Symantec™ Managed PKI®

Integrating Symantec™ Managed PKI® with Citrix® XenMobile® Mobile Device Management

Integrating Symantec™ Managed PKI® with Citrix® XenMobile® Mobile Device Management

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated July 25, 2014

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec® product.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

https://www.symantec.com/contactsupport

Contents

Introduction

The enterprise workplace has moved beyond the walls of the organization into a global, mobile environment. To maintain productivity, your end users need to access company resources using a mobile platform. However, you need to be able to trust the end users accessing your systems, and the mobile devices they use, whether you provide their devices or they bring their own.

Symantec's Managed PKI digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from several devices to thousands of devices, providing an in-the-cloud solution for quick deployment and easy management. It also incorporates features from Symantec's other leading security products.

Symantec's Managed PKI issues certificates that can be used to authenticate users for secure communications with company resources, such as VPNs and websites.

This document discusses the following:

- Integrating the Symantec Managed PKI MDM certificate with Citrix XenMobile Mobile Device Management (MDM).
- Configuring Citrix NetScaler Gateway to authenticate a user's device based on the Managed PKI certificate.
- Configuring the Microsoft Exchange server to allow users to synchronize their emails on their mobile device.

Partner Information

The following procedures have been tested on the following platforms:

Table 1-1 Partner Information

Partner Name	Citrix
Product Name	XenMobile MDM
Version	8.6
End-user device	iOS/Android

Architecture Diagrams

Interaction between Citrix XenMobile MDM and Symantec Managed PKI

Figure 1-1 describes how the XenMobile MDM interacts with Symantec Managed PKI to obtain a certificate for a device:

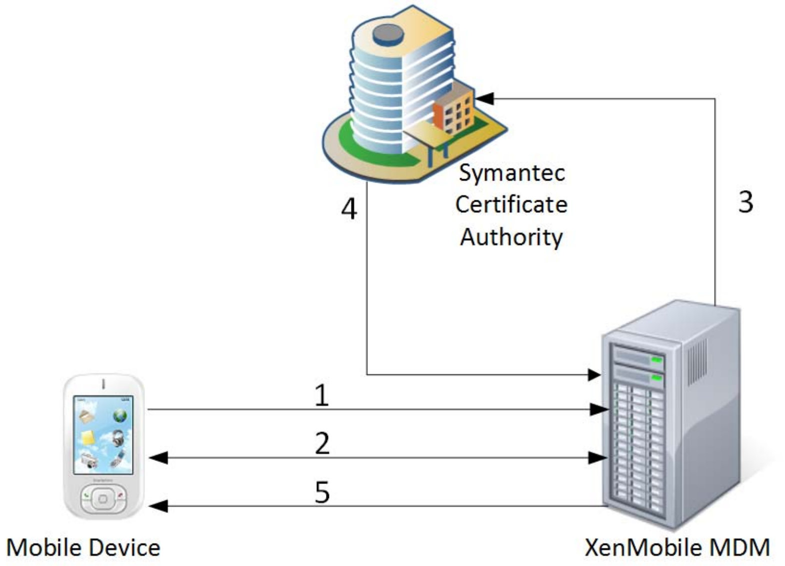


Figure 1-1 Interaction between Citrix XenMobile MDM and Symantec's Managed PKI

1. The mobile device initiates registration with the XenMobile MDM using the Citrix WorxHome agent installed on the device.
2. The XenMobile MDM authenticates the user and mobile device, and gathers the device details from the WorxHome agent on the device.
3. The XenMobile MDM requests Symantec Managed PKI to enroll for a certificate.
4. Symantec Managed PKI enrolls the device for a certificate and sends the certificate to XenMobile MDM.
5. The XenMobile MDM sends the certificate to the mobile device.

Interaction between a User’s Device and XenMobile MDM

Figure 1-2 describes how a user’s device interacts with the XenMobile MDM and the XenMobile App Controller through the NetScaler Gateway to securely access the corporate network:

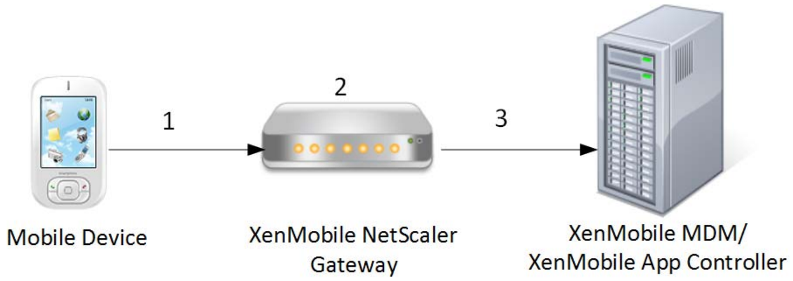


Figure 1-2 Interaction between a user’s device and XenMobile MDM through NetScaler Gateway

1 The end-user’s mobile device accesses the corporate network through the NetScaler Gateway.

2 The Gateway authenticates the end-user’s certificate using the trusted CAs.

3 Based on this authentication, the end-user’s mobile device is allowed access to the corporate network through a secure communication.

Interaction between a User’s Device and Microsoft Exchange Server

Figure 1-3 diagram describes how a user’s device connects to the Microsoft Exchange server to synchronize emails:

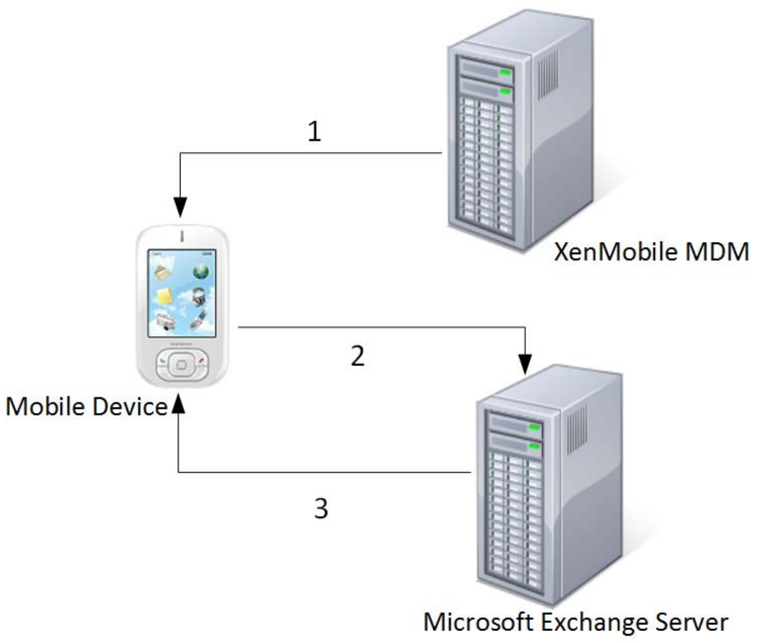


Figure 1-3 interaction between a user’s device and Microsoft Exchange Server

1 The XenMobile MDM pushes the ActiveSync configuration policy package to be deployed on the end-user device.

2 The end user connects to the Microsoft Exchange server. The server verifies the client device against the certificate mapped to the user in the Active Directory.

3 The end user’s mobile device synchronizes with the Exchange server to receive emails.

Integrating Managed PKI with Citrix® XenMobile® MDM

Integration Workflow

The following tasks describe the general steps required to set up the Symantec Managed PKI account and obtain the RA and CA certificates to establish the trust between Symantec Managed PKI and Citrix XenMobile MDM.

Task 1. Set up your Managed PKI 8.x account

Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

You will need to complete and return the following documents. As needed, your Symantec representative will assist you with obtaining and completing these forms.

- Master Service Agreement
- Issuing Authority Naming Application (also known as the CA Naming Document)
- Symantec Services Order Form
- Purchase Order, credit card, or reference number

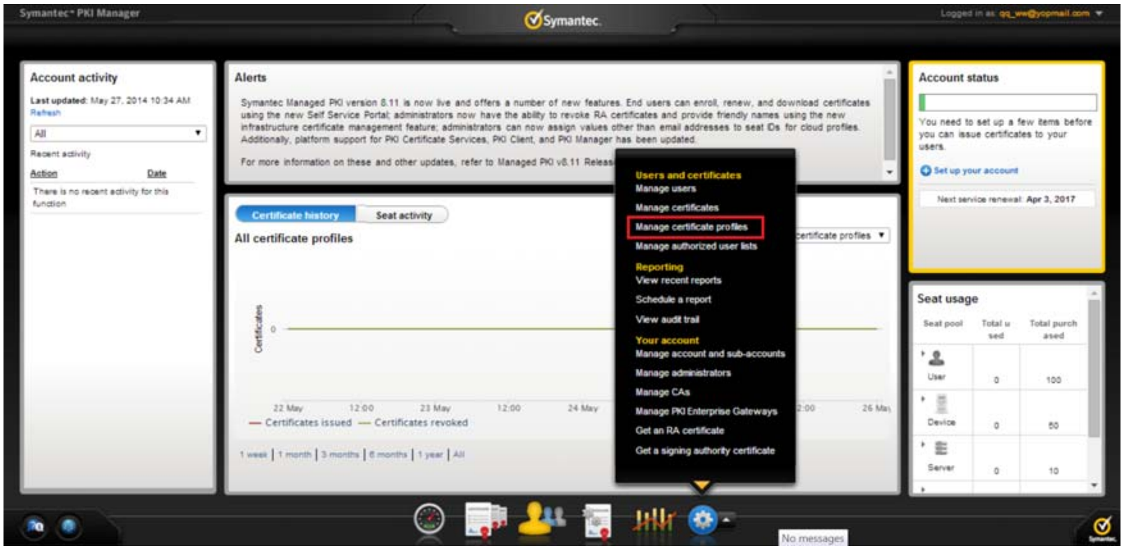
You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. For more information on configuring Managed PKI, refer to PKI Manager and its online help.

Task 2. Create the Managed PKI MDM (Web Service Client) certificate profile

Managed PKI uses a certificate profile to define issued certificates. Complete the following steps to create your Managed PKI MDM (Web Services Client) certificate profile:

1 Log into PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.

2 On the PKI Manager dashboard, click **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.



Symantec Managed PKI version 8.11 is now live and offers a number of new features. End users can enroll, renew, and download certificates using the new Self Service Portal; administrators now have the ability to revoke RA certificates and provide friendly names using the new infrastructure certificate management feature; administrators can now assign values other than email addresses to seat IDs for cloud profiles. Additionally, platform support for PKI Certificate Services, PKI Client, and PKI Manager has been updated.

For more information on these and other updates, refer to Managed PKI v8.11 Releas

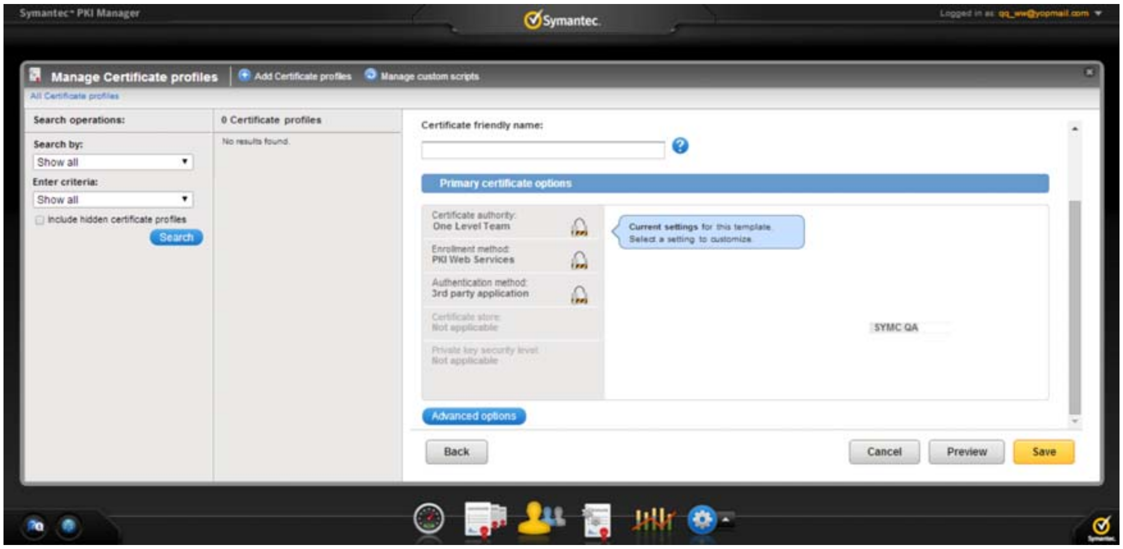
You need to set up a few items before you can issue certificates to your users.

Figure 2-1 Manage Certificate Profiles

3 Click **Add Certificate profiles** from the top of the resulting Manage Certificate profiles page. The Create profile page appears.

4 Select whether these certificates will be issued in **Test mode** or **Production Mode**, and click **Continue**.

5 Select **MDM (Web Service Client)** as the certificate template and click **Continue**. The Customize certificate options page appears.



No results found.

Certificate authority: One Level Team

Enrollment method: PKI Web Services

Authentication method: 3rd party application

Certificate store: Not applicable

Private key security level: Not applicable

Current settings for this template. Select a setting to customize.

SYMC QA

Figure 2-2 MDM (Web Service Client) certificate options

6 Enter a unique name for the certificate profile.

7 Click **Advanced Options**. Table 2-1lists the advanced options.

Table 2-1 Advanced certificate options

Options	Configuration
Subject DN Common Name (CN)	Locked to a fixed value.
Organization Unit (OU)	Locked to a fixed value.
SubjectAltName Other Name (UPN)	Select **Webservice Request** as Source for the field's value.

8 Click **Save**. The system displays the confirmation page, which shows that the certificate profile is successfully created. The page also displays the Certificate Profile OID.

Note: Make a note of the Certificate Profile OID as this is required later when configuring the XenMobile MDM. You can return to the confirmation screen by clicking the **Manage certificate profiles** option and then selecting the certificate profile you created.

Task 3. Generate the key pair

Complete the following steps to generate the key pair needed to create your certificate signing request:

Note: This procedure requires the Java keytool to generate the keys and import them into your keystore. Symantec recommends that you use strong passwords (6 or more characters with a mixture of numbers and upper- and lower-case letters) and store them in a secure location.

```
keytool -genkey -alias pki_ra -keyalg RSA -keysize 2048 -sigalg
SHA1withRSA -dname "CN=<common name>" -keypass <password>
-keystore <keystore name> -storepass <password>
```

where keystore is a Java based software module where the keys are stored.

Task 4. Generate the CSR

Complete the following steps to create the CSR needed to request your Registration Authority (RA) certificate.

Note: This procedure requires the Java keytool to generate the CSR and import it into your keystore.

```
keytool -certreq -alias pki_ra -sigalg SHA1withRSA -file
pki_raCSR.req -keypass <password> -keystore <keystore name>
-storepass <password>
```

The CSR file must meet the following additional requirements:

- The key algorithm must be RSA.
- The key size must be 2048-bit.

Task 5. Obtain the RA certificate

Complete the following steps to obtain the RA certificate:

1 Log into PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.

2 On the PKI Manager dashboard, click **Get an RA certificate** from the Tasks menu on the bottom navigation bar.

3 In the **Paste your CSR** field, paste the CSR you previously copied. See “Generate the CSR” on page 7.

4 Enter a unique name to distinguish your certificate and click **Continue**.

5 Download and save the RA certificate to a temporary location on the system where the key pair was generated.

Task 6. Import the RA and root CA certificates

The CA certificate is required to establish the trust between Symantec Managed PKI and the XenMobile MDM.

1 Import the RA certificate into your keystore by using the following command:

```
keytool -import -alias pki_ra -file cert.p7b -noprompt -keypass
<password> -keystore <keystore name> -storepass <password>
```

2 The Web Services zip package, containing the root and issuing CAs for the RA certificate, are available by clicking on the Symantec PKI Resources icon in the lower left corner of Symantec PKI Manager. You will need to import these CAs as trusted root CAs into the keystore using the appropriate command. This insures that the RA certificate you install is correctly trusted.

- For intermediate CAs:

```
keytool -import -trustcacerts -alias pki_ca -file RAintermegiateCA.cer -keystore
<keystore name> -storepass <password>
```

- For root CAs:

```
keytool -import -trustcacerts -alias root -file RAroot.cer -keystore <keystorename> -
storepass <password>
```

Task 7. Download the CA certificate

Complete the following steps to obtain the issuer root CA certificate:

1 Log into PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.

2 On the PKI Manager dashboard, click **Manage CAs** from the Tasks menu on the bottom navigation bar.

3 Select the appropriate CA certificate and click **Download root certificate**.

4 Save the certificate to the desired location on your system.

Configuring the Citrix® XenMobile® MDM

This chapter discusses how to configure the Citrix XenMobile MDM to use the Managed PKI MDM certificate.

Prerequisites

- CA certificates (obtained from the Symantec Managed PKI – Web Services package). See Step 2 of "Import the RA and root CA certificates" on page 8.
- RA certificate keystore. See Step 1 of "Import the RA and root CA certificates" on page 8.
- Symantec.war file (obtained from Citrix customer support).
- custom_gpki_adapter properties file (located inside the Symantec.war file).

Configuring the Citrix XenMobile MDM

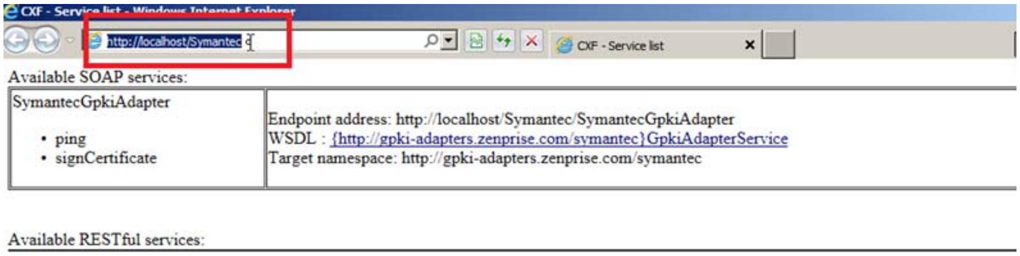
Note: In the following procedure, the XenServer instance is used to launch the XenMobile MDM. You can also directly launch the XenMobile MDM console.

1. From XenServer, create a new instance of the XenMobile MDM and launch the console.
2. Navigate to *C:\* and create a new directory (for example, Symantec) and copy the prerequisite files, mentioned in "Prerequisites" on page 9, to this directory.
3. Copy the *Symantec.war* file to C:\Program Files\Citrix\XenMobile Device Manager\tomcat\webapps.
4. Edit the *gpki_adapter.properties* file. The default location is C:\Program Files\Citrix\XenMobile Device Manager\tomcat\webapps\Symantec\WEB-INF\Classes.
   The location of this file depends on where you have installed Citrix XenMobile Device Manager.
   Update the property value for customProperties to provide the path to the directory that you created in Step 2 of "Configuring the Citrix XenMobile MDM" on page 9. The default path *is /zenprise/custom_gpki_adapter.properties*.

   Note: In this procedure, we use the default web server that comes with the XenMobile MDM server. If you plan to use a separate instance of a web server, you must customize the property file accordingly.

5. Edit the custom_gpki_adapter_properties file in C:/Symantec. Update the following property values:
   a **Gpki.CaSvc.Url**: Enter the Symantec PKI Manager URL (Partner or Production).
   b **keyStore**: Enter the path for the keystore.
   c **keyStorePassword**: Enter the keystore password.
   d **trustStore**: Enter */Symantec/cacerts*.

6 If you are configuring the XenMobile MDM from the same machine that hosts the XenMobile MDM instance, open a browser and navigate to http://localhost/Symantec. Otherwise, navigate to http://<IPAddress:Port>/Symantec.


CXF - Service list - Windows Internet Explorer
http://localhost/Symantec
CXF - Service list

Available SOAP services:

SymantecGpkiAdapter • ping • signCertificate	Endpoint address: http://localhost/Symantec/SymantecGpkiAdapter WSDL : {http://gpki-adapters.zenprise.com/symantec}GpkiAdapterService Target namespace: http://gpki-adapters.zenprise.com/symantec

Available RESTful services:

Figure 3-1 Web Services Description Language (WSDL) URL

7 Click the AdapterService WSDL URL. Make a note of the WSDL URL as it is required later.

Configuring the XenMobile Device Manager Console

You must configure the XenMobile Device Manager console to create the certificate package that can be pushed to the device from the MDM.

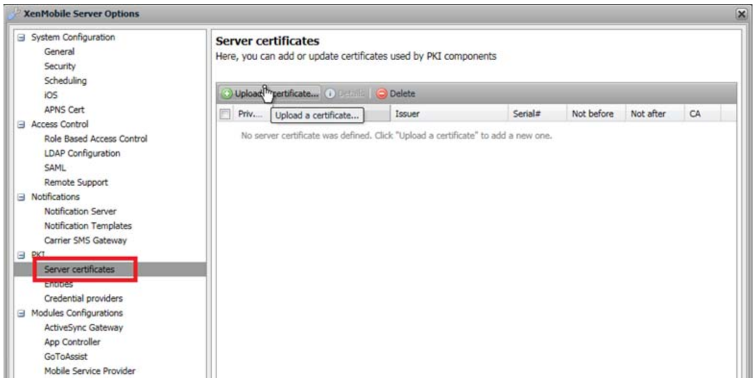
Task 1. Upload a server certificate

Complete the following steps to upload the Symantec CA certificate you obtained to establish the trust between Symantec and Citrix XenMobile MDM:

1 Log into the XenMobile Administrator console.

2 Click **Options**.

3 Under **PKI**, click **Server Certificates** → **Upload a certificate**.



Server certificates

Here, you can add or update certificates used by PKI components

Priv...	Issuer	Serial#	Not before	Not after	CA

No server certificate was defined. Click "Upload a certificate" to add a new one.

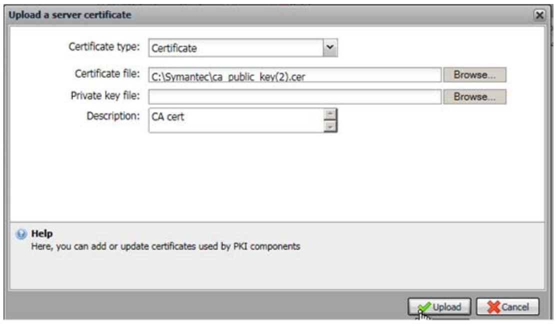
Figure 3-2 Server certificate screen

4 Enter the following:

a **Certificate type**: Select **Certificate**.

b **Certificate file**: Browse for, and select the CA certificate. See “Download the CA certificate” on page 8.

c **Description**: Enter a description for the server certificate.



Upload a server certificate

Certificate type: Certificate

Certificate file: C:\Symantec\ca_public_key(2).cer

Private key file:

Description: CA cert

Help
Here, you can add or update certificates used by PKI components

Figure 3-3 Administrator console - Upload a server certificate

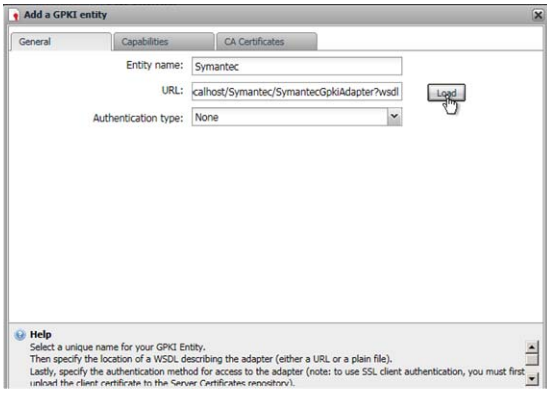
5 Click **Upload**.

Task 2. Add a Generic PKI (GPKI) entity

1 In the PKI section, click **Entities** → **New** → **New Generic PKI Entity**.

2 Provide a name for the entity and enter the WSDL URL that you noted in step 7 of “Configuring the Citrix XenMobile MDM” on page 9.

.



Add a GPKI entity

Entity name: Symantec

URL: calhost/Symantec/SymantecGpkiAdapter?wsdl

Authentication type: None

Help
Select a unique name for your GPKI Entity.
Then specify the location of a WSDL describing the adapter (either a URL or a plain file).
Lastly, specify the authentication method for access to the adapter (note: to use SSL client authentication, you must first upload the client certificate to the Server Certificates repository).

Figure 3-4 Adding a GPKI entity

3 Click **Load**. The **Capabilities** tab displays the GPKI entity parameter types.

4 Click the **CA Certificates** tab.

5 Click **Add a CA certificate** and select the CA certificate you obtained. See “Download the CA certificate” on page 8.

6 Click **Add** to create the GPKI entity.

Task 3. Create a credential provider

Complete the following steps to define a credential provider to handle issuance, distribution, and management of the certificate that will be installed on the devices:

1 Click **Credential Providers** in the **PKI** section.

2 Click **New credential provider**.

3 In the Define a new credential provider dialog box, enter the details as shown in Table 3-1

Table 3-1 Values for New Credential Provider

Field	Description
Credential provider name:	Provide a unique name to distinguish the credential provider.
Description	Enter a description for the credential provider.
Issuing entity	Select the GPKI entity. See "Add a Generic PKI (GPKI) entity" on page 11.
Issuing method	Double click the default value **SIGN** to select the issuing method.
certificateProfileId	Enter the profile OID that you noted in Step 8 of "Create the Managed PKI MDM (Web Service Client) certificate profile" on page 5
certParams:	Enter the following: `commonName=${user.username},otherNameUPN=${user.userprincipalname},mail=${user.userprincipalname}`
Key algorithm	RSA. This value should match the CSR requirement. See "Generate the CSR" on page 7.
Key size	Enter 2048. This value should match the CSR requirement. See "Generate the CSR" on page 7.
Signature algorithm	Select **SHA1withRSA**.
Subject name	Enter the following: `cn=${user.username}`
Issuer	Select the issuer.
Distribution mode	Select **Prefer Centralized**.

4 Click **Add** to save the credential provider.

Creating the Configuration Policy

Complete the following steps to configure a policy to use the credential provider you created in "Create a credential provider" on page 11.

1 Click **Policies** on the Administrator dashboard.

2 Depending on the device OS type, select the configuration policy and click **New Configuration → Add a new configuration profile → Credentials**. If you are creating a configuration policy for ActiveSync, see "Creating an ActiveSync Configuration Policy" on page 30.

3 Complete the required information in the **General** tab.

4 Click the **Credential** tab and enter the following:

a **Credential type**: Select **Credential Provider**.

b **Credential provider**: Select the credential provider that you created in "Create a credential provider" on page 11.

5 Click **Create** to create the credential configuration policy.

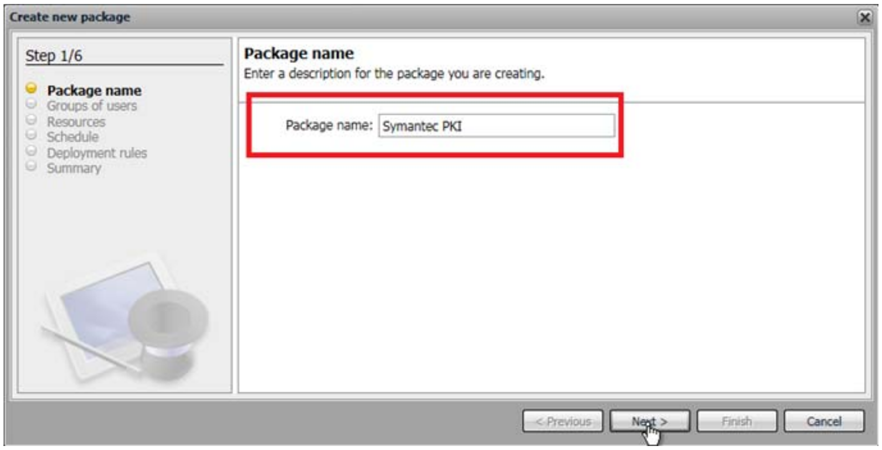
Creating the Deployment Package

Complete the following steps to create a package that will deploy the policy configuration onto a device:

1 On the Administrator dashboard, click **Deployment**.

2 Under New package, select the package depending on the device OS type.

3 Complete the steps in the Create new package wizard as follows:



Create new package

Step 1/6

Package name
Enter a description for the package you are creating.

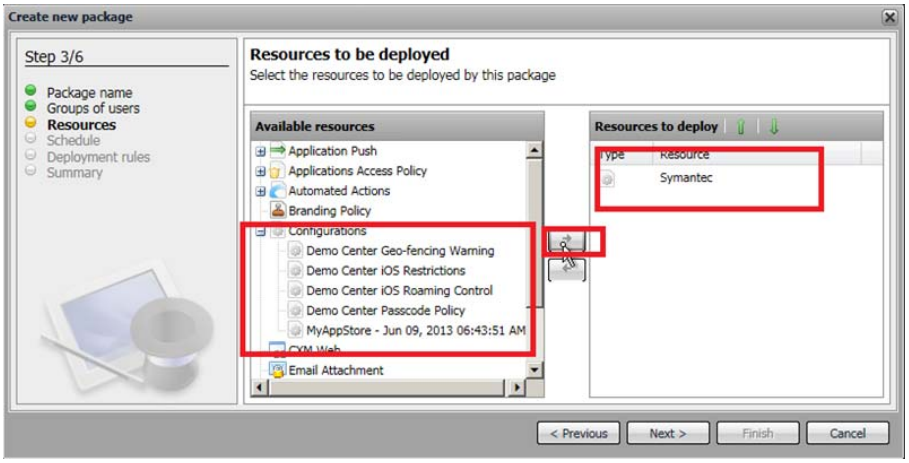
Package name: Symantec PKI

Figure 3-5 Create New Package screen

a Enter a package name and click Next.

b Select the group of users that will receive the package. Click Next.

c Select the configuration package that needs to be deployed. See “Add a Generic PKI (GPKI) entity” on page 11.



Create new package

Step 3/6

Resources to be deployed
Select the resources to be deployed by this package

Available resources
- Application Push
- Applications Access Policy
- Automated Actions
- Branding Policy
- Configurations
  - Demo Center Geo-fencing Warning
  - Demo Center iOS Restrictions
  - Demo Center iOS Roaming Control
  - Demo Center Passcode Policy
  - MyAppStore - Jun 09, 2013 06:43:51 AM
- CXM Web
- Email Attachment

Resources to deploy

Type	Resource
	Symantec

Figure 3-6

d Select the schedule when the package needs to be deployed.

e Select the deployment rules.

f View the summary of the new package.

g Click **Finish** to create the new package.

Chapter 4

Configuring Citrix® NetScaler Gateway

This chapter discusses how to configure the Citrix NetScaler Gateway to authenticate a user based on the Managed PKI certificate. It also discusses how to configure the authentication mechanism on the XenMobile AppController and to configure the XenMobile server for the XenMobile AppController.

Configuring NetScaler Gateway

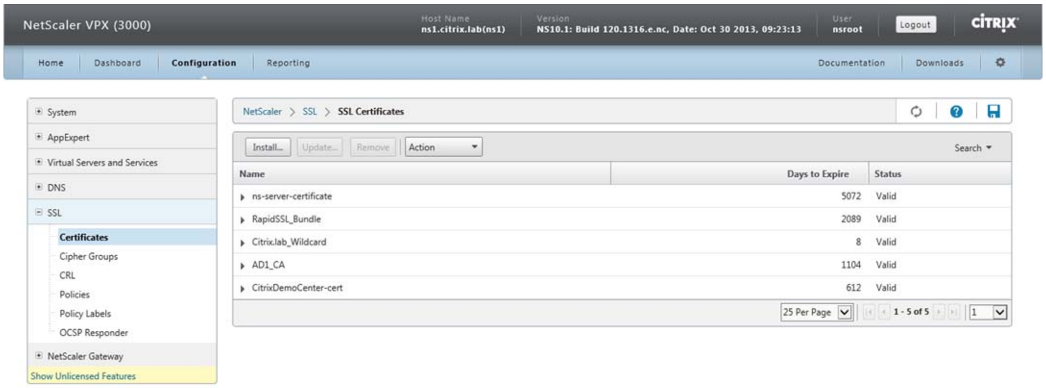
The Citrix NetScaler Gateway acts as the VPN server that uses the Managed PKI certificates to authenticate the user's devices.

Task 1. Uploading the CA certificate

Complete the following steps to upload the CA certificate for the NetScaler Gateway to use:

1 Log into NetScaler Gateway using your administrator credentials.

2 Click **Configuration** → **SSL** → **Certificates**.



Name	Days to Expire	Status
ns-server-certificate	5072	Valid
RapidSSL_Bundle	2089	Valid
Citrix.lab_Wildcard	8	Valid
AD1_CA	1104	Valid
CitrixDemoCenter-cert	612	Valid

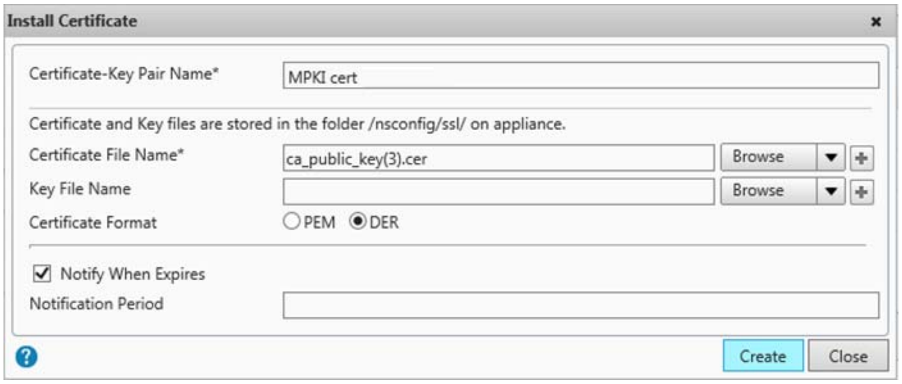
Figure 4-1 SSL Certificates

3 Click **Install** and do the following:

a In the Install Certificate dialog box enter the following:

- **Certificate-Key Pair Name**: Enter a certificate-key pair name.
- **Certificate File Name**: Click the arrow next to **Browse** and select **Local** or **Appliance** to browse to the location where you downloaded and saved the CA certificate. See "Download the CA certificate" on page 8.

- **Certificate Format**: Select **DER**.



Install Certificate

Certificate-Key Pair Name*: MPKI cert

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*: ca_public_key(3).cer

Key File Name:

Certificate Format: ○ PEM ● DER

☑ Notify When Expires

Notification Period:

Figure 4-2 Install certificate

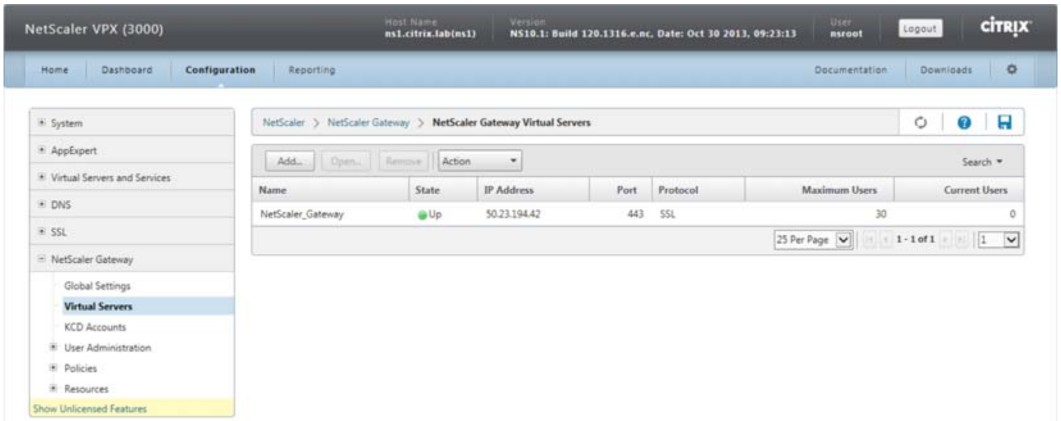
b Click **Create** to upload the CA certificate.

4 Click the arrow button next to the certificate name to view the details of the certificate.

Task 2. Configuring the NetScaler Gateway server

Complete the following steps to configure the NetScaler Gateway server to use the CA certificate:

1 Click **NetScaler Gateway → Virtual Servers**.



NetScaler VPX (3000)

Host Name: ns1.citrix.lab(ns1)

Version: NS10.1: Build 120.1316.e.nc, Date: Oct 30 2013, 09:23:13

User: nsroot

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
NetScaler_Gateway	Up	50.23.194.42	443	SSL	30	0

Figure 4-3 Virtual Servers

2 Select the virtual server and click **Open** to load the NetScaler applet.

3 In the Configure NetScaler Gateway Virtual Server window, do the following:

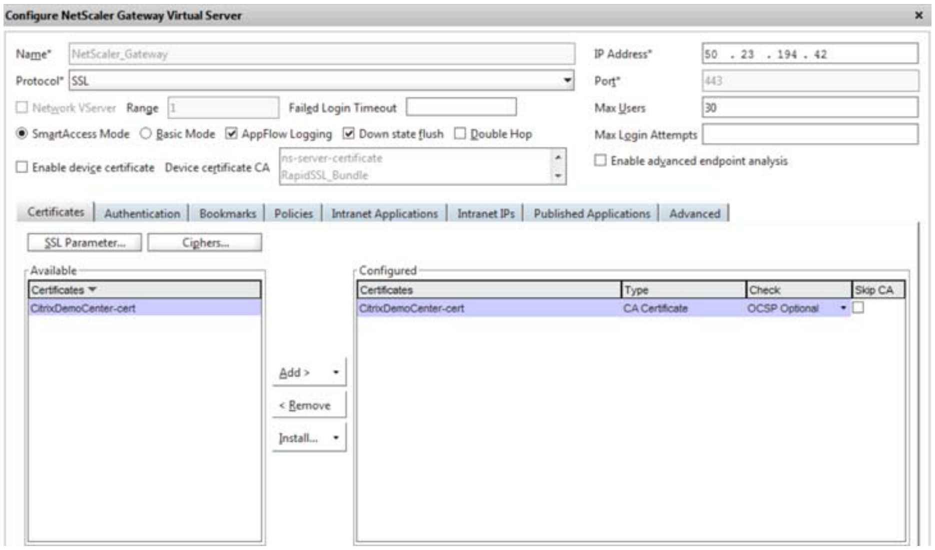
a Under **Available Certificates**, select the CA certificate that you uploaded in Task 1. See “Uploading the CA certificate” on page 15.

b Click the arrow button next to **Add.**

c Click **as CA**.

d Under **Check**, select the appropriate option.

e Click **OK**.



Configure NetScaler Gateway Virtual Server

Name* NetScaler_Gateway

Protocol* SSL

IP Address* 50 . 23 . 194 . 42

Port* 443

□ Network VServer Range 1 Failed Login Timeout

Max Users 30

Max Login Attempts

● SmartAccess Mode ○ Basic Mode ☑ AppFlow Logging ☑ Down state flush □ Double Hop

□ Enable device certificate Device certificate CA ns-server-certificate RapidSSL_Bundle

□ Enable advanced endpoint analysis

Available

Certificates
CitrixDemoCenter-cert

Configured

Certificates	Type	Check	Skip CA
CitrixDemoCenter-cert	CA Certificate	OCSP Optional	□

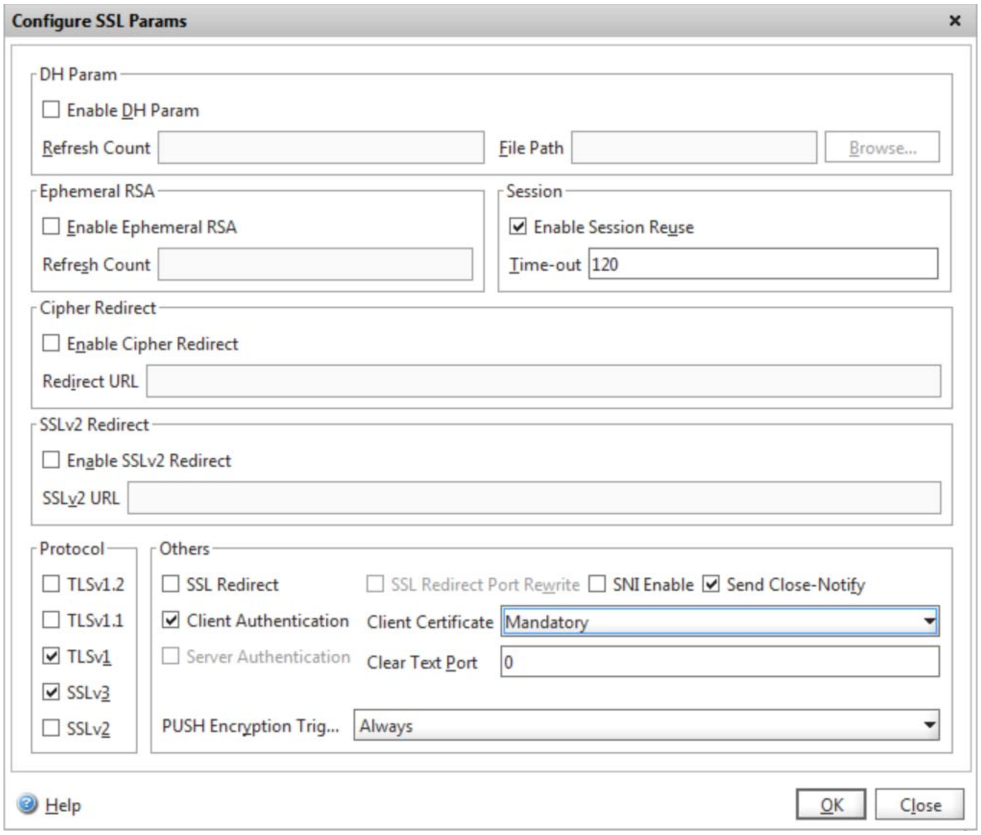
Figure 4-4 Configure NetScaler Gateway Virtual Server - Certificates tab

4 Click **SSL Parameter**, and do the following:

a Select the **Client Authentication** check box.

b Select **Client Certificate** as **Mandatory** to make authentication stricter by authenticating the user’s device using only the certificate.

c Click **OK**.



DH Param

☐ Enable DH Param

Refresh Count

File Path

Ephemeral RSA

☐ Enable Ephemeral RSA

Refresh Count

Session

☑ Enable Session Reuse

Time-out 120

Cipher Redirect

☐ Enable Cipher Redirect

Redirect URL

SSLv2 Redirect

☐ Enable SSLv2 Redirect

SSLv2 URL

Protocol

☐ TLSv1.2

☐ TLSv1.1

☑ TLSv1

☑ SSLv3

☐ SSLv2

Others

☐ SSL Redirect

☐ SSL Redirect Port Rewrite

☐ SNI Enable

☑ Send Close-Notify

☑ Client Authentication

Client Certificate Mandatory

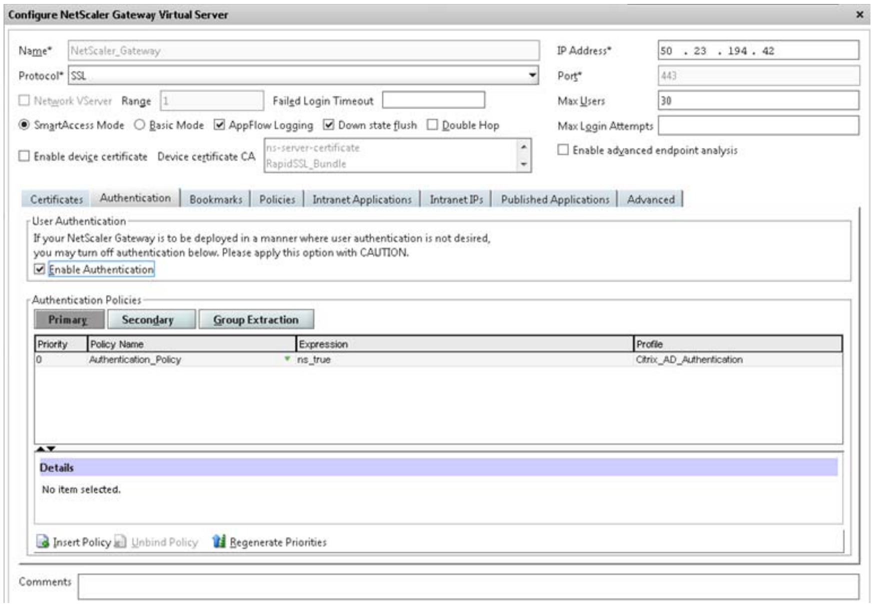
☐ Server Authentication

Clear Text Port 0

PUSH Encryption Trig... Always

Figure 4-5 Configure SSL parameters

5 In the Configure NetScaler Gateway Virtual Server window, click the **Authentication** tab.



Configure NetScaler Gateway Virtual Server

Name* NetScaler_Gateway

Protocol* SSL

IP Address* 50 . 23 . 194 . 42

Port* 443

□ Network VServer Range 1 Failed Login Timeout

Max Users 30

● SmartAccess Mode ○ Basic Mode ☑ AppFlow Logging ☑ Down state flush □ Double Hop

Max Login Attempts

□ Enable device certificate Device certificate CA ns-server-certificate RapidSSL_Bundle

□ Enable advanced endpoint analysis

User Authentication

If your NetScaler Gateway is to be deployed in a manner where user authentication is not desired, you may turn off authentication below. Please apply this option with CAUTION.

☑ Enable Authentication

Authentication Policies

Priority	Policy Name	Expression	Profile
0	Authentication_Policy	ns_true	Citrix_AD_Authentication

Details

No item selected.

Comments

Figure 4-6 Configure NetScaler Gateway Virtual Server - Authentication tab

6 Click **Insert Policy** → **New Policy**.

7 In the Create Authentication Policy window, do the following:

   a **Name**: Enter a name for the authentication policy.

   b **Authentication Type**: Select **CERT**.

   c **Server**: Select **SymantecCert**.

   d To enter an expression, click **Add** and select **Named Expression** as **Logical_TRUE**. The system loads the Preview Expression as `ns_true`.

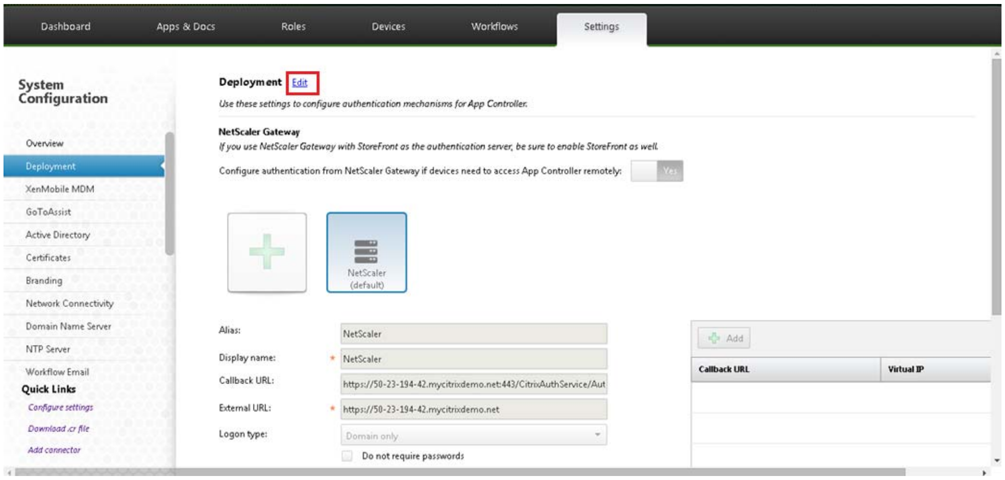
   e Click **OK** in the Configure Authentication Policy window.

8 Click **OK** in the Configure NetScaler Gateway Virtual Server window.

Configuring XenMobile App Controller

The XenMobile App Controller hosts the numerous applications for the various end-user devices. Complete the following steps to configure the authentication mechanism on the XenMobile App Controller:

1. Log into the XenMobile App Controller using your administrator credentials.
2. Click **Settings**. The system displays the Settings page.
3. Click **Deployment** on the left-hand side of the Settings page.
4. Click **Edit** to edit the authentication mechanism, and do the following:
   a. Delete the default **Callback URL**.
   b. Select **Certificate** as the **Logon type**.
   c. Select the **Do not require passwords** check box.



Use these settings to configure authentication mechanisms for App Controller.

If you use NetScaler Gateway with StoreFront as the authentication server, be sure to enable StoreFront as well.

Configure authentication from NetScaler Gateway if devices need to access App Controller remotely: Yes

Alias: NetScaler

Display name: * NetScaler

Callback URL: https://50-23-194-42.mycitrixdemo.net:443/CitrixAuthService/Aut

External URL: * https://50-23-194-42.mycitrixdemo.net

Logon type: Domain only

□ Do not require passwords

Figure 4-7 App Controller Deployment Screen

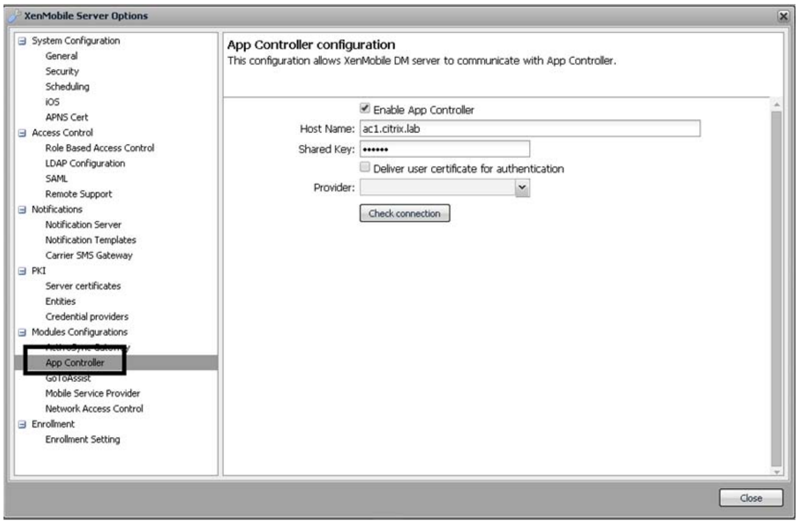
5. Click **Save**.

Configuring the XenMobile MDM for XenMobile App Controller

The user connects to the XenMobile App Controller using the XenMobile MDM.

Complete the following steps to configure the XenMobile MDM for the XenMobile App Controller:

1. Log into the XenMobile Device Manager console using your administrator credentials.
2. Click **Options**.
3. Under the **Modules Configurations** section, click **App Controller**.



App Controller configuration

This configuration allows XenMobile DM server to communicate with App Controller.

☑ Enable App Controller

Host Name: ac1.citrix.lab

Shared Key: ••••••

□ Deliver user certificate for authentication

Provider:

Figure 4-8 App Controller Configuration Screen

4 On the App Controller configuration page, do the following:

  a Select the **Deliver user certificate for authentication** check box.

  b Select the credential provider. See “Create a credential provider” on page 11.

5 Click **Close**.

6 You will need to configure and test the end-user mobile device, and deploy the package, using procedures in “Configuring Citrix® WorxHome” on page 33.

Chapter 5

Configuring Microsoft ActiveSync

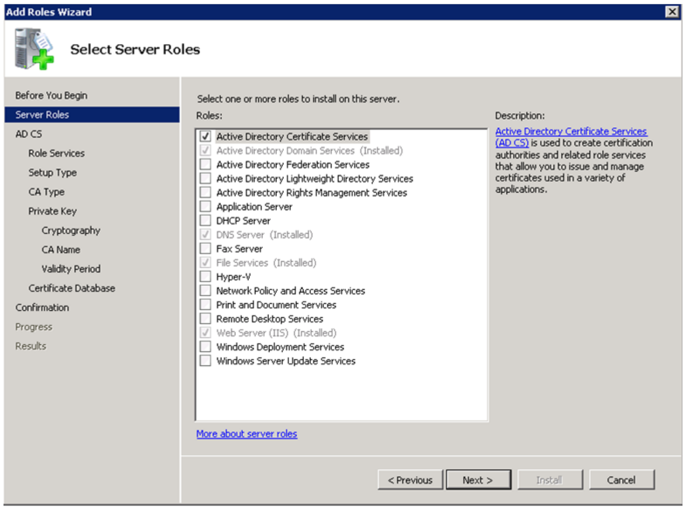
This chapter discusses how to configure the Microsoft Exchange server to allow users to synchronize their emails on their mobile devices.

Configuring Windows Server 2008 R2

Complete the following steps to configure the Windows Server 2008 R2 to use the Managed PKI certificate:

1 Log into the Windows Server 2008 R2 and launch the Add Roles wizard to configure the server.

2 Click **Server Roles**, select the **Active Directory Certificate Services** check box, and click **Next**.



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

Roles:

☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Application Server
☐ DHCP Server
☑ DNS Server (Installed)
☐ Fax Server
☑ File Services (Installed)
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Desktop Services
☑ Web Server (IIS) (Installed)
☐ Windows Deployment Services
☐ Windows Server Update Services

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Figure 5-1 Add Roles

3 Click **Role Services**, select the **Certification Authority** check box and click **Next**.

4 Click **Setup Type**, select **Enterprise**, and click **Next**.

5 Click **CA Type**, select **Root CA**, and click **Next**.

6 Select **Private Key**, select **Create a new private key**, and click **Next**.

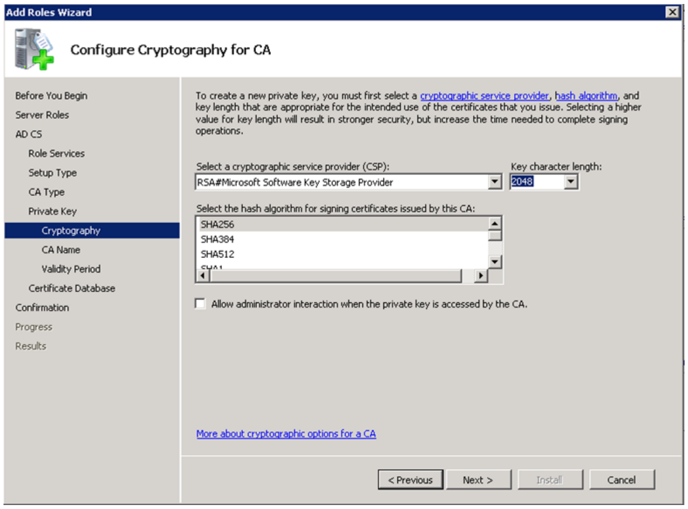
7 Click **Cryptography** and do the following:

   a Select a cryptographic service provider (CSP).

   b Select the key character length.

   c Select the hash algorithm for signing certificates issued by this CA.

   d Click **Next**.



To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

Key character length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512

□ Allow administrator interaction when the private key is accessed by the CA.

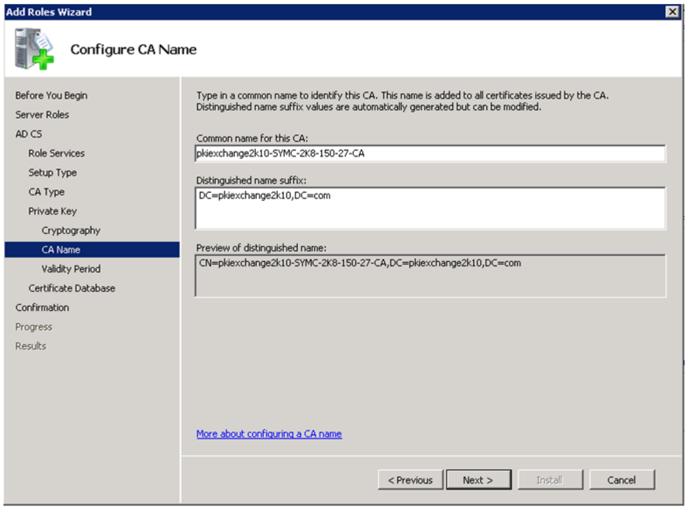
Figure 5-2 Configure Cryptography For CA

8 Click **CA Name** and do the following:

a Enter a **Common name for this CA**.

b Enter a **Distinguished name suffix**.

c The **Preview of distinguished name** field displays the preview of the common name and distinguished name. Verify the results and click **Next**.



Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: pkiexchange2k10-SYMC-2K8-150-27-CA

Distinguished name suffix: DC=pkiexchange2k10,DC=com

Preview of distinguished name: CN=pkiexchange2k10-SYMC-2K8-150-27-CA,DC=pkiexchange2k10,DC=com

Figure 5-3 Configure CA Name

9 Select **Validity Period**, enter the validity period for the certificate generated for this CA, and click **Next**.

10 Click **Next** and then **Install** to install the selected features.

11 Click **Close** to close the Add Roles wizard.

Configuring Microsoft Exchange Server 2010

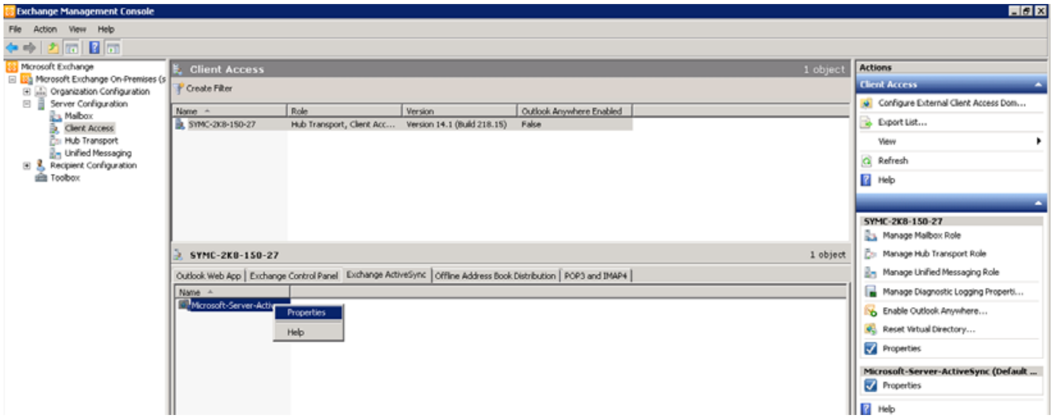
Complete the following steps to set up and configure the Microsoft Exchange Server 2010 for ActiveSync:

1 Click Start and launch the Exchange Management Console.

2 Click **Server Configuration** → **Client Access** → **Exchange ActiveSync** tab.

> **Note:** If the system does not display the **Server configuration** option, you need to relogin as another user with the appropriate privileges.

3 Right-click the ActiveSync profile and click **Properties**.

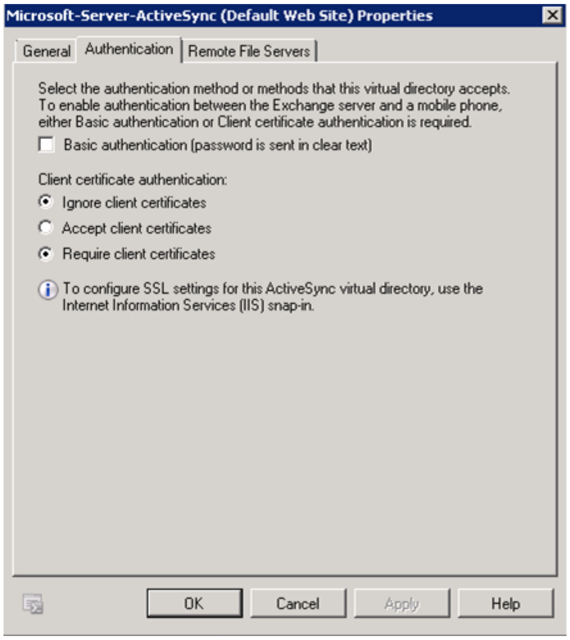


Name	Role	Version	Outlook Anywhere Enabled
SYMC-2K8-150-27	Hub Transport, Client Acc...	Version 14.1 (Build 218.15)	False

Figure 5-4 Exchange Management Console - Exchange Sync tab

4 In the Microsoft-Server-ActiveSync (Default Web Site) Properties window, select the **Authentication** tab.

5 Clear the **Basic Authentication (password is sent in clear text)** check box and select the **Require client certificates** check box.



Microsoft-Server-ActiveSync (Default Web Site) Properties

Select the authentication method or methods that this virtual directory accepts. To enable authentication between the Exchange server and a mobile phone, either Basic authentication or Client certificate authentication is required.

☐ Basic authentication (password is sent in clear text)

Client certificate authentication:

● Ignore client certificates

○ Accept client certificates

● Require client certificates

To configure SSL settings for this ActiveSync virtual directory, use the Internet Information Services (IIS) snap-in.

Figure 5-5 Microsoft-Server-ActiveSync (Default Web Site) Properties - Authentication Tab

6 Open the command prompt window and enter the following commands to enable client authentication:

```
Import-Module ServerManager
Add-WindowsFeature Web-Client-Auth
```

Configuring the Internet Information Services (IIS) Server

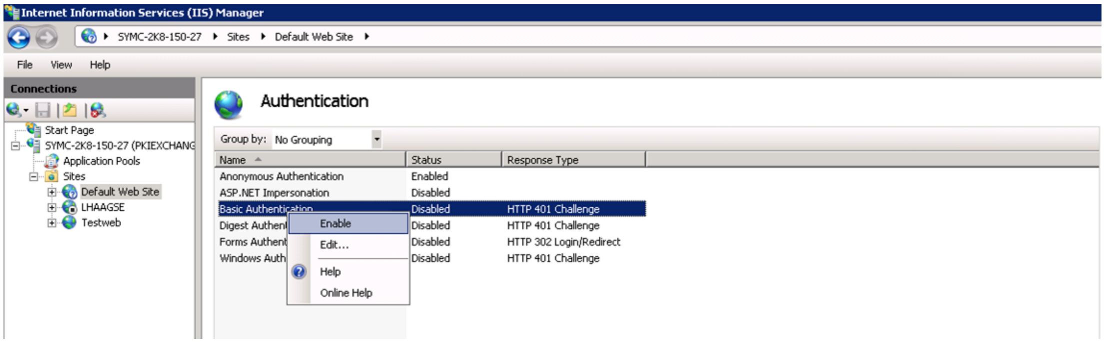
Complete the following steps to set up and configure the IIS sever for ActiveSync:

Note: IIS is not turned on by default when Windows is installed.

1 Launch the IIS Manager console from the Microsoft Management Console or from Administrative Tools in the Control Panel.

2 Click the IIS server and then click **Authentication**.

3 Right-click **Basic Authentication** and click **Enable**. Disable the other authentication modes.



Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authent	Disabled	HTTP 401 Challenge
Forms Authent	Disabled	HTTP 302 Login/Redirect
Windows Auth	Disabled	HTTP 401 Challenge

Figure 5-6 Basic Authentication - Enable

4 Open Windows Power Shell and run the following commands:

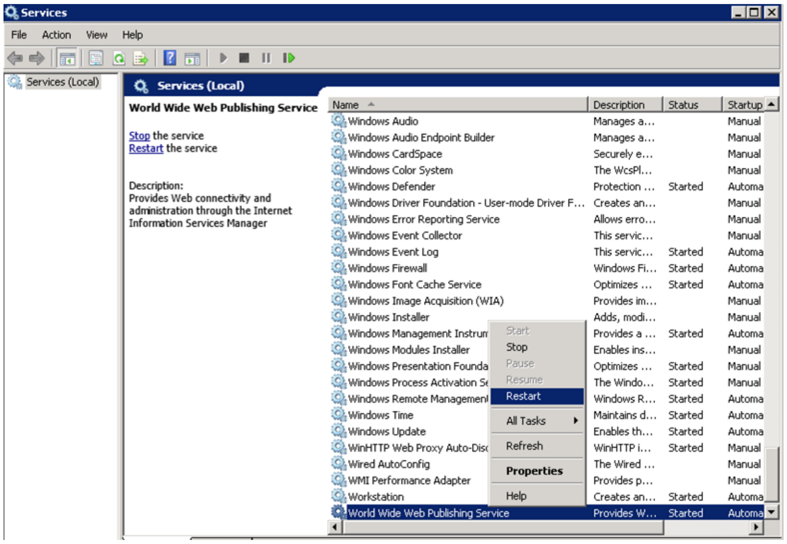
```
C:\Windows\Syswow64\inetsrv\appcmd.exe unlock config /section:client
```

```
C:\WINDOWS\SYSTEM32\INETSRV\APPCMD.EXE set config “Default Web Site” -
section:system.webServer/security/authentication/
clientCertificateMappingAuthentication /enabled:”True” /commit:apphost
```

```
iisreset /noforce
```

5 Click **Start** → **Control Panel** → **Administrative Tools** → **Services**.

6 Right-click **World Wide Web Publishing Service** and click **Restart**.



World Wide Web Publishing Service

Stop the service
Restart the service

Description:
Provides Web connectivity and administration through the Internet Information Services Manager

Name	Description	Status	Startup
Windows Audio	Manages a...		Manual
Windows Audio Endpoint Builder	Manages a...		Manual
Windows CardSpace	Securely e...		Manual
Windows Color System	The WcsPl...		Manual
Windows Defender	Protection ...	Started	Automa
Windows Driver Foundation - User-mode Driver F...	Creates an...		Manual
Windows Error Reporting Service	Allows erro...		Manual
Windows Event Collector	This servic...		Manual
Windows Event Log	This servic...	Started	Automa
Windows Firewall	Windows Fi...	Started	Automa
Windows Font Cache Service	Optimizes ...	Started	Automa
Windows Image Acquisition (WIA)	Provides im...		Manual
Windows Installer	Adds, modi...		Manual
Windows Management Instrum	Provides a ...	Started	Automa
Windows Modules Installer	Enables ins...		Manual
Windows Presentation Founda	Optimizes ...	Started	Manual
Windows Process Activation Se	The Windo...	Started	Manual
Windows Remote Management	Windows R...	Started	Automa
Windows Time	Maintains d...	Started	Automa
Windows Update	Enables th...	Started	Automa
WinHTTP Web Proxy Auto-Disc	WinHTTP i...	Started	Manual
Wired AutoConfig	The Wired ...		Manual
WMI Performance Adapter	Provides p...		Manual
Workstation	Creates an...	Started	Automa
World Wide Web Publishing Service	Provides W...	Started	Automa

Figure 5-7 World Wide Web Publishing Service

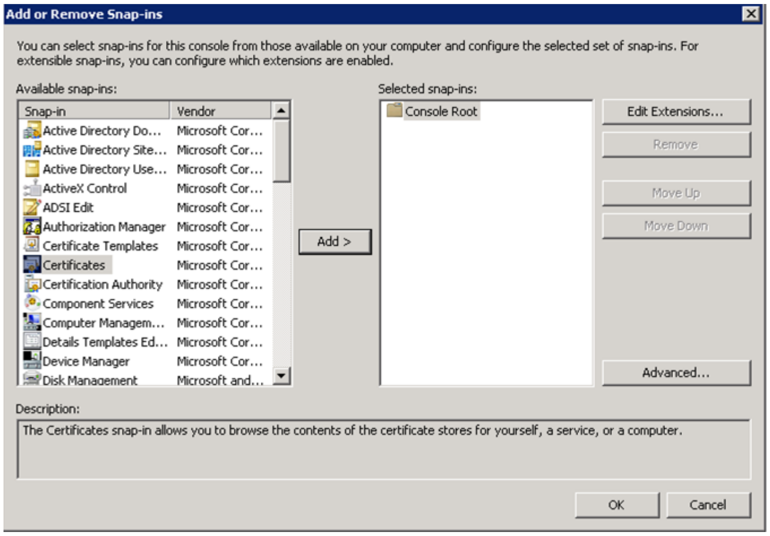
Configuring the Microsoft Management Console

Complete the following steps to add a certificate snap-in:

1 From your Windows Server 2008 R2, open the command prompt and type `mmc` to launch the Microsoft Management Console.

2 On the console, click **File** → **Add/Remove Snap-ins**.

3 In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Details Templates Ed...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

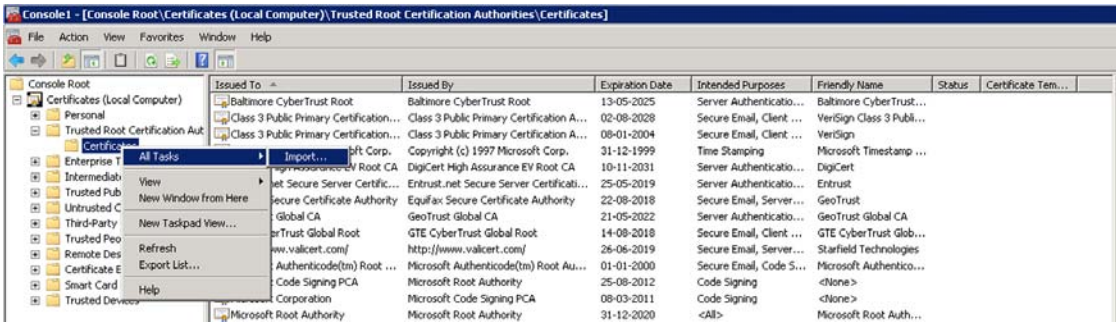
Figure 5-8 Add/Remove Snap-ins

4 In the Certificate snap-in window, select **Computer account**.

5 In the Select Computer window, select **Local Computer: (the computer this console is running on)** and click **Finish**.

6 Expand the **Certificates** snap-in and right-click **Certificates** under **Trusted Root Certification Authority**.

7 Select **All Tasks → Import** to import all the trusted CA certificates that you obtained from Symantec Managed PKI Web Services package.



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13-05-2025	Server Authenticatio...	Baltimore CyberTrust...		
Class 3 Public Primary Certification...	Class 3 Public Primary Certification A...	02-08-2028	Secure Email, Client ...	VeriSign Class 3 Publi...		
Class 3 Public Primary Certification...	Class 3 Public Primary Certification A...	08-01-2004	Secure Email, Client ...	VeriSign		
oft Corp.	Copyright (c) 1997 Microsoft Corp.	31-12-1999	Time Stamping	Microsoft Timestamp ...		
V Root CA	DigiCert High Assurance EV Root CA	10-11-2031	Server Authenticatio...	DigiCert		
et Secure Server Certific...	Entrust.net Secure Server Certificati...	25-05-2019	Server Authenticatio...	Entrust		
ecure Certificate Authority	Equifax Secure Certificate Authority	22-08-2018	Secure Email, Server...	GeoTrust		
Global CA	GeoTrust Global CA	21-05-2022	Server Authenticatio...	GeoTrust Global CA		
erTrust Global Root	GTE CyberTrust Global Root	14-08-2018	Secure Email, Client ...	GTE CyberTrust Glob...		
ww.valicert.com/	http://www.valicert.com/	26-06-2019	Secure Email, Server...	Starfield Technologies		
Authenticode(tm) Root ...	Microsoft Authenticode(tm) Root Au...	01-01-2000	Secure Email, Code S...	Microsoft Authentico...		
Code Signing PCA	Microsoft Root Authority	25-08-2012	Code Signing	<None>		
Corporation	Microsoft Code Signing PCA	08-03-2011	Code Signing	<None>		
Microsoft Root Authority	Microsoft Root Authority	31-12-2020	<All>	Microsoft Root Auth...		

Figure 5-9 Import Certificate

8 Select a certificate store from where you must import the certificates, and click **Next**. The system displays a message that the import was successful.

9 Repeat Step 7 and Step 8 for all the root certificates.

For intermediate certificates, right-click **Certificates** under **Intermediate Root Certification Authority** and repeat Step 7 and Step 8.

Configuring Microsoft Active Directory

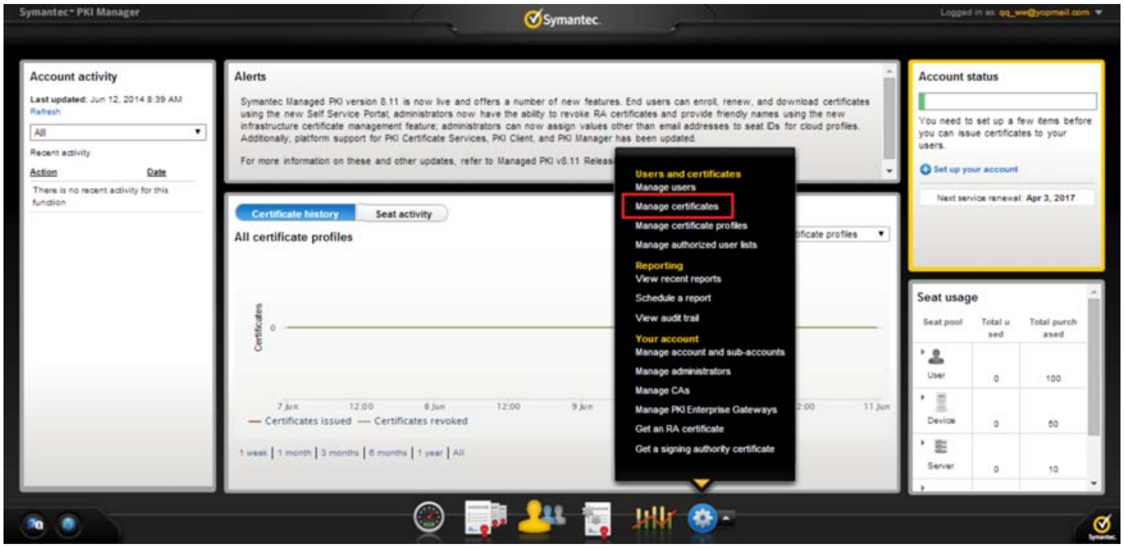
This section discusses how to download the device certificate for a user and map the certificate to the user in the corporate Active Directory.

Downloading the Device Certificate

The device certificate is mapped against the appropriate user in the Active Directory. Complete the following steps to download the device certificate:

1 Log into PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.

2 On the PKI Manager dashboard, click **Manage certificates** from the Tasks menu on the bottom navigation bar.



Symantec Managed PKI version 8.11 is now live and offers a number of new features. End users can enroll, renew, and download certificates using the new Self Service Portal; administrators now have the ability to revoke RA certificates and provide friendly names using the new infrastructure certificate management feature; administrators can now assign values other than email addresses to seat IDs for cloud profiles. Additionally, platform support for PKI Certificate Services, PKI Client, and PKI Manager has been updated.

For more information on these and other updates, refer to Managed PKI v8.11 Releas

Last updated: Jun 12, 2014 8:39 AM

There is no recent activity for this function

You need to set up a few items before you can issue certificates to your users.

Next service renewal: Apr 3, 2017

Seat pool	Total used	Total purchased
User	0	100
Device	0	50
Server	0	10

Figure 5-10 Manage Certificates

3 Select the root certificate and click **Download certificate**.

4 Save the certificate to a location in your system.

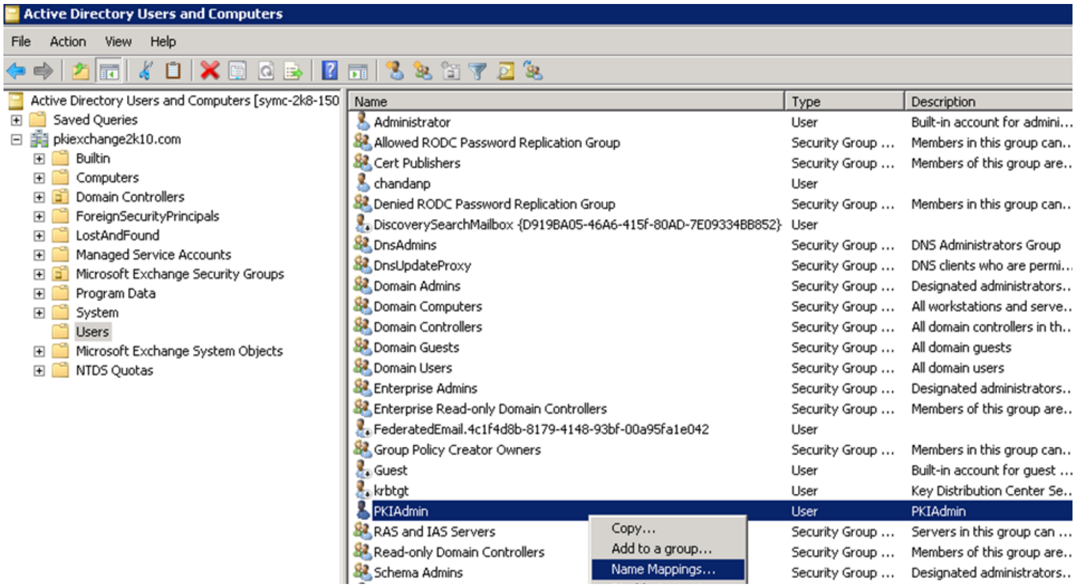
Mapping the Certificate to a User in your Active Directory

1 On the Windows Server 2008 R2, click **Start** → **Active Directory Users and Computers**.

2 Click **View** → **Advanced Features**.

3 Double-click **Users**.

4 Right-click on the appropriate user name and select **Name Mappings**.



Name	Type	Description
Administrator	User	Built-in account for admini...
Allowed RODC Password Replication Group	Security Group ...	Members in this group can..
Cert Publishers	Security Group ...	Members of this group are..
chandanp	User	
Denied RODC Password Replication Group	Security Group ...	Members in this group can..
DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}	User	
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators..
Domain Computers	Security Group ...	All workstations and serve..
Domain Controllers	Security Group ...	All domain controllers in th..
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators..
Enterprise Read-only Domain Controllers	Security Group ...	Members of this group are..
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	User	
Group Policy Creator Owners	Security Group ...	Members in this group can..
Guest	User	Built-in account for guest ...
krbtgt	User	Key Distribution Center Se..
PKIAdmin	User	PKIAdmin
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are..
Schema Admins	Security Group ...	Designated administrators..

Figure 5-11 Active Directory Users and Computers - Name Mappings

5 In the Security Identity Mapping window, click **Add** to select the device certificate that you downloaded in “Downloading the Device Certificate” on page 29

6 Click **Open** to verify the certificate details, and then click **OK** in the Add Certificate window.

7 Click **OK** in the Security Identity Mapping window to save the mapping of the certificate for the user.

Configuring the XenMobile MDM for ActiveSync

This section discusses how to configure the XenMobile MDM for to create and deploy a configuration policy for ActiveSync.

Creating an ActiveSync Configuration Policy

Complete the following steps to create an ActiveSync configuration policy:

1 Log into the XenMobile Device Manager console using your administrator credentials.

2 Click **Policies**.

3 Select the mobile device OS and then click **Configurations** → **New Configuration** → **Policies and Settings** → **Exchange ActiveSync configuration**.

4 In the Exchange ActiveSync configuration creation window, do the following:

a Complete the information required in the **General** tab.

b Complete the information required in the **Exchange ActiveSync** tab and configure the following specific settings:

- Select the **Use SSL** check box.
- Select **Symantec** as the **Identity credential (Keystore or PKI credential)**.

c Complete the information required in the **Policy** tab.

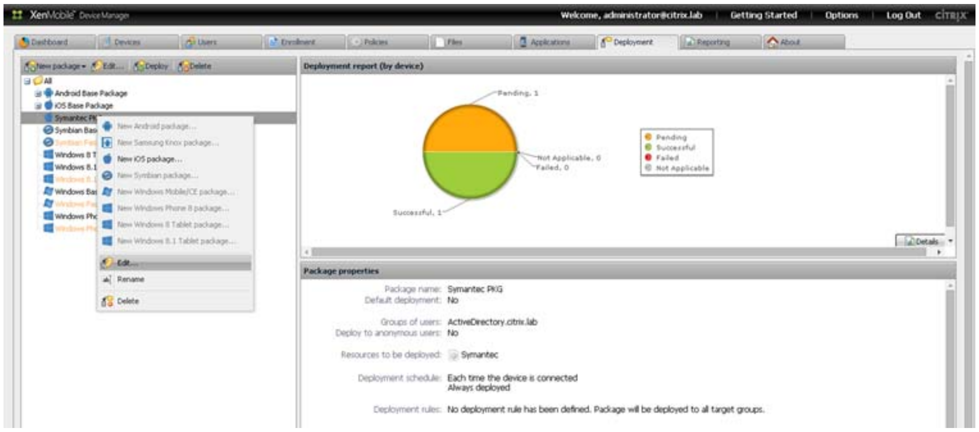
5 Click **Create** to create the new ActiveSync configuration policy.

Editing the Configuration Policy for ActiveSync

1 On the XenMobile Device Manager console, click **Deployment**.

2 Select the deployment package that you created when configuring the XenMobile MDM. See "Creating the Deployment Package" on page 12. The system displays the deployment report.

3 Right-click the deployment package and select **Edit**.



Package name: Symantec PKG
Default deployment: No

Groups of users: ActiveDirectory.citrix.lab
Deploy to anonymous users: No

Resources to be deployed: Symantec

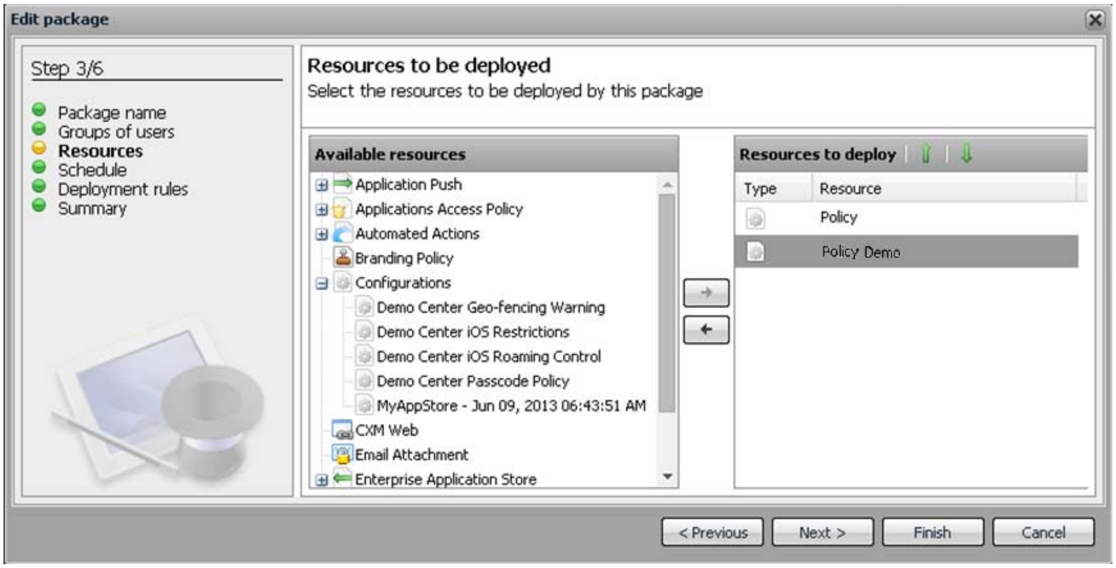
Deployment schedule: Each time the device is connected
Always deployed

Deployment rules: No deployment rule has been defined. Package will be deployed to all target groups.

Figure 5-12 Deployment

4 In the Edit Package window, click **Resources**.

5 Under **Available resources**, select the ActiveSync configuration policy and click → to add it to the **Resources to deploy** section. See "Creating an ActiveSync Configuration Policy" on page 30.



Resources to be deployed
Select the resources to be deployed by this package

Type	Resource
	Policy
	Policy Demo

Figure 5-13 Resources to Deploy

6 Click **Finish** to update the package.

7 You will need to configure and test the end-user mobile device, and deploy the package, using procedures in "Configuring Citrix® WorxHome" on page 33.

Configuring Citrix® WorxHome

This chapter discusses how to test the configuration by enrolling a mobile device and attempting to access the configured applications on the Citrix App Controller through NetScaler Gateway. It also discusses accessing the Microsoft Exchange server for email from the mobile device.

Prerequisities

- You must have downloaded and installed the Citrix WorxHome application on your mobile device. The Citrix WorxHome application is available in Google Play or App Store.
- The URL for the XenMobile server.
- End-user enterprise user name and password.

Configuring WorxHome to Register with the MDM

You must configure WorxHome in order to allow the user's mobile device to connect to the MDM for enrollment.

Enrolling Your Device

Complete the following procedure to enroll the user's device and install the deployment package.

1. Open the Citrix WorxHome application on your mobile device.
2. Enter the URL for the XenMobile server.
3. Tap **Next**. The device searches for the network and authorizes itself to the server.
4. Tap **Yes** to enroll your mobile device.
5. Enter your enterprise user name and password. After successfully logging in, the enrollment process initiates and the MDM pushes the certificate to the device.
6. Tap **Install** to install the certificate.
7. In the Install Profile dialog box, tap **Install Now.**
8. Enter your device passcode.
9. Tap **Install Now**. Once the certificate is installed, the device will be managed by the MDM.

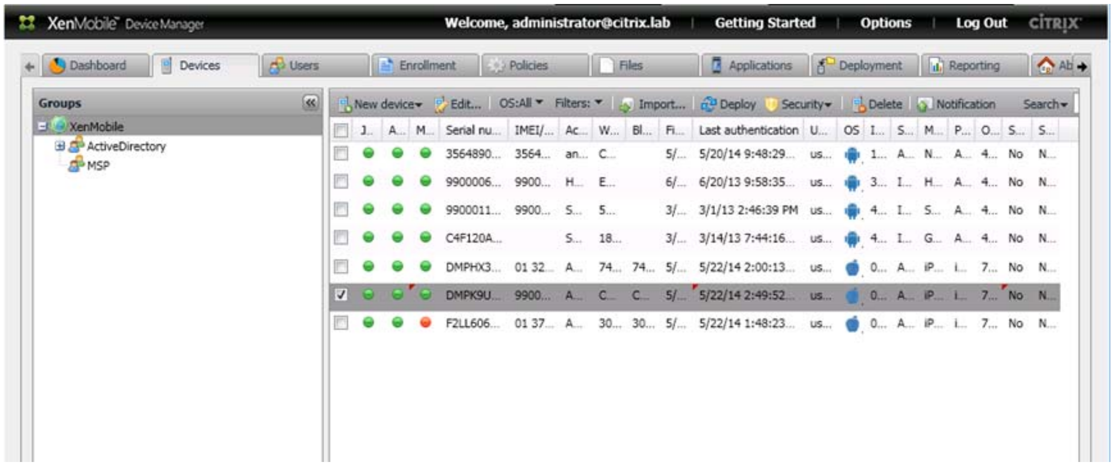
Note: To view the certificate details, tap **Settings** → **General** → **Profile** → **Symantec**. On the certificate, tap **More Details**.

Testing the Configuration

Complete the following procedure to view the status of the deployment package:

1 Log into the Citrix XenMobile console using your administrator credentials.

2 On the Administrator dashboard, click **Devices**.



□	J...	A...	M...	Serial nu...	IMEI/...	Ac...	W...	Bl...	Fi...	Last authentication	U...	OS	I...	S...	M...	P...	O...	S...	S...
□	●	●	●	3564890...	3564...	an...	C...		5/...	5/20/14 9:48:29...	us...		1...	A...	N...	A...	4...	No	N...
□	●	●	●	9900006...	9900...	H...	E...		6/...	6/20/13 9:58:35...	us...		3...	I...	H...	A...	4...	No	N...
□	●	●	●	9900011...	9900...	S...	5...		3/...	3/1/13 2:46:39 PM	us...		4...	I...	S...	A...	4...	No	N...
□	●	●	●	C4F120A...		S...	18...		3/...	3/14/13 7:44:16...	us...		4...	I...	G...	A...	4...	No	N...
□	●	●	●	DMPHX3...	01 32...	A...	74...	74...	5/...	5/22/14 2:00:13...	us...		0...	A...	iP...	i...	7...	No	N...
☑	●	●	●	DMPK9U...	9900...	A...	C...	C...	5/...	5/22/14 2:49:52...	us...		0...	A...	iP...	i...	7...	No	N...
□	●	●	●	F2LL606...	01 37...	A...	30...	30...	5/...	5/22/14 1:48:23...	us...		0...	A...	iP...	i...	7...	No	N...

Figure 6-1 XenMobile Device Manager dashboard

3 Select a device to view the profile information and click **Edit**.

4 Click the **Deployment** tab to view the deployment status of the package. The status should show **Success**.

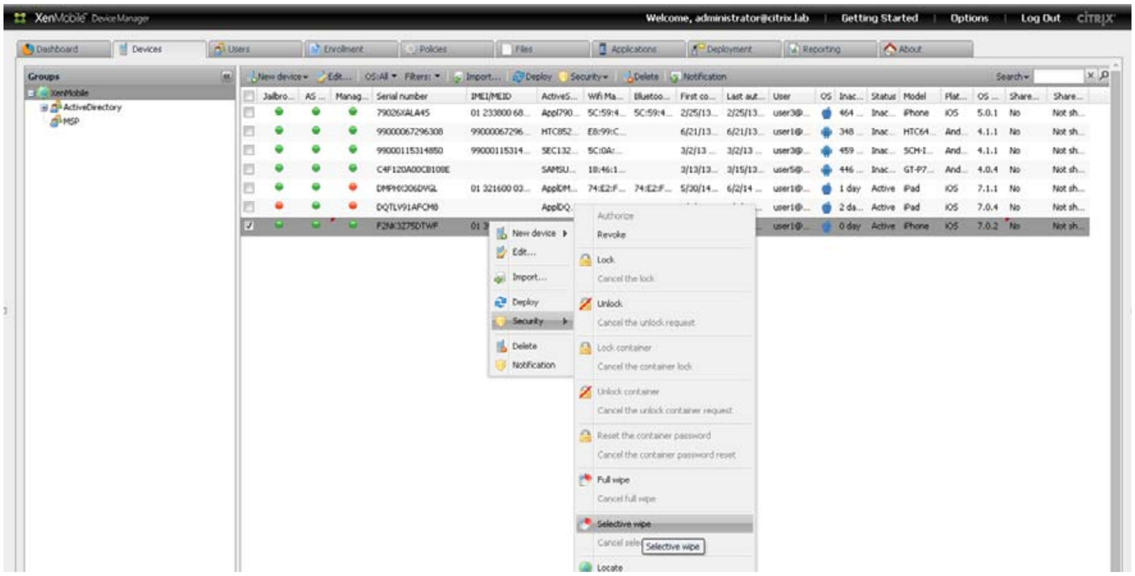
Redeploying the package

At times, you may need to redeploy a package (for example, after you edit a configuration policy). The following procedure describes how to redeploy a package:

1 Log into the Citrix XenMobile console using your administrator credentials.

2 On the Device Manager console, click **Devices**.

3 Right-click a device, select **Security** → **Selective wipe**.



□	Jailbro...	AS ...	Manag...	Serial number	IMEI/MEID	ActiveS...	Wifi Ma...	Bluetoo...	First co...	Last aut...	User	OS	Inac...	Status	Model	Plat...	OS ...	Share...	Share...
□	🟢	🟢	🟢	79026XALA445	01 233800 68...	Appl790...	5C:59:4...	5C:59:4...	2/25/13...	2/25/13...	user3@...		464 ...	Inac...	iPhone	iOS	5.0.1	No	Not sh...
□	🟢	🟢	🟢	99000067296308	99000067296...	HTC852...	E8:99:C...		6/21/13...	6/21/13...	user1@...		348 ...	Inac...	HTC64...	And...	4.1.1	No	Not sh...
□	🟢	🟢	🟢	99000115314850	99000115314...	SEC132...	5C:0A:...		3/2/13 ...	3/2/13 ...	user3@...		459 ...	Inac...	SCH-I...	And...	4.1.1	No	Not sh...
□	🟢	🟢	🟢	C4F120A00CB108E		SAMSU...	18:46:1...		3/13/13...	3/15/13...	user5@...		446 ...	Inac...	GT-P7...	And...	4.0.4	No	Not sh...
□	🟢	🟢	🔴	DMPHX306DVGL	01 321600 03...	ApplDM...	74:E2:F...	74:E2:F...	5/30/14...	6/2/14 ...	user1@...		1 day	Active	iPad	iOS	7.1.1	No	Not sh...
□	🔴	🟢	🔴	DQTLV91AFCM8		ApplDQ...					user1@...		2 da...	Active	iPad	iOS	7.0.4	No	Not sh...
☑	🟢	🟢	🟢	F2NK3275DTWF	01 3						user1@...		0 day	Active	iPhone	iOS	7.0.2	No	Not sh...

Figure 6-2 Redeploy a package

Verifying Your Device Works for NetScaler Gateway

1. Complete the steps in "Enrolling Your Device" on page 33 to enroll your device and install the deployment package.
   The system installs the provisioned certificates on the device.
2. Connect to the NetScaler Gateway from the device.
   Based on this authentication, the end-user's mobile device is allowed access to the corporate network through a secure communication.

Verifying Your Device Works for ActiveSync

1. Open the Citrix WorxHome application on your mobile device.
2. After you enroll your device, tap **Settings** → **General** → **Profiles**.

   If you configured a credential provider and configured an ActiveSync policy, you will see two Symantec profiles. If you configured only an ActiveSync policy, you will see only one Symantec profile that can be used for both, client authentication and ActiveSync configuration.
3. Tap **Settings** → **Mail, Contacts, Calendars**. The mail settings have been pushed to the device from the MDM.
4. Tap the account that you configured on the Microsoft Exchange server. After the connection to the mail server is verified, the mail settings are synchronized with the device.
5. Tap the mail box to view your emails.