

XenMobile Server 10.5 中的新增功能

Apr 04, 2017

本 PDF 包含 XenMobile Server 10.5 的整套产品文档。如需当前版本的产品文档，请参阅 [XenMobile Server](#)。

有关升级的信息，请参阅[升级](#)。要访问 XenMobile 管理控制台，只能使用节点的 XenMobile Server 完全限定域名或 IP 地址。

Important

要访问 XenMobile 管理控制台，只能使用节点的 XenMobile Server 完全限定域名 (FQDN) (注册 FQDN) 或 IP 地址。不能再直接通过负载均衡虚拟 IP 地址或 NAT 的 IP 地址进行控制台访问，除非安装 2017 年 3 月 22 日发布的 XenMobile Server 10.5 Rolling Patch 1。有关详细信息，请参阅 <https://support.citrix.com/article/CTX221304>。

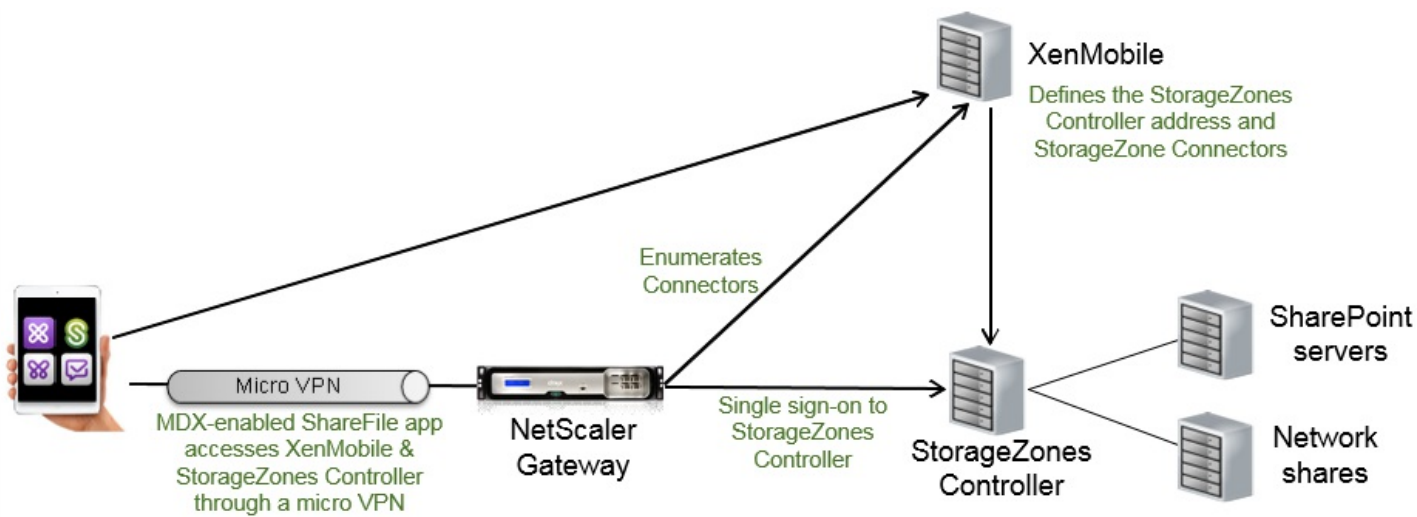
XenMobile Server 10.5 包括以下新增功能。有关缺陷修复的信息，请参阅[已修复的问题](#)。

简化了 ShareFile StorageZone 连接器的管理和部署

现在可以使用 XenMobile 控制台来配置 StorageZone 连接器。作为替代将 XenMobile 与 ShareFile Enterprise 结合使用的方式，提供了将 XenMobile 与 StorageZone 连接器结合使用的方式：

- 提供对现有内部部署存储库（例如 SharePoint 站点和网络文件共享）的安全移动访问。不需要设置 ShareFile 子域、向 ShareFile 置备用户或托管 ShareFile 数据。
- 为用户提供通过适用于 iOS 的 ShareFile XenMobile Apps 对数据进行移动访问的权限。用户可以编辑 Microsoft Office 文档。用户还可以从移动设备预览和批注 Adobe PDF 文件。
- 文件访问仅限于连接器。用户无权访问其他 ShareFile 功能，例如数据共享或同步。
- 遵守防止在企业网络外部泄漏用户信息的安全限制。
- 可以通过 XenMobile 控制台对 StorageZone 连接器进行简单设置。如果您以后决定在 XenMobile 中使用完整的 ShareFile 功能，可以在 XenMobile 控制台中更改配置。
- 需要 XenMobile Enterprise Edition。

下图显示了 XenMobile 与 StorageZone 连接器结合使用的高级体系结构。



在您第一次访问配置 > ShareFile 页面时，会显示 XenMobile 与 ShareFile Enterprise 结合使用和 XenMobile 与 StorageZone 连接器结合使用之间的差异的说明。

The screenshot shows the XenMobile configuration interface for ShareFile. It offers two integration methods: ShareFile Enterprise and StorageZone Connectors Only. The following table summarizes the capabilities of each method:

Capability	ShareFile Enterprise	StorageZone Connectors Only
Access network shares and SharePoint data from mobile devices	✓	✓
Edit Microsoft Office documents from mobile devices	✓	✓
Preview and annotate Adobe PDF files from mobile devices	✓	✓
Store data in Citrix-managed or customer-managed StorageZones or both	✓	
Securely share files with people inside and outside the enterprise	✓	
Sync files and data across multiple devices	✓	
Access files through the ShareFile website	✓	
Access Office 365 content and Personal Cloud connectors from mobile devices	✓	
Use auditing and reporting capabilities	✓	

如果单击配置连接器，则会提供有关连接器和 StorageZones Controller 的信息。

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps Actions **ShareFile** Enrollment Profiles Delivery Groups

StorageZone Connector

- Connector Info
- Delivery Group Assignment (Optional)
- Summary

Connector Info

Configuring a connector will allow end users to connect to their existing SharePoint sites and CIFS (Common Internet File System) based on their authorizations.

Connector Name*

Description

Type* SharePoint

StorageZone* iosDev [Manage StorageZones](#)

Location*

Manage StorageZones

[Add New](#)

Name* ShareFileTest

FQDN* mw-sfprod.mwdemo.local

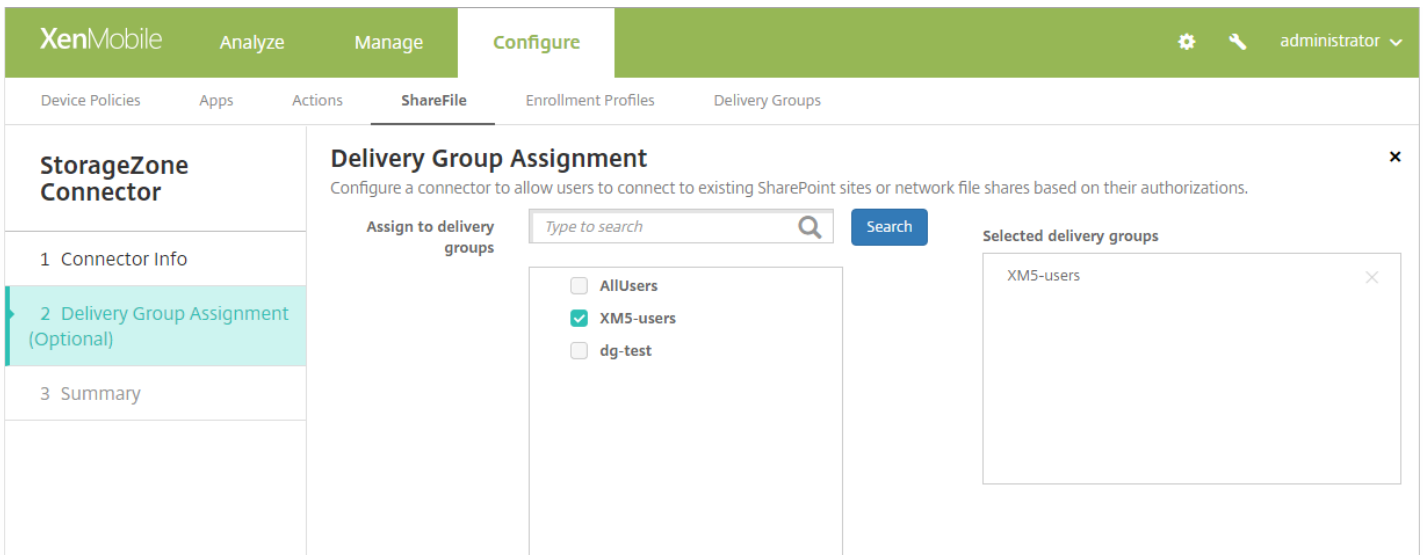
Port* 443

Secure Connection ON

Administrator user na...* mwdemo\administrator

Administrator passw...*

可以在创建连接器时将连接器与交付组关联。



还可以通过使用配置 > 交付组页面将连接器与交付组关联。

有关将 StorageZone 连接器与 XenMobile 集成的详细信息，请参阅 [ShareFile 与 XenMobile 结合使用](#)。

重命名的客户端属性

与 Citrix PIN 有关的 XenMobile 客户端属性名称已更改：

旧属性名称	新属性名称
启用 Worx PIN 身份验证	启用 Citrix PIN 身份验证
Worx PIN 类型	PIN 类型
PIN 强度要求	PIN 强度要求
Worx PIN 长度要求	PIN 长度要求
Worx PIN 更改要求	PIN 更改要求
Worx PIN 历史记录	PIN 历史记录

属性关键字保持相同，如下示例中所示：

Settings > Client Properties

Client Properties

To change a property, select the property and then click Edit.



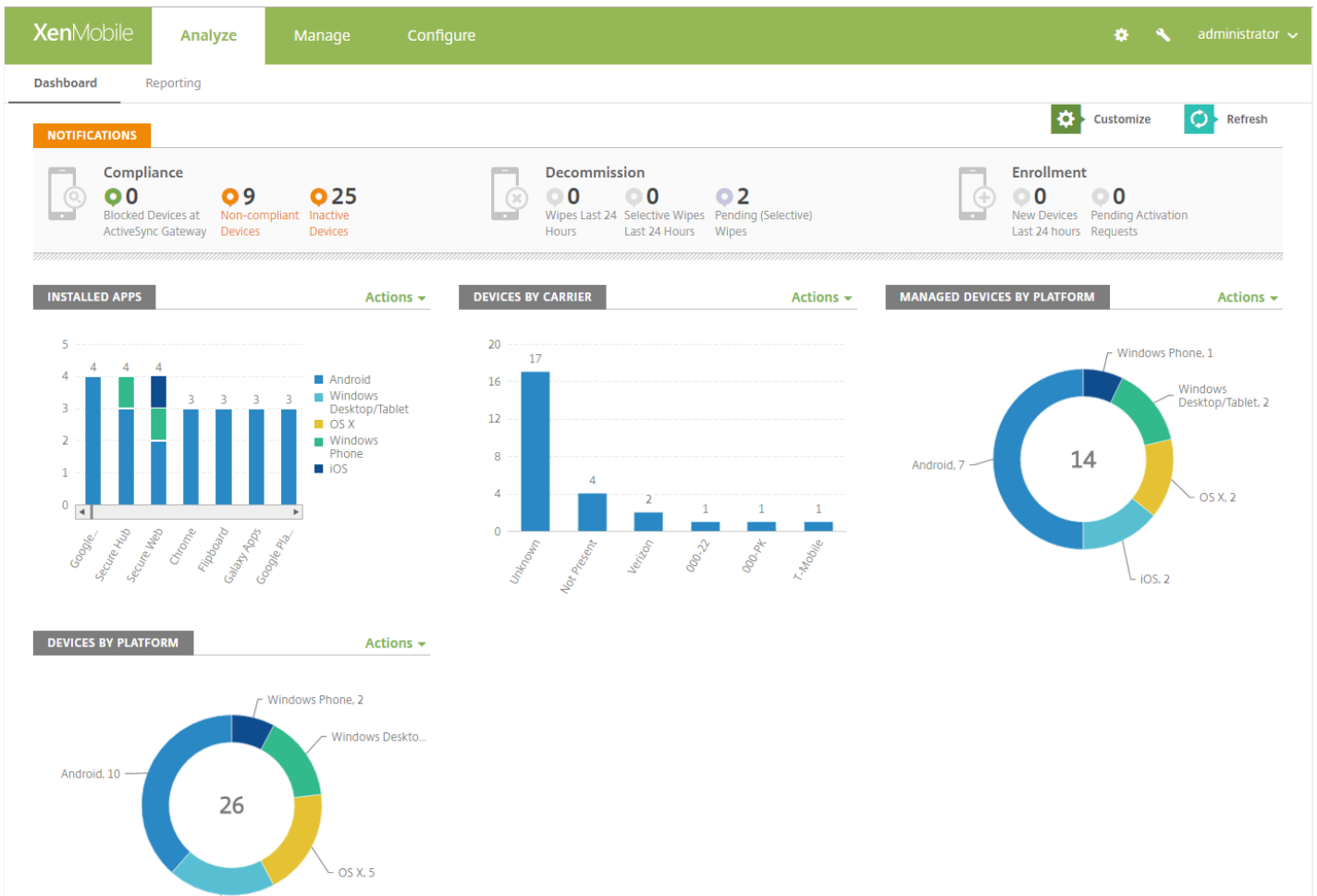
Add

<input type="checkbox"/>	Name	Key	Value	Description	▾
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication	
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching	
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password	
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement	
<input type="checkbox"/>	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type	
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement	
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement	
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History	
<input type="checkbox"/>	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer	
<input type="checkbox"/>	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode	

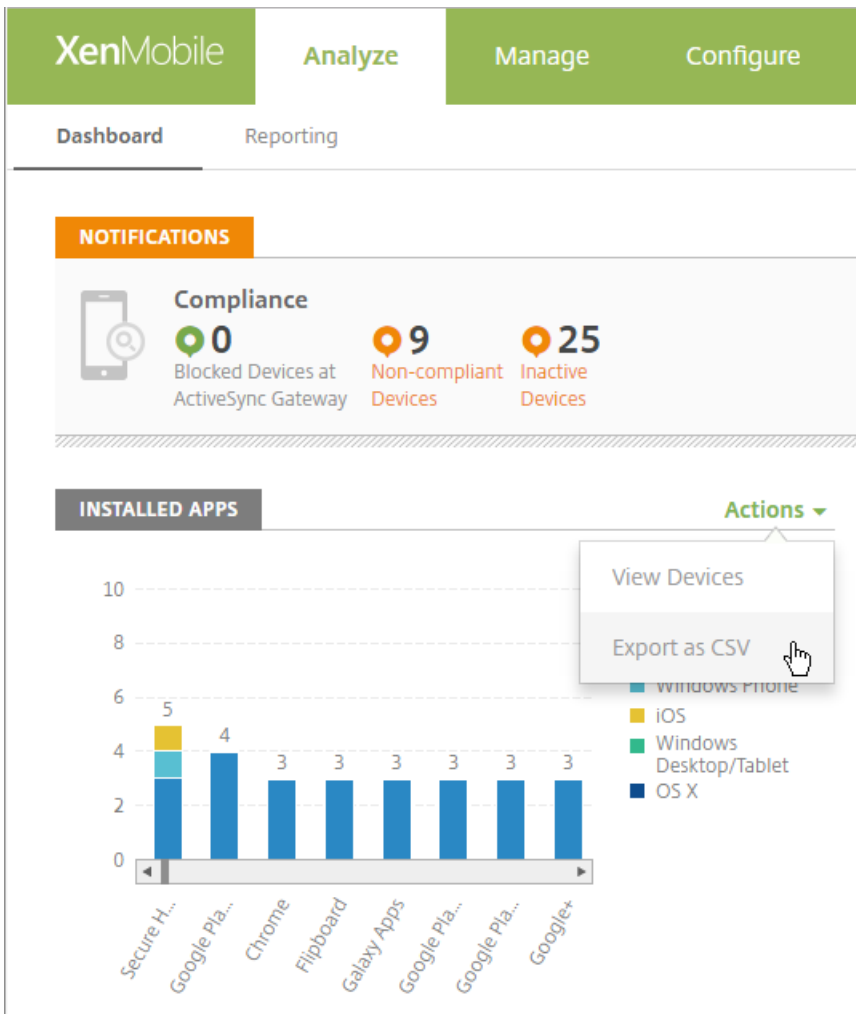
控制板改进功能

XenMobile 分析 > 控制板 页面具有快速响应的设计，可改善在较小设备上的查看速度。其他改进功能包括：

- “已安装的应用程序”小组件现在显示排名前 10 的应用程序。要查看其他应用程序，请使用搜索栏。
- 要将已安装的应用程序导出为 CSV 文件，请执行以下操作：
 - 选择某个应用程序，然后将其导出以仅获得该应用程序的报告。
 - 不选择任何应用程序，则获取所有应用程序的报告。
 - 报告包括应用程序的以下信息：名称、所有者、版本、大小、ID 和安装时间。
- “VPP 应用程序许可证使用情况”小组件现在显示软件清单中的所有应用程序。您不再需要搜索应用程序。

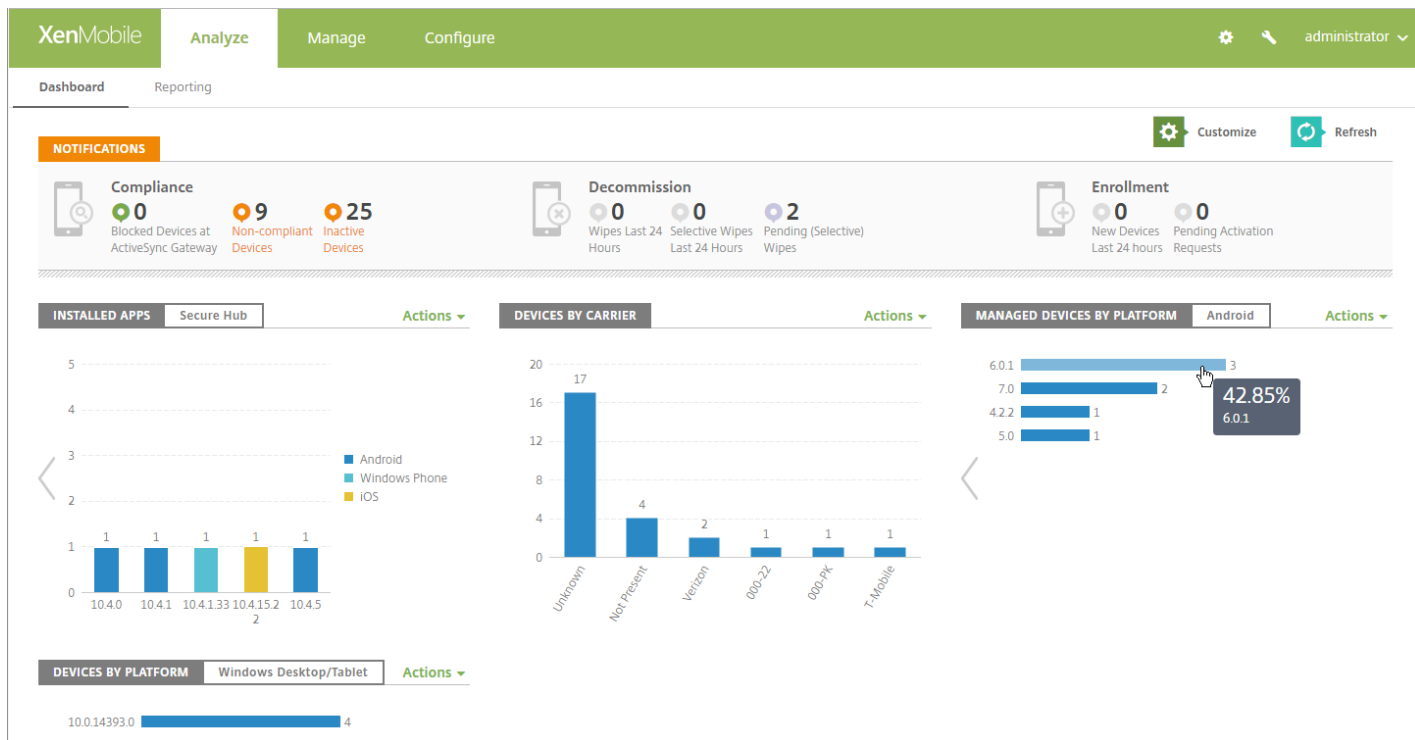


- 图表按降序显示计数。
- 每个小组件使用最佳图表类型显示信息。
- 可用于每个小组件的操作显示在**操作菜单**中，该菜单现在仅包括从控制板最常执行的操作：
 - 查看设备 - 打开管理 > 设备页面。
 - 导出为 CSV - 将数据保存到 CSV 文件。



- “导出为 CSV”操作会导出每个已安装应用程序的以下信息：
 - 名称
 - 版本
 - 所有者
 - 大小
 - ID
 - 安装时间
- 可以逐级浏览到以下图表的两级详细信息：单击某个平台以查看版本计数的条形图，然后单击某个版本以打开管理 > 设备页面。
 - 设备(按平台)
 - 托管设备(按平台)
 - 非托管设备(按平台)
 - 已安装的应用程序
- 要打开管理 > 设备页面，请单击以下任意图表：
 - 设备(按运营商)
 - 设备(按 ActiveSync Gateway 状态)
 - 设备(按所有权)
 - Android TouchDown 许可证状态

失败的交付组部署
设备(按阻止原因)
VPP 应用程序许可证使用情况



向 XenMobile 控制台添加了“测试连接”按钮

现在，XenMobile 控制台的以下页面上包含测试连接按钮：

- **配置 > ShareFile**：可以使用测试连接按钮以确认 ShareFile 管理员帐户的用户名和密码是否可以向指定的 ShareFile 帐户进行身份验证。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions **ShareFile** Enrollment Profiles Delivery Groups

ShareFile

Configure settings to connect to the ShareFile account and administrator service account for user account management.

Domain*

Assign to delivery groups

AllUsers

Selected delivery groups

AllUsers

ShareFile Administrator Account Logon

User name*

Password*

User account provisioning

SAML certificate

Name XMS.example.com

Advanced ShareFile Configuration

- 设置 > XenApp/XenDesktop : 可以使用测试连接按钮以确认 XenMobile 是否可以连接到指定的 XenApp 和 XenDesktop 服务器。

XenMobile Analyze Manage **Configure**

Settings > XenApp/XenDesktop

XenApp/XenDesktop

Allows users to add XenApp and XenDesktop through Secure Hub.

Host*

Port*

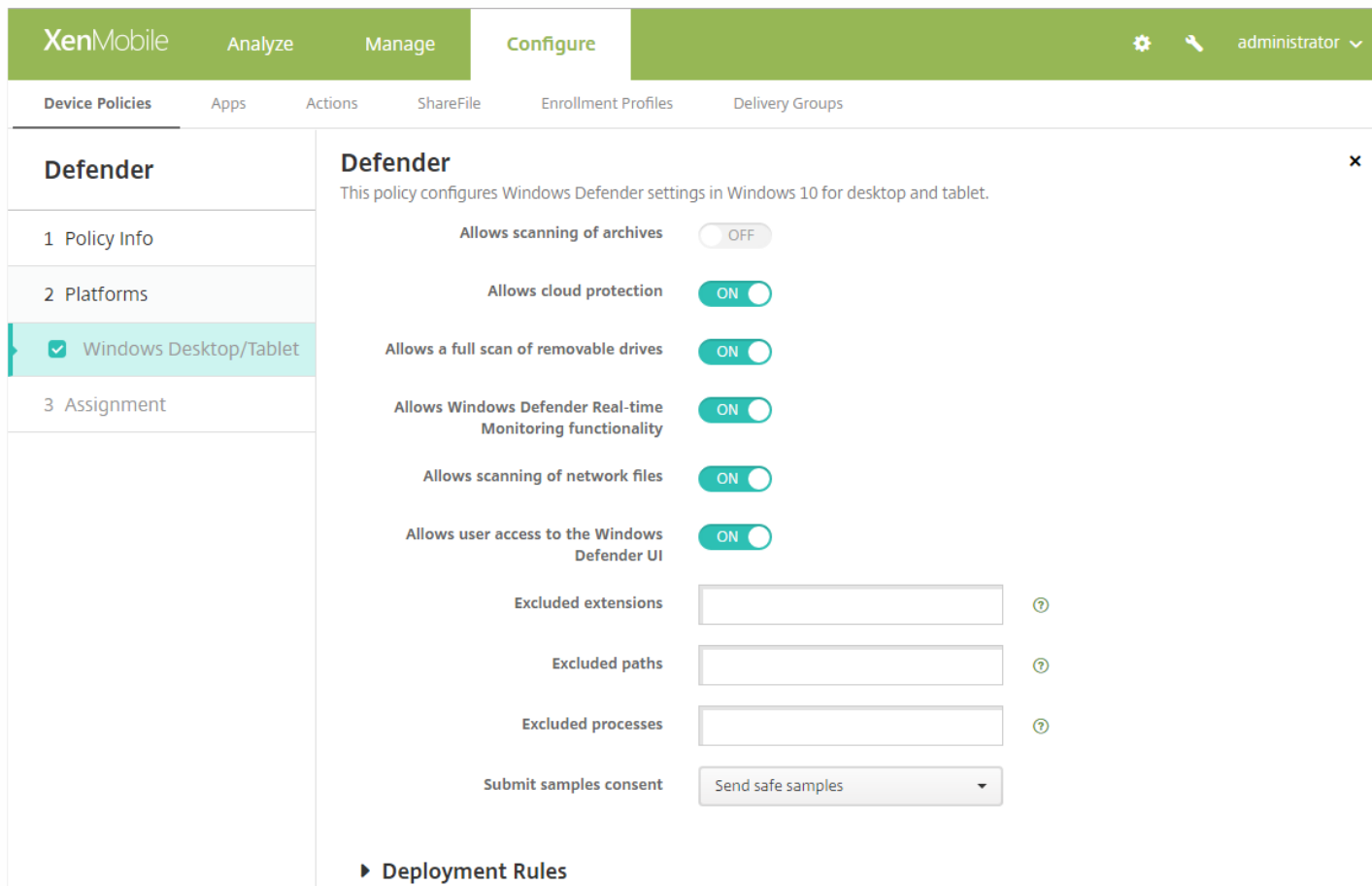
Relative Path*

Use HTTPS

Connection succeeded

适用于台式机和平板电脑的 Windows 10 中的 Windows Defender 设备策略

Windows Defender 是 Windows 10 附带的恶意软件防护功能。可以使用 XenMobile 设备策略 Defender 来配置 Microsoft Defender 策略。要添加 Defender 策略，请转至配置 > 设备策略，单击添加，开始键入 Defender，然后单击搜索结果中的该名称。



The screenshot shows the XenMobile configuration interface for the Windows Defender policy. The interface is divided into several sections:

- Navigation:** Top bar with "XenMobile", "Analyze", "Manage", and "Configure" tabs. A user profile "administrator" is visible in the top right.
- Policy List:** On the left, a list of policies includes "Defender". Under "Defender", the "Windows Desktop/Tablet" platform is selected.
- Policy Configuration:** The main area shows the "Defender" policy configuration. It includes a description: "This policy configures Windows Defender settings in Windows 10 for desktop and tablet." Below this are several settings:
 - Allows scanning of archives: OFF
 - Allows cloud protection: ON
 - Allows a full scan of removable drives: ON
 - Allows Windows Defender Real-time Monitoring functionality: ON
 - Allows scanning of network files: ON
 - Allows user access to the Windows Defender UI: ON
 - Excluded extensions: (empty text box)
 - Excluded paths: (empty text box)
 - Excluded processes: (empty text box)
 - Submit samples consent: Send safe samples (dropdown menu)
- Deployment Rules:** A section at the bottom with a right-pointing arrow.

有关详细信息，请参阅 [Defender 设备策略](#)。

针对 Windows 10 的 WiFi 设备策略支持

WiFi 设备策略现在支持 Windows 10，让您可以在 WiFi 网络中使用客户端证书身份验证。要更新 WiFi 设备策略，请转至配置 > 设备策略。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

WiFi Policy

This policy lets you configure a WiFi profile for devices.

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Android
 - Windows Phone
 - Windows Desktop/Tablet
 - Windows Mobile/CE
- 3 Assignment

Network name* WiFi_24G ?

Authentication WPA-2 Enterprise

Encryption AES

EAP Type TLS

Connect if hidden OFF

Connect automatically ON

Push certificate via SCEP ON

Credential provider for SCEP* certsrv-cpwifi

Proxy server settings

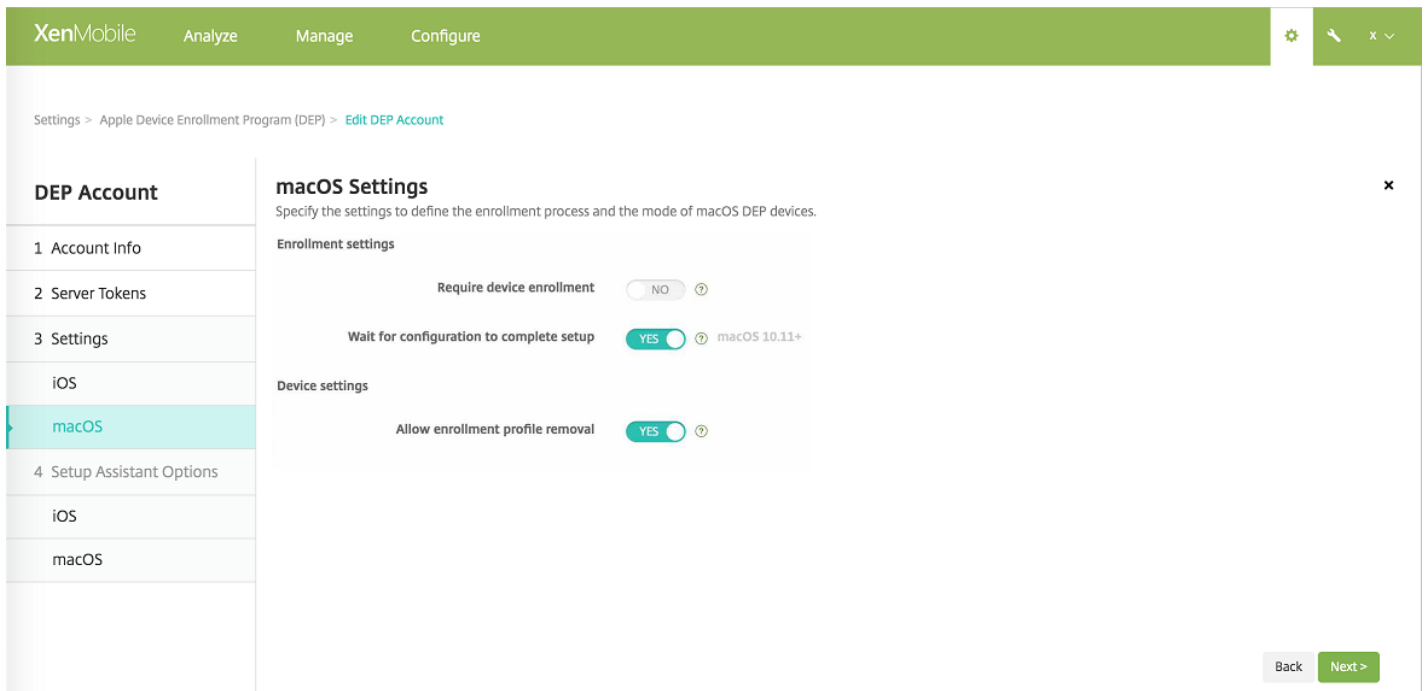
Host name or IP address

Port

有关详细信息，请参阅 [WiFi 设备策略](#)。

批量注册 macOS 设备

XenMobile 中的 Apple Device Enrollment Program (DEP) 设置现在支持运行 OS X 10.10 或更高版本的 macOS 设备。可按照 [批量注册 iOS 和 macOS 设备](#) 中所述的相同过程进行操作。如果您从 **设置 > Apple Device Enrollment Program (DEP)** 添加 DEP 帐户，**设置**和**设置助理**选项现在包括用于 macOS 的页面。

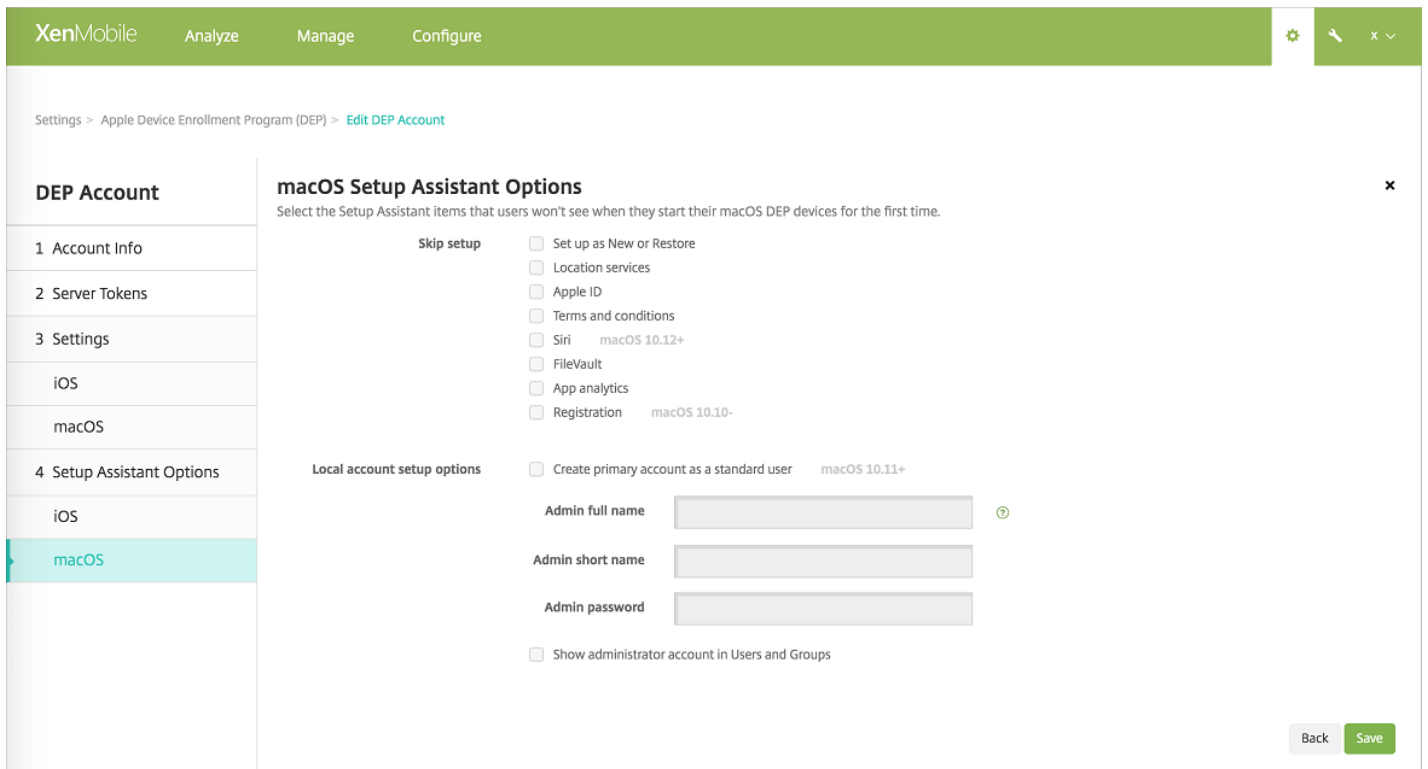


注册设置

- **要求设备注册**：是否要求用户注册其设备。默认值为是。
- **等待完成配置设置**：如果启用此设置，在 MDM 资源通行码部署到设备之前，macOS 设备不会继续出现在设置助理中。MDM 资源通行码部署在创建本地帐户之前进行。此设置适用于 macOS 10.11 及更高版本的设备。默认值为否。

设备设置

- **允许删除注册配置文件**：是否允许设备使用能够远程删除的配置文件。默认值为否。



- **设置为新对象或还原**：将设备设置为新设备或从 iCloud 或 iTunes 备份设置设备。
- **定位服务**：在设备上设置定位服务。
- **Apple ID**：设置设备的 Apple ID 帐户。
- **条款和条件**：要求用户接受条款和条件才能使用设备。
- **Siri**：是否在设备上使用 Siri。
- **FileVault**：使用 FileVault 加密启动磁盘。仅当系统具有一个已登录到 iCloud 的本地用户帐户时，XenMobile 才会应用 FileVault 设置。

可以使用 macOS FileVault 磁盘加密功能为系统卷的内容加密来保护系统卷。请参阅 Apple 支持文章 <https://support.apple.com/en-us/HT204837>。如果在 FileVault 处于关闭状态的新型便携式 Mac 上运行设置助理，系统可能会提示您打开此功能。如果系统满足以下要求，则会在新系统上和已升级到 OS X 10.10 或 10.11 的系统上显示该提示：

- 系统有一个本地管理员帐户
- 该帐户已登录到 iCloud
- **应用程序分析**：设置是否与 Apple 共享崩溃数据和使用情况统计信息。
- **注册**：要求用户注册其设备。

已通过 OS X 10.9 提供注册信息设置。您已通过注册过程将系统注册信息发送给 Apple。此信息已将您的联系信息与 Mac 硬件关联。Apple 主要使用该信息来协助 Apple 支持。如果您以前指定了 Apple ID，则设置助理（可选）已基于您的 Apple ID 帐户提交注册。如果您未指定 Apple ID，可以手动键入您的联系信息。

- 在**本地帐户设置选项**下方，指定设置以创建管理员帐户（这是 macOS 必需的）。XenMobile 将使用指定的信息来创建帐户。

对 iOS 和 macOS 设备支持多个 Apple Device

Enrollment Program 帐户

现在可以定义多个 Apple Device Enrollment Program (DEP) 帐户。通过此功能可以使用不同的注册设置、设备设置及设置助理选项。可以按国家/地区、部门和其他结构指定这些设置和选项。然后通过部署规则将 DEP 帐户与不同的设备策略和不同的应用程序关联。

例如，可以将来自不同国家/地区的所有 DEP 帐户集中在同一 XenMobile Server 上。然后可以导入和监督所有 DEP 设备。通过按国家/地区或其他结构自定义注册设置，可以确保策略在整个组织中提供合适的功能。通过按国家/地区或其他结构自定义设置助理选项，可以确保设备用户获得合适的设置帮助。

为了能够支持多个 DEP 帐户，以下页面替换设置 > iOS 批量注册：

- **设置 > Apple Device Enrollment Program (DEP)：** 此页面用于：
 - 创建 DEP 帐户。
 - 按每个帐户配置注册设置、iOS 和 macOS 设备设置以及设置助理选项。

The screenshot shows the XenMobile interface for configuring the Apple Device Enrollment Program (DEP). The navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main content area is titled 'Settings > Apple Device Enrollment Program (DEP)'. Below the title, there is a brief description of DEP. The configuration is presented in three numbered steps:

- 1. Download Public Key**
A Public Key will be automatically generated for you and signed by Citrix.
[Download]
- 2. Create a Server Token file**
 - Sign in to [Apple Deployment Programs Portal](#) with your corporate Apple ID.
 - Navigate to Device Enrollment Program > Manage Servers. Click Add MDM Server.
 - Enter a MDM Server Name, then click Choose File... and upload your Public Key.
 - Download the Server Token file provided.
- 3. Add DEP Account**
Follow the wizard to add the account.
[Add]

设备 > Apple Configurator Device Enrollment： 用于准备 iOS 和 macOS 设备以及配置策略。

Settings > [Apple Configurator Device Enrollment](#)

Apple Configurator Device Enrollment

Use Apple Configurator to mass configure and deploy iPhone, iPad or iPod Touch.



Export anchor certificates

- Enable Apple Configurator device enrollment YES
- Enrollment URL to enter in Apple Configurator <https://example.domain.net:8443/zdm/ios/otae/dobulkenrollment>
- Require device registration before enrollment NO
- Require credentials for device enrollment YES iOS 7.1+

Cancel

Save

有关详细信息，请参阅 [通过 Apple DEP 部署 iOS 设备](#)。

iOS 主屏幕布局

可使用新的主屏幕布局设备策略来指定 iOS 主屏幕上应用程序和文件夹的布局。此策略在 iOS 9.3 及更高版本的受监督设备上受支持。要添加策略，请转至 [配置 > 设备策略](#)。

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

1 Policy Info

2 Platforms

iOS

3 Assignment

Home Screen Layout Policy

Dock

Type	Display Name*	Value*	Add
			+ Add

Page 1

Type	Display Name*	Value*	Add
			+ Add

Page 2

Type	Display Name*	Value*	Add
			+ Add

Page 3

Type	Display Name*	Value*	Add
			+ Add

Page 4

Type	Display Name*	Value*	Add
			+ Add

Page 5

Type	Display Name*	Value*	Add
			+ Add

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

1 Policy Info

2 Platforms

iOS

3 Assignment

Home Screen Layout Policy

Dock

Type	Display Name*	Value*	Save	Cancel
Application	<input type="text"/>	<input type="text"/>	Save	Cancel

Page 1

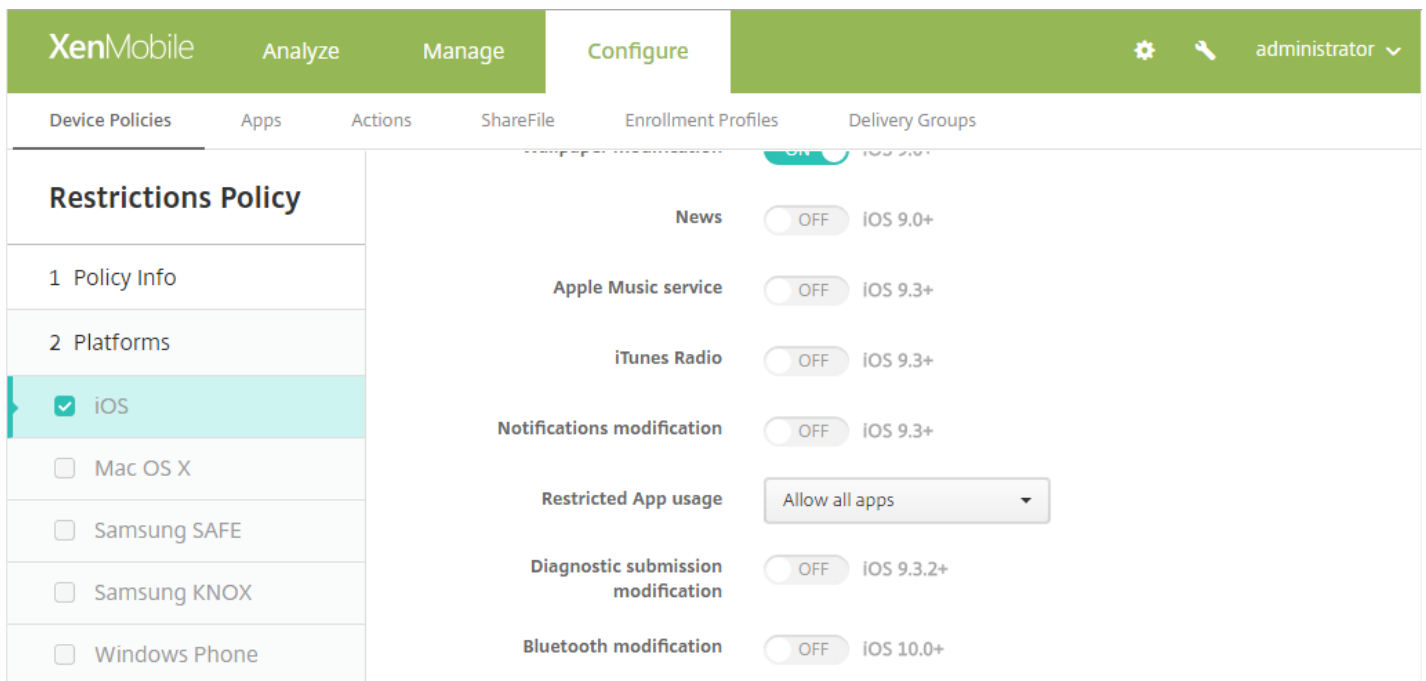
Type	Display Name*	Value*	Add
			+ Add

有关详细信息，请参阅[主屏幕布局设备策略](#)。

适用于 iOS 设备的更多功能限制选项

适用于 iOS 的限制策略现在有以下其他限制选项：

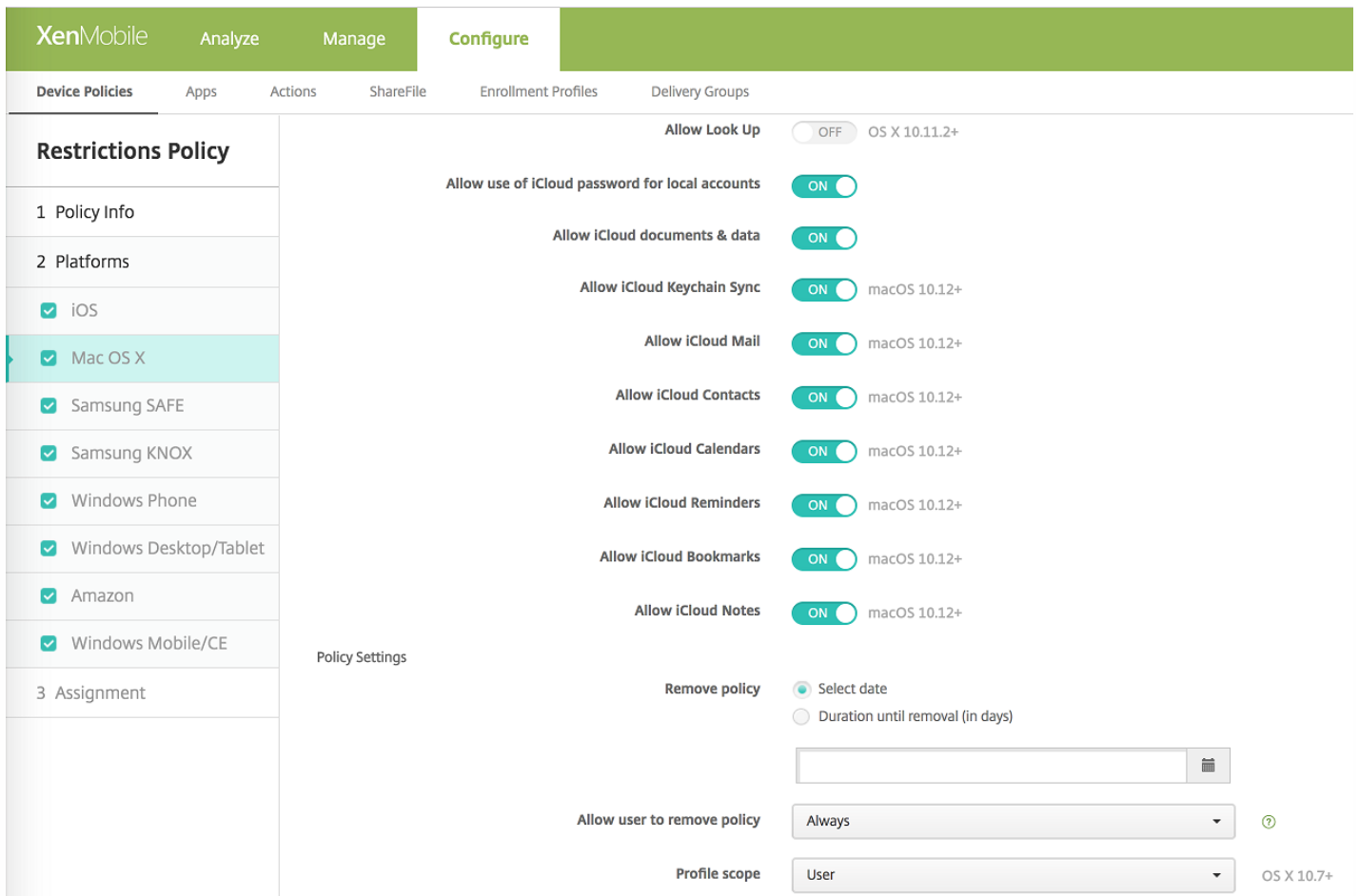
- **新闻**：允许用户使用新闻应用程序（在 iOS 9.0 及更高版本中可用）。仅适用于受监督的设备。
- **Apple 音乐服务**：允许用户使用 Apple 音乐服务（在 iOS 9.3 及更高版本中可用）。如果您不允许 Apple 音乐服务，则音乐应用程序以经典模式运行。仅适用于受监督的设备。
- **iTunes Radio**：允许用户使用 iTunes Radio（在 iOS 9.3 及更高版本中可用）。仅适用于受监督的设备。
- **通知修改**：允许用户更改通知设置（在 iOS 9.3 及更高版本中可用）。仅适用于受监督的设备。
- **受限应用程序使用**：允许用户使用所有应用程序或仅使用按捆绑包 ID 允许或拒绝的应用程序（在 iOS 9.3 及更高版本中可用）。仅适用于受监督的设备。
- **诊断提交修改**：允许用户在“设置”的“诊断和使用”窗格中更改诊断提交和应用程序分析设置（在 iOS 9.3.2 及更高版本中可用）。仅适用于受监督的设备。
- **蓝牙修改**：允许用户更改蓝牙设置（在 iOS 10.0 及更高版本中可用）。仅适用于受监督的设备。



适用于 macOS 设备的更多功能限制选项

对于 macOS 10.12 及更高版本，限制策略有以下附加限制选项。默认情况下，XenMobile 允许使用这些功能。

- 允许 Apple 音乐：如果您不允许 Apple 音乐服务，则音乐应用程序以经典模式运行。仅适用于受监督的设备。
- 允许 iCloud 钥匙串同步
- 允许 iCloud 邮件
- 允许 iCloud 通讯录
- 允许 iCloud 日历
- 允许 iCloud 提醒事项
- 允许 iCloud 书签
- 允许 iCloud 备忘录



支持 iOS 9.3 托管丢失模式

在 iOS 9.3 或更高版本中，可使用 Apple MDM 将受监督的设备置于托管丢失模式，这是一种专用模式。可以使用托管丢失模式阻止或定位丢失或被盗的受监督设备。

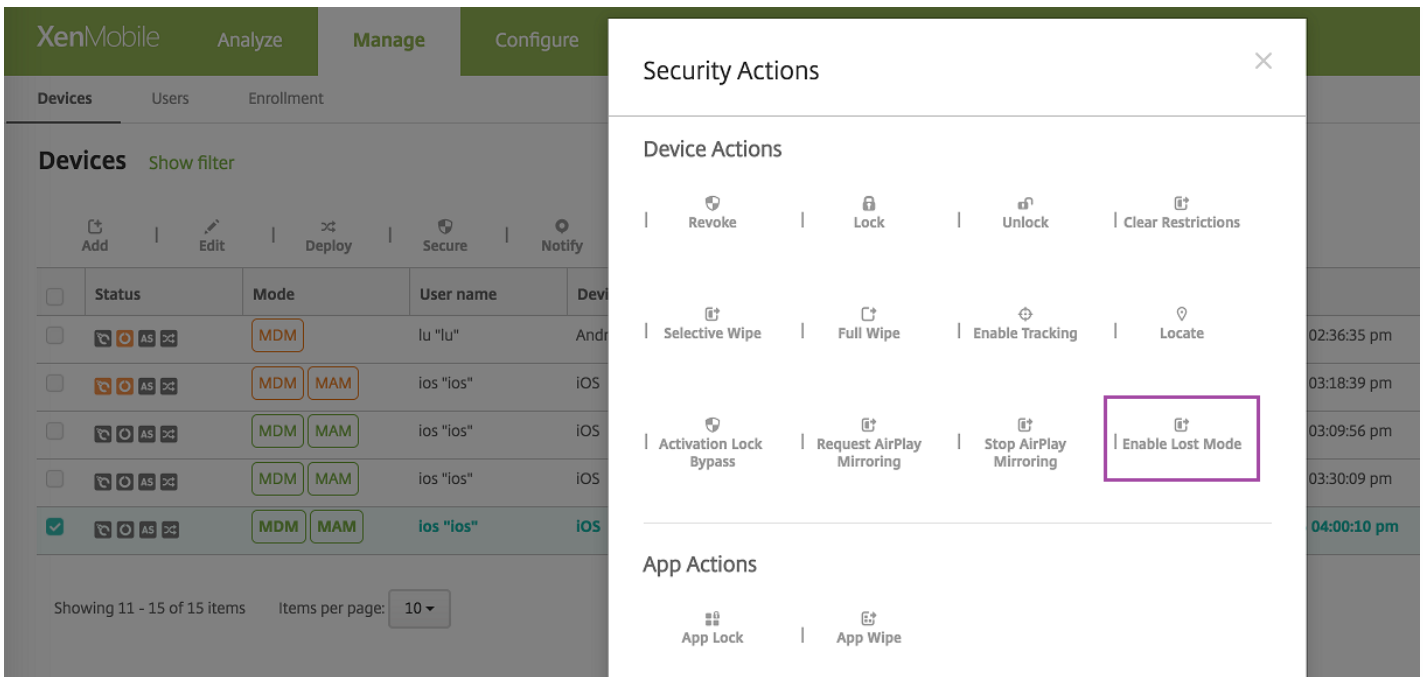
XenMobile 现在有丢失模式设备属性。与 Apple 托管丢失模式不同，XenMobile 丢失模式不要求用户执行以下任一操作来启用定位其设备：配置“查找我的 iPhone/iPad”设置或为 Citrix Secure Hub 启用定位服务。

XenMobile 丢失模式功能类似于 XenMobile 设备锁定功能。但是，在 XenMobile 丢失模式下，只有 XenMobile Server 可以解锁设备。通过使用设备锁定，用户可以通过使用管理员提供的 PIN 码直接解锁设备。

注意

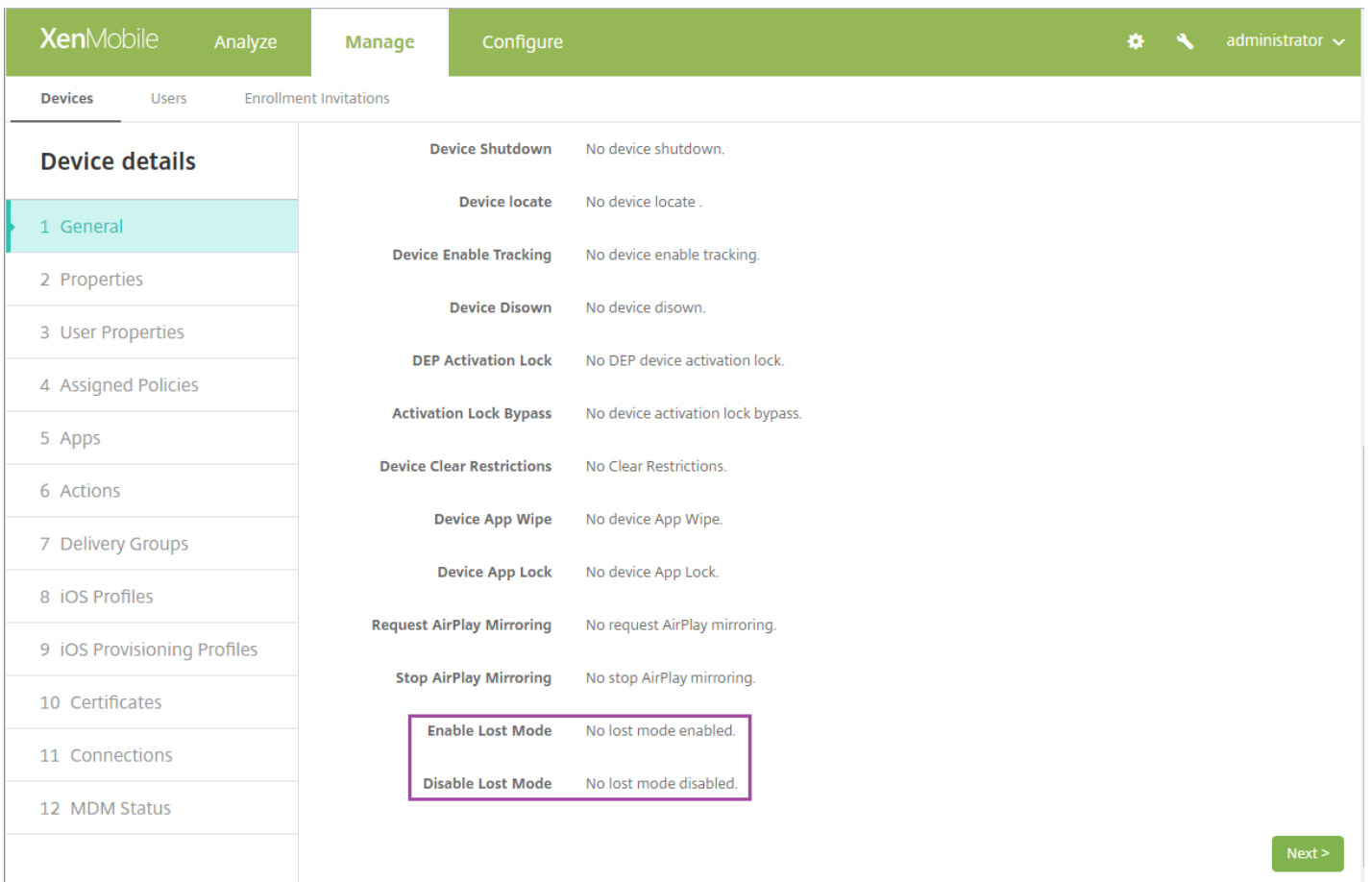
在 iOS 7 及更高版本中，还可以使用 iOS 设备锁定来远程锁定丢失或被盗的受监督设备或未受监督的设备。Apple 建议您避免将 iOS 设备锁定用于其他目的。

启用或禁用丢失模式：转至管理 > 设备，选择某个受监督的 iOS 设备，并单击安全。然后，单击启用丢失模式或禁用丢失模式。



可使用以下任何方法来检查丢失模式状态：

- 在安全操作窗口中，确认按钮是否为禁用丢失模式。
- 在管理 > 设备中常规选项卡上的安全下方，查看最后一次“启用丢失模式”或“禁用丢失模式”操作。



- 在管理 > 设备中属性选项卡上，确认已启用 MDM 丢失模式设置的值。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The user is logged in as 'administrator'. The main content area is divided into a left sidebar with 'Device details' selected, and a main panel showing device attributes. The 'MDM lost mode enabled' attribute is highlighted with a red box, showing its value as 'No'. Below this, there are sections for 'Storage space' and 'System information'.

Attribute	Value
Activation lock enabled	No
Hardware encryption capabilities	Block and file levels encryption
Internal storage encrypted	No
Jailbroken/Rooted	No
MDM lost mode enabled	No
Passcode compliant	Yes
Passcode compliant with configuration	Yes
Passcode present	No
Supervised	No
- Storage space Add	
Available storage space	10.92 GB
Total storage space	12.28 GB ×
- System information Add	
Active iTunes account	Yes
Cloud backup enabled	No

如果在 iOS 设备上启用 XenMobile 丢失模式，XenMobile 控制台也会更改，如下所示：

- 在配置 > 操作中，操作列表中不包括这些自动化操作：吊销设备，选择性擦除设备和完全擦除设备。
- 在管理 > 设备中，安全操作列表中不再包括吊销和选择性擦除设备的操作。您仍可以根据需要使用安全操作来执行完全擦除操作。

对于运行 iOS 7 及更高版本的 iPad：iOS 将“丢失的 iPad”字样附加到您在安全操作对话框的消息框中输入的内容后。对于运行 iOS 7 及更高版本的 iPhone：如果将消息框留空，并提供电话号码，Apple 将在设备锁屏界面上显示消息“呼叫所有者”。

适用于 HDX 应用程序的 SmartAccess

通过 SmartAccess 功能可以根据设备属性、用户属性或已安装的应用程序控制对 HDX 应用程序的访问。可以通过使用自动化操作将设备标记为不合规来控制访问。要使用 SmartAccess，请为 XenApp 和 XenDesktop 中的 HDX 应用程序配置拒绝访问不合规设备的 SmartAccess 策略。XenMobile 设备使用签名的加密标记将设备状态传送给 StoreFront。StoreFront 根据应用程序的访问控制策略来允许或拒绝访问。

有关详细信息，请参阅[适用于 HDX 应用程序的 SmartAccess](#)。

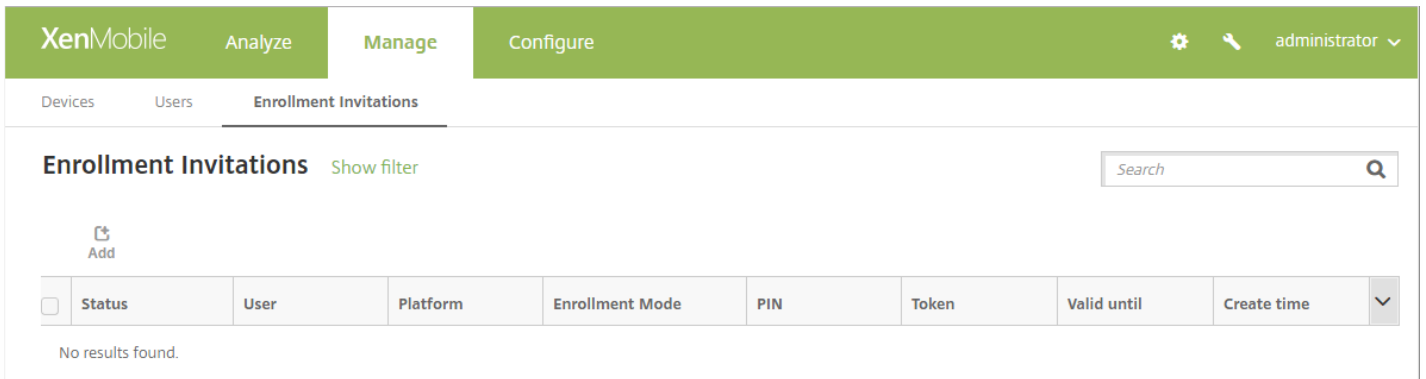
其他改进

- 支持更多语言。XenMobile 控制台现在提供日语版本。Secure Hub 现在提供阿拉伯语和俄语版本。
- WiFi 设备策略。WiFi 设备策略现在支持 Windows 10，让您可以在 WiFi 网络中使用客户端证书身份验证。要更新 WiFi 设备策略，请转至配置 > 设备策略。
- 向“PKI 实体”页面添加了“测试连接”按钮。添加 Microsoft 证书服务实体时，可以测试连接以确保服务器可访问。
- 通过数据库优化提高了稳定性。
- 针对仅 MAM 设备更改了最后访问时间。以前，在 MAM 模式下注册的设备的设备统计信息使用设备注册时间作为最后访问时间。XenMobile 现在使用最后一次联机身份验证或最后一次活动的最近时间作为最后一次访问时间。管理 > 设备页面现在包括最后一次访问时间。
- 管理域策略现在包括 Safari 密码自动填充域。对于 iOS 9.3 及更高版本的受监督设备，现在可以指定用户可以在 Safari 中从其保存密码的 URL。为此，请转至配置 > 设备策略。然后，添加或打开托管域策略，并在 Safari 密码自动填充域下方完成设置。

The screenshot shows the XenMobile 'Configure' interface for the 'Managed Domains Policy'. The left sidebar shows 'Managed Domains Policy' with sub-items: 1 Policy Info, 2 Platforms, 3 Assignment. The 'iOS' platform is selected. The main content area is titled 'Managed Domains Policy' and includes a description: 'This policy lets you define managed domains that apply to the Safari browser. The policy is supported only on iOS 8 and later devices.' Below this are three sections for adding domains: 'Unmarked Email Domains' with a 'Managed Email Domain' field and 'Add' button; 'Managed Safari Web Domains' with a 'Managed Web Domain' field and 'Add' button; and 'Safari Password AutoFill Domains' with a 'Safari Password AutoFill Domain' field and 'Add' button. The 'Policy Settings' section has 'Remove policy' options: 'Select date' (selected) and 'Duration until removal (in days)'. There is a date input field with a calendar icon. Below that is 'Allow user to remove policy' set to 'Always' with a help icon. At the bottom, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

- Secure Hub 要求 TLS 1.2。Apple 现在要求提交到 Apple App Store 的所有应用程序采用应用程序传输安全性 (ATS)。ATS 使用传输层安全性 (TLS) 协议 1.2 版，这是现在 Secure Hub 要求的服务器协议。
- 改进了用于管理注册邀请的控制台界面。为了阐明术语，XenMobile 控制台进行了以下改进：
 - 管理 > 注册页面更改为管理 > 注册邀请。

- **注册状态**列更改为**状态**。与之前一样，该列包含注册邀请状态，而不是注册状态。
- 现在，管理注册邀请时使用的术语与创建邀请时使用的术语一致。我们更改了下列标签：
类型列现在更改为**平台**。
模式列现在更改为**注册模式**。
在过滤器中，**邀请状态**现在更改为**状态**。
在过滤器中，**邀请模式**现在更改为**注册模式**。
- **模式**列中的值标签现在是创建邀请时使用的相同标签。例如，**模式**列现在显示“用户名”而不是“经典”。



- **新的服务器属性用于设置 VPP 许可证基准最小时间间隔。** XenMobile 定期重新导入 Apple 提供的 VPP 许可证以确保许可证反映所有更改。此类更改包括您何时从 VPP 手动删除导入的应用程序。默认情况下，XenMobile 按每 720 分钟的最小时间间隔为基准刷新 VPP 许可证。现在，可以通过新的服务器属性 **VPP 基准时间间隔** (vpp.baseline) 更改基准时间间隔。

如果您安装的 VPP 许可证超过 50,000，Citrix 建议增加基准时间间隔以降低导入许可证的频率和开销。如果您预计 Apple 会频繁更改 VPP 许可证，Citrix 建议降低该值以使更改及时更新到 XenMobile 中。两个基准之间的最小时间间隔为 60 分钟。

此外，XenMobile 每隔 60 分钟执行一次增量导入，以捕获自上次导入后所做的更改。将 VPP 基准最小时间间隔设置为 60 分钟可能会使基准之间的时间间隔延迟达到 119 分钟。

- **管理 > 设备的证书**选项卡现在包括 NetScaler Gateway 证书过期之前的天数。

XenMobile Analyze **Manage** Configure administrator

Devices Users Enrollment Invitations

Device details km1user1@test.com | net | 58-4200

1 General
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Actions
7 Delivery Groups
8 Certificates
9 Connections
10 TouchDown

Valid certificates

Type	Provider	Issuer	Serial number	Days to expire	Valid to
SHTTP agent		CN=Devices Certificate Authority	10252	638	11/01/2018 04:02:52 pm
NetScaler Gateway Credentials		CN=test-TEST CA, DC=test-DC=net	2787593150871711642979487540679053	2	02/03/2017 02:52:15 pm

Showing 1 - 2 of 2 items

Expired or revoked certificates

Type	Provider	Issuer	Serial number	Days to expire	Valid to
No results found.					

- 管理 > 设备页面和设备的属性选项卡现在包括 XenMobile Agent 版本和版本号。

XenMobile Analyze **Manage** Configure administrator

Devices Users Enrollment Invitations

Devices Show filter Search

Add Import Export Refresh

<input type="checkbox"/>	Status	Mode	Device platform	Operating system version	Device model	XenMobile agent revision	XenMobile agent version
<input type="checkbox"/>		MDM MAM	iOS	10.1.1	iPhone	184	10.4.5
<input type="checkbox"/>		MDM MAM	iOS	8.4.1	iPhone	22	10.4.15
<input type="checkbox"/>		MDM MAM	Android	6.0.1	Nexus 5	382546	10.4.0
<input type="checkbox"/>		MDM MAM	Android	7.0	Nexus 9	381553	10.4.0

XenMobile Analyze Manage Configure ⚙️ 🔍 administrator ▾

Devices Users Enrollment Invitations

Device details

- 1 General
- 2 Properties**
- 3 User Properties
- 4 Assigned Policies
- 5 Apps
- 6 Actions
- 7 Delivery Groups
- 8 Certificates
- 9 Connections
- 10 TouchDown

+ Screen Add

+ Security information Add

+ Storage space Add

+ System information Add

- XenMobile Agent Add

Amazon MDM API available	False
HTC MDM API available	False
NitroDesk TouchDown installed	False
Samsung KNOX API available	False
Samsung KNOX API version	1.0
Samsung SAFE API available	True
Samsung SAFE API version	4
Sony Enterprise API available	False
XenMobile agent ID	com.zenprise
XenMobile agent revision	378981
XenMobile agent version	10.3.10

- 故障排除和支持页面已经过重新排列以改进可用性。

XenMobile Analyze Manage Configure ⚙️ 🔍 administrator ▾

Troubleshooting and Support

Diagnostics

[NetScaler Gateway Connectivity Checks](#)

[XenMobile Connectivity Checks](#)

Log Operations

[Logs](#)

[Log Settings](#)

Support Bundle

[Create Support Bundles](#)

Advanced

[Cluster Information](#)

[Garbage Collection](#)

[Java Memory Properties](#)

[Macros](#)

[PKI Configuration](#)

[Anonymization and De-anonymization](#)

Links

[Citrix Product Documentation](#)

[Citrix Knowledge Center](#)




Tools

[APNs Signing Utility](#)

[Citrix Insight Services](#)

[Device NetScaler Connector Status](#)

- **日志消息。**找不到用户时生成的日志消息现在包括可能的原因。例如：无效凭据、LDAP 配置或者 LDAP 域或用户基础 DN 中缺少用户。
- **列表分页。**管理 > 设备、管理 > 注册邀请、管理 > 用户、配置 > 设备策略、配置 > 应用程序、配置 > 操作、配置 > 注册配置文件以及 配置 > 交付组上的列表现在进行分页。可以选择要在一个页面上显示的项目数。

<input type="checkbox"/>		Microsoft OneDrive - CS	Public App Store	Default	11/15/16 2:30 AM	11/15/16 2:30 AM
<input type="checkbox"/>		Microsoft PowerPoint - CS	Public App Store	Default	11/15/16 2:30 AM	11/15/16 2:30 AM
<input type="checkbox"/>		GoToMeeting - CS	Public App Store	Default	11/15/16 2:30 AM	11/15/16 2:30 AM

Showing 76 - 96 of 96 items Items per page: Page of 4

- **在用于 REST 服务的 XenMobile 公共 API 中添加了项。** REST API 现在在使用过滤器的设备调用中发送所有设备属性。API 将设备属性打包在 JSON 对象中，并在响应中包括这些属性。

REST API 现在包括针对 ShareFile Enterprise、ShareFile StorageZones 和 ShareFile StorageZone 连接器的调用。

有关详细信息，请参阅 [XenMobile Public API for REST Services](#) (用于 REST 服务的 XenMobile 公共 API) PDF。

已弃用的项目

不再支持 Windows 8.1 平板电脑。XenMobile Server 不支持 Windows 8.1 平板电脑。

适用于 Windows 8.1 平板电脑的设备策略已删除。旁加载密钥和签名证书设备策略已弃用。

已修复的问题

Apr 24, 2017

XenMobile 10.5 包含以下修复的问题。升级工具的已修复问题在本文的 [XenMobile 升级工具](#) 中列出。

有关与 XenMobile 应用程序相关的已修复问题，请参阅[已修复的问题](#)。

对于 iPhone6 设备，用户尝试使用绑定到设备 IMEI/MEID 的一次性密码邀请注册设备时，第一个配置文件成功安装。第二个 MDM 配置文件安装会失败并显示错误消息“Profile Installation Fails. A connection to the server could not be established”（配置文件安装失败。无法与服务器建立连接）。在 iPhone 设备上，一次性密码绑定到 MEID 号，而不是 IMEI 数字。[# 606162]

根据设置 > Google Play 凭据页面上的说明，不能在您的手机上通过键入 `***#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]

升级到 XenMobile 服务器 10.4 之后：

- 如果打开 ShareFile 选项卡，可能不会加载页面且不显示信息。
- 尝试添加或编辑交付组时，可能出现以下错误消息：500 Internal Server error（500 内部服务器错误）。[663344, 663788, CXM-19085]

使用 MDX Toolkit 对使用 Mowbly 框架开发的应用程序打包后，应用程序导航按钮不再有效。[#654962]

在 Secure Hub 中访问聚合的 HDX 应用程序可能会失败，并显示错误消息“获取应用程序详细信息失败，请稍后再试”。[#658058]

Citrix Launcher 部署到设备后，应用程序不显示在后台任务下。[#680978]

如果 App Controller 9.0 的 Web 代理 JSON 文件中的 Web 代理用户名中包含非转义反斜杠字符，XenMobile 服务器无法启动。[CXM-13721]

在由 Hazelcast 管理的群集 XenMobile 部署中，群集中的节点可能会间歇性地无法出现在 Hazelcast 成员列表中。[CXM-16537]

如果配置 IPsec VPN 设备策略，组名称和共享密钥未保存在设备上并丢失。[CXM-17002]

在升级到 10.3.6 后，具有多个有效身份的设备无法续订。如果有多个续订失败，XenMobile 可能会反复崩溃。[CXM-17358]

用于客户端证书身份验证的中间 CA 证书可能会出现这个问题。此问题会导致在 Android 设备上出现网络访问错误。[CXM-17401]

从 XenMobile 10.3.5 版更新至 10.3.6 版时，SQL 数据库配置可能会发生问题。[CXM-17565]

XenMobile 的内部部署版本定期对许可证服务器同步 XenMobile 签出的许可证。同步可确保计数与设备和用户的数量匹配。这样，如果 XenMobile 检测到不匹配，会在 24 小时内解决问题。[CXM-18129]

XenMobile 控制台要求您为 WiFi 策略指定密码，尽管该密码是可选的。[CXM-18249]

由于日期格式错误，XenMobile 不会部署用户配置文件。[CXM-18250]

如果在 Internet Explorer 11 浏览器上使用 XenMobile 控制台，无法添加和编辑 LDAP 配置。[CXM-18324]

如果为所有设备类型创建 Exchange 策略，且该策略包含针对域 `$user.dnsroot` 的宏，则该策略不会部署。[CXM-18545]

如果交付组名称包含 & 符号，将策略分配到该交付组会导致出现错误。[CXM-18768]

在**设置 > iOS 批量注册**中首次配置 DEP 设置后，单击**保存**时显示此错误：“不存在名为‘Worx Home by Citrix’的资源包(容器)”。为了解决此问题，请在配置 DEP 设置后创建交付组 (**配置 > 交付组**)，并在错误页面上单击**确定**。交付组必须包含以下内容：

- 名为 **Device Enrollment Program Group** 的用户组
- **策略 DEP 软件清单**
- 所需的应用程序 **Secure Hub by Citrix**

如果在 2016 年 10 月 6 日 Citrix Secure Hub 出现在 Apple Store 中之前配置了 DEP，此问题不会影响现有注册。[CXM-19158]

对于邀请注册或注册 PIN 模板：如果模板中的消息包括某些宏，则发送给用户的消息包括宏，而不是用户信息。这些宏是注册 URL (`{enrollment.url}`) 和注册 PIN (`{enrollment.pin}`)。[CXM-19210]

有时无法上载企业应用程序，因为尽管有应用程序图标，但是 XenMobile 仍无法找到该图标。[CXM-19213]

在**设置 > PKI 实体 > 任意 CA**页面上，如果有多页证书，只能查看第一页的 CA 证书。[CXM-19736]

对于部署到多个设备的交付组：如果在**配置 > 交付组**上单击交付组，然后单击**部署**下方的按钮，则**管理 > 设备**页面上显示不正确的设备列表。[CXM-19737]

如果 iOS App Store 或 Google Play 应用商店中有 XenMobile 应用程序更新：在用户打开应用程序后，不会在 XenMobile Store 中显示应用程序更新提示。[CXM-19927]

对于父域和子域处于树-根信任关系中的域，包括 `$user.dnsroot` 的 XenMobile 宏不能进行解析。[CXM-20366]

如果 sAMAccountName 与 UPN 的名称部分不同，客户端属性 SEND_LDAP_ATTRIBUTES 的宏解析会失败。例如：sAMAccountName 是 `samplename`，而 UPN 是 `sample@example.com`。[CXM-20414]

如果 XenMobile 处于 MDM 模式，并且您要使用 DEP 阶段提供的用户凭据进行 DEP 注册：如果用户在注册后较短时间间隔内从设备中删除 Secure Hub，服务器将进入不一致的状态。较短时间间隔可能是一个小时。[CXM-20924]

设备不会在自动化操作后自动进入合规状态。[CXM-21006]

对于包括某些用户组限制的自定义 RBAC 角色的 RBAC 管理员：如果用户组中的 Active Directory 用户具有一些注册的设备，**管理 > 设备**页面打开速度较慢。[CXM-21007, CXM-21009]

升级到 XenMobile 10.3.6 后，即使 RBAC 配置限制了访问权限，具有自定义 RBAC 角色访问权限的管理员仍可以看到其他域中的已注册设备。[CXM 21008]

XenMobile 群集成员可能不响应某些 HTTP 请求，这会导致用户由于**公司网络不可用**错误而无法注册。[CXM-21010]

如果 iOS 批量注册设置中启用了**需要提供凭据才能完成设备注册**，针对 DEP 注册的任何类型的邀请都会导致 XenMobile 服务器出现错误。错误包括 Secure Hub 中的错误消息、XenMobile 控制台中的错误消息以及所有设备丢失 MDM 功能。要解决此问题，请在**管理 > 注册**页面上删除受影响用户的所有注册邀请。然后重新启动 XenMobile 服务器。[CXM-21500]

对于配置了通行码的 iOS 设备，XenMobile 丢失模式触发的自动操作失败。丢失模式触发的所有可用操作都存在此问题：**应用程序擦除**、**应用程序锁定**、**将设备标记为不合规**以及**发送通知**。[CXM-21579]

从**分析 > 报告生成**的设备和应用程序报告中显示的每个设备的应用程序安装计数不正确。[CXM-21773]

在 XenMobile 控制台上添加 Skype for Business 公共应用程序时，可能不显示图标。但是，可以在控制台中搜索并添加应用程序。

序，且该应用程序可以安装在设备上。[CXM-21774, #668341]

一些适用于 Android 的企业应用程序不能上载到以 MDM 或 XME 模式配置的 XenMobile 控制台。[CXM-22377]

基于动态设备属性（例如当前移动国家/地区代码）部署资源不起作用。XenMobile 忽略规则并允许资源（例如设备策略、应用程序和操作）在设备上部署。[CXM-22565]

无法使用 XenMobile CLI 创建支持包。解决方法：使用 XenMobile 控制台：转到**支持 > 创建支持包**，然后单击**创建**。[CXM-23091]

升级到 XenMobile 10.3.6 后，Secure Hub 不再包括 HDX 应用程序。日志包括条目“Unable to get the Config xml data Host name”（无法获取配置 xml 数据主机名称）。[CXM-23177]

如果只编辑设备策略的平台详细信息：所做编辑不会在**配置 > 设备策略**上触发对上次更新时间的更改。上次更新时间在添加或删除平台后更改。[CXM-23178]

如果您的浏览器语言设置为法语，无法在 XenMobile 控制台中创建和编辑 WiFi 设备策略。[CXM-23180]

尽管 iOS 设备处于活动状态并与正在与 XenMobile 服务器通信，但**管理 > 设备**页面上 iOS 设备显示为非活动状态。在日志中此问题如下所示：

```
java.lang.IllegalStateException: Cannot load backing target entity: has been deleted. [CXM-23181]
```

如果服务器属性 **StorageZone 连接器支持的值是不支持**且您配置 **ShareFile**：导航到另一个控制台页面后，然后返回到**配置 > ShareFile**，**ShareFile** 页面上不会显示配置，尽管保存了配置。要解决此问题，请将服务器属性 **ShareFile 配置类型**更改为**企业**。[CXM-23337]

删除了 DEP 设备，然后重新注册该设备，重新注册可能会失败，并出现错误“Invalid profile”（配置文件无效）。[CXM-24078]

此版本包含 CVE-2016-5195 的深度防御措施，也称为 Linux 脏牛 (Dirty Cow)。

如果 XenMobile 9 中的部署包括 **gpsstats.apk** 企业应用程序，升级到 XenMobile 10.4 可能会失败。[CXM-17992]

从 XenMobile 9 升级到 XenMobile 10.4 后，Windows 和 iOS 设备处于 MDM 模式而不是 MAM+MDM 模式。此外，XenMobile Store 不会打开。解决办法：用户可以重新注册迁移的设备。[CXM-18532, CXM-23408]

从 XenMobile 9 升级到 XenMobile 10.4 后，XenMobile 有来自先前重新注册的重复的非活动仅 MAM 记录。即使 XenMobile 9 要求了 Device Manager 注册，也会出现该问题。[CXM-18544]

从 XenMobile 9.0 升级到 XenMobile 时 10.4.x 过程中：升级工具不会在设备属性表中更新在 XME (MDM+MAM) 模式下注册的设备的设备名称。[CXM-20821]

如果 App Controller 数据库包含 **username** 数据格式的用户，从 XenMobile 9.0 升级到 XenMobile 10.x 会失败。应使用 **domain\username** 或 **username@domain** 数据格式。[CXM-21072]

如果 HTTP 和 HTTPS 的 .p12 服务器证书的路径的大小写不同，从 XenMobile 9.0 升级到 XenMobile 10.4.x 会失败。例如，如果 HTTP 路径是 **Certificates\MDM.p12**，HTTPS 路径是 **certificates\MDM.p12**。[CXM-21581]

从 XenMobile 9 升级到 10.x 之后，XenMobile Store 不包含应用程序。此外，XenMobile 不会将本地组分配到交付组。如果本地用户属于本地组且本地用户注册设备，会出现此问题。[CXM-23375]

如果 Device Manager 有 Active Directory 用户的两条记录，且那些记录不匹配（如下所示），升级会失败：

- 记录有不同的 UPN。例如，一条用户记录的 UPN 为 john.smith@eng.domain.com。另一条记录为 john.smith@domain.com。
- 记录中的 sAMAccountName 大小写不同。例如，一条用户记录的 sAMAccountName 为 johns。另一条记录为 JOHNS。
[CXM-23382]

从 XenMobile 9 升级到 XenMobile 10.x 之后：无法使用 iPhone 配置实用程序或 Apple Configurator 在升级的 XenMobile 控制台中编辑之前在 Device Manager 中自定义的配置策略。[CXM-23942]

已知问题

May 11, 2017

XenMobile 10.5 包括以下已知问题。已修复的升级工具问题在本文中的标题“XenMobile 升级工具”下列出。

要了解与 XenMobile 应用程序有关的已知问题，请参阅[已知问题](#)。

使用 NetScaler 12.0.41.16 时，如果 Secure Mail 配置了 STA，在 iOS 和 Android 设备上邮件同步会失败。此问题在 NetScaler 12.0 Build 41.22 中已修复。有关详细信息和更新，请参阅此[支持知识中心](#)文章。[#685075]

将 StoreFront 与 XenMobile 集成并部署 HDX 应用程序时，更改了 Active Directory 密码后，HDX 应用程序从 XenMobile Store 冲消失。[CXM-9859]

升级到 XenMobile 10.4.2 后，对于嵌套 Active Directory 组中的用户，Android for Work 应用程序不显示在设备上。[CXM-19930]

从 XenMobile 10.3.6 升级到 XenMobile 10.5 可能会将已注册的运行 Android for Work 的设备的设备所有者更改为“anonymous”。[CXM-19933]

即使您的 XenMobile 配置中的在证书过期时续订设置为关，用户也可以续订证书。[CXM-20923]

针对组中有权使用 StorageZone 连接器的 Active Directory 用户：如果将用户移出该组，ShareFile for iOS 用户仍然能够访问与这些连接器关联的网络共享。要解决此问题，请重新安装 ShareFile for iOS 应用程序。[CXM-21859]

如果将某个 StorageZone 连接器从交付组 A 移至 B，交付组 A 中的 ShareFile for iOS 用户可以继续使用该连接器。[CXM-21860]

如果 XenMobile 使用自签名证书，用户无法将 iOS 10.3 设备注册到 XenMobile 中。此限制源于 iOS 10.3 中的一个更改。要将运行 iOS 10.3 或更高版本的设备注册到 XenMobile 中，必须在 XenMobile 中使用可信 SSL 证书。[CXM-24120]

部署应用程序时，如果应用程序已安装在设备上，但从未打开，系统将显示一条提示，告知用户安装该应用程序。作为此问题的修复的一部分，如果在服务器上更新了某个应用程序，则在启动该应用程序之前，不会在用户设备上对其进行更新。[CXM-32193]

从 XenMobile 9 升级到 XenMobile 10.4 后，适用于 Windows 设备的某些策略将在 XenMobile 控制台中显示，即使在 XenMobile 部署这些策略后亦如此。具体而言，这些策略保留在管理 > 设备的已分配的策略页面的挂起选项卡上。解决方法：编辑并重新部署显示为“挂起”的所有策略。该操作将从挂起选项卡中清除适用于 Windows Phone 的策略。适用于 Windows Tablet 的 Web 剪辑策略保留在挂起选项卡上，即使该策略在设备上正常运行也是如此。[CXM-21769]

体系结构

Apr 13, 2017

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，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，以及跟踪用户设备类型，可以部署 XenMobile 与 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。通过该连接可以访问内部网络中的应用程序和桌面。
- 设备注册。用户可以在 XenMobile 中注册移动设备，这样一来，您便可以在 XenMobile 控制台中管理连接到网络资源的设备。
- Web、SaaS 和移动应用程序。用户可以从 XenMobile 通过 Secure Hub 访问其 Web、SaaS 和移动应用程序。
- 基于 Windows 的应用程序和虚拟桌面。用户可以通过 Citrix Receiver 或 Web 浏览器进行连接，以从 StoreFront 或 Web Interface 访问基于 Windows 的应用程序和虚拟桌面。

要在内部部署的 XenMobile 服务器上实现其中任何功能，Citrix 建议按以下顺序部署 XenMobile 组件：

- NetScaler Gateway。可以使用快速配置向导在 NetScaler Gateway 中配置设置，以实现与 XenMobile、StoreFront 或 Web Interface 的通信。在 NetScaler Gateway 中使用快速配置向导前，必须先安装以下组件之一才能建立通信：XenMobile、StoreFront 或 Web Interface。
- XenMobile。安装 XenMobile 后，可以在 XenMobile 控制台中配置策略和设置，以允许用户注册其移动设备。您也可以配置移动应用程序、Web 应用程序和 SaaS 应用程序。移动应用程序可以包括 Apple App Store 或 Google Play 中的应用程序。用户还可以连接到您通过 MDX Toolkit 打包并上载到控制台的移动应用程序。
- MDX Toolkit。MDX Toolkit 可以安全地打包在贵组织中或公司外创建的移动应用程序，例如 XenMobile 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 通过 XenMobile 控制台提供设备管理和应用程序管理。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。此外，利用 NetScaler SSL 卸载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 NetScaler 上配置两个负载平衡虚拟 IP 地址来设置 XenMobile 群集的详细信息，请参阅[群集](#)。

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

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[适用于内部部署的参考体系结构](#)和[适用于云部署的参考体系结构](#)。有关端口的完整列表，请参阅[端口要求](#)（内部部署）和[端口要求](#)（云）。

移动设备管理 (MDM) 模式

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

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

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

移动应用程序管理 (MAM) 模式

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

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

设备不能进行 MDM 注册。

在此部署模型中，XenMobile 服务器与 NetScaler Gateway 位于前端，后者为 XenMobile 提供更多的保护。

MDM+MAM 模式

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

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

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

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

系统要求和兼容性

Mar 31, 2017

有关更多要求和兼容性信息，请参阅以下文章：

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

要运行 XenMobile 10.5，需要满足以下最低系统要求：

- 以下其中一种：
 - XenServer（支持的版本：6.5.x 或 7.0）；有关详细信息，请参阅 [XenServer](#)
 - VMware（支持的版本：ESXi 5.5 或 ESXi 6.0）；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
- 4 个虚拟 CPU
- 对于生产环境：8 GB RAM；对于概念验证和测试环境：4 GB RAM
- 50 GB 磁盘空间

XenMobile 10.5 版要求使用 Citrix 许可证服务器 11.12.1 或更高版本。

要在 XenMobile 10.5 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：6.5 或 7.0）
 - VMWare（支持的版本：ESXi 4.1、ESXi 5.1、ESXi 5.5、ESXi 6.0）
 - Hyper-V（支持的版本：Windows Server 2008 R2、Windows Server 2012 或 Windows Server 2012 R2）
- 2 个虚拟 CPU
- 2 GB RAM
- 20 GB 磁盘空间

您还必须能够与 Active Directory 通信，这需要使用服务帐户。您只需具有查询和读取权限。

XenMobile 需要使用以下数据库之一：

- Microsoft SQL Server

XenMobile 存储库支持在以下其中一个受支持的版本上运行的 Microsoft SQL Server 数据库。有关 Microsoft SQL Server 数据库的详细信息，请参阅 [Microsoft SQL Server](#)。

Microsoft SQL Server 2016

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

XenMobile 10.5 支持 SQL AlwaysOn 可用性组和 SQL 群集以实现数据库高可用性。

Citrix 建议远程使用 Microsoft SQL。

注意：确保要在 XenMobile 上使用的 SQL Server 服务帐户具有 DBcreator 角色权限。有关 SQL Server 服务帐户的详细信息，请参阅 Microsoft Developer Network 站点上的以下页面。这些链接提供有关 SQL Server 2014 的信息。如果您使用的是其他版本，请从 **Other Versions**（其他版本）列表中选择您的服务器版本：

[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 9.5.2 和 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

StoreFront 3.9

StoreFront 3.8

StoreFront 3.7

StoreFront 3.6

StoreFront 3.5

StoreFront 3.0

Web Interface 5.4

XenApp 和 XenDesktop 7.13

XenApp 和 XenDesktop 7.12

XenApp 和 XenDesktop 7.11

XenApp 和 XenDesktop 7.9

XenApp 和 XenDesktop 7.8

XenApp 和 XenDesktop 7.7

XenApp 和 XenDesktop 长期服务版本 (LTSR)

XenApp 和 XenDesktop 7.6

XenApp 和 XenDesktop 7.5

XenApp 6.5

XenMobile 10.5 支持以下邮件服务器：

- Exchange 2016
- Exchange 2013
- Exchange 2010

XenMobile 兼容性

Jun 05, 2017

Important

- Citrix 同时支持 XenMobile 生产力应用程序的企业分发和公共应用商店分发，直到 2017 年 12 月 31 日。有关详细信息，请参阅 [Citrix Product Matrix](#) (Citrix 产品列表)。您必须在此日期之前迁移到公共应用商店应用程序。之后，只支持公共应用商店分发。有关从 XenMobile Apps 企业版本迁移到公共应用商店版本的应用内指南的详细信息，请参阅[面向迁移到公共应用商店应用程序的应用内指南](#)。MDX Toolkit 继续面向应用程序开发人员支持企业打包功能。
- 自版本 10.4 起，Worx 移动应用程序已重命名为 XenMobile Apps。所有的 XenMobile Apps 都已重命名。有关详细信息，请参阅[关于 XenMobile Apps](#)。

本文概述了可以集成的受支持的 XenMobile 组件的版本。这些组件包括 NetScaler Gateway 以及打包、配置和分发 XenMobile Apps 时需要运行的 MDX Toolkit 版本。

支持的版本和升级路径

对于 XenMobile Server 和应用程序，Citrix 支持当前版本以及之前两个版本的 XenMobile。例如，如果当前版本是 XenMobile Server 10.5，Citrix 还支持 10.4 和 10.3.6 版。版本包括发行版和服务包。XenMobile 10.4 是服务包，而不是完整发行版。

已结束对 XenMobile 9 的维护。有关详细信息，请参阅[产品列表](#)。Citrix 支持从 XenMobile 9 升级到 XenMobile 10 最新版本。

	升级支持声明	最新版本	升级自
企业打包应用程序 (例如 Secure Mail 和 Secure Web)	最后两个版本	10.4.5 (iOS), 10.4.6 (Android)	10.3.10 或 10.4
公共应用商店应用程序 (例如 Secure Hub、Secure Mail 和 Secure Web)	最后两个版本 启用了自动更新的用户从应用程序商店接收最新版本。 最新的应用程序支持以前的两个 MDX 文件。	10.5.20 (Secure Hub) 10.5.20 (Secure Mail) 10.5.20 (Secure Web)	10.5.10 或 10.5.15 (Secure Hub) 10.5.10 或 10.5.15 (Secure Mail) 10.5 和 10.5.10 (Secure Web) 例如，10.5.20 版本的 Secure Mail 与 10.5.15 或 10.5.10 MDX 文件兼容。
MDX	早期版本	10.4.10	10.4.5

服务器（内部部署）	最后两个版本和从 XenMobile 9 RP5 的升级	10.5	10.4、10.3.6、XenMobile 9 RP5
-----------	------------------------------	------	-----------------------------

XenMobile 兼容性

要使用新增功能、修复和策略更新，Citrix 建议您安装最新版本的 MDX Toolkit、Secure Hub 和 XenMobile Apps。

- 适用于企业分发的应用程序、MDX Toolkit 和 Secure Hub :
 - 最新版本的应用程序和 MDX Toolkit 需要最新版本的 Secure Hub。
 - 对于最新版本的应用程序，需要最新版本的 MDX Toolkit。
 - 前两个版本的应用程序和前一个版本的 MDX Toolkit 与最新版本的 Secure Hub 兼容。
- 客户端和服务端：最新版本的 Secure Hub、MDX Toolkit 和 XenMobile Apps 与最新版本和前两个版本的 XenMobile Server 兼容。
- 公共应用商店应用程序只与 XenMobile 10.4 及更高版本兼容。
- 在 XenMobile 9 于 2017 年 6 月结束生命周期之前，企业打包应用程序与 XenMobile 9 兼容。

支持的 NetScaler Gateway 版本：

- 11.1.x
- 11.0.x
- 10.5.x

Important

XenMobile 当前不支持 NetScaler 12.0.41.16。此问题在 NetScaler 12.0 Build 41.22 中已修复。有关详细信息和更新，请参阅此[支持知识中心文章](#)。

MDX Toolkit for iOS 和 MDX Toolkit for Android 版本	兼容的 Secure Hub 版本	
	Android	iOS
10.4.10	10.5.20	10.5.20
10.4.5	10.5.15	10.5.15
适用于 Windows Phone 的 MDX Toolkit	兼容的 Secure Hub 版本	
10.3.9	10.3.5	
10.3.1	10.3	

注意

XenMobile 10.1 不支持 Windows Phone 10。

对于 XenMobile 9，必须安装面向应用程序的修补程序才能正确运行。有关详细信息，请参阅 [CTX217942](#)。

	Android	iOS
Secure Hub	10.5.20	10.5.20
Secure Mail	10.5.20	10.5.20
Secure Web	10.5.20	10.5.20
Secure Notes	10.4.5	10.4.5
Secure Tasks	10.4.5	10.4.5
QuickEdit	6.10	6.10
ShareFile	5.4	5.3
ShareConnect		3.3
ScanDirect		1.2.2

XenMobile 10.x 和 9 支持下表中列出的 Worx 移动应用程序/XenMobile Apps 版本。

应用程序	Android	iOS	Windows Phone ¹
Secure Hub	10.5.15	10.4.10	
	10.5.10	10.4.5	
Worx Home	10.3.10	10.3.10	10.0.3

	10.3.9	10.3.9	10.0.0
Secure Forms		10.4.5 10.4.1	
Secure Mail	10.4.6 10.4.5	10.4.5 10.4.0.19	
WorxMail	10.3.10 10.3.9	10.3.10 10.3.9	10.2 10.0.7
Secure Notes	10.4.5 10.4.1	10.4.5 10.4.1	
Worx Notes	10.3.10 10.3.9	10.3.10 10.3.9	
Secure Tasks	10.4.5 10.4.1	10.4.5 10.4.1	
WorxTasks	10.3.10 10.3.9	10.3.10 10.3.9	
Secure Web	10.4.5 10.4.1	10.4.5 10.4.1	
WorxWeb	10.3.10 10.3.9	10.3.10 10.3.9	10.2 10.0.3
QuickEdit ²	6.10	6.10	
ScanDirect		1.2.2	
ShareConnect	3.2.341	3.3	

ShareFile	5.4	5.3	
-----------	-----	-----	--

¹ XenMobile 10.1 不支持 Windows Phone 10。

² XenMobile 仅支持最新版本的 QuickEdit、ShareConnect 和 ShareFile。

XenMobile 10.x 支持以下浏览器：

- Internet Explorer 9 或更早版本
- Chrome
- Firefox
- 移动设备上的 Safari，用于访问自助服务门户

XenMobile 10.x 与最新版本的浏览器以及当前版本之前的一个版本兼容。

支持的设备操作系统

Jun 05, 2017

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

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

本文中支持的设备平台信息还适用于 XenMobile Mail Manager 和 XenMobile NetScaler Connector。

注意

- Citrix 最低支持每个主操作系统平台的当前版本和之前版本。并非 XenMobile 较新版本的所有功能都能在较旧的平台版本上运行。本文详细介绍了 Citrix 支持的适用于每个操作系统的功能。本文还包括 Citrix 测试过的设备型号。对于在使用其他设备型号时遇到的问题，请联系 Citrix 支持。
- 自 10.4 版起，Worx 移动应用程序已重命名为 XenMobile 应用程序。所有的 XenMobile 应用程序都已重命名。有关详细信息，请参阅[关于 XenMobile 应用程序](#)。

Android

XenMobile 10.x

所有模式都支持的操作系统：Android 4.4.x、5.x、6.x、7

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

Worx Home/Secure Hub 在基于 x86 的 Android 设备上支持 MDM 功能。在 XenMobile 10 和 10.1 上，应用程序管理仅在使用基于 ARM 的处理器器的 Android 设备上可用。MDX 打包的应用程序在基于 x86 的 Android 设备上不受支持。

MDX 打包的 Worx 应用程序/XenMobile 应用程序在基于 x64 的 Android 设备上受支持。

在 MDM+MAM (企业) 模式下 XenMobile 10.x 上专门测试过的 Android 设备和操作系统

- Google Nexus 7 平板电脑 (操作系统 4.4.4)
- Google Nexus 9 平板电脑 (操作系统 7.0)
- Google Nexus 5 (操作系统 6.0.1)
- Google Nexus 5X (操作系统 7.1.1)
- Google Pixel
- Galaxy S4 型号 GT-I9500 (获得 Root 权限) (操作系统 4.2.2)
- Galaxy S7 (操作系统 7.0)
- Galaxy S6 (操作系统 6.0.1、5.0)
- Galaxy Tab A (操作系统 6.0)
- Galaxy Note3 型号 SM-N900 (操作系统 5.0)
- Galaxy S4, GT-I9500 (操作系统 5.0.1)
- Galaxy S3 型号 GT-I9305 (操作系统 4.4.4)

- Galaxy S4 GT-I9505 (操作系统 4.3)
- Moto Turbo (操作系统 6.0.1)
- Nexus 9 Tab (操作系统 5.0.1)
- Nexus 9 Tab (操作系统 5.1.1)
- Nexus 7 (操作系统 4.4)
- Nexus 6P 操作系统 7.1.1 版
- Nexus 5 (操作系统 5.0.1)
- Galaxy S6 Edge , SM-G925F (操作系统 6.0.1)
- 华为 Nexus 6 (操作系统 6.0.1 和 7.0)
- Sony Xperia , 型号 : SGP311 (操作系统为 5.0.1)
- Galaxy S5 SM-G900F (操作系统 6.0.1)
- Galaxy S5 SM-G900H (操作系统 6.0.1)
- HTC One M8 (操作系统 4.4.2)

在仅 MDM 模式下 XenMobile 10.x 上专门测试过的 Android 设备和操作系统

- Google Nexus 7 平板电脑 (操作系统 4.4.4)
- Google Nexus 9 平板电脑 (操作系统 7.0)
- Google Nexus 5 (操作系统 6.0.1)
- Google Nexus 5X (操作系统 7.1.1)
- Google Pixel
- Galaxy S7 (操作系统 7.0)
- Galaxy S6 (操作系统 6.0.1、5.0)
- Galaxy Tab A (操作系统 6.0)
- Galaxy S4 型号 GT-I9500 (获得 Root 权限) (操作系统 4.2.2)
- Galaxy Note3 型号 SM-N900 (操作系统 5.0)
- Galaxy S4 , GT-I9500 (操作系统 5.0.1)
- Galaxy S3 型号 GT-I9305 (操作系统 4.4.4)
- Galaxy S4 GT-I9505 (操作系统 4.3)
- Nexus 9 Tab (操作系统 5.0.1)
- Nexus 9 Tab (操作系统 5.1.1)
- Nexus 7 (操作系统 4.4)
- Nexus 5 (操作系统 5.0.1)
- Galaxy S6 Edge , SM-G925F (操作系统 6.0.1)
- 华为 Nexus 6 (操作系统 6.0.1 和 7.0)
- Sony Xperia , 型号 : SGP311 (操作系统为 5.0.1)
- Galaxy S5 SM-G900F (操作系统 6.0.1)
- Galaxy S5 SM-G900H (操作系统 6.0.1)
- HTC One M8 (操作系统 4.4.2)

此外，还使用 Secure Mail 测试了以下设备类型。

设备类型	操作系统
Samsung S7	7.0
Samsung S6	6.0.1

Samsung S5	5
Samsung Tab A	6.0.1
Nexus 7	4.4.4

SAFE 和 KNOX

在兼容的 Samsung 设备上，XenMobile 10.x 可同时支持和扩展 Samsung for Enterprise (SAFE) 和 Samsung KNOX 策略。XenMobile 要求您先启用 SAFE API，然后再部署 SAFE 策略和限制。为此，应将内置 Samsung Enterprise License Management (ELM) 密钥部署到设备。要启用 Samsung KNOX API，请执行以下操作：

1. 使用 Samsung KNOX License Management System (KLMS) 购买 Samsung KNOX 许可证。
2. 部署 Samsung ELM 密钥。

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

iOS

注意

iOS 10.3 设备不支持自签名证书。如果 XenMobile 使用自签名证书，用户无法将 iOS 10.3 设备注册到 XenMobile 中。要将运行 iOS 10.3 或更高版本的设备注册到 XenMobile 中，必须在 XenMobile 中使用可信 SSL 证书。

所有 Worx 应用程序/XenMobile 应用程序都与自版本 10.3.10 或更高版本起的 iOS 10 兼容。应使用 MDX Toolkit 10.3.10 或更高版本打包移动应用程序或企业应用程序，才能确保与 iOS 10 正确兼容。如果用户升级到 iOS 10，还必须升级到 Worx Home 10.3.10 或更高版本 (Secure Hub) 才能使用 MDX 应用程序。有关详细信息，请参阅此[知识中心文章](#)。

XenMobile 10.3.x、10.4 和 10.5

- iOS 10.x
- iOS 9.x
- iOS 8.x (仅限 MDM 部署中的 Worx Home/Secure Hub)

XenMobile 10.3.x 和 10.4 支持的部分 iOS 设备：

- iPhone 7 + 10.2.1 (XenMobile 10.5 及更高版本)
- iPhone 6、6+、6S、6S+、5s、5、5c
- iPad 2、3
- iPad Air、iPad Air-2、iPad Mini-4、Mini-3、Mini-2
- iPad Pro
- Mac OS X

- MacBook、Air、Mini、Mini Retina 10.9.5、10.10、10.11

XenMobile 10 和 10.1

- iOS 10.x
- iOS 9.x
- iOS 8.x (仅限 MDM 部署中的 Worx Home)

XenMobile 10 和 10.1 支持的部分 iOS 设备：

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

Windows Phone 和 Tablet

XenMobile 10.5

- Windows 10 Phone 和 Tablet
 - 如果 XenMobile 处于仅 MAM 模式，则不支持。
- Windows Phone 8.1 与 Worx Home 的兼容性。
 - 如果 XenMobile 处于企业模式：Worx Home 10.0。
 - 如果 XenMobile 处于仅 MDM 模式：Worx Home 9.1.0。
- Windows Mobile/CE
 - 如果 XenMobile 处于仅 MAM 模式，则不支持。

XenMobile 10.3.x 和 10.4

- Windows 10 RS1，8.1 Tablet
 - 如果 XenMobile 处于仅 MAM 模式，不支持 Windows 10 Tablet。
- Windows Tablet Surface Pro 3、Surface 2、RT
- Windows Phone 10、8.1
 - 对于 Windows Phone 10，必须安装从 [XenMobile 下载页面](#) 中的修补程序。
 - 如果 XenMobile 处于仅 MAM 模式，则不支持。
- Windows Phone 8.1 与 Worx Home 的兼容性：
 - Worx Home 10.0 (如果 XenMobile 处于企业模式)。
 - Worx Home 9.1.0 (如果 XenMobile 处于仅 MDM 模式)。
- Windows 8.1 Pro Edition 和 Enterprise Edition (32 位和 64 位)
- Windows RT 8.1
- Windows Mobile/CE
 - 如果 XenMobile 处于仅 MAM 模式，则不支持。

XenMobile 10.3 支持的部分 Windows 设备：

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

- Windows Tablet RT

XenMobile 10 和 10.1

- Windows 10 RS1 Tablet
- Windows Phone 8.1/10 :
 - 如果 XenMobile 处于仅 MAM 模式，不支持 Windows Phone 8.1。
 - Windows Phone 10 在 XenMobile 10.3 及更高版本上受支持。
 - Windows Phone 10 在 XenMobile 9 上受支持，但必须安装 Device Manager 滚动修补程序，如此[知识中心文章](#)中所述。此外，请记录适用于 Windows Phone 的 Windows 10 Anniversary Update 1607 的修补程序。有关详细信息，请参阅此[知识中心文章](#)。
- Windows Phone 8.1 与 Worx Home 的兼容性 :
 - Worx Home 10.0 (如果 XenMobile 处于企业模式)
 - Worx Home 9.0.3 (如果 XenMobile 处于仅 MDM 模式)
- Windows 8.1 Pro Edition 和 Enterprise Edition (32 位和 64 位)
- Windows RT 8.1
- Windows Mobile : XenMobile 10.1 不支持 Windows Mobile 设备。如果用户使用的是运行 Windows Mobile 或 Windows CE 的设备，则必须继续使用 XenMobile 9。

XenMobile 10 和 10.1 支持的部分 Windows 设备 :

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

Windows Phone 7 通过 XenMobile Mail Manager 进行管理。有关详细信息，请参阅[安装 XenMobile Mail Manager](#)。

Symbian

XenMobile 10.3.x、10.4 和 10.5

XenMobile 10.3.x、10.4 和 10.5 不支持 Symbian。

XenMobile 10 和 10.1

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

- Symbian 3
- Symbian S60 第五版
- Symbian S60 第三版，Feature Pack 2
- Symbian S60 第三版，Feature Pack 1
- Symbian S60 第三版
- Symbian S60 第二版，Feature Pack 3
- Symbian S60 第二版，Feature Pack 2

黑莓

黑莓设备通过 XenMobile Mail Manager 进行管理。有关详细信息，请参阅[安装 XenMobile Mail Manager](#)。

端口要求

May 22, 2017

要使设备和应用程序能够与 XenMobile 通信，应在防火墙中打开特定端口。下表列出了必须打开的端口。有关 XenMobile Service 的端口要求，请参阅[端口要求](#)。

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

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

- XenMobile
- StoreFront
- XenDesktop
- XenMobile NetScaler Connector
- 其他内部网络资源，例如 Intranet Web 站点

要实现从 NetScaler 到 Launch Darkly 的通信，可以使用此[支持知识中心文章](#)中所述的 IP 地址。

有关 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，请参阅 NetScaler 文档中的[NetScaler 如何与客户端和服务进行通信](#)。该节包括有关 NetScaler IP (NSIP) 虚拟服务器 IP (VIP) 和子网 IP (SNIP) 地址的信息。

TCP 端口	说明	源	目标
21 或 22	用于将支持包发送到 FTP 或 SCP 服务器。	XenMobile	FTP 或 SCP 服务器
53 (TCP 和 UDP)	用于 DNS 连接。	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	用于枚举、票证记录和身份验证的 XML 和 Secure Ticket Authority (STA) 端口。	StoreFront 和 Web Interface XML 网络流量	XenDesktop 或 XenApp
443	Citrix 建议使用端口 443。	NetScaler Gateway STA	

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

	Windows 的应用程序。Citrix 建议保持此端口处于打开状态。		
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

打开以下端口以允许 XenMobile 在网络中通信。

TCP 端口	说明	源	目标
25	用于 XenMobile 通知服务的 SMTP 端口。如果 SMTP 服务器使用其他端口，请确保防火墙不会阻止该端口。	XenMobile	SMTP 服务器
80 和 443	与 Apple iTunes App Store (ax.itunes.apple.com)、Google Play (必须使用 80) 或 Windows Phone 应用商店建立的企业应用商店连接。用于通过 iOS 上的 Citrix Mobile Self-Serve、适用于 Android 的 Secure Hub 或适用于 Windows Phone 的 Secure Hub 从应用商店发布应用程序。	XenMobile	Apple iTunes App Store (ax.itunes.apple.com 和 *.mzstatic.com) Apple 批量购买计划 (vpp.itunes.apple.com) 对于 Windows Phone : login.live.com 和 *.notify.windows.com Google Play (play.google.com)
80 或 443	用于 XenMobile 与 Nexmo SMS Notification Relay 之间的出站连接。	XenMobile	Nexmo SMS Relay 服务器
389	用于非安全 LDAP 连接。	XenMobile	LDAP 身份验证服务器或 Active Directory
443	用于 Android 和 Windows Mobile 的注册和代理安装。 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。	Internet 内部 LAN 和 WiFi	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	WiFi 网络上的 iOS 设备	Internet (使用公用 IP 地址)

	*.push.apple.com 的 APNs 出站连接。		17.0.0.0/8 的 APNs 主机)
8081	用于来自可选 MDM 远程支持客户端的应用程序通道。默认设置为 8081。	远程支持客户端	Internet，针对用户设备的应用程序通道（仅适用于 Android 和 Windows)
8443	用于 iOS 和 Windows Phone 设备注册。	Internet LAN 和 WiFi	XenMobile

此端口配置可确保从 Secure Hub for Android 连接的 Android 设备能够从内部网络访问 Citrix 自动发现服务 (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 连接可能不支持您的代理服务器。在这种情况下，允许 ADS 连接跳过代理服务器。

如果您希望启用证书固定，应满足以下必备条件：

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

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

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

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

204.236.239.233

107.20.198.193

可扩展性和性能

Jun 26, 2017

注意

有关最新的 XenMobile 可扩展性和性能指南，请参阅[可扩展性和性能](#)。

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

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

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

本文中的数据源自对规模范围从 10,000 个设备到 60,000 个设备的部署的测试。测试中的移动设备使用已知工作负载。

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

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

此表汇总了可扩展性测试结果：

可扩展性	多达 60000 台设备	
登录速率	现有用户的重新连接速率	每小时最多 7500 台设备
配置	NetScaler	MPX 8200
	XenMobile Enterprise Edition	XenMobile Server 5 节点群集
	数据库	Microsoft SQL Server 外部数据库

测试结果（按设备数量和硬件配置）

此表提供了与测试的部署设备数量和硬件配置对应的可扩展性测试结果。

设备数量	10,000	30,000	60,000

每小时现有设备的重新连接速率	1250	3,750	7,500
XenMobile Server - 模式	独立	群集	群集
XenMobile Server - 群集	不适用	3	5
XenMobile Server - 虚拟设备	内存 = 8 GB RAM vCPU = 4	内存 = 16 GB RAM vCPU = 8	内存 = 24 GB RAM vCPU = 8
Active Directory	内存 = 4 GB RAM vCPU = 2	内存 = 8 GB RAM vCPU = 4	内存 = 16 GB RAM vCPU = 4
Microsoft SQL Server 外部数据库	内存 = 8 GB RAM vCPU = 4	内存 = 16 GB RAM vCPU = 8	内存 = 48 GB RAM vCPU = 24

可扩展性配置文件

这些表格汇总了得出本文数据所用的测试配置文件：

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

XenMobile Server 配置	总数	每个用户
策略	20	20
应用程序	270	50
公共应用程序	200	0
MDX	50	30

Web 和 SaaS 应用程序	20	20
操作	50	
交付组	20	
每个交付组的 Active Directory 组数	10	

SQL	
数据库数	1

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

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

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

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

在 8 小时的测试时间间隔内，发生了以下应用程序相关活动：

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

参考体系结构

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

附加说明和限制

考虑本文中的可扩展性测试结果时请注意以下内容：

- 未测试 Windows 平台。
- 针对 iOS 和 Android 设备测试了策略推送功能。
- 每个 XenMobile Server 节点最多同时支持 10,000 台设备。

许可

Apr 13, 2017

XenMobile Service 和 XenMobile 服务器的许可不同：

- Citrix Cloud Ops 处理 XenMobile Service 的许可。
- XenMobile 服务器和 NetScaler Gateway 需要许可证。

有关 NetScaler Gateway 许可的详细信息，请参阅 NetScaler Gateway 文档中的[许可](#)。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 服务器时，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)。

有关显示每个 XenMobile 版本中可用的 XenMobile 功能的数据表，请参阅此 [PDF](#)。

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 最新版本要求使用 Citrix 许可证服务器 11.12.1 或更高版本。早期许可证服务器版本与 XenMobile 最新版本不兼容。

Important

如果打算将 XenMobile 的节点或实例群集在一起，必须在远程服务器上使用 Citrix Licensing。

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

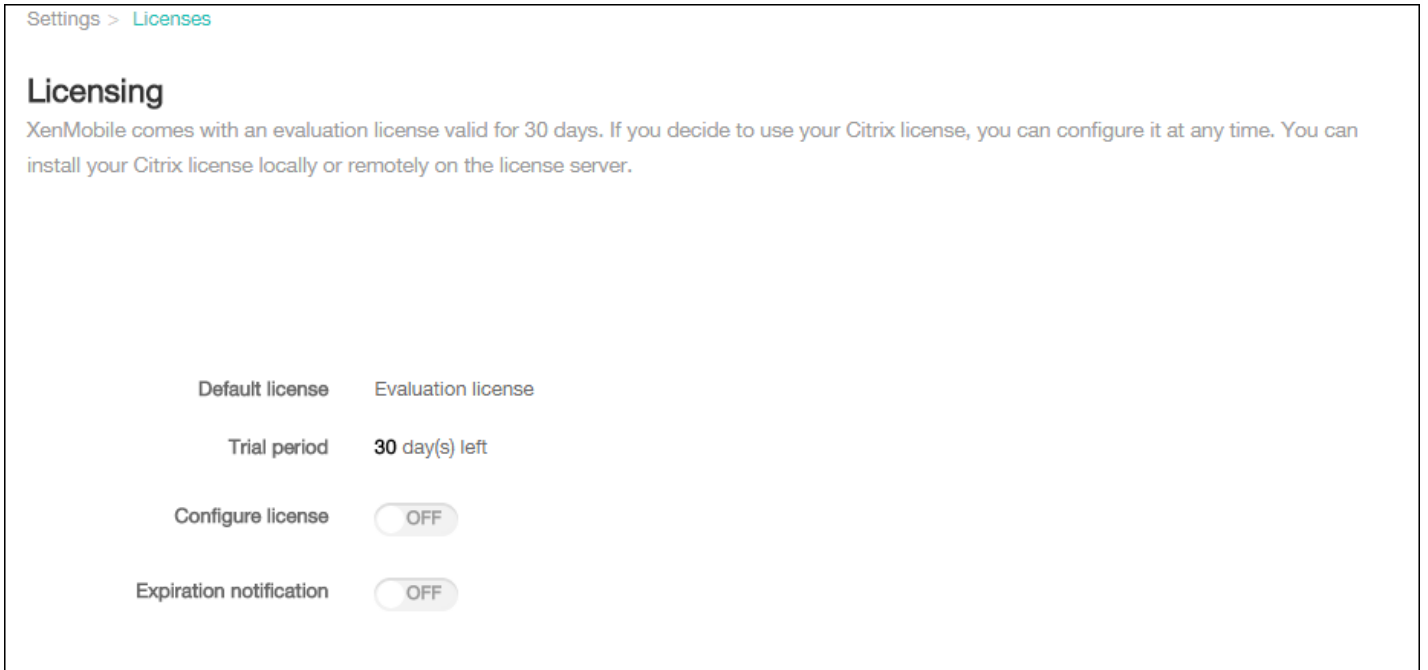
在不提供许可证的情况下，XenMobile 将在宽限期为 30 天的试用模式下运行，功能齐全。此试用模式只能使用一次，期限为从安装 XenMobile 开始持续 30 天。无论是否有可用的有效 XenMobile 许可证，均不会阻止对 XenMobile Web 控制台的访问。在 XenMobile 控制台中，您可以看到试用期剩余的天数。

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

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

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

可证。

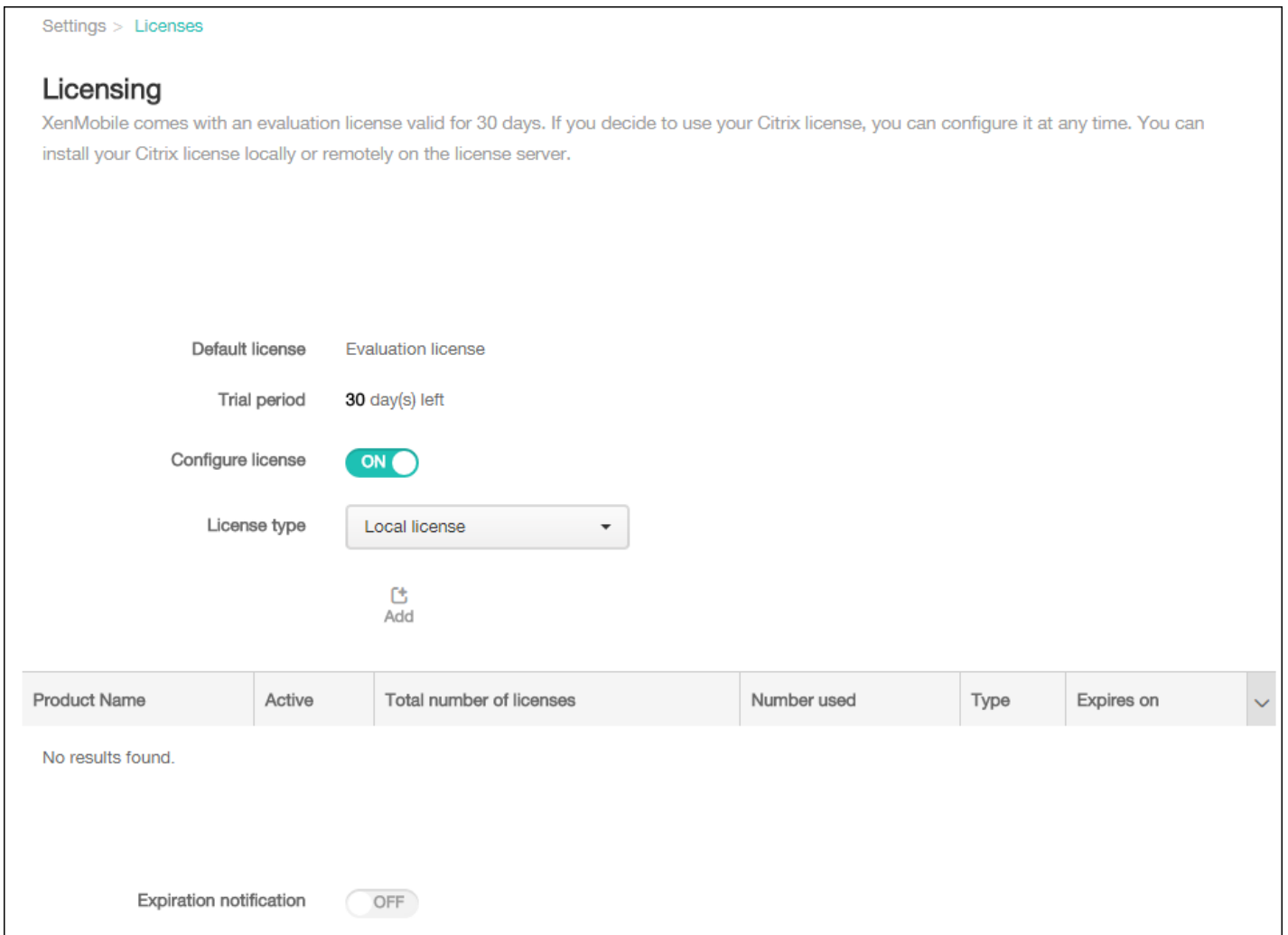


1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击许可。此时将显示许可页面。

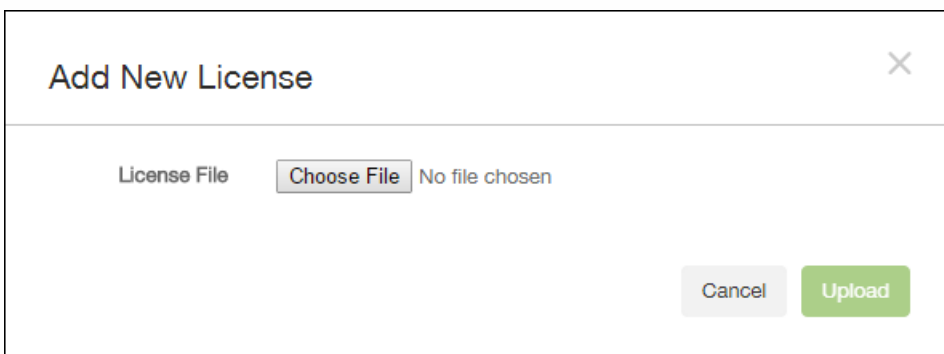
添加新许可证时，新许可证将显示在表格中。添加的第一个许可证自动被激活。如果添加同一类别（如企业）和类型的多个许可证，这些许可证将显示在表格的同一行中。在这些情况下，许可证总数和使用的数量反应公共许可证的总数。过期日期显示公共许可证中的最新过期日期。

通过 XenMobile 控制台管理所有本地许可证。

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



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



6. 在添加新许可证对话框中，单击选择文件，然后浏览到许可证文件的位置。

7. 单击上载。许可证将上载到本地并显示在表格中。

License type: Local license

Add | Delete All

Product Name	Active	Total number of licenses	Number used	Type	Expires on
Citrix XenMobile Enterprise Edition Device	✓	15002	0	Retail	01-DEC-2015

Showing 1 - 1 of 1 items

Expiration notification: OFF

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

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

1. 在许可页面上，将配置许可证设为开。在许可证类型列表中，单击添加按钮，将显示许可表。许可表包含已用于 XenMobile 的许可证。如果尚未添加任何 Citrix 许可证，此表为空。

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

License type: Remote license

License server*:

Port*: 27000

Test Connection

Product name	Active	Total number of licenses	Number used	Type	Expires on
		1001	0	Retail	01-DEC-2015

4. 配置以下设置：

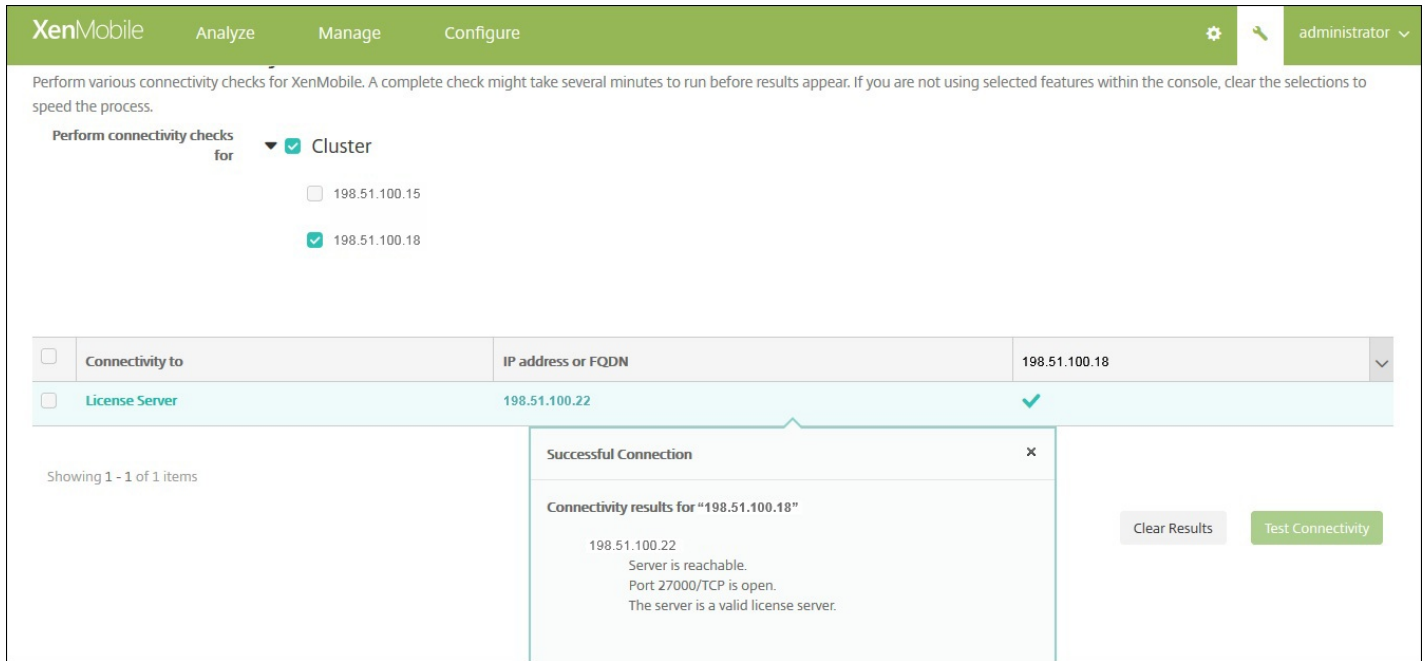
- 许可证服务器：键入远程许可服务器的 IP 地址或完全限定的域名 (FQDN)。
- 端口：接受默认端口或键入用于与许可服务器通信的端口号。

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

单击测试连接后，XenMobile 会确认以下信息：

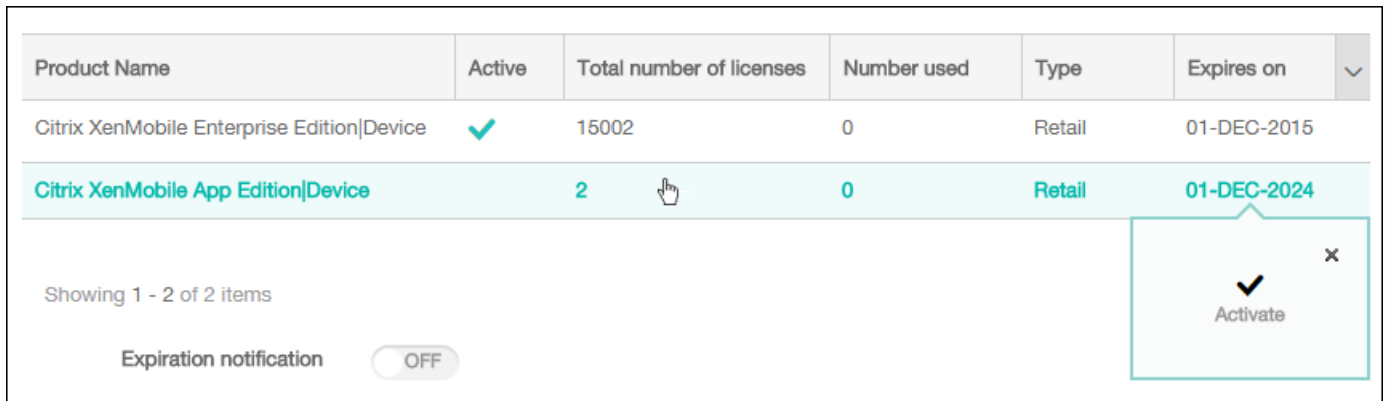
- XenMobile 可以与许可证服务器通信。
- 许可证服务器上的许可证有效。
- 许可证服务器与 XenMobile 兼容。

如果连接不成功，请检查显示的错误消息，进行必要的修改，然后单击测试连接。



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

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



2. 单击激活。此时将显示激活对话框。

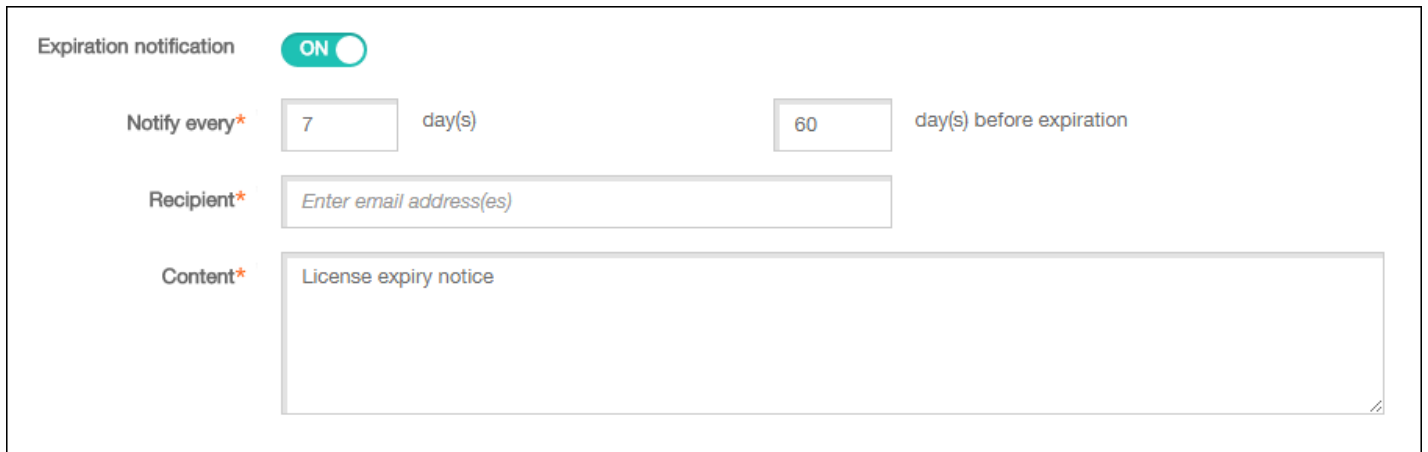
3. 单击激活。所选许可证现已激活。

Important

如果激活所选许可证，当前激活的许可证将取消激活。

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

1. 在许可页面上，将到期通知设为开。将显示新的与通知相关的字段。



The screenshot shows a configuration panel for 'Expiration notification'. At the top, there is a toggle switch labeled 'ON'. Below this, there are three main sections: 'Notify every*', 'Recipient*', and 'Content*'. The 'Notify every*' section has two input fields: the first contains the number '7' followed by the text 'day(s)', and the second contains the number '60' followed by the text 'day(s) before expiration'. The 'Recipient*' section has a text input field with the placeholder text 'Enter email address(es)'. The 'Content*' section has a larger text area containing the text 'License expiry notice'.

2. 配置以下设置：

- **通知时间间隔：**键入：
 - 发送通知的频率，如每 7 天一次。
 - 开始发送通知的时间，如在许可证过期前 60 天发送。
- **收件人：**键入您的电子邮件地址或许可证负责人的电子邮件地址。
- **内容：**键入收件人在通知中看到的过期通知消息。

3. 单击**保存**。根据您的设置，XenMobile 开始向您**在收件人中键入的收件人**发送电子邮件，其中包含您在**内容中键入的文本**。通知按照您设置的频率发送。

FIPS 140-2 合规性

Feb 27, 2017

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： 仅对 XenMobile 服务器内部部署安装提供 FIPS 支持。只可以在初始安装时启用 XenMobile FIPS 模式。

注意： 只要未使用任何 HDX 应用程序，XenMobile 仅移动设备管理、XenMobile 仅移动应用程序管理和 XenMobile Enterprise 均与 FIPS 兼容。

在 iOS 上执行的所有静态数据 (data-at-rest) 和传输中数据 (data-in-transit) 加密操作使用 OpenSSL 和 Apple 提供的 FIPS 认证加密模块。在 Android 上，从移动设备到 NetScaler Gateway 的所有静态数据加密操作和所有传输中数据加密操作使用 OpenSSL 提供的 FIPS 认证加密模块。

受支持的 Windows 设备上 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 上受支持，在 Windows Phone 上使用 FIPS 兼容的加密库和 API。Windows Phone 上 MDX 应用程序的所有静态数据和 Windows Phone 设备与 NetScaler Gateway 之间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。

语言支持

Apr 05, 2017

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

本文列出了 XenMobile 最新版本支持的语言。

- 法语
- 德语
- 日语
- 韩语
- 葡萄牙语
- 简体中文

X 表示应用程序可在该特定语言中使用。Secure Forms 应用程序目前仅提供英语版本。

注意：自发布版本 10.4 起，Worx 移动应用程序已重命名为 XenMobile 应用程序。大多数单个 XenMobile 应用程序也进行了重命名。有关详细信息，请参阅[关于 XenMobile 应用程序](#)。

iOS 和 Android

	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
日语	X	X	X	X	X	X
简体中文	X	X	X	X	X	X
繁体中文	X	X	X	X	X	X
法语	X	X	X	X	X	X
德语	X	X	X	X	X	X
西班牙语	X	X	X	X	X	X
韩语	X	X	X	X	X	X

葡萄牙语	X	X	X	X	X	X
荷兰语	X	X	X	X	X	X
意大利语	X	X	X	X	X	X
丹麦语	X	X	X	X	X	X
瑞典语	X	X	X	X	X	X
希伯来语	X	X	X	X	X	仅限 iOS
阿拉伯语	X	X	X	X	X	X
俄语	X	X	X	X	X	X
土耳其语	X	X	仅限 Android			

Windows

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

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

	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
Secure Tasks	X	X
Secure Notes	X	X
QuickEdit	X	X

安装和配置

Feb 27, 2017

开始之前：

可以使用以下预安装核对表记录安装 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。

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](#)。

有关安装步骤，请参阅本文后面的[安装 XenMobile](#) 一节。

预安装核对表

基本网络连接


以下是 XenMobile 解决方案需要的网络设置。

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

<p>识别并记下 NetScaler Gateway 主机名。</p> <p>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。</p>	NetScaler Gateway	
<p>记录 XenMobile 的 IP 地址。</p> <p>如果安装一个 XenMobile 实例，请保留一个 IP 地址。</p> <p>配置群集时，请记录需要的所有 IP 地址。</p>	XenMobile	
<ul style="list-style-type: none"> • 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	
<p>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）。</p> <p>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)。</p>	XenMobile NetScaler Gateway	
<p>记录默认网关 IP 地址。</p>	XenMobile NetScaler Gateway	
<p>记录系统 IP (NSIP) 地址和子网掩码。</p>	NetScaler Gateway	
<p>记录子系统 IP (SNIP) 地址和子网掩码。</p>	NetScaler Gateway	
<p>记录证书中的 NetScaler Gateway 虚拟服务器 IP 地址和 FQDN。</p> <p>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。</p>	NetScaler Gateway	
<p>记录用户可经由 NetScaler Gateway 访问的内部网络。</p> <p>例如：10.10.0.0/24</p> <p>输入用户通过 Secure Hub 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）。</p>	NetScaler Gateway	
<p>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。</p>	XenMobile NetScaler Gateway	

许可

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)。

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


证书

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

	必备条件	组件	注意
	获取并安装必需证书。	XenMobile NetScaler Gateway	

端口

您需要打开端口，以允许与 XenMobile 组件进行通信。

	必备条件	组件	注意
	打开用于 XenMobile 的端口	XenMobile NetScaler Gateway	

数据库

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

	必备条件	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	XenMobile	

DBcreator 角色权限。		
-----------------	--	--

Active Directory 设置

•	必备条件	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	

XenMobile 与 NetScaler Gateway 之间的连接

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

用户连接：访问 XenDesktop、XenApp 和 Citrix Secure Hub

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 Secure Hub 之间的连接设置。创建第二个虚拟服务器，使用户能够从 Citrix 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。

✓	必备条件	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 Secure Hub 的公共 FQDN。	NetScaler Gateway	

安装 XenMobile

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

注意

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

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

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

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

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

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

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

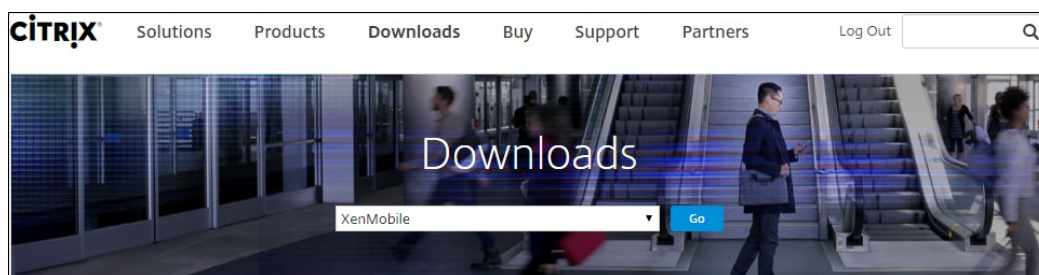
Windows Server 2012 R2 不要求执行这些额外步骤。

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

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

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，展开您所使用的 NetScaler Gateway 版本。
7. 在固件下面，单击要下载的设备软件版本。
注意：还可以单击 Virtual Appliances（虚拟设备）以下载 NetScaler VPX。选择此选项时，将显示适用于每个虚拟机管理程序所对应的虚拟机的软件列表。
8. 单击要下载的设备软件版本。
9. 在要下载版本的设备软件页面上，单击相应虚拟设备的下载。
10. 按照屏幕上的说明下载软件。

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。

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。

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

在命令提示窗口中配置 XenMobile

1. 将 XenMobile 虚拟机导入 Citrix XenServer、Microsoft Hyper-V 或 VMware ESXi。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 !、#、\$、%)

```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through the initial configuration of XenMobile. Accept options offered by pressing Enter/Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the command prompt.
Username: admin
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。

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

```
Network settings:
IP address: 192.0.2.0
Netmask: 225.225.225.128
Default gateway: 203.0.113.3
Primary DNS server: 192.0.2.4
Secondary DNS server [optional]: 192.0.2.5
Commit settings [y/n]: y█
```

注意：本图片和后面的图片中显示的地址并不可用，仅作为示例提供。

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

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

- 6. （可选）启用美国联邦信息处理标准 (FIPS)。有关 FIPS 的详细信息，请参阅 [FIPS](#)。此外，请务必完成一组必备条件，如[配置 FIPS](#) 中所述。

```
Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]: █
```

- 7. 提供以下信息以配置数据库连接。

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

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

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

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

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

12. 由于您是首次安装 XenMobile，请跳过下一个关于从之前的 XenMobile 版本进行升级的问题。
13. 如果要为每个公钥基础设施 (PKI) 证书使用相同的密码，请键入 y。有关 XenMobile PKI 功能的详细信息，请参阅[上传证书](#)。

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

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile console 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** 键提交设置。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 ]

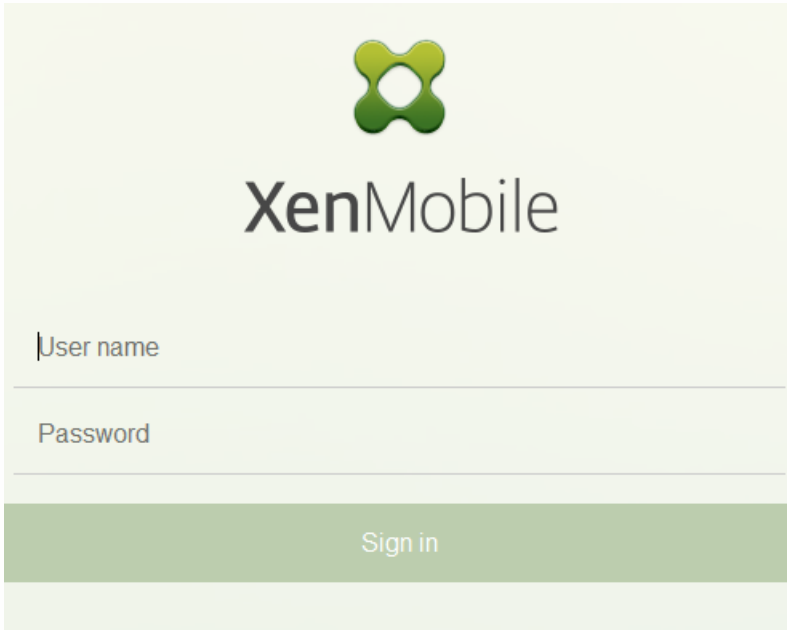
To access the console, from a web browser, go to the following location and
log on with your console credentials:
https://203.0.113.8:4443/

Starting monitoring... [ OK ]
```

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

1. 在 Web 浏览器中，导航到命令提示窗口配置的结论部分提供的位置。

2. 键入在命令提示窗口中创建的 XenMobile 控制台管理员帐户的用户名和密码。

The image shows the XenMobile login interface. At the top center is the XenMobile logo, a green four-lobed shape. Below the logo is the text "XenMobile" in a large, dark font. Underneath, there are two input fields: "User name" and "Password", each with a horizontal line below it. At the bottom of the form is a green button with the text "Sign in" in white.

3. 在“入门”页面中，单击开始。此时将显示“许可”页面。

4. 配置许可证。如果未上载许可证，则使用有效期为 30 天的评估版许可证。有关添加和配置许可证以及配置过期通知的详细信息，请参阅[许可](#)。

重要：如果打算通过添加 XenMobile 的群集节点或实例来使用 XenMobile 群集，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。如果管理 iOS 设备，需要 APNs 证书。有关使用证书的详细信息，请参阅[证书](#)。

注意：此步骤需要重新启动服务器。

7. 如果适用于环境，请配置 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[通知](#)。

后续条件：重新启动 XenMobile 服务器以激活您的证书。

在 XenMobile 中配置 FIPS

Feb 27, 2017

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 命令行接口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. 在初始设置过程中，启用 **FIPS mode**（FIPS 模式）。
2. 上载 SQL Server 的根 CA 证书。如果在 SQL Server 上使用了自签名 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 [将证书上载到 XenMobile](#)。
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，但您使用的登录凭据必须具有 DBcreator 角色。

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

要确认 FIPS 模式是否已成功配置，请登录 XenMobile 命令行接口。登录横幅中将显示阶段 **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**下方，单击**添加**。
 - h. 输入在之前的步骤中复制的 SQL 服务帐户名称。
 - i. 取消选中**允许完全控制**选项。默认情况下，该服务帐户将被同时授予完全控制和读取权限，但只需要能够读取私钥。
 - j. 关闭 **MMC** 并启动 SQL 服务。
3. 确保 SQL 服务已正确启动。

Internet Information Services (IIS) 必备条件

1. 下载 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 Internet 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. 完成安装后，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 [Web 服务器 \(IIS\)](#)。

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 (domain\username)。
- 密码 : 服务帐户的密码。
- 数据库名称 : 这是您选择的名称。

配置群集

Feb 27, 2017

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均衡虚拟 IP 地址。

- **移动设备管理 (MDM) 负载均衡虚拟 IP 地址**：与群集中配置的 XenMobile 节点进行通信需要使用 MDM 负载均衡虚拟 IP 地址。此负载均衡在 SSL 桥接模式下完成。
- **移动应用程序管理 (MAM) 负载均衡虚拟 IP 地址**：NetScaler Gateway 与群集中配置的 XenMobile 节点进行通信需要使用 MAM 负载均衡虚拟 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 上路由到负载均衡虚拟 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 负载均衡器的公用 IP 地址和一个用于 MAM 的专用 IP 地址。
- 服务器证书。
- 一个用作 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](#)。

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。



```
*****
          Citrix XenMobile
          (in First Time Use mode)
*****

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password:
Re-enter new password: _
```

2. 提供网络配置详细信息，如下图所示。

```

Network settings:
IP address []: 10.147.75.51
Netmask []: 255.255.255.0
Default gateway []: 10.147.75.1
Primary DNS server []: 10.147.75.240
Secondary DNS server (optional) []:

Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps

```

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

```

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

```

4. 如果要使用 FIPS，请键入 y；否则，请键入 n。

```

Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]:

```

5. 配置数据库，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）。

```

Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:

Server []: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service1]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
to enable realtime communication between cluster members please open port 88 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

```

6. 输入与为第一个 VM 提供的证书相同的密码。

```
Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:

Server [l]: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
```

输入密码后，第二个节点上的初始配置将完成。

```
Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
y
New password:
Re-enter new password:
Saving server and client certs password...

Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
this may take a few seconds..... [ OK ]
application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
this may take a few minutes....._
```

7. 配置完成后，服务器重新启动并显示登录对话框。

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

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
  this may take a few seconds..... [ OK ]
  application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
  this may take a few minutes.....^ [ .....
.....
  application started [ OK ]

To access the console, from a web browser, go to the following location and
log on with your console credentials:
https://10.147.75.59:4443/

Starting monitoring... [ OK ]

xms51.wg.lab login: |
```

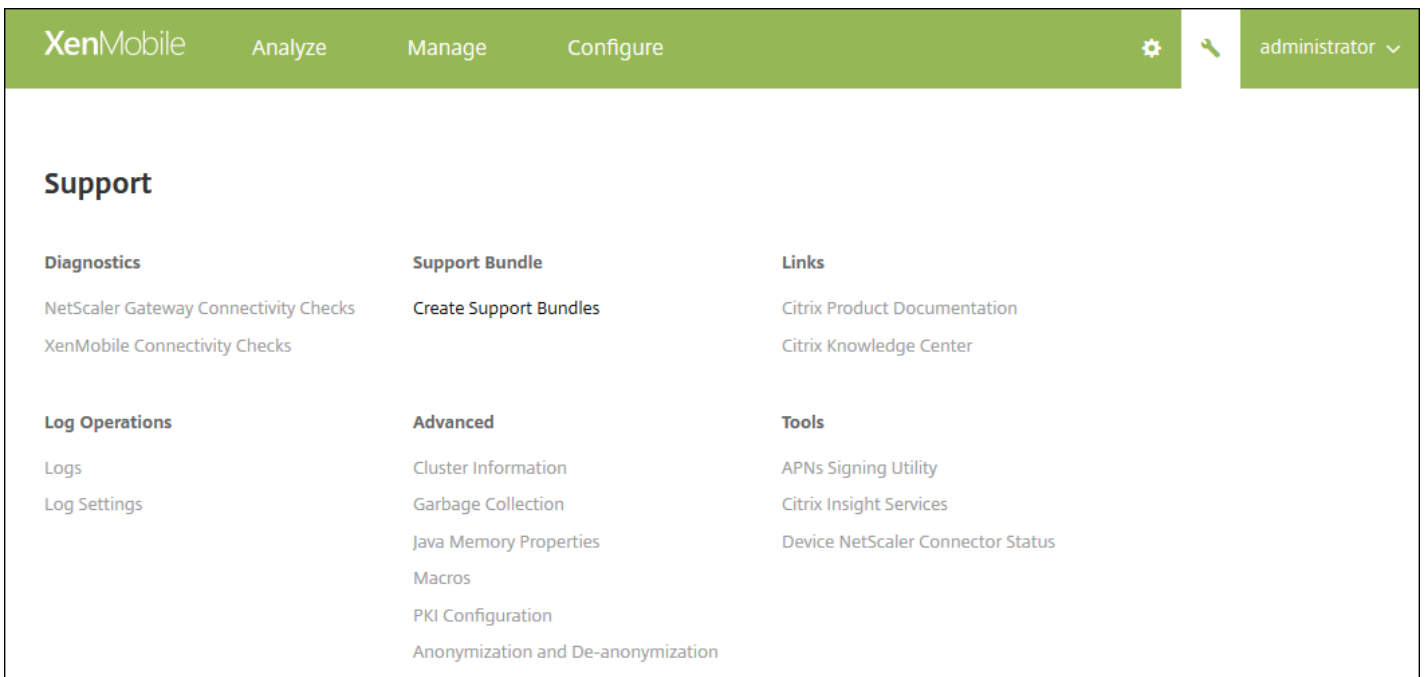
注意：登录对话框与第一个 VM 的登录对话框相同。这种相同是供您确认两个 VM 使用相同的数据库服务器的一种途径。

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



此时将打开支持页面。

- 10. 在高级下，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。

Node ID	Node name	Status	Role	First check-in	Next check-in
17742s211		ACTIVE	null	2015-04-22 14:40:34.877	2015-04-22 01:02:06.293
17742s203		ACTIVE	OLDEST	2015-04-22 14:30:08.47	2015-04-22 02:09:02.61

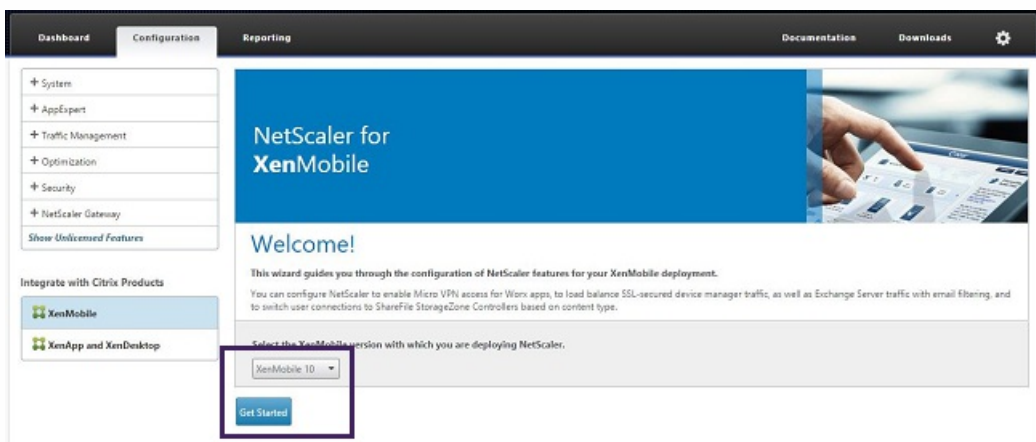
您可以按照相同的步骤添加其他节点。添加到节点的第一个群集的角色为最早。在其后添加的群集的角色将为无或空。

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。

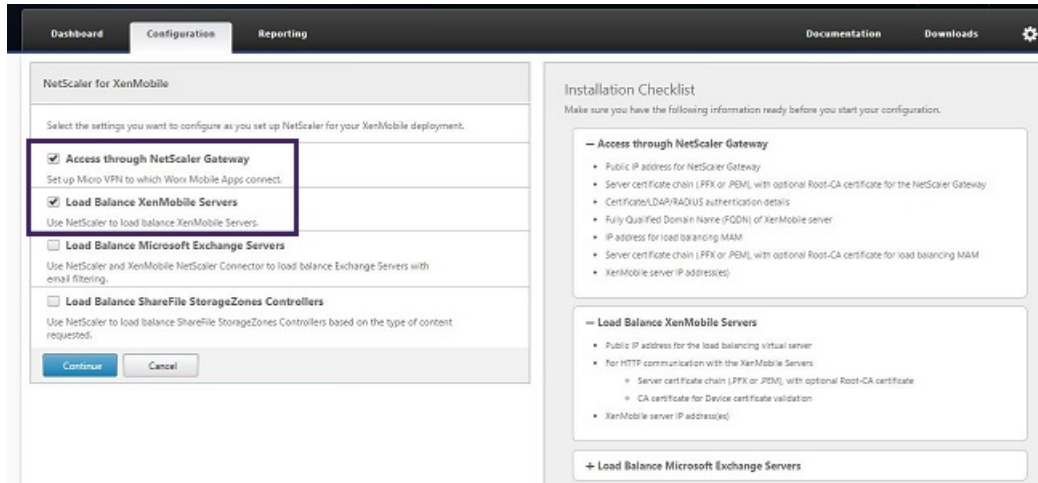


2. 在配置选项卡上，单击 XenMobile，然后单击开始。

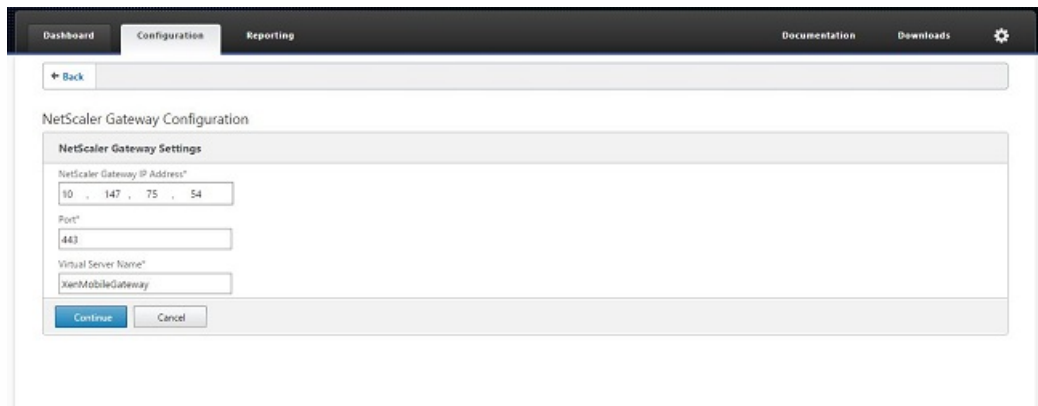


3. 选中 Access through NetScaler Gateway（通过 NetScaler Gateway 访问）复选框和 Load Balance XenMobile

Servers (XenMobile 服务器负载均衡) 复选框，然后单击 Continue (继续)。

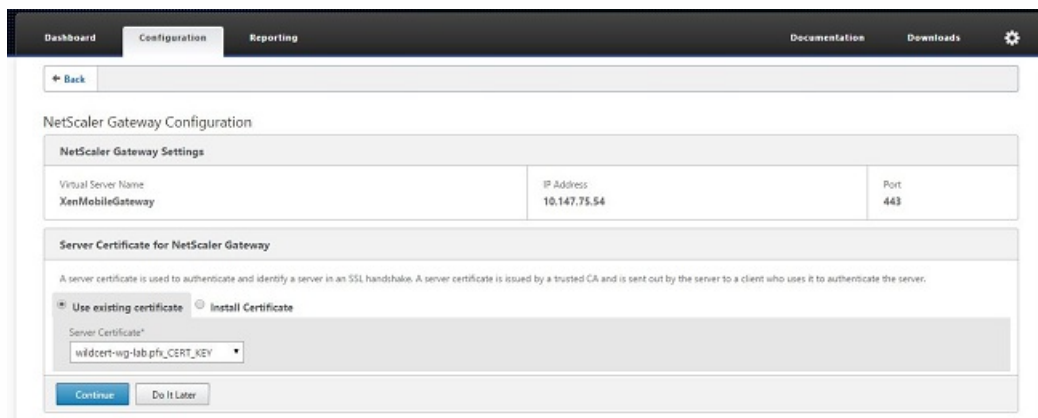


4. 输入 NetScaler Gateway 的 IP 地址，然后单击 Continue (继续)。



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)。

Authentication Settings

Select a primary authentication method for client connections. Primary authentication can be configured to use Active Directory/LDAP, RADIUS, or client certificate methods. For two-factor authentication, configure a secondary method from either RADIUS or Active Directory/LDAP methods.

Primary authentication method*
Active Directory/LDAP

IP Address*
10 . 147 . 75 . 240 IPv6

Port*
389

Base DN*
dc=wg,dc=lab

Service account*
administrator@wg.lab

Password*

Confirm Password*

Time out (seconds)*
3

Server Logon Name Attribute*
userPrincipalName

Secondary authentication method*
None

Continue Cancel

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。

- 在 XenMobile settings（XenMobile 设置）中，输入 Load Balancing FQDN for MAM（MAM 的负载均衡 FQDN），然后单击 Continue（继续）。

XenMobile Settings

Load Balancing FQDN for MAM*
xms51.wg.lab

Load Balancing IP address for MAM*
10 . 147 . 75 . 55

Port*
8443

SSL Traffic Configuration*
 HTTPS communication to XenMobile Server HTTP communication to XenMobile Server

Split DNS mode for Micro VPN*
BOTH

Enable split tunneling

Continue Cancel

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

- 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)。
- 绑定 MAM 负载均衡虚拟 IP 地址的服务器证书，然后单击 Continue（继续）。

XenMobile Settings

Load Balancing FQDN for MAM: xms51.wg.lab
Load Balancing IP address for MAM: 10.147.75.55
Port: 8443

SSL Traffic Configuration: HTTPS communication to XMS Server
Split Tunnel: OFF
Split DNS: BOTH

Server Certificate for MAM Load Balancing

A server certificate is used to authenticate and identify a server in an SSL handshake. A server certificate is issued by a trusted CA and is sent out by the server to a client who uses it to authenticate the server.

Use existing certificate Install Certificate

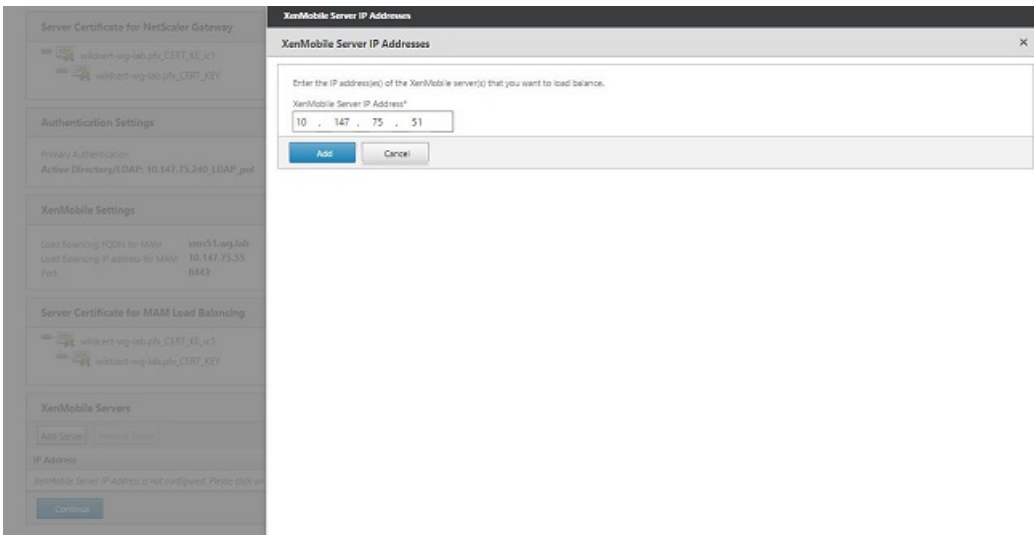
Server Certificate*
wildcert-wg-lab.pfx_CERT_KEY

Continue Do It Later

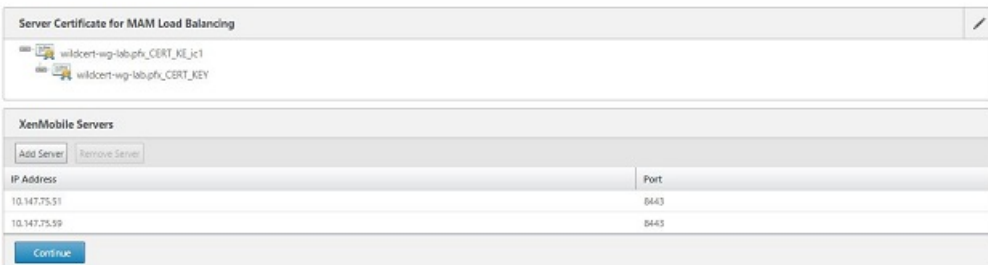
- 在 XenMobile Servers（XenMobile 服务器）下面，单击 Add Server（添加服务器）以添加 XenMobile 节点。



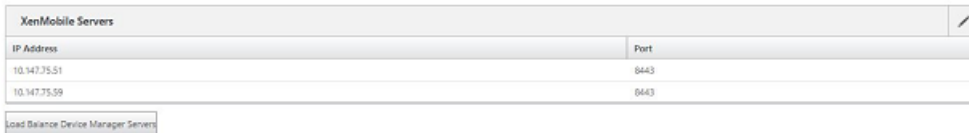
11. 输入 XenMobile 节点的 IP 地址，然后单击 Add（添加）。



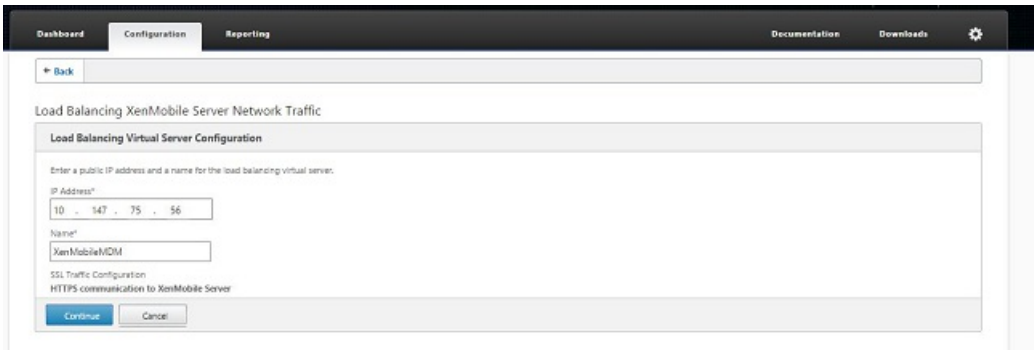
12. 重复步骤 10 和 11 以添加其他 XenMobile 节点，作为 XenMobile 群集的一部分。您将看到已添加的所有 XenMobile 节点。单击继续。



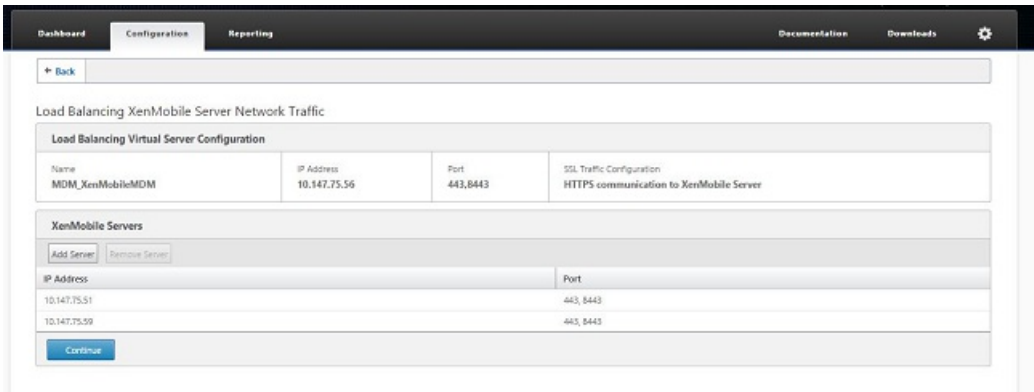
13. 单击 Load Balance Device Manager Servers（Device Manager 服务器负载均衡）以继续执行 MDM 负载均衡配置。



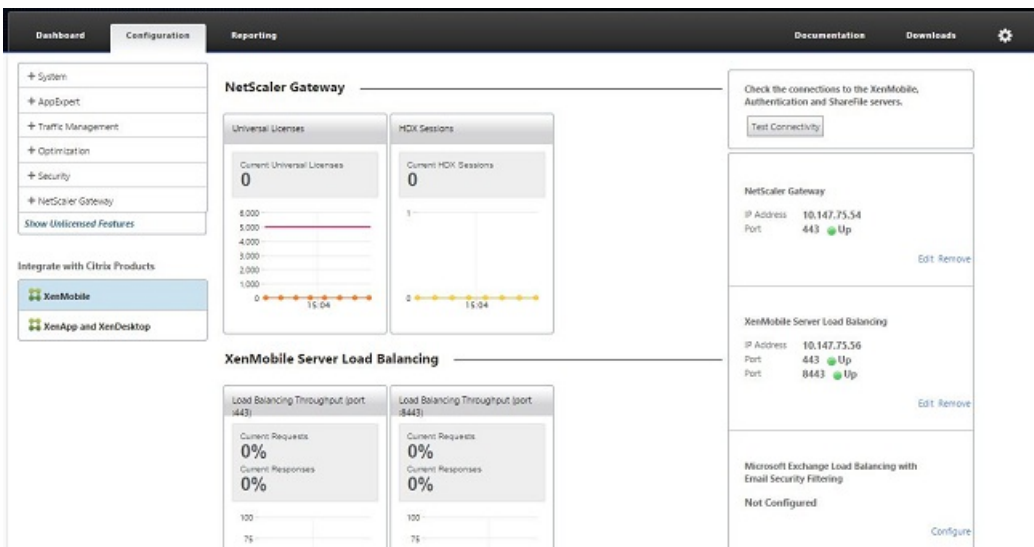
14. 输入要用作 MDM 负载均衡 IP 地址的 IP 地址，然后单击 Continue（继续）。



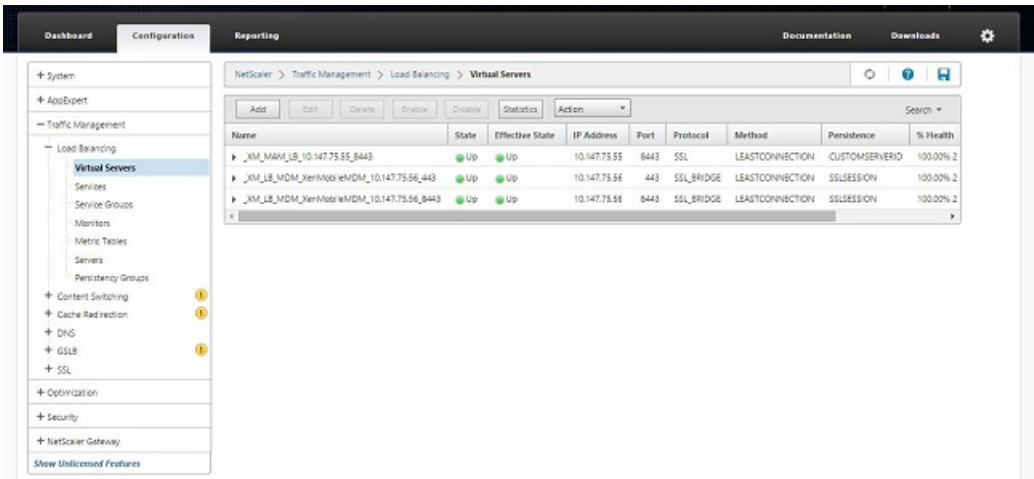
15. 列表中显示 XenMobile 节点后，单击 Continue（继续），然后单击 Done（完成）以完成此过程。



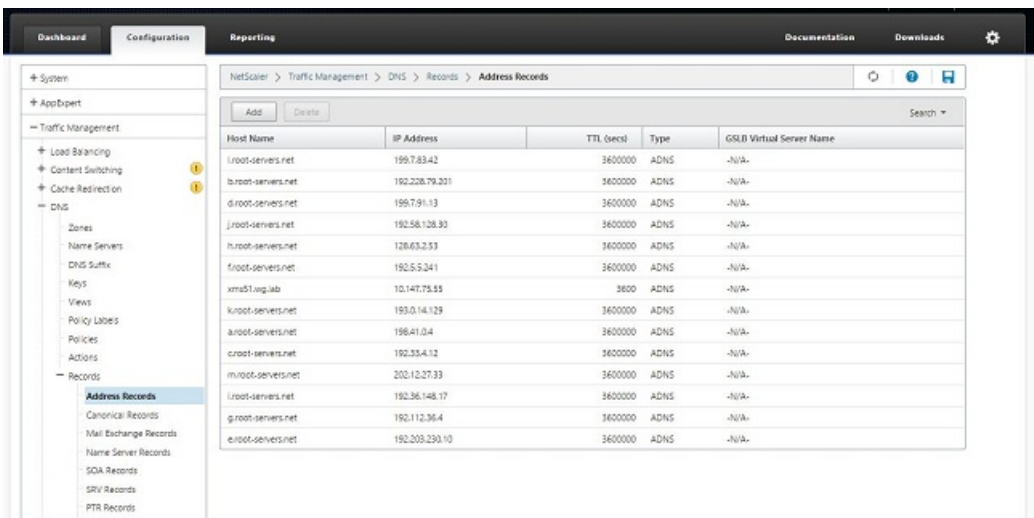
您将在 XenMobile 页面上看到虚拟 IP 地址状态。



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。



灾难恢复指南

Feb 27, 2017

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

启用代理服务器

Feb 27, 2017

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。

```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
Choice: [0 - 5] 2
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] Admin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----
```

3. 在“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。

```
Choice: [0 - 10] 6
-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
```

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

代理类型	支持的目标
SOCKS	APNS

HTTP	APNS、Web、PKI
HTTPS	Web、PKI
HTTP 并进行身份验证	Web、PKI
HTTPS 并进行身份验证	Web、PKI

```

-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 1

Enter socks proxy information
Address [1]: 203.0.113.23
Port[]: 1080
Target - APNS
Proxy configuration updated successfully.
Please restart all nodes in the cluster for the changes to take effect
Are you sure to restart the system? [y/n]: █

```

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。

```

[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 2

Enter https proxy information
Address [1]: 203.0.113.23
Port[]: 4443
Configure username & password [y/n]: y
Username: Justaname
Password:
Target - WEB
WEB proxy configured. Override proxy settings?[y/n]: █

```

6. 键入 y 将完成代理服务器设置。

服务器属性

Jun 06, 2017

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

一些属性是自定义键。要添加自定义键，请单击添加，然后从键中选择自定义键。

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

服务器属性定义

始终添加设备

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

AG 客户端证书颁发限制时间间隔

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

Audit Log Cleanup Execution Time (审核日志清理执行时间)

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

Audit Log Cleanup Interval (in Days) (审核日志清理时间间隔(天))

XenMobile 服务器保留审核日志的天数。默认值为 1。

Audit Logger (审核记录器)

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

Audit Log Retention (in Days) (审核日志保留时间(天))

XenMobile 服务器保留审核日志的天数。默认值为 7。

`auth.ldap.connect.timeout`

`auth.ldap.read.timeout`

为了补偿 LDAP 响应慢的情况，Citrix 建议为以下自定义键添加服务器属性。

键：自定义键

键：`auth.ldap.connect.timeout`

值：`60000`

显示名称：`auth.ldap.connect.timeout=60000`

说明：LDAP 连接超时

键：自定义键

键 : `auth.ldap.read.timeout`
值 : `60000`
显示名称 : `auth.ldap.read.timeout=60000`
说明 : LDAP 读取超时

证书续订(秒)。

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

连接超时

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

与 Microsoft 证书服务器连接超时

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

默认部署渠道

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

Deploy Log Cleanup (in Days) (部署日志清理(天))

XenMobile 服务器保留部署日志的天数。默认值为 7。

Disable SSL Server Verification (禁用 SSL 服务器验证)

如果为 `True`，则在满足所有以下条件时禁用 SSL 服务器证书验证：

- 在 XenMobile 服务器上启用了基于证书的身份验证
- Microsoft CA 服务器是证书颁发者
- 其根 XenMobile 服务器不信任的内部 CA 已为您的证书签名。

默认值为 `true`。

启用控制台

如果设置为 `true`，则允许用户访问自助服务门户控制台。默认设置为 `true`。

启用/禁用用于诊断的 Hibernate 统计日志

如果设为 `True`，则会启用 Hibernate 统计信息日志记录，以协助排除应用程序性能问题。Hibernate 是用于与 Microsoft SQL Server 建立 XenMobile 连接的组件。默认情况下，此日志记录功能已禁用，因为它会影响应用程序的性能。只应在短时间内启用日志记录功能，以避免生成巨大的日志文件。XenMobile 将此日志写入 `/opt/sas/logs/hibernate_stats.log`。默认设置为 `False`。

启用通知触发器

启用或禁用 Secure Hub 客户端通知. 值 `true` 启用通知。默认设置为 `true`。

ActiveSync 完全下拉允许和拒绝的用户

XenMobile 在执行 PowerShell 命令以获取 ActiveSync 设备基线时等待来自域的响应的秒数。默认值为 **28800** 秒。

hibernate.c3p0.max_size

此自定义键确定 XenMobile 可以打开的与 SQL Server 数据库的最大连接数。XenMobile 使用您为此自定义键指定的值作为上限。仅当需要连接时才会打开连接。设置基于数据库服务器的容量。有关详细信息，请参阅[调整 XenMobile 操作](#)。按如下所示配置建。默认值为 **1000**。

键：`hibernate.c3p0.max_size`

值：`500`

显示名称：`hibernate.c3p0.max_size=nnn`

说明：DB 与 SQL 的连接数

hibernate.c3p0.timeout

此自定义键确定空闲超时。默认值为 **300**。

键：自定义键

键：`hibernate.c3p0.timeout`

值：`30`

显示名称：`hibernate.c3p0.timeout=30`

说明：数据库空闲超时

确定是否已启用遥测

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

Inactivity Timeout in Minutes (不活动超时(分钟))

如果 `WebServices timeout type`（Web 服务超时类型）服务器属性为 `INACTIVITY_TIMEOUT`：此属性定义分钟数，超过此时间后，XenMobile 注销执行了以下操作的不活动管理员：

- 使用了 XenMobile Public API for REST 服务来访问 XenMobile 控制台
- 使用了 XenMobile Public API for REST 服务来访问任何第三方应用程序。超时为 **0** 意味着不活动用户保持登录状态。

默认值为 **5**。

已启用 iOS 设备管理注册自动安装

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

iOS 设备管理注册第一个步骤延迟

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

iOS 设备管理注册最后一个步骤延迟

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

iOS 设备管理身份交付模式

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

iOS 设备管理身份密钥大小

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

iOS 设备管理身份续订天数

指定 XenMobile 在证书过期之前开始续订证书的天数。例如：如果证书将于 10 天后过期，并且此属性设置为 10 天，当设备在过期之前 9 天连接时，XenMobile 会颁发新证书。默认值为 30 天。

iOS MDM APNS 私钥密码

此属性包含 APNs 密码，XenMobile 向 Apple 服务器推送通知需要该密码。

iOS MDM APNS 私钥密码

此属性包含 APNs 密码，XenMobile 向 Apple 服务器推送通知需要该密码。

设备断开连接之前不活动的时长

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

仅 MAM 设备最大值

此自定义键限制每个用户可以注册的仅 MAM 设备数。按如下所示配置键。值为 0 表示设备注册数不受限制。

键 = `number.of.mam.devices.per.user`

值 = 5

显示名称 = 仅 MAM 设备最大值

说明 = 限制每个用户可以注册的 MAM 设备数。

NetScaler 单点登录

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

连续失败的上载次数

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

每个设备的用户数

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

提取允许和被拒绝的用户的增量更改

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

从 Microsoft 证书服务器读取超时

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

REST Web 服务

启用 REST Web 服务。默认值为 true。

以指定大小的块检索设备信息

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

Session Log Cleanup (in Days) (会话日志清理(天))

XenMobile 服务器保留会话日志的天数。默认值为 7。

服务器模式

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

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

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

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

XenMobile 会在服务器日志中为以下每个活动添加服务器模式：激活某个许可证、删除某个许可证以及在“服务器属性”中更改服务器模式。有关创建和查看日志文件的详细信息，请参阅[日志](#)和[查看和分析 XenMobile 中的日志文件](#)。

ShareFile 配置类型

指定 ShareFile 存储类型。**ENTERPRISE** 表示启用 ShareFile Enterprise 模式。**CONNECTORS** 表示仅提供对通过 XenMobile 控制台创建的 StorageZone 连接器的访问权限。默认值为 **NONE** (无)，此时显示 **Configure (配置) > ShareFile** 屏幕的初始视图，在该屏幕中可以选择“ShareFile Enterprise”与“Connectors”。默认值为无。

静态超时 (分钟)

如果 **WebServices timeout type** (Web 服务超时类型) 服务器属性为 **STATIC_TIMEOUT**：此属性定义分钟数，超过此时间后，XenMobile 注销执行了操作的管理员：

- 使用了 XenMobile Public API for REST 服务来访问 XenMobile 控制台。
- 使用了 XenMobile Public API for REST 服务来访问任何第三方应用程序。

默认值为 **60**。

触发代理消息抑制

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

触发代理声音抑制

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

Unauthenticated App Download for Android Devices (面向 Android 设备的未经身份验证的应用程序下载)

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

Unauthenticated App Download for Windows Devices (面向 Windows 设备的未经身份验证的应用程序下载)

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

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

如果设置为 **true**，XenMobile Mail Manager 将使用 ActiveSync 标识符作为 **asWipeDevice** 方法的参数。默认设置为 **false**。

仅 Exchange 用户

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

VPP 基准时间间隔

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

如果您安装了许多 VPP 许可证 (例如，超过 50,000)：Citrix 建议增加基准时间间隔以降低导入许可证的频率和开销。如果您预计 Apple 会频繁更改 VPP 许可证：Citrix 建议降低该值以使更改及时更新到 XenMobile 中。两个基准之间的最小时间间隔为 60 分钟。此外，XenMobile 每隔 60 分钟执行一次增量导入，以捕获自上次导入后所做的更改。因此，如果 VPP 基准时间间隔为 60 分钟，则基准之间的时间间隔可能会最长延迟 119 分钟。

WebServices 超时类型

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

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

Windows Phone MDM 证书扩展有效性 (5y)

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

Windows WNS 通道 - 续订之前的天数

ChannelURI 的续订频率。默认值 **10** 天。

Windows WNS 检测信号时间间隔

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

XAM One-Time Ticket (XAM 一次性票证)

一次性身份验证令牌 (OTT) 对下载应用程序有效的毫秒数。此属性与属性 **Unauthenticated App download for Android** (面向 Android 的未经身份验证的应用程序下载) 和 **Unauthenticated App Download for Windows** (面向 Windows 的未经身份验证的应用程序下载) 一起使用。这些属性指定是否允许进行未经身份验证的应用程序下载。默认值为 **3600000**。

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

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

添加、编辑或删除服务器属性

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

注意

要重新启动 XenMobile，请通过虚拟机管理程序使用命令提示窗口。

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

XenMobile Analyze Manage Configure admin

Settings > Server Properties

Server Properties

You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

<input type="checkbox"/>	Display name	Key	Value	Default value	Description
<input type="checkbox"/>	NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
<input type="checkbox"/>	Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
<input type="checkbox"/>	Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata.id, url	odata.metadata, id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
<input type="checkbox"/>	Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE
<input type="checkbox"/>	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
<input type="checkbox"/>	Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
<input type="checkbox"/>	Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
<input type="checkbox"/>	User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

Showing 1 - 10 of 111 items Showing 1 of 12

1. 单击添加。此时将显示添加新服务器属性页面。

XenMobile Analyze Manage Configure

admin

Settings > Server Properties > Add New Server Property

Add New Server Property

Key ?

Value*

Display name*

Description

Cancel Save

2. 配置以下设置：

- **密钥**：在列表中，选择合适的密钥。键区分大小写。如果要编辑属性值或申请特殊密钥，请联系 Citrix 支持。
- **值**：根据选择的密钥输入一个值。
- **显示名称**：输入新属性值显示在**服务器属性**表格中的名称。
- **说明**：（可选）键入新服务器属性的说明。

3. 单击保存。

1. 在**服务器属性**表格中，选择要编辑的服务器属性。

注意：选中服务器属性旁边的复选框时，选项菜单将显示在服务器属性列表上方。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。

2. 单击**编辑**。此时将显示**编辑新服务器属性**页面。

XenMobile Analyze Manage Configure

Settings > Server Properties > Edit New Server Property

Edit New Server Property

Key	ag.client.cert.throttling.mi
Value*	30
Display name*	NetScaler Gateway Client
Description	Throttling interval for issuance of NetScaler Gateway client certificates.

Cancel Save

3. 适当更改以下信息：

- **密钥**：无法更改此字段。
- **值**：属性值。
- **显示名称**：属性名称。
- **说明**：属性说明。

4. 单击**保存**以保存您的更改，或单击**取消**保持属性不变。

1. 在**服务器属性**表格中，选择要删除的服务器属性。

注意：可以通过选中每个属性旁边的复选框，选择要删除的多个属性。

2. 单击**删除**。此时将显示确认对话框。再次单击**删除**。

命令行接口选项

Apr 13, 2017

对于本地安装的 XenMobile 服务器，您可以随时按如下所示访问 CLI 选项：

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

可以使用 CLI 执行各种配置和故障排除任务。下面是 CLI 的顶层菜单。

```
-----  
Main Menu  
-----  
[0] Configuration  
[1] Clustering  
[2] System  
[3] Troubleshooting  
[4] Help  
[5] Log Out  
-----
```

下面是 Configuration（配置）菜单以及为每个选项所显示的设置的示例。

```
-----  
Configuration Menu  
-----  
[0] Back to Main Menu  
[1] Network  
[2] Firewall  
[3] Database  
[4] Listener Ports  
-----
```

[1] Network (网络)

```
Reboot is required to save the changes.  
Do you want to proceed? (y/n) [y]: y  
IP address [10.207.87.75]: 10.200.87.75  
Netmask [255.255.254.0]: 255.255.254.0  
Default gateway [10.207.86.1]: 10.200.86.1  
Primary DNS server [10.207.86.50]: 10.200.86.50  
Secondary DNS server (optional) []:  
  
Applying network settings...  
  
Are you sure to restart the system? [y/n]: █
```

[2] Firewall (防火墙)

```

Configure which services are enabled through the firewall.

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

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

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

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

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

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

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

```

[3] Database (数据库)

```

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

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

```

[4] Listener Ports (侦听器端口)

```

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

```

下面是 Clustering（群集）菜单以及为每个选项所显示的设置的示例。

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

[1] Show Cluster Status（显示群集状态）

```
Current Node ID: 181360459

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

[2] Enable/Disable cluster（启用/禁用群集）

选择启用群集时，将显示以下消息：

To enable realtime communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings for restricted access.（要在群集成员之间启用实时通信，请使用 CLI 菜单上的“Firewall”菜单选项打开端口 80。同时在“Firewall”设置下配置访问白名单以限制访问。）

选择禁用群集时，将显示以下消息：

You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.（您已选择禁用群集。无需访问端口 80。请禁用此端口）。

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

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

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

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

当选择启用或禁用 SSL 卸载时，将显示以下消息：

Enabling SSL offload will open port 80 for everyone. Please configure Access white list under Firewall settings for

restricted access. (启用 SSL 卸载将为所有人打开端口 80。请在“Firewall”设置下配置访问白名单以限制访问。)

[5] Display Hazelcast Cluster (显示 Hazelcast 群集)

选择显示 Hazelcast 群集时，将显示以下选项：

Hazelcast Cluster Members: (Hazelcast 群集成员:)

[列出 IP 地址]

注意：如果所配置的某个节点不属于群集，请重新启动该节点。

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

```
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----
```

[12] Advanced Settings (高级设置)

```
***** WARNING *****
Please only modify these options if you are
in contact with Citrix Support
*****

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] Reset SSL Certificate
[4] Reset pki.xml
[5] Server Tuning
-----
```

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

下面是 Troubleshooting (故障排除) 菜单以及为每个选项所显示的设置的示例。

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

[1] Network Utilities (网络实用程序)

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

[2] Logs (日志)

```
Logs Menu
-----
[0] Back to Troubleshooting Menu
[1] Display Log File
-----
```

[3] Support Bundle (支持包)

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

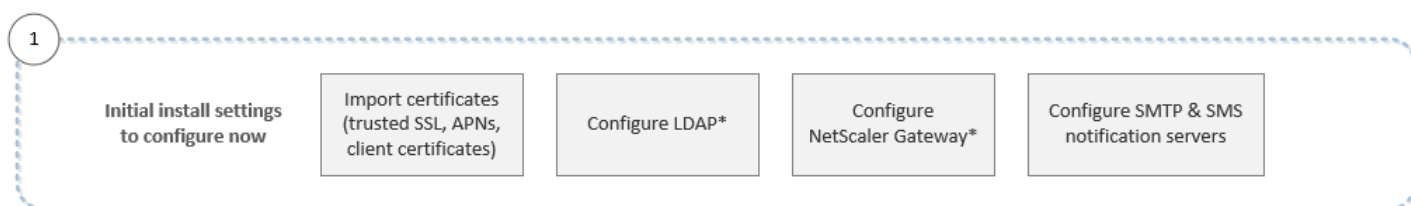
XenMobile 控制台工作流程入门

Mar 10, 2017

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

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

注意：带星号的项目为可选项目。



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

- [身份验证](#)
- [NetScaler Gateway 和 XenMobile](#)
- [通知](#)

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

Android

- 创建 Google Play 凭据。有关详细信息，请参阅 [Google Play 启动](#)。
- 创建一个 Android for Work 管理员帐户。有关详细信息，请参阅 [Android at Work](#)。
- 通过 Google 验证您的域名。有关详细信息，请参阅 [Verify your domain for G Suite](#)（验证您的 G Suite 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 [Android Enterprise 帮助](#)。

iOS

- 创建一个 Apple ID 和开发人员帐户。有关详细信息，请参阅 [Apple Developer Program](#)（Apple 开发者计划）Web 站点。
- 创建一个 Apple 推送通知服务 (APNs) 证书。如果您打算通过 XenMobile Service（云）部署管理 iOS 设备，则需要使用 Apple APNs 证书。如果您为您的 WorxMail 部署使用推式通知，您还需要 Apple APNs 证书。有关获取 Apple APNs 证书的详细信息，请参阅 [Apple 推送证书门户](#)。有关 XenMobile 和 APNs 的详细信息，请参阅 [APNs 证书](#)和 [WorxMail for iOS 的推送通知](#)。
- 创建一个批量购买计划 (VPP) 公司令牌。有关详细信息，请参阅 [Apple Volume Purchasing Program](#)。

Windows

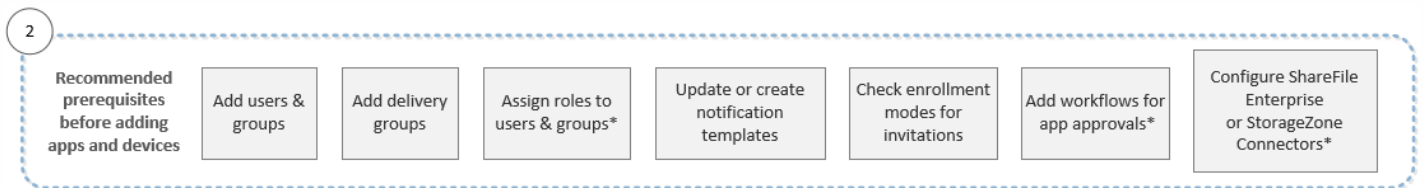
- 创建一个 Microsoft Windows 应用商店开发人员帐户。有关详细信息，请参阅 [Microsoft Windows Dev Center](#)（Microsoft Windows 开发人员中心）。
- 获取一个 Microsoft Windows 应用商店发布者 ID。有关详细信息，请参阅 [Microsoft Windows Dev Center](#)（Microsoft

Windows 开发人员中心)。

- 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 开发人员中心)。
- 如果计划在注册 Windows Phone 时使用 XenMobile 自动发现功能，请确保您具有可用的公用 SSL 证书。有关详细信息，请参阅 [XenMobile 自动发现服务](#)。
- 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 开发人员中心)。

此工作流程显示在添加应用程序和设备之前要配置的必备条件。

注意：带星号的项目为可选项目。

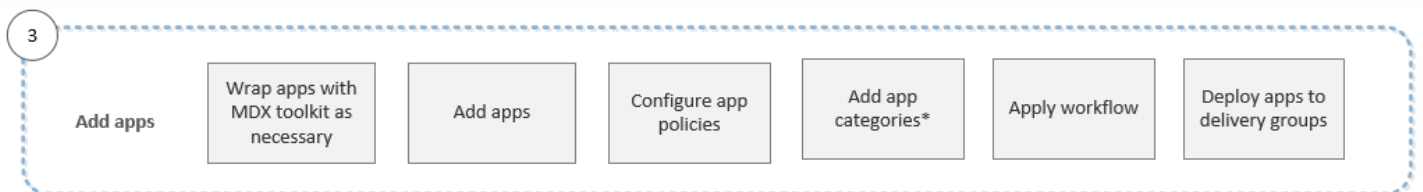


有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章和各节：

- [用户帐户、角色和注册](#)
- [部署资源](#)
- [使用 RBAC 配置角色](#)
- [通知](#)
- [创建和管理 workflow](#)
- [ShareFile 与 XenMobile 结合使用](#)

此工作流程显示了向 XenMobile 中添加应用程序时应遵循的建议顺序。

注意：带星号的项目为可选项目。



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

- [关于 MDX Toolkit](#)
- [添加应用程序](#)
- [MDX 策略概览](#)
- [创建和管理 workflow](#)
- [部署资源](#)

此工作流程显示了向 XenMobile 中添加和注册设备时应遵循的建议顺序。

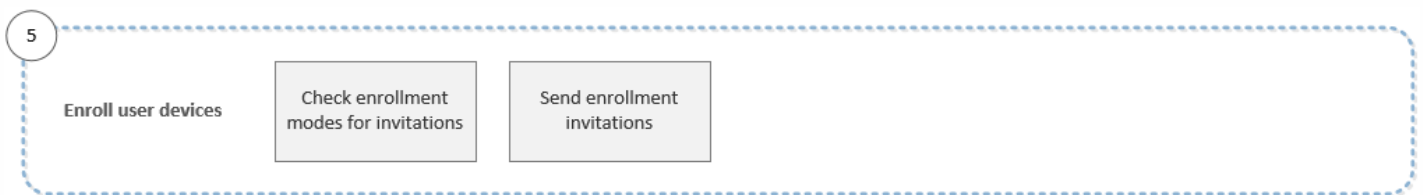
注意：带星号的项目为可选项目。



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

- [设备](#)
- [支持的设备操作系统](#)
- [部署资源](#)
- [监视和支持](#)
- [自动化操作](#)

此工作流程显示了在 XenMobile 中注册用户设备时应遵循的建议顺序。

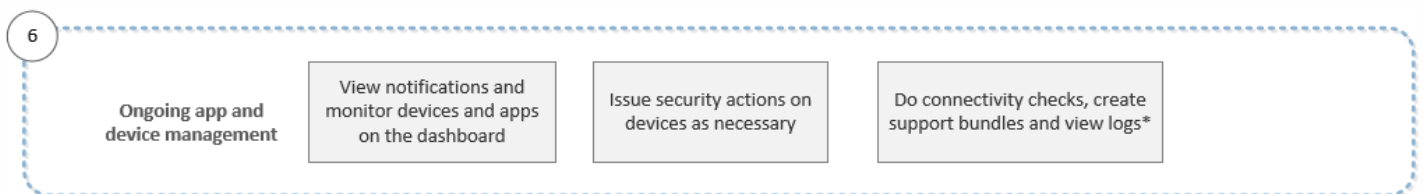


有关每项设置的详细信息及分步说明，请参阅以下 Citrix 产品文档文章：

- [用户帐户、角色和注册](#)
- [通知](#)

此工作流程显示您可以在控制台中执行的应用程序和设备管理活动。

注意：带星号的项目为可选项目。



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

证书和身份验证

Feb 27, 2017

在 XenMobile 操作期间，若干组件都会参与身份验证：

- **XenMobile 服务器**：在 XenMobile 服务器中可以定义注册安全性和注册体验。加入用户的选项包括向所有用户开放注册还是仅对收到邀请的用户开放注册，以及要求执行双重身份验证还是三重身份验证。通过 XenMobile 中的客户端属性，您可以启用 Citrix PIN 身份验证以及配置 PIN 复杂性和过期时间。
- **NetScaler**：NetScaler 为 Micro VPN SSL 会话提供终端。NetScaler 还提供网络在途安全，并允许您定义用户每次访问应用程序时的身份验证体验。
- **Secure Hub**：注册期间，Secure Hub 会与 XenMobile 服务器协同工作。Secure Hub 是设备上可以与 NetScaler 通信的实体：会话过期时，Secure Hub 会从 NetScaler 获取身份验证票证，并将该票证传递给 MDX 应用程序。Citrix 建议使用证书固定，以防中间人攻击。有关详细信息，请参阅 [Secure Hub](#) 一文中的证书固定部分。

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

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

有关如何配置身份验证的注意事项的详细信息，包括单重方法和双重方法概述，请参阅《部署手册》中的[身份验证](#)一文。

使用 XenMobile 中的证书创建安全连接并对用户进行身份验证。本文余下部分将介绍证书。有关其他配置详细信息，请参阅以下文章：

- [域或域加安全令牌身份验证](#)
- [客户端证书或证书加域身份验证](#)
- [PKI 实体](#)
- [凭据提供程序](#)
- [APNs 证书](#)
- [SAML 单点登录与 ShareFile](#)
- [Microsoft Azure Active Directory 服务器设置](#)

证书

默认情况下，XenMobile 附带有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。

注意

iOS 10.3 设备不支持自签名证书。如果 XenMobile 使用自签名证书，用户无法将 iOS 10.3 设备注册到 XenMobile 中。要将运行 iOS 10.3 或更高版本的设备注册到 XenMobile 中，必须在 XenMobile 中使用可信 SSL 证书。

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

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

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

下表显示了每个 XenMobile 组件的证书格式和类型：

XenMobile 组件	证书格式	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	.p12 (在基于 Windows 的计算机上为 .pfx)	SSL、SAML、APNs XenMobile 还在安装过程中生成完全 PKI。 重要： XenMobile 服务器不支持扩展名为 .pem 的证书。
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。

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

本部分内容介绍了上载证书的常规过程。有关创建、上载和配置客户端证书的详细信息，请参阅 [客户端证书或证书加域身份验证](#)。

私钥要求

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

向控制台上载证书

将证书上载到控制台的主要方式有两种：

- 您可以单击以导入一个密钥库。然后，您在密钥库存储库中识别要安装的条目，除非您要上载 PKCS#12 格式。

- 可以单击以导入一个证书。

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

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

导入密钥库

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

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击证书。此时将显示证书页面。

Settings > Certificates

Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import | Add

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key	▼
<input type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2015-11-16	2025-11-13	SAML	✓	
<input type="checkbox"/>	*.agsag.com		⚠ Expired	2013-10-23	2015-10-23	SSL Listener	✓	
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2015-11-16	2035-11-14	Devices CA		
<input type="checkbox"/>	ent-root-ca		Up to date	2012-02-22	2017-02-21	Root or intermediate		
<input type="checkbox"/>	APSP:3623302e-7c6e-4df8-aa91		🕒 22 days left	2015-09-30	2016-09-29	APNs	✓	

Showing 1 - 5 of 5 items

3. 单击导入。此时将显示导入对话框。

4. 配置以下设置：

- 导入：在列表中，单击密钥库。导入对话框将更改以反应可用的密钥库选项。

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import Keystore

Keystore type PKCS#12

Use as Server

Keystore file* Browse

Password*

Description

Cancel
Import

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

5. 单击导入。密钥库将添加到证书表中。

导入证书

从文件或密钥库条目导入证书时，XenMobile 将尝试基于输入内容构建证书链，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）。仅当文件或密钥库条目中的证书形成链时，才可执行此操作。例如，如果链中每个后续证书是前一个证书的颁发者。

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

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击证书。

2. 在证书页面上，单击导入。此时将显示导入对话框。

3. 在导入对话框的导入中，如果尚未选择，请单击证书。

4. 导入对话框将更改以反应可用的证书选项。在用作中，单击使用密钥库的方式。可用选项如下：

- **服务器**。服务器证书是 XenMobile 服务器功能性使用的证书，这些证书上载到 XenMobile Web 控制台中。这些证书包括 CA 证书、RA 证书以及用于您基础结构其他组件的客户端身份验证的证书。此外，您还可以使用服务器证书来存储您要部署到设备的证书。此选项特别适用于在设备上建立信任所使用的 CA。
- **SAML**。安全声明标记语言 (SAML) 认证允许您提供对服务器、Web 站点和应用程序的单点登录 (SSO) 访问权限。
- **SSL 侦听器**。安全套接字层 (SSL) 侦听器向 XenMobile 通知 SSL 加密活动。

5. 浏览查找要导入的文件类型为 .p12（在基于 Windows 的计算机上为 .pfx）的密钥库。

6. 浏览以查找证书的可选私钥文件。私钥用于与证书一起使用以便进行加密和解密。

7. 键入证书的说明（可选），以帮助您将其与其他证书区分开。

8. 单击导入。证书将添加到证书表中。

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，可以替换现有条目或将其删除。

要最有效地更新您的证书，请在 XenMobile 控制台上执行以下操作。单击控制台右上角的齿轮图标以打开设置页面，然后单击证书。在导入对话框中，导入新证书。

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

XenMobile 证书管理

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

您的环境中可能包含以下部分或所有证书：

XenMobile 服务器

用于 MDM FQDN 的 SSL 证书

SAML 证书（用于 ShareFile）

用于前述证书以及任何其他内部资源（StoreFront/代理等）的根 CA 证书和中间 CA 证书

用于 iOS 设备管理的 APN 证书

用于 XenMobile 服务器 Secure Hub 通知的内部 APNs 证书

用于连接到 PKI 的 PKI 用户证书

MDX Toolkit

Apple 开发者证书

Apple 置备配置文件（按应用程序）

Apple APNs 证书（用于 Citrix Secure Mail）

Android 密钥库文件
Windows Phone - 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
用于前述证书的根 CA 证书和中间 CA 证书

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。

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

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

可以通过登录 Apple 推送证书门户来查看 APNs 证书状态和过期日期。必须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，您还会收到 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 Apple ID CustomerID will expire on Date. Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

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

在物理 iOS 设备上运行的应用程序 (Apple App Store 中的应用程序除外) 必须通过置备配置文件进行签名。还必须使用相应的分发证书为应用程序签名。

要验证您的 iOS 分发证书是否有效，请执行以下操作：

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

要确认所有 XenMobile 服务器证书是否有效，请执行以下操作：

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

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 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。用户无法安装公司发布和签名的应用程序，也不能启动手机上安装的公司应用程序。

有关如何处理 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，用户将无法注册和访问应用商店。过期的证书还会阻止用户使用 Secure Mail 时连接到 Exchange Server。此外，用户不能枚举和打开 HDX 应用程序（具体取决于哪个证书过期）。

Expiry Monitor 和 Command Center 可以帮助您跟踪 NetScaler 证书。Center 会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：

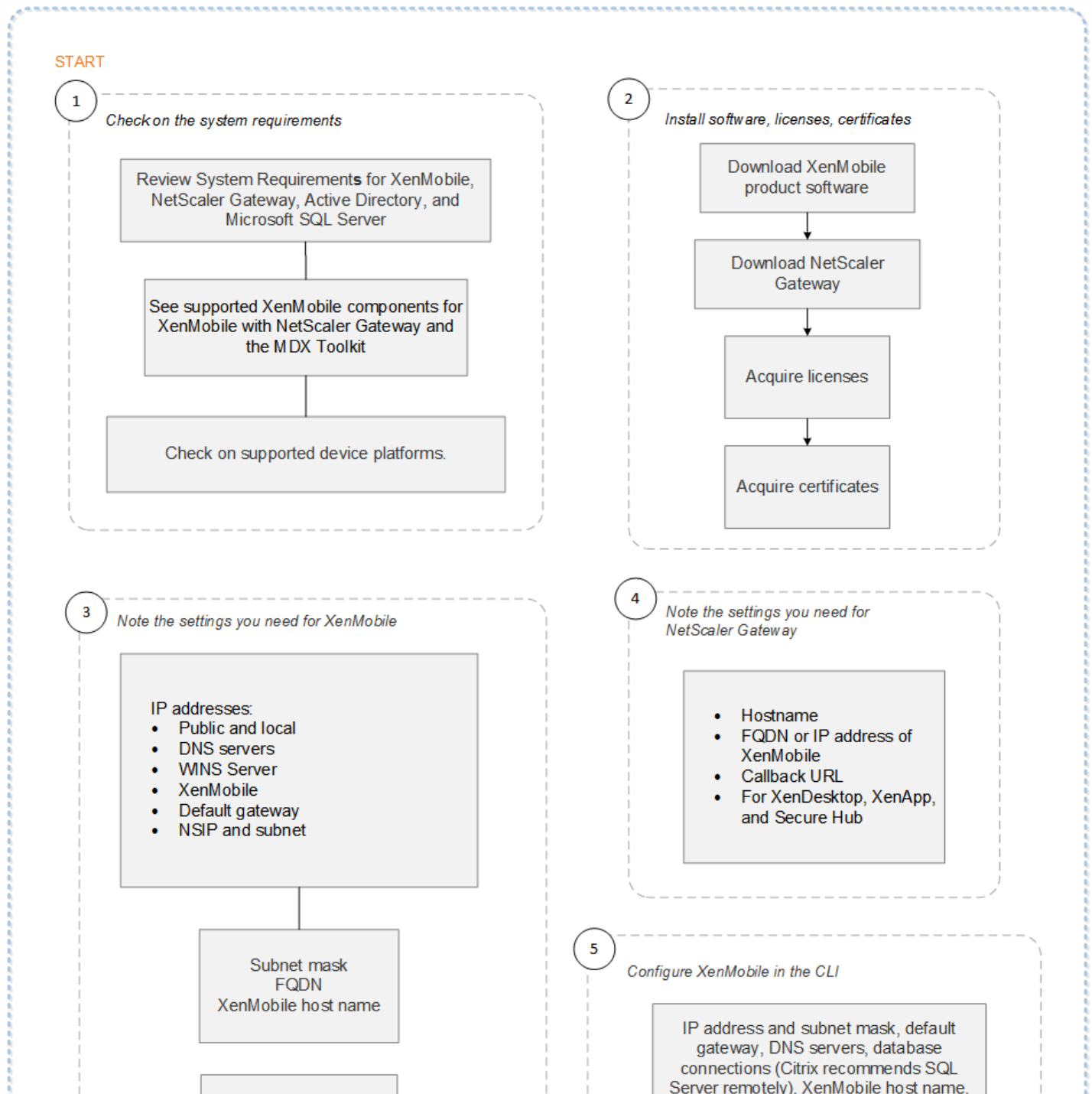
- 用于 MDM FQDN 的 SSL 证书
- 用于网关 FQDN 的 SSL 证书
- 用于 ShareFile SZC FQDN 的 SSL 证书
- 用于 Exchange 负载平衡（卸载配置）的 SSL 证书
- 用于 StoreFront 负载平衡的 SSL 证书
- 用于前述证书的根 CA 证书和中间 CA 证书

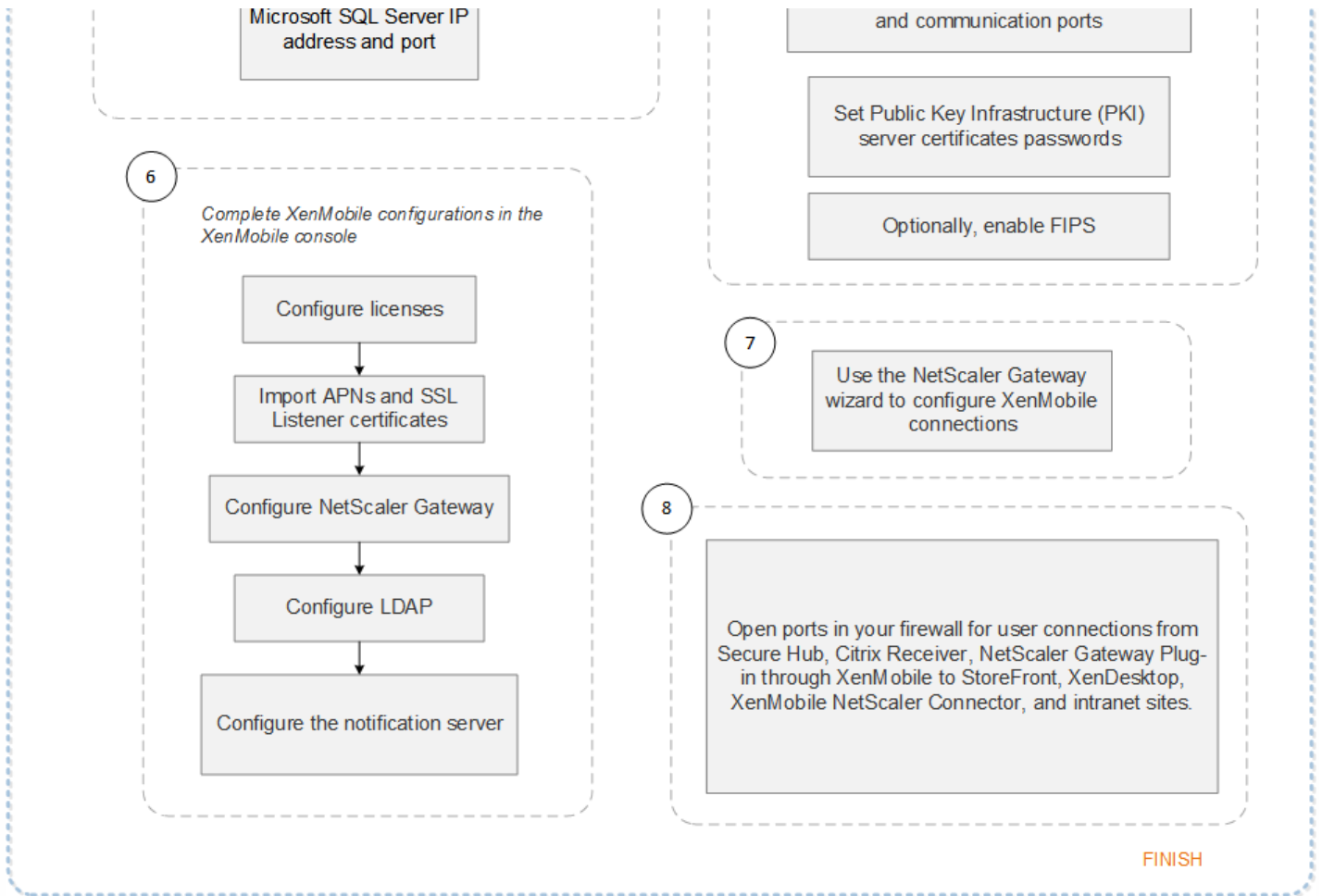
NetScaler Gateway 和 XenMobile

Feb 27, 2017

使用 XenMobile 配置 NetScaler Gateway 时，为远程设备访问内部网络建立身份验证机制。利用此功能，移动设备上的应用程序可以访问位于 Intranet 上的企业服务器，方法是在设备上的应用程序与 NetScaler Gateway 之间创建 Micro VPN。请按照本文所述在 XenMobile 控制台中配置 NetScaler Gateway。

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





1

- 系统要求和兼容性

2

- 安装和配置

3

- 预安装核对表

4

- 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

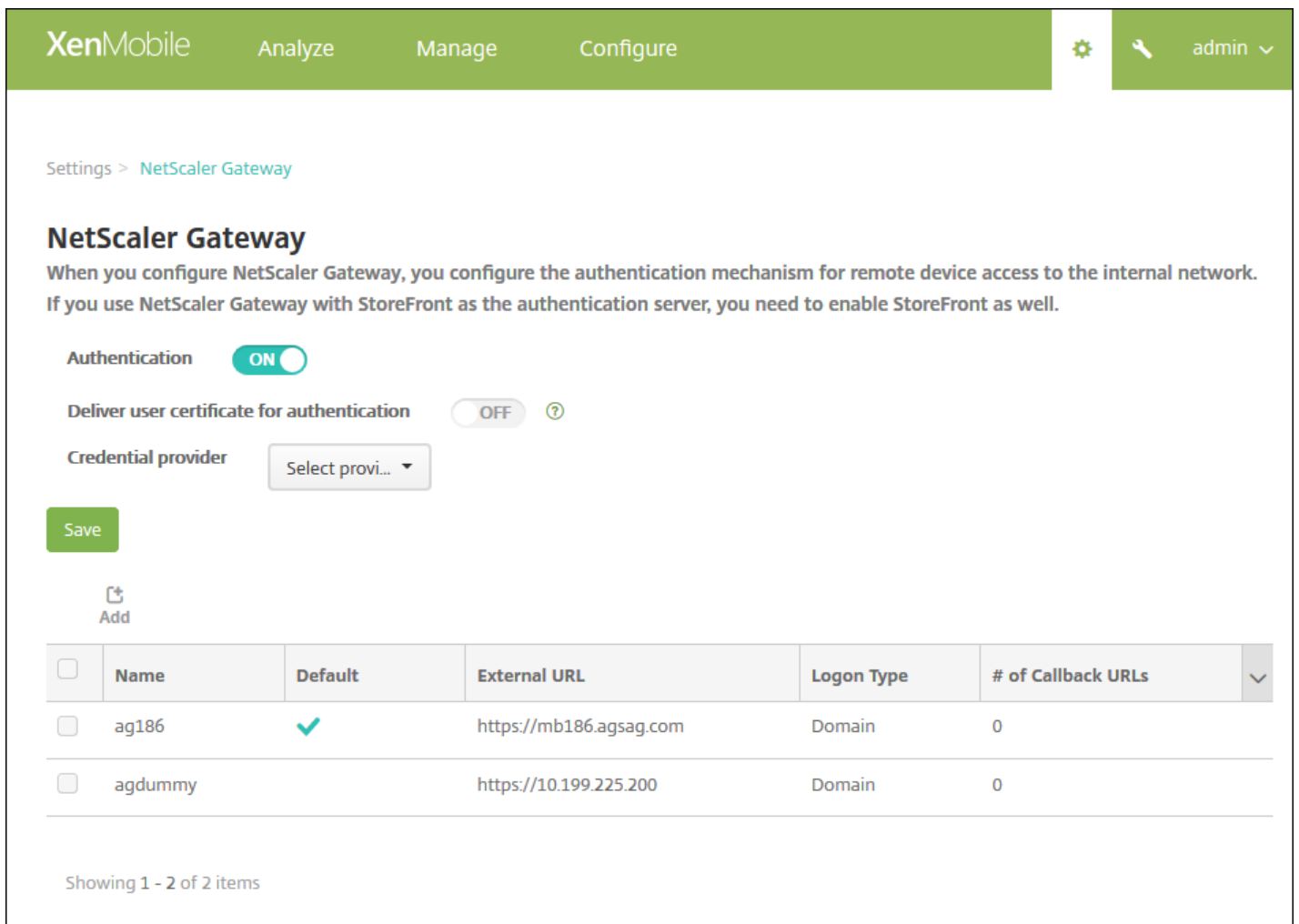
8

- 端口

流程图还以 PDF 格式提供。

 [部署 XenMobile 的流程图](#)

1. 在 XenMobile Web 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **NetScaler Gateway**。此时将显示 **NetScaler Gateway** 页面。



配置以下设置：

- **身份验证**：选择是否启用身份验证。默认值为开。
- **向用户提供用于身份验证的证书**：选择是否希望 XenMobile 与 Secure Hub 共享身份验证证书，以便 NetScaler Gateway 处理客户端证书身份验证。默认值为关。
- **凭据提供程序**：在列表中，单击要使用的凭据提供程序。有关详细信息，请参阅[凭据提供程序](#)。

6. 单击保存。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将打开**设置**页面。
2. 在**服务器**下方，单击 **NetScaler Gateway**。此时将显示 **NetScaler Gateway** 页面。
3. 单击**添加**。此时将显示添加新的 **NetScaler Gateway** 页面。

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name*

Alias

External URL*

Logon Type

Password Required

Set as Default

Callback URL* Virtual IP*

4. 配置以下设置：

- **名称**：键入 NetScaler Gateway 实例的名称。
- **别名**：可以选择包含别名。
- **外部 URL**：键入 NetScaler Gateway 的公共访问 URL。例如，https://receiver.com。
- **登录类型**：在列表中，单击某个登录类型。类型包括仅限域、仅限安全令牌、域和安全令牌、证书、证书和域以及证书和安全令牌。默认值为仅限域。

如果您拥有多个域，**仅限域**类型将不起作用，您必须使用**证书和域**。对于某些选项，例如**仅限域**，无法更改密码字段。

对于此登录类型，此字段始终为开。此外，**需要密码**字段的默认值会根据所选的登录类型发生变化。

如果使用**证书和安全令牌**，需要在 NetScaler Gateway 上执行一些额外配置以支持 Secure Hub。有关信息，请参阅为 [XenMobile 配置证书和安全令牌身份验证](#)。

- **需要密码**：选择是否希望使用需要密码的身份验证。默认值为开。
- **设为默认值**：选择是否将此 NetScaler Gateway 用作默认选项。默认值为关。

5. 单击保存。此时 NetScaler Gateway 已添加并显示在表格中。可以通过单击列表中的名称编辑或删除实例。

添加 NetScaler Gateway 实例后，可以添加一个回调 URL 并指定 NetScaler Gateway VPN 虚拟 IP 地址。**注意**：这是可选字段，但是可以进行配置以增强安全性，特别是当 XenMobile 服务器位于 DMZ 时。

1. 在 NetScaler Gateway 屏幕中，选择表格中的 NetScaler Gateway，然后单击**添加**。此时将显示**添加新的 NetScaler Gateway** 页面。

2. 在列出回调 URL 的表格中，单击**添加**。
3. 指定回调 URL。此字段表示完全限定的域名 (FQDN)，并验证请求是否来自 NetScaler Gateway。回调 URL 必须解析为可从 XenMobile 服务器访问的 IP 地址，但不必是外部 NetScaler Gateway URL。
4. 输入 NetScaler Gateway 的虚拟 IP 地址，然后单击**保存**。

域或域加安全令牌身份验证

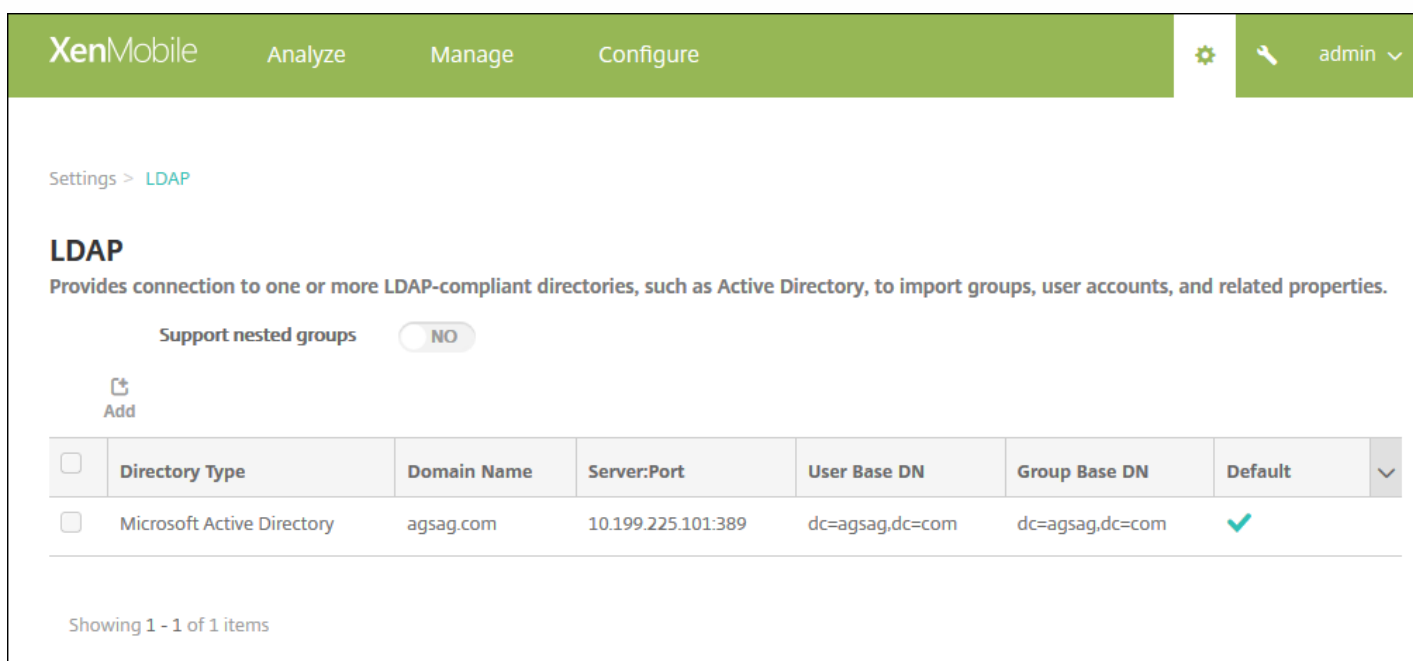
Feb 27, 2017

XenMobile 支持根据一个或多个目录执行基于域的身份验证，例如与轻型目录访问协议 (LDAP) 兼容的 Active Directory。您可以在 XenMobile 中配置与一个或多个目录的连接，然后使用 LDAP 配置导入组、用户帐户和相关属性。

LDAP 是一个独立于供应商的开源应用程序协议，用于通过 Internet 协议 (IP) 网络访问和维护分布式目录信息服务。目录信息服务用于共享通过网络可用的用户、系统、网络、服务和应用程序信息。LDAP 的常见用处是为用户提供单点登录 (SSO)，即每个用户在多项服务之间共享一个密码，使用户登录一次公司 Web 站点之后，即可自动登录到公司的 Intranet。

客户端通过连接到 LDAP 服务器（称为目录系统代理程序 (Directory System Agent, DSA)）启动 LDAP 会话。然后，客户端向服务器发送操作请求，服务器通过相应的身份验证进行响应。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击 **LDAP**。此时将显示 **LDAP** 页面。可以从此页面[添加](#)、[编辑](#)或[删除](#)兼容 LDAP 的目录。




XenMobile Analyze Manage Configure admin

Settings > LDAP

LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups NO

 Add

<input type="checkbox"/>	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default	
<input checked="" type="checkbox"/>	Microsoft Active Directory	agsag.com	10.199.225.101:389	dc=agsag,dc=com	dc=agsag,dc=com	<input checked="" type="checkbox"/>	✓

Showing 1 - 1 of 1 items

1. 在 **LDAP** 页面上，单击添加。此时将显示添加 **LDAP** 页面。

Settings > LDAP > Add LDAP

Add LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	<input type="text" value="Microsoft Active Directory"/>	?
Primary server*	<input type="text" value="IP Address or FQDN"/>	
Secondary server	<input type="text" value="IP Address or FQDN"/>	
Port*	<input type="text" value="389"/>	
Domain name*	<input type="text"/>	
User base DN*	<input type="text" value="dc=example,dc=com"/>	?
Group base DN*	<input type="text" value="dc=example,dc=com"/>	?
User ID*	<input type="text"/>	
Password*	<input type="password"/>	
Domain alias*	<input type="text"/>	
XenMobile Lockout Limit	<input type="text" value="0"/>	?
XenMobile Lockout Time	<input type="text" value="1"/>	?
Global Catalog TCP Port	<input type="text" value="3268"/>	?
Global Catalog Root Context	<input type="text" value="dc=example,dc=com"/>	?
User search by	<input type="text" value="userPrincipalName"/>	
Use secure connection	<input type="radio" value="NO"/>	

Cancel

Save

2. 配置以下设置：

- **目录类型**：在列表中，单击相应的目录类型。默认值为 **Microsoft Active Directory**。
- **主服务器**：键入用于 LDAP 的主服务器；可以输入 IP 地址或完全限定的域名 (FQDN)。
- **辅助服务器**：(可选) 如果配置了辅助服务器，请输入辅助服务器的 IP 地址或 FQDN。此服务器是故障转移服务器，在无法访问主服务器时使用。
- **端口**：键入 LDAP 服务器使用的端口号。默认情况下，对于不安全的 LDAP 连接，端口号设置为 389。请为安全的 LDAP 连接使用端口号 636，为 Microsoft 的不安全 LDAP 连接使用 3268，或者为 Microsoft 的安全 LDAP 连接使用 3269。

- **域名**：键入域名。
- **用户基础 DN**：通过唯一的标识符在 Active Directory 中键入用户的位置。语法示例包括：ou=users、dc=example 或 dc=com。
- **组基本 DN**：在 Active Directory 中键入组的位置。例如，cn=users, dc=domain, dc=net，其中 cn=users 表示组的容器名称，dc 表示 Active Directory 的域组件。
- **用户 ID**：键入与 Active Directory 帐户关联的用户 ID。
- **密码**：键入与用户关联的密码。
- **域别名**：键入域名称的别名。
- **XenMobile 锁定限制**：键入介于 0 至 999 之间的数字，表示失败登录尝试次数。将此字段设置为 0 表示 XenMobile 从不会根据失败登录尝试次数锁定用户。
- **XenMobile 锁定时间**：键入介于 0 至 99999 之间的数字，表示用户超过锁定限制后必须等待的分钟数。将此字段设为 0 表示不会强制用户在锁定后等待。
- **全局目录 TCP 端口**：键入全局目录服务器的 TCP 端口号。默认情况下，TCP 端口号设为 3268；对于 SSL 连接，使用端口号 3269。
- **全局目录根上下文**：可选，键入用于在 Active Directory 中启用全局目录搜索的全局根上下文值。此搜索是除标准 LDAP 搜索之外的方法，可在任何域中使用，无需指定实际的域名。
- **用户搜索依据**：在此列表中，单击 **userPrincipalName** 或 **sAMAccountName**。默认值为 **userPrincipalName**。
- **使用安全连接**：选择是否使用安全连接。默认值为否。

3. 单击保存。

1. 在 LDAP 表中，选择要编辑的目录。

注意：如果选中某个目录旁边的复选框，选项菜单将显示在 LDAP 列表上方；如果单击此列表的任何其他位置，选项菜单将显示在列表右侧。

2. 单击编辑。此时将显示编辑 LDAP 页面。

Edit LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	10.61	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*	.net	
User base DN*	dc=,dc=net	?
Group base DN*	dc=,dc=net	?
User ID*	administrator@.net	
Password*		
Domain alias*	.net	
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

3. 适当更改以下信息：

- **目录类型**：在列表中，单击相应的目录类型。
- **主服务器**：键入用于 LDAP 的主服务器；可以输入 IP 地址或完全限定的域名 (FQDN)。
- **辅助服务器**：(可选) 键入辅助服务器的 IP 地址或 FQDN (如果配置了辅助服务器)。
- **端口**：键入 LDAP 服务器使用的端口号。默认情况下，对于不安全的 LDAP 连接，端口号设置为 389。请为安全的 LDAP 连接使用端口号 636，为 Microsoft 的不安全 LDAP 连接使用 3268，或者为 Microsoft 的安全 LDAP 连接使用 3269。
- **域名**：无法更改此字段。
- **用户基础 DN**：通过唯一的标识符在 Active Directory 中键入用户的位置。语法示例包括：ou=users、dc=example 或 dc=com。
- **组基础 DN**：键入组基础 DN 组名，以 cn=groupname 的形式指定。例如，cn=users, dc=servername, dc=net，其中 cn=users 是组名；DN 和 servername 表示运行 Active Directory 的服务器的名称。
- **用户 ID**：键入与 Active Directory 帐户关联的用户 ID。
- **密码**：键入与用户关联的密码。
- **域别名**：键入域名称的别名。
- **XenMobile 锁定限制**：键入介于 0 至 999 之间的数字，表示失败登录尝试次数。将此字段设置为 0 表示 XenMobile 从不会根据失败登录尝试次数锁定用户。
- **XenMobile 锁定时间**：键入介于 0 至 99999 之间的数字，表示用户超过锁定限制后必须等待的分钟数。将此字段设为 0 表示不会强制用户在锁定后等待。
- **全局目录 TCP 端口**：键入全局目录服务器的 TCP 端口号。默认情况下，TCP 端口号设为 3268；对于 SSL 连接，使用端口号 3269。
- **全局目录根上下文**：可选，键入用于在 Active Directory 中启用全局目录搜索的全局根上下文值。此搜索是除标准 LDAP 搜索之外的方法，可在任何域中使用，无需指定实际的域名。
- **用户搜索依据**：在此列表中，单击 **userPrincipalName** 或 **sAMAccountName**。
- **使用安全连接**：选择是否使用安全连接。

4. 单击**保存**以保存您的更改，或单击**取消**保持属性不变。

1. 在 **LDAP** 表格中，选择要删除的目录。

注意：可以通过选中每个属性旁边的复选框，选择要删除的多个属性。

2. 单击**删除**。此时将显示确认对话框。再次单击**删除**。

配置域加安全令牌身份验证

可以将 XenMobile 配置为要求用户通过 RADIUS 协议使用其 LDAP 凭据以及一次性密码进行身份验证。

为实现最佳可用性，您可以将此配置与 Citrix PIN 和 Active Directory 密码缓存组合在一起，以使用户不需要重复输入其 Active Directory 用户名和密码。用户需要在注册、密码过期和帐户锁定时输入用户名和密码。

使用 LDAP 进行身份验证要求您在 XenMobile 上安装证书颁发机构颁发的 SSL 证书。有关详细信息，请参阅[在 XenMobile 中上传证书](#)。

1. 在**设置**中，单击 **LDAP**。

2. 选择 **Microsoft Active Directory**，然后单击**编辑**。

XenMobile Analyze Manage Configure admin

Settings > LDAP

LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups NO

Add Edit Delete

<input type="checkbox"/>	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
<input checked="" type="checkbox"/>	Microsoft Active Directory	xmlab.net	10.207.86.51:389	dc=xmlab,dc=net	dc=xmlab,dc=net	<input checked="" type="checkbox"/>

3. 确认“端口”为 636（适用于安全 LDAP 连接）还是 3269（适用于 Microsoft 安全 LDAP 连接）。

4. 将使用安全连接更改为是。

XenMobile Analyze Manage Configure admin

Port* 636

Domain name* .net

User base DN* dc=.net

Group base DN* dc=.net

User ID* administrator@.net

Password*

Domain alias* .net

XenMobile Lockout Limit 0

XenMobile Lockout Time 1

Global Catalog TCP Port 3269

Global Catalog Root Context dc=example,dc=com

User search by userPrincipalName

Use secure connection

Cancel Save

以下步骤假定您已向 XenMobile 中添加 NetScaler Gateway 实例。要添加 NetScaler Gateway 实例，请参阅[配置新 NetScaler Gateway 实例](#)。

1. 在设置中，单击 **NetScaler Gateway**。
2. 选择 **NetScaler Gateway**，然后单击**编辑**。
3. 在登录类型中，选择域和安全令牌。

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name*

Alias

External URL*

Logon Type

Password Required

Set as Default

Callback URL*	Virtual IP*	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

要启用 Citrix PIN 和用户密码缓存，请转至设置 > 客户端属性，然后选中这些复选框：启用 Citrix PIN 身份验证和启用户密码缓存。有关详细信息，请参阅[客户端属性](#)。

为与 XenMobile 配合使用的虚拟服务器配置 NetScaler Gateway 会话配置文件和策略。有关信息，请参阅 NetScaler Gateway 文档中的[为 XenMobile 配置域和安全令牌身份验证](#)。

客户端证书或证书加域身份验证

Feb 27, 2017

XenMobile 的默认配置是用户名和密码身份验证。要为 XenMobile 环境中的注册和访问再增加一个安全层，请考虑使用基于证书的身份验证。在 XenMobile 环境中，此配置是用于实现安全性和用户体验的最佳解决方案，同时，通过 NetScaler 进行的双重身份验证还能提供最佳 SSO 选择和安全。

如果禁用了 LDAP 并且不希望使用智能卡或类似方法，配置证书可代替智能卡来访问 XenMobile。用户随后使用 XenMobile 生成的唯一 PIN 进行注册。用户获取访问权限后，XenMobile 会创建和部署后续用来在 XenMobile 环境中执行身份验证的证书。

使用 NetScaler 仅证书身份验证或证书加域身份验证时，可以使用 NetScaler for XenMobile 向导设置 XenMobile 所需的配置。只能运行一次 NetScaler for XenMobile 向导。

在对安全性要求极高的环境中，在组织外的公共或不安全网络中使用 LDAP 凭据会被视为组织面临的首要安全威胁，这时可以使用客户端证书和安全令牌这种双重身份验证方案。有关信息，请参阅[XenMobile 配置证书和安全令牌身份验证](#)。

客户端证书身份验证适用于 XenMobile MAM 模式（仅 MAM）和 ENT 模式（当用户注册到 MDM 时）。当用户注册到旧版 MAM 模式时，客户端证书身份验证不适用于 XenMobile ENT 模式。必须依次配置 Microsoft 服务器、XenMobile 服务器和 NetScaler Gateway，才能对 XenMobile ENT 和 MAM 模式使用客户端证书身份验证。执行本文所述的如下常规步骤。

在 Microsoft 服务器上：

1. 向 Microsoft 管理控制台中添加证书管理单元。
2. 向证书颁发机构 (CA) 中添加模板。
3. 从 CA 服务器创建 PFX 证书。

在 XenMobile 服务器上：

1. 将证书上载到 XenMobile。
2. 为基于证书的身份验证创建 PKI 实体。
3. 配置凭据提供程序。
4. 将 NetScaler Gateway 配置为提供用于进行身份验证的用户证书。

在 NetScaler Gateway 上，按照 NetScaler Gateway 文档中的[配置客户端证书或客户端证书和域身份验证](#)所述执行配置。

必备条件

- 对于使用客户端证书身份验证和 SSL 卸载的 Windows Phone 8.1 设备，必须在 NetScaler 中的两个负载平衡服务器上对端口 443 禁用 SSL 会话重用。为此，请在虚拟服务器上对端口 443 运行以下命令：

```
set ssl vserver sessReuse DISABLE
```

注意：如果禁用 SSL 会话重用，还将禁用 NetScaler 提供的某些优化功能，这会导致 NetScaler 上的性能下降。

- 要为 Exchange ActiveSync 配置基于证书的身份验证，请参阅此 [Microsoft 博客](#)。
- 如果正在使用专用服务器证书来确保流向 Exchange Server 的 ActiveSync 通信安全，请确保移动设备具有所有根证书/中间

证书。否则，在 Secure Mail 中设置邮箱时，基于证书的身份验证将失败。在 Exchange IIS 控制台中，必须执行以下操作：

- 添加一个 Web 站点以供 XenMobile 和 Exchange 使用，并绑定 Web 服务器证书。
- 使用端口 9443。
- 对于该 Web 站点，必须添加两个应用程序，一个用于 Microsoft-Server-ActiveSync，一个用于 EWS。对于这两个应用程序，请在 **SSL Settings** (SSL 设置) 下方选择 **Require SSL** (需要 SSL)。
- 确保使用最新 MDX Toolkit 打包 Secure Mail (如果您的部署方法需要)。

向 Microsoft 管理控制台添加证书管理单元

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

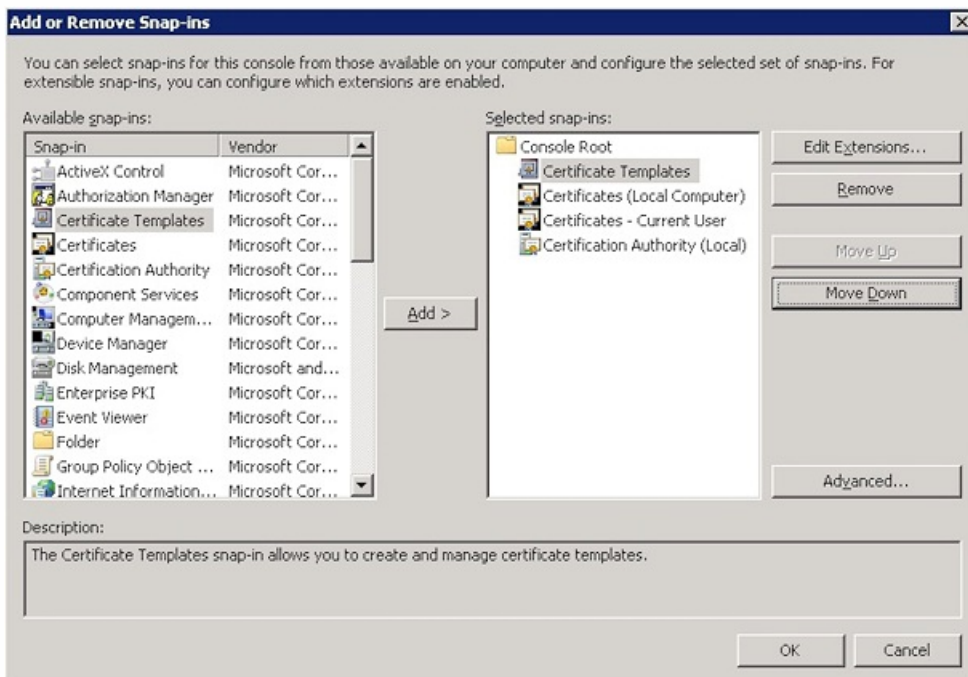
2. 添加以下管理单元：

证书模板

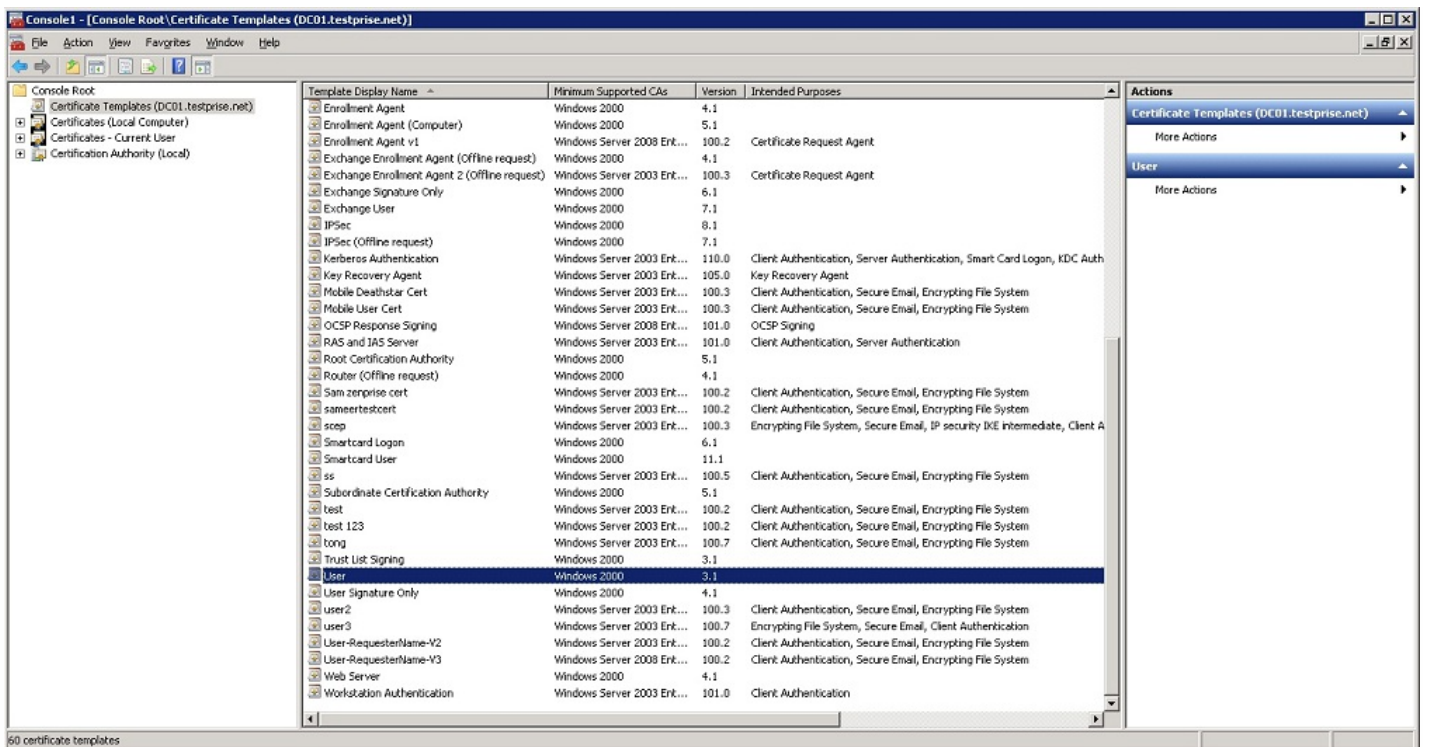
证书(本地计算机)

证书 - 当前用户

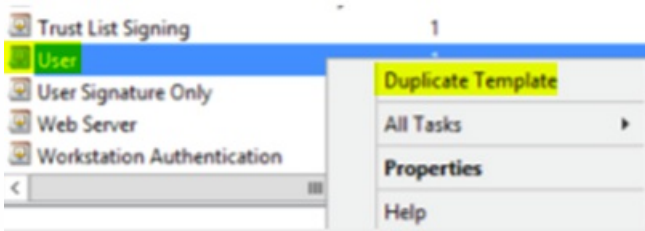
证书颁发机构(本地)



3. 展开证书模板。



4. 选择用户模板和复制模板。

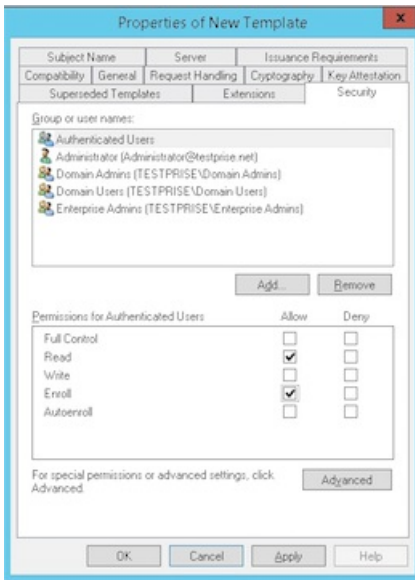


5. 提供模板显示名称。

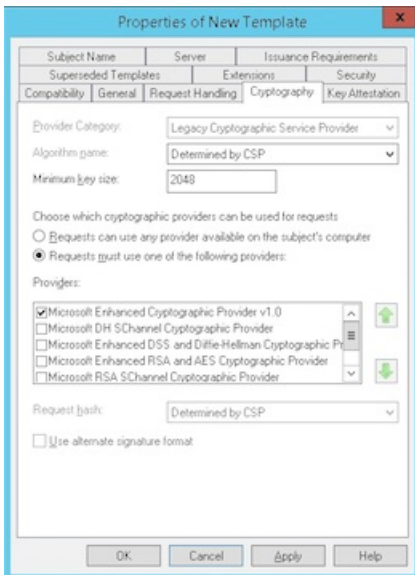
重要：除非需要，否则请勿选中在 **Active Directory** 中发布证书复选框。如果选中了此选项，则将在 Active Directory 中推送/创建所有用户客户端证书，这可能会导致您的 Active Directory 数据库混乱不堪。

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

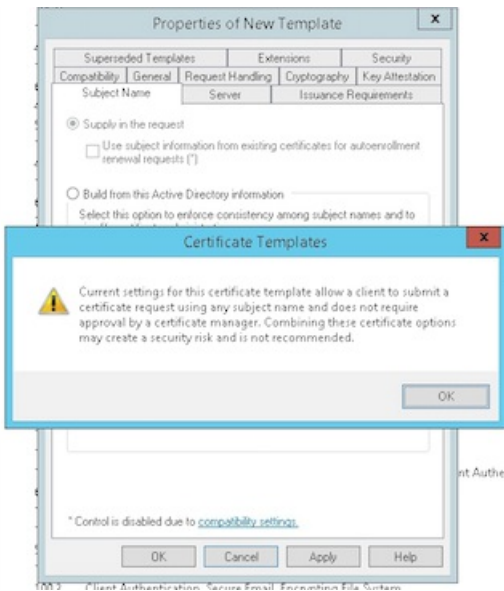
7. 在安全下方，在已通过身份验证的用户对应的允许列中选择注册选项。



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

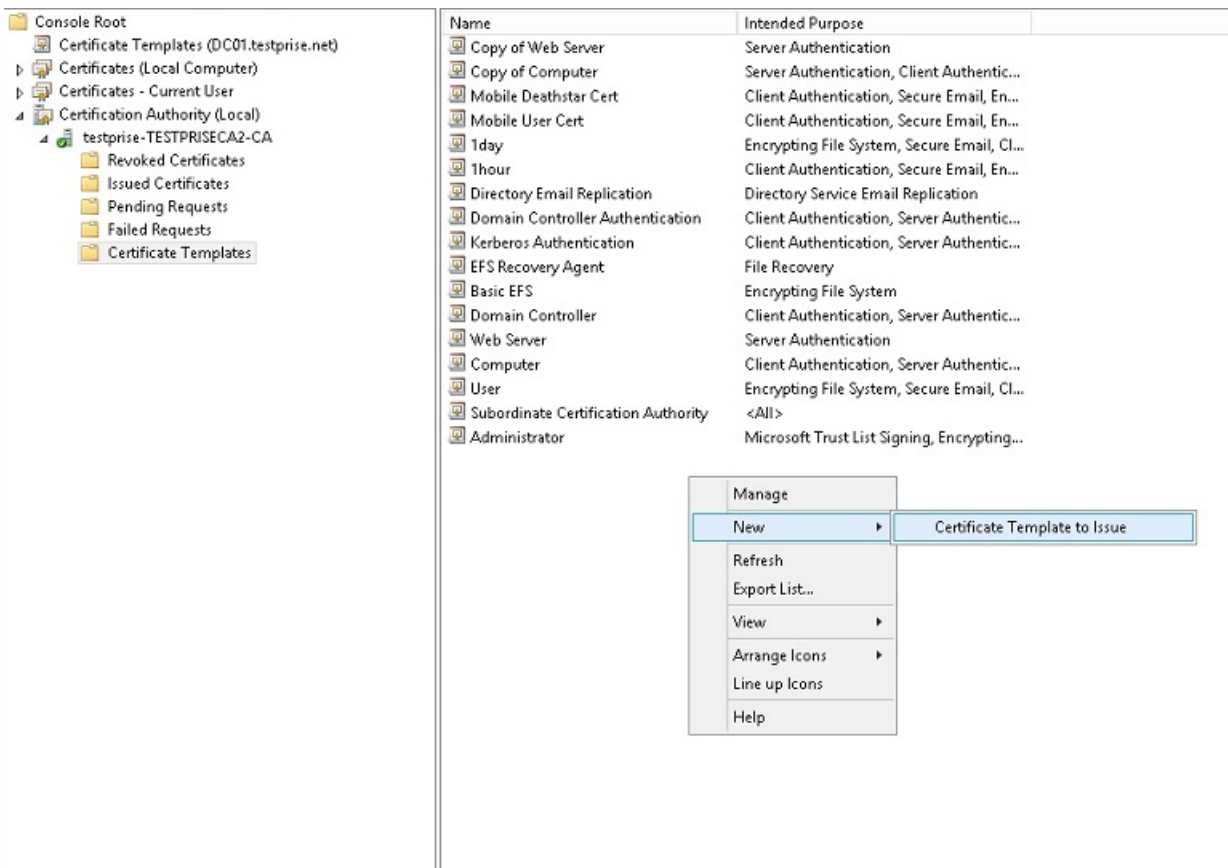


9. 在使用者名称下方，选择在请求中提供。应用更改并保存。

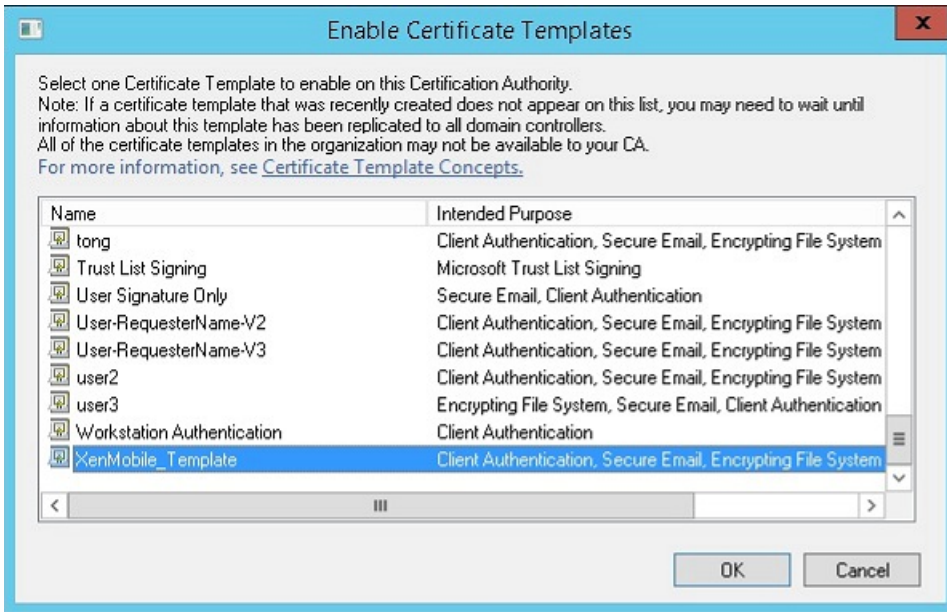


向证书颁发机构中添加模板

1. 转至证书颁发机构并选择证书模板。
2. 在右侧窗格中单击鼠标右键，然后选择新建 > 要颁发的证书模板。

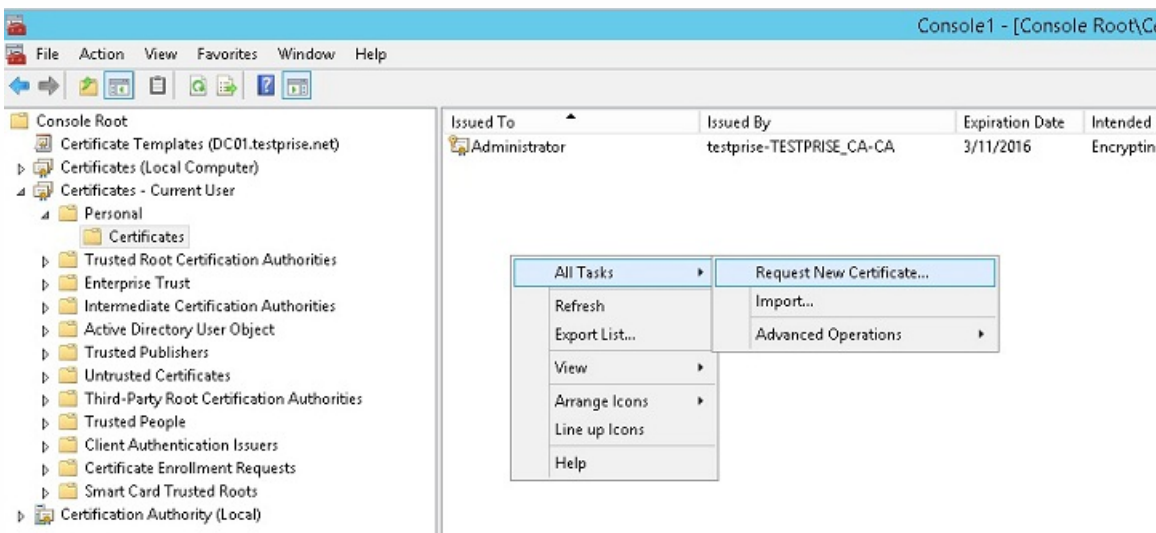


3. 选择在上一步中创建的模板，然后单击**确定**将其添加到证书颁发机构。

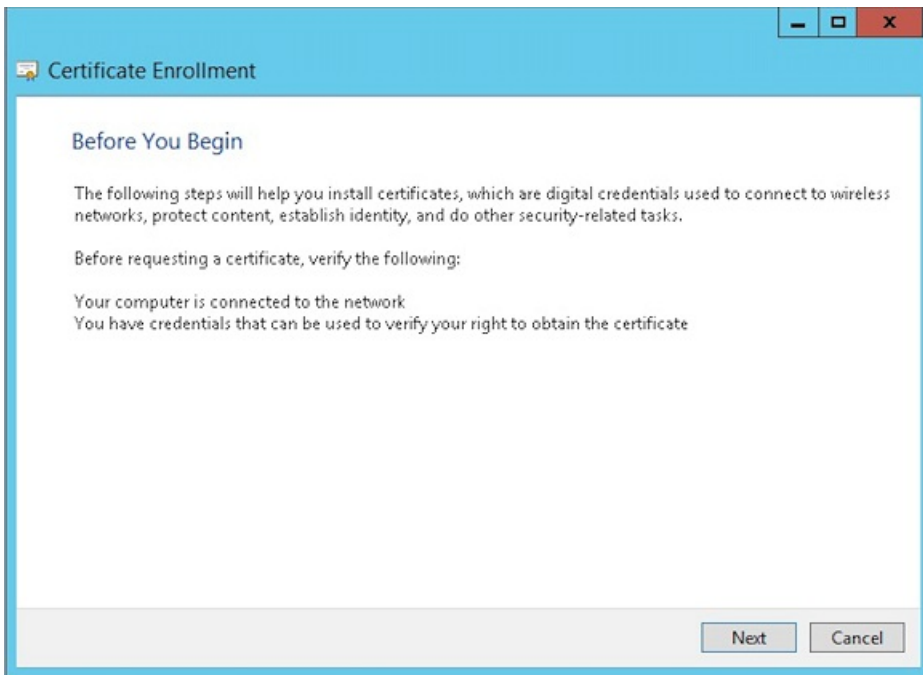


从 CA 服务器创建 PFX 证书

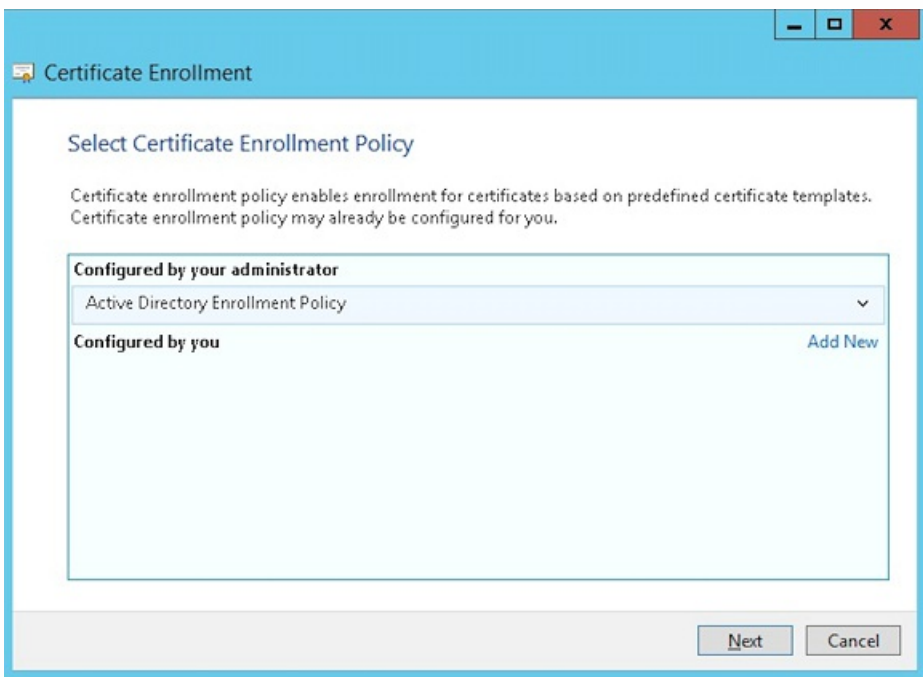
1. 使用登录时使用的服务帐户创建用户 .pfx 证书。此 .pfx 将上载到 XenMobile 中，而 XenMobile 将代表注册其设备的用户申请用户证书。
2. 在当前用户下方，展开证书。
3. 在右侧窗格中单击鼠标右键，然后单击**申请新证书**。



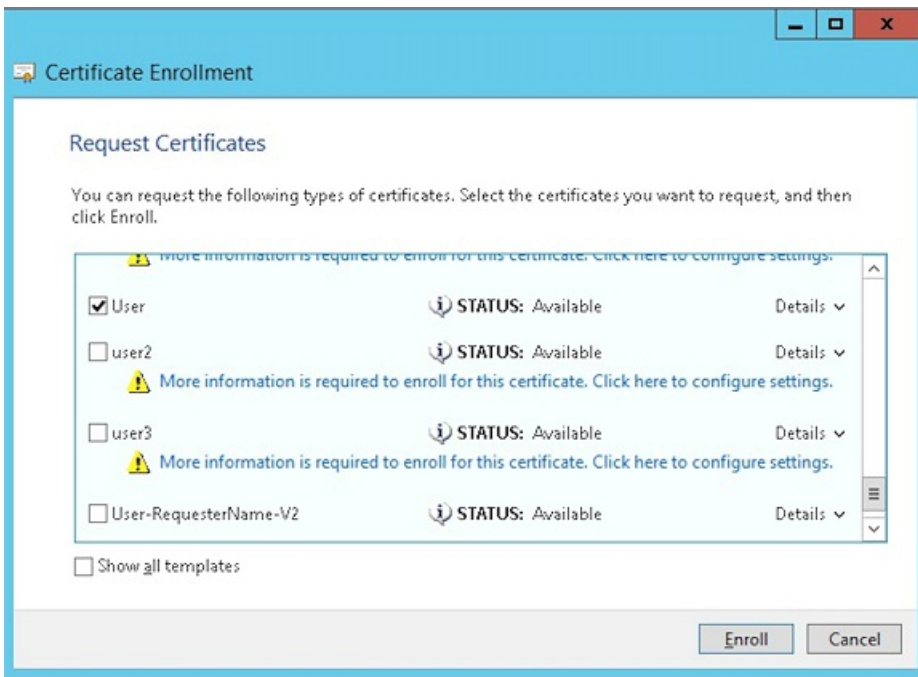
4. 此时将显示证书注册屏幕。单击下一步。



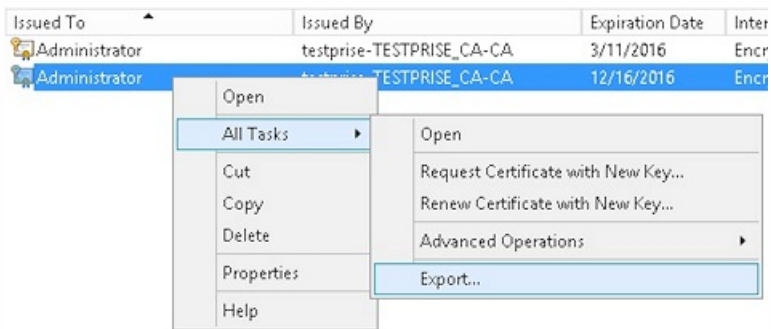
5. 选择 **Active Directory** 注册策略，然后单击下一步。



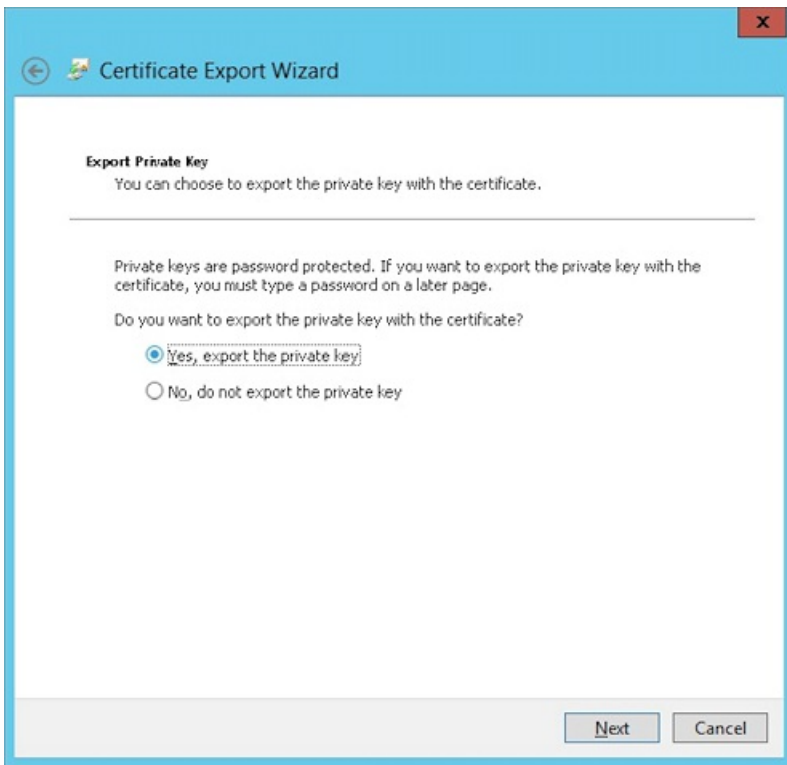
6. 选择用户模板，然后单击注册。



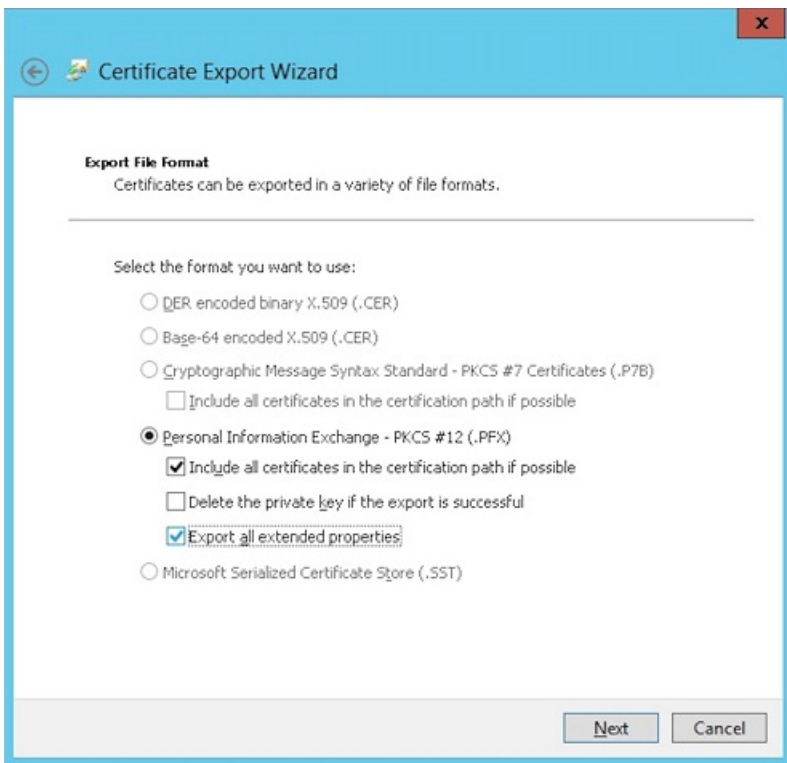
7. 导出在上一步中创建的 .pfx 文件。



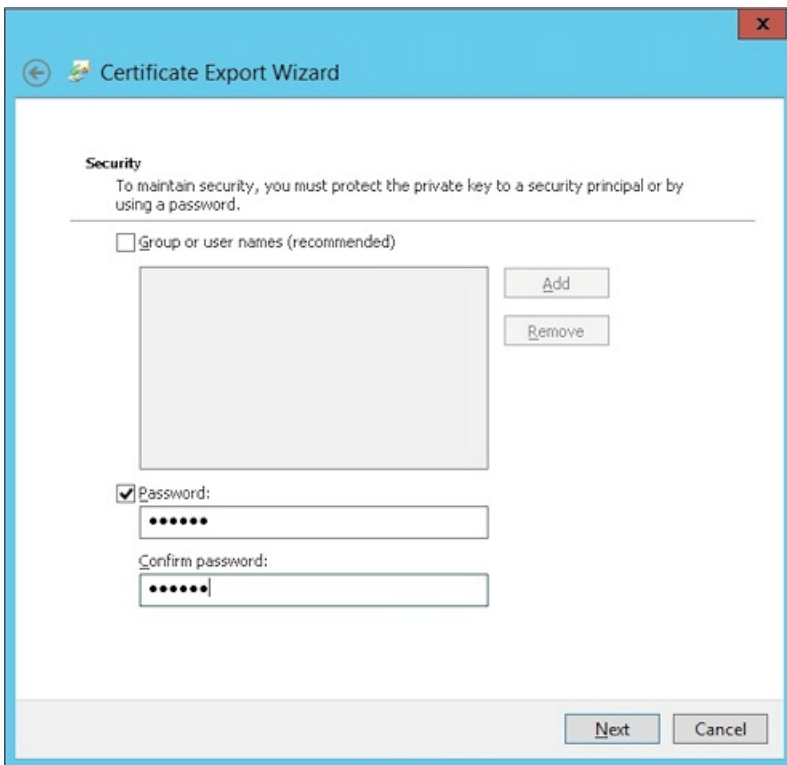
8. 单击是，导出私钥。



9. 选中如果可能，则包括证书路径中的所有证书和导出所有扩展属性复选框。



10. 设置要在将此证书上载到 XenMobile 中时使用的密码。



11. 将证书保存到您的硬盘驱动器。

将证书上载到 XenMobile

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

2. 依次单击证书和导入。

3. 输入以下参数：

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

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import	<input type="text" value="Keystore"/>
Keystore type	<input type="text" value="PKCS#12"/>
Use as	<input type="text" value="Server"/>
Keystore file*	<input type="text"/> <input type="button" value="Browse"/>
Password*	<input type="password"/>
Description	<input type="text"/>

4. 单击导入。

5. 验证是否已正确安装证书。证书应显示为用户证书。

为基于证书的身份验证创建 PKI 实体

1. 在设置中，转至更多 > 证书管理 > PKI 实体。

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

3. 输入以下参数：

- **名称**：键入任意名称
- **Web 注册服务根 URL**：https://RootCA-URL/certsrv/
请务必在 URL 路径结尾添加一个斜杠 (/)。
- **certnew.cer 页面名称**：certnew.cer (默认值)
- **certfnsh.asp**：certfnsh.asp (默认值)
- **身份验证类型**：客户端证书
- **SSL 客户端证书**：选择要用于颁发 XenMobile 客户端证书的用户证书。

Microsoft Certificate Services Entity 1 General 2 Templates 3 HTTP Parameters 4 CA Certificates	Microsoft Certificate Services Entity: General Information	
	Name*	test
	Web enrollment service root URL*	https://10.10.10.10/certsrv/
	certnew.cer page name*	certnew.cer
	certfnsh.asp*	certfnsh.asp
Authentication type	Client certificate	
SSL client certificate	Select an option	
	<input type="button" value="Import SSL certificate"/>	

4. 在模板下方，添加配置 Microsoft 证书时创建的模板。请勿添加空格。

Microsoft Certificate Services Entity 1 General 2 Templates 3 HTTP Parameters 4 CA Certificates	Microsoft Certificate Services Entity: Templates					
	Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.					
	Templates					
	<table border="1"> <thead> <tr> <th>Templates*</th> <th></th> </tr> </thead> <tbody> <tr> <td>XMTemplate</td> <td><input type="button" value="Add"/></td> </tr> </tbody> </table>	Templates*		XMTemplate	<input type="button" value="Add"/>	
	Templates*					
XMTemplate	<input type="button" value="Add"/>					

5. 跳过“HTTP 参数”，然后单击 **CA 证书**。

6. 选择与您的环境对应的根 CA 名称。此根 CA 属于从 XenMobile 客户端证书中导入的链的一部分。

Microsoft Certificate Services Entity 1 General 2 Templates 3 HTTP Parameters 4 CA Certificates	Microsoft Certificate Services Entity: CA Certificates													
	Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.													
	<table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Name</th> <th>Serial number</th> <th>Valid from</th> <th>Valid to</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>training-AD-CA</td> <td>145-00000000000000000000000000000000</td> <td>02/22/2013</td> <td>02/22/2023</td> </tr> </tbody> </table>				<input type="checkbox"/>	Name	Serial number	Valid from	Valid to	<input checked="" type="checkbox"/>	training-AD-CA	145-00000000000000000000000000000000	02/22/2013	02/22/2023
	<input type="checkbox"/>	Name	Serial number	Valid from	Valid to									
	<input checked="" type="checkbox"/>	training-AD-CA	145-00000000000000000000000000000000	02/22/2013	02/22/2023									

7. 单击保存。

配置凭据提供程序

1. 在设置中，转至更多 > 证书管理 > 凭据提供程序。

2. 单击添加。

3. 在常规下方，输入以下参数：

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

Credential Providers	Credential Providers: General Information
1 General	You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.
2 Certificate Signing Request	<p>Name* <input type="text" value="XenMobile_PKI"/></p> <p>Description <input type="text" value="XenMobile PKI Configuration"/></p> <p>Issuing entity <input type="text" value="MS PKI"/></p> <p>Issuing method <input type="text" value="SIGN"/></p> <p>Templates <input type="text" value="XMTemplate"/></p>
3 Distribution	
4 Revocation XenMobile	
5 Revocation PKI	
6 Renewal	

4. 单击证书签名请求，然后输入以下参数：

- **密钥算法**：RSA
- **密钥大小**：2048
- **签名算法**：SHA1withRSA
- **使用者名称**：cn=\$user.username

对于使用者备用名称，请单击添加，然后输入以下参数：

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

Credential Providers	Credential Providers: Certificate Signing Request						
1 General	Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.						
2 Certificate Signing Request	<p>Key algorithm <input type="text" value="RSA"/></p> <p>Key size* <input type="text" value="2048"/></p> <p>Signature algorithm <input type="text" value="SHA1withRSA"/></p> <p>Subject name* <input type="text" value="cn=\$user.username"/></p> <p>Subject alternative names</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Value*</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>User Principal name</td> <td>\$user.userprincipalname</td> <td><input type="button" value="Add"/></td> </tr> </tbody> </table>	Type	Value*	Add	User Principal name	\$user.userprincipalname	<input type="button" value="Add"/>
Type	Value*	Add					
User Principal name	\$user.userprincipalname	<input type="button" value="Add"/>					
3 Distribution							
4 Revocation XenMobile							
5 Revocation PKI							
6 Renewal							

5. 单击分发并输入以下参数：

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

Credential Providers	Credential Providers: Distribution
1 General	Issuing CA certificate: <input type="text" value="CN=training-AD-CA, Serial: [redacted]"/>
2 Certificate Signing Request	Select distribution mode: <ul style="list-style-type: none"> <input checked="" type="radio"/> Prefer centralized: Server-side key generation <input type="radio"/> Prefer distributed: Device-side key generation <input type="radio"/> Only distributed: Device-side key generation
3 Distribution	
4 Revocation XenMobile	

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

7. 单击续订。

8. 对于在证书过期时续订，请选择开。

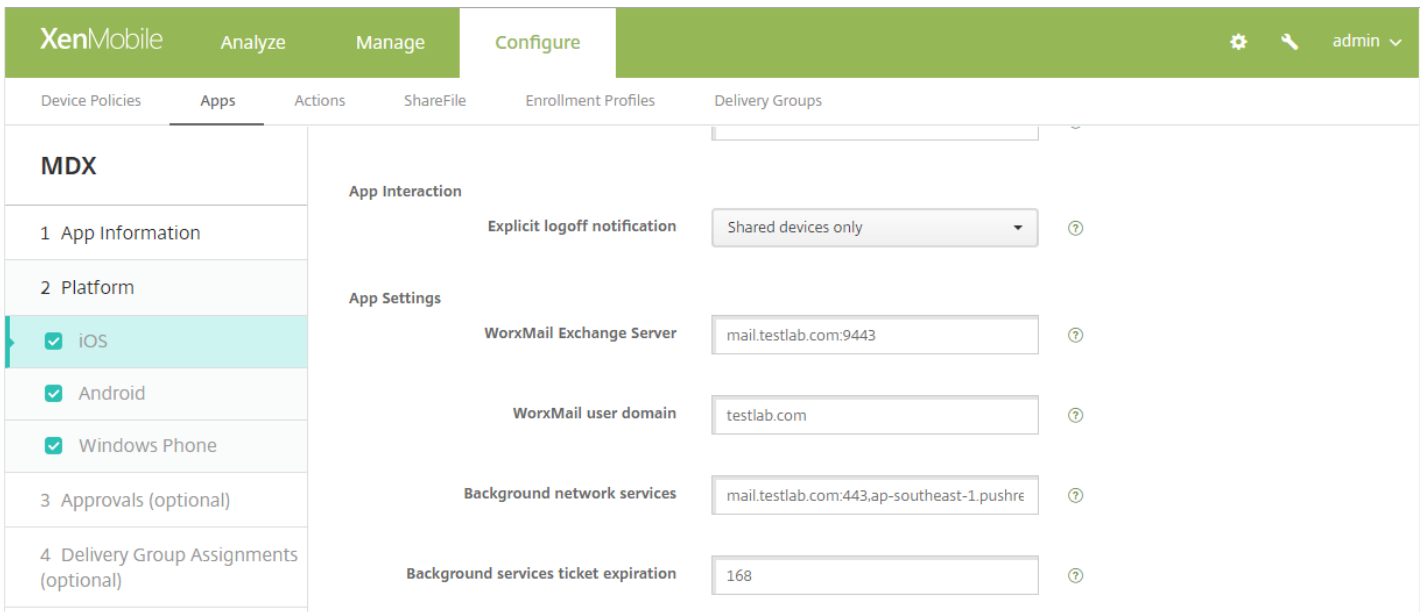
9. 让所有其他设置保留为默认设置，或者根据需要进行更改。

Credential Providers	Credential Providers: Renewal
1 General	Renew certificates when they expire: <input checked="" type="checkbox"/>
2 Certificate Signing Request	Renew when the certificate comes within*: <input type="text" value="30"/> days of expiration
3 Distribution	<input type="checkbox"/> Do not renew certificates that have already expired
4 Revocation XenMobile	Send notification: <input type="checkbox"/>
5 Revocation PKI	Notify when the certificate nears expiration: <input type="checkbox"/>
6 Renewal	

10. 单击保存。

将 Secure Mail 配置为使用基于证书的身份验证

将 Secure Mail 添加到 XenMobile 时，请务必在应用程序设置下方配置 Exchange 设置。



在 XenMobile 中配置 NetScaler 证书交付

1. 登录到 XenMobile 控制台并单击右上角的齿轮图标。此时将显示设置屏幕。
2. 在服务器下方，单击 **NetScaler Gateway**。
3. 如果尚未添加 NetScaler Gateway，请单击添加并指定以下设置：
 - 外部 URL：https://YourNetScalerGatewayURL
 - 登录类型：证书
 - 需要密码：关
 - 设为默认值：开
4. 对于向用户提供用于身份验证的证书，请选择开。

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway

NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication

Deliver user certificate for authentication ?

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs
--------------------------	------	---------	--------------	------------	--------------------

5. 对于凭据提供程序，请选择一个提供程序，然后单击保存。

6. 如果要使用用户证书中的 sAMAccount 属性作为用户主体名称 (UPN) 的备用名称，请按如下所示在 XenMobile 中配置 LDAP 连接器：转至设置 > LDAP，选择目录并单击编辑，然后在用户搜索依据中选择 sAMAccountName。

XenMobile Analyze Manage Configure admin

User base DN* ?

Group base DN* ?

User ID*

Password*

Domain alias*

XenMobile Lockout Limit ?

XenMobile Lockout Time ?

Global Catalog TCP Port ?

Global Catalog Root Context ?

User search by

Use secure connection

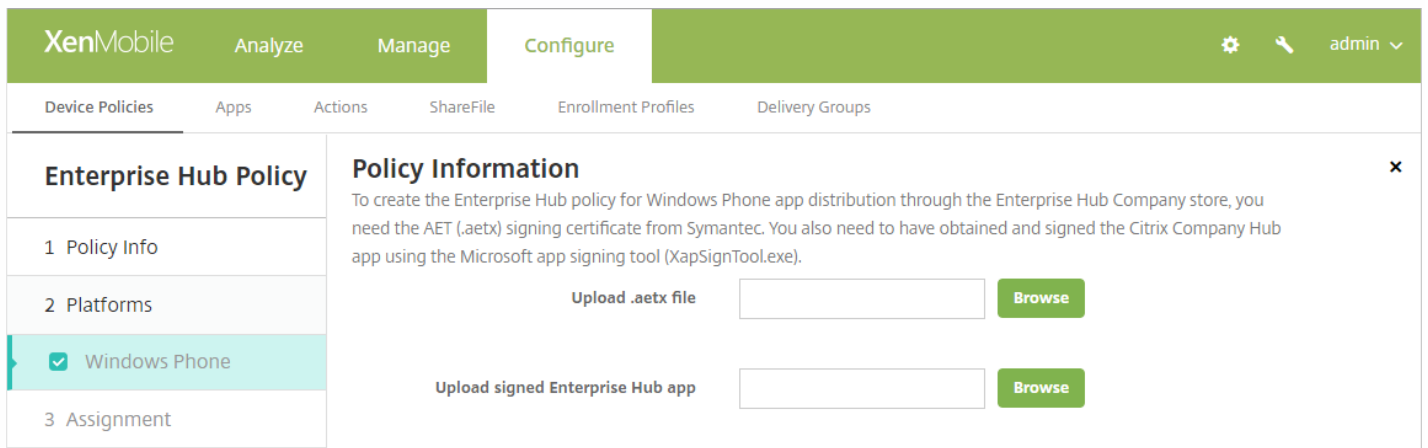
为 Windows Phone 创建企业中心策略

对于 Windows Phone 设备，必须创建企业中心设备策略才能交付 AETX 文件和 Secure Hub 客户端。

注意

请确保 AETX 和 Secure Hub 文件都使用证书提供程序提供的相同企业证书以及来自 Windows 应用商店开发人员帐户的相同发布者 ID。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。
2. 单击**添加**，然后在**更多 > XenMobile Agent** 下方单击**企业中心**。
3. 命名该策略后，请务必为企业中心选择正确的 .AETX 文件和签名 Secure Hub 应用程序。



The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Enterprise Hub Policy' and contains a 'Policy Information' section. This section provides instructions: 'To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe)'. Below the text are two upload fields: 'Upload .aetx file' and 'Upload signed Enterprise Hub app', each with a 'Browse' button. On the left, a sidebar shows a list of policy steps: '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Windows Phone' (which is currently selected and highlighted).

4. 将该策略分配给交付组并保存。

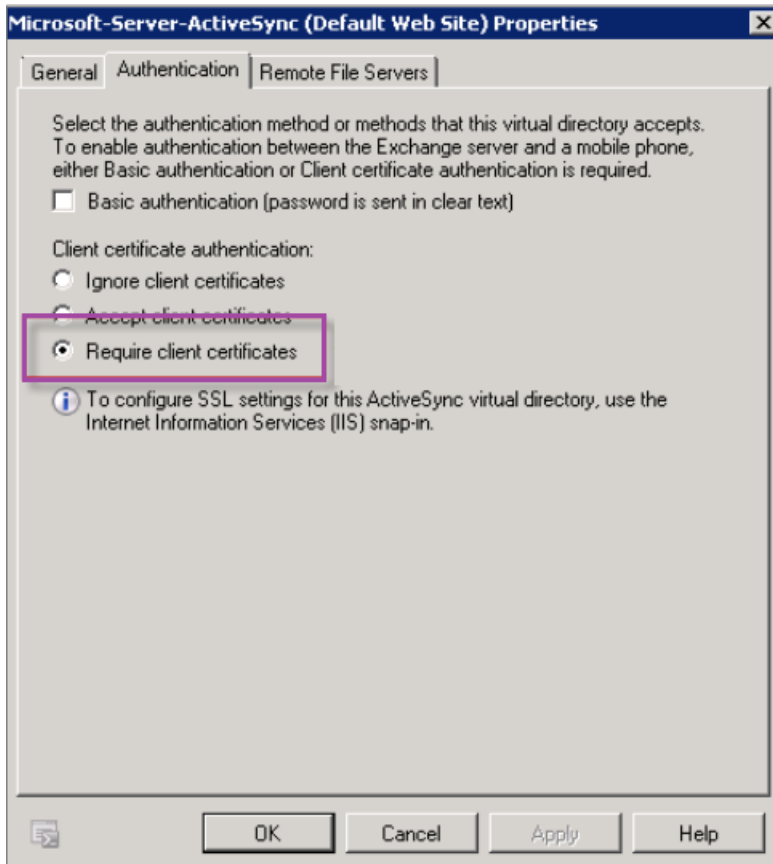
客户端证书配置故障排除

成功配置前述配置及 NetScaler Gateway 配置后，用户 workflow 如下：

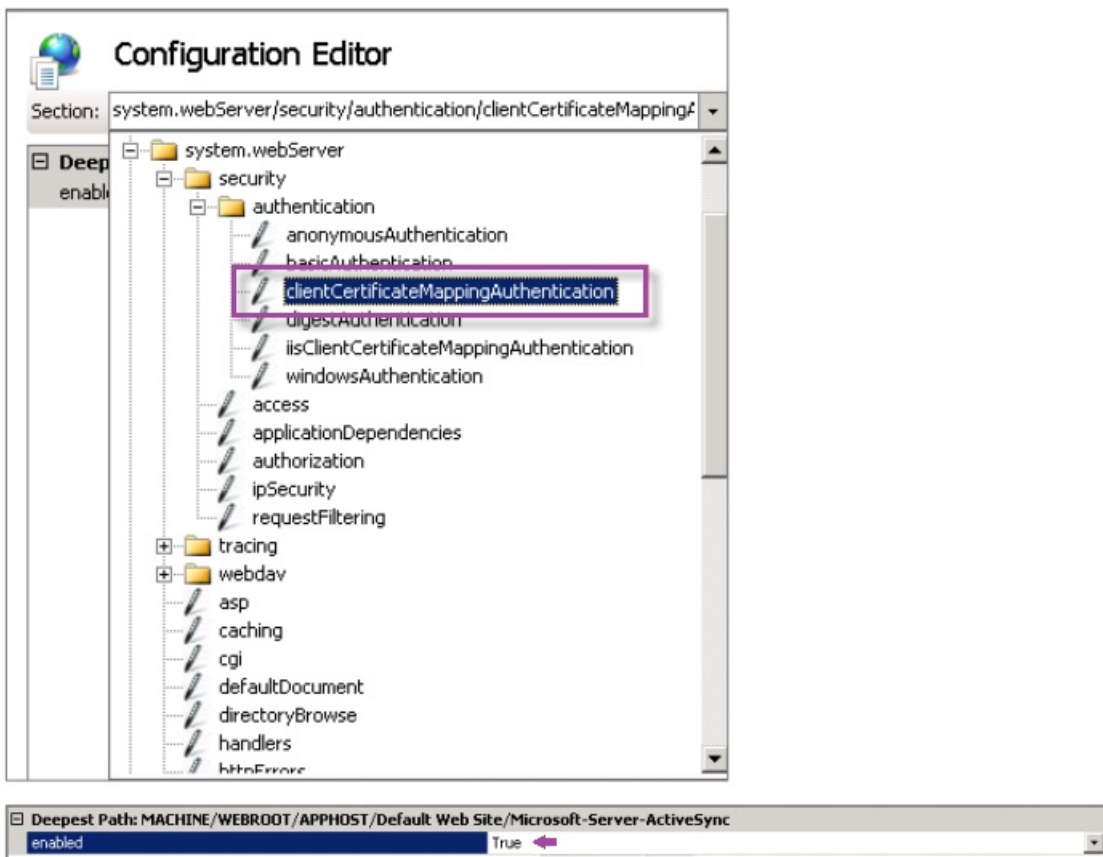
1. 用户注册其移动设备。
2. XenMobile 提示用户创建 Citrix PIN。
3. 随后用户被重定向到 XenMobile Store。
4. 用户启动 Secure Mail 时，XenMobile 将不提示其提供用户凭据以配置其邮箱。相反，Secure Mail 将从 Secure Hub 请求客户端证书，并将其提交给 Microsoft Exchange Server 以进行身份验证。如果 XenMobile 在用户启动 Secure Mail 时提示用户提供凭据，请检查您的配置。

如果用户能够下载并安装 Secure Mail，但邮箱配置过程中 Secure Mail 无法完成配置：

1. 如果 Microsoft Exchange Server ActiveSync 使用专用 SSL 服务器证书来确保通信安全，请确认是否已在移动设备上安装根证书/中间证书。
2. 验证为 ActiveSync 选择的身份验证类型是否为 **Require client certificates**（需要客户端证书）。



3. 在 Microsoft Exchange Server 上，检查 **Microsoft-Server-ActiveSync** 站点是否已启用客户端证书映射身份验证（默认禁用）。该选项位于 **Configuration Editor (配置编辑器) > Security (安全性) > Authentication (身份验证)** 下方。



注意：选择 **True** 后，请务必单击 **Apply**（应用）以使更改生效。

4. 在 XenMobile 控制台中检查 NetScaler Gateway 设置：确保向用户提供用于身份验证的证书设置为开，并且凭据提供程序选择了正确的配置文件，如上文“在 XenMobile 中配置 NetScaler 证书交付”中所述。

要确定是否已向移动设备提供客户端证书，请执行以下操作：

1. 在 XenMobile 控制台中，转至管理 > 设备，然后选择设备。
2. 单击编辑或显示更多。
3. 转至交付组部分，并搜索以下条目：

NetScaler Gateway Credentials : Requested credential, CertId=

要验证是否已启用客户端证书协商，请执行以下操作：

1. 运行以下 netsh 命令以显示 IIS Web 站点上绑定的 SSL 证书配置：

```
netsh http show sslcert
```

2. 如果 **Negotiate Client Certificate**（协商客户端证书）的值为 **Disabled**（已禁用），请运行以下命令将其启用：

```
netsh http delete sslcert ipport=0.0.0.0:443
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name  
verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
clientcertnegotiation=Enable
```

例如：

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid=  
{4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName  
verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
clientcertnegotiation=Enable
```

如果无法通过 XenMobile 向 Windows Phone 8.1 设备提供根证书/中间证书，请执行以下操作：

- 通过电子邮件将根证书/中间证书 (.cer) 文件发送到 Windows Phone 8.1 设备并直接安装。

如果无法在 Windows Phone 8.1 上成功安装 Secure Mail，请执行以下操作：

- 验证应用程序注册令牌 (AETX) 文件是否已使用企业中心设备策略通过 XenMobile 提供。
- 验证创建应用程序注册令牌时使用的证书提供程序提供的企业证书是否与用于打包 Secure Mail 并对 Secure Hub 应用程序进行签名的企业证书相同。
- 验证是否正在使用相同的发布者 ID 签名并打包 Secure Hub、Secure Mail 和应用程序注册令牌。

PKI 实体

Feb 27, 2017

XenMobile 公钥基础设施 (PKI) 实体配置代表执行实际 PKI 操作 (颁发、吊销和状态信息) 的组件。这些组件可能是 XenMobile 的内部组件 (在此情况下称为任意实体) 或者 XenMobile 外部组件 (如果组件是企业基础结构的一部分)。

XenMobile 支持以下类型的 PKI 实体：

- 任意证书颁发机构 (CA)
- 通用 PKI (GPKI)
- Microsoft 证书服务

XenMobile 支持以下 CA 服务器：

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

无论何种类型，每个 PKI 实体均拥有下列功能的子集：

- 签名：基于证书签名请求 (CSR) 颁发新证书。
- 提取：恢复现有证书和密钥对。
- 吊销：吊销客户端证书。

关于 CA 证书

配置 PKI 实体时，必须向 XenMobile 指明哪个 CA 证书将成为该实体所颁发 (或从该实体恢复) 的证书的签署者。同一 PKI 实体可以返回任意多个不同 CA 签名 (提取或新签名) 的证书。必须在 PKI 实体配置时提供其中每个 CA 的证书。为此，需要将证书上载到 XenMobile，然后在 PKI 实体中引用这些证书。对于任意 CA，证书是隐式签名 CA 证书，但对于外部实体，必须手动指定证书。

通用 PKI (GPKI) 协议是 XenMobile 专有协议，在 SOAP Web 服务层之上运行，用于实现与各种 PKI 解决方案的统一交互。

GPKI 协议定义以下三个基本 PKI 操作：

- 签名：适配器可以接收 CSR，将其传输到 PKI 并返回新签名的证书。
- 提取：适配器能够从 PKI 检索 (恢复) 现有证书和密钥对 (取决于输入参数)。
- 吊销：适配器能够让 PKI 吊销给定证书。

GPKI 协议的接收端是 GPKI 适配器。该适配器将基本操作转换为其构建所针对的特定类型的 PKI。换言之，RSA 有一个 GPKI 适配器，EnTrust 有另一个适配器，依此类推。

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

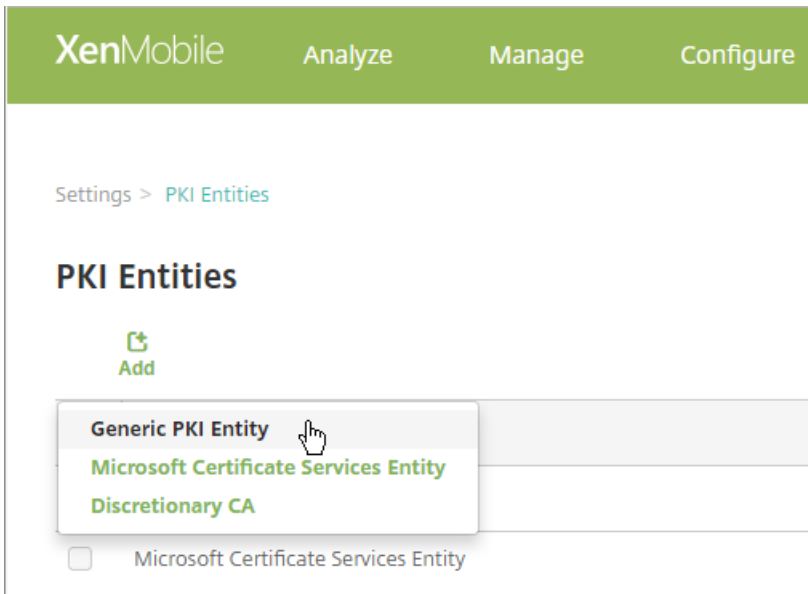
可以选择是否支持适配器中的各个 PKI 操作。如果适配器支持某个给定操作，可以称之为拥有相应功能 (签名、提取或吊销)。这些功能中的每一项均可与一组用户参数相关联。

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

1. 在 XenMobile 控制台中，单击设置 > PKI 实体。

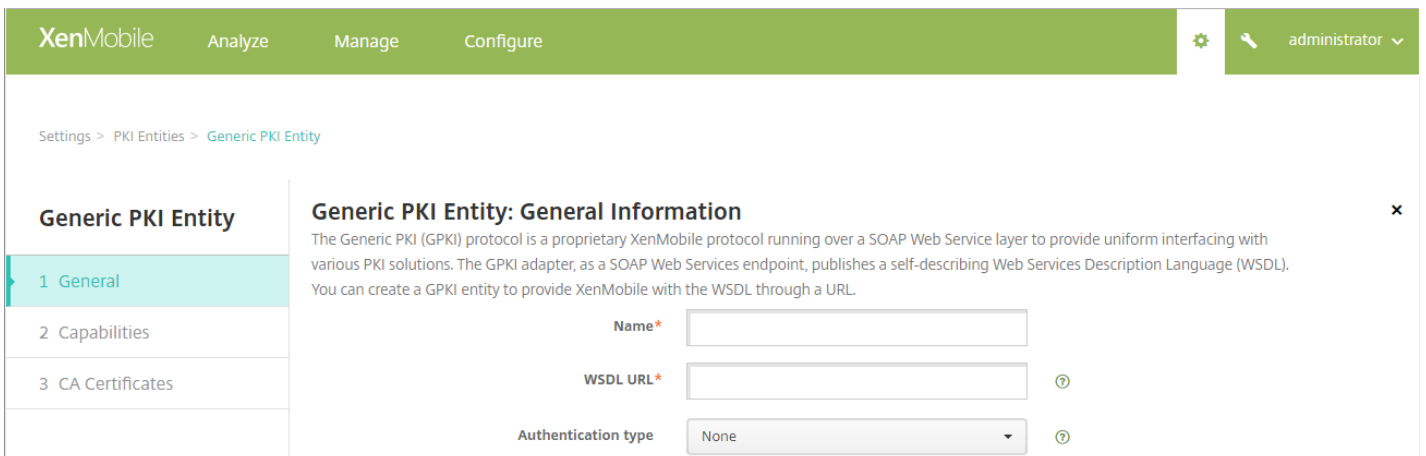
2. 在 PKI 实体页面上，单击添加。

此时将显示一个 PKI 实体类型菜单。



3. 单击通用 PKI 实体。

此时将显示“通用 PKI 实体: 常规信息”页面。



4. 在通用 PKI 实体: 常规信息页面上，执行以下操作：

- 名称：键入 PKI 实体的描述性名称。

- **WSDL URL** : 键入描述适配器的 WSDL 的位置。
- **身份验证类型** : 单击要使用的身份验证方法。
- 无
- **HTTP 基本认证** : 提供连接到适配器所需的用户名和密码。
- **客户端证书** : 选择正确的 SSL 客户端证书。

5. 单击下一步。

此时将显示通用 PKI 实体: 适配器功能页面。

6. 在通用 PKI 实体: 适配器功能页面上, 检查与适配器关联的功能和参数, 然后单击下一步。

此时将显示通用 PKI 实体: 颁发 CA 证书页面。

7. 在通用 PKI 实体: 颁发 CA 证书页面上, 选择要用于此实体的证书。

注意 : 尽管实体可能会返回不同 CA 签发的证书, 但通过给定证书提供商获取的所有证书必须由同一个 CA 颁发。相应地, 在配置凭据提供程序设置时, 在分发页面上, 选择在此处配置的证书之一。

8. 单击保存。

实体将显示在 PKI 实体表格中。

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

要在 XenMobile 中创建 Microsoft CA PKI 实体, 必须指定证书服务 Web 界面的基本 URL。如果选择此项, 则使用 SSL 客户端身份验证保护 XenMobile 与证书服务 Web 界面之间的连接。

1. 在 XenMobile 控制台中, 单击控制台右上角的齿轮图标, 然后单击 **PKI 实体**。

2. 在 **PKI 实体** 页面上, 单击**添加**。

此时将显示一个 PKI 实体类型菜单。

3. 单击 **Microsoft 证书服务实体**。

此时将显示 **Microsoft 证书服务实体: 常规信息** 页面。

4. 在 **Microsoft 证书服务实体: 常规信息** 页面上, 配置以下设置 :

- **名称** : 为新建实体键入一个名称, 此名称以后将用于指代该实体。实体名称必须唯一。
- **Web 注册服务根 URL** : 键入 Microsoft CA Web 注册服务的基本 URL, 例如, <https://192.0.2.13/certsrv/>。该 URL 可能会使用纯 HTTP 或 HTTP-over-SSL。
- **certnew.cer 页面名称** : certnew.cer 页面的名称。若非因为某些原因重命名了此页面, 请使用默认名称。
- **certfnsh.asp** : certfnsh.asp 页面的名称。若非因为某些原因重命名了此页面, 请使用默认名称。
- **身份验证类型** : 选择要使用的身份验证方法。
 - 无
 - **HTTP 基本** : 键入连接所需的用户名和密码。

- **客户端证书**：选择正确的 SSL 客户端证书。

5. 单击**测试连接**以确保服务器可以访问。如果不可访问，则会显示一条消息，指出连接失败。请检查配置设置。

6. 单击**下一步**。

此时将显示 **Microsoft 证书服务实体: 模板** 页面。在此页面上，指定 Microsoft CA 所支持模板的内部名称。创建凭据提供程序时，从此处定义的列表中选择模板。使用此实体的每个凭据提供程序仅使用一个此类模板。

有关 Microsoft 证书服务模板的要求，请参阅您的 Microsoft Server 版本对应的 Microsoft 文档。除了**证书**中所述的证书格式要求外，XenMobile 对其分发的证书并无其他要求。

7. 在 **Microsoft 证书服务实体: 模板** 页面上，单击**添加**，键入模板的名称，然后单击**保存**。为要添加的每个模板重复执行此步骤。

8. 单击**下一步**。

此时将显示 **Microsoft 证书服务实体: HTTP 参数** 页面。在此页面上，您可以指定 XenMobile 应在 Microsoft Web 注册界面的 HTTP 请求中引入的自定义参数。仅当您已在 CA 上自定义脚本时，此操作才有用。

9. 在 **Microsoft 证书服务实体: HTTP 参数** 页面上，单击**添加**，键入要添加的 HTTP 参数的名称和值，然后单击**下一步**。

此时将显示 **Microsoft 证书服务实体: CA 证书** 页面。在此页面上，您需要将系统通过该实体获取的证书的签署者告诉 XenMobile。续订 CA 证书时，在 XenMobile 中更新此证书，随之更改将以透明方式应用于实体。

10. 在 **Microsoft 证书服务实体: CA 证书** 页面上，选择要用于此实体的证书。

11. 单击**保存**。

实体将显示在 PKI 实体表格中。

XenMobile 支持对第三方证书颁发机构使用证书吊销列表 (CRL)。如果您配置了 Microsoft CA，XenMobile 将使用 NetScaler 管理吊销。配置基于客户端证书的身份验证时，请考虑是否需要配置 NetScaler 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh** (启用 CRL 自动刷新)。此步骤可确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证；XenMobile 将重新颁发新证书，因为 XenMobile 在某个证书被吊销的情况下不限制用户生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

向 XenMobile 提供 CA 证书及关联的私钥时，将创建任意 CA。XenMobile 将根据您指定的参数，在内部处理证书颁发、吊销和状态信息。

配置任意 CA 时，可以选择为此 CA 激活联机证书状态协议 (OCSP) 支持。当且仅当启用 OCSP 支持时，CA 会向 CA 颁发的证书添加 id-pe-authorityInfoAccess 扩展，并在后面的位置指向 XenMobile 内部 OCSP 响应者。

`https://server/instance/ocsp`

配置 OCSP 服务时，必须为相关任意实体指定 OCSP 签名证书。可以将 CA 证书本身用作签署者。如果要避免 CA 私钥的不必要暴露 (建议避免)，必须创建一个由 CA 证书签名并包含 id-kp-OCSPSigning extendedKeyUsage 扩展的委派 OCSP 签名证书。

XenMobile OCSP Responder Service 支持在请求中使用基本 OCSP 响应及以下散列算法：

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

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

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标，然后单击**更多 > PKI 实体**。

2. 在 **PKI 实体** 页面上，单击**添加**。

此时将显示一个 PKI 实体类型菜单。

3. 单击**任意 CA**。

此时将显示**任意 CA: 常规信息**页面。

4. 在**任意 CA: 常规信息**页面上，执行以下操作：

- **名称**：键入任意 CA 的描述性名称。
- **用于对证书请求进行签名的 CA 证书**：单击任意 CA 用于为证书请求签名的证书。此证书列表使用您通过**配置 > 设置 > 证书**上载到 XenMobile 的私钥从 CA 证书生成。

5. 单击**下一步**。

此时将显示 **Discretionary CA: Parameters** (任意 CA: 参数) 页面。

6. 在 **Discretionary CA: Parameters** (任意 CA: 参数) 页面上，执行以下操作：

- **序列号生成器**：任意 CA 为其颁发的证书生成序列号。从此列表中，单击**按顺序**或**不按顺序**，以确定生成此序列号的方式。
- **下一个序列号**：键入一个值，用于确定颁发的下一个号码。
- **证书有效期**：键入证书有效的天数。
- **密钥用法**：通过将相应的密钥设置为**开**，标识任意 CA 所颁发证书的目的。设置后，CA 仅限于为这些目的颁发证书。
- **扩展密钥用法**：要添加其他参数，请单击**添加**，键入密钥名称，然后单击**保存**。

7. 单击**下一步**。

此时将显示 **Discretionary CA: Distribution** (任意 CA: 分发) 页面。

8. 在 **Discretionary CA: Distribution** (任意 CA: 分发) 页面上，选择分发模式：

- **集中式: 服务器端密钥生成**。Citrix 建议使用集中选项。在服务器上生成并存储私钥，然后分发到用户设备。
- **分布式: 设备端密钥生成**。私钥在用户设备上生成。分布式模式使用 SCEP 并需要采用 keyUsage keyEncryption 的 RA 加密证书和采用 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可以同时用于加密和签名。

9. 单击**下一步**。

此时将显示 **Discretionary CA: Online Certificate Status Protocol (OCSP)** (任意 CA: 在线证书状态协议(OCSP)) 页面。

在 **Discretionary CA: Online Certificate Status Protocol (OCSP)** (任意 CA: 在线证书状态协议(OCSP)) 页面上，执行以下操作：

- 如果要向此 CA 签署的证书添加 AuthorityInfoAccess (RFC2459) 扩展，请将为此 **CA 启用 OCSP 支持** 设置为开。此扩展指向位于 <https://server/instance/ocsp> 的 CA OCSP 响应者。
- 如果启用了 OCSP 支持，请选择 OSCP 签名 CA 证书。此证书列表使用您上载到 XenMobile 的 CA 证书生成。

10. 单击**保存**。

任意 CA 将显示在 PKI 实体表格中。

凭据提供程序

Feb 27, 2017

凭据提供程序是在 XenMobile 系统的各个部分中使用的实际证书配置。它们定义证书的来源、参数和生命周期，无论这些证书是设备配置的一部分还是独立的配置，都将按原样推送到设备。

设备注册约束证书生命周期。也就是说，XenMobile 在注册前不颁发证书，尽管 XenMobile 可能会在注册的过程中颁发某些证书。此外，在某个注册环境下从内部 PKI 颁发的证书会在注册被吊销时吊销。管理关系终止后，不保留任何有效证书。

一个凭据提供程序配置可用于多个位置，从而达到通过一个配置同时控制任意多个证书的效果。这时，其唯一性在于部署资源和部署。例如，如果凭据提供程序 P 作为配置 C 的一部分部署到设备 D，则 P 的颁发设置将决定部署到 D 的证书。同样，在更新 C 时将应用 D 的续订设置，在删除 C 时或吊销 D 时应用 D 的吊销设置。

基于此，XenMobile 中的凭据提供程序配置执行以下操作：

- 确定证书的来源。
- 确定获取证书的方法：签发新证书还是提取（恢复）现有证书和密钥对。
- 确定用于颁发或恢复的参数。例如，密钥大小、密钥算法、标识名、证书扩展名等证书签名请求 (CSR) 参数。
- 确定将证书交付给设备的方式。
- 决定吊销条件。尽管在管理关系终止后 XenMobile 中的所有证书都将被吊销，但该配置可以指定在更早时间吊销，例如在删除关联设备配置时吊销。此外，在某些情况下，XenMobile 中关联证书的吊销可能会发送给后端公钥基础结构 (PKI)；也就是说，XenMobile 中关联证书的吊销可能导致其在 PKI 上也随之吊销。
- 决定续订设置。通过指定凭据提供程序获取的证书可以在即将过期时自动续订，或者采用与之不同的方式，在接近过期时由系统发送通知。

各种配置选项的可用程度主要取决于为凭据提供程序选择的 PKI 实体的类型和颁发方法。

可以采用两种途径获取证书（称为颁发方法）：

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

凭据提供程序使用签名或提取颁发方法。所选方法会影响可用配置选项。具体而言，仅当颁发方法为签名时，才可以使用 CSR 配置和分散交付。提取的证书始终作为 PKCS#12 发送给设备，相当于签名方法的集中交付模式。

XenMobile 中可用的证书交付模式共有两种：集中和分散。分布式模式使用简单证书注册协议 (SCEP)，并且只有在客户端支持该协议时方可使用（仅限 iOS）。在某些情况下，必须采用分布式模式。

对于支持分散式 (SCEP 辅助) 交付的凭据提供程序，需要特殊的配置步骤：设置注册机构 (RA) 证书。需要 RA 证书是因为，使用 SCEP 协议时，XenMobile 充当实际证书颁发机构的委派者（注册者）。XenMobile 必须向客户端证实自己有权执行此类操作。通过向 XenMobile 上载上述证书，可以建立该机构。

需要两种不同的证书角色（尽管同一证书即可满足这两项要求）：RA 签名和 RA 加密。这些角色的限制如下：

- RA 签名证书必须拥有 X.509 密钥用法数字签名。
- RA 加密证书必须拥有 X.509 密钥用法密钥加密。

要配置凭据提供程序的 RA 证书，必须首先将证书上载到 XenMobile，然后在凭据提供程序中链接到这些证书。

仅当凭据提供程序为证书角色配置了证书时，才可将凭据提供程序视为支持分散式交付。可以将每个凭据提供程序配置为首选集中式模式、首选分布式模式或要求分布式模式。实际结果取决于具体环境：如果环境不支持分布式模式，但是凭据提供程序要求使用该模式，部署将失败。同样地，如果环境要求使用分布式模式，但凭据提供程序不支持该模式，部署也将失败。在所有其他情况下，将会应用首选设置。

下面显示了 SCEP 在整个 XenMobile 的分布：

上下文	支持 SCEP	需要 SCEP
iOS 配置文件服务	是	是
iOS 移动设备管理注册	是	否
iOS 配置文件	是	否
SHTP 注册	否	否
SHTP 配置	否	否
Windows Phone 和 Windows Tablet 注册	否	否
Windows Phone 和 Windows Tablet 配置	否，WiFi 设备策略除外， Windows Phone 8.1 和最新版本的 Windows 10 支持该策略	否

有三种类型的吊销。

- **内部吊销。**内部吊销影响由 XenMobile 维护的证书状态。在 XenMobile 评估收到的证书时，或者 XenMobile 必须提供某些证书的 OCSP 状态信息时，将考虑此状态。凭据提供程序配置决定在各种条件下此状态受到的影响。例如，凭据提供程序可以指定：将通过证书提供商获取的证书从设备中删除后，将这些证书标记为已吊销。
- **外部传播的吊销。**又称“吊销 XenMobile”，这种类型的吊销适用于从外部 PKI 获取的证书。在凭据提供程序配置定义的情况下，当证书由 XenMobile 在内部吊销时也会同时在 PKI 上吊销。用于执行吊销的调用需要使用支持吊销的通用 PKI (GPKI) 实体。
- **外部引起的吊销。**又称“吊销 PKI”，这种类型的吊销适用于从外部 PKI 获取的证书。每次 XenMobile 评估指定证书的状态时，XenMobile 都将向 PKI 查询该状态。如果证书已吊销，XenMobile 将在内部吊销该证书。此机制使用 OCSP 协议。

这三种类型并不互斥，而是可以一起应用：外部吊销或独立查询结果导致内部吊销，内部吊销进而潜在影响外部吊销。

证书续订由吊销现有证书和颁发另一个证书两个过程组成。

请注意，XenMobile 将首先尝试获取新证书，然后再吊销之前的证书，以避免在颁发失败时造成服务中断。如果采用分散式（支持 SCEP）交付，仅当证书成功安装到设备后再进行吊销，否则，将在新证书发送给设备之前进行吊销，无论新证书是否

安装成功。

配置吊销时，需要指定特定的持续时间（天）。如果设备已连接，服务器将验证证书的“不晚于”日期是否晚于当前日期减去指定的持续时间。如果晚于两者之差，则尝试续订。

凭据提供程序的配置方式有多种，主要取决于为其选择的颁发实体和颁发方法。可以将使用内部实体（如任意实体）和使用外部实体（如 Microsoft CA 或 GPKI）的凭据提供程序区分开。任意实体的颁发方法始终为签名。这意味着，在执行每个颁发操作时，XenMobile 都将使用为该实体选择的 CA 证书给新密钥对签名。该密钥对是在设备上生成还是在服务器上生成取决于所选的分发方法。

1. 在 XenMobile Web 控制台中，单击控制台右上角的齿轮图标，然后单击**更多 > 凭据提供程序**。
2. 在**凭据提供程序**页面上，单击**添加**。

此时将显示**凭据提供程序: 常规信息**页面。

3. 在**凭据提供程序: 常规信息**页面上，执行以下操作：

- **名称**：键入新提供程序配置的唯一名称。此名称之后将用于在 XenMobile 控制台的其他部分引用该配置。
- **说明**：凭据提供程序的说明。尽管此字段为可选字段，但说明在以后可帮助您记住此凭据提供程序的详细信息。
- **颁发实体**：单击凭据颁发实体。
- **颁发方法**：单击**签名**或**提取**以选择系统用于从已配置的实体获取证书的方法。对于客户端证书身份验证，请使用**签名**。
- 如果模板列表可用，请为凭据提供程序选择模板。

4. 单击**下一步**。

注意：在**设置 > 更多 > PKI 实体**中添加 Microsoft 证书服务实体后，这些模板将变为可用。

此时将显示**凭据提供程序: 证书签名请求**页面。

5. 在**凭据提供程序: 证书签名请求**页面上，执行以下操作：

- **密钥算法**：单击用于获取新密钥对的密钥算法。可用值为 **RSA**、**DSA** 和 **ECDSA**。
- **密钥大小**：键入密钥对的大小，以位为单位。此字段为必填字段。
注意：允许的值取决于密钥类型；例如，DSA 密钥的最大大小为 1024 位。为避免错误的负值（取决于基础硬件或软件），XenMobile 不强制实施密钥大小。您应始终先在测试环境中测试凭据提供程序配置，然后在生产环境中激活这些配置。
- **签名算法**：单击用于新证书的值。值取决于密钥算法。
- **使用者名称**：键入新证书使用者的标识名 (DN)。例如：CN=\${user.username}, OU=\${user.department}, O=\${user.companyname}, C=\${user.c}\endquotation。此字段为必填字段。

例如，对于客户端证书身份验证，请使用以下设置：

密钥算法：RSA

密钥大小：2048

签名算法：SHA1withRSA

使用者名称：cn=\${user.username}

6. 要向使用者备用名称表格中添加新条目，请单击**添加**。选择备用名称的类型，然后在第二列中键入一个值。

对于客户端证书身份验证，请指定以下设置：

类型：用户主体名称

值：\$user.userprincipalname

注意：与使用者名称相同，可以在值字段中使用 XenMobile 宏。

7. 单击下一步。

将显示凭据提供程序：分发页面。

8. 在凭据提供程序：分发页面上，执行以下操作：

- 在颁发 CA 证书列表中，单击提供的 CA 证书。由于凭据提供程序使用任意 CA 实体，因此该凭据提供程序的 CA 证书将始终为在该实体上配置的 CA 证书；该证书在此显示是为了与使用外部实体的配置保持一致。
- 在选择分发模式中，单击以下生成和分发密钥方式中的一种：
 - 首选集中式：服务器端密钥生成。Citrix 建议采用此集中模式选项。它支持 XenMobile 支持的所有平台，并且在使用 NetScaler Gateway 身份验证时也需要使用此模式。在服务器上生成并存储私钥，然后分发到用户设备。
 - 首选分布式：设备端密钥生成。在用户设备上生成并存储私钥。此分布式模式使用 SCEP 并需要采用 keyUsage keyEncryption 的 RA 加密证书和采用 KeyUsage digitalSignature 的 RA 签名证书。同一个证书可以同时用于加密和签名。
 - 仅限分布式：设备端密钥生成。此选项与首选分布式：设备端密钥生成的工作方式相同，但是此选项是“仅限”而非“首选”，当设备端生成密钥失败或不可用时，没有其他选项可用。

如果选择首选分布式：设备端密钥生成或仅限分布式：设备端密钥生成，请单击 RA 签名证书和 RA 加密证书。同一个证书可用于这两个目的。此时将显示有关这些证书的新字段。

9. 单击下一步。

此时将显示凭据提供程序：吊销 XenMobile 页面。在此页面上，配置 XenMobile 在内部将通过此提供程序配置颁发的证书标记为吊销的条件。

12. 在凭据提供程序：吊销 XenMobile 页面上，执行以下操作：

- 在吊销已颁发的证书中，选择一个表明何时应吊销证书的选项。
- 如果希望 XenMobile 在吊销证书时发送通知，请将发送通知设置为开并选择通知模板。
- 如果要在从 XenMobile 吊销证书后也在 PKI 上吊销此证书，请将吊销 PKI 上的证书设置为开，并在实体列表中，单击某个模板。实体列表将显示具有吊销功能的所有可用 GPKI 实体。从 XenMobile 吊销证书后，吊销调用将发送给在实体列表中选择选择的 PKI。

13. 单击下一步。

此时将显示凭据提供程序：吊销 PKI 页面。请在此页面上指出吊销证书时应对 PKI 执行的操作。您还可以选择创建通知消息。

14. 在凭据提供程序：吊销 PKI 页面上，如果要从 PKI 吊销证书，请执行以下操作：

- 将启用外部吊销检查设置更改为开。此时将显示其他与吊销 PKI 相关的字段。
- 在 OCSP 响应者 CA 证书列表中，单击证书使用者的标识名 (DN)。注意：可以为 DN 字段值使用 XenMobile 宏。例如：
CN=\${user.username}, OU=\${user.department}, O=\${user.companyname}, C=\${user.c}\endquotation
- 在吊销证书时列表中，单击吊销证书时对 PKI 实体执行的以下操作之一：

不执行任何操作。

续订证书。

吊销和擦除设备。

- 如果希望 XenMobile 在吊销证书时发送通知，请将**发送通知**的值设置为开。

可以从两个通知选项中选择：

- 如果选择**选择通知模板**，则可以选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
- 如果选择**输入通知详细信息**，则可以自行编写通知消息。除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

15. 单击**下一步**。

此时将显示**凭据提供程序: 续订**页面。在此页面上，您可以配置 XenMobile 以使其执行以下操作：

- 续订证书、在证书完成续订时发送通知（续订时通知）并从操作中排除已过期的证书（后两项操作为可选操作）。
- 为即将过期的证书发送通知（续订前通知）。

16. 在**凭据提供程序: 续订**页面上，如果要在证书过期时进行续订，请执行以下操作：将**续订证书**设置为开。

此时将显示其他字段。

- 在**证书在此时间内提供时续订**字段中，键入应在过期前多少天续订证书。
- （可选）选择**不续订已过期的证书**。注意：在此情况下，“已过期”表示证书的“不晚于”日期在过去，不是指证书已经被吊销。内部吊销后，XenMobile 将不会续订证书。

17. 如果希望 XenMobile 在续订证书后发送通知，请将**发送通知**的值设置为开。可以从两个通知选项中选择：

- 如果选择**选择通知模板**，则可以选择预先写好的通知消息，且之后可以进行自定义。这些模板位于通知模板列表中。
- 如果选择**输入通知详细信息**，则可以自行编写通知消息。除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

18. 如果希望 XenMobile 在证书接近过期时发送通知，请将**证书即将过期时发送通知**设置为开。可以从两个通知选项中选择：

- 如果选择**选择通知模板**，则可以选择预先写好的通知消息，且之后可以进行自定义。这些模板位于**通知模板**列表中。
- 如果选择**输入通知详细信息**，则可以自行编写通知消息。除了提供收件人的电子邮件地址和消息，还可以设置发送通知的频率。

19. 在**证书在此时间内提供时通知**字段中，键入应在证书过期前多少天发送通知。

20. 单击**保存**。

凭据提供程序将添加到凭据提供程序表格中。

APNs 证书

Feb 27, 2017

要使用 XenMobile 注册和管理 iOS 设备，需要从 Apple 设置并创建 Apple 推送通知服务 (APNs) 证书。本节概述了用于请求 APNs 证书的以下基本步骤：

- 使用 Windows Server 2012 R2 或 Windows 2008 R2 Server 和 Microsoft Internet Information Server (IIS) 或 Mac 计算机生成证书签名请求 (CSR)。
- 要求 Citrix 为 CSR 签名。
- 从 Apple 请求 APNs 证书。
- 将证书导入到 XenMobile。

注意：

- 利用 Apple 的 APNs 证书可通过 Apple 推送网络启用移动设备管理。如果您无意或有意吊销了该证书，则无法管理自己的设备。
- 如果使用 iOS Developer Enterprise Program 创建 Mobile Device Manager 推送证书，则可能会因为将现有证书迁移到 Apple 推送证书门户而需要采取相应措施。

这些主题逐步概述了操作步骤，在本节中依次列出，如下所示：

步骤 1	在 IIS 上创建 CSR 在 Mac 上创建 CSR	使用 Windows Server 2012 R2 或 Windows 2008 R2 Server 和 Microsoft IIS 或在 Mac 计算机上生成 CSR。Citrix 建议采用这种方法。
步骤 2	为 CSR 签名	在 XenMobile APNs CSR Signing Web 站点 上将 CSR 提交给 Citrix（需要 MyCitrix ID）。Citrix 使用其移动设备管理签名证书给 CSR 签名并返回 .plist 格式的已签名文件。
步骤 3	将已签名 CSR 提交给 Apple	在 Apple 推送证书门户 上将已签名 CSR 提交给 Apple（需要 Apple ID），然后从 Apple 下载 APNs 证书。
步骤 4	使用 Microsoft IIS 创建 .pfx APNs 证书 在 Macintosh 计算机上创建 .pfx APNs 证书 使用 OpenSSL 创建 .pfx APNs 证书	将 APNs 证书导出为 PKCS #12 (.pfx) 证书（在 IIS、Mac 或 SSL 上）。
步骤 5	将 APNs 证书导入到 XenMobile	将证书导入到 XenMobile。

在 iOS Developer Enterprise Program 中创建的移动设备管理 (MDM) 推送证书已迁移到 Apple 推送证书门户。此迁移影响新 MDM 推送证书的创建以及现有 MDM 推送证书的续订、吊销和下载。迁移不影响其他 (非 MDM) APNs 证书。

如果 MDM 推送证书是在 iOS Developer Enterprise Program 中创建的，则以下情况适用：

- 已为您自动迁移证书。
- 可以在 Apple 推送证书门户续订证书，不会影响您的用户。
- 需要使用 iOS Developer Enterprise Program 吊销或下载预先存在的证书。

如果没有即将过期的 MDM 推送证书，则无需进行任何操作。如果有即将过期的 MDM 推送证书，请联系您的 MDM 解决方案提供商。然后将 iOS Developer Program Agent 登录到 Apple 推送证书门户 (使用其 Apple ID)。

所有新的 MDM 推送证书都必须在 Apple 推送证书门户中创建。iOS Developer Enterprise Program 不再允许创建带有包含 com.apple.mgmt 的产品组合 ID (APNs 主题) 的 App ID。

注意：必须跟踪用于创建证书的 Apple ID。此外，该 Apple ID 应是公司 ID，而不是个人 ID。

生成 iOS 设备的 APNs 证书请求的第一步是创建证书签名请求 (CSR)。在 Windows 2012 R2 或 Windows 2008 R2 Server 上，可以使用 Microsoft IIS 生成 CSR。

1. 打开 Microsoft IIS。
2. 双击 IIS 的服务器证书图标。
3. 在“服务器证书”窗口中，单击**创建证书请求**。
4. 键入相应的标识名 (DN) 信息，然后单击下一步。
5. 为加密服务提供程序选择 **Microsoft RSA SChannel Cryptographic Provider**，并为位长度选择 **2048**，然后单击下一步。
6. 输入文件名并指定保存 CSR 的位置，然后单击**完成**。

1. 在运行 Mac OS X 的 Mac 计算机上，在**应用程序 > 实用工具**下方，启动钥匙串访问应用程序。
2. 打开**钥匙串访问**菜单，然后单击**偏好设置**。
3. 单击**证书**选项卡，将 **OCSP** 和 **CRL** 的选项更改为关，然后关闭“首选项”窗口。
4. 在**钥匙串访问**菜单上，单击**证书助理 > 从证书颁发机构请求证书**。
5. “证书助理”将提示您输入以下信息：
 1. **电子邮件地址**。负责管理证书的个人或角色帐户的电子邮件地址。
 2. **公用名**。负责管理证书的个人或角色帐户的公用名。
 3. **CA 电子邮件地址**。证书颁发机构的电子邮件地址。
6. 选择**保存到磁盘**和**让我指定密钥对信息**选项，然后单击**继续**。
7. 输入 CSR 文件的名称，在您的计算机上保存此文件，然后单击**保存**。
8. 通过选择**密钥大小 2048 位**以及 **RSA 算法**，指定密钥对信息，然后单击**继续**。作为 APNs 证书流程的一部分，CSR 文件已可供上载。
9. 证书助理完成 CSR 流程后，单击**完成**。

如果不能使用 Windows 2012 R2 或 Windows 2008 R2 Server 和 Microsoft Internet Information Server (IIS) 或 Mac 计算机生成证书签名请求 (CSR)，以提交到 Apple 来获取 Apple 推送通知服务 (APNs) 证书，可以使用 OpenSSL。

注意：要使用 OpenSSL 创建 CSR，首先需要从 OpenSSL Web 站点下载并安装 OpenSSL。

1. 在安装 OpenSSL 的计算机上，从命令提示窗口或 Shell 执行以下命令。
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.csr -newkey rsa:2048

2. 此时将显示以下要求证书命名信息的信息。根据请求输入信息。

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:RWC

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

Organizational Unit Name (eg, section) []:Marketing

Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com

3. 在下一条消息中，输入 CSR 私钥的密码。

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:

An optional company name []:

4. 将生成的 CSR 发送给 Citrix。

Citrix 会准备签名的 CSR 并通过电子邮件向您返回相关文件。

证书需要通过 Citrix 签名以便可用于 XenMobile，然后您才能将其提交给 Apple。

1. 在浏览器中，转到 [XenMobile APNs CSR Signing](#) Web 站点。

2. 单击 **Upload the CSR** (上载 CSR)。

3. 浏览并选择证书。

注意：证书必须采用 .pem/txt 格式。

4. 在“XenMobile APNs CSR Signing”页面上，单击 **Sign** (签名)。将为 CSR 签名并将签名后的 CSR 自动保存到已配置的下载文件夹。

从 Citrix 收到已签名的证书签名请求 (CSR) 后，需要将其提交给 Apple，以获取 APNs 证书。

注意：有些用户报告登录 Apple 推送门户时遇到问题。作为替代方法，可以先登录到 Apple 开发人员门户 (<http://developer.apple.com/devcenter/ios/index.action>)，之后再转到步骤 1 中的 identity.apple.com 链接。

1. 在浏览器中，转到 <https://identity.apple.com/pushcert>。

2. 单击 **Create a Certificate** (创建证书)。
3. 如果是首次使用 Apple 创建证书, 请选中 **I have read and agree to these terms and conditions** (我已阅读并同意这些条款和条件) 复选框, 然后单击 **Accept** (接受)。
4. 单击 **Choose File** (选择文件), 浏览到计算机上已签名的 CSR, 然后单击 **Upload** (上载)。此时应显示一条确认消息, 表明上载成功。
5. 单击 **Download** (下载) 以检索 .pem 证书。
注意: 如果您使用的是 Internet Explorer 且文件扩展名丢失, 则单击 **Cancel** (取消) 两次, 然后从下一个窗口下载。

要将来自 Apple 的 APNs 证书用于 XenMobile, 需要在 Microsoft IIS 中完成证书请求, 将证书导出为 PCKS #12 (.pfx) 文件, 然后将 APNs 证书导入 XenMobile。

重要: 此任务需要使用用于生成 CSR 的 IIS 服务器。

1. 打开 Microsoft IIS。
2. 单击“服务器证书”图标。
3. 在**服务器证书**窗口中, 单击**完成证书请求**。
4. 浏览至来自 Apple 的 Certificate.pem 文件。然后, 键入友好名称或证书名称并单击**确定**。
5. 选择在步骤 4 中确定的证书, 然后单击**导出**。
6. 为 .pfx 证书指定位置和文件名以及密码, 然后单击**确定**。
注意: 在 XenMobile 安装期间需要该证书的密码。
7. 将 .pfx 证书复制到要安装 XenMobile 的服务器上。
8. 以管理员身份登录到 XenMobile 控制台。
9. 在 XenMobile 控制台中, 单击控制台右上角的齿轮图标。此时将显示**设置**页面。
10. 单击**证书**。此时将显示证书页面。
11. 单击**导入**。此时将显示导入对话框。
12. 在**导入**菜单中, 选择**密钥库**。
13. 在**用作**中, 选择**APNs**。
14. 在**密钥库**文件中, 单击**浏览**并导航到要导入的密钥库文件的位置, 选择该文件。
15. 在**密码**中, 键入分配给证书的密码。
16. 单击**导入**。

1. 在用于生成 CSR 的运行 Mac OS X 的 Mac 计算机上, 找到从 Apple 接收的生产标识 (.pem) 证书。
2. 双击证书文件, 将文件导入到钥匙串。
3. 如果提示将证书添加到指定钥匙串, 则保持已选择的默认登录钥匙串, 然后单击**确定**。新添加的证书会出现在证书列表中。
4. 单击该证书, 然后在**文件**菜单上, 单击**导出**, 开始将证书导出到 PCKS #12 (.pfx) 证书中。
5. 为证书文件命名用于 XenMobile 服务器的唯一名称, 为保存的证书选择文件夹位置, 选择 .pfx 文件格式, 然后单击**保存**。
6. 输入用于导出证书的密码。Citrix 建议使用具有唯一性的强密码。还要确保证书和密码的安全性, 以供以后使用和引用。
7. 钥匙串访问应用程序会提示您输入登录密码或选定的钥匙串。输入密码, 然后单击**确定**。保存的证书现在即可用于 XenMobile 服务器。

注意: 如果计划不保存和保留最初用于生成 CSR 并完成证书导出过程的计算机及用户帐户, Citrix 建议从本地系统保存或导出个人密钥及公钥。否则, 不能访问 APNs 证书以重新使用, 且必须重复整个 CSR 和 APNs 过程。

使用 OpenSSL 创建证书签名请求 (CSR) 后, 还可使用 OpenSSL 创建 .pfx APNs 证书。

1. 在命令提示窗口或者 Shell 中，执行以下命令。
openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
2. 输入 .pfx 证书文件的密码。记住此密码，因为在将证书上载到 XenMobile 时需要再次使用该密码。
3. 记下 .pfx 证书文件的位置，然后将该文件复制到 XenMobile 服务器中，以便可以使用 XenMobile 控制台来上载文件。

在请求并接收到新 APNs 证书后，可将 APNs 证书导入 XenMobile，以便首次添加该证书或者替换现有证书。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击**证书**。此时将显示证书页面。
3. 单击**导入**。此时将显示导入对话框。
4. 在**导入**菜单中，选择**密钥库**。
5. 在**用作**中，选择**APNs**。
6. 浏览到计算机上的 .p12 文件。
7. 输入密码，然后单击**导入**。

有关 XenMobile 中的证书的详细信息，请参阅[证书](#)部分。

要续订 APNs 证书，需要执行与创建新证书相同的步骤。然后，访问 [Apple 推送证书门户](#) 并上载新证书。登录后，就可看见自己的现有证书，或者看见从自己之前的 Apple 开发人员帐户导入的证书。在“证书门户”上，续订证书的唯一区别是要单击续订。要访问该站点，您必须拥有证书门户的开发人员帐户。续订您的证书时，请务必使用相同的组织名称和 Apple ID。

注意：要确定 APNs 证书的过期时间，请在 XenMobile 控制台中单击**配置 > 设置 > 证书**。如果证书已过期，请勿吊销它。

1. 请使用 Microsoft Internet Information Services (IIS) 生成 CSR。
2. 在 [XenMobile APNs CSR Signing](#) (XenMobile APNs CSR 签名) Web 站点上，上载新 CSR，然后单击 **Sign** (签名)。
3. 将签名后的 CSR 提交给 Apple，站点为 [Apple 推送证书门户](#)。
4. 单击**续订**。
5. 使用 Microsoft IIS 生成 PCKS #12 (.pfx) APNs 证书。
6. 在 XenMobile 控制台中更新新 APNs 证书。单击控制台右上角的齿轮图标。此时将显示设置页面。
7. 单击**证书**。此时将显示证书页面。
8. 单击**导入**。此时将显示导入对话框。
9. 在**导入**菜单中，选择**密钥库**。
10. 在**用作**中，选择**APNs**。
11. 浏览到计算机上的 .p12 文件。
12. 输入密码，然后单击**导入**。

SAML 单点登录与 ShareFile

Apr 27, 2017

可以将 XenMobile 和 ShareFile 配置为使用安全声明标记语言 (SAML) 来提供对 ShareFile 移动应用程序的单点登录 (SSO) 访问。此功能包括使用 MDX Toolkit 打包的 ShareFile 应用程序和未打包的 ShareFile 客户端（例如 Web 站点、Outlook 插件或同步客户端）。

- **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 Secure Hub 进行用户身份验证以及获取 SAML 令牌。成功进行身份验证后，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 Secure Mail 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。

要将 XenMobile 作为 SAML 身份提供程序 (IdP) 用于 ShareFile，必须将 XenMobile 配置为使用 ShareFile Enterprise，如本文所述。或者，可以将 XenMobile 配置为只与 StorageZone 连接器一起使用。有关详细信息，请参阅 [ShareFile 与 XenMobile 结合使用](#)。

有关详细的参考体系结构图，请参阅《XenMobile 部署手册》中的[适用于本地部署的参考体系结构](#)一文。

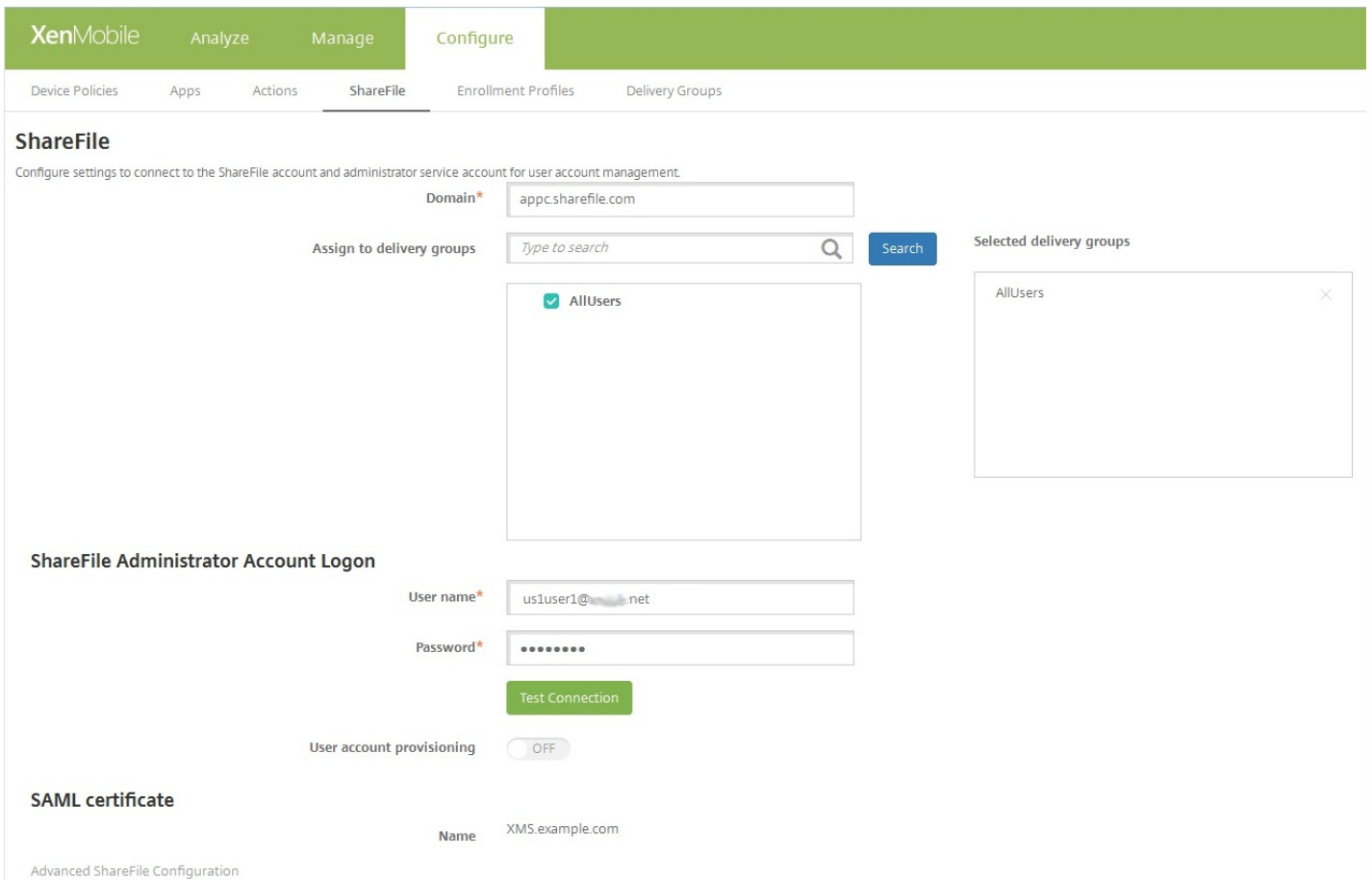
必须先完成以下必备条件，才能对 XenMobile 和 ShareFile 应用程序配置 SSO：

- 兼容版本的 MDX Toolkit（适用于 ShareFile 移动应用程序）
- 兼容版本的 ShareFile 移动应用程序和 Secure Hub
- ShareFile 管理员帐户

验证 XenMobile 与 ShareFile 之间的连接。

为 ShareFile 设置 SAML 之前，请按如下所示提供 ShareFile 访问信息：

1. 在 XenMobile Web 控制台中，单击**配置 > ShareFile**。此时将显示 **ShareFile** 配置页面。



2. 配置以下设置：

- **域**：键入 ShareFile 子域的名称，例如 example.sharefile.com。
- **分配给交付组**：选择或搜索希望能够对 ShareFile 使用 SSO 的交付组。
- **ShareFile 管理员帐户登录**
 - **用户名**：键入 ShareFile 管理员用户名。此用户必须具有管理员权限。
 - **密码**：键入 ShareFile 管理员的密码。
 - **用户帐户置备**：如果要在 XenMobile 中启用用户置备，请打开此选项；如果计划使用 ShareFile 用户管理工具来置备用户，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 ShareFile 帐户，前提是您启用了“用户帐户置备”。Citrix 建议您使用具有小型成员关系的角色以测试配置。这样可以避免出现大量没有 ShareFile 帐户的用户的可能性。

3. 单击**测试连接**按钮以确认 ShareFile 管理员帐户的用户名和密码是否可以向指定的 ShareFile 帐户进行身份验证。
4. 单击**保存**。XenMobile 将与 ShareFile 同步并更新 ShareFile 设置 **ShareFile 颁发者/实体 ID** 和**登录 URL**。

以下步骤适用于 iOS 和 Android 应用程序和设备。

1. 使用 MDX Toolkit 打包 ShareFile 移动应用程序。有关使用 MDX Toolkit 打包应用程序的详细信息，请参阅[使用 MDX Toolkit 打包应用程序](#)。

2. 在 XenMobile 控制台中，上载打包的 ShareFile 移动应用程序。有关上载 MDX 应用程序的信息，请参阅[向 XenMobile 中添加 MDX 应用程序](#)。

3. 使用在上面配置的管理员用户名和密码登录 ShareFile 来验证 SAML 设置。

4. 确认为 ShareFile 和 XenMobile 配置了相同的时区。

注意：确保 XenMobile 显示所配置时区对应的正确时间。如果时间不正确，SSO 可能会失败。

验证 ShareFile 移动应用程序

1. 在用户设备上，如果尚未安装和配置 Secure Hub，请进行安装和配置。

2. 从 XenMobile Store 下载并安装 ShareFile 移动应用程序。

3. 启动 ShareFile 移动应用程序。ShareFile 将启动，但不提示输入用户名和密码。

使用 Secure Mail 验证

1. 在用户设备上，如果尚未安装和配置 Secure Hub，请进行安装和配置。

2. 从 XenMobile Store 下载、安装并设置 Secure Mail。

3. 打开新的电子邮件窗体，然后轻按从 **ShareFile 附加**。此时将显示可以附加到电子邮件中的文件，但不提示输入用户名或密码。

如果要配置对未打包的 ShareFile 客户端（例如 Web 站点、Outlook 插件或同步客户端）的访问，必须将 NetScaler Gateway 配置为支持使用 XenMobile 作为 SAML 身份提供程序，如下所示：

- 禁用主页重定向。
- 创建 ShareFile 会话策略和配置文件。
- 在 NetScaler Gateway 虚拟服务器上配置策略。

禁用主页重定向

必须禁用通过 /cginfra 路径发出的请求的默认行为，以使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** 下方，键入 XenMobile 内部服务器的名称和端口号。

3. 在 **AppController** 下方，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 配置实用程序的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 **+** 按钮创建新操作。此时将显示 **Create NetScaler Gateway Session Profile (创建 NetScaler Gateway 会话配置文件)** 页面。

Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Accounting Policy
[Dropdown]

Override Global

Display Home Page

Home Page
none

URL for Web-Based Email
[Text Box]

Split Tunnel*
OFF

Session Time-out (mins)
1

Client Idle Time-out (mins)
[Text Box]

Clientless Access*
Allow

Clientless Access URL Encoding*
Obscure

Clientless Access Persistent Cookie*
DENY

Plug-in Type*
Windows/MAC OS X

Single Sign-on to Web Applications

Credential Index*
PRIMARY

KCD Account
[Text Box]

Single Sign-on with Windows*

配置以下设置：

- **Name** (名称)：键入 ShareFile_Profile。
- 单击 **Client Experience** (客户端体验) 选项卡，然后配置以下设置：
 - **Home Page** (主页)：键入“none” (无)。
 - **Session Time-out (mins)** (会话超时(分钟))：键入 1。
 - **Single Sign-on to Web Applications** (单点登录到 Web 应用程序)：选择此设置。
 - **Credential Index** (凭据索引)：在列表中，单击“PRIMARY” (主要)。
- 单击 **Published Applications** (已发布的应用程序) 选项卡。

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security **Published Applications**

Override Global

ICA Proxy*
ON

Web Interface Address
https://xms.citrix.lab:8443 ?

Web Interface Address Type*
IPV4

Web Interface Portal Mode*
NORMAL

Single Sign-on Domain
citrix

Citrix Receiver Home Page

Account Services Address

OK Close

配置以下设置：

- **ICA Proxy** (ICA 代理)：在列表中，单击 **ON** (开)。
- **Web Interface Address** (Web Interface 地址)：键入 XenMobile 服务器的 URL。
- **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)。

← Back Add Expression

Create NetScaler Gateway Session Policy

Name*
ShareFile_Policy

Action*
Sharefile_Profile

Expression*
Operators Saved Policy Expressions Freq

Create Close

Select Expression Type: General

Flow Type
REQ

Protocol
HTTP

Qualifier
HEADER

Operator
CONTAINS

Value*
NSC_FSRD

Header Name*
COOKIE

Length
Offset

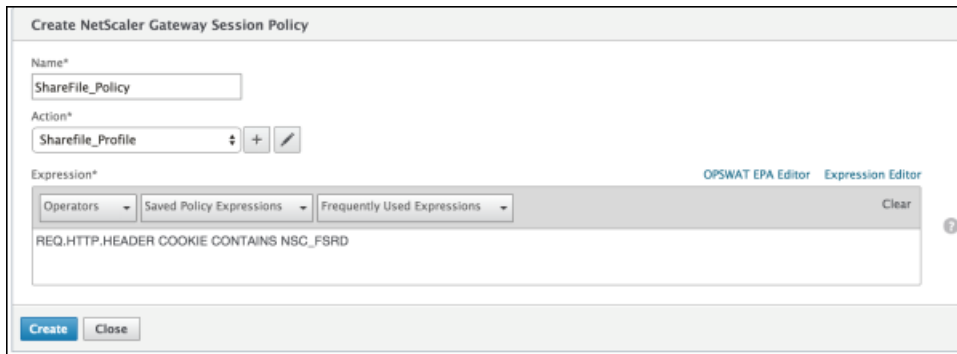
Done Cancel

Expression Editor
Clear

配置以下设置：

- **Value** (值)：键入 NSC_FSRD。
- **Header Name** (标头名称)：键入 COOKIE。
- 单击 **Done** (完成)。

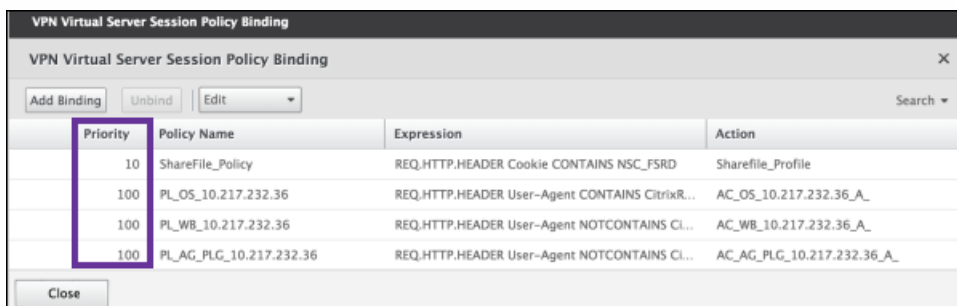
7. 单击 **Create** (创建)，然后单击 **Close** (关闭)。



在 NetScaler Gateway 虚拟服务器上配置策略

在 NetScaler Gateway 虚拟服务器上配置以下设置。

1. 在 NetScaler Gateway 配置实用程序的左侧导航窗格中单击 **NetScaler Gateway > Virtual Servers** (虚拟服务器)。
2. 在 **Details** (详细信息) 窗格中，单击 NetScaler Gateway 虚拟服务器。
3. 单击编辑。
4. 单击 **Configured policies** (已配置的策略) > **Session policies** (会话策略)，然后单击 **Add binding** (添加绑定)。
5. 选择 **ShareFile_Policy**。
6. 编辑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。

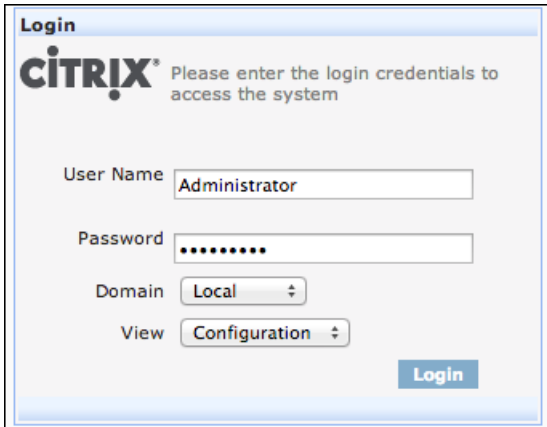


Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_WB_10.217.232.36_A
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_AG_PLG_10.217.232.36_A

7. 单击 **Done** (完成)，然后保存运行的 NetScaler 配置。

请执行以下步骤，查找 ShareFile 配置的内部应用程序名称。

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 **View** (查看) 列表中，单击 **Configuration** (配置)。



3. 单击 **Applications** (应用程序) > **Applications** (应用程序)，并记录 **Display Name** (显示名称) 为 ShareFile 的应用程序的 **Application Name** (应用程序名称)。

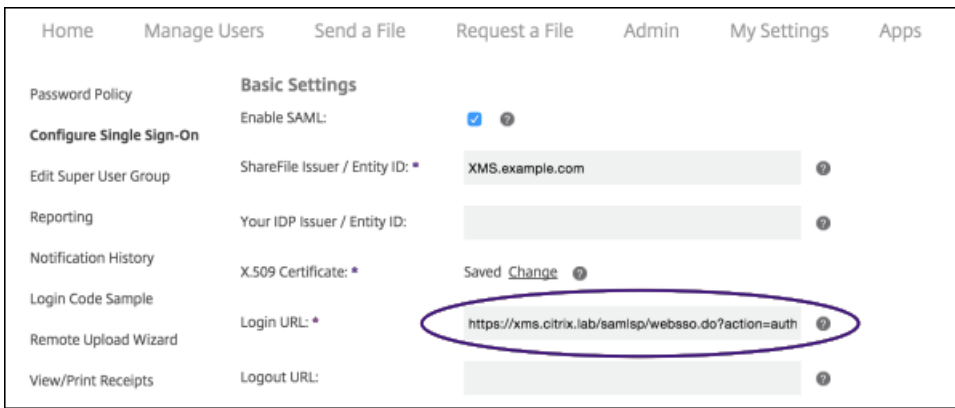


Application Name	Display Name	Description
activedirectory	activedirectory	
AmericanExpress	AmericanExpress	Online access to world-class card, financial, insu...
Fidelity	Fidelity	Your Personal Investing Resource
LinkedIn	LinkedIn	Business-oriented social networking site
ShareFile_SAML	ShareFile	Online storage for business
MobileApp11	ShareFile_220	ShareFile 2.2.0
MobileApp13	ShareFile_iPhone_303	ShareFile 3.0.3

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。



- 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。

URL 现在应如下所示：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

- 将参数 `&app=ShareFile_SAML_SP` 更改为 [SAML 单点登录与 ShareFile](#) 中步骤 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`，依此类推）。

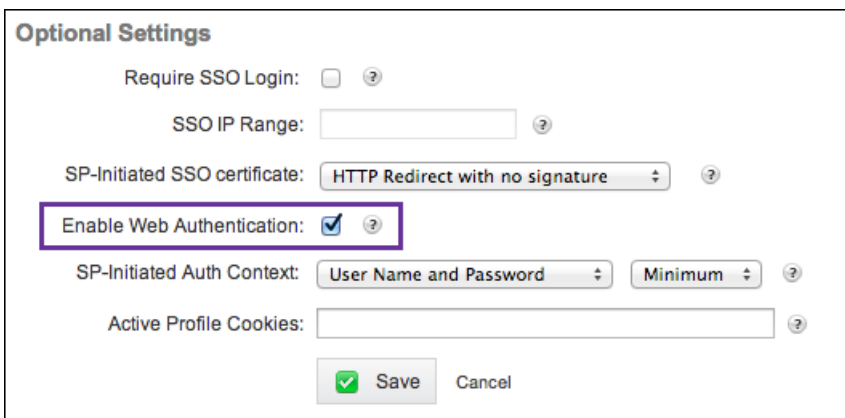
URL 现在应如下所示：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- 向 URL 的结尾末尾添加 `&nssso=true`。

修改后的 URL 现在应如下所示：`https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`。

重要：每次在 XenMobile 控制台中编辑或重新创建 ShareFile 应用程序或更改 ShareFile 设置时，都会在内部应用程序名称后附加一个新数字，这意味着您还必须在 ShareFile Web 站点中更新登录 URL，以反映更新后的应用程序名称。

- 在 **Optional Settings**（可选设置）下方，选中 **Enable Web Authentication**（启用 Web 身份验证）复选框。



请执行以下配置以验证设置。

1. 将浏览器指向 <https://<子域>sharefile.com/saml/login>。

系统会将您重定向到 NetScaler Gateway 登录表单。如果未被重定向，请验证前面的配置设置。

2. 输入所配置的 NetScaler Gateway 和 XenMobile 环境的用户名和密码。

此时将在 <子域>.sharefile.com 下显示您的 ShareFile 文件夹。如果未显示您的 ShareFile 文件夹，请确保您输入了正确的登录凭据。

Microsoft Azure Active Directory 服务器设置

Feb 27, 2017

需要具有 Microsoft Azure Active Directory 高级许可证才可以将 XenMobile 与 Microsoft Azure 集成。启用 MDM 与 Azure AD 的集成需要许可证，以便使用 Windows 10 设备的用户可以使用 Azure AD 注册。有关获取高级许可证的信息，请参阅 [Microsoft Azure](#)。有关定价信息，请参阅 [Azure Active Directory 定价](#)。

必须在 XenMobile 中配置 Microsoft Azure 服务器设置，并为 Windows 设备设置“条款和条件”设备策略，Windows 设备用户才可以使用 Azure 注册。本文介绍如何配置 Microsoft Azure 设置。有关为 Windows 设备配置“条款和条件”设备策略的信息，请参阅 [条款和条件设备策略](#)。



您需要登录到 Azure AD 门户并执行以下操作，才能在 XenMobile 中设置 Microsoft Azure 服务器设置：

1. 注册自定义域并验证域。有关详细信息，请参阅 [Add your own domain name to Azure Active Directory](#)（将自己的域名添加到 Azure Active Directory）。
2. 使用目录集成工具，将本地目录扩展到 Azure Active Directory。有关详细信息，请参阅 [目录集成](#)。
3. 将 MDM 设为 Azure AD 的可信部分。为此，请单击 **Azure Active Directory** > **应用程序**，然后单击添加。从库中选择添加 **应用程序**。转至 **移动设备管理**，选择本地 **MDM 应用程序**，然后保存设置。
4. 在应用程序中，按如下所述配置 XenMobile 服务器发现、终端使用条款和应用程序 ID URI：
 - MDM 发现 URL：https://:8443/zdm/wpe
 - MDM 使用条款 URL：https://:8443/zdm/wpe/tou
 - 应用程序 ID URI：https://:8443/
5. 选择在第 3 步创建的本地 MDM 应用程序并启用 **管理这些用户的设备** 选项，以便为所有用户或任何特定用户组启用 MDM 管理。

还需要记下 Microsoft Azure 帐户提供的以下信息，才能在 XenMobile 控制台中配置设置：

- 应用程序 ID URI – 运行 XenMobile 的服务器的 URL。
- 租户 ID – 来自 Azure 应用程序设置页面。
- 客户端 ID – 您的应用程序的唯一标识符。
- 密钥 – 来自 Azure 应用程序设置页面。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示 **设置** 页面。
2. 在平台下方，单击 **Microsoft Azure**。此时将显示 **Microsoft Azure** 页面。


XenMobile Analyze Manage Configure   admin ▾

Settings > Microsoft Azure


Microsoft Azure

Integrate XenMobile with Microsoft Azure to let devices running Windows 10 enroll with Azure as a federated means of Active Directory authentication. You derive the values to enter here from your Azure directory settings. Note that you must also configure a Terms & Conditions device policy for Windows; otherwise, users cannot enroll with Azure.

App ID URI*

Tenant ID* 

Client ID*

Key* 

3. 配置以下设置：

- **应用程序 ID URI**：键入运行 XenMobile 的服务器的 URL（在配置 Azure 设置时输入的）。
- **租户 ID**：从 Azure 应用程序设置页面复制此值。在浏览器地址栏中，复制由数字和字母组成的部分。例如，在 <https://manage.windowsazure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...> 中，租户 ID 为：*abc123-abc123-abc123*。
- **客户端 ID**：从“Azure 配置”页面复制并粘贴此值。这是应用程序的唯一标识符。
- **密钥**：从 Azure 应用程序设置页面复制此值。在密钥下方，从列表中选择一個持续时间并保存设置。然后，可以复制此密钥并将其粘贴到此字段中。应用程序在 Microsoft Azure AD 中读写数据时需要密钥。

4. 单击保存。

Important

用户在其 Windows 设备上加入 Azure AD 时，您在 XenMobile 中配置的 XenMobile Store 和 Web 链接设备策略将仅适用于 Azure AD 用户，不适用于本地用户。对于能够使用这些设备策略的本地用户，必须执行以下操作：

1. 在 **设置 > 关于 > 加入 Azure AD** 中，代表 Azure 用户加入 Azure AD。
2. 注销 Windows，然后使用 Azure AD 帐户进行登录。

升级

Apr 13, 2017

Important

升级到 XenMobile 10.5 (内部部署) 之前的准备工作

1. 如果运行要升级的 XenMobile 服务器的虚拟机的 RAM 低于 4 GB，请将 RAM 增加到至少 4 GB。请注意，对于生产环境，建议的最低 RAM 是 8 GB。
2. 记下适用于 Windows 平板电脑的通行码和限制设备策略的配置相关信息。这些策略不再基于 WMI。因此，升级会删除现有配置。升级后，重新配置适用于 Windows 平板电脑的通行码和限制设备策略。
3. 要访问 XenMobile 管理控制台，只能使用节点的 XenMobile 服务器完全限定域名 (FQDN) (注册 FQDN) 或 IP 地址。如果要直接通过负载均衡虚拟 IP 地址或 NAT 的 IP 地址进行控制台访问，需要 XenMobile 服务器 10.5 Rolling Patch 1。此修补程序于 2017 年 3 月 22 日发布。有关详细信息，请参阅 <https://support.citrix.com/article/CTX221304>。
4. 您的 Citrix 许可证上的专享升级服务 (SA) 日期必须晚于 2016 年 6 月 1 日。可以在许可证服务器中的许可证旁边查看您的 SA 日期。要续订许可证上的 SA 日期，请从 Citrix 门户网站下载最新的许可证文件，然后将该文件上载到 Licensing 服务器。有关详细信息，请参阅 <http://support.citrix.com/article/CTX209580>。

Citrix 将 XenMobile 的新版本或重要更新发布到 Citrix.com。同时，向每个客户的在案联系人发送通知。

可以采用以下方案升级 XenMobile：

- **从 XenMobile 9.0 升级到 XenMobile 最新版本。**

使用 XenMobile 最新版本内置的 XenMobile 升级工具。有关详细信息，请参阅本文的此部分。

该升级工具支持所有 XenMobile 9 版本：MDM、App 和 Enterprise。

有关已修复的问题和已知问题，请参阅[已修复的问题](#)和[已知问题](#)。

Citrix.com 上不再提供较早版本的升级工具。

- **从 XenMobile 10.3.6 或 10.4 升级到 XenMobile 10.5。**

使用 XenMobile 控制台中的版本管理页面。有关详细信息，请参阅本文中的说明。

对于 XenMobile 9.0 以外的 XenMobile 版本，不使用升级工具。

- **从 XenMobile 10 或 10.1 升级到 XenMobile 10.5。**

首先，使用 XenMobile 控制台中的版本管理页面，从 XenMobile 10 或 XenMobile 10.1 升级到 XenMobile 10.3.6。然后，使用 XenMobile 控制台中的版本管理页面，从 XenMobile 10.3.6 升级到 XenMobile 10.5。有关详细信息，请参阅本文中的说明。请勿使用升级工具安装这些版本。

XenMobile Server version	Release number	Upgrade to	Release number	Upgrade path	Update location
安装了 App Controller 滚动修补程序 9 的 XenMobile 服务器 9	9.0.0_97106	XenMobile 服务器 10.5	10.5.0.24	XenMobile 服务器 9 升级到 XenMobile 服务器 10.5	下载 App Controller 滚动修补程序必备项。 <ul style="list-style-type: none"> 适用于 XenMobile 10.5 的升级工具内置在 XenMobile 服务器中。 有关详细信息，请参阅升级工具必备条件。
XenMobile 服务器 10 或 XenMobile 10.1	10.1.0.63030	XenMobile 服务器 10.3.6	10.3.6	XenMobile 10 或 XenMobile 10.1 升级到 XenMobile 10.3.6	下载
XenMobile 服务器 10.3.6	10.3.6	XenMobile 服务器 10.5	10.5.0.24	XenMobile 10.3.x 升级到 XenMobile 10.5	下载
XenMobile 服务器 10.4	10.4.x	XenMobile 服务器 10.5	10.5.0.24	XenMobile 10.4 升级到 XenMobile 10.5	下载

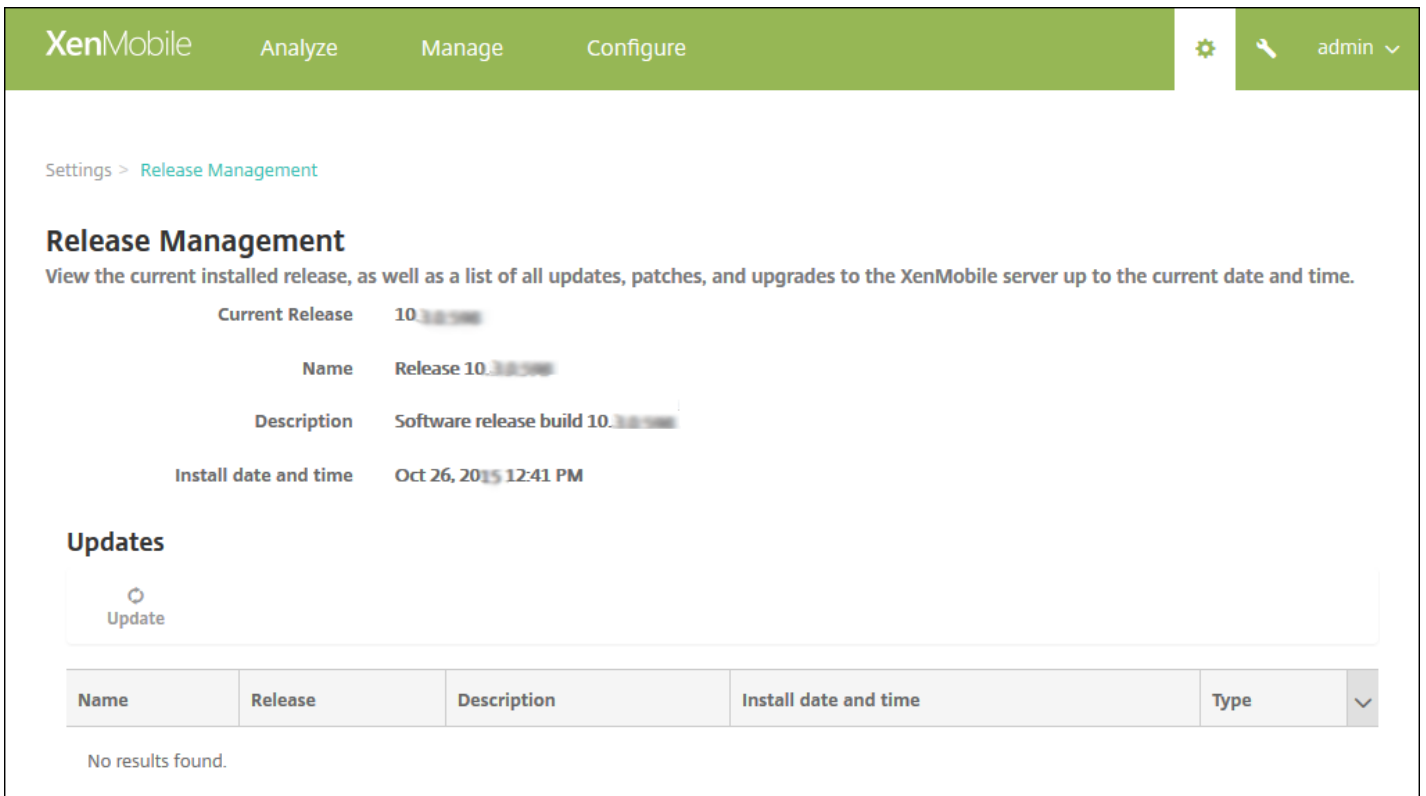
可使用版本管理页面从支持的 XenMobile 10 版本（上表中所示）升级到最新版本的 XenMobile 服务器。

必备条件：

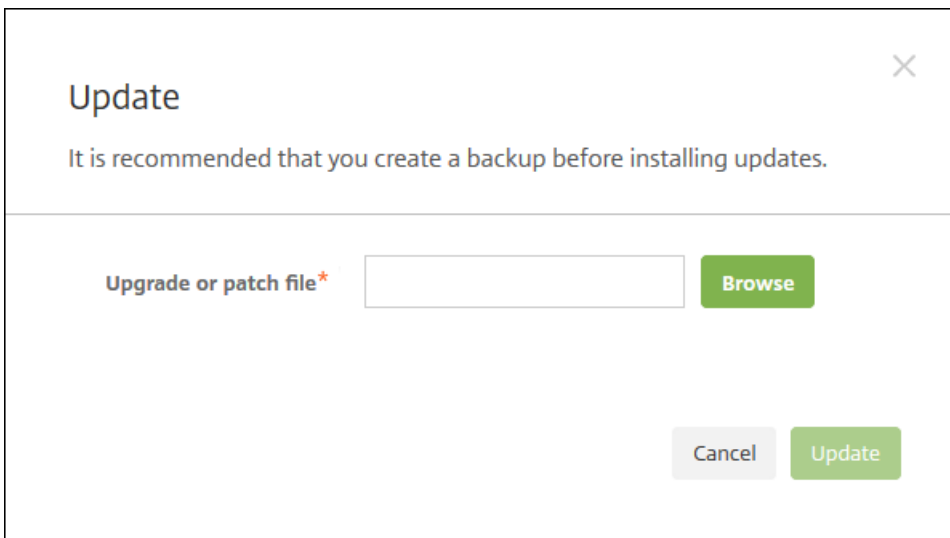
- 安装 XenMobile 更新前，请使用虚拟机 (VM) 中的功能创建系统的快照。
- 备份系统配置数据库。
- 检查要更新到的版本的系统要求。有关 XenMobile 最新版本的信息，请参阅[系统要求](#)。

您有群集部署时，请参阅本文结尾处的说明。

1. 在 Citrix Web 站点上登录您的帐户，然后将 XenMobile 升级 (.bin) 文件下载到合适的位置。
2. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
3. 单击版本管理。此时将显示版本管理页面。



4. 在更新下方，单击更新。此时将显示更新对话框。



5. 单击浏览并导航到从 Citrix.com 下载的 XenMobile 升级文件的位置，选择此文件。

6. 单击更新，然后在收到提示时，重新启动 XenMobile。

如果由于某些原因，更新未能成功完成，会显示一条指出问题的错误消息。系统会恢复到尝试更新之前的状态。

注意：升级后，XenMobile 需要重新启动。可使用 XenMobile CLI 重新启动 XenMobile 服务器。系统重新启动后清除浏览器缓存非常重要。

升级群集 XenMobile 部署

如果系统是在群集模式下配置的，请按照以下步骤从 XenMobile 10 版本更新每个节点：

1. 在所有节点上从**设置 > 版本管理**上载 .bin 文件。
2. 在 CLI 中从**系统菜单**关闭所有节点。
3. 在 CLI 中从**系统菜单**提出一个节点，并检查服务是否正在运行。
4. 按顺序逐一提取其他节点。

如果 XenMobile 无法成功完成更新，会显示一条指出问题的错误消息。XenMobile 随后将系统还原到尝试更新之前的状态。

升级工具必备条件

Feb 27, 2017

要从 XenMobile 9.0 升级到 XenMobile 最新版本，请使用 XenMobile 内置的升级工具。

该升级工具支持：

- 在所有 XenMobile 服务器模式 (ENT、MAM、MDM) 下注册的 iOS 和 Android 设备
- 在 MDM 模式下注册的 Windows Phone 和 Tablet
- 在企业模式下注册的 Windows Phone
- MDM 模式下的 Windows CE 设备

如果在 XenMobile 9.0 上启用了 Multi-Tenant Console (MTC)，则可以将 MTC 迁移到独立的 XenMobile 最新版本部署。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。完成本文中所述的必备条件后，请参阅[将 MTC 租户服务器升级到 XenMobile](#)。

XenMobile 最新版本支持 NetScaler Gateway 11.1.x、11.0.x 和 10.5.x 版。

XenMobile 内置的升级工具还支持 NetScaler Gateway 10.1.x 版。Citrix 不支持将 NetScaler Gateway 10.1 与 XenMobile 最新版本结合使用。但是，可以使用 XenMobile 内置的升级工具升级 NetScaler Gateway 10.1 部署。之后，Citrix 建议将 NetScaler Gateway 升级到支持的最新版本。

Important

升级过程比较复杂。开始升级前，请务必按照本文所述，查看[已知问题](#)、规划升级工作并完成所有必备条件。此外，此[博客](#)含有一份有助于规划升级工作的必备条件核对表。

运行升级工具后，请务必完成所有后续条件。

如果未完成必备条件，升级可能会失败。那么就必须在命令行控制台中配置 XenMobile 最新版本新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. 在过渡环境中进行试用，完成所有必备条件和升级工具步骤。Citrix 建议您先进行升级试用，以大体了解过程以及在进行全面的生产升级后的预期效果。在试用升级期间测试的是配置数据而不是用户数据的升级情况。

在 NetScaler 11.1（最低要使用 NetScaler 10.5 版本）中，Citrix 建议使用 NetScaler for XenMobile 向导设置含有 NetScaler Gateway 和 NetScaler 负载均衡虚拟服务器的全新 NetScaler。

2. 确认试用是否正确升级了配置数据，例如 LDAP、策略和应用程序。确认测试设备。

3. 在生产环境中执行生产升级并使其生效。为升级期间的停机工作做好规划。

关于试用升级和生产升级

首先使用 XenMobile 升级工具测试升级，然后执行全面的生产升级。

选择“Test Drive”（试用）时：

升级工具对生产配置数据执行升级试用，在不影响生产环境的情况下比较 XenMobile 9.0 和 XenMobile 最新版本。试用升级仅测试配置数据，而不会测试设备数据（使用 XenMobile Enterprise Edition 部署时）和用户数据。

升级试用的结果仅供测试之用。不能升级试用部署。相反，必须重新开始执行生产升级。升级试用适用于任何 XenMobile 9.0 版本。

选择“Upgrade”（升级）时：

升级工具首先将 XenMobile 9.0 中的所有配置、设备和用户数据复制到一个具有相同的完全限定域名 (FQDN) 的 XenMobile 最新版本新实例。XenMobile 9.0 中的所有数据保持不变，直至将新 XenMobile 服务器移动到生产环境中。

升级后登录到新 XenMobile 服务器实例的控制台时，您会看到升级从 XenMobile 9.0 移动来的所有用户和设备数据。

升级工具不执行的操作

使用升级工具时，不会将以下信息升级到 XenMobile 最新版本：

- 许可信息。
- 报告数据。
- 服务器组策略及关联的部署（在 XenMobile 最新版本中不受支持）。
- 托管服务提供程序 (MSP) 组。
- 与 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。
- 升级日志文件中所述的其他任何配置或用户数据。
- CXM Web（由 Citrix Secure Web 替代）。
- DLP 策略（由 Citrix Sharefile 替代）。
- 自定义 Active Directory 属性。
- 如果已在 XenMobile 9.0 中配置多个外观方案策略，不会升级外观方案策略。XenMobile 最新版本支持一个外观方案策略；必须在 XenMobile 9.0 中保留一个外观方案策略，才能成功升级到 XenMobile 最新版本。
- XenMobile 9.0 的 auth.jsp 文件中用于限制访问控制台的任何设置。XenMobile 最新版本中的控制台访问限制是在命令行接口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 最新版本中不受支持）。

XenMobile 变更

- 升级工具不升级已分配给本地组的 Active Directory 用户。您随后可以将 Active Directory 用户分配到本地组。
- XenMobile 10 不支持嵌套的本地组。从 XenMobile 9 升级会使本地组层次结构变得平整。
- Device Manager 中的部署软件包现在在 XenMobile 中称为交付组，如下图所示。有关详细信息，请参阅[部署资源](#)。

The screenshot shows the XenMobile Configure interface for Delivery Groups. The top navigation bar includes XenMobile, Analyze, Manage, and Configure. The main navigation includes Device Policies, Apps, Actions, ShareFile, Enrollment Profiles, and Delivery Groups. The page title is "Delivery Groups" with a "Show filter" link and a search box. Below the title are "Add" and "Export" buttons. A table lists three delivery groups:

<input type="checkbox"/>	Status	Name	Last Updated	Disabled
<input type="checkbox"/>		AllUsers		<input type="checkbox"/>
<input type="checkbox"/>		Domain users	Jun 13 2016 5:10 PM	<input type="checkbox"/>
<input type="checkbox"/>		Sales	Apr 13 2016 12:50 PM	<input type="checkbox"/>

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。

The screenshot shows the "Delivery Group Information" form in the XenMobile Configure interface. The left sidebar lists navigation options: 1 Delivery Group Info (selected), 2 User, 3 Resource (optional), Policies, Apps, Actions, ShareFile, Enrollment Profile, and 4 Summary. The main form area contains the following fields:

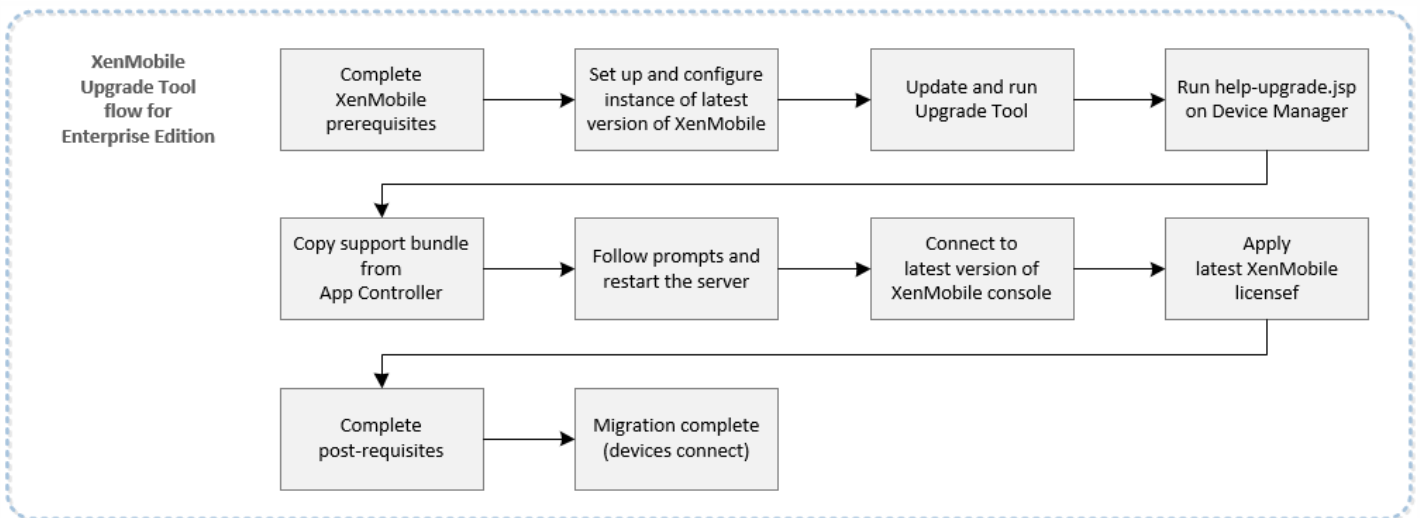
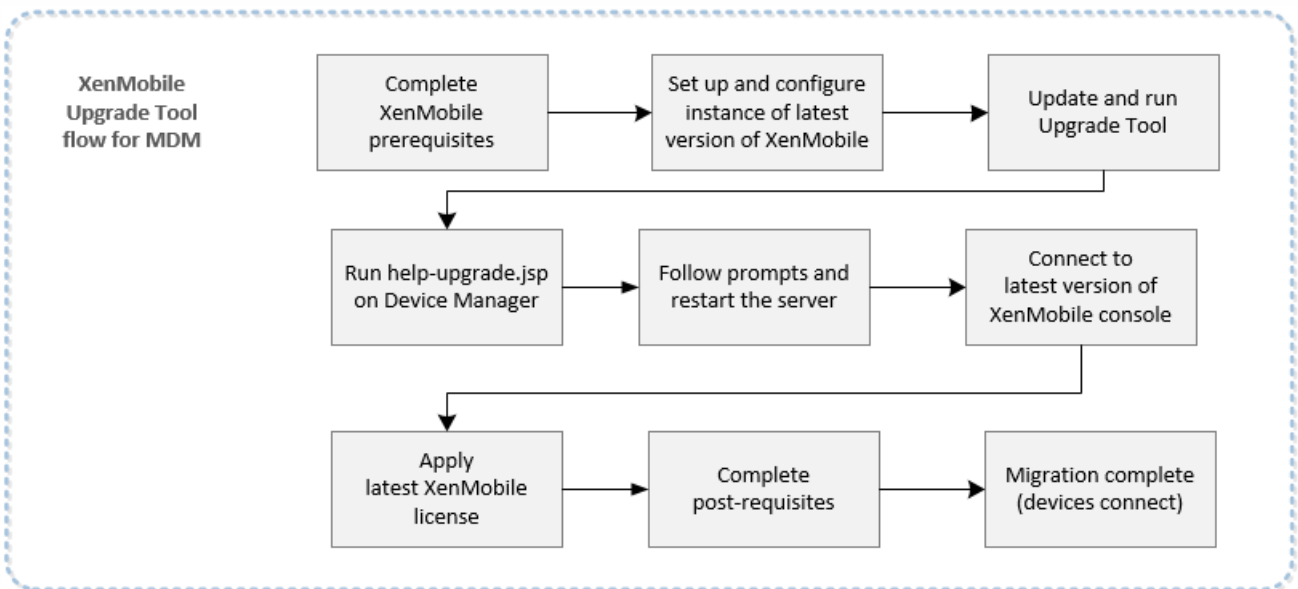
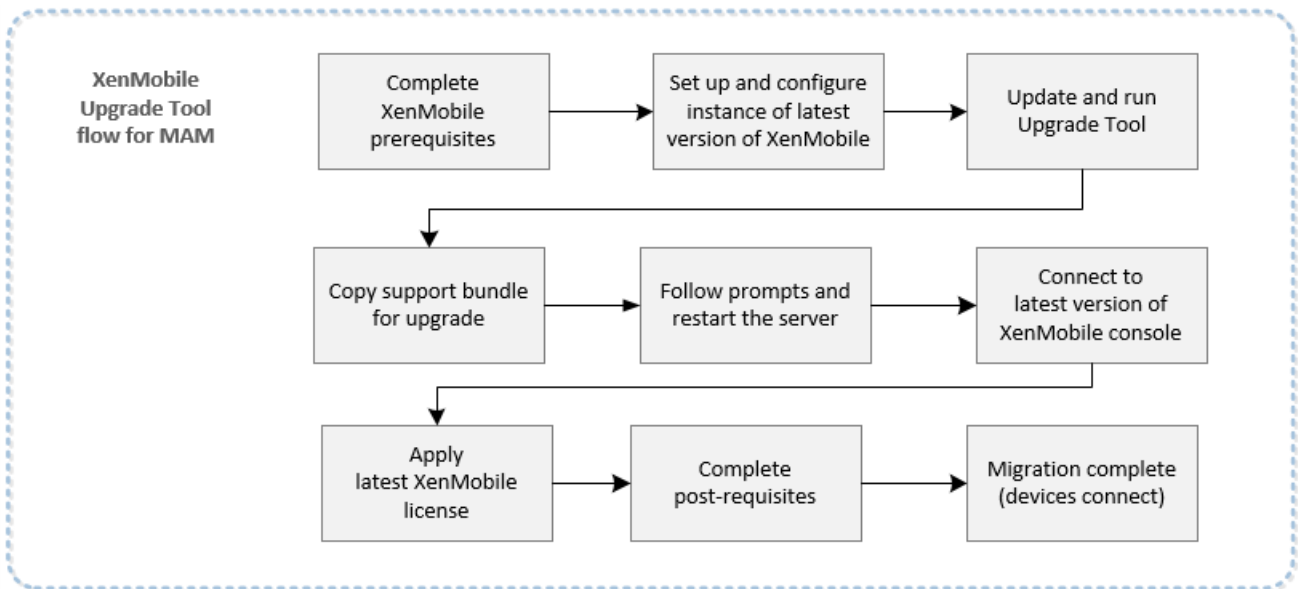
Delivery Group Information ×

Enter a name for the delivery group and any information that will help you keep track of it later.

Name

Description

下图说明了从 XenMobile 9.0 升级需要执行的基本步骤。



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 最新版本时，Citrix 建议执行以下步骤：

1. 将 Device Manager 上安装的 Worx Home 升级到 Worx Home 10.2 或更高版本，然后部署 Worx Home 10.2。
2. 从用户设备中手动卸载 Worx Home 9.x。
3. 指示用户转至其手机上的下载中心以安装 Worx Home 10.2 或更高版本（您已从 Device Manager 中部署该版本）。
4. 完成本文所述的必备条件后，按[启用和运行 XenMobile 升级工具](#)中所述升级到 XenMobile 最新版本。
5. 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。

从 <https://support.citrix.com/article/CTX218552> 下载 XenMobile 9.0 App Controller Rolling Patch 9。

在 App Controller 管理控制台中，转至 **设置 > 版本管理**。单击 **更新**，然后选择已下载的修补程序文件。单击 **上载**，然后重新启动 App Controller。

将 XenMobile 9 升级到 XenMobile 最新版本之前，必须将自定义应用商店名称改回其默认值，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**。

Beacons [Edit](#)

Store name: *

Default store view:

有关相关组件（例如 Citrix License Server）所需的版本，请参阅[系统要求](#)及其中的各节。

- **NetScaler**：升级 NetScaler 之前，请务必保存一份 Netscaler 配置文件 (ns.conf) 的副本。当前的 Netscaler 发行版中包括一个易于使用的快速部署实用程序，即 NetScaler for XenMobile 向导。该向导用于引导您完成集成 NetScaler 和 XenMobile 的步骤。有关详细信息，请参阅[配置 XenMobile 环境的设置](#)和[常见问题解答：XenMobile 10 和 NetScaler 10.5 集成](#)。
- **防火墙端口**：为新 XenMobile 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。有关 XenMobile 端口要求的信息，请参阅[端口要求](#)。
- **LDAP 服务器**：确保新 XenMobile 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。

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 数据库要求](#)。

从 **XenMobile 9.0** 到 **XenMobile 最新版本**

Enterprise Edition

App Controller

MDM

本地 PostgreSQL	本地 PostgreSQL	本地 PostgreSQL
本地 PostgreSQL	MS SQL	MS SQL
本地 PostgreSQL	远程 PostgreSQL	远程 PostgreSQL

应用程序版本

本地 PostgreSQL	本地 PostgreSQL
本地 PostgreSQL	远程 PostgreSQL
本地 PostgreSQL	MS SQL

MDM 版本

本地 PostgreSQL	本地 PostgreSQL
MS SQL	MS SQL
远程 PostgreSQL	远程 PostgreSQL

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

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

要允许对 PostgreSQL 进行远程连接，必须完成以下步骤：

1. 打开文件 `pg_hba.conf`，找到以下行：

```
host all all 127.0.0.1/32 md5
```

2. 要允许使用所有 IP 地址，请将该行内容更改为：

```
host all all 0.0.0.0/0 md5
```

或者，添加另一个主机条目，以允许连接到 XenMobile 服务器 IP 地址：

```
host all all 10.x.x.x/32 md5
```

3. 保存该文件。

4. 停止并启动服务。

5. 打开 `postgresql.conf` 文件，然后找到以下行：

```
#listen_addresses = 'localhost'
```

6. 将该行内容更改为：

```
listen_addresses = '*'
```

7. 停止并启动 PostgreSQL 服务以应用所做的更改。

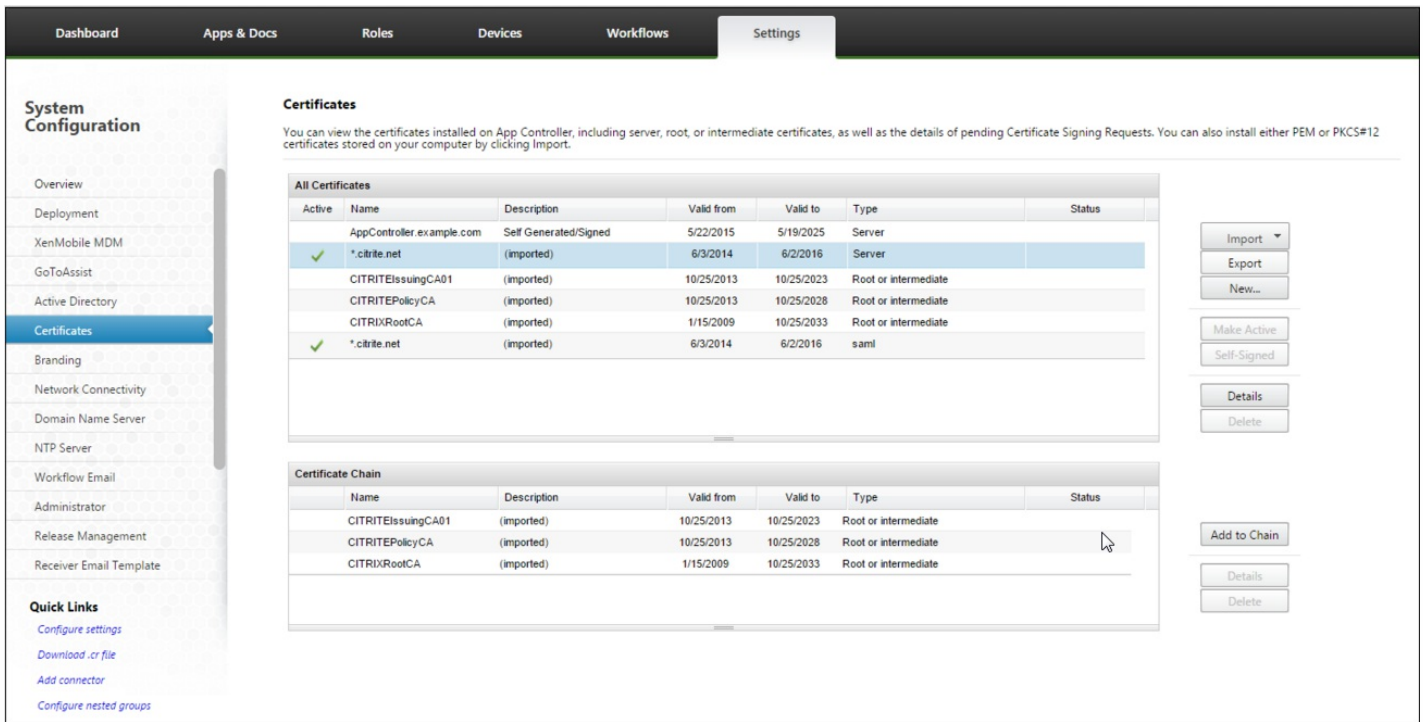
如果已将自定义端口分配给数据库解决方案，则必须确保允许使用该端口，并且在保护 XenMobile 9.0 Device Manager 的防火墙中打开该端口。这样可以使 XenMobile 新实例连接到数据库并迁移所需信息。

XenMobile 9.0 中名称含有特殊字符 (!、\$、()、#、%、+、*、~、?、|、{} 和 []) 的部署软件包可以升级，但升级后无法在 XenMobile 新实例中编辑交付组。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 新实例中创建注册邀请时出现问题。升级之前，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。

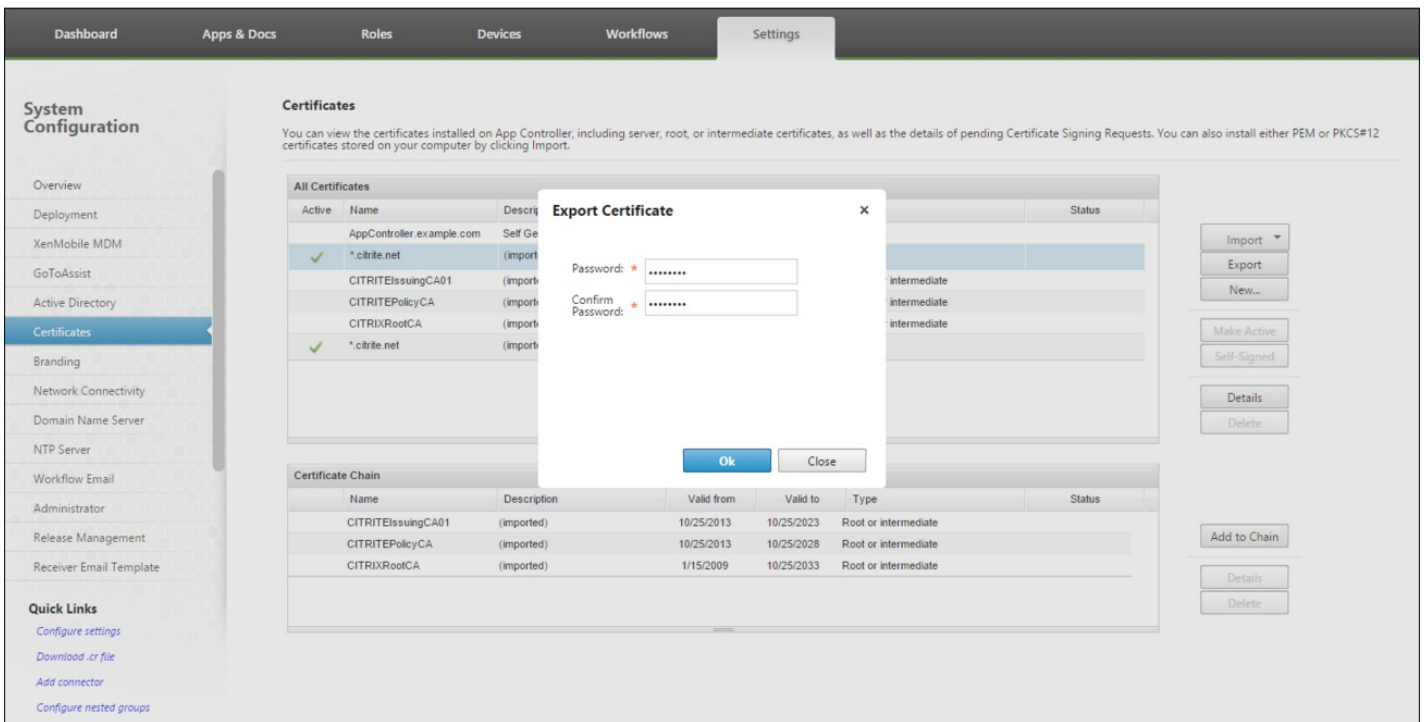
外部 SSL 证书必须满足 Citrix 支持文章[如何配置外部 SSL 证书](#)中列出的条件。请务必在开始升级之前查看 `pki.xml`，以确保 SSL 证书满足这些条件。

如果要升级 XenMobile 9.0 Enterprise Edition 部署，必须导出 App Controller 服务器证书。然后，在处理升级后续条件时，必须将该服务器证书导入 NetScaler Gateway。请按照以下步骤进行操作以导出服务器证书：

1. 登录 XenMobile 9.0 App Controller 并单击 **Certificates**（证书）。
2. 在证书列表中，单击要导出的服务器证书，然后单击 **Export**（导出）。



3. 在 **Export Certificate** (导出证书) 对话框中，在两个字段中键入证书密码，然后单击 **OK** (确定)。



准备一台服务器，以便从该服务器使用文件传输协议 (FTP) 或安全复制协议 (SCP) 通过 XenMobile 命令行接口上载加密支持包。

启用和运行 XenMobile 升级工具

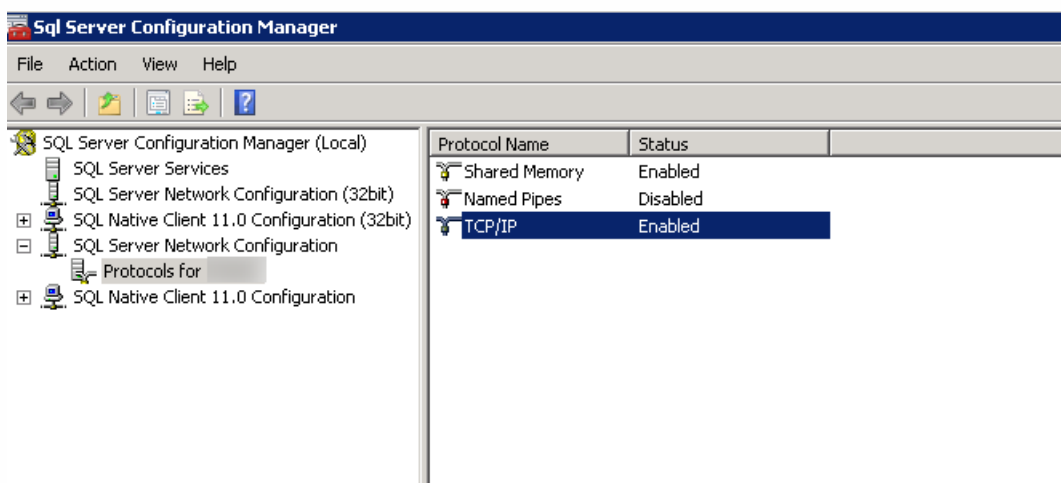
Feb 27, 2017

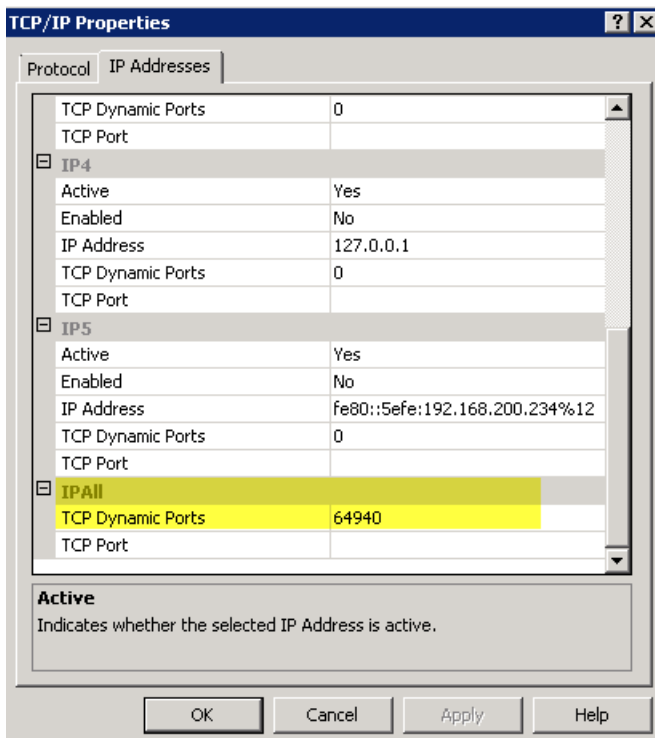
如果您的 XenMobile 9 环境满足以下必备条件，请按照本部分中的步骤进行升级。

- XenMobile 9 MDM Edition 或 Enterprise Edition 带有一个外部 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

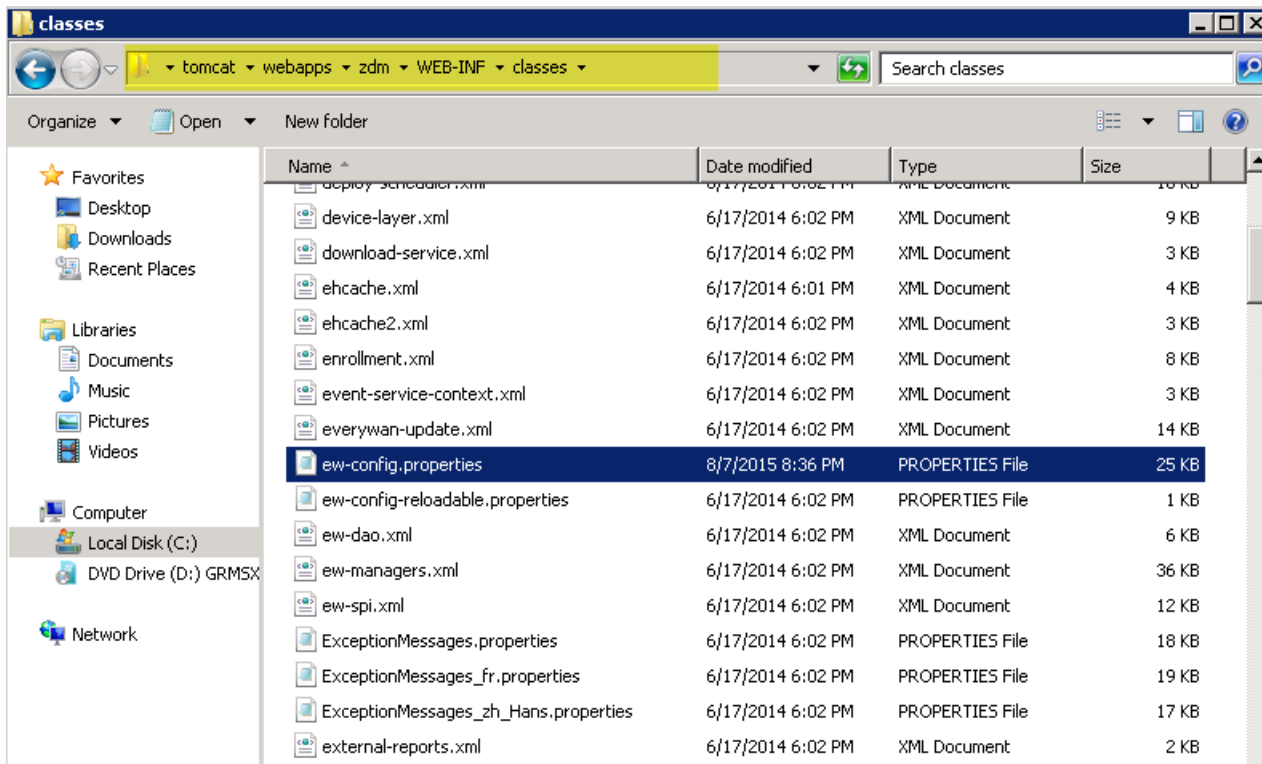
Citrix 建议 SQL Server 数据库实例始终在静态端口上运行，因为 XenMobile 服务器需要继续访问该数据库。此连接通常通过防火墙遍历。因此，您需要在防火墙中打开恰当的端口，并且需要在静态端口上运行数据库实例。





升级前步骤

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=

```
ew-config.properties
18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everwyan
19 # For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everwyan;instance=SQLEXPRESS
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everwyan;instance=SQLEXPRESS;domain=sparus-
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:everwyan/everwyan@//localhost:1521/everwyan
22 pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.net/-11aug;instance=
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234.net
25 # Pooled datasource database
26 pooled.datasource.database=-11aug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everwyan01
31 pooled.datasource.password={aes}==
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everwyan
37 # No pooled datasource user
38 #no.pooled.datasource.user=everwyan
39 # No pooled datasource password
40 #no.pooled.datasource.password=everwyan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jtds:sqlserver://ah-234.net/-11aug;instance=
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234.net
48 # Audit datasource database
49 audit.datasource.database=-11aug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password
```

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://ah-234.net:64940/

audit.datasource.url=jdbc:jtds:sqlserver://ah-234.net:64940/

注意

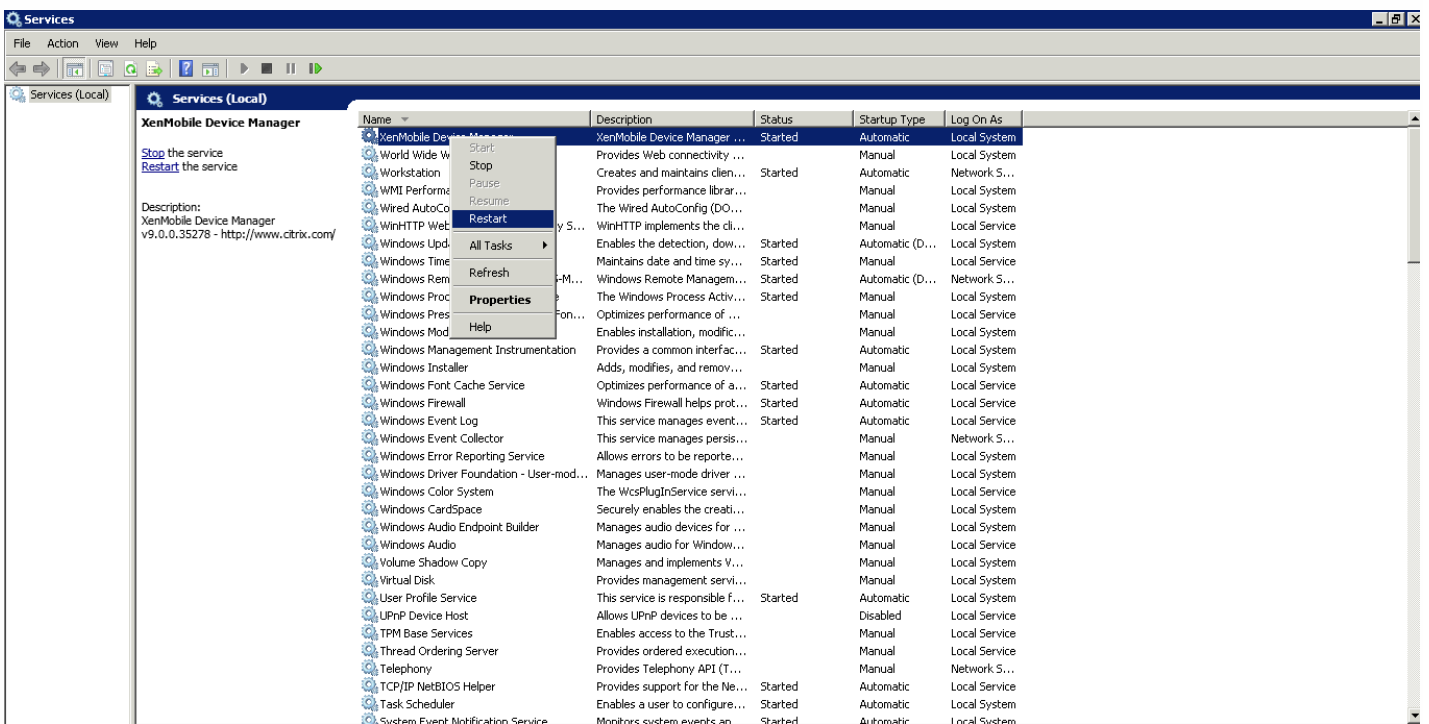
Citrix 建议您先备份、复制或记录在 ew-config.properties 文件中所做的更改。此信息在升级失败时非常有用。

```

18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
19 # For Microsoft SQL server url1 with a named instance (url12): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/instance=SQLExpress
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/instance=SQLExpress;domain=sparus-s
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@localhost:1521/everywan
22 pooled.datasource.url=jdbc:jtds:sqlserver://ah-234. net: -llaug
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234. .net
25 # Pooled datasource database
26 pooled.datasource.database=-llaug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
31 pooled.datasource.password={aes} ==
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
37 # No pooled datasource user
38 #no.pooled.datasource.user=everywan
39 # No pooled datasource password
40 #no.pooled.datasource.password=everywan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jtds:sqlserver:// -inc.net: -llaug
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234. .net
48 # Audit datasource database
49 audit.datasource.database=-llaug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password

```

4. 重新启动 Device Manager 服务。Device Manager 实例重新启动后刷新设备连接。



5. 确定新 XenMobile 10.x 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 建议您将该端口转换为静态端口。稍后，在升级过程中执行到数据库设置的以下部分时，请在新 XenMobile 服务器上配置该静态端口。

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

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

现在，您可以继续升级。

如果将系统配置为群集模式：

1. 关闭除要先升级的节点以外的所有节点。要关闭节点，请在命令行接口中使用设置。
2. 升级仍在运行的节点，如下一节“启用和运行升级工具”中所述。
3. 确保第一个升级按预期完成后，逐个重新加入其余的每个节点。重新加入节点：
 - a. 重新启动节点。
 - b. 请勿升级节点（如果提示）。
 - c. 将节点加入群集数据库。

将节点重新加入群集后，XenMobile 将自动升级节点。

4. 在将节点重新加入群集后，在每个节点上执行所有后续任务。

首次安装最新版本的 XenMobile 时，请通过命令行接口 (CLI) 启用升级工具。

Important

如果要生成系统快照，请在完成最新版本的 XenMobile 的初始配置之后、使用升级工具之前进行。

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。

```
*****
*      Citrix XenMobile      *
* (in First Time Use mode) *
*****

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password:
Re-enter new password:

Network settings:
IP address [I]: 10.207.87.35
Netmask [I]: 255.255.254.0
Default gateway [I]: 10.207.86.1
Primary DNS server [I]: 10.207.86.50
Secondary DNS server (optional) [I]: 10.207.86.51

Commit settings (y/n) [y]:
```

3. 键入 **y** 进行升级。

注意

如果不在此处选择 **y**，则必须在命令行控制台中配置最新版本的 XenMobile 的新实例并重新启动升级工具。

4. 选择生成随机密码，以及启用 FIPS（可选）。输入数据库连接信息。

5. 键入 **y** 提交设置。

```
Commit settings (y/n) [y]:
Applying network settings...

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

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

Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]:

Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:
Server [I]: sql01.xmlab.net
Port [1433]:
Username [sa]: xmsadmin
Password:
Database name [DB_service]: migdemo

Commit settings (y/n) [y]:
```

XenMobile 初始化数据库。

```
Checking database status...
Database does not exist.
Initializing database...
```

6. 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 环境和新环境的 FQDN 必须匹配。

```
Cluster:
Please press y to enable cluster? [y/n]: y
To enable realtime communication between cluster members please open port 80 u
sing Firewall menu option in CLI menu, once the system configuration is complete
.
Xenmobile Server FQDN:
Hostname []: migdemo.xs.citrix.com

Commit settings (y/n) [y]:
Applying fqdn settings...
```

7. 键入 **y** 提交设置。

8. 设置通信端口。

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

Commit settings (y/n) [y]:
```

9. 键入 **y** 提交设置。

10. 选择是否为所有证书使用相同的密码，然后键入要对证书使用的密码。

11. 键入 **y** 提交设置。

```
Applying port listener configuration...

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
- A Node Identification certificate for cluster node client auth
Do you want to use the same password for all the certificates of the PKI [y]:
New password:
Re-enter new password:

Commit settings (y/n) [y]:
Generating SAML signing certificate...
Generating server and client certificates...

XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile console through a web browser.
Username [administrator]:
```

12. 键入 XenMobile 控制台管理员的用户名和密码。

13. 键入 **y** 提交设置。

XenMobile 启用一次性升级工具。

```
Re-enter new password:

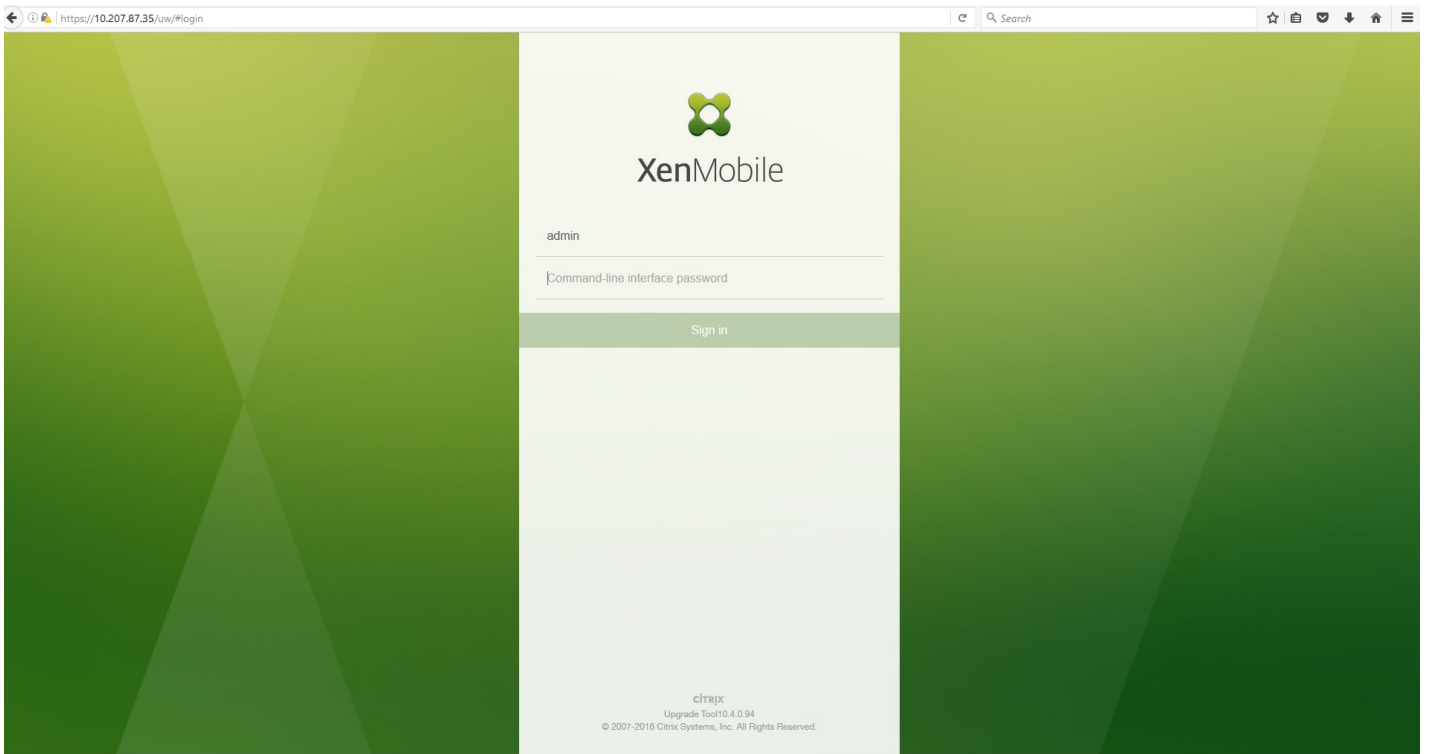
Commit settings (y/n) [y]: y
Creating console administrator...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

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

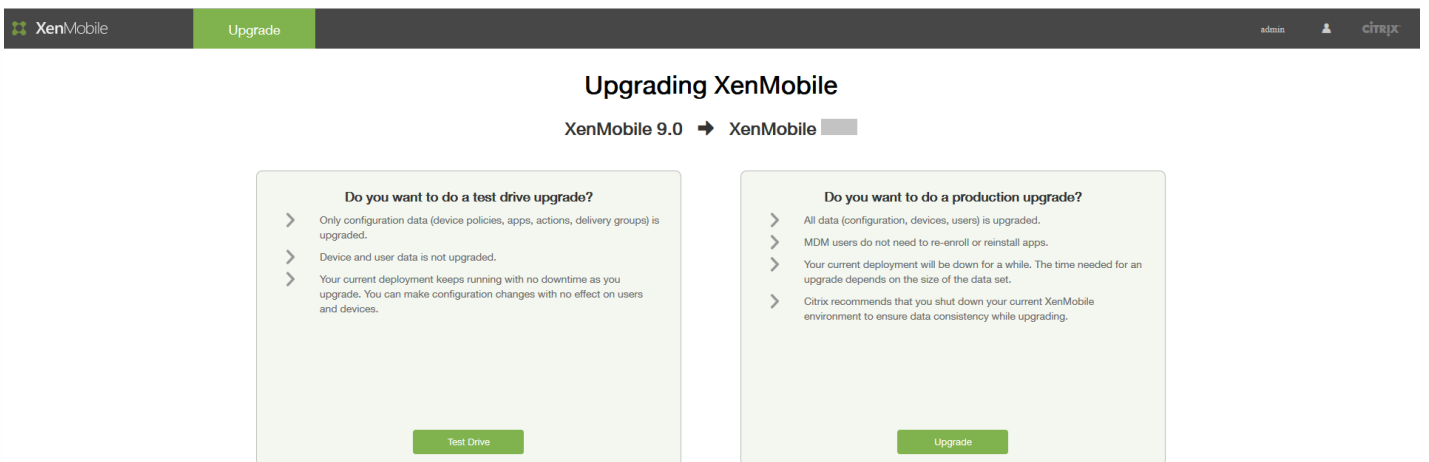
To complete the upgrade process, from a web browser, go to the following
location and log on with your command prompt credentials:
https://10.207.87.35/uw/

Starting monitoring... [ OK ]
migdemo.xs.citrix.com login:
```

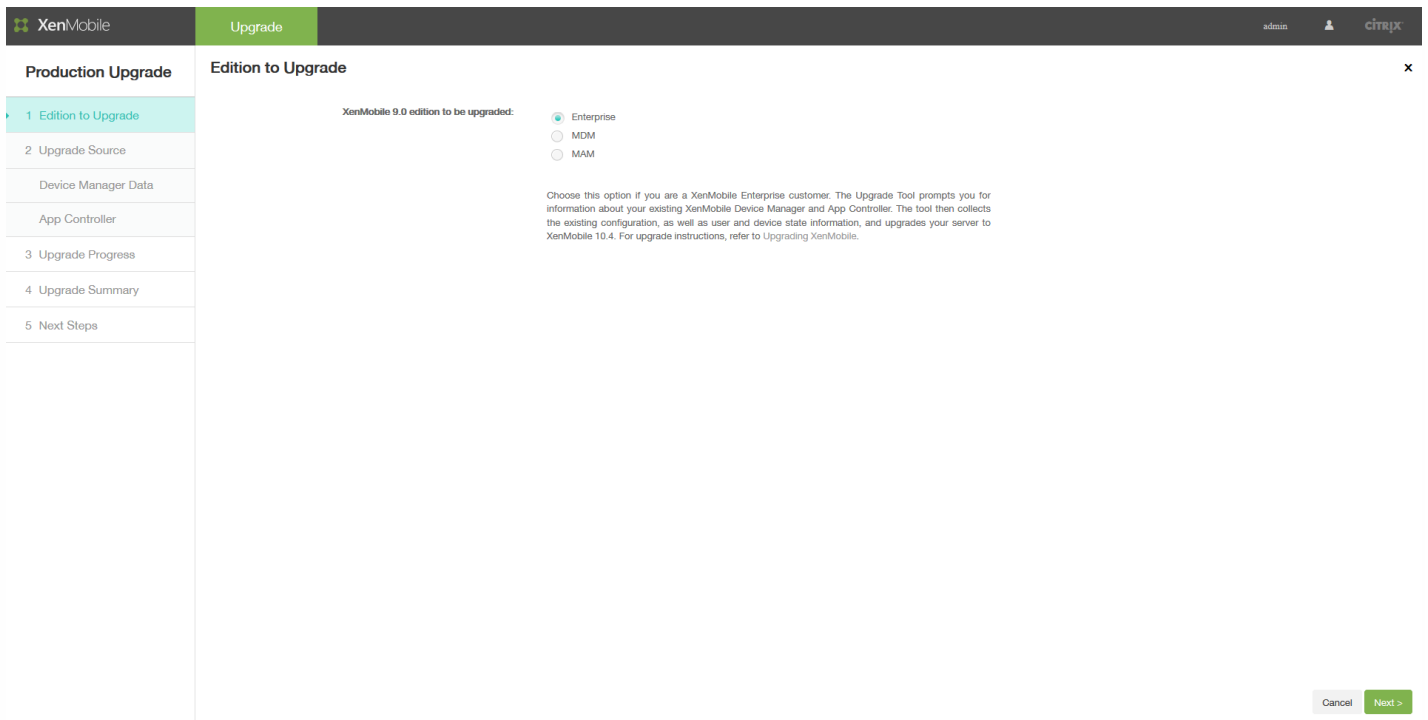
14. 在 Web 浏览器中键入 <https://uw/> 访问升级工具，然后使用在 CLI 中指定的凭据进行登录。



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 **Edition to Upgrade** (要升级的版本) 页面中，选择您的版本。下面的屏幕示例显示了选择 Enterprise Edition 时的情况。



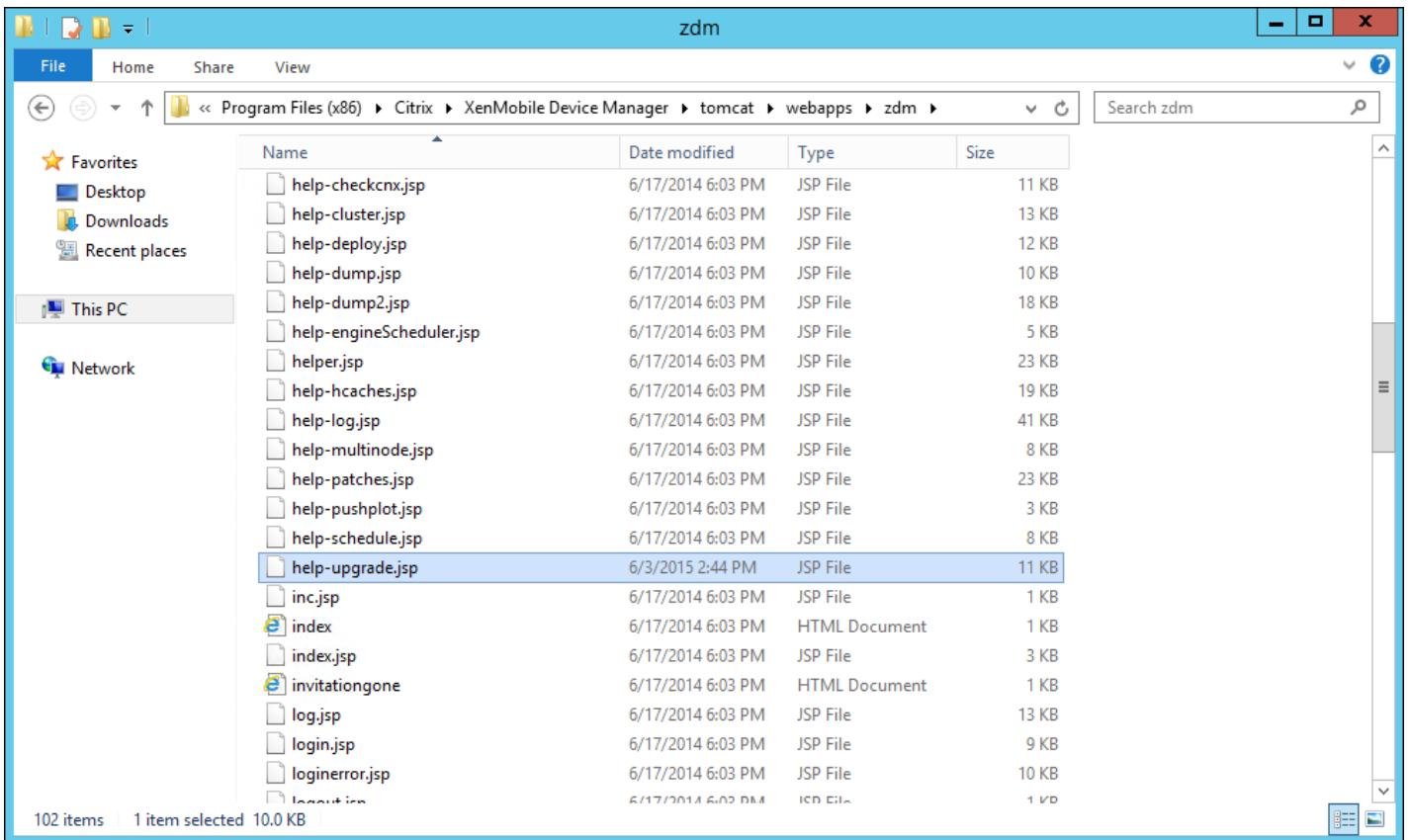
17. 单击下一步。

如果正在升级 Enterprise 或 MDM Edition，则会显示 **Device Manager** 页面。按照步骤 18 至 22 完成此页面上的操作。

如果正在升级 MAM Edition，请跳到步骤 23 完成 **App Controller** 页面上的操作。

18. 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。

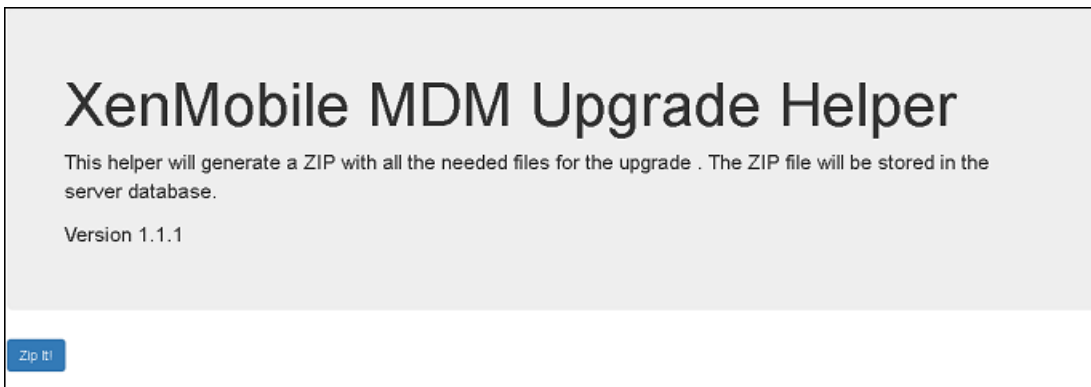
- a. 单击 **Device Manager** 页面的步骤 1 中的链接并保存下载的 help-upgrade.zip 文件。
- b. 将 help-upgrade.jsp 文件解压到现有 XenMobile 9.0 Device Manager 上的 \tomcat\webapps\zdm。



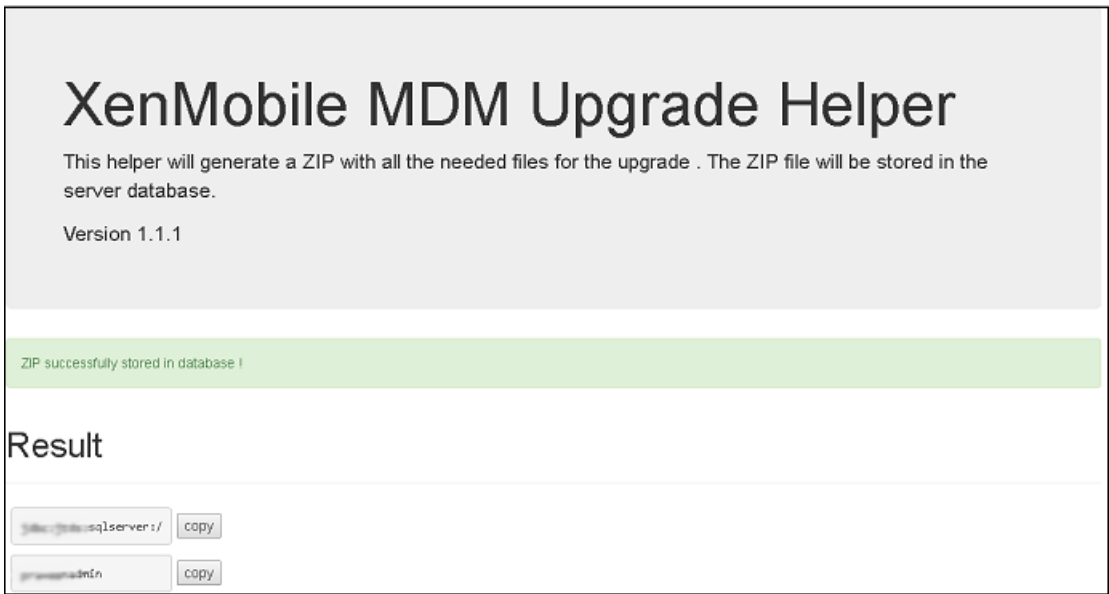
c. 在浏览器窗口中，登录到 XenMobile 9.0 服务器。

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，用于收集并打包从 XenMobile 9.0 升级到最新版本的 XenMobile 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。

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。

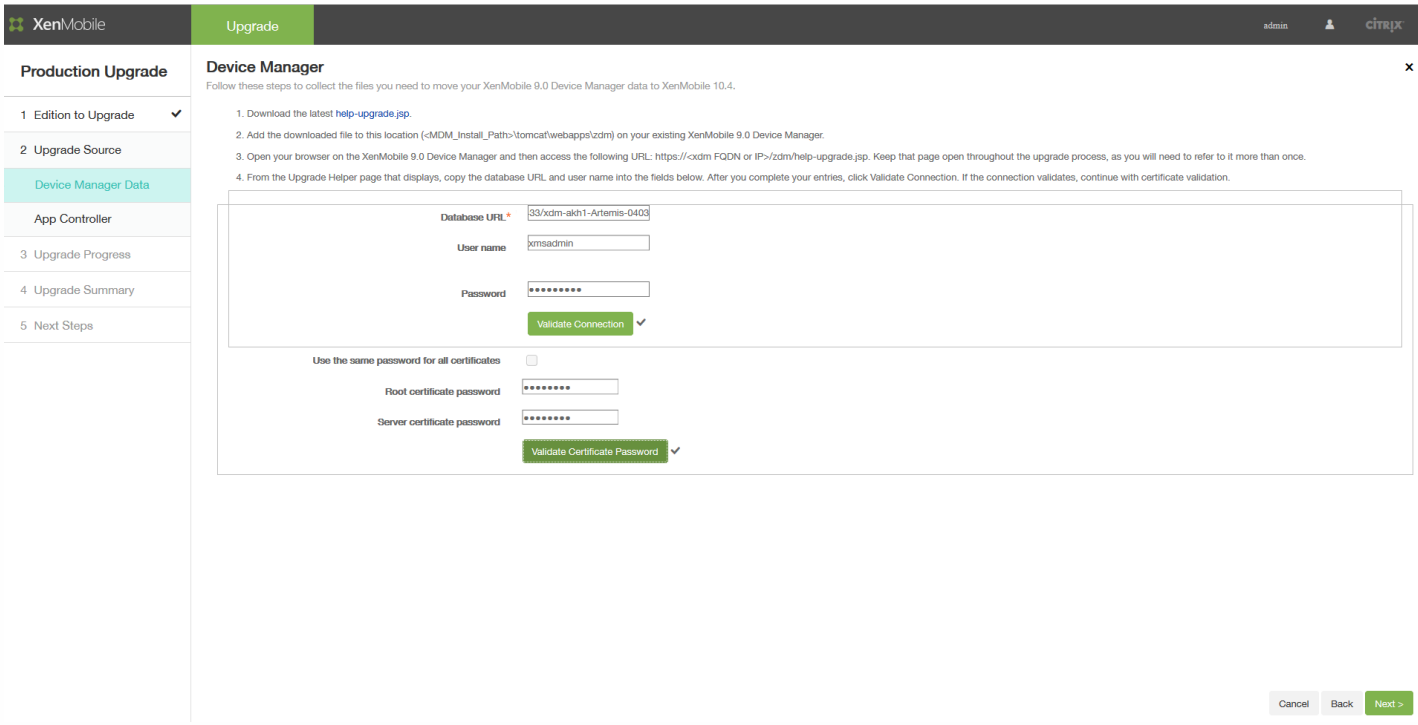


19. 在 **Result**（结果）下，复制 URL 并将其粘贴到升级工具的 **Device Manager** 页面的 **Database URL**（数据库 URL）字段中。然后复制用户名并将其复制到 **Device Manager** 页面。



20. 在升级工具中：

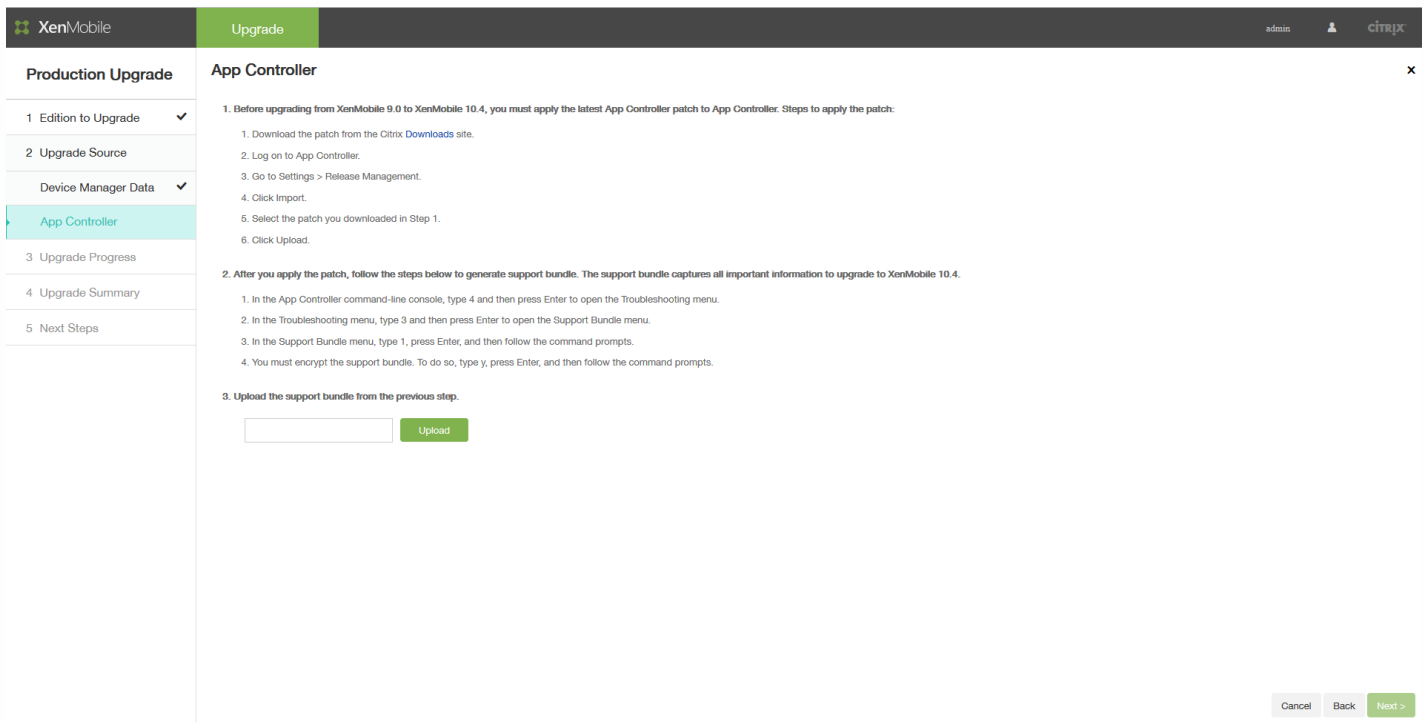
- a. 输入密码，然后单击 **Validate Connection**（验证连接）。
- b. 输入每个证书的密码，然后单击 **Validate Password**（验证密码）。



21. 单击下一步。

22. 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 以重新打包文件。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。

23. 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** 页面第 1 部分的说明升级 App Controller。



The screenshot shows the XenMobile Upgrade interface. The left sidebar has 'Production Upgrade' and 'App Controller' selected. The main content area is titled 'App Controller' and contains the following instructions:

- Before upgrading from XenMobile 9.0 to XenMobile 10.4, you must apply the latest App Controller patch to App Controller. Steps to apply the patch:
 - Download the patch from the Citrix Downloads site.
 - Log on to App Controller.
 - Go to Settings > Release Management.
 - Click Import.
 - Select the patch you downloaded in Step 1.
 - Click Upload.
- After you apply the patch, follow the steps below to generate support bundle. The support bundle captures all important information to upgrade to XenMobile 10.4.
 - In the App Controller command-line console, type 4 and then press Enter to open the Troubleshooting menu.
 - In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu.
 - In the Support Bundle menu, type 1, press Enter, and then follow the command prompts.
 - You must encrypt the support bundle. To do so, type y, press Enter, and then follow the command prompts.
- Upload the support bundle from the previous step.

Below the instructions, there is an input field and an 'Upload' button.

25. 继续按照 **App Controller** 页面第 2 部分的说明执行操作：

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。

```
AppController 9.0.0.973503, 2015-05-26
-----
Main Menu
-----
[0] Express Setup
[1] High Availability
[2] Clustering
[3] System
[4] Troubleshooting
[5] Help
[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] █
```

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

```
[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] █
```

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

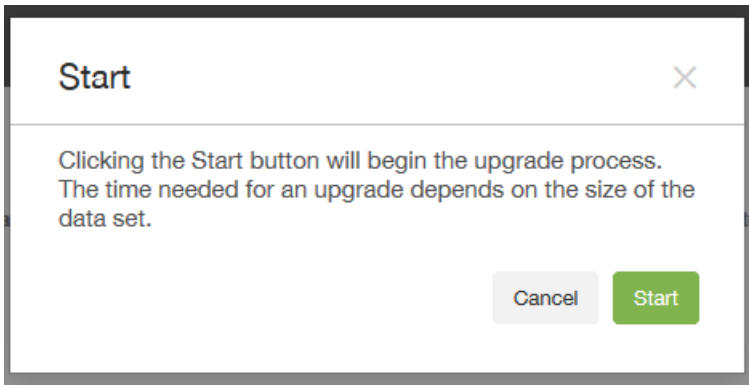
注意：必须加密支持包。

```
[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
```

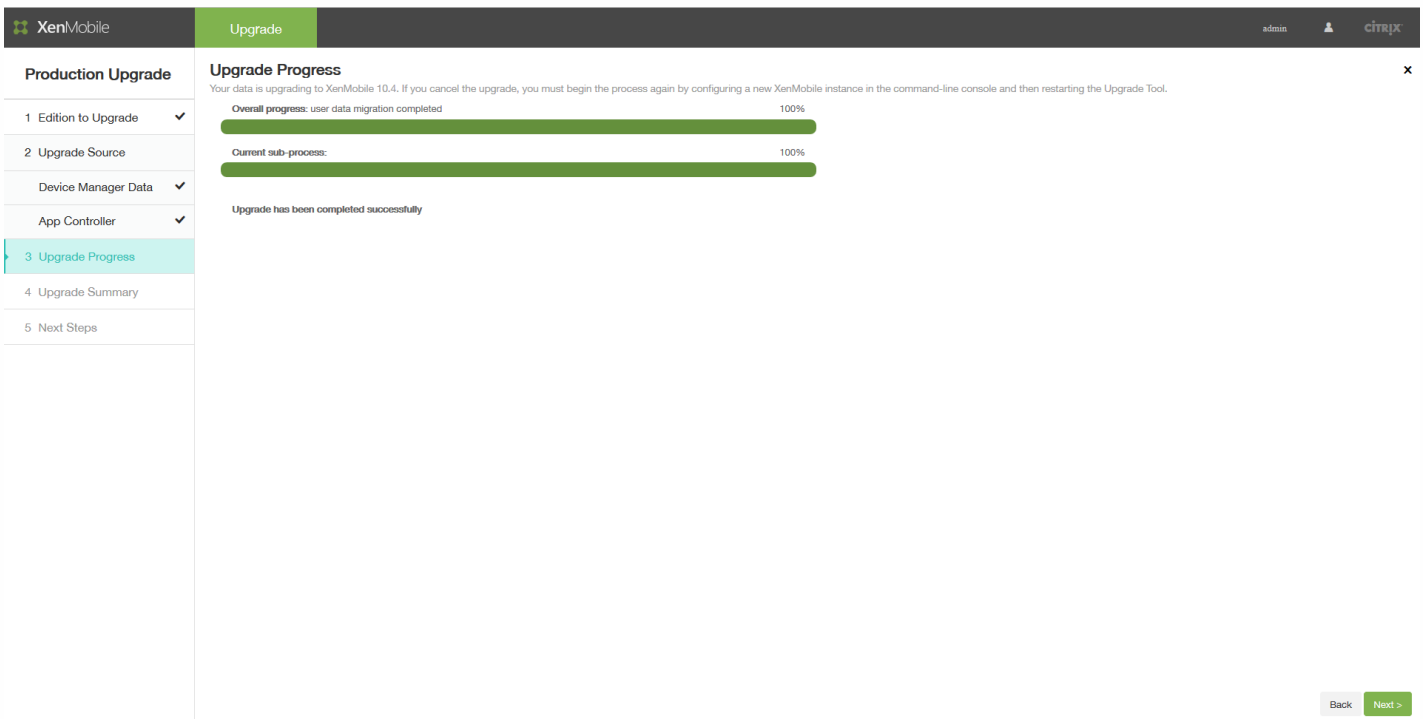
26. 在 **App Controller** 页面的第 3 部分中，指定支持包，然后单击 **Upload**（上载）。

升级工具处理收集的文件（针对 XenMobile Enterprise 和 MAM 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**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 Progress**（升级进度） 页面，让您跟踪从 XenMobile 9.0 进行的数据升级。升级完成时，进度指示条将指示 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 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**下一步**。此时将显示 **Upgrade Summary**（升级摘要） 页面。

如果正在升级 Enterprise 或 MAM Edition ， **Upgrade Summary**（升级摘要） 页面可能类似如下内容所示：

Production Upgrade

Upgrade Summary
Review the upgrade results and debug logs to ensure that all data upgraded successfully to XenMobile 10.4. Be sure to download the log before continuing.

Upgrade log

Devices Upgraded	5
Apps Upgraded	46
Users Upgraded	323
Delivery Groups Upgraded	12
Policies Upgraded	44
Smart Actions Upgraded	0

Cancel Back Next >

如果正在升级 MDM Edition，**Upgrade Summary**（升级摘要）页面可能类似如下内容所示：

Production Upgrade

Upgrade Summary
Review the upgrade results and debug logs to ensure that all data upgraded successfully to XenMobile 10.4. Be sure to download the log before continuing.

Upgrade log

Devices Upgraded	604
Apps Upgraded	23
Users Upgraded	316
Delivery Groups Upgraded	5

Cancel Back Next >

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最新版本的 XenMobile 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。

XenMobile
Upgrade
admin

Production Upgrade

- 1 Edition to Upgrade ✓
- 2 Upgrade Source
- Device Manager Data ✓
- App Controller ✓
- 3 Upgrade Progress ✓
- 4 Upgrade Summary ✓
- 5 Next Steps

Next Steps

1. You must configure licenses on XenMobile 10.4 to enable user connections. To do so, go to Configure > Settings > Licensing.
2. If you deployed the server running XenMobile 9.0 in the DMZ, you must change the external DNS for XenMobile to point to the new XenMobile 10.4 server.
3. If you deployed the server running XenMobile 9.0 behind a load balancing NetScaler appliance, in NetScaler, you must configure the load balancing Device Manager instance with the new IP address for the XenMobile 10.4 server.
4. If you deploy XenMobile 10.4 in a cluster, you must use the command-line interface to enable cluster support and then join the new XenMobile nodes.

Note:

Please collect support bundle from a newly upgraded XenMobile server before restarting it:

1. In the command-line console, type 3 and then press Enter to open the Troubleshooting menu.
2. In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu.
3. In the Support Bundle menu, type 2, press Enter to Generate support bundle.

Restart the server. Go to Manage > Device and make sure all devices have been upgraded properly before making any NetScaler changes.

Find more information and procedures in [Upgrading XenMobile](#).

Cancel Back Finish & Restart

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

Feb 27, 2017

升级工具完成操作后，该工具会提供一个常用后续步骤列表。您的环境中需要完成的后续任务会因以下因素而异：已安装的 NetScaler 版本、是否使用 NetScaler for XenMobile 向导来配置 NetScaler 以及 XenMobile 的版本。

请务必查看以下后续任务列表，并完成适用于您的环境的所有任务。

1. 在 XenMobile 上配置许可证以启用用户连接。有关详细信息，请参阅此[过程](#)。
2. 如果在 DMZ 中部署了运行 XenMobile 9.0 的服务器，请更改 XenMobile 的外部 DNS，以指向新的 XenMobile 服务器实例。
3. 如果在负载均衡 NetScaler 设备后面部署了运行 XenMobile 9.0 的服务器，请在 NetScaler 上做以下更改：
 - a. 为升级配置新的负载均衡虚拟服务器。有关详细信息，请参阅此[过程](#)。
 - b. 配置一条地址记录以将 App Controller 服务器 FQDN 指向用于升级的新负载均衡器。有关详细信息，请参阅此[过程](#)。
 - c. 将 Device Manager 负载均衡虚拟服务器改为指向新的 XenMobile 服务器 IP 地址。有关详细信息，请参阅此[过程](#)。
 - d. 将 NetScaler Gateway 更改为指向新的 XenMobile 服务器 FQDN。有关详细信息，请参阅此[过程](#)。
 - e. 只需在以下情况下完成以下任务：
 - 如果将 NetScaler for XenMobile 向导 9 与 NetScaler 11.1、11.0 或 10.5 结合使用；或
 - 如果使用 NetScaler Gateway 10.1（不建议使用）；或
 - 如果为 XenMobile 配置 NetScaler 10.5 或更高版本时未使用 NetScaler for XenMobile 向导。

有关上述情况下应遵循的过程，请参阅 XenMobile 升级工具 10.1 文档中的下列文章：

[根据 SSL 桥接 MDM 配置创建新的 MAM 负载均衡虚拟服务器](#)
[根据 SSL 卸载 MDM 配置创建新的 MAM 负载均衡虚拟服务器](#)

4. 如果在群集中部署 XenMobile 最新版本，则必须使用 XenMobile 命令行接口 (CLI) 启用群集支持，然后加入新的 XenMobile 节点。有关 XenMobile CLI 的帮助，请参阅[群集菜单选项](#)。
5. 根据环境需要完成其余的后续任务。

本文还介绍与 Secure Ticket Authority、网络时间协议 (NTP) 服务器、XenMobile 服务器主机名、未升级的更新信息、自定义应用商店名称和升级后注册 XenMobile 设备等设置有关的后续任务。

XenMobile 最新版本仅支持 Citrix V6 许可。必须新的 XenMobile 控制台中设置本地或远程许可证配置以启用用户连接，如下所述。

1. 下载许可证文件。要执行此操作，请参阅 [Citrix Licensing](#)。
2. 登录到新的 XenMobile 控制台：转至 <https://:4443>。

- 对于 MDM 或 ENT 升级，请使用 XenMobile 9.0 Device Manager 管理员凭据登录。
- 对于 MAM 升级，请使用 XenMobile 9.0 App Controller 管理员凭据登录。

3. 转至设置 > 许可。

Settings > Licensing

Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

License type: Remote license

License server*: lic1.xmlab.net

Port*: 27000

Test Connection

Product name	Status	Active	Total number of licenses	Number used	Type	Expires on
--------------	--------	--------	--------------------------	-------------	------	------------

有关添加本地和远程许可证的详细信息，请参阅[许可](#)。

Important

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。

XenMobile Enterprise Edition 生产升级已升级到 XenMobile 最新版本后，必须为 XenMobile 9.0 App Controller FQDN 配置新的负载均衡虚拟服务器。为此，请使用 NetScaler Gateway 配置工具。

本部分中与 NetScaler Gateway 11.1 有关的示例屏幕与 NetScaler Gateway 11.0 和 10.5 版本的屏幕相似。

1. 单击[流量管理](#) > [负载均衡](#) > [虚拟服务器](#)。

Traffic Management / Load Balancing / Virtual Servers

Virtual Servers

<input type="checkbox"/>	Name	State	Effective State	IP Address	Port
<input type="checkbox"/>	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443

2. 单击添加。

3. 在负载均衡虚拟服务器页面上，配置以下设置，然后单击确定。

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

Protocol*

IP Address Type*

IP Address*

Port*

▶ More

- **名称**：键入新负载均衡器的名称。
- **协议**：设置为 **SSL**。默认值为 **HTTP**。
- **IP 地址**：输入遵循 RFC 1918 的新负载均衡器的 IP 地址，例如 192.168.1.10。
- **端口**：设置为 **443**。

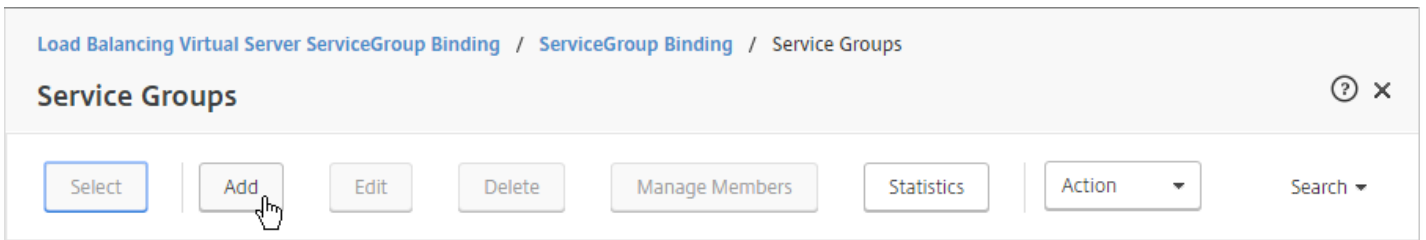
4. 在 **Services and Service Groups**（服务和组）下方，单击 **No Load Balancing Virtual Server Service Group Binding**（无负载均衡虚拟服务器服务组绑定）。

Basic Settings	
Name	MigrationLB
Protocol	SSL
State	UP
IP Address	192.168.1.10
Port	443
Traffic Domain	0
Listen Priority	-
Listen Policy Expression	NONE
Range	1
Redirection Mode	IP
RHI State	PASSIVE
AppFlow Logging	ENABLED
Redirect From Port	
HTTPS Redirect URL	

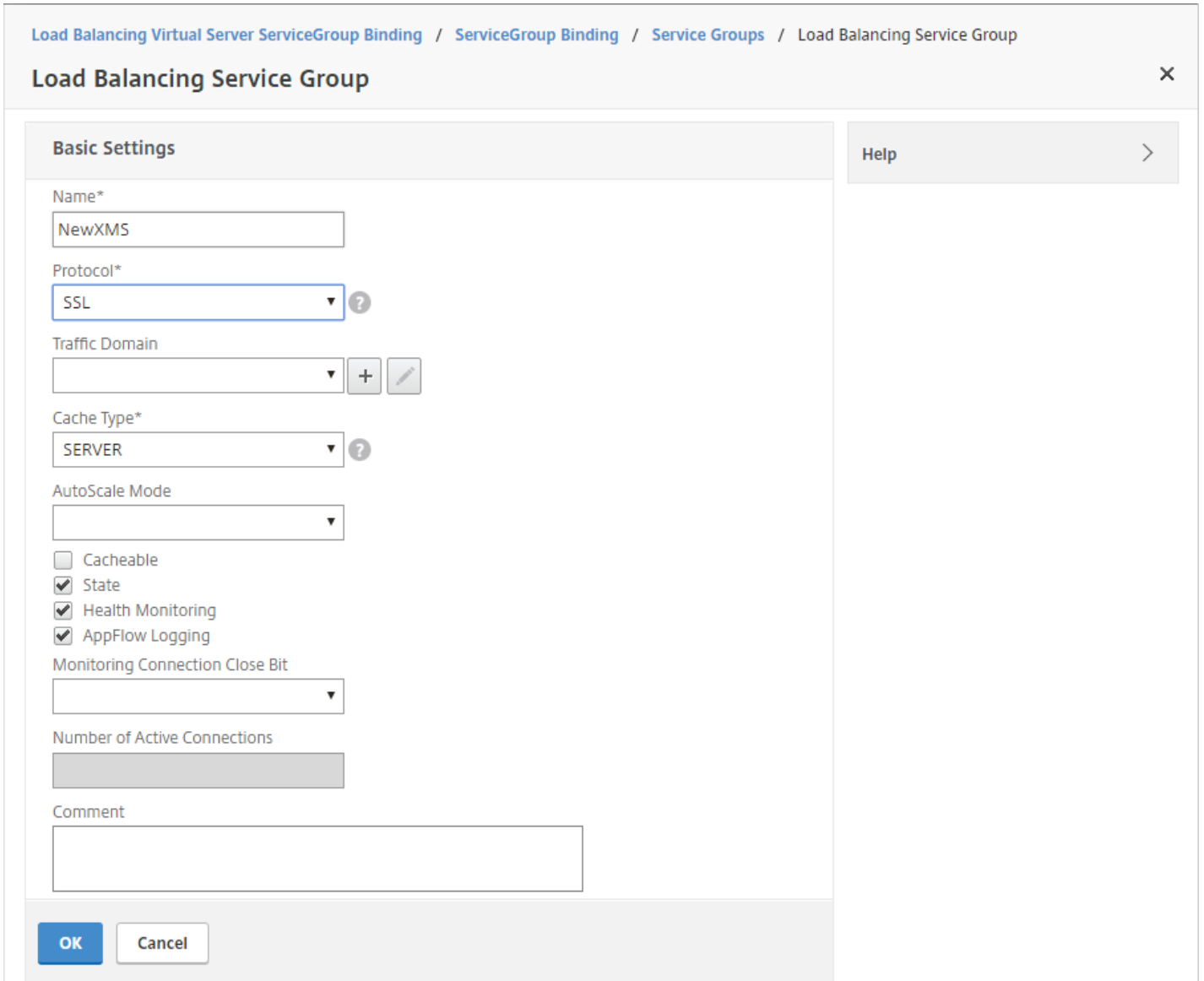
Services and Service Groups	
No Load Balancing Virtual Server Service Binding	>
No Load Balancing Virtual Server ServiceGroup Binding	>

5. 在 **Select Service Group Name**（选择服务组名称）下方，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**（负载均衡服务组）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 **No Service Group Member**（无服务组成员）。

Load Balancing Service Group

Basic Settings

Name	NewXMS	Cache Type	SERVER
Protocol	SSL	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

Service Group Members

No Service Group Member

9. 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)：输入新的 XenMobile 服务器实例的 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 环境迁移到新的 XenMobile 群集环境，请输入当前 XenMobile 服务器的服务器节点 ID。可以登录 XenMobile 服务器命令行接口 (CLI)，然后键入 **1** 转至 **Clustering** (群集) 菜单，以获取服务器节点 ID。CLI 中的服务器节点 ID 标记为 **Current Node ID** (当前节点 ID)。

```
-----
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] 1
Current Node ID: 181356771
```

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups / Load Balancing Service Group / Service Group Members Binding / Create Service Group

Create Service Group Member

IP Based
 Server Based

IP Address/IP Address Range*

10 . 207 . 87 . 38 IPv6 -

Port*

8443

Weight

1

Server Id

181356771

Hash Id

12345

State

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

Load Balancing Virtual Server ServiceGroup Binding / Load Balancing Service Group

Load Balancing Service Group

Basic Settings

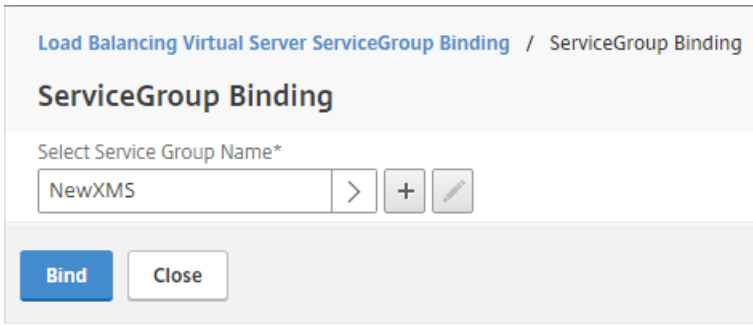
Name	NewXMS	Cache Type	SERVER
Protocol	SSL	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

Service Group Members

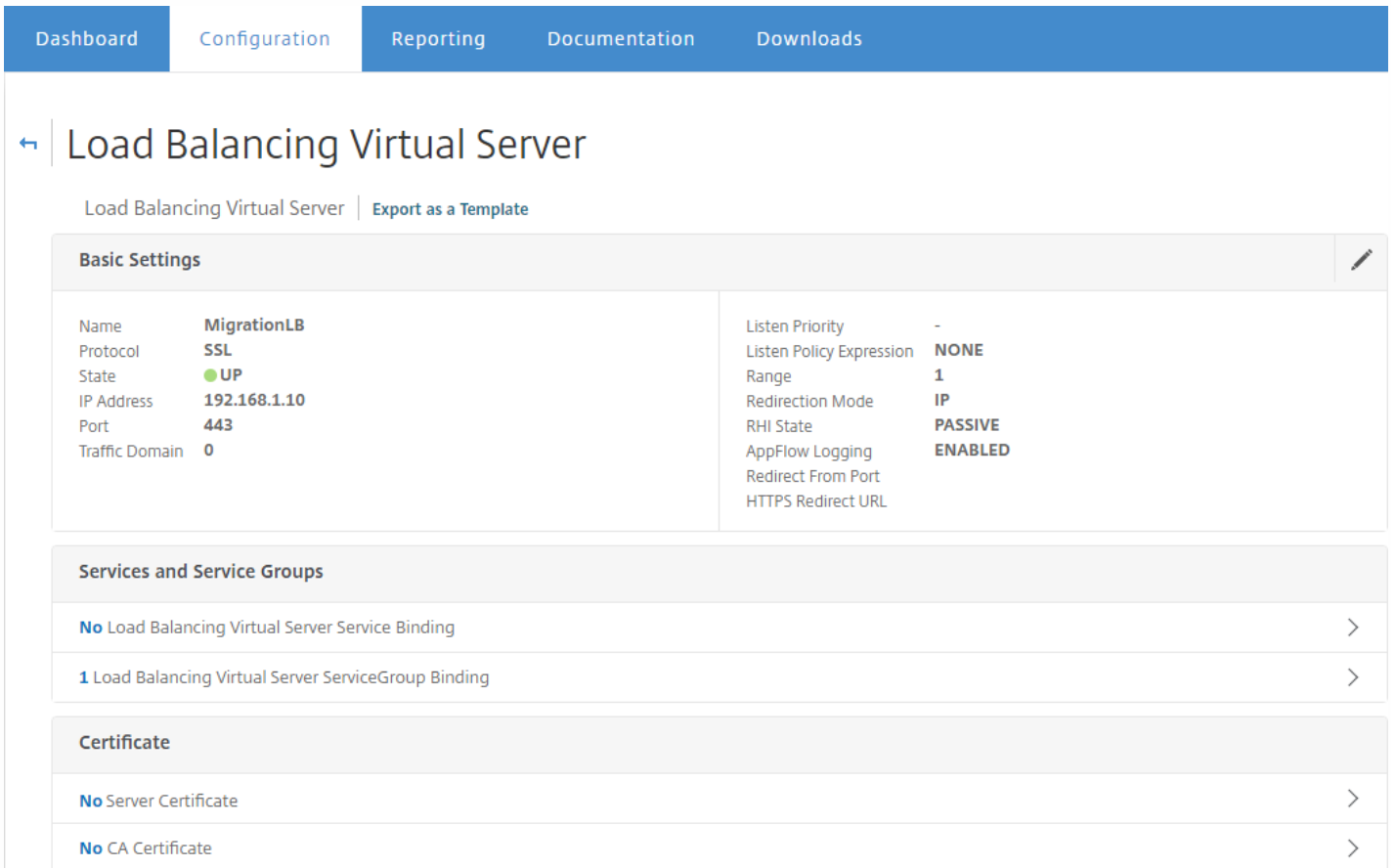
1 Service Group Member

11. 单击 **Done**（完成），然后单击 **OK**（确定）。

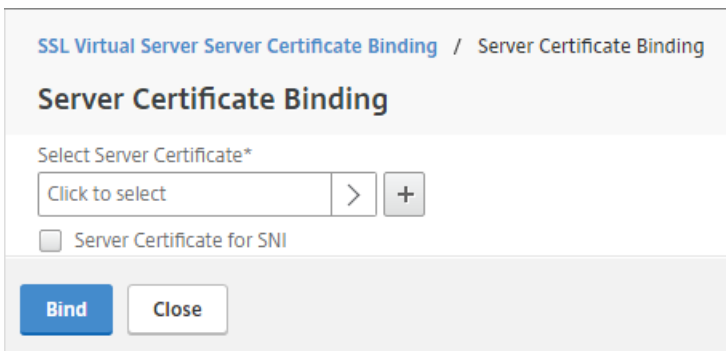
12. 单击 **Bind**（绑定），然后在下一屏幕上单击 **Done**（完成）。



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



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



15. 在 **Certificates** (证书) 下方，单击在[升级工具必备条件](#)中导出的 XenMobile 9.0 服务器证书，单击 **OK** (确定)。

	Name	Common Name	Issuer Name
<input type="radio"/>	ns-sftrust-certificate
<input type="radio"/>	ns-server-certificate
<input type="radio"/>	xs-full	...com	...
<input type="radio"/>	xmlab-server	...net	...

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

Select Server Certificate*

xmlab-server > +

Server Certificate for SNI

Bind Close

← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings ✎

Name	MigrationLB	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● UP	Range	1
IP Address	192.168.1.10	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

Services and Service Groups

- No Load Balancing Virtual Server Service Binding >
- 1 Load Balancing Virtual Server ServiceGroup Binding >

Certificate

- 1 Server Certificate >
- No CA Certificate >

17. 单击刷新按钮以确认服务器已启动。

[Traffic Management](#) / [Load Balancing](#) / [Virtual Servers](#)

Virtual Servers ↻ ? 📄

Add Edit Delete Enable Disable Statistics Action ▾

Search ▾

	Name	State	Effective State	IP Address	Port	Protocol	Method
<input type="checkbox"/>	MigrationLB	● UP	● UP	192.168.1.10	443	SSL	LEASTCONNECT
<input type="checkbox"/>	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443	SSL	LEASTCONNECT
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443	SSL_BRIDGE	LEASTCONNECT
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443	SSL_BRIDGE	LEASTCONNECT

1. 登录到 NetScaler，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)。

注意

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

← Create Address Record

Host Name*
appc-akh3.xmlab.net

IPAddress*
192.168.1.10

TTL (secs)
3600

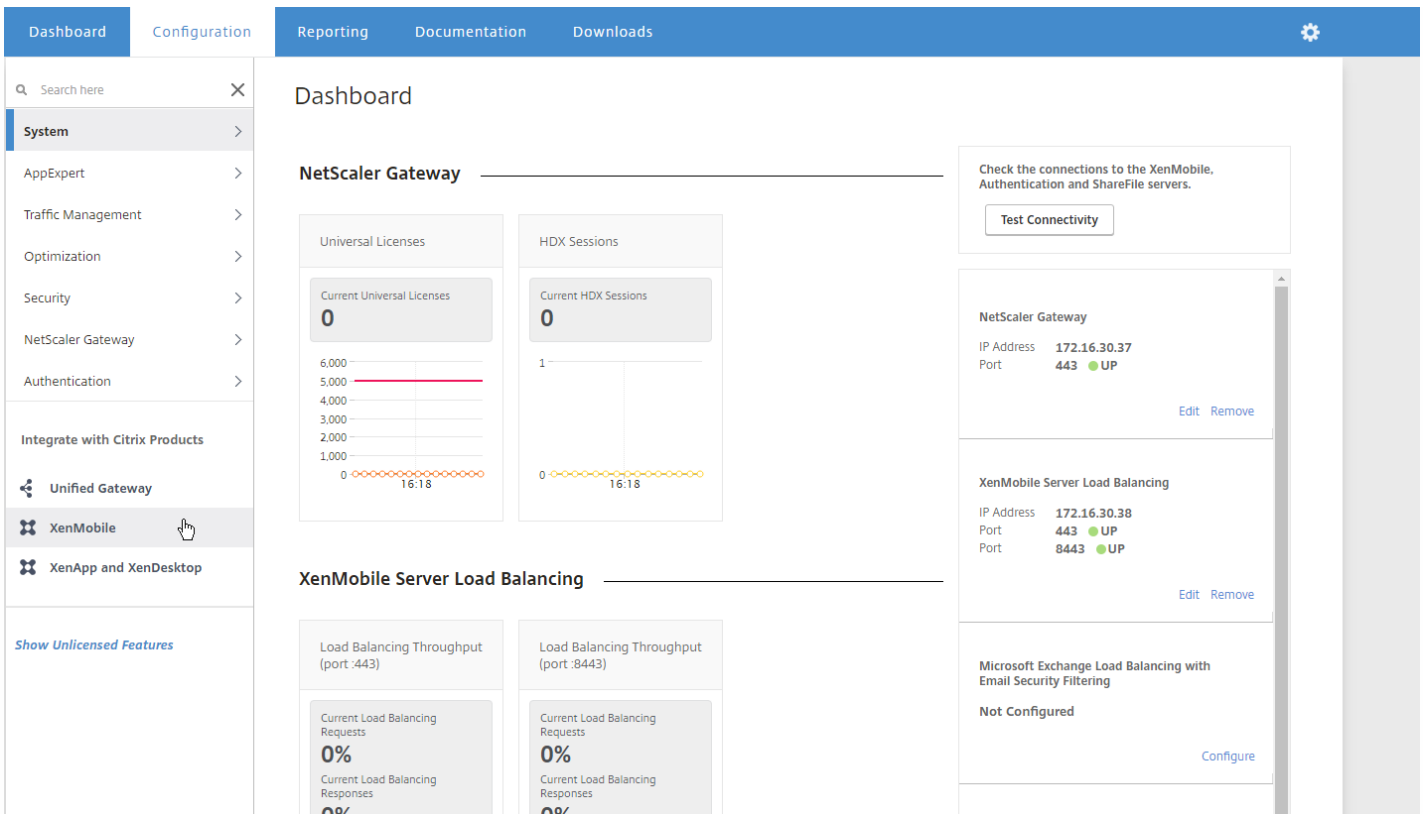
Create Close

如果在负载均衡 NetScaler 设备之后部署运行 XenMobile 9.0 的服务器，则必须使用新的 XenMobile 服务器实例的 IP 地址在 NetScaler 中配置负载均衡 XenMobile 9.0 Device Manager 实例。

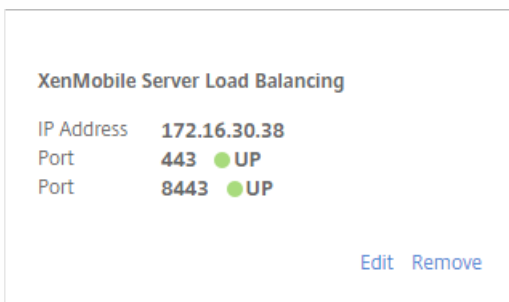
具体配置步骤取决于您在使用 NetScaler 11.1 还是 NetScaler 11.0 或 10.5。

使用 NetScaler 11.1 时

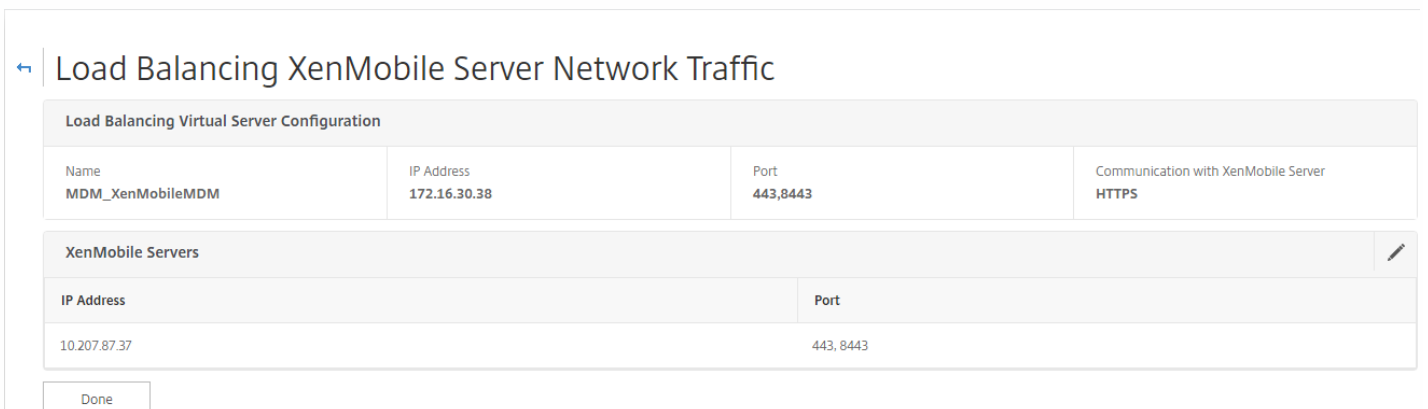
1. 在 **Integrate with Citrix Products** (与 Citrix 产品集成) 下方，单击 **XenMobile**。



2. 在屏幕右侧的 **XenMobile Server Load Balancing** (XenMobile 服务器负载均衡) 下方，单击 **Edit** (编辑)。



此时将显示 **Load Balancing XenMobile Server Network Traffic** (负载均衡 XenMobile 服务器网络流量) 页面。



3. 单击 XenMobile 服务器的铅笔图标，打开这些设置。

← Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration			
Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

XenMobile Servers

Add Server Remove Server

<input type="checkbox"/>	IP Address	Port
<input type="checkbox"/>	10.207.87.37	443, 8443

Continue

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

← Load Balancing XenMobile Server Network Traffic

Load Balancing Virtual Server Configuration			
Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

XenMobile Servers

Add Server Remove Server

<input checked="" type="checkbox"/>	IP Address	Port
<input checked="" type="checkbox"/>	10.207.87.37	443, 8443

Continue

5. 单击 **Add Server**（添加服务器），然后添加新的 XenMobile 服务器 IP 地址。

XenMobile Server IP Addresses

Enter the IP address of the XenMobile server that you want to load balance.

XenMobile Server IP Address*

10 . 207 . 87 . 38

Add Cancel

对于 NetScaler 11.0 或 10.5

1. 在 **Integrate with Citrix Products** (与 Citrix 产品集成) 下方，单击 **XenMobile**。

The screenshot shows the NetScaler Configuration Dashboard. The left sidebar contains a navigation menu with categories like System, AppExpert, Traffic Management, Optimization, Security, NetScaler Gateway, and Authentication. Under 'Integrate with Citrix Products', 'XenMobile' is highlighted. The main dashboard area is titled 'NetScaler Gateway' and includes two charts: 'Universal Licenses' (showing 0 current licenses) and 'HDX Sessions' (showing 0 current sessions). On the right, there are configuration cards for 'NetScaler Gateway' and 'Device Manager Load Balancing'. The 'NetScaler Gateway' card shows IP Address 10.217.232.37 and Port 443 Up. The 'Device Manager Load Balancing' card shows IP Address 10.217.232.39 and Ports 443 Up and 8443 Up. A 'Test Connectivity' button is visible in the top right.

2. 在屏幕右侧的 **Device Manager Load Balancing** (Device Manager 负载平衡) 下方，单击 **Edit** (编辑)。

This is a close-up of the 'Device Manager Load Balancing' configuration card. It displays the following information: IP Address 10.217.232.39, Port 443 Up, and Port 8443 Up. There are 'Edit' and 'Remove' links at the bottom right of the card.

此时将显示 **Load Balancing Device Manager Network Traffic** (负载平衡 Device Manager 网络流量) 页面。

Load Balancing Device Manager Network Traffic

Load Balancing Virtual Server Configuration		
Name	IP Address	Port
MDM_XenMobileMDM	10.217.232.39	443,8443

Device Manager Server IP Addresses		
IP Address	Port	State
10.207.72.216	443, 8443	Up

Done

3. 单击 **Device Manager Server IP Addresses** (Device Manager 服务器 IP 地址) 铅笔图标，打开这些设置。

Device Manager Server IP Addresses		
<input type="button" value="Add Server"/>	<input type="button" value="Remove Server"/>	<input type="button" value="Add from existing servers"/>
IP Address	Port	State
10.207.72.216	443, 8443	Up
<input type="button" value="Continue"/>		

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

Device Manager Server IP Addresses		
<input type="button" value="Add Server"/>	<input type="button" value="Remove Server"/>	<input type="button" value="Add from existing servers"/>
IP Address	Port	State
10.207.72.216	443, 8443	Up
<input type="button" value="Continue"/>		

5. 单击 **Add Server** (添加服务器)，然后添加新的 XenMobile 服务器 IP 地址。

Device Manager Server IP Addresses	
Enter the IP address(es) of the device manager server(s) that you want to load balance. If the server IP address is already added to the NetScaler, click Add from existing servers to select the device manager server IP.	
Device Manager Server IP Address*	
<input type="text" value="10 . 207 . 87 . 38"/>	
<input type="button" value="Add"/>	<input type="button" value="Cancel"/>

此时，NetScaler Gateway 将指向 App Controller FQDN。必须将 NetScaler 更改为指向新的 XenMobile FQDN。XenMobile 最新版本侦听端口 8443 而非端口 443。如果使用 NetScaler for XenMobile 向导 9 设置 NetScaler，必须如下表中的示例所示，同时包括端口号和 FQDN。

XenMobile Enterprise Edition

将 App Controller FQDN 更改为指向新的 XenMobile 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。

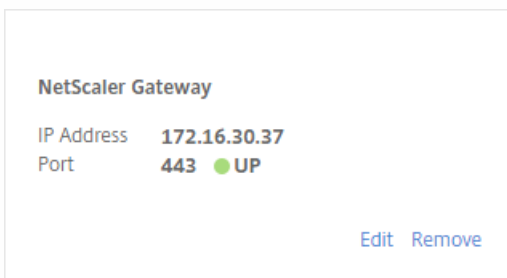
XenMobile 9.0 组件	组件 FQDN	新的 XenMobile Enterprise Edition FQDN
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	不适用
NetScaler Gateway	access.example.com	不适用

XenMobile App Edition

将 App Controller FQDN 更改为指向新的 XenMobile 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。

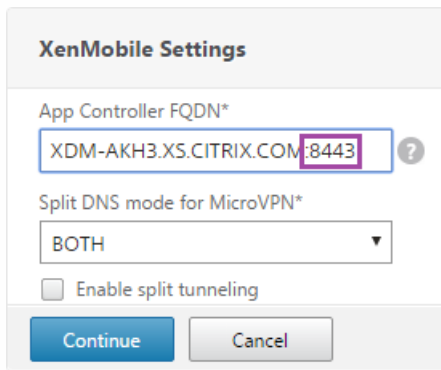
XenMobile 9.0 组件	组件 FQDN	新的 XenMobile Enterprise Edition FQDN
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	不适用

1. 在 **Integrate with Citrix Products** (与 Citrix 产品集成) 下方，单击 **XenMobile**。
2. 在 **NetScaler Gateway** 下方，单击 **Edit** (编辑)。



3. 单击 **XenMobile Settings** (XenMobile 设置) 旁边的铅笔图标，然后将 App Controller FQDN 更改为 XenMobile 服务器

FQDN 并将 **:8443** 附加到 FQDN。例如，**SAMPLE-XENMOBILE.FQDN.COM:8443**。



XenMobile Settings

App Controller FQDN*
XDM-AKH3.XS.CITRIX.COM:8443 ?

Split DNS mode for MicroVPN*
BOTH

Enable split tunneling

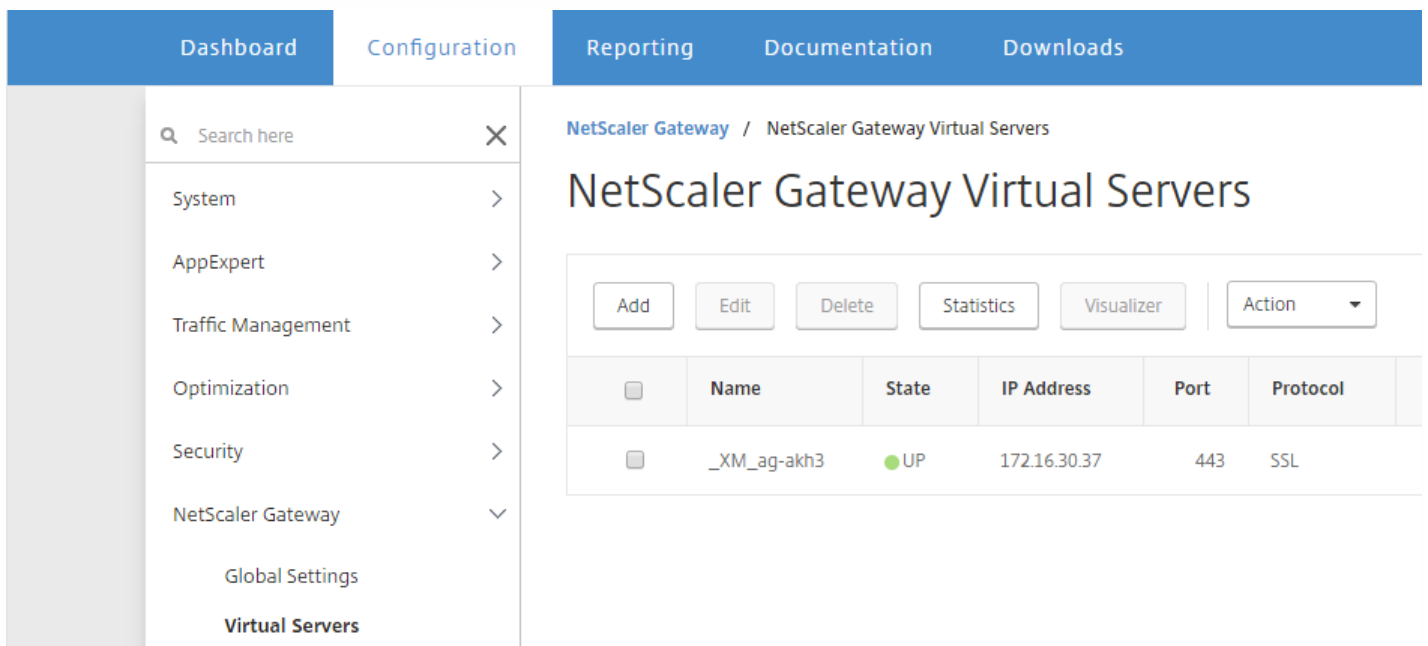
Continue Cancel

4. 单击 **Continue** (继续) 和 **Finish** (完成)。

接下来，必须将解析运行 Secure Ticket Authority 的服务器的 FQDN 的 DNS 更新为 XenMobile 服务器实例的 IP 地址。有时，在后续条件发生变化后，Secure Ticket Authority 服务器并未在 NetScaler 中绑定，尽管它仍旧显示在 **VPN Virtual Server STA Server Binding** (VPN 虚拟服务器 STA 服务器绑定) 列表中。

这时，请在 NetScaler Gateway 中添加运行 Secure Ticket Authority 的服务器的 IP 地址或 FQDN，具体如下所示：

1. 单击 **Netscaler Gateway > Virtual Servers** (虚拟服务器)。



Dashboard Configuration Reporting Documentation Downloads

Search here

System >
AppExpert >
Traffic Management >
Optimization >
Security >
NetScaler Gateway >
Global Settings
Virtual Servers

NetScaler Gateway / NetScaler Gateway Virtual Servers

NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action

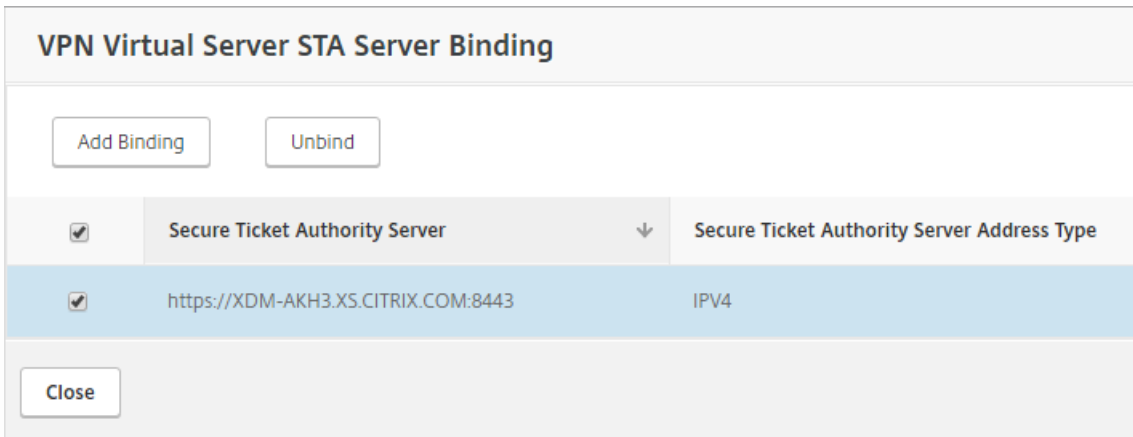
<input type="checkbox"/>	Name	State	IP Address	Port	Protocol
<input type="checkbox"/>	_XM_ag-akh3	UP	172.16.30.37	443	SSL

2. 确保 NetScaler Gateway 虚拟服务器处于 **Up** (正常运行) 状态。选择已配置的 Netscaler Gateway 虚拟服务器，然后单击 **Edit** (编辑)。

3. 在 **Published Applications** (已发布的应用程序) 下方，单击 **STA server** (STA 服务器)。

Published Applications
No Next HOP Server
1 STA Server
No Url

4. 记下 **Secure Ticket Authority Server** (Secure Ticket Authority 服务器) 的 URL，在步骤 6 中需要输入该 URL。然后选择列表中的 Secure Ticket Authority 服务器。



5. 单击 **Unbind** (取消绑定)，然后单击 **Add Binding** (添加绑定)。

6. 在 **Secure Ticket Authority Server** (Secure Ticket Authority 服务器) 字段中，键入在步骤 4 中记下的 URL。

7. 依次单击 **Bind** (绑定)、**Close** (关闭) 和 **Done** (完成)。

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。

如果 XenMobile 9.0 主机名含有大写字母，请完成以下步骤，以确保移动设备能够访问 Citrix Store：

1. 在新的 XenMobile 控制台中，转至 **设置 > 服务器属性**。

2. 单击 **添加**，然后填写以下字段：

- **键**：选择自定义键。
- **键**：输入 **host.name.uselowercase**。
- **值**：输入 **true**。
- **显示名称**：输入键的说明。

Settings > Server Properties > Add New Server Property

Add New Server Property

Key	Custom Key ?
Key*	host.name.uselowercase
Value*	true
Display name*	Use lowercase for host name
Description	

3. 重新启动 XenMobile 服务器。

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

执行本地升级时，RBAC 设置会出现问题。有关信息，请参阅[已知问题](#)。

- 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

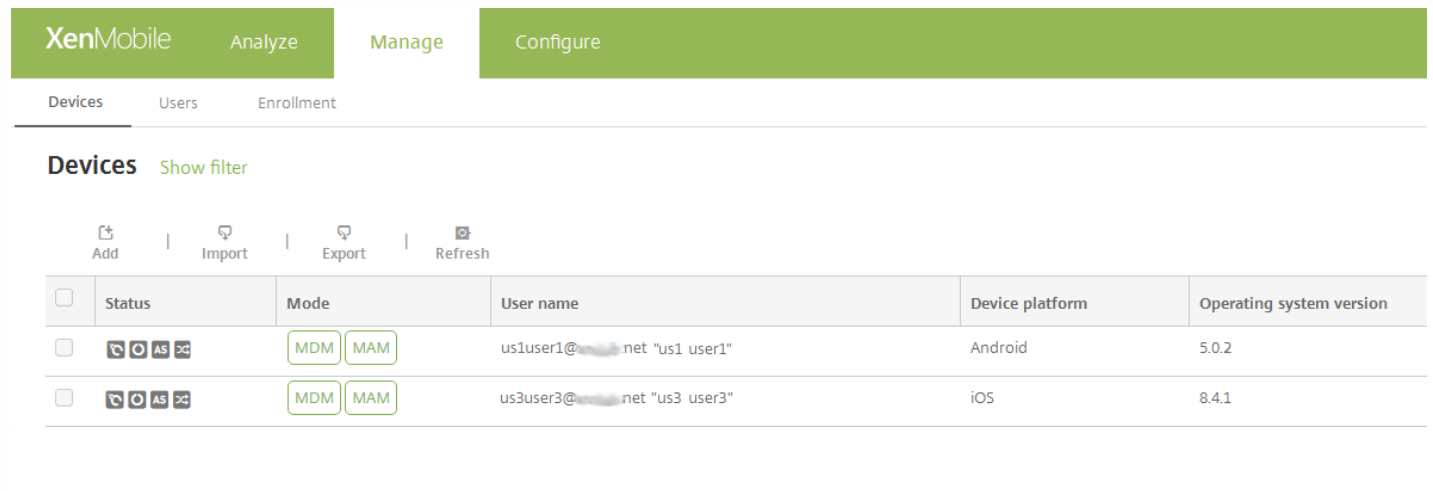
升级前需要执行的一个必备步骤是将自定义 Citrix Store 名称改回默认值。如果未完成该必备操作，则必须在使用最新版本的 XenMobile 服务器之前按照以下后续必备步骤之一进行操作：

- 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 Citrix Secure Hub (以前称为 Worx Home) 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>。

生产升级到 XenMobile 最新版本后，用户不需要重新注册其设备。设备应根据检测信号时间间隔自动连接到新的 XenMobile 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。

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。



The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: "XenMobile", "Analyze", "Manage", and "Configure". Below these are sub-tabs: "Devices", "Users", and "Enrollment". The "Devices" tab is active, and a "Show filter" link is visible. Below the navigation, there are icons for "Add", "Import", "Export", and "Refresh". The main content is a table with the following columns: "Status", "Mode", "User name", "Device platform", and "Operating system version". There are two rows of device data.

Status	Mode	User name	Device platform	Operating system version
	MDM MAM	us1user1@...net "us1 user1"	Android	5.0.2
	MDM MAM	us3user3@...net "us3 user3"	iOS	8.4.1

将 MTC 租户服务器升级到 XenMobile

Feb 27, 2017

如果 XenMobile 9.0 MDM 或 Enterprise Edition 启用了 Multi-Tenant Console (MTC)，则可以将 MTC 管理的 XenMobile 9 实例迁移到独立的 XenMobile 最新版本实例。XenMobile 10.x 不支持 MTC，因此，必须单独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 最新版本实例。
3. 如果未对 MTC 租户启用任何端口映射，请执行下列操作：
 - a. 确保对于新的 XenMobile 实例，允许使用证书进行 HTTPS 通信的服务器端口（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. 如果启用端口映射，请使用所映射到的端口，而非 XenMobile 服务器所侦听的端口。
4. 在 XenMobile 服务器启动期间，请使用实例名称 **zdm**。
5. 通过 XenMobile 命令行接口启用升级工具时，必须在升级提示中回答 **Yes**。
6. 在要升级的服务器上，从 C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\webapps\tenant-name\WEB-INF\classes 中复制以下文件：
 - ew-config.properties
 - pki.xml
 - variables.xml
7. 从 C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name 中复制以下文件：
 - cacerts.pem.jks
 - https.p12
 - pki-ca-devices.p12
 - pki-ca-root.p12
 - pki-ca-servers.p12
8. 复制 C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xml 的一份副本，并按以下步骤所述修改该文件。
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，但保留端口 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"
```

至：

```
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.pemjks"
```

至：

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

12. 创建一个 .zip 文件，其中包含在步骤 6 至 8 中复制的文件。

13. 如下所述，打开新 XenMobile 服务器的 IP 地址：<https://ipAddress:port/uw/?cloudMode>，其中 *port* 是与证书建立的 HTTPS 连接。升级向导将打开。

14. 按照升级向导中所述步骤，选择 **MDM** 或 **Enterprise**。

对于 **MDM** 升级，向导会提示您上载 .zip 文件。您还必须验证数据库是否正确，并输入 CA 证书的密码。

对于 **Enterprise** 升级，向导会提示您上载适用于 App Controller 的支持包。

15. 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。

16. 更改 NAT，以指向新的服务器。

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

用户帐户、角色和注册

Mar 29, 2017

请在 XenMobile 控制台中的**管理选项卡**和**设置**页面上配置以下项：

- 用户帐户和组
- 用户帐户和组的角色
- 注册模式和邀请

在**管理选项卡**中，可以执行以下操作：

- 单击**用户**手动添加用户帐户，或者使用 .csv 置备文件导入帐户并管理本地组。有关详细信息，请参阅：
 - [添加、编辑或删除本地用户帐户](#)
 - [使用 .csv 置备文件导入用户帐户和置备文件格式](#)
 - [在 XenMobile 中添加或删除组](#)

也可以使用工作流来管理用户帐户创建和删除操作，具体如本文后面的[创建和管理工作流](#)中所述。

- 单击**注册**可以配置最多七种模式并发送注册邀请。每种注册模式均具有自己的安全级别和用户注册自己的设备必须采取的步数。有关详细信息，请参阅：
 - [配置注册模式并启用自助服务门户](#)
 - [在 XenMobile 中启用自动发现以执行用户注册](#)

在**设置**页面上，可以执行以下操作：

- 单击**基于角色的访问控制**，向用户和组分配预定义角色或权限集合。这些权限控制用户对系统功能的访问级别。有关详细信息，请参阅：
 - [使用 RBAC 配置角色](#)
- 单击**通知模板**以在自动化操作、注册和发送给用户的标准通知消息中使用。配置通知模板以通过三种不同的通道发送消息：Secure Hub、SMTP 或 SMS。有关详细信息，请参阅：
 - [创建和更新通知模板](#)

可以手动向 XenMobile 中添加本地用户帐户，也可以使用置备文件导入帐户。有关从置备文件导入用户的步骤，请参阅[使用 .csv 置备文件导入用户帐户](#)。

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

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Manage' tab is active. Below the tabs, there are navigation options for 'Devices', 'Users', and 'Enrollment Invitations'. The 'Users' section is selected, and a search bar is visible. Below the search bar, there are icons for 'Add Local User', 'Import Local Users', 'Manage Local Groups', and 'Export'. A table of users is displayed below, with columns for 'User name', 'First name', 'Last name', 'User type', 'Roles', 'Groups', 'Domain', 'Created', and 'Last authenticated'. The 'administrator' user is listed with 'ADMIN' as the role and 'local' as the domain.

<input type="checkbox"/>	User name	First name	Last name	User type	Roles	Groups	Domain	Created	Last authenticated	▼
<input type="checkbox"/>	administrator				ADMIN		local	6/18/16 10:21 PM	6/18/16 10:21 PM	

添加本地用户帐户

1. 在用户页面上，单击添加本地用户。此时将显示添加本地用户页面。

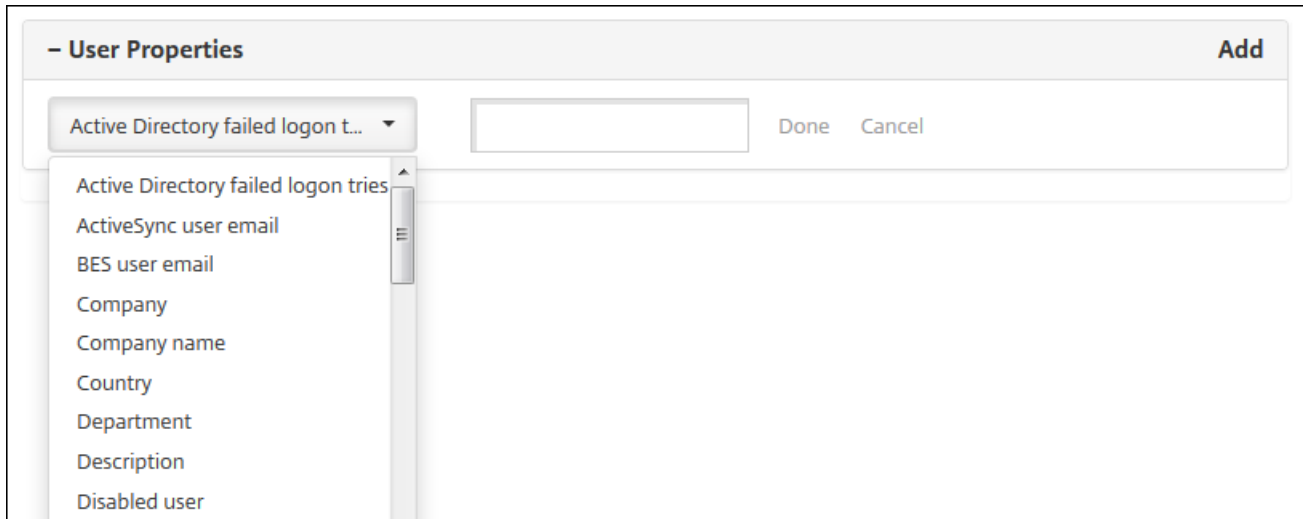
The screenshot shows the 'Add Local User' form in the XenMobile interface. The form is titled 'Add Local User' and is located under the 'Users' tab. It contains four main sections: 'User name*' with a text input field containing 'Enter user name'; 'Password' with a text input field containing 'Enter new password'; 'Role*' with a dropdown menu currently set to 'ADMIN'; and 'Membership' with two checkboxes: 'local\Device Enrollment Program Group' and 'local\MSP'. To the right of the membership section is a blue button labeled 'Manage Groups'. At the bottom of the form is a grey bar with '- User Properties' on the left and 'Add' on the right.

2. 配置以下设置：

- **用户**：键入名称，这是必填字段。可以在名称中包含空格，也可以包含大写和小写字母。
- **密码**：键入可选用户密码。
- **角色**：在列表中，单击用户角色。有关角色的详细信息，请参阅[使用 RBAC 配置角色](#)。可能的选项包括：
 - ADMIN
 - DEVICE_PROVISIONING
 - SUPPORT
 - USER
- **成员身份**：在列表中，单击要添加此用户的一个或多个组。
- **用户属性**：添加可选用户属性。对于您要添加的每个用户属性，请单击**添加**，然后执行以下操作：
 - **用户属性**：在列表中，单击某个属性，然后在该属性旁边的字段中键入用户属性。
 - 单击**完成**保存用户属性或单击**取消**。

注意：要删除现有用户属性，请将鼠标悬停在包含此属性的行上，然后单击右侧的 X。属性立即被删除。

要编辑现有用户属性，请单击属性并进行更改。单击**完成**保存更改后的列表，或者单击**取消**保持列表不发生变化。



3. 单击**保存**。

编辑本地用户帐户

1. 在**用户**页面上的用户列表中，单击以选中某个用户，然后单击**编辑**。此时将显示**编辑本地用户**页面。

2. 适当更改以下信息：

- **用户名**：无法更改用户名。
- **密码**：更改或添加用户密码。
- **角色**：在列表中，单击用户角色。
- **成员身份**：在列表中，单击要添加或编辑此用户帐户的一个或多个组。要从组中删除用户帐户，请取消选中组名称旁边的复选框。
- **用户属性**：请执行以下操作之一：
 - 对于您要更改的各个用户属性，请单击属性并进行更改。单击**完成**保存更改后的列表，或者单击**取消**保持列表不发生变化。
 - 对于您要添加的每个用户属性，请单击**添加**，然后执行以下操作：
 - **用户属性**：在列表中，单击某个属性，然后在该属性旁边的字段中键入用户属性。
 - 单击**完成**保存用户属性或单击**取消**。
 - 对于要删除的每个现有用户属性，请将鼠标悬停在包含此属性的行上，然后单击右侧的 X。属性立即被删除。

3. 单击**保存**保存您的更改，或者单击**取消**保持用户不发生变化。

删除本地用户帐户

1. 在用户页面上的用户帐户列表中，单击以选中某个用户帐户。

注意：可以通过选中每个用户帐户旁边的复选框，选择要删除的多个用户帐户。

2. 单击**删除**。此时将显示确认对话框。
3. 单击**删除**以删除用户帐户或单击**取消**。

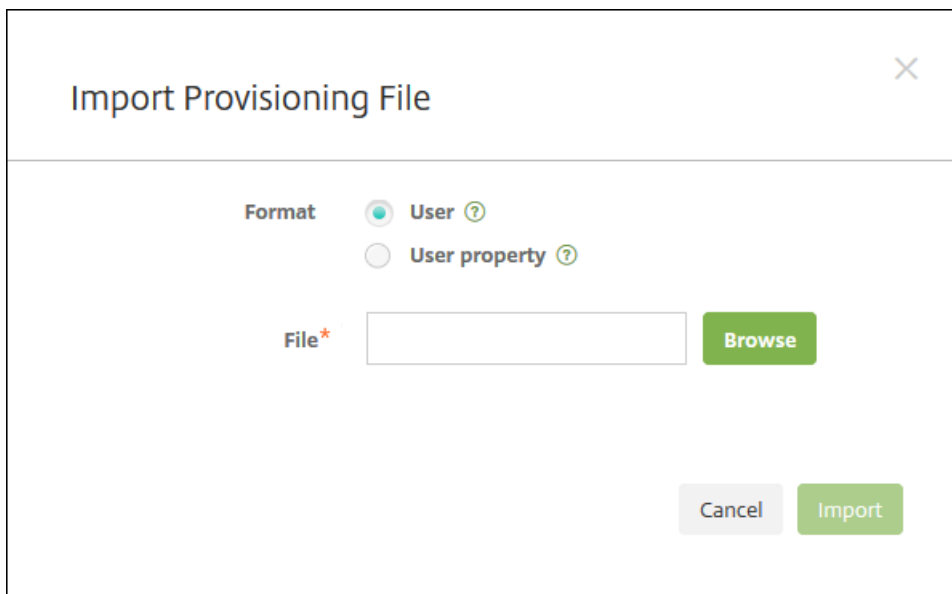
您可以从称为置备文件的 .csv 文件导入本地用户帐户和属性，该文件可以手动创建。有关置备文件格式的信息，请参阅[置备文件的格式](#)。

注意：

- 对于本地用户，请使用域名以及导入文件中的用户名。例如，指定 username@domain。如果在 XenMobile 中将创建或导入的本地用户用于托管域，则用户无法使用对应的 LDAP 凭据进行注册。
- 如果将用户帐户导入到 XenMobile 内部用户目录，请禁用默认域以加快导入过程的速度。请记住，禁用域会影响注册，因此，应在内部用户导入完成后重新启用默认域。
- 本地用户可以采用用户主体名称 (UPN) 格式。但是，Citrix 建议您不要使用托管域。例如，如果 example.com 处于托管状态，请勿使用以下 UPN 格式创建本地用户：user@example.com。

准备好置备文件后，请按照以下步骤将此文件导入到 XenMobile 中。

1. 在 XenMobile 控制台中，单击**管理 > 用户**。此时将显示 **Users**（用户）页面。
2. 单击**导入本地用户**。此时将显示导入置备文件对话框。



The screenshot shows a dialog box titled "Import Provisioning File". It contains a "Format" section with two radio buttons: "User" (selected) and "User property". Below this is a "File*" input field with a "Browse" button. At the bottom, there are "Cancel" and "Import" buttons.

3. 对于要导入的置备文件的格式，选择**用户或属性**。
4. 通过单击**浏览**并导航到置备文件所在的位置，选择该文件。
5. 单击**导入**。

手动创建且用于将用户帐户和属性导入到 XenMobile 中的置备文件必须采用以下格式之一：

- 用户置备文件字段：user;password;role;group1;group2
- 用户属性置备文件字段：user;propertyName1;propertyValue1;propertyName2;propertyValue2

注意：

- 使用分号 (;) 分隔置备文件中的字段。如果某个字段的某一部分包含分号，请使用反斜杠字符 (\) 进行转义。例如，在置备文件中，按照 **propertyV\;test\;1\;2** 形式键入属性 **propertyV;test;1;2**。
- 角色的有效值为预定义的角色 USER、ADMIN、SUPPORT 和 DEVICE_PROVISIONING 以及您定义的任何其他角色。
- 使用句点字符 (.) 作为分隔符来创建组层次结构。请勿在组名称中使用句点。
- 属性置备文件中的属性使用小写。数据库区分大小写。

用户置备内容示例

user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01 条目表示：

- 用户：user01
- 密码：pwd;01
- 角色：USER
- 组：
 - myGroup.users01
 - myGroup.users02
 - myGroup.users.users01

另一个示例 AUser0;1.password;USER;ActiveDirectory.test.net 表示：

- 用户：AUser0
- 密码：1.password
- 角色：USER
- 组：ActiveDirectory.test.net

用户属性置备内容示例

user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value 条目表示：

- 用户：user01
- 属性 1
 - 名称：propertyN
 - 值：propertyV;test;1;2
- 属性 2：
 - 名称：prop 2
 - 值：prop2 value

配置设备注册模式以允许用户在其 XenMobile 中注册其设备。XenMobile 提供七种模式，每种均具有自己的安全级别和用户注册其设备必须执行的步骤。您可以在自助服务门户上提供某些模式。用户可以登录门户并生成可通过其注册自己的设备的注册链接，也可以选择向自己发送注册邀请。在 XenMobile 控制台的 **设置 > 注册** 页面配置注册模式。

从 **管理 > 注册邀请** 页面发送注册邀请。有关信息，请参阅 [发送注册邀请](#)。

注意：如果您计划使用自定义通知模板，必须在配置注册模式之前设置模板。有关通知模板的详细信息，请参阅 [创建或更新通](#)

知模板。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击注册。此时将显示注册页面，其中包含所有可用注册模式的表格。默认情况下，启用所有注册模式。
3. 在列表中选择任何注册模式以对其进行编辑。然后将该模式设置为默认模式、禁用该模式或允许用户通过自助服务门户访问。

注意：选中注册模式旁边的复选框时，选项菜单将在注册模式列表上方显示。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。

The screenshot shows the XenMobile administration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The user is logged in as 'admin'. The breadcrumb trail is 'Settings > Enrollment'. The main heading is 'Enrollment'. Below the heading is a descriptive text: 'Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Worx Home and enroll their devices, or to send themselves an enrollment invitation.' Below this is a table of enrollment modes.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates	▼
<input type="checkbox"/>	User name + Password	✓	✓							
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL	✓			1 day(s)					
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3				
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric		

Showing 1 - 7 of 7 items

可从这些注册模式中选择：

- 用户名 + 密码
- 高安全性
- 邀请 URL
- 邀请 URL + PIN
- 邀请 URL + 密码
- 双重身份验证

- 用户名 + PIN

您可以使用注册邀请来限制仅收到邀请的用户可以注册。

您可以使用一次性 PIN (OTP) 注册邀请作为双重解决方案。OTP 注册邀请控制用户可以注册的设备数。

对于安全要求非常高的环境，您可以通过 SN/UDID/EMEI 将注册邀请关联到设备。双重选项也可用于要求 Active Directory 密码和 OTP。

编辑注册模式

1. 在注册列表中，选择注册模式，然后单击编辑。此时将显示编辑注册模式页面。根据所选择的模式，您会看到不同的选项。

The screenshot shows the 'Edit Enrollment Mode' page in the XenMobile console. The breadcrumb trail is 'Settings > Enrollment > Edit Enrollment Mode'. The page title is 'Edit Enrollment Mode'. The current mode is 'High Security'. The settings are as follows:

Name	Value	Unit/Type
Expire after*	1	Days
Maximum attempts*	3	
PIN Length*	8	Numeric

Notification templates:

Template for	Value
enrollment URL	-- SELECT ONE --
Enrollment PIN	-- SELECT ONE --
enrollment confirmation	-- SELECT ONE --

Buttons: Cancel, Save

2. 适当更改以下信息：

- **此时间后过期**：键入过期期限，此时间后用户将无法注册其设备。此值显示在用户和组注册邀请配置页面。
注意：键入 0 可防止邀请过期。
- **天**：在列表中，单击天或小时，对应于您在此时间后过期中输入的过期期限。
- **最大尝试次数**：键入用户可以尝试注册的次数，超出此次数后用户将被锁定，无法开始注册过程。此值显示在用户和组注册邀请配置页面。
注意：键入 0 表示尝试次数不受限制。

- **PIN 长度**：键入用于设置生成的 PIN 的长度的数字。
- **数字**：在列表中，单击数字或字母数字以选择 PIN 类型。
- **通知模板**：
 - **注册 URL 模板**：在列表中，单击用于注册 URL 的模板。例如，注册邀请模板向用户发送电子邮件或 SMS。方法取决于您是如何配置用于允许用户在 XenMobile 中注册其设备的模板。有关通知模板的详细信息，请参阅[创建或更新通知模板](#)。
 - **注册 PIN 模板**：在列表中，单击用于注册 PIN 的模板。
 - **注册确认模板**：在列表中，单击用于通知用户注册已成功的模板。

3. 单击保存。

将注册模式设为默认模式

将注册模式设为默认模式后，若不选择其他注册模式，此模式将用于所有设备注册请求。如果未将任何注册模式设为默认模式，必须为每个设备注册创建注册请求。

注意：可以用作默认注册模式的注册模式只能是**用户名 + 密码、双重或用户名 + PIN**。

1. 选择默认注册模式：**用户名 + 密码、双重或用户名 + PIN**。

注意：要将某个模式用作默认模式，请先启用它。

2. 单击**默认**。所选模式现已成为默认模式。如果将任何其他注册模式设为默认模式，此模式将不再作为默认模式。

禁用注册模式

禁用注册模式将使此模式不可供用户使用，既不可用于组注册邀请，也不可自助服务门户中提供。通过禁用某种注册模式并启用另一种注册模式，可以更改允许用户注册其设备的方式。

1. 选择注册模式。

注意：无法禁用默认注册模式。如果要禁用默认注册模式，必须首先删除其默认状态。

2. 单击**禁用**。注册模式不再处于启用状态。

在自助服务门户上启用注册模式

通过在自助服务门户上启用注册模式，可允许用户单独在 XenMobile 中注册其设备。

注意：

- 注册模式必须启用并绑定通知模板，才能在自助服务门户上提供。
- 同一时间只能在自助服务门户上启用一种注册模式。

1. 选择注册模式。

2. 单击**自助服务门户**。此注册模式现已在自助服务门户上提供，可供用户使用。已经在自助服务门户上启用的任何模式均不再可供用户使用。

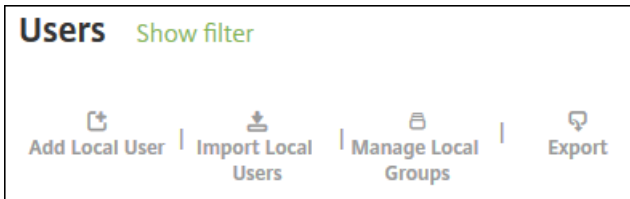
在 XenMobile 控制台中以下页面上的**管理组**对话框中**管理组**：**用户、添加本地用户或编辑本地用户**。没用组编辑命令。

如果删除组，请注意删除组不影响用户帐户。删除组只是删除用户与该组的关联。用户还会丧失此组关联的交付组提供的应用程序或配置文件的访问权限，但是其他组关联性不受影响。如果用户不与任何其他本地组关联，它们将在顶层关联。

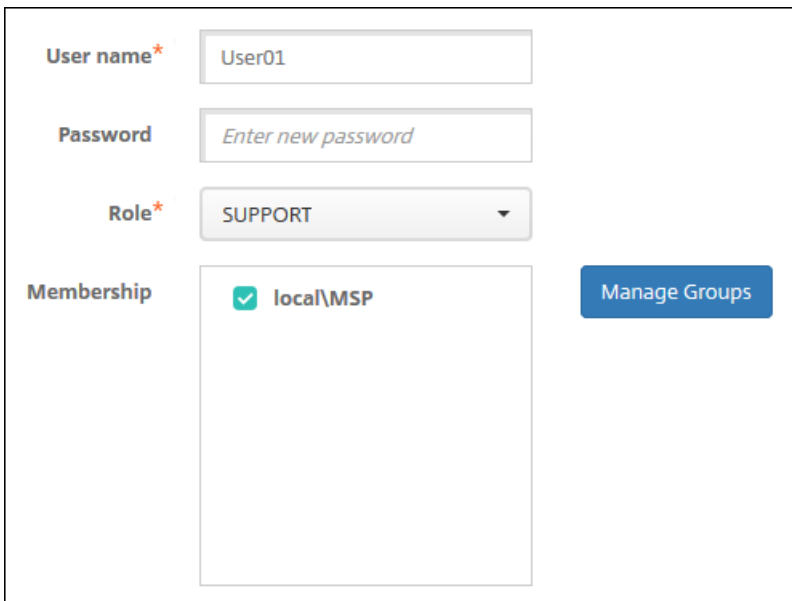
添加本地组

1. 执行以下操作之一：

- 在用户页面上，单击**管理本地组**。

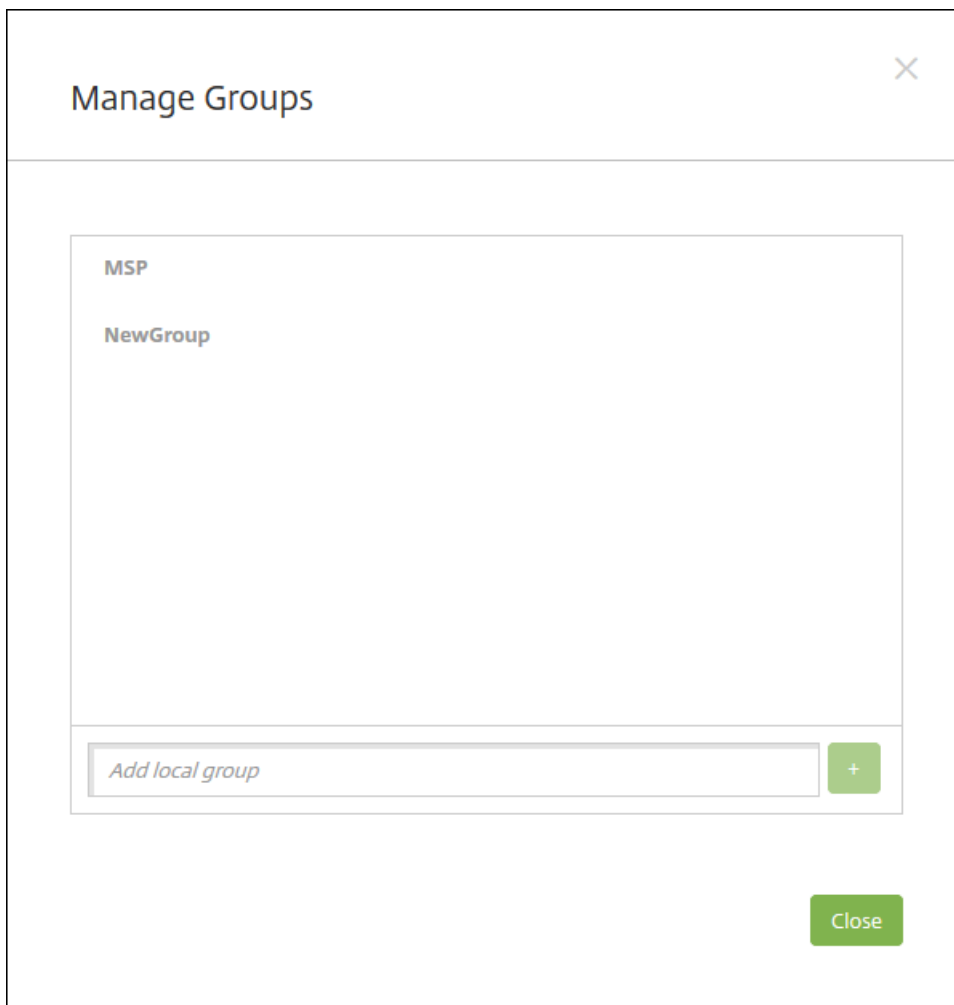


- 在**添加本地用户**页面或**编辑本地用户**页面上，单击**管理组**。



The screenshot shows a form for adding or editing a local user. The fields are: 'User name*' with the value 'User01'; 'Password' with the placeholder 'Enter new password'; 'Role*' with a dropdown menu showing 'SUPPORT'; and 'Membership' with a list containing 'local\MSP' which has a green checkmark next to it. To the right of the membership list is a blue button labeled 'Manage Groups'.

此时将显示**管理组**对话框。



2. 在组列表下方，键入组名称，然后单击加号 (+)。用户组已添加到列表中。

3. 单击关闭。

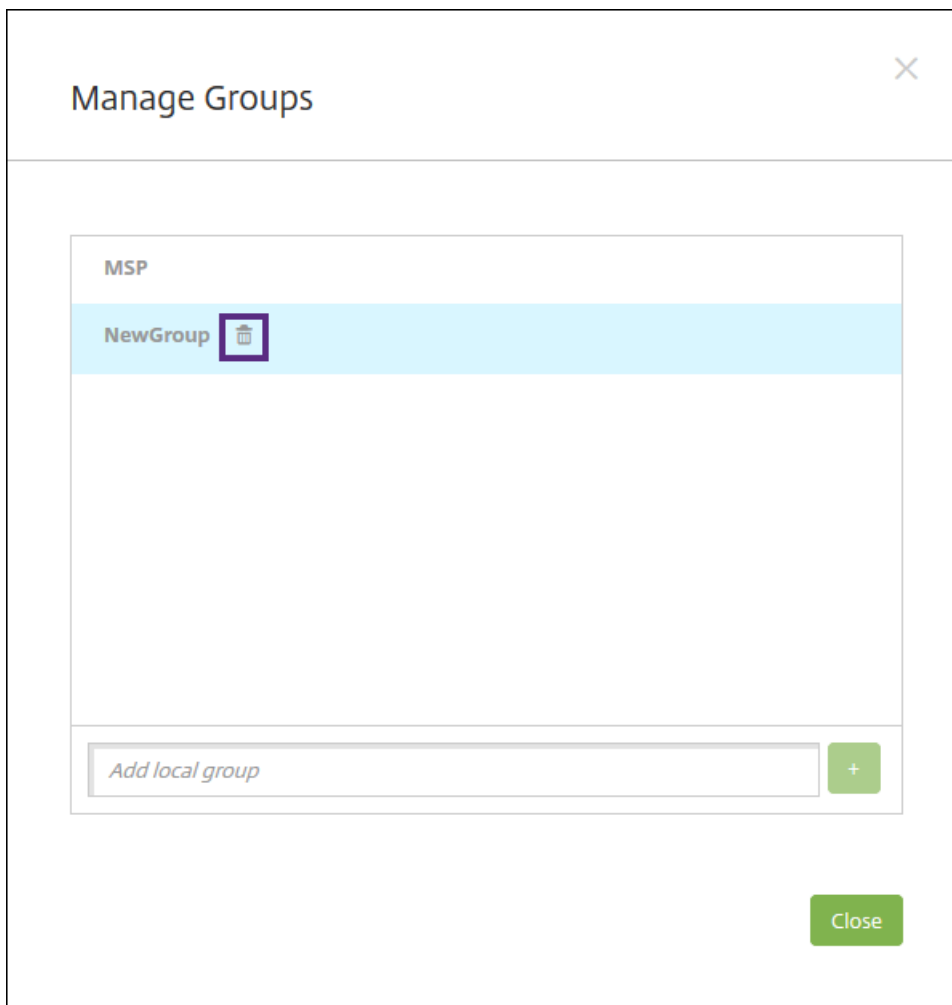
删除组

注意：删除组不会影响用户帐户。删除组只会删除用户与此组的关联。用户还会丧失此组关联的交付组提供的应用程序或配置文件的访问权限，但是其他组关联性不受影响。如果用户不与任何其他本地组关联，它们将在顶层关联。

1. 执行以下操作之一：

- 在用户页面上，单击**管理本地组**。
- 在**添加本地用户页面**或**编辑本地用户页面**上，单击**管理组**。

此时将显示**管理组**对话框。



2. 在管理组对话框上，单击要删除的组。
 3. 单击组名称右侧的垃圾箱图标。此时将显示确认对话框。
 4. 单击删除以确认操作并删除该组。
- 重要：**此操作无法撤消。
5. 在管理组对话框上，单击关闭。

可以使用工作流对用户帐户的创建和删除进行管理。应先确定组织中有权批准用户帐户请求的人员，才能使用工作流。然后可以使用工作流模板创建和批准用户帐户请求。

首次设置 XenMobile 时，要配置工作流电子邮件设置，您必须先配置此设置才能使用工作流。随时可以更改工作流电子邮件设置。这些设置包括电子邮件服务器、端口、电子邮件地址以及创建用户帐户的请求是否需要审批。

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经理审批级别。如果需要其他人员批准用户帐户，可以使用其姓名或电子邮件地址搜索和选择这些人员。XenMobile 找到相应的人员时，您可以将其添加到工作流中。工作流中的所有人员都将收到电子邮件，以批准或拒绝新用户帐户。

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

2. 单击**工作流**。此时将显示**工作流**页面。

3. 单击**添加**。此时将显示**添加工作流**页面。

4. 配置以下设置：

- **名称**：键入工作流的唯一名称。
- **说明**：（可选）键入工作流的说明。
- **电子邮件审批模板**：在列表中，选择要指定的电子邮件审批模板。在 XenMobile 控制台的**设置**下方的**通知模板**部分创建电子邮件模板。单击此字段右侧的眼睛图标，即可预览正在配置的模板。
- **经理审批级别**：在列表中，选择此工作流所需的经理审批级别数。默认值为 **1 级**。可能的选项包括：
 - 不需要
 - 1 级
 - 2 级
 - 3 级
- **选择 Active Directory 域**：在列表中，选择用于工作流的合适的 Active Directory 域。
- **查找所需的其他审批者**：在搜索字段中键入姓名，然后单击**搜索**。源于 Active Directory 的姓名。
- 姓名显示在此字段中后，选中姓名旁边的复选框。姓名和电子邮件地址显示在**选定的其他所需审批者**列表中。
 - 要从列表中删除某个姓名，请执行以下操作之一：
 - 单击**搜索**以查找选定域中的所有人员列表。
 - 在搜索框中键入完整名称或部分名称，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。

5. 单击**保存**。已创建的工作流显示在**工作流**页面上。

创建工作流后，您可以查看工作流详细信息，查看与工作流相关的应用程序，或者删除工作流。工作流创建后无法进行编辑。如果需要不同审批级别或审批者的工作流，请创建另一个工作流。

查看详细信息和删除工作流

1. 在**工作流**页面上的现有工作流列表中，选择一个特定的工作流。为此，请单击列表中的行，或者选中工作流旁边的复选框。

2. 要删除工作流，请单击**删除**。此时将显示确认对话框。再次单击**删除**。

重要：此操作无法撤消。

使用 RBAC 配置角色

Apr 07, 2017

每个预定义的基于角色的访问控制 (RBAC) 角色具有某些与该角色关联的访问权限和功能权限。本文描述其中的每个权限可以执行的操作。要获取每个内置角色的默认权限的完整列表，请下载[基于角色的访问控制默认设置](#)。

应用权限时，您将定义 RBAC 角色具有管理权限的用户组。请注意，默认管理员无法更改应用的权限设置；默认情况下，所应用的权限适用于所有用户组。

进行分配时，要向组分配 RBAC 角色，以使用户组拥有 RBAC 管理员权限。

管理角色	▼
设备置备角色	▼
支持角色	▼
用户角色	▼

使用 RBAC 配置角色

通过 XenMobile 中基于角色的访问控制 (RBAC) 功能，可以向用户和组分配预定义的角色（或称权限集）。这些权限控制用户对系统功能的访问级别。

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

- **管理员**。授予完整系统访问权限。
- **设备置备**。授权访问针对 Windows CE 设备的基本设备管理。
- **支持**。授予对远程支持的访问权限。
- **用户**。供可以注册设备和访问自助服务门户的用户使用。

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

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

注意：本地用户可以仅分配有一个角色。

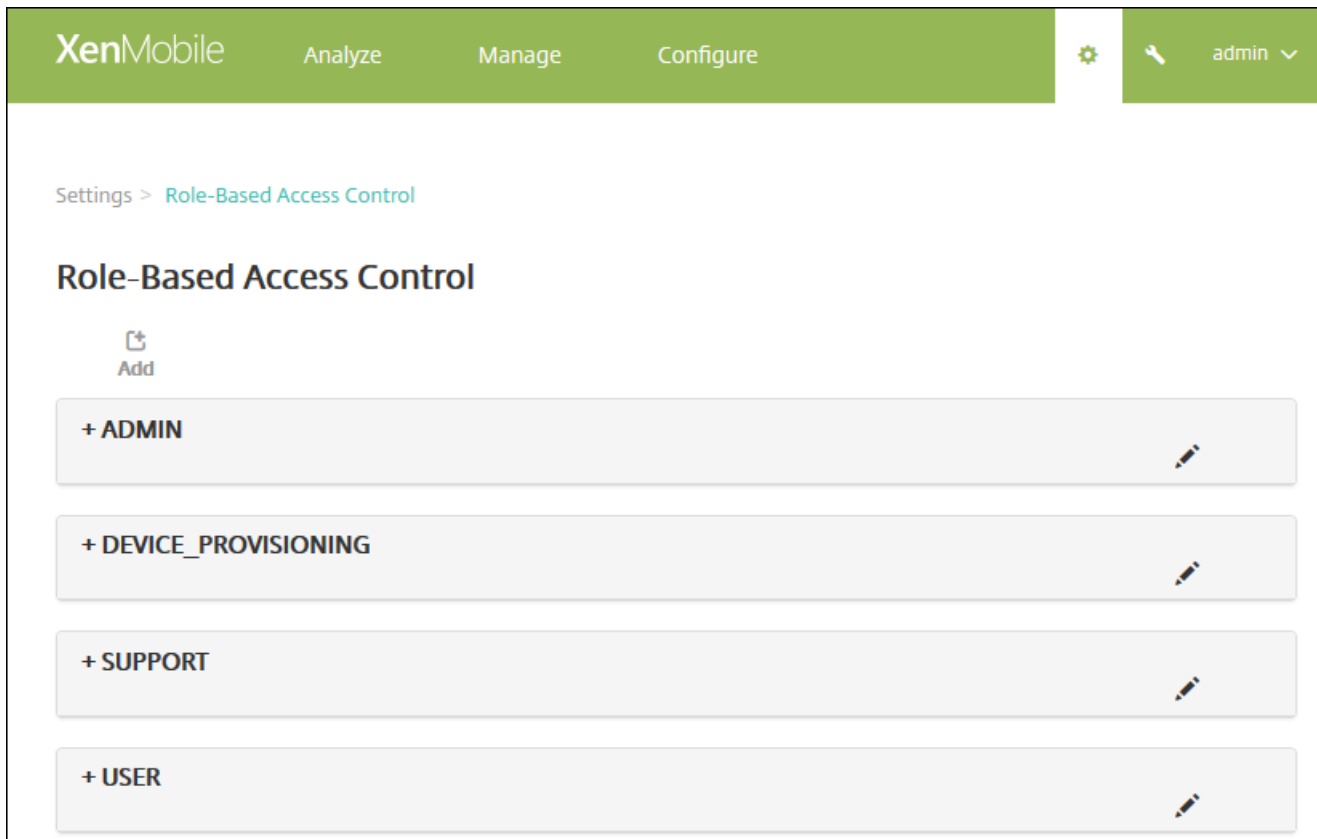
可以使用 XenMobile 中的 RBAC 功能执行以下操作：

- 创建新角色。
- 将组添加到角色。
- 向本地用户分配角色。

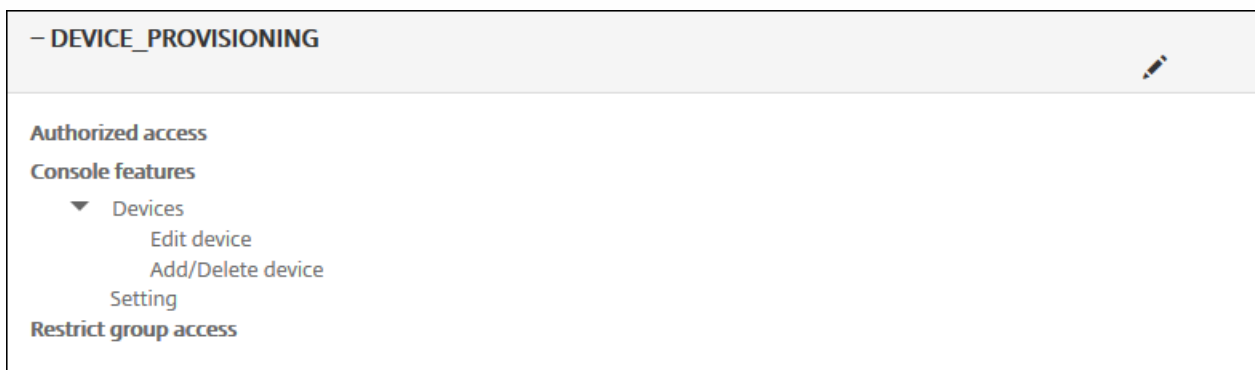
1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。

2. 单击[基于角色的访问控制](#)。此时将显示[基于角色的访问控制](#)页面，其中显示了四种默认用户角色以及您之前添加的任何角

色。



如果单击某个角色旁边的加号 (+)，角色将展开以显示此角色的所有权限，如下图所示。



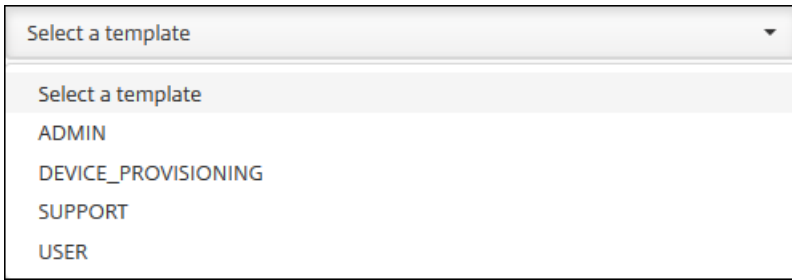
3. 单击添加可添加新用户角色，单击现有角色右侧的铅笔图标可以编辑此角色，单击您之前所定义角色右侧的垃圾箱图标可以删除此角色。无法删除默认用户角色。

- 单击添加或铅笔图标时，将显示添加角色或编辑角色页面。
- 单击垃圾桶图标时，将显示一个确认对话框。单击删除将删除选定角色。

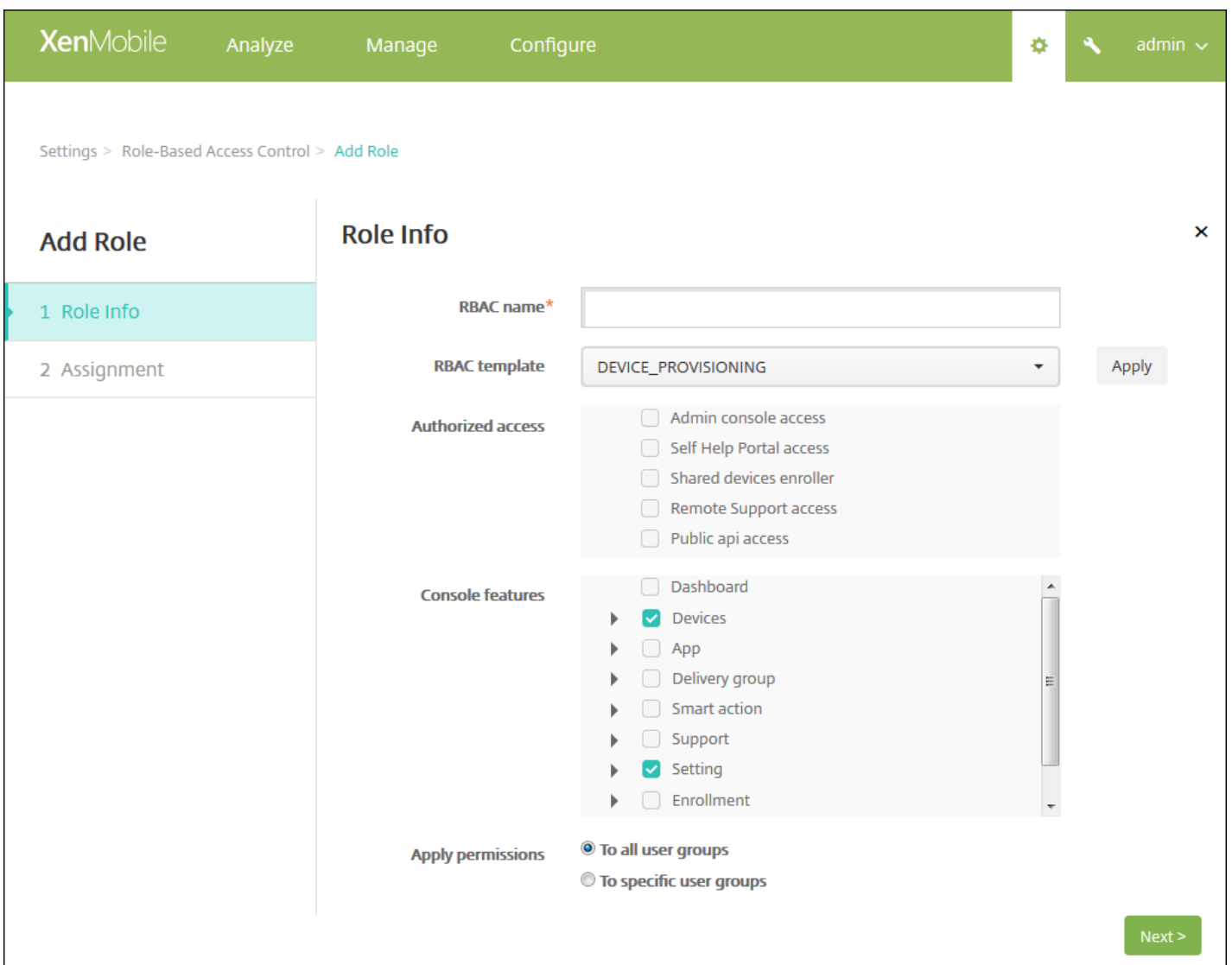
4. 要创建新用户角色或编辑现有用户角色，请输入以下信息：

- **RBAC 名称**：输入新用户角色的描述性名称。无法更改现有角色的名称。
- **RBAC 模板**：可选，单击某个模板以将其作为新角色的起点。如果正在编辑现有角色，则无法选择模板。

RBAC 模板是默认用户角色。它们定义与此角色关联的用户对系统功能的访问权限。选择某个 RBAC 模板后，可以在授权访问和控制台功能字段看到此角色关联的所有权限。使用模板为可选操作；您也可以直接在授权访问和控制台功能字段选择要分配给角色的选项。



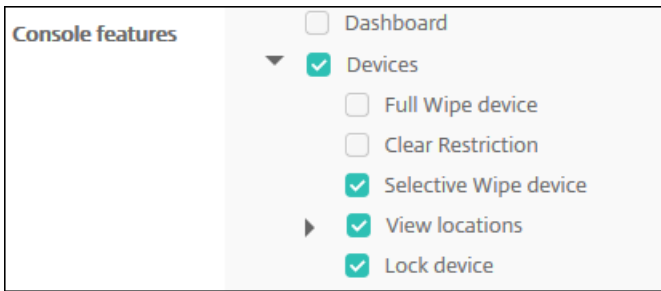
5. 单击 **RBAC 模板** 字段右侧的应用以使用选定模板的预定义访问权限和功能权限填充授权访问和控制台功能复选框。



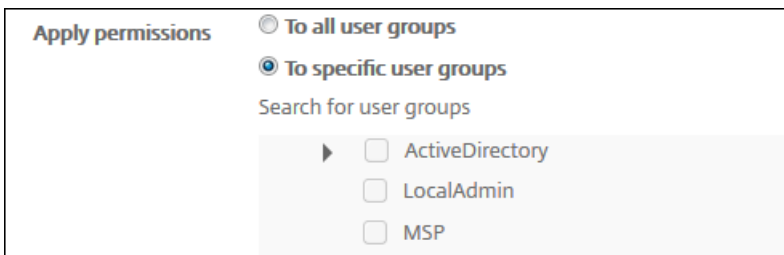
6. 选中或取消选中授权访问和控制台功能复选框可自定义角色。

如果单击某项控制台功能旁边的三角形，将显示特定于此功能的权限，您可以选中或取消选中相应的权限。单击顶层的复选框

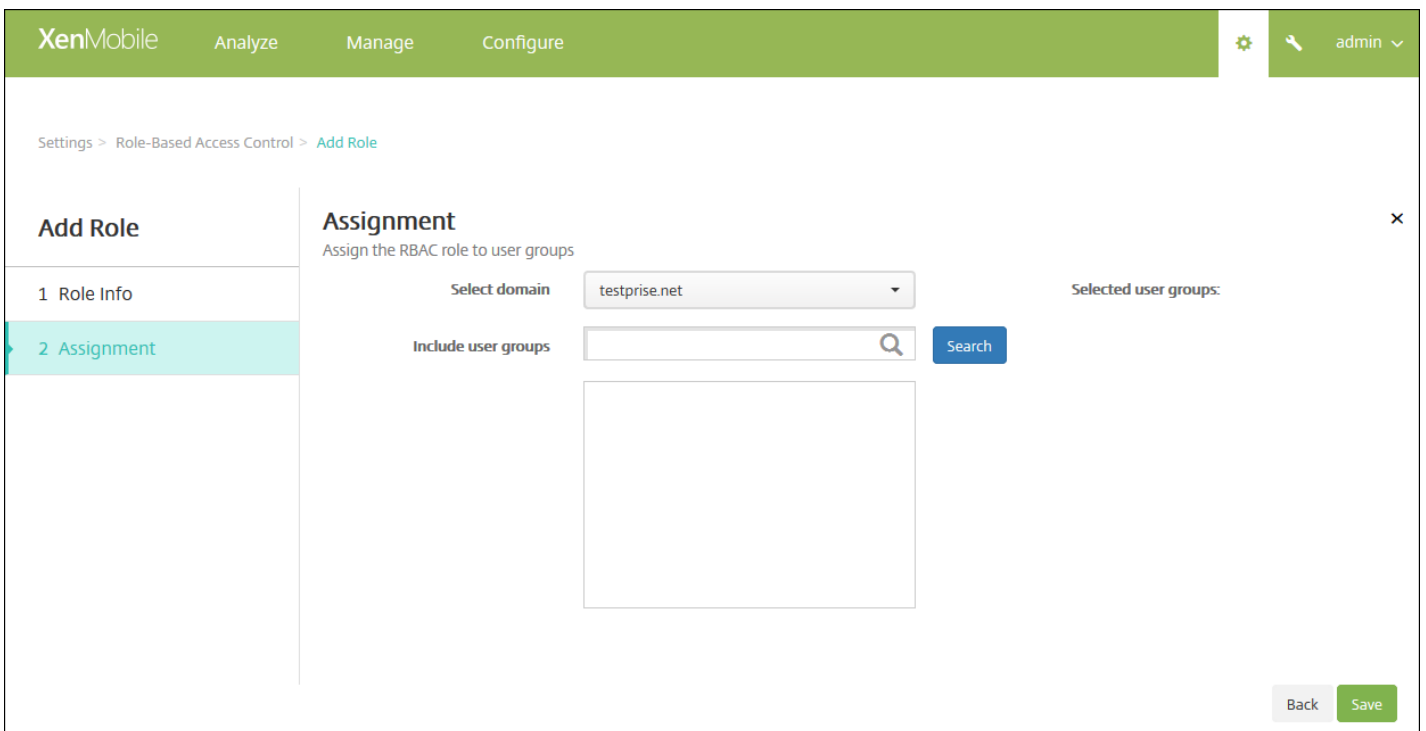
可以阻止访问此控制台部分；您必须选择顶层下面的单独选项，才能启用这些选项。例如，在下图中，完全擦除设备和清除限制选项不会显示在分配给此角色的用户的控制台上，但是，选中的选项会显示。



7.应用权限：选择要向其应用选定权限的组。如果单击至特定用户组，将显示组的列表，您可以从中选择一个或多个组。



8.单击下一步。此时将显示分配页面。



9.输入下列信息，以将角色分配给用户组。

- **选择域**：在列表中，单击某个域。
- **包括用户组**：单击搜索以查看所有可用组的列表，或键入完整或部分组名称以将列表限制为仅显示具有此名称的组。

- 在显示的列表中，选择要向其分配角色的用户组。选择某个用户组后，此组将显示在**选定用户组**列表中。

The screenshot displays the 'Add Role' configuration interface in XenMobile. The left sidebar shows '1 Role Info' and '2 Assignment' (highlighted). The main content area is titled 'Assignment' and includes the following elements:

- Select domain:** A dropdown menu currently showing 'testprise.net'.
- Include user groups:** A search input field containing 'user' and a 'Search' button.
- User Group Selection List:**
 - testprise.net\Remote Desktop Users
 - testprise.net\Performance Monitor Users
 - testprise.net\Performance Log Users
- Selected user groups:** A panel on the right showing the selected groups: 'testprise.net' (header), 'Remote Desktop Users', and 'Performance Monitor Users', each with an 'X' icon for removal.
- Navigation:** 'Back' and 'Save' buttons at the bottom right.

注意：要从选定用户组列表删除用户组，请单击用户组名称旁边的 X。

10. 单击**保存**。

通知

Feb 27, 2017

可以将 XenMobile 中的通知用于以下目的：

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

有关自动化操作的详细信息，请参阅[自动化操作](#)。

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

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

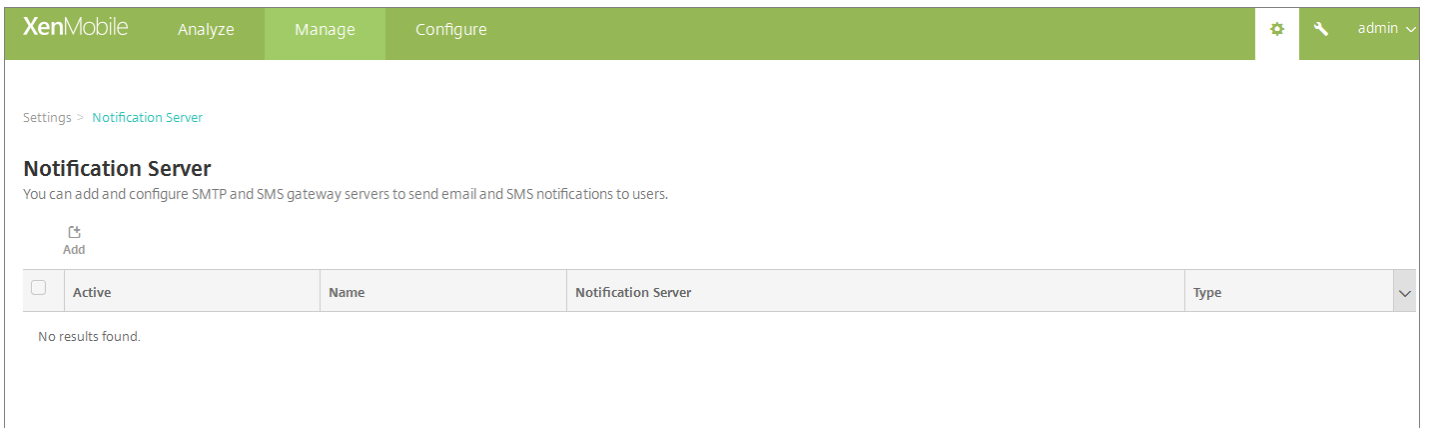
还可以在 XenMobile 中设置运营商 SMS 网关，以配置通过运营商的 SMS 网关发送的通知。运营商使用 SMS 网关发送和接受来往于电信网络的 SMS 传输。这些基于文本的消息使用标准化通信协议，允许固定线路或移动电话设备交换短文本消息。

本文中的过程讨论如何配置 [SMTP 服务器](#) 和 [SMS 网关](#)，以及 [运营商 SMS 网关](#)。

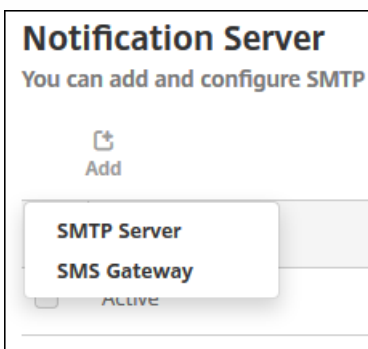
- 配置 SMS 网关之前，请咨询系统管理员以确定服务器信息。了解 SMS 服务器是否托管在内部企业服务器上或者服务器是否属于托管电子邮件服务至关重要。在这种情况下，您需要服务提供商 Web 站点上的信息
- 可配置 SMTP 通知服务器以向用户发送消息。如果此服务器托管在内部服务器上，请联系系统管理员以获取配置信息。如果此服务器是托管的邮件服务，请在服务提供商的 Web 站点上查找适当的配置信息。
- 请确保一次只能激活一个 SMTP 服务器和一个 SMS 服务器。
- 从位于网络的 DMZ 中的 XenMobile 打开端口 25 以指回内部网络上的 SMTP 服务器。这样，XenMobile 能够成功发送通知。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示[设置](#)页面。

2. 在[通知](#)下方，单击[通知服务器](#)。此时将显示[通知服务器](#)页面。



2. 单击添加。此时将显示一个菜单，其中包含用于配置 SMTP 服务器或 SMS 网关的选项。



- 要添加 SMTP 服务器，请单击 **SMTP 服务器**，然后参阅[添加 SMTP 服务器](#)了解配置此设置的步骤。
- 要添加 SMS 网关，请单击 **SMS 网关**，然后参阅[添加 SMS 网关](#)了解配置此设置的步骤。

Settings > Notification Server > [Add SMTP Server](#)

Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
SMTP Server*	<input type="text"/>
Secure channel protocol	<input type="text" value="None"/>
SMTP server port*	<input type="text" value="25"/>
Authentication	<input type="checkbox" value="OFF"/>
Microsoft Secure Password Authentication (SPA)	<input type="checkbox" value="OFF"/>
From name*	<input type="text"/>
From email*	<input type="text"/>

Test Configuration

▶ [Advanced Settings](#)

Cancel

Add

1. 配置以下设置：

- **名称**：键入与此 SMTP 服务器帐户关联的名称。
- **说明**：（可选）输入服务器的说明。
- **SMTP 服务器**：键入服务器的主机名。主机名可以是完全限定的域名 (FQDN) 或 IP 地址。
- **安全通道协议**：在列表中，单击服务器使用的相应安全通道协议（如果服务器配置为使用安全身份验证）**SSL**、**TLS** 或**无**。默认值为**无**。
- **SMTP 服务器端口**：键入 SMTP 服务器使用的端口。默认情况下，此端口设置为 25；如果 SMTP 连接使用 SSL 安全通道协议，则此端口设置为 465。

- **身份验证**：选择开或关。默认值为关。
- 如果启用**身份验证**，可以配置以下设置：
 - **用户名**：键入进行身份验证时使用的用户名。
 - **密码**：键入身份验证用户的密码。
- **Microsoft 安全密码身份验证(SPA)**：如果 SMTP 服务器使用的是 SPA，请单击开。默认值为关。
- **发件人姓名**：键入客户端接收来自此服务器的通知电子邮件时，显示在**发件人**框中的名称。例如，公司 IT。
- **发件人电子邮件**：键入电子邮件收件人回复 SMTP 服务器发送的通知时使用的电子邮件地址。

2. 单击**测试配置**以发送测试电子邮件通知。

3. 展开**高级设置**，然后配置以下设置：

- **SMTP 重试次数**：键入 SMTP 服务器发送邮件失败的重试次数。默认值为 5。
- **SMTP 超时**：键入发送 SMTP 请求时等待的持续时间（以秒为单位）。如果频繁出现因超时导致消息发送失败的情况，请增加此值。降低此值时请格外小心；此操作可增加超时次数和未送达的消息。默认值为 30 秒。
- **最大 SMTP 收件人数**：键入 SMTP 服务器发送的每封电子邮件的最大收件人数。默认值为 100。

4. 单击**添加**。

Settings > Notification Server > Add SMS Gateway

Add SMS Gateway

Please consult with your IT department about the server info if the SMS server is hosted on internal corporate server; if this is a hosted email service, the info is available from the service provider's website. Only one SMS server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
Key*	<input type="text"/>
Secret*	<input type="text"/>
Virtual phone number*	<input type="text"/>
HTTPS	<input type="checkbox"/> OFF
Country code	<input type="text" value="Afghanistan +93"/>
Use Carrier Gateway	<input checked="" type="checkbox"/> ON
	<input type="button" value="Test Configuration"/>

注意

XenMobile 仅支持 Nexmo SMS 消息传递。如果还没有使用 Nexmo 消息传递的帐户，请访问其 [Web 站点](#) 以创建帐户。

1. 配置以下设置：

- **名称**：键入 SMS 网关配置的名称。此字段为必填字段。
- **说明**：(可选) 键入配置の説明。
- **密钥**：键入系统管理员在激活帐户时提供的数字标识符。此字段为必填字段。
- **密码**：键入系统管理员提供的密码，当密码丢失或被盗时用于访问您的帐户。此字段为必填字段。
- **虚拟电话号码**：向北美电话号码（前缀为 +1）发送时使用此字段。在此字段中，必须键入 Nexmo 虚拟电话号码，且只能使用数字。可以在 Nexmo Web 站点上购买虚拟电话号码。

- **HTTPS** : 如果是否使用 HTTPS 将 SMS 请求传输到 Nexmo。默认值为关。

重要 : 让 HTTPS 设置为开, 除非 Citrix 支持指导您将其改为关。

- **国家/地区代码** : 在此列表中, 单击贵组织中收件人的默认 SMS 国家/地区代码前缀。此字段始终以 + 符号开头。默认值为阿富汗 **+93**。



2. 单击**测试配置**以使用当前的配置发送测试消息。系统将立即检测并显示连接错误, 如身份验证或虚拟电话号码错误。接收消息的时间范围与移动电话之间发送消息的时间范围相同。

2. 单击**添加**。

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



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

2. 在**通知**下方, 单击**运营商 SMS 网关**。此时将显示**运营商 SMS 网关**页面。



XenMobile Analyze Manage Configure   admin ▾

Settings > Carrier SMS Gateway

Carrier SMS Gateway

 Add |  Detect

<input type="checkbox"/>	Carrier	SMTP domain	Country code	Sending prefix	▾
<input type="checkbox"/>	Alltel	message.alltel.com	+1		
<input type="checkbox"/>	AT&T	txt.att.net	+1		
<input type="checkbox"/>	Boost Mobile	myboostmobile.com	+1		
<input type="checkbox"/>	Bouygues Telecom	mms.bouyguestelecom.fr	+33		
<input type="checkbox"/>	Cingular	cingularme.com	+1		
<input type="checkbox"/>	Metro PCS	mymetropcs.com	+1		
<input type="checkbox"/>	Nextel	messaging.nextel.com	+1		
<input type="checkbox"/>	Orange	websmsmms.orange.fr	+33		
<input type="checkbox"/>	Powertel	ptel.net	+1		
<input type="checkbox"/>	SFR	sfr.fr	+33		

Showing 1 - 10 of 16 items Showing 1 of 2  

3. 执行以下操作之一：

- 单击**检测**以自动发现网关。此时将显示一个对话框，指出没有检测到新的运营商或列出在已注册设备中间检测到的新运营商。
- 单击**添加**。此时将显示添加运营商 **SMS 网关**对话框。

Add a Carrier SMS Gateway ✕

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

Carrier*

Gateway SMTP domain*

Country code*

Email sending prefix

注意：XenMobile 仅支持 Nexmo SMS 消息传递。如果还没有使用 Nexmo 消息传递的帐户，请访问其 [Web 站点](#) 以创建帐户。

4. 配置以下设置：

- **运营商**：键入运营商的名称。
- **网关 SMTP 域**：键入与 SMTP 网关关联的域。
- **国家/地区代码**：在列表中，单击运营商的国家/地区代码。
- **电子邮件发送前缀**：（可选）指定电子邮件发送前缀。

5. 单击**添加**以添加新运营商，或单击**取消**不添加新运营商。

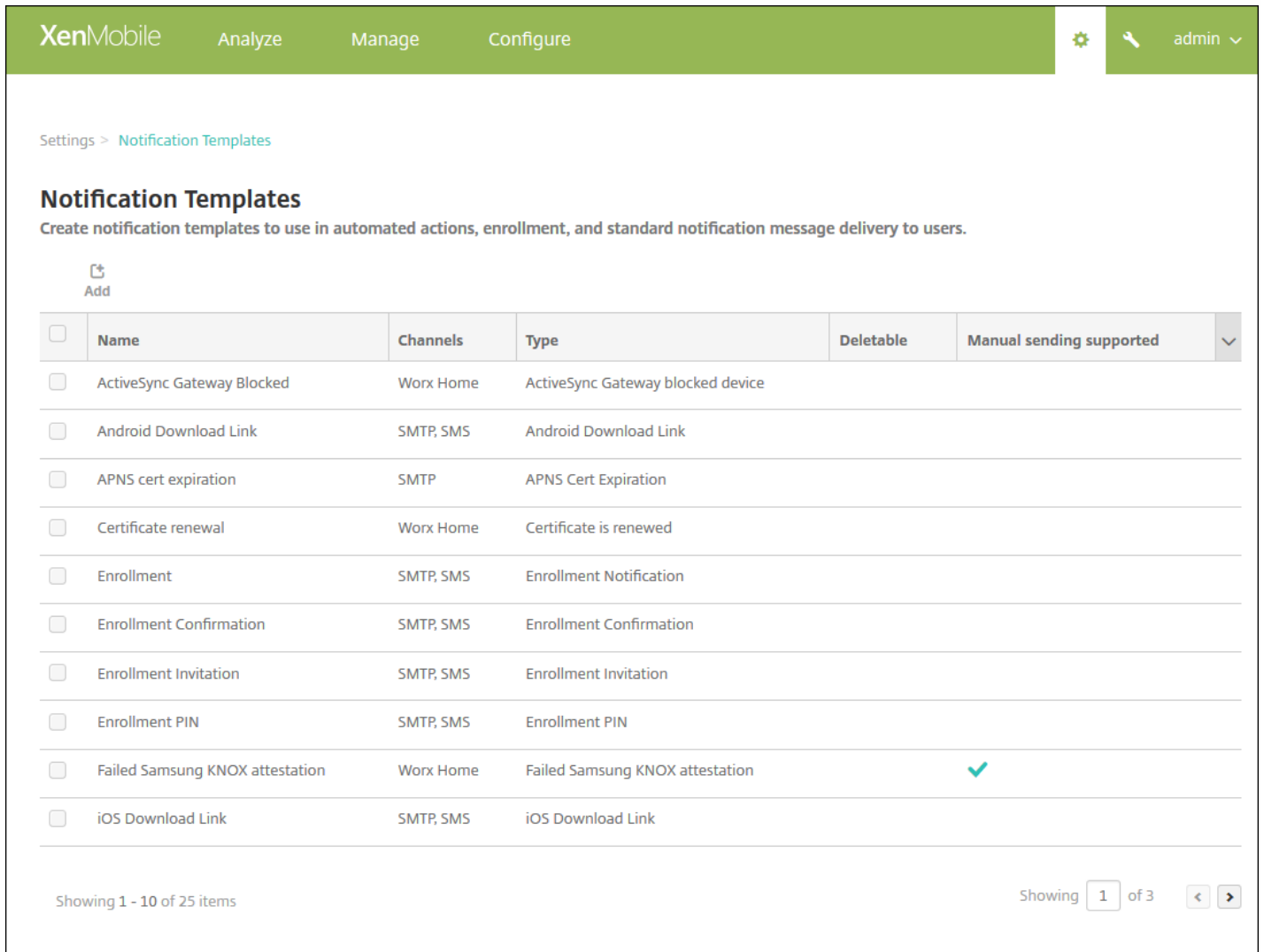
创建和更新通知模板

可以在 XenMobile 中创建或更新用于自动化操作、注册和发送给用户的标准通知消息的通知模板。配置通知模板以通过三种不同的通道发送消息：Secure Hub、SMTP 或 SMS。

XenMobile 包含很多反应不同事件类型的预定义通知模板，XenMobile 会自动针对这些事件类型向系统中的每台设备发出响应。

注意：如果计划使用 SMTP 或 SMS 通道向用户发送通知，必须设置通道后才能将其激活。如果尚未设置通道，当添加通知模板时，XenMobile 会提示您设置通道。

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 单击通知模板。此时将显示通知模板页面。



XenMobile Analyze Manage Configure

Settings > Notification Templates

Notification Templates

Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

Add

<input type="checkbox"/>	Name	Channels	Type	Deletable	Manual sending supported
<input type="checkbox"/>	ActiveSync Gateway Blocked	Worx Home	ActiveSync Gateway blocked device		
<input type="checkbox"/>	Android Download Link	SMTP, SMS	Android Download Link		
<input type="checkbox"/>	APNS cert expiration	SMTP	APNS Cert Expiration		
<input type="checkbox"/>	Certificate renewal	Worx Home	Certificate is renewed		
<input type="checkbox"/>	Enrollment	SMTP, SMS	Enrollment Notification		
<input type="checkbox"/>	Enrollment Confirmation	SMTP, SMS	Enrollment Confirmation		
<input type="checkbox"/>	Enrollment Invitation	SMTP, SMS	Enrollment Invitation		
<input type="checkbox"/>	Enrollment PIN	SMTP, SMS	Enrollment PIN		
<input type="checkbox"/>	Failed Samsung KNOX attestation	Worx Home	Failed Samsung KNOX attestation	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	iOS Download Link	SMTP, SMS	iOS Download Link		

Showing 1 - 10 of 25 items

Showing 1 of 3

添加通知模板

1. 单击**添加**。如果尚未设置任何 SMS 网关或 SMTP 服务器，会显示一条关于使用 SMS 和 SMTP 通知的消息。可以选择立即或稍后设置 SMTP 服务器或 SMS 网关。

如果选择立即设置 SMS 或 SMTP 服务器设置，将重定向到设置页面上的**通知服务器**页面。设置了要使用的通道后，可以返回到**通知模板**页面，继续添加或修改通知模板。

Important

如果选择稍后设置 SMS 或 SMTP 服务器设置，将无法在添加或编辑通知模板时激活这些通道，这意味着这些通道将不能用于发送用户通知。

2. 配置以下设置：

- **名称**：键入模板的描述性名称。
- **说明**：键入模板的说明。
- **类型**：在列表中，单击通知类型。仅显示选定类型支持的通道。仅允许一个 APNS 证书过期模板，此为预定义模板。这表示您无法添加此类型的新模板。

注意：对于某些模板类型，类型的下面会显示短语“支持手动发送”。这表示此模板会显示在控制板和设备页面上的通知列表中，允许您手动向用户发送模板。在“主题”或“消息”字段中使用以下宏的任何模板在任何通道上均不可以使用手动发送。

- `{outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `{outofcompliance.reason(smg_block)}`

3. 在通道下方，配置用于此通知的每个通道的信息。可以选择任何通道或所有通道。您选择的通道取决于您希望发送通知的方式。

- 如果选择 **Secure Hub**，则仅 iOS 和 Android 设备接收通知，通知将显示在设备的通知托盘中。
- 如果选择 **SMTP**，大多数用户应该可以接收邮件，因为他们已使用其电子邮件地址注册。
- 如果选择 **SMS**，则仅使用的设备带有 SIM 卡的用户接收通知。

Secure Hub :

- **激活**：单击以启用通知通道。
- **消息**：键入要发送给用户的消息。如果使用的是 Secure Hub，此字段为必填字段。
- **声音文件**：在列表中，单击用户收到通知时听到的通知声音。

SMTP :

- **激活**：单击以启用通知通道。

重要：如果已设置 SMTP 服务器，则仅可以激活 SMTP 通知。

- **发件人**：键入通知的可选发件人，可以是名称、电子邮件地址或同时包含二者。
- **收件人**：此字段包含除临时通知以外的所有通知的预置宏，以确保将通知发送给正确的 SMTP 收件人地址。Citrix 建议您不要修改模板中的宏。除了用户，您还可以通过添加以分号 (;) 分隔的收件人地址，添加其他收件人（如企业管理员）。要发送临时通知，可以在此页面上输入特定收件人，或从管理 > 设备页面选择设备并从此处发送通知。有关详细信息，请参阅[设备](#)。
- **主题**：键入通知的描述性主题。此字段为必填字段。
- **消息**：键入要发送给用户的消息。

SMS :

- **激活**：单击以启用通知通道。

重要：如果已设置 SMS 网关，则只能激活 SMS 通知。

- **收件人**：此字段包含除临时通知以外的所有通知的预置宏，以确保将通知发送给正确的 SMS 收件人地址。Citrix 建议您不要修改模板中的宏。要发送临时通知，可以输入特定收件人，或从管理 > 设备页面选择设备。
- **消息**：键入要发送给用户的消息。此字段为必填字段。

5. 单击**添加**。正确配置所有通道后，通道将按照以下顺序显示在通知模板页面：SMTP、SMS 和 Secure Hub。未正确配置的通道将在经过正确配置后显示。

编辑通知模板

1. 选择通知模板此时将显示特定于此模板的编辑页面，您可以在此页面上更改类型字段以外的所有内容，以及激活或取消激活通道。

2. 单击保存。

删除通知模板

注意：您只能删除自己添加的通知模板；不能删除预定义通知模板。

1. 选择现有通知模板。

2. 单击删除。此时将显示确认对话框。

2. 单击删除以删除通知模板，或单击取消以取消删除通知模板。

设备

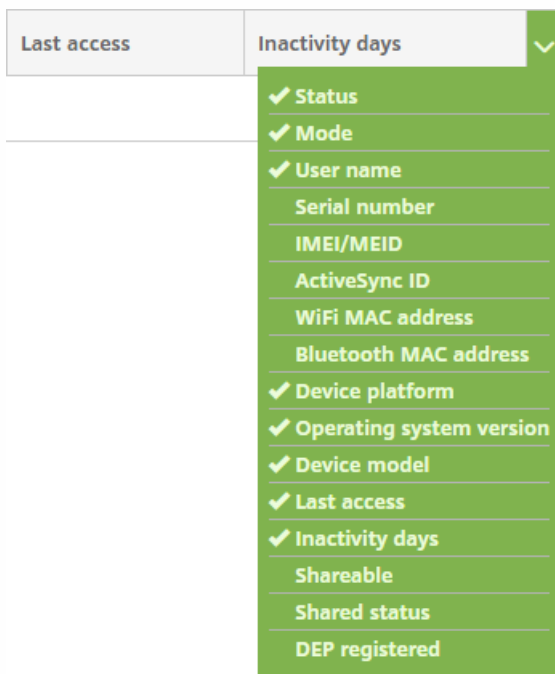
Feb 27, 2017

XenMobile 服务器数据库存储移动设备的列表。唯一的序列号或国际移动设备标识 (IMEI)/移动设备标识符 (MEID) 标识唯一地定义每个移动设备。要将设备填充到 XenMobile 控制台中，可以手动添加设备或从文件导入设备列表。有关设备置备文件格式的详细信息，请参阅[设备置备文件格式](#)。

XenMobile 控制台中的设备页面列出每个设备以及以下信息：

- **状态** (图标指示设备是否已越狱，是否托管，Active Sync Gateway 是否可用以及部署状态)
- **模式** (设备模式是 MDM、MAM 还是两者)
- 与设备有关的其他信息，例如用户名、设备平台、操作系统版本、设备型号、上次访问时间以及不活动天数。这是显示的默认标题。

要自定义设备表，请单击最后一个标题上的向下箭头，然后单击要在表中显示的其他标题，或者取消选中不希望删除的标题。



可以手动添加设备、从设备置备文件中导入设备、编辑设备详细信息、执行安全操作、向设备发送通知以及删除设备。还可以将所有设备表数据导出到 .csv 文件，以创建自定义报告。服务器将导出所有设备属性，如果应用过滤器，XenMobile 会在创建 .csv 文件时使用这些过滤器。

有关管理设备的详细信息，请参阅以下部分：

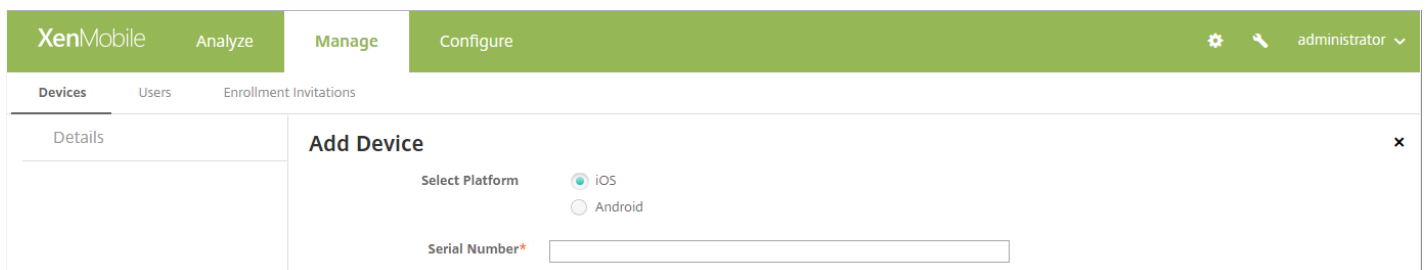
- [手动添加设备](#)
- [从设备置备文件导入设备](#)
- [执行安全操作](#)
- [向设备发送通知](#)
- [删除设备](#)
- [导出设备表](#)
- [手动标记用户设备](#)

- 设备置备文件格式
- 设备属性名称和值

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



2. 单击添加。此时将显示添加设备页面。



3. 配置以下设置：

- 选择平台：单击 **iOS** 或 **Android**。
- 序列号：键入设备序列号。
- **IMEI/MEID**：（可选，仅适用于 Android 设备）键入设备的 IMEI/MEID 信息。

4. 单击添加。设备将添加到所显示的设备表格的列表底部。在此列表中，选择添加的设备，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右侧。

5.常规页面列出设备标识符，例如序列号、 ActiveSync ID 以及平台类型的其他信息。对于设备所有权，请选择公司或 **BYOD**。

常规页面还列出了设备安全属性，例如强 ID、锁定设备、激活锁绕过和平台类型的其他信息。

6.属性页面列出了 XenMobile 要置备的设备属性。此列表显示了用于添加设备的置备文件中包含的任何设备属性。要添加属性，请单击添加，然后从列表中选择一种属性。有关每个属性的有效值，请参阅本文中的[设备属性名称和值](#)。

添加属性时，它最初将显示在添加了该属性的类别下方。单击下一步，然后返回到属性页面后，属性将显示在相应列表中。

要删除某个属性，请将鼠标悬停在列表上方，然后单击右侧的 **X**。XenMobile 将立即删除该项目。

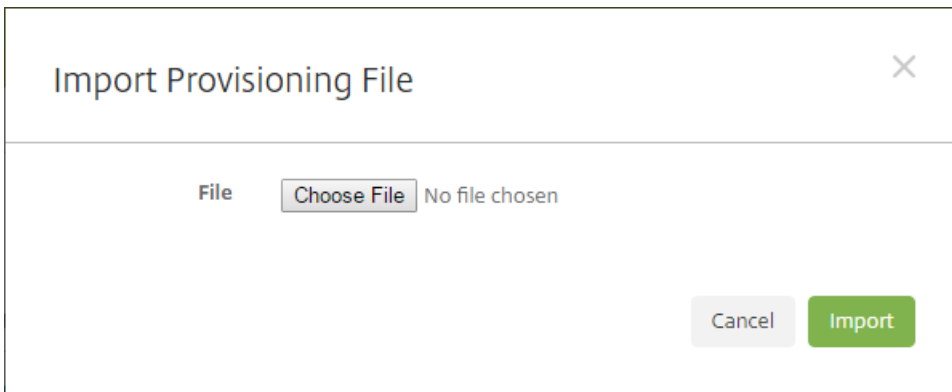
7. 其余的设备详细信息部分包含设备的摘要信息。

- **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。提供每个策略的策略名称、类型和上次部署信息。
- **应用程序**：显示上个清单的已安装、挂起和失败的应用程序数量。提供应用程序名称、标识符、类型和其他信息。
- **操作**：显示已部署、挂起和失败的操作数量。提供上个部署的操作名称和时间。
- **交付组**：显示成功、挂起和失败的交付组数量。对于每个部署，提供交付组的名称和部署时间。选择一个交付组以查看更多详细信息，包括状态、操作以及通道或用户。
- **iOS 配置文件**：显示上一个 iOS 配置文件清单，包括名称、类型、组织和说明。
- **iOS 置备配置文件**：显示企业分发置备配置文件信息，例如 UUID、过期日期以及是否托管。

- **证书**：显示有效证书、已过期证书或已吊销证书信息，例如类型、提供商、颁发者、序列号、过期之前的剩余天数。
- **连接**：显示第一个连接状态和最后一个连接状态。提供每个连接的用户名、倒数第二次身份验证和上次身份验证时间。
- **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。提供每个适用策略的名称和策略值。

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。有关详细信息，请参阅本文中的[设备置备文件格式](#)。

1. 转至**管理 > 设备**，然后单击**导入**。此时将显示导入置备文件对话框。



2. 单击**选择文件**，然后导航到要导入的文件。

3. 单击**导入**。**设备表**将列出导入的文件。

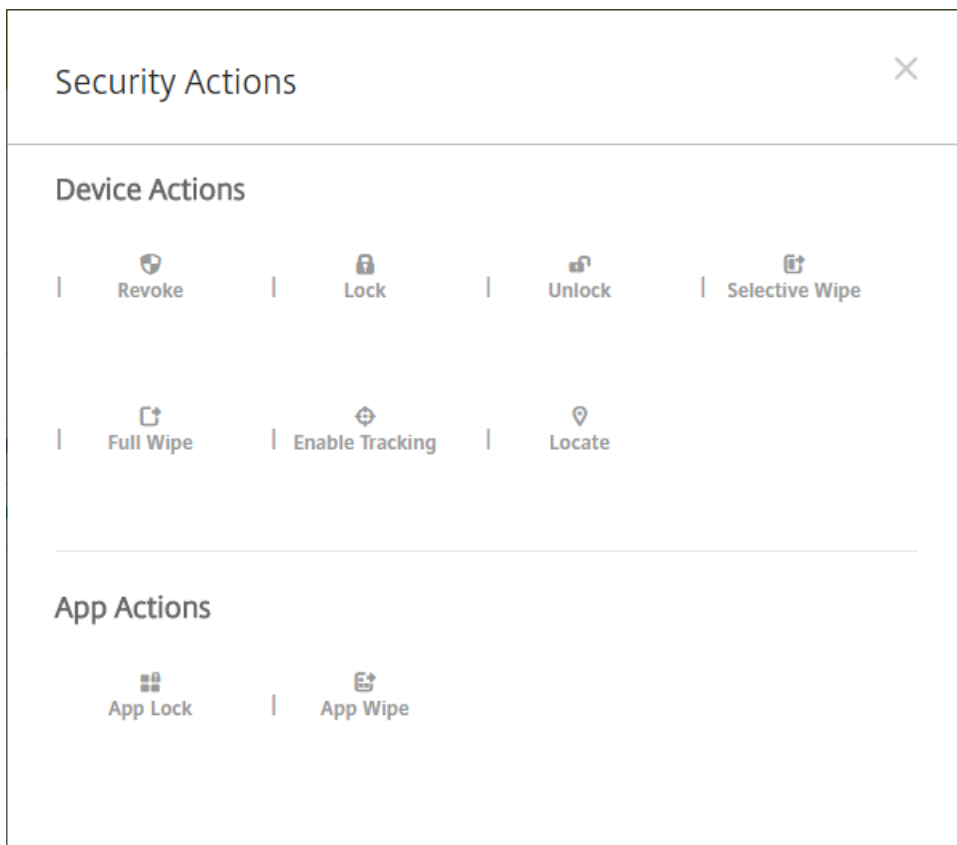
4. 要编辑设备信息，请将其选中，然后单击**编辑**。有关**设备详细信息**页面的信息，请参阅[手动添加设备](#)。

可以从**设备**页面执行设备和应用程序安全操作。设备操作包括吊销、锁定、解锁及擦除。应用程序安全操作包括应用程序锁定和应用程序擦除。

1. 转至**管理 > 设备**，选择一个设备，然后单击**安全**。

2. 在**安全操作**中，单击某项操作并响应任何提示。

有关操作的详细信息，请参阅[自动化操作](#)。



要手动执行应用程序锁定、解锁、擦除或取消擦除操作，请执行以下步骤：

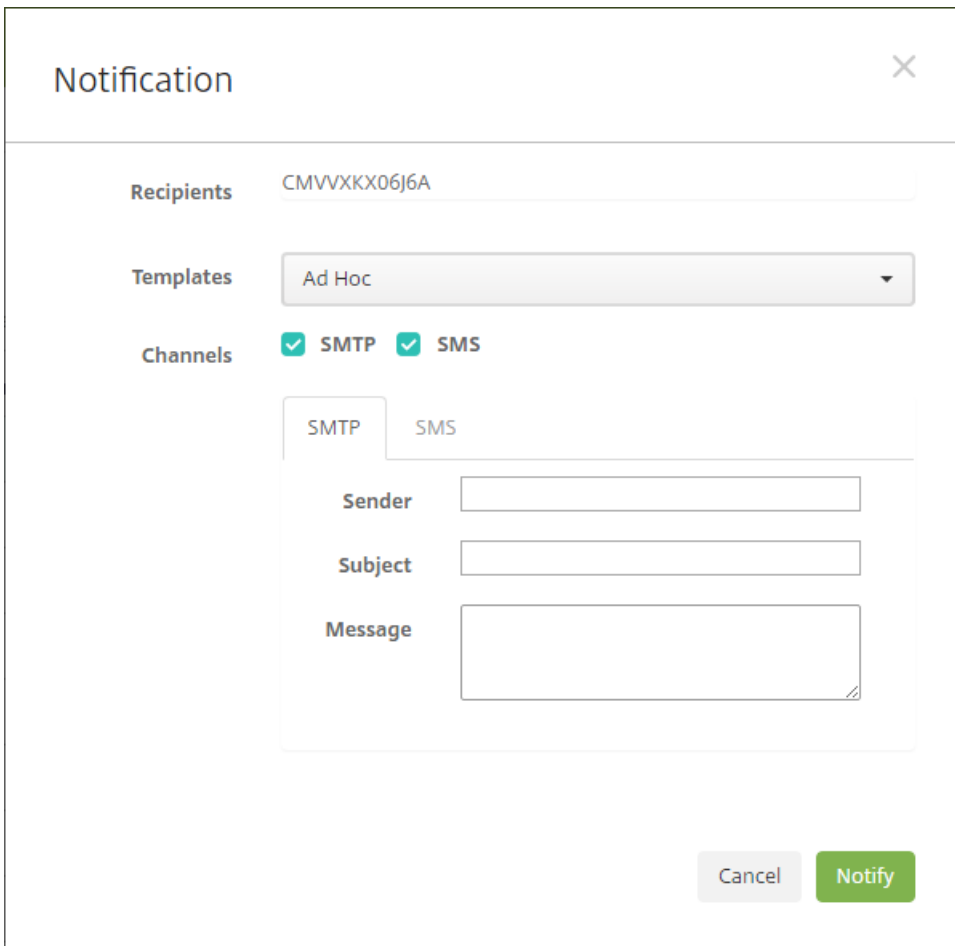
1. 转至**管理 > 设备**，选择一个托管设备，然后单击**安全**。
2. 在**安全操作**对话框中，单击某项操作。

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

3. 确认操作。

您可以从设备页面向设备发送通知。有关通知的详细信息，请参阅[通知](#)。

1. 在**管理 > 设备**页面上，选择要向其发送通知的一个或多个设备。
2. 单击**通知**。此时将显示**通知**对话框。收件人字段中列出要接收通知的所有设备。



The image shows a 'Notification' dialog box with the following fields and options:

- Recipients:** A text input field containing 'CMVVXKX06J6A'.
- Templates:** A dropdown menu currently showing 'Ad Hoc'.
- Channels:** Two checkboxes, 'SMTP' and 'SMS', both of which are checked.
- Configuration Panel:** A sub-dialog with two tabs: 'SMTP' (selected) and 'SMS'. It contains three input fields:
 - Sender:** An empty text input field.
 - Subject:** An empty text input field.
 - Message:** A larger text area for entering the message content.
- Buttons:** 'Cancel' and 'Notify' buttons at the bottom right.

3. 配置以下设置：

- **模板：**在列表中，单击要发送的通知类型。对于除临时外的每个模板，主题和消息字段将显示为所选模板配置的文本。
- **通道：**选择发送消息的方式。默认值为 **SMTP** 和 **SMS**。单击选项卡以查看每个通道的消息格式。
- **发件人：**输入可选发件人。
- **主题：**输入临时消息的主题。
- **消息：**输入临时消息的消息。

4. 单击通知。

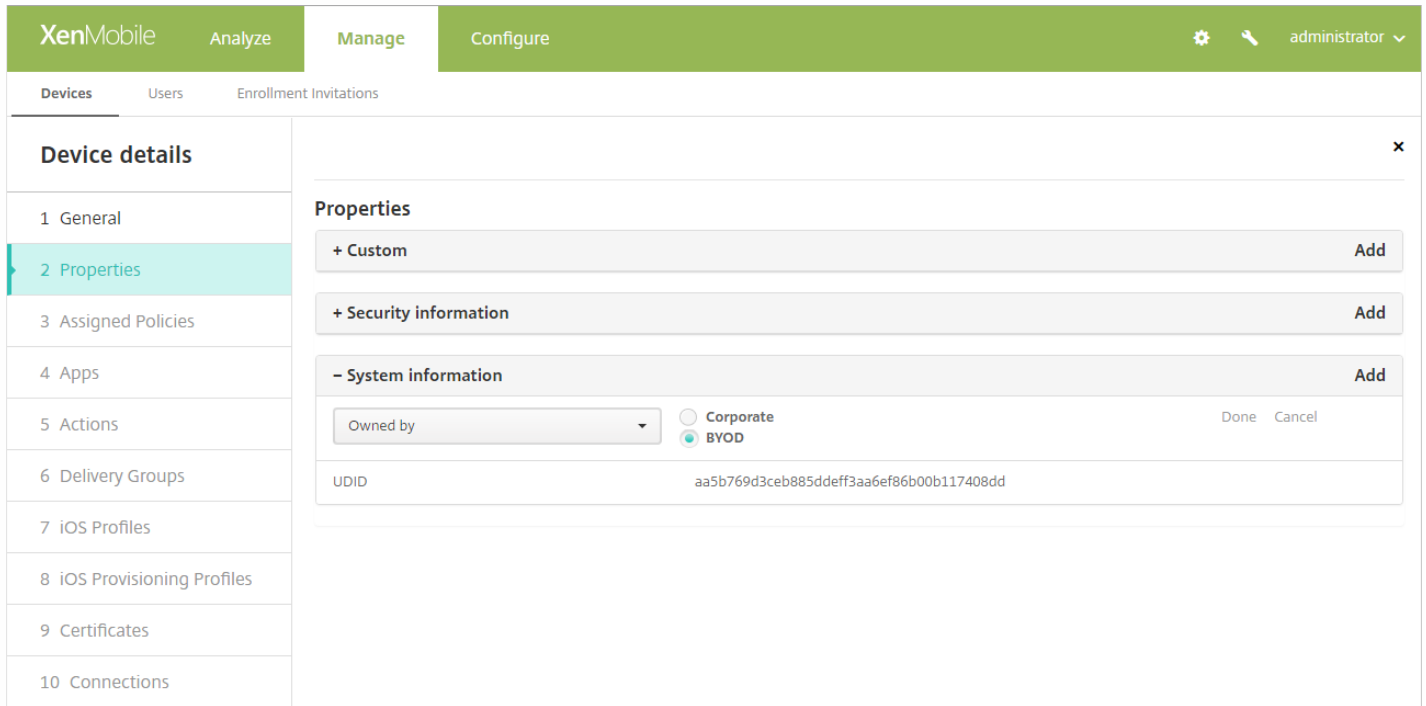
1. 在**设备表**中，选择要删除的一个或多个设备。
2. 单击**删除**。此时将显示确认对话框。再次单击**删除**。此操作无法撤消。

1. 根据您希望在导出文件中显示的内容过滤**设备表**。
2. 单击**设备表**上方的**导出**按钮。XenMobile 将提取过滤后的**设备表**中的信息，并将其转换为 .csv 文件。
3. 系统提示时，打开或保存 .csv 文件。执行此操作的方式取决于所使用的浏览器。您也可以取消此操作。

可以在 XenMobile 中通过以下方式手动标记设备：

- 在基于邀请的注册过程中。
- 在自助服务门户注册过程中。
- 通过添加设备所有权作为设备属性

您可以选择将设备标记为公司所有或员工所有。使用自助服务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

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：

- 有关属性名称和值，请参阅下一部分中的“设备属性名称和值”。
- 使用 UTF-8 字符集。
- 使用分号 (;) 分隔置备文件中的字段。如果某个字段的某一部分包含分号，请使用反斜杠字符 (\) 进行转义。

例如，对于属性
propertyV;test;1;2

, 请按如下所示进行转义 :

```
propertyV\;test\;1\;2
```

- 对于 iOS 设备, 必须提供序列号, 因为序列号是 iOS 设备标识符。
- 对于其他设备平台, 必须包括序列号或 IMEI。
- **OperatingSystemFamily** 的有效值为 **WINDOWS**、**ANDROID** 或 **iOS**。

```
1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;propertyV$*&&ééétest

3050BF3F517301081610065510590393;35244201625379903;iOS;test;

4050BF3F517301081610065510590393;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;
```

文件中的每行都描述一个设备。上述示例中第一个条目的含义如下 :

- 序列号 : 1050BF3F517301081610065510590391
- IMEI : 15244201625379901
- 操作系统系列 : WINDOWS
- 属性名 : propertyN
- 属性值 : propertyV\;test\;1\;2;prop 2

设备属性名称和值

“管理”>“设备”页面中的属性名称	设备置备文件的名称和值	值类型
AIK 是否存在?	WINDOWS_HAS_AIK_PRESENT	字符串
帐户已暂停?	GOOGLE_AW_DIRECTORY_SUSPENDED	字符串
激活锁绕过码	ACTIVATION_LOCK_BYPASS_CODE	字符串

已启用激活锁	ACTIVATION_LOCK_ENABLED 值 (含义) : 1 (是) 0 (否)	布尔值
活动 iTunes 帐户	ACTIVE_ITUNES 值 (含义) : 1 (是) 0 (否)	布尔值
ActiveSync ID	EXCHANGE_ACTIVASYNC_ID	字符串
MSP 已知的 ActiveSync 设备	AS_DEVICE_KNOWN_BY_ZMSP 值 (含义) : 1 (True) 0 (False)	布尔值
已禁用管理员	ADMIN_DISABLED 值 (含义) : 1 (是) 0 (否)	布尔值
Amazon MDM API 可用	AMAZON_MDM 值 (含义) : 1 (True) 0 (False)	布尔值
Android for Work 设备 ID	GOOGLE_AW_DEVICE_ID	字符串
启用了 Android for Work 的设备 ?	GOOGLE_AW_ENABLED_DEVICE	字符串
Android for Work 安装类型	GOOGLE_AW_INSTALL_TYPE 值 : DeviceAdministrator (设备所有者) AvengerManagedProfile (工作托管设备)	字符串

	ManagedProfile (工作配置文件)	
资产标签	ASSET_TAG	字符串
自动更新状态	AUTOUPDATE_STATUS	字符串
可用 RAM	MEMORY_AVAILABLE	整数
可用存储空间	TOTAL_DISK_SPACE	整数
BIOS 信息	BIOS_INFO	字符串
备份电池	BACKUP_BATTERY_PERCENT	整数
基带固件版本	MODEM_FIRMWARE_VERSION	字符串
电池状态	BATTERY_STATUS	字符串
电池充电	BATTERY_CHARGING 值 (含义) : 1 (True) 0 (False)	布尔值
MSP 已知的 Bes 设备	BES_DEVICE_KNOWN_BY_ZMSP 值 (含义) : 1 (True) 0 (False)	布尔值
BES PIN	BES_PIN	字符串
BES 服务器代理 ID	ENROLLMENT_AGENT_ID	字符串

BES 服务器名称	BES_SERVER	字符串
BES 服务器版本	BES_VERSION	字符串
Bit Locker 状态	WINDOWS_HAS_BIT_LOCKER_STATUS	字符串
蓝牙 MAC 地址	BLUETOOTH_MAC	字符串
已启用启动调试？	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED	字符串
启动管理器修订列表版本	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION	字符串
CPU 时钟速度	CPU_CLOCK_SPEED	整数
CPU 类型	CPU_TYPE	字符串
运营商设置版本	CARRIER_SETTINGS_VERSION	字符串
手机网络纬度	GPS_LATITUDE_FROM_CELLULAR	字符串
手机网络经度	GPS_LONGITUDE_FROM_CELLULAR	字符串
手机网络技术	CELLULAR_TECHNOLOGY	整数
手机网络时间戳	GPS_TIMESTAMP_FROM_CELLULAR	日期
下次登录时更改密码？	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN	字符串
客户端设备 ID	CLIENT_DEVICE_ID	字符串

已启用云备份	CLOUD_BACKUP_ENABLED 值 (含义) : 1 (是) 0 (否)	布尔值
已启用代码完整性 ?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED	字符串
代码完整性修订列表版本	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION	字符串
颜色	COLOR	字符串
创建时间	GOOGLE_AW_DIRECTORY_CREATION_TIME	字符串
当前运营商网络	CURRENT_CARRIER_NETWORK	字符串
当前移动国家/地区代码	CURRENT_MCC	整数
当前移动网络代码	CURRENT_MNC	字符串
DEP 帐户名称	BULK_ENROLLMENT_DEP_ACCOUNT_NAME	字符串
DEP 策略	WINDOWS_HAS_DEP_POLICY	字符串
允许数据漫游	DATA_ROAMING_ENABLED 值 (含义) : 1 (是) 0 (否)	布尔值
最后一次 iCloud 备份日期	LAST_CLOUD_BACKUP_DATE	日期
说明	DESCRIPTION	字符

		串
Device Enrollment Program 配置文件分配时间	PROFILE_ASSIGN_TIME	日期
Device Enrollment Program 配置文件推送时间	PROFILE_PUSH_TIME	日期
Device Enrollment Program 配置文件删除时间	PROFILE_REMOVE_TIME	日期
Device Enrollment Program 注册者	DEVICE_ASSIGNED_BY	字符串
Device Enrollment Program 注册日期	DEVICE_ASSIGNED_DATE	日期
设备类型	DEVICE_TYPE	字符串
设备型号	MODEL_ID	字符串
设备名称	DEVICE_NAME	字符串
已激活“请勿打扰”	DO_NOT_DISTURB 值 (含义) : 1 (是) 0 (否)	布尔值
已加载 ELAM 驱动程序?	WINDOWS_HAS_ELAM_DRIVER_LOADED	字符串
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE	日期
企业 ID	ENTERPRISE_ID	字符串
外部存储 1 : 可用空间	EXTERNAL_STORAGE1_FREE_SPACE	整数

外部存储 1：名称	EXTERNAL_STORAGE1_NAME	字符串
外部存储 1：总空间	EXTERNAL_STORAGE1_TOTAL_SPACE	整数
外部存储 2：可用空间	EXTERNAL_STORAGE2_FREE_SPACE	整数
外部存储 2：名称	EXTERNAL_STORAGE2_NAME	字符串
外部存储 2：总空间	EXTERNAL_STORAGE2_TOTAL_SPACE	整数
已加密外部存储	EXTERNAL_ENCRYPTION 值 (含义) : 1 (是) 0 (否)	布尔值
防火墙状态	FIREWALL_STATUS	字符串
固件版本	FIRMWARE_VERSION	字符串
首次同步	ZMSP_FIRST_SYNC	日期
GPS 海拔	GPS_ALTITUDE_FROM_GPS	字符串
GPS 纬度	GPS_LATITUDE_FROM_GPS	字符串
GPS 经度	GPS_LONGITUDE_FROM_GPS	字符串
GPS 时间戳	GPS_TIMESTAMP_FROM_GPS	日期
Google Directory 别名	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS	字符串

Google Directory 系列名称	GOOGLE_AW_DIRECTORY_FAMILY_NAME	字符串
Google Directory 名称	GOOGLE_AW_DIRECTORY_NAME	字符串
Google Directory 主电子邮件	GOOGLE_AW_DIRECTORY_PRIMARY	字符串
Google Directory 用户 ID	GOOGLE_AW_DIRECTORY_USER_ID	字符串
HAS_CONTAINER	HAS_CONTAINER 值 (含义) : 1 (是) 0 (否)	布尔值
HTC API 版本	HTC_MDM_VERSION	字符串
HTC MDM API 可用	HTC_MDM 值 (含义) : 1 (是) 0 (否)	布尔值
硬件加密功能	HARDWARE_ENCRYPTION_CAPS	整数
当前登录的 iTunes 应用商店帐户的哈希	ITUNES_STORE_ACCOUNT_HASH	字符串
主运营商网络	SIM_CARRIER_NETWORK	字符串
主移动国家/地区代码	SIM_MCC	整数
主移动网络代码	SIM_MNC	字符串
ICCID	ICCID	字符

		串
IMEI/MEID 编号	IMEI	字符串
IMSI	IMSI	字符串
IP 位置	IP_LOCATION	字符串
身份	AS_DEVICE_IDENTITY	字符串
已加密内部存储	LOCAL_ENCRYPTION 值 (含义) : 1 (True) 0 (False)	布尔值
颁发时间	WINDOWS_HAS_ISSUED_AT	字符串
已越狱/获得 Root 权限	ROOT_ACCESS 值 (含义) : 1 (是) 0 (否)	布尔值
已启用内核调试?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	字符串
Kiosk 模式	IS_KIOSK 值 (含义) : 1 (True) 0 (False)	布尔值
上次已知 IP 地址	LAST_IP_ADDR	字符串
上次策略更新时间	LAST_POLICY_UPDATE_TIME	日期

上次同步	ZMSP_LAST_SYNC	日期
已启用定位器服务	DEVICE_LOCATOR 值 (含义) : 1 (是) 0 (否)	布尔值
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY	字符串
MEID	MEID	字符串
邮箱设置	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP	字符串
主电池	MAIN_BATTERY_PERCENT	整数
移动电话号码	TEL_NUMBER	字符串
型号 ID	SYSTEM_OEM	字符串
网络适配器类型	NETWORK_ADAPTER_TYPE	字符串
已安装 NitroDesk TouchDown	TOUCHDOWN_FIND 值 (含义) : 1 (True) 0 (False)	布尔值
已通过 MDM 授权使用 NitroDesk TouchDown	TOUCHDOWN_LICENSED_VIA_MDM 值 (含义) : 1 (True) 0 (False)	布尔值
操作系统内部版本号	SYSTEM_OS_BUILD	字符串

操作系统语言 (区域设置)	SYSTEM_LANGUAGE	字符串
操作系统版本	SYSTEM_OS_VERSION	字符串
组织地址	ORGANIZATION_ADDRESS	字符串
组织电子邮件	ORGANIZATION_EMAIL	字符串
组织幻数	ORGANIZATION_MAGIC	字符串
组织名称	ORGANIZATION_NAME	字符串
组织电话号码	ORGANIZATION_PHONE	字符串
其他	其他	字符串
不合规	OUT_OF_COMPLIANCE 值 (含义) : 1 (True) 0 (False)	布尔值
所有者	CORPORATE_OWNED 值 (含义) : 1 (公司) 0 (BYOD)	布尔值
PCRO	WINDOWS_HAS_PCRO	字符串
地理围栏的 PIN 码	PIN_CODE_FOR_GEO_FENCE	字符

		串
通行码合规性	PASSCODE_IS_COMPLIANT 值 (含义) : 1 (是) 0 (否)	布尔值
通行码遵从配置	PASSCODE_IS_COMPLIANT_WITH_CFG 值 (含义) : 1 (是) 0 (否)	布尔值
通行码存在	PASSCODE_PRESENT 值 (含义) : 1 (是) 0 (否)	布尔值
超出边界	GPS_PERIMETER_BREACH 值 (含义) : 1 (是) 0 (否)	布尔值
已激活个人热点	PERSONAL_HOTSPOT_ENABLED 值 (含义) : 1 (是) 0 (否)	布尔值
平台	SYSTEM_PLATFORM	字符串
平台 API 级别	API_LEVEL	整数
策略名称	POLICY_NAME	字符串
主电话号码	IDENTITY1_PHONENUMBER	字符串
主 SIM IMEI	IDENTITY1_IMEI	字符

		串
主 SIM IMSI	IDENTITY1_IMSI	字符串
主 SIM 漫游	IDENTITY1_ROAMING 值 (含义) : 1 (True) 0 (False)	布尔值
产品名称	PRODUCT_NAME	字符串
发布者设备 ID	PUBLISHER_DEVICE_ID	字符串
重置计数	WINDOWS_HAS_RESET_COUNT	字符串
重新启动计数	WINDOWS_HAS_RESTART_COUNT	字符串
SBCP 哈希	WINDOWS_HAS_SBCP_HASH	字符串
具有 SMS 功能	IS_SMS_CAPABLE 值 (含义) : 1 (True) 0 (False)	布尔值
已启用安全模式?	WINDOWS_HAS_SAFE_MODE	字符串
Samsung KNOX API 可用	SAMSUNG_KNOX 值 (含义) : 1 (True) 0 (False)	布尔值
Samsung KNOX API 版本	SAMSUNG_KNOX_VERSION	字符串

Samsung KNOX 认证	SAMSUNG_KNOX_ATTESTED 值 (含义) : 1 (通过) 0 (未通过)	布尔值
Samsung KNOX 认证更新日期	SAMSUNG_KNOX_ATT_UPDATED_TIME	日期
Samsung SAFE API 可用	SAMSUNG_MDM 值 (含义) : 1 (True) 0 (False)	布尔值
Samsung SAFE API 版本	SAMSUNG_MDM_VERSION	字符串
屏幕 : X 轴分辨率	SCREEN_XDPI	整数 (PPI)
屏幕 : Y 轴分辨率	SCREEN_YDPI	整数 (PPI)
屏幕 : 高度	SCREEN_HEIGHT	整数 (像素)
屏幕 : 颜色数量	SCREEN_NB_COLORS	整数
屏幕 : 大小	SCREEN_SIZE	十进制 (英寸)
屏幕 : 宽度	SCREEN_WIDTH	整数 (像素)
辅助电话号码	IDENTITY2_PHONENUMBER	字符串

辅助 SIM IMEI	IDENTITY2_IMEI	字符串
辅助 SIM IMSI	IDENTITY2_IMSI	字符串
辅助 SIM 漫游	IDENTITY2_ROAMING 值 (含义) : 1 (True) 0 (False)	布尔值
已启用安全启动 ?	WINDOWS_HAS_SECURE_BOOT_ENABLED	字符串
已启用 SecureContainer	WINDOWS_HAS_BIT_LOCKER_STATUS	字符串
序列号	SERIAL_NUMBER	字符串
Sony Enterprise API 可用	SONY_MDM 值 (含义) : 1 (True) 0 (False)	布尔值
Sony Enterprise API 版本	SONY_MDM_VERSION	字符串
受监督	受监督 值 (含义) : 1 (是) 0 (否)	布尔值
暂停原因	GOOGLE_AW_DIRECTORY_SUSPENSION_REASON	字符串
被篡改状态	TAMPERED_STATUS	字符串

条款和条件	TERMS_AND_CONDITIONS	字符串
已接受条款和协议？	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS	字符串
已启用测试签名？	WINDOWS_HAS_TEST_SIGNING_ENABLED	字符串
RAM 总量	MEMORY	整数
总存储空间	FREEDISK	整数
UDID	UDID	字符串
用户代理	USER_AGENT	字符串
用户定义的第一个	USER_DEFINED_1	字符串
用户定义的第二个	USER_DEFINED_2	字符串
用户定义的第三个	USER_DEFINED_3	字符串
用户语言（区域设置）	USER_LANGUAGE	字符串
已启用 VSM？	WINDOWS_HAS_VSM_ENABLED	字符串
供应商	VENDOR	字符串
语音支持	IS_VOICE_CAPABLE 值（含义）： 1 (True)	布尔值

	0 (False)	
允许语音漫游	VOICE_ROAMING_ENABLED 值 (含义) : 1 (是) 0 (否)	布尔值
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY	字符串
WNS 通知状态	WNS_PUSH_STATUS	字符串
WNS 通知 URL	PROPERTY_WNS_PUSH_URL	字符串
WNS 通知 URL 过期日期	PROPERTY_WNS_PUSH_URL_EXPIRY	字符串
WiFi MAC 地址	WIFI_MAC	字符串
已启用 WinPE ?	WINDOWS_HAS_WINPE	字符串
XenMobile Agent ID	AGENT_ID	字符串
XenMobile Agent 修订版	EW_REVISION	字符串
XenMobile Agent 版本	EW_VERSION	字符串

锁定 iOS 设备

Feb 27, 2017

您可以锁定丢失的 iOS 设备，同时在设备锁定屏幕上显示消息和电话号码。运行 iOS 7 及更高版本的设备支持此功能。

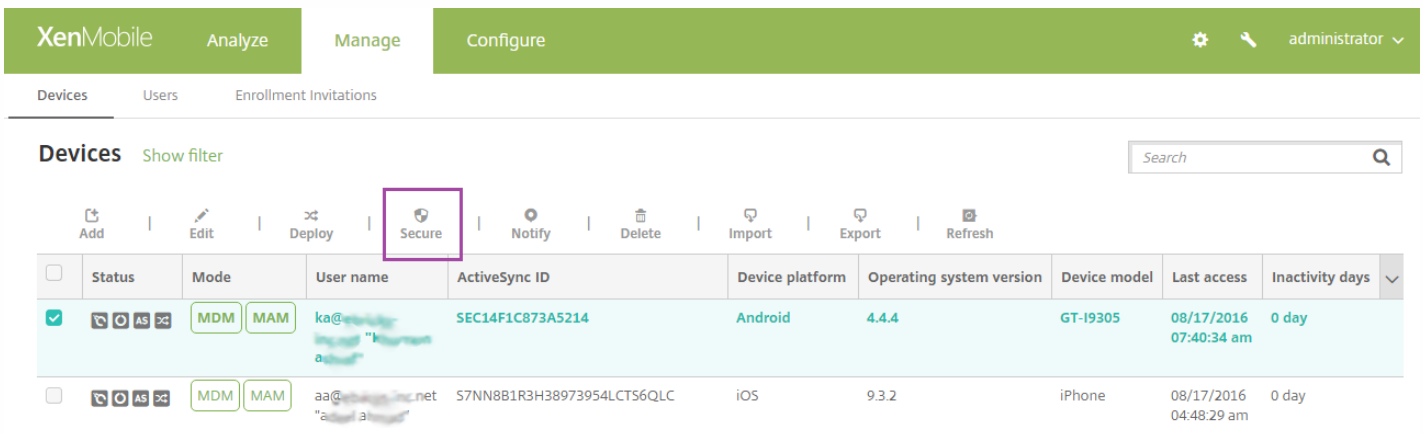
必须在 XenMobile 控制台中将通行码策略设置为 true，才能使消息和电话号码在锁定设备上显示。此外，用户必须手动在设备上启用通行码。

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。

选中某个设备旁边的复选框时，选项菜单将在设备列表上方显示。可以单击列表中的某个项目以在此列表的右侧显示选项菜单。



XenMobile Analyze Manage Configure administrator

Devices Users Enrollment Invitations

Devices Show filter Search

Add Import Export Refresh

Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
	MDM MAM	ka@...	SEC14F1C873A5214	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
	MDM MAM	aa@... net	S7NN8B1R3H38973954LCTS6QLC	iOS				

Edit Deploy **Secure** Notify Delete

XME Device Managed

Delivery Groups	2	Policies	5
Actions	2	Apps	15

Show more >

3. 在选项菜单中，选择安全。此时将显示安全操作对话框。

Security Actions

Device Actions

Revoke

Lock

Unlock

Selective Wipe

Full Wipe

Enable Tracking

Locate

Request AirPlay Mirroring

4. 单击锁定。此时将显示安全操作确认对话框。

Security Actions

Are you sure you want to lock this device?

Message

Phone

Cancel Lock Device

5. (可选) 键入将显示在设备锁屏界面消息和电话号码。

对于运行 iOS 7 及更高版本的 iPad: iOS 将“丢失的 iPad”字样附加到您在消息字段中键入的内容后。对于运行 iOS 7 及更高版本的 iPhone: 如果将消息字段留空, 并提供电话号码, Apple 将在设备锁屏界面上显示消息“呼叫所有者”。

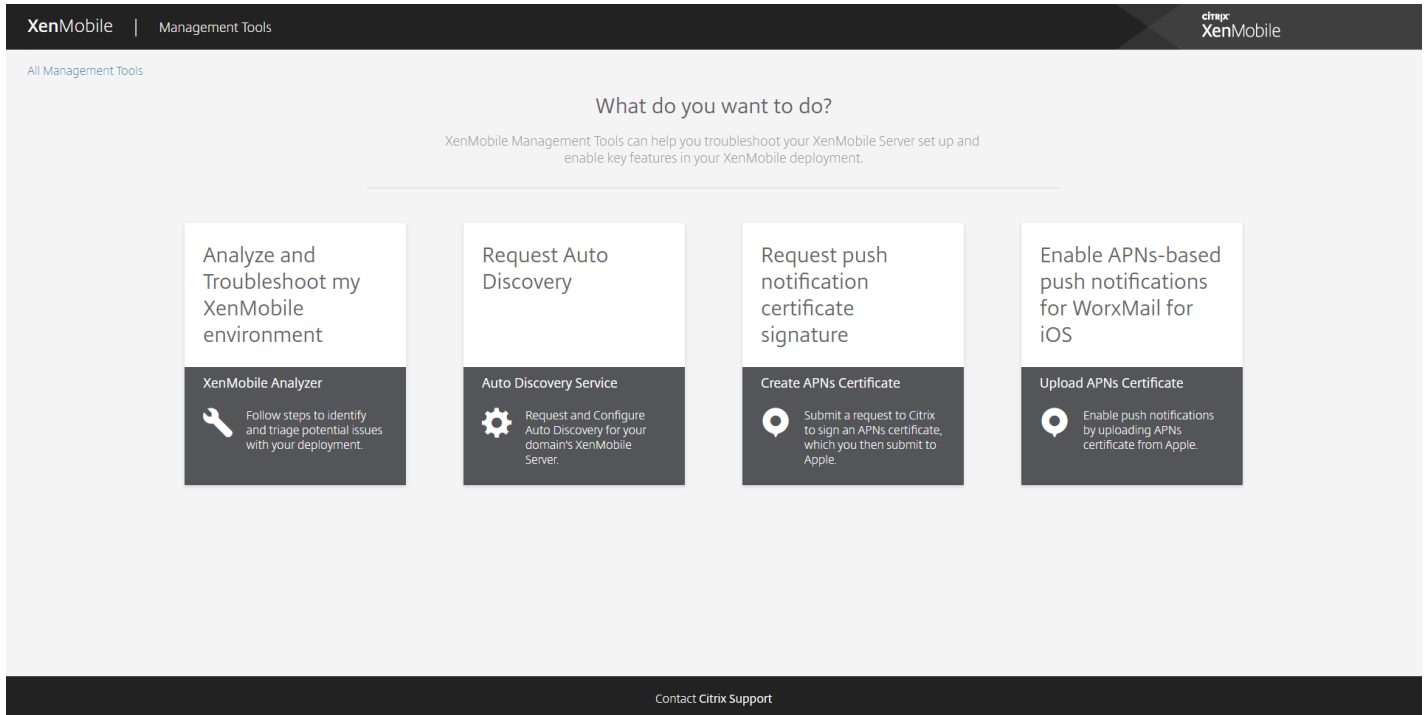
6. 单击锁定设备。

XenMobile 自动发现服务

Feb 27, 2017

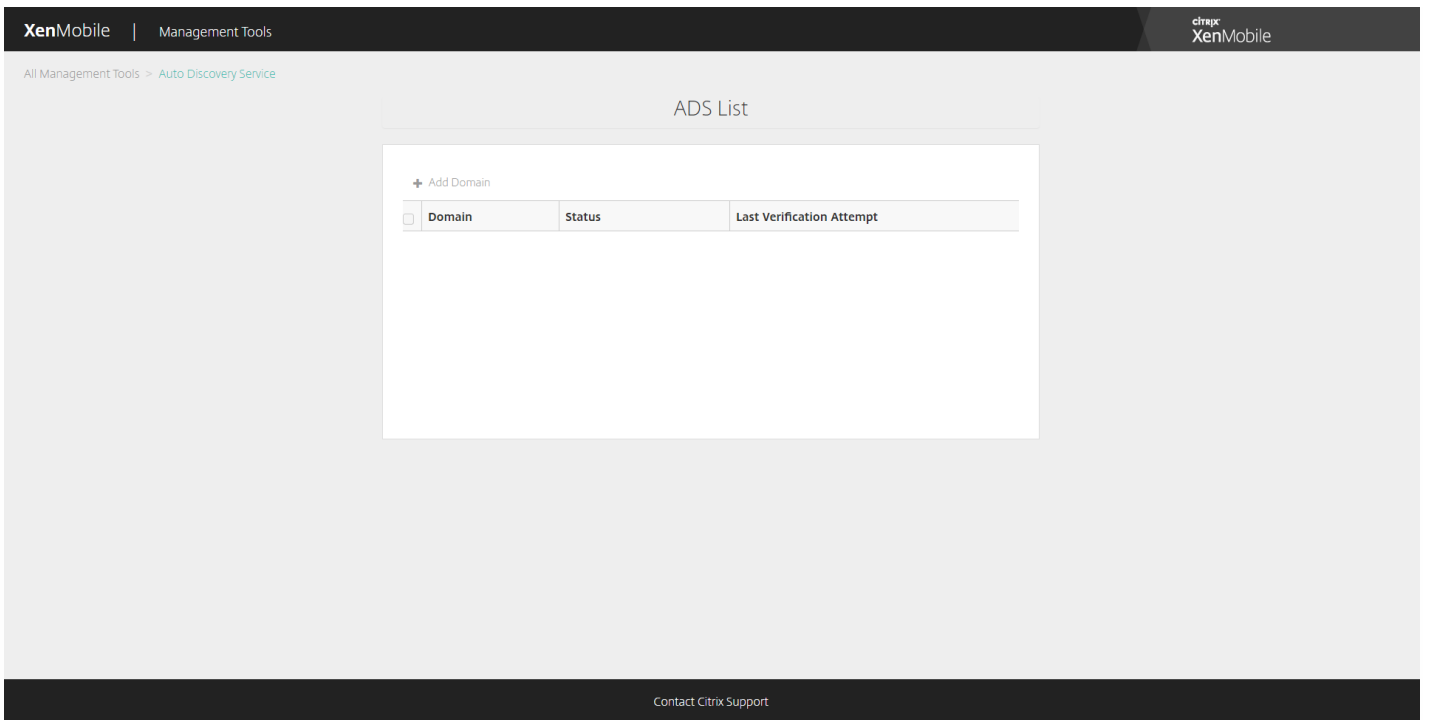
自动发现是许多 XenMobile 部署的重要部分。自动发现可简化用户的注册过程。用户可以使用他们的网络用户名和 Active Directory 密码注册其设备，无需再输入 XenMobile 服务器的详细信息。用户以用户主体名称 (UPN) 格式输入其用户名，例如，user@mycompany.com。通过 XenMobile 自动发现服务，不需要 Citrix 支持的帮助即可创建或编辑自动发现记录。

要访问 XenMobile 自动发现服务，请导航到 <https://xenmobiletools.citrix.com>，然后单击 **Request Auto Discovery**（申请自动发现）。

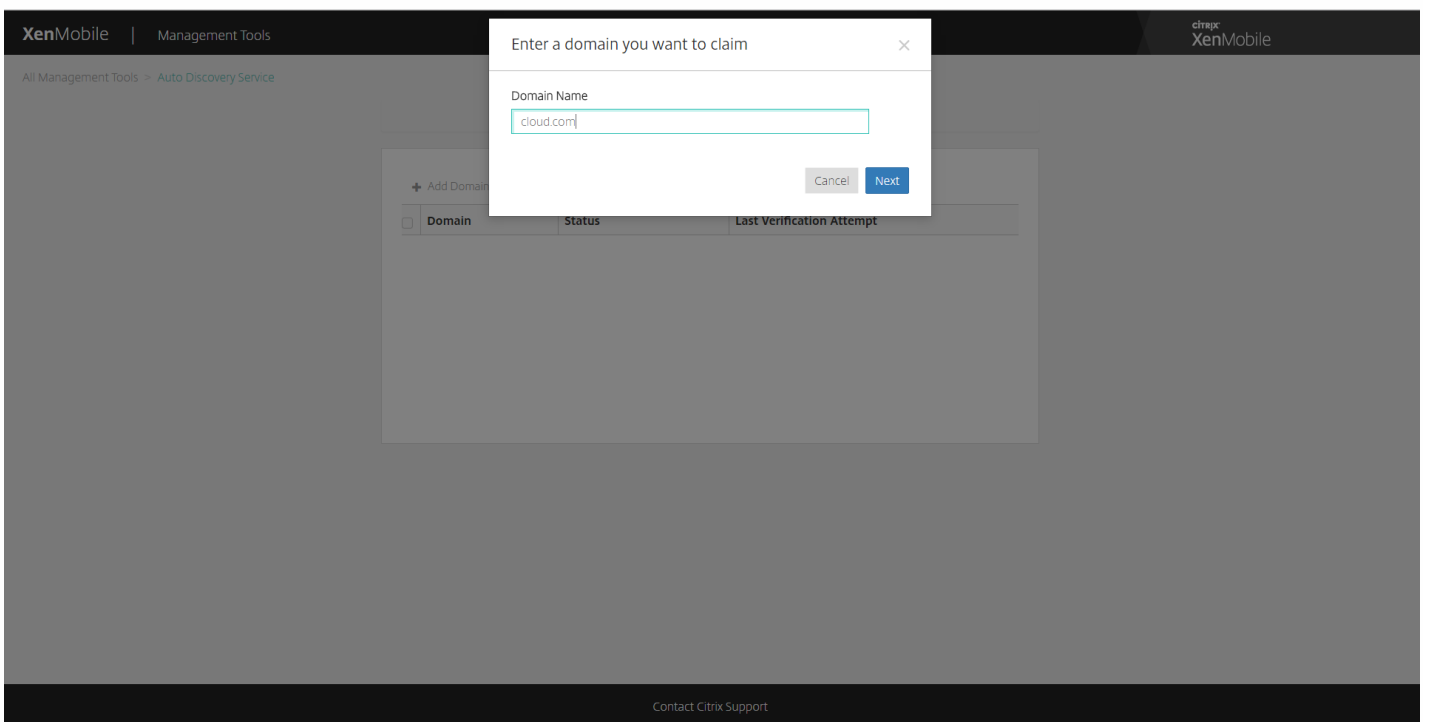


申请自动发现

1. 在“AutoDiscovery Service”（自动发现服务）页面上，需要先声明一个域。单击 **Add Domain**（添加域）。



2. 在打开的对话框中，输入 XenMobile 环境的域名，然后单击 **Next**（下一步）。



3. 下一步将提供有关验证您是否拥有域的说明。

- a. 复制在 XenMobile Tools 门户网站中提供的 DNS 令牌。
- b. 在托管提供程序门户网站的域中，在您的域对应的区域文件中创建一条 DNS TXT 记录。

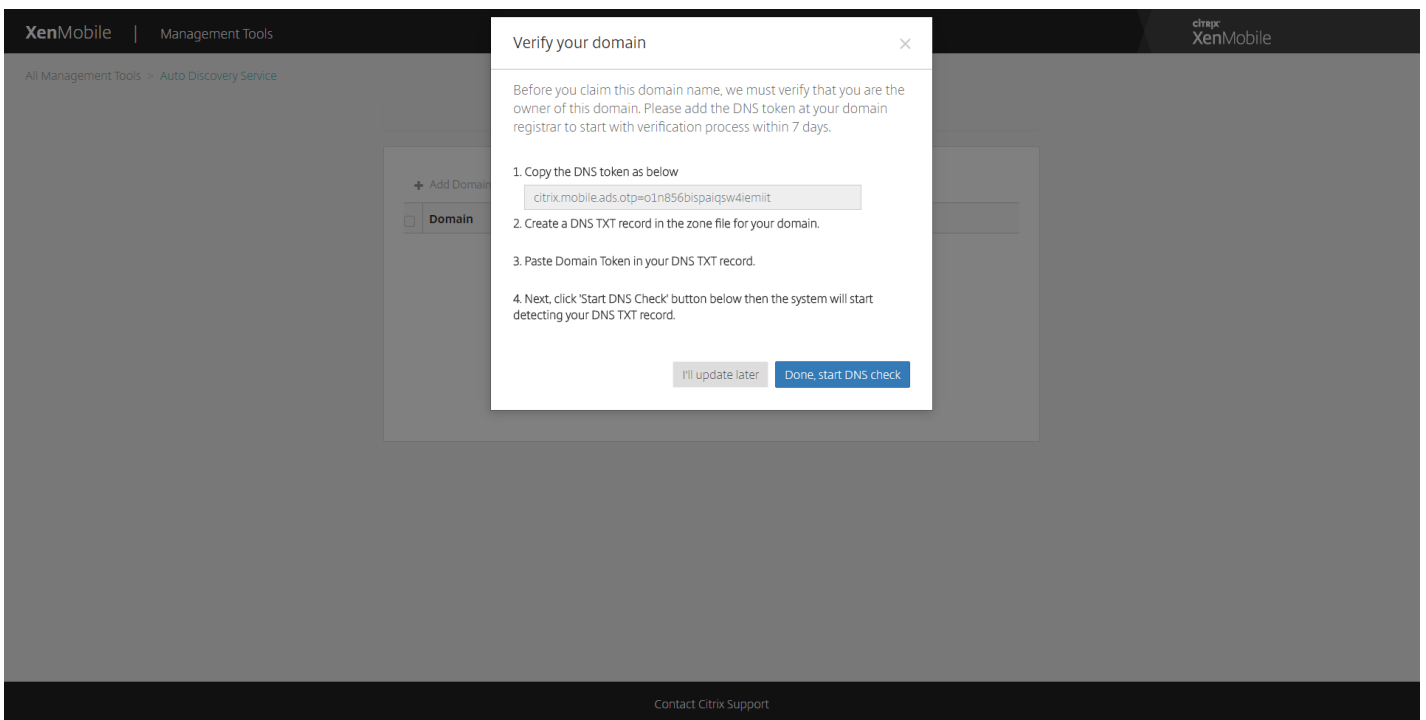
要创建 DNS TXT 记录，需要登录您在上面的步骤 2 中添加的域的域托管提供程序门户网站。在域托管门户网站中，可以编辑您的域名服务器记录以及添加自定义 TXT 记录。下例说明了如何在示例域 domain.com 的托管门户中添加 DNS TXT 条目。

c. 粘贴 DNS TXT 记录中的域令牌并保存您的域名服务器记录。

d. 返回 XenMobile Tools 门户，单击“Done”（完成），启动 DNS 检查。

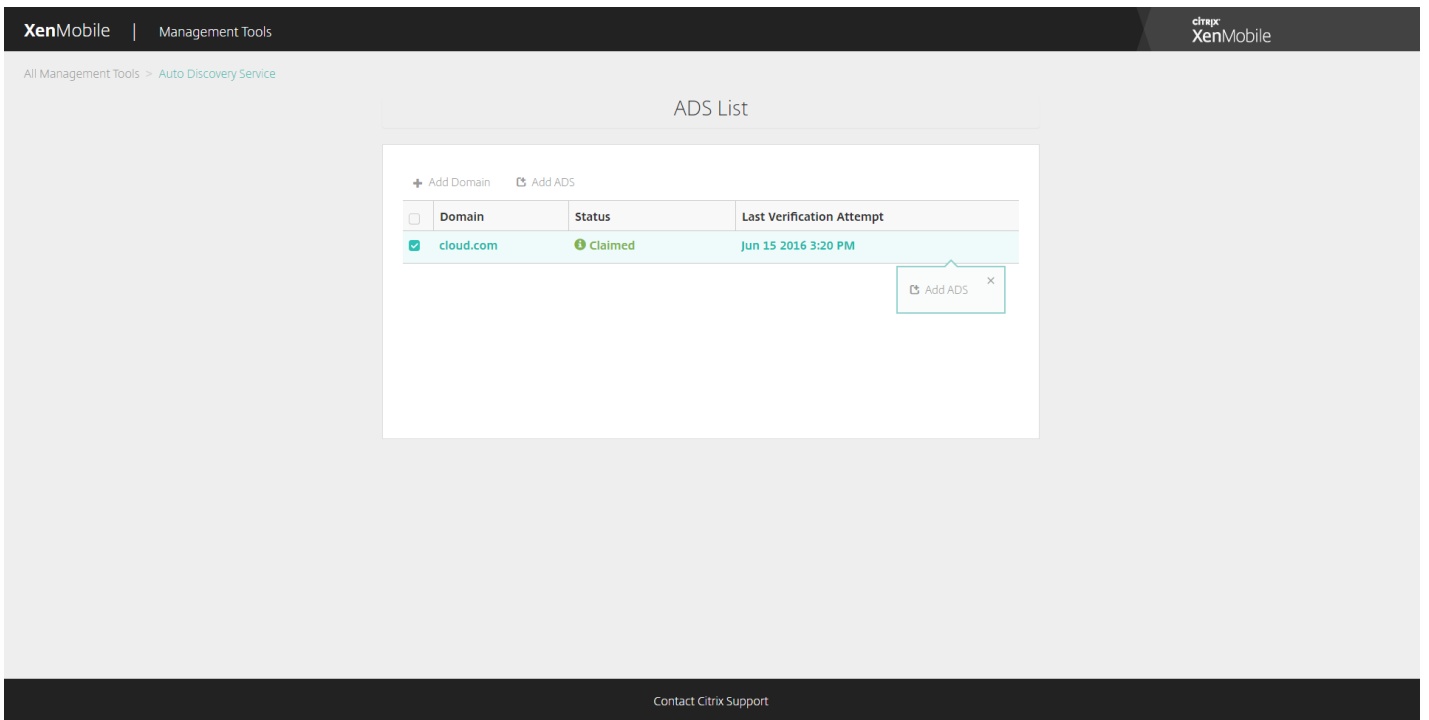
系统将检测您的 DNS TXT 记录。或者，可以单击 I'll update later（我将在以后更新），记录将被保存。DNS 检查在您选择“Waiting”（等待）记录并单击“DNS Check”（DNS 检查）后才会启动。

此检查的理想时间大约为一小时，但最长需要两天时间才能返回响应。此外，您可能需要离开该门户并返回以查看状态变更。

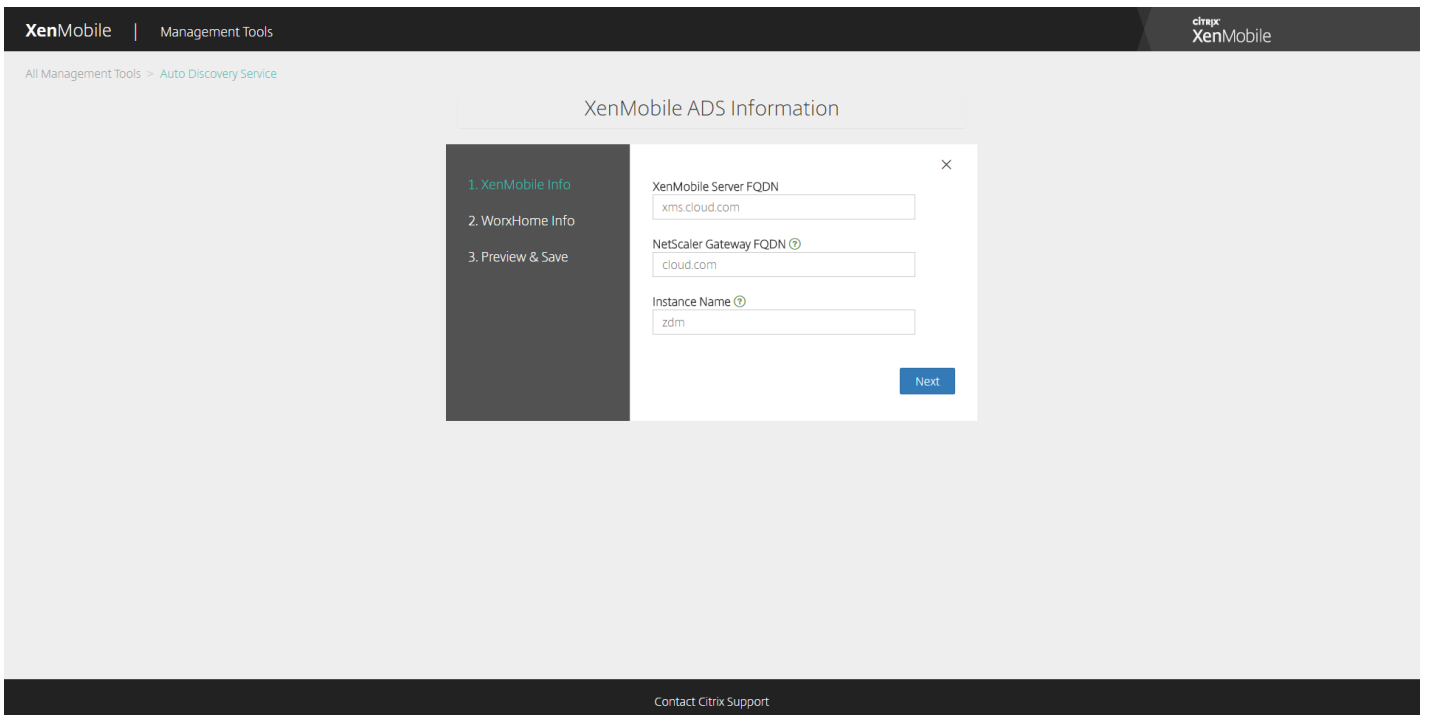


4. 声明您的域后，可以输入自动发现服务信息。右键单击要为其申请自动发现的域记录，然后单击 **Add ADS**（添加 ADS）。

如果您的域已有自动发现记录，请通过 Citrix 技术支持记录一个案例以根据需要修改详细信息。



5. 输入 **XenMobile Server FQDN** (XenMobile 服务器 FQDN)、**NetScaler Gateway FQDN** 和 **Instance Name** (实例名称)，然后单击 **Next** (下一步)。如不确定，请添加默认实例“zdm”。



在上面的屏幕截图中，请注意 Worx Home 现在称为 Secure Hub。

6. 输入 Secure Hub 的以下信息，然后单击 **Next** (下一步)。

a. **User ID Type** (用户 ID 类型)：选择用户登录时使用的 ID 类型，即 **E-mail address** (电子邮件地址) 或 **UPN**。

用户的 UPN（用户主体名称）与其电子邮件地址相同时将使用 **UPN**。这两种方法都使用输入的域来查找服务器地址。使用 **E-mail address**（电子邮件地址）时，系统将要求用户输入其用户名和密码，使用 **UPN** 时，系统将要求用户输入其密码。

b. **HTTPS Port**（HTTPS 端口）：输入用于通过 HTTPS 访问 Secure Hub 的端口。通常为端口 443。

c. **iOS Enrollment Port**（iOS 注册端口）：输入注册 iOS 时用于访问 Secure Hub 的端口。通常为端口 8443。

d. **Required Trusted CA for XenMobile**（XenMobile 所需的可信 CA）：指示是否需要可信证书才能访问 XenMobile。此选项可以为 **OFF**（关）或 **ON**（开）。当前无法上载适用于此功能的证书。如果要使用此功能，需要联系 Citrix 支持，请其设置自动发现。要了解与证书固定有关的详细信息，请参阅 XenMobile 应用程序文档的 [Secure Hub](#) 中有关证书固定的部分。要了解与使证书固定起作用所需的端口有关的信息，请参阅 [XenMobile Port Requirements for ADS Connectivity](#)（ADS 连接的 XenMobile 端口要求）上的技术支持文章。

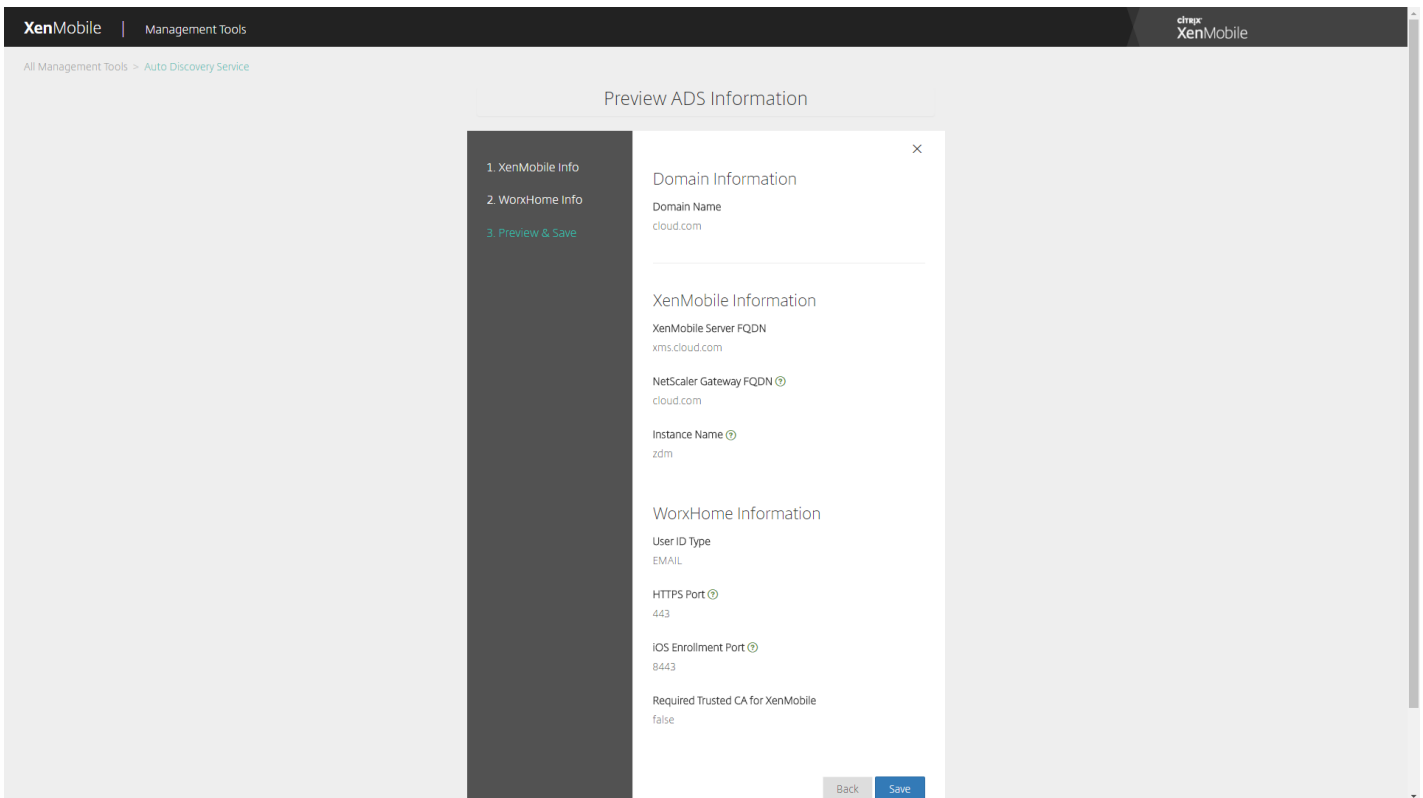
The screenshot shows the 'WorxHome ADS Information' configuration window in the XenMobile Management Tools interface. The window has a sidebar on the left with three steps: 1. XenMobile Info, 2. WorxHome Info (highlighted in green), and 3. Preview & Save. The main content area contains the following fields and controls:

- User ID Type**: A dropdown menu set to 'E-mail address'.
- HTTPS Port**: A text input field containing '443'.
- iOS Enrollment Port**: A text input field containing '8443'.
- Required Trusted CA for XenMobile**: A radio button control set to 'OFF'.
- At the bottom right, there are 'Back' and 'Next' buttons.

The top of the interface shows 'XenMobile | Management Tools' and the Citrix XenMobile logo. The bottom of the interface has a 'Contact Citrix Support' link.

在上面的屏幕截图中，请注意 Worx Home 现在称为 Secure Hub。

7. 摘要页面将显示您在上述步骤中输入的所有信息。验证该数据是否正确，然后单击 **Save**（保存）。



在上面的屏幕截图中，请注意 Worx Home 现在称为 Secure Hub。

启用自动发现

自动发现可简化用户的注册过程。用户可以使用他们的网络用户名和 Active Directory 密码注册其设备，无需再输入 XenMobile 服务器的详细信息。用户以用户主体名称 (UPN) 格式输入其用户名，例如，user@mycompany.com。

要启用自动发现，可以访问自动发现服务门户 <https://xenmobiletools.citrix.com>。

在有限的几种情况下，您可能需要联系 Citrix 支持以启用自动发现。为此，可以按照下面的步骤，将部署信息告知 Citrix 技术支持团队，如果使用 Windows 设备，则应将 SSL 证书告知 Citrix 技术支持团队。Citrix 收到此信息后，会在用户注册其设备时，提取域信息并将其映射到服务器地址。此信息保留在 XenMobile 数据库中，以使用户注册时随时访问和获取。

1. 如果无法使用自动发现服务门户（网址为 <https://xenmobiletools.citrix.com>）启用自动发现，请使用 [Citrix 支持门户](#) 打开一个技术支持案例，然后提供以下信息：

- 包含用户注册所用帐户的域。
- XenMobile 服务器完全限定的域名 (FQDN)。
- XenMobile 实例名称。默认情况下，实例名称为 zdm 并区分大小写。
- 用户 ID 类型，可以是 UPN 或电子邮件。默认情况下，类型为 UPN。
- 用于 iOS 注册的端口（如果更改了默认端口号 8443）。
- XenMobile 服务器通过其接受连接的端口（如果更改了默认端口号 443）。
- （可选）XenMobile 管理员的电子邮件地址。

2. 如果计划注册 Windows 设备，请执行以下操作：

- 请获取 enterpriseenrollment.mycompany.com 的公共签名非通配符 SSL 证书，其中 mycompany.com 是包含用户注册时要使用的帐户的域。请在您的请求中附上 .pfx 格式的 SSL 证书及其密码。
- 在您的 DNS 中创建一条规范名称 (CNAME) 记录，并将 SSL 证书的地址 (enterpriseenrollment.mycompany.com) 映射到 autodisc.zc.zenprise.com。Windows 设备用户使用 UPN 注册时，除了提供 XenMobile 服务器的详细信息外，Citrix 注册服务器还指导设备从 XenMobile 服务器请求一个有效证书。

当您的详细信息和证书（如适用）添加到 Citrix 服务器时，您的技术支持案例将更新。此时，用户可使用自动发现开始注册。

注意：如果要使用多个域进行注册，还可以使用多域证书。多域证书应具有以下结构：

- SubjectDN，包含用于指定所服务的主域的 CN（例如 enterpriseenrollment.mycompany1.com）。
- 适用于其余域的恰当 SAN（例如 enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.com 等）。

注册设备

May 11, 2017

为了安全地远程管理用户设备，将在 XenMobile 中注册这些设备。将 XenMobile 客户端软件安装在用户设备上并验证用户的身份。然后，安装 XenMobile 和用户配置文件。之后，您可以在 XenMobile 控制台中执行设备管理任务。可以应用策略、部署应用程序、将数据推送到设备以及锁定、擦除和定位丢失或被盗的设备。

借助 XenMobile Service 10.5.1，iOS、Android 和 Windows 10 设备支持 Azure Active Directory 注册。有关将 Azure 配置为身份提供程序 (IDP) 的详细信息，请参阅 XenMobile Service [新增功能](#)一文中的“XenMobile 与作为 IDP 的 Azure Active Directory 的集成”。

注意：必须先申请 APNs 证书才能注册 iOS 设备用户。有关详细信息，请参阅[证书](#)。

要针对用户和设备更新配置选项，请使用[管理 > 注册邀请](#)页面。有关详细信息，请参阅本文中的[发送注册邀请](#)。

Android 设备

1. 在 Android 设备上转到 Google Play 应用商店，下载 Citrix Secure Hub 应用程序，然后轻按该应用程序。
2. 提示安装应用程序时，单击下一步，然后单击**安装**。
3. Secure Hub 安装完毕后，轻按**打开**。
4. 输入企业凭据，如组织的 XenMobile 服务器名称、用户主体名称 (UPN) 或电子邮件地址，然后单击下一步。
5. 在 **Activate device administrator** (激活设备管理员) 屏幕上，轻按**激活**。
6. 输入贵公司密码，然后轻按**登录**。
7. 系统可能要求您创建 Citrix PIN (这取决于 XenMobile 的配置方式)，可使用它来登录 Secure Hub 和其他支持 XenMobile 的应用程序，如 Secure Mail、Secure Web、ShareFile，等。需要输入 Citrix PIN 两次。在**创建 Citrix PIN** 屏幕上，输入一个 PIN。
8. 重新输入 PIN。此时会打开 Secure Hub。这时即可访问 XenMobile Store 来查看您可以安装在 Android 设备上的应用程序。
9. 如果您在注册后将 XenMobile 配置为向用户的设备自动推送应用程序，将显示提示他们安装应用程序的消息。此外，您在 XenMobile 中配置的策略将部署到设备。轻按**安装**，安装应用程序。

取消注册和重新注册 Android 设备

用户可以从 Secure Hub 内部取消注册。用户通过以下过程取消注册时，设备将仍然在 XenMobile 控制台的设备清单中显示。但您无法在设备上执行操作。无法跟踪设备，也无法监视设备合规性。

1. 轻按以打开 Secure Hub 应用程序。
2. 执行以下操作，具体取决于您拥有的是手机还是平板电脑：

在手机上：

- a. 从屏幕左侧轻扫以打开设置窗格。
- b. 依次轻按**首选项**、**帐户**和**删除帐户**。

在平板电脑上：

- a. 轻按右上角的电子邮件地址旁边的箭头。

b. 依次轻按首选项、帐户和删除帐户。

3. 轻按重新注册。将显示一条消息，提示您确认是否要重新注册自己的设备。

4. 轻按确定。

您的设备将取消注册。

5. 请按照屏幕上的说明重新注册设备。

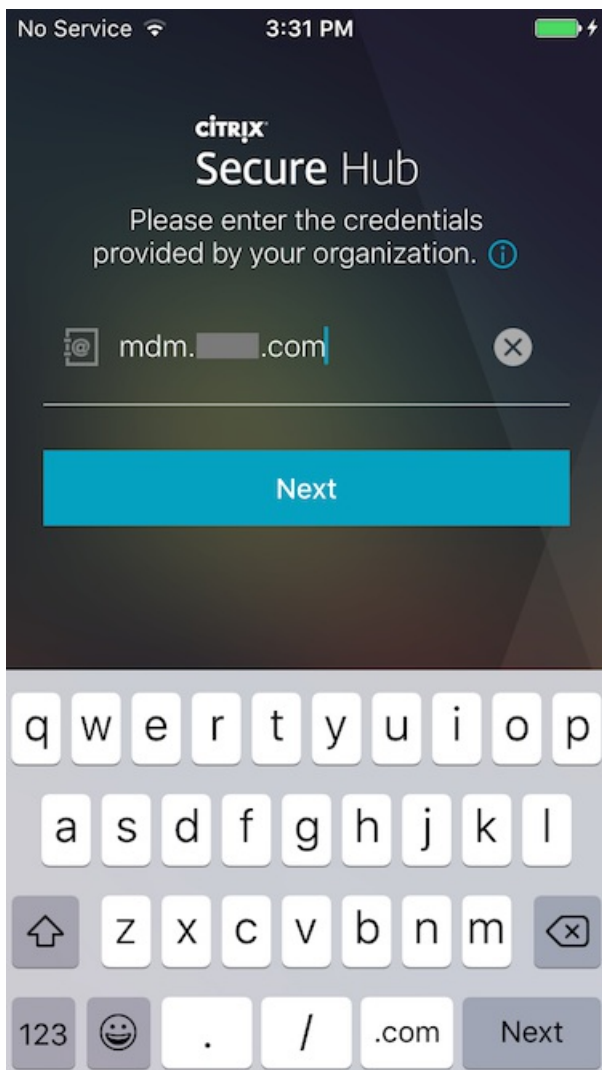
iOS 设备

1. 从设备上的 Apple iTunes App Store 下载 Secure Hub 应用程序，然后在设备上安装该应用程序。

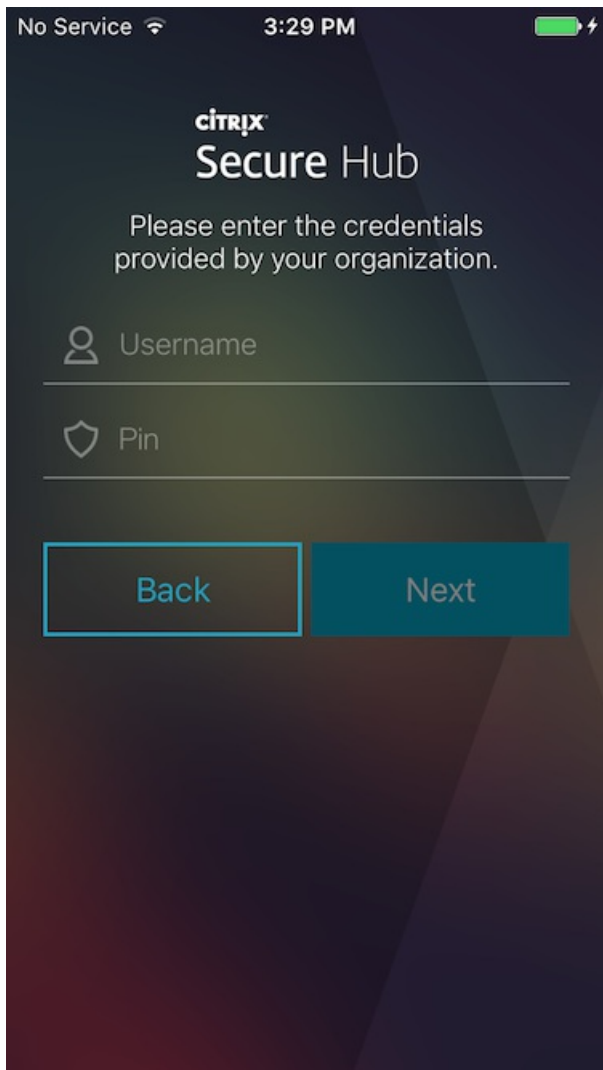
2. 在 iOS 设备主屏幕上，轻按 Secure Hub 应用程序。

3. Secure Hub 应用程序打开时，输入技术支持人员提供的服务器地址。

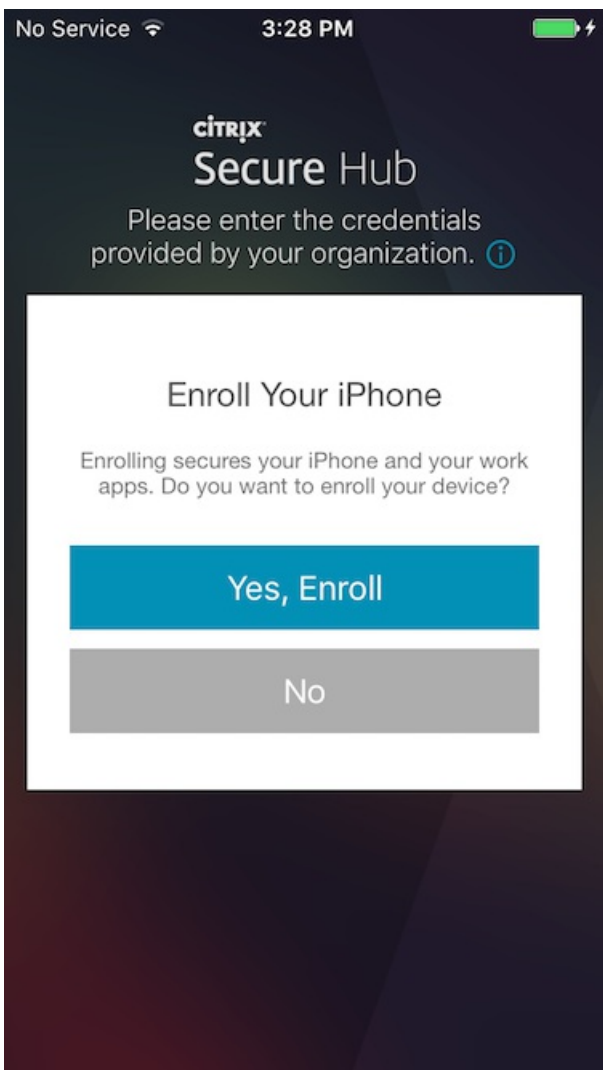
(显示的屏幕可能因示例而异，具体取决于 XenMobile 的配置方式。)

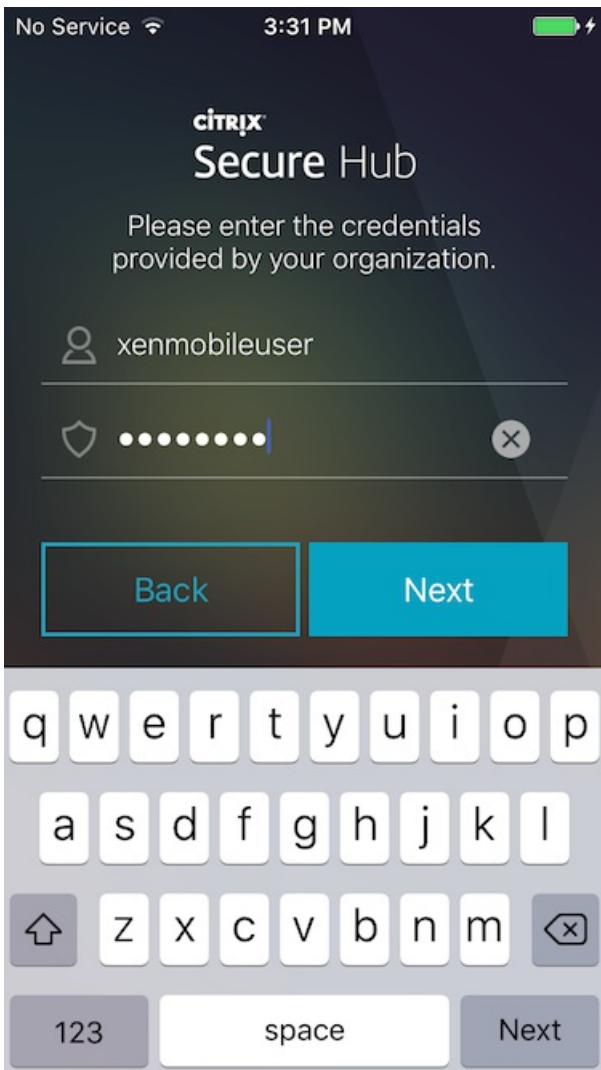


4. 系统提示时，输入您的用户名和密码或 PIN。单击下一步。

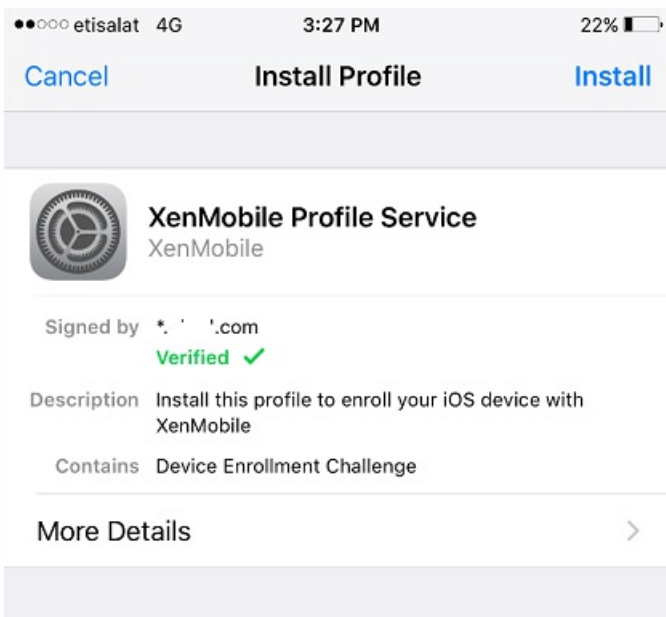


5. 系统提示注册时，单击是，注册，然后在收到提示时输入您的凭据。

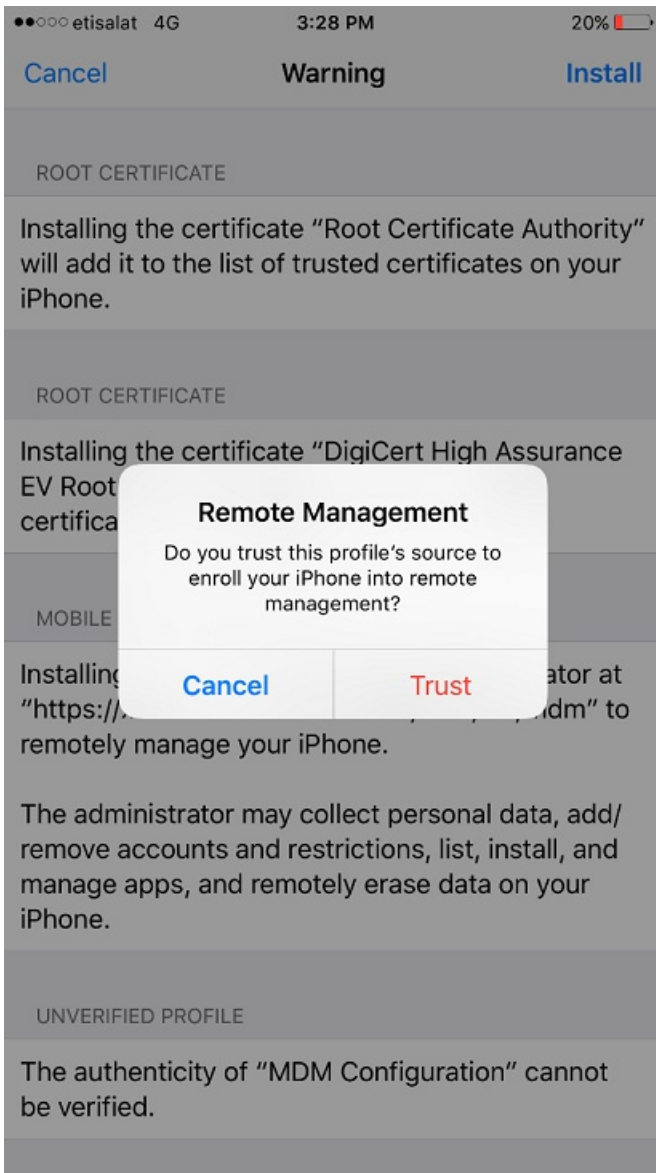




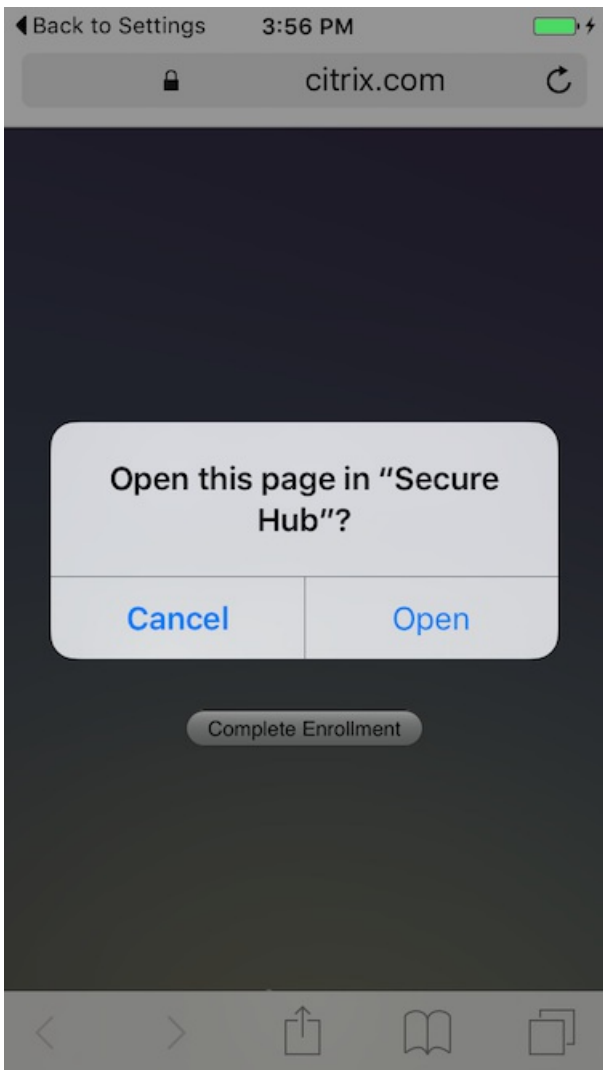
6. 轻按安装，安装 Citrix Profile Service。

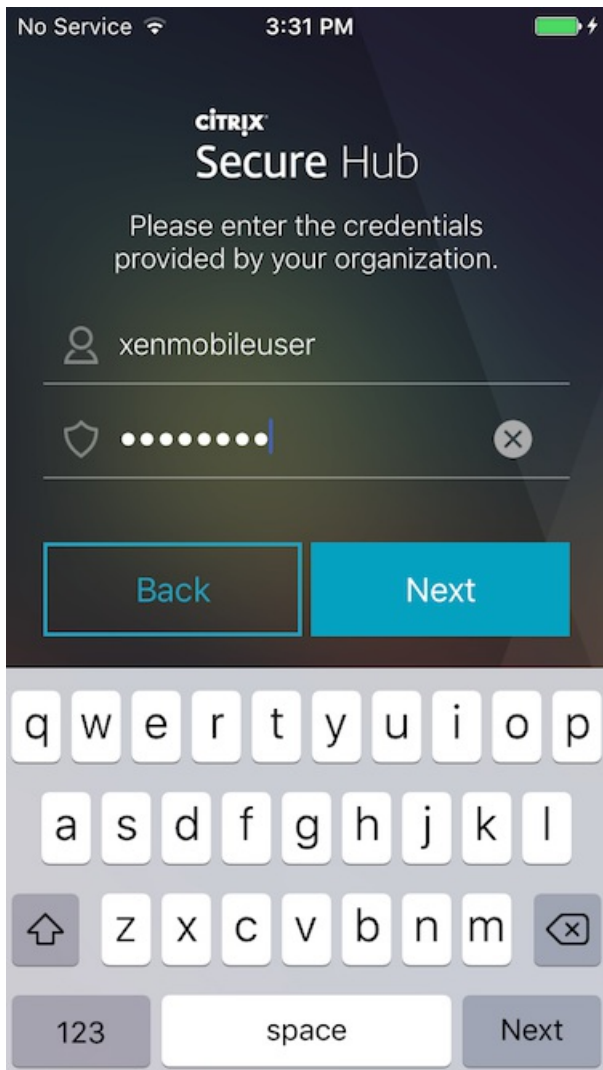


7. 轻按信任。



8. 轻按打开，然后输入您的凭据。





Mac OS X

可以在 XenMobile 中注册运行 OS X 的 Mac。Mac 用户直接从其设备无线注册。

注册 Mac 的步骤包括：

1. (可选) 在 XenMobile 控制台中注册 Mac 设备策略。有关设备策略的详细信息，请参阅[设备策略](#)。要了解可以为 Mac 配置的设备策略，请参阅[XenMobile 设备策略 \(按平台\)](#)。
2. 发送注册链接 `https://serverFQDN:8443/zdm/macos/otae`，用户可以在 Safari 中打开该链接。其中
 - **serverFQDN** 是运行 XenMobile 的服务器的完全限定域名 (FQDN)。
 - 端口 **8443** 是默认安全端口；如果已配置其他端口，请使用该端口替换 8443。
 - **zdm** 是服务器安装期间使用的实例名称。

有关发送安装链接的详细信息，请参阅[发送安装链接](#)。

3. 用户根据需要安装证书。用户是否会收到安装证书的提示取决于您是否为 iOS 和 Mac OS 配置了公众信任的 SSL 证书和公众信任的数字签名证书。有关证书的详细信息，请参阅[证书](#)。

4. 用户登录其 Mac 设备。
5. 安装 Mac 设备策略。

现在即可以像管理移动设备一样使用 XenMobile 管理 Mac。

Windows 设备

运行 Windows 10 的设备向 Azure 注册是一种联合 Active Directory 身份验证方法。可以采用下列方法之一将 Windows 10 设备连接到 Microsoft Azure AD：

- 首次打开设备电源时在 Azure AD 联接启用过程中在 MDM 中注册。
- 配置设备后，从“Windows 设置”页面执行 Azure AD 联接过程中在 MDM 中注册。

可以在 XenMobile 中注册运行以下 Windows 操作系统的设备：

- Windows 10 Phone 和 Tablet
- Windows Phone 8.1

用户可以直接通过其设备注册。

必须为用户注册配置自动发现和 Windows 发现服务，才能启用对受支持的 Windows 设备的管理。

必须先先在 XenMobile 中配置 Microsoft Azure 服务器，Windows 设备用户才能使用 Azure 进行注册。有关详细信息，请参阅 [Microsoft Azure Active Directory 服务器设置](#)。

注意

SSL 侦听器证书必须是公用证书，才能注册 Windows 设备。如果上载了自签名 SSL 证书，注册将失败。

在配置自动发现的情况下注册 Windows 设备

要启用对 Windows 设备的管理，Citrix 建议您配置自动发现和 Windows 发现服务。有关详细信息，请参阅 [在 XenMobile 中启用自动发现以执行用户注册](#)。

1. 在设备上，找到并安装所有可用的 Windows 更新。
2. 对于 Windows 10：在超级按钮菜单中，轻按设置，然后轻按帐户 > 访问工作单位或学校 > 连接到工作单位或学校。对于 Windows 8.1 Phone：轻按 PC 设置 > 网络 > 工作区。
3. 输入您的公司电子邮件地址，然后轻按继续（在 Windows 10 上）或打开设备管理（在 Windows 8.1 上）。要注册为本地用户，输入带有正确域名的不存在的电子邮件地址（例如，foo@mydomain.com）。这将允许您跳过已知 Microsoft 限制，即注册由 Windows 上的内置设备管理执行；在正在连接到服务对话框中，输入与本地用户关联的用户名和密码。设备即会自动发现 XenMobile 服务器并开始注册过程。
4. 输入您的密码。使用与某帐户相关的密码，该帐户应该是 XenMobile 中用户组的一部分。
5. 对于 Windows 10：在使用条款对话框中，指明您同意托管自己的设备，然后轻按接受。对于 Windows 8.1：在允许 IT 管理员提供的应用和服务对话框中，指明您同意托管自己的设备，然后轻按打开。

在未配置自动发现的情况下注册 Windows 设备

可以在不配置自动发现的情况下注册 Windows 设备。但是，Citrix 建议您配置自动发现。由于在不配置自动发现的情况下进行注册会导致在连接到所需的 URL 前调用端口 80，因此，这不是用于生产部署的最佳做法。Citrix 建议您仅在测试环境和概念验证部署中使用此过程。

1. 在设备上，找到并安装所有可用的 Windows 更新。

2. 对于 Windows 10：在超级按钮菜单中，轻按**设置**，然后轻按**帐户 > 访问工作单位或学校 > 连接到工作单位或学校**。对于 Windows 8.1：轻按**PC 设置 > 网络 > 工作区**。

3. 输入企业电子邮件地址。

4. 对于 Windows 10：如果未配置自动发现，则将显示一个选项，您可以在此处输入服务器详细信息，如步骤 5 中所述。对于 Windows 8.1：如果**自动检测服务器地址**设置为开，请轻按以关闭此选项。

5. 对于 Windows 10：在**输入服务器地址**字段中，键入地址：

`https://beta.managedm.com:8443/zdm/wpe`。

如果用于未经身份验证 SSL 连接的端口不是 8443，请使用相应的端口号替换此地址中的 8443。

对于 Windows 8.1：采用以下格式键入服务器地址：

`https://serverfqdn:8443/serverInstance/Discovery.svc`。

如果用于未经身份验证 SSL 连接的端口不是 8443，请使用相应的端口号替换此地址中的 8443。

6. 键入密码。

7. 对于 Windows 10：在**使用条款**对话框中，指明您同意托管自己的设备，然后轻按**接受**。对于 Windows 8.1：在**允许 IT 管理员提供的应用和服务**对话框中，指明您同意托管自己的设备，然后轻按**打开**。

注册 Windows Phone 设备

要在 XenMobile 中注册 Windows Phone 设备，用户需要使用其 Active Directory 或内部网络电子邮件地址和密码。如果未设置自动发现，用户还需要 XenMobile 服务器的服务器 Web 地址。然后，他们需要按照此过程在设备上完成注册。

注意：如果您计划通过 Windows Phone 企业应用商店部署应用程序，则在用户注册前，请确保您已配置**企业中心策略**（具有签名的 Secure Hub、适用于您支持的每个平台的 Windows Phone 应用程序）。

1. 在 Windows Phone 的主屏幕上，轻按**设置**图标。

- 对于 Windows 10：轻按**帐户 > 访问工作单位或学校 > 连接到工作单位或学校**，或轻按**帐户 > 工作单位访问权限 > 注册设备管理**，具体取决于您使用的版本。
- 对于 Windows 8.1：轻按**PC 设置 > 网络 > 工作区**，然后轻按**添加帐户**。

2. 在下一屏幕上，输入电子邮件地址和密码，然后轻按**登录**。

如果为域配置了自动发现，随后几个步骤中所需的信息将会自动填充。继续执行步骤 8。

如果没有为域配置自动发现，请继续执行下一步。要注册为本地用户，输入带有正确域名的不存在的电子邮件地址（例如，foo@mydomain.com）。这样允许您绕过已知的 Microsoft 限制；在正在连接到**服务**对话框中，输入与本地用户关联的用户名和密码。

3. 在下一屏幕上，输入 XenMobile 服务器的 Web 地址，例如 `https://:<端口号>/<实例名称>/wpe`。例

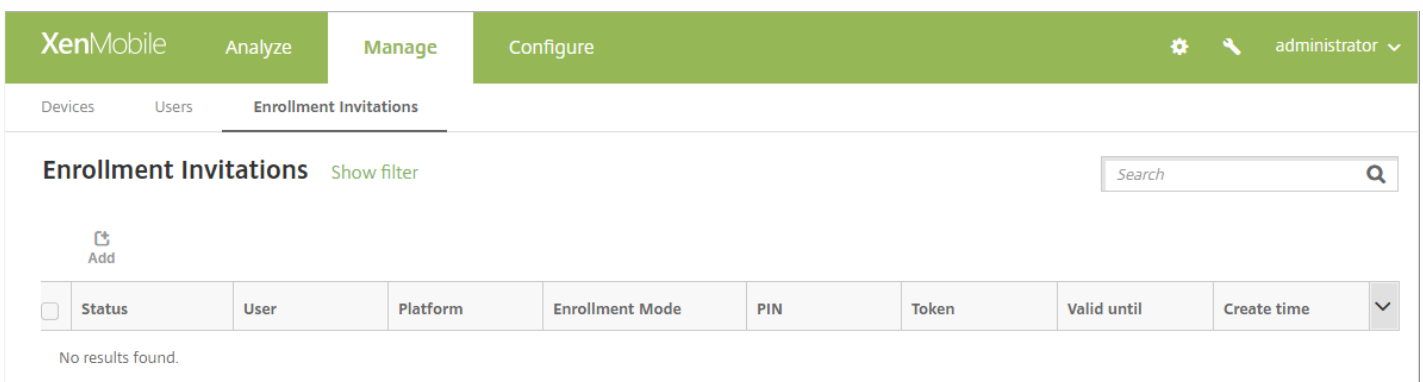
如，`https://mycompany.mdm.com:8443/zdm/wpe`。**注意：**端口号必须适应您的实现，但应该与您进行 iOS 注册时使用的端口相同。

4. 如果通过用户名和域进行身份验证，请输入用户名和域，然后轻按登录。
5. 如果出现提示证书有问题的屏幕，该错误是由于使用自签名证书造成的。如果服务器可信，轻按继续。否则，轻按取消。
6. 在 Windows Phone 8.1 上，添加帐户时，可以选择 **Install company app**（安装企业应用程序）。如果管理员已配置企业应用商店，请选中此选项，然后轻按完成。如果取消选中此选项，您需要重新注册设备才能接收 Company App Store。
7. 在 Windows Phone 8.1 上，在已添加帐户屏幕上，轻按完成。
8. 要强制连接到某一服务器，请轻按“刷新”图标。如果设备没有手动连接到服务器，XenMobile 会尝试重新连接。XenMobile 会每 3 分钟连续 5 次连接设备，然后间隔改为 2 小时。您可以在服务器属性中的 **Windows WNS 检测信号间隔** 中修改此连接率。注册完成后，Secure Hub 将在后台注册。安装完成时不会提示。从所有应用程序屏幕轻按 Secure Hub。

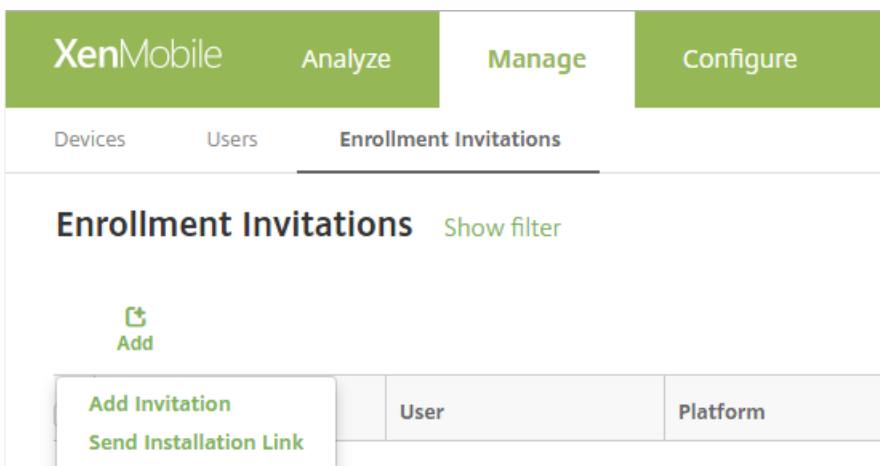
发送注册邀请

在 XenMobile 控制台中，可以向 iOS 或 Android 设备的用户发送注册邀请。还可以向 iOS、Android、Windows 或 Mac 设备的用户发送安装链接。

1. 在 XenMobile 控制台中，单击管理 > 注册邀请。此时将显示注册邀请页面。



2. 单击添加。将显示一个菜单，其中列出了注册选项。

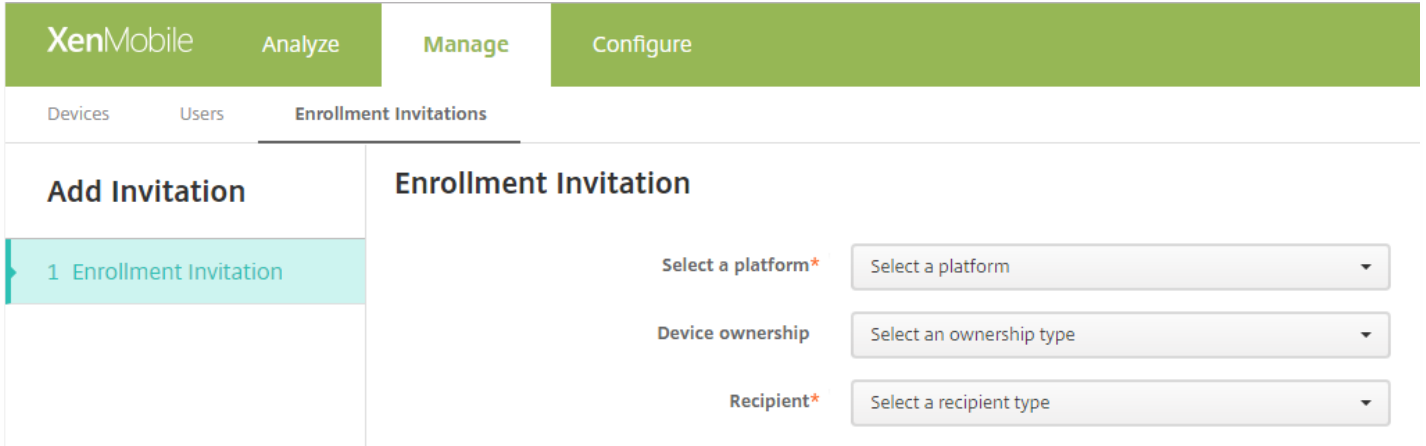


- 要向用户或组发送注册邀请，请单击添加邀请，然后，请参阅“发送邀请”了解配置此设置的步骤。

- 要通过 SMTP 或 SMS 向一系列收件人发送注册安装链接，请单击**发送安装链接**，然后，请参阅“发送安装链接”了解配置此设置的步骤。

发送邀请

1. 单击**添加邀请**。此时将显示注册邀请屏幕。



2. 配置以下设置：

- **选择平台**：在列表中，单击 **iOS** 或 **Android**。
- **设备所有权**：在列表中，单击**公司**或**员工**。
- **收件人**：在列表中，单击**用户**或**组**。

根据您选择的收件人，您将看到要配置的更多设置。对于**用户**设置，请参阅“向用户发送注册邀请”；对于**组**设置，请参阅“向组发送注册邀请”。

向用户发送注册邀请

1. 配置以下用户设置：

- **用户名**：键入用户名。用户必须作为本地用户或 Active Directory 中的用户存在于 XenMobile 服务器中。如果用户是本地用户，确保设置用户的电子邮件属性以便发送用户通知。如果用户是 Active Directory 中的用户，请确保配置 LDAP。
- **设备信息**：在列表中，单击**序列号**、**UDID** 或 **IMEI**。选择某个选项后，将显示一个字段，您可以在此处键入设备的相应值。
- **电话号码**：可选，键入用户的电话号码。
- **运营商**：在列表中，单击用户电话号码关联的运营商。
- **注册模式**：在列表中，单击希望用户采用的注册模式。默认值为**用户名 + 密码**。可能的选项包括：
 - 高安全性
 - 邀请 URL
 - 邀请 URL + PIN
 - 邀请 URL + 密码
 - 双重身份验证
 - 用户名 + PIN

注意：选择包含 PIN 的注册模式时，会显示**注册 PIN 模板**字段，您可以在此处单击**注册 PIN**。

- **代理下载模板**：在列表中，单击用于注册邀请的模板。此选项的选择项基于平台类型。例如，如果选择 **iOS** 平台，将显示 **iOS Download Link** (iOS 下载链接) 选项。
- **注册 URL 模板**：在列表中，单击**注册邀请**。
- **注册确认模板**：在列表中，单击**注册确认**。
- **此时间后过期**：此字段在配置注册模式时设置，用于指出注册的过期时间。有关配置注册模式的详细信息，请参阅[配置注册模式](#)。
- **最大尝试次数**：此字段在配置注册模式时设置，用于指出注册过程发生的最大次数。有关配置注册模式的详细信息，请参阅[配置注册模式](#)。

- **发送邀请**：选择开以立即发送邀请，或单击关仅将邀请添加到注册邀请页面上的表格中。

2. 如果已启用**发送邀请**，请单击**保存并发送**；否则，请单击**保存**。邀请将显示在注册邀请页面上的表格中。

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name
	MDM MAM	net		iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account
	MDM MAM	net		iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days	
	MDM MAM	net		iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days	

向组发送注册邀请

Add Invitation

1 Enrollment Invitation

Enrollment Invitation

Select a platform* iOS

Device ownership Corporate

Recipient* Group

Domain* Select a domain

Group* Select a group

Enrollment mode* User name + Password

Template for agent download Select a template

Template for enrollment URL Select a template

Template for enrollment confirmation Select a template

Expire after Never

Maximum Attempts 0

Send invitation OFF

1. 配置以下设置：

- **域**：在列表中，单击要从中选择组的域。
- **组**：在列表中，单击要接受邀请的组。
- **注册模式**：在列表中，单击希望组中的用户采用的注册方法。默认值为**用户名 + 密码**。可能的选项包括：

- 高安全性
- 邀请 URL
- 邀请 URL + PIN
- 邀请 URL + 密码
- 双重身份验证
- 用户名 + PIN

注意：选择包含 PIN 的注册模式时，会显示注册 **PIN** 模板字段，您可以在此处单击注册 **PIN**。

- **代理下载模板**：在列表中，单击用于注册邀请的模板。对此选项的选择基于平台类型。例如，如果选择 **iOS** 平台，将显示 **iOS Download Link** (iOS 下载链接) 选项。
- **注册 URL 模板**：在列表中，单击注册邀请。
- **注册确认模板**：在列表中，单击注册确认。
- **此时间后过期**：此字段在配置注册模式时设置，用于指出注册的过期时间。有关配置注册模式的详细信息，请参阅[配置注册模式](#)。
- **最大尝试次数**：此字段在配置注册模式时设置，用于指出注册过程发生的最大次数。有关配置注册模式的详细信息，请参阅[配置注册模式](#)。
- **发送邀请**：选择开以立即发送邀请，或单击关仅将邀请添加到注册邀请页面上的表格中。

2. 如果已启用发送邀请，请单击保存并发送；否则，请单击保存。邀请将显示在注册邀请页面上的表格中。

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name
	MDM MAM	net		iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account
	MDM MAM	net		iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days	
	MDM MAM	net		iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days	

发送安装链接

XenMobile Analyze Manage Configure

Devices Users Enrollment Invitations

Send Link

1 Details

Send Installation Link

Recipients* Add

Channels ⓘ

SMTP ⚠ Channel cannot be activated until you define the SMTP server in the [Notification Server](#) section in Settings.

Sender

Subject

Message

SMS ⚠ Channel cannot be activated until you define the SMS server in the [Notification Server](#) section in Settings.

Message

您必须通过设置页面在通知服务器上配置通道（SMTP 或 SMS），才能发送注册安装链接。有关详细信息，请参阅[通知](#)。

1. 配置以下设置：

- **收件人**：对于您要添加的每个收件人，请单击“添加”并执行以下操作：
 - **电子邮件**：键入收件人的电子邮件地址。此字段为必填字段。
 - **电话号码**：键入收件人的电话号码。此字段为必填字段。
 - 单击**保存**。

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

要编辑现有收件人，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

- **通道**：选择用于发送注册安装链接的通道。可以通过 **SMTP** 或 **SMS** 发送通知。在[通知服务器](#)的[设置](#)页面上配置服务器设置后，才能激活这些通道。有关详细信息，请参阅[通知](#)。
 - **SMTP**：配置以下可选设置。如果不在这些字段中键入任何内容，将使用为所选平台配置的通知模板中指定的默认值：
 - **发件人**。键入可选发件人。
 - **主题**：键入消息的可选主题。例如，“注册您的设备”。
 - **消息**：键入要发送给收件人的可选消息。例如，“注册您的设备以获取组织应用程序和电子邮件的访问权限。”
 - **SMS**：配置以下设置。如果不在此字段中键入任何内容，将使用为所选平台配置的通知模板中指定的默认值：
 - **消息**：键入要发送给收件人的消息。对于基于 SMS 的通知，此为必填字段。

注意：在北美，超过 160 个字符的 SMS 消息将通过多条消息发送。

2. 单击发送。

注意

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

设备注册限制

Feb 27, 2017

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

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

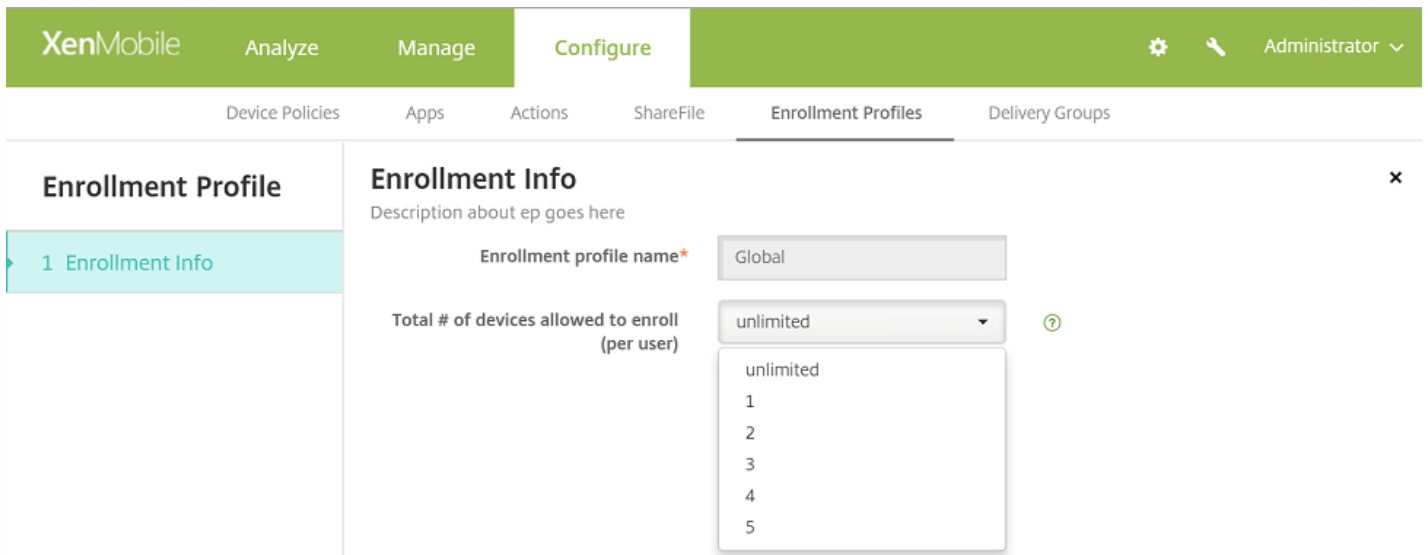
配置全局设备注册限制

1. 转至配置 > 注册配置文件。
2. 单击全局，然后选择编辑。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-navigation options: 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Enrollment Profiles' section is active, displaying a table with columns for 'Enrollment profile name', 'Created on', 'Updated on', and 'Device limit'. Two profiles are listed: 'ep1' with a limit of 3, and 'Global' with a limit of 'unlimited'. The 'Global' profile is highlighted in light blue. Below the table, it says 'Showing 1 - 2 of 2 items'. A context menu is open over the 'Global' profile, showing 'Edit' and 'Reset' options.

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	ep1	2/11/16 1:44 PM	2/11/16 1:44 PM	3
<input type="checkbox"/>	Global	2/8/16 11:21 AM	2/8/16 11:21 AM	unlimited

此时会显示注册信息屏幕，其中全局自动填充为配置文件名称。在此屏幕中，您可以选择允许用户注册的设备总数。此限制适用于所有 XenMobile 注册者。

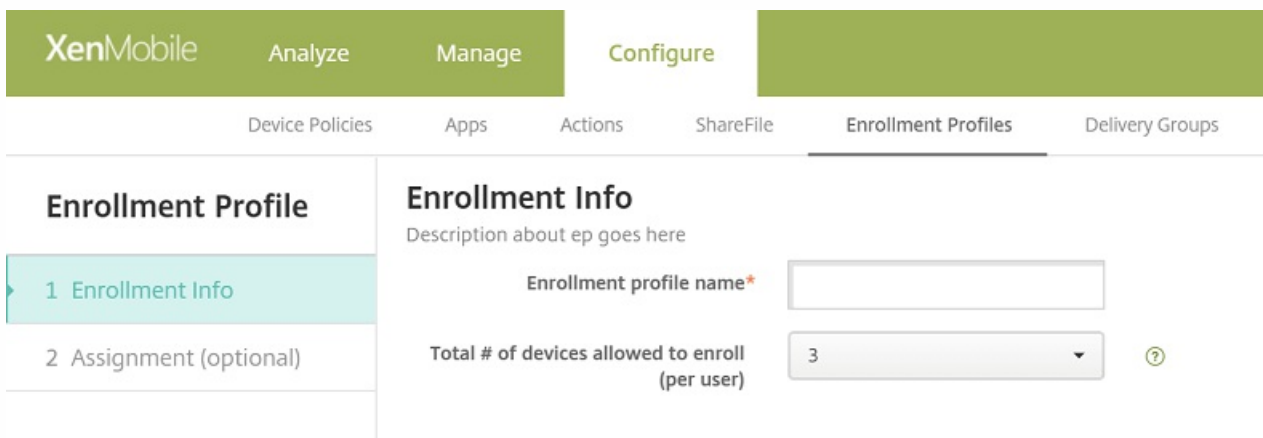


配置交付组设备注册限制

1. 转至**配置 > 注册配置文件 > 添加**。

此时会显示注册信息屏幕。

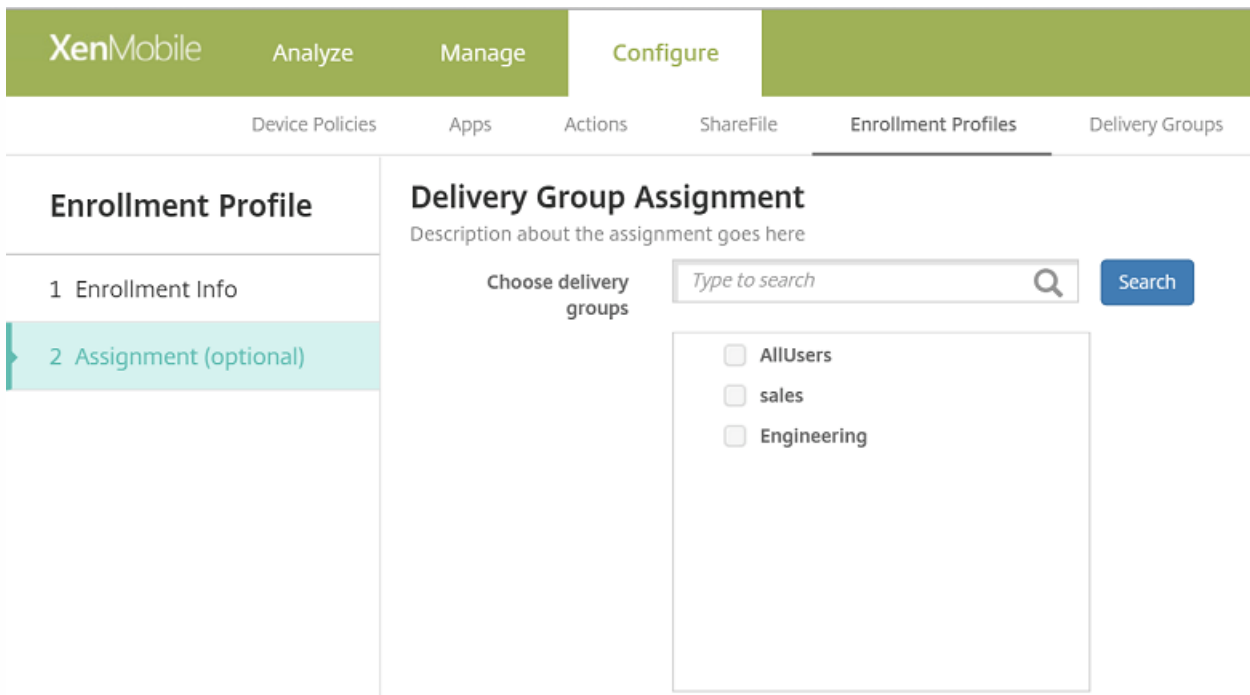
2. 输入新的注册配置文件的名称，然后选择此配置文件的成员允许注册的设备数量。



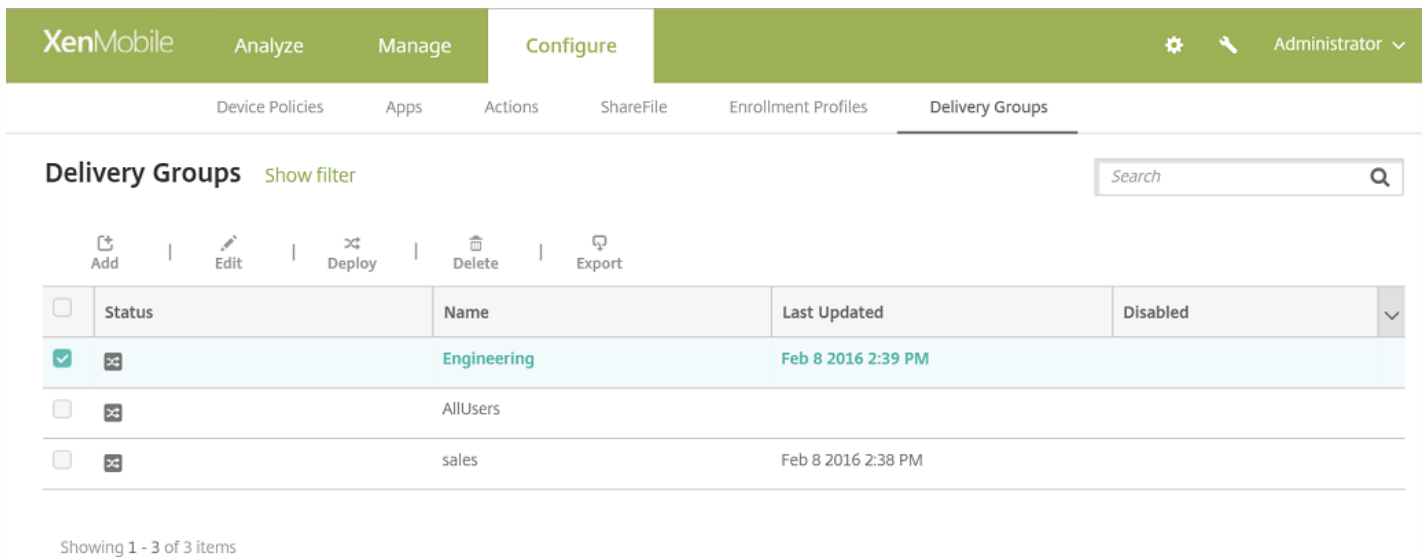
3. 单击**下一步**。

此时会显示交付组分配屏幕。

4. 选择要将设备注册限制应用到的交付组，然后单击**保存**。



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



此时会显示注册配置文件屏幕。

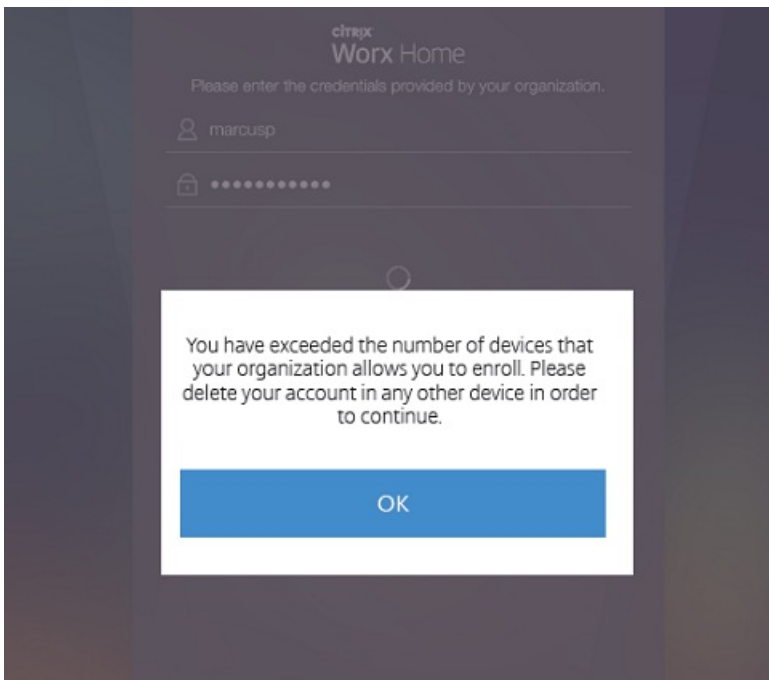
5. 在此屏幕中，选择要应用到此交付组的注册配置文件，然后单击下一步查看并保存更改。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, with sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' tab is selected, and the 'Enrollment Profile' sub-tab is active. The main content area displays the 'Enrollment Profile' configuration page. On the left, a sidebar lists the steps: 1 Delivery Group Info, 2 User, 3 Resource (optional), Policies, Apps, Actions, ShareFile, Enrollment Profile (highlighted), and 4 Summary. The main area shows the 'Enrollment Profile' title and a subtitle: 'Select the enrollment profile that you want the users in this delivery group to see'. Below this, there are three radio button options: 'ep1', 'ep2', and 'Global'. The 'Global' option is selected. At the bottom right, there are 'Back' and 'Next >' buttons.

实行设备注册限制时的用户体验

设置了设备注册限制后，如果用户尝试注册一个新设备，他们要遵循以下步骤：

1. 登录到 Secure Hub。
2. 输入要注册的服务器地址。
3. 输入凭据。
4. 如果达到了设备限制，则会显示一条错误消息，告知用户注册设备数已超过上限，他们应联系管理员。



此时会再次显示 Secure Hub 注册屏幕。

共享设备

Feb 27, 2017

XenMobile 允许您配置可由多个用户共享的设备。例如，利用共享设备功能，医院的临床医生可以使用附近的任何设备访问应用程序和数据，而无需随身携带特定设备。您可能还希望执法、零售和制造等领域的工作者转向使用共享设备，以降低装备成本。

关于共享设备的要点

MDM 模式

- 可在 iOS 和 Android 平板电脑和手机上使用。XenMobile Enterprise 共享设备不支持基本 Device Enrollment Program (DEP) 注册。必须使用经过授权的 DEP 在此模式下注册共享设备。
- 不支持客户端证书身份验证、Citrix PIN、Touch ID、用户熵和双重身份验证。

MDM+MAM 模式

- 只能在 iOS 和 Android 平板电脑上使用。
- 在 XenMobile 10.3.x 及更高版本上支持。
- 仅支持 Active Directory 用户名和密码身份验证。
- 不支持客户端证书身份验证、Worx PIN、Touch ID、用户熵和双重身份验证。
- 不支持仅 MAM 模式。设备必须在 MDM 下注册。
- 仅支持 Secure Mail、Secure Web 和 ShareFile 移动应用程序。不支持 HDX 应用程序。
- 仅支持 Active Directory 用户；不支持本地用户和组
- 现有仅 MDM 共享设备要更新到 MDM+MAM 模式需要重新注册。
- 用户只能共享 XenMobile 应用程序以及 MDX 打包应用程序；他们无法共享设备上的本机应用程序。
- 在首次注册期间下载好 XenMobile 应用程序后，不必在新用户每次登录设备时重新下载。新用户拿到设备后，只需登录即可使用。
- 在 Android 设备上，为了出于安全考虑隔离每个用户的数据，应在 XenMobile 控制台将 **Disallow rooted devices**（不允许已获得 root 权限的设备）策略设置为开。

注册共享设备的必备条件

您必须先执行以下操作，才能注册共享设备：

- 创建共享设备注册用户角色。请参阅[使用 RBAC 配置角色](#)。
- 创建共享设备用户。请参阅在[XenMobile 中添加、编辑或删除本地用户](#)。
- 创建包含要应用于共享设备注册用户的基本策略、应用程序和操作的交付组。请参阅[管理交付组](#)。

使用 MDM+MAM 模式的必备条件

1. 创建一个名称类似于 **Shared Device Enrollers** 的 Active Directory 组。
2. 将要注册共享设备的 Active Directory 用户添加到此组。如果要使用一个专用于注册共享设备的新帐户，请创建新的 Active Directory 用户（例如 **sdenroll**），并将该用户添加到 Active Directory 组。

共享设备要求

为提供最佳用户体验，包括无提示安装和应用程序删除，Citrix 建议在下列平台上配置共享设备：

- iOS 9 和 10
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x (仅 MDM 模式)

配置共享设备

按照以下步骤配置共享设备。

1. 从 XenMobile 控制台，单击右上角的齿轮图标。此时将显示设置页面。
2. 单击基于角色的访问控制，然后单击添加。此时会显示添加角色屏幕。
3. 创建一个名为共享设备注册用户的共享设备注册用户角色，并在授权访问下设置共享设备注册人员权限。请务必展开控制台功能中的设备，然后选择选择性擦除设备。此设置可确保在取消设备注册后，使用共享设备注册人员帐户置备的应用程序和策略通过 Secure Hub 被删除。

请保留应用权限的默认设置至所有用户组，或者使用至特定用户组向特定 Active Directory 用户组分配权限。

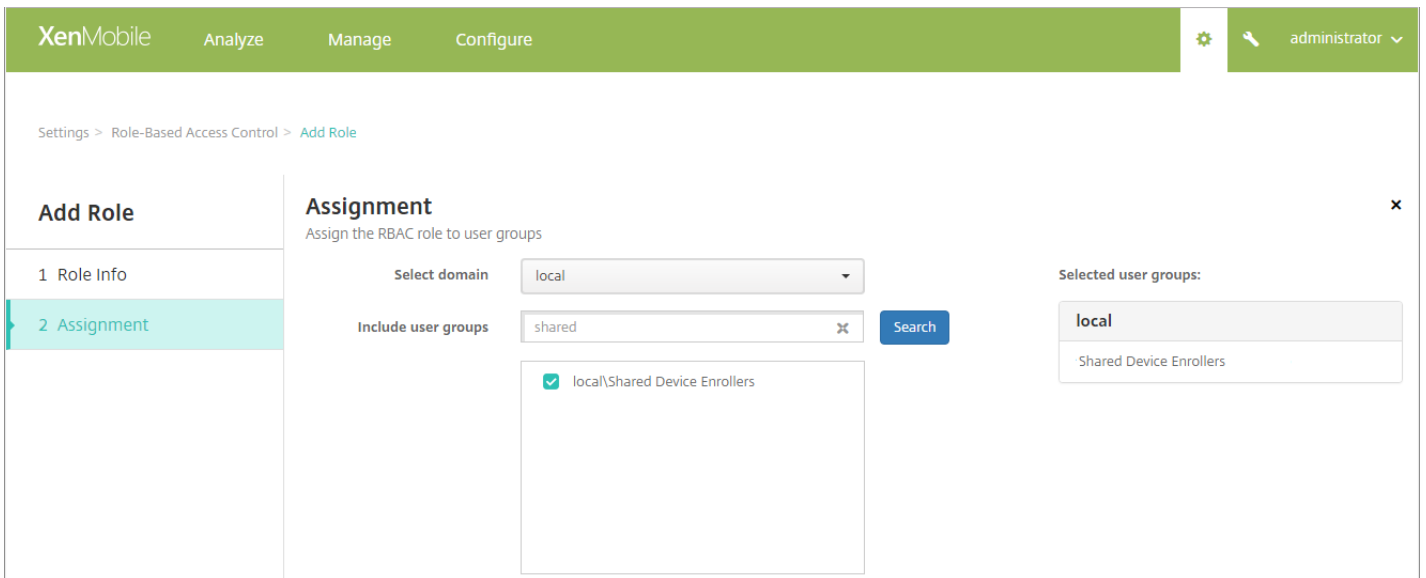
The screenshot shows the 'Add Role' configuration page in the XenMobile console. The 'Role Info' section is expanded, showing the following settings:

- RBAC name:** An empty text input field.
- RBAC template:** A dropdown menu with 'Select a template' and an 'Apply' button.
- Authorized access:** A list of permissions with checkboxes:
 - Admin console access
 - Self Help Portal access
 - Shared devices enroller
 - Remote Support access
 - Public api access
- Console features:** A list of features with checkboxes and a dropdown menu:
 - Dashboard
 - Reporting
 - Devices
 - Full Wipe device
 - Clear Restriction
 - Selective Wipe device
 - View locations
 - Lock device
 - Unlock device

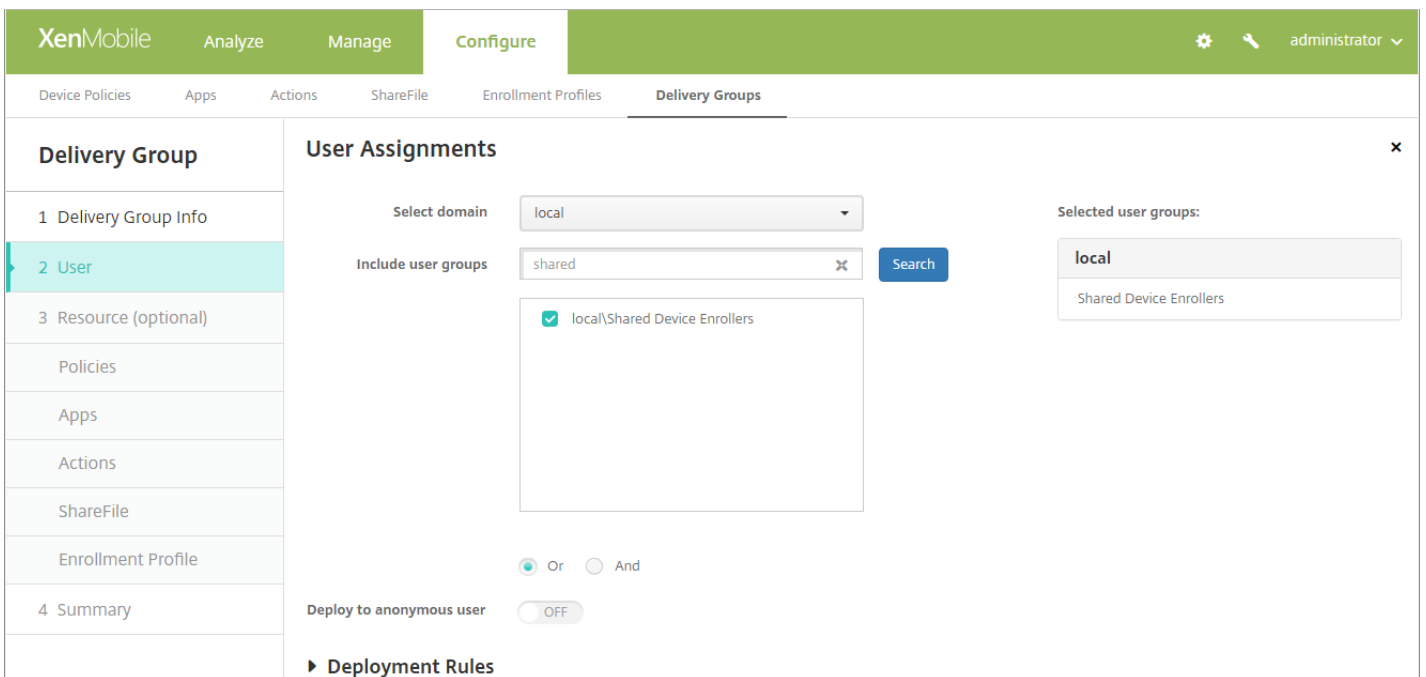
- Apply permissions:** Two radio buttons:
- To all user groups
- To specific user groups

A 'Next >' button is located at the bottom right of the configuration area.

单击下一步转至分配屏幕。将刚创建的共享设备注册角色分配给在步骤 1 中的“必备项”下为共享设备注册用户创建的 Active Directory 组。在下图中，**citrix.lab** 是 Active Directory 域，而共享设备注册人员是 Active Directory 组。



4. 创建一个交付组以包含要在用户未登录时应用于设备的基本策略、应用程序和操作，然后将该交付组与共享设备注册用户 Active Directory 组相关联。



5. 在共享设备上安装 Secure Hub，然后使用共享设备注册用户帐户将其注册到 XenMobile 中。现在即可通过 XenMobile 控制台查看并管理设备。有关详细信息，请参阅[注册设备](#)。

6. 要为已验证身份的用户应用不同的策略或提供额外的应用程序，必须创建与这些用户关联的交付组，并将该交付组仅部署到共享设备。在创建交付组时，请配置相应的部署规则，以确保将软件包部署到共享设备。有关详细信息，请参阅[配置部署规则](#)。

7. 要停止共享设备，请执行选择性擦除，从设备中删除共享设备注册用户帐户以及部署到该设备的所有应用程序和策略。

共享设备用户体验

MDM 模式

用户只会看到他们可用的资源，而且在每个共享设备上都能获得同样的使用体验。共享设备注册策略和应用程序会始终保留在设备上。当未在共享设备中注册的用户登录到 Secure Hub 时，该用户的策略和应用程序将部署到设备中。在用户注销时，与共享设备注册不同的策略和应用程序会被删除，而共享设备注册资源则保持不变。

MDM+MAM 模式

Secure Mail 和 Secure Web 将在由共享设备注册用户注册后部署到设备中。用户数据会安全地保留在设备上。当其他用户登录到 Secure Mail 或 Secure Web 时，系统不会将这些数据公开给这些用户。

一次只能有一个用户登录到 Secure Hub。上一个用户必须注销，下一个用户才能登录。出于安全原因，Secure Hub 不在共享设备上存储用户凭据，因此用户必须在每次登录时输入其凭据。为确保新用户不能访问为前面的用户提供的资源，Secure Hub 在删除与以前用户相关的策略、应用程序和数据时不允许新用户登录。

共享设备注册不会更改应用程序升级过程。您可以照常将升级推送给共享设备的用户，而共享设备的用户可以直接在其设备上升级应用程序。

建议的 Secure Mail 策略

- 要确保 Secure Mail 获得最佳性能，请根据要共享设备的用户数设置 **Max sync period**（最长同步期限）。不建议允许无限同步。

共享设备的用户数量	建议的最长同步期限
21 到 25	1 周或更短
6 到 20	2 周或更短
5 或更少	1 个月或更短

- 阻止启用联系人导出以避免向共享设备的其他用户显示用户的联系人。
- 在 iOS 上，只能基于用户设置以下设置。所有其他设置在共享该设备的用户之间相同：

通知
签名
外出
同步邮件期限
S/MIME
检查拼写

Android at Work

Feb 27, 2017

Android at Work (以前称为 Android for Work) 是运行 Android 5.0 及更高版本的 Android 设备上提供的一个安全工作区。该工作区将企业帐户、应用程序和数据与个人帐户、应用程序和数据隔离开来。在 XenMobile 中, 通过允许用户在其设备上创建单独的工作配置文件来管理自带设备 (BYOD) 以及公司拥有的 Android 设备。通过结合使用硬件加密以及您所部署的策略, 可以安全地隔离设备上的企业和个人区域。您可以在不影响用户个人区域的情况下, 远程管理或擦除所有公司策略、应用程序和数据。有关支持的 Android 设备的详细信息, 请参阅 [Google Android Enterprise Web](#) 页面。

使用 Google Play 可添加、购买和审批应用程序, 以便部署到设备上的 Android at Work 工作区。可以使用 Google Play 部署您的私有 Android 应用程序, 以及公共和第三方应用程序。向 XenMobile 中添加面向 Android at Work 的付费公共应用商店应用程序时, 可以查看批量购买许可状态。该状态显示可用许可证总数、现在正在使用的数量以及占用这些许可证的每个用户的电子邮件地址。有关向 XenMobile 中添加应用程序的详细信息, 请参阅 [向 XenMobile 中添加公共应用商店应用程序](#)。

Android at Work 的要求:

- 可公开访问的域
- Google 管理员帐户
- 支持托管配置文件并且运行 Android 5.0+ Lollipop 的设备
- 安装了 Google Play 的 Google 帐户
- 用户设备上设置的工作配置文件

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

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

管理 Android at Work 时可以使用以下链接:

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

Android at Work 必备条件

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

- 创建 Android at Work 帐户。
- 设置一个服务帐户。
- 下载 Android at Work 证书
- 启用并授权 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 设置, 并在 XenMobile 中管理 Android 应用程序。有关创建一组凭据的详细信息, 请参阅 [Google Play 凭据](#)。

创建一个 Android at Work 帐户

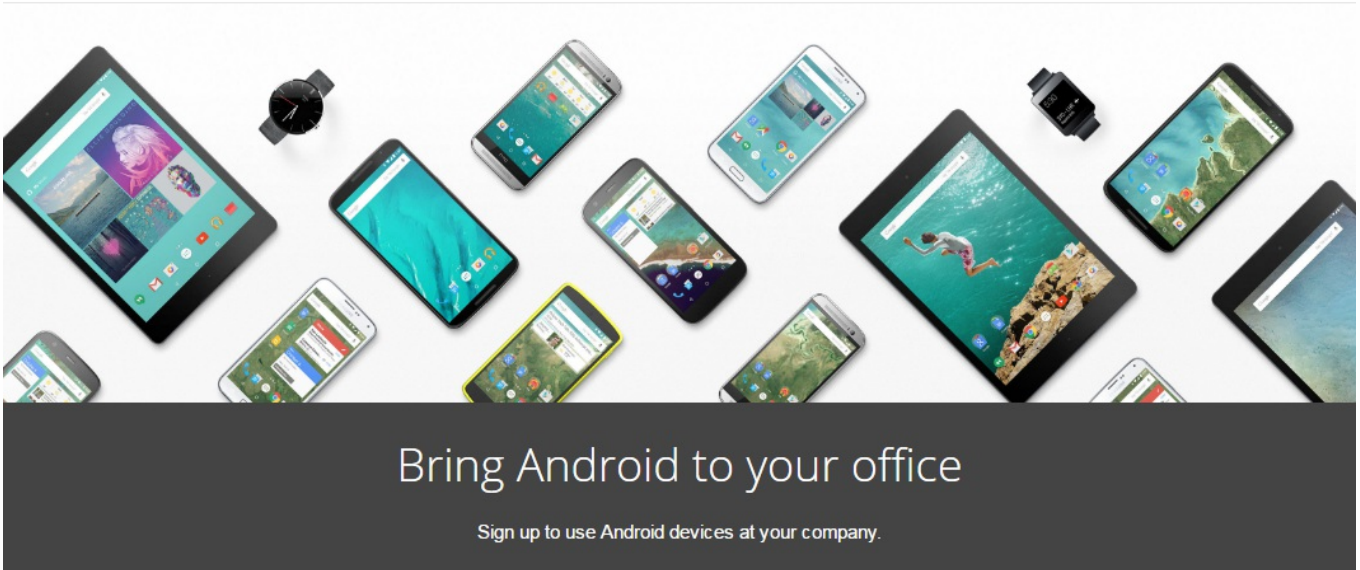
必须满足以下必备条件, 才能设置 Android at Work 帐户:

- 拥有域名; 例如 example.com。
- 允许 Google 验证您是否拥有该域。
- 通过企业移动性管理 (EMM) 提供程序 (例如 XenMobile 10.1 或更高版本) 启用和管理 Android at Work。

如果已向 Google 验证您的域名, 可以跳至此步骤: [设置 Android at Work 服务帐户并下载 Android at Work 证书](#)。

1. 导航到 https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK。

此时将显示以下页面, 您可以在此页面中键入管理员和公司信息。



1 About you

Name

Current work email

Doesn't have to be an official business email.

Phone

2. 键入管理员用户信息。

1 About you

Name

 ✓ ✓

Current work email

 ✓ Doesn't have to be an official business email.

Phone

 ✓

2. 键入您的公司信息（管理员帐户信息除外）。

② About your business

Business name

EXAMPLE CORP ✓

Business domain address

You'll need to verify that you own this domain.

example.com ✓

Number of employees

Country/Region

1 employee ▾

United States ▾

③ Your Google admin account [Why do I need this?](#)

Username

Create an account to manage Android for Work

justa.user ✓

@

example.com

Create a password

8-character minimum; case sensitive

..... ✓

..... ✓

此过程中的第一个步骤已完成，请继续查看下面的页面。



Bring Android to your office

With Android, you can manage your company's devices and keep them secure.



Create your domain admin account



Verify domain ownership

Verify you're the owner of your company's domain and protect its security.

START



Connect with your provider

Allow an enterprise mobility management (EMM) provider to keep your organization's devices secure.

验证域所有权


允许 Google 通过以下方式之一验证您的域：

- 将 TXT 或 CNAME 记录添加到域主机的 Web 站点。
- 向域的 Web 服务器上载 HTML 文件。
- 向您的主页添加 标记。Google 建议使用第一种方法。本文不包含验证域所有权的步骤，但您可以从以下网址找到所需的信息：<https://support.google.com/a/answer/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. 单击 **Verify**（验证）。



Verify domain ownership


Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)

After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

Note: Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

[VERIFY](#)



Verify domain ownership


Verification checklist

Follow these steps to help Google verify that you own the domain **example.com**. [Learn more](#)

- I have successfully logged in.
- I have opened the control panel for my domain.
- I have created the CNAME record.
- I have saved the CNAME record.

[VERIFY](#)

3. Google 验证您的域所有权。



Verify domain ownership

Verifying your domain ownership

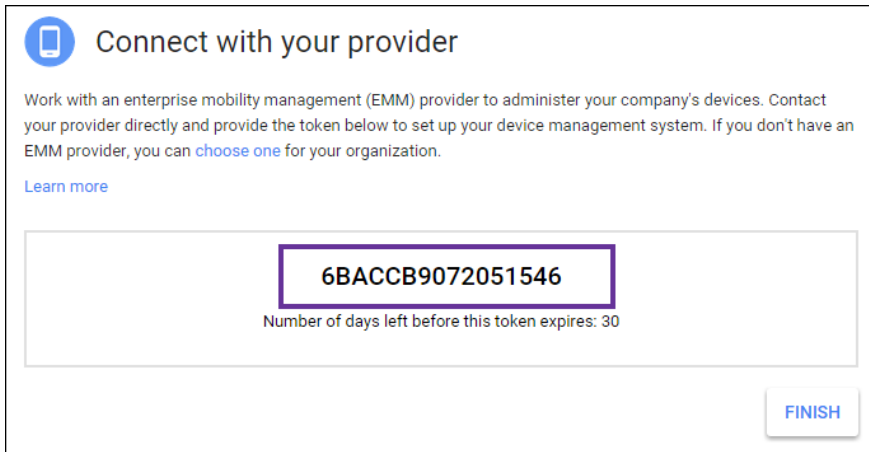
The domain host is updating your information. This might take a bit—you can close this window and come back to [admin.google.com](#) later without interrupting the process. [Learn more](#)

Estimated time remaining: 5 minutes

4. 成功验证后，将显示以下页面。单击继续。



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



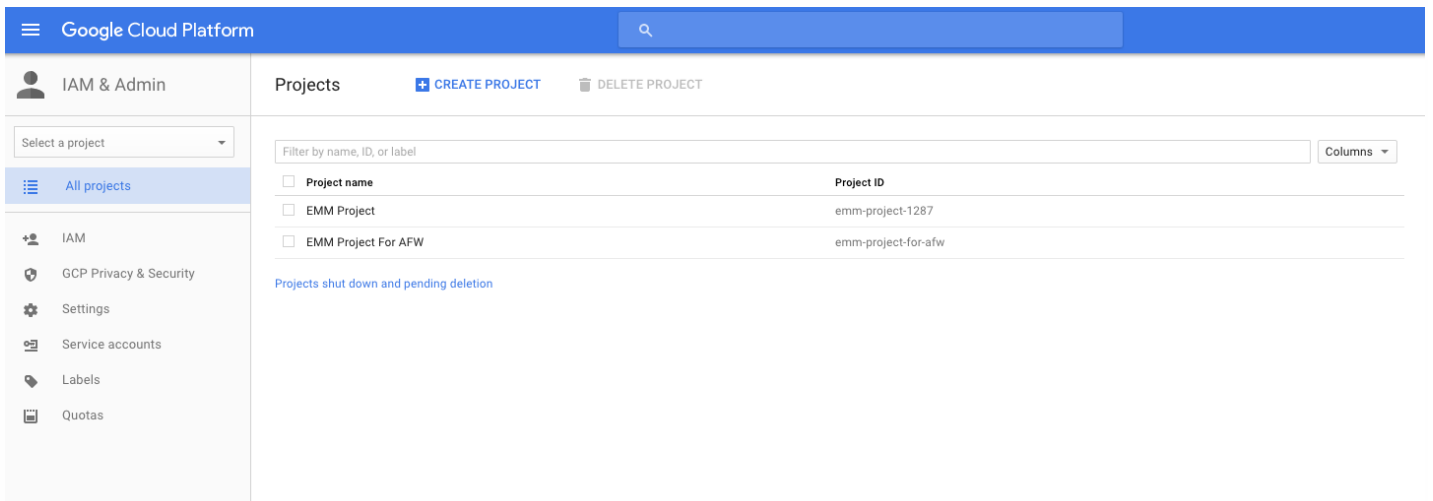
6. 单击 **Finish** (完成) 以完成 Android at Work 设置。此时将显示一个页面，指示您已成功验证您的域。

创建 Android at Work 服务帐户后，可以登录 Google 管理控制台管理您的移动性管理设置。

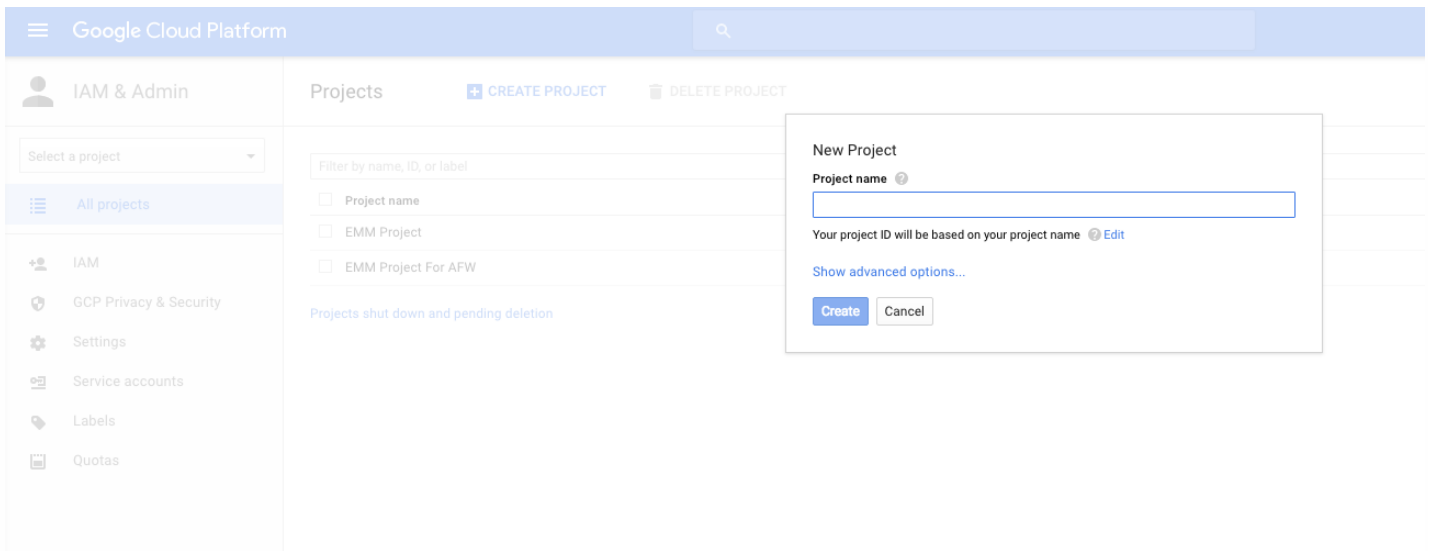
设置 Android at Work 服务帐户并下载 Android at Work 证书

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

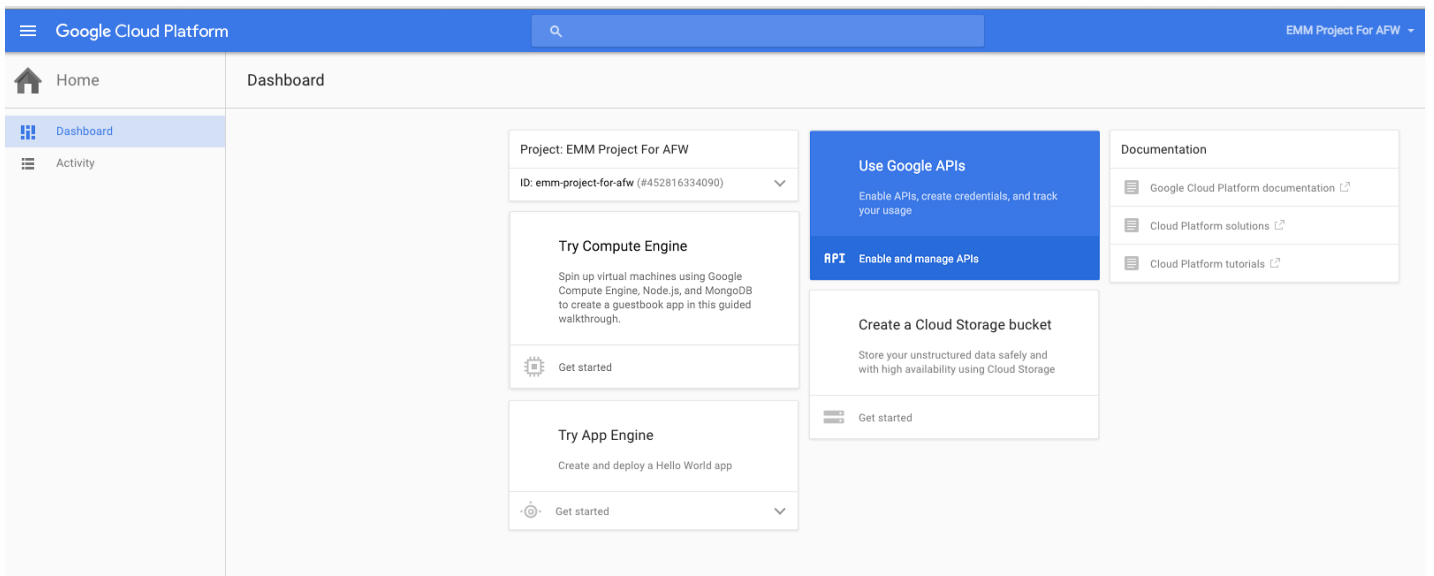
1. 在 Web 浏览器中，转至 <https://console.cloud.google.com/project> 并使用您的 Google 管理员凭据登录。
2. 在 **Projects** (项目) 列表中，单击 **Create Project** (创建项目)。



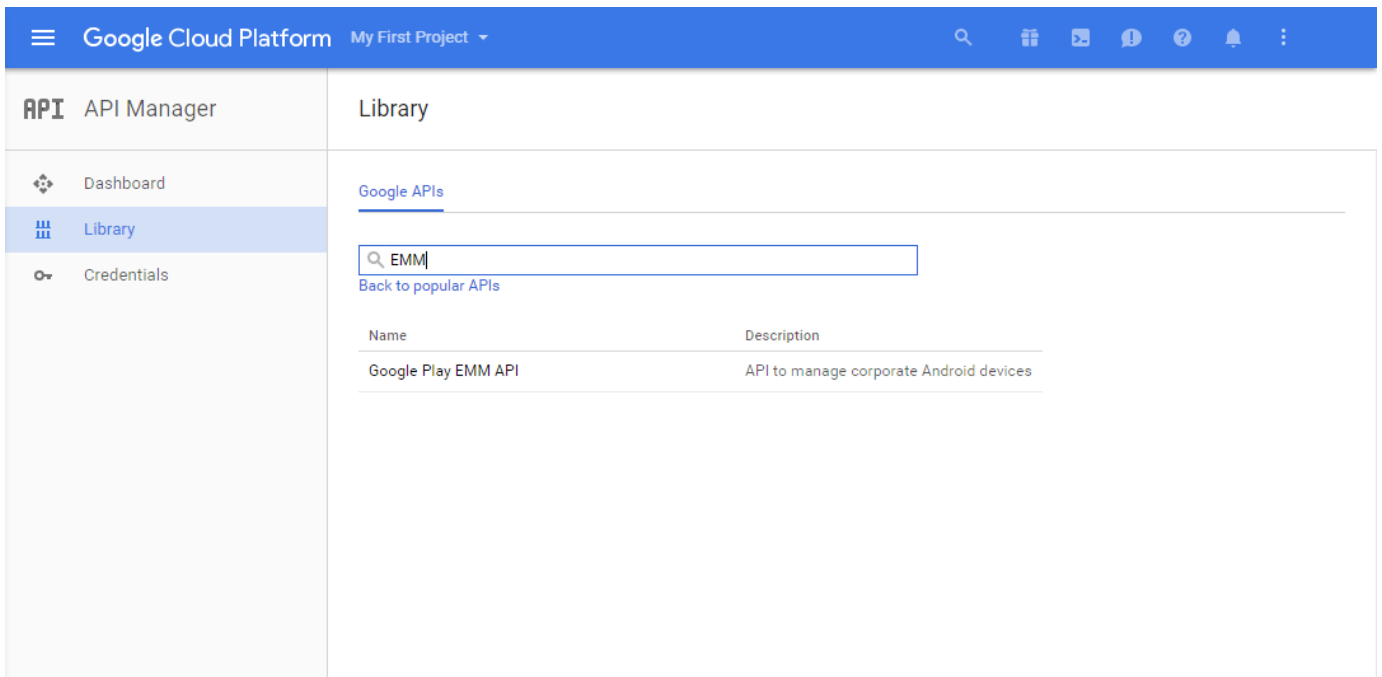
3. 在 **Project name** (项目名称) 中，键入项目的名称。



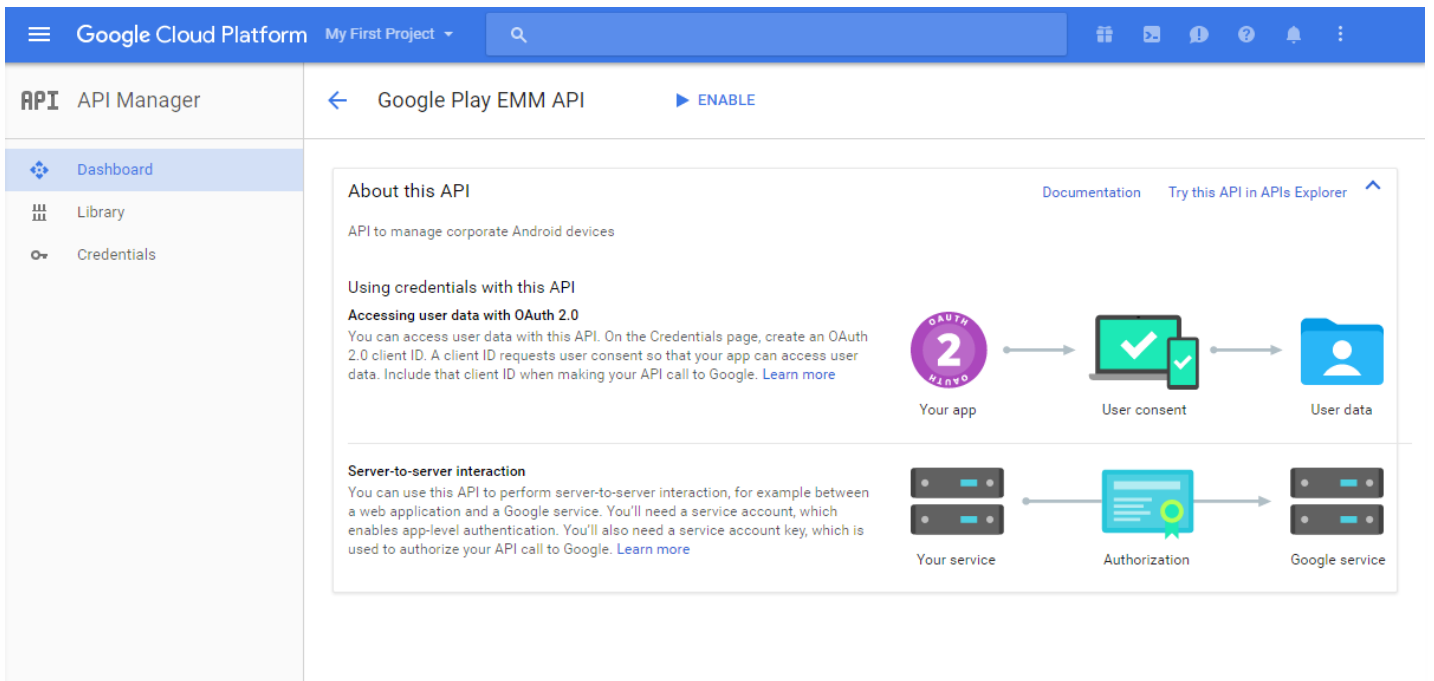
4. 在“Dashboard”（控制板）上，单击 **Use Google APIs**（使用 Google API）。



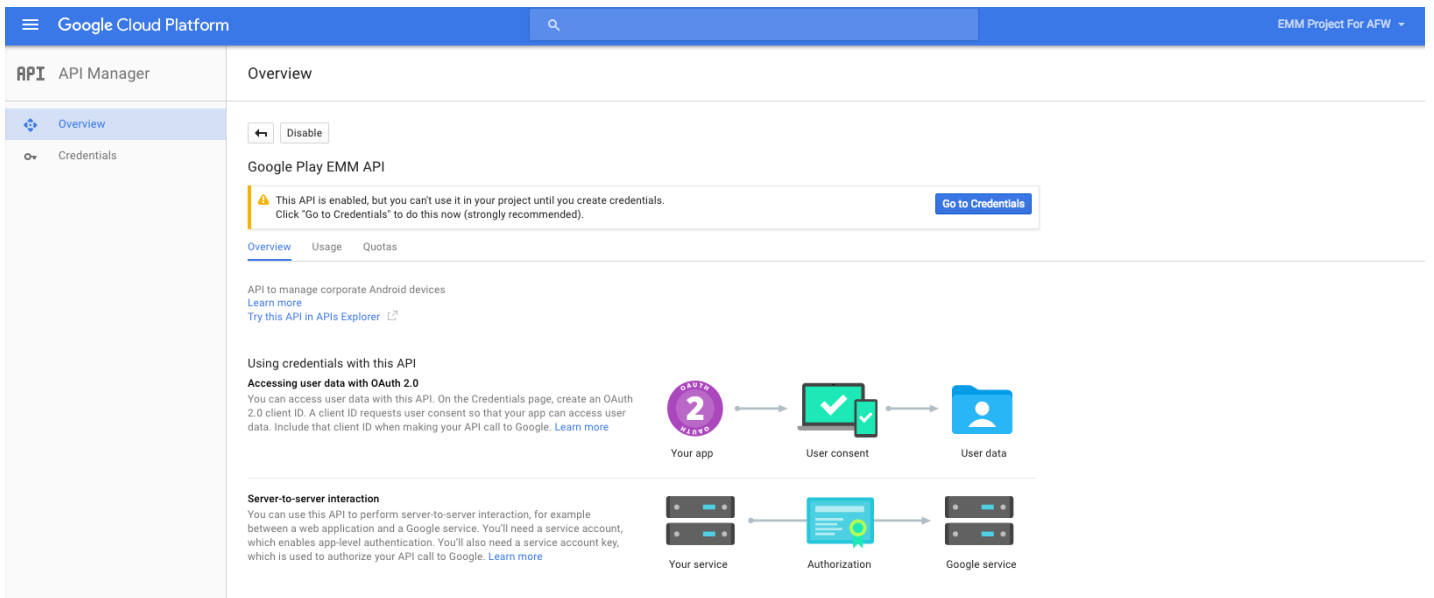
5. 单击 **Library**（库），在 **Search**（搜索）中，键入 **EMM**，然后单击搜索结果。



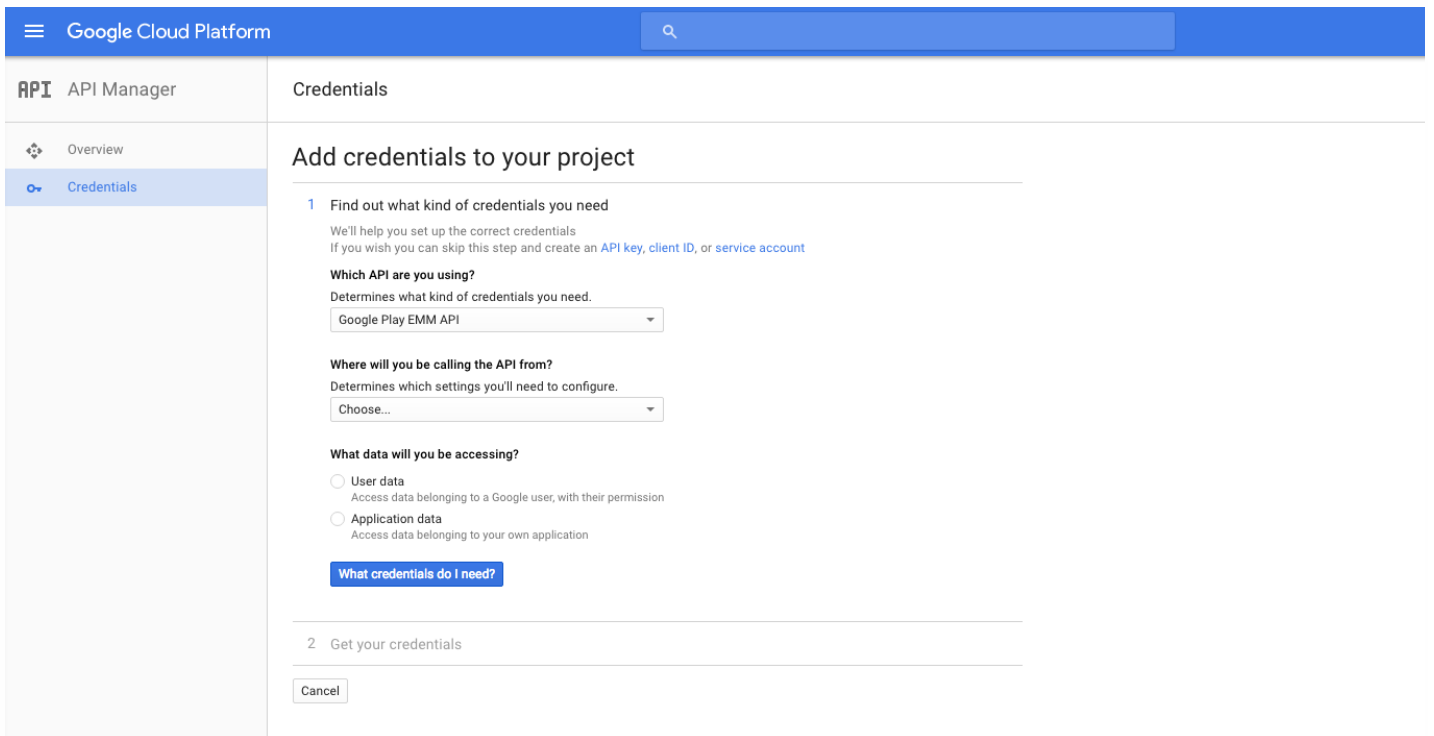
6. 在 **Overview** (概览) 页面上, 单击 **Enable** (启用)。



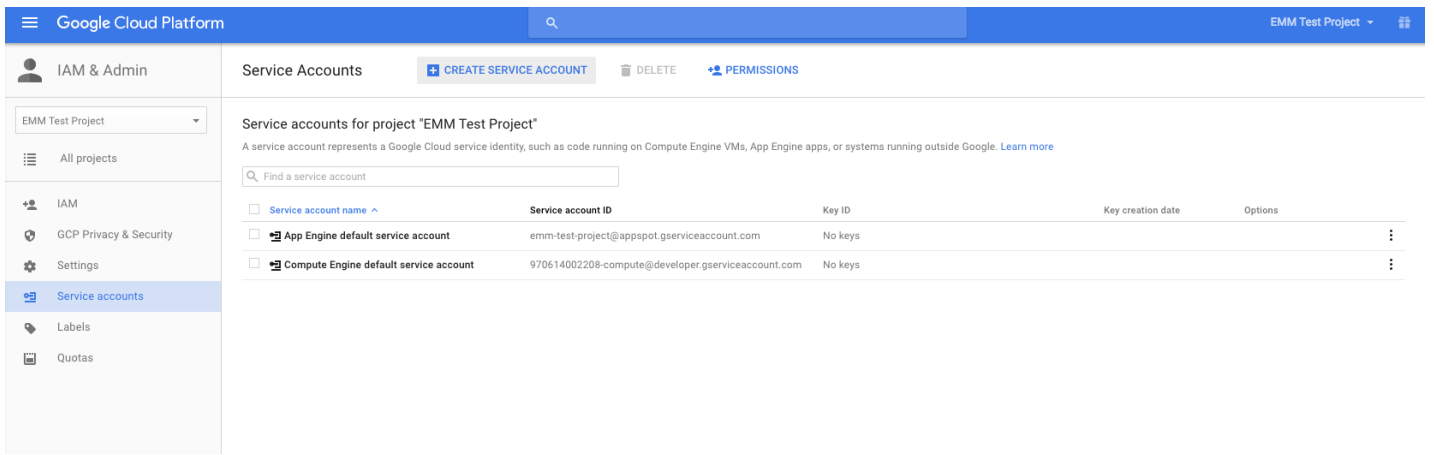
7. 在 **Google Play EMM API** 旁边, 单击 **Go to Credentials** (转至凭据)。



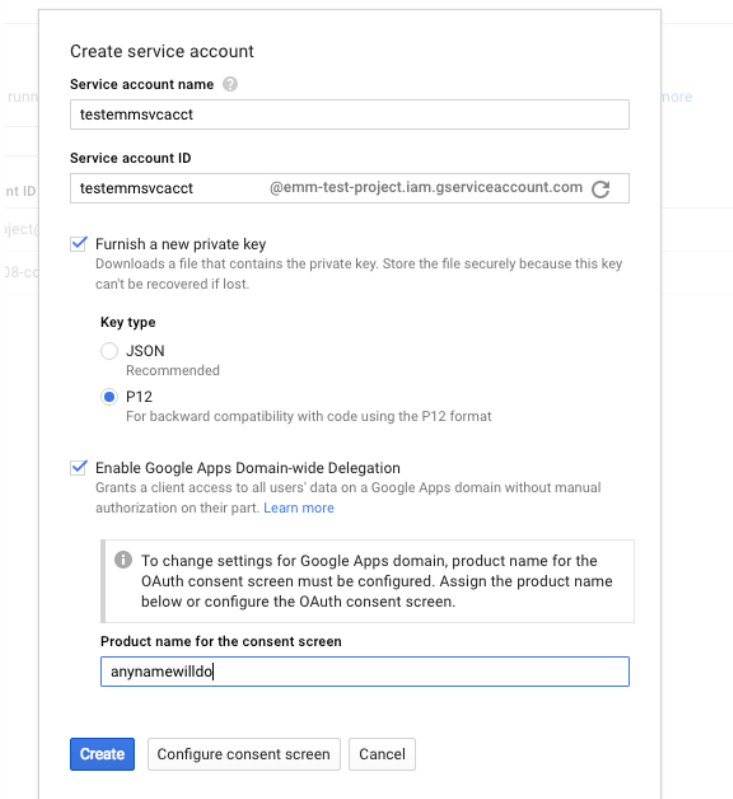
8. 在 **Add credentials to our project** (向我们的项目中添加凭据) 列表中，在步骤 1 中单击 **service account** (服务帐户)。



9. 在 **Service Accounts** (服务帐户) 页面上，单击 **Create Service Account** (创建服务帐户)。

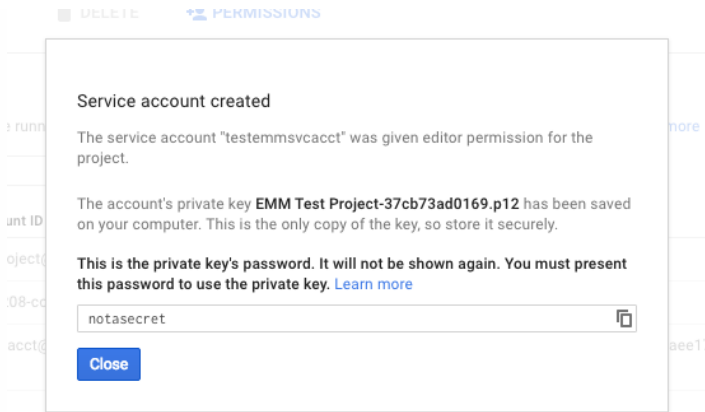


10. 在 **Create service account** (创建服务帐户) 中, 命名该帐户, 然后选中 **Furnish a new private key** (提供新私钥) 复选框。单击 **P12**, 选中 **Enable Google Apps Domain-wide Delegation** (启用 Google App 域范围的委派) 复选框, 然后单击 **Create** (创建)。

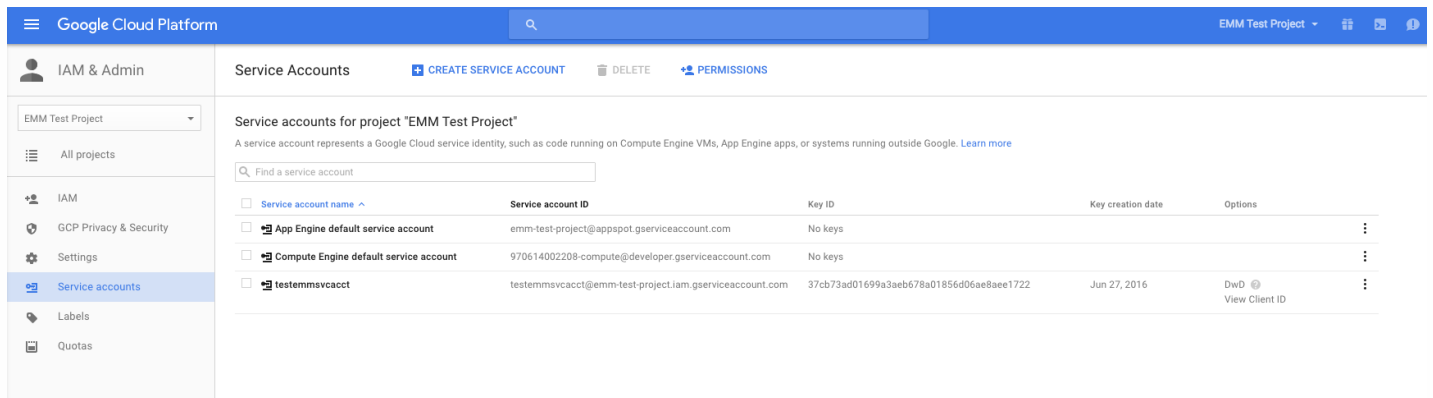


证书 (P12 文件) 将下载到您的计算机。请务必将该证书保存到一个安全的位置。

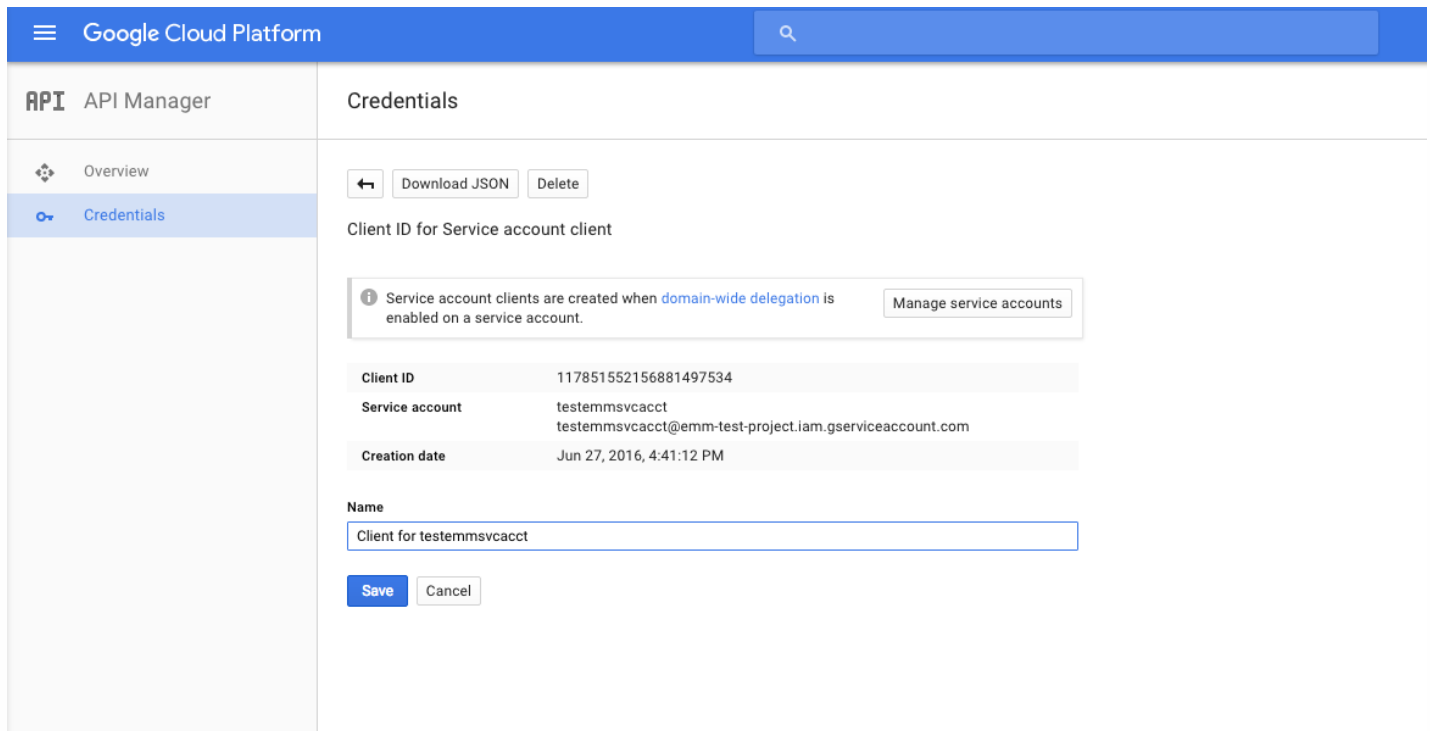
11. 在 **Service account created** (已创建服务帐户) 确认屏幕上, 单击 **Close** (关闭)。



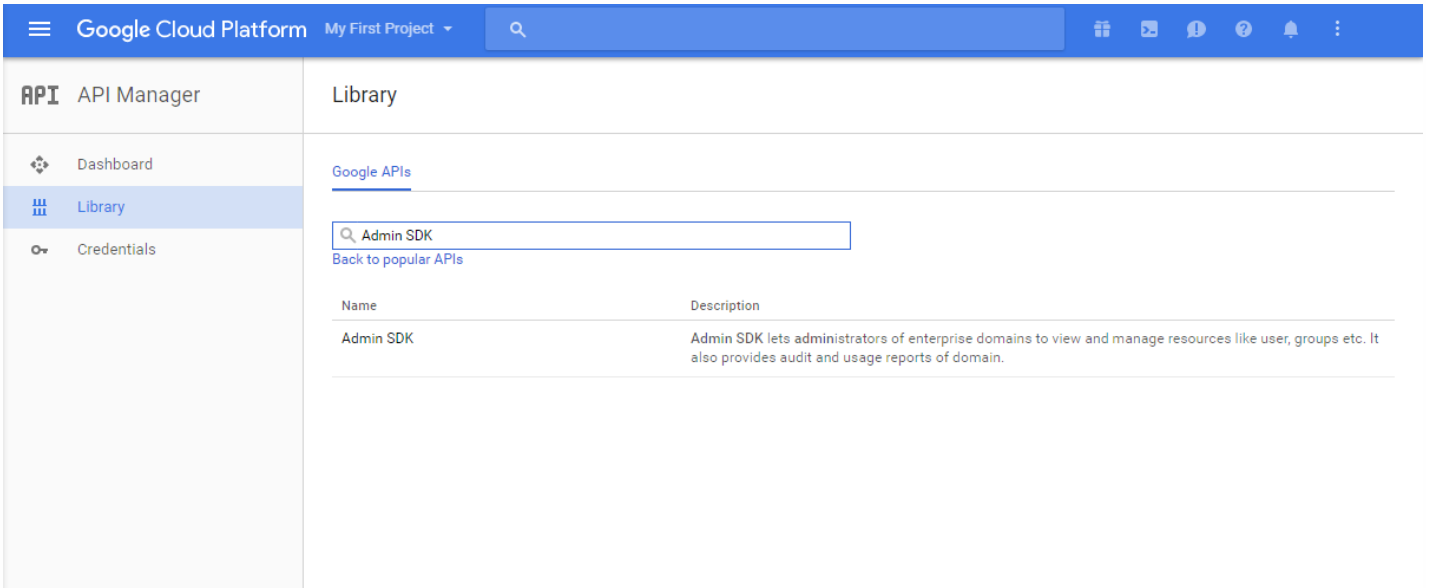
12. 在 **Permissions** (权限) 中, 单击 **Service accounts** (服务帐户), 然后在您的服务帐户对应的 **Options** (选项) 下, 单击 **View Client ID** (查看客户端 ID) 。



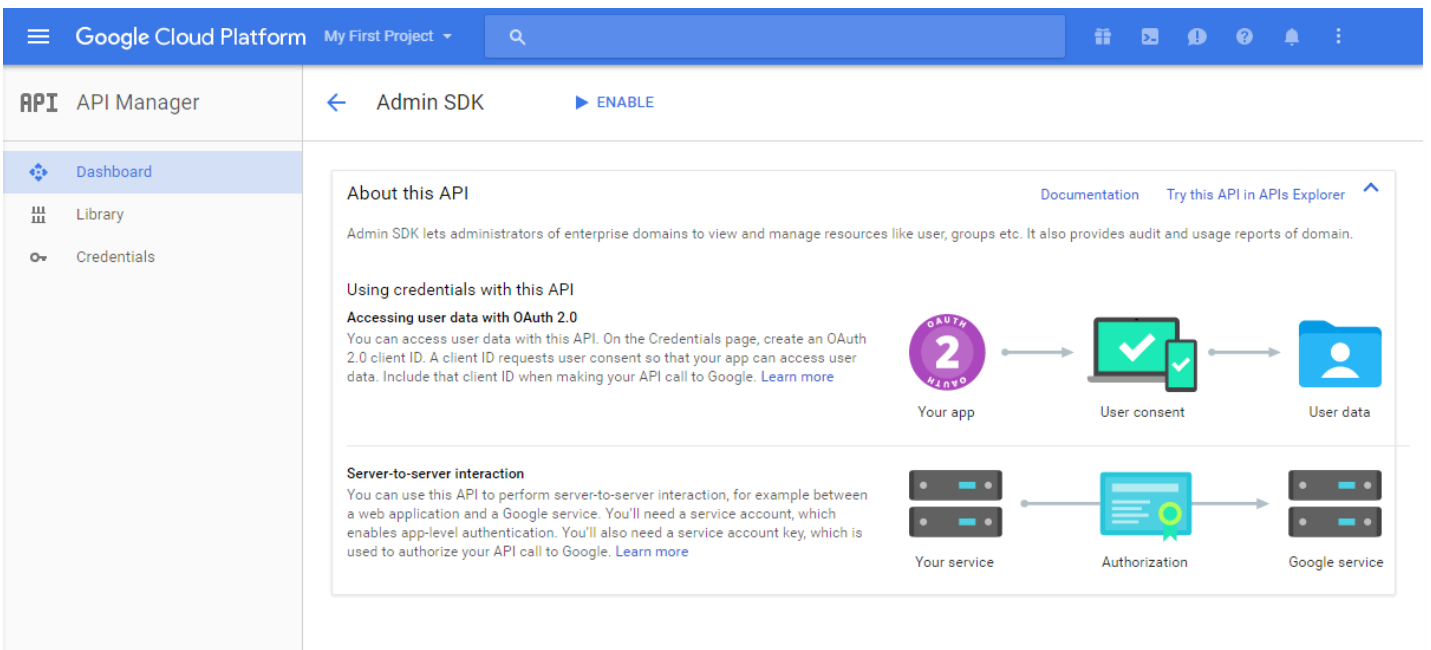
13. 此时将显示 Google 管理控制台上的帐户授权所需的详细信息。将 **Client ID** (客户端 ID) 和 **Service account ID** (服务帐户 ID) 复制到以后能够从中检索信息的位置。需要提供此信息以及域名, 才能发送给 Citrix 技术支持用于添加到白名单。



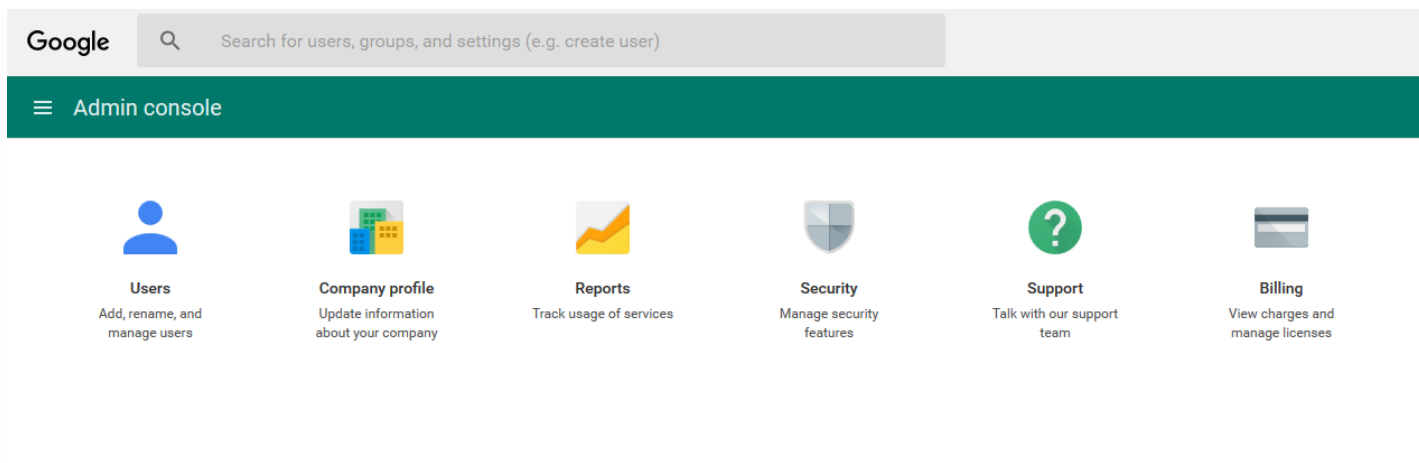
14. 在 **Library** (库) 页面上, 搜索 **Admin SDK** (管理 SDK) , 然后单击搜索结果。



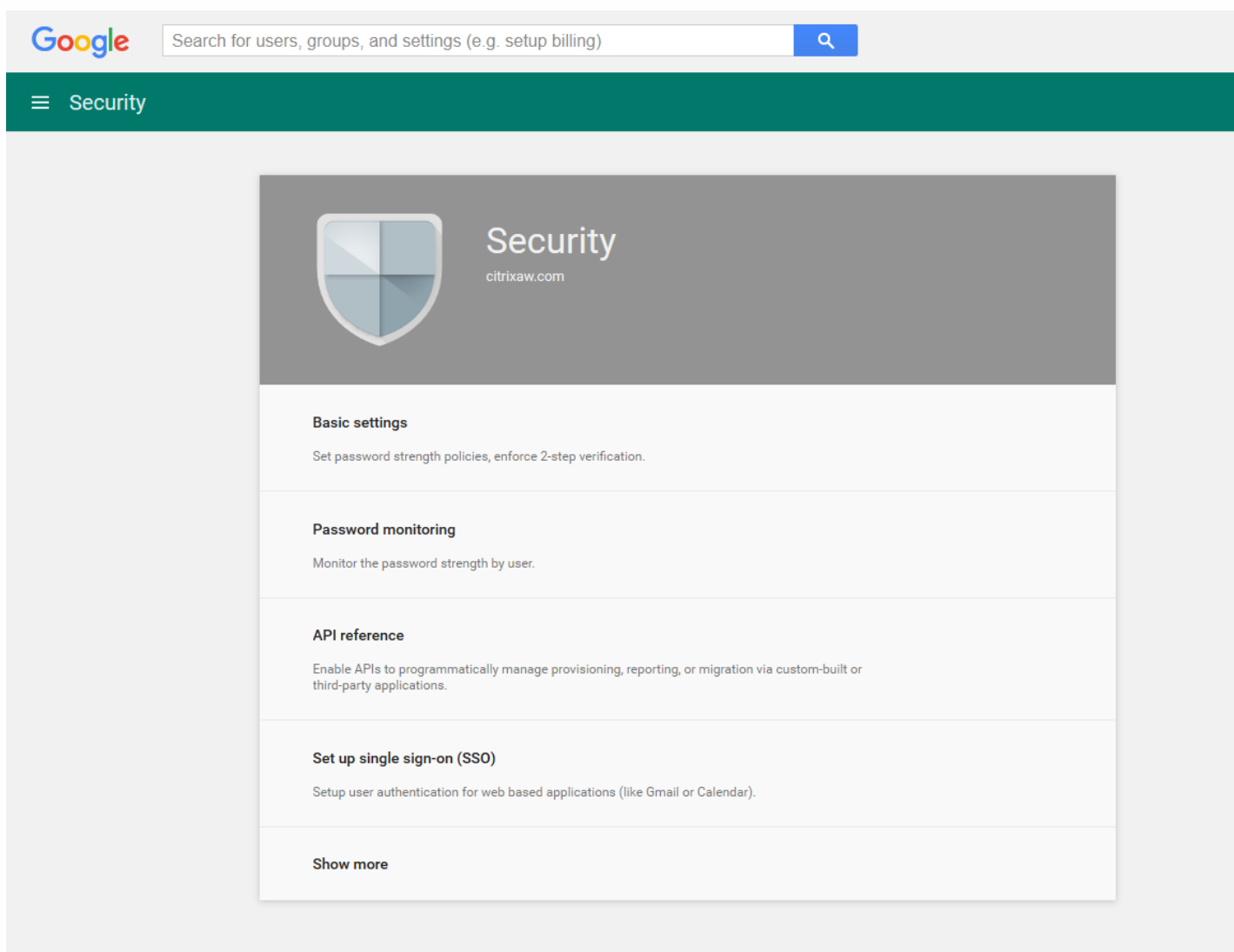
15. 在 **Overview** (概览) 页面上, 单击 **Enable** (启用) 。



16. 打开您的域对应的 Google 管理控制台, 然后单击 **Security** (安全) 。



17. 在 **Settings** (设置) 页面上, 单击 **Show more** (显示更多), 然后单击 **Advanced settings** (高级设置)。





Security

citrixaw.com

Basic settings

Set password strength policies, enforce 2-step verification.

Password monitoring

Monitor the password strength by user.

API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

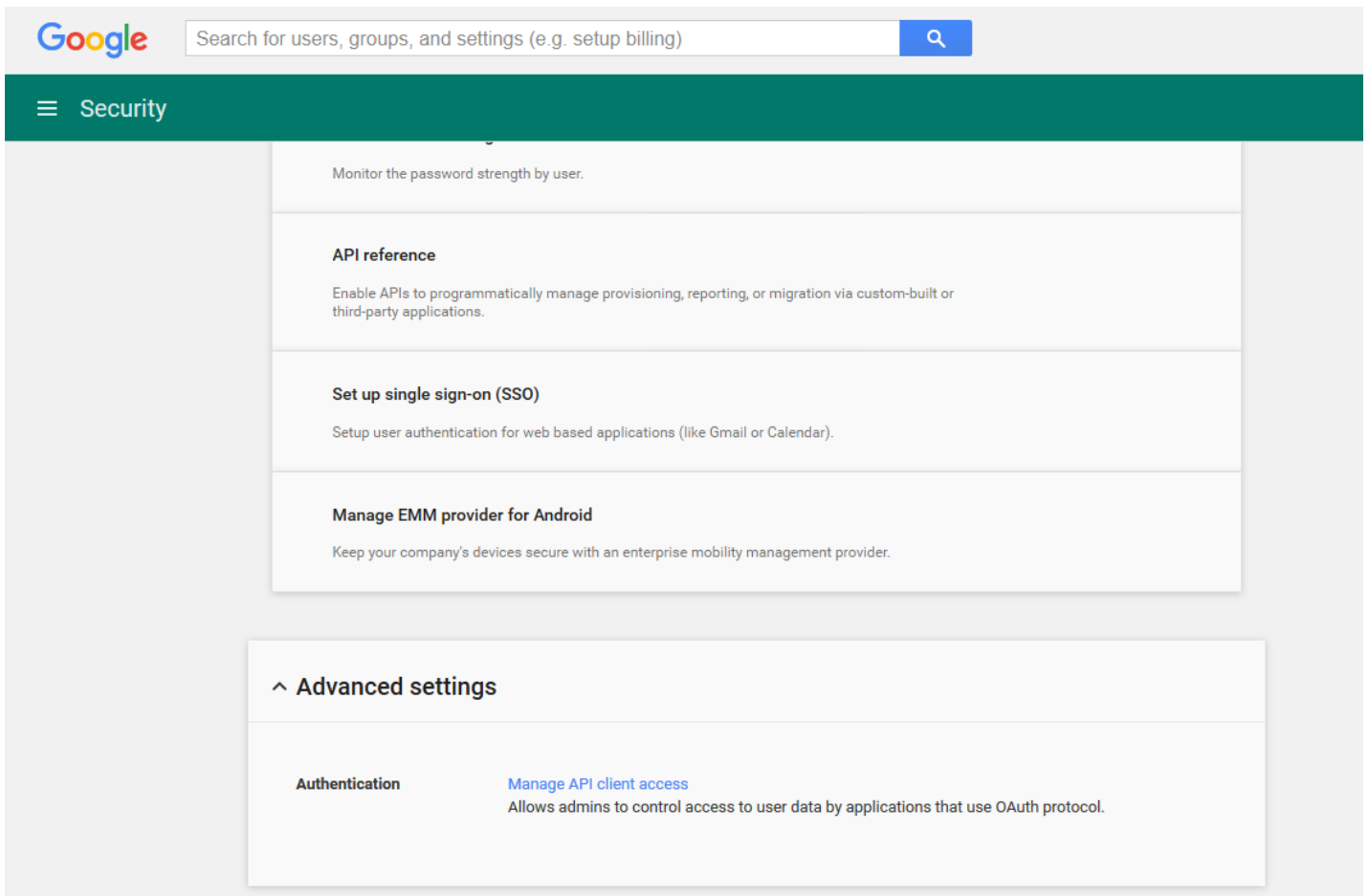
Manage EMM provider for Android

Keep your company's devices secure with an enterprise mobility management provider.

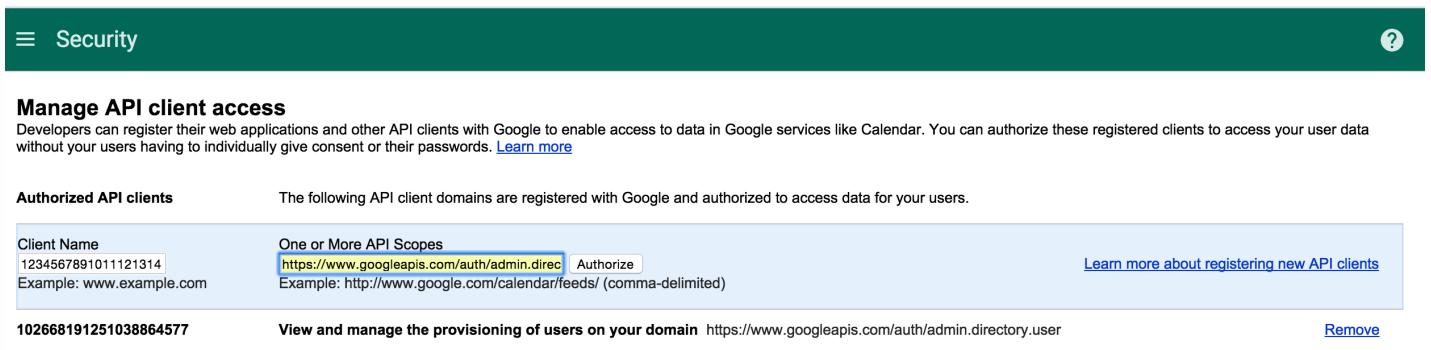
Advanced settings

Manage advanced security features such as authentication, and integrating G Suite with internal services.

18. 单击 **Manage API client access** (管理 API 客户端访问)。



19. 在 **Client Name** (客户端名称) 中, 输入您之前保存的客户端 ID, 在 **One or More API Scopes** (一个或多个 API 作用域) 中, 键入 <https://www.googleapis.com/auth/admin.directory.user>, 然后单击 **Authorize** (授权) 。



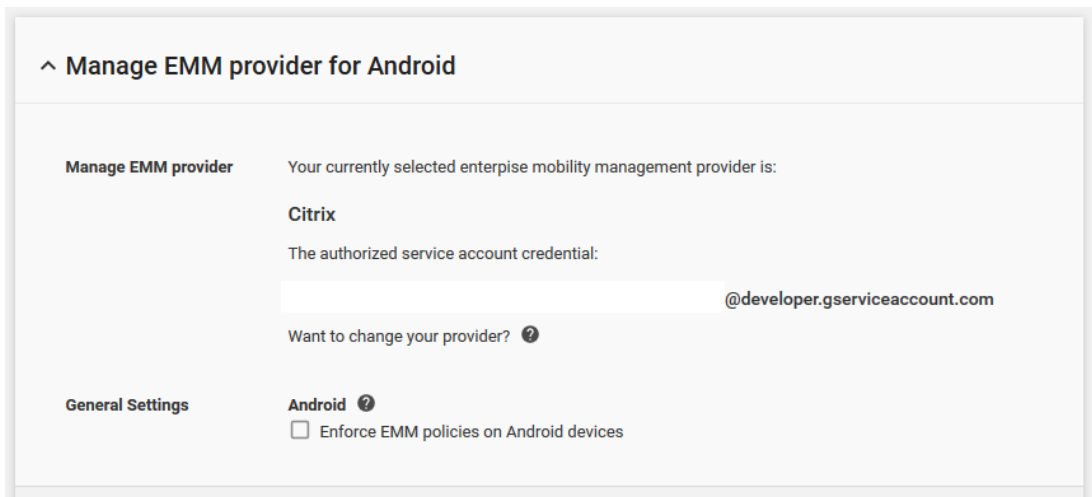
绑定到 EMM

必须先联系 Citrix 技术支持并提供您的域名、服务帐户和绑定令牌, 才能使用 XenMobile 管理您的 Android 设备。Citrix 会将该令牌绑定到 XenMobile 作为企业移动性管理 (EMM) 提供程序。有关 Citrix 技术支持的联系信息, 请参阅 [Citrix 技术支持](#)。

1. 要确认绑定, 请登录 Google 管理门户, 然后单击 **Security** (安全) 。
2. 单击 **Manage EMM provider for Android** (管理适用于 Android 的 EMM 提供程序) 。

您将看到自己的 Google Android for Work 帐户绑定到 Citrix, 用作 EMM 提供程序。

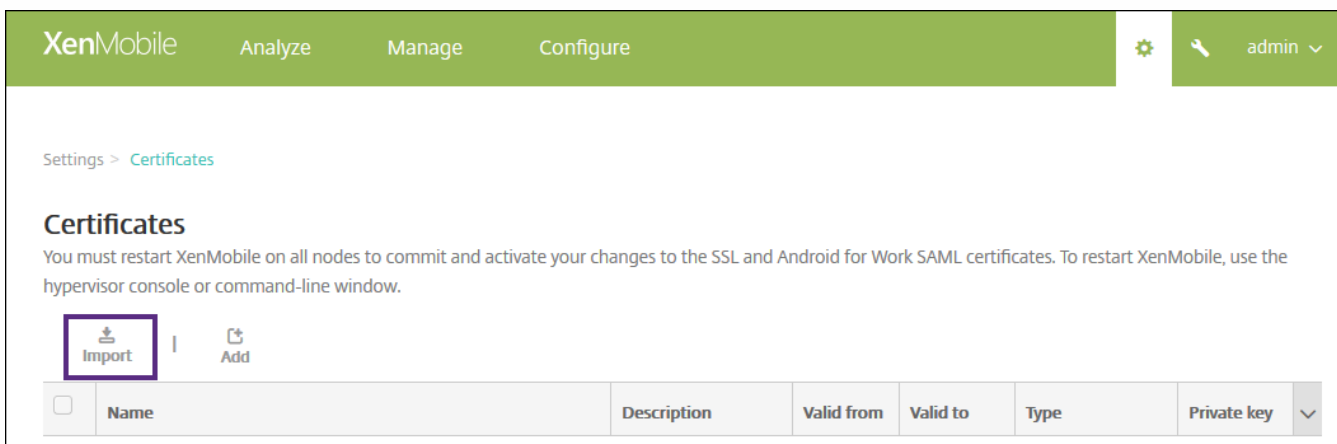
确认令牌绑定后, 可以开始使用 XenMobile 控制台管理您的 Android 设备。导入在步骤 14 中生成的 P12 证书。设置 Android at Work 服务器设置, 启用基于 SAML 的单点登录 (SSO), 并至少定义一条 Android for Work 设备策略。



导入 P12 证书

请按照以下步骤导入 Android at Work P12 证书：

1. 登录到 XenMobile 控制台。
2. 单击控制台右上角的齿轮图标以打开设置页面，然后单击证书。此时将显示证书页面。



3. 单击导入。此时将显示导入对话框。

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import: Keystore

Keystore type: PKCS#12

Use as: Server

Keystore file*: A 4d... Browse

Cancel Import

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 at Work 服务器设置

1. 在 XenMobile 控制台中，单击控制台右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下，单击 **Android for Work**。此时将显示 **Android for Work** 页面。

XenMobile Analyze Manage Configure admin

Settings > Android for Work

Android for Work
Provide Android for Work configuration parameters.

Domain Name*

Domain Admin Account*

Service Account ID*

Enable Android for Work NO

Cancel Save

配置以下设置：

- 域名：键入 Android at Work 的域名，例如 domain.com。
- 域管理员帐户：键入域管理员的用户名，例如，用于 Google 开发人员门户的电子邮件帐户。
- 服务帐户 ID：键入服务帐户 ID，例如，Google 服务帐户中关联的电子邮件 (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com)。
- 启用 **Android for Work**：单击可启用或禁用 Android at Work。

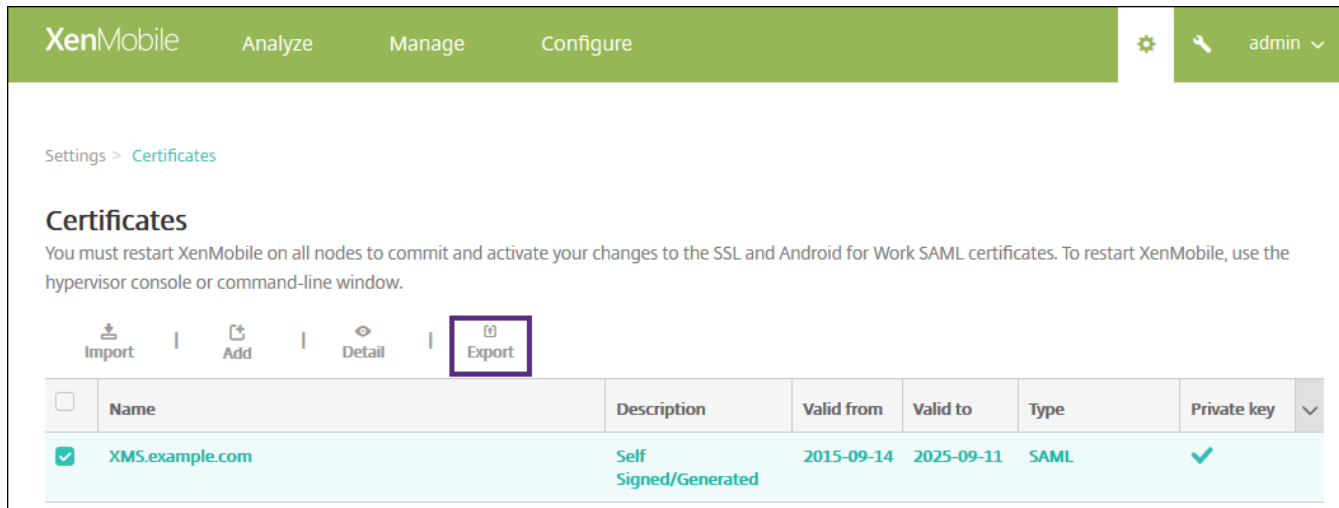
3. 单击保存。

启用基于 SAML 的单点登录

1. 登录到 XenMobile 控制台。

2. 单击控制台右上角的齿轮图标。此时将显示设置页面。

3. 单击证书。此时将显示证书页面。

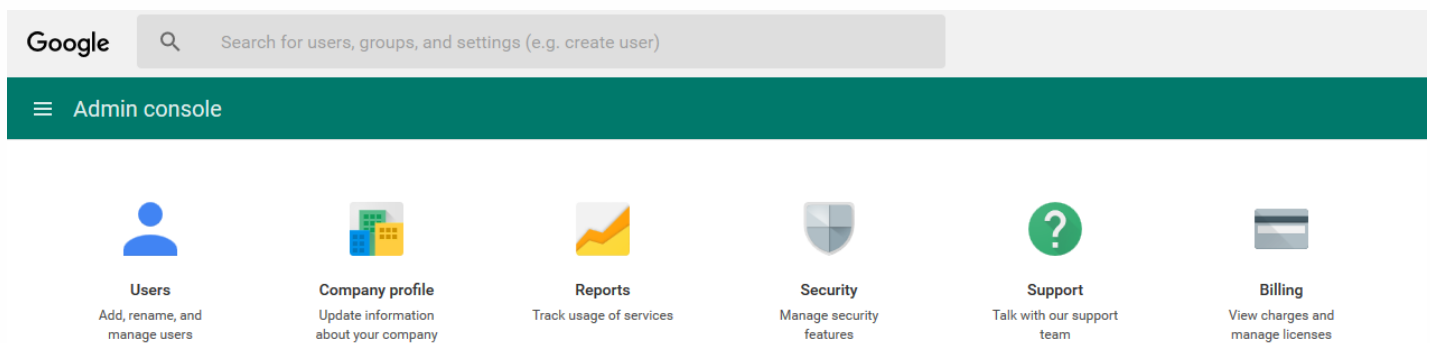


3. 在证书列表中，单击 SAML 证书。

4. 单击导出并将证书保存到您的计算机。

5. 使用您的 Android at Work 管理员凭据登录到 Google 管理门户。有关门户的访问权限，请参阅 [Google 管理门户](#)。

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。

^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL
URL for signing in to your system and Google Apps

Sign-out page URL
URL for redirecting users to when they sign out

Change password URL
URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate

The certificate file must contain the public key for Google to verify sign-in requests. ?

Use a domain specific issuer ?

Network masks

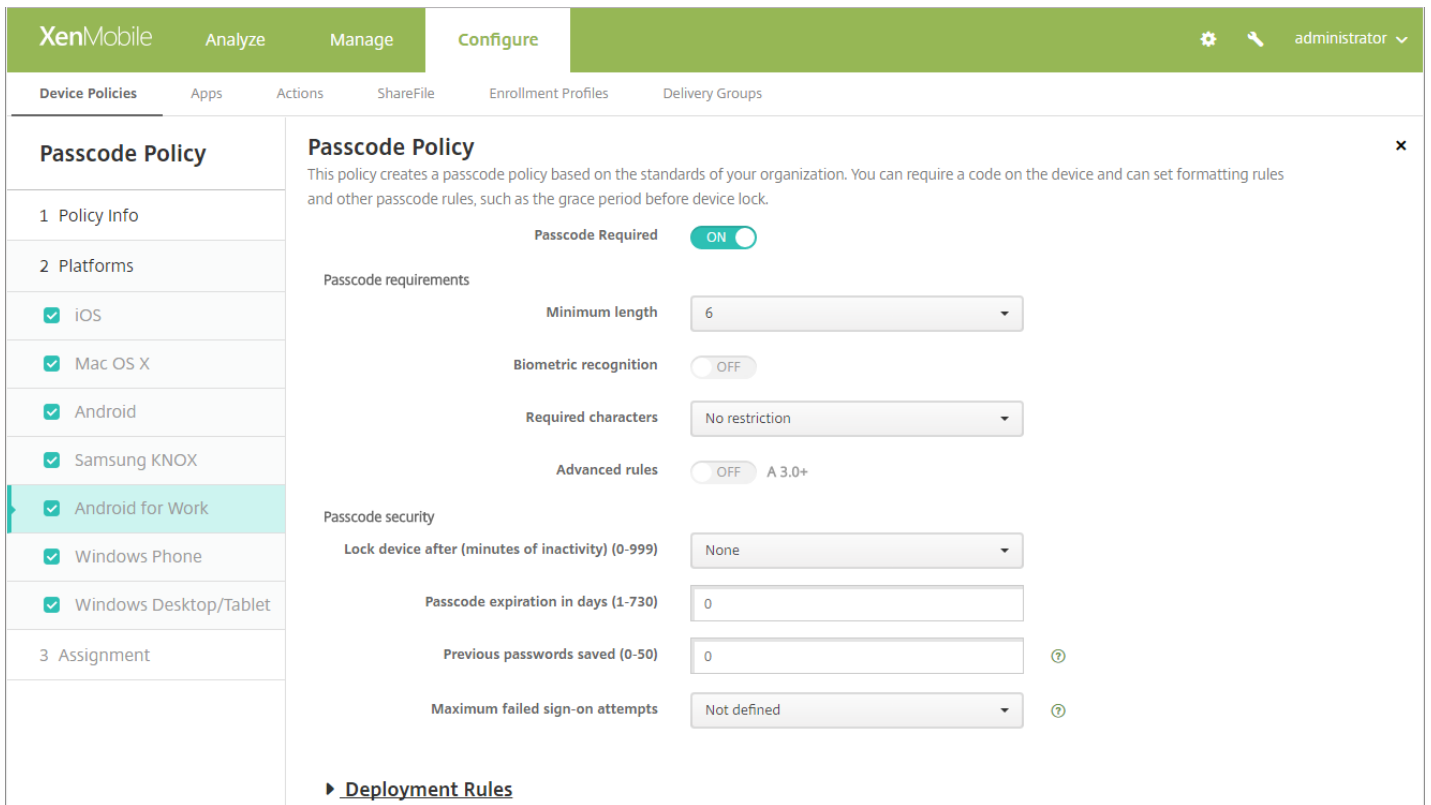
Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

- **登录页面 URL**：键入用户登录您的系统和 Google 应用程序使用的 URL。例如：https://aw/saml/signin。
- **注销页面 URL**：键入注销时用户被定向到的 URL。例如：https://aw/saml/signout。
- **Change password URL**（更改密码 URL）：键入 URL 以允许用户更改其系统中的密码。例如：https://aw/saml/changepassword。如果定义了此字段，用户将看到此提示，即使 SSO 不可用时也是如此。
- **Verification certificate**（验证证书）：单击 **CHOOSE FILE**（选择文件）并导航到从 XenMobile 导出的 SAML 证书。

8. 单击 **SAVE CHANGES**（保存更改）。

设置 Android at Work 设备策略

最好设置通行码策略，以便用户在首次注册时必须在其设备上创建通行码。



设置任何设备策略的基本步骤如下。

1. 登录到 XenMobile 控制台。
2. 单击**配置**，然后单击**设备策略**。
3. 单击**添加**，然后在**添加新策略**对话框中选择要添加的策略。在此示例中，请单击**通行码**。
4. 完成**策略信息**页面。
5. 单击 **Android for Work** 并配置策略设置。
6. 将策略分配到交付组。

有关设置适用于 Android for Work 的其他设备策略的详细信息，请参阅 [XenMobile 设备策略（按平台）](#)。

配置 Android at Work 帐户设置

您必须在 XenMobile 中设置 Android at Work 域和帐户信息，才能开始管理设备上的 Android 应用程序和策略。首先，请在 Google 上完成 Android at 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。

1. 在 XenMobile Web 控制台中，单击右上角的齿轮图标。此时将显示**设置**页面。
2. 在**服务器**下，单击 **Android for Work**。此时将显示 **Android for Work** 配置页面。

Settings > [Android for Work](#)

Android for Work

Provide Android for Work configuration parameters.

Domain Name*	<input type="text"/>
Domain Admin Account*	<input type="text"/>
Service Account ID*	<input type="text"/>
Enable Android for Work	<input checked="" type="checkbox"/>

3. 在 **Android for Work** 页面上，配置以下设置：

- **域名**：键入域名。
- **域管理员帐户**：键入域管理员用户名。
- **服务帐户 ID**：键入 Google 服务帐户 ID。
- **启用 Android for Work**：选择是否启用 Android for Work。

4. 单击**保存**。

在 Android at Work 中置备设备所有者模式

如果要在设备所有者模式下置备 Android at Work，必须在两个设备之间通过近场通信(NFC)碰撞传输数据。其中一个必须运行 XenMobile Provisioning Tool，并且必须将另一个还原到其出厂设置。设备所有者模式仅适用于企业拥有的设备。

为什么通过 **NFC**？蓝牙、Wi-Fi 和其他通信模式在恢复出厂设置的设备上处于禁用状态。NFC 是此状态下设备可以使用的唯一通信协议。

必备条件

- 为 Android at Work 启用的 XenMobile 服务器 10.4。
- 恢复出厂设置的设备，在设备所有者模式下针对 Android at Work 置备。可以在本文中查找完成此必备条件的步骤。
- 另一台设备具有 NFC 功能，运行已配置的 Provisioning Tool。Provisioning Tool 在 Secure Hub 10.4 或 [Citrix 下载页面](#)上提供。

每个设备只能配备一个 Android at Work 配置文件，通过企业移动性管理 (EMM) 应用程序管理。在 XenMobile 中，Secure Hub 为 EMM 应用程序。仅允许在每个设备上配备一个配置文件。尝试添加第二个 EMM 应用程序将删除第一个 EMM 应用程序。

可以在新设备上或还原为出厂设置的设备上启动设备所有者模式。您将通过 XenMobile 管理整个设备。

设备所有者模式下的 NFC 碰撞

置备恢复出厂设置的设备需要您通过 NFC 碰撞发送以下数据以启动 Android at Work：

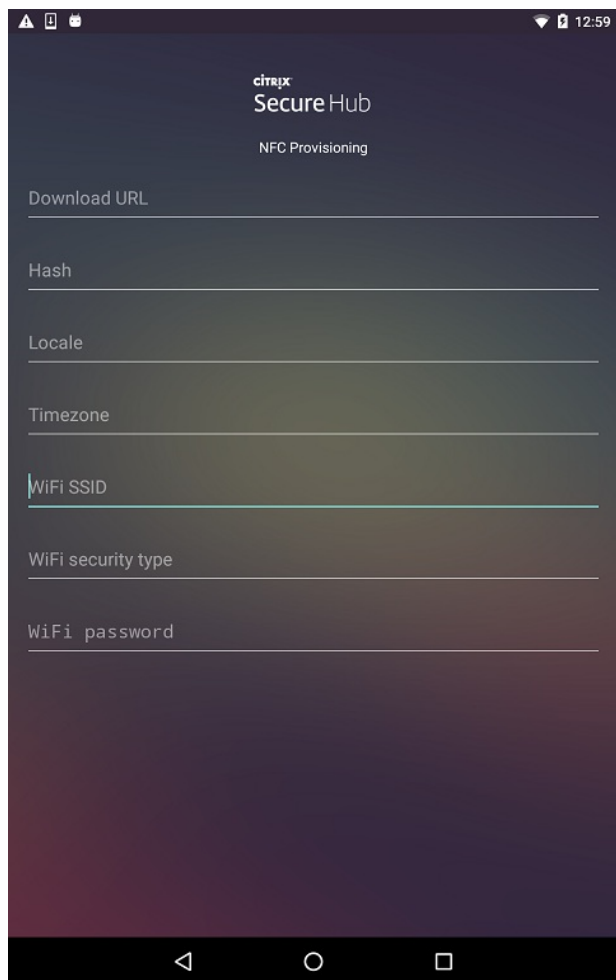
- 要作为设备所有者（在此示例中为 Secure Hub）的 EMM 提供程序应用程序的包名称。
- 可以从中下载 EMM 提供程序应用程序的 Intranet/Internet 位置。
- 用于验证下载是否成功的 EMM 提供程序应用程序的 SHA1 哈希。
- Wi-Fi 连接详细信息，以便恢复出厂设置的设备能够连接和下载 EMM 提供程序应用程序。注意：Android 现在不支持在此步骤中使用 802.1x Wi-Fi。
- 设备的时区（可选）。
- 设备的地理位置（可选）。

碰撞两台设备时，来自 Provisioning Tool 的数据将发送到恢复出厂设置的设备。该数据随后用于下载使用管理员设置的 Secure Hub。如果未输入时区和位置

值，Android 将在新设备上自动配置值。

配置 XenMobile Provisioning Tool

执行 NFC 碰撞之前，必须配置 Provisioning Tool。此配置随后在 NFC 碰撞过程中被传输到恢复出厂设置的设备。



可以将数据键入到必填字段中，或者通过文本文件进行填充。下一个过程中的步骤介绍了如何配置文本文件，并且包含每个字段的说明。键入后，该应用程序将不保存信息，因此，您可能希望创建一个文本文件以保留该信息供将来使用。

使用文本文件配置 Provisioning Tool

将文件命名为 `nfcprovisioning.txt` 并将其放置在设备的 SD 卡中的 `/sdcard/` 文件夹下。该应用程序随后可以读取文本文件并填充值。

文本文件必须包含以下数据：

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=

此行为 EMM 提供程序应用程序的 intranet/internet 位置。恢复出厂设置的设备在进行 NFC 碰撞后连接到 Wi-Fi 之后，该设备必须有权访问此位置才能进行下载。该 URL 为常规 URL，不需要特殊格式。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=

此行是 EMM 提供程序的校验和。此校验和用于验证下载是否成功。本文中后面的内容介绍了获取校验和的步骤。

android.app.extra.PROVISIONING_WIFI_SSID=

此行是运行 Provisioning Tool 的设备的已连接的 Wi-Fi SSID。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=

支持的值为 WEP 和 WPA2。如果 Wi-Fi 未受保护，此字段必须留空。

android.app.extra.PROVISIONING_WIFI_PASSWORD=

如果 Wi-Fi 未受保护，此字段必须留空。

android.app.extra.PROVISIONING_LOCALE=

输入语言和国家/地区代码。语言代码为包含两个小写字母的 ISO 语言代码（例如 en），如 ISO 639-1 所定义。国家/地区代码为包含两个大写字母的 ISO 国家/地区代码（例如 US），如 ISO 3166-1 所定义。例如，请键入 en_US 表示在美国所讲的英语。如果未输入任何代码，则会自动填充国家/地区和语言。

android.app.extra.PROVISIONING_TIME_ZONE=

设备运行时所在的时区。请键入 [表单区域/位置的 Olson 名称](#)。例如，America/Los_Angeles 表示太平洋时间。如果未输入名称，则将自动填充时区。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=

此数据不是必需的，因为该值已硬编码到应用程序中作为 Secure Hub。在本文中提及的目的只是为了保持完整性。

如果存在使用 WPA2 保护的 Wi-Fi，完整的 `nfcprovisioning.txt` 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmf dj72LGRFkke4CrbAK\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
android.app.extra.PROVISIONING_LOCALE=en_US
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

如果存在不受保护的 Wi-Fi，完整的 `nfcprovisioning.txt` 文件可能如下所示：

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmf dj72LGRFkke4CrbAK\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

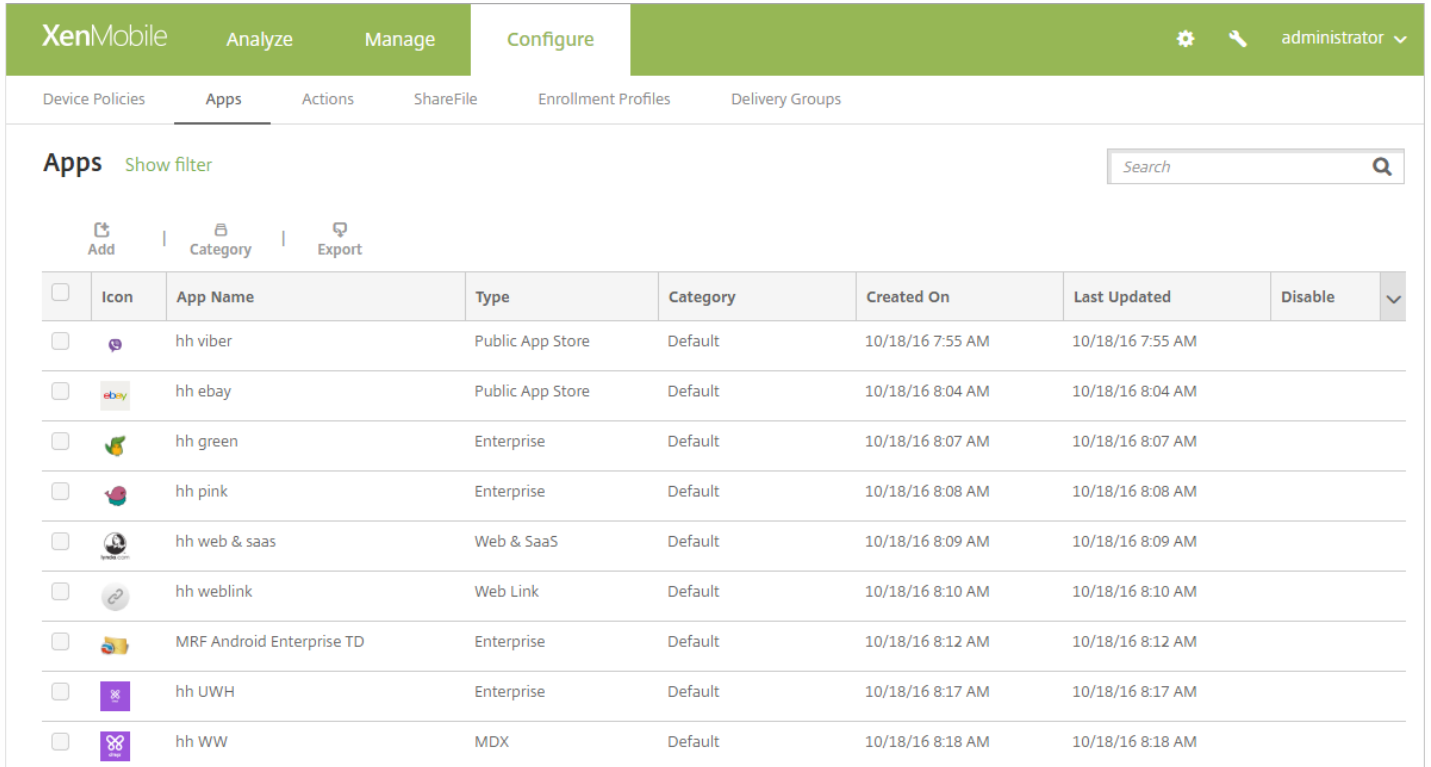

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

获取 Secure Hub 校验和

要获取任何应用程序的校验和，请添加该应用程序作为企业应用程序。

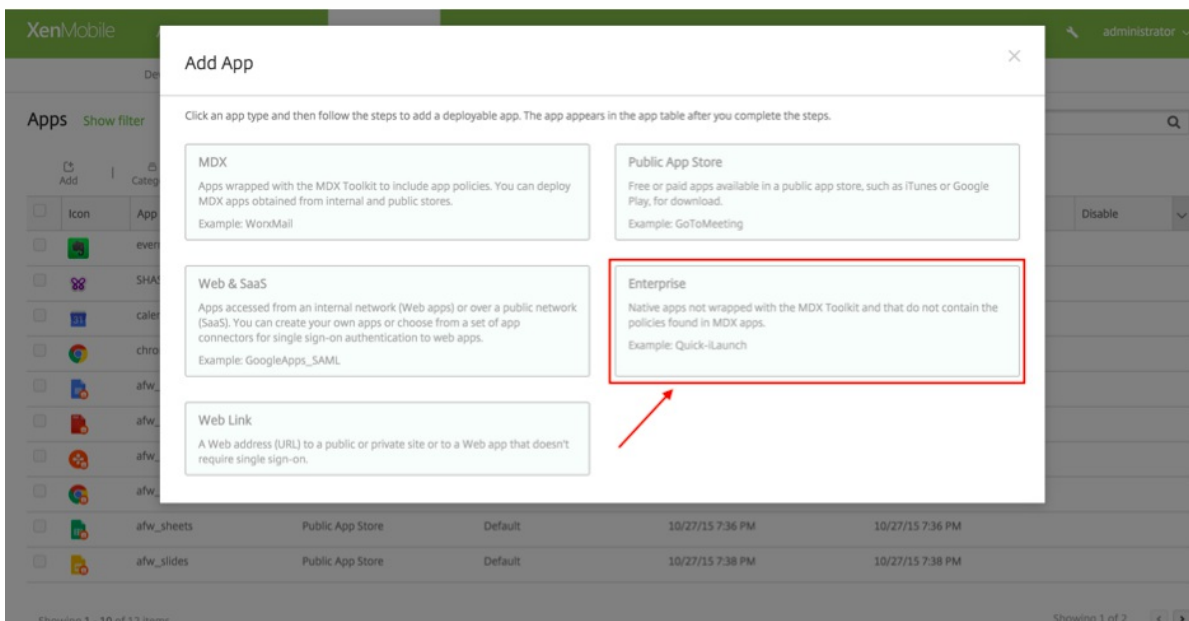
1. 在 XenMobile 控制台中，单击配置 > 应用程序，然后单击添加。



此时将显示添加应用程序窗口。

2. 单击企业。

此时将显示应用程序信息页面。



3. 选择以下配置并单击下一步。

此时将显示 **Android for Work** 企业应用程序页面。

XenMobile Analyze Manage Configure administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Enterprise

1 App Information

2 Platform

iOS

Android

Samsung KNOX

Android for Work

Windows Phone

Windows Tablet

Windows CE

3 Approvals (optional)

4 Delivery Group Assignments (optional)

App Information

Name* Secure Home

Description

App category All Selected

Next >

4. 提供 .apk 的路径，然后单击下一步以上载文件。

上传完成后，系统将显示上传的软件包的详细信息。

XenMobile Analyze Manage Configure administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Enterprise

1 App Information

2 Platform

iOS

Android

Samsung KNOX

Android for Work

Windows Phone

Windows Tablet

Windows CE

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Android for Work Enterprise App

Upload an apk file Upload

App name* Secure Home

Description* Secure Home

App version 10.4.0

Minimum OS version 14

Maximum OS version

Excluded devices example: manufacturer or model...

Deployment Rules

Worx Store Configuration

Back Next >

5. 单击下一步显示下载 JSON 文件的页面，随后可以在该页面上下载到 Google Play。对于 Secure Hub，不需要下载到 Google Play，但需要 JSON 文件才能从中读取 SHA1 值。

批量注册 iOS 和 macOS 设备

Feb 27, 2017

可以通过两种方式在 XenMobile 中注册大量 iOS 和 macOS 设备。

- 可以使用 Apple 的 Device Enrollment Program (DEP) 注册您直接从 Apple、Apple 授权经销商或运营商处购买的 iOS 和 macOS 设备。

针对 macOS 设备的 DEP 注册，XenMobile 要求设备运行 OS X 10.10 或更高版本。

- 也可以使用 Apple Configurator 注册 iOS 设备，无论这些设备是否直接从 Apple 购买，皆可注册。

使用 DEP 注册时，您不需要触摸或准备设备。只需通过 DEP 提交设备序列号或采购订单编号，即可配置并注册设备。XenMobile 注册设备后，可以将其提供给能够立即开箱使用这些设备的用户。此外，通过 DEP 设置设备时，可以不执行用户在首次启动设备时需要完成的某些设置助理步骤。有关设置 DEP 的详细信息，请参阅 Apple [Device Enrollment Program](#) 页面。

使用 Apple Configurator 注册时，需要将 iOS 设备连接到运行 OS X 10.7.2 或更高版本以及 Apple Configurator 2 应用程序的 Apple 计算机。请通过 Apple Configurator 2 准备 iOS 设备并配置策略。为设备置备所需的策略后，首次将设备连接到 XenMobile 时，这些设备将从 XenMobile 接收策略。您之后可以开始管理设备。有关使用 Apple Configurator 的详细信息，请参阅 [Apple Configurator](#) 帮助。

Important

必须打开所需的端口才能在 XenMobile 与 Apple 之间建立连接。有关详细信息，请参阅[端口要求](#)。

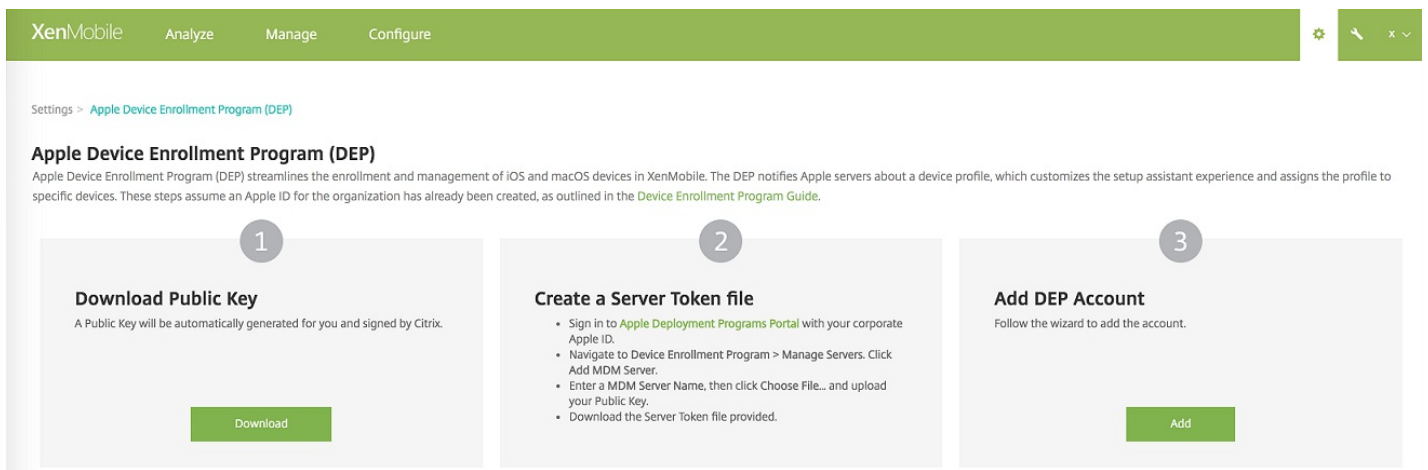
将 Apple DEP 帐户与 XenMobile 相集成

如果没有 Apple DEP 帐户，请参阅[通过 Apple DEP 部署 iOS 和 macOS 设备](#)。

要将您的 Apple DEP 帐户与 XenMobile 服务器部署相连接，请在 XenMobile 控制台和 Apple DEP 门户中输入信息，如以下步骤中所述。

步骤 1：从 XenMobile 服务器下载公钥。

1. 登录到 XenMobile 控制台，转至设置 > **Apple Device Enrollment Program (DEP)**。

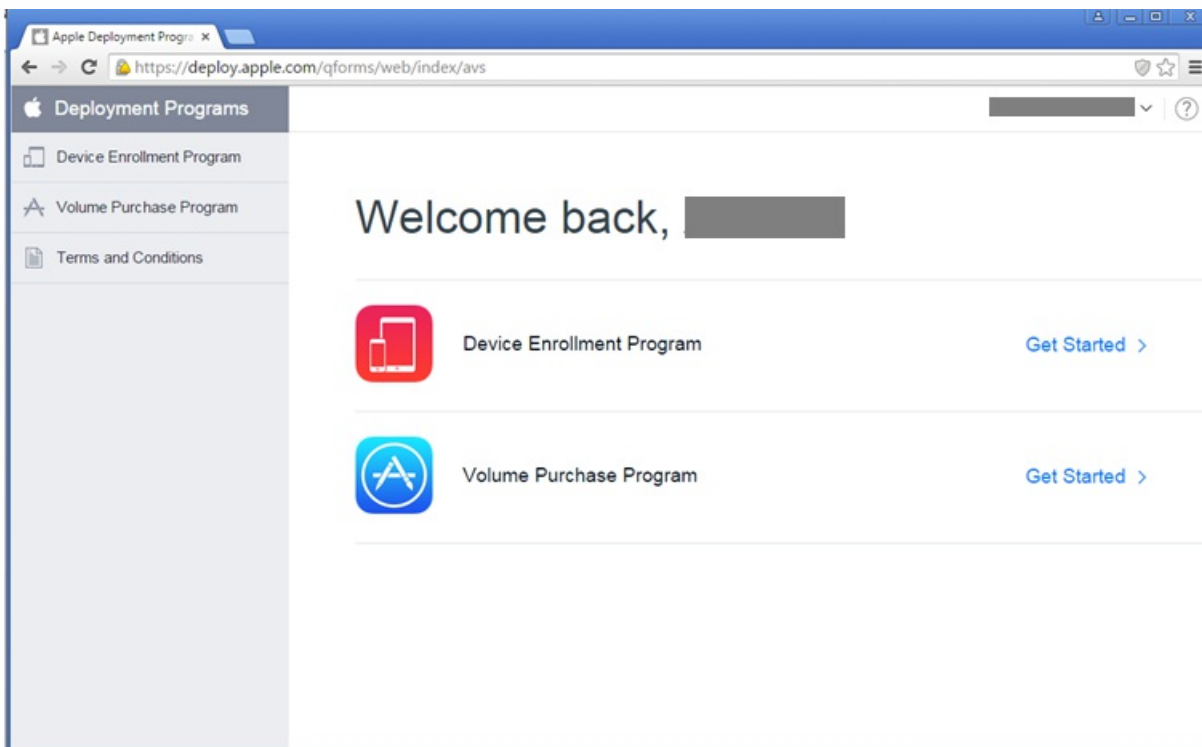


2. 在下载公钥下，单击下载。

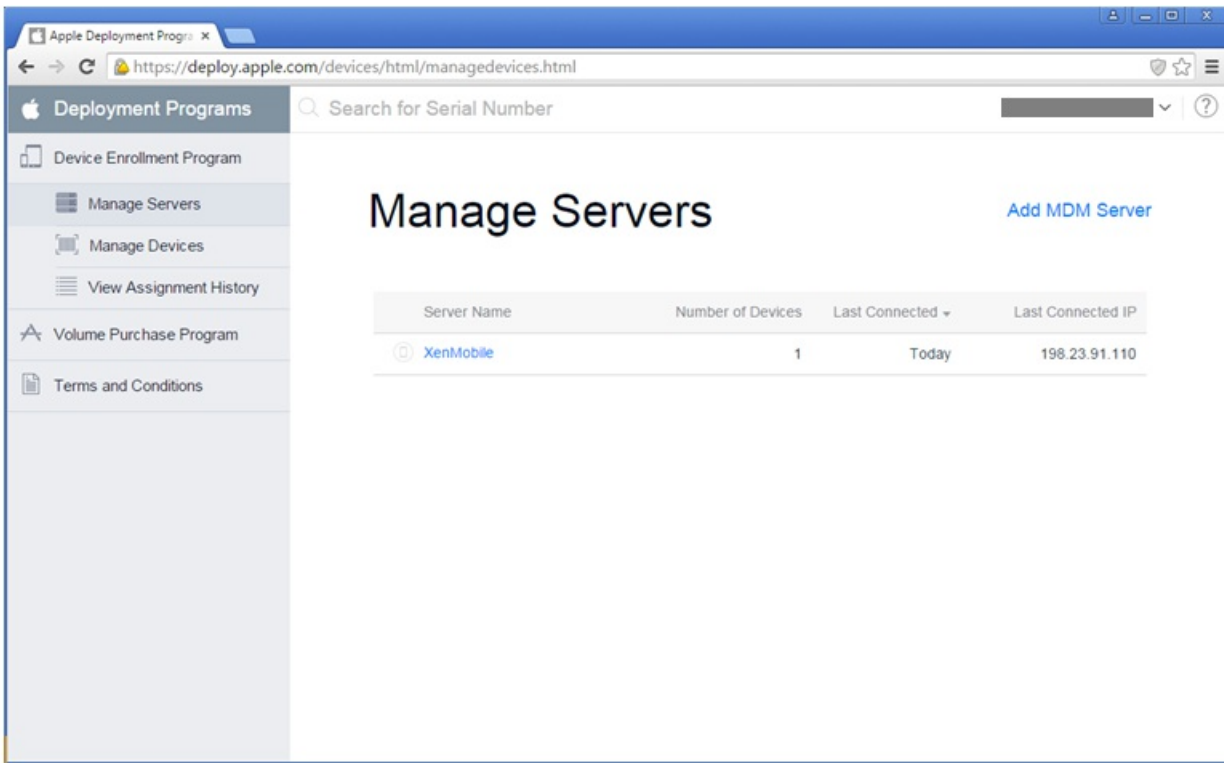
步骤 2：在您的 Apple 帐户中创建并下载服务器令牌文件

1. 使用您的公司 Apple ID 登录到 [Apple Deployment Program Portal](#)（Apple 部署计划门户）。

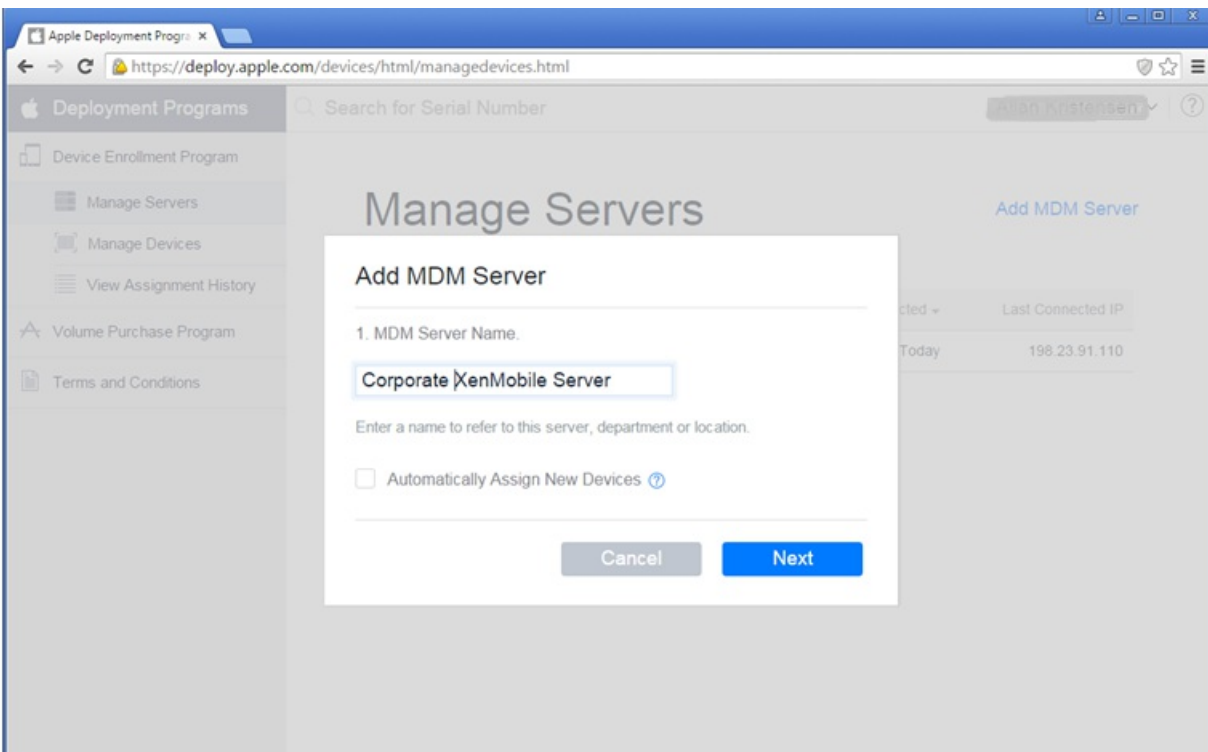
2. 在 Apple DEP 门户中，单击 **Device Enrollment Program**。



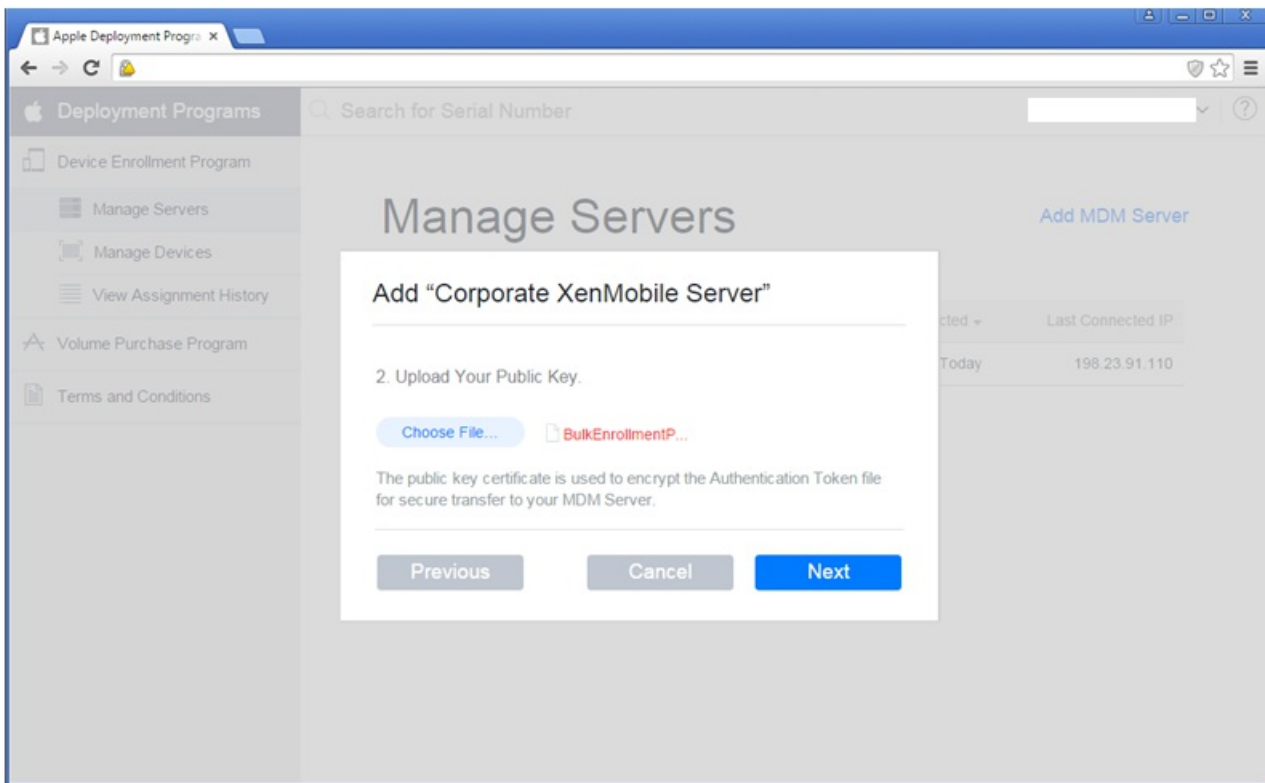
3. 单击 **Manage Servers**（管理服务器），然后单击右侧的 **Add MDM Server**（添加 MDM 服务器）。



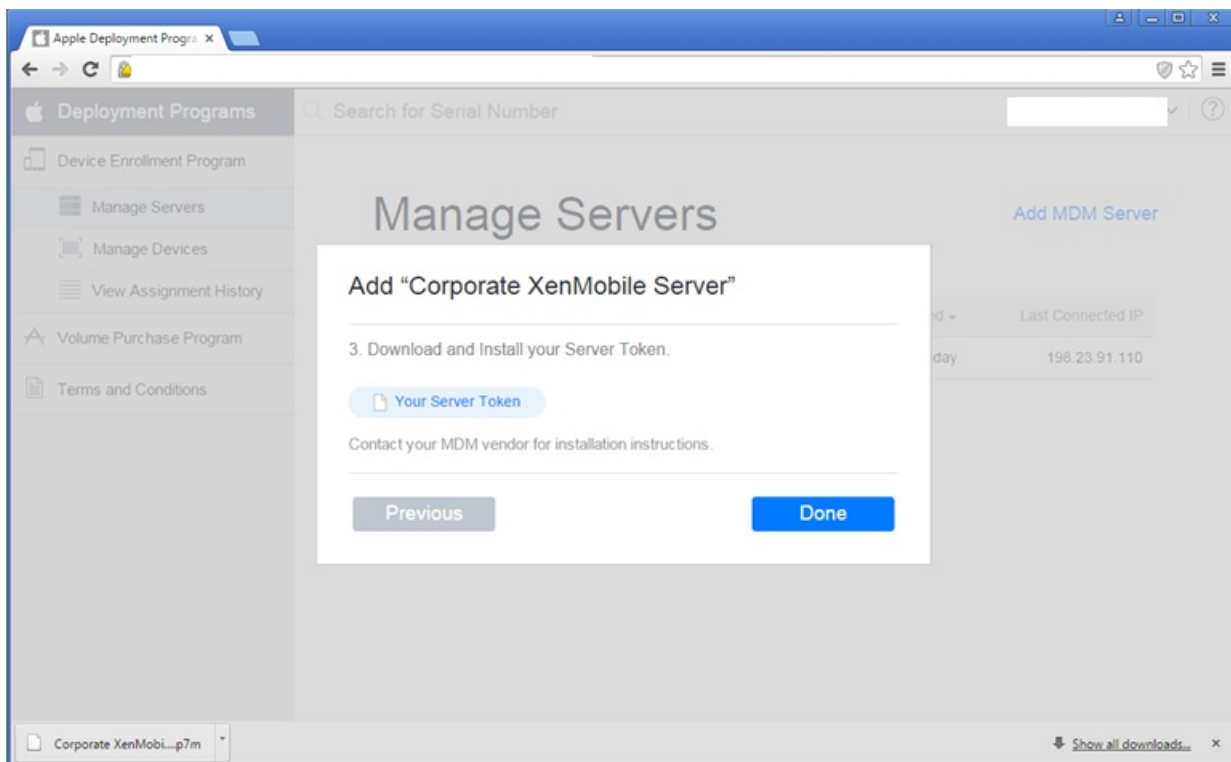
4. 在 **Add MDM Server** (添加 MDM 服务器) 中, 输入 XenMobile 服务器的名称, 然后单击 **Next** (下一步)。



5. 在 Apple DEP 门户上, 单击 **Choose file** (选择文件) 选择从 XenMobile 下载的公钥, 然后单击 **Next** (下一步)。



6. 单击 **Your Server Token** (您的服务器令牌) 生成一个服务器令牌 (可以从浏览器下载) , 然后单击 **Done** (完成) 。



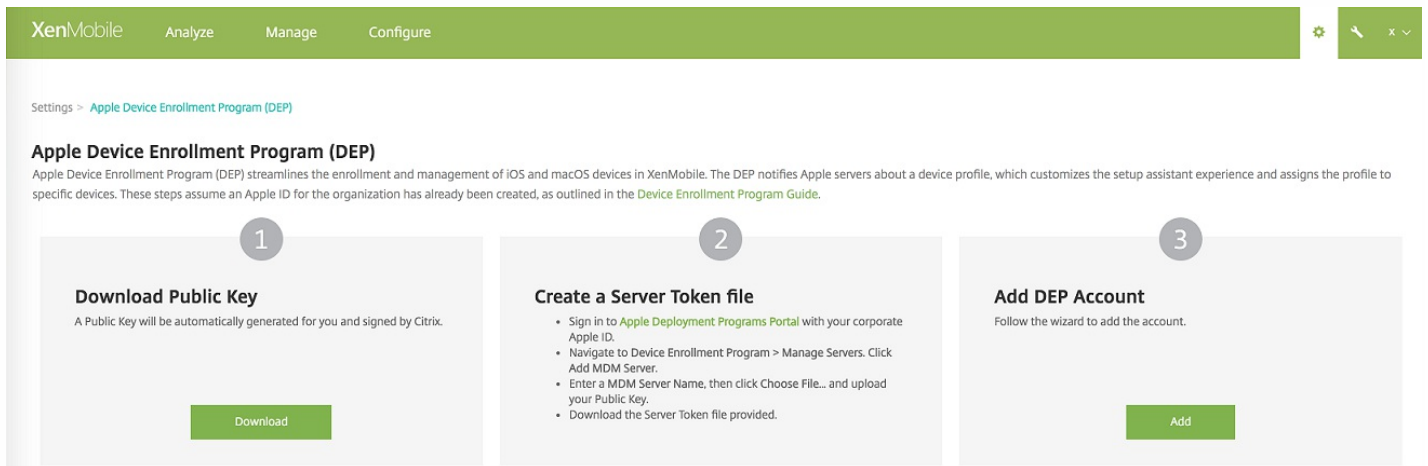
导入令牌文件后, 您的 Apple DEP 令牌信息将在 XenMobile 控制台中显示。您将在向 XenMobile 中添加 DEP 帐户时上载服务器令牌文件。

步骤 3：向 XenMobile 中添加 DEP 帐户

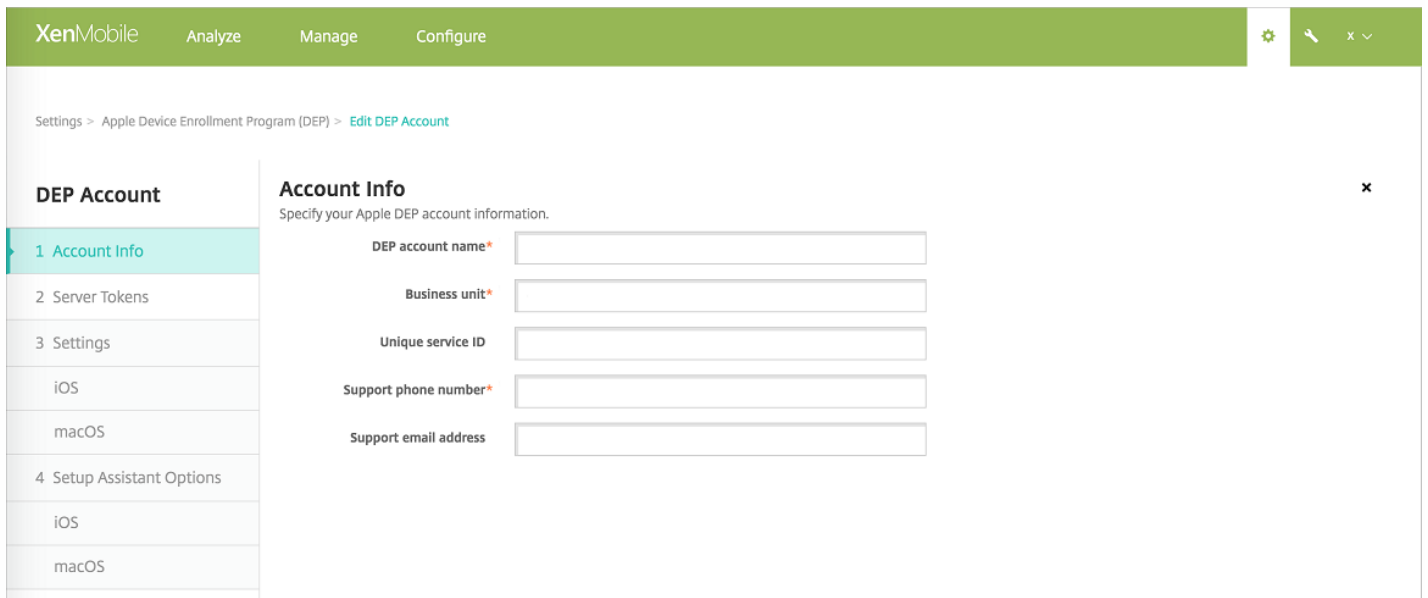
可以向 XenMobile 中添加多个 DEP 帐户。有了此功能，可以按国家/地区和部门等使用不同的注册设置和设置助理选项。然后将 DEP 帐户与不同的设备策略相关联。

例如，可以将来自不同国家/地区的所有 DEP 帐户集中在同一 XenMobile 服务器上，以导入和监督所有 DEP 设备。通过按部门、组织层次结构或其他结构自定义注册设置和设置助手选项，可以确保策略在整个组织中提供合适的功能，并确保设备用户获得合适的设置帮助。

1. 在 XenMobile 控制台中，转至设置 > **Apple Device Enrollment Program (DEP)**，在**添加 DEP 帐户**下，单击**添加**。



2. 在**帐户信息**页面中，指定以下设置：



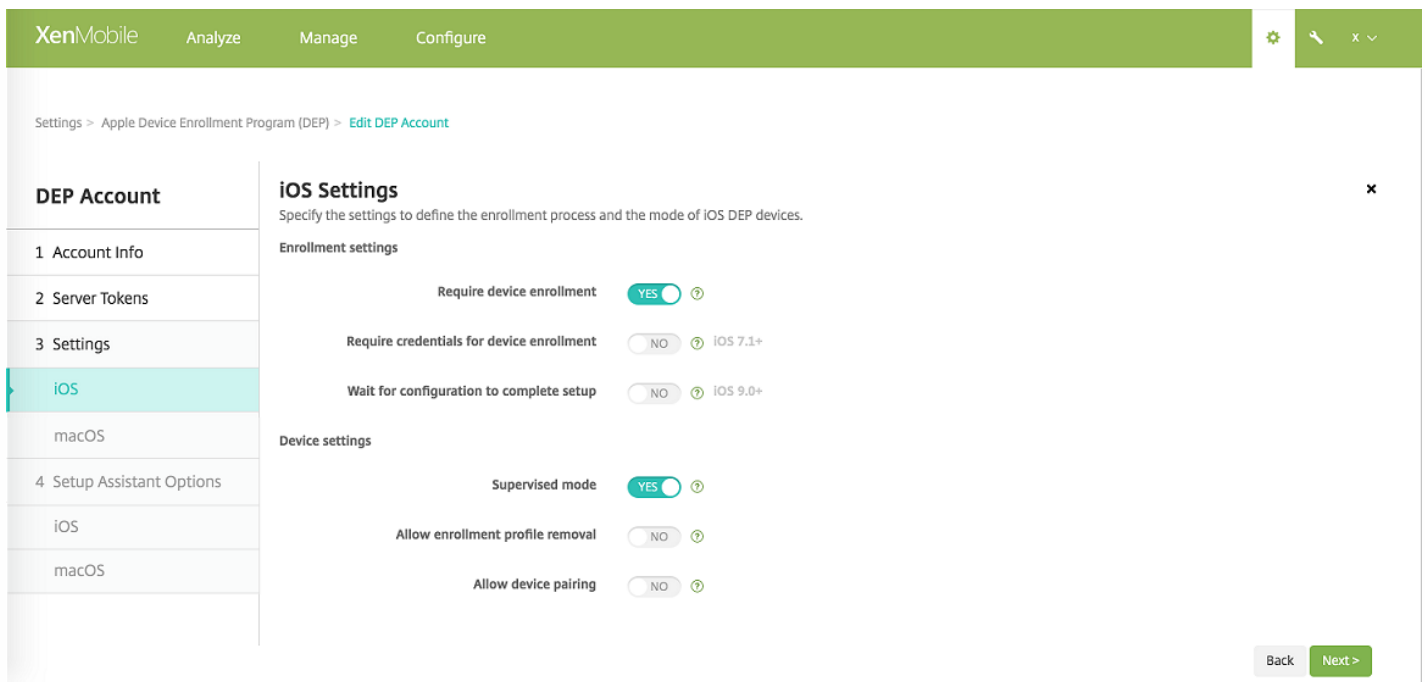
- **DEP 帐户名称**：此 DEP 帐户的唯一名称。请使用反映您如何组织 DEP 帐户（例如按国家/地区或组织层次结构）的名称。
- **业务部门**：将设备分配到的业务部门。此字段为必填字段。
- **唯一服务 ID**：有助于您进一步识别帐户的可选唯一 ID。
- **支持电话号码**：支持电话号码，用户在设置期间可以拨打此号码寻求帮助。此字段为必填字段。
- **支持电子邮件地址**：向用户提供的可选支持电子邮件地址。

3. 在服务器令牌页面中，指定您的服务器令牌文件，然后单击上载。

The screenshot shows the XenMobile configuration interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, the breadcrumb path is 'Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account'. On the left, a sidebar titled 'DEP Account' contains a list of sections: '1 Account Info', '2 Server Tokens' (which is highlighted), '3 Settings', 'iOS', 'macOS', '4 Setup Assistant Options', 'iOS', and 'macOS'. The main content area is titled 'Server Tokens' and includes the instruction 'Upload the Server Token file that you downloaded from Apple DEP portal.' Below this instruction is a form with a label 'Select Server Token file*' followed by a text input field and an 'Upload' button. The form also contains several other fields: 'Consumer key', 'Consumer secret', 'Access token', 'Access secret', 'Access token expiration', 'Server name', 'Server UUID', 'Apple admin ID', 'Organization name', 'Organization email', 'Organization phone', and 'Organization address'. At the bottom right of the form, there are 'Back' and 'Next >' buttons.

此时将显示您的服务器令牌信息。

4. 在 **iOS** 设置中，指定以下设置：



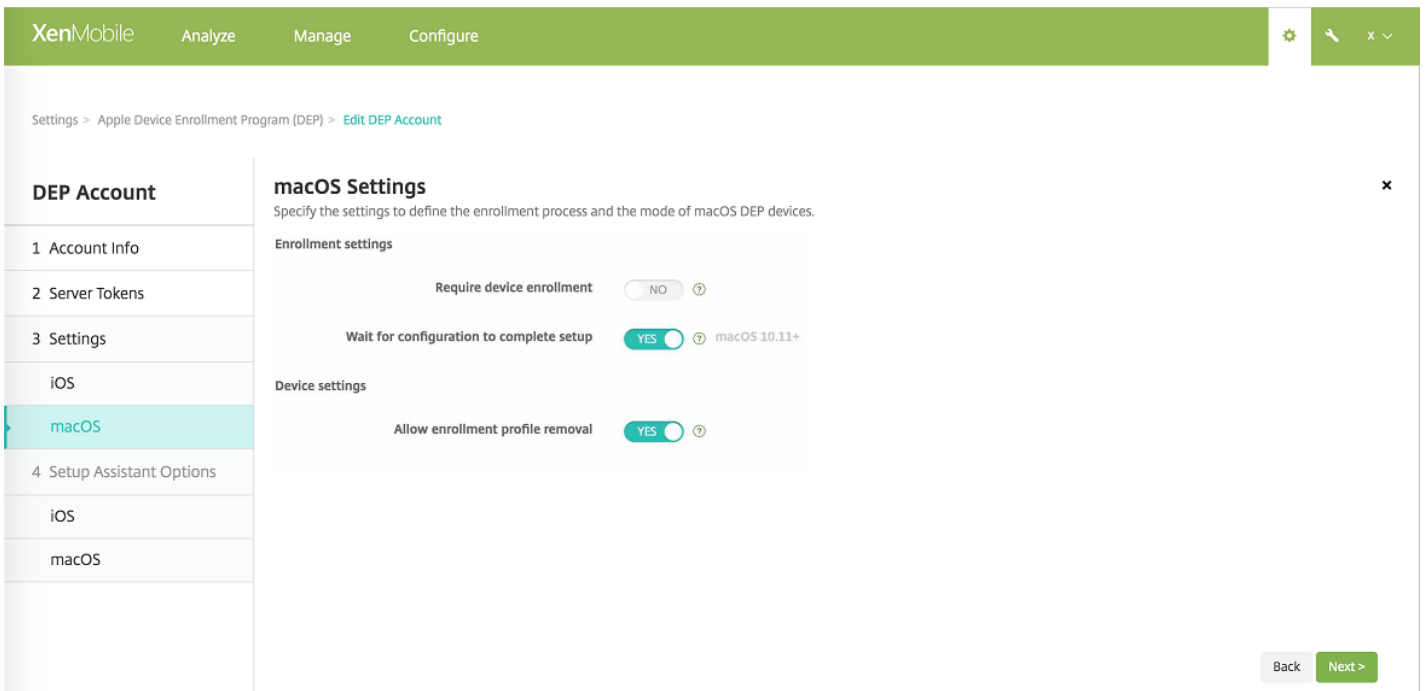
注册设置

- **要求设备注册**：是否要求用户注册其设备。默认值为是。
- **需要提供凭据才能完成设备注册**：DEP 设置过程中是否需要用户输入其凭据。此功能适用于 iOS 7.1 及更高版本。默认值为否。
注意：当 DEP 打开以进行首次设置并且您未选中此选项时，将创建 DEP 组件，例如 DEP 用户、Secure Hub、软件清单和 DEP 部署组。如果未选择此选项，XenMobile 将不创建这些组件。因此，如果您在以后清除此选项，则尚未输入其凭据的用户将无法执行 DEP 注册，因为这些 DEP 组件不存在。在这种情况下，要添加 DEP 组件，应禁用并启用 DEP 帐户。
- **等待完成配置设置**：是否要求用户的设备一直保持在“设置助理”模式，直到将所有 MDM 资源部署到设备。此选项适用于采用受监督模式的 iOS 9.0 及更高版本。默认值为否。
 - Apple 文档指出，当设备处于“设置助手”模式时，以下命令可能无法使用：
 - InviteToProgram
 - InstallApplication
 - ApplyRedemptionCode
 - InstallMedia
 - RequestMirroring
 - DeviceLock

设备设置

- **受监督模式**：如果要使用 Apple Configurator 管理 DEP 注册的设备或启用等待完成配置设置，则必须设置为是。默认值为是。有关将 iOS 设备置于受监督模式的详细信息，请参阅[使用 Apple Configurator 将 iOS 设备置于受监督模式](#)。
- **允许删除注册配置文件**：是否允许设备使用能够远程删除的配置文件。默认值为否。
- **允许设备配对**：是否允许通过 DEP 注册的设备通过 iTunes 和 Apple Configurator 进行管理。默认值为否。

5. 在 macOS 设置中，指定以下设置：



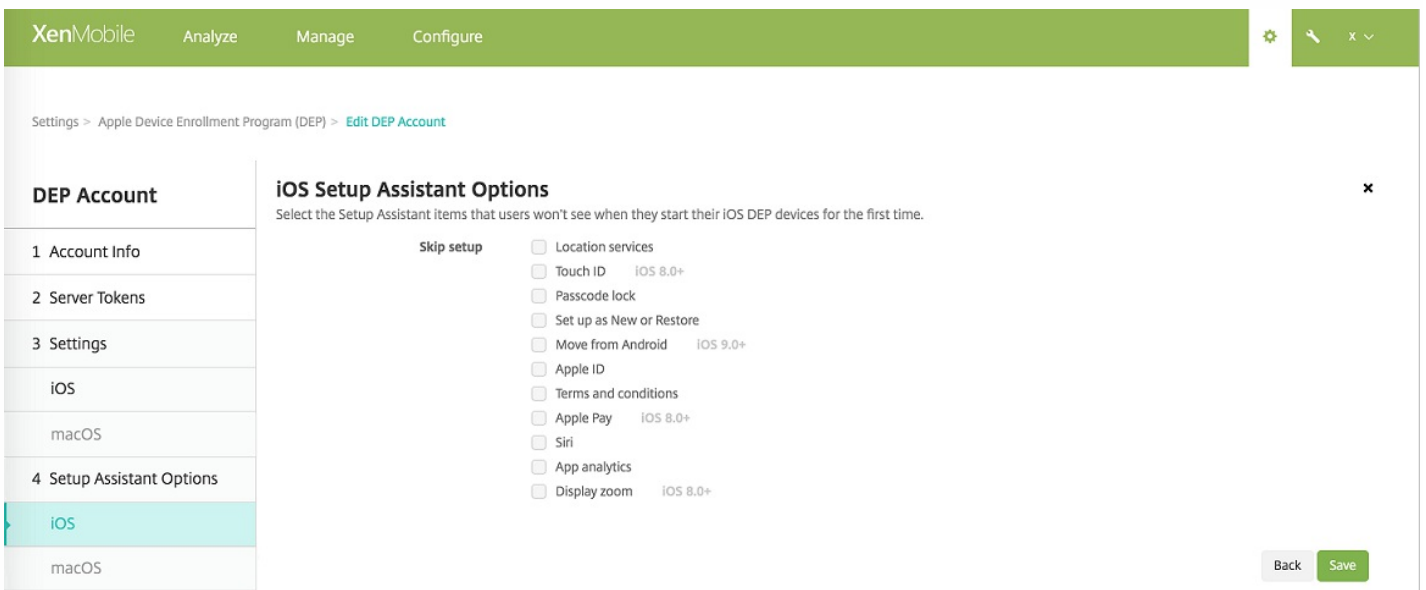
注册设置

- **要求设备注册**：是否要求用户注册其设备。默认值为是。
- **等待完成配置设置**：如果选择是，macOS 设备将不继续在设置助理中操作，直至将 MDM 资源通行码部署到设备。该部署在创建本地帐户之前进行。这一点适用于 macOS 10.11 及更高版本的设备。默认值为否。

设备设置

- **允许删除注册配置文件**：是否允许设备使用能够远程删除的配置文件。默认值为否。

6. 在 **iOS 设置助理选项** 中，选择用户在首次开始使用其设备时不需要执行的 iOS 设置助理步骤（即要跳过的步骤）。所有项目的默认设置为未选中。



- **定位服务**：在设备上设置定位服务。
- **Touch ID**：在 iOS 8.0 及更高版本的设备上设置 Touch ID。
- **通行码锁**：为设备创建通行码。
- **设置为新对象或还原**：将设备设置为新设备或从 iCloud 或 iTunes 备份设置设备。
- **从 Android 移动**：启用从 Android 设备向 iOS 9 或更高版本设备传递数据。此选项仅在已选择**设置为新对象或还原**（即跳过此步骤）时可用。
- **Apple ID**：设置设备的 Apple ID 帐户。
- **条款和条件**：要求用户接受条款和条件才能使用设备。
- **Apple Pay**：在 iOS 8.0 及更高版本的设备上设置 Apple Pay。
- **Siri**：是否在设备上使用 Siri。
- **应用程序分析**：设置是否与 Apple 共享崩溃数据和使用统计信息。
- **显示缩放**：设置 iOS 8.0 或更高版本设备上的显示分辨率（标准或放大）。

DEP 帐户在**设置 > Apple Device Enrollment Program (DEP)** 上显示。

7. 在 **macOS 设置助理选项** 中，选择用户在首次开始使用其设备时不需要执行的 macOS 设置助理步骤（即要跳过的步骤）。所有项目的默认设置为未选中。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The breadcrumb trail is 'Settings > Apple Device Enrollment Program (DEP) > Edit DEP Account'. The left sidebar shows a 'DEP Account' section with sub-items: '1 Account Info', '2 Server Tokens', '3 Settings', 'iOS', 'macOS', and '4 Setup Assistant Options'. Under '4 Setup Assistant Options', 'iOS' and 'macOS' are listed, with 'macOS' selected. The main content area is titled 'macOS Setup Assistant Options' and includes a sub-header 'Skip setup' with the following options:

- Set up as New or Restore
- Location services
- Apple ID
- Terms and conditions
- Siri macOS 10.12+
- FileVault
- App analytics
- Registration macOS 10.10-

 Below this is the 'Local account setup options' section:

- Create primary account as a standard user macOS 10.11+

 There are three input fields: 'Admin full name', 'Admin short name', and 'Admin password'. At the bottom, there is a checkbox for 'Show administrator account in Users and Groups' and 'Back' and 'Save' buttons.

- **设置为新对象或还原**：将设备设置为新设备或从 iCloud 或 iTunes 备份设置设备。
- **定位服务**：在设备上设置定位服务。
- **Apple ID**：设置设备的 Apple ID 帐户。
- **条款和条件**：要求用户接受条款和条件才能使用设备。
- **Siri**：是否在设备上使用 Siri。
- **FileVault**：使用 FileVault 加密启动磁盘。仅当系统具有一个本地用户帐户并且该帐户已登录到 iCloud 时 XenMobile 才应用 FileVault 设置。

注意：可以使用 macOS FileVault 磁盘加密功能通过加密其内容来保护系统卷的安全 (<https://support.apple.com/en->

us/HT204837)。如果您在未打开 FileVault 功能的新型便携式 Mac 上运行设置助理，系统可能会提示您打开此功能。该提示在新系统以及升级到 OS X 10.10 或 10.11 的系统中显示，但仅当系统具有一个本地管理员帐户并且该帐户已登录到 iCloud 时显示。

- **应用程序分析**：设置是否与 Apple 共享崩溃数据和使用统计信息。
- **注册**：要求用户注册其设备。

注册信息设置通过 OS X 10.9 获取。注册过程允许您向 Apple 发送系统注册信息。此信息将您的联系信息与 Mac 硬件相关联。Apple 主要使用该信息来帮助提供 AppleCare 支持。如果以前输入了 Apple ID，设置助理将根据您的 Apple ID 帐户有选择地提交注册。如果未输入 Apple ID，可以手动输入您的联系信息。

在**本地帐户设置选项**下，指定用于创建管理员帐户的设置，这是 macOS 所需的设置。XenMobile 将使用指定的信息创建帐户。

8. 要测试 XenMobile 与 Apple 之间的连接，请选择该帐户并单击**测试连接**。

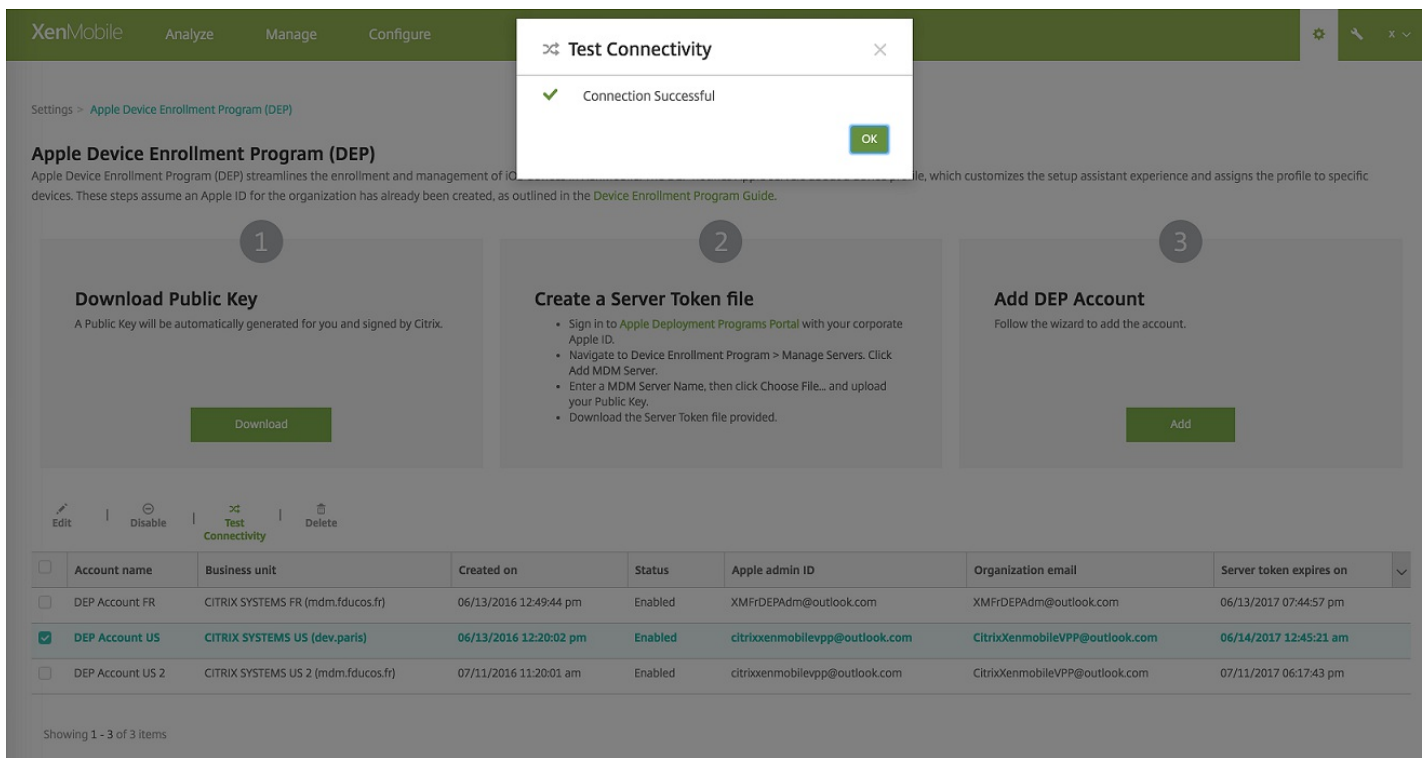
The screenshot shows the XenMobile console interface for configuring the Apple Device Enrollment Program (DEP). The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main content area is titled 'Apple Device Enrollment Program (DEP)' and contains three numbered steps:

- Download Public Key**: A Public Key will be automatically generated for you and signed by Citrix. A 'Download' button is present.
- Create a Server Token file**: Includes instructions to sign in to the Apple Deployment Programs Portal, navigate to Device Enrollment Program > Manage Servers, click Add MDM Server, enter an MDM Server Name, click Choose File... and upload your Public Key, and download the Server Token file provided. An 'Add' button is present.
- Add DEP Account**: Follow the wizard to add the account. An 'Add' button is present.

Below the steps is a table of DEP accounts. The 'DEP Account US' row is selected, and a context menu is open over it with the 'Test Connectivity' option highlighted.

<input type="checkbox"/>	Account name	Business unit	Created on	Status	Apple admin ID	Organization email	Server token expires on
<input type="checkbox"/>	DEP Account FR	CITRIX SYSTEMS FR (mdm.fducos.fr)	06/13/2016 12:49:44 pm	Enabled	XMFrDEPAdm@outlook.com	XMFrDEPAdm@outlook.com	06/13/2017 07:44:57 pm
<input checked="" type="checkbox"/>	DEP Account US	CITRIX SYSTEMS US (dev.paris)	06/13/2016 12:20:02 pm	Enabled	citrixxenmobilevpp@outlook.com	CitrixXenmobileVPP@outlook.com	06/14/2017 12:45:21 am
<input type="checkbox"/>	DEP Account US 2	CITRIX SYSTEMS US 2 (mdm.fducos.fr)	07/11/2016 11:20:01 am	Enabled	citrixxenmobilevpp@outlook.com	CitrixXenmobileVPP@outlook.com	06/14/2017 12:45:21 am

此时将显示一条状态消息。



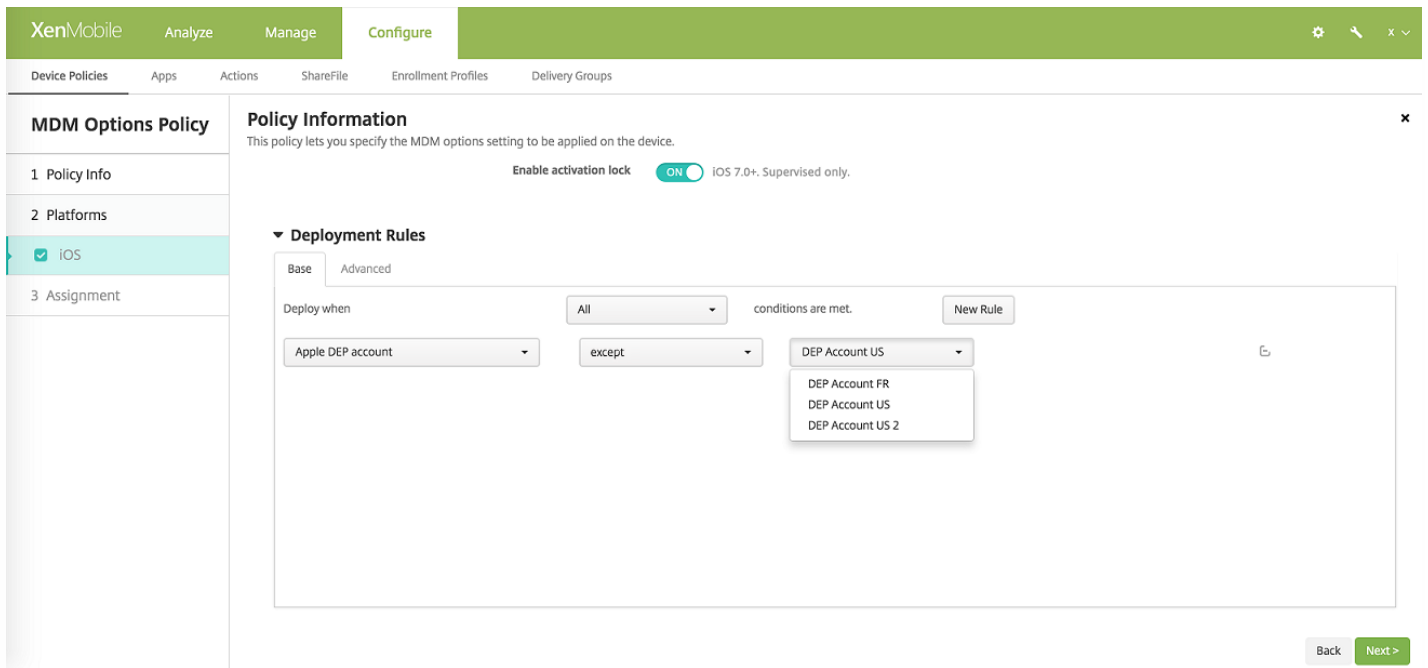
配置 DEP 帐户的设备策略和应用程序的部署规则

可以使用配置 > 设备策略和配置 > 应用程序下的部署规则部分将 DEP 帐户与不同的设备策略和应用程序相关联。可以指定某个策略或应用程序：

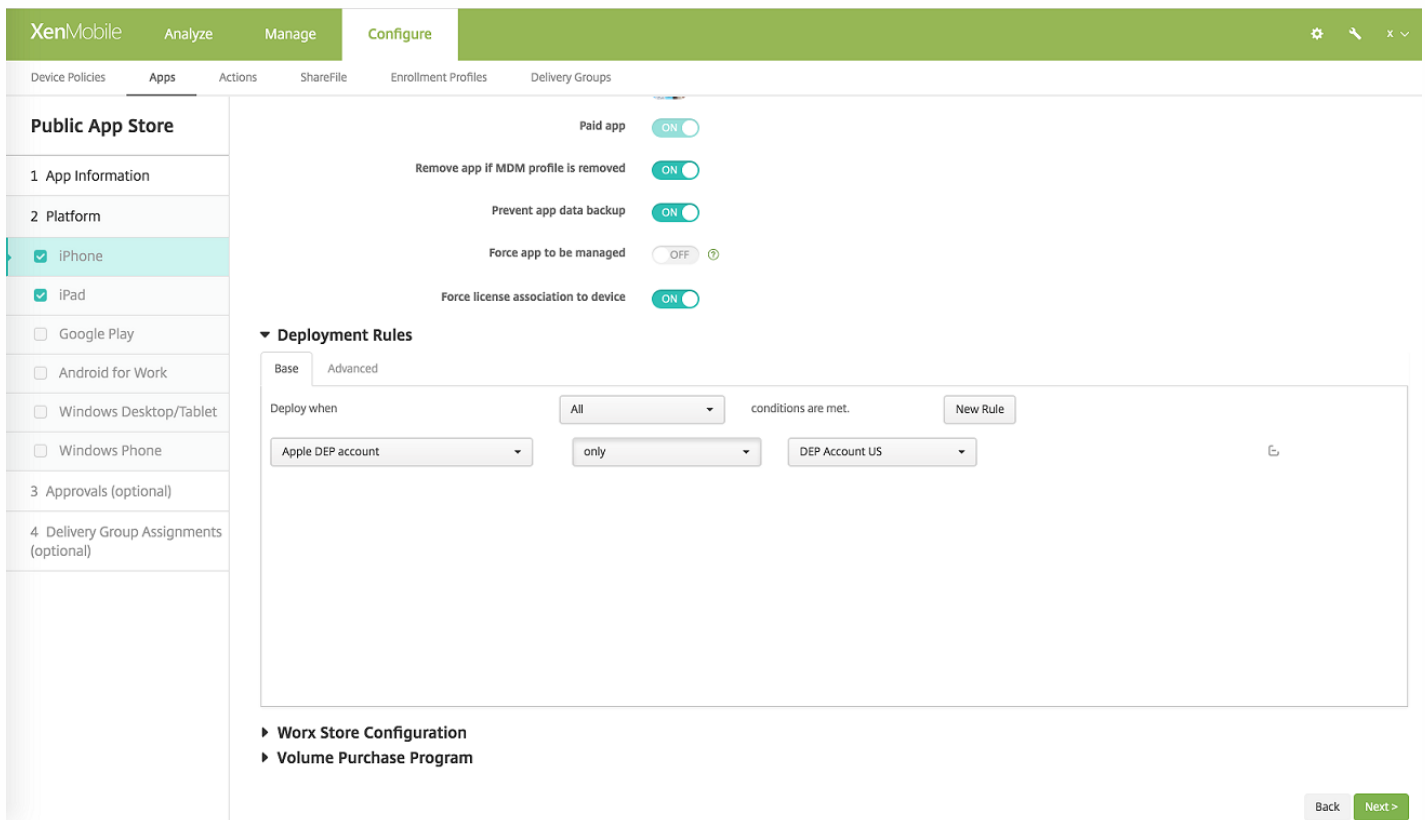
- 仅针对特定的 Apple DEP 帐户部署。
- 针对除所选帐户外的所有 Apple DEP 帐户部署。

DEP 帐户的列表仅包括状态为已启用或已禁用的帐户。如果 DEP 帐户已禁用，DEP 设备将不属于该帐户。因此，XenMobile 不会将应用程序或策略部署到该设备。

在下例中，适用于 iOS 的 MDM 选项策略将部署到不使用 Apple DEP 帐户“DEP Account US”的设备。



在下列中，适用于 iPhone 的公共应用商店应用程序将仅针对使用 Apple DEP 帐户“DEP Account US”的设备进行部署。



配置 Apple Configurator 设置

1. 在 XenMobile 控制台中，转至设置 > Apple Configurator 设备注册。

Settings > [Apple Configurator Device Enrollment](#)

Apple Configurator Device Enrollment

Use Apple Configurator to mass configure and deploy iPhone, iPad or iPod Touch.



Export anchor
certificates

Enable Apple Configurator device enrollment YES

Enrollment URL to enter in Apple Configurator

Require device registration before enrollment NO

Require credentials for device enrollment YES iOS 7.1+

Cancel

Save

2. 将启用 **Apple Configurator** 设备注册设置为是。

3. **Enrollment URL to enter in Apple Configurator** (要在 Apple Configurator 中输入的注册 URL) 为只读字段。这是 XenMobile 服务器与 Apple 通信时使用的 URL。稍后在这些步骤中，请将该 URL 复制并粘贴到 Apple Configurator 中。在 Apple Configurator 2 中，注册 URL 是指 XenMobile 服务器的完全限定域名 (FQDN) (例如 `mdm.server.url.com`) 或 IP 地址。

4. 要防止注册未知设备，请将 **要求在注册之前注册设备** 设置为是。注意：如果此设置为是，必须先在 XenMobile 中手动或通过 CSV 文件将所配置的设备添加到 **管理 > 设备**，然后再进行注册。

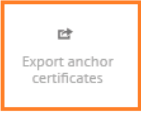
5. 请将 **需要提供凭据才能完成设备注册** 设置为是，才能要求使用 iOS 7.1 及更高版本的设备的用户在注册时输入其凭据。默认不要求提供注册凭据。

6. 注意：如果 XenMobile 服务器使用的是可信 SSL 证书，请跳过此步骤。单击 **Export anchor certs** (导出锚点证书)，然后将 `certchain.pem` 文件保存到 OS X 钥匙串中 (登录或系统)。

Settings > [Apple Configurator Device Enrollment](#)

Apple Configurator Device Enrollment

Use Apple Configurator to mass configure and deploy iPhone, iPad or iPod Touch.



Enable Apple Configurator device enrollment

Enrollment URL to enter in Apple Configurator

Require device registration before enrollment ?

Require credentials for device enrollment ? iOS 7.1+

Cancel Save

7. 启动 Apple Configurator，然后转至 **Prepare (准备)** > **Setup (设置)** > **Configure Settings (配置设置)**。

8. 在**设备注册**设置中，将步骤 4 中的 MDM 服务器 URL 粘贴到 Configurator 中的 **MDM server URL** (MDM 服务器 URL) 字段。

9. 如果 XenMobile 不使用可信 SSL 证书，请在**设备注册**设置中，将根证书颁发机构和 SSL 服务器证书颁发机构复制到 **Anchor (锚点)** 证书中。

10. 使用 USB 电缆的基座接口将设备连接到运行 Apple Configurator 的 Mac，以便同时配置多达 30 台已连接的设备。如果没有基座接口，请使用一个或多个有源 USB 2.0 高速集线器连接设备。

11. 单击 **Prepare (准备)**。有关通过 Apple Configurator 准备设备的详细信息，请参阅 Apple Configurator 帮助页面[准备设备](#)。

12. 在 Apple Configurator 中，配置所需的设备策略。

13. 在配置每个设备的过程中，请将其打开以启动 iOS 设置助理，以便为首次使用准备好设备。

使用 Apple DEP 时续订或更新证书

续订 XenMobile 安全套接字层 (SSL) 证书时，请在 XenMobile 控制台的**设置 > 证书**中上传新证书。在**导入对话框的用作**中，请务必单击 **SSL 侦听器**，以便将该证书用于 SSL。重新启动服务器后，XenMobile 将使用新 SSL 证书。有关 XenMobile 中的证书的详细信息，请参阅[上传 XenMobile 中的证书](#)。

续订或更新 SSL 证书时，不需要在 Apple DEP 与 XenMobile 之间重新建立信任关系。但是，可以按照本文中之前的步骤随时重新配置 DEP 设置。

有关 Apple DEP 的详细信息，请参阅 [Apple 文档](#)。

使用 Apple Configurator 将 iOS 设备置于受监督模式

Important

将设备置于受监督模式时，系统将会在设备上安装所选版本的 iOS，同时完全擦除设备上以前存储的任何用户数据或应用程序。

1. 从 iTunes 安装 [Apple Configurator](#)。
2. 将 iOS 设备连接到 Apple 电脑。
3. 启动 Apple Configurator。Configurator 显示您有一台设备需要进行监督前的准备工作。
4. 设备监督前准备工作：
 - a. 将 **Supervision**（监督）控件值切换到 **On**（开）。如果您打算通过定期重新应用配置来维护对设备的控制，Citrix 建议您选择此设置。
 - b. 提供设备的名称（可选）。
 - c. 在 iOS 中，单击 **Latest**（最新），获取您要安装的最新版本的 iOS。
5. 当您准备进行设备监督前的准备工作时，请单击 **Prepare**（准备）。

通过 Apple DEP 部署 iOS 和 macOS 设备

Feb 27, 2017

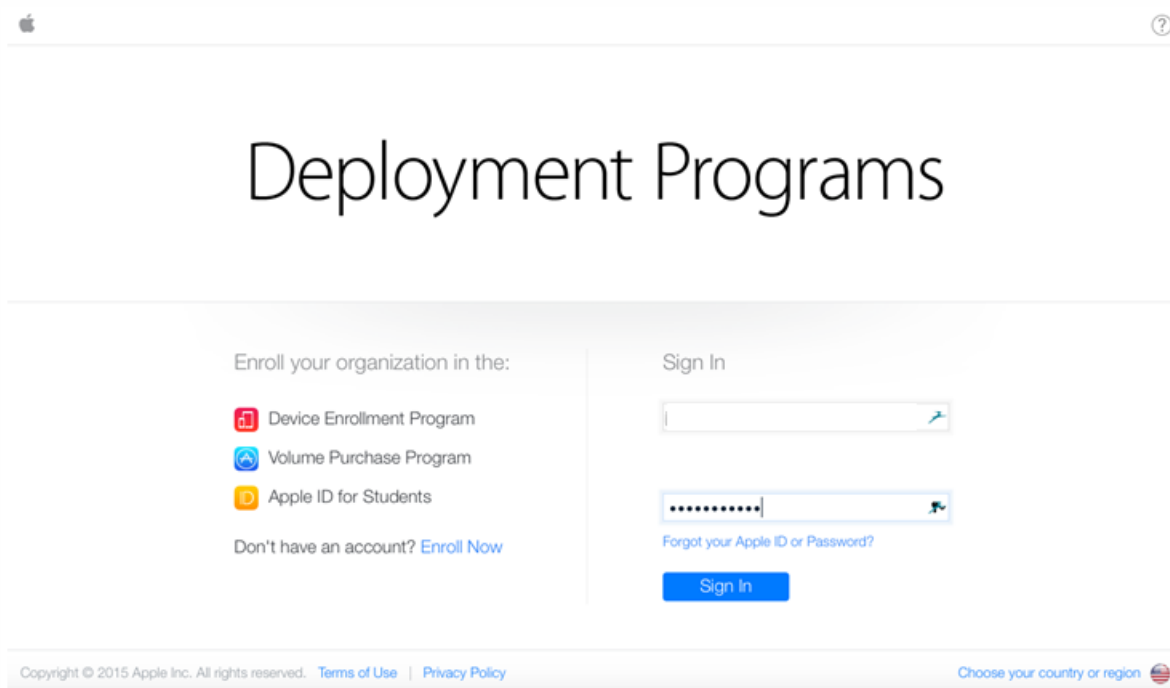
必须在“Apple 部署计划”中注册才能使用 Apple Device Enrollment Program (DEP) 在 XenMobile 中进行 iOS 和 macOS 设备注册和管理。有关如何注册“Apple 部署计划”帐户的信息，请参阅此 Apple PDF。

请注意：“Apple 部署计划”面向组织而非个人提供。您必须提供很多企业细节和信息才能创建“Apple 部署计划”帐户。因此，可能需要一些时间才能完成帐户申请并收到帐户批准。

注册 Apple 部署计划

1. 访问 deploy.apple.com 以申请“Apple 部署计划”帐户。申请 DEP 帐户时，最佳做法是使用组织的电子邮件地址，例如 `dep@company.com`。

注意：如果是教育机构帐户，请访问 <https://school.apple.com/>。



2. 键入组织信息后，Apple 会通过电子邮件向您发送新 Apple ID 的临时密码。

- 1 Your Details
- 2 Verification Contact
- 3 Institution Details
- 4 Review

Check Your E-mail

An e-mail has been sent to [redacted] with your Apple ID and temporary password, and the next steps to continue your enrollment.

1. Complete your Apple ID setup.

[Visit My Apple ID >](#)

Using the Apple ID and temporary password included in the e-mail, sign in and complete your account setup at My Apple ID.

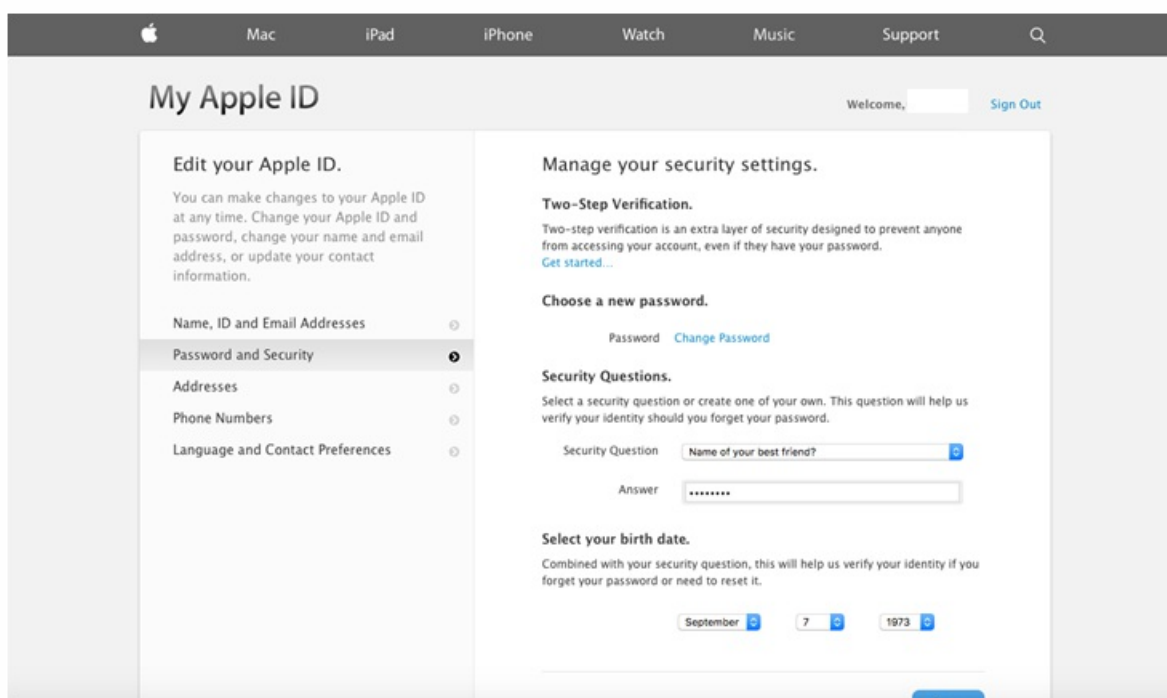
2. Enable two-step verification for this account as it is required by some programs.

3. Continue your Deployment Programs enrollment.

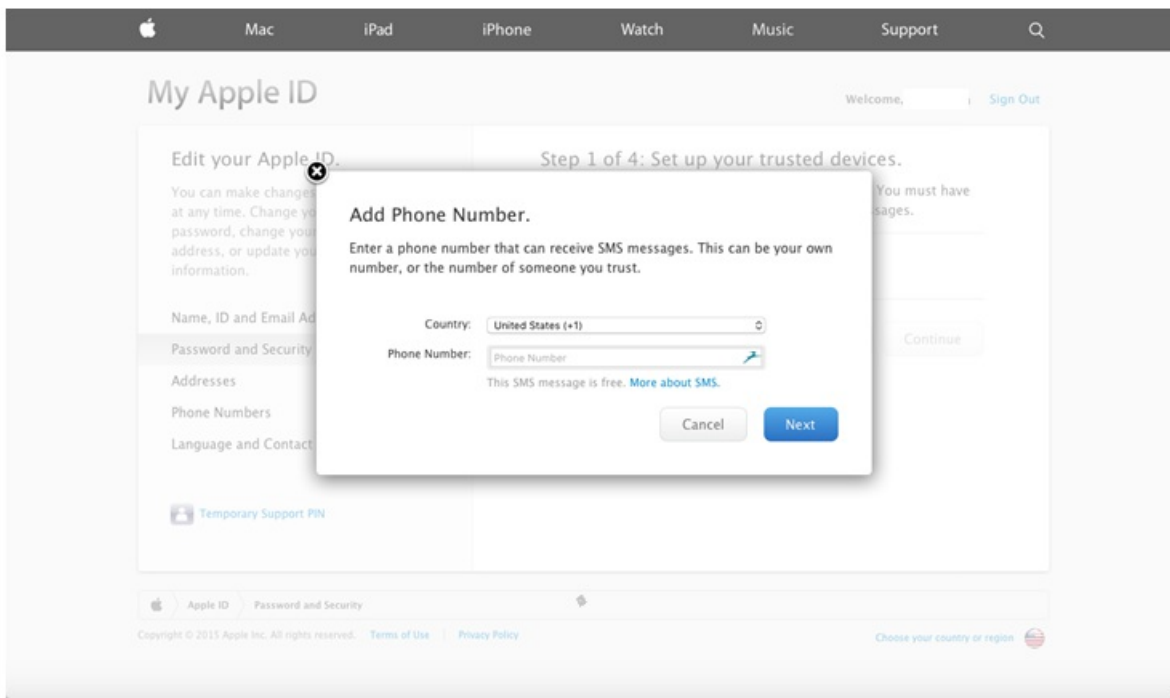
After completing the steps above, please return and continue this enrollment here at deploy.apple.com.

Next Step

3. 随后请使用 Apple ID 登录并完成帐户的安全设置。

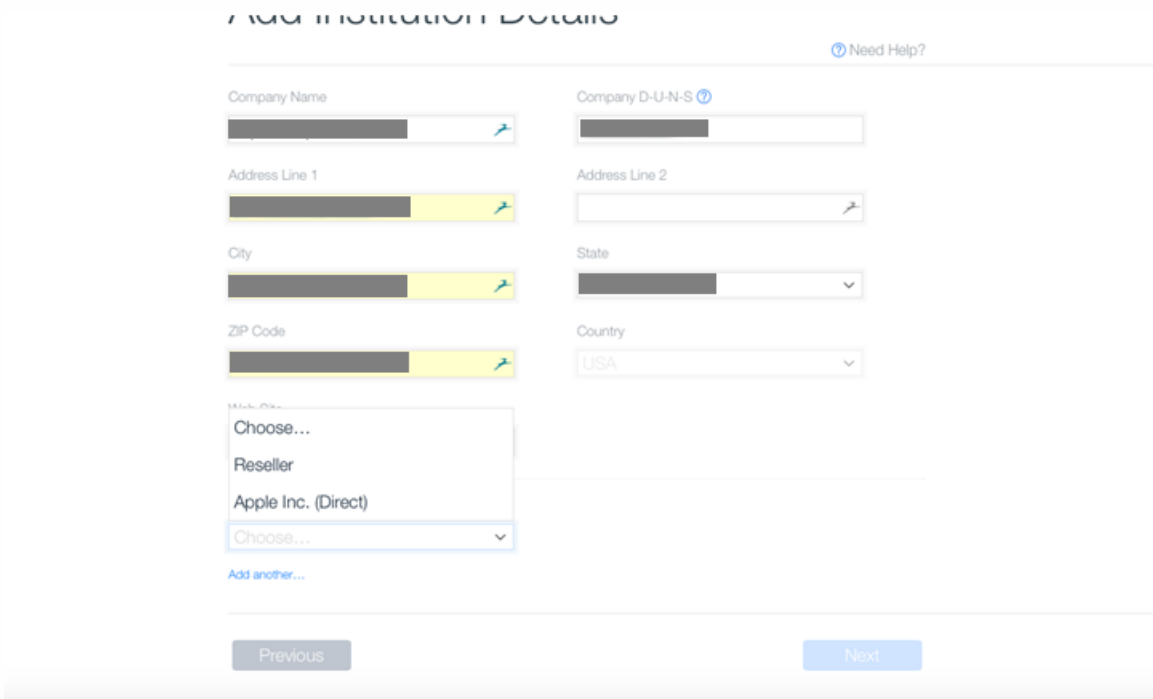


4. 配置并启用双重验证（需要在 DEP 门户上使用该验证方法）。在执行这些步骤的过程中，您添加一个电话号码后，您会收到用于双重验证的 4 位数 PIN 码。



5. 登录 DEP 门户以使用设置的双重验证完成帐户配置。

6. 添加您的公司详细信息，然后选择购买设备的地点。有关购买选项的详细信息，请参阅下一部分[订购启用了 DEP 的设备](#)。



7. 添加 Apple 客户编号或 DEP 经销商 ID。然后验证注册详细信息并等待 Apple 审批您的帐户。

7 ADD INSTITUTION DETAILS

[Need Help?](#)

Company Name	Company D-U-N-S ?
Address Line 1	Address Line 2
City	State
ZIP Code	Country
Web Site	
Devices Purchased From	DEP Reseller ID ?
Reseller	CDW

[Add another...](#)

Previous

Next

Deployment Programs

1 Your Details 2 Verification Contact 3 Institution Details 4 Review

Review Your Enrollment Details

[Need Help?](#)

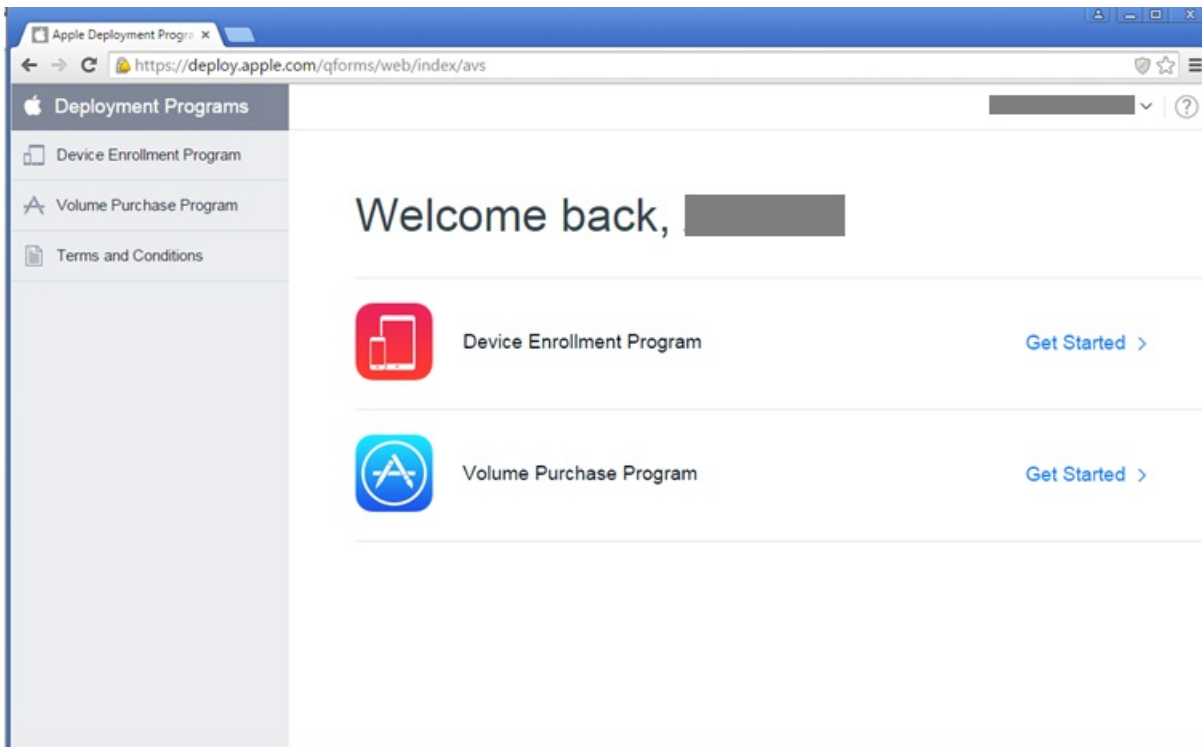
Your Details Verification Contact Institution Details

Your Name	Verification Contact Name	Company Name
Your Work E-mail	Verification Contact Work E-mail	Web Site
Your Work Phone	Verification Contact Work Phone	Address
Your Title / Position	Title / Position	Devices Purchased From
General Manager	General Manager	

Edit

Submit

8. 收到 Apple 发送的登录凭据后，登录 Apple DEP 门户。



要将您的帐户连接到 XenMobile，请参阅[批量注册 iOS 和 macOS 设备](#)中的“将 Apple DEP 帐户与 XenMobile 集成”。

订购启用了 DEP 的设备

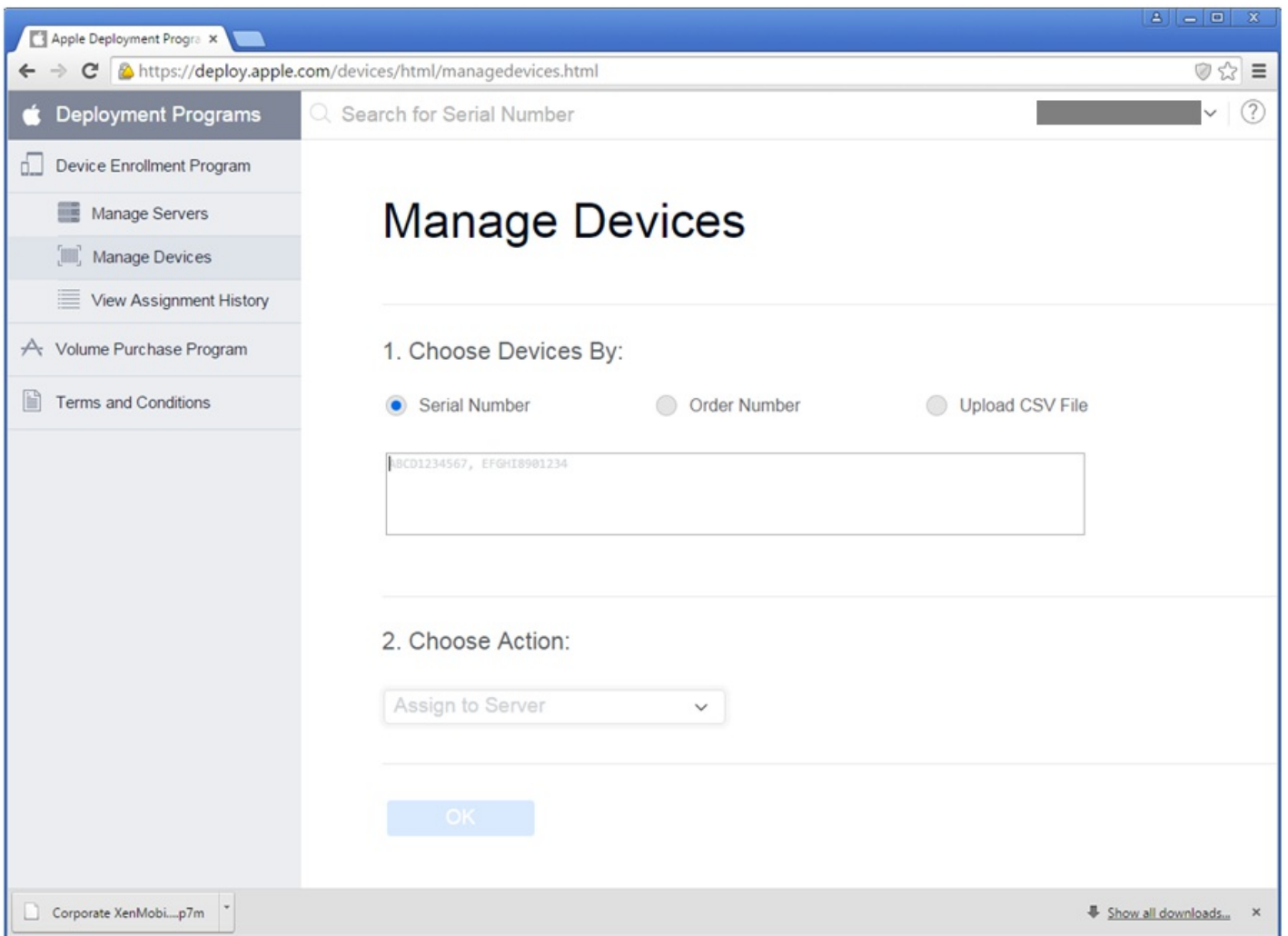
可以直接从 Apple 或启用了 DEP 的授权经销商或运营商处订购启用了 DEP 的设备。要从 Apple 订购，请在 Apple DEP 门户中提供您的 Apple 客户 ID。Apple 可以通过您的客户 ID 将您购买的设备与您的 Apple DEP 帐户关联。

要从经销商或运营商处订购，请联系 Apple 经销商或运营商，确认其是否加入了 Apple DEP。购买设备时，请要求提供经销商的 Apple DEP ID。您将您的 Apple DEP 经销商添加到您的 Apple DEP 帐户时，Apple 要求提供此信息。添加经销商的 Apple DEP ID 后，您将收到 DEP 客户 ID。请向经销商提供 DEP 客户 ID，经销商将使用该 ID 将您购买的设备的相关信息提交给 Apple。有关详细信息，请参阅 [Apple Web 站点](#)。

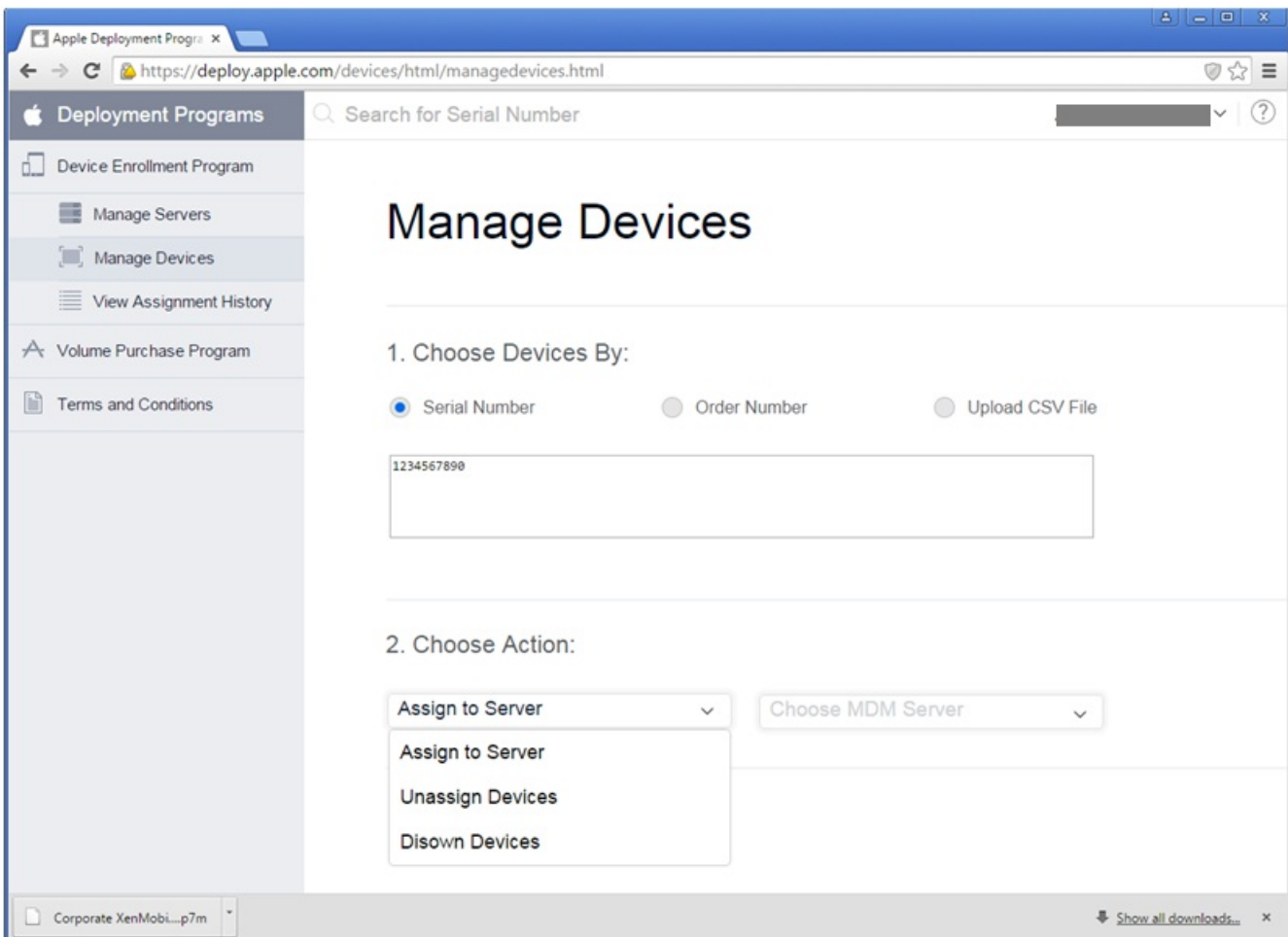
管理启用了 DEP 的设备

请按照以下步骤使用 DEP 门户更新您的 Apple DEP 帐户来将设备与 XenMobile 服务器关联。

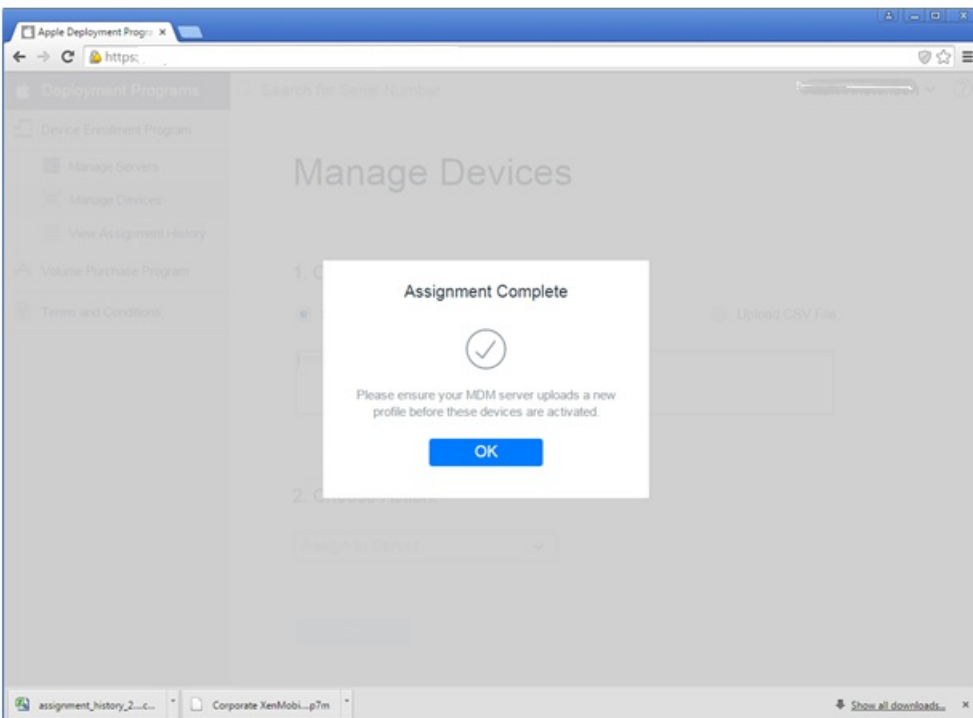
1. 登录 Apple DEP 门户。
2. 单击 **Device Enrollment Program**，然后单击 **Manage Devices**（管理设备）。在 **Choose Devices By**（选择设备依据）中，选择上载并定义启用了 Apple DEP 的设备时使用的选项，即 **Serial Number**（序列号）、**Order Number**（订单号）或 **Upload CSV File**（上载 CSV 文件）。



3. 要将您的设备分配给 XenMobile 服务器，请单击 **Choose Action**（选择操作）下方的 **Assign to Server**（分配给服务器）。然后，在列表中选择 XenMobile 服务器的名称。单击 **OK**（确定）。



您的 Apple DEP 设备现在已与选定 XenMobile 服务器相关联。



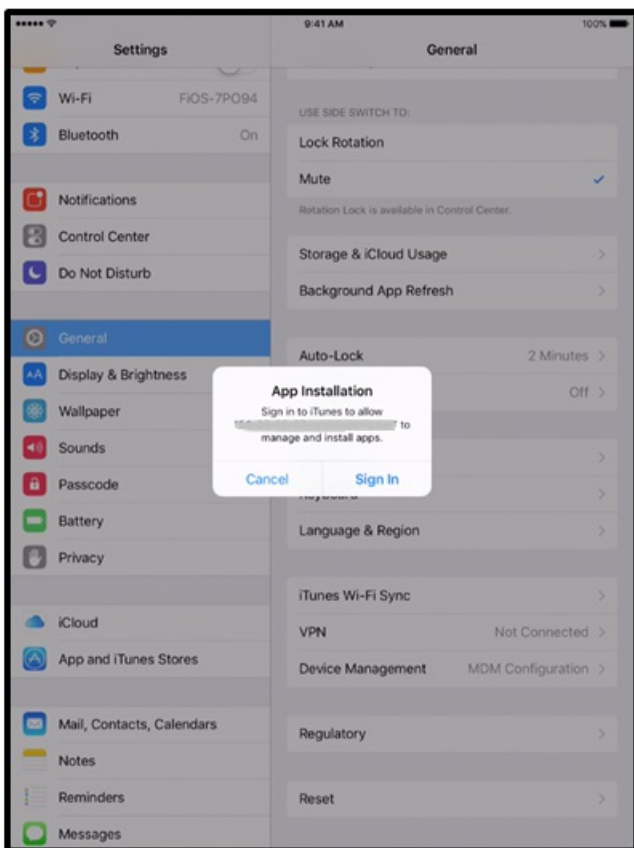
注册启用了 Apple DEP 的设备时的用户体验

用户注册启用了 Apple DEP 的设备时，其体验如下。

1. 用户启动启用了 Apple DEP 的设备。
2. XenMobile 将您在 XenMobile 控制台中配置的 Apple DEP 配置提交至启用了 Apple DEP 的设备。
3. 用户在其设备上配置初始设置。
4. 该设备将自动启动 XenMobile 设备注册过程。
5. 用户继续在其设备上配置其他初始设置。
6. 在主屏幕中，系统可能会提示用户登录 iTunes，以便他们可以下载 Citrix Secure Hub。

注意

如果 XenMobile 已配置为使用基于设备的批量购买计划 (VPP) 应用程序分配来部署 Secure Hub 应用程序，则此步骤是可选的。在这种情况下，不需要创建 iTunes 帐户，也不需要使用现有帐户。



7. 用户打开 Secure Hub 并键入其凭据。如果策略要求，系统可能会提示用户创建并验证 Citrix PIN。

XenMobile 将任何其他必备应用程序部署到设备。

客户端属性

Apr 26, 2017

客户端属性包含用户设备上直接提供给 Secure Hub 的信息。可以使用这些属性配置高级设置，如 Citrix PIN。从 Citrix 支持获取客户端属性。

每次发布客户端应用程序（尤其是 Secure Hub）时，均会更改客户端属性。有关通常要配置的客户端属性的详细信息，请参阅本文中后面的内容介绍的[客户端属性参考](#)。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在客户端下方，单击客户端属性。此时将显示客户端属性页面。可以从此页面添加、编辑和删除客户端属性。

XenMobile Analyze Manage Configure administrator

Settings > Client Properties

Client Properties

To change a property, select the property and then click Edit.

Add

<input type="checkbox"/>	Name	Key	Value	Description
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
<input type="checkbox"/>	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History
<input type="checkbox"/>	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
<input type="checkbox"/>	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

添加客户端属性

1. 单击添加。此时将显示添加新客户端属性页面。

XenMobile Analyze Manage Configure

Settings > Client Properties > Add New Client Property

Add New Client Property

Key ?

Value*

Name*

Description*

Cancel Save

2. 配置以下设置：

- **键**：在列表中，单击要添加的属性键。**重要**：执行任何更改或请求特殊键以进行更改时请联系 Citrix 支持。
- **值**：输入选定属性的值。
- **名称**：输入属性的名称。
- **说明**：输入属性的说明。

3. 单击保存。

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：

- **密钥**：无法更改此字段。
- **值**：属性的值。
- **名称**：属性的名称。
- **说明**：属性的说明。

4. 单击**保存**以保存您的更改，或单击**取消**保持属性不变。

删除客户端属性

1. 在**客户端属性**表格中，选择要删除的客户端属性。

注意：可以通过选中每个属性旁边的复选框，选择要删除的多个属性。

2. 单击**删除**。此时将显示确认对话框。再次单击**删除**。

客户端属性参考

XenMobile 首选客户端属性及其默认设置如下所示。

CONTAINER_SELF_DESTRUCT_PERIOD

显示名称：MDX 容器自毁期限

自毁功能阻止在经过特定天数的非活动状态后访问 Secure Hub 和托管应用程序。超过此时间限制后，应用程序不再可用，用户设备取消从 XenMobile 服务器注册。擦除数据包括清除已安装的各应用程序的应用程序数据，包括应用程序缓存和用户数据。不活动时间是指在经过特定时间长度后，服务器不接收身份验证请求以验证用户。例如，如果为此策略设置 30 天，用户不使用 Secure Hub 或其他应用程序的时间超过 30 天，则此策略生效。

此全局安全策略适用于 iOS 和 Android 平台，是对现有应用程序锁定和擦除策略的增强。

要配置此全局策略，请转至设置 > **客户端属性**，然后添加自定义键 **CONTAINER_SELF_DESTRUCT_PERIOD**。

值：天数

DEVICE_LOGS_TO_IT_HELP_DESK

显示名称：向 IT 技术支持人员发送设备日志

此属性启用或禁用向 IT 技术支持人员发送日志的功能。

可能的值：**true** 或 **false**

默认值：**false**

DISABLE_LOGGING

显示名称：禁用日志记录

此属性允许您禁用用户从其设备收集并上载日志的功能。将为 Secure Hub 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 Secure Hub 和 MDX 应用程序的日志设置。

将此属性设置为 **true** 时，Secure Hub 将阻止应用程序日志设置为 **true**，以确保在应用新策略时 MDX 应用程序停止记录日志。

可能的值：**true** 或 **false**

默认值：**false**（不禁用日志记录）

ENABLE_CRASH_REPORTING

显示名称：启用崩溃报告

此属性启用或禁用使用 XenMobile 应用程序的 Crashlytics 的崩溃报告。

可能的值：**true** 或 **false**

默认值：**false**

ENABLE_CREDENTIAL_STORE

显示名称：启用凭据存储区

启用凭据存储区意味着 Android 或 iOS 用户在访问 XenMobile 应用程序时输入一次其密码。可以使用凭据存储区，无论是否启用 Citrix PIN。如果不启用 Citrix PIN，用户输入其 Active Directory 密码。XenMobile 只对 Secure Hub 和公共应用商店应用程序支持将 Active Directory 密码用于凭据存储区。如果您将 Active Directory 密码用于凭据存储区，XenMobile 不支持 PKI 身份验证。

要在 Secure Mail 中自动注册，需要将此属性设置为 **true**。

要配置此自定义客户端策略，请转至设置 > 客户端属性，添加自定义键 **ENABLE_CREDENTIAL_STORE**，并将值设置为 **true**。

ENABLE_FIPS_MODE

显示名称：启用 FIPS 模式

此属性在移动设备上启用或禁用 FIPS 模式。更改此值后，Secure Hub 会在执行下一次联机身份验证时将新值传递到设备。

可能的值：**true** 或 **false**

默认值：**false**

ENABLE_NETWORK_EXTENSION

显示名称：ENABLE_NETWORK_EXTENSION

默认情况下，XenMobile 在 Secure Hub 安装时启用 Apple 网络扩展框架。要禁用网络扩展，请转至**设置 > 客户端属性**，添加自定义键 **ENABLE_NETWORK_EXTENSION** 并将值设置为 **false**。

默认值：**true**

ENABLE_PASSCODE_AUTH

显示名称：启用 Citrix PIN 身份验证

此属性允许您打开 Citrix PIN 功能。启用 Citrix PIN 或通行码后，系统将提示用户定义要使用的 PIN（而非其 Active Directory 密码）。如果启用了 ENABLE_PASSWORD_CACHING，或者如果 XenMobile 使用证书身份验证，此设置将自动启用。

如果用户执行脱机身份验证，Citrix 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，Citrix 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。

此属性允许在移动设备本地缓存用户的 Active Directory 密码。将此属性设置为 **true** 时，还必须将 ENABLE_PASSCODE_AUTH 属性设置为 **true**。如果启用了用户密码缓存，XenMobile 将提示用户设置 Citrix PIN 或通行码。

可能的值：**true** 或 **false**

默认值：**false**

ENABLE_TOUCH_ID_AUTH

显示名称：启用 Touch ID 身份验证

对于支持 Touch ID 身份验证的设备，此属性将在设备上启用或禁用 Touch ID 身份验证。要求：

用户设备必须启用 Citrix PIN 或 LDAP。如果 LDAP 身份验证处于关闭状态（例如，因为使用了仅基于证书的身份验证），则用户必须设置 Citrix PIN。在这种情况下，XenMobile 要求使用 Citrix PIN，即使客户端属性 **ENABLE_PASSCODE_AUTH** 为 **false** 也是如此。

将 **ENABLE_PASSCODE_AUTH** 设置为 **false**，以使用户启动应用程序时，他们必须响应提示以使用 Touch ID。

可能的值：**true** 或 **false**

默认值：**false**

ENABLE_WORXHOME_CEIP

显示名称：启用 Worx Home CEIP

此属性将打开客户体验改善计划。这样会定期向 Citrix 发送匿名配置和使用数据。此数据可帮助 Citrix 改善 XenMobile 的品质、可靠性和性能。

值：**true** 或 **false**

默认值：**false**

ENABLE_WORXHOME_GA

显示名称：在 Worx Home 中启用 Google Analytics

此属性启用或禁用在工作区中使用 Google Analytics 收集数据的功能。更改此设置时，仅当用户下次登录 Secure Hub (Worx Home) 时才设置新值。

可能的值：**true** 或 **false**

默认值：**true**

ENCRYPT_SECRETS_USING_PASSCODE

显示名称：使用通行码加密机密

此属性允许将敏感数据存储在移动设备上的 Secret Vault 中（而非基于平台的本机存储中），例如 iOS 钥匙串。此属性允许您使用强加密的密钥，但还会添加用户熵（用户生成的只有自己知道的随机 PIN 代码）。

Citrix 建议您启用此属性以帮助提高用户设备的安全性。因此，用户将遇到多个要求输入 Citrix PIN 的身份验证提示。

可能的值：**true** 或 **false**

默认值：**false**

INACTIVITY_TIMER

显示名称：不活动计时器

此属性定义用户可以保持其设备处于不活动状态且之后访问应用程序不会提示输入 Citrix PIN 或通行码的时间（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 Secure Hub 以执行完全身份验证。更改此设置时，该值将在系统下次提示用户进行身份验证时生效。

注意：在 iOS 上，不活动计时器还将管理 MDX 应用程序和非 MDX 应用程序对 Secure Hub 的访问。

可能的值：任意正整数

默认值：**15**

ON_FAILURE_USE_EMAIL

显示名称：失败时使用电子邮件向 IT 技术支持人员发送设备日志

此属性启用或禁用使用电子邮件向 IT 发送设备日志的功能。

可能的值：**true** 或 **false**

默认值：**true**

PASSCODE_EXPIRY

显示名称：PIN 更改要求

此属性定义 Citrix PIN 或通行码的有效时间（单位为天），超过此时间后，系统将强制用户更改其 Citrix PIN 或通行码。更改此设置时，仅当用户的当前 Citrix PIN 或通行码过期时才设置新值。

可能的值：**1** - 建议使用 **99**。如果希望用户永远不需要重置其 PIN 代码，请将该值设置为一个非常大的值（例如 100000000000）。如果最初设置的过期期限介于 1 到 99 天之间，然后在该时间段内更改为更大的数值，PIN 在初始期限结束时仍会过期，但之后永不过期。

默认值：**90**

PASSCODE_HISTORY

显示名称：PIN 历史记录

此属性定义之前使用的 Citrix PIN 或通行码的数量，用户在更改其 Citrix PIN 或通行码时不能重用。如果更改此设置，用户下次重置其 Citrix PIN 或通行码时将设置新值。

可能的值：**1** - **99**

默认值：**5**

PASSCODE_MAX_ATTEMPTS

显示名称：PIN 尝试次数

此属性定义用户可以尝试输入错误 Citrix PIN 或通行码的次数，之后系统将提示用户进行完全身份验证。用户成功执行完全身份验证后，系统将提示其创建新 Citrix PIN 或通行码。

可能的值：任意正整数

默认值：**15**

PASSCODE_MIN_LENGTH

显示名称：PIN 长度要求

此属性定义 Citrix PIN 的最小长度。

可能的值：**1** - **99**

默认值：**6**

PASSCODE_STRENGTH

显示名称：PIN 强度要求

此属性定义 Citrix PIN 或通行码的强度。更改此设置时，系统将在下次提示用户进行身份验证时提示其设置新 Citrix 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 PASSCODE_TYPE 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~
高	与“中”Citrix PIN 通行码强度相同。	通行码应该至少包含一个大写字母和一个小写字母。 不允许：abcd12、DFGH2 允许：Abcd12、jkrtA2、23Bc#、AbCd
强	与“中”Citrix PIN 通行码强度相同。	通行码至少应包括一个数字、一个特殊符号、一个大写字母以及一个小写字母。 不允许使用：abcd12、Abcd12、dfgh12、jkrtA2 允许使用：Abcd1#、Ab123~、xY12#3、Car12#、AAbc1#

PASSCODE_TYPE

显示名称：PIN 类型

此属性定义用户能够定义数字型 Citrix PIN 还是字母数字型通行码。选择**数字**时，用户只能定义数字 (Citrix PIN)。选择**字母数字**时，用户可以使用字母和数字的组合 (通行码)。

注意：更改此设置时，用户必须在系统下次提示进行身份验证时设置新 Citrix PIN 或通行码。

可能的值：**数字或字母数字**

默认值：**数字**

REFRESHINTERVAL

显示名称：REFRESHINTERVAL

默认情况下，XenMobile 每隔 3 天会对自动发现服务器 (ADS) 执行 ping 命令查找固定证书。要更改刷新时间间隔，请转至**设置 > 客户端属性**，添加自定义键 **REFRESHINTERVAL**，并将值设置为小时数。

默认值：**72 小时 (3 天)**

SEND_LDAP_ATTRIBUTES

对于仅 MAM 部署，可以配置 XenMobile，以便使用电子邮件凭据在 Secure Hub 中注册的 Android 或 iOS 设备用户能够自动注册 Secure Mail。这意味着用户无需输入额外的信息或执行额外的步骤即可注册 Secure Mail。

要配置此全局客户端策略，请转至**设置 > 客户端属性**，添加自定义键 **SEND_LDAP_ATTRIBUTES**，并按如下所示设置值。

值：`userPrincipalName=${user.userprincipalname},sAMAccountName=${user.samaccountname},displayName=${user.displayName},mail=${user.mail}`

与 MDM 策略类似，属性值会指定为宏。

以下示例介绍了帐户服务如何响应此属性：

注意：对于此属性，XenMobile 会将逗号字符视为字符串终止符。因此，如果属性值包含逗号，则必须在逗号前面加上反斜杠，以防止客户端将嵌入的逗号视为属性值的结尾。反斜杠字符表示为“\”。

ActiveSync Gateway

Feb 27, 2017

ActiveSync 是 Microsoft 开发的移动数据同步协议。ActiveSync 与手持设备和台式（便携式）计算机同步数据。

可以在 XenMobile 中配置 ActiveSync Gateway 规则。根据这些规则，可以允许或拒绝设备访问 ActiveSync 数据。例如，如果激活“缺少必备应用程序”规则，XenMobile 将检查应用程序访问策略中是否存在必备应用程序，如果缺少必备应用程序，则会拒绝对 ActiveSync 数据的访问。对于每个规则，可以选择**允许**或**拒绝**。默认设置为**允许**。

有关应用程序访问设备策略的详细信息，请参阅[应用程序访问设备策略](#)。

XenMobile 支持以下规则：

匿名设备：检查设备是否处于匿名模式。如果在设备尝试重新连接时 XenMobile 无法重新对用户进行身份验证，则可以执行此检查。

Samsung KNOX 认证失败：检查设备是否无法通过 Samsung KNOX 认证服务器的查询。

禁止的应用程序：检查设备是否具有应用程序访问策略中定义的禁止的应用程序。

隐式允许和拒绝：此操作是 ActiveSync Gateway 的默认操作。网关创建不满足其他任何过滤器规则条件的所有设备的设备列表，并根据该列表允许或拒绝连接。如果任何规则均不匹配，则默认规则为“隐式允许”。

不活动设备：按照“服务器属性”中“Device Inactivity Days Threshold”（设备不活动天数阈值）设置的定义，检查设备是否处于不活动状态。

缺少必备应用程序：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：检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码：检查用户密码是否合规。在 iOS 和 Android 设备上，XenMobile 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。例如，在 iOS 设备上，如果 XenMobile 向该设备发送了通行码策略，则用户可在 60 分钟内设置密码。在用户设置密码之前，通行码可能不合规。

不合规设备：根据“不合规”设备属性检查设备是否不合规。该属性通常由自动化操作进行更改，或由第三方利用 XenMobile API 进行更改。

吊销状态：检查设备证书是否已吊销。再次授权之前，已吊销的设备无法重新注册。

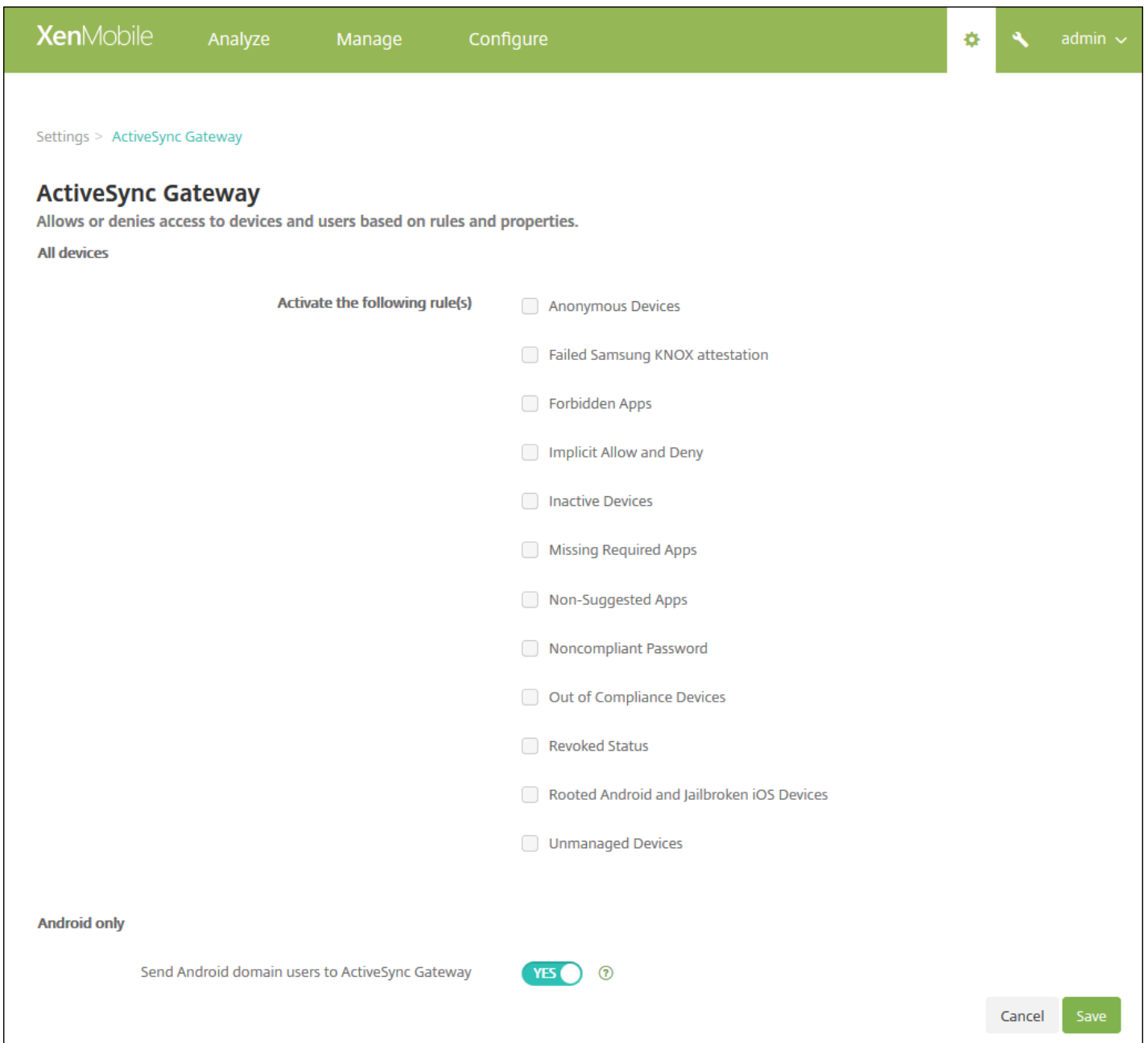
已获得 root 权限的 Android 设备和已越狱的 iOS 设备：检查 Android 设备或 iOS 设备是否已越狱。

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

将 Android 域用户发送到 ActiveSync Gateway：单击是**可**确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。

配置 ActiveSync Gateway 设置

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示**设置**页面。
2. 在**服务器**下面，单击 **ActiveSync Gateway**。此时将显示 **ActiveSync Gateway** 页面。



3. 在激活以下规则中，选择要激活的一个或多个规则。

4. 在仅限 **Android** 中的将 **Android** 域用户发送到 **ActiveSync Gateway** 中，单击是 以确保 XenMobile 将 Android 设备信息发送到 ActiveSync Gateway。

5. 单击保存。

网络访问控制

Feb 27, 2017

如果已在网络中设置了网络访问控制 (NAC) 设备 (如 Cisco ISE) , 则在 XenMobile 中, 可以启用过滤器以根据规则或属性设置设备的 NAC 兼容性。如果 XenMobile 中的托管设备不满足指定条件, 并因此被标记为“不合规”, NAC 设备将在您的网络中阻止该设备。

在 XenMobile 控制台中, 从列表选择一个或多个条件, 以将设备设为“不合规”。

XenMobile 支持以下 NAC 合规性过滤器:

匿名设备: 检查设备是否处于匿名模式。如果在设备尝试重新连接时 XenMobile 无法重新对用户进行身份验证, 则可以执行此检查。

Samsung KNOX 认证失败: 检查设备是否无法通过 Samsung KNOX 认证服务器的查询。

禁止的应用程序: 检查设备是否具有应用程序访问策略中定义的禁止的应用程序。有关应用程序访问策略的详细信息, 请参阅[应用程序访问设备策略](#)。

不活动设备: 按照“服务器属性”中“Device Inactivity Days Threshold” (设备不活动天数阈值) 设置的定义, 检查设备是否处于不活动状态。有关详细信息, 请参阅[服务器属性](#)。

缺少必备应用程序: 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: 检查设备是否具有应用程序访问策略中定义的非推荐应用程序。

不合规密码: 检查用户密码是否合规。在 iOS 和 Android 设备上, XenMobile 可以确定设备上的当前密码是否符合发送到该设备的通行码策略。例如, 在 iOS 设备上, 如果 XenMobile 向该设备发送了通行码策略, 则用户可在 60 分钟内设置密码。在用户设置密码之前, 通行码可能不合规。

不合规设备: 根据“不合规”设备属性检查设备是否不合规。该属性通常由自动化操作进行更改, 或由第三方利用 XenMobile API 进行更改。

吊销状态: 检查设备证书是否已吊销。再次授权之前, 已吊销的设备无法重新注册。

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

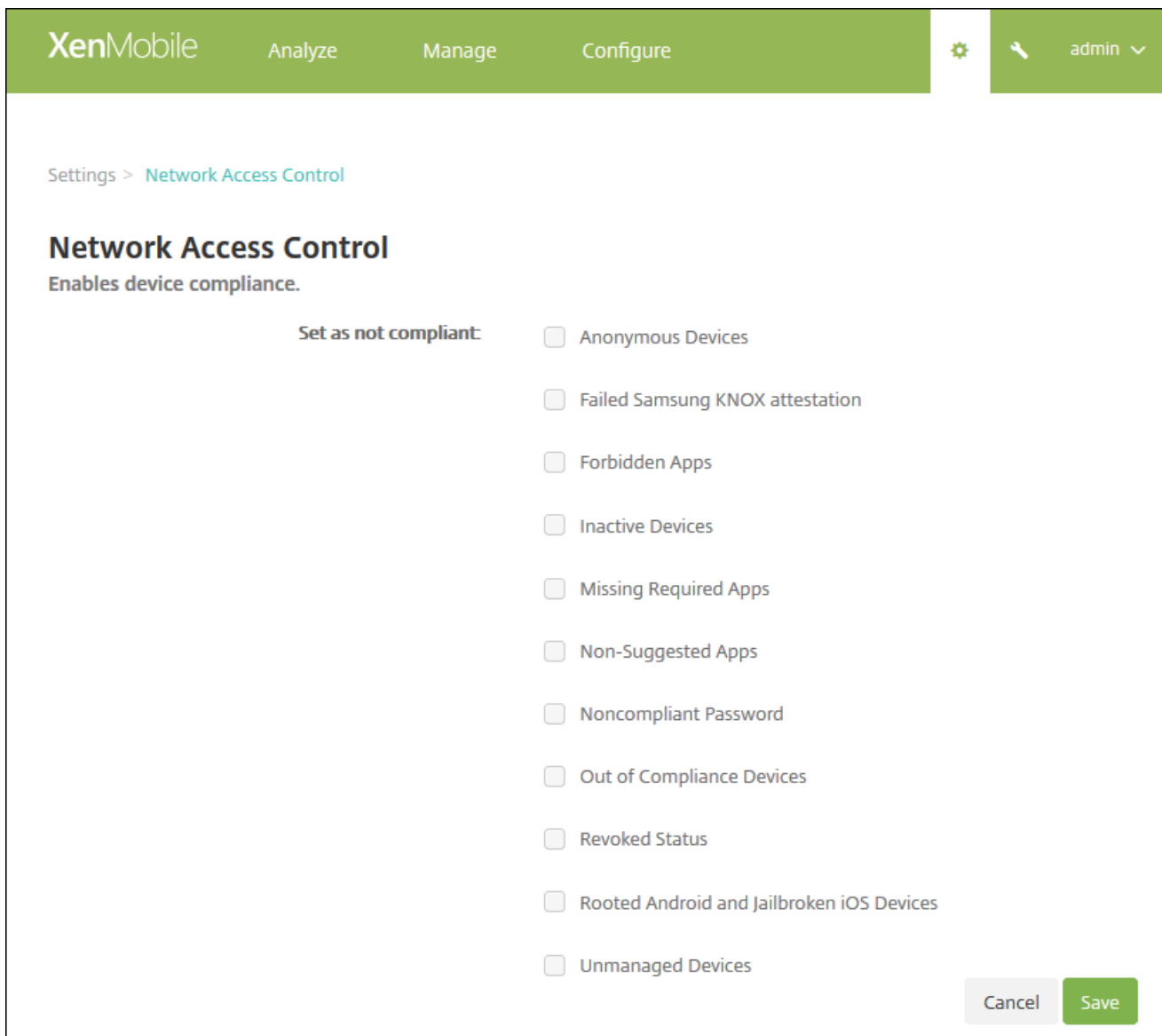
非托管设备: 检查设备是否仍处于托管状态, 受 XenMobile 控制。例如, 在 MAM 模式下运行的设备或已取消注册的设备为非托管设备。

注意

“隐式合规/不合规”过滤器仅在由 XenMobile 托管的设备上设置默认值。例如, 任何已安装黑名单应用程序的设备或未注册的设备都将被标记为“不合规”, 并会被 NAC 设备阻止在您的网络外。

配置网络访问控制

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在服务器下方，单击网络访问控制。此时将显示网络访问控制页面。



3. 选中要启用的设为不合规过滤器旁边的复选框。
4. 单击保存。

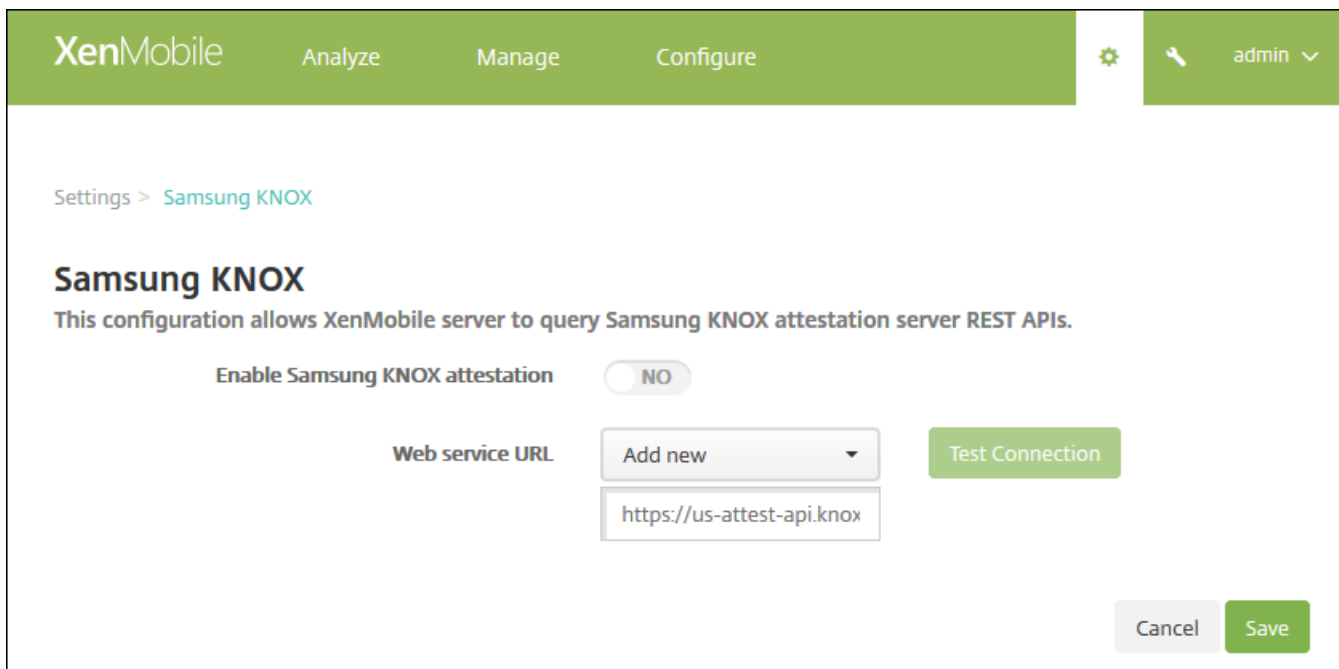
Samsung KNOX

Feb 27, 2017

可以配置 XenMobile 以查询 Samsung KNOX 认证服务器 REST API。

Samsung KNOX 利用为操作系统和应用程序提供多级别保护的硬件安全功能。其中一种安全级别驻留在通过认证的平台上。认证服务器提供移动设备的核心系统软件（例如，引导加载程序和内核）验证。该验证基于在可信引导期间收集的数据在运行时进行。

1. 在 XenMobile Web 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在平台下方，单击 **Samsung KNOX**。此时将显示 **Samsung KNOX** 页面。



The screenshot shows the XenMobile configuration interface for Samsung KNOX. At the top, there's a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs, along with a gear icon and a user profile 'admin'. The main content area is titled 'Settings > Samsung KNOX'. Below the title, there's a sub-header 'Samsung KNOX' and a descriptive sentence: 'This configuration allows XenMobile server to query Samsung KNOX attestation server REST APIs.' There are two main configuration options: 'Enable Samsung KNOX attestation' with a toggle switch currently set to 'NO', and 'Web service URL' which includes a dropdown menu with 'Add new' and a text input field containing 'https://us-attest-api.knox'. To the right of the URL field is a green 'Test Connection' button. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. 在启用 **Samsung KNOX 认证** 中，选择是否启用 Samsung KNOX 认证。默认值为否。
4. 将启用 **Samsung KNOX 认证** 设置为是时，**Web 服务 URL** 选项即被启用。然后在列表中执行以下操作之一：
 - a. 单击适当的认证服务器。
 - b. 单击**新增**，然后输入 Web 服务 URL。
5. 单击**测试连接**以验证连接性。将显示成功或失败消息。
6. 单击**保存**。

注意

可以使用 Samsung KNOX Mobile Enrollment 将多个 Samsung KNOX 设备注册到 XenMobile（或任何移动设备管理器）中，无需手动配置每个设备。有关信息，请参阅 [Samsung KNOX 批量注册](#)。

Firebase Cloud Messaging

Feb 28, 2017

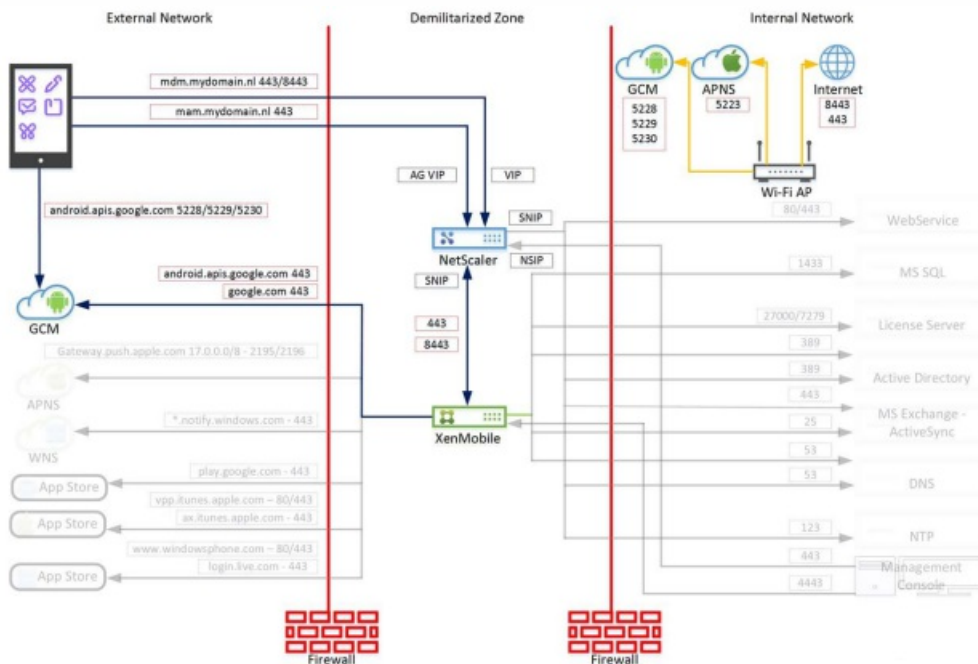
作为策略活动轮询期限的备选策略，可以使用 Firebase Cloud Messaging (GCM) 控制 Android 设备如何以及何时连接到 XenMobile。通过使用以下配置，任何安全操作或部署命令都将触发推送通知，以提示用户重新连接到 XenMobile 服务器。

必备条件

- XenMobile 10.3.x
- 最新版本 Secure Hub 客户端
- Google 开发人员帐户凭据
- 在 XenMobile 上打开指向 `android.apis.google.com` 和 `google.com` 的端口 443

体系结构

此图显示了外部和内部网络中 FCM 的通信流。



为 GCM 配置 Google 帐户

1. 使用您的 Google 开发人员帐户凭据登录以下 URL：

<https://console.firebase.google.com/?pli=1>

2. 单击 **Create a project**（创建项目）。

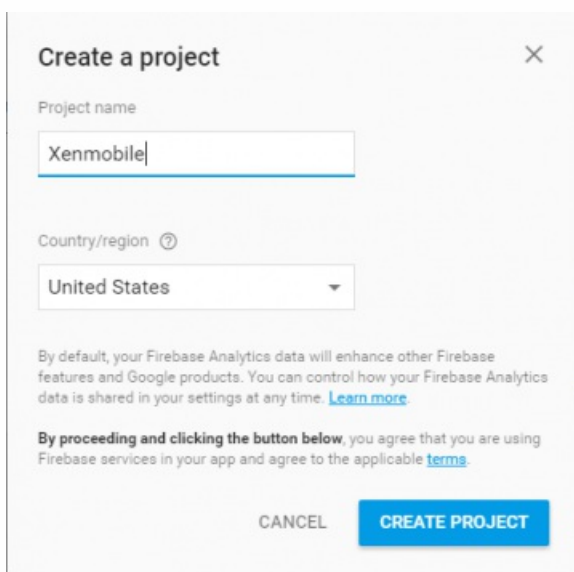
Welcome to Firebase

Tools from Google for developing great apps, engaging with your users and earning more through mobile ads. [Learn more](#)

CREATE NEW PROJECT

[or import a Google project](#)

- 键入 **Project name** (项目名称) , 然后单击 **Create** (创建) 。



Create a project [X]

Project name
Xenmobile

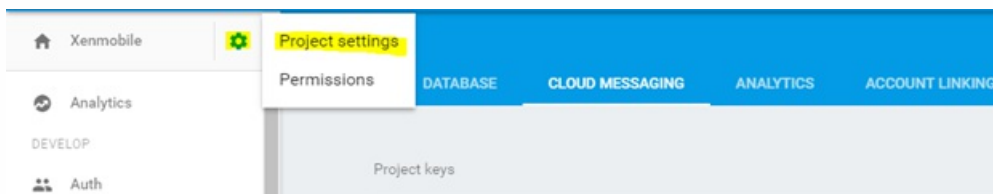
Country/region ⓘ
United States

By default, your Firebase Analytics data will enhance other Firebase features and Google products. You can control how your Firebase Analytics data is shared in your settings at any time. [Learn more](#)

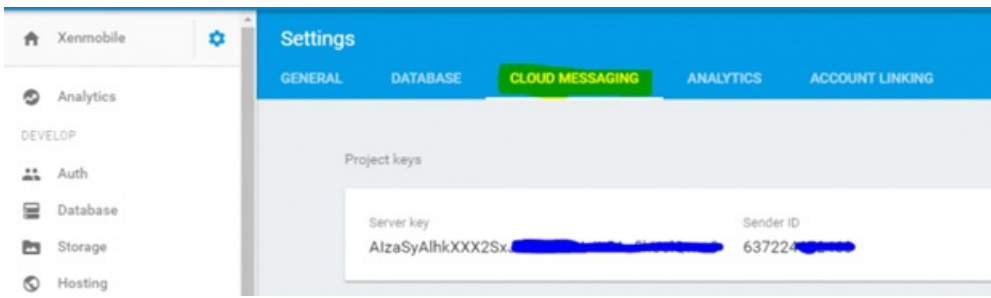
By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable [terms](#).

CANCEL CREATE PROJECT

- 单击左上角项目名称旁边的齿轮图标，然后单击 **Project Settings** (项目设置) 。

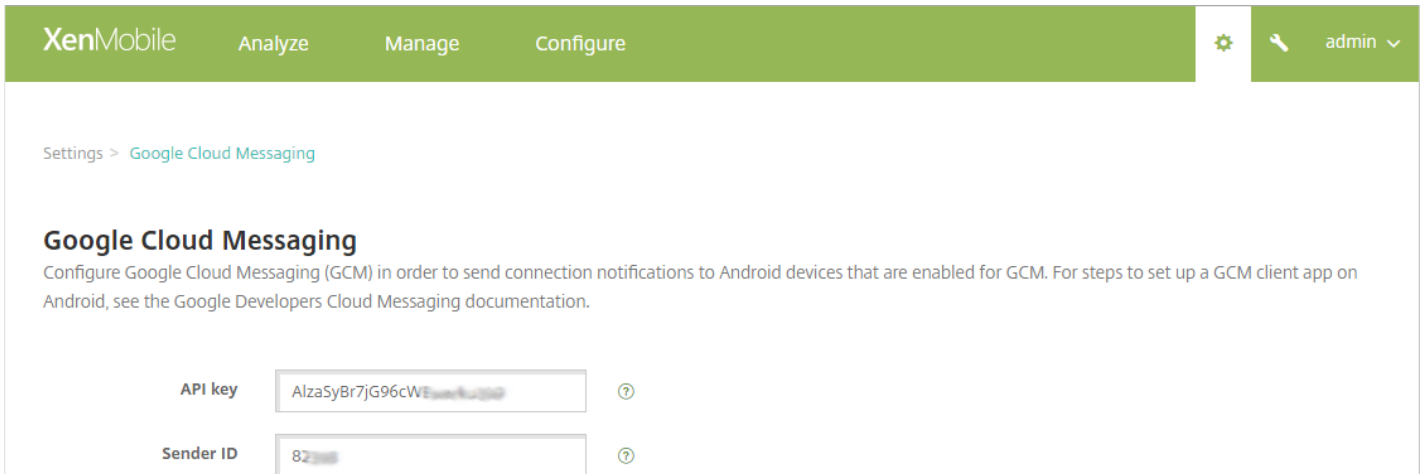


- 选择 **Cloud Messaging** 选项卡。可以在此页面上查找发件人 ID 和服务器密钥。复制这些值，因为必须在 XenMobile 服务器中提供它们。请务必注意，必须在 Firebase 控制台中创建 2016 年 9 月之后创建的任何服务器密钥。



为 GCM 配置 XenMobile

1. 登录 XenMobile 控制台，然后单击 **设置 > 服务器属性**。在搜索栏中，键入 **GCM** 并单击“搜索”。
 - a. 编辑 **GCM API 密钥**，并键入在 Firebase Cloud Messaging 配置的最后一步中复制的 Firebase Cloud Messaging API 密钥。
 - b. 编辑 **GCM 发件人 ID**，并键入在前一个步骤中记录的发件人 ID 值。



测试您的配置

作为测试 FCM 配置的先决条件，不配置计划策略。此外，请勿将该策略设置为 **Always Connect**（始终连接）。有关配置 **Scheduling**（计划）策略的详细信息，请参阅 [Scheduling device policy](#)（“计划”设备策略）。

1. 注册 Android 设备。
2. 保持设备在一段时间内处于空闲状态，以使其与 XenMobile 服务器断开连接。
3. 登录 XenMobile 管理员控制台，单击 **管理**，选择 Android 设备，然后单击 **安全**。

XenMobile Analyze **Manage** Configure administrator

Devices Users Enrollment Invitations

Devices Show filter

Add Edit Secure Notify Delete Import Export Refresh

<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered	Activation
<input checked="" type="checkbox"/>		MDM MAM		Android	6.0.1	Nexus 9	07/27/2016 06:05:25 pm	2 days	No	

4. 在设备操作下，单击选择性擦除。

Security Actions ×

Device Actions ⏶

Revoke Lock **Selective Wipe** Full Wipe

Locate

成功配置后，即可在设备上执行选择性擦除。

Google Play 凭据

Feb 27, 2017

XenMobile 使用 Google Play 凭据为设备提取应用程序信息。

要查找 Android ID，请在您的手机上输入 `***#8255***`。如果代码在您的设备类型中不显示设备 ID，可以使用第三方应用程序派生设备 ID。要获取的 ID 为带有 GSF ID 标签的 Google Services Framework ID。

注意

在 XenMobile 控制台中搜索 Google Play 应用商店应用程序时，搜索操作会根据设备上安装的 Android 操作系统返回应用程序。例如，Samsung S6 Edge 运行操作系统版本 6.0.1。搜索应用程序时，搜索结果中显示的唯一应用程序为与 Android 6.0.1 兼容的应用程序。

Important

要启用 XenMobile 来提取应用程序信息，可能需要将 Gmail 帐户配置为允许非安全连接。有关步骤的信息，请参阅 [Google 支持站点](#)。

1. 在 XenMobile 控制台中，单击右上角的齿轮图标。此时将显示设置页面。
2. 在平台下方，单击 **Google Play 凭据**。此时将显示 Google Play 凭据页面。

The screenshot shows the XenMobile interface with a green header bar containing 'XenMobile', 'Analyze', 'Manage', and 'Configure'. On the right, there is a gear icon and a user profile 'admin'. Below the header, the breadcrumb 'Settings > Google Play Credentials' is visible. The main heading is 'Google Play Credentials'. A message states: 'XenMobile cannot extract app information without logon information. To find your Android ID, you can type ***#8255*** on your phone.' There are three input fields: 'User name*' with the value '@gmail.com', 'Password*' with masked characters, and 'Device ID*' with the value '123456789123CD01'. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. 配置以下设置：

- 用户名：键入与 Google Play 帐户关联的名称。
- 密码：键入用户密码。

- **设备 ID**：键入 Android ID。

请参阅本文前面的注意部分，了解有关获取 Android ID 的步骤。

3. 单击保存。

设备策略

Jul 13, 2017

可以通过创建策略，配置 XenMobile 与您的设备的交互方式。尽管很多策略对所有设备通用，但是每种设备均具有一组特定于其操作系统的策略。因此，您可能会发现平台之间的差异，甚至 Android 设备的不同制造商之间的差异。

有关按平台列表的策略，请下载 [Device Policies by Platform Matrix PDF](#)（设备策略（按平台）列表PDF）有关每个设备策略的摘要说明，请参阅本文中的[设备策略摘要](#)。

Important

在创建策略之前，请完成以下要求：

- 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. 为一个或多个平台配置策略。
3. 创建部署规则（可选）。
4. 将策略分配到交付组。
5. 配置部署计划（可选）。

要创建和管理设备策略，请转到[配置 > 设备策略](#)。

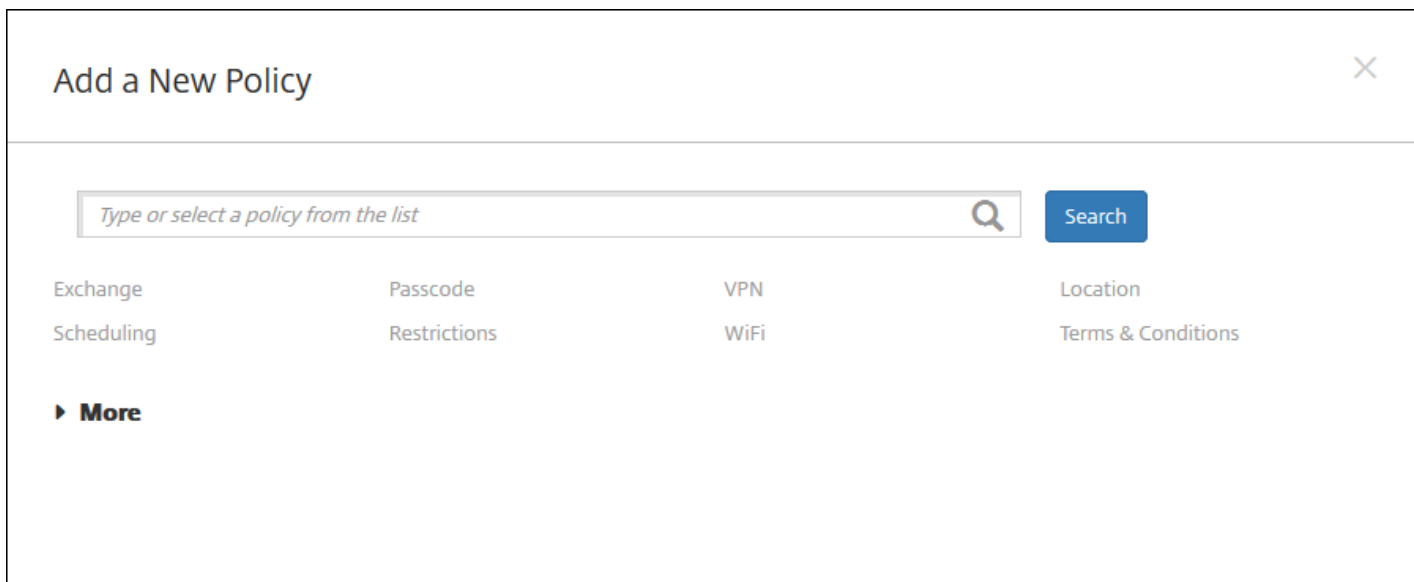
The screenshot shows the XenMobile web interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, with sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' tab is selected, displaying a list of policies. The list has columns for 'Policy name', 'Type', 'Created on', 'Last updated on', and 'Status'. There are four policies listed: MBWifi, Passcode, Restrictions, and Personal Hotspot. Each policy has a checkbox in the first column. Below the list, it says 'Showing 1 - 4 of 4 items'. There are also 'Add' and 'Export' buttons above the table.

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status
<input type="checkbox"/>	MBWifi	Wifi	10/26/15 1:03 PM	10/26/15 1:03 PM	
<input type="checkbox"/>	Passcode	Password	10/29/15 8:33 AM	10/29/15 8:33 AM	
<input type="checkbox"/>	Restrictions	Restrictions	10/29/15 8:34 AM	10/29/15 8:34 AM	
<input type="checkbox"/>	Personal Hotspot	Personal Hotspot	10/29/15 8:35 AM	10/29/15 8:35 AM	

添加设备策略

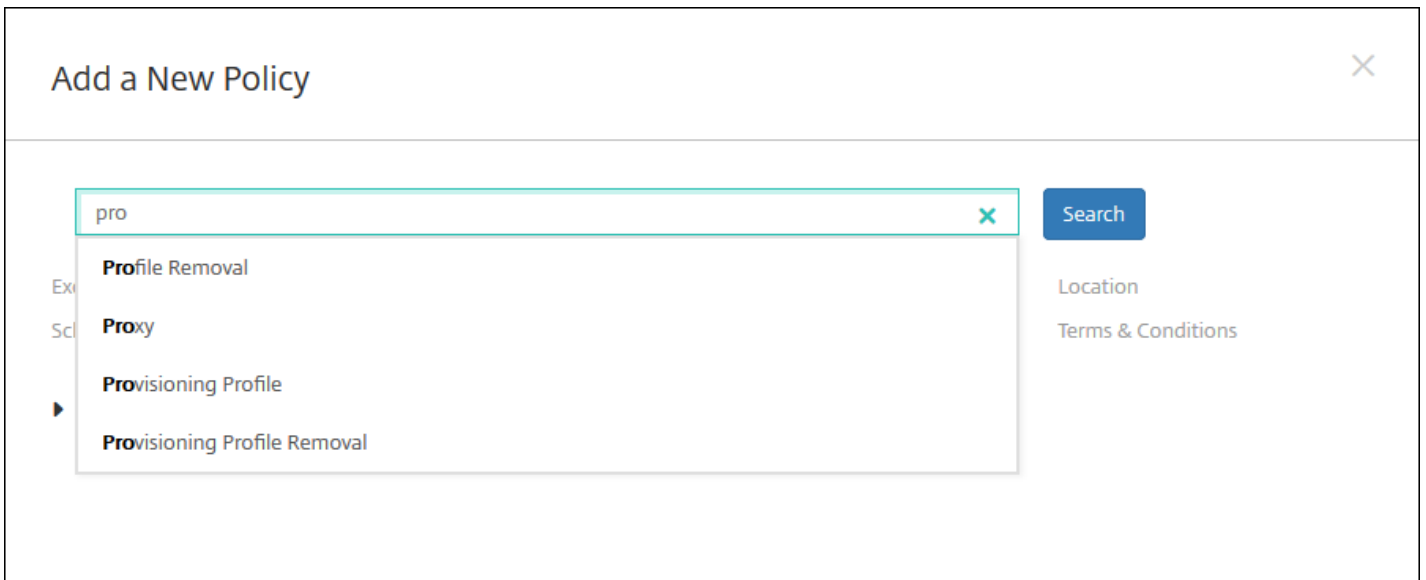
1. 在设备策略页面上，单击添加。

此时将显示添加新策略对话框。展开更多以查看更多策略。



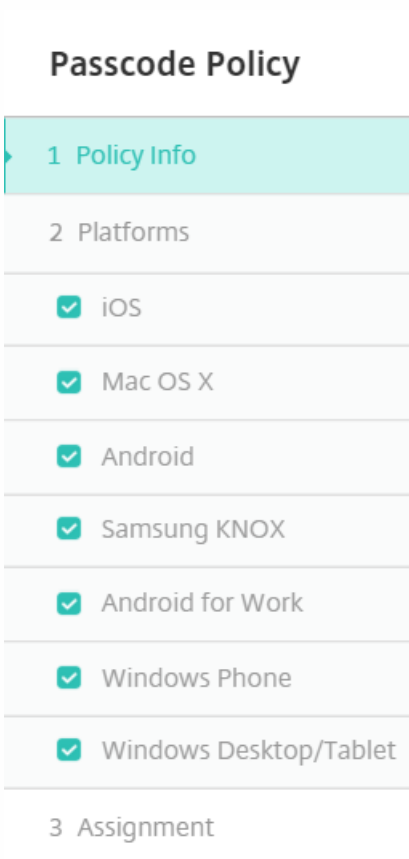
2. 查找要添加的策略，执行以下操作之一：

- 单击策略。
此时将显示所选策略的策略信息页面。
- 在搜索框中键入策略的名称。随着键入，将显示可能的匹配项。如果列表中存在您的策略，请单击此策略。只有选中的策略保留在结果中。单击此策略以打开其策略信息页面。
如果选定的策略位于 **More**（更多）区域中，则只有展开 **More**（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。策略可能会因平台而异。并非所有策略都

适用于所有平台。

配置部署规则：

注意：有关配置部署规则的详细信息，请参阅[部署资源](#)。

a. 展开部署规则，然后配置以下设置。默认情况下将显示基础选项卡。

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

b. 单击高级选项卡以使用布尔选项组合规则。此时将显示您在基础选项卡上选择的条件。

c. 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。
- 在列表中，选择要添加到规则的条件。然后单击右侧的加号 (+) 向规则添加条件。

您随时可以通过单击选择某个条件，然后单击编辑以更改此条件或单击删除以删除此条件。

- 单击新建规则添加其他条件。

6. 单击下一步移到下一个平台页面，或者在完成所有平台页面后移到分配页面。

7. 在分配页面上，选择要应用此策略的交付组。如果单击某个交付组，此组将显示在用于接收应用程序分配的交付组框中。

注意：用于接收应用程序分配的交付组您选择某个交付组之后才显示。

Passcode Policy ✕

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Choose delivery groups

- AllUsers
- sales

Delivery groups to receive app assignment

- AllUsers

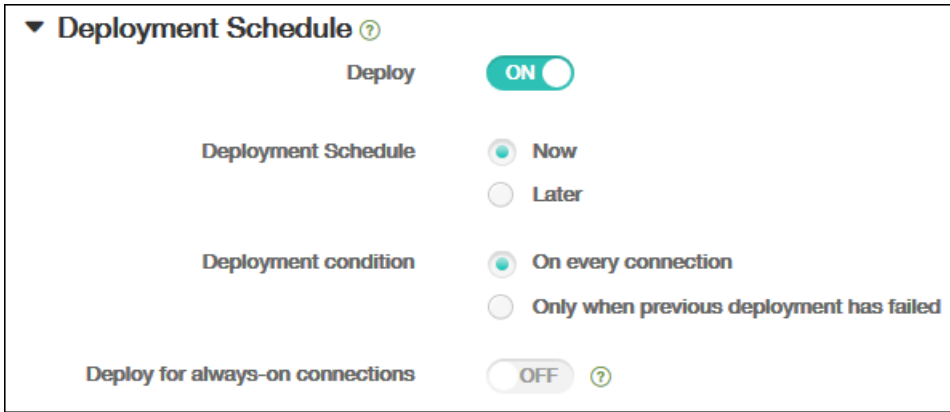
8. 在分配页面上，展开部署计划，然后配置以下设置：

- 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。
- 在部署计划旁边，单击立即或稍后。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。



The screenshot shows a configuration panel titled "Deployment Schedule" with a help icon. It contains four settings:

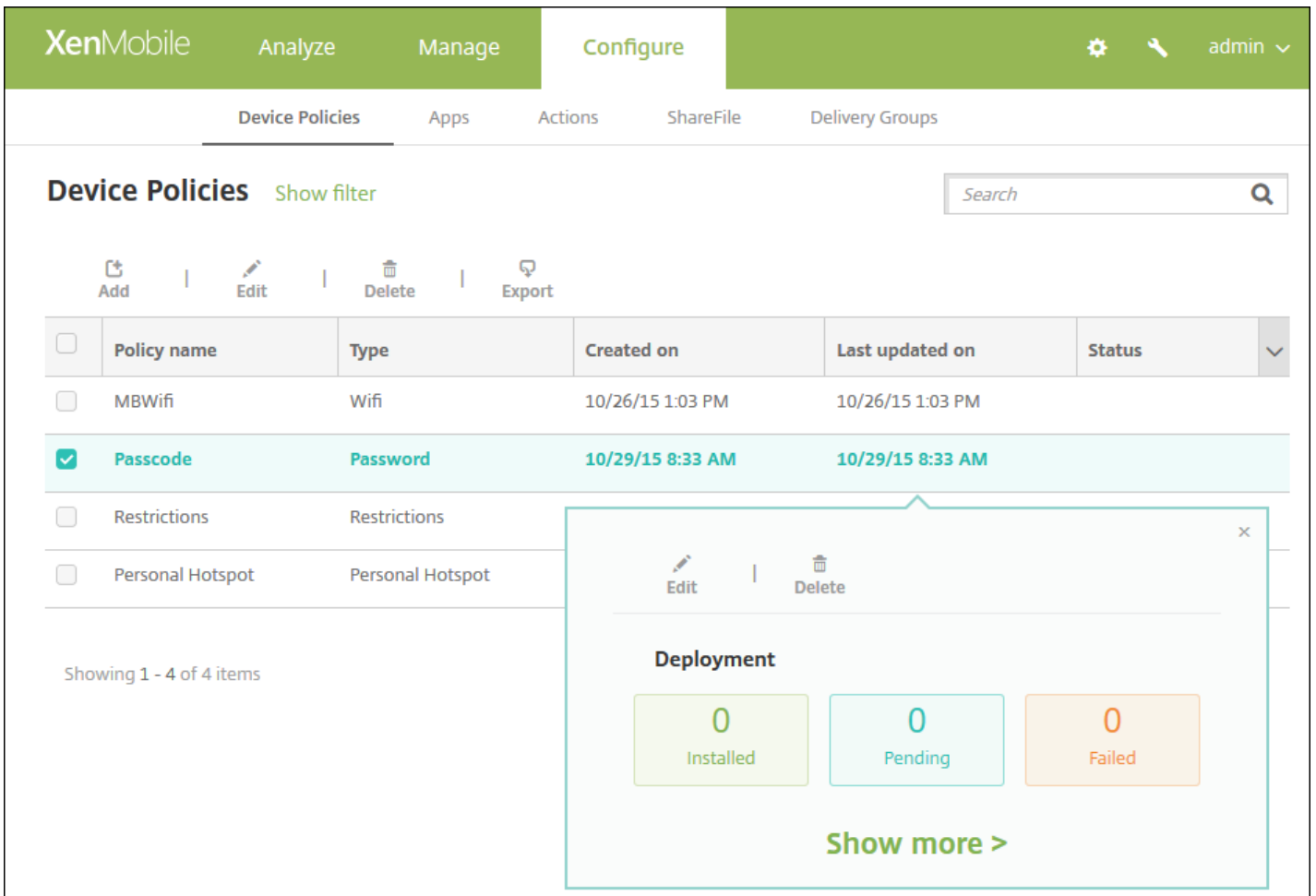
- Deploy**: A toggle switch set to "ON".
- Deployment Schedule**: Radio buttons for "Now" (selected) and "Later".
- Deployment condition**: Radio buttons for "On every connection" (selected) and "Only when previous deployment has failed".
- Deploy for always-on connections**: A toggle switch set to "OFF" with a help icon.

9. 单击保存。

该策略显示在设备策略表中。

编辑或删除设备策略

要编辑或删除某个策略，请选中策略旁边的复选框，以在策略列表上方显示选项菜单。或者单击列表中的某个策略，以在此列表右侧显示选项菜单。



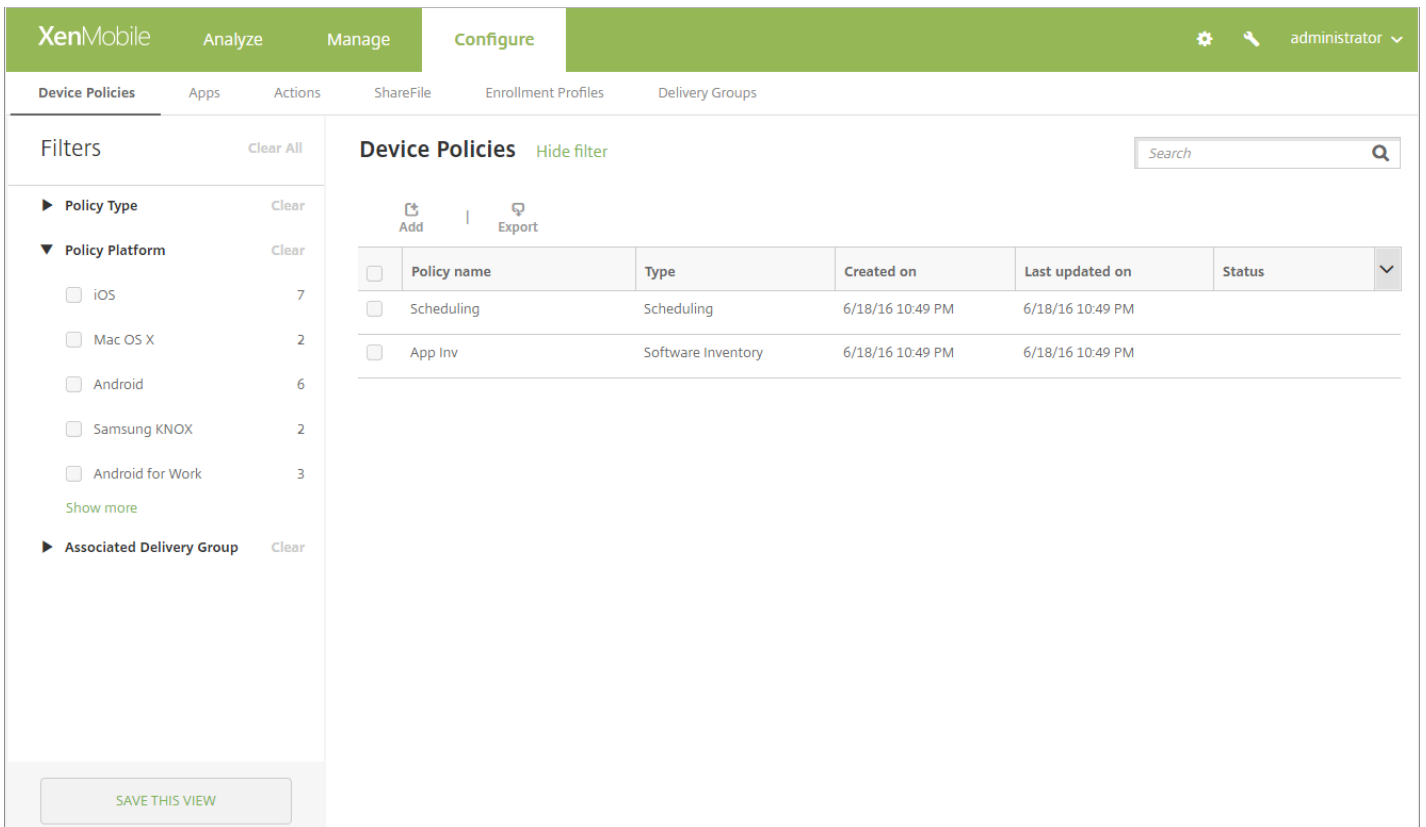
要查看策略详细信息，请单击**显示更多**。

要编辑某个设备策略的所有设置，请单击**编辑**。

如果单击**删除**，将显示确认对话框。再次单击**删除**。

过滤已添加的设备策略列表

可以按策略类型、平台和关联的交付组过滤已添加的策略列表。在**配置 > 设备策略**页面中，单击**显示过滤器**。在列表中，选择您要查看的项对应的复选框。



单击**保存此视图**以保存过滤器。之后过滤器的名称显示在**保存此视图**按钮下面的一个按钮中。

设备策略摘要

设备策略名称	设备策略说明
AirPlay 镜像	此策略用于将特定 AirPlay 设备（如 Apple 电视或其他 Mac 计算机）添加到 iOS 设备。您还可以将设备添加到受监督设备的白名单，从而使用户仅限于白名单上的 AirPlay 设备。
AirPrint	此策略允许您向 iOS 设备上的 AirPrint 打印机列表添加 AirPrint 打印机。通过此策略可以更加轻松地为用户提供支持。适用于 iOS 7.0 及更高版本。 注意：请确保知道每个打印机的 IP 地址和资源路径。
Android for Work 应用程序限制	此策略允许您更改与 Android 应用程序关联的限制，但是在更改前，必须满足以下必备条件： <ul style="list-style-type: none"> 在 Google 上完成 Android 设置任务。有关详细信息，请参见 Android at Work。 将 Android 应用程序添加到 XenMobile。有关详细信息，请参阅 添加公共应用商店应用程序。
APN	如果贵组织不使用使用者 APN 从移动设备连接到 Internet，可以使用此策略。此策略用于确定将设备连接到特定电话运营商的通用分组无线服务 (GPRS) 所使用的设置。大多数新式电话中已经定义此设置。

应用程序访问	<p>此策略允许您定义以下应用程序列表：</p> <ul style="list-style-type: none"> ● 需要安装在设备上的应用程序 ● 或者，可以安装在设备上的应用程序 ● 或者，不得安装在设备上的应用程序 <p>然后，可以创建自动化操作，以使设备符合此应用程序列表。</p>
应用程序属性	<p>此策略允许您为 iOS 设备指定各种属性，例如托管应用程序捆绑包 ID 或“为应用单独设置 VPN”标识符。</p>
应用程序配置	<p>此策略允许您远程为支持托管配置的应用程序配置各种设置和行为。为此，您要将 XML 配置文件（称为属性列表或 plist）部署到 iOS 设备。或者，将键/值对部署到 Windows 10 手机、台式机或平板电脑设备。</p>
应用程序清单	<p>此策略允许您收集托管设备上的应用程序清单。之后 XenMobile 将清单与部署到这些设备的任何应用程序访问策略进行比较。这样一来，便可以检测应用程序黑名单或白名单上的应用程序，然后采取相应操作。</p>
应用程序锁定	<p>此策略定义用户可以在设备上运行或无法在设备上运行的应用程序列表。</p> <p>可以同时为 iOS 和 Android 设备配置此策略，但策略的执行方式则因平台而异。例如，不能阻止在 iOS 设备上运行多个应用程序</p> <p>应用程序锁定策略适用于大多数 Android L 和 M 的设备。但是，应用程序锁定策略不适用于 Android N 或更高版本的设备，因为 Google 弃用了所需的 API。</p> <p>对于 iOS 设备，每个策略只能选择一个 iOS 应用程序。因此，用户只能使用其设备运行单个应用程序。在强制执行应用程序锁定策略时，用户无法在设备上执行除您明确允许的选项之外的任何其他活动。</p>
应用程序网络使用	<p>此策略用于设置网络使用规则，以指定 iOS 设备上托管应用程序使用网络（如手机网络数据网络）的方式。规则仅适用于托管应用程序。托管应用程序是指您通过 XenMobile 部署到用户设备的应用程序。托管应用程序不包括这些应用程序：</p> <ul style="list-style-type: none"> ● 用户直接下载到其设备的应用程序。即，应用程序不是通过 XenMobile 部署的。 ● 在 XenMobile 中注册设备时，设备上已安装的应用程序。
应用程序限制	<p>此策略用于创建您要阻止用户在 Samsung KNOX 设备上安装的应用程序的黑名单。您还可以创建您要允许用户安装的应用程序的白名单。</p>
应用程序卸载	<p>此策略允许您出于以下几种原因从用户设备中删除应用程序。例如，您可能不希望支持某些应用程序。或者，您的公司可能希望将现有应用程序替换为不同供应商提供的类似应用程序。当此策略部署到用户设备时，应用程序被删除。用户会收到卸载应用程序的提示，但 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。</p>

应用程序卸载限制	此策略允许您指定用户可以或无法卸载的应用程序。
浏览器	此策略允许您定义用户设备是否可以使用浏览器或设备可以使用的浏览器功能。在 Samsung 设备上，可以禁用浏览器，也可以启用或禁用弹出消息、JavaScript、Cookie、自动填充以及是否强制显示欺诈警告。
日历(CalDav)	此策略用于将日历 (CalDAV) 帐户添加到 iOS 或 Mac OS X 设备。使用 CalDAV 帐户，用户可以将计划数据与支持 CalDAV 的任何服务器同步。
手机网络	该策略允许您配置手机网络设置。
连接管理器	此策略用于为自动连接到 Internet 和专用网络的应用程序指定连接设置。此策略仅适用于 Windows Pocket PC。
联系人 (CardDAV)	此策略用于将 iOS 联系人 (CardDAV) 帐户添加到 iOS 或 Mac OS X 设备。使用 CardDAV 帐户，用户可以将联系人数据与支持 CardDAV 的任何服务器同步。
将应用程序复制到 Samsung 容器	此策略用于将已安装在设备上的应用程序复制到受支持的 Samsung 设备上的 SEAMS 或 KNOX 容器。复制到 SEAMS 容器的应用程序显示在设备主屏幕上。复制到 KNOX 容器的应用程序仅当用户登录 KNOX 容器时可用。
凭据	<p>此策略用于支持使用 XenMobile 中的 PKI 配置进行集成身份验证。例如，使用 PKI 实体、密钥库、凭据提供程序或服务证书。有关凭据的信息，请参阅证书和身份验证。</p> <p>每种设备平台都需要一组不同的值，“凭据策略”一文将对此进行介绍。</p>
自定义 XML	<p>此策略用于自定义以下功能：</p> <ul style="list-style-type: none"> • 置备，例如配置设备以及启用或禁用功能 • 设备配置，例如允许用户更改设置和设备参数 • 软件升级，例如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，例如接收来自设备的错误和状态报告 <p>可以在 Windows 中使用 Open Mobile Alliance Device Management (OMA DM) API 创建自己的自定义 XML 配置。本主题中不介绍如何使用 OMA DM API。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。</p>
Defender	此策略用于配置适用于台式机和平板电脑的 Windows 10 的 Windows Defender 设置。
删除文件和文件夹	此策略用于从 Windows Mobile/CE 设备中删除特定的文件或文件夹。

删除注册表项和值	此策略用于从 Windows Mobile/CE 设备中删除特定的注册表项和值。
设备运行状况证明	<p>此策略需要 Windows 10 设备报告其运行状况的状态。为此，它们向 Health Attestation Service (HAS) 发送特定数据和运行时信息以供分析。HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 XenMobile。XenMobile 收到运行状况证明证书后，根据该证书的内容，部署您设置的自动操作。</p> <p>有关详细信息，请参阅 Microsoft Device HealthAttestation CSP 页面。</p>
设备名称	此策略用于对 iOS 和 Mac OS X 设备设置名称，以便您可以轻松识别设备。可以使用宏、文本或二者的组合定义设备名称。有关宏的信息，请参阅 宏 。
企业中心	<p>此面向 Windows Phone 的策略允许您通过企业中心公司应用商店分发应用程序。</p> <p>对于一种 Windows Phone Secure Hub 模式，XenMobile 仅支持一种企业中心策略。例如，不要使用不同版本的 Secure Home for XenMobile Enterprise Edition 创建多个企业中心策略。只能在设备注册过程中部署初始企业中心策略。</p>
Exchange	XenMobile 提供两个传递电子邮件的选项。可以使用此 MDM 策略为在设备上的本机电子邮件客户端启用 ActiveSync 电子邮件。或者，您可以容器化的 Secure Mail 应用程序提供 ActiveSync 电子邮件。
文件	此策略用于将为用户执行某些功能的脚本文件添加到 XenMobile。或者，您可以添加您希望 Android 设备用户能够在其设备上访问的文档文件。添加文件时，还可以指定设备上要存储该文件的目录。例如，要向 Android 用户发送一份公司文档或 .pdf 文件，请将该文件部署到设备。然后，告诉用户文件所在位置。
字体	此策略用于向 iOS 和 Mac OS X 设备添加更多字体。字体必须是 TrueType (.TTF) 字体或 OpenType (.OTF) 字体。不支持字体集合 (.TTC 或 .OTC) 。对于 iOS，此策略仅适用于 iOS 7.0 及更高版本。
主屏幕布局	此策略用于指定 iOS 9.3 及更高版本的受监督设备上的 iOS 主屏幕的应用程序和文件夹布局。
导入 iOS 和 Mac OS X 配置文件	此策略用于将 iOS 和 OS X 设备的设备配置 XML 文件导入到 XenMobile 中。此文件包含您通过使用 Apple Configurator 准备的设备安全策略和限制。有关使用 Apple Configurator 创建配置文件的详细信息，请参阅 Apple Configurator 帮助 页面。
是否需要 Kiosk	此策略用于限制应用程序在 Samsung SAFE 设备上的使用。您可以将可用应用程序限于特定的一个或多个应用程序。此策略对计划仅运行特定类型或类别的应用程序的企业设备很有用。此策略还允许您针对 Kiosk 模式选择设备主屏幕和锁屏界面墙纸使用的自定义图片。
Launcher 配置	<p>此面向 Android 设备的策略用于为 Citrix Launcher 指定以下内容：</p> <ul style="list-style-type: none"> 允许的应用程序

	<ul style="list-style-type: none"> • 用于 Citrix Launcher 图标的自定义徽标图像 • Citrix Launcher 的自定义背景图像 • 退出 Launcher 时的密码要求
LDAP	此面向 iOS 设备的策略提供有关要使用的 LDAP 服务器的信息，包括任何必要的帐户信息（例如 LDAP 主机名）。此策略还提供了一组在查询 LDAP 服务器时使用的 LDAP 搜索策略。
位置	此策略允许您在地图上对设备进行地理定位（假定该设备已为 Secure Hub 启用 GPS）。将此策略部署到设备之后，可以从 XenMobile 服务器发送定位命令。之后设备会返回其位置坐标。XenMobile 还支持地理围栏和跟踪策略。
邮件	此策略用于在 iOS 或 Mac OS X 设备上配置电子邮件帐户。
托管域	此策略用于定义应用于电子邮件和 Safari 浏览器的托管域。托管域可以控制哪些应用程序可以使用 Safari 打开从域下载的文档，从而保护企业数据。对于 iOS 8 及更高版本的受监管设备，可以指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。
MDM 选项	此策略用于在受监督的 iOS 7.0 及更高版本的手机设备上管理“查找我的 iPhone 和 iPad 激活锁”。有关将 iOS 设备置于受监督模式的步骤，请参阅 批量注册 iOS 和 macOS 设备 。
组织信息	此策略用于为 XenMobile 部署到 iOS 设备的警报消息指定组织信息。适用于 iOS 7 及更高版本。
需要通行码	此策略允许您在托管设备上强制执行 PIN 代码或密码。您可以为设备上的通行码设置复杂性和超时。
个人热点	此策略允许用户不在 WiFi 网络的范围内时连接到 Internet。用户通过其 iOS 设备上手机网络数据连接并使用个人热点功能进行连接。适用于 iOS 7.0 及更高版本。
配置文件删除	此策略用于在部署时从 iOS 或 Mac OS X 设备中删除应用程序配置文件。
置备配置文件	此策略用于指定要发送到设备的企业分发置备配置文件。在开发 iOS 企业应用程序以及为其进行代码签名时，通常会包括置备配置文件。Apple 要求应用程序的配置文件在 iOS 设备上运行。如果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。
删除置备配置文件	此策略用于删除 iOS 置备配置文件。有关置备配置文件的的信息，请参阅 置备配置文件设备策略 。
代理	此策略用于为运行 Windows Mobile/CE 和 iOS 6.0 或更高版本的设备指定全局 HTTP 代理设置。只能为每个设备部署一个全局 HTTP 代理策略。
注册表	Windows Mobile/CE 注册表存储关于应用程序、驱动器、用户首选项和配置设置的数据。此策略用于定义用于管理 Windows Mobile/CE 设备的注册表项和值。

远程支持	此策略允许您远程访问 Samsung KNOX 设备。
限制	此策略用于提供在托管设备上执行锁定和控制功能的数百种选项。限制选项示例：禁用相机或麦克风、强制执行漫游规则以及强制访问第三方服务（例如应用商店）。
漫游	此策略用于配置在 iOS 和 Windows Mobile/CE 设备上是否允许语音和数据漫游。如果禁用语音漫游，会自动禁用数据漫游。对于 iOS，此策略适用于 iOS 5.0 及更高版本的设备。
Samsung SAFE 防火墙	此策略允许您为 Samsung 设备配置防火墙设置。提供要允许设备访问或要阻止设备访问的 IP 地址、端口和主机名。还可以配置代理和代理重新路由设置。
Samsung MDM 许可证密钥	此策略用于指定内置 Samsung Enterprise License Management (ELM) 密钥，必须先将该密钥部署到设备，才能部署 SAFE 策略和限制。XenMobile 支持并扩展了 Samsung for Enterprise (SAFE) 和 Samsung KNOX 策略。
计划	此策略是必需的策略，用于使 Android 和 Windows Mobile 设备重新连接到 XenMobile 服务器以进行 MDM 管理、应用程序推送和策略部署。如果不向设备发送此策略并且未启用 Google FCM，设备将无法重新连接回服务器。
SCEP	此策略用于配置 iOS 和 Mac OS X 设备以从外部 SCEP 服务器检索证书。您还可以使用 SCEP 从连接到 XenMobile 的 PKI 向设备交付证书。为此，请在分布式模式下创建 PKI 实体和 PKI 提供程序。有关详细信息，请参阅 PKI 实体 。
SSO 帐户	此策略用于创建单点登录 (SSO) 帐户，以便用户只需登录设备一次，即可访问 XenMobile 和内部公司资源。用户无需在设备上存储任何凭据。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。此策略与 Kerberos 身份验证兼容。适用于 iOS 7.0 及更高版本。
存储加密	此策略用于对内部和外部存储进行加密。对于某些设备，此策略可防止用户在其设备上使用存储卡。
订阅日历	此策略用于将订阅日历添加到 iOS 设备上的日历列表。 www.apple.com/downloads/macosx/calendars 提供了您可以订阅的公共日历列表。 请务必先订阅某个日历，才能将其添加到用户设备上已订阅的日历列表中。
条款和条件	此策略需要用户接受贵公司控制与公司网络的连接的特定策略。当用户向 XenMobile 注册其设备时，系统会向其显示条款和条件，用户必须接受这些条款和条件才能注册其设备。拒绝这些条款和条件会取消注册过程。
通道	此策略用于提高移动应用程序的服务连续性和数据传输可靠性。应用程序通道定义移动设备应用程序的

	<p>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。</p> <p>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。然后流量被重定向到运行该应用程序的服务器。</p>
VPN	<p>此策略用于提供对使用传统 VPN 网关技术的后端系统的访问。此策略用于提供可以部署到设备的 VPN 网关连接的详细信息。XenMobile 支持多个 VPN 提供商，包括 Cisco AnyConnect、Juniper 及 Citrix VPN。如果您的 VPN 网关支持此选项，您可以将此策略链接到 CA 并按需启用 VPN。</p>
墙纸	<p>此策略用于添加 .png 或 .jpg 文件，以设置 iOS 设备锁屏界面、主屏幕或二者的墙纸。适用于 iOS 7.1.2 及更高版本。要在 iPad 和 iPhone 上使用不同的墙纸，请创建不同的墙纸策略并将其部署到相应的用户。</p>
Web 内容过滤器	<p>此策略用于过滤 iOS 设备上的 Web 内容。XenMobile 使用 Apple 自动过滤功能和您添加到白名单和黑名单的站点。仅适用于 iOS 7.0 及更高版本的受监督设备。有关将 iOS 设备置于受监督模式的信息，请参阅使用 Apple Configurator 将 iOS 设备置于受监督模式。</p>
Web 剪辑	<p>此策略用于向 Web 站点中放置快捷方式或 Web 剪辑，以使它们和应用程序一起出现在用户设备上。您可以指定自己的图标来表示 iOS、Mac OS X 和 Android 设备的 Web 剪辑。Windows 平板电脑只需要一个标签和一个 URL。</p>
WiFi	<p>此策略允许管理员将 WiFi 路由器详细信息部署到托管设备。路由器详细信息包括 SSID、身份验证数据和配置数据。</p>
Windows CE 证书	<p>此策略用于从外部 PKI 创建 Windows Mobile/CE 证书并将其交付给用户设备。有关证书和 PKI 实体的详细信息，请参阅证书和身份验证。</p>
XenMobile Store	<p>此策略用于指定 XenMobile Store Web 剪辑是否显示在用户设备的主屏幕上。</p>
XenMobile 选项	<p>此策略用于配置在从 Android 和 Windows Mobile/CE 设备连接到 XenMobile 时 Secure Hub 的行为。</p>
XenMobile 卸载	<p>此策略用于从 Android 和 Windows Mobile/CE 设备卸载 XenMobile。部署此策略时，它将从部署组中的所有设备上删除 XenMobile。</p>

设备策略（按平台）

Mar 29, 2017

要按平台查看策略，请下载 [Device Policies by Platform Matrix PDF](#)（设备策略（按平台）列表 PDF）。在 XenMobile 控制台中，可以从 [配置 > 设备策略](#) 添加和配置设备策略。

XenMobile 最新版本支持适用于以下平台的设备策略：

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Android Sony
- Samsung SAFE
- Samsung KNOX
- Samsung SEAMS
- Windows Phone 8.1
- Windows 10 Phone
- Windows 10 Desktop/Tablet
- Windows Mobile/CE

有关 XenMobile 最新版本中的支持设备的详细信息，请参阅[支持的设备平台](#)。

注意

如果您的环境配置了组策略对象 (GPO)：

为 Windows 10 配置 XenMobile 设备策略时，请记住以下规则。如果已注册的一台或多台 Windows 10 设备上的某个策略冲突，则优先应用与 GPO 对应的策略。

AirPlay 镜像设备策略

Feb 27, 2017

Apple AirPlay 功能允许用户通过 Apple 电视采用流技术将 iOS 设备中的内容无线推送到电视屏幕，或将设备上显示的内容精确显示到电视屏幕或其他 Mac 计算机上。

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

注意：继续操作前，请确保您具有要添加的所有设备的设备 ID 和任何密码。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**最终用户**下方，单击**AirPlay 镜像**。此时将显示**AirPlay 镜像策略**页面。

The screenshot shows the XenMobile configuration interface for an AirPlay Mirroring Policy. The interface is divided into several sections:

- Navigation:** XenMobile, Analyze, Manage, Configure (active), and a user profile 'admin'.
- Sub-navigation:** Device Policies (active), Apps, Actions, ShareFile, Enrollment Profiles, Delivery Groups.
- Policy Information:** A modal window titled 'Policy Information' with a close button (X). It contains the text: 'This policy lets you specify specific AirPlay devices to add to users' iOS and Mac OS X devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.'
- Form Fields:** 'Policy Name*' (text input) and 'Description' (text area).
- Platforms:** A list of platforms with checkboxes: 'iOS' (checked), 'Mac OS X' (checked).
- Assignment:** A section titled 'Assignment' is partially visible.
- Buttons:** A green 'Next >' button is located at the bottom right of the modal.

4. 在**策略信息**窗格中，输入以下信息：

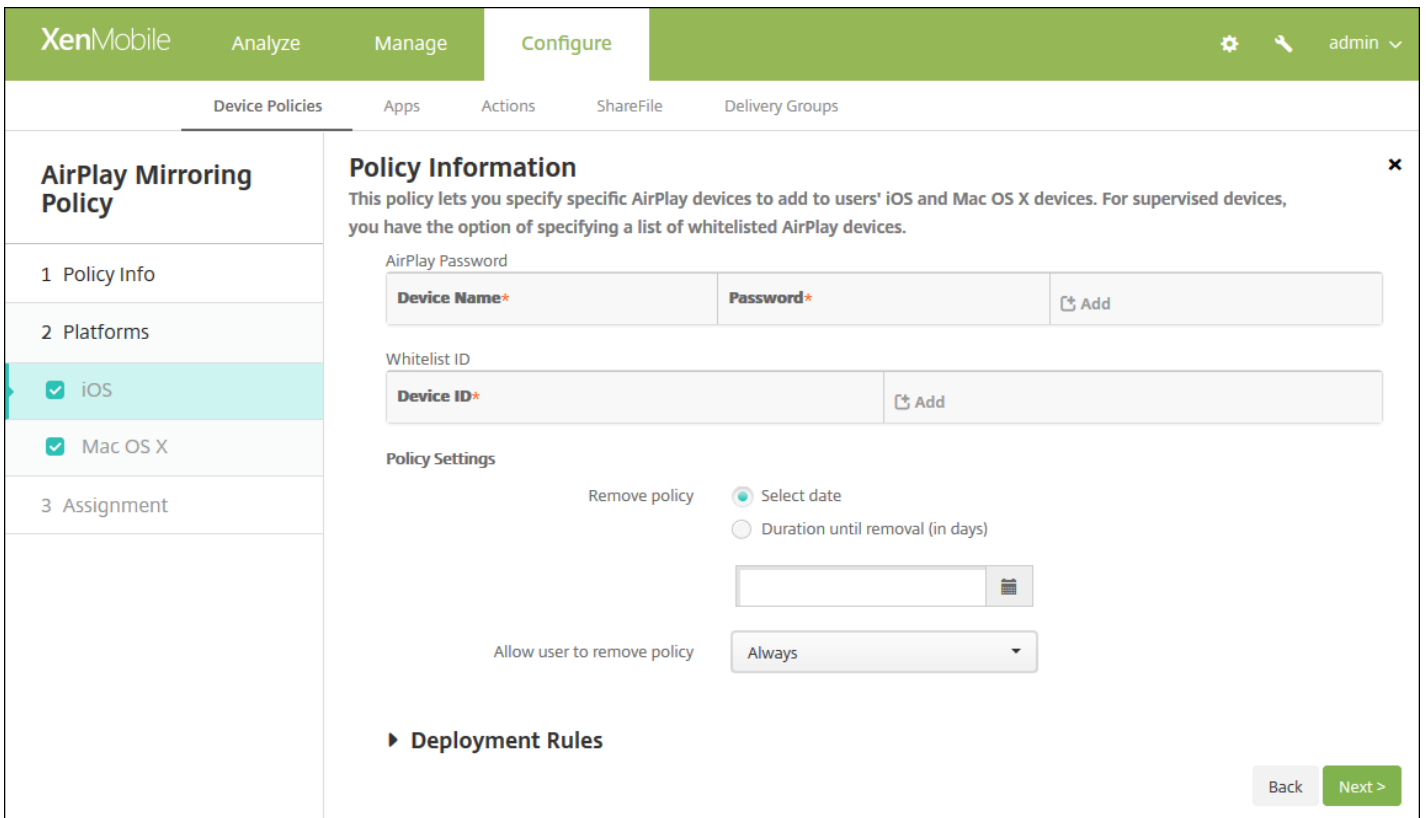
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。此时将显示**策略平台**页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置



配置以下设置：

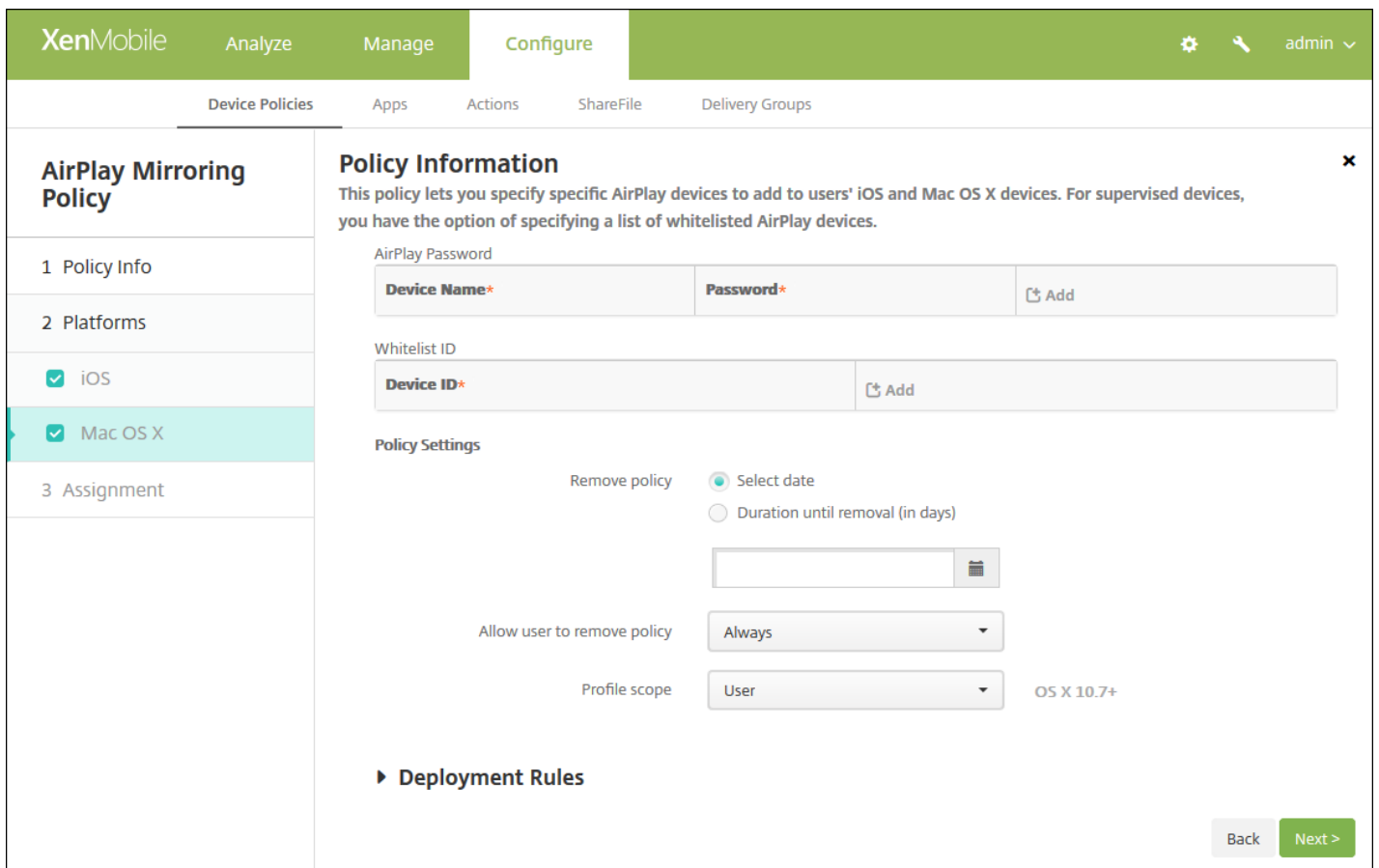
- **AirPlay 密码**：对于要添加的每个设备，单击**添加**，然后执行以下操作：
 - **设备 ID**：以 xx:xx:xx:xx:xx:xx 格式输入硬件地址（Mac 地址）。此字段不区分大小写。
 - **密码**：输入设备的可选密码。
 - 单击**添加**以添加设备，或单击**取消**以取消添加设备。
- **白名单 ID**：对于未受监督的设备，忽略此列表。此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。对于希望添加到此列表中的每个 AirPlay 设备，请单击**添加**，然后执行以下操作：
 - **设备 ID**：以 xx:xx:xx:xx:xx:xx 格式键入设备 ID。此字段不区分大小写。
 - 单击**添加**以添加设备，或单击**取消**以取消添加设备。

注意：要删除现有设备，请将鼠标悬停在包含此列表的行上，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**以保留列表。

要编辑现有设备，请将鼠标悬停在包含此列表的行上，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

配置 Mac OS X 设置



配置以下设置：

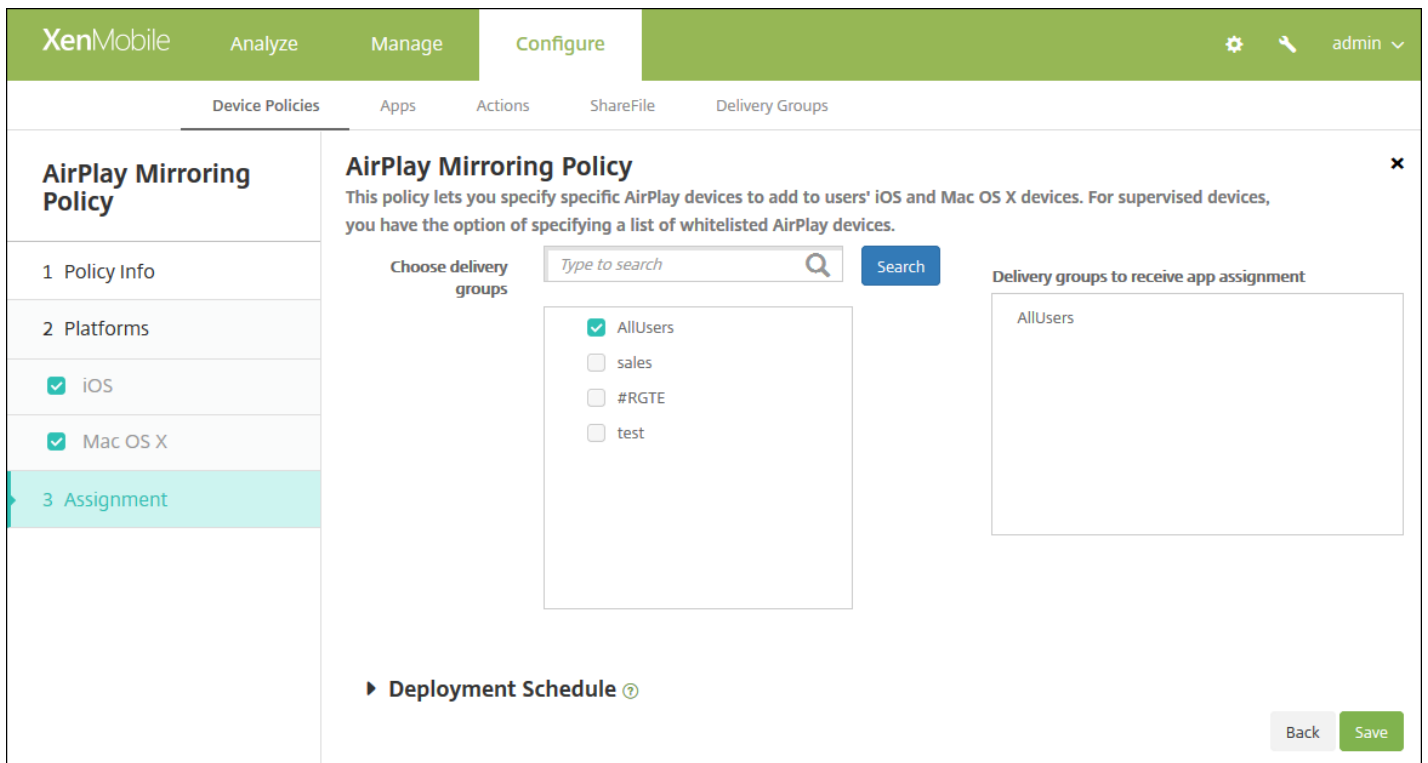
- **AirPlay 密码：**对于要添加的每个设备，单击**添加**，然后执行以下操作：
 - **设备 ID：**以 xx:xx:xx:xx:xx:xx 格式输入硬件地址（Mac 地址）。此字段不区分大小写。
 - **密码：**输入设备的可选密码。
 - 单击**添加**以添加设备，或单击**取消**以取消添加设备。
- **白名单 ID：**对于未受监督的设备，忽略此列表。此列表中的设备 ID 仅包括可用于用户设备的 AirPlay 设备。对于希望添加到此列表中的每个 AirPlay 设备，请单击**添加**，然后执行以下操作：
 - **设备 ID：**以 xx:xx:xx:xx:xx:xx 格式键入设备 ID。此字段不区分大小写。
 - 单击**添加**以添加设备，或单击**取消**以取消添加设备。

注意：要删除现有设备，请将鼠标悬停在包含此列表的行上，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**以保留列表。

要编辑现有设备，请将鼠标悬停在包含此列表的行上，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。
 - 在**配置文件作用域**旁边，单击**用户**或**系统**。默认值为**用户**。

8. 单击下一步。此时将显示 **AirPlay 镜像策略分配** 页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所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。

AirPrint 设备策略

Feb 27, 2017

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。通过此策略可以更加轻松地为用户提供支持。

注意：

- 此策略适用于 iOS 7.0 及更高版本。
- 请确保知道每个打印机的 IP 地址和资源路径。

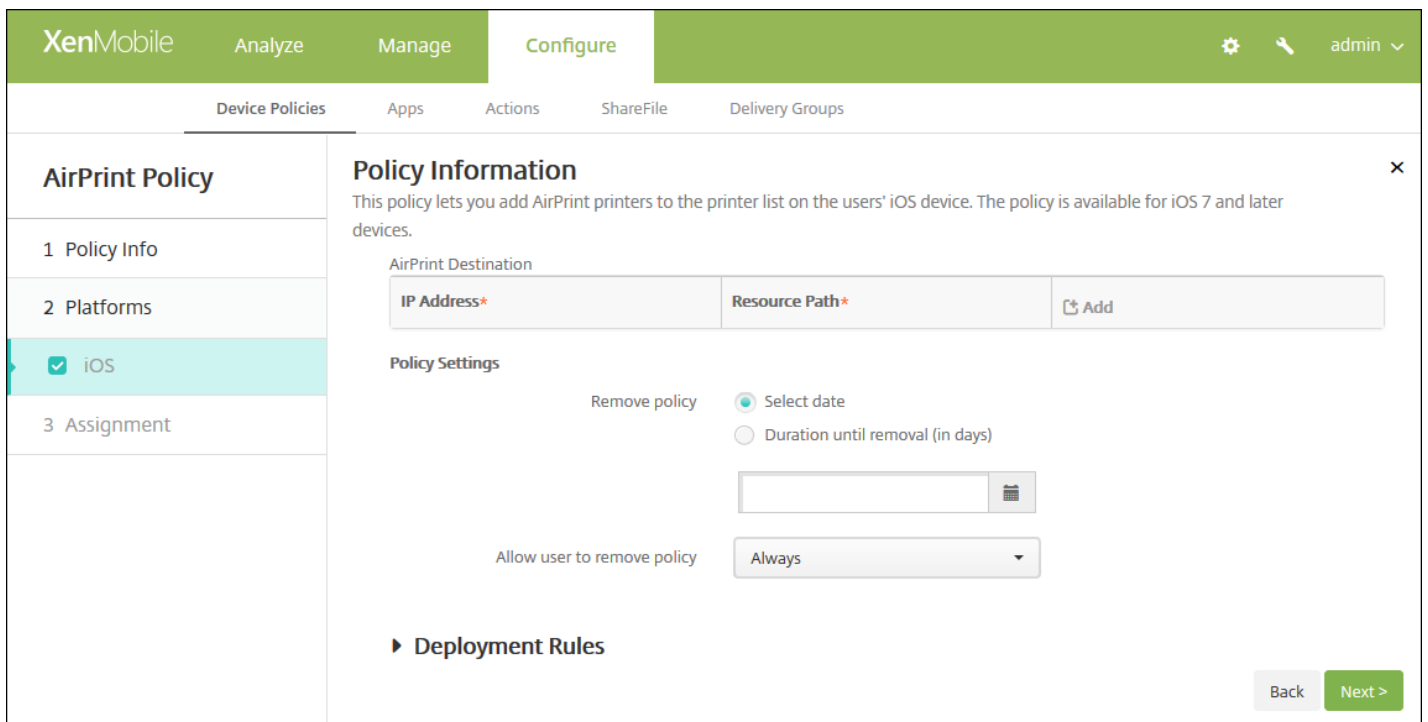
1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 单击更多，然后在最终用户下面，单击 **AirPrint**。此时将显示 **AirPrint** 策略页面。

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'AirPrint Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you add AirPrint printers to the printer list on the users' iOS device. The policy is available for iOS 7 and later devices.' Below the description are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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. 配置以下设置：

- **AirPrint 目标**：对于您要添加的各个 AirPrint 目标，单击**添加**，然后执行以下操作：
 - **IP 地址**：输入 AirPrint 打印机 IP 地址。
 - **资源路径**：输入与打印机关联的资源路径。此值与 _ipps.tcp Bonjour 记录的参数相对应。例如，printers/Canon_MG5300_series 或 printers/Xerox_Phaser_7600。
 - 单击**保存**以添加打印机，或单击**取消**以取消添加打印机。

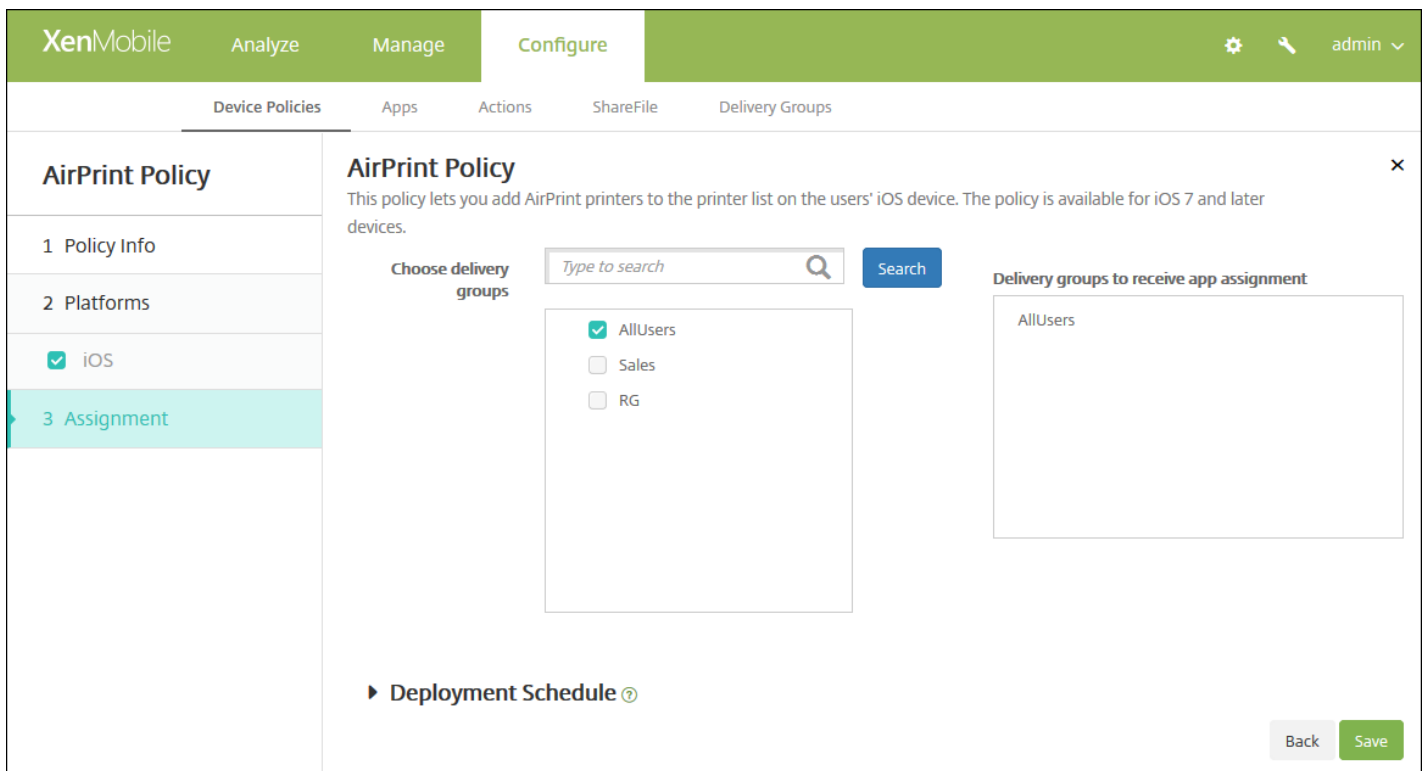
注意：要删除现有打印机，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击“删除”以删除列表，或单击“取消”以保留列表。

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。对列表进行任何更改，然后单击保存以保存更改后的列表，或单击取消以保持列表不变。

- **策略设置**
 - 在**策略设置**下方的**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**删除密码**旁边，键入必需的密码。

7. 配置部署规则

8. 单击下一步。此时将显示 **AirPrint 策略分配** 页面。



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**。

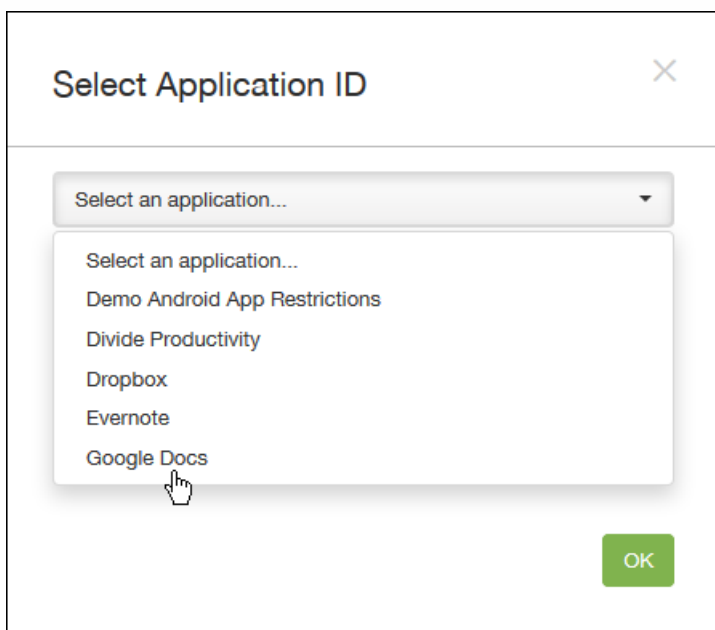
Android for Work 应用程序限制策略

Feb 27, 2017

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：

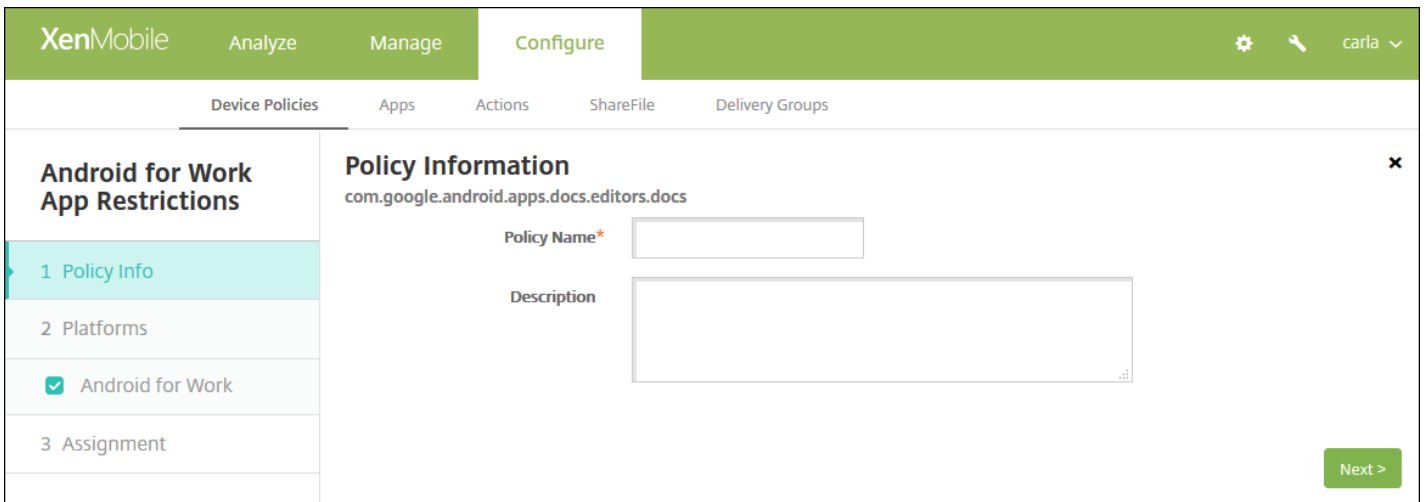
- 在 Google 上完成 Android for Work 设置任务。有关详细信息，请参阅[使用 Android for Work 管理设备](#)。
- 创建 Android for Work 帐户。有关详细信息，请参阅[创建 Android for Work 帐户](#)。
- 将 Android for Work 应用程序添加到 XenMobile。有关详细信息，请参阅[向 XenMobile 添加应用程序](#)。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加添加新策略。此时将显示添加新策略页面。
3. 展开更多，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**。

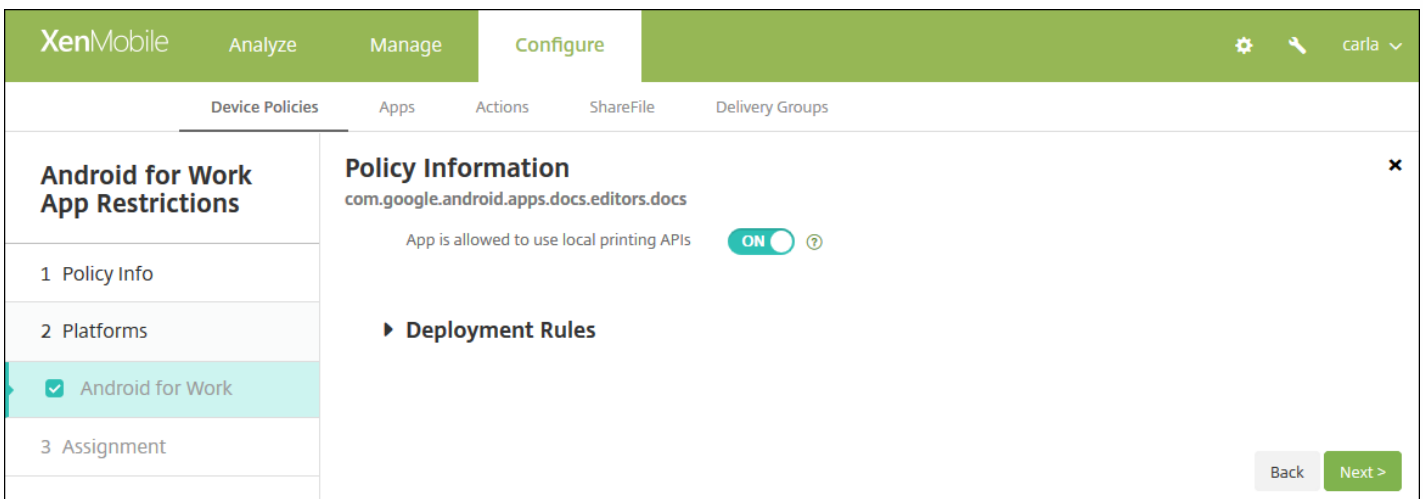
- 如果没有要添加到 XenMobile 中的 Android for Work 应用程序，将无法继续操作。有关向 XenMobile 添加应用程序的详细信息，请参阅[向 XenMobile 添加应用程序](#)。
- 如果应用程序没有关联任何限制，将显示有关相关影响的通知。单击**确定**取消对话框。
- 如果应用程序具有与之关联的限制，将显示 **Android for Work 应用程序限制策略** 信息页面。



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。

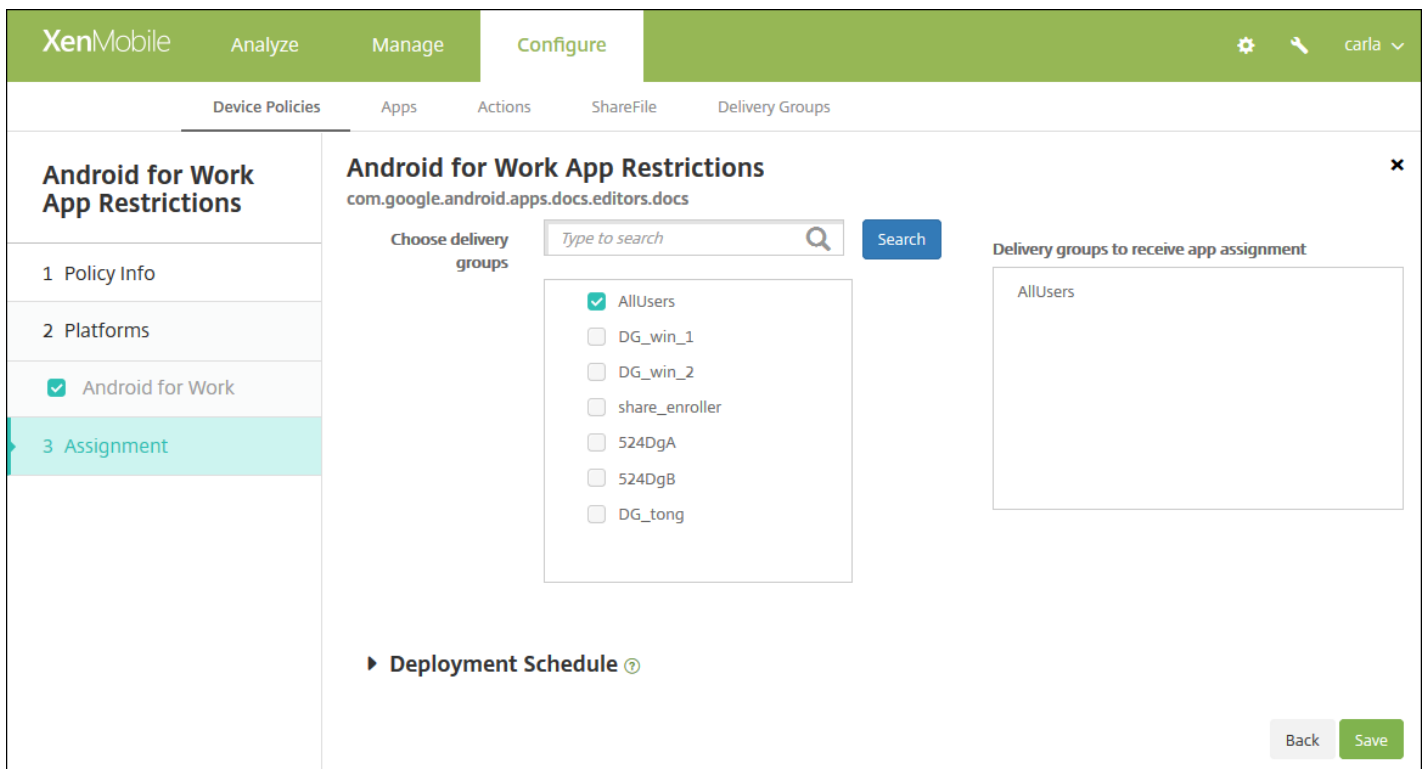
6. 单击下一步。此时将显示 **Android for Work** 平台页面。



7. 为选择的应用程序配置设置。显示的设置取决于与所选应用程序关联的限制。

8. 配置部署规则

9. 单击下一步。此时将显示 **Android for Work** 应用程序限制策略分配页面。



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

11. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用。

12. 单击保存。

APN 设备策略

Feb 27, 2017

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

[iOS 设置](#)

[Android 设置](#)

[Windows Mobile/CE 设置](#)

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**更多**，然后在**网络访问权限**下方，单击**APN**。此时将显示**APN 策略**信息页面。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'APN Policy' and contains a 'Policy Information' section. This section has a text input field for 'Policy Name*' and a larger text area for 'Description'. A note explains that this policy creates a custom APN on the device. On the left, a sidebar shows a navigation menu with 'APN Policy' selected, and sub-items '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing checkboxes for 'iOS', 'Android', and 'Windows Mobile/CE', all of which are checked. A 'Next >' button is visible in the bottom right corner of the 'Policy Information' section.

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. 在平台下方，选择要添加的平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

The screenshot shows the XenMobile configuration interface for an APN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'APN Policy' configuration steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS', 'Android', and 'Windows Mobile/CE' are all checked. The main content area is titled 'Policy Information' and contains the following fields and settings:

- APN***: A text input field with a calendar icon.
- User name**: A text input field.
- Password**: A text input field with a password icon.
- Server proxy address**: A text input field.
- Server proxy port**: A text input field.
- Policy Settings**:
 - Remove policy**: Two radio buttons: 'Select date' (selected) and 'Duration until removal (in days)'. Below the second option is a date picker.
 - Allow user to remove policy**: A dropdown menu currently set to 'Always'.
- Deployment Rules**: A section header with a right-pointing arrow.

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **APN**：键入接入点的名称。此信息必须与接受的某个 iOS APN 匹配，否则策略将失败。
- **用户名**：该字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- **密码**：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- **服务器代理地址**：APN 代理的 IP 地址或 URL。
- **服务器代理端口**：APN 代理的端口号。如果已输入服务器代理地址，则此字段为必填字段。
- 在**策略设置**下方的**删除策略**旁边，单击**选择日期**或**删除前保留时间(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**删除密码**旁边，键入必需的密码。

配置 Android 设置

The screenshot shows the XenMobile configuration interface for an APN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar is titled 'APN Policy' and has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS', 'Android', and 'Windows Mobile/CE' are listed with checkboxes, all of which are checked. The main content area is titled 'Policy Information' and contains a description: 'This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.' Below the description are several input fields: 'APN*' (with a help icon), 'User name', 'Password' (with a password icon), 'Server', 'APN type', 'Authentication type' (a dropdown menu currently set to 'None'), 'Server proxy address', 'Server proxy port', 'MMSC', 'Multimedia Messaging Server (MMS) proxy address', and 'MMS port'. At the bottom of the main area, there is a section for 'Deployment Rules' and two buttons: 'Back' and 'Next >'.

配置以下设置：

- **APN**：键入接入点的名称。此信息必须与接受的某个 Android APN 匹配，否则策略将失败。
- **用户名**：该字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- **密码**：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。
- **服务器**：此设置在智能手机之前出现，通常为空白。它是指无法访问或显示标准 Web 站点的手机的无线应用协议 (WAP) 网关服务器。
- **APN 类型**：此设置必须匹配运营商的接入点用途。它是 APN 服务说明符的逗号分隔字符串，必须与无线运营商的发布定义匹配。示例包括：
 - *。所有流量均通过此接入点。
 - mms。多媒体流量通过此接入点。
 - default（默认）。包括多媒体在内的所有流量均通过此接入点。
 - supl。与 GPS 关联的安全用户层面定位 (Secure User Plane Location)
 - dun。拨号网络已经过时，很少使用。
 - hipri。高优先级网络。
 - fota。无线固件升级用于接收固件更新。
- **身份验证类型**：在列表中，单击要使用的身份验证类型。默认值为“无”。
- **服务器代理地址**：运营商的 APN HTTP 代理的 IP 地址或 URL。
- **服务器代理端口**：APN 代理的端口号。如果已输入服务器代理地址，则此字段为必填字段。

- **MMSC**：运营商提供的 MMS 网关服务器地址。
- **多媒体消息服务器(MMS)代理地址**：指 MMS 通信的多媒体消息服务服务器。MMS 使得 SMS 可以发送包含多媒体内容（如图片或视频）的大型消息。这些服务器需要特定的协议（如 MM1、... MM11）。
- **MMS 端口**：用于 MMS 代理的端口。

配置 Windows Mobile/CE 设置

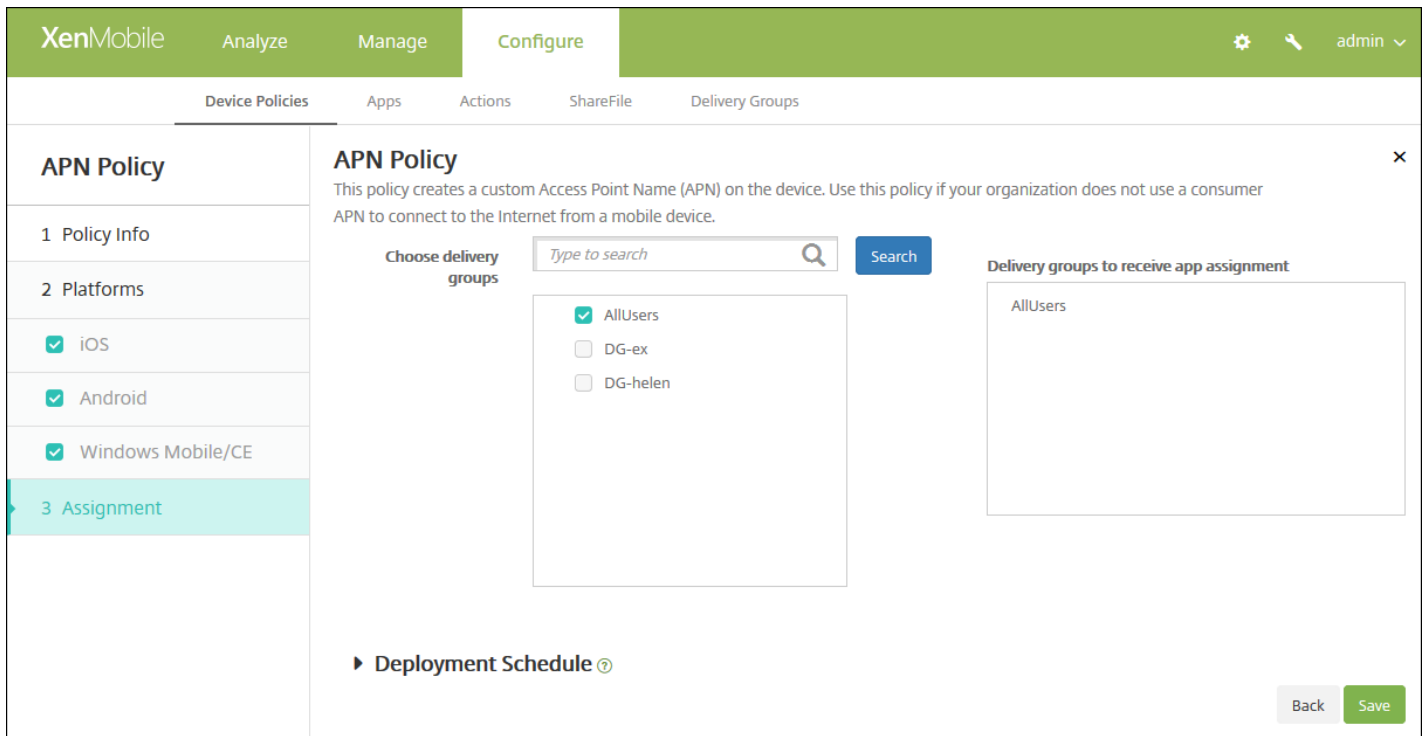
The screenshot shows the XenMobile web interface in the 'Configure' section. The 'APN Policy' configuration page is displayed, with a sidebar on the left containing a list of policy steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', three options are listed: iOS, Android, and Windows Mobile/CE, all of which are checked. The 'Windows Mobile/CE' option is currently selected. The main content area is titled 'Policy Information' and includes a description: 'This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.' Below this, there are four input fields: 'APN*' (a text box with a copy icon), 'Network' (a dropdown menu set to 'Built-in office'), 'User name' (a text box with a clear icon), and 'Password' (a text box with a show/hide icon). At the bottom of the main area, there is a section for 'Deployment Rules' with a right-pointing arrow. In the bottom right corner, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **APN**：键入接入点的名称。此信息必须与接受的某个 Android APN 匹配，否则策略将失败。
- **网络**：在列表中，单击要使用的网络类型。默认值为**内置办公网络**。
- **用户名**：该字符串指定此 APN 的用户名。如果用户名丢失，则在配置文件安装期间设备会提示该字符串。
- **密码**：此 APN 的用户密码。为进行混码处理，对密码进行了编码。如果负载中缺少密码，则配置文件安装期间设备会提示输入密码。

7. 配置部署规则

8. 单击下一步。此时将显示 **APN 策略分配** 页面。



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。

应用程序访问设备策略

Feb 27, 2017

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

一次只能配置一种类型的访问策略。可以针对必选的应用程序列表、推荐的应用程序列表或禁止的应用程序列表添加策略，但不能在一个应用程序访问策略中混合这些应用程序列表。如果为每种列表类型创建一个策略，建议谨慎地为每个策略命名，以便于了解 XenMobile 中的哪项策略适用于哪种应用程序列表。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**应用程序**下面，单击**应用程序访问**。此时将显示**应用程序访问策略**信息页面。

The screenshot shows the XenMobile configuration interface for an 'App Access Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Access Policy' and is divided into two sections: 'Policy Info' and 'Platforms'. The 'Policy Info' section is currently active and shows a 'Policy Name' field and a 'Description' text area. The 'Platforms' section has three checkboxes: 'iOS', 'Android', and 'Windows Mobile/CE', all of which are checked. A 'Next >' button is located at the bottom right of the page.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。此时将显示**策略平台**页面。

在平台下，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

6. 分别为选择的每个平台配置以下设置。

- **访问策略**：单击必需、推荐或禁止。默认值为“必需”。
- 要向列表中添加一个或多个应用程序，请单击**添加**，然后执行以下操作：
 - **应用程序名称**：输入应用程序的名称。
 - **应用程序标识符**：输入可选应用程序标识符。
 - 单击**保存**或**取消**。
 - 对要添加的每个应用程序重复这些步骤。

注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击**删除**以删除列表，或单击**取消**以保留列表。

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。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击下一步。此时将显示下一个平台页面或**应用程序访问策略**分配页面。
9. 在**选择交付组**旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。选择的组显示在右侧**用于接收应用程序分配的交付组**列表中。
10. 展开**部署计划**，然后配置以下设置：
 - 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。默认选项为开。如果选择关，无需配置其他选项。
 - 在**部署计划**旁边，单击**立即**或**稍后**。默认选项为**立即**。
 - 如果单击**稍后**，请单击日历图标，然后选择部署的日期和时间。
 - 在**部署条件**旁边，单击**每次连接时**或单击**仅当之前的部署失败时**。默认选项为**每次连接时**。
 - 在为**始终启用的连接部署**旁边，单击**开**或**关**。默认选项为关。

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS。

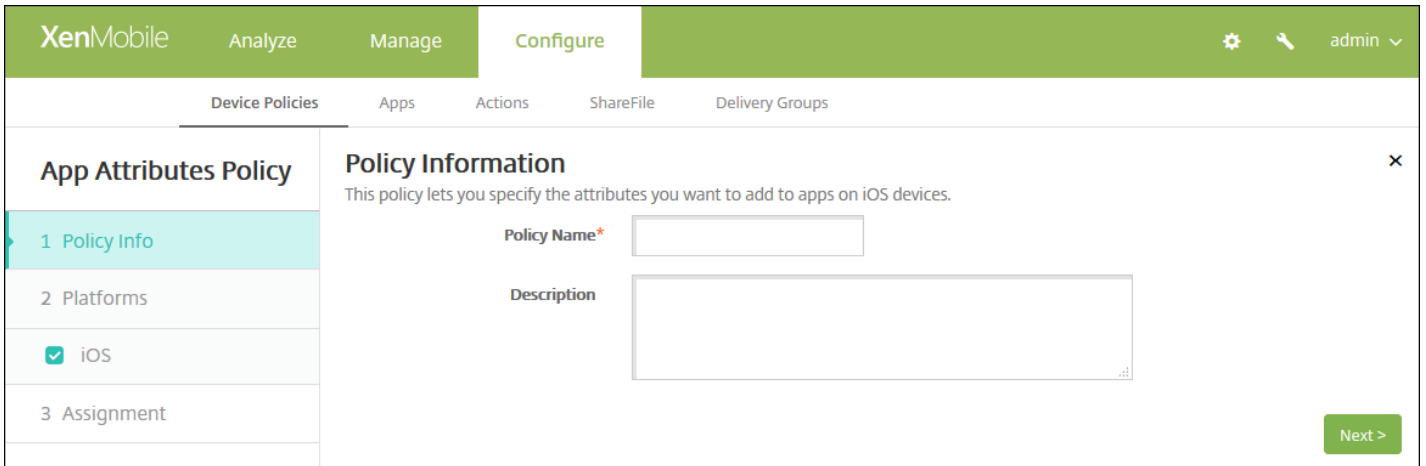
11. 单击**保存**。

应用程序属性设备策略

Mar 07, 2017

在“应用程序属性”设备策略中可以为 iOS 设备指定各种属性，例如托管应用程序捆绑包 ID 或“为应用单独设置 VPN”标识符。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略页面。
3. 展开更多，然后在应用程序下方，单击应用程序属性。此时将显示应用程序属性策略信息页面。

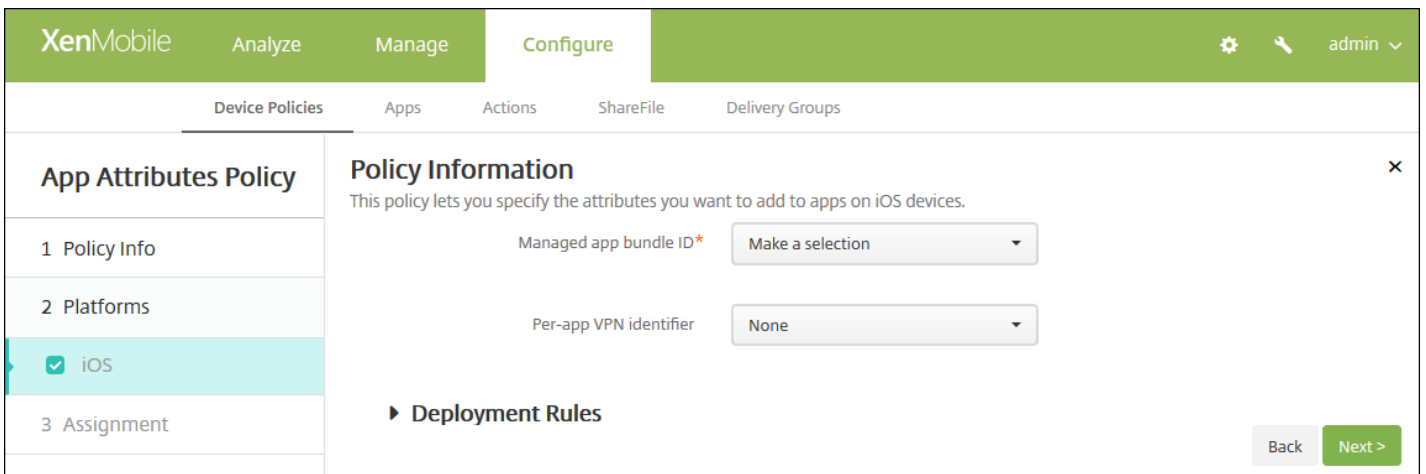


The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Attributes Policy' and 'Policy Information'. It includes a description: 'This policy lets you specify the attributes you want to add to apps on iOS devices.' There are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is visible at the bottom right.

4. 在策略信息窗格中，输入以下信息：

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

5. 单击下一步。此时将显示应用程序属性平台信息页面。



The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Attributes Policy' and 'Policy Information'. It includes a description: 'This policy lets you specify the attributes you want to add to apps on iOS devices.' There are two dropdown menus: 'Managed app bundle ID*' and 'Per-app VPN identifier'. A 'Deployment Rules' section is visible at the bottom. 'Back' and 'Next >' buttons are visible at the bottom right.

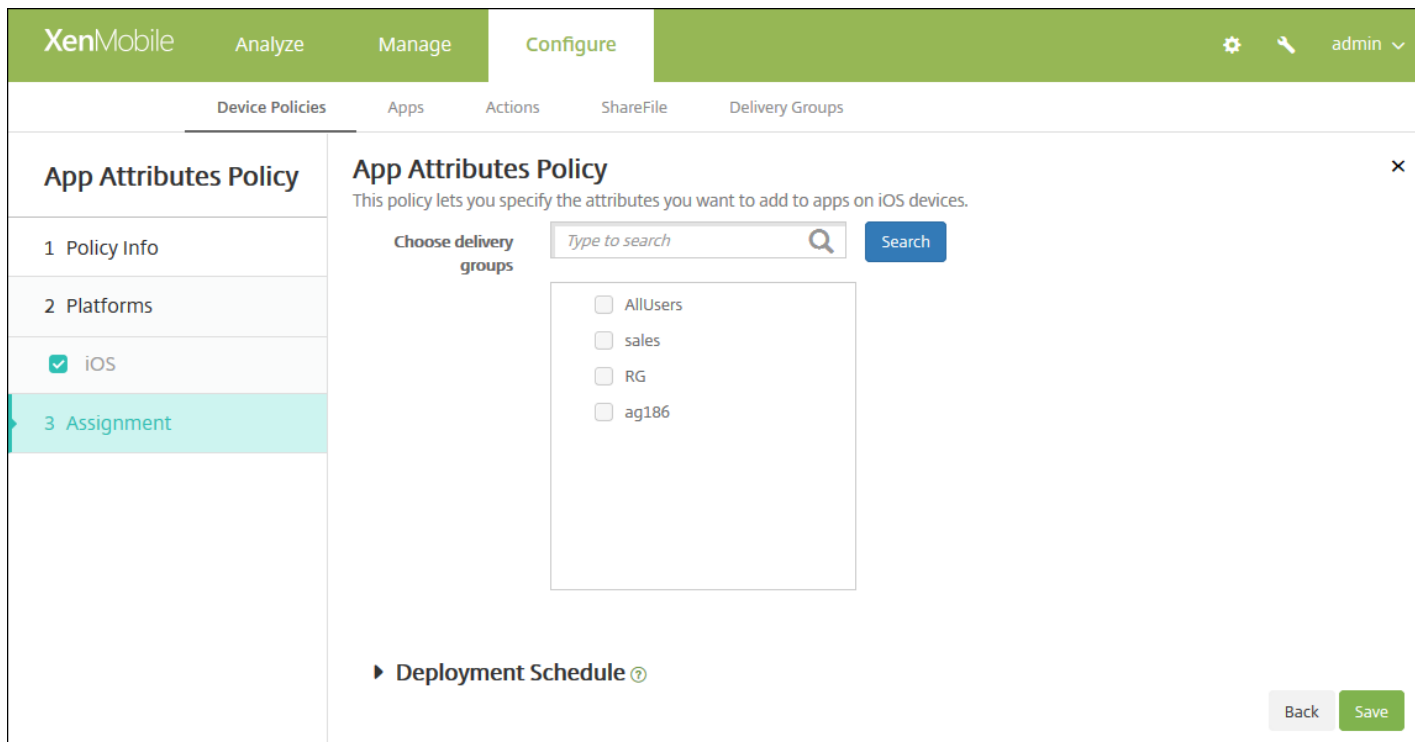
6. 配置以下设置：

- **托管应用程序捆绑包 ID**：在列表中，单击某个应用程序捆绑包 ID 或单击新增。

- 如果单击新增，请在显示的字段中键入应用程序捆绑包 ID。
- “为应用单独设置 VPN”标识符：在列表中，单击“为应用单独设置 VPN”标识符。

7. 配置部署规则

8. 单击下一步。此时将显示应用程序属性策略分配页面。



9. 在选择交付组旁边，键入以查找交付组。或者，在列表中选择要将策略分配到的一个或多个组。选择的组显示在用于接收应用程序分配的交付组列表中。

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。

应用程序配置设备策略

Feb 27, 2017

可以通过向用户的 iOS 设备部署 XML 配置文件（称为属性列表或 plist）或向 Windows 10 Phone、Tablet 或 Desktop 设备部署键/值对来远程配置支持托管配置的应用程序。配置指定应用程序中的各种设置和行为。XenMobile 在用户安装应用程序时将配置推送到设备。可以配置的实际设置和行为取决于应用程序，不在本文的探讨范围之内。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**页面。
3. 展开**更多**，然后在**应用程序**下面，单击**应用程序配置**。此时将显示**应用程序配置策略**信息页面。

The screenshot shows the XenMobile console interface. At the top, there's a green navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'App Configuration Policy' and has a sidebar with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' step is selected. The 'Policy Information' section contains a text box for 'Policy Name*' and a larger text area for 'Description'. Below this, there are three checked checkboxes for 'iOS', 'Windows Phone', and 'Windows Desktop/Tablet'.

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。

在平台下，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 6 以了解如何设置此平台的部署规则。

[配置 iOS 设置](#)

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

App Configuration Policy

- 1 Policy Info
- 2 Platforms
 - iOS
- 3 Assignment

Policy Information

This policy lets you define a configuration of a managed app to be applied on the iOS device. After you enter the dictionary content, you can check the syntax.

Identifier*

Dictionary content*

► Deployment Rules

配置 Windows Phone 或 Windows Desktop/Tablet 设置 ▾

XenMobile Analyze Manage **Configure** ⚙️ 🔍 administrator ▾

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

App Configuration Policy

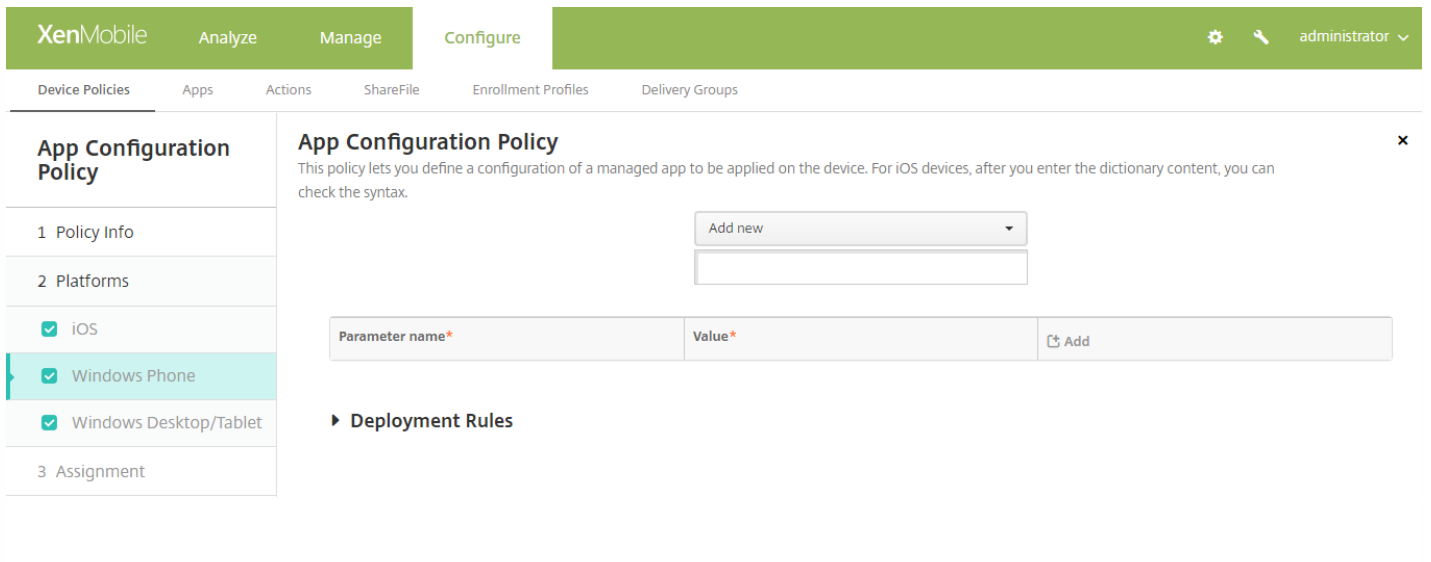
- 1 Policy Info
- 2 Platforms
 - iOS
 - Windows Phone
 - Windows Desktop/Tablet
- 3 Assignment

App Configuration Policy

This policy lets you define a configuration of a managed app to be applied on the device. For iOS devices, after you enter the dictionary content, you can check the syntax.

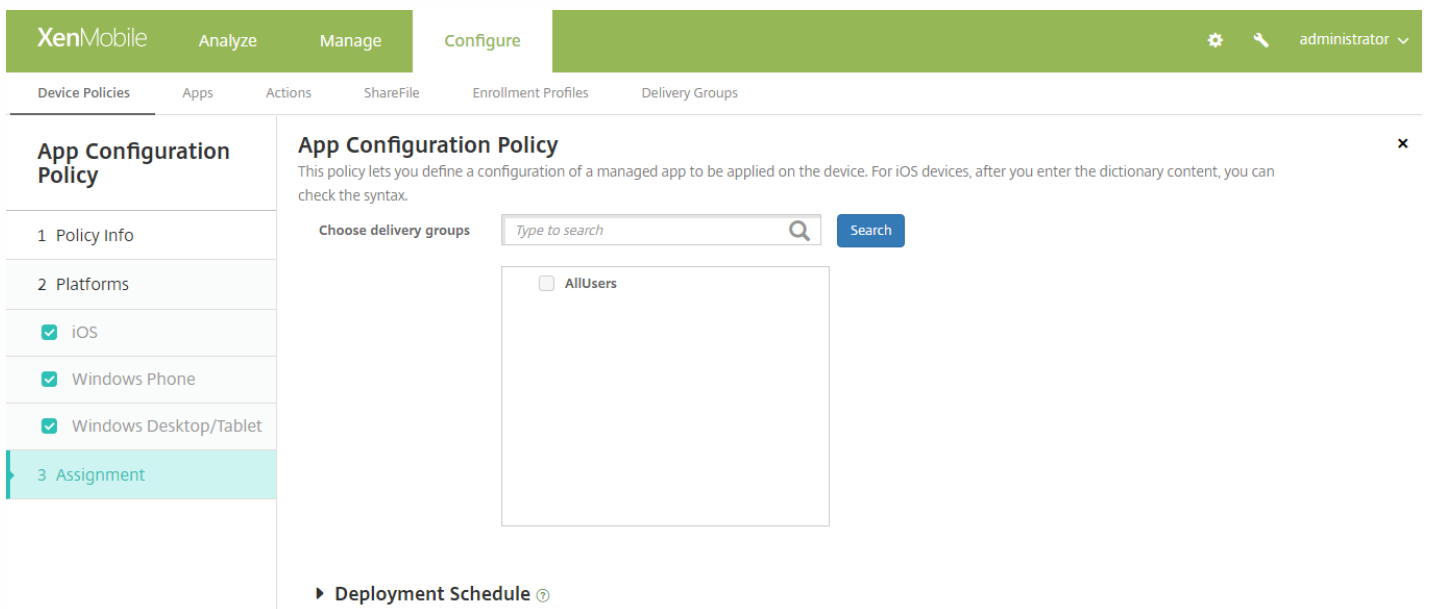
Parameter name*	Value*	<input type="button" value="Add"/>

► Deployment Rules



6. 配置部署规则

7. 单击下一步。此时将显示应用程序配置策略分配页面。



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：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，**为始终启用的连接部署除外**，它不适用于 iOS。

10. 单击**保存**。

应用程序清单设备策略

Feb 27, 2017

借助 XenMobile 中的应用程序清单策略，您可以收集托管设备上应用程序的清单，然后根据该清单对比部署到这些设备上的任何应用程序访问策略。这样，您可以发现出现在应用程序黑名单（在应用程序访问策略中禁止）或白名单（在应用程序访问策略中需要）上的应用程序，并采取相应的操作。可以为 iOS、Mac OS X、Android（包括为 Android for Work 启用的设备）、Windows Desktop/Tablet、Windows Phone 或 Windows Mobile/CE 设备创建应用程序访问策略。

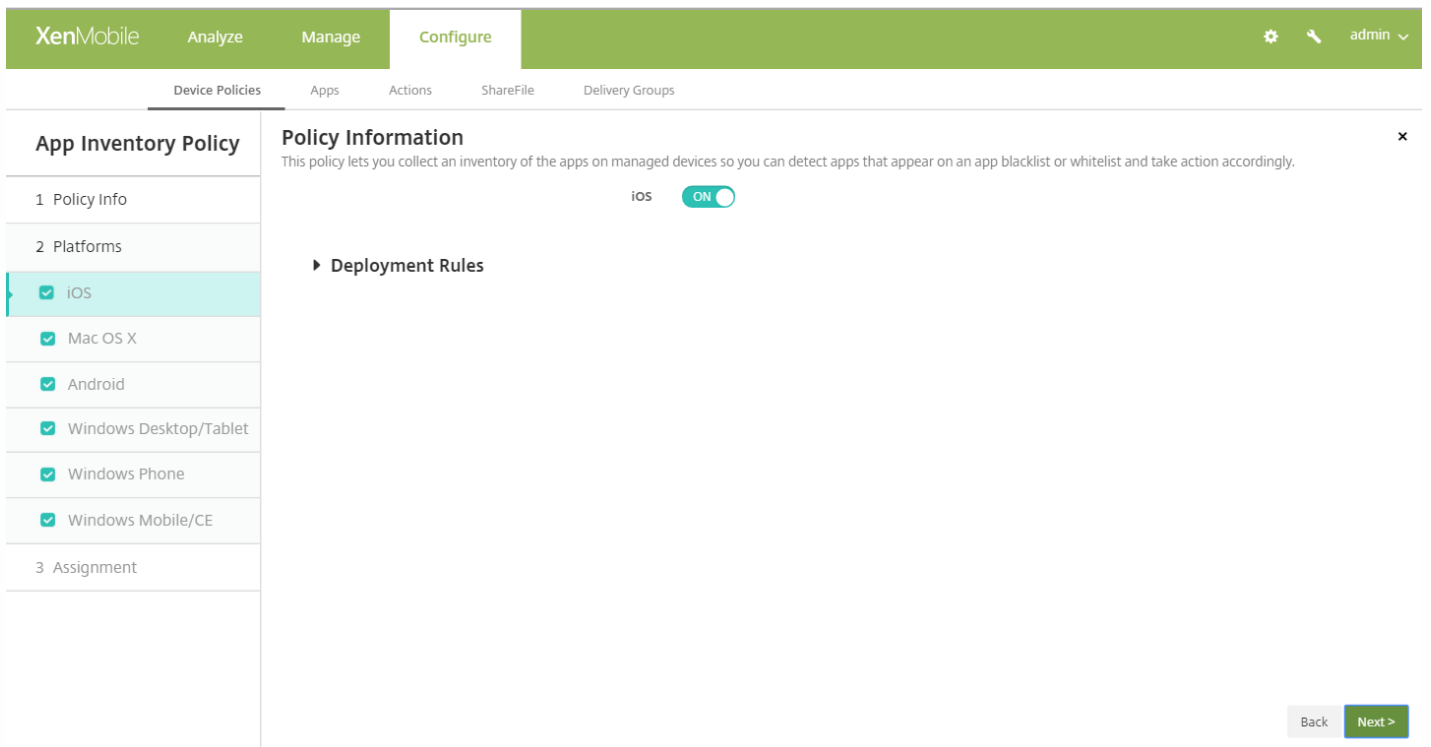
1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略页面。
3. 展开更多，然后在应用程序下面，单击应用程序清单。此时将显示应用程序清单策略页面。

The screenshot shows the XenMobile console interface for configuring an App Inventory Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Inventory Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Windows Desktop/Tablet, Windows Phone, and Windows Mobile/CE, all of which are checked. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.' Below the description are two input fields: 'Policy Name' and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

4. 在策略信息窗格中，键入以下信息：

- 策略名称：键入策略的名称。
- 说明：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。



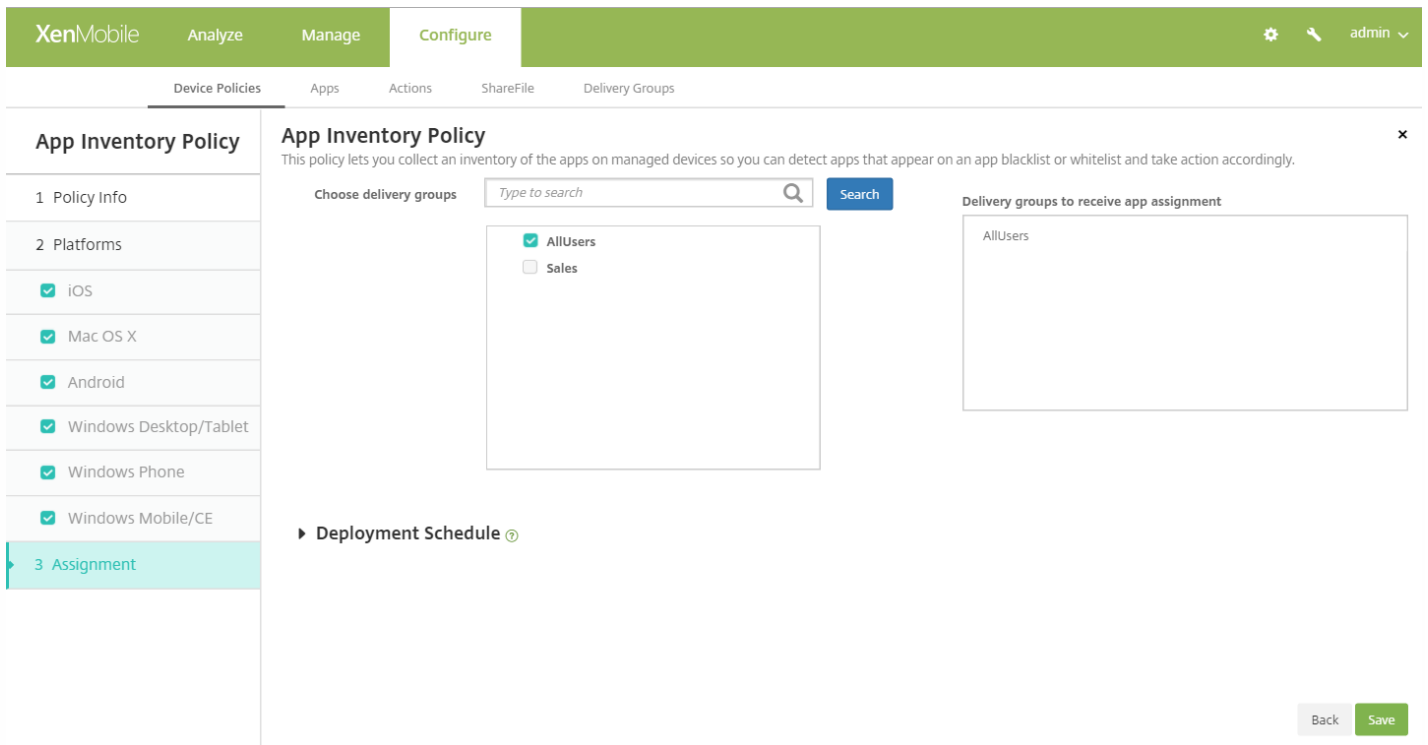
在平台下，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

6. 对于所选的每个平台，保留默认设置或将设置更改为关。默认值为开。

7. 配置部署规则

8. 单击下一步。此时将显示应用程序清单策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 如果在 **设置 > 服务器属性** 中配置了计划后台部署密钥，则适用此选项。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS

11. 单击保存。

应用程序锁定设备策略

Feb 27, 2017

可以在 XenMobile 中创建一条策略，用于定义允许在设备上运行的应用程序列表，或阻止在设备上运行的应用程序列表。可以同时为 iOS 和 Android 设备配置此策略，但策略具体的执行方式则因平台而异。例如，不能阻止在 iOS 设备上运行多个应用程序。

同样，对于 iOS 设备，每个策略只能选择一个 iOS 应用程序。这表示用户只能使用其设备运行单个应用程序。在强制执行应用程序锁定策略时，用户无法在设备上执行除您明确允许的选项之外的任何其他活动。

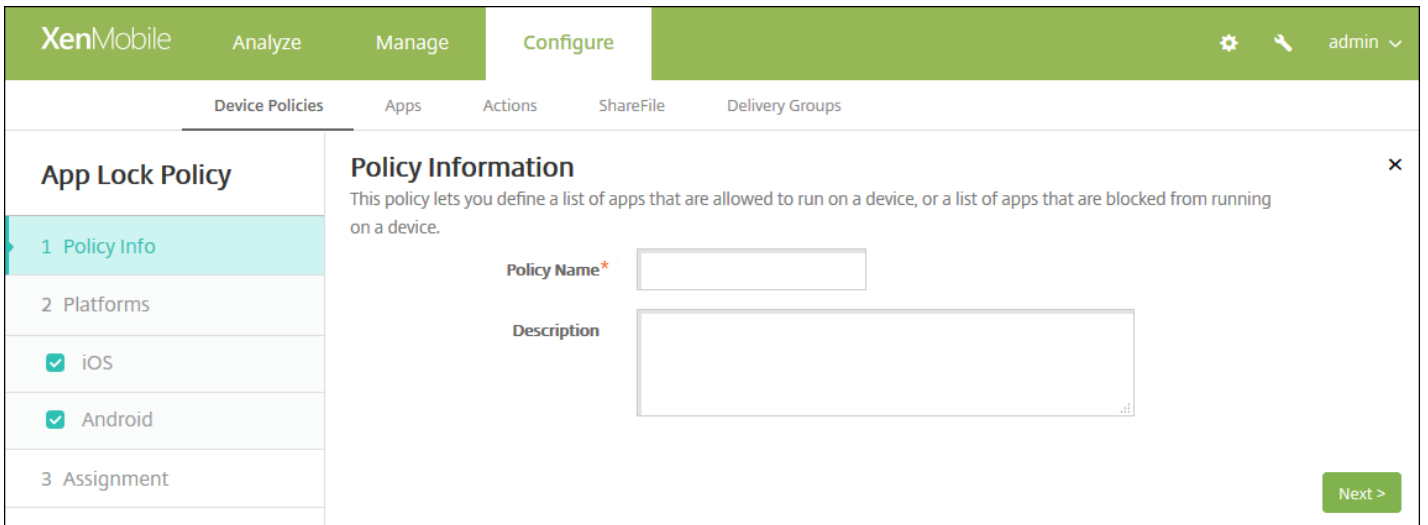
此外，必须监督 iOS 设备才能推送应用程序锁定策略。

虽然设备策略在大多数 Android L 和 M 设备上起作用，但是，由于 Google 弃用了所需的 API，因此，应用程序锁定策略在 Android N 或更高版本的设备上不起作用。

iOS 设置

Android 设置

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在安全性下面，单击应用程序锁定。此时将显示应用程序锁定策略页面。



The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Lock Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.' There are two input fields: 'Policy Name*' and 'Description'. The 'Policy Name*' field is currently empty. The 'Description' field is a larger text area, also empty. On the left side, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checkboxes: 'iOS' and 'Android', both of which are checked. At the bottom right of the main content area, there is a green button labeled 'Next >'.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：如有需要，请键入策略的说明。

5. 单击下一步。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

App Lock Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Android
- 3 Assignment

Policy Information ✕

This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.

App bundle ID*

Options

- Disable touch screen ON iOS 7.0+
- Disable device rotation sensing OFF iOS 7.0+
- Disable volume buttons OFF iOS 7.0+
- Disable ringer switch OFF iOS 7.0+
- Disable sleep/wake button OFF iOS 7.0+
- Disable auto lock OFF iOS 7.0+
- Enable VoiceOver OFF iOS 7.0+
- Enable zoom OFF iOS 7.0+
- Enable invert colors OFF iOS 7.0+
- Enable AssistiveTouch OFF iOS 7.0+
- Enable speak selection OFF iOS 7.0+
- Enable mono audio OFF iOS 7.0+

User Enabled Options

- Allow VoiceOver adjustment OFF iOS 7.0+
- Allow zoom adjustment OFF iOS 7.0+
- Allow invert colors adjustment OFF iOS 7.0+
- Allow AssistiveTouch adjustment OFF iOS 7.0+

Policy Settings

Remove policy Select date Duration until removal (in days)

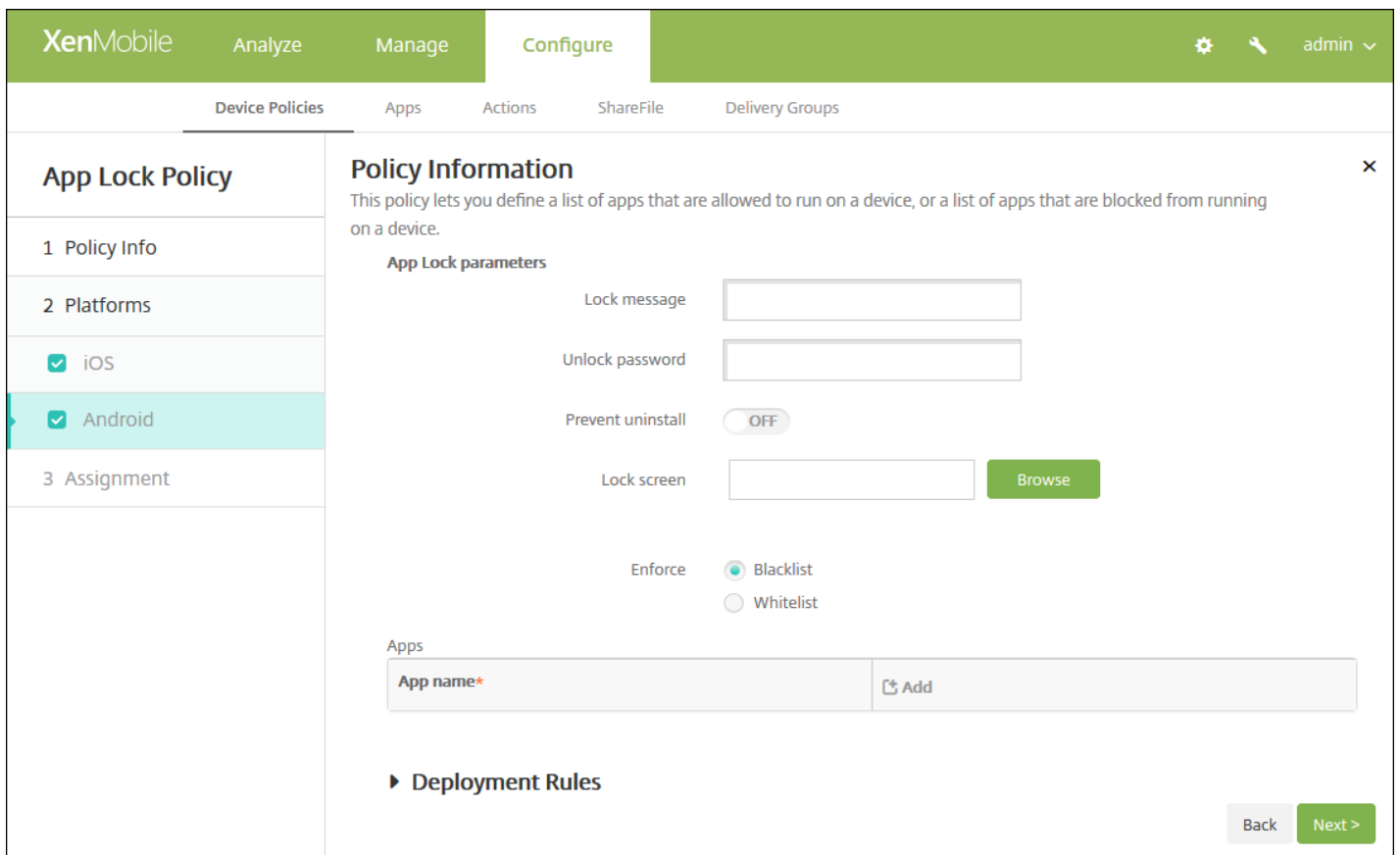
Allow user to remove policy

▶ Deployment Rules

配置以下设置：

- **应用程序捆绑包 ID**：在列表中，单击此策略适用的应用程序，或单击**新增**向列表中添加新应用程序。如果选择**新增**，请在显示的字段中键入应用程序名称。
- **选项**：以下各选项仅适用于 iOS 7.0 或更高版本。对于每个选项，除“禁用触摸屏”默认设置为开之外，默认情况下均设置为关。
 - 禁用触摸屏
 - 禁用设备旋转感应
 - 禁用音量按钮
 - 禁用铃声开关 - 注意：禁用此选项时，铃声行为取决于首次禁用时开关所处的位置。
 - 禁用睡眠/唤醒按钮
 - 禁用自动锁定
 - 禁用 VoiceOver
 - 启用缩放
 - 启用反转颜色
 - 启用 AssistiveTouch
 - 启用朗读所选内容
 - 启用单声道音频
- **用户已启用的选项**：以下各选项仅适用于 iOS 7.0 或更高版本。对于各选项，默认值为关。
 - 允许 VoiceOver 调整
 - 允许缩放调整
 - 允许反转颜色调整
 - 允许 AssistiveTouch 调整
- **策略设置**
 - ○ 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - ○ 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - ○ 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - ○ 如果单击**需要密码**，在**删除密码**旁边键入必需的密码。

配置 Android 设置



配置以下设置：

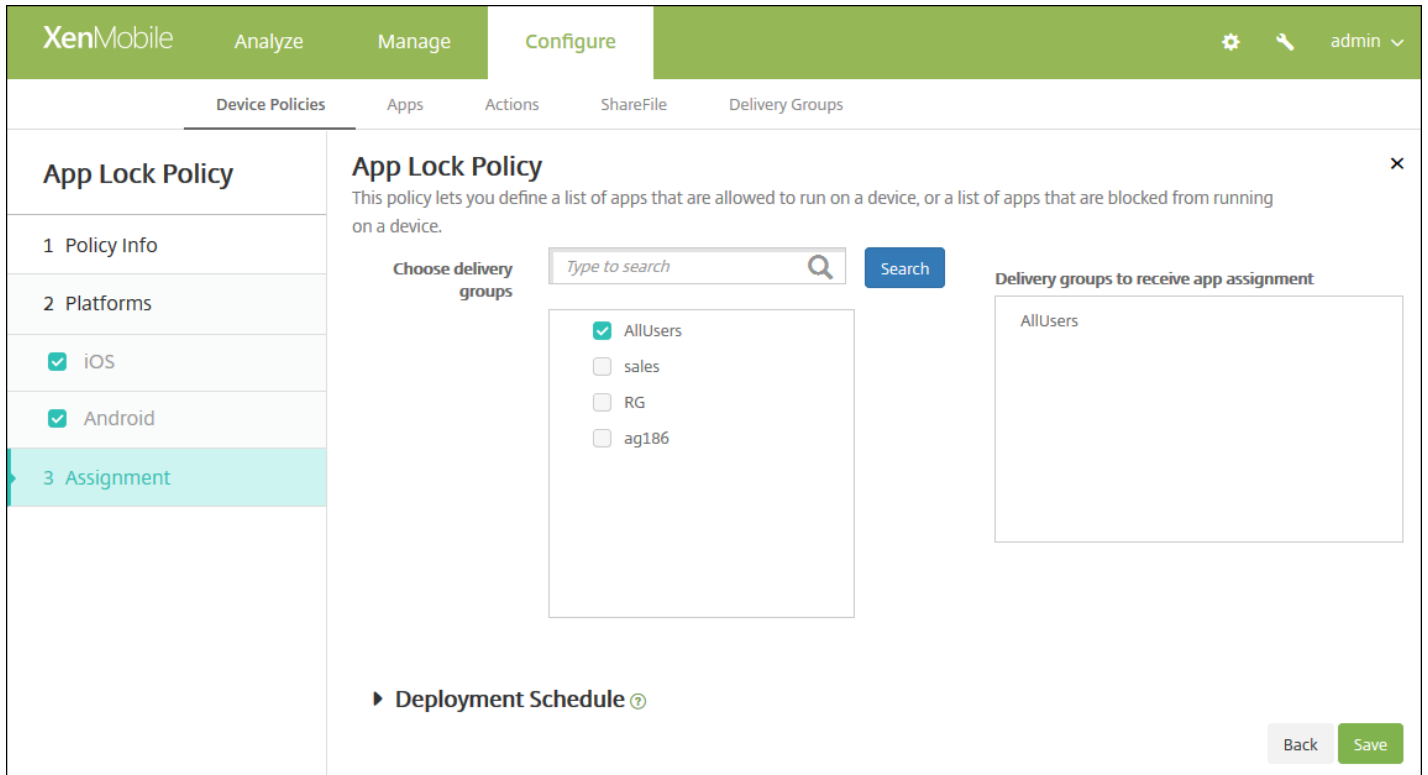
- **应用程序锁定参数**
 - **锁定消息**：键入用户尝试打开锁定的应用程序时看到的消息。
 - **解锁密码**：键入解锁应用程序的密码。
 - **阻止卸载**：选择是否允许用户卸载应用程序。默认值为关。
 - **锁定屏幕**：单击“浏览”并导航到显示在设备锁定屏幕上的图像所在的位置，选择此图像。
 - **强制执行**：单击黑名单以创建不允许在设备上运行的应用程序的列表，或单击白名单以创建允许在设备上运行的应用程序的列表。
- **应用程序**：单击添加，然后执行以下操作：
 - **应用程序名称**：在列表中，单击要添加到白名单或黑名单的应用程序的名称，或单击新增向可用应用程序列表中添加新应用程序。
 - 如果选择新增，请在显示的字段中键入应用程序名称。
 - 单击保存或取消。
 - 为要添加到白名单或黑名单中的每个应用程序重复执行这些步骤。

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

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。对列表进行任何更改，然后单击保存以保存更改后的列表，或单击取消以保持列表不变。

7. 配置部署规则

8. 单击下一步，将显示应用程序锁定策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

应用程序网络使用设备策略

Feb 27, 2017

您可以设置网络使用规则，以指定 iOS 设备上托管应用程序使用网络（如手机网络数据网络）的方式。规则仅适用于托管应用程序。托管应用程序是您通过 XenMobile 部署到用户设备的应用程序。其中不包括用户直接下载到设备上且未通过 XenMobile 部署的应用程序，或者在设备向 XenMobile 注册时已经安装到设备上的应用程序。

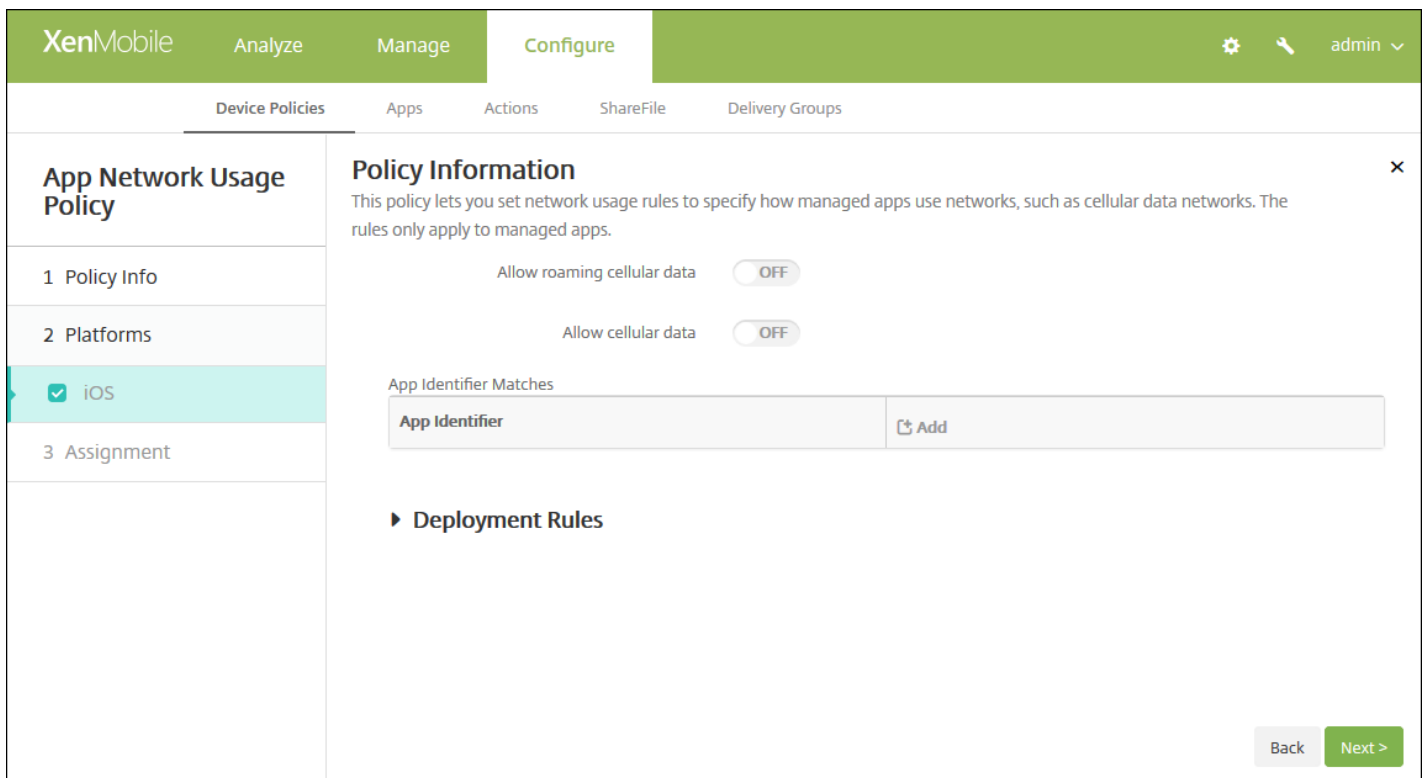
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**应用程序**下面，单击**应用程序网络使用**。此时将显示**应用程序网络使用策略**信息页面。

The screenshot shows the XenMobile console interface for configuring an App Network Usage Policy. The main heading is 'App Network Usage Policy'. Below it, there are three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' step is currently active. The 'Policy Information' section provides instructions: 'This policy lets you set network usage rules to specify how managed apps use networks, such as cellular data networks. The rules only apply to managed apps.' It includes two input fields: 'Policy Name*' (required) and 'Description'. A 'Next >' button is located at the bottom right of the configuration area.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。此时将显示**策略平台**页面。



6. 配置以下设置。

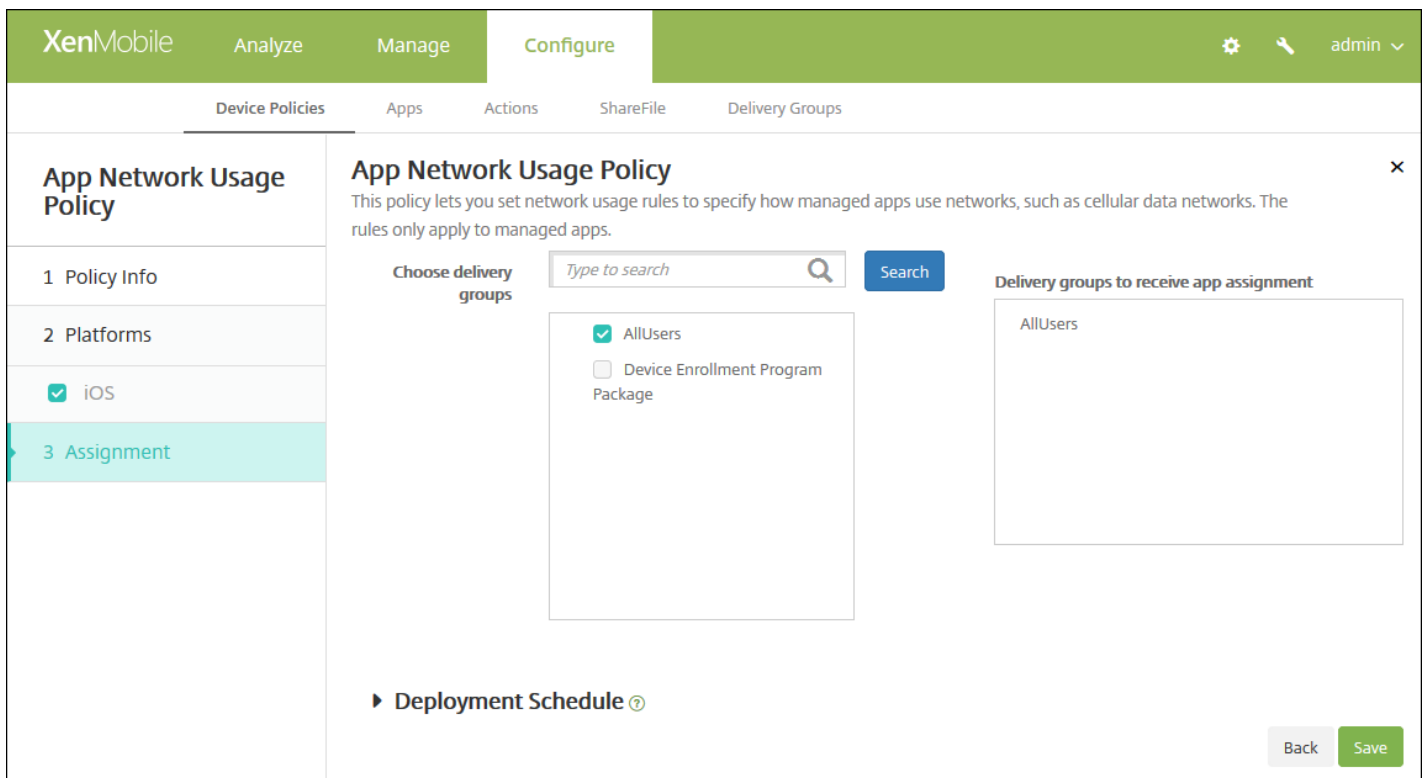
- **允许手机网络数据漫游**：选择指定应用程序是否可以在漫游时使用手机网络数据连接。默认值为关。
- **允许手机网络数据**：选择指定应用程序是否可以使用手机网络数据连接。默认值为关。
- **应用程序标识符匹配**：对于要添加到此列表中的每个应用程序，请单击**添加**，然后执行以下操作：
 - **应用程序标识符**：输入应用程序标识符。
 - 单击**保存**将应用程序保存到列表，或单击**取消**不将应用程序保存到列表中。

注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上方，然后单击右侧的垃圾箱图标。此时将显示确认对话框。单击**删除**以删除列表，或单击**取消**以保留列表。

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。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击**下一步**。此时将显示**应用程序网络使用策略分配**页面。



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。

应用程序限制设备策略

Feb 27, 2017

可以为希望阻止用户在 Samsung KNOX 设备上安装的应用程序创建黑名单，以及为希望允许用户安装的应用程序创建白名单。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在安全性下方，单击应用程序限制。此时将显示应用程序限制策略信息页面。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

App Restrictions Policy

- 1 Policy Info
- 2 Platforms
- Samsung KNOX
- 3 Assignment

Policy Information

This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

Policy Name*

Description

Next >

4. 在策略信息窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示 Samsung KNOX 平台页面。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

App Restrictions Policy

- 1 Policy Info
- 2 Platforms
- Samsung KNOX
- 3 Assignment

Policy Information

This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

Allow/Deny	New app restriction*	Add
		<input type="button" value="Add"/>

Deployment Rules

Back Next >

6. 对于要添加到“允许/拒绝”列表中的每个应用程序，请单击添加，然后执行以下操作：

- **允许/拒绝**：选择是否允许用户安装应用程序。
- **新应用程序限制**：键入应用程序软件包 ID；例如 com.kmdmaf.crackle。
- 单击**保存**将应用程序保存到“允许/拒绝”列表，或单击**取消**不将应用程序保存到“允许/拒绝”列表中。

注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上，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。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击下一步。此时将显示应用程序限制策略分配页面。

The screenshot shows the XenMobile Configure interface for an App Restrictions Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Restrictions Policy' and includes a description: 'This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.' The 'Assignment' section is active, showing a search bar for delivery groups and a list of groups: 'AllUsers' (checked) and 'sales'. A 'Delivery groups to receive app assignment' box also shows 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section and 'Back' and 'Save' buttons.

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。

应用程序通道设备策略

Feb 27, 2017

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

注意：通过在此策略中定义的通道发送的任何应用程序流量均先通过 XenMobile，然后再被重定向到运行此应用程序的服务器。

Android 设置

Windows Mobile/CE 设置

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**更多**，然后在**网络访问**下方，单击**通道**。此时将显示**通道策略**页面。

The screenshot shows the XenMobile console interface for configuring a Tunnel Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Tunnel Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is active and displays 'Policy Information' with a description: 'This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.' There are two input fields: 'Policy Name*' and 'Description'. The '2 Platforms' section shows two checked options: 'Android' and 'Windows Mobile/CE'. The '3 Assignment' section is currently empty. A 'Next >' button is visible in the bottom right corner.

4. 在**策略信息**窗格中，输入以下信息：

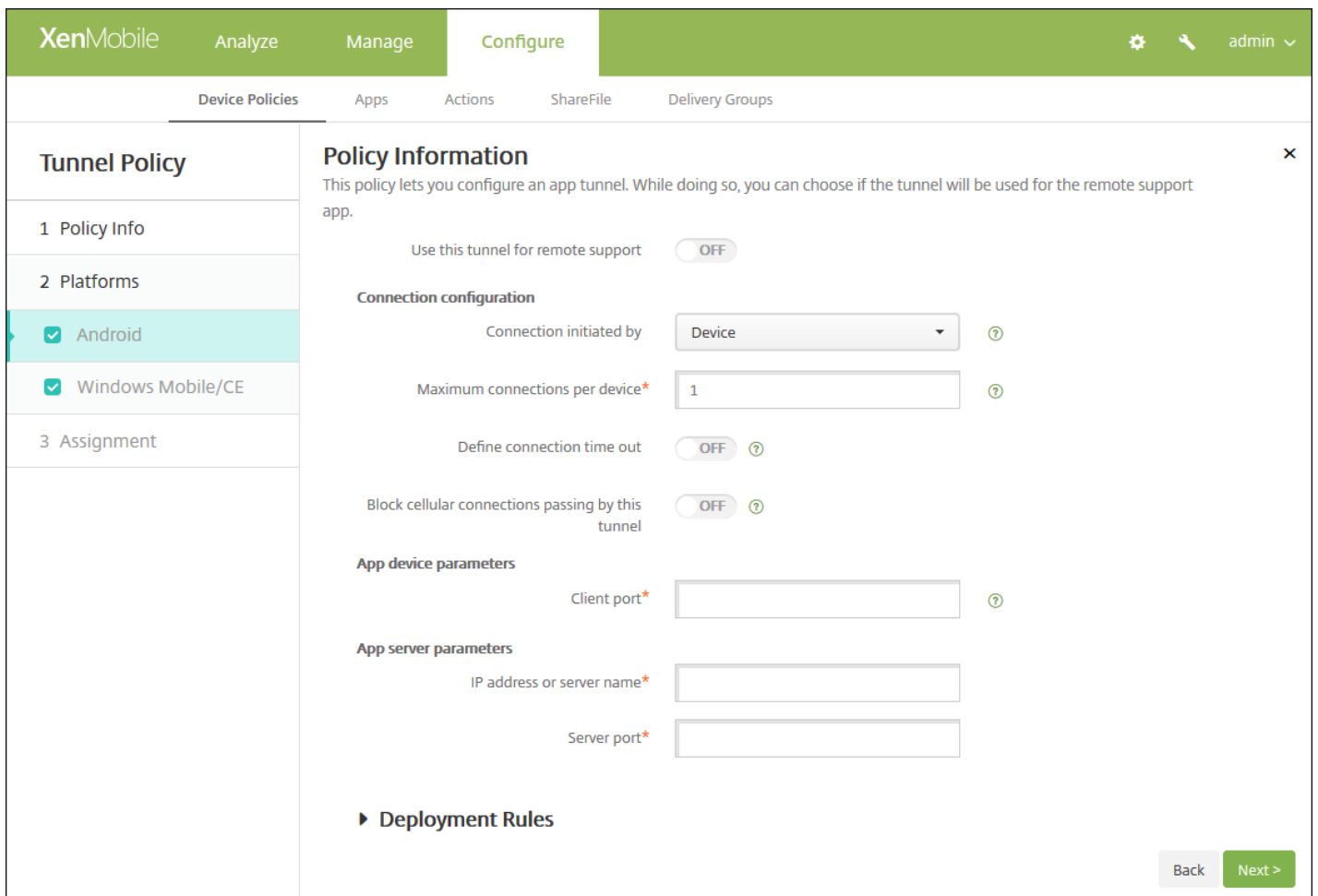
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。此时将显示**策略平台**页面。

6. 在**平台**下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Android 设置



配置以下设置：

- 使用此通道进行远程支持：选择是否将此通道用于远程支持。
注意：根据是否选择远程支持，配置步骤会有所不同。
- 如果不选择远程支持，请执行以下操作：
 - 连接发起者：单击设备或服务器以指定发起连接的源。
 - 每台设备最大连接数：键入一个数字，用于指定应用程序可以建立的并发 TCP 连接数。此字段仅适用于设备发起的连接。
 - 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
 - 连接超时：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度（以秒为单位）。
 - 阻止手机网络连接通过此通道：选择是否在漫游时阻止此通道。
注意：不会阻止 WiFi 和 USB 连接。
 - 客户端端口：键入客户端端口号。在大多数情况下，此值与服务器端口相同。
 - IP 地址或服务器名称：键入应用程序服务器的 IP 地址或名称。此字段仅适用于设备发起的连接。
 - 服务器端口：键入服务器端口号。
- 如果选择远程支持，请执行以下操作：
 - 使用此通道进行远程支持：设置为开。
 - 定义连接超时：选择是否设置通道关闭前应用程序可以空闲的时间长度。
 - 连接超时：如果将定义连接超时设置为“开”，则键入通道关闭前应用程序可以空闲的时间长度（以秒为单位）。

- **使用 SSL 连接**：选择是否为此通道使用安全 SSL 连接。
- **阻止手机网络连接通过此通道**：选择是否在漫游时阻止此通道。
注意：不会阻止 WiFi 和 USB 连接。

配置 Windows Mobile/CE 设置

配置以下设置：

- **使用此通道进行远程支持**：选择是否将此通道用于远程支持。
注意：根据是否选择远程支持，配置步骤会有所不同。
- 如果不选择远程支持，请执行以下操作：
 - **连接发起者**：单击设备或服务器以指定发起连接的源。
 - **协议**：在列表中，单击要使用的协议。默认值为通用 TCP。
 - **每台设备最大连接数**：键入一个数字，用于指定应用程序可以建立的并发 TCP 连接数。此字段仅适用于设备发起的连接。
 - **定义连接超时**：选择是否设置通道关闭前应用程序可以空闲的时间长度。
 - **连接超时**：如果将定义连接超时设置为开，则键入通道关闭前应用程序可以空闲的时间长度（以秒为单位）。

- **阻止手机网络连接通过此通道**：选择是否在漫游时阻止此通道。
注意：不会阻止 WiFi 和 USB 连接。
- **重新定向到 XenMobile**：在列表中，单击设备连接到 XenMobile 的方式。默认值为**通过应用程序设置**。
 - 如果选择**使用本地别名**，请在**本地别名**中键入别名。默认值为 **localhost**。
 - 如果选择 **IP 地址范围**，请在 **IP 地址范围起点**中键入起始 IP 地址，在 **IP 地址范围终点**中键入结束 IP 地址。
- **客户端端口**：键入客户端端口号。在大多数情况下，此值与服务器端口相同。
- **IP 地址或服务器名称**：键入应用程序服务器的 IP 地址或名称。此字段仅适用于设备发起的连接。
- **服务器端口**：键入服务器端口号。
- 如果选择**远程支持**，请执行以下操作：
 - **使用此通道进行远程支持**：设置为**开**。
 - **定义连接超时**：选择是否设置通道关闭前应用程序可以空闲的时间长度。
 - **连接超时**：如果将“定义连接超时”设置为“开”，则键入通道关闭前应用程序可以空闲的时间长度（以秒为单位）。
 - **使用 SSL 连接**：选择是否为此通道使用安全 SSL 连接。
 - **阻止手机网络连接通过此通道**：选择是否在漫游时阻止此通道。
注意：不会阻止 WiFi 和 USB 连接。

7. 配置部署规则

8. 单击下一步。此时将显示**通道策略分配**页面。

The screenshot shows the XenMobile configuration interface for a Tunnel Policy. The 'Assignment' step is selected in the left-hand navigation pane. The main content area displays a search bar for delivery groups, a list of available groups (AllUsers, DG-helen, DG-ex12) with checkboxes, and a 'Delivery groups to receive app assignment' box containing 'AllUsers'. A 'Deployment Schedule' section is visible at the bottom with a collapse icon. 'Back' and 'Save' buttons are located in the bottom right corner.

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

10. 展开**部署计划**，然后配置以下设置：

- 在**部署**旁边，单击**开**以计划部署，或单击**关**以阻止部署。默认选项为**开**。如果选择**关**，无需配置其他选项。

- 在部署计划旁边，单击立即或稍后。默认选项为立即。
- 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
- 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
- 在为始终启用的连接部署旁边，单击开或关。默认选项为关。

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

应用程序卸载设备策略

Feb 27, 2017

您可以为 iOS、Android、Samsung KNOX、Android for Work、Windows Desktop/Tablet 和 Windows Mobile/CE 平台创建应用程序卸载策略。通过应用程序卸载策略，您可以因任何原因将应用程序从用户设备中删除。原因可以是您不再想要支持某些应用程序，贵公司可能要将现有应用程序替换为其他供应商的类似应用程序等等。当此策略部署到用户的设备时，应用程序被删除。用户会收到卸载应用程序的提示，但是 Samsung KNOX 设备除外；Samsung KNOX 设备用户不会收到卸载应用程序的提示。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**应用程序**下方，单击**应用程序卸载**。此时将显示**应用程序卸载策略**页面。

The screenshot shows the XenMobile console interface for configuring an 'App Uninstall Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is currently selected and shows 'Policy Information' with a detailed description: 'This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.' There are two input fields: 'Policy Name' and 'Description'. The 'Platforms' section shows a list of platforms with checkboxes: iOS, Android, Samsung KNOX, Android for Work, Windows Desktop/Tablet, and Windows Mobile/CE. All checkboxes are checked. A 'Next >' button is located at the bottom right of the configuration area.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。此时将显示**策略平台**页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

配置以下设置：

- **托管应用程序捆绑包 ID**：在列表中，单击现有应用程序或单击**新增**。如果此平台没有配置应用程序，该列表将是空的，您必须添加新的应用程序。
 - 如果单击**添加**，您可在出现的字段中键入应用程序的名称。

配置所有其他平台设置

配置以下设置：

- **要卸载的应用程序**：对于您要添加的每个设备，单击**添加**，然后执行以下操作：
 - **应用程序名称**：在列表中，单击现有的应用程序，或单击**新增**输入新的应用程序名称。如果此平台没有配置应用程序，该列表将是空的，您必须添加新的应用程序。
 - 单击**添加**以添加应用程序，或单击**取消**以取消添加应用程序。

注意：要从卸载策略中删除现有应用程序，请将鼠标悬停在包含此列表的行上，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，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击下一步。此时将显示**应用程序卸载策略分配**页面。

The screenshot shows the XenMobile configuration interface for the 'App Uninstall Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Policy' and includes a description: 'This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.' There is a search box for 'Choose delivery groups' with a 'Search' button. Below the search box, there are two checkboxes: 'AllUsers' and 'Sales'. At the bottom right, there are 'Back' and 'Save' buttons.

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

10. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

应用程序卸载限制设备策略

Feb 27, 2017

可以指定用户在 Samsung SAFE 或 Amazon 上可以卸载或不能卸载的应用程序。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在应用程序下方，单击应用程序卸载限制。此时将显示应用程序卸载限制策略信息页面。

The screenshot shows the 'App Uninstall Restrictions Policy' configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below the navigation, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Restrictions Policy' and includes a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is active, showing a 'Policy Name*' field and a 'Description' text area. The 'Platforms' section shows 'Samsung SAFE' and 'Amazon' both selected with checkmarks. A 'Next >' button is located at the bottom right of the main content area.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。

The screenshot shows the 'App Uninstall Restrictions Policy' configuration interface, specifically the 'Deployment Rules' section. The top navigation bar and sidebar are the same as in the previous screenshot. The main content area is titled 'Policy Information' and includes a section for 'App Uninstall Restriction Settings' with a table for 'App Name*' and 'Rule', and an 'Add' button. Below the table is a 'Deployment Rules' section with a right-pointing arrow. A 'Back' button and a 'Next >' button are located at the bottom right of the main content area.

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

7. 为您选择的每个平台配置以下设置：

- **应用程序卸载限制设置**：对于要添加的每个应用程序规则，单击**添加**，然后执行以下操作：
 - **应用程序名称**：在列表中，单击某个应用程序，或单击**新增**以添加新应用程序。
 - **规则**：选择是否用户可以卸载应用程序。默认值为允许卸载。
 - 单击**保存**或**取消**。

注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上，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。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

8. 配置部署规则

9. 单击下一步。此时将显示**应用程序卸载限制策略分配**页面。

The screenshot shows the XenMobile configuration interface for the 'App Uninstall Restrictions Policy'. The interface is divided into a left sidebar and a main content area. The sidebar contains a list of steps: '1 Policy Info', '2 Platforms', and '3 Assignment', with '3 Assignment' currently selected. The main content area is titled 'App Uninstall Restrictions Policy' and includes a description: 'This policy lets you specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.' Below the description, there is a section for 'Choose delivery groups' with a search input field and a 'Search' button. Two radio button options are listed: 'AllUsers' and 'Device Enrollment Program Package'. At the bottom of the main content area, there is a 'Deployment Schedule' section with a dropdown arrow. The interface also features a top navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs, and a user profile 'admin' in the top right corner. At the bottom right, there are 'Back' and 'Save' buttons.

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

11. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS。

12. 单击**保存**。

浏览器设备策略

Feb 27, 2017

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

在 Samsung 设备上，可以完全禁用浏览器，也可以启用或禁用弹出消息、JavaScript、Cookie、自动填充和是否强制显示欺诈警告。

Samsung SAFE 和 Samsung KNOX 设置

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**添加新策略。此时将显示**添加新策略**对话框。
3. 单击**更多**，然后在**应用程序**下，单击**浏览器**。此时将显示**浏览器策略**信息页面。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Browser Policy' and 'Policy Information'. It contains a description: 'This policy lets you set rules for using the browser on Samsung and Android for Work devices.' There are two input fields: 'Policy Name*' and 'Description'. The 'Policy Name*' field is currently empty. The 'Description' field is also empty. On the left side, there is a sidebar with 'Browser Policy' selected, and sub-items '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '1 Policy Info', there are two checked checkboxes: 'Samsung SAFE' and 'Samsung KNOX'. At the bottom right, there is a 'Next >' button.

4. 在**策略信息**窗格中，输入以下信息：

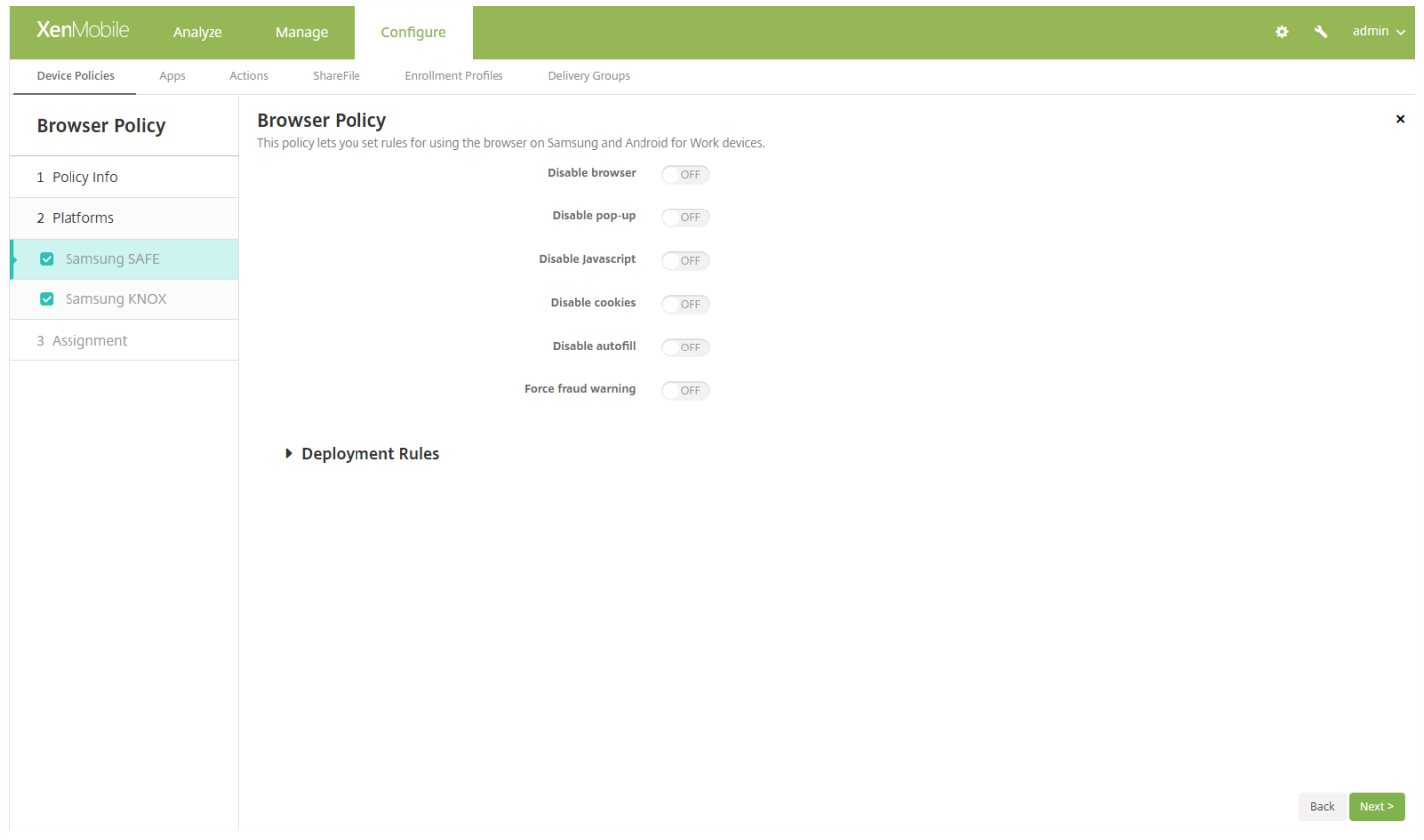
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。此时将显示**策略平台**页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Samsung SAFE 和 Samsung KNOX 设置



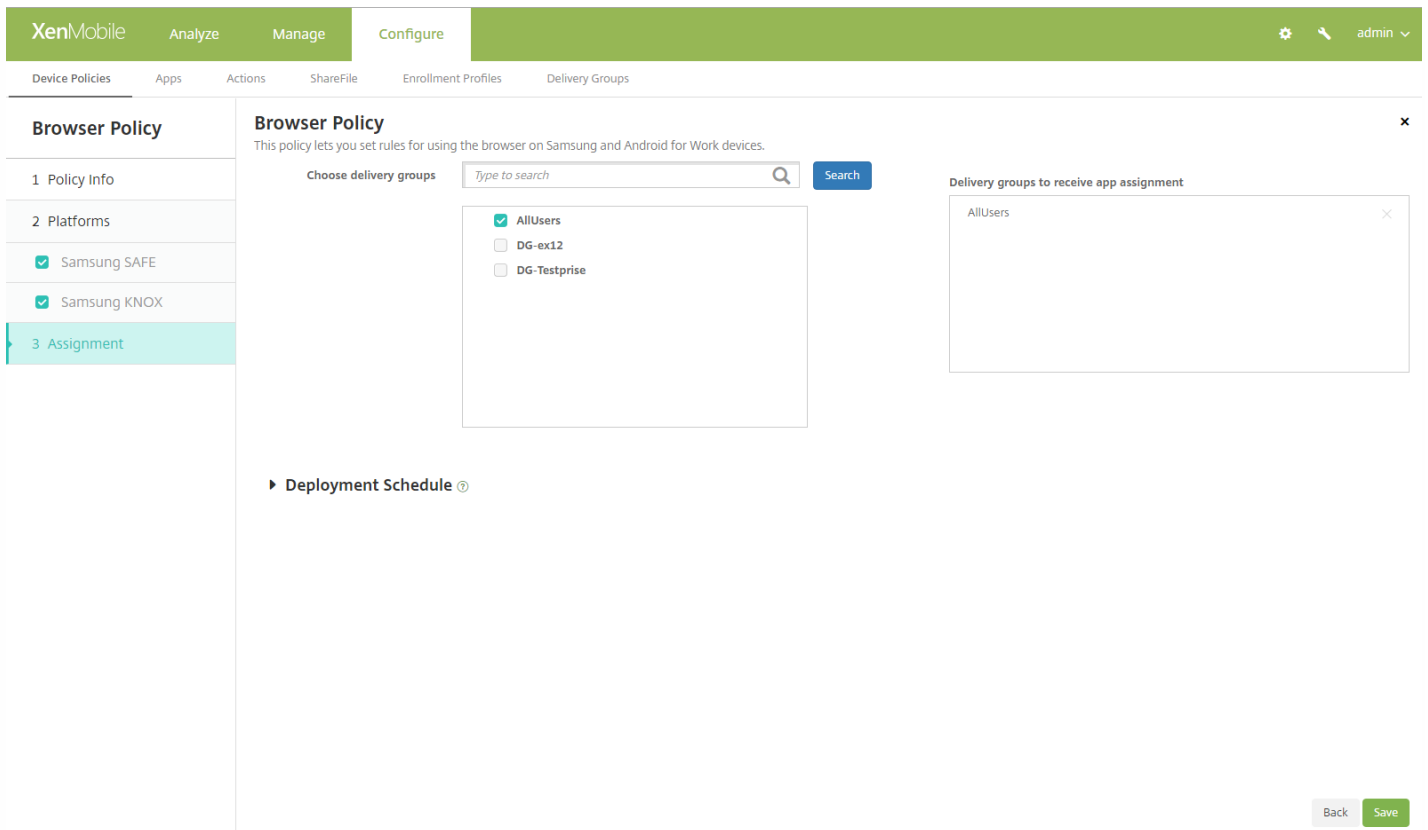
The screenshot shows the XenMobile configuration interface for a Browser Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Browser Policy' section is active, showing a list of settings on the right: 'Disable browser', 'Disable pop-up', 'Disable Javascript', 'Disable cookies', 'Disable autofill', and 'Force fraud warning', all of which are currently set to 'OFF'. A 'Deployment Rules' section is partially visible below. At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **禁用浏览器**：选择是否在用户设备上完全禁用 Samsung 浏览器。默认值为关，表示允许用户使用此浏览器。禁用此浏览器后，将不再显示以下选项。
- **禁用弹出窗口**：选择是否允许在此浏览器上显示弹出消息。
- **禁用 Javascript**：选择是否允许在此浏览器上运行 Javascript。
- **禁用 Cookie**：选择是否允许 Cookie。
- **禁用自动填充**：选择是否允许用户启用此浏览器的自动填充功能。
- **强制显示欺诈警告**：选择在用户访问欺诈性或存在漏洞的 Web 站点时是否显示警告。

7. 配置部署规则

8. 单击下一步。此时将显示浏览器策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存以保存此策略。

日历 (CalDav) 设备策略

Feb 27, 2017

可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 或 Mac OS X 设备添加日历 (CalDAV) 帐户，使用户可以将其计划数据与任何支持 CalDAV 的服务器同步。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在最终用户下面，单击日历(CalDav)。此时将显示日历(CalDav)策略页面。

The screenshot shows the XenMobile configuration interface for a Calendar (CalDAV) Policy. The interface is divided into a sidebar and a main content area. The sidebar on the left has a header 'Calendar (CalDAV) Policy' and three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section has two checkboxes: 'iOS' and 'Mac OS X', both of which are checked. The main content area has a header 'Policy Information' and a sub-header 'Policy Information'. Below the sub-header is a description: 'This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.' There are two input fields: 'Policy Name*' (required) and 'Description'. A 'Next >' button is located in the bottom right corner of the main content area.

4. 在策略信息窗格中，输入以下信息：

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

5. 单击下一步。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Calendar (CalDAV) Policy

- Policy Info
- Platforms
 - iOS
 - Mac OS X
- Assignment

Policy Information

This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.

Account description*

Host name*

Port*

Principal URL*

User name*

Password

Use SSL

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy

► Deployment Rules

Back Next >

配置以下设置：

- **帐户说明**：键入帐户说明。此字段为必填字段。
- **主机名**：键入 CalDAV 服务器的地址。此字段为必填字段。
- **端口**：键入连接到 CalDAV 服务器使用的端口。此字段为必填字段。默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的登录名称。此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为开。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

配置 Mac OS X 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Calendar (CalDAV) Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
- 3 Assignment

Policy Information

This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.

Account description*

Host name*

Port*

Principal URL*

User name*

Password

Use SSL

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy

Profile scope OS X 10.7+

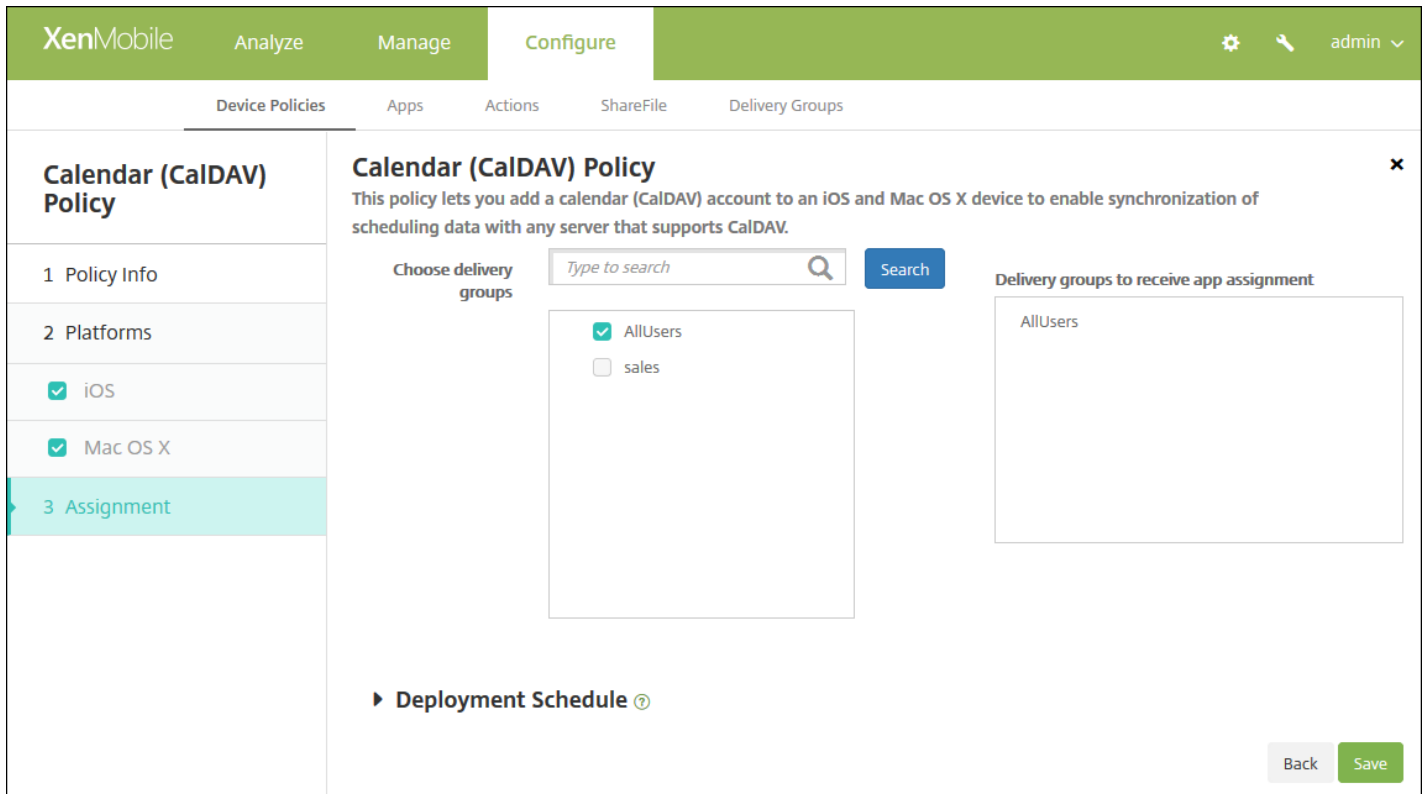
► Deployment Rules

配置以下设置：

- **帐户说明**：键入帐户说明。此字段为必填字段。
- **主机名**：键入 CalDAV 服务器的地址。此字段为必填字段。
- **端口**：键入连接到 CalDAV 服务器使用的端口。此字段为必填字段。默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的登录名称。此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CalDAV 服务器。默认值为开。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。
 - 在**配置文件作用域**旁边，单击**用户**或**系统**。默认值为**用户**。此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击下一步。此时将显示日历(CalDAV)策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

手机网络设备策略

Feb 27, 2017

此策略允许您在 iOS 设备上配置手机网络设置。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略页面。
3. 展开更多，然后在网络访问权限下，单击手机网络。此时将显示手机网络策略信息页面出现。

The screenshot shows the XenMobile configuration interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. The 'Configure' tab is active. Below the navigation bar, there are several tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' tab is selected. On the left side, there is a sidebar with 'Cellular Policy' selected. Under 'Cellular Policy', there are three sub-items: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. The '1 Policy Info' sub-item is expanded, showing a 'Policy Information' window. The 'Policy Information' window has a title bar with a close button (X). Below the title bar, there is a description: 'This policy lets you configure cellular network settings on an iOS device.' There are two input fields: 'Policy Name*' (required) and 'Description'. A 'Next >' button is located at the bottom right of the 'Policy Information' window.

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。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Cellular Policy

- 1 Policy Info
- 2 Platforms
 - iOS
- 3 Assignment

Policy Information

This policy lets you configure cellular network settings on an iOS device.

Attach APN

Name

Authentication type **PAP**

User name

Password

APN

Name

Authentication type **PAP**

User name

Password

Proxy server

Proxy server port

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy **Always**

► **Deployment Rules**

Back Next >

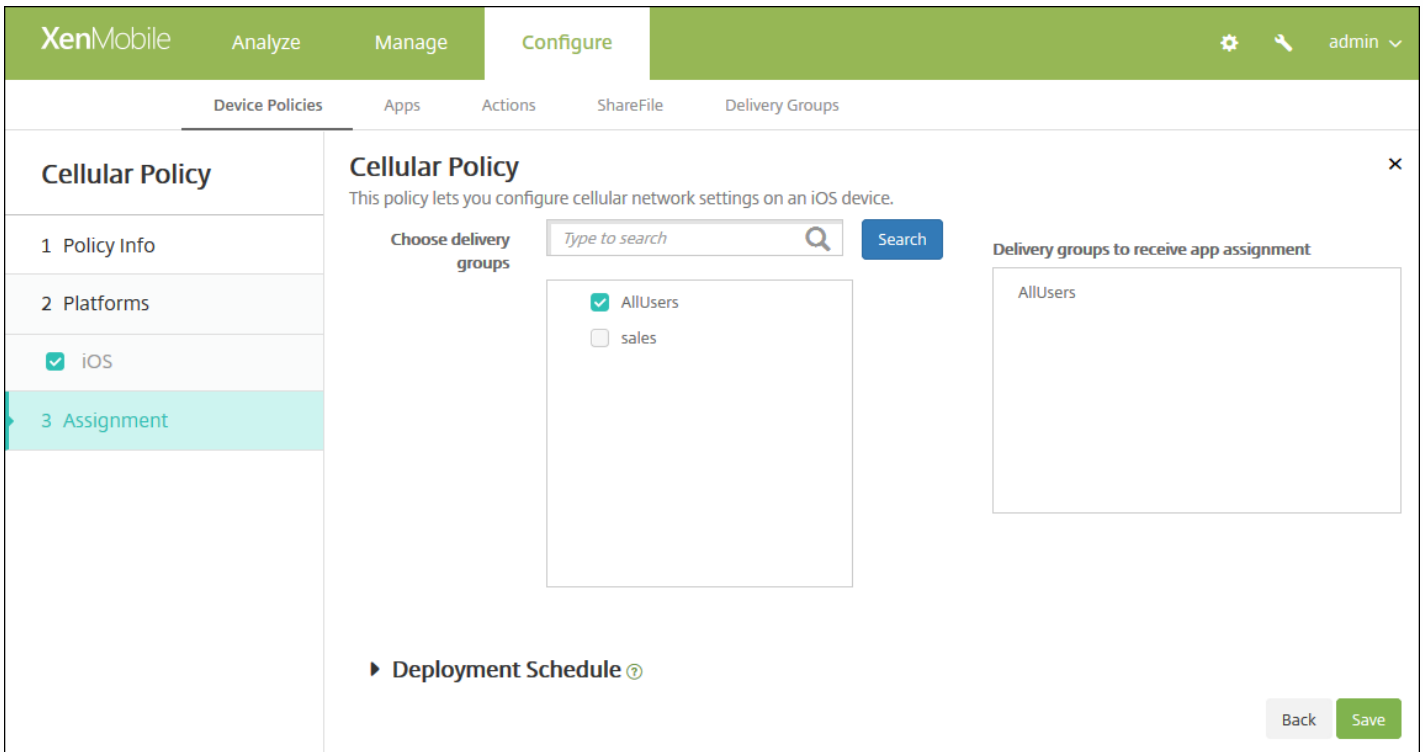
6. 配置以下设置：

- **连接 APN**
 - 名称：键入此配置的名称。
 - 身份验证类型：在清单上，单击质询握手身份验证协议 (**CHAP**) 或密码身份验证协议 (**PAP**)。默认值为 **PAP**。
 - 用户名：键入用于身份验证的用户名。
- **APN**
 - 名称：键入接入点名称 (APN) 配置的名称。
 - 身份验证类型：在列表中，单击 **CHAP** 或 **PAP**。默认值为 **PAP**。
 - 用户名：键入用于身份验证的用户名。
 - 密码：键入用于身份验证的密码。
 - 代理服务器：键入代理服务器网络地址。
- **策略设置**

- 在删除策略旁边，单击选择日期或删除前保留时间(天)。
- 如果单击选择日期，请单击日历以选择具体删除日期。
- 在允许用户删除策略列表中，单击始终、需要密码或从不。
- 如果单击需要密码，在删除密码旁边，键入必需的密码。

7. 配置部署规则

8. 单击下一步。此时将显示手机网络策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

连接管理器设备策略

Feb 27, 2017

在 XenMobile 中，可以为自动连接到 Internet 的应用程序指定连接设置并提供网络。此策略仅适用于 Windows Pocket PC。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 单击更多，然后在网络访问下方，单击连接管理器。将显示连接管理器策略信息页面。

The screenshot shows the XenMobile Configuration console. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Connection Manager Policy' and 'Policy Information'. It includes a sub-header 'Sets how apps connect to the Internet or to a private network. This policy only applies to Pocket PCs.' There are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示 **Windows Mobile/CE** 平台页面。

The screenshot shows the XenMobile Configuration console. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Connection Manager Policy' and 'Policy Information'. It includes a sub-header 'Sets how apps connect to the Internet or to a private network. This policy only applies to Pocket PCs.' There are two dropdown menus: 'Apps that connect to a private network automatically use' and 'Apps that connect to the Internet automatically use'. A 'Deployment Rules' section is visible below. A 'Back' button and a 'Next >' button are located at the bottom right.

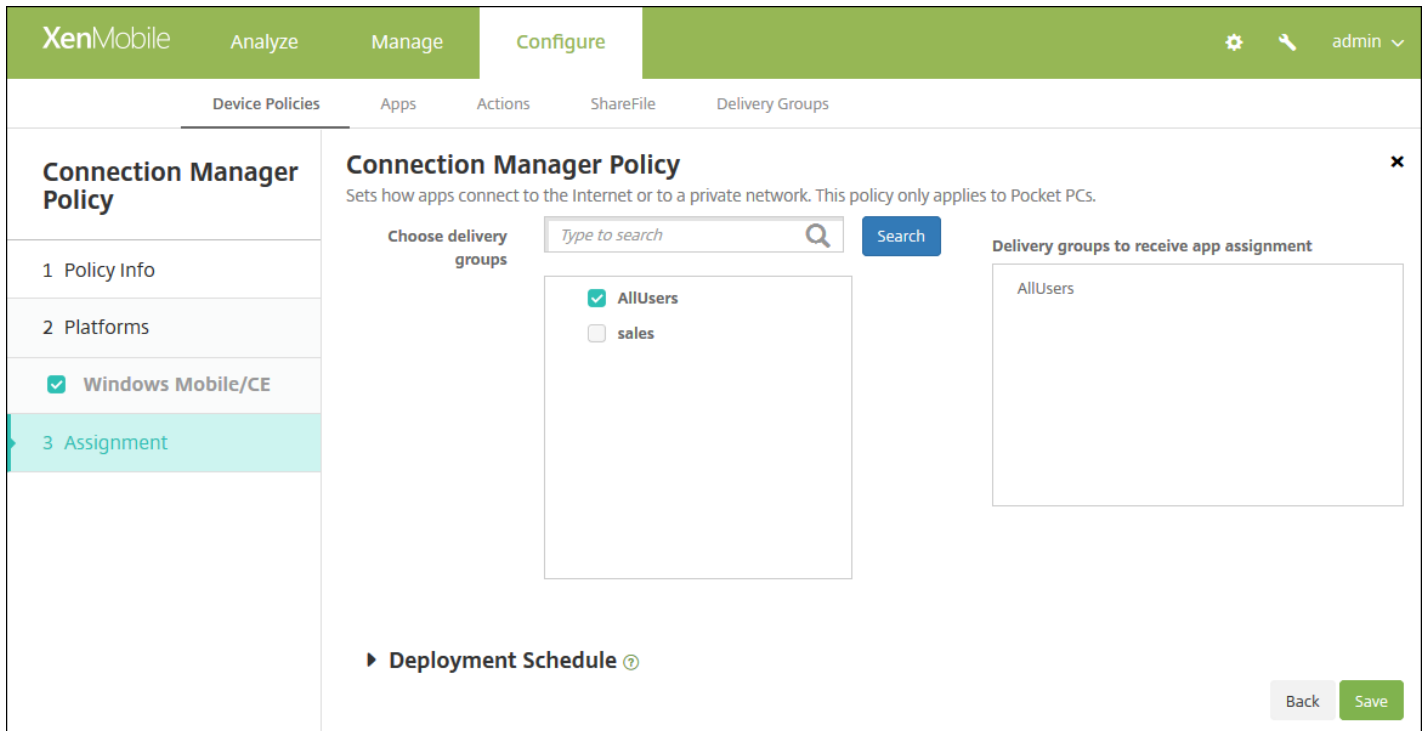
6. 配置以下设置。

注意：内置办公网络表示所有连接均指向公司的 Intranet，内置 Internet 表示所有连接均指向 Internet。

- 自动连接到专用网络的应用程序使用：在列表中，单击内置办公网络或内置 Internet。默认值为内置办公网络。
- 自动连接到 Internet 的应用程序使用：在列表中，单击内置办公网络或内置 Internet。默认值为内置办公网络。

7. 配置部署规则

8. 单击下一步。此时将显示连接管理器分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

连接计划设备策略

Feb 27, 2017

可以创建连接计划策略，用于控制用户的设备连接到 XenMobile 的方式和时间。请注意，对于为 Android for Work 启用的设备，也可以配置此策略。

可以指定用户需要手动连接其设备、设备永久保持连接状态或设备在定义的时间范围内进行连接。

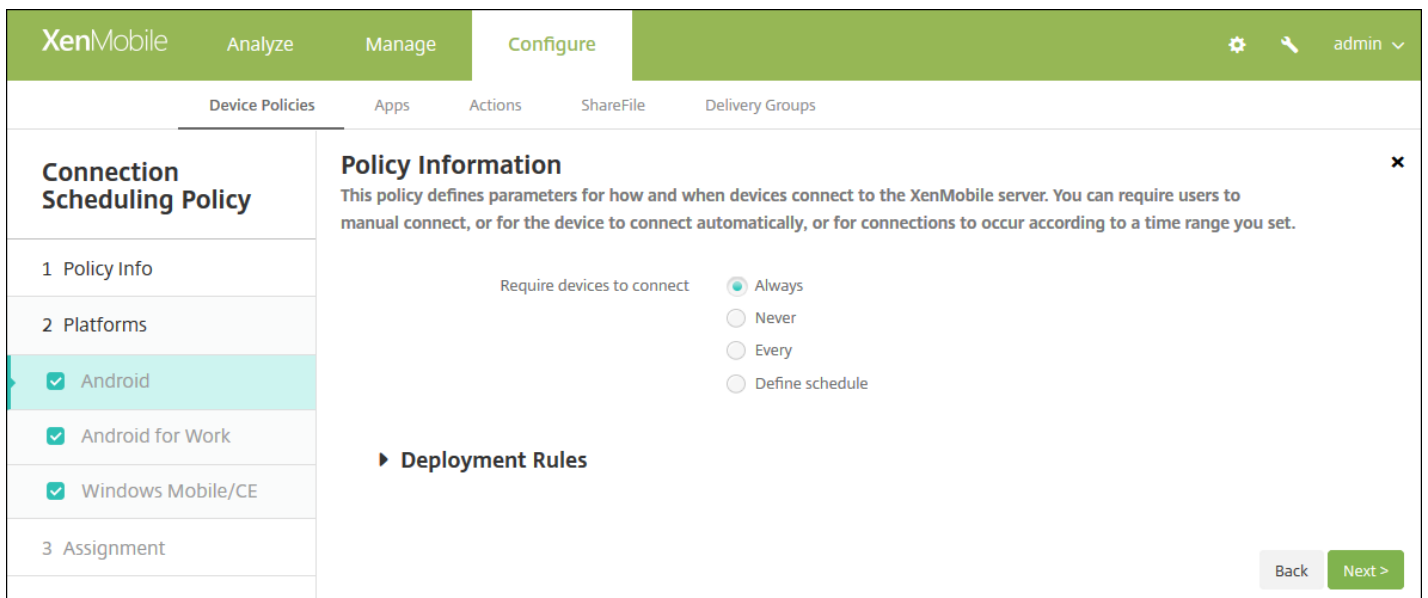
1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 单击计划。将显示连接计划策略信息页面。

The screenshot shows the XenMobile Configuration console. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active, and the 'Device Policies' sub-tab is selected. The main content area is titled 'Connection Scheduling Policy' and contains a 'Policy Information' section. The description states: 'This policy defines parameters for how and when devices connect to the XenMobile server. You can require users to manual connect, or for the device to connect automatically, or for connections to occur according to a time range you set.' Below the description are two input fields: 'Policy Name*' (a text box) and 'Description' (a text area). On the left, a sidebar shows the 'Connection Scheduling Policy' section with three sub-sections: '1 Policy Info' (selected), '2 Platforms' (with checkboxes for Android, Android for Work, and Windows Mobile/CE, all checked), and '3 Assignment'. A 'Next >' button is located at the bottom right of the main content area.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。



6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 8 以了解如何设置此平台的部署规则。

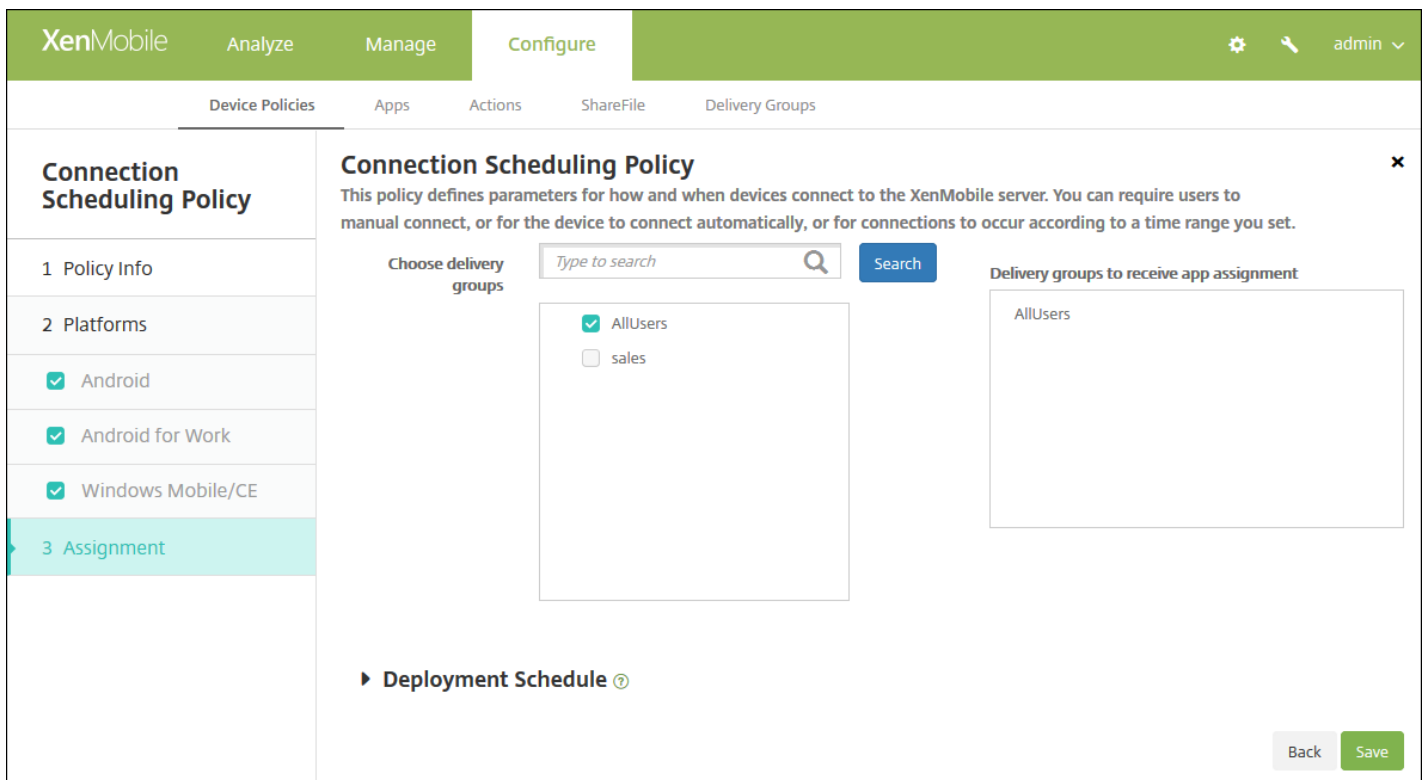
7. 分别为选择的每个平台配置以下设置：

- **需要连接设备**：单击要为此计划设置的选项。
 - **总是**：连接永久保持活动状态。在丢失网络连接后，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。Citrix 建议使用此选项以优化安全性。选择**总是**时（还适用于**设备通道策略**），**定义连接超时**设置可确保连接不会耗尽电池电量。通过保持连接处于活动状态，您可以根据需要将擦除或锁定等安全命令推送到设备。还必须在部署到设备的每个策略中选择**部署计划**选项为**始终启用的连接部署**。
 - **从不**：手动进行连接。用户必须从其设备上的 XenMobile 启动连接。Citrix 建议不要对生产部署使用此选项，因为这会阻止您将安全策略部署到设备，因此，用户从不会收到任何新应用程序或策略。
 - **每隔**：按照指定间隔进行连接。如果此选项生效，则当您发送锁定或擦除等安全策略时，XenMobile 将在下次设备连接时在设备上处理该操作。选择此选项后，将显示**每隔 N 分钟连接一次**字段，您必须在此处输入分钟数，在经过此分钟数之后，设备必须重新连接。默认值为 20。
 - **定义计划**：如果启用，在丢失网络连接后，用户设备上的 XenMobile 尝试重新连接到 XenMobile 服务器，并在您定义的时间范围内通过以固定间隔传输控制数据包监视连接。有关如何定义连接时间范围的信息，请参阅[定义连接的时间范围](#)。
 - **在此时段内保持永久连接**：在定义的时间范围内，用户设备必须连接。
 - **要求每个范围内存在一个连接**：在定义的任何时间范围内用户设备必须至少连接一次。
 - **使用本地设备时间而非 UTC**：将定义的时间范围与本地设备时间而非世界协调时间 (UTC) 同步。

定义连接的时间范围

启用下列选项时，将显示一个时间表，您可以利用此时间表设置所需的时间范围。您可以启用其中一个选项，也可以同时启用两个选项，以满足在指定时间需要永久连接或在特定时限内需要连接的需求。时间表中的每个方格代表 30 分钟，因此，如果您希望在每个工作日的上午 8:00 到上午 9:00 之间连接，应单击时间表上每个工作日的上午 8:00 到上午 9:00 之间的两个方格。

例如，下图中的两个时间表需要在每个工作日的上午 8:00 到上午 9:00 之间进行永久连接，在周六上午 12:00 到周日上午 1:00 之间进行永久连接，在每个工作日的上午 5:00 到上午 8:00 或上午 10:00 到下午 11:00 点之间至少有一个连接。



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

11. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

12. 单击保存。

联系人 (CardDAV) 设备策略

Feb 27, 2017

可以在 XenMobile 中添加一个设备策略，从而向用户的 iOS 或 Mac OS X 设备添加 iOS 联系人 (CardDAV) 帐户，使用户可以将其联系人数据与任何支持 CardDAV 的服务器同步。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在安全性下方，单击联系人 CardDAV。此时将显示 CardDAV 策略页面。

The screenshot shows the XenMobile configuration interface for a CardDAV Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'CardDAV Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a description: 'This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.' Below the description are two input fields: 'Policy Name*' (required) and 'Description'. The 'Policy Name*' field is empty. The 'Description' field is also empty. A 'Next >' button is located at the bottom right of the form.

4. 在策略信息窗格中，键入以下信息：

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

5. 单击下一步。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

CardDAV Policy

1 Policy Info

2 Platforms

iOS

Mac OS X

3 Assignment

Policy Information

This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.

Account description *

Host name *

Port * 8443

Principal URL *

User name *

Password

Use SSL ON

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy Always

► Deployment Rules

Back Next >

配置以下设置：

- **帐户说明**：键入帐户说明。此字段为必填字段。
- **主机名**：键入 CardDAV 服务器的地址。此字段为必填字段。
- **端口**：键入连接到 CardDAV 服务器使用的端口。此字段为必填字段。默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的登录名称。此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为开。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在“删除密码”旁边，键入必需的密码。

配置 Mac OS X 设置

XenMobile
Analyze
Manage
Configure
⚙️ 🔍 admin ▾

Device Policies
Apps
Actions
ShareFile
Delivery Groups

CardDAV Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
- 3 Assignment

Policy Information

This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.

Account description*

Host name*

Port*

Principal URL*

User name*

Password

Use SSL

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy ▾

Profile scope ▾ OS X 10.7+

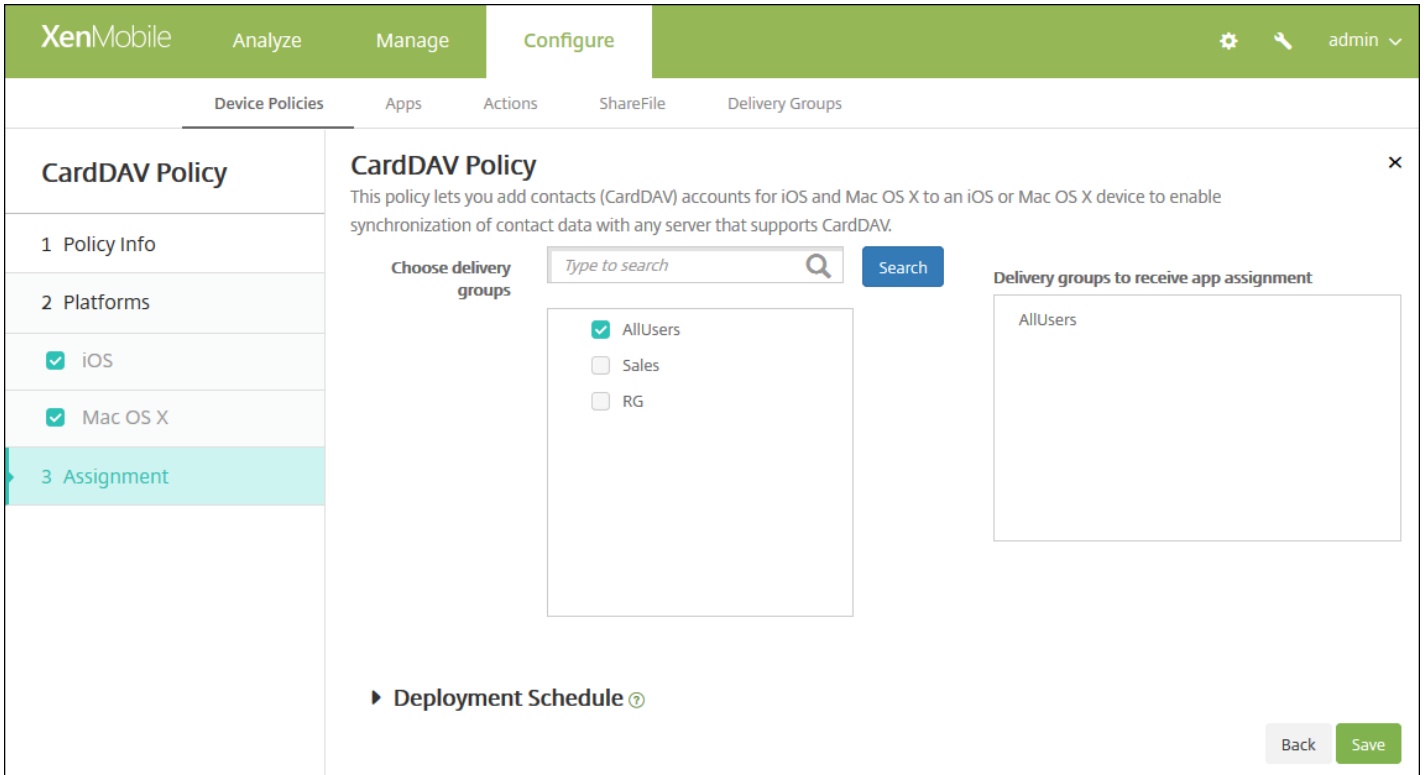
▶ **Deployment Rules**

配置以下设置：

- **帐户说明**：键入帐户说明。此字段为必填字段。
- **主机名**：键入 CardDAV 服务器的地址。此字段为必填字段。
- **端口**：键入连接到 CardDAV 服务器使用的端口。此字段为必填字段。默认值为 **8443**。
- **主体 URL**：键入用户日历的基本 URL。
- **用户名**：键入用户的登录名称。此字段为必填字段。
- **密码**：键入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到 CardDAV 服务器。默认值为开。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在“删除密码”旁边，键入必需的密码。
 - 在**配置文件作用域**旁边，单击**用户**或**系统**。默认值为用户。此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击下一步。此时将显示 **CardDAV 策略分配** 页面。



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

10. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

将应用程序复制到 Samsung 容器设备策略

Feb 27, 2017

可以指定将设备上已经安装的应用程序复制到受支持 Samsung 设备上的 SEAMS 容器或 KNOX 容器（有关受支持设备的信息，请参阅 Samsung 的 [Samsung KNOX Supported Devices](#)（Samsung KNOX 支持的设备）页面）。复制到 SEAMS 容器的应用程序在用户的主屏幕上可用；复制到 KNOX 容器的应用程序仅当用户登录 KNOX 容器时可用。

必备条件：

- 设备必须在 XenMobile 上注册。
- 必须部署 Samsung MDM 密钥（ELM 和 KLM）（有关操作方法，请参阅 Samsung MDM 许可证密钥设备策略）。
- 应用程序已经安装到设备上
- 在设备上初始化 KNOX 以将应用程序复制到 KNOX 容器。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。

2. 单击添加。此时将显示添加新策略对话框。

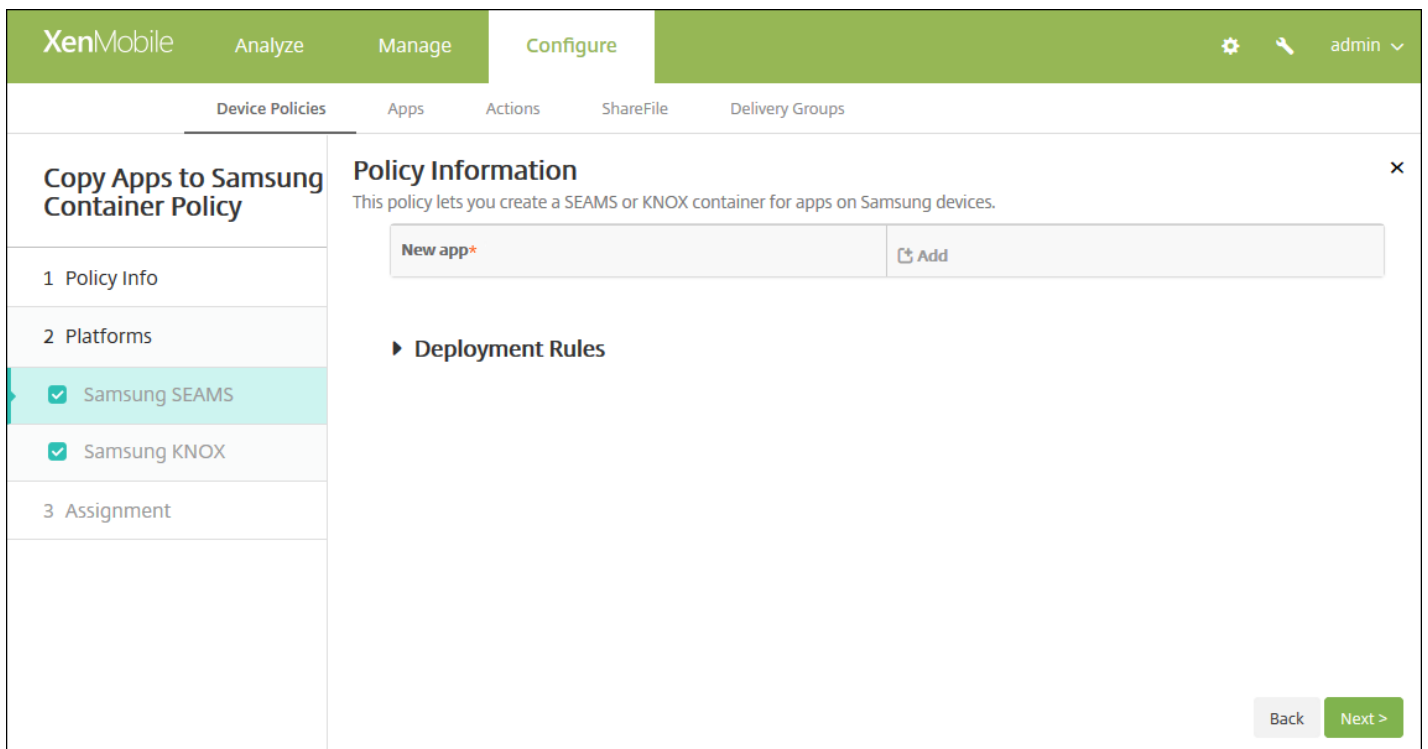
3. 展开更多，然后在安全性下方，单击将应用程序复制到 Samsung 容器。此时将显示将应用程序复制到 Samsung 容器策略信息页面。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Copy Apps to Samsung Container Policy' and 'Policy Information'. The description states: 'This policy lets you create a SEAMS or KNOX container for apps on Samsung devices.' There are two input fields: 'Policy Name*' and 'Description'. The 'Policy Name*' field is empty. The 'Description' field is a large text area, also empty. On the left side, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checked options: 'Samsung SEAMS' and 'Samsung KNOX'. At the bottom right of the main content area, there is a green 'Next >' button.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。



6. 在“平台”下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 8 以了解如何设置此平台的部署规则。

7. 为选择的每个平台配置以下设置。

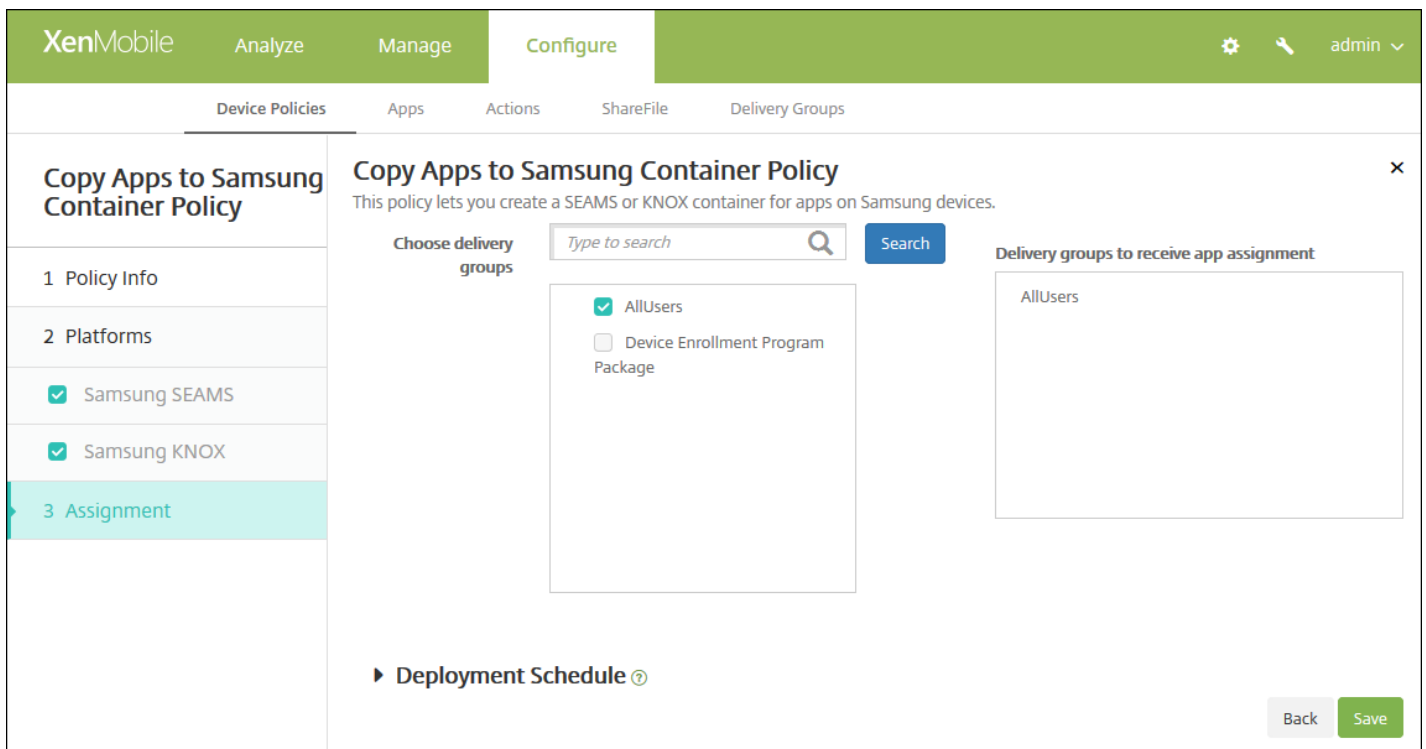
- **新建应用程序**：对于要添加到此列表中的每个应用程序，请单击**添加**，然后执行以下操作：
 - 键入包 ID，例如，对于 LacingArt 应用程序，请键入 com.mobiwolf.lacingart。
 - 单击**保存**或**取消**。

注意：要删除现有应用程序，请将鼠标悬停在包含此列表的行上，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。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

8. 配置部署规则

9. 单击**下一步**。此时将显示下一个平台页面或将应用程序复制到 **Samsung** 容器策略分配页面。



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

11. 展开部署计划，然后配置以下设置：

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

注意：

- 已在“设置”>“服务器属性”中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

12. 单击保存以保存此策略。

成功部署策略后，SEAMS 应用程序显示在设备详细信息页面上标题位置：企业 SEAMS 位置下方，KNOX 应用程序显示在标题位置：企业位置下方。

凭据设备策略

Feb 27, 2017

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

可以为 iOS、Mac OS X、Android、Android for Work、Windows Desktop/Tablet、Windows Mobile/CE 和 Windows Phone 设备创建凭据策略。每种平台需要一组不同的值，本文将对此进行介绍。

[iOS 设置](#)

[Mac OS X 设置](#)

[Android 和 Android for Work 设置](#)

[Windows Desktop/Tablet 设置](#)

[Windows Mobile/CE 设置](#)

[Windows Phone 设置](#)

创建此策略前，需要具有计划用于各平台的凭据信息，以及任何证书和密码。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**安全性**下方，单击**凭据**。此时将显示**凭据策略**信息页面。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

Credentials Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Android
 - Android for Work
 - Windows Phone
 - Windows Desktop/Tablet
 - Windows Mobile/CE
- 3 Assignment

Policy Information

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Policy Name*

Description

Next >

4. 在策略信息窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

The screenshot shows the XenMobile 'Configure' interface for a 'Credentials Policy'. The left sidebar lists platforms with checkboxes: iOS (checked), Mac OS X (checked), Android (checked), Android for Work (checked), Windows Phone (checked), Windows Desktop/Tablet (checked), and Windows Mobile/CE (checked). The main content area is titled 'Policy Information' and includes a description: 'This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' Below this are several configuration fields: 'Credential type' (set to 'Certificate (.cer, .crt, .der and .pem)'), 'Credential name' (empty), 'The credential file path' (empty) with a 'Browse' button, 'Policy Settings' (with 'Remove policy' set to 'Select date' and 'Duration until removal (in days)' set to an empty field), and 'Allow user to remove policy' (set to 'Always'). At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **凭据类型**：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
 - **证书**
 - **凭据名称**：输入凭据的唯一名称。
 - **凭据文件路径**：单击“浏览”并导航到凭据文件的位置，选择该文件。
 - **密钥库**
 - **凭据名称**：输入凭据的唯一名称。
 - **凭据文件路径**：单击“浏览”并导航到凭据文件的位置，选择该文件。
 - **密码**：输入凭据的密钥库密码。
 - **服务器证书**
 - **服务器证书**：在列表中，单击要使用的证书。
 - **凭据提供程序**
 - **凭据提供程序**：在列表中，单击凭据提供程序的名称。
- **策略设置**

- 在删除策略旁边，单击选择日期或删除前保留时间(天)。
- 如果单击选择日期，请单击日历以选择具体删除日期。
- 在允许用户删除策略列表中，单击始终、需要密码或从不。
- 如果单击需要密码，在删除密码旁边，键入必需的密码。

配置 Mac OS X 设置

Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Credential type: Certificate (.cer, .crt, .der and .pem)

Credential name*: [Text Input]

The credential file path: [Text Input] **Browse**

Policy Settings

Remove policy: Select date Duration until removal (in days)

Allow user to remove policy: Always

Profile scope: User OS X 10.7+

Deployment Rules

Back Next >

配置以下设置：

- **凭据类型**：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
 - **证书**
 - **凭据名称**：输入凭据的唯一名称。
 - **凭据文件路径**：单击浏览并导航到凭据文件的位置，选择该文件。
 - **密钥库**
 - **凭据名称**：输入凭据的唯一名称。
 - **凭据文件路径**：单击浏览并导航到凭据文件的位置，选择该文件。
 - **密码**：输入凭据的密钥库密码。
 - **服务器证书**
 - **服务器证书**：在列表中，单击要使用的证书。
 - **凭据提供程序**
 - **凭据提供程序**：在列表中，单击凭据提供程序的名称。
- **策略设置**
 - 在删除策略旁边，单击选择日期或删除前保留时间(天)。
 - 如果单击选择日期，请单击日历以选择具体删除日期。
 - 在允许用户删除策略列表中，单击始终、需要密码或从不。
 - 如果单击需要密码，在删除密码旁边，键入必需的密码。
 - 在 **Policy scope** (策略范围) 旁边，单击用户或系统。默认值为用户。此选项仅适用于 OS X 10.7 及更高版本。

配置 Android 和 Android for Work 设置

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Credentials Policy' and includes a sidebar with a list of platforms: iOS, Mac OS X, Android (highlighted), Android for Work, Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE. The main area contains a 'Credential type' dropdown menu set to 'Certificate (.cer, .crt, .der and .pem)', a text input field for 'The credential file path', and a 'Browse' button. Below this is a 'Deployment Rules' section. At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **凭据类型**：在列表中，单击要用于此策略的凭据类型，然后输入所选凭据的以下信息：
 - **证书**
 - **凭据名称**：键入凭据的唯一名称。
 - **凭据文件路径**：单击“浏览”并导航到凭据文件的位置，选择该文件。
 - **密钥库**
 - **凭据名称**：键入凭据的唯一名称。
 - **凭据文件路径**：单击浏览，然后导航到凭据文件的位置，选择此凭据文件。
 - **密码**：键入凭据的密钥库密码。
 - **服务器证书**
 - **服务器证书**：在列表中，单击要使用的证书。
 - **凭据提供程序**
 - **凭据提供程序**：在列表中，单击凭据提供程序的名称。

配置 Windows Desktop/Tablet 设置

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

- OS version* 10
- Certificate Type ROOT
- Store device root
- Location System
- Credential type Certificate (.cer, .crt, .der and .pem)
- Credential file path* Browse

► Deployment Rules

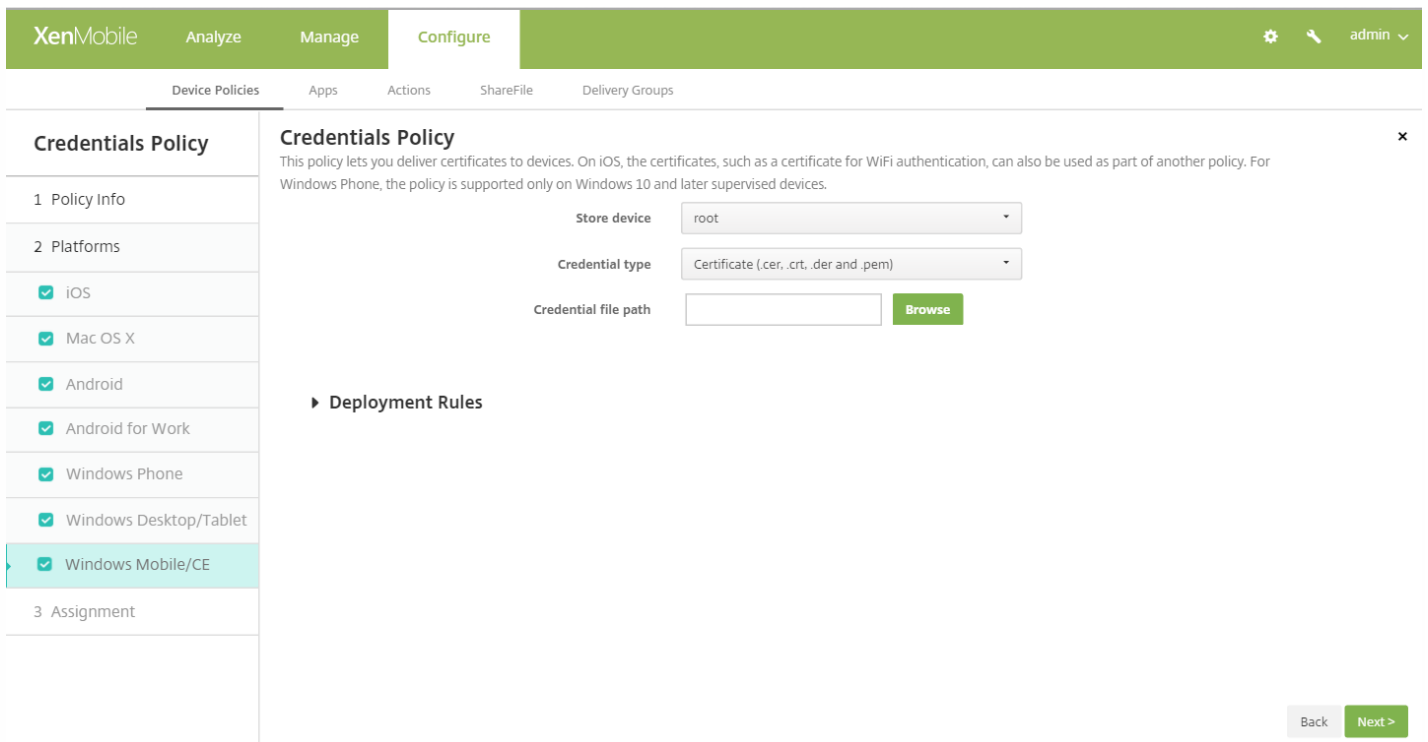
Back Next >

配置以下设置：

操作系统版本：在列表中，单击 **8.1** 以使用 Windows 8.1 或单击 **10** 以使用 Windows 10。默认值为 **10**。

- [Windows 10 设置](#) ▼
- [Windows 8.1 Phone 设置](#) ▼

配置 Windows Mobile/CE 设置



配置以下设置：

- **存储设备**：在列表中，单击凭据的证书存储位置。默认值为 **root**（根）。选项包括：
 - **特许执行信任颁发机构** - 使用属于此存储的证书签名的应用程序将在特许信任级别下运行。
 - **非特许执行信任颁发机构** - 使用属于此存储的证书签名的应用程序将在一般信任级别下运行。
 - **SPC(软件发行程序证书)** - 软件发行程序证书 (SPC) 用于签名 .cab 文件。
 - **root**（根） - 包含根证书或自签名证书的证书存储。
 - **CA** - 包含加密信息（包括中间证书颁发机构）的证书存储。
 - **MY**（我的） - 包含最终用户个人证书的证书存储。
- **凭据类型**：证书是适用于 Windows Mobile/CE 设备的唯一凭据类型。
- **凭据文件路径**：单击**浏览**并导航到凭据文件的位置，选择该文件。

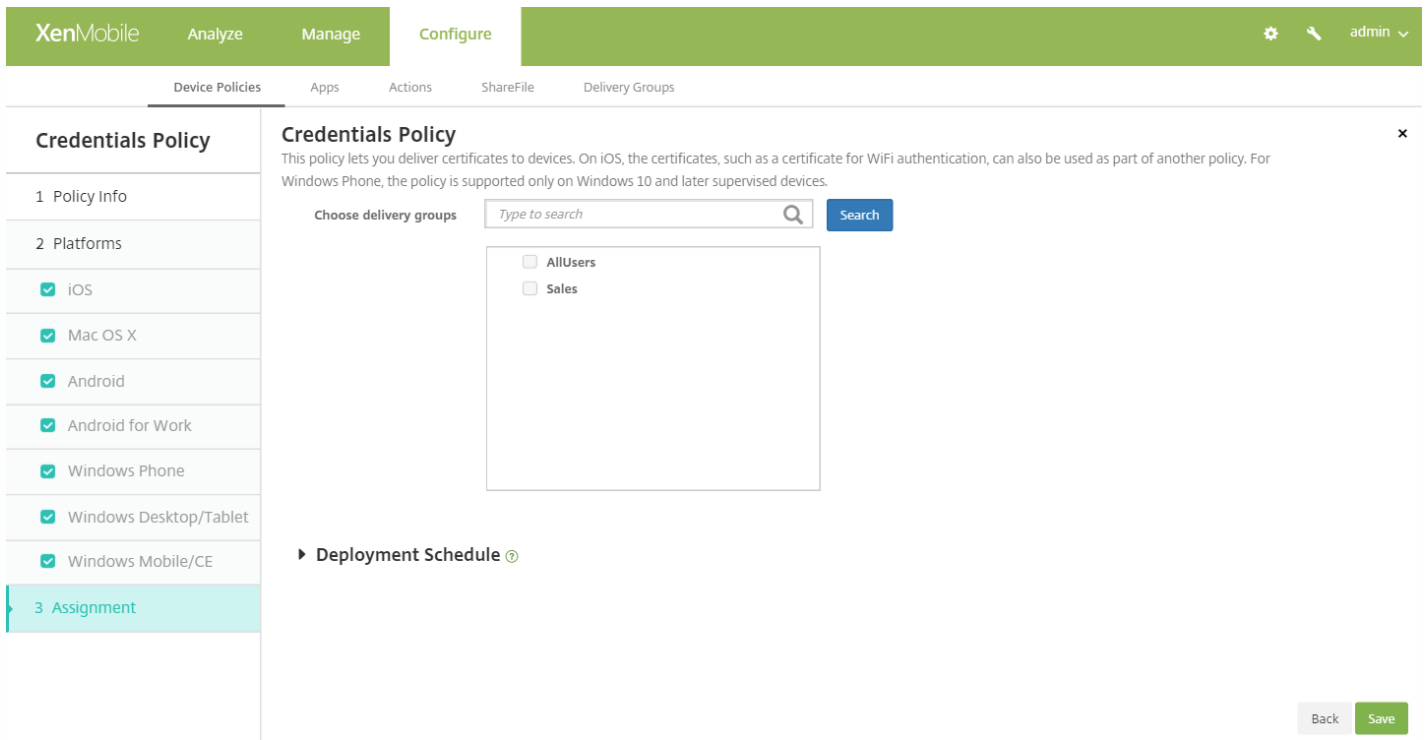
配置 Windows Phone 设置

配置以下设置：

- 证书类型：在列表中，单击根证书或客户端证书。
- 如果单击根证书，可以配置以下设置：
 - 存储设备：在列表中，单击 **root**（根）、**My**（我的）或 **CA** 以选择凭据的证书存储位置。**My**（我的）将证书存储在用户的证书存储中。
 - 位置：“系统”是适用于 Windows Phone 的唯一位置。
 - 凭据类型：“证书”是适用于 Windows Phone 的唯一凭据类型。
 - 凭据文件路径：单击浏览，导航到证书文件的位置，以选择此证书文件。
- 如果单击客户端证书，可以配置以下设置：
 - 位置：系统是适用于 Windows Phone 的唯一位置。
 - 凭据类型：密钥库是适用于 Windows Phone 的唯一凭据类型。
 - 凭据名称：键入凭据的名称。此字段为必填字段。
 - 凭据文件路径：单击浏览，导航到证书文件的位置，以选择此证书文件。
 - 密码：键入与凭据关联的密码。此字段为必填字段。

7. 配置部署规则

8. 单击下一步。此时将显示凭据策略分配页面。



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

10. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

自定义 XML 设备策略

Feb 27, 2017

如果需要在 Windows Phone、Windows Desktop/Tablet 和 Windows Mobile/CE 设备上自定义以下功能，可以在 XenMobile 中创建自定义 XML 策略：

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

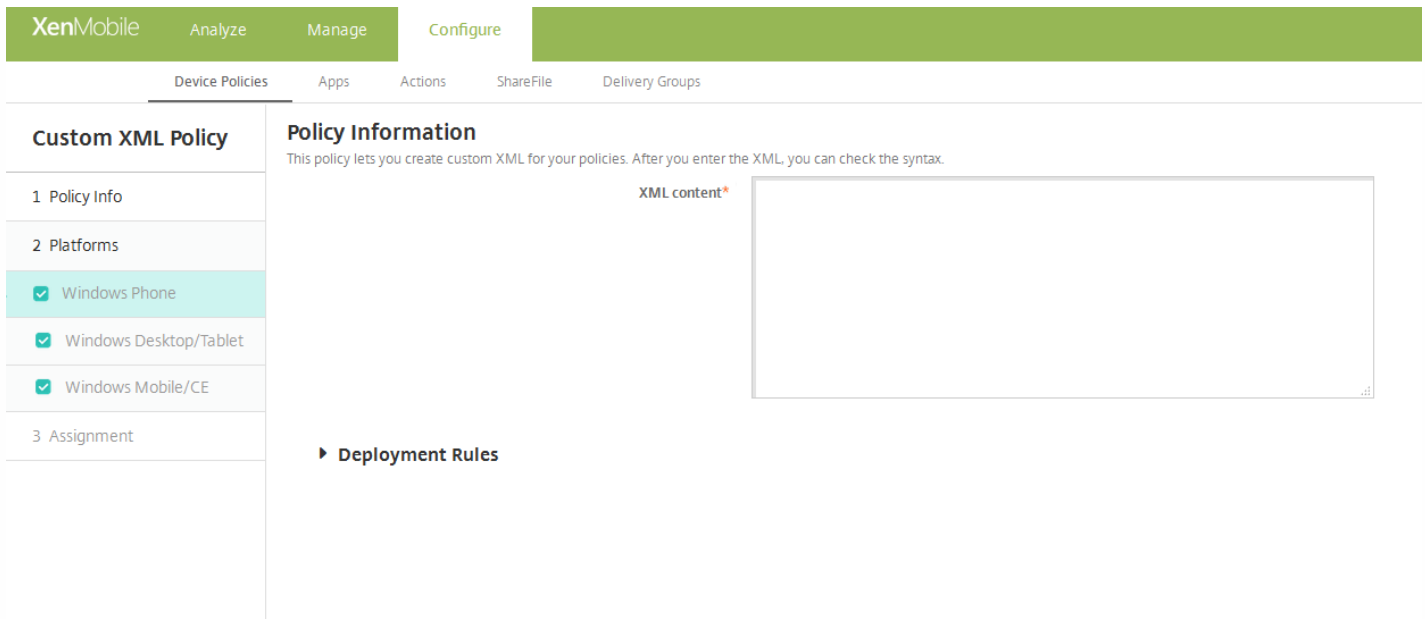
可以在 Windows 中使用 Open Mobile Alliance Device Management (OMA DM) API 创建自己的自定义 XML 配置。本主题中不介绍如何使用 OMA DM API 创建自定义 XML。有关使用 OMA DM API 的详细信息，请参阅 Microsoft Developer Network 站点上的 [OMA 设备管理](#)。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在自定义下方，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：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。



6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

7. 为选择的每个平台配置以下设置：

- **XML 内容**：键入或复制并粘贴要添加到策略的自定义 XML 代码。

8. 配置部署规则

9. 单击下一步。XenMobile 检查 XML 内容语法。内容框下将显示所有语法错误。必须先修复所有错误才能继续。

如果没有语法错误，将显示自定义 **XML 策略** 分配页面。

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

11. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。
- 配置的部署计划对所有平台相同。您做出的任何更改都会应用到所有平台。

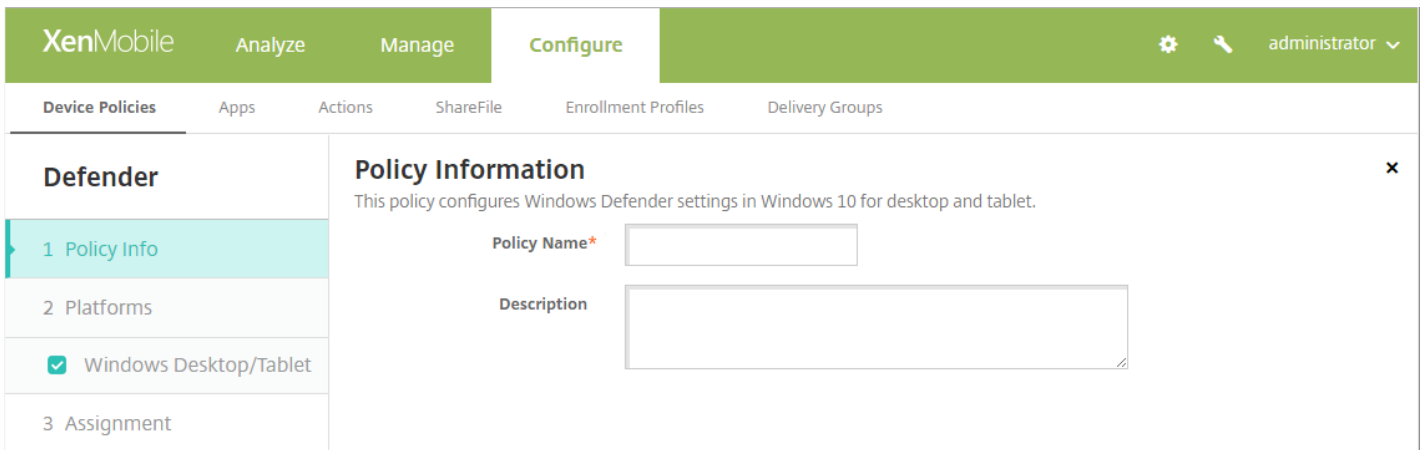
12. 单击保存。

Defender 设备策略

Feb 27, 2017

Windows Defender 是 Windows 10 附带的恶意软件防护功能。可以使用 XenMobile 设备策略 Defender 来为台式机和平板电脑配置适用于 Windows 10 的 Microsoft Defender 策略。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 开始键入 **Defender**，然后在搜索结果中单击该名称。此时将显示 **Defender 策略信息** 页面。

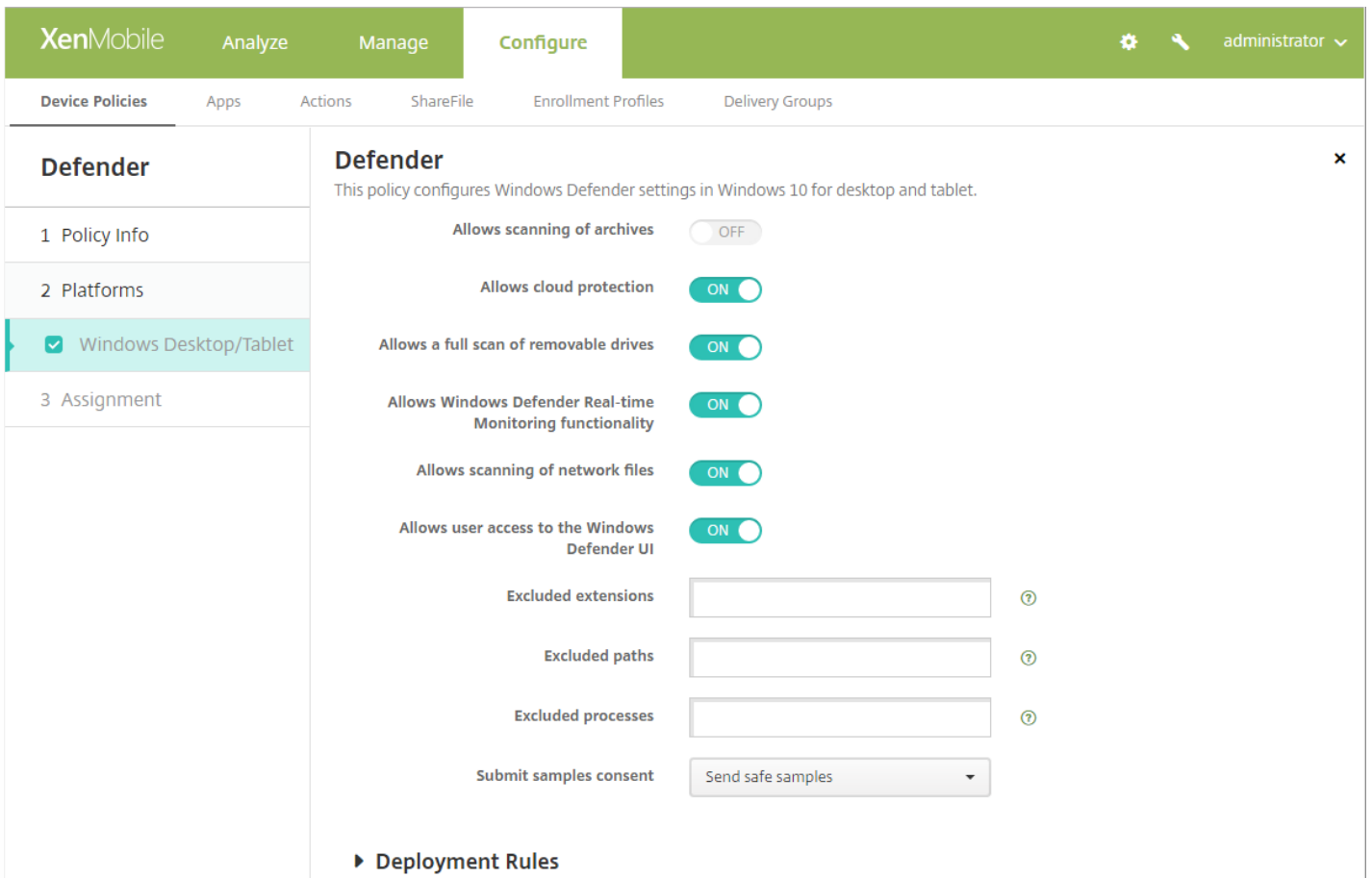


The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. On the left side, there is a sidebar with the title 'Defender' and three items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' item is selected. The main content area is titled 'Policy Information' and contains the following text: 'This policy configures Windows Defender settings in Windows 10 for desktop and tablet.' Below this text, there are two input fields: 'Policy Name*' and 'Description'. The 'Policy Name*' field is empty, and the 'Description' field is also empty. The 'Policy Name*' field has a small asterisk next to it. The 'Description' field has a small icon in the bottom right corner. In the top right corner of the console, there are icons for settings, search, and a user profile dropdown labeled 'administrator'.

4. 在策略信息窗格中，键入以下信息：

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

5. 单击下一步。此时将显示策略平台页面。



配置以下设置：

- 允许扫描存档：允许或不允许 Defender 扫描存档的文件。默认值为关。
- 允许启用云保护：允许或不允许 Defender 向 Microsoft 发送有关恶意软件活动的信息。默认值为开。
- 允许完全扫描可移动驱动器：允许或不允许 Defender 扫描可移动驱动器，例如 U 盘。默认值为开。
- 允许启用 **Windows Defender 实时监视功能**：默认值为开。
- 允许扫描网络文件：允许或不允许 Defender 扫描网络文件。默认值为开。
- 允许用户访问 **Windows Defender UI**：指定用户是否可以访问 Windows Defender 用户界面。此设置在下次启动用户设备时生效。如果此设置为关，则用户不会收到任何 Windows Defender 通知。默认值为开。
- 排除的扩展名：要从实时扫描或计划的扫描中排除的扩展名。要分隔扩展名，请使用 | 字符。例如，“lib | obj”。
- 排除的路径：要从实时扫描或计划的扫描中排除的路径。要分隔路径，请使用 | 字符。例如，“C:\Example | C:\Example1”。
- 排除的进程：要从实时扫描或计划的扫描中排除的进程。要分隔进程，请使用 | 字符。例如，“C:\Example.exe | C:\Example1.exe”。
- 提交示例许可：控制是否向 Microsoft 发送可能需要进一步分析以确定是否是恶意的文件。选项：**始终提示**、**发送安全示例**、**从不发送**、**发送所有示例**。默认设置为**发送安全示例**。

6. 配置部署规则

7. 单击下一步。此时将显示 **Defender** 分配页面。

8. 在**选择交付组**旁边，键入以查找交付组。要将策略分配到一个或多个组，请在列表中选择组。选择的组显示在**用于接收应用程序分配的交付组**列表中。

9. 展开部署计划，然后配置以下设置：

- 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。如果单击关，则其他选项不适用。
- 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。

10. 单击保存以保存此策略。

删除文件和文件夹设备策略

Feb 27, 2017

可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的文件或文件夹。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在应用程序下面，单击删除文件和文件夹。此时将显示删除文件和文件夹策略信息页面。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

Delete Files and Folders Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows you to specify which files and folders need to be deleted.

Policy Name*

Description

Next >

4. 在策略信息窗格中，键入以下信息：

- 策略名称：键入策略的描述性名称。
- 说明：键入策略的可选说明。

5. 单击下一步。此时将显示 Windows Mobile/CE 平台页面。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

Delete Files and Folders Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows you to specify which files and folders need to be deleted.

Files and folders to delete

Path*	Type	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Deployment Rules

Back Next >

6. 配置以下设置：

- 要删除的文件和文件夹：对于要删除的每个文件或文件夹，单击“添加”，然后执行以下操作：

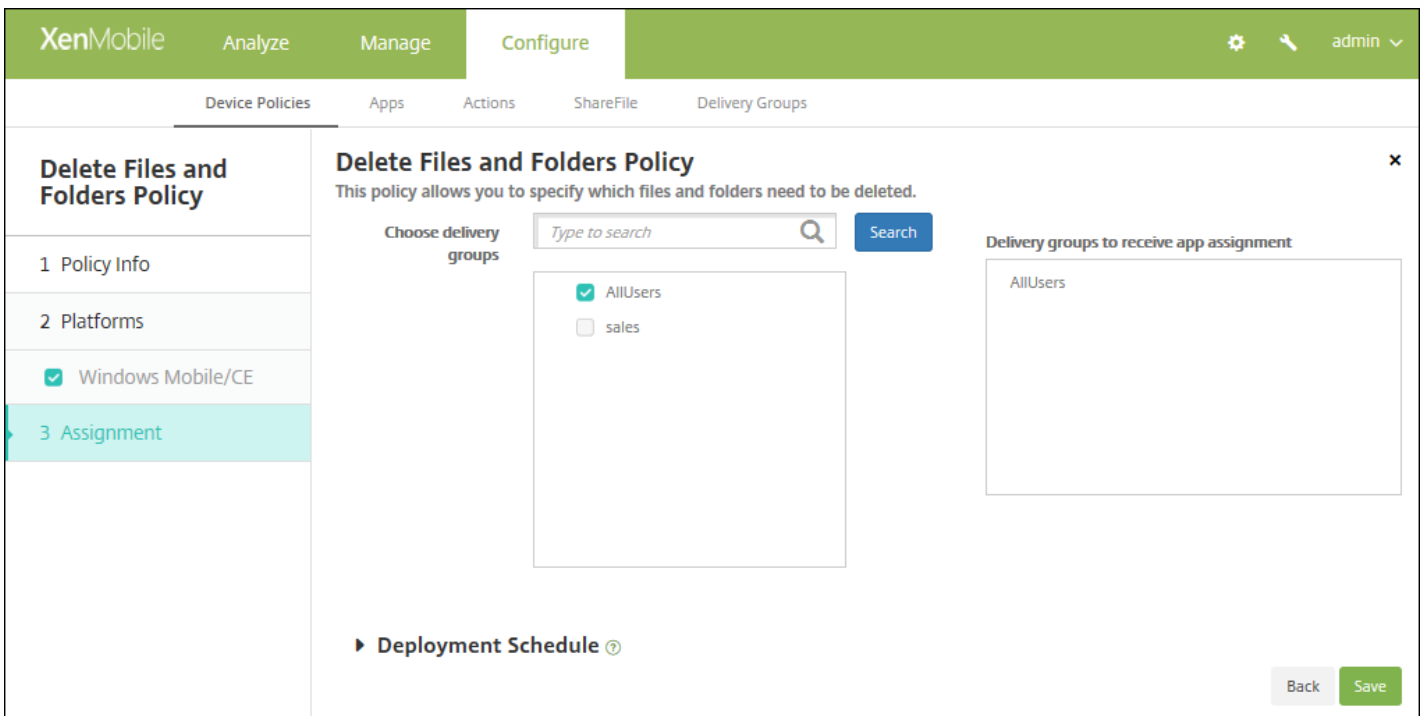
- **路径**：键入文件或文件夹的路径。
- **类型**：在列表中，单击“文件”或“文件夹”。默认值为“文件”。
- 单击**保存**将保存此文件或文件夹，或单击**取消**不保存此文件夹或文件夹。

注意：要删除现有列表，请将鼠标悬停在包含此列表的行上，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**以保留列表。

要编辑现有列表，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击下一步。此时将显示**删除文件和文件夹策略分配**页面。



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

10. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS。

11. 单击保存。

删除注册表项和值设备策略

Feb 27, 2017

可以在 XenMobile 中创建一个策略，用于从 Windows Mobile/CE 设备删除特定的注册表项和值。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在应用程序下方，单击删除注册表项和值。此时将显示删除注册表项和值信息页面。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

Delete Registry Keys and Values Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

Policy Information

This policy allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key.

Policy Name*

Description

Next >

4. 在策略信息窗格中，键入以下信息：

- 策略名称：键入策略的描述性名称。
- 说明：键入策略的可选说明。

5. 单击下一步。此时将显示 Windows Mobile/CE 平台页面。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

Delete Registry Keys and Values Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

Policy Information

This policy allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key.

Registry keys and values to delete

Key*	Value	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Deployment Rules

Back Next >

6. 配置以下设置：

- 要删除的注册表项和值：对于要删除的每个注册表项和值，单击添加，然后执行以下操作：

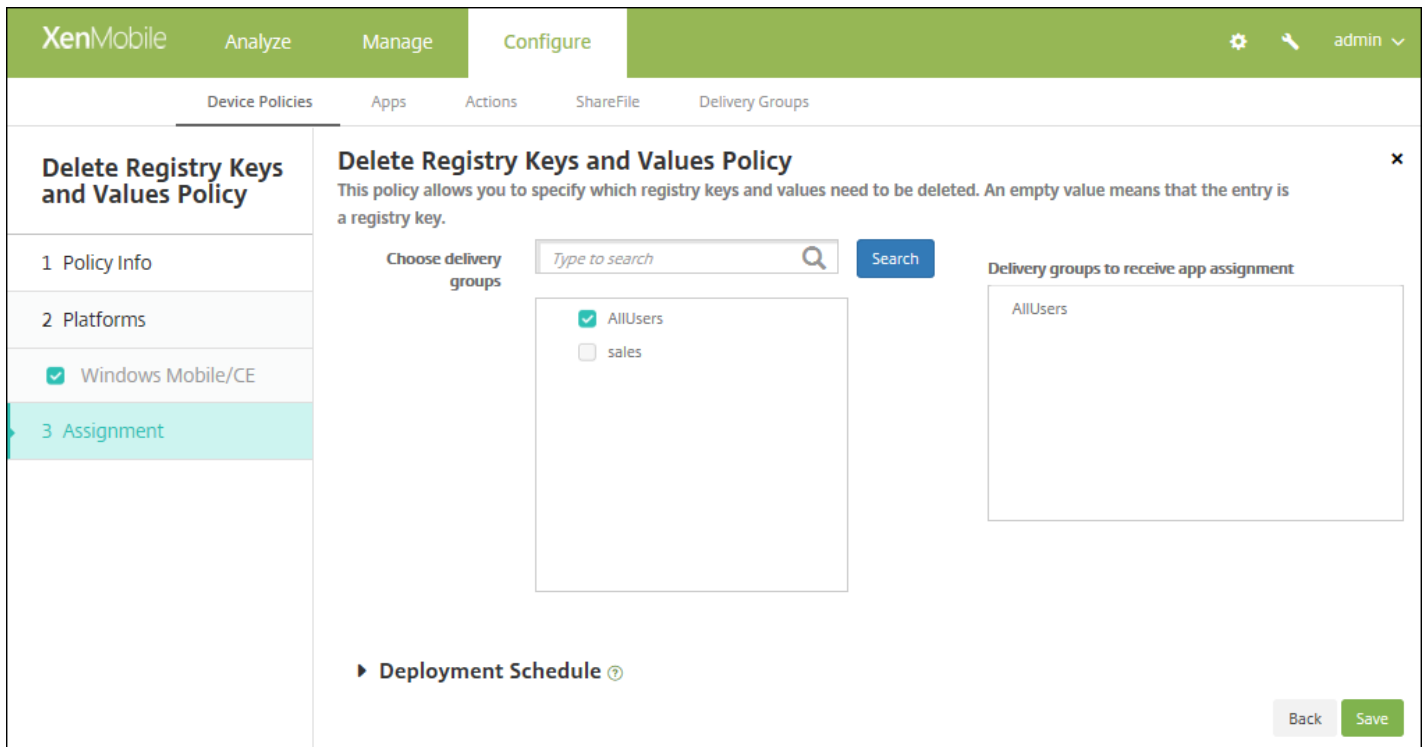
- **注册表项**：键入注册表项路径。这是必填字段。注册表项路径应以 HKEY_CLASSES_ROOT\ 或 HKEY_CURRENT_USER\ 或 HKEY_LOCAL_MACHINE\ 或 HKEY_USERS\ 开头。
- **值**：键入要删除的值名称，或让此字段留空以删除整个注册表项。
- 单击**保存**以保存此注册表项和值，或单击**取消**不保存此注册表项和值。

注意：要删除现有列表，请将鼠标悬停在包含此列表的行上，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**以保留列表。

要编辑现有列表，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击下一步。此时将显示**删除注册表项和值策略**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。

设备运行状况证明设备策略

Feb 27, 2017

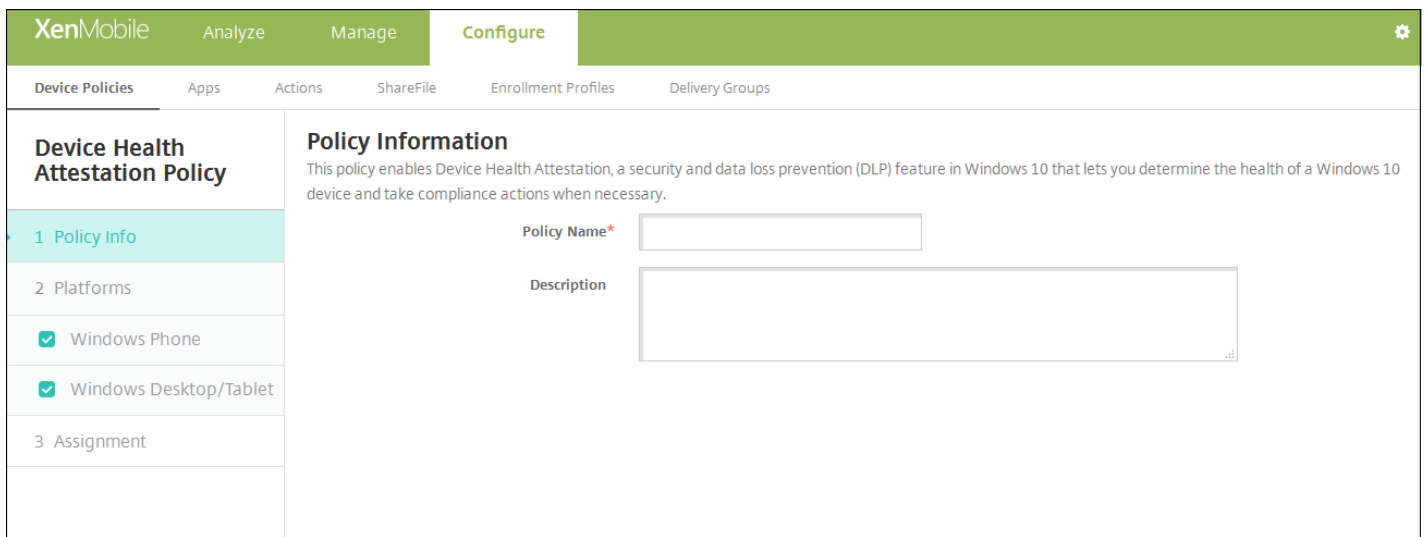
在 XenMobile 中，您可以要求 Windows 10 设备报告其运行状况，方法是让这些设备将特定数据和运行时信息发送给 Health Attestation Service (HAS) 进行分析。HAS 创建并返回运行状况证明证书，然后，设备将此证书发送给 XenMobile。XenMobile 收到运行状况证明证书后，根据运行状况证明证书的内容，部署您之前设置的自动操作。

HAS 验证的数据包括：

- AIK 是否存在
- Bit Locker 状态
- 启动调试是否已启用
- 启动管理器修订列表版本
- 代码完整性是否已启用
- 代码完整性修订列表版本
- DEP 策略
- ELAM 驱动程序是否已加载
- 颁发时间
- 内核调试是否已启用
- PCR
- 重置计数
- 重新启动计数
- 安全模式是否已启用
- SBCP 哈希
- 安全启动是否已启用
- 测试签名是否已启用
- 已启用 VSM
- 已启用 WinPE

有关详细信息，请参阅 Microsoft [HealthAttestation CSP](#) 页面。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**添加新策略。此时将显示**添加新策略**对话框。
3. 单击**更多**，然后在自定义下方，单击**设备运行状况证明策略**。此时将显示**设备运行状况证明策略**信息页面。



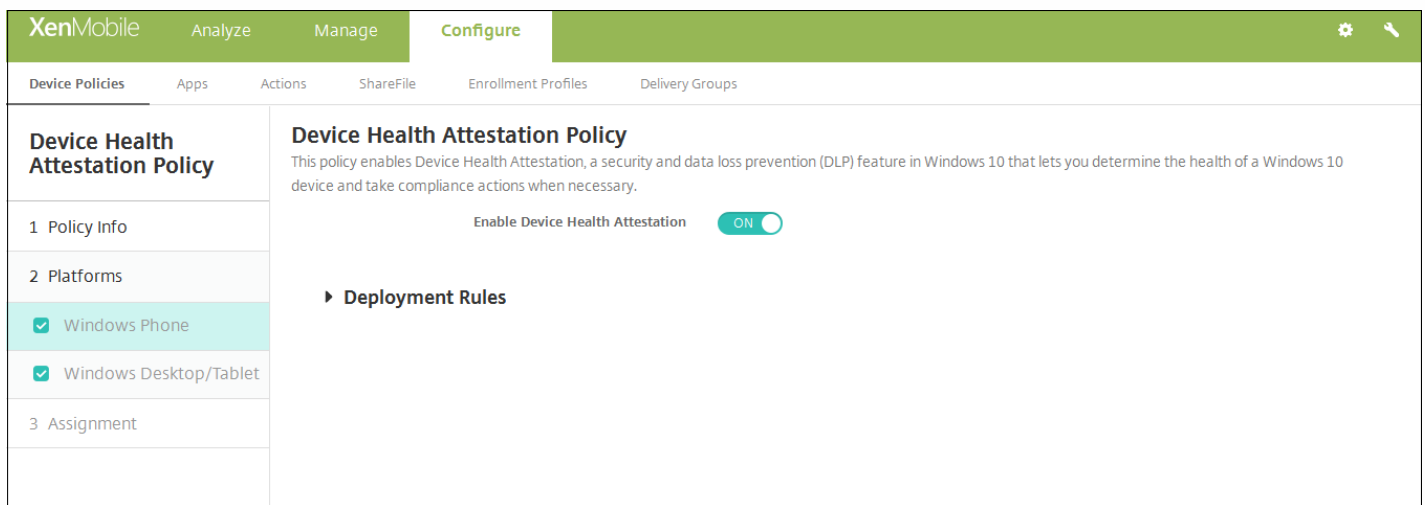
4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

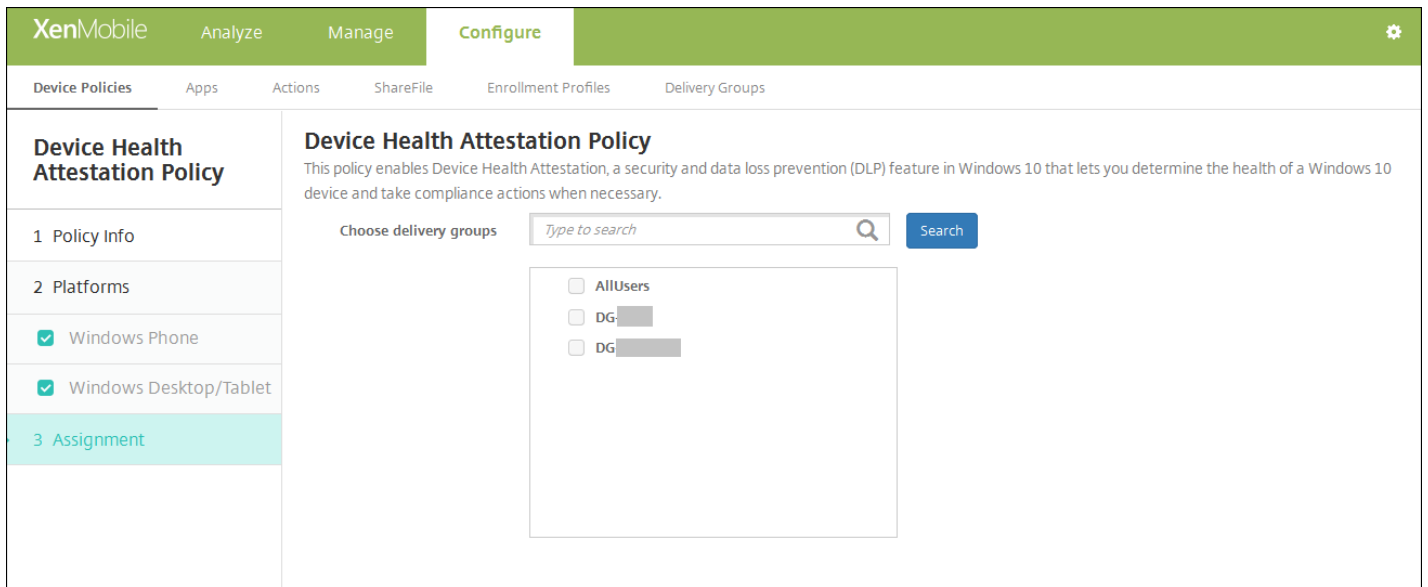


为您选择的各个平台配置此设置：

- **启用设备运行状况证明**：选择是否需要设备运行状况证明。默认值为关。

7. 配置部署规则

8. 单击下一步。此时将显示设备运行状况证明策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

设备名称设备策略

Feb 27, 2017

可以在 iOS 和 Mac OS X 设备上设置名称，以便轻松识别设备。可以使用宏、文本或二者的组合定义设备的名称。例如，要将设备名称设置为设备的序列号，可以使用 `${device.serialnumber}`。要将设备的名称设置为用户名和域的组合，可以使用 `${user.username}@example.com`。有关宏的详细信息，请参阅 [XenMobile 中的宏](#)。

1. 在 XenMobile 控制台中，单击 **配置 > 设备策略**。此时将显示 **设备策略** 页面。
2. 单击 **添加**。此时将显示 **添加新策略** 页面。
3. 展开 **更多**，然后在 **最终用户** 下方，单击 **设备名称**。此时将显示 **设备名称策略** 信息页面。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Device Name Policy' and contains a 'Policy Information' section with a description: 'This policy lets you apply a name on a supervised device on iOS and Mac OS X devices. Available in iOS 8 and later.' Below this are two input fields: 'Policy Name*' and 'Description'. To the left, there is a sidebar with a 'Platforms' section containing checkboxes for 'iOS' and 'Mac OS X', both of which are checked. At the bottom right, there is a 'Next >' button.

4. 在策略信息窗格中，键入以下信息：

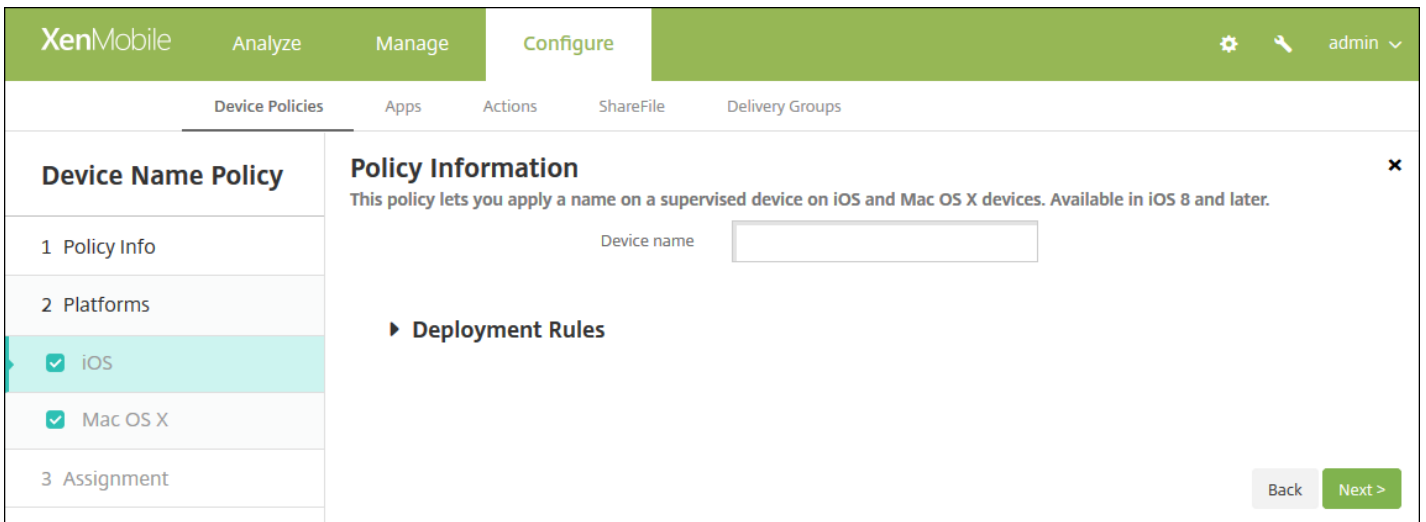
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击 **下一步**。此时将显示 **策略平台** 页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 和 Mac OS X 设置

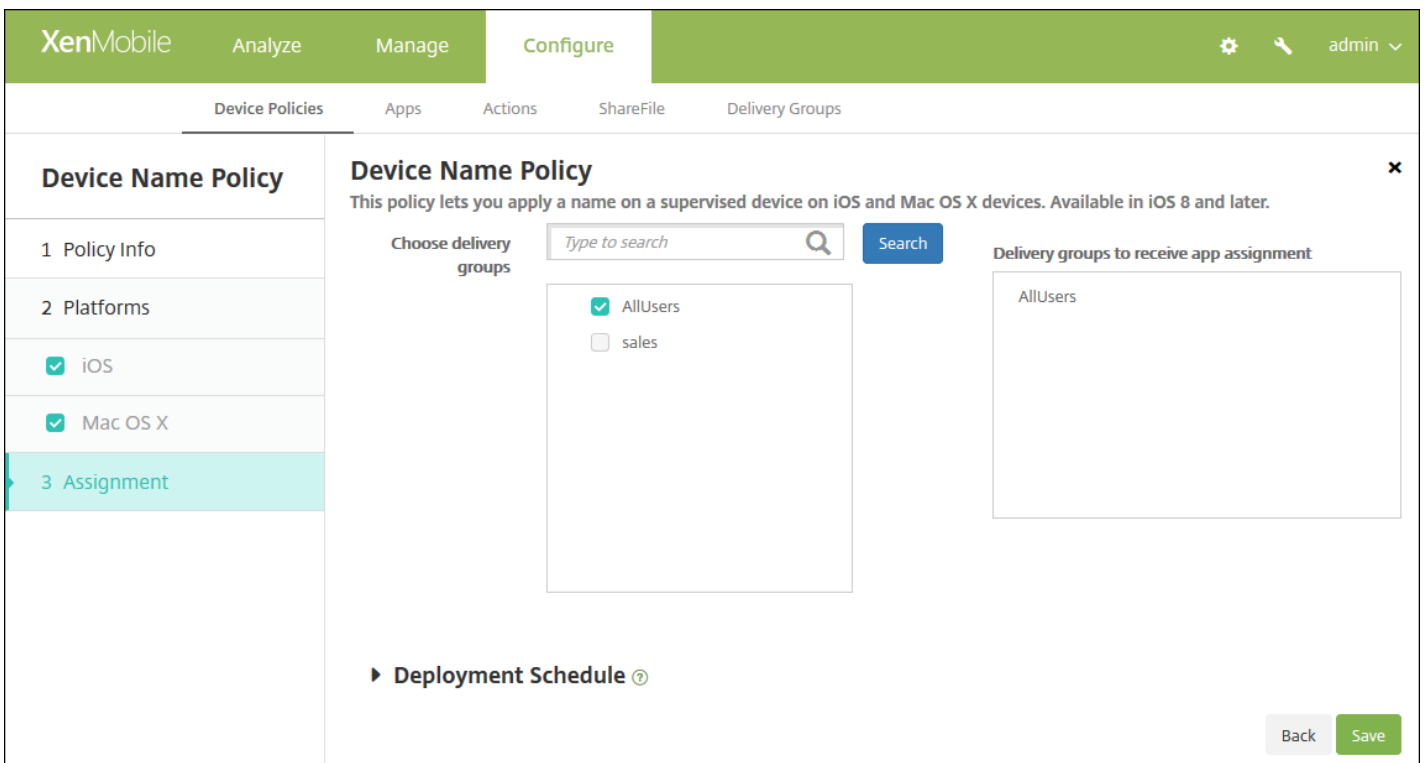


为您选择的平台配置此设置：

- **设备名称**：键入宏、宏的组合或宏和文本的组合，为每个设备设置唯一名称。例如，使用 `${device.serialnumber}` 将设备名称设置为每个设备的序列号，或使用 `${device.serialnumber} ${user.username}` 使设备名称中包含用户名。

7. 配置部署规则

8. 单击下一步。此时将显示设备名称策略分配页面。



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

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。

企业中心设备策略

Feb 27, 2017

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

需要具备以下各项才能创建策略：

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

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

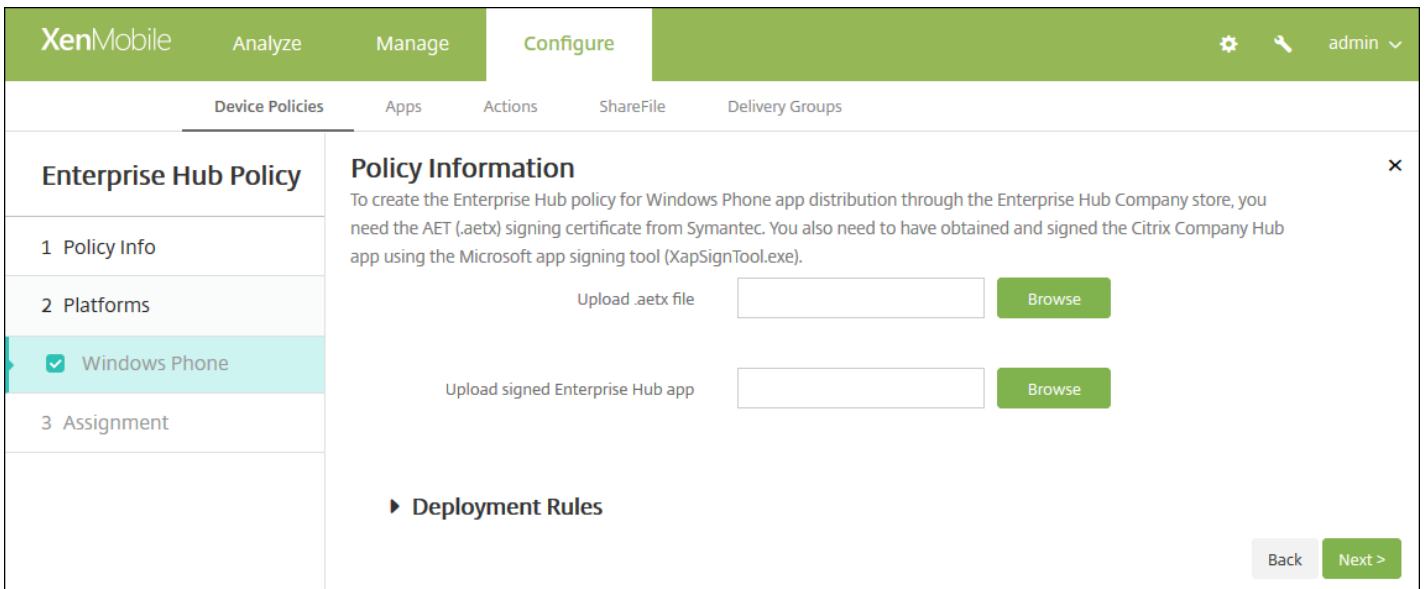
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在 **XenMobile Agent** 下方单击**企业中心**。此时将显示**企业中心策略**页面。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Enterprise Hub Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is selected. The main content area is titled 'Policy Information' and contains a text box for 'Policy Name*' and a larger text box for 'Description'. A 'Next >' button is located at the bottom right of the main content area.

4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。此时将显示 **Windows Phone** 平台页面。

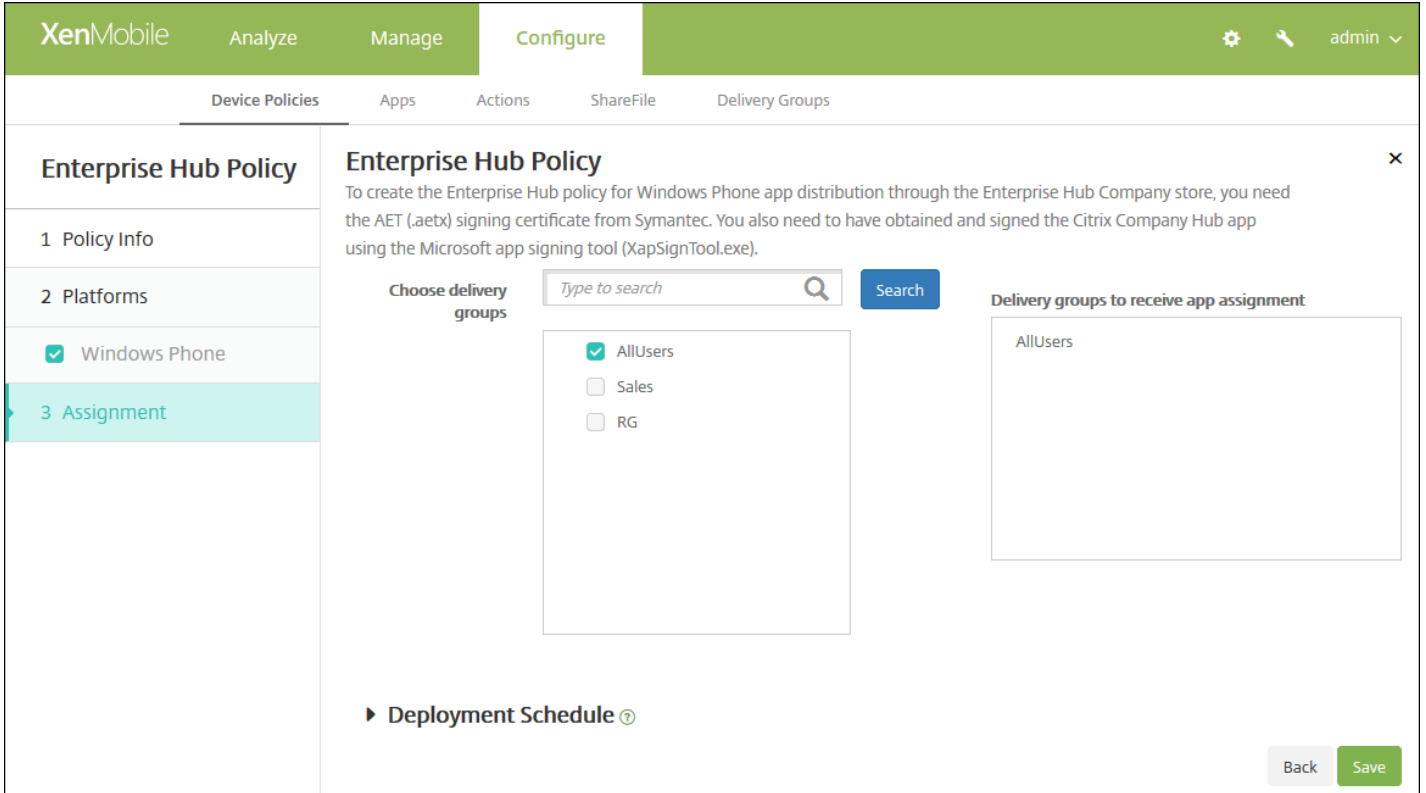


6. 配置以下设置：

- 上载 .aetx 文件：单击浏览并导航到 .aetx 文件的位置，选择该文件。
- 上载签名的企业中心应用程序：单击浏览并导航到企业中心应用程序的位置，选择此应用程序。

7. 配置部署规则

8. 单击下一步。此时将显示企业中心策略分配页面。



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

10. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

文件设备策略

Feb 27, 2017

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

利用此策略可以添加以下文件类型：

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

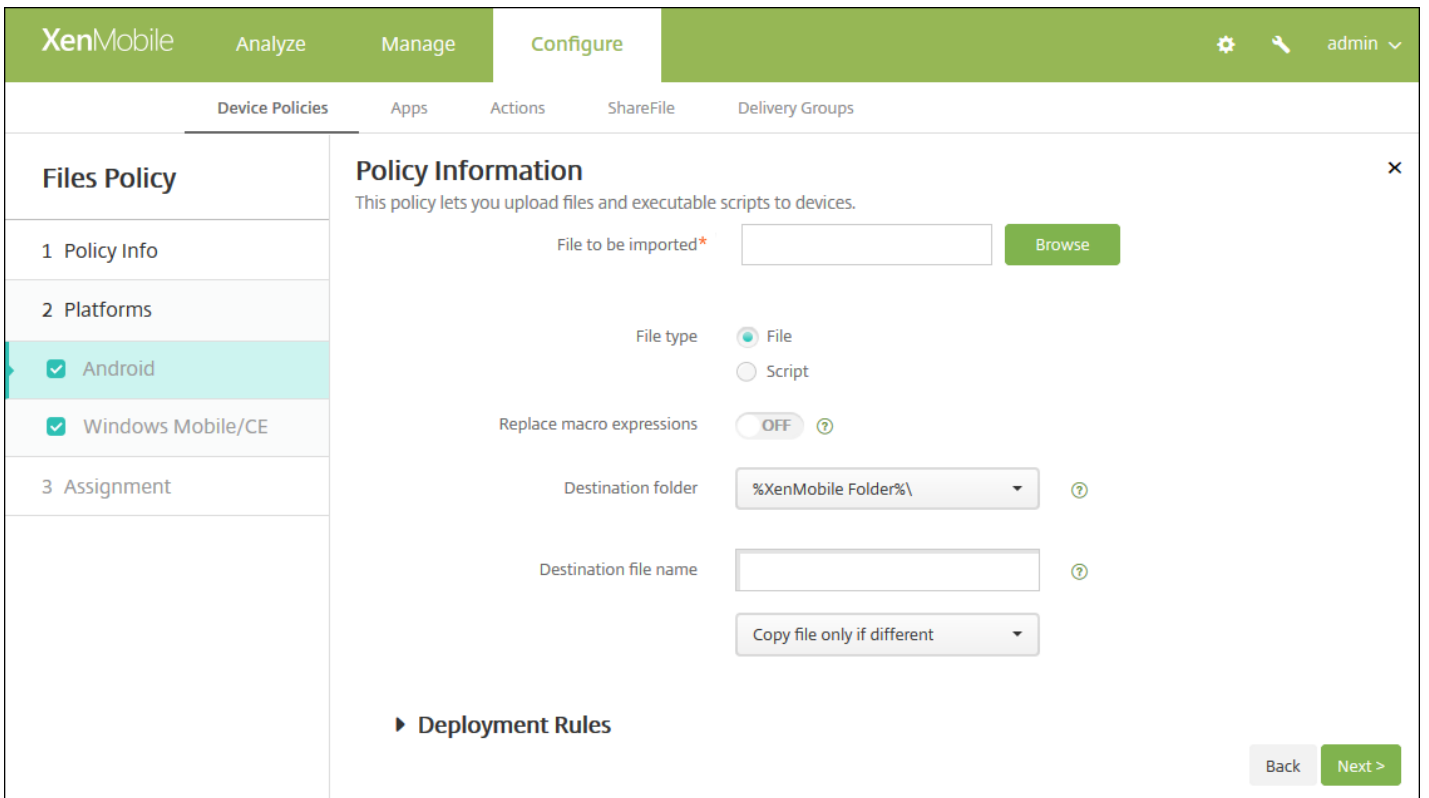
1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在应用程序下方，单击文件。此时将显示文件策略信息页面。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure' (highlighted). Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' tab is active, showing a 'Files Policy' configuration page. The page has a sidebar with three sections: '1 Policy Info' (highlighted), '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checked checkboxes: 'Android' and 'Windows Mobile/CE'. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you upload files and executable scripts to devices.' Below the description are two input fields: 'Policy Name*' (a text box) and 'Description' (a larger text area). A 'Next >' button is located at the bottom right of the form.

4. 在策略信息窗格中，输入以下信息：

- 策略名称：键入策略的描述性名称。
- 说明：（可选）键入策略的说明。

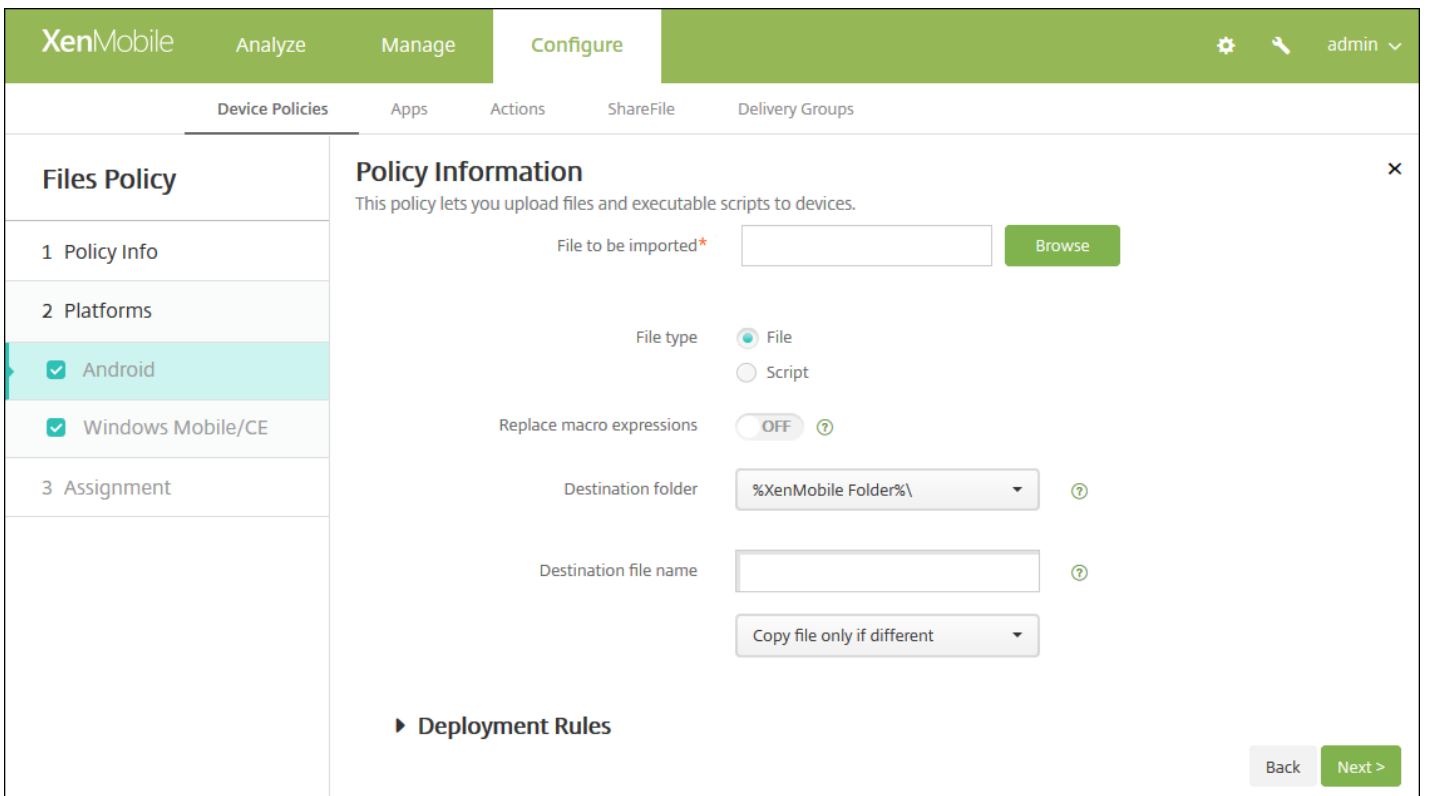
5. 单击下一步。此时将显示策略平台页面。



6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 Android 设置



配置以下设置：

- **要导入的文件**：单击“浏览”并导航到要导入的文件的位置，选择该文件。
- **文件类型**：选择文件或脚本。如果选择脚本，将显示立即执行。选择是否在上载文件后立即执行脚本。默认值为关。
- **替换宏表达式**：选择是否将脚本中的宏令牌名称替换为设备或用户属性。默认值为关。
- **目标文件夹**：在列表中，选择存储已上载文件的位置，或单击**新增**选择未列出的文件位置。此外，还可以使用宏 %XenMobile Folder%\ 或 %Flash Storage%\ 作为路径标识符的开头。
- **目标文件夹名**：（可选）如果必须在部署到设备上之前更改文件名，请键入一个不同名称。
- **仅在不同时复制文件**：在列表中，选择是否仅在与现有文件存在差异时复制文件。默认值为仅在文件存在差异时复制文件

配置 Windows Mobile/CE 设置

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure' (selected). Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Files Policy' and includes a sidebar with '1 Policy Info', '2 Platforms' (with 'Android' and 'Windows Mobile/CE' checked), and '3 Assignment'. The 'Policy Information' section contains the following settings:

- File to be imported*: [Text input field] [Browse button]
- File type: File, Script
- Replace macro expressions: OFF [Help icon]
- Destination folder: %My Documents%\ [Dropdown menu]
- Destination file name: [Text input field] [Help icon]
- Copy file only if different: [Dropdown menu]
- Read only file: OFF
- Hidden file: OFF

At the bottom, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

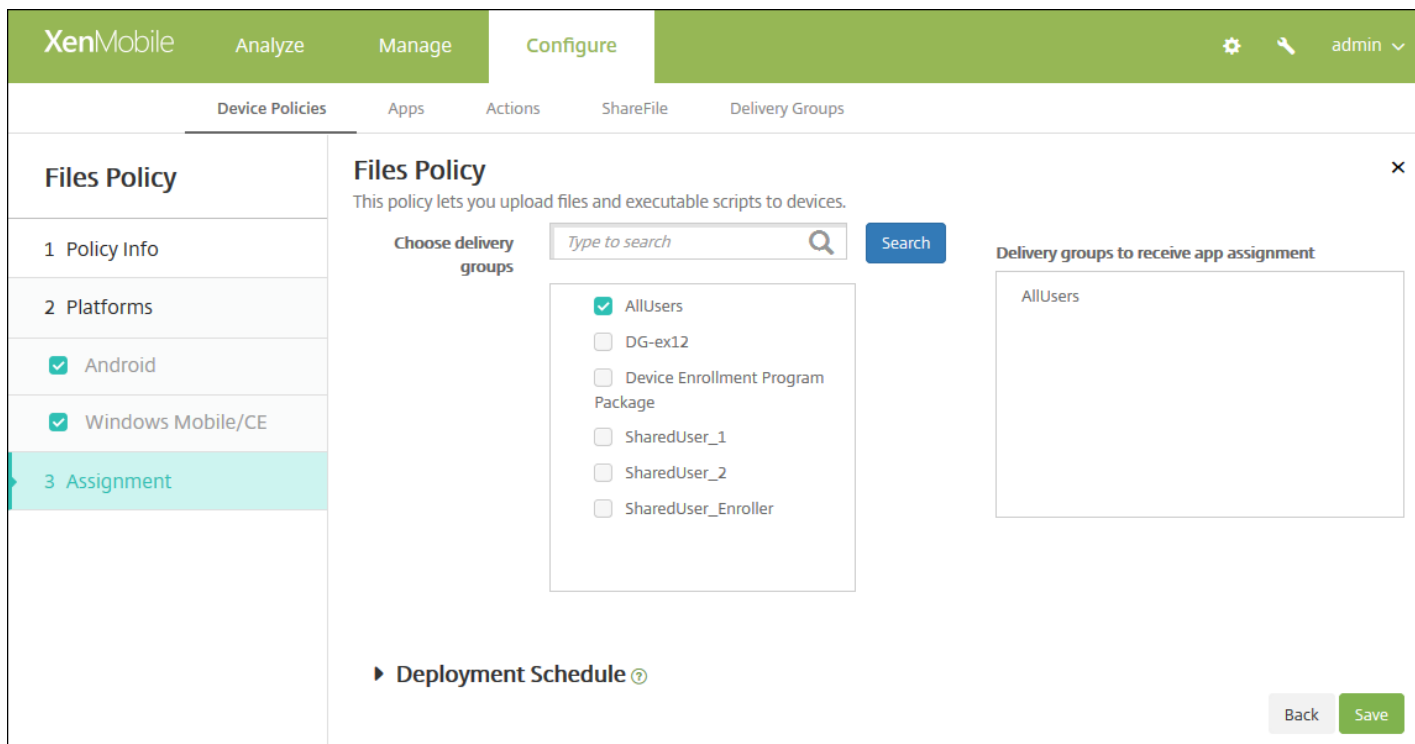
配置以下设置：

- **要导入的文件**：单击“浏览”并导航到要导入的文件的位置，选择该文件。
- **文件类型**：选择文件或脚本。如果选择脚本，将显示立即执行。选择是否在上载文件后立即执行脚本。默认值为关。
- **替换宏表达式**：选择是否将脚本中的宏令牌名称替换为设备或用户属性。默认值为关。
- **目标文件夹**：在列表中，选择存储已上载文件的位置，或单击**新增**选择未列出的文件位置。此外，还可以使用以下宏作为路径标识符的开头：
 - %Flash Storage%\
 - %XenMobile Folder%\

- %Program Files%\
- %My Documents%\
- %Windows%\
- 目标文件夹名：（可选）如果必须在部署到设备上之前更改文件名，请键入一个不同名称。
- 仅在不同时复制文件：在列表中，选择是否仅在与现有文件存在差异时复制文件。默认值为仅在文件存在差异时复制文件
- 只读文件：选择文件是否为只读文件。默认值为关。
- 隐藏文件：选择文件是否显示在文件列表中。默认值为关。

7. 配置部署规则

8. 单击下一步。将显示文件策略分配页面。



9. 在选择交付组旁边，键入以查找交付组，或在列表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。

字体设备策略

Feb 27, 2017

可以在 XenMobile 中添加一个设备策略，以向用户的 iOS 和 Mac OS X 设备添加其他字体。字体必须是 TrueType (.ttf) 或 OpenType (.oft) 字体。不支持字体集合 (.ttc 或 .otc)。

注意：对于 iOS，此策略仅适用于 iOS 7.0 及更高版本。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**最终用户**下方，单击**字体**。此时将显示**字体策略**页面。

The screenshot shows the XenMobile configuration interface for a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Font Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you add additional fonts to an iOS and Mac OS X device. The policy is available on iOS 7 and later devices.' Below the description are two input fields: 'Policy Name*' (with a red asterisk indicating it is required) and 'Description'. The 'Policy Name*' field is currently empty. The 'Description' field is a large text area. To the left of the 'Policy Information' section, there is a sidebar with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checkboxes: 'iOS' and 'Mac OS X', both of which are checked. At the bottom right of the page, there is a green 'Next >' button.

4. 在策略信息窗格中，输入以下信息：

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

5. 单击**下一步**。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

The screenshot shows the XenMobile configuration interface for a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Font Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms' (with 'iOS' and 'Mac OS X' selected), and '3 Assignment'. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you add additional fonts to an iOS and Mac OS X device. The policy is available on iOS 7 and later devices.' Below this, there are input fields for 'User-visible name' and 'Font file*' with a 'Browse' button. The 'Policy Settings' section includes radio buttons for 'Remove policy' (with 'Select date' selected) and 'Duration until removal (in days)', a date picker, and a dropdown for 'Allow user to remove policy' set to 'Always'. At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- 用户可见名称：键入用户在其字体列表中看到的名称。
- 字体文件：单击浏览，然后导航到要添加到用户设备的字体文件的位置，选择该文件。
- 策略设置
 - 在删除策略旁边，单击选择日期或删除前保留时间(天)。
 - 如果单击选择日期，请单击日历以选择具体删除日期。
 - 在允许用户删除策略列表中，单击始终、需要密码或从不。
 - 如果单击需要密码，在删除密码旁边，键入必需的密码。

配置 Mac OS X 设置

The screenshot shows the XenMobile configuration interface for a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows 'Font Policy' with sub-sections: '1 Policy Info', '2 Platforms' (with 'iOS' and 'Mac OS X' checked), and '3 Assignment'. The main content area is titled 'Policy Information' and contains the following fields:

- User-visible name:** A text input field with a help icon.
- Font file:** A text input field with a 'Browse' button.
- Policy Settings:**
 - Remove policy:** Radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'. Below the radio buttons is a date picker.
 - Allow user to remove policy:** A dropdown menu currently set to 'Always'.
 - Profile scope:** A dropdown menu currently set to 'User'. To its right, the text 'OS X 10.7+' is displayed.
- Deployment Rules:** A section header with a right-pointing arrow.

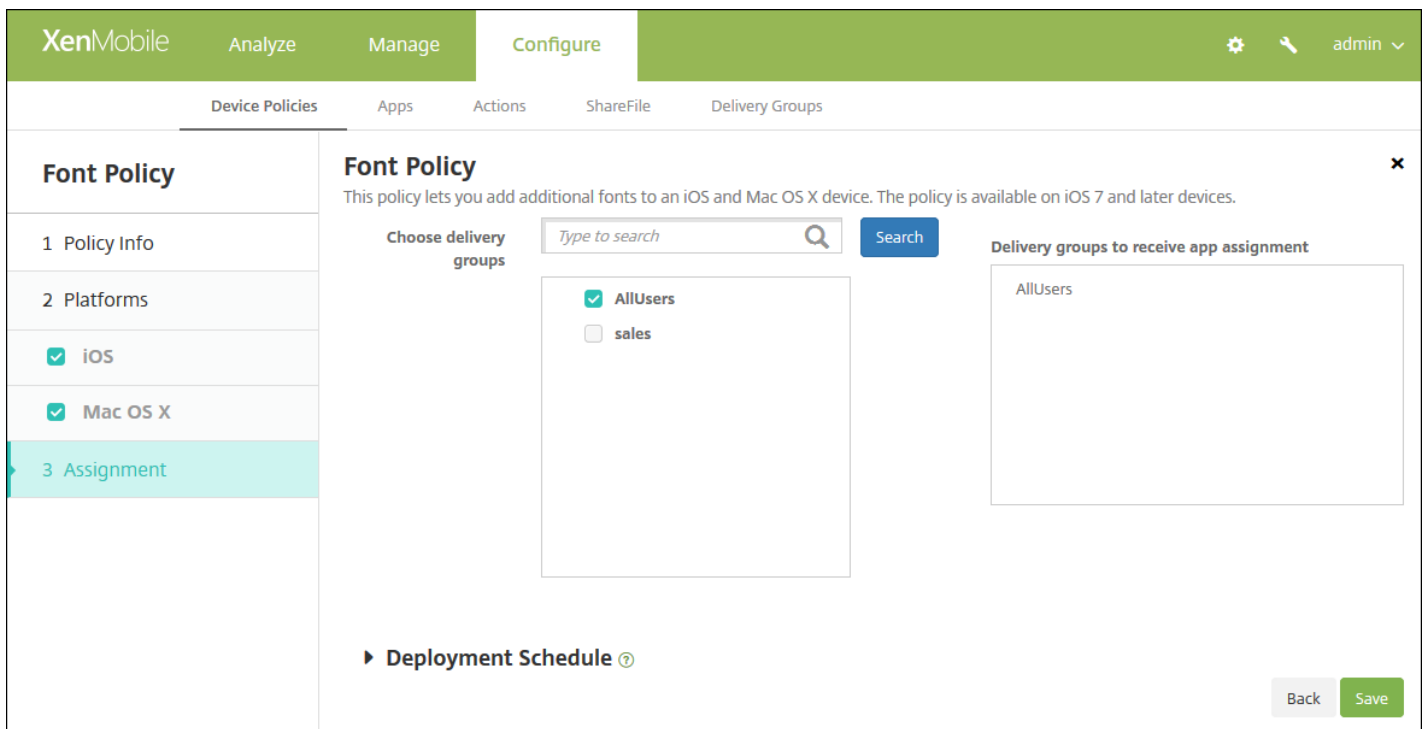
At the bottom right of the main area, there are 'Back' and 'Next >' buttons.

配置以下设置：

- 用户可见名称：键入用户在其字体列表中看到的名称。
- 字体文件：单击浏览，然后导航到要添加到用户设备的字体文件的位置，选择该文件。
- 策略设置
 - 在删除策略旁边，单击选择日期或删除前保留时间(天)。
 - 如果单击选择日期，请单击日历以选择具体删除日期。
 - 在允许用户删除策略列表中，单击始终、需要密码或从不。
 - 如果单击需要密码，在删除密码旁边，键入必需的密码。
 - 在配置文件作用域旁边，单击用户或系统。默认值为用户。此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击下一步。此时将显示字体策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

主屏幕布局设备策略

Feb 27, 2017

可以为 iOS 主屏幕指定应用程序和文件夹的布局。主屏幕布局设备策略适用于 iOS 9.3 及更高版本的受监督设备。

注意

向设备部署多个主屏幕布局策略会导致在设备上产生 iOS 错误。无论是通过此 XenMobile 策略还是通过 Apple Configurator 定义主屏幕，都存在此限制。

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. 开始键入主屏幕布局，然后在搜索结果中单击该名称。此时将显示主屏幕布局策略信息页面。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Home Screen Layout Policy' and contains a 'Policy Information' section. This section includes a description of the policy and two input fields: 'Policy Name*' and 'Description'.

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

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

Dock

Type	Display Name*	Value*	Add
			+

Page 1

Type	Display Name*	Value*	Add
			+

Page 2

Type	Display Name*	Value*	Add
			+

Page 3

Type	Display Name*	Value*	Add
			+

Page 4

Type	Display Name*	Value*	Add
			+

Page 5

Type	Display Name*	Value*	Add
			+

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy

6. 配置以下设置：

- 对于要配置的每个屏幕区域（例如基站或第 1 页），单击添加。
- 类型：选择应用程序或文件夹。

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Home Screen Layout Policy

This policy defines a layout of apps and folders for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application you should enter the bundle identifier as value. For a folder, you should enter a list of bundle identifiers separated with a comma.

Dock

Type	Display Name*	Value*	Save	Cancel
Application	<input type="text"/>	<input type="text"/>	Save	Cancel

Page 1

Type	Display Name*	Value*	Add
			+

- **显示名称**：应用程序或文件夹在主屏幕上显示的名称。
- **值**：对于应用程序，为捆绑包标识符。对于文件夹，为捆绑包标识符列表（以逗号分隔）。

策略设置

- **删除策略**：选择**选择日期**并从日历中选择日期，或选择**删除前保留时间**并指定天数。
- **允许用户删除策略**：指定何时允许用户删除主屏幕定义：**始终**、**需要通行码**（仅当他们提供通行码）或**从不**。

7. 配置部署规则

8. 单击**下一步**。此时将显示 **Windows 信息保护策略分配** 页面。
9. 在**选择交付组** 旁边，键入以查找交付组。要将策略分配到一个或多个组，请在列表中选择组。选择的组显示在用于接收应用程序分配的交付组列表中。
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**，则其他选项不适用。
 - 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**。

导入 iOS 和 Mac OS X 配置文件设备策略

Feb 27, 2017

可以将 iOS 和 OS X 设备的设备配置 XML 文件导入到 XenMobile 中。此文件包含您使用 Apple Configurator 准备的设备安全策略和限制。

您可使用 Apple Configurator 将 iOS 设备置于受监督模式，如本文稍后所述。有关使用 Apple Configurator 创建配置文件的详细信息，请参阅 Apple [Configurator 帮助](#) 页面。

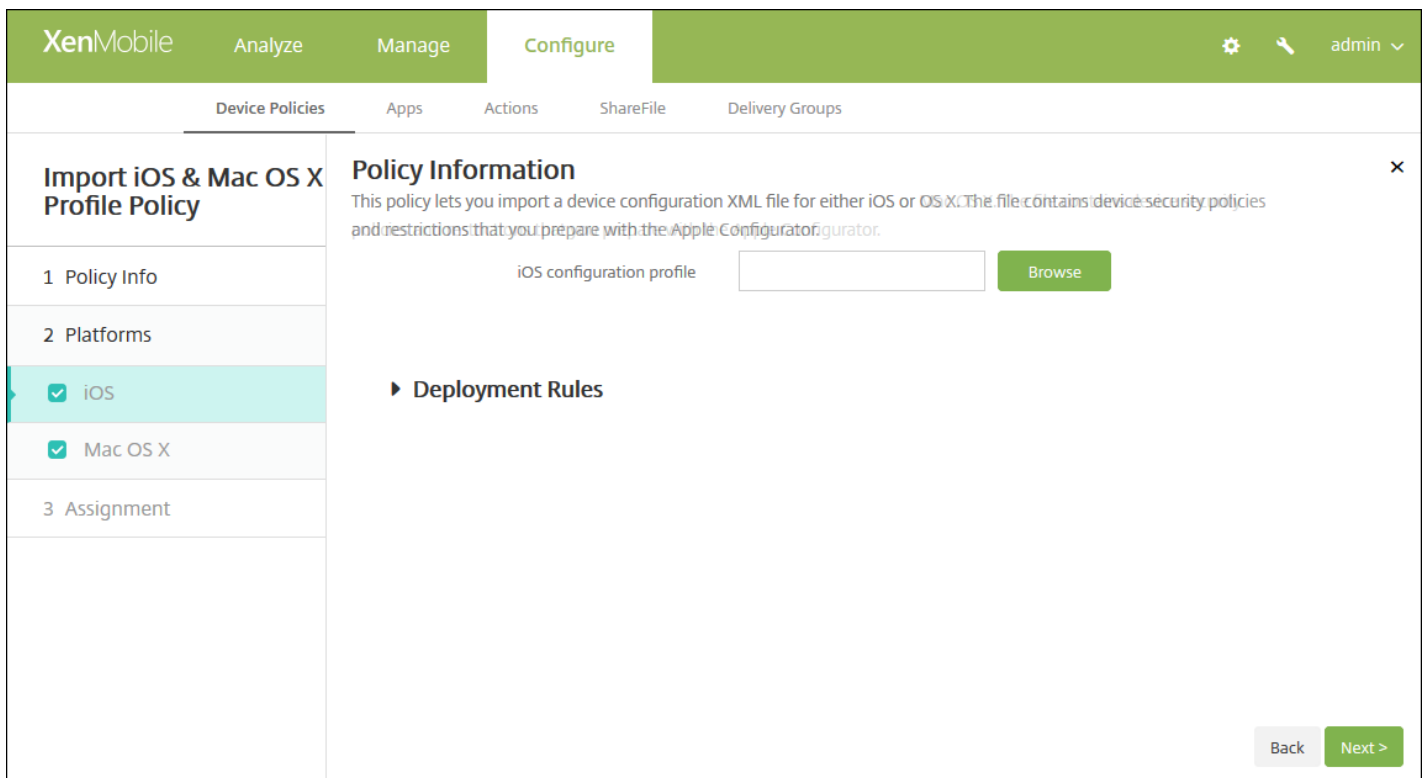
1. 在 XenMobile 控制台中，单击 **配置 > 设备策略**。
2. 单击 **添加**。此时将显示 **添加新策略** 对话框。
3. 展开 **更多**，然后在自定义下面，单击 **导入 iOS 和 Mac OS X 配置文件**。此时将显示 **导入 iOS 和 Mac OS X 配置文件策略** 信息页面。

The screenshot shows the 'Import iOS & Mac OS X Profile Policy' dialog in the XenMobile interface. The dialog is titled 'Import iOS & Mac OS X Profile Policy' and has a close button (X) in the top right. It contains a 'Policy Information' section with a description: 'This policy lets you import a device configuration XML file for either iOS or Mac OS X. The file contains device security policies and restrictions that you prepare with the Apple Configurator.' Below this are two input fields: 'Policy Name*' (required) and 'Description'. On the left side, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' and 'Mac OS X' are both checked. At the bottom right, there is a green 'Next >' button.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。



6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

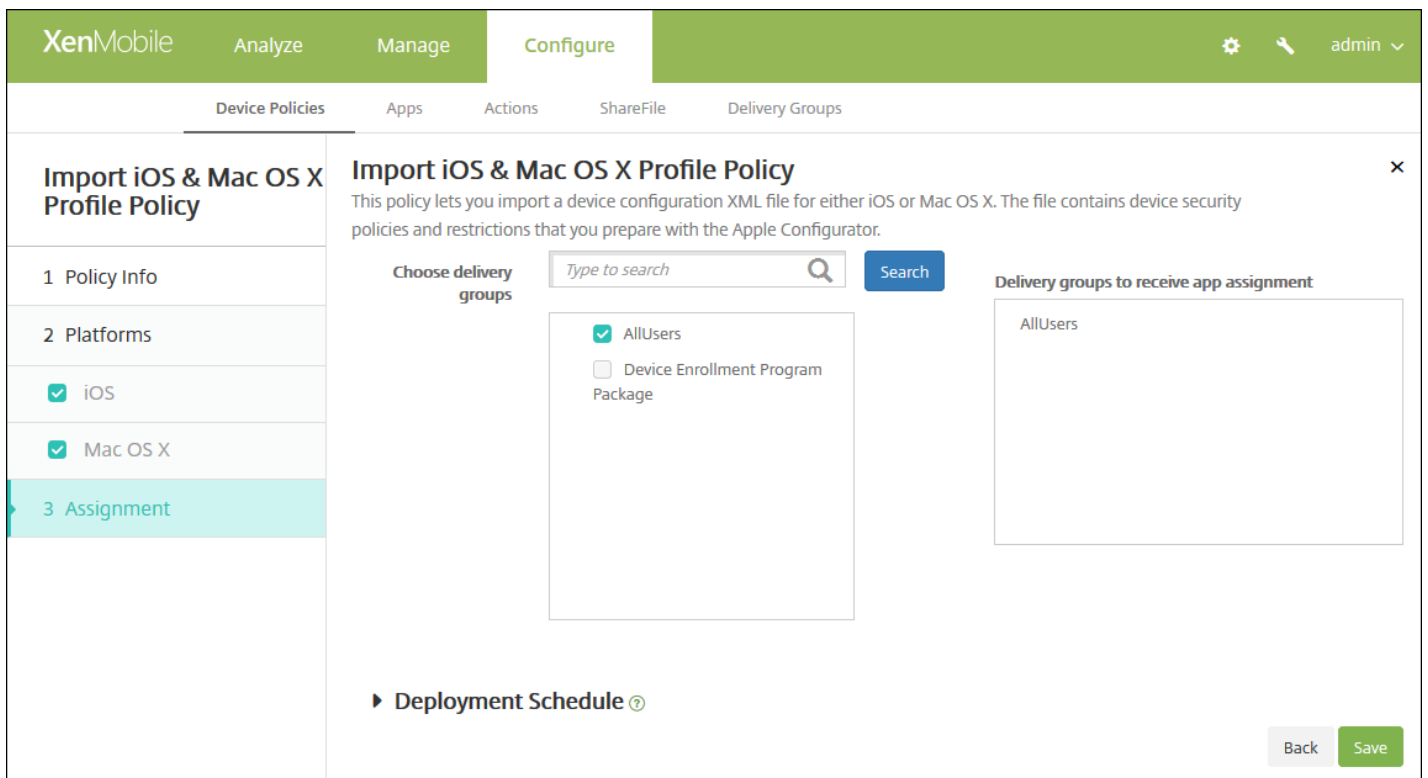
完成对平台设置的配置后，请参阅步骤 8 以了解如何设置此平台的部署规则。

7. 为您选择的每个平台配置以下设置：

- **iOS 配置文件或 Mac OS X 配置文件**：单击浏览并导航到要导入的配置文件的位置，选择该文件。

8. 配置部署规则

9. 单击下一步。此时将显示导入 **iOS 和 Mac OS X 配置文件策略分配** 页面。



10. 在选择交付组旁边，键入以查找交付组，或在列表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：

- 如果在设置 > 服务器属性中配置了计划后台部署密钥，则适用此选项。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

12. 单击保存以保存此策略。

使用 Apple Configurator 将 iOS 设备置于受监督模式

要使用 Apple Configurator，需要一台运行 OS X 10.7.2 或更高版本的 Apple 计算机。

Important

将设备置于受监督模式时，系统将会在设备上安装所选版本的 iOS，同时完全擦除设备上以前存储的任何用户数据或应用程序。

1. 从 iTunes 安装 [Apple Configurator](#)。
2. 将 iOS 设备连接到 Apple 电脑。
3. 启动 Apple Configurator。Configurator 显示您有一台设备需要进行监督前的准备工作。
4. 设备监督前准备工作：
 - a. 将 **Supervision**（监督）控件值切换到 **On**（开）。如果您打算通过定期重新应用配置来随时维护对设备的控制，Citrix 建议您选择此设置。
 - b. 提供设备的名称（可选）。
 - c. 在 iOS 中，单击 **Latest**（最新），获取您要安装的最新版本的 iOS。
5. 当您准备进行设备监督前的准备工作时，请单击 **Prepare**（准备）。

适用于 Samsung SAFE 的 Kiosk 设备策略

Feb 27, 2017

可以在 XenMobile 中创建 Kiosk 策略以便能够指定只能在 Samsung SAFE 设备上使用一个或多个特定的应用程序。此策略对旨在仅运行特定类型或类别的应用程序的企业设备非常有用。此策略还允许您为设备选择处于 Kiosk 模式时设备主屏幕和锁屏界面墙纸使用的自定义图片。

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，如下一节所述。
4. 将这三个设备策略分配给恰当的交付组。考虑是否要在这些交付组中包括其他策略，例如“应用程序清单”。

如果以后要从 Kiosk 模式中删除设备，请创建一个 **Kiosk 模式** 设置为禁用的新 Kiosk 设备策略。更新交付组以删除启用了 Kiosk 模式的 Kiosk 策略以及添加禁用了 Kiosk 模式的 Kiosk 策略。

添加 Kiosk 设备策略

注意：

- 为 Kiosk 模式指定的所有应用程序必须已安装在用户设备上。
- 某些选项仅适用于 Samsung Mobile Device Management API (MDM) 4.0 及更高版本。

1. 在 XenMobile 控制台中，单击 **配置 > 设备策略**。此时将显示 **设备策略** 页面。
2. 单击 **添加**。此时将显示 **添加新策略** 对话框。
3. 展开 **更多**，然后在 **安全性** 下方，单击 **Kiosk**。此时将显示 **Kiosk 策略** 页面。

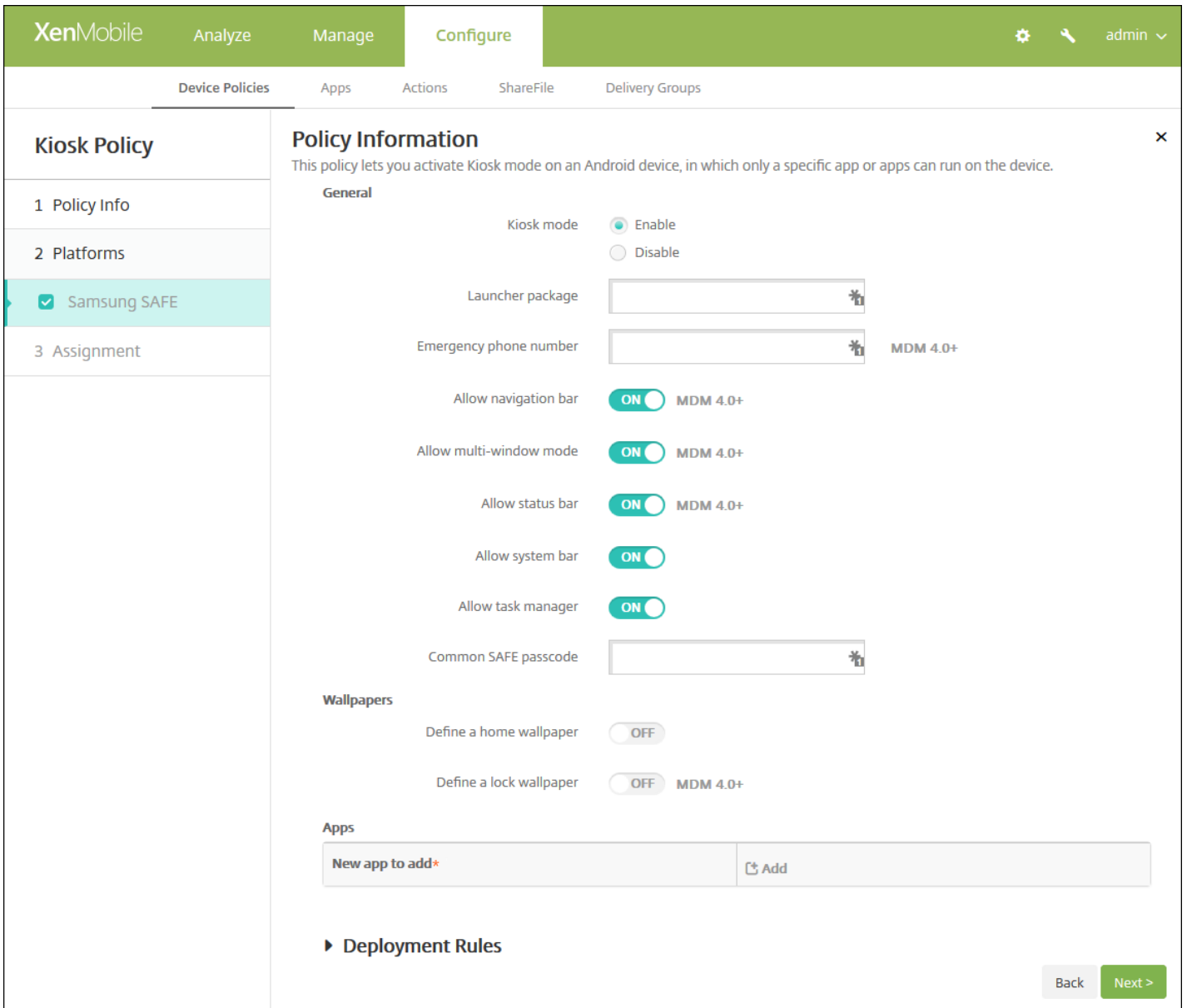
The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Kiosk Policy' and contains a 'Policy Information' section. The description reads: 'This policy lets you activate Kiosk mode on an Android device, in which only a specific app or apps can run on the device.' There are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. 在策略信息窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。

- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示 **Samsung SAFE** 平台信息页面。



6. 配置以下设置：

- **Kiosk 模式**：单击启用或禁用。默认值为启用。单击禁用时，以下所有选项将消失。
- **启动程序软件包**：除非您开发了内部启动程序以使用户能够打开一个或多个 Kiosk 应用程序，否则 Citrix 建议您让此字段留空。如果您使用的是内部启动程序，请输入启动程序应用程序软件包的完整名称。
- **紧急电话号码**：输入可选电话号码。查找所丢失设备的任何人都可以使用此号码与贵公司联系。仅适用于 MDM 4.0 及更高版本。
- **允许使用导航栏**：选择是否允许用户在处于 Kiosk 模式时看到和使用导航栏。仅适用于 MDM 4.0 及更高版本。默认值为开。
- **允许多窗口模式**：选择是否允许用户在处于 Kiosk 模式时使用多个窗口。仅适用于 MDM 4.0 及更高版本。默认值为开。
- **允许使用状态栏**：选择是否允许用户在处于 Kiosk 模式时看到状态栏。仅适用于 MDM 4.0 及更高版本。默认值为开。

- **允许使用系统栏**：选择是否允许用户在处于 Kiosk 模式时看到系统栏。默认值为开。
- **允许使用任务管理器**：选择是否允许用户在处于 Kiosk 模式时看到和使用任务管理器。默认值为开。
- **通用 SAFE 通行码**：如果您为所有 Samsung SAFE 设备设置了一个通用通行码策略，请在此字段中输入该可选通行码。
- **墙纸**
 - **定义主页墙纸**：选择是否在处于 Kiosk 模式时为主屏幕使用自定义图片。默认值为关。
 - **主页图片**：启用定义主页墙纸时，单击浏览并导航到图片文件的位置，选择该文件。
 - **定义锁定墙纸**：选择是否在处于 Kiosk 模式时为锁定屏幕使用自定义图片。默认值为关。仅适用于 MDM 4.0 及更高版本。
 - **锁屏图片**：启用定义锁屏墙纸时，单击浏览并导航到图片文件的位置，选择该文件。
- **应用程序**：对于要添加到 Kiosk 模式的每个应用程序，请单击**添加**，然后执行以下操作：
 - **添加新应用程序**：输入要添加的应用程序的完整名称。例如，com.android.calendar 允许用户使用 Android 日历应用程序。
 - 单击**保存**以添加应用程序，或单击**取消**以取消添加应用程序。

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，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。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击下一步。此时将显示 **Kiosk 策略分配** 页面。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Kiosk Policy' and includes a description: 'This policy lets you activate Kiosk mode on an Android device, in which only a specific app or apps can run on the device.' The 'Assignment' step is highlighted in the left sidebar. The main area shows a search for delivery groups with a search bar containing 'Type to search' and a 'Search' button. Below the search bar, there are two checkboxes: 'AllUsers' (checked) and 'sales' (unchecked). To the right, there is a box titled 'Delivery groups to receive app assignment' which currently contains 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

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。

适用于 Android 的 Launcher 配置设备策略

Feb 27, 2017

使用 Citrix Launcher 可以自定义由 XenMobile 部署的 Android 设备的用户体验。您可以添加 Launcher 配置策略来控制以下 Citrix Launcher 功能：

- 管理 Android 设备，确保用户只能访问指定的应用程序。
- （可选）为 Citrix Launcher 图标指定自定义徽标图片以及为 Citrix Launcher 指定自定义背景图片。
- 指定用户在退出启动程序前必须输入的密码。

尽管使用 Citrix Launcher 可以应用这些设备级别限制，但 Citrix Launcher 也为用户提供了所需的操作灵活性，允许他们通过内置访问途径配置设备设置，例如 WiFi 设置、蓝牙设置和设备通行码设置。Citrix Launcher 并不是设备平台在已提供的安全层之外额外提供的一个安全层。

部署 Citrix Launcher 后，XenMobile 会安装它，取代默认 Android 启动程序。

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. 键入 **Launcher**，然后从列表中选择 **Launcher 配置**。此时将显示 **Launcher 配置策略**页面。
4. 在**策略信息**窗格中，输入以下信息：
 - **策略名称**：键入策略的描述性名称。
 - **说明**：（可选）键入策略的说明。
5. 单击**下一步**。此时将显示 **Android 平台信息**页面。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Launcher Configuration Policy

- 1 Policy Info
- 2 Platforms
- Android
- 3 Assignment

Policy Information

This policy lets you define a configuration of an Android device launcher.

Launcher app configuration

Define a logo image

Logo image

Define a background image

Background image

Allowed apps

App name	Package Name*	Add
test	test.com	<input type="button" value="Add"/>

Password

Deployment Rules

6. 配置以下设置：

- **定义徽标图片**：选择是否为 Citrix Launcher 图标使用自定义徽标图片。默认值为关。
- **徽标图片**：启用定义徽标图片时，单击浏览并导航到图片文件的位置，选择该文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- **定义背景图片**：选择是否为 Citrix Launcher 背景使用自定义图片。默认值为关。
- **背景图片**：启用定义背景图片时，单击浏览并导航到图片文件的位置，选择该文件。支持的文件类型包括 PNG、JPG、JPEG 和 GIF。
- **允许的应用程序**：对于要在 Citrix Launcher 中允许使用的每个应用程序，请单击**添加**，然后执行以下操作：
 - **添加新应用程序**：输入要添加的应用程序的完整名称。例如，com.android.calendar 表示 Android 日历应用程序。
 - 单击**保存**以添加应用程序，或单击**取消**以取消添加应用程序。

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，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，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

- **密码**：用户必须输入密码才能退出 Citrix Launcher。

7. 配置部署规则

8. 单击下一步。此时将显示 **Launcher 配置策略分配** 页面。

9. 配置部署规则

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。

12. 单击**保存**。

LDAP 设备策略

Feb 27, 2017

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

配置此策略之前，您需要提供 LDAP 主机名。

iOS 设置

Mac OS X 设置

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**添加新策略。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**最终用户**下面，单击**LDAP**。此时将显示**LDAP 策略**页面。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'LDAP Policy' and contains a 'Policy Information' section with a description: 'This policy lets you configure an LDAP server and search policies for querying the server.' Below this are two input fields: 'Policy Name*' and 'Description'. To the left, there is a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' and 'Mac OS X' are both checked. A 'Next >' button is located at the bottom right of the main content area.

4. 在**策略信息**窗格中，输入以下信息：

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

5. 单击**下一步**。此时将显示**策略平台信息**页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

配置以下设置：

- **帐户说明**：输入可选帐户说明。
- **帐户用户名**：输入可选手用户名。
- **帐户密码**：输入可选密码。此选项仅适用于加密的配置文件。
- **LDAP 主机名**：输入 LDAP 服务器的主机名。此字段为必填字段。
- **使用 SSL**：选择是否使用安全套接字层连接到 LDAP 服务器。默认值为开。
- **搜索设置**：添加查询 LDAP 服务器时要使用的搜索设置。可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。单击**添加**，然后执行以下操作：
 - **说明**：输入搜索设置的说明。此字段为必填字段。
 - **范围**：在列表中，单击**基础**、**一级**或**子树**以定义要搜索的 LDAP 树的深度。默认值为**基础**。
 - 范围搜索搜索基础指向的节点。
 - 一级搜索范围节点及其下一级节点。
 - 子树搜索范围节点及其所有子节点，而无论深度为何。
 - **搜索基础**：输入开始搜索时所在节点的路径。例如 ou=people 或 O=example corp。此字段为必填字段。
 - 单击**保存**添加搜索设置，或单击**取消**以取消添加搜索设置。
 - 为要添加的每个搜索设置重复执行这些步骤。

注意：要删除现有搜索设置，请将鼠标悬停在包含列表的行上方，然后单击右侧的垃圾桶图标。此时将显示确认对话框。单击**删除**以删除列表，或单击**取消**以保留此列表。

要编辑现有搜索设置，请将鼠标悬停在包含列表的行上方，然后单击右侧的铅笔图标。更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

- 在策略设置下，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，在删除密码旁边，键入必需的密码。

配置 Mac OS X 设置

The screenshot shows the XenMobile Configure interface for an LDAP Policy. The left sidebar contains a navigation menu with sections: 1 Policy Info, 2 Platforms (with 'Mac OS X' selected), and 3 Assignment. The main content area is titled 'Policy Information' and includes the following sections:

- Account Information:** Fields for Account description, Account user name, Account password, and LDAP host name*.
- Use SSL:** A toggle switch currently set to 'ON'.
- Search Settings:** A table with columns for Description*, Scope, and Search base*, and an 'Add' button.
- Policy Settings:** Includes 'Remove policy' options (Select date or Duration until removal (in days)), 'Allow user to remove policy' (set to 'Always'), and 'Profile scope' (set to 'User'). A version indicator 'OS X 10.7+' is shown.
- Deployment Rules:** A section header with a right-pointing arrow.

At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **帐户说明：**输入可选帐户说明。
- **帐户用户名：**输入可选用户名。
- **帐户密码：**输入可选密码。此选项仅适用于加密的配置文件。
- **LDAP 主机名：**输入 LDAP 服务器的主机名。此字段为必填字段。
- **使用 SSL：**选择是否使用安全套接字层连接到 LDAP 服务器。默认值为开。
- **搜索设置：**添加查询 LDAP 服务器时要使用的搜索设置。可以根据需要输入任意数量的搜索设置，但至少应添加一个搜索设置以使帐户有用。单击添加，然后执行以下操作：

- **说明**：输入搜索设置的说明。此字段为必填字段。
- **范围**：在列表中，单击**基础**、**一级**或**子树**以定义要搜索的 LDAP 树的深度。默认值为**基础**。
 - 范围搜索搜索基础指向的节点。
 - 一级搜索范围节点及其下一级节点。
 - 子树搜索范围节点及其所有子节点，而无论深度为何。
- **搜索基础**：输入开始搜索时所在节点的路径。例如 ou=people 或 0=example corp。此字段为必填字段。
- 单击**保存**添加搜索设置，或单击“取消”以取消添加搜索设置。
- 为要添加的每个搜索设置重复执行这些步骤。

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

要编辑现有搜索设置，请将鼠标悬停在包含列表的行上方，然后单击右侧的铅笔图标。更改列表，然后单击保存以保存更改的列表，或单击取消以保持列表不更改。

- 在**策略设置**下，**删除策略**旁边，单击**选择日期** 或 **删除前保留时间(天)**。
- 如果单击**选择日期**，请单击日历以选择具体删除日期。
- 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
- 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。
- 在**配置文件作用域**中，单击**用户**或**系统**。默认值为**用户**。此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击下一步。此时将显示 **LDAP 策略分配** 页面。

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

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。

位置设备策略

Mar 24, 2017

可以在 XenMobile 中创建定位设备策略以强制实施地理边界。用户超出定义的边界（也称为**地理围栏**）时，XenMobile 可以执行某些操作。例如，您可以配置策略以在用户超出定义的外围时向用户发出警告消息。您还可以配置策略以在用户超出外围时立即或延迟一段时间后擦除用户的公司数据。有关安全操作的信息（例如启用跟踪和定位设备），请参阅**设备**中的“执行安全操作”部分。

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

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**位置**。此时将显示**定位策略**信息页面。

The screenshot shows the XenMobile configuration interface for a Location Policy. The interface is divided into a sidebar and a main content area. The sidebar on the left has a 'Location Policy' section with three sub-items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section has two checkboxes: 'iOS' and 'Android', both of which are checked. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below the description are two input fields: 'Policy Name*' (a text box) and 'Description' (a large text area). A 'Next >' button is located in the bottom right corner of the main content area.

4. 在**策略信息**窗格中，输入以下信息：

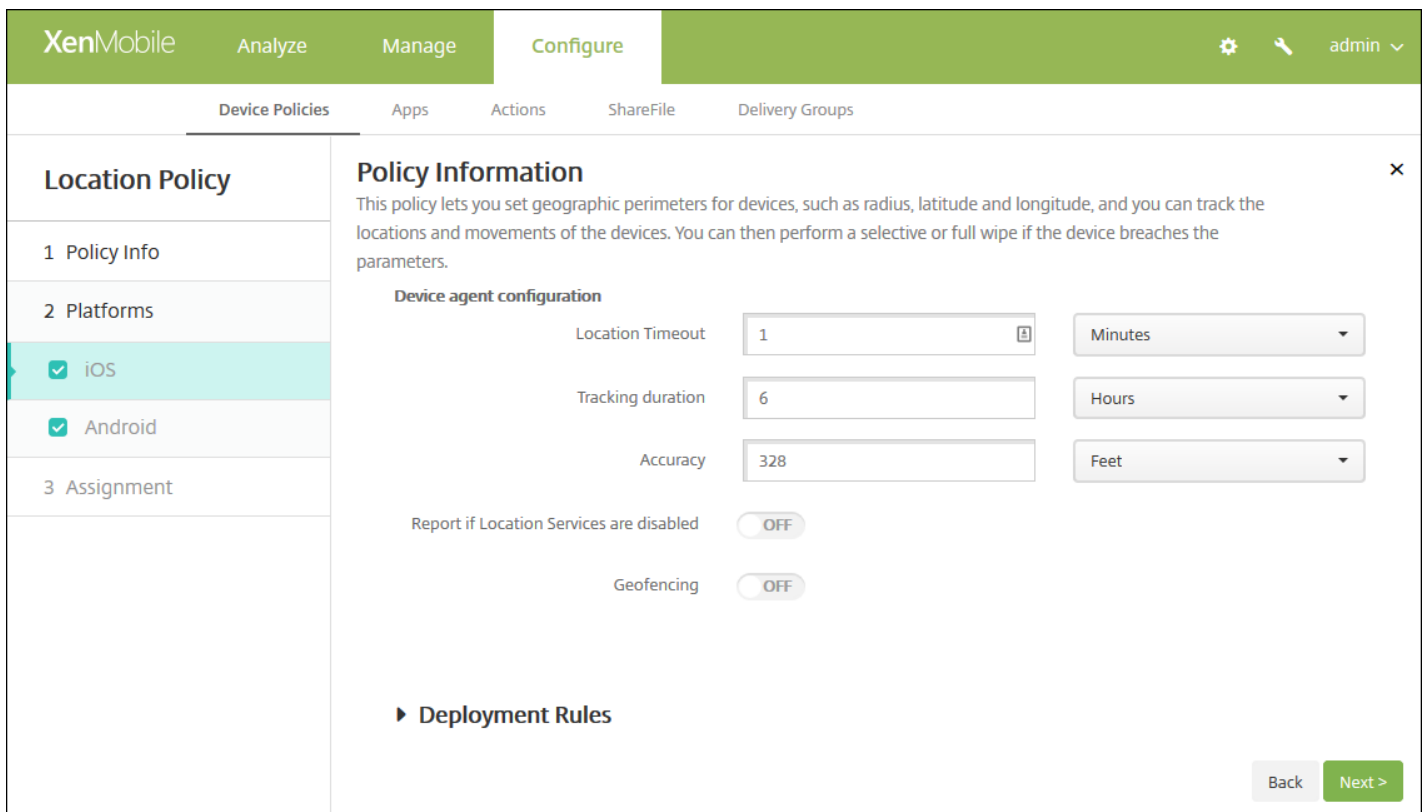
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

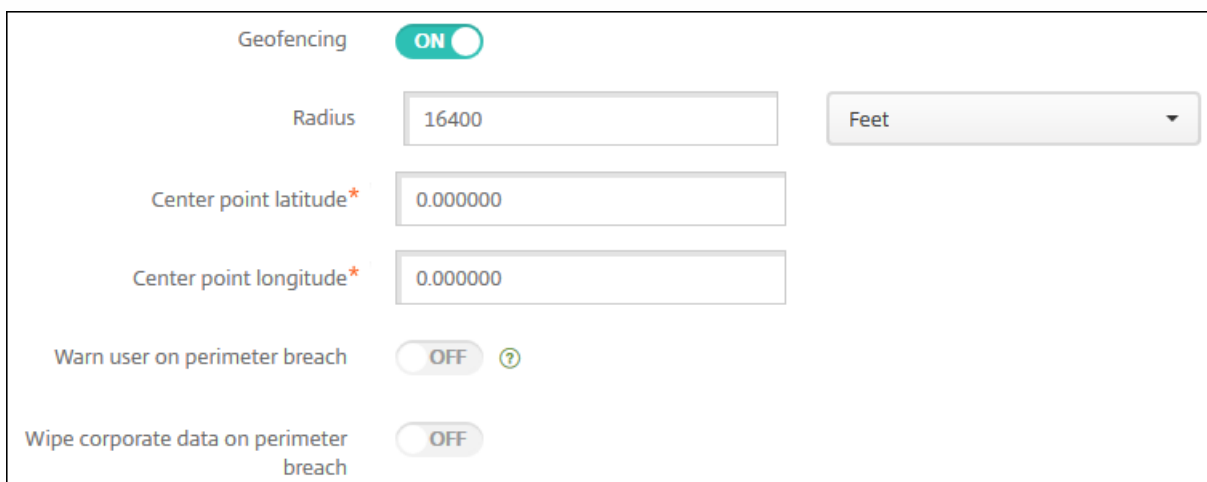
为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置



配置以下设置：

- **定位超时**：键入数值，然后在列表中单击**秒**或**分钟**以设置 XenMobile 尝试修复设备位置的频率。有效值为 60-900 秒或 1-15 分钟。默认值为 1 分钟。
- **跟踪持续时间**：键入数值，然后在列表中单击**小时**或**分钟**以设置 XenMobile 跟踪设备的时间长度。有效值为 1-6 小时或 10-360 分钟。默认值为 6 小时。
- **准确度**：键入数值，然后在列表中单击**米**、**英尺**或**码**以设置 XenMobile 跟踪设备的接近程度。有效值为 10-5000 码或米，或者 30-15000 英尺。默认值为 328 英尺。
- **禁用定位服务时报告**：选择禁用 GPS 时设备是否向 XenMobile 发送报告。默认值为关。
- **地理围栏**



启用地理围栏时，请配置以下设置：

- **半径**：键入数值，然后在列表中单击要用于衡量半径的单位。默认值为 16,400 英尺。半径的有效值如下：
 - 164-164000 英尺
 - 50-50000 米
 - 54-54680 码
 - 1-31 英里
- **中心点纬度**：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- **中心点经度**：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- **超出边界时警告用户**：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 XenMobile 即可显示警告消息。
- **超出边界时擦除公司数据**：选择当用户超出边界时是否擦除用户设备。默认值为关。启用此选项时，将显示本地擦除延迟字段。
 - 键入数值，然后在列表中单击**秒**或**分钟**以设置从用户设备中擦除公司数据之前延迟的时间长度。这使用户有机会在 XenMobile 选择性擦除其设备之前返回到允许的位置。默认值为 0 秒。

配置 Android 设置

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure' (which is active). Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Location Policy' and has a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' and 'Android' are listed, with 'Android' selected. The main content area for 'Android' shows 'Policy Information' with a description: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below this is the 'Device agent configuration' section with three settings: 'Poll interval' set to 10 minutes, 'Report if Location Services is disabled' set to OFF, and 'Geofencing' set to OFF. At the bottom of the main content area is a 'Deployment Rules' section with a right-pointing arrow. At the bottom right of the page are 'Back' and 'Next >' buttons.

- **轮询间隔**：键入数值，然后在列表中单击**分钟**、**小时**或**天**以设置 XenMobile 尝试修复设备位置的频率。有效值为 1-1440 分钟、1-24 小时或任意天数。默认值为 10 分钟。将此值设置为小于 10 分钟可能会对设备的电池寿命产生不利影响。
- **禁用定位服务时报告**：选择禁用 GPS 时设备是否向 XenMobile 发送报告。默认值为关。
- **地理围栏**

Geofencing

Radius Feet

Center point latitude*

Center point longitude*

Warn user on perimeter breach

Device connects to XenMobile for policy refresh

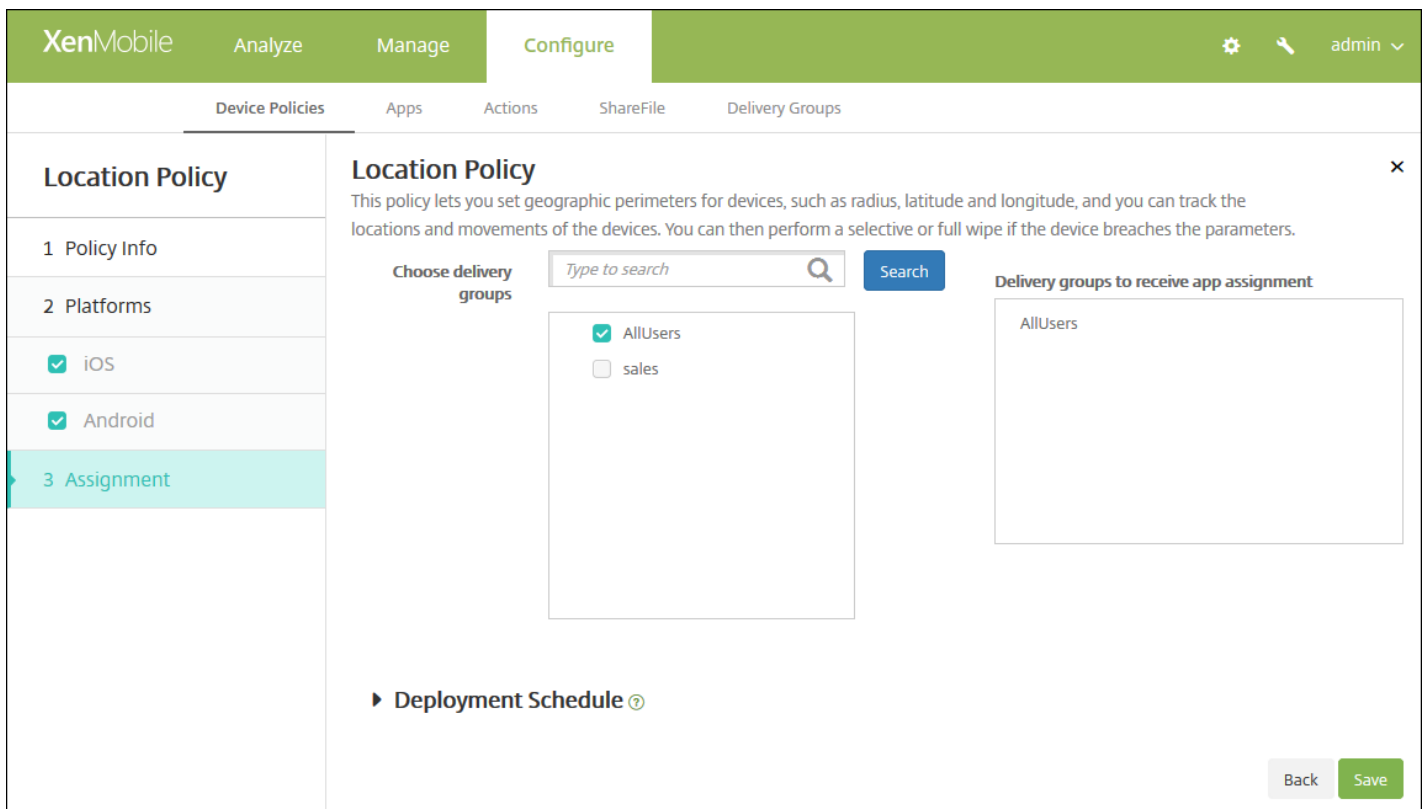
- Perform no action on perimeter breach
- Wipe corporate data on perimeter breach
- Lock device locally

启用地理围栏时，请配置以下设置：

- **半径**：键入数值，然后在列表中单击要用于衡量半径的单位。默认值为 16,400 英尺。半径的有效值如下：
 - 164-164000 英尺
 - 1-50 千米
 - 50-50000 米
 - 54-54680 码
 - 1-31 英里
- **中心点纬度**：键入纬度（例如 37.787454）以定义地理围栏中心点的纬度。
- **中心点经度**：键入经度（例如 122.402952）以定义地理围栏中心点的经度。
- **超出边界时警告用户**：选择用户超出定义的边界时是否发出警告消息。默认值为关。不需要连接到 XenMobile 即可显示警告消息。
- **设备连接到 XenMobile 以刷新策略**：为用户超出边界时选择以下选项之一：
 - **超出边界时不执行任何操作**：不执行任何操作。这是默认值。
 - **超出边界时擦除公司数据**：指定时间长度后擦除公司数据。启用此选项时，将显示本地擦除延迟字段。
 - 键入数值，然后在列表中单击秒或分钟以设置从用户设备中擦除公司数据之前延迟的时间长度。这使用户有机会在 XenMobile 选择性擦除其设备之前返回到允许的位置。默认值为 0 秒。
 - **锁定延迟**：指定时间长度后锁定用户设备。启用此选项时，将显示锁定延迟字段。
 - 键入数值，然后在列表中单击秒或分钟以设置锁定用户设备之前延迟的时间长度。这使用户有机会在 XenMobile 锁定其设备之前返回到允许的位置。默认值为 0 秒。

7. 配置部署规则

8. 单击下一步。此时将显示定位策略分配页面。



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。

邮件设备策略

Feb 27, 2017

可以在 XenMobile 中添加邮件设备策略以在用户的 iOS 或 Mac OS X 设备上配置电子邮件帐户。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加添加新策略。此时将显示添加新策略对话框。
3. 单击更多，然后在最终用户下，单击邮件。此时将显示邮件策略页面。

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Device Policies', the 'Mail Policy' section is expanded. The 'Policy Information' dialog is open, containing the following fields:

- Policy Name***: A text input field.
- Description**: A larger text area for notes.

On the left, the 'Mail Policy' sidebar shows three steps: 1 Policy Info (active), 2 Platforms, and 3 Assignment. Under 'Platforms', 'iOS' and 'Mac OS X' are both checked. A 'Next >' button is located at the bottom right of the dialog.

4. 在策略信息窗格中，输入以下信息：

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

5. 单击下一步。此时将显示邮件策略平台页面。

This screenshot shows the same XenMobile interface, but the 'Policy Information' dialog has advanced to the platform configuration step. The 'Platforms' sidebar now shows 'iOS' and 'Mac OS X' checked. The 'Policy Information' dialog contains the following fields:

- Account description***: A text input field.
- Account type**: A dropdown menu currently set to 'IMAP'.
- Path prefix**: A text input field.
- User display name***: A text input field.
- Email address***: A text input field.
- Incoming email**: A section header for the following field.
- Email server host name***: A text input field.

The screenshot shows a configuration page for email settings. It includes the following sections and fields:

- Incoming email:**
 - Email server port*: 143
 - User name*
 - Authentication type: Password
 - Password
 - Use SSL: OFF
- Outgoing email:**
 - Email server host name*
 - Email server port*
 - User name*
 - Authentication type: Password
 - Password
 - Outgoing password same as incoming: OFF
 - Use SSL: OFF
- Policy:**
 - Authorize email move between accounts: OFF iOS 5.0+
 - Sending email only from mail app: OFF iOS 5.0+
 - Disable mail recents syncing: OFF iOS 6.0+
 - Enable S/MIME: OFF iOS 5.0+
- Policy Settings:**
 - Remove policy:
 - Select date
 - Duration until removal (in days)
 - Allow user to remove policy: Always
- Deployment Rules** (indicated by a right-pointing triangle)

At the bottom right, there are two buttons: "Back" and "Next >".

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 8 以了解如何设置此平台的部署规则。

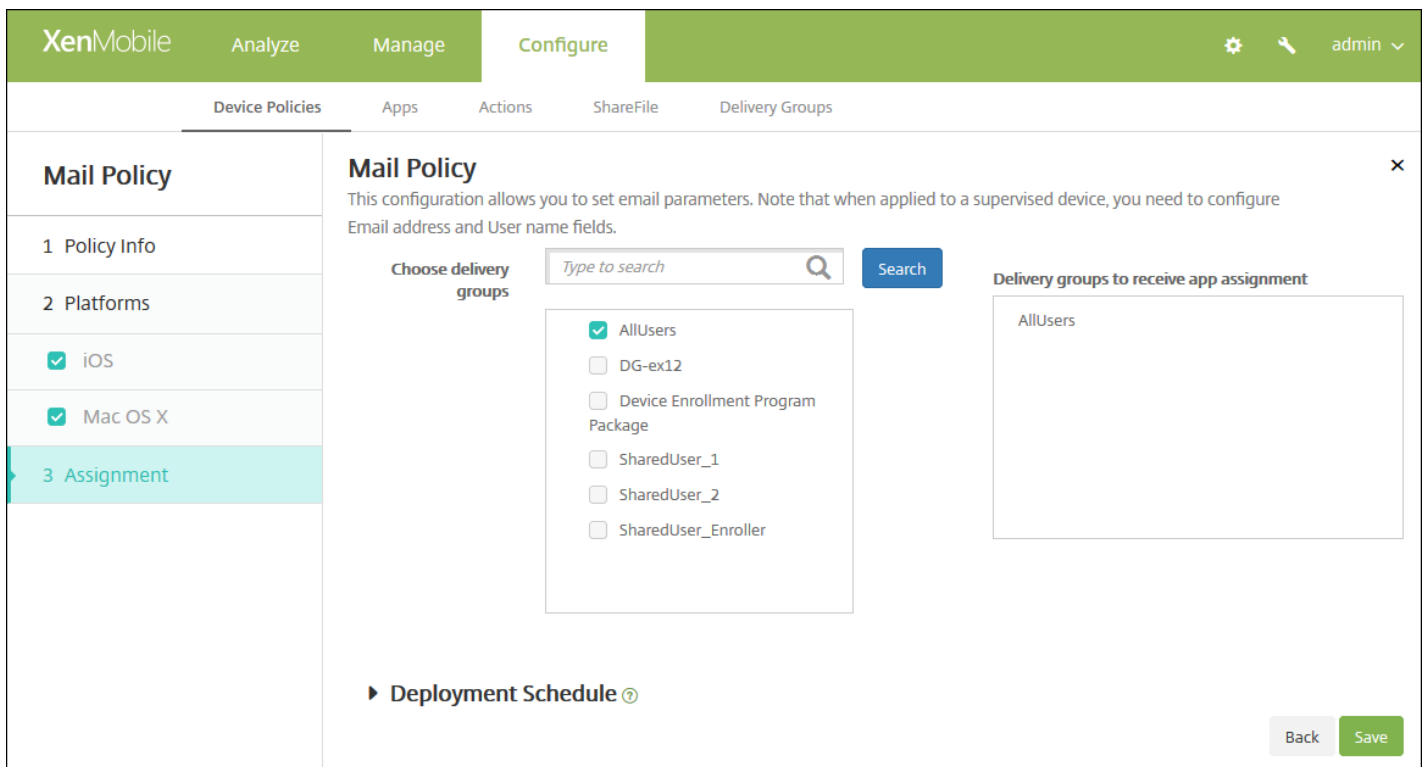
7. 为选择的平台配置以下设置。

- **帐户说明**：键入在“邮件”和“设置”应用程序中显示的帐户说明。此字段为必填字段。
- **帐户类型**：在列表中，单击 **IMAP** 或 **POP** 以选择要对用户帐户使用的协议。默认值为 **IMAP**。选择 **POP** 时，以下路径前缀选项将消失。

- **路径前缀**：键入 **INBOX** 或您的 IMAP 邮件帐户路径前缀（如果不是 **INBOX**）。此字段为必填字段。
- **用户显示名称**：键入要对邮件等使用的完整用户名。此字段为必填字段。
- **电子邮件地址**：键入帐户的完整电子邮件地址。此字段为必填字段。
- **传入电子邮件设置**
 - **电子邮件服务器主机名**：键入传入电子邮件服务器主机名或 IP 地址。此字段为必填字段。
 - **电子邮件服务器端口**：键入传入邮件服务器端口号。默认值为 **143**。此字段为必填字段。
 - **用户名**：键入电子邮件帐户的用户名。此名称通常与用户的电子邮件地址中 @ 字符前面的部分相同。此字段为必填字段。
 - **身份验证类型**：在列表中，单击以选择要使用的身份验证类型。默认值为**密码**。选中无时，以下**密码**字段将消失。
 - **密码**：键入传入邮件服务器的可选密码。
 - **使用 SSL**：选择传入邮件服务器是否使用安全套接字层身份验证。默认值为**关**。
- **传出电子邮件设置**
 - **电子邮件服务器主机名**：输入传出邮件服务器主机名或 IP 地址。此字段为必填字段。
 - **电子邮件服务器端口**：键入传出邮件服务器端口号。如果未输入端口号，将使用指定协议的默认端口。
 - **用户名**：键入电子邮件帐户的用户名。此名称通常与用户的电子邮件地址中 @ 字符前面的部分相同。此字段为必填字段。
 - **身份验证类型**：在列表中，单击以选择要使用的身份验证类型。默认值为**密码**。选中无时，以下**密码**字段将消失。
 - **密码**：键入传出邮件服务器的可选密码。
 - **传出密码和传入密码相同**：选择传入和传出密码是否相同。默认值为**关**，表示密码不相同。设置为**开**时，上述**密码**字段将消失。
 - **使用 SSL**：选择传出邮件服务器是否使用安全套接字层身份验证。默认值为**关**。
- **策略**
 - **注意**：配置 iOS 设置时，这些选项仅适用于 iOS 5.0 及更高版本；配置 Mac OS X 时无限制。
 - **授权电子邮件在帐户之间移动**：选择是否允许用户将电子邮件从此帐户移出到另一个帐户以及从其他帐户转发和答复。默认值为**关**。
 - **仅从邮件应用程序发送电子邮件**：选择是否限制用户只能从 iOS 邮件应用程序发送电子邮件。
 - **禁用最新邮件同步**：选择是否阻止用户同步最近使用的地址。默认值为**关**。此选项仅适用于 iOS 6.0 及更高版本。
 - **启用 S/MIME**：选择此帐户是否支持 S/MIME 身份验证和加密。默认值为**关**。设置为**开**时，将显示以下两个字段。
 - **签署身份凭据**：在列表中，选择要使用的签名凭据。
 - **加密身份凭据**：在列表中，选择要使用的加密凭据。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。
 - 在**配置文件作用域**旁边：在列表中，单击**用户**或**系统**。默认值为**用户**。此选项仅在 Mac OS X 10.7 及更高版本上可用。

8. 配置部署规则

9. 单击下一步。此时将显示**邮件策略**分配页面。



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

11. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

12. 单击保存以保存此策略。

托管域设备策略

Feb 27, 2017

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。

对于 iOS 8 及更高版本的受监管设备，请指定 URL 或子域以控制用户通过浏览器打开文档、附件或下载内容的方式。对于 iOS 9.3 及更高版本的受监督设备，可以在 Safari 中指定用户能够从中保存密码的 URL。

有关将 iOS 设备置于受监督模式的步骤，请参阅[使用 Apple Configurator 将 iOS 设备置于受监督模式](#)。

用户向域不在托管电子邮件域列表上的收件人发送电子邮件时，在用户的设备上此邮件将带有标记，以警告用户正在向企业域外部的人员发送邮件。

对于文档、附件或下载内容等项目：当用户使用 Safari 从位于托管 Web 域列表上的 Web 域打开某个项目（文档、附件或下载内容）时，将由合适的企业应用程序打开此项目。如果此项目所在的 Web 域不在托管 Web 域列表上，用户无法使用合适的企业应用程序打开此项目。必须使用未托管的个人应用程序打开。

对于受监督的设备，即使您未指定 Safari 密码自动填充域：如果设备配置为暂时多用户，用户将无法保存密码。但是，如果设备未配置为暂时多用户，用户可以保存所有密码。

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**。此时将显示**托管域策略**信息页面。

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Managed Domains Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

Policy Information

This policy lets you define managed domains that apply to the Safari browser. The policy is supported only on iOS 8 and later devices.

Policy Name*

Description

Next >

4. 在策略信息窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示 **iOS** 平台页面。

Managed Domains Policy

This policy lets you define managed domains that apply to the Safari browser. The policy is supported only on iOS 8 and later devices.

Managed Domains

Unmarked Email Domains

Managed Email Domain

Managed Safari Web Domains

Managed Web Domain

Safari Password AutoFill Domains

Safari Password AutoFill Domain

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy

Deployment Rules

Back Next >

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。

- **Safari 密码自动填充域**：

对于要包含在列表中的每个自动填充域，请单击**添加**，然后执行以下操作：

- **Safari 密码自动填充域**：键入自动填充域。
- 单击**保存**以保存自动填充域，或者单击**取消**不保存自动填充域。

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

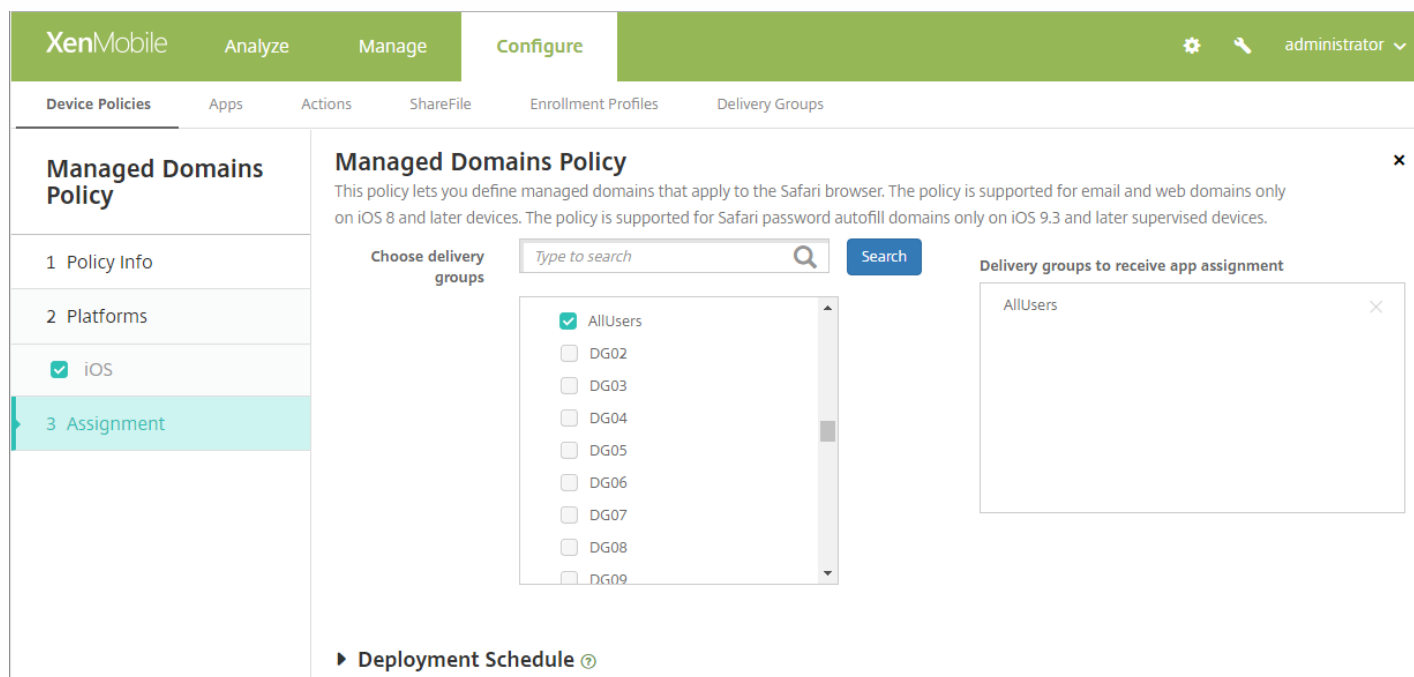
更改的列表，或者单击取消。

● 策略设置

- 在策略设置下方的删除策略旁边，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。

MDM 选项设备策略

Feb 27, 2017

可以在 XenMobile 中创建一个设备策略，用于在受监督的 iOS 7.0 及更高版本的手机设备上管理“查找我的 iPhone/iPad 激活锁”。有关将 iOS 设备置于受监督模式的步骤，请参阅[使用 Apple Configurator 将 iOS 设备置于受监督模式](#)。

激活锁是一项“查找我的 iPhone/iPad”功能，目的是在任何人都可以关闭“查找我的 iPhone”、擦除设备或重新激活并使用设备之前，通过要求提供用户的 Apple ID 和密码阻止重新激活丢失或失窃的设备。在 XenMobile 中，可以通过在 MDM 选项设备策略中启用激活锁，跳过 Apple ID 和密码要求。当用户返回已启用“查找我的 iPhone”功能的设备时，您无需具有其 Apple 凭据便可以从 XenMobile 控制台管理此设备。

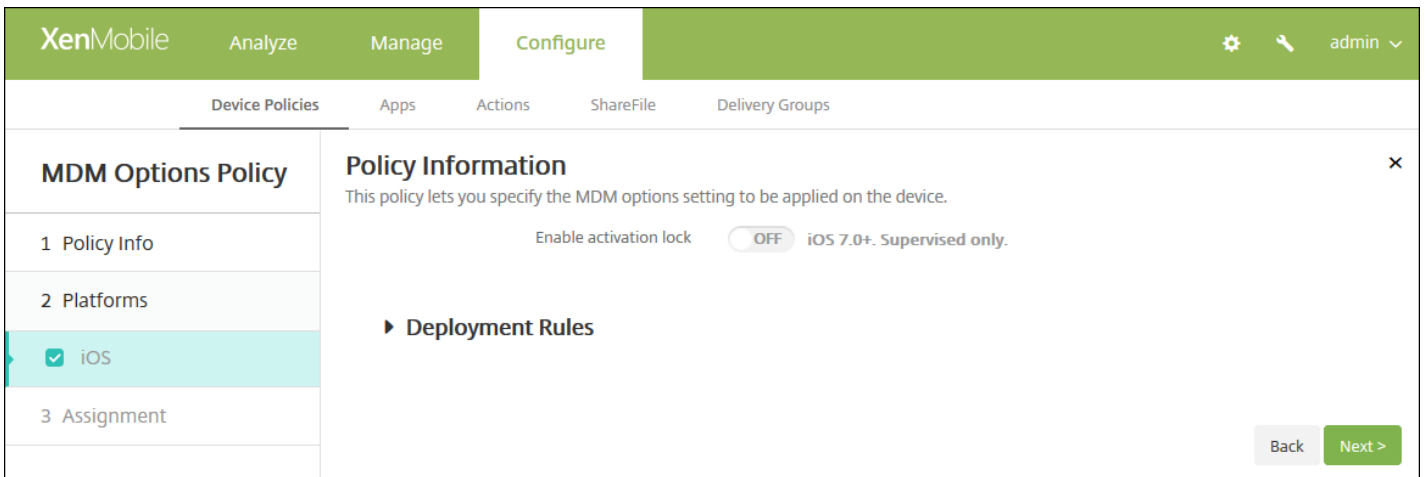
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**最终用户**下面，单击**MDM 选项**。此时将显示**MDM 选项策略**信息页面。

The screenshot shows the XenMobile configuration interface. At the top, there is a navigation bar with tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'MDM Options Policy' and 'Policy Information'. It includes a sidebar with steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' step is selected. The main area contains a form with fields for 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. 在策略信息窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击**下一步**。此时将显示**iOS MDM 策略**平台页面。

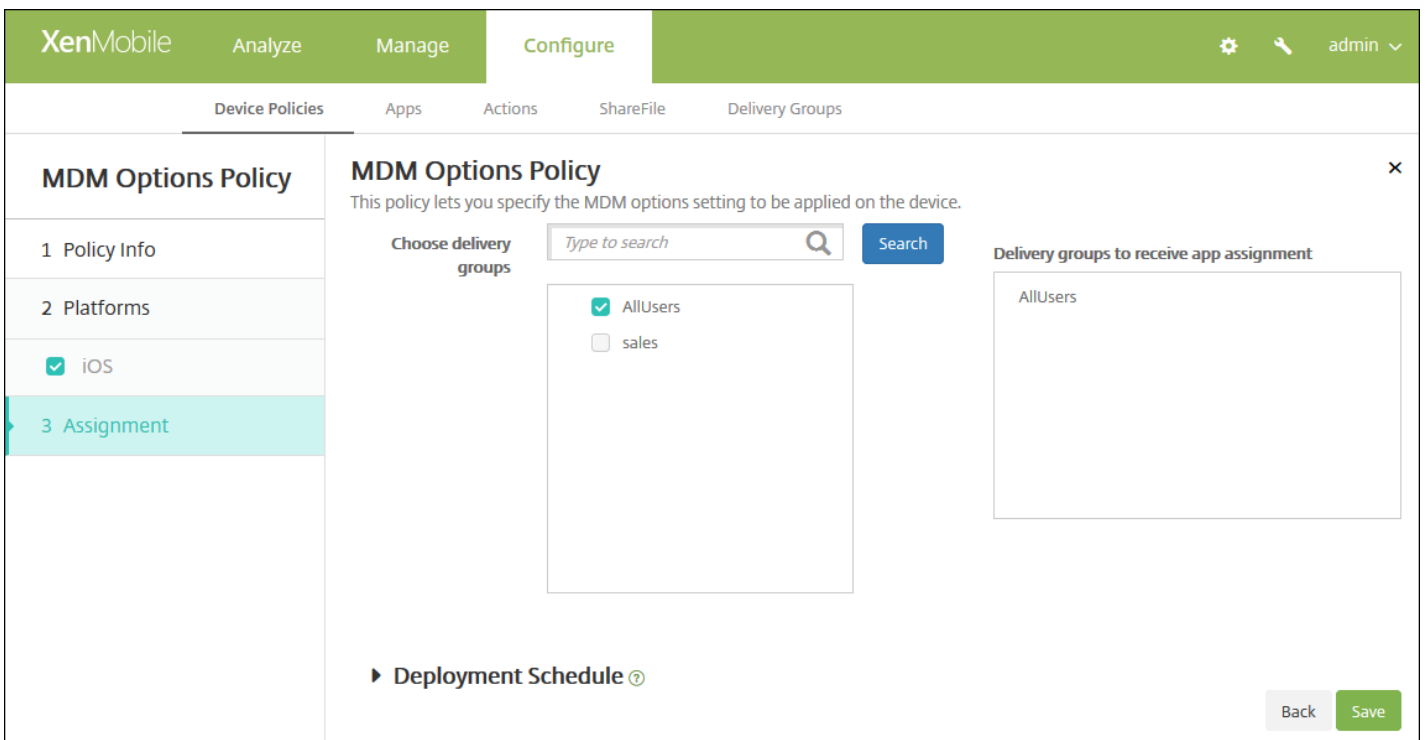


6. 配置以下设置：

- 启用激活锁：选择是否要在部署此策略的设备上启用激活锁。默认值为关。



8. 单击下一步。此时将显示 MDM 选项策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

- 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。如果选择关，无需配置其他选项。

- 在部署计划旁边，单击立即或稍后。默认选项为立即。
- 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
- 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
- 在为始终启用的连接部署旁边，单击开或关。默认选项为关。

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

Microsoft Exchange ActiveSync 设备策略

Feb 27, 2017

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

[iOS 设置](#)

[Mac OS X 设置](#)

[Android HTC 设置](#)

[Android TouchDown 设置](#)

[Android for Work 设置](#)

[Samsung SAFE 和 Samsung KNOX 设置](#)

[Windows Phone 设置](#)

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**。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。

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Exchange Policy' configuration window is open, showing a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Platforms' section lists: iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX, and Windows Phone, all with checked boxes. The main 'Policy Information' section includes a text box for 'Policy Name*' and a larger text area for 'Description'. A 'Next >' button is at the bottom right.

4. 在策略信息窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 在平台下，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

Exchange Policy

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Samsung SAFE
- Samsung KNOX
- Windows Phone

3 Assignment

Policy Information

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Exchange ActiveSync account name*

Exchange ActiveSync host name*

Use SSL **ON**

Domain

User

Email address

Password

Email sync interval: 3 days

Identity credential (keystore or PKI credential): None

Back Next >

配置以下设置：

- **Exchange ActiveSync 帐户名称**：键入显示在用户设备上的电子邮件帐户的说明。
- **Exchange ActiveSync 主机名**：键入电子邮件服务器的地址。
- **使用 SSL**：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为开。
- **域**：输入 Exchange Server 所在的域。可以在此字段中使用系统宏 `${user.domainname}` 自动查找用户的域名。
- **用户**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `${user.username}` 自动查找用户的名称。
- **电子邮件地址**：指定用户的完整电子邮件地址。可以在此字段中使用系统宏 `${user.mail}` 自动查找用户的域名。
- **密码**：输入 Exchange 用户帐户的可选密码。
- **电子邮件同步时间间隔**：在列表中，选择电子邮件与 Exchange Server 同步的频率。默认值为 **3 天**。
- **身份凭据(密钥库或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。默认值为无。
- **授权电子邮件在帐户之间移动**：选择是否允许用户将电子邮件从此帐户移出到另一个帐户以及从其他帐户转发和答复。默认值为关。
- **仅从电子邮件应用程序发送电子邮件**：选择是否限制用户只能从 iOS 邮件应用程序发送电子邮件。默认值为关。
- **禁用最新电子邮件同步**：选择是否阻止用户同步最近使用的地址。默认值为关。此选项仅适用于 iOS 6.0 及更高版本。
- **启用 S/MIME**：选择此帐户是否支持 S/MIME 身份验证和加密。默认值为关。设置为开时，将显示以下两个字段：
 - **签署身份凭据**。默认值为无。
 - **加密身份凭据**。默认值为无。
- **启用“为消息单独设置 S/MIME”开关**：选择是否允许用户基于每个消息加密传出电子邮件。默认值为关。

配置 Mac OS X 设置

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Exchange Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several options are checked, including 'Mac OS X'. The main content area is titled 'Policy Information' and contains a description: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' Below the description are several input fields: 'Exchange ActiveSync account name*', 'User*', 'Email address*', 'Password', 'Internal Exchange host', 'Internal server port', 'Internal server path', 'Use SSL for internal Exchange host' (a toggle switch currently set to 'ON'), and 'External Exchange host'. At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **Exchange ActiveSync 帐户名称**：键入显示在用户设备上的电子邮件帐户的说明。
- **用户**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `${user.username}` 自动查找用户的名称。
- **电子邮件地址**：指定用户的完整电子邮件地址。可以在此字段中使用系统宏 `${user.mail}` 自动查找用户的域名。
- **密码**：输入 Exchange 用户帐户的可选密码。
- **内部 Exchange 主机**：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选内部 Exchange 主机名。
- **内部服务器端口**：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选内部 Exchange Server 端口。
- **内部服务器路径**：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选内部 Exchange Server 路径。
- **对内部 Exchange 主机使用 SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。默认值为开。
- **外部 Exchange 主机**：如果希望内部和外部 Exchange 主机使用不同的名称，请键入可选外部 Exchange 主机名。
- **外部服务器端口**：如果希望内部和外部 Exchange Server 使用不同的端口，请键入可选外部 Exchange Server 端口。
- **外部服务器路径**：如果希望内部和外部 Exchange Server 使用不同的路径，请键入可选外部 Exchange Server 路径。
- **对外部 Exchange 主机使用 SSL**：选择是否确保用户设备与内部 Exchange 主机之间的连接安全。默认值为开。
- **允许投递邮件**：选择是否允许用户在两个 Mac 之间通过无线共享文件，且无须连接到现有网络。默认值为关。

配置 Android HTC 设置

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Exchange Policy' is selected in the left sidebar. The main area is titled 'Policy Information' and contains the following fields:

- Configuration display name* (text input)
- Server address* (text input)
- User ID* (text input)
- Password (text input)
- Domain (text input)
- Email address* (text input)
- Use SSL (toggle switch, currently ON)

Below the fields is a section for 'Deployment Rules'. At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **配置显示名称**：为此策略键入要在用户设备上显示的名称。
- **服务器地址**：键入 Exchange Server 的主机名或 IP 地址。
- **用户 ID**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `${user.username}` 自动查找用户的名称。
- **密码**：输入 Exchange 用户帐户的可选密码。
- **域**：输入 Exchange Server 所在的域。可以在此字段中使用系统宏 `${user.domainname}` 自动查找用户的域名。
- **电子邮件地址**：指定用户的完整电子邮件地址。可以在此字段中使用系统宏 `${user.mail}` 自动查找用户的域名。
- **使用 SSL**：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为开。

配置 Android TouchDown 设置

Exchange Policy

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Samsung SAFE
- Samsung KNOX
- Windows Phone

3 Assignment

Policy Information

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Server name or IP address*

Domain

User ID*

Password

Email address

Identity credential (keystore or PKI)

Policies and Apps

App Setting

Name	Value	Add
		<input type="button" value="Add"/>

Policy

Name	Value	Add
		<input type="button" value="Add"/>

Back Next >

配置以下设置：

- **服务器名称或 IP 地址**：键入 Exchange Server 的主机名或 IP 地址。
- **域**：键入 Exchange Server 所在的域。 可以在此字段中使用系统宏 `${user.domainname}` 自动查找用户的域名。
- **用户 ID**：指定 Exchange 用户帐户的用户名。 可以在此字段中使用系统宏 `${user.username}` 自动查找用户的名称。
- **密码**：键入 Exchange 用户帐户的可选密码。
- **电子邮件地址**：指定用户的完整电子邮件地址。 可以在此字段中使用系统宏 `${user.mail}` 自动查找用户的域名。
- **身份凭据(密钥库或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。默认值为无。
- **应用程序设置**：为此策略选择性添加 TouchDown 应用程序设置。
- **策略**：为此策略选择性添加 TouchDown 策略。

配置 Android for Work

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Exchange Policy' section is active, showing a sidebar with various platform options (iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX, Windows Phone) and an 'Assignment' section. The main area is titled 'Policy Information' and contains the following fields:

- Server name or IP address*
- Domain
- User ID*
- Password
- Email address
- Identity credential (keystore or PKI) with a dropdown menu set to 'None'

Below the fields is a section for 'Deployment Rules'. At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **服务器名称或 IP 地址**：键入 Exchange Server 的主机名或 IP 地址。
- **域**：键入 Exchange Server 所在的域。可以在此字段中使用系统宏 `${user.domainname}` 自动查找用户的域名。
- **用户 ID**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `${user.username}` 自动查找用户的名称。
- **密码**：键入 Exchange 用户帐户的可选密码。
- **电子邮件地址**：指定用户的完整电子邮件地址。可以在此字段中使用系统宏 `${user.mail}` 自动查找用户的域名。
- **身份凭据(密钥库或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。默认值为无。

配置 Samsung SAFE 和 Samsung KNOX 设置

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Exchange Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several options are checked, including 'Samsung SAFE'. The main configuration area, titled 'Policy Information', contains the following fields and settings:

- Server name or IP address* (text input)
- Domain (text input)
- User ID* (text input)
- Password (text input)
- Email address* (text input)
- Identity credential (keystore or PKI) (dropdown menu, currently set to 'None')
- Use SSL connection (toggle switch, currently 'ON')
- Sync contacts (toggle switch, currently 'ON')
- Sync calendar (toggle switch, currently 'ON')

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **服务器名称或 IP 地址**：键入 Exchange Server 的主机名或 IP 地址。
- **域**：键入 Exchange Server 所在的域。可以在此字段中使用系统宏 `${user.domainname}` 自动查找用户的域名。
- **用户 ID**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `${user.username}` 自动查找用户的名称。
- **密码**：键入 Exchange 用户帐户的可选密码。
- **电子邮件地址**：指定用户的完整电子邮件地址。可以在此字段中使用系统宏 `${user.mail}` 自动查找用户的域名。
- **身份凭据(密钥库或 PKI)**：如果为 XenMobile 配置了身份提供程序，请在列表中，单击可选身份凭据。仅当 Exchange 需要执行客户端证书身份验证时才需要配置此字段。
- **使用 SSL 连接**：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为开。
- **同步联系人**：选择是否在用户设备与 Exchange Server 之间启用用户联系人的同步。默认值为开。
- **同步日历**：选择是否在用户设备与 Exchange Server 之间启用用户日历的同步。默认值为开。
- **默认帐户**：选择是否将用户的 Exchange 帐户设置为默认帐户，用于从其设备发送电子邮件。默认值为开。

配置 Windows Phone 设置

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Exchange Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' The configuration fields are: 'Account name or display name*', 'Server name or IP address*', 'Domain', 'User ID or user name*', 'Email address*', 'Use SSL connection' (set to OFF), 'Sync items' (set to All content), and 'Sync scheduling' (set to When item arrives). There are 'Back' and 'Next >' buttons at the bottom right.

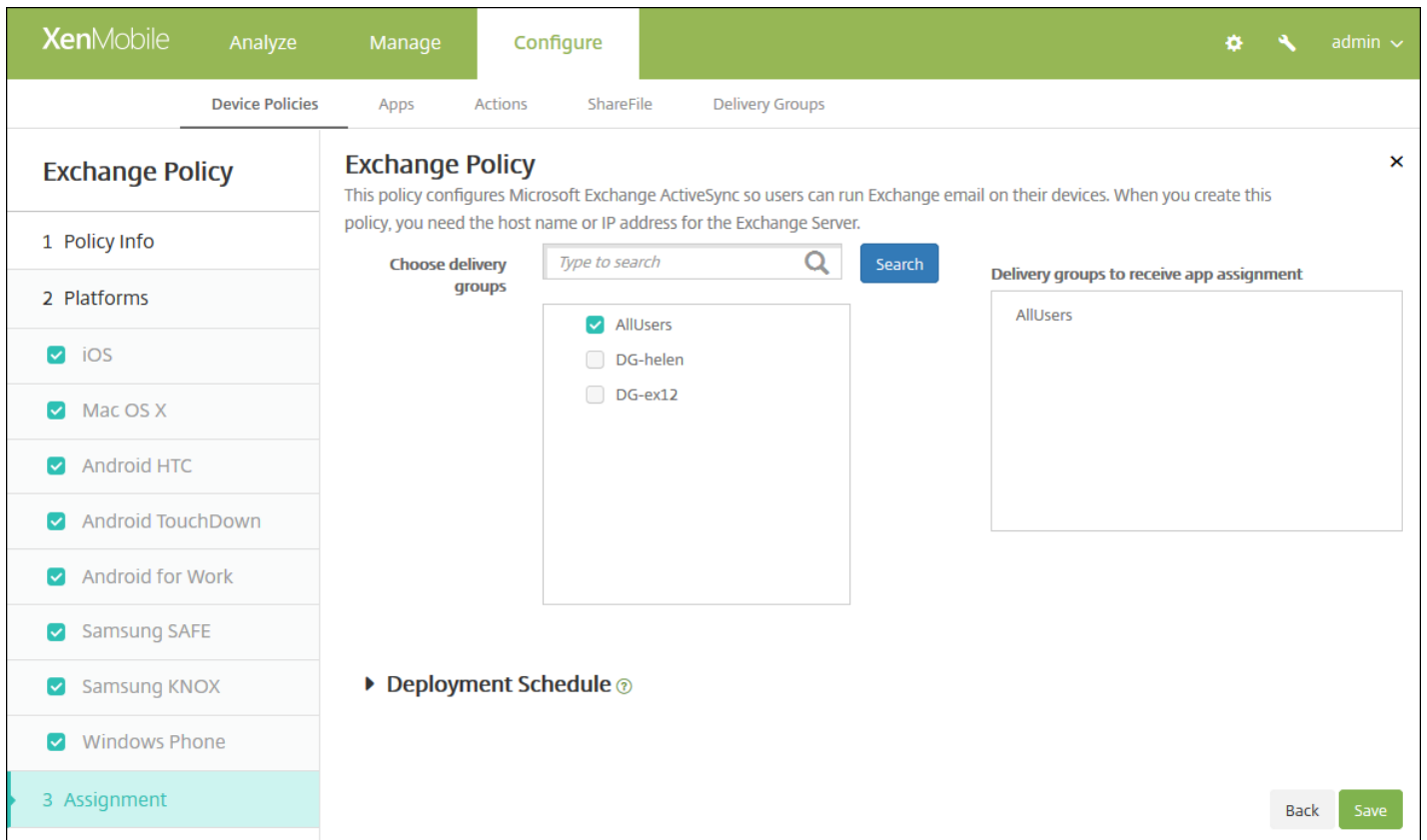
配置以下设置：

注意：此策略不允许您设置用户密码。用户在推送策略后必须从其设备设置该参数。

- **帐户名称或显示名称**：键入 Exchange ActiveSync 帐户名称。
- **服务器名称或 IP 地址**：键入 Exchange Server 的主机名或 IP 地址。
- **域**：输入 Exchange Server 所在的域。可以在此字段中使用系统宏 `${user.domainname}` 自动查找用户的域名。
- **用户 ID 或用户名**：指定 Exchange 用户帐户的用户名。可以在此字段中使用系统宏 `${user.username}` 自动查找用户的名称。
- **电子邮件地址**：指定用户的完整电子邮件地址。可以在此字段中使用系统宏 `${user.mail}` 自动查找用户的域名。
- **使用 SSL 连接**：选择是否确保用户设备与 Exchange Server 之间的连接安全。默认值为关。
- **同步内容天数**：在列表中，请单击要将设备上过去多少天内的所有内容与 Exchange Server 同步。默认值为**所有内容**。
- **频率**：在列表中，请单击同步从 Exchange Server 发送到设备的数据时要使用的计划。默认值为**When it arrives**（当其到达时）。
- **日志记录级别**：在列表中，请单击已禁用、基本或高级以指定记录 Exchange 活动时的详细级别。默认值为**已禁用**。

7. 配置部署规则

8. 单击下一步。此时将显示 **Exchange 策略分配** 页面。



9. 在选择交付组旁边，键入以查找交付组，或在列表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。

组织信息设备策略

Feb 27, 2017

可以在 XenMobile 中添加设备策略以指定贵组织从 XenMobile 推送到 iOS 设备的警报消息信息。此策略适用于 iOS 7 及更高版本的设备。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 单击更多，然后在最终用户下，单击组织信息。此时将显示组织信息策略页面。

The screenshot shows the XenMobile interface for configuring an 'Organization Info Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is divided into a sidebar and a main panel. The sidebar has three sections: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is expanded to show '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded to show a checked checkbox for 'iOS'. The main panel is titled 'Policy Information' and contains the following text: 'This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.' Below this text are two input fields: 'Policy Name*' (a text box) and 'Description' (a larger text box). A 'Next >' button is located at the bottom right of the main panel.

4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：如有需要，请键入策略的说明。

5. 单击下一步。此时将显示 iOS 平台信息页面。

Organization Info Policy

1 Policy Info

2 Platforms

iOS

3 Assignment

Policy Information ✕

This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.

Name ⓘ iOS 7.0+

Address ⓘ iOS 7.0+

Phone ⓘ iOS 7.0+

Email ⓘ iOS 7.0+

Magic ⓘ iOS 7.0+

► Deployment Rules

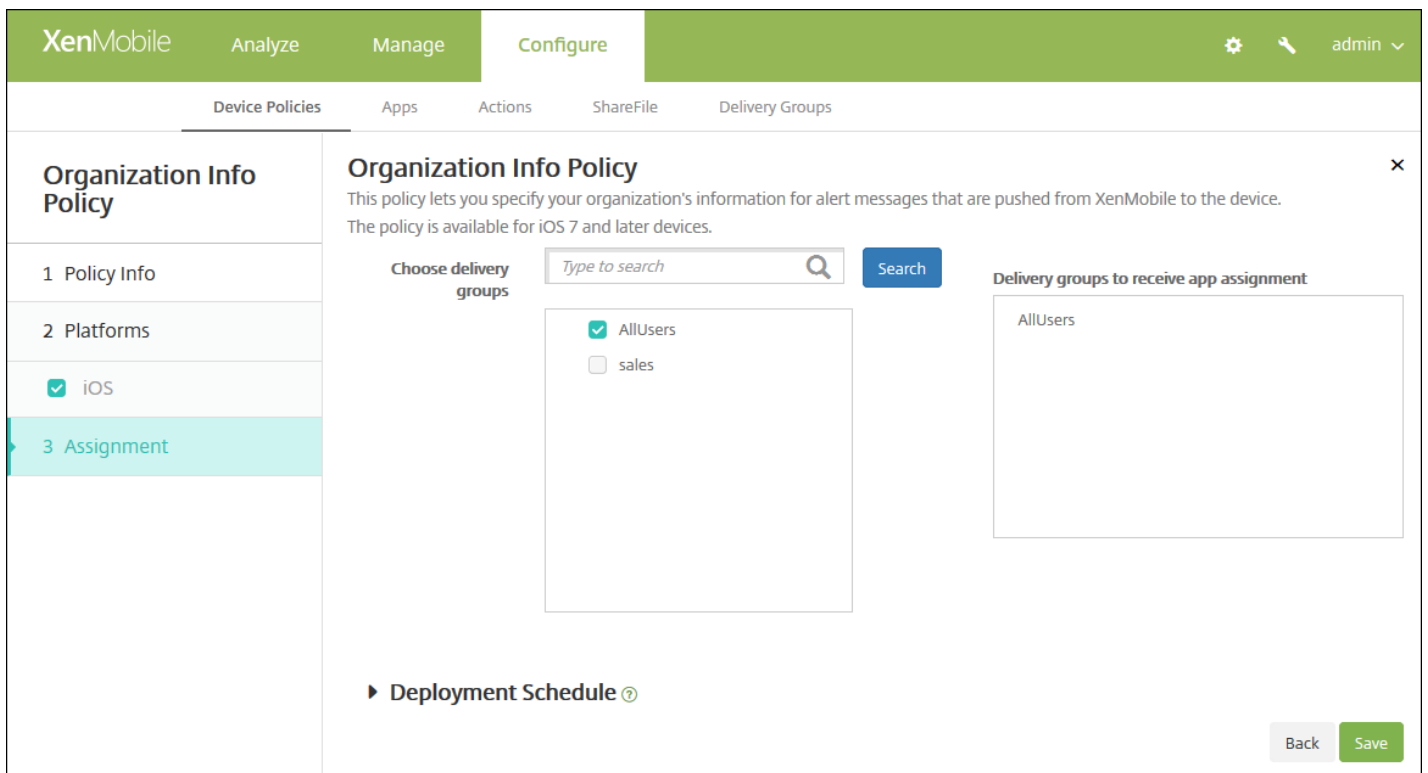
Back Next >

配置以下设置：

- **名称**：键入运行 XenMobile 的组织名称。
- **地址**：键入组织的地址。
- **电话**：键入组织的技术支持电话号码。
- **电子邮件**：键入技术支持电子邮件地址。
- **魔术字**：键入用于描述组织托管的服务的单词或短语。

7. 配置部署规则

8. 单击下一步。此时将显示组织信息策略分配页面。



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**。

通行码设备策略

Feb 27, 2017

可以根据贵组织的标准在 XenMobile 中创建通行码策略。可以要求在用户设备上输入通行码，并且可以设置各种格式和通行码规则。您可以为 iOS、Mac OS X、Android、Samsung KNOX、Android for Work、Windows Phone 和 Windows Desktop/Tablet 创建策略。每种平台需要一组不同的值，本文将对此进行介绍。

[iOS 设置](#)

[Mac OS X 设置](#)

[Android 设置](#)

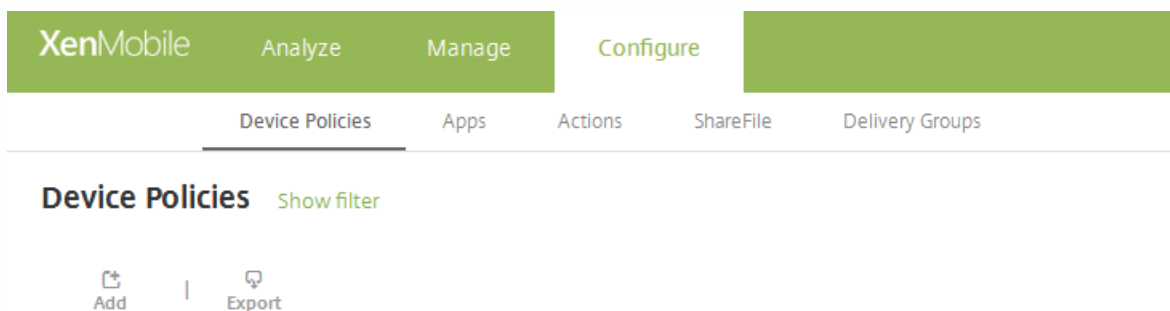
[Samsung KNOX 设置](#)

[Android for Work 设置](#)

[Windows Phone 设置](#)

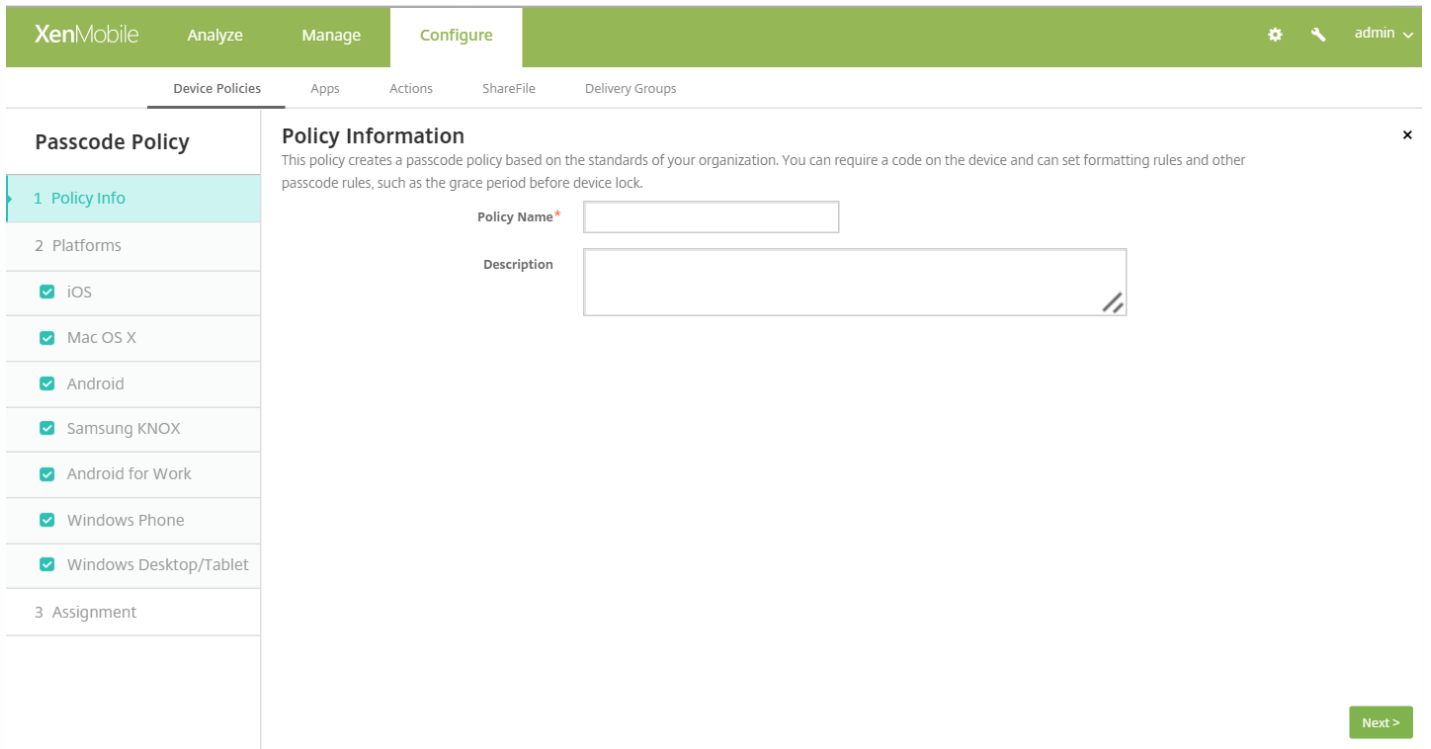
[Windows Desktop/Tablet 设置](#)

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



2. 单击添加。此时将显示“添加新策略”页面。

3. 单击通行码。此时将显示通行码策略信息页面。



4. 在策略信息窗格中，输入以下信息：

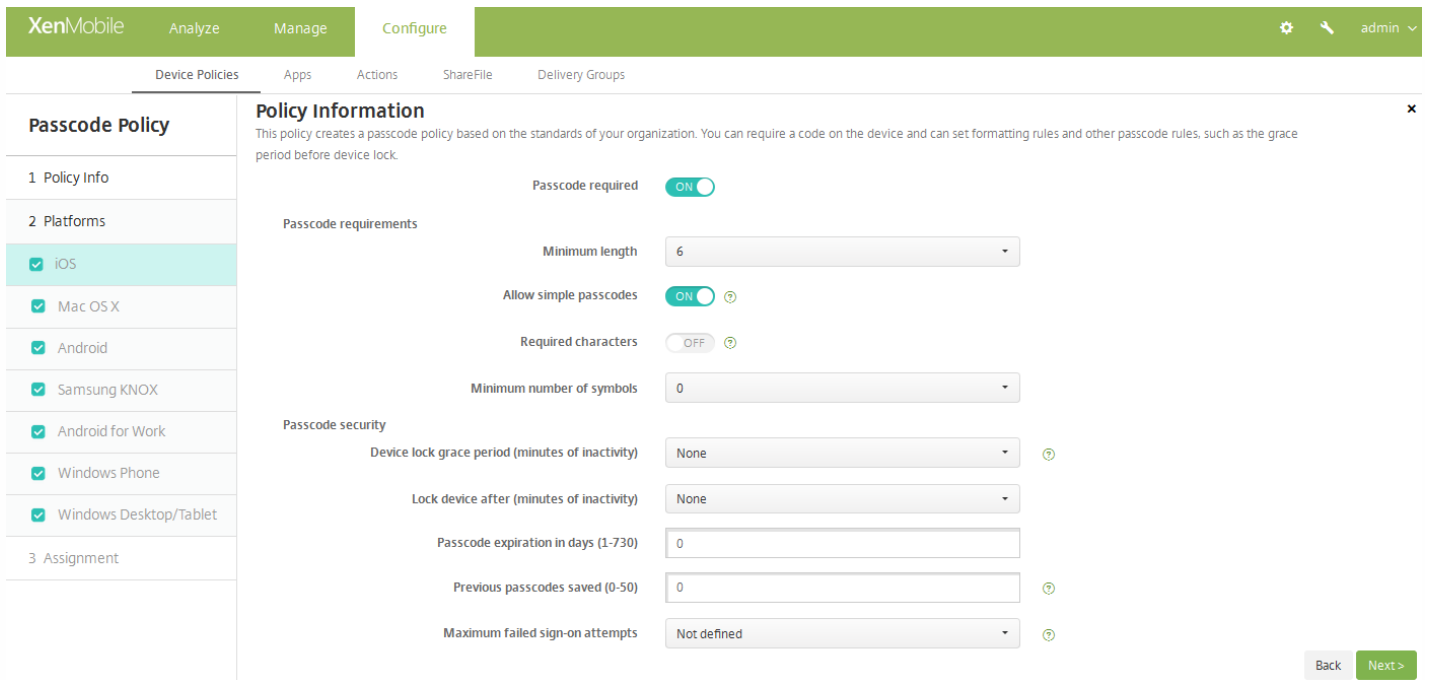
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击下一步。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

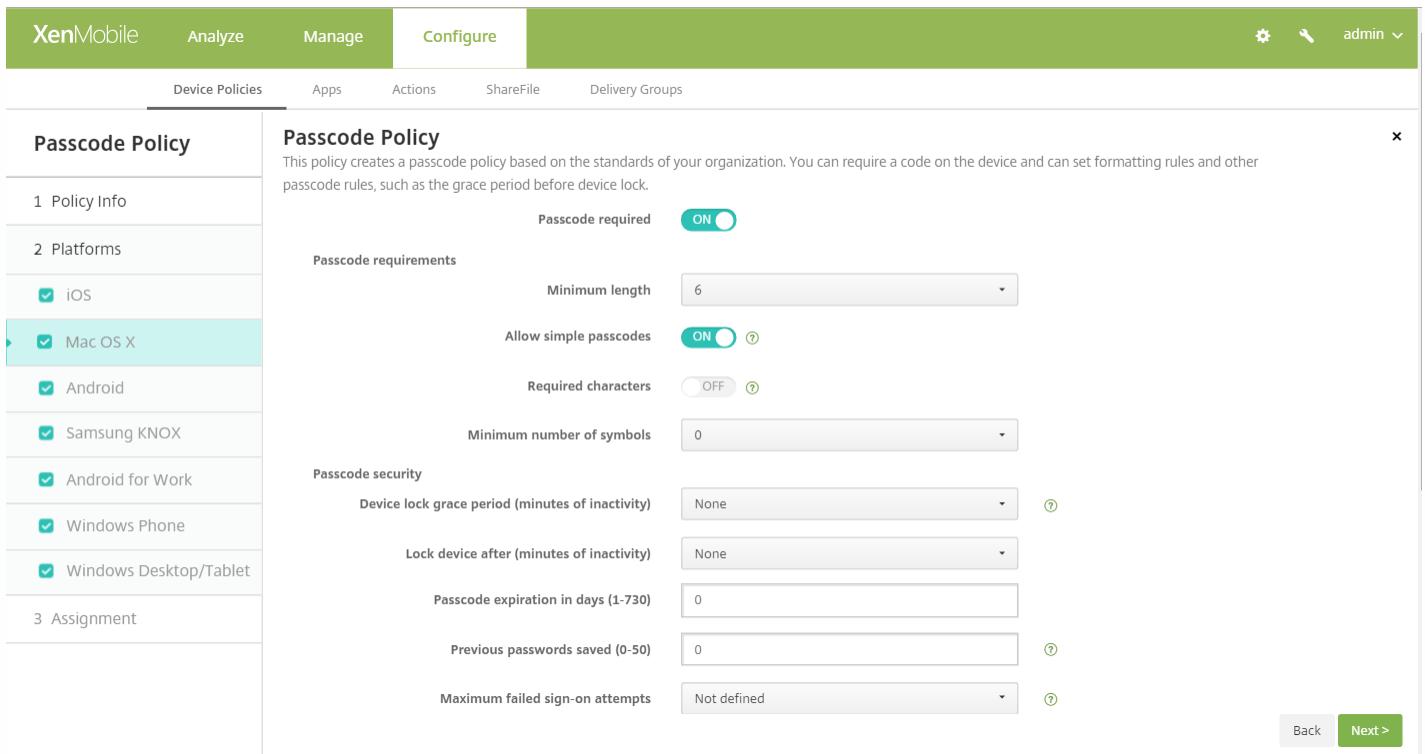
配置 iOS 设置



配置以下设置：

- **需要通行码**：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。
- **通行码要求**
 - **最小长度**：在列表中，单击通行码的最小长度。默认值为 6。
 - **允许使用简单通行码**：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为开。
 - **需含字符**：选择是否要求通行码至少包含一个字母。默认值为关。
 - **符号数下限**：在列表中，单击通行码必须包含的符号数量。默认值为 0。
- **通行码安全**
 - **设备锁定宽限期(不活动分钟)**：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。默认值为无。
 - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的时间长度。默认值为“无”。
 - **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 0，表示通行码永不过期。
 - **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中的任何密码。有效值为 0-50。默认值为 0，表示用户可以重复使用密码。
 - **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被完全擦除。默认值为未定义。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

配置 Mac OS X 设置



配置以下设置：

- **需要通行码**：选择此选项以要求输入通行码并显示 iOS 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性和策略设置的相关设置。
- 如果未启用**需要通行码**，请在**尝试登录失败后的延迟时间(分钟)**旁边，键入允许用户重新输入其通行码之前延迟的分钟数。
- 如果启用**需要通行码**，可以配置以下设置：
- **通行码要求**
 - **最小长度**：在列表中，单击通行码的最小长度。默认值为 6。
 - **允许使用简单通行码**：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为开。
 - **需含字符**：选择是否要求通行码至少包含一个字母。默认值为关。
 - **符号数下限**：在列表中，单击通行码必须包含的符号数量。默认值为 0。
- **通行码安全**
 - **设备锁定宽限期(不活动分钟)**：在列表中，单击用户必须输入通行码以解锁锁定设备之前的时间长度。默认值为无。
 - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的时间长度。默认值为无。
 - **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 0，表示通行码永不过期。
 - **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到任何密码。有效值为 0-50。默认值为 0，表示用户可以重复使用密码。
 - **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被锁定。默认值为未定义。
 - **尝试登录失败后的延迟时间(分钟)**：键入允许用户重新输入其通行码之前延迟的分钟数。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

- 在配置文件作用域旁边，单击用户或系统。默认值为用户。此选项仅适用于 OS X 10.7 及更高版本。

配置 Android 设置

配置以下设置：

注意：Android 的默认值为关。

- **需要通行码**：选择此选项以要求输入通行码并显示 Android 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求、通行码安全性、加密和 Samsung SAFE 的相关设置。
- **通行码要求**
 - **最小长度**：在列表中，单击通行码的最小长度。默认值为 6。
 - **生物特征识别**：选择是否启用生物特征识别。如果启用此选项，需含字符字段将隐藏。默认值为关。
 - **需含字符**：在列表中，单击“无限制”、“数字和字母”、“仅限数字”或“仅限字母”以配置通行码的组成方式。默认值为“无限制”。
 - **高级规则**：选择是否应用高级通行码规则。此选项适用于 Android 3.0 及更高版本。默认值为关。
 - 启用高级规则时，请在以下每个列表中，单击通行码必须包含的每种字符类型的最小数量：
 - **符号**：符号的最小数量。
 - **字母**：字母的最小数量。
 - **小写字母**：小写字母的最小数量。
 - **大写字母**：大写字母的最小数量。
 - **数字或符号**：数字或符号的最小数量。
 - **数字**：数字的最小数量。
- **通行码安全**
 - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的时间长度。默认值为无
 - **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 0，表示通行码永不过期。

- **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
- **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，设备将被擦除。默认值为未定义。
- **加密**
 - **启用加密**：选择是否启用加密。此选项适用于 Android 3.0 及更高版本。无论需要通行码设置为何，此选项都可用。

注意：要加密其设备，用户必须首先具有充电电池并将此设备接通电源一个小时或更长时间，以便进行加密。如果中断加密过程，可能会丢失其设备上的部分或全部数据。设备加密后，过程无法逆转，除非执行出厂重置，但这样会擦除设备上的所有数据。

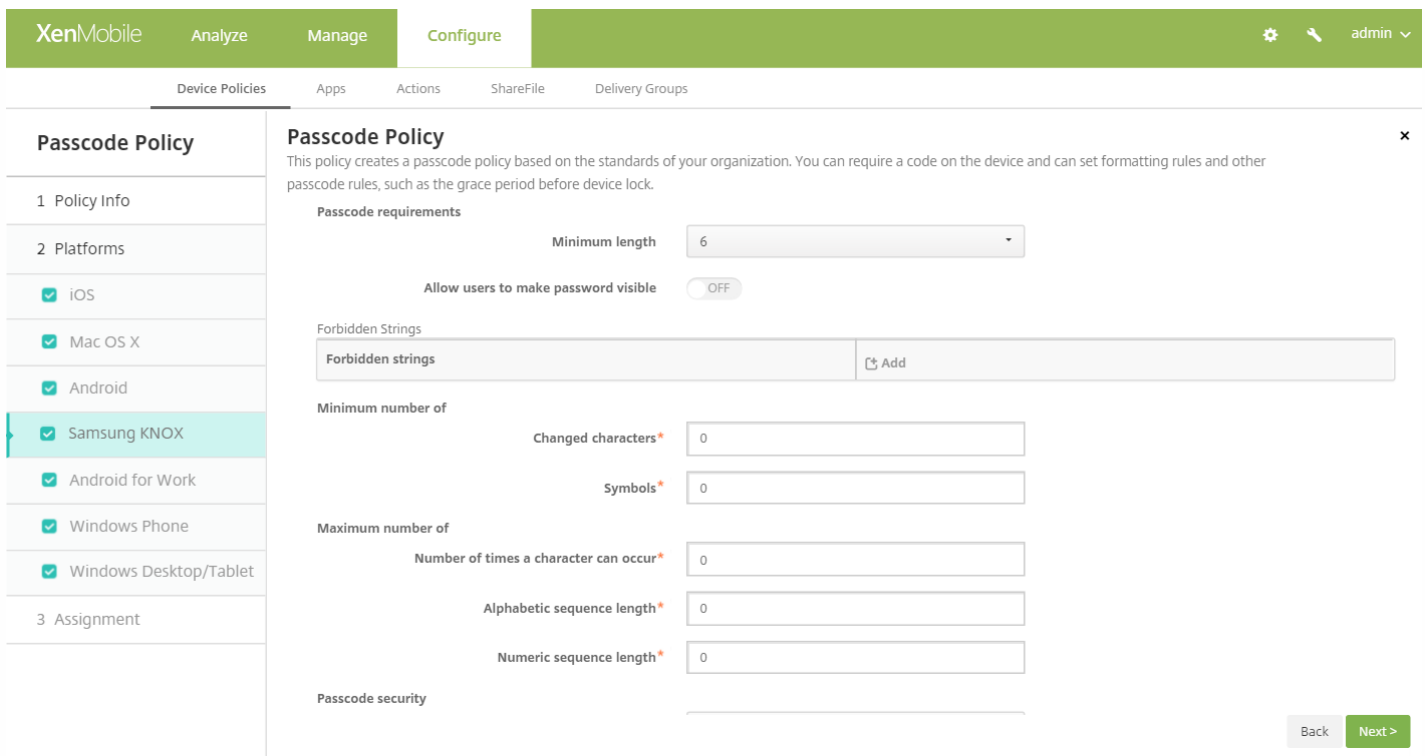
- **Samsung SAFE**

- **对所有用户使用相同的通行码**：选择是否对所有用户使用相同的通行码。默认值为关。此设置仅适用于 Samsung SAFE 设备，无论需要通行码设置为何，此选项都可用。
- **启用对所有用户使用相同的通行码时**，在**通行码**字段键入供所有用户使用的通行码。
- 如果启用需要通行码，可以配置以下 Samsung SAFE 设置：
 - **更改的字符**：键入以前的通行码中用户必须更改的字符数量。默认值为 **0**。
 - **字符可以出现的次数**：键入某个字符可以在通行码中出现的最大次数。默认值为 **0**。
 - **字母序列长度**：键入通行码中字母序列的最大长度。默认值为 **0**。
 - **数字序列长度**：键入通行码中数字序列的最大长度。默认值为 **0**。
 - **允许用户将密码设为可见**：选择用户是否可以将通行码设为可见。默认值为开。
 - **禁止的字符**：可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。对于要拒绝的每个字符串，请单击**添加**并执行以下操作：
 - **禁止的字符**：键入用户不能使用的字符串。
 - 单击**保存**以添加字符串，或单击**取消**以取消添加字符串。

注意：要删除现有字符串，请将鼠标悬停在包含此列表的行上，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**以保留列表。

要编辑现有字符串，请将鼠标悬停在包含此列表的行上，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

配置 Samsung KNOX 设置



配置以下设置：

- **通行码要求**

- **最小长度**：在列表中，单击通行码的最小长度。默认值为 6。
- **允许用户将密码设为可见**：选择是否允许用户将密码设为可见。
- **禁止的字符**：可以创建禁止的字符串以阻止用户使用 password、pwd、welcome、123456、111111 等很容易被猜到的不安全字符串。对于要拒绝的每个字符串，请单击“添加”并执行以下操作：
 - **禁止的字符**：键入用户不能使用的字符串。
 - 单击**保存**以添加字符串，或单击**取消**以取消添加字符串。

注意：要删除现有字符串，请将鼠标悬停在包含此列表的行上，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**以保留列表。

要编辑现有字符串，请将鼠标悬停在包含此列表的行上，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

- **最小数目**

- **更改的字符**：键入以前的通行码中用户必须更改的字符数量。默认值为 0。
- **符号**：键入通行码中所需符号的最小数量。默认值为 0。

- **最大数目**

- **字符可以出现的次数**：键入某个字符可以在通行码中出现的最大次数。默认值为 0。
- **字母序列长度**：键入通行码中字母序列的最大长度。默认值为 0。
- **数字序列长度**：键入通行码中数字序列的最大长度。默认值为 0。

- **通行码安全**

- **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的秒数。默认值为无。
- **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 0，表示通行码永不过期。

- **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中找到任何密码。有效值为 0-50。默认值为 0，表示用户可以重复使用密码。
- **如果超过失败登录尝试次数，设备将锁定**：在列表中，单击用户在成功登录之前能够失败的次数，超过此次数后，设备将被锁定。默认值为未定义。
- **如果超过失败登录尝试次数，设备将被擦除**：在列表中，单击用户在成功登录之前能够失败的次数，超过此次数后，将从设备中擦除 KNOX 容器（以及 KNOX 数据）。擦除后，用户需要重新初始化 KNOX 容器。默认值为未定义。

配置 Android for Work 设置

The screenshot shows the XenMobile configuration interface for a Passcode Policy. The interface is divided into a sidebar and a main content area. The sidebar has three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android for Work' is selected. The main content area is titled 'Policy Information' and contains the following settings:

- Passcode Required**: ON
- Passcode requirements**
 - Minimum length**: 6
 - Biometric recognition**: OFF
 - Required characters**: No restriction
 - Advanced rules**: OFF A 3.0+
- Passcode security**
 - Lock device after (minutes of inactivity)**: None
 - Passcode expiration in days (1-730)**: 0
 - Previous passwords saved (0-50)**: 0
 - Maximum failed sign-on attempts**: Not defined

配置以下设置：

- **需要通行码**：选择此选项以要求输入通行码并显示 Android for Work 通行码设备策略的配置选项。页面将展开以允许您配置通行码要求和通行码安全性的相关设置。
- **通行码要求**
 - **最小长度**：在列表中，单击通行码的最小长度。默认值为 6。
 - **生物特征识别**：选择是否启用生物特征识别。如果启用此选项，需含字符字段将隐藏。默认值为关。请注意，目前尚不支持此功能。
 - **需含字符**：在列表中，单击无限制、数字和字母、仅限数字或仅限字母以配置通行码的组成方式。默认值为无限制。
 - **高级规则**：选择是否应用高级通行码规则。此选项不适用于 Android 5.0 之前的 Android 设备。默认值为关。
 - **启用高级规则时**，请在以下每个列表中，单击通行码必须包含的每种字符类型的最小数量：
 - **符号**：符号的最小数量。
 - **字母**：字母的最小数量。
 - **小写字母**：小写字母的最小数量。
 - **大写字母**：大写字母的最小数量。
 - **数字或符号**：数字或符号的最小数量。
 - **数字**：数字的最小数量。
- **通行码安全**
 - **此时间后锁定设备(不活动分钟数)**：在列表中，单击设备在锁定之前可以不活动的分钟数。默认值为无

- **通行码有效期限(1 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。有效值为 1-730。默认值为 **0**，表示通行码永不过期。
- **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中的任何密码。有效值为 0-50。默认值为 **0**，表示用户可以重复使用密码。
- **失败登录尝试次数上限**：在列表中，单击用户在成功登录之前能够失败的次数，超过此次数后，将从设备中擦除 KNOX 容器（以及 KNOX 数据）。擦除后，用户需要重新初始化 KNOX 容器。默认值为未定义。

配置 Windows Phone 设置

The screenshot shows the XenMobile Configure interface for setting a Passcode Policy. The left sidebar has three main sections: 1. Policy Info, 2. Platforms, and 3. Assignment. Under Platforms, several options are checked: iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone (highlighted), and Windows Desktop/Tablet. The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' The configuration options are as follows:

- Passcode required**: ON (toggle)
- Allow simple passcodes**: OFF (toggle)
- Passcode requirements**:
 - Minimum length**: 6
 - Characters required**: Letters only
 - Minimum number of symbols**: 1
- Passcode security**:
 - Lock device after (minutes of inactivity)**: 0
 - Passcode expiration in 0-730 days***: 0
 - Previous passwords saved (0-50)**: 0
 - Maximum failed sign-on attempts before wipe (0-999)***: 0

At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **需要通行码**：选择此选项将不要求提供 Windows Phone 设备的通行码。默认值为开，即需要使用通行码。禁用此设置时，页面折叠，不再显示以下选项。
- **允许使用简单通行码**：选择是否允许使用简单通行码。简单通行码是指重复或连续的字符集。默认值为关。
- **通行码要求**
 - **最小长度**：在列表中，单击通行码的最小长度。默认值为 6。
 - **需含字符**：在列表中单击数字或字母数字、仅限字母或仅限数字以配置通行码的组成方式。默认值为仅限字母。
 - **符号数下限**：在列表中，单击通行码必须包含的符号数量。默认值为 1。
- **通行码安全**
 - **此时间后锁定设备(不活动分钟数)**：键入设备在锁定之前可以不活动的分钟数。默认值为 0。
 - **通行码在 0 - 730 天内有效**：键入有效天数，超过此天数后，通行码将过期。有效值为 0-730。默认值为 0，表示通行码永不过期。
 - **保存的以前用过的密码数量(0-50)**：键入要保存的使用过的密码数量。用户无法使用在此列表中的任何密码。有效值为 0-50。默认值为 0，表示用户可以重复使用密码。
 - **擦除前的最大失败登录尝试次数(0 - 999)**：键入用户在成功登录之前能够失败的次数，超过此次数后，将擦除设备中的企业数据。默认值为 0。

配置 Windows Desktop/Tablet 设置

Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Disallow convenience logon OFF

Minimum passcode length 6

Maximum passcode attempts before wipe 4

Passcode expiration in days (0-730)* 0

Passcode history (1-24)* 0

Maximum inactivity before device lock in minutes (1-999) 0

► **Deployment Rules**

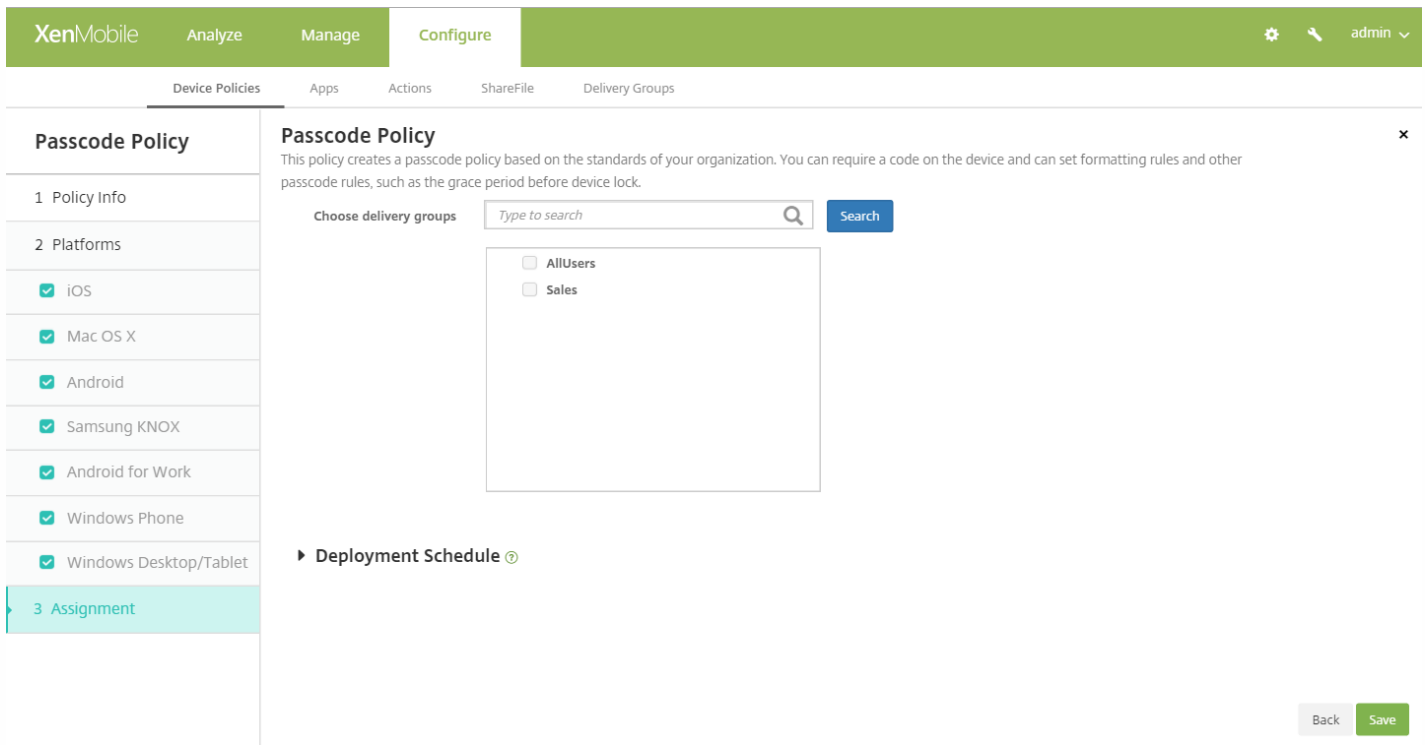
Back Next >

配置以下设置：

- **不允许便捷登录**：选择是否允许用户使用图片密码或生物特征登录访问其设备。默认值为关。
- **最小通行码长度**：在列表中，单击通行码的最小长度。默认值为 6。
- **擦除前的通行码尝试次数上限**：在列表中，单击用户在成功登录之前可以失败的次数，超过此次数后，将擦除设备中的企业数据。默认值为 4。
- **通行码有效期限(0 - 730 天)**：键入有效天数，超过此天数后，通行码将过期。有效值为 0-730。默认值为 0，表示通行码永不过期。
- **通行码历史记录: (1-24)**：键入要保存的使用过的通行码数量。用户无法使用在此列表中的任何通行码。有效值为 1-24。必须在此字段中输入介于 1 到 24 之间的数值。默认值为 0。
- **设备锁定前的最长不活动时间(1 - 999 分钟)**：输入设备在锁定之前可以不活动的时间长度（分钟）。有效值为 1-999。必须在此字段中输入介于 1 到 999 之间的数值。默认值为 0。

7. 配置部署规则

8. 单击下一步。此时将显示通行码策略分配页面。



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**。

个人热点设备策略

Feb 27, 2017

当用户不在 WiFi 网络范围内，可以允许用户通过其 iOS 设备的个人热点功能，使用手机数据网络连接到 Internet。适用于 iOS 7.0 及更高版本。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略页面。
3. 展开更多，然后在网络访问权限下，单击个人热点。此时将显示个人热点策略信息页面。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

Personal Hotspot Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

Policy Information

This policy lets you enable or disable a personal hotspot on a device. This policy is available for iOS 7 and later devices.

Policy Name*

Description

Next >

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。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

Personal Hotspot Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

Policy Information

This policy lets you enable or disable a personal hotspot on a device. This policy is available for iOS 7 and later devices.

Disable personal hotspot OFF iOS 7.0+

► Deployment Rules

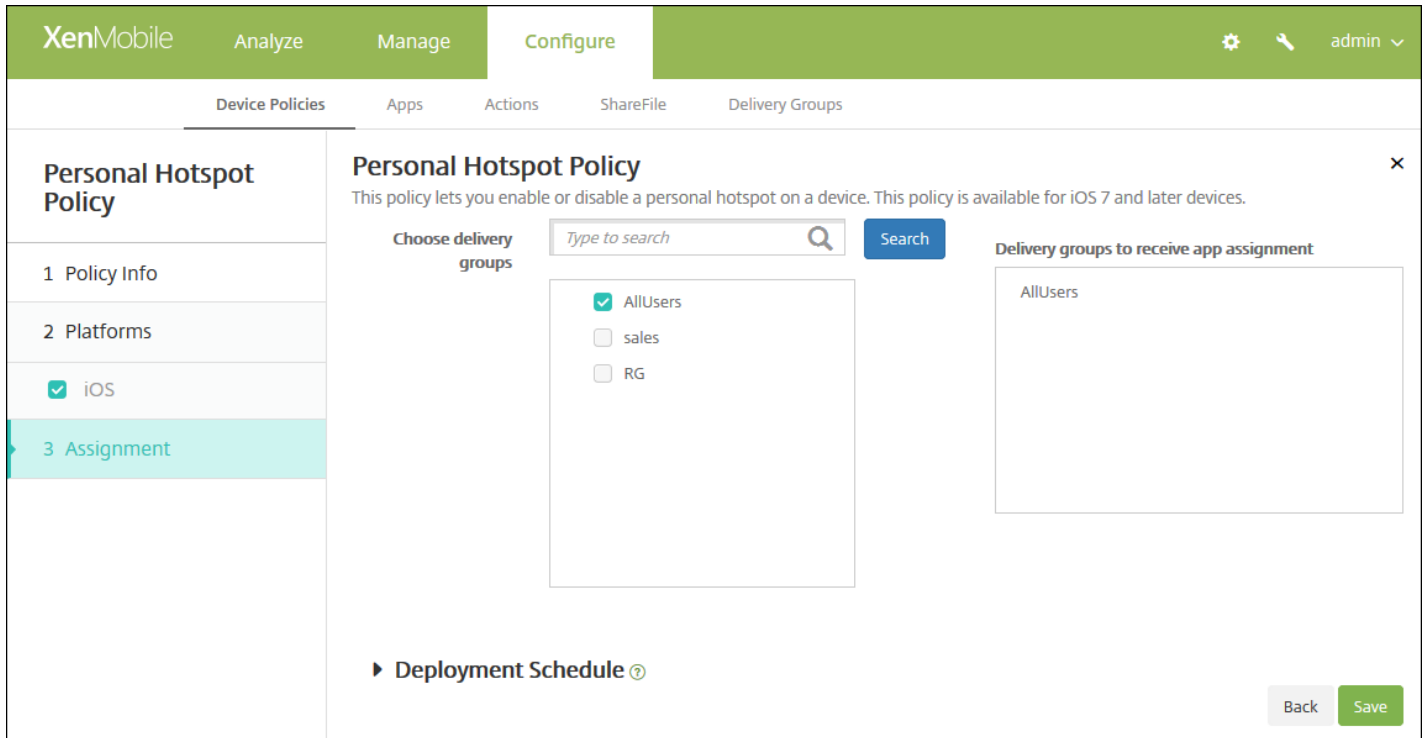
Back Next >

6. 配置以下设置：

- **禁用个人热点**：选择是否在用户设备上禁用个人热点功能。默认值为关，即在用户设备上关闭个人热点。此策略不禁用该功能；用户仍可以在其设备上使用个人热点，但是部署此策略后，将关闭个人热点功能，因此默认情况下不打开此功能。

7. 配置部署规则

8. 单击下一步。将显示个人热点策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

配置文件删除设备策略

Feb 27, 2017

可以在 XenMobile 中创建应用程序配置文件删除设备策略。此策略在部署时，将从用户的 iOS 或 Mac OS X 设备删除应用程序配置文件。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在删除下方，单击配置文件删除。将显示配置文件删除策略信息页面。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Profile Removal Policy' and 'Policy Information'. It includes a sidebar with steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' step is active, showing a form with 'Policy Name*' and 'Description' fields. The 'Platforms' step shows 'iOS' and 'Mac OS X' selected with checkboxes. A 'Next >' button is visible at the bottom right.

4. 在策略信息窗格中，键入以下信息：

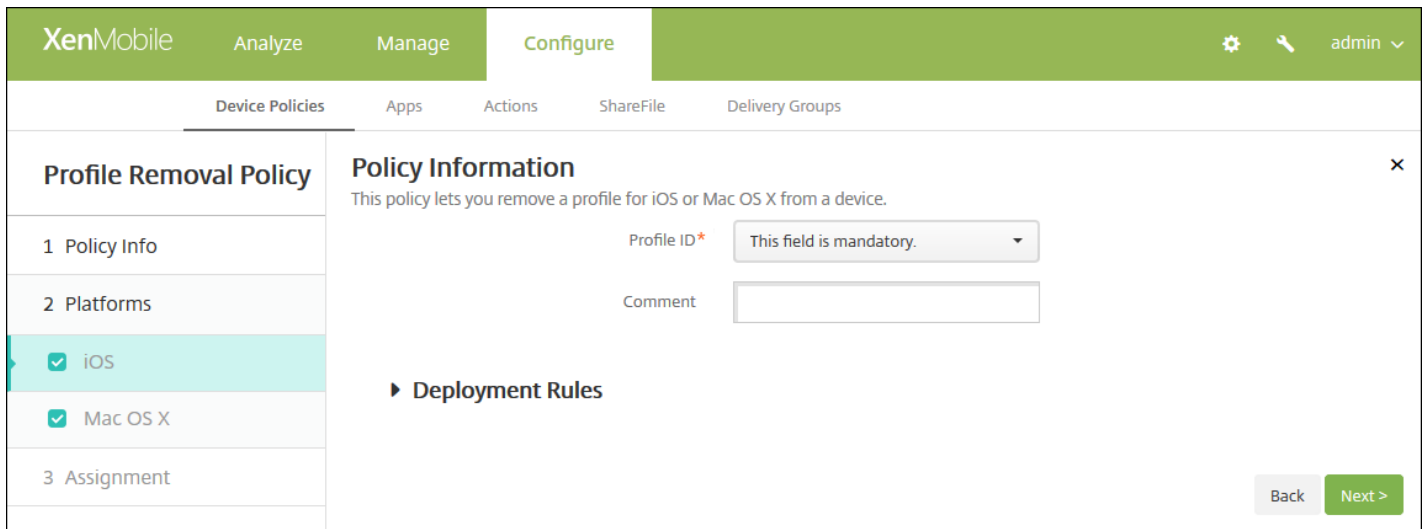
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

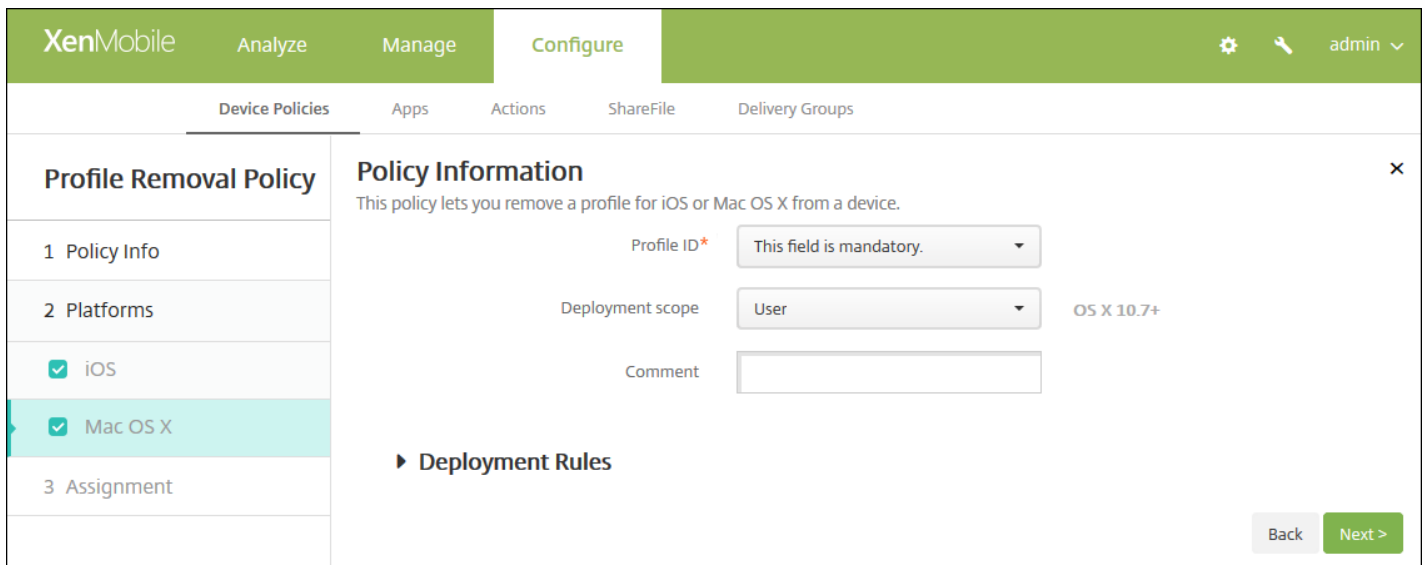
配置 iOS 设置



配置以下设置：

- **配置文件 ID**：在列表中，单击应用程序配置文件 ID。此字段为必填字段。
- **备注**：键入可选备注。

配置 Mac OS X 设置

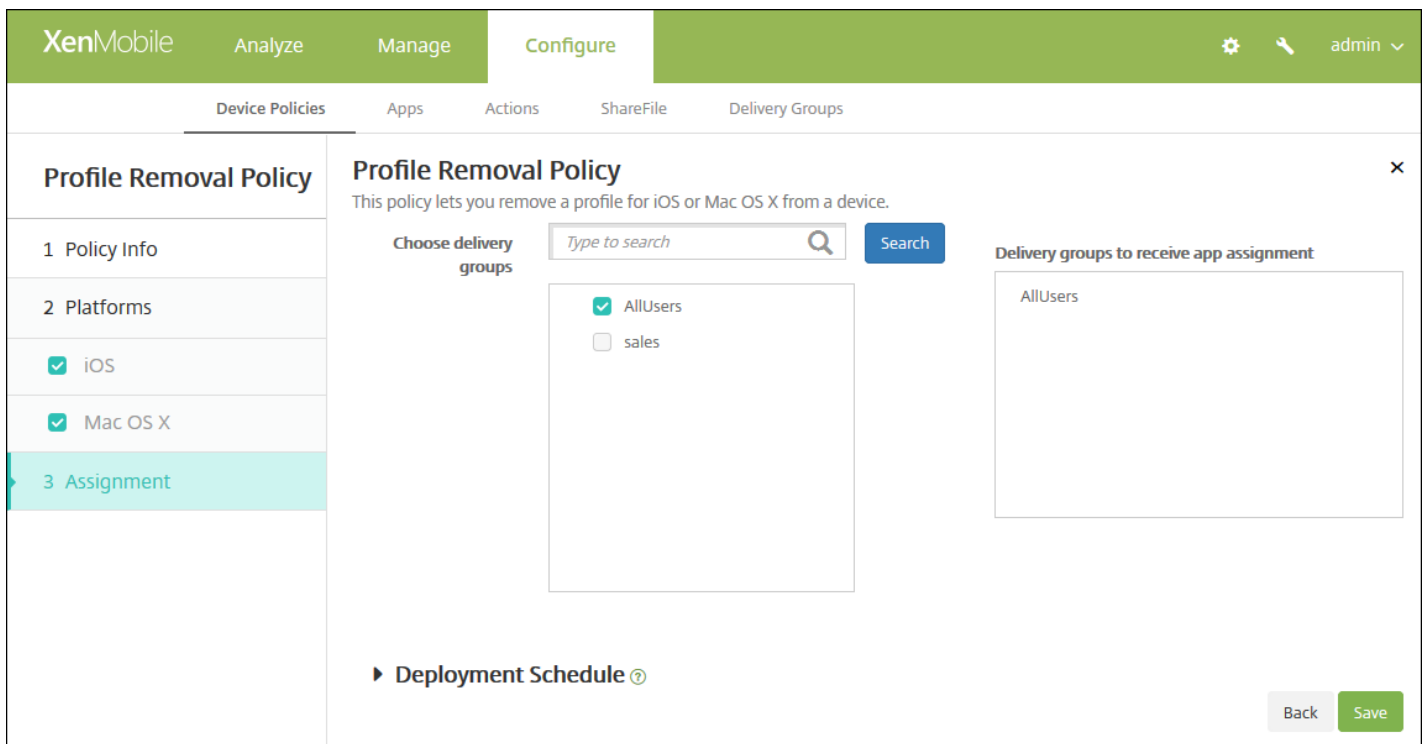


配置以下设置：

- **配置文件 ID**：在列表中，单击应用程序配置文件 ID。此字段为必填字段。
- **部署范围**：在列表中，单击用户或系统。默认值为用户。此选项仅适用于 OS X 10.7 及更高版本。
- **备注**：键入可选备注。

7. 配置部署规则

8. 单击下一步。将显示配置文件删除策略分配页面。



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**。

置备配置文件设备策略

Feb 27, 2017

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。两种解决方案分别为通过电子邮件将置备配置文件发送给用户或者将其置于 Web 门户中以供下载和安装。这些解决方案可行，但容易出错，因为需要用户响应电子邮件中的说明，或访问 Web 门户并下载正确的配置文件，然后再进行安装。

要使此过程对用户透明，您可以在 XenMobile 使用设备策略来安装和删除置备配置文件。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）。

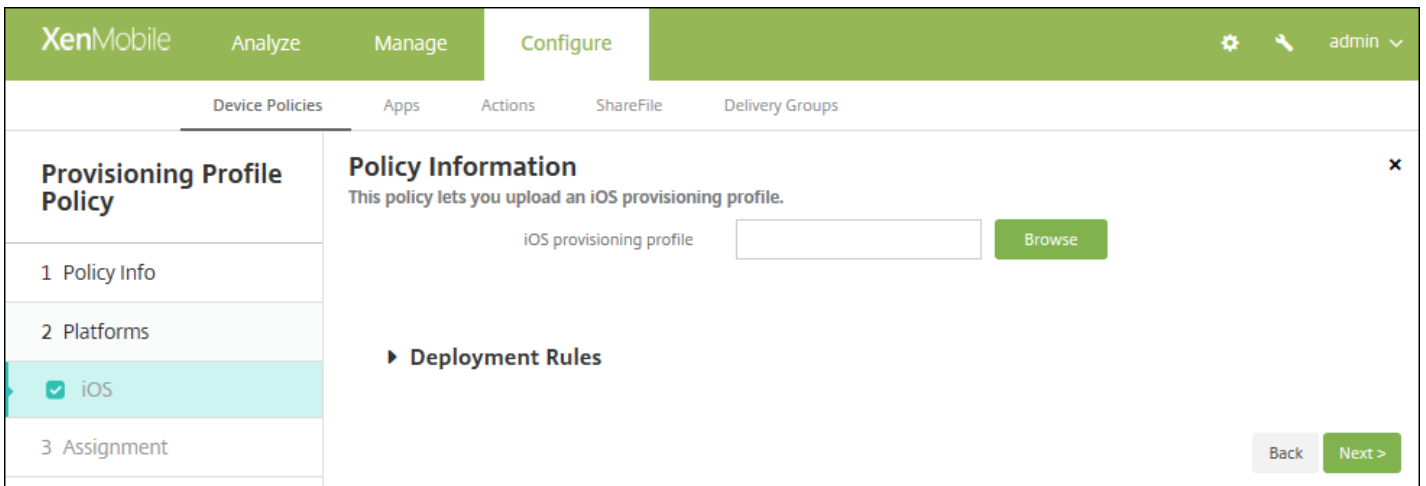
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**页面。
3. 展开**更多**，然后在**应用程序**下面，单击**置备配置文件**。此时将显示**置备配置文件策略**信息页面。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Provisioning Profile Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you upload an iOS provisioning profile.' Below the description are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form. On the left side, there is a sidebar with a list of steps: '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Assignment'. The '1 Policy Info' step is currently selected and highlighted in light blue.

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。

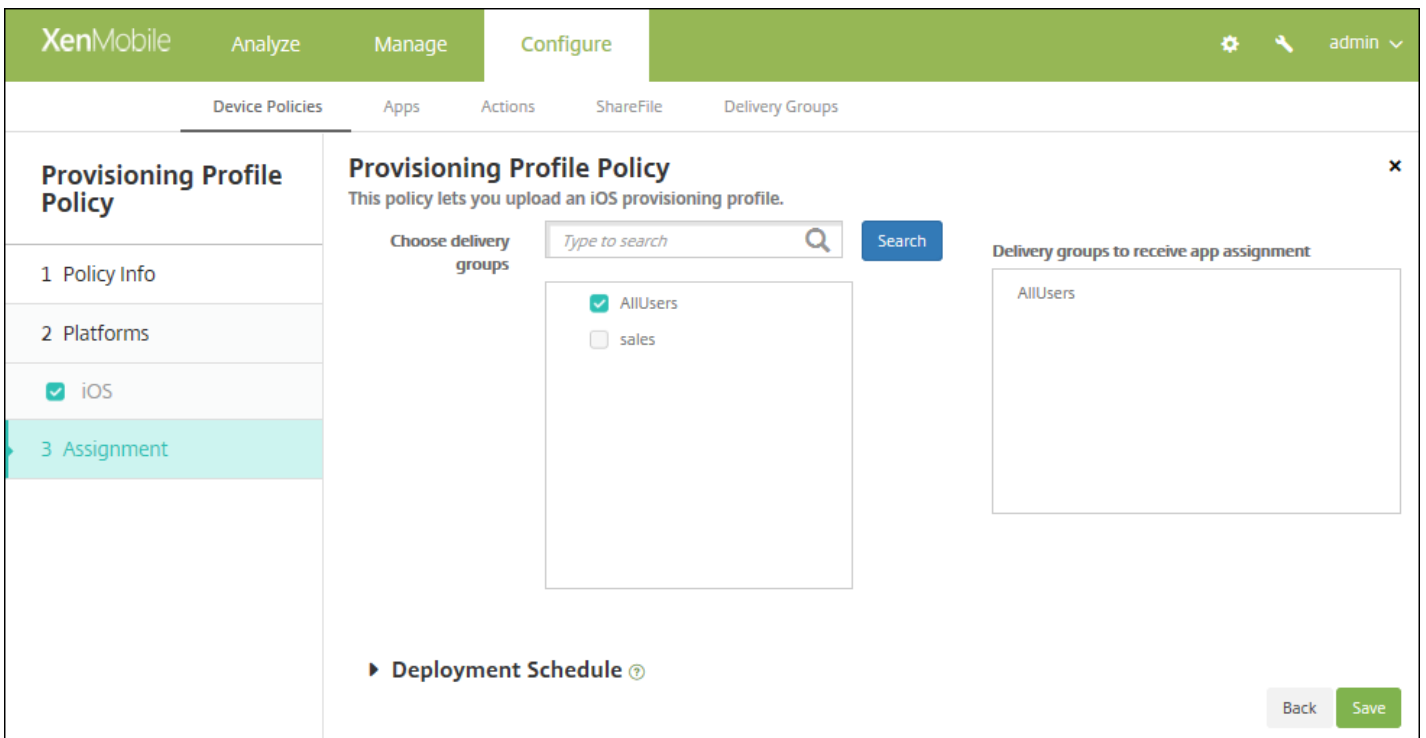


6. 配置以下设置：

- **iOS 置备配置文件**：单击浏览，然后导航到要导入的置备配置文件所在的位置，选择此文件。

7. 配置部署规则

8. 单击下一步。此时将显示置备配置文件策略分配页面。



9. 在选择交付组旁边，键入以查找交付组，或在列表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：

- 如果在设置 > 服务器属性中配置了计划后台部署密钥，则适用此选项。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

删除置备配置文件设备策略

Feb 27, 2017

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

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略页面。
3. 展开更多，然后在删除下方，单击删除置备配置文件。此时将显示置备配置文件删除策略信息页面。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Provisioning Profile Removal Policy' and contains a 'Policy Information' form. The form has two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form. On the left side, there is a sidebar with a 'Provisioning Profile Removal Policy' section containing three items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' item is currently selected.

4. 在策略信息窗格中，输入以下信息：

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

5. 单击下一步。此时将显示 iOS 平台页面。

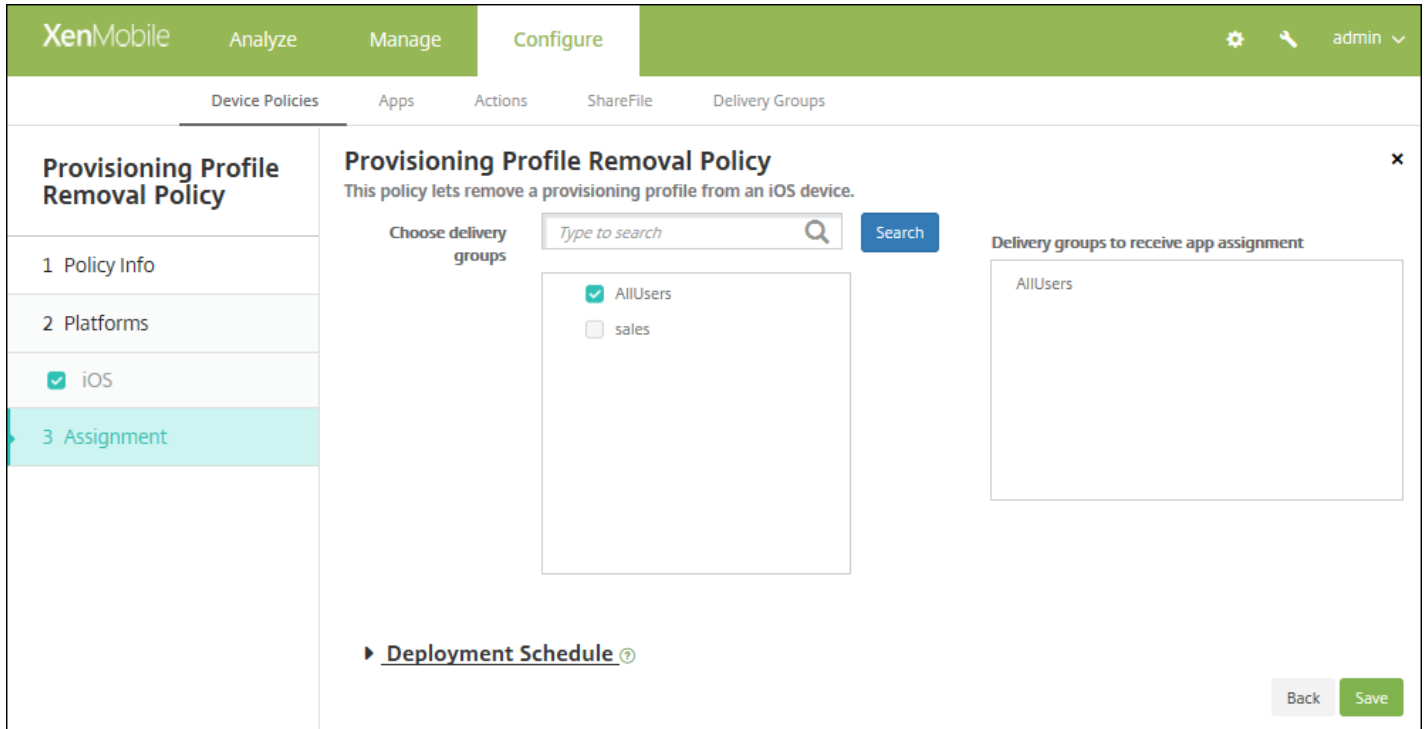
The screenshot shows the XenMobile console interface, similar to the previous one. The main content area is titled 'Provisioning Profile Removal Policy' and contains a 'Provisioning Profile Removal Policy' form. The form has two input fields: 'iOS provisioning profile*' (a dropdown menu with 'Select an option' as the selected value) and 'Comment'. A 'Deployment Rules' section is visible below the form. A 'Back' button and a 'Next >' button are located at the bottom right of the form. On the left side, there is a sidebar with a 'Provisioning Profile Removal Policy' section containing three items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' item is currently selected.

6. 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. 配置部署规则

8. 单击下一步。此时将显示置备配置文件删除策略分配页面。



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

10. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，**为始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

代理设备策略

Feb 27, 2017

可以在 XenMobile 中添加一个设备策略，为运行 Windows Mobile/CE 和 iOS 6.0 或更高版本的设备指定全局 HTTP 代理设置。只能为每个设备部署一个全局 HTTP 代理策略。

注意：在部署此策略之前，请务必将要为其设置全局 HTTP 代理的所有 iOS 设备设置为受监督模式。有关详细信息，请参阅[使用 Apple Configurator 将 iOS 设备置于受监督模式](#)。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**更多**，然后在**网络访问**下方，单击**代理**。此时将显示**代理策略**页面。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Proxy Policy' and contains a sidebar with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section is active, showing a description and two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. 在**策略信息**窗格中，输入以下信息：

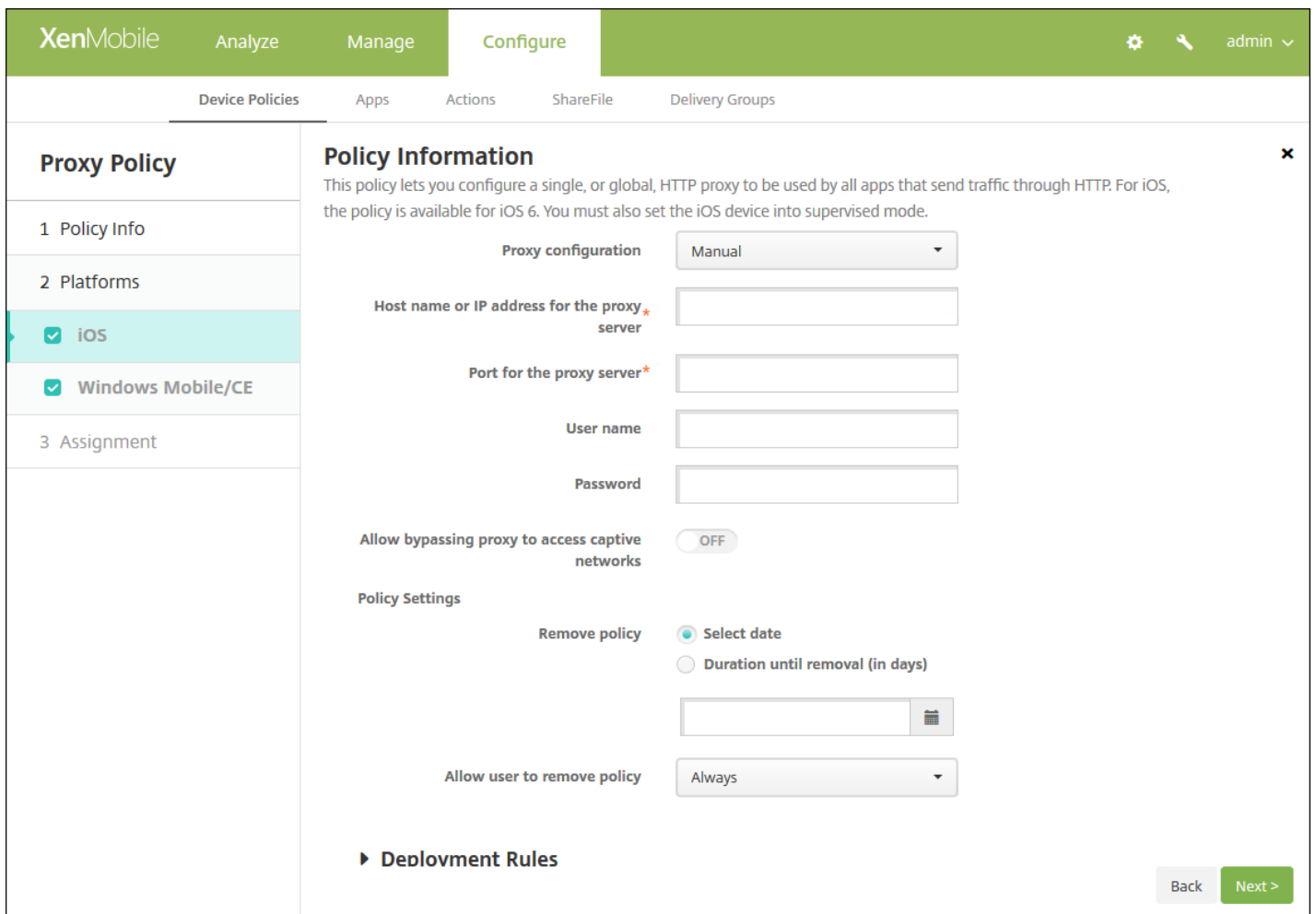
- **策略名称**：输入策略的描述性名称。
- **说明**：（可选）输入策略的说明。

5. 单击**下一步**。此时将显示**策略平台**页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

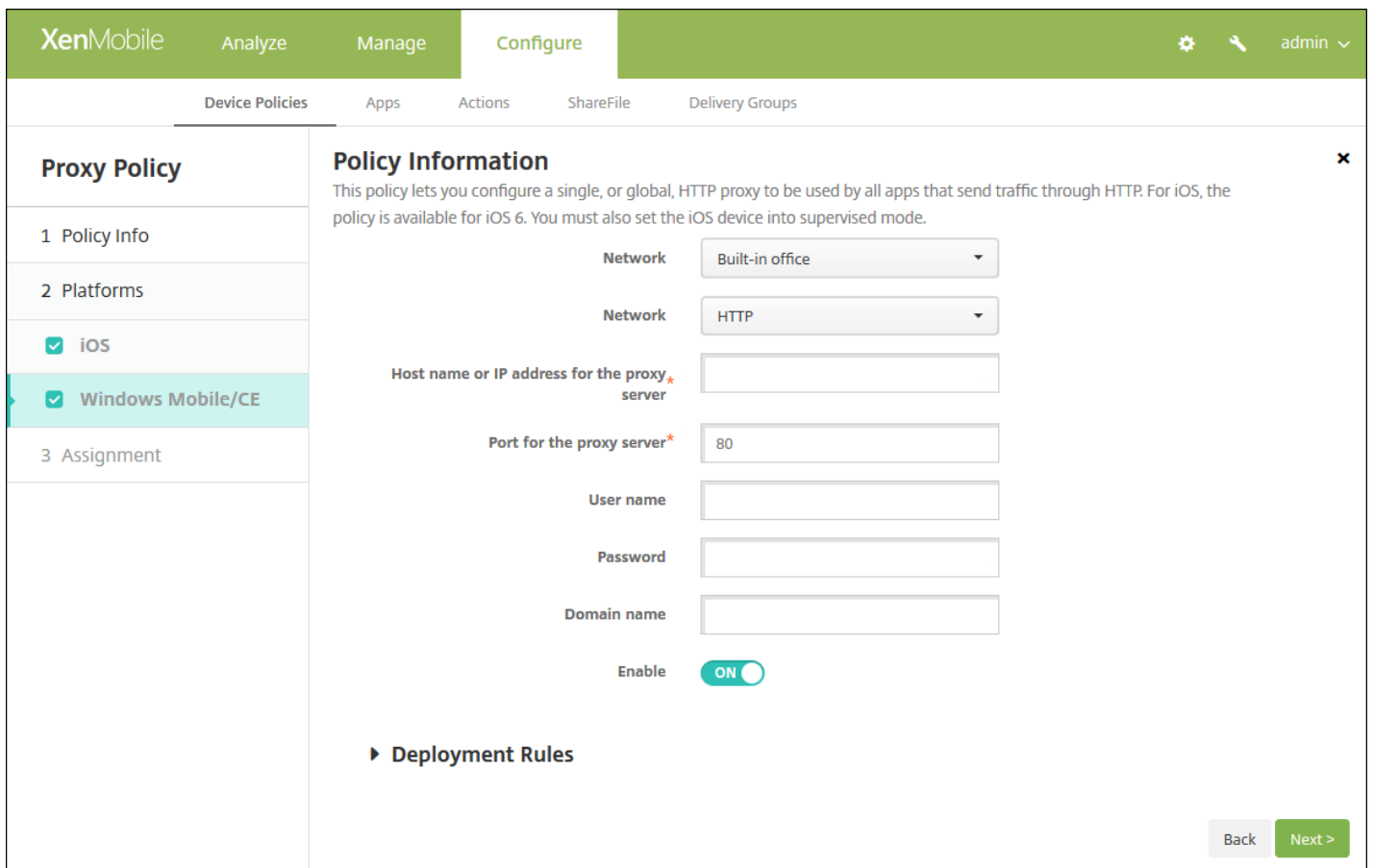
配置 iOS 设置



配置以下设置：

- **代理配置**：单击**手动**或**自动**以设置代理在用户设备上的配置方式。
 - 如果选择**手动**，可以配置以下设置：
 - **代理服务器的主机名或 IP 地址**：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
 - **代理服务器的端口**：键入代理服务器的端口号。此字段为必填字段。
 - **用户名**：键入向代理服务器进行身份验证的可选用户名。
 - **密码**：键入向代理服务器进行身份验证的可选密码。
 - 如果单击**自动**，可以配置以下设置：
 - **代理 PAC URL**：键入用于定义代理配置的 PAC 文件的 URL。
 - **允许在无法访问 PAC 时直接连接**：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。默认值为开。此选项仅适用于 iOS 7.0 及更高版本。
- **允许旁路代理以访问俘获型网络**：选择是否允许绕过代理来访问俘获型网络。默认值为关。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略列表**中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

配置 Windows Mobile/CE 设置

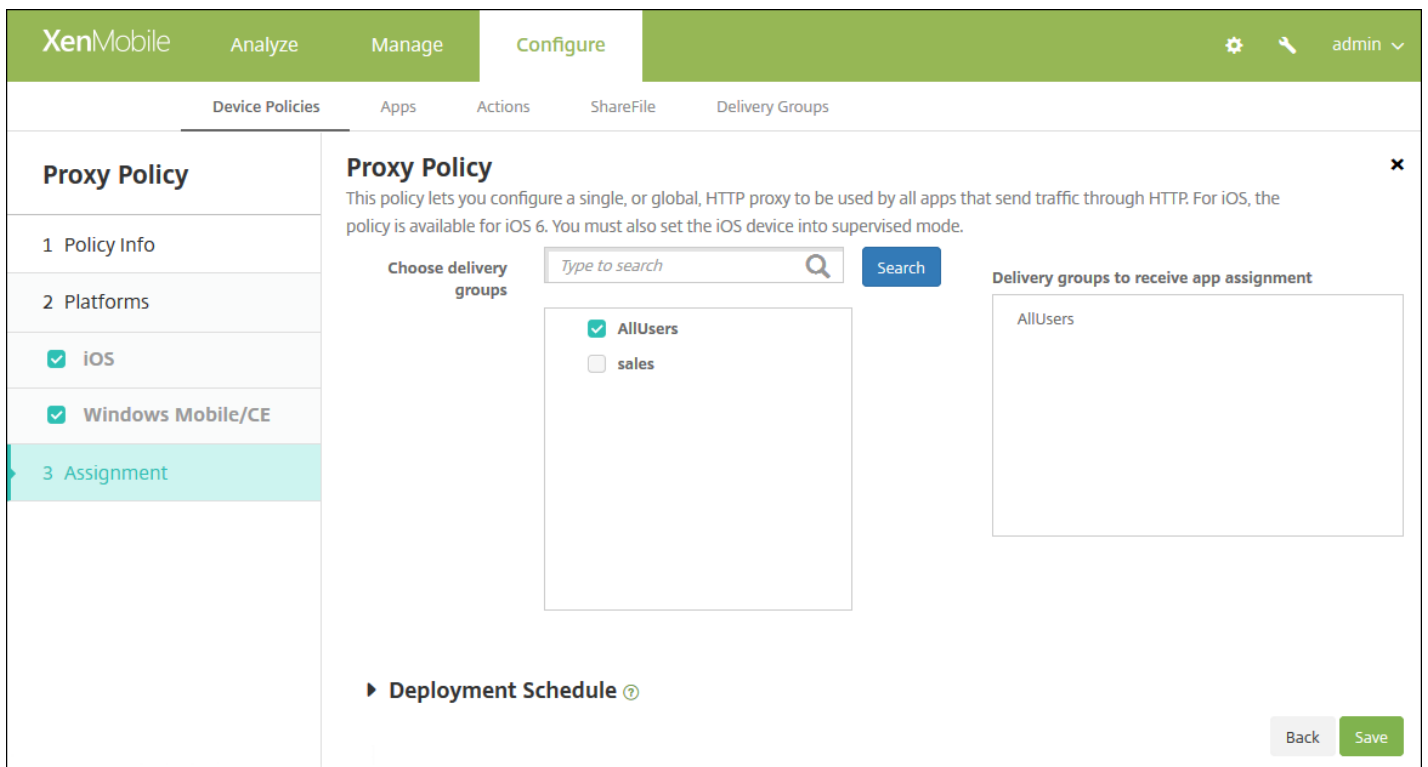


配置以下设置：

- **网络**：在列表中，单击要使用的网络类型。默认值为**内置办公网络**。可能的选项包括：
 - 用户定义的办公网络
 - 用户定义的 Internet
 - 内置办公网络
 - 内置 Internet
- **网络**：在列表中，单击要使用的网络连接协议。默认值为**HTTP**。可能的选项包括：
 - HTTP
 - WAP
 - Socks 4
 - Socks 5
- **代理服务器的主机名或 IP 地址**：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
- **代理服务器的端口**：键入代理服务器的端口号。此字段为必填字段。默认值为**80**。
- **用户名**：键入向代理服务器进行身份验证的可选用户名。
- **密码**：键入向代理服务器进行身份验证的可选密码。
- **域名**：键入可选域名。
- **启用**：选择是否启用代理。默认值为开。

7. 配置部署规则

8. 单击下一步。此时将显示代理策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

注册表设备策略

Feb 27, 2017

Windows Mobile/CE 注册表存储关于应用程序、驱动器、用户首选项和配置设置的数据。在 XenMobile 中，可以定义用于管理 Windows Mobile/CE 设备的注册表项和值。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在自定义下方，单击注册表。此时将显示注册表策略信息页面。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

Registry Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows you to specify which registry keys and values need to be defined on the device. An empty value means that the entry is a registry key.

Policy Name*

Description

Next >

4. 在策略信息窗格中，键入以下信息：

- 策略名称：键入策略的描述性名称。
- 说明：键入策略的可选说明。

5. 单击下一步。此时将显示 Windows Mobile/CE 平台页面。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

Registry Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows you to specify which registry keys and values need to be defined on the device. An empty value means that the entry is a registry key.

Registry key path*	Registry value name	Type	Value	Add
--------------------	---------------------	------	-------	-----

Deployment Rules

Back Next >

6. 配置以下设置：

- 对于要添加的每个注册表项或注册表项/值对，请单击**添加**并执行以下操作：
- **注册表项路径**：键入注册表项的完整路径。例如，键入 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows` 以指定从 HKEY_LOCAL_MACHINE 根注册表项到 Windows 注册表项的路由。
- **注册表值的名称**：键入注册表项值的名称。例如，键入 `ProgramFilesDir` 将该值名称添加到注册表项路径 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion`。如果将此字段留空，表示将添加注册表项而非注册表项/值对。
- **类型**：在列表中，单击值的数据类型。默认值为 **DWORD**。可能的选项包括：
 - **DWORD**：32 位无符号整数。
 - **字符串**：任意字符串。
 - **扩展字符串**：可以包含环境变量（例如 `%TEMP%` 或 `%USERPROFILE%`）的字符串值。
 - **二进制**：任意二进制数据。
- **值**：键入与注册表值名称关联的值。例如，要指定 `ProgramFilesDir` 的值，请键入 `C:\Program Files`。
- 单击**保存**以保存注册表项信息，或单击**取消**不保存注册表项信息。

注意：要删除现有注册表项，请将鼠标悬停在包含此列表的行上，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**以保留列表。

要编辑现有注册表项，请将鼠标悬停在包含此列表的行上，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

7. 配置部署规则

8. 单击**下一步**。此时将显示注册表策略分配页面。

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

10. 展开**部署计划**，然后配置以下设置：

- 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。

远程支持设备策略

Feb 27, 2017

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

- **基本**：使用此选项，您可以查看与设备有关的诊断信息（例如系统信息）、正在运行的进程、任务管理器（内存和 CPU 使用率）以及已安装的软件文件夹内容等。
- **高级**：使用此选项，您可以远程控制设备的屏幕，包括控制颜色（在主窗口中或者在独立的浮动窗口中）、在技术支持人员与用户之间建立 VoIP 会话、配置设置以及在技术支持人员与用户之间建立聊天会话的功能。

注意：要实施此策略，必须执行以下操作：

- 在您的环境中安装 XenMobile Remote Support 应用程序。
- 配置远程支持应用程序通道。有关详细信息，请参阅[应用程序通道设备策略](#)。
- 按本主题中所述配置 Samsung KNOX 远程支持设备策略。
- 同时对用户设备部署应用程序通道远程支持策略和 Samsung KNOX 远程支持策略。

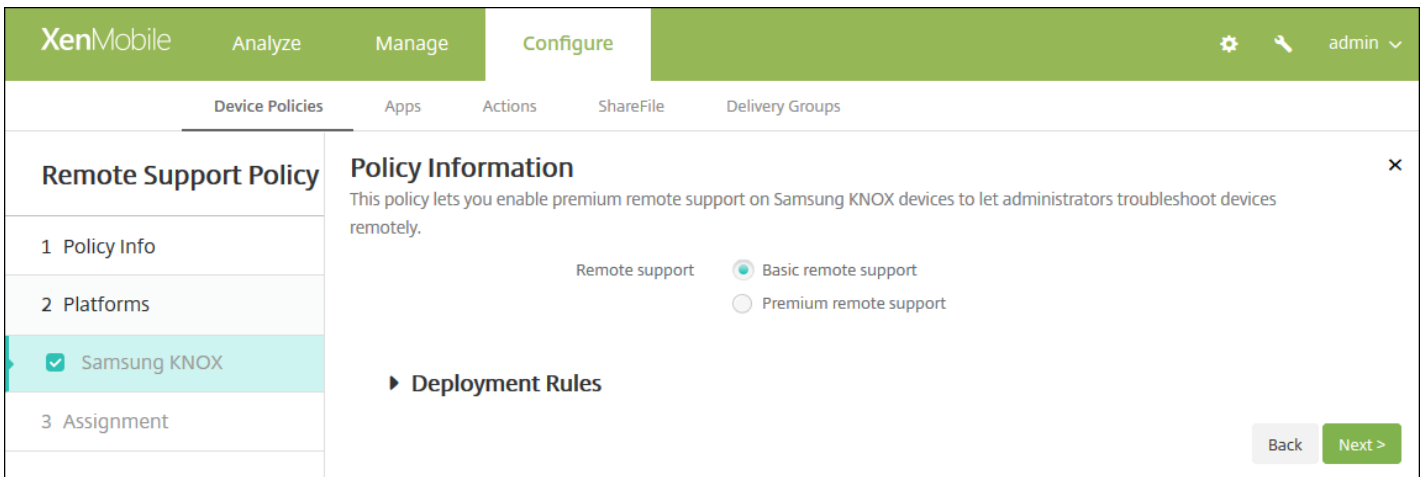
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**网络访问权限**下方，单击**远程支持**。此时将显示**远程支持策略**页面。

The screenshot shows the XenMobile configuration interface for a Remote Support Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Remote Support Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a description: 'This policy lets you enable premium remote support on Samsung KNOX devices to let administrators troubleshoot devices remotely.' Below the description are input fields for 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. 在策略信息窗格中，输入以下信息：

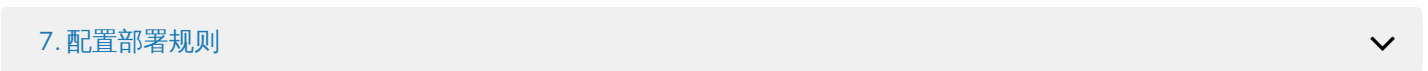
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击**下一步**。此时将显示 **Samsung KNOX 平台信息** 页面。

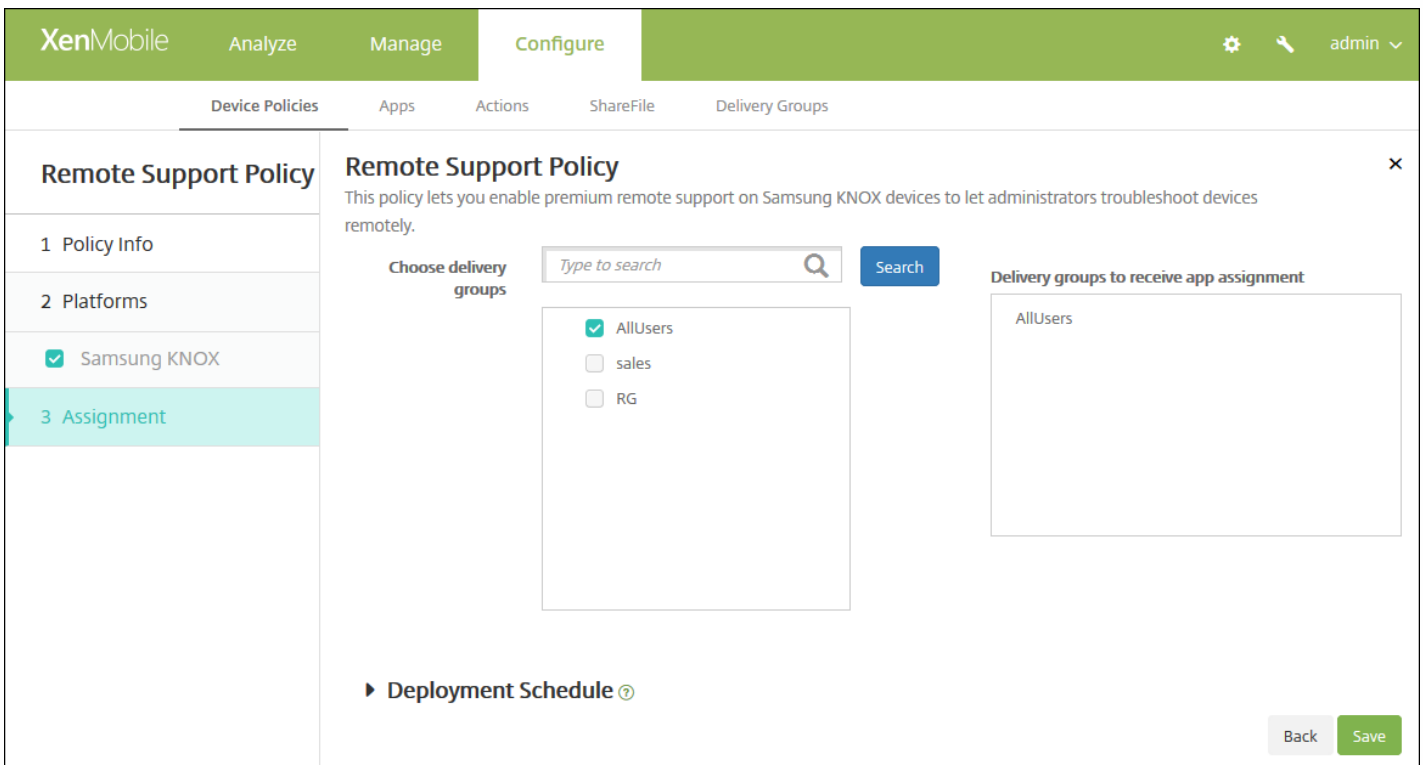


6. 配置以下设置：

- 远程支持：选择基本远程支持或高级远程支持。默认值为基本远程支持。



8. 单击下一步。此时将显示远程支持策略分配页面。



9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。选择的组显示在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。

限制设备策略

Feb 27, 2017

“限制”设备策略允许或限制用户设备上的某些特性或功能，例如相机。您还可以设置安全限制、对媒体内容的限制以及对用户能够和不安装的应用程序类型的限制。大多数限制设置默认为开、或允许。主要的例外情况是 iOS 安全 - 强制功能和所有 Windows Tablet 功能，其默认值为关或限制。

提示：如果您为任何选项选择开，则意味着用户可以执行该操作或使用该功能。例如：

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

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**页面。
3. 单击**限制**。此时将显示限制 **Policy information**（策略信息）页面。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Restrictions Policy' and contains a 'Policy Information' section. This section includes a description and two input fields for 'Policy Name*' and 'Description'. A sidebar on the left lists various platforms with checkboxes, all of which are currently checked. A 'Next >' button is located at the bottom right of the page.

4. 在**策略信息**窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

4. 单击**下一步**。此时将显示**策略平台**页面。

5. 在平台下方，选择要添加的一个或多个平台。然后，您可以更改每个选中平台的策略信息。在下面的步骤中，单击以将设置更改为关，从而限制相应功能。除非另有说明，否则默认设置为启用该功能。

如果选择：

[iOS，请配置以下设置](#)

[Mac OS X，请配置以下设置](#)

[Samsung SAFE，请配置以下设置](#)

[Samsung KNOX，请配置以下设置](#)

[Windows Phone，请配置以下设置](#)

[Windows Tablet，请配置以下设置](#)

[Amazon，请配置以下设置](#)

[Windows Mobile/CE，请配置以下设置](#)

设置完平台限制后，请参阅本文后面的步骤 7 以了解如何设置此平台的部署规则。

如果选择 iOS，可以配置以下设置

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Restrictions Policy' section is active, showing a list of platforms on the left and configuration options on the right. The 'iOS' platform is selected and highlighted in light blue. The configuration options for iOS include: Camera (ON), FaceTime (checked), Screen shots (ON), Photo streams (ON, iOS 5.0+), Shared photo streams (ON, iOS 6.0+), Voice dialing (ON), Siri (ON), Allow while device is locked (checked), Siri profanity filter (unchecked), and Installing apps (ON). There are 'Back' and 'Next >' buttons at the bottom right of the configuration area.

[iOS 设置](#)

[配置 Mac OS X 设置](#)

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Restrictions Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Samsung SAFE
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet
 - Amazon
 - Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Preferences

- Restrict items in System Preferences OFF

Apps

- Allow use of Game Center ON OS X 10.11+
- Allow adding Game Center friends ON
- Allow multiplayer gaming ON
- Allow Game Center account modification ON
- Allow App Store adoption ON
- Allow Safari AutoFill ON
- Require admin password to install or update apps OFF

Back Next >

Mac OS X 设置 ▾

配置 Samsung SAFE 设置

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

- Enable ODE Trusted Boot Verification
- Allow Development Mode
- Allow Emergency Calls Only
- Allow Firmware Recovery
- Allow Fast Encryption
- Common Criteria Mode
- Factory reset
- Date Time Change
- DOD boot banner
- Settings changes
- Backup
- Over The Air Upgrade ⓘ
- Background data
- Camera

Back Next >

Samsung SAFE 设置

配置 Samsung KNOX 设置

Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

- Allow use of camera
- Enable Revocation Check
- Move Apps To Container
- Enforce Multifactor Authentication
- Enable TIMA Key store
- Enforce Auth For Container
- Share List
- Enable Audit Log
- Use Secure Keypad
- Enable Google Apps
- Authentication Smart Card Browser

► Deployment Rules

[Back](#) [Next >](#)

Samsung KNOX 设置

配置 Windows Phone 设置

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

Restrictions Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Samsung SAFE
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet
 - Amazon
 - Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

WiFi Settings

- Allow WiFi
- Allow Internet sharing
- Allow auto-connect to WiFi Sense hotspots
- Allow hotspot reporting
- Allow manual configuration

Connectivity

- Allow NFC
- Allow bluetooth
- Allow VPN over cellular
- Allow VPN over cellular while roaming

Back Next >

Windows Phone 设置

配置 Windows Desktop/Tablet 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Restrictions Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Samsung SAFE
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet**
 - Amazon
 - Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Network

Roaming data OFF

Security

User account control ▾

Enable Windows error reporting OFF

Enable smart screen OFF

Other

Enterprise client sync product's URL enable OFF

Enterprise client sync product's URL

▶ **Deployment Rules**

Windows Desktop/Tablet 设置 ▾

配置 Amazon 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Restrictions Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Samsung SAFE
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet
 - Amazon
 - Windows Mobile/CE
- 3 Assignment

Policy Information ✕

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

- Factory reset
- Profiles

Allow apps

- Non-Amazon Appstore apps
- Social networks

Network

- Bluetooth
- WiFi switch
- WiFi settings
- Cellular data

Back Next >

Amazon 设置 ▾

配置 Windows Mobile/CE 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Restrictions Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Samsung SAFE
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet
 - Amazon
 - Windows Mobile/CE
- 3 Assignment

Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

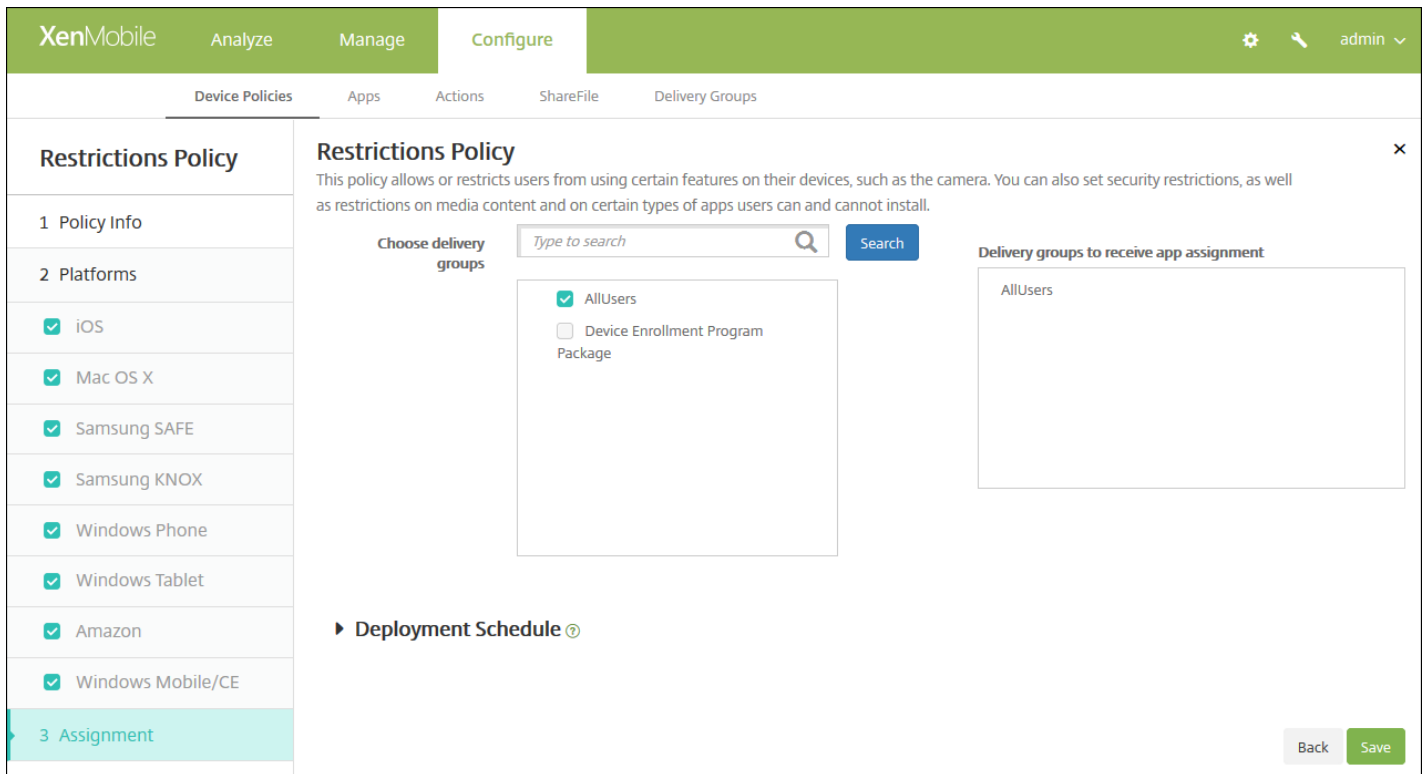
- Bluetooth/infrared beaming (Obex)
- Camera
- WiFi switch
- Bluetooth

Deployment Rules

Back Next >

- Windows Mobile/CE 设置 ▾
- 7. 配置部署规则 ▾

8. 单击下一步，将显示限制策略分配页面。



9. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

10. 单击保存以保存此策略。

漫游设备策略

Feb 27, 2017

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

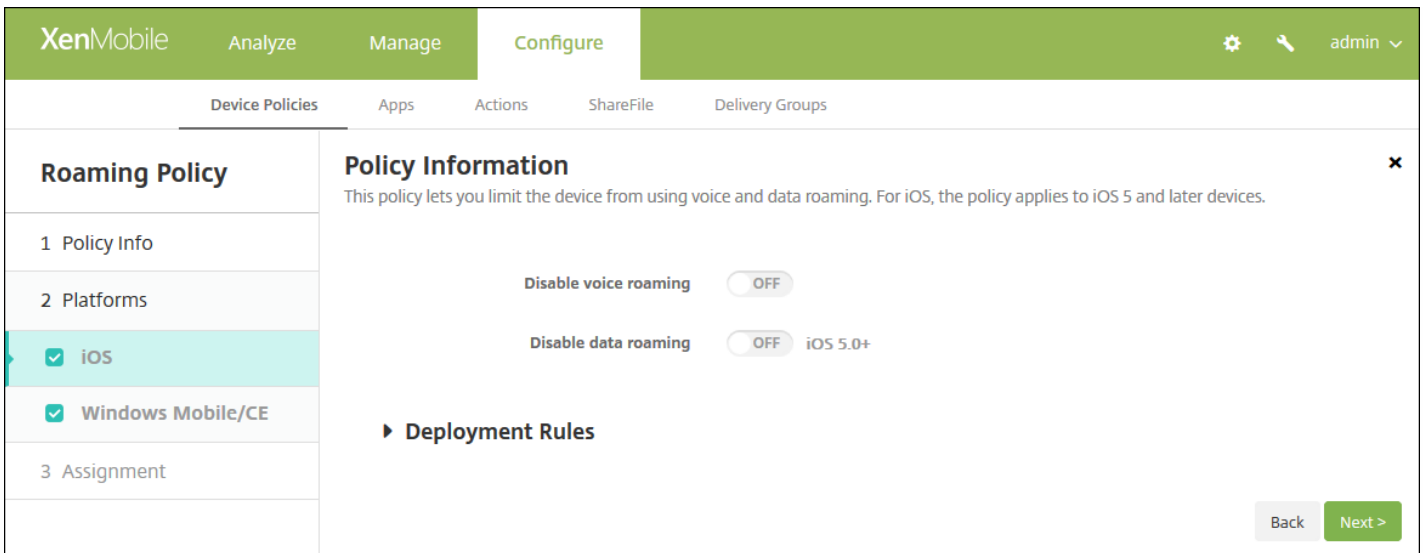
1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 单击更多，然后在网络访问下面，单击漫游。此时将显示漫游策略信息页面。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Roaming Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing checkboxes for 'iOS' and 'Windows Mobile/CE', both of which are checked. The 'Policy Information' section is open, displaying a text input field for 'Policy Name*' and a larger text area for 'Description'. A note above these fields states: 'This policy lets you limit the device from using voice and data roaming. For iOS, the policy applies to iOS 5 and later devices.' A 'Next >' button is located in the bottom right corner of the configuration area.

4. 在策略信息窗格中，输入以下信息：
 - 策略名称：键入策略的描述性名称。
 - 说明：（可选）键入策略的说明。
5. 单击下一步。此时将显示平台页面。
6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

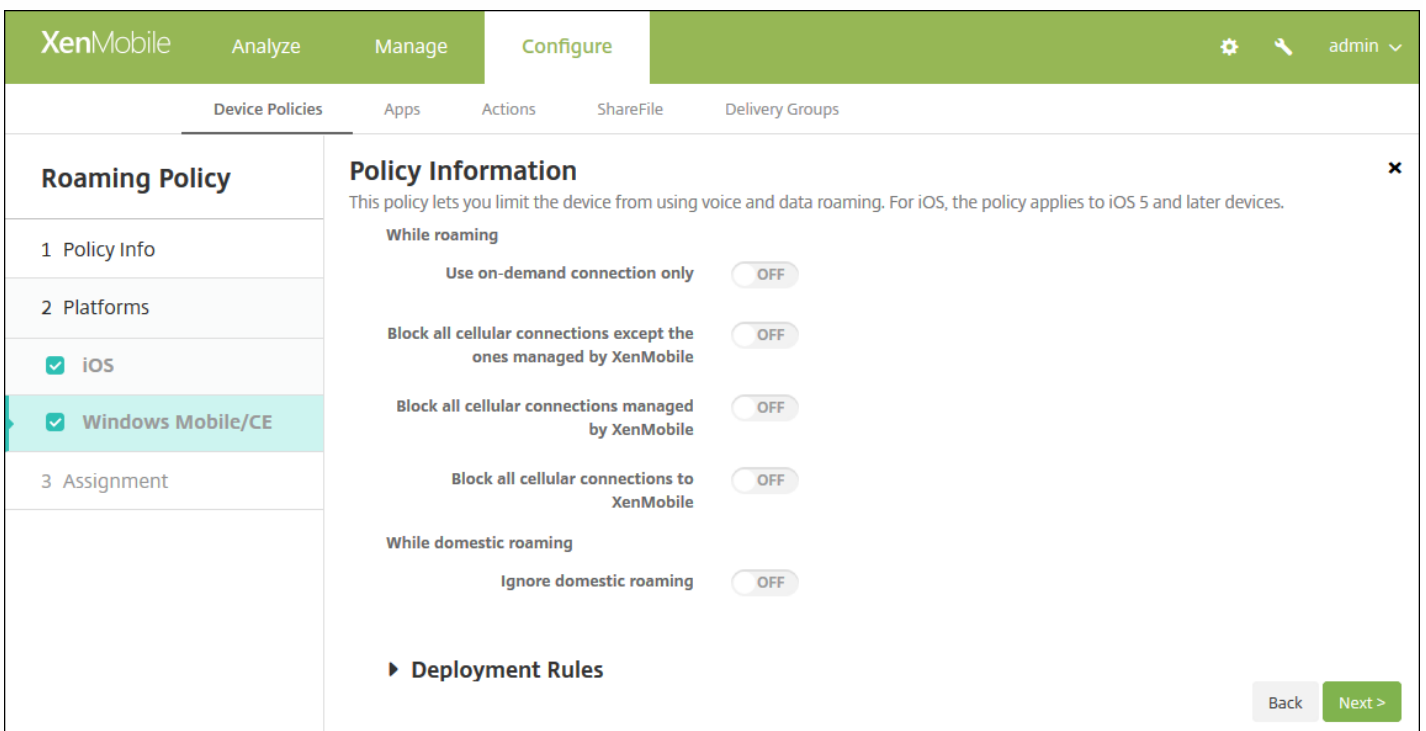
配置 iOS 设置



配置以下设置：

- **禁用语音漫游**：选择是否禁用语音漫游。启用此选项时，会自动禁用数据漫游。默认值为关，表示允许语音漫游。
- **禁用数据漫游**：选择是否禁用数据漫游。此选项仅在启用语音漫游时可用。默认值为关，表示允许数据漫游。

配置 Windows Mobile/CE 设置



配置以下设置：

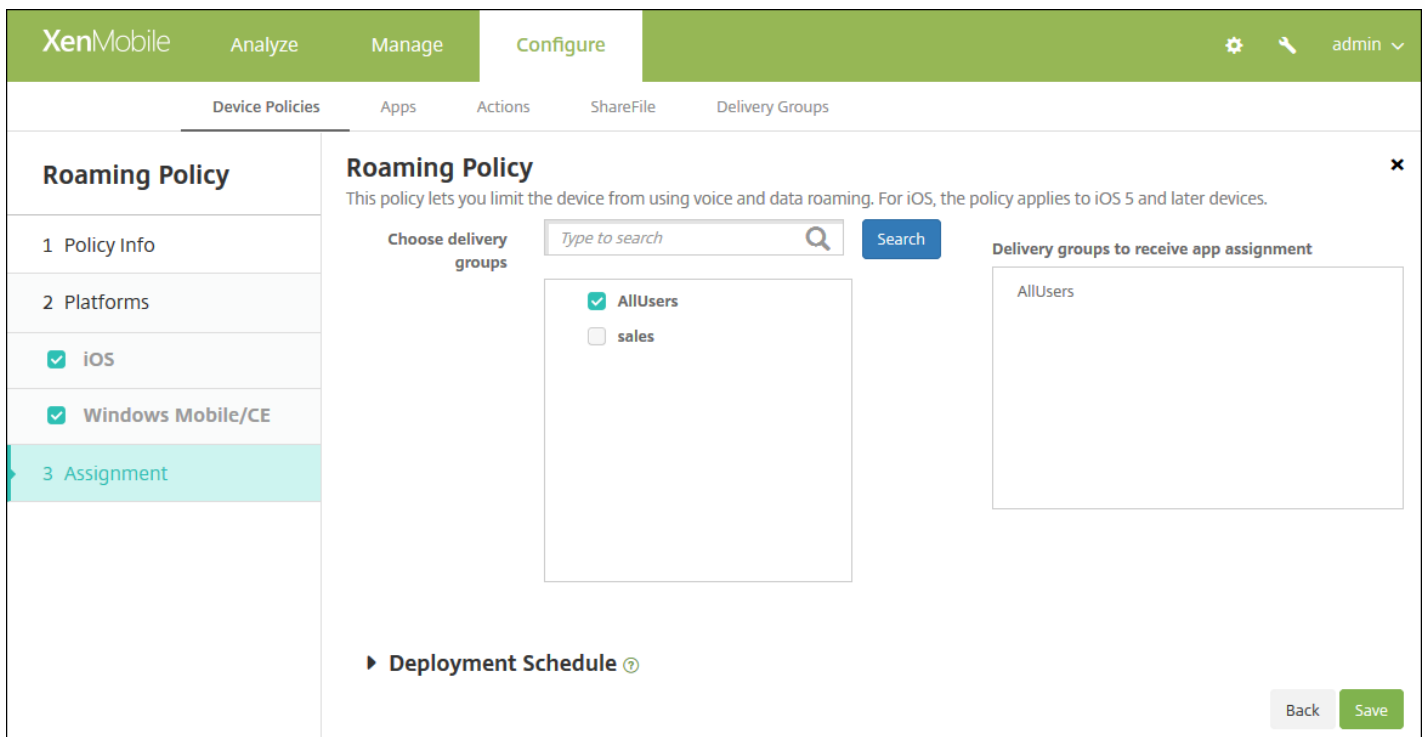
- **在漫游时**
 - **只使用按需连接**：如果用户在其设备上手动触发连接，或者如果移动应用程序请求强制进行连接（例如在已相应设置 Exchange Server 时的推送邮件请求），设备才会连接到 XenMobile。请注意，此选项会临时禁用默认设备连接计划策

略。

- **阻止所有手机网络连接，但 XenMobile 管理的连接除外**：除了在 XenMobile 应用程序通道或其他 XenMobile 设备管理任务中正式声明的数据流量外，该设备不会发送或接收任何其他数据。例如，此选项将禁用所有通过设备的 Web 浏览器到 Internet 的连接。
- **阻止 XenMobile 管理的所有手机网络连接**：所有通过 XenMobile 通道传输的应用程序数据都将被阻止（包括 XenMobile Remote Support）。但是，不会阻止与纯“设备管理”相关的数据流量。
- **阻止与 XenMobile 的所有手机网络连接**：在这种情况下，除非设备通过 USB、WiFi 或其默认移动运营商手机网络重新进行连接，否则在设备和 XenMobile 之间不会传输任何流量。
- **国内漫游时**
 - **忽略国内漫游**：用户在国内漫游时不阻止任何数据。

7. 配置部署规则

8. 单击下一步。此时将显示漫游策略分配页面。



9. 在选择交付组旁边，键入以查找交付组，或在列表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**。

Samsung MDM 许可证密钥设备策略

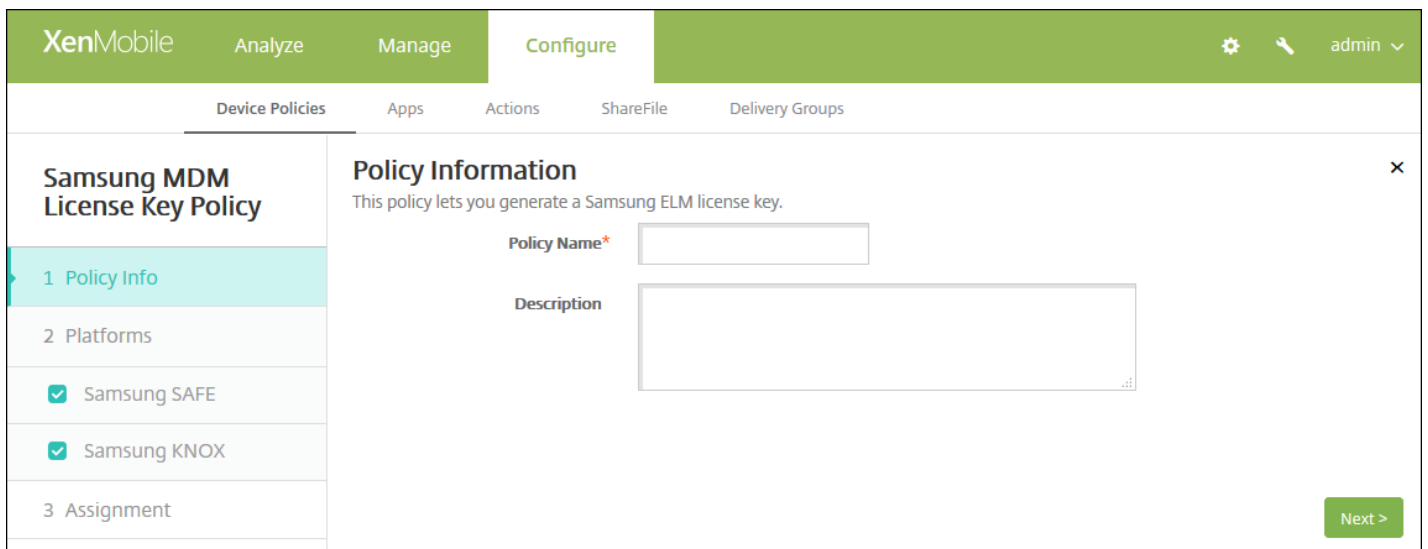
Feb 27, 2017

XenMobile 支持并扩展了 Samsung for Enterprise (SAFE) 和 Samsung KNOX 策略。SAFE 是一个解决方案系列，它通过与移动设备管理解决方案集成为业务使用提供安全性和增强功能。Samsung KNOX 属于提供更安全的 Android 平台以供企业使用的 SAFE 计划中的一种解决方案。

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

要启用 SAFE 和 Samsung KNOX API，必须部署 Secure Hub 以及 Samsung ELM 密钥。可以通过检查设备属性来验证是否已启用 SAFE API。部署 Samsung ELM 密钥时，将 **Samsung MDM API 可用性** 设置为 **True**。

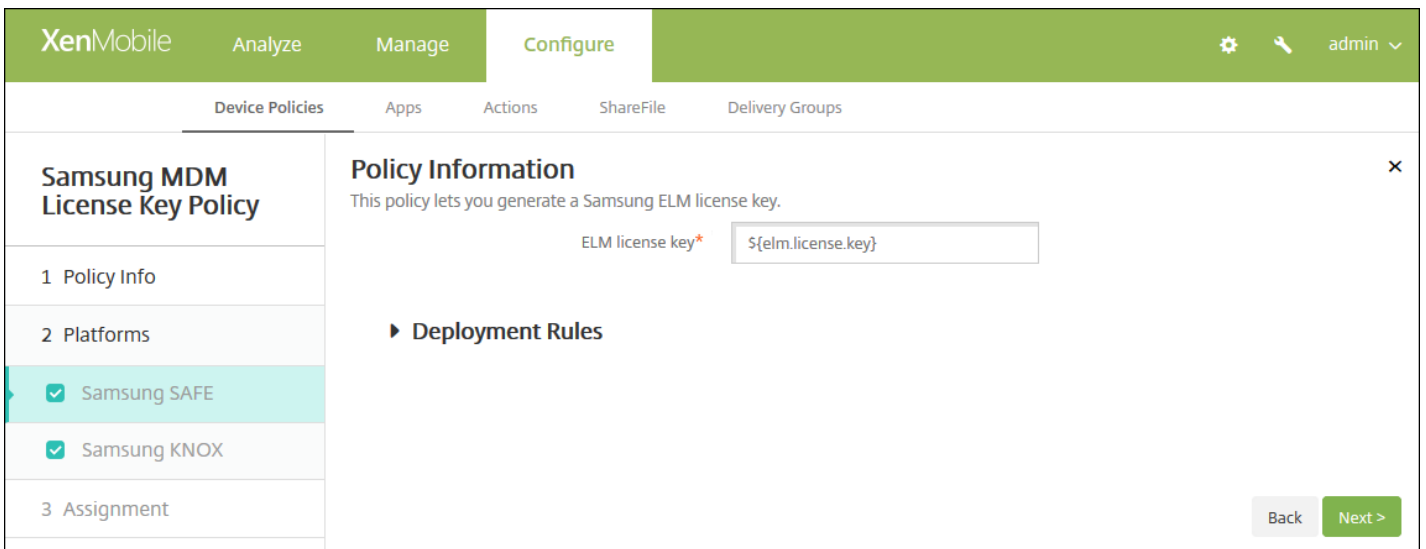
1. 在 XenMobile 控制台中，单击 **配置 > 设备策略**。此时将显示 **设备策略** 页面。
2. 单击 **添加**。此时将显示 **添加新策略** 对话框。
3. 单击 **更多**，然后在 **安全性** 下方，单击 **Samsung MDM 许可证密钥**。此时将显示 **Samsung MDM 许可证密钥策略** 信息页面。



4. 在策略信息窗格中，输入以下信息：
 - **策略名称**：键入策略的描述性名称。
 - **说明**：键入策略的可选说明。
5. 单击下一步。此时将显示平台页面。
6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

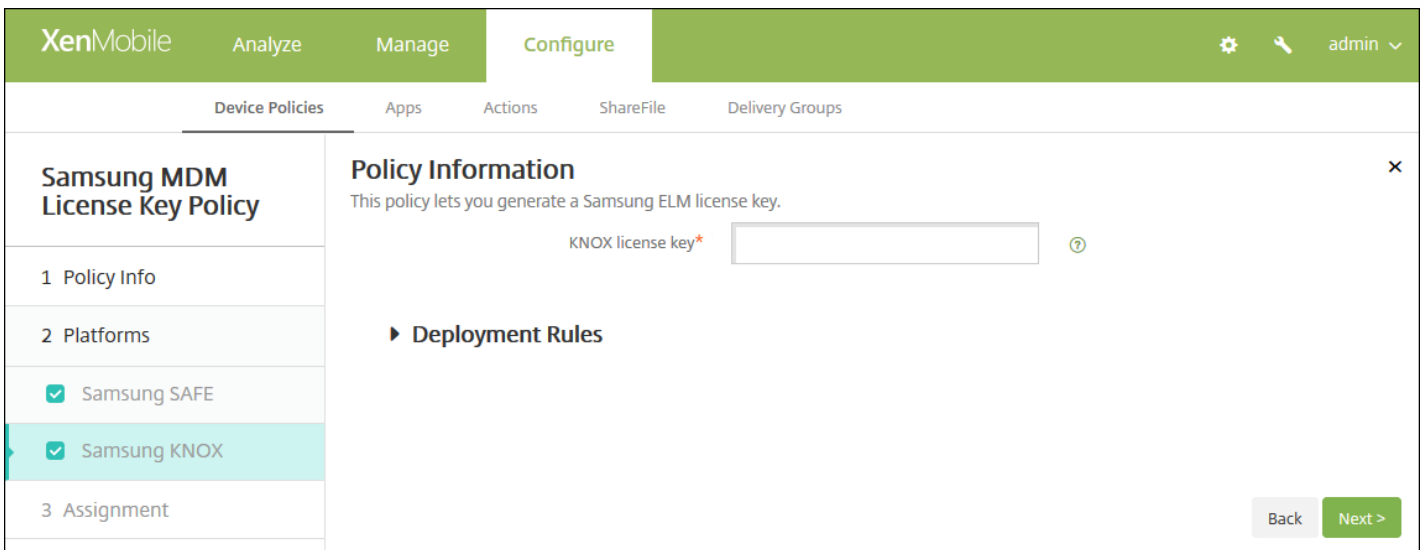
配置 Samsung SAFE 设置



配置以下设置：

- **ELM 许可证密钥**：此字段应该已包含生成 ELM 许可证密钥的宏。如果此字段为空，请键入宏 `${elm.license.key}`。

配置 Samsung KNOX 设置

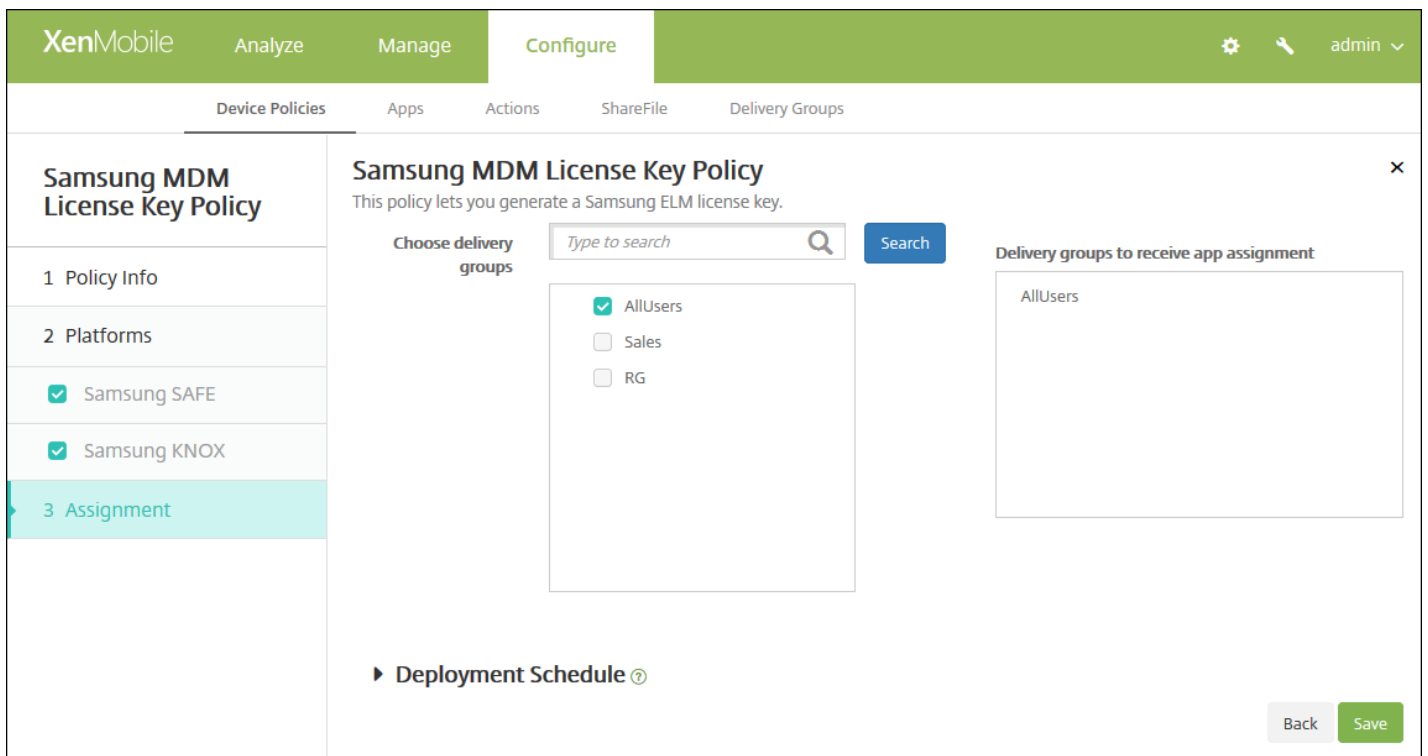


配置以下设置：

- **KNOX 许可证密钥**：键入从 Samsung 获取的 KNOX 许可证密钥。

7. 配置部署规则

8. 单击下一步。此时将显示 **Samsung MDM 许可证密钥策略分配** 页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

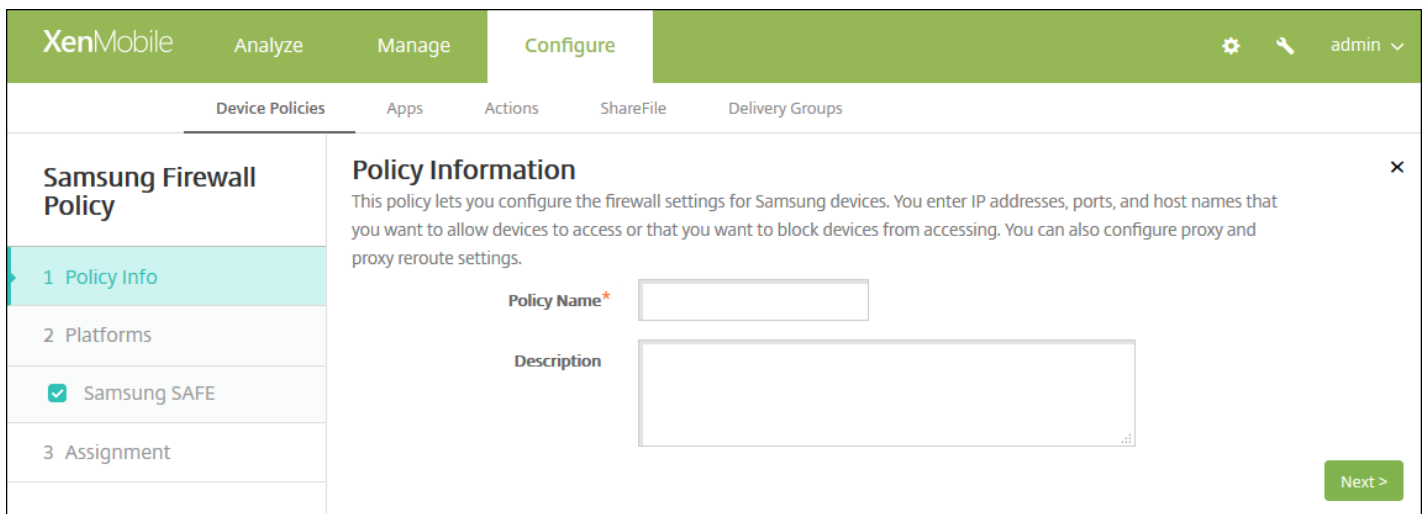
11. 单击保存。

Samsung SAFE 防火墙设备策略

Feb 27, 2017

此策略允许您为 Samsung 设备配置防火墙设置。输入允许设备访问或阻止设备访问的 IP 地址、端口和主机名。还可以配置代理和代理重新路由设置。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在网络访问下方，单击 Samsung 防火墙。此时将显示 Samsung 防火墙策略页面。

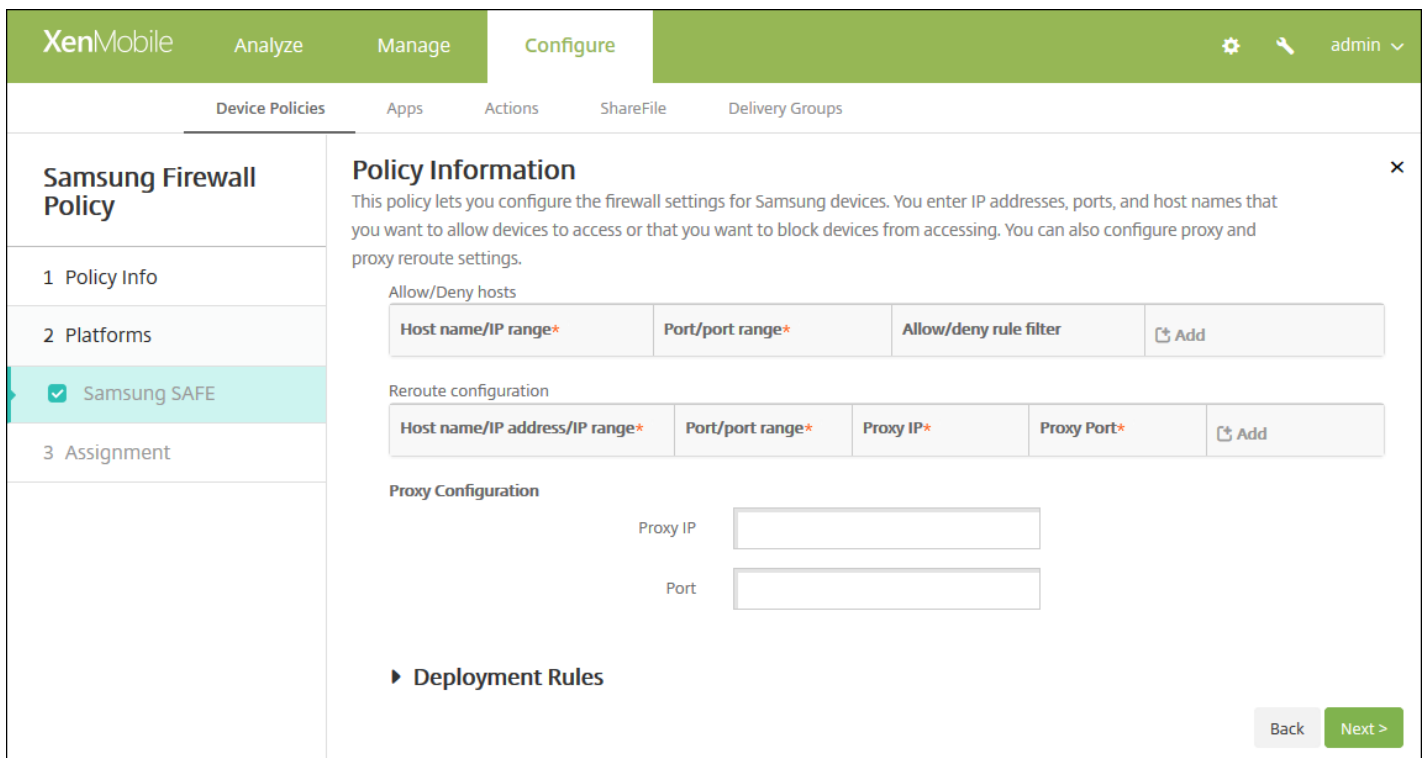


The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Samsung Firewall Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is currently active and shows 'Policy Information' with a description: 'This policy lets you configure the firewall settings for Samsung devices. You enter IP addresses, ports, and host names that you want to allow devices to access or that you want to block devices from accessing. You can also configure proxy and proxy reroute settings.' Below the description are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. 在策略信息窗格中，输入以下信息：

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

5. 单击下一步。此时将显示 Samsung SAFE 平台信息页面。



6. 配置以下设置：

• 允许/拒绝主机

- 对于希望允许访问或拒绝访问的每个主机，请单击**添加**并执行以下操作：
 - **主机名/IP 范围**：键入希望影响的站点的主机名和 IP 地址范围。
 - **端口/端口范围**：键入端口或端口范围。
 - **允许/拒绝规则过滤**：选择“白名单”以允许访问站点或单击“黑名单”以拒绝访问站点。
 - 单击**保存**或**取消**。

• 重新路由配置

- 对于要配置的每个代理，单击**添加**并执行以下操作：
 - **主机名/IP 范围**：键入代理重新路由的主机名或 IP 地址范围。
 - **端口/端口范围**：键入端口或端口范围。
 - **代理 IP**：键入代理 IP 地址。
 - **代理端口**：键入代理端口。
 - 单击**保存**或**取消**。

注意：要删除现有项目，请将鼠标悬停在包含此列表的行上，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**以保留列表。

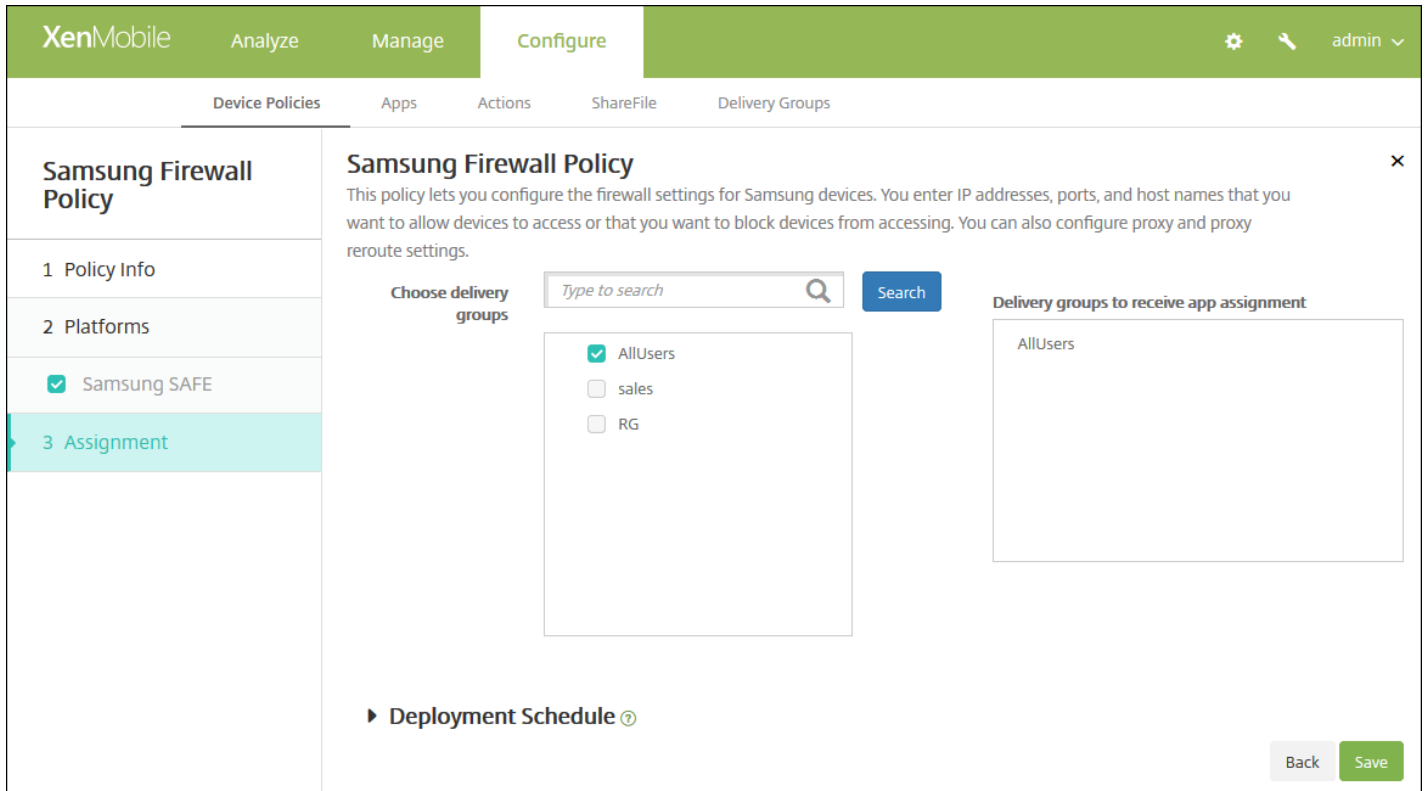
要编辑现有项目，请将鼠标悬停在包含此列表的行上，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

• 代理配置

- **代理 IP**：键入代理服务器的 IP 地址。
- **端口**：键入代理服务器端口。

7. 配置部署规则

8. 单击下一步。此时将显示 **Samsung 防火墙策略分配** 页面。



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

10. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS。

11. 单击**保存**。

SCEP 设备策略

Feb 27, 2017

利用此策略，可以将 iOS 和 Mac OS X 设备配置为使用简单证书注册协议 (SCEP) 从外部 SCEP 服务器检索证书。如果希望从连接到 XenMobile 的 PKI 向使用 SCEP 的设备交付证书，应采用分布式模式创建 PKI 实体和 PKI 提供程序。有关详细信息，请参阅 [PKI 实体](#)。

iOS 设置

Mac OS X 设置

1. 在 XenMobile 控制台中，单击 **配置 > 设备策略**。此时将显示设备策略页面。
2. 单击 **添加**。此时将显示添加新策略对话框。
3. 展开 **更多**，然后在 **安全性** 下面，单击 **SCEP**。此时将显示 **SCEP 策略** 信息页面。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'SCEP Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing checkboxes for 'iOS' and 'Mac OS X', both of which are checked. The '3 Assignment' section is currently empty. The 'Policy Information' section is visible, containing a description: 'This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.' Below the description are two input fields: 'Policy Name *' and 'Description'.

4. 在策略信息窗格中，键入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击 **下一步**。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

XenMobile
Analyze
Manage
Configure
⚙️ 🔍 admin ▾

Device Policies
Apps
Actions
ShareFile
Delivery Groups

SCEP Policy

1 Policy Info

2 Platforms

iOS

Mac OS X

Windows Phone

Windows Tablet

3 Assignment

Policy Information ✕

This policy lets you create a Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority. For Windows Phone/Tablet, the payloads are supported only on Windows 10 and later supervised devices.

URL base*

Instance name*

Subject X.500 name (RFC 2253)

Subject alternative names type None ▾

Maximum retries

Retry delay

Challenge password

Key size (bits) 1024 ▾

Use as digital signature OFF

Use for key encipherment OFF

SHA1/MD5 fingerprint (hexadecimal string)

Policy Settings

Remove policy
 Select date
 Duration until removal (in days)

📅

Allow user to remove policy Always ▾

▶ **Deployment Rules**

Back
Next >

配置以下设置：

- **URL 基**：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。但是，如果允许重复使用一次性密码，则应该使用 HTTPS 来保护密码。此步骤不是必需步骤。
- **实例名称**：键入任何 SCEP 服务器可以识别的字符串。例如，可以是类似 example.org 的域名。如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。此步骤不是必需步骤。
- **使用者 X.500 名称(RFC 2253)**：键入表示为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。例如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 将转换为：[[["C", "US"], [{"O", "Apple Inc."}], ..., [{"1.2.5.3", "bar"}]]。OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。

- **使用者备用名称类型**：在列表中，单击备用名称类型。SCEP 策略可指定可选的备用名称类型，用于提供 CA 颁发证书所需的值。可以指定无、**RFC 822 名称**、**DNS 名称**或 **URI**。
- **最大重试次数**：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。默认值为 **3**。
- **重试延迟**：键入执行下次重试之前需要等待的秒数。第一次重试尝试没有延迟。默认值为 **10**。
- **质询密码**：输入预共享密钥。
- **密钥大小(位)**：在列表中，单击以位为单位的密钥大小 **1024** 或 **2048**。默认值为 **1024**。
- **用作数字签名**：指定是否要将证书用作数字签名。如果有人使用证书来验证数字签名，如验证证书是否由 CA 颁发，SCEP 服务器将在使用公钥解密哈希之前确认该证书是否可以用于此目的。
- **用于密钥加密**：指定是否要将证书用于密钥加密。如果服务器正在使用客户端提供的证书中包含的公钥来验证数据段是否使用私钥进行加密，服务器将首先检查证书是否可用于密钥加密。否则，操作将失败。
- **SHA1/MD5 指纹(十六进制字符串)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹，供设备在注册期间用于确认 CA 响应的可靠性。可以输入 SHA1 或 MD5 指纹，或选择证书来导入其签名。
- **策略设置**
 - 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
 - 如果单击选择日期，请单击日历以选择具体删除日期。
 - 在允许用户删除策略列表中，单击始终、需要密码或从不。
 - 如果单击需要密码，在删除密码旁边，键入必需的密码。

配置 Mac OS X 设置

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

SCEP Policy

- Policy Info
- Platforms
 - iOS
 - Mac OS X
 - Windows Phone
 - Windows Tablet
- Assignment

Policy Information

This policy lets you create a Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority. For Windows Phone/Tablet, the payloads are supported only on Windows 10 and later supervised devices.

URL base*

Instance name*

Subject X.500 name (RFC 2253)

Subject alternative names type

Maximum retries

Retry delay

Challenge password

Key size (bits)

Use as digital signature

Use for key encipherment

SHA1/MD5 fingerprint (hexadecimal string)

Certificate expiration notification threshold

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy

Profile scope OS X 10.7+

► Deployment Rules

配置以下设置：

- **URL 基**：键入 SCEP 服务器的地址以定义通过 HTTP 或 HTTPS 发送 SCEP 请求的位置。由于私钥不与证书签名请求 (CSR) 一起发送，因此发送未加密的请求可能不会有什么风险。但是，如果允许重复使用一次性密码，则应该使用 HTTPS 来保护密码。此步骤不是必需步骤。
- **实例名称**：键入任何 SCEP 服务器可以识别的字符串。例如，可以是类似 example.org 的域名。如果 CA 具有多个 CA 证书，则可以使用此字段识别所需的域。此步骤不是必需步骤。
- **使用者 X.500 名称(RFC 2253)**：键入表示为一系列对象标识符 (OID) 和值的 X.500 名称的表示形式。例

如，/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar 将转换为：[[["C", "US"], [{"O", "Apple Inc."}], ..., [{"1.2.5.3", "bar"}]]。OID 可表示为句点分隔的数字，并采用以下快捷方式：国家/地区 (C)、地点 (L)、州 (ST)、组织 (O)、组织单位 (OU) 以及公用名 (CN)。

- **使用者备用名称类型**：在列表中，单击备用名称类型。SCEP 策略可指定可选的备用名称类型，用于提供 CA 颁发证书所需的值。可以指定无、**RFC 822 名称**、**DNS 名称**或 **URI**。
- **最大重试次数**：键入 SCEP 服务器发送 PENDING 响应时设备应重试的次数。默认值为 **3**。
- **重试延迟**：键入执行下次重试之前需要等待的秒数。第一次重试尝试没有延迟。默认值为 **10**。
- **质询密码**：键入预共享密钥。
- **密钥大小(位)**：在列表中，单击以位为单位的密钥大小 **1024** 或 **2048**。默认值为 **1024**。
- **用作数字签名**：指定是否要将证书用作数字签名。如果有人使用证书来验证数字签名，如验证证书是否由 CA 颁发，SCEP 服务器将在使用公钥解密哈希之前确认该证书是否可以用于此目的。
- **用于密钥加密**：指定是否要将证书用于密钥加密。如果服务器正在使用客户端提供的证书中包含的公钥来验证数据段是否使用私钥进行加密，服务器将首先检查证书是否可用于密钥加密。否则，操作将失败。
- **SHA1/MD5 指纹(十六进制字符串)**：如果 CA 使用 HTTP，则使用此字段提供 CA 证书的指纹，供设备在注册期间用于确认 CA 响应的可靠性。可以输入 SHA1 或 MD5 指纹，或选择证书来导入其签名。
- **策略设置**
 - 在策略设置下，删除策略旁边，单击选择日期或删除前保留时间(天)。
 - 如果单击选择日期，请单击日历以选择具体删除日期。
 - 在允许用户删除策略列表中，单击始终、需要密码或从不。
 - 如果单击需要密码，在删除密码旁边，键入必需的密码。
 - 在配置文件作用域旁边，单击用户或系统。默认值为用户。此选项仅适用于 OS X 10.7 及更高版本。

7. 配置部署规则

8. 单击下一步。此时将显示 **SCEP 策略分配** 页面。
 9. 在选择交付组旁边，键入以查找交付组，或在列表中选择一个或多个要向其分配策略的交付组。选择的组显示在右侧用于接收应用程序分配的交付组列表中。
 10. 展开部署计划，然后配置以下设置：
 - 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。如果选择关，无需配置其他选项。
 - 在部署计划旁边，单击立即或稍后。默认选项为立即。
 - 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
 - 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
 - 在为始终启用的连接部署旁边，单击开或关。默认选项为关。
- 注意：**
- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
 - 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。
11. 单击保存以保存此策略。

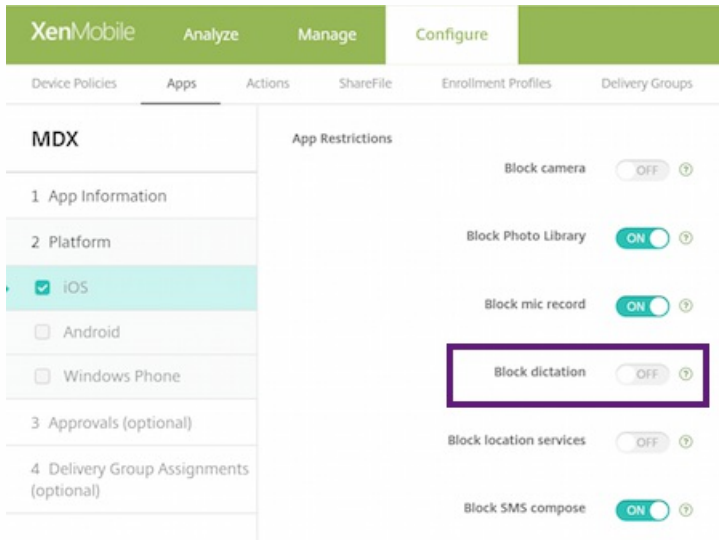
Siri 和听写策略

Feb 27, 2017

用户向 Siri 提问时或在托管 iOS 设备上听写文本时，Apple 将收集语音数据以改进 Siri 的功能。语音数据通过 Apple 的基于云的服务传输，因此存在于安全的 XenMobile 容器外部。但是，由听写产生的文本仍保留在容器内部。

XenMobile 允许您根据安全性要求阻止 Siri 和听写服务。

在 MAM 部署中，每个应用程序的阻止听写策略都默认设置为开，这样将禁用设备的麦克风。如果要允许听写，请将其设置为关。可以在 XenMobile 控制台的配置 > 应用程序下找到该策略。选择应用程序，单击编辑，然后单击 iOS。



在 MDM 部署中，还可以通过配置 > 设备策略 > 限制策略 > iOS 下的 Siri 策略禁用 Siri。默认允许使用 Siri。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

- Camera ON
- FaceTime
- Screen shots ON
- Photo streams ON iOS 5.0+
- Shared photo streams ON iOS 6.0+
- Voice dialing ON
- Siri ON
- Allow while device is locked
- Siri profanity filter

Back Next >

决定是否允许使用 Siri 和听写服务时，需要注意以下几点事项：

- 根据 Apple 公开发布的信息，Apple 最长将保留 Siri 和听写语音数据两年时间。该数据将被分配一个随机编号以代表用户，并且语音文件与此随机编号相关联。有关详细信息，请参阅此 Wired 文章 [Apple reveals how long Siri keeps your data](#)（Apple 揭示 Siri 保留数据的时长）。
- 可以通过在任意 iOS 设备上转至设置 > 通用 > 键盘并轻按启用听写下的链接来查看 Apple 的隐私政策。

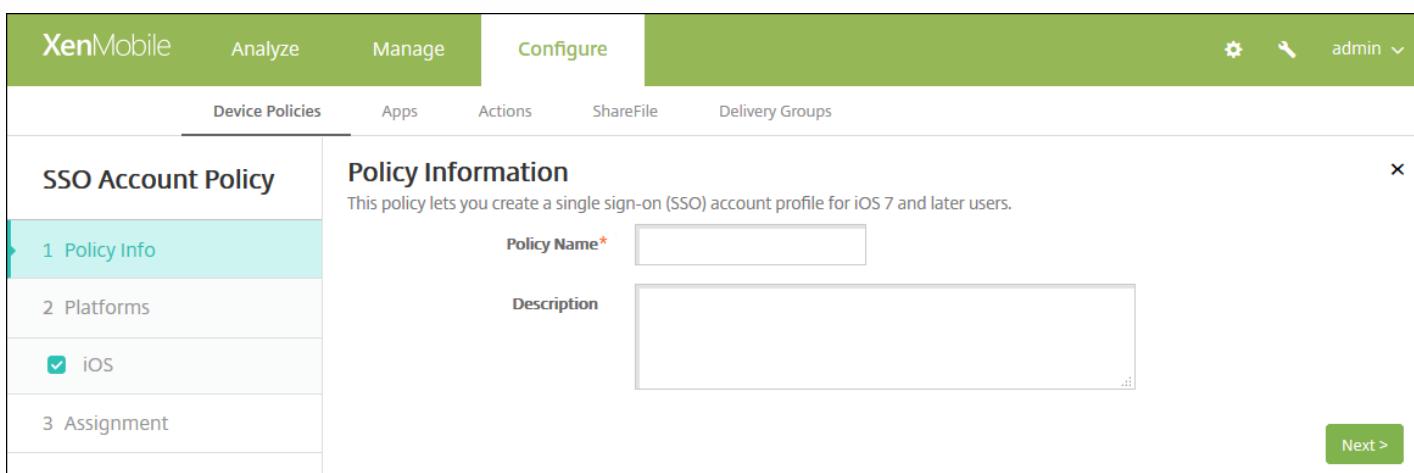
SSO 帐户设备策略

Feb 27, 2017

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

注意：此策略仅适用于 iOS 7.0 及更高版本。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**更多**，然后在**最终用户**下方，单击**SSO 帐户**。此时将显示**SSO 帐户策略**页面。



The screenshot shows the XenMobile configuration interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. The 'Configure' tab is active. Below the navigation bar, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. On the left, there is a sidebar with 'SSO Account Policy' and a list of steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' step is selected. The main content area shows 'Policy Information' with a description: 'This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.' There are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. 在 **SSO 帐户策略信息** 窗格中，输入以下信息：

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

5. 单击**下一步**。此时将显示 **iOS 平台** 信息页面。

SSO Account Policy

1 Policy Info

2 Platforms

iOS

3 Assignment

Policy Information

This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.

Account name*

Kerberos principal name*

Identity credential (Keystore or PKI credential) None

Kerberos realm*

Permitted URLs

Permitted URL Add

App Identifiers

App Identifier Add

Policy Settings

Remove policy Select date Duration until removal (in days)

Allow user to remove policy Always

► Deployment Rules

Back Next >

6. 配置以下设置：

- **帐户名称**：输入显示在用户设备上的 Kerberos SSO 帐户名称。此字段为必填字段。
- **Kerberos 主体名称**：输入 Kerberos 主体名称。此字段为必填字段。
- **身份凭据(密钥库或 PKI 凭据)**：在此列表中，单击可用于在无需用户交互的情况下续订 Kerberos 凭据的可选身份凭据。
- **Kerberos 领域**：输入此策略的 Kerberos 领域。这通常是您的域名，所有字母均大写（例如，EXAMPLE.COM）。此字段为必填字段。
- **允许访问的 URL**：对于需要 SSO 的每个 URL，单击**添加**，然后执行以下操作：
 - **允许访问的 URL**：输入当用户从 iOS 设备访问时需要 SSO 的 URL。例如，当用户尝试浏览某个站点，且该 Web 站点发起 Kerberos 质询时，如果该站点不在此 URL 列表中，iOS 设备将不会通过提供 Kerberos 在以前的 Kerberos 登录中缓存在设备上的 Kerberos 令牌来尝试 SSO。URL 的主机部分必须完全匹配，例如：http://shopping.apple.com 可以，但 http://*.apple.com 却不行。此外，如果 Kerberos 未基于主机匹配激活，URL 将仍然回退到标准 HTTP 调用。如果 URL 仅配置为使用 Kerberos 实现 SSO，这可能意味着一切，包括标准密码质询或 HTTP 错误。
 - 单击**添加**以添加 URL，或单击**取消**以取消添加 URL。
- **应用程序标识符**：对于允许使用此登录的每个应用程序，单击**添加**，然后执行以下操作：
 - **应用程序标识符**：输入允许使用此登录的应用程序的应用程序标识符。如果不添加任何应用程序标识符，此登录将匹配所有应用程序标识符。
 - 单击**添加**以添加应用程序标识符，或单击**取消**以取消添加应用程序标识符。

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，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。

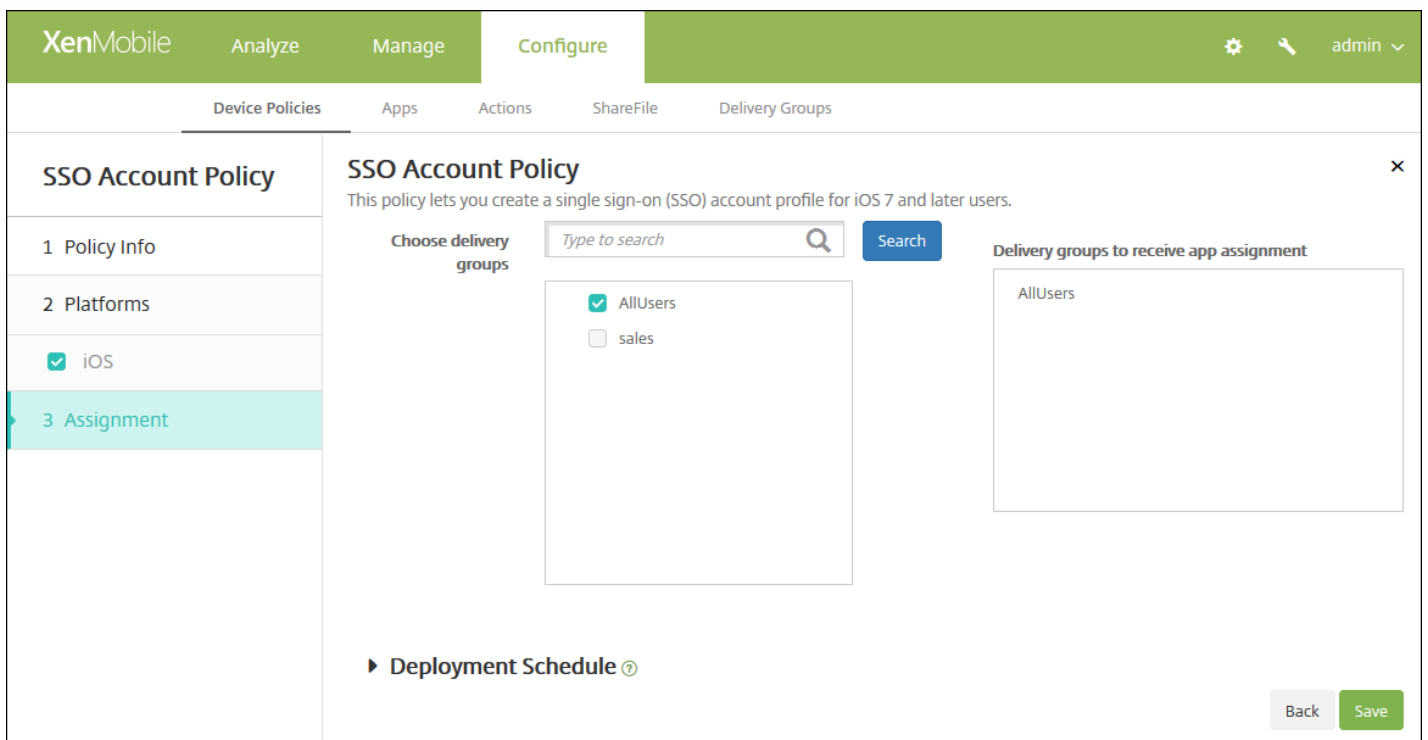
要编辑现有 URL 或应用程序标识符，请将鼠标悬停在包含此列表的行上，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击“保存”以保存更改的列表，或单击“取消”以保持列表不变。

● 策略设置

- 在删除策略旁边，单击选择日期或删除前保留时间(天)。
- 如果单击选择日期，请单击日历以选择具体删除日期。
- 在允许用户删除策略列表中，单击始终、需要密码或从不。
- 如果单击需要密码，在删除密码旁边，键入必需的密码。

7. 配置部署规则

8. 单击下一步。此时将显示 SSO 帐户策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

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

- 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。

存储加密设备策略

Feb 27, 2017

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

可以创建适用于 Samsung SAFE、Windows Phone 和 Android Sony 设备的策略。每种平台需要一组不同的值，本文将对此进行详细介绍。

[Samsung SAFE 设置](#)

[Windows Phone 设置](#)

[Android Sony 设置](#)

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

- 必须在用户设备上设置屏幕锁定选项。
- 用户设备必须已接通电源并且已充电 80%。
- 设备必须使用包含数字和字母或符号的密码。

1. 在 XenMobile 控制台中，单击 **配置 > 设备策略**。此时将显示 **设备策略** 页面。
2. 单击 **添加**。此时将显示 **添加新策略** 对话框。
3. 单击 **更多**，然后在 **安全性** 下方，单击 **存储加密**。此时将显示 **存储加密策略** 信息页面。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Storage Encryption Policy' and contains a 'Policy Information' section. The description states: 'This policy lets you encrypt stored data and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.' There are two input fields: 'Policy Name*' and 'Description'. The 'Policy Name*' field is empty, and the 'Description' field is a large text area. On the left side, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', three options are listed with checked checkboxes: 'Samsung SAFE', 'Windows Phone', and 'Android Sony'. At the bottom right of the main content area, there is a green 'Next >' button.

4. 在策略信息窗格中，键入以下信息：

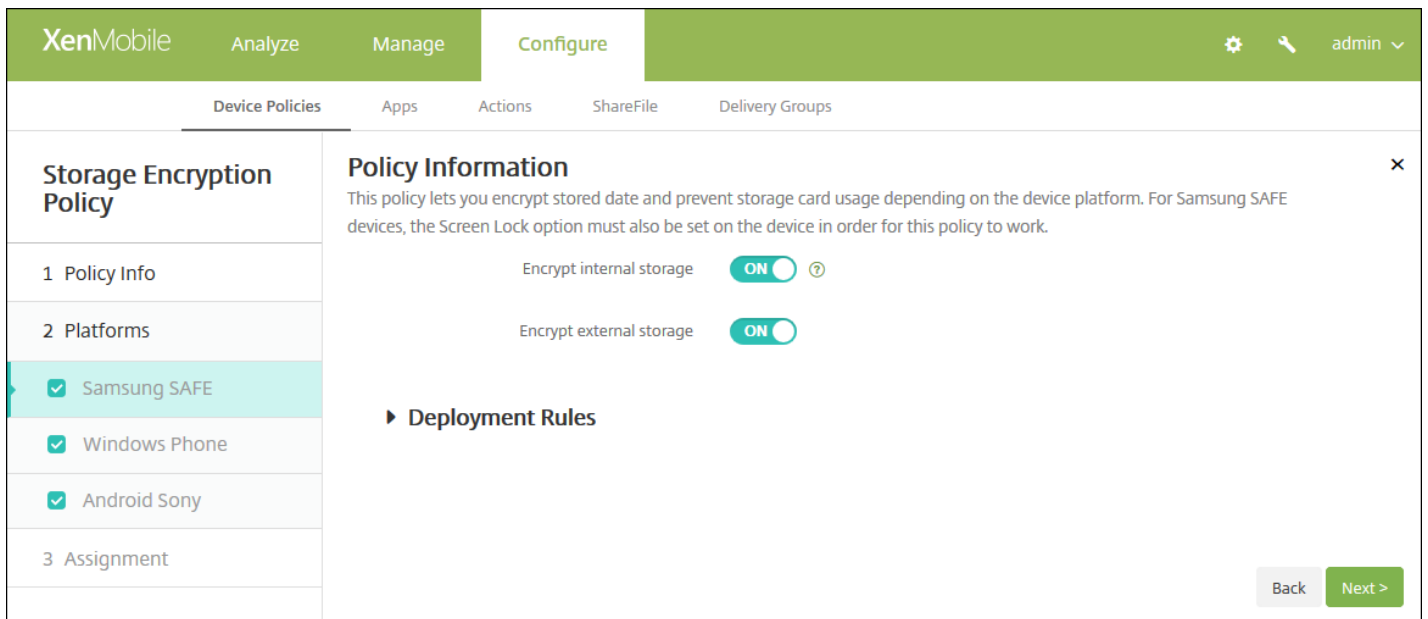
- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

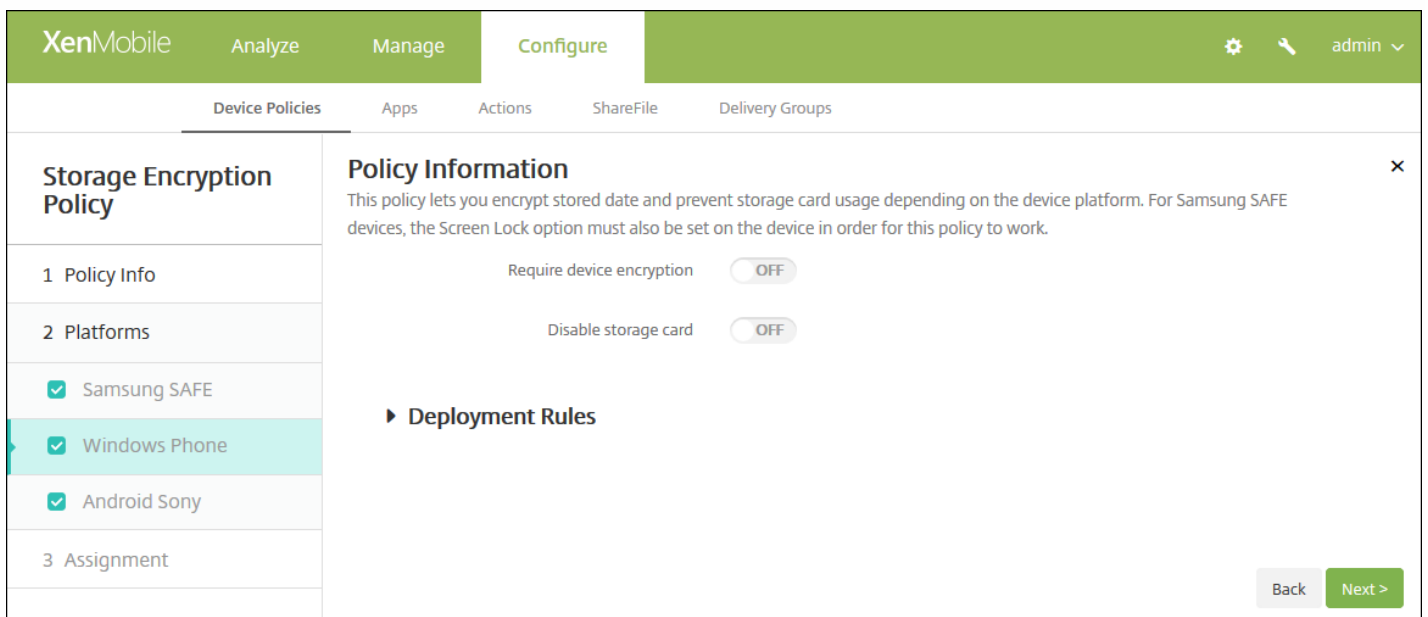
配置 Samsung SAFE 设置



配置以下设置：

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

配置 Windows Phone 设置



配置以下设置：

- **Require device encryption:** Select whether to encrypt users' devices. 默认值为关。
- **禁用存储卡：**选择是否阻止用户在其设备上使用存储卡。默认值为关。

配置 Android Sony 设置

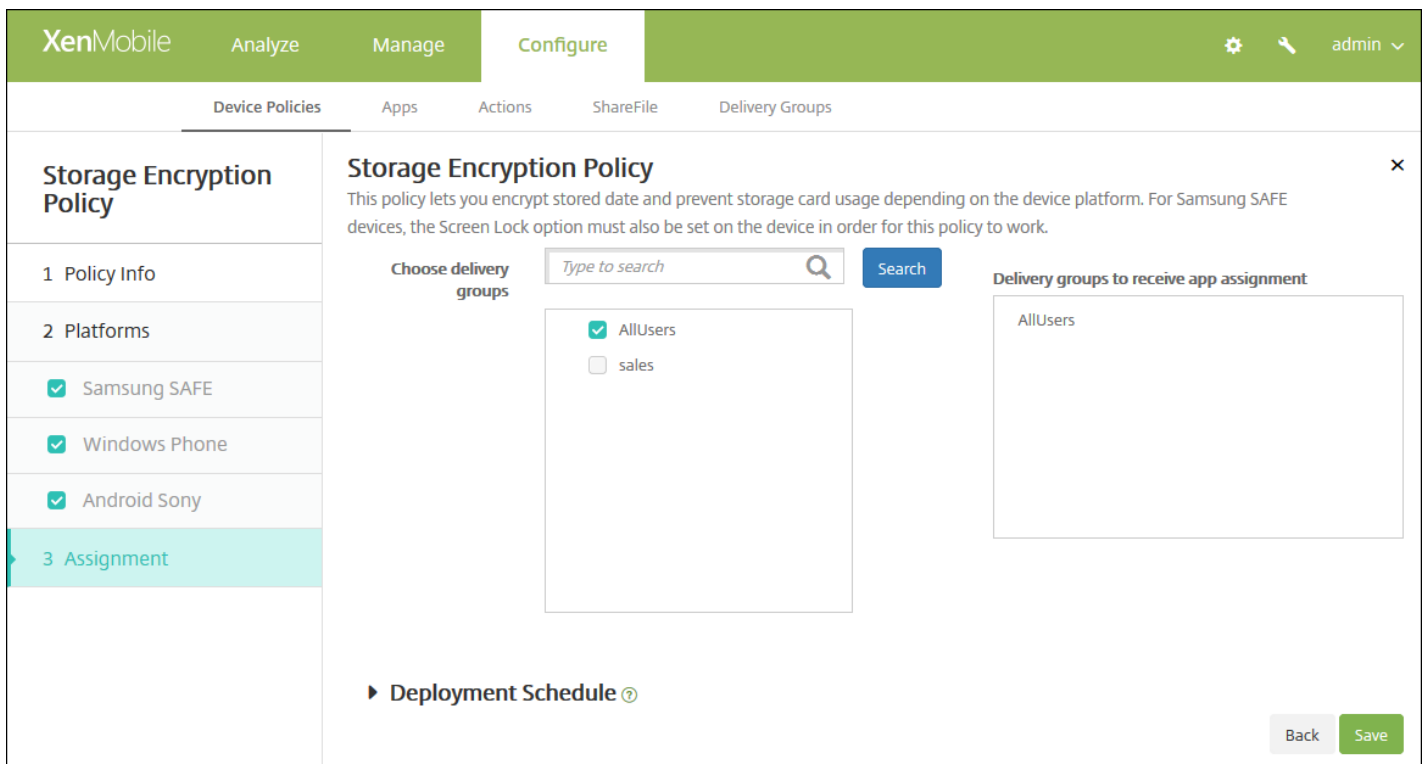
The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Storage Encryption Policy' and includes a 'Policy Information' section with a description and a toggle for 'Encrypt external storage' which is currently turned ON. There is also a 'Deployment Rules' section. A sidebar on the left lists steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android Sony' is selected. At the bottom right, there are 'Back' and 'Next >' buttons.

配置以下设置：

- **加密外部存储：**选择是否加密用户设备上的外部存储。设备必须使用包含数字和字母或符号的密码。默认值为开。

7. 配置部署规则

8. 单击下一步。此时将显示存储加密策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

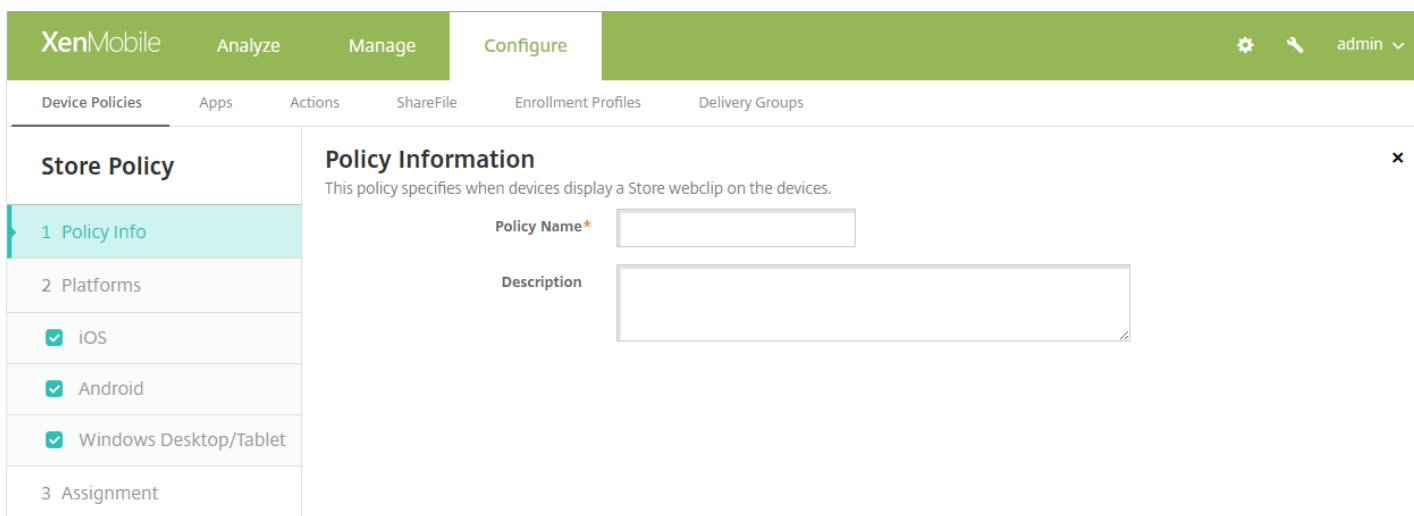
11. 单击保存。

应用商店设备策略

Feb 27, 2017

可以在 XenMobile 中创建一个策略，以指定 iOS、Android 或 Windows Tablet 设备是否在设备的主屏幕上显示 XenMobile Store Web 剪辑。

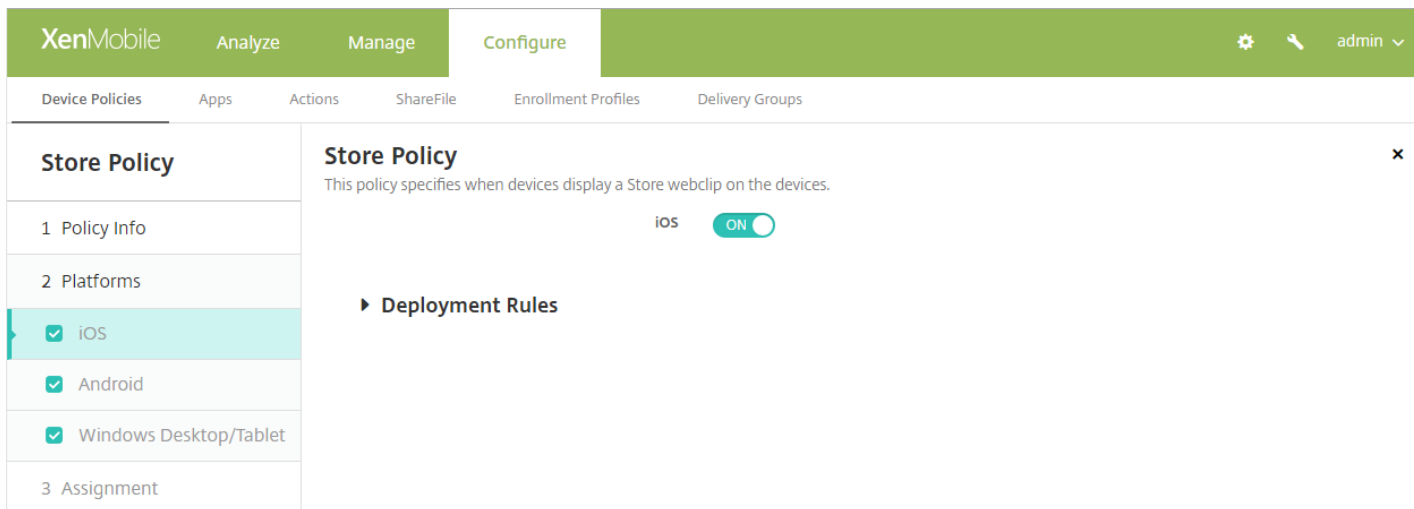
1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 展开更多，然后在应用程序下面，单击应用商店。此时将显示应用商店策略页面。



4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：如有需要，请键入策略的说明。

5. 单击下一步。此时将显示平台页面。



6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

7. 对于所配置的每个平台，请选择是否在用户的设备上显示 XenMobile Store Web 剪辑。默认值为开。

配置好各个平台后，请参阅步骤 8 以了解如何设置此平台的部署规则。

8. 配置部署规则

9. 单击下一步，将显示 **XenMobile Store 策略分配** 页面。

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

11. 展开**部署计划**，然后配置以下设置：

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

注意：

- 已在**设置 > 服务器属性**中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为**始终启用的连接部署**除外，它不适用于 iOS。

12. 单击**保存**。

已订阅的日历设备策略

Feb 27, 2017

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

注意：必须已经订阅某个日历，才能将其添加到用户设备上已订阅的日历列表中。

1. 在 XenMobile 控制台中，单击配置 > 设备策略。此时将显示设备策略页面。
2. 单击添加。此时将显示添加新策略对话框。
3. 单击更多，然后在最终用户下方，单击已订阅的日历。此时将显示已订阅的日历策略页面。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Subscribed Calendars Policy' and 'Policy Information'. It includes a description: 'This policy adds the parameters for a subscribed calendar to a users' calendars list.' There are two input fields: 'Policy Name*' and 'Description'. The 'Policy Name*' field is a text box, and the 'Description' field is a larger text area. A 'Next >' button is located at the bottom right of the form. The left sidebar shows a navigation menu with '1 Policy Info' selected, '2 Platforms', and '3 Assignment'.

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。

The screenshot shows the XenMobile configuration interface for a 'Subscribed Calendars Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', 'Configure', and 'admin'. Below the navigation bar, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Subscribed Calendars Policy' section with sub-items: '1 Policy Info', '2 Platforms', '3 Assignment', and 'iOS' (which is selected). The main content area is titled 'Policy Information' and contains the following fields and settings:

- Description***: A text input field with a help icon.
- URL***: A text input field with a help icon.
- User name***: A text input field.
- Password**: A text input field with a password icon.
- Use SSL**: A toggle switch set to 'OFF'.
- Policy Settings**:
 - Remove policy**: Two radio buttons: 'Select date' (selected) and 'Duration until removal (in days)'.
 - Allow user to remove policy**: A dropdown menu set to 'Always'.
- Deployment Rules**: A section header with a right-pointing arrow.

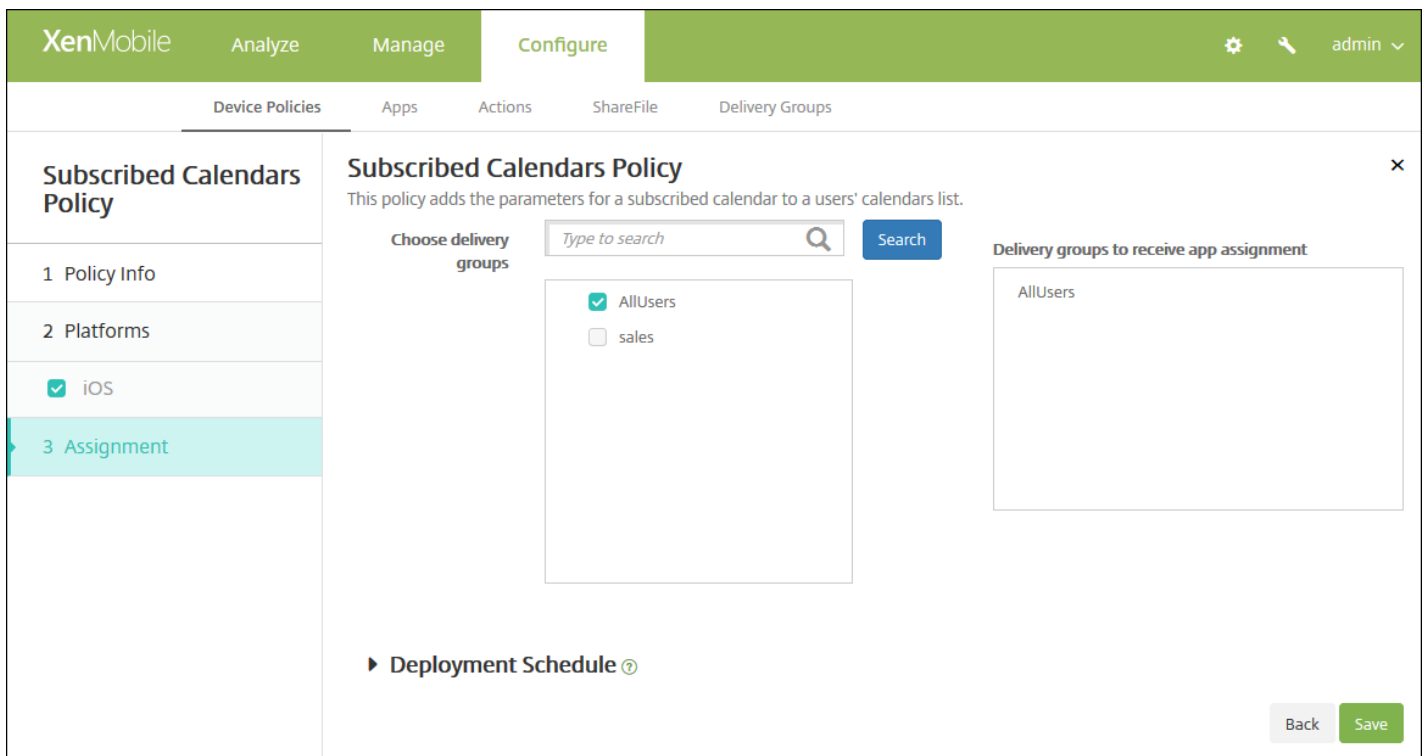
At the bottom right of the main content area, there are 'Back' and 'Next >' buttons.

6. 配置以下设置：

- **说明**：输入日历的说明。此字段为必填字段。
- **URL**：输入日历 URL。可以输入 iCalendar 文件 (.ics) 的 webcal:// URL 或 http:// 链接。此字段为必填字段。
- **用户名**：输入用户的登录名称。此字段为必填字段。
- **密码**：输入可选用户密码。
- **使用 SSL**：选择是否使用安全套接字层连接到日历。默认值为“关”。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

7. 配置部署规则

8. 单击下一步。此时将显示已订阅的日历策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

条款和条件设备策略

Feb 27, 2017

如果希望用户接受贵公司用于控制企业网络连接的特定政策，可以在 XenMobile 中创建“条款和条件”设备策略。当用户向 XenMobile 注册其设备时，系统会向其显示条款和条件，用户必须接受这些条款和条件才能注册其设备。拒绝这些条款和条件会取消注册过程。

如果贵公司具有国际用户，并且希望用户接受采用其本地语言描述的条款和条件，则可以采用不同的语言创建不同的条款和条件策略。必须为计划部署的每个平台和语言组合提供一个文件。对于 Android 和 iOS 设备，必须提供 PDF 文件。对于 Windows 设备，必须提供文本 (.txt) 文件和随附的图像文件。

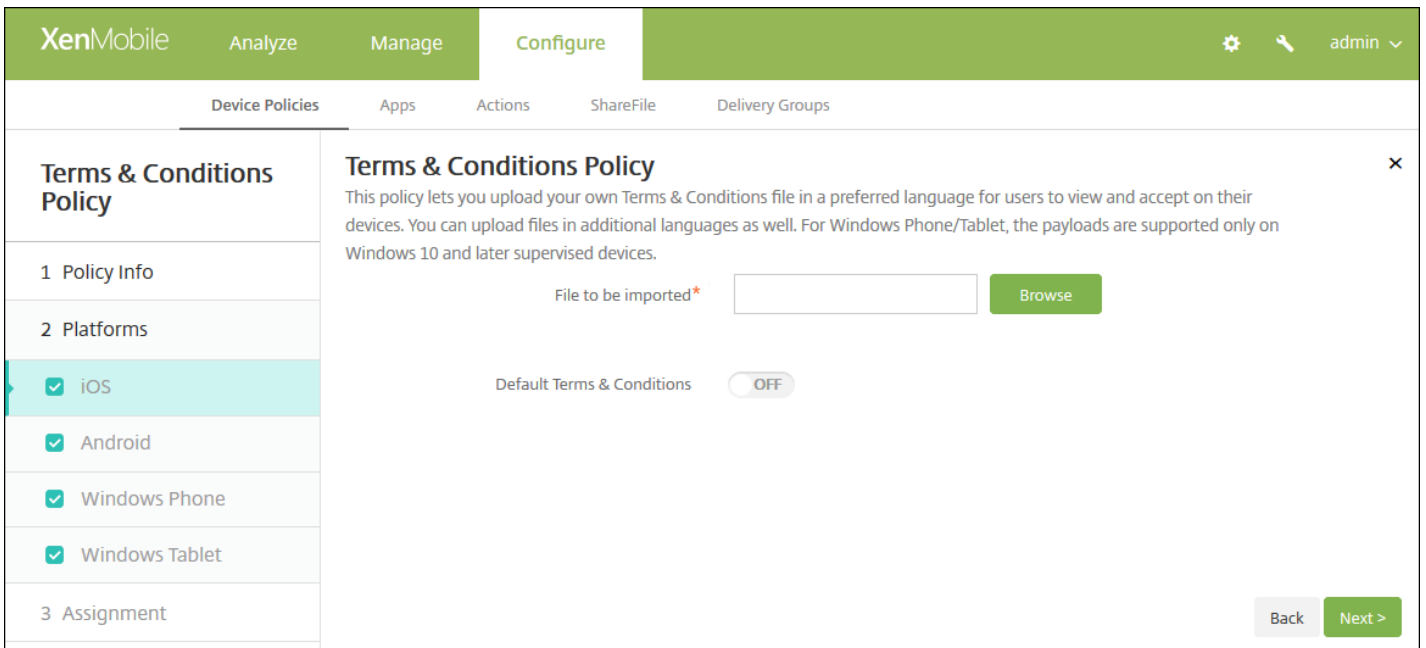
iOS 和 Android 设置

Windows Phone 和 Windows Tablet 设置

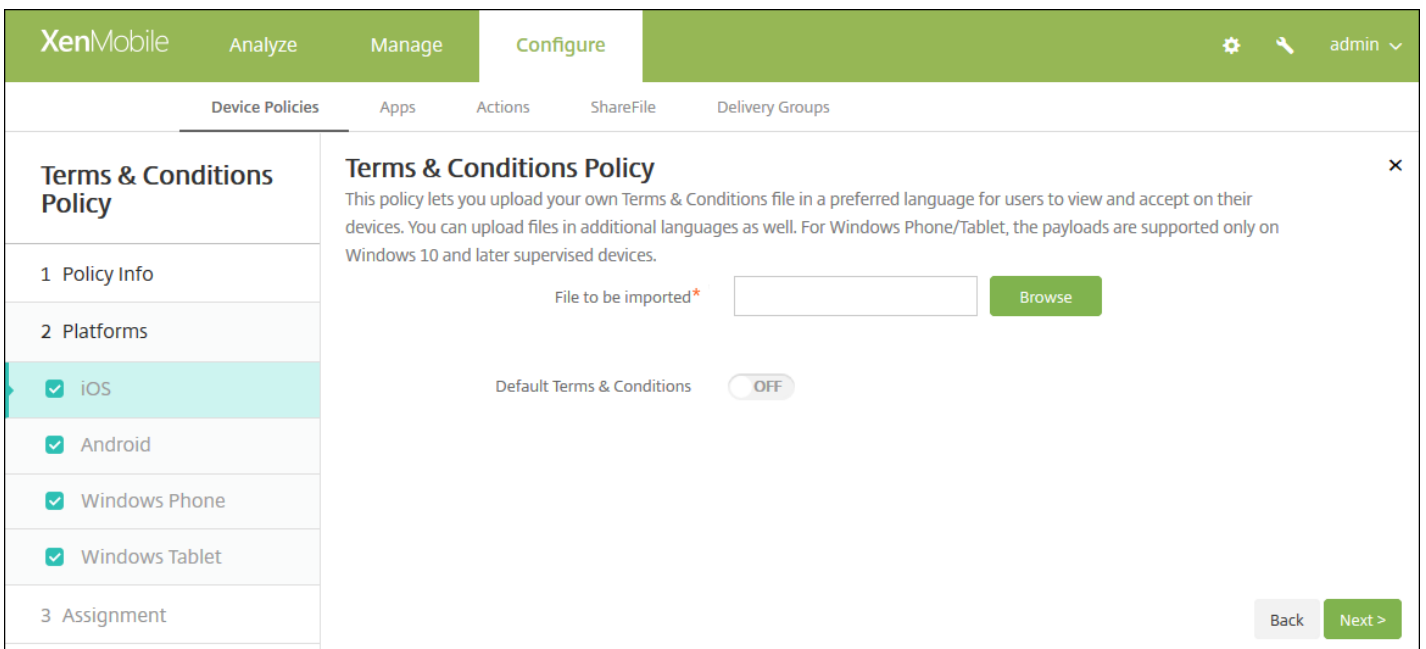
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**条款和条件**。此时将显示**条款和条件策略**页面。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Terms & Conditions Policy' and 'Policy Information'. It contains a description of the policy and two input fields: 'Policy Name*' and 'Description'. The 'Policy Name*' field is empty. The 'Description' field is a large text area, also empty. On the left side, there is a sidebar with 'Terms & Conditions Policy' and three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are four checkboxes, all of which are checked: 'iOS', 'Android', 'Windows Phone', and 'Windows Tablet'. At the bottom right of the main content area, there is a green 'Next >' button.

4. 在策略信息窗格中，输入以下信息：
 - **策略名称**：键入策略的描述性名称。
 - **说明**：（可选）键入策略的说明。
5. 单击下一步。此时将显示**条款和条件平台信息**页面。



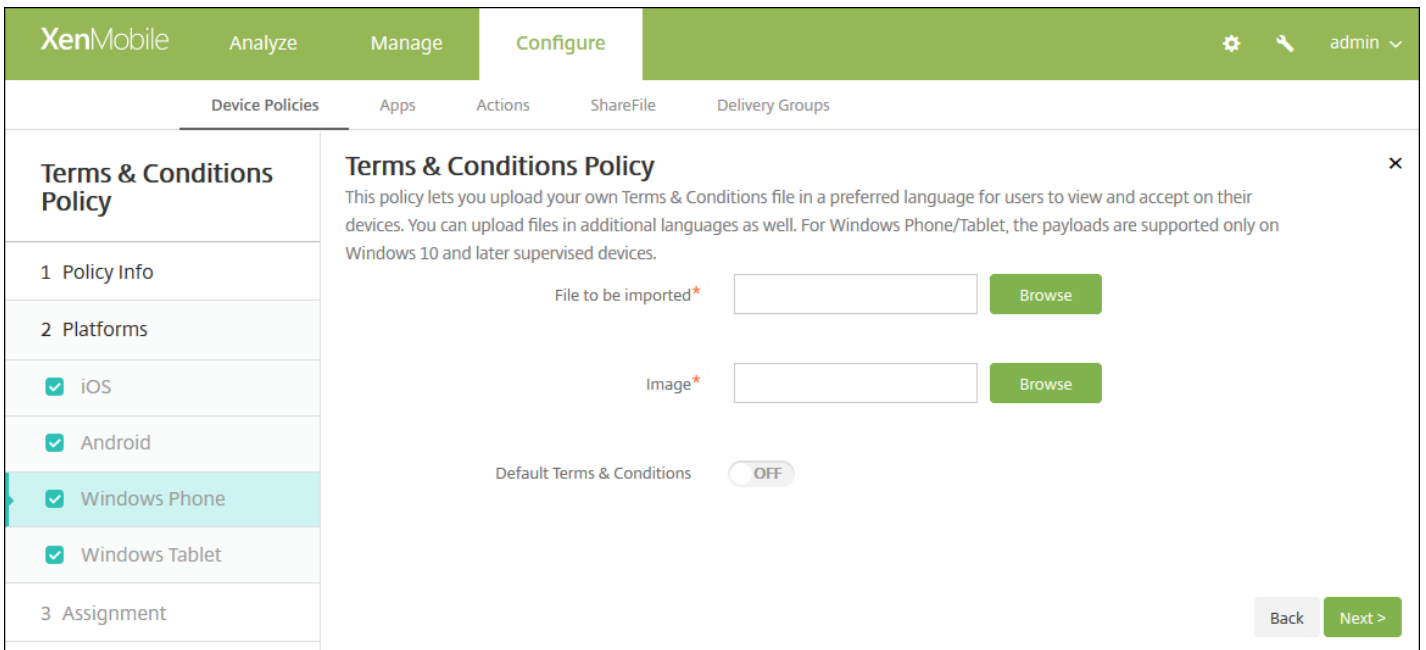
iOS 和 Android 设置



配置以下设置：

- 要导入的文件：单击**浏览**，然后导航到要导入的条款和条件文件的位置，选择此文件。
- 默认条款和条件：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。默认值为**关**。

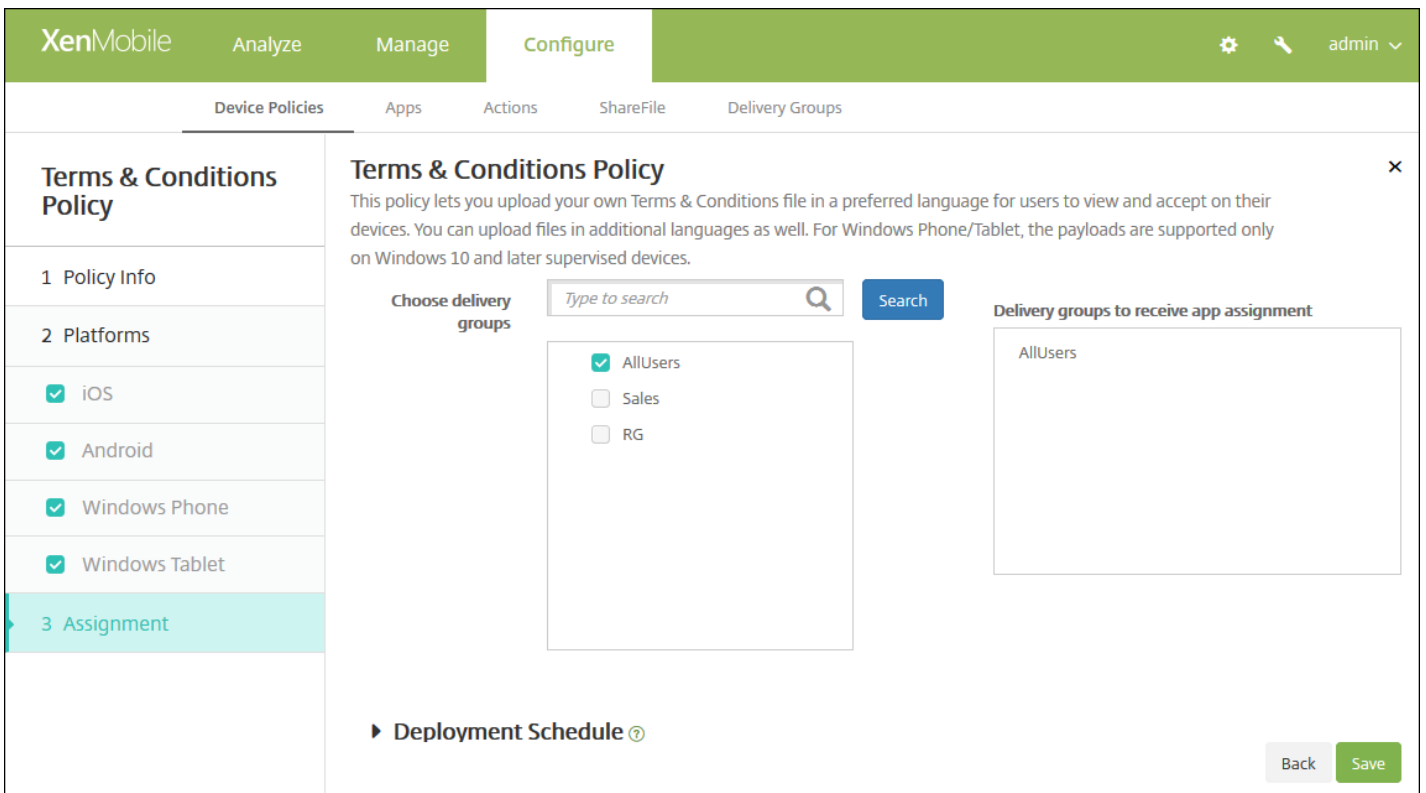
Windows Phone 和 Windows Tablet 设置



配置以下设置：

- 要导入的文件：单击**浏览**，然后导航到要导入的条款和条件文件的位置，选择此文件。
- 图片：单击**浏览**并导航到要导入的图片文件的位置，选择此文件。
- 默认条款和条件：选择是否将此文件作为默认文档，当用户属于采用不同条款和条件的多个组时，将使用此文件。默认值为关。

6. 单击下一步。此时将显示条款和条件策略分配页面。



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

8. 单击保存。

VPN 设备策略

May 07, 2017

可以在 XenMobile 中添加用于配置虚拟专用网络 (VPN) 设置的设备策略，使用户设备安全地连接到企业网络。可以为以下平台配置 VPN 策略：iOS、Android（包括为 Android for Work 启用的设备）、Samsung SAFE、Samsung KNOX、Windows Tablet、Windows Phone 和 Amazon。每种平台需要一组不同的值，本文将对此进行详细介绍。

[iOS 设置](#)

[Mac OS X 设置](#)

[Android 设置](#)

[Samsung SAFE 设置](#)

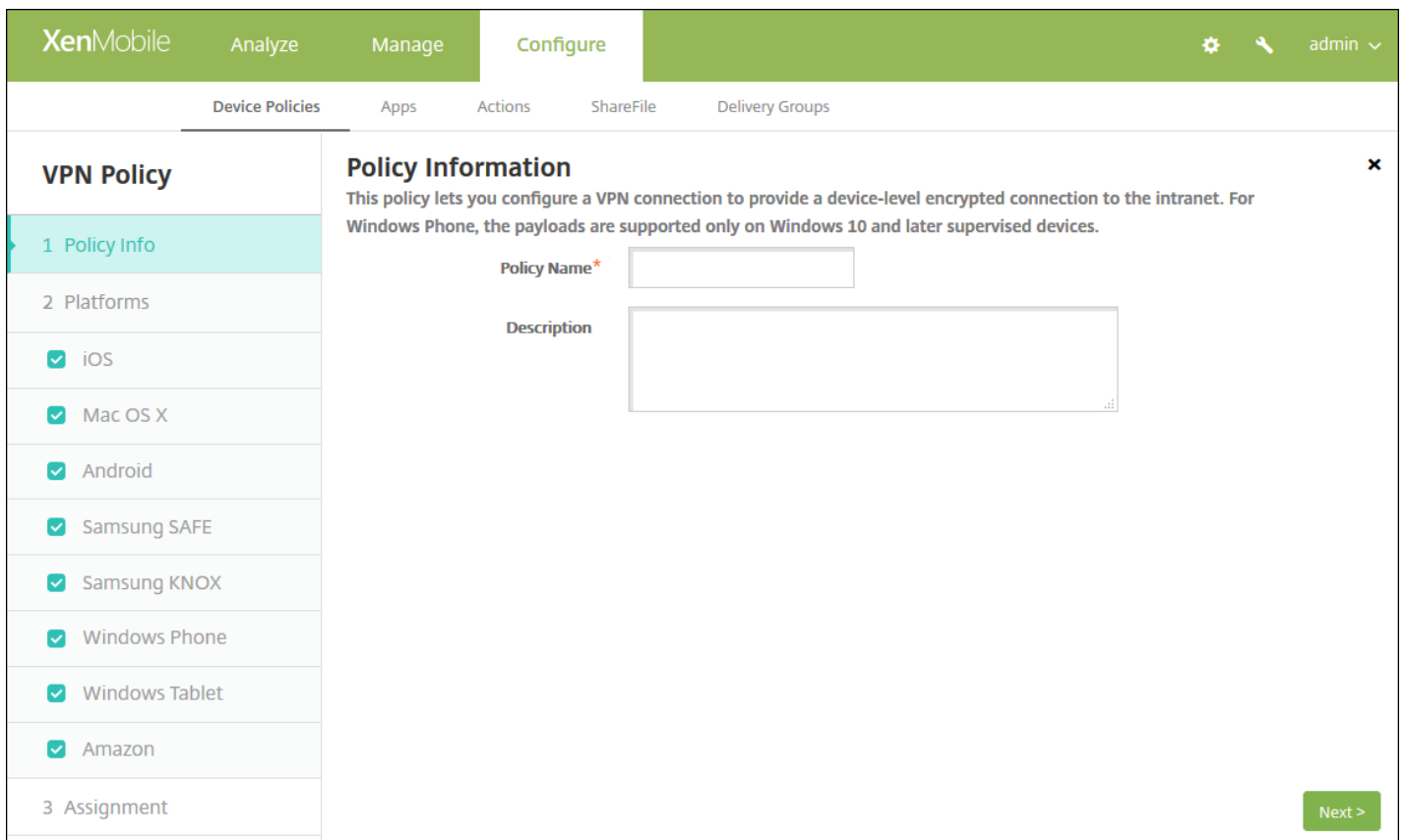
[Samsung KNOX 设置](#)

[Windows Phone 设置](#)

[Windows Tablet 设置](#)

[Amazon 设置](#)

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**VPN**。此时将显示**VPN 策略**页面。



4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。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. 在平台下方，选择要添加的一个或多个平台。清除不希望配置的平台。

为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

VPN Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Android
 - Samsung SAFE
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet
 - Amazon
- 3 Assignment

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name:

Connection type: **L2TP**

Server name or IP address*:

User account:

Password authentication
 RSA SecureID authentication

Shared secret:

Send all traffic: **OFF**

Proxy

Proxy configuration: **None**

Policy Settings

Remove policy:

 Select date

 Duration until removal (in days)

Allow user to remove policy: **Always**

► **Deployment Rules**

Back Next >

配置以下设置

- **连接名称**：键入连接的名称。
- **连接类型**：在列表中，单击将用于此连接的协议。默认值为 **L2TP**。
 - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
 - **PPTP**：点对点通道。
 - **IPSec**：企业 VPN 连接。
 - **Cisco AnyConnect**：Cisco AnyConnect VPN 客户端。
 - **Juniper SSL**：Juniper Networks SSL VPN 客户端。
 - **F5 SSL**：F5 Networks SSL VPN 客户端。
 - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。
 - **Ariba VIA**：Ariba Networks Virtual Internet Access 客户端。
 - **IKEv2 (仅限 iOS)**：仅限适用于 iOS 的 Internet 密钥交换 2 版。
 - **Citrix VPN**：适用于 iOS 的 Citrix VPN 客户端。
 - **自定义 SSL**：自定义安全套接字层。

以下部分列出了前面每种连接类型的配置选项。

配置 L2TP 协议	∨
配置 PPTP 协议	∨
配置 IPsec 协议	∨
配置 Cisco AnyConnect 协议	∨
配置 Juniper SSL 协议	∨
配置 F5 SSL 协议	∨
配置 SonicWALL 协议	∨
配置 Ariba VIA 协议	∨
配置 IKEv2 协议	∨
配置 Citrix VPN 协议	∨
配置自定义 SSL 协议	∨
配置“按需启用 VPN”选项	∨

- 代理

- 代理配置：在列表中，选择 VPN 连接通过代理服务器进行路由的方式。默认值为无。
 - 如果启用手动，可以配置以下设置：
 - 代理服务器的主机名或 IP 地址：键入代理服务器的主机名或 IP 地址。此字段为必填字段。
 - 代理服务器的端口：键入代理服务器的端口号。此字段为必填字段。
 - 用户名：键入可选代理服务器用户名。
 - 密码：键入可选代理服务器密码。
 - 如果配置自动，可以配置以下设置：
 - 代理服务器 URL：键入代理服务器的 URL。此字段为必填字段。

- 策略设置

- 在策略设置下方的删除策略旁边，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，在删除密码旁边，键入必需的密码。

配置 Mac OS X 设置

VPN Policy

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Tablet
- Amazon

3 Assignment

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name

Connection type **L2TP**

Server name or IP address*

User account

Password authentication
 RSA SecureID authentication
 Kerberos authentication
 CryptoCard authentication

Shared secret

Send all traffic **OFF**

Proxy

Proxy configuration **None**

Policy Settings

Remove policy Select date
 Duration until removal (in days)

Allow user to remove policy **Always**

Profile scope **User** OS X 10.7+

Deployment Rules

Back Next >

配置以下设置：

- **连接名称**：键入连接的名称。
- **连接类型**：在列表中，单击将用于此连接的协议。默认值为 L2TP。
 - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
 - **PPTP**：点对点通道。
 - **IPSec**：企业 VPN 连接。
 - **Cisco AnyConnect**：Cisco AnyConnect VPN 客户端。
 - **Juniper SSL**：Juniper Networks SSL VPN 客户端。
 - **F5 SSL**：F5 Networks SSL VPN 客户端。
 - **SonicWALL Mobile Connect**：适用于 iOS 的 Dell 统一 VPN 客户端。

- **Ariba VIA** : Ariba Networks Virtual Internet Access 客户端。
- **Citrix VPN** : Citrix VPN 客户端。
- **自定义 SSL** : 自定义安全套接字层。

以下部分列出了前面每种连接类型的配置选项。

配置 L2TP 协议	∨
配置 PPTP 协议	∨
配置 IPsec 协议	∨
配置 Cisco AnyConnect 协议	∨
配置 Juniper SSL 协议	∨
配置 F5 SSL 协议	∨
配置 SonicWALL 协议	∨
配置 Ariba VIA 协议	∨
配置 Citrix VPN 协议	∨
配置自定义 SSL 协议	∨
配置“按需启用 VPN”选项	∨

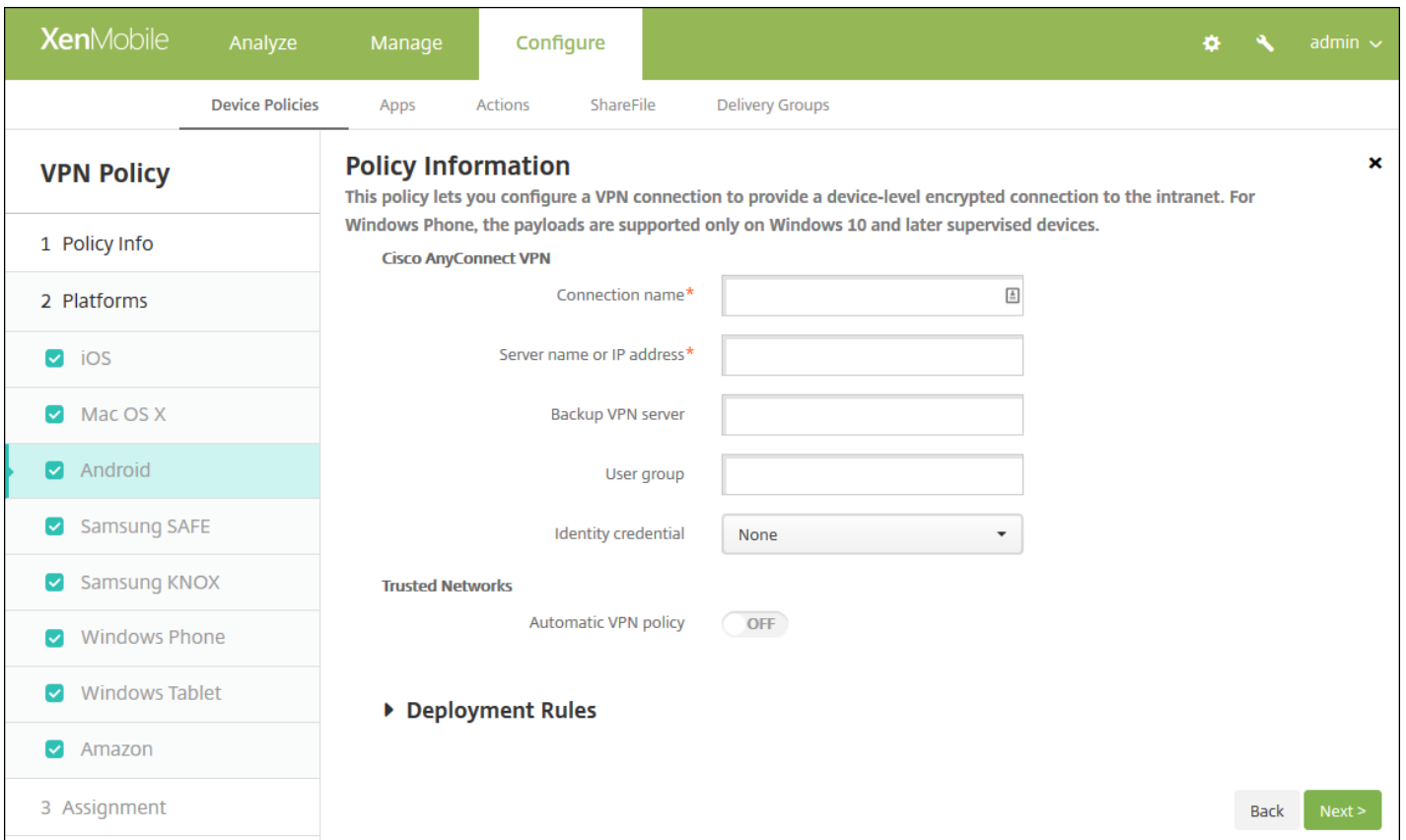
- **代理**

- **代理配置** : 在列表中, 选择 VPN 连接通过代理服务器进行路由的方式。默认值为无。
 - 如果启用手动, 可以配置以下设置 :
 - **代理服务器的主机名或 IP 地址** : 键入代理服务器的主机名或 IP 地址。此字段为必填字段。
 - **代理服务器的端口** : 键入代理服务器的端口号。此字段为必填字段。
 - **用户名** : 键入可选代理服务器用户名。
 - **密码** : 键入可选代理服务器密码。
 - 如果配置自动, 可以配置以下设置 :
 - **代理服务器 URL** : 键入代理服务器的 URL。此字段为必填字段。

- **策略设置**

- 在**策略设置**下方的**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**删除密码**旁边, 键入必需的密码。
- 在**配置文件作用域**旁边, 单击**用户**或**系统**。默认值为**用户**。此选项仅适用于 OS X 10.7 及更高版本。

配置 Android 设置



配置以下设置：

- **Cisco AnyConnect VPN**
 - **连接名称**：输入 Cisco AnyConnect VPN 连接的名称。此字段为必填字段。
 - **服务器名称或 IP 地址**：键入 VPN 服务器的名称或 IP 地址。此字段为必填字段。
 - **备份 VPN 服务器**：键入备份 VPN 服务器信息。
 - **用户组**：键入用户组信息。
 - **身份凭据**：在列表中，选择身份凭据。
- **可信网络**
 - **自动 VPN 策略**：启用或禁用此选项，以设置 VPN 响应可信网络和不可信网络的方式。如果启用，可以配置以下设置：
 - **可信网络策略**：在列表中，单击所需的策略。默认值为**断开连接**。可能的选项包括：
 - **断开连接**：客户端终止可信网络中的 VPN 连接。这是默认值。
 - **连接**：客户端在可信网络中启动 VPN 连接。
 - **不执行任何操作**：客户端不执行任何操作。
 - **暂停**：用户在可信网络外部建立 VPN 会话后进入配置为可信的网络时，挂起 VPN 会话（而不是断开会话的连接）。用户再次离开可信网络时，会话恢复。这样无需在离开可信网络后建立新的 VPN 会话。
 - **不可信网络策略**：在列表中，单击所需的策略。默认值为**连接**。可能的选项包括：
 - **连接**：客户端在不可信网络中启动 VPN 连接。
 - **不执行任何操作**：客户端在不可信网络中启动 VPN 连接。此选项将禁用始终启用 VPN。
 - **可信域**：对于客户端位于可信网络时网络接口可能具有每个域后缀，请单击**添加**以执行下列操作：
 - **域**：键入要添加的域。
 - 单击**保存**以保存域，或单击**取消**不保存域。
 - **可信服务器**：对于客户端位于可信网络时网络接口可能具有每个服务器地址，请单击**添加**并执行下列操作：
 - **服务器**：键入要添加的服务器。

- 单击**保存**以保存服务器，或单击**取消**不保存服务器。

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

要编辑现有服务器，请将鼠标悬停在包含此列表的行上方，然后单击右侧的铅笔图标。对列表进行任何更改，然后单击**保存**以保存更改后的列表，或单击**取消**以保持列表不变。

配置 Samsung SAFE 设置

配置以下设置：

- **连接名称**：键入连接的名称。
- **Vpn 类型**：在列表中，单击将用于此连接的协议。默认值为带有**预共享密钥**的 **L2TP**。可能的选项包括：
 - **带有预共享密钥的 L2TP**：使用预共享密钥身份验证的第二层通道协议。此为默认设置。
 - **带有证书的 L2TP**：使用证书的第二层通道协议。
 - **PPTP**：点对点通道。
 - **Enterprise**：企业 VPN 连接。适用于 SAFE 2.0 之前的版本。
 - **通用**：通用 VPN 连接。适用于 SAFE 2.0 或更高版本。

以下部分列出了前面每种 VPN 类型的配置选项。

[配置带有预共享密钥的 L2TP 协议](#)

[配置使用证书的 L2TP 协议](#)

配置 PPTP 协议



配置企业协议



配置通用协议



配置 Samsung KNOX 设置

XenMobile
Analyze
Manage
Configure

admin ▾

Device Policies
Apps
Actions
ShareFile
Delivery Groups

VPN Policy

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Tablet
- Amazon

3 Assignment

Policy Information ✕

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Vpn Type Enterprise ▾

Connection name*

Host name*

Enable backup server OFF

Enable user authentication OFF

Group name

Authentication method Certificate ▾

Identity credential None ▾

CA certificate Select certificate ▾

Enable default route OFF

Enable smartcard authentication OFF

Enable mobile option OFF

Diffie-Hellman group value (key strength) 0 ▾

Split tunnel type Auto ▾

SuiteB Type GCM-128 ▾

Forward routes

Forward route

Forward route	
	Add

► Deployment Rules

Back
Next >

注意：为 Samsung KNOX 配置任何策略时，策略仅在 Samsung KNOX 容器内适用。

配置以下设置：

- **Vpn 类型**：在列表中，单击要配置的 VPN 连接类型，即**企业**（适用于 KNOX 2.0 之前的版本）或**通用**（适用于 KNOX 2.0 或更高版本）。默认值为企业。

以下部分列出了前面每种连接类型的配置选项。

配置企业协议 ▼

配置通用协议 ▼

配置 Windows Phone 设置

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'VPN Policy' and is divided into three sections: 'Policy Info', 'Platforms', and 'Assignment'. The 'Platforms' section lists various operating systems with checkboxes: iOS, Mac OS X, Android, Samsung SAFE, Samsung KNOX, Windows Phone (highlighted), Windows Tablet, and Amazon. The 'Assignment' section is currently empty. The right-hand side of the page displays 'Policy Information' for the selected policy, including a description and various configuration fields: 'Connection name' (text input), 'Profile type' (dropdown menu set to 'Native'), 'VPN server name' (text input), 'Tunneling protocol' (dropdown menu set to 'L2TP'), 'Authentication method' (dropdown menu set to 'EAP'), 'EAP method' (dropdown menu set to 'TLS'), 'DNS suffix' (text input), and 'Trusted networks' (text input). Below these fields are several toggle switches, all currently set to 'OFF': 'Require smart card certificate', 'Automatically select client certificate', 'Remember credential', 'Always-on VPN', and 'Bypass For Local'. At the bottom right, there are 'Back' and 'Next >' buttons.

注意：这些设置仅在 Windows 10 及更高版本的受监督手机上受支持。

配置以下设置：

- **连接名称**：输入连接的名称。此字段为必填字段。
- **配置文件类型**：在列表中，单击**本机**或**插件**。默认值为**本机**。以下部分将分别介绍这些选项的设置。
- **配置本机配置文件类型设置** - 这些设置适用于内置于用户 Windows Phone 的 VPN。
 - **VPN 服务器名称**：键入 VPN 服务器的 FQDN 或 IP 地址。此字段为必填字段。
 - **通道协议**：在列表中，单击要使用的 VPN 通道的类型。默认值为 **L2TP**。可能的选项包括：
 - **L2TP**：使用预共享密钥身份验证的第二层通道协议。
 - **PPTP**：点对点通道。
 - **IKEv2**：Internet 密钥交换第 2 版。
 - **身份验证方法**：在列表中，单击要使用的身份验证方法。默认值为 **EAP**。可能的选项包括：
 - **EAP**：扩展身份验证协议。
 - **MSChapV2**：使用 Microsoft 的质询-握手身份验证相互验证身份。选择 IKEv2 作为通道类型时，此选项不可用。选择 MSChapV2 时，会显示**自动使用 Windows 凭据**选项；默认值为关。
 - **EAP 方法**：在列表中，单击要使用的 EAP 方法。默认值为 **TLS**。启用 MSChapV2 身份验证时此字段不可用。可能的选项包括：
 - **TLS**：传输层安全性
 - **PEAP**：受保护的可扩展身份验证协议
 - **DNS 后缀**：键入 DNS 后缀。
 - **可信网络**：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
 - **需要智能卡证书**：选择是否需要智能卡证书。默认值为“关”。
 - **自动选择客户端证书**：选择是否自动选择用于身份验证的客户端证书。默认值为“关”。启用“需要智能卡证书”时此选项不可用。
 - **记住凭据**：选择是否缓存凭据。默认值为“关”。启用时，会在合适的时候缓存凭据。
 - **始终启用 VPN**：选择是否始终启用 VPN。默认值为“关”。启用后，VPN 连接保持可用，直到用户手动断开连接。
 - **跳过本地地址**：键入地址和端口号，以允许本地资源跳过代理服务器。
- **配置插件协议类型** - 这些设置适用于从 Windows 应用商店获取并安装在用户设备上的 VPN 插件。
 - **服务器地址**：键入 VPN 服务器的 URL、主机名或 IP 地址。
 - **客户端应用程序 ID**：键入 VPN 插件的软件包系列名称。
 - **插件配置文件 XML**：单击“浏览”并导航到要使用的自定义 VPN 插件配置文件的位置，选择该文件。有关格式及详细信息，请联系插件提供商。
 - **DNS 后缀**：键入 DNS 后缀。
 - **可信网络**：键入无需使用 VPN 连接进行访问的网络列表，以逗号分隔。例如，当用户在使用公司无线网络时，他们可以直接访问受保护的资源。
 - **记住凭据**：选择是否缓存凭据。默认值为“关”。启用时，会在合适的时候缓存凭据。
 - **始终启用 VPN**：选择是否始终启用 VPN。默认值为“关”。启用后，VPN 连接保持可用，直到用户手动断开连接。
 - **跳过本地地址**：键入地址和端口号，以允许本地资源跳过代理服务器。

配置 Windows Tablet 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

VPN Policy

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Android
 - Samsung SAFE
 - Samsung KNOX
 - Windows Phone
 - Windows Tablet**
 - Amazon
- 3 Assignment

Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

OS version* 10 ▾

Connection name*

Profile type Native ▾

Server address*

Remember credential OFF

DNS suffix

Tunnel type* L2TP ▾

Authentication method* EAP ▾

EAP method* TLS ▾

Trusted networks

Require smart card certificate OFF

Automatically select client certificate OFF

Always-on VPN OFF

Bypass For Local OFF

► Deployment Rules

[Back](#) [Next >](#)

<https://web.mail.comcast.net/zimbra/mail?app=mail#1>

配置以下设置：

[配置 Windows 10 设置](#)

[配置 Amazon 设置](#)

The screenshot shows the XenMobile 'Configure' interface for a VPN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'VPN Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Android, Samsung SAFE, Samsung KNOX, Windows Tablet, Windows Phone, and Amazon (which is highlighted). The 'Policy Information' section contains the following fields:

- Connection name* (text input)
- Vpn Type (dropdown menu, currently set to L2TP PSK)
- Server address* (text input)
- User name (text input)
- Password (text input)
- L2TP Secret (text input)
- IPSec Identifier (text input)
- IPSec pre-shared key (text input)
- DNS search domains (text input)
- DNS servers (text input)
- Forwarding routes (text input)

At the bottom of the main area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

配置以下设置：

- **连接名称**：输入连接的名称。
- **VPN 类型**：单击连接类型。可能的选项包括：
 - **L2TP PSK**：使用预共享密钥身份验证的第二层通道协议。这是默认值。
 - **L2TP RSA**：使用 RSA 身份验证的第二层通道协议。
 - **IPSEC XAUTH PSK**：使用预共享密钥和扩展身份验证的 Internet 协议安全性。
 - **IPSEC HYBRID RSA**：使用混合 RSA 身份验证的 Internet 协议安全性。
 - **PPTP**：点对点通道。

以下部分列出了前面每种连接类型的配置选项。

- [配置 L2TP PSK 设置](#) ▼
- [配置 L2TP RSA 设置](#) ▼
- [配置 IPSEC XAUTH PSK 设置](#) ▼

配置 IPSEC AUTH RSA 设置



配置 IPSEC HYBRID RSA 设置



配置 PPTP 设置



7. 配置部署规则



8. 单击下一步，将显示 VPN 策略分配页面。

The screenshot shows the XenMobile configuration interface for a VPN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main navigation includes 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'VPN Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. The '2 Platforms' section is expanded, showing a list of operating systems with checkboxes: iOS, Mac OS X, Android, Samsung SAFE, Samsung KNOX, Windows Phone, Windows Tablet, and Amazon. The '3 Assignment' section is highlighted. The main content area shows 'Choose delivery groups' with a search box and a list of groups: AllUsers (checked) and sales (unchecked). Below this is a 'Deployment Schedule' section. At the bottom right, there are 'Back' and 'Save' buttons.

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

10. 展开部署计划，然后配置以下设置：

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

注意：

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

- 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。

墙纸设备策略

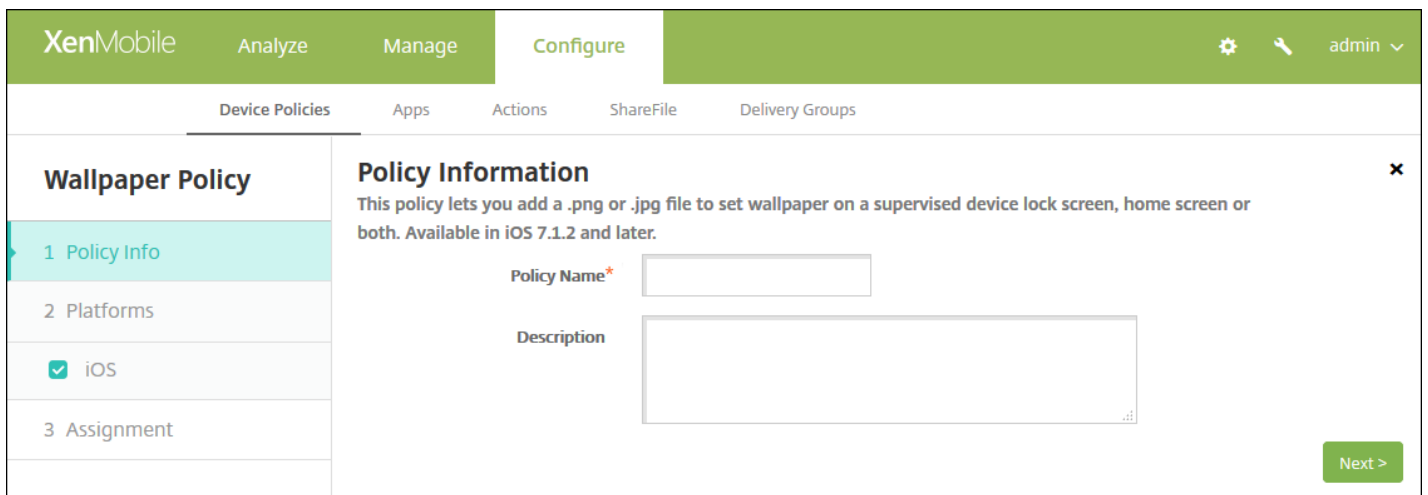
Feb 27, 2017

您可以添加 .png 或 .jpg 文件，以设置 iOS 设备锁屏界面、主屏幕或二者的墙纸。适用于 iOS 7.1.2 及更高版本。要在 iPad 和 iPhone 上使用不同的墙纸，需要创建不同的墙纸策略并将其部署到相应的用户。

下表列出了 Apple 建议的用于 iOS 设备的图片尺寸。

设备		图片尺寸 (像素)
iPhone	iPad	
4、4s		640 x 960
5、5c、5s		640 x 1136
6、6s		750 x 1334
6 Plus		1080 x 1920
	Air、2	1536 x 2048
	4、3	1536 x 2048
	Mini 2、3	1536 x 2048
	Mini	768 x 1024

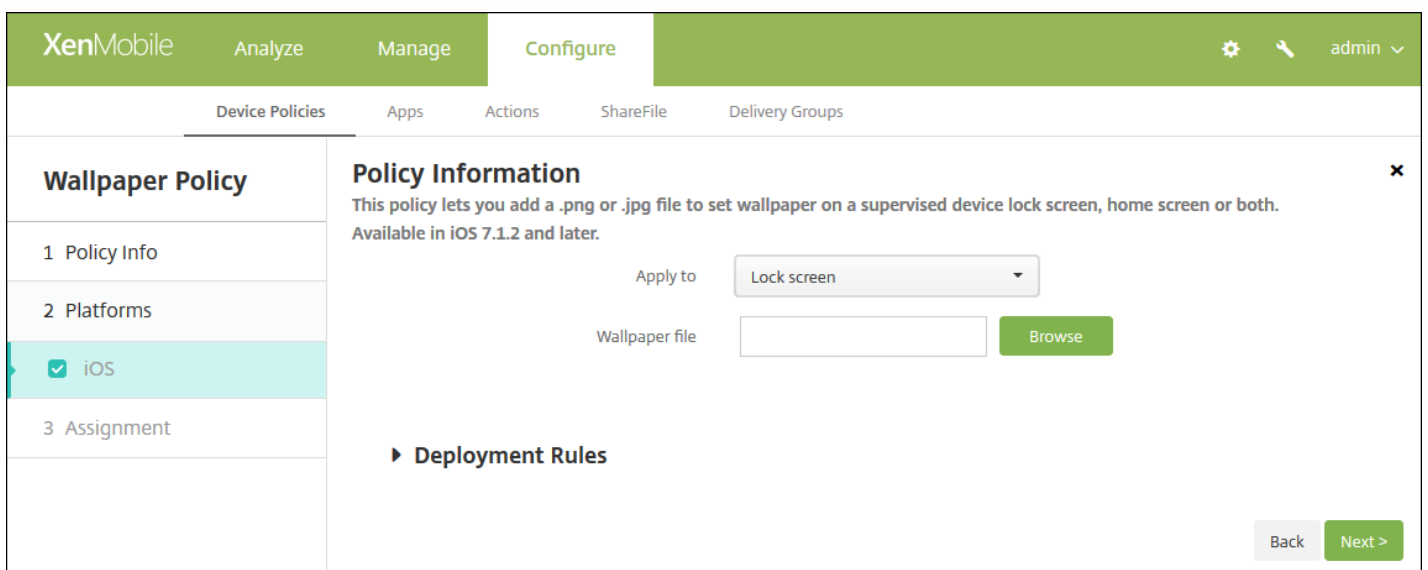
1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**最终用户**下方，单击**墙纸**。此时将显示**墙纸策略**页面。



4. 在策略信息窗格中，输入以下信息：

- **策略名称**：键入策略的描述性名称。
- **说明**：键入策略的可选说明。

5. 单击下一步。此时将显示策略平台页面。

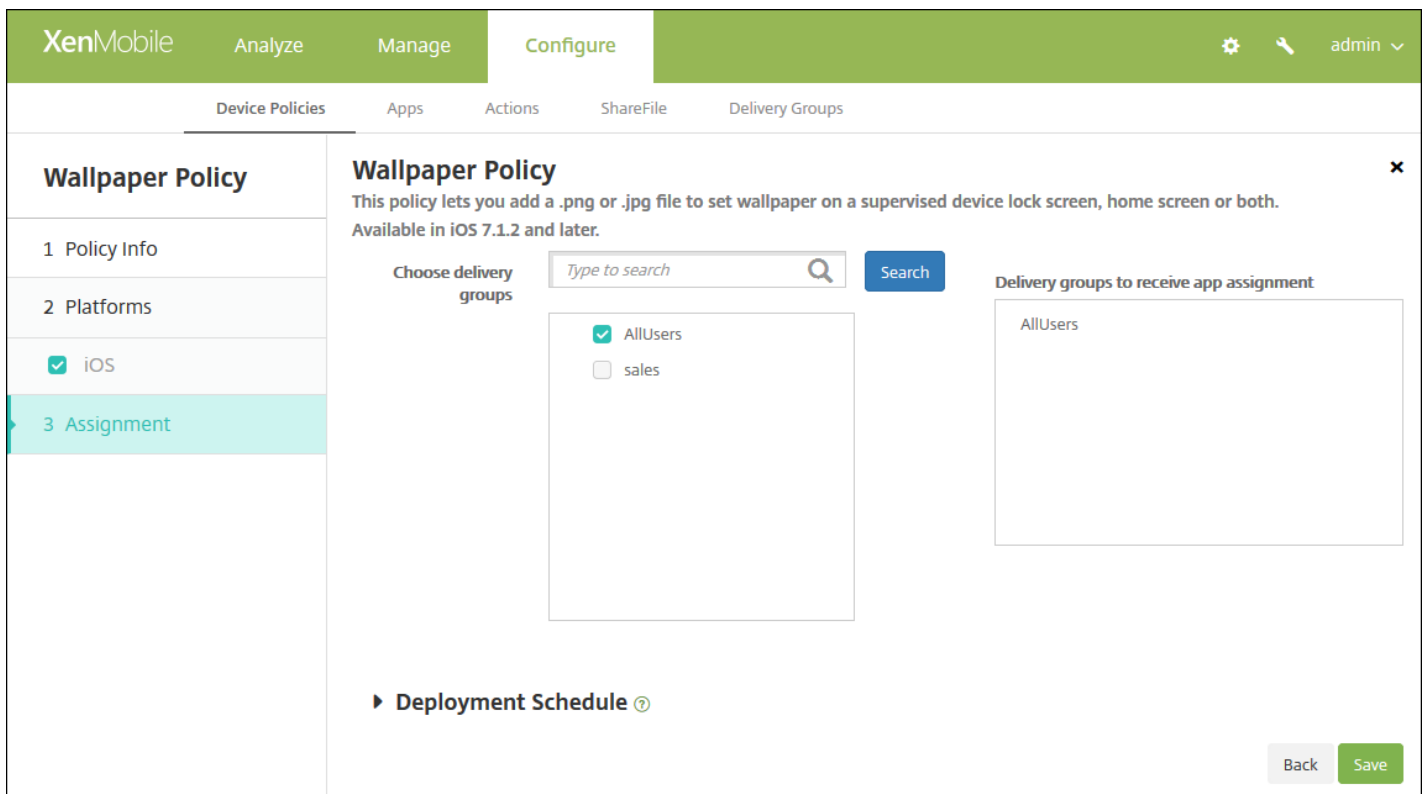


配置以下设置：

- **适用于**：在列表中，选择锁定屏幕、主(图标列表)屏幕或锁定屏幕和主屏幕以设置墙纸出现的位置。
- **墙纸文件**：单击浏览并导航到墙纸文件的位置，选择该文件。

7. 配置部署规则

8. 单击下一步。此时将显示墙纸策略分配页面。



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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用

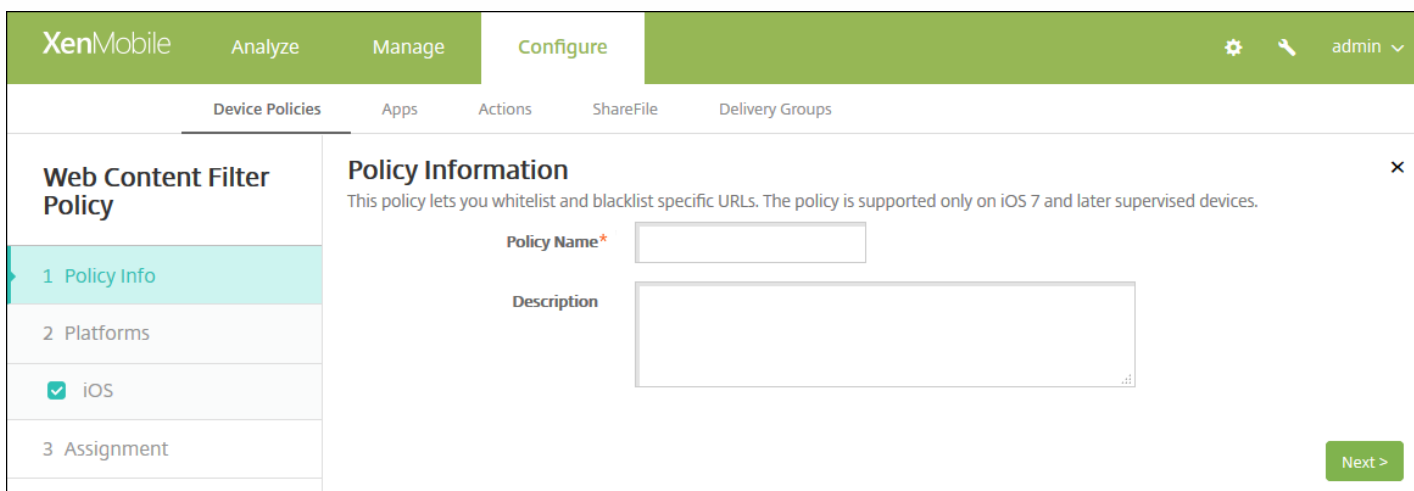
11. 单击保存。

Web 内容过滤器设备策略

Feb 27, 2017

可以在 XenMobile 中添加一个设备策略，通过结合使用 Apple 的自动过滤功能和添加到白名单和黑名单中的特定站点，在 iOS 设备上过滤 Web 内容。此策略仅适用于采用受监督模式的 iOS 7.0 及更高版本。有关将 iOS 设备置于受监督模式的信息，请参阅[使用 Apple Configurator 将 iOS 设备置于受监督模式](#)。

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 单击**更多**，然后在**安全性**下面，单击**Web 内容过滤器**。此时将显示**Web 内容过滤策略**页面。

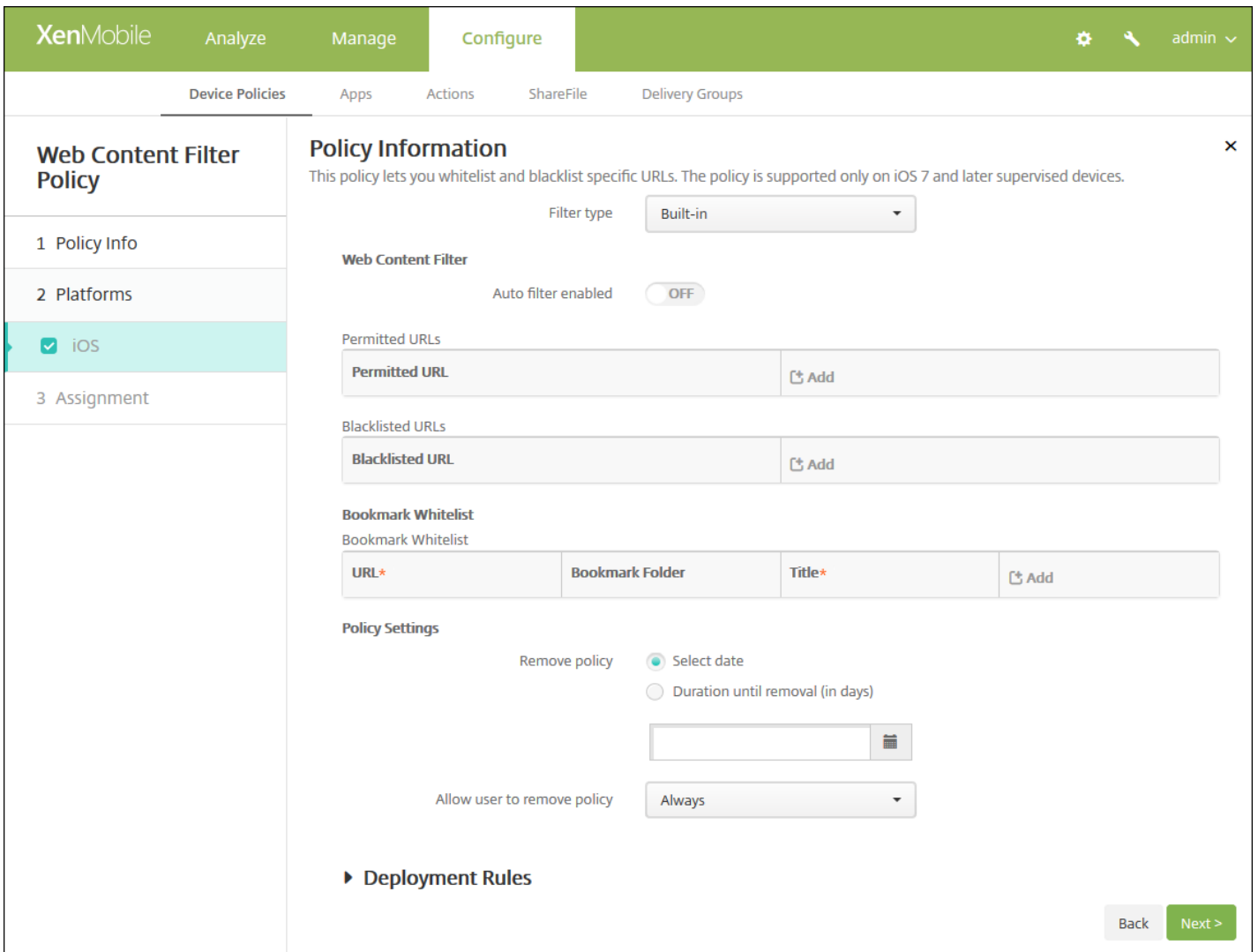


The screenshot shows the XenMobile configuration interface for a 'Web Content Filter Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Web Content Filter Policy' and contains a sidebar with steps: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. The 'Policy Information' section includes a description: 'This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.' There are two input fields: 'Policy Name*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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. 配置以下设置：

- **过滤器类型**：在列表中，单击**内置**或**插件**，然后按照所选选项后面的步骤操作。默认值为**内置**。

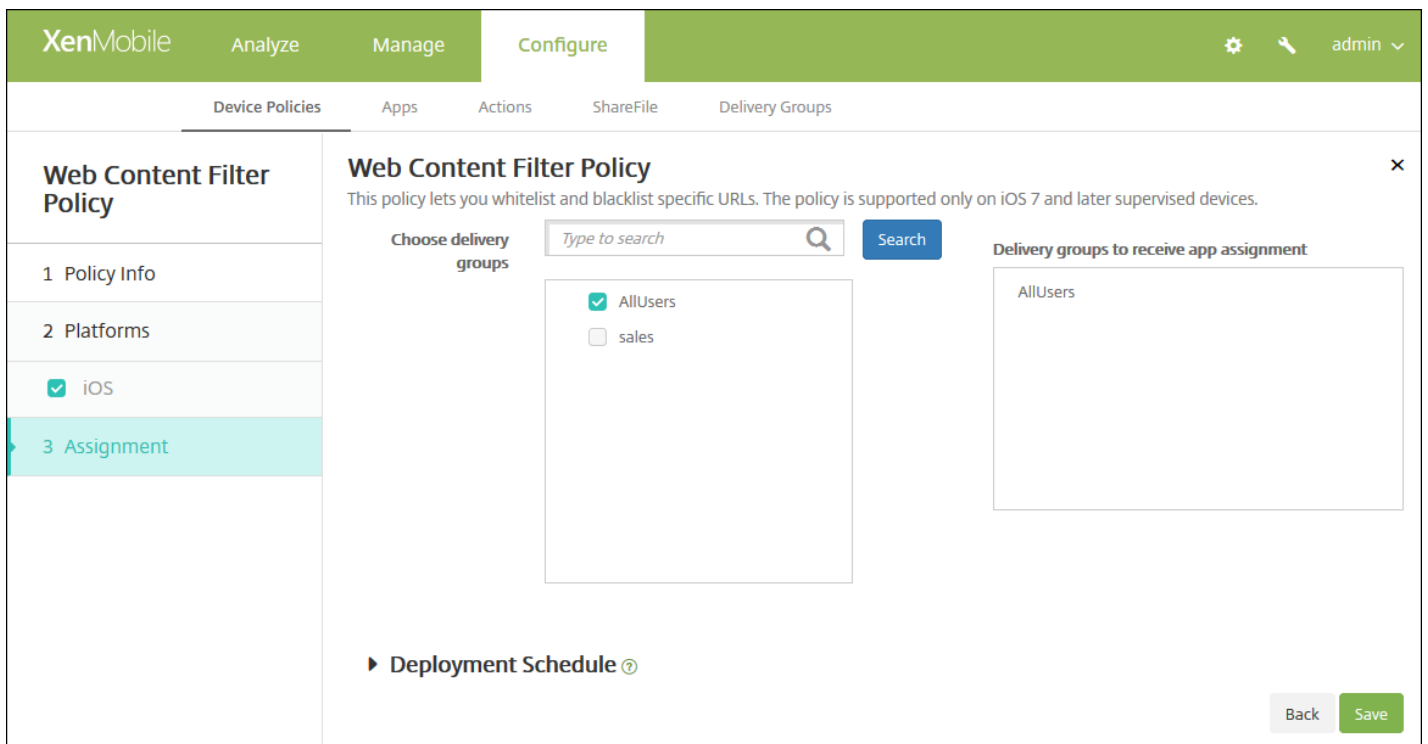
[内置过滤器类型设置](#) ▼

[插件过滤器类型设置](#) ▼

- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

[7. 配置部署规则](#) ▼

8. 单击**下一步**。此时将显示 **Web 内容过滤策略分配** 页面。



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

10. 展开部署计划，然后配置以下设置：

- 在部署旁边，单击开以计划部署，或单击关以阻止部署。默认选项为开。如果选择关，无需配置其他选项。
- 在部署计划旁边，单击立即或稍后。默认选项为立即。
- 如果单击稍后，请单击日历图标，然后选择部署的日期和时间。
- 在部署条件旁边，单击每次连接时或单击仅当之前的部署失败时。默认选项为每次连接时。
- 在“为始终启用的连接部署”旁边，单击“开”或“关”。默认选项为关。

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用于 iOS。

11. 单击保存。

Web 剪辑设备策略

Feb 27, 2017

您可以向 Web 站点中放置快捷方式或 Web 剪辑，使它们和应用程序一起出现在用户的设备上。您可以指定自己的图标来表示 iOS、Mac OS X 和 Android 设备的 Web 剪辑；Windows 平板电脑只需要使用标签和 URL。

[iOS 设置](#)

[Mac OS X 设置](#)

[Android 设置](#)

[Windows Desktop/Tablet 设置](#)

1. 在 XenMobile 控制台中，单击**配置 > 设备策略**。此时将显示**设备策略**页面。
2. 单击**添加**。此时将显示**添加新策略**对话框。
3. 展开**更多**，然后在**应用程序**下面，单击**Web 剪辑**。此时将显示**Web 剪辑策略**页面。

The screenshot shows the XenMobile configuration interface for a Webclip Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Webclip Policy' and contains a 'Policy Information' section. The description reads: 'This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.' There are two input fields: 'Policy Name*' and 'Description'. To the left, there is a sidebar with a list of platforms: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are four checked items: 'iOS', 'Mac OS X', 'Android', and 'Windows Desktop/Tablet'.

4. 在**策略信息**窗格中，输入以下信息：
 - **策略名称**：键入策略的描述性名称。
 - **说明**：键入策略的可选说明。
 5. 单击**下一步**。此时将显示**策略平台**页面。
 6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。
- 为平台配置了设置后，请参阅步骤 7 以了解如何设置此平台的部署规则。

配置 iOS 设置

The screenshot shows the XenMobile configuration interface for a Webclip Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Webclip Policy' and includes a description: 'This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.' The configuration is organized into sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', the 'iOS' checkbox is selected. The 'Policy Settings' section includes fields for 'Label*', 'URL*', 'Removable' (set to OFF), 'Icon to be updated' (with a 'Browse' button), 'Precomposed icon' (set to OFF), 'Full screen' (set to OFF), 'Remove policy' (with radio buttons for 'Select date' and 'Duration until removal (in days)'), and 'Allow user to remove policy' (set to 'Always').

配置以下设置：

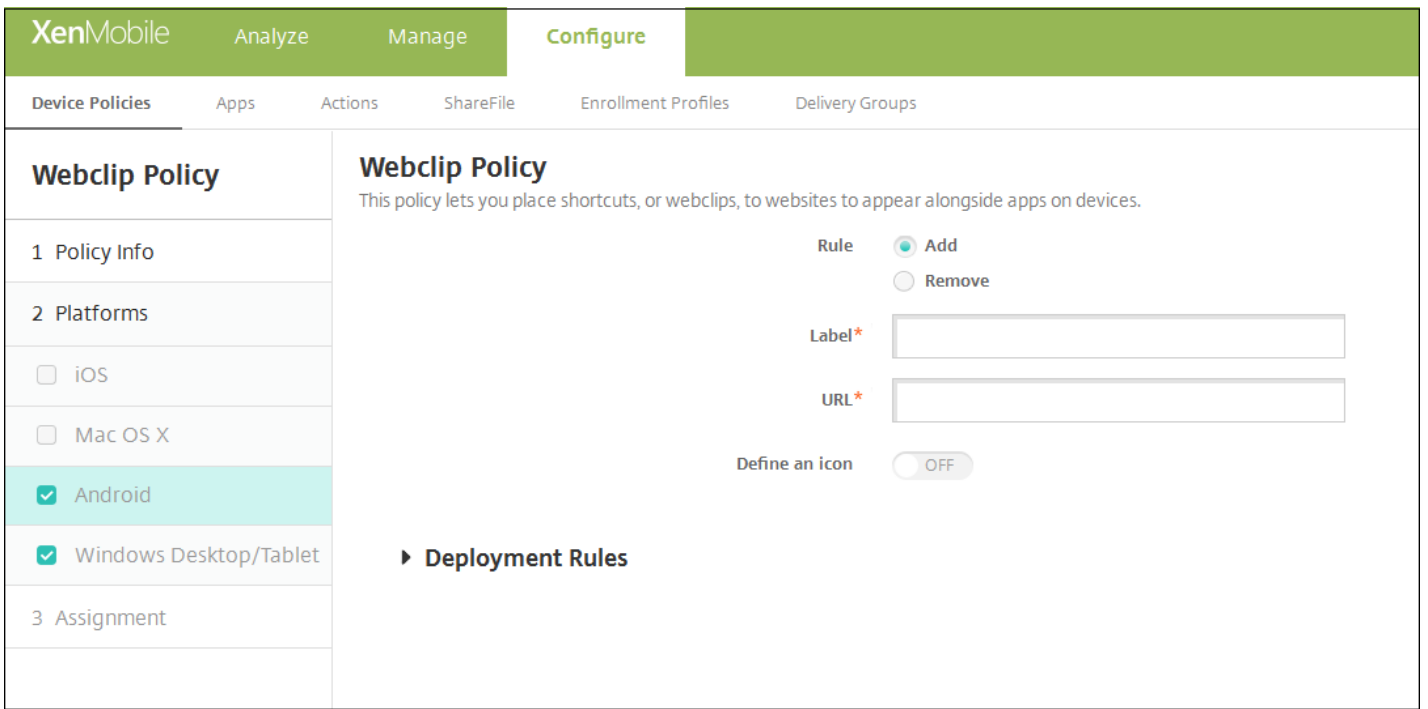
- **标签**：键入随 Web 剪辑一同显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。URL 的开头必须为协议，例如 http://server。
- **可删除**：选择用户是否可以删除 Web 剪辑。默认值为关。
- **待更新的图标**：单击**浏览**，然后导航到文件的位置，选择要用于 Web 剪辑的图标。
- **复合图标**：选择此图标是否应用了某些效果（圆角、阴影和光照反射）。默认设置为关，表示添加效果。
- **全屏**：选择链接的 Web 页面是否以全屏模式打开。默认值为关。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期**或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。

配置 Mac OS X 设置

配置以下设置：

- **标签**：键入随 Web 剪辑一同显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。URL 的开头必须为协议，例如 http://server。
- **待更新的图标**：单击“浏览”，然后导航到文件的位置，选择要用于 Web 剪辑的图标。
- **策略设置**
 - 在**删除策略**旁边，单击**选择日期** 或**删除前保留时间(天)**。
 - 如果单击**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，单击**始终**、**需要密码**或**从不**。
 - 如果单击**需要密码**，在**删除密码**旁边，键入必需的密码。
 - 在**配置文件作用域**列表中，单击**用户**或**系统**。此选项适用于 OS X 10.7 及更高版本。

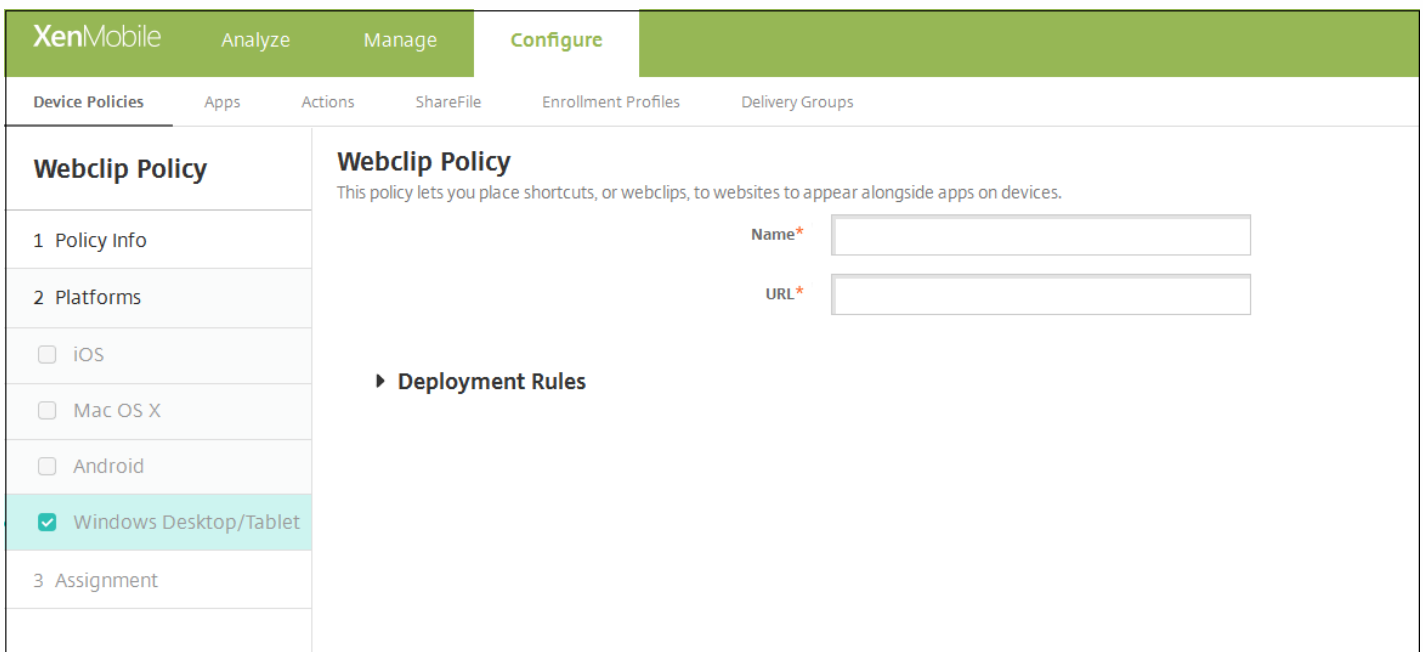
配置 Android 设置



配置以下设置：

- **规则：**选择此策略是添加还是删除 Web 剪辑。默认值为添加。
- **标签：**键入随 Web 剪辑一同显示的标签。
- **URL：**键入与 Web 剪辑关联的 URL。
- **定义图标：**选择是否使用图标文件。默认值为关。
- **图标文件：**如果定义图标设置为开，请单击浏览并导航到要使用的图标文件的位置，选择此文件。

配置 Windows Desktop/Tablet 设置



配置以下设置：

- **名称**：键入随 Web 剪辑一同显示的标签。
- **URL**：键入与 Web 剪辑关联的 URL。

7. 配置部署规则

8. 单击下一步。此时将显示 **Web 剪辑策略分配** 页面。

The screenshot shows the 'Webclip Policy' configuration page in XenMobile. The page is divided into three main sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Windows Desktop/Tablet' is selected. The '3 Assignment' section is currently active, showing a search box for 'Choose delivery groups' and a list of delivery groups with checkboxes. The 'Deployment Schedule' section is partially visible at the bottom.

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

10. 展开部署计划，然后配置以下设置：

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

注意：

- 已在设置 > 服务器属性中配置了计划后台部署密钥的情况下此选项适用。始终启用选项不适用于 iOS 设备。
- 配置的部署计划对所有平台相同。您所做的更改适用于所有平台，为始终启用的连接部署除外，它不适用。

11. 单击保存以保存此策略。

WiFi 设备策略

Apr 24, 2017

通过使用[配置 > 设备策略](#)页面，在 XenMobile 中创建新的 WiFi 设备策略或编辑现有 WiFi 设备策略。借助 WiFi 策略，您可以通过定义以下项目来管理用户将其设备连接到 WiFi 网络的方式：

- 网络名称和类型
- 身份验证和安全策略
- 代理服务器使用
- 与 WiFi 有关的其他详细信息

可以为以下平台的用户配置 WiFi 设置。每种平台需要一组不同的值，本文将对此进行详细介绍。

[iOS 设置](#)

[Mac OS X 设置](#)

[Android 设置](#) (包括为 Android for Work 启用的设备)

[Windows Phone 设置](#)

[Windows Desktop/Tablet 设置](#)

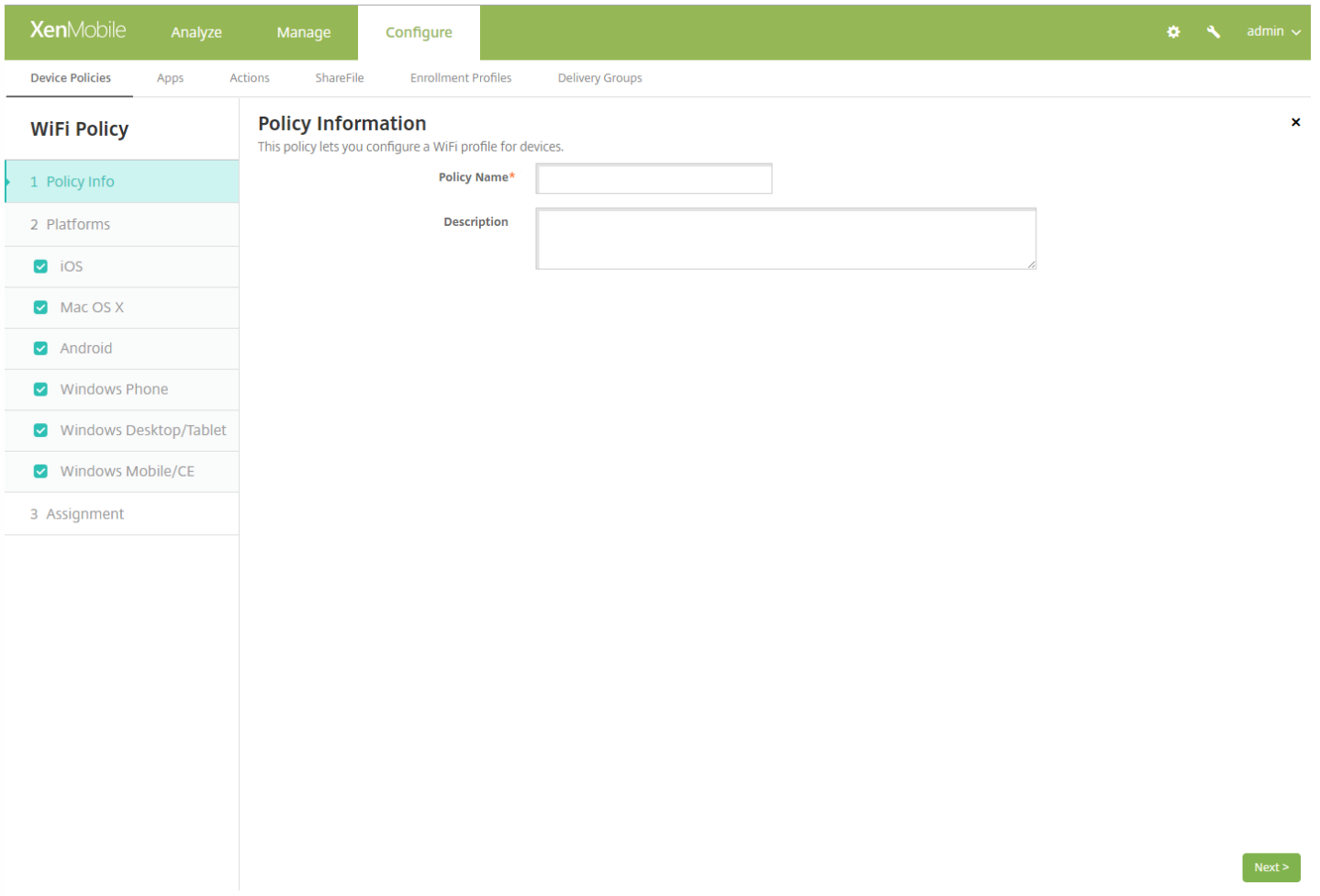
Important

在创建策略之前，请务必完成以下步骤：

- 创建计划使用的任何交付组。
- 了解网络名称和类型。
- 了解计划使用的任何身份验证或安全类型。
- 了解可能需要的任何代理服务器信息。
- 安装所有必需的 CA 证书。
- 具有所有必需共享密钥。
- 为基于证书的身份验证创建 PKI 实体。
- 配置凭据提供程序。

有关详细信息，请参阅[身份验证](#)及文中各节。

1. 在 XenMobile 控制台中，单击[配置 > 设备策略](#)。此时将显示[设备策略](#)页面。
2. 单击[添加](#)。此时将显示[添加新策略](#)对话框。
3. 单击 **WiFi**。此时将显示 **WiFi 策略**页面。



4. 在策略信息窗格中，键入以下信息：

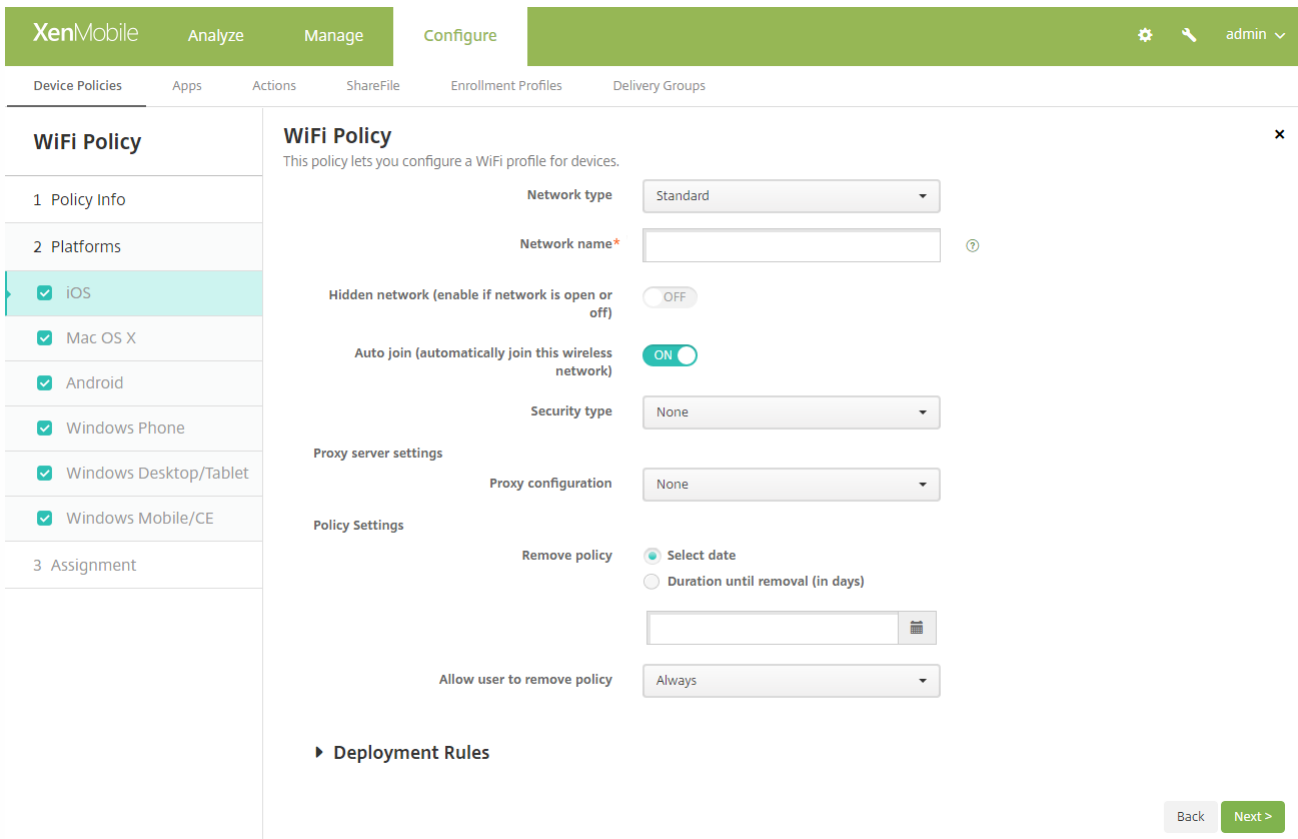
- **策略名称**：键入策略的描述性名称。
- **说明**：（可选）键入策略的说明。

5. 单击下一步。此时将显示平台页面。

6. 在平台下方，选择要添加的平台。如果只为一个平台配置，请取消选中其他平台。

完成对平台设置的配置后，请参阅步骤 7 以设置该平台的部署规则。

配置 iOS 设置



配置以下设置：

- **网络类型**：在列表中，选择**标准**、**传统热点**或**Hotspot 2.0**以设置您计划使用的网络类型。
- **网络名称**：键入显示在设备的可用网络列表中的 SSID。不适用于 **Hotspot 2.0**。
- **隐藏的网络(网络打开或关闭时启用)**：选择是否隐藏网络。
- **自动连接(自动连接此无线网络)**：选择是否自动连接网络。默认值为**开**。
- **安全类型**：在列表中，选择您计划使用的安全类型。不适用于 **Hotspot 2.0**。
 - 无 - 无需进一步配置。
 - WEP
 - WPA/WPA2 Personal
 - 任何(Personal)
 - WEP Enterprise
 - WPA/WPA2 Enterprise：对于最新版本的 Windows 10，需要配置 SCEP 才能使用 WPA-2 Enterprise。XenMobile 之后可以将证书发送到设备以对 WiFi 服务器进行身份验证。要配置 SCEP，请转至**设置 > 凭据提供程序**的“分发”页面。有关详细信息，请参阅**凭据提供程序**。
 - 任何(Enterprise)

以下部分列出了要为上述各个连接类型配置的选项。

WPA、WPA Personal、任何(Personal) ▼

WEP Enterprise、WPA Enterprise、WPA2 Enterprise、任何(Enterprise) ▼

- **代理服务器设置**
 - **代理配置**：在列表中，选择**无**、**手动**或**自动**以设置 VPN 连接通过代理服务器路由的方式，然后配置其他选项。默认值为**无**，选择此项无需进一步配置。
 - 如果选择**手动**，可以配置以下设置：
 - **主机名/IP 地址**：键入代理服务器的主机名或 IP 地址。
 - **端口**：键入代理服务器端口号。
 - **用户名**：键入向代理服务器进行身份验证的可选用户名。
 - **密码**：键入向代理服务器进行身份验证的可选密码。
 - 如果选择**自动**，可以配置以下设置：
 - **服务器 URL**：键入用于定义代理配置的 PAC 文件的 URL。
 - **允许在无法访问 PAC 时直接连接**：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。默认值为**开**。此选项仅适用于 iOS 7.0 及更高版本。
- **策略设置**
 - 在**删除策略**旁边，选择**选择日期**或**删除前保留时间(天)**。
 - 如果选择**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，选择**始终**、**需要密码**或**从不**。
 - 如果选择**需要密码**，在**删除密码**旁边，键入必需的密码。

配置 Mac OS X 设置

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

WiFi Policy

This policy lets you configure a WiFi profile for devices.

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Android
 - Windows Phone
 - Windows Desktop/Tablet
 - Windows Mobile/CE
- 3 Assignment

Network type: Standard

Network name*:

Hidden network (enable if network is open or off): OFF

Auto join (automatically join this wireless network): ON

Security type: None

Proxy server settings

Proxy configuration: None

Policy Settings

Remove policy: Select date Duration until removal (in days)

Allow user to remove policy: Always

Profile scope: User OS X 10.7+

► Deployment Rules

Back Next >

配置以下设置：

- **网络类型**：在列表中，选择**标准**、**传统热点**或**Hotspot 2.0**以设置您计划使用的网络类型。
- **网络名称**：键入显示在设备的可用网络列表中的 SSID。不适用于 **Hotspot 2.0**。
- **隐藏的网络(网络打开或关闭时启用)**：选择是否隐藏网络。
- **自动连接(自动连接此无线网络)**：选择是否自动连接网络。默认值为**开**。
- **安全类型**：在列表中，选择您计划使用的安全类型。不适用于 **Hotspot 2.0**。
 - 无 - 无需进一步配置。
 - WEP
 - WPA/WPA2 Personal
 - 任何(Personal)
 - WEP Enterprise
 - WPA/WPA2 Enterprise
 - 任何(Enterprise)

以下部分列出了要为上述各个连接类型配置的选项。

WPA、WPA Personal、WPA 2 Personal、任何(Personal)

WEP Enterprise、WPA Enterprise、WPA2 Enterprise、任何(Enterprise)

- **用作登录窗口配置**：选择是否使用在登录窗口中输入的同一凭证对用户进行身份验证。
- **代理服务器设置**
 - **代理配置**：在列表中，选择**无**、**手动**或**自动**以设置 VPN 连接通过代理服务器路由的方式，然后配置其他选项。默认值为**无**，选择此项无需进一步配置。
 - 如果选择**手动**，可以配置以下设置：
 - **主机名/IP 地址**：键入代理服务器的主机名或 IP 地址。
 - **端口**：键入代理服务器端口号。
 - **用户名**：键入向代理服务器进行身份验证的可选用户名。
 - **密码**：键入向代理服务器进行身份验证的可选密码。
 - 如果选择**自动**，可以配置以下设置：
 - **服务器 URL**：键入用于定义代理配置的 PAC 文件的 URL。
 - **允许在无法访问 PAC 时直接连接**：选择是否允许用户在无法访问 PAC 文件时直接连接到目标位置。默认值为**开**。此选项仅适用于 iOS 7.0 及更高版本。
- **策略设置**
 - 在**删除策略**旁边，选择**选择日期**或**删除前保留时间(天)**。
 - 如果选择**选择日期**，请单击日历以选择具体删除日期。
 - 在**允许用户删除策略**列表中，选择**始终**、**需要密码**或**从不**。
 - 如果选择**需要密码**，在**删除密码**旁边，键入必需的密码。
 - 在**配置文件作用域**旁边，选择**用户**或**系统**。默认值为**用户**。此选项仅适用于 OS X 10.7 及更高版本。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network name*

Authentication Open

Encryption WEP

Password*

Hidden network (enable if network is open or off) OFF

► **Deployment Rules**

Back **Next >**

配置以下设置：

- **网络名称**：键入在用户设备上的可用网络列表中的 SSID。
- **身份验证**：在列表中，选择用于 WiFi 连接的安全类型。
 - 开放
 - 共享虚拟机
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK
 - 802.1x EAP

以下部分列出了要为上述各个连接类型配置的选项。

打开，共享

WPA、WPA-PSK、WPA2、WPA2-PSK

802.1x

- **隐藏的网络(网络打开或关闭时启用)**：选择是否隐藏网络。

配置 Windows Phone 设置

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

WiFi Policy

This policy lets you configure a WiFi profile for devices.

- 1 Policy Info
- 2 Platforms
 - iOS
 - Mac OS X
 - Android
 - Windows Phone
 - Windows Desktop/Tablet
 - Windows Mobile/CE
- 3 Assignment

Network name* ⓘ

Authentication

Encryption

EAP Type

Connect if hidden OFF

Connect automatically ON

Push certificate via SCEP ON

Credential provider for SCEP*

Proxy server settings

Host name or IP address

Port

配置以下设置：

- **网络名称**：键入在用户设备上的可用网络列表中的 SSID。
- **身份验证**：在列表中，选择用于 WiFi 连接的安全类型。
 - 开放
 - WPA Personal
 - WPA-2 Personal
 - WPA-2 Enterprise：对于最新版本的 Windows 10，需要配置 SCEP 才能使用 WPA-2 Enterprise。通过 SCEP 配置，XenMobile 可以将证书发送到设备以对 WiFi 服务器进行身份验证。要配置 SCEP，请转至 [设置 > 凭据提供程序的分发](#) 页面。有关详细信息，请参阅 [凭据提供程序](#)。

以下部分列出了要为上述各个连接类型配置的选项。

- 开放
- WPA Personal、WPA-2 Personal
- WPA-2 Enterprise
- **代理服务器设置**
 - **主机名或 IP 地址**：键入代理服务器的名称或 IP 地址。
 - **端口**：键入代理服务器的端口号。

配置 Windows Desktop/Tablet 设置

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

WiFi Policy

This policy lets you configure a WiFi profile for devices.

1 Policy Info	OS version* 10
2 Platforms	Network name* WiFi_24G
<input type="checkbox"/> iOS	Authentication WPA-2 Enterprise
<input type="checkbox"/> Mac OS X	Encryption AES
<input type="checkbox"/> Android	EAP Type PEAP-MSCHAPv2
<input checked="" type="checkbox"/> Windows Phone	Hidden network (enable if network is open or off) OFF
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Connect automatically ON
<input type="checkbox"/> Windows Mobile/CE	Enable SCEP? ON
3 Assignment	Credential provider for SCEP* certsrv-cpwifi
	Proxy server settings
	Host name or IP address
	Port

配置以下设置：

Windows 10 设置

- **身份验证**：在列表中，单击用于 WiFi 连接的安全类型。
 - 开放
 - WPA Personal
 - WPA-2 Personal
 - WPA Enterprise
 - WPA-2 Enterprise：对于最新版本的 Windows 10，需要配置 SCEP 才能使用 WPA-2 Enterprise。通过 SCEP 配置，XenMobile 可以将证书发送到设备以对 WiFi 服务器进行身份验证。要配置 SCEP，请转至 [设置 > 凭据提供程序的分发](#) 页面。有关详细信息，请参阅 [凭据提供程序](#)。

以下部分列出了要为上述各个连接类型配置的选项。

开放	▼
WPA Personal、WPA-2 Personal	▼
WPA-2 Enterprise	▼

配置 Windows Mobile/CE

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

WiFi Policy

This policy lets you configure a WiFi profile for devices.

1 Policy Info

- iOS
- Mac OS X
- Android
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

2 Platforms

3 Assignment

WiFi Policy

Network name*

Device-to-device connection (ad-hoc) OFF

Network

Authentication

Encryption

Key provided (automatic) OFF

Password

Key index

► Deployment Rules

Back Next >

配置以下设置：

- **网络名称**：键入在用户设备上的可用网络列表中的 SSID。
- **设备到设备连接(临时)**：允许两个设备直接连接。默认值为关。
- **网络**：选择设备是连接到外部 Internet 来源还是官方 Intranet。
- **身份验证**：在列表中，选择用于 WiFi 连接的安全类型。
 - 开放
 - WPA Personal
 - WPA-2 Personal
 - WPA-2 Enterprise

以下部分列出了要为上述各个连接类型配置的选项。

开放

WPA Personal、WPA-2 Personal

WPA-2 Enterprise

- **提供的密钥(自动)**：选择是否自动提供密钥。默认值为关。
- **密码**：在此字段中键入密码。
- **密钥索引**：选择密钥索引。可用选项包括 1、2、3 和 4。

7. 配置部署规则

8. 单击下一步。此时将显示 **WiFi 策略 分配** 页面。

8. 单击下一步。此时将显示 WiFi 策略分配页面。

8. 单击下一步。此时将显示 WiFi 策略分配页面。

8. 单击下一步。此时将显示 WiFi 策略分配页面。

The screenshot shows the XenMobile configuration page for a WiFi Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows the 'WiFi Policy' configuration steps: 1 Policy Info, 2 Platforms, 3 Assignment (highlighted), and 4 Deployment Schedule. The main content area is titled 'WiFi Policy' and contains a search bar for delivery groups, a list of selected groups (AllUsers, DG-ex12, DG-Testprise), and a 'Deployment Schedule' section. At the bottom right, there are 'Back' and 'Save' buttons.

9. 在**选择交付组**旁边，键入以查找交付组或者选择一个或多个组。选择的组显示在**用于接收应用程序分配的交付组**列表中。

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**。
- 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**。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Windows CE Certificate Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

Policy Information

This configuration allows you to create and deliver a certificate from an External PKI to your device. ✕

Policy Name*

Description

Next >

-
-

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Windows CE Certificate Policy ✕

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

Policy Information

This configuration allows you to create and deliver a certificate from an External PKI to your device.

Credential Provider*

Password of generated PKCS#12*

Destination folder

Destination file name* ?

▶ **Deployment Rules**

-
-
-
-
-
-
-
-
-
-

7. 配置部署规则 ▾

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

Windows CE Certificate Policy

This configuration allows you to create and deliver a certificate from an External PKI to your device. ✕

Choose delivery groups

Type to search

- AllUsers
- sales

Delivery groups to receive app assignment

AllUsers

► **Deployment Schedule** ?

-
-
-
-
-

-
-

The screenshot shows the XenMobile web interface. At the top, there is a navigation bar with 'XenMobile' on the left and 'Analyze', 'Manage', and 'Configure' in the center. On the right of the navigation bar are icons for settings, search, and a user profile labeled 'admin'. Below the navigation bar, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'XenMobile Options Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is currently selected and highlighted in light blue. It contains two sub-sections: 'Policy Name*' with an empty text input field, and 'Description' with an empty text area. Below the 'Description' field is a green 'Next >' button. The main content area also has a sub-header 'Policy Information' with a sub-description: 'This policy lets you configure parameters for connections to XenMobile.'

-
-

配置 Android 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

XenMobile Options Policy

- 1 Policy Info
- 2 Platforms
 - Android
 - Windows Mobile/CE
- 3 Assignment

XenMobile Options Policy ✕

This policy lets you configure parameters for connections to XenMobile.

Device agent configuration

Traybar notification - hide traybar icon OFF

Connection time-out(s)*

Keep-alive interval(s)*

Remote support

Prompt the user before allowing remote control OFF

Before a file transfer

▶ Deployment Rules

-
-
-
-
-

配置 Windows Mobile/CE 设置



XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

XenMobile Options Policy

This policy lets you configure parameters for connections to XenMobile.

Choose delivery groups

Type to search

- AllUsers
- sales

Delivery groups to receive app assignment

AllUsers

► **Deployment Schedule** ⓘ

XenMobile Options Policy

- 1 Policy Info
- 2 Platforms
 - Android
 - Windows Mobile/CE
- 3 Assignment

-
-
-
-
-

-
-

The screenshot shows the XenMobile web interface in the 'Configure' section. The main heading is 'XenMobile Uninstall Policy'. A left-hand navigation pane lists three steps: '1 Policy Info' (highlighted), '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' and 'Windows Mobile/CE' are both checked. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you choose to uninstall XenMobile on Android, Windows Mobile, and Windows CE devices upon deployment of the policy.' Below this, there are two input fields: 'Policy Name*' (a single-line text box) and 'Description' (a multi-line text area). A 'Next >' button is located in the bottom right corner of the main content area. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', 'Configure', and a user profile 'admin'.

-
-

配置 Android 和 Windows Mobile/CE 设置

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

XenMobile Uninstall Policy

- 1 Policy Info
- 2 Platforms
- 3 Assignment

Policy Information

This policy lets you choose to uninstall XenMobile on Android, Windows Mobile, and Windows CE devices upon deployment of the policy.

Uninstall XenMobile from devices OFF ⓘ

▶ **Deployment Rules**

Back Next >

7. 配置部署规则 ▾

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

XenMobile Uninstall Policy

- 1 Policy Info
- 2 Platforms
- 3 Assignment

XenMobile Uninstall Policy

This policy lets you choose to uninstall XenMobile on Android, Windows Mobile, and Windows CE devices upon deployment of the policy.

Choose delivery groups

AllUsers
 sales

🔍

Search

Delivery groups to receive app assignment

AllUsers

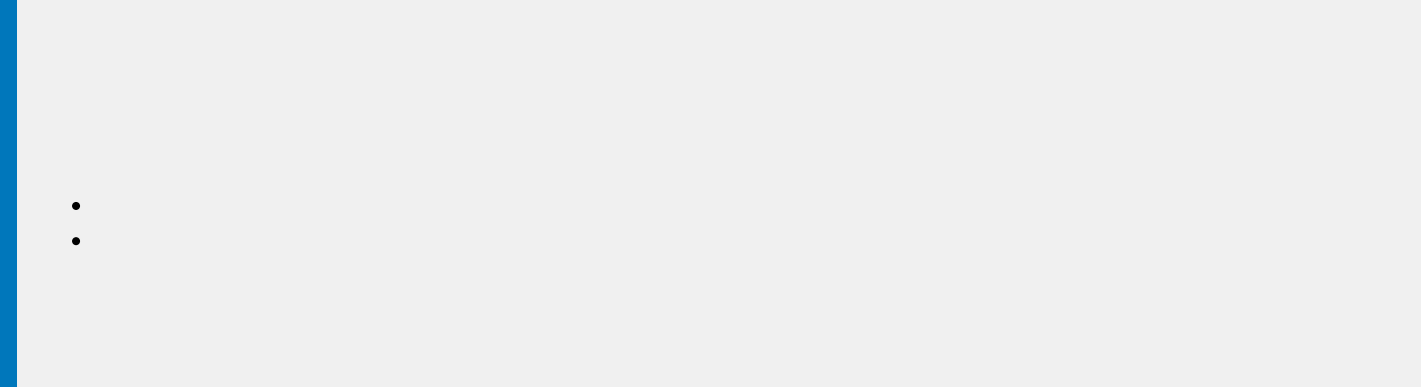
▶ **Deployment Schedule** ⓘ

Back Save

-
-
-
-
-

-
-

-
-
-
-
-



移动应用程序和 MDX 应用程序的工作原理

-
-

Web 和 SaaS 应用程序的工作原理

企业应用程序的工作原理

公共应用商店的工作原理

Web 链接的工作原理

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

Apps [Show filter](#)

[Add](#) | [Category](#) | [Export](#)

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		hh viber	Public App Store	Default	10/18/16 7:55 AM	10/18/16 7:55 AM		
<input type="checkbox"/>		hh ebay	Public App Store	Default	10/18/16 8:04 AM	10/18/16 8:04 AM		
<input type="checkbox"/>		hh green	Enterprise	Default	10/18/16 8:07 AM	10/18/16 8:07 AM		
<input type="checkbox"/>		hh pink	Enterprise	Default	10/18/16 8:08 AM	10/18/16 8:08 AM		
<input type="checkbox"/>		hh web & saas	Web & SaaS	Default	10/18/16 8:09 AM	10/18/16 8:09 AM		
<input type="checkbox"/>		hh weblink	Web Link	Default	10/18/16 8:10 AM	10/18/16 8:10 AM		
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	10/18/16 8:12 AM	10/18/16 8:12 AM		
<input type="checkbox"/>		hh UWH	Enterprise	Default	10/18/16 8:17 AM	10/18/16 8:17 AM		
<input type="checkbox"/>		hh WW	MDX	Default	10/18/16 8:18 AM	10/18/16 8:18 AM		

Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

MDX

1 App Information

2 Platform

iOS

Android

Windows Phone

Windows Desktop/Tablet

3 Approvals (optional)

4 Delivery Group Assignments (optional)

App Information

Name*



Description



App category

All Selected

-
-
-

-

-
-
-
-
-
-
-
-
-
-
-



▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>
<p>Choose File</p>			

Allow app ratings

Allow app comments

-
-
-
-
-

XenMobile Analyze Manage Configure administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

MDX

- 1 App Information
- 2 Platform
 - iOS
 - Android
 - Windows Phone
 - Windows Desktop/Tablet
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

Delivery Group Assignments (optional)

Assign this app to one or more delivery groups.

Choose delivery groups

Type to search Search

- AllUsers
- OA DG for Mac users

Delivery groups to receive app assignment

AllUsers

► Deployment Schedule ⓘ

-
-
-
-
-

-
-

Categories



Add and manage categories in which apps will appear in your Store. After selecting an app or apps in the Apps list, here you can select the categories in which the app(s) appear.

Default

Add new category



-
-

Categories



Add and manage categories in which apps will appear in your Store. After selecting an app or apps in the Apps list, here you can select the categories in which the app(s) appear.

Default

XenMobile Apps

Weblink

Enterprise Apps

Public Store Apps

Add new category



-
-
-
-
-

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

Apps [Show filter](#)

[Add](#) | [Category](#) | [Export](#)

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		hh viber	Public App Store	Default	10/18/16 7:55 AM	10/18/16 7:55 AM		
<input type="checkbox"/>		hh ebay	Public App Store	Default	10/18/16 8:04 AM	10/18/16 8:04 AM		
<input type="checkbox"/>		hh green	Enterprise	Default	10/18/16 8:07 AM	10/18/16 8:07 AM		
<input type="checkbox"/>		hh pink	Enterprise	Default	10/18/16 8:08 AM	10/18/16 8:08 AM		
<input type="checkbox"/>		hh web & saas	Web & SaaS	Default	10/18/16 8:09 AM	10/18/16 8:09 AM		
<input type="checkbox"/>		hh weblink	Web Link	Default	10/18/16 8:10 AM	10/18/16 8:10 AM		
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	10/18/16 8:12 AM	10/18/16 8:12 AM		
<input type="checkbox"/>		hh UWH	Enterprise	Default	10/18/16 8:17 AM	10/18/16 8:17 AM		
<input type="checkbox"/>		hh WW	MDX	Default	10/18/16 8:18 AM	10/18/16 8:18 AM		

Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

-
-
-

XenMobile Analyze Manage Configure

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Public App Store

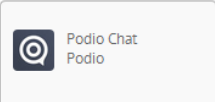
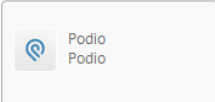
- 1 App Information
- 2 Platform
 - iPhone
 - iPad
 - Google Play
 - Android for Work
 - Windows Desktop/Tablet
 - Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

iPhone App Settings

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

podio

Search results for podio in iPhone apps



Didn't find the app you were looking for?

App Details


Name*

Description*

The ultimate companion app for Podio – enabling you to run your projects and collaborate with your team from anywhere.

Take your content and conversations with you, no matter where your workday takes you.

Version

Image 

Paid app

Remove app if MDM profile is removed

Prevent app data backup

Force app to be managed ⓘ

Force license association to device

[Back](#) [Next >](#)

-
-
-
-
-
-

10. 配置部署规则。



▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings



Allow app
comments



-
-
-
-
-

▼ **Volume Purchase Program**

VPP License Do not use VPP ▼

Do not use VPP

Upload a VPP license file

Public App Store

1 App Information

2 Platform

iPhone

iPad

Google Play

Android for Work

Windows Desktop/Tablet

Windows Phone

3 Approvals (optional)

Android for Work
Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

App Details

Name*

Description*

Version Check for Updates

Image

- ▶ **Deployment Rules**
- ▶ **Store Configuration**
- ▶ **Bulk Purchase**

▼ **Bulk Purchase**

License Assignment

License Usage: 2 of 3

⊗ Disassociate

<input type="checkbox"/>	Associated User
<input checked="" type="checkbox"/>	@.net
<input type="checkbox"/>	

Showing 1 - 2 of 2 items

Add App



Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

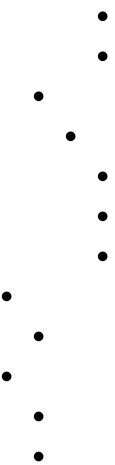
Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.



XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

Web & SaaS

- 1 Web & SaaS App
- 2 Details
- 3 Policies
- 4 Approvals (optional)
- 5 Delivery Group Assignments (optional)

App Information ✕

Add a Web & SaaS app, or choose one from the app index.

App Connector Choose from existing connectors Create a new connector

Name*

Description*

Logon URL*

SAML version 1.1 2.0

Entity ID*

Relay state URL

Name ID format Email Address Unspecified

ACS URL*

Image Use default Upload your own app image



XenMobile Analyze Manage **Configure** ⚙️ 🔑 admin ▾

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

Web & SaaS

- 1 Web & SaaS App
- 2 Details
- 3 Policies
- 4 Approvals (optional)
- 5 Delivery Group Assignments (optional)

App Policy ✕

Fill in app information

Device Security

Block jailbroken or rooted

Network Requirements

WiFi required

Internal network required

Internal WiFi networks

▶ **Store Configuration**

Back Next >

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>
<p>Choose File</p>			

Allow app ratings

Allow app comments

-
-
-
-
-

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

Web & SaaS

- 1 Web & SaaS App
- 2 Details
- 3 Policies
- 4 Approvals (optional)
- 5 Delivery Group Assignments (optional)**

Delivery Group Assignments (optional) ✕

Assign this app to one or more delivery groups.

Choose delivery groups

- AllUsers
- sales

Delivery groups to receive app assignment

AllUsers

► **Deployment Schedule** ⓘ

-
-
-
-
-

-
-

-
-
-
-

-
-
-

Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

<p>MDX</p> <p>Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.</p> <p>Example: WorxMail</p>	<p>Public App Store</p> <p>Free or paid apps available in a public app store, such as iTunes or Google Play, for download.</p> <p>Example: GoToMeeting</p>
<p>Web & SaaS</p> <p>Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.</p> <p>Example: GoogleApps_SAML</p>	<p>Enterprise</p> <p>Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.</p> <p>Example: Quick-iLaunch</p>
<p>Web Link</p> <p>A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.</p>	

Enterprise

1 App Information

2 Platform

iOS

Android

Samsung KNOX

Android for Work

Windows Phone

Windows Desktop/Tablet

Windows Mobile/CE

3 Approvals (optional)

4 Delivery Group Assignments (optional)

App Information

Name*



Description



App category

Default

-
-
-

-
-
-
-
-
-
-
-
-



▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>
<p>Choose File</p>			

Allow app ratings

Allow app comments

MDX

- 1 App Information
- 2 Platform
 - iOS
 - Android
 - Windows Phone
 - Windows Desktop/Tablet
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)**

Delivery Group Assignments (optional)

Assign this app to one or more delivery groups.

Choose delivery groups

Type to search

Search

- AllUsers
- OA DG for Mac users

Delivery groups to receive app assignment

- AllUsers

► Deployment Schedule ⓘ

-
-
-
-
-

-
-

-
-
-

-
-
-

Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

<p>MDX</p> <p>Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.</p> <p>Example: WorxMail</p>	<p>Public App Store</p> <p>Free or paid apps available in a public app store, such as iTunes or Google Play, for download.</p> <p>Example: GoToMeeting</p>
<p>Web & SaaS</p> <p>Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.</p> <p>Example: GoogleApps_SAML</p>	<p>Enterprise</p> <p>Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.</p> <p>Example: Quick-iLaunch</p>
<p>Web Link</p> <p>A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.</p>	

-
-
-
-
-
-
-

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>
<p>Choose File</p>			

Allow app ratings

Allow app
comments

-
-
-

-
-

-
-
-

-
-

-
-



Settings > [Workflows](#)

Workflows


Add

<input type="checkbox"/>	Name	Description	Workflow email template	▾
<input type="checkbox"/>	WF 1		Workflow Approval Request	

Showing 1 - 1 of 1 items

Settings > Workflows > Add Workflow

Add Workflow

Name*

Description

Email Approval Templates

Workflow Approval Request ▾



Levels of manager approval

1 level ▾

Select Active Directory domain

agsag.com ▾

Find additional required approvers



Search

Selected additional required approvers

Cancel

Save

-
-
-

Apps [Show filter](#)

|
 |

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM		
<input type="checkbox"/>		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/10/15 3:13 PM		
<input type="checkbox"/>		worxweb	MDX	Worxapps				
<input type="checkbox"/>		Angrybird	Public App Store	Public				
<input type="checkbox"/>		WorxTasks	MDX	Default				
<input type="checkbox"/>		WorxMail2	MDX	MDX				
<input type="checkbox"/>		WorxNotes-iOS	MDX	MDX				
<input type="checkbox"/>		worxweb2	MDX	MDX				
<input type="checkbox"/>		ShareFile1	MDX	MDX				

|
 |
 |

Deployment

0 Installed	0 Pending	0 Failed
----------------	--------------	-------------

[Show more >](#)

Showing 1 - 9 of 9 items

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM		
<input type="checkbox"/>		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled	

-
-
-

-
-
-

7. 配置部署规则



▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>	<p>Choose File</p>
<p>Choose File</p>			

Allow app ratings

Allow app comments

-
-
-
-
-

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

MDX

1 App Information

2 Platform

iOS

Android

Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Delivery Group Assignments (optional) ✕

Assign this app to one or more delivery groups.

Choose delivery groups

🔍

AllUsers

Cyrus DG

Search

Delivery groups to receive app assignment



AllUsers

▶ **Deployment Schedule** ?

Back
Save

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-

XenMobile Dashboard Manage Configure   Admin ▾

Settings

<p>Certificate Management</p> <hr/> <p>Certificates</p> <hr/> <p>Credential Providers</p> <hr/> <p>PKI Entities</p> <hr/>	<p>Notifications</p> <hr/> <p>Carrier SMS Gateway</p> <hr/> <p>Notification Server</p> <hr/> <p>Notification Templates</p> <hr/>	<p>Server</p> <hr/> <p>ActiveSync Gateway</p> <hr/> <p>Enrollment</p> <hr/> <p>LDAP</p> <hr/> <p>Licensing</p> <hr/> <p>Local Users and Groups</p> <hr/> <p>Mobile Service Provider</p> <hr/> <p>NetScaler Gateway</p> <hr/> <p>Network Access Control</p> <hr/> <p>Release Management</p> <hr/> <p>Role-Based Access Control</p> <hr/> <p>Server Properties</p> <hr/> <p>SysLog</p> <hr/> <p>Workflows</p> <hr/> <p>XenApp/XenDesktop</p> <hr/>	<p>Frequently Accessed</p> <p>Certificates</p> <p>Enrollment</p> <p>Licensing</p> <p>Local Users and Groups</p> <p>Role-Based Access Control</p> <p>Release Management</p>
<p>Client</p> <hr/> <p>Client Branding</p> <hr/> <p>Client Properties</p> <hr/> <p>Client Support</p> <hr/>	<p>Platforms</p> <hr/> <p>Android for Work</p> <hr/> <p>Google Play Credentials</p> <hr/> <p>iOS Bulk Enrollment</p> <hr/> <p>iOS Settings</p> <hr/> <p>Samsung KNOX</p> <hr/>		

Settings > [Client Branding](#)

Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

Store name*



Default store view

 Category A-Z

Device

 Phone Tablet

Branding file

[Browse](#)**Note:**

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
A .zip file should be created from the files, not a folder with the files inside of it.

-
-
-

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Launcher Configuration Policy

- 1 Policy Info
- 2 Platforms
- ✓ Android
- 3 Assignment

Policy Information ✕

This policy lets you define a configuration of an Android device launcher.

Launcher app configuration

Define a logo image ON

Logo image Browse

Define a background image ON

Background image Browse

Allowed apps

App name	Package Name*	
test	test.com	+ Add

Password

▶ **Deployment Rules**

Back
Next >

Add App ×

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

-
-
-

Deployment Order ×

Change the deployment order by dragging the policies, apps and actions into position.

Citrix Launcher

Launcher Configuration

Cancel Save

Settings > [iOS Settings](#)

iOS Settings

Configure these iOS-specific settings. When saved and validated, the Volume Purchase Program (VPP) apps are added to the table on the Apps tab.

Store user password in Secure Hub ⓘ

User property for VPP country mapping

 ⓘ

VPP Accounts



Add

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login	▾
<input type="checkbox"/>	VPP	VPP	CITRIX SYSTEMS, INC.	United States	04/12/2017 02:57:32 pm	TestAccount@outlook.com	

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

Public App Store

- 1 App Information
- 2 Platform
 - iPhone
 - iPad
 - Google Play
 - Android for Work
 - Windows Desktop/Tablet
 - Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

iPhone App Settings


Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

App Details

Name*

Description*

Version Check for Updates

Image 

Paid app

Remove app if MDM profile is removed

Prevent app data backup

Force app to be managed ⓘ

Force license association to device

▶ **Deployment Rules**
 ▶ **Store Configuration**
 ▶ **Volume Purchase Program**

Back
Next >

Public App Store

1 App Information

2 Platform

iPhone

iPad

Google Play

Android for Work

Windows Desktop/Tablet

Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Remove app if MDM profile is removed

Prevent app data backup

Force app to be managed ?

Force license association to device

► Deployment Rules

► Store Configuration

▼ Volume Purchase Program

VPP ID Assignment

Disassociate

License Usage: 2 of 2

<input type="checkbox"/>	License ID	Usage Status	Associated User	Associated Device
<input type="checkbox"/>	82684302	Used		
<input type="checkbox"/>	82684301	Used		F9FMW440FCM5

Showing 1 - 2 of 2 items

VPP License Keys

Import

Manage Con admin

Disassociate VPP license ✕

Are you sure you want to disassociate the selected users with this VPP license ID?

Cancel Disassociate

Force li

- ▶ Deployment Rules
- ▶ Store Configuration
- ▼ Volume Purchase Program
 - VPP License Use VPP company token
 - VPP Account VPP

VPP ID Assignment License Usage: 2 of 2

✕ Disassociate

<input type="checkbox"/>	License ID	Usage Status	Associated User	Associated Device
<input checked="" type="checkbox"/>	82684302	Used		
<input type="checkbox"/>	82684301	Used		F9FMW440FCM5

Showing 1 - 2 of 2 items

VPP License Keys

📄 Import

Device details

- 1 General
- 2 Properties
- 3 User Properties
- 4 Assigned Policies
- 5 Apps
- 6 Actions
- 7 Delivery Groups
- 8 iOS Profiles
- 9 iOS Provisioning Profiles
- 10 Certificates
- 11 Connections
- 12 MDM Status

User Properties

User name user123

Password Enter new password

Role* USER

Membership local\MSP

Manage Groups

VPP Accounts VPP

Retire

Back Next >

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

Public App Store

- 1 App Information
- 2 Platform
 - iPhone
 - iPad
 - Google Play
 - Android for Work
 - Windows Desktop/Tablet
 - Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

iPhone App Settings


Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

App Details

Name*

Description*

Version Check for Updates

Image 

Paid app OFF

Remove app if MDM profile is removed ON

Prevent app data backup ON

Force app to be managed ON ⓘ

Force license association to device ON

▶ **Deployment Rules**
 ▶ **Store Configuration**
 ▶ **Volume Purchase Program**

Back Next >

Settings > [XenApp/XenDesktop](#)

XenApp/XenDesktop

Allows users to add XenApp and XenDesktop through Secure Hub.

Host*

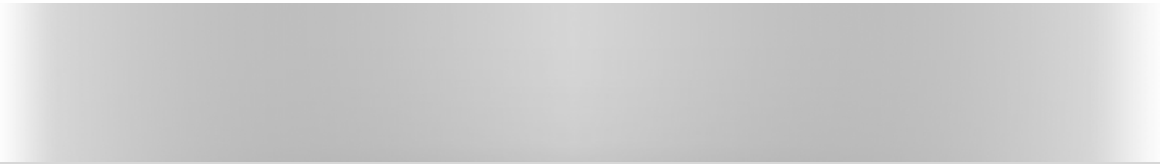
Port*

Relative Path*

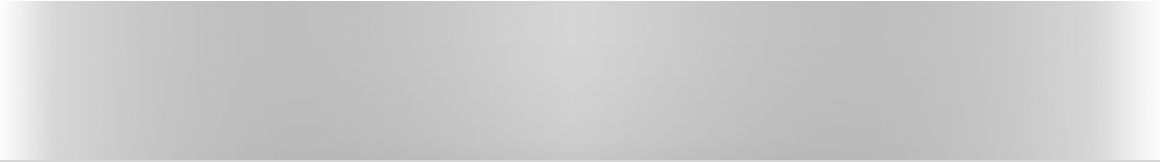
Use HTTPS OFF

✓ Connection succeeded

-
-
-
-



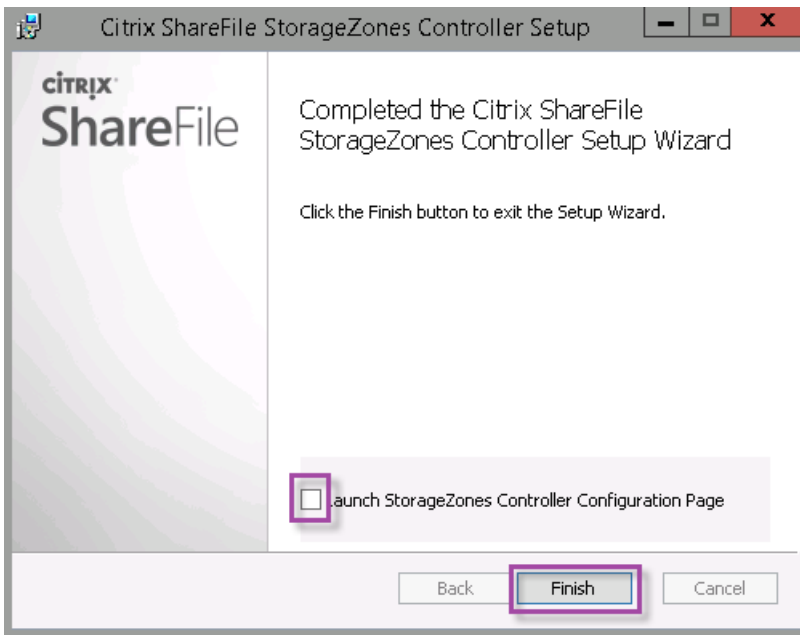
-
-
-



-
-
-
-
-
-
-
-

安装 StorageZones Controller

-
-



准备 StorageZones Controller 以仅与 StorageZone 连接器配合使用

-
-

Windows Sysinternals

Home Learn **Downloads** Community

Windows Sysinternals > Downloads > Process Utilities > PsExec


Utilities

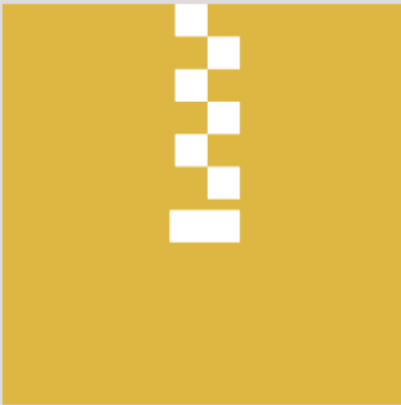
- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities

PsExec v2.11

By Mark Russinovich
Published: May 2, 2014

 [Download PsTools](#)
(1,648 KB)



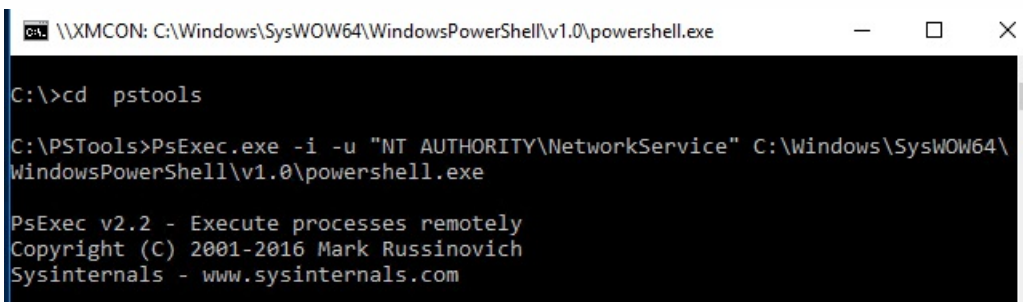
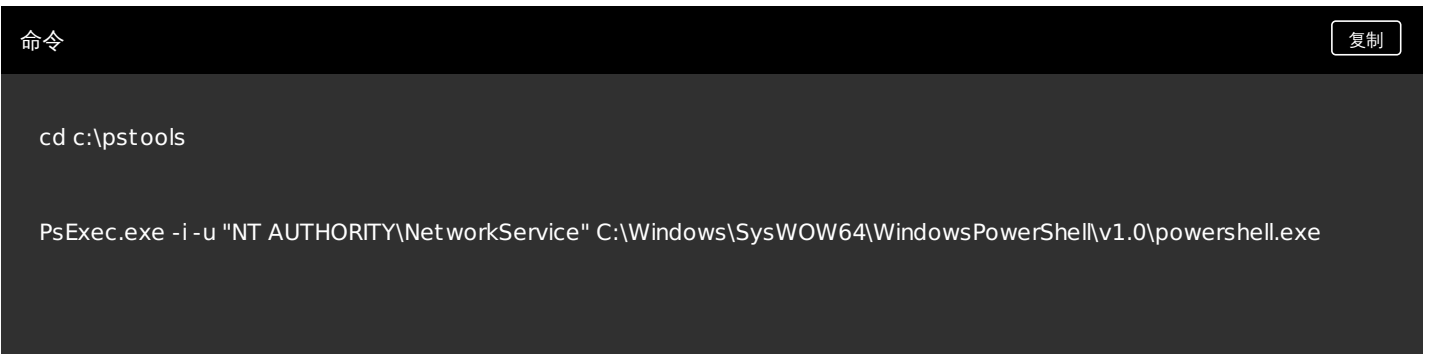
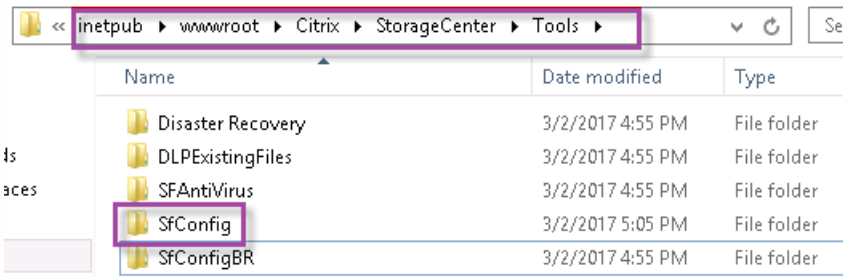
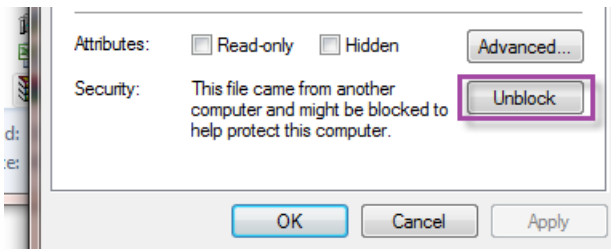
SfConfig.zip

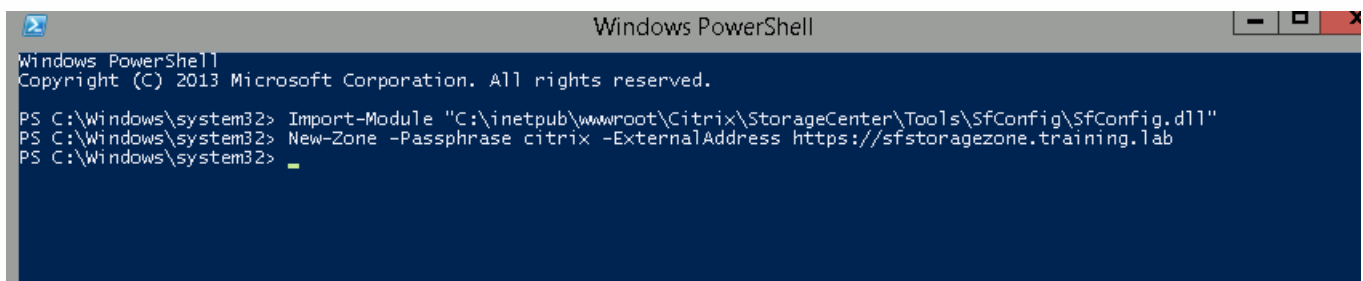
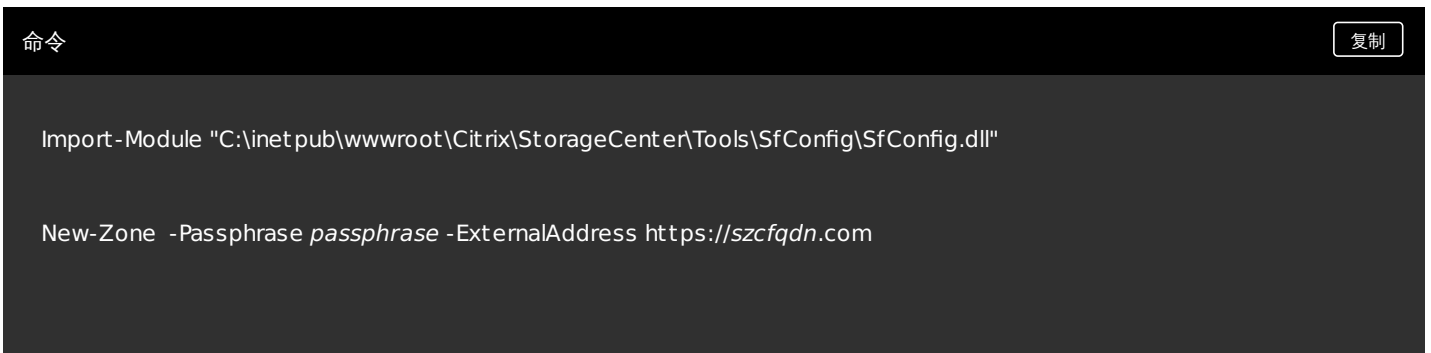
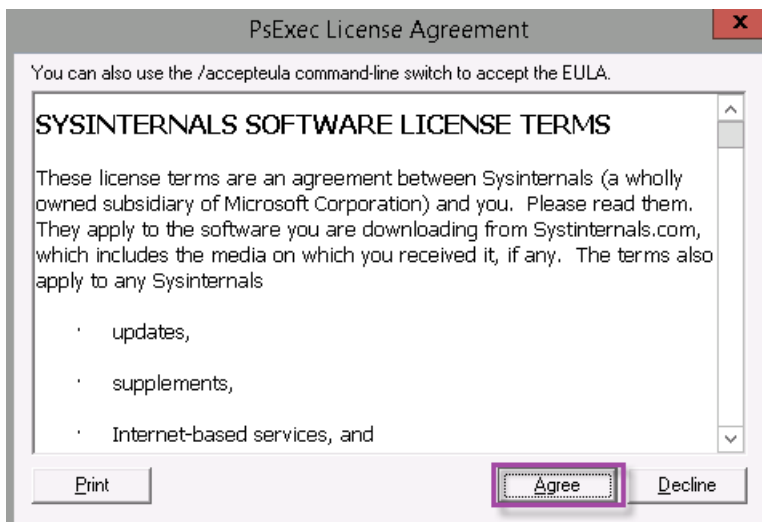
436 KB

Modified: 03/02/2017 12:46PM

Creator: Lenny Soletti

[Download](#)





将辅助 StorageZones Controller 加入 StorageZone

在 XenMobile 中定义 StorageZones 控制器连接

XenMobile Analyze Manage **Configure** ⚙️ 🔑 administrator

Device Policies Apps Actions **ShareFile** Enrollment Profiles Delivery Groups

Choose a method for integrating ShareFile with XenMobile or learn more about which mode to select.

	ShareFile Enterprise	StorageZone Connectors Only
Access network shares and SharePoint data from mobile devices	✓	✓
Edit Microsoft Office documents from mobile devices	✓	✓
Preview and annotate Adobe PDF files from mobile devices	✓	✓
Store data in Citrix-managed or customer-managed StorageZones or both	✓	
Securely share files with people inside and outside the enterprise	✓	
Sync files and data across multiple devices	✓	
Access files through the ShareFile website	✓	
Access Office 365 content and Personal Cloud connectors from mobile devices	✓	
Use auditing and reporting capabilities	✓	

[Configure ShareFile Enterprise](#) [Configure Connectors](#)

XenMobile Analyze Manage **Configure** ⚙️ 🔑 administrator

Device Policies Apps Actions **ShareFile** Enrollment Profiles Delivery Groups

StorageZone Connectors Show filter

🔍

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

[Add](#) | [Manage StorageZones](#)

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
					▼

XenMobile Analyze Manage **Configure** ⚙️ 🔍 administrator ▾

Device Policies Apps Actions **ShareFile** Enrollment Profiles Delivery Groups

StorageZone Connectors ▾ Show filter

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

➕ Add 📁 Manage StorageZones

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
--------------------------	----------------	------	-------------	----------	-----------------

Manage StorageZones ✕

[Add New](#)

Name*

FQDN*

Port*

Secure Connection ON

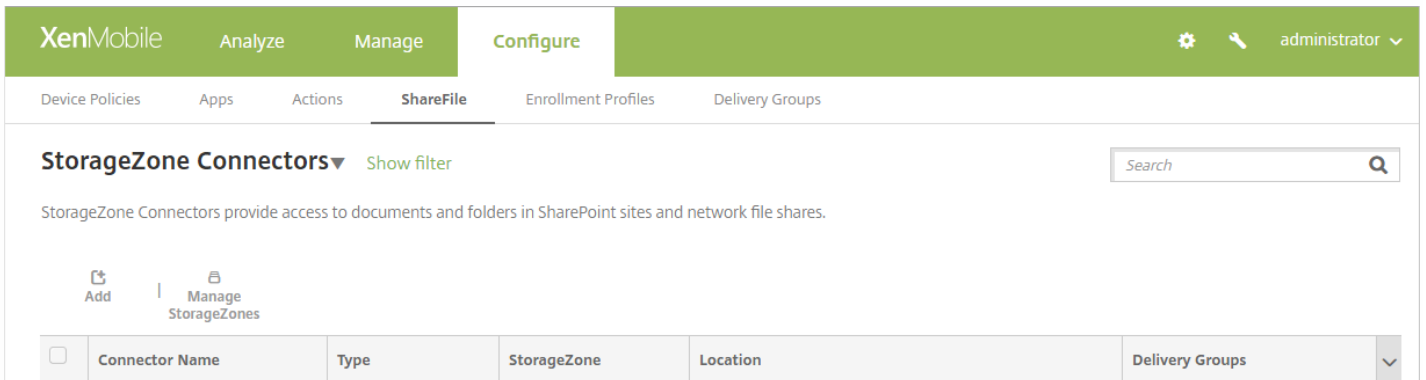
Administrator user na...*

Administrator passw...* 👁️

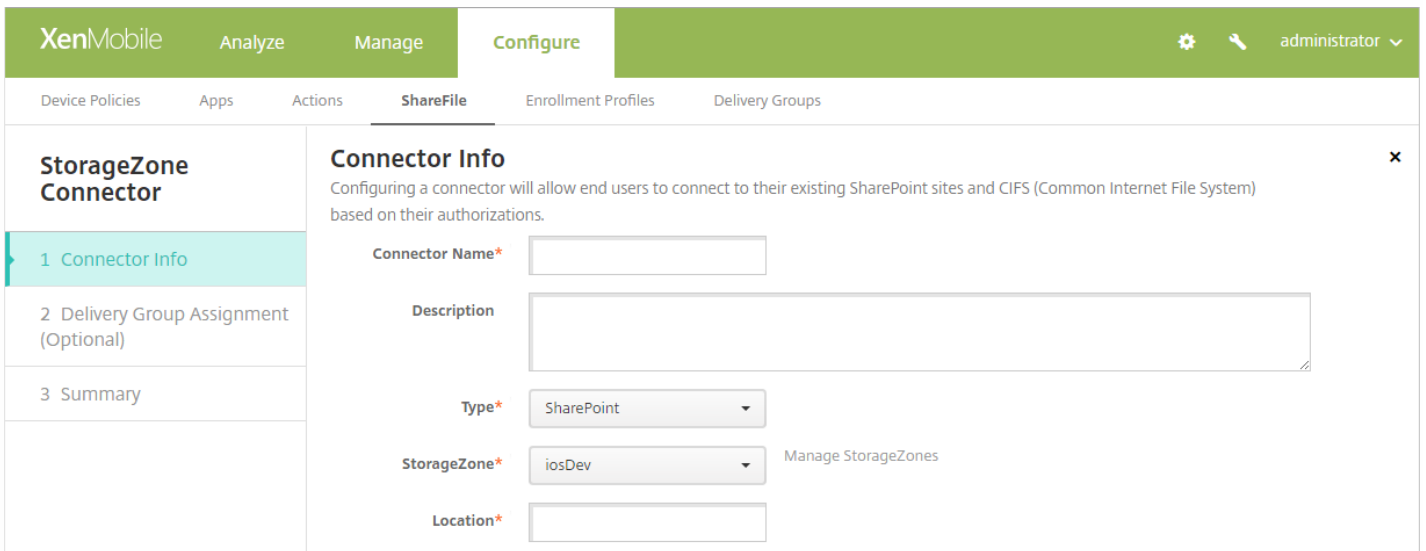
➕ Add Cancel Save

-
-
-
-

在 XenMobile 中添加 StorageZone 连接器



The screenshot shows the XenMobile Configure page. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, with sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'ShareFile' tab is selected. Below the navigation, there is a 'StorageZone Connectors' section with a 'Show filter' link and a search box. A description states: 'StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.' Below this, there are two buttons: 'Add' and 'Manage StorageZones'. At the bottom, a table header is visible with columns: Connector Name, Type, StorageZone, Location, and Delivery Groups.



The screenshot shows the 'Connector Info' configuration form. The top navigation bar is the same as the previous screenshot. The 'StorageZone Connector' section is expanded, showing a sidebar with three steps: '1 Connector Info', '2 Delivery Group Assignment (Optional)', and '3 Summary'. The 'Connector Info' step is active. The form includes the following fields:

- Connector Name***: A text input field.
- Description**: A large text area for optional description.
- Type***: A dropdown menu currently set to 'SharePoint'.
- StorageZone***: A dropdown menu currently set to 'iosDev', with a 'Manage StorageZones' link next to it.
- Location***: A text input field.

-
-
-
-
-

StorageZone Connector

1 Connector Info

2 Delivery Group Assignment (Optional)

3 Summary

Delivery Group Assignment

Configure a connector to allow users to connect to existing SharePoint sites or network file shares based on their authorizations.

Assign to delivery groups

Type to search




Search


- AllUsers
- XM5-users
- dg-test

Selected delivery groups

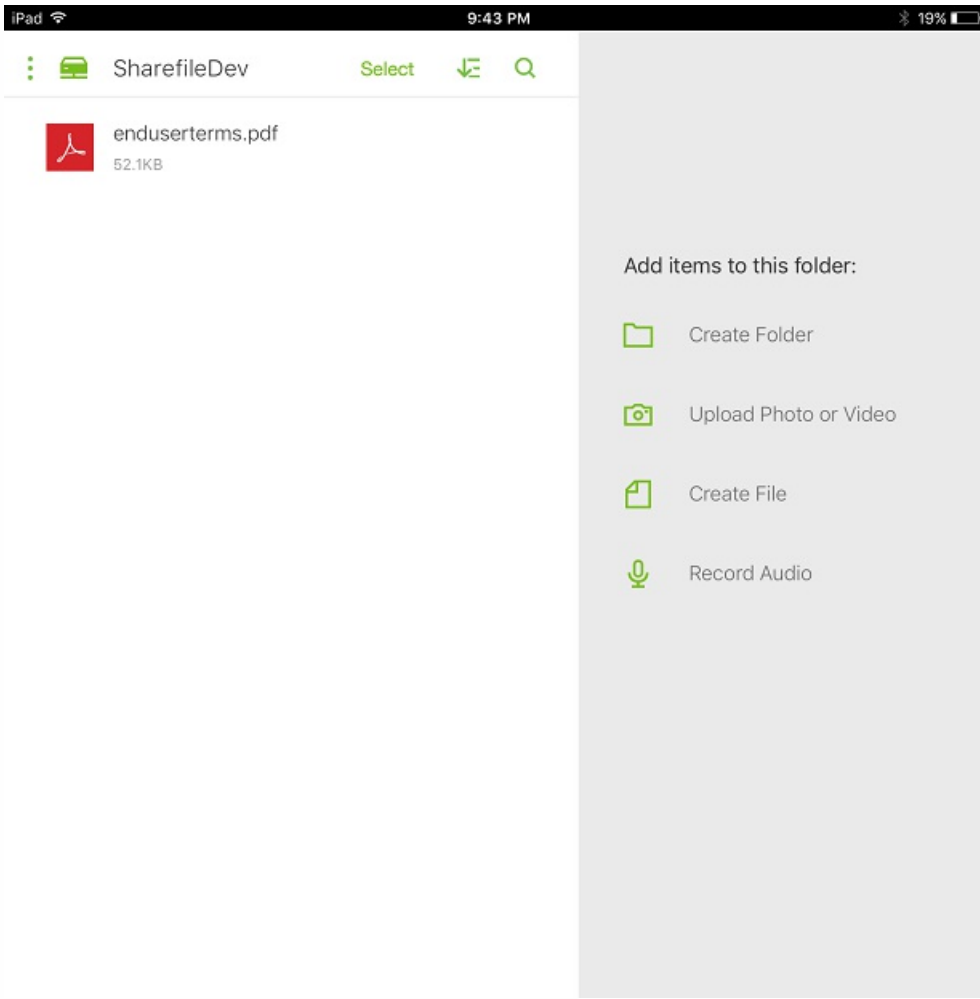
XM5-users



-  Dashboard
-  SharefileDev

-  Queue
-  Settings





过滤 StorageZone 连接器列表

The screenshot shows the XenMobile 'Configure' page. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section has tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'ShareFile' tab is active, showing 'StorageZone Connectors'. A 'Show filter' button is highlighted with a purple box. Below the title, there is a search bar and a description: 'StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.' There are 'Add' and 'Manage StorageZones' buttons. A table lists two connectors:

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
<input type="checkbox"/>	TestNS	NetworkFile	iosDev	\\Kylec-az-sz2\DevTestSZ	XM5-users
<input type="checkbox"/>	TestSP	Sharepoint	iosDev	http://sf-az-sp2013.sfazure.com:80	XM5-users,AllUsers

Showing 1 - 2 of 2 items

Filters Clear All

- Type Clear
 - NetworkFile 2
 - Sharepoint 1
- Assigned Delivery Groups Clear
- StorageZone Clear

StorageZone Connectors Hide filter

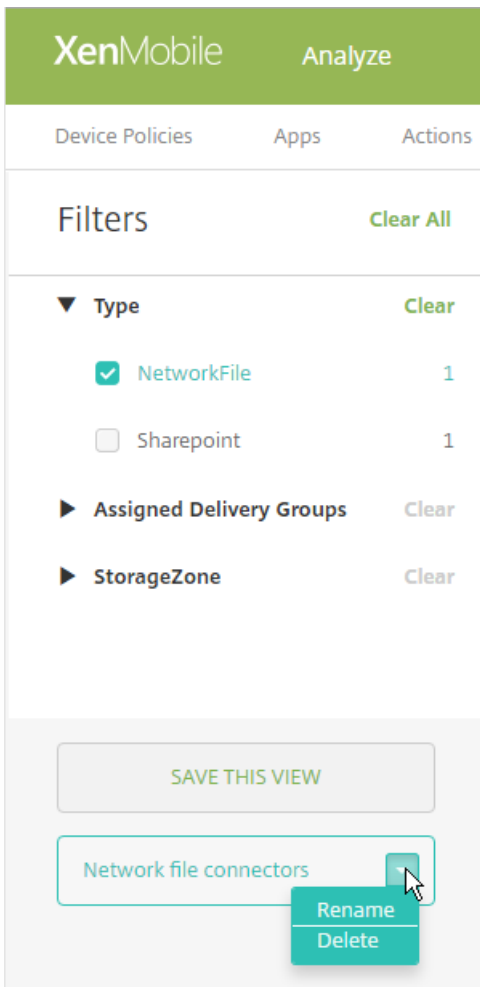
StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

|

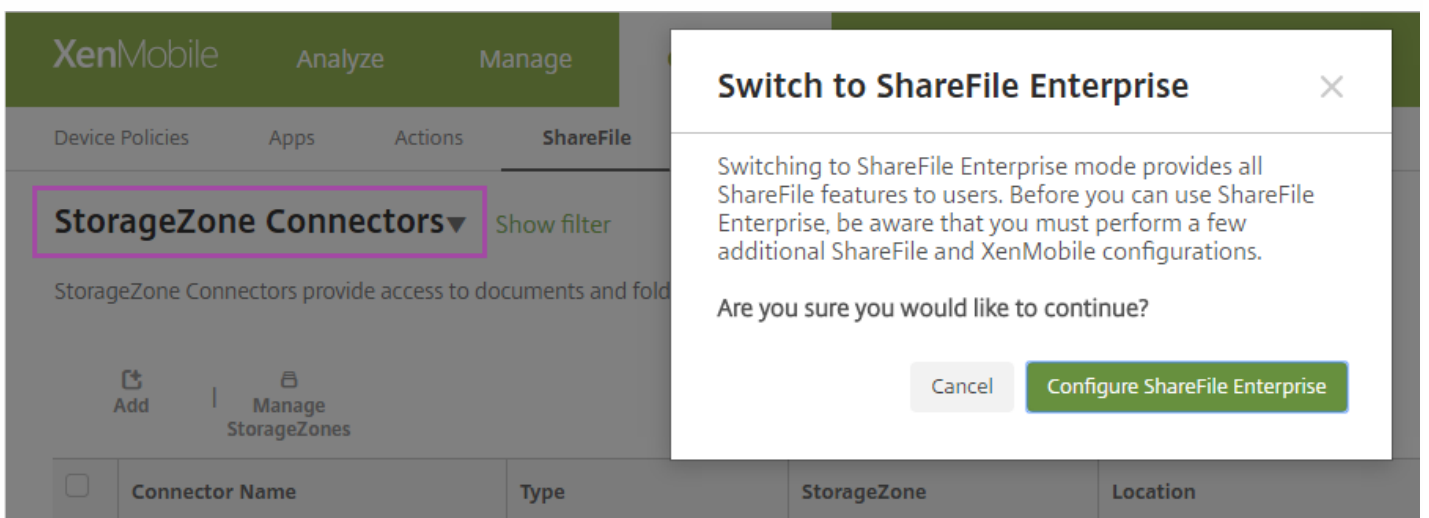
<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
<input type="checkbox"/>	TestNS	NetworkFile	sz2	\\sz2\Storagezone	XM5-users
<input type="checkbox"/>	testxm	NetworkFile	sz1	\\sz1\Storagezone	XM5-users

Showing 1 - 2 of 2 items

SAVE THIS VIEW



切换到 ShareFile Enterprise






-
-
-
-
-
-
-


从 XenMobile 服务器中导出 SAML 证书

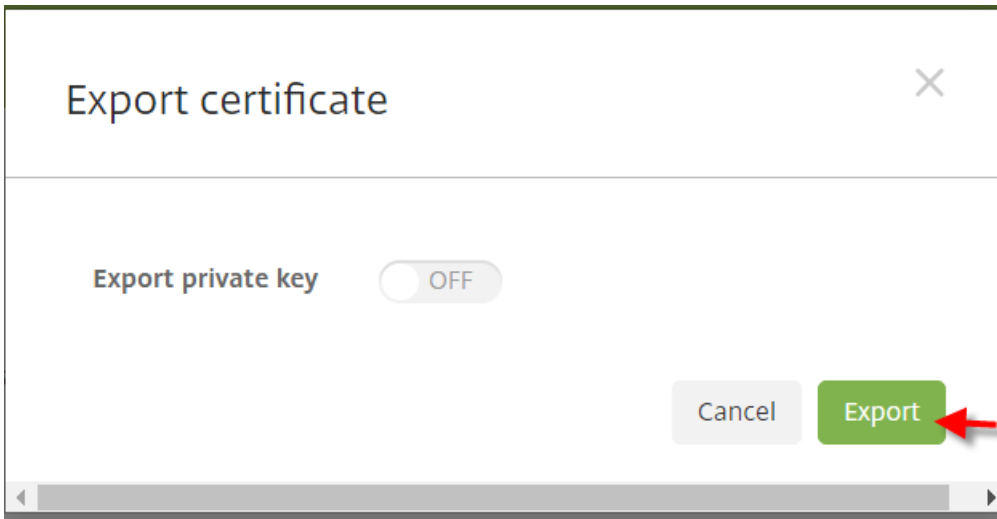
Settings > Certificates

Certificates

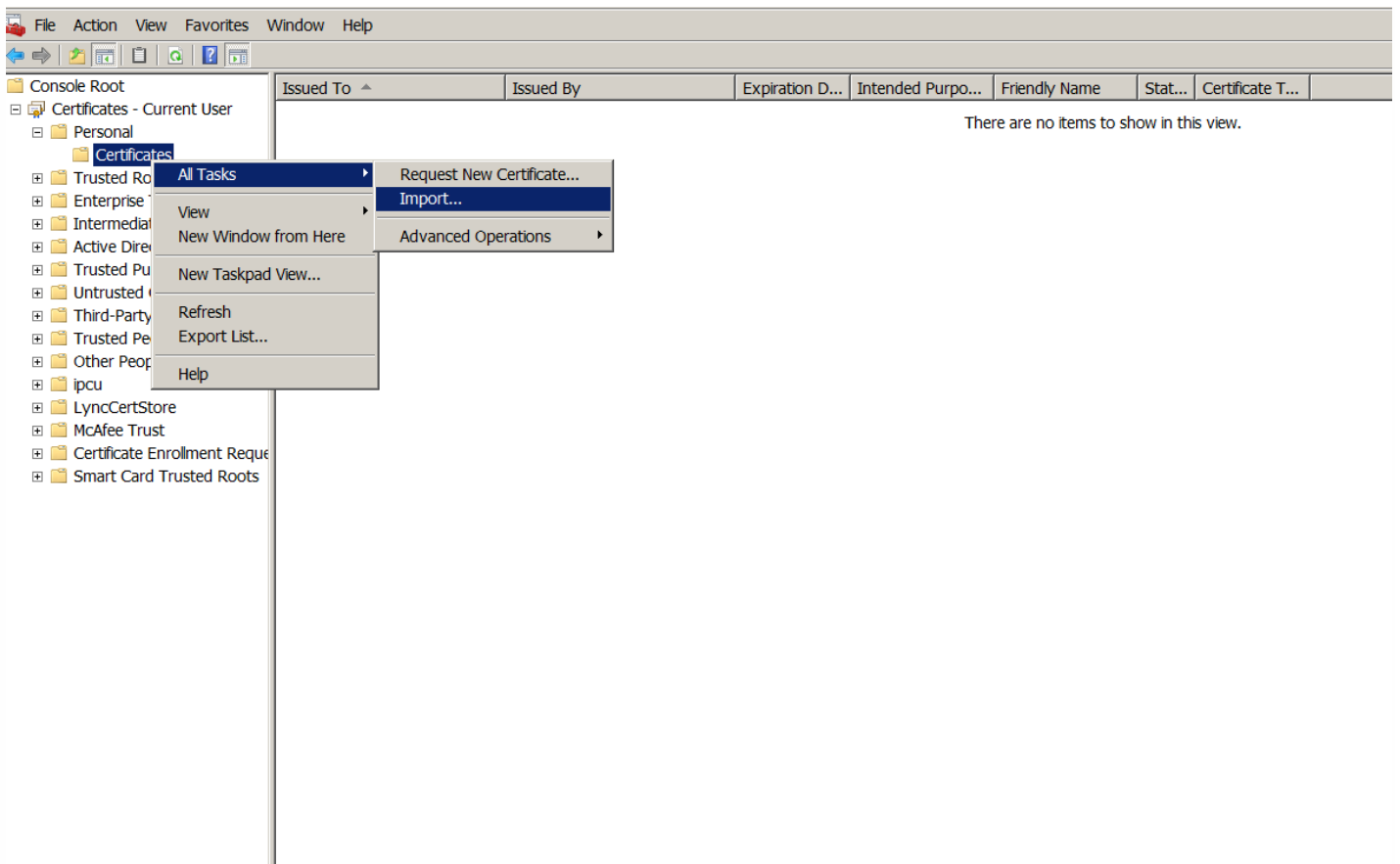
You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

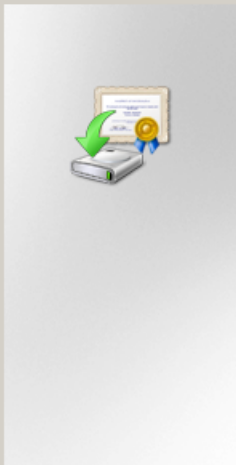
 |
  |
  |
 

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input checked="" type="checkbox"/>	XMS.example.com 	Self Signed/Generated	Up to date	2016-05-23	2026-05-21	SAML	✓
<input type="checkbox"/>	*.mpg.citrix.com		Up to date	2016-04-20	2017-05-27	SSL Listener	✓
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2016-05-23	2036-05-21	Devices CA	
<input type="checkbox"/>	Verizon Public SureServer CA G14-SHA2		Up to date	2014-04-09	2021-04-09	Root or intermediate	
<input type="checkbox"/>	Baltimore CyberTrust Root		Up to date	2000-05-12	2025-05-12	Root or intermediate	



将证书从 PEM 转换为 CER





Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

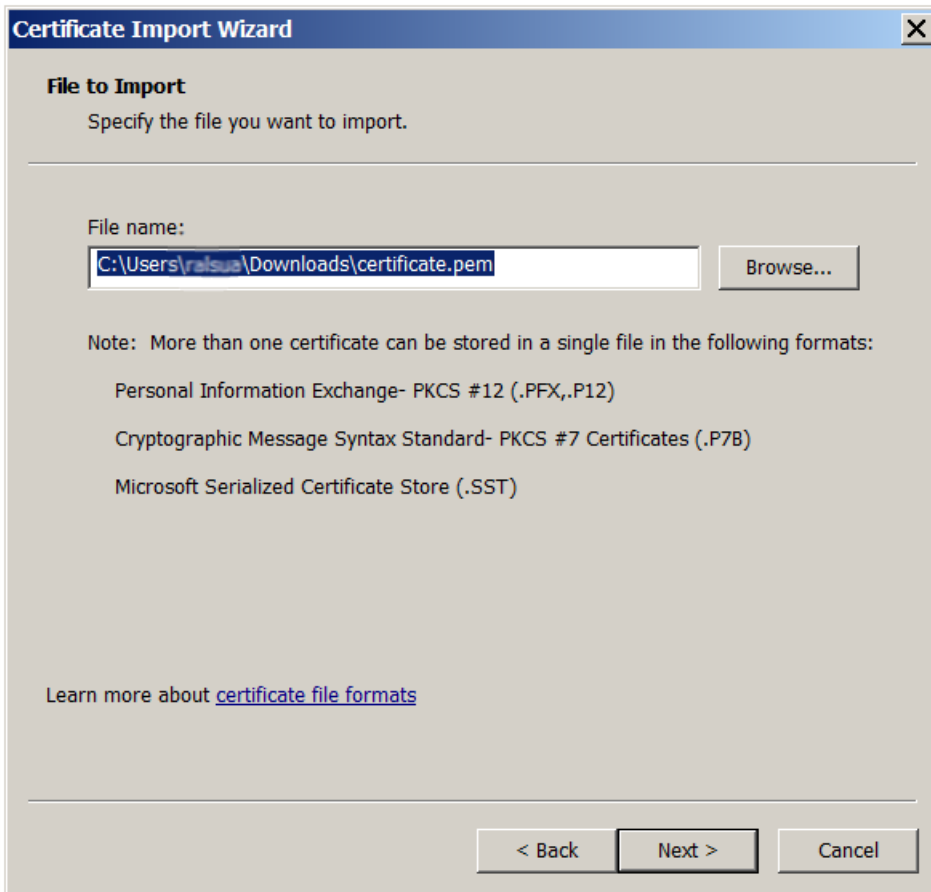
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

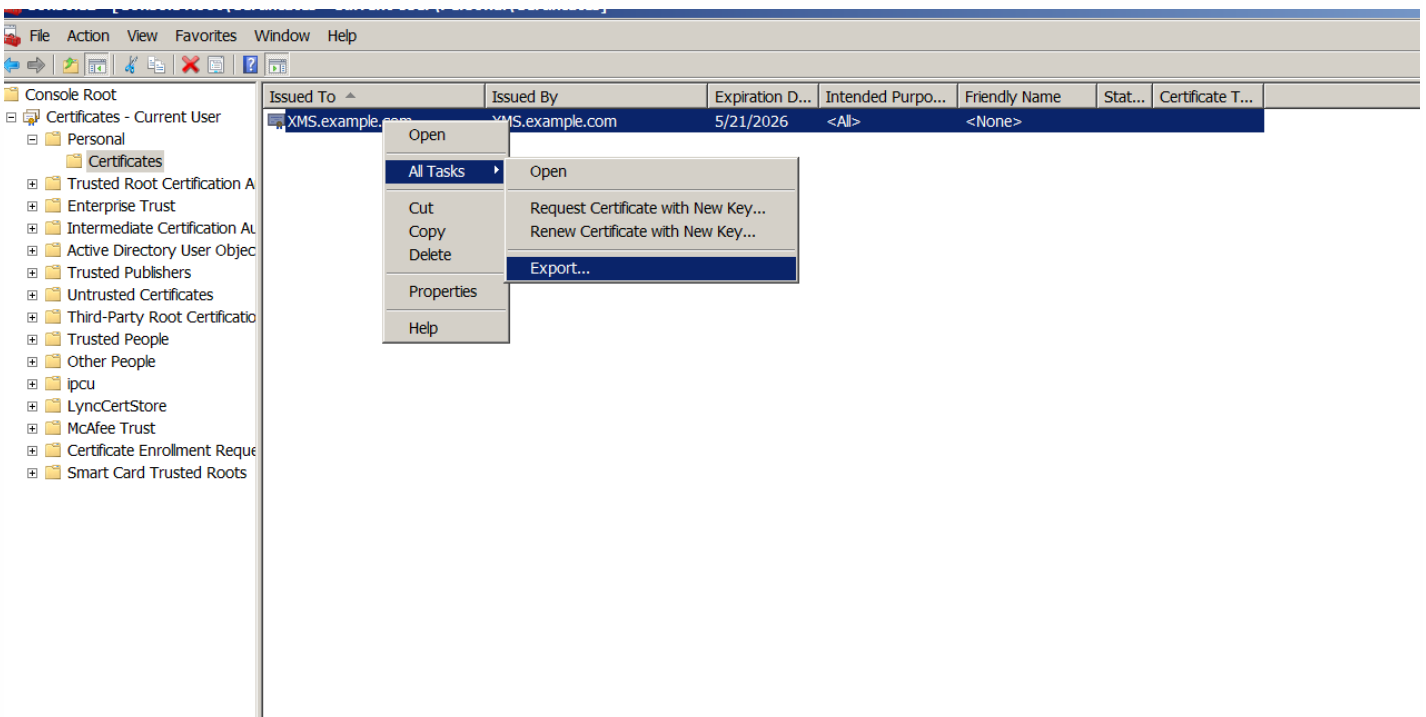
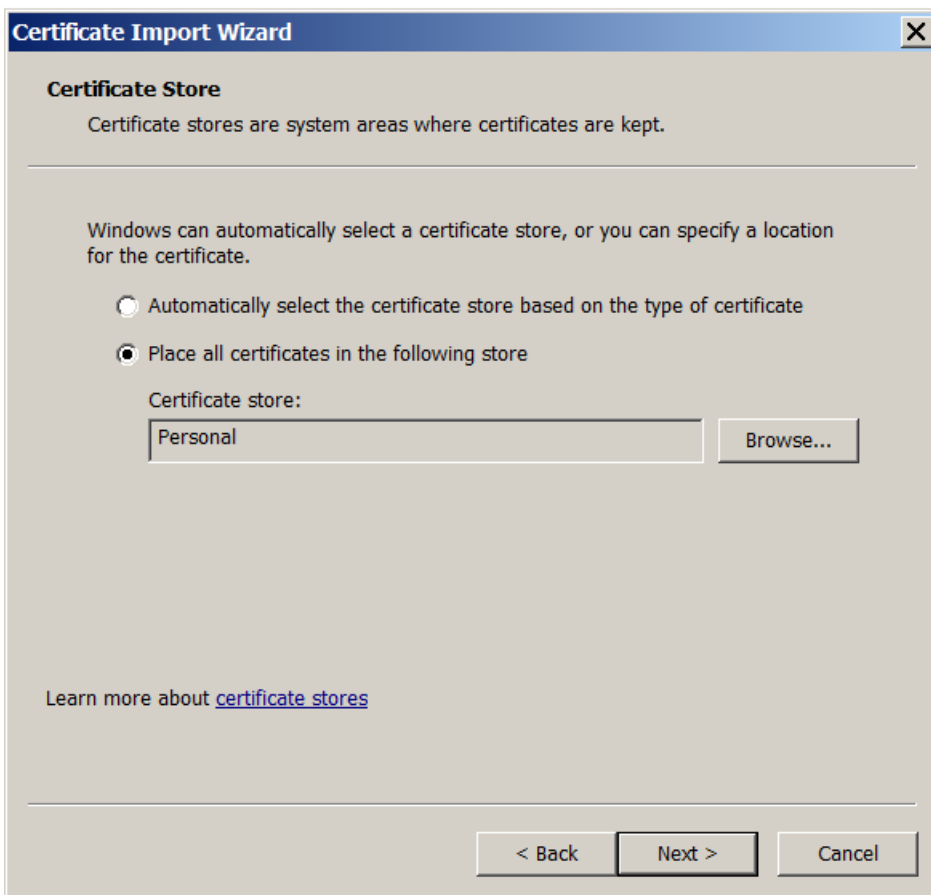
To continue, click Next.

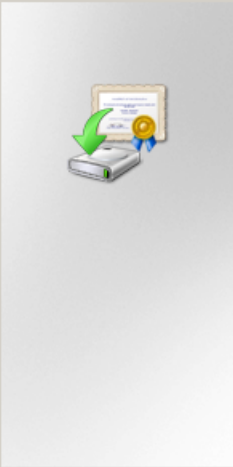
< Back

Next >

Cancel







Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

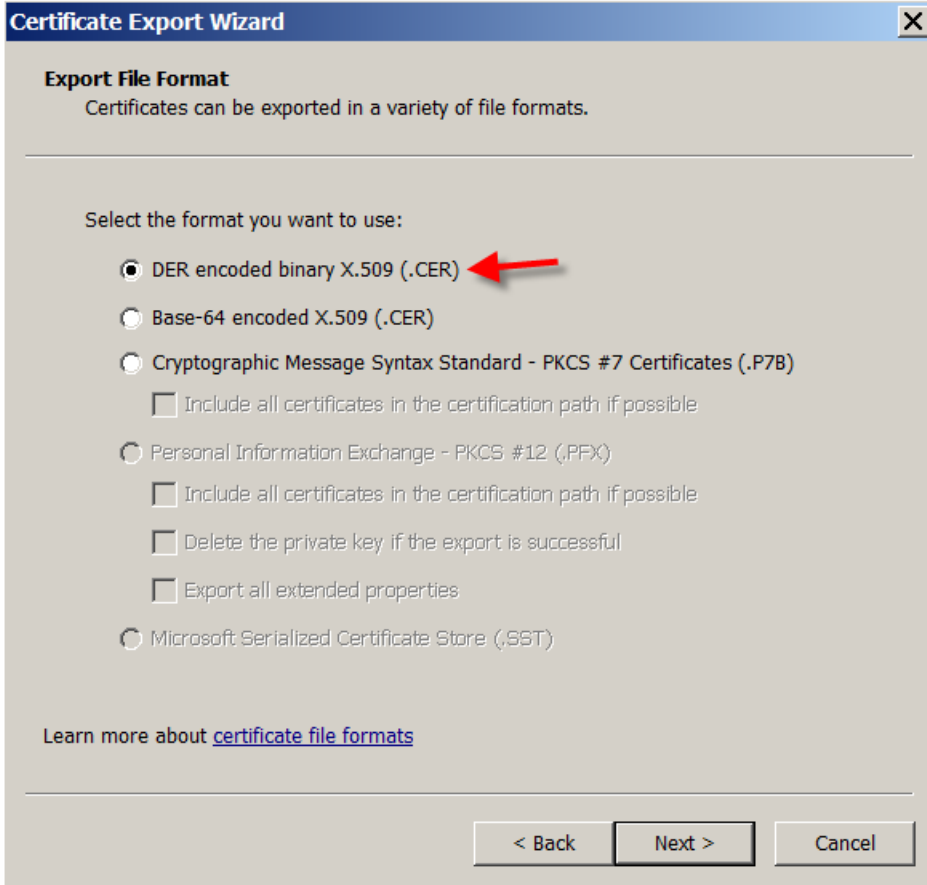
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

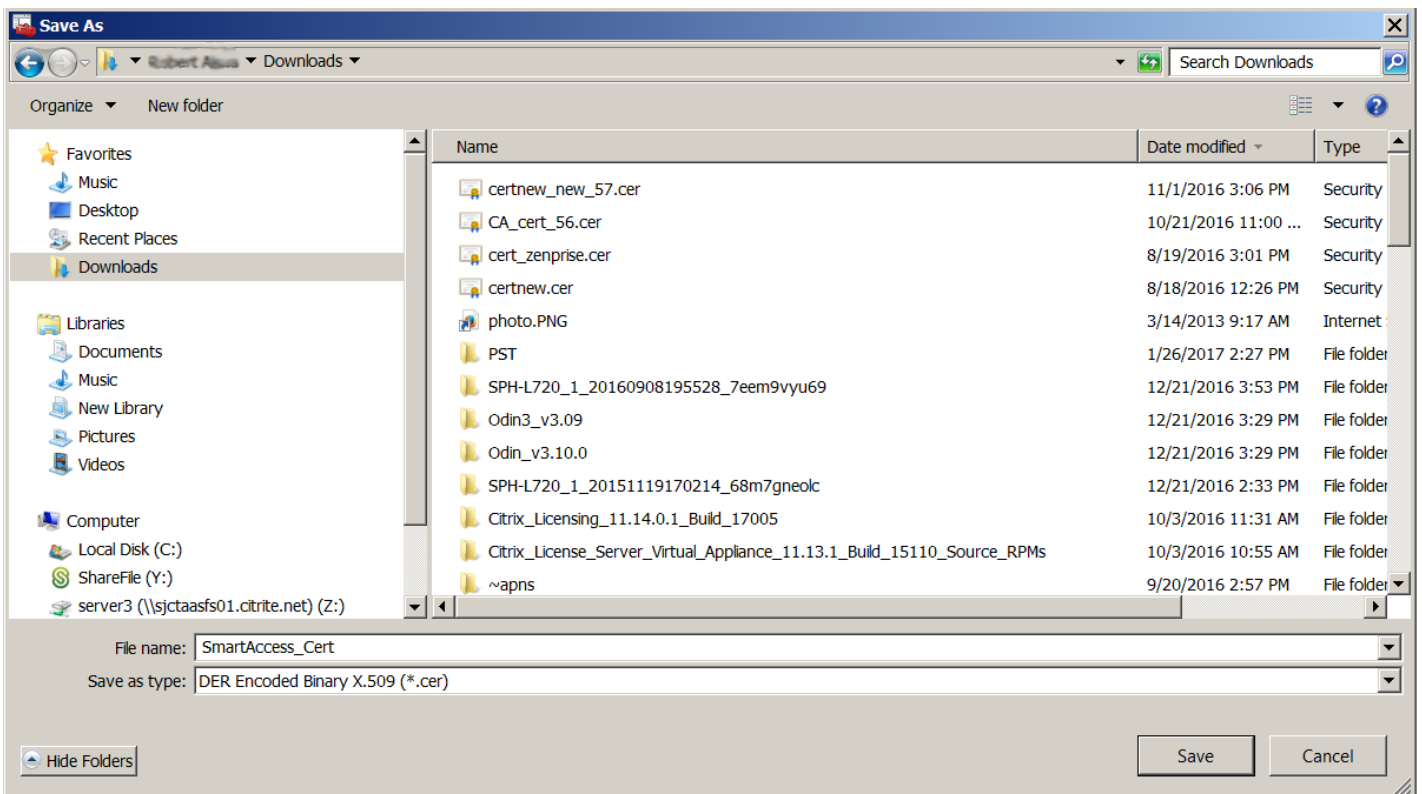
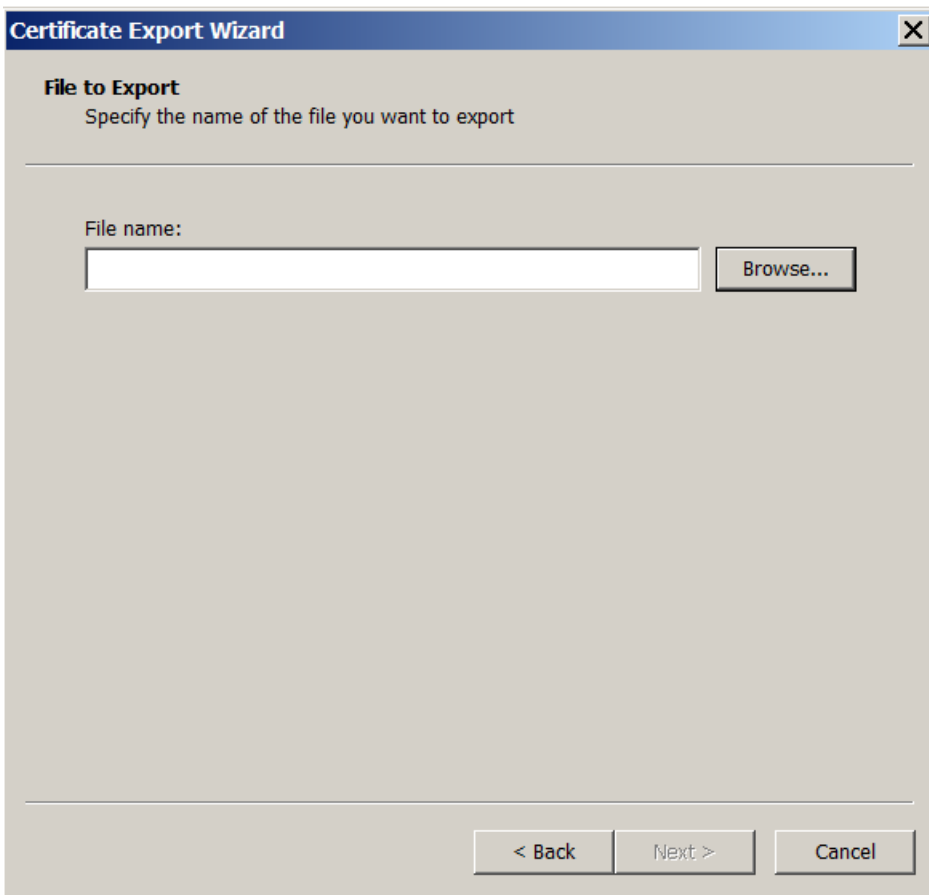
To continue, click Next.

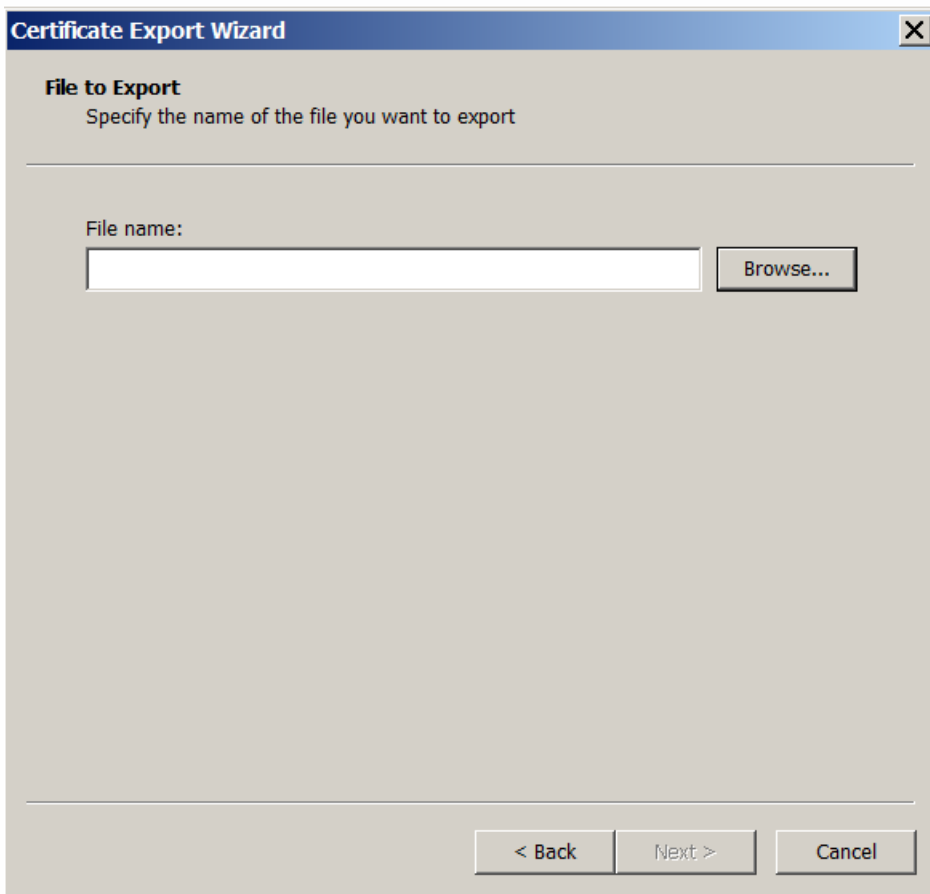
< Back

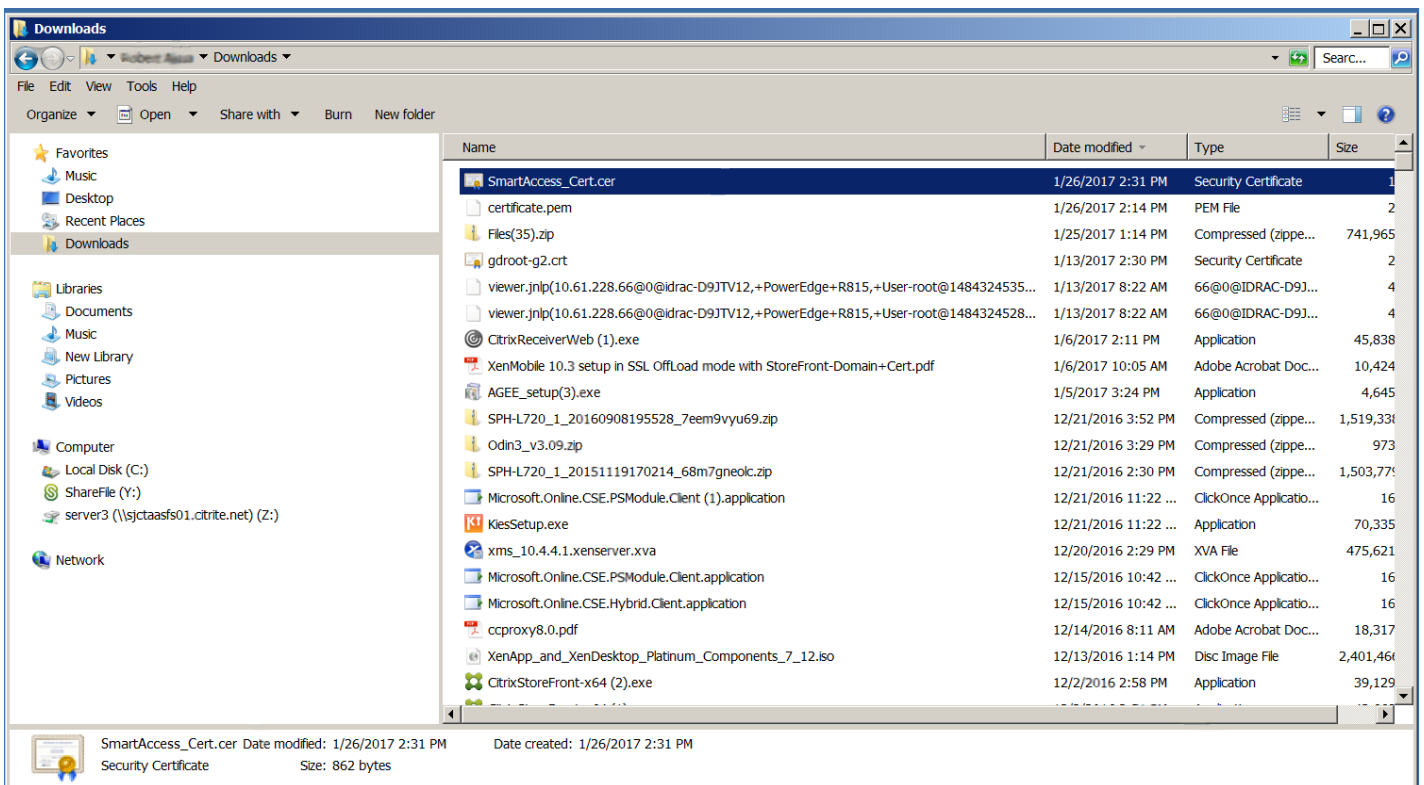
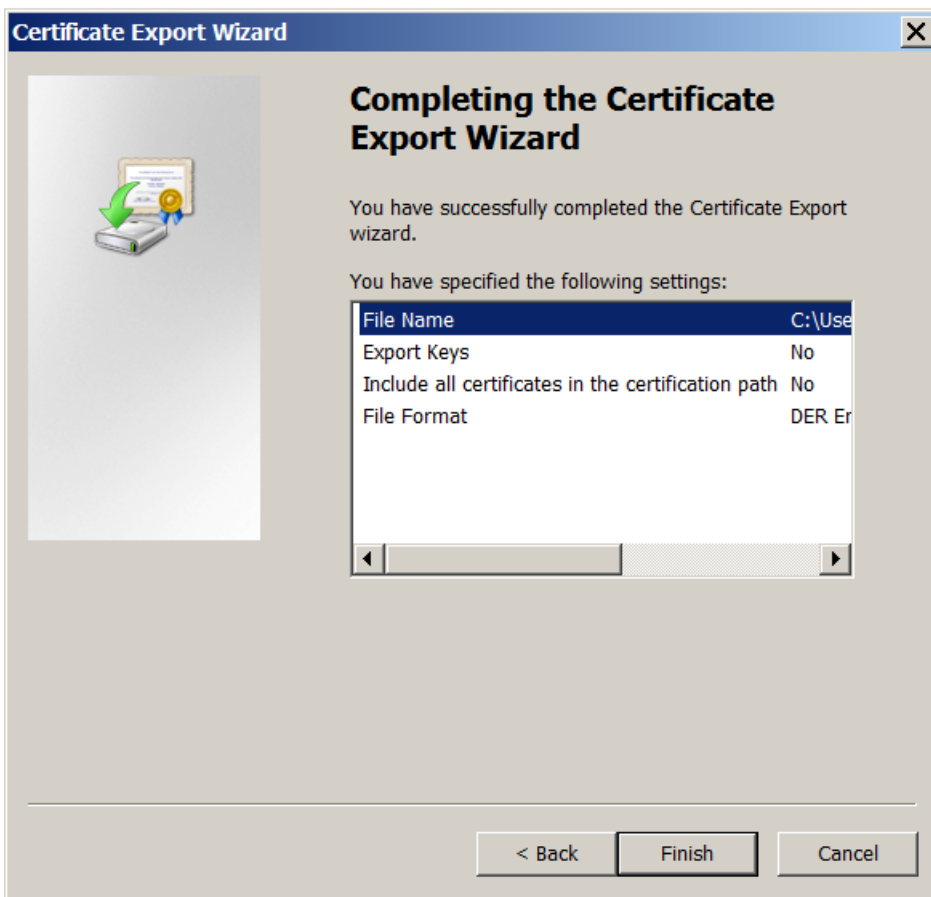
Next >

Cancel

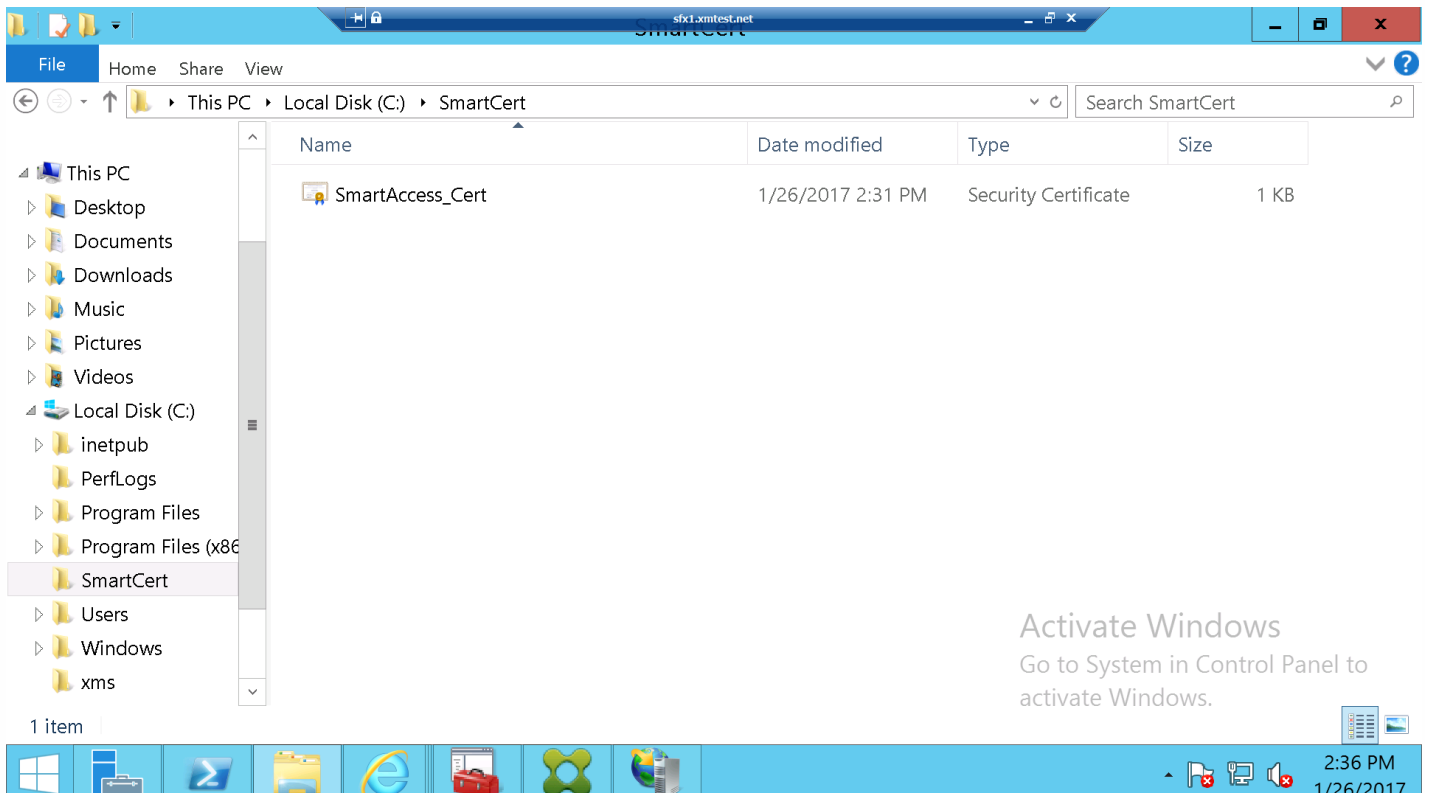




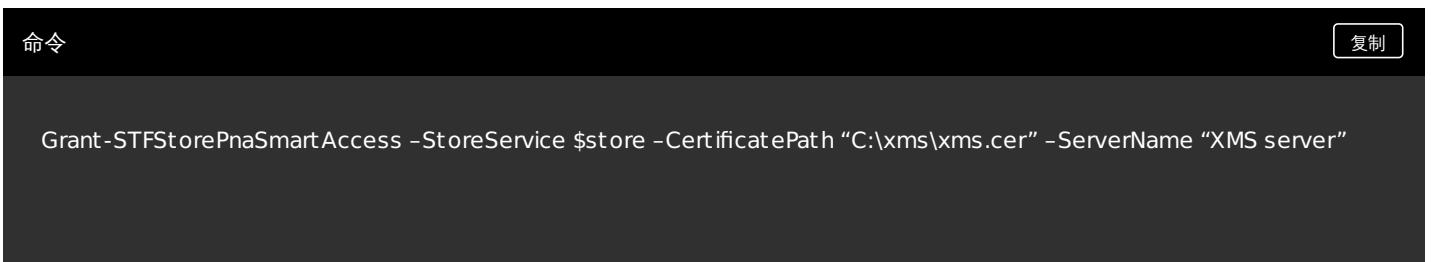




将证书复制到 StoreFront 服务器



在 StoreFront 应用商店中配置证书



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $store =Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Grant-STFStorePnaSmartAccess -StoreService $store -CertificatePath C:\SmartCert\SmartAccess_Cert
.cer -ServerName "XMS Server"

Confirm
Are you sure you want to perform this action?
Performing the operation "Grant-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32> _
```

```
命令 复制

Revoke-STFStorePnaSmartAccess -StoreService $store -All
```

```
PS C:\Windows\system32> $store =Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Revoke-STFStorePnaSmartAccess -StoreService $store -All

Confirm
Are you sure you want to perform this action?
Performing the operation "Revoke-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32> _
```

```
命令 复制

$store = Get-STFStoreService -VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "My XM Server"
```

```
命令 复制
```

```
$store = Get-STFStoreService -VirtualPath /Citrix/Store
```

```
Revoke-STFStorePnaSmartAccess -StoreService $store -CertificateThumbprint "1094821dec7834d5d42 bb456329efe4fca8"
```

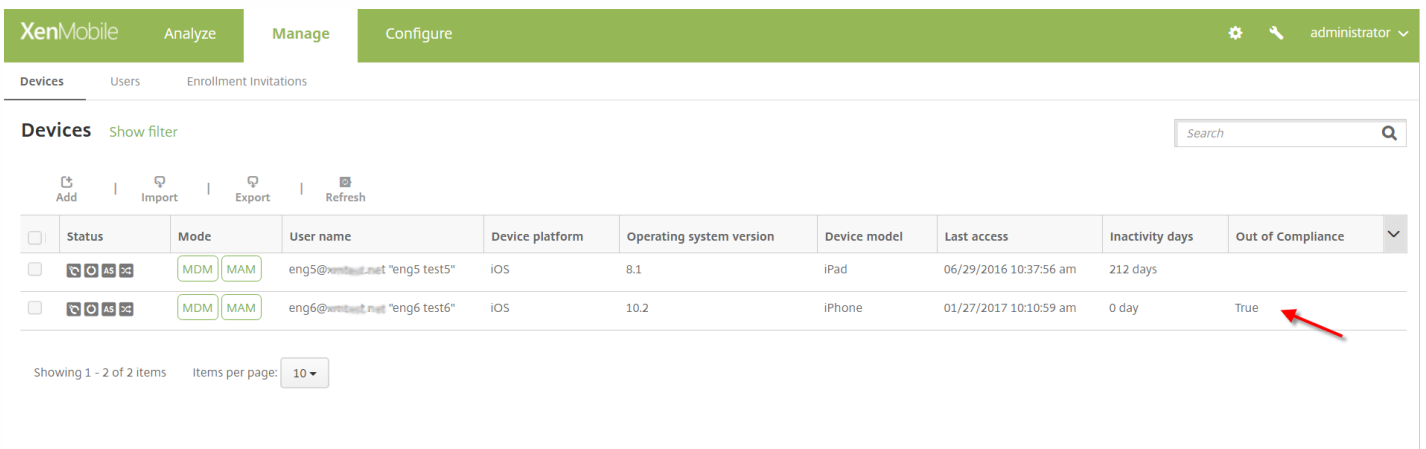
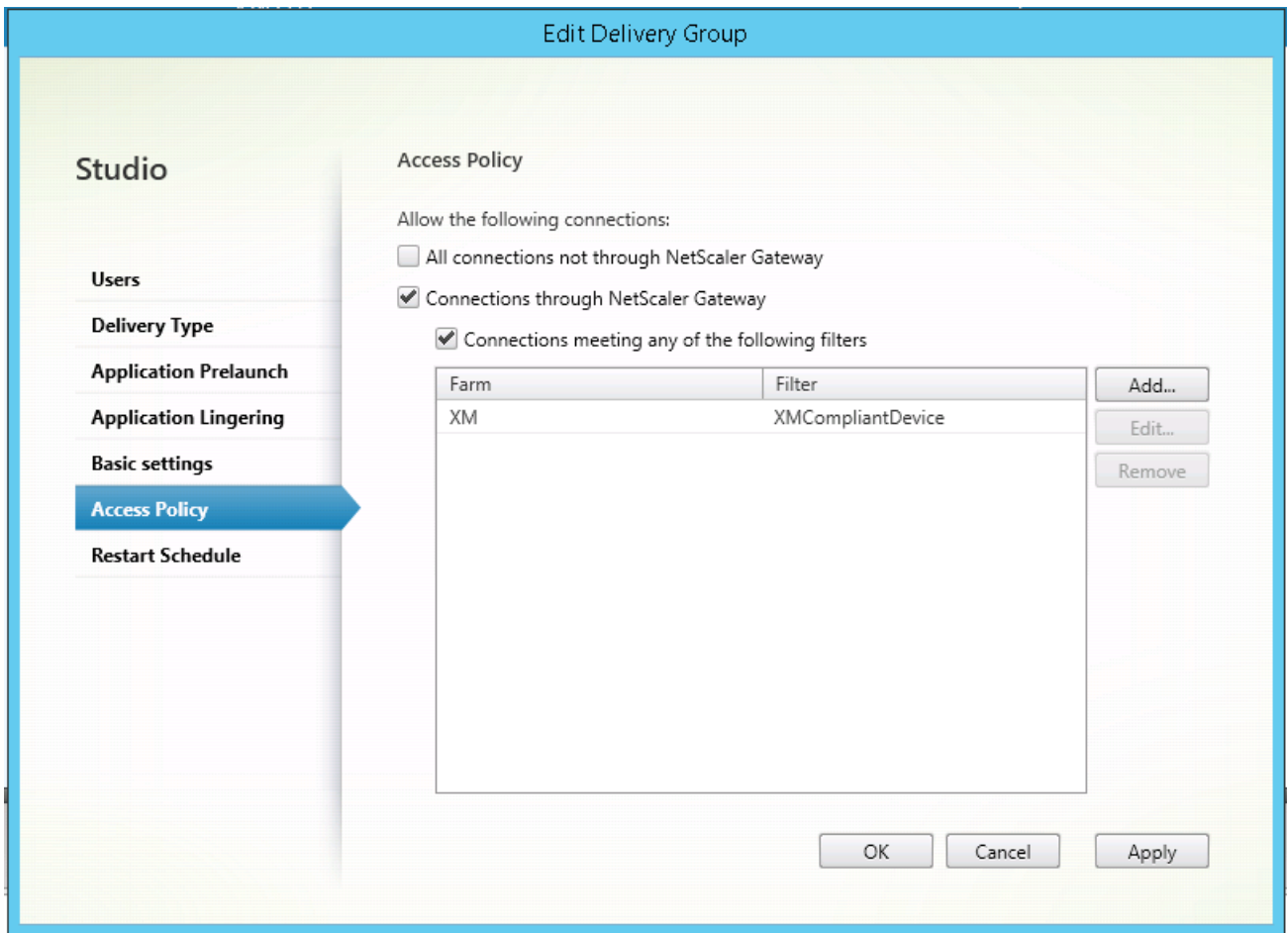
命令

复制

```
$store = Get-STFStoreService -VirtualPath /Citrix/Store
```

```
$access = Get-STFStorePnaSmartAccess -StoreService $store
```

```
Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess $access.AccessConditionsTrusts[0]
```



Actions

- 1 Action Info
- 2 Details
- 3 Assignment (optional)
- 4 Summary

Action Information

Actions automate common compliance requirements based on specific trigger events.

Name*

Description

Actions

- 1 Action Info
- 2 Details
- 3 Assignment (optional)
- 4 Summary

Action details

Choose a trigger event and the associated action for that event.

Trigger*

User property

Name

Is

eng6 test6

Action*

Mark the device as out of compliance

Is

True

0

Hours

Back Next >

-
-
-
-

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps **Actions** ShareFile Enrollment Profiles Delivery Groups

Actions

- 1 Action Info
- 2 Details
- 3 Assignment (optional)**
- 4 Summary

Assign to Delivery Group

To deploy this action, assign it to one or more delivery groups.

Choose delivery groups

AllUsers

Delivery groups to receive app assignment

AllUsers

► Deployment Schedule ⓘ

Actions

1 Action Info

2 Details

3 Assignment (optional)

4 Summary

Summary

Review your settings, and then save or deploy this action.

General

Name Name

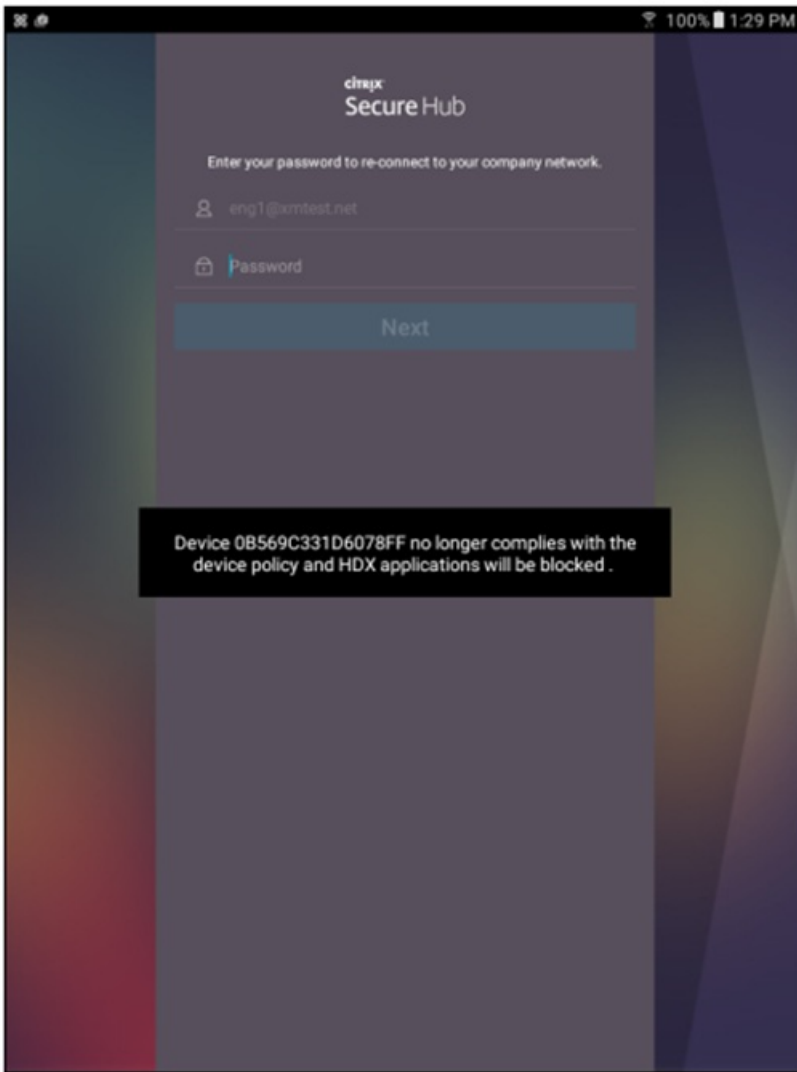
Description

Action details

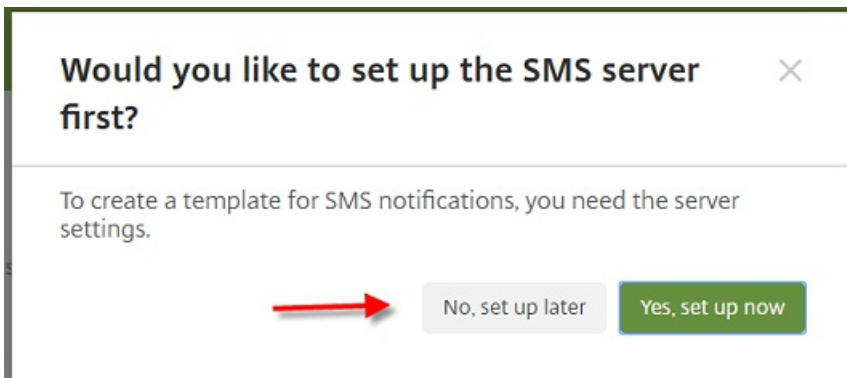
If name is "eng6 test6", then mark the device as out of compliance immediately.

Assignment

Delivery groups AllUsers



创建当设备被标记为不合规时用户看到的通知



-
-
-
-
-

Name*

Description

Type
 Manual sending supported

SMTP

Sender

Recipient

Subject

Message

Secure Hub

Message*

创建当设备标记为不合规时用于发送通知的操作

-
-

Actions

- 1 Action Info
- 2 Details
- 3 Assignment (optional)
- 4 Summary

Action Information ✕

Actions automate common compliance requirements based on specific trigger events.

Name* HDX blocked notification Ⓞ

Description HDX blocked notification because device is out of compliance

-
-
-
-

Actions

- 1 Action Info
- 2 Details
- 3 Assignment (optional)
- 4 Summary

Trigger*

Device property ▾

Out of compliance ▾

Is ▾

True ▾

Action*

Send notification ▾

HDX Application Block ▾ Ⓞ

Preview notification message

0 Ⓞ

Minutes ▾

Specify an action repeat interval Ⓞ

Days ▾

Back Next >

-

-
-

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps **Actions** ShareFile Enrollment Profiles Delivery Groups

Actions

- 1 Action Info
- 2 Details
- 3 Assignment (optional)**
- 4 Summary

Assign to Delivery Group

To deploy this action, assign it to one or more delivery groups.

Choose delivery groups

- AllUsers
- DG1
- DG2
- DG3
- DG4
- DG5
- DG6
- DG7
- DG8

Delivery groups to receive app assignment

AllUsers

► Deployment Schedule

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps **Actions** ShareFile Enrollment Profiles Delivery Groups

Actions

- 1 Action Info
- 2 Details
- 3 Assignment (optional)
- 4 Summary**

Summary

Review your settings, and then save or deploy this action.

General

Name HDX blocked notification
Description HDX blocked notification because device is out of compliance

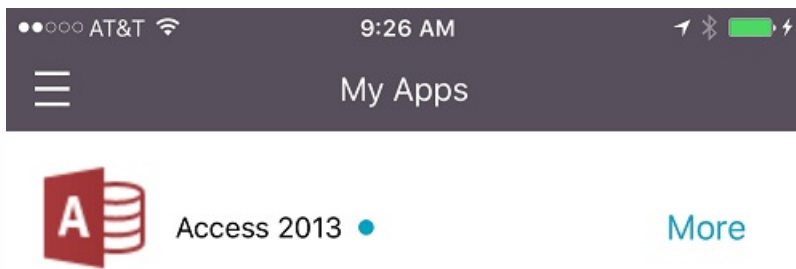
Action details

if device has been marked as Out of Compliance, then notify using the template "HDX Application Block" immediately.

Assignment

Delivery groups AllUsers

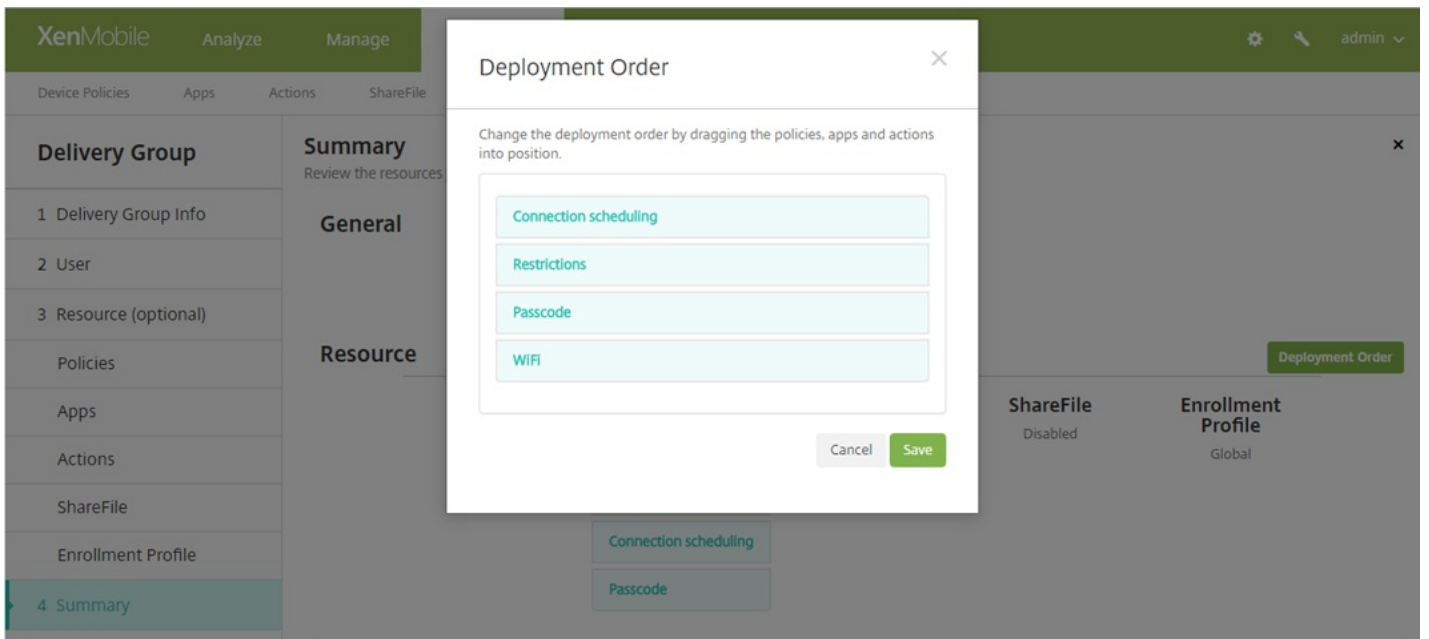
用户如何重新获取对 HDX 应用程序的访问权限



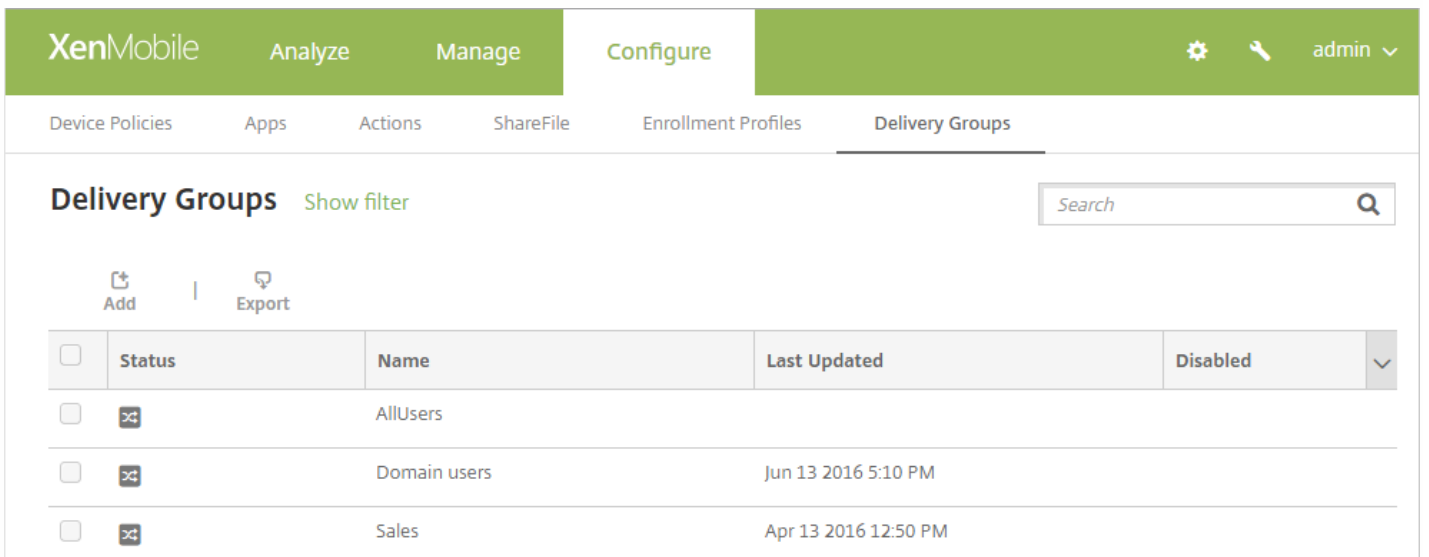
-
-
-

-
-

-
-



添加交付组



Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Actions

ShareFile

Enrollment Profile

4 Summary

Delivery Group Information ✕

Enter a name for the delivery group and any information that will help you keep track of it later.

Name

Description

-
-

Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Actions

ShareFile

Enrollment Profile

4 Summary

User Assignments

Select domain

local

Include user groups



Search

Or And

Deploy to anonymous user

OFF

Deployment Rules

-
-
-
-
-
-
-
-
-
-
-
-

6. 配置部署规则



向交付组添加可选资源


Delivery Group
1 Delivery Group Info
2 User
3 Resource (optional)
Policies
Apps
Actions
ShareFile
Enrollment Profile
4 Summary

Policies

Drag the policies that you want to include in the delivery group.

▼ Policies

- WiFi
- Passcode
- Connection scheduling
- Restrictions
- Launcher Configuration



-
-
-

Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Actions

ShareFile

Enrollment Profile

4 Summary

Apps

Drag the apps that you want to include in the delivery group.

Enter app name

▼ Apps

Office365_SAML

Web Ent



Required Apps

Optional Apps

-
-
-

Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Actions

ShareFile

Enrollment Profile

4 Summary

Actions

Drag the actions that you want to include in the delivery group.

Enter action name



Search

▼ Actions

Action - Out of compliance

Action - Send notification



-
-
-

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

Delivery Group

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

ShareFile

Enable ShareFile to provide users in the delivery group with single sign-on (SSO) access to content and data.

Enable ShareFile OFF

XenMobile Analyze Manage **Configure** ⚙️ 🔍 administrator ▾

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

Delivery Group

- 1 Delivery Group Info
- 2 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile
- Enrollment Profile
- 3 Summary

ShareFile

Drag the StorageZone Connectors that you want to include in the delivery group.

▼ Connectors

TestNS

TestSP

☞

TestSP ✕

注册配置文件

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

Delivery Group

- 1 Delivery Group Info
- 2 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile
- Enrollment Profile
- 3 Summary

Enrollment Profile

Select the enrollment profile that you want the users in this delivery group to see

Enrollment Profile Global

•

检查已配置的选项并更改部署顺序

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

Delivery Group

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

Summary

Review the resources you are about to assign to the delivery group. ✕

General

Name Local

Description

Resource

Deployment Order				
Apps 0	Policies 0	Actions 0	ShareFile Disabled	Enrollment Profile Global

更改部署顺序

Deployment Order ×

Change the deployment order by dragging the policies, apps and actions into position.

Jailbroken device

MBWifi

Out of compliance

Passcode

Personal Hotspot

Restrictions

ShareFile1

编辑交付组

Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Actions

ShareFile

Enrollment Profile

4 Summary

User Assignments

Select domain

local

Include user groups



Search

Or And

Deploy to anonymous user

OFF

► Deployment Rules

-
-
-
-
-

-
-

启用和禁用 AllUsers 交付组

-
-

部署交付组

-
-

-
-

Delivery Groups [Show filter](#)

[Add](#) | [Export](#)

<input type="checkbox"/>	Status	Name	Last Updated	Disabled
<input type="checkbox"/>		AllUsers		
<input type="checkbox"/>		sales	Oct 26 2015 12:48 PM	
<input type="checkbox"/>		DG for CAT		

Showing 1 - 3 of 3 items

[Edit](#) | [Deploy](#) | [Delete](#)

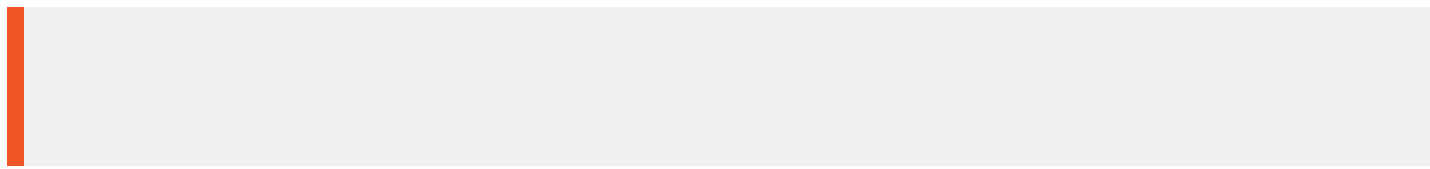
Deployment

1 Installed	0 Pending	0 Failed
-----------------------	---------------------	--------------------

[Show more >](#)

删除交付组

-
-



导出交付组表

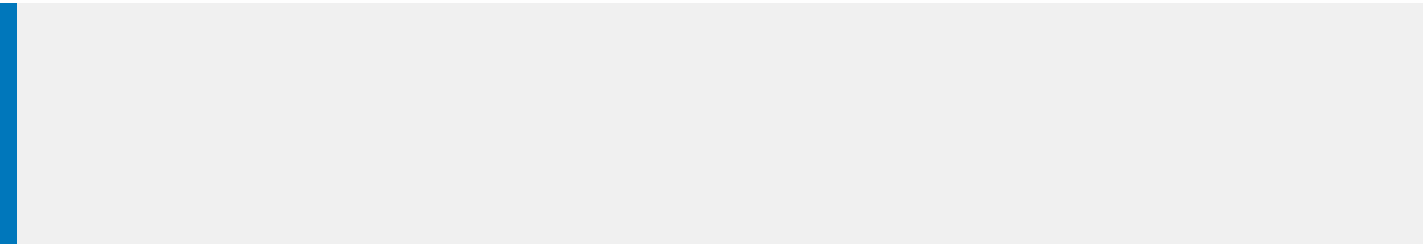
-
-
-
-
-
-
-

宏语法

-
-

-
-
-
-

-
-
-
-



-
-

-
-

XenMobile Analyze Manage **Configure** admin

Device Policies Apps **Actions** ShareFile Enrollment Profiles Delivery Groups

Actions

- 1 Action Info
- 2 Details**
- 3 Assignment (optional)
- 4 Summary

Action details

Choose a trigger event and the associated action for that event.

Trigger*

Select a trigger

Action*

Select an action

Summary

If **CONDITION IS FULFILLED**, then **DO ACTION**.

- ▶ Deployment Rules (iOS)
- ▶ Deployment Rules (Mac OS X)
- ▶ Deployment Rules (Android)
- ▶ Deployment Rules (Windows Mobile/CE)
- ▶ Deployment Rules (Windows Desktop/Tablet)
- ▶ Deployment Rules (Windows Phone)

Internet Explorer Back Next >

-
-
-
-
-

-
-
-
-

-
-
-

Action*

Send notification

Select a template

1

Hours

Specify an action repeat interval

Days

?

?

?

Action*

Send notification

Failed Samsung KNOX attestation

Preview notification message

1

Hours

0

Minutes

Summary

If The installed app name is " APP ", then notify USING TEMPLATE after 1 hour(s).

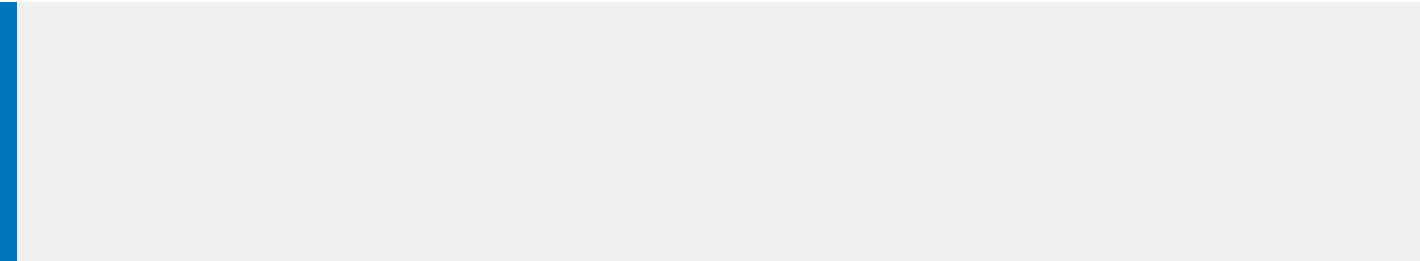
13. 配置部署规则



-
-
-
-
-

面向仅 MAM 模式的应用程序锁定和应用程序擦除操作

-
-
-



XenMobile Analyze Manage **Configure** ⚙️ 🔑 Administrator ▾

Device Policies Apps **Actions** ShareFile Enrollment Profiles Delivery Groups

Actions

- 1 Action Info
- 2 Details**
- 3 Assignment (optional)
- 4 Summary

Device property ▾

Select a device property ▾

Action*

App wipe ▾

1 ?

Hours ▾

Summary

If **DEVICE PROPERTY CONDITION IS FULFILLED**, then app wipe the device after 1 hour(s).

Back Next >

Samsung_S5 04/14/2016 10:47:08 am 1 days

Edit | Deploy | Secure | Notify | Delete
×

XME Device Managed

Delivery Groups	1	⊞	Policies	0	⊞
Actions	0	⊞	Apps	0	⊞

Show more >

>

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Devices Users Enrollment Invitations

Device details

- 1 General
- 2 Properties
- 3 User Properties
- 4 Assigned Policies
- 5 Apps
- 6 Actions
- 7 Delivery Groups
- 8 Certificates
- 9 Connections
- 10 TouchDown

WiFi MAC Address NONE

Bluetooth MAC Address NONE

Device Ownership Corporate BYOD

Security

Strong ID YEMXRMSG

Full Wipe of Device No device wipe.

Selective Wipe of Device No device selective wipe.



Lock Device No device lock.

Device locate No device locate.

Device App Wipe No device App Wipe.

Device App Lock App Lock was requested at 04/15/2016 01:59:47 pm.

Next >

XenMobile Analyze Manage Configure   administrator ▾

Troubleshooting and Support

<p>Diagnostics</p> <hr/> <p>NetScaler Gateway Connectivity Checks</p> <hr/> <p>XenMobile Connectivity Checks</p> <hr/>	<p>Support Bundle</p> <hr/> <p>Create Support Bundles</p> <hr/>	<p>Links</p> <hr/> <p>Citrix Product Documentation</p> <hr/> <p>Citrix Knowledge Center</p> <hr/>
<p>Log Operations</p> <hr/> <p>Logs</p> <hr/> <p>Log Settings</p> <hr/>	<p>Advanced</p> <hr/> <p>Cluster Information</p> <hr/> <p>Garbage Collection</p> <hr/> <p>Java Memory Properties</p> <hr/> <p>Macros</p> <hr/> <p>PKI Configuration</p> <hr/> <p>Anonymization and De-anonymization</p> <hr/>	<p>Tools</p> <hr/> <p>APNs Signing Utility</p> <hr/> <p>Citrix Insight Services</p> <hr/> <p>Device NetScaler Connector Status</p> <hr/>

-
-
-
-
-
-

NOTIFICATIONS

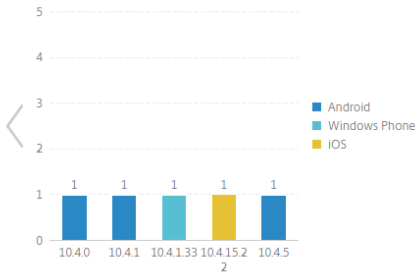
Customize Refresh

Compliance
0 Blocked Devices at ActiveSync Gateway
9 Non-compliant Devices
25 Inactive Devices

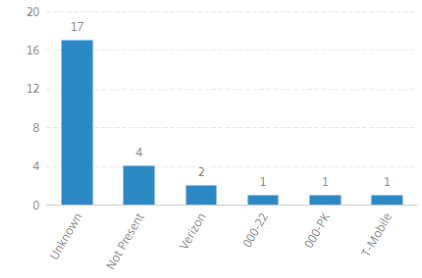
Decommission
0 Wipes Last 24 Hours
0 Selective Wipes Last 24 Hours
2 Pending (Selective) Wipes

Enrollment
0 New Devices Last 24 hours
0 Pending Activation Requests

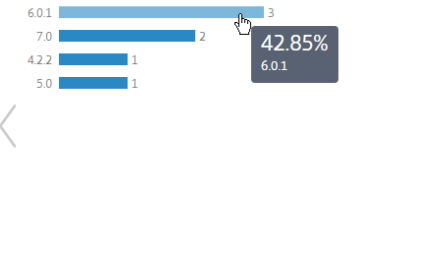
INSTALLED APPS Secure Hub Actions



DEVICES BY CARRIER Actions



MANAGED DEVICES BY PLATFORM Android Actions



DEVICES BY PLATFORM Windows Desktop/Tablet Actions



NOTIFICATIONS



Compliance

0

Blocked Devices at
ActiveSync Gateway

9

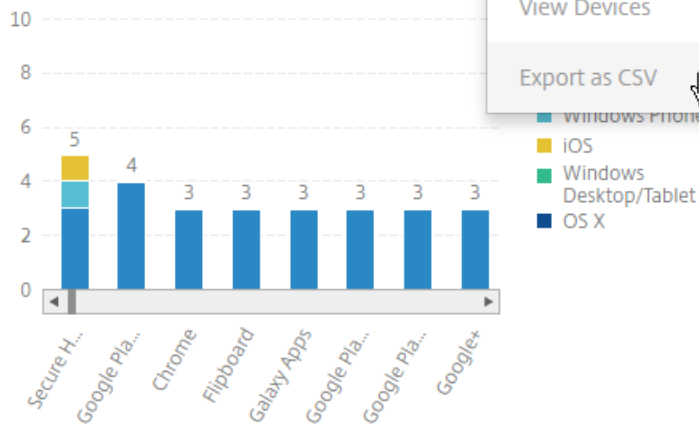
Non-compliant
Devices

25

Inactive
Devices

INSTALLED APPS

Actions



-
-
-
-
-
-
-
-
-
-
-
-

XenMobile Analyze Manage Configure administrator

Dashboard Reporting

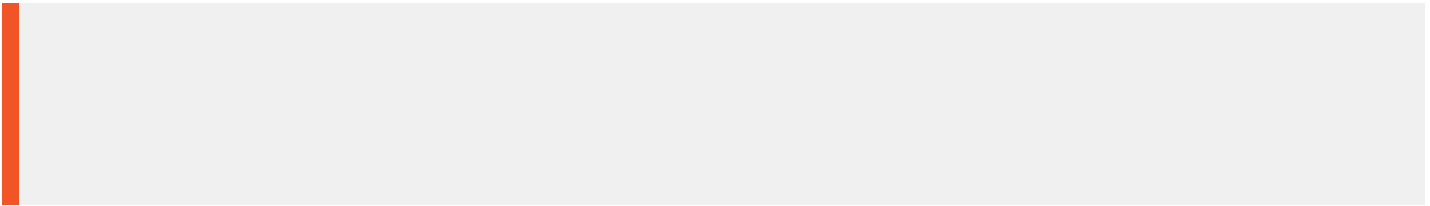
Reporting

Terms & Conditions



List of accepted and declined Terms and Conditions agreements by device users.

Report Data: document name, created on, platform, user name, delivery group, acceptance status.

	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORIES	AVAILABLE_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	GoToMeeting	6.6.4.1127	Default	10/17/2016 14:21		7	7	0	0	Public App Store
3	Secure Web - Inception	10.4.0-11	Default	10/17/2016 14:37	citrix.com	7	6	0	1	MDX
4	Secure Mail	10.4.1-221	Default	10/17/2016 16:06	citrix.com	6	5	0	1	MDX
5	Twitter	6.64	appstore	10/17/2016 17:04		3	3	0	0	Public App Store
6	Salesforce1	11.0.3	Default	12/14/2016 17:52		2	2	0	0	Public App Store



-
-

XenMobile Analyze Manage Configure   admin ▾

Settings > [Mobile Service Provider](#)

Mobile Service Provider

Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.

Web service URL*

User name*

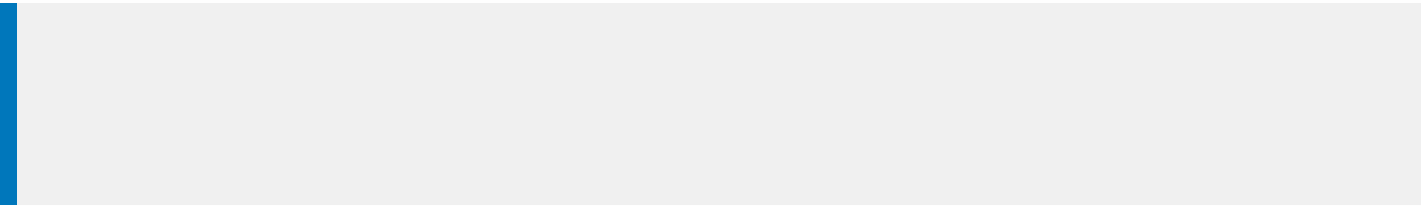
Password*

Automatically update BlackBerry and ActiveSync device connections OFF

-
-
-
-
-

-
-

-
-
-
-
-



Settings > SysLog

SysLog

You can configure XenMobile to send log files to a systems log (syslog) server using the server host name or IP address.

Server*

Port*

Information to log System Logs

Audit

-
-
-
-
-

客户体验改善计划

Feb 27, 2017

Citrix 客户体验改善计划 (CEIP) 从 XenMobile 收集匿名配置和使用数据，并自动将数据发送到 Citrix。此数据可帮助 Citrix 改善 XenMobile 的品质、可靠性和性能。参与 CEIP 完全自愿。首次安装 XenMobile 时或安装更新时，可以选择是否参与 CEIP。选择参与后，通常每周收集一次数据，而性能和使用数据则每小时收集一次。这些数据存储在磁盘上，每周一次通过 HTTPS 安全地传输给 Citrix。您可以在 XenMobile 控制台更改是否参与 CEIP。有关 CEIP 的详细信息，请参阅[关于 Citrix 客户体验改善计划 \(CEIP\)](#)。

选择参与 CEIP

首次安装 XenMobile 或进行更新时，您会看到提示您参与的以下对话框。


Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

[Learn more](#)



Would you like to help make Citrix products better by joining the program?
(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)

Yes, send anonymous usage and statistics information.

No

更改 CEIP 参与设置

1. 要更改 CEIP 参与设置，请在 XenMobile 控制台中，单击控制台右上角的齿轮图标以打开[设置](#)页面。
2. 在[服务器](#)下方，单击[体验改善计划](#)。此时将显示[客户体验改善计划](#)页面。所显示的确切页面取决于您当前是否已参与 CEIP。

Settings > [Experience Improvement Program](#)

Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer



[Learn more](#)

You are currently participating in the Customer Experience Improvement Program.

- Continue participating
- Stop participating

Cancel

Save

3. 如果当前已参与 CEIP 并希望停止，请单击停止参与。

4. 如果当前未参与 CEIP 并希望开始参与，请单击开始参与。

5. 单击保存。

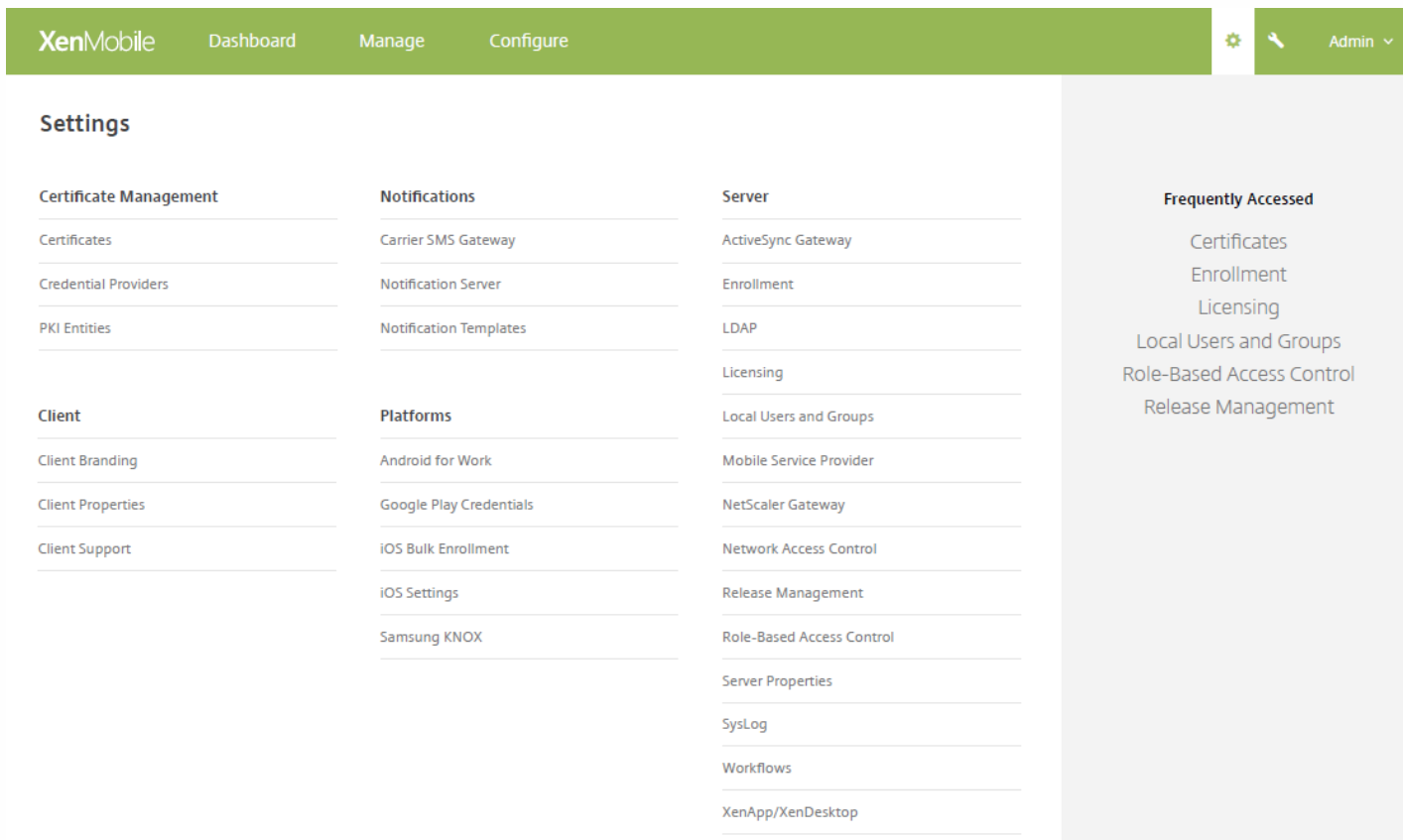
支持选项和远程支持

Apr 26, 2017

可以提供电子邮件地址，以便用户联系技术支持人员。当用户从其设备请求帮助时，他们会看到该电子邮件地址。

还可以配置用户如何将日志从其设备发送给技术支持。可以将日志配置为直接发送或者通过电子邮件发送。

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



2. 在客户端下面，单击客户端支持。此时将显示客户端支持页面。

3. 配置以下设置：

- **支持电子邮件(IT 技术支持)**：键入 IT 技术支持联系人的电子邮件地址。
- **将设备日志发送给 IT 技术支持人员**：选择设备日志是直接发送还是通过电子邮件发送。默认值为通过电子邮件。
 - 启用直接时，会显示“在 ShareFile 上存储日志”对应的设置。如果启用了“在 ShareFile 上存储日志”，日志将直接发送至 ShareFile。否则，日志将发送至 XenMobile，然后通过电子邮件发送给技术支持。此外，还会显示**如果直接发送失败，请使用电子邮件选项**，默认情况下启用此选项。如果不希望使用客户端电子邮件发送服务器问题的日志，可以禁用此选项。但是，如果禁用了此选项时出现服务器问题，则不会发送日志。
 - 启用通过电子邮件时，客户端电子邮件始终用于发送日志。

4. 单击保存。

远程支持

通过 Remote Support，您的技术支持代表能够远程控制托管的 Windows 和 Android 移动设备。

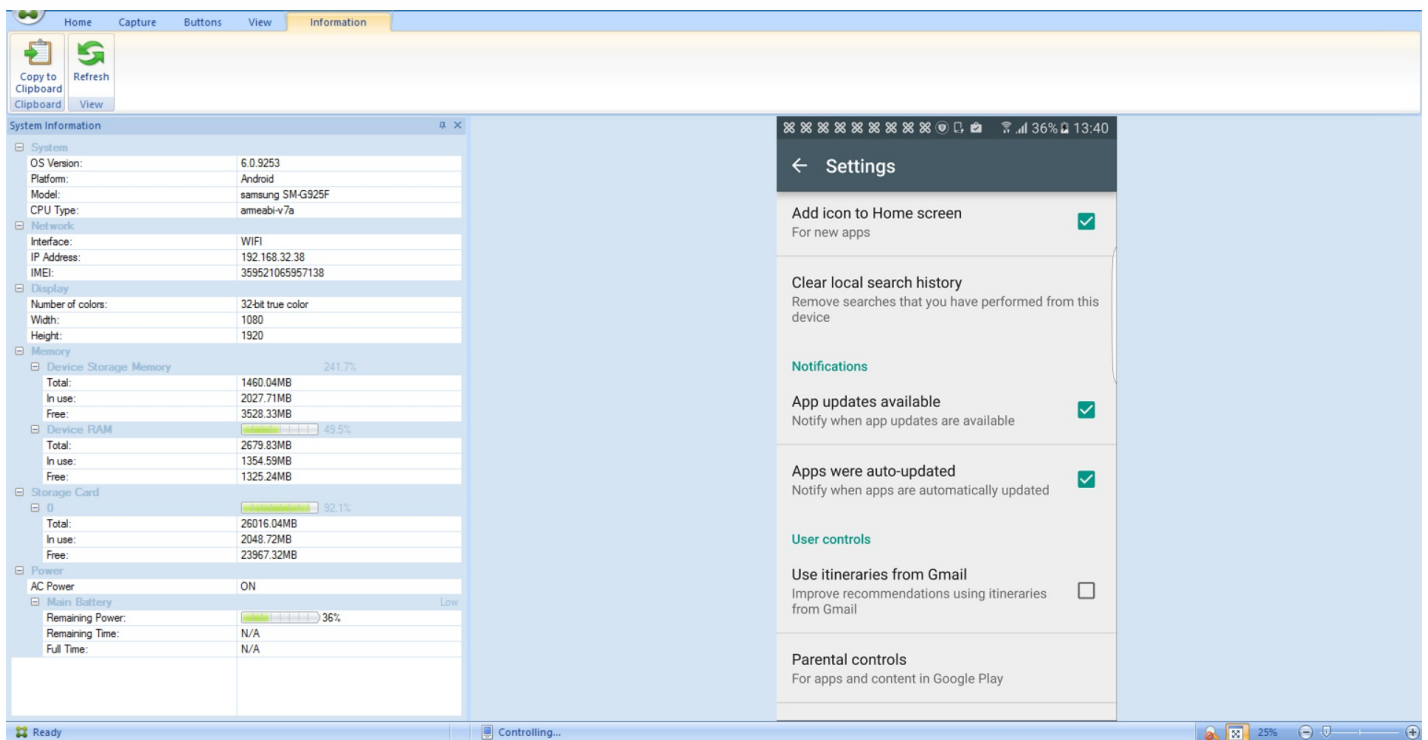
Remote Support 适用于所有 Windows 移动设备、Android Samsung SAFE 设备和非 Samsung 设备。此 Remote Support 客户端在适用于 Windows CE 和 Samsung Android 设备的 XenMobile Service 10.x 版本中不可用。

屏幕录像功能仅在 Samsung KNOX 设备上受支持。

不支持对 iOS 设备进行远程控制。

在远程控制会话期间：

- 用户会在其移动设备上看到一个图标，指示远程控制会话处于活动状态。
- Remote Support 用户会看到 Remote Support 应用程序窗口以及显示受控设备的远程控制窗口。



使用 Remote Support，可以执行以下操作：

- 远程登录到用户设备并控制屏幕。用户可观看您在屏幕上的操作，这对于培训用户而言也很有帮助。
- 实时导航和修复远程设备。您可以更改配置、对操作系统问题进行故障排除、禁用或停止有问题的应用程序或进程。
- 通过远程禁用网络访问权限、停止恶意进程以及删除应用程序或恶意软件，可以隔离和遏制这些威胁，使其不会传播到其他移动设备。
- 远程启用设备响铃和拨打电话，以帮助用户找到设备。如果用户找不到设备，可以擦除设备以确保敏感数据不会受到损害。

Remote Support 还使技术支持人员能够执行以下操作：

- 显示 XenMobile 的一个或多个实例中所有已连接设备的列表。
- 显示系统信息，包括设备型号、操作系统级别、国际移动设备标识 (IMEI)、序列号、内存和电池状态及连接性。
- 显示 XenMobile 的用户和组。
- 运行设备任务管理器，可在其中显示活动进程、结束活动进程以及重新启动移动设备。
- 运行远程文件传输，包括移动设备与中央文件服务器之间的双向文件传输。

- 成批下载软件程序并安装到一个或多个移动设备上。
- 配置设备上的远程注册表项设置。
- 利用实时设备屏幕远程控制功能优化低带宽移动网络的响应时间。
- 显示大多数移动设备品牌和型号的设备外观。显示用于添加新设备型号和映射物理键的皮肤编辑器。
- 启用设备屏幕捕获、录制和播放，并能够捕获设备上的一系列交互操作以创建视频 AVI 文件。
- 利用共享白板、VoIP 语音通信和移动用户与技术支持人员之间的聊天功能举行实时会议。

远程支持的系统要求

Remote Support 软件可安装在满足以下要求的 Windows 计算机上。有关端口要求的信息，请参阅[端口要求](#)。

支持的平台：

- Intel Xeon/Pentium 4 -1 GHz 工作站类（最低要求）
- 最低 512 MB RAM
- 最低 100 MB 可用磁盘空间

支持的操作系统：

- Microsoft Windows 2003 Server Standard Edition 或 Enterprise Edition SP1 或更高版本
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 或更高版本
- Microsoft Windows Vista SP1 或更高版本
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

安装 Remote Support 软件

1. 要下载 Remote Support 安装程序，请转到 [XenMobile 10 下载页面](#) 并登录您的帐户。
2. 展开工具，然后下载 XenMobile Remote Support v9。
Remote Support 文件名为 XenMobileRemoteSupport-9.0.0.35265.exe。
3. 双击 Remote Support 安装程序，然后按照安装向导中的说明进行操作。

要通过命令行安装 **Remote Support**，请执行以下命令：

运行以下命令：

```
RemoteSupport.exe /S
```

RemoteSupport 为安装程序的名称。例如：

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

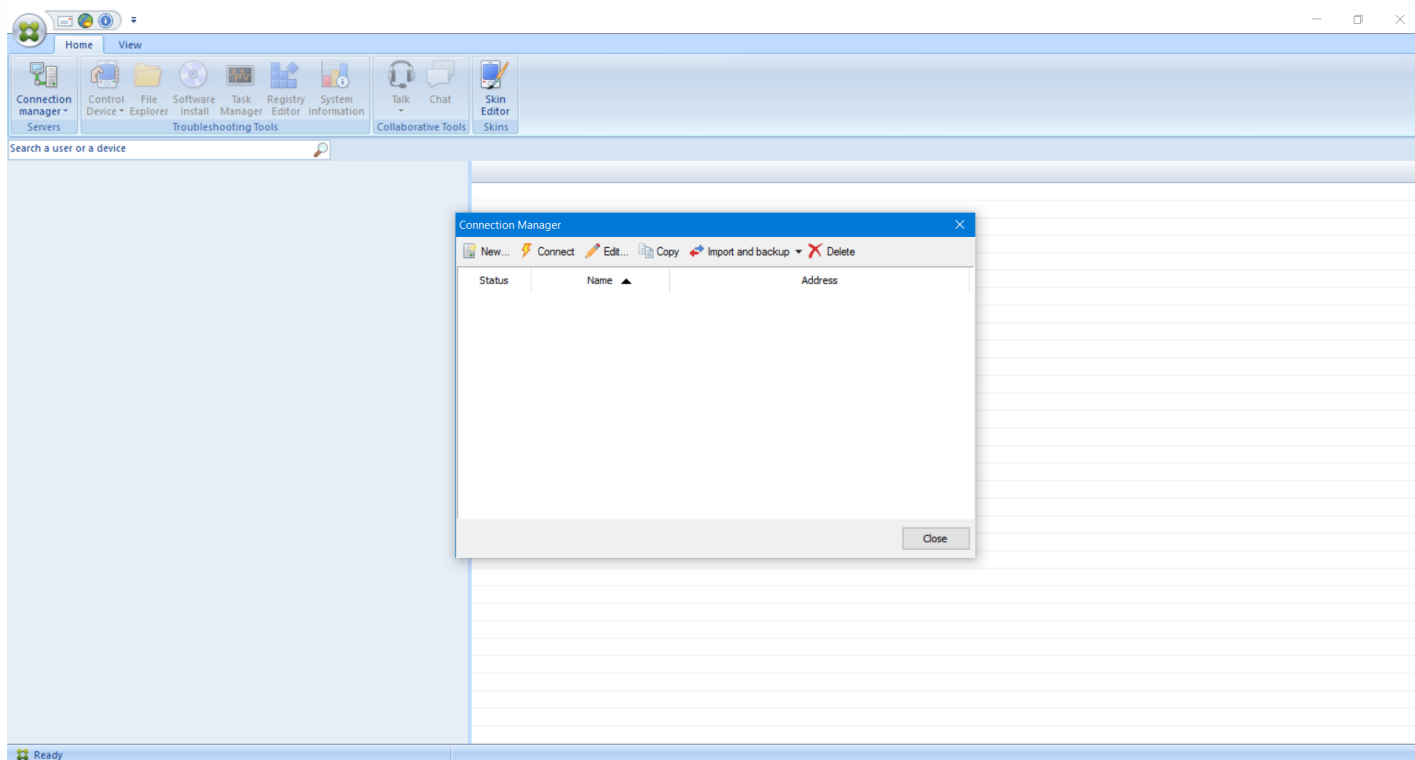
安装 Remote Support 软件时，可以使用以下变量：

- /S：使用默认参数无提示安装 Remote Support 软件。
- /D=dir: 指定自定义安装目录。

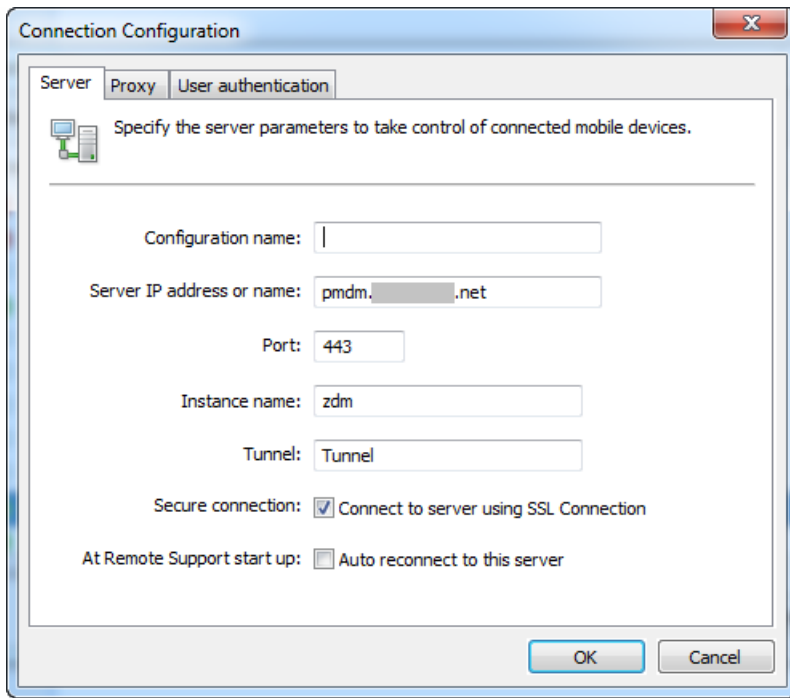
将 Remote Support 连接到 XenMobile

要建立与托管设备的远程支持连接，必须添加从 Remote Support 到用于管理设备的一台或多台 XenMobile 服务器的连接。该连接在通道 MDM 策略（一项适用于 Android 和 Windows Mobile/CE 设备的设备策略）中定义的应用程序通道上运行。应先定义应用程序通道，才能将 Remote Support 连接到 XenMobile。有关详细信息，请参阅[应用程序通道设备策略](#)。

1. 启动 Remote Support 软件，并使用您的 XenMobile 凭据登录。
2. 在 **Connection Manager**（连接管理器）中，单击 **New**（新建）。

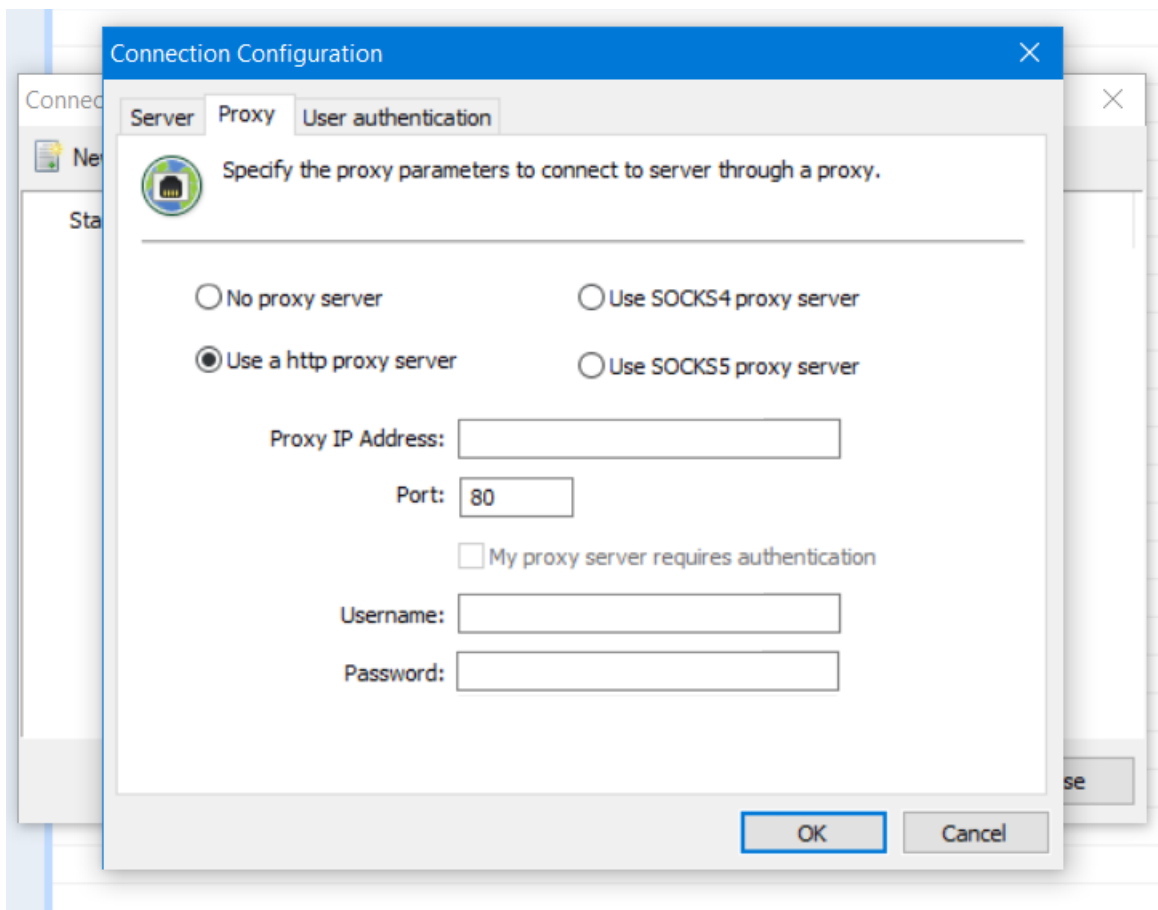


3. 在 **Connection Configuration**（连接配置）对话框中的 **Server**（服务器）选项卡上，输入以下值：
 - a. 在 **Configuration name**（配置名称）中，键入配置条目的名称。
 - b. 在 **Server IP address or name**（服务器 IP 地址或名称）中，键入 XenMobile 服务器的 IP 地址或 DNS 名称。
 - c. 在 **Port**（端口）中，键入在 XenMobile 服务器配置中定义的 TCP 端口号。
 - d. 如果 XenMobile 属于多租户部署的一部分，请在 **Instance name**（实例名称）中键入实例名称。
 - e. 在**通道**中，键入通道策略的名称。
 - f. 选中 **Connect to server using SSL Connection**（使用 SSL 连接连接到服务器）复选框。
 - g. 选中 **Auto reconnect to this server**（自动重新连接此服务器）复选框，在 Remote Support 应用程序每次启动时连接到所配置的 XenMobile 服务器。



4. 在 **Proxy**（代理）选项卡中，选择 **Use a http proxy server**（使用 HTTP 代理服务器），然后键入以下信息：

- a. 在 **Proxy IP Address**（代理 IP 地址）中，键入代理服务器的 IP 地址。
- b. 在 **Port**（端口）中，键入代理使用的 TCP 端口号。
- c. 代理服务器要求执行身份验证才能传输流量时，请选中 **My proxy server requires authentication**（我的代理服务器要求执行身份验证）复选框。
- d. 在 **Username**（用户名）中，键入在代理服务器上执行身份验证时使用的用户名。
- e. 在 **Password**（密码）中，键入在代理服务器上执行身份验证时使用的密码。



5. 在 **User Authentication**（用户身份验证）选项卡中，选中 **Remember my login and password**（记住我的登录名和密码）复选框，然后输入凭据。

6. 单击**确定**。

要连接到 XenMobile，请双击所创建的连接，然后输入为该连接配置的用户名和密码。

为 Samsung KNOX 设备启用远程支持

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

- **基本**：允许您查看有关设备的诊断信息。例如系统信息、正在运行的进程、任务管理器（内存和 CPU 使用率）以及已安装的软件文件夹内容。
- **高级**：允许您远程控制设备屏幕。例如，控制窗口颜色、在技术支持人员与用户之间建立 VoIP 会话以及在技术支持人员与用户之间建立聊天会话。

高级支持要求在 XenMobile 控制台中配置“Samsung MDM 许可证密钥”设备策略。配置此策略时，只选择 **Samsung KNOX** 平台。对于 Samsung SAFE 平台，在 XenMobile 中注册 Samsung 设备时，ELM 密钥会自动部署在这些设备上。因此，不需要为此策略选择 Samsung SAFE 平台。有关详细信息，请参阅 [Samsung MDM 许可证密钥](#)。

有关如何配置远程支持策略的信息，请参阅[远程支持设备策略](#)。

使用 Remote Support 会话

启动 Remote Support 后，Remote Support 应用程序窗口左侧将显示您在 XenMobile 控制台中定义的 XenMobile 用户组。默认情况下，仅显示包含当前已连接的用户组。您可以在用户条目旁边看到每个用户的设备。

1. 要查看所有用户，请展开左侧列中的每个组。
当前已连接到 XenMobile 服务器的用户用绿色图标指示。
2. 要显示所有用户（包括当前未连接的用户），请单击 **View**（查看）并选择 **Non-connected devices**（未连接的设备）。
此时将显示未连接的用户，但不带绿色小图标。

连接到 XenMobile 服务器但未分配给用户的设备以匿名模式显示。（字符串 **Anonymous**（匿名）将出现在列表中。）您可以像控制登录用户的设备一样控制这些设备。

要控制某个设备，请单击该设备对应的行，然后单击 **Control Device**（控制设备）以将其选中。该设备将出现在远程控制窗口中。可通过以下方法与被控制的设备交互：

- 在主窗口或独立的浮动窗口中控制设备的屏幕，包括控制颜色。
- 建立技术支持人员与用户之间的 VoIP 会话。配置 VoIP 设置。
- 与用户建立聊天会话。
- 访问设备的任务管理器以管理项目，例如内存使用率、CPU 使用率和正在运行的应用程序。
- 浏览移动设备的本地目录。传输文件。
- 在 Windows 移动设备中编辑设备注册表。
- 显示设备系统信息和所有已安装的软件。
- 更新移动设备与 XenMobile 服务器的连接状态。

连接检查

Feb 27, 2017

从 XenMobile 的支持页面，可以检查 XenMobile 与 NetScaler Gateway 及其他服务器和位置的连接情况。
执行 XenMobile 连接检查

1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。此时将显示支持页面。
2. 在诊断下面，单击 **XenMobile 连接检查**。此时将显示 **XenMobile 连接检查** 页面。如果 XenMobile 环境包含加入群集节点，将显示所有节点。

<input type="checkbox"/>	Connectivity to	IP address or FQDN
<input type="checkbox"/>	Windows Phone Store	windowsphone.com
<input type="checkbox"/>	Database	.net
<input type="checkbox"/>	Apple Feedback Push Notification Server	feedback.push.apple.com
<input type="checkbox"/>	LDAP	.net
<input type="checkbox"/>	Domain Name System (DNS)	
<input type="checkbox"/>	Nexmo Gateway	-
<input type="checkbox"/>	Apple Push Notification Server	gateway.push.apple.com
<input type="checkbox"/>	iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
<input type="checkbox"/>	Google Play	play.google.com
<input type="checkbox"/>	Windows Security Token Service	login.live.com

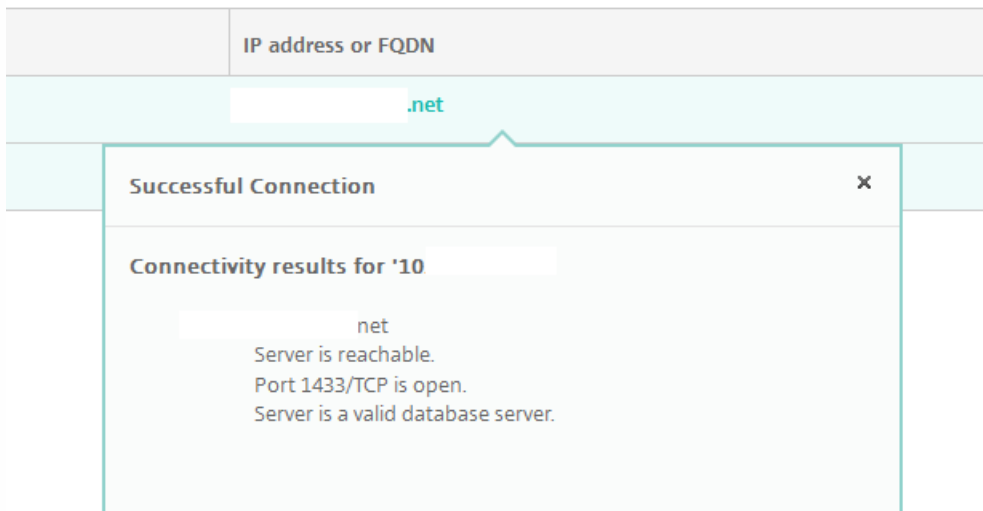
2. 选择执行连接测试时要包括的服务器，然后单击**测试连接**。此时将显示测试结果页面。

<input type="checkbox"/>	Connectivity to	IP address or FQDN	
<input type="checkbox"/>	Database	.net	✓
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	✓

Showing 1 - 2 of 2 items

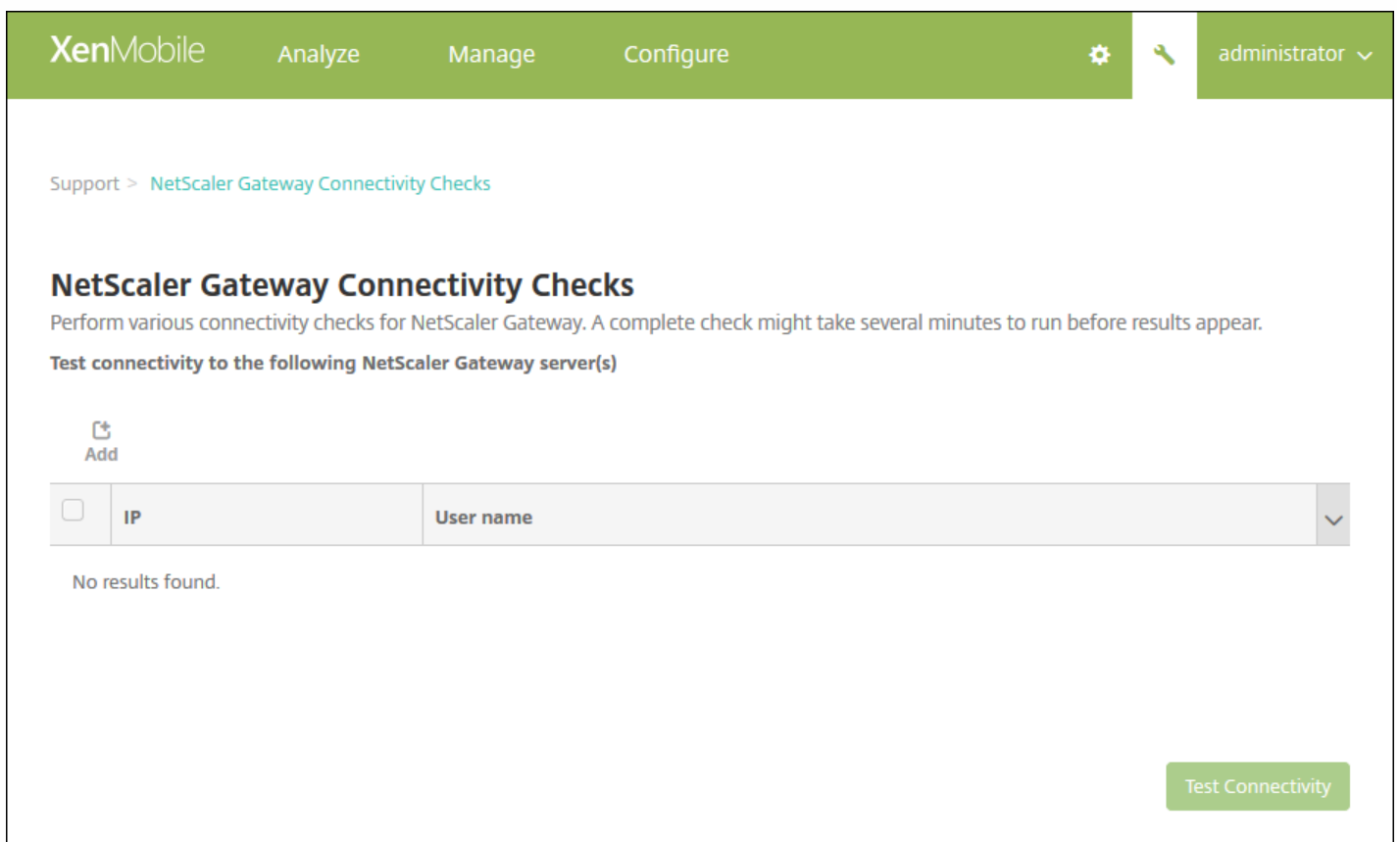
Clear Results Test Connectivity

3. 在测试结果表中选择一个服务器以查看该服务器的详细结果。



执行 NetScaler Gateway 连接检查

1. 在支持页面的**诊断**下面，单击 **NetScaler Gateway 连接检查**。此时将显示 **NetScaler Gateway 连接检查** 页面。如果尚未添加任何 NetScaler Gateway 服务器，此表格为空。



2. 单击**添加**。将显示**添加 NetScaler Gateway 服务器**对话框。

Add NetScaler Gateway Server

NetScaler Gateway Management IP*

User name*

Password*

Cancel Add

3. 在 **NetScaler Gateway 管理 IP** 中，键入运行要测试的 NetScaler Gateway 的服务器的管理 IP 地址。

注意：如果要对以前已添加的 NetScaler Gateway 服务器执行连接检查，系统会提供 IP 地址。

4. 键入关于此 NetScaler Gateway 的管理员凭据。

注意：如果要对以前已添加的 NetScaler Gateway 服务器执行连接检查，系统会提供用户名。

5. 单击**添加**。此 NetScaler Gateway 将添加到 **NetScaler Gateway 连接检查** 页面上的表格中。

6. 选择 NetScaler Gateway 服务器，然后单击**测试连接**。结果将显示在测试结果表格中。

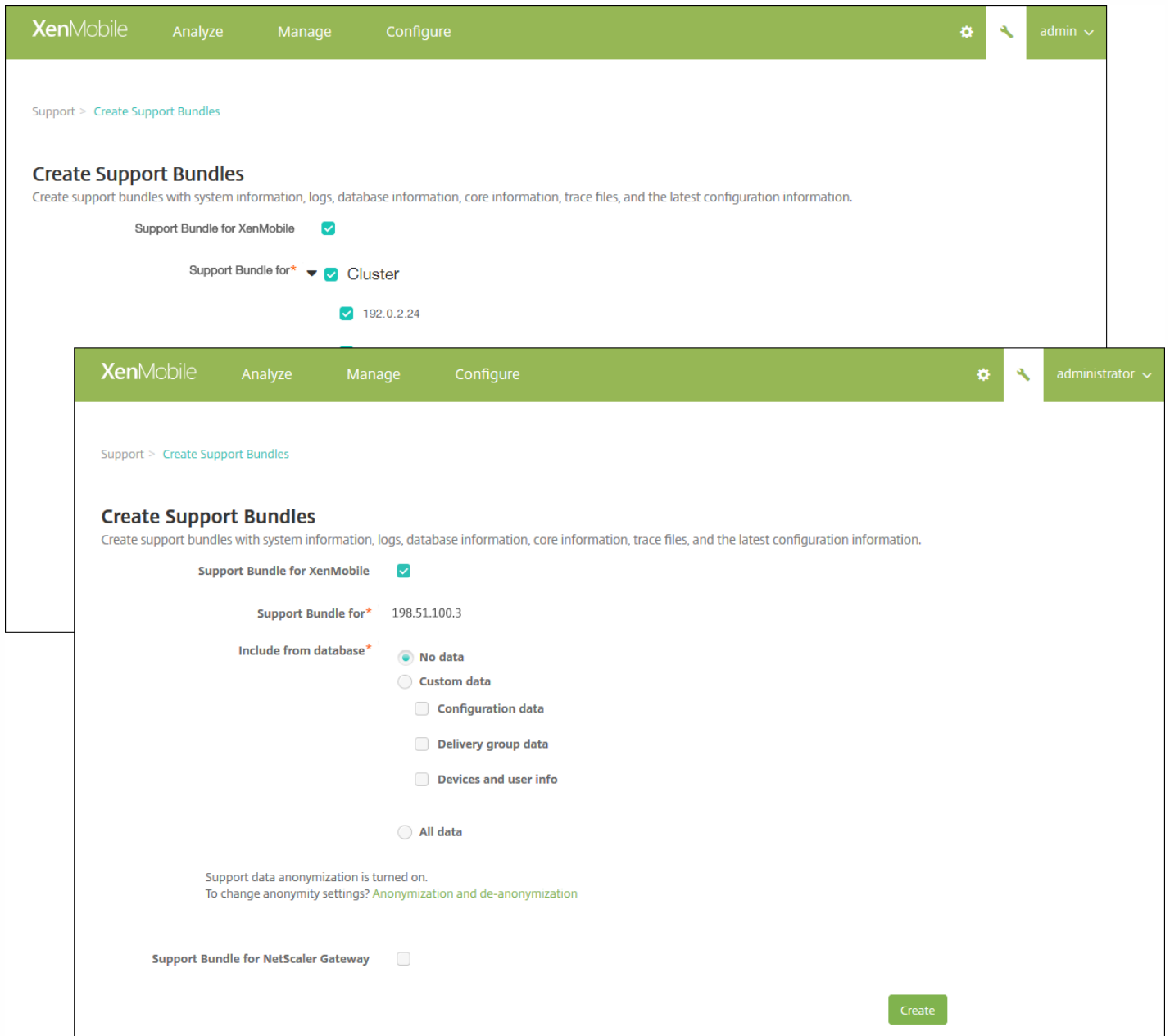
7. 在测试结果表中选择一个服务器以查看该服务器的详细结果。

支持包

Feb 27, 2017

如果要向 Citrix 报告问题或排除故障，可以创建支持包，然后将支持包上传到 Citrix Insight Services (CIS)。

1. 在 XenMobile 控制台中，单击右上角的扳手图标。此时将显示支持页面。
2. 在支持页面上，单击**创建支持包**。此时将显示创建支持包页面。如果 XenMobile 环境包含加入群集的节点，将显示所有节点。

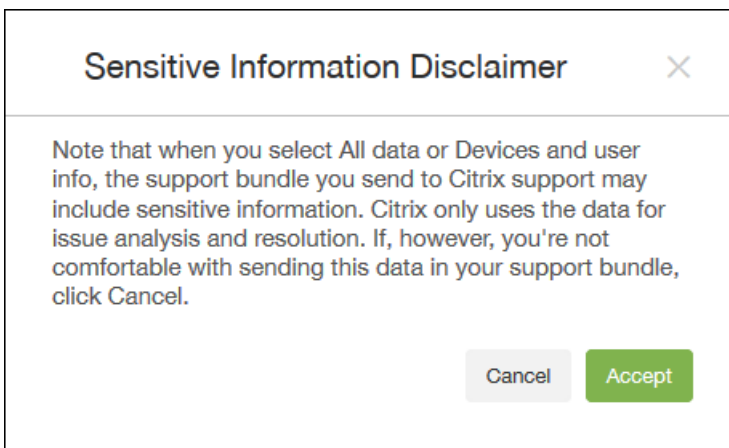


3. 确保选中适用于 **XenMobile** 的支持包复选框。
4. 如果 XenMobile 环境包含群集节点，在适用于此对象的支持包中，可以选择所有节点或任何节点组合，用于从中提取数据。

5. 在包含的数据库内容中，执行以下操作之一：

- 单击无数据。
- 单击自定义数据，然后选择以下任意选项或全部选项（默认情况下，选择所有选项）：
 - 配置数据库：包括证书配置和设备管理器策略。
 - 交付组数据：包括应用程序交付组信息，其中包含应用程序类型和应用程序交付策略详细信息。
 - 设备和用户信息：包括设备策略、应用程序、操作和交付组。
- 单击所有数据。

注意：如果选择设备和用户信息或所有数据，并且这是您创建的第一个支持包，则会显示敏感信息免责声明对话框。阅读免责声明，然后单击接受或取消。如果单击取消，支持包将无法上载到 Citrix。如果单击接受，则可以将支持包上载到 Citrix，并且下次创建包含设备或用户数据的支持包时不会再出现免责声明。

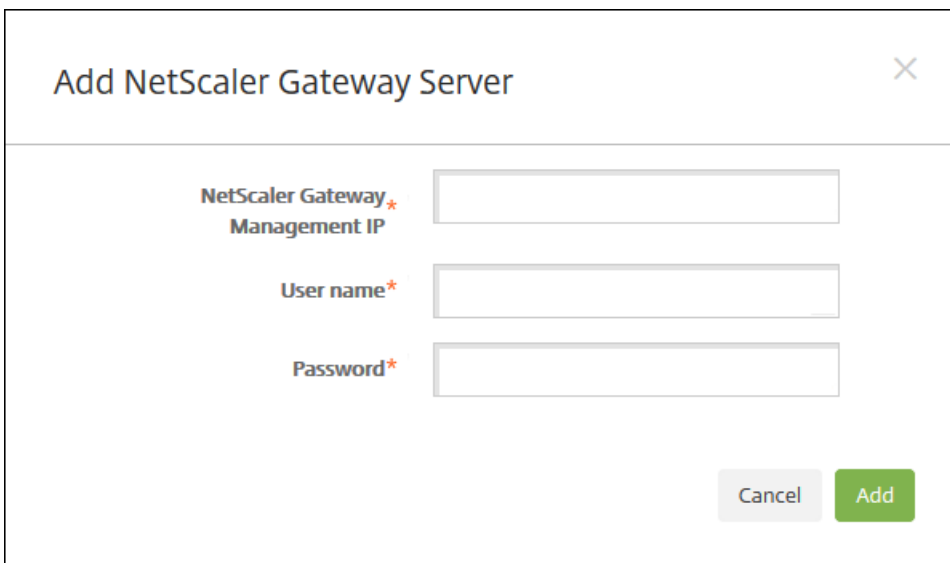


6. 支持数据匿名已打开选项指示默认设置是将数据匿名化处理，这意味着敏感用户、服务器和网络数据在支持包中进行匿名化处理。

要更改此设置，请单击匿名和取消匿名。有关数据匿名的详细信息，请参阅[在支持包中将数据匿名化处理](#)。

7. 如果要包含来自 NetScaler Gateway 的支持包，请选中适用于 **NetScaler Gateway** 的支持包复选框，然后执行以下操作：

a. 单击添加。将显示添加 **NetScaler Gateway** 服务器对话框。



b. 在 **NetScaler Gateway 管理 IP** 中，键入要从中提取支持包数据的 NetScaler Gateway 的 NetScaler 管理 IP 地址。

注意：如果要从已经添加的 NetScaler Gateway 服务器创建支持包，系统会提供 IP 地址。

c. 在 **用户名和密码** 中，键入访问运行 NetScaler Gateway 的服务器所需的用户凭据。

注意：如果要从已经添加的 NetScaler Gateway 服务器创建支持包，系统会提供用户名。

7. 单击**添加**。新的 NetScaler Gateway 支持包将添加到表格中。

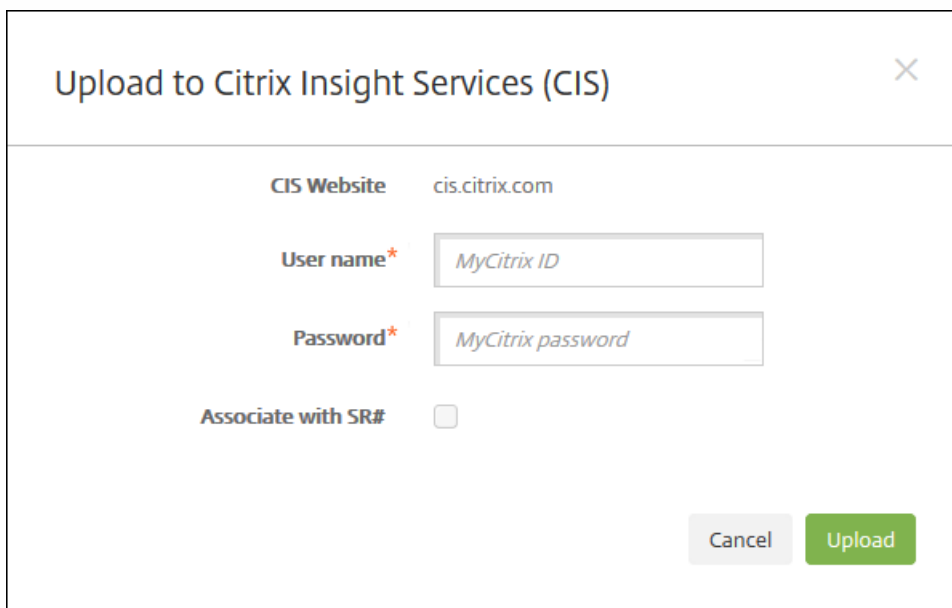
8. 重复步骤 7 以添加更多 NetScaler Gateway 支持包。

9. 单击**创建**。将创建支持包，并显示两个新按钮：**上载到 CIS** 和**下载到客户端**。

将支持包上载到 Citrix Insight Services

创建支持包后，可以将支持包上载到 Citrix Insight Services (CIS) 或将其下载到您的计算机。下面的步骤显示如何将支持包上载到 CIS。上载到 CIS 需要使用 MyCitrix ID 和密码。

1. 在**创建支持包**页面上，单击**上载到 CIS**。此时将显示**上载到 Citrix Insight Services (CIS)** 对话框。



Upload to Citrix Insight Services (CIS)

CIS Website cis.citrix.com

User name* MyCitrix ID

Password* MyCitrix password

Associate with SR#

Cancel Upload

2. 在**用户名**中，键入 MyCitrix ID。

3. 在**密码**中，键入 MyCitrix 密码。

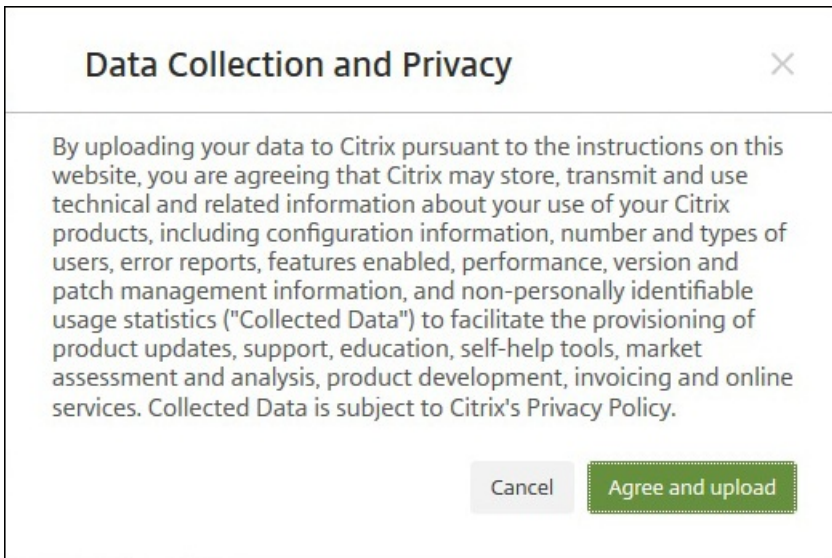
4. 如果要将此支持包与现有服务请求号码关联，请选中与 **SR 编号** 关联复选框，并在显示的两个新字段中执行以下操作：

- 在 **SR#** 中，键入要将此包关联到的八位数服务请求号码。
- 在 **SR 说明** 中，键入 SR 的说明。

5. 单击**上载**。

如果这是您第一次将支持包上载到 CIS，并且您尚未通过其他产品在 CIS 上创建帐户和接受“数据收集和隐私声明”协议，系统会

显示以下对话框；您必须接受此协议才能开始上载操作。如果您已经具有 CIS 帐户并且之前接受过此协议，支持包会立即开始上载。



6. 阅读协议，然后单击**同意并上载**。将上载支持包。

将支持包下载到您的计算机

创建支持包之后，可以将此包上载到 CIS 或将其下载到您的计算机。如果希望自己进行故障排除，可以将支持包下载到您的计算机。

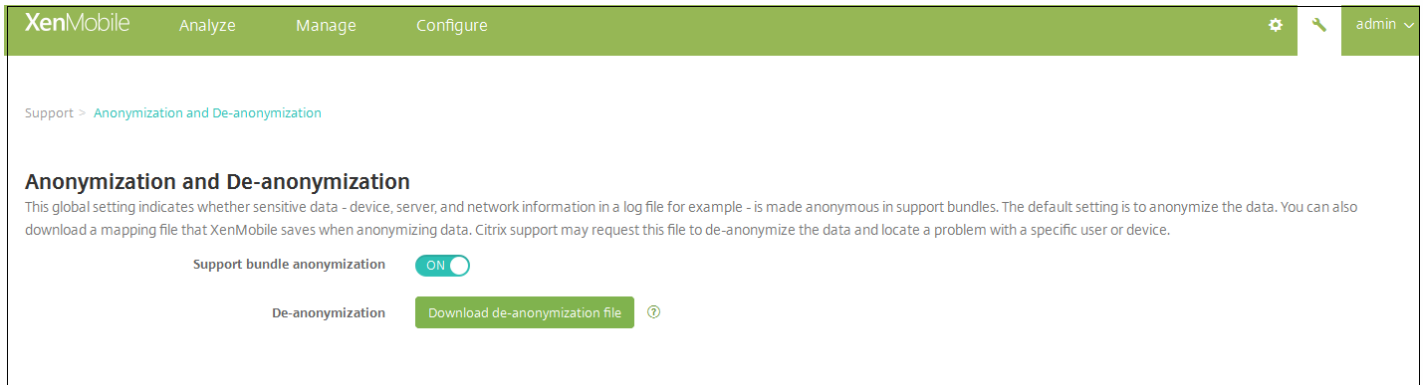
在创建支持包页面上，单击下载到客户端。支持包将下载到您的计算机。

匿名化支持包中的数据

Feb 27, 2017

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

1. 在 XenMobile 控制台中，单击右上角的扳手图标。此时将显示支持页面。
2. 在支持页面上的高级下方，单击匿名和取消匿名。此时将显示匿名和取消匿名页面。



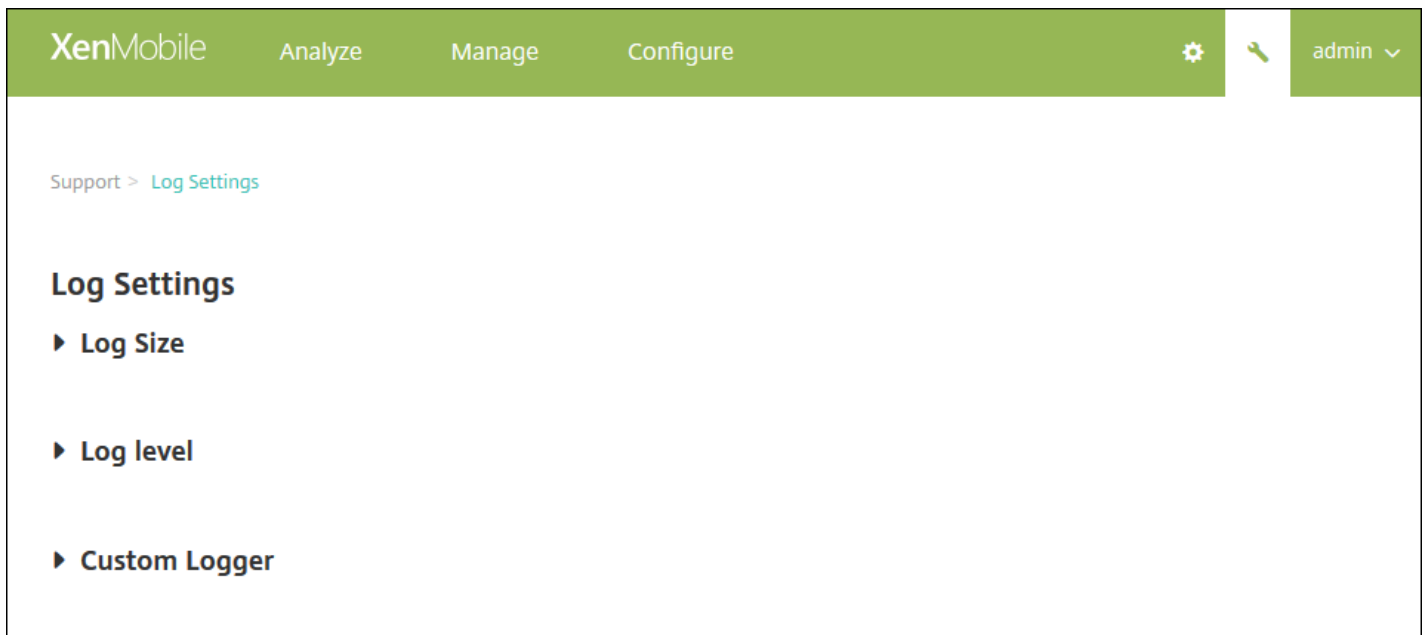
3. 在支持包匿名中，选择数据是否匿名。默认值为开。
4. 在取消匿名旁边，单击下载取消匿名文件以下载映射文件，在 Citrix 支持需要特定设备或用户信息来诊断问题时，将此文件发送给他们。

日志

Feb 27, 2017

您可以配置日志设置，以自定义 XenMobile 生成的日志的输出。如果您的 XenMobile 服务器已加入群集，则在 XenMobile 控制台中配置日志设置时，这些设置将与群集中的所有其他服务器共享。

1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。此时将显示支持页面。
2. 在日志操作下方，单击日志设置。此时将显示日志设置页面。

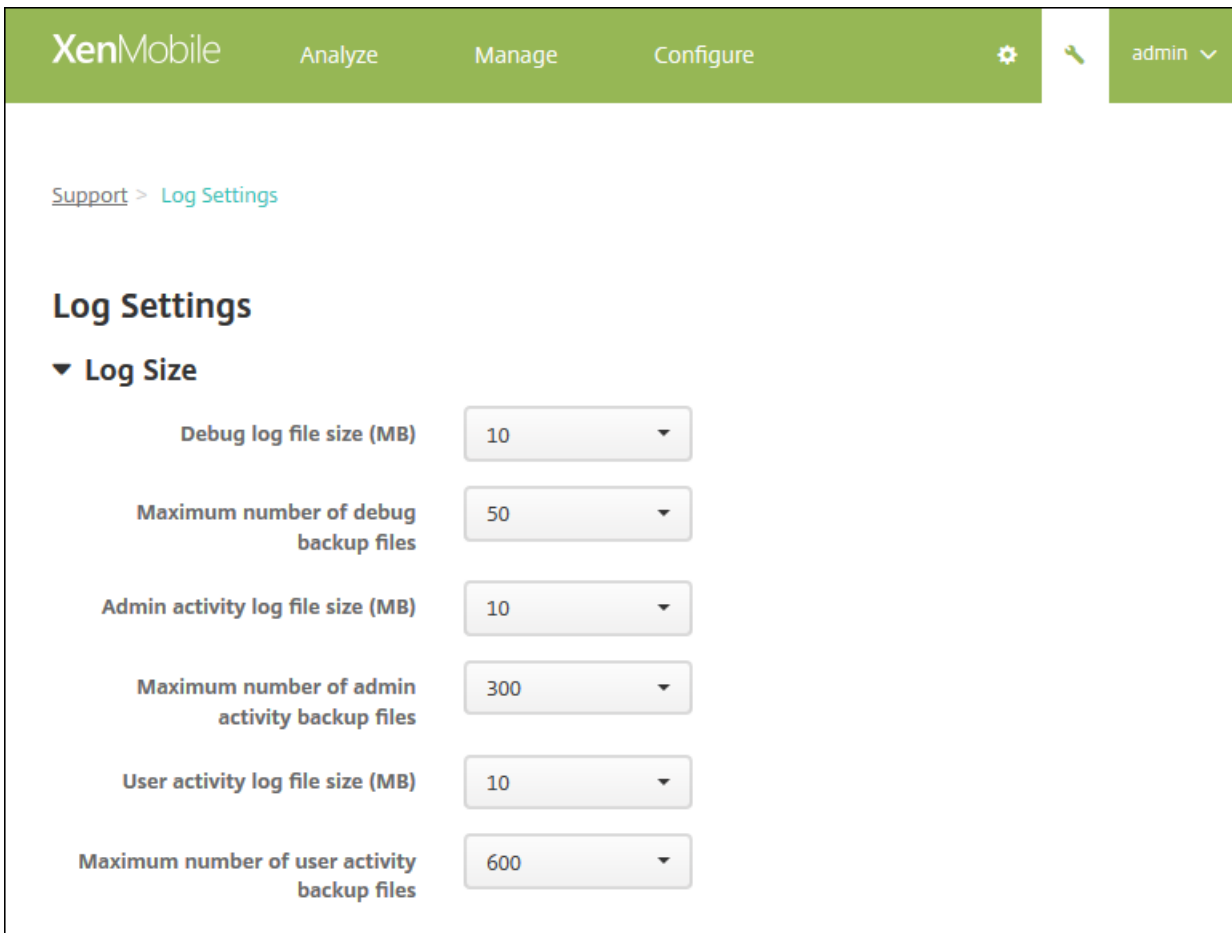


在日志设置页面上，可以访问以下选项：

- **日志大小。**使用此选项可以控制日志文件的大小和保留在数据库中的日志备份文件的最大数量。日志大小适用于 XenMobile 支持的每个日志（调试日志、管理活动日志和用户活动日志）。
- **日志级别。**使用此选项可将日志级别更改为静态设置。
- **自定义记录器。**使用此选项可以创建自定义的日志记录器；自定义日志需要一个类名称和日志级别。

配置“日志大小”选项

1. 在日志设置页面上，展开日志大小。






2. 配置以下设置：

- **调试日志文件大小(MB)**：在列表中，单击一个介于 5 MB 到 20 MB 之间的大小，以更改调试文件的最大大小。默认文件大小为 **10 MB**。
- **调试备份文件数上限**：在列表中，单击服务器保留的调试文件的最大数量。默认情况下，XenMobile 在服务器上保留 50 个备份文件。
- **管理活动日志文件大小(MB)**：在列表中，单击一个介于 5 MB 到 20 MB 之间的大小，以更改管理活动文件的最大大小。默认文件大小为 **10 MB**。
- **管理活动备份文件数上限**：在列表中，单击服务器保留的管理活动文件的最大数量。默认情况下，XenMobile 在服务器上保留 300 个备份文件。
- **用户活动日志文件大小(MB)**：在列表中，单击一个介于 5 MB 到 20 MB 之间的大小，以更改用户活动文件的最大大小。默认文件大小为 **10 MB**。
- **用户活动备份文件数上限**：在列表中，单击服务器保留的用户活动文件的最大数量。默认情况下，XenMobile 在服务器上保留 300 个备份文件。

配置“日志级别”选项

通过日志级别，您可以指定 XenMobile 在日志中收集的信息类别。可以为所有类别设置相同的级别，也可以将各个类别设置为特定的级别。

1. 在**日志设置**页面上，展开**日志级别**。此时将显示一个包含所有日志类别的表格。



XenMobile Analyze Manage Configure   admin 


Support > [Log Settings](#)

Log Settings

▶ Log Size

▼ Log level

 Edit all |  Reset

<input type="checkbox"/>	Class	Sub-class	Log level	
<input type="checkbox"/>	Data Access	All	Info	
<input type="checkbox"/>	Data Access	XDM	Info	
<input type="checkbox"/>	Data Access	XAM	Info	
<input type="checkbox"/>	Data Access	Console	Info	
<input type="checkbox"/>	Data Access	OCA	Info	
<input type="checkbox"/>	IMI Services	All	Info	
<input type="checkbox"/>	IMI Services	Category Service	Info	
<input type="checkbox"/>	IMI Services	OPN Service	Info	

2. 执行以下操作之一：

- 单击某个类别旁边的复选框，然后单击**设置级别**以仅更改此类别的日志级别。
- 单击**编辑全部**以对表格中的所有类别应用日志级别更改。

此时将显示**设置日志级别**对话框，您可以在该对话框中设置日志级别并选择是否在重新启动 XenMobile 服务器时保留日志级别设置。

- **类别名称**：如果要更改所有类别的日志级别，此字段将显示“全部”，否则将显示单个类别的名称；此字段不可编辑。
- **子类别名称**：如果要更改所有类别的日志级别，此字段将显示“全部”，否则将显示单个子类别的名称；此字段不可编辑。
- **日志级别**：在列表中，单击日志级别。支持的日志级别包括：
 - 致命
 - 错误
 - 警告
 - 信息
 - 调试
 - 跟踪
 - 关
- **包括记录器**：如果要更改所有类别的日志级别，此字段将为空，否则将显示单个类别的当前已配置的记录器；此字段不可编辑。
- **静态设置**：如果希望重新启动服务器时日志级别设置保持不变，请选中此复选框。未选中此复选框表示当您重新启动服务器时，日志级别设置将恢复为默认值。

3. 单击设置提交更改。

添加自定义日志记录器

1. 在日志设置页面上，展开自定义记录器。此时将显示自定义记录器表格。如果尚未添加任何自定义记录器，此表格最初为空。

Support > [Log Settings](#)

Log Settings

▶ Log Size

▶ Log level

▼ Custom Logger

 Add |  Set Level |  Delete

<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

Showing 1 - 2 of 2 items

2. 单击添加。此时将显示添加自定义记录器对话框。

Add custom logger ×

Class name

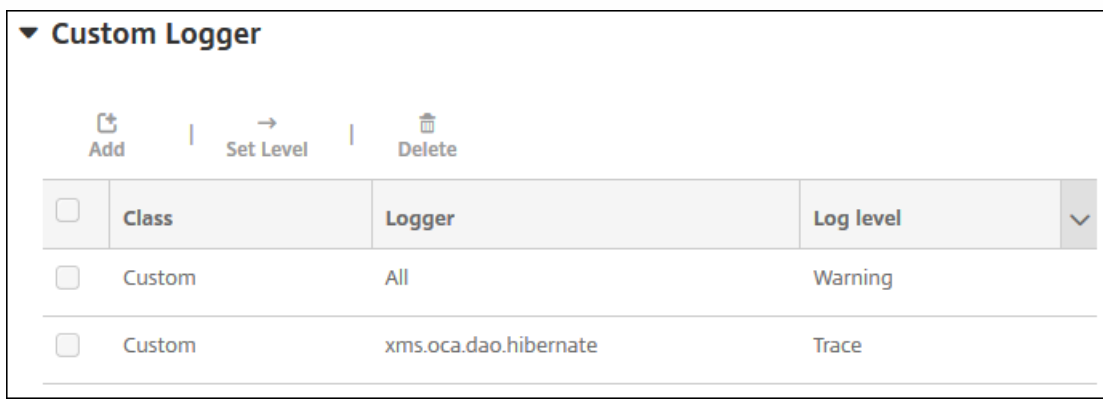
Log level

Included loggers

3. 配置以下设置：

- **类别名称**：此字段显示自定义；此字段不可编辑。
- **日志级别**：在列表中，单击日志级别。支持的日志级别包括：
 - 致命
 - 错误
 - 警告
 - 信息
 - 调试
 - 跟踪
 - 关
- **包括记录器**：键入要包含在自定义记录器中的特定记录器，或将此字段留空以包括所有记录器。

4. 单击添加。自定义记录器将添加到自定义记录器表格中。



<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

删除自定义日志记录器

1. 在日志设置页面上，展开自定义记录器。
2. 选择要删除的自定义记录器。
3. 单击**删除**。此时将显示一个对话框，询问您是否要删除该自定义日志记录器。单击**确定**。

重要：此操作无法撤消。

XenMobile Analyzer 工具

Apr 10, 2017

XenMobile Analyzer 是一个基于云的工具，可以使用该工具诊断与 XenMobile 的安装和其他功能有关的问题并进行故障排除。该工具检查您的 XenMobile 环境中是否存在设备或用户注册和身份验证问题。

将该工具配置为指向您的 XenMobile 服务器，并提供服务器部署类型、移动平台、身份验证类型以及用户凭据等信息。该工具随后将连接到服务器并扫描您的环境，检查是否存在配置问题。如果 XenMobile Analyzer 发现问题，该工具将提供更正问题的建议。

在本文中：

- [访问和启动 XenMobile Analyzer](#)
- [执行环境检查](#)
- [执行 NetScaler 检查](#)
- [向环境检查添加计划](#)
- [执行其他信息性检查](#)

主要功能

- 基于云的安全微服务，可对 XenMobile 相关的所有问题进行故障排除。
- 解决 XenMobile 配置问题的准确建议。
- 减少了支持呼叫数量以及加快了 XenMobile 环境的故障排除速度。
- 为 XenMobile 服务器版本提供零天支持。
- 能够安排每天或每周运行状况检查。
- NetScaler 配置检查。
- 执行 Secure Web 测试，确认能否访问 Intranet 站点。
- Secure Mail 自动发现服务检查。
- ShareFile 单点登录 (SSO) 检查。

访问和启动 XenMobile Analyzer

必备条件

产品	支持的版本
XenMobile 服务器	10.3.0 及更高版本
NetScaler Gateway	10.5 及更高版本
客户端注册模拟	iOS 和 Android

可以使用 My Citrix 凭据从 <https://xenmobiletools.citrix.com> 获取该工具。在打开的 XenMobile 管理工具页面上，要启动 XenMobile Analyzer，请单击 **Analyze and Troubleshoot my XenMobile Environment**（分析我的 XenMobile 环境并进行故障排除）。

All Management Tools

What do you want to do?

XenMobile Management Tools can help you troubleshoot your XenMobile Server set up and enable key features in your XenMobile deployment.

Analyze and
Troubleshoot my
XenMobile
environment

XenMobile Analyzer



Follow steps to identify and triage potential issues with your deployment.

Request Auto
Discovery

Auto Discovery Service



Request and Configure Auto Discovery for your domain's XenMobile Server.

Request push
notification
certificate
signature

Create APNs Certificate



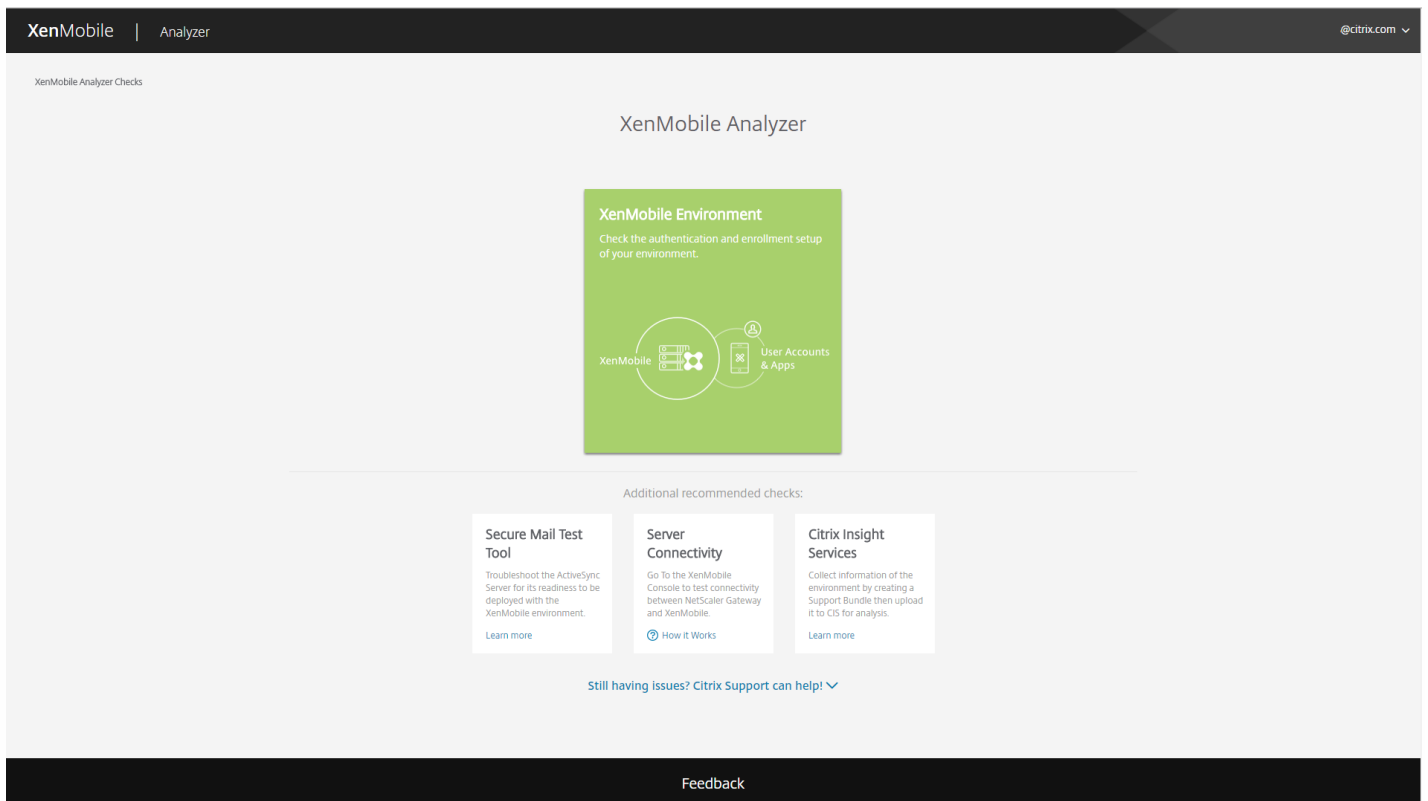
Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.

Enable APNs-based

XenMobile Analyzer 包含五个设计用于引导您完成会审过程以及减少支持票证数量的选项。这些选项可以降低每个人的成本。

这些选项如下所示：

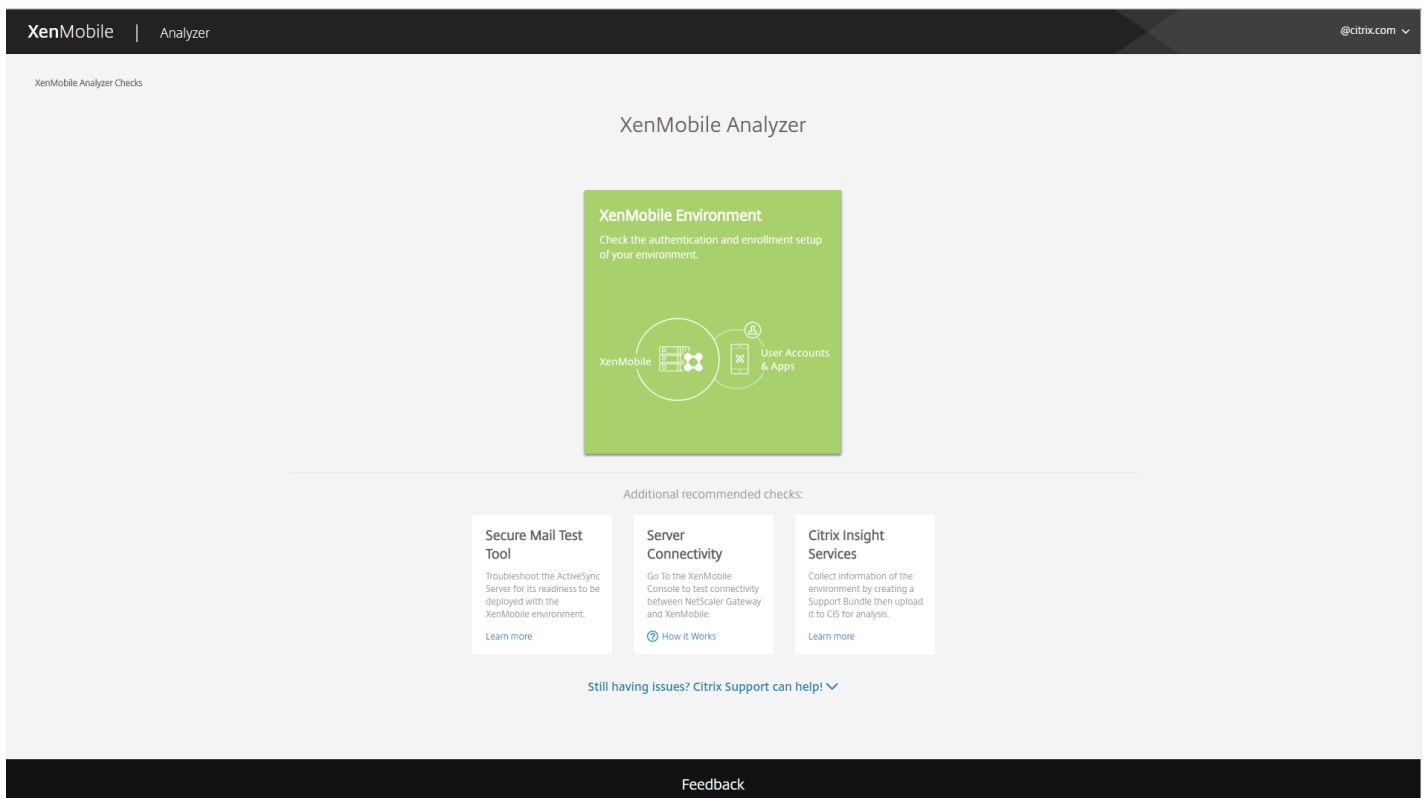
- **Environment Check** (环境检查) - 此步骤引导您设置测试以检查您的设置是否存在问题。此步骤还提供与设备、用户注册和身份验证问题有关的建议和解决方案。
- **NetScaler 检查** - 此步骤指导您检查您的 NetScaler 配置是否符合 XenMobile 部署就绪条件。
- **Advanced Diagnostics** (高级诊断) - 此步骤提供与使用 Citrix Insight Services 进一步查找环境检查可能错过的问题有关的信息。
- **Secure Mail Readiness** (Secure Mail 就绪)：此步骤指导您下载 XenMobile Exchange ActiveSync Test 应用程序。此工具用于帮助对 ActiveSync 服务器进行故障排除，以确认其是否已准备好在 XenMobile 环境中部署。
- **Server Connectivity Checks** (服务器连接检查) - 此步骤指导您测试服务器的连接。
- **Contact Citrix Support** (联系 Citrix 支持) - 如果您仍遇到问题，此步骤将您链接到能够在其中创建 Citrix 支持案例的站点。



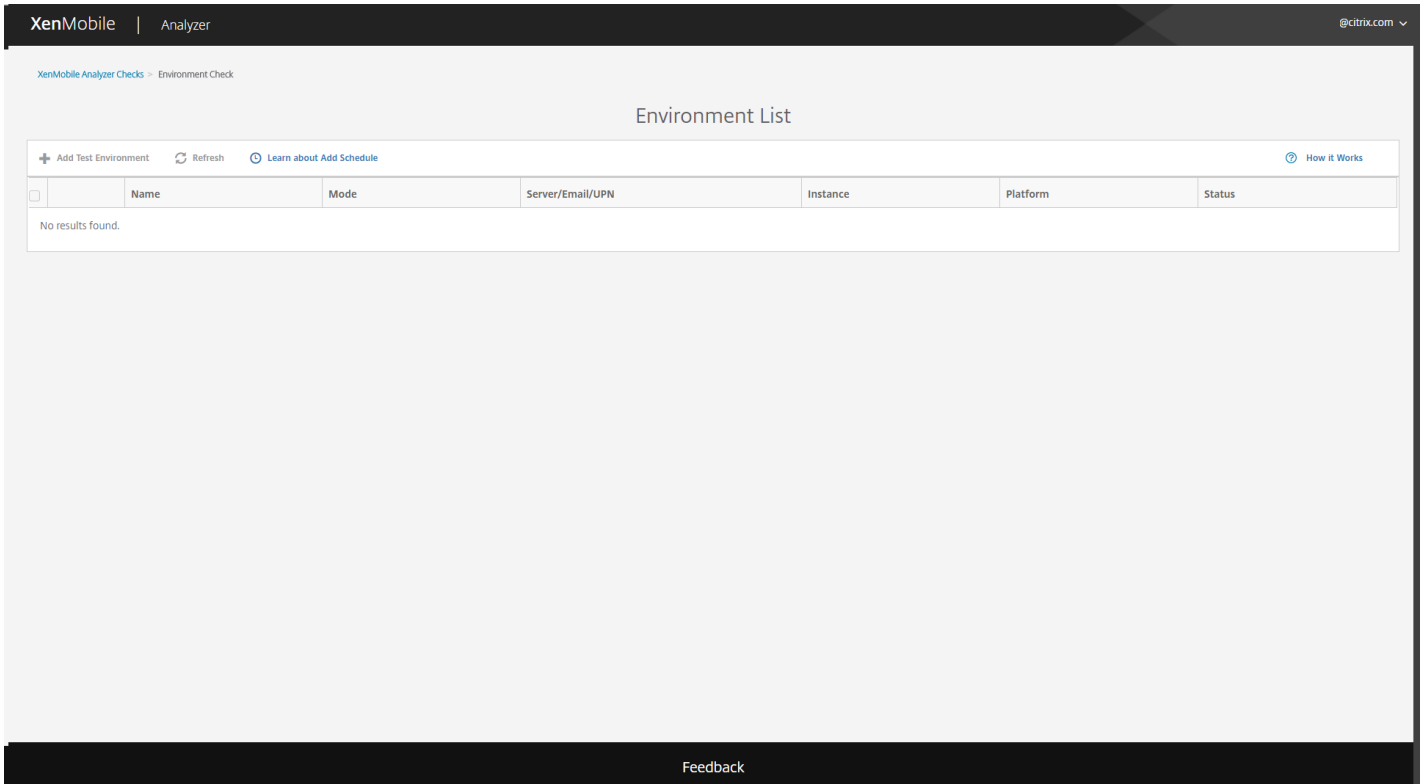
以下各节更加详细地介绍了每个选项。

执行环境检查

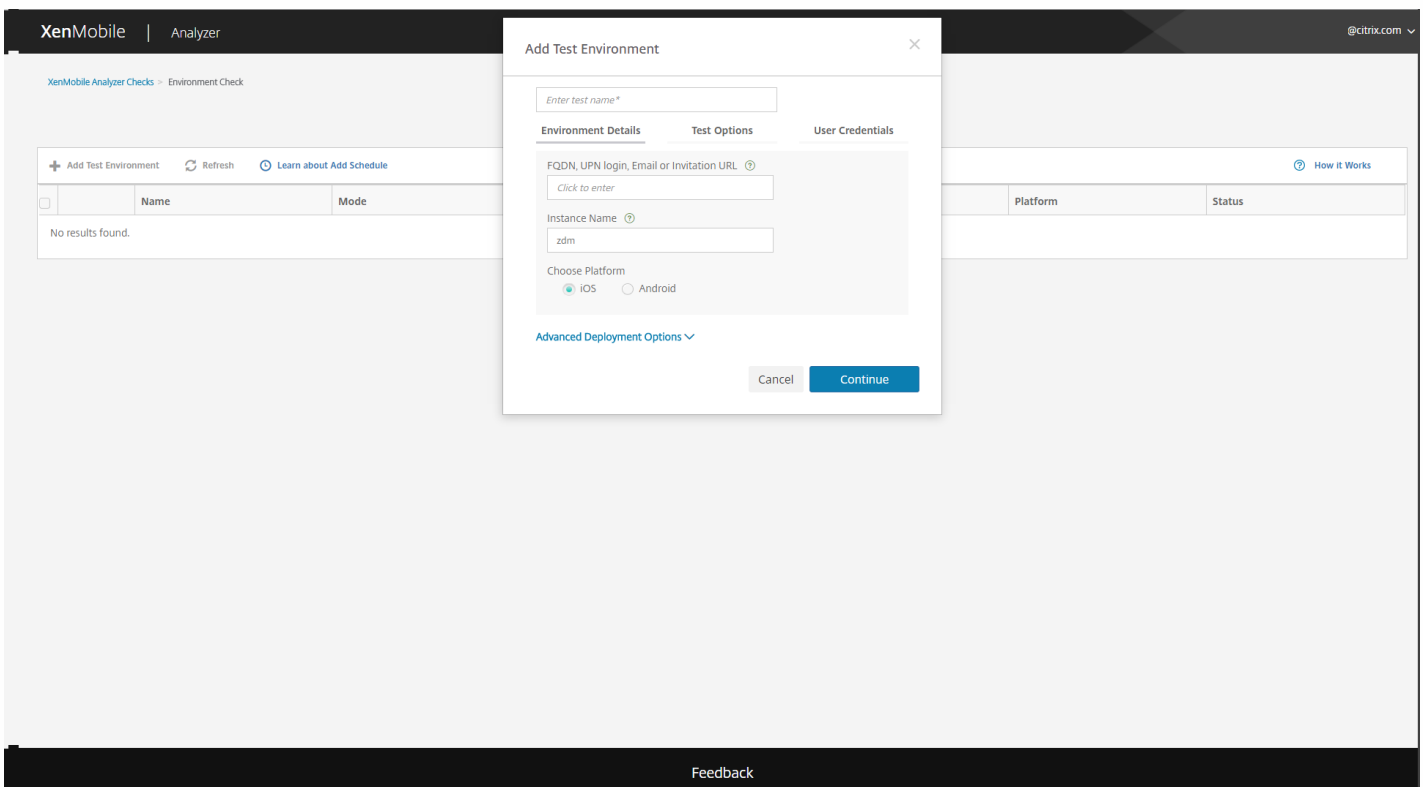
1. 登录 XenMobile Analyzer，然后单击 **Environment Checks**（环境检查）。



2. 单击 **Add Test Environment** (添加测试环境)。

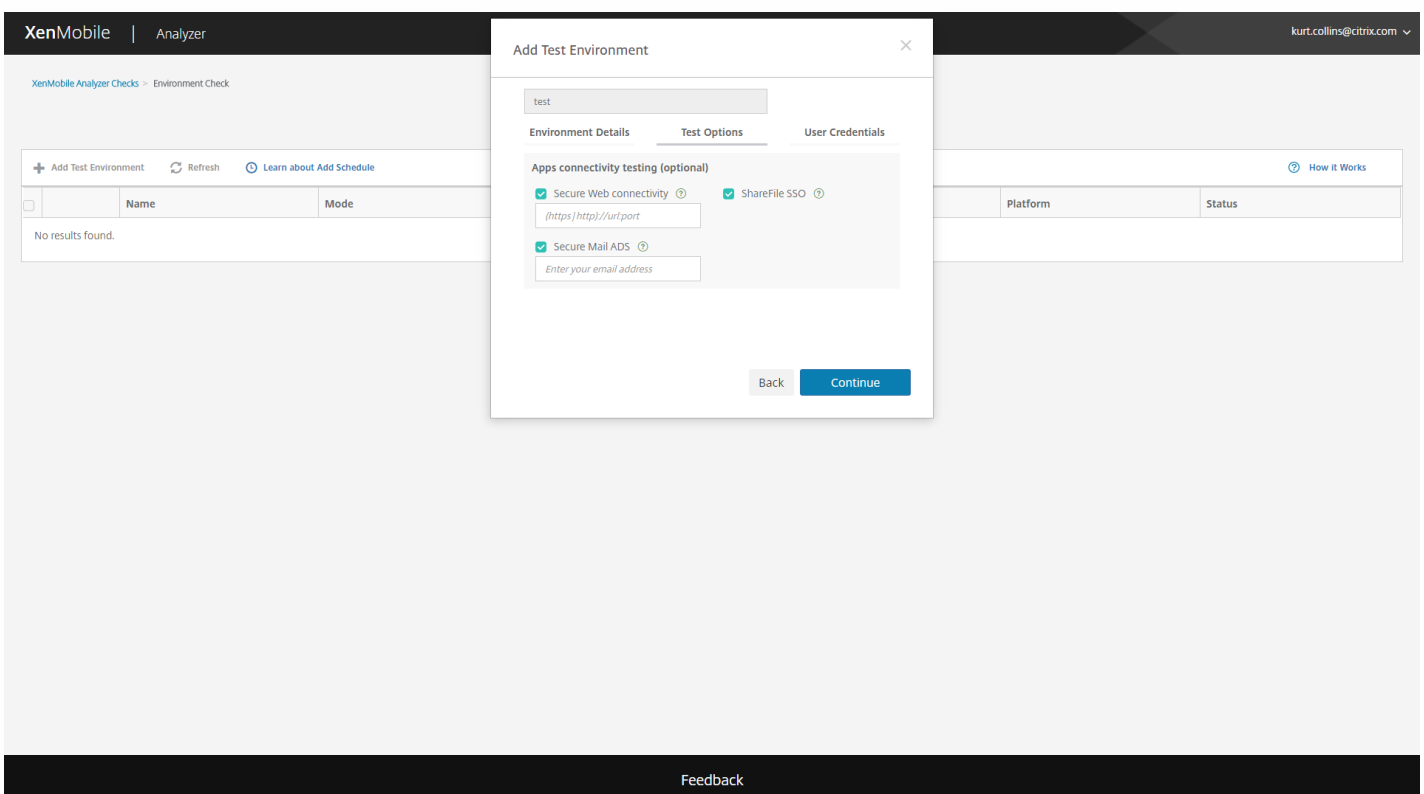


3. 在新的 **Add Test Environment** (添加测试环境) 对话框中，执行以下操作：



- a. 为测试提供将来能够帮助您识别测试的唯一名称。
- b. 在 **FQDN, UPN login, Email or URL Invitation** (FQDN、UPN 登录、电子邮件或 URL 邀请) 字段中, 输入访问服务器时使用的信息。
- c. 在 **XMS Instance** (XMS 实例) 中, 如果使用自定义实例, 则可以提供该值。
- d. 在 **Choose Platform** (选择平台) 中, 选择 **iOS** 或 **Android** 作为测试平台。
- e. 如果展开 **Advanced Deployment Options** (高级部署选项), 则可以在 **Deployment Mode** (部署模式) 列表中选择您的 XenMobile 部署模式。可用选项为 **Enterprise (MDM + MAM)** (企业(MDM + MAM))、**App Management (MAM)** (应用程序管理(MAM)) 或 **Device Management (MDM)** (设备管理(MDM))。

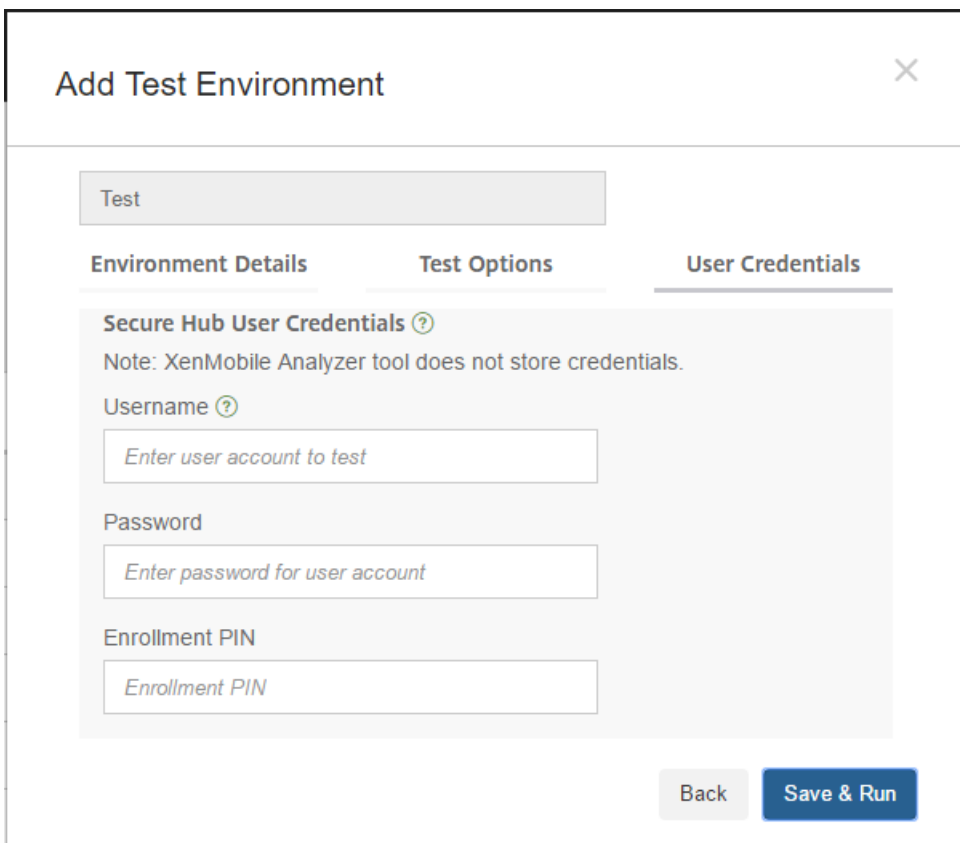
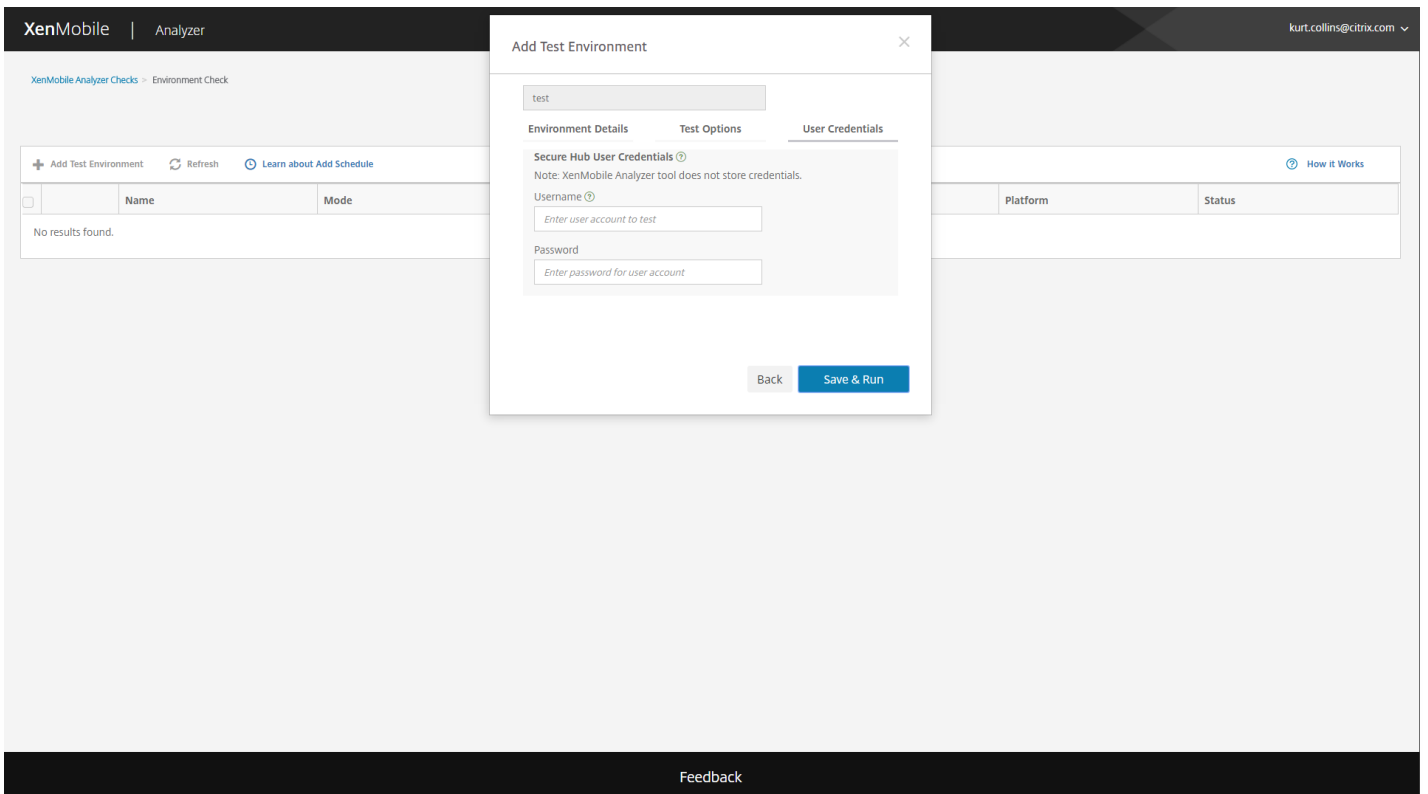
4. 单击 **Continue** (继续)。



5. 可以选择要运行的应用程序级别测试。可以选择以下一个或多个测试。

- a. **Secure Web 连接**。提供 Intranet URL。该工具测试该 URL 能否访问。在尝试访问 Intranet URL 期间, 此测试会检测 Secure Web 应用程序中是否可能发生任何连接问题。
- b. **Secure Mail ADS**。提供用户电子邮件 ID。此 ID 用于测试在 XenMobile 环境中自动发现 Microsoft Exchange Server 的情况。它检测是否存在与 Secure Mail 自动发现有关的任何问题。
- c. **ShareFile SSO**。如果选择此项, XenMobile Analyzer 会测试 ShareFile DNS 能否成功解析以及 ShareFile 单点登录 (SSO) 是否与提供的用户凭据兼容。

6. 单击 **Continue** (继续)。



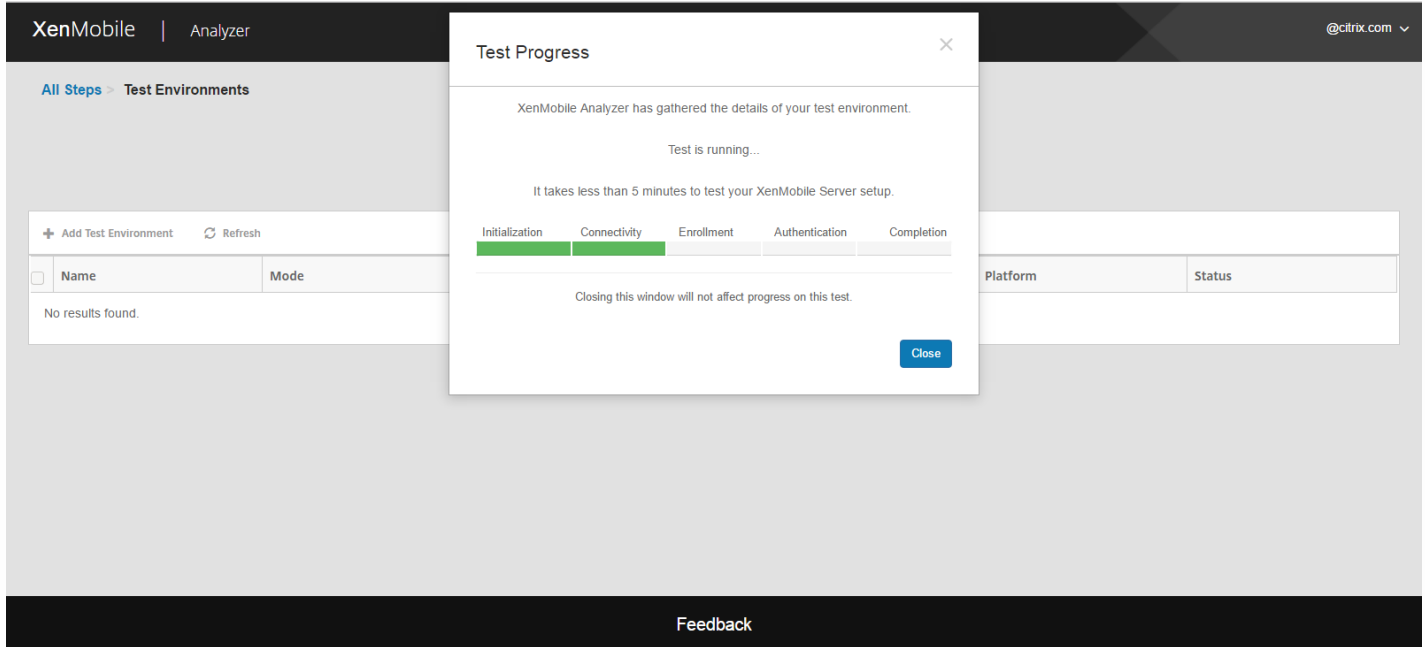
7. 您可能会看到不同字段可用于输入用户凭据，具体取决于您的服务器设置。可能的字段为只包含 **Username**（用户名）、**Username**（用户名）和 **Password**（密码）或 **Username**（用户名）、**Password**（密码）和 **Enrollment**

PIN (注册 PIN) 。

8. 输入此信息后，单击 **Save & Run** (保存并运行) 开始测试。

此时将显示进度通知。可以让将进度对话框保留在打开状态，也可以关闭该对话框，测试将继续运行。

通过的测试将显示为绿色。失败的测试将显示为红色。



8. 在关闭进度对话框之后，可以返回到 **Environments List** (环境列表) 页面，并单击 **View Report** (查看报告) 图标查看测试结果。

Results (结果) 页面显示“Test Details” (测试详细信息)、“Recommendations” (建议) 和“Results” (结果)。

XenMobile | Analyzer kurt.collins@citrix.com

XenMobile Analyzer Checks - Environment Check - Report

This test is not yet on a schedule. [Add Schedule](#) to run test in a selected frequency. [Learn more](#).

Check Report

Check Complete: No Issues Found

Check Summary

Test Environment: test
 Start Time: 2017-Mar-28 12:44 PM UTC
 Deployment Mode: Citrix XenMobile Enterprise Edition
 Server FQDN: kurt.collins@citrix.com
 Platform: IOS

[Add Schedule](#) [Run Again](#)

Do you need assistance?

[Citrix Support is here to help!](#)

For additional information, please refer to the [Support Knowledge Center](#).
 Download and share this report with your Citrix Support contact.

[Download Report](#)

Next, continue troubleshooting the XenMobile Environment using additional recommended checks:
[Troubleshoot the ActiveSync server using Secure Mail Test Tool.](#)
 Test [connectivity](#) of XenMobile Server and NetScaler Gateway.
[Analyze logs and scan for known issues](#) using Citrix Insight Services.

[Go to XenMobile Analyzer Checks](#)

Detailed Results View all details of your test

	Category	Checks	Results
✓	Initialization and Connectivity	XenMobile Server FQDN DNS Resolution	Pass
		XenMobile Server FQDN Connectivity	Pass
		XenMobile Server Certificate Validation	Pass
		XenMobile Server instance name validation	Pass
✓	Enrollment	Enrollment Authentication	Pass
		XenMobile Enrollment	Pass
✓	Authentication	Is NetScaler Gateway configured?	Yes
		NetScaler Gateway Cert Auth Enabled?	No
		NetScaler Gateway DNS Resolution	Pass
		NetScaler Gateway Connectivity	Pass

Feedback

XenMobile | Analyzer @citrix.com

✓	Authentication	NetScaler Gateway DNS Resolution	Pass
		NetScaler Gateway Connectivity	Pass
		NetScaler Gateway Certificate Validation	Pass
		NetScaler Gateway Login	Pass
		XenMobile Server connectivity through NetScaler Gateway	Pass
		XenMobile Server Authentication	Pass
✓	App Enumeration	Store Connectivity	Pass
		Device Registration	Pass
		Store App Listing	Pass
		Secure Mail - Deprecated - Use A...	Pass
		Secure Notes - Deprecated - Use ...	Pass
		Podio	Pass
		ShareConnect - Deprecated - Use...	Pass
		NotePad++	Pass
		ScanDirect - Public Store	Pass
		Secure Forms - Public Store	Pass
	Secure Notes - Public Store	Pass	
	Secure Tasks - Public Store	Pass	
	ShareConnect - Public Store	Pass	
	ShareFile - Public Store	Pass	
	Secure Web - Deprecated - Use A...	Pass	
⚠	Secure Web Connectivity	NetScaler Gateway DNS Resolution	Not Tested
		NetScaler Gateway server connectivity	Not Tested
✓	ShareFile	ShareFile Subdomain Discovery	Pass
		ShareFile SAML SSO	Pass
⚠	Secure Mail ADS	Secure Mail Auto Discovery	Not Tested
✓	Logout	XenMobile Server Logout	Pass
		NetScaler Gateway Logout	Pass

Feedback

如果任何建议都有与之关联的 Citrix 知识库文章，相应的文章将在此页面上列出。

9. 单击 **Results** (结果) 选项卡显示该工具执行的各个类别和测试及其结果。

- a. 要下载报告，请单击 **Download Report**（下载报告）。
- b. 要返回测试环境列表，请单击 **Environment Check**（环境检查）。
- c. 要重新运行同一个测试，请单击 **Run Again**（重新运行）。
- d. 如果要重新运行另一个测试，请返回 **Test Environments**（测试环境），选择测试，然后单击 **Start Test**（开始测试）。
- e. 要选择另一个 XenMobile Analyzer 选项，请单击 **Go To XenMobile Analyzer Checks**（转到 XenMobile Analyzer 检查）。

XenMobile | Analyzer @citrix.com

All Steps > Test Environments

Test Environment List

Test your server setup before deploying

+ Add Test Environment Refresh Delete Start Test View Report

<input type="checkbox"/>	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input checked="" type="checkbox"/>	RGTE	Citrix XenMobile Enterprise Edition	rgte.xm.citrix.com	zdm	iOS	Completed: Issues Found

Showing 1 - 1 of 1 items Items per page: 10

Feedback

10. 在“Test Environments”（测试环境）页面上，可以复制并编辑测试。为此，请选择一个测试，然后单击 **Duplicate and Edit**（复制并编辑）。此时会创建所选测试的副本，并打开“Add Test Environment”（添加测试环境）对话框，从而允许您修改新测试。

XenMobile | Analyzer testuser

All Steps > Test Environments

Test Environment List

Test your server setup before deploying

+ Add Test Environment Refresh

<input type="checkbox"/>	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input type="checkbox"/>	a_xms97_mam(Duplicate2)	Citrix XenMobile Enterprise Edition	xms97.blrcit.com	zdm	iOS	Completed: No Issues Found
<input checked="" type="checkbox"/>	a_xms97_mam(Duplicate)	Citrix XenMobile Enterprise Edition				Completed: No Issues Found
<input type="checkbox"/>	a_xms97_mam	Citrix XenMobile App Edition				Completed: No Issues Found
<input type="checkbox"/>	xms97_mam	Citrix XenMobile App Edition	xms97.blrcit.com	zdm	iOS	Completed: No Issues Found
<input type="checkbox"/>	CXM-21425	Citrix XenMobile MDM Edition	xms97.blrcit.com	zdm	Android	Completed: No Issues Found

Start Test View Report Duplicate and Edit Delete

XenMobile | Analyzer testuser ▾

All Steps > Test Environments

Test Environment List

Test your server setup before deploying


+ Add Test Environment Refresh ▶ Start Test View Report Duplicate and Edit Delete

<input type="checkbox"/>	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input checked="" type="checkbox"/>	a_xms97_mam(Duplicate2)	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	iOS	Completed: No Issues Found
<input type="checkbox"/>	a_xms97_mam(Duplicate)	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	a_xms97_mam	Citrix XenMobile App Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	xms97_mam	Citrix XenMobile App Edition	xms97.blrclt.com	zdm	iOS	Completed: No Issues Found

XenMobile | Analyzer testuser ▾

All Steps > Test Environments

Add Test Environment



Duplicating Test...

+ Add Test Environment Refresh

<input type="checkbox"/>	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input type="checkbox"/>	a_xms97_mam(Duplicate2)	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	iOS	Completed: No Issues Found
<input type="checkbox"/>	a_xms97_mam(Duplicate)	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	a_xms97_mam	Citrix XenMobile App Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	xms97_mam	Citrix XenMobile App Edition	xms97.blrclt.com	zdm	iOS	Completed: No Issues Found
<input type="checkbox"/>	CXM-21425	Citrix XenMobile MDM Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	xms195	Citrix XenMobile App Edition	xms195.blrclt.com	zdm	iOS	Completed: Issues Found
<input type="checkbox"/>	a_xms97	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	CXM-21364	Citrix XenMobile MDM Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	NSG logout	Citrix XenMobile Enterprise Edition	xms170.blrclt.com	zdm	Android	Completed: Issues Found
<input type="checkbox"/>	A_SB	Citrix XenMobile Enterprise Edition	rgte.xm.citrix.com	zdm	Android	Completed: No Issues Found

XenMobile | Analyzer testuser ▾

All Steps > Test Environments

Add Test Environment

Environment Details
Test Options
User Credentials

FQDN, UPN login, Email or Invitation URL ⓘ

Instance Name ⓘ

Choose Platform
 iOS Android

[Advanced Deployment Options ▾](#)

Cancel Continue

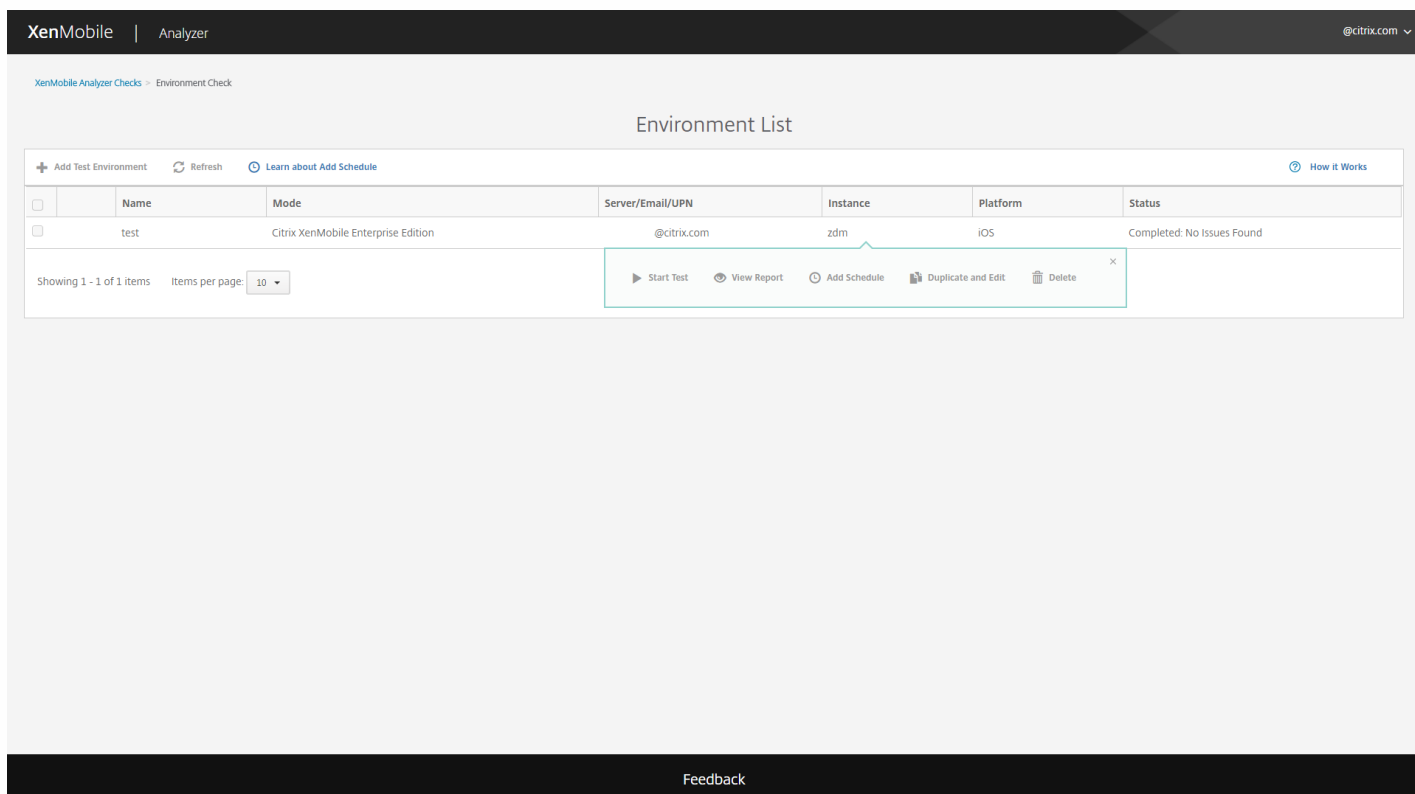
+ Add Test Environment Refresh

<input type="checkbox"/>	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input type="checkbox"/>	a_xms97_mam(Duplicate2)	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	iOS	Completed: No Issues Found
<input type="checkbox"/>	a_xms97_mam(Duplicate)	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	a_xms97_mam	Citrix XenMobile App Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	xms97_mam	Citrix XenMobile App Edition	xms97.blrclt.com	zdm	iOS	Completed: No Issues Found
<input type="checkbox"/>	CXM-21425	Citrix XenMobile MDM Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	xms195	Citrix XenMobile App Edition	xms195.blrclt.com	zdm	iOS	Completed: Issues Found
<input type="checkbox"/>	a_xms97	Citrix XenMobile Enterprise Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	CXM-21364	Citrix XenMobile MDM Edition	xms97.blrclt.com	zdm	Android	Completed: No Issues Found
<input type="checkbox"/>	NSG logout	Citrix XenMobile Enterprise Edition	xms170.blrclt.com	zdm	Android	Completed: Issues Found

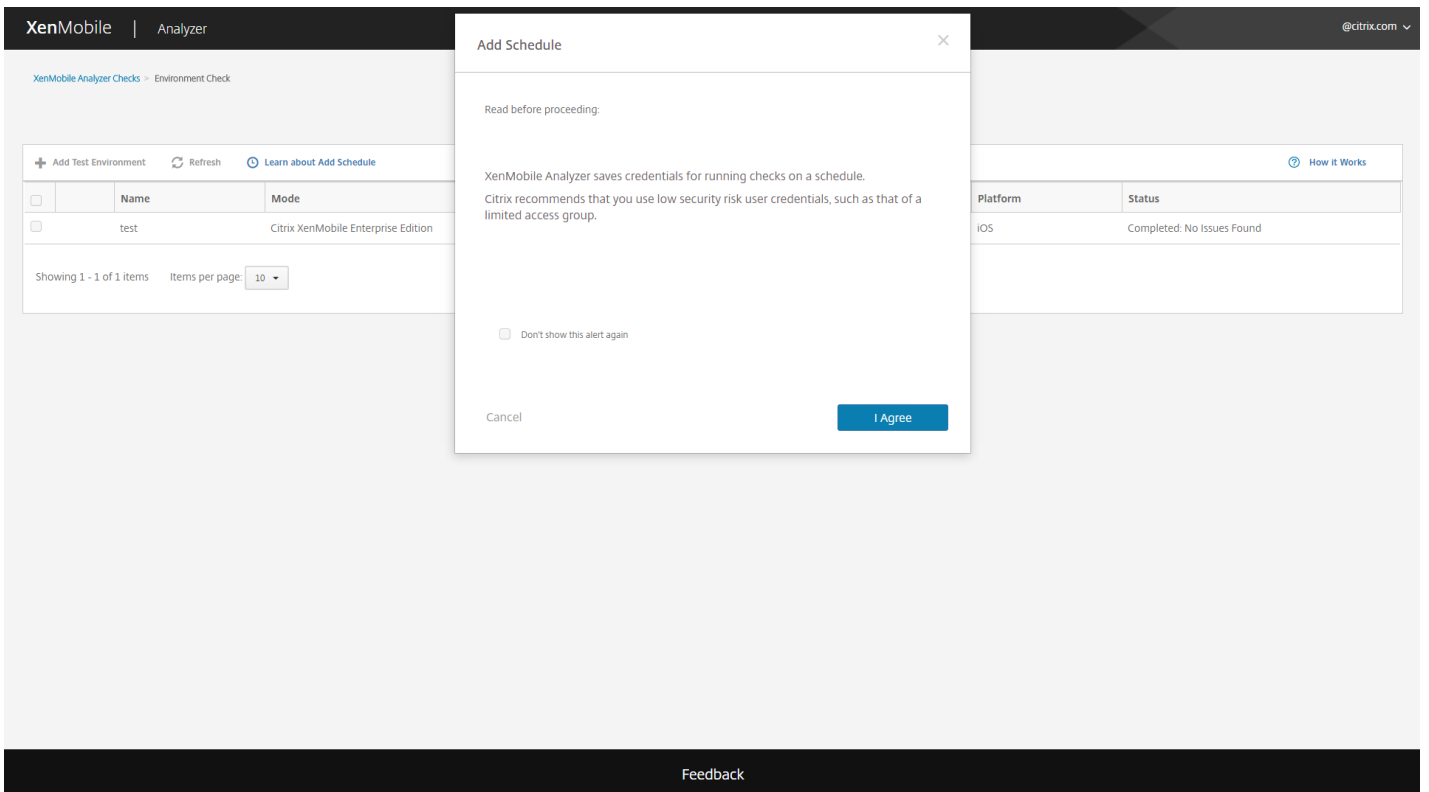
向环境检查添加计划

您可以将测试配置为按计划自动执行，且将结果发送给您配置的用户列表。

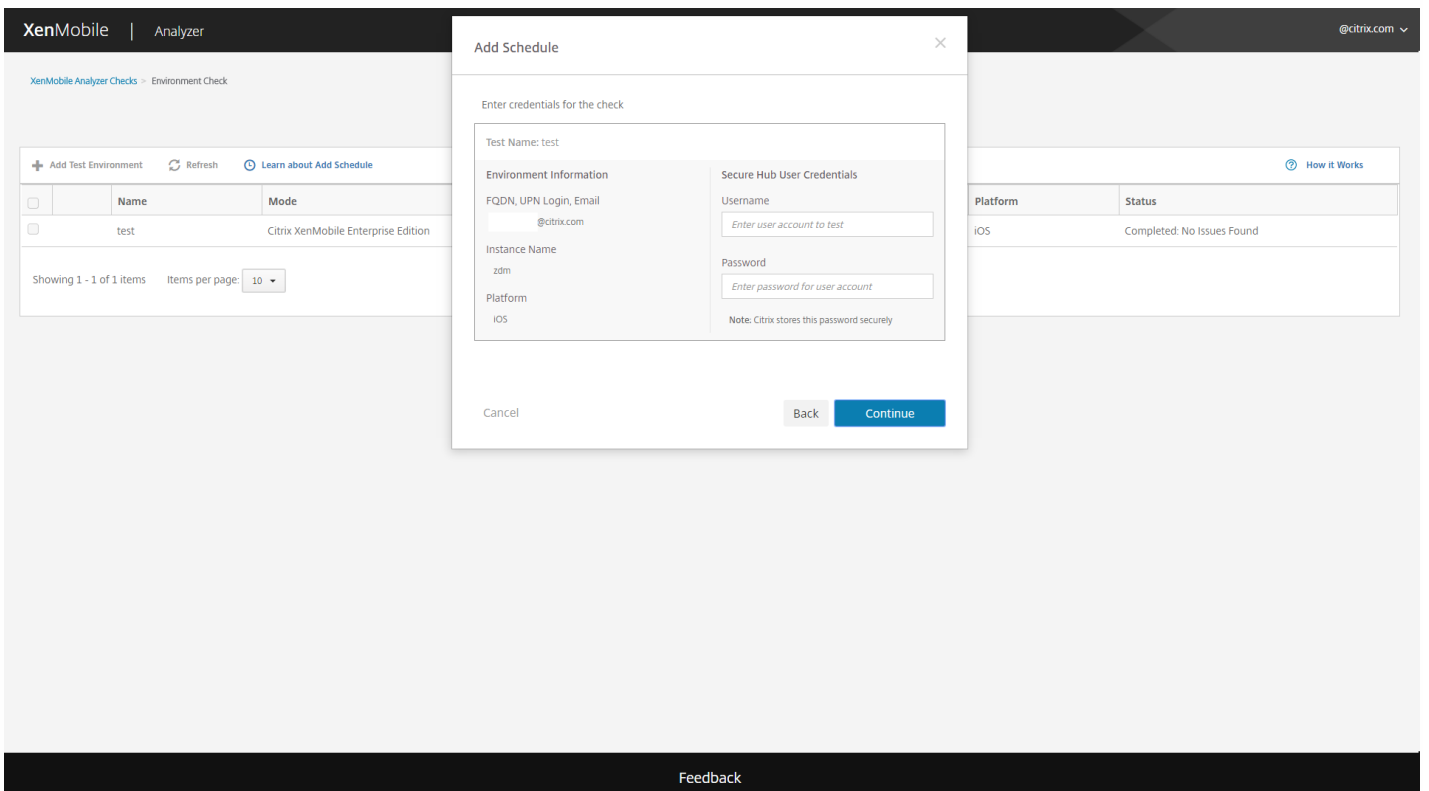
1. 在 **Environment List**（环境列表）页面上，选择您要为其设置计划的环境，并单击 **Add Schedule**（添加计划）。



2. **Add Schedule**（添加计划）窗口中将显示一条消息，提醒您 XenMobile Analyzer 会保存凭据用于按计划运行测试。Citrix 建议您使用具有有限访问权限的帐户来运行计划的测试。单击**我同意**继续。

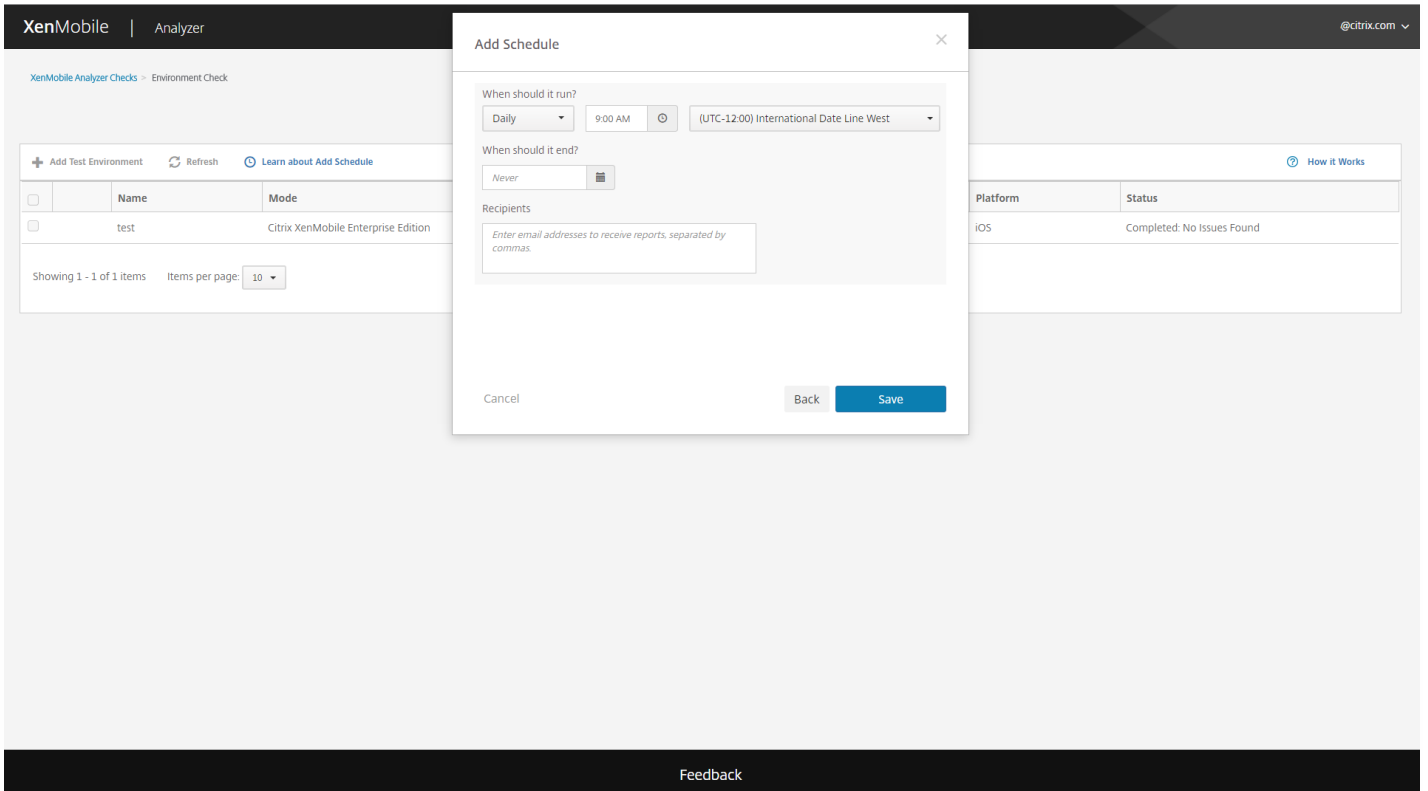


3. 输入用于运行测试的用户名和密码。

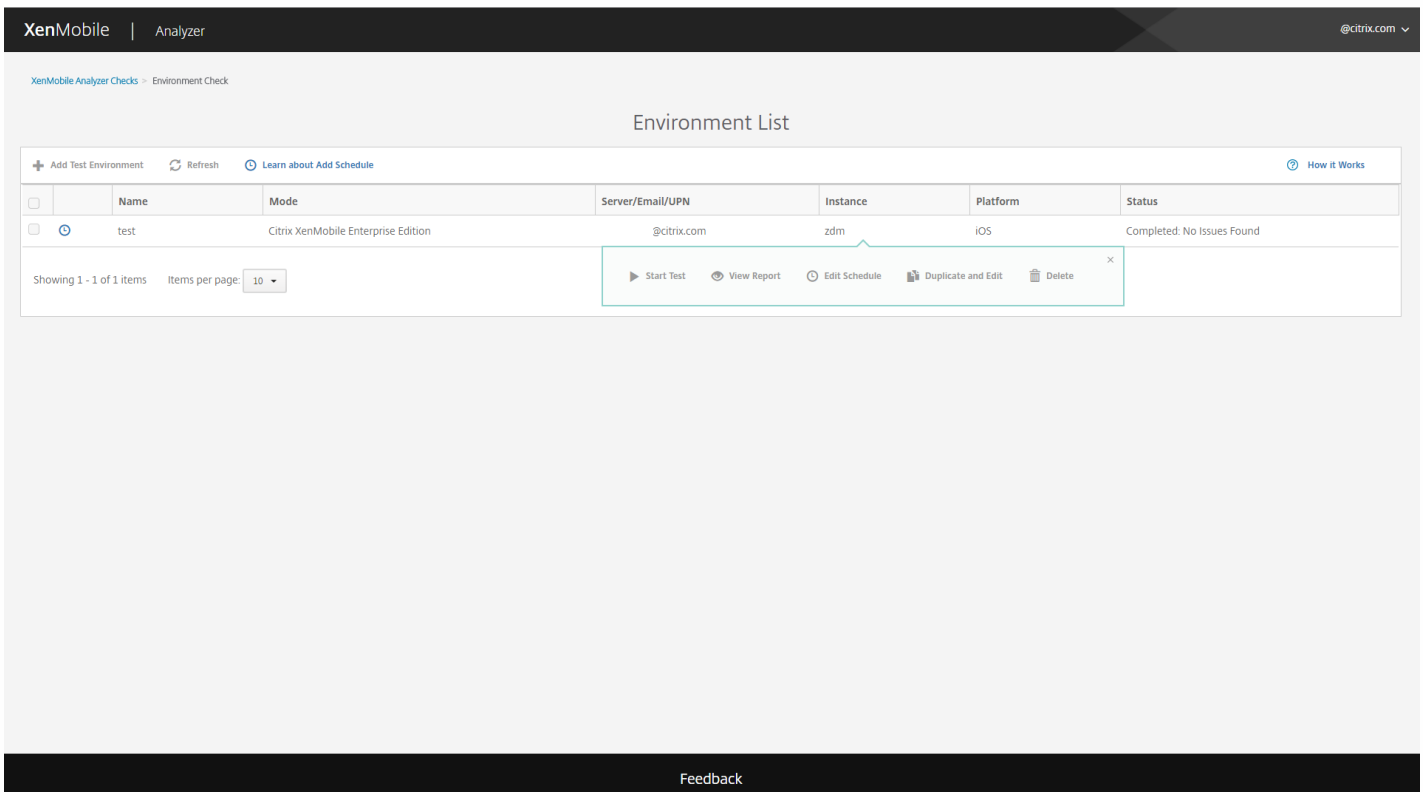


4. 配置测试的运行计划。您可以从下拉框中选择**每天**或**每周**。选择测试的运行时间和时区。可使用日期选取器来选择计划的测试停止运行的日期，或留空以让测试无限期地运行。请输入电子邮件地址列表（以逗号分隔）以接收报告。单击保

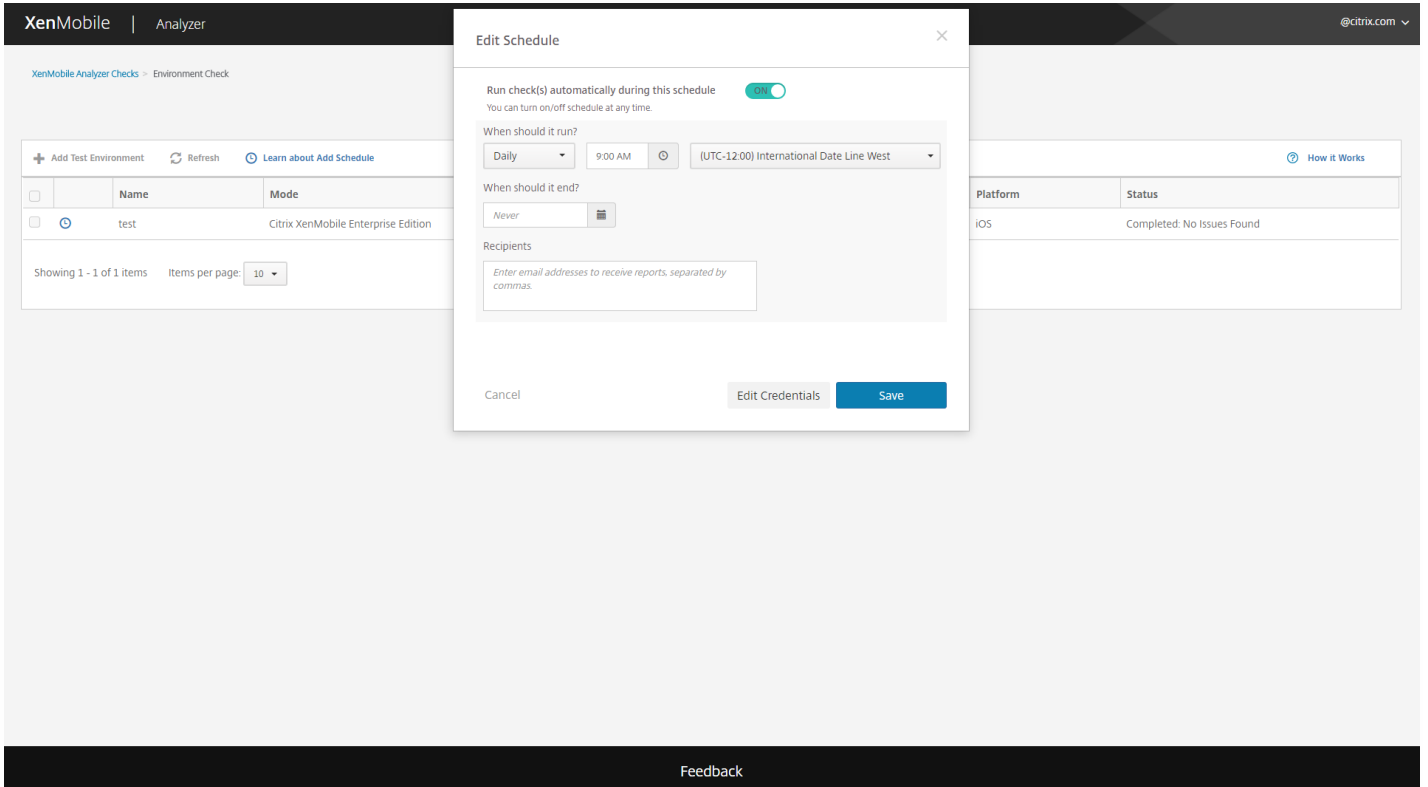
存。



5. 测试左侧的时钟符号表示配置了计划。如果您选择测试，您可以单击 **Edit Schedule**（编辑计划）更改测试运行时间。



6. 在此窗口中，您可以更改测试运行时间。您还可以单击顶部的开关来禁用它。完成时单击 **Save**（保存）。

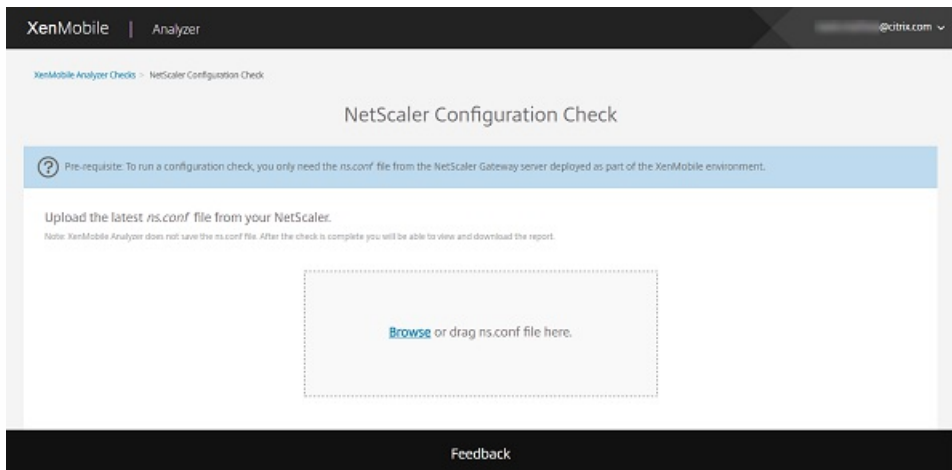


执行 NetScaler 检查

1. 登录到 XenMobile Analyzer，然后单击 **NetScaler Configuration**（NetScaler 配置）。



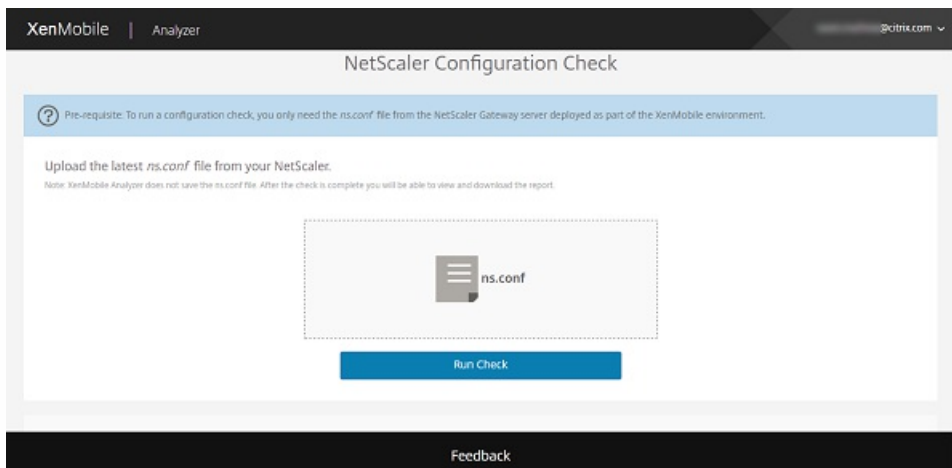
2. 上载您的 NetScaler 实例中的最新 ns.conf 文件。您可以将文件拖到上载框中，也可以单击 **Browse**（浏览）搜索并添加 ns.conf 文件。有关如何下载最新 ns.conf 文件的详细信息，请参阅[支持知识中心](#)。



注意

XenMobile Analyzer 不保存 ns.conf 文件。检查完成后，您可以查看和下载报告。

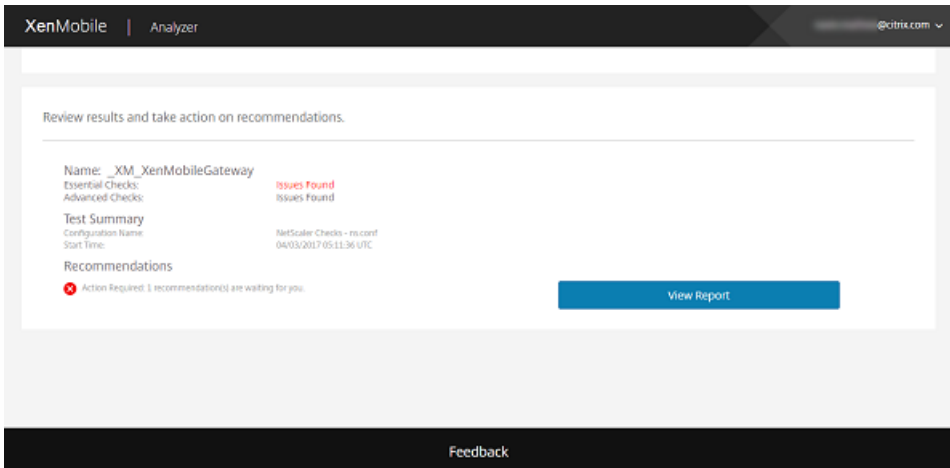
3. 单击 **Run Check** (运行检查)。



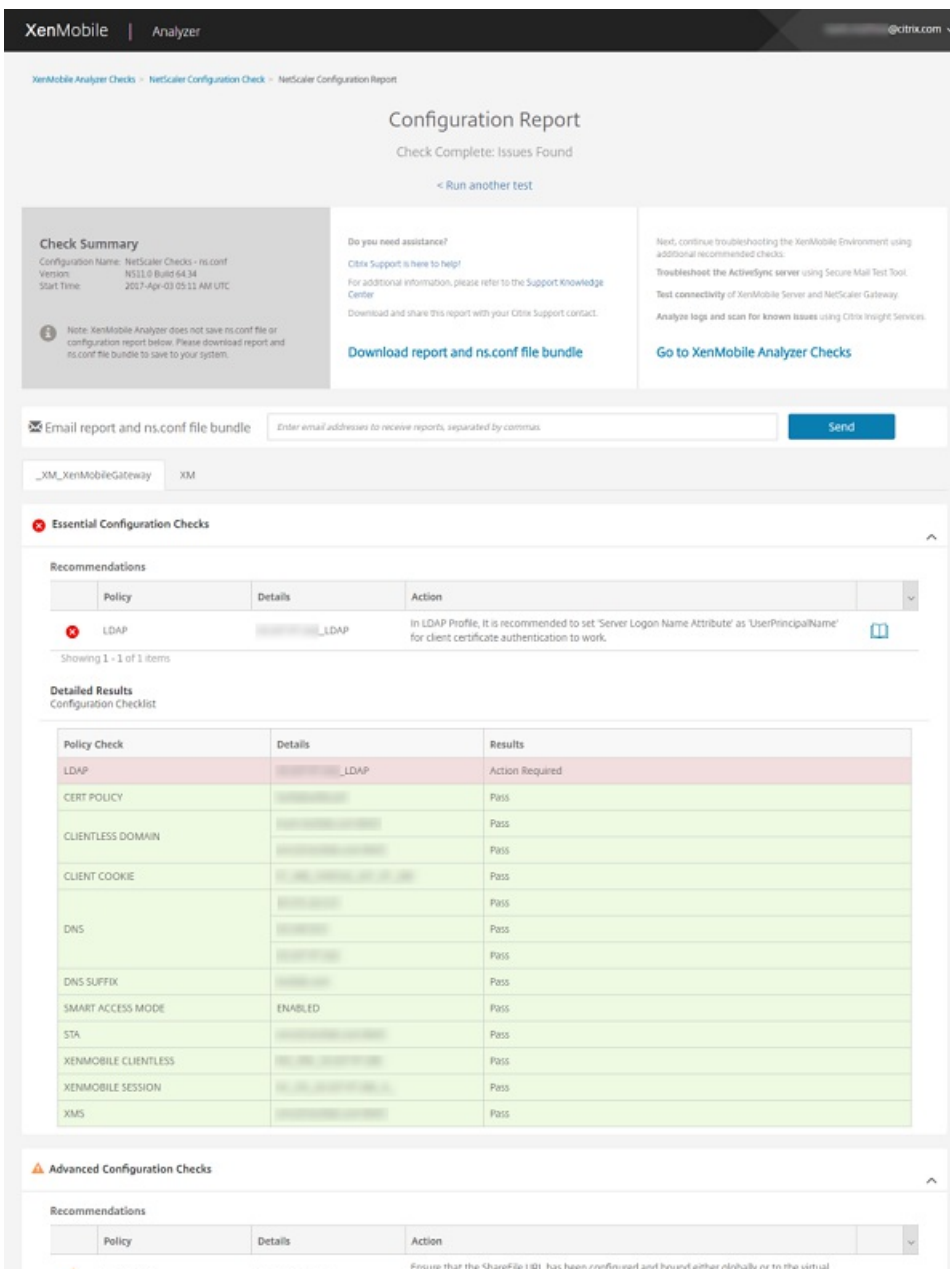
XenMobile Analyzer 运行两种类型的配置检查。

- 基本检查会查找对成功完成 XenMobile 部署至关重要的组件。
- 高级检查会查找对 XenMobile 部署不是至关重要但是补充性的组件。

4. 要查看有关 NetScaler 的基本检查和高级检查的建议，请单击查看报告。



此时将显示 **Configuration Report**（配置报告）页面。



Policy Check	Details	Results
SHAREFILE	Not Configured	Action Recommended
SHAREFILE AUTH	Not Configured	Action Recommended
SHAREFILE STORAGE ZONE LB	Not Configured	Action Recommended
SPLIT TUNNEL	Not Configured	Action Recommended
XNC SERVER	Not Configured	Action Recommended
MAM LB	IP: 10.10.10.10, 10.10.10.10	Pass
MDM LB	IP: 10.10.10.10, 10.10.10.10	Pass

注意

XenMobile Analyzer 支持通过 NetScaler 向导配置的网关服务器。NetScaler Gateway 实例始终具有以下标题约定：‘_XM_*name-provided-by-user-when-deploying’。

通过了基本配置检查时，整体状态为成功。

基本配置检查失败时，“Recommendations”（建议）表列出了 **Policy**（策略）、**Details**（详细信息）和 **Results (Action Recommended)**（结果(所需操作)）。

高级配置检查失败时，“Recommendations”（建议）表列出了 **Policy**（策略）、**Details**（详细信息）和 **Results (Action Recommended)**（结果(建议操作)）。



在 **Configuration Report**（配置报告）页面上，提供了以下选项。

- 要查看详细信息，请单击 **Essential Configuration Checks/Advanced Configuration Checks**（基本配置检查/高级配置检查）（或展开图标）。
- 要运行另一个 NetScaler 配置检查，请单击 **Run another test**（运行另一个测试）。
- 要查看其他故障排除和分析工具，请单击 **Go to XenMobile Analyzer Checks**（转到 XenMobile Analyzer 检查）。

d. 要下载结果报告，请单击 **Download Report and ns.conf file bundle**（下载报告和 ns.conf 文件包）或在 **Email report and ns.conf bundle**（通过电子邮件发送报告和 ns.conf 包）中键入您的电子邮件地址。然后，单击 **Send**（发送）。

执行其他信息性检查

您直接与 XenMobile Analyzer 的环境检查步骤交互以执行测试，而其他选项属于信息性的。其中每个选项都会提供与可用于确保正确设置 XenMobile 环境的其他支持工具有关的信息。

- **Advanced Diagnostics**（高级诊断）：指导您收集与环境有关的信息，然后将该信息上载到 Citrix Insight Services。该工具分析您的数据并提供包含建议的解决方案在内的个性化报告。
- **Secure Mail Readiness**（Secure Mail 就绪）：指导您下载并运行 XenMobile Exchange ActiveSync Test 应用程序。该应用程序将对 ActiveSync 服务器进行故障排除，以确认其是否已准备好在 XenMobile 环境中部署。该应用程序运行后，可以查看报告或将报告与其他人共享。
- **Server Connectivity Checks**（服务器连接检查）：为您提供检查与 XenMobile、身份验证和 ShareFile 服务器的连接的说明。
- **Contact Citrix Support**（联系 Citrix 支持）：如果所有其他步骤都失败，可以通过 Citrix 支持创建一个支持票证。

已知问题

下面是与 XenMobile Analyzer 有关的已知问题：

- 如果在 XenMobile 服务器上设置了平台限制策略，列出的应用程序数量可能会因客户端而异。
- 执行 Secure Web 连接检查时，不支持在文本框中输入多个 URL。
- 不支持使用 Secure Hub 的共享设备身份验证功能。
- Secure Hub 测试只检查与输入的 URL 的连接，不检查对相应站点的身份验证。

已修复的问题

XenMobile Analyzer 存在的以下问题已修复：

- 使用注册邀请执行检查时，测试将传递，但不替换注册邀请。

在 XenMobile 中查看和分析日志文件

Feb 27, 2017

1. 在 XenMobile 控制台中，单击控制台右上角的扳手图标。此时将打开支持页面。
2. 在日志操作下，单击日志。此时将显示日志页面。单独的日志将显示在表格中。

XenMobile Analyze Manage Configure administrator

Support > Logs

Logs

Analyze the details of various types of logs.

Download All

<input type="checkbox"/>	Log Name	Log Type
<input type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

3. 选择要查看的日志：

- 调试日志文件中包含对 Citrix 技术支持有用的信息，例如错误消息和服务器相关操作。
- 管理员审核日志文件中包含与 XenMobile 控制台上的活动有关的审核信息。
- 用户审核日志文件中包含与配置的用户有关的信息。

4. 使用表格顶部的操作可下载所有日志，查看、轮转或下载单个日志，或者删除选定的日志。

Logs

Analyze the details of various types of logs.

Download All |
 View |
 Rotate |
 Download |
 Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug

注意：

- 如果选择了多个日志文件，则只有**全部下载**和**轮转**可用。
- 如果您有群集 XenMobile 服务器，只能查看所连接到的服务器的日志。要查看其他服务器的日志，请使用以下下载选项之一。

5. 执行以下操作之一：

- **全部下载**：控制台下载系统中存在的所有日志（包括调试、管理员审核、用户审核、服务器日志等）。
- **查看**：在表格下方显示所选日志的内容。
- **轮转**：将当前日志文件存档并创建新文件以捕获日志条目。存档日志文件时会显示一个对话框，请单击轮转以继续。
- **下载**：控制台仅下载选定的一种日志文件类型，此外，还下载该类型对应的所有已存档的日志。
- **删除**：永久删除所选日志文件。

Logs

Analyze the details of various types of logs.

Download All |
 View |
 Rotate |
 Download |
 Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```

2016-11-06T06:28:38.908-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:29:38.926-0800 | INFO | node.scheduled.executor-10 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:30:38.762-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | Begin method executeNonPrvsnTaskJob: Sun Nov 06 06:45:38 PST 2016
2016-11-06T06:30:38.766-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | The number of non provision tasks Picked 2.
2016-11-06T06:30:38.945-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:31:38.965-0800 | INFO | node.scheduled.executor-9 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:32:38.985-0800 | INFO | node.scheduled.executor-4 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:33:39.3-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:34:39.24-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:35:39.42-0800 | INFO | node.scheduled.executor-5 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:36:39.502-0800 | INFO | pool-7-thread-1 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
                
```

REST API

Feb 27, 2017

借助 XenMobile REST API，可以调用通过 XenMobile 控制台展现的服务。可以使用任何 REST 客户端调用 REST 服务。API 不要求您登录 XenMobile 控制台即可调用这些服务。

有关可用 API 的最新完整集合，请下载 [XenMobile REST API 参考 PDF](#)。

访问 REST API 所需的权限

访问 REST API 需要具有以下权限：

- 公共 API 访问权限，作为基于角色的访问配置的一部分设置（有关设置基于角色的访问权限的详细信息，请参阅[使用 RBAC 配置角色](#)）
- 超级用户权限

调用 REST API 服务

可以使用 REST 客户端或 CURL 命令调用 REST API 服务。以下示例使用适用于 Chrome 的高级 REST 客户端。

注意

在下面的示例中，请更改主机名和端口号以匹配您的环境。

登录

URL : `https://:/xenmobile/api/v1/authentication/login`

请求 : `{ "login":"administrator", "password":"password" }`

方法类型 : POST

内容类型 : application/json

https://localhost:4443/xenmobile/api/v1/publicapi/login

GET
 POST
 PUT
 PATCH
 DELETE
 HEAD
 OPTIONS
 Other

Raw Form Headers

Raw Form Files (0) Payload

Encode payload Decode payload

```

{
  "login": "administrator",
  "password": "password"
}

```

application/json Set "Content-Type" header to overwrite this value.

Clear Send

Status **200 OK** Loading time: 265 ms

Request headers

```

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36
Origin: chrome-extension://hgmlloofddfdnphfgcellkdfbfjeloo
Content-Type: application/json
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163

```

Response headers

```

Server: Apache-Coyote/1.1
Content-Type: text/plain
Content-Length: 53
Date: Sun, 22 Mar 2015 22:43:48 GMT

```

Raw Parsed Response

Open output in new window Copy to clipboard Save as file Open in JSON tab

```

{"auth_token": "d4fdecf6-2e5a-4aed-8d60-f9a513b5c358"}

```

Code highlighting thanks to [Code Mirror](#)

XenMobile Mail Manager 10.x

Feb 27, 2017

XenMobile Mail Manager 可以采用以下方式扩展 XenMobile 的功能：

- 用于 Exchange Active Sync (EAS) 设备的动态访问控制。可以自动允许或阻止 EAS 设备访问 Exchange 访问。
- 使 XenMobile 能够访问 Exchange 提供的 EAS 设备合作信息。
- 使 XenMobile 能够在移动设备上执行 EAS 擦除。
- 使 XenMobile 能够访问关于黑莓设备的信息以及执行控制操作，如擦除和重置密码。

要下载 XenMobile Mail Manager，请转到 Citrix.com 中 XenMobile 10 Server 下的“服务器组件”部分。

XenMobile Mail Manager 10.1 中的新增功能

访问规则

“Rule Analysis”（规则分析）窗口包含一个复选框，选中该复选框时，将仅显示冲突、替代、冗余或增补规则。

分别为在您的 XenMobile 部署中配置的每个 Microsoft Exchange 环境设置默认访问【“Allow”（允许）、“Block”（阻止）或“Unchanged”（保持不变）】和 ActiveSync 命令模式（“PowerShell”或“Simulation”（模拟）】。

快照

可以配置在快照历史记录中显示的最大快照数。

可以创建主要快照期间要忽略的错误。如果主要快照返回的错误未配置为可忽略，则将放弃快照的结果。

要将错误配置为可忽略，请使用 XML 编辑器编辑 config.xml 文件：

- 如果 Exchange Server 为 Office 365，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors 节点，并使用与现有错误子元素相同的格式添加要匹配的文本作为子元素。支持正则表达式。
- 如果 Exchange Server 为本地服务器，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors 节点，并使用与现有错误子元素相同的格式添加要匹配的文本作为子元素。支持正则表达式。
- 如果配置了多个 Exchange 环境，请导航到 /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='与所需的 Exchange 环境对应的 ID']/ExchangeServer/Specialists/PowerShell 节点针对要忽略的每个错误，将 IgnorableErrors 子节点添加到 PowerShell 节点。将错误子节点添加到 CDATA 部分中含有匹配文本的 IgnorableErrors 节点。支持正则表达式。

保存 config.xml 并重新启动 XenMobile Mail Manager 服务。

PowerShell 和 Exchange

XenMobile Mail Manager 现在根据所连接到的 Exchange 版本动态决定要使用的 cmdlet。例如，对于 Exchange 2010，将使用 Get-ActiveSyncDevice，而对于 Exchange 2013 和 Exchange 2016，则使用 Get-MobileDevice。

Exchange 配置

无需启动 XenMobile Mail Manager 服务即可编辑和更新 Exchange Server 配置。

向 Exchange 环境的摘要选项卡中添加的两个新列显示了每个环境的命令模式【“PowerShell”或“Simulation”（模拟）】和访问模式【“Allow”（允许）、“Block”（阻止）或“Unchanged”（保持不变）】。

故障排除和诊断

Support\PowerShell 文件夹中提供了一组用于故障排除的 PowerShell 实用程序。

使用控制台的“Configuration”（配置）窗口中的“Test Connectivity”（测试连接）按钮测试与 Exchange 服务的连接将运行服务所使用的每个只读 cmdlet，针对所配置的用户 Exchange Server 运行 RBAC 权限测试，以及使用不同颜色显示所有错误或警告（蓝色-黄色表示警告，红色-橙色表示错误）。

新的故障排除工具将对用户的邮箱和设备执行深度分析（从而检测错误条件和潜在的故障区域），并对用户执行深度 RBAC 分析。该工具可以将所有 cmdlet 的原始输出保存到一个文本文件。

在支持场景中，可以通过选中控制台中的一个诊断复选框来保存 XenMobile Mail Manager 管理的所有设备上的所有邮箱的所有属性。

在支持场景中，现在支持跟踪级别日志记录。

身份验证

XenMobile Mail Manager 支持对本地部署进行“Basic”（基本）身份验证。这将允许在 XenMobile Mail Manager 服务器不属于 Exchange Server 所在域的成员的情况下使用 XenMobile Mail Manager。

已修复的问题

访问规则

XenMobile Mail Manager 对 Active Directory (AD) 组中的所有用户应用本地访问控制规则，即使 AD 组包含的用户数超过 1000 也是如此。以前，XenMobile Mail Manager 仅对 AD 组的前 1000 个用户应用本地访问控制规则。[#548705]

查询含有 1000 个或更多用户的 Active Directory 组时，XenMobile Mail Manager 控制台有时会无法响应。[CXM-11729]

“LDAP Configuration”（LDAP 配置）窗口不再显示不正确的身份验证模式。[CXM-5556]

快照

带撇号的用户名不再导致次要快照出现故障。[#617549]

在禁用了流水线操作的支持场景中，【Disable Pipelining（禁用流水线操作）选项在 XenMobile Mail Manager 控制台的“Configuration”（配置）窗口中处于选中状态】，主要快照在本地 Exchange 环境中将不再出现故障。[#586083]

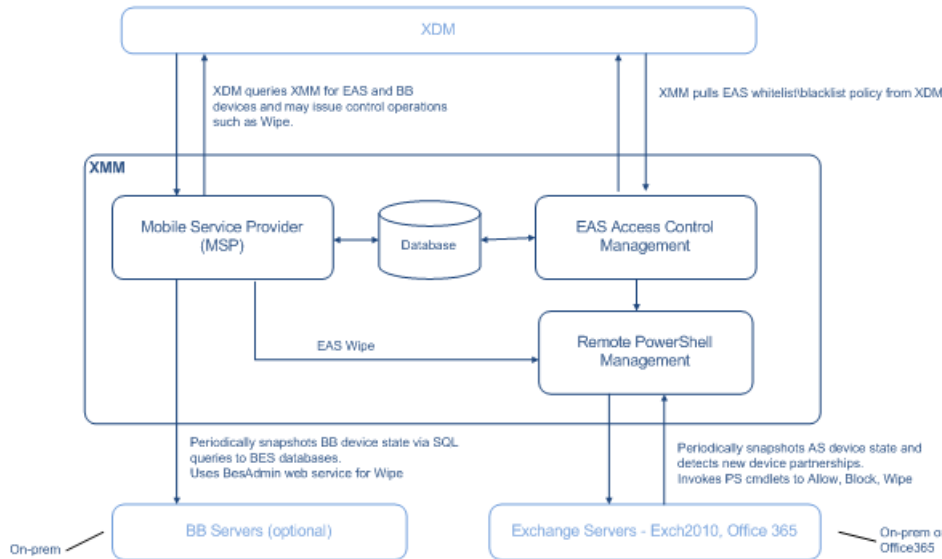
在禁用了流水线操作的支持场景中【“Disable Pipelining”（禁用流水线操作）选项在 XenMobile Mail Manager 控制台的“Configuration”（配置）窗口中处于选中状态】，不再收集深层快照的数据，与环境是针对深层快照还是浅表快照配置的无关。现在，仅当环境是针对深层快照配置的情况下，才收集深层快照的数据。[#586092]

初始安装完成后创建的第一个主要快照有时会遇到阻止 XenMobile Mail Manager 运行另一个主要快照的错误，直至重新启动 XenMobile Mail Manager 服务。此错误不再发生。[CXM-5536]

体系结构

Feb 27, 2017

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

Feb 27, 2017

要使用 XenMobile Mail Manager，需要满足以下最低系统要求：

- Windows Server 2012 R2、Windows Server 2008 R2（必须是基于英语的服务器）
- Microsoft SQL Server 2016、SQL Server 2012、SQL Server 2012 Express LocalDB 或 SQL Server Express 2008
- Microsoft .NET Framework 4.5
- 黑莓 Enterprise Service 版本 5（可选）

Microsoft Exchange Server 的最低支持版本

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 SP2

设备电子邮件客户端

并非所有电子邮件客户端都一致地为设备返回相同的 ActiveSync ID。由于 XenMobile Mail Manager 要求每个设备具有唯一的 ActiveSync ID，因此，仅支持为每个设备一致地生成相同的唯一 ActiveSync ID 的电子邮件客户端。这些电子邮件客户端已通过 Citrix 测试，执行时没有错误：

- HTC 本机电子邮件客户端
- Samsung 本机电子邮件客户端
- iOS 本机电子邮件客户端
- 适用于智能手机的 TouchDown

XenMobile Mail Manager 必备条件

- 必须安装 Windows Management Framework。
 - PowerShell V5、V4 和 V3
- 必须通过 Set-ExecutionPolicy RemoteSigned 将 PowerShell 执行策略设置为 RemoteSigned。
- 必须在运行 XenMobile Mail Manager 的计算机和远程 Exchange Server 之间打开 TCP 端口 80。

运行 Exchange 的本地计算机的要求

权限。在 Exchange 配置用户界面中指定的凭据必须能够连接到 Exchange Server，并且具有执行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：

- 针对 **Exchange Server 2010 SP2**：
 - Get-CASMailbox
 - Set-CASMailbox
 - Get-Mailbox
 - Get-ActiveSyncDevice
 - Get-ActiveSyncDeviceStatistics
 - Clear-ActiveSyncDevice
 - Get-ExchangeServer
 - Get-ManagementRole
 - Get-ManagementRoleAssignment
- 对于 **Exchange Server 2013** 和 **Exchange Server 2016**：
 - Get-CASMailbox

- Set-CASMailbox
 - Get-Mailbox
 - Get-MobileDevice
 - Get-MobileDeviceStatistics
 - Clear-MobileDevice
 - Get-ExchangeServer
 - Get-ManagementRole
 - Get-ManagementRoleAssignment
- 如果将 XenMobile Mail Manager 配置为查看整个林，则必须授权运行 Set-AdServerSettings -ViewEntireForest \$true
 - 提供的凭据必须具有通过远程 Shell 连接到 Exchange Server 的权限。默认情况下，安装 Exchange 的用户具有此权限。
 - 根据 Microsoft TechNet 文章[关于远程要求](#)，要建立远程连接并运行远程命令，凭据必须与远程计算机上的管理员用户对应。根据此博客文章 [You Don't Have to Be An Administrator to Run Remote PowerShell Commands](#)（您不需要成为管理员即可运行远程 PowerShell 命令），Set-PSSessionConfiguration 可以用来消除管理要求，但是对此命令的细节的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。达到连接限制时，XenMobile Mail Manager 无法连接到 Exchange Server。存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。如果有兴趣，可以通过 PowerShell 调查与远程管理相关的 Exchange 限制策略。

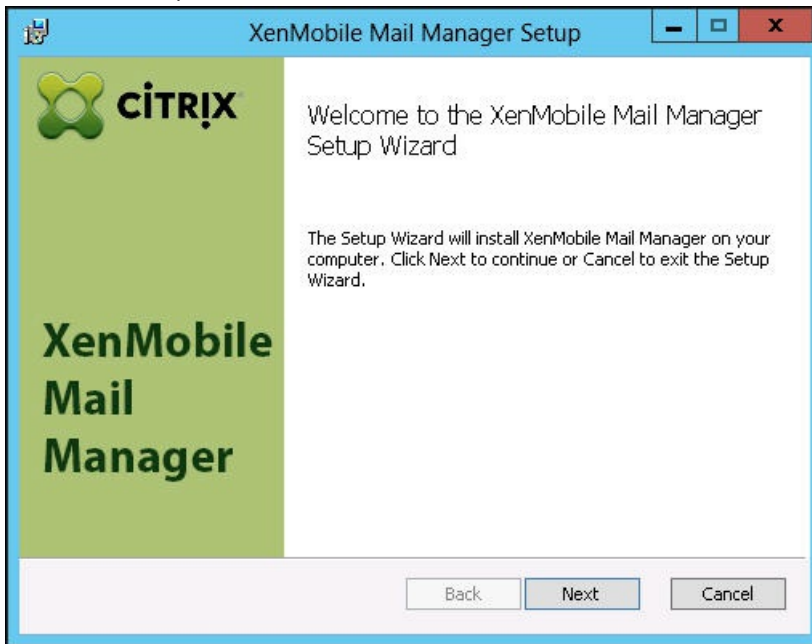
Office 365 Exchange 的要求

- **权限。**在 Exchange 配置用户界面中指定的凭据必须能够连接到 Office 365，并且具有执行以下 Exchange 特定的 PowerShell cmdlet 的完全权限：
 - Get-CASMailbox
 - Set-CASMailbox
 - Get-Mailbox
 - Get-MobileDevice
 - Get-MobileDeviceStatistics
 - Clear-MobileDevice
 - Get-ExchangeServer
 - Get-ManagementRole
 - Get-ManagementRoleAssignment
- **特权。**提供的凭据必须已获得授权，可以通过远程 Shell 连接到 Office 365 服务器。默认情况下，Office 365 联机管理员具有必备特权。
- **限制策略。**Exchange 有许多限制策略。其中一个策略控制每个用户允许的并发 PowerShell 连接的数目。在 Office 365 中，一个用户允许的同时连接数默认为三个。达到连接限制时，XenMobile Mail Manager 无法连接到 Exchange Server。存在通过不在本文档范围内的 PowerShell 更改允许的同时连接数上限的方法。如果有兴趣，可以通过 PowerShell 调查与远程管理相关的 Exchange 限制策略。

安装和配置

Feb 27, 2017

1. 单击 XmmSetup.msi 文件，然后按照安装程序中的提示安装 XenMobile Mail Manager。



2. 保留在设置向导的最后一个屏幕中选中的 **Launch the Configure utility**（启动配置实用程序）选项。或者，从开始菜单中打开 **XenMobile Mail Manager**。

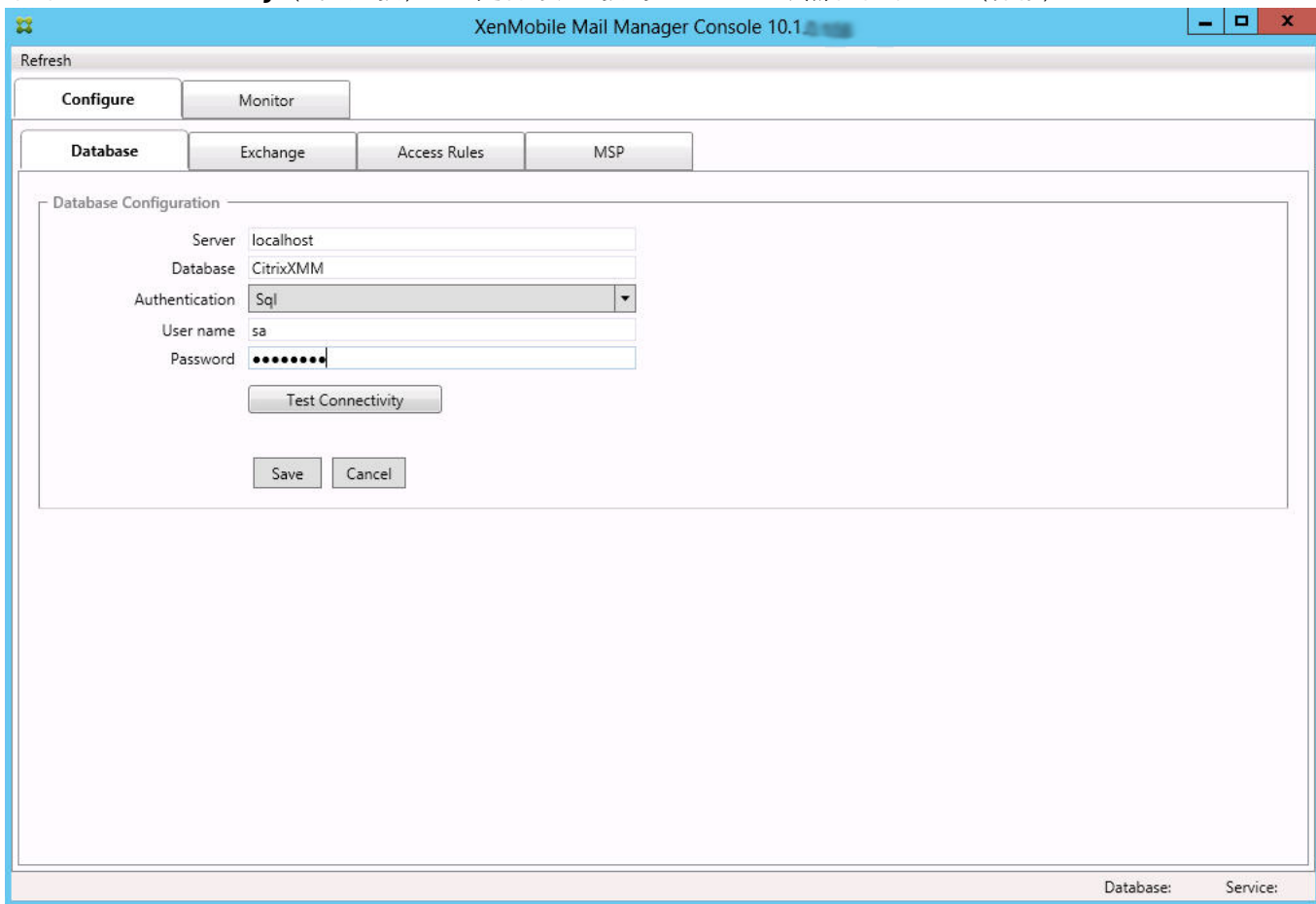


3. 配置以下数据库属性：
 1. 选择 **Configure**（配置） > **Database**（数据库）选项卡。
 2. 输入 SQL Server 的服务器名称（默认为 localhost）。
 3. 将数据库保留为默认 CitrixXmm。
 4. 选择以下用于 SQL 的身份验证模式之一：
 - **Sql**。输入有效 SQL 用户的用户名和密码。

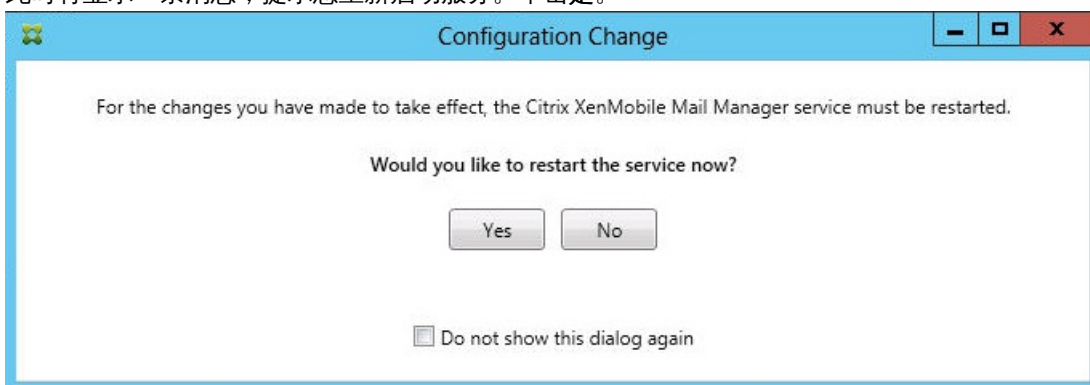
- **Windows 集成**。如果选择此选项，XenMobile Mail Manager 服务的登录凭据必须更改为具有访问 SQL Server 权限的 Windows 帐户。为此，请打开控制面板 > 管理工具 > 服务，在 XenMobile Mail Manager 服务条目上单击鼠标右键，然后单击登录选项卡。

注意：如果还为黑莓数据库连接选择了 Windows 集成，必须同时为此处指定的 Windows 帐户提供黑莓数据库访问权限。

5. 单击 **Test Connectivity**（测试连接）检查是否可以连接到 SQL Server，然后单击 **Save**（保存）。

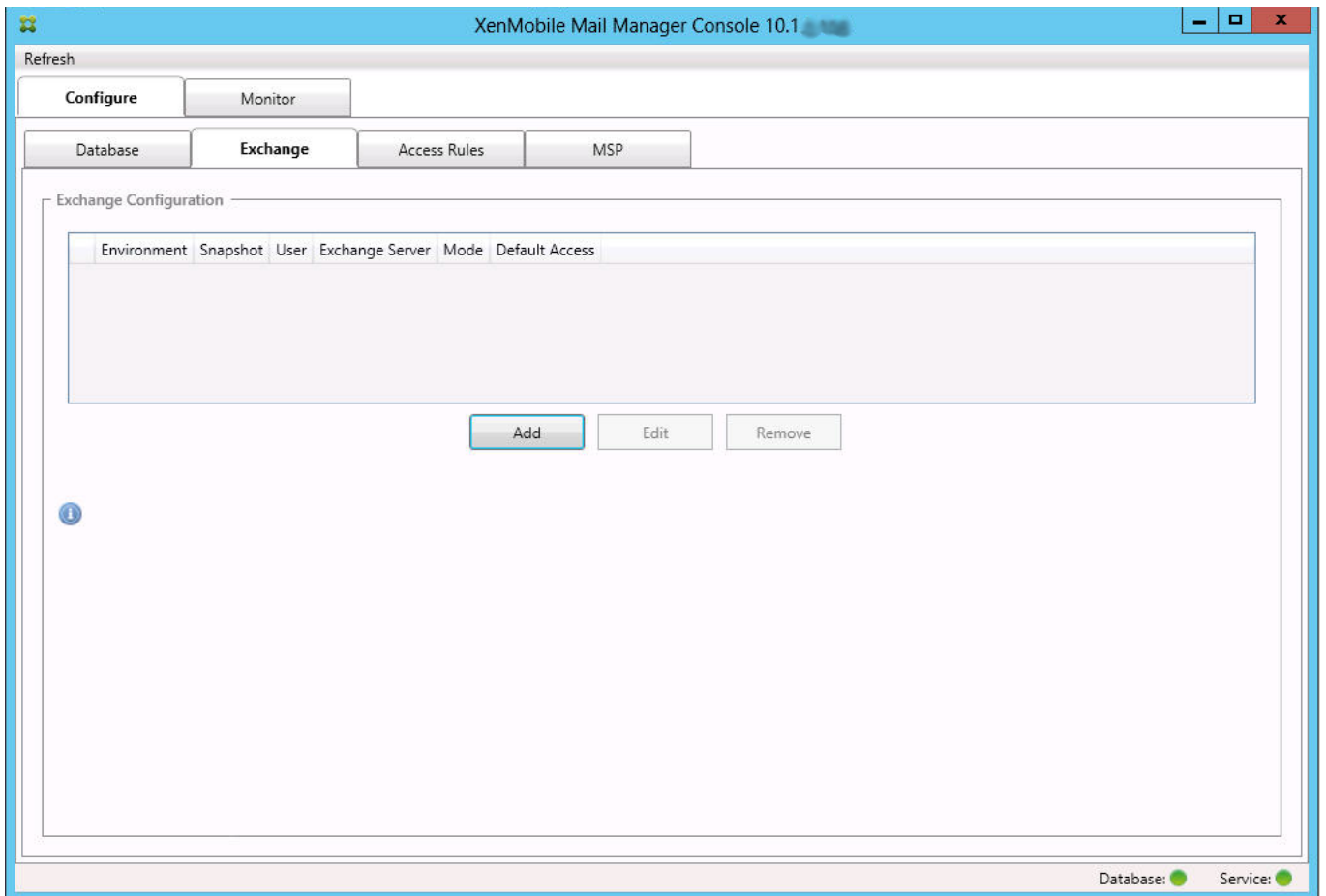


4. 此时将显示一条消息，提示您重新启动服务。单击是。

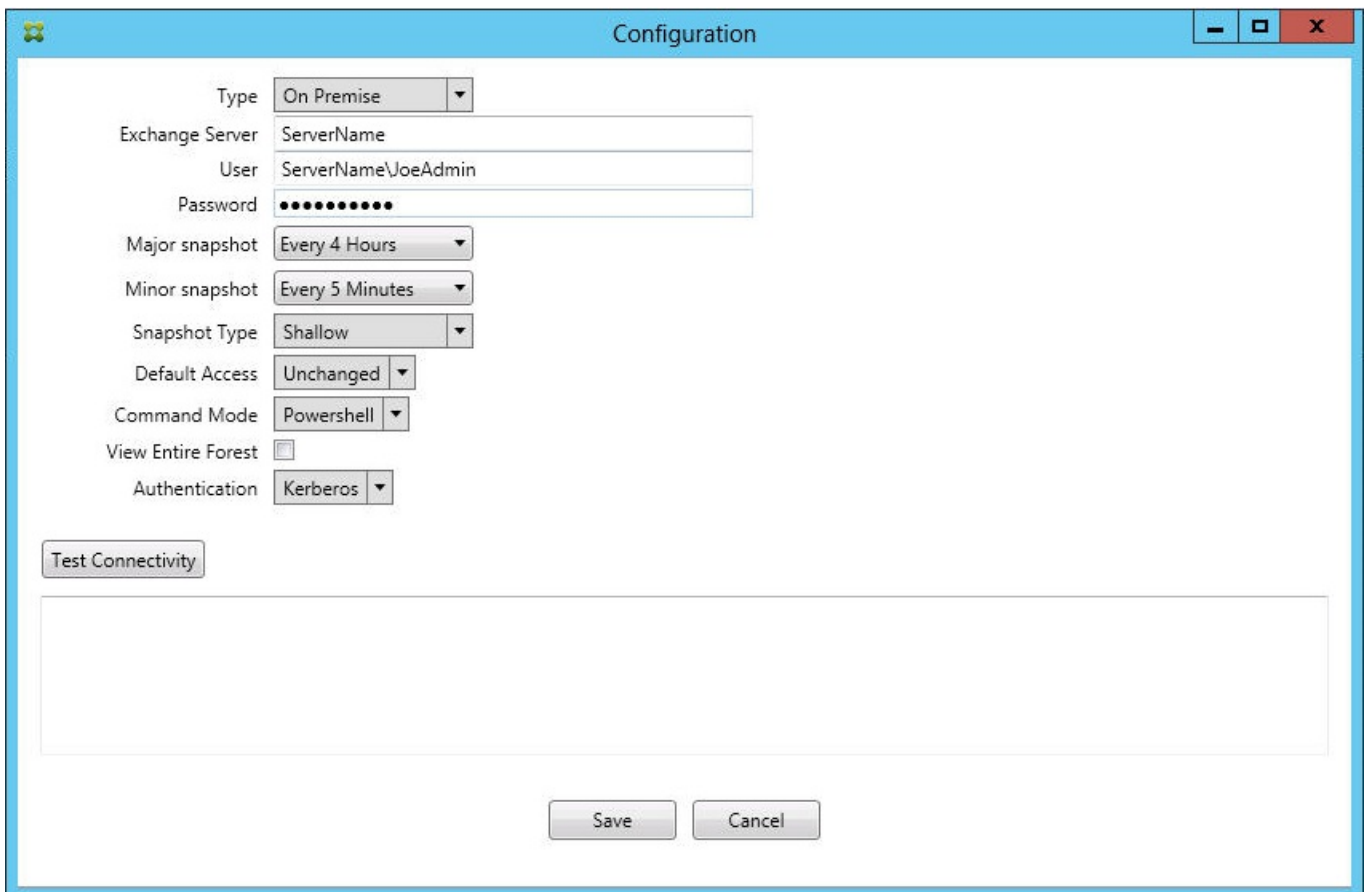


5. 配置一个或多个 Exchange Server :

1. 如果管理单个 Exchange 环境，您仅需要指定一个服务器。如果管理多个 Exchange 环境，您需要为每个 Exchange 环境指定一个 Exchange Server。
2. 选择 **Configure**（配置）> **Exchange** 选项卡。

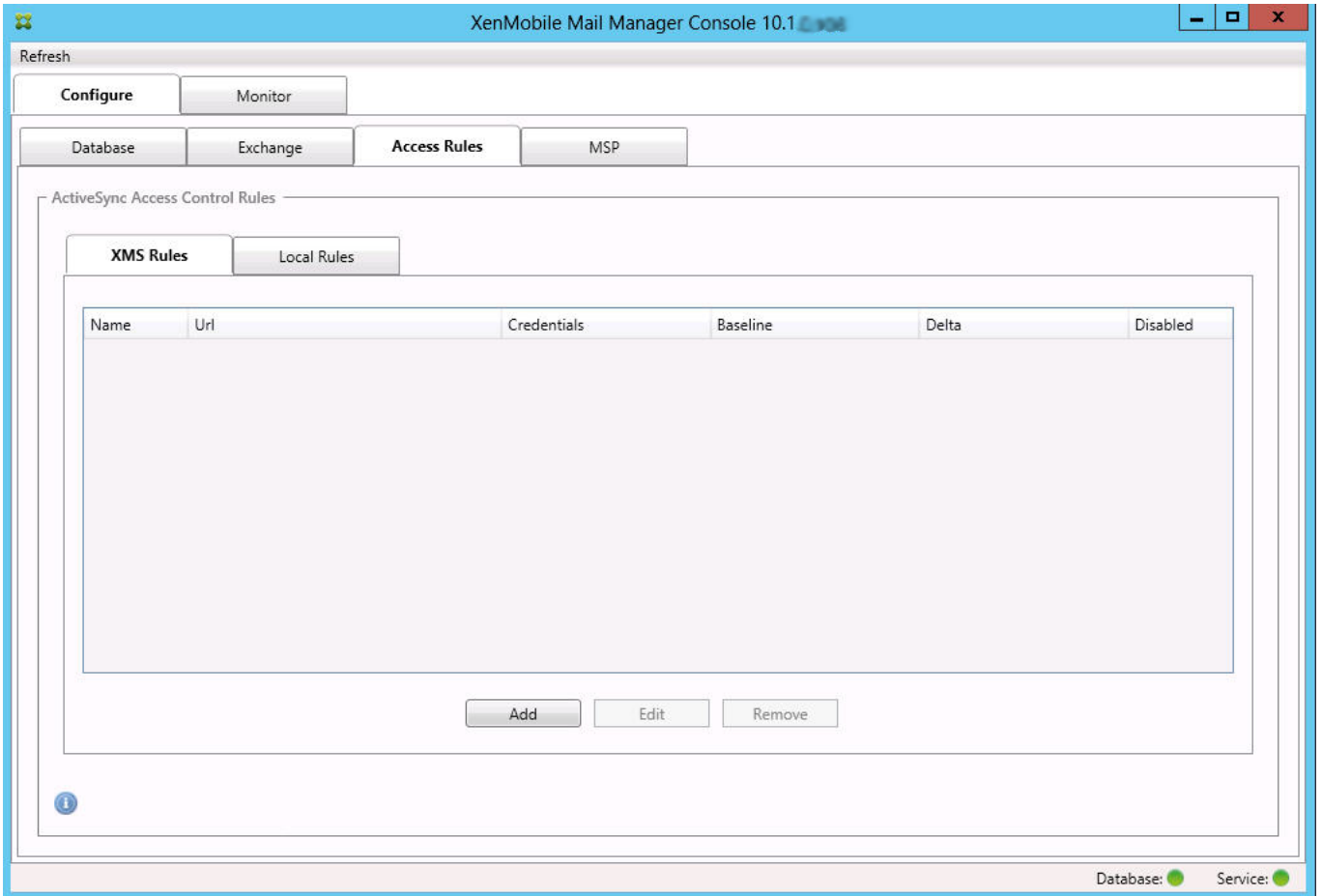


3. 单击添加。
4. 选择 Exchange Server 环境类型，**On Premise**（内部部署）或 **Office 365**。

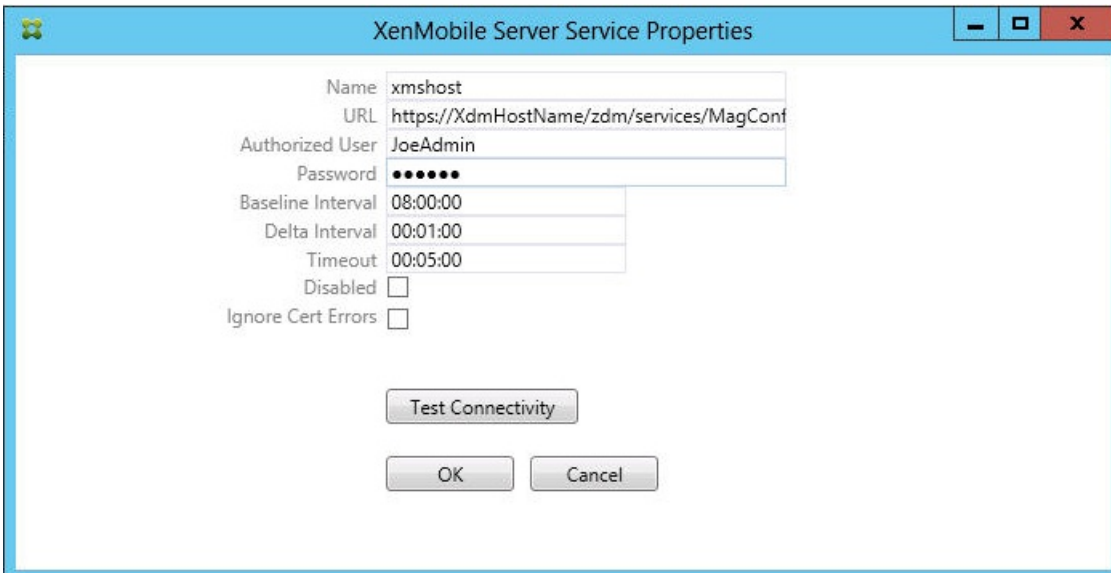


5. 如果选择 **On Premise**（内部部署），请输入要用于远程 Powershell 命令的 Exchange Server 的名称。
6. 输入在要求部分中指定的 Exchange Server 上具有适当权限的 Windows 身份的用户名。
7. 输入用户的 **Password**（密码）。
8. 选择运行主要快照的计划。主要快照检测每个 Exchange ActiveSync 合作关系。
9. 选择运行次要快照的计划。次要快照检测新创建的 Exchange ActiveSync 合作关系。
10. 选择快照类型：**Deep**（深）或 **Shallow**（浅）。浅表快照通常更快并且足以执行 XenMobile Mail Manager 的所有 Exchange ActiveSync 访问控制功能。深层快照可能需要花费更长时间，并且仅在为 ActiveSync 启用移动服务提供商（允许 XenMobile 查询未托管的设备）后才需要。
11. 选择“Default Access”（默认访问）：**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。
12. 选择 ActiveSync 命令模式：**PowerShell** 或 **Simulation**（模拟）。
 - 在 PowerShell 模式下，XenMobile Mail Manager 会发出 PowerShell 命令以执行所需的访问控制。
 - 在“Simulation”（模拟）模式下，XenMobile Mail Manager 不发出 PowerShell 命令，但是会将预期命令和预期结果记录到数据库中。在模拟模式中，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。
13. 选择 **View Entire Forest**（查看整个林）可将 XenMobile Mail Manager 配置为查看 Exchange 环境中的整个 Active Directory 林。
14. 选择身份验证协议：**Kerberos** 或 **Basic**（基本）。XenMobile Mail Manager 支持对本地部署进行“Basic”（基本）身份验证。这将允许在 XenMobile Mail Manager 服务器不属于 Exchange Server 所在域的成员的情况下使用 XenMobile Mail Manager。
15. 单击 **Test Connectivity**（测试连接）检查是否可以连接到 Exchange Server，然后单击 **Save**（保存）。
16. 此时将显示一条消息，提示您重新启动服务。单击是。
6. 配置访问规则：
 1. 选择 **Configure**（配置）> **Access Rules**（访问规则）选项卡。

2. 单击 **XDM Rules** (XDM 规则) 选项卡。



3. 单击添加。

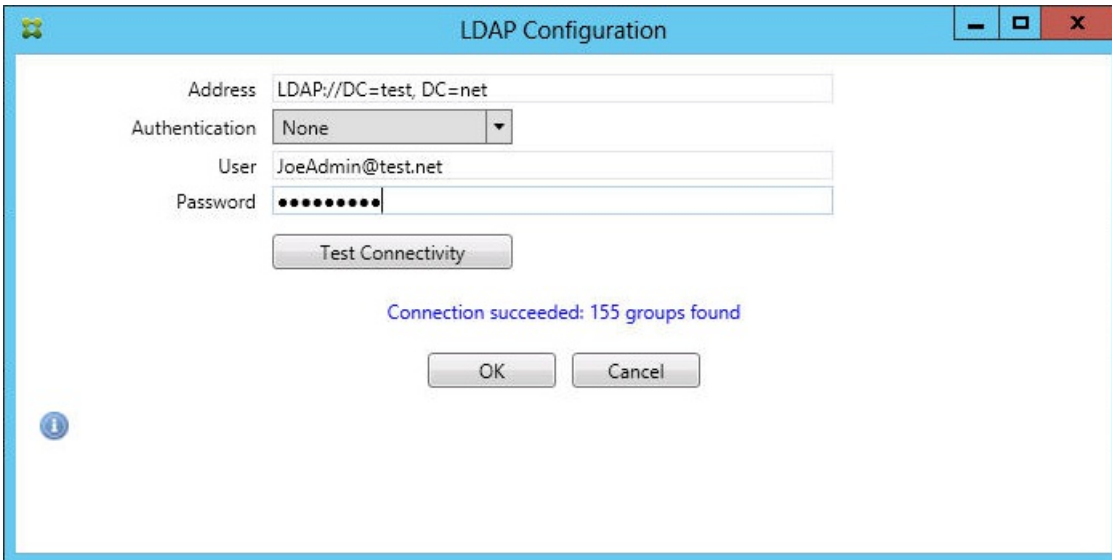


4. 输入 XenMobile 服务器规则的名称，例如 XdmHost。

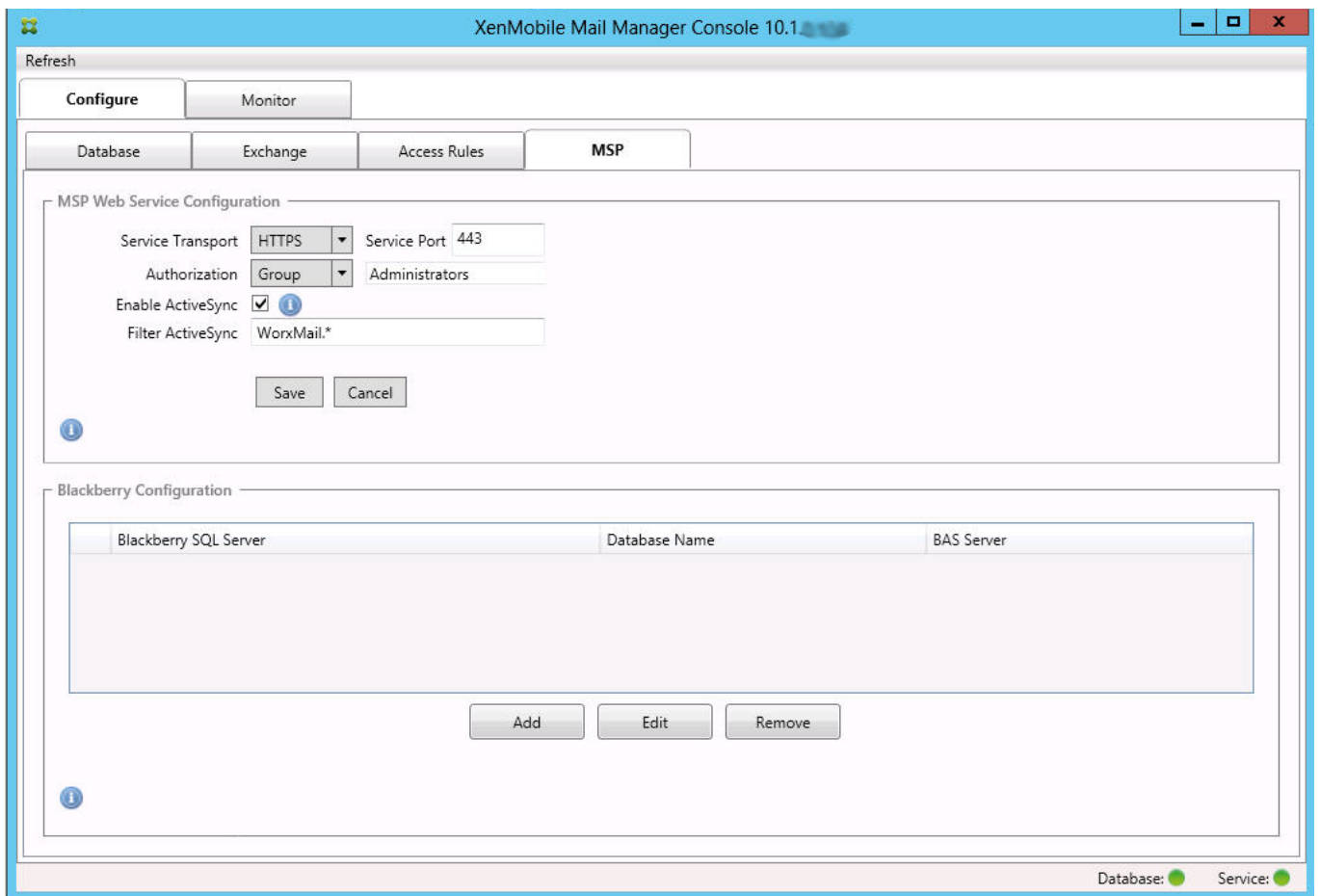
5. 修改 URL 字符串以引用 XenMobile 服务器；例如，如果服务器名称为 XdmHost，输入 http://XdmHostName/zdm/services/MagConfigService。

6. 在该服务器上输入授权用户。

7. 输入用户密码。
 8. 保留 **Baseline Interval** (基准时间间隔)、**Delta Interval** (增量时间间隔) 和 **Timeout values** (超时值) 的默认值。
 9. 单击 **Test Connectivity** (测试连接) , 检查与服务器的连接。
注意：如果选中“Disabled” (已禁用) 复选框, XenMobile Mail Service 将不从 XenMobile 服务器收集策略。
 10. 单击**确定**。
7. 单击 **Local Rules** (本地规则) 选项卡。
 1. 如果要建立在 Active Directory 组中操作的本地规则, 请单击 **Configure LDAP** (配置 LDAP) , 然后配置 LDAP 连接属性。



2. 您可以基于 **ActiveSync Device ID** (ActiveSync 设备 ID)、**设备类型**、**AD Group** (AD 组)、**用户**或设备 **UserAgent** (用户代理) 添加本地规则。在列表中选择适当的类型。有关详细信息, 请参阅 [XenMobile Mail Manager 访问控制规则](#)。
3. 在文本框中输入文本或文本片段。也可单击查询按钮, 查看与片段匹配的实体。
注意：对于除 **Group** (组) 以外的所有类型, 系统依赖在快照中找到的设备。因此, 如果刚刚开始且尚未完成快照, 则没有实体可用。
4. 选择一个文本值, 然后单击 **Allow** (允许) 或 **Deny** (拒绝) , 将其添加到右侧的 **Rule List** (规则列表) 窗格。可以使用 **Rule List** (规则列表) 窗格右侧的按钮改变规则的顺序或移除规则。该顺序很重要, 因为对于指定的用户和设备, 将按照显示的顺序评估规则, 并且一旦与较靠前的规则 (离顶部较近) 匹配, 则后续的规则将失效。例如, 如果存在一条允许所有 iPad 设备的规则, 而后续的规则阻止用户“Matt”, 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 **Analyze** (分析) 。
6. 单击**保存**。
8. 配置移动服务提供商。
注意：移动服务提供商可选, 仅当同时将 XenMobile 配置为使用移动服务提供商界面查询未托管的设备时必需。
 1. 选择 **Configure** (配置) > **MSP** 选项卡。



2. 将移动服务提供商服务的服务传输类型设置为 **HTTP** 或 **HTTPS**。
3. 为移动服务提供商服务设置服务端口（通常为 80 或 443）。
注意：如果使用端口 443，该端口需要在 IIS 中绑定 SSL 证书。
4. 设置授权组或用户。这样可以设定能够从 XenMobile 连接到移动服务提供商服务的用户或用户组。
5. 设置是否已启用 ActiveSync 查询。
注意：如果为 XenMobile 服务器启用 ActiveSync 查询，必须将一个或多个 Exchange Server 的快照类型设置为 **Deep**（深层）；这样拍摄快照可能对性能造成很大损耗。
6. 默认情况下，不会将与正则表达式 Secure Mail.* 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**。
9. 另外，可以配置一个或多个 BlackBerry Enterprise Server (BES)：
 1. 单击**添加**。
 2. 输入 BES SQL Server 的服务器名称。

The screenshot shows the 'BES Properties' dialog box. It is divided into two main sections. The top section, 'BES Sql Server', includes input fields for 'Server' (BesServer), 'Database' (BesMgmt), a dropdown for 'Authentication' (Sql), 'User name' (JoeAdmin), and a masked 'Password' field. A 'Test Connectivity' button is located below these fields. The bottom section, 'Blackberry Device Administration from XMS', features a checked 'Enabled' checkbox, fields for 'BAS Server' (BASServer), 'BAS Port' (443), 'Domain\User' (ServerName\JoeAdmin), and a masked 'Password' field, with another 'Test Connectivity' button below. At the very bottom of the dialog are 'Save' and 'Cancel' buttons.

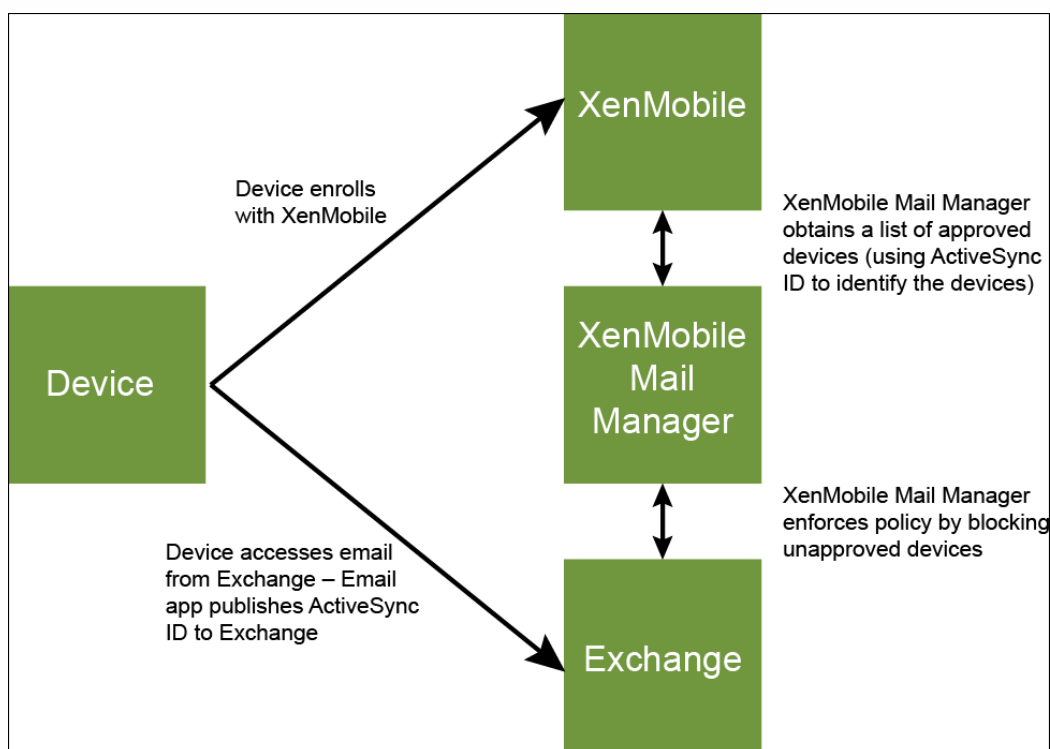
3. 输入 BES Management 数据库的数据库名称。
4. 选择身份验证模式。如果选择 Windows 集成身份验证，则 XenMobile Mail Manager 服务的用户帐户就是用于连接 BES SQL Server 的帐户。
注意：如果还为 XenMobile Mail Manager 数据库连接选择了 Windows 集成，则必须同时为此处指定的 Windows 帐户提供 XenMobile Mail Manager 数据库的访问权限。
5. 如果选择 **SQL authentication**（SQL 身份验证），请输入用户名和密码。
6. 设置 **Sync Schedule**（同步计划）。这是用于连接到 BES SQL Server 并检查任何设备更新的计划。
7. 单击 **Test Connectivity**（测试连接），检查与 SQL 服务器的连接。
注意：如果选择了 Windows 集成，则此测试使用当前登录的用户而非 XenMobile Mail Manager 服务用户，因此不能准确测试 SQL 身份验证。
8. 如果要支持 XenMobile 中的黑莓设备的远程擦除和/或重置密码功能，请选中 **Enabled**（已启用）复选框。
 1. 输入 BES 完全限定的域名 (FQDN)。
 2. 输入用于管理员 Web 服务的 BES 端口。
 3. 输入 BES 服务所需的完全限定用户和密码。
 4. 单击 **Test Connectivity**（测试连接），测试与 BES 的连接。
 5. 单击保存。

使用 ActiveSync ID 强制执行电子邮件策略

Feb 27, 2017

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。Secure Hub 获取类似的标识符，并在注册设备时将标识符发送给 XenMobile。通过比较两个设备 ID，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

Feb 27, 2017

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将丢失您对此窗口所做的任何更改。

XenMobile Mail Manager 有三种类型的规则，即本地规则、XenMobile 服务器规则（也称为 XDM 规则）和默认访问规则。

本地规则。本地规则具有最高优先级：如果设备与本地规则匹配，规则评估将停止。既不查询 XenMobile 服务器规则又不查询默认访问规则。本地规则是通过 Configure（配置）> Access Rules（访问规则）> Local Rules（本地规则）选项卡在 XenMobile Mail Manager 本地配置的。支持匹配基于给定的 Active Directory 组内用户的成员身份。支持匹配基于以下字段的正则表达式：

- Active Sync Device ID（Active Sync 设备 ID）
- ActiveSync Device Type（ActiveSync 设备类型）
- User Principal Name (UPN)（用户主体名称(UPN)）
- ActiveSync User Agent（ActiveSync 用户代理）（通常为设备平台或电子邮件客户端）

只要完成了主要快照并找到设备，您应能够添加常规或正则表达式规则。如果尚未完成主要快照，则只能添加正则表达式规则。

XenMobile 服务器规则。XenMobile 服务器规则是对提供托管设备相关规则的外部 XenMobile 服务器的引用。XenMobile 服务器可通过自身的高级规则进行配置，这些规则可标识要基于 XenMobile 已知属性允许或阻止的设备（例如设备是否越狱或设备是否包含禁用的应用程序）。XenMobile 评估高级规则并生成一组允许或阻止的 ActiveSync 设备 ID，然后将其传递到 XenMobile Mail Manager。

默认访问规则。默认访问规则是唯一的，它可以潜在匹配每个设备，并且始终是最后一个被评估。此规则是一条笼统的规则，这意味着如果给定的设备与本地规则或 XenMobile 服务器规则不匹配，该设备的所需访问状态将由默认访问规则的所需访问状态决定。

- **Default Access - Allow**（默认访问 - 允许）。允许与本地规则或 XenMobile 服务器规则不匹配的任何设备。
- **Default Access - Block**（默认访问 - 阻止）。阻止与本地规则或 XenMobile 服务器规则不匹配的任何设备。
- **Default Access - Unchanged**（默认访问 - 未更改）。与本地规则或 XenMobile 服务器规则不匹配的任何设备将不会由 XenMobile Mail Manager 以任何方式修改其访问状态。如果设备已被 Exchange 置于隔离模式，则不会采取任何措施；例如，从隔离模式删除设备的唯一方法是使用显式本地规则或 XDM 规则覆盖隔离。

关于规则评估

对于 Exchange 向 XenMobile Mail Manager 报告的每个设备，将按照优先级从最高到最低的顺序对这些规则进行评估，如下所示：

- 本地规则
- XenMobile 服务器规则
- 默认访问规则

找到匹配项时，评估将停止。例如，如果本地规则与给定设备匹配，则不会根据任意 XenMobile 服务器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）。

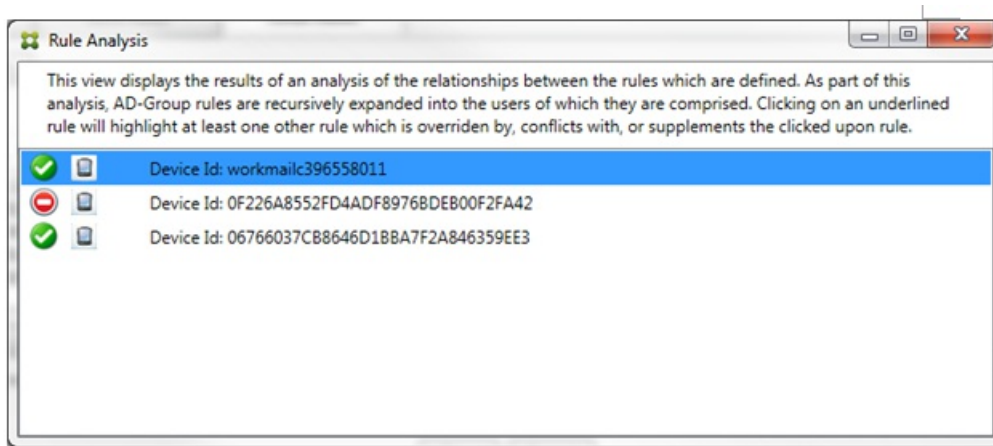
规则术语：

- **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。

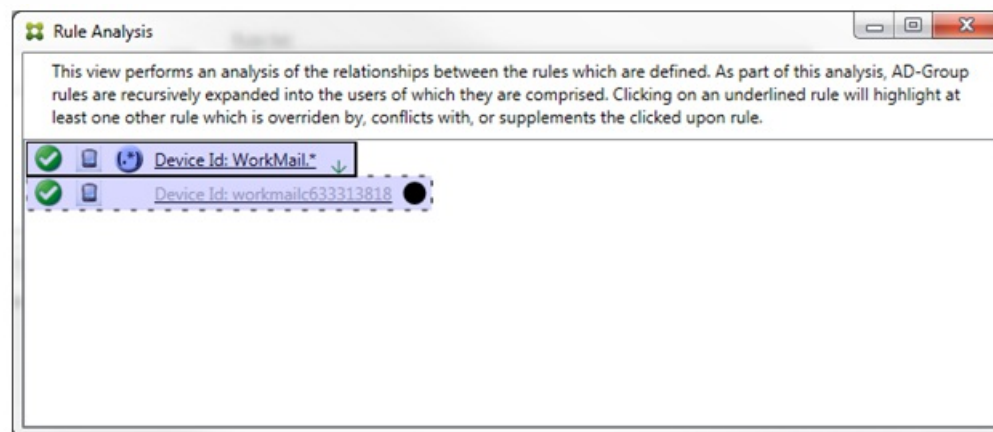
“Rule Analysis”（规则分析）窗口包含一个复选框，选中该复选框时，将仅显示冲突、替代、冗余或增补规则。



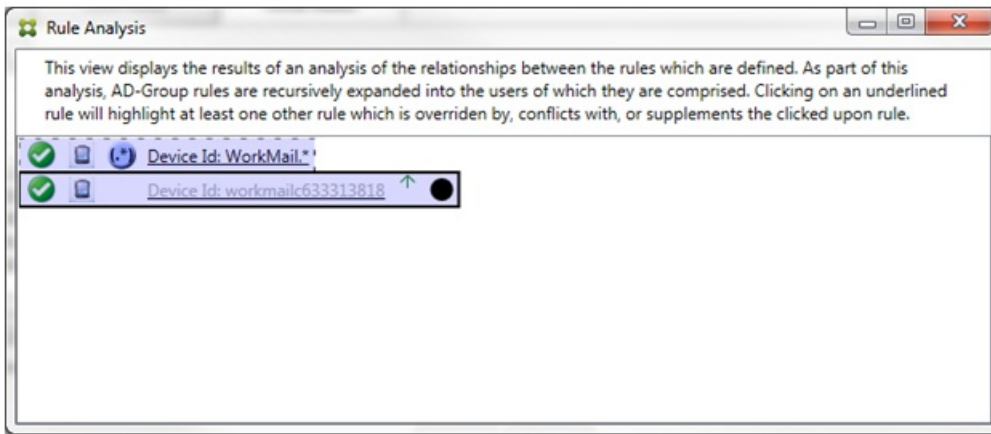
当出现覆盖时，至少有两条规则将加下划线，即主要规则以及一条或多条辅助规则。至少有一条辅助规则将以较浅字体显示，指示该规则已被优先级较高的规则覆盖。您可以单击覆盖的规则以了解覆盖该规则的一条或多条规则。任何时间覆盖的规则都由于规则是主要规则或辅助规则而突出显示，并且将在它旁边将显示一个黑色圆圈，以进一步指示该规则处于不活动状态。例如，在单击该规则之前，对话框显示如下：



单击优先级最高的规则时，对话框显示如下：

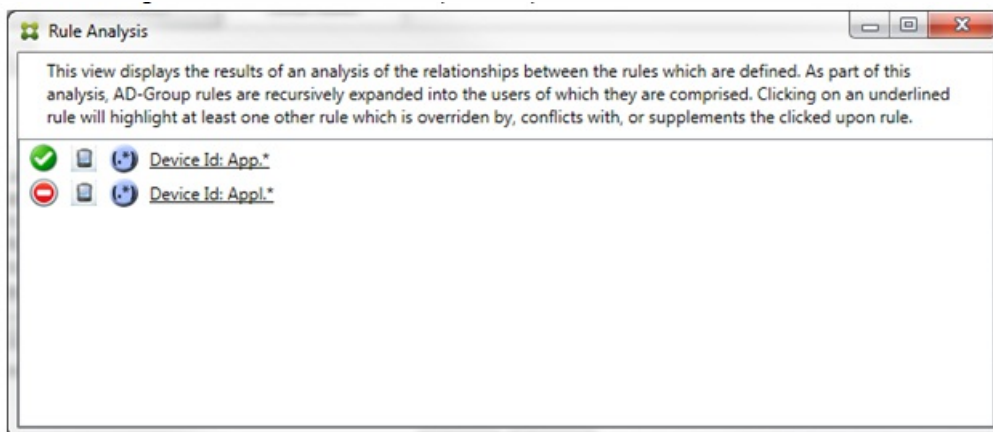


在此示例中，正则表达式规则 WorkMail.* 是主要规则（以实线框指示），常规规则 workmailc633313818 是辅助规则（以虚线框指示）。辅助规则旁边的黑点是一个视觉提示，可进一步指示由于它的前面有较高优先级的正则表达式而处于不活动状态（永远不会被评估）。单击覆盖的规则后，对话框显示如下：

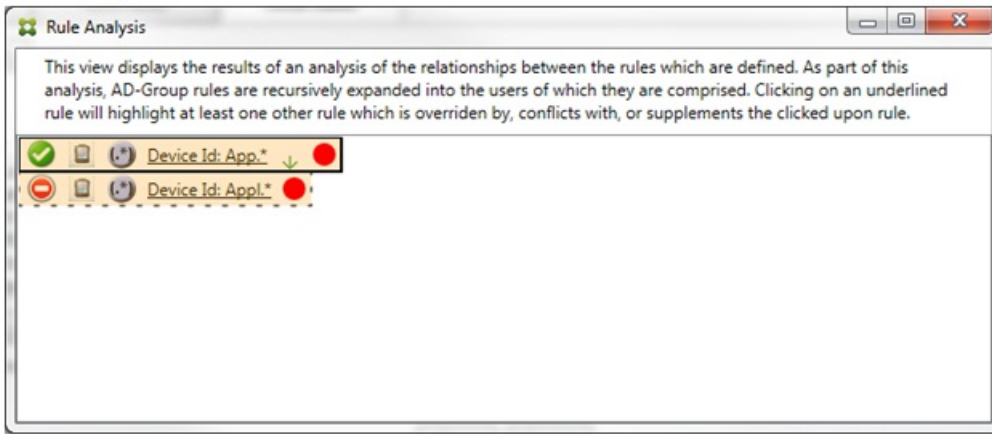


在上例中，正则表达式规则 WorkMail.* 是辅助规则（以虚线框指示），常规规则 workmail633313818 是主要规则（以实线框指示）。对于这一简单的示例，没有太大差异。对于更为复杂的示例，请参阅本主题中后面所述的复杂表达式示例。在定义了许多规则的情景中，单击覆盖的规则将快速识别已覆盖该规则的一条或多条规则。

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：

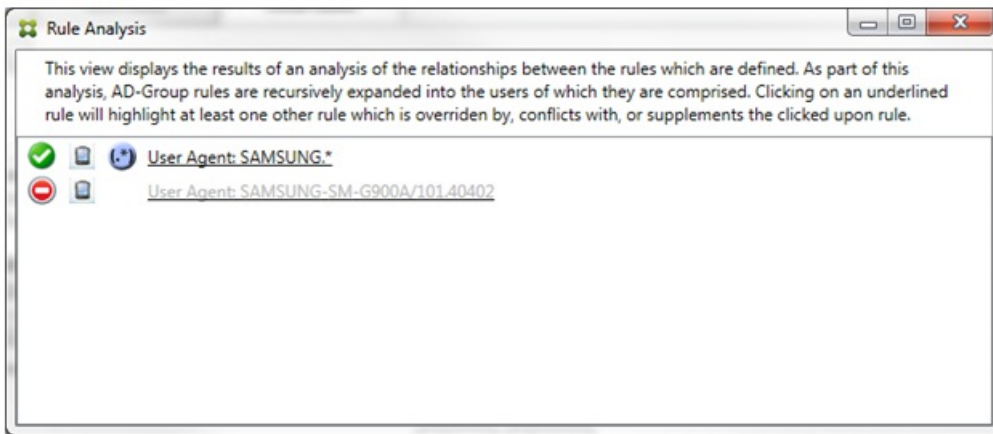


检查这两条正则表达式规则即可明显发现，第一条规则允许设备 ID 包含“App”的所有设备，第二条规则拒绝设备 ID 包含 Appl 的所有设备。此外，即使第二条规则拒绝了设备 ID 包含 Appl 的所有设备，也不会拒绝符合条件的设备，因为允许规则的优先级较高。单击第一条规则后，对话框显示如下：



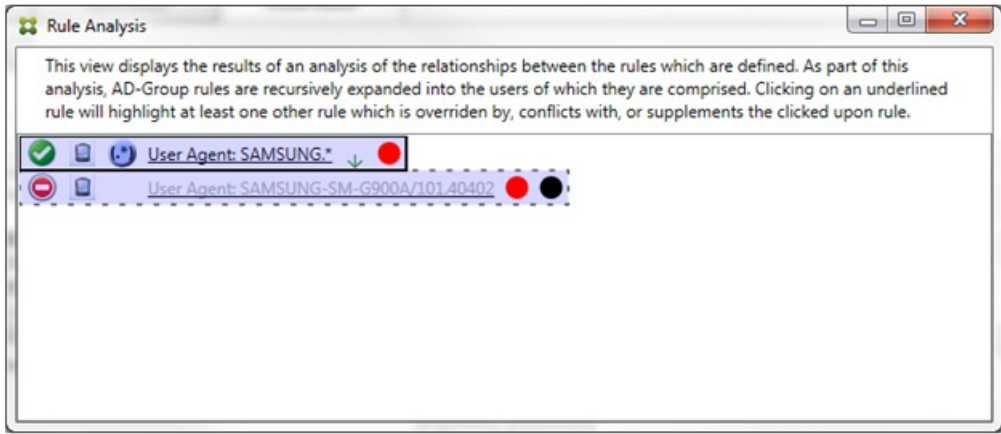
在上述情景中，主要规则（正则表达式规则 App.*）和辅助规则（正则表达式规则 Appl.*）均以黄色突出显示。这只是一个视觉警告，提示您已将多条正则表达式规则应用到单个匹配字段，这可能意味着会出现冗余问题或更严重的问题。

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。



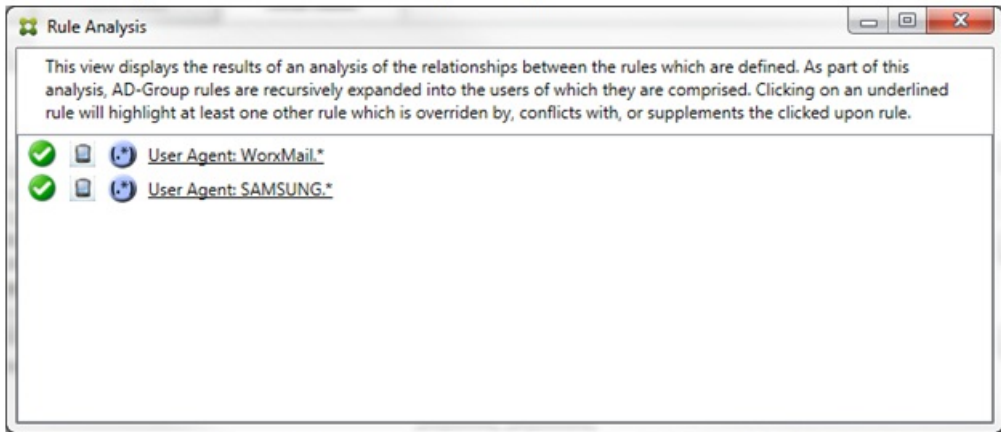
在上例中，显而易见，第一条规则（正则表达式规则 SAMSUNG.*）不仅覆盖下一条规则（常规规则 SAMSUNG-SM-G900A/101.40402），而且这两条规则的访问状态有所不同（主要规则指定“允许”，辅助规则指定“阻止”）。第二条规则（常规规则 SAMSUNG-SM-G900A/101.40402）以较浅文本显示，指示该规则已被覆盖，并因此处于不活动状态。

单击正则表达式规则后，对话框显示如下：

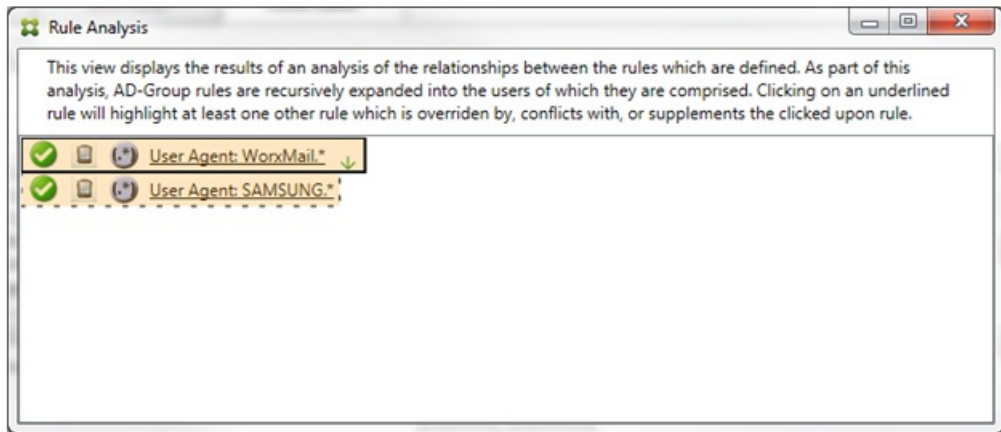


主要规则（正则表达式规则 SAMSUNG.*）后跟一个红点，指示其访问状态与一条或多条辅助规则发生冲突。辅助规则（常规规则 SAMSUNG-SM-G900A/101.40402）后跟一个红点，指示其访问状态与主要规则发生冲突，以及如果后跟黑点，则进一步指示该规则已被覆盖，并因此处于不活动状态。

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：




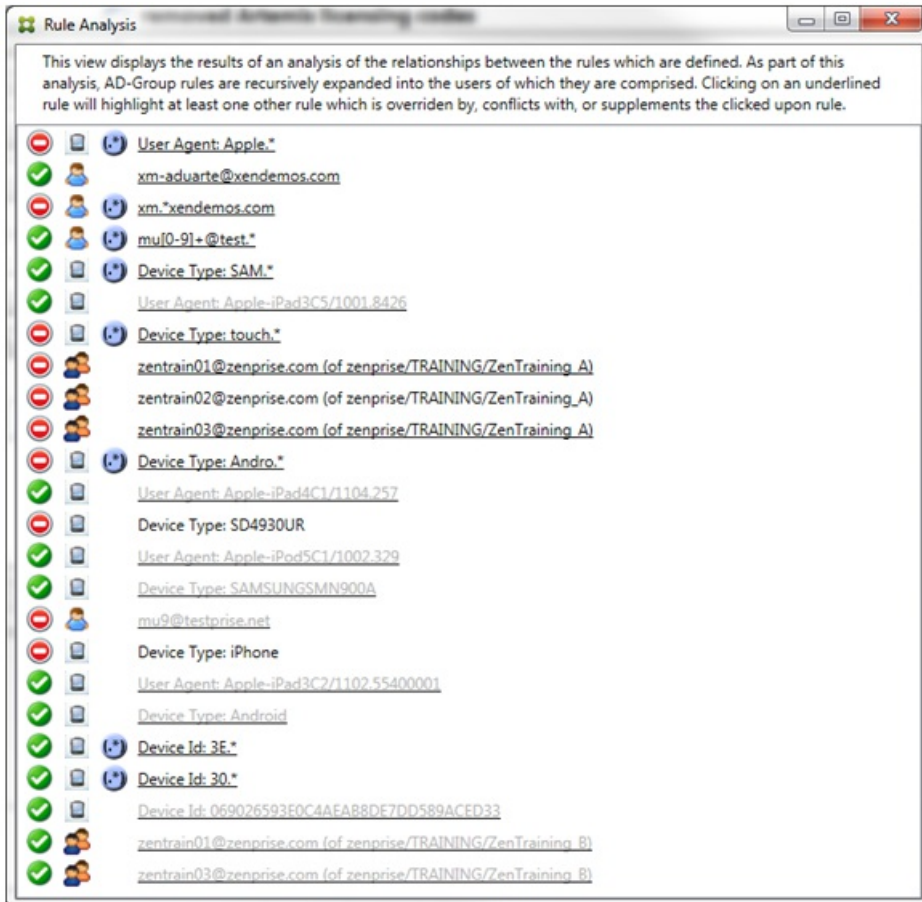
目测会很容易发现这两条规则都是正则表达式规则，都已应用到 XenMobile Mail Manager 中的 ActiveSync 设备 ID 字段。单击第一条规则后，对话框显示如下：



主要规则（正则表达式规则 WorkMail.*）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

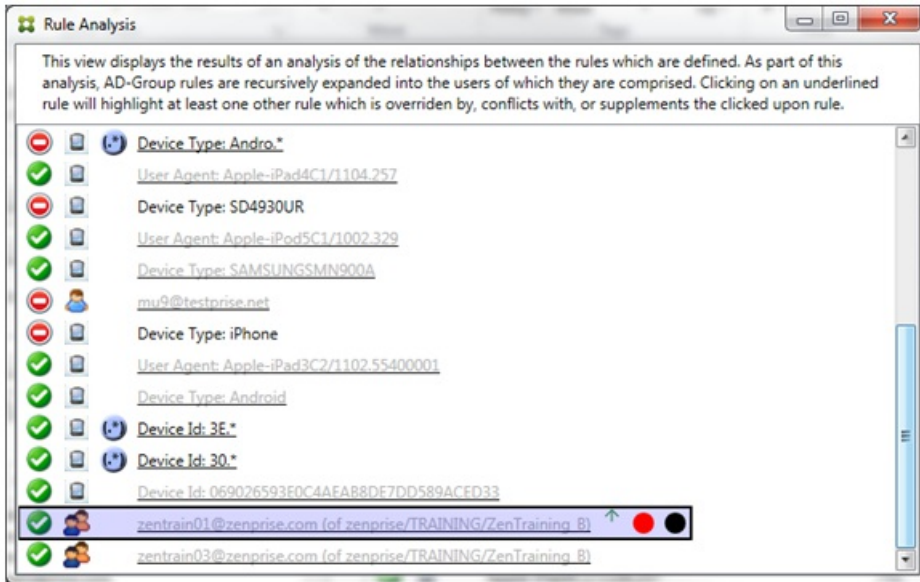
许多潜在的覆盖、冲突或补充都可能会发生，使其不可能举例说明所有可能的情景。下例探讨了不会执行的操作，同时还阐明了规则分析视觉构建的强大功能。大多数项目在下图中加了下划线。许多项目以较浅的字体显示，指示存在问题的规则已被优先级较高的规则以某种方式覆盖。多条正则表达式规则也包括在列表中，由  图标指示。



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。

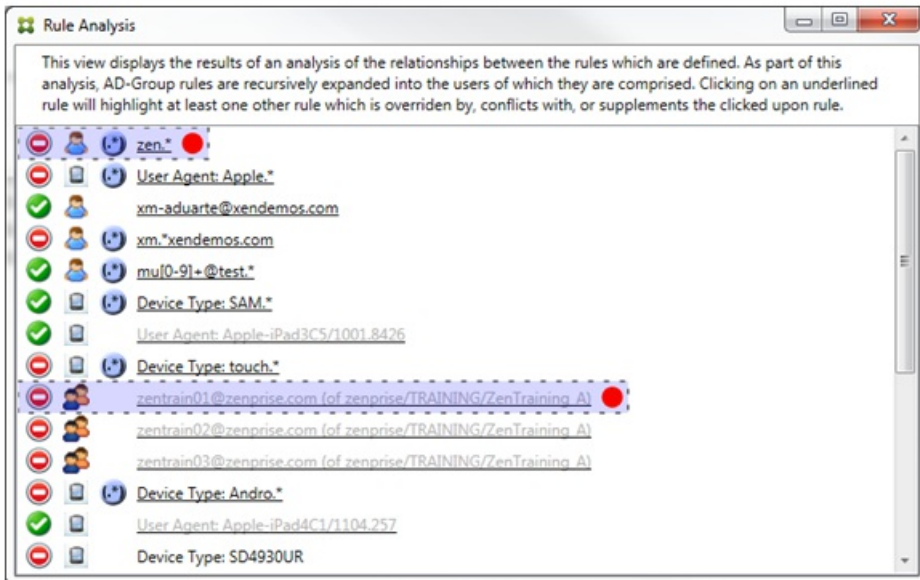
示例 1：此示例调查了覆盖 zentrain01@zenprise.com 的原因。



主要规则（AD-Group 规则 zenprise/TRAINING/ZenTraining B，zentrain01@zenprise.com 是其中的一个成员）具有以下特性：

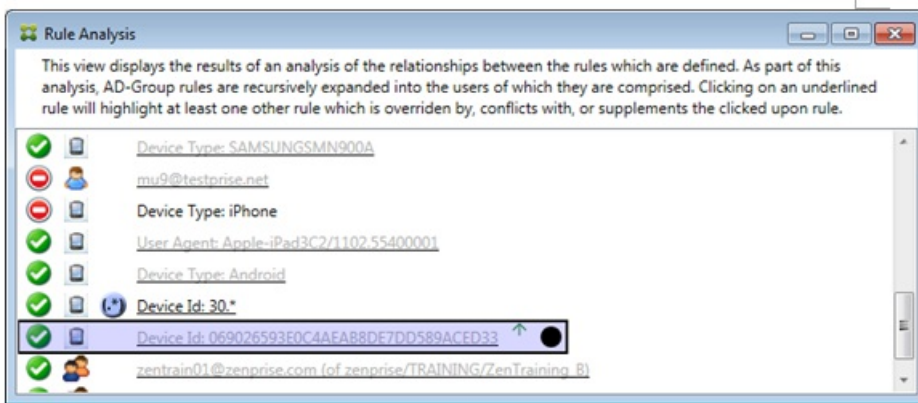
- 以蓝色突出显示并且具有实线框。
- 具有一个指向上方的绿色箭头（指示一条或多条辅助规则都能够在该箭头上方找到）。
- 后跟一个红色圆圈和一个黑色圆圈，分别指示一条或多条辅助规则与其访问状态存在冲突，并且主要规则已被覆盖且因此处于不活动状态。

向上滚动时，您会看到以下内容：



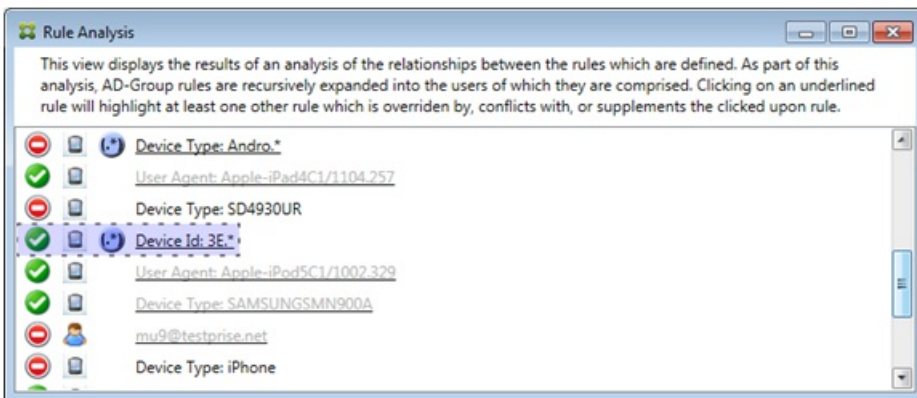
在这种情况下，有两条辅助规则覆盖主要规则：正则表达式规则 zen.* 和常规规则 zentrain01@zenprise.com（属于 zenprise/TRAINING/ZenTraining A）。对于后一条辅助规则，出现了以下情况：Active Directory 组规则 ZenTraining A 包含用户 zentrain01@zenprise.com，Active Directory 组规则 ZenTraining B 也包含用户 zentrain01@zenprise.com。但是，由于辅助规则的优先级高于主要规则，因此主要规则被覆盖。主要规则的访问状态是“允许”，并且由于这两条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。

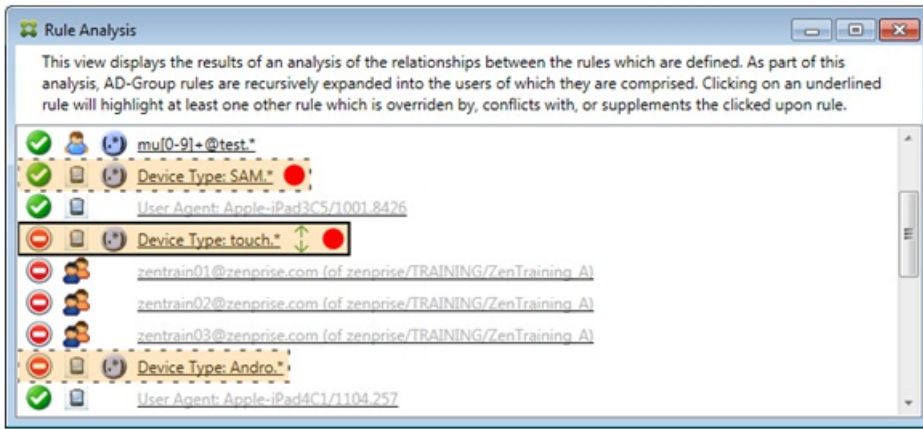


在这种情况下 : 一条辅助规则将覆盖主要规则 : 正则表达式 ActiveSync 设备 ID 规则 3E.*。由于正则表达式 3E.* 将与 069026593E0C4AEAB8DE7DD589ACED33 匹配, 因此, 主要规则永远不会被评估。

如何分析补充和冲突

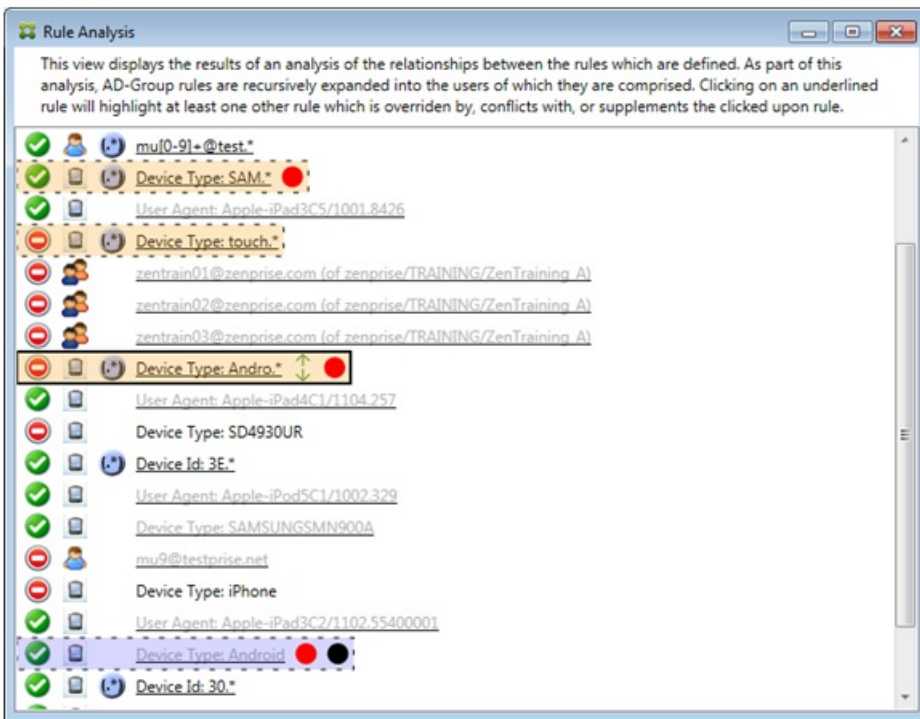
在这种情况下, 主要规则是正则表达式 ActiveSync 设备类型规则 touch.*。特性如下 :

- 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

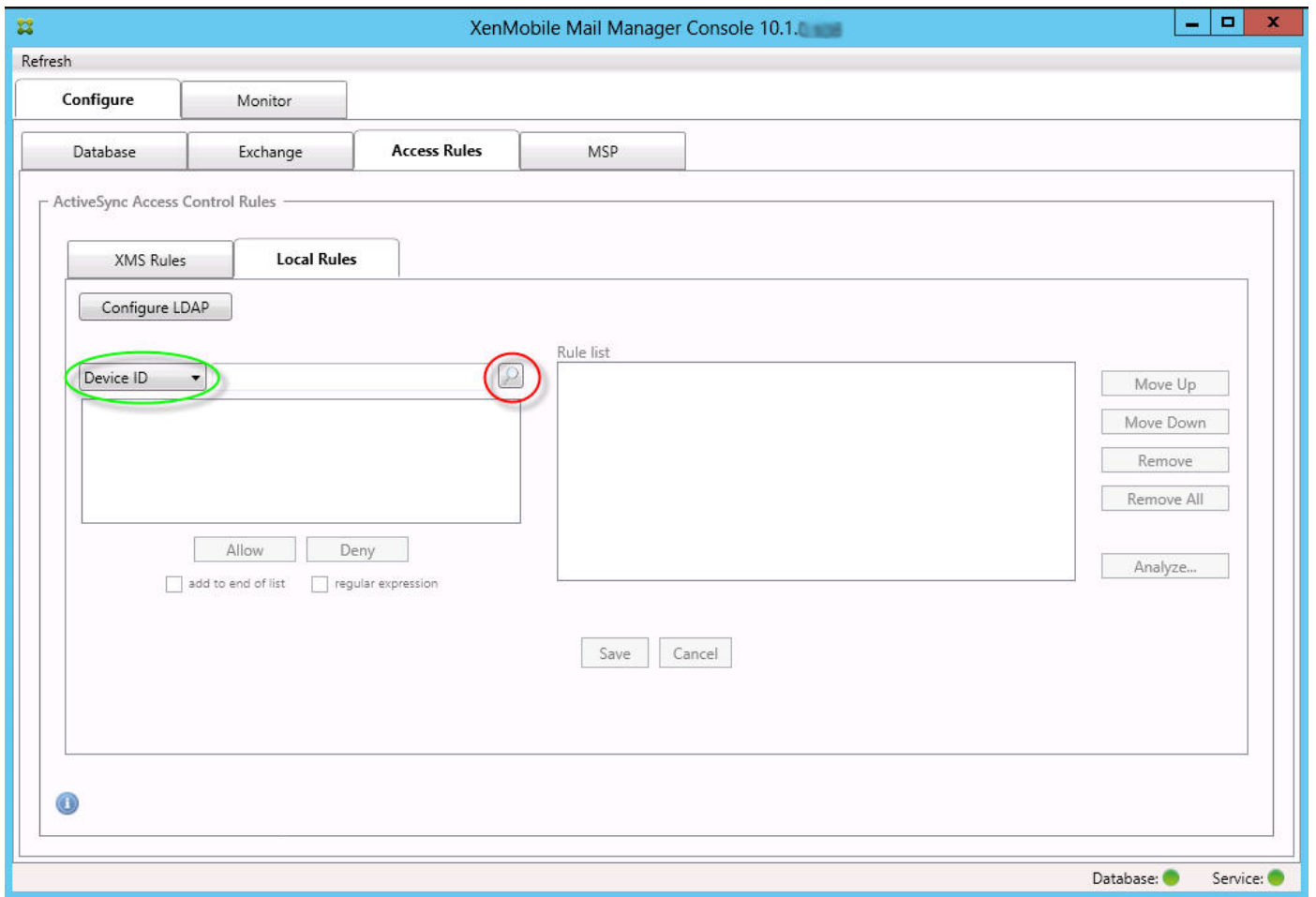
本示例探讨了规则关系如何始终从主要规则的角度建立。上例显示了如何单击应用到设备类型值为 touch.* 的规则字段的正则表达式规则。单击辅助规则 Andro.* 将显示一组不同的辅助规则已突出显示。



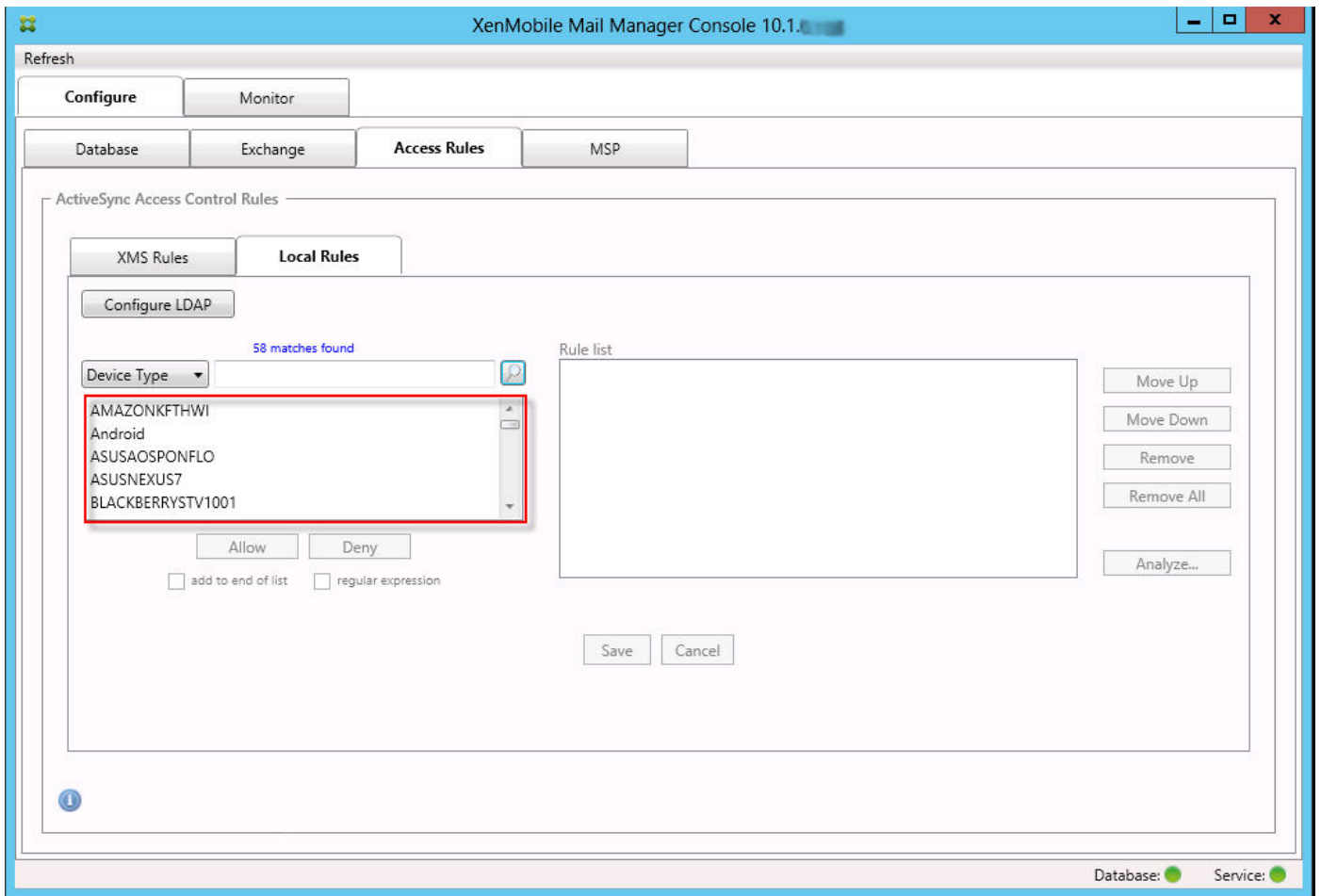
此示例显示了规则关系中不包含的覆盖规则。此规则是常规 ActiveSync 设备类型规则 Android，已被覆盖（通过旁边的浅色字体和黑色圆圈指示）并且其访问状态还与主要规则正则表达式 ActiveSync 设备类型规则 Andro.* 发生冲突；在单击该规则之前，该规则是辅助规则。在上例中，常规 ActiveSync 设备类型规则 Android 未显示为辅助规则，因为从主要规则（正则表达式 ActiveSync 设备类型规则 touch.*）的角度来看，该规则与主要规则不相关。

配置常规表达式本地规则

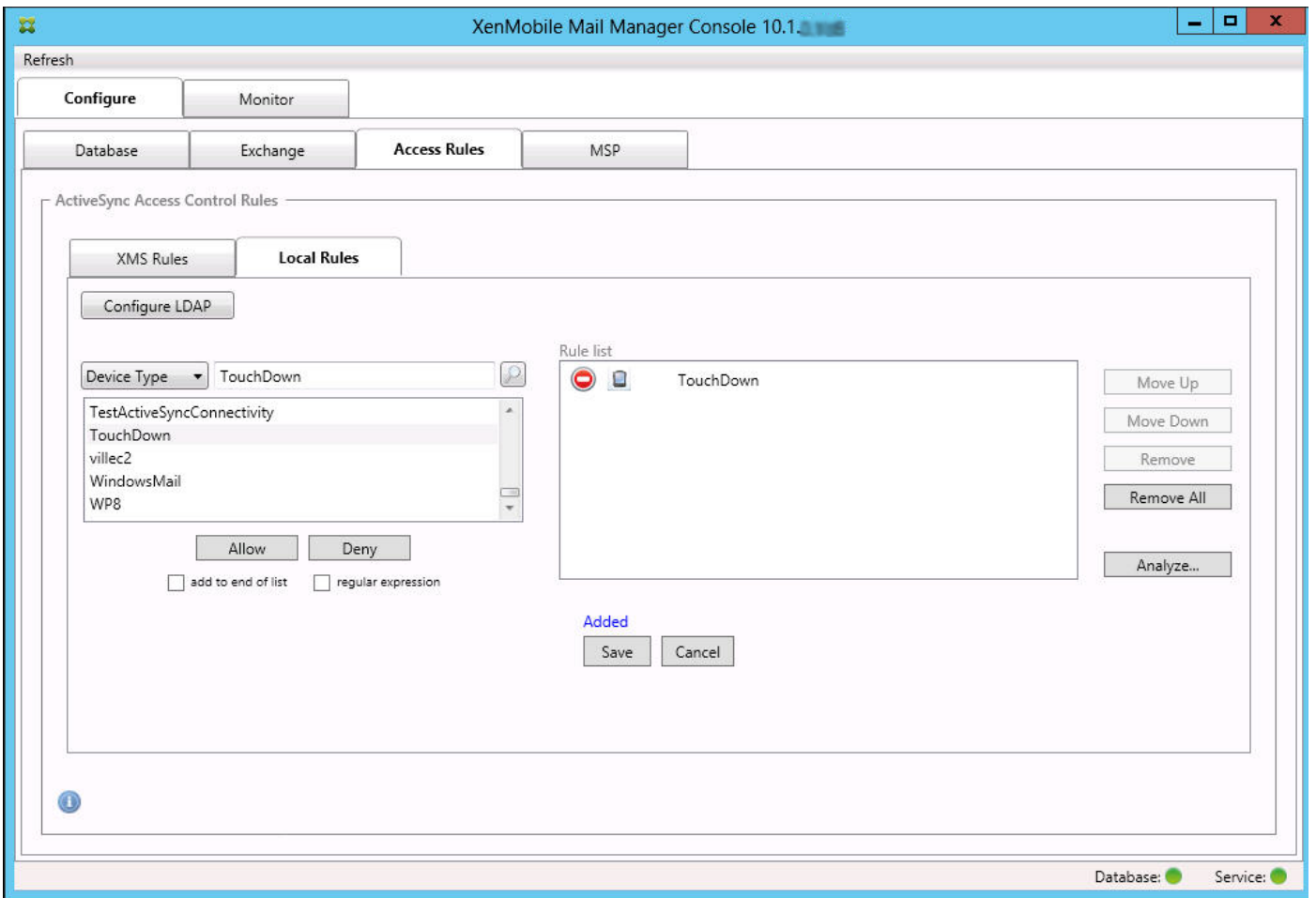
1. 单击 Access Rules（访问规则）选项卡。




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。

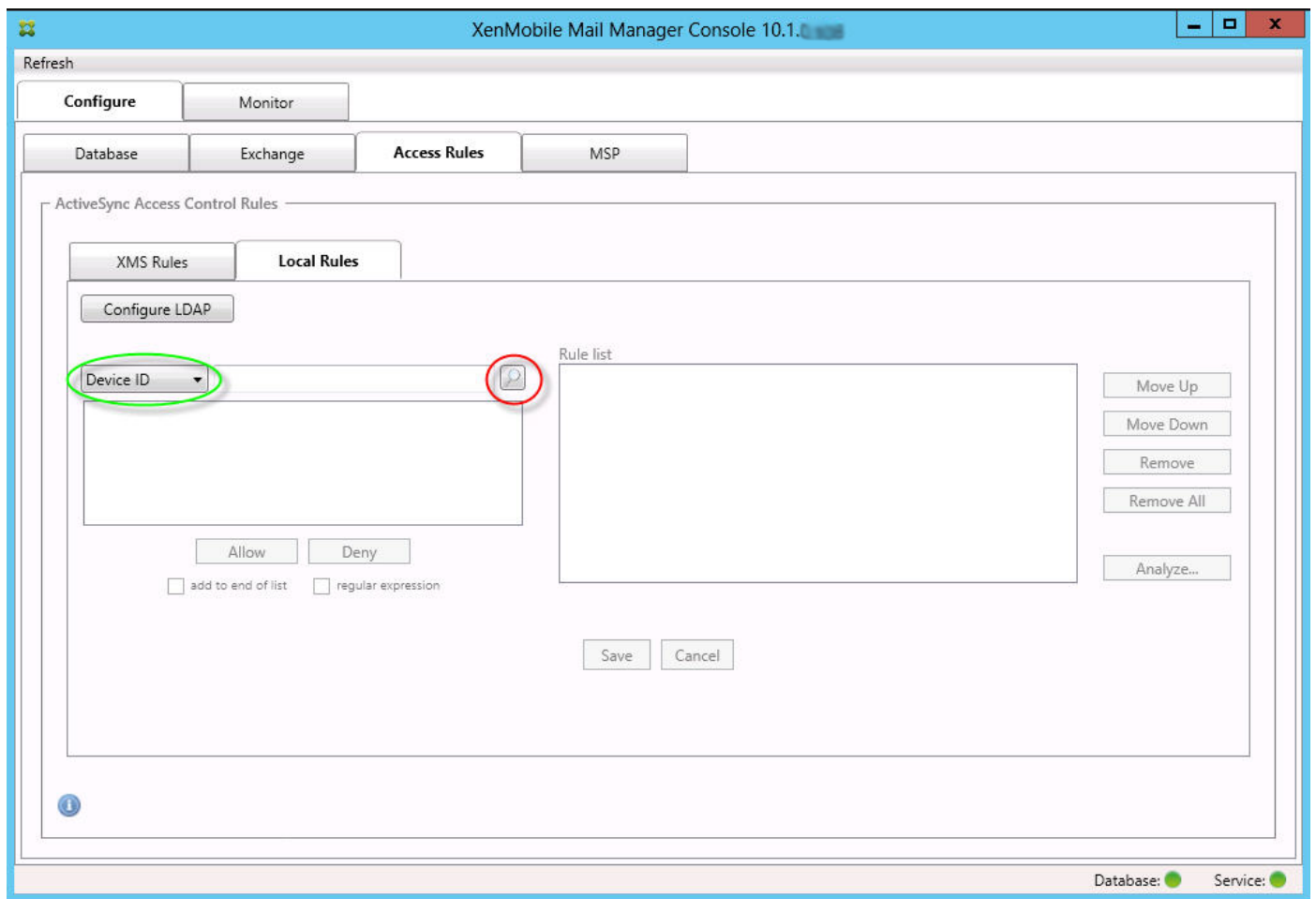


添加正则表达式

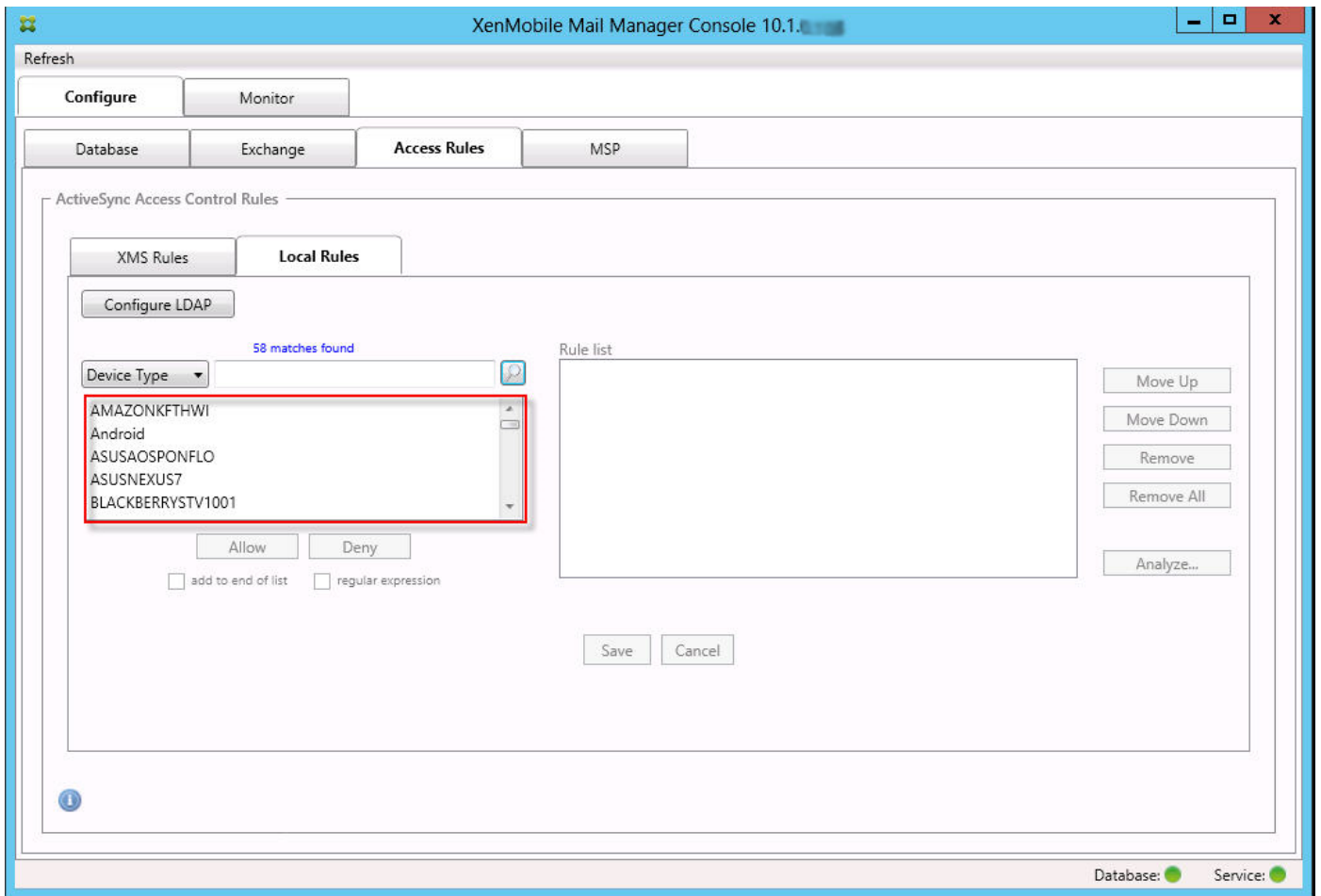
正则表达式本地规则可通过其旁边显示的图标进行区分 - 。要添加正则表达式规则，您可以通过给定字段的结果列表中的现有值来构建正则表达式规则（只要已完成主要快照），或只需键入您想要的正则表达式。

从现有字段值构建正则表达式

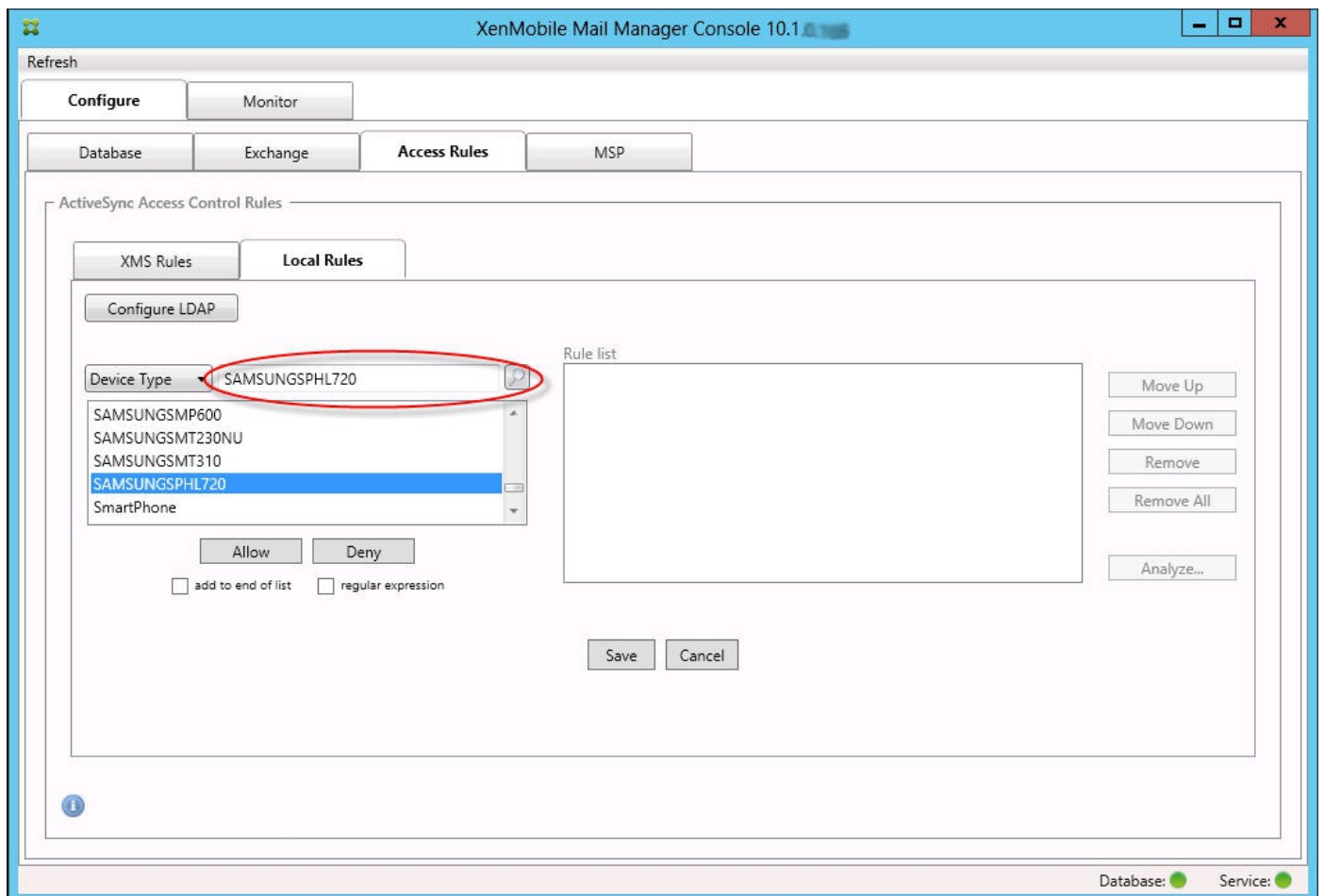
1. 单击 Access Rules（访问规则）选项卡。



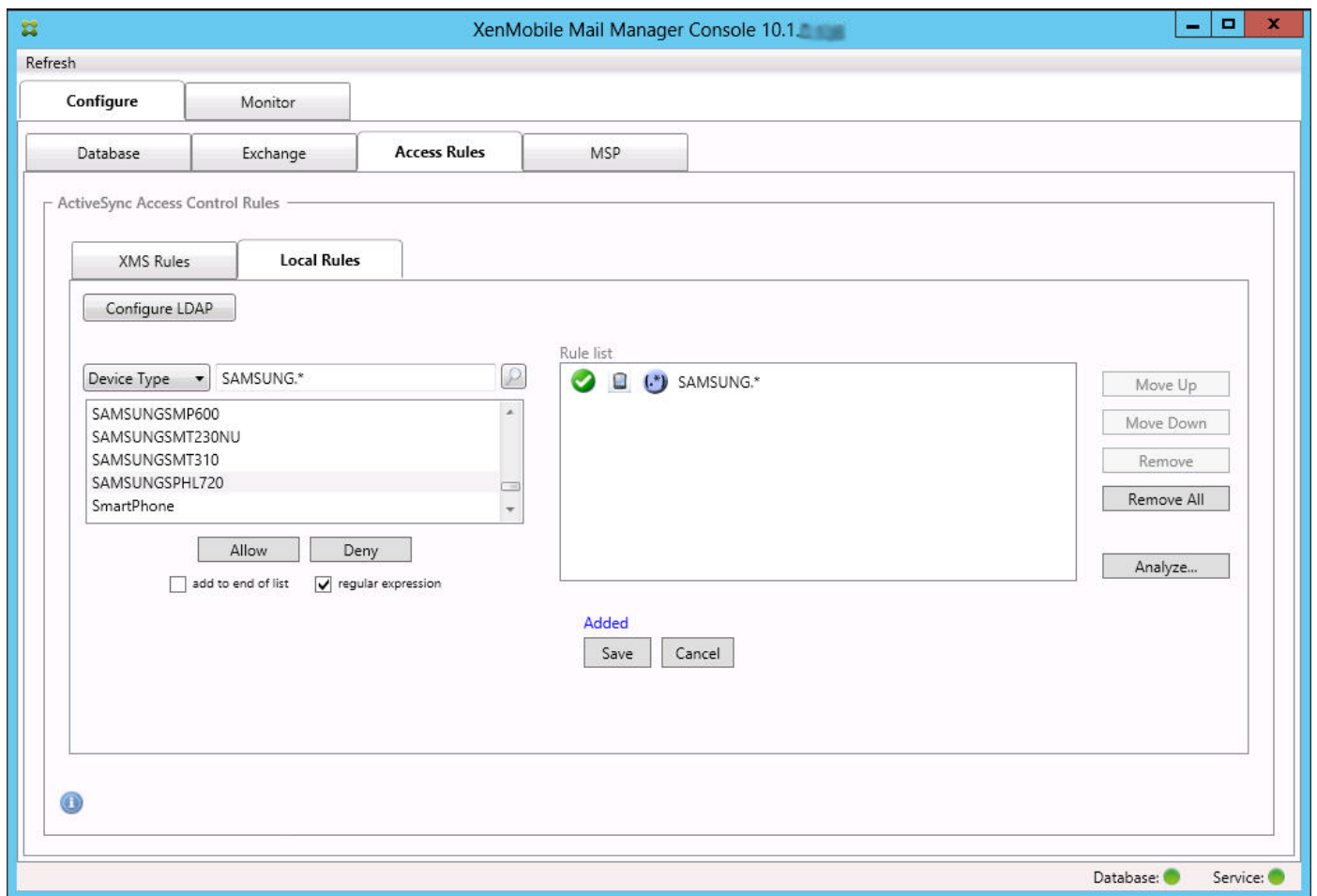
2. 在设备 ID 列表中，选择要为其创建正则表达式本地规则的字段。
3. 单击放大镜图标显示所选字段的所有唯一匹配项。在此示例中，已选择设备类型字段，选项显示在下面的列表框中。



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。

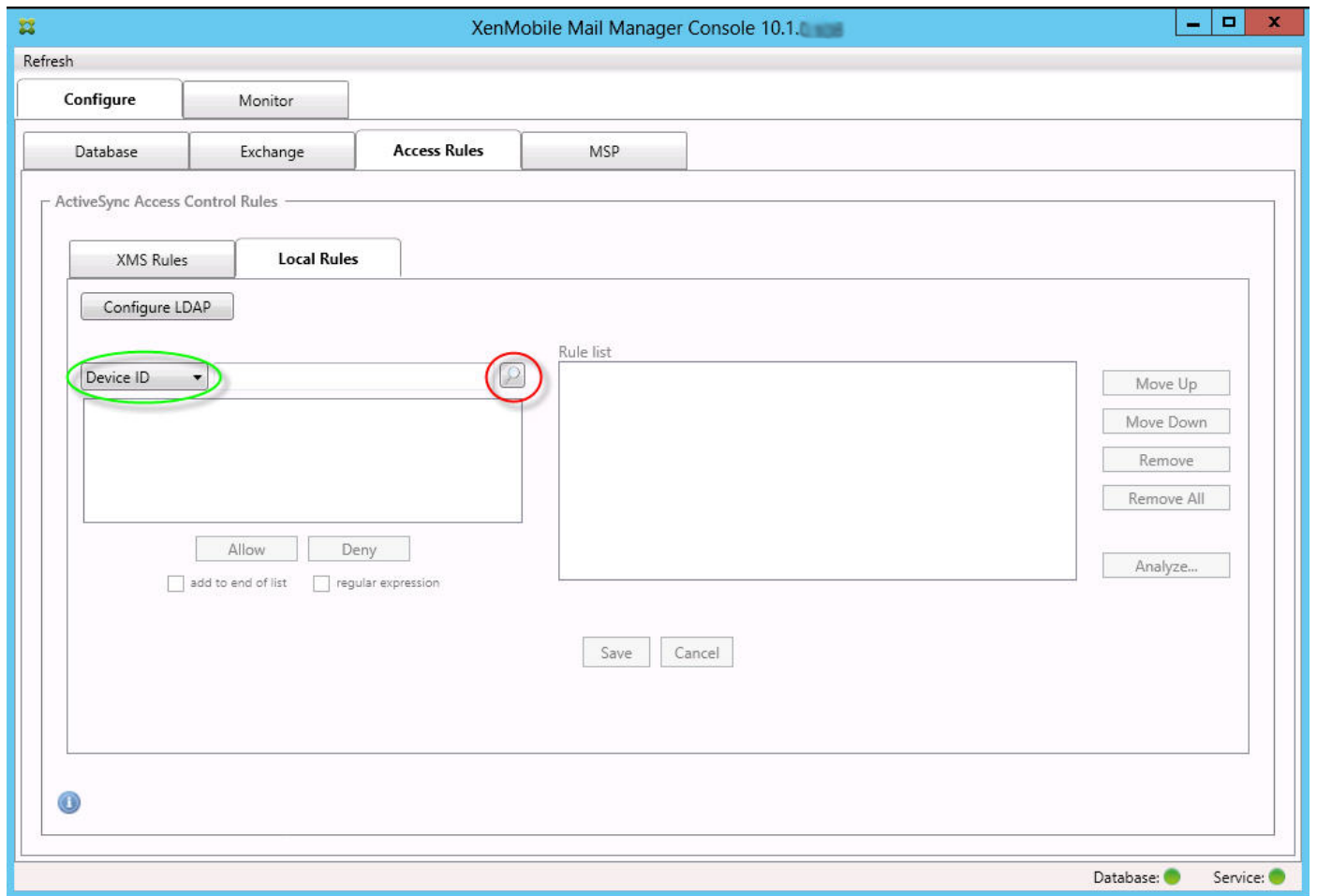


5. 要允许设备类型值中包含“Samsung”的所有设备，请按照以下步骤添加正则表达式规则：
 1. 在所选项目文本框内单击。
 2. 将文本从 SAMSUNGSPHL720 更改为 SAMSUNG.*
 3. 确保选中正则表达式复选框。
 4. 单击允许。

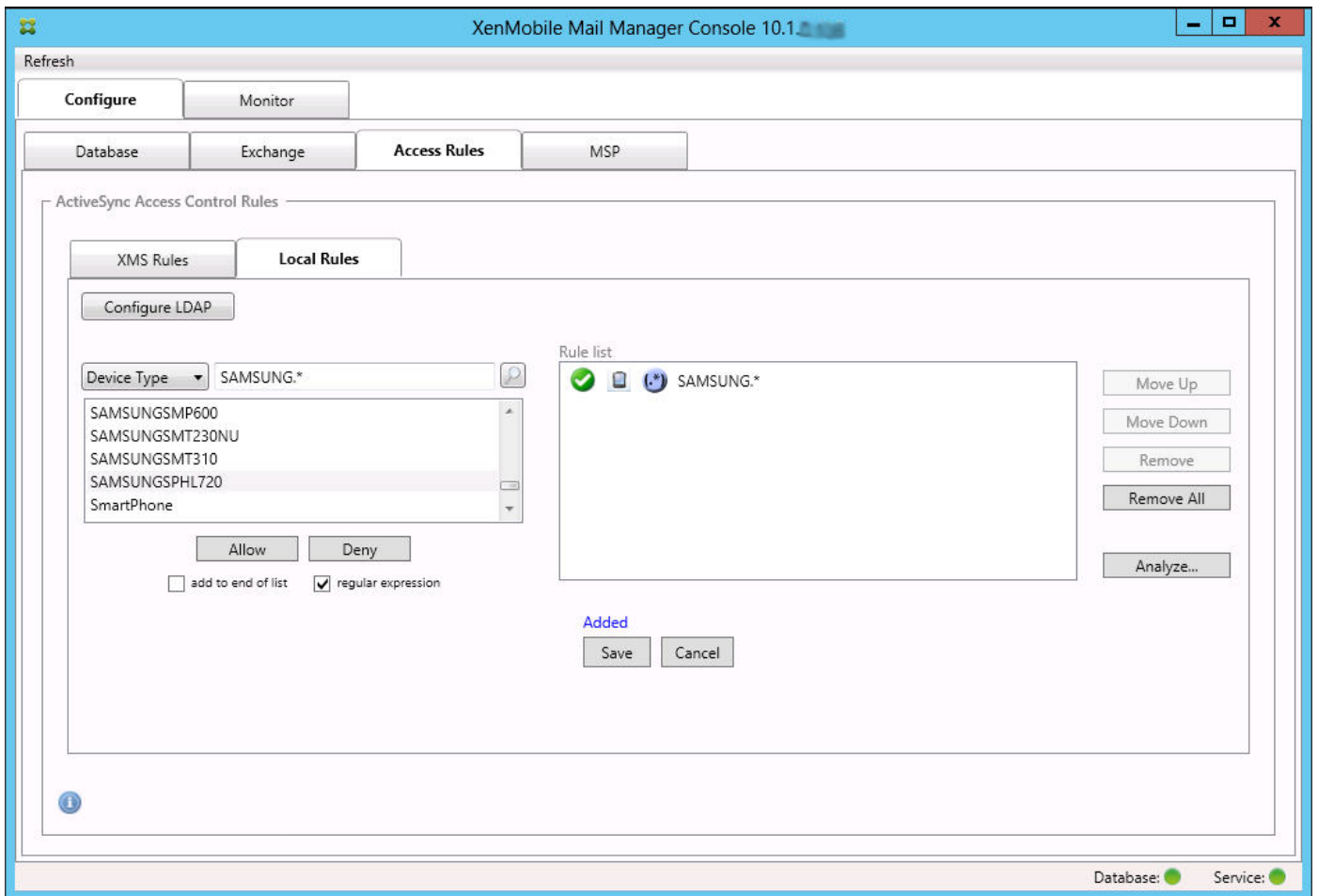


构建访问规则

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。



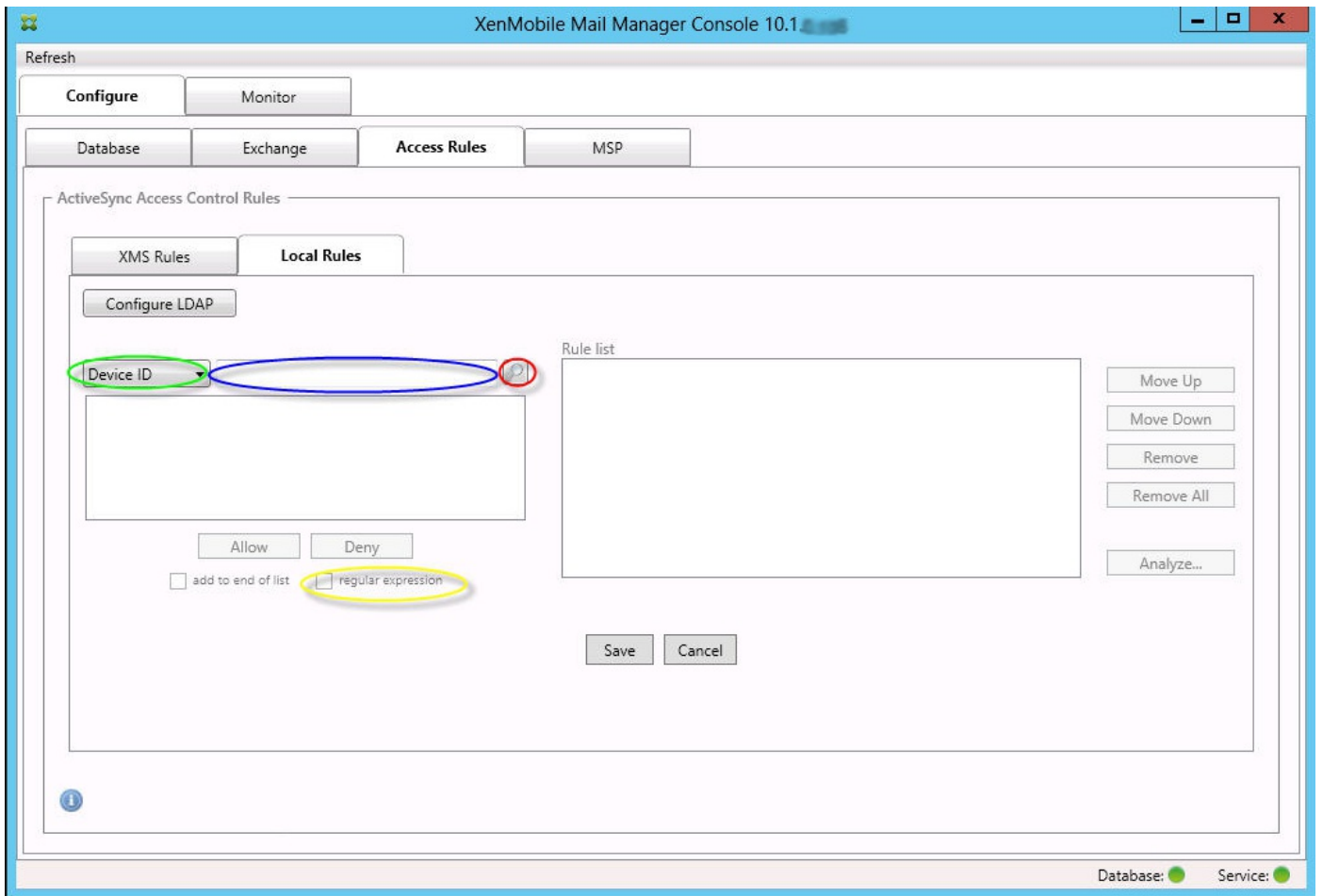
3. 选择要匹配的字段。此示例使用设备类型。
4. 键入正则表达式。此示例使用 `samsung.*`
5. 确保选中正则表达式复选框，然后单击允许或拒绝。在此示例中，选择的是允许，因此最终结果如下所示：



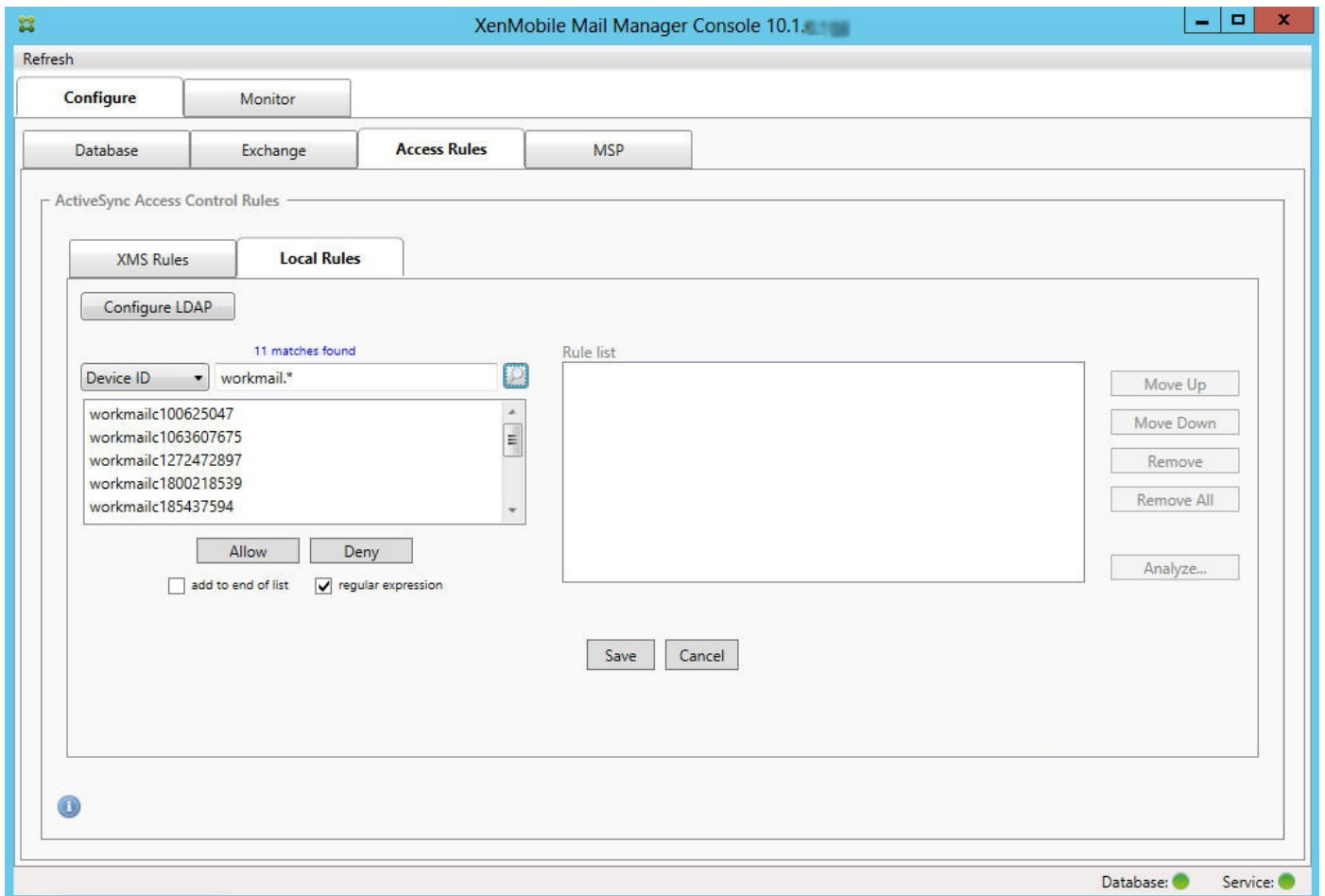
查找设备

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）中单击，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。

XenMobile Mail Manager Console 10.1

Refresh

Configure **Monitor**

ActiveSync Devices Blackberry Devices Automation History

Selection

All Devices Anytime User: user Device: Go Export...

Reported State	Requested State	User	Device ID	Type	Model
✓	?	auser1@xmlab.net	workmailc1800218539	MOTOROLAXT1528	XT1528
User Agent: WorkMail/10.3.0.225 (MOT Identity: xmlab.net/XM1/Lorna J Chan Last snapshot: 8/10/2016 1:49:52 PM First Sync: 4/12/2016 2:28:49 PM					
✓	?	auser1@xmlab.net	A182EB4483E64A99B4CED204444A63C7	iPad	iPad
✓	?	auser101@xmlab.net	96D3D564B5EA4EF28E891EE1D987817A	iPad	iPad
✓	?	auser101@xmlab.net	E4562615700543C58C68E5125D67DFBD	iPad	iPad
✓	?	auser101@xmlab.net	38939C2CE9254CE5A0A2ED18E906F9C1	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc680977375	MOTOROLAXT1068	XT1068
✓	?	auser101@xmlab.net	workmailc1929821768	MOTOROLANEXUS6	Nexus 6
✓	?	auser101@xmlab.net	0BD6E5254A6348FC9E3BF3EAF8FD8901	iPhone	iPhone
✓	?	auser101@xmlab.net	580D5785F02F48669457BD7E680DB38B	iPhone	iPhone
✓	?	auser101@xmlab.net	7DA7ED6B6ACE43C3928C6C357F6D7B97	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc185437594	HTCNEXUS9	Nexus 9
✓	?	auser101@xmlab.net	workmailc100625047	SAMUNGSM230NU	SM-T230NU
✓	?	auser101@xmlab.net	2FAFE4CF00794BA18AB4647F581C0148	iPhone	iPhone

70 records read, 39 records displayed

Database: ● Service: ●

设备监视

Feb 27, 2017

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。
- Blackberry Devices (黑莓设备)
- Automation History (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

Feb 27, 2017

XenMobile Mail Manager 将错误和其他操作信息记录到其日志文件：<安装文件夹>\log\XmmWindowsService.log。

XenMobile Mail Manager 还将重要事件记录到 Windows 事件日志。

常见错误

以下列表包括常见错误：

XenMobile Mail Manager Service 未启动

检查日志文件和 Windows 事件日志中的错误。包括以下典型原因：

- XenMobile Mail Manager Service 无法访问 SQL Server。以下这些问题可能导致此情况：
 - SQL Server 服务不在运行。
 - 身份验证失败。

如果已配置 Windows 集成身份验证，必须允许 XenMobile Mail Manager Service 的用户帐户进行 SQL 登录。XenMobile Mail Manager Service 的帐户默认设置为“Local System”（本地系统），但是可能更改为任何具有本地管理员权限的帐户。

如果已配置 SQL 身份验证，必须在 SQL 中正确配置 SQL 登录。

- 为移动服务提供商 (MSP) 配置的端口不可用。必须选择未被系统中其他进程使用的侦听端口。

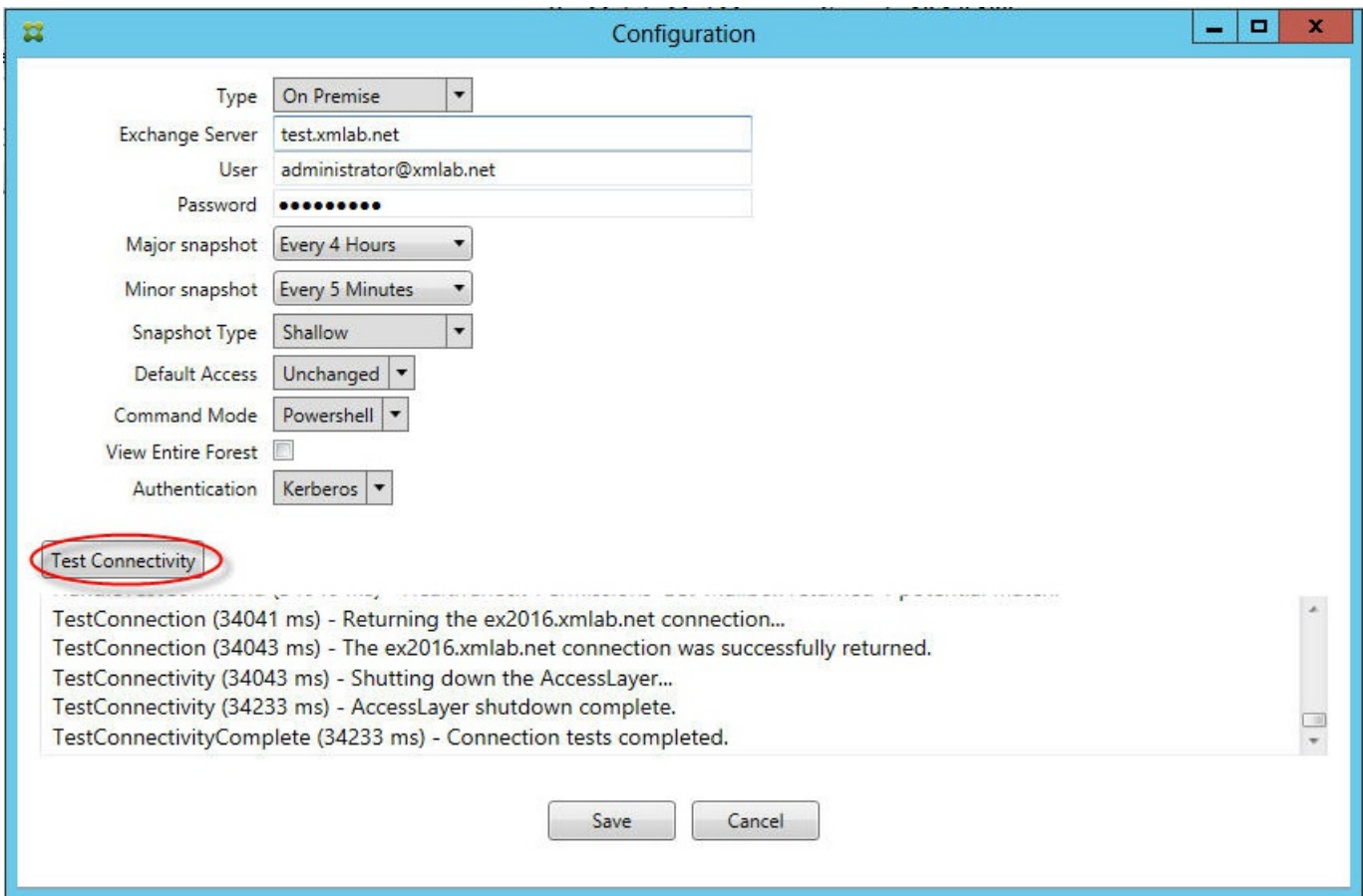
XenMobile 无法连接到 MSP

检查是否已在 XenMobile Mail Manager 控制台的配置 > MSP 选项卡中正确配置 MSP 服务端口和传输。检查是否已正确设置授权组或用户。

如果已配置 HTTPS，则必须安装有效的 SSL 服务器证书。如果已安装 IIS，IIS Manager 可以用来安装证书。如果未安装 IIS，有关安装证书的详细信息，请参见 <http://msdn.microsoft.com/en-us/library/ms733791.aspx>。

XenMobile Mail Manager 包含测试与 MSP Service 的连接实用程序。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，请确保至少具有一条 ActiveSyncDevice 记录，否则测试可能会失败。



故障排除工具

Support\PowerShell 文件夹中提供了一组用于故障排除的 PowerShell 实用程序。

故障排除工具将对用户的邮箱和设备执行深度分析（从而检测错误条件和潜在的故障区域）并对用户执行深度 RBAC 分析。该工具可以将所有 cmdlet 的原始输出保存到一个文本文件。

XenMobile NetScaler Connector

Feb 27, 2017

XenMobile NetScaler Connector 向 NetScaler 提供 ActiveSync 客户端的设备级别授权服务，而 NetScaler 用作 Exchange ActiveSync 协议的反向代理。授权由在 XenMobile 中定义的策略组合以及 XenMobile NetScaler Connector 本地定义的规则控制。

有关详细信息，请参阅以下文章：

- [XenMobile NetScaler Connector](#)
- [XenMobile 中的 ActiveSync Gateway](#)

有关详细的参考体系结构图，请参阅《XenMobile 部署手册》文章[适用于本地部署的参考体系结构](#)。

高级概念

Aug 09, 2017

内部部署 XenMobile 与 Active Directory 的交互

Siddhartha Vuppala | Aug 09, 2017

本文解释 XenMobile Server 与 Active Directory 之间的交互。XenMobile Server 与 Active Directory 可以进行内联交互，也可以在后台交互。以下部分将详细介绍涉及到 Active Directory 交互的内联操作和后台操作。

注意

本文是对交互的概述，不提供具体细节。有关在 XenMobile 控制台中配置 Active Directory 和 LDAP 的详细信息，请参阅[域或域加安全令牌身份验证](#)。

内联交互

XenMobile Server 使用管理员配置的 LDAP 与 Active Directory 通信。这些设置会检索用户和组的有关信息。以下是会导致 XenMobile Server 与 Active Directory 之间发生交互的操作。

1. **LDAP 配置。**配置 Active Directory 本身会导致与 Active Directory 交互。XenMobile Server 会尝试通过使用 Active Directory 进行身份验证来验证信息。服务器通过使用 Internet 协议、端口和提供的服务帐户凭据完成此操作。成功绑定表示已正确配置连接。
2. **基于组的交互。**
 - a. 在创建基于角色的访问控制 (RBAC) 和交付组定义期间搜索一个或多个组。XenMobile Server 管理员在 XenMobile 控制台中输入搜索文本字符串。XenMobile Server 在选定的域中搜索包含所提供子字符串的所有组。然后，XenMobile Server 检索通过搜索识别出的组的 objectGUID、sAMAccountName 和标识名属性。

注意

此信息存储在 XenMobile Server 数据库中。

- b. RBAC 和部署组定义的添加或更新。XenMobile Server 管理员根据之前的搜索选择感兴趣的 Active Directory 组并将其包含在部署组定义中。XenMobile Server 在 Active Directory 中搜索特定组，每次搜索一个。XenMobile Server 搜索 objectGUID 属性并检索选定的属性，其中包括成员身份信息。组成员身份信息可帮助在检索到的组与 XenMobile Server 数据库的现有用户或组之间确定成员身份。更改组成员身份会导致受影响的用户成员发生 RBAC 和部署组派生，从而导致用户授权。

注意

更改部署组定义可能会导致受影响用户的应用程序或策略授权发生变化。

- c. **一次性 PIN (OTP) 邀请。**XenMobile Server 管理员从 XenMobile Server 数据库中的 Active Directory 组列表中选择某个组。对于此组，所有用户（包括直接用户和间接用户）均检索自 Active Directory。OTP 邀请发送给在上述步骤中识别出的用户。

注意

上述三个交互说明基于组的交互因 XenMobile Server 配置更改而触发。如果配置没有发生变更，则意味着不包含与 Active Directory 的交互。它们也说明后台作业无需定期捕获组的变化。

3. 基于用户的交互。

a. 用户身份验证。用户身份验证工作流程会产生与 Active Directory 的两种交互：

- 用于使用提供的凭据对用户进行身份验证。
- 将所选用户属性添加或更新到 XenMobile Server 数据库，这些属性包括 objectGUID、标识名、sAMAccountName 和对组的直接成员关系。更改组成员身份会导致重新评估应用程序、策略和访问授权。

用户可以从设备或 XenMobile Server 控制台进行身份验证。在这两种情况下，与 Active Directory 的交互都遵循相同的行

b. 应用商店访问和刷新。刷新应用商店会导致刷新用户属性，其中包括直接组成员身份。此操作会引起重新评估用户授权。

c. 设备签入。管理员可以在 XenMobile 控制台中定期配置设备签入。每次签入设备时，都会刷新相应的用户属性，其中包括直接组成员身份。这些签入会引起重新评估用户授权。

d. 按组进行 OTP 邀请。XenMobile Server 管理员从 XenMobile Server 数据库中的 Active Directory 组列表中选择某个组。包括直接和间接（缘于嵌套）在内的用户成员均检索自 Active Directory 并保存在 XenMobile Server 数据库中。OTP 邀请会发送给在上述步骤中识别出的用户成员。

e. 按用户进行 OTP 邀请。管理员在 XenMobile 控制台中输入搜索文本字符串。XenMobile Server 查询 Active Directory 并返回与输入的文本字符串匹配的用户记录。然后，管理员选择要向其发送 OTP 邀请的用户。在向用户发送邀请前，XenMobile Server 会从 Active Directory 检索用户的详细信息，并在数据库中更新同样的详细信息。

后台交互

从与 Active Directory 的内联通信可以得出一个结论，即基于组的交互因更改 XenMobile Server 配置而触发。如果配置没有发生变更，则意味着不包含与 Active Directory 的交互。

这种交互需要后台作业：与 Active Directory 定期同步并将相关更改更新到感兴趣的组。

以下是与 Active Directory 交互的后台作业。

1. **组同步作业。**此作业的目的是查询 Active Directory，每次针对一个感兴趣的组，以获取标识名或 sAMAccountName 属性的更改情况。对 Active Directory 的搜索查询使用感兴趣组的 objectGUID，以获取标识名和 sAMAccountName 属性的当前值。感兴趣组的标识名或 sAMAccountName 值的变化将更新到数据库中。

注意

此作业不更新用户相对于组的成员身份信息。

2. **嵌套组同步作业。**此作业更新感兴趣组的嵌套层次结构中发生的变化。XenMobile Server 允许感兴趣组的直接成员和间接成员获得授权。用户的直接成员身份在基于用户的内联交互过程中更新。此作业在后台运行，跟踪间接成员身份。如果用户所

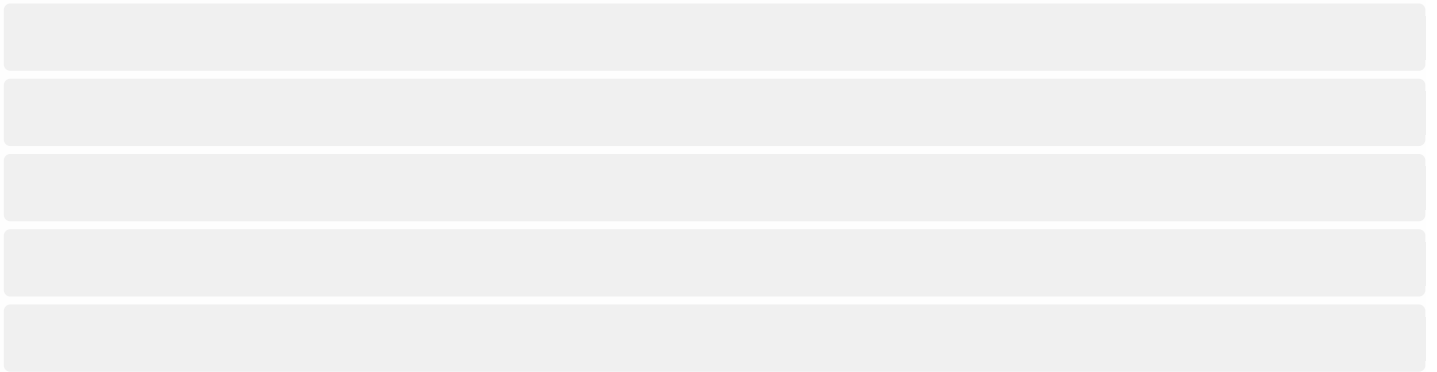
属的组是感兴趣组的成员，则形成间接成员身份。

此作业从 XenMobile Server 数据库搜集 Active Directory 组的列表。这些组属于部署组或 RBAC 定义。对于此列表中的每个组，XenMobile Server 会获取该组的成员。组的成员是代表用户和组的标识名列表。XenMobile Server 再查询 Active Directory，以获取感兴趣组的用户成员。这两个列表的差异仅针对感兴趣组的组成员。成员组中的变化将更新到数据库。会针对层次结构中的所有组重复相同的过程。

嵌套更改会导致处理受影响的用户以执行授权更改。

3. **禁用的用户检查。** 仅当 XenMobile 管理员创建用于检查被禁用用户的操作时才会运行此作业。此作业在组同步作业的范围
内运行。此作业查询 Active Directory 以检查感兴趣用户的禁用状态，每次一个用户。

常见问题解答



内部部署 XenMobile 与 Active Directory 的交互

Siddhartha Vuppala | Aug 09, 2017

本文解释 XenMobile Server 与 Active Directory 之间的交互。XenMobile Server 与 Active Directory 可以进行内联交互，也可以在后台交互。以下部分将详细介绍涉及到 Active Directory 交互的内联操作和后台操作。

注意

本文是对交互的概述，不提供具体细节。有关在 XenMobile 控制台中配置 Active Directory 和 LDAP 的详细信息，请参阅[域或域加安全令牌身份验证](#)。

内联交互

XenMobile Server 使用管理员配置的 LDAP 与 Active Directory 通信。这些设置会检索用户和组的有关信息。以下是会导致 XenMobile Server 与 Active Directory 之间发生交互的操作。

1. **LDAP 配置。**配置 Active Directory 本身会导致与 Active Directory 交互。XenMobile Server 会尝试通过使用 Active Directory 进行身份验证来验证信息。服务器通过使用 Internet 协议、端口和提供的服务帐户凭据完成此操作。成功绑定表示已正确配置连接。
2. **基于组的交互。**
 - a. 在创建基于角色的访问控制 (RBAC) 和交付组定义期间搜索一个或多个组。XenMobile Server 管理员在 XenMobile 控制台中输入搜索文本字符串。XenMobile Server 在选定的域中搜索包含所提供子字符串的所有组。然后，XenMobile Server 检索通过搜索识别出的组的 objectGUID、sAMAccountName 和标识名属性。

注意

此信息存储在 XenMobile Server 数据库中。

- b. RBAC 和部署组定义的添加或更新。XenMobile Server 管理员根据之前的搜索选择感兴趣的 Active Directory 组并将其包含在部署组定义中。XenMobile Server 在 Active Directory 中搜索特定组，每次搜索一个。XenMobile Server 搜索 objectGUID 属性并检索选定的属性，其中包括成员身份信息。组成员身份信息可帮助在检索到的组与 XenMobile Server 数据库的现有用户或组之间确定成员身份。更改组成员身份会导致受影响的用户成员发生 RBAC 和部署组派生，从而导致用户授权。

注意

更改部署组定义可能会导致受影响用户的应用程序或策略授权发生变化。

- c. **一次性 PIN (OTP) 邀请。**XenMobile Server 管理员从 XenMobile Server 数据库中的 Active Directory 组列表中选择某个组。对于此组，所有用户（包括直接用户和间接用户）均检索自 Active Directory。OTP 邀请发送给在上述步骤中识别出的用户。

注意

上述三个交互说明基于组的交互因 XenMobile Server 配置更改而触发。如果配置没有发生变更，则意味着不包含与 Active Directory 的交互。它们也说明后台作业无需定期捕获组的变化。

3. 基于用户的交互。

a. 用户身份验证。用户身份验证工作流程会产生与 Active Directory 的两种交互：

- 用于使用提供的凭据对用户进行身份验证。
- 将所选用户属性添加或更新到 XenMobile Server 数据库，这些属性包括 objectGUID、标识名、sAMAccountName 和对组的直接成员关系。更改组成员身份会导致重新评估应用程序、策略和访问授权。

用户可以从设备或 XenMobile Server 控制台进行身份验证。在这两种情况下，与 Active Directory 的交互都遵循相同的行

b. 应用商店访问和刷新。刷新应用商店会导致刷新用户属性，其中包括直接组成员身份。此操作会引起重新评估用户授权。

c. 设备签入。管理员可以在 XenMobile 控制台中定期配置设备签入。每次签入设备时，都会刷新相应的用户属性，其中包括直接组成员身份。这些签入会引起重新评估用户授权。

d. 按组进行 OTP 邀请。XenMobile Server 管理员从 XenMobile Server 数据库中的 Active Directory 组列表中选择某个组。包括直接和间接（缘于嵌套）在内的用户成员均检索自 Active Directory 并保存在 XenMobile Server 数据库中。OTP 邀请会发送给在上述步骤中识别出的用户成员。

e. 按用户进行 OTP 邀请。管理员在 XenMobile 控制台中输入搜索文本字符串。XenMobile Server 查询 Active Directory 并返回与输入的文本字符串匹配的用户记录。然后，管理员选择要向其发送 OTP 邀请的用户。在向用户发送邀请前，XenMobile Server 会从 Active Directory 检索用户的详细信息，并在数据库中更新同样的详细信息。

后台交互

从与 Active Directory 的内联通信可以得出一个结论，即基于组的交互因更改 XenMobile Server 配置而触发。如果配置没有发生变更，则意味着不包含与 Active Directory 的交互。

这种交互需要后台作业：与 Active Directory 定期同步并将相关更改更新到感兴趣的组。

以下是与 Active Directory 交互的后台作业。

1. **组同步作业。**此作业的目的是查询 Active Directory，每次针对一个感兴趣的组，以获取标识名或 sAMAccountName 属性的更改情况。对 Active Directory 的搜索查询使用感兴趣组的 objectGUID，以获取标识名和 sAMAccountName 属性的当前值。感兴趣组的标识名或 sAMAccountName 值的变化将更新到数据库中。

注意

此作业不更新用户相对于组的成员身份信息。

2. **嵌套组同步作业。**此作业更新感兴趣组的嵌套层次结构中发生的变化。XenMobile Server 允许感兴趣组的直接成员和间接成员获得授权。用户的直接成员身份在基于用户的内联交互过程中更新。此作业在后台运行，跟踪间接成员身份。如果用户所

属的组是感兴趣组的成员，则形成间接成员身份。

此作业从 XenMobile Server 数据库搜集 Active Directory 组的列表。这些组属于部署组或 RBAC 定义。对于此列表中的每个组，XenMobile Server 会获取该组的成员。组的成员是代表用户和组的标识名列表。XenMobile Server 再查询 Active Directory，以获取感兴趣组的用户成员。这两个列表的差异仅针对感兴趣组的组成员。成员组中的变化将更新到数据库。会针对层次结构中的所有组重复相同的过程。

嵌套更改会导致处理受影响的用户以执行授权更改。

3. **禁用的用户检查。** 仅当 XenMobile 管理员创建用于检查被禁用用户的操作时才会运行此作业。此作业在组同步作业的范围
内运行。此作业查询 Active Directory 以检查感兴趣用户的禁用状态，每次一个用户。

常见问题解答

默认情况下，后台作业运行的频率是多少？



为什么需要执行组同步作业？



是否可以关闭组同步作业？



为什么需要嵌套组处理后台作业？



是否可以关闭嵌套组处理作业？

