PoC标准化实施指南

基础环境

部署XenMobile并与XenDeskotp集成

版本：1.0

思杰 | CITRIX

目　　录

思杰 | CITRIX®

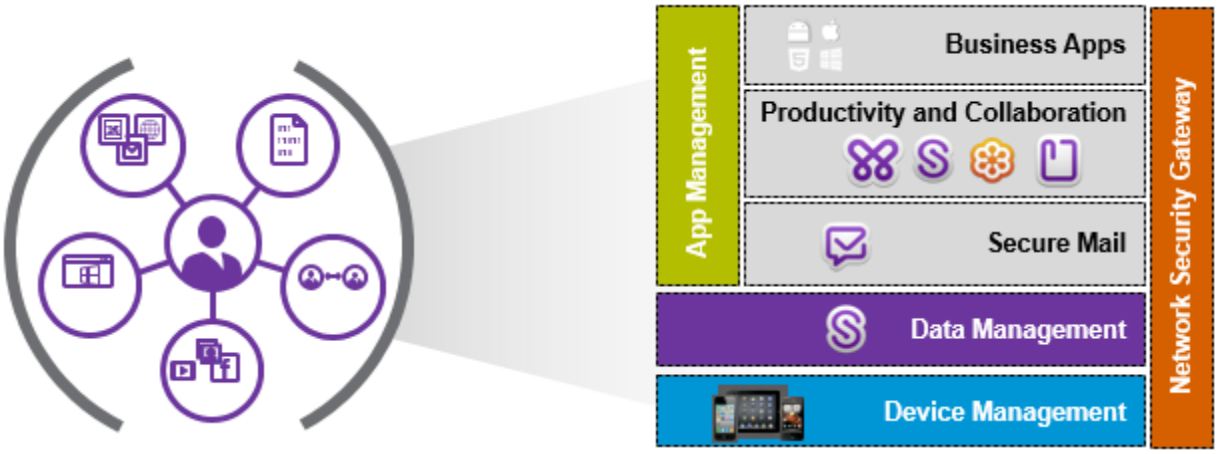
修正历史

修正	改变说明	更新者	日期
V1.0	新建	钱凯	2015年08月18日
V1.0	审核	Michael Zhang	2015年08年25日

第1章 XenMobile 简述

随着中国互联网基础设施建设的提速和各种移动终端设备的普及，企业中的雇员越来越多地使用移动终端设备，如：iPhone、PAD 平板电脑，帮助处理日常事务。这些新型设备为强企业员工带来便利的同时，却给企业管理带来了新的调整。为了更好的规范管理 Phone、Pad 设备和移动应用，防范因越狱及木马程序可能造成的数据外泄等安全隐患，保障企业邮件信息处理的安全性，通过建设企业级移动设备管理系统（Enterprise Mobile Management），以实现对移动终端设备和应用程序的集中安全管控，变成为新的企业 IT 的选择。

所以现阶段 Citrix 的解决不仅可以交付传统 Windows 桌面和应用，还可以管理移动设备并统一化的交付企业开发的移动应用，通过附加 Citrix XenMobile 的移动沙箱技术，提供企业移动化场景中高安全基准，形成统一的企业资源（Windows 应用、桌面、原生应用、数据）的交付平台。



同时 Citrix 不仅可以交付客户自开发的应用，同时 Citrix 从企业员工的移动化角度出发，为企业人员在移动设备上最常使用的应用，邮箱以及通过邮箱相关各型需求，如：内网访问，数据交付等，Citrix 开发了市面最易用、最安全的邮箱客户端 Worxmail 以及其他相关应用。

本例中，完成 XenMobile 的基本安装部署和 Citrix 部分自用产品的交付，对于如何使用 Citrix XenMobile 封装自有应用以及更复杂的策略，请参见官方网站。

思杰 | CITRIX

第2章 主要步骤

本章节主要介绍如何安装、部署和配置XenMobile，以及如何与现有的XenDesktop/XenApp，NetScaler做集成。其包括了：

- XenMobile的基本安装
- XenMobile的基本配置及策略设定
- 配置NetScaler、StoreFront以完成XenMobile集成

第3章 准备工作

由于移动化产品是一个更新极为快速的 IT 产品分支，Citrix XenMobile 产品基本保持 18 个星期更新一次 WorxApps 应用（WorxMail 等），3~6 个月更新一次 XenMobile 服务器端的速度进行发布。所以所有相关产品的更新周期频度都要高于传统的 IT 产品，本例中产品版本为：

XenMobile	10.1.63030
NetScaler	10.5.56.22
XenDesktop	7.6FP2
StoreFront	3.0

随着 XenMobile10 中 MDM/MAM 体系的统一，架构将保持稳定，所以后续版本基本可以参考此文档。请注意，本 PoC 文档不适用 XenMobile 8.X/9.X。

思杰 | CITRIX

第4章 XenMobile 的基本安装

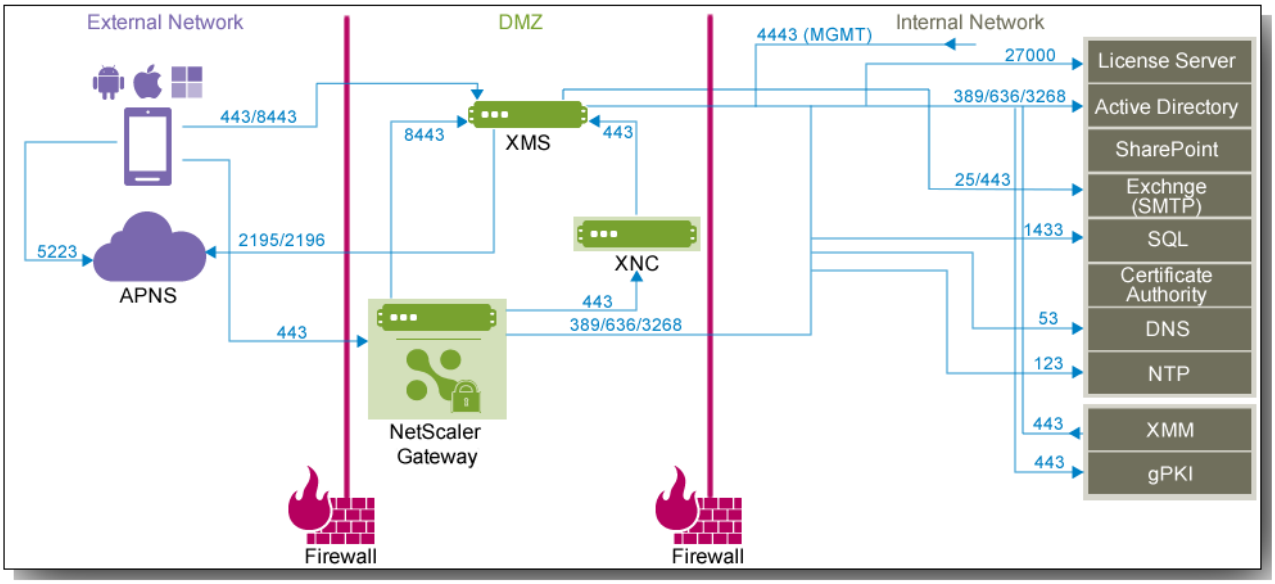
4.1 准备工作

XenMobile 在部署、运维阶段最重要的是网络规划，请在在部署前做好相应的规划。下面是本例中一些使用到 IP 和域名信息。

前提条件或设置	组件或功能	记录设置
远程用户连接使用的外网域名（FQDN），包括：XenMobile 服务器使用的 FQDN，以及端口（缺省 443,8443，如果与 AG 共享 IP，可使用 444,8443） 和 AG 网关使用的 FQDN 及端口（缺省 443）	XenMobile Server FQDN NetScaler 网关 FQDN（如果使用 AG）	XMS 外网 FQDN 及端口： xms.citrixlab.com 443, 8443 AG 外网 FQDN 及端口： mam.citrixlab.com 443
环境使用的公共和本地 IP 地址段，子网掩码，网关地址，DNS，IP 地址	XenMobile NetScaler	192.168.10.x Mask:255.255.255.0 GW:192.168.10.1 DNS: 10.151
XenMobile 的 IP 地址。 为您安装 XenMobile 的每一个实例保留一个 IP 地址。 如果配置集群，请注意记录所有节点 IP 地址。	XenMobile	XMS IP： 192.168.10.156
Netscaler 的 IP 地址： NSIP：NS 的管理 IP SNIP:对内资源访问使用的 IP VIP：包括 LB VIP 和 AG VIP 并分别为其分配一个公网的域名记录。并且确保该 FQDN 与 SSL 证书中配置的域名一致。	NetScaler 的网关	NSIP： 192.168.10.145 SNIP： 192.168.10.146 LBVIP：(本例无) 192.168.10.xx mam NS VIP： 192.168.10.149
确保 XenMobile 服务器，NetScaler 网关，外部 Microsoft SQL Server 和 DNS 服务器，域控制器等各组件之间的网络连接是否联通。	XenMobile NetScaler 的网关	本例使用 XMS 自带数据库

4.1.1 XenMobile MDM+MAM+NS 逻辑架构图

请确保图中所示端口都已经正确开放。本例中不涉及到 XNC，可以忽略。



4.1.2 完整端口列表

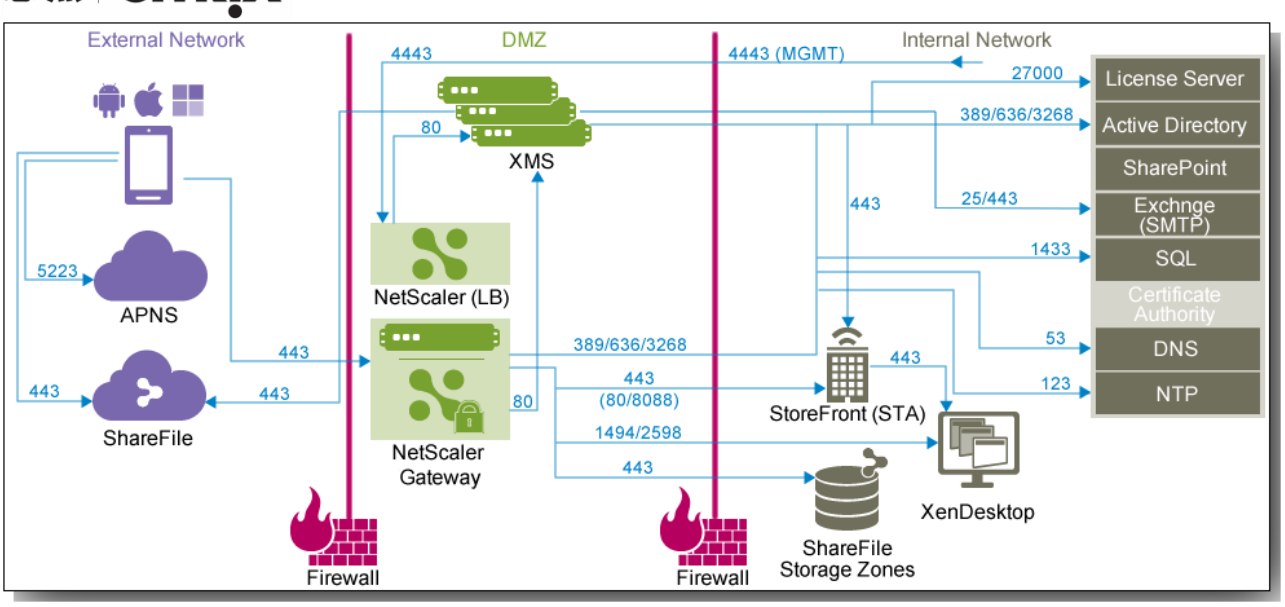
如果客户网络环境较为复杂，请严格参考如下规则与客户的网络部门协调端口开放事宜：

TCP Port	Description	Source	Destination
Inbound from the Internet to Access Gateway			
443	Worx Home connecting to Access Gateway	Internet	Access Gateway
Inbound from the Internet to XMS			
443	SSL OTA Enrollment/Agent Setup (Android & Windows Mobile), All Device related traffic and data connections (iOS, Android & Windows Mobile) , XMDM Web Console	Internet	XMS Server
8443	Over-the-Air (OTA) Enrollment for iOS Devices only	Internet	XMS Server
Inbound from Access Gateway (DMZ) to Internal Network			
389 or 636	LDAP/LDAPS connection from the AG NSIP to Active Directory	DMZ	Active Directory
53	DNS connection from the AG SNIP to the DNS Server	DMZ	DNS Server
123	NTP connection from the AG SNIP to the NTP Server	DMZ	NTP Server
443	HTTPS connection from the AG SNIP to XMS	DMZ	XMS
80	HTTP connection from the AG SNIP to XMS	DMZ	XMS
443	HTTPS connection from the AG SNIP to the Exchange Server	DMZ	Exchange
Other Resources Ports (Example:	HTTP/HTTPS connections from the AG SNIP to Other Internal Resources	DMZ	Other Resources

Intranet, Expense App etc.)			
Outbound from Access Gateway (DMZ) to the Internet (If Restricted)			
SaaS App Ports	HTTP/HTTPS connections from the AG SNIP to SaaS Apps	DMZ	Internet
Inbound from XMS (DMZ) to Internal Network (If Firewall Exists)			
389 or 636	LDAP/LDAPS connection from the XMS to Active Directory	DMZ	Active Directory
53	DNS connection from the XMS to the DNS Server	DMZ	DNS Server
123	NTP connection from the XMS to the NTP Server	DMZ	NTP Server
Web App Ports	HTTP/HTTPS connections from the XMS to Web Apps	DMZ	Web Apps
1433	Remote database server connection to separate SQL Server (if not using built-in DB)	XMDM Server	SQL Server
25	Connector for SMTP notifications	XMDM Server	SMTP Server
Outbound from XMS (DMZ) to Internet			
SaaS App Ports	HTTP/HTTPS connections from the XMS to SaaS Apps	Internal Network	Internet
80	iTunes App Store connectivity for App importation	XMDM Server	LDAP / AD Directory Services
443	Connector for SMS notifications	XMDM Server	DNS Server
2195	Apple APNS (Push Notification Service) outbound connection to gateway.push.apple.com, used for iOS device notifications & device policy push	XMDM Server	Internet (Apple APNS Service Hosts on public IP network 17.0.0.0/8)
2196	Apple APNS (Push Notification Service) outbound connection to feedback.push.apple.com, used for iOS device notifications & device policy push	XMDM Server	Internet (Apple APNS Service Hosts on public IP network 17.0.0.0/8)
Outbound from the Wi-Fi network to Internet			
5223	Apple APNS (Push Notification Service) outbound connection for iOS devices connected via Wi-Fi network to *.push.apple.com	iOS device on Wi-Fi network service	Internet (Apple APNS Service Hosts on public IP network 17.0.0.0/8)

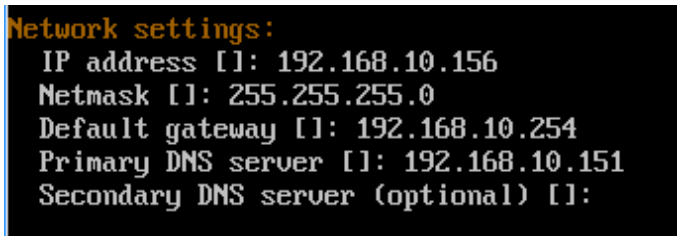
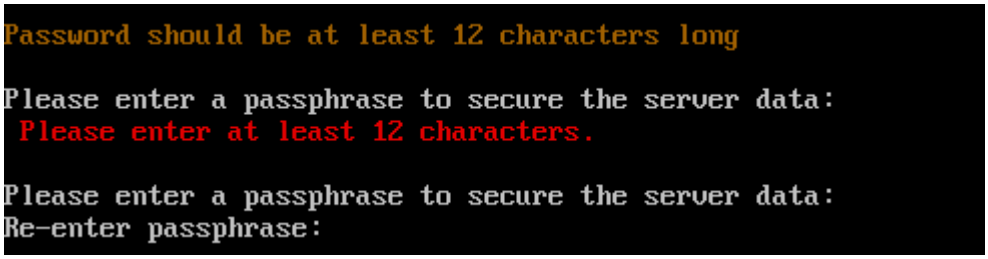
4.1.3 XenMobile 与 XenDesktop 集成架构图

本图涵盖了 NetScaler、XenMobile 与 StoreFront、XenDesktop 通信的示意图，如需完成集成，请仔细阅读。


External Network
DMZ
Internal Network
4443
4443 (MGMT)
27000
License Server
389/636/3268
Active Directory
80
XMS
SharePoint
443
25/443
Exchnge (SMTP)
1433
SQL
5223
APNS
NetScaler (LB)
Certificate Authority
53
DNS
389/636/3268
443
443
443
(80/8088)
StoreFront (STA)
123
NTP
443
443
80
ShareFile
NetScaler Gateway
1494/2598
443
XenDesktop
Firewall
Firewall
ShareFile Storage Zones

思杰 | CITRIX

4.2 XenMobile 的基本安装

步骤	操作
1.	由于移动端设备在注册（enroll）到 XenMobile 时，XenMobile 需要通过互联网联系 Apple 的官网，所以请务必确保 XenMobile 虚拟机能够访问互联网。
2.	打开 XenCenter 将 XenMobile 10.1 的镜像文件导入，所有参数默认。2vCPU，4G 内存，50G 硬盘空间。
3.	通过 Console 进行 XenMobile 配置，输入 IP 地址、子网、网关及 DNS 等基本信息。 
4.	输入一个 12 位密码进行数据加密。 
5.	对于是否需要启用 FIPS，请选 n。如果是外资公司，需要执行 FIPS 标准，请选择 Y。 选择数据库，由于本例为准备 PoC，选择 r。如果要启用 Cluster 功能，需要输入 r 并指向对应的 SQL Server 服务器。 
6.	输入主机名。请注意，此次输入的名称必须为规划中发布到公网上名称，即用户使用 WorxHome 注册时输入的地址。 

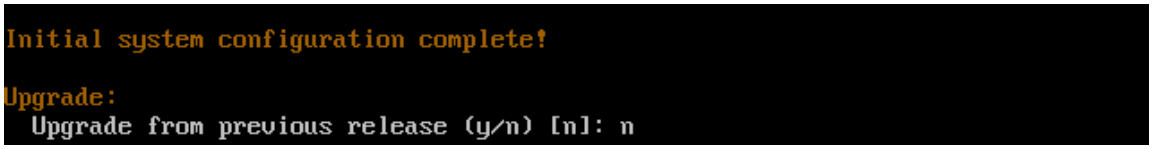
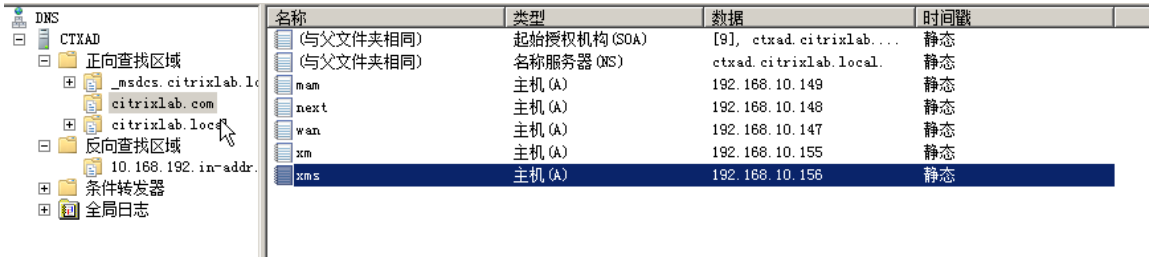
步骤	操作

7.	通讯端口，正常情况下选择默认，即不输入任何信息直接回车。如有需要请自行修改。
	`Communication ports:`
	`  HTTP [80]: 80`
	`  HTTPS with certificate authentication [443]: 443`
	`  HTTPS with no certificate authentication [8443]: 8443`
	`  HTTPS for management [4443]: 4443`
	`  Commit settings (y/n) [y]: y`
	`Applying port listener configuration...`

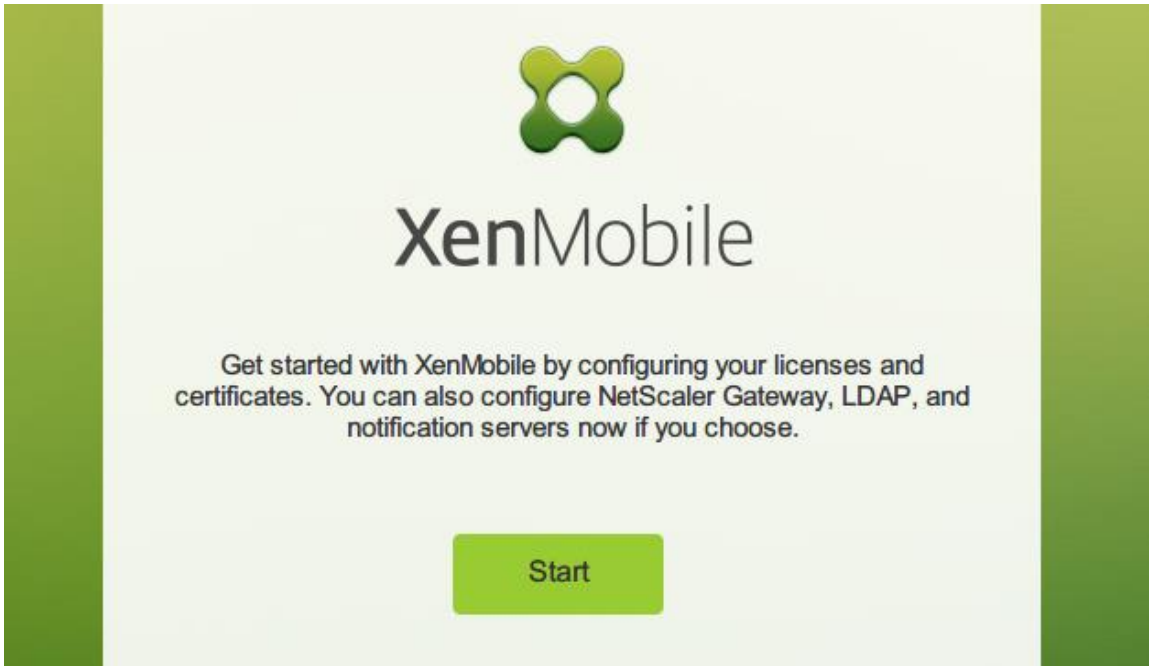
8.	输入 instance name，
	`Device management instance name. If you are upgrading from a previous release, t`
	`he name must match the previous configured name.`
	`  Instance name [zdm]: zdm`
	`  Commit settings (y/n) [y]: y`
	`The wizard will now generate an internal Public Key Infrastructure (PKI):`
	` - 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`

9.	输入一个特定的 password 来保存 PKI 证书的相关加密、认证信息。
	`  Do you want to use the same password for all the certificates of the PKI [y]:`
	`y`
	`  New password:`
	`  Re-enter new password:`
	`  Commit settings (y/n) [y]: y`
	`Generating SAML signing certificate...`
	`Generating server and client certificates...`

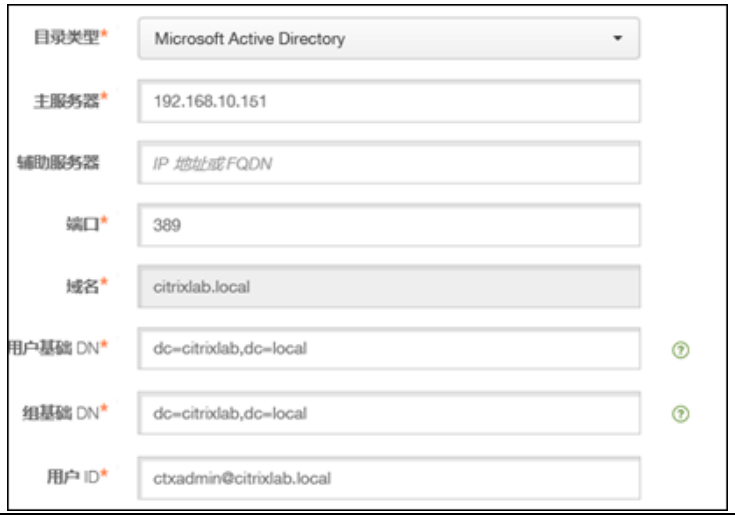
10.	输入初始管理员账号密码，默认账号为 administrator
	`  Username [administrator]: administrator`
	`  Password:`
	`  Re-enter new password:`
	`  Commit settings (y/n) [y]: y`
	`Creating console administrator...`
	`Applying firewall settings ...`
	`Writing iptables configuration...`
	`Restarting iptables...`
	`Initial system configuration complete!`

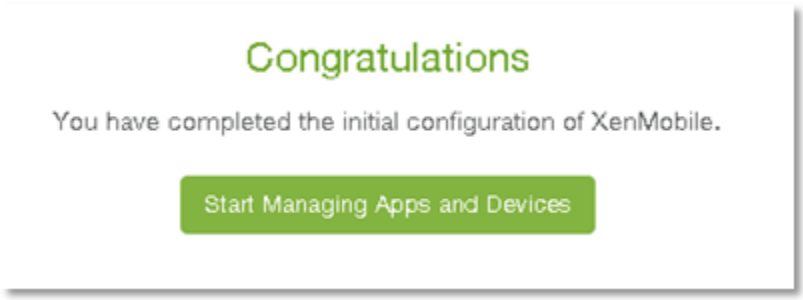
步骤	操作
11.	如果不是老版本升级，选择 n 
12.	完成选择后，点击确认，XenMobile 系统会自动完成初始化的安装过程，这个过程需要几分钟的时间。
13.	登录 AD/DNS 服务器，增加一个 host 记录 192.168.10.156; xms.citrixlab.com 

4.3 XenMobile 基本配置

步骤	操作
1.	打开浏览器访问 XenMobile 管理控制台，https://192.168.10.156:4443 
2.	输入前序中输入的管理员账号及密码，将开始进入初始化配置阶段。 本例中截图为英文，如使用中文系统或浏览器则显示中文，使用英文系统则显示英文。XenMobile 会自适应。 

步骤	操作
3.	在许可 配置界面，配置对应的许可服务器或者导入专用 lic。 
4.	XenMobile 安装默认会生成多个证书。在此需要手动导入苹果的 APNS 证书。 
5.	在证书页面点击导入， 选择：密钥库 密钥库类型：PKCS#12 用作：APNs 密钥文件以及密码。 

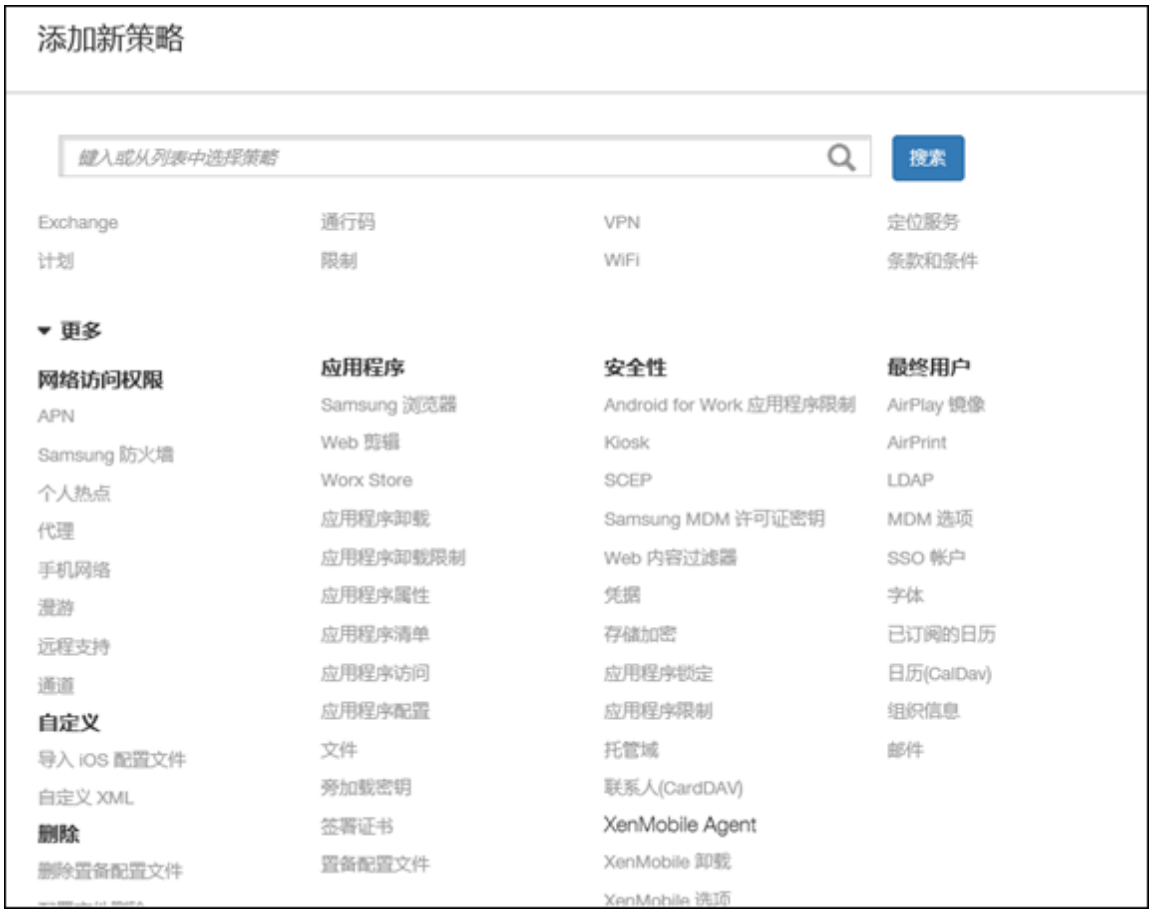
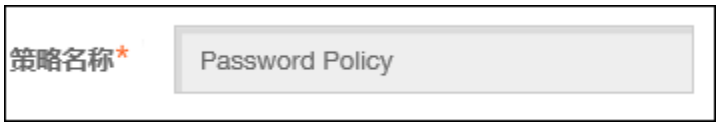
步骤	操作
6.	确保导入成功，APNs 证书已经生效 
7.	考虑到环境中相当部分使用的 Windows CA 版本，导入其 ROOT CA 证书文件，方便后续与 XD/XA 集成时，如果使用 SSL 认证，方便相互信息。
8.	配置 NetScaler Gateway 外部 URL：https://mam.citrixlab.com 登录类型：仅限域 密码为必填项：开 
9.	添加 LDAP 目录类型： Microsoft Active Directory 主服务：192.168.10.151 端口：389 域名：citrixlab.local 用户基础 DN：dc=citrixlab,dc=local 组基础 DN：dc=citrixlab,dc=local 用户 ID：ctxadmin@citrixlab.local 

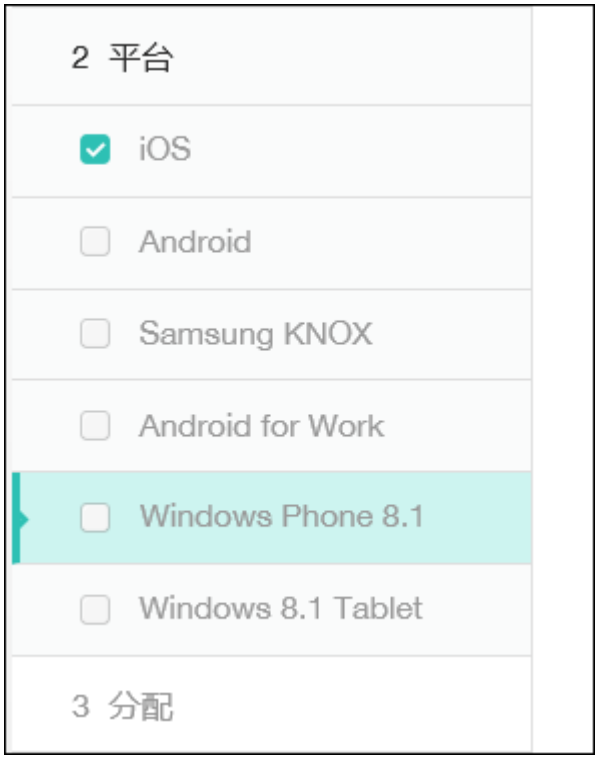
步骤	操作
10.	继续前序信息 用户名对应密码： 域别名：citrixlab.local 用户搜索依据：sAMAccountName 注：在只有单域的环境中，建议使用 sAMAccoutName，这样用户登录时可以选用短命名格式输入自己的账号。如果是林内多域，请使用 userPrincialName，则用户登录时需要输入自己 ID 的完整 FQDN。 
11.	至此，XenMobile 的基本配置就完成了。 

第5章 XenMobile 常规设定

由于 XenMobile 涵盖了太多的各型策略，所以本文档只能抛砖引玉介绍几个，更为详细的内容请查阅官网或自行研究。

5.1 设定 Pin code 策略

步骤	操作
1.	在任何 Mobile 项目中，移动设备接入系统都会要求设定一个 pin code 作为基本的认证要求，用来替代用户账号密码。所以第一个策略就是设定 Pin code。
2.	访问 XenMobile 配置 -> 设备策略，选择添加，选择通行码 
3.	输入策略名称，名称建议使用英文。 

步骤	操作
4.	左侧跳出支持的平台版本，本例中只配置了 iOS 版本，其他版本请根据向导自行调整。 
5.	需要通行码，点击 打开 对于更项策略，请自行调整， 如：最小长度， 是否需要包含字符， 有效期限等 

步骤	操作
6.	选择所有用户，并点击保存

5.2 阻止相机

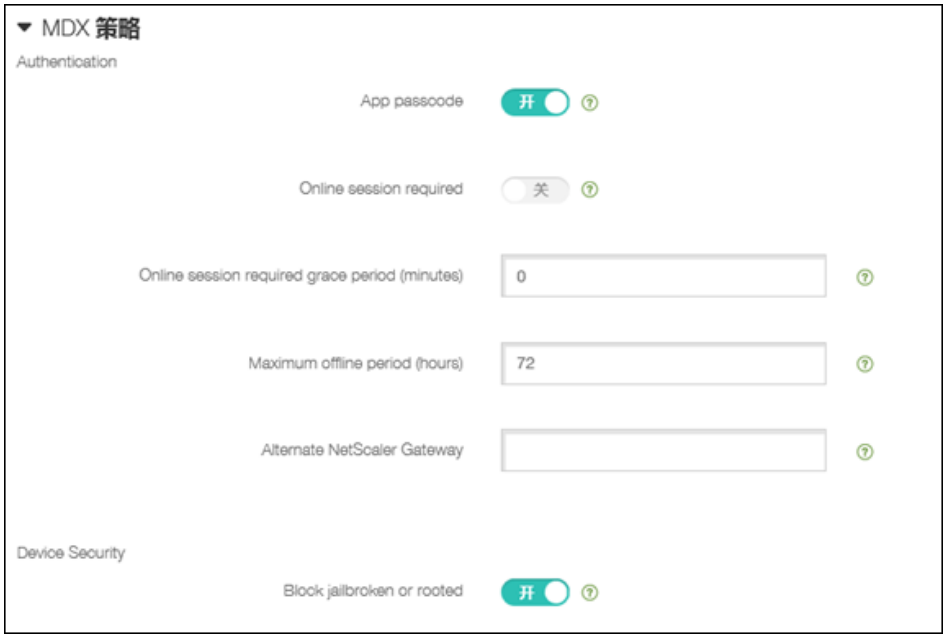
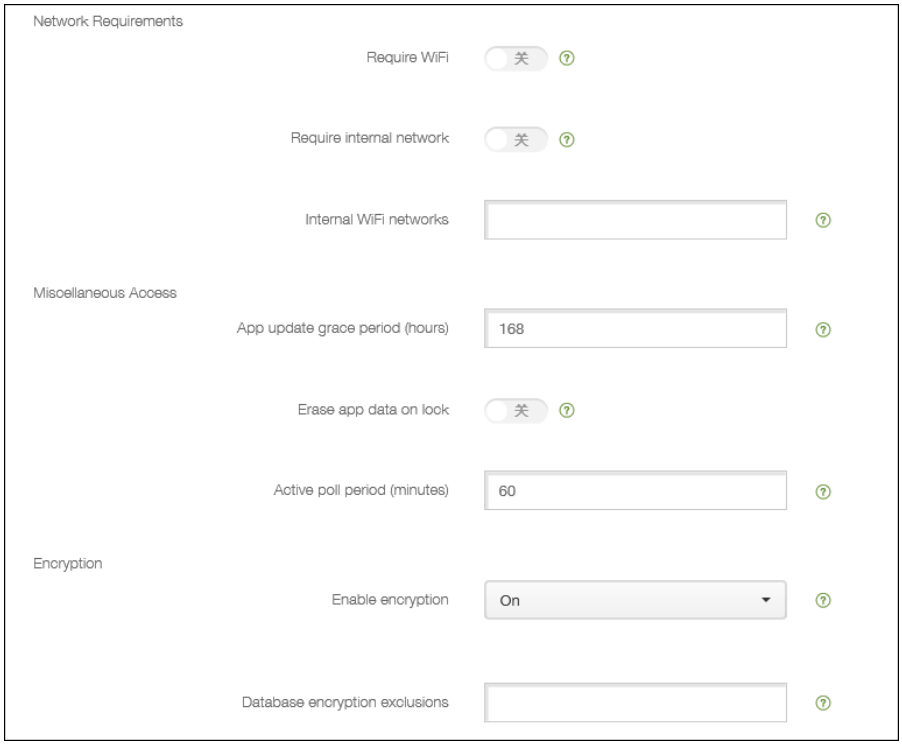
步骤	操作
1.	在 MDM 项目，各种限制、阻止策略是经常会遇到的。在此以设定阻止相机为例子。
2.	添加策略，选择限制

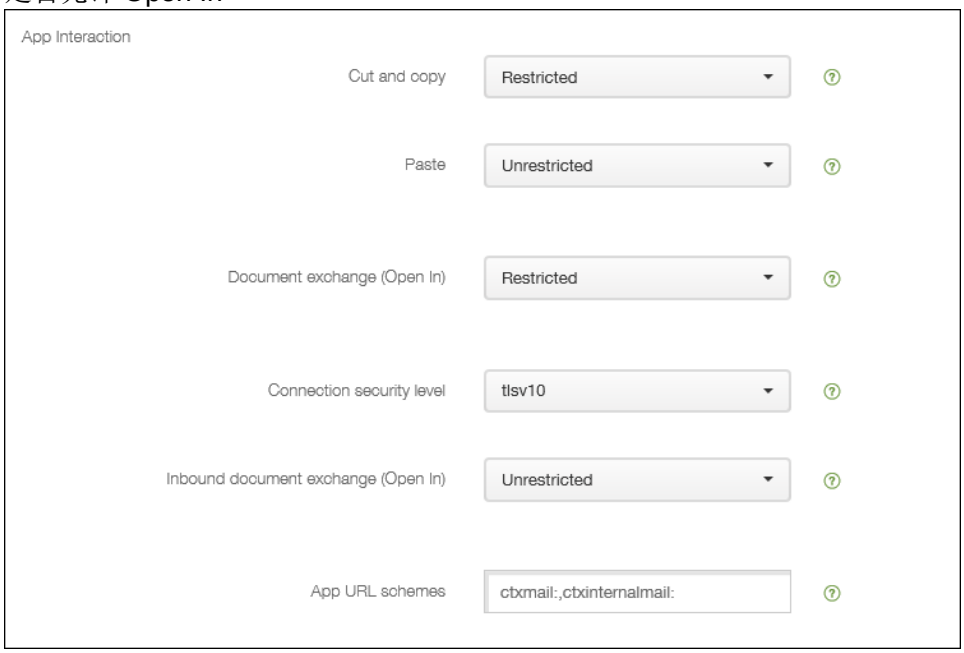
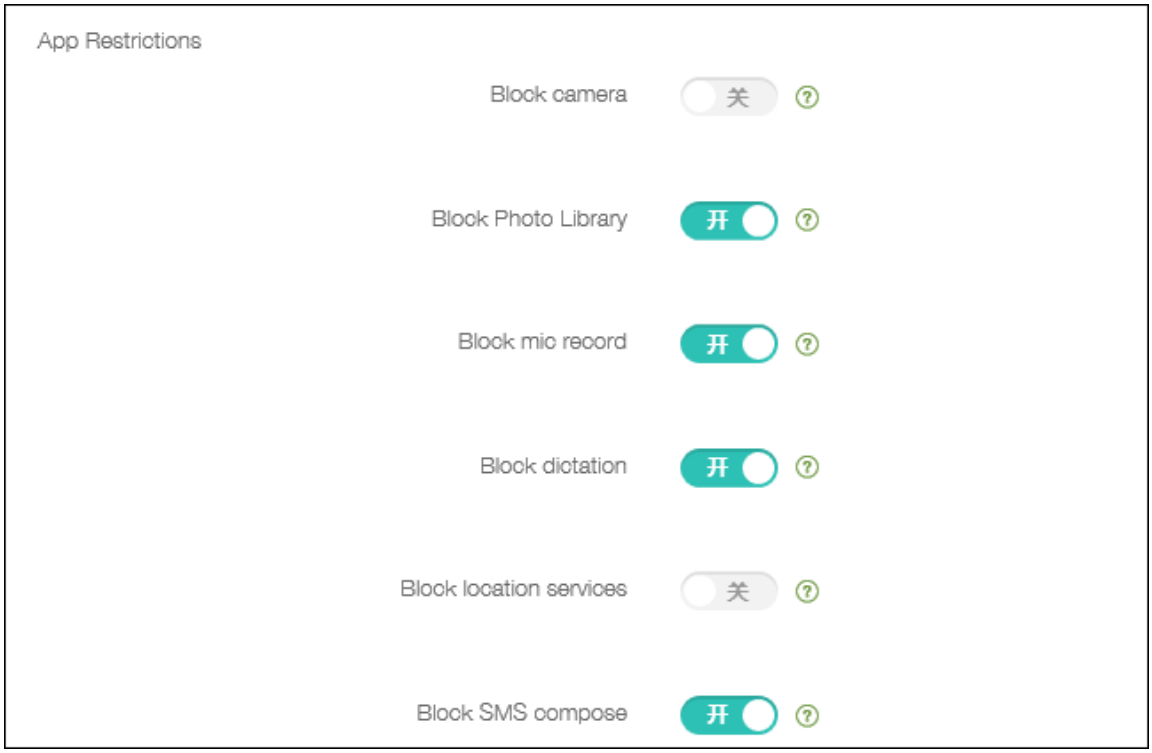
步骤	操作
3.	关闭相机和屏幕截图 
4.	策略太多，其他策略请根据情况自行决定 
5.	点击下一步，并分发给所有的用户。

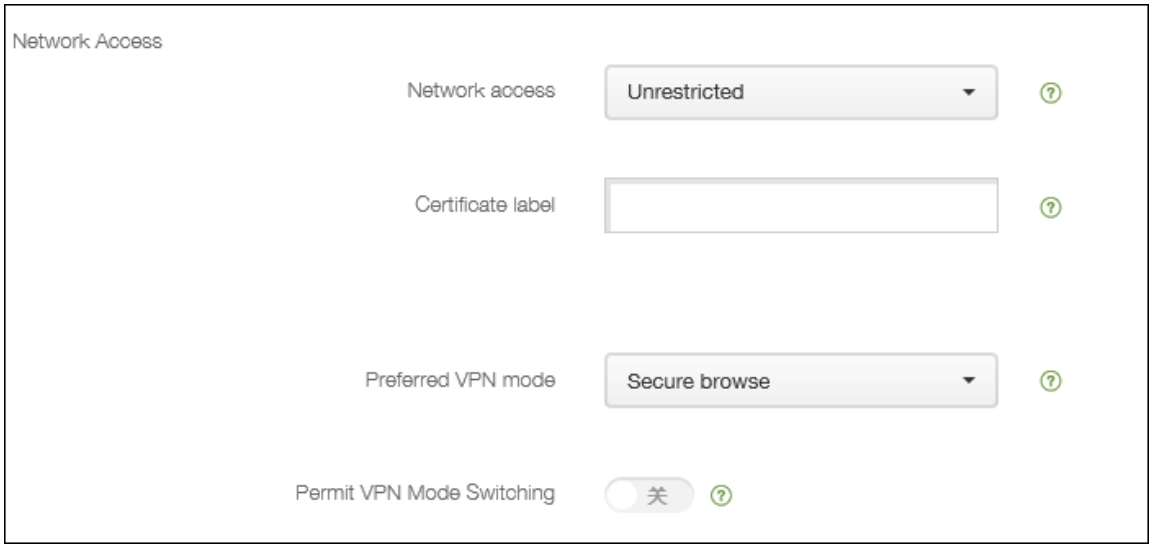
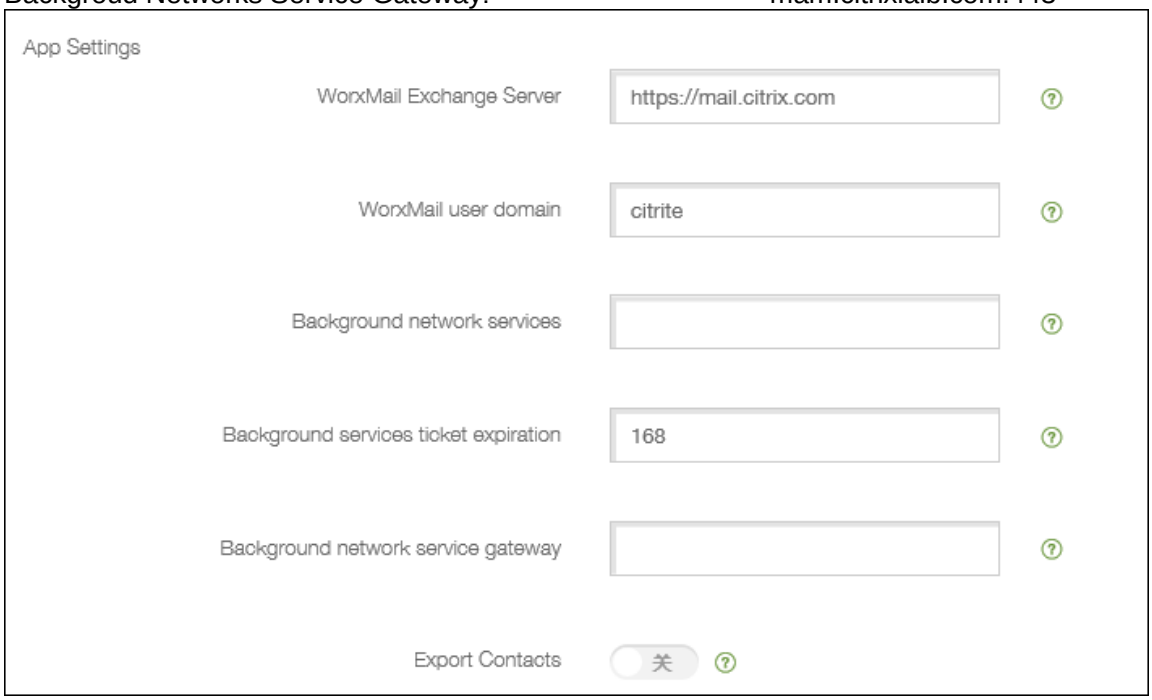
思杰 | CITRIX®

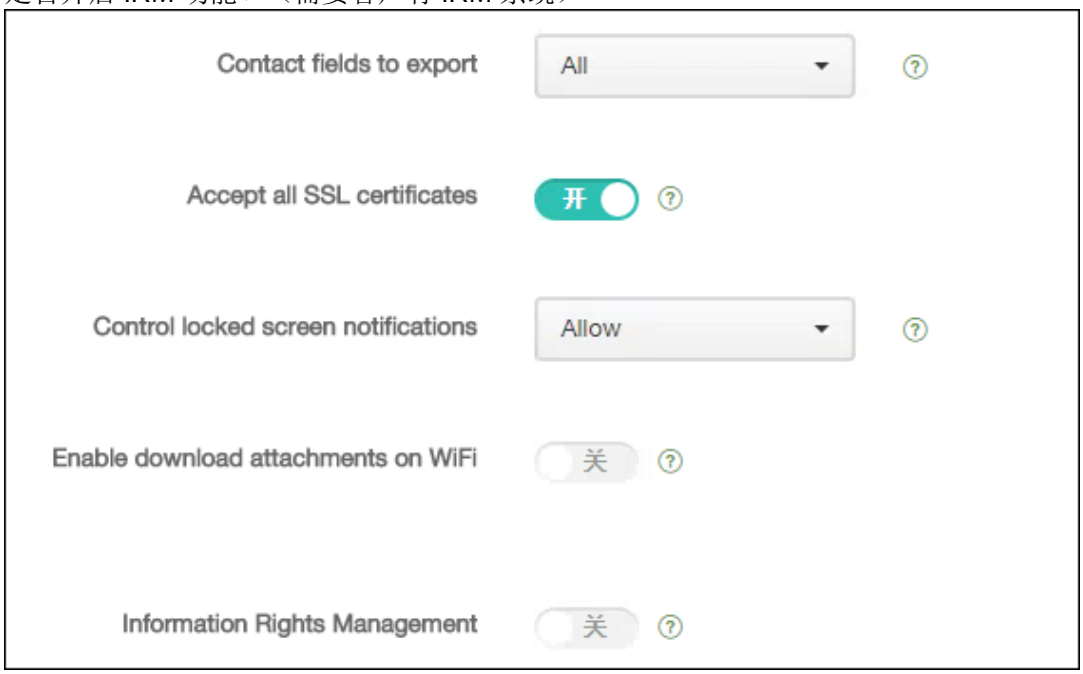
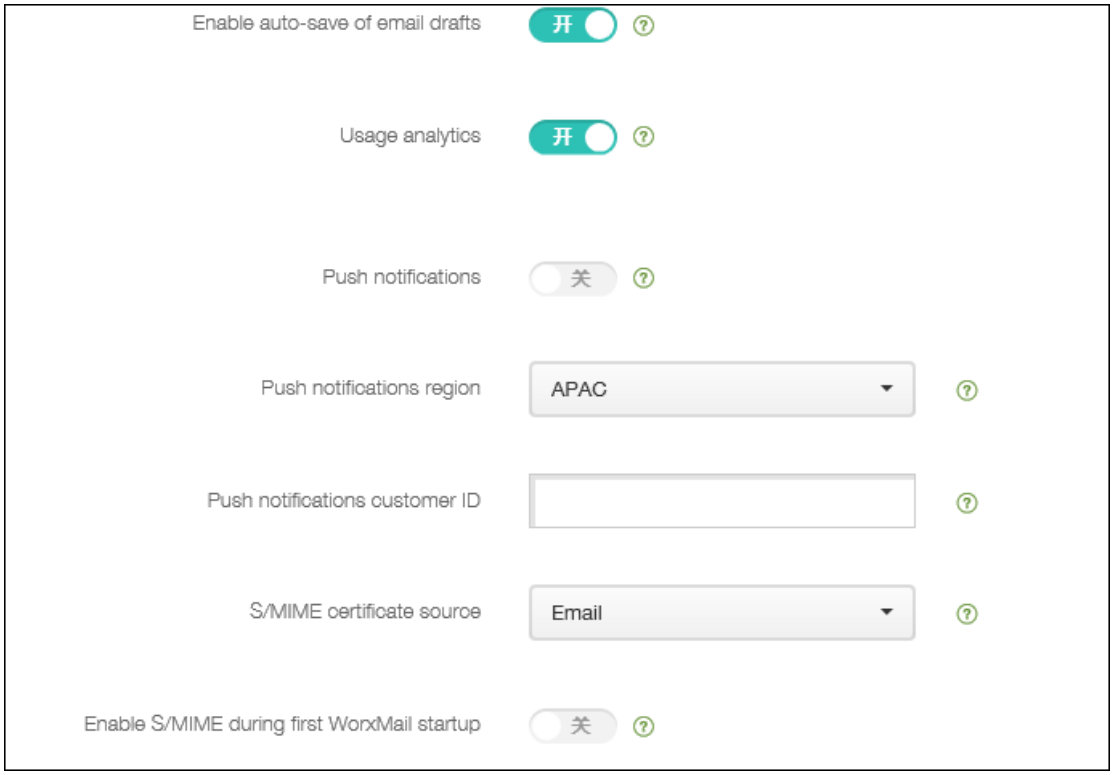
5.3 交付 WorxMail

步骤	操作
1.	相比其他的 EMM 厂商，Citrix 的 MAM 优势极为明显，尤其在安全沙箱技术方面，Citrix 目前可以说是独步天下。本例中使用 WorxMail 企业级安全沙箱邮件客户端作为样板，展示 XenMobile 丰富的的安全策略。 本例中 WorxMail 除了与 Exchange 相关的策略之外，其他所有策略普通应用在完成封装滞后也可以实现。
2.	点击配置 -> 应用程序，点击添加，输入名称 WorxMail， 
3.	上载对应 WorxMail MDX 文件，相关基础信息自行显示。 如最低 iOS 版本要求，MDM 是否允许删除等。 

步骤	操作
4.	丰富的 MDX 策略： App passcode，登录时是否需要 Pin 码解锁 Online session required：是否必须联网 Block jailbroken or rooted：是否允许越狱或 rooted 的设备 Session 时间等 
5.	丰富的 MDX 策略： 是否需要访问特定 WIFI App 更新检测间隔时间 是否对数据加密 

步骤	操作
6.	丰富的 MDX 策略： 是否允许剪切、复制 是否允许粘贴 是否允许 Open In 
7.	丰富的 MDX 策略： 是否允许访问摄像头、相片库等 

步骤	操作
8.	丰富的 MDX 策略 是否限制特定网络才能接入，VPN 通道类型 
9.	丰富的 MDX 策略： 配置 Exchange Server，限制应用只能访问指定的 Exchange 服务器地址。(本例中由于没有自建邮件服务器，所以访问的是公网地址，如果是客户自有环境，建议指向客户 Exchange 的 CAS 服务器地址) 短域名 Backgroud network Servie、Backgroud Networks Service Gateway。 配置 iOS 时，这两个配置可以为空。 配置 Andorid 版本时， Backgroud network Servie：mail.citrix.com:443 Backgroud Networks Service Gateway:mam.citrixialb.com:443 

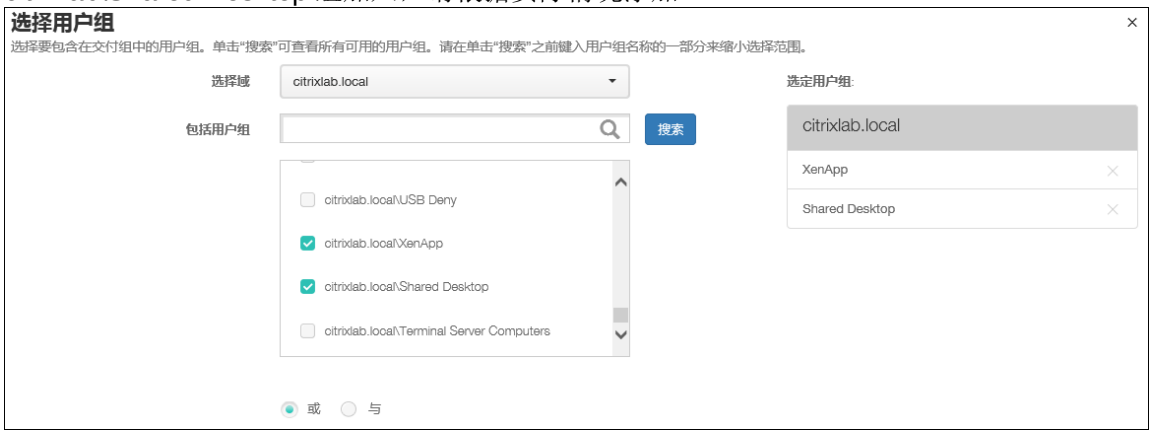
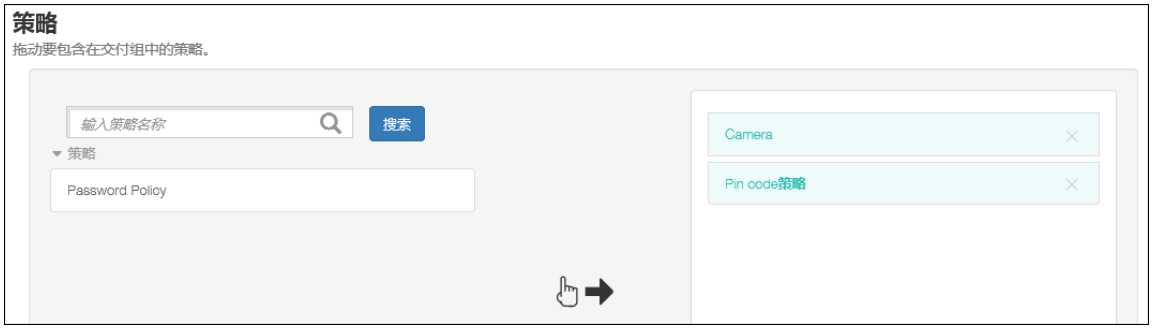
步骤	操作
10.	是否允许导出通讯录 是否接受所有的 SSL 证书？ 是否允许调整屏幕提醒？ 是否允许在 WIFI 下下载附件？ 是否开启 IRM 功能？（需要客户有 IRM 系统） 
11.	丰富的 MDX 策略： 信息推送策略、自动保存邮件草稿 

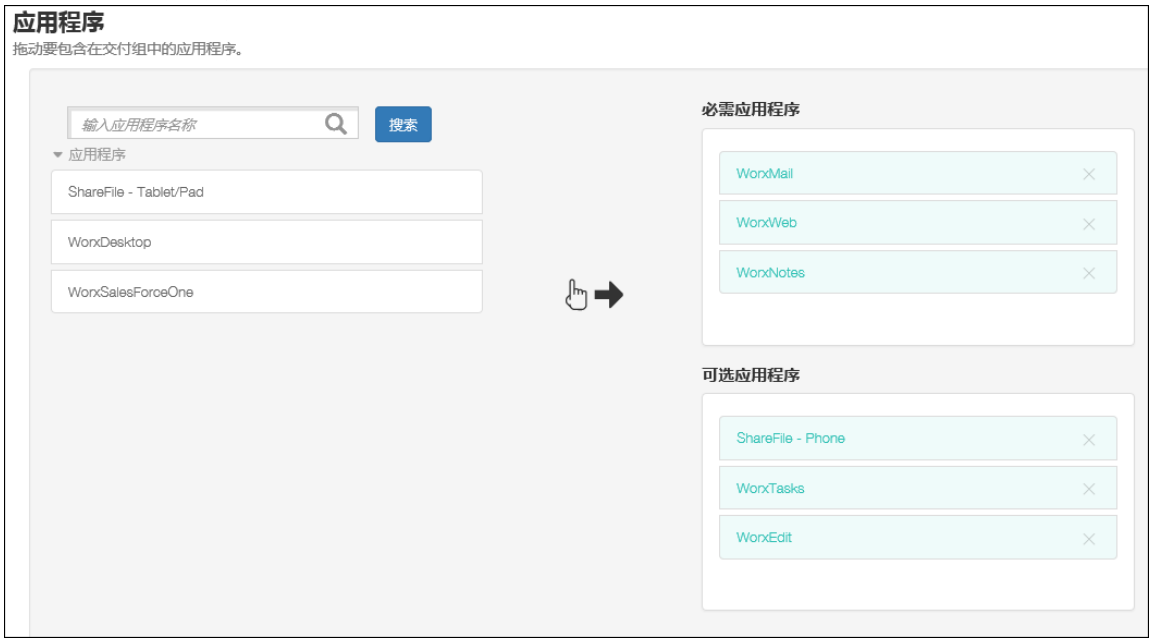
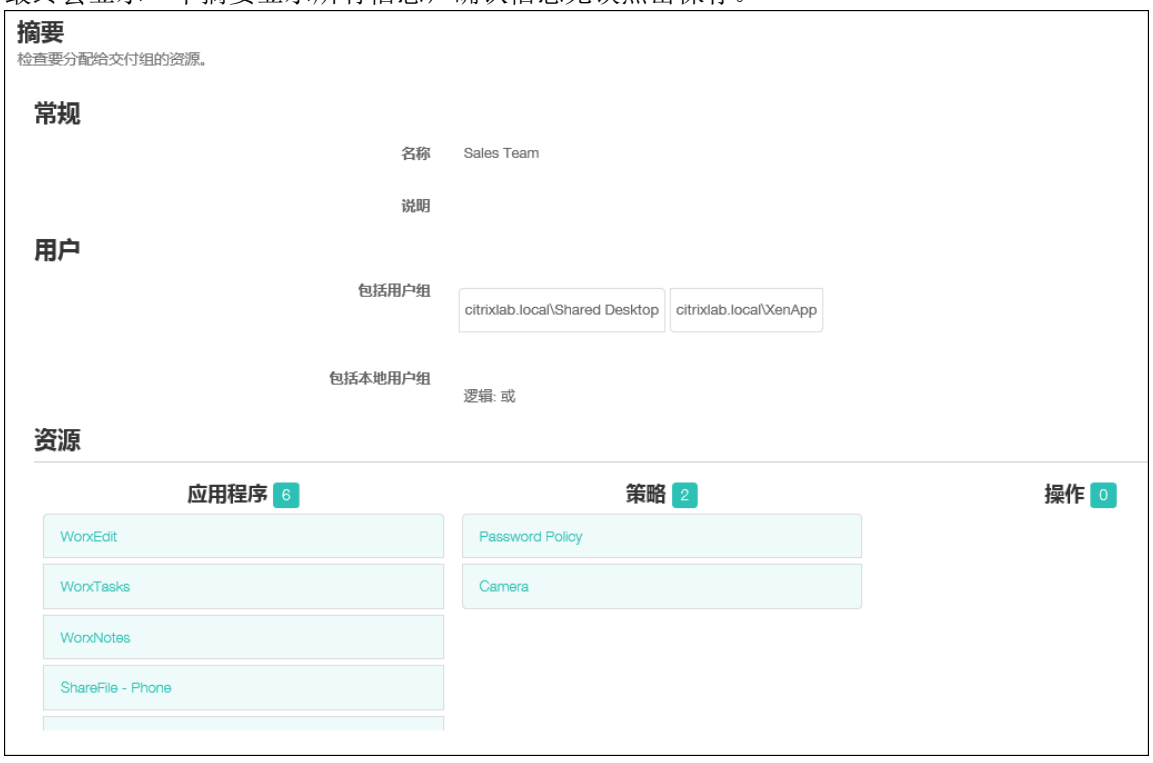
步骤	操作
12.	创建审批流程（可选），本例中选择无， 
13.	分配用户，完成应用交付。

思杰 | CITRIX

5.4 创建 XenMobile 交付组

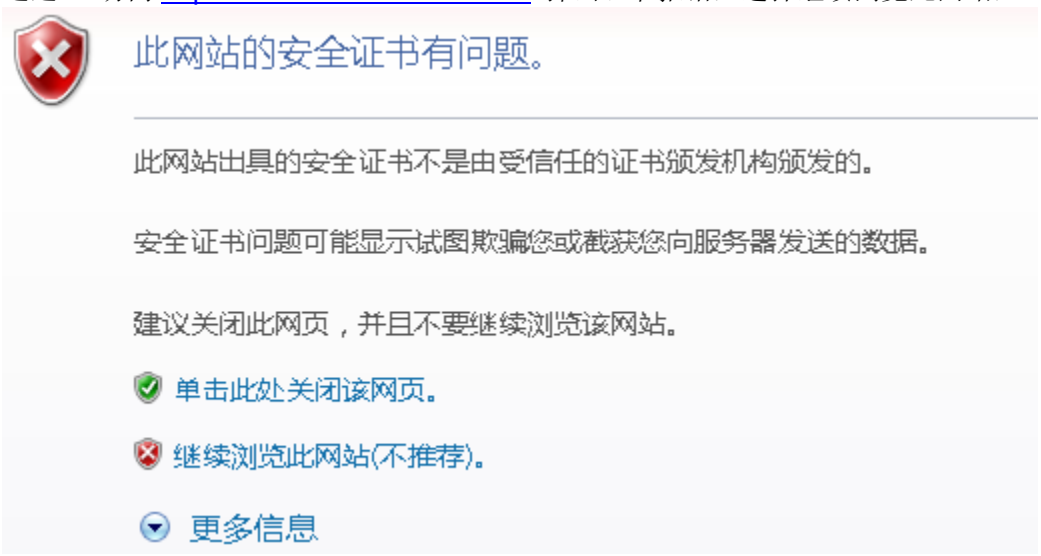
XenMobile 是一个独立的应用系统，有其独立用户交付管理体系，本章节介绍相关内容

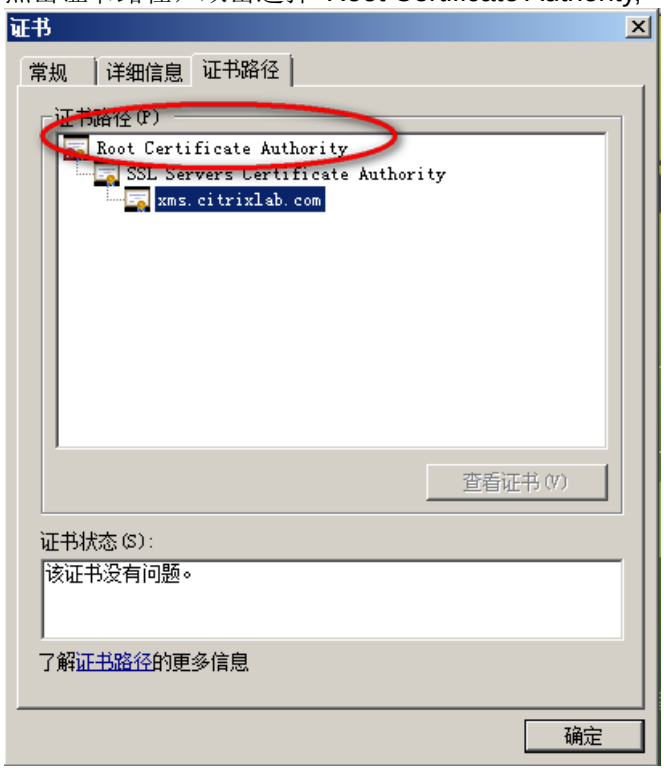
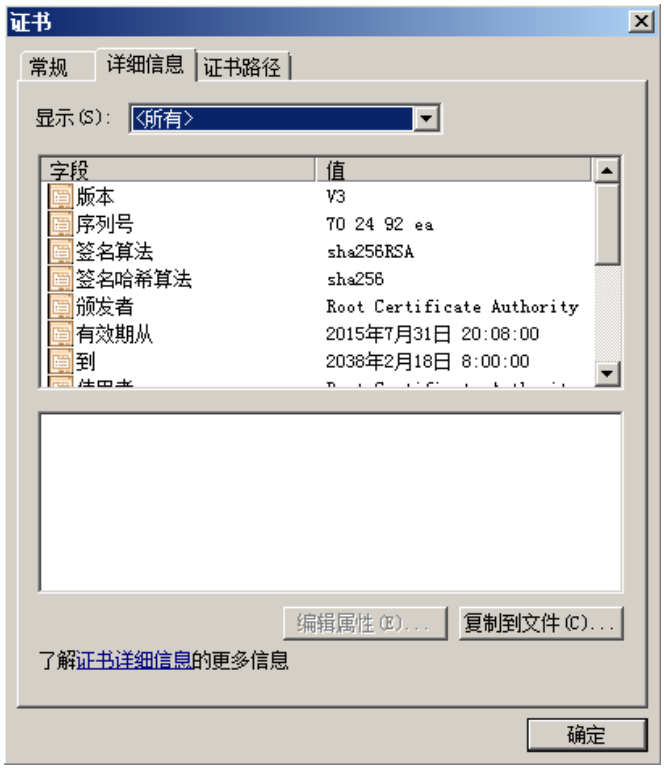
步骤	操作
1.	访问 https://xms.citrixlab.com:4443 管理控制台，展开配置 - > 交付组，选择添加并输入名称， 
2.	在域下，选择 搜索，找寻需要的用户组，本例中为做特别规划，将 citrixlab\XenApp, citrixlab\Shared Desktop 组加入，请根据实际情况添加。 
3.	选择可用的策略，本例中将前序的摄像头和 pin code 策略选择。 注：操作方式选中策略，拖拽至右侧即可。 

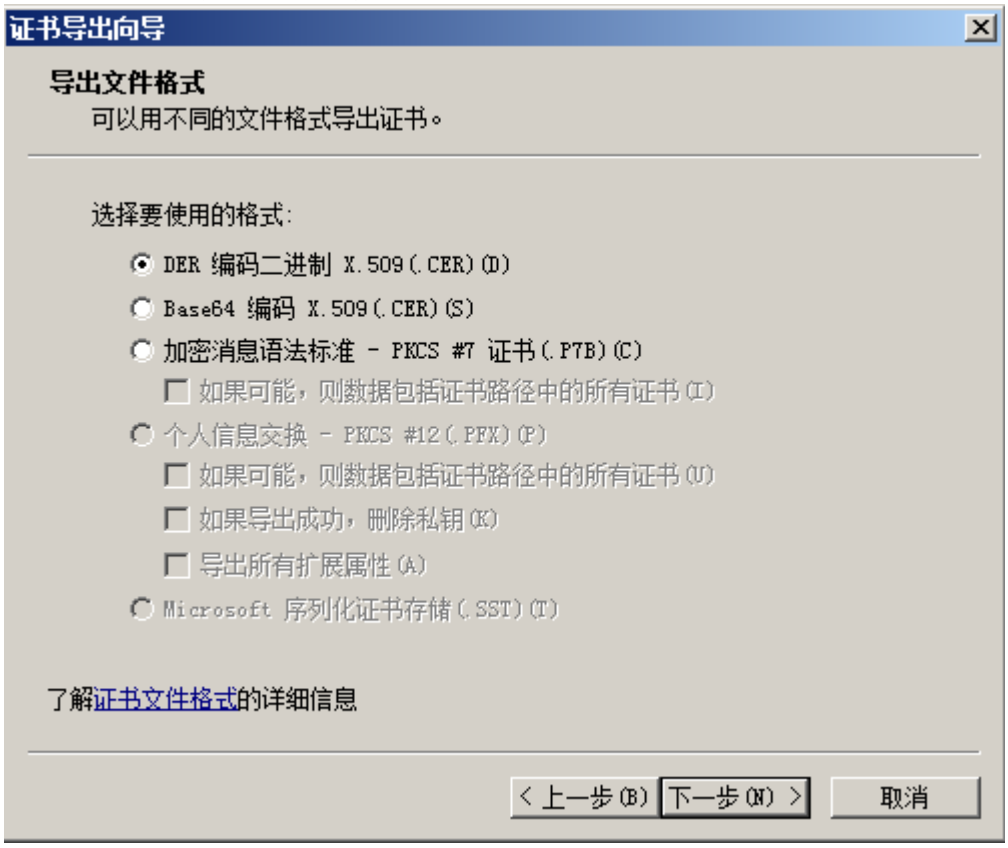
步骤	操作
4.	应用程序： 必需应用程序：代表设备通过 MDM 注册后，就会直接推送安装。 可选应用程序：代表应用程序需要用户在应用商店中手动安装。 
5.	最终会显示一个摘要显示所有信息，确认信息无误点击保存。 

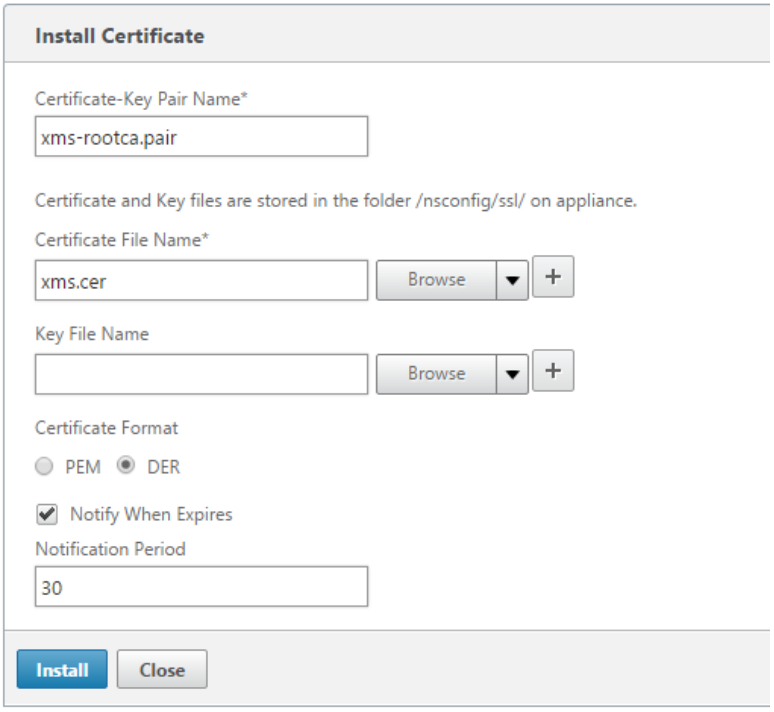
第6章 配置 NetScaler、StoreFront 以完成 XenMobile 集成

6.1 将 XenMobile 服务器上证书导入至 NetScaler（可选）

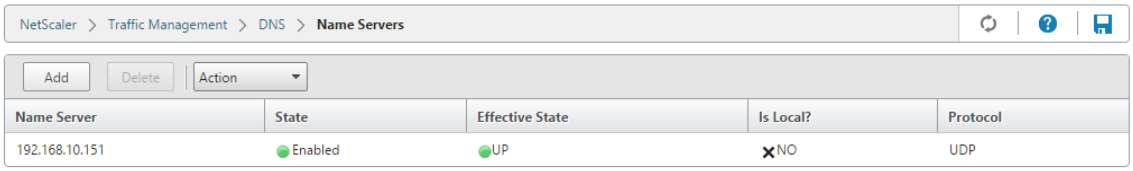
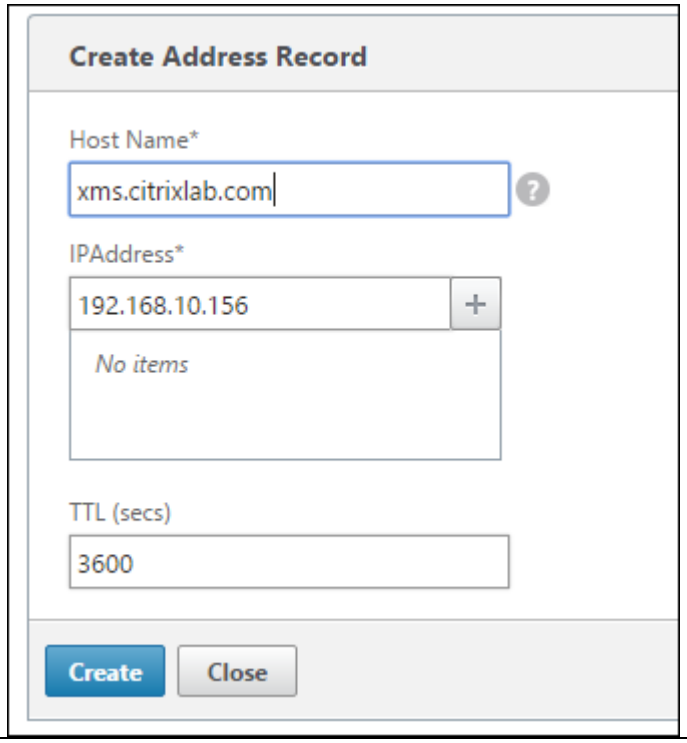
步骤	操作
6.	由于 XenMobile 安装时会自签一张证书，所以为了保证 NetSclaer 与 XenMobile 通信是信任保证，建议将 XenMobile 自签根证书导入至 NetScaler 上。同时也建议导入只进行 XenMobile 管理的终端 PC 上。 如果 XenMobile 有单独申请公网证书，则无需执行操作。
7.	通过 IE 访问 https://xms.citrixlab.com:4443 弹出证书报错，选择继续浏览此网站， 
8.	在 IE 右上角有证书错误，点击 选择查看证书 

步骤	操作
9.	点击证书路径，双击选择 Root Certificate Authority, 
10.	在弹出页面选择详细信息， 

步骤	操作
11.	选择 复制到文件，点击下一步 
12.	将文件保存为 cer 文件，如 xms.cer
13.	访问 NetScaler，选择 Traffic Management -> SSL -> Certificates

步骤	操作
14.	点击 Install，输入如下信息： Certificate-key pair name: xms-rootca.pair 导入前序保存的 xms.cer 文件 选择 DER 格式 
15.	回到 Certificates，确认导入成功。 

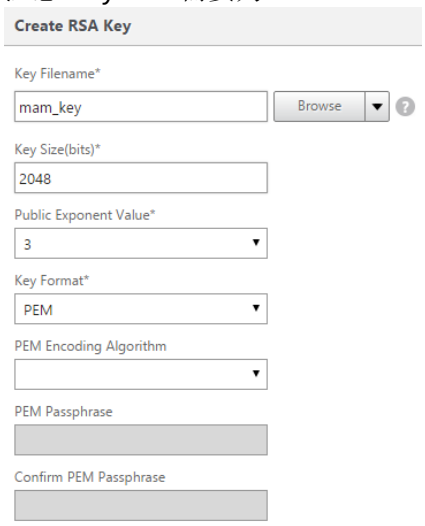
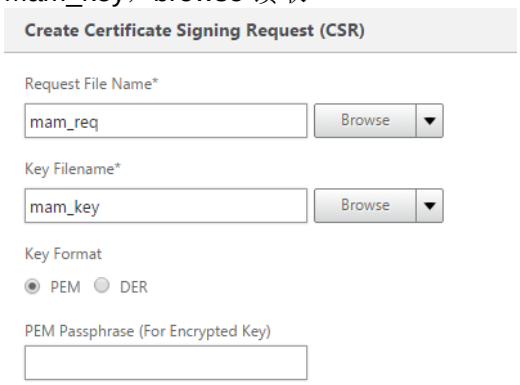
6.2 创建 xms host 记录(可选)

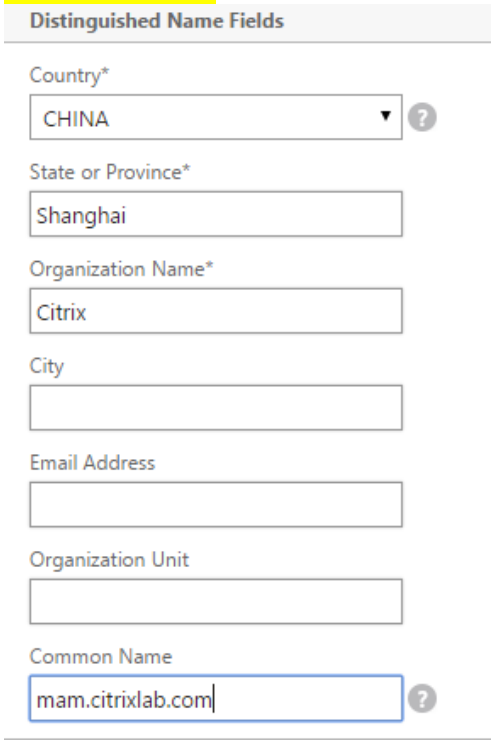
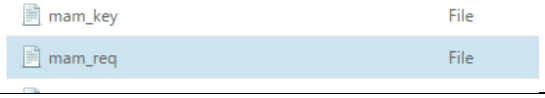
步骤	操作
1.	访问 NetScaler，展开 Traffic Management -> DNS，点击 Name Servers，确保 192.168.10.151 记录存在并工作正常。 
2.	展开 DNS – Address Records，添加一个记录 xms.citrixlab.com 192.168.10.156 

6.3 配置 NetScaler

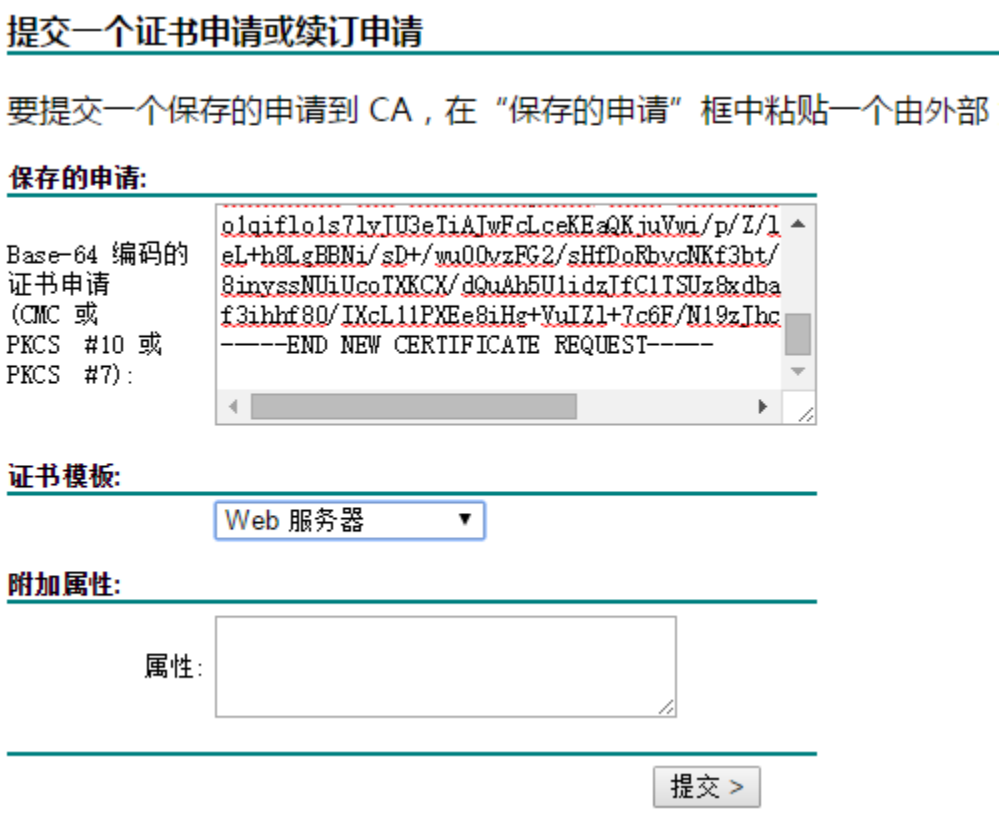
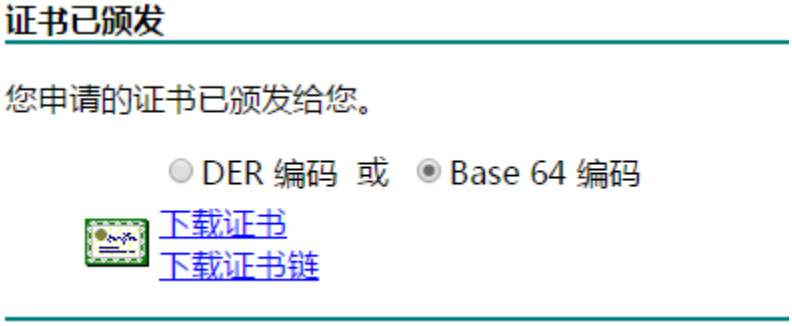
对于 XenMobile10 及其以后的版本来说，其 MDM 和 MAM 对于 NetScaler 需求是各不相同的。如果是纯 MDM 环境，是只需要拥有负载均衡能力的设备来支持即可，所以在此种场景中 MDM 是可选的，使用其他品牌的负载均衡设备是可以的。但是用户如果需要 MAM 即需要建立 micro-vpn，则此时必须使用 NetScaler 来完成相关功能。

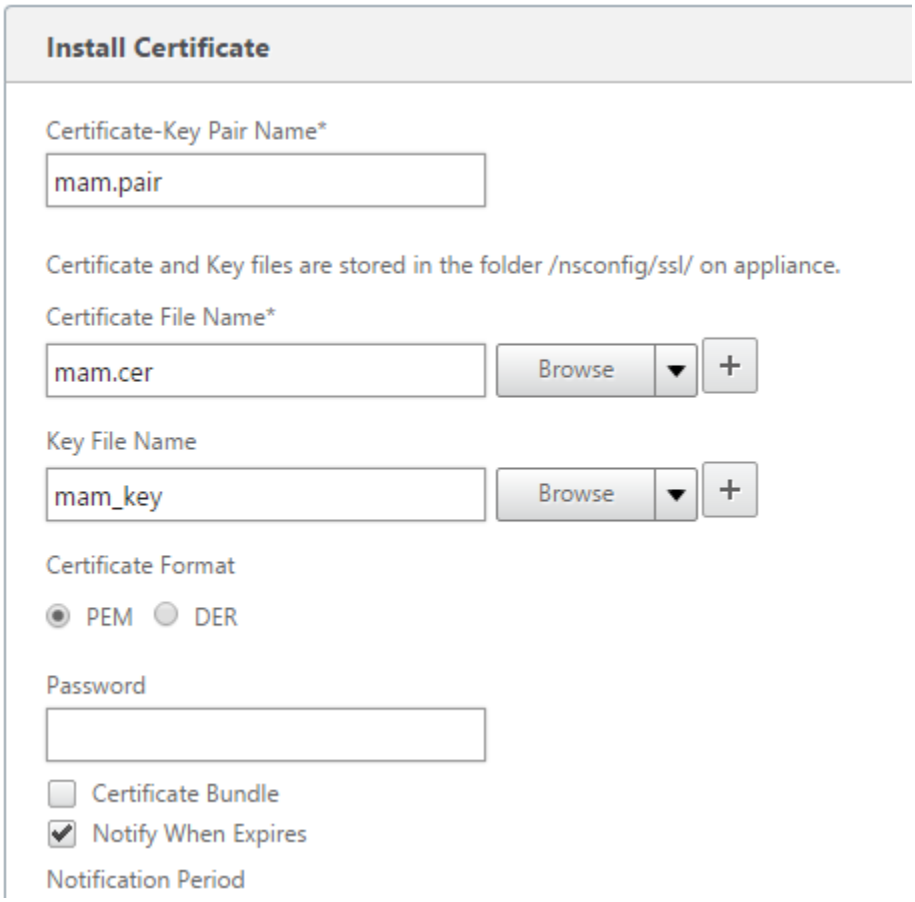
所以本例中，主要是完成 MAM 的 NetScaler 集成交付。

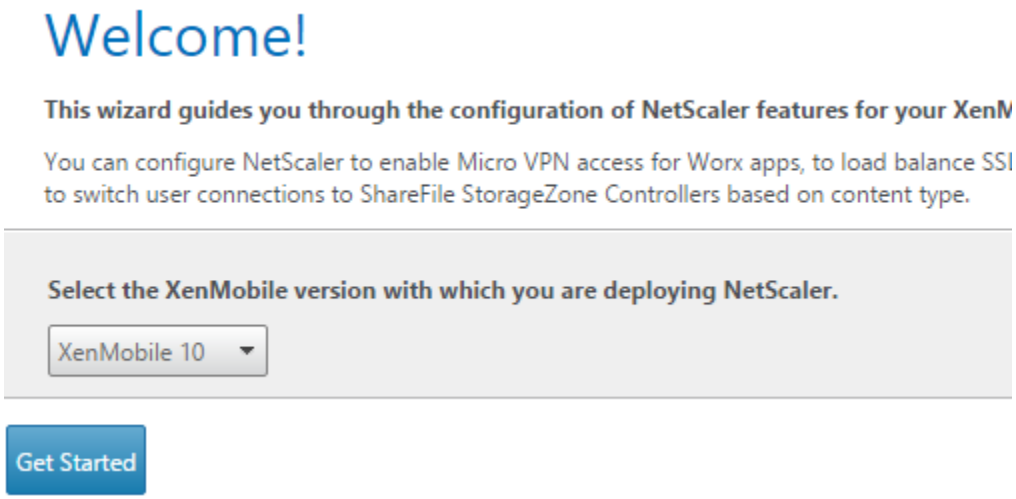
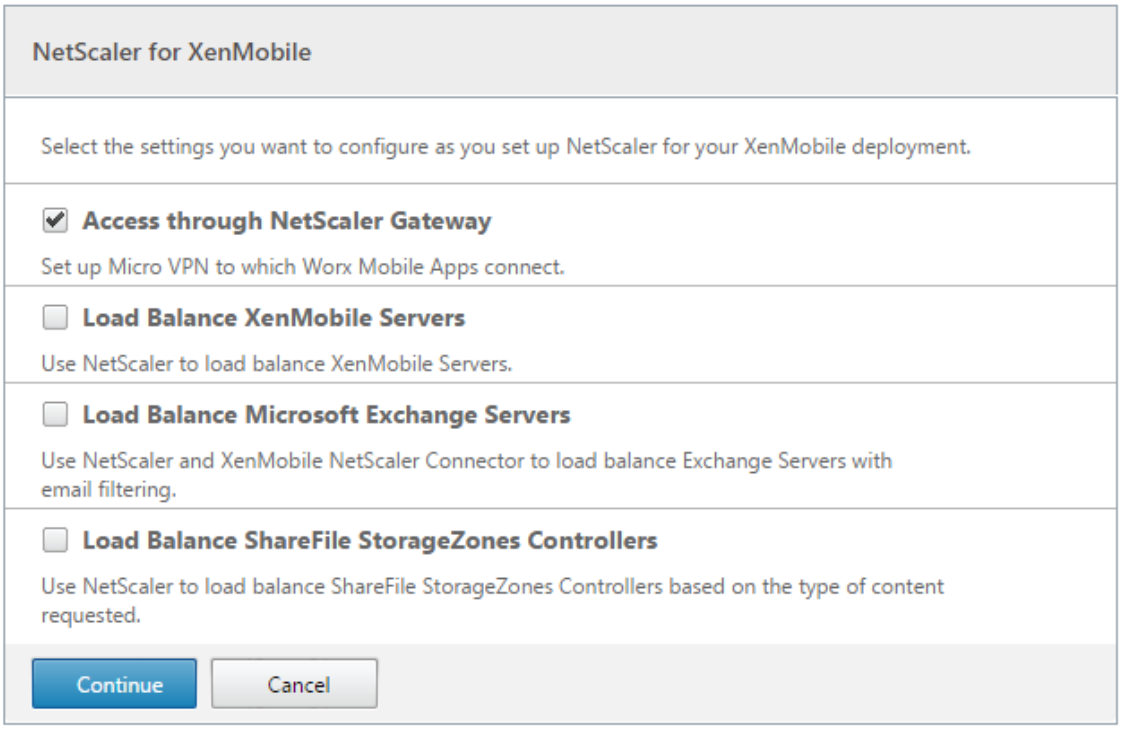
步骤	操作
3.	NetScaler 与 XenMobile 集成和 XenDesktop、XenApp 一样，先得准备一个证书。
4.	在 Traffic Management –> SSL，选择 Create RSA key， 注意 Key size 需要为 2048 
5.	选择 Create Certificate Signing Request (CSR) ，输入相关信息， Mam_req 输入 Mam_key，browse 读取 

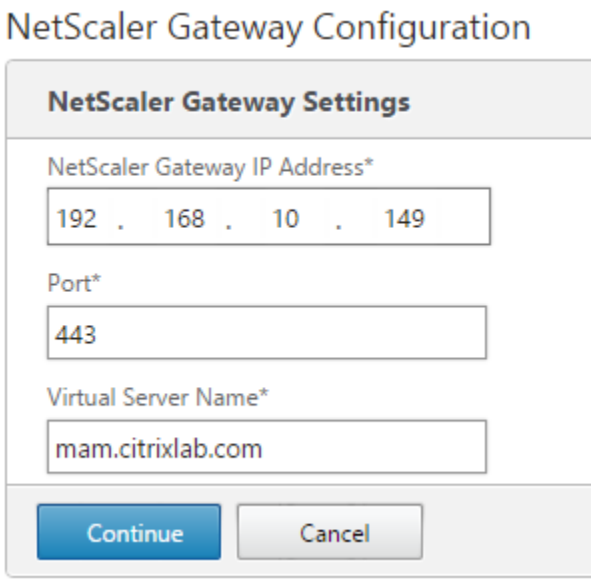
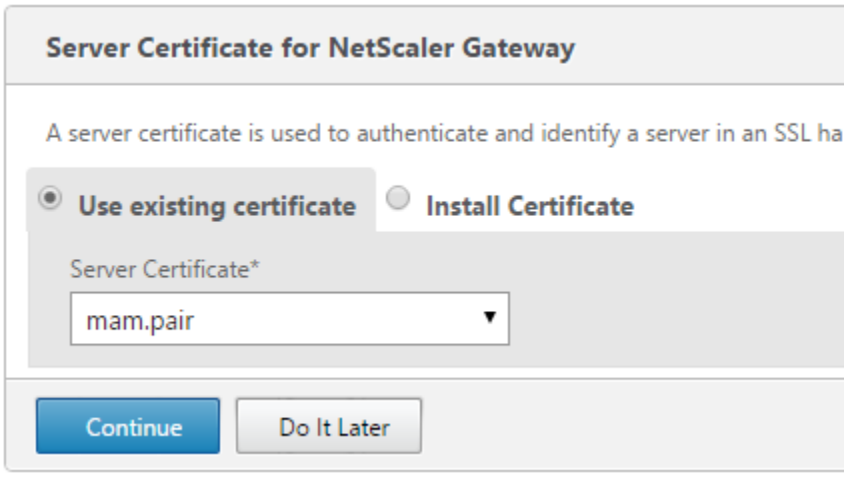
步骤	操作
6.	选择基本信息，关键是 common name，需要具体发布到公网的域名，本例中为：mam.citrixlab.com 
7.	在 Manage Certificates 中，选择 mam_req 文件并 download， 

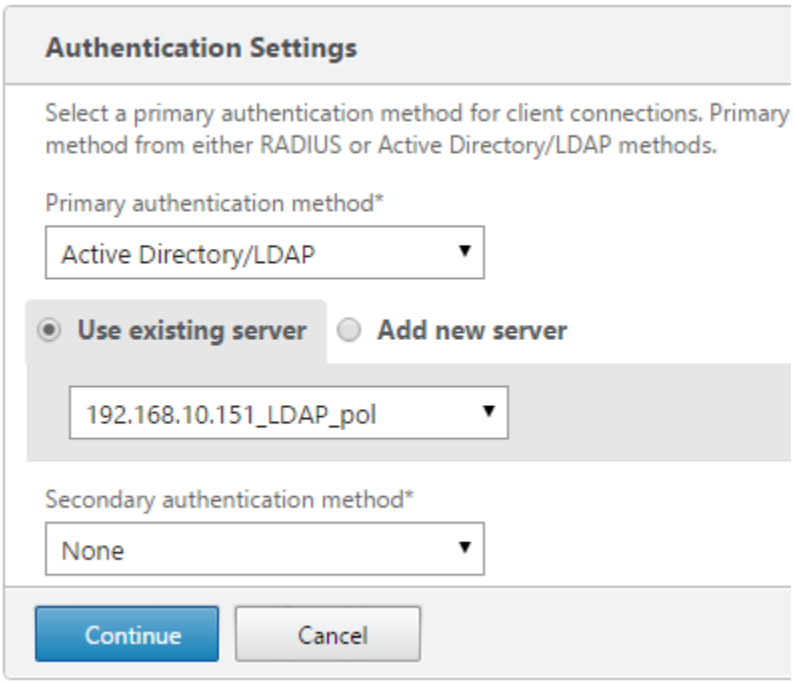
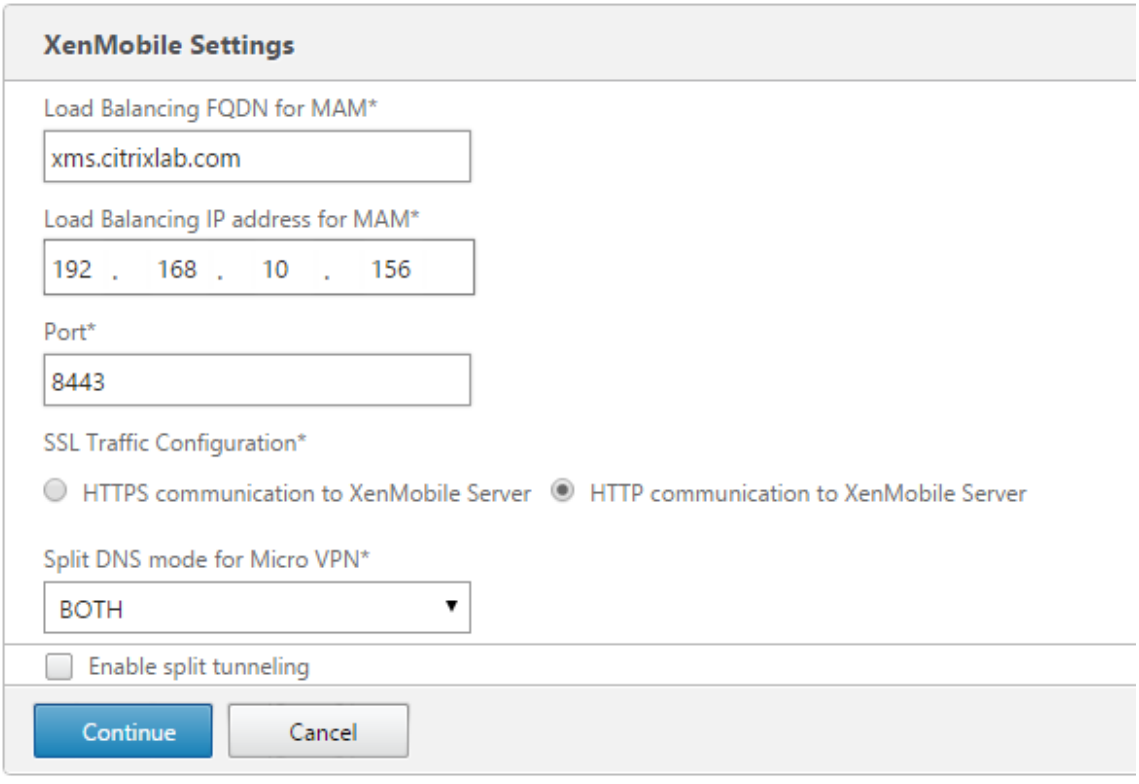
步骤	操作
8.	通过文本编辑其打开此文件， View File -----BEGIN NEW CERTIFICATE REQUEST----- MIICkzCCAXsCAQAwTjELMAkGA1UEBhMCQ04xETAPBgNVBAgTCFNoYW5naGFpMQ8w DQYDVQQKEwZDaXRyaXgxGzAZBgNVBAMTEm51eHQuY210cml4bGFiLmNvbTCCASIw DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALdm99ohPSVV/hzAA1EyAvW83yYF 8Wi7CNyVGOPkk9uNJX9jfqrMechBkGcEgtahyKwgI61JUAwh90e03kEB3CaweEq6 hmtAwOAgh2g96GCzPkr6SK5K3EBkIxqD4wiaUNSw/wWVy++Nav7vqeEJR4VZKQoe L4373Qk6C1OH6IZYMX3oqjvYyTUOWESOw9kXIAYkAdoKOmwdRjGtoiJq1ExQ64Kp F++G1p/9qwXQVQGRwm7UGOVa/cxmI5sDtzBe/K0vYjnZaDftI3Jqb/f+1ZP7IfXP 4jWddwxcLtRbRECQAecNtUKWxWAEM/kSt4DvAIimJRzASbl2AeQVF7ffHiECAwEA AaAAMAOGCSqGSIb3DQEBBQUAA4IBAQAyEBeJcrgAZvnQGXWUf491qQiTYkgIkZ78 2wp7LVbif2PTApNMUSp/pu/AlJS6ZRNhO2UdwcgpL1tF/VvRHHENsUeEuGro/6o7 PDm7QN7XLFqXeWn5uPphGn5LjZLZZpt3ouoRDbEj3KKQB2meWuBPqdW2LxSkKAaW JTEONREC1132O12F+uqPzFtk4JbojrAAK/oZQZoglCvuqczBgyolEgefmWjhOdoB 4cKKARzRjrzkf5qQdlUBqhNW2mBci3cgunkT1+OzK3vyA4g47TJZq9IVw6D3QaI8 /lULsnEa59RQzjKyrzHG7DfawBjhbEGY+gFPZ5V87GjWQSwYGmUx -----END NEW CERTIFICATE REQUEST-----
9.	访问 Windows CA, http://192.168.10.151/certsrv ， 申请证书，选择高级证书 Microsoft Active Directory 证书服务 -- citrixlab-CTXAD-CA 申请一个证书 选择一个证书类型: 用户证书 或者，提交一个 高级证书申请。

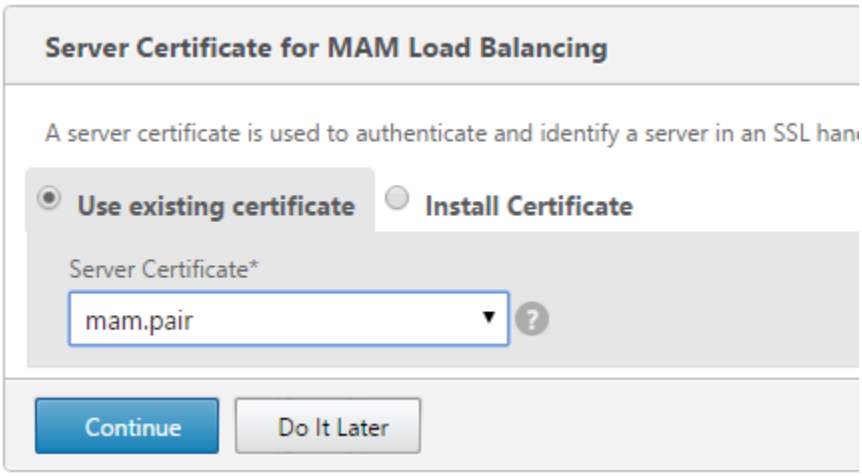
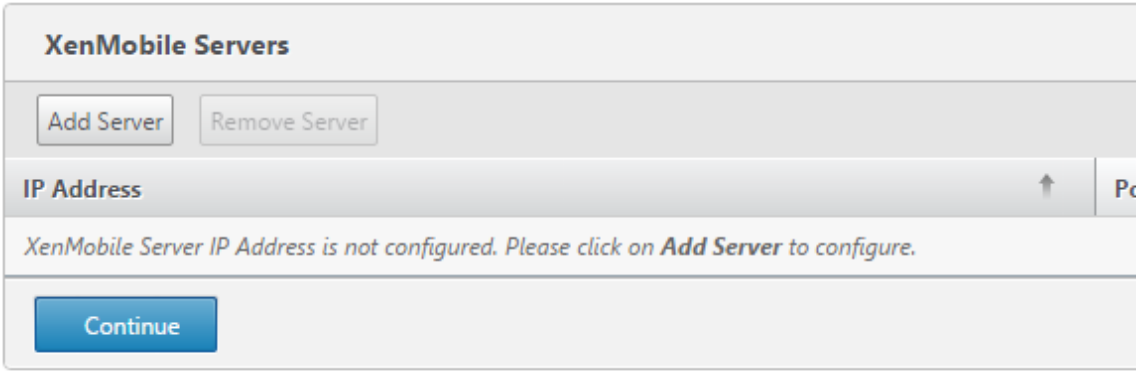
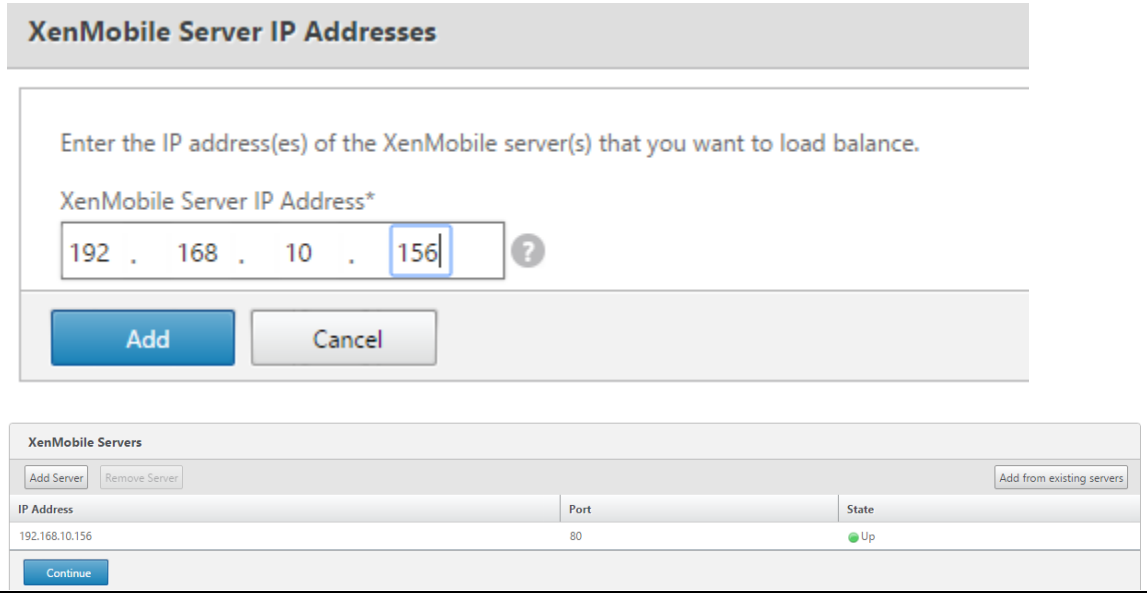
步骤	操作
10.	选择 Web 证书类型，并粘贴前序复制的证书 Request 信息，点击提交 
11.	由于前序我们选择的 PEM 加密格式，此处需选择 Base 64 编码，并下载证书。 
12.	回到 NetScaler 的 manage Certificate，导入此证书。 

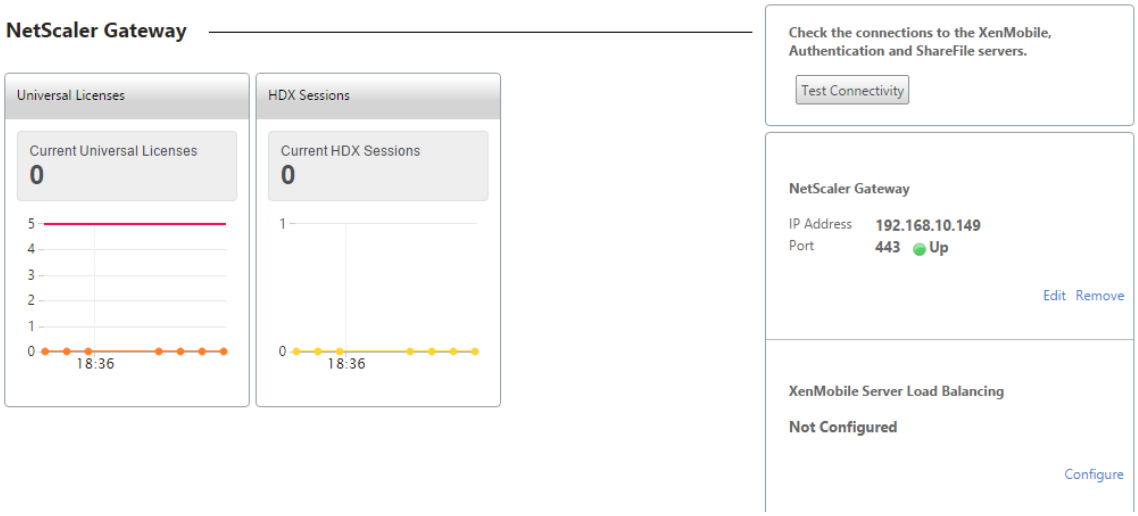
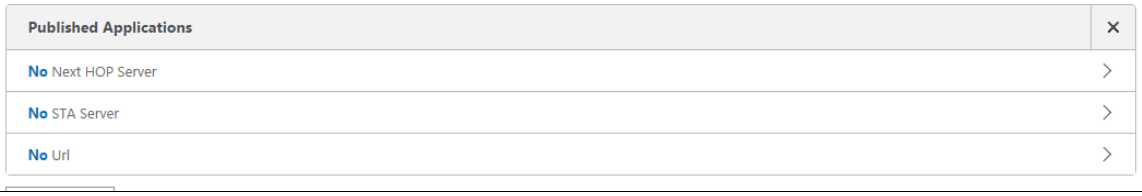
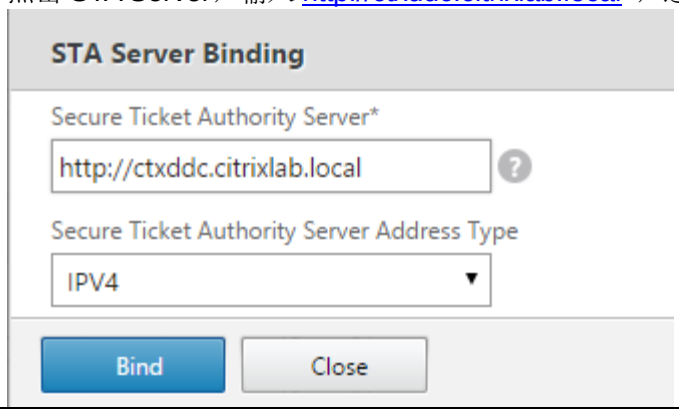
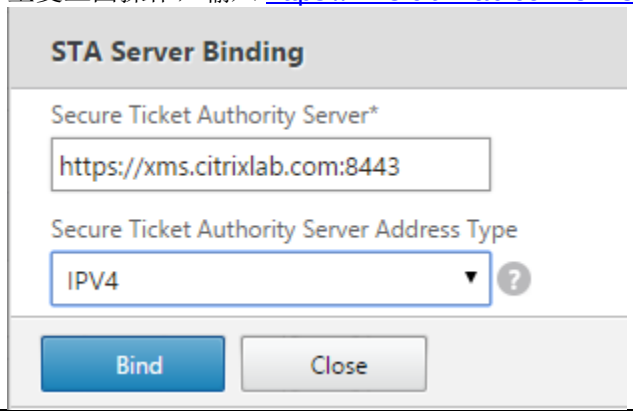
步骤	操作
13.	点击 SSL -> Certificates，选择 Install， Pair name: mam.pair Certificate file name: mam.cer (browse 选择) Key File name: mam_key（browse 选择） 
14.	这样证书就准备好了。 
15.	回到 NetScaler 主页面，点击下面的 XenMobile 

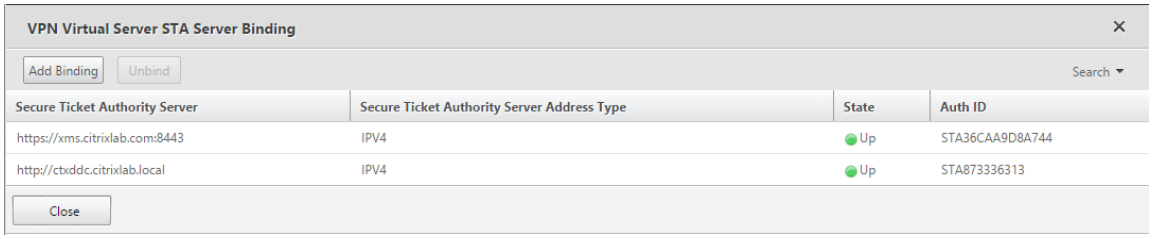
步骤	操作
16.	选择 XenMobile 10，Get Started 
17.	勾选掉 Load Balance XenMobile Servers，只保留 Access through NetScaler Gateway。 注：勾选掉原因是在此环境中只有 1 台 XenMobile，没有 LB 需求。如有 LB 需求，请自行选择并配置。 

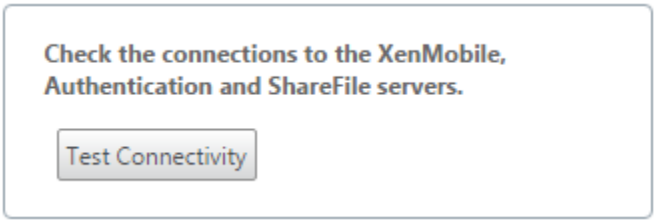
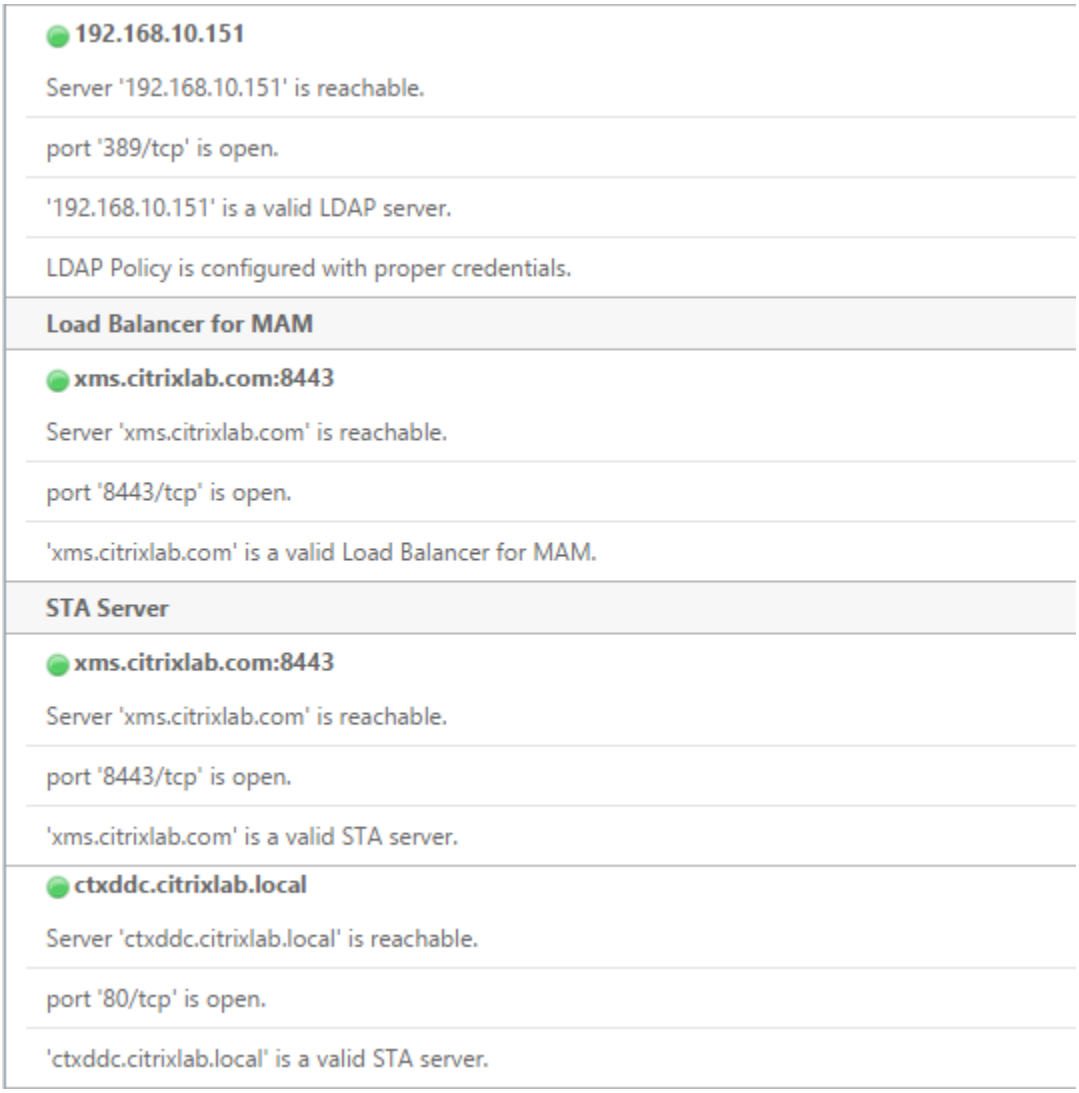
步骤	操作
18.	输入对应的 mam vs 的 IP 地址， 
19.	选择前序中配置好的 mam 证书 

步骤	操作
20.	由于使用的相同域，所以 AD 配置可以继续使用 XD/XA 环境中使用的。 
21.	本例中，由于本例中 XenMobile 服务器只有一台，所以所有的信息都直接指向对应服务器 IP 地址。 SSL traffic configuration，选择 http communication to XenMobile Server。 如需要 HTTP communication，则需要确保对应证书信任。 

步骤	操作
22.	选择 do it later。 
23.	Add Servers 
24.	输入 XenMobile 服务器 IP 地址，点击 Done 完成配置。 

步骤	操作
25.	基本配置就完成了。 
26.	点击左侧的 NetScaler Gateway - > Virtual Server，选择前序 mam.citrixlab.com，双击展开后点击右侧的 Published Applications, 
27.	点击 STA Server，输入 http://ctxddc.citrixlab.local ，选择 IPV4， 
28.	重复上面操作，输入 https://xms.citrixlab.com:8443 ,选择 IPV4， 

步骤	操作
29.	确保两个 STA 都显示状态正常的绿色， 

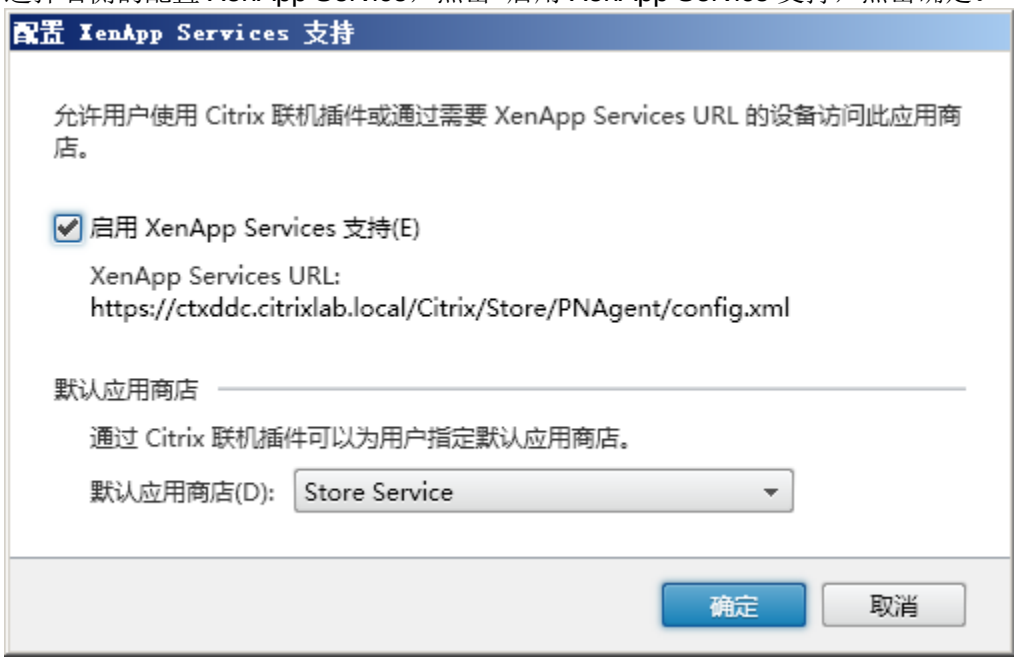
步骤	操作
30.	为了确保 NetScaler 都配置正确，可以到 XenMobile 向导界面，选择 Test Connectivity 做一个健康检查，  确保基本配置都是显示正常的绿色。 

步骤	操作
31.	登录 AD/DNS 服务器，增加一个 host 记录 192.168.10.149; mam.citrixlab.com

6.4 安装配置 StoreFront

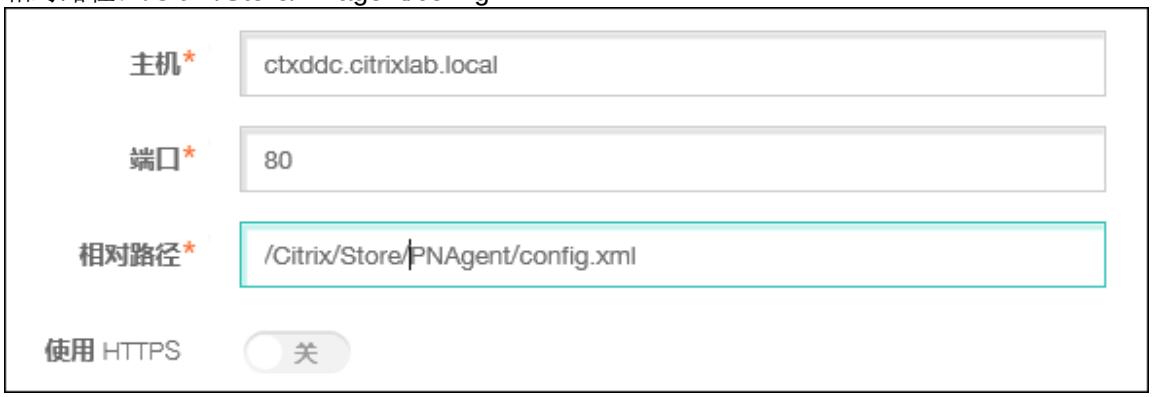
本例已经假设 XenDesktop 与 NetScaler 完成了集成，即用户使用 Receiver 可以在公网通过 NetScaler 获取虚拟桌面和应用。如果没有，请参考 PoC Runbook 手册中《PoC 手册 - Lab 07 NetScaler 基本安装及配置》进行配置。

步骤	操作
1.	登录 StoreFront 服务器打开 StoreFront Studio，点击 应用商店，并选择 Store

步骤	操作
2.	选择右侧的配置 XenApp Service，点击 启用 XenApp Service 支持，点击确定。 
3.	选择 NetScaler Gateway，选择添加 NetScaler Gateway，输入信息： NetScaler Gateway URL: https://mam.citrixlab.com 回调 URL（可选）https://mam.citrixlab.com 注：此次就是前序 NetScaler 配置中所设定的 MAM vserver 所对应的 URL。 

步骤	操作
4.	确保此时此时有两个 NetScaler gateway 配置， 第一个是 XenDesktop/XenApp 所对应的 NetScaler Gateway， 第二个是 XenMobile MAM 所对应的 NetScaler gateway。 
5.	回到应用商店，继续选择你所需要发布的 Store，并点击右侧的 启用远程访问，确保两个 NetScaler Gateway 的配置都已经添加。 默认设备为 XenDesktop 对应 NetScaler Gateway 没有问题。 

6.5 配置 XenMobile 集成 XenDesktop、XenApp

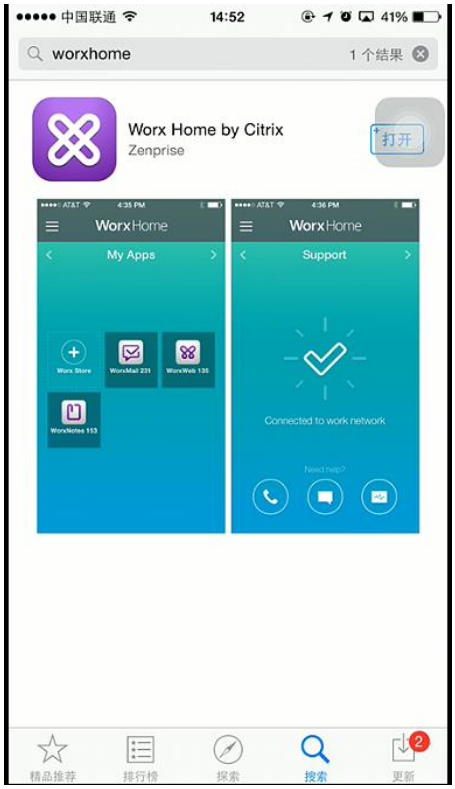
步骤	操作
1.	访问到 XenMobile 服务器管理控制台，点击 配置 -> 设置 –> XenApp/XenDesktop， 
2.	输入如下信息，保存并推出。 主机：ctxddc.citrixlab.local 端口：80 相对路径：/Citrix/Store/PNagent/config.xml 

第7章 用户端配置

由于本例中没有条件将 xms.citrixlab.com 和 mam.citrixlab.com 发布到公网，所以所有测试是在一个局域网+AP 热点网络中实现。实际项目中请参考 4.1.1 的网络架构图，将对应 IP 和端口映射至公网。

1.	由于本例中所有的证书都是通过 Windows CA 颁发，所以在进行操作之前，请通过邮件将根证书发送到测试设备上，并进行安装，确保不会出现无法注册的问题。 

2. 打开移动设备上的应用商店，搜索 WorxHome 并下载，如果后续还要集成使用 Windows 应用程序，请搜索 Receiver 并下载



3. 在 WorxHome 中输入 xms.citrixlab.com，

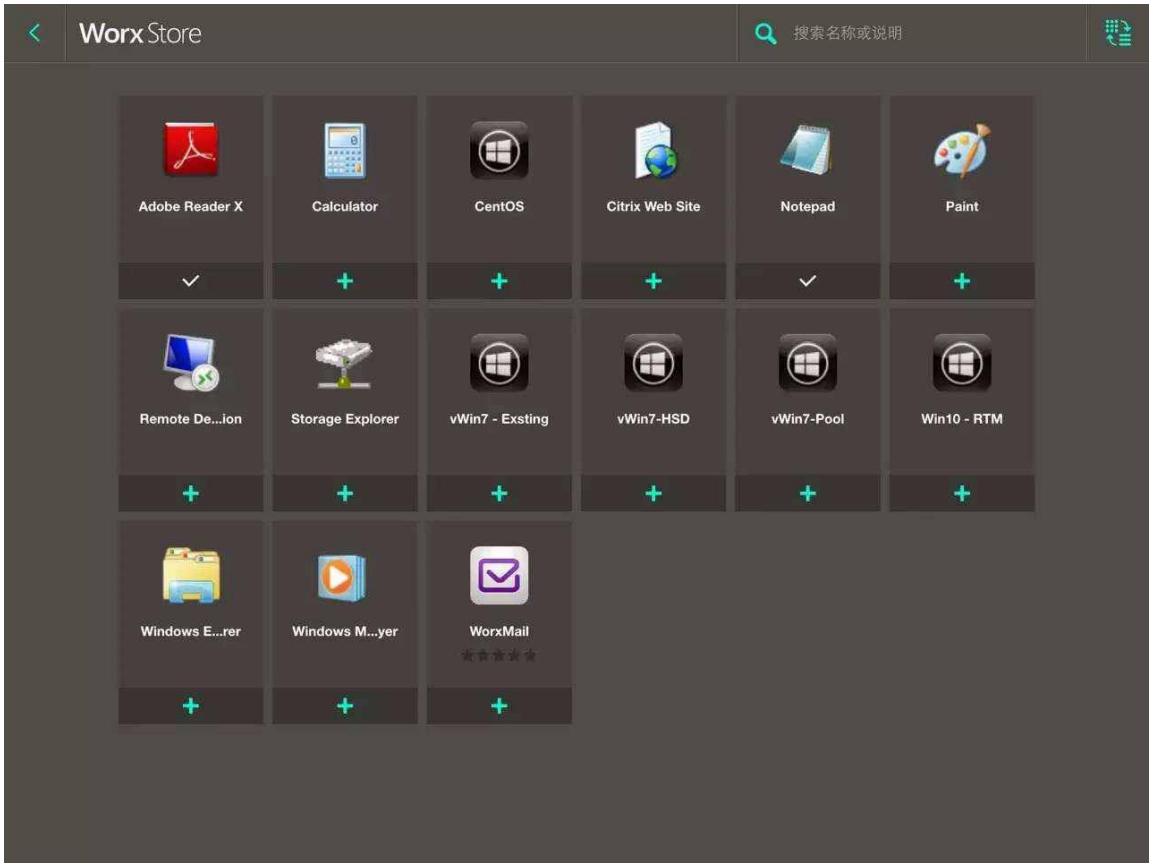
4.	按照提示注册设备，如果需要 MDM 设备管理选择 是，不希望设备被管理选择 否（所有应用需要手动安装，而且 Windows 应用图标不能推送到 iOS 设备主页上） 
5.	输入账号密码，完成用户验证， 

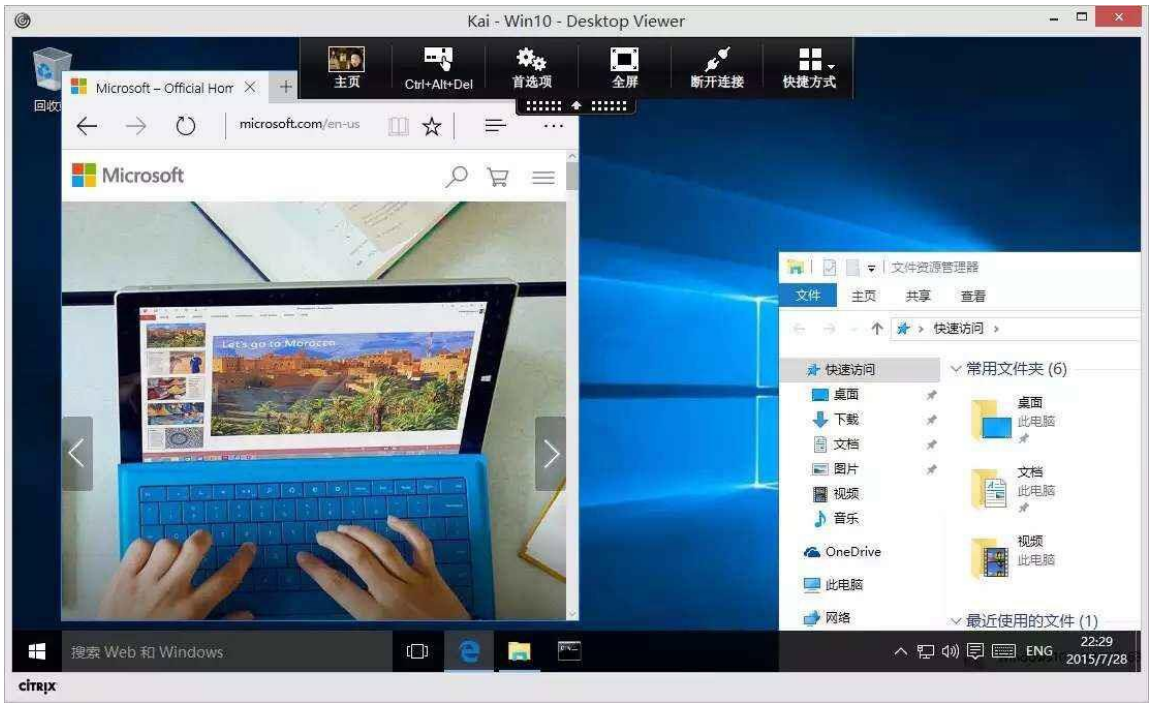
6. 按照提示进行安装，

7. 安装过程会提示输入密码，即安装 Pin code 要求设定的密码，

8. 安装 XenMobile profile 完成初始配置化的推送。

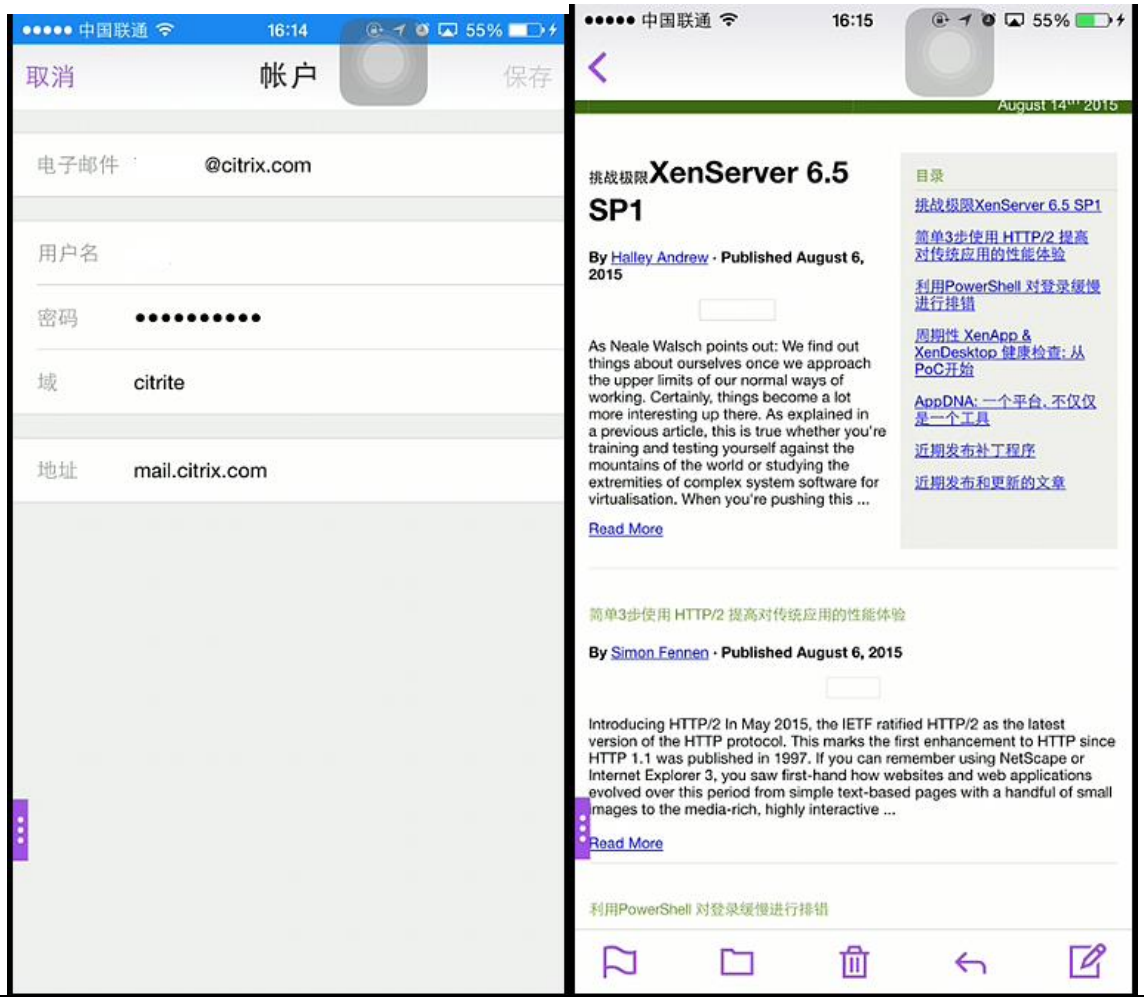
9. 注册完成后，在 WorxHome 中我就可以看到此用户分配的原生应用和 Windows 应用和桌面。



10.	打开 Windows 10 VDA 
11.	打开 Linux VDA 

12. 打开 WorxMail，完成初始配置后，即可收发邮件，并可以实验一下是否邮件内容是否可以拷贝到个人设备的文本应用中。

如果想允许用户把邮件正文拷贝到设备的文本应用中，策略需要如何调整？之后多久能生效？很多奇妙的事情等着你慢慢去发现哦！



产品版本

产品	版本
XenDesktop	7.6 FP2
XenApp	7.6 FP2
XenServer	6.5 SP1
Provisioning Server	7.6
NetScaler	10.5
XenMobile	10.1