

Cloudpath Enrollment System Integration with Microsoft NPS Configuration Guide, 5.9

Supporting Cloudpath Software Release 5.9

Copyright, Trademark and Proprietary Rights Information

© 2021 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, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED 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	5
About this Document	5
Overview of Network Policy Server	5
Prerequisites	7
Configuring Firewall Rules for Use with Cloudpath	7
Configuring Policies	9
Configuring Cloudpath	15
Overview of Configuring Cloudpath	15
Create the Certificate Authority	15
Set Up Client Certificate Template Settings for NPS	17
Client Certificate Template Advanced Options	19
Set Up a Certificate Template for the NPS Server Certificate	21
Server Certificate Template Advanced Options	22
Generate the Server Certificate for the NPS	24
Download the RADIUS Server Certificate	24
Download the Public Key of the Intermediate CA	25
Adding RADIUS Policies to the NPS Certificate Template	27
Steps to Add Policies	27
Policy Rules	28
Additional Policy Information	31
Testing Policies	31
Test Policy Evaluation - Example 1	31
Test Policy Evaluation - Example 2	33
Test Policy Evaluation - Example 3	35
Viewing Policy Information	37
Viewing RADIUS Attribute Information	39
Switching Pre-Release-5.8 Microsoft NPS Certificate Templates to Policy-Assigned Templates	41
Configuring the Network Policy Server	43
Overview of Configuring the Network Policy Server	43
Import the RADIUS Server Certificate for the NPS	43
Add a Certificates Snap-in	43
Import the RADIUS Server Certificate into the Local Computer Personal Certificate Store	45
Import the Public Key of the Intermediate CA	46
Set Up Roles and Services	47
Network Policy Setup for EAP/TLS	48
Prioritize the 802.1X Configuration	52
Verify Network Policy	55
Review the Network Policy	55
Verify Conditions of a Connection Request Policy	55
Verify Authentication Method	56
Verify Network Policy Settings	57
Connection Request Policies	59

Setting Up RADIUS Proxy on NPS.....	61
Overview of Setting Up RADIUS Proxy on NPS.....	61
Add a Remote RADIUS Server Group for RADIUS Proxy.....	61
Configure a Connection Request Policy for RADIUS Proxy.....	62
Tips and Troubleshooting.....	67
Validate Server Certificate Setting in the License Server.....	67
LDAP.....	67
OSCP Issues.....	67
Credentials Mismatch.....	68
Certificate Template Issues.....	68
EAP Method is Not Available on the Server.....	68
Certificate Chain Not Trusted.....	69

Overview

- [About this Document.....](#) 5
- [Overview of Network Policy Server.....](#) 5
- [Prerequisites.....](#) 7
- [Configuring Firewall Rules for Use with Cloudpath.....](#) 7

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.

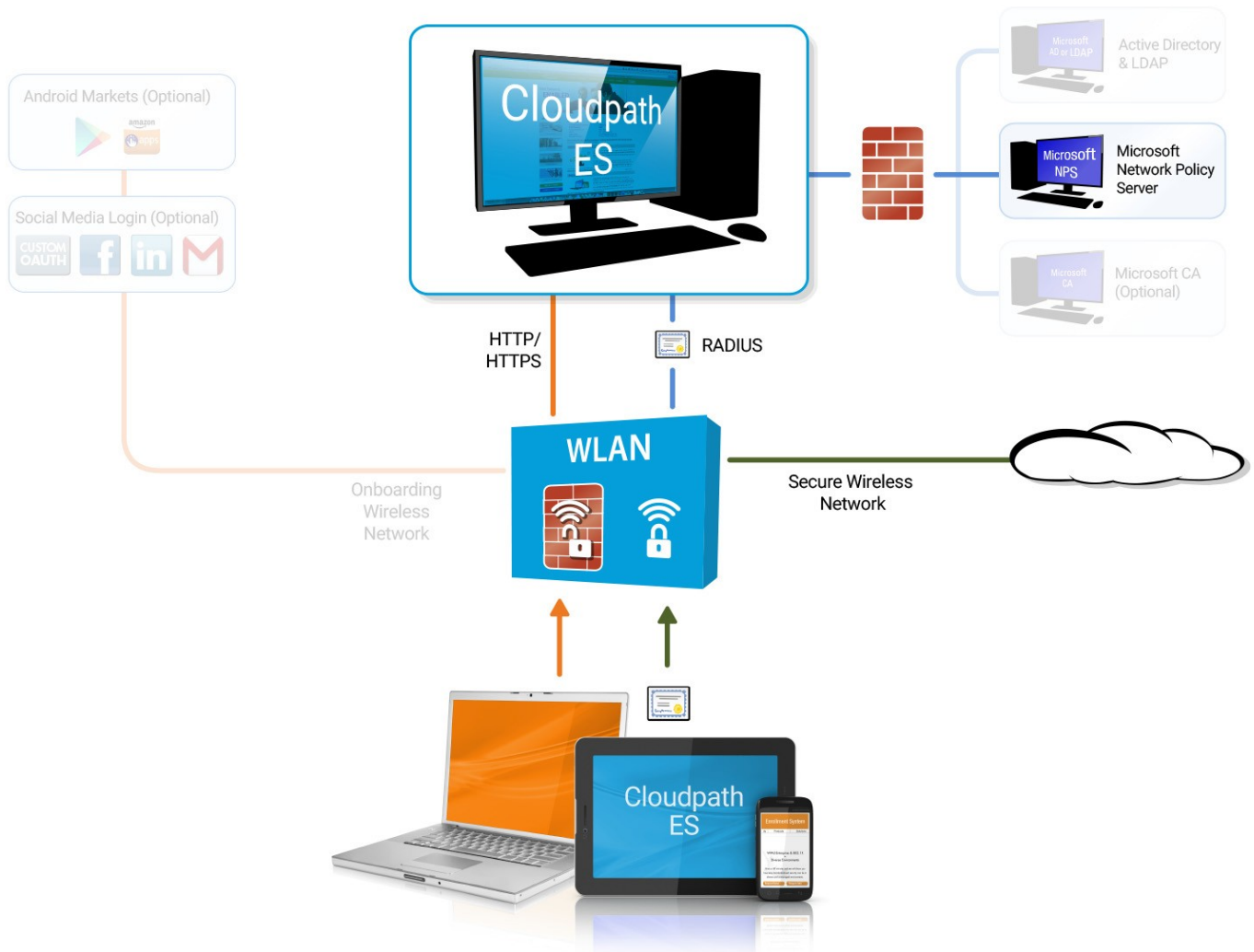
As a RADIUS server, NPS performs authentication and authorization of network connection attempts. NPS authenticates users and devices by verifying their Active Directory credentials.

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.

Overview

Overview of Network Policy Server

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 and 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 67 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 67 for additional information about firewall settings. Additional firewall information can be found on the **Administration > Advanced > Firewall Requirements** page.

Configuring Policies

Policies allow for mapping incoming successful RADIUS authentication requests to a set of RADIUS response attributes based on dynamic conditions of the request. Each policy has an associated RADIUS attribute group which defines the RADIUS response attributes (such as VLAN ID, filter ID, and class). Each authentication is matched against an assigned list of candidate policies in sequential order. Criteria of a policy can include dynamic conditions such as a user's physical location, username, or the time of day.

Policies can be used with EAP-TLS certificate-based authentications through configuration of the certificate template that generated the client certificate.

The following procedure guides you first through creating RADIUS attribute groups for your policies, then creating the policies themselves. You must create at least one RADIUS attribute group before you can configure a policy because a policy needs to have at least one RADIUS attribute group available for selection.

1. In the Cloudpath UI, go to **Configuration > Policies**.
2. Select the **RADIUS Attribute Groups** tab, then click the **Add RADIUS Attribute Group** button.
3. In the ensuing Create Radius Attribute Group screen, enter the information to create the group, then click **Save**.

NOTE

You can configure as many RADIUS Attribute groups as you want. One RADIUS Attribute group will later be assigned to each policy you create.

An example screen and field descriptions follow:

FIGURE 2 Create RADIUS Attribute Screen

- Display Name: The name of the RADIUS attribute group. This should be a descriptive name. It is visible only to Cloudpath administrators
- Description: Optionally, enter a description of this RADIUS attribute group. It is visible only to Cloudpath administrators.
- Assigned Policies: This field lists the names of all the policies that are using this RADIUS attribute group. There will be no policies listed here during the initial configuration of the group.
- Certificate Reply Username: For certificate authentications, the RADIUS server replies by default with the username based on the command name (CN) of the certificate. This username is used by some WLAN infrastructures as the username displayed within the WLAN UI. Options you can select for this field are:
 - Certificate Common Name (default): Returns the certificate CN as the username.
 - Enrollment Username: Returns the username from the enrollment record as the username.
 - Enrollment Username + Device Name: Returns the username and device name from the enrollment record as the username.
 - Certificate Unique ID: Returns the unique ID of the certificate as the username. This option provides anonymity but is traceable.
 - Certificate Common Name + ID: Returns the CN of the certificate plus the unique ID of the certificate as the username.
- VLAN ID: If this field is populated, the VLAN ID is included in the RADIUS reply to the controller for successful authentications. Cloudpath sends Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID. If your network policy is wireless, the Tunnel-Type value is VLAN, the Tunnel-Medium-Type value is 802 (this includes all 802 media plus Ethernet canonical format), and the Tunnel-Private-Group-ID is the integer that represents the VLAN number to which group members will be assigned.
 If the VLAN ID field is left blank, Cloudpath will not return a VLAN ID in the RADIUS reply; therefore the controller assigns the VLAN ID based on its own configuration.
- Filter ID: If this field is populated, the Filter ID is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Filter ID in the RADIUS reply.

- **Class:** If this field is populated, the Class is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Class in the RADIUS reply.
 - **Reauthentication:** The number of seconds included in the RADIUS reply for successful authentications. If the device stays connected for longer than this period, the WLAN or switch requires that the device be reauthenticated. In wireless devices, this causes the encryption keys to rotate.
 - **Additional Attributes:** You can add other attributes in the "Attributes" section of the screen by clicking the + button, and selecting the desired fields and values. These attributes will be returned to the controller in an access-accept RADIUS server packet.
4. Configure your policies:
- a. In the **Configuration > Policies** area of the UI, select the **Policies** tab, then click **Add Policies**.
 - b. In the ensuing Create Policy screen, enter the information to create the policy, then click **Save**.

NOTE

You can configure as many policies as you want.

An example screen and field descriptions follow:

FIGURE 3 Create Policy Screen

- Display Name: The name of the policy. This should be a descriptive name. It is visible only to Cloudpath administrators
- Description: Optionally, enter a description of this policy. It is visible only to Cloudpath administrators.
- "Conditions": In the Conditions section, use any or all of these fields to create the matching criteria you desire so that the appropriate policy gets applied to each user.

NOTE

You can use the asterisks that appear in some of the Conditions fields, when selected, to denote that any value is acceptable in the place of the asterisk.

- Username Regex: When the user is prompted for credentials, the username specified by the user will be verified against this regular expression for proper format. For example, `^d{8}$` will ensure that the user enters an 8-digit id.

NOTE

Due to the complexity of regular expressions, it is recommended to use this field only if you are experienced with regular expressions. If you need assistance creating a regular expression to match your needs, contact support.

- SSID (regex): A regular expression that lists any Wi-Fi SSID(s) to which you want to limit this policy.
- NAS Identifier: The Network access server (NAS) identifier to limit the policy.

NOTE

If you use this field, and no NAS Identifier is provided in the response, the policy will be "false" and will not get applied to a user.

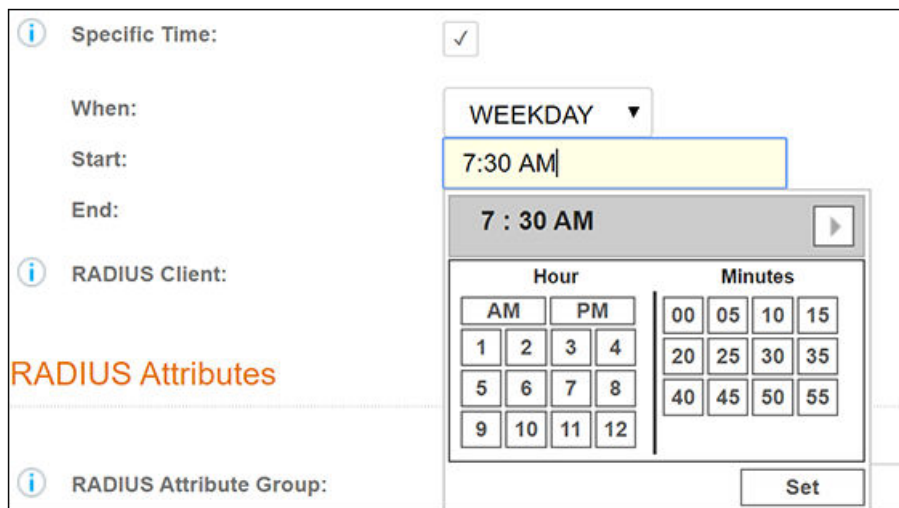
- RADIUS Realm (regex): The RADIUS realm to use in this policy, in the form of @company.com or company.com
- DPSK Reference Name (regex): A regular expression to test against the DPSK Reference Name.

NOTE

This field is applicable only when the policy is applied to a DPSK pool.

- Allow by AD Group: A regular expression that defines the usernames within the Active Directory that this policy allows.
- Specific Time: If checked, drop-downs appear where you can specify the days and times that this policy allows enrollment. Be sure to click the **Set** button to set the desired time (see the following illustration):

FIGURE 4 Setting a Time for a Policy



- RADIUS Client: If you check this box, you are presented with a drop-down where you can then select a RADIUS client if you have already configured this client in the **Configuration > RADIUS Server > Clients** tab. This RADIUS client would then be associated with this policy.
- RADIUS Attribute Group: From this drop-down, select the attribute group that you want associated with this policy.

The following illustration shows the Policies tab after one policy has been added. The information shown in the table represents the policy configuration shown in the example in Figure 3. The attribute group name and its attributes come from the attribute group name selected in the Create Policy Screen drop-down list. The RADIUS attribute information shown below comes from the example in Figure 2.

FIGURE 5 Policies Table Example After One Policy Is Configured

The screenshot shows a web interface for configuring policies. At the top, there is a breadcrumb 'Configuration > Policies' and a tab 'RADIUS Attribute Groups'. Below this, there is a section titled 'Policies' with an 'Add Policy' button. A table displays the configured policy. The table has columns for Name, Policy, Attribute Group Name, Attributes, DPSK Rel., Cert.Template Rel., and PEAP Rel. The single row shows a policy named 'Building 1 on weekdays' with a specific NAS Id and time restriction, associated with 'VLAN 1' and specific attributes.

	Name	Policy	Attribute Group Name	Attributes	DPSK Rel.	Cert.Template Rel.	PEAP Rel.
	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	0	0	0

Configuring Cloudpath

- Overview of Configuring Cloudpath..... 15
- Create the Certificate Authority..... 15
- Set Up Client Certificate Template Settings for NPS..... 17
- Set Up a Certificate Template for the NPS Server Certificate..... 21
- Generate the Server Certificate for the NPS..... 24
- Download the Public Key of the Intermediate CA..... 25

Overview of Configuring Cloudpath

If you deploy certificate-based authentication, a server running NPS must have a server certificate. During the authentication 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:

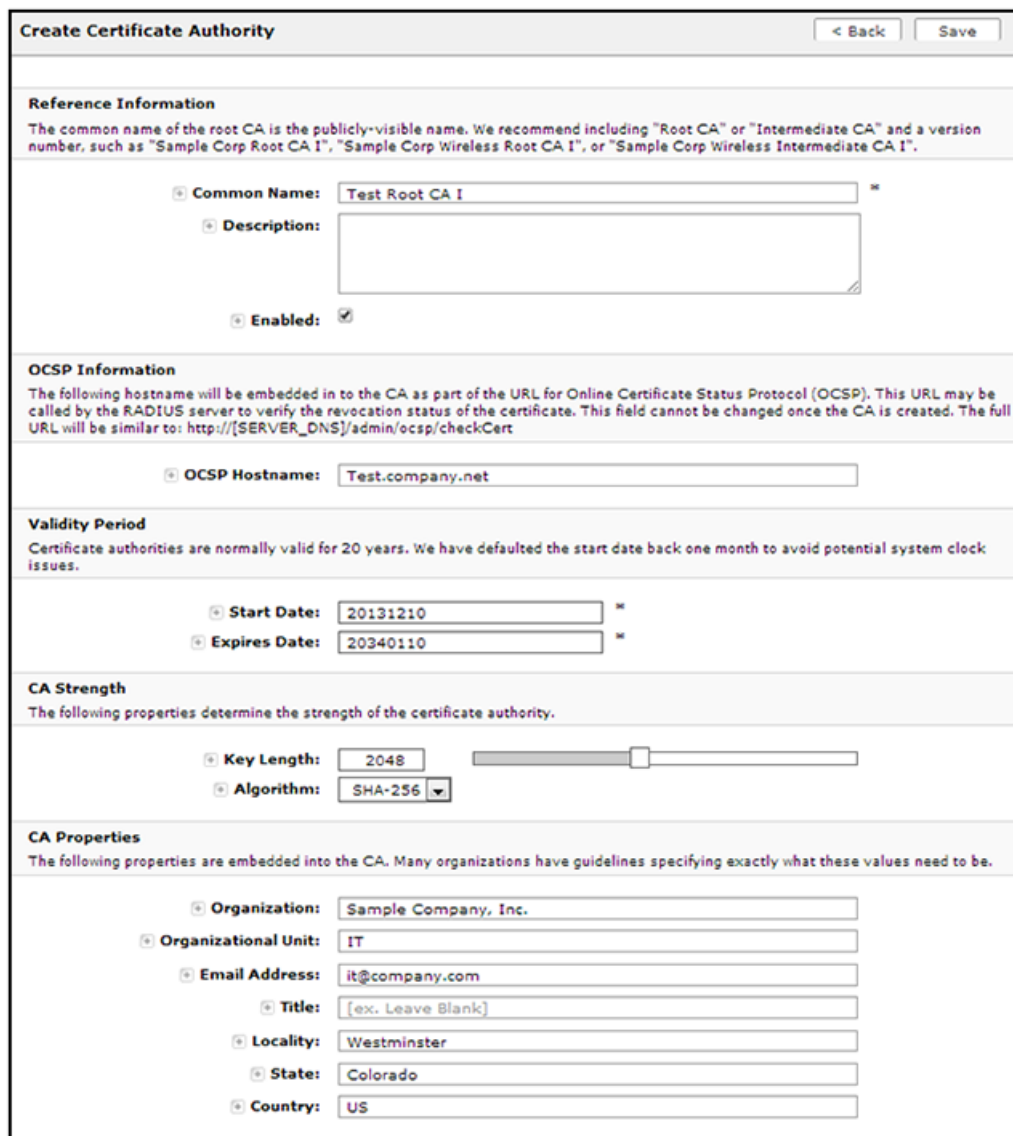
1. From the Cloudpath left menu, select **Certificate Authority > Manage CA**.
2. Click **Add/Upload CA**.
3. Select **Generate New Certificate Authority**.

Configuring Cloudpath

Create the Certificate Authority

- 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.
 - OCSP 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 6 Create Root CA



Create Certificate Authority < Back Save

Reference Information
The common name of the root CA is the publicly-visible name. We recommend including "Root CA" or "Intermediate CA" and a version number, such as "Sample Corp Root CA I", "Sample Corp Wireless Root CA I", or "Sample Corp Wireless Intermediate CA I".

Common Name: Test Root CA I *
Description:
Enabled:

OCSP Information
The following hostname will be embedded in to the CA as part of the URL for Online Certificate Status Protocol (OCSP). This URL may be called by the RADIUS server to verify the revocation status of the certificate. This field cannot be changed once the CA is created. The full URL will be similar to: http://{SERVER_DNS}/admin/ocsp/checkCert

OCSP Hostname: Test.company.net

Validity Period
Certificate authorities are normally valid for 20 years. We have defaulted the start date back one month to avoid potential system clock issues.

Start Date: 20131210 *
Expires Date: 20340110 *

CA Strength
The following properties determine the strength of the certificate authority.

Key Length: 2048
Algorithm: SHA-256

CA Properties
The following properties are embedded into the CA. Many organizations have guidelines specifying exactly what these values need to be.

Organization: Sample Company, Inc.
Organizational Unit: IT
Email Address: it@company.com
Title: [ex. Leave Blank]
Locality: Westminster
State: Colorado
Country: US

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.

Configuring Cloudpath

Set Up Client Certificate Template Settings for NPS

4. Select **Client Certificates**.

FIGURE 7 Create Client Certificate Template

Certificate Authority > Manage Templates > Create

Client Certificates

Used on clients to authenticate the client. The decoration of the username within the certificate allows RADIUS policies to be applied appropriately.

Username Decoration:

- username@byod.company.com
- username@contractor.company.com
- username@faculty.company.com
- username@guest.company.com
- username@it.company.com
- username@student.company.com
- username@other.company.com

Grant Access Until: 1 Years after issuance.

Configure Advanced Options:

Lifecycle Notifications

The Cloudpath ES supports events related to the lifecycle of the certificate. These events allow the system to interact with the end-user, the administrator, as well as external systems. Additional notifications can be configured once the template is created, but the notifications below are some of the most common ones.

Notifications:

- Send welcome email on issuance.
- Send email 7 days before certificate expiration.
- Send email if certificate is revoked.
- Email administrator if revoked certificate is used.

RADIUS Response

By default, this certificate template will be honored for RADIUS authentications. RADIUS attribute policies may be assigned under the 'RADIUS Policies' tab of the certificate template once created.

Server Certificates

Used on servers, such as a RADIUS server, to identify the server to a client.

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**. For more information about the advanced options, refer to [Client Certificate Template Advanced Options](#) on page 19.

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. After the template has been created, you can assign RADIUS attribute policies from within the "RADIUS Policies" tab. For more information, refer to [Adding RADIUS Policies to the NPS Certificate Template](#) on page 27.

NOTE

By default, this certificate template will be honored for RADIUS authentications.

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. The Modify Certificate Template page is shown below in two screens.

TABLE 1 Fields on the Modify Certificate Template Page

Field	Action
Certificate Template 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.
RADIUS Options	Used for RADIUS policy information. If no policies have been assigned to this template, you may add policies to an existing template by following the instructions in Adding RADIUS Policies to the NPS Certificate Template on page 27.
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 ECU - 1.3.6.1.5.5.7.3.2*. This establishes the **Extended Key Usage** properties for the certificate.

Configuring Cloudpath
Set Up Client Certificate Template Settings for NPS

FIGURE 8 Modify Client Certificate Template - Screen 1

Certificate Template Information

Certificate Template Name: *

Certificate Authority: Jack Test Root CA 1 test 22

Notes:

Enabled?

Identity

The following property is normally used to provide identity information within the certificate. Variables, such as `$(USERNAME)`, will be replaced at the time of issuance with the appropriate value from the enrollment.

Common Name Pattern:

Validity Period

The following properties determine the lifespan of the issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with end-user system clocks.

Start Date: before issuance.

Expiration Date: after issuance.

OCSP Monitoring: Revoke if unseen for days.

FIGURE 9 Modify Client Certificate Template - Screen 2

RADIUS Options

Allow Authentication via RADIUS:

The following listing displays the currently assigned policies that will be evaluated for each authentication for this template to determine RADIUS response attributes. Changes to assigned policies may be made via the 'RADIUS Policies' tab for a Certificate Template.

Assigned Candidate Policies:

Name	Policy	Attributes
Building 1 on weekends	NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	Reply Username: 'Certificate Common Name (Default)' VLAN: '2'
Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	Reply Username: 'Certificate Common Name (Default)' VLAN: '1'
Username and RADIUS Realm	Username (Regex): 'bob' RADIUS Realm(Regex): 'company.com'	Reply Username: 'Certificate Common Name (Default)' VLAN: '3' Filter ID: '10'

Default Access(No Match): **Accept** ▾

- > Certificate Strength
- > Organization Information
- > Advanced Settings
- > Cleanup

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:

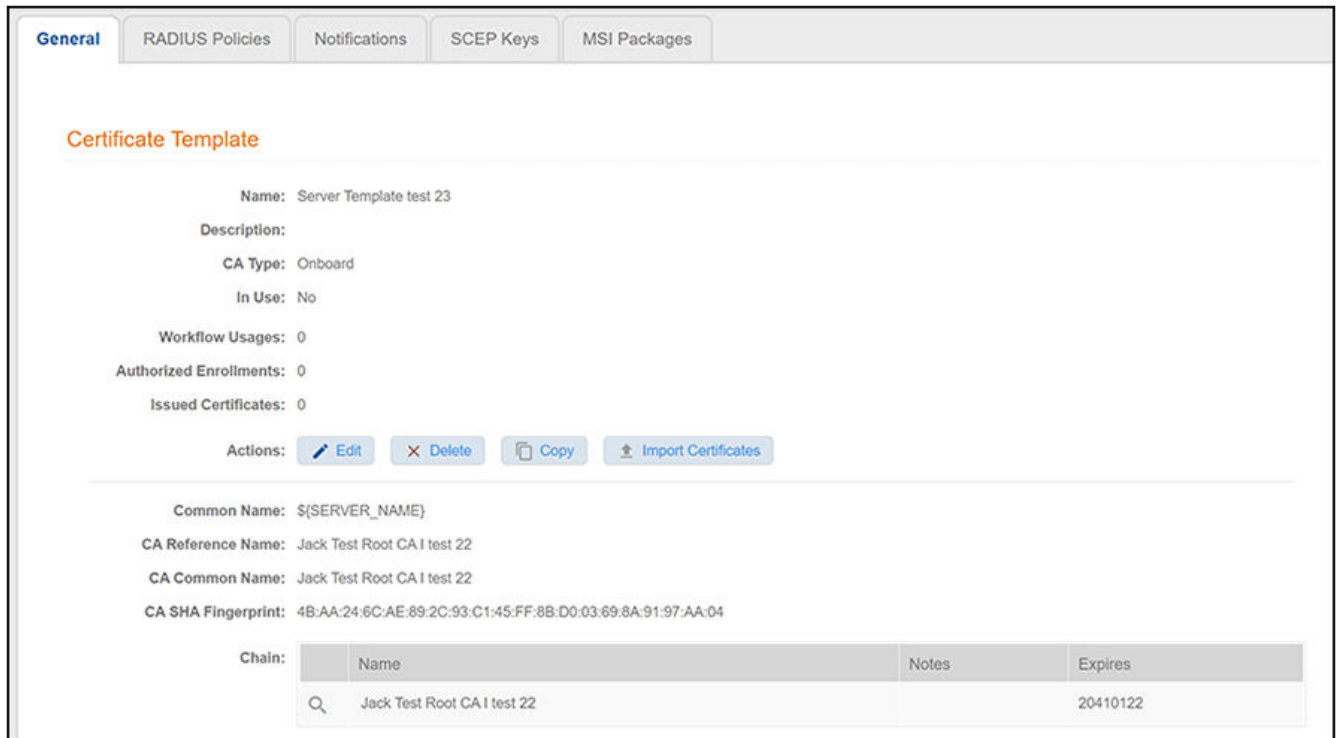
1. From the Cloudpath left menu, select **Certificate Authority > Manage Templates**.
2. Click **Add Template** to create a new certificate template.
3. Choose **Use an onboard certificate authority**, and select the onboard CA you created in the previous section.
4. Select **Server Certificates**.

Configuring Cloudpath

Set Up a Certificate Template for the NPS Server Certificate

5. Enter a validity period for the server certificate, then click **Next** to use the default settings. The initial configuration is complete, and a screen such as the following is displayed.

FIGURE 10 NPS Onboard Server Certificate Example Configuration Screen



6. From this view, you can do the following:
 - Add notifications, SCEP keys, or MSI packages by clicking on the corresponding tabs.
 - Click **Edit** to edit current settings as well as to configure advanced settings. For more information, refer to [Server Certificate Template Advanced Options](#) on page 22.

NOTE

The RADIUS Policies tab is applicable only if the certificate template may issue client certificates based on the template EKU setting. Therefore, the tab does not apply to the default server certificate template.

Server Certificate Template Advanced Options

The following table describes the actions you can take for each of the fields on the Modify Certificate Template page, which displays if you click **Edit** from the Certificate Template Configuration screen ([Figure 10 on page 22](#)). The Modify Server Certificate Template page is shown below in two screens.

TABLE 2 Fields on the Modify Certificate Template Page

Field	Action
Certificate Template Information	Enter information in the Certificate Template Name and Notes fields. This information is for reference only. Enable the template.

TABLE 2 Fields on the Modify Certificate Template Page (continued)

Field	Action
Identity	Enter the Common Name Pattern used to determine the common name for certificates generated using the template. Variables, such as <code>\${SERVER_NAME}</code> 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 11 Modify Server Certificate Template - Screen 1

Certificate Template Information

i Certificate Template Name: *

i Certificate Authority: Jack Test Root CA I test23

i Notes:

i Enabled?

Identity

The following property is normally used to provide identity information within the certificate. Variables, such as `${USERNAME}`, will be replaced at the time of issuance with the appropriate value from the enrollment.

i Common Name Pattern:

Configuring Cloudpath

Generate the Server Certificate for the NPS

FIGURE 12 Modify Server Certificate Template - Screen 2

Validity Period

The following properties determine the lifespan of the issued certificates. We recommend setting the start date to 1 month before issuance to avoid issues with end-user system clocks.

- Start Date:** Specific Date (dropdown) 20210124
- Expiration Date:** 1 (input) Years (dropdown) after issuance.
- OCSP Monitoring:** Revoke if unseen for 30 (input) days.

▼ Certificate Strength

The following properties determine the strength of the certificates.

- Key Length:** 2048 (input) [Slider]
- Algorithm:** SHA-256 (dropdown)

> Organization Information

> Advanced Settings

> Cleanup

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 CAs**.
2. Click the wrench icon for the onboard CA that you previously created .
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 13 Download Public Key of Intermediate CA

The screenshot displays the configuration page for the 'Anna Test Intermediate CA I'. It includes fields for Common Name, Parent CA, and SHA Fingerprint. Below this, organizational details like 'Sample Company, Inc.' and 'IT' are listed alongside technical specifications such as 'Start Date', 'Expires', 'Key Length', and 'Algorithm'. A 'Public Key' section is highlighted with a red box, containing buttons for 'View', 'Download PEM', 'Download DER', and 'View Details'. Other sections include 'Chain', 'Private Key', 'P12 Format', 'Sub CAs', and a 'Templates' table.

Templates:	Name	Notes	Common Name Pattern
Add	BYOD Policy Template		`\${USERNAME}@byod.company.com`
	Guest Policy Template		`\${USERNAME}@guest.company.com`
	Server Template		`\${SERVER_NAME}`
	username@byod.company.com		`\${USERNAME}@byod.company.com`
	username@test.company.com		`\${USERNAME}@test.company.com`

Adding RADIUS Policies to the NPS Certificate Template

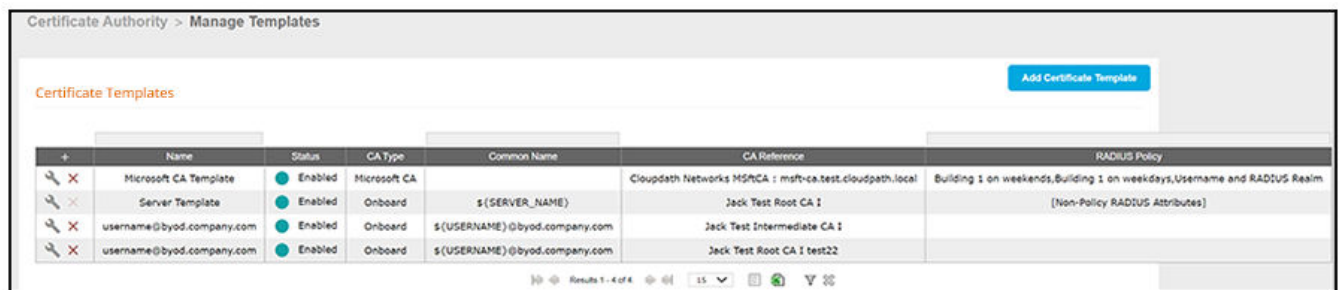
You can add as many policies as you want, but only one policy can be associated with a given user. For a user to successfully connect to the network, the user must be a match for at least one policy (or you can allow users to connect even if they do not match a policy).

Steps to Add Policies

Follow these steps to add a policy from the RADIUS Policies tab of a configured certificate template:

1. If you are not already in the RADIUS Policies tab of a configured certificate template, go to **Certificate Authority > Manage Templates** to view all existing certificate templates:

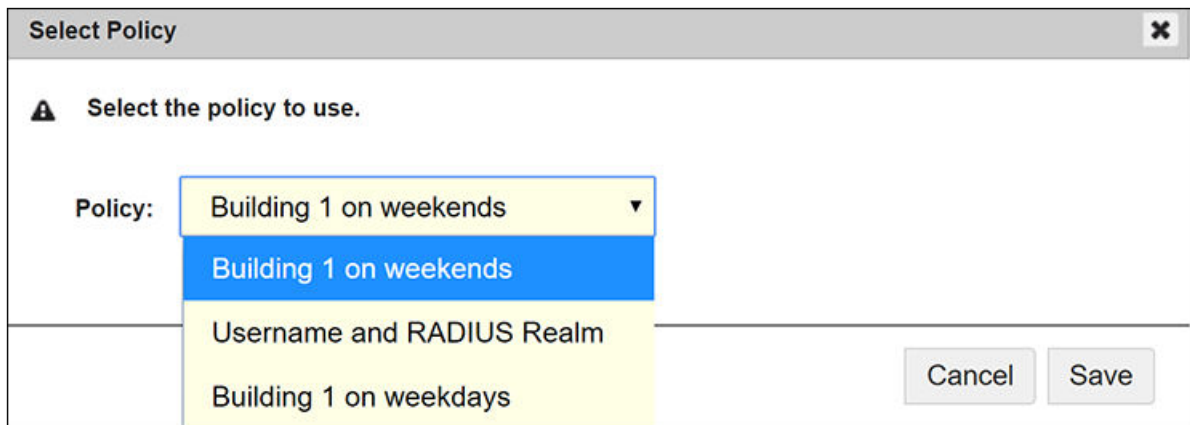
FIGURE 14 Certificate Templates View



	Name	Status	CA Type	Common Name	CA Reference	RADIUS Policy
	Microsoft CA Template	Enabled	Microsoft CA		Cloudpath Networks MSNCA : mst-ca.test.cloudpath.local	Building 1 on weekends, Building 1 on weekdays, Username and RADIUS Realm
	Server Template	Enabled	Onboard	\$(SERVER_NAME)	Jack Test Root CA 1	[Non-Policy RADIUS Attributes]
	username@byod.company.com	Enabled	Onboard	\$(USERNAME)@byod.company.com	Jack Test Intermediate CA 1	
	username@byod.company.com	Enabled	Onboard	\$(USERNAME)@byod.company.com	Jack Test Root CA 1 test22	

2. Click the wrench icon for the desired Microsoft NPS onboard client certificate template.
3. In the ensuing screen, click the RADIUS Policies tab, then click **Assign Policy**. The Select Policy Drop-down list appears, as shown in the following example list. The policies that you have already configured are available for you to add:

FIGURE 15 Select Policy Drop-down List



Select Policy

Select the policy to use.

Policy: Building 1 on weekends ▼

- Building 1 on weekends
- Username and RADIUS Realm
- Building 1 on weekdays

Cancel Save

Adding RADIUS Policies to the NPS Certificate Template Policy Rules

4. Select the policy you wish to add, then click **Save**.
5. Continue to add policies as you desire. If you have added all available policies, you will receive the message: " All Defined Policies have been assigned."

Policy Rules

The following illustration shows an example of how the page appears after three policies have been added:

FIGURE 16 Policies Added to Microsoft NPS Onboard Client Certificate Template

The screenshot displays the 'RADIUS Policies' tab in the NPS configuration console. At the top, a yellow banner indicates 'Certificate Template Policy Added'. Below this, a diagram shows a laptop logging in by certificate to a server, with RADIUS policies (e.g., VLAN 50) being returned. The 'Certificate Template' section shows the name 'username@byod.company.com'. The 'RADIUS Policies' section includes buttons for '+Assign Policy', 'Test Policy Evaluation', and 'Reset Counts'. A table lists three assigned candidate policies:

Assigned Candidate Policies:	Name	Description	Policy	Attributes	Usage Count
X ^ v	Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	Reply Username: 'Certificate Common Name (Default)' VLAN: '2'	0
X ^ v	Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	Reply Username: 'Certificate Common Name (Default)' VLAN: '1'	0
X ^ v	Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'company.com'	Reply Username: 'Certificate Common Name (Default)' VLAN: '3' Filter ID: '10'	0

When none of the policies are matched, the default access will be: Accept

- There may be many policies whose criteria are matched by a user, but the first policy that is a match is the one that gets applied. For example, if you have three policies, as shown above, the order in which you have them listed is the order in which they will be tested for matches with an enrolling user.

NOTE

You can use the arrows in the screen show above to list the policies in the desired order. If you want to remove a policy from being used in the template, click the X next to the policy, then confirm the removal of the policy when prompted.

- Because the "Building 1 on weekends" policy is listed first, the matching criteria in that policy (listed in the Policy column) will first be checked against an enrolling user. If there is a match, the policy is applied to the user (meaning that the attributes listen in the Attributes column are applied to the user). If there is no match, the next policy ("Building 1 on weekdays") is checked against the enrolling user, and so on.

NOTE

If none of the policies match a specific user, the default access setting (configured when you create a certificate template) is used to either accept or reject the user. In the example above, at the bottom of the illustration, the default access is to accept the user because that is how the field was set when the certificate template was configured.

Additional Policy Information

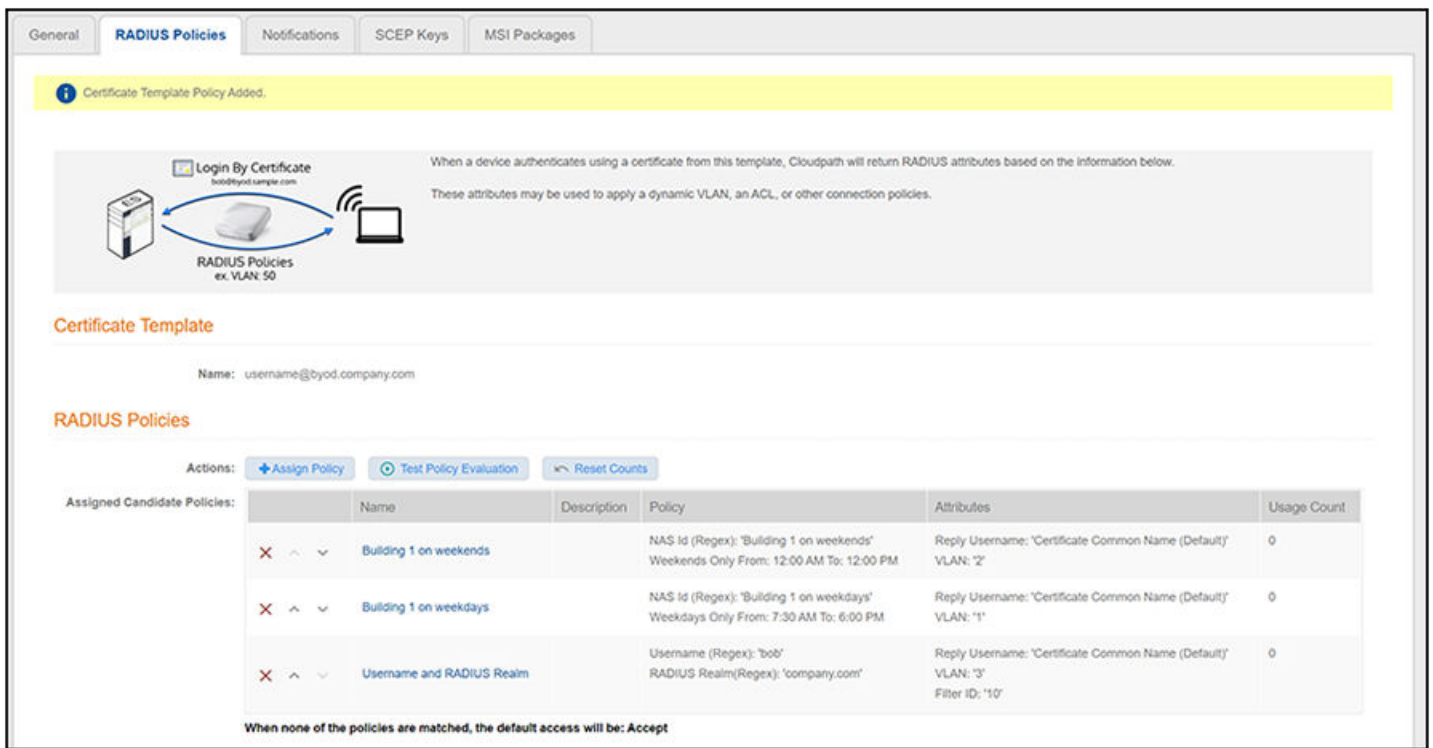
- Testing Policies..... 31
- Viewing Policy Information..... 37
- Viewing RADIUS Attribute Information..... 39

Testing Policies

You can test your policies to be sure they are working as desired before you implement them in a live environment.

The following screen shows an example of three policies that have been added to a Microsoft NPS onboard client certificate template. To get to this screen, go to **Certificate Authority > Manage Templates**, click the wrench icon next to the desired certificate template, then click the **RADIUS Policies** tab.

FIGURE 17 Three-Policy Example



Test Policy Evaluation - Example 1

1. Click the **Test Policy Evaluation** button (see the screen above).
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 18 Test Policy Selection - Example 1 Values

Configuration > DPSK Pools > DPSKs > Test Policy Selection
Cancel Apply ▶

User, Radius and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

i
Username:

i
SSID:

i
Authentication Groups:

i
NAS ID:

i
DPSK Reference Name

i
Authentication Date:

i
Authentication Time

i
Client Short Name:

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob*' RADIUS Realm(Regex): '@company.com'	VLAN: '3' Filter ID: 'filter ID 10'

The sample values shown above have been entered to test that the "Building 1 on weekdays" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

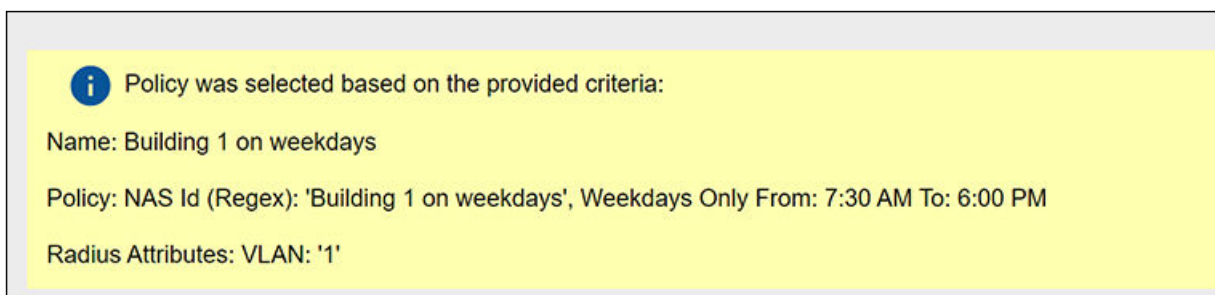
NOTE

The sample values can include fields that are not configured in a policy, and could still be a match for the policy. For example, there could be a value entered in the Client Short Name field in the example above, and it would have no impact on the results of the policy evaluation test because none of the three policies shown above show a value for Client Short Name (as evidenced by the values shown in the Policy column for each policy).

- Username (required): Must be a valid username that your Cloudpath system will accept when this user attempts enrollment.
- SSID: Matches the Wi-Fi SSID name for the connecting device. If this field is populated, this will match only the Wi-Fi based connections.

- Authentication Groups (required): The list of groups returned from a user (as configured in your authorization server; you need a workflow step that requires authentication to an authorization server for the user to have groups).
 - NAS ID: The NAS ID that is expected to be returned from the controller. In the example above, the value "Building 1 on weekdays" is entered because it matches the NAS ID of the "Building 1 on weekdays" policy.
 - Authentication Date: The date on which the user would attempt to authenticate. In the example above, the date is on a weekday because the "Building 1 on weekdays" policy specifies weekdays only for authentication.
 - Authentication Time: The time when the user would attempt to authenticate. In the example above, the time is 5:10 p.m., which falls in the range of 7:30 a.m. to 6 p.m. that the policy specifies for authentication.
 - Client Short Name: RADIUS Client-Shortname expected to be returned from the controller.
3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
- a. The values entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy.
 - b. The values entered are next compared to the second policy in the list, which is the "Building 1 on weekdays" policy. You can see that the values entered for testing all *do* match those listed for this policy. Therefore, the expected behavior is that, when you click the **Apply** button, the "Building 1 on weekdays" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
 - c. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 19 Test Policy Selection - Example 1 Results



Test Policy Evaluation - Example 2

1. Click the **Test Policy Evaluation** button.
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 20 Test Policy Selection - Example 2 Values

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob*' RADIUS Realm(Regex): '@company.com'	VLAN: '3' Filter ID: 'filter ID 10'

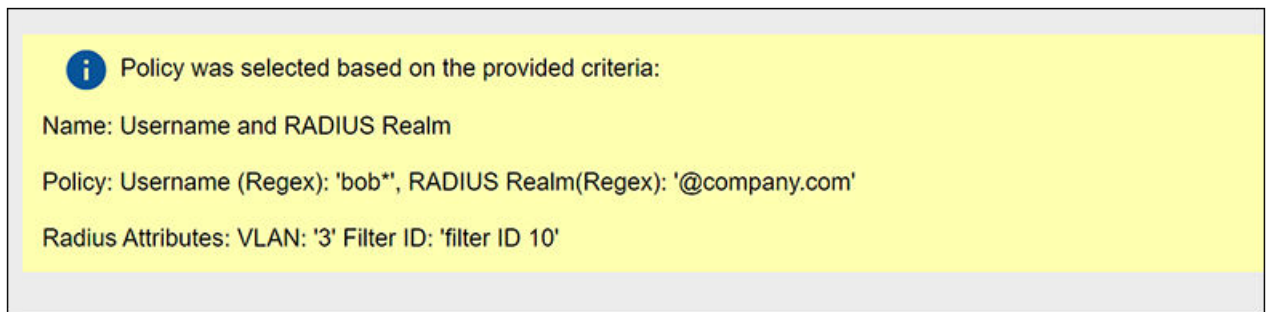
The sample values shown above have been entered to test that the "Username and RADIUS Realm" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
 - a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy. For example, the "Building 1 on weekends" policy includes a Regex value of "Building 1 on weekends," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.
 - b. The values entered in the upper portion of the screen are next compared to the policy named "Building 1 on weekdays" because that is the next policy listed (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekdays" policy either. For example, the "Building 1 on

weekdays" policy includes a Regex value of "Building 1 on weekdays," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.

- c. The values entered are next compared to the third policy in the list, which is the "Username and RADIUS Realm" policy. You can see that the values entered for testing all *do* match the conditions listed for this policy: A username in the form of bob* (where the * can be replaced with any value) and a RADIUS realm (in the username field for the sample test values) in the form of company.com. Therefore, the expected behavior is that, when you click the **Apply** button, the "Username and RADIUS Realm" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
- d. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 21 Test Policy Selection - Example 2 Results



Test Policy Evaluation - Example 3

1. Click the **Test Policy Evaluation** button.
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 22 Test Policy Selection - Example 3 Values

Configuration > DPSK Pools > DPSKs > Test Policy Selection Cancel Apply ▶

User, Radius and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

i Username:

i SSID:

i Authentication Groups:

i NAS ID:

i DPSK Reference Name:

i Authentication Date:

i Authentication Time:

i Client Short Name:

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob*' RADIUS Realm(Regex): 'company.com'	VLAN: '3' Filter ID: 'filter ID 10'

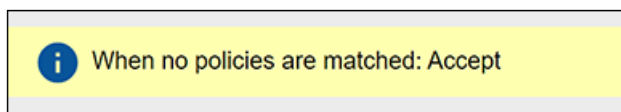
The sample values shown above have been entered to test that no policy will be applied to users who do not match the criteria defined by any of the policies belonging to the certificate template (refer to the information in the "Policy" column in the figure above).

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
 - a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy. For example, the "Building 1 on weekends" policy includes a Regex value of "Building 1 on weekends," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.
 - b. The values entered in the upper portion of the screen are next compared to the policy named "Building 1 on weekdays" because that is the next policy listed (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekdays" policy either. For example, the "Building 1 on

weekdays" policy includes a Regex value of "Building 1 on weekdays," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.

- c. The values entered are next compared to the third policy in the list, which is the "Username and RADIUS Realm" policy. You can see that the username does not match the conditions listed for this policy, eliminating any chance of a match to this policy. Therefore, the expected behavior is that, when you click the **Apply** button, you should receive a message indicating that no policies matched, but that the user is still accepted onto the network. provided that the " Default Access (No Match)" field was configured to "Accept" a user if there was no policy match. You can confirm this is true for the example Microsoft CA Certificate template by checking [Figure 17](#).
- d. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 23 Test Policy Selection - Example 3 Results



Viewing Policy Information

To view your currently configured policies, go to **Configuration > Policies** in the UI, and be sure to highlight the Policies tab.

The following table shows you an example of what a policy table looks like after three different policies have been created and assigned to DPSK pools, certificate templates, or PEAP.

FIGURE 24 Policy Table Example

Policies									Add Policy		
	Name	Policy	Attribute Group Name	Attributes	DPSK Rel.	Cert.Template Rel.	PEAP Rel.				
Q ✖	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	1	0	0				
Q ✖	Building 1 on weekends	NAS Id (Regex): 'Building 1 on weekends', Weekends Only From: 12:00 AM To: 12:00 PM	VLAN 2	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	1	0	0				
Q ✖	Username and RADIUS Realm	Username (Regex): 'bob', RADIUS Realm(Regex): 'company.com'	VLAN 3 and Filter ID	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	1	0	0				

Results 1 - 3 of 3 | 15 | [Icons]

You can use the policy table as follows:

Additional Policy Information

Viewing Policy Information

TABLE 3 Description of Policy Table

Column Title	Description
+	<ul style="list-style-type: none"> You can view details of the policy by clicking on the magnifying glass icon (for an example of the Policy Information screen that gets invoked, see Figure 25). You can edit the policy by clicking on the pencil icon. If the policy has not yet been assigned (such as to PEAP, a certificate template, or a DPSK pool), there will be a X next to the policy name. Clicking that X deletes the policy. However, in the example above, all three policies are in use; therefore the - sign denotes that you cannot delete the policy as long as it remains in use. You would first need to remove the policy from where it is being used before you can delete the policy from the table shown above.
Name	The name of the policy as configured in the Display Name field in the Policy configuration screen, an example of which is shown in Figure 3 on page 12.
Policy	All the conditions that you set when you created the policy are listed in this column. For example, the "Building 1 on weekdays" policy conditions are the ones that were configured in the example shown in Figure 3 on page 12.
Attribute Group Name	The name of the group that has been selected in the RADIUS Attribute Group drop-down when the policy was created. For the "Building 1 on weekdays" policy shown in this example, the group name VLAN 1 matches the selection that was shown in the example in Figure 3 on page 12.
Attributes	Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 2 on page 10. NOTE The "Reply Username" attribute applies only to certificate templates.
DPSK Rel, Cert Template Rel, and PEAP Rel	The number of times that a policy has been assigned to each category of authentication.

FIGURE 25 Policy Information Screen Example

Policy Information

Name: Building 1 on weekdays

Description:

Conditions: NAS Id (Regex): 'Building 1 on weekdays',
Weekdays Only From: 7:30 AM To: 6:00 PM

RADIUS Attribute Group: Reply Username: 'Certificate Common Name (Default)',
VLAN: '1'

Relationships

Type	Location	Usage Count
PEAP	PEAP	0
DPSK	DPSK Pool 17	0
CERTIFICATE	username@byod.company.com	0

The screen above indicates that the policy is currently being used by PEAP, one DPSK pool, and one certificate. The "Location" column of this screen in the UI provides live links to the specific configuration areas where the policy is used.

The Usage column will be incremented each time a device is assigned to the policy in question. Also, If a device then gets assigned to a different policy and later gets reassigned to its original policy, the usage count of the original policy will be incremented.

Viewing RADIUS Attribute Information

To view your currently configured RADIUS attribute groups, go to **Configuration > Policies** in the UI, and be sure to select the RADIUS Attribute Groups tab.

The following table shows you an example of what a RADIUS Attribute Groups table looks like after three different RADIUS attribute groups have been created.

FIGURE 26 RADIUS Attribute Groups Example

	Name	Description	Policy Count	Attributes	Timestamp
+ [pencil] [X]	VLAN 1		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	20210118 1509 MST
[pencil] [X]	VLAN 2		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	20210118 2024 MST
[pencil] [X]	VLAN 3 and Filter ID		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	20210118 2025 MST

You can use the RADIUS Attribute Groups table as follows:

TABLE 4 Description of RADIUS Attribute Groups Table

Column Title	Description
+	<ul style="list-style-type: none"> You can edit the RADIUS attribute group by clicking on the pencil icon. If the RADIUS attribute group has not yet been assigned to any policy, there will be a X next to the name. Clicking that X deletes the group. However, in the example screen shown above, all the groups have already been assigned to at least one policy; therefore the X is not selectable, which denotes that you cannot delete the group as long as it remains in use by one or more policies. You would have to edit the policy itself to remove the RADIUS attribute from the policy if you then want to delete the RADIUS attribute.
Name	The name of the RADIUS attribute group as configured in the Display Name field in the RADIUS Attribute Group configuration screen, an example of which is shown in Figure 2 on page 10.
Description	Any optional description that was entered in the configuration of the RADIUS attribute group.
Policy Count	The number of policies that the RADIUS attribute group is currently assigned to.

Additional Policy Information

Viewing RADIUS Attribute Information

TABLE 4 Description of RADIUS Attribute Groups Table (continued)

Column Title	Description
Attributes	<p>Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 2 on page 10.</p> <p>NOTE The "Reply Username" attribute applies only to certificate authentications.</p>
Timestamp	Time that the RADIUS attribute group was created.

Switching Pre-Release-5.8 Microsoft NPS Certificate Templates to Policy-Assigned Templates

Microsoft NPS onboard client certificate templates are created differently in Release 5.8 (and later) from prior releases. If you have older Microsoft NPS onboard client certificate templates in your system, you can continue to use them the same way in 5.8 or later, or you can convert them to the policy-type templates that are created in Release 5.8 going forward. Once you switch an old template to the new policy-type format, you cannot revert back to the pre-5.8 template configuration.

Follow the steps below to convert an old certificate template to the policy-based template:

1. In the UI, go to **Certificate Authority > Manage Templates**, then click the Wrench icon for the desired certificate template.
2. On the ensuing screen, click the **Edit RADIUS Attributes** button in the "RADIUS Attributes (Non-Policy)" portion of the screen. The following screen is then displayed.


FIGURE 27 Modify Microsoft NPS Certificate Template Configuration Screen: Pre-Release 5.8 Template

Certificate Authority >
Manage Templates >
Modify Certificate Template RADIUS Options
Cancel
Save

Certificate Template

Name: username@byod.company.com

RADIUS Options



When a device authenticates using a certificate from this template, Cloudpath will return RADIUS attributes based on the information below.

These attributes may be used to apply a dynamic VLAN, an ACL, or other connection policies.

Allow Authentication via RADIUS:

Switch to Policy based Attributes:

Reply Username: Certificate Common Name (Default) v

Allowed SSID(s): *

VLAN ID: [ex. 50 or BYOD]

Filter ID: [ex. BYOD]

Class: [ex. BYOD]

Reauthentication: [ex. 86400] Seconds

+ Add

NOTE

Be sure to take note of the existing values of the fields shown in the screen above because you will re-use these values when you create a new RADIUS attribute group.

3. Under RADIUS Options, check the "Switch to Policy-Based Attributes" box.
4. On the ensuing screen, select your settings in the "RADIUS Options" portion of the screen, then click **Save** to complete the process of converting the certificate template to the policy-based template.
5. Select the **RADIUS Policies** tab and add any desired policies. For instructions on adding policies, see [Adding RADIUS Policies to the NPS Certificate Template](#) on page 27.

Configuring the Network Policy Server

- Overview of Configuring the Network Policy Server..... 43
- Import the RADIUS Server Certificate for the NPS..... 43
- Import the Public Key of the Intermediate CA..... 46
- Set Up Roles and Services..... 47
- Network Policy Setup for EAP/TLS..... 48

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 **certmgr** 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.

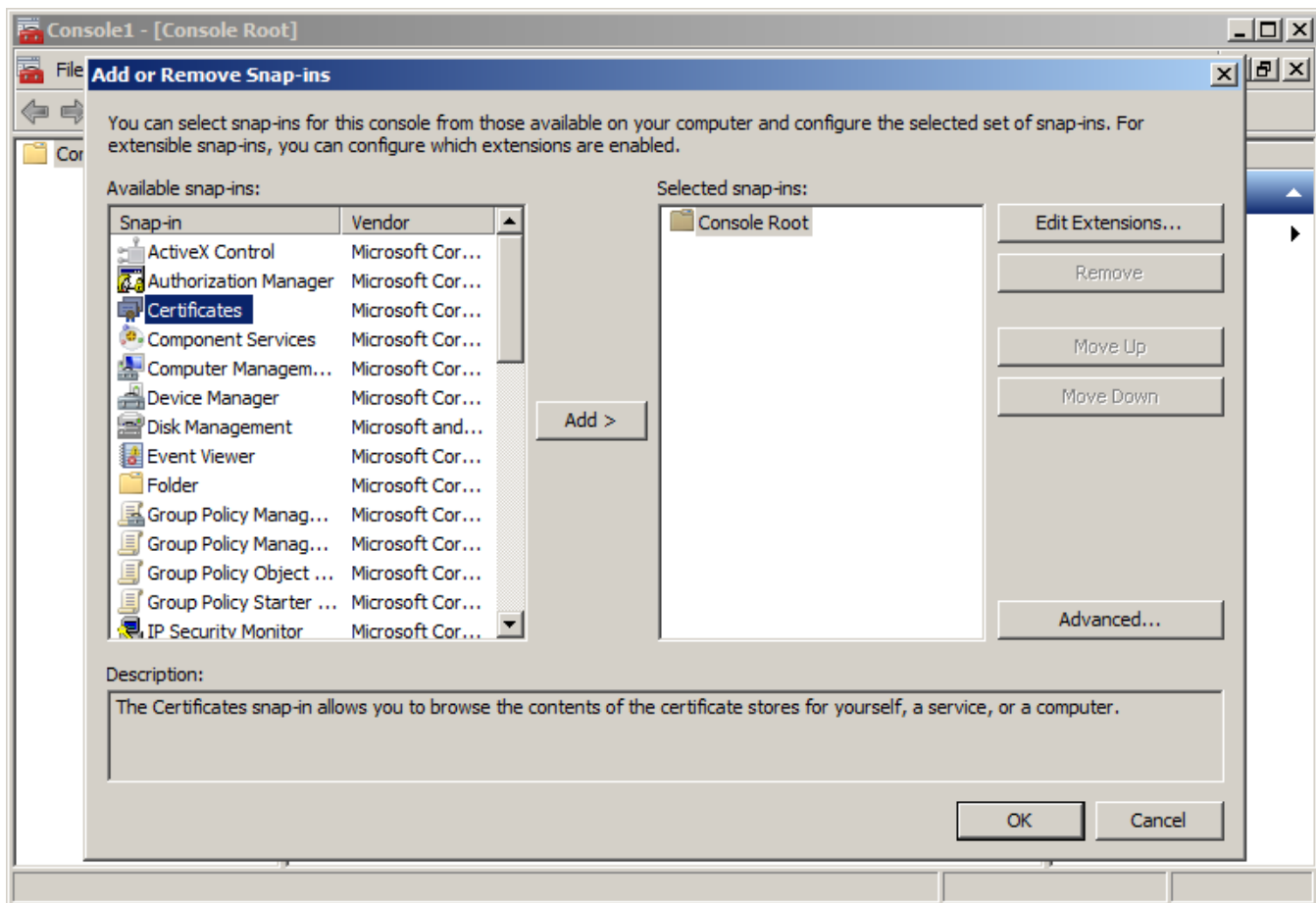
2. Go to **File > Add/Remove Snap-in**.

Configuring the Network Policy Server

Import the RADIUS Server Certificate for the NPS

3. On the **Add or Remove Snap-ins** page, select **Certificates** from the left pane (**Available Snap-ins:**) and click **Add**.

FIGURE 28 Add Snap-in



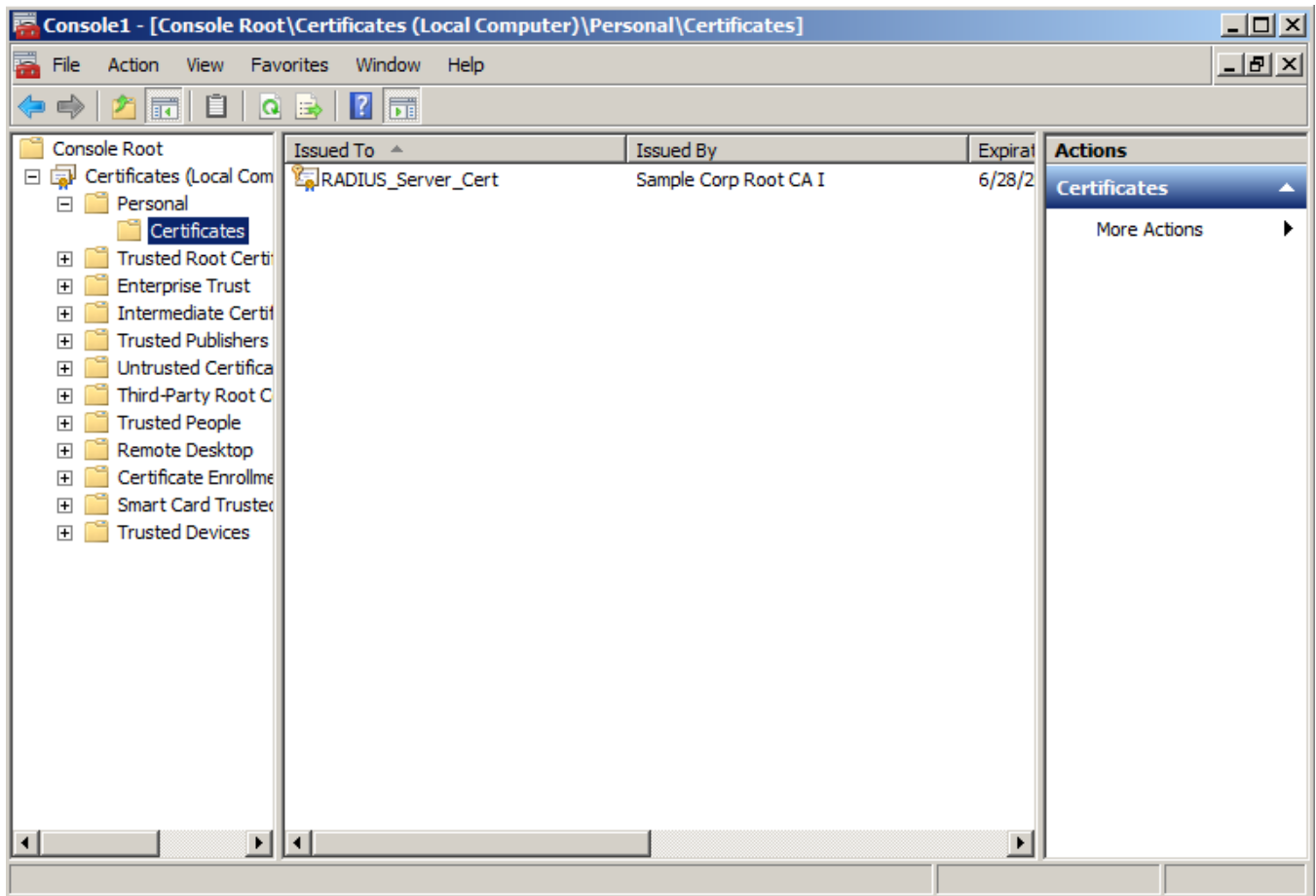
4. In the **Certificates** snap-in window, select **Computer Account** and click **Next**.
5. In the **Select Computer** window, select **Local Computer** and click **Finish**.
Certificates (Local Computer) should be listed in the right pane (**Selected Snap-ins:**) of the **Add or Remove Snap-ins** 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 29 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**.

Configuring the Network Policy Server

Import the Public Key of the Intermediate CA

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

TIP


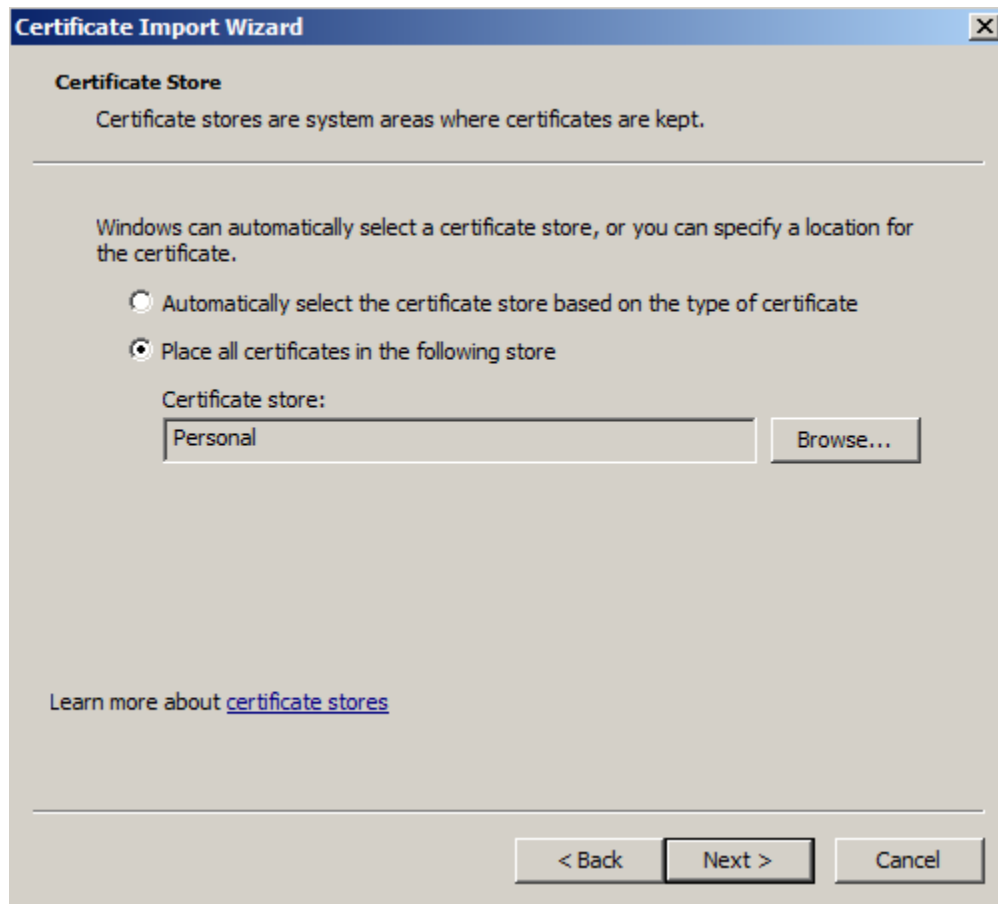
Be sure that the RADIUS server certificate show the key icon . If it does not show it, you do not have the private key for the RADIUS certificate. If you have issues, try downloading the RADIUS certificate and private key in P12 format. You can also try using the command line interface to install the private key for the RADIUS certificate. See [Missing EKU in the RADIUS Server Certificate](#) on page 68.

FIGURE 30 Certificate Import Wizard



- 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.

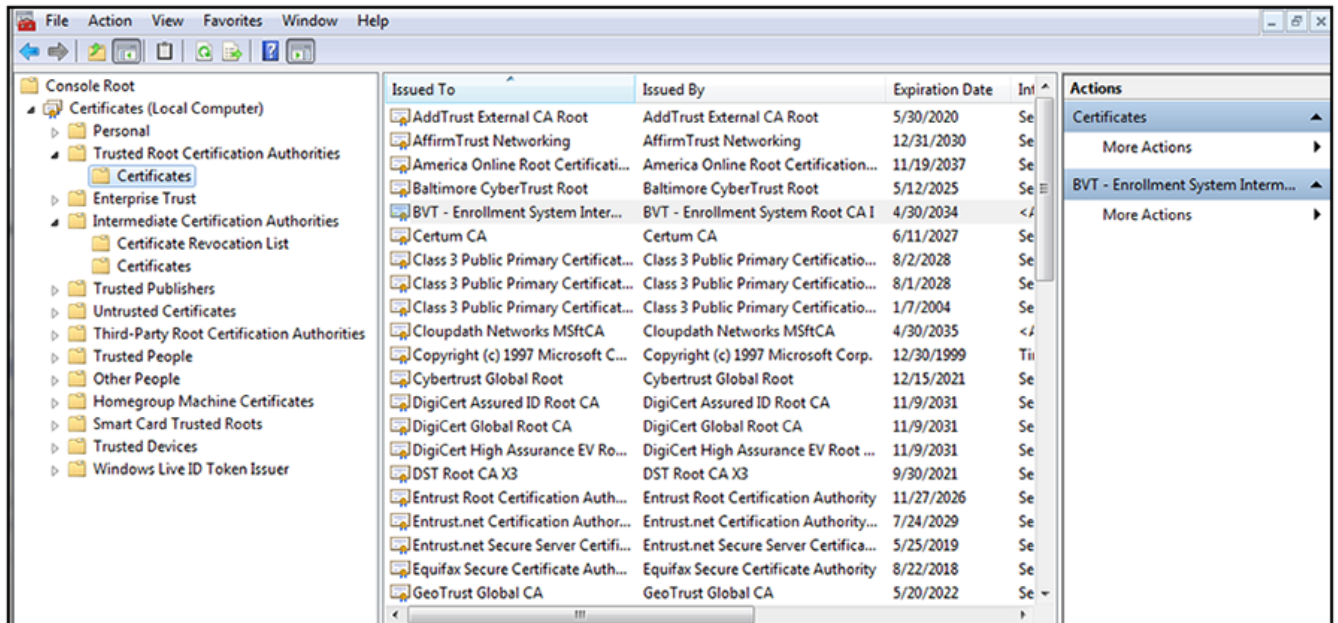
To import the public key of the intermediate CA to the Enterprise Trust Store, perform the following steps:

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 31 Root Certificate in the Enterprise Certificate Store



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

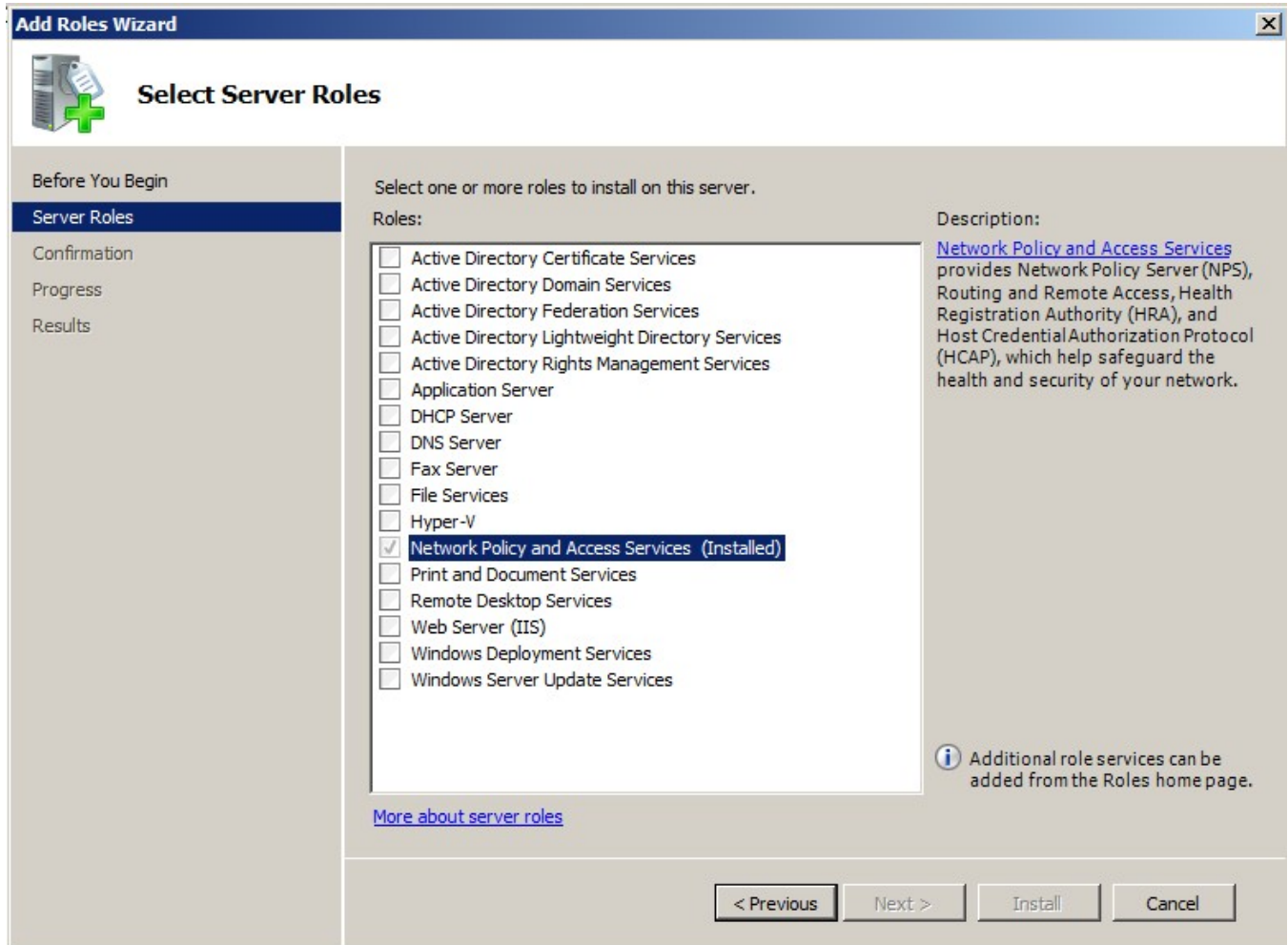
Set Up Roles and Services

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 32 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.

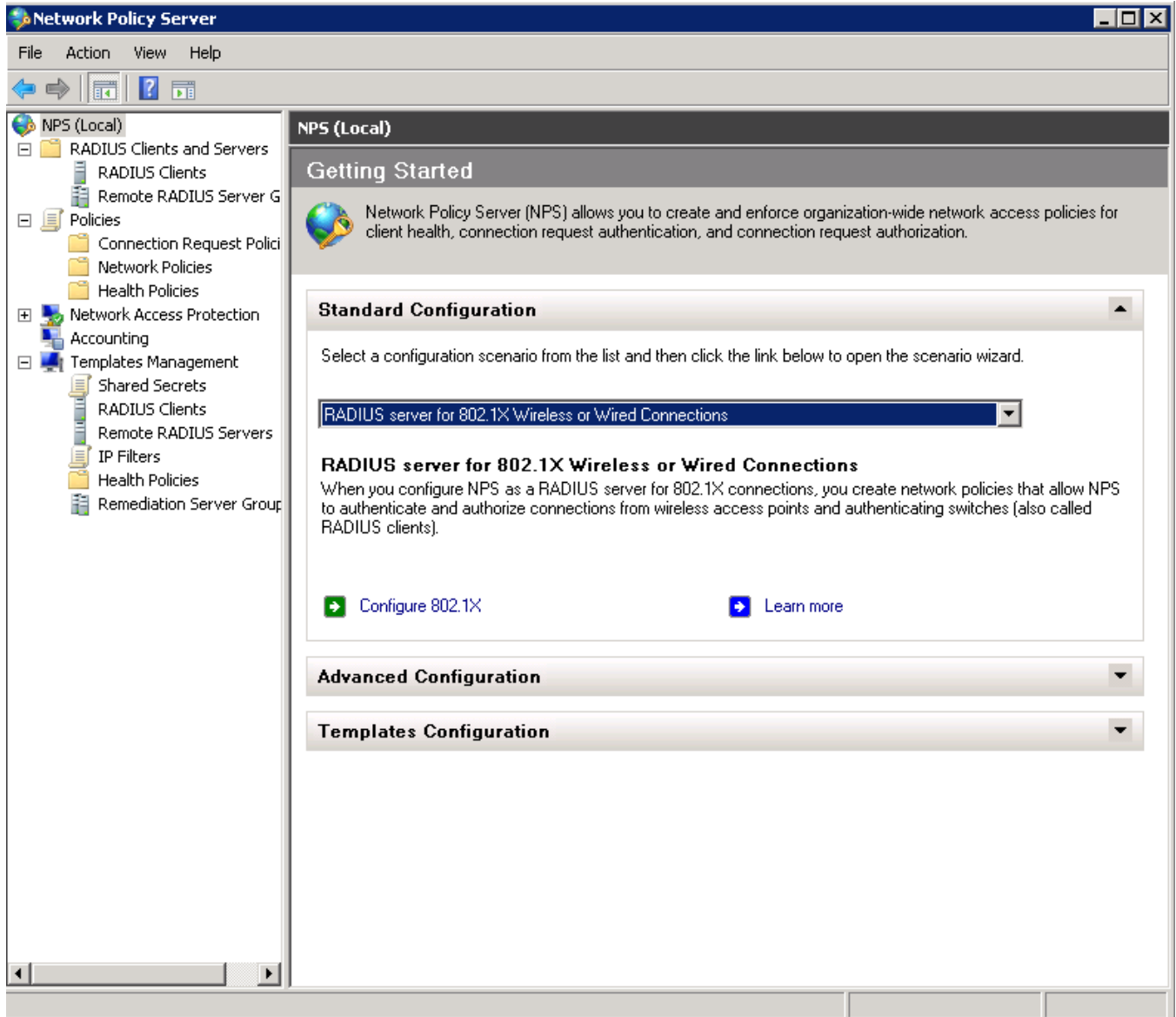
Network Policy Setup for EAP/TLS

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)**.

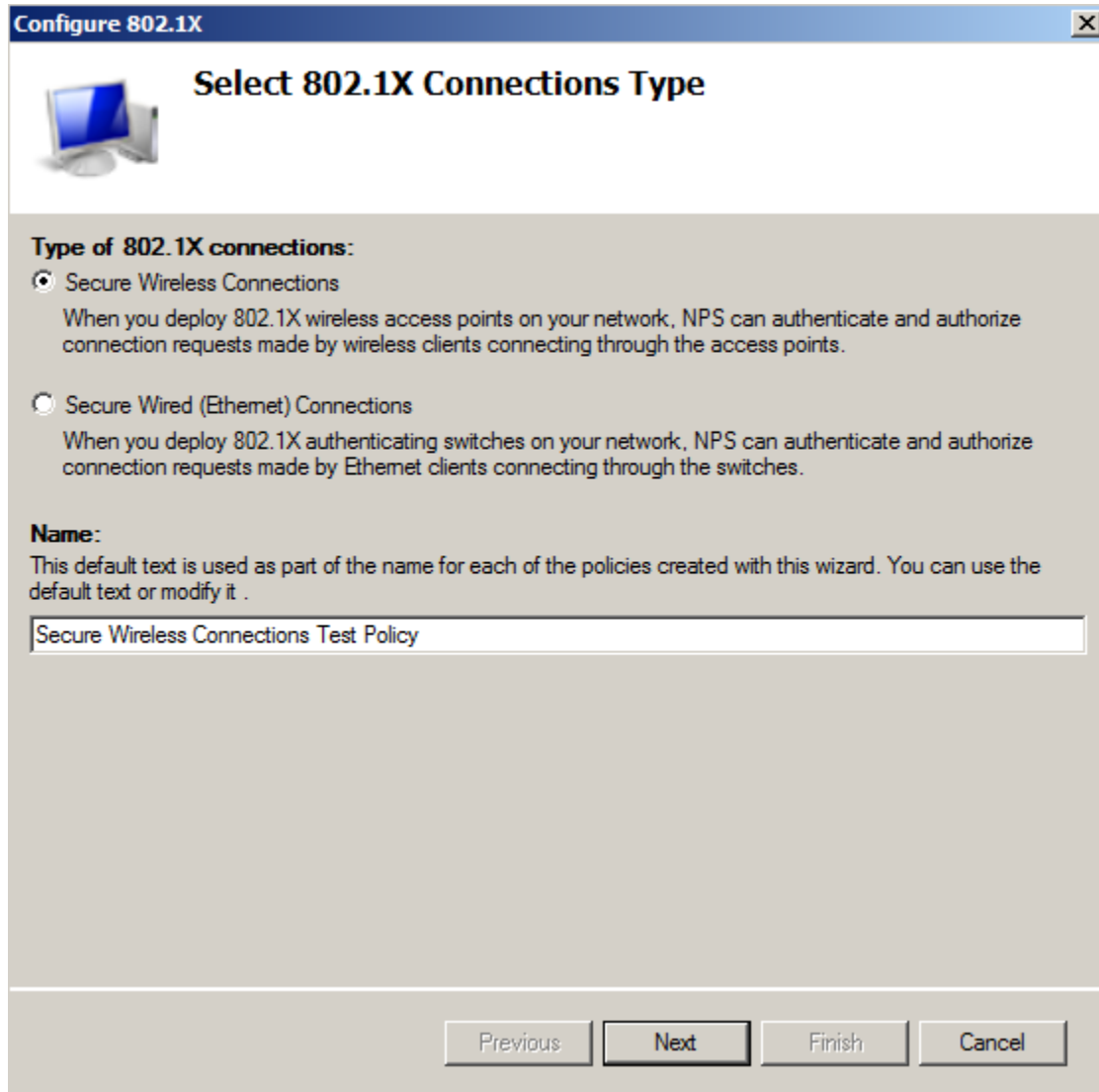
The **Standard Configuration** section should appear in the center pane.

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 33 Select 802.1X Connection Type



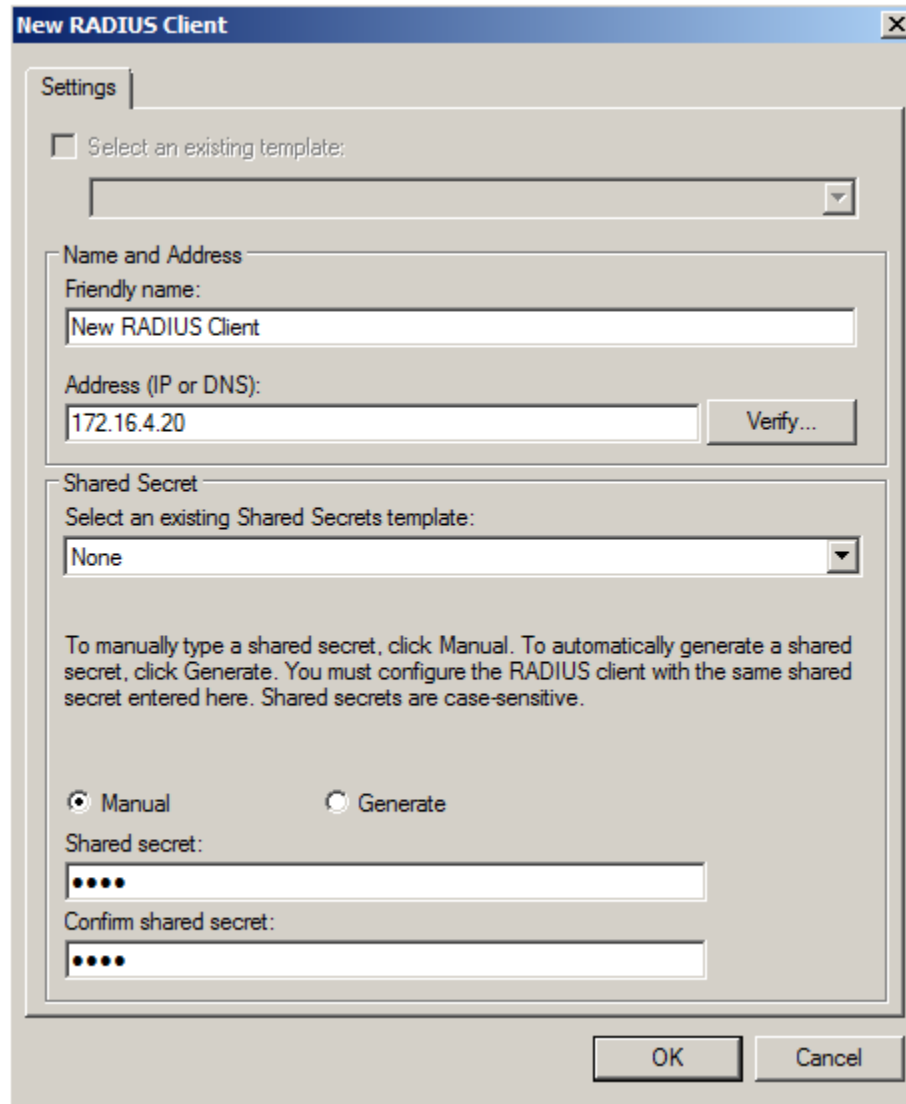
5. In the **Specify 802.1X Switches** window, click **Add** to configure a wireless access point (RADIUS client).

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.

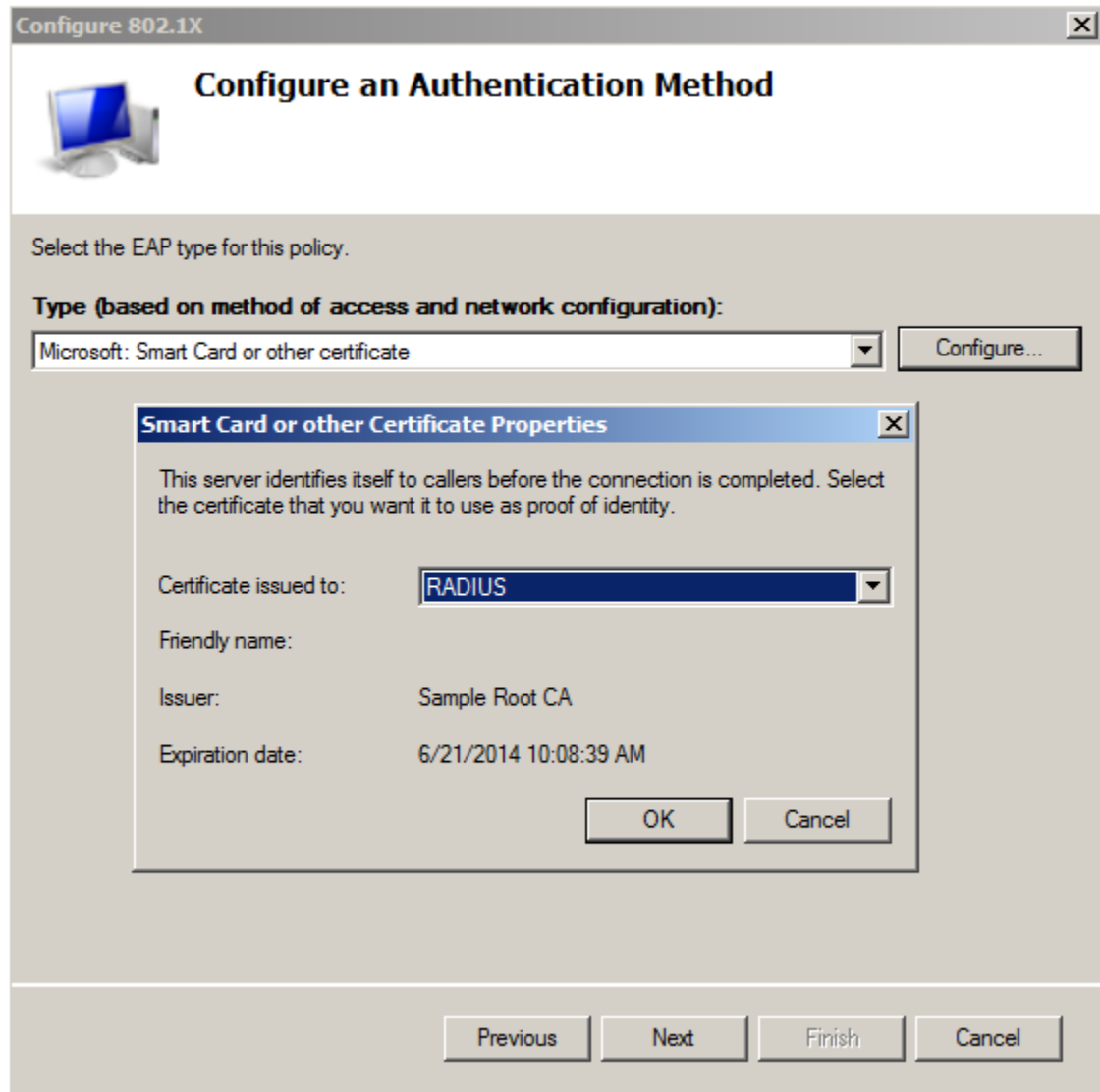
FIGURE 34 New RADIUS Client



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 43.) Click OK.

FIGURE 35 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.

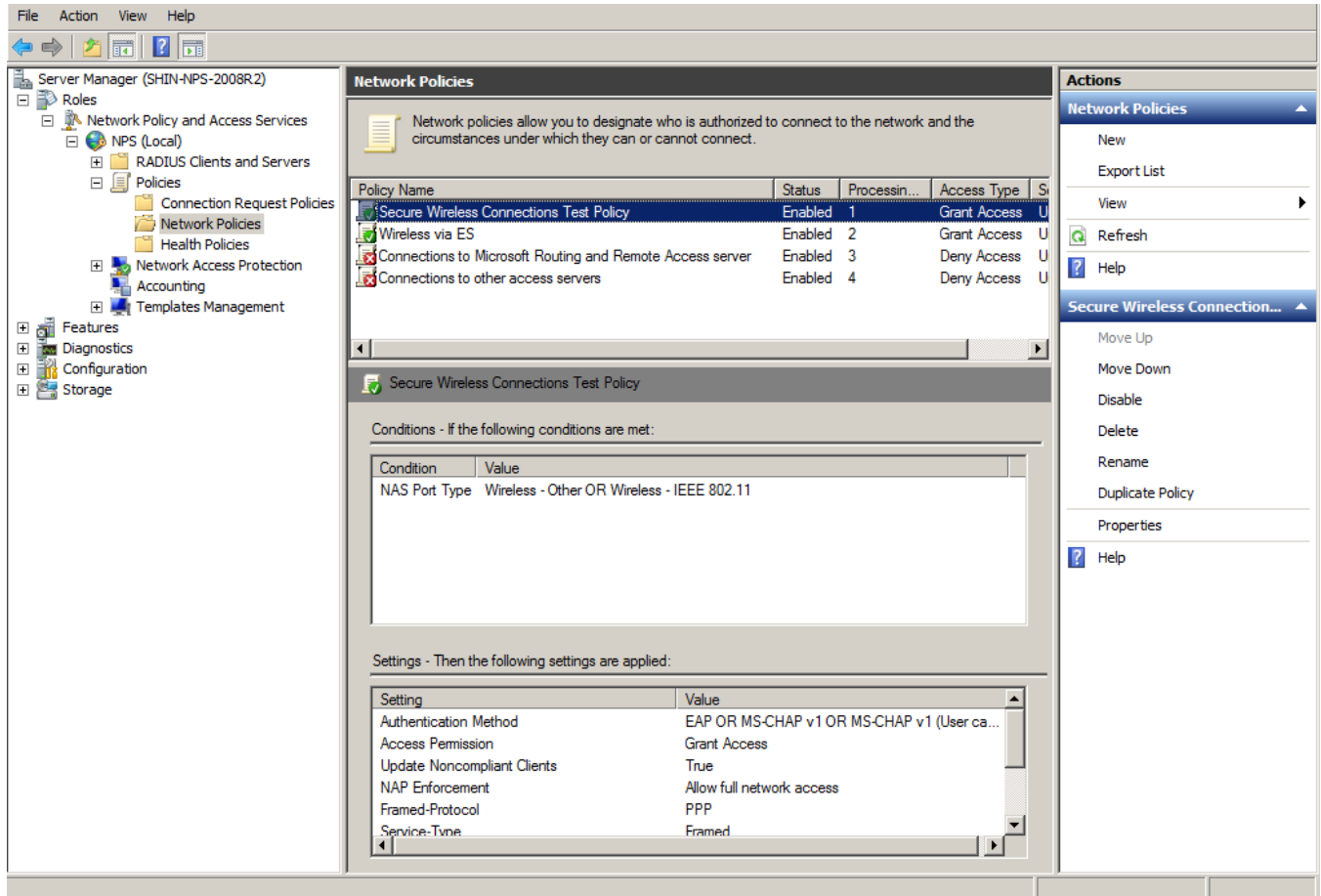
Prioritize the 802.1X Configuration

To prioritize the 802.1X 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.

- 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 36 Network Policies



Verify Network Policy

- [Review the Network Policy.....](#) 55
- [Verify Conditions of a Connection Request Policy.....](#) 55
- [Verify Authentication Method.....](#) 56
- [Verify Network Policy Settings.....](#) 57

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 Access 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:

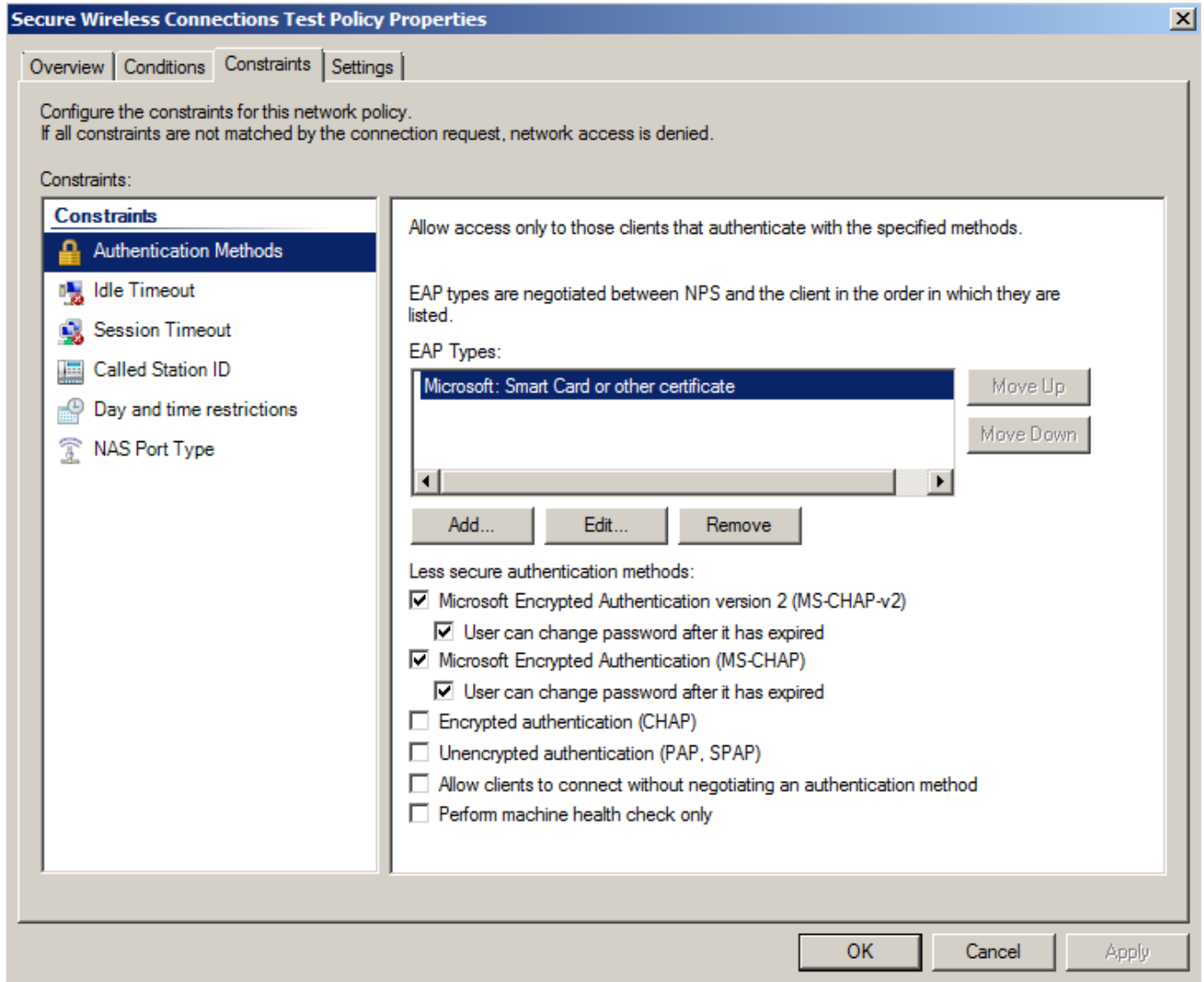
1. Go to the **Secure Wireless Connections Properties > Conditions** tab.
2. Verify that the **Conditions** match the Connection Request Policy.
See [Connection Request Policies](#) on page 59.

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 37 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 62 for more information.

Setting Up RADIUS Proxy on NPS

- Overview of Setting Up RADIUS Proxy on NPS..... 61
- Add a Remote RADIUS Server Group for RADIUS Proxy..... 61
- Configure a Connection Request Policy for RADIUS Proxy..... 62

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:

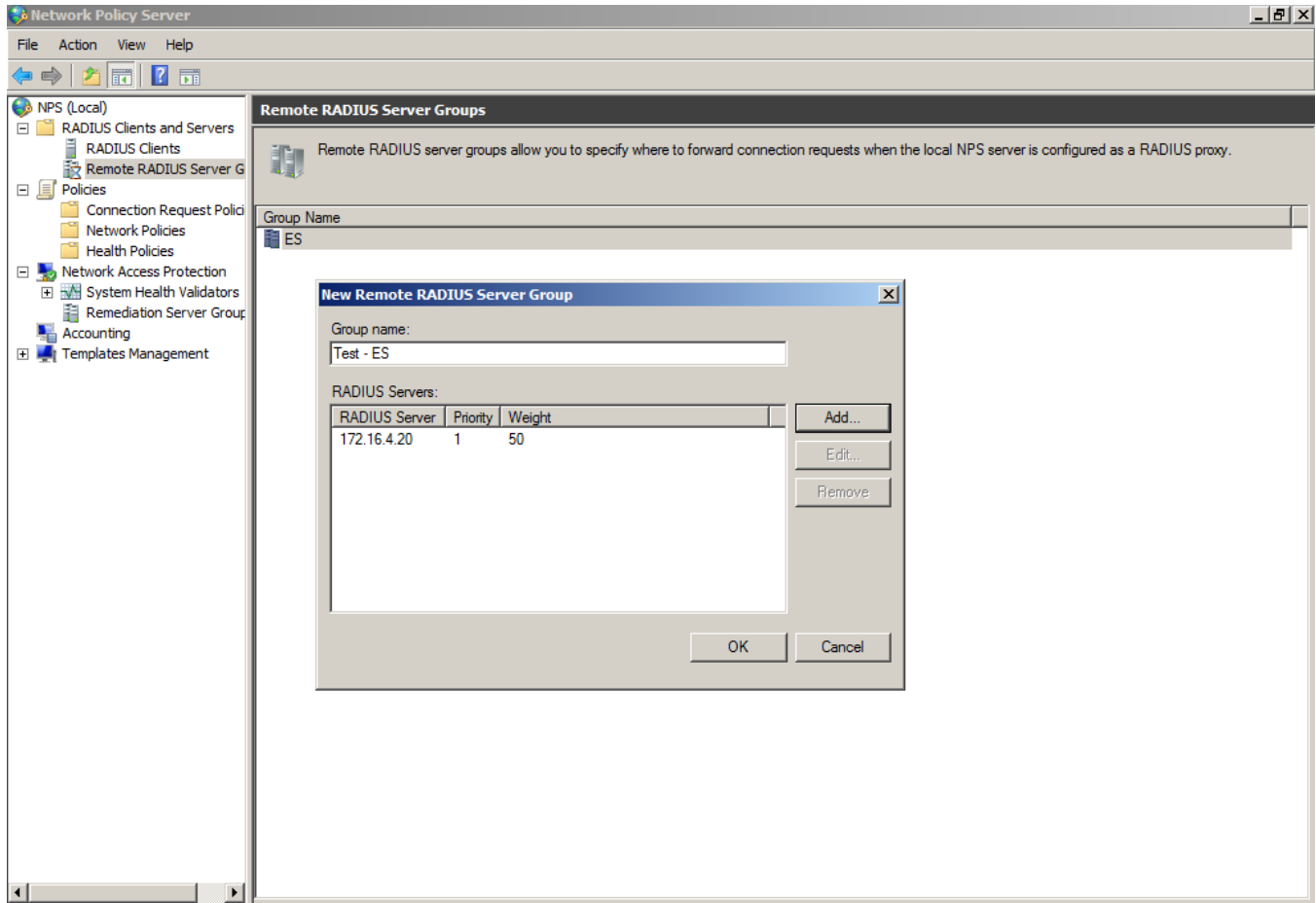
1. On the NPS (local), expand **RADIUS Clients and Servers**, and select **Remote RADIUS Server Groups**.
2. From the **Action** menu, select **New**.
(Alternately, you can right-click and select **New**.)

Setting Up RADIUS Proxy on NPS

Configure a Connection Request Policy for RADIUS Proxy

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

FIGURE 38 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.

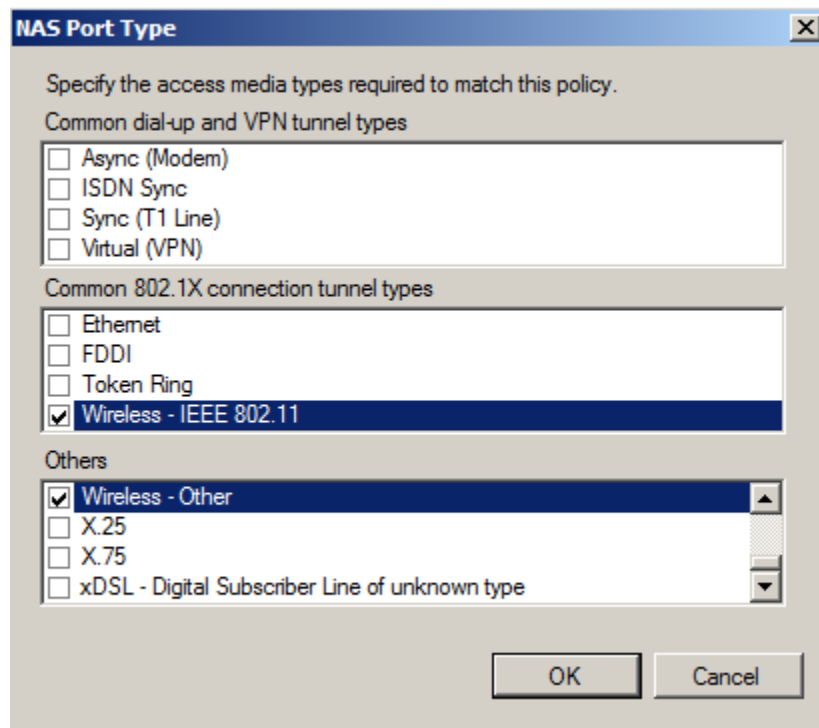
You can configure a connection policy request to look for <@guest> in the user name, and, if found, forward the request to the remote RADIUS server group. To configure a connection request policy for a RADIUS proxy, perform the following steps:

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 39 NAS Port Type



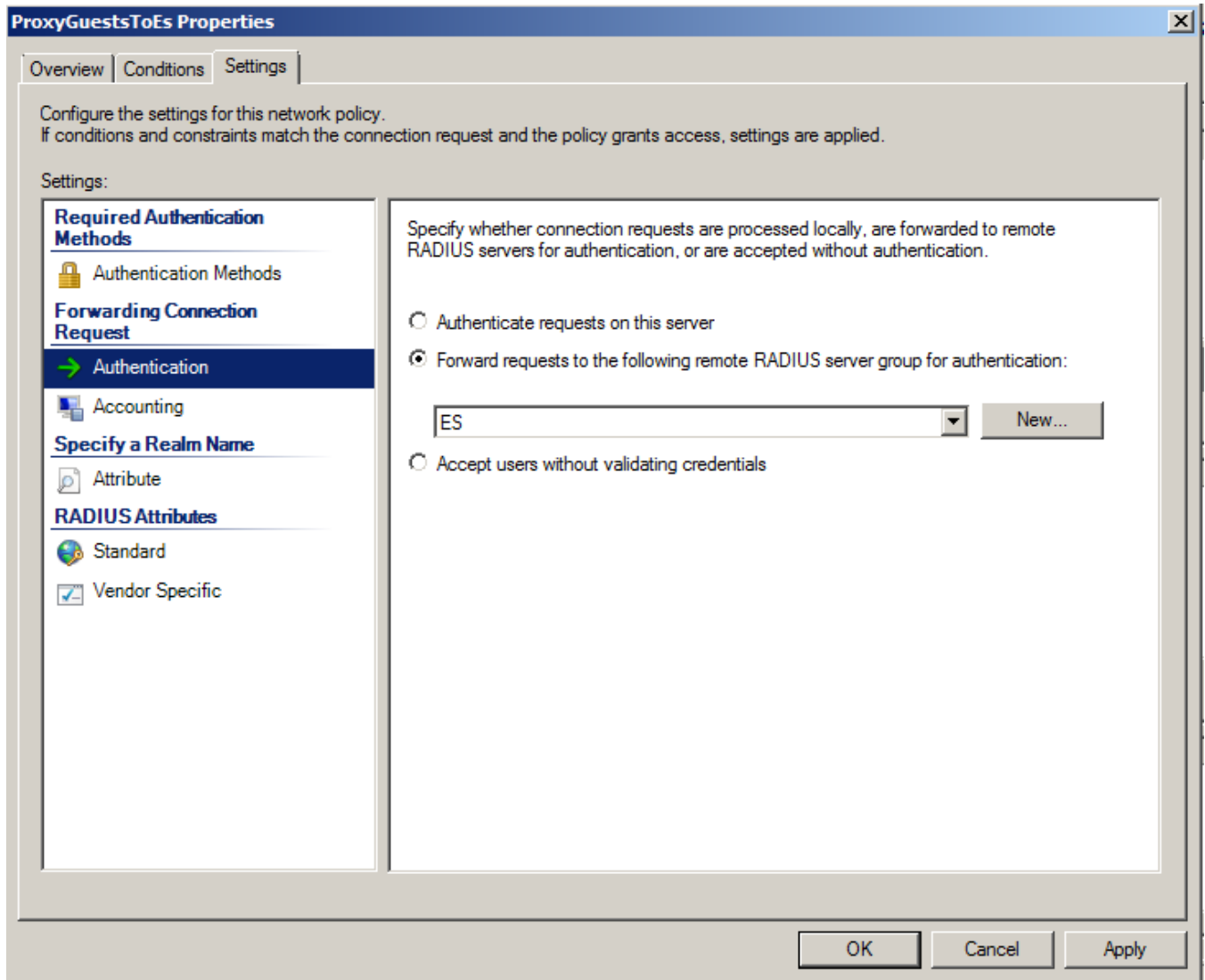
7. In the **Specify Conditions** window, click **Add**.
8. Select **User name** and click **Add**.
9. In the **User Name** window, enter **.*@guest**. Click **OK**.
10. In the **Specify Conditions** window, click **Next**.

Setting Up RADIUS Proxy on NPS

Configure a Connection Request Policy for RADIUS Proxy

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 40 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.

OSCP provides the ability to revoke certificates. However, if using OSCP affects the performance of your system, you could disable OSCP 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 OSCP response from the CA, it looks up the domain name of the CA's OSCP server in the DNS, as well as establishing a connection to the OSCP 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 15. 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 17 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 24 for instructions on downloading the certificate from Cloudpath, or use the following command examples from the NPS Administrator prompt:

```
certutil -dspublish -f root.cer NTAAuthCA  
certutil -enterprise -addstore NTAAuth 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 25 for more information.

