
# Citrix® XenMobile™ Mobile Device Management

Gain an insight into the industry's best and most secure Enterprise Mobility Management solution

Akash Phoenix

[PACKT] PUBLISHING enterprise professional expertise distilled

# Citrix® XenMobile™ Mobile Device Management

Gain an insight into the industry's best and most secure Enterprise Mobility Management solution

**Akash Phoenix**

[PACKT] PUBLISHING enterprise professional expertise distilled

BIRMINGHAM - MUMBAI

# Citrix® XenMobile™ Mobile Device Management



First published: February 2014

Production Reference: 1140214

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78217-214-7

www.packtpub.com

Cover Image by Seenivasan Kumaravel (kseenivasan@hotmail.com)

# Credits

**Author**
Akash Phoenix

**Reviewers**
Jan Hendrik Meier
Joseph Muniz

**Acquisition Editor**
Sam Wood

**Content Development Editor**
Poonam Jain

**Technical Editors**
Shashank Desai
Menza Mathew

**Copy Editor**
Laxmi Subramanian

**Project Coordinator**
Akash Poojary

**Proofreader**
Stephen Copestake

**Indexer**
Mariammal Chettiyar

**Production Coordinator**
Sushma Redkar

**Cover Work**
Sushma Redkar

# Notice

The statements made and opinions expressed herein belong exclusively to the author and reviewers of this publication, and are not shared by or represent the viewpoint of Citrix Systems®, Inc. This publication does not constitute an endorsement of any product, service, or point of view. Citrix ® makes no representations, warranties or assurances of any kind, express or implied, as to the completeness, accuracy, reliability, suitability, availability, or currency of the content contained in this publication or any material related to this publication. Any reliance you place on such content is strictly at your own risk. In no event shall Citrix®, its agents, officers, employees, licensees, or affiliates be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business information, or loss of information) arising out of the information or statements contained in the publication, even if Citrix® has been advised of the possibility of such loss or damages.

.

# About the Author

**Akash Phoenix** is a leading Messaging and Enterprise Mobility Solutions expert with a diverse global background in technologies such as Microsoft Exchange, Windows Servers, Cisco Ironport and ISE, Citrix® NetScaler® Gateway, and App Controller. Also, he has an in-depth, hands-on knowledge of Enterprise Mobility Management Solutions, such as Citrix® XenMobile™, AirWatch, MobileIron, BlackBerry, SOTI, and many others. He also operates his own blog named *TeamXchange* on Messaging, Enterprise Mobility, and multiple other technologies.

---

I would like to thank the three most beautiful ladies in my life: my mother, Mira; my wife, Lasang; and my precious daughter, Araaya. Without you, I could never have made it to anywhere. Dad, thanks for being the best friend I've ever had. I would like to thank my friends for always being a constant support and encouraging me in whatever I did.

---

# About the Reviewers

**Jan Hendrik Meier** had his initial experience with IT during LAN parties before he decided to make this hobby, his job. Therefore, he started as an IT-Specialist trainee. During this time, he came across the company named Citrix®. He collected initial experiences with an early XenDesktop® (or better known as XenApp®) Version – MetaFrame XP. He deepened his knowledge in products such as Presentation Server, XenApp®, and XenDesktop®, and started to extend his knowledge with various other Citrix® products, such as Provisioning Server, NetScaler®, and XenMobile™.

After staying for about half a year in Australia, he picked up a job as a consultant in a mid-size company. Here, he helped customers with the planning and implementation of different Citrix® and Microsoft technologies. Furthermore, he is writing books and professional articles about different technologies. Whenever he chances upon any interesting problems during his job, he writes their description and the solutions for them in his blog `http://www.jhmeier.de`.

---

I would like to thank Andrea for being so patient while I was investing my available spare time in reviewing this book and writing articles, blog, or books on IT.

---

**Joseph Muniz** is a CSE at Cisco Systems® and a security researcher. He started his career in software development and later managed networks as a contracted technical resource. Joseph moved into consulting and found a passion for security while meeting with a variety of customers. He has been involved with the design and implementation of multiple projects ranging from Fortune 500 corporations to large federal networks.

Joseph runs *The Security Blogger*, a popular resource describing security and product implementation. You can also find Joseph speaking at live events as well as involved with other publications. His recent events include speaking for *Social Media Deception* at both the *2013 ASIS International* conference and *RSA Europe security conference*.

He is the author of *Web Penetration Testing with Kali Linux*, *Packt Publishing,* September 2013 and an article on *Compromising Passwords* in the *PenTest* magazine, *Backtrack Compendium*, in July 2013. Also, he was a reviewer of the books, *Kali Linux Social Engineering*, *Packt Publishing* in December 2013 and *Instant XenMobile MDM*, *Packt Publishing*, in September 2013.

Outside work, he can be found behind turntables, scratching classic vinyl, or on the soccer pitch, hacking away at the local club teams.

---

I couldn't have contributed my time to this book without the support of my charming wife, Ning, and creative inspirations from my daughter, Raylin. Also, I must credit my passion for learning to my brother, Alex, who raised me, along with my loving parents Irene and Ray. And I would like to give a final thank you to all of my friends, family, and colleagues who have supported me over the years.

This is the fourth time I've written an acknowledgement for a book; so, I'm grateful to continue to have opportunities to work on publications.

---

# www.PacktPub.com

## Support files, eBooks, discount offers and more

You might want to visit `www.PacktPub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.


`http://PacktLib.PacktPub.com`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

## Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

## Free Access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

## Instant Updates on New Packt Books

Get notified! Find out when new books are published by following `@PacktEnterprise` on Twitter, or the *Packt Enterprise* Facebook page.

# Table of Contents

# Preface

With the launch of a new mobile device every day, **Mobile Device Management** (**MDM**) solutions are on the top priority list for most of the corporate houses. This book deals with the Citrix® XenMobile™ Solution, which has been acknowledged as one of the most secure solutions available as of now. In this book, we will introduce each of the XenMobile™ Solution components and further provide detailed step-by-step instructions to successfully deploy these components.

## What this book covers

*Chapter 1*, *XenMobile™ Solutions Bundle,* introduces our readers to the XenMobile™ Solutions Bundle and its components.

*Chapter 2*, *XenMobile™ Solution Deployment Prerequisites*, covers the system requirements and prerequisites required to successfully deploy the XenMobile™ components.

*Chapter 3*, *NetScaler® Gateway VPX Deployment*, introduces our readers to the NetScaler Gateway VPX Solution and its step-by-step deployment procedure.

*Chapter 4*, *XenMobile™ Device Manager Deployment*, covers the XenMobile™ Device Manager Installation and configuration steps.

*Chapter 5*, *XenMobile™ App Controller Deployment*, covers the step-by-step installation and configuration for the XenMobile™ App Controller.

*Chapter 6*, *XenMobile™ Remote Support*, covers the installation steps for XenMobile™ Remote Support tool and configuration to remotely access enrolled mobile devices.

*Chapter 7*, *Device Enrollment and Revoking Access*, covers the steps to enroll devices with the XenMobile™ Device Manager server and revoke access to these devices.

*Chapter 8*, *Managing Applications*, explains how to manage applications residing on enrolled devices using the XenMobile™ Device Manager and XenMobile™ App Controller.

*Chapter 9*, *Deploying Policies*, introduces XenMobile™ Device Manager and App Controller policies with examples.

*Chapter 10*, *Troubleshooting*, covers the most common installation and configuration challenges faced by admins, with their best possible resolutions.

# What you need for this book

You need to install the following software applications:

- XenMobile™ Device Manager 8.5
- App Controller 2.9
- NetScaler VPX 10
- XenMobile™ Remote Support 8.5
- VMware Workstation 8 (used for testing purpose)
- VMware ESX or XenServer® (for production environments)
- Worx Home 8.5.0 for mobile devices

# Who this book is for

This book is for professionals who want to familiarize themselves with MDM and who aspire to discover how MDM software is designed to meet the most complex and demanding mobile requirements when it comes to securing their mobile enterprise.

# Conventions

In this book, you will find a number of styles of text that distinguishes between different kinds of information. Here are some examples of these styles and an explanation of their meaning.

Code words in text are shown as follows: "We can include other contexts through the use of the `include` directive."

A block of code is set as follows:

```
[default]
exten => s,1,Dial(Zap/1|30)
exten => s,2,Voicemail(u100)
exten => s,102,Voicemail(b100)
exten => i,1,Voicemail(s0)
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
[default]
exten => s,1,Dial(Zap/1|30)
exten => s,2,Voicemail(u100)
exten => s,102,Voicemail(b100)
exten => i,1,Voicemail(s0)
```

Any command-line input or output is written as follows:

```
# cp /usr/src/asterisk-addons/configs/cdr_mysql.conf.sample
     /etc/asterisk/cdr_mysql.conf
```

**New terms** and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "clicking the **Next** button moves you to the next screen".

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

# Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

# Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

# Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/submit-errata`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

# Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

# Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

# 1

# XenMobile™ Solutions Bundle

**Citrix XenMobile** is one of the most sought-after MDM solutions in today's market due to its complete end-to-end security offering. Previously known as **Zenprise**, before the acquisition of the company by Citrix, it offered a Device Management and a Secure Mobile Gateway solution. Later, Citrix added its complete network and virtualized environment support to this solution by integrating the NetScaler Gateway, App Controller, and XenDesktop. This was launched as the **XenMobile Solutions Bundle**. In this chapter, we will introduce our readers to the XenMobile Solution and all of its components. The topics covered in this chapter are as follows:

- Introduction
- Features
- Deployment flowchart

## Introduction to XenMobile™ Solution

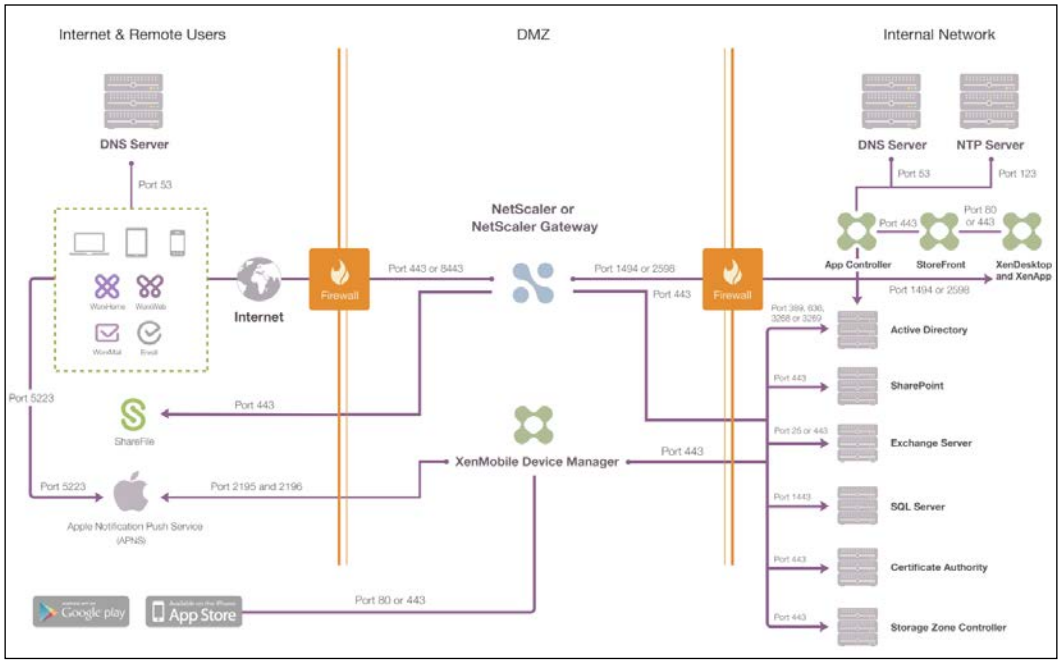
The XenMobile Solution allows to manage mobile devices, the applications inside these devices, and the data in these applications. This enables users to access their apps, which may be mobile-, SaaS-, web-, or Windows-based from a universal app store. It provides administrators with a granular level control over the devices and manages them accordingly by implementing multiple security policies. It provides admins with the options to securely deliver productivity apps such as e-mails or intranet websites to end users. Also, it permits options to securely wrap applications before deployment without compromising application security and productivity.

With more and more enterprises welcoming the **Bring Your Own Device** (**BYOD**) concept, a scenario where the employees are allowed to bring their own devices at work, XenMobile components allow admins to securely manage these devices without hampering the end-user device experience.

In this section, we will introduce our readers to the following XenMobile Solution components and their role in the XenMobile Solution:

- **NetScaler Gateway**: This is a secure, access-control management solution allowing users to securely access internal resources. It also provides administrators with granular control policies to manage how devices will function once they are connected to internal resources. These internal resources can be an intranet portal, corporate e-mails, or in-house apps.
- **XenMobile Device Manager**: The XenMobile Device Manager allows administrators to manage devices, users, enroll devices, deploy applications and files, and set policies. XenMobile Device Manager also has the option to integrate Active Directory and detailed reporting features.
- **App Controller:** App Controller allows users to access the Web, SaaS-based applications, iOS and Android apps, and integrate ShareFile apps on their device from anywhere on an internal network. When integrated with NetScaler Gateway, the XenMobile Solution provides the users with access to these resources from an external network. Administrators have granular security policies to implement on devices connecting either from an internal or external network.
- **MDX Toolkit:** The MDX toolkit is a software that must be installed on Mac OS to wrap iOS or Android-based apps and ensures the apps are secure and compliant when installed on end-user devices. Administrators can also define a set of default policies while wrapping the app to limit how it works.
- **Worx Apps**: These are client-based apps that communicate with App Controller and allow users to access internal resources anywhere. They contain Worx Home for user enrollment, Worx Web to access web-based resources, and WorxMail for accessing corporate e-mails.
- **ShareFile**: This is a cloud-based, file-sharing service that enables users to securely share documents from different apps or access shared resources on a desktop from mobile devices. ShareFile data can be accessed as an app, web resource, or through integration with Outlook as an add-in.

The XenMobile Solution with its components creates a highly secure and enterprise-compliant solution. The following diagram is a detailed network diagram for the XenMobile Solution provided by Citrix:





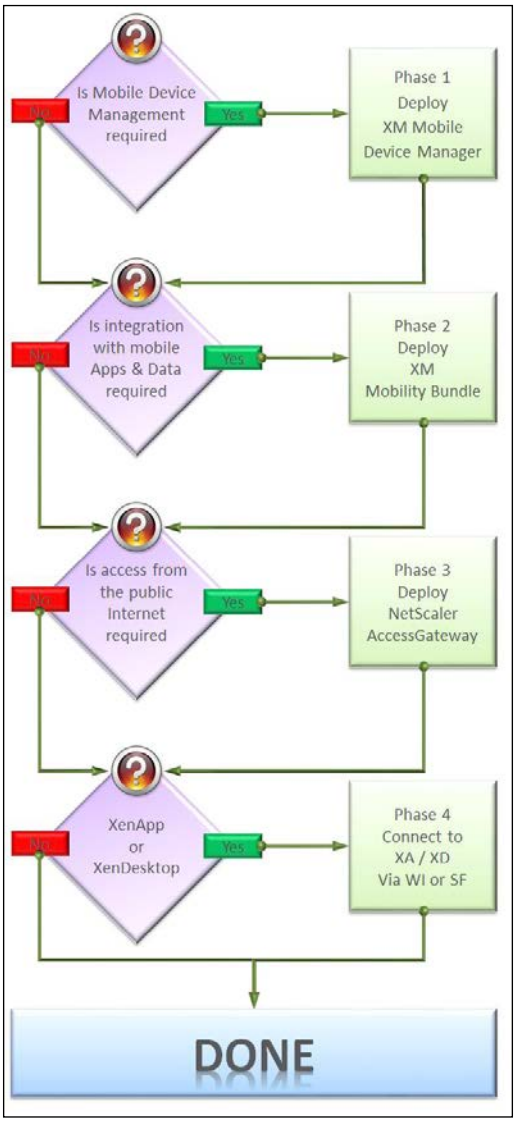

# XenMobile™ Solution features

XenMobile contains some of the most sought-after features when compared to its competitors. In this section, we will list some of the features available in XenMobile, as follows:

- Configuring, provisioning, and managing mobile devices on Windows Mobile, Symbian, iOS, and Android platforms
- Mobile Content Management using SharePoint and network-driven integration
- Secure mobile web browser
- App-specific micro VPN
- Integrating Windows apps
- Unified app store
- Secure document sharing, syncing, and editing

# The deployment flowchart

While implementing a **Mobile Device Management** (**MDM**) solution, it's very important to have a deployment pattern. This helps in understanding which components are required or are not suitable as per the environment needs. This brings in the requirement to have a detailed flowchart of the Solution deployment. The following diagram shows the Citrix-recommended best practice's deployment flowchart for the XenMobile Solution:



# Explanation

In this section, we will break down the deployment flowchart to understand the component selection phase. The flowchart is based upon our requirements and will vary from one scenario to other.

## Phase 1

The essentials for phase 1 are as follows:

- **Requirement**: Do we want an MDM solution to manage the enrolled devices?
- **Decision**: If an MDM solution is required, then we proceed with the XenMobile Device Manager installation; alternatively, we can move to the next requirement

## Phase 2

The essentials for phase 2 are as follows:

- **Requirement**: Is application and content management required?
- **Decision**: If application and content integration is required then we can deploy the XenMobile Solutions Bundle; alternatively, move to the next requirement

## Phase 3

The essentials for phase 3 are as follows:

- **Requirement**: Will there be users accessing the integrated applications and data from the public Internet?
- **Decision**: If `Yes`, then move ahead with the NetScaler Gateway deployment; alternatively, move to the next requirement

## Phase 4

The essentials for phase 4 are as follows:

- **Requirement**: Is access to XenApp or XenDesktop required?
- **Decision**: If `Yes`, then connect using StoreFront

# Summary

This chapter provided a brief overview of XenMobile Solution and each of its components. We also covered many of its features make it unique and the Network architecture of the solution. Additionally, we have addressed the best practice deployment flowchart of the XenMobile Solution as recommended by Citrix.

In the upcoming chapter, we will cover the deployment prerequisites for XenMobile Solution.

# 2

# XenMobile™ Solution Deployment Prerequisites

To ensure the successful deployment of a XenMobile Solution, the system requirements and prerequisites should be met. This chapter will prepare you to configure the preinstallation tasks for the XenMobile Solution. We will also identify the settings, certificates, ports, hardware, and so on, required to build a complete XenMobile Solution. All settings and configurations in this chapter will be done with an assumption of catering to 100 user devices or connections. In this chapter, we will be covering the following topics:

- Network settings
- Licensing
- Certificates
- Ports
- Active Directory settings
- Database requirements
- Server (hardware/hypervisor) sizing requirements

## Network settings

All existing as well as post-deployment network settings should be identified in order to properly configure the XenMobile components in your infrastructure. You must gather the following settings before starting the implementation.

- Internal **Fully Qualified Domain Name** (**FQDN**)
- Public and private IP address (for existing AD and Exchange servers)

- Subnet mask
- Default gateway
- DNS settings
- Reserve NetScaler Gateway IP addresses
- Reserve App Controller IP address
- Reserve XenMobile DM server IP address
- NTP server IP address

# Licensing

You must ensure all licenses are available before proceeding with the installation of XenMobile components. Both XenMobile MDM Edition and NetScaler Gateway require individual licenses to function. After buying the XenMobile Solutions Bundle, you can obtain your licenses by logging on to the Citrix portal.

Further detailed instructions on Licensing can be found at `http://www.citrix.com/products/xenmobile/how-it-works/licensing.html`.

The backup of the configuration files contains all uploaded licenses. If you reinstall XenMobile DM or NetScaler Gateway and do not have a configuration backup, you will need the original license files to complete the installation.

# Certificates

The certificates ensure that the connection made between two entities is secure and authenticated depending on the environment (for example, LDAP authentication for Microsoft Active Directory services).

When a user device tries to create a secure connection using a web browser, the server sends its certificate to the device. The browser on the device then checks for **Certificate Authority** (**CA**) of the device and whether the CA is trusted by the device. In the case that the CA is trusted, the user is granted access to the service. Otherwise, the browser notifies the user that the CA is not trusted with an option to either accept or decline the certificate.

The wildcard or SAN certificates are supported by XenMobile. Most deployments require only two (external and internal) certificates.

The XenMobile components require certain specific certificates to function properly. A better understanding of the following certificates and their functioning will help you to manage and troubleshoot XenMobile components effectively:

- **Server Certificate**: The identity of a server (for example, NetScaler Gateway/App Controller/XenMobile DM) is certified by a server certificate.
- **Root Certificate**: The root certificate identifies and verifies the CA that signed the server certificates.

# Apple Push Notification Service certificates

The **Apple Push Notification Service** (**APNS**) is a mobile notification service created by Apple. APNS uses push technology through an accredited and encrypted IP connection to forward notifications over persistent connections from application servers such as XenMobile to iOS devices such as the iPhone, iPad, and iPod Touch. An APNS certificate is a provisioned security certificate obtained through **Apple Push Certificates Portal**, which can be found at `https://identity.apple.com/pushcert/`. The APNS certificate can be obtained by enrolling for an Apple ID, which will allow you to upload certificates and further download Apple-signed APNS certificates.

# Security Assertion Markup Language certificates

The **Security Assertion Markup Language** (**SAML**) services integrate with XenMobile components and identity providers, enabling authentication capabilities that are not dependant on Active Directory services.

The following table shows the certificate format and type supported by each XenMobile component:

| Component | Certificate format | Certificate type required | Location |
|---|---|---|---|
| NetScaler® Gateway | PEM (BASE64) | • Server<br>• root | External |
| App Controller | PEM or PFX (PKCS#12) | • Server<br>• SAML<br>• root | Internal |
| StoreFront | PFX (PKCS#12) | • Server<br>• root | Internal |
| XenMobile™ DM | P12 format (PKCS#12) | • APNS<br>• Server | External |

# Opening ports

Ports act as communication endpoints, allowing applications to successfully communicate with the XenMobile components. You must ensure the relevant ports are opened on your firewall. The following table defines the ports that you need to open.

| Port | Description |
|---|---|
| 21 | FTP services. |
| 25 | SMTP services. |
| 53 | DNS. |
| 80 | HTTP requests. |
| 443 | HTTPS requests. |
| 123 | **Network Time Protocol** (**NTP**) services. |
| 389/636/3268 | LDAP requests. |
| 1433 | SQL server database requests. |

| Port | Description |
|---|---|
| 1494 | Provides a connection between Windows-based applications in the internal network by using the ICA protocol. Citrix recommends keeping this port open. |
| 1812 | RADIUS connection. |
| 2598 | Provides a connection between Windows-based applications in the internal network by using session reliability. Citrix recommends keeping this port open. |
| 2195 | Outbound APNS requests to `gateway.push.apple.com` for iOS Notifications and Policy deployment. |
| 2196 | Outbound APNS requests to `feedback.push.apple.com` for iOS notifications and policy deployment. |
| 5223 | Outbound APNS requests from iOS devices on Wi-Fi networks. |
| 9080 | HTTP requests from NetScaler to XNC. |
| 9443 | HTTPS requests from NetScaler to XNC. |
| 8443 | iOS device's enrollment requests. |

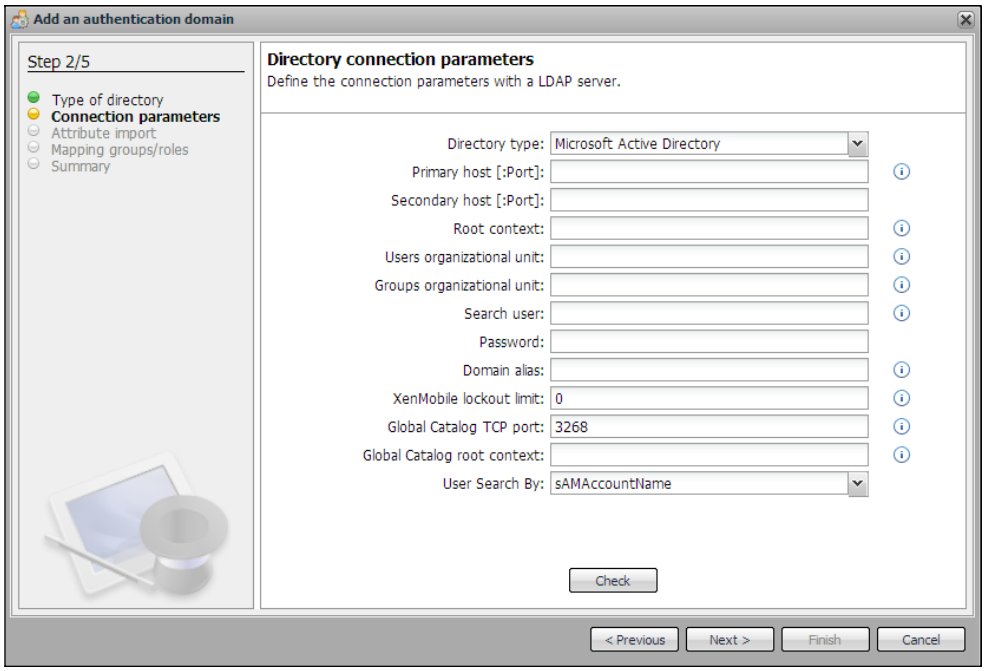
# Active Directory settings

XenMobile components, when integrated with Active Directory, allow access to users, groups, and other objects existing in the infrastructure. Ensure that you gather the following Active Directory settings before installing the XenMobile components:

- Primary DNS server IP address
- LDAP ports
- Root context (for example, `DC=TEAMXCHANGE,DC=IN`)
- Domain alias
- LDAP user ID and password

It's always recommended to have a separate user created in Active Directory for LDAP usage.

The following screenshot consists of the Active Directory settings:




# Database requirements

The XenMobile DM installer contains the **PostgreSQL** (**Postgres**) database server bundles within it. XenMobile also supports Microsoft SQL server. Citrix suggests using Postgres only for test deployments. XenMobile supports the following databases to manage its repository:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012

The service account should have Administrator rights and Creator, Owner, and Read/Write permissions.

[ Refer to Microsoft SQL Server Documentation for System Requirements and prerequisites ]

# Server sizing requirements for hardware/hypervisor

Each XenMobile component has dependencies on the type of hardware or hypervisor required to set up. The sizing of XenMobile components depends on the number and type of devices to be enrolled on the Device Manager server. The following configuration will help you decide on the sizing aspects of the XenMobile components for 100 devices.

## Citrix® NetScaler® Gateway

The **NetScaler Gateway** is available in the following three models depending on the deployment scenario chosen:

- **NetScaler SDX**: It's a hardware platform on which virtual instances of NetScaler or NetScaler Gateway can be installed and can handle up to 60,000 user connections
- **NetScaler MPX**: It's a physical appliance capable of handling up to 7,000 user connections
- **NetScaler VPX**: It's a virtual instance of the NetScaler Gateway that can be installed on a Windows Hyper-V or VMware ESX server and is capable of handling up to 870 user connections as recommended by Citrix

In this book, we will be deploying the NetScaler VPX solution for managing user devices.

## XenMobile™ Device Manager

The Device Manager server is Windows-based and its system requirements are as follows:

- Windows server requirements:
    - Microsoft Windows Server 2012 64-bit Standard or Enterprise Edition
    - Microsoft Windows Server 2008 R2 Standard or Enterprise Edition
- Java requirements:
    - Oracle Java SE 7 JDK (JDK Download Edition) with Version 11 and above
    - Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7

- Hardware requirements:
    - Physical or Virtual Host Machine
    - Intel Xeon 3 Ghz or AMD Opteron-1.8 Ghz server class
    - 4 GB RAM minimum
    - 500 MB minimum disk space
    - 2 Core or 2v CPU

# App Controller

The App Controller virtual instance can be installed either on XenServer 5.6 SP1 or above, Microsoft Hyper-V 2012, or VMware ESXi 4.0 or above. The App Controller server virtual machine requires the following minimum system configurations:

- **Memory**: 4 GB
- **Virtual CPU**: 2 VCPUs
- **Disk Space**: 50 GB
- **Virtual Network Interface**: 1

# Summary

As discussed in this chapter, we have identified the mandatory system requirements and prerequisites that need to be met before the deployment phase of the XenMobile components. In the next chapter, we will get started with installation of the NetScaler VPX Solution and its configuration.

# 3
# NetScaler® Gateway VPX Deployment

**NetScaler** is a secure Network Access Control solution that allows users to access their applications and data from anywhere across the web. In addition, it also helps administrators to apply granular policies to control these applications and data. The administrators can manage user activity from a single console based on the user identities or the devices they use to access network resources.

In this chapter, we will install **Netscaler Gateway 10.1 VPX**, a virtual appliance, on a VMware-based virtual machine and configure the virtual appliance.

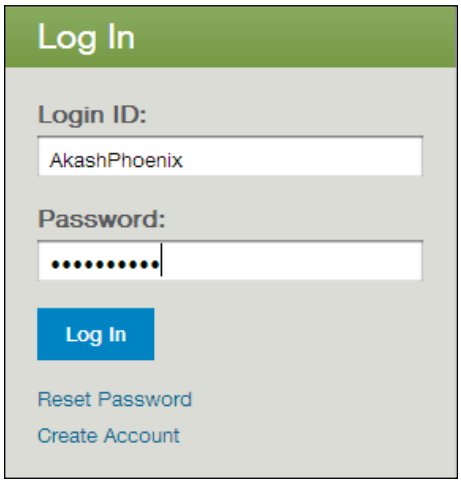
## Downloading the NetScaler® Gateway software

To download the XenMobile components, we need to go to the Citrix **Downloads** portal, which can be found at: `http://www.citrix.com/downloads.html`.

1. Click on **My Account (Log In)** and log on.

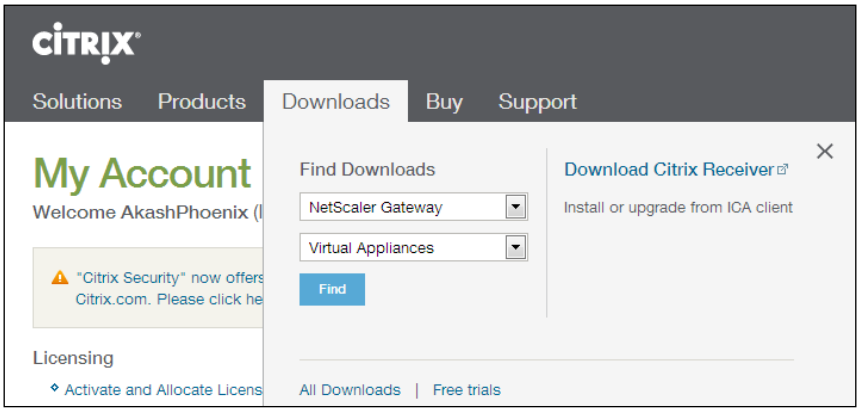
A Citrix account is mandatory to download any software from the Citrix download center. Register for a customer or a partner account at `https://www.citrix.com/welcome/create-account.html`.

The **Log In** window is shown as follows:





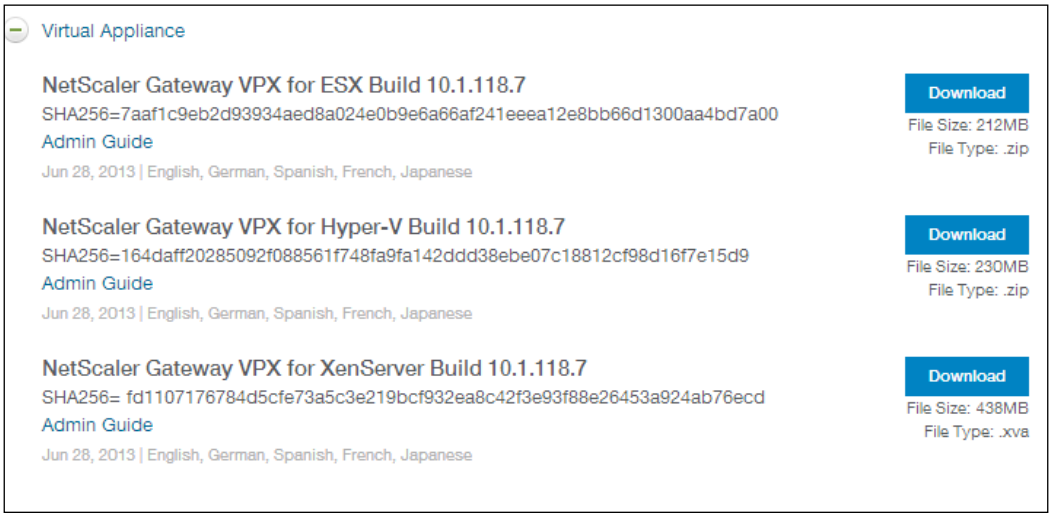

2. Click on **Downloads**.
3. Select **NetScaler Gateway** as the **Product** and **Virtual Appliances** as the **Download Type**.



4. Collapse **NetScaler Gateway** and click on **NetScaler Gateway 10.1 – Virtual Appliance**.




5. Download the VPX Build depending on the hypervisor being used.



# Importing the virtual appliance

After we have successfully downloaded the NetScaler VPX Build, we need to import it to the hypervisor. In the case of the VMware-based hypervisor, you should have the following three files available after download:

- `NSVPX-ESX-10.1-118.7_nc.mf`
- `NSVPX-ESX-10.1-118.7_nc.ovf`
- `NSVPX-ESX-10.1-118.7_nc-disk1.vmdk`

To deploy the virtual appliance, the following steps should be followed:

1. Log in to the VMware VSphere client.
2. Click on **File** and then choose **Deploy OVF Template**.
3. Click on **Browse** and locate the **NSVPX-ESX-10.1-118.7_nc.ovf** file.
4. Click on **Open** and select **Next**.
5. Agree to accept the terms of the licenses and click on **Next**.
6. Enter a **Name** for the virtual machine and click on **Next**.
7. Select a **Datastore** to store the deployed OVF template and click on **Next**.
8. Choose the Network Adapter you want to allot to the Virtual Machine and click on **Next**.
9. Verify the information and click on **Finish**. The OVF Deployment progress bar should appear.

Once the import procedure is completed, the NetScaler VPX appliance should appear on the VSphere Client. This completes the import procedure for the virtual appliance.

# Configuring NetScaler® VPX

In this section, we will configure the virtual appliance we imported into the Hypervisor in the last section. The NetScaler Gateway comes preconfigured with some default settings for management purposes, listed as follows:

| Default | Value |
|---|---|
| IP Address | `192.168.100.1` |
| Subnet Mask | `255.255.0.0` |
| Root Username | `nsroot` |
| Root Password | `nsroot` |

To proceed further with the installation, we need to ensure we have the following details in hand:

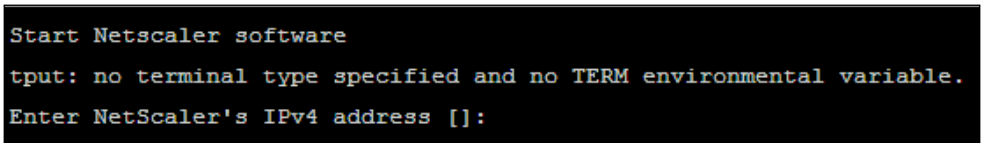
- **NetScaler IP Address** (**NSIP**): It's used for managing the NetScaler Virtual Appliance. Reserve a Static IP address to be assigned to the NetScaler Virtual Appliance.
- **Subnet IP Address** (**SNIP**): An SNIP is used in the case of multiple subnet scenarios to avoid configuration of alternate or additional routes on systems. In the case of a single subnet scenario, we can assign an IP address available in the same subnet.
- **Virtual Server IP Address** (**VIP**): A VIP is the IP address associated with a virtual server. It's the public IP address to which clients connect.
- **The Netmask**: It's the subnet mask of the IP address assigned to NetScaler Virtual Appliance
- **Default Gateway**: It passes traffic from the local subnet to a device on different subnets. It allows managing the NetScaler Gateway from devices that belong to a different subnet. Note down the Default Gateway for the IP address assigned to the NetScaler Virtual Appliance.

Now, let's proceed with the installation and configuration of the NetScaler Virtual Appliance.

# Command-line-based configuration

In this section, we will configure the settings on the NetScaler VPX server using command lines. Here, we will configure the IP address and the subnet mask of the NetScaler gateway to make it available for end-user devices and other XenMobile component discovery by performing the following steps:

1. Power on the virtual appliance. (The installation of the NetScaler Virtual Appliance is automatically done as soon as you power on the virtual machine.) Refer to the following screenshots.
2. When prompted, enter the IPv4 address reserved for NetScaler and its corresponding subnet mask.



3. Select option `4` to **Save and Exit** and let the **Virtual Machine** (**VM**) boot up.
4. At the **Login** prompt, enter the default root credentials `nsroot`, as mentioned in the preceding table.

```
login: nsroot
Password:
Dec  2 06:33:39 <auth.notice> ns login: ROOT LOGIN (nsroot) ON ttyv0
Copyright (c) 1992-2008 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

 Done
> 
```

The root password is not shown while entering, so ensure that *Caps Lock* is off to avoid any mistakes.

5. Next, we will verify the settings made earlier. Type `show ns config` and hit **Enter**. This will display the current IP address and the subnet mask of the NetScaler Virtual Appliance.

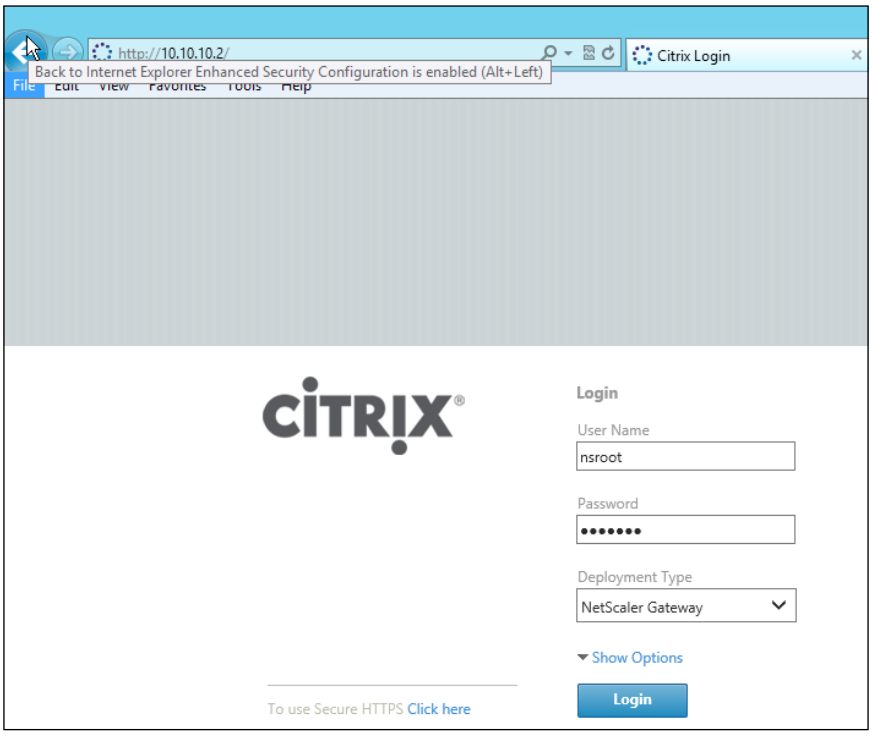
```
login: nsroot
Password:
Dec  9 05:24:57 <auth.notice> ns login: ROOT LOGIN (nsroot) ON ttyv0
Copyright (c) 1992-2008 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

 Done
> show ns config
        NetScaler IP: 10.10.10.2  (mask: 255.0.0.0)
         NW FWMODE: NOFIREWALL
        Number of MappedIP(s): 0
        Node: Standalone
                          System Time: Mon Dec  9 05:25:06 2013
              Last Config Changed Time: Mon Dec  9 04:14:30 2013
                Last Config Saved Time: Mon Dec  9 04:07:07 2013
 Done
> 
```

# Graphical user interface-based configuration

In this section, we will configure further detailed settings on the NetScaler VPX server using a graphical user interface. Here, we can check the configurations made using the command-line interface as well as other DNS configurations by performing the following steps:

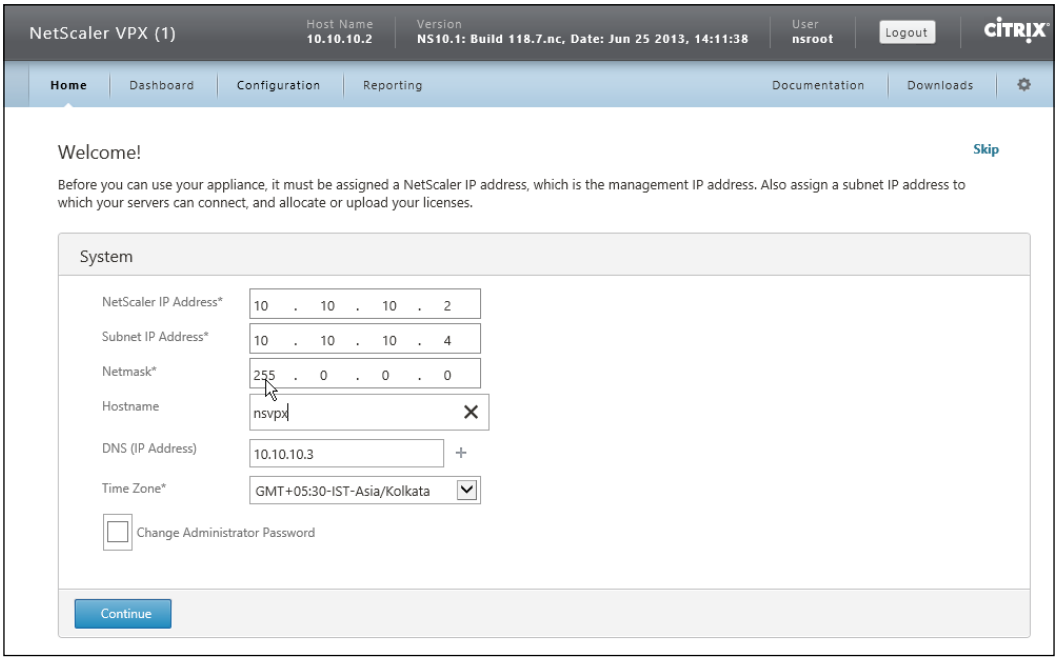
1. Log on to a system in the same subnet as NetScaler, open a web browser, and point to `http://ipaddress.of.netscaler` (for example, `http://10.10.10.2`).
2. Enter **User Name** and **Password**. Select **Deployment Type** as **NetScaler Gateway**. Refer to the following screenshot:




3. After logging in, the next screen will require some additional configurations, which are as follows:
    - **Subnet IP Address**: An SNIP is used in the case of multiple subnet scenarios to avoid configuration of alternate or additional routes on systems. In the case of a single subnet scenario, we can assign an IP address available in the same subnet.

- **Hostname**: Assign a name to the NetScaler Virtual Appliance.
- **DNS (IP Address)**: Enter the IP address of the Domain Name Server of the domain.
- **Time Zone**: Select the time zone according to your specific region or location.

4. Click on **Continue** after entering the preceding details.




# Adding licenses

In this section, we will assume you have purchased or applied for a NetScaler license as discussed in *Chapter 2, XenMobile™ Solution Deployment Prerequisites*. The next step is to add the NetScaler license file, which will enable license-based features in the product.

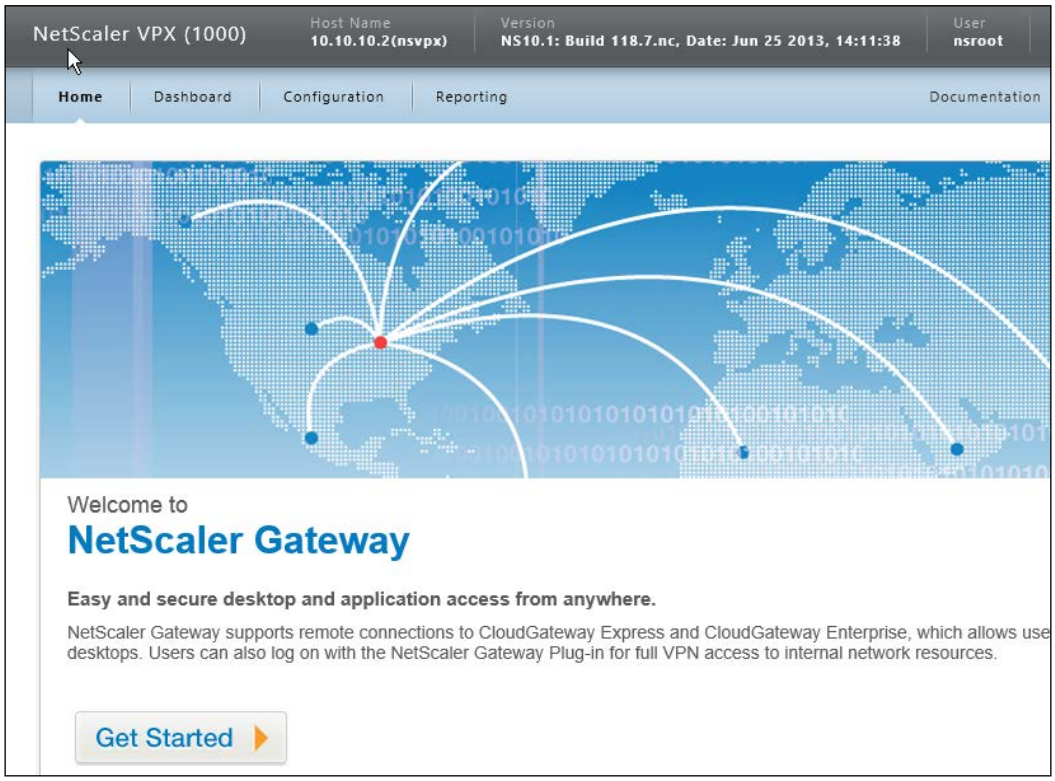
1. Log on to the Citrix web portal and download the NetScaler license file. The license file is in the `.lic` format.
2. Log on to the NetScaler web console.

3. Go to **Home** and click on **Continue.**
4. Select **Upload License Files** and click on **Browse**. The license should be updated successfully.
5. Click on **Continue** and then on **Done**.
6. Click on **Yes** to reboot the server for the changes to take effect.

# Configuring NetScaler® Gateway

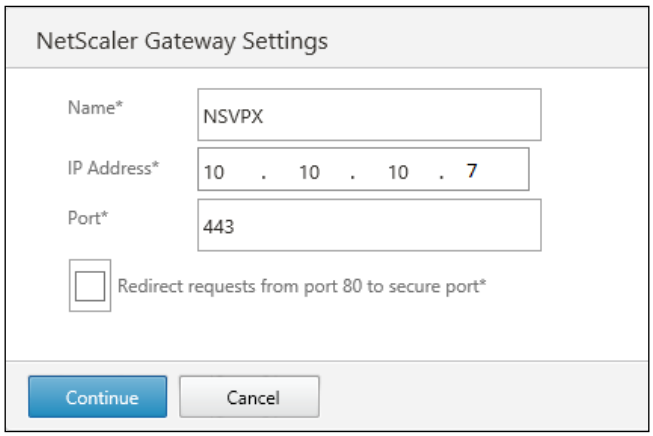
In this section, we will configure a virtual server on NetScaler, which will communicate with App Controller to provide web application and SaaS-based services to end-user devices. To do so, perform the following steps:

1. Log on to NetScaler Gateway with the default credentials.
2. Click on **Get Started** to configure the virtual server.



3. Enter the **Name** (choose a unique name for the server), **IP Address**, and **Port** for the virtual server

The naming convention for the server can be the external FQDN, which is used to connect to the NetScaler Gateway.




When the **Redirect requests from port 80 to secure port** option is selected, it allows NetScaler Gateway to redirect the `http` requests to secure `https` requests.

4. Click on **Continue**.

# Assigning certificates

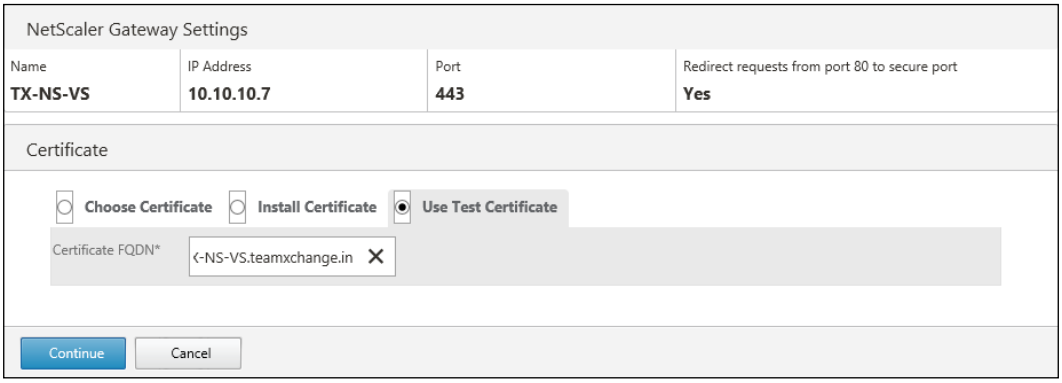
The certificates assigned in this section ensure communication between the Gateway and the App Controller is secure. To assign certificates, perform the following steps:

1. On the **Certificate** page, we need to assign a **Secure Socket Layer** (**SSL**) certificate to the virtual server. We have three options for assigning certificates:
    - **Choose Certificate**: It allows you to choose from an existing certificate on the NetScaler Virtual Appliance

- **Install Certificate**: It allows you to install an existing `.cer` or `.pfx` certificate file
- **Use Test Certificate**: It allows you to use a self-signed test certificate for testing purpose

In our case, we will be using **Use Test Certificate**.

2. In **Certificate FQDN**, enter the FQDN contained in the test certificate.
3. Click on **Continue**.




# Authentication settings

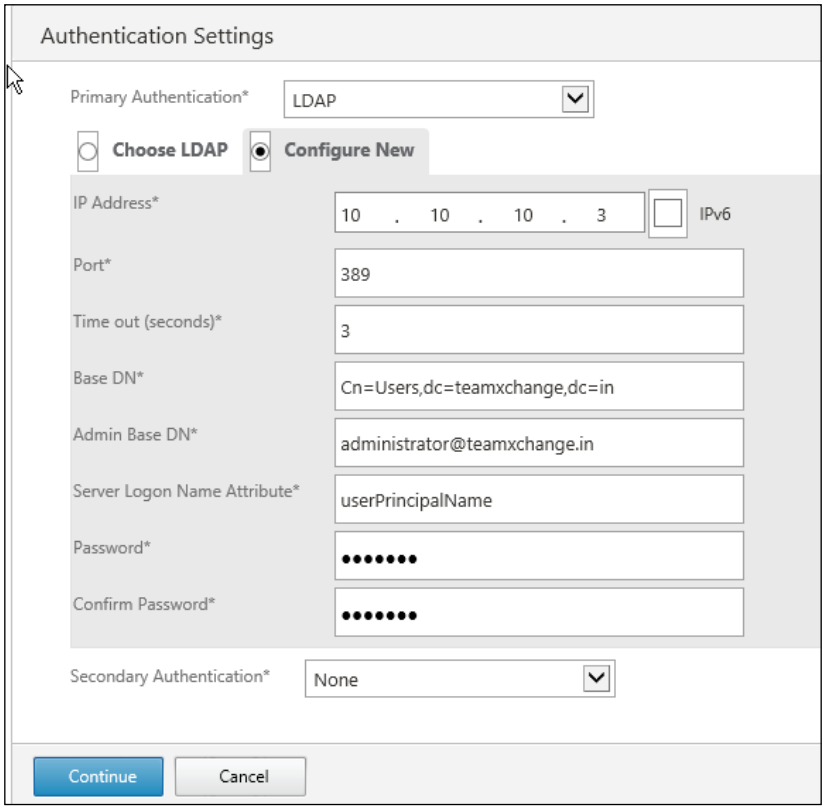
The NetScaler Gateway Authentication settings authenticate incoming user connections based on two types of authentication methods. They are as follows:

- **LDAP**: It's also known as **Lightweight Active Directory Protocol** and is based on the client-server model. It gives authenticated access to connected applications over an existing directory to connect or perform search-based operations. LDAP runs on port 389.
- **RADIUS**: It's also known as **Remote Authentication Dial-In User Service**, which is a networking protocol that provides centralized **Authentication, Authorization, and Accounting** (**AAA**) management for computers to connect and use a network service. RADIUS ports depend on their proprietary servers (for example, Microsoft RADIUS servers default to 1812 and 1813 ports).

NetScaler Gateway allows two-factor authentication; hence, both LDAP and RADIUS can be used. They can be assigned either as a Primary or Secondary Authentication method.

In our scenario, we will use LDAP authentication. Perform the following steps to assign the authentication settings:

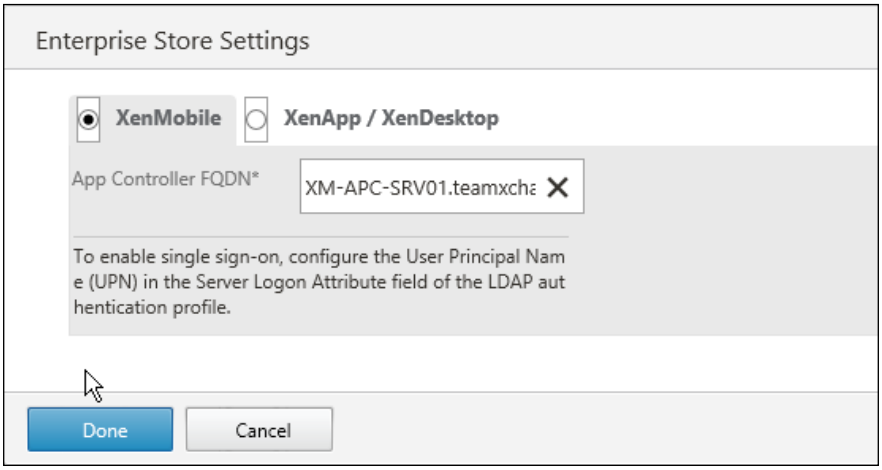
1. Choose **Configure New**.
2. Enter the IP address of the domain controller.
3. Enter port `389`.
4. Leave the **Time Out** setting as default.
5. Enter the **Base DN**, for example, `Cn=Users,dc=teamxchange,dc=in`.
6. Enter the complete ID for the LDAP Admin ID in **Admin Base DN**. For example, `administrator@teamxchange.in`.
7. Under **Server Logon Name Attribute**, type `userPrincipalName`. This will help us to later enable Single Sign-On for App Controller.
8. Type the password for the Admin ID mentioned above and retype to confirm.
9. Click on **Continue**.



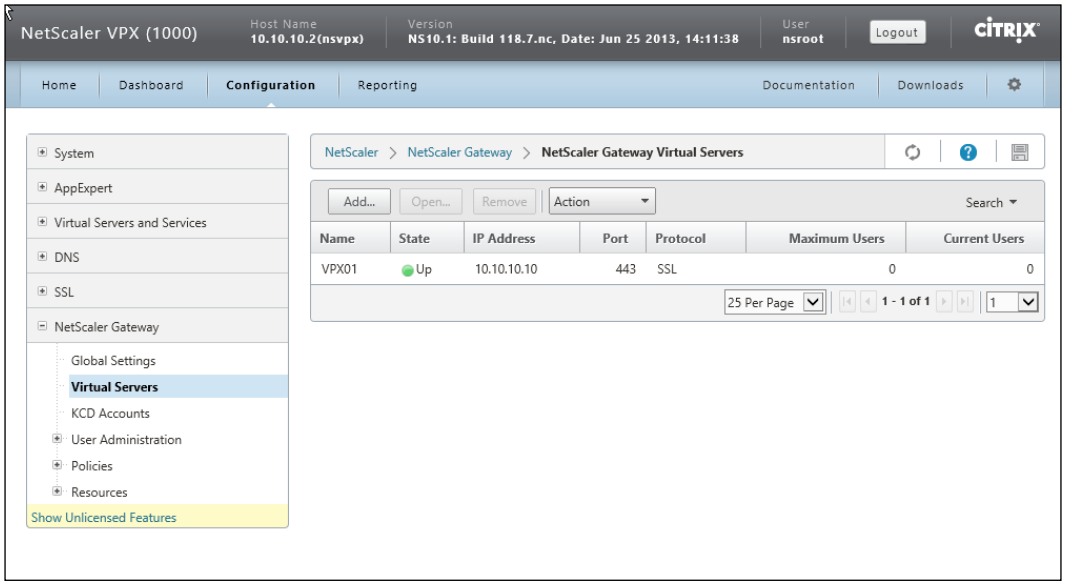
# Enterprise Store Settings

In this section, we will configure the NetScaler Gateway to communicate with the App Controller. Performing this configuration will allow NetScaler Gateway to support user access to web, mobile apps, SaaS, XenApp, or XenDesktop-based apps, and ShareFile through App Controller.

1. Choose **XenMobile**.
2. Type the **App Controller FQDN** (the full computer name of the App Controller Server). Note down this name as we will assign the same hostname to the App Controller Server while installation.
3. Click on **Done**.



To verify successful configuration of the NetScaler gateway, navigate to **Configuration | NetScaler Gateway | Virtual Servers** and ensure that **State** of the virtual server is **Up**.




# Summary

As discussed in this chapter, we have successfully installed and configured the NetScaler Gateway. Also, we have performed the initial configuration for the enterprise store, which will be further addressed while installing the App Controller server. In the upcoming chapter, we will install and configure the XenMobile Device Manager server.

# 4

# XenMobile™ Device Manager Deployment

**XenMobile Device Manager**, also known as **Zenprise Device Manager** before the acquisition of Zenprise by Citrix, is one of the industry's leading **Enterprise Mobility Management** (**EMM**) solutions. The Device Manager server is responsible for enrolling, deploying policies, application, and content management on mobile devices. The Device Manager server is also capable of extensive reporting, remote support, and a Self-help portal for end users. In this chapter, we will cover the following topics:

- XenMobile DM software download
- XenMobile DM installation
- Active Directory Integration

## Downloading the XenMobile™ DM software

In this section, we will download the XenMobile Device Manager software from the Citrix website. To download the XenMobile components; we need to follow these simple steps:

1. Go to the Citrix downloads portal that can be found at `http://www.citrix.com/downloads.html`.
2. Click on **My Account** and log in.

3. A Citrix account is mandatory to download any software from the Citrix download center. Register for a customer or a partner account at `https://www.citrix.com/welcome/create-account.html`.
4. Click on **Downloads**.
5. Select **XenMobile** as the **Product** and **Product Software** as the **Download Type** from the drop-down options.
6. Collapse **XenMobile** and click on **XenMobile MDM Edition**.
7. Download XenMobile Device Manager and its demo license that is available.

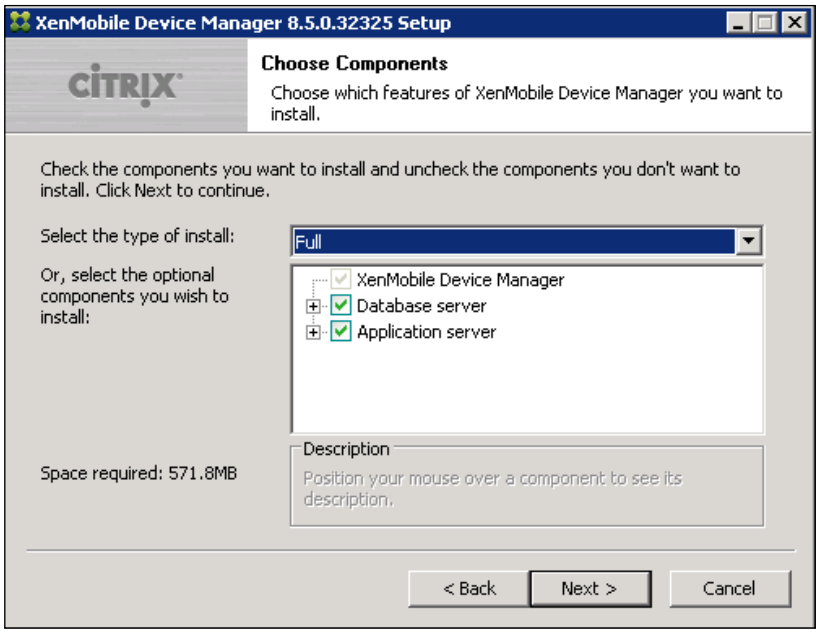
# Installing XenMobile™ DM

In this section, we will install the XenMobile DM software that we downloaded.

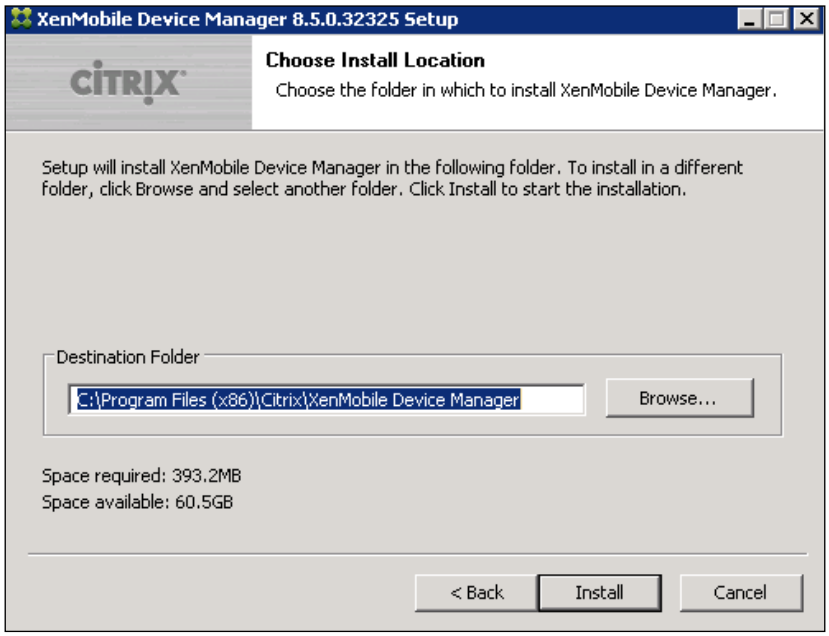
All prerequisites for XenMobile DM, as mentioned in *Chapter 2, XenMobile™ Solution Deployment Prerequisites*, should be met before installing the software.

Now, let's go ahead and start the software installation:

1. Double-click on the `.exe` file we downloaded.
2. Select the desired language at the **Installer Language** prompt.
3. Click on **Next** to proceed.
4. Click on **I Agree** on the License Agreement popup.
5. On the **Choose Components** screen, we can choose the components to be installed. The XenMobile DM has the PostgreSQL database server bundled with the software, which should be used only for testing or demonstration purposes (as per Citrix). Citrix suggests using Microsoft SQL server in production environments. In our demo, we will be using the PostgreSQL database server:




6. Click on **Next**.
7. Under **Choose Install Location**, we will define the folder for the Device Manager installation. Then, click on **Install**:

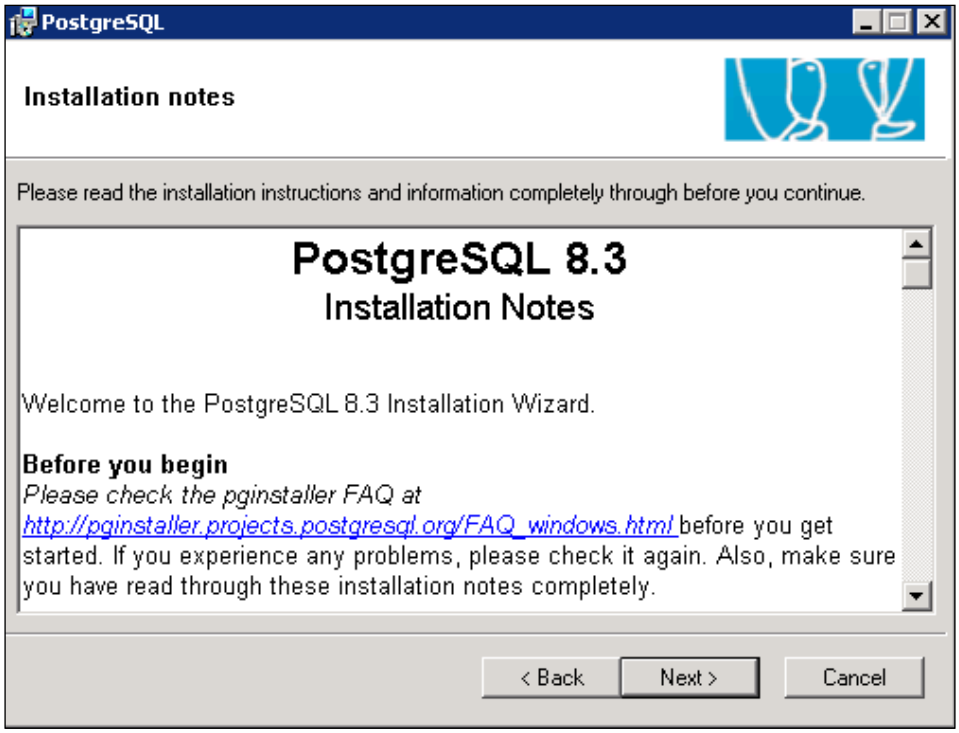


8. After this, the installation will start. We can click on the **Show details** button to see the installation process.

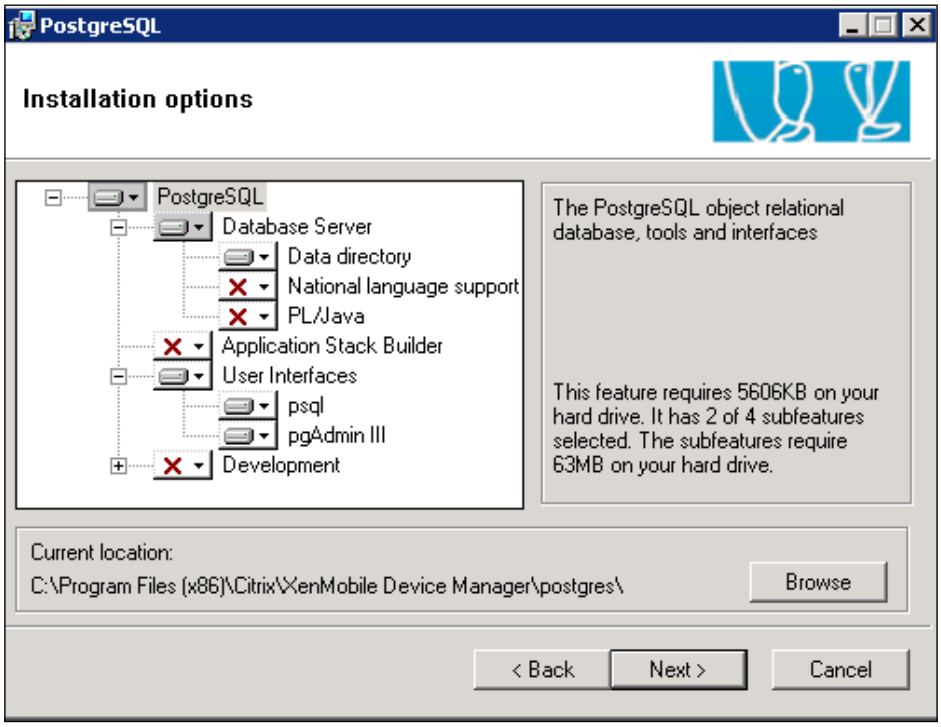
# Installing the XenMobile™ DM database

In this section, the installer leads us to the installation of the database for the XenMobile Device Manager. The steps are as follows:

1. The **PostgreSQL** page marks the beginning of the database server installation procedure. In this section, we will install the various database services required by the XenMobile DM. Now, click on **Next**.
2. The **Installation Notes** section has instructions and information regarding PostgreSQL. Then, click on **Next**:



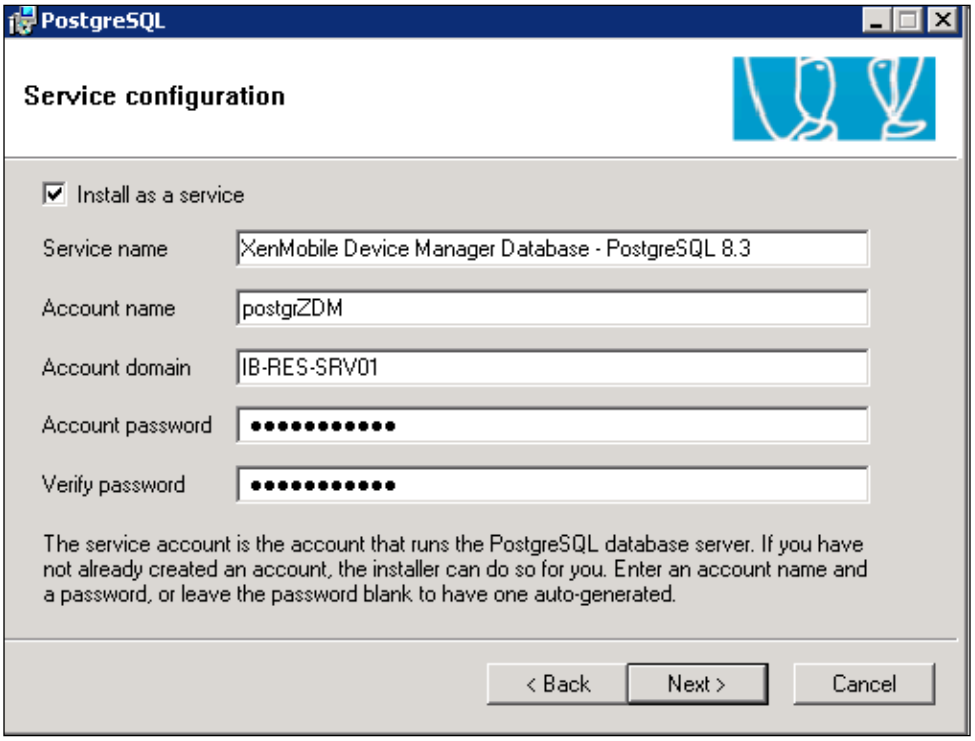
3. The **Installation options** section lists out the PostgreSQL components that we can choose to install. We can use the default selection as it contains all the components that will make the XenMobile DM server work fine. We can also select the **PostgreSQL** install folder on this screen. In our scenario, we will go ahead with the default settings. Then, click on **Next**.




4. The **Service configuration** panel sets up a service and the service account for the PostgreSQL server. This section is divided into multiple sections as follows:
    - **Install as a service**: This is autoselected. Check this box to install the XenMobile DM Database Service.
    - **Service name**: This is the field with the name of the XenMobile DM database service. This section is autopopulated.

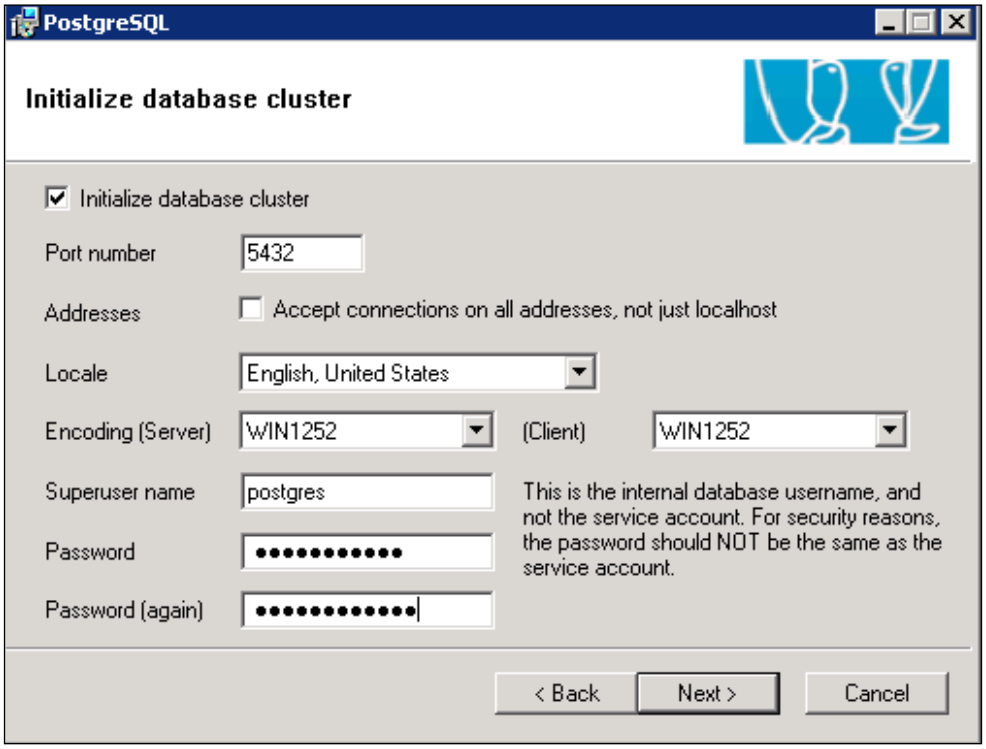
- **Account name**: This is the field with the account responsible for running the database server. This section is autopopulated.
- **Account domain**: This is the field where we enter the domain name (for example, `teamxchange.in`) or the hostname (for example, `TX-XDM-SRV01`) if the system is in a workgroup.

5. After entering the desired settings, click on **Next**.



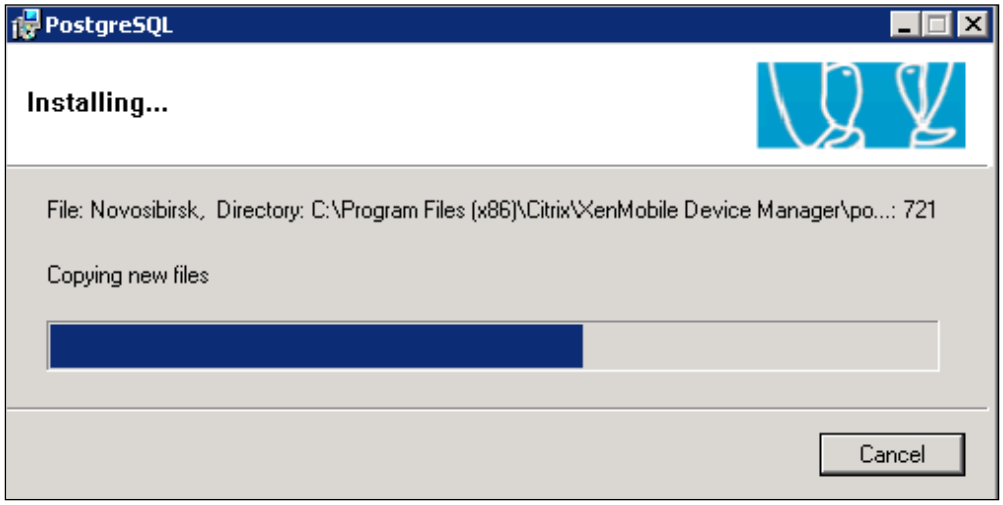

6. The **Initialize database cluster** section creates the internal PostgreSQL database user. It is mostly autopopulated; just enter the password to verify and click on **Next**.

Keep a note of all the usernames and passwords as they come in handy while troubleshooting or other database-related activities. The user created by the database is independent of the service user.

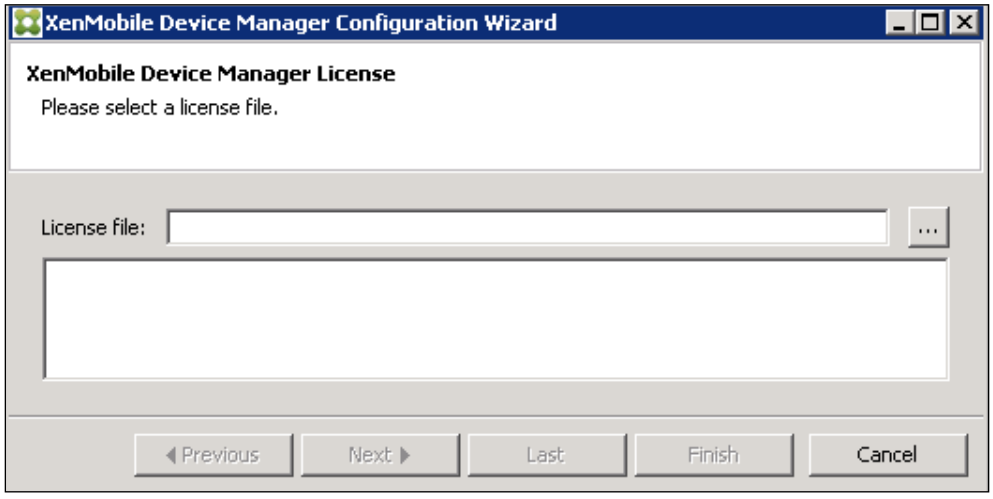



7. On **Enable procedural languages**, click on **Next**.
8. On **Enable contrib modules**, ensure **Adminpack** is selected and then click on **Next**.

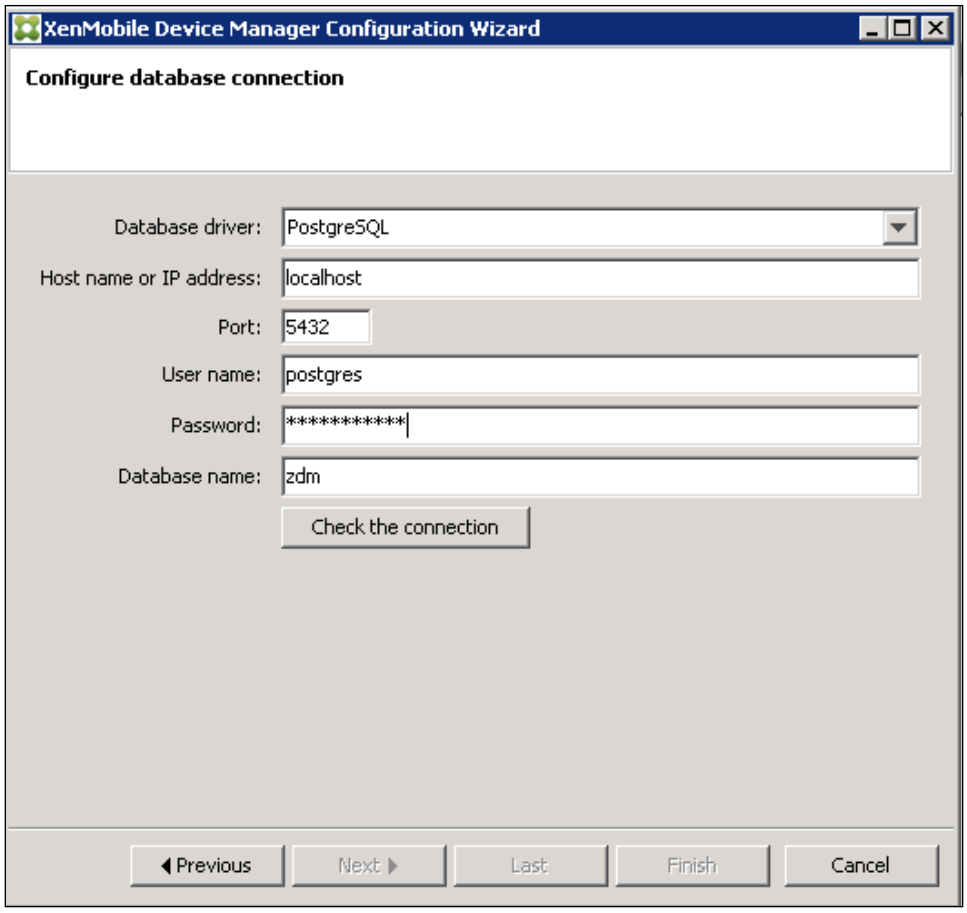
9. When we click on **Next**, the database installation will continue and the installation progress screen should appear as shown in the following screenshot:



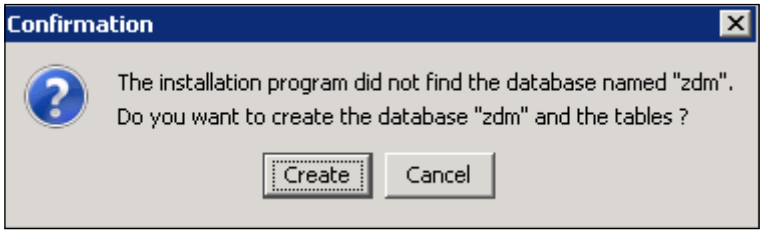

10. Once the installation is completed, we will be greeted with the **Congratulations** page. Click on **Finish**.
11. Now we will add the XenMobile DM license to use all the features and functionalities in the software. Upload the license file (`.crt` format) and click on **Next**.



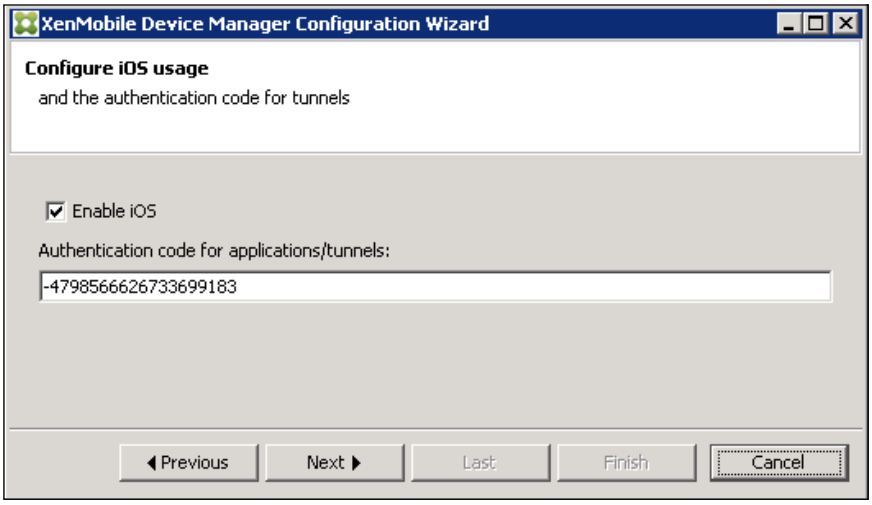
12. The **Configure database connection** section connects the PostgreSQL Database super user created earlier with the Device Manager. All the fields are autopopulated except the password we chose for the super user. After entering the password, click on **Check the connection**:




13. Once successfully connected, click on **OK** and it will prompt you to create a database named `zdm`. Then, click on **Create**.



14. On the **Configure iOS usage** screen, you can choose support for iOS devices. If you keep this option unchecked, you need to reinstall the Device Manager server to enable support for iOS devices:




15. Keep a note of the authentication code that is provided here, as we will require it while setting up remote tunnels for iOS devices. In the next section of this installation, we will be setting up the XenMobile connectors and certificates.

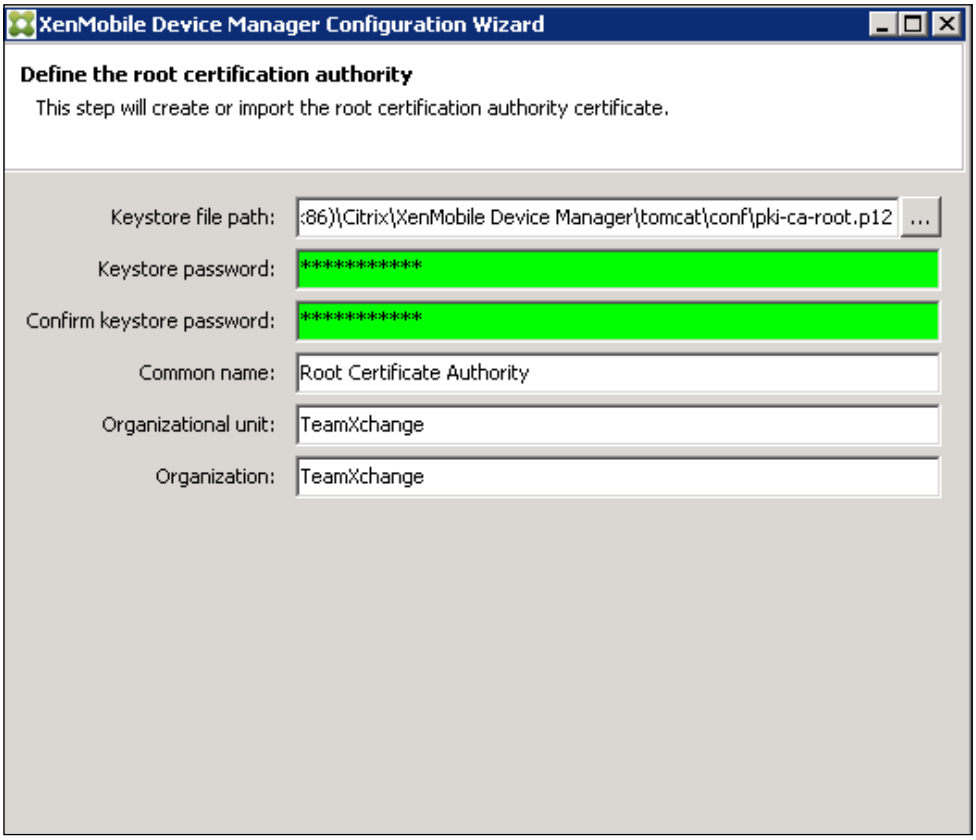
# Configuring XenMobile™ connector and certificate

In this section, we need to configure the server connectors. The XenMobile DM works on connectors to communicate between the Device Manager Agent and the Device Manager Server. The connectors are as follows:

- **HTTP Connector**: This allows unsecure connections over port 80
- **HTTPS Connector (certificate-based)**: This allows secure connections over port 443 with a certificate
- **HTTPS Connector**: This allows a secure connection over port 8443 and is used for device enrollment

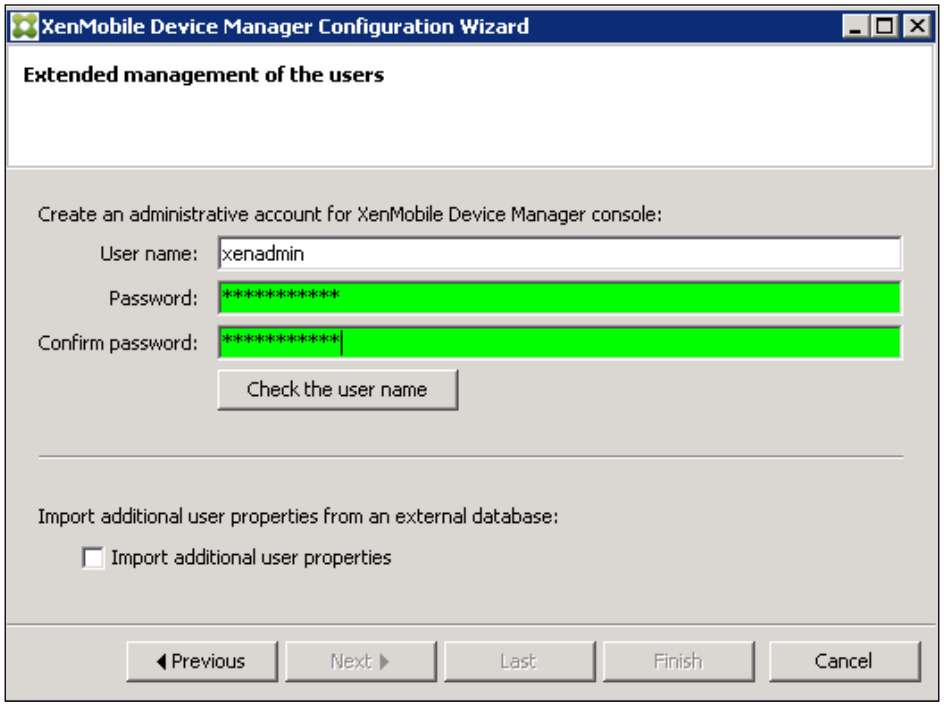
Once the server connectors are done, we perform the following steps:

1. We need to upload the Root, Server, and the APNS certificates. An APNS certificate is a must to support iOS devices; the reference for this has been provided in *Chapter 2, XenMobile™ Solution Deployment Prerequisites*. If there are no existing Root or Server certificates, enter the desired password and click on **Next**. The session will automatically create one for future reference:

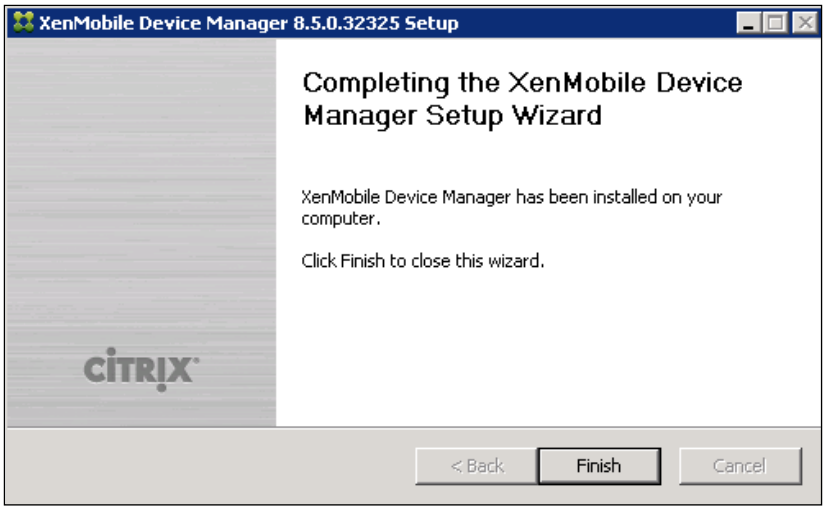



2. In the next section, we can define a range of ports used for **Remote Support**. In our scenario, we will go with the default option of 8081. **Remote Support** allows admins to remotely control devices and perform specific tasks on the device.

3. Enter a **User name** and **Password** for the XenMobile Device Manager admin console. The credentials entered here will be used to manage the XenMobile admin console.




4. Click on **Finish** and reboot the server:



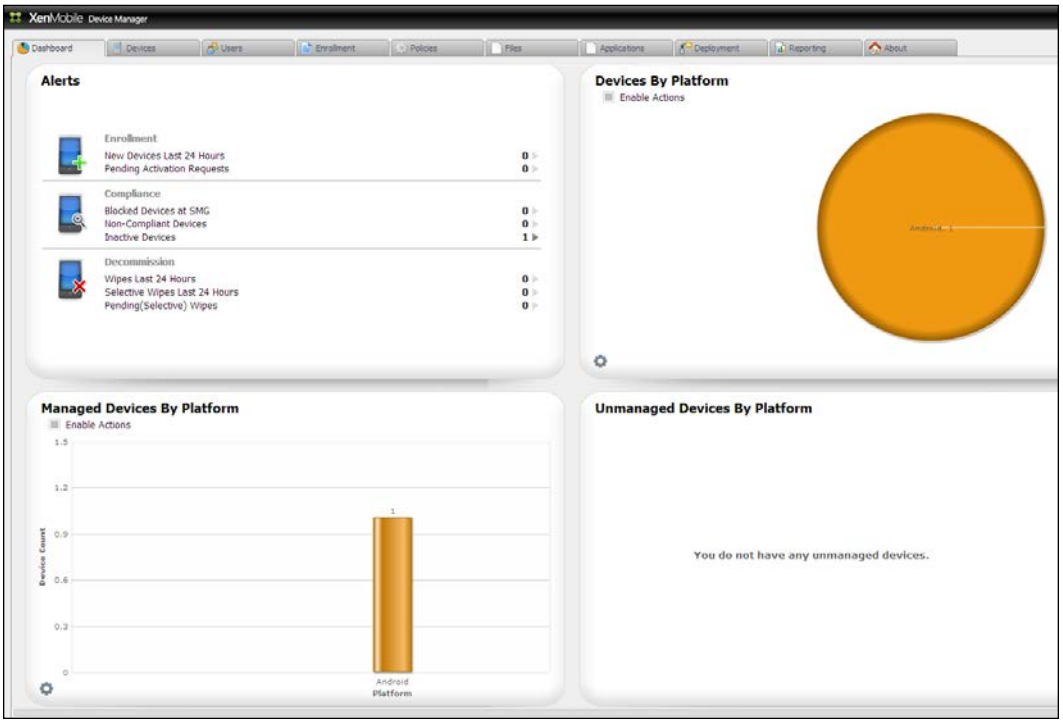
# The XenMobile™ Device Manager admin console

Once the server is up, we will open up the browser and try to access the XenMobile Device Manager administrative console. Type `https://ipaddress: 8443 /zdm` for example, `https://10.10.10.1:8443/zdm`. This should open up the XenMobile Device Manager console as shown in the following screenshot:


Log on to the admin console with the username and password set during the installation stage. The XenMobile Device Manager section is divided into 10 tabs for performing various activities as described in the following points:

- **Dashboard**: This tab gives you an overview of all the devices enrolled to the DM server based on their platform, which may be iOS, Android, Symbian, or Windows.
- **Devices**: This tab gives out detailed information regarding the devices enrolled. It also displays information about the user groups to which these enrolled devices belong to.
- **Users**: This tab has information regarding the XenMobile users and their respective roles such as administrator, user, support, or any other custom role.
- **Enrollment**: This tab has options to send device enrollment invitations and the MDM client installation link, which can be sent to users via e-mail or SMS.

- **Policies**: This tab has various policies that can be applied to enrolled devices. It also has remote support tunneling options and SharePoint integration options to enable Mobile Content Management.
- **Files**: This tab is used to share files with the enrolled devices. We can also set read-only or hidden attributes on these files.
- **Applications**: This tab is used to deploy iOS or Android-based apps to the enrolled devices. These apps can be either internal (Enterprise Apps) or external (Play Store) apps.
- **Deployment**: This tab can be used to deploy packages containing policies, files, or applications to enrolled devices. These packages can be automated, for example, to deploy a set of policies as soon as a device is enrolled.
- **Reporting**: This tab contains various reports based on devices or applications, which can be generated to ensure a proper inventory.
- **About**: This section has details regarding the XenMobile DM server and its build. It also contains Device Manager License and APNS certificate information, which can be updated from here when required.



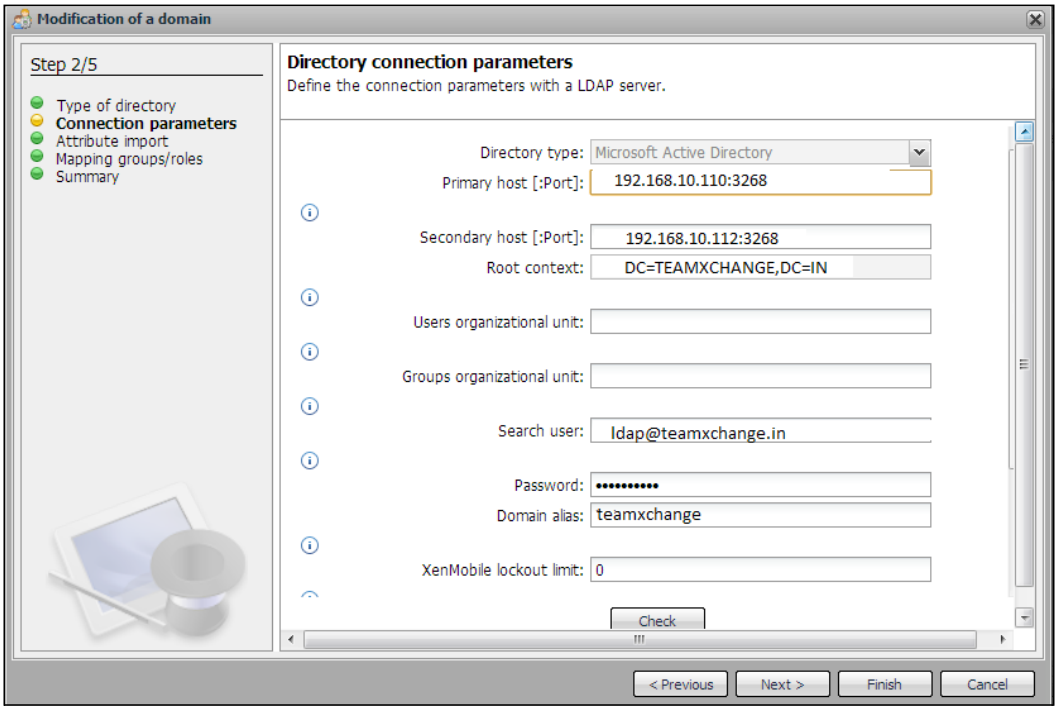
# Integrating Active Directory

When we integrate XenMobile DM with Active Directory, it allows us to manage multiple users belonging to the same Active Directory group using the Device Manager. Integration with Active Directory enables users to enroll their devices using their Domain-based ID's and passwords. The XenMobile Device Manager server polls with the AD server using the LDAP protocol to check with the users and their passwords. The steps to integrate Active Directory are as follows:

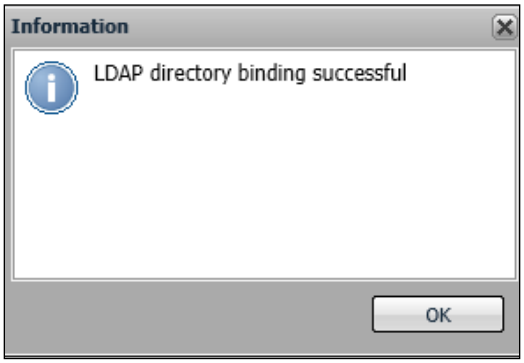
1. Log on to Device Manager admin console.
2. Click on **Options** and select **LDAP Configuration**.
3. Click on **New** and select **LDAP**.
4. The integration page has some parameters that have to be defined to enable LDAP authentication. The parameters are as follows:
    - **Directory type**: This field lets you to choose the type of directory used, for example, Microsoft Active Directory or others.
    - **Primary host [:Port]**: This field lets you mention the IP address of the primary LDAP server (or Domain Controller) and the LDAP port (389/636/3268) being used. For example, `192.168.10.110:3268`.
    - **Secondary host [:Port]**: This field lets you mention the IP address of the secondary LDAP server and the LDAP port (389/636/3268) being used.
    - **Root context**: This is the distinguished name of the domain. For example, for the domain `teamxchange`, the alias will be `DC=TEAMXCHANGE,DC=IN`.
    - **Users organization unit**: This is the Active Directory OU to which the LDAP user belongs. This is an optional parameter.
    - **Groups organizational unit**: This is the Active Directory group to which the LDAP user belongs. This is an optional parameter.
    - **Search user**: This field lets you enter the complete username of the LDAP search user. For example, `ldap@teamxchange.com`. It is advisable to create a separate user for LDAP search purposes.
    - **Domain alias**: This is the alias for the LDAP users' domain. For example, for the domain `teamxchange.in`, the alias will be `teamxchange`.

- **XenMobile lockout limit**: This parameter defines the number of failed attempts allowed to any user after which access to LDAP will be locked.

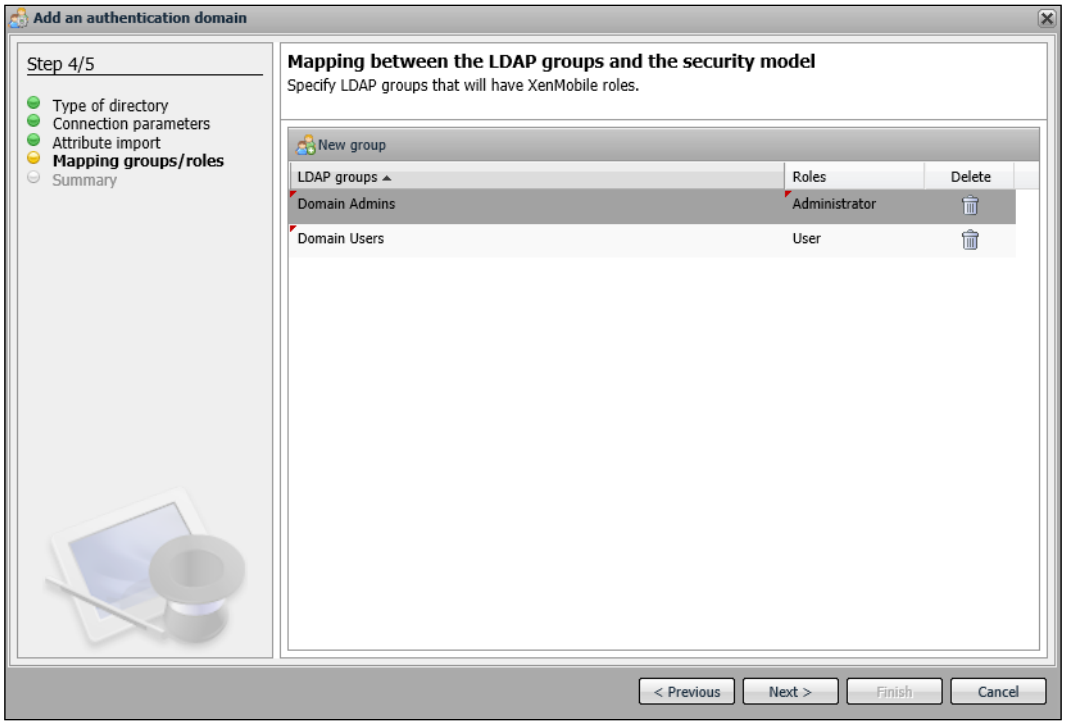
5. Kindly add the desired settings in the **Directory connection parameters** section as shown in the following screenshot:




6. After entering all the required parameters, we need to click on **Check**. If the information provided is correct, it should give the following prompt:



7. Click on **OK** and then click on **Next** on the **LDAP attributes import** page.
8. On the LDAP group and the **Security Model Mapping** page, you can choose which users have access to XenMobile and the users who have admin rights on the admin console. For example, **Domain Admin** can have **Administrator** roles and **Domain Users** can be given **User** roles; alternatively, we can keep the default settings. Then, click on **Next**:




9. On the **Summary** page, we have the summary of all the settings that will be applied once we click on **Finish**.

# Summary

As discussed in this chapter, we have successfully installed and configured the XenMobile Device Manager. Also, we learned the various settings for the XenMobile Console and the Active Directory integration procedure.

In the next chapter, we will be installing the **App Controller** server, which helps to deliver access to the Web, SaaS, and mobile-based applications.

# 5

# XenMobile™ App Controller Deployment

The **XenMobile App Controller** delivers web-, SaaS-, Android-, and iOS-based apps, and ShareFile-integrated data and documents to end users. App Controller uses either Citrix Receiver or Receiver for the Web available in Worx Home to deliver these resources. This chapter will help you learn and understand the following topics:

- Downloading XenMobile App Controller
- Importing the virtual appliance
- Configuring XenMobile App Contoller
- Configuring certificates
- Configuring App Controller with NetScaler Gateway
- Configuring App Controller and Device Manager

## Downloading XenMobile™ App Controller

In this section, we will download the XenMobile App Controller software from the Citrix Web Portal. To download the XenMobile components, we need to go to the Citrix **Downloads** portal, which can be found at `http://www.citrix.com/downloads.html`. To download the XenMobile App Controller, perform the following steps:

1. Click on **My Account** and log in.
2. Click on **Downloads**.

3. Select **XenMobile** as the **Product** and **Product Software** as the **Download Type**. Click on **Find**.
4. Click on **XenMobile 8.6 App Edition** from the list.
5. Download the appropriate App Controller virtual image to install on XenServer, VMware, or Hyper-V (in our case, we will be using VMware).

# Importing the virtual appliance

After we have successfully downloaded the XenMobile App Controller build, we need to import it to the hypervisor. In case of VMware-based hypervisor, you should have the file named `App Controller_2.8.0.162000.vmware.ova`, available after download.

The steps to import the software into the hypervisor are as follows:

1. Log in to the VMware VSphere client.
2. Click on **File** and then choose **Deploy OVF Template**.
3. Click on **Browse** and locate the file `App Controller_2.8.0.162000.vmware.ova`.
4. Click on **Open** and then select **Next**. Agree to accept the terms of the licenses and click on **Next**.
5. Enter a **Name** for the virtual machine and click on **Next**.
6. Select a **Datastore** value to store the Deployed OVF template and click on **Next**.
7. Choose the **Network Adapter** you want to allot to the virtual machine and click on **Next**.
8. Verify the information and click on **Finish**. The OVF Deployment progress bar should appear.

Once the import procedure is completed, the XenMobile App Controller appliance should appear on the VSphere client. This completes the import procedure for the virtual appliance.

# Configuring XenMobile™ App Controller

In this section, we will configure the virtual appliance that we imported into the Hypervisor in the last section. The XenMobile App Controller comes preconfigured with some default settings for management purposes, listed as follows:

| Default | Value |
|---|---|
| IP address | 10.20.30.40 |
| Subnet Mask | 255.255.0.0 |
| Root Username | `Administrator` |
| Root Password | `password` |

To proceed further, we need to ensure we have the following details in hand:

- **XenMobile App Controller IP Address**: The XenMobile App Controller IP address is used for managing the App Controller virtual appliance. Reserve a static IP address to be assigned to the XenMobile App Controller virtual appliance.
- **Netmask**: The subnet mask of the IP address assigned to XenMobile App Controller virtual appliance.
- **Default Gateway:** A **Default Gateway**: It passes traffic from local subnets to devices on different subnets. It helps in managing the XenMobile App Controller from devices that belong to a different subnet. Write down the Default Gateway for the IP address assigned to the XenMobile App Controller virtual appliance.

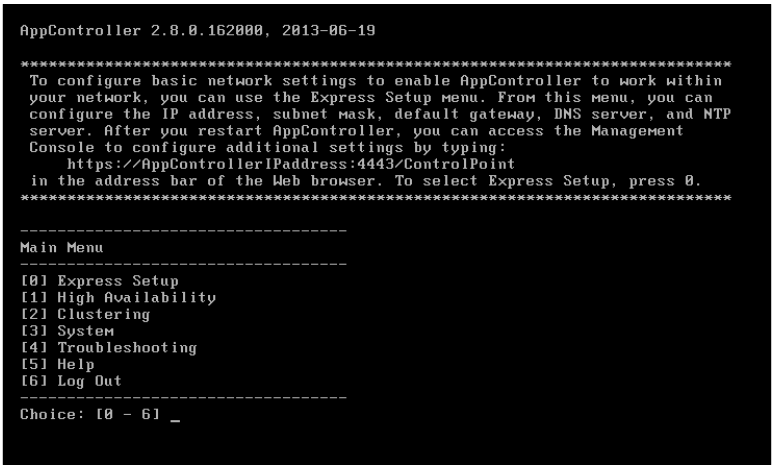
Now, let's proceed with the configuration of the XenMobile App Controller virtual appliance.

# Command-line-based configuration

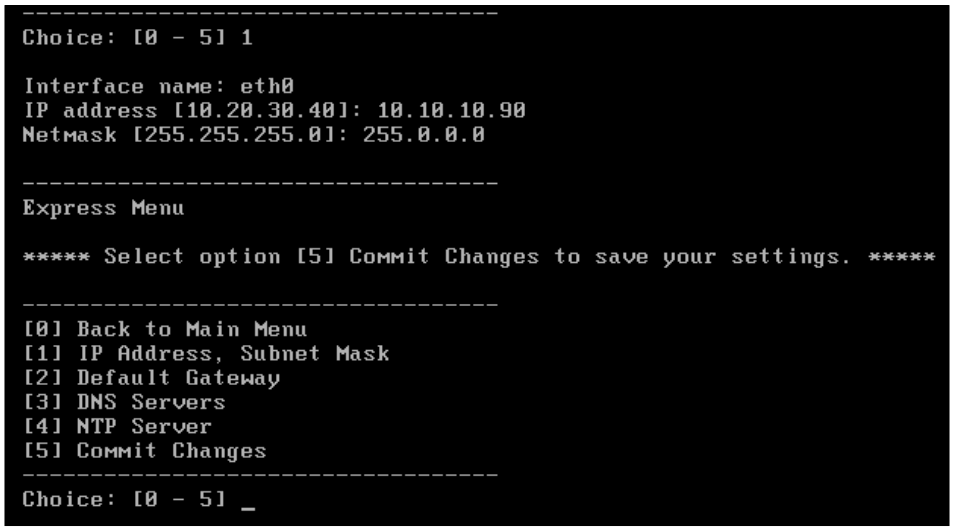
We can use the command line to configure the App Controller on a basic level by assigning the server an IP address, subnet mask, and its DNS server. The steps to configure the App Controller server through the command line are as follows:

1. Power on the virtual appliance (The installation of the XenMobile App Controller is automatically done as soon as you power on the virtual machine.) Refer to the following screenshot:

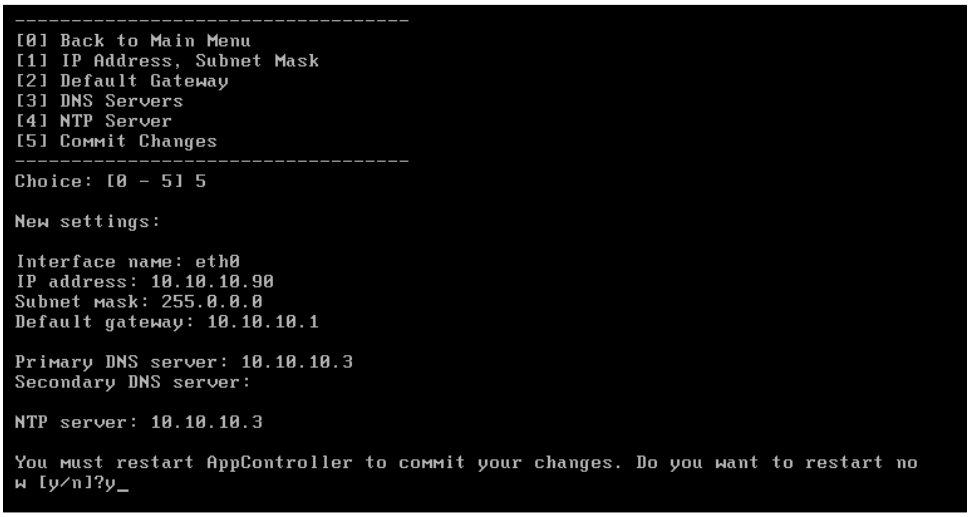

2. At the **Login** prompt, enter the default credentials as mentioned in the preceding table.
3. After a successful log in, we should be greeted with the following screenshot:



4. Press *0* for **Express Setup**.




5. Now, press *1* for **IP Address, Subnet Mask**.
6. Similarly, select options **2**, **3**, and **4** for **Default Gateway**, **DNS Servers**, and **NTP Server**, respectively.
7. Select option **5** to **Commit Changes** and press *Y* to reboot the server.

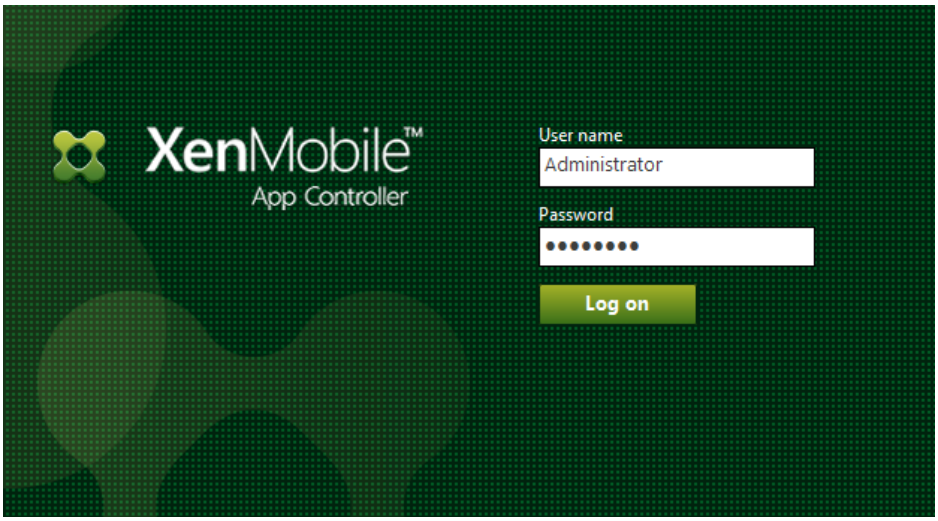



Once the server boots up, you can log on to the App Controller web console from a system in the same subnet.

# Graphical user interface-based configuration

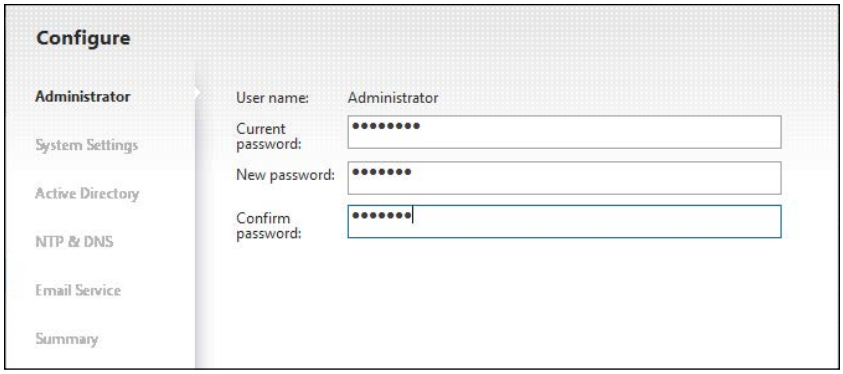
In this section, we will configure detailed settings on the XenMobile App Controller server using a graphical user interface. To do so, perform the following steps:

1. Log on to a system in the same subnet as the App Controller server and open a web browser pointing to `https://ipaddress.of.App controller:4443/controlpoint` (for example, `https://10.10.10.90:4443/controlpoint`)
2. Enter the default **Username** and **Password** (refer to the preceding default table):

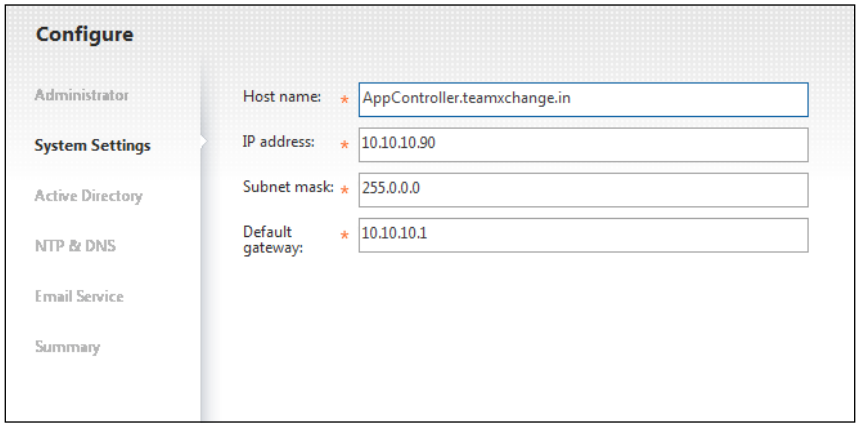


After logging in, the next screen requires the following additional configuration:

- Configure the **Administrator** password: Change the default password here:



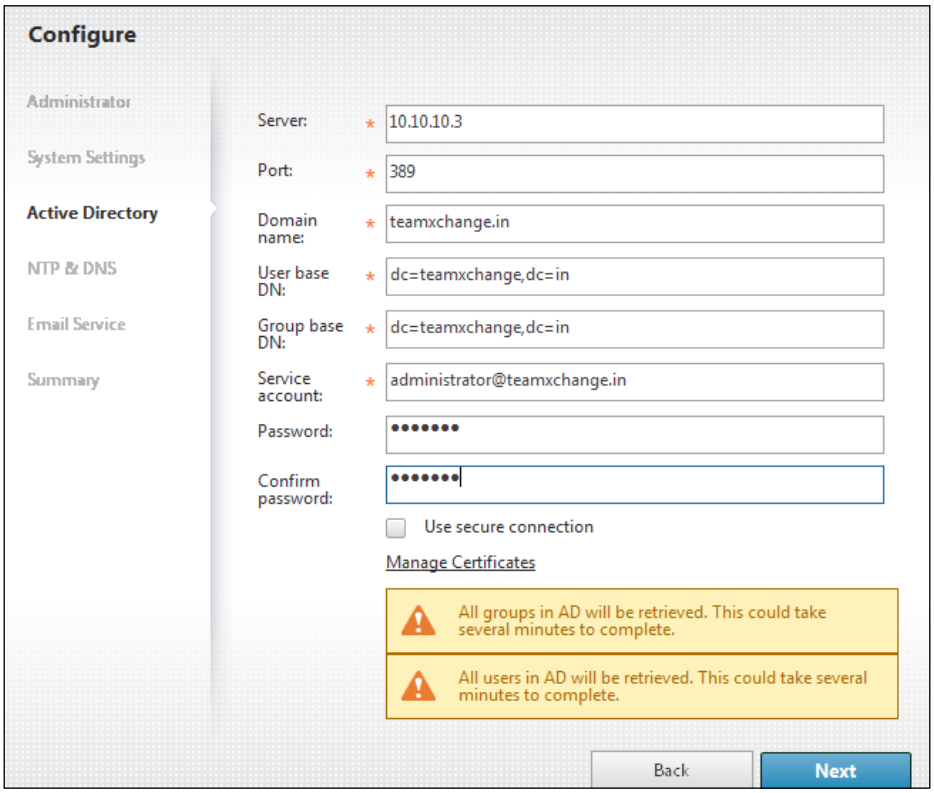

- Configure **System Settings**: Here, we can change the settings we made while in the command-line interface:



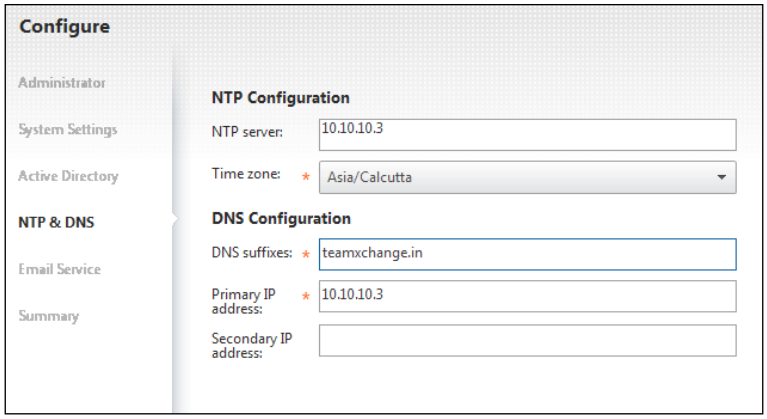

- The **Active Directory** integration: Here, we will have to enter in Active Directory settings to integrate App Controller with LDAP.

It's recommended to create a separate service account for App Controller and also for other XenMobile components.

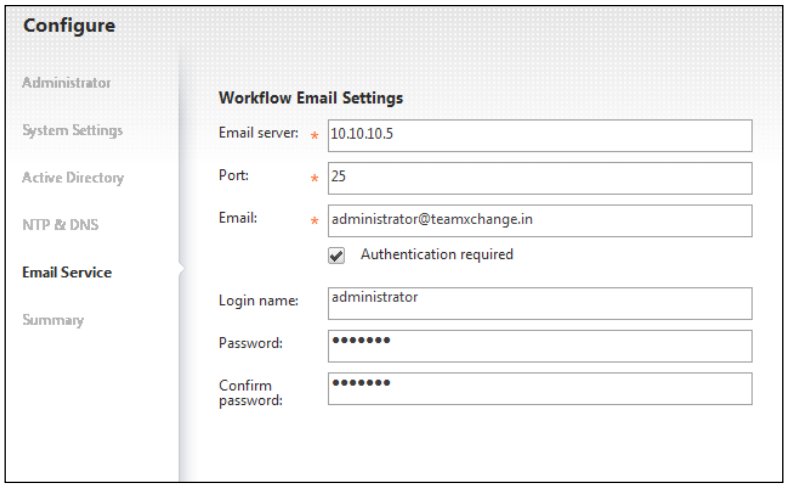
The following screenshot consists of the **Active Directory** integration settings:



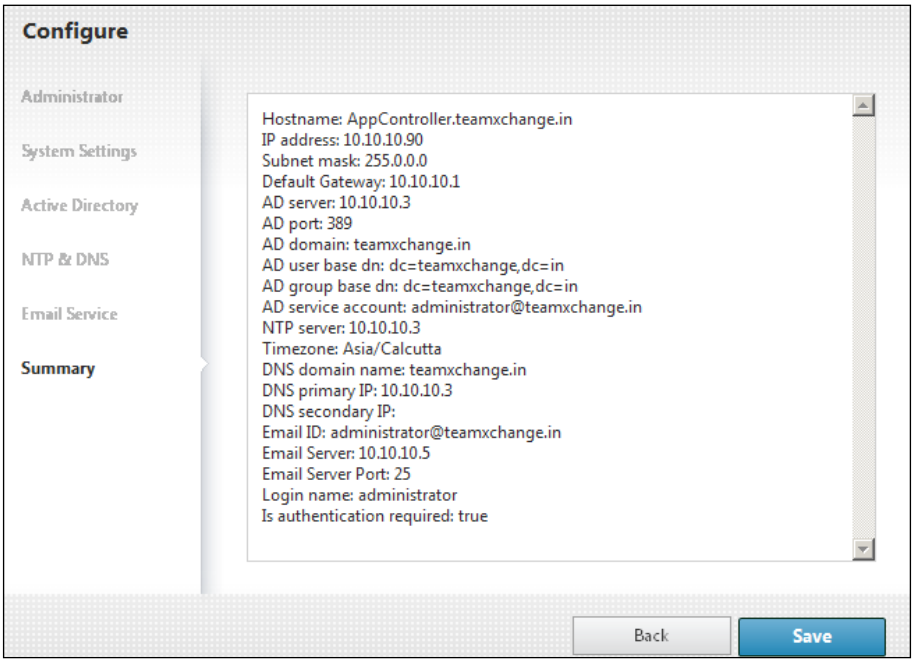

- **NTP & DNS** configuration: In this section, we will configure the Network Time Protocol server and the Domain Name System server.
  In our case, we have taken our DC to be the NTP server:



- **Email Service** settings: In this section, we will enter in the settings for our Mail Server and provide credentials for a user who will receive workflow notifications. Workflows are used to manage the creation and removal of user accounts:




3. Once we have entered all the aforementioned settings, we can verify them on the **Summary** screen shown as follows and finally, click on **Save**:



4. Once we click on **Save**, we will get a prompt to log off for changes to take effect. Click on **Yes**. Once done, you can re-log on with the new password.

# Configuring certificates

App Controller requires certificates to ensure secure communication with the App Controller Management console applications and StoreFront. There are three SSL certificates that are required by the App Controller server for communicating with the Management console and StoreFront. These SSL certificates are used for user account-management, and SAML-based applications.

The SSL certificates need to be signed by a certificate authority such as VeriSign and Entrust, and then uploaded to the App Controller server.

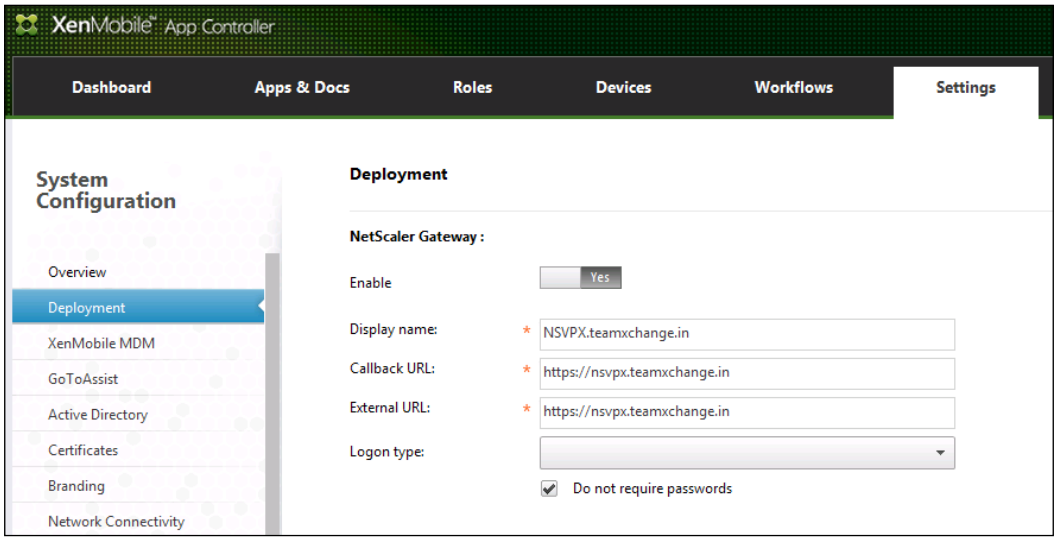
1. Log in to the App Controller Management console and click on the **Settings** tab.
2. Go to **System Configuration** and then select **Certificates**.
3. Click on **Import** and then select **Server (.pem)** for a root CA-signed server certificate or **Trusted (.pem)** to import a CA-signed root certificate.
4. In the **Upload** section, select **Browse**, navigate to the certificate, and click on **Open**.
5. Once we have added the certificate, click on **Make Active**. This will log us out from the console. We need to log back in; the new certificate should be successfully added now.

# Configuring App Controller with NetScaler® Gateway

We have seen many applications that are internal to an organization. Sometimes, users connect to these applications from the Internet. In this case, we can publish such an app in the App Controller and route the connections of the app to the end user device through NetScaler Gateway. This will in turn provide us with secure access control management and granular application and data-level controls. For this, we need to set up trust settings between the App Controller and the NetScaler Gateway. In this section, we will learn to set up this trust between these two XenMobile components. To configure App Controller with NetScaler Gateway, perform the following steps:

1. Log in to the App Controller Management console and click on **Settings**.
2. Go to **System Configuration** and select **Deployment**.

3. Select **NetScaler Gateway** and click on **Edit**.
4. Under the **Enable** section, select **Yes**.
5. Under **Display Name**, enter the NetScaler Gateway server name.
6. Under **Callback URL** and the **External URL**, type the NetScaler Gateway web address. For example, `https://nsvpx.teamxchange.in` or `https://nsvpx.teamxchange.in:443`.



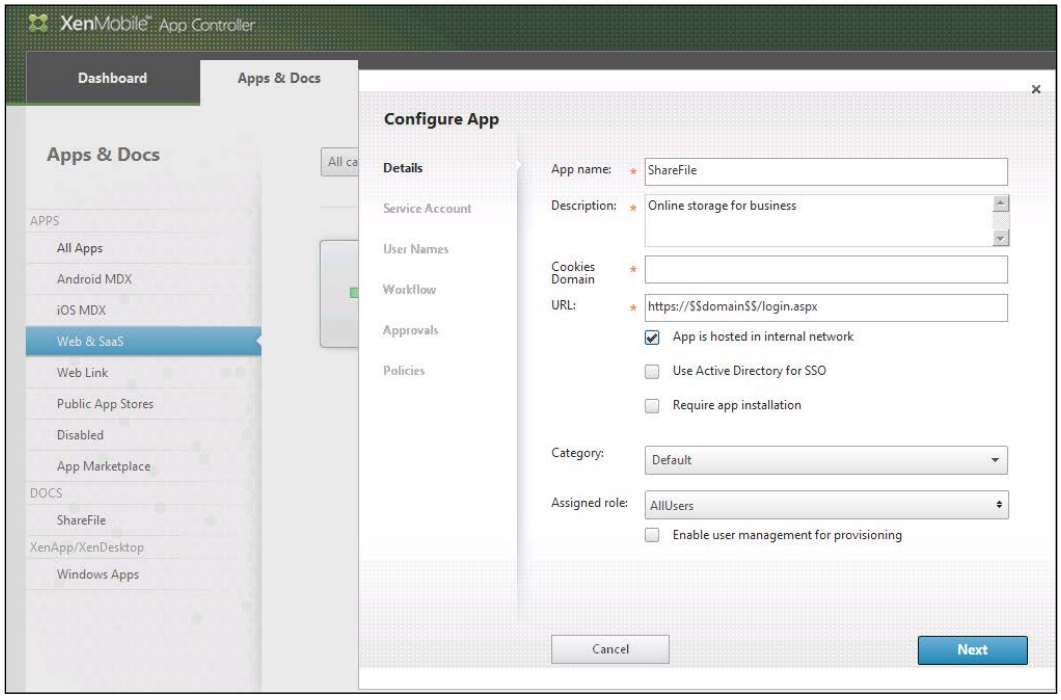

7. We can also configure the following optional **Logon type** for users when accessing applications through NetScaler Gateway:
    - **Domain only**: Users need to use their Active Directory credentials
    - **Security token only**: Users need to enter security token-based codes for authentication
    - **Domain and security token**: Users in this logon type need to enter their AD credentials and security token codes

8. We can also check **Do not require passwords** to disable any password policy.
9. Click on **Save**

# Publishing access to an app through NetScaler® Gateway

In order to allow an app to use NetScaler Gateway connection for access management, you need to perform the following steps:

1. Log on to the App Controller web console.
2. Navigate to **App & Docs** and then the application type (web, SaaS, Android or iOS). For demonstration purposes, we will be using a Web & SaaS app.
3. Click on **Web & SaaS** and then click on the **+** icon to select an app.
4. Check the box beside **App is hosted in internal network** to use the NetScaler Gateway connection.
5. Further, we can configure the app as per our requirement, and click on **Save** for the settings to take effect.



# Configuring App Controller and Device Manager

In this section, we will configure the App Controller to communicate with the Device Manager. In order to ensure the communication between both the components is secure, Citrix recommends to install a publically trusted certificate on both the components as communication can be initiated from either App Controller or the Device Manager, where it first tries to validate the certificate installed. The communication handshake will fail if either of the components is unable to validate the certificate installed on the other one.

## Configuring Device Manager

The XenMobile Device Manager configuration will allow the server to communicate with the App Controller server. To do so, perform the following steps:

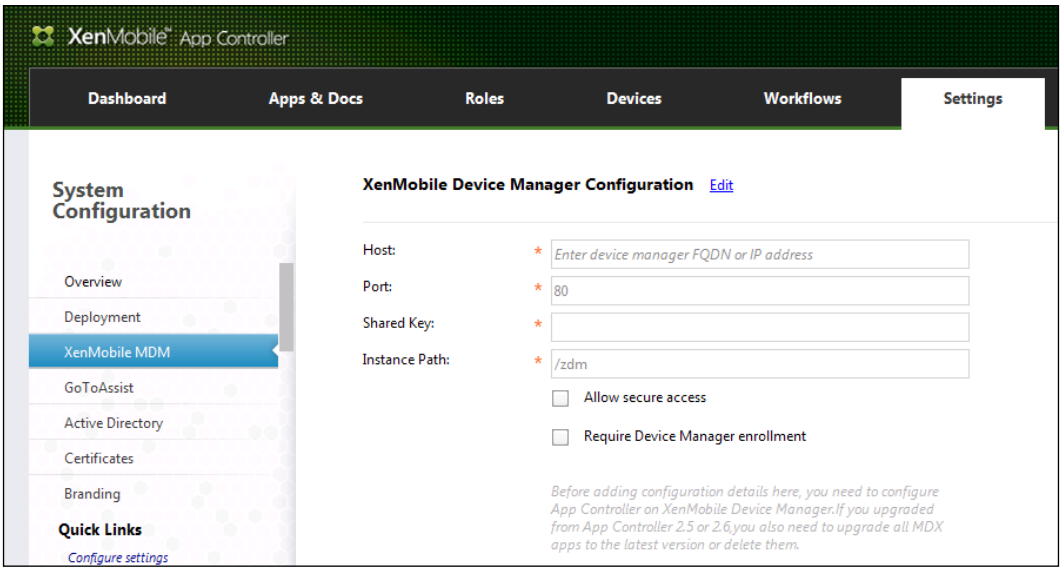
1. Log on to the XenMobile Device Manager web console.
2. Go to **Options** and select **Modules Configuration**.
3. Go to **AppC Webservice API**.
4. Enter **Hostname** of the App Controller server and **Shared Key** (a password), which we will also enter in App Controller server to authenticate.
5. Check the box for `Enable App Controller`.
6. At this point, we are half way done with configuration. Click on **Check the Connection**; we should receive an error as the configuration on the App Controller server needs to be completed before testing the connection.
7. Click on **Close** and select **Yes** to save the modifications.

## Configuring App Controller

The App Controller configuration will allow the server to communicate with the XenMobile Device Manager server.

1. Log on to the App Controller server and navigate to the **Settings** tab.

2. Select **XenMobile MDM** and click on **Edit** on the **Settings** section.




Fill the following section:

- **Host**: Type the hostname or the FQDN of the XenMobile DM server.
- **Port**: Leave it set to the default port as: `80`.
- **Shared Key**: Enter the shared key that we entered while configuring the Device Manage server.
- **Allow secure access**: If selected, communications between both the components will default to secure port 443. We will leave this option unchecked in our scenario.
- **Require Device Manager enrollment**: If selected, then all devices need to be enrolled and managed by the Device Manager server. We will leave this option unchecked in our scenario

3. Once we have entered these settings, we will click on **Test Connection** and should get the **Connection was successful** prompt if the settings were entered correctly.
4. Click on **Close** and hit **Save**.

Now, we will go back to the Device Manager console and hit **Check the Connection**; it should successfully communicate with the App Controller server.

# Summary

As discussed in this chapter, we have successfully installed the App Controller server and integrated it with XenMobile Device Manager and NetScaler Gateway to ensure a secure communication. We also configured certificates and integrated Active Directory and the e-mail server with the App Controller server.

In the next chapter, we will learn how to manage applications with the XenMobile Device Manager and App Controller.

# 6

# XenMobile™ Remote Support

**Remote Support** is one of the most sought-after features when it comes to MDM solutions. The Remote Support feature allows admins to remotely control and monitor enrolled devices and perform specific tasks. In this chapter, we will learn how to set up XenMobile Remote Support and control enrolled devices. The topics covered in this chapter are as follows:

- Installation prerequisites
- Installation of a Remote Support application
- Adding the Device Manager connection

## Installation prerequisites

It's necessary that all installation prerequisites be met before proceeding with the installation. In this section, we will list the system prerequisites for installing the XenMobile Remote Support application.

For a list of XenMobile Remote Support functionality, kindly refer to the document at `http://support.citrix.com/proddocs/topic/cloudgateway/xmob-resupp-landing-con.html`.

The following table lists the resources and minimum requirements for installing the Remote Support application:

| Resources | Minimum Requirements |
|---|---|
| RAM | 512 MB Minimum |
| Free Disk Space | 500 Mb |
| Processor | Dual Core Pentium 4-based or above |
| Operating System | Windows 7/8, Server 2003/2008 or above |

The XenMobile Remote Support application supports all the Windows Mobile-based and Android Samsung SAFE-based devices. Remote control of iOS devices is not yet supported.

More details on Samsung SAFE and generic Android devices can be found at `http://searchconsumerization.techtarget.com/definition/Samsung-for-Enterprise-SAFE`.

# Downloading the Software

To download the Remote Support application from the Citrix web portal, we need to perform the following steps:

1. Go to the Citrix **Downloads** portal, which can be found at `http://www.citrix.com/downloads.html`.
2. Click on **My Account** and log in.

A Citrix account is mandatory to download any software from the Citrix Download Center. Register for a Customer or a Partner account at `https://www.citrix.com/welcome/create-account.html`.

3. Click on **Downloads**.
4. Select **XenMobile** as the **Product** and **Product Software** as the **Download Type** from the drop-down options.
5. Collapse **XenMobile** and click on **XenMobile Remote Support**. Download the software.

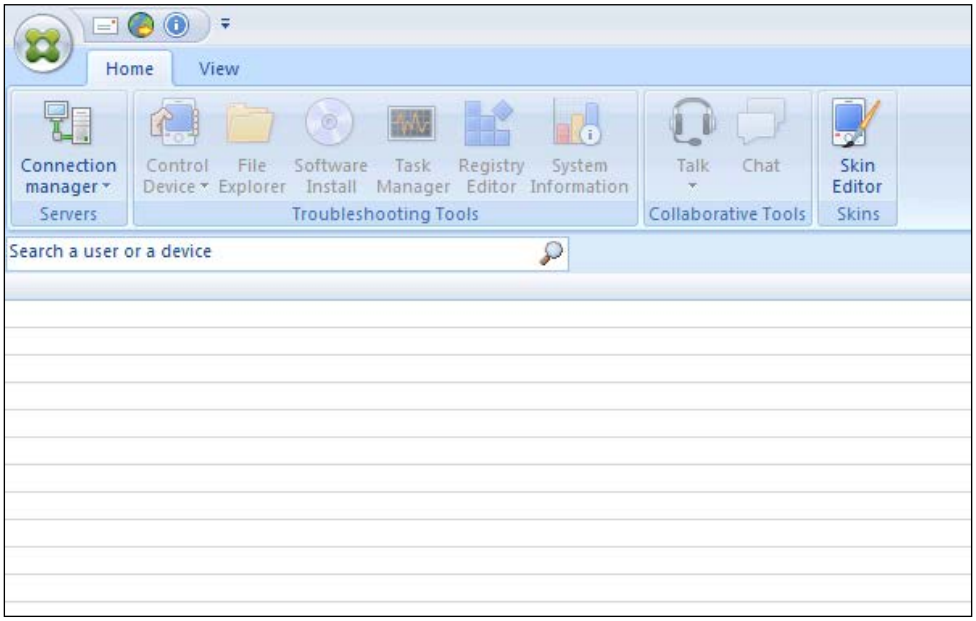
Once both the hardware and software prerequisites have been met successfully, we can move ahead and start installing the product.

# Installing a Remote Support application

Installation of the Remote Support application is pretty simple and self-explanatory. We can install the Remote Support application either on the XenMobile DM server or any other Windows OS as mentioned in the *Installation Prerequisites* section. We need to perform the following steps to successfully install the application:

1. Double-click on the `XenMobileRemoteSupport-8.6.0.33286.exe` file downloaded from the Citrix web portal.
2. Click on **Next** to continue with the Remote Support setup wizard.
3. Agree to the license agreement by clicking on **I Agree**.
4. Choose the location to install the software and click on **Next**.
5. Check the options for **Add an icon to the desktop** and **Allow the user to save login and password** and click on **Next**.
6. Click on **Finish** to complete the installation.

Once the preceding steps have been completed, the software should be installed on the computer and the Remote Support application should open up automatically as shown in the following screenshot:

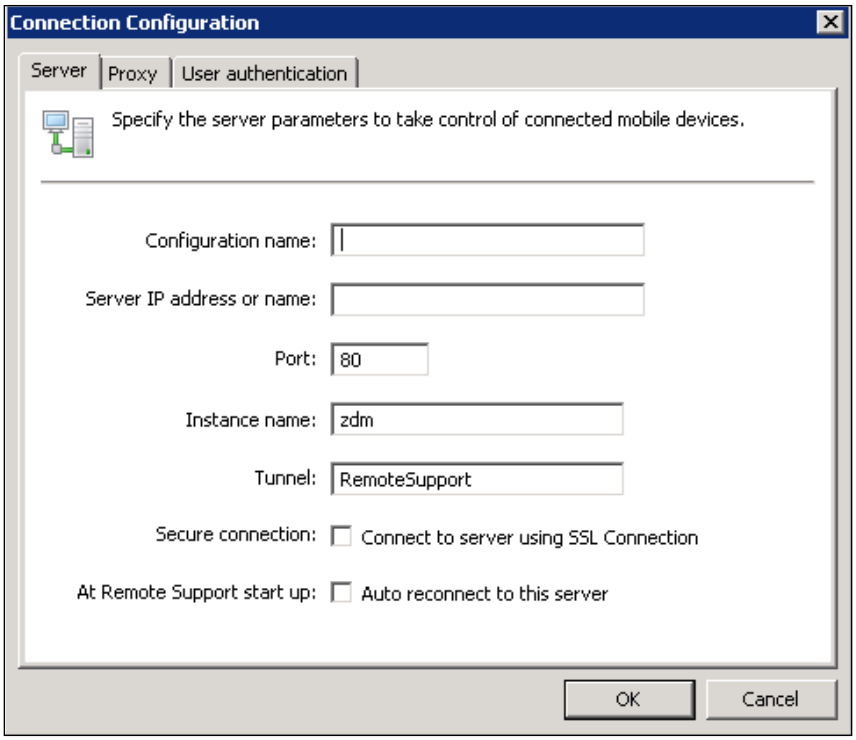


# Adding the Device Manager connection

A Device Manager connection allows the Remote Support application to communicate with the XenMobile Device Manager, which allows us to remotely access the enrolled devices.

The connection created in the Remote Support application communicates with the default Remote Support tunnel created by XenMobile and installed by the application itself. To locate the tunnel, log on to the XenMobile Device Manager web console and navigate to **Policies** | **Android/Windows Mobile** | **Tunnels** | **RemoteSupport**. In this section, we will create a Device Manager connection to establish Remote Support sessions. To do so, perform the following steps:

1. Open the Remote Support application and select **New**.
2. Next to **Configuration name**, enter a name for the connection.
3. Enter the IP address or the name of the Device Manager server.
4. Enter the **Port** number as defined in the `RemoteSupport` tunnel in the Device Manager web console (**Policies** | **Android/Windows Mobile** | **Tunnels** | **RemoteSupport)**.
5. Leave the **Instance name** and **Tunnel** option as it is.
6. Check the box next to **Connect to server using SSL Connection** to ensure a secure communication.
7. The **Proxy** tab is used in case we have a proxy server in place, and the **User Authentication** tab binds this connection with a specific ID and password. In our case, we want admins to enter their individual credentials before logging in, so it's kept blank.
8. Click on **OK** and enter your XenMobile Admin credentials when prompted to establish the connection.




Once you are successfully connected, you can view the enrolled devices, users, and groups available in Device Manager from the Remote Support console. We can start a remote session by selecting the device and clicking on **Control Device**. The end user gets a prompt to allow the admin to remotely access the device. Once the access is granted, the session can be started.

# Summary

In this chapter, we have covered the hardware and software prerequisites required to install the Remote Support application. Also, we have installed the Remote Support application and configured it to manage enrolled devices.

In the next chapter, we will learn how to enrol mobile devices and perform specific tasks such as revoking or wiping in case the device is lost or mishandled.

# 7
# Device Enrollment and Revoking Access

After having successfully implemented the XenMobile components, now we will start enrolling devices; iOS and Android-based devices will be used as examples in this chapter. While enrolling a device, an agent is installed on the device that communicates with the XenMobile server periodically and helps to update the policies and settings on the device that are applied from the server.

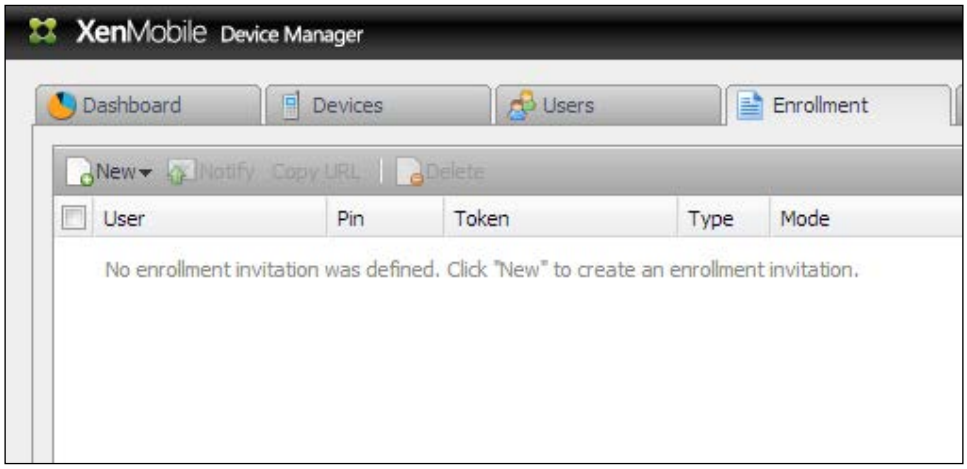
In this chapter, we will go through the various ways a device can be enrolled, using the XenMobile Device Manager. Also, there are some situations where an enrolled device is lost or compromised. In such situations, XenMobile gives us an option to remotely wipe the data on the device so that it's not misused. We will also learn how to wipe a device from the console to take care of such situations. The topics covered in this chapter are as follows:

- Enrolling devices
- Enrolling iOS devices
- Enrolling Android devices
- Revoking device access
- Wiping devices
- Self-help portals

# Enrolling devices

There are multiple options for enrolling Android or iOS devices on the XenMobile Device Manager server. The steps to achieve the same are as follows:

1. To enrol a device, we need to log in to the XenMobile Device Manager web console and then navigate to the **Enrollment** tab.
2. Through the **Enrollment** tab, the administrator can send an **Enrollment Invitation** and MDM link to users by choosing their platform (Android, iOS, Symbian, or Windows Mobile) and the enrollment mode.
3. Once the invitation has been received, the user can go to the link and download the **Worx Home** app and enrol the device.



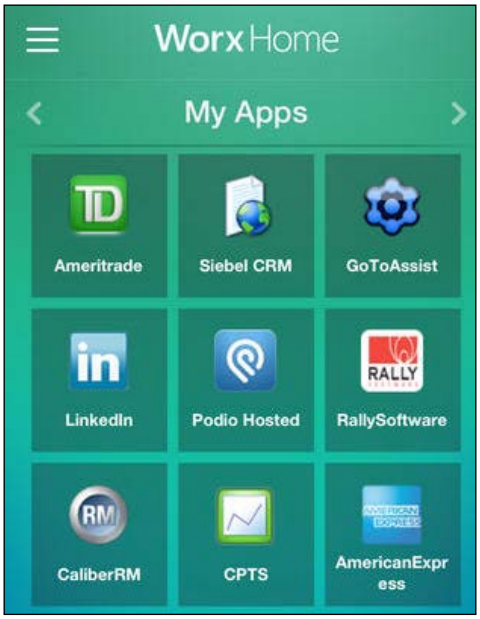

# Enrolling iOS devices

In this section, we will enrol an iOS device with the XenMobile MDM server by installing the Worx Home agent. To do so, perform the following steps:

Citrix Enroll is no longer required for enrolling iOS devices. Enrollment can now be done with Worx Home using the one step enrollment process. Read more at `http://blogs.citrix.com/2013/11/12/xenmobile-end-of-standalone-enroll-application/`.

1. Download the Worx Home app from the App Store at `https://itunes.apple.com/us/app/worx-home-by-citrix/id434682528?mt=8`.

2. Launch the Worx Home app and enter the XenMobile Device Manager Server URL, for example, `mdm.teamxchange.in` or the e-mail address of the user.
3. Now, enter the **Username** and **Password** for the user and tap on **Sign On**.
4. After successful authentication, the application should open up the Safari browser to complete the enrollment process. Once we click on **Enroll**, the application prompts us to accept and install the device profiles corresponding to the XenMobile server.
5. Once the profiles are successfully installed, we should be logged on the Worx Home app and be able to see the server-deployed apps, if any.




# Enrolling Android devices

In this section, we will enrol Android devices with the XenMobile MDM server by installing the Worx Home agent. To do so, perform the following steps:

1. Download and install the Worx Home by Citrix app from the Google Play Store.
2. Launch the Worx Home app and enter the XenMobile Device Manager Server URL, for example, `mdm.teamxchange.in` or the e-mail address of the user.

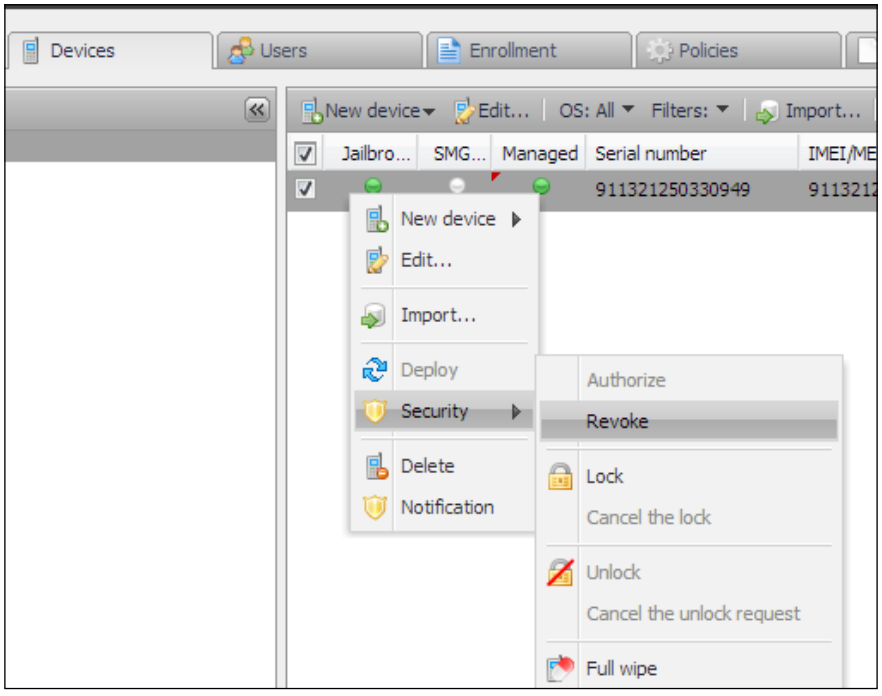
3. Now, enter the **Username** and **Password** for the user and click on **Sign On**.
4. Select **Activate** when the **Activate Device Administrator** screen appears.
5. On successful authentication, we should be logged on to the Worx Home and should see the enrolled device on the XenMobile Device Manager console in the **Devices** tab.

# Revoking device access

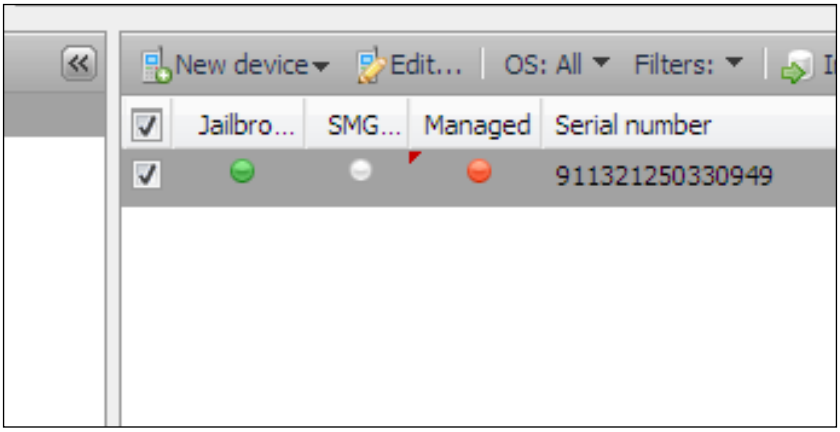
Administrators can block access to an enrolled device and mark its certificates as invalid, which will restrict the device from connecting to the Device Manager server or accessing corporate data. This can be helpful in scenarios where the user has left the organization and should not be allowed any further access to corporate data.

We can revoke a device by performing the following steps:

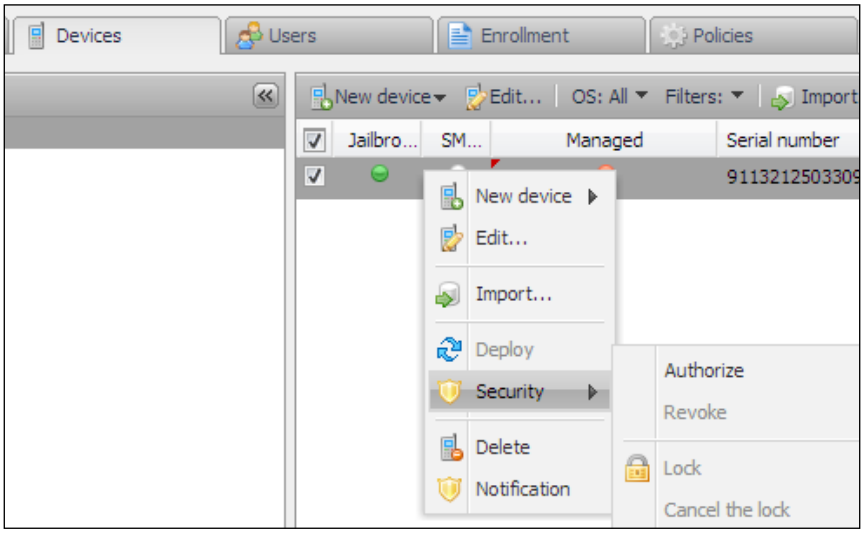
1. Log on to the XenMobile Device Manager console and navigate to the **Devices** tab.
2. Right-click on the enrolled device, select **Security**, and click on **Revoke**.



3. Click on **Yes** to accept the device revoke prompt.
4. This should disconnect the device from the DM server and we should be able to see a red icon under **Managed** if the device has been successfully revoked.




5. Further, a revoked device can again be authorized by right-clicking on the device, navigating to **Security,** and then clicking on **Authorize**.




Authorize Device

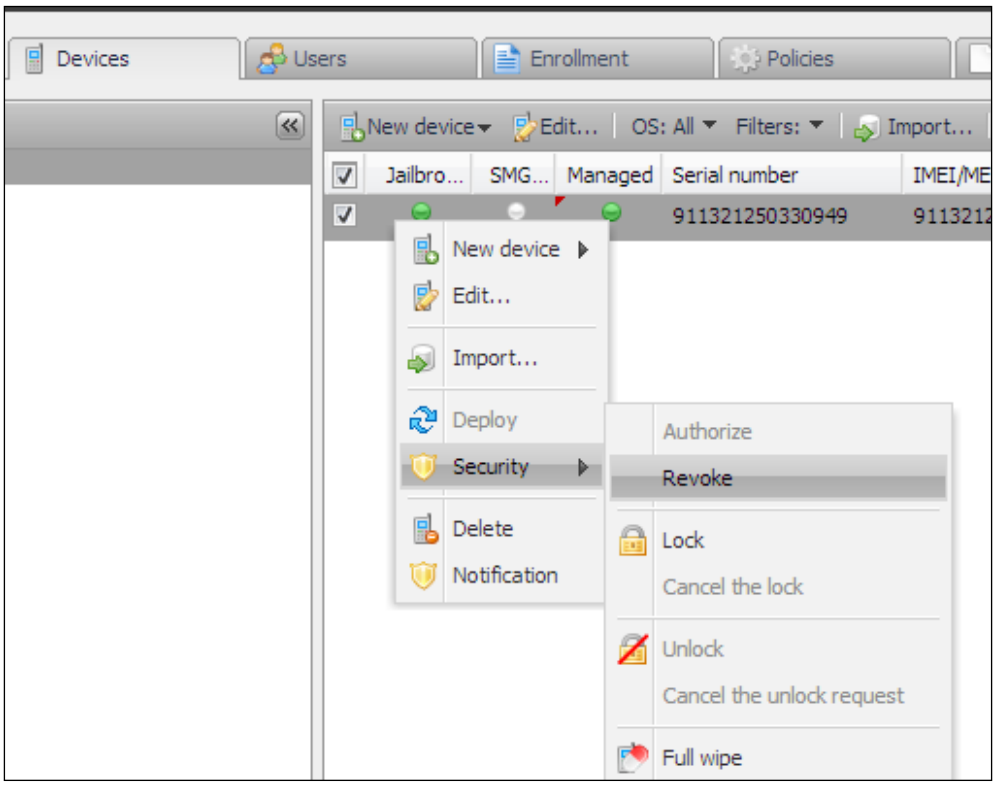
# Device wipe

Device wipe was always one of the most sought-after feature of MDM solutions. It provides the option to the administrator as well as end users, using Self-help portals, to wipe a lost or stolen device. Wipes are generally of two categories, listed as follows:

- **Selective wipe**: When this is performed, only the corporate data from the end user's device is deleted, leaving the personal data intact.
- **Full wipe**: When this is selected, a complete factory reset occurs, leading to the deletion of both company as well as personal data.

Wipe is an irreversible option and can lead to data loss; thus, it should be carried out with extreme caution.

To perform a device wipe, right-click on the enrolled device, navigate to **Security**, and then select **Full wipe** or **Selective wipe**.



# The Self-help portal

XenMobile Device Manager integrates the Self- Help portal for users, allowing them to manage their devices. Using the Self-help portal, a user can enrol their device by sending an enrollment request on their device. The Self-help portal also allows users to locate their own devices or wipe the content residing on it, in case the device is lost or stolen. In such cases, the user can also opt to lock the device using the Self-help portal.

Any Active Directory-based user or XenMobile Device Manager user automatically gets access to the Self-help portal, which can be accessed at `https://<device.manager.ip.address>:8443/zdm/`

# Summary

In this chapter, we have learned how administrators can send invitations to end users to get their devices enrolled, and how iOS-and Android-based devices can be enrolled with the XenMobile DM server. We also learned how to manage these devices by revoking them, and how to perform a selective and full device wipe.

In the next chapter, we will learn to manage applications using the XenMobile components.

# 8
# Managing Applications

With the increasing demand for MDM came the dire requirement to safeguard the applications residing on the devices. Every device we use has a set of applications belonging to different genres, for example, productivity, games, or messaging. Many of these applications have the potential to increase the productivity of employees, but a few can also pose a high security risk to enterprises. The usage of such applications can lead to the leakage of data, which might be crucial to organizations. This leads to the introduction of a very crucial technology now known as **Mobile Application Management (MAM)**. MAM lets you complete data and manage the application lifecycle from the device provisioning stage until the time the employee leaves the organization.

In this chapter, we will learn how to deploy applications on mobile platforms, using the XenMobile components. The contents of the chapter will be as follows:

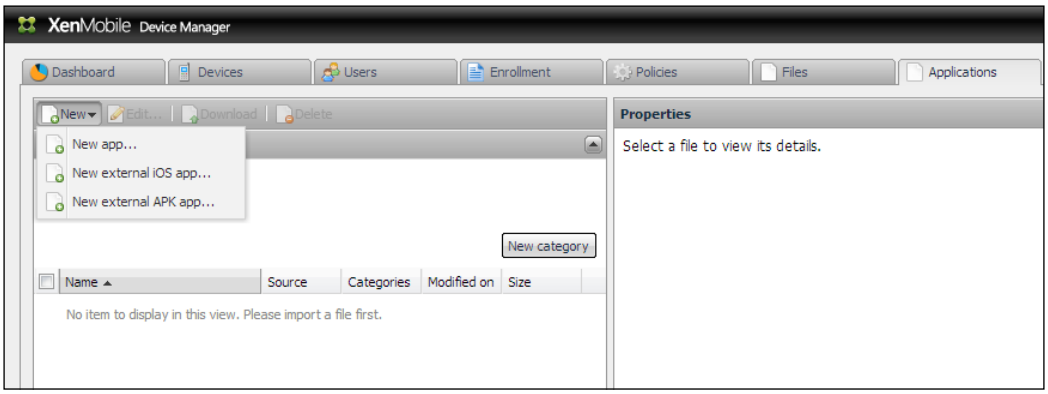
- Application deployment from XenMobile Device Manager console
- Application deployment from XenMobile App Controller

## Deploying application from the XenMobile™ Device Manager console

We can deploy either iOS - or Android-based applications from the XenMobile Device Manager. The Device Manager has the following three options for app deployment on end user devices:

- **New app…**: This option allows an administrator to upload a valid application package file, for example, `.apk` or `.ipa`, to be deployed to end-user devices

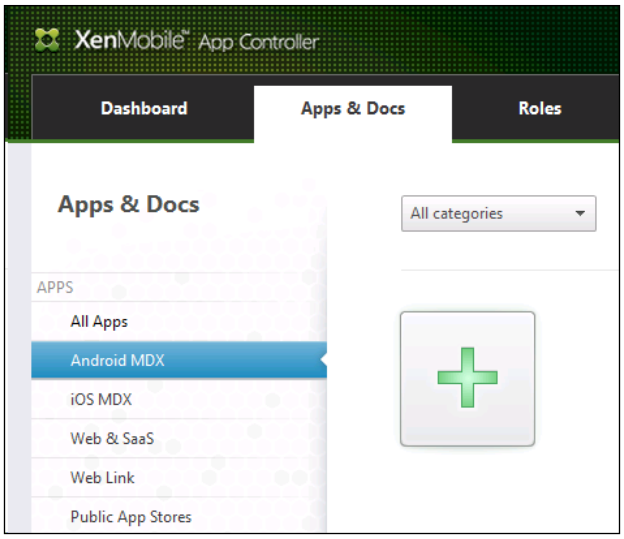
- **New external iOS app…**: This option allows administrators to specify the app URL (from App Store) to be downloaded and installed on devices
- **New external APK app…**: This option allows administrators to specify the app URL (from Google Play Store) to be downloaded and installed on devices




# Application deployment from XenMobile™ App Controller

XenMobile gives administrators an option to deploy applications through the XenMobile App Controller. Similar to the XenMobile Device Manager, the App Controller provides options to deploy iOS - and Android-based apps on end-user devices. To deploy an app from App Controller, perform the following steps:

1. Log on to the App Controller web console as described in *Chapter 5, XenMobile™ App Controller Deployment*.
2. Click on **App & Docs** and choose the type of application to be uploaded (**iOS MDX**, **Android MDX**, **Web & SaaS**, and so on).




3. Click on the plus icon on the right-hand side section.
4. Browse to the location of the application package file and click on **Next**.
5. Fill in the details such as **Application name**, **Description**, and **Category** and click on **Next**.
6. Enter details for the e-mail server under the **Workflow** settings and click on **Next**.
7. In the **Policies** section, we can choose policies to be deployed on the app, for example, block cut-and-copy feature, document exchange restrictions, blocking camera usage, and so on.
8. Once you're done, click on **Save**.

Following the preceding steps should add the app to the App Controller server, and the app is provisioned to end-user devices once they enroll their devices using Worx Home. Refer to *Chapter 7*, *Device Enrollment and Revoking Access* for the steps on device enrollment.

# Summary

In this chapter, we have learned the various ways an app can be deployed, using the XenMobile Device Manager and App Controller. We have also learned the various options we get to upload applications from these XenMobile components.

In the next chapter, we will learn how to deploy policies to manage the applications deployed on end-user devices.

# 9
# Deploying Policies

Policies are used to manage devices that are enrolled with the XenMobile Device Manager. By applying a policy, a XenMobile administrator can decide how enrolled devices will work once connected to the corporate network. In XenMobile, there are policies that manage which application needs to be installed and implement security policies on these devices. It also gives the option to deploy policies on individual groups as required. Once a policy has been implemented, the admin can push a package to the selected devices and track the deployment status to ensure a successful policy deployment.

Through XenMobile Policies, admins can enforce Passcode policies to lock devices after a certain period of inactivity to ensure the device is not misused. Sometimes users tend to uninstall the device agent, to prevent such activities; XenMobile can restrict users from uninstalling the XenMobile agent.

In this chapter, we will learn the following topics:

- XenMobile policies
- Passcode policy creation for iOS devices
- Device-jailbroken-detection policy
- Application access policy

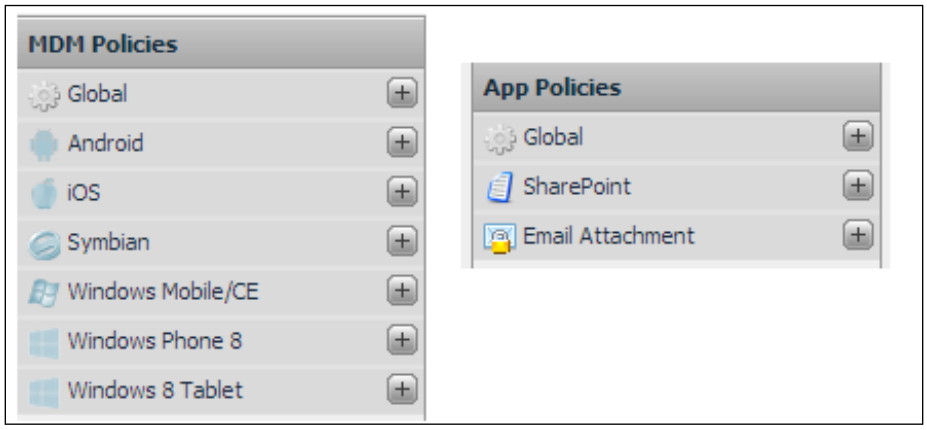
# XenMobile™ policies

A policy controls how an enrolled device functions, for example, locking a device to a specific Wi-Fi connection or pushing e-mail configurations and deciding the level of access to be allotted to the owner of the device. Policies can manage e-mail, Wi-Fi, GPRS, certificates, and other configurations on end-user devices.

> MDM clients can only leverage features available on a device but cannot add any new feature on a device.

XenMobile has distributed policies into the following two major categories on its Device Manager console:

- **MDM Policies**: They control device-based configurations (e-mail, VPN, encryption, and so on) depending on individual device platforms (iOS, Android, Symbian, Windows, and others). In addition to this, MDM Policies also manage tunnels, which can be used to secure applications and their contents residing on the device. A remote support tunnel can be created to enable Remote Support services for end-user devices.
- **App Policies**: They manage the content residing on the enrolled devices and provide application access policies to blacklist-/whitelist-specific apps on devices, depending on their respective platforms.



# Creating the passcode policy

Passcode policies, also known as **Password** policies, when deployed on devices, ensure that the end user enters the specific password in order to unlock the device. We need to perform the following steps to deploy a passcode policy on an iOS device:

1. Log on to the XenMobile Device Manager console.
2. Navigate to **Policies** and click on **iOS**.
3. Select **Configurations** and in the right pane click on **New Configurations**; now select **Passcode**.
4. Under the **General** tab, specify the **Identifier** (the profile name for the policy).
5. Enter a desired **Display Name** for the policy, for example, `Passcode Policy`.
6. Click on the **Policy** tab and select **Require a code on the device**.
7. Now, check the box besides **Allow simple values**. This allows the user to enter a simple passcode, which may consist of only alphabetic characters or numbers.
8. Select the value for **Minimum length of codes**. For simplicity, we will keep it to **4** and click on **Create**.

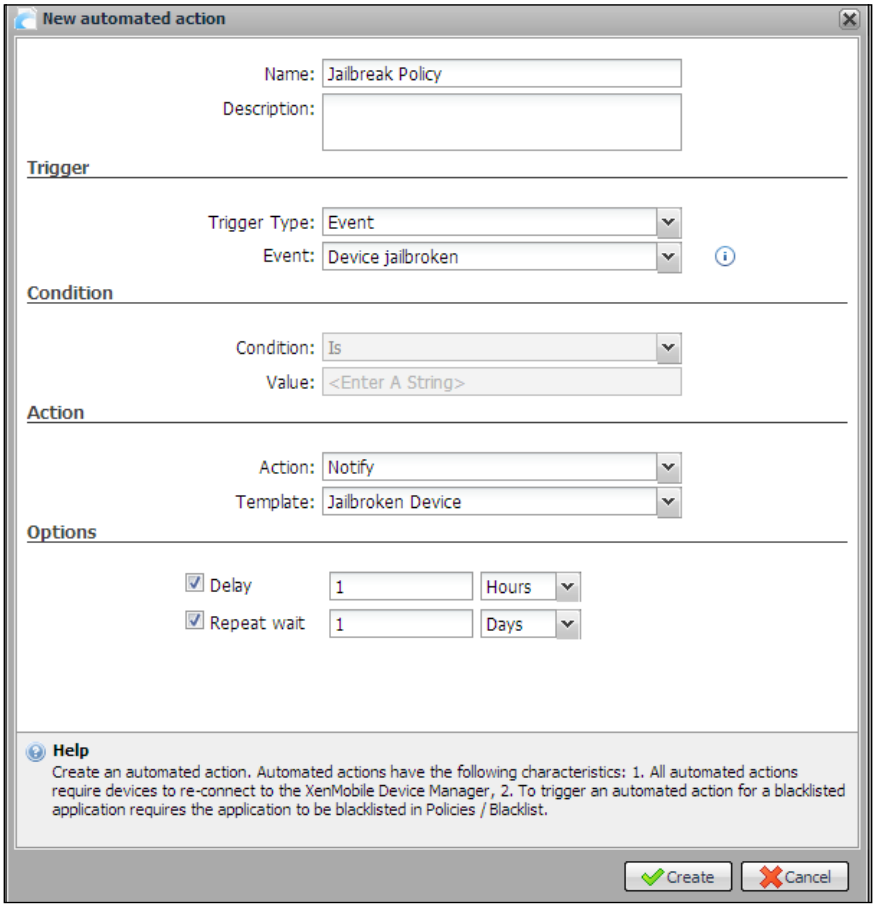
Once this policy is deployed, the user will be prompted to choose a password to set the passcode policy.

# The device-jailbroken detection policy

There can be instances where a user brings in a device that is jailbroken or rooted (a software/hardware-exploited device with root access). These devices can be a security risk; hence, blocking these devices is a must. In this section, we will create a policy to detect such devices:

1. Navigate to the **Policies** tab and select **Global**.
2. Click on **Automated Actions** and then on **New**.
3. Enter a **Name** for the policy, for example, `Jailbreak Policy`.
4. Select **Event** as the **Trigger Type**.
5. In **Event**, select **Device jailbroken**.

6. Select **Notify** as the **Action**, or as desired.
7. Choose the **Jailbroken Device** template and click on **Create**.




Once we deploy this policy, any jailbroken device that connects to the XenMobile Device Manager server will be notified to the Admin and the user for further actions. We can also choose other actions for this policy, which may be a selective wipe or a complete wipe.

# The Application Access Policy

1. Application Access Policy determines how an app installed on an end user device will be treated when enrolled with the XenMobile Device Manager server. A policy can be used to suggest, mandate, or forbid an app on enrolled devices. In this section, we will create a policy to restrict the usage of the Facebook app on end-user devices. To do so, perform the following steps:
2. Navigate to **Policies** | **App Policies**.
3. Select **Global** and click on **Application Access Policies**.
4. Click on **New Application Access Policy**.
5. Enter a **Name** for the policy, for example, `Facebook Restriction Policy`.
6. Select the **Access Policy** as **Forbidden**.
7. Choose the **OS type** as **Android** and click on **New app**.
8. Under **App Name**, enter the name of the app, for example, `Facebook` and click on **Create**.

We can also enter the App Package Name for the application, which is the bundle identifier for the application. This will provide greater accuracy, for example, `com.facebook.katana`, for Facebook. Try using the application ApkSpy on PCs to get the Bundle Identifiers for apks.

9. Click on **Create** on the policy window.

Once the policy has been deployed, it will restrict enrolled devices from accessing the desired app such as Facebook, or the desired app on the enrolled devices as shown in our example.

# Summary

In this chapter, we have covered a few common policies available in the XenMobile Device Manager. We have learned how to create a passcode policy and the identified jailbroken or rooted device section. We have also covered how to restrict unsecure applications from being accessed on an enrolled device.

In the next chapter, we will learn how to troubleshoot issues while installing and managing the XenMobile components, and managing enrolled mobile devices.

# 10
# Troubleshooting

With every application come issues ranging from its installation, management, configuration, and so on. But these issues can be tactfully handled by following a logical and properly documented approach. In this chapter, we will deal with three of the most common issues that arise while working with XenMobile, discuss their cause, and provide resolutions. The topics covered in this chapter are as follows:

- Installation issues
- LDAP integration issues
- Remote Support issues

## Installation issues

Most of the XenMobile installation issues can occur due to not meeting system requirements. Before installing the XenMobile MDM Solution, ensure all the deployment prerequisites, as mentioned in *Chapter 2*, *XenMobile™ Solution Deployment Prerequisites*, have been met successfully. We will see one of the common error messages received during the installation of XenMobile Device Manager.

- **Error**: The configuration failed due to the following errors:

  `java.lang.ExceptionInInitializerError` or **Error 404**, while updating XenMobile DM

- **Cause**: Incomplete Java prerequisites
- **Resolution**: Install Java prerequisites as mentioned at `http://support.citrix.com/proddocs/topic/xenmobile-prepare/xmob-deploy-device-manager-sys-reqs-con.html`.

  Ensure the prerequisites, as mentioned in *Chapter 2*, *XenMobile™ Solution Deployment Prerequisites*, have been met successfully or refer to the preceding link.

# LDAP integration issues

LDAP integration enables XenMobile to communicate with Microsoft Active Directory services. This in turn allows XenMobile to gather a list of Active Directory users. It has been noted that, while configuring LDAP in XenMobile Device Manager, admins can face issues due to incorrect LDAP settings. For example, consider the following scenario:

- **Issue**: In many organizations, the internal domain name may be different from the external (on the Internet) published domain name. For example, internally, it is `teamxchange.in`, while it is published externally as `teamxchange.com`. In such cases, setting up LDAP can cause problems if domains don't match.
- **Cause**: Incorrect **Domain Alias** mentioned in XenMobile Device Manager under **Option | LDAP**.
- **Resolution**: **Domain Alias** mentioned should be the externally published domain name, that is, `teamxchange.com`.

# Remote Support issues

Remote Support application in XenMobile bundle allows administrators to remotely access devices and perform specific tasks on enrolled devices. The following instance deals with an issue faced while remotely accessing a device:

- **Issue**: When trying to remotely access a device, the administrator receives an **Access Denied** error.
- **Cause**: Remote Support not supported.
- **Resolution**: Before remotely accessing a device, we need to ensure that the device is either Samsung SAFE-enabled or a Windows Mobile-based device. XenMobile only supports the mentioned devices at the time of writing.

# Summary

In this chapter, we discussed the most common installation, LDAP, and Remote Support issues. Also, we have discussed their best-known causes and resolution. To add to Troubleshooting, the most important factor is to regularly monitor the XenMobile components and their functionalities. This sums up our lesson on the XenMobile Solutions Bundle and its setup to ensure a secure and compliant environment.

# Index

## D



## E



## F



## G



## H



## I



## L



## M



## N

## P



## R



## S



## T



## V



## W



## X

## Z


## Thank you for buying
# Citrix® XenMobile™ Mobile Device Management

## About Packt Publishing

Packt, pronounced 'packed', published its first book "Mastering phpMyAdmin for Effective MySQL Management" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: `www.packtpub.com`.

## About Packt Enterprise

In 2010, Packt launched two new brands, Packt Enterprise and Packt Open Source, in order to continue its focus on specialization. This book is part of the Packt Enterprise brand, home to books published on enterprise software – software created by major vendors, including (but not limited to) IBM, Microsoft and Oracle, often for use in other corporations. Its titles will offer information relevant to a range of users of this software, including administrators, developers, architects, and end users.

## Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to `author@packtpub.com`. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

[PACKT] PUBLISHING enterprise professional expertise distilled


## Instant XenMobile MDM

ISBN: 978-1-84969-626-5 Paperback: 60 pages

A guide to effectively equipping mobile devices with configuration, security, provisioning, and support capabilities using XenMobile, the world's most popular mobile management software

1. Learn something new in an Instant! A short, fast, focused guide delivering immediate results.
2. Install and set up XenMobile.
3. Use Smartphones and tablets at the workplace with XenMobile.
4. Create security policies for mobile devices.

---

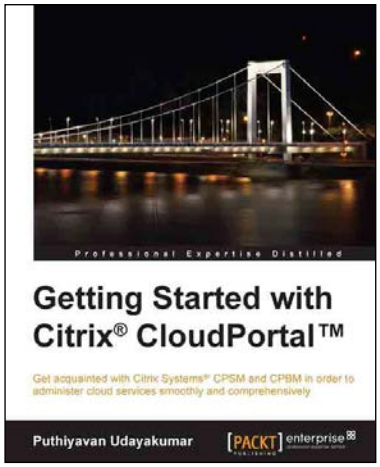

## Getting Started with Citrix® Provisioning Services 7.0

ISBN: 978-1-78217-670-1 Paperback: 134 pages

An example-packed guide to help you successfully administer Citrix® Provisioning Services

1. Install and configure Citrix Provisioning Services quickly and efficiently.
2. Master the architecture of Citrix Provisioning Services.
3. Successfully manage and operate Citrix Provisioning Services.

[PACKT] enterprise
professional expertise distilled
PUBLISHING



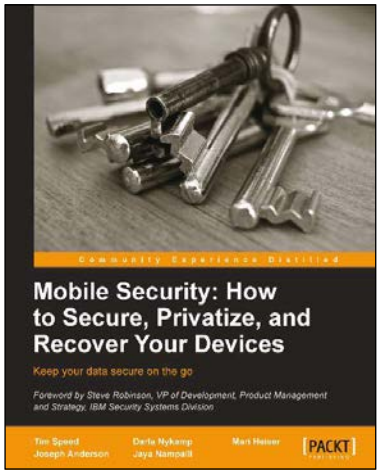

## Getting Started with Citrix® CloudPortal™

ISBN: 978-1-78217-682-4 Paperback: 128 pages

Get acquainted with Citrix Systems® CPSM and CPBM in order to administer cloud services and comprehensively

1. Overview of CPSM and CPBM architectures, and planning CPSM and CPBM.
2. Become efficient in product management, workflow management, and billing and pricing management.
3. Provision services efficiently to cloud consumers and clients.

---




## Mobile Security: How to Secure, Privatize, and Recover Your Devices

ISBN: 978-1-84969-360-8 Paperback: 242 pages

Keep your data secure on the go

1. Learn how mobile devices are monitored and the impact of cloud computing.
2. Understand the attacks hackers use and how to prevent them.
3. Keep yourself and your loved ones safe online.