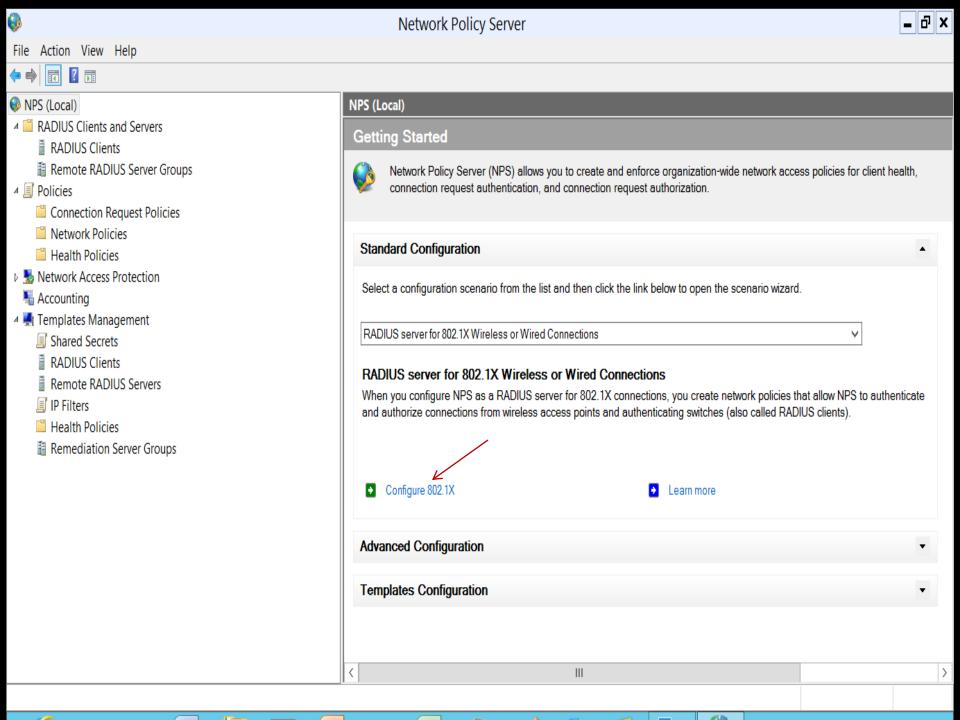
# Radius server for 802.1x wireless or wired connections







## **Select 802.1X Connections Type**

T۱	/ne	of	802	1X	connections:
		•	002.	-	COHINECTIONS.

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.

Secure Wired (Ethernet) Connections

Previous Next

Finish

### Configure 802.1X





# 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			Add		
Template1			Edit		
			Remove		
	Descious No.	. Finish	Canad		

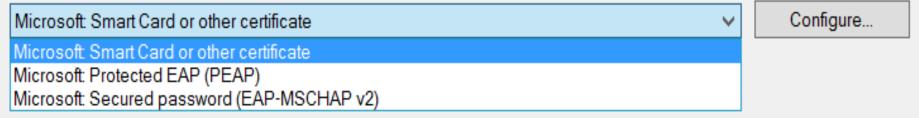




# **Configure an Authentication Method**

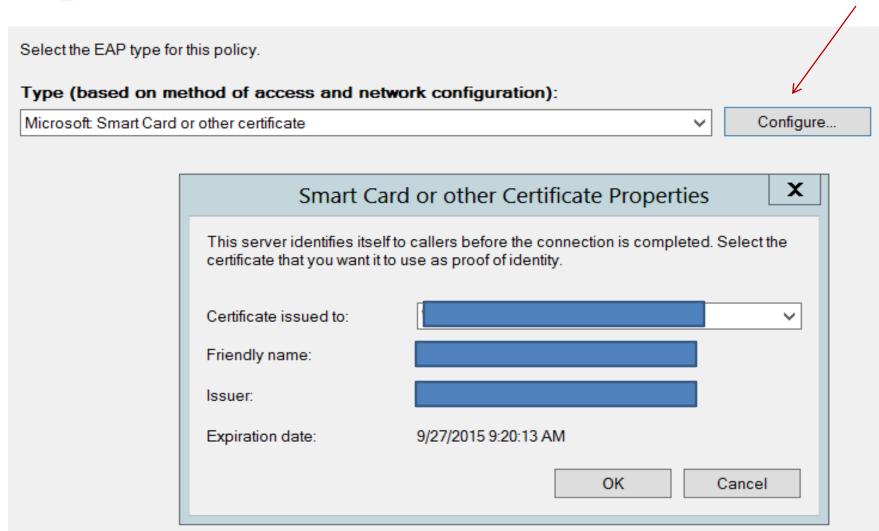
Select the EAP type for this policy.

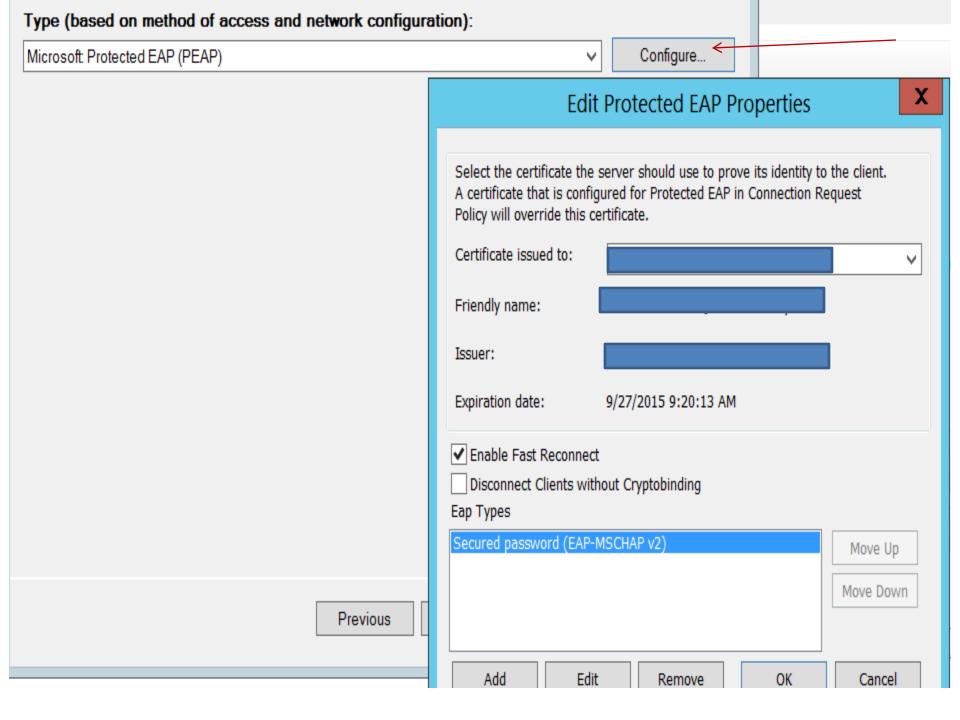
## Type (based on method of access and network configuration):





# **Configure an Authentication Method**









# **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)

EAP MSCHAPv2 Properties					
Number of authentication retries: 2					
✓ Allow client to change password after it has expired					
OK Cancel					

#### Configure 802.1X





### **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





## **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.



Previous Next Finish Cancel

#### 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=""></not>	
Tunnel-Type	<not configured=""></not>	
Tunnel-Medium-Type	<not configured=""></not>	
Tunnel-Pvt-Group-ID	<not configured=""></not>	
Tunnel-Assignment-ID	<not configured=""></not>	

#### Description:

Specifies the tunneling protocols used.

Edit...

OK





#### 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