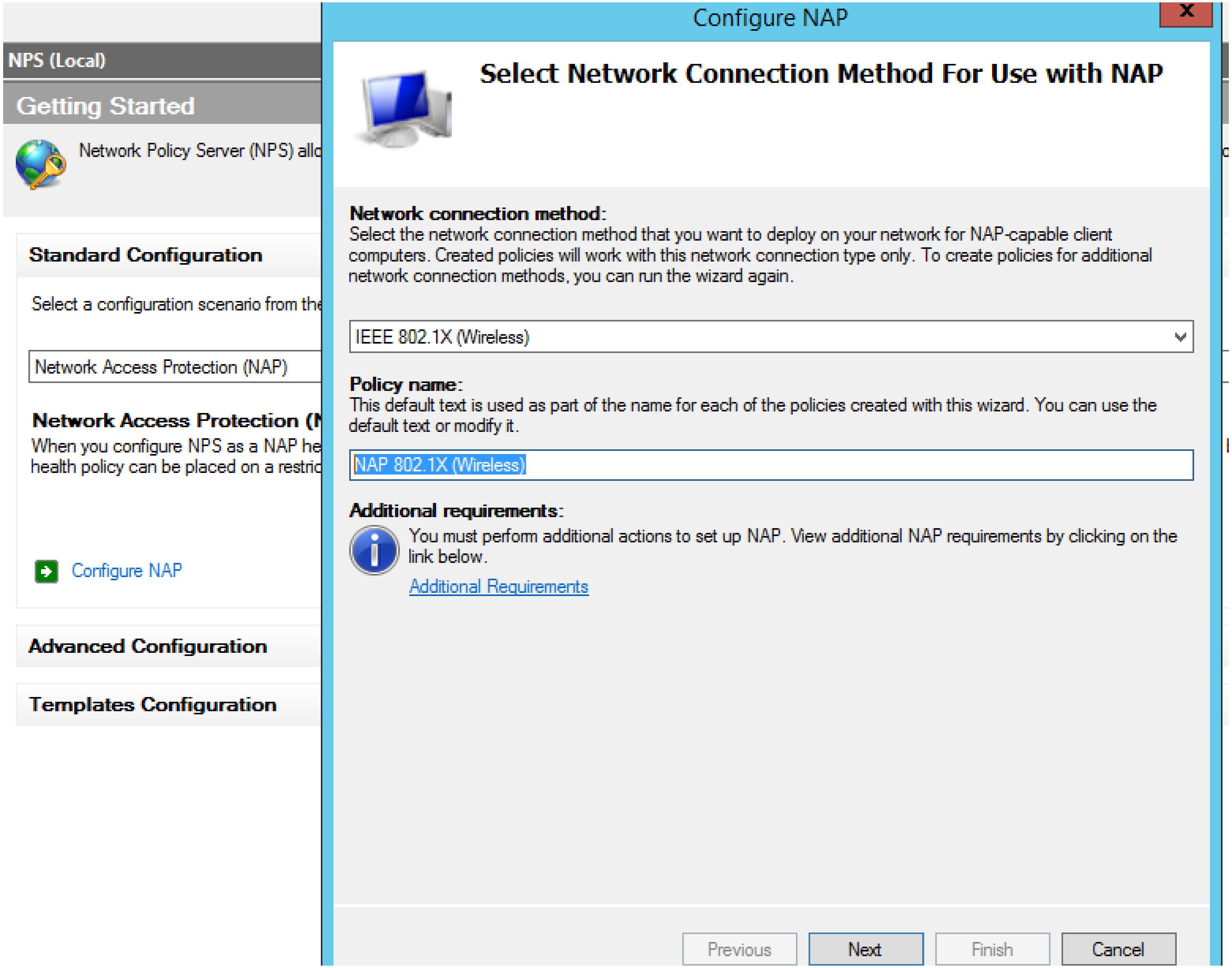
NAP 802.1X (Wireless)

SERVER 2012R2


NPS (Local)
Getting Started
Network Policy Server (NPS) allo
Standard Configuration
Select a configuration scenario from the
Network Access Protection (NAP)
Network Access Protection (N
When you configure NPS as a NAP he
health policy can be placed on a restric
Configure NAP
Advanced Configuration
Templates Configuration
Configure NAP
X

Select Network Connection Method For Use with NAP

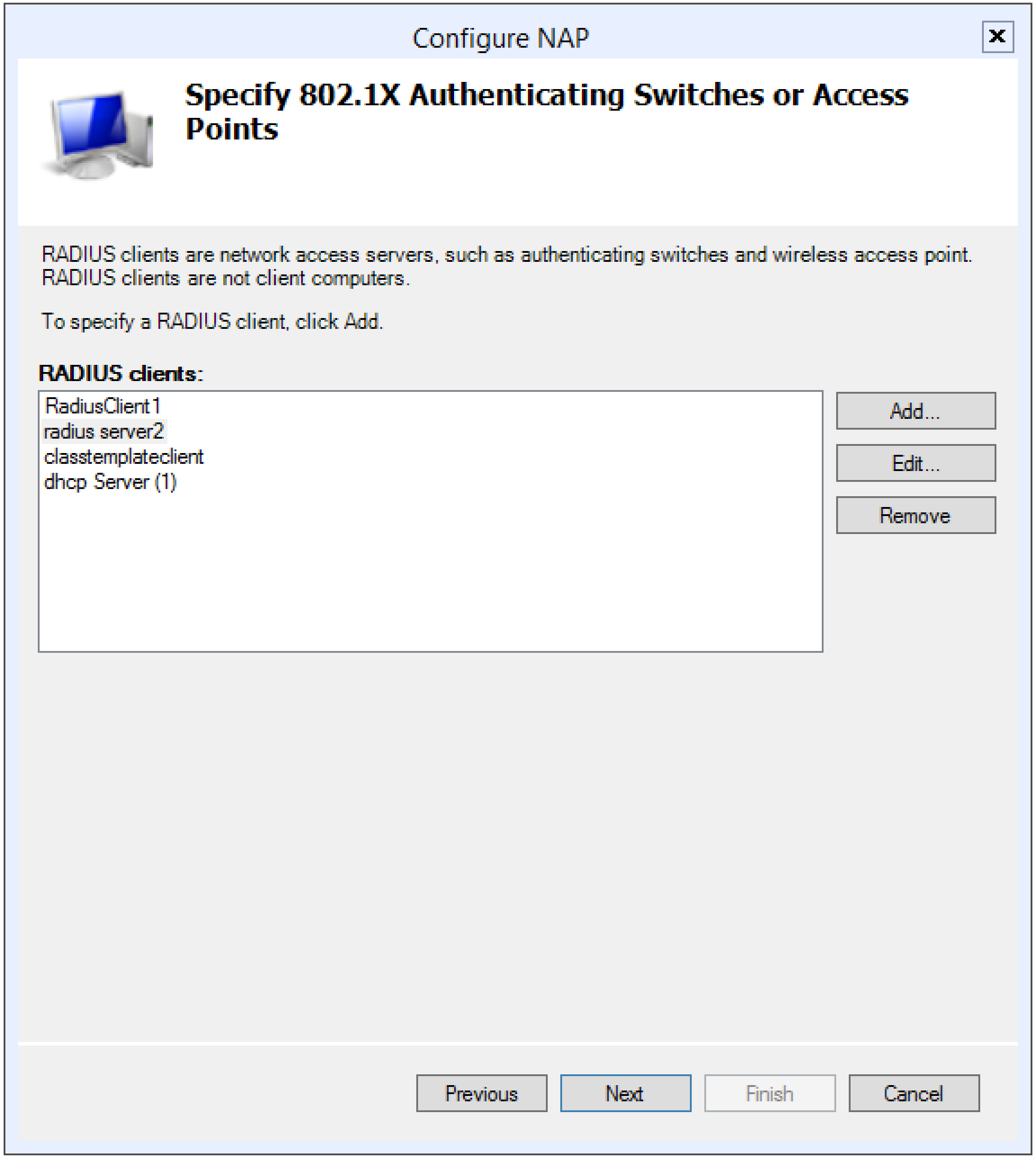
Network connection method:
Select the network connection method that you want to deploy on your network for NAP-capable client computers. Created policies will work with this network connection type only. To create policies for additional network connection methods, you can run the wizard again.

IEEE 802.1X (Wireless)

Policy 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.

NAP 802.1X (Wireless)

Additional requirements:
You must perform additional actions to set up NAP. View additional NAP requirements by clicking on the link below.
Additional Requirements



Configure NAP

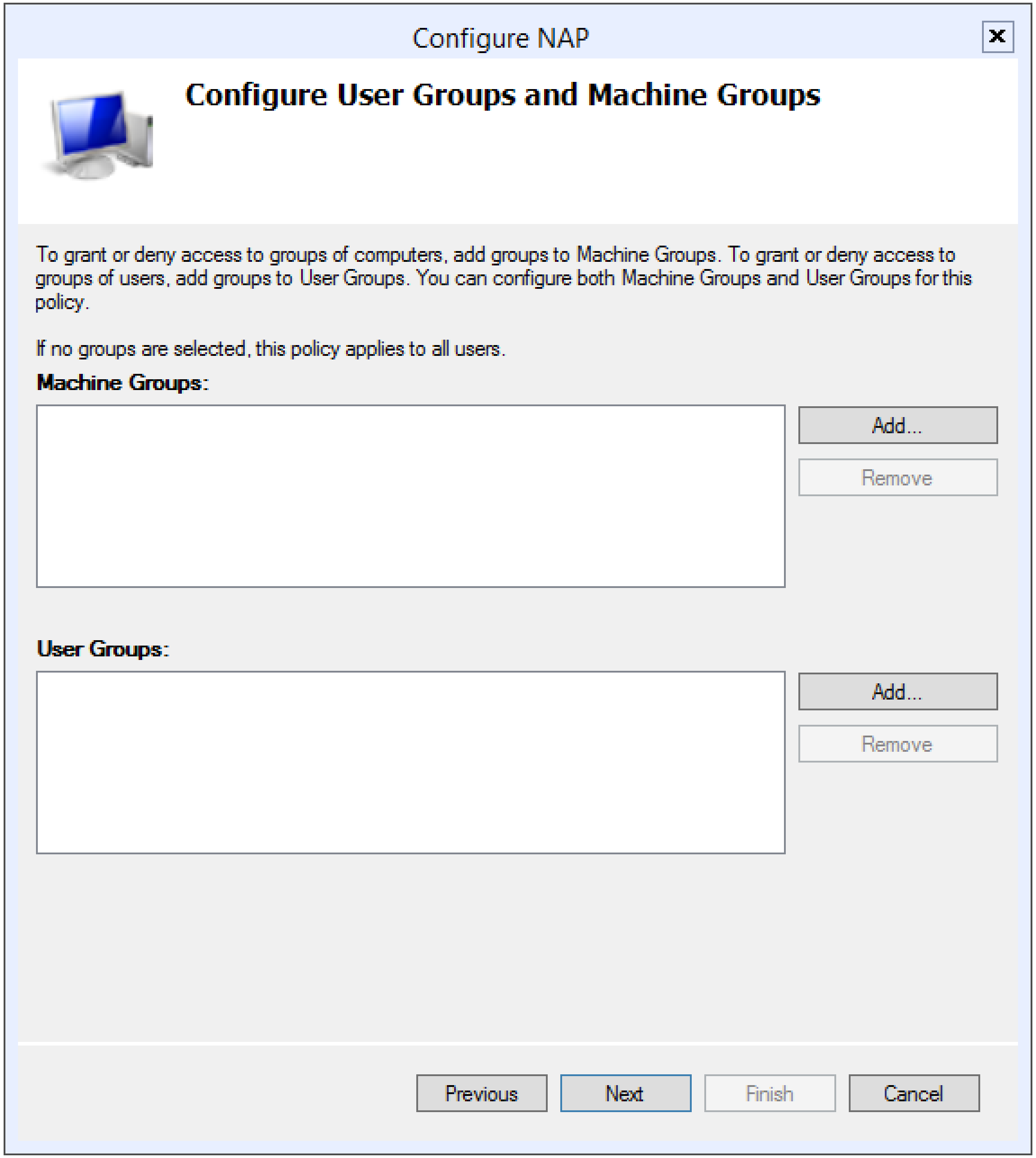
Specify 802.1X Authenticating Switches or Access Points

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

To specify a RADIUS client, click Add.

RADIUS clients:

RadiusClient1
radius server2
classtemplateclient
dhcp Server (1)



Configure NAP

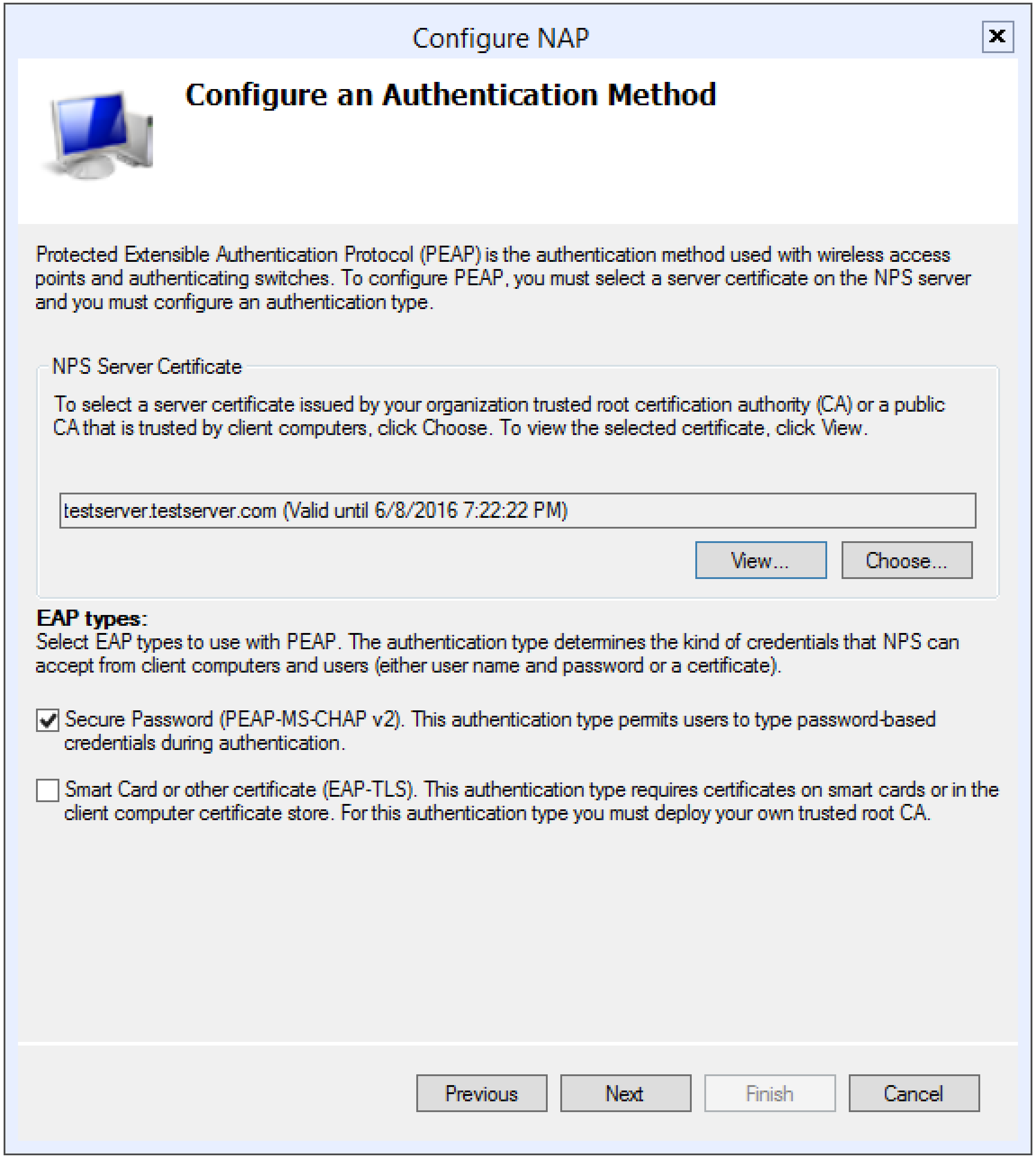
Configure User Groups and Machine Groups

To grant or deny access to groups of computers, add groups to Machine Groups. To grant or deny access to groups of users, add groups to User Groups. You can configure both Machine Groups and User Groups for this policy.

If no groups are selected, this policy applies to all users.

Machine Groups:

User Groups:



Configure an Authentication Method

Protected Extensible Authentication Protocol (PEAP) is the authentication method used with wireless access points and authenticating switches. To configure PEAP, you must select a server certificate on the NPS server and you must configure an authentication type.

NPS Server Certificate

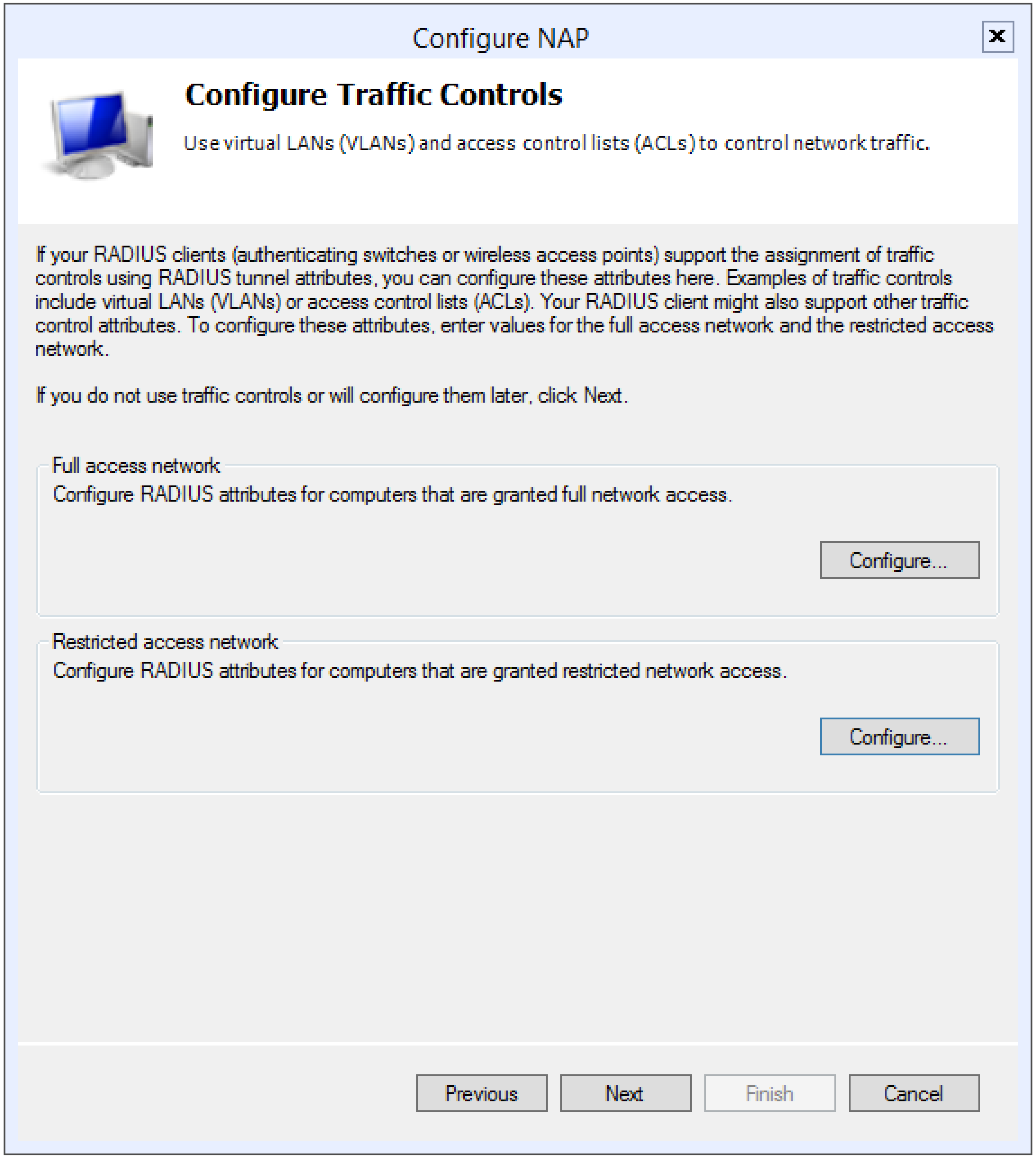
To select a server certificate issued by your organization trusted root certification authority (CA) or a public CA that is trusted by client computers, click Choose. To view the selected certificate, click View.

testserver.testserver.com (Valid until 6/8/2016 7:22:22 PM)

EAP types:
Select EAP types to use with PEAP. The authentication type determines the kind of credentials that NPS can accept from client computers and users (either user name and password or a certificate).

☑ Secure Password (PEAP-MS-CHAP v2). This authentication type permits users to type password-based credentials during authentication.

□ Smart Card or other certificate (EAP-TLS). This authentication type requires certificates on smart cards or in the client computer certificate store. For this authentication type you must deploy your own trusted root CA.



Configure NAP

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. Examples of traffic controls include virtual LANs (VLANs) or access control lists (ACLs). Your RADIUS client might also support other traffic control attributes. To configure these attributes, enter values for the full access network and the restricted access network.

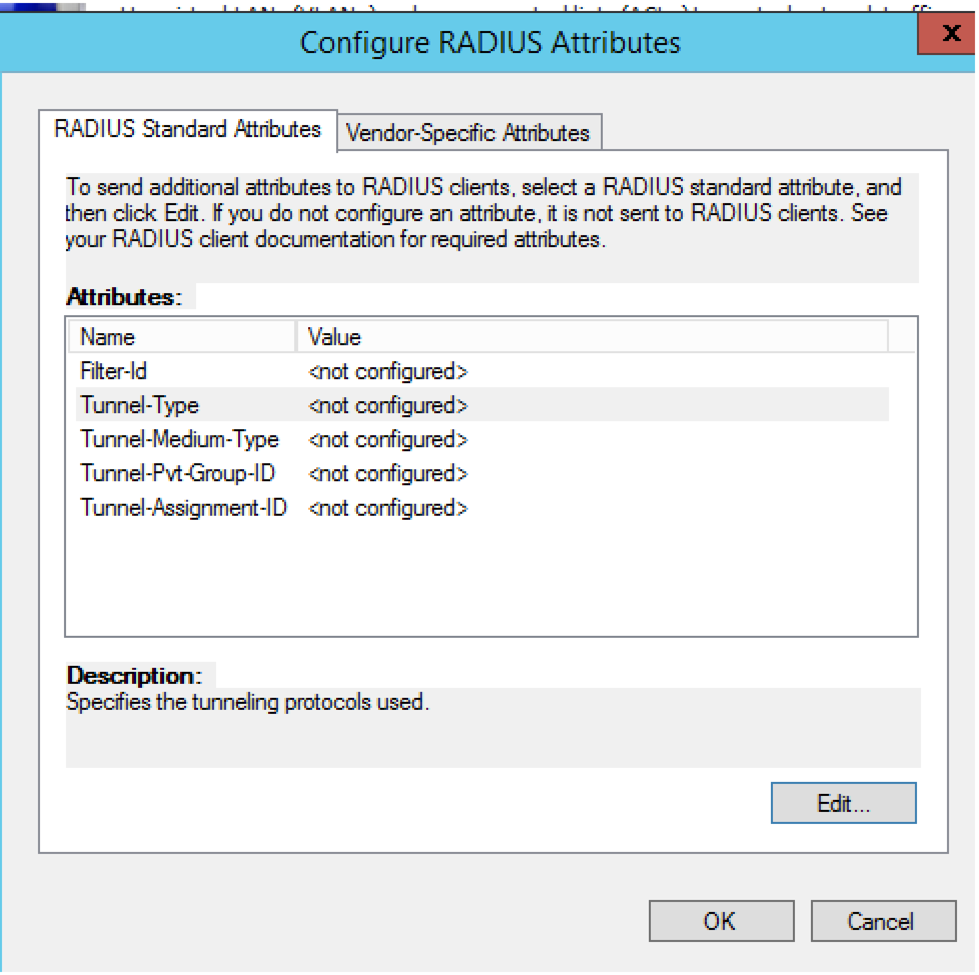
If you do not use traffic controls or will configure them later, click Next.

Full access network

Configure RADIUS attributes for computers that are granted full network access.

Restricted access network

Configure RADIUS attributes for computers that are granted restricted network access.

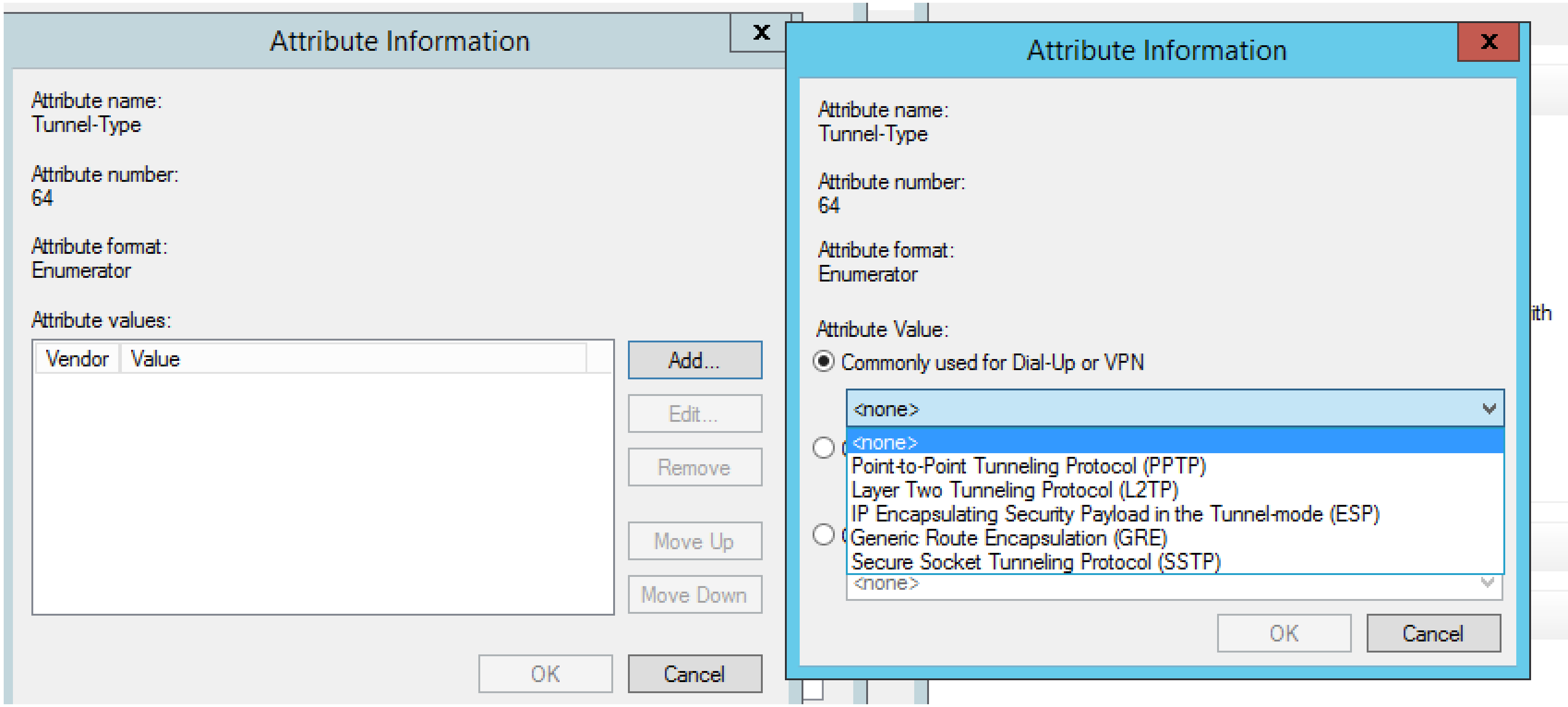

Configure RADIUS Attributes
RADIUS Standard Attributes
Vendor-Specific Attributes
Edit...
OK
Cancel

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.



Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute values:

Vendor	Value

Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute Value:

● Commonly used for Dial-Up or VPN

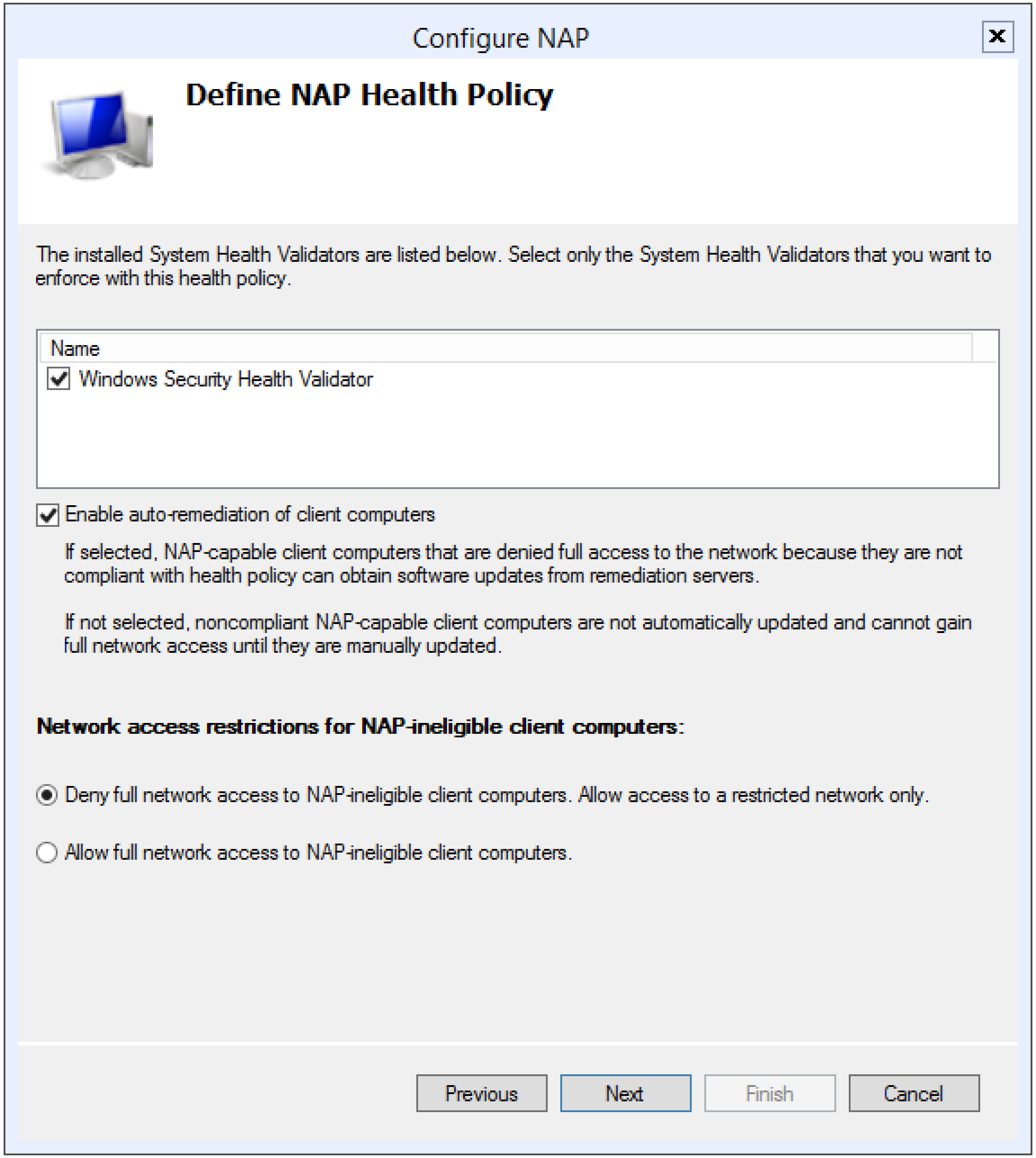
<none>

- <none>
- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- IP Encapsulating Security Payload in the Tunnel-mode (ESP)
- Generic Route Encapsulation (GRE)
- Secure Socket Tunneling Protocol (SSTP)

○

○

<none>



Define NAP Health Policy

The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.

Name
☑ Windows Security Health Validator

☑ Enable auto-remediation of client computers

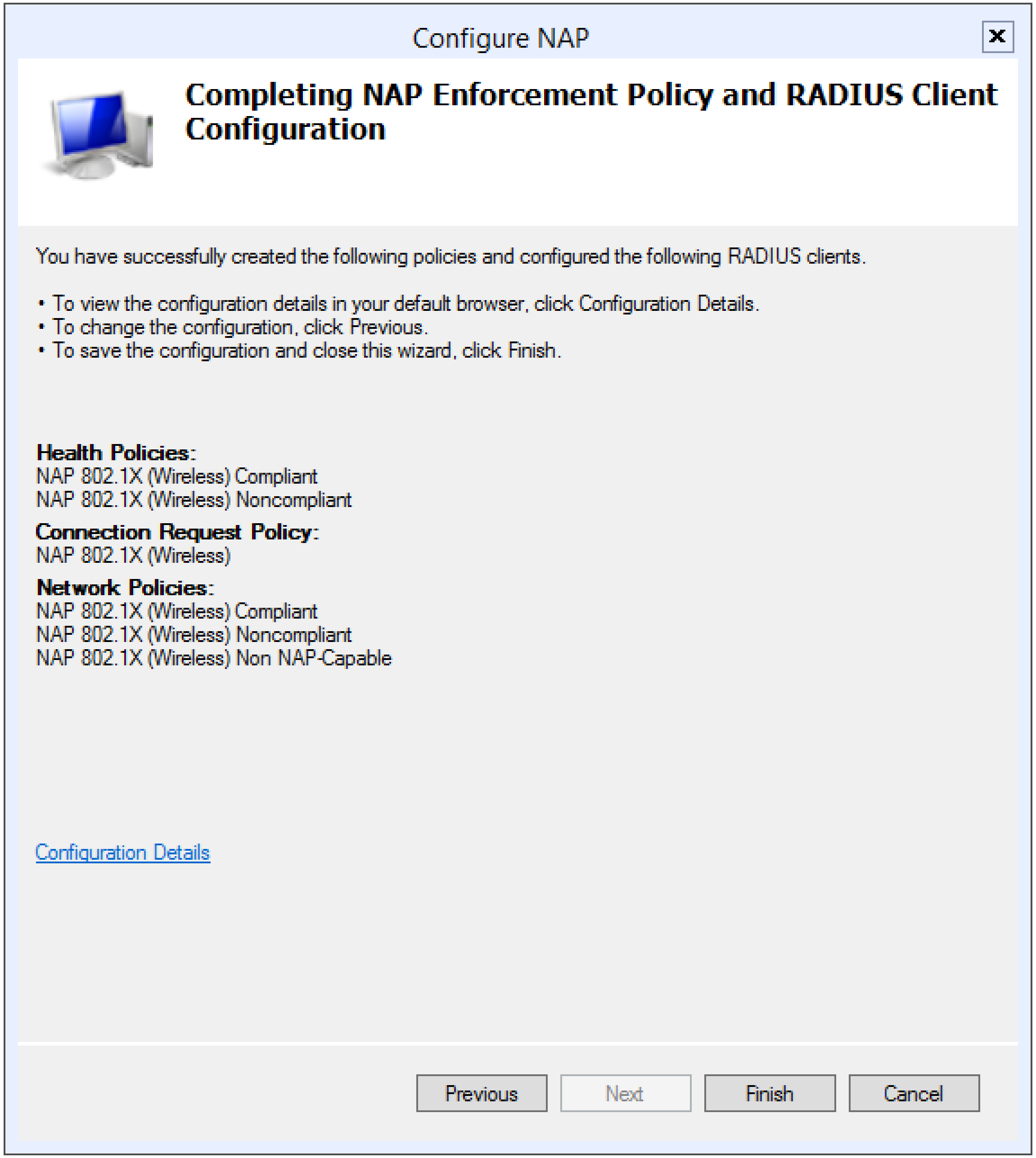
If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.

If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.

Network access restrictions for NAP-ineligible client computers:

● Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.

○ Allow full network access to NAP-ineligible client computers.



Completing NAP Enforcement Policy and RADIUS Client Configuration

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.

Health Policies:
NAP 802.1X (Wireless) Compliant
NAP 802.1X (Wireless) Noncompliant

Connection Request Policy:
NAP 802.1X (Wireless)

Network Policies:
NAP 802.1X (Wireless) Compliant
NAP 802.1X (Wireless) Noncompliant
NAP 802.1X (Wireless) Non NAP-Capable

Configuration Details