

# Cloudpath Enrollment System

# Integration with Microsoft<sup>™</sup> NPS Configuration Guide

Software Release 4.3 April 2016

**Summary:** This document describes how to configure a Microsoft Network Policy Server to act as the RADIUS server for use with the Cloudpath ES in a wireless network with EAP-TLS authentication. This guide provides instructions for configuring firewall rules, configuring the Cloudpath ES to act as a private CA and issue certificates to be imported by the NPS, how to configure RADIUS proxy, and troubleshooting information.

**Document Type:** Configuration **Audience:** Network Administrator



# Integration with Microsoft NPS Configuration Guide

Software Release 4.3 April 2016

Copyright © 2016 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex<sup>™</sup>, BeamFlex<sup>™</sup>, MediaFlex<sup>™</sup>, ChannelFly<sup>™</sup>, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2016 Ruckus Wireless, Inc. All rights reserved.

# Integration with Microsoft<sup>™</sup> NPS Configuration Guide

# **Overview**

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.

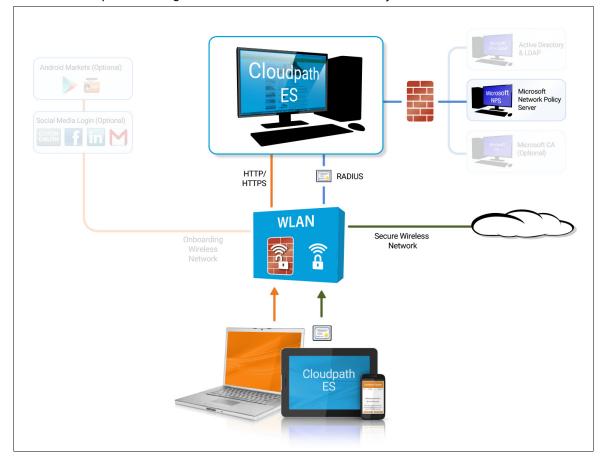


FIGURE 1. Cloudpath ES Integrated with Microsoft Network Policy Server

You can configure an NPS as a RADIUS server that integrates with the Cloudpath Enrollment System (ES). The Cloudpath ES can be used as a private CA for certificate deployments using either PEAP-TLS or EAP-TLS authentication. The ES 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 ES in a 802.11 wireless network with EAP-TLS authentication.

# Prerequisites

Before you can configure an NPS to work with the Cloudpath ES, you must have the following devices/ 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 27 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 NPS for 802.1X wireless connections-standard configuration.

### Note >>

We recommend that you install Microsoft NPS services on a separate server from your Microsoft Active Directory services.

# **Configuring Firewall Rules For Use With the Cloudpath ES**

This section describes how to configure firewall rules for use with the Cloudpath ES. Additional firewall information can be found on the *Administration > Advanced > Firewall Requirements* page.

The network firewall must be configured to allow the Cloudpath ES and the Network Policy Server to communicate.

Depending on where the Cloudpath ES is placed in your network, certain TCP ports are required to allow the ES to communicate with NPS and Active Directory (AD) services.

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

### Note >>

See the Tips and Troubleshooting section for additional information about firewall settings.

2

# **Configuring the Cloudpath ES**

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

This section describes how to configure the Cloudpath ES 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**

This section describes how to create a standalone CA in the Cloudpath ES.

### How to Set Up a Standalone Certificate Authority

- 1. In the ES, on the left menu, select Certificate Authority > Manage CA.
- 2. Create new CA.
- 3. Select Generate New Certificate Authority.
- 4. On the Create Certificate Authority page, enter the following information:
  - Common Name This is the publicly-visible name of the root CA. We recommend 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 This host name is embedded into the CA as part of the URL for the OCSP.
  - Validity Period Leave the default, or specify the Start and Expires dates.
  - CA Strength Configure the strength of the CA by specifying the Key Length and Algorithm.
  - CA Properties These properties are embedded into the CA. Enter the appropriate information as required by your network policy.

3

FIGURE 2. Cr	eate Certificate Authority
--------------	----------------------------

Create Certificate Authority		< Back Save
Reference Information		
	blicly-visible name. We recommend including "Root C , "Sample Corp Wireless Root CA I", or "Sample Corp	
Common Name:	Test Root CA I	*
Description:		
e Description.		
Enabled:	×.	
OCSP Information		
	n to the CA as part of the URL for Online Certificate S	
URL will be similar to: http://[SERVER_DN	revocation status of the certificate. This field cannot    S]/admin/ocsp/checkCert	be changed once the CA is created. The full
OCSP Hostname:	Test.company.net	
Validity Period		
	or 20 years. We have defaulted the start date back on	e month to avoid potential system clock
issues.	,	
• Start Date:	20131210 *	
Expires Date:	20340110 *	
Expires Date.	20340110	
CA Strength		
The following properties determine the stre	ength of the certificate authority.	
🖲 Key Length:		
	2048	
Algorithm:	SHA-256 💌	
CA Properties		
The following properties are embedded into	the CA. Many organizations have guidelines specifyi	ing 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. Save the CA.

# **Client Certificate Template Settings For NPS**

In the Cloudpath ES, 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.

### How to Set Up a Client Certificate Template Using an Onboard CA

- 1. In the ES, on the 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
-----------	--------	--------	-------------	----------

	type of certificates should be iss	sued?	Cancel Next >
۲	Client Certificates		
	Used on clients to authenticate the be applied appropriately.	e client. The decoration of the username within the certificate a	Ilows RADIUS policies to
	It 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	
		o username@other.company.com	
	🗄 Grant Access Until:	1         Years         ▼ after issuance.	
	• Configure Advanced Options:		
	Lifecycle Notifications		
	The Manual Constant Fourthment Conta		
	interact with the end-user, the admi is created, but the notifications belo	em supports events related to the lifecycle of the certificate. These even inistrator, as well as external systems. Additional notifications can be of ware some of the most common ones.	
	interact with the end-user, the admi is created, but the notifications belo	inistrator, as well as external systems. Additional notifications can be o	
	interact with the end-user, the admi is created, but the notifications belo	inistrator, as well as external systems. Additional notifications can be o w are some of the most common ones. Send welcome email on issuance. Send email 7 days before certificate expiration.	
	interact with the end-user, the admi is created, but the notifications belo	inistrator, as well as external systems. Additional notifications can be of w are some of the most common ones. Send welcome email on issuance. Send email 7 days before certificate expiration. Send email if certificate is revoked.	· · · · · · · · · · · · · · · · · · ·
	interact with the end-user, the admi is created, but the notifications belo	inistrator, as well as external systems. Additional notifications can be o w are some of the most common ones. Send welcome email on issuance. Send email 7 days before certificate expiration.	
	interact with the end-user, the admi is created, but the notifications belo	inistrator, as well as external systems. Additional notifications can be of w are some of the most common ones. Send welcome email on issuance. Send email 7 days before certificate expiration. Send email if certificate is revoked.	
	interact with the end-user, the admi is created, but the notifications belo <b>Notifications:</b> <b>RADIUS Options</b> By default, this certificate template	inistrator, as well as external systems. Additional notifications can be of w are some of the most common ones. Send welcome email on issuance. Send email 7 days before certificate expiration. Send email if certificate is revoked.	configured once the template
	interact with the end-user, the admi is created, but the notifications belo <b>Notifications:</b> <b>RADIUS Options</b> By default, this certificate template	<ul> <li>inistrator, as well as external systems. Additional notifications can be of w are some of the most common ones.</li> <li>Send welcome email on issuance.</li> <li>Send email 7 days before certificate expiration.</li> <li>Send email if certificate is revoked.</li> <li>Email administrator if revoked certificate is used.</li> <li>will be honored for RADIUS authentications. The RADIUS attributes be</li> </ul>	configured once the template
	interact with the end-user, the admi is created, but the notifications belo <b>Notifications:</b> <b>RADIUS Options</b> By default, this certificate template used attributes. If additional attribut	<ul> <li>inistrator, as well as external systems. Additional notifications can be of ware some of the most common ones.</li> <li>Send welcome email on issuance.</li> <li>Send email 7 days before certificate expiration.</li> <li>Send email if certificate is revoked.</li> <li>Email administrator if revoked certificate is used.</li> </ul> will be honored for RADIUS authentications. The RADIUS attributes be tes are required, they may be added by editing the certificate template	configured once the 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 a 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 RADIUS Options to assign a VLAN ID or Filter ID to certificates that use this template. These settings only applies if you are using the ES onboard RADIUS server.

### **Client Certificate Template Advanced Options**

This section describes the fields on the on the *Modify Certificate Template* page, which displays if you checked *Configure Advanced Options* while creating a **Client** certificate template.

- Reference Information Enter the *Certificate Template Name* and *Notes* This information is for reference only. Enable the template.
- Identity Enter the *Common Name Pattern* used to determine the common name for certificates generated suing this 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* to for certificates using this template.
- Advanced Settings Enter the *Patterns* to for certificates using this template.

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

Modify Certificate Template				Cancel Save
Reference Information				
Certificate Template Name:	username@byod.company.	com		*
Certificate Authority:				
• Notes:				1
			/	
Enabled?				
Identity				
The following property is normally used to pro- issuance with the appropriate value from the	vide identity information withir enrollment.	the certificate.	Variables, such as \${USERNAME	}, will be replaced at the time of
Common Name Pattern:	\${USERNAME}@byod.com	pany.com		
Validity Period				
The following properties determine the lifespar end-user system clocks.	n of the issued certificates. We	recommend sett	ing the start date to 1 month bef	ore issuance to avoid issues with
• Start Date:	1 Months	<ul> <li>before issues</li> </ul>	uance.	
Expiration Date:	1 Years T	 after issuan	ce.	
	Revoke if unseen for 3			<b></b>
Policy - RADIUS Attributes	C Revoke il diseen for [3	j juays.		•
Allow Authentication via RADIUS :     Login	By Certificate	_	When a device authenticates usin this template, Cloudpath will retu- based on the information below, may be used to apply a dynamic other connection policies.	um RADIUS attributes These attributes
	Policies			
ex. VL	AN: 50			
Reply Username:	Certificate Common Name	(Default) 🔹		
Allowed SSID(s):	*			
• VLAN ID:	[ex. 50 or BYOD]	]		
• Filter ID:	[ex. BYOD]	]		
• Class:	[ex. BYOD]	]		
Reauthentication:	[ex. 86400]	Seconds		
	+	-		
Certificate Strength				
Organization Information				
Advanced Settings				
▶ Cleanup				

### FIGURE 4. Modify Client Certificate Template

• Use the options in the *Cleanup* section to delete client certificate templates and associated data.

# **Create 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.

This section describes how to set up a server certificate template in the Cloudpath ES.

### How to Set Up a Server Certificate Template Using an Onboard CA

- 1. In the ES, on the left menu, select Certificate Authority > Manage Templates.
- 2. Click Add Template to create a new certificate template.
- 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

This section describes the fields on the on the *Modify Certificate Template* page, which displays if you checked *Configure Advanced Options* while creating a **Server** certificate template.

- Reference Information Enter the *Certificate Template Name* and *Notes* This information is for reference only. Enable the template.
- Identity Enter the *Common Name Pattern* used to determine the common name for certificates generated suing this 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 to for certificates using this template.
- Advanced Settings Enter the Patterns and EKUs for certificates using this template.

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 >>

Server certificate templates must use the *Microsoft Server EKU - 1.3.6.1.5.5.7.3.1*. This establishes the *Extended Key Usage* properties for the certificate.

FIGURE 5.	Modify	/ Server	Certificate	Template
-----------	--------	----------	-------------	----------

Modify Certificate Template		Cancel Save
Reference Information		
Reference Information		
🗉 Certificate Template Name:	Server Template	*
🗉 Certificate Authority:	Anna Test Intermediate CA I	
Notes:		
Enabled?	8	
Identity The following property is normally used to pro- time of issuance with the appropriate value fro	ride identity information within the certificate. Variables, such as \${U: m the enrollment.	SERNAME}, will be replaced at the
🗄 Common Name Pattern:	\${SERVER_NAME}	
Validity Period		
	of the issued certificates. We recommend setting the start date to 1	month before issuance to avoid
🗄 Start Date:	Specific Date    20150617	
Expiration Date:	1 Years ▼ after issuance.	
· OCSP Monitoring:	Revoke if unseen for 30 days.	
Certificate Strength The following properties determine the strengt	n of the certificates.	
🗄 Key Length:	2048	
🗉 Algorithm:	SHA-256 ¥	
• Organization Information		
Advanced Settings		
▶ Cleanup		

# **Generate the Server Certificate for the NPS**

This section describes how to generate a server certificate from the server certificate template and the Cloudpath ES onboard CA you created in the previous steps.

### How to Generate the Server Certificate

- 1. In the ES, go to Certificate Authority > Generate Certificate.
- 2. Select the NPS server certificate template you just created.
- 3. Use the default SERVER\_NAME.

4. Select *Auto-Generate CSR* from the *CSR* source and *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 ES for generating the RADIUS server certificate. You use the same server certificate template, but instead of allowing ES to auto generate the certificate, you select the *Copy & Paste CSR* option from the *CSR source*.

### How to Download the RADIUS Server Certificate

- 1. Navigate to the Configuration > Advanced > RADIUS Server page.
- 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.

This section describes how to download the public key of the Intermediate CA to use with NPS.

#### Note >>

By default, the Intermediate CA (ES 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.

#### How to Download the Public Key

- 1. In the ES, go To Certificate Authority > Manage CA. Expand the onboard CA you created in a previous step.
- 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.

CA: Anna T	est Intermediate CA I		J
Parent CA:	Anna Test Intermediate CA I <u>Anna Test Root CA I</u> BBF7A9C5312550FE1D700398571B58651F77C	964	
Organizational Unit: Email Address: Locality: State: Country:	it@company.com Westminster Colorado	Key Length: Algorithm: Serial Number: OCSP Hash:	20350616 2048 SHA-256 000000000000000000000000000000000000
Public Key: Cham: Private Key: P12 Format:	View Download PEM Download PKCS7 View Download	View Details	Primary Workflow
Sub CAs:	No sub-CAs exist. Add Sub CA		
Templates:	Name          Ø         BVOD Policy Template          Ø         Guest Policy Template          Ø         Server Template          Ø         server Template          Ø         username@byod.company.com          Ø         username@test.company.com	Notes	Common Name Pattern \${USERNAME}@byod.company.com \${USERNAME}@guest.company.com \${USERNAME} \${USERNAME} \${USERNAME}@byod.company.com \${USERNAME}@test.company.com }

#### FIGURE 6. Download Public Key of Intermediate CA

# **Configuring the Network Policy Server**

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

#### Prerequisite >>

The NPS must be configured within your domain.

# Import the RADIUS Server Certificate for the NPS

This section describes how to import the server certificate to the NPS Certificate Store.

#### How to Add a Certificates Snap-In

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.
- 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

		Remove
		Mana La
—		Move Up
		Move Down
<b>.</b>		Advanced
	Add >	Add >

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

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

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

🚟 Console1 - [Console Root	\Certificates (Local Computer)\I	Personal\Certificates]		<u>_0×</u>
🚠 File Action View Fav	orites Window Help			_ B ×
🧢 🔿 🖄 📅 🗎 🙆	🔒 🛛 🖬			
Console Root	Issued To 🔺	Issued By	Expirat	Actions
Certificates (Local Com Personal	RADIUS_Server_Cert	Sample Corp Root CA I	6/28/2	Certificates 🔺
Certificates				More Actions
🕀 📔 Trusted Root Certi				
Intermediate Certif     Trusted Publishers				
Indiced Fidencial				
🕀 🧮 Third-Party Root C				
🕀 🚞 Trusted People				
🕀 🚞 Remote Desktop				
🕀 🧮 Certificate Enrollme				
🕀 🧮 Smart Card Truster				
It is the second sec				
• •	•		•	

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 the Cloudpath ES 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 shows the key icon 2. If it doesn't, 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 "RADIUS Server Certificate Missing Private Key" on page 29.

#### FIGURE 9. Certificate Import Wizard

ertificate Import Wizard	×
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location fo the certificate.	r
$\odot$ Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Personal Browse	1
	-
Learn more about <u>certificate stores</u>	
< Back Next > Car	ncel
	icei

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

# Import the Public Key of the Intermediate CA

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

This section describes how to import the public key of the Intermediate CA to the NPS Certificate Store.

#### Note >>

By default, the Intermediate CA (ES 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.

#### How to Import the Public Key of the Intermediate CA to the Enterprise Trust Store

- 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 ES 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 Authorties* store and click *Next*.

#### Note >>

We have found that there are fewer issues when you import into the Trusted Root CA store. However, if you import the public key of the ES onboard Intermediate CA into the Intermediate CA store, this should also work.

FIGURE 10.	Root	Certificate	in the	Enterprise	Certificate Store
------------	------	-------------	--------	------------	-------------------

🚰 File Action View Favorites Window Hel	p				_ 8 ×
🗢 🔿 🖄 🖬 📋 🔍 📑 🚺					
Console Root	Issued To	Issued By	Expiration Date	Int ^	Actions
Certificates (Local Computer)	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Se	Certificates 🔺
Personal Trusted Root Certification Authorities	AffirmTrust Networking	AffirmTrust Networking	12/31/2030	Se	More Actions
Certificates	America Online Root Certificati	America Online Root Certification	11/19/2037	Se	
Enterprise Trust	🔄 Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Se ≡	BVT - Enrollment System Interm 🔺
Intermediate Certification Authorities	BVT - Enrollment System Inter	BVT - Enrollment System Root CA I	4/30/2034	<4	More Actions
Certificate Revocation List	🔄 Certum CA	Certum CA	6/11/2027	Se	
Certificates	🔄 Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/2/2028	Se	
Trusted Publishers	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/1/2028	Se	
Untrusted Certificates	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	1/7/2004	Se	
Third-Party Root Certification Authorities	Cloupdath Networks MSftCA	Cloupdath Networks MSftCA	4/30/2035	<4	
Trusted People	🔄 Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Tii	
Other People	🔄 Cybertrust Global Root	Cybertrust Global Root	12/15/2021	Se	
Homegroup Machine Certificates	🔄 DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Se	
Smart Card Trusted Roots	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Se	
Trusted Devices	🔄 DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root	11/9/2031	Se	
Windows Live ID Token Issuer	🔄 DST Root CA X3	DST Root CA X3	9/30/2021	Se	
	Entrust Root Certification Auth	Entrust Root Certification Authority	11/27/2026	Se	
	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029	Se	
	Entrust.net Secure Server Certifi	Entrust.net Secure Server Certifica	5/25/2019	Se	
	🔄 Equifax Secure Certificate Auth	Equifax Secure Certificate Authority	8/22/2018	Se	
	🔄 GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Se 🔻	
	٠ III			•	

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

# **Set up Roles and Services**

This section describes how to install Network Policy and Access Services (NPAS) as a Server Role.

### How to Add NPAS as a Server Role

- 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

Add Roles Wizard		×
Select Server Ro	les	
Before You Begin Server Roles Confirmation Progress Results	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services DHCP Server DHCP Server DHCP Server Flas Server Flas Services Hyper-V Network Policy and Access Services (Installed) Print and Document Services Remote Desktop Services Web Server (IIS) Windows Deployment Services Windows Server Update Services	Description: Network Policy and Access Services provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.
	More about server roles	Additional role services can be added from the Roles home page.
	< Previous Next	> Install Cancel

- 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.

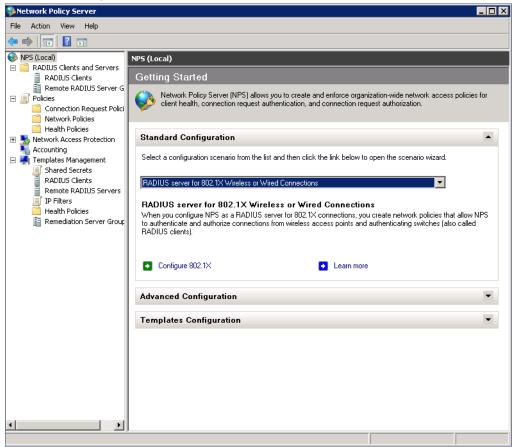
# **Network Policy Setup for EAP/TLS**

This section describes how to configure the 802.1X connection policy.

### How to Set Up 802.1X Connections

- 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.

### FIGURE 12. 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 13. Select 802.1X Connection Type

Configure 802.1X	X
Select 802.1X Connections Type	
<ul> <li>Type of 802.1X connections:</li> <li>Secure Wireless Connections         When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize         connection requests made by wireless clients connecting through the access points.</li> <li>Secure Wired (Ethemet) Connections         When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize         connection requests made by Ethemet clients connecting through the switches.</li> <li>Name:         This default text is used as part of the name for each of the policies created with this wizard. You can use the         default text or modify it .         Secure Wireless Connections Test Policy</li> </ul>	
Previous Next Finish Cancel	l

- 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 14. New RADIUS Client

Select an existing te	molator	
j pelect an existing te	mplate:	
Name and Address		
Friendly name:		
New RADIUS Client		
Address (IP or DNS):		
172.16.4.20		Verify
172.10.4.20		veniy
Shared Secret		
	ed Secrets template:	
Select an existing Shar None		ia-lly accords a share
Select an existing Shar None To manually type a sha secret, click Generate.	ed Secrets template: red secret, click Manual. To automat You must configure the RADIUS clie hared secrets are case-sensitive.	
Select an existing Shar None To manually type a sha secret, click Generate, secret entered here. Si Manual	red secret, click Manual. To automat You must configure the RADIUS clie nared secrets are case-sensitive.	
Select an existing Shar None To manually type a sha secret, click Generate, secret entered here. Si Manual Shared secret:	red secret, click Manual. To automat You must configure the RADIUS clie nared secrets are case-sensitive.	
Select an existing Shar None To manually type a sha secret, click Generate, secret entered here. Si Manual Shared secret:	red secret, click Manual. To automat You must configure the RADIUS clie nared secrets are case-sensitive.	

- 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 you imported to the Computer Enterprise Trust store. See "Import the RADIUS Server Certificate for the NPS" on page 11. Click *OK*.

19

FIGURE 15. Co	onfigure	Authentication	Method
---------------	----------	----------------	--------

Configure	802.1X	x
	Configure a	n Authentication Method
Select the	EAP type for this policy.	
Type (ba	ased on method of acce	ss and network configuration):
	: Smart Card or other certifica	
	Smart Card or other C	
		If to callers before the connection is completed. Select ant it to use as proof of identity.
	Certificate issued to:	RADIUS
	Friendly name:	
	Issuer:	Sample Root CA
	Expiration date:	6/21/2014 10:08:39 AM
		OK Cancel
		Previous Next Finish Cancel

- **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

- 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.

File Action View Help		
🗢 🔿 🔀 🗊  🖬		
Server Manager (SHIN-NPS-2008R2)	Network Policies	Actions
Roles     Network Policy and Access Services	— * Network policies allow you to designate who is authorized to connect to the network and the	Network Policies 🔺
Source and Access Schrees	Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.	New
RADIUS Clients and Servers		Export List
Connection Request Policies	Policy Name Status Processin Access Type S	View
Network Policies	Secure Wireless Connections Test Policy Enabled 1 Grant Access U Wireless via ES Enabled 2 Grant Access U	Q Refresh
📔 Health Policies 🗉 駴 Network Access Protection	Connections to Microsoft Routing and Remote Access server Enabled 3 Deny Access U	
Accounting	Connections to other access servers Enabled 4 Deny Access U	? Help
🛨 🌉 Templates Management		Secure Wireless Connection 🔺
Features     Diagnostics		Move Up
Configuration		Move Down
🕀 📇 Storage	Secure Wireless Connections Test Policy	Disable
	Conditions - If the following conditions are met:	Delete
		Rename
	Condition Value NAS Port Type Wireless - Other OR Wireless - IEEE 802.11	Duplicate Policy
		· · · ·
		Properties
		? Help
	Settings - Then the following settings are applied:	
	Setting Value  Authentication Method EAP OR MS-CHAP v1 OR MS-CHAP v1 (User ca	
	Access Permission Grant Access	
	Update Noncompliant Clients True	
	NAP Enforcement Allow full network access Framed-Protocol PPP	
	Service-Type Framed	
	)	J
	· · · · · · · · · · · · · · · · · · ·	J

#### FIGURE 16. Network Policies

# **Verify Network Policy**

This section describes how to review your network policy and verify that it is configured correctly to work with the Cloudpath ES.

### How to Review the Network Policy

- 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 you created in previous steps.
- 3. Click Properties.

### How to Verify Conditions

If using a Connection Request Policy, go to the Secure Wireless Connections Properties > Conditions tab to verify that your Conditions match the Connection Request Policy. See "Connection Request Policies" on page 23.

### How to Verify Authentication Method

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

FIGURE 17. Secure Wireless Connection Properties

- 2. Verify that the Microsoft Smart Card or other certificate EAP Type is listed.
- 3. If it is not listed, click Add. On the Add EAP Type window, select Microsoft Smart Card or other certificate and click OK. Select the Microsoft Smart Card or other certificate EAP Type and 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.

### How to Verify Network Policy Settings

If using a Connection Request Policy, go to the Secure Wireless Connections Properties > Settings tab to 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 How to Configure a Connection Request Policy for RADIUS Proxy for more information.

# Setting up RADIUS Proxy on NPS

This section describes how to configure Network Policy Server as a RADIUS proxy that forwards connection requests to other RADIUS servers for authentication and authorization.

To configure NPS as a RADIUS proxy, you must:

- 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.

# **Remote RADIUS Server Groups**

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

### How to Add a Remote RADIUS Server Group for RADIUS Proxy

- 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.

👶 Network Policy Server		- 8 ×
File Action View Help		
🗢 🔿 🖄 📅 🛛 🖬		
● № (Local)                 ■ ■ RADIUS Clients and Servers                 ■ RADIUS Clients                 ■ RADIUS Clients                 ■ RADIUS Clients                 ■ RADIUS Clients	Remote RADIUS Server Groups Remote RADIUS server groups allow you to specify where to forward connection requests when the local NPS server is configured as a RADIUS proxy.	
Policies     Connection Request Polici		
Network Policies	Group Name	
Network Access Protection		
System Health Validators     Area and the system Health Validators	New Remote RADIUS Server Group	
<ul> <li>Accounting</li> <li>Image: Image: Image:</li></ul>	Group name: Test - ES	
	RADIUS Servers:	
	RADIUS Server         Priority         Weight         Add           172.16.4.20         1         50         4	
	Edit	
	Remove	
	OK Cancel	
	3	

### FIGURE 18. 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.

# **Connection Request Policy**

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

### How to Configure a Connection Request Policy for RADIUS Proxy

This section describes how to 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.

- 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 Wireless IEEE 802.11 in the 802.1X connection tunnel types section, and for Wireless Other in the Others section. Click OK.

#### FIGURE 19. NAS Port Type

NAS Port Type	×
Specify the access media types required to match this policy. Common dial-up and VPN tunnel types	
Async (Modem) ISDN Sync Sync (T1 Line) Virtual (VPN)	
Common 802.1X connection tunnel types	
<ul> <li>□ Ethemet</li> <li>□ FDDI</li> <li>□ Token Ring</li> <li>✓ Wireless - IEEE 802.11</li> </ul>	
Others	
Wireless - Other       ▲         ∴ X.25       ∴         ∴ X.75       ∴         ∴ xDSL - Digital Subscriber Line of unknown type       ▼	
OK Cancel	

- 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, in the left pane, select Authentication. In the right pane, select Forward requests to the following remote RADIUS server group for authentication and select the ES remote RADIUS server group created in a previous step. Click Next.

ProxyGuestsToEs Properties		X
Overview Conditions Settings		
Settings:	ection request and the policy grants access, settings are applied.	_
Required Authentication Methods Authentication Methods Forwarding Connection	Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.	
Request       Authentication       Accounting       Specify a Realm Name       Attribute       RADIUS Attributes       Standard       Vendor Specific	Authenticate requests on this server     Forward requests to the following remote RADIUS server group for authentication:     ES     New     Accept users without validating credentials	
	OK Cancel Apply	

### FIGURE 20. Specify Connection Request - Authentication

- 12. In the *Configure Settings* window, in the left pane, select Attribute under *Specify a Realm Name*. In the right pane, select *User Name* from the *Attribute* list. 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 the Cloudpath ES for authentication, while *user* is authenticated directly by the NPS.

# **Tips and Troubleshooting**

This section describes issues to consider when testing or troubleshooting the configuration for the Cloudpath ES 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 EAP-TLS/PEAP protocol. Once successful, enable the 'validate server certificate' setting in the Cloudpath ES. 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. Changing the port to 3268, but keeping the same Base DN allows LDAP access to users from the child AD domain (Reference http://technet.microsoft.com/en-us/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 might 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 the Cloudpath ES. See "Create the Certificate Authority" on page 3. 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 ES 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 the Cloudpath ES, you must check the box for the Microsoft Server EKU. See "Client Certificate Template Settings For NPS" on page 4 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 "How to Download the RADIUS Server Certificate" on page 10 for instructions on downloading the certificate from the ES, 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 10 for more information.

# **Additional Documentation**

You can find detailed information in the Cloudpath ES configuration guides, located on the left-menu *Support* tab of the ES Admin UI.

# About Cloudpath

Cloudpath Networks, Inc. provides software solutions and services that simplify the adoption of standards-based security, including WPA2-Enterprise and 802.1X, in diverse BYOD environments. Our goal is to make secure as simple as insecure; simple for network administrators to deploy and simple for users to access.

To learn more about the Cloudpath ES and how it can simplify your wireless environment, visit <u>www.cloudpath.net</u> or contact a Cloudpath representative.

# **Contact Information**

General Inquiries:info@cloudpath.net Support:support@cloudpath.net Sales:sales@cloudpath.net Media:media@cloudpath.net Marketing:marketing@cloudpath.net Phone:+1 303.647.1495 (US) +1 866.472.6053 (US) +44 (01) 161.261.1400 (UK) Fax:+1 760.462.4569 Address:1120 W 122nd Ave, Suite 302 Westminster, CO 80234 USA