CONFIGURATION GUIDE

Cloudpath Enrollment System Integration with Microsoft NPS Configuration Guide, 5.6

Supporting Cloudpath Software Release 5.6

Part Number: 800-72500-001 Rev A
Publication Date: 15 December 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Overview **4**
About this Document 4
Overview of Network Policy Server 4
Prerequisites 5
Configuring Firewall Rules for Use with Cloudpath 6

Configuring Cloudpath **6**
Overview of Configurating Cloudpath 6
Create the Certificate Authority 6
Set Up Client Certificate Template Settings for NPS 8
Set Up a Certificate Template for the NPS Server Certificate 12
Generate the Server Certificate for the NPS 13
Download the Public Key of the Intermediate CA 14

Configuring the Network Policy Server **15**
Overview of Configuring the Network Policy Server 15
Import the RADIUS Server Certificate for the NPS 15
Import the Public Key of the Intermediate CA 18
Set Up Roles and Services 19
Network Policy Setup for EAP/TLS 20

Verify Network Policy **25**
Review the Network Policy 26
Verify Conditions of a Connection Request Policy 26
Verify Authentication Method 27
Verify Network Policy Settings 28

Connection Request Policies **28**

Setting Up RADIUS Proxy on NPS **28**
Overview of Setting Up RADIUS Proxy on NPS 28
Add a Remote RADIUS Server Group for RADIUS Proxy 28
Configure a Connection Request Policy for RADIUS Proxy 29

Tips and Troubleshooting **32**
Validate Server Certificate Setting in the License Server 32
LDAP 32
OSCP Issues 32
Credentials Mismatch 33
Certificate Template Issues 33
EAP Method is Not Available on the Server 33
Certificate Chain Not Trusted 34

Overview

About this Document

This document helps network administrators configure a Microsoft™ Network Policy Server to act as the RADIUS server for use with Cloudpath in a wireless network with EAP-TLS authentication.

This guide provides instructions for configuring firewall rules, configuring Cloudpath to act as a private CA and issue certificates to be imported by the NPS, how to configure RADIUS proxy, and troubleshooting information.

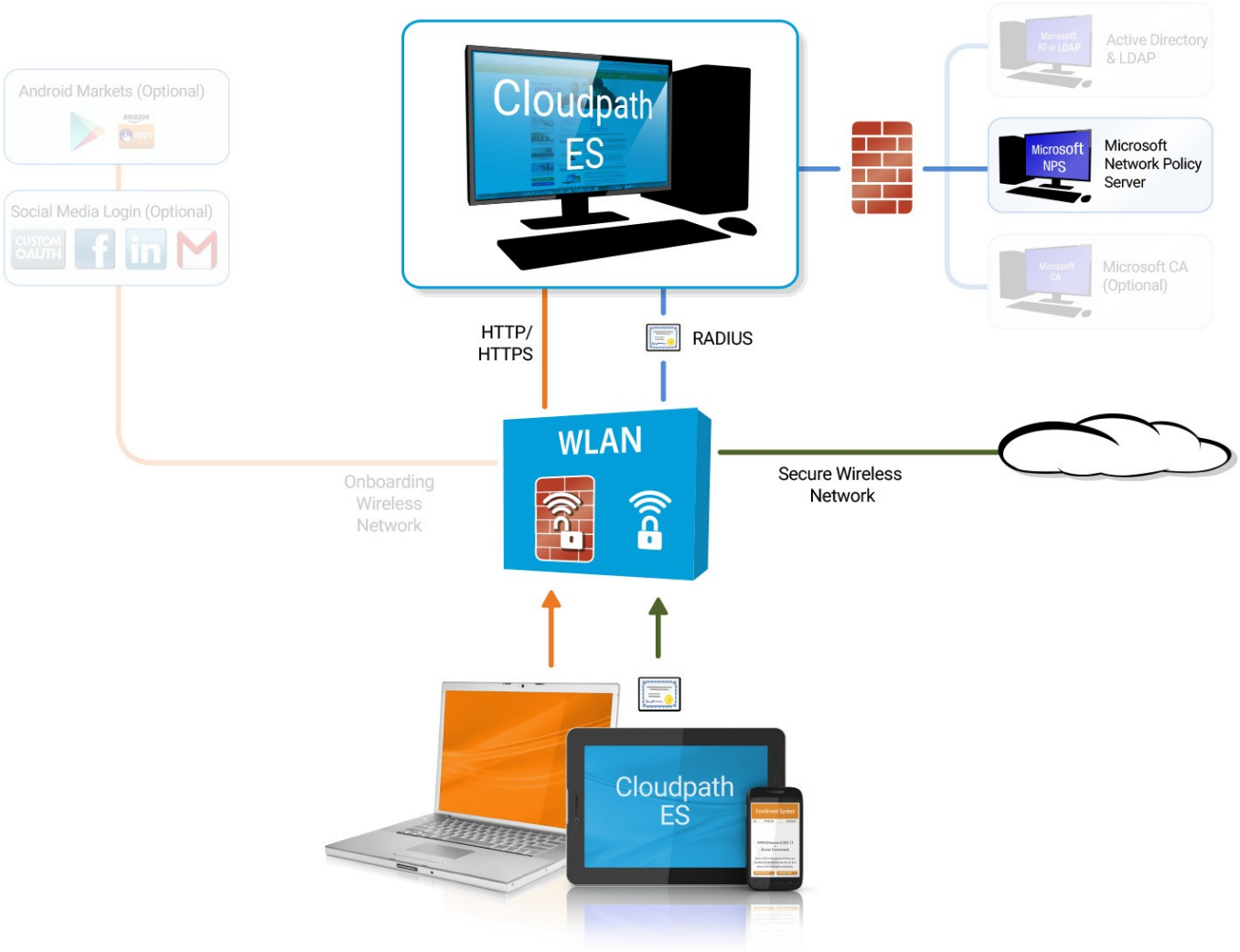
Overview of Network Policy Server

Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy.

As a RADIUS server, NPS performs authentication and authorization of network connection attempts. NPS authenticates users and devices by verifying their Active Directory credentials.

RADIUS clients are network access servers such as wireless access points (APs), 802.1X-capable switches, virtual private network (VPN) servers, and dial-up servers because they use the RADIUS protocol to communicate with RADIUS servers, such as NPS servers.

FIGURE 1 Cloudpath Integrated with Microsoft Network Policy Server



You can configure an NPS as a RADIUS server that integrates with the Cloudpath Enrollment System (ES). Cloudpath can be used as a private CA for certificate deployments using either PEAP-TLS or EAP-TLS authentication. Cloudpath provides certificates to your NPS server acting as a RADIUS server, and client certificates to your client computers and users. NPS servers are logically connected to your network so that they can receive incoming access requests directly from wireless APs or wireless controllers.

This guide describes how to configure a Microsoft 2008 NPS as a RADIUS server for use with the Cloudpath in an 802.11 wireless network with EAP-TLS authentication.

Prerequisites

Before you can configure an NPS to work with Cloudpath, your network must have certain devices and services.

You must have the following devices ad services set up in your network:

- Microsoft 2008 Domain Controller configured with Active Directory services.

- Microsoft 2008 Network Policy Server must be configured (and registered) within your domain. See Tips and Troubleshooting on page 32 for more information.
- Wireless Controllers and/or Access Points configured for EAP-TLS authentication. Make note of the IP address of the RADIUS client. This is required when configuring the standard configuration for NPS for 802.1X wireless connections.

  NOTE
  It is recommended that you install Microsoft NPS services on a server separate from your Microsoft Active Directory services.

Configuring Firewall Rules for Use with Cloudpath

Network firewall rules must be configured to allow Cloudpath and the Network Policy Server to communicate.

Depending on where Cloudpath is placed in your network, certain TCP ports are required to allow Cloudpath to communicate with NPS and Active Directory (AD) services. Ensure you have done the following procedures to configure firewall rules for use with Cloudpath.

- Open TCP port 389 to allow Cloudpath to query AD for users and groups during user login.
- Open TCP port 80 to allow the NPS to query Cloudpath for OCSP.

  NOTE
  Refer to Tips and Troubleshooting on page 32 for additional information about firewall settings. Additional firewall information can be found on the **Administration** > **Advanced** > **Firewall Requirements** page.

Configuring Cloudpath

Overview of Configurating Cloudpath

If you deploy certificate=based authentication, a server running NPS must have a server certificate. During the autentication process, the NPS sends the server certificate to the client computer as proof of identity.

To work with Cloudpath, the NPS requires a server certificate and the private key of the Root CA from Cloudpath. The certificates are generated and downloaded from Cloudpath and then uploaded to the NPS.

This section describes how to configure Cloudpath as a private CA, generate the RADIUS server certificate, download the public and private key of the RADIUS server certificate, and download the public key of the intermediate CA.

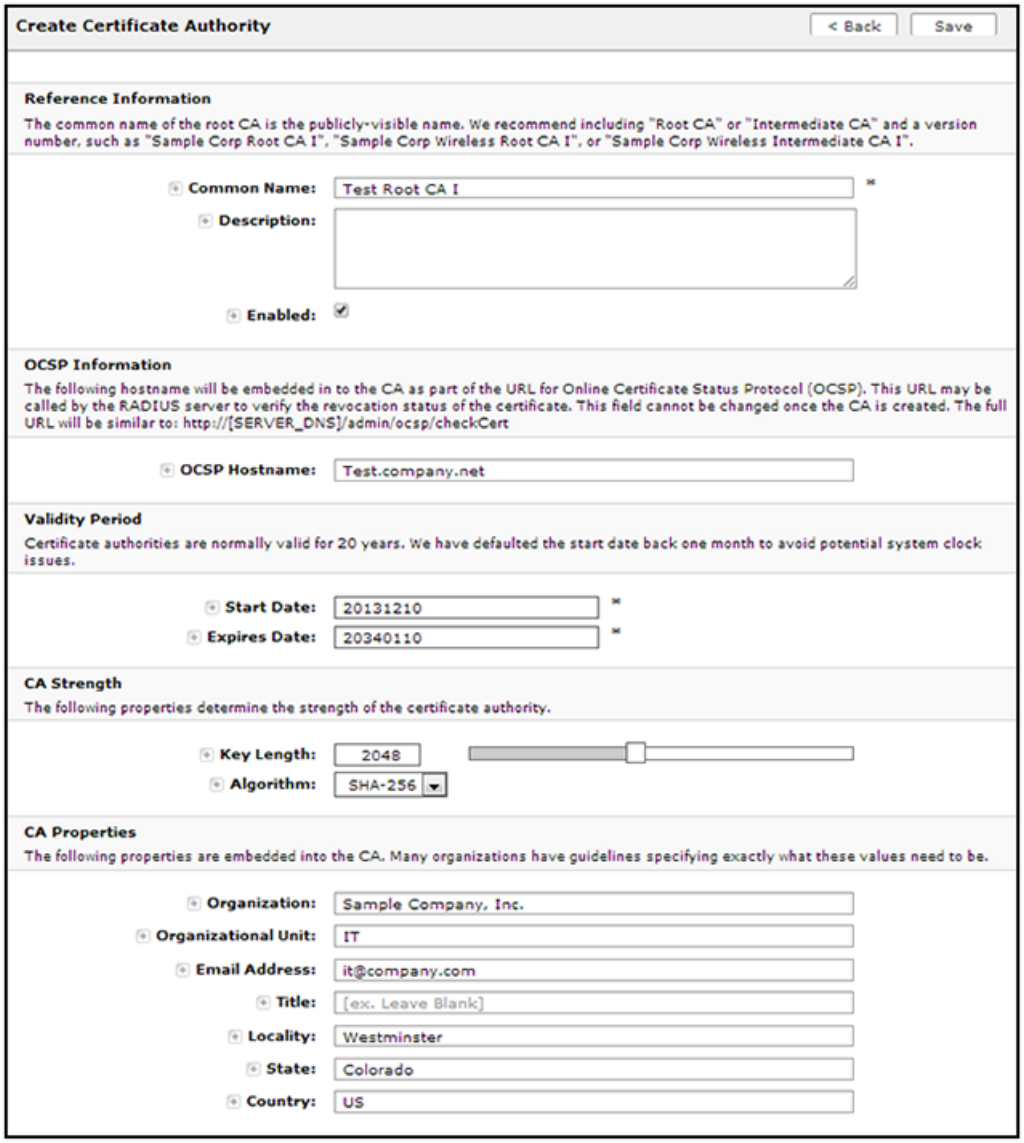
Create the Certificate Authority

To set up a standalone certificate authority in Cloudpath, perform the following steps:

1. From the Cloudpath left menu, select **Certificate Authority** > **Manage CA**.
2. Click **Add/Upload CA**.
3. Select **Generate New Certificate Authority**.

4. On the **Create Root CA** page, enter the following information:
   - **Common Name:** The publicly visible name of the root CA. It is recommended that you use the word "Root" in the name and include a version number.
   - **Description:** Enter a description useful to other administrators.
   - **Enabled:** The default is enabled. Be sure this box is checked.
   - **OSCP Host Name:** The host name embedded into the CA as part of the URL for the OCSP.
   - **Validity Period:** Retain the default, or specify the **Start** and **Expires** dates.
   - **CA Strength:** Configure the strength of the CA by specifying the **Key Length** and **Algorithm**.
   - **CAP Properties:** Properties embedded into the CA. Enter the appropriate information as required by your network policy.

FIGURE 2 Create Root CA



5. Click **Save** to save the CA.

Set Up Client Certificate Template Settings for NPS

In Cloudpath, certificate templates are used to generate certificates.

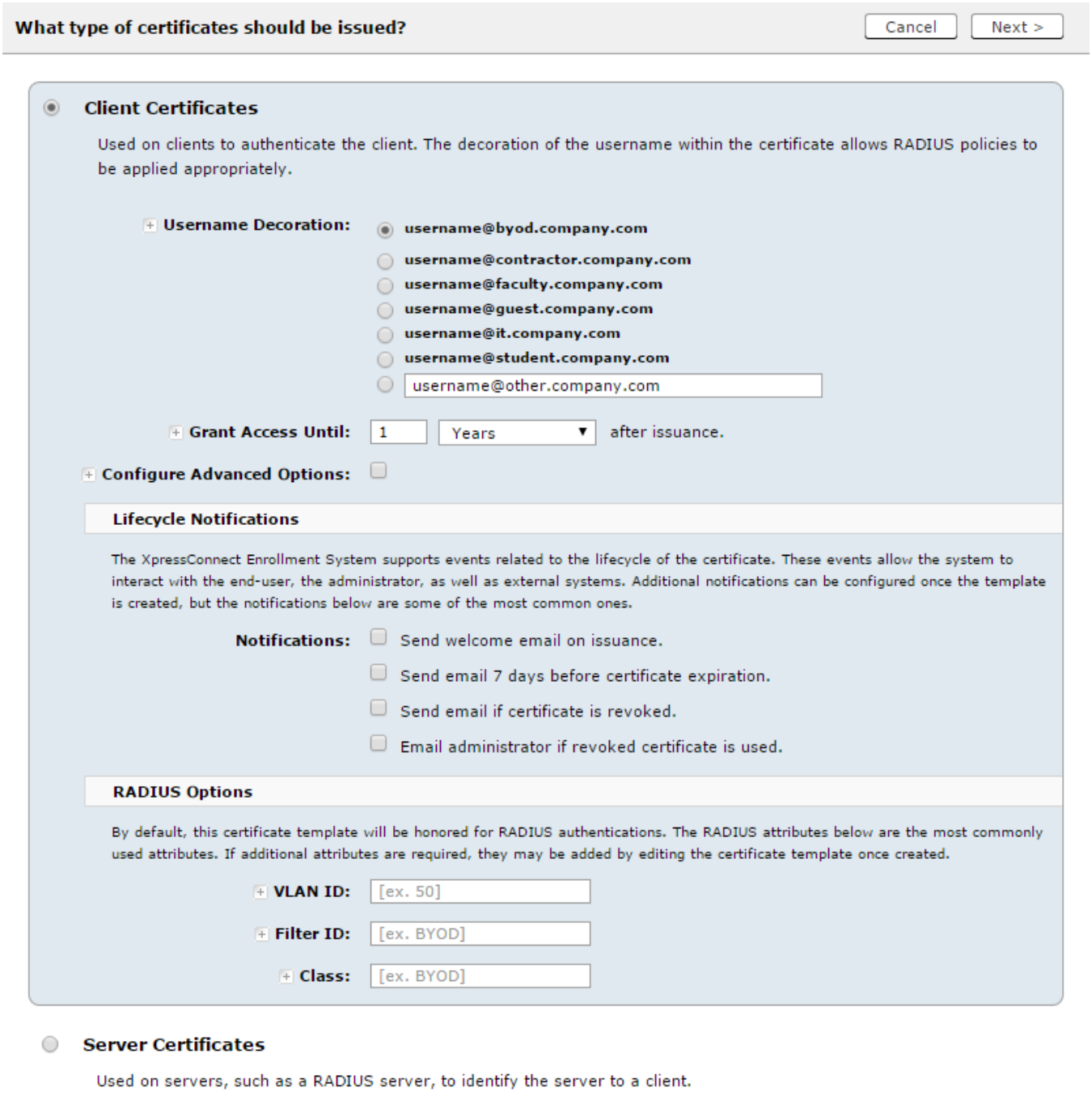
A template defines the properties embedded into a certificate when it is issued. Some properties are static and remain the same for every certificate. Other properties are calculated or use variables, allowing them to differ per certificate, based on user and device.

To set up a client certificate template using an onboard CA, perform the following steps:

1. From the Cloudpath left menu, select **Certificate Authority** > **Manage Templates**.
2. Click **Add Template** to create a new certificate template.
3. Choose **Use an onboard certificate authority** and select the onboard CA you created in the previous section.

4. Select **Client Certificates**.

FIGURE 3 Create Client Certificate Template



5. Select or enter a Username Decoration. The decoration of the username within the certificate allows RADIUS policies to be applied appropriately.

6. Grant access for the appropriate amount of time.

   For example, you might have client certificate template for a guest user that is valid for one, or a few days, another for a contractor that is valid for 6 months, and one for employees that is good for a year.

   TIP
   To configure pattern attributes, certificate strength, and EKUs, check the **Configure Advanced Options** box before you click **Next**.

7. Select any email notifications to be sent to the user related to the lifecycle of the certificate.

   Additional certificate notifications can be configured after the template is created.

8. Enter data in the **RADIUS Options** fields to assign a VLAN ID or Filter ID to certificates that use this template.

   These settings only apply if you are using the onboard RADIUS server.

Client Certificate Template Advanced Options

The following table describes the actions to take for each of the fields on the Modify Certificate Template page, which displays if you checked **Configure Advanced Options** while creating a client certificate template.

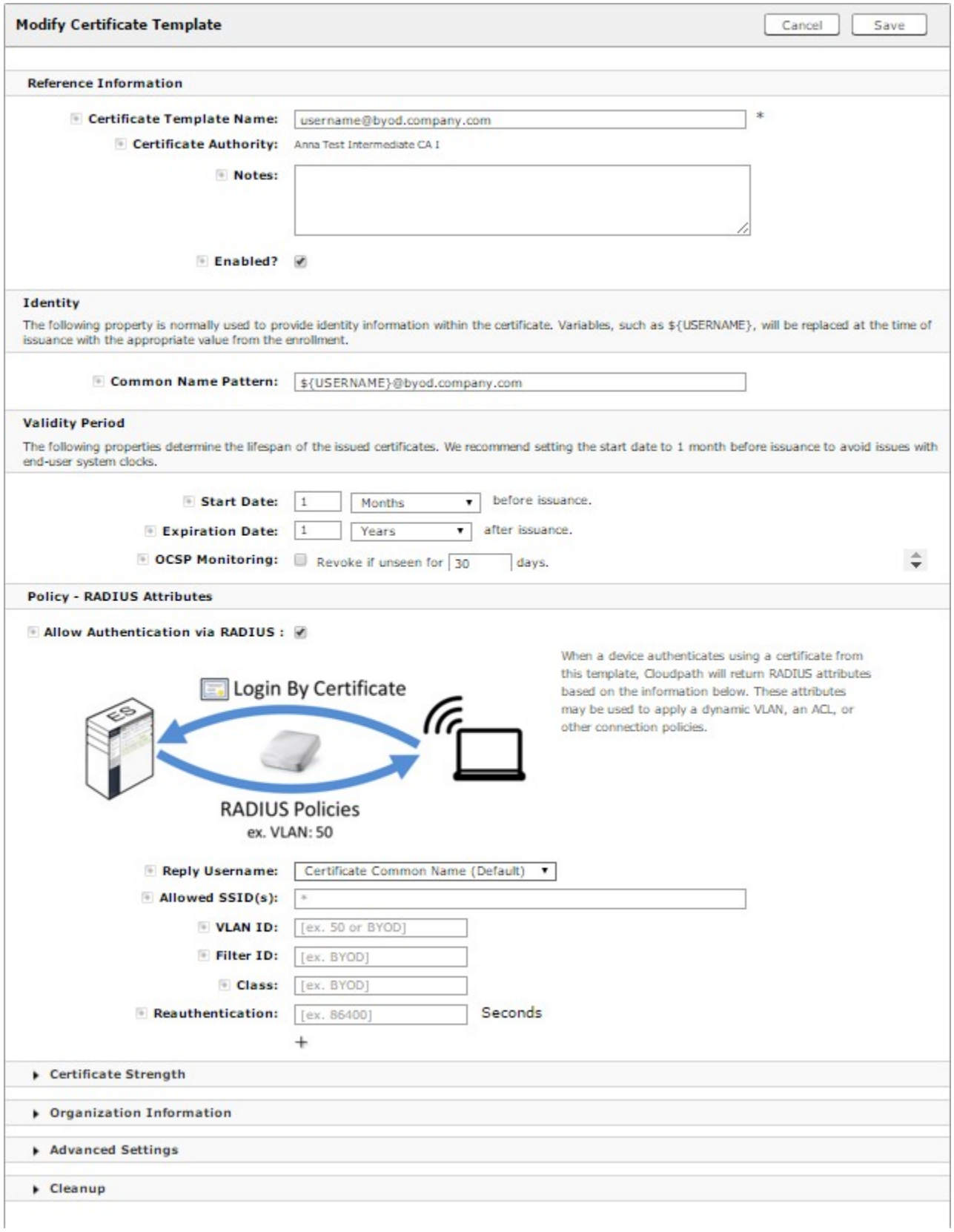
TABLE 1 Fields on the Modify Certificate Template Page

Field	Action
Reference Information	Enter information in the **Certificate Template Name** and **Notes** fields. This information is for reference only. Enable the template.
Identity	Enter the **Common Name Pattern** used to determine the common name for certificates generated using the template. Variables, such as ${SERVER_NAME} are replaced when issued with the value from enrollment.
Validity Period	Used to determine the lifespan of the issued certificate.
Certificate Strength	Enter the **Key Length** and **Algorithm** for certificates using this template.
Organization Information	Enter the **Patterns** for certificates using this template.
Advanced Settings	Enter the **Patterns** for certificates using this template.
Cleanup	Use these options to delete client certificate templates and associated data.

If you are using the NPS as a RADIUS server in your environment, the server certificate requires that you have a **SAN Other Name** in addition to the **Common Name** properties. The **SAN Other Name Pattern** must match the variable used in the **Common Name Pattern** field.

NOTE
Client certificate templates must use *Microsoft Client EKU - 1.3.6.1.5.5.7.3.2*. This establishes the **Extended Key Usage** properties for the certificate.

FIGURE 4 Modify Client Certificate Template



Set Up a Certificate Template for the NPS Server Certificate

The server certificate helps to verify the identity of the NPS (acting as a RADIUS server) to wireless clients.

To set up a server certificate template in Cloudpath, perform the following steps:

1. From the Cloudpath left menu, select **Certificate Authority** > **Manage Templates**.
2. Click **Add Template** to create a new certificate template.
3. Choose **Use an onboard certificate authority**, and select the onboard CA you created in the previous section.
4. Select **Server Certificates**.
5. Enter a validity period for the server certificate, and click **Next** to use the default settings.

> **TIP**
> To configure pattern attributes, certificate strength, and EKUs, check the **Configure Advanced Options** box before you click **Next**.

Server Certificate Template Advanced Options

The following table describes the actions to take for each of the fields on the Modify Certificate Template page, which displays if you checked **Configure Advanced Options** while creating a server certificate template.

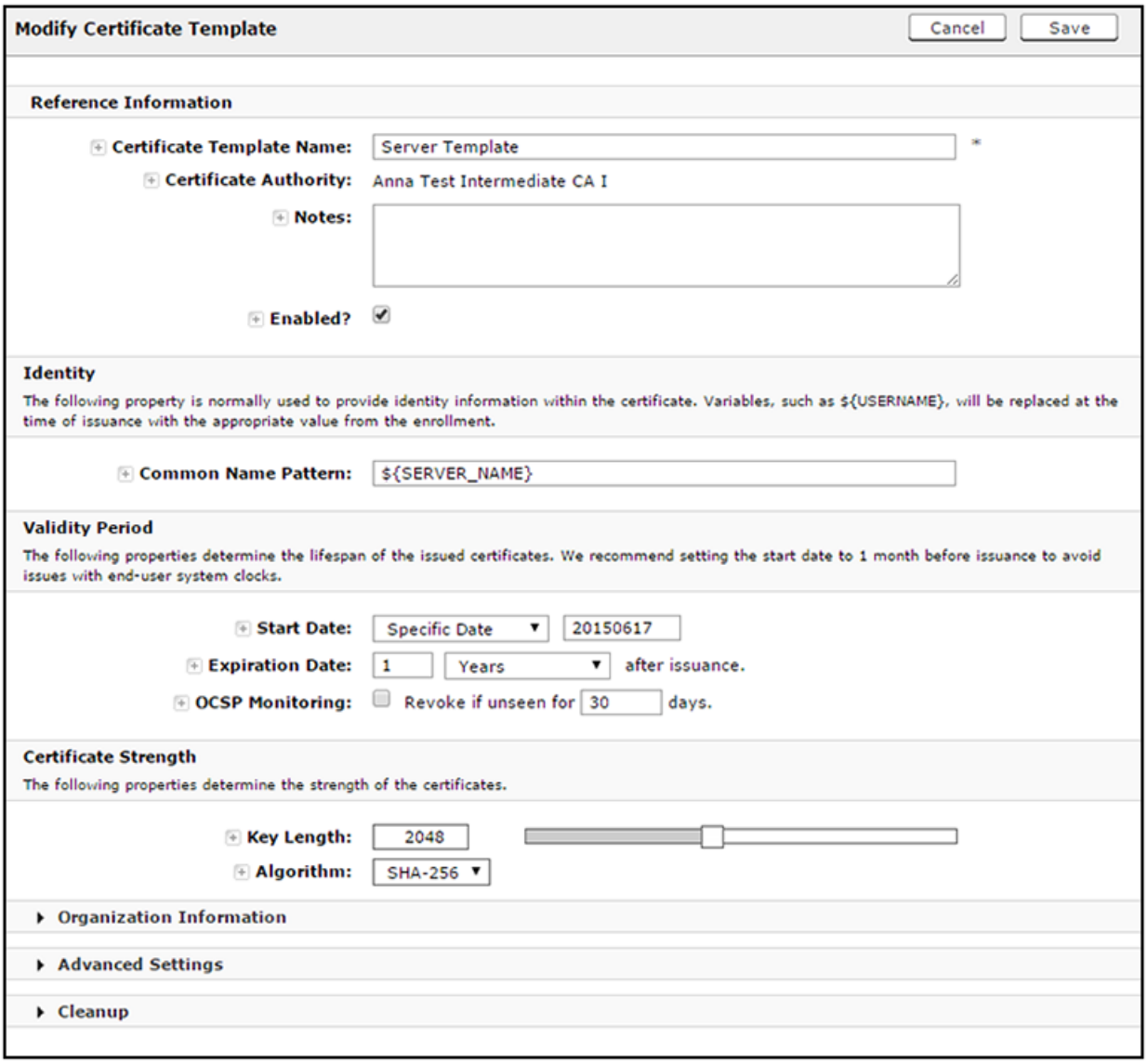
TABLE 2 Fields on the Modify Certificate Template Page

Field	Action
Reference Information	Enter information in the **Certificate Template Name** and **Notes** fields. This information is for reference only. Enable the template.
Identity	Enter the **Common Name Pattern** used to determine the common name for certificates generated using the template. Variables, such as ${SERVER_NAME} are replaced when issued with the value from enrollment.
Validity Period	Used to determine the lifespan of the issued certificate.
Certificate Strength	Enter the **Key Length** and **Algorithm** for certificates using this template.
Organization Information	Enter the **Patterns** for certificates using this template.
Advanced Settings	Enter the **Patterns** for certificates using this template.
Cleanup	Use these options to delete client certificate templates and associated data.

If you are using the NPS as a RADIUS server in your environment, the server certificate requires that you have a **SAN Other Name** in addition to the **Common Name** properties. The **SAN Other Name Pattern** must match the variable used in the **Common Name Pattern** field.

> **NOTE**
> Client certificate templates must use *Microsoft Client EKU - 1.3.6.1.5.5.7.3.2*. This establishes the **Extended Key Usage** properties for the certificate.

FIGURE 5 Modify Server Certificate Template



Generate the Server Certificate for the NPS

You can generate a server certificate from the server certificate template and Cloudpath onboard CA that you created in previous procedures.

To generate the server certificate, perform the following steps:

1. From the Cloudpath left menu, go to **Certificate Authority** > **Generate Certificate**.
2. Select the NPS server certificate template that you previously created.
3. Use the default **SERVER_NAME**.

4. Select **Auto-Generate CSR** from the **SCR source** and click **Save**.

   The certificate is generated and displayed on the **View Certificate** page.

   NOTE
   Alternately, NPS can generate a Certificate Signing Request (CSR) to be used within Cloudpath for generating the RADIUS server certificate. You use the same server certificate template, but instead of allowing Cloudpath to auto-generate the certificate, you select the **Copy & Paste CR** option from the **CSR source**.

Download the RADIUS Server Certificate

To download the RADIUS Server Certificate, perform the following steps:

1. Navigate to the **Configuration** > **RADIUS Server** page.
2. In the **RADIUS Server Certificate** section, download the **Public Key** for the server certificate.

   Alternately, you can download the **CSR** or certificate **Chain** or replace an existing RADIUS server certificate.

Download the Public Key of the Intermediate CA

The Public Key of the Intermediate CA is used to establish the proper chaining of the RADIUS server certificate. Proper chaining is necessary for the wireless end-points to establish a 'trust' for the RADIUS server certificate to the Intermediate CA, which is used to sign the client certificates.

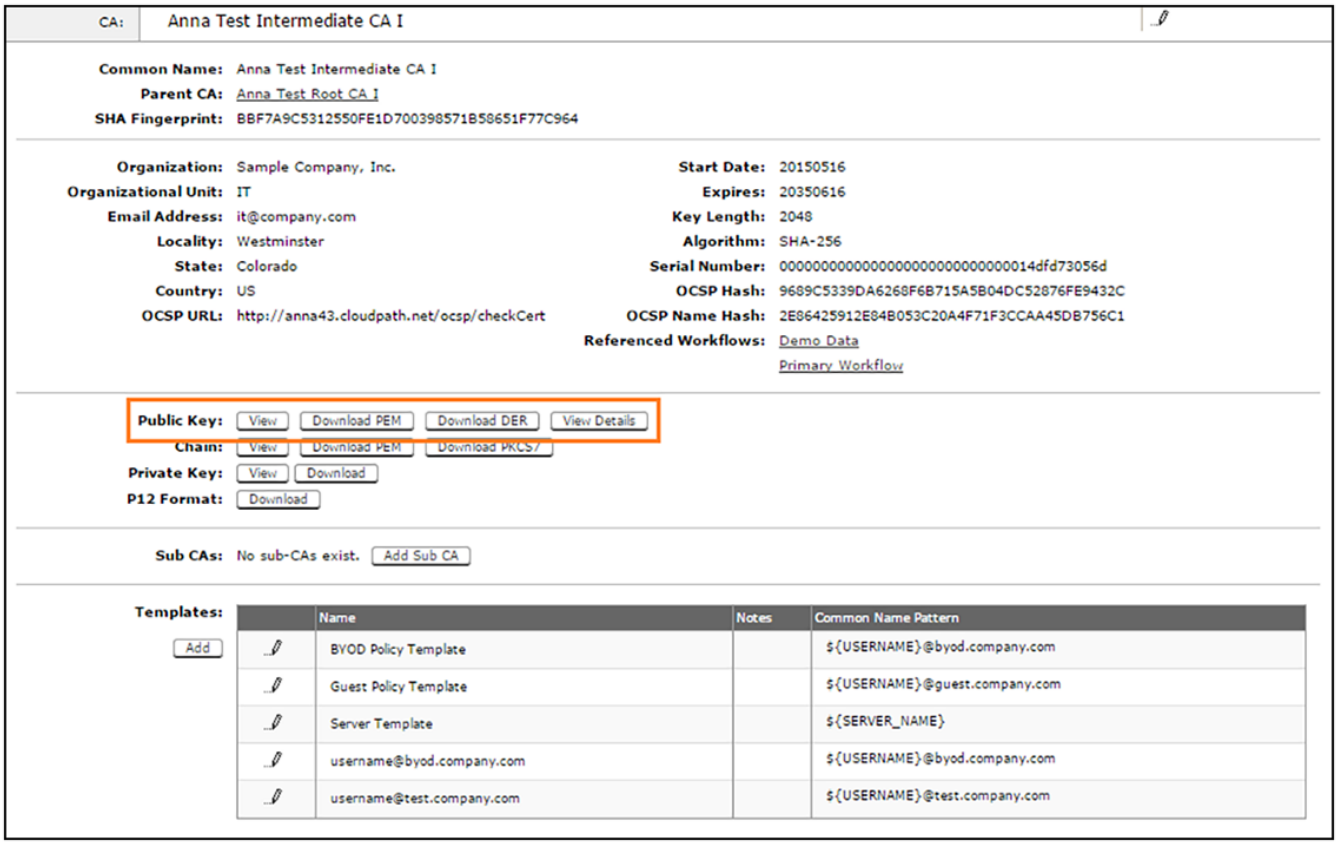
NOTE
By default, the Intermediate CA (onboard CA) signs the user certificate. If your environment is set up to have the Root CA sign the client certificate, you must download and install the public key of the Root CA.

To download the public key of the Intermediate CA, perform the following steps:

1. From the Cloudpath left menu, navigate to **Certificate Authority** > **Manage CA**. Expand the onboard CA you previously created.
2. Expand the onboard CA.
3. In the **Sub CAs** section, click the link to open the **Intermediate CA** page.

4. Download the **Public Key** of the Intermediate CA.

FIGURE 6 Download Public Key of Intermediate CA



Configuring the Network Policy Server

Overview of Configuring the Network Policy Server

The following sections describe how to configure Microsoft 2008 Network Policy Server (NPS) to use as a RADIUS server with Cloudpath.

PREREQUISITE
The NPS must be configured within your domain.

Import the RADIUS Server Certificate for the NPS

To import the RADIUS Server Certificate for the NPS, perform the following procedures, which are described in the following sections.

- Add a Certificates Snap-in

- Import the RADIUS Server Certificate into the Local Computer Personal Certificate Store

Add a Certificates Snap-in

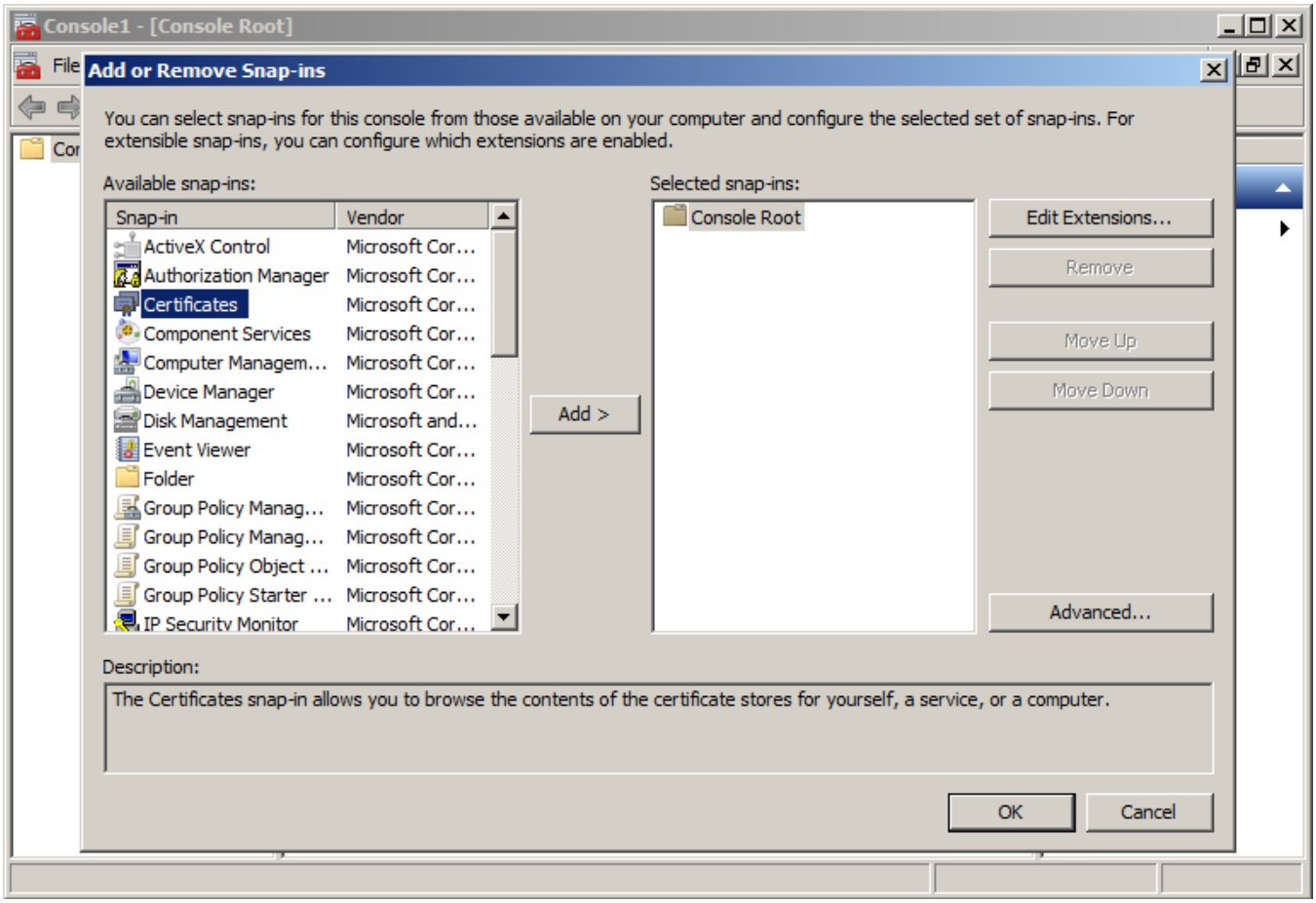
To import the server certificate to the NPS Certificate Store, perform the following steps:

1. From a command window, run **mmc** to open a console window.

   TIP
   Do not use certngr to import the server certificate. The certmgr allows you to manage certificates for the **Current User**. However, you must import the server certificate into the **NPS Computer** certificate store.

2. Go to **File** > **Add/Remove Snap-in**.
3. On the **Add or Remove Snap-ins** page, select **Certificates** from the left pane (**Available Snap-ins:**) and click **Add**.

   FIGURE 7 Add Snap-in



4. In the **Certificates** snap-in window, select **Computer Account** and click **Next**.
5. In the **Select Computer** window, select **Local Computer** and click **Finish**.

   Certificates (Local Computer) should be listed in the right pane (**Selected Snap-ins:**) of the **Add or Remove Snap-ins** window.

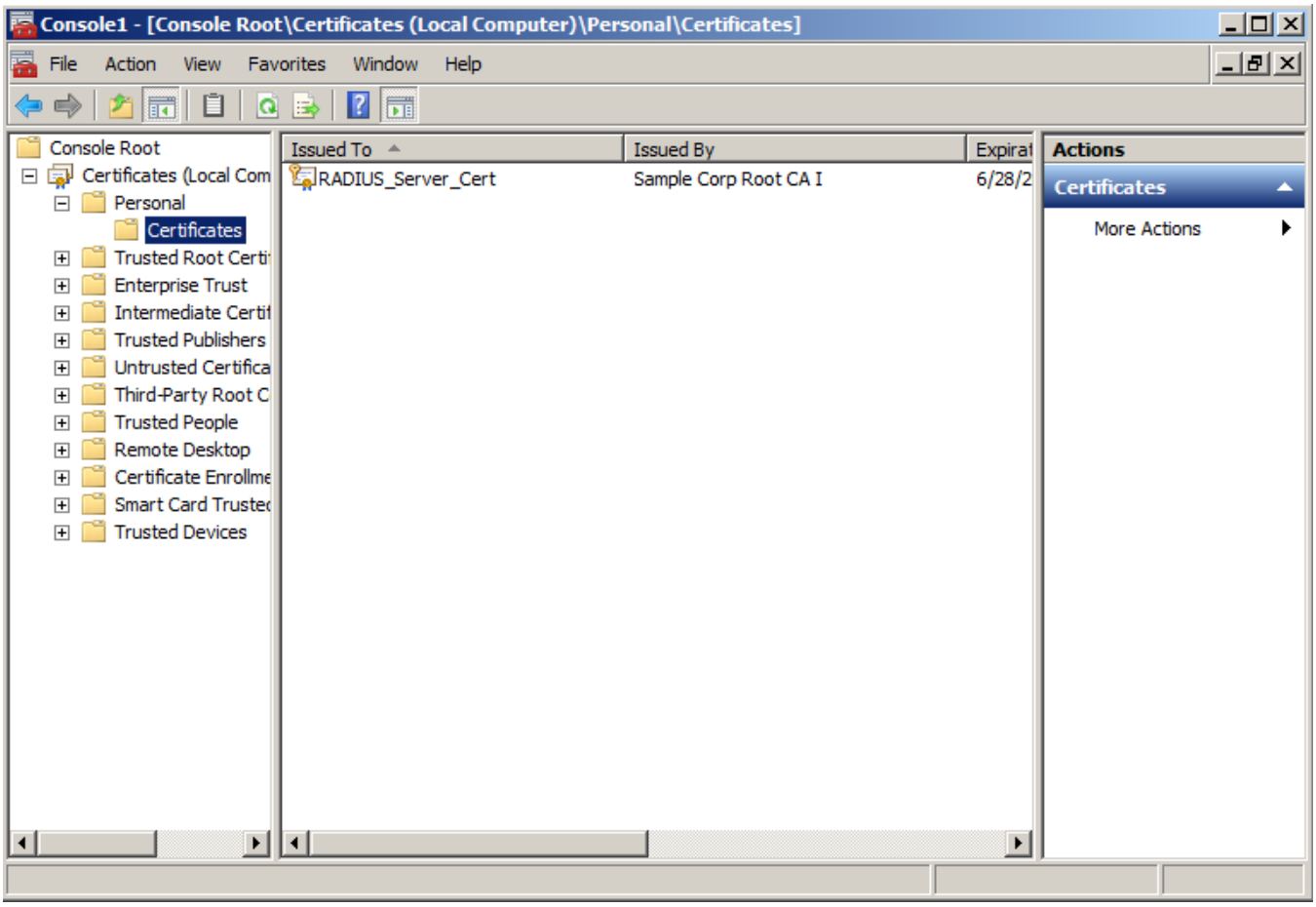
6. Click **OK**.

Import the RADIUS Server Certificate into the Local Computer Personal Certificate Store

To import the RADIUS Server Certificate, perform the following steps:

1. On the **Console** window, expand **Certificate (Local Computer)** to locate the **Personal/Certificates** folder.

FIGURE 8 Certificates Folder in Console Window



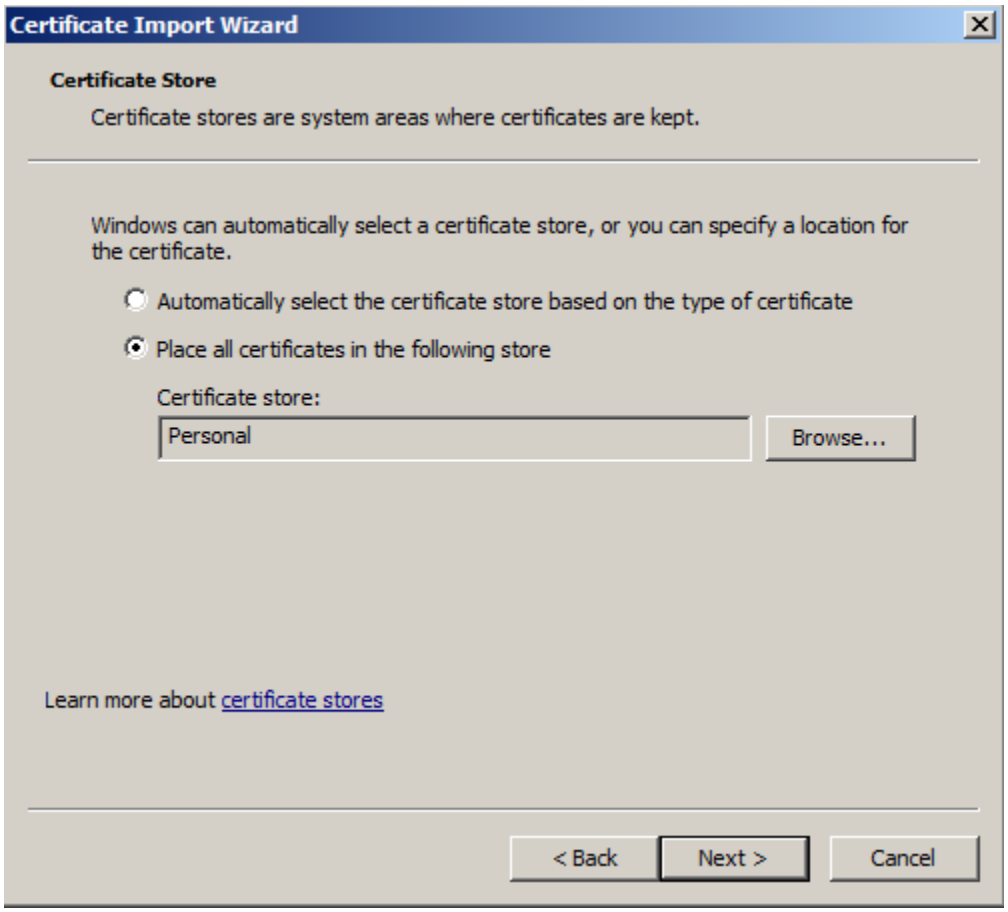
2. Go to **Action** > **All Tasks** > **Import** to start the **Certificate Import Wizard**.
3. Browse to locate the private key of the server certificate you generated in Cloudpath to use for the NPS, and click **Open**.
4. On the **Certificate Import Wizard**, click **Next**.

5. Place the NPS server certificates in the **Personal** store, and click **Next**.

   TIP

   Be sure that the RADIUS server certificate show the key icon . If it does not show it, you do not have the private key for the RADIUS certificate. If you have issues, try downloading the RADIUS certificate and private key in P12 format. You can also try using the command line interface to install the private key for the RADIUS certificate. See Missing EKU in the RADIUS Server Certificate on page 33.

FIGURE 9 Certificate Import Wizard



6. Review the imported certificate, and click **Finish**.

Import the Public Key of the Intermediate CA

The public key of the Intermediate CA (onboard CA) establishes the proper trust chain of the RADIUS server certificate.

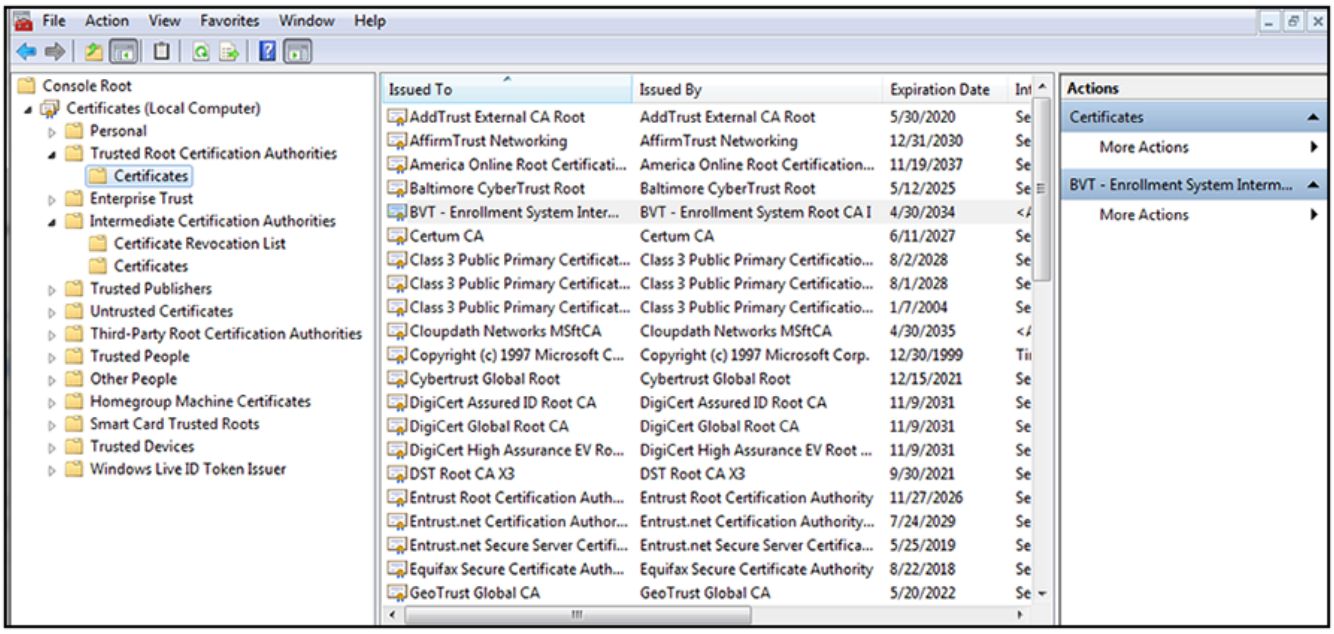
NOTE
By default, the Intermediate CA (onboard CA) signs the user certificate. If your environment is set up to have the Root CA sign the client certificate, you must download and install the public key of the Root CA.

To import the public key of the intermediate CA to the Enterprise Trust Store, perform the following steps:

1. On the Console window, expand **Certificate (Local Computer)** to locate the **Enterprise Trust/Certificates** folder.
2. Go to **Action** > **All Tasks** > **Import** to start the **Certificate Import Wizard**.
3. Browse to locate the public key of the Cloudpath on-board Intermediate CA, and click **Open**.
4. On the **Certificate Import Wizard**, click **Next**.
5. Import the public key of the Intermediate CA in the **Certificate (Local Computer) Trusted Root Certificate Authorities** store, and click **Next**.

   NOTE
   You will encounter fewer issues when you import into the Trusted Root CA store. However, if you import the public key of the onboard Intermediate CA into the Intermediate CA store, this should also work.

FIGURE 10 Root Certificate in the Enterprise Certificate Store



6. Review the imported certificate, and click **Finish**.

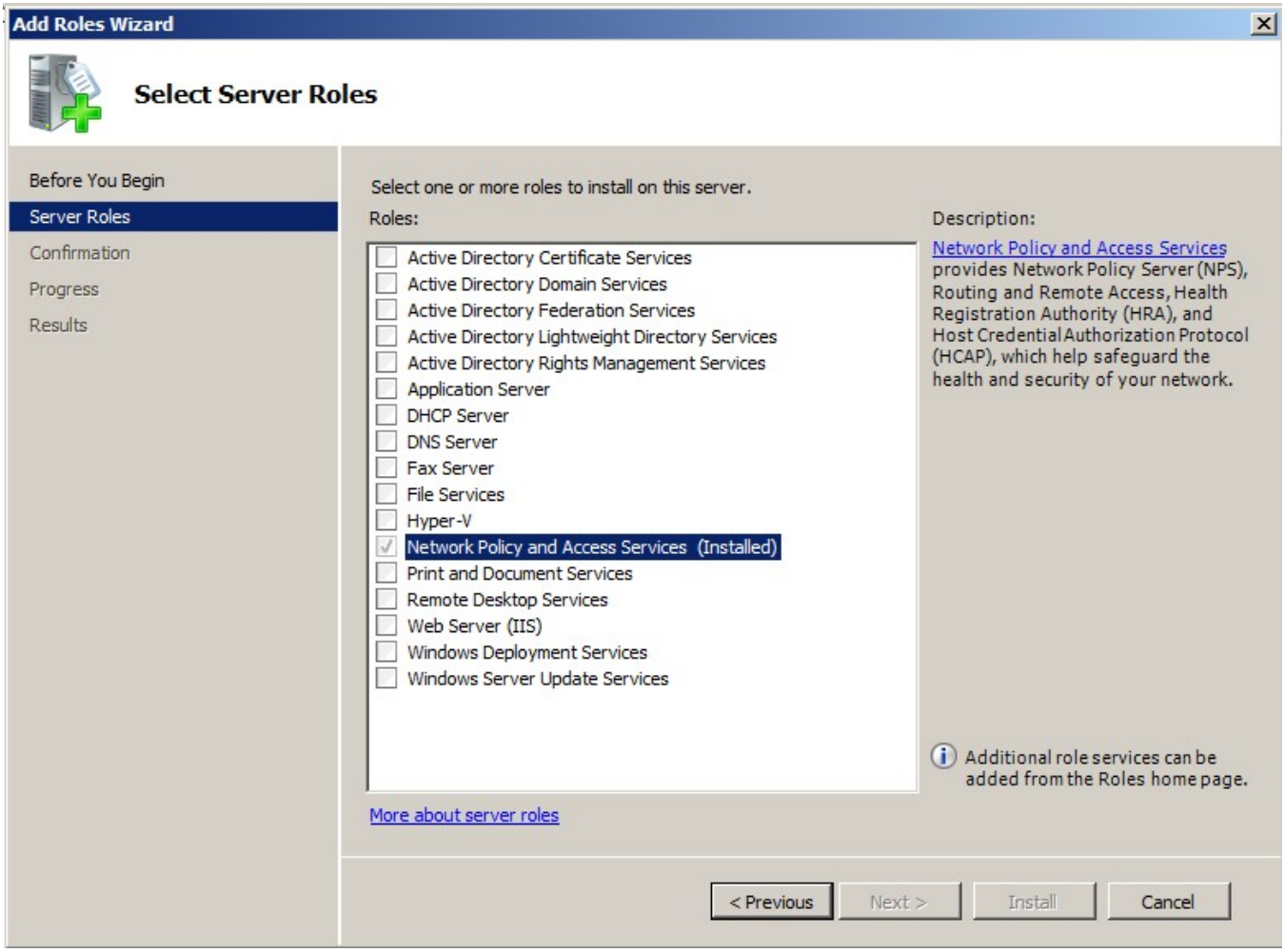
Set Up Roles and Services

To install Network Policy and Access Services (NPAS) as a Server Role, perform the following steps:

1. Open Server Manager.

2. Open the **Add Roles** wizard and install **Network Policy and Access Services**.

FIGURE 11 Install Network Policy and Access Services



3. Open the **Add Role Services** window and verify that the **Network Policy Server** is installed for **Network Policy and Access Services**.
4. In the **Role Summary** section, verify that NPS is running.

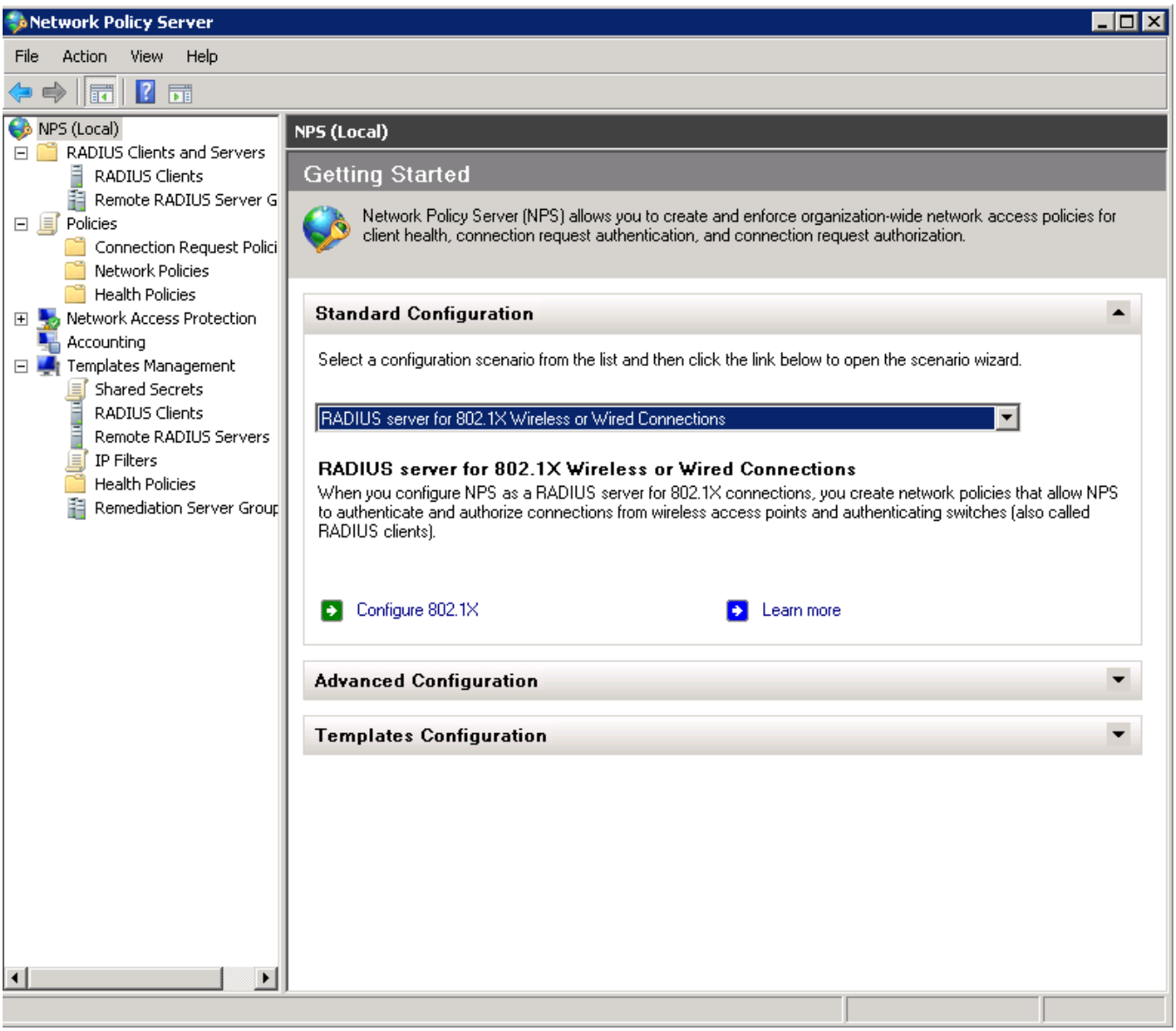
Network Policy Setup for EAP/TLS

To configure the 802.1X connection policy to set up 802.1X connections, perform the following steps:

1. Open Server Manager.
2. Expand **Network Policy and Access Services**, and select **NPS (Local)**.

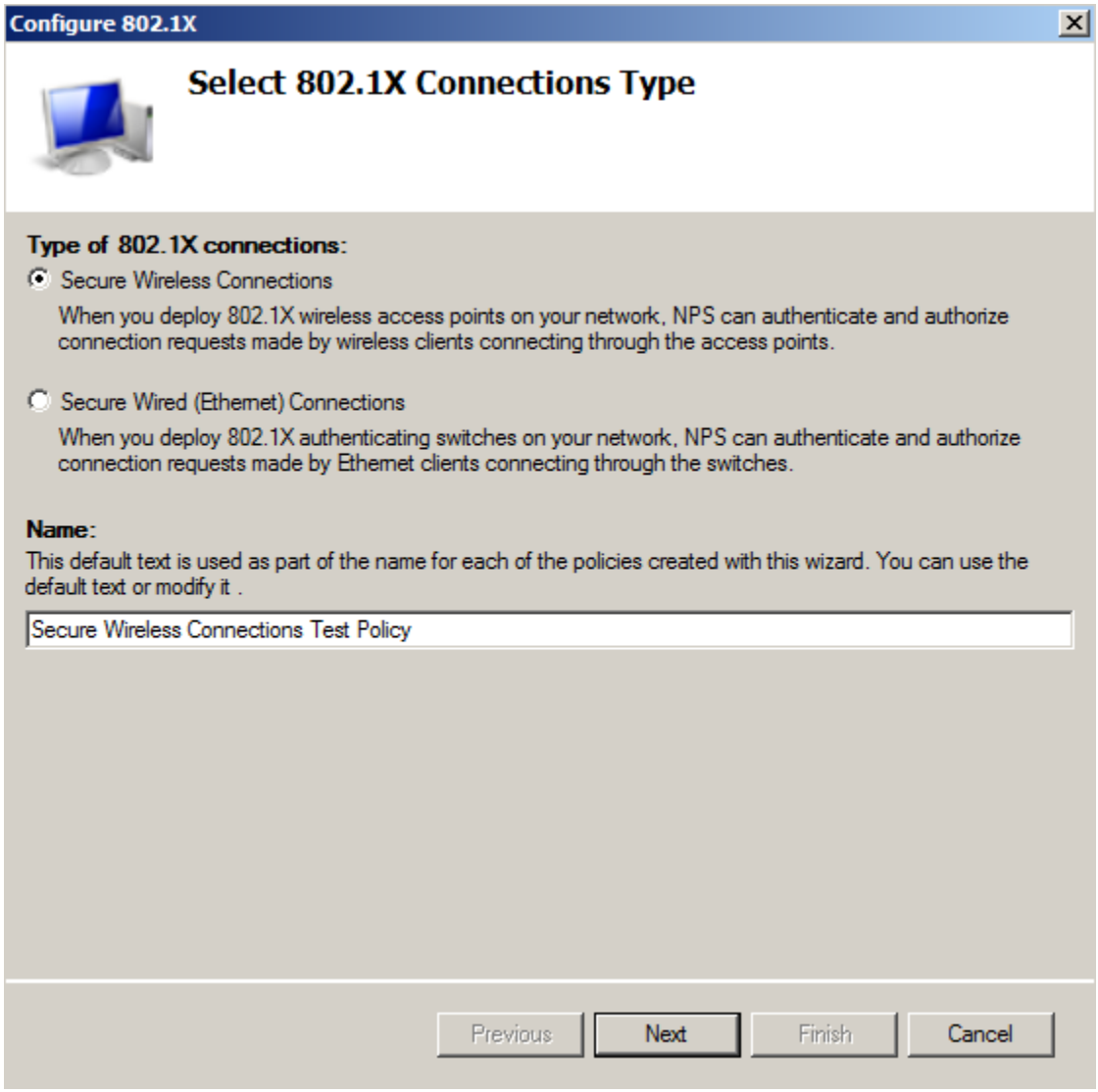
   The **Standard Configuration** section should appear in the center pane.

3. Select **RADIUS server for 802.1X Wireless or Wired Connections**, and click **Configure 802.1X**.



4. In the **Select 802.1X Connection Type** window, select **Secure Wireless Connections**, enter a **Name** for the wireless connection, and click **Next**.

FIGURE 12 Select 802.1X Connection Type

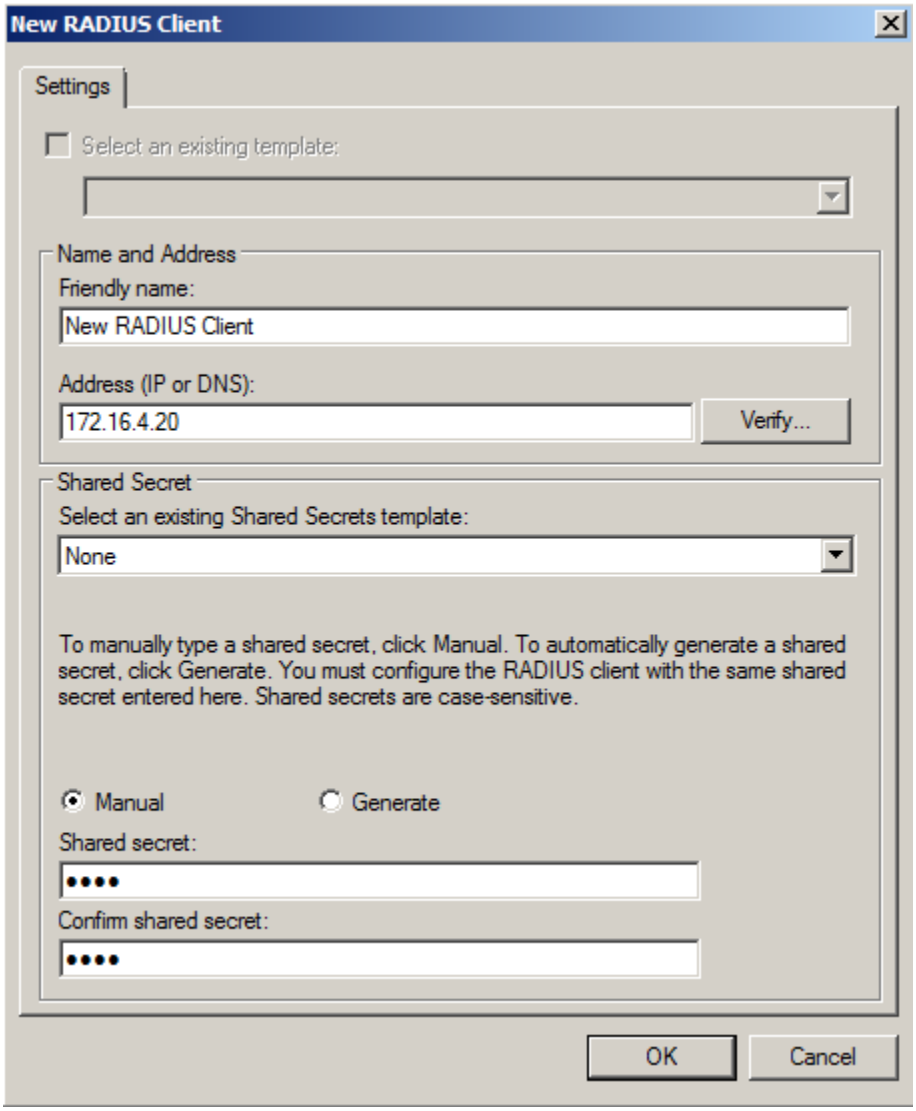


5. In the **Specify 802.1X Switches** window, click **Add** to configure a wireless access point (RADIUS client).

6. In the **New RADIUS Client** window, enter settings for the wireless access point, and click **OK**. Repeat this step to add additional RADIUS clients. Click **Next** on the **Specify 802.1X Switches** window to continue.

   NOTE
   If you already have a RADIUS client configured, skip to Step 10.

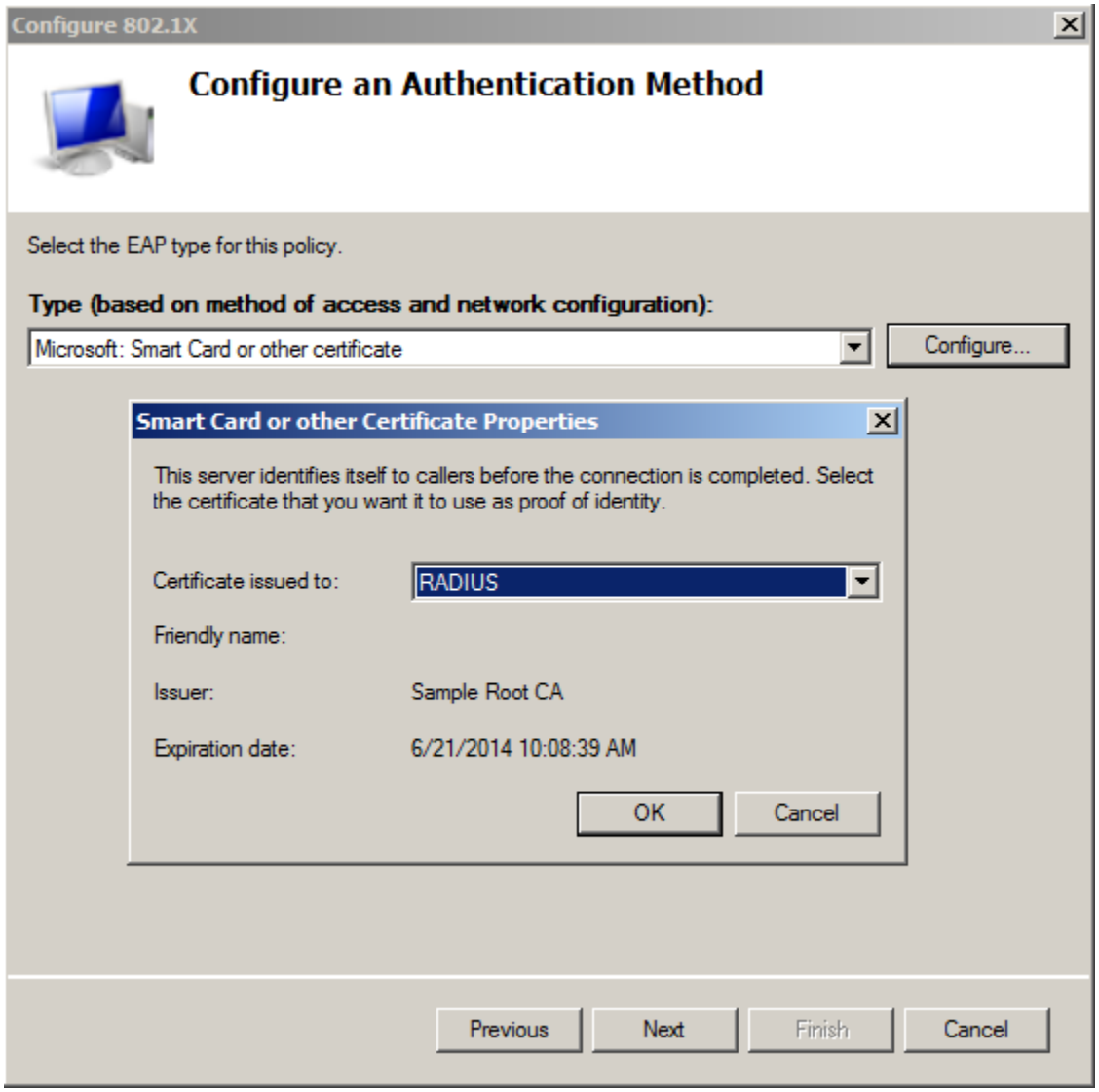
FIGURE 13 New RADIUS Client



7. In the **Configure Authentication Method** window, select **Smart Card or other certificate**.
8. To configure a RADIUS client, click **Configure**.

9. In the **Smart Card or other Certificate Properties** window, select the NPS RADIUS server certificate that you imported to the Computer Enterprise Trust store. (See Import the RADIUS Server Certificate for the NPS on page 15.) Click OK.

FIGURE 14 Configure Authentication Method



10. When you select the server certificate, click **Next** in the **Configure an Authentication Method** window.
11. Set up **User Groups** and **Traffic Controls**, if needed.
12. Click **Finish**.

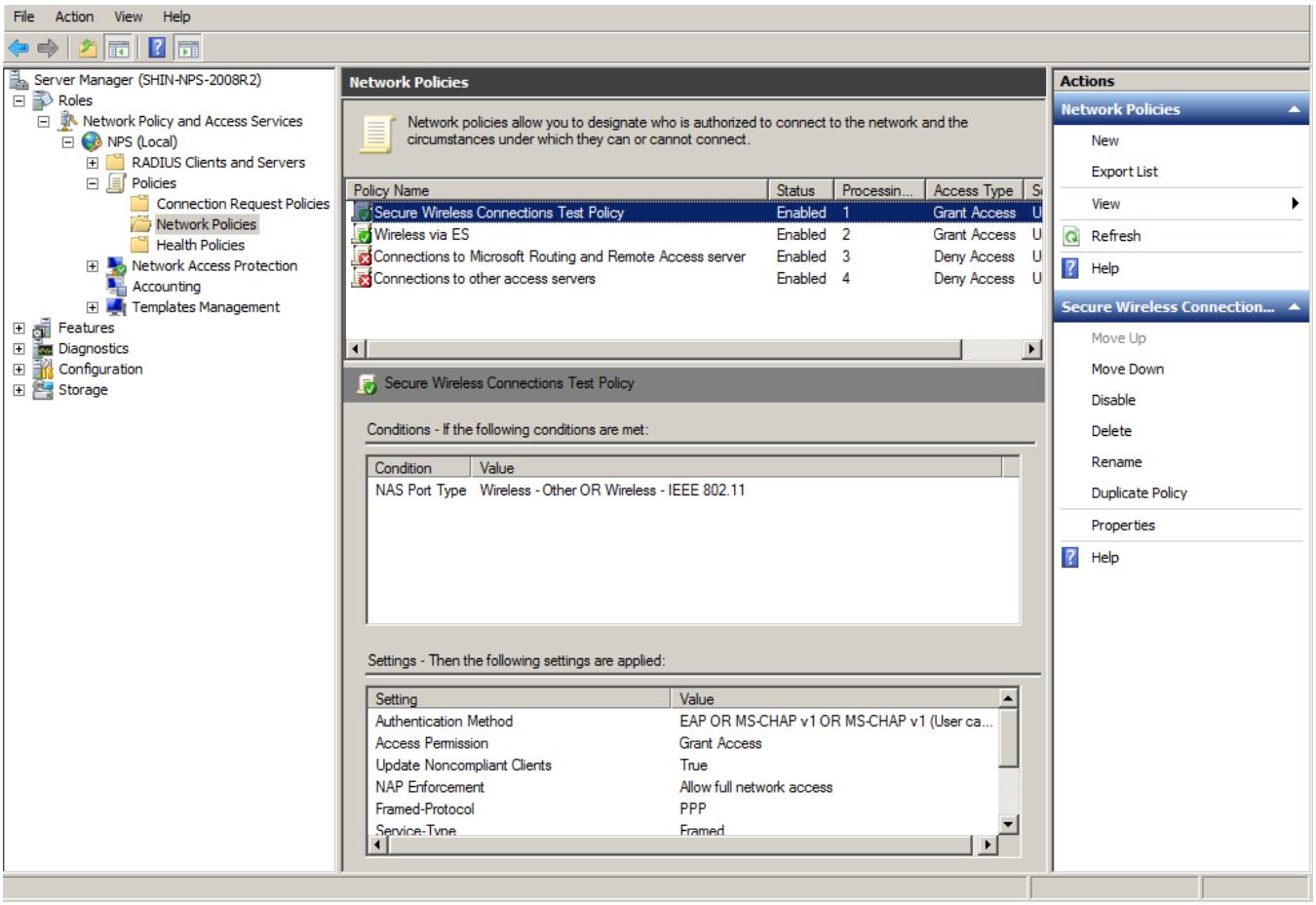
    The RADIUS client configuration is added.

Prioritize the 802.1X Configuration

To prioritize the 8021.X configuration, perform the following steps:

1. From the Server manager, expand **Network Policy and Access Services** > **NPS (Local)** > **Policies**, and select the **Network Policies** folder.
2. The 802.1X policy you just created should be at the top of the list. If needed, select the policy, and select **Move Up** until the policy is at the top of the list.

FIGURE 15 Network Policies



Verify Network Policy

You need to review your network policy, verify the conditions, verify that it uses the correct authentication method, and verify the network policy settings.

The following sections describe each part of the procedure.

Review the Network Policy

To review the network policy, perform the following steps:

1. From the Server manager, expand **Network Policy and Acess Services** > **NPS (Local)** > **Policies**, and select the **Network Policies** folder.
2. Select the 802.1X policy that you previously created.
3. Click **Properties** to view the network policy properties and verify they are correct.

Verify Conditions of a Connection Request Policy

If you are using a Connection Request Policy, perform the following steps to verify the conditions:

1. Go to the **Secure Wireless Connections Properties** > **Conditions** tab.
2. Verify that the **Conditions** match the Connection Request Policy.

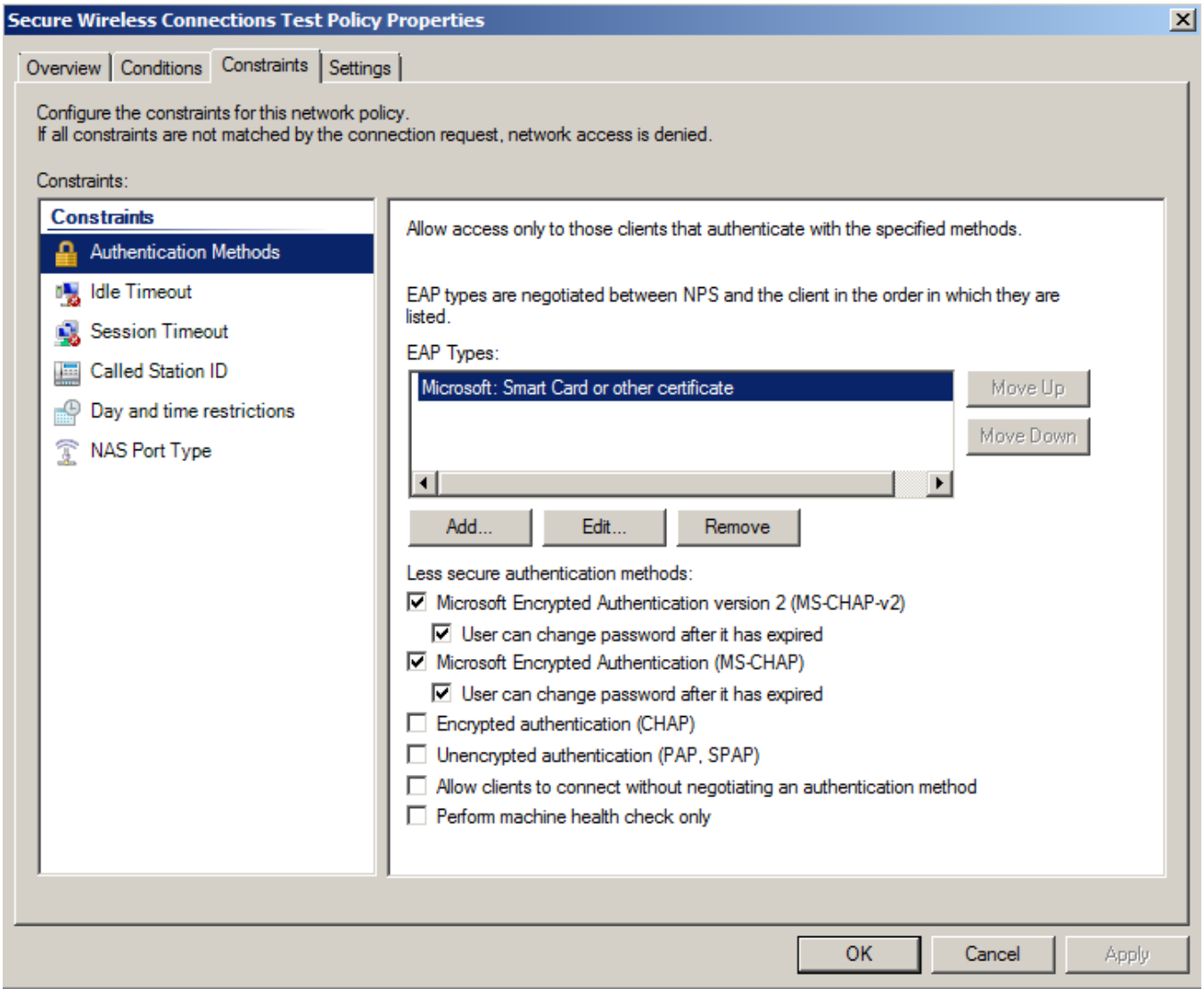
See Connection Request Policies on page 28.

Verify Authentication Method

To verify the authentication method, perform the following steps:

1. On the **Secure Wireless Connections Properties** > **Constraints** tab, select **Authentication Methods**.

FIGURE 16 Secure Wireless Connection Properties



2. Verify that the **Microsoft Smart Card or other certificate** EAP Type is listed.

3. If it is not listed, perform the following steps:.
   a) click **Add**.
   b) On the **Add EAP Type** window, select **Microsoft Smart Card or other certificate**.
   c) Click **OK**.
   d) Select the **Microsoft Smart Card or other certificate** EAP Type.
   e) Use the **Move Up** button to place it at the top of the list.
      EAP Types are negotiated between NPS and the client in the order in which they are listed.
4. Click **OK**.

Verify Network Policy Settings

If you are using a Connection Request Policy, perform the following steps to verify network policy settings:

1. Go to the **Secure Wireless Connections Properties** > **Settings** tab.
2. Verify that your **Settings** match the Connection Request Policy.
   If Conditions and **Constraints** match the connection request, and the **Policy** grants access, these **Settings** are applied.

Connection Request Policies

If you are using the NPS as a RADIUS server to authenticate, you can use the NPS default connection policy.

If you are using the NPS as a RADIUS proxy, you must configure a connection request policy for the remote RADIUS server group. See Configure a Connection Request Policy for RADIUS Proxy on page 29 for more information.

Setting Up RADIUS Proxy on NPS

Overview of Setting Up RADIUS Proxy on NPS

A Network Policy Server (NPS) must be configured as a RADIUS proxy so it can forward connection requests to other RADIUS servers for authentication and authorization.

To configure an NPS as a RADIUS proxy, you perform the following procedures, which are described in the following sections.

- Create a remote server group with one or more RADIUS servers to which RADIUS messages are forwarded.
- Create a connection request policy to forward connection requests and accounting information to the remote RADIUS server group.

Add a Remote RADIUS Server Group for RADIUS Proxy

Remote RADIUS server groups allow you to specify where to forward connection requests when the local NPS server is configured as a RADIUS proxy.

To add a remote RADIUS server group as a RADIUS proxy, perform the following steps:

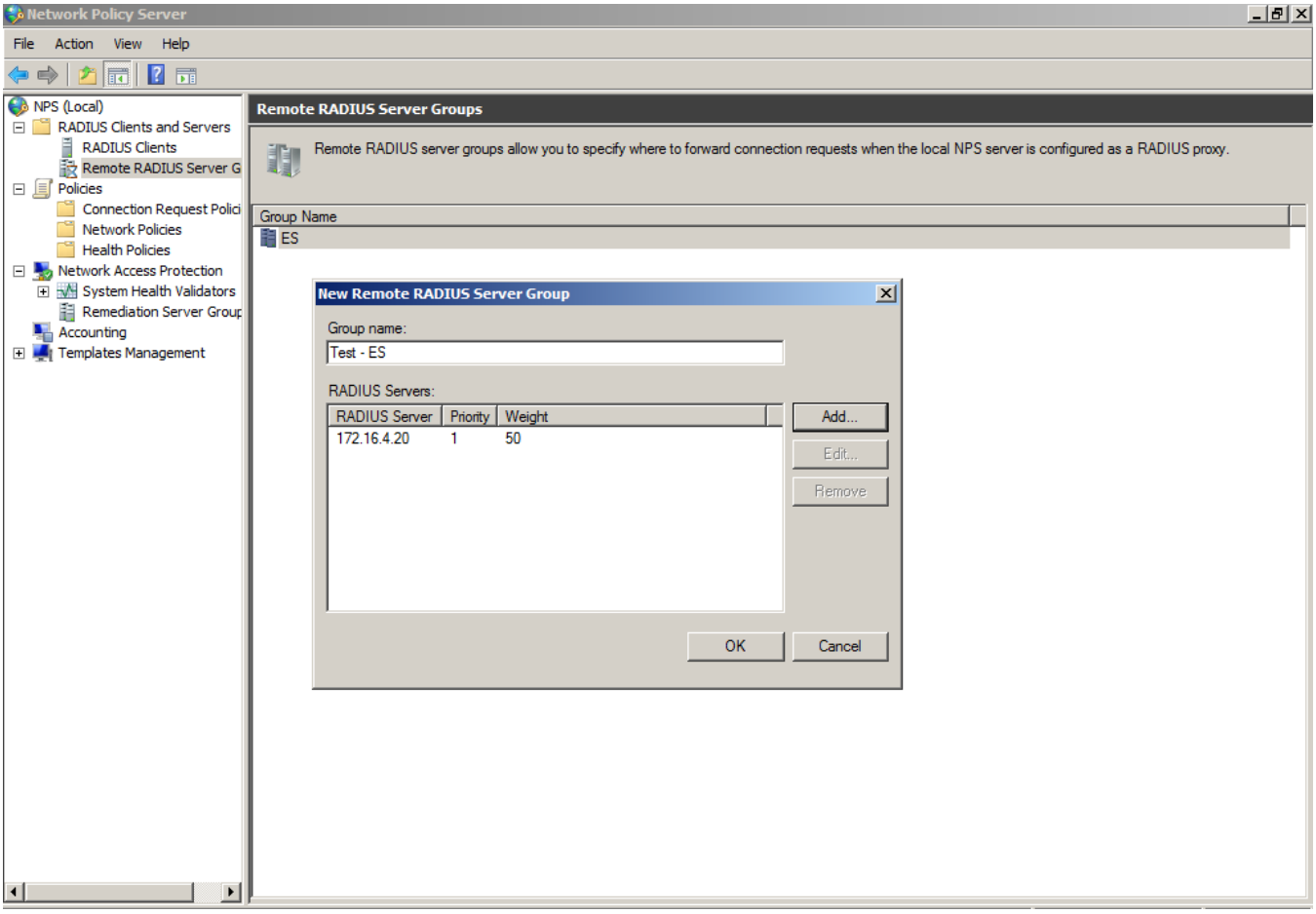
1. On the NPS (local), expand **RADIUS Clients and Servers**, and select **Remote RADIUS Server Groups**.

2. From the **Action** menu, select **New**.

   (Alternately, you can right-click and select **New**.)

3. In the **New Remote RADIUS Server Group** window, enter a **Group name** (for example, enter **ES**), and click **Add**.

FIGURE 17 Remote RADIUS Server Group



4. In the **Add RADIUS server** window, on the **Address** tab, enter the IP address of the NPS acting as a RADIUS server.
5. On the **Authentication/Accounting** tab, enter the **Shared secret** of the NPS, and confirm. Click **OK**.
6. Click **OK** in the **New Remote RADIUS server** window.

   The **ES** remote RADIUS server group is added.

Configure a Connection Request Policy for RADIUS Proxy

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

You can configure a connection policy request to look for <@guest> in the user name, and, if found, forward the request to the remote RADIUS server group. To configure a connection request policy for a RADIUS proxy, perform the following steps:

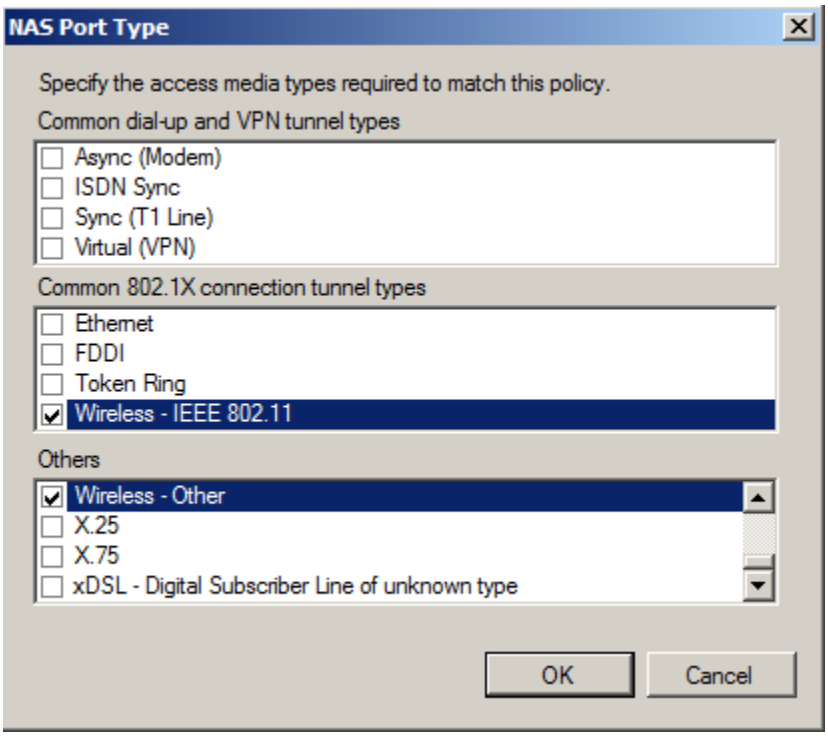
1. On the NPS, expand **Policies** and select **Connection Request Policy**.

2. From the **Action** menu, select **New**

   (Alternately, you can right-click and select **New**.)
3. In the **New Connection Request Policy** window, enter a **Policy name**, and click **Next**.
4. In the **Specify Conditions** window, click **Add**.
5. In the **Select Condition** window, select **NAS Port Type**, and click **Add**.
6. In the **NAS Port Type** window, check the box for the following settings:
   - **Wireless IEEE 802.11** in the **802.1X connection tunnel types** section.
   - **Wireless - Other** in the **Others** section.

   Click **OK**.

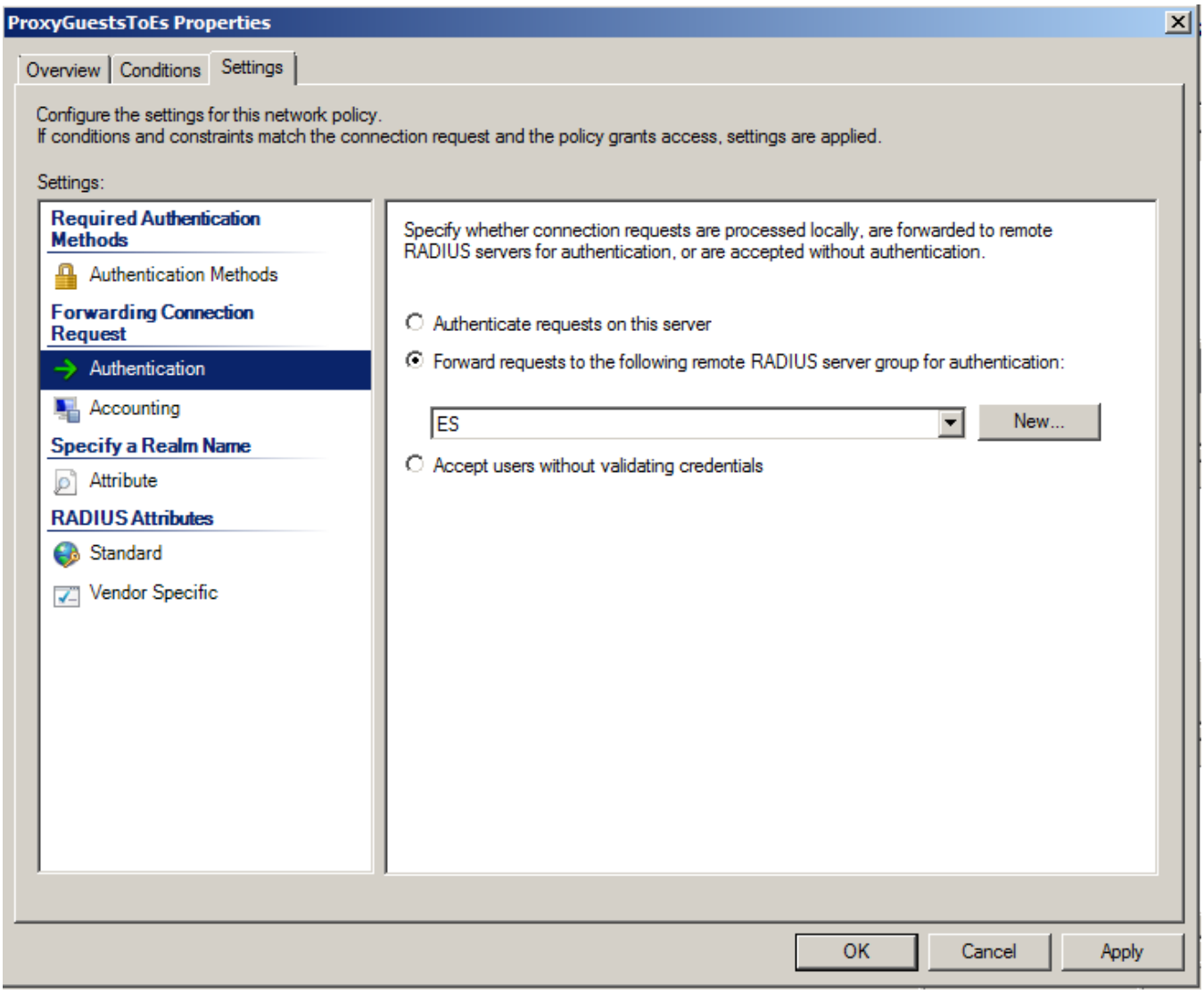
FIGURE 18 NAS Port Type



7. In the **Specify Conditions** window, click **Add**.
8. Select **User name** and click **Add**.
9. In the **User Name** window, enter **.*@guest**. Click **OK**.
10. In the **Specify Conditions** window, click **Next**.

11. In the **Specify Connection Request Forwarding** window, perform the following steps:
    a) In the left pane, select **Authentication**.
    b) In the right pane, select **Forward requests to the following remote RADIUS server group for authentication**.
    c) Select the **ES** remote RADIUS server group you previously created.
    d) Click **Next**.

FIGURE 19 Specify Connection Request - Authentication



12. In the **Configure Settings** window, perform the following steps:
    a) In the left pane, select **Attribute** under **Specify a Realm Name**.
    b) In the right pane, select **User Name** from the **Attribute** list.
    c) Click **Next**.

13. Review the connection request policy configuration in the **Completing Connection Request Policy Wizard** window, and click **Finish**.

With this configuration, *user@guest* is forwarded by the NPS to Cloudpath for authentication, while *user* is authenticated directly by the NPS.

Tips and Troubleshooting

Consider the following issues when you are testing or troubleshooting the configuration for Cloudpath integrated with a Network Policy Server.

Validate Server Certificate Setting in the License Server

When testing your configuration, begin with the **validate server certificate** setting unchecked on the Cloudpath system. This allows you to troubleshoot any certificate configuration issues for the EAPTLS/ PEAP protocol. After it is successful, enable the **validate server certificate** setting in Cloudpath.

After the certificate has been validated, the Network Policy Server (NPS) looks up the name on the certificate in AD and applies network policy.

LDAP

Using LDAP's default port (TCP-389) with a Base DN of the parent Active Directory domain will only show objects from the parent domain. Change the port to 3268, but keep the same Base DN to allow LDAP access to users from the child AD domain (Reference http://technet.microsoft.com/enus/library/cc978012.aspx).

Global Catalog queries are directed to port 3268, which explicitly indicates that Global Catalog semantics are required. By default, ordinary LDAP searches are received through port 389. If you bind to port 389, even if you bind to a Global Catalog server, your search includes a single domain directory partition. If you bind to port 3268, your search includes all directory partitions in the forest. If the server you attempt to bind to over port 3268 is not a Global Catalog server, the server refuses the bind.

OSCP Issues

OSCP Validation

The NPS server first attempts to validate a client certificate using the Online Certificate Status Protocol (OSCP). If the OSCP validation is successful, the validation verification is satisfied; otherwise, it attempts to perform a CRL validation of the user or computer certificate.

OCSP provides the ability to revoke certificates. However, if using OCSP affects the performance of your system, you could disable OCSP and use CRL only.

Certificate revocation checking behavior for NPS can be modified with registry settings (http:// technet.microsoft.com/en-us/library/cc771995%28v=ws.10%29.aspx).

OSCP Server in the DNS

When the client fetches the OCSP response from the CA, it looks up the domain name of the CA's OCSP server in the DNS, as well as establishing a connection to the OCSP server.

If you receive a message that indicates the server cannot resolve the OSCP URL, check the hostname listed in the OSCP URL for the onboard Root CA you created in Cloudpath. See Create the Certificate Authority on page 6. You might need to add this hostname to the DNS of the domain.

Credentials Mismatch

If you receive an error that an authentication failed due to a user credentials mismatch, either the user name provided does not map to an existing user account, or the password was incorrect.

Certificate Template Issues

Common Name

The CN in the certificate template may need to include domain information. This can be specified as *${USERNAME}@domain* within Cloudpath on the specific certificate template.

SAN Other Name

If the NPS logs show an issue with credentials, check the **SAN Other Name Pattern** in the certificate template. The variable listed in the **SAN Other Name Pattern** field should match the variable used in the Common Name Pattern field.

Missing EKU in the RADIUS Server Certificate

RADIUS certificates must contain Microsoft Server EKU-1.3.6.1.5.5.7.3.1. When you create the server certificate template in Cloudpath, you must check the box for the Microsoft Server EKU. See Set Up Client Certificate Template Settings for NPS on page 8 for more information.

EAP Method is Not Available on the Server

If you are receiving a message that the EAP message is not available on the server, check the following configuration issues.

Register the NPS With the Domain

If the NPS is not registered to the domain, you might receive an error message that the EAP method is not available on the server.

To see if the NPS is registered with the domain, right-click the NPS server. If the server is registered, the **Register with domain option** is not available.

If there is a problem with your working registration, try deleting and re-adding the registration using the NPS **Administrator** prompt and the commands in this example:

```
net stop ias
netsh ras delete registeredserver domain=x server=y
net start ias

net stop ias
netsh ras add registeredserver domain=samplecorp.local server=SAMPLE-NPS-Server
net start ias
```

RADIUS Server Certificate Missing Private Key

If the RADIUS server certificate is missing the private key, you might receive an error message that the EAP Method is not available on the server, you might be missing the private key for the RADIUS server certificate.

Be sure that the RADIUS server certificate in the Local Computer Personal Certificate Store shows the **certificate with key** icon

next to it. This indicates that the certificate is signed with the private key. If it does not show the icon, you do not have the private key for the RADIUS certificate. Try downloading the RADIUS certificate and private key in P12 format.

See Download the RADIUS Server Certificate on page 14 for instructions on downloading the certificate from Cloudpath, or use the following command examples from the NPS Administrator prompt:

```
certutil -dspublish -f root.cer NTAuthCA
certutil -enterprise -addstore NTAuth root.cer
```

Certificate Chain Not Trusted

If you receive an error that indicates the certificate chain is not trusted, verify that you have the public certificate and any intermediate certificates for the root CA. See Download the Public Key of the Intermediate CA on page 14 for more information.

© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com