Symantec™ Managed PKI®

Integration Guide for Citrix® Netscaler VPN

Symantec

Symantec™ Managed PKI Integration Guide for Citrix® NetScaler VPN

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 June 11, 2015

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

https://www.symantec.com/contactsupport

Contents

Chapter 1

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 mobile devices such as laptops, smartphones, and tablets. However, you need to be able to trust the end users accessing your systems, and the mobile device they use, no matter if you have provided their devices or if they are using their own mobile devices.

Symantec Managed PKI's digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from a few to thousands of devices, and its in-the-cloud solution provides quick deployment and easy management while also offering Symantec's industry leading security that is unmatched by in-house PKI solutions.

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

This document describes how to integrate Managed PKI 8.13 or higher certificates with the Citrix® NetScaler VPN. This integration allows user devices to securely access the company's data and applications through the Citrix® NetScaler VPN connection. The procedures in this guide assume that these user devices are not managed using any Mobile Device Management (MDM) software.

If your company has the necessary infrastructure to implement an MDM, you can manage user devices with an MDM, such as the Citrix® XenMobile MDM. For information on integrating Managed PKI 8.13 or higher certificates with user devices managed by Citrix® XenMobile MDM, see *Integrating Symantec Managed PKI with Citrix XenMobile Mobile Device Management Guide*.

Partner Information

These procedures have been tested on the following platform:

Table 1-1 Partner Information

Partner Name	Citrix® Systems
Product Name and Version	Citrix® NetScaler VPX 10.5

How the Citrix NetScaler VPN Works

The following diagram describes how the Managed PKI certificates integrate with Citrix NetScaler VPN to provide secure authentication.

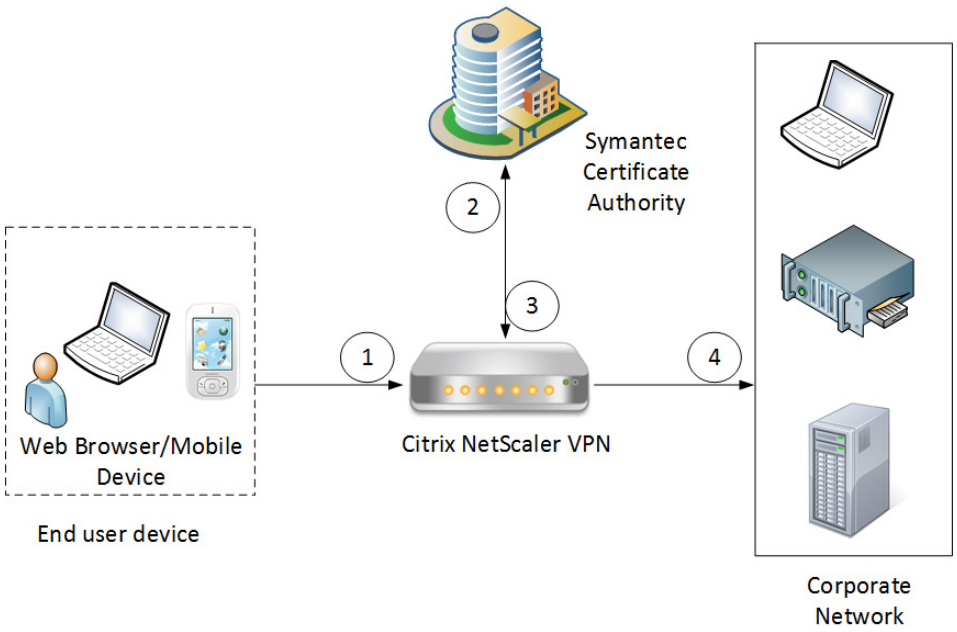

Figure 1-1 Authenticating Citrix NetScaler VPN with a Managed PKI certificate

1. The end-user device accesses the corporate network through the Citrix NetScaler VPN. In this process, the user device presents a Managed PKI certificate to the VPN for authentication.
2. Depending on how the VPN is configured, it attempts to obtain the status of the certificate:
   - If Online Certificate Status Protocol (OCSP) is configured, the VPN communicates to the Symantec CA to obtain the real-time status of the certificate.
   - If Certificate Revocation List (CRL) is configured, the VPN communicates to the Symantec CA to obtain the status of the certificate based on the most recent certificate revocation list. CRLs are updated on a regular basis.
3. When the Citrix NetScaler VPN receives the certificate status, it authenticates the end-user's certificate based on the CAs it has been configured to trust.
4. If this authentication succeeds, the end user device is allowed access to the corporate network, and the Citrix NetScaler VPN secures communication with the corporate network.

Chapter 2

Integrating Managed PKI with Citrix® NetScaler VPN

This chapter discusses how to integrate your Managed PKI account with Citrix NetScaler VPN.

Integration Workflow

This section describes the tasks that you must perform to set up the Symantec Managed PKI account and integrate the Managed PKI certificates with Citrix NetScaler VPN.

- Task 1, "Set up your Managed PKI 8.x account" on page 3
- Task 2, "Create a Managed PKI Client Authentication certificate profile" on page 3
- Task 3, "Download the root CA certificate" on page 6
- Task 4, "Add users to the certificate profile" on page 6
- Task 5, "Have the user enroll for and pick up the certificate" on page 7

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 must 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 must 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 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 a Managed PKI Client Authentication certificate profile

Managed PKI uses a certificate profile to define issued certificates. To issue certificates that can be used for the NetScaler VPN, you first create the certificate profile that will define the certificates you will issue to your end users. The end user certificate will be installed on the user's device and assist in authenticating on the VPN. After the device authentication succeeds, the user can access the corporate network.

Complete the following steps to create your Managed PKI certificate profile:

1 Log into PKI Manager using your administrator certificate and when prompted, enter the PIN for PKI Client.

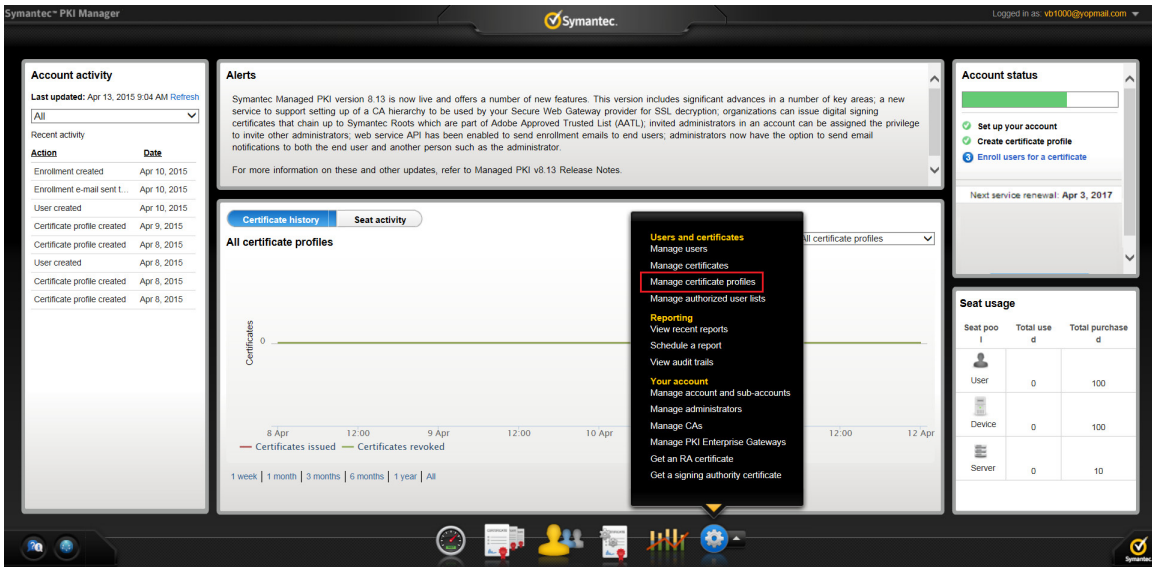

Figure 2-1 Manage Certificate Profile

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

3 Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page.

The Create profile page appears.

4 Select whether you will issue the certificates in **Test mode** or **Production mode**, and click **Continue**.

5 Select **Client Authentication** as the certificate template and click **Continue**.

The Customize certificate options page appears.

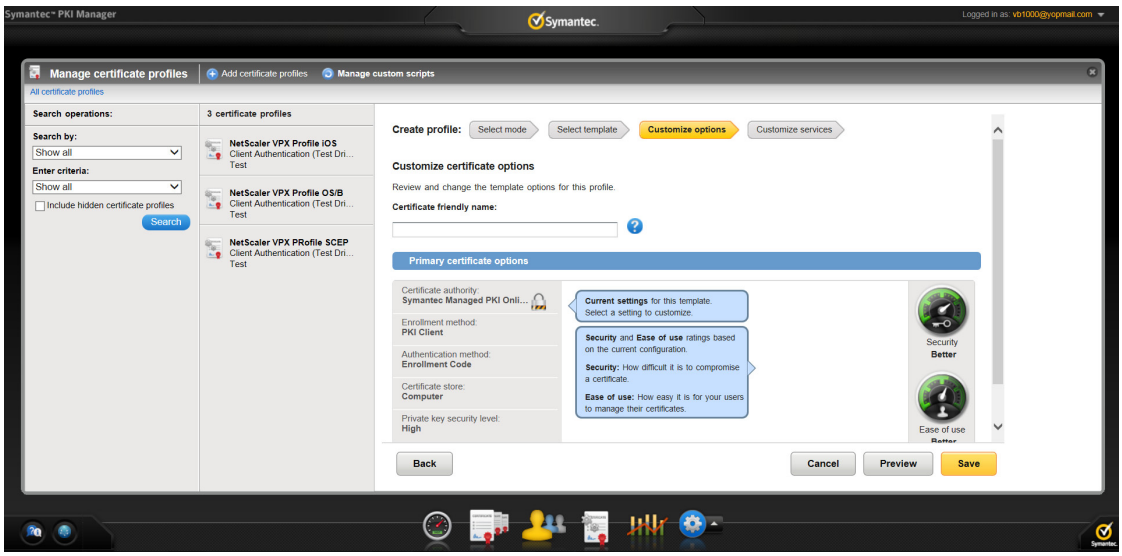

Figure 2-2 Customize certificate options

6 In the Customize certificate options page, edit the following fields:

a In the **Certificate friendly name** field, enter a certificate profile name. For example, NetScaler VPX profile OS/B.

b Select the appropriate **Enrollment method** from the following:

- Select **OS/browser** if your user will enroll for certificates using the desktop or device browser.
- Select **SCEP** if your user will enroll for certificates using the Simple Certificate Enrollment Protocol.
- Select **PKI Client** if your user will enroll for certificates using the Symantec PKI Client.

7 Click **Advanced options** to view or edit additional certificate options listed in Table 2-1.

Table 2-1 Advanced certificate options

Option	Configuration
Subject DN	
Common Name (CN)	In the **Source for the field's value** field, select one of the following options: ■ PKI Manager (entered/uploaded by administrator) ■ Entered by user during enrollment In the **Required** field, select **Yes** or **No** to identify if CN must be a mandatory field in certificate enrollment.
Organization Unit (OU)	In the **Source for the field's value** field, select one of the following options: ■ PKI Manager (entered/uploaded by administrator) ■ Entered by user during enrollment ■ Fixed value. If you select this option, also enter the value of the OU in the resulting **Fixed value** field. In the **Required** field, select **Yes** or **No** to identify if OU must be a mandatory field in certificate enrollment.
Organization (O)	Locked to a fixed value.
SubjectAltName	
Other Name (UPN)	In the **Source for the field's value** field, select one of the following options: ■ PKI Manager (entered/uploaded by administrator) ■ Entered by user during enrollment ■ Fixed value. If you select this option, also enter the value of the OU in the resulting **Fixed value** field.

Note: Before saving a certificate profile, you can customize it further by setting the fields in the **Additional certificate options** section, such as Validity Period, Key size, Signing algorithm, and so on.

8 Click **Save**.

After you save a certificate profile, you can also customize it further, such as adding custom scripts, and customizing languages or e-mail notifications on this page.

Task 3. Download the root CA certificate

Complete the following steps to download the root CA certificate:

1. Log into PKI Manager using your administrator certificate and when prompted, enter the PIN for PKI Client.
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 required location on your system.

Task 4. Add users to the certificate profile

You must add the user to the certificate profile in PKI Manager before the user can enroll for and pick up a certificate.

1. Log into PKI Manager using your administrator certificate and when prompted, enter the PIN for PKI Client.
2. On the PKI Manager dashboard, click **Manage users** from the Tasks menu on the bottom navigation bar.
3. Click **Add users** from the top of the resulting Manage users page.
4. Complete one of the following options:
   - If you are adding a single user to the profile, select **A single user**, enter the end user's seat ID (typically, the user's e-mail address) in the **Seat ID** field, and then click **Continue**.
     - Enter the **First Name** and **Last Name** of the user, select **I want to enroll this user for a certificate**, and then click **Continue**.
   - If you are adding several users at one time to the profile, select **multiple users**, click **Choose**, and upload a comma-separated value (.csv) file with your user data.
5. In the **certificate profile** field, select the certificate profile that you created in Task 2, "Create a Managed PKI Client Authentication certificate profile" on page 3 and click **Continue**.
6. Enter the **Other Name (UPN)**, **Department**, and **Email**, and optionally select **Have the system send the enrollment email to the user** and click **Continue**.

   The enrollment link is displayed with the enrollment code required by the end user for authentication during enrollment. Symantec recommends that you send the enrollment code to the end user separately from the enrollment link, and that you do not send the enrollment code by e-mail.

Note: The enrollment link is not displayed if you select **Have the system send the enrollment email to the user**.

Task 5. Have the user enroll for and pick up the certificate

After you add a user to the certificate profile, the user must enroll for and pick up the certificate. The following are the steps a user completes to pick up certificates for different enrollment methods.

Table 2-2 Steps for picking up certificates

Enrollment Method	How Certificates are Picked Up
OS/browser or SCEP	**Supported Browsers**: ■ **Windows 7**–Internet Explorer and Firefox ■ **Apple OS X**–Safari and Firefox For supported browser versions, refer to the Managed PKI documentation. 1 Click the enrollment link received in an e-mail or paste it into your browser. 2 Enter the e-mail address used for enrollment and click **Continue**. 3 Enter the enrollment code (provided by the administrator or received in an e-mail) and click **Continue**. This step authenticates the end user to ensure that the correct user picks the certificate. 4 Click **Continue**. 5 Click **Install certificate** to install the certificate.
PKI Client	If PKI Client is not already installed on the user's machine, the user will be prompted to install it during enrollment. 1 Click the enrollment link in the e-mail or paste it into your browser. 2 Enter the e-mail address used for enrollment and click **Continue**. 3 Enter the enrollment code (provided by the administrator or received in an e-mail) and click **Continue**. This step authenticates the end user to ensure that the correct user picks the certificate. 4 Click **Continue**. 5 Click **Install Certificate**. 6 Enter the PIN for the certificate store (PKI Client) when prompted, and click **OK**. (The user sets the PIN when installing PKI Client on the device.)

Chapter 3

Configuring Citrix® NetScaler Gateway

This chapter discusses how to configure the Citrix NetScaler Gateway to authenticate a user's device with a Managed PKI certificate. It also discusses how to configure the Citrix XenMobile App Controller so that an authenticated user device can access the corporate network.

You must complete the following procedures to configure the Citrix NetScaler VPN:

- "Configuring the NetScaler Gateway" on page 9
- "Configuring the XenMobile App Controller" on page 14

Configuring the NetScaler Gateway

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

Task 1. Uploading the CA certificate

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

1 Log into the NetScaler Gateway using your administrator credentials.

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

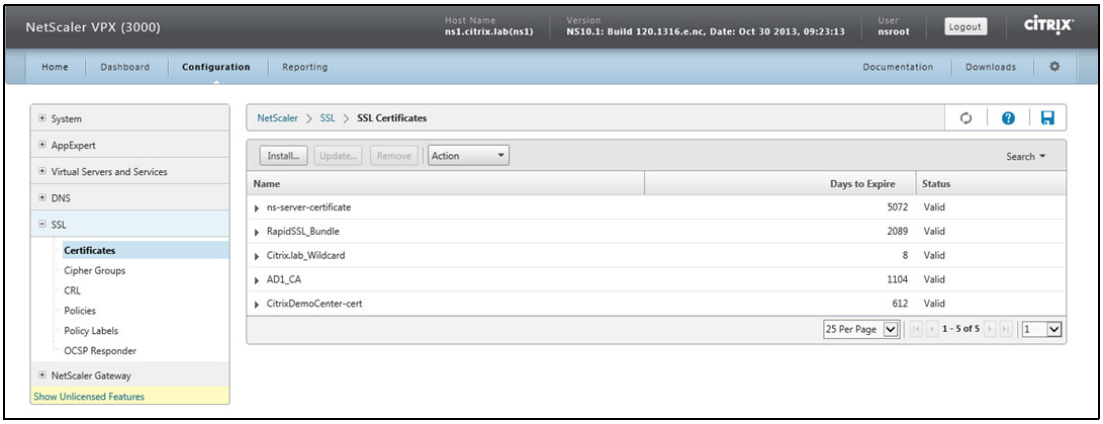

Figure 3-1 SSL Certificates

3 Click **Install**. The Install Certificate dialog box appears.

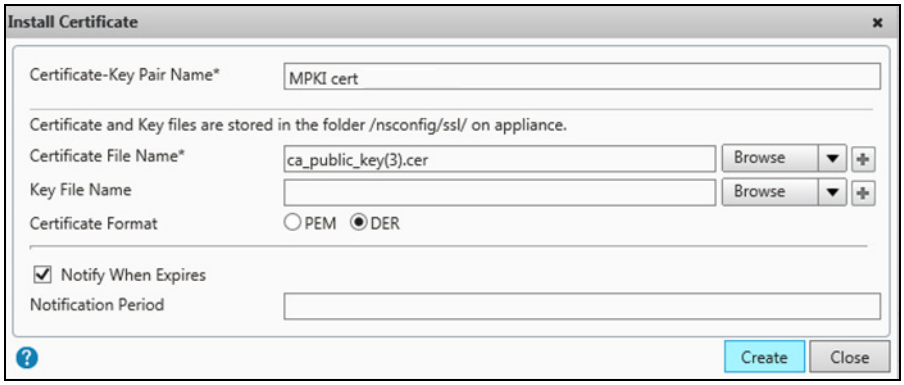

Figure 3-2 Install Certificate dialog box

4 In the Install Certificate dialog box, edit the following fields:

   a In the **Certificate-Key Pair Name** field, enter a friendly certificate name.

   b In the **Certificate File Name** field, click **Browse** and select **Local** or **Appliance** to browse to the location where you downloaded and saved the root CA certificate. (For details on downloading the root CA certificate, see Task 3, "Download the root CA certificate" on page 6.)

   c In the **Certificate Format** field, select **DER**.

   d If you want the NetScaler Gateway to send you notifications when a certificate is due to expire, select **Notify When Expires**, and in the **Notification Period** field, enter the number of days before certificate expiry when the administrator must be notified.

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

   To view the details of the newly uploaded certificate, click the arrow next to the certificate name.

Task 2. Configuring the NetScaler Gateway server

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

1 Log into the NetScaler Gateway using your administrator credentials.

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

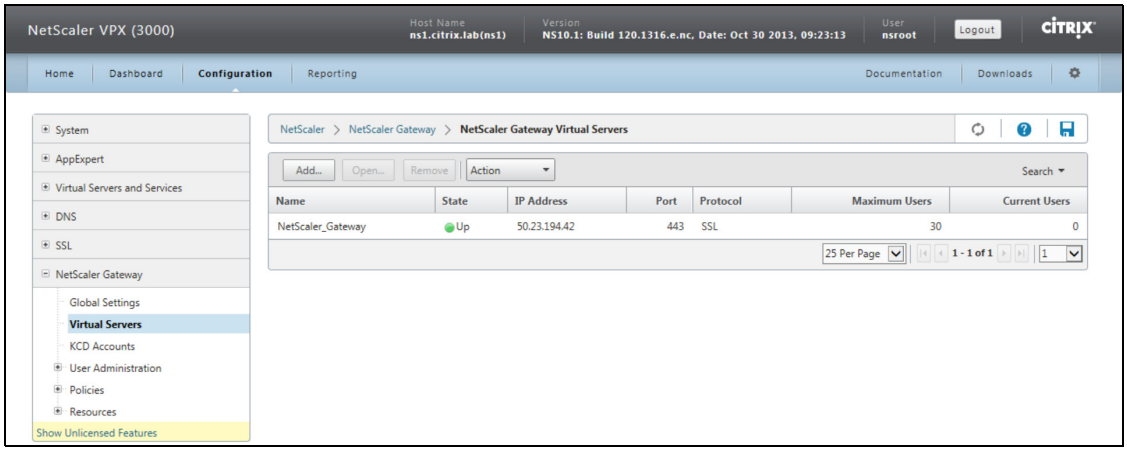

Figure 3-3 Configure NetScaler Gateway Virtual Server

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

Loading the applet may take a few minutes.

4 Click **Allow** if a Security Warning pop-up is displayed requesting access to the applet or web site.

The Configure NetScaler Gateway Virtual Server dialog box is displayed.

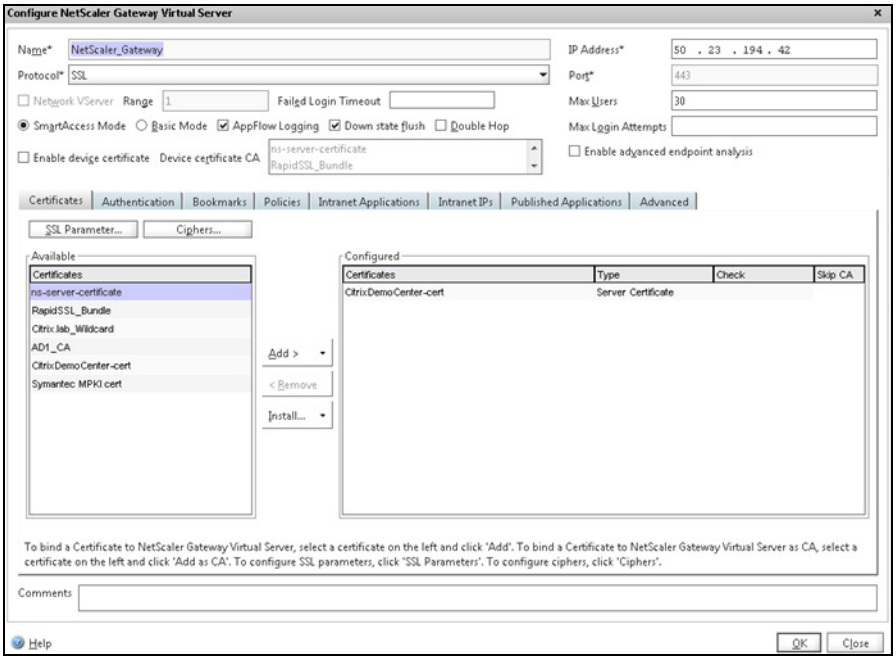

Figure 3-4 Configure NetScaler Gateway Virtual Server–Certificates tab

5 In the **Certificates** tab, edit the following fields:

- **a** In the **Available** section, click **Certificates** and select the CA certificate that you uploaded in Task 1, "Uploading the CA certificate" on page 9.
- **b** Click the arrow next to **Add** and then select **as CA**.

  The newly added CA certificate appears in the **Configured** section.
- **c** In the **Check** column of the **Configured** section, select **OCSP Optional** from the drop-down list.

6 Click **SSL Parameter**.

The Configure SSL Params dialog box is displayed.

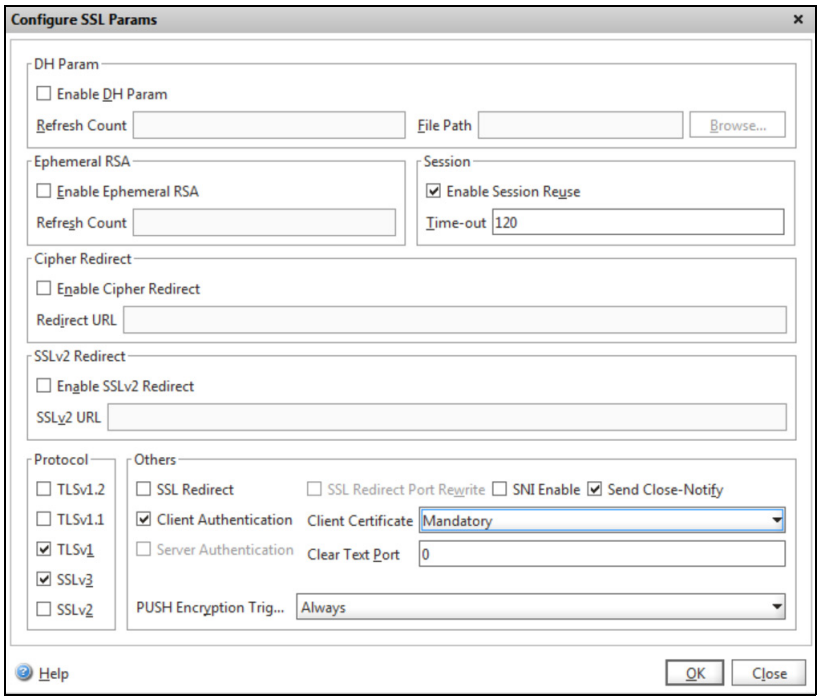

Figure 3-5 Configure SSL parameters

7 In the **Others** section of the Configure SSL Params dialog box, edit the following fields:

   a Select **Client Authentication**.

   b Set **Client Certificate** as **Mandatory** to make authentication stricter. This enforces authentication of the user's device using only the certificate.

   c Click **OK**.

   The Configure SSL Params dialog box is closed.

8 In the Configure NetScaler Gateway Virtual Server dialog box (Figure 3-4), click the **Authentication** tab.

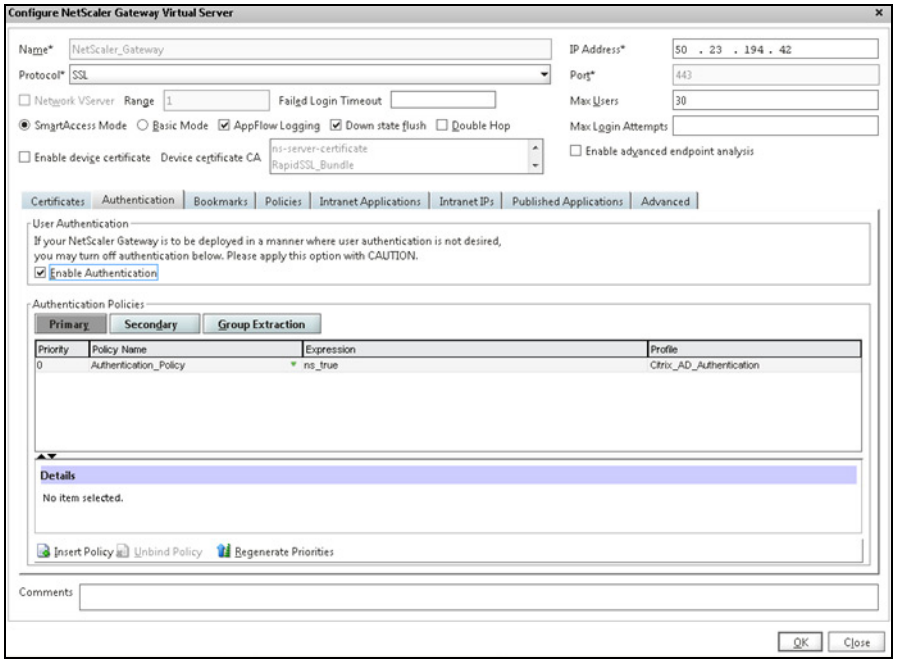

Figure 3-6 Configure NetScaler Gateway Virtual Server–Authentication tab

9 Click **Insert Policy → New Policy** to add a new authentication policy.

The Create Authentication Policy dialog box is displayed.

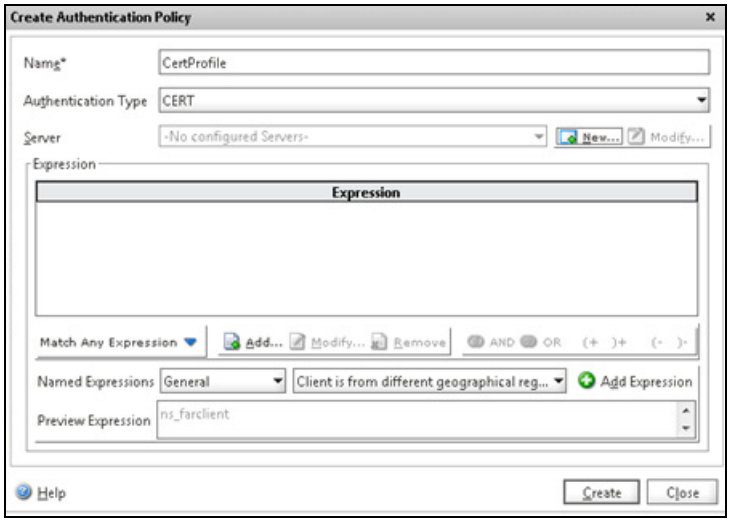

Figure 3-7 Create Authentication Policy

10 In the Create Authentication Policy dialog box, edit the following fields:

- **a** In the **Name** field, enter a unique name for the authentication policy.
- **b** In the **Authentication Type** field, select **CERT**.
- **c** In the **Server** field, select the certificate that you configured in Step 5.
- **d** In the **Expression** section, click **Add** and enter **ns_true** as the expression value.

e Click **OK**.

The new authentication policy is created and the dialog box closes.

11 In the Configure NetScaler Gateway Virtual Server dialog box (Figure 3-4), click **OK** to complete the configuration process.

Configuring the XenMobile App Controller

The XenMobile App Controller hosts applications for the 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 the **Settings** menu and then click **Deployment** from the left pane.

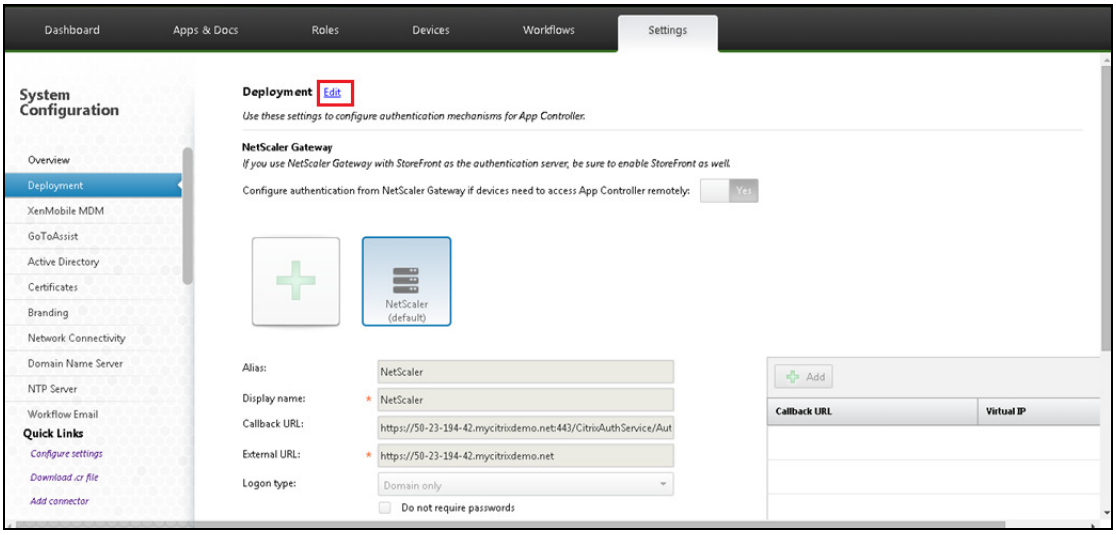

Figure 3-8 XenMobile App Controller Deployment

3 Click **Edit** to modify the deployment settings. Edit the following fields:

a In the **Callback URL** field, delete the displayed default value.

b In the **Logon type** field, select **Certificate**.

c Select **Do not require passwords**.

4 Click **Save**.

Chapter 4

Connecting to VPN

This chapter discusses how users can securely connect their preferred devices to the Citrix NetScaler VPN Gateway and access the company's protected applications and websites.

Contact your company's IT Help Desk or system administrator to obtain the URL to the Citrix NetScaler VPN.

Note: If the user devices are managed using an MDM such as Citrix® XenMobile MDM, you must install the **Citrix Receiver** application on the user device and configure it to access the Citrix Worx Home application. For details, see *Integrating Symantec Managed PKI with Citrix XenMobile Mobile Device Management Guide*.

Users can connect their non-managed devices to the Citrix NetScaler VPN Gateway in either of the following ways:

- "Connecting with Citrix Worx Home Application" on page 15
- "Connecting with the Browser" on page 16

Connecting with Citrix Worx Home Application

This section describes the workflow for connecting a non-managed device to the corporate network using the Citrix Worx Home application.

1. Download and install the Citrix Worx Home application on your mobile device. The Citrix Worx Home application is available in the Google Play or App Store.
2. Open the Citrix Worx Home application and enter the URL of the corporate network.
3. The user device presents a Managed PKI certificate to the Citrix NetScaler VPN for authentication.
4. The Citrix NetScaler VPN may be configured to obtain the certificate status from the Symantec CA using either Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL).
5. The Citrix NetScaler VPN authenticates the end-user's certificate based on the CAs it has been configured to trust.
6. If this authentication succeeds, the end user device is allowed access to the corporate network, and the Citrix NetScaler VPN secures communication with the corporate network.

Connecting with the Browser

Table 4-1 lists various device types and the procedure an end user follows to connect a non-managed device to the Citrix NetScaler Gateway using the browser.

Table 4-1 Steps for connecting various device types to the VPN

Device Type	Connection Procedure
■ iOS ■ Android ■ Desktop/laptop (without PKI Client)	1 Open the browser on the device where the Managed PKI certificate is installed. 2 Access the URL to the Citrix NetScaler VPN. The browser prompts you to select the certificate that will authenticate you on the VPN URL. 3 Select the certificate and click **OK**. The Citrix NetScaler VPN communicates with the Symantec CA to authenticate the certificate. If the authentication succeeds, the VPN connection is established. The start-up screen displays the applications that are available to your user account. Tap or double-click an application to open and to use it.
Desktop/laptop (with PKI Client)	1 Open the browser on the device where the Managed PKI certificate is installed. 2 Access the URL to the Citrix NetScaler VPN. The browser prompts you to select the certificate that will authenticate you on the VPN URL. 3 Select the certificate and click **OK**. 4 Enter the PIN for PKI Client when prompted, and click **OK**. The Citrix NetScaler VPN communicates with the Symantec CA to authenticate the certificate. If the authentication succeeds and the PIN is valid, the VPN connection is established. The start-up screen displays the applications that are available to your user account. Double-click an application to open and to use it.