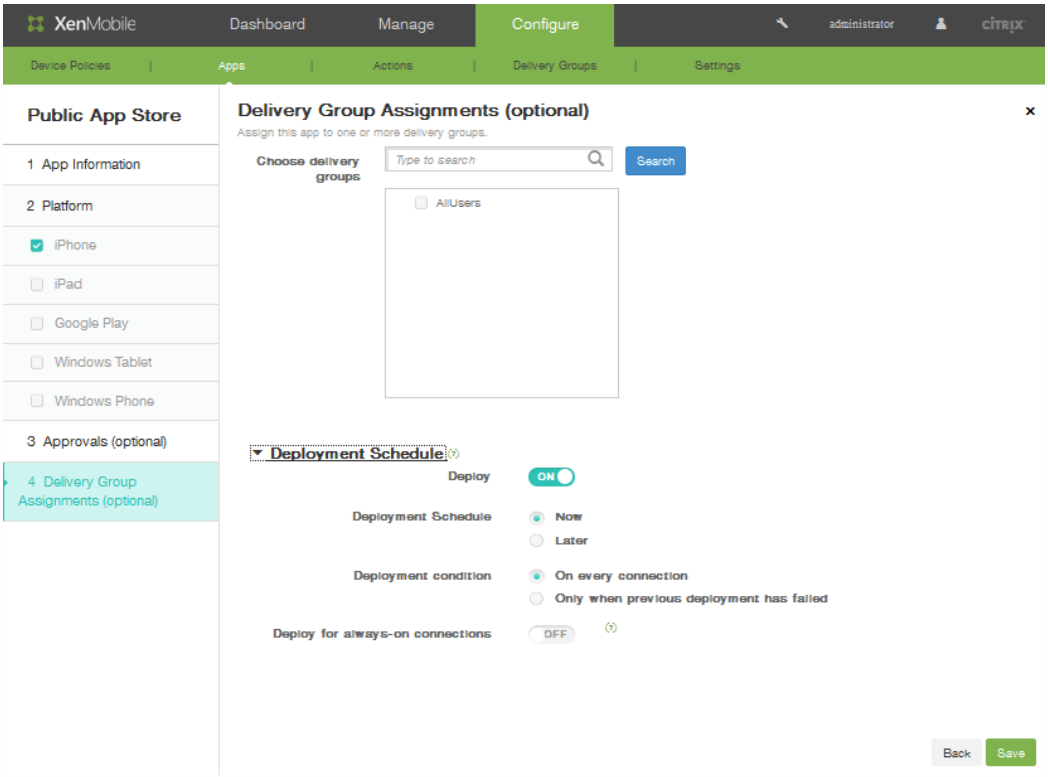
13. 单击 Next（下一步），然后为要添加公共应用程序的每个平台类型重复执行步骤 7 至 16。
14. 在**审批**页面上的**要使用的工作流**列表中，可以选择单击某个工作流或单击**创建新工作流**。



15. 创建新工作流时，XenMobile 控制台将改为显示批准流程的配置选项。 将在下面的步骤中介绍其中的每个字段。
    1. 指定工作流的**名称**。
    2. 可以选择输入**说明**。
    3. 在 **Email Approval Templates**（电子邮件批准模板）字段中，单击通知选项。单击眼睛**图标**以预览所选模板。



    4. 在**经理审批级别**中，单击无至3之间的某个级别。。
    5. 在 **Select Active Directory domain**（选择 Active Directory 域）中，单击域。
    6. 在 Find additional required approvers（查找其他必需批准者）中，可以选择输入所需的其他批准者，然后单击 Search（搜索）。
16. 单击**下一步**。
17. 在 **Delivery Groups Assignment**（交付组分配）页面上，可以选择将应用程序分配给一个或多个交付组。



18. 在 Choose delivery groups（选择交付组）中，搜索一个或多个交付组。选中 **All Users**（所有用户）复选框可将应用程序分配给每个 XenMobile 用户。
19. 展开部署计划可进一步精简交付组。
    1. Deploy（部署）：单击 ON（启用）以启用部署计划。
    2. 部署计划：单击立即或稍后以设置部署 计划。
    3. 部署条件：单击以选择是在每次连接时部署应用程序，还是仅在上一个部署失败时再部署应用程序。
    4. 在为始终启用的连接部署中，单击开以在设置始终启用的连接策略时部署。
       注意：仅当同时在 XenMobile 控制台的“设置”区域的“服务器属性”部分中配置了全局后台部署密钥时此选项才适用。始终启用计划策略不适用于 iOS 设备
20. 单击保存。XenMobile 控制台将应用应用程序信息。

向 XenMobile 添加 Web 和 SaaS 应用程序

Oct 22, 2015

使用 XenMobile 控制台，可以向用户提供对移动应用程序、企业应用程序、Web 应用程序和 SaaS 应用程序的单点登录 (SSO) 功能。可以通过使用应用程序连接器模板，为应用程序启用 SSO。有关 XenMobile 中可用的连接器类型的列表，请参阅应用程序连接器类型列表。

您也可以在 XenMobile 中构建自己的连接器。

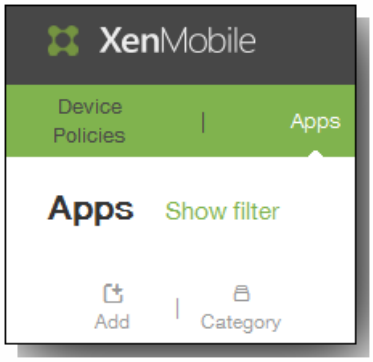
通过提供以下参数配置连接器：

- 不同的名称（可选）。使用控制台中显示的任意应用程序连接器。不再支持 Box 连接器。
- 应用程序的说明。
- 使用完全限定的域名 (FQDN) 提供的 Web 地址。例如，如果要将 LinkedIn 添加到应用程序列表中，应访问 http://www.linkedin.com，然后单击 Sign in（登录）。显示登录页面时，使用 Web 地址 https://www.linkedin.com 配置应用程序。
- 应用程序的位置，在 Internet 上或您的内部网络上。
- SSO 的凭据。用户可以使用应用程序凭据。
- 应用程序的类别。利用类别可以在 Worx Home 中对应用程序分类。
- 在 XenMobile 中配置的每个应用程序的应用程序策略。
- 所有应用程序的工作流审批设置，包括指定可以审批用户帐户的人员。
- 要分配应用程序的用户交付组。

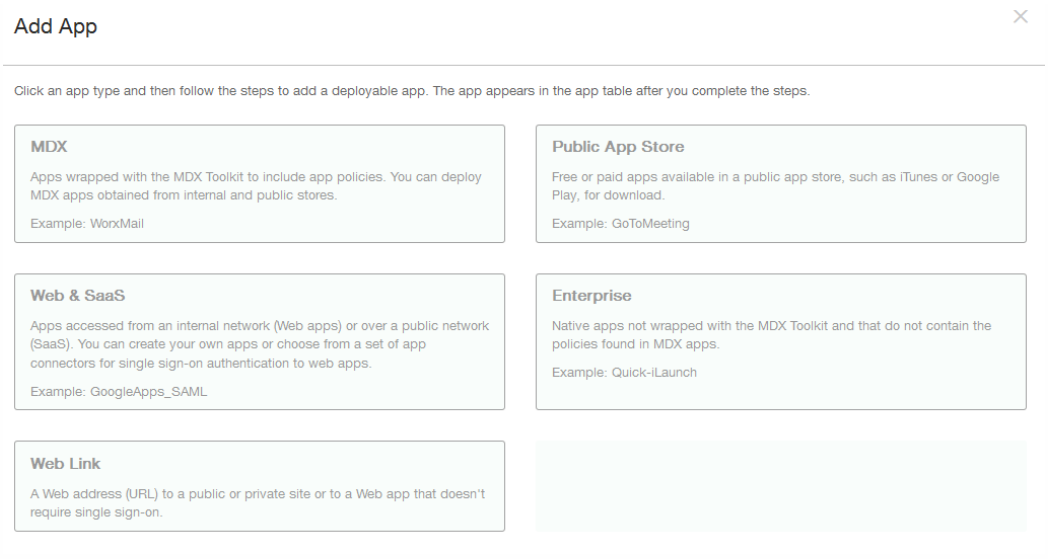
如果应用程序仅可进行 SSO，则在配置完前面的设置后，保存这些设置，应用程序将显示在 XenMobile 控制台的应用程序选项卡中。

在 XenMobile 中添加应用程序连接器

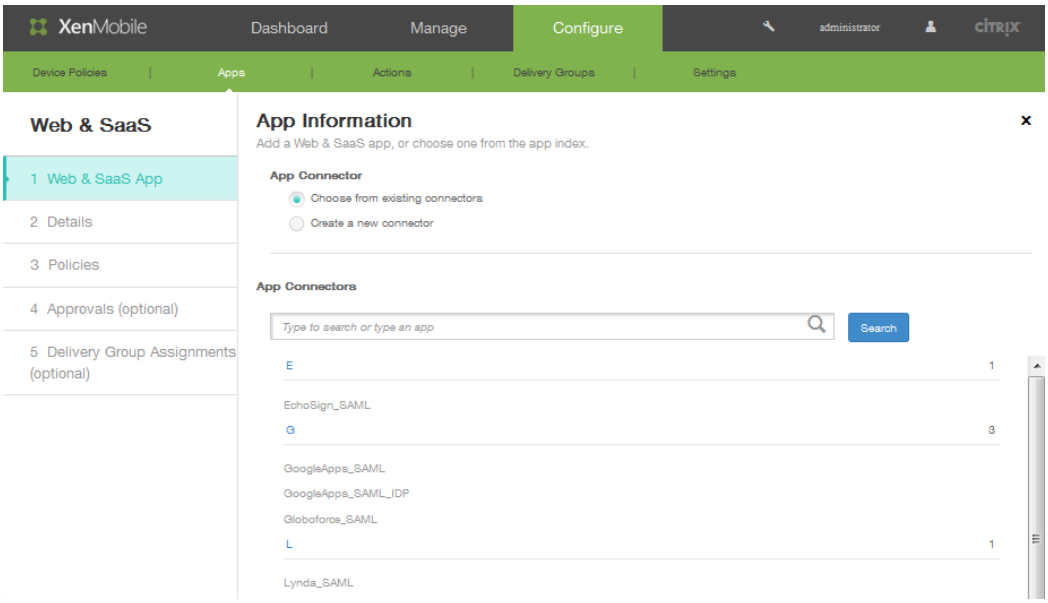
1. 在 XenMobile Web 控制台中，单击配置 > 应用程序。 将打开应用程序页面。
2. 在应用程序页面上，单击**添加**。



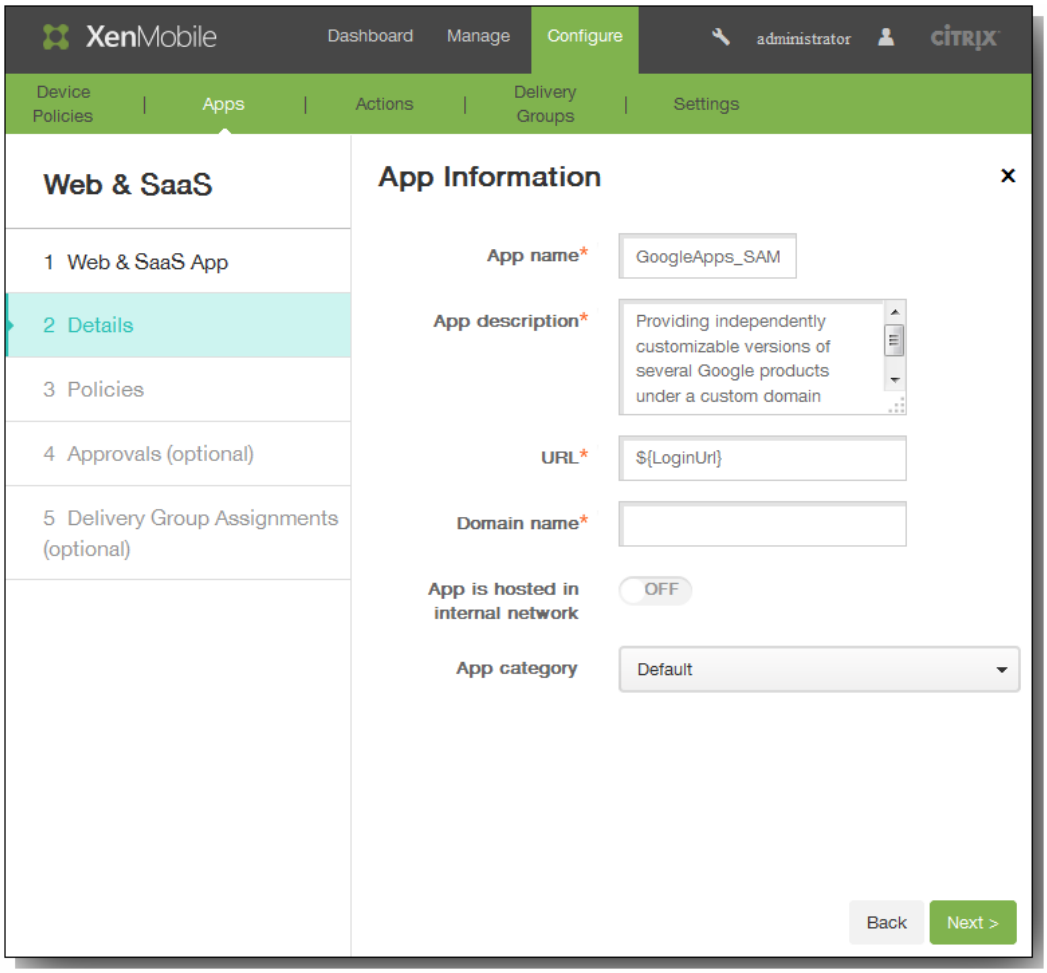
3. 在**添加应用程序**页面上，单击 **Web 和 SaaS**。



4. 在应用程序信息页面上，单击从现有连接器中选择或创建新连接器。

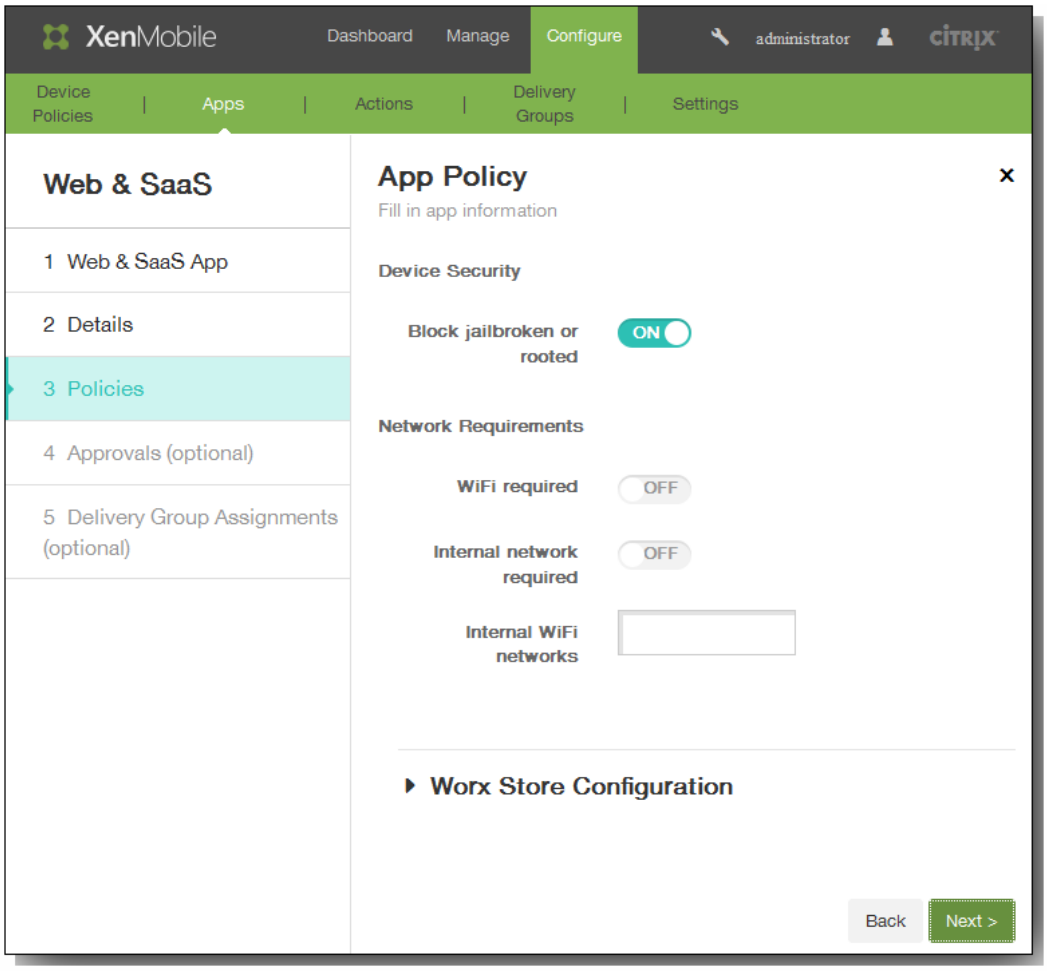


5. 如果单击列表中的某个应用程序，将显示详细信息页面。 应用程序名称、说明和 URL 字段已经预填充。

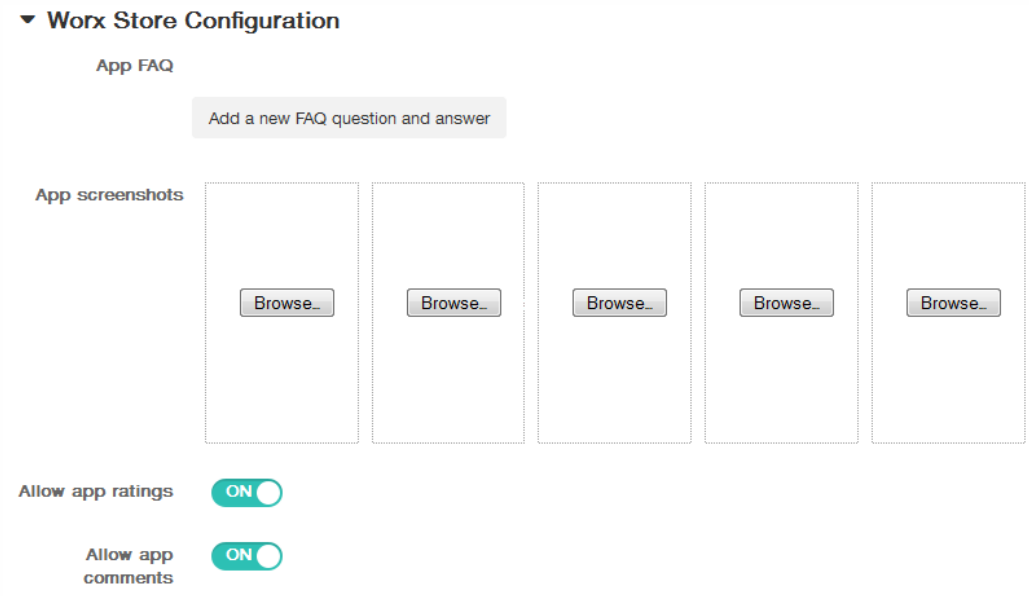


1. 如果适用，在 URL 中输入应用程序的 Web 地址或保留默认地址。
2. 如果应用程序正在内部网络中的服务器上运行，请在应用程序托管在内部网络中，单击开。 如果用户从远程位置连接到内部应用程序，则必须通过 NetScaler Gateway 进行连接。 将此选项设置为开将向应用程序添加 VPN 关键字，并允许用户通过 NetScaler Gateway 连接。
3. 在应用程序类别列表中，单击某个类别。
4. 在启用用户管理功能以进行置备中，单击开。 如果要使用 Globalforce_SAML 连接器，必须启用启用用户管理功能以进行置备以确保无缝 SSO 集成。

6. 单击下一步。 此时将显示策略页面。

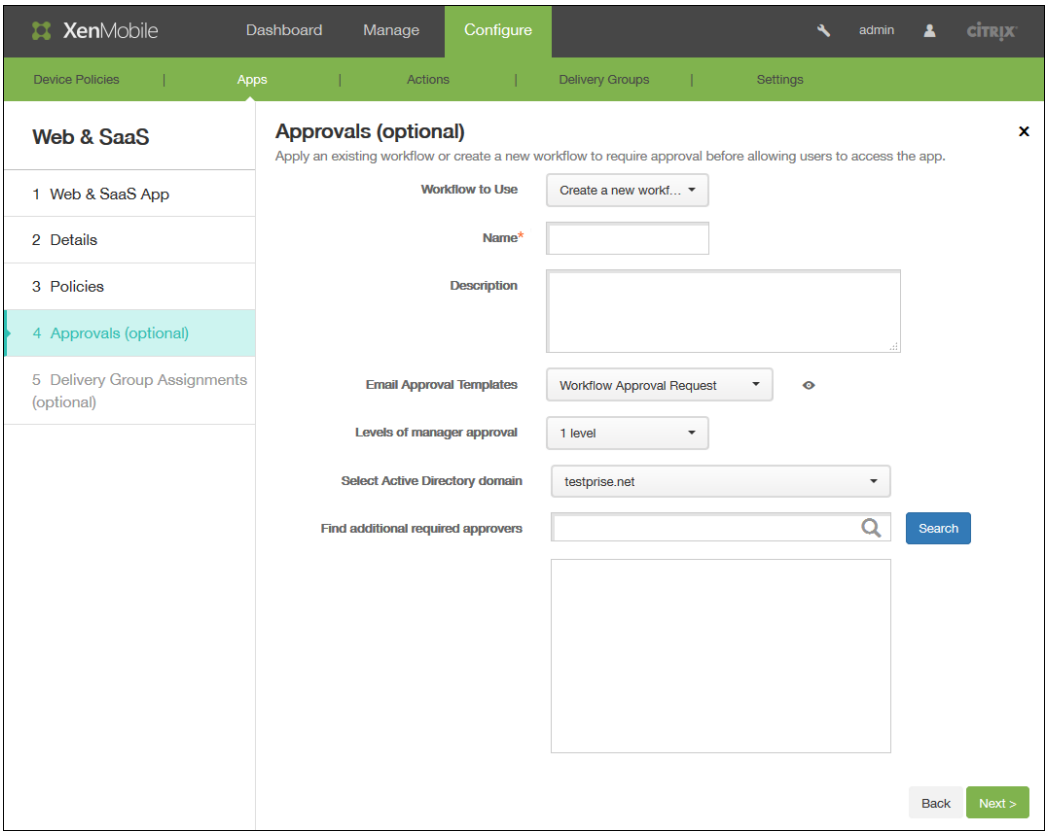


7. 在设备安全性中的阻止越狱或获得 Root 权限中，单击开。
8. 在网络要求中，配置以下设置：
   1. 在需要连接 WiFi 中，单击开，然后指定内部 WiFi 网络。
   2. 如果运行应用程序需要使用内部网络，请在需要使用内部网络中，单击开。
9. 展开 Worx Store 配置以添加应用程序的 FAQ，或添加屏幕拍图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形类型必须为 PNG。 不能上载 GIF 或 JPEG 图形。

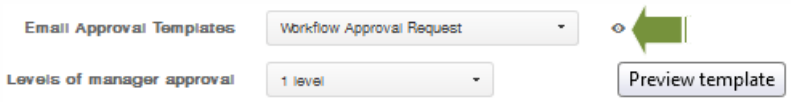


在允许对应用程序评分中，单击开以允许用户对应用程序进行评分。

10. 在允许评价应用程序中，单击开以允许用户评价选定的应用程序。
11. 单击下一步。
12. 在审批页面上的要使用的工作流列表中，可以选择单击某个工作流或单击创建新工作流。

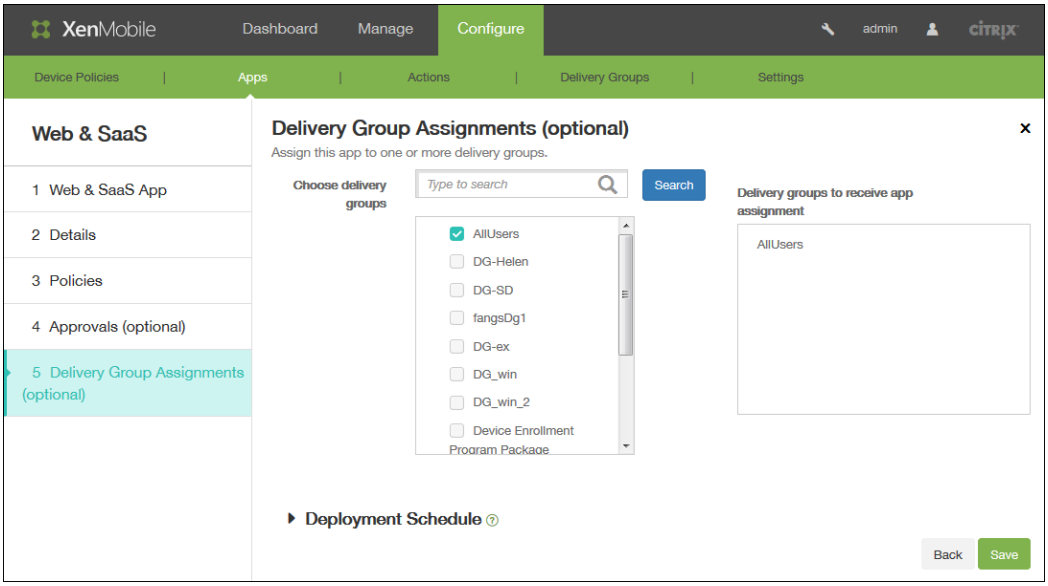


13. 创建新工作流时，XenMobile 控制台将改为显示批准流程的配置选项。 将在下面的步骤中介绍其中的每个字段。 如果需要对创建用户帐户进行审批，请配置这些字段。
    1. 指定工作流的**名称**。
    2. 可以选择输入**说明**。
    3. 在**电子邮件审批模板**字段中，单击通知选项。 单击眼睛**图标**以预览所选模板。



    4. 在**经理审批级别**中，单击无至 3 之间的某个级别。
    5. 在**选择 Active Directory 域**中，单击域。
    6. 在查找所需的其他审批者中，可以选择输入所需的其他审批者，然后单击搜索。
14. 单击下一步。
15. （可选）在**交付组分配**页面上的选择交付组旁边，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。

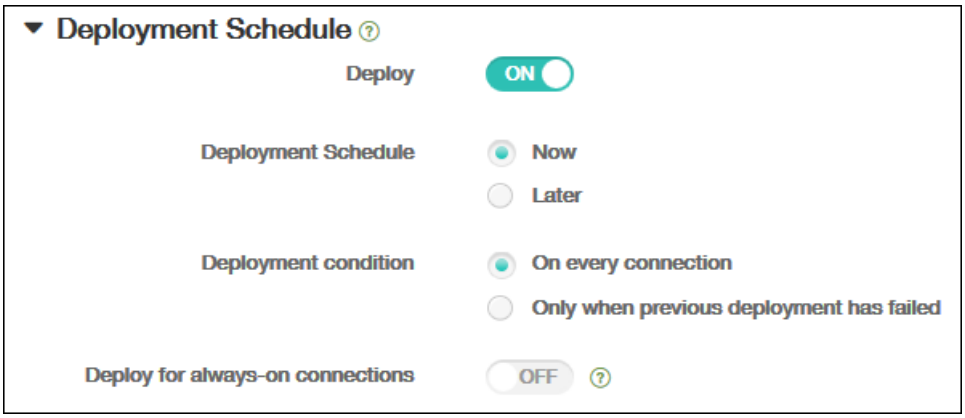
    选择的组显示在右侧用于接收应用程序分配的交付组列表中。



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**。

应用程序连接器类型列表

Oct 22, 2015

下表列出了适用于 XenMobile 的连接器及连接器类型。表中还指出各连接器是否支持用户帐户管理。支持用户帐户管理时，您可以自动或通过工作流程创建新的帐户。

连接器名称	SSO SAML	支持用户帐户管理
EchoSign_SAML	是	是
Globoforce_SAML		注意：使用此连接器时，必须启用用户管理功能以进行置备以确保无缝 SSO 集成。
GoogleApps_SAML	是	是
GoogleApps_SAML_IDP	是	是
Lynda_SAML	是	是
Office365_SAML	是	是
Salesforce_SAML	是	是
Salesforce_SAML_SP	是	是
SandBox_SAML	是	
SuccessFactors_SAML	是	
ShareFile_SAML	是	
ShareFile_SAML_SP	是	
WebEx_SAML_SP	是	是

向 XenMobile 中添加企业应用程序

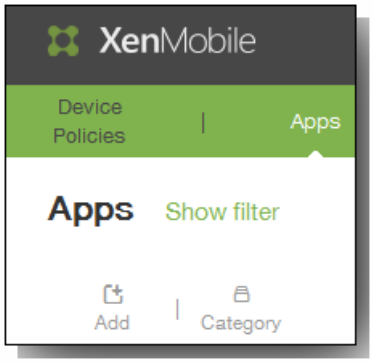
Nov 20, 2015

XenMobile 中的企业应用程序代表未通过 MDX Toolkit 打包的本机应用程序，并且不包含与 MDX 应用程序关联的策略。可以在 XenMobile 控制台中的应用程序选项卡上上载企业应用程序。企业应用程序支持以下平台（和相应的文件类型）：

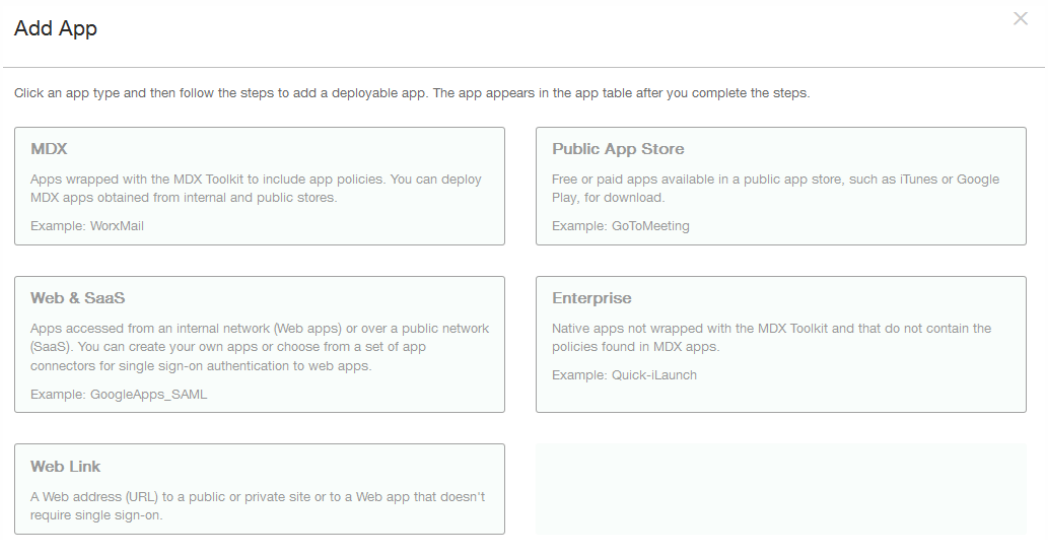
- iOS（.ipa 文件）
- Android（.apk 文件）
- Samsung KNOX（.apk 文件）
- Android for Work（.apk 文件）
- Windows Phone（.xap 或 .appx 文件）
- Windows Tablet（.appx 文件）

创建企业应用程序

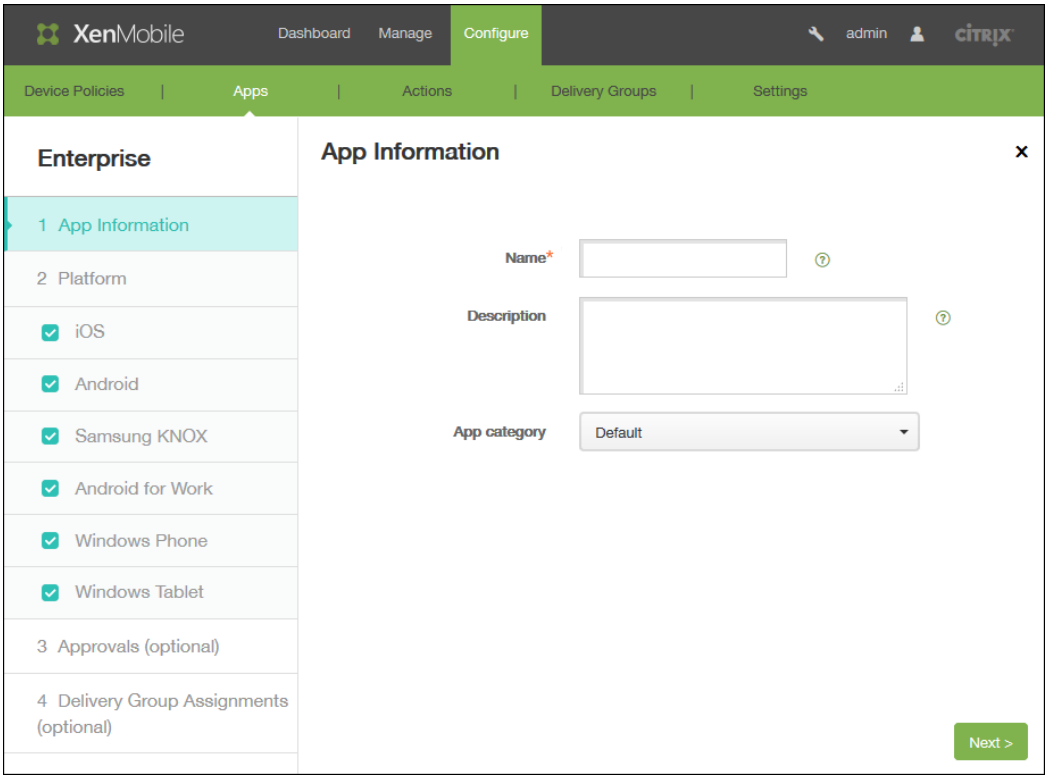
1. 在 XenMobile 控制台中，单击配置 > 应用程序。
2. 在“应用程序”页面上，单击**添加**。



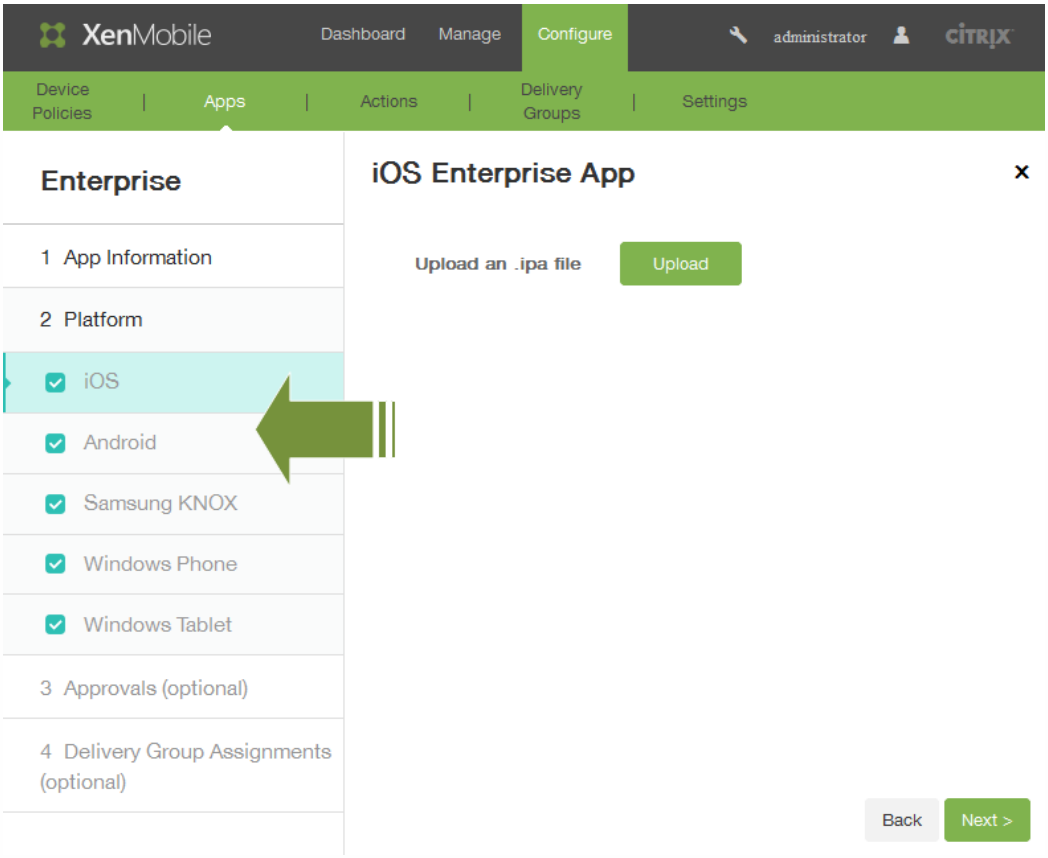
3. 在 Add App（添加应用程序）页面上，单击 **Enterprise**（企业）。



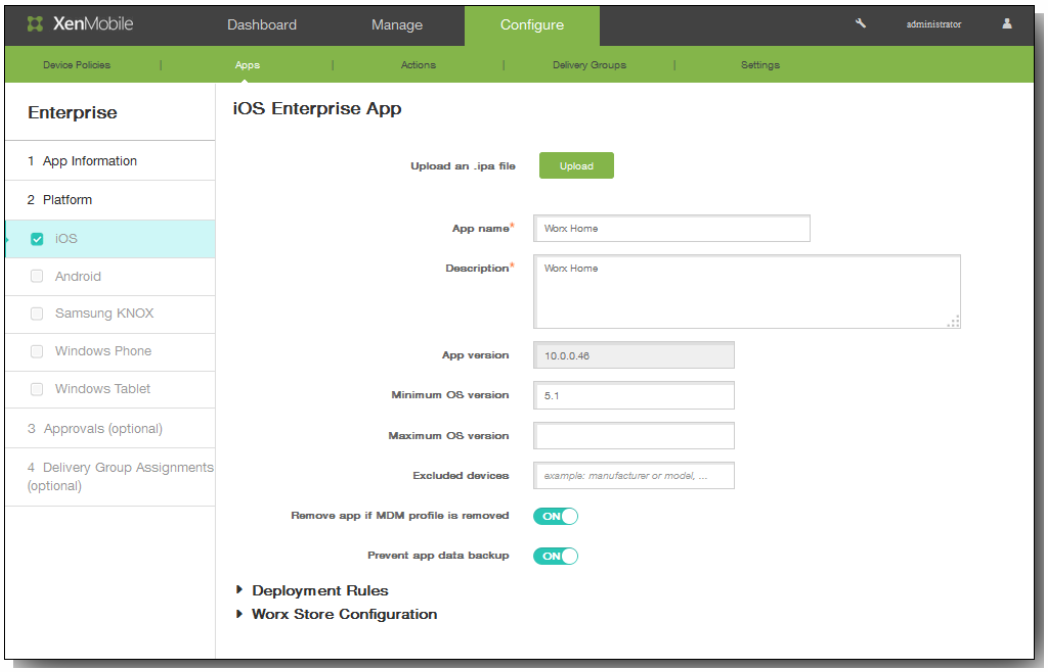
此时将显示 App Information（应用程序信息）页面。



4. 在 App Information（应用程序信息）页面上，完成以下设置：
   1. 名称：键入应用程序的名称。
   2. 说明：键入应用程序的说明。
   3. 在 **App category**（应用程序类别）中，单击某个类别，然后单击 Next（下一步）。
5. 在页面左侧的 Platform（平台）区域中，选择要为其添加应用程序的设备平台（例如，iOS 或 Android）。

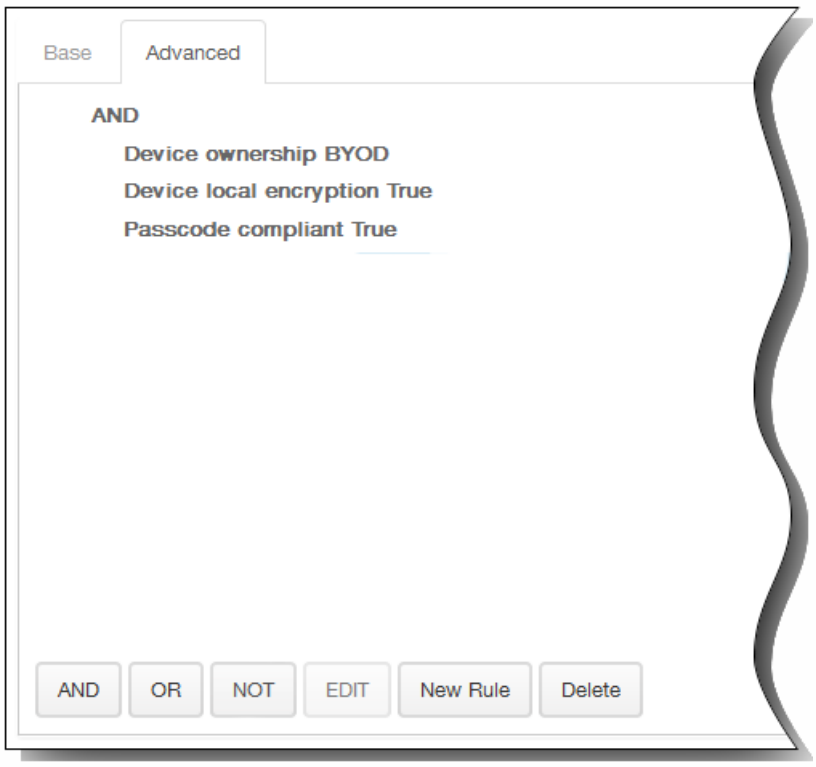


6. 单击 Upload（上载）浏览到文件的位置，然后单击 Next（下一步）。此时将显示平台类型的应用程序信息页面。这些字段已经预填充了与所选应用程序相关的信息（包括关联的名称、说明、版本号和图像）。如有需要，可更改应用程序的名称和说明。



7. 如果要在删除 MDM 配置文件时删除应用程序，请在如果删除了 MDM 配置文件，则删除应用程序中，单击开。 默认情况下，此选项设置为 ON（启用）。
8. 如果要阻止应用程序备份数据，请在阻止备份应用程序数据中，单击开。 默认情况下，此选项设置为 ON（启用）。
9. 展开部署规则。默认情况下将显示基础选项卡。

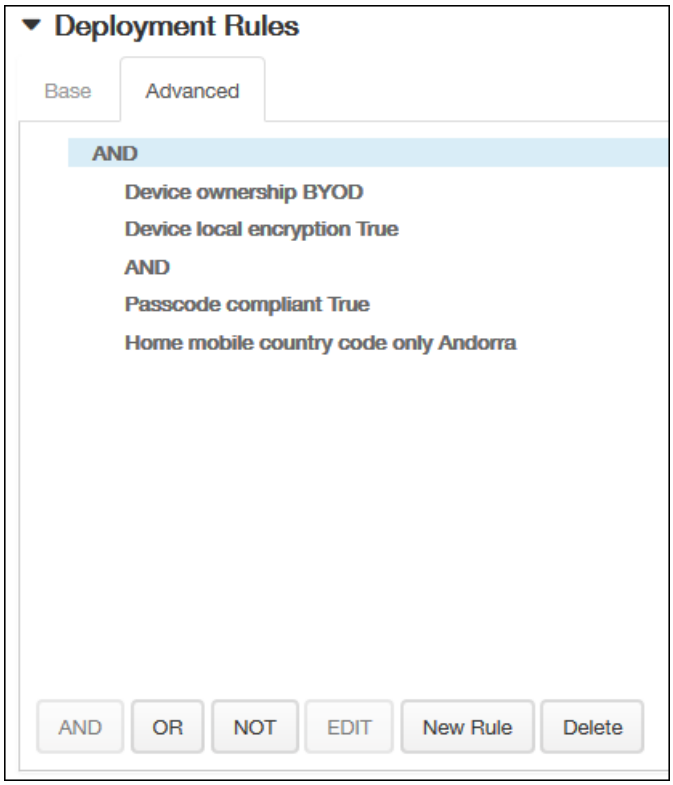
1. 在此列表中，单击选项以确定部署应用程序的时间。
   1. 可以选择在满足所有条件时部署应用程序，或在满足任意条件时部署应用程序。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。



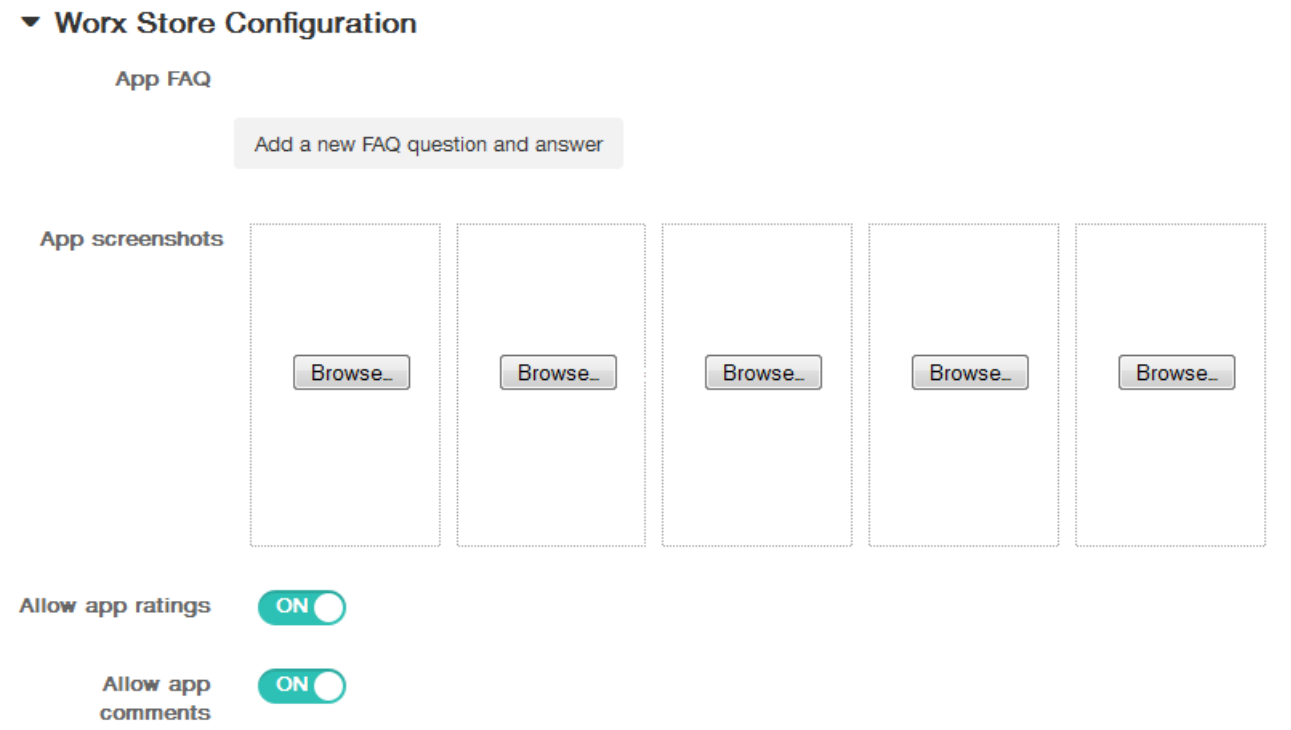
将显示您在基础选项卡上选择的条件。

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，设备必须兼容通行码，并且移动设备国家/地区代码不能仅为安道尔。

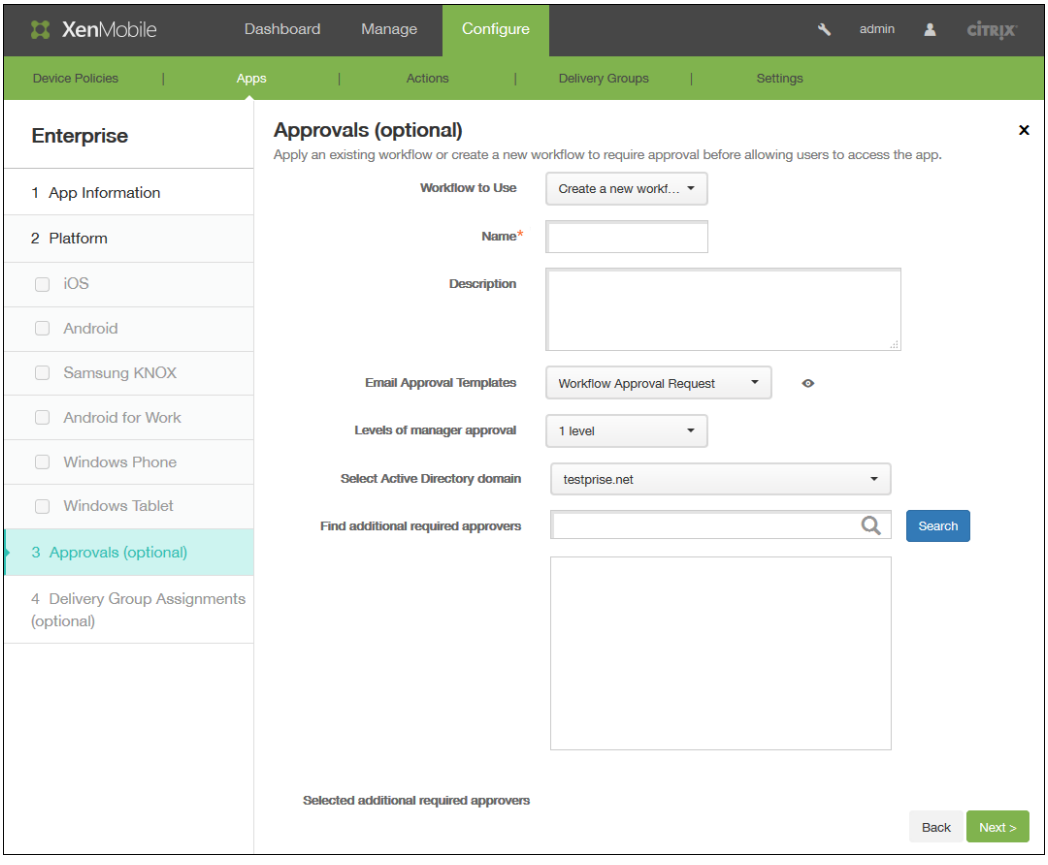


10. 展开 Worx Store Configuration（Worx Store 配置）以添加应用程序的 FAQ，或添加屏幕拍图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形类型必须为 PNG。 不能上载 GIF 或 JPEG 图形。

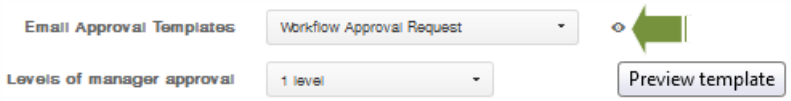


在 Allow app ratings（允许应用程序评级）中，单击 ON（启用）以允许用户对应用程序进行评级。

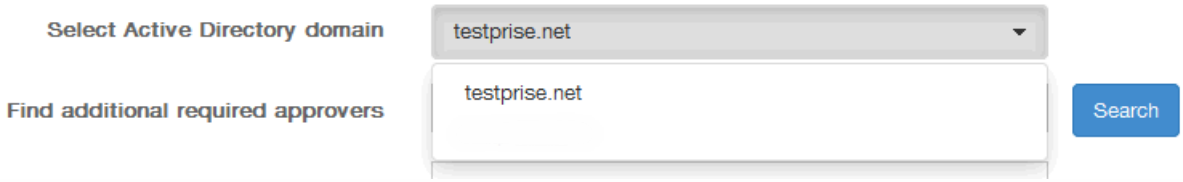
11. 在 Allow app comments（允许应用程序注释）中，单击 ON（启用）以允许用户对选定的应用程序添加注释。
12. 单击下一步。
13. 在审批页面上的要使用的工作流列表中，可以选择单击某个工作流或单击创建新工作流。



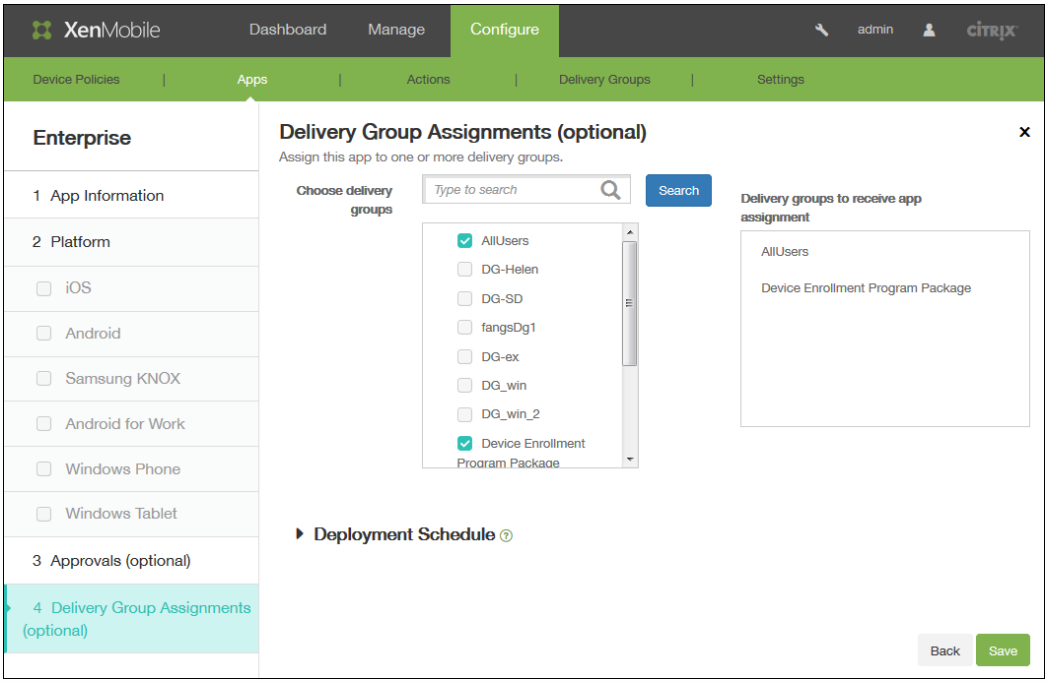
14. 创建新工作流时，XenMobile 控制台将改为显示批准流程的配置选项。 将在下面的步骤中介绍其中的每个字段。 如果需要对创建用户帐户进行审批，请配置这些字段。
    1. 指定工作流的**名称**。
    2. 可以选择输入**说明**。
    3. 在 **Email Approval Templates**（电子邮件批准模板）字段中，单击通知选项。单击眼睛图标以预览所选模板。



    4. 在 **Levels of manager approval**（管理员批准级别）中，单击 None（无）至 3 之间的级别。
    5. 在 **Select Active Directory domain**（选择 Active Directory 域）中，从下拉菜单中选择域；此列表中仅显示已连接的 Active Directory 域（例如，testprise.net）：



    6. 在 Find additional required approvers（查找其他必需批准者）中，可以选择输入所需的其他批准者，然后单击 Search（搜索）。
15. 在 **Delivery Groups Assignment**（交付组分配）页面上，可以选择将应用程序分配给一个或多个交付组。



16. 在 Choose delivery groups（选择交付组）中，搜索一个或多个交付组。选中 **All Users**（所有用户）复选框可将应用程序分配给每个 XenMobile 用户。
17. 展开 Deployment Schedule（部署计划）可进一步精简交付组。
    1. Deploy（部署）：单击 ON（启用）以启用部署计划。
    2. Deployment Schedule（部署计划）：单击 Now（立即）或 Later（稍后）以设置部署计划。
    3. 部署条件：单击以选择是在每次连接时部署应用程序，还是仅在上一个部署失败时再部署应用程序。
    4. 在为始终启用的连接部署中，单击开以在设置始终启用的连接策略时部署。
       注意：仅当同时在 XenMobile 控制台的设置区域的服务器属性部分中配置了全局后台部署密钥时此选项才适用。始终启用计划策略不适用于 iOS 设备。
18. 单击保存。

向 XenMobile 添加 Web 链接应用程序

Oct 22, 2015

在 XenMobile 中，可以建立公共或专用站点或者无需单点登录 (SSO) 的 Web 应用程序的 Web 地址 (URL)。

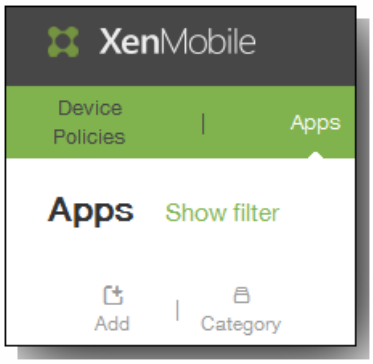
可以从 XenMobile 控制台的应用程序选项卡配置 Web 链接。Web 链接配置完成后，该链接将以链接图标的形式显示在应用程序表格中。当用户通过 Worx Home 登录时，将显示该链接以及可用应用程序和桌面的列表。

要添加链接，请提供以下信息：

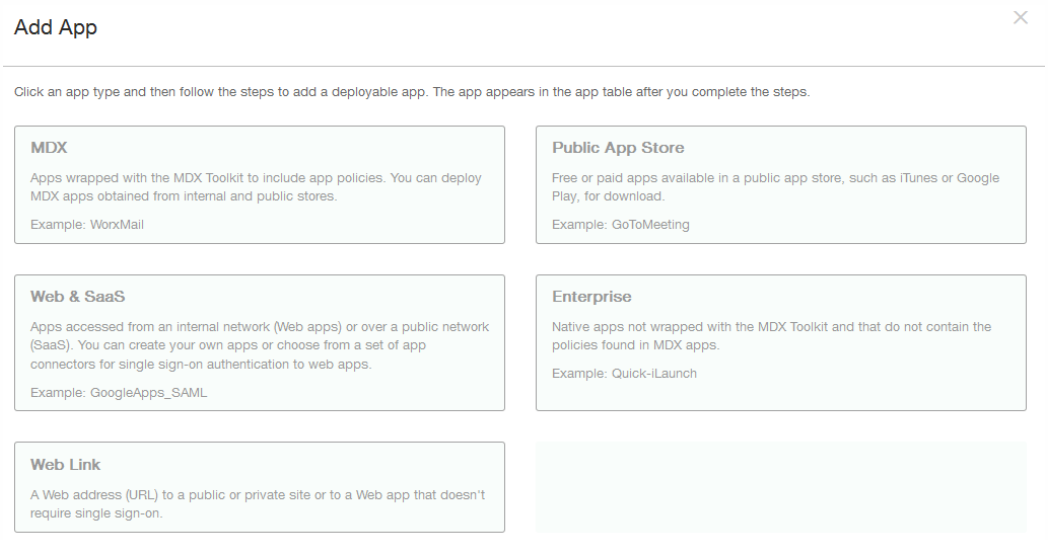
- 链接的名称
- 链接的说明
- Web 地址 (URL)
- 类别
- 角色
- .png 格式的图像（可选）

在 XenMobile 中添加 Web 链接

1. 配置 > 应用程序. 将打开应用程序页面。
2. 在应用程序页面上，单击添加。

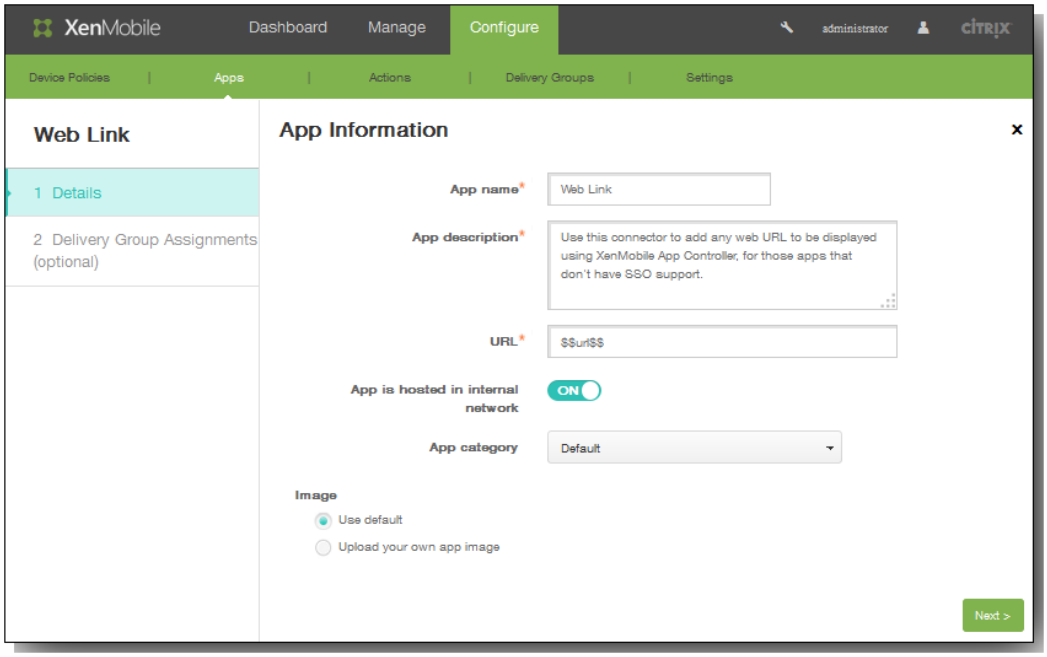


3. 在添加应用程序页面上，单击 Web 链接。

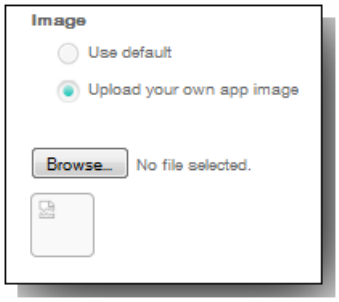


此时将显示应用程序信息页面。

4. 应用程序名称、说明和 URL 字段已经预填充。

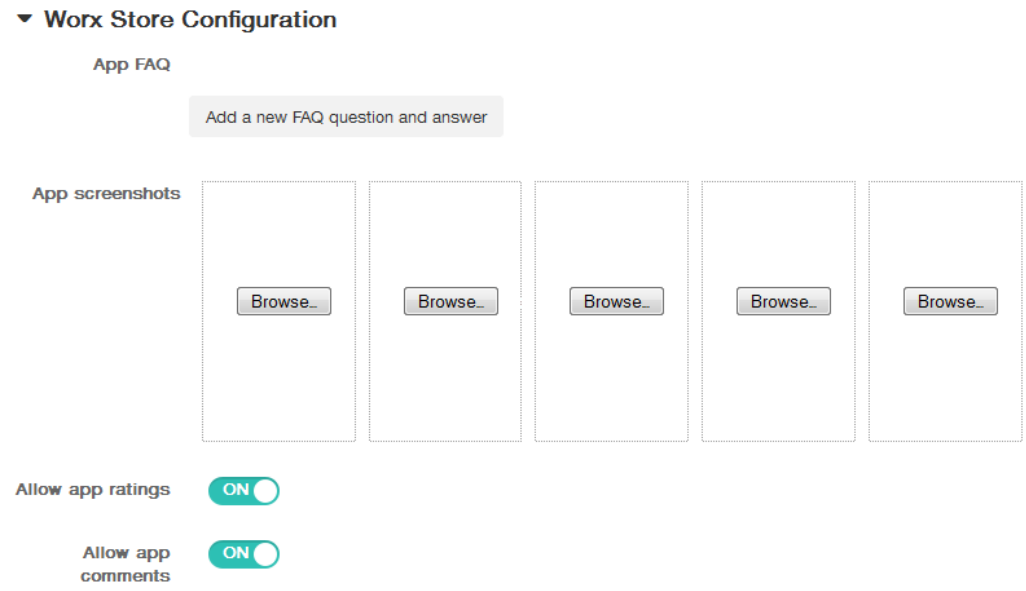


1. 如果适用，在 URL 中输入应用程序的 Web 地址或保留默认地址。
2. 如果应用程序正在内部网络中的服务器上运行，请在应用程序托管在内部网络中，单击开。 如果用户从远程位置连接到内部应用程序，则必须通过 NetScaler Gateway 进行连接。 将此选项设置为开将向应用程序添加 VPN 关键字，并允许用户通过 NetScaler Gateway 连接。
3. 在应用程序类别列表中，单击某个类别。
4. 如果要与连接器关联自己的缩略图，请选择上载您自己的应用程序图片。 单击浏览以查找所需的图像：



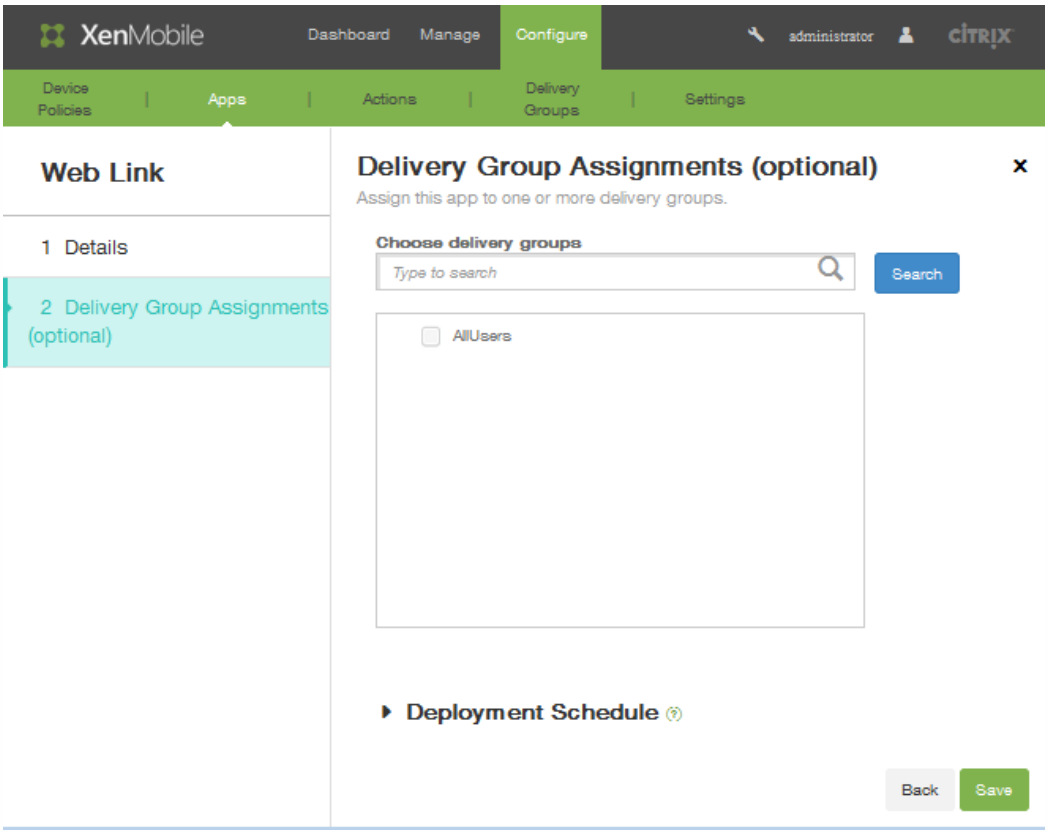
图像的类型必须是 PNG。

5. 展开 Worx Store 配置以添加应用程序的 FAQ，或添加屏幕拍图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形类型必须为 PNG。 不能上载 GIF 或 JPEG 图形。



在允许对应用程序评分中，单击开以允许用户对应用程序进行评分。

6. 在允许评价应用程序中，单击开以允许用户评价选定的应用程序。
7. 单击下一步。
8. 在**交付组分配**页面上，可以选择将应用程序分配给一个或多个交付组。



9. 在选择交付组中，搜索一个或多个交付组。 选中**所有用户**复选框可将应用程序分配给每个 XenMobile 用户。
10. 展开部署计划可进一步精简交付组。

1. 部署：单击开以启用部署计划。
2. 部署计划：单击立即或稍后以设置部署计划。
3. 部署条件：单击以选择是在每次连接时部署应用程序，还是仅在上一个部署失败时再部署应用程序。
4. 在为始终启用的连接部署中，单击开以在设置始终启用的连接策略时部署。
   注意：仅当同时在 XenMobile 控制台设置区域的服务器属性部分中配置了全局后台部署密钥时此选项才适用。始终启用计划策略不适用于 iOS 设备。

11. 单击保存。

创建和管理工作流

Oct 22, 2015

可以使用工作流对用户帐户的创建和删除进行管理。需要先确定组织中有权批准用户帐户请求的人员，然后才能使用工作流。然后可以使用工作流模板创建和批准用户帐户请求。

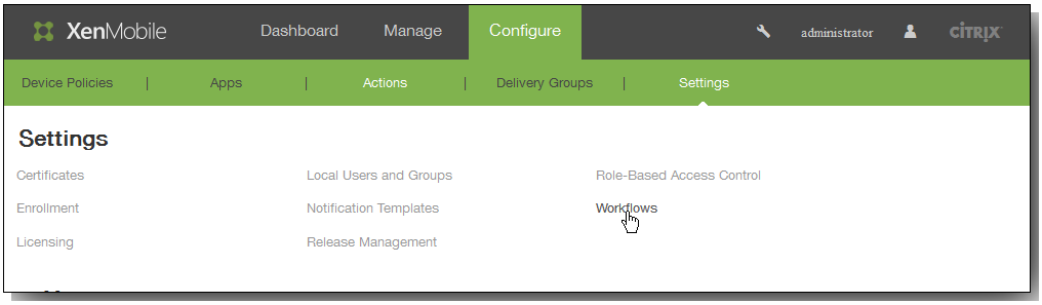
首次配置 XenMobile 时，应配置工作流电子邮件设置。必须配置工作流电子邮件设置才能使用工作流。随时可以更改工作流电子邮件设置。这些设置包括电子邮件服务器、端口、电子邮件地址以及创建用户帐户的请求是否需要进行审批。

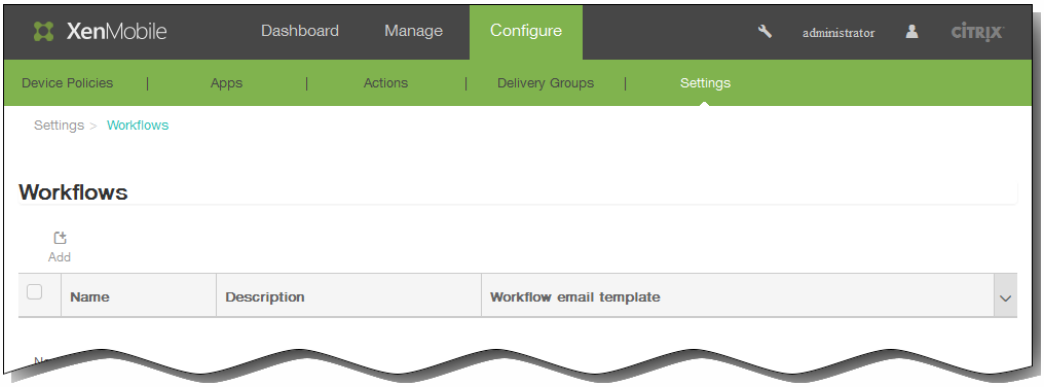
可以在 XenMobile 中的两个位置配置工作流：

- 在 XenMobile 控制台的工作流页面中。在工作流页面上，可以配置多个用于应用程序配置的工作流。在工作流页面上配置工作流时，可以在配置应用程序时选择工作流。
- 配置应用程序连接器时，在应用程序中提供工作流名称，然后配置可以审批用户帐户请求的人员。请参阅向 XenMobile 添加应用程序。

可以为用户帐户分配最多三个管理者审批级别。如果需要其他人员审批用户帐户，可以使用该人员的姓名或电子邮件地址搜索和选择其他审批者。XenMobile 找到人员时，您可以将其添加到工作流中。工作流中的所有人员都将收到电子邮件，以批准或拒绝新用户帐户。

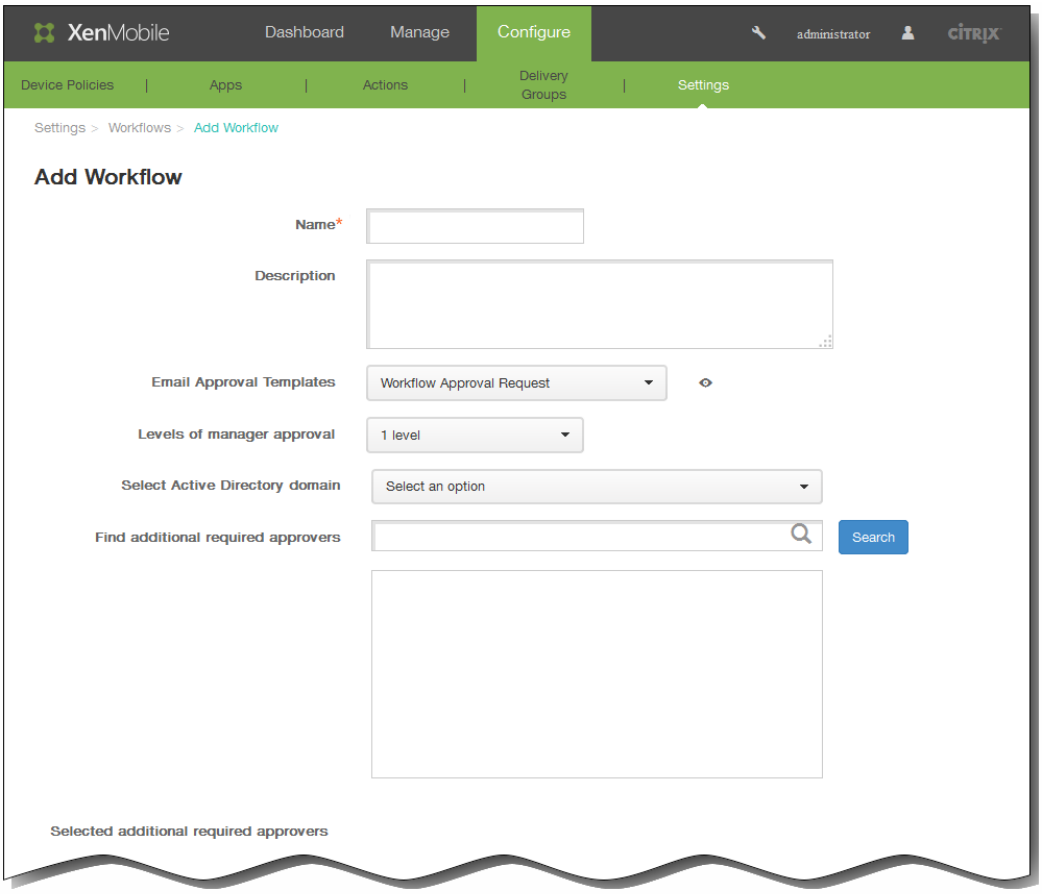
1. 在 XenMobile 控制台中，单击配置 > 设置 > 工作流。



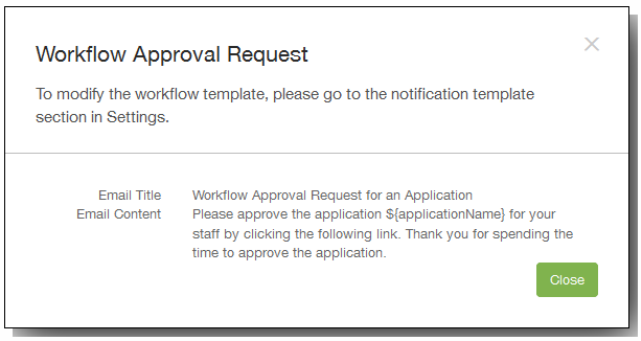


此时将显示工作流页面。

2. 在工作流页面上，单击添加。 此时将显示添加工作流页面。



3. 在添加工作流页面的名称字段中，键入工作流的唯一名称。
4. 在说明中，可以选择键入工作流的说明。
5. 在电子邮件审批模板列表中，选择要分配的电子邮件审批模板。 在 XenMobile 控制台设置下的通知模板部分创建电子邮件模板。单击此字段右边的眼睛图标时，将显示以下提示。



6. 在 Levels of manager approval（管理员审批级别）列表中，选择此工作流所需的管理员审批的级别数。
7. 在选择 Active Directory 域列表中，选择用于工作流的合适 Active Directory 域。
8. 在查找所需的其他审批者旁边，在搜索字段中键入其他必需人员的姓名，然后单击搜索。 源于 Active Directory 的姓名。
9. 人员的姓名显示在此字段中后，选中其姓名旁边的复选框。 人员的姓名和电子邮件地址显示在选定的其他所需审批者列表中。要从选定的其他所需审批者列表中删除人员，请执行以下操作：
   - 单击搜索以查找选定域中的所有人员列表。
   - 在搜索框中键入完整名称或部分名称，然后单击搜索以限制搜索结果。

在搜索结果列表中，选定的其他所需审批者列表中的人员姓名旁边有一个复选标记。滚动列表，并取消选中要删除的各个姓名旁边的复选框。

10. 单击保存。
    已创建的工作流显示在工作流页面。

    创建工作流后，您可以查看工作流详细信息，查看与工作流相关的应用程序，或者删除工作流。工作流创建后无法进行编辑。如果需要使用不同审批级别或审批者的工作流，必须创建新工作流。

查看详细信息和删除工作流

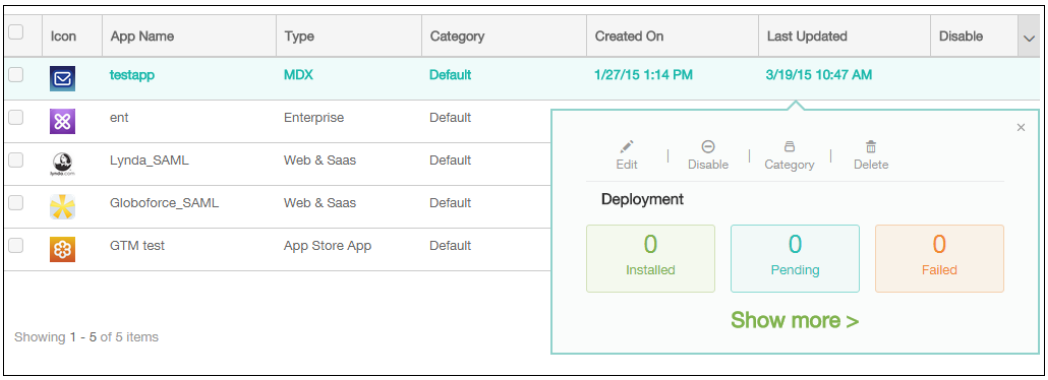
1. 在工作流页面的现有工作流列表中，通过单击表格中的行或选中工作流旁边的复选框，选择特定工作流。
2. 要删除工作流，请单击删除。 此时将显示确认对话框。再次单击删除。
   重要：此操作无法撤消。

在 XenMobile 中升级应用程序

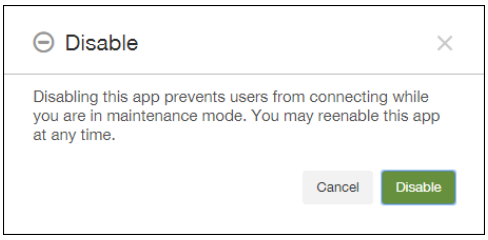
Oct 22, 2015

要在 XenMobile 中升级应用程序，您可在 XenMobile 控制台中禁用该应用程序，然后上载该应用程序的新版本。

1. 在 XenMobile 控制台中，单击配置 > 应用程序。
2. 对于托管设备（在 XenMobile 中注册用于移动设备管理的设备），跳至步骤 3。 对于未托管设备（在 XenMobile 中注册仅用于企业版应用程序管理目的的设备），请执行以下操作：
   1. 在“应用程序”表中，单击选择要更新的应用程序，然后在显示的菜单中单击禁用。



   2. 在确认对话框中，单击禁用。

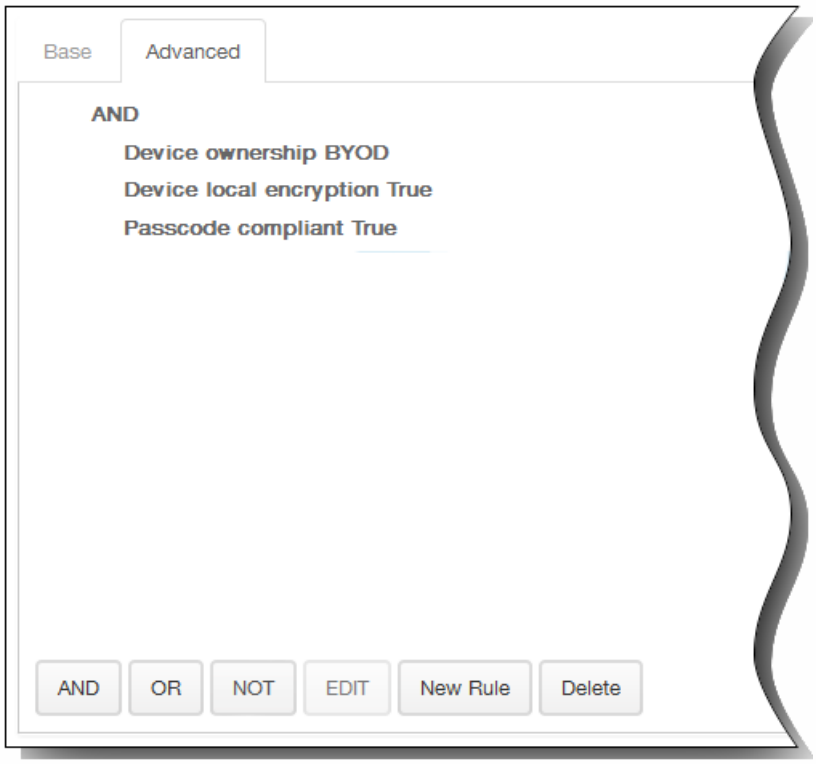


   该应用程序在“应用程序”表中显示为已禁用状态。

   注意：禁用应用程序会将应用程序置于维护模式。当应用程序处于已禁用状态时，用户在注销之后无法再连接到该应用程序。禁用应用程序是可选设置，但 Citrix 建议禁用应用程序以避免应用程序功能出现问题。例如，可能会由于策略更新而出现问题，或者如果用户在您将应用程序上载到 XenMobile 的同时请求下载。
3. 单击选择应用程序，然后在显示的菜单中单击编辑。 您最初为应用程序选择的平台显示为选中状态。
4. 在应用程序信息页面上，您可以选择更改名称、说明或应用程序类别，然后单击下一步。
5. 单击上载选择要上载的文件以替换当前应用程序，然后单击下一步。

   应用程序即上载到 XenMobile。另外，您可以更改应用程序详细信息和策略设置。
6. 单击下一步，然后在步骤 8 到步骤 14 中保留当前设置，或对升级进行相关更改。
7. 展开部署规则。 默认情况下将显示基础选项卡。

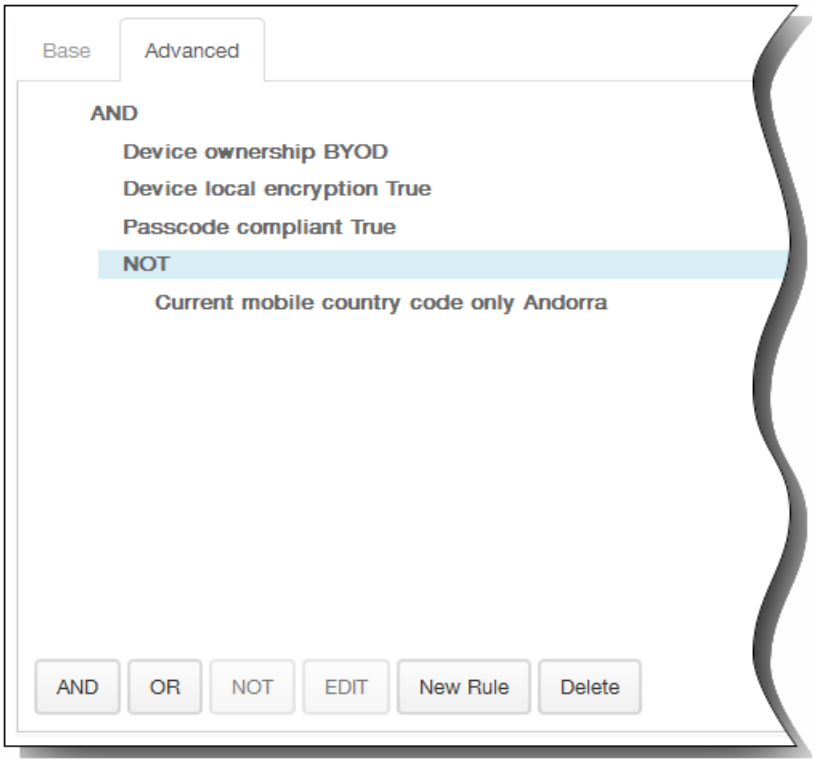
1. 在此列表中，单击选项以确定部署应用程序的时间。
   1. 可以选择在满足所有条件时部署应用程序，或在满足任意条件时部署应用程序。默认选项是全部。
   2. 单击新建规则以定义条件。
   3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
   4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。



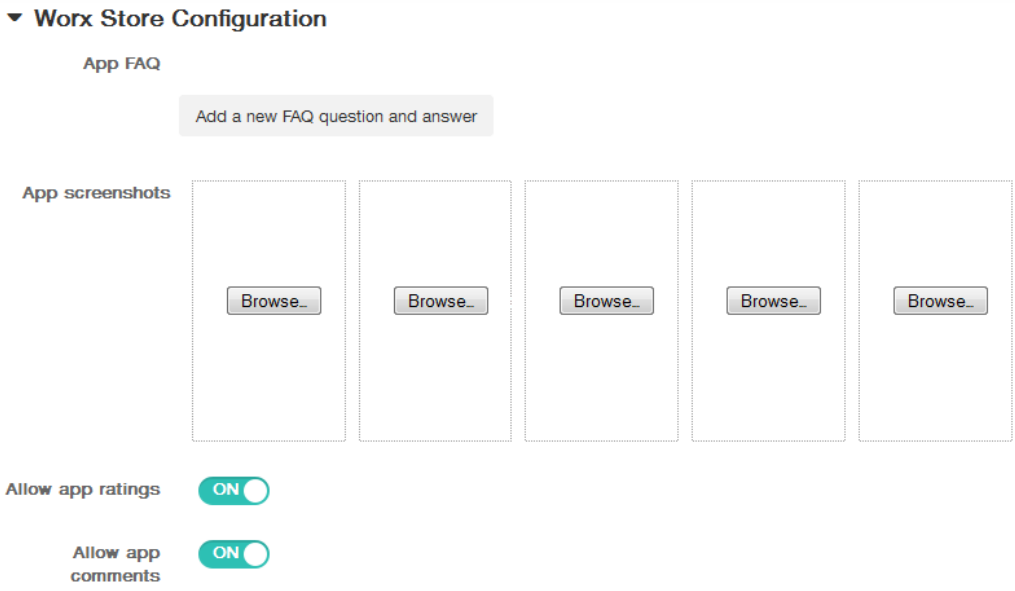
将显示您在基础选项卡上选择的条件。

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，设备必须兼容通行码，并且移动设备国家/地区代码不能仅为安道尔。

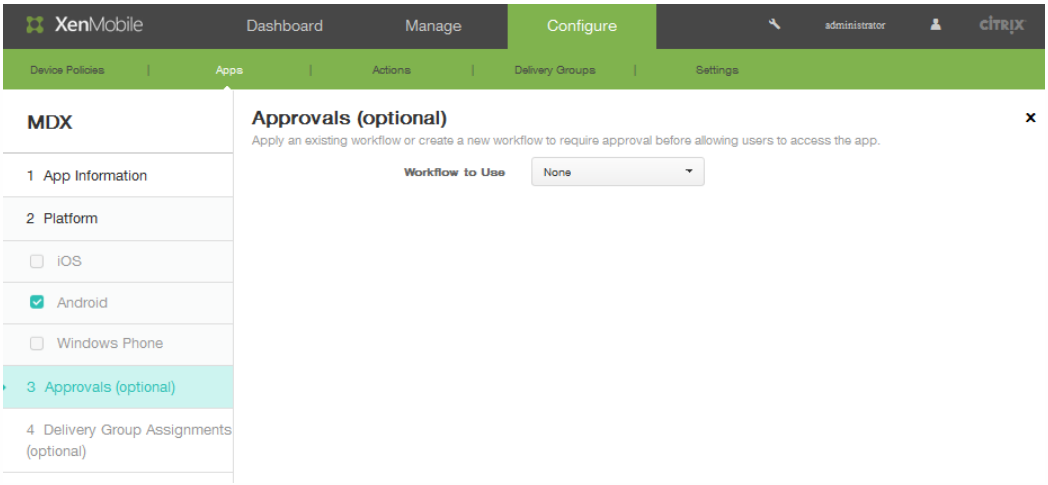


8. 展开 Worx Store 配置以添加应用程序的 FAQ，或添加屏幕拍图以帮助在 Worx Store 中对应用程序进行分类。 上载的图形类型必须为 PNG。 不能上载 GIF 或 JPEG 图形。

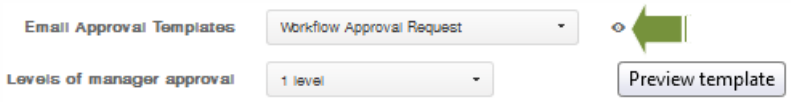


在允许对应用程序评分中，单击开以允许用户对应用程序进行评分。

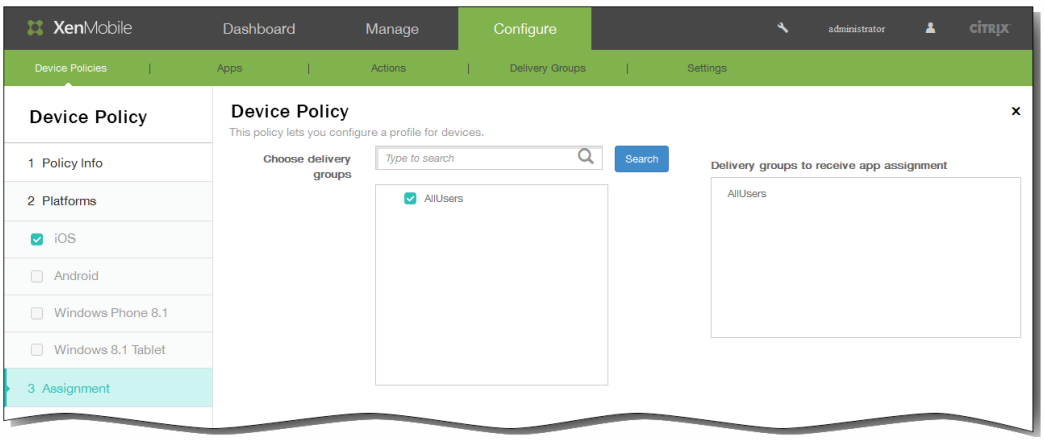
9. 在允许评价应用程序中，单击开以允许用户评价选定的应用程序。
10. 单击下一步。 此时将显示审批屏幕。



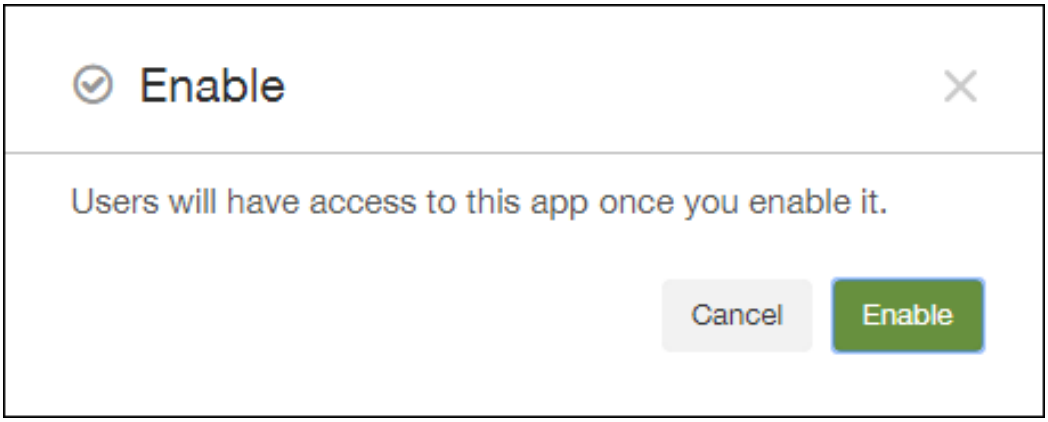
11. 创建新工作流时，XenMobile 控制台将改为显示批准流程的配置选项。 将在下面的步骤中介绍其中的每个字段。 如果需要对创建用户帐户进行审批，请配置这些字段。
    1. 指定工作流的**名称**。
    2. 可以选择输入**说明**。
    3. 在**电子邮件审批模板**字段中，单击通知选项。 单击眼睛**图标**以预览所选模板。



    4. 在**经理审批级别**中，单击无至 3 之间的某个级别。 。
    5. 在**选择 Active Directory 域**中，单击域。
    6. 在查找所需的其他审批者中，可以选择输入所需的其他审批者，然后单击搜索。
12. 单击下一步。
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. 单击保存。此时将显示应用程序页面。
15. 如果在步骤 2 中已禁用该应用程序，请执行以下操作：
    1. 在应用程序表中，单击选择已更新的应用程序，然后在显示的菜单中单击启用。
    2. 在显示的确认消息中，单击启用。



用户现在可以再次访问该应用程序并接收提示用户升级应用程序的通知。

MDX 应用程序策略概览

Apr 22, 2016

有关列出适用于 iOS、Android 和 Windows Phone 以及有关限制和 Citrix 建议的备注的表格，请参阅 MDX Toolkit 文档中的 MDX 应用程序策略概览。

注意：Worx Home 在特定操作期间会刷新策略。有关详细信息，请参阅 Worx Home。

将 XenMobile 和 ShareFile 应用程序配置为使用 SAML 进行单点登录

Oct 13, 2016

可以将 XenMobile 和 ShareFile 配置为使用安全声明标记语言 (Security Assertion Markup Language, SAML) 提供对通过 MDX Toolkit 打包的 ShareFile 移动应用程序以及未打包的 ShareFile 客户端（例如 Web 站点、Outlook 插件或同步客户端）的单点登录 (SSO) 访问。

- **面向打包的 ShareFile 应用程序**。 通过 ShareFile 移动应用程序登录 ShareFile 的用户将被重定向到 Worx Home 进行用户身份验证以及获取 SAML 令牌。 成功进行身份验证后，ShareFile 移动应用程序会将 SAML 令牌发送到 ShareFile。 初始登录后，用户可以通过 SSO 访问 ShareFile 移动应用程序，并且可以将 ShareFile 中的文档附加到 WorxMail 电子邮件，而不需要每次都登录。
- **面向未打包的 ShareFile 客户端**。 使用 Web 浏览器或其他 ShareFile 客户端登录 ShareFile 的用户将被重定向到 XenMobile 进行用户身份验证以及获取 SAML 令牌。 成功进行身份验证后，SAML 令牌将被发送到 ShareFile。 初始登录后，用户可以通过 SSO 访问 ShareFile 客户端，而不需要每次都登录。

有关详细的参考体系结构图，请参阅“XenMobile Deployment Handbook”（《XenMobile 部署手册》）文章 Reference Architecture for On-Premises Deployments（适用于本地部署的参考体系结构）。

必备条件

必须先完成以下必备条件，才能对 XenMobile 和 ShareFile 应用程序配置 SSO：

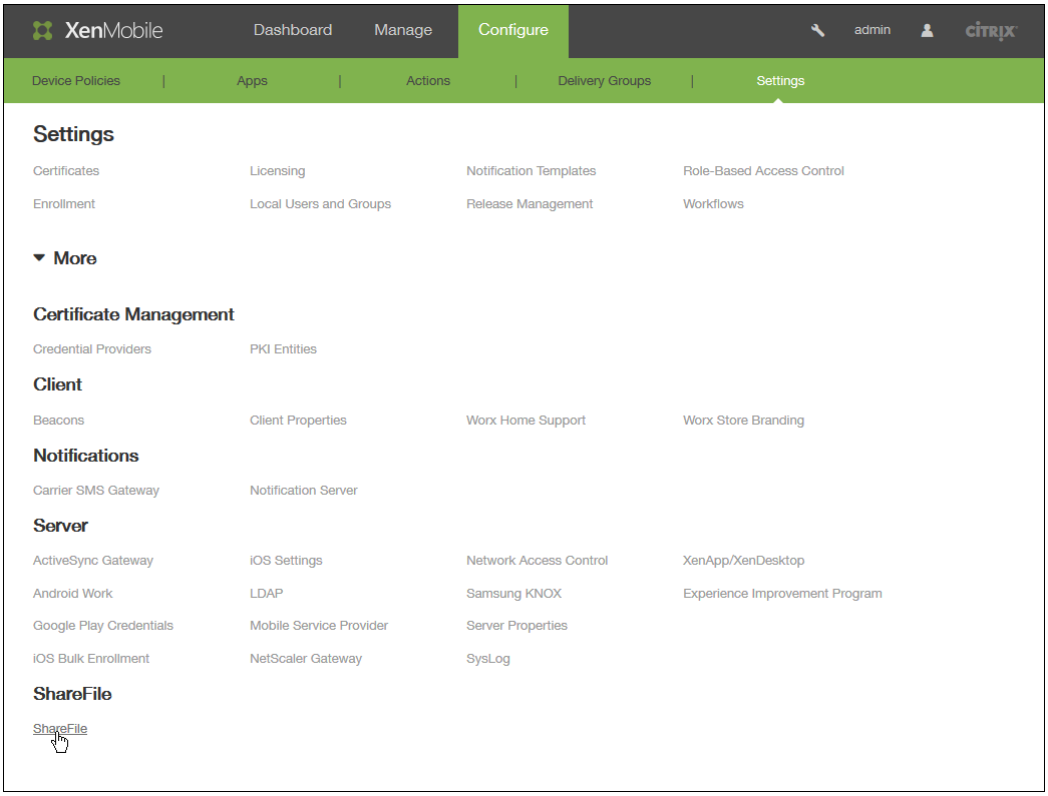
- MDX Toolkit 9.0.4 或更高版本（适用于 ShareFile 移动应用程序）
- 恰当的 ShareFile 移动应用程序：
  - ShareFile for iPhone 3.0.x
  - ShareFile for iPad 2.2.x
  - ShareFile for Android 3.2.x
- Worx Home 9.0（适用于 ShareFile 移动应用程序）
  根据需要安装 iOS 或 Android 版本。
- ShareFile 管理员帐户

请确保 XenMobile 和 ShareFile 能够连接。有关检查连接的信息，请参阅执行连接检查。

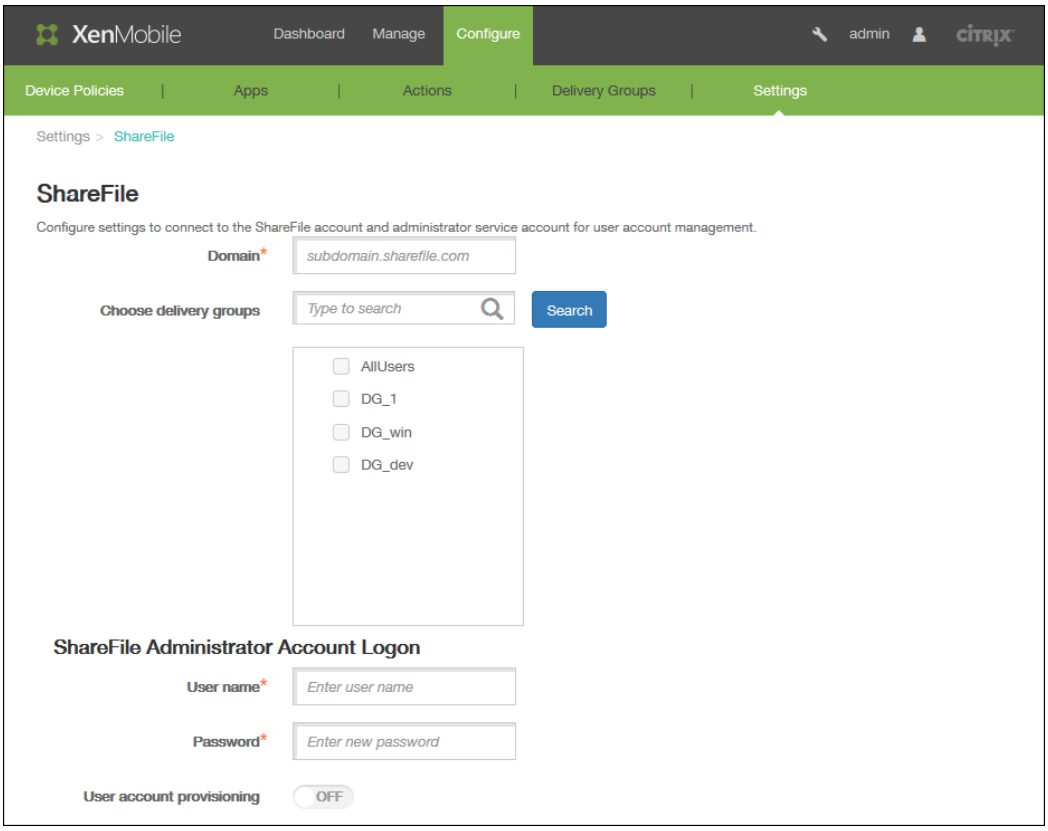
配置 ShareFile 访问

为 ShareFile 配置 SAML 之前，请按如下所示提供 ShareFile 访问信息：

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



2. 单击更多，然后在 ShareFile 下，单击 ShareFile。此时将显示 ShareFile 配置页面。



3. 配置以下设置：
   - 域：键入 ShareFile 子域的名称，例如 example.sharefile.com。
   - 选择交付组：选择或搜索希望能够对 ShareFile 使用 SSO 的交付组。
   - 用户名：键入 ShareFile 管理员用户名。此用户必须具有管理员权限。
   - 密码：键入 ShareFile 管理员的密码。
   - 用户帐户置备：如果要在 XenMobile 中启用用户置备，请打开此选项；如果要使用 ShareFile 用户管理工具置备用户，请将其保留在禁用状态。
     注意：如果选定的角色中包含没有 ShareFile 帐户的用户，XenMobile 会自动为该用户置备一个 ShareFile 帐户，前提是您启用了用户帐户置备。Citrix 建议您使用具有小型成员关系的角色以测试配置。这样可以避免出现大量没有 ShareFile 帐户的用户的可能性。
4. 单击保存。

为打包的 ShareFile MDX 应用程序配置 SAML

以下步骤适用于 iOS 和 Android 应用程序和设备。

1. 使用 MDX Toolkit 打包 ShareFile 移动应用程序。有关使用 MDX Toolkit 打包应用程序的详细信息，请参阅使用 MDX Toolkit 打包应用程序。
2. 在 XenMobile 中，上载打包的 ShareFile 移动应用程序。有关上载 MDX 应用程序的信息，请参阅向 XenMobile 中添加 MDX 应用程序。
3. 使用在配置 ShareFile 访问中配置的管理员用户名和密码登录 ShareFile，验证 SAML 设置。
4. 请务必为 ShareFile 和 XenMobile 配置相同的时区。
   注意：时区不同可能会导致时间戳不匹配，进而导致 SSO 失败。

验证 ShareFile 移动应用程序

1. 在用户设备上，如果尚未安装和配置 Worx Home，请进行安装和配置。
2. 从 Worx Store 中下载并安装 ShareFile 移动应用程序。
3. 启动 ShareFile 移动应用程序。
   ShareFile 将启动，但不提示输入用户名或密码。

使用 WorxMail 进行验证

1. 在用户设备上，如果尚未安装和配置 Worx Home，请进行安装和配置。
2. 从 Worx Store 中下载、安装并配置 WorxMail。
3. 打开新的电子邮件窗体，然后轻按从 ShareFile 附加。
   此时将显示可以附加到电子邮件中的文件，但不提示输入用户名或密码。

为其他 ShareFile 客户端配置 NetScaler Gateway

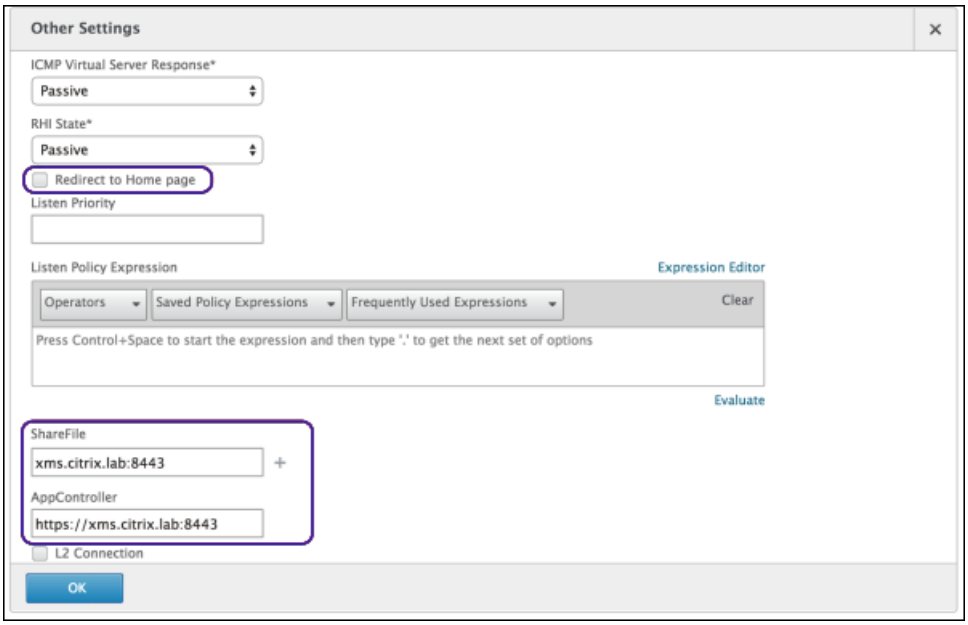
如果要配置对未打包的 ShareFile 客户端（例如 Web 站点、Outlook 插件或同步客户端）的访问，必须将 NetScaler Gateway 配置为支持使用 XenMobile 作为 SAML 身份提供程序，如下所示：

- 禁用主页重定向。
- 创建 ShareFile 会话策略和配置文件。
- 在 NetScaler Gateway 虚拟服务器上配置策略。

禁用主页重定向

必须禁用通过 /cginfra 路径发出的请求的默认行为，以便用户能够看到最初请求的内部 URL，而非配置的主页。

1. 编辑用于 XenMobile 登录的 NetScaler Gateway 虚拟服务器的设置。在 NetScaler 10.5 中，转至 Other Settings（其他设置），然后取消选中标记了 Redirect to Home Page（重定向到主页）的复选框。

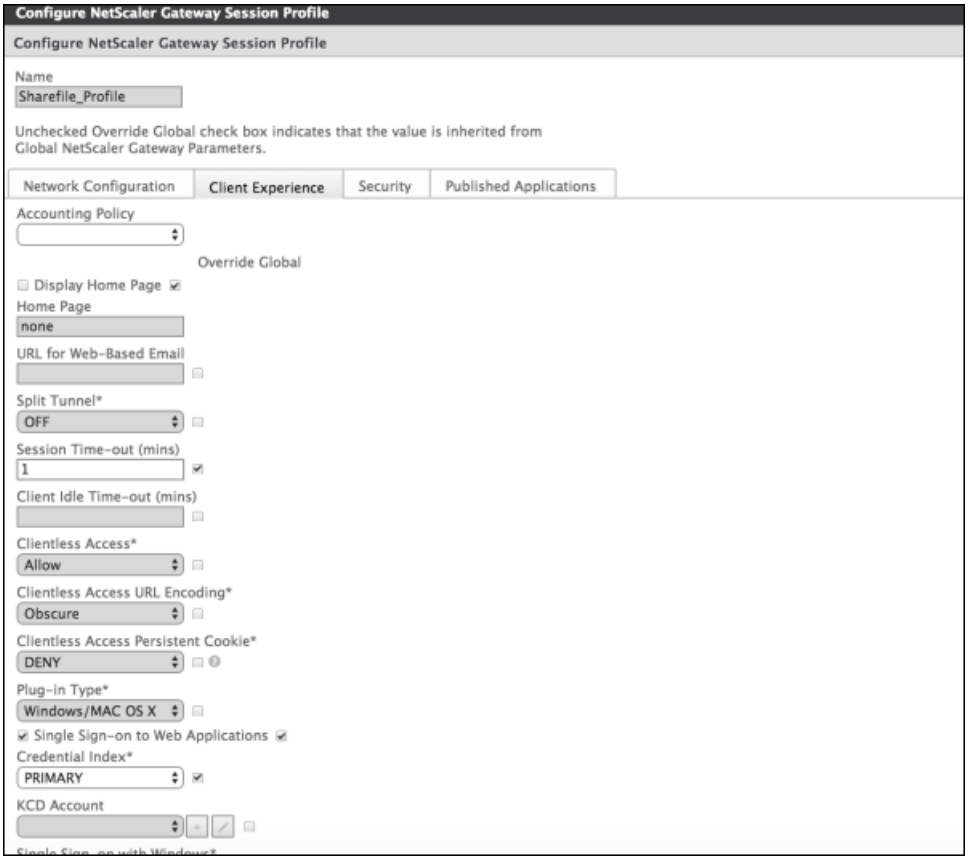


2. 在 ShareFile 下，键入 XenMobile 内部服务器的名称和端口号。
3. 在 AppController 下，键入 XenMobile URL。
   此配置授权您向通过 /cginfra 路径输入的 URL 发送请求。

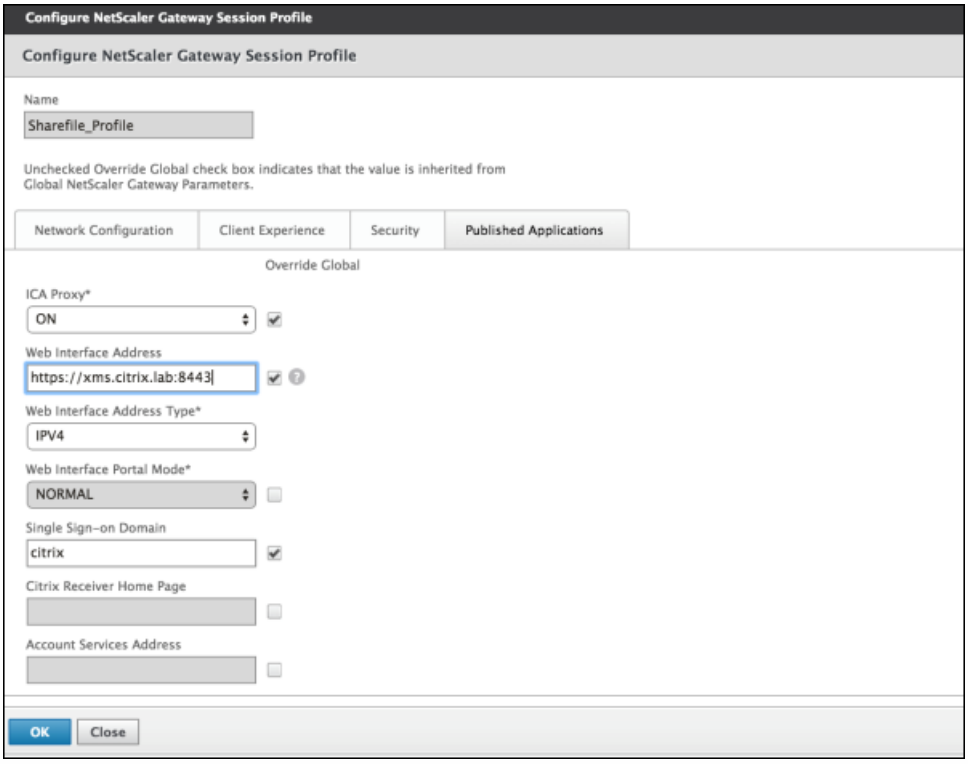
创建 ShareFile 会话策略并请求配置文件

请配置以下设置以创建 ShareFile 会话策略并请求配置文件：

1. 在 NetScaler Gateway 配置实用程序中，在左侧导航窗格中单击 NetScaler Gateway > Policies（策略）> Session（会话）。
2. 创建一个新会话策略。在 Policies（策略）选项卡上，单击 Add（添加）。
3. 在 Name（名称）字段中，键入 ShareFile_Policy。
4. 单击 + 按钮创建一项新操作。
   此时将显示 Create NetScaler Gateway Session Profile（创建 NetScaler Gateway 会话配置文件）屏幕。配置以下设置：

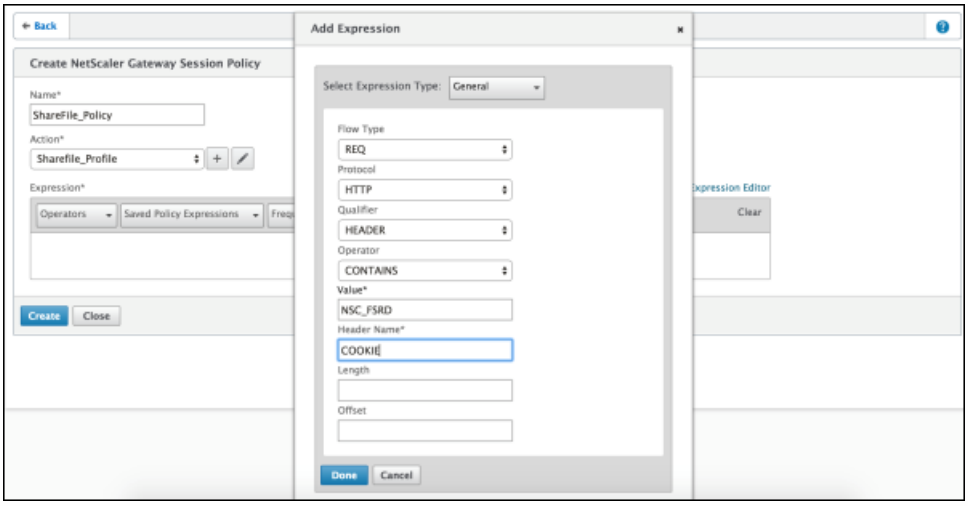


1. Name（名称）：键入 ShareFile_Profile。
2. 单击 Client Experience（客户端体验）选项卡，然后配置以下设置：
   1. Home Page（主页）：键入 none（无）。
   2. Session Time-out (mins)（会话超时(分钟)）：键入 1。
   3. Single Sign-on to Web Applications（单点登录到 Web 应用程序）：选择此设置。
   4. Credential Index（凭据索引）：在列表中，单击 PRIMARY（主要）。
3. 单击 Published Applications（已发布的应用程序）选项卡，然后配置以下设置：



1. ICA Proxy（ICA 代理）：在列表中，选择 ON（开）。
2. Web Interface Address（Web Interface 地址）：键入 XenMobile 服务器的 URL。
3. Single Sign-on Domain（单点登录域）：键入 Active Directory 的域名。
   注意：配置 NetScaler Gateway 会话配置文件时，Single Sign-on Domain（单点登录域）的域后缀必须与在 LDAP 中定义的 XenMobile 域别名匹配。

5. 单击 Create（创建）以定义会话配置文件。
6. 单击 Expression Editor（表达式编辑器），然后配置以下设置：



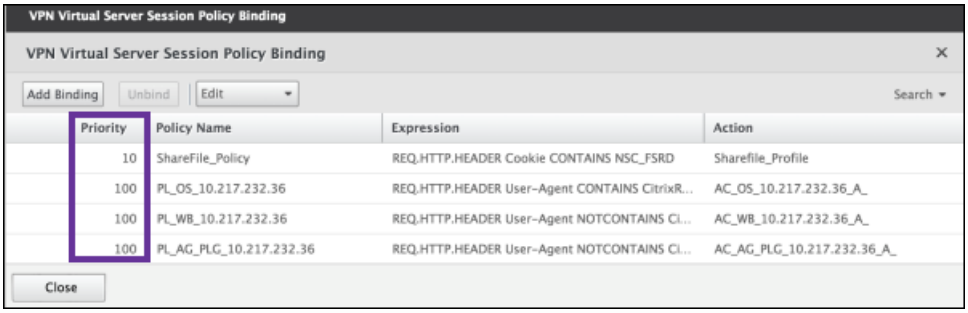
1. Value（值）：键入 NSC_FSRD。
2. Header Name（标头名称）：键入 COOKIE。
3. 单击 Done（完成）。

7. 单击 Create（创建），然后单击 Close（关闭）。

在 NetScaler Gateway 虚拟服务器上配置策略

请在 NetScaler Gateway 虚拟服务器上配置以下设置。

1. 在 NetScaler Gateway 配置实用程序中，在左侧导航窗格中单击 NetScaler Gateway > Virtual Servers（虚拟服务器）。
2. 在 Details（详细信息）窗格中，单击 NetScaler Gateway 虚拟服务器。
3. 单击 Edit（编辑）。
4. 单击 Configured policies（已配置的策略） > Session policies（会话策略），然后单击 Add binding（添加绑定）。
5. 选择 ShareFile_Policy。
6. 编辑为选定策略自动生成的 Priority（优先级）编号，以便与列出的任何其他策略相比，其优先级最高（编号最小），如下图所示。



7. 单击 Done（完成），然后保存运行的 NetScaler 配置。

为非 MDX ShareFile 应用程序配置 SAML

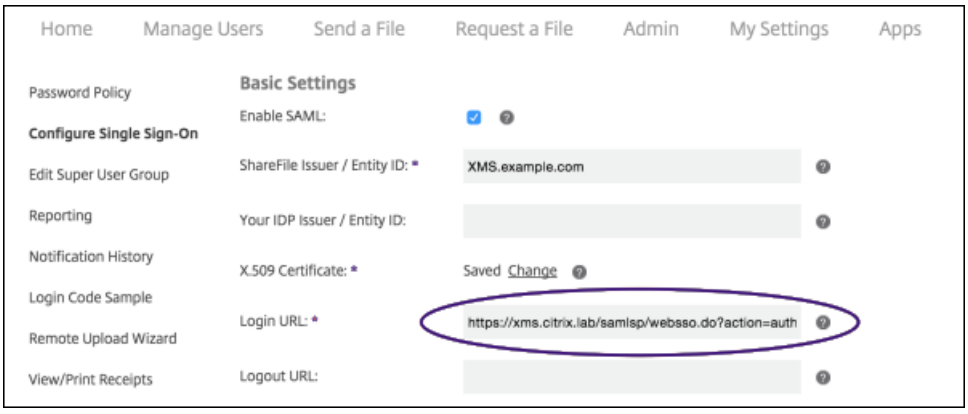
请执行以下步骤，查找 ShareFile 配置的内部应用程序名称。

1. 使用 URL https://:4443/OCA/admin/ 登录 XenMobile 管理工具。请务必使用大写字母输入 OCA。
2. 在查看列表中，单击配置。

3. 单击应用程序 > 应用程序，并记录显示名称为 ShareFile 的应用程序的应用程序名称。

修改 ShareFile.com 的 SSO 设置

1. 以 ShareFile 管理员身份登录 ShareFIle 帐户 (https://<子域>.sharefile.com)。
2. 在 ShareFile Web 界面中，单击 Admin（管理），然后选择 Configure Single Sign-on（配置单点登录）。
3. 按如下所示编辑 Login URL（登录 URL）：
   Login URL（登录 URL）应如下所示：https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1。



1. 在 XenMobile 服务器的 FQDN 前面插入 NetScaler Gateway 虚拟服务器的外部 FQDN 和 /cginfra/https/，然后在 XenMobile 的 FQDN 后面添加 8443。

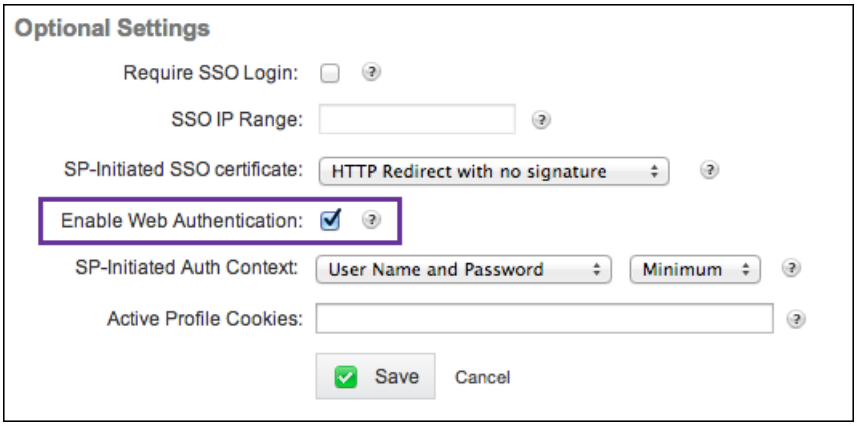
登录 URL 现在应如下所示：https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

2. 将参数 **&app=ShareFile_SAML_SP** 更改为为非 MDX ShareFile 应用程序配置 SAML 步骤 3 中的内部 ShareFile 应用程序名称。内部名称默认为 **ShareFile_SAML**，但是，每次更改配置时，都会在内部名称后面附加一个数字（ShareFile_SAML_2、ShareFile_SAML_3，以此类推）。
   登录 URL 现在应如下所示：https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

3. 向 URL 的结尾末尾添加 &nssso=true。
   修改后的 URL 现在应如下所示：https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**。

   重要：每次在 XenMobile 控制台中编辑或重新创建 ShareFIle 应用程序或更改 ShareFile 设置时，都会在内部应用程序名称后附加一个新数字，这意味着您还必须在 ShareFile Web 站点中更新登录 URL，以反映更新后的应用程序名称。

4. 在 Optional Settings（可选设置）下，选中 Enable Web Authentication（启用 Web 身份验证）复选框。



5. 单击保存。

验证配置

请执行以下配置以验证设置。

1. 将浏览器指向 https://<子域>sharefile.com/saml/login。
   系统会将您重定向到 NetScaler Gateway 登录表单。如果未被重定向，请验证前面的配置设置。

2. 输入所配置的 NetScaler Gateway 和 XenMobile 环境的用户名和密码。
   此时将在 <子域>.sharefile.com 下显示您的 ShareFile 文件夹。如果未显示您的 ShareFile 文件夹，请确保您输入了正确的登录凭据。

自动化操作

Oct 22, 2015

在 XenMobile 中创建自动化操作以计划对事件、用户或设备属性或者用户设备上存在应用程序做出反应。创建自动化操作后，您可以在基于操作中的触发器连接到 XenMobile 时对用户设备建立影响。触发事件后，您可以在采取更实质性的操作之前向用户发送通知以更正问题。

例如，如果要检测先前已加入黑名单的应用程序（如 Words with Friends），您可以指定一个触发器，设置在用户设备上检测到 Words with Friends 时不合规的用户设备。然后，该操作会通知用户必须删除该应用程序才能使其设备重新合规。在采取更实质性的操作（例如选择性地擦除设备）之前，您可以设置等待用户合规的时限。

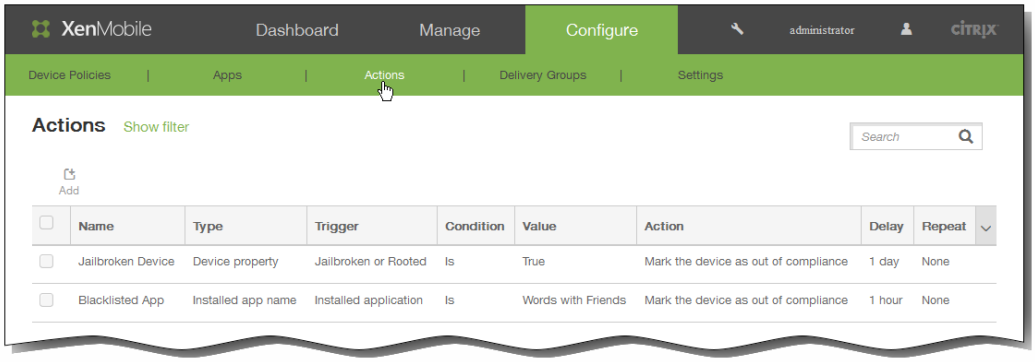
设置为自动出现的影响范围如下：

- 完全或选择性地擦除设备。
- 将设备设置为不合规。
- 吊销设备。
- 在采取更严重的操作之前，向用户发送通知以更正问题。

注意：在可以通知用户之前，必须已在设置中为 SMTP 和 SMS 配置通知服务器，以便 XenMobile 可以发送消息，请参阅 XenMobile 中的通知。此外，请在继续操作前设置打算使用的通知模板。有关设置通知模板的详细信息，请参阅在 XenMobile 中创建或更新通知模板。

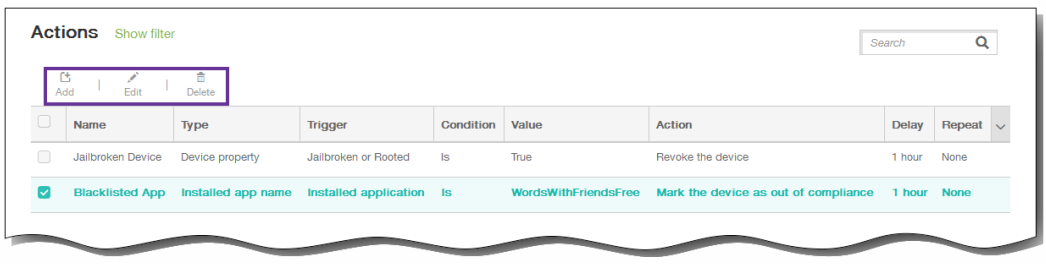
本主题介绍了如何在 XenMobile 中添加、编辑和过滤自动化操作。

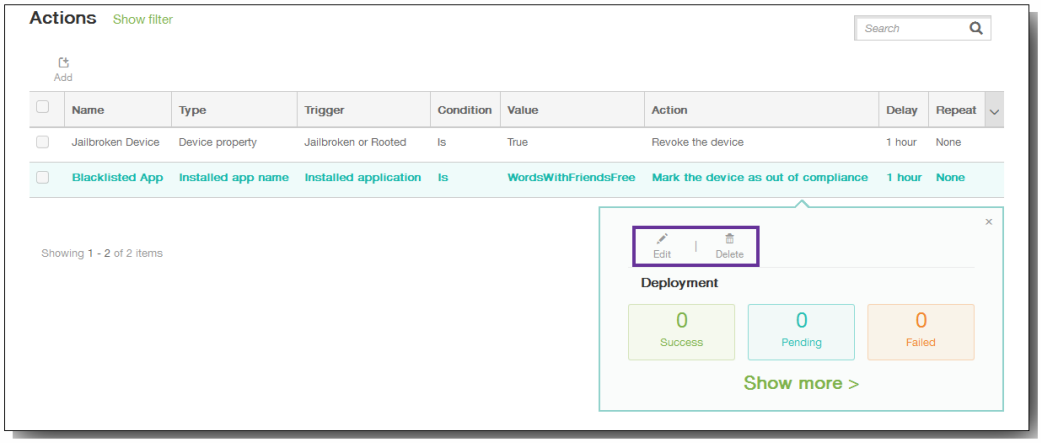
1. 在 XenMobile 控制台中，单击配置 > 操作。 此时将出现操作页面。



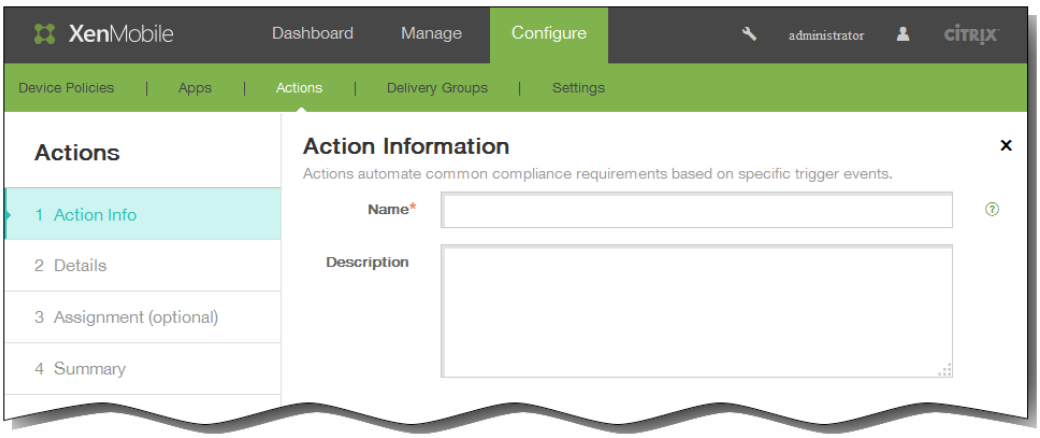
2. 在操作页面上，执行以下操作之一：
   - 单击添加以添加新操作。
   - 选择要编辑或删除的现有操作。单击要使用的选项。

     注意：如果选中某项操作旁边的复选框，选项菜单将显示在操作列表的上方；如果单击此列表的任何其他位置，选项菜单将显示在列表的右侧。



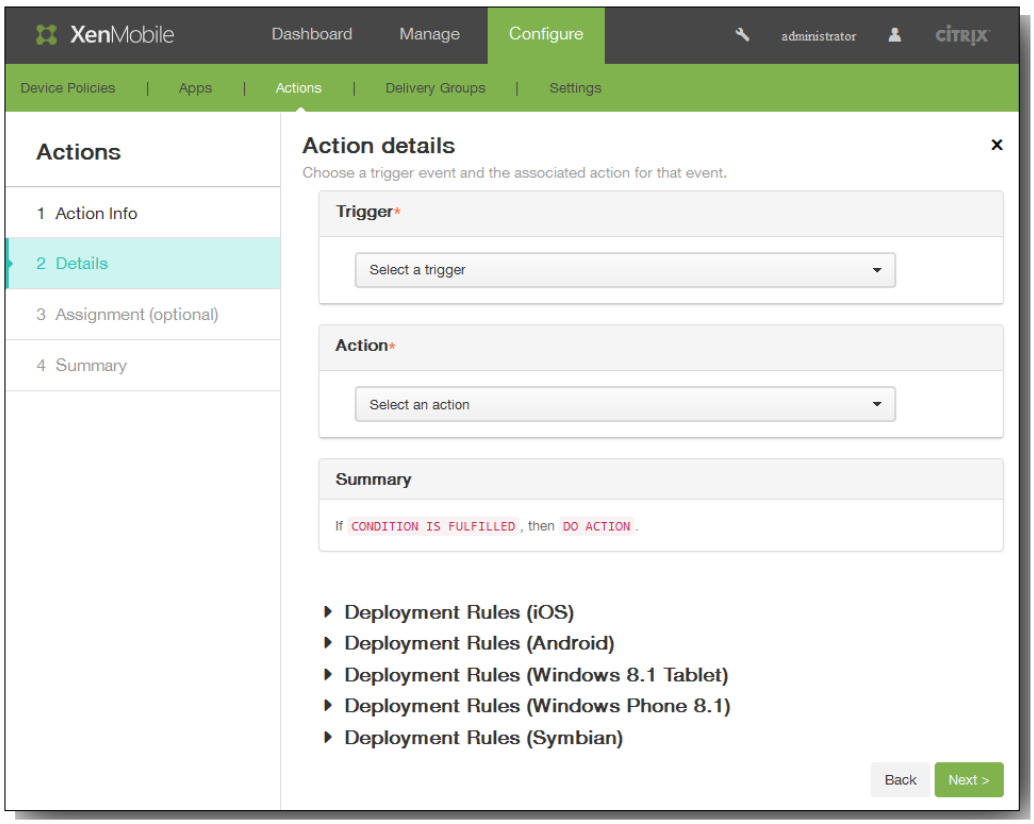


此时将显示操作信息页面。

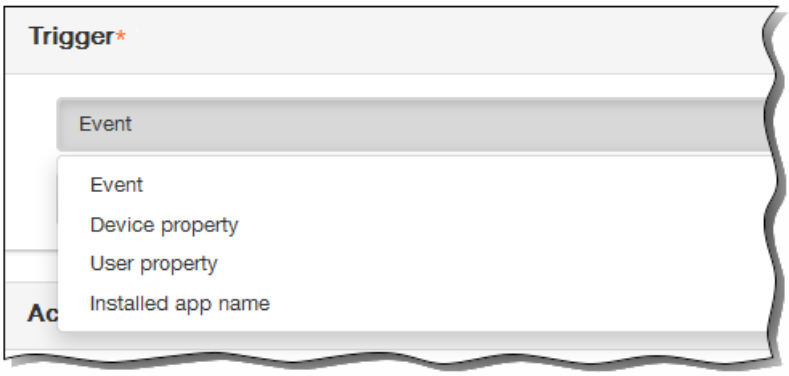


3. 在操作信息页面上，输入或修改以下信息：
   1. 名称：键入一个名称来唯一地标识操作。 此字段为必填字段。
   2. 说明：描述执行该操作的目的。
4. 单击下一步。 此时将显示操作详细信息页面。

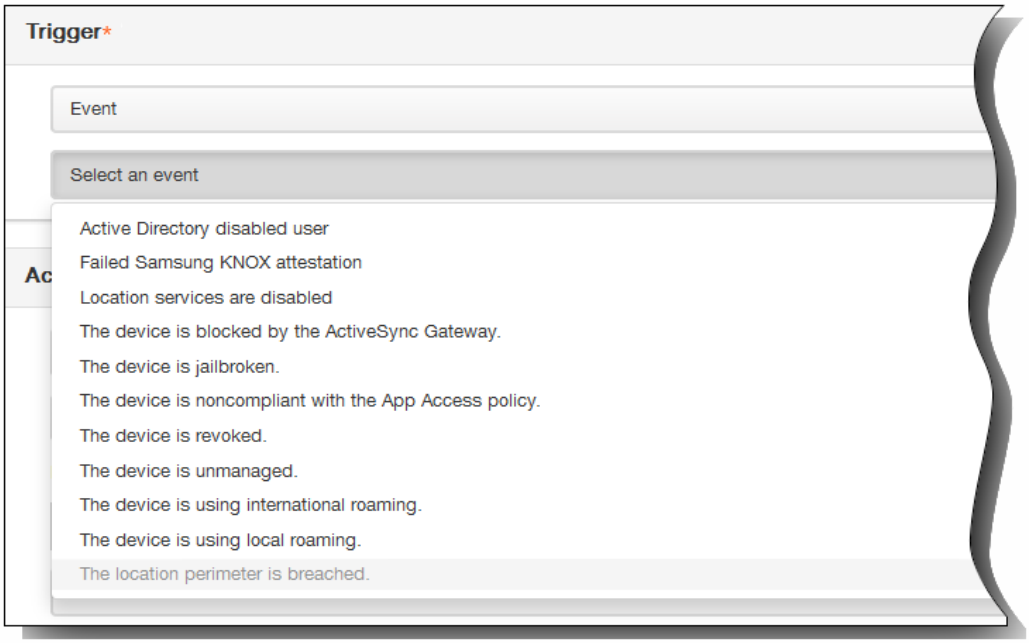
   注意：下面的示例显示如何设置事件触发器。如果选择其他触发器，生成的选项将与此处显示的选项有所不同。



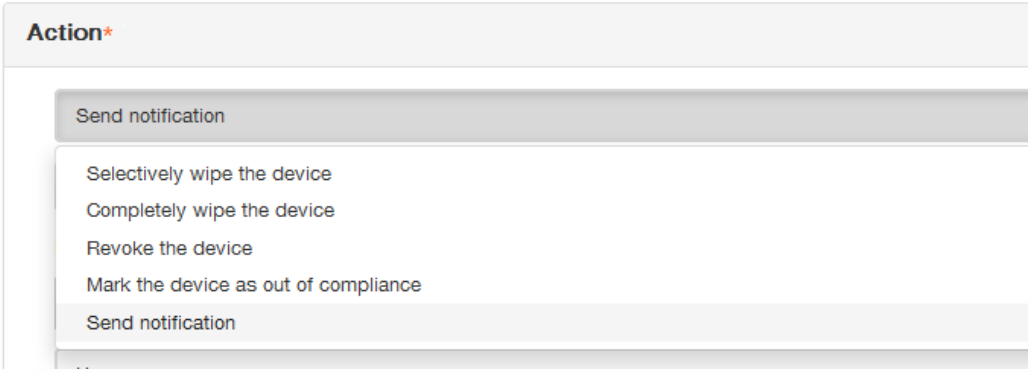
5. 在操作详细信息页面上，输入或修改以下信息：
   1. 在触发器列表中，单击适用于此操作的事件触发器类型。 每个触发器的含义如下所示：
      - 事件：对预定义的事件做出反应。
      - 设备属性：检查在 MDM 模式下收集的设备上的设备属性，并对其做出反应。
      - 用户属性：对用户属性做出反应，通常通过 Active Directory。
      - Installed app name（已安装的应用程序名称）：对正在安装的应用程序做出反应。要求在设备上启用应用程序清单策略。默认情况下，应用程序清单策略在所有平台上均处于启用状态。有关详细信息，请参阅添加应用程序清单设备策略。



   2. 在下一个列表中，单击对触发器的响应。

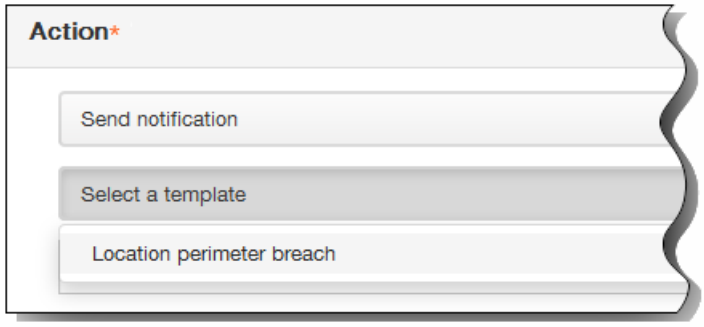


3. 在操作列表中，单击符合触发器条件时要执行的操作。 除发送通知之外，选择一个时间范围，让用户可以解决引起触发的问题。 如果在该时间范围内未解决此问题，将执行选定的操作。



此过程的其余部分介绍了如何发送通知操作。

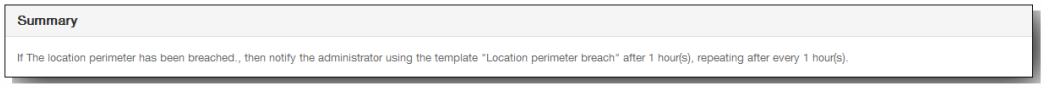
4. 在下一个列表中，选择用于通知的模板。 此时将显示与选定事件相关的通知模板。
注意：在可以通知用户之前，必须已在设置中为 SMTP 和 SMS 配置通知服务器，以便 XenMobile 可以发送消息，请参阅 XenMobile 中的通知。此外，请在继续操作前设置打算使用的通知模板。有关设置通知模板的详细信息，请参阅在 XenMobile 中创建或更新通知模板。



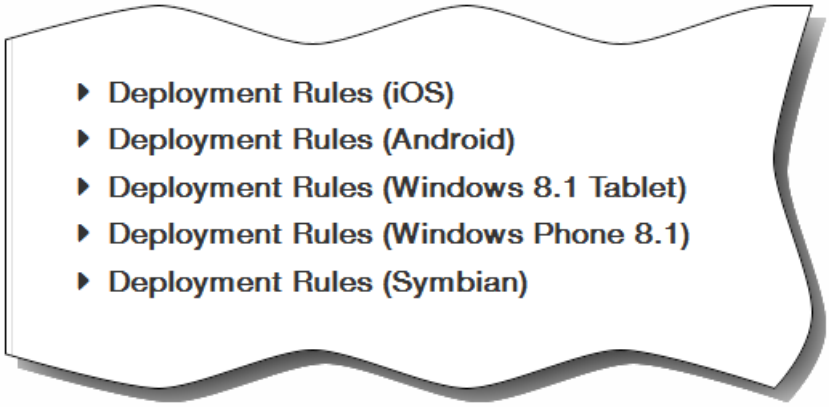
注意：选择模板后，可以通过单击预览通知消息预览通知。

5. 在以下字段中，设置延迟时间（以天、小时或分钟为单位）后再执行操作，并设置操作重复的时间间隔，直到用户解决触发问题。

6. 在摘要中，验证您是否已按预期创建自动化操作。

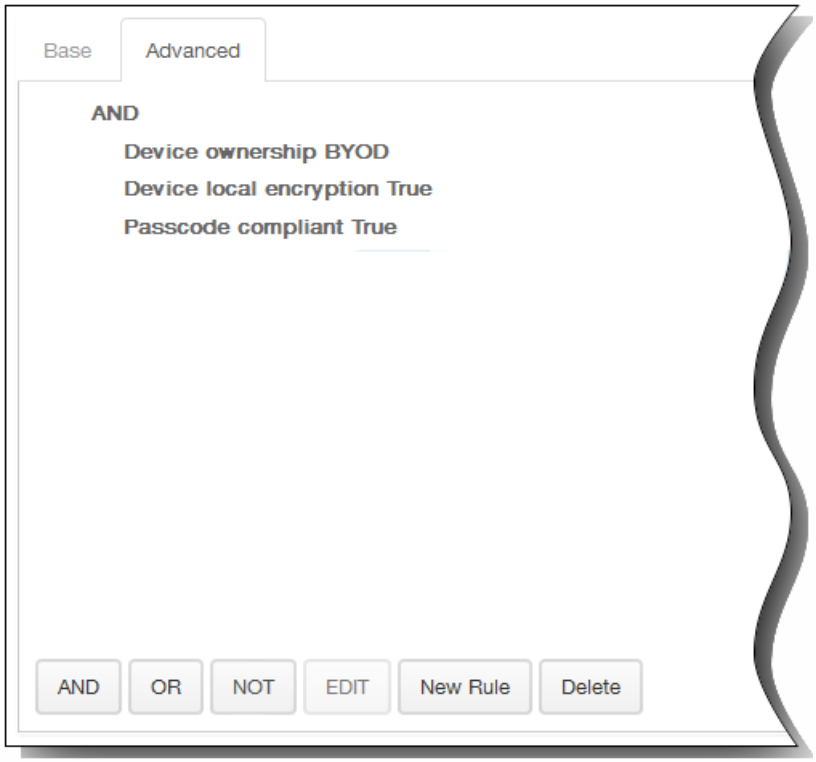


配置操作详细信息后，可以分别为以下每个平台配置部署规则：iOS、Android、Windows 8.1 Tablet、Windows Phone 8.1 和 Symbian。为此，针对您选择的每个平台执行步骤 6 到步骤 9。



6. 展开部署规则。 默认情况下将显示基础选项卡。

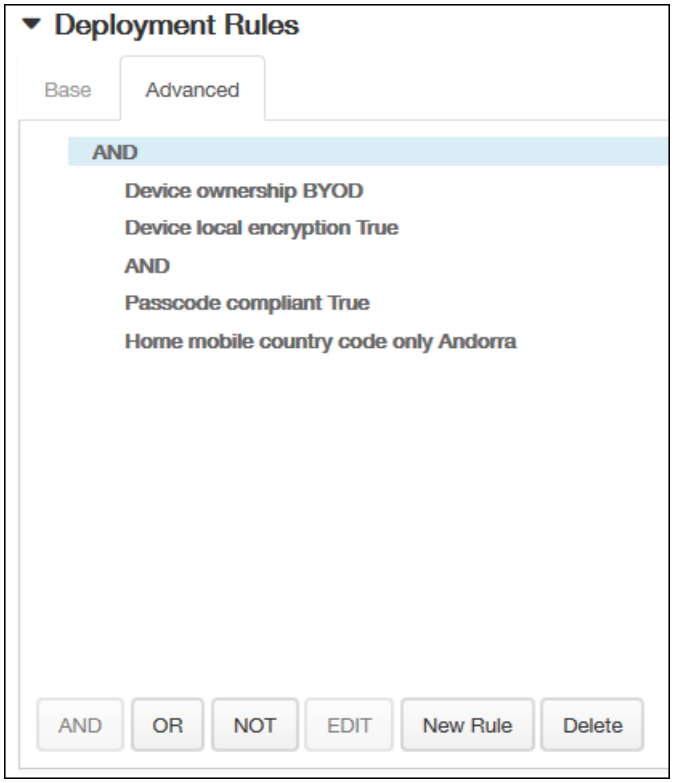
1. 在此列表中，单击选项以确定部署操作的时间。
    1. 可以选择在满足所有条件时部署操作，或在满足任意条件时部署操作。默认选项是全部。
    2. 单击新建规则以定义条件。
    3. 在列表中，单击条件，如设备所有权和 BYOD，如上图所示。
    4. 如果要添加更多条件，请再次单击新建规则。您可以添加任意多项条件。
2. 单击高级选项卡以使用布尔选项组合规则。



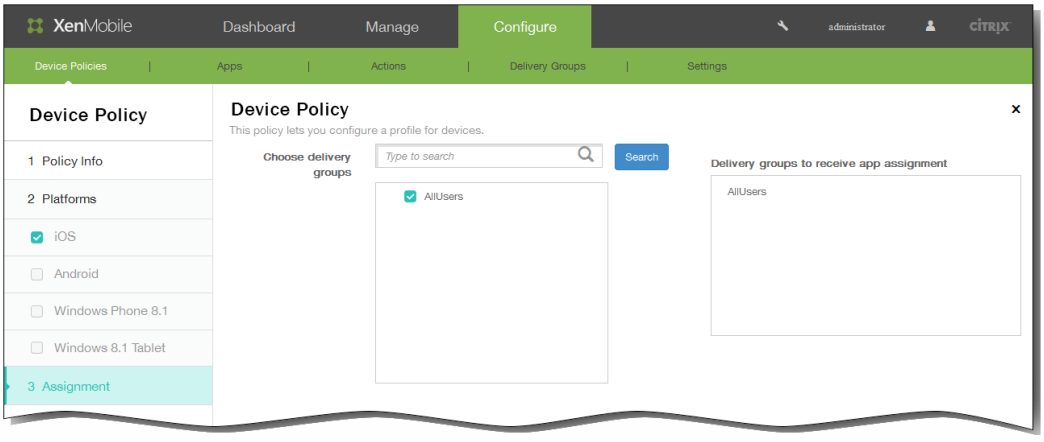
将显示您在基础选项卡上选择的条件。

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，设备必须兼容通行码，并且移动设备国家/地区代码不能仅为安道尔。

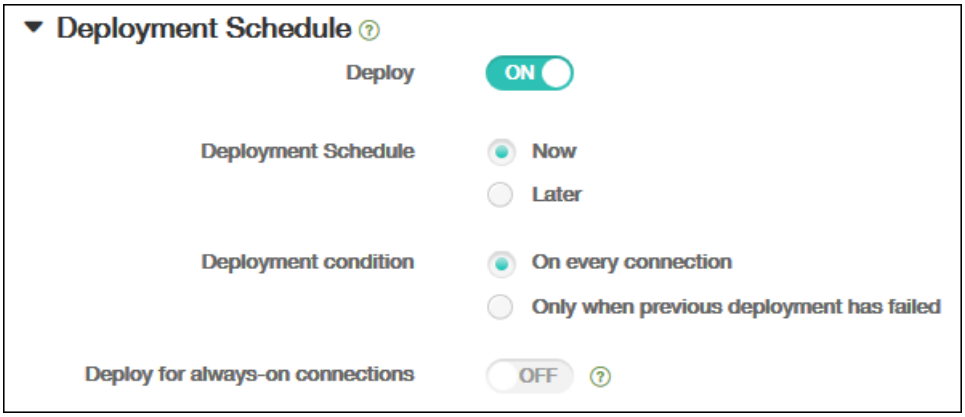


7. 针对该操作完成配置平台部署规则后，单击下一步。 此时将出现操作分配页面，您可以在其中将操作分配给一个或多个交付组。此步骤可选。
8. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。 选择的组显示在右侧用于接收应用程序分配的交付组列表中。

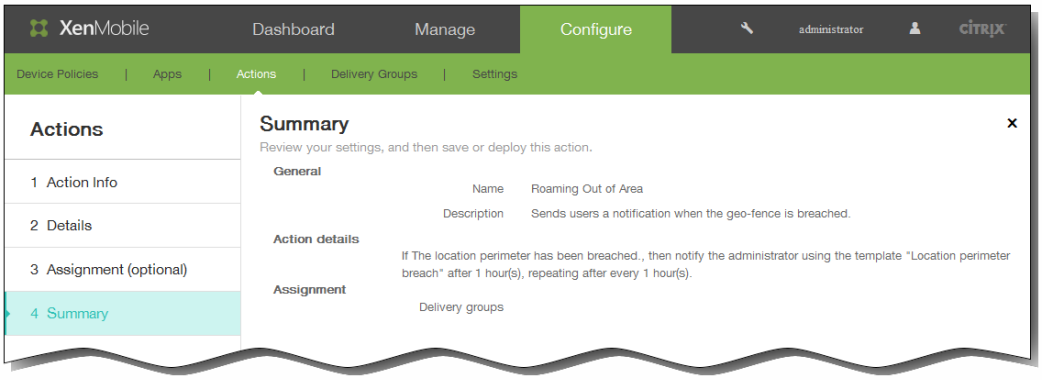


9. 展开部署计划，然后配置以下设置：
   1. 在部署旁边，单击开以计划部署，或单击关以阻止部署。 默认选项为开。 如果选择关，无需配置其他选项。
   2. 在部署计划旁边，单击立即或稍后。 默认选项为立即。
   3. 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
   4. 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。 默认选项为每次连接时。
   5. 在为始终启用的连接部署旁边，单击开或关。 默认选项为关。
      注意：已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。

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. 单击下一步。 此时将显示摘要页面，您可以在其中验证操作配置。



11. 单击保存以保存操作。

XenMobile 客户端设置

Apr 22, 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。

客户端属性参考

Aug 04, 2016

XenMobile 首选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）。 如果启用了 ENABLE_PASSWORD_CACHING，或者如果 XenMobile 使用证书身份验证，此设置将自动启用。

如果用户执行脱机身份验证，Worx PIN 将在本地验证，并且允许用户访问所请求的应用程序或内容。 如果用户执行联机身份验证，Worx PIN 或通行码将用于解锁 Active Directory 密码或证书，随后将发送后者以通过 XenMobile 执行身份验证。

可能的值：true 或 false

默认值：false

ENABLE_PASSWORD_CACHING

显示名称：启用用户密码缓存。

此键允许您在移动设备本地缓存用户的 Active Directory 密码。 当您将此键设置为 true 时，系统将提示用户设置 Worx PIN 或通行码。 当您将此键设置为 true 时，必须将 ENABLE_PASSCODE_AUTH 键设置为 true。

可能的值：true 或 false

默认值：false

ENCRYPT_SECRETS_USING_PASSCODE

显示名称：使用通行码加密机密

此键允许将机密数据存储在移动设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串。 此配置键允许使用强加密的密钥，但还会添加用户熵（用户生成的只有自己知道的随机 PIN 码）。

Citrix 建议您启用此键以帮助提高用户设备的安全性。

注意：启用此键将影响用户体验，具体表现为会出现过多要求输入 Worx PIN 的身份验证提示。

可能的值：true 或 false

默认值：false

PASSCODE_TYPE

显示名称：Worx PIN 类型

此键定义用户能够定义数字型 Worx PIN 还是字母数字型 Worx 通行码。 选择“数字”时，用户只能定义数字型 Worx PIN。 选择“字母数字”时，用户可以为 Worx 通行码使用字母和数字的组合。

注意：更改此设置时，系统将在下次提示用户进行身份验证时提示其设置新 Worx PIN 或通行码。

可能的值：数字或字母数字

默认值：数字

PASSCODE_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。 如果更改此设置，用户下次重置其 Worx PIN 或通行码时将设置新值。

可能的值：1-99

默认值：5

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且之后访问应用程序不会提示输入 Worx PIN 或通行码的时间（单位为分钟）。 要为 MDX 应用程序启用此设置，必须将应用程序通行码设置设为开。 如果应用程序通行码设置设为关，用户将被重定向到 Worx Home 以执行完全身份验证。 更改此设置时，该值将在系统下次提示用户进行身份验证时生效。

注意：在 iOS 上，非活动计时器也将管理对 Worx Home 的访问，而不仅仅是对 MDX 应用程序的访问。

可能的值：任意正整数

默认值：15

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

此键启用或禁用使用适用于 Worx 应用程序的 Crashlytics 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并上载日志的功能。 将为 Worx Home 和安装的所有 MDX 应用程序禁用日志记录功能。 用户无法从“支持”页面发送任何应用程序的日志；即使通过显示的电子邮件撰写对话框，也无法附加日志，但会添加指出日志记录功能被禁用的消息。 除了在用户设备上产生的影响，您也无法在 XenMobile 控制台中修改 Worx Home 和 MDX 应用程序的日志设置。

将此项设置为 True 时，Worx Home 将“阻止应用程序日志”设置为 True，以确保在应用新策略时 MDX 应用程序停止记录日志。

可能的值：true 或 false

默认值：false（不禁用日志记录）

创建适用于 iOS 设备的自定义 Worx Store 品牌设计

Aug 04, 2016

可以设置应用程序在应用商店中的显示方式并添加徽标以在移动设备上设计适用于 iOS 和 Android 的 Worx Home 和 WorxStore 的外观方案。

注意：开始之前，请确保您的自定义图片已准备就绪并且可供访问。

- 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，需要创建一个部署软件包并部署该软件包。

创建 Worx Home 和 GoToAssist 支持选项

Oct 22, 2015

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 文字消息标记
    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。

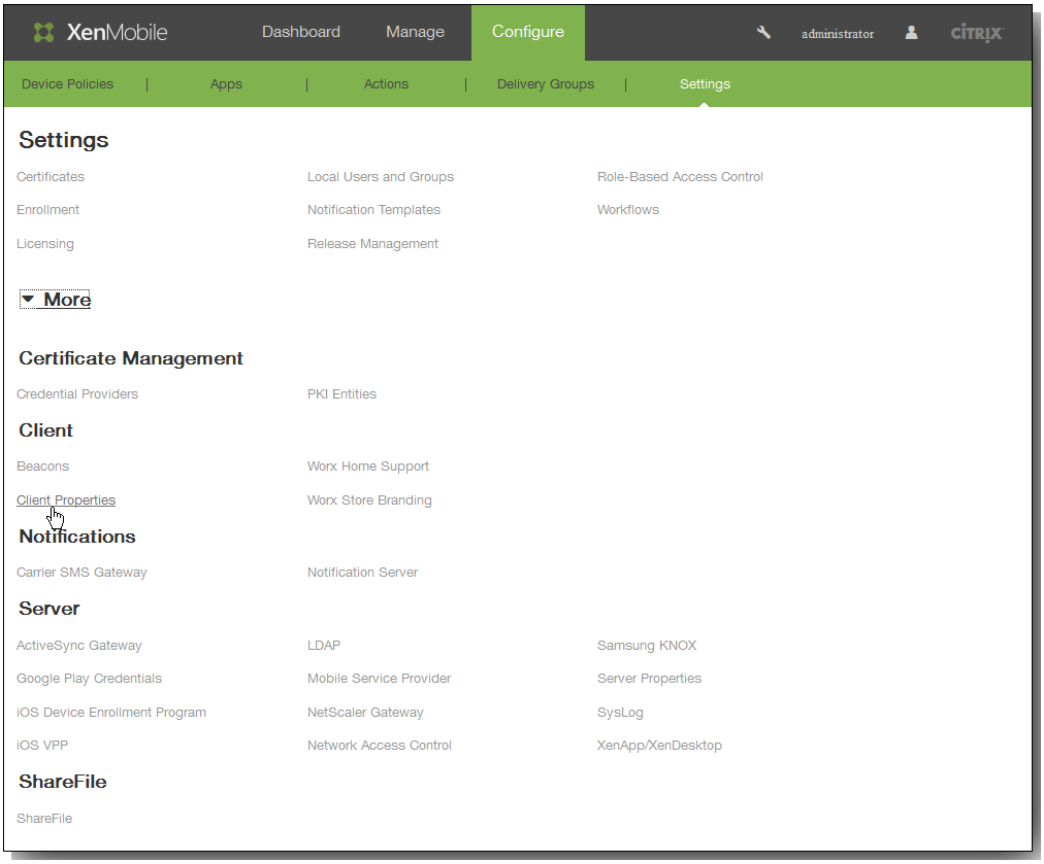
添加、编辑或删除客户端属性

Oct 22, 2015

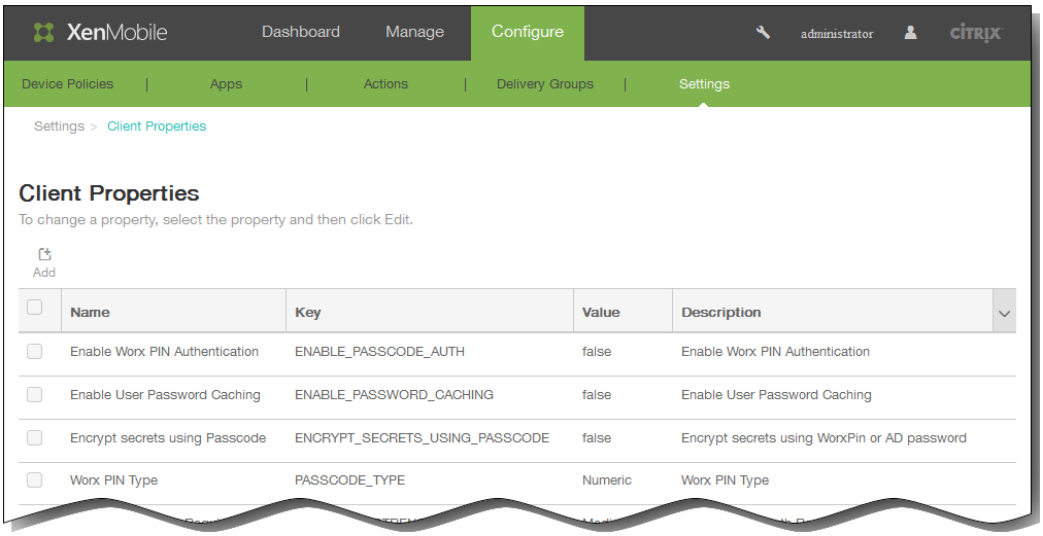
客户端属性包含用户设备上直接提供给 Worx Home 的信息。这些属性用于配置高级设置，如 Worx PIN。从 Citrix 技术支持获取客户端属性。

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。

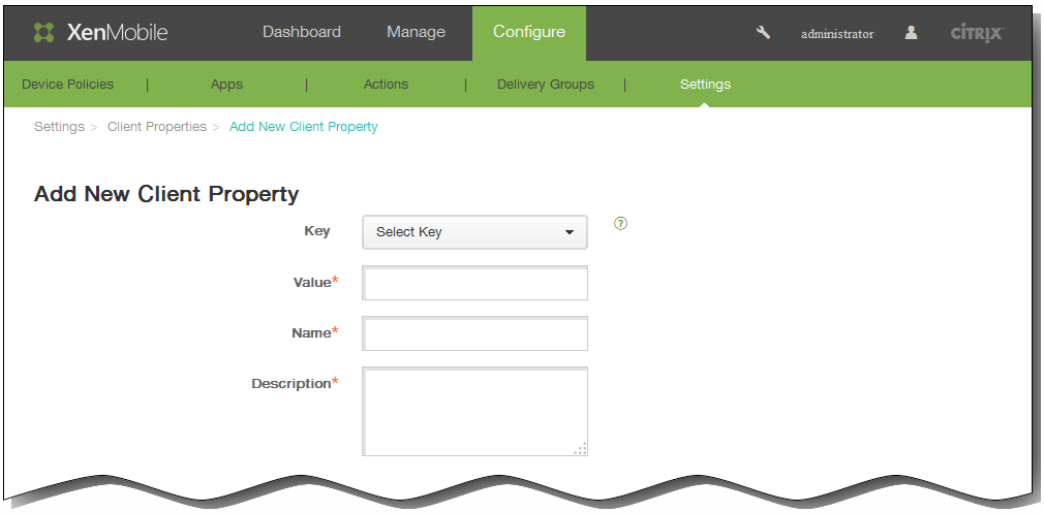


此时将显示客户端属性页面。可以从此页面添加、编辑和删除客户端属性。



添加客户端属性

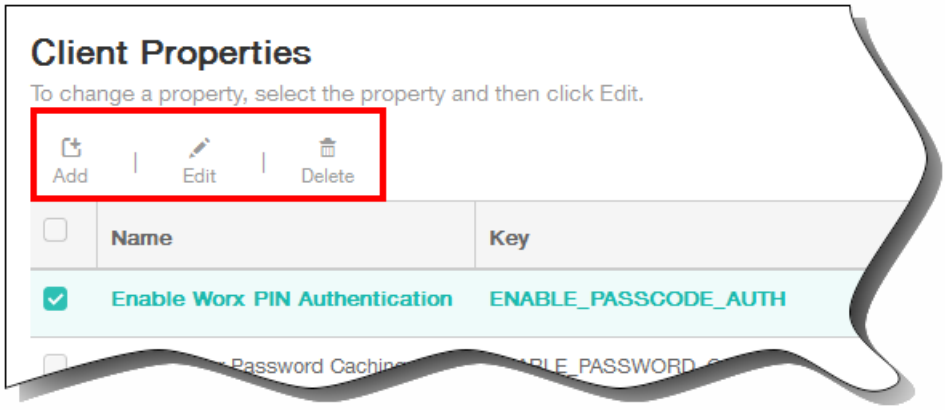
1. 在客户端属性页面中，单击添加。 此时将显示添加新客户端属性页面。

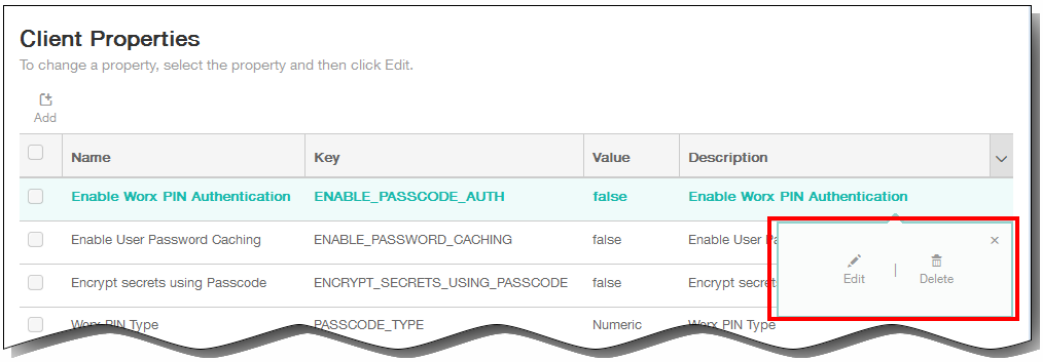


2. 在添加新客户端属性页面中，输入以下信息：
   注意：所有字段均为必填字段。
   1. 键：在列表中，单击要添加的属性键。
      重要：执行任何更改或请求特殊键以进行更改时请联系 Citrix 技术支持。
   2. 值：输入选定的属性值。
   3. 名称：输入属性的名称。
   4. 说明：输入属性的说明。

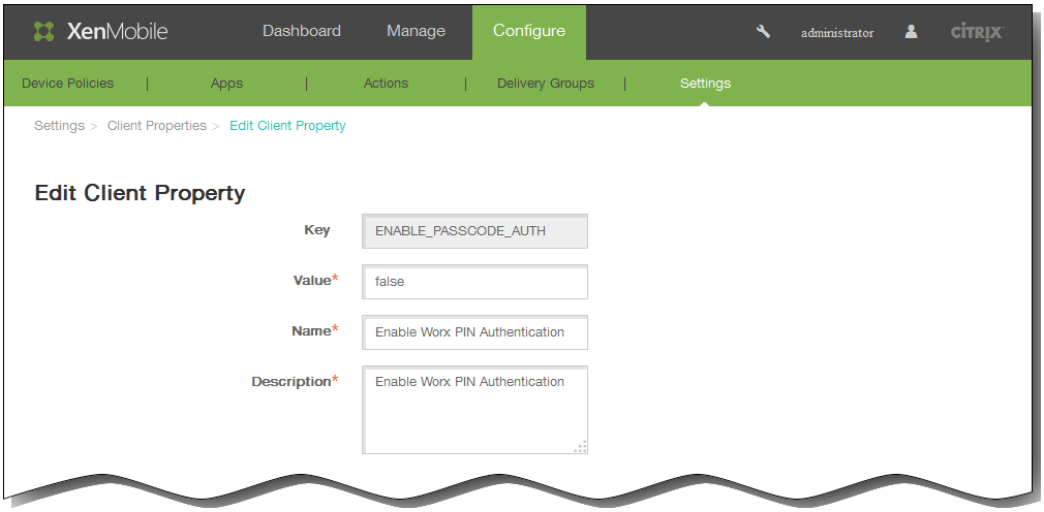
编辑客户端属性

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。

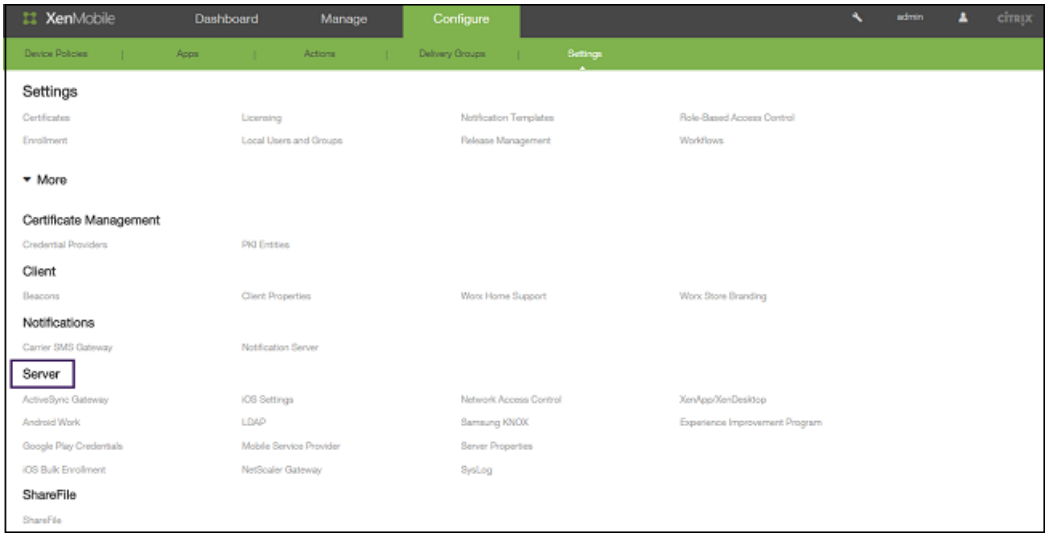
XenMobile 服务器设置

Apr 22, 2016

在 XenMobile Web 控制台中配置的 XenMobile 服务器设置包括：

- ActiveSync Gateway
- Android for Work
- Google Play 凭据
- iOS 批量注册
- iOS 设置
- LDAP
- 移动服务提供商
- NetScaler Gateway
- 网络访问控制
- Samsung KNOX
- 服务器属性
- SysLog
- XenApp/XenDesktop
- 体验改善计划

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

Apr 22, 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。

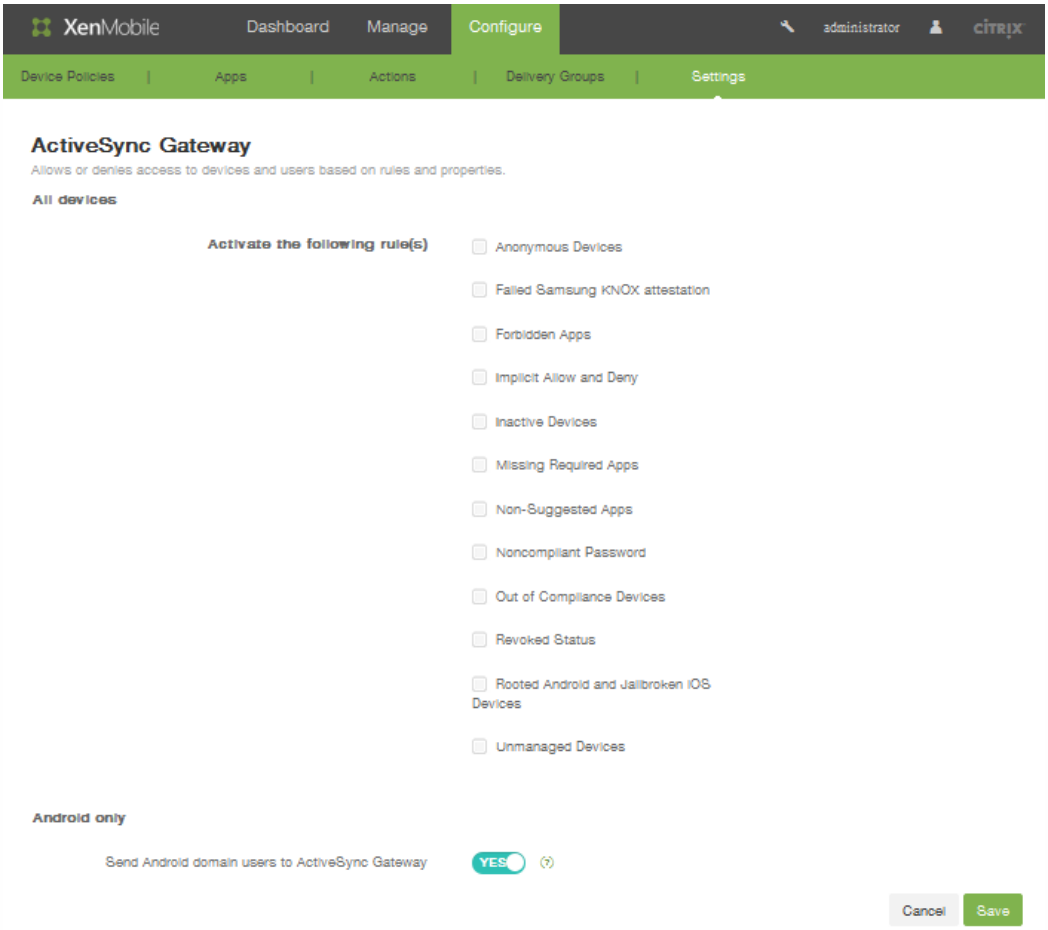
已获得 root 权限的 Android 设备和已越狱的 iOS 设备：检查 Android 设备或 iOS 设备是否已越狱。

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

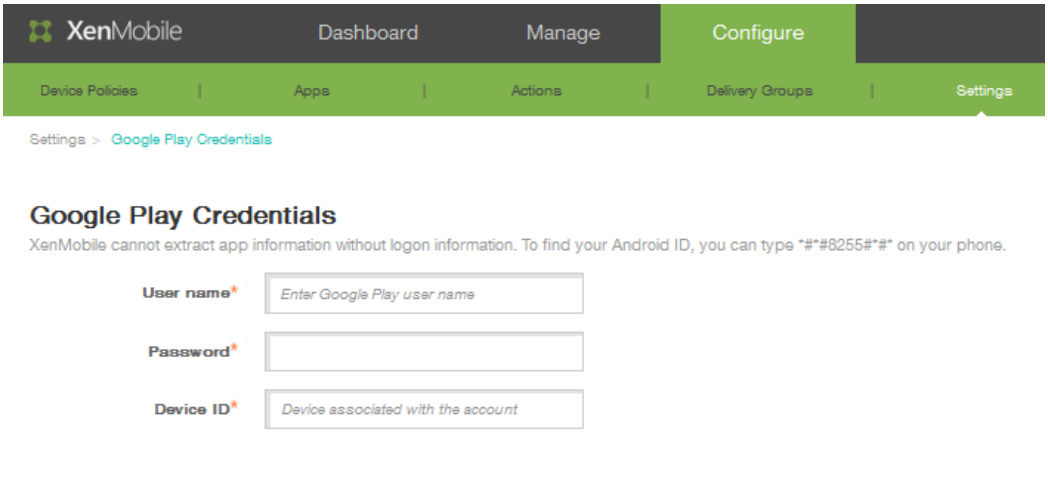
Apr 22, 2016

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。



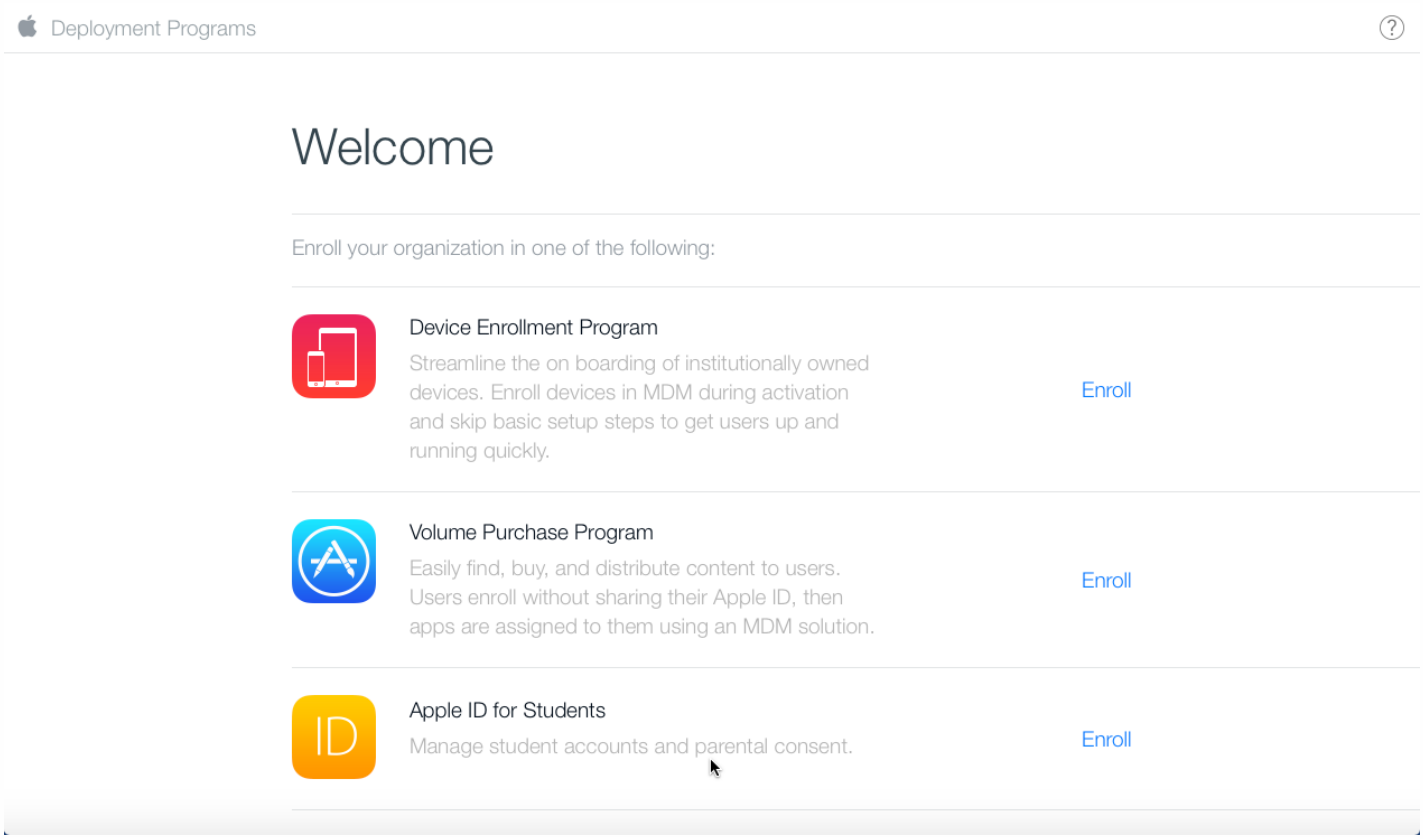
2. 在用户名中，输入与 Google Play 帐户关联的名称。
3. 在密码中，输入用户密码。
4. 在设备 ID 中，输入 Android ID。
   在电话上输入 *#*#8255#*#* 以确定 Android ID。
5. 单击保存。

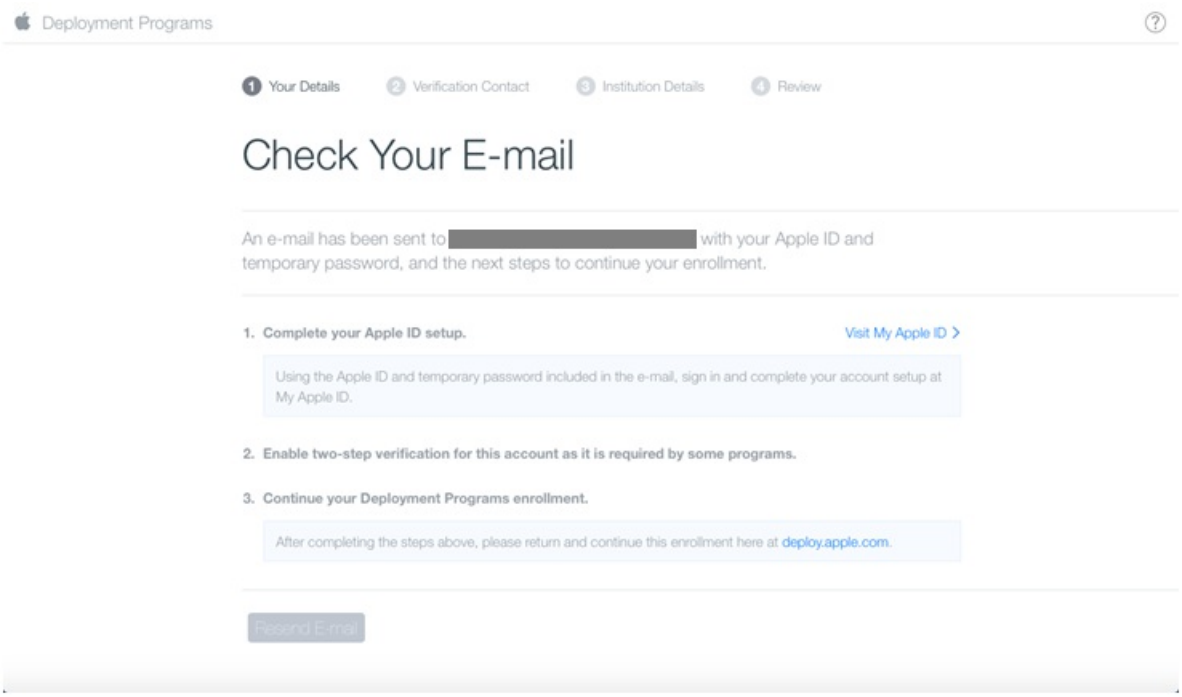
iOS Device Enrollment Program

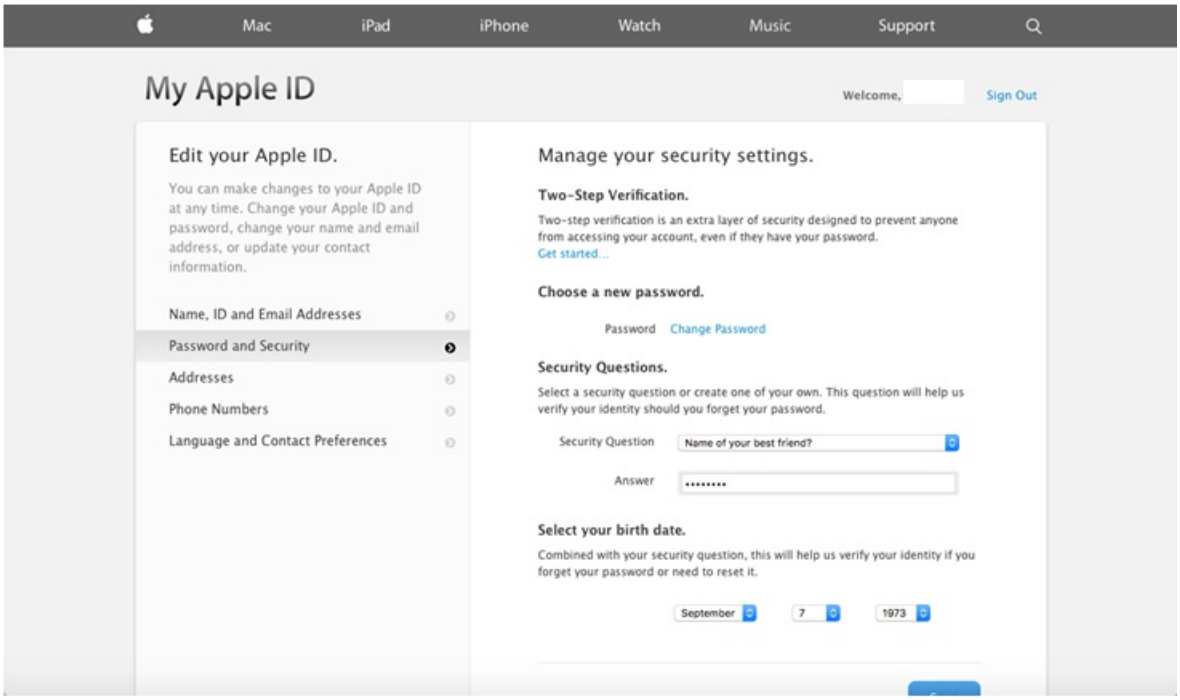
通过 Apple DEP 部署 iOS 设备

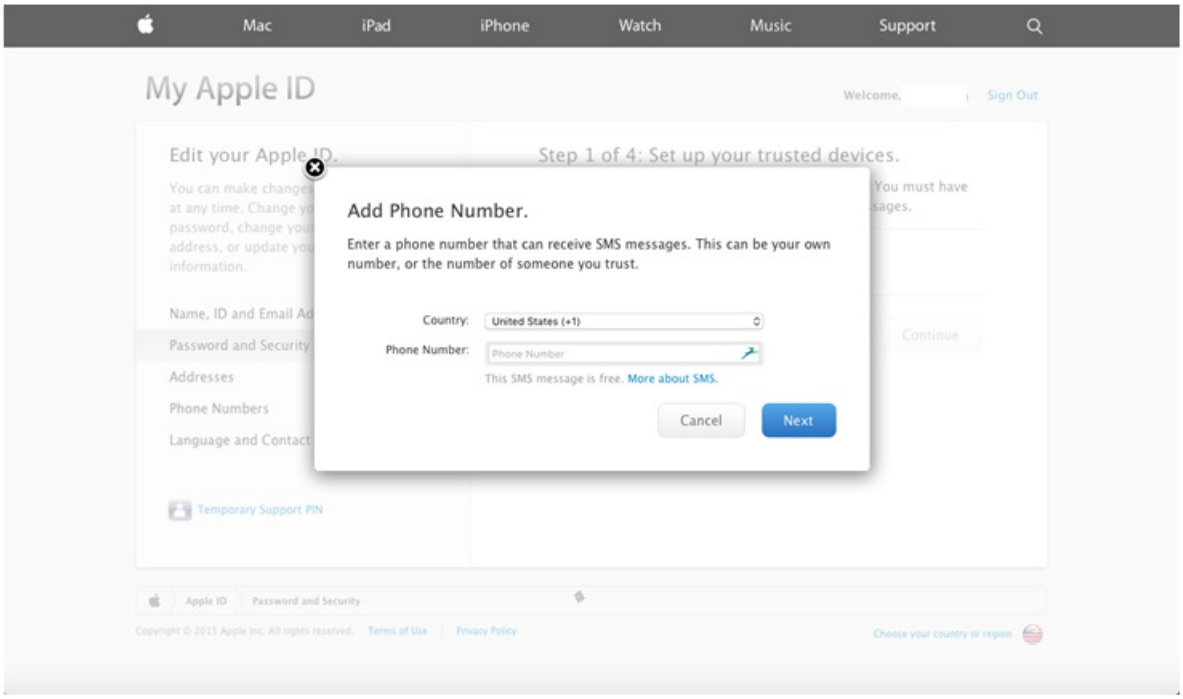
-
-
-
-

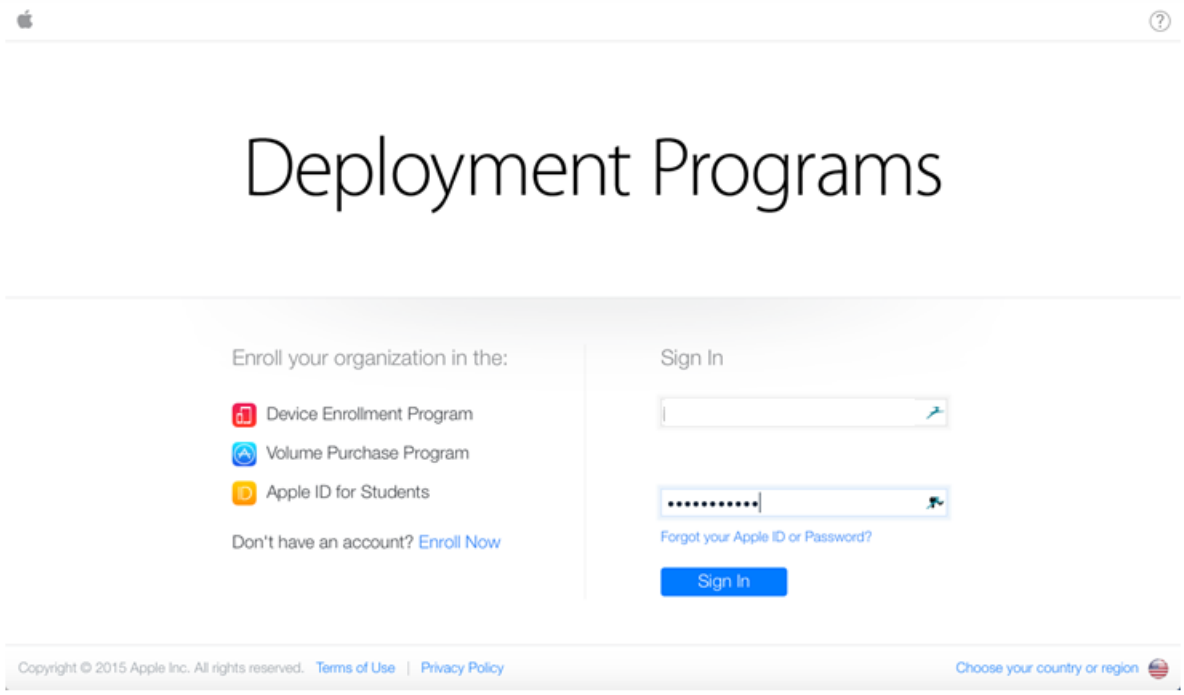
申请 Apple DEP 帐户

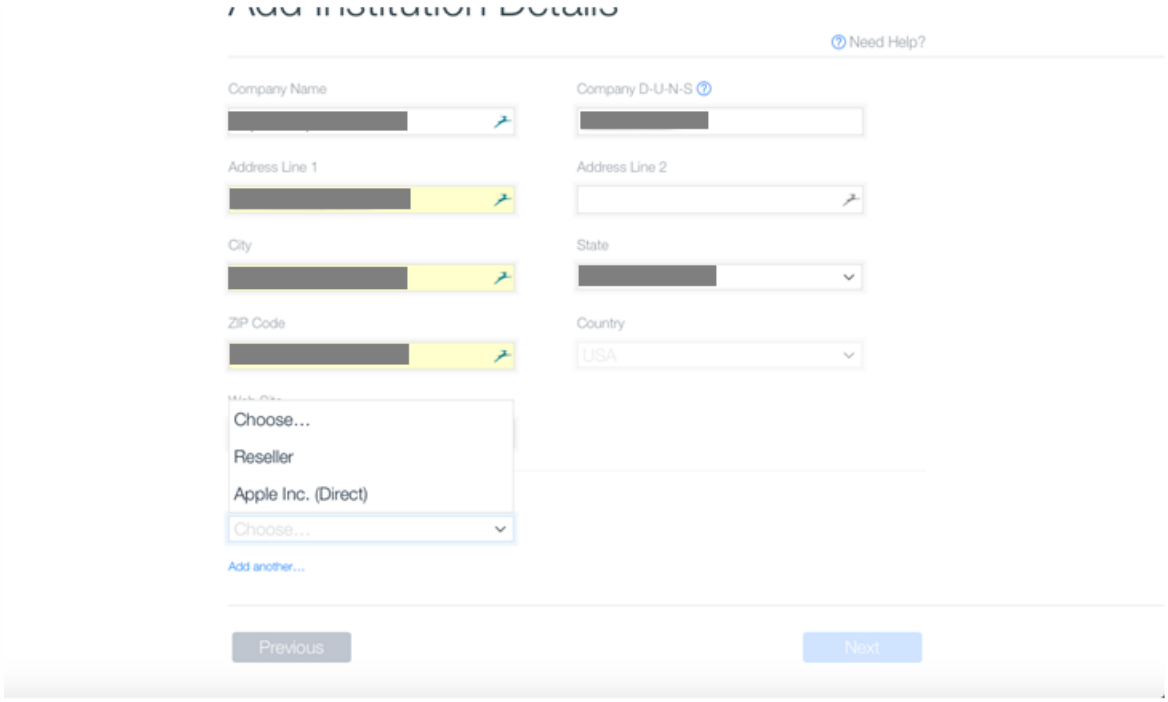


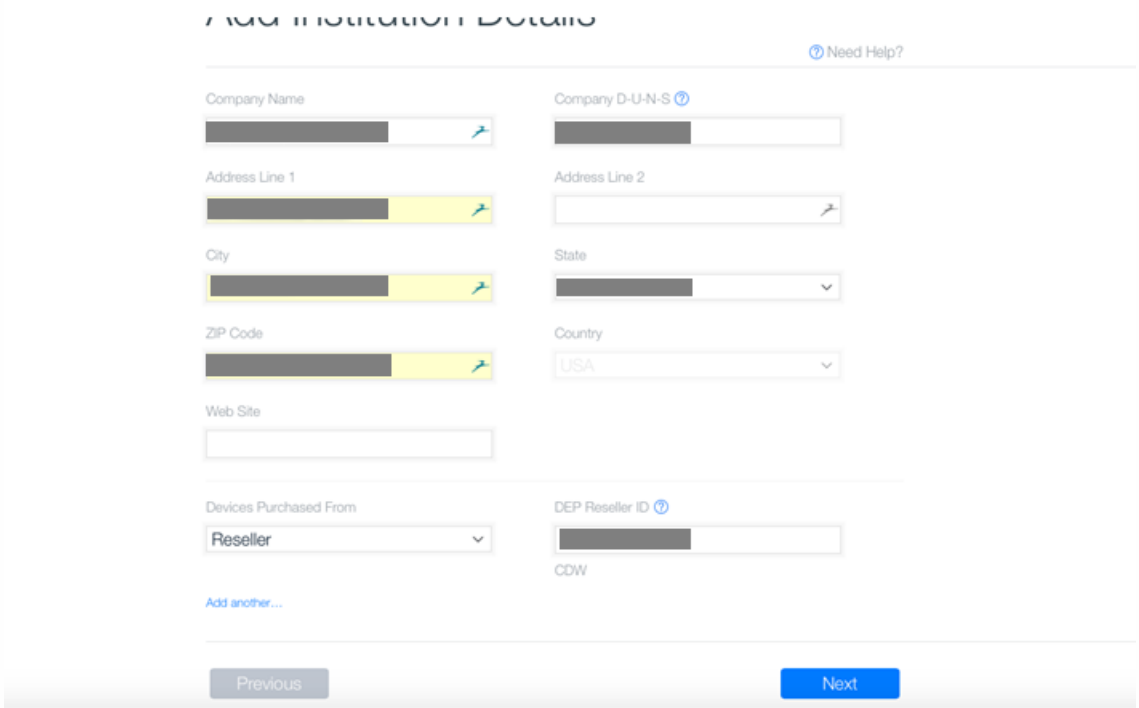


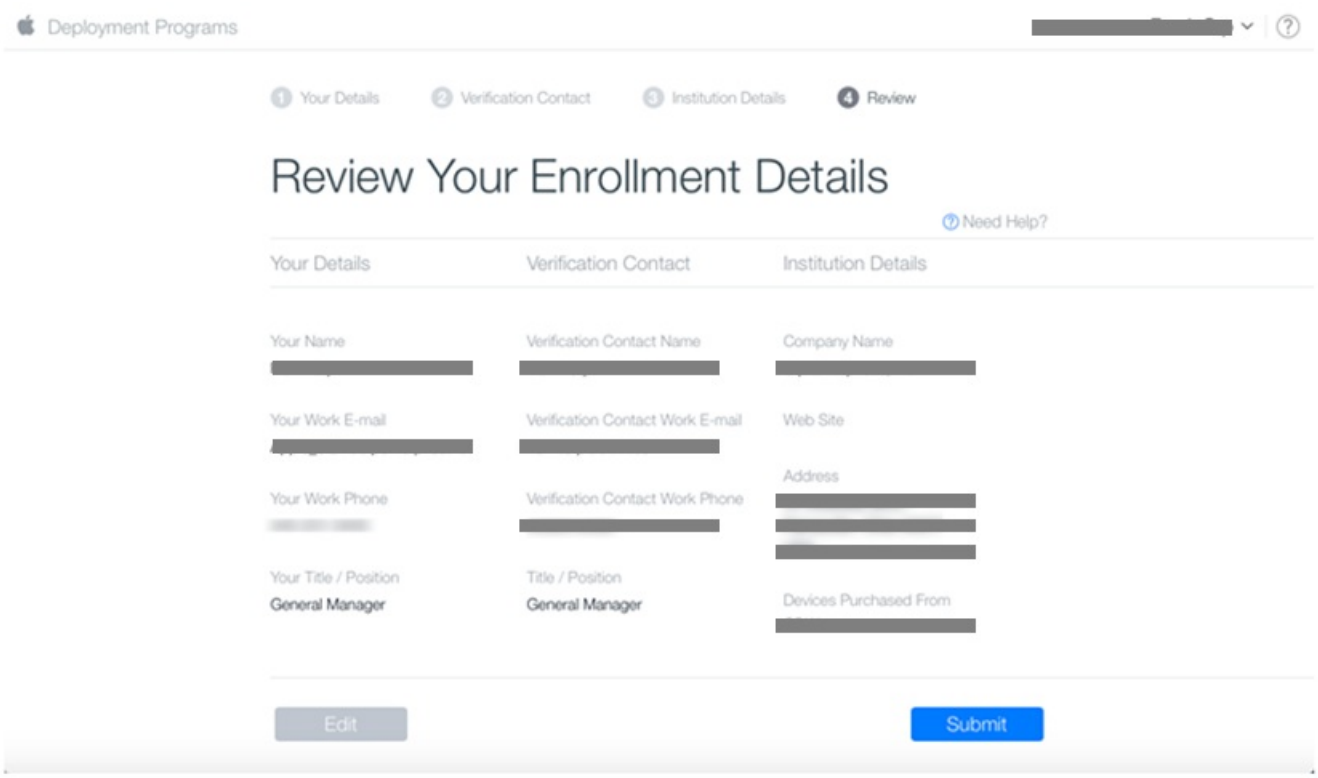


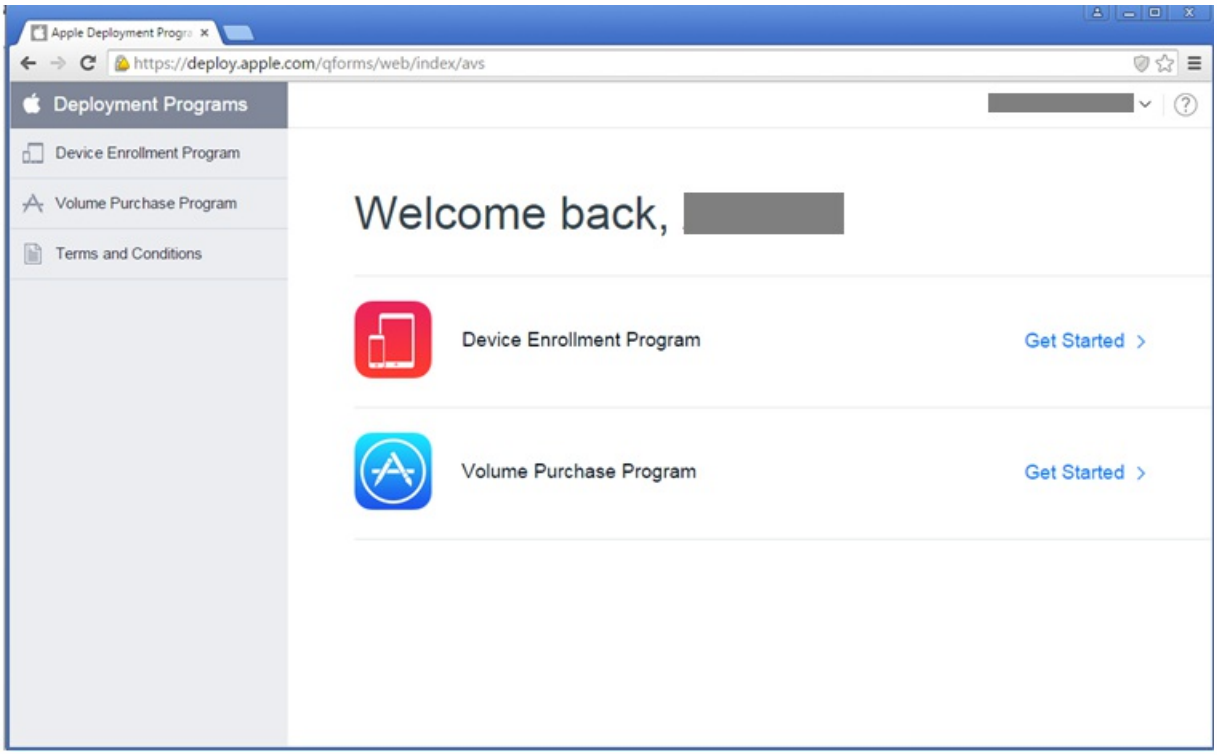




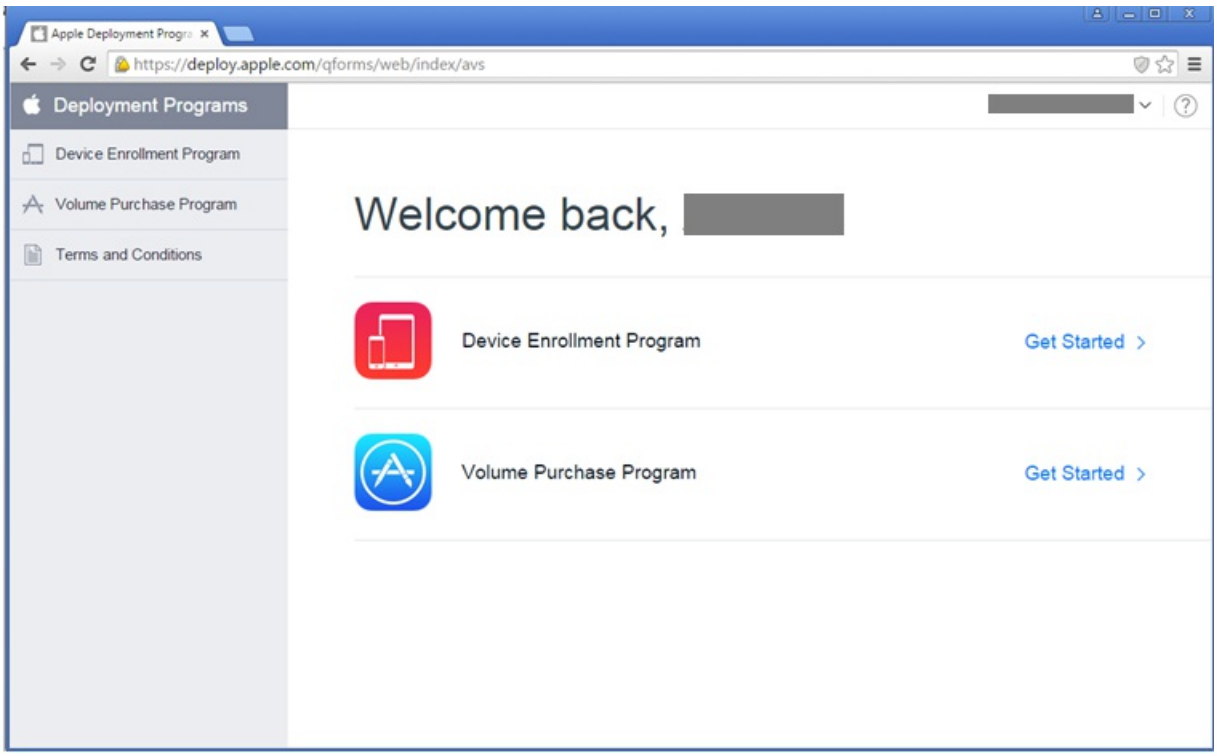


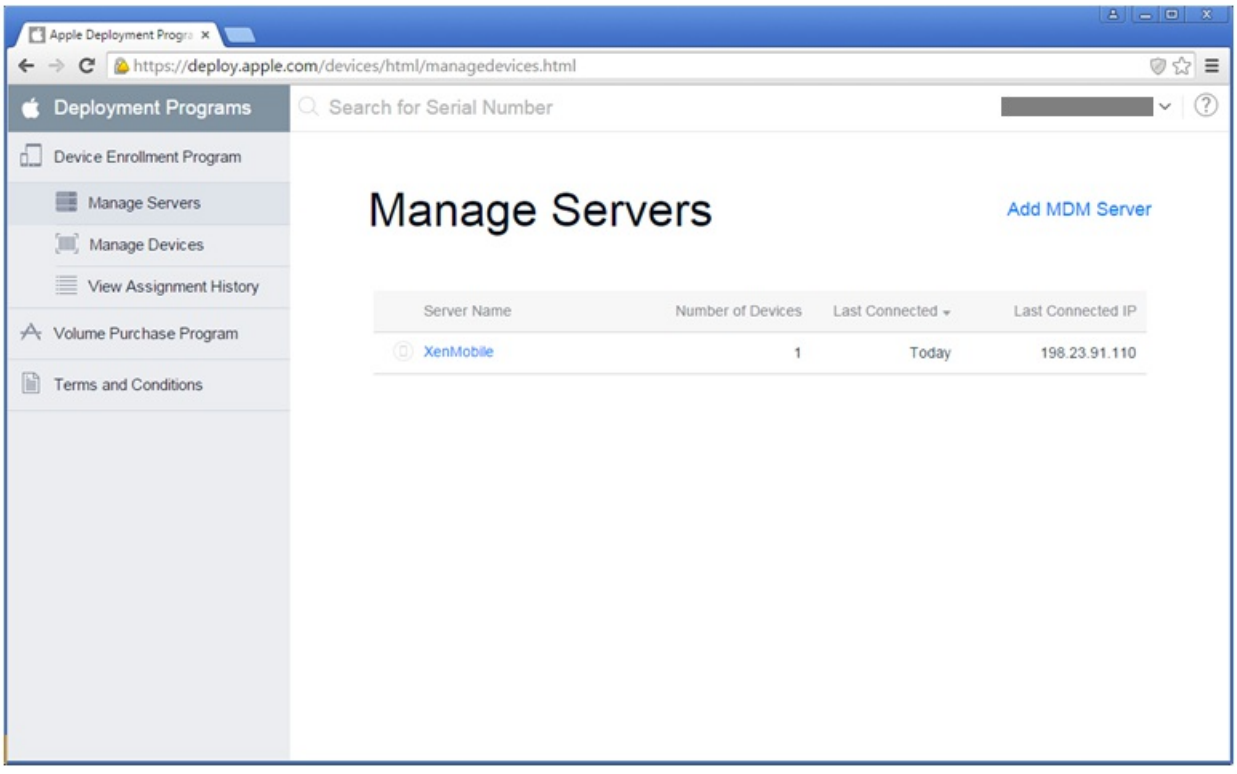


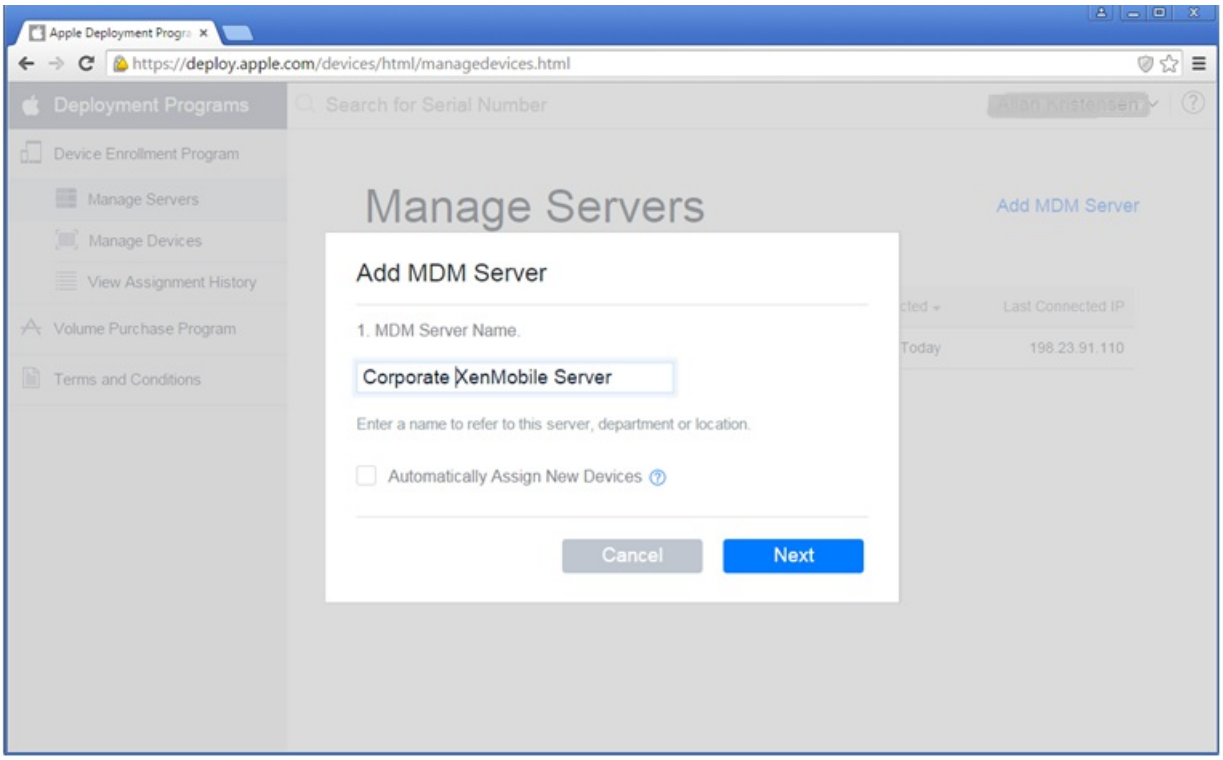


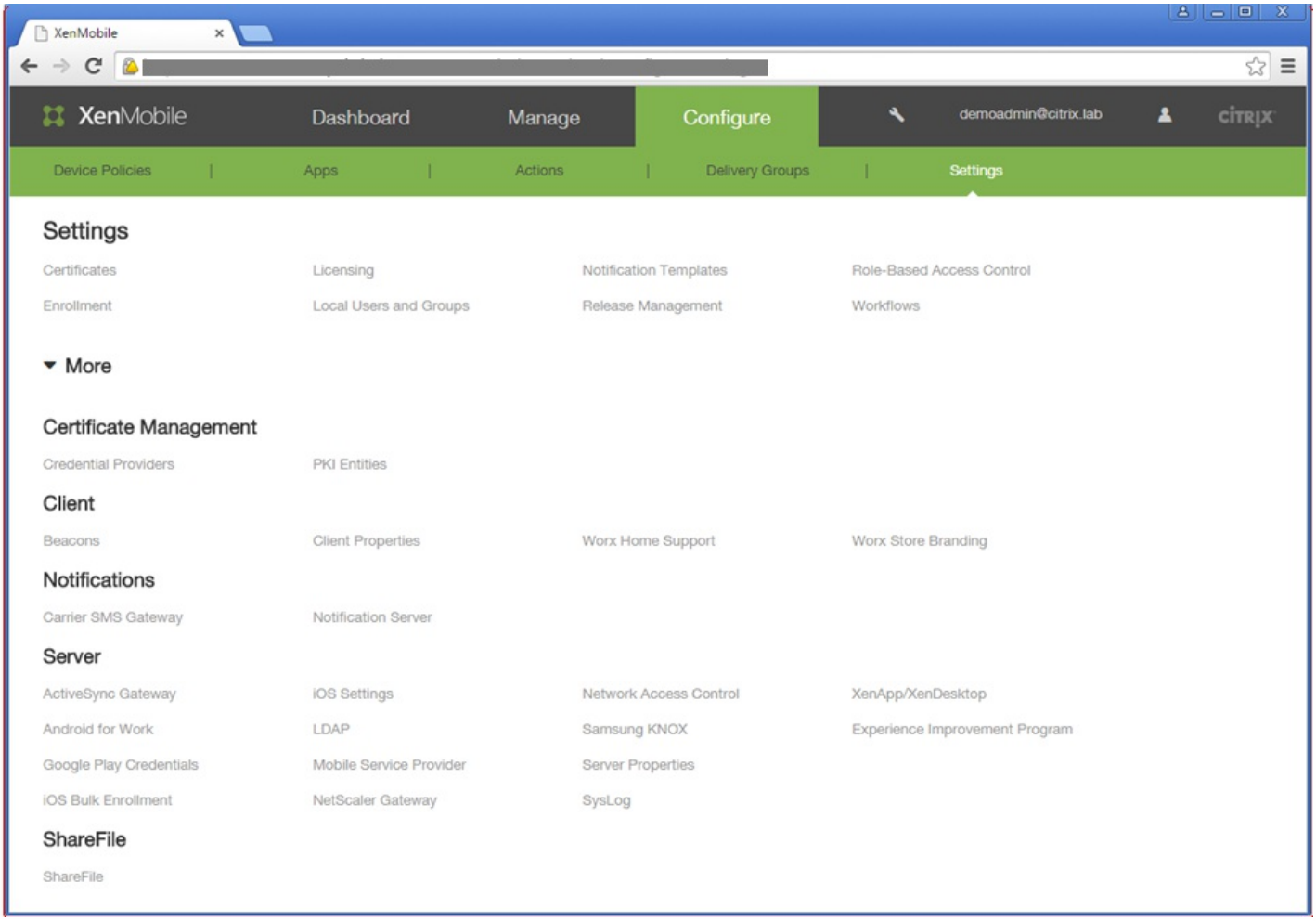


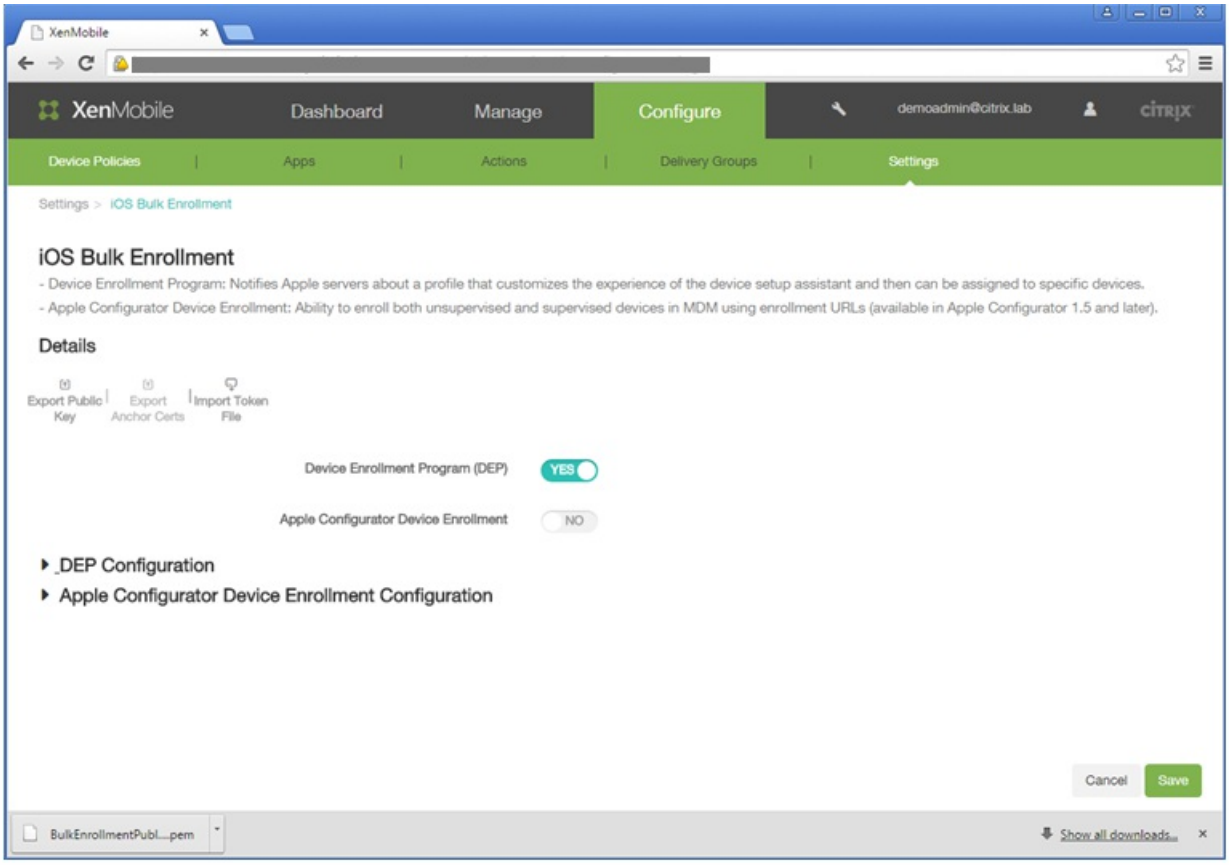
将 Apple DEP 帐户与 XenMobile 相集成

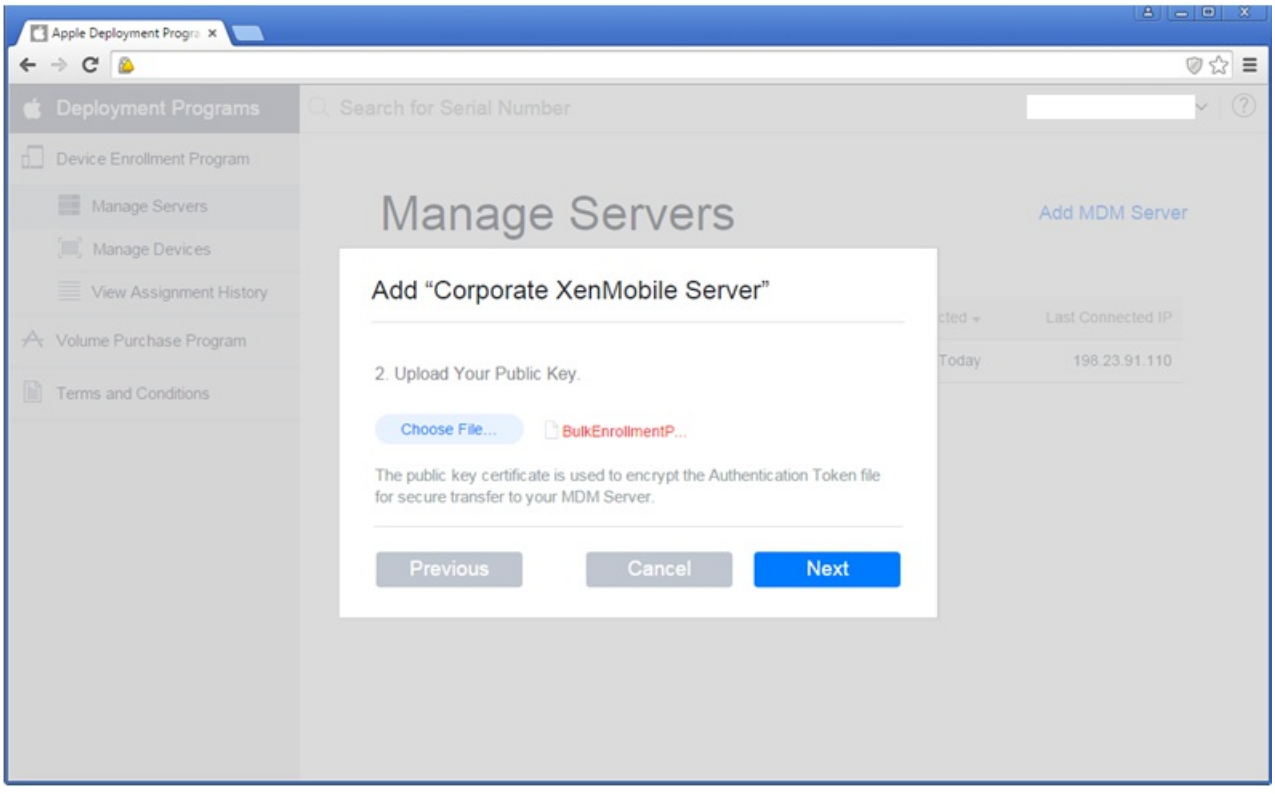


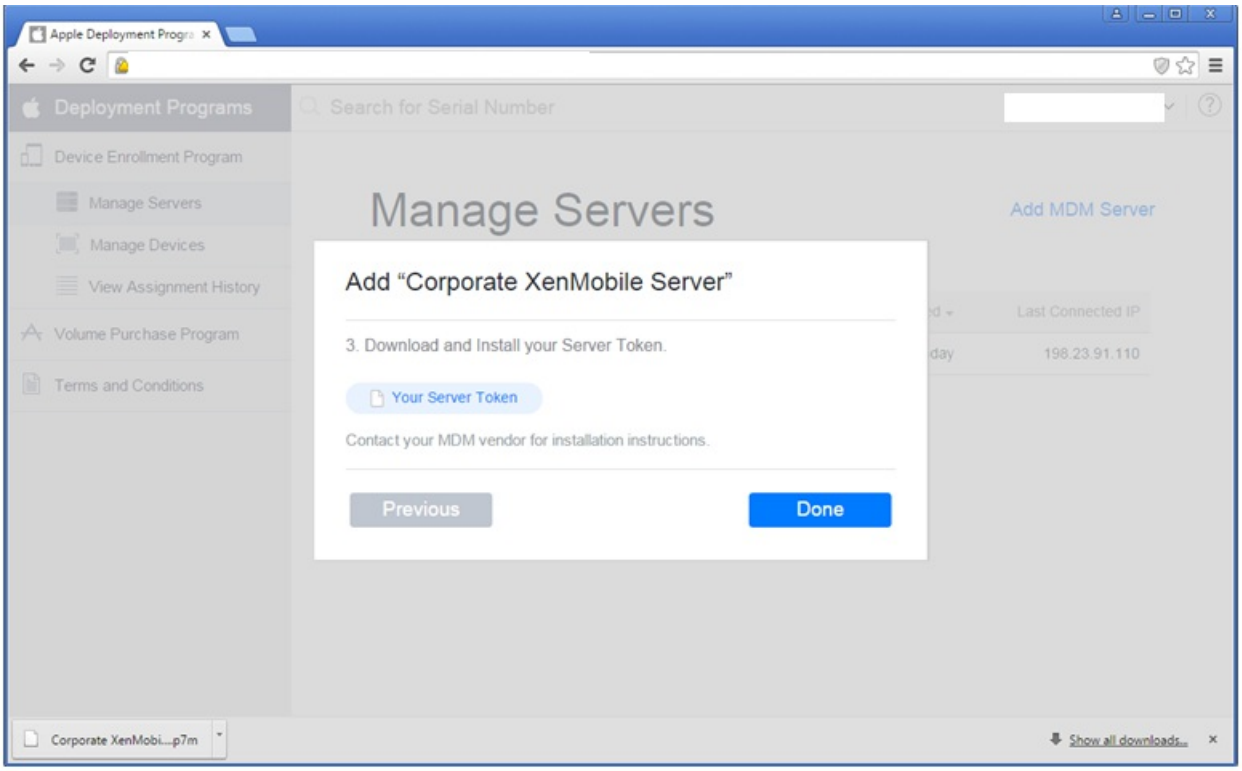


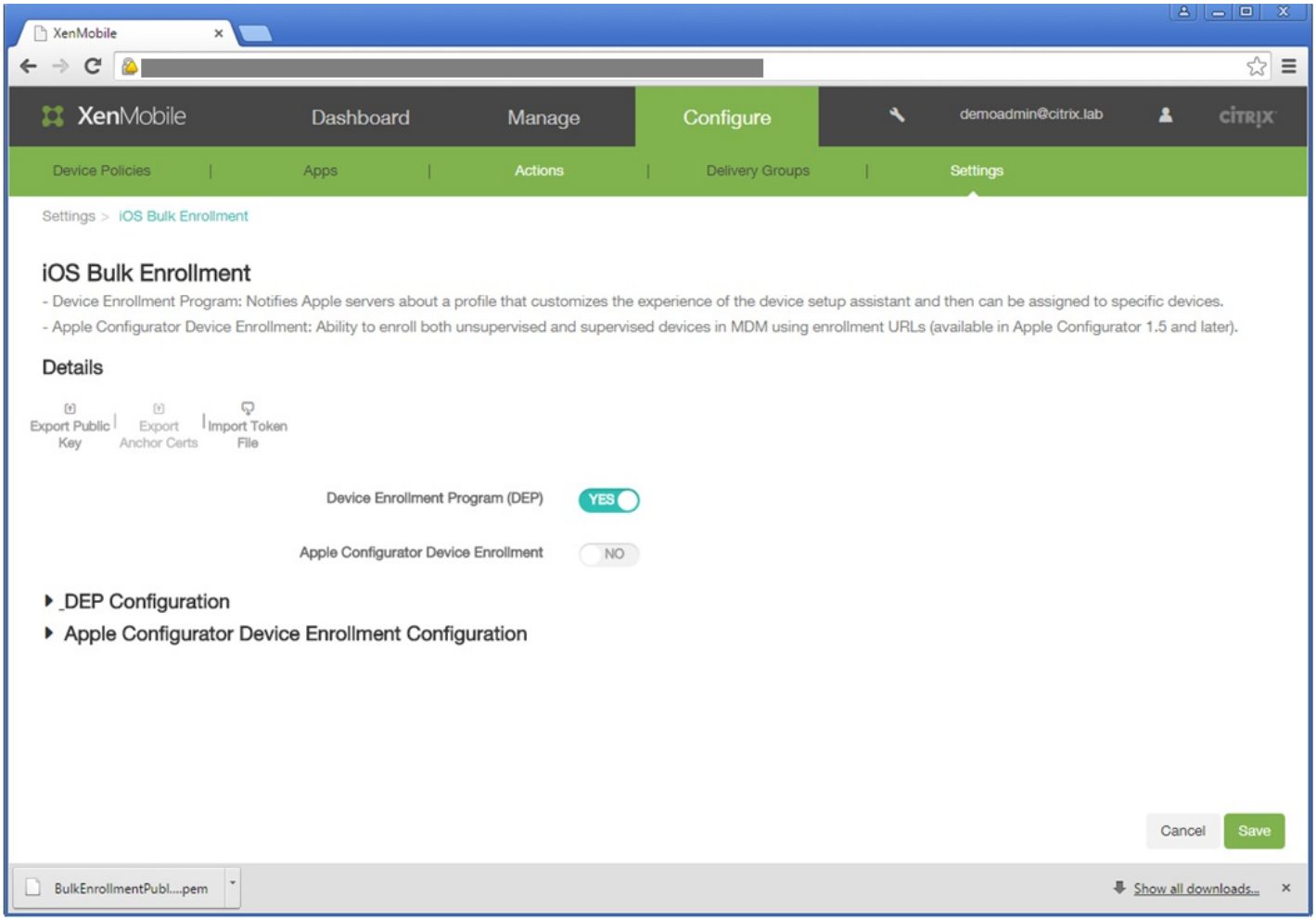


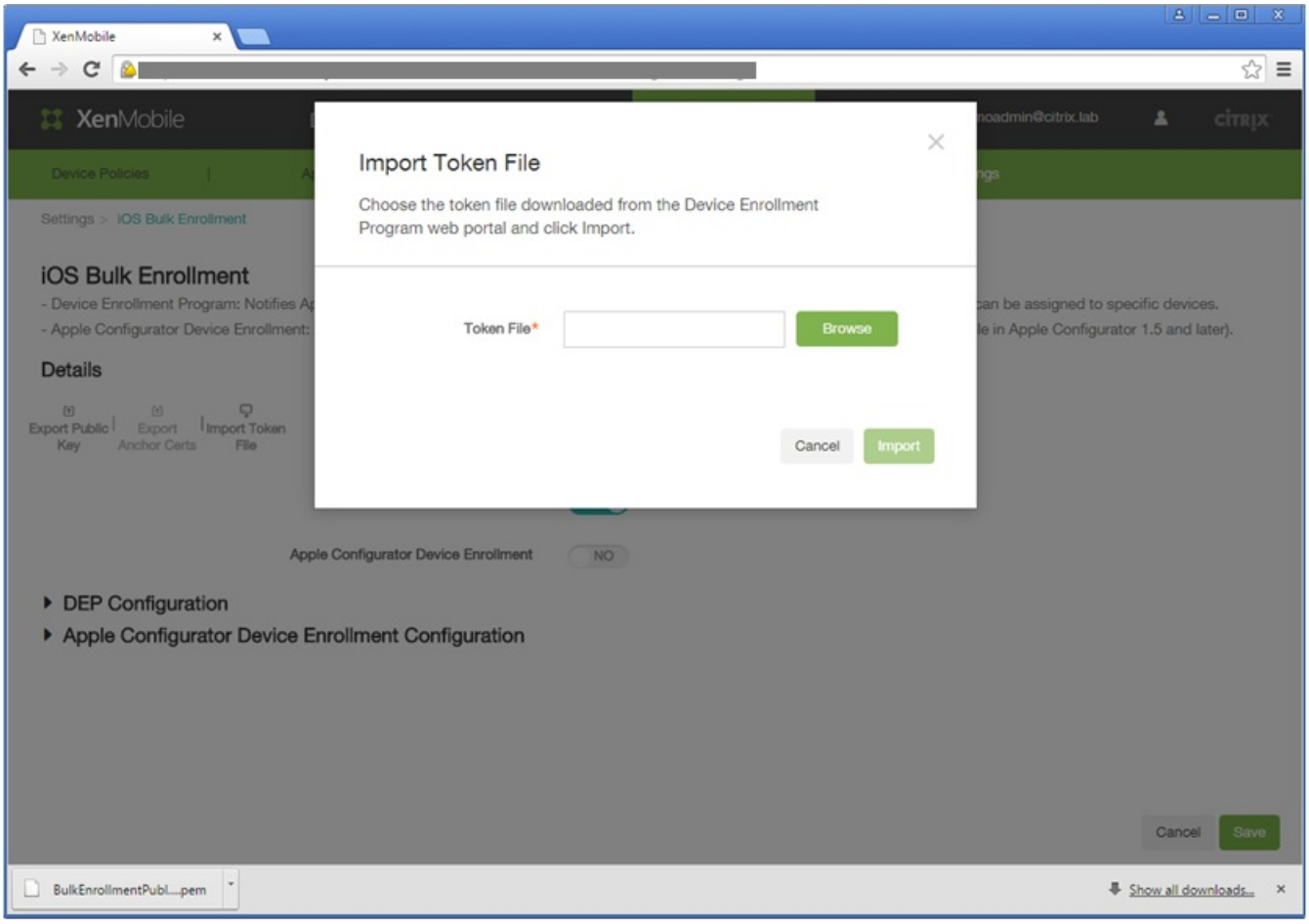


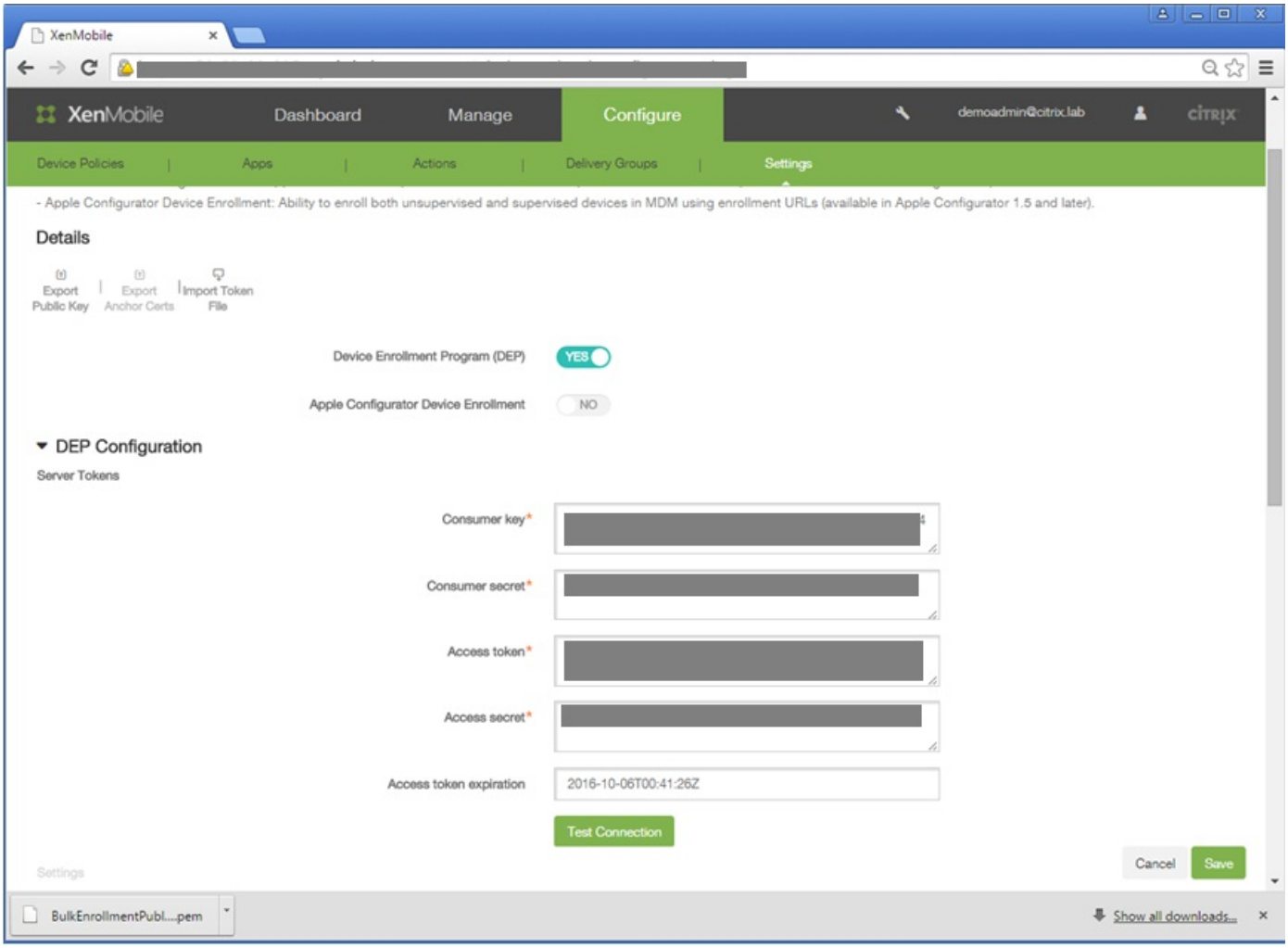


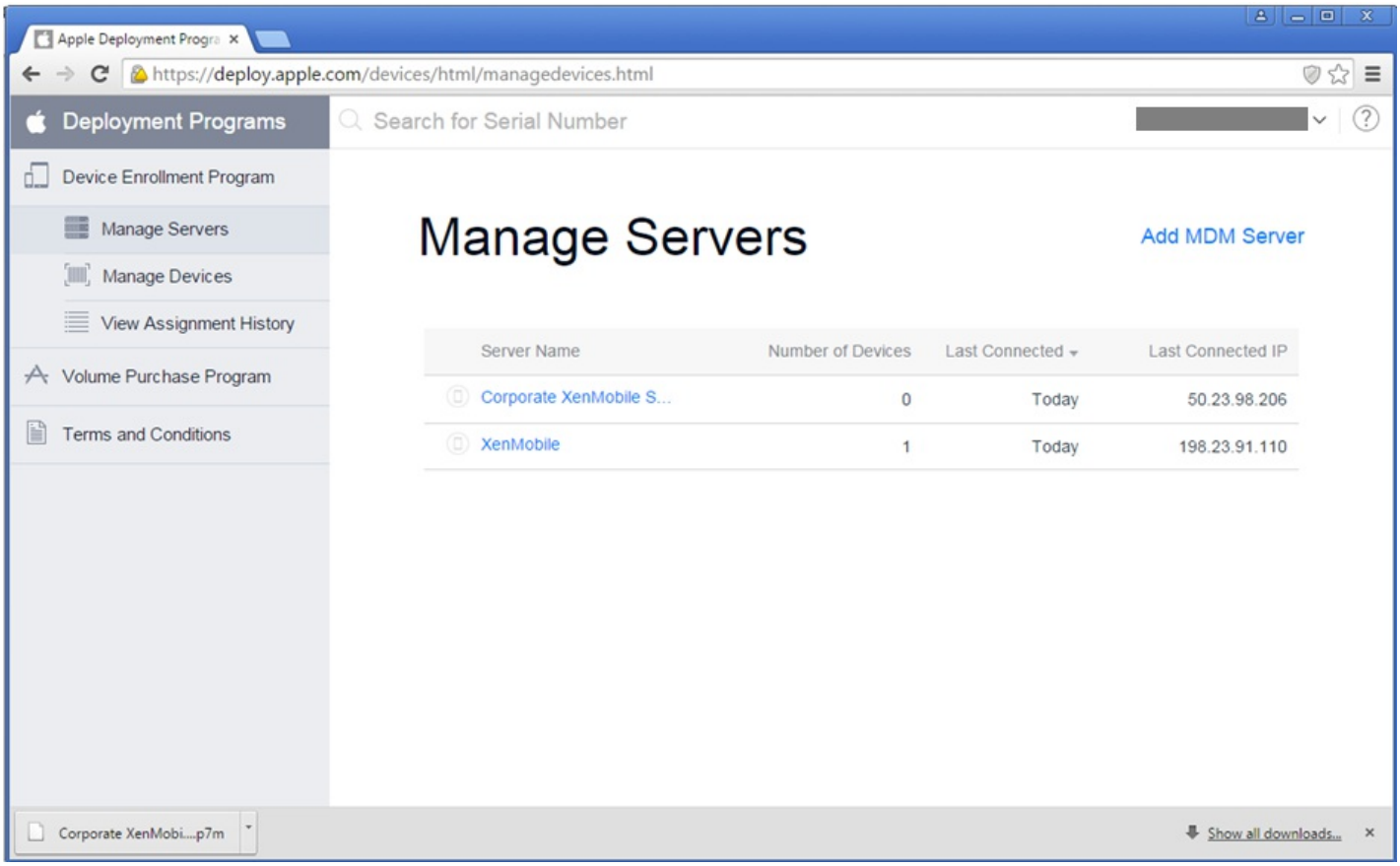






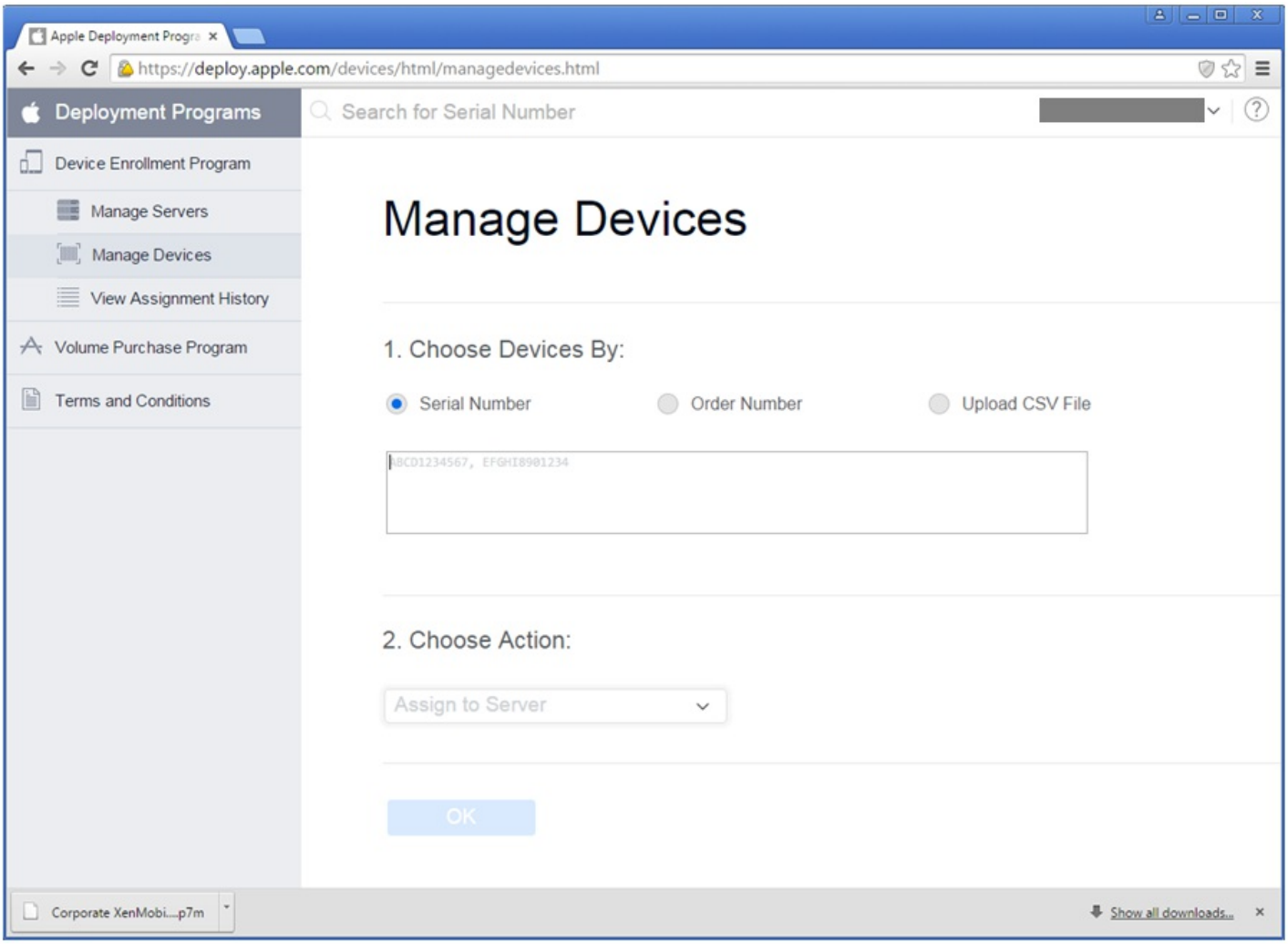


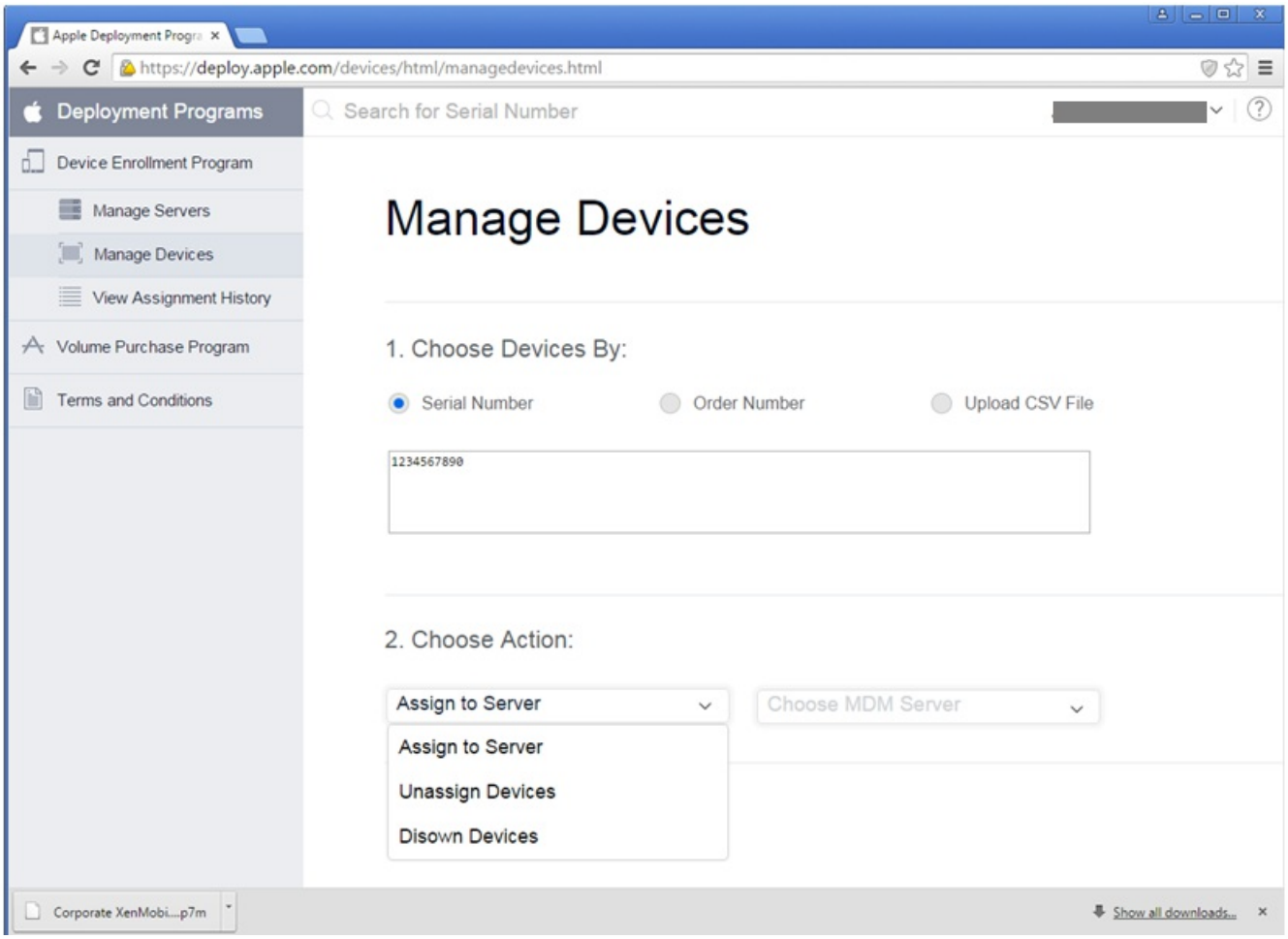


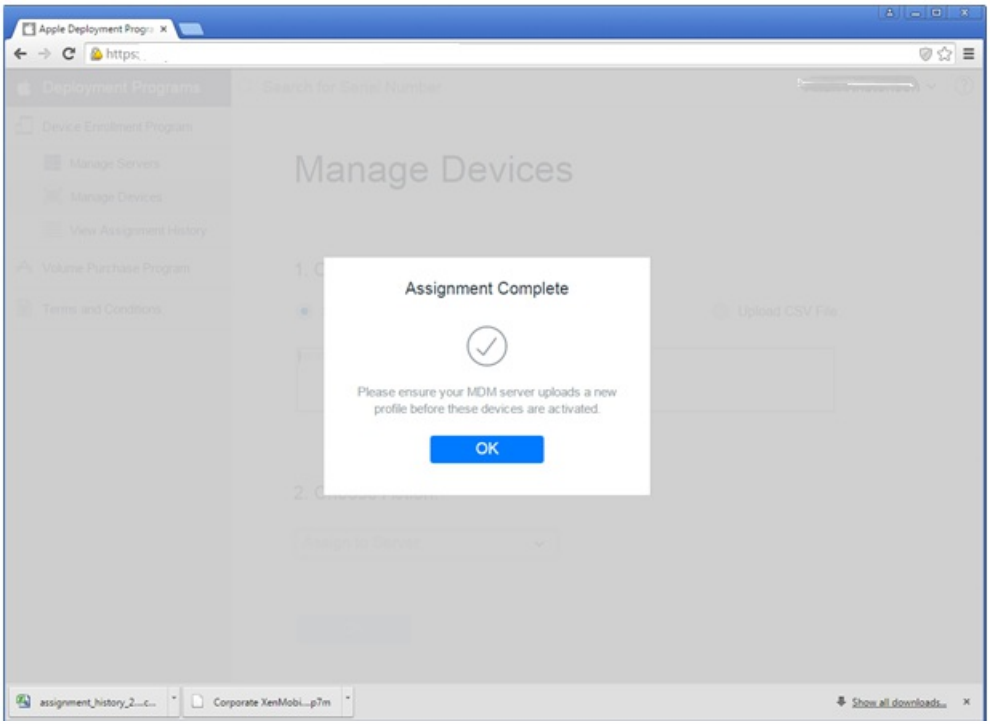


订购启用了 DEP 的设备

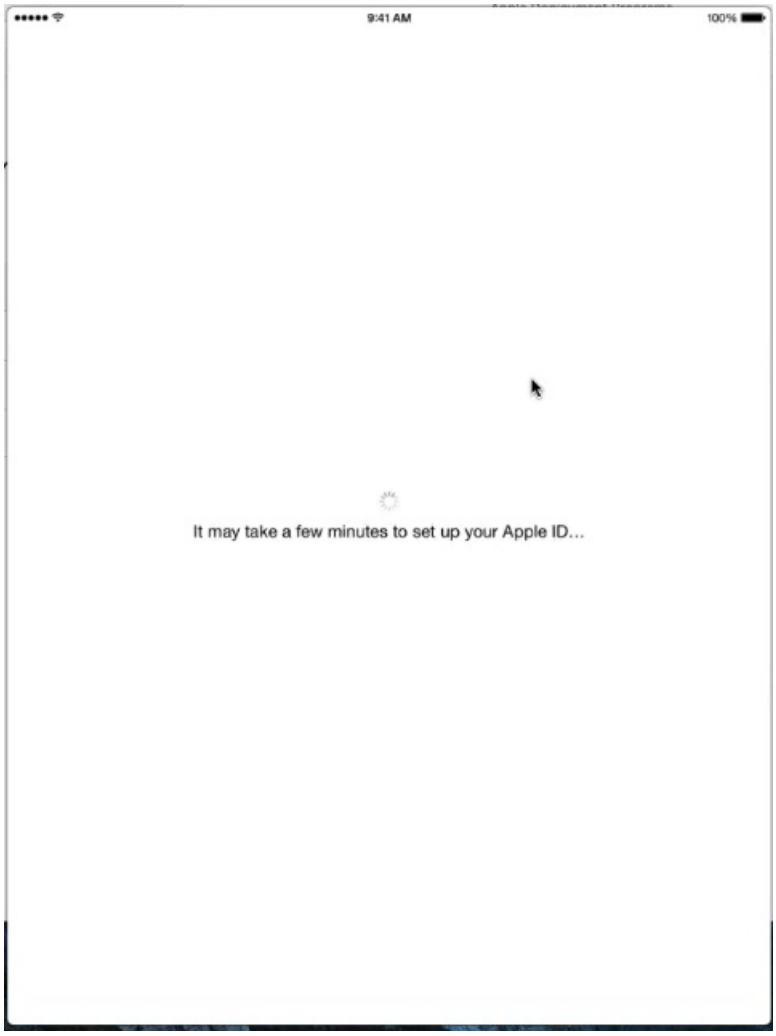
管理启用了 DEP 的设备

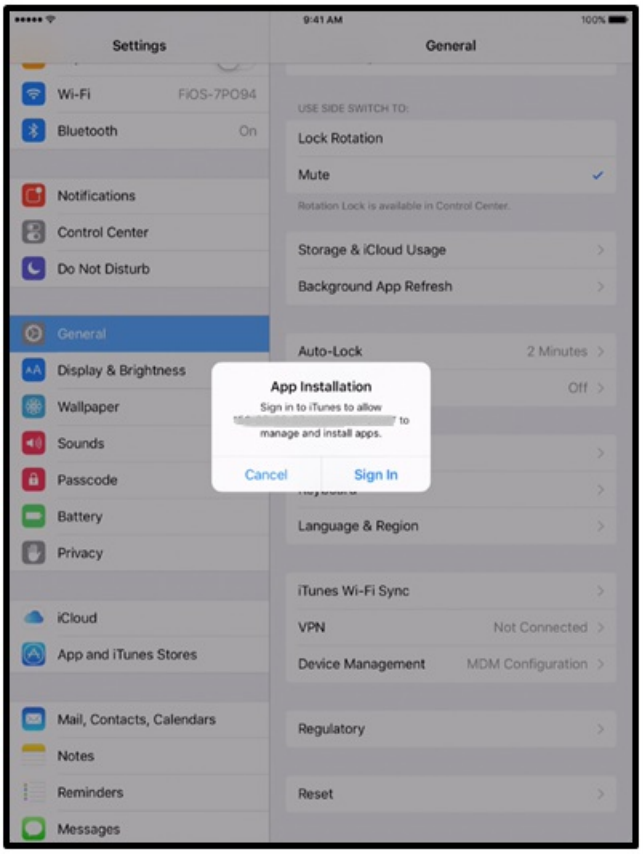




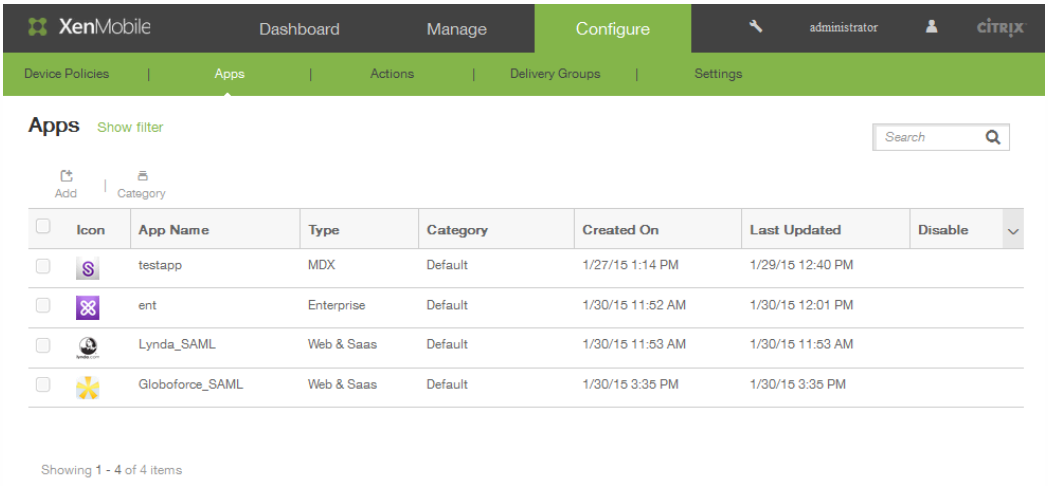


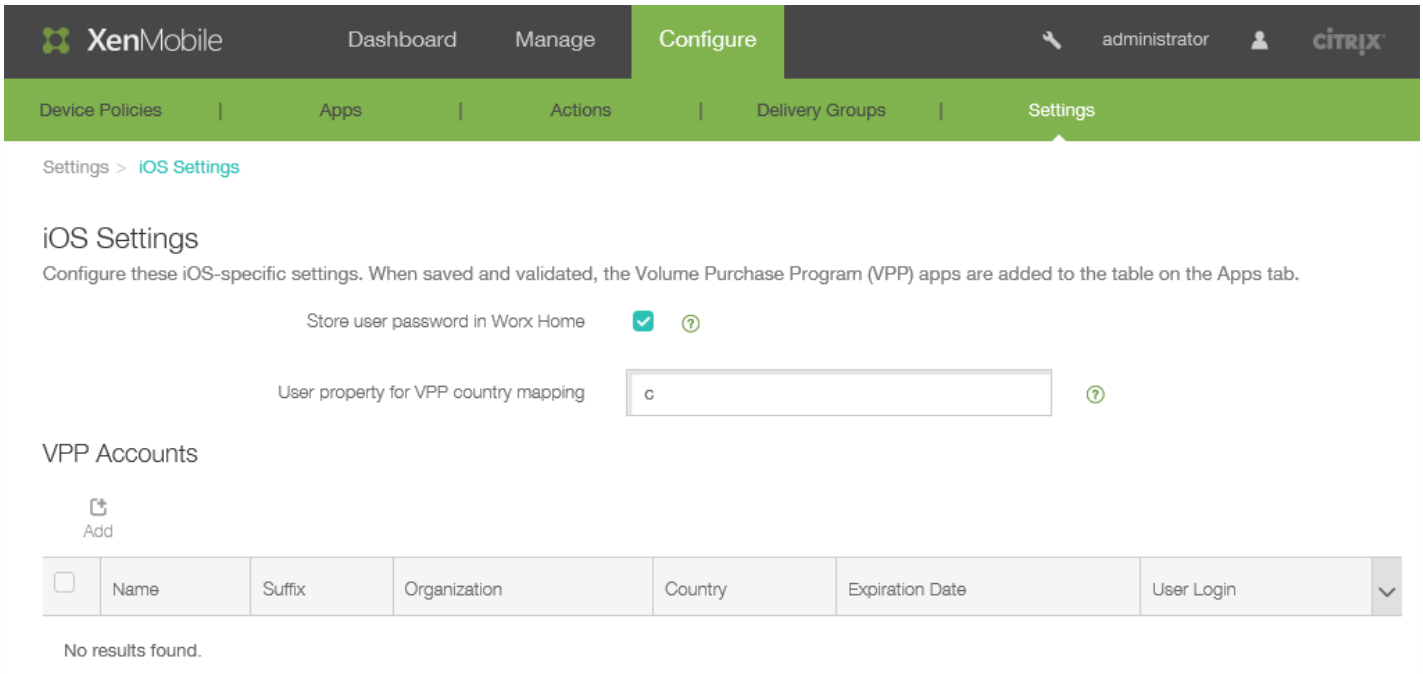
注册启用了 Apple DEP 的设备时的用户体验

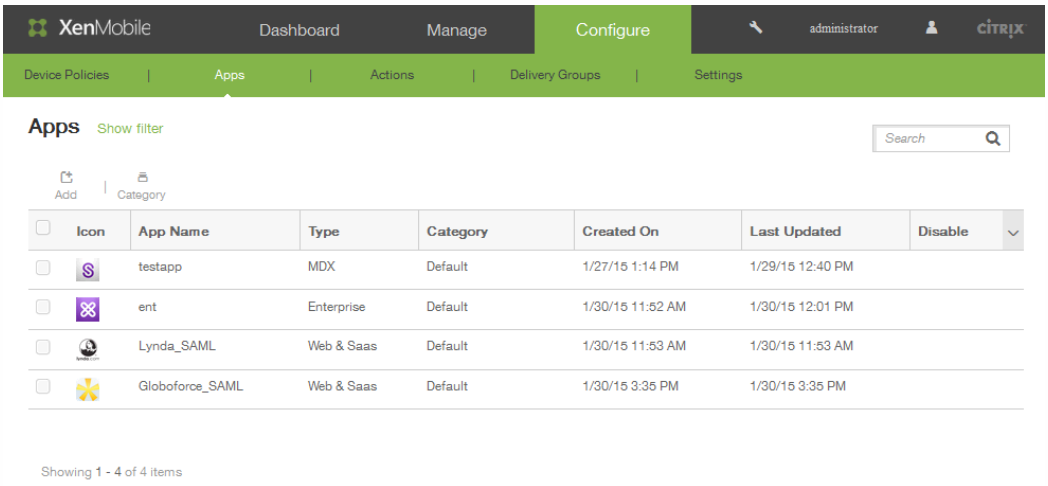




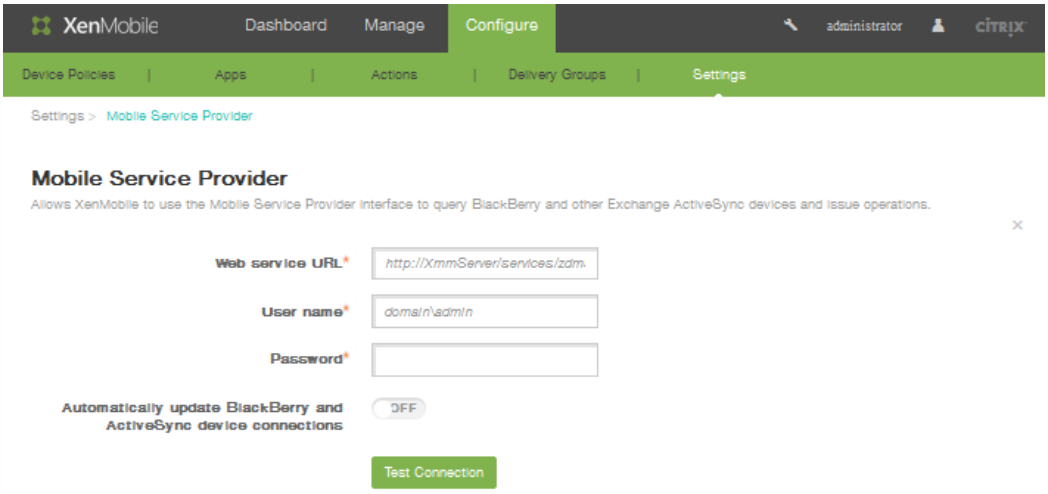
iOS VPP





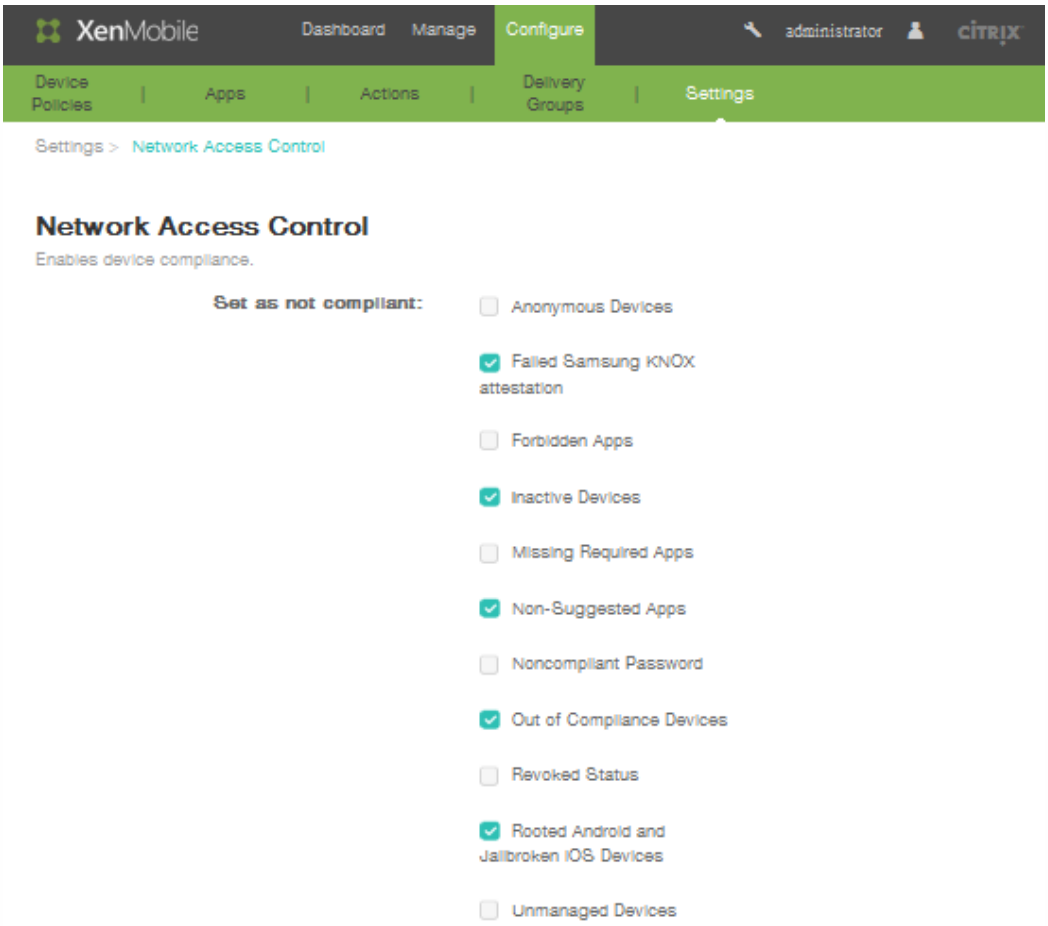


移动服务提供商

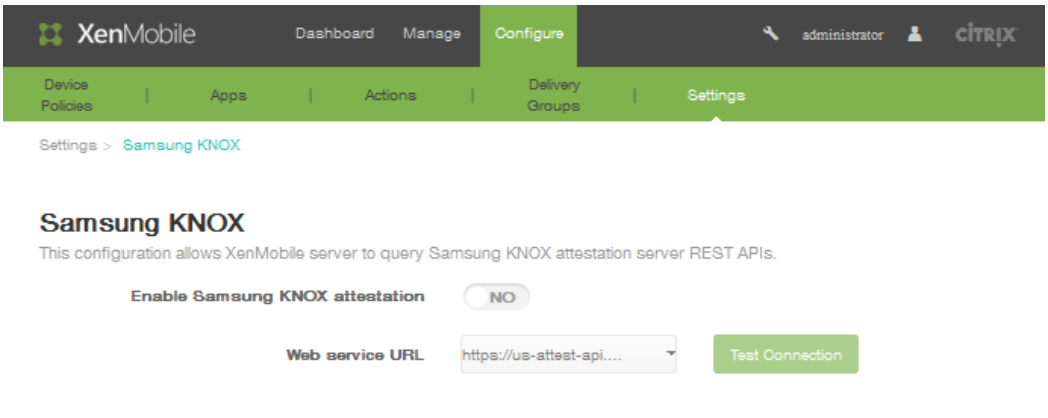


网络访问控制

> 注意



Samsung KNOX

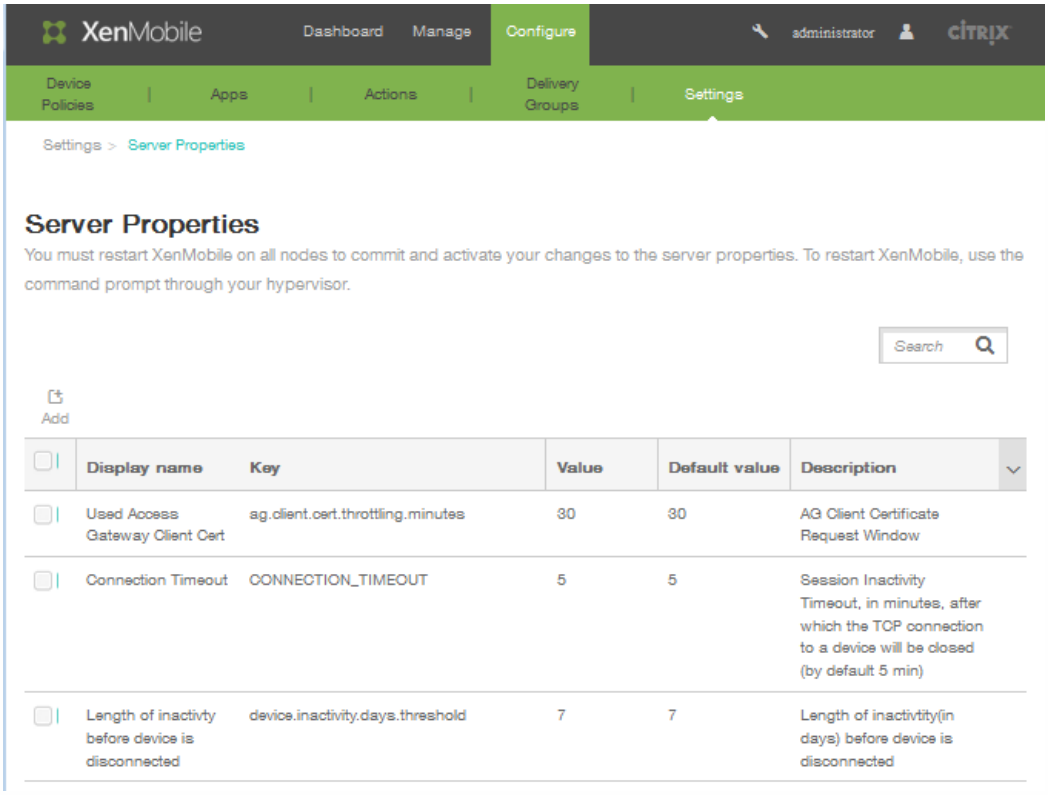


服务器属性

服务器属性定义

添加、编辑或删除服务器属性

> 注意



-
-

-

-
-
-

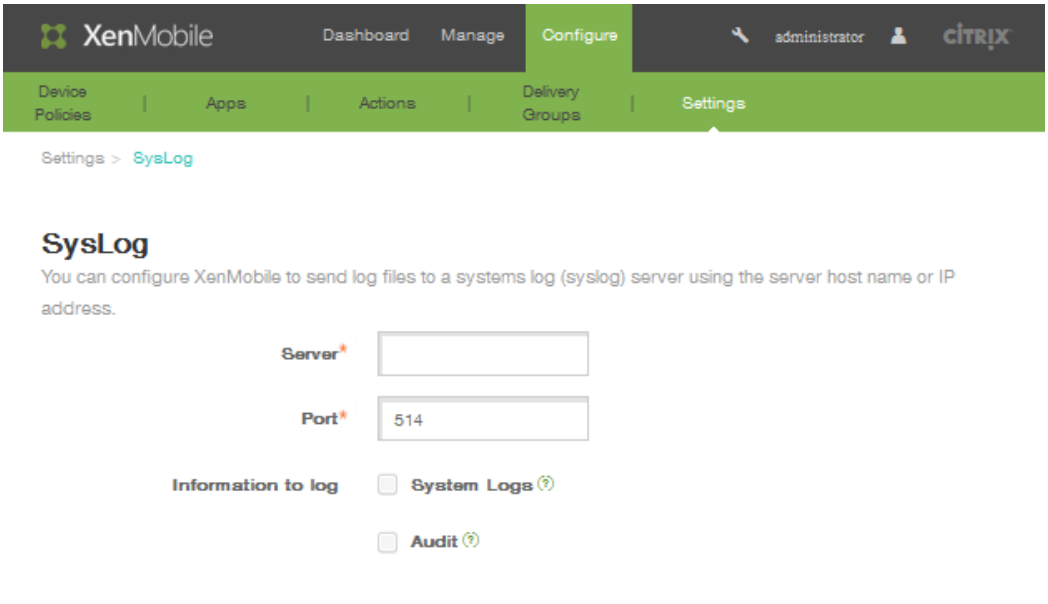
配置 XenMobile 有效服务器模式

SysLog

-
-

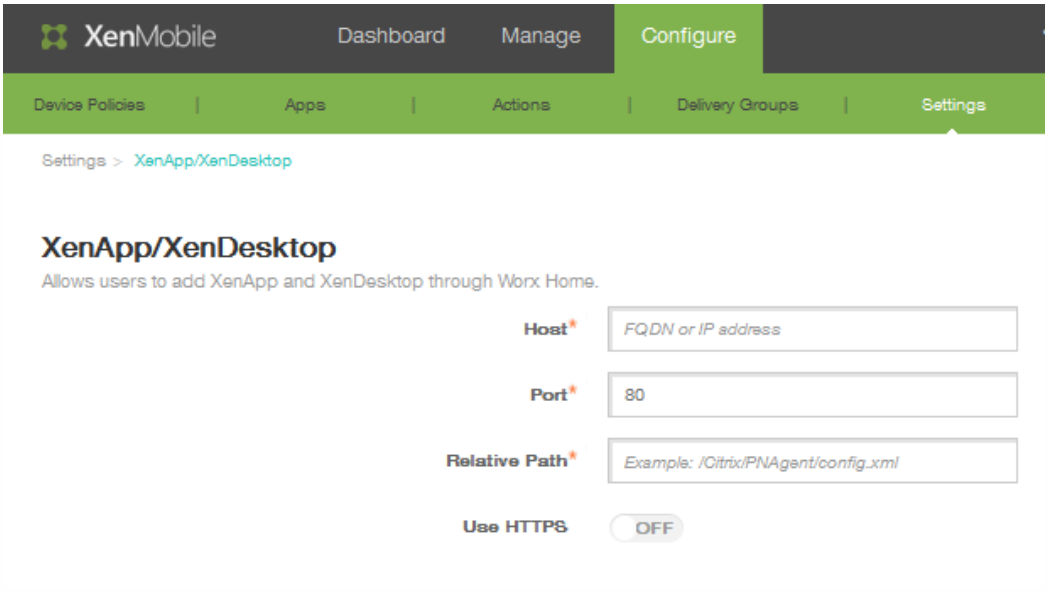
-
-
-
-
-

> 注意



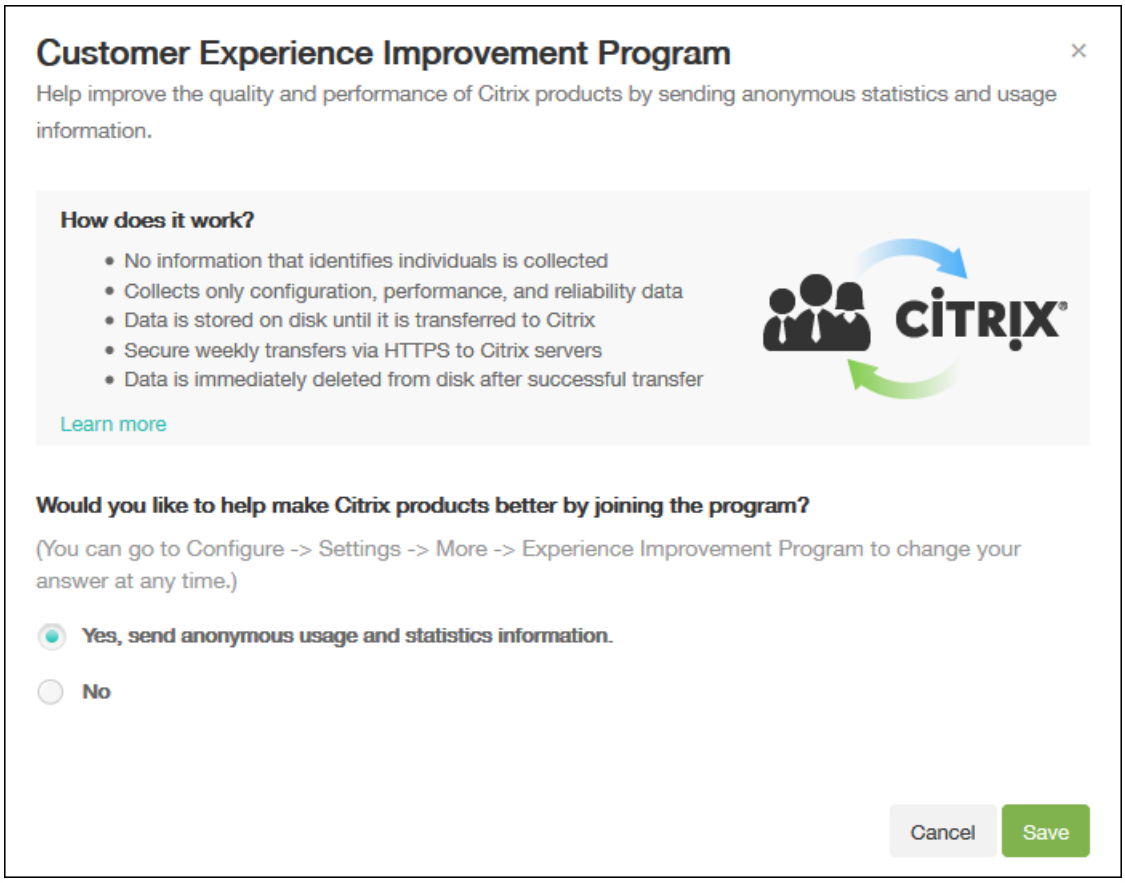
-
-

配置 XenApp 和 XenDesktop

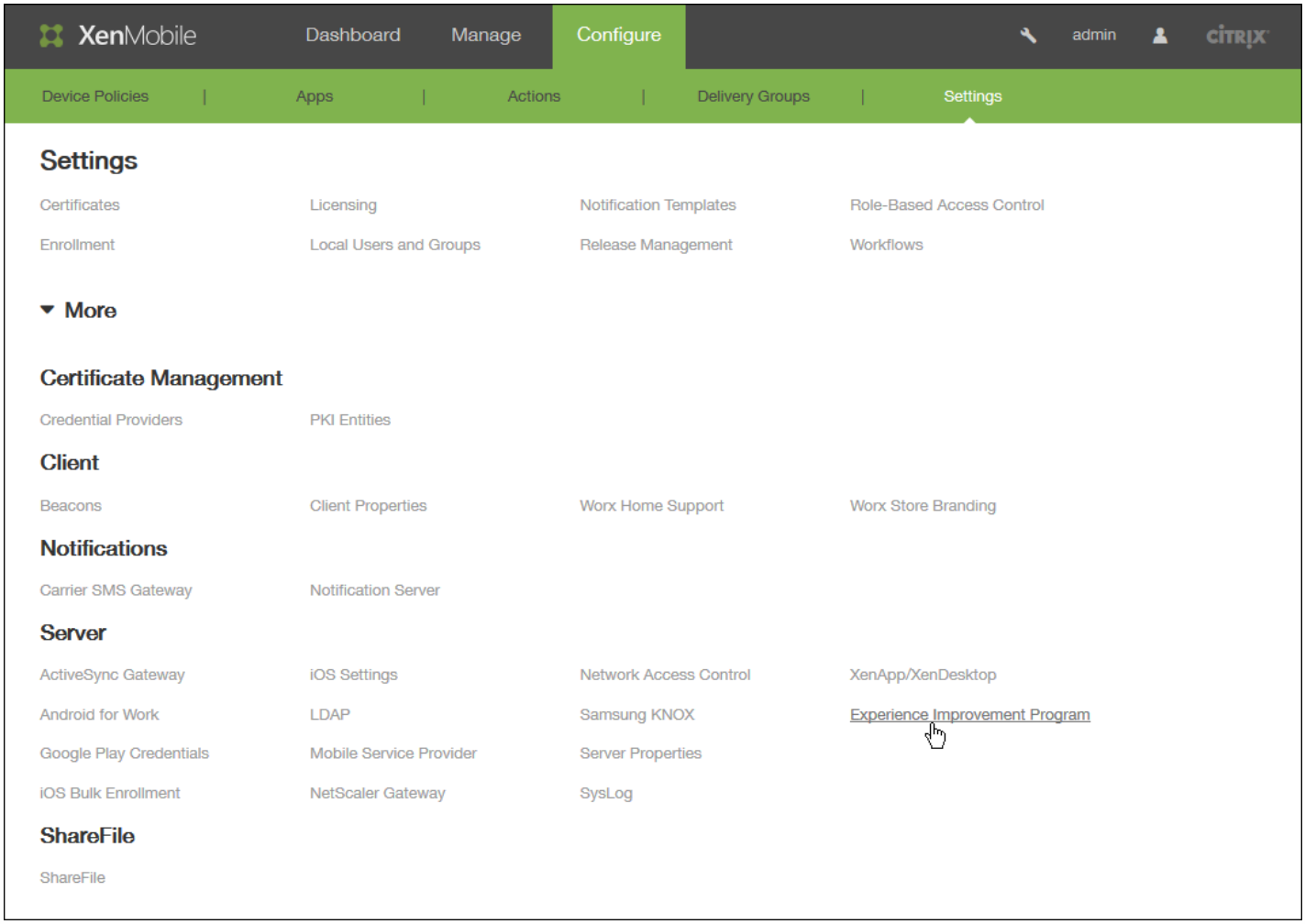


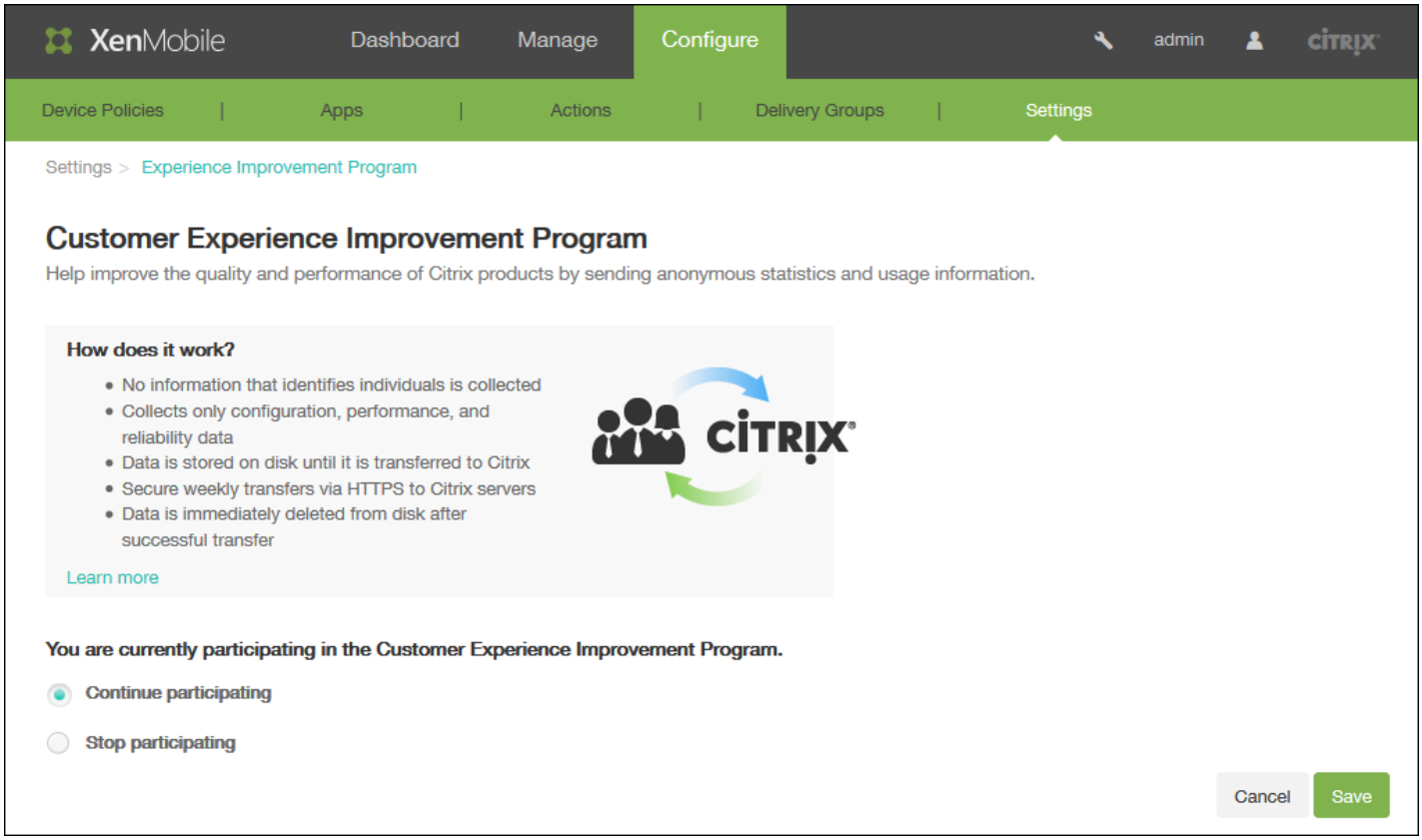
客户体验改善计划

安装或更新 XenMobile 时参与 CEIP

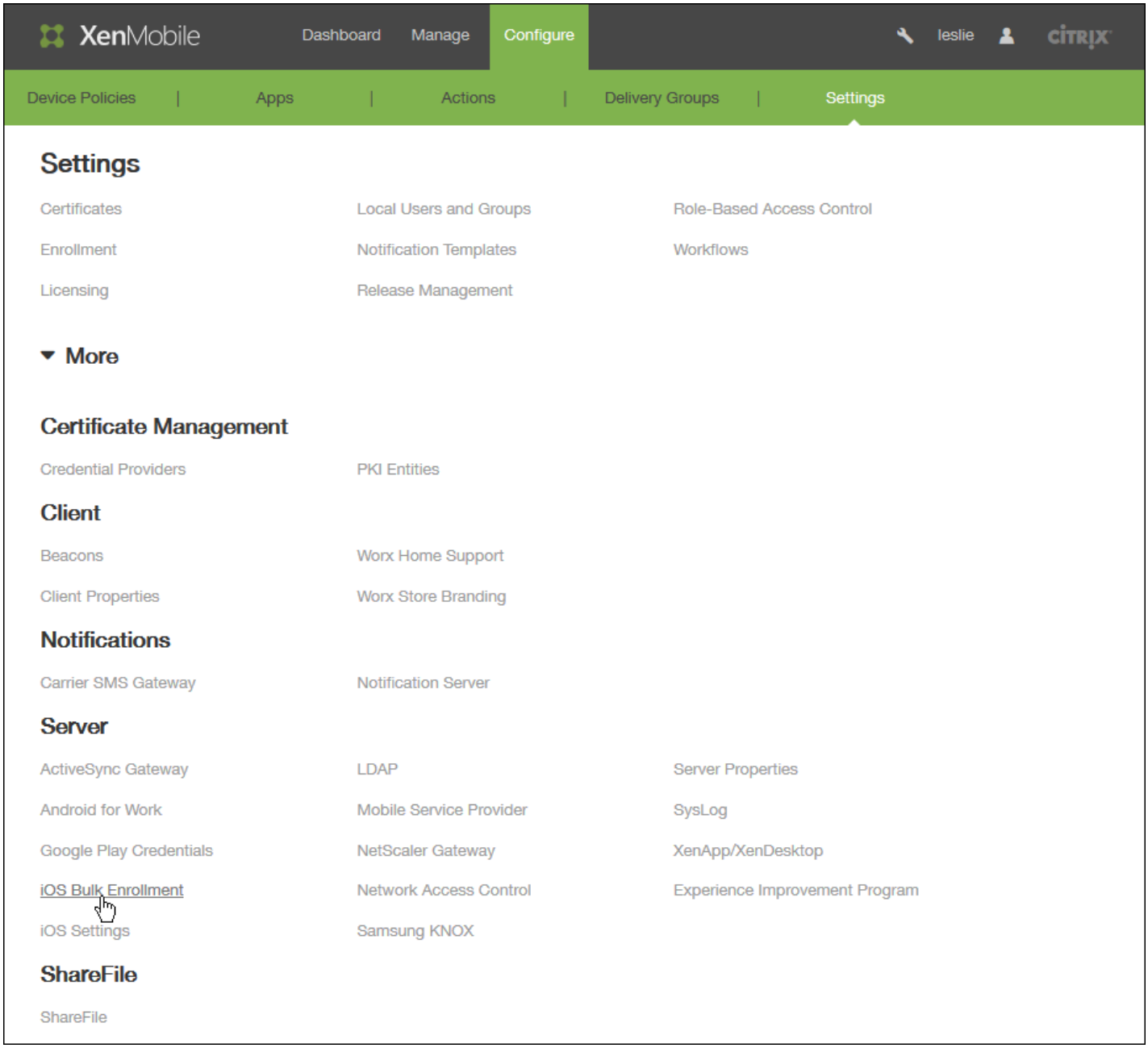


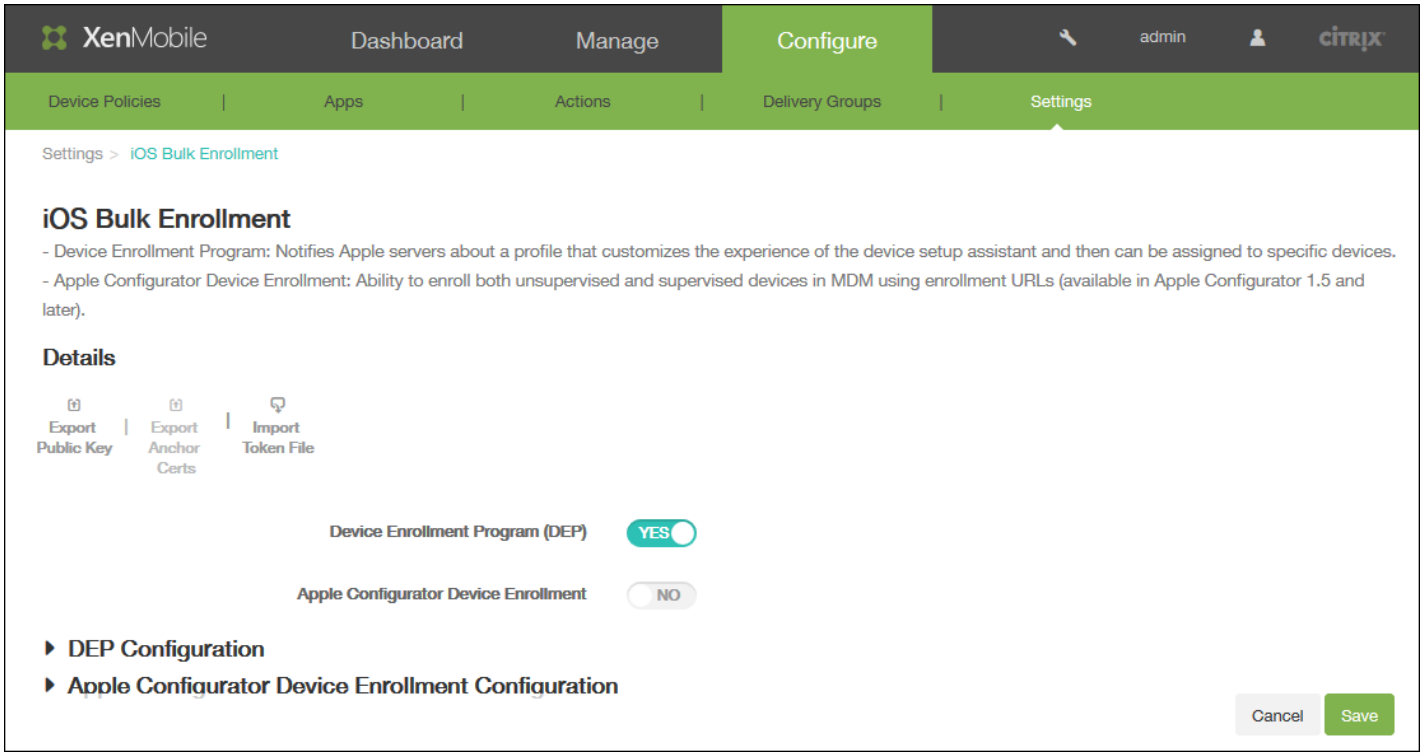
更改 CEIP 参与设置



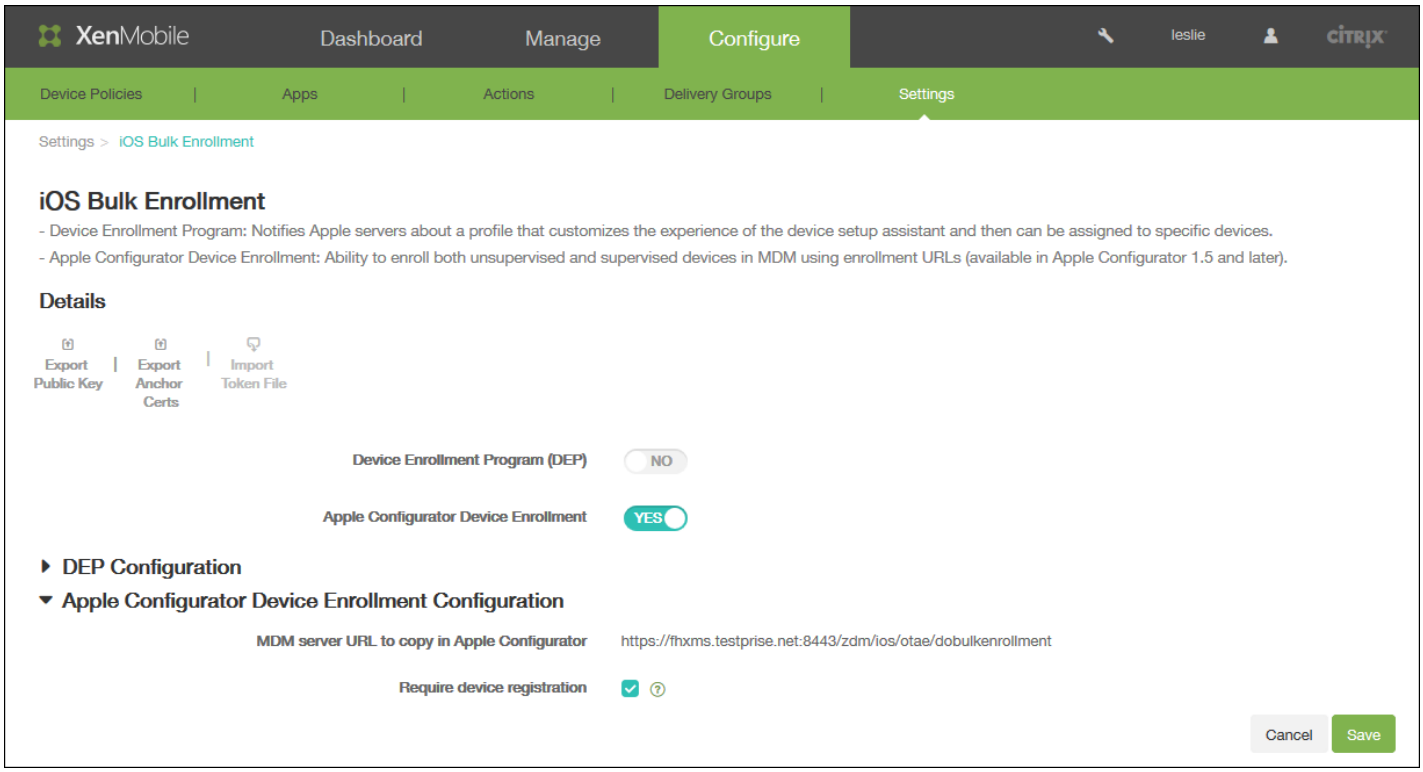


批量注册 iOS 设备





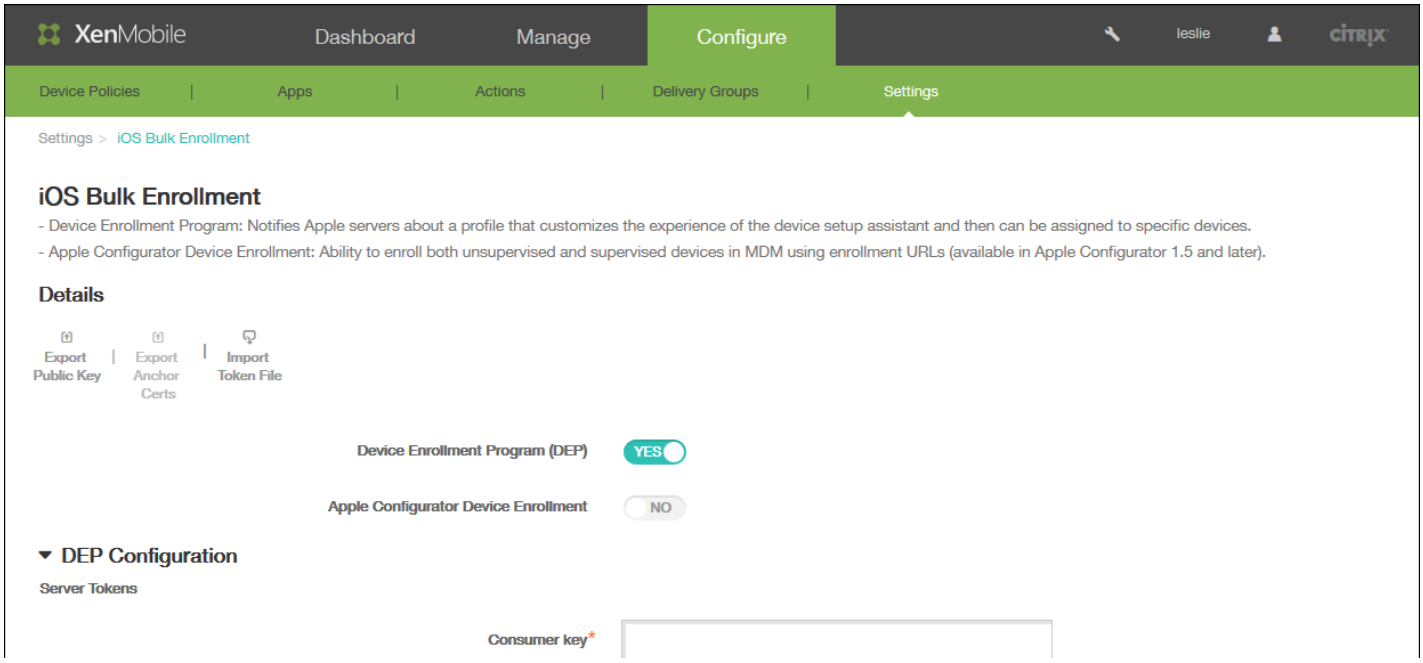
配置 Apple Configurator 设置

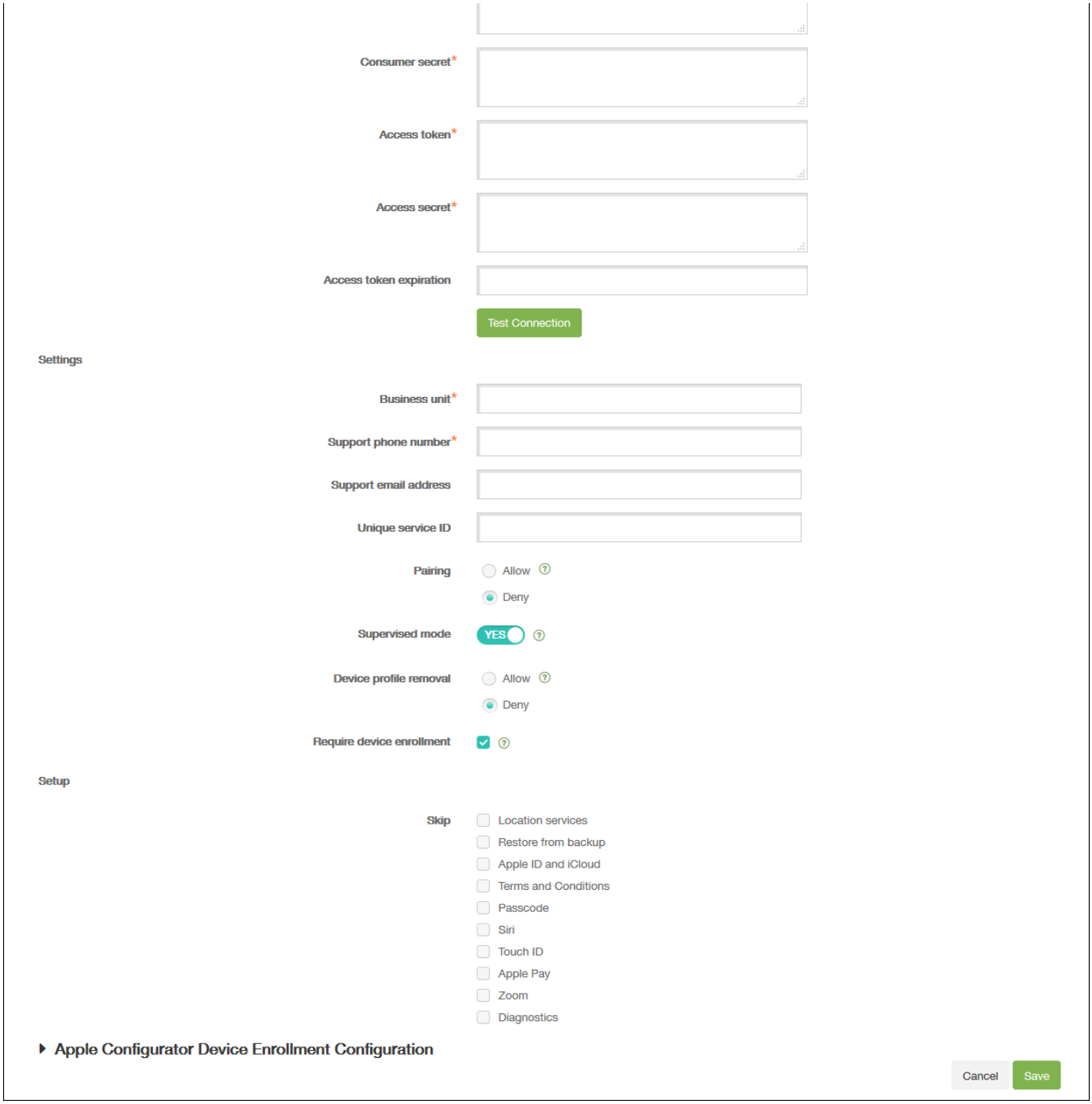


-
-

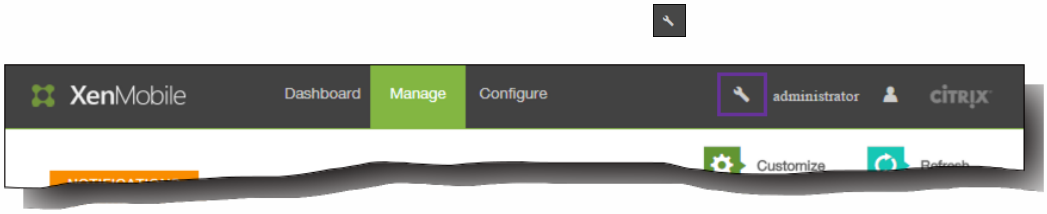
> **注意**

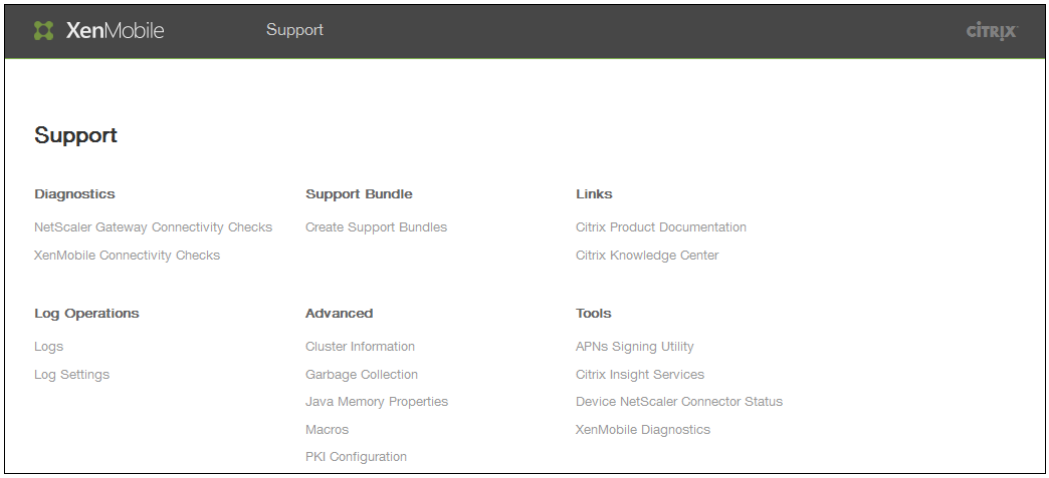
配置 DEP 设置





XenMobile 支持与维护





-
-
-
-
-
-

XenMobile REST API 参考

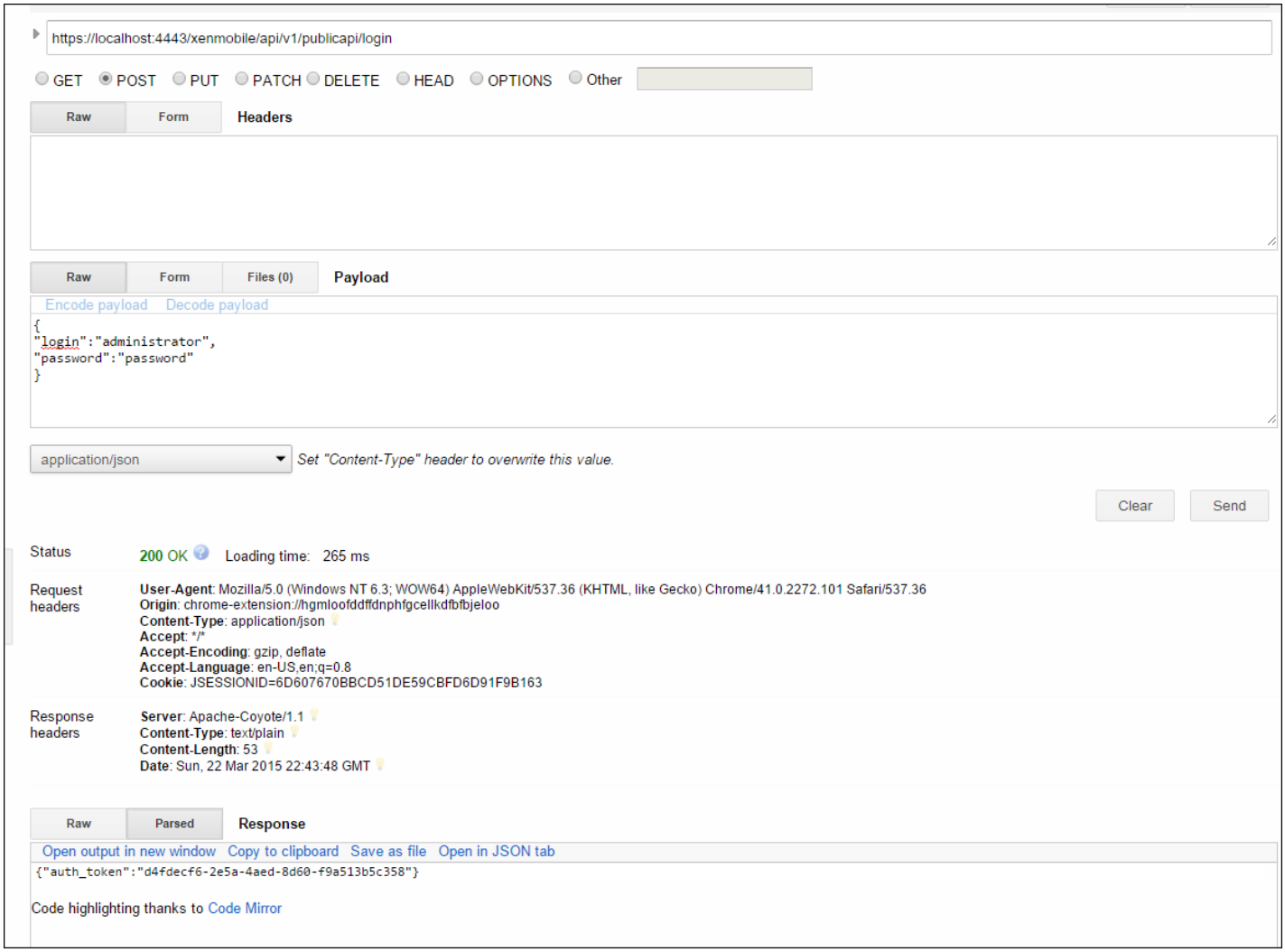
-
-

调用 REST API 服务

> 注意

使用 REST 客户端

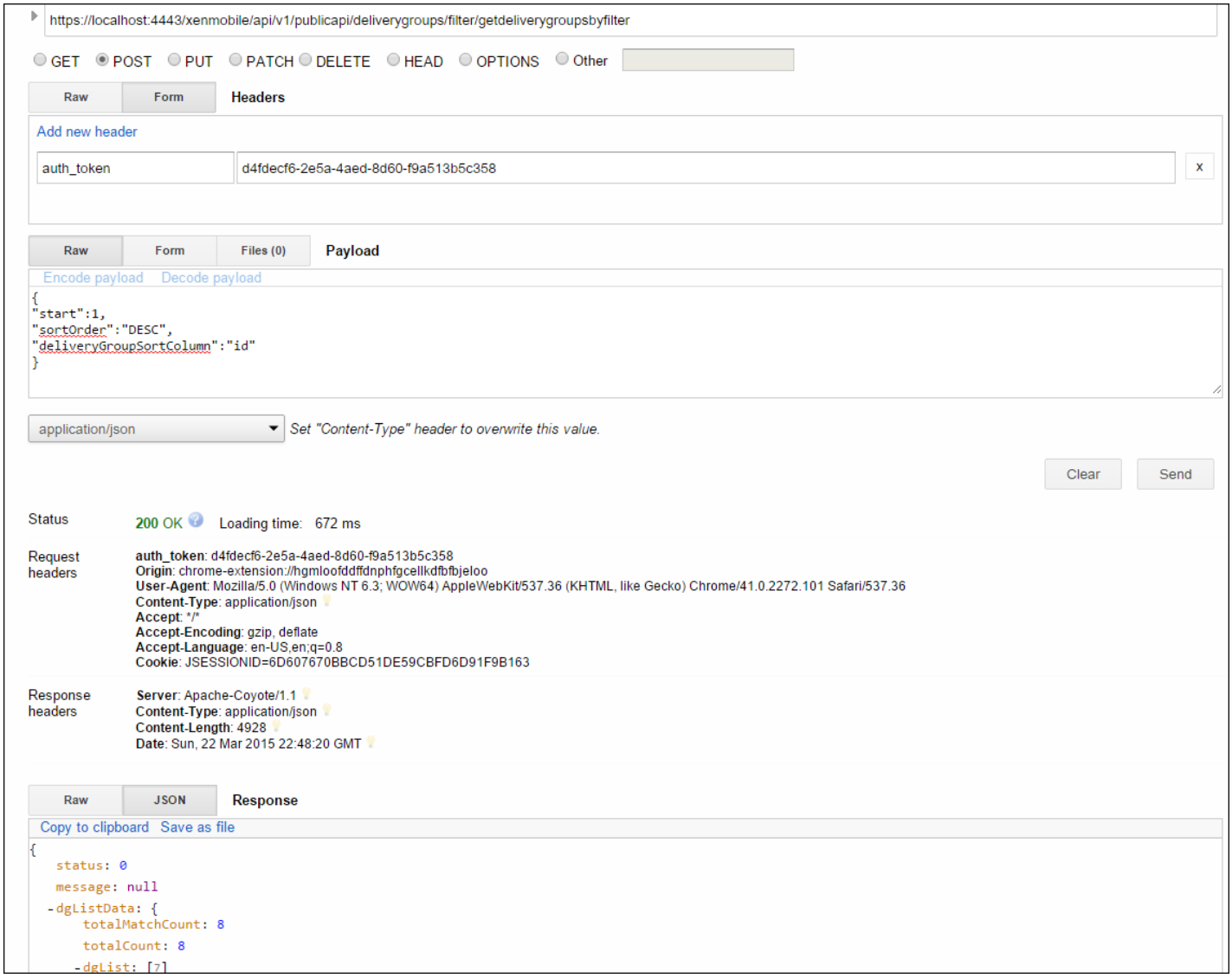
登录



通过过滤获取交付组

请求 复制

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

    "search":"add"

}
```



公共 API REST 服务

REST API 定义

登录公共 API

请求参数 复制

```
{ "login":"administrator", "password":"password" }
```

响应示例 复制

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

注销公共 API

请求参数 复制

```
{“login”:”administrator”}
```

响应示例 复制

```
{"Status":"user administrator logged out successfully."}
```

管理证书

获取所有证书

响应示例 复制


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
```



```
"signatureAlgo": "SHA1WithRSAEncryption",

"version": null,

"serialNum": "348237881800118418457268346483687164l3",

"issuerName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,

    "state": null,

    "country": null,

    "description": null

},

"subjectName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,
```



```
                    "locality": null,
                    "state": null,
                    "country": null,
                    "description": null
                }
            }
        }
    ],
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


删除证书

请求参数 复制

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

将证书作为 SAML 证书导入

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'saml',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```

```
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
        },
        "certificate": null,
        "apnsCheckObj": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
        }
    }
```


将证书作为服务器证书导入

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```


将证书作为侦听器证书导入

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'listener',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```

```
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


创建证书

请求参数 复制

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

响应示例 复制

```
{

    status: 0

    message: "Success"

    csrRequest: ""

    apnsCheck: null

    certificate: null

    apnsCheckObj:

    {

    topicNameMismatch: false

    certExpired: false

    certNotYetValid: false

    malformed: false

    }

}
```


导出证书

请求参数 复制

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

管理密钥库

导入服务器密钥库

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```

```
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


导入 SAML 密钥库

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
}
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
```

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


导入 APNs 密钥库

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


导入 SSL 侦听器密钥库

请求参数 复制

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

响应示例 复制

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
"certificate": null,
"apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


管理许可证

获取许可证信息

响应示例 复制

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```

```
    {
        sadate: "2015.1210"
        notice: "Example Systems Inc."
        vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
        licensesInUse: 0
        licensesAvailable: 102
        overdraftLicenseCount: 2
        p_E_M: "CXM_ENTU_UD"
        serialNumber: "cxmretailent1000user"
        licenseType: "Retail"
        expirationDate: "01-DEC-2015"
    }
    licenseNotification:
    {
        id: 1
        notificationEnabled: false
        notifyFrequency: 7
        notifyNumberDaysBeforeExpire: 60
        recepientList: ""
        emailContent: "License expiry notice"
```

```
        }

    }

}
```

保存许可证信息

请求参数 复制

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,

    "isScheduleNotificationNeeded": true
```

```
    "isScheduleNotificationNeeded": true,
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success"
}
```

上载许可证文件

响应示例 复制

```
{
   "status": 0,
   "message": "Success"
}
```

激活许可证

响应示例 复制

```
{
    "status": 0,
    "message": "Success"
    "cpLicenseServer": null
}
```

删除所有许可证

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "isConnected": null
}
```

测试许可证服务器

请求参数 复制

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "isConnected": true
}
```

获取最早的过期日期

响应示例 复制

```
{

    "status": 0,

    "message": "Success",

    "expiredDate": 1448956800000,

    "daysBeforeExpire": 229,

    "daysInPOC": 0

}
```


管理 LDAP 配置

列出 LDAP 配置

响应示例 复制

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userB

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","us

    ]

}
```

添加新的 LDAP 配置

请求参数 复制

```
{
    "primaryHost":"192.0.2.7",
    "secondaryHost":"",
    "port":"389",
    "username":"aaa@example.com",
    "password":"1.pwd",
    "userBaseDN":"dc=example,dc=com",
    "groupBaseDN":"dc=example,dc=com",
    "lockoutLimit":"0",
    "lockoutTime":"1",
    "useSecure":"false",
    "userSearchBy":"upn",
    "domain":"example.com",
    "domainAlias":"exampleAlias",
    "globalCatalogPort":"0",
    "gcRootContext":""
}
```

响应示例 复制

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

编辑 LDAP 配置

请求参数 复制

```
{
    "primaryHost":"192.0.2.7",
    "secondaryHost":"",
    "port":"389",
    "username":"aaa@example.com",
    "password":"1.pwd",
    "userBaseDN":"dc=example,dc=com",
    "groupBaseDN":"dc=example,dc=com",
    "lockoutLimit":"0",
    "lockoutTime":"1",
    "useSecure":"false",
    "userSearchBy":"upn",
    "domain":"example.com",
    "domainAlias":"exampleAlias",
    "globalCatalogPort":"0",
    "gcRootContext":""
}
```

设置默认 LDAP 配置

删除 LDAP 配置

管理 NetScaler Gateway 配置

列出所有 NetScaler Gateway 配置

响应示例 复制

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",
```

```
        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false",

        "id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        }

    ]

}
```

添加新的 NetScaler Gateway 配置

请求参数 复制

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

编辑 NetScaler Gateway 配置

请求参数 复制

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

删除 NetScaler Gateway 配置

设置默认 NetScaler Gateway 配置

管理 SMS 和 SMTP 通知服务器配置

列出所有 SMS 和 SMTP 服务器

响应示例 复制

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

获取服务器详细信息

SMS 响应示例 复制

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

SMTP 响应示例 复制

```
{
    name":"displayName",
    "description":"",
    "server":"192.0.2.12",
    "secureChannelProtocol":"true",
    "port":"345",
    "authentication":"false”,
    “username”: “test”,
    “password”: “testPassword”,
    "msSecurePasswordAuth":"true",
    "fromName":"Email name",
    "fromEmail":test@example.com,
    "numOfRetries":5,
    "timeout":30,
    "maxRecipients":100
}
```

添加 SMS 服务器配置

请求参数 复制

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false”,
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

编辑 SMS 服务器配置

请求参数 复制

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false”,
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

添加 SMTP 服务器配置

请求参数 复制

```
{
    name":"displayName",
    "description":"",
    "server":"192.0.2.9"
    "secureChannelProtocol":"true",
    "port":"345",
    "authentication":"false”,
    “username”: “test”,
    “password”: “testPassword”,
    "msSecurePasswordAuth":"true",
    "fromName":"Email name",
    "fromEmail":test@example.com,
    "numOfRetries":5,
    "timeout":30,
    "maxRecipients":100
}
```

编辑 SMTP 配置

请求参数 复制

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

删除服务器配置

设置默认 SMS 配置

设置默认 SMTP 配置

管理本地用户和组

获取所有用户

响应示例 复制

```
{
```

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }
```



```
    ]
}
```

获取一个用户

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "userid": 8,
        "username": "admin",
        "password": null,
        "confirmPassword": null,
        "groups": [],
        "attributes": {
            "company": "example"
```

```
            company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }

}
```


添加用户

请求参数 复制

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

响应示例 复制

```
{
    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 0,

    "username": "justaname_XX",

    "password": "password",

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": null,

    "lastAuthenticated": null,

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

更新用户

请求参数 复制

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

响应示例 复制

```
{
    "status": 0,
```

```
"message": "Success",

"user": {

    "userid": 108,

    "username": "justaname_XX",

    "password": null,

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": "3/27/15 1:10 PM",

    "lastAuthenticated": "3/27/15 1:10 PM",

    "domainName": null,
```



```
        "adUser": false,

        "vppUser": false

    }

}
```

更改用户密码

请求参数 复制

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

响应示例 复制

Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.

删除多个用户

请求参数 复制

```
{ justaname XX }
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

删除一个用户

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

导入置备文件

请求参数 复制

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

响应示例 复制

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

管理应用程序

通过过滤获取所有应用程序

请求参数 复制

```
{
    "start": 0,
    "limit": 10,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

按容器获取移动应用程序

响应示例 复制

```
{
```

```
"status": 0,

"message": "Success",

"result": {

    "id": 14,

    "name": "testApp",

    "description": "",

    "createdOn": null,

    "lastUpdated": null,

    "disabled": false,

    "nbSuccess": 0,

    "nbFailure": 0,

    "nbPending": 0,

    "schedule": {

        "enableDeployment": true,

        "deploySchedule": "NOW",

        "deployScheduleCondition": "EVERYTIME",

        "deployDate": null,

        "deployTime": null,

        "deployInBackground": false

    },
```



```
"iconData": "",
"appType": "MDX",
"categories": [
    "Default"
],
"roles": [],
"workflow": null,
"ios": {
    "displayName": "GoToMeeting",
    "description": "G2MW_IOS_5.3.3_075_01",
    "paid": false,
    "removeWithMdm": true,
    "preventBackup": true,
    "appVersion": "5.3.3.075",
    "minOsVersion": "",
    "maxOsVersion": "",
    "excludedDevices": "",
    "avppParams": null,
    "avppTokenParams": null,
```



```
"rules": null,

"appType": "mobile_ios",

"uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",

"id": 0,

"store": {

    "rating": {

        "rating": 0,

        "reviewerCount": 0

    },

    "screenshots": [],

    "faqs": [],

    "storeSettings": {

        "rate": true,

        "review": true

    }

},

"policies": [

    {

        "policyName": "ReauthenticationPeriod",

        "policyValue": "480",
```



```
            "policyType": "integer",

            "policyCategory": "Authentication",

            "title": "Reauthentication period (minutes)",

            "description": "\nDefines the period before a user is challenged to authenticate again. ",

            "units": "minutes",

            "explanation": null

        },

        {

            "policyName": "BlockJailbrokenDevices",

            "policyValue": "true",

            "policyType": "boolean",

            "policyCategory": "Device Security",

            "title": "Block jailbroken or rooted",

            "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",

            "units": null,

            "explanation": null

        },

        {

            "policyName": "CertificateLabel",

            "policyValue": "",
```



```
                    "policyType": "string",

                    "policyCategory": "Network Access",

                    "title": "Certificate label",

                    "description": "\nThe label for the certificate.\n                                                    Default value is er

                    "units": null,

                    "explanation": null

                }

            ]

        },

        "android": null,

        "android_knox": null,

        "android_work": null,

        "windows": null,

        "windows_tab": null

    }

}
```


按容器获取 SaaS 应用程序

按容器获取公共应用商店应用程序

按容器获取 Web 链接应用程序

删除应用程序容器

管理交付组配置

通过过滤获取交付组

请求参数 复制

```
{
    "start": 1,
    "sortOrder": "DESC",
    "deliveryGroupSortColumn": "id",
    “limit”:10,
    "search": "add"
}
```

响应示例 复制

```
{
     "status": 0,
     "message": "Success",
     "dgListData": {
          "totalMatchCount": 7,
          "totalCount": 10,
          "dgList": [
```

```
{
    "id": null,
    "name": "add delivery group 6.0",
    "description": "testing add delivery group 6.0",
    "groups": [
        {
            "id": 1,
            "userListId": 1,
            "name": "MSP",
            "uniqueName": "MSP",
            "uniqueId": "MSP",
            "domainName": "local",
            "primaryToken": 0
        }
    ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\"
    "disabled": false,
    "lastUpdated": 1427144713353,
```



```
"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "Web Link",

        "required": false

    },

    {

        "name": "GoogleApps_SAML",

        "required": true

    }

],

"devicePolicies": [

    "test terms conditions"

],

"smartActions": [

    "shankar ganesh"

],

"nbSuccess": 0,

"nbFailure": 0
```



```
        "nbFailure": 0,

        "nbPending": 0

    },

    {

        "id": null,

        "name": "add delivery group 5.0",

        "description": "testing add delivery group 5.0",

        "groups": [

            {

                "id": 1,

                "userListId": 1,

                "name": "MSP",

                "uniqueName": "MSP",

                "uniqueId": "MSP",

                "domainName": "local",

                "primaryToken": 0

            }

        ],

        "zoneId": null,

        "zoneDomain": null,
```



```
"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\"

"disabled": false,

"lastUpdated": 1426891345698,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "GoogleApps_SAML",

        "required": true

    },

    {

        "name": "Web Link",

        "required": false

     }

],

"devicePolicies": [

    "test terms conditions"

],

"smartActions": [

    "shankar ganesh"
```



```
                ],
                "nbSuccess": 0,
                "nbFailure": 0,
                "nbPending": 0
            }
        ]
    }
}
```

根据名称获取交付组

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
```

```
"name": "AllUsers",

"description": "default role",

"groups": [],

"zoneId": null,

"zoneDomain": null,

"rules": null,

"disabled": false,

"lastUpdated": null,

"anonymousUser": false,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "test mdx",

        "required": false

    },

    {

        "name": "test all",

        "required": false

    },

    {
```



```
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ],
    "smartActions": [
        "justa name"
    ],
    "nbSuccess": 0,
    "nbFailure": 0
```



```
        "nbPending": 0
    }
}
```

编辑交付组

请求参数 复制

```
{
    "name": "add delivery group 2",
    "description": "Changing the description of the delivery group xxx",
    "groups": [
        {
            "name": "MSP",
            "uniqueName": "MSP",
            "uniqueId": "MSP",
            "domainName": "local"
        },
```

```
        {
            "name":"CN=Users,CN=Builtin,DC=example,DC=com",
            "uniqueName": "Users",
            "uniqueId":"a4169204-45f6-48fb-8a0d-847a3200d47e",
            "domainName": "example.com"
        }
        ],
    "disabled": false,
    "anonymousUser": false,
    "applications": [
        {
            "name": "GoogleApps_SAML",
            "required": true
        },
        {
            "name": "test mdx",
            "required": false
        }
        ],
    "devicePolicies": [
```

```
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
    "smartActions": [
        {
            "name":"Smart Action Name 1",
            "priority":-1
        }
        ],
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-restrictU
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
```

```
"role": {
    "id": null,
    "name": "add delivery group 2",
    "description": "Changing the description of the delivery group xxx",
    "groups": [
        {
            "id": null,
            "userListId": null,
            "name": "MSP",
            "uniqueName": "MSP",
            "uniqueId": "MSP",
            "domainName": "local",
            "primaryToken": null
        },
        {
            "id": null,
            "userListId": null,
            "name": "CN=Users,CN=Builtin,DC=example,DC=com",
            "uniqueName": "Users",
            "uniqueId": "a4169204-45f6-48fb-8a0d-847a3200d47e",
```



```
            "domainName": "example.com",
            "primaryToken": null
        }
      ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-rest
    "disabled": false,
    "lastUpdated": null,
    "anonymousUser": false,
    "roledefLangVersionId": null,
    "applications": [
      {
       "name": "GoogleApps_SAML",
            "required": true
      },
      {
            "name": "test mdx",
            "required": false
      }
```



```
                ],
            "devicePolicies": [
                "test terms conditions"
                ],
            "smartActions": [
                "justa name"
                ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0
        }
    }
```


添加交付组

请求参数 复制

```
{

    "name": "add delivery group 4.0",

    "description": "testing add delivery group 4.0",

    "anonymousUser": true,

    "devicePolicies": [

        {

            "name":"test terms conditions",

            "priority":-1

        }

        ],

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false

            }

        ]
```

```
    ],
"devicePolicies": [
    {
        "name":"test terms conditions",
        "priority":-1
    }
    ],
 "smartActions": [
    {
        "name":"Smart Action Name 1",
        "priority":-1
    }
    ],
"groups": [
    {
        "uniqueName": "MSP",
        "domainName": "local",
        "name": "MSP",
        "uniqueId": "MSP"
    }
```

```
        ],
    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"ju
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": 16,
        "name": "add delivery group 11.0",
        "description": "testing add delivery group 4.0",
        "groups": [
            {
                "id": null,
                "userListId": null,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
```

```
            "domainName": "local",

            "primaryToken": null

        }

       ],

    "zoneId": null,

    "zoneDomain": null,

    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\"

    "disabled": false,

    "lastUpdated": null,

    "anonymousUser": true,

    "roledefLangVersionId": null,

    "applications": [

        {

            "name": "GoogleApps_SAML",

            "required": true

        },

        {

            "name": "Web Link",

            "required": false

        }
```



```
            ],
        "devicePolicies": [
            "test terms conditions"
            ],
        "smartActions": [
            "justa name"
            ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    }
}
```

删除交付组

请求参数 复制

```
[ "add delivery group 11.0" ]
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "roleNames": [
        "add delivery group 11.0"
    ]
}
```

管理服务器属性

获取所有服务器属性。

响应示例 复制

```
{
```

```
"status": 0,

"message": "Success",

"allEwProperties": [

    {

        "id": 1,

        "name": "ios.mdm.pki.ca-root.certificatefile",

        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayName": "ios.mdm.pki.ca-root.certificatefile",

        "description": "",

        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayFlag": false,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    } ,

    {

        "id": 2,

        "name": "ios.mdm.https.host",

        "value": "192.0.2.4",
```



```
        "displayName": "ios.mdm.https.host",

        "description": "",

        "defaultValue": "192.0.2.4",

        "displayFlag": false,

        "editFlag": false,

        "deleteFlag": false,

        "markDeleted": false

    },

    {

        "id": 3,

        "name": "ios.mdm.enrolment.checkRemoteAddress",

        "value": "false",

        "displayName": "iOS Device Management Enrollment - Check Remote Address",

        "description": "",

        "defaultValue": "false",

        "displayFlag": true,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    },
```



```
    ]
}
```

通过过滤获取服务器属性

请求参数 复制

```
{
    "start": 0,
    "limit": 1000,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

响应示例 复制

```
{
```

```
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
            "value": "justaserver1",
            "displayName": "justarserver display name",
            "description": "justaserver description",
            "defaultValue": "justaserver1",
            "displayFlag": true,
            "editFlag": true,
            "deleteFlag": true,
            "markDeleted": false
        }
    ]
}
```


添加服务器属性

请求参数 复制

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 1",
    "description": "Description 1"
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```


编辑服务器属性

请求参数 复制

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

重置服务器属性

请求参数 复制

```
{
    "names": [,
        "justaname7"
        ]
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```

删除服务器属性

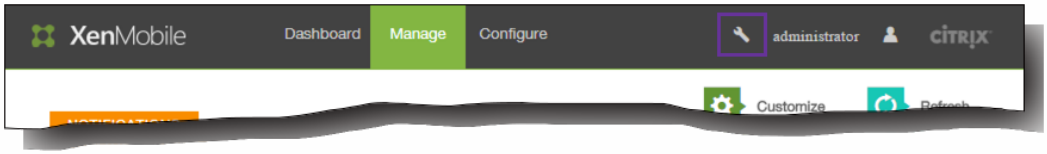
请求参数 复制

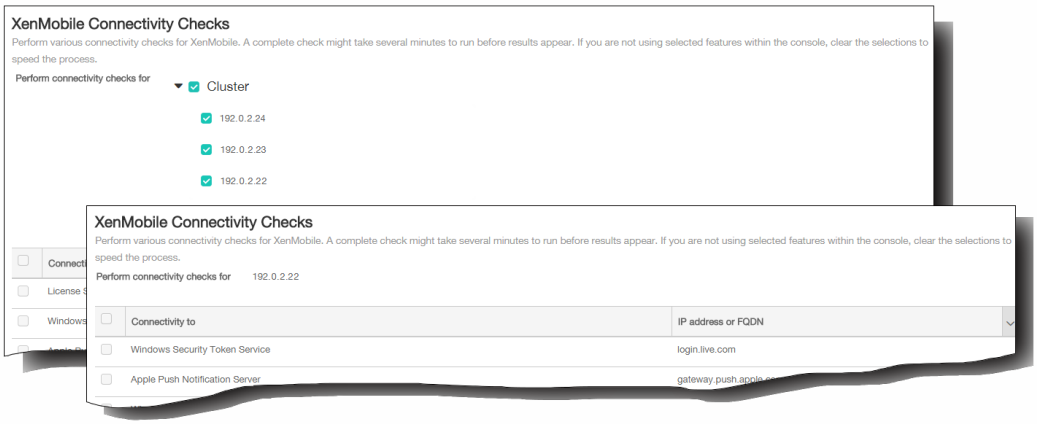
```
{
    "justaname3",
    "justaname4"
}
```

响应示例 复制

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

执行连接检查

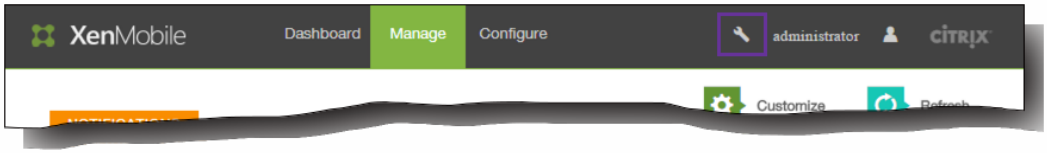


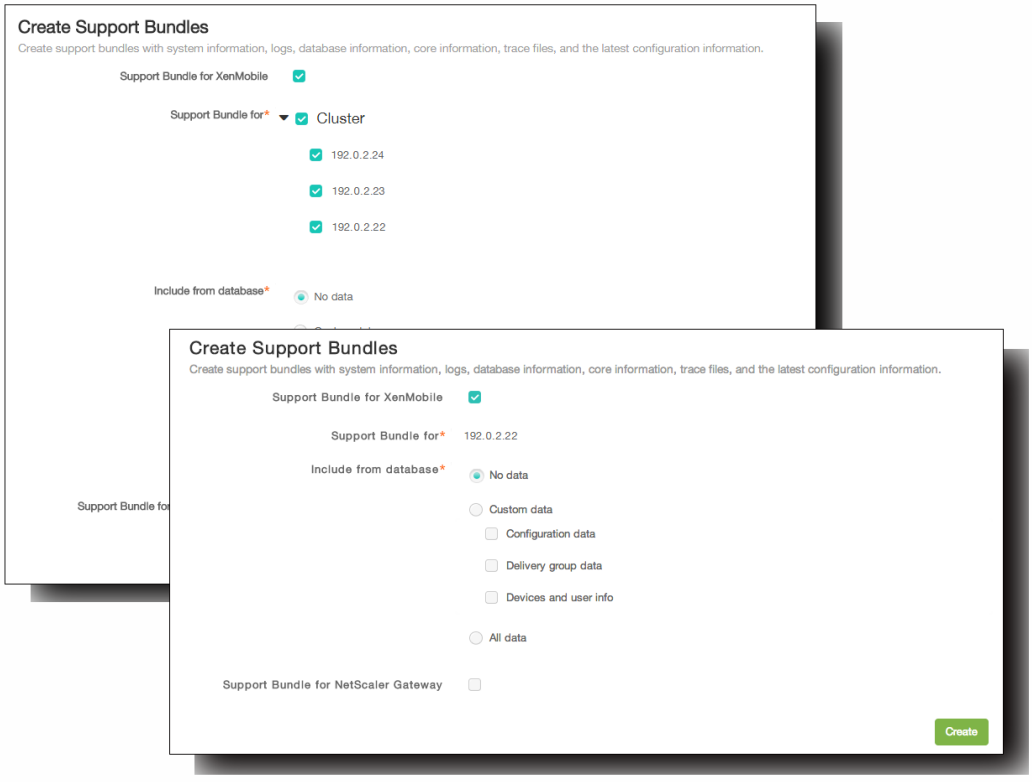


执行 XenMobile 连接检查

执行 NetScaler Gateway 连接检查

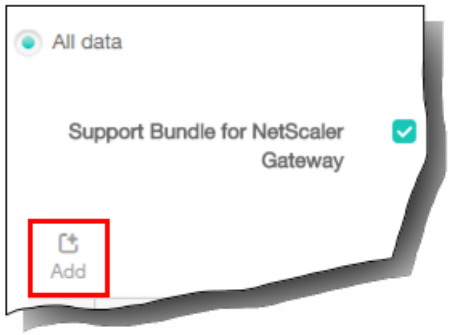
在 XenMobile 中创建支持包

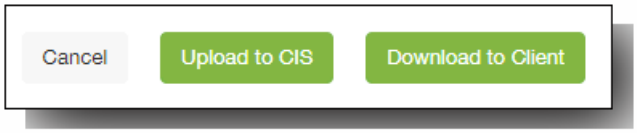




-
-
  -

-
-
-

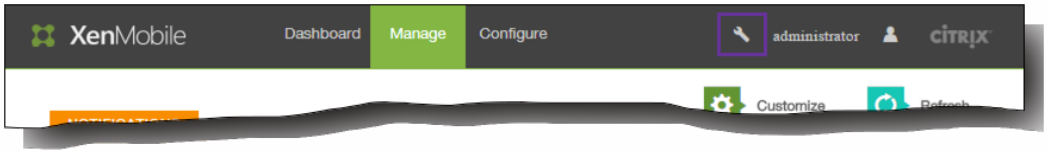


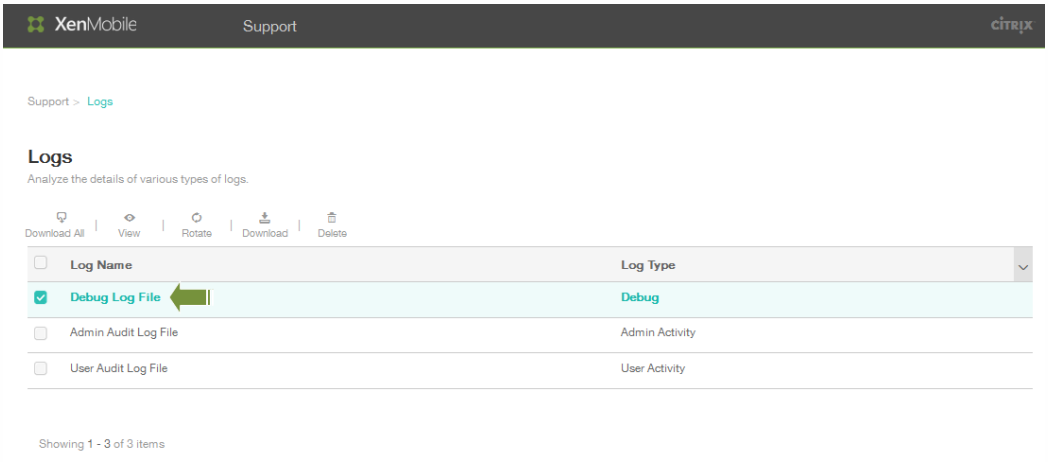


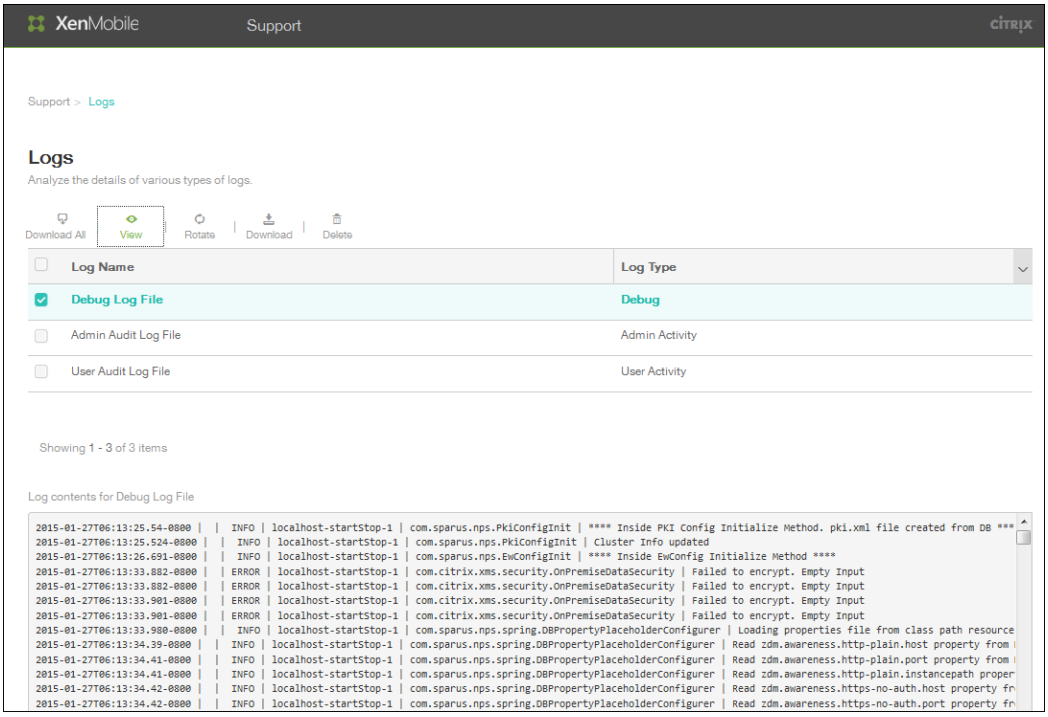
将支持包上载到 Citrix Insight Services

将支持包下载到您的计算机

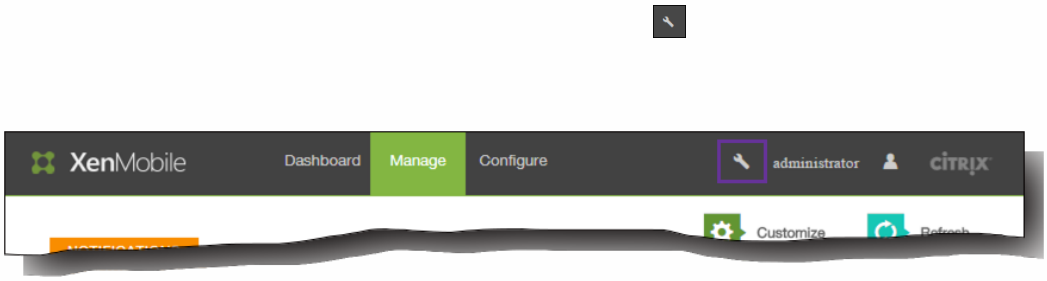
查看调试日志文件

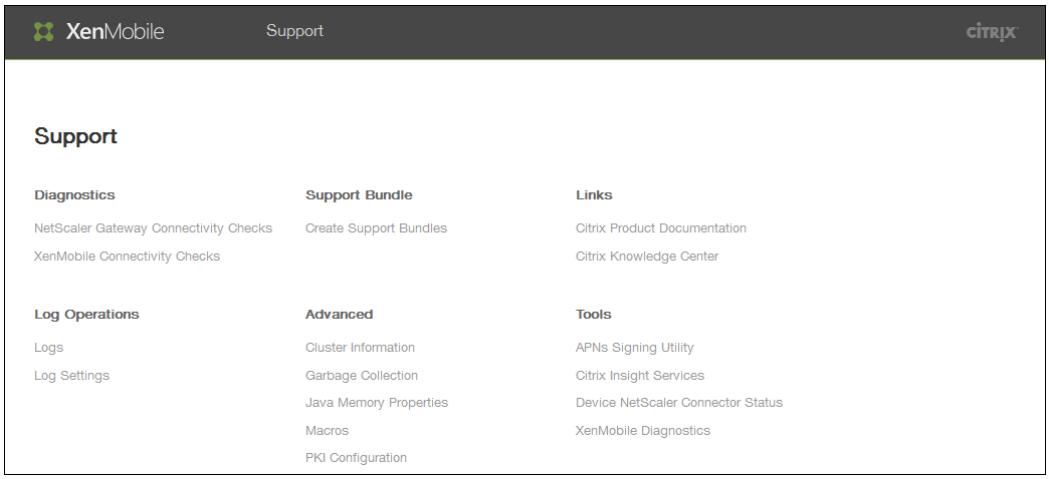


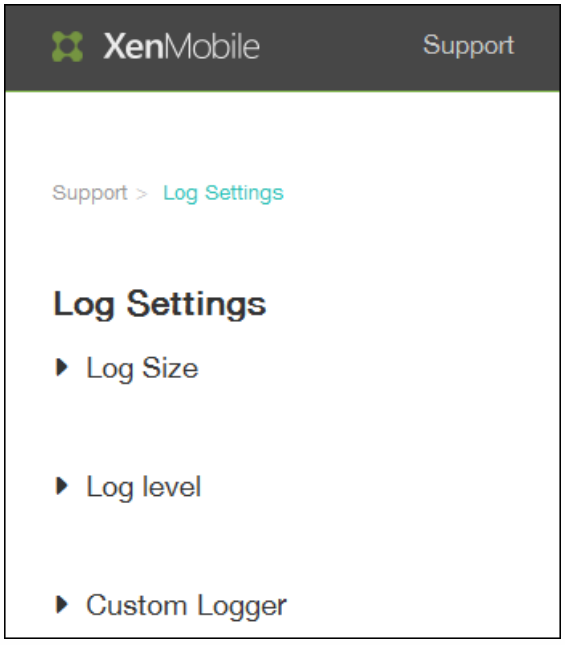




配置日志设置

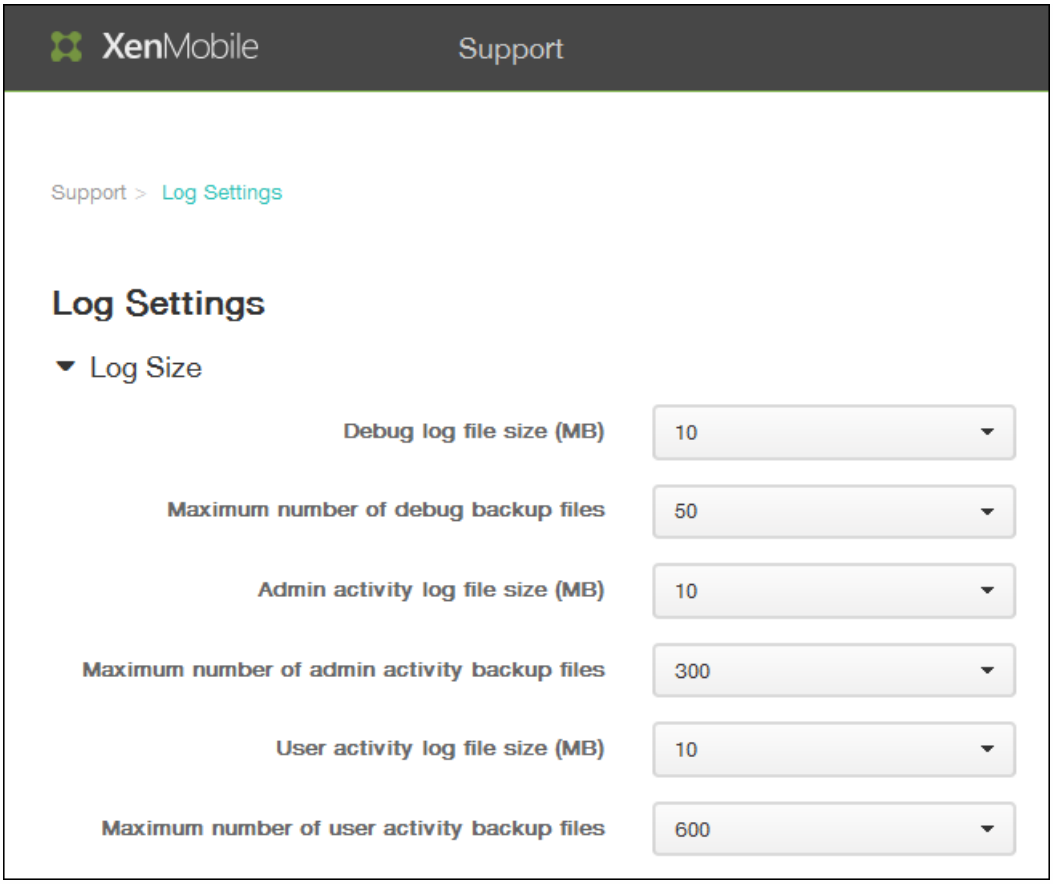






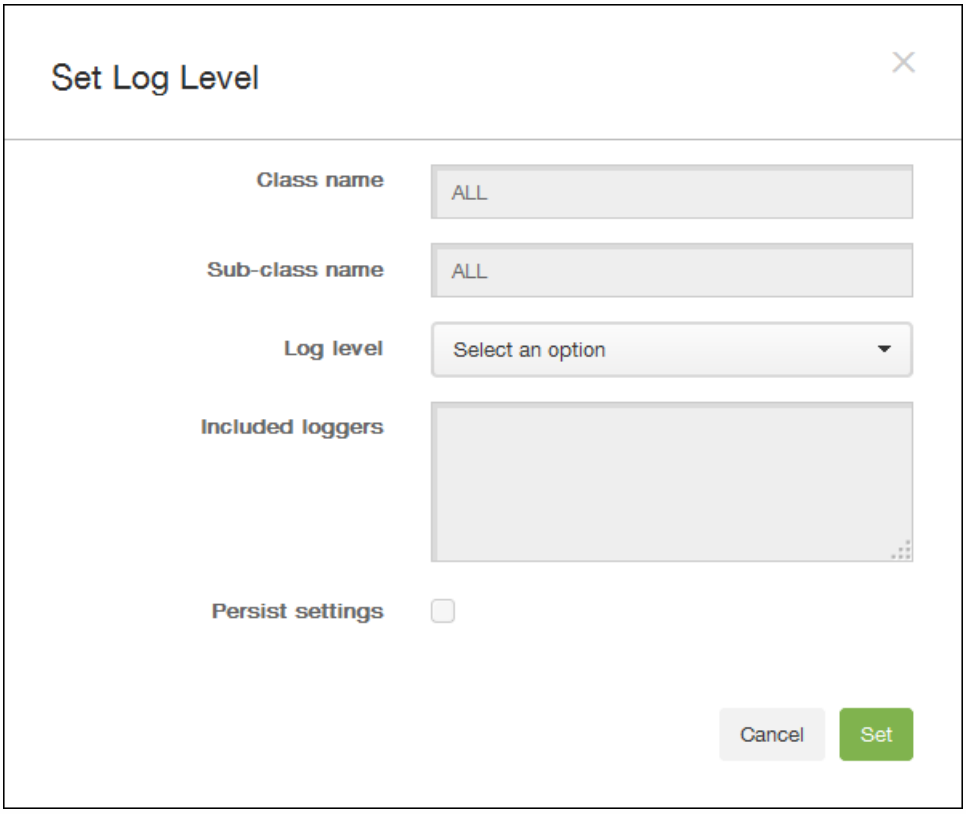
-
-
-

配置“日志大小”选项



配置“日志级别”选项

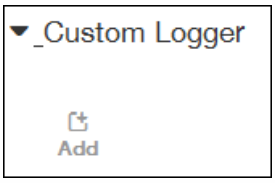
-
-

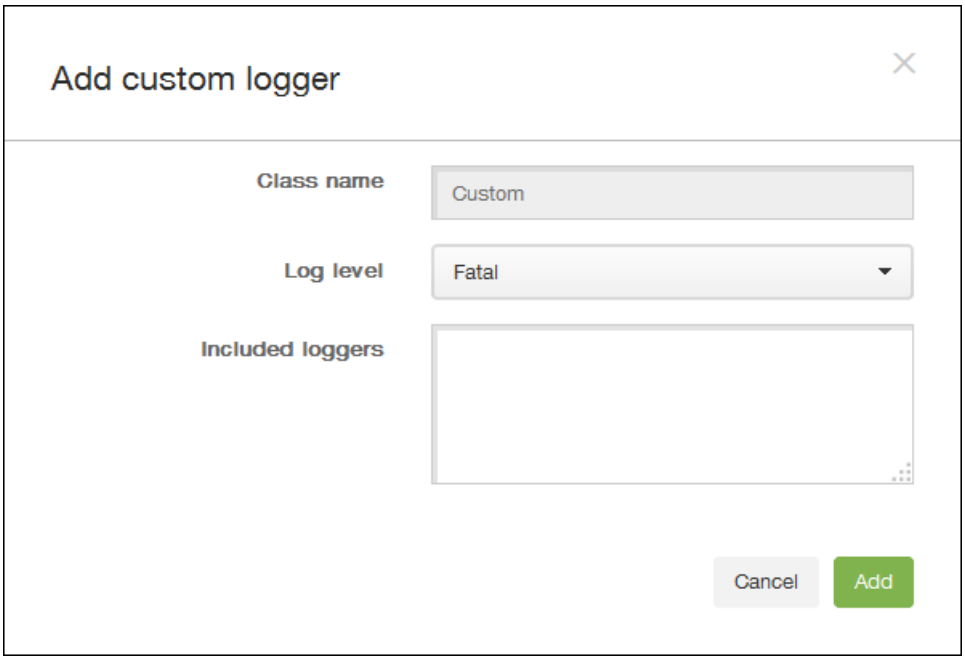


-
-
-
-
-

-
-

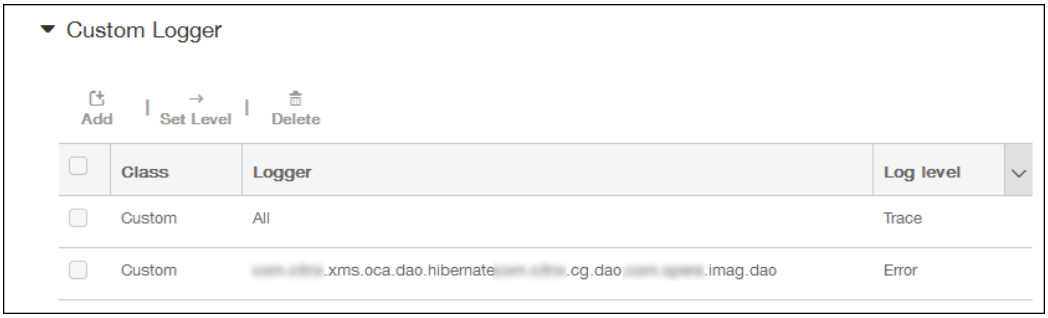
添加自定义日志记录器





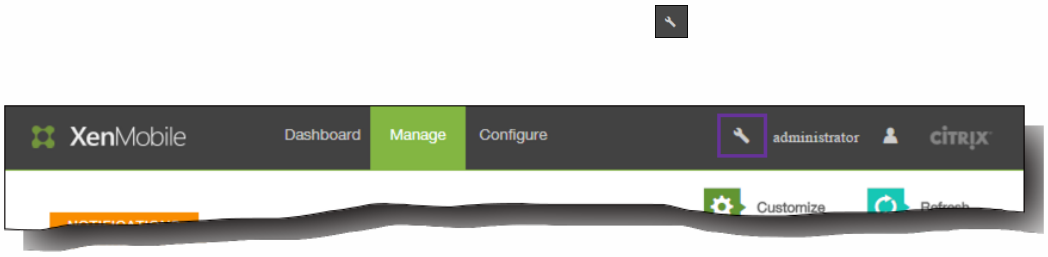
-
-
-
-

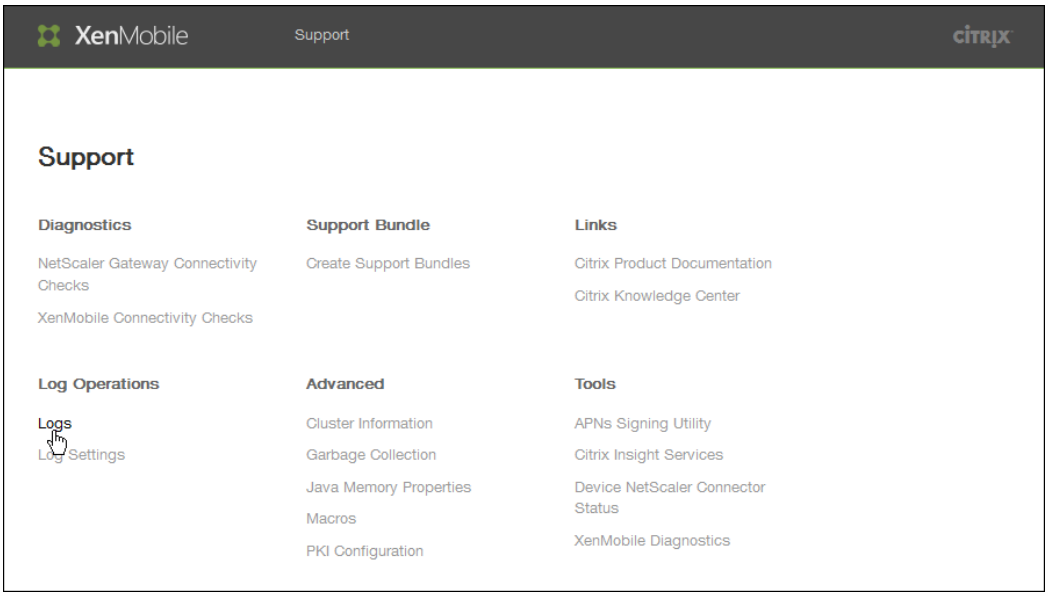
-
-
-

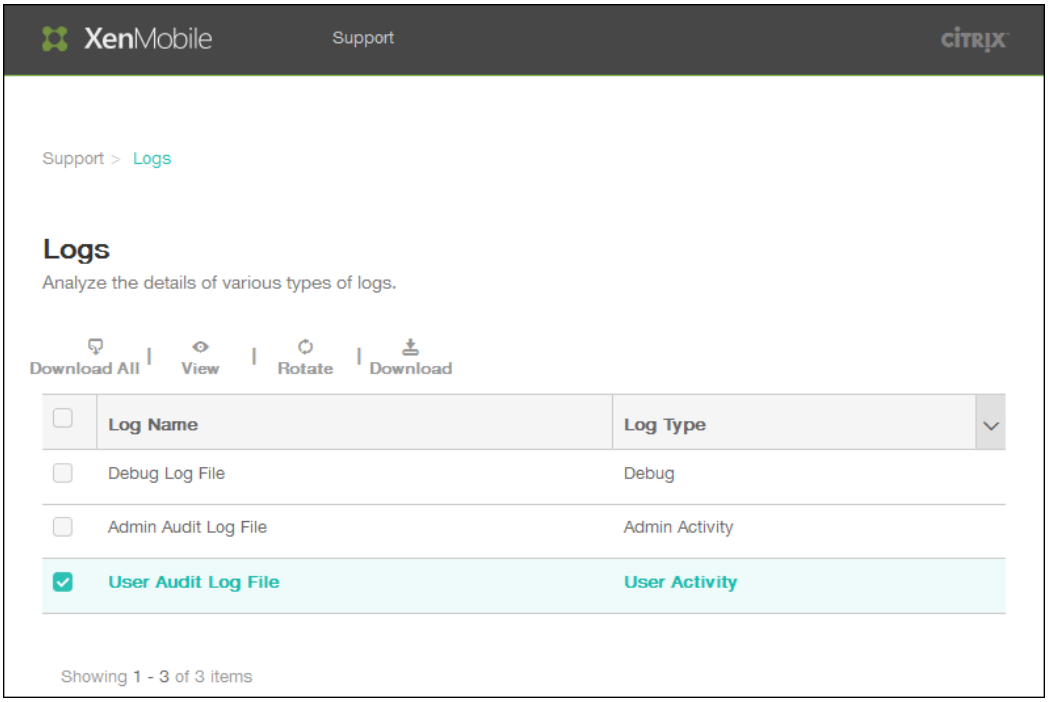


删除自定义日志记录器

在 XenMobile 中查看和分析日志文件

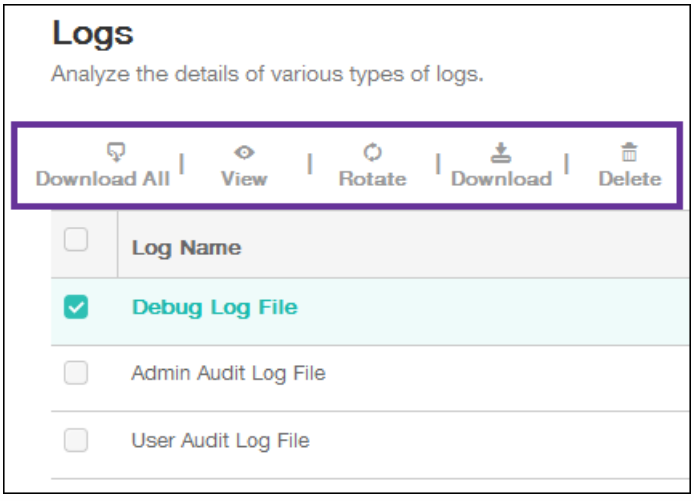




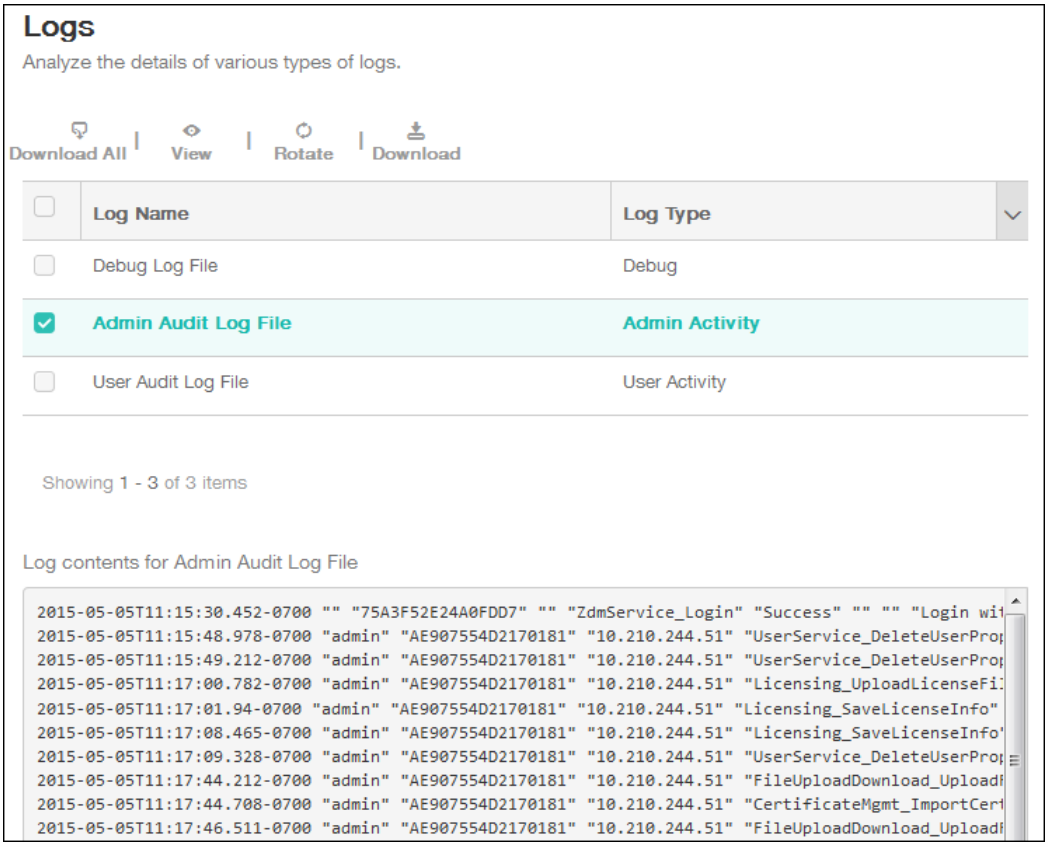


-
-
-

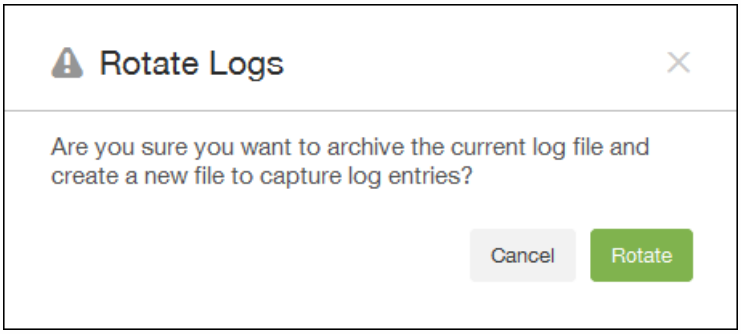
-
-



-
-



-



-
-

XenMobile 命令行接口选项

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]）

“Configuration”（配置）菜单选项

[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]）

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]:）

Type: [mi]（类型: [mi]）

Use SSL (y/n) [y]:（使用 SSL (y/n) [y]:）

Upload Root Certificate (y/n) [y]:（上载根证书 (y/n) [y]:）

Copy or Import (c/i) [c]:（复制或导入 (c/i) [c]:）

“Clustering”（群集）菜单选项

[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]）

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。）

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）。

Cluster is disabled.Please enable it.（群集已被禁用，请将其启用。）

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:）

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。）

Hazlecast Cluster Members:（Hazlecast 群集成员:）

[列出 IP 地址]

NOTE: If an configured node is not part of the cluseter, please reboot that node.（注意: 如果某个配置节点不属于群集，请重新启动此节点。）

“System”（系统）菜单选项

---

[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]）

“Troubleshooting”（故障排除）菜单选项

---

[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]）

Choice: [0 - 7]（选择: [0 - 7]）

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 APIs

Oct 22, 2015

可以在 XenMobile 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

Apr 22, 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。

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”。

已修复的问题

Power Shell/Exchange 管理

在特定的 Microsoft Exchange 环境（主要是 Office 365）中，对 XenMobile Mail Manager 设置限制可有效限制带宽，阻止应用程序发出任何 PowerShell 请求或命令。现在可在 Exchange 配置选项卡中使用备用 PowerShell cmdlet 途径，会将 XenMobile Mail Manager 置于备用快照模式中，此模式可绕过原始数据路径。

通过一个新标志，您可以对非 Microsoft Office 365 环境公开 **AllowRedirection** 标志。使用 Microsoft Exchange 配置选项卡启用此标志。

规则管理

LDAP 本地规则现在针对大型 Active Directory 环境支持任意数量的组。

XenMobile 复制 WorxMail 客户端的设备信息。解决此问题要求您启用 XenMobile Mail Manager 的 Managed Service Provider (MSP) 部分中的正则表达式支持，这样做会过滤返回到 XenMobile 的记录集。满足过滤条件的设备不会返回到 XenMobile。

MSP

从黑莓 Enterprise Server (BES) 数据库中删除的用户现在已从本地数据库中删除。

UI

现在可以将进度对话框类用于发生持续进程的情形。在此类过程中，XenMobile Mail Manager 会发送用户反馈，并向他们提供取消的机会（如果适合）。

现在将新 Microsoft Exchange 实例的默认值设置为 *Shallow*（浅）。

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。

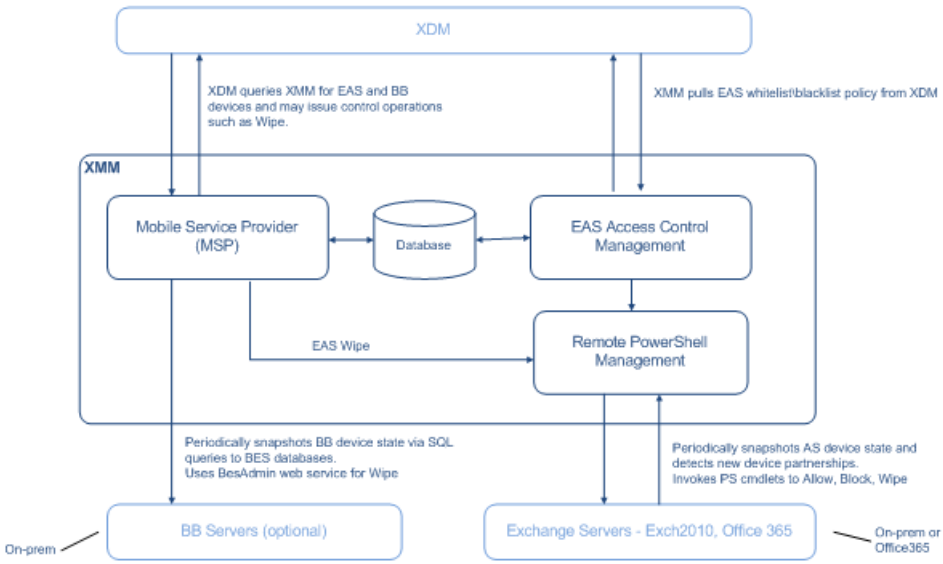
日志记录

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

Oct 13, 2016

下图显示了 XenMobile Mail Manager 的主要组件。 有关详细的参考体系结构图，请参阅《XenMobile 部署手册》文章适用于本地部署的参考体系结构。



这三个主要组件如下：

- **Exchange ActiveSync 访问控制管理**。与 XenMobile 进行通信以从 XenMobile 中检索 Exchange ActiveSync 策略，并将此策略与所有本地定义的策略合并以确定应被允许或拒绝访问 Exchange 的 Exchange ActiveSync 设备。本地策略允许扩展策略规则，以允许 Active Directory 组、用户、设备类型或设备用户代理（通常为移动平台版本）执行访问控制。
- **远程 Powershell 管理**。此组件负责计划和调用远程 PowerShell 命令，以执行 Exchange ActiveSync 访问控制管理编译的策略。此组件定期创建 Exchange ActiveSync 数据库的快照，以检测新的或已更改的 Exchange ActiveSync 设备。
- 移动服务提供商。提供 Web 服务界面，以便 XenMobile 可以查询 Exchange ActiveSync 和/或黑莓设备以及对这些设备执行“擦除”等问题控制操作。

系统要求和必备条件

Apr 22, 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

XenMobile Mail Manager 必备条件

- 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

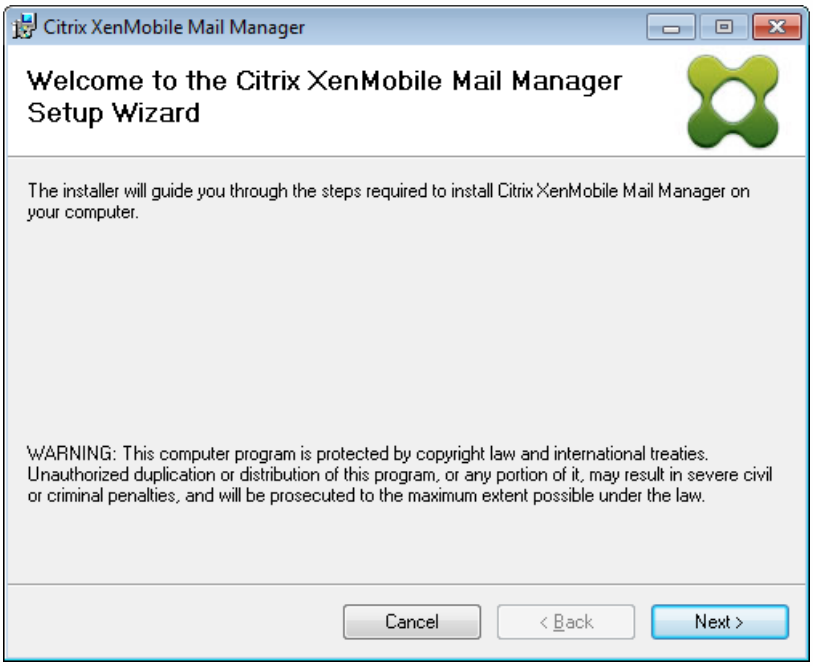
- **权限**。Exchange 基于角色的访问控制 (RBAC) 不在本文档的范围内。话虽如此，至少，在 Exchange 配置 UI 中指定的凭据必须能够连接到 Office 365，并且具有执行以下指定 Exchange 的 PowerShell cmdlet 的完全权限：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- 提供的凭据必须已获得授权，可以通过远程 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

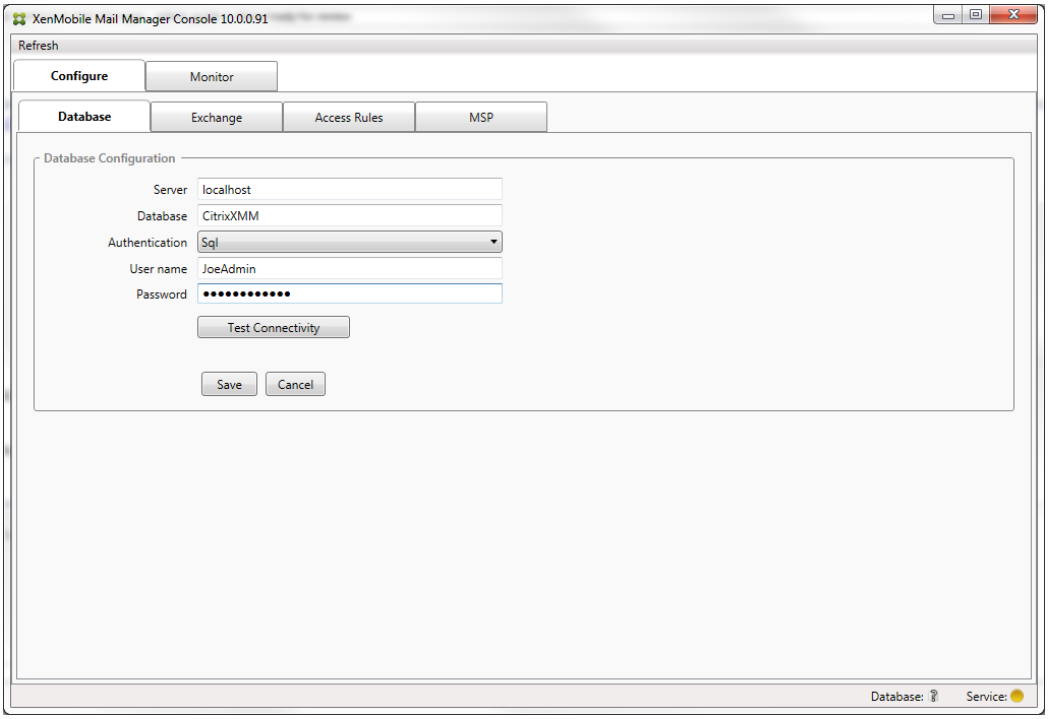
Nov 20, 2015

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。

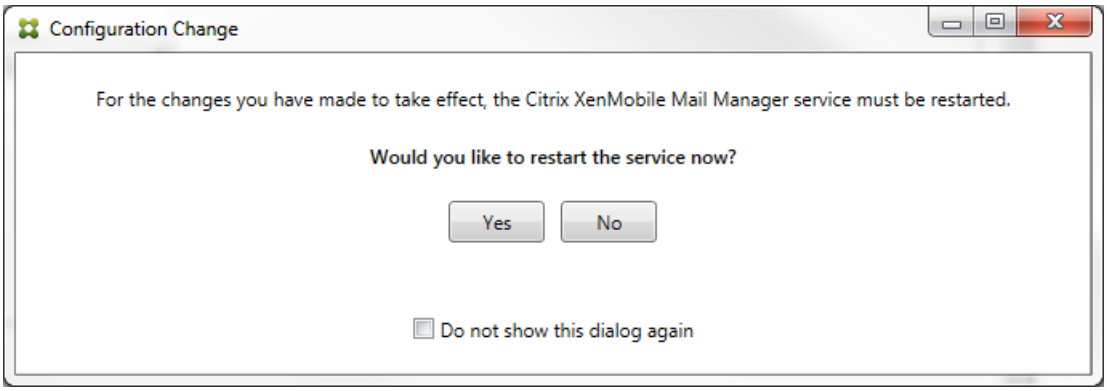


2. 从开始菜单中打开 XenMobile Mail Manager。
3. 配置以下数据库属性：
   1. 选择配置 > 数据库选项卡。
   2. 输入 SQL Server 的服务器名称（默认为 localhost）。
   3. 将数据库保留为默认 CitrixXmm。
   4. 选择以下用于 SQL 的身份验证模式之一：
      - Sql。输入有效 SQL 用户的用户名和密码。
      - Windows 集成。如果选择此选项，XenMobile Mail Manager Service 的登录凭据必须更改为具有访问 SQL Server 权限的 Windows 帐户。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。

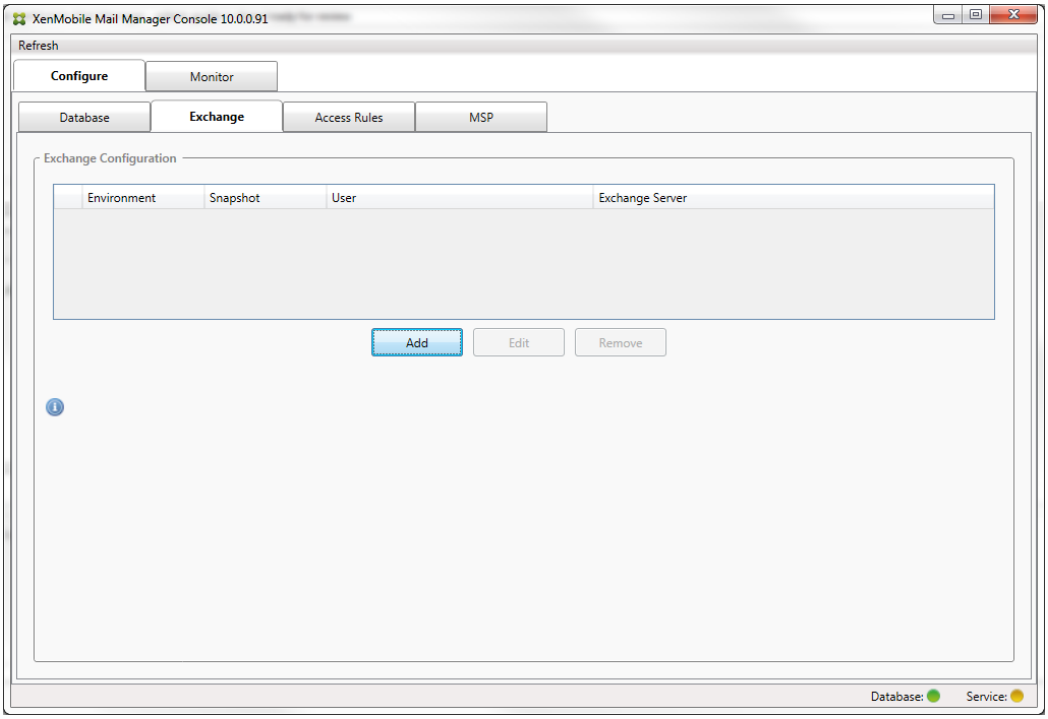


5. 单击测试连接检查是否可以连接到 SQL Server，然后单击保存。

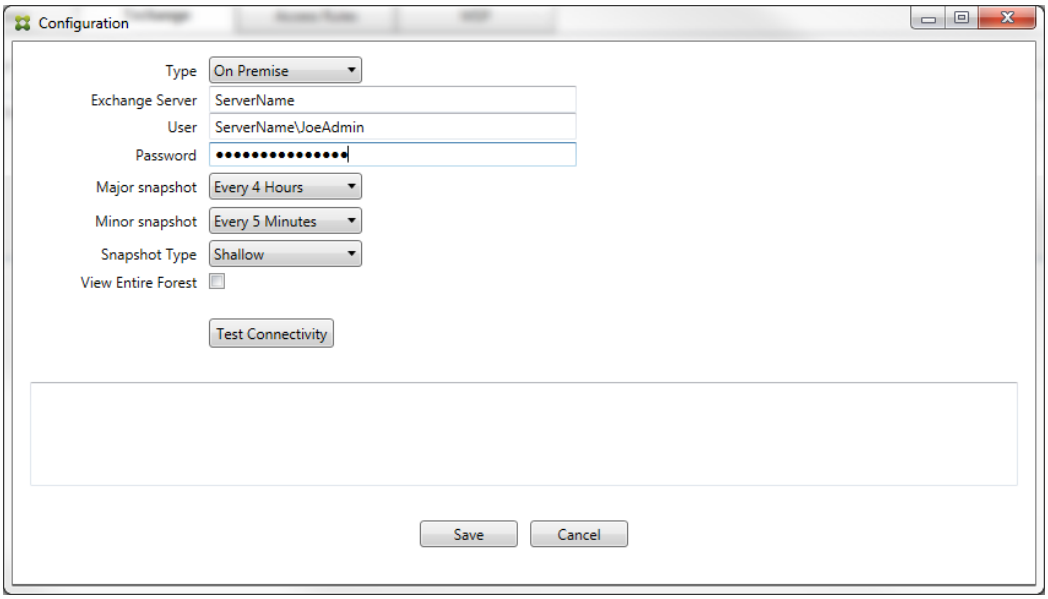
4. 此时将显示一条消息，提示您重新启动服务。 单击是。



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。

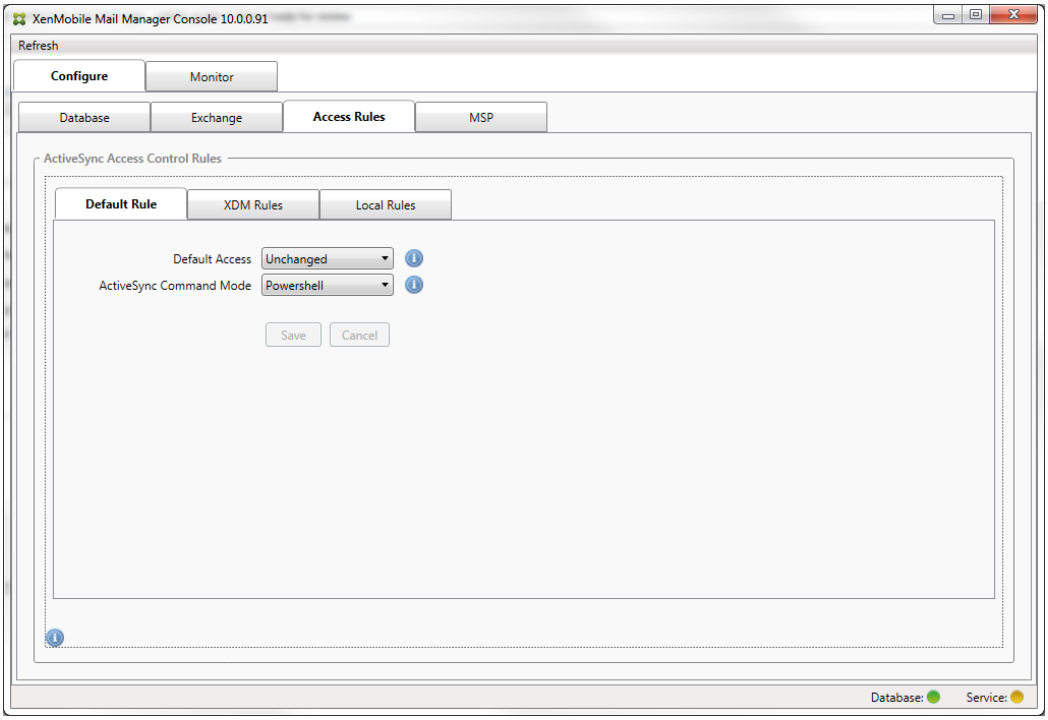


3. 单击添加。
4. 选择 Exchange Server 环境类型，On Premise（内部部署）或 Office 365。

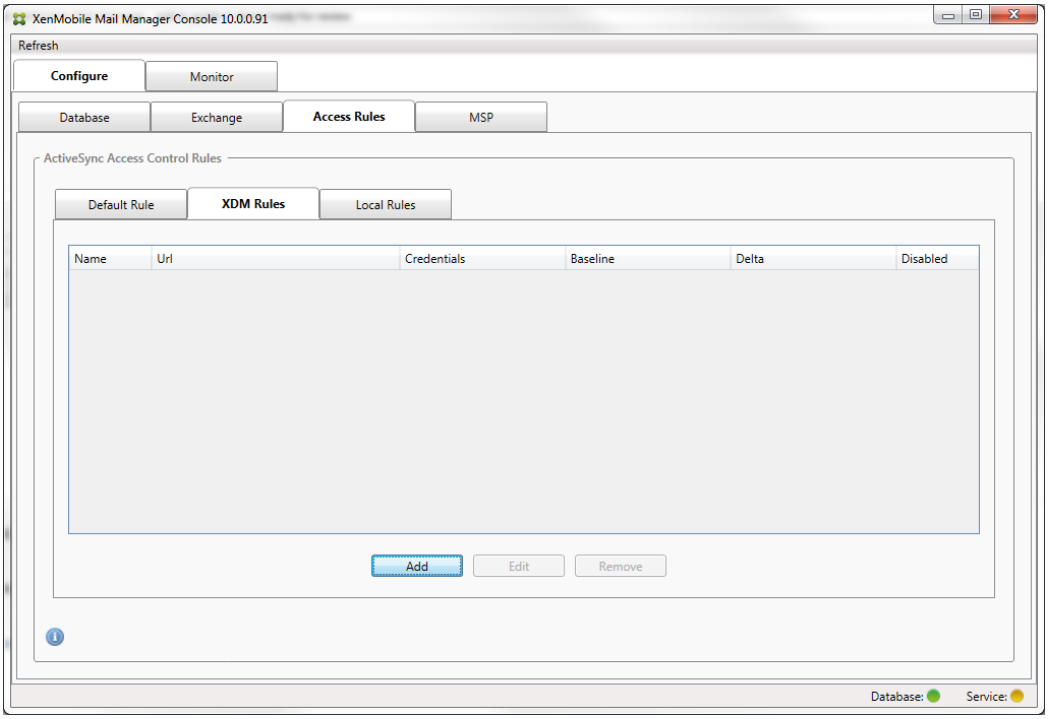


5. 如果选择 On Premise（内部部署），请输入要用于远程 Powershell 命令的 Exchange Server 的名称。
6. 输入在要求部分中指定的 Exchange Server 上具有适当权限的 Windows 身份的用户名。
7. 输入用户的密码。
8. 选择运行主要快照的计划。 主要快照检测每个 Exchange ActiveSync 合作关系。
9. 选择运行次要快照的计划。 次要快照检测新创建的 Exchange ActiveSync 合作关系。
10. 选择快照类型：Deep（深）或 Shallow（浅）。 浅快照通常更快并且足以执行 XenMobile Mail 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。

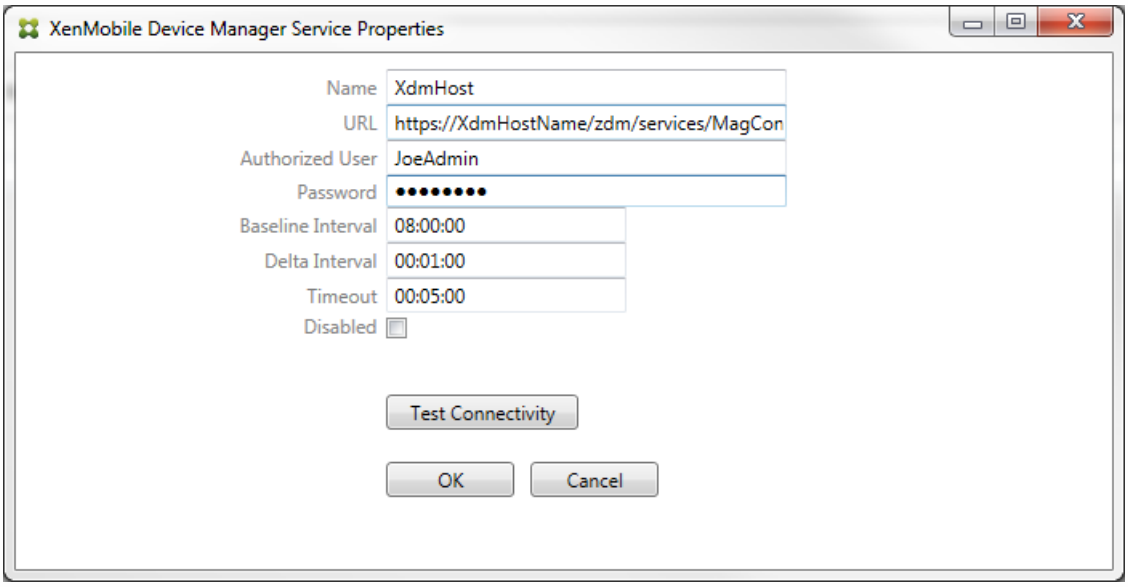
6. 配置访问规则：
    1. 选择配置 > 访问规则选项卡。



    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。

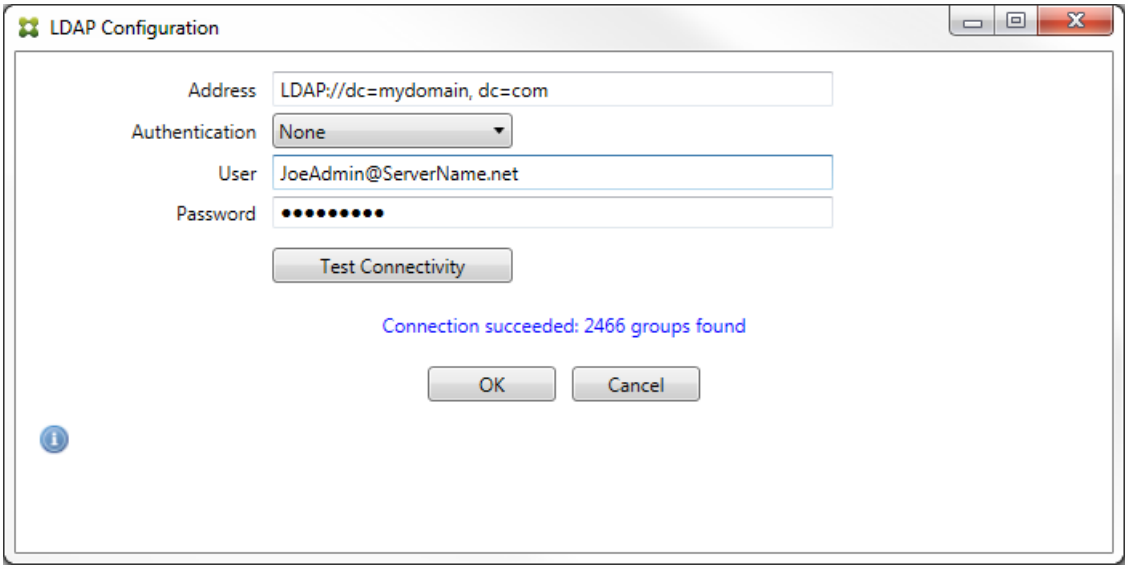


1. 单击添加。
2. 为 XDM 规则输入名称，例如 XdmHost。



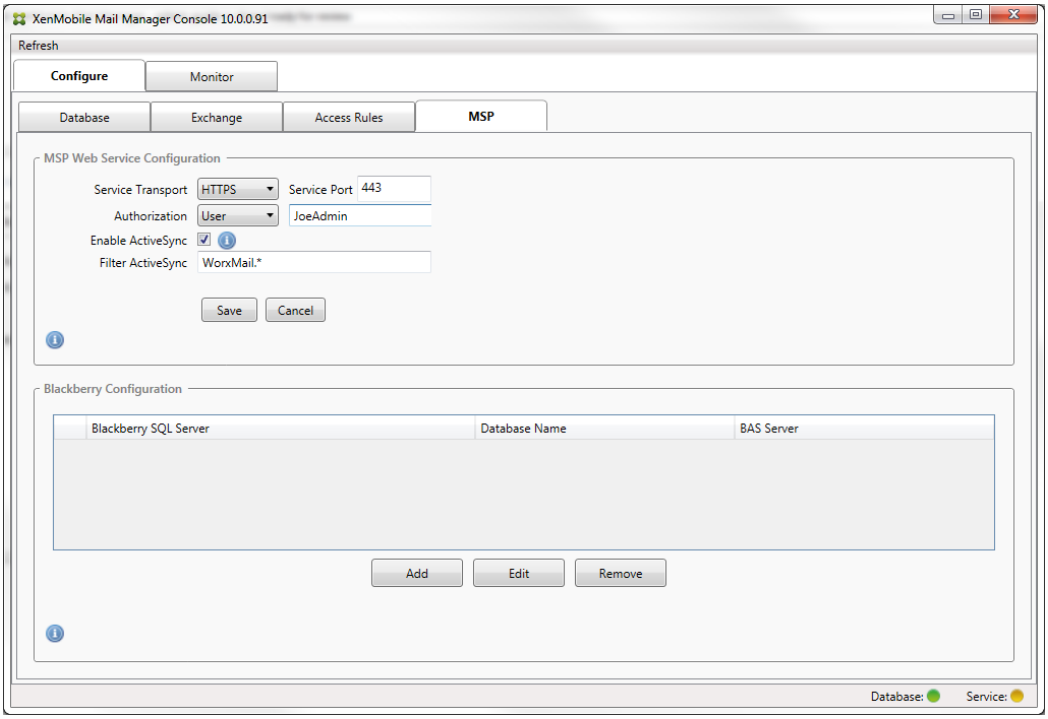
3. 修改 URL 字符串以引用 XenMobile 服务器；例如，如果服务器名称为 XdmHost，输入 http://XdmHostName/zdm/services/MagConfigService。
4. 在该服务器上输入授权用户。
5. 输入用户密码。
6. 保留 Baseline Interval（基准时间间隔）、Delta Interval（增量时间间隔）和 Timeout values（超时值）的默认值。
7. 单击测试连接，检查与服务器的连接。
   注意：如果选中“已禁用”复选框，XenMobile Mail Service 将不会从 XenMobile 服务器收集策略。
8. 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。



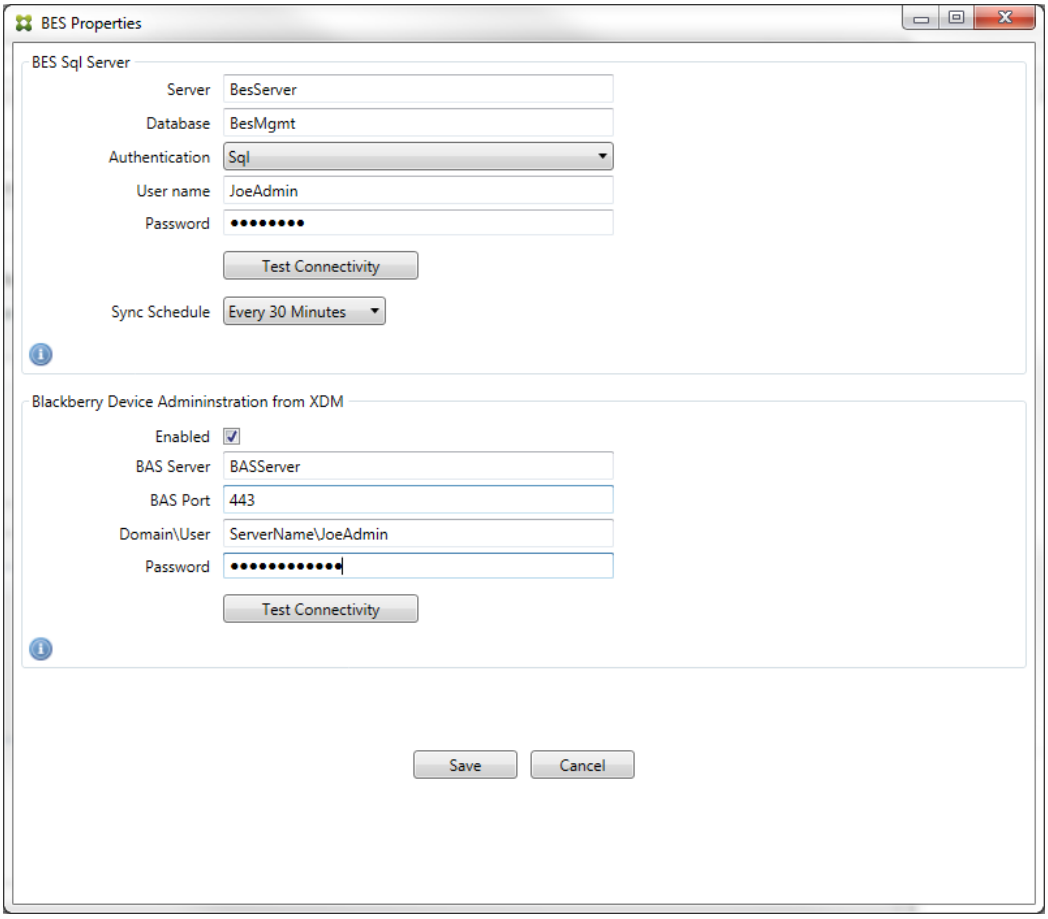
2. 您可以基于 ActiveSync Device ID（ActiveSync 设备 ID）、设备类型、AD Group（AD 组）、用户或设备 UserAgent（用户代理）添加本地规则。 在列表中选择适当的类型。 有关详细信息，请参阅 XenMobile Mail Manager 访问控制规则。
3. 在文本框中输入文本或文本片段。 也可单击查询按钮，查看与片段匹配的实体。
   注意：对于除组以外的所有类型，系统依赖在快照中找到的设备。因此，如果刚刚开始且尚未完成快照，则没有实体可用。
4. 选择一个文本值，然后单击允许或拒绝，将其添加到右侧的 Rule List（规则列表）窗格中。 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。



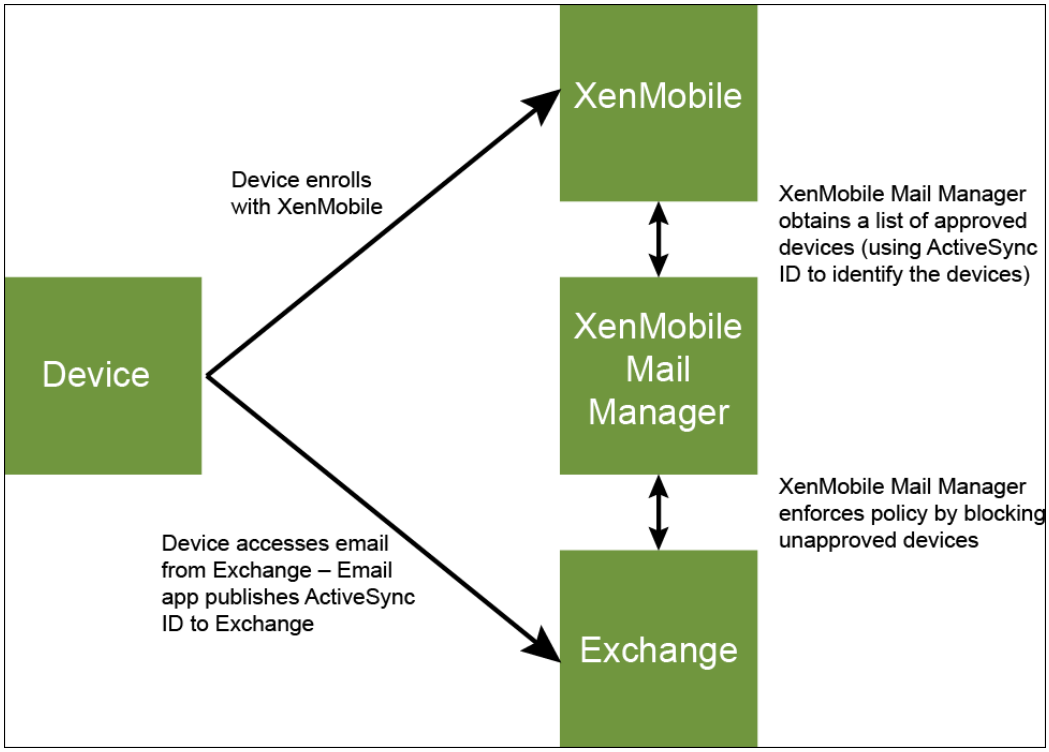
3. 输入 BES Management 数据库的数据库名称。
4. 选择身份验证模式。 如果选择 Windows 集成身份验证，则 XenMobile Mail Manager Service 的用户帐户就是用于连接 BES SQL Server 的帐户。
   注意：如果还为 XenMobile Mail Manager 数据库连接选择了 Windows 集成，则必须同时为此处指定的 Windows 帐户提供 XenMobile Mail Manager 数据库的访问权限。
5. 如果选择 SQL authentication（SQL 身份验证），请输入用户名和密码。
6. 设置 Sync 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

Nov 20, 2015

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

Nov 20, 2015

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。

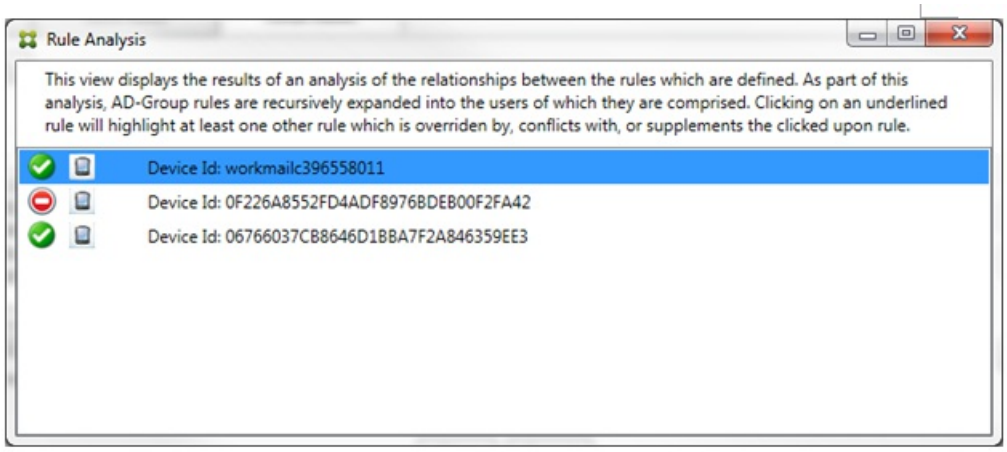
在为相同的字段定义了多条规则的情况下，分析特别有用。您可以对规则之间的关系进行故障排除。请从规则字段的角度来执行分析；例如，规则是在组中基于匹配的字段进行分析的（例如 ActiveSync 设备 ID、ActiveSync 设备类型、用户、用户代理等）。

规则术语：

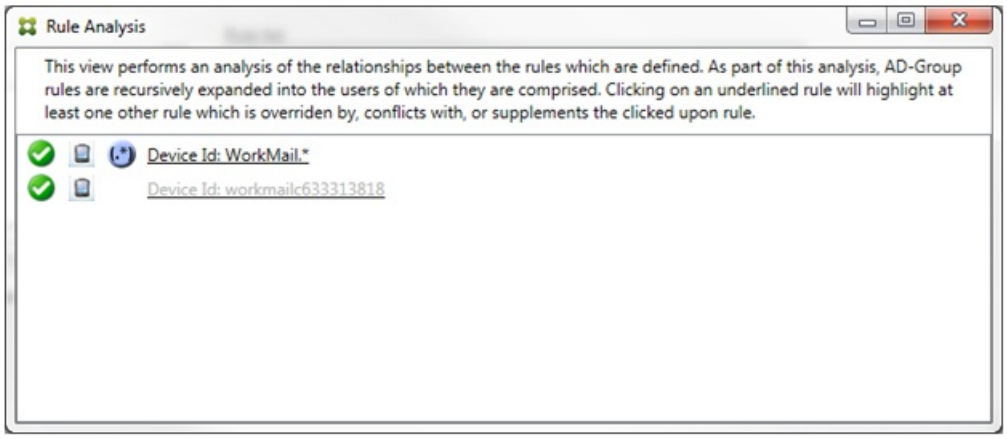
- **覆盖规则**。当多条规则可以应用到同一设备时会发生覆盖。因为规则是按照列表中的优先级进行评估的，可能会应用的后面的规则实例可能永远不会被评估。
- **冲突规则**。当多条规则可以应用到同一设备但访问状态（允许/阻止）不匹配时会发生冲突。如果冲突规则不是正则表达式规则，冲突将始终隐式包含覆盖
- **补充规则**。当多条规则是正则表达式规则时会发生补充，因此可能需要确保两个（或多个）正则表达式可以合并为一个正则表达式，或者不复制功能。补充规则的访问状态（允许/阻止）可能还会发生冲突。
- **主要规则**。主要规则是已在对话框内单击的规则。规则通过围绕它的实线框可视化地指示出来。该规则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

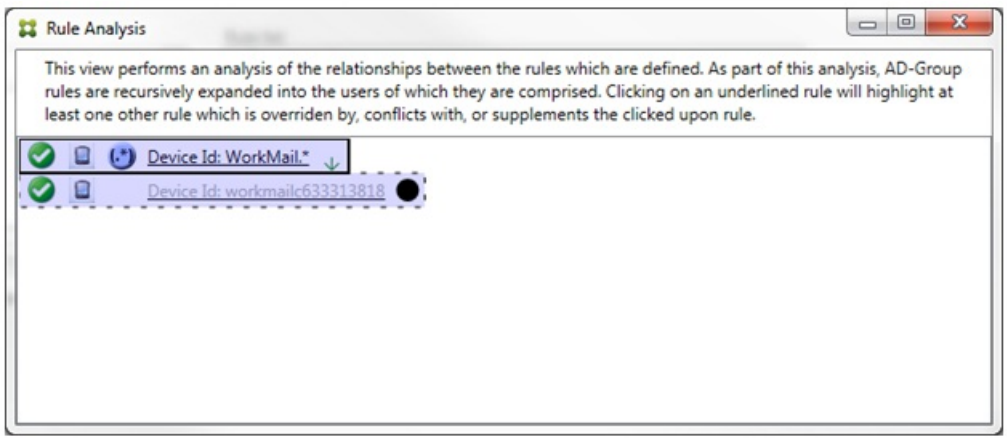
当没有冲突、覆盖或补充时，Rule Analysis （规则分析）对话框中不包含带有下划线的条目。单击任何没有影响的项目；例如，正常选定项目的视觉效果将会出现。



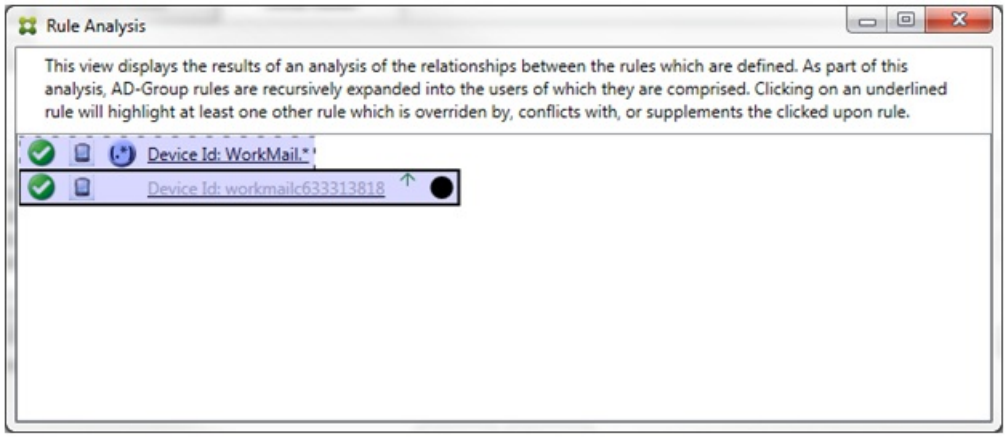
当出现覆盖时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。至少有一条辅助规则将以较浅字体显示，指示该规则已被优先级较高的规则覆盖。您可以单击覆盖的规则以了解覆盖该规则的一条或多条规则。任何时间覆盖的规则都由于规则是主要规则或辅助规则而突出显示，并且将在它旁边将显示一个黑色圆圈，以进一步指示该规则处于不活动状态。例如，在单击该规则之前，对话框显示如下：



单击优先级最高的规则时，对话框显示如下：

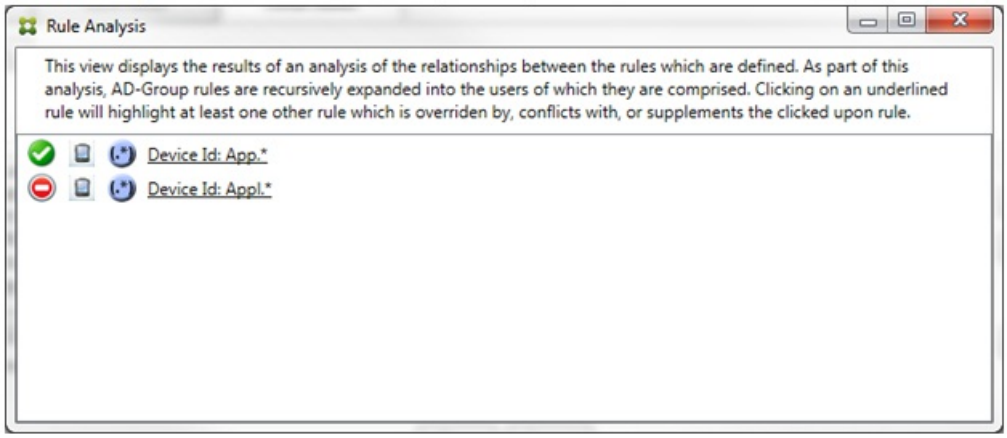


在此示例中，正则表达式规则 WorkMail.* 是主要规则（以实线框指示），常规规则 workmailc633313818 是辅助规则（以虚线框指示）。辅助规则旁边的黑点是一个视觉提示，可进一步指示由于它的前面有较高优先级的正则表达式而处于不活动状态（永远不会被评估）。单击覆盖的规则后，对话框显示如下：

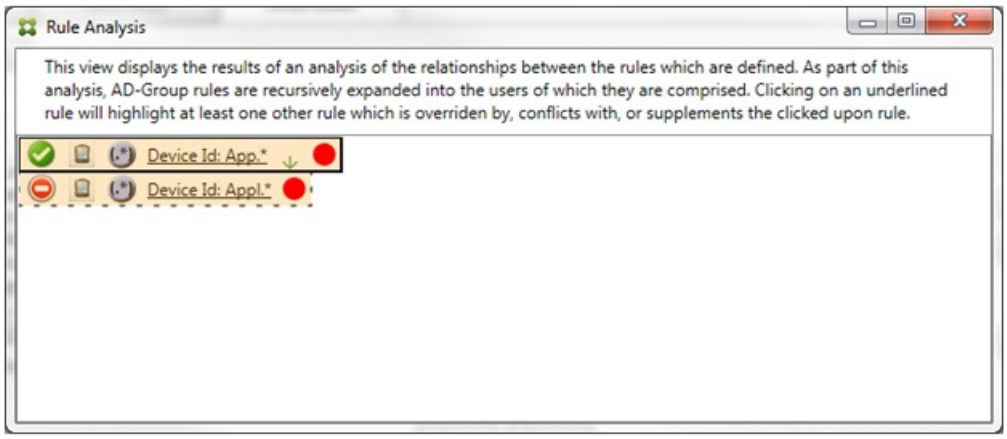


在上例中，正则表达式规则 WorkMail.* 是辅助规则（以虚线框指示），常规规则 workmailc633313818 是主要规则（以实线框指示）。对于这一简单的示例，没有太大差异。对于更为复杂的示例，请参阅本主题中后面所述的复杂表达式示例。在定义了许多规则的情景中，单击覆盖的规则将快速识别已覆盖该规则的一条或多条规则。

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：

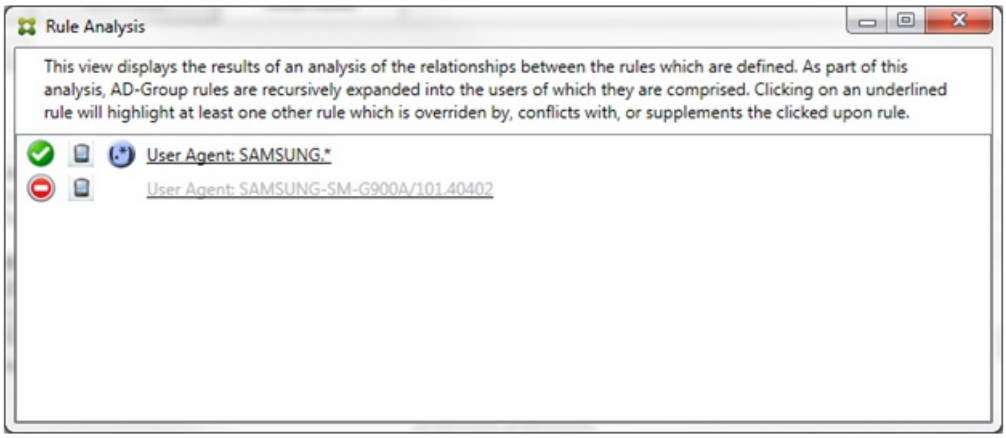


检查这两条正则表达式规则即可明显发现，第一条规则允许设备 ID 包含“App”的所有设备，第二条规则拒绝设备 ID 包含 Appl 的所有设备。此外，即使第二条规则拒绝了设备 ID 包含 Appl 的所有设备，也不会拒绝符合条件的设备，因为允许规则的优先级较高。单击第一条规则后，对话框显示如下：



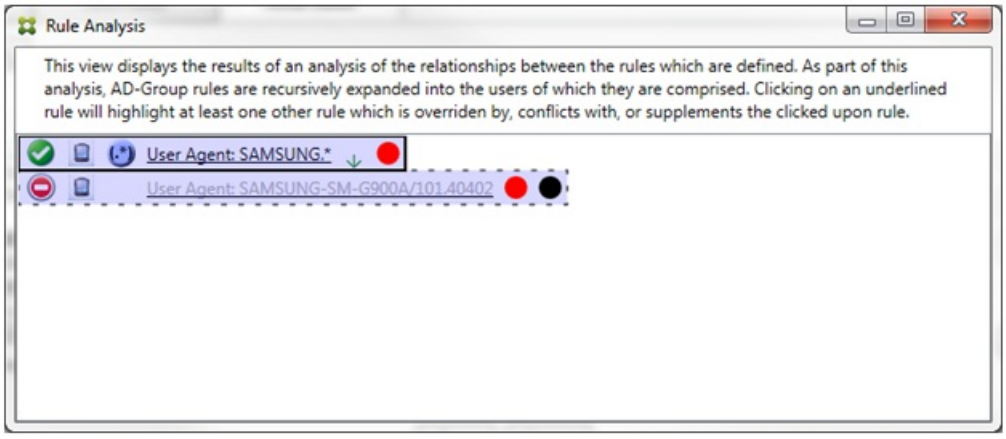
在上述情景中，主要规则（正则表达式规则 App.*）和辅助规则（正则表达式规则 Appl.*）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

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。



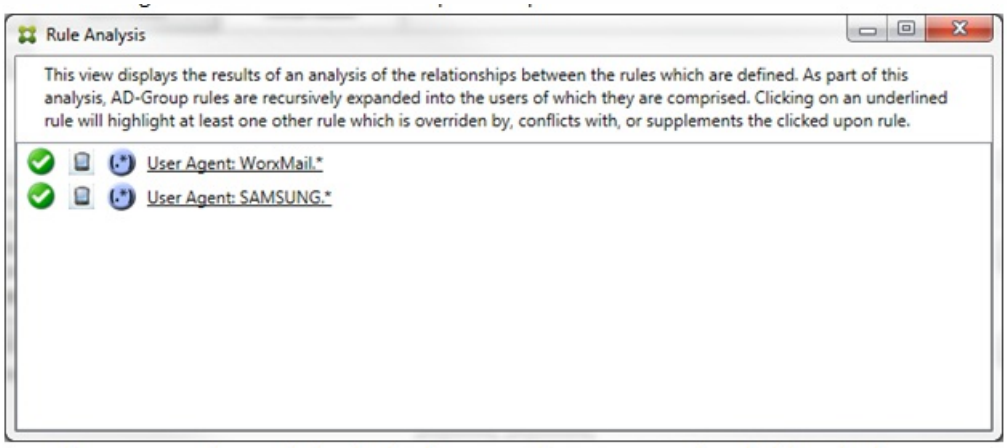
在上例中，显而易见，第一条规则（正则表达式规则 SAMSUNG.*）不仅覆盖下一条规则（常规规则 SAMSUNG-SM-G900A/101.40402），而且这两条规则的访问状态有所不同（主要规则指定“允许”，辅助规则指定“阻止”）。第二条规则（常规规则 SAMSUNG-SM-G900A/101.40402）以较浅文本显示，指示该规则已被覆盖，并因此处于不活动状态。

单击正则表达式规则后，对话框显示如下：

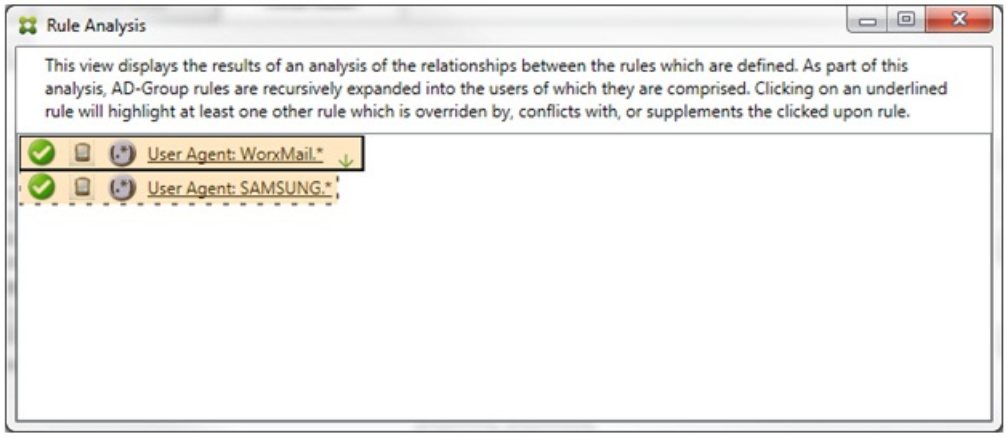


主要规则（正则表达式规则 SAMSUNG.*）后跟一个红点，指示其访问状态与一条或多条辅助规则发生冲突。辅助规则（常规规则 SAMSUNG-SM-G900A/101.40402）后跟一个红点，指示其访问状态与主要规则发生冲突，以及如果后跟黑点，则进一步指示该规则已被覆盖，并因此处于不活动状态。

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：



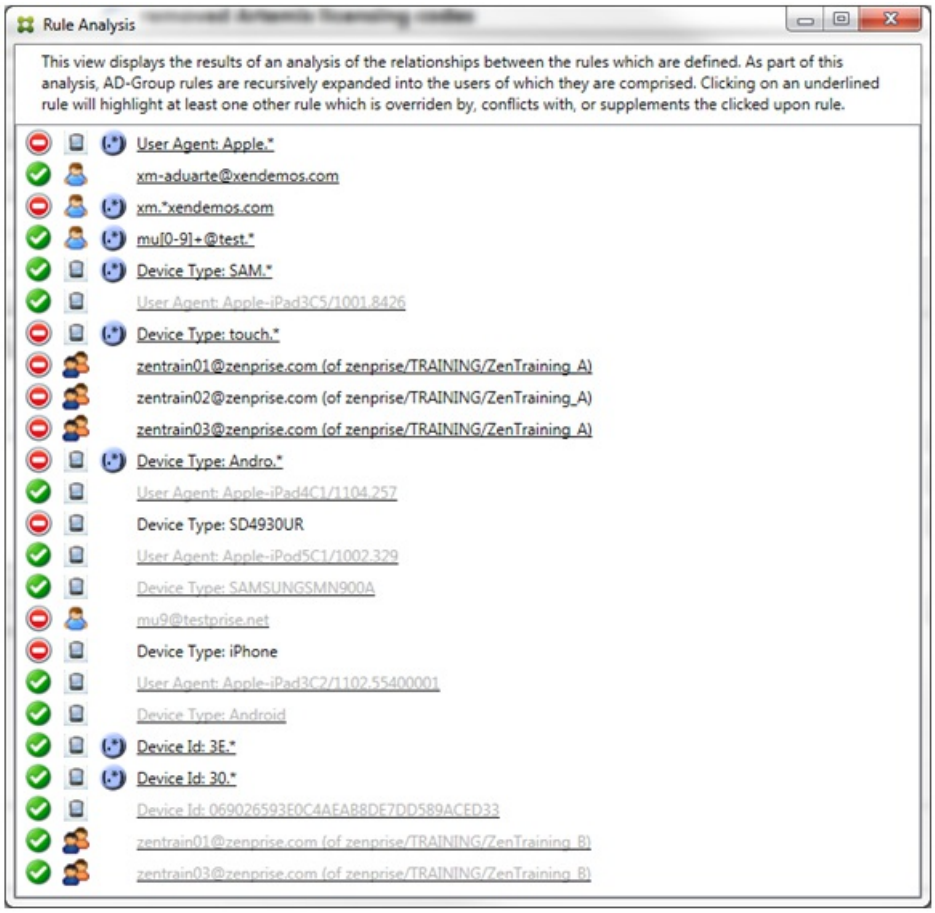
目测会很容易发现这两条规则都是正则表达式规则，都已应用到 XenMobile Mail Manager 中的 ActiveSync 设备 ID 字段。单击第一条规则后，对话框显示如下：



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

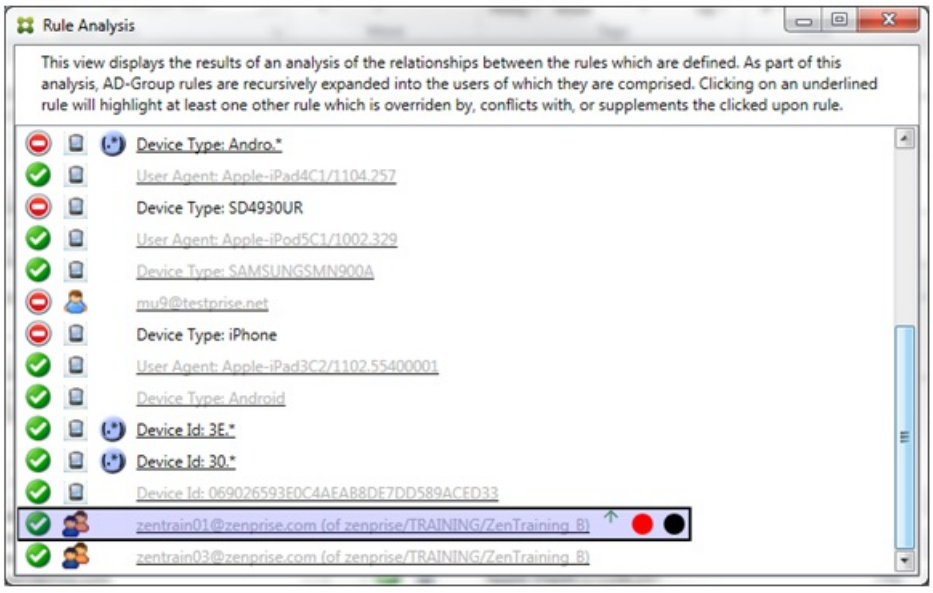
许多潜在的覆盖、冲突或补充都可能会发生，使其不可能举例说明所有可能的情景。下例探讨了不会执行的操作，同时还阐明了规则分析视觉构建的强大功能。大多数项目在下图中加了下划线。许多项目以较浅的字体显示，指示存在问题的规则已被优先级较高的规则以某种方式覆盖。多条正则表达式规则也包括在列表中，由 (.*) 图标指示。



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。

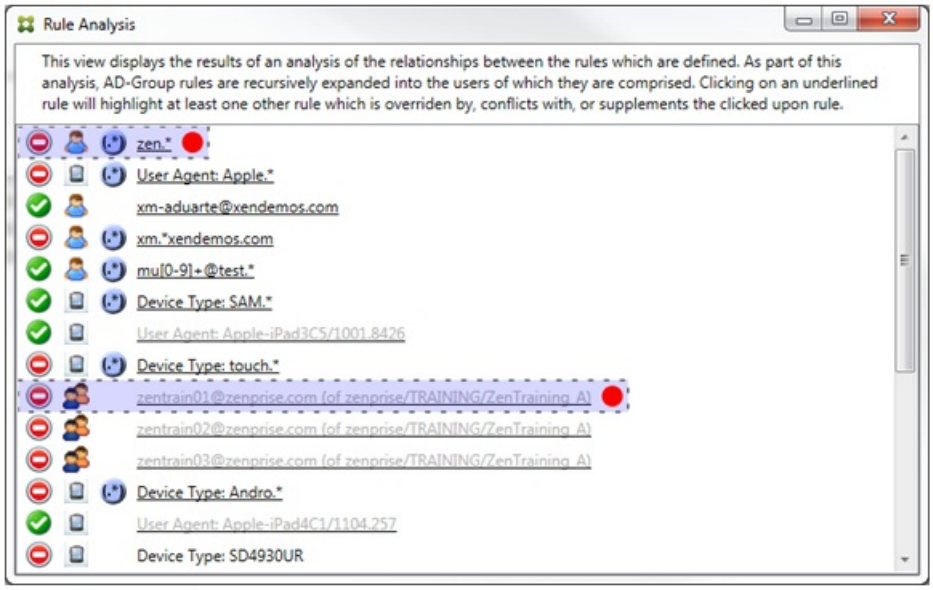
示例 1：本示例调查了覆盖 zentrain01@zenprise.com 的原因。



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：

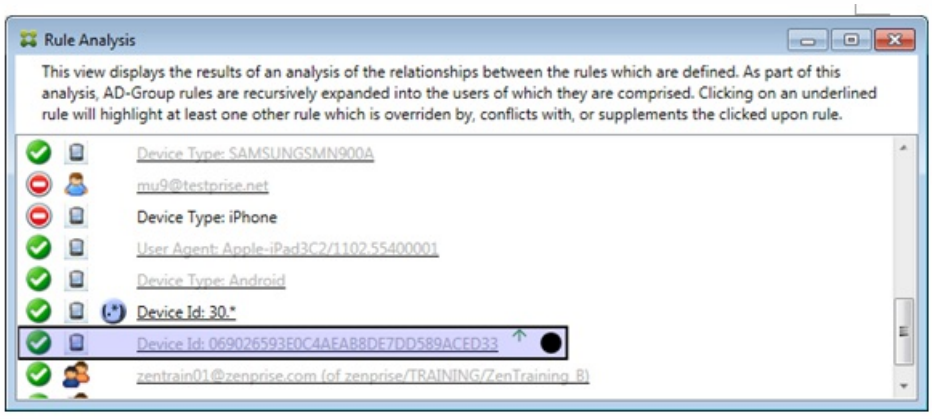
- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示一条或多条辅助规则都能够在该箭头上方找到）。
- 后跟一个红色圆圈和一个黑色圆圈，分别指示一条或多条辅助规则与其访问状态存在冲突，并且主要规则已被覆盖且因此处于不活动状态。

向上滚动时，您会看到以下内容：



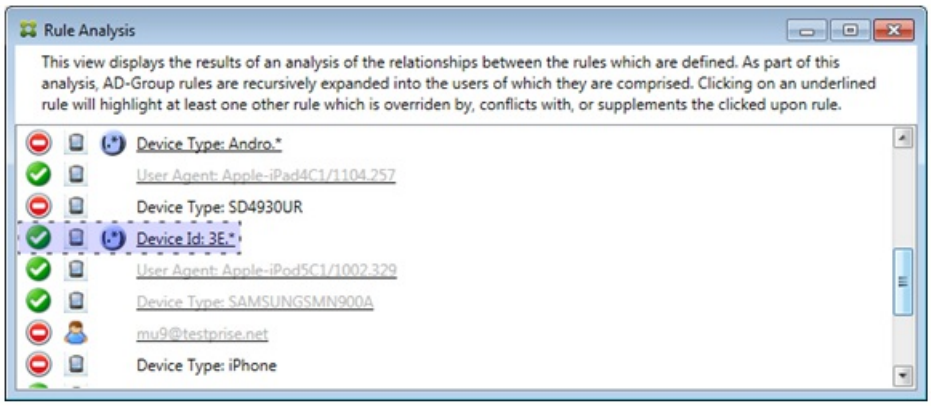
在这种情况下，有两条辅助规则覆盖主要规则：正则表达式规则 zen.* 和常规规则 zentrain01@zenprise.com（属于 zenprise/TRAINING/ZenTraining A）。对于后一条辅助规则，出现了以下情况：Active Directory 组规则 ZenTraining A 包含用户 zentrain01@zenprise.com，Active Directory 组规则 ZenTraining B 也包含用户 zentrain01@zenprise.com。但是，由于辅助规则的优先级高于主要规则，因此主要规则被覆盖。主要规则的访问状态是“允许”，并且由于这两条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。

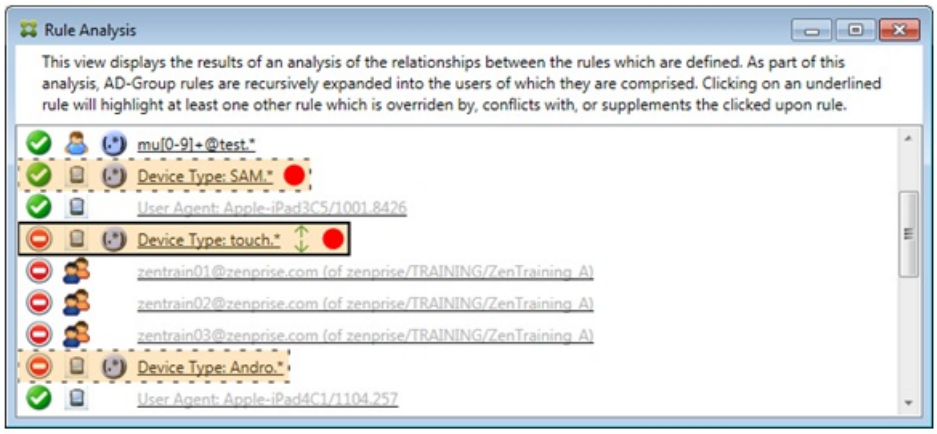


在这种情况下：一条辅助规则将覆盖主要规则：正则表达式 ActiveSynce 设备 ID 规则 3E.*。由于正则表达式 3E.* 将与 069026593E0C4AEAB8DE7DD589ACED33 匹配，因此，主要规则永远不会被评估。

如何分析补充和冲突

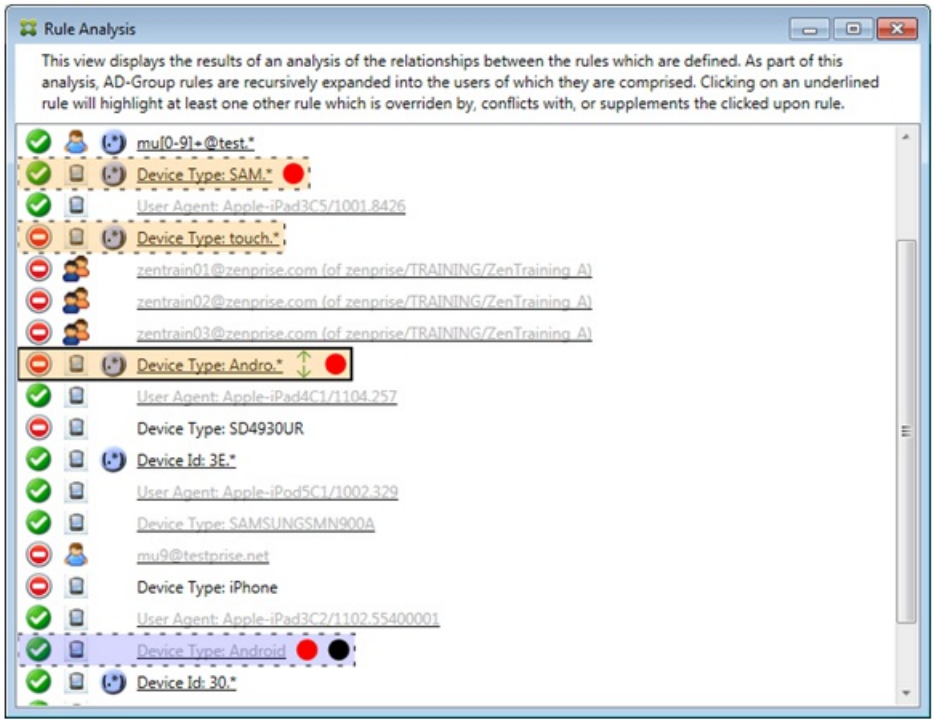
在这种情况下，主要规则是正则表达式 ActiveSync 设备类型规则 touch.*。特性如下：

- 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

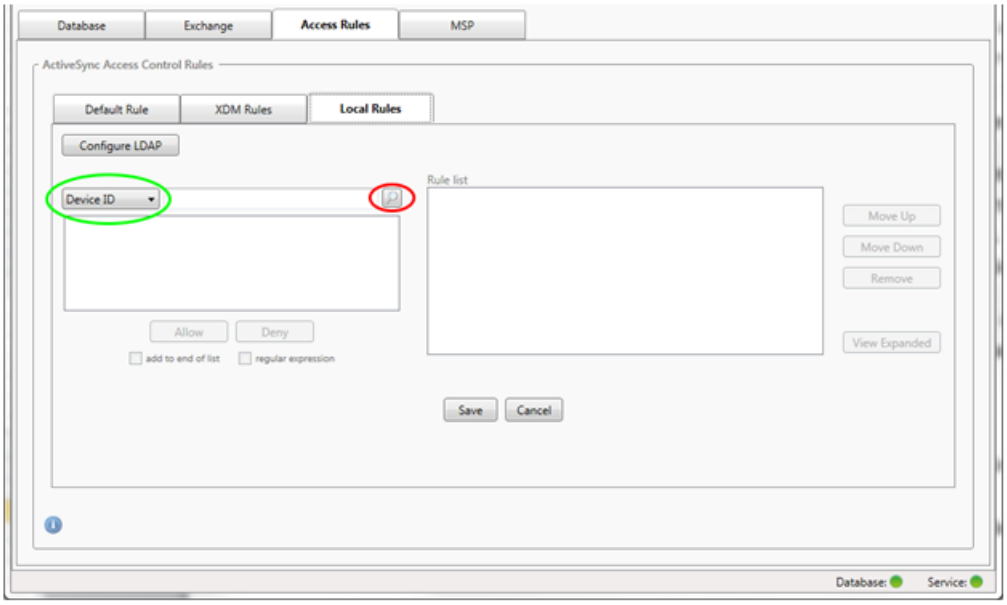
本示例探讨了规则关系如何始终从主要规则的角度建立。上例显示了如何单击应用到设备类型值为 touch.* 的规则字段的正则表达式规则。单击辅助规则 Andro.* 将显示一组不同的辅助规则已突出显示。



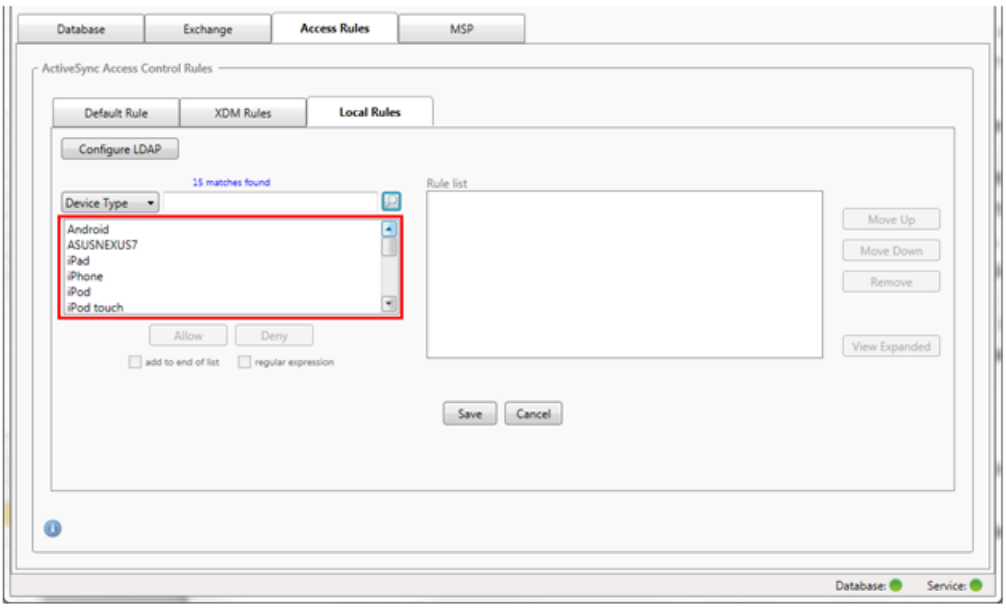
此示例显示了规则关系中包含的覆盖规则。此规则是常规 ActiveSync 设备类型规则 Android，已被覆盖（通过旁边的浅色字体和黑色圆圈指示）并且其访问状态还与主要规则正则表达式 ActiveSync 设备类型规则 Andro.* 发生冲突；在单击该规则之前，该规则是辅助规则。在上例中，常规 ActiveSync 设备类型规则 Android 未显示为辅助规则，因为从主要规则（正则表达式 ActiveSync 设备类型规则 touch.*）的角度来看，该规则与主要规则不相关。

配置常规表达式本地规则

1. 单击 Access Rules（访问规则）选项卡。

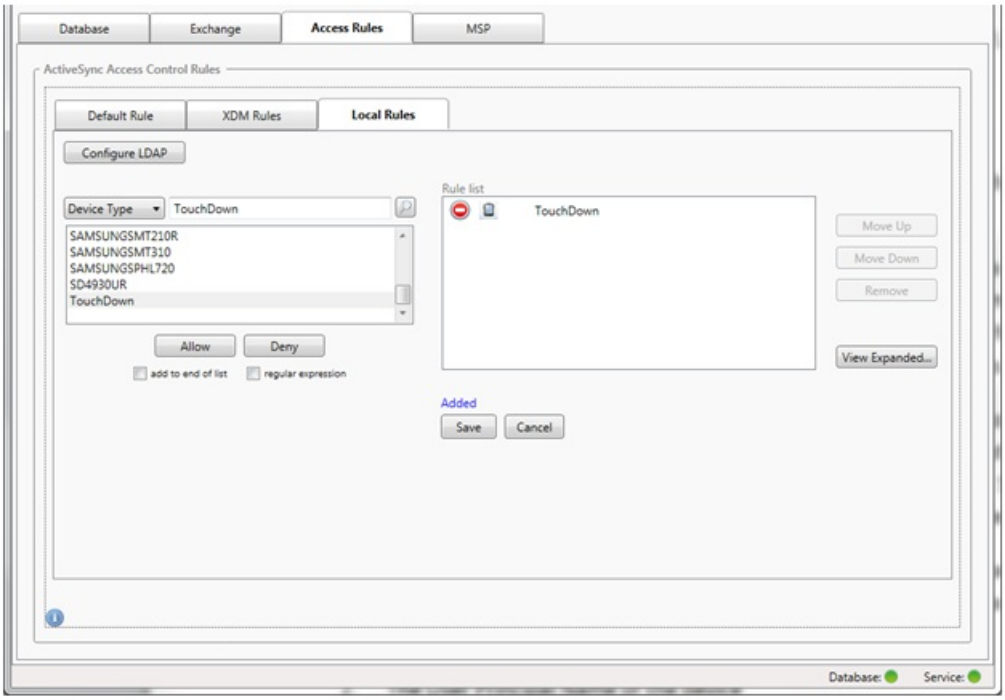


2. 在设备 ID 列表中，选择要为其创建本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。 在此示例中，已选择设备类型字段，选项显示在下面的列表框中。



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。

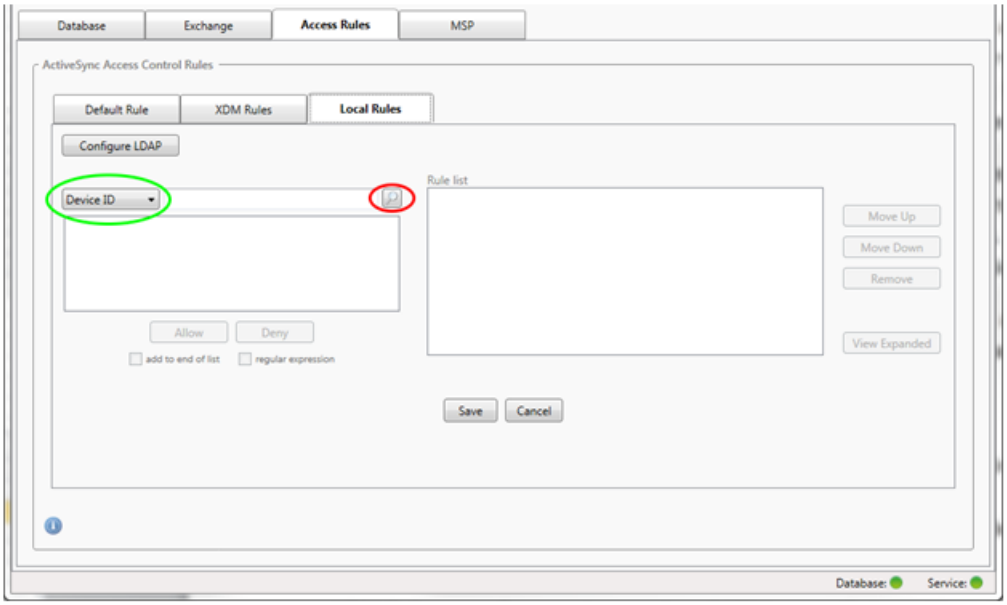


添加正则表达式

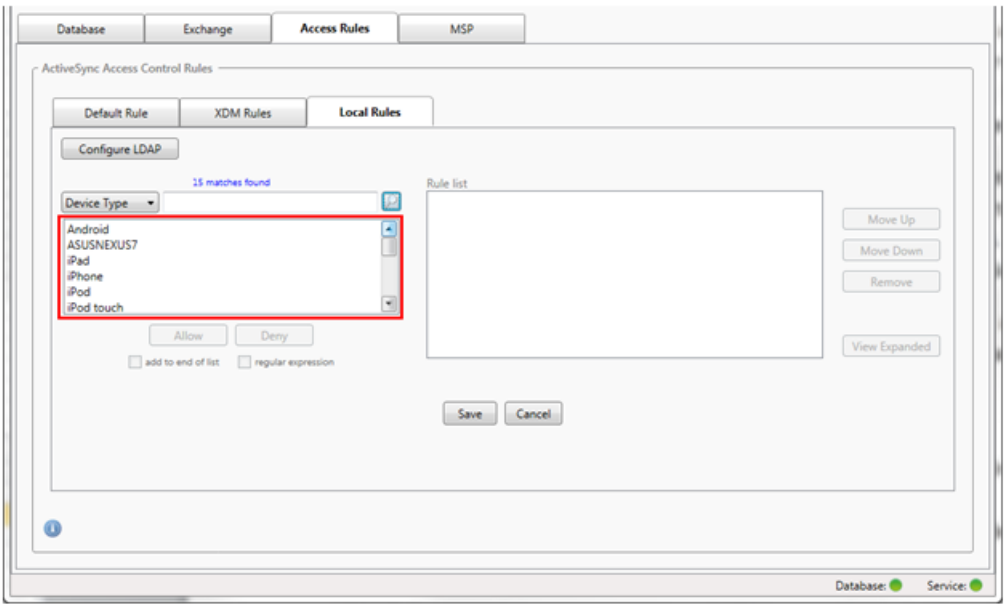
正则表达式本地规则可通过其旁边显示的图标进行区分 - (.*)。要添加正则表达式规则，您可以通过给定字段的结果列表中的现有值来构建正则表达式规则（只要已完成主要快照），或只需键入您想要的正则表达式。

从现有字段值构建正则表达式

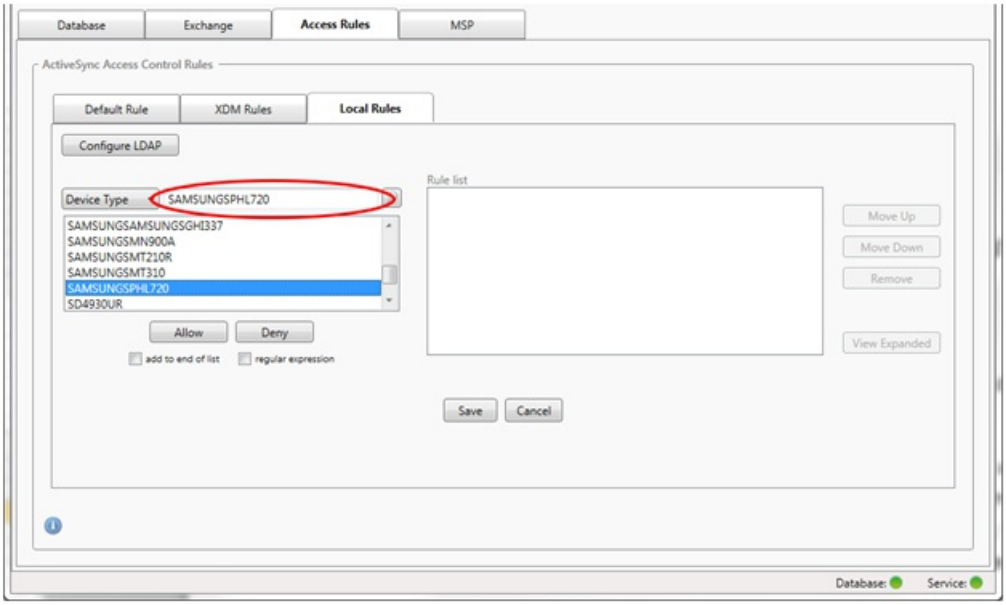
1. 单击 Access Rules（访问规则）选项卡。



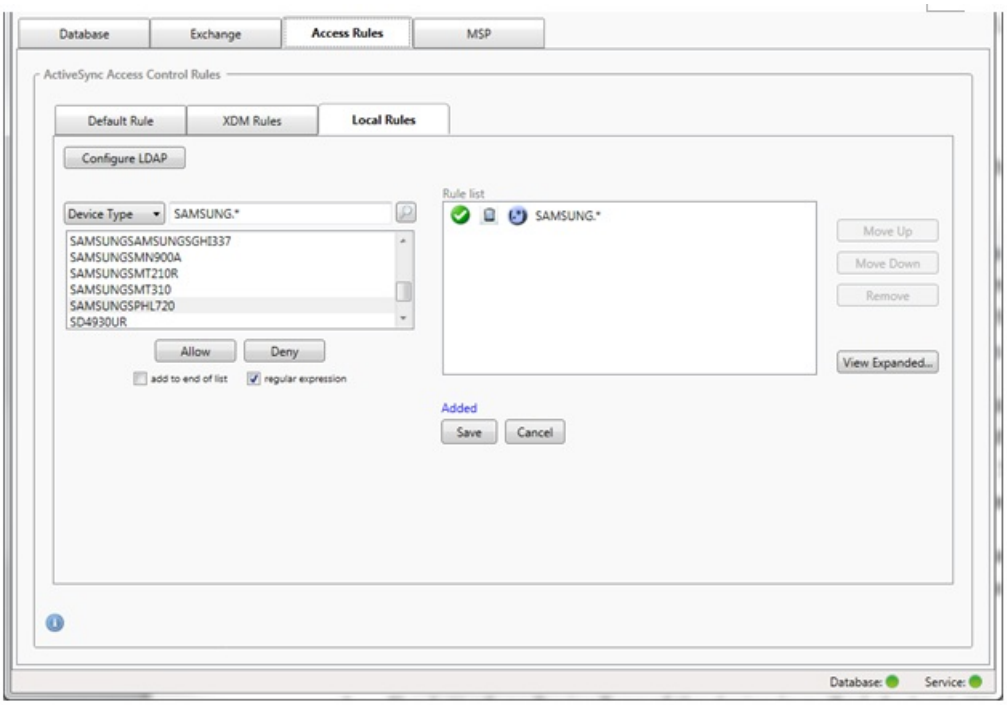
2. 在设备 ID 列表中，选择要为其创建正则表达式本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。 在此示例中，已选择设备类型字段，选项显示在下面的列表框中。



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。

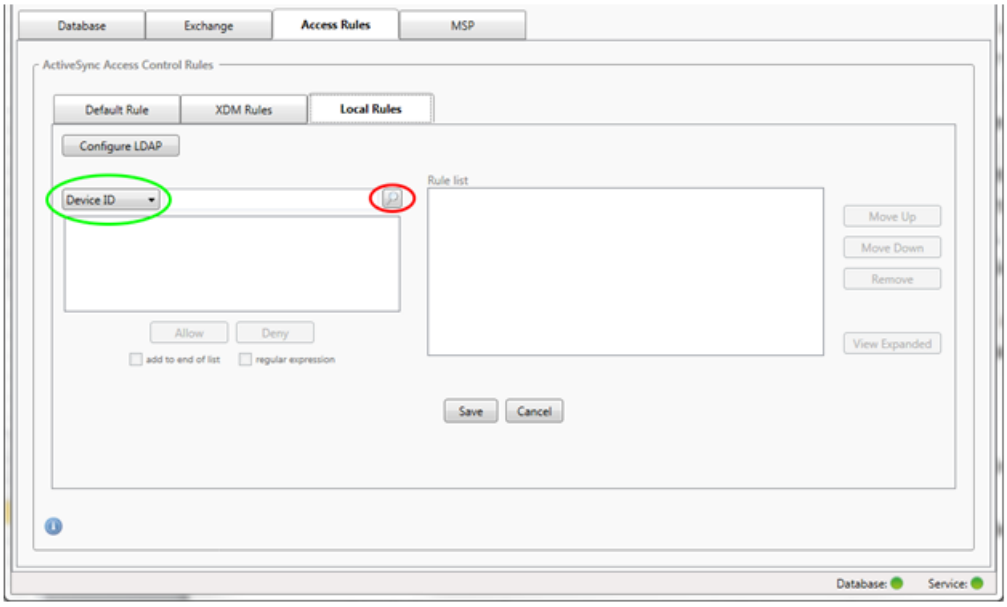


5. 要允许设备类型值中包含“Samsung”的所有设备，请按照以下步骤添加正则表达式规则：
   1. 在所选项目文本框内单击。
   2. 将文本从 SAMSUNGSPHL720 更改为 SAMSUNG.*
   3. 确保选中正则表达式复选框。
   4. 单击允许。

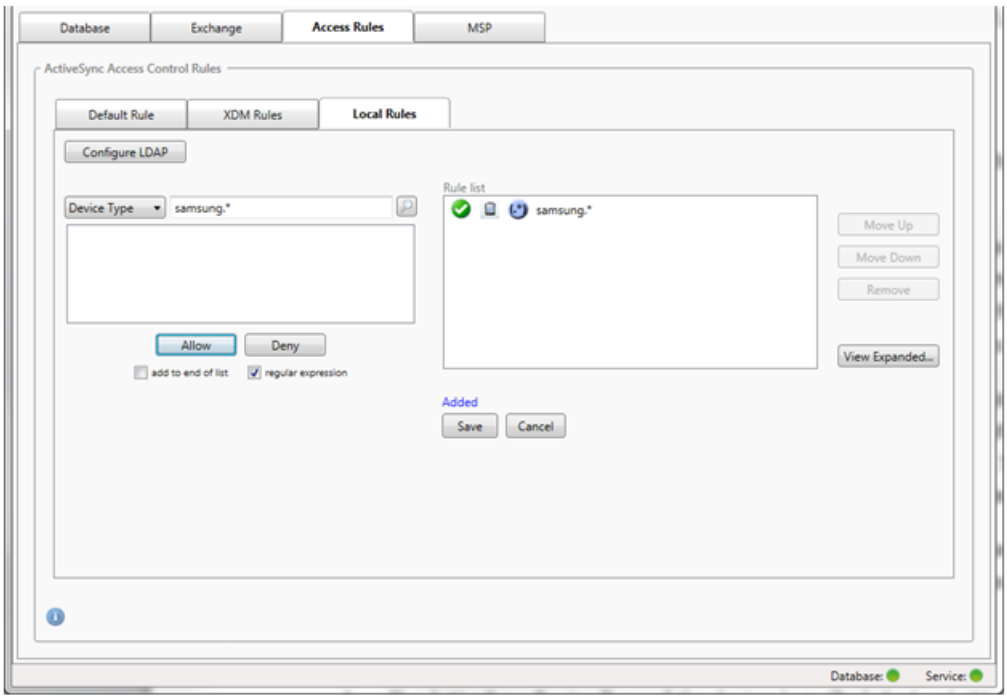


构建访问规则

1. 单击 Local Rules（本地规则）选项卡。
2. 要输入正则表达式，需要使用“设备 ID”列表和所选项目文本框。



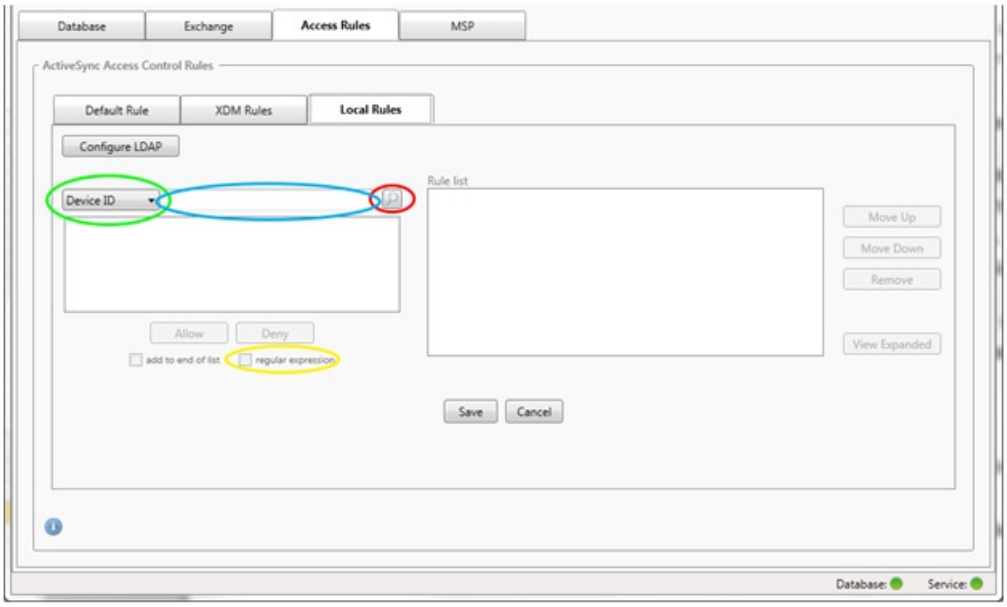
3. 选择要匹配的字段。 此示例使用设备类型。
4. 键入正则表达式。 此示例使用samsung.*
5. 确保选中正则表达式复选框，然后单击允许或拒绝。 在此示例中，选择的是允许，因此最终结果如下所示：



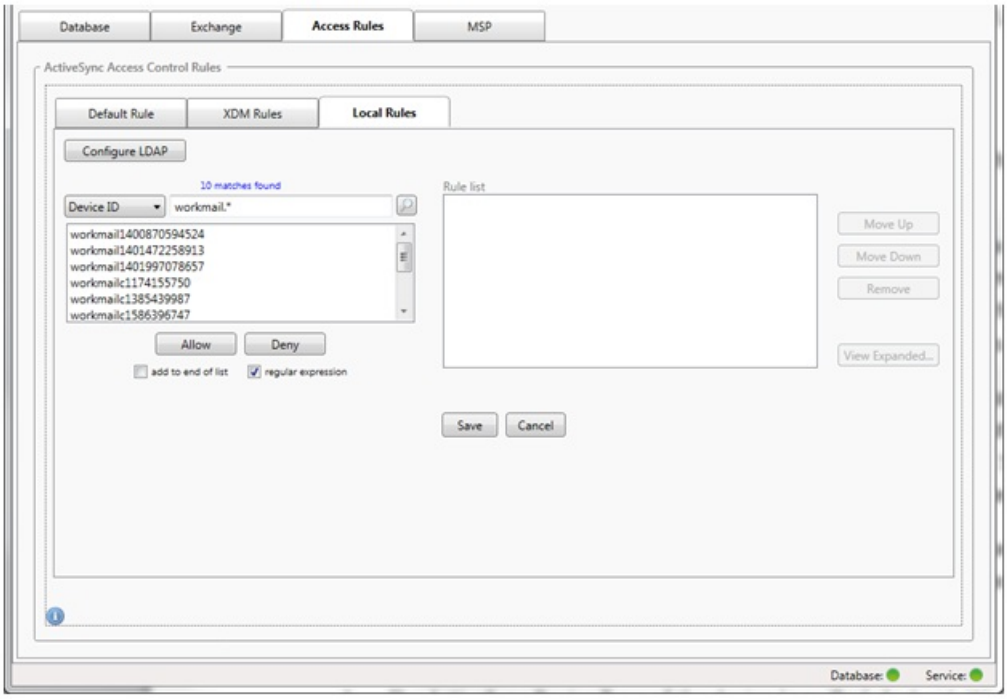
查找设备

通过选中正则表达式复选框，可以针对与给定表达式匹配的特定设备运行搜索。此功能仅在成功完成主要快照时可用。即使没有计划使用正则表达式规则，您也可以使用此功能。例如，假定您要查找 ActiveSync 设备 ID 中包含文本“workmail”的所有设备。为此，请执行以下过程。

1. 单击 Access Rules（访问规则）选项卡。
2. 确保设备匹配字段选择器设置为设备 ID（默认）。



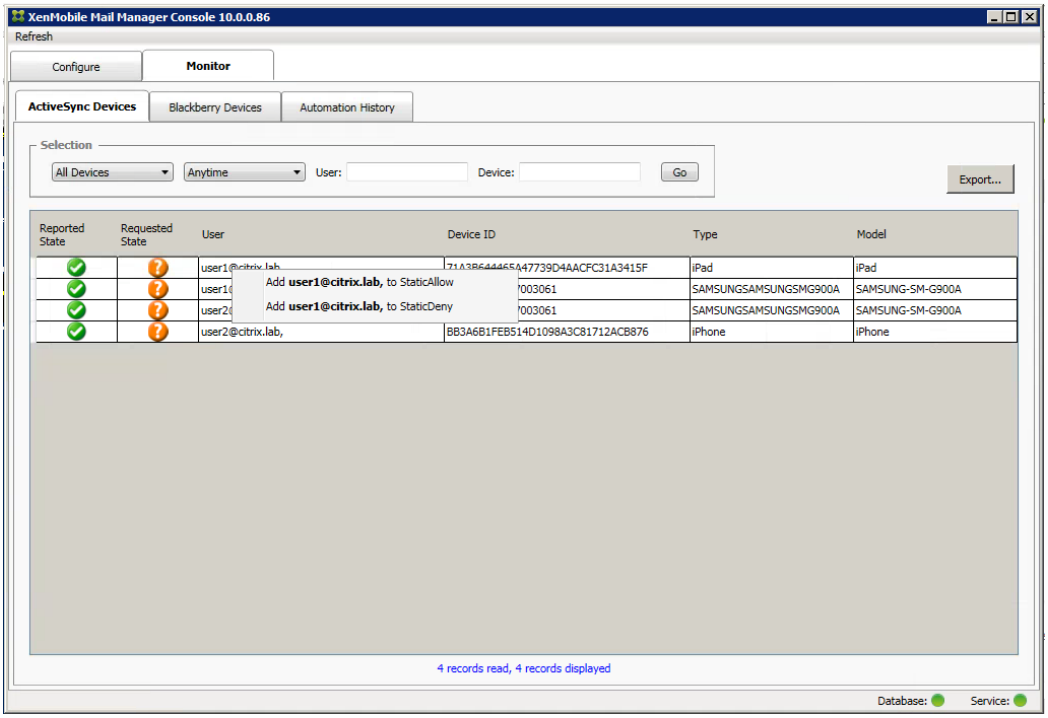
3. 在所选项目文本框（上图中以蓝色显示的框）内单击，然后键入workmail.*。
4. 确保选中正则表达式复选框，然后单击放大镜图标显示匹配项，如下图所示。



将单个用户、设备或设备类型添加到静态规则

可以基于 ActiveSync 设备选项卡上的用户、设备 ID 或设备类型添加静态规则。

1. 单击 ActiveSync 设备选项卡。
2. 在列表中，右键单击用户、设备或设备类型，然后选择是允许所选内容还是拒绝所选内容。
   下图显示了选定 user1 时的“允许”/“拒绝”选项。



设备监视

Nov 20, 2015

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

Nov 20, 2015

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

Aug 04, 2016

XenMobile NetScaler Connector 向 NetScaler 提供 ActiveSync 客户端的设备级别授权服务，而 NetScaler 用作 Exchange ActiveSync 协议的反向代理。 授权由在 XenMobile 中定义的策略组合以及 XenMobile NetScaler Connector 本地定义的规则控制。

有关详细信息，请参阅以下文章：

- XenMobile NetScaler Connector
- XenMobile 中的 ActiveSync Gateway

有关详细的参考体系结构图，请参阅 XenMobile Deployment Handbook（《XenMobile 部署手册》）中的“Reference Architecture for On-Premises Deployments”（适用于本地部署的参考体系结构）部分。