

Radius server for 802.1x wireless  
or wired connections



File Action View Help



NPS (Local)

- 4 RADIUS Clients and Servers
  - RADIUS Clients
  - Remote RADIUS Server Groups
- 4 Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
- Accounting
- 4 Templates Management
  - Shared Secrets
  - RADIUS Clients
  - Remote RADIUS Servers
  - IP Filters
  - Health Policies
  - Remediation Server Groups

NPS (Local)

## Getting Started



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.


### Standard Configuration


Select a configuration scenario from the list and then click the link below to open the scenario wizard.

RADIUS server for 802.1X Wireless or Wired Connections

#### RADIUS server for 802.1X Wireless or Wired Connections

When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

 [Configure 802.1X](#)

 [Learn more](#)

### Advanced Configuration

### Templates Configuration





## Select 802.1X Connections Type

### Type of 802.1X connections:

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.

Secure Wired (Ethernet) Connections

When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

### 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.

Previous

Next

Finish

Cancel



## Specify 802.1X Switches

Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)

RADIUS clients are network access servers, such as authenticating switches. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

### RADIUS clients:

Radius client No1  
myradiusclient  
Template1

Add...

Edit...

Remove

Previous

Next

Finish

Cancel



## Configure an Authentication Method

Select the EAP type for this policy.

**Type (based on method of access and network configuration):**

Microsoft: Smart Card or other certificate



Microsoft: Smart Card or other certificate

Microsoft: Protected EAP (PEAP)

Microsoft: Secured password (EAP-MSCHAP v2)

Configure...



## Configure an Authentication Method

Select the EAP type for this policy.

**Type (based on method of access and network configuration):**

Microsoft: Smart Card or other certificate



Configure...



### Smart Card or other Certificate Properties



This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued to:

Friendly name:

Issuer:

Expiration date:

9/27/2015 9:20:13 AM

OK

Cancel

Type (based on method of access and network configuration):

Microsoft Protected EAP (PEAP) ▼

Configure... ←

### Edit Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued to:

Friendly name:

Issuer:

Expiration date: 9/27/2015 9:20:13 AM

Enable Fast Reconnect

Disconnect Clients without Cryptobinding

#### Eap Types

Secured password (EAP-MSCHAP v2)

Move Up

Move Down

Previous

Add

Edit

Remove

OK

Cancel



## Configure an Authentication Method

Select the EAP type for this policy.

**Type (based on method of access and network configuration):**

Microsoft: Secured password (EAP-MSCHAP v2) ▼

Configure...

### EAP MSCHAPv2 Properties



Number of authentication retries:

2

Allow client to change password after it has expired

OK

Cancel





## Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Groups

Add...

Remove

Previous

Next

Finish

Cancel



## Configure Traffic Controls


Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.

If you do not use traffic controls or you want to configure them later, click Next.

### Traffic control configuration

To configure traffic control attributes, click Configure.



## Configure RADIUS Attributes



RADIUS Standard Attributes

Vendor-Specific Attributes

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

### Attributes:

Name	Value
Filter-Id	<not configured>
Tunnel-Type	<not configured>
Tunnel-Medium-Type	<not configured>
Tunnel-Pvt-Group-ID	<not configured>
Tunnel-Assignment-ID	<not configured>

### Description:

Specifies the tunneling protocols used.

Edit..

OK

Cancel



## Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

**Connection Request Policy:**

Secure Wired (Ethernet) Connections

**Network Policies:**

Secure Wired (Ethernet) Connections

[Configuration Details](#)

Previous

Next

Finish

Cancel