

Lesson 12: Configuring a Network Policy Server

MOAC 70-411: Administering
Windows Server 2012

Overview

- Exam Objective 4.1: Configure Network Policy Server (NPS)
- Configuring a Network Policy Server Infrastructure

Configuring a Network Policy Server Infrastructure

Lesson 12: Configuring a Network Policy Server

RADIUS Terms

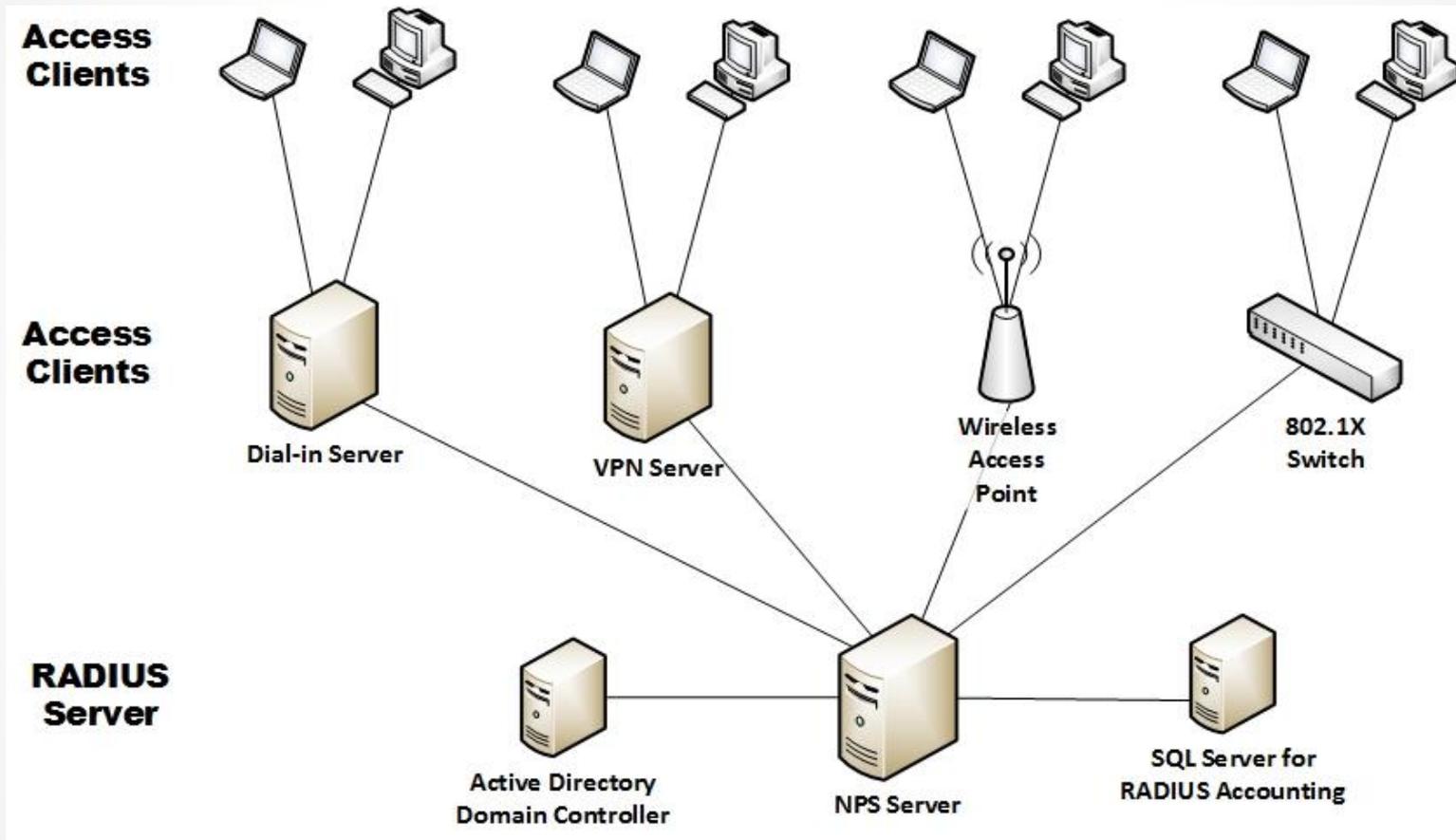
Network Policy Server (NPS): Microsoft's RADIUS server.

Authorization: The process that determines what a user is permitted to do on a computer system or network.

RADIUS client: A server or device that forwards RADIUS requests to a RADIUS server.

Access client: A computer or device that contacts or connects to a RADIUS client, which requires authentication and authorization to connect.

A Network with RADIUS



RADIUS servers and clients

Authentication, Authorization, and Accounting

When NPS is used as a RADIUS server, authentication, authorization, and accounting follows these steps:

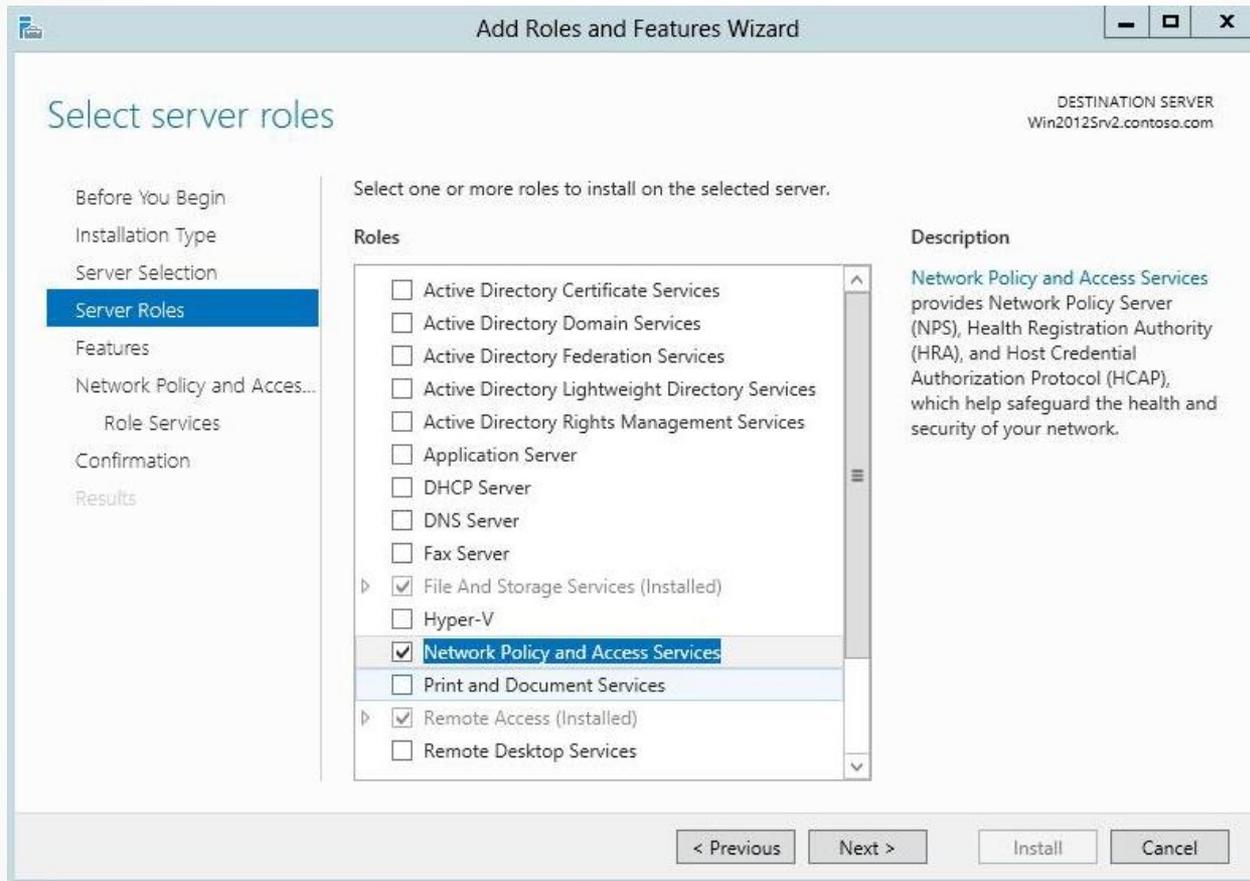
1. When an access client accesses a VPN server or wireless access point, a connection request is created that is sent to the NPS server.
2. The NPS server evaluates the Access-Request message.
3. If required, the NPS server sends an Access-Challenge message to the access server. The access server processes the challenge and sends an updated Access-Request to the NPS server.
4. The user credentials are checked and the dial-in properties of the user account are obtained by using a secure connection to a domain controller.

Authentication, Authorization, and Accounting

When NPS is used as a RADIUS server, authentication, authorization and accounting follows these steps (cont.):

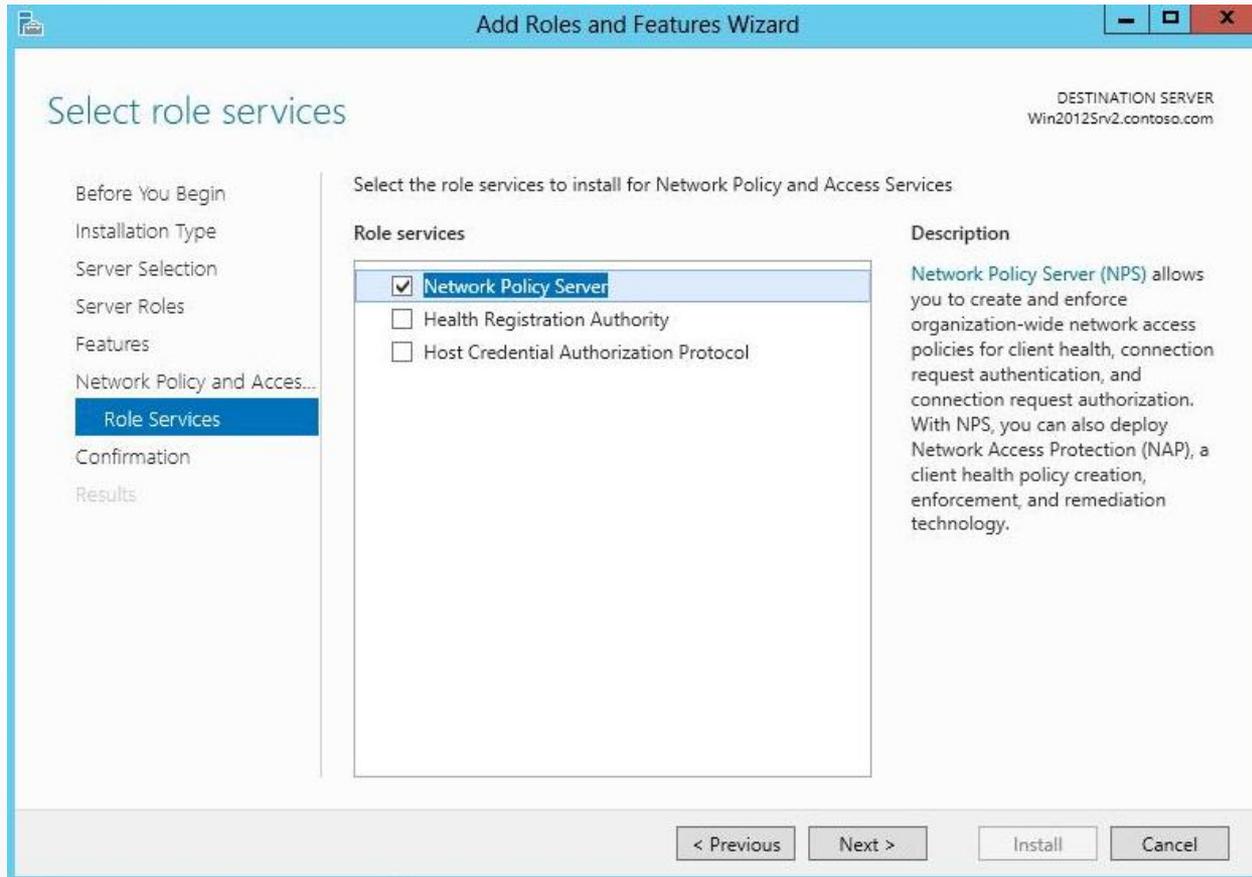
5. When the connection attempt is authorized with both the dial-in properties of the user account and network policies, the NPS server sends an Access-Accept message to the access server. If the connection attempt is either not authenticated or not authorized, the NPS server sends an Access-Reject message to the access server.
6. The access server completes the connection process with the access client and sends an Accounting-Request message to the NPS server, where the message is logged.
7. The NPS server sends an Accounting-Response to the access server.

Installing Network Policy Server



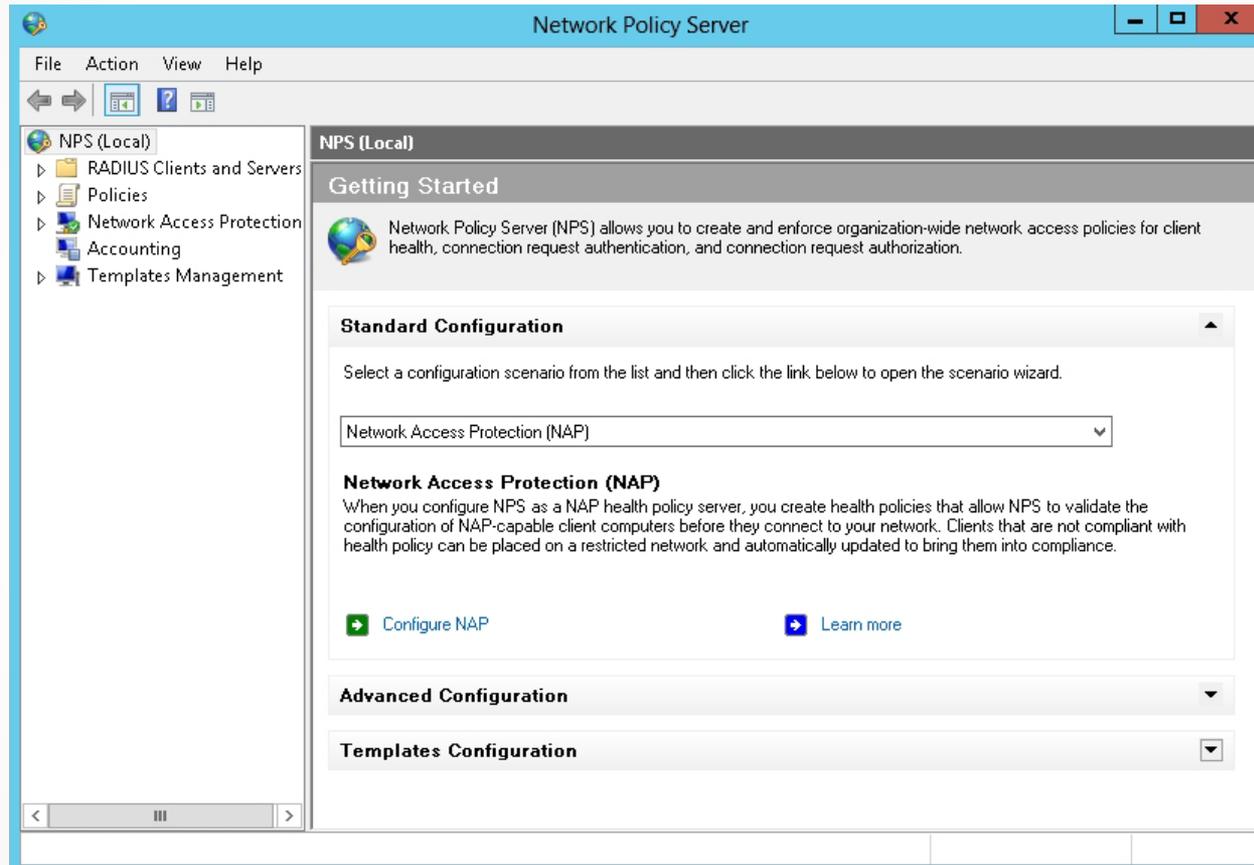
Installing Network Policy and Access Services

Installing Network Policy Server



Selecting Network Policy and Access Service Role Services

Installing Network Policy Server



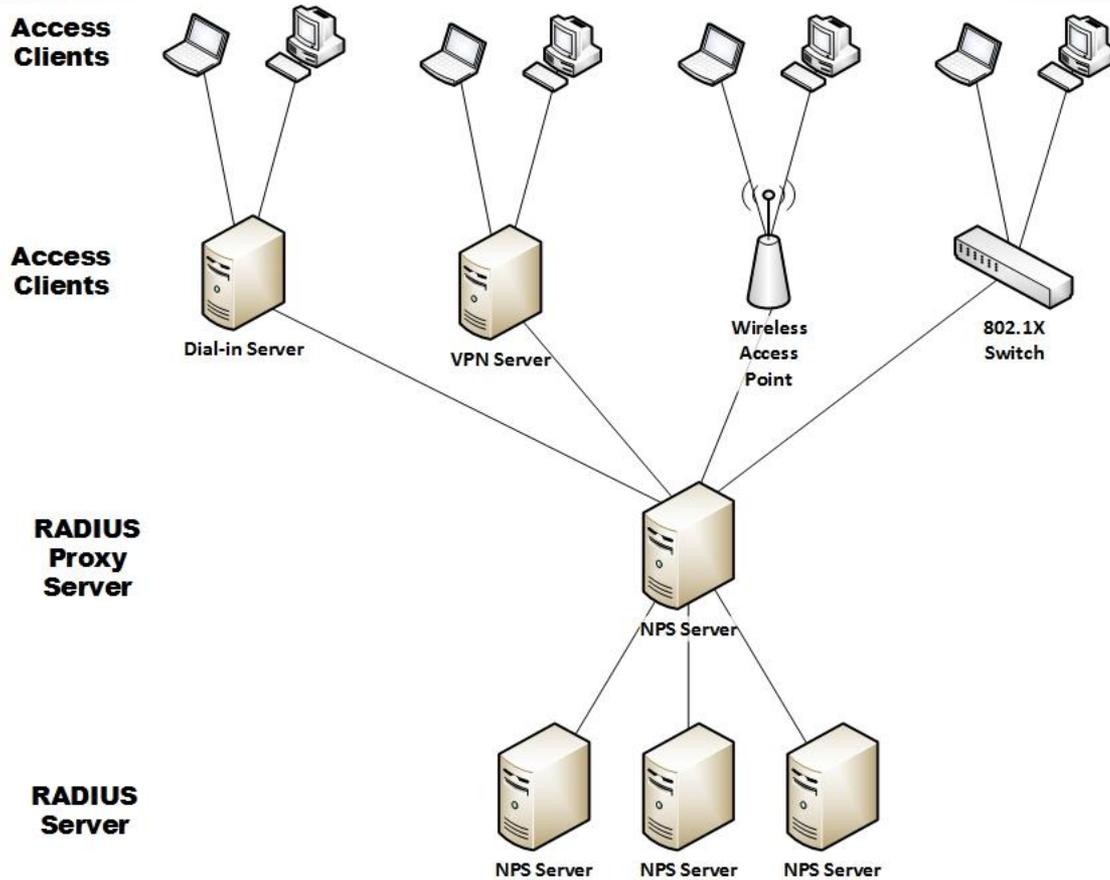
Opening the Network Policy Server console

Configuring RADIUS Server Infrastructures

Multiple RADIUS server configurations:

- Primary RADIUS server and alternate RADIUS servers
- A **RADIUS proxy** located between the RADIUS server and the RADIUS clients

Configuring RADIUS Server Infrastructures



Using a RADIUS proxy server

Configuring RADIUS Server Infrastructures

Load balancing options:

- Priority
- Weight
- Advanced settings

Add a Remote RADIUS Server Group

The dialog box is titled "New Remote RADIUS Server Group" and has a close button (X) in the top right corner. It contains the following elements:

- Group name:** A text input field.
- RADIUS Servers:** A table with the following structure:

RADIUS Server	Priority	Weight	
- Buttons:** "Add...", "Edit...", "Remove", "OK", and "Cancel".

Creating a new RADIUS server group

Add a Remote RADIUS Server Group

Add RADIUS Server

Address: Authentication/Accounting | Load Balancing

Select an existing Remote RADIUS Servers template:
None

Type the name or IP address of the RADIUS server you want to add.

Server:
192.168.3.121 Verify...

OK Cancel

Adding a RADIUS server to the RADIUS server group

Add a Remote RADIUS Server Group

Add RADIUS Server

Address Authentication/Accounting Load Balancing

Authentication port: 1812

Select an existing Shared Secrets template: None

Shared secret:

Confirm shared secret:

Request must contain the message authenticator attribute

Accounting

Accounting port: 1813

Use the same shared secret for authentication and accounting.

Select an existing Shared Secrets template: None

Shared secret:

Confirm shared secret:

Forward network access server start and stop notifications to this server

OK Cancel

Configuring Authentication and Accounting RADIUS

Add a Remote RADIUS Server Group

Add RADIUS Server [X]

Address Authentication/Accounting **Load Balancing**

The priority of ranking indicates the status of a server. A primary server has a priority of 1.

Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority.

Priority: Weight:

Advanced settings

Number of seconds without response before request is considered dropped:

Maximum number of dropped requests before server is identified as unavailable:

Number of seconds between requests when server is identified as unavailable:

OK Cancel

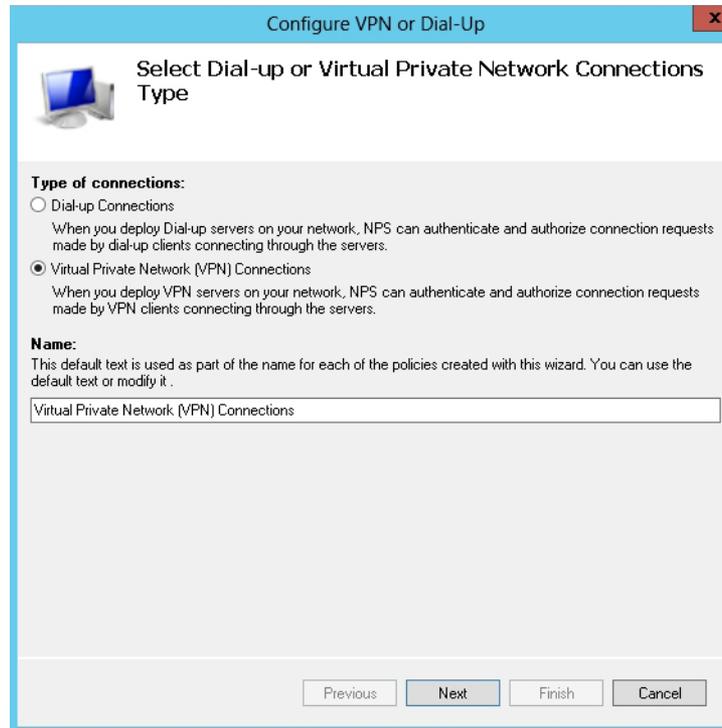
Configuring RADIUS load balancing

Configuring RADIUS Clients

The standard configuration includes:

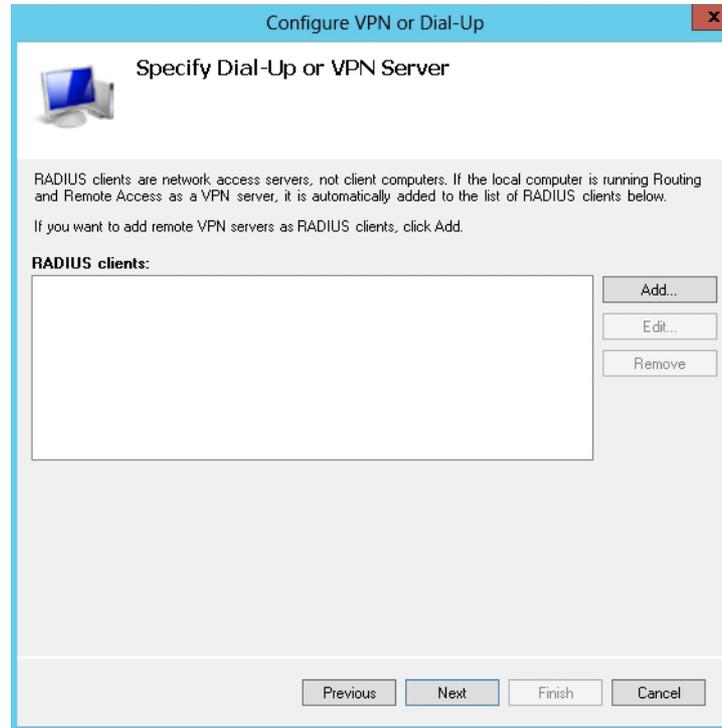
- RADIUS server for dial-up or VPN connections
- RADIUS server for 802.1X wireless or wired connections
- NAP policy server (discussed in Lesson 14)

Configure NPS for RADIUS Server for VPN Connections



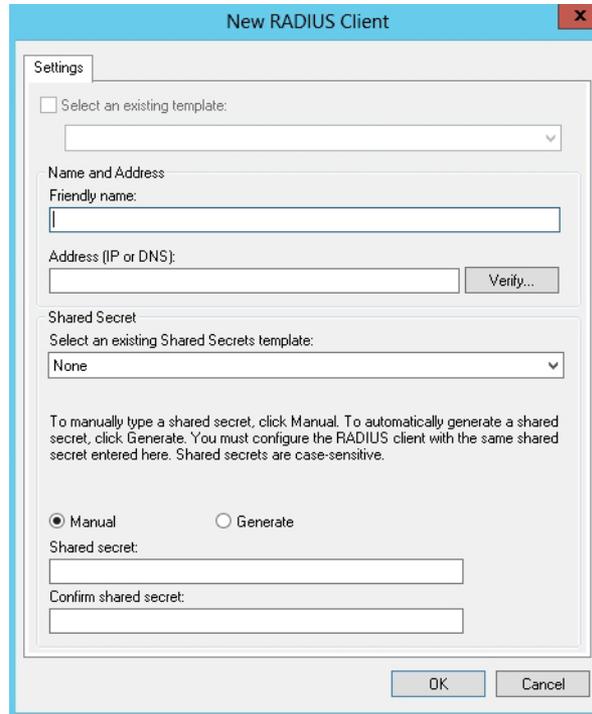
Specifying connections on the Dial-up or Virtual Private Network Connections Type page

Configure NPS for RADIUS Server for VPN Connections



Showing the RADIUS clients page

Configure NPS for RADIUS Server for VPN Connections



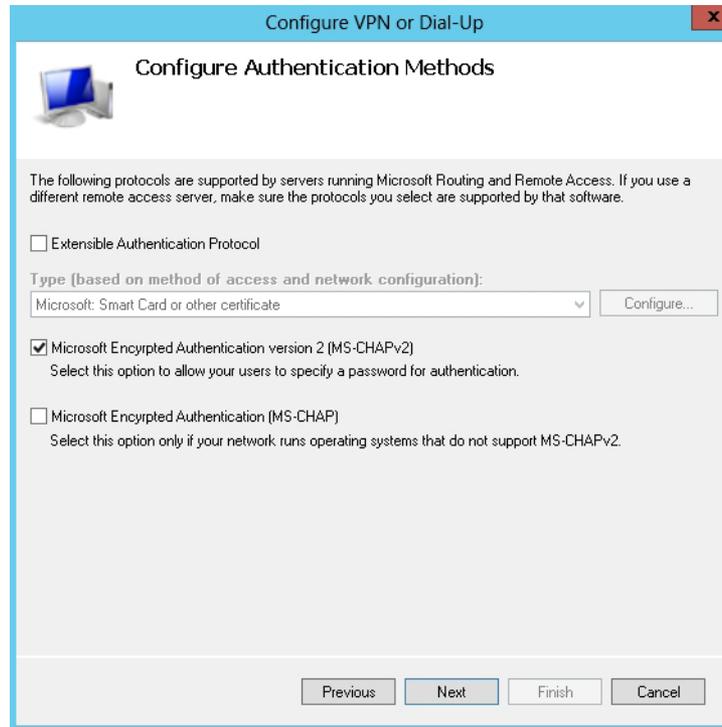
The image shows a screenshot of the 'New RADIUS Client' dialog box in Windows Network Policy Server (NPS) configuration. The dialog has a title bar with the text 'New RADIUS Client' and a close button (X). The main content area is titled 'Settings' and contains the following fields and options:

- Select an existing template:
A dropdown menu is located below this checkbox.
- Name and Address**
 - Friendly name: [Text input field]
 - Address (IP or DNS): [Text input field] [Verify... button]
- Shared Secret**
 - Select an existing Shared Secrets template:
A dropdown menu showing 'None' is located below this label.
 - To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
 - Manual Generate
 - Shared secret: [Text input field]
 - Confirm shared secret: [Text input field]

At the bottom right of the dialog, there are 'OK' and 'Cancel' buttons.

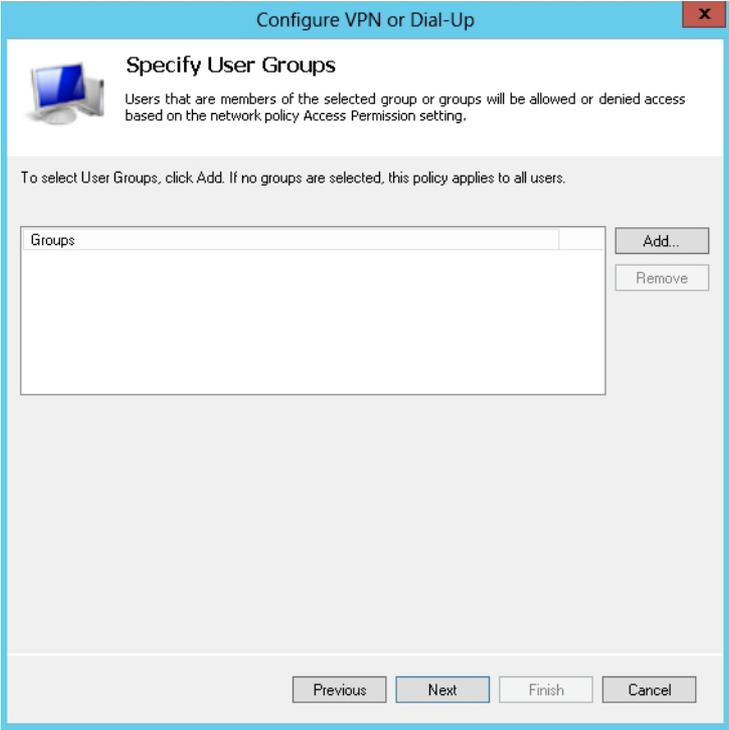
Adding RADIUS clients

Configure NPS for RADIUS Server for VPN Connections



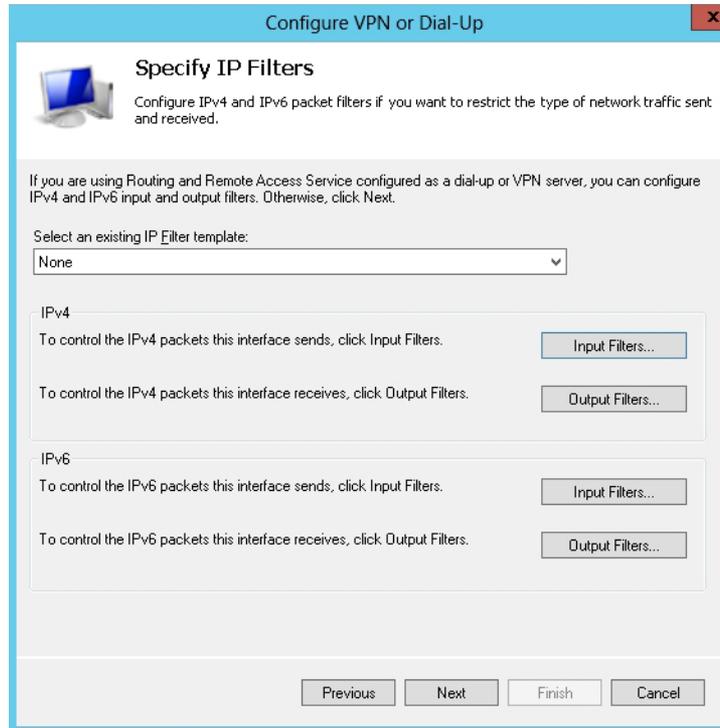
Specifying authentication methods

Configure NPS for RADIUS Server for VPN Connections



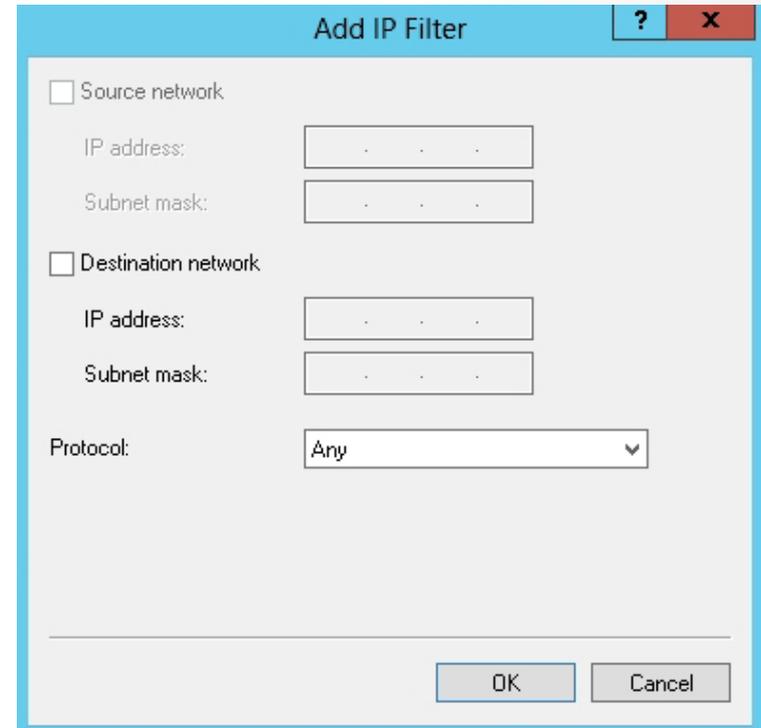
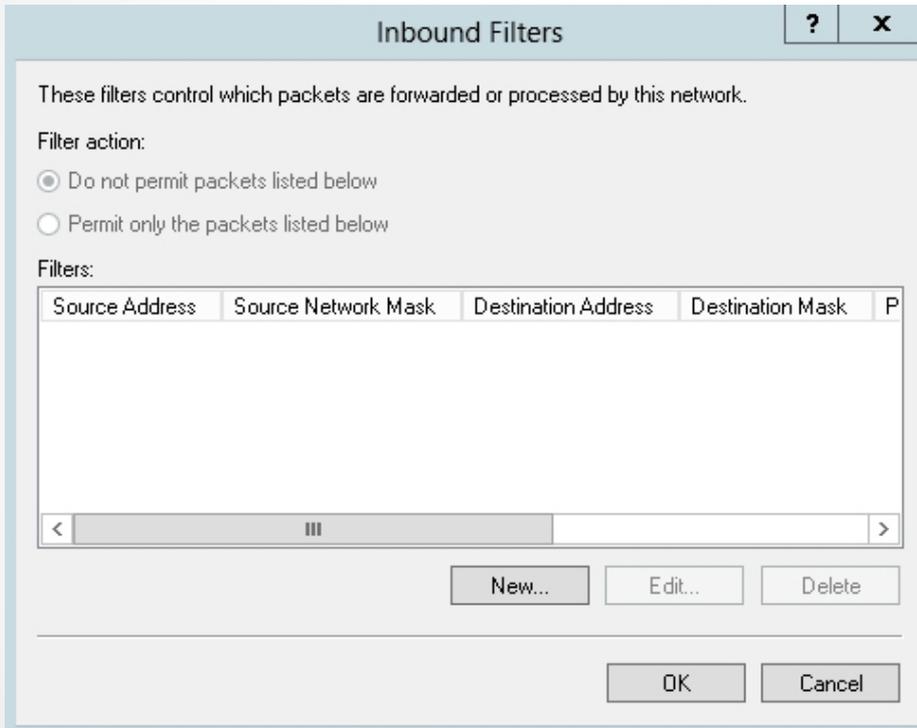
Specifying user groups

Configure NPS for RADIUS Server for VPN Connections



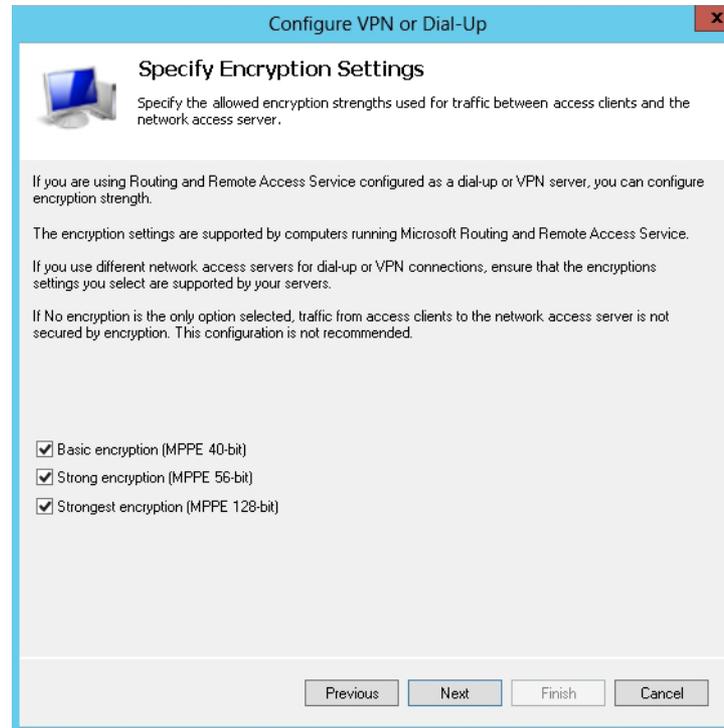
Specifying IP filters

Configure NPS for RADIUS Server for VPN Connections



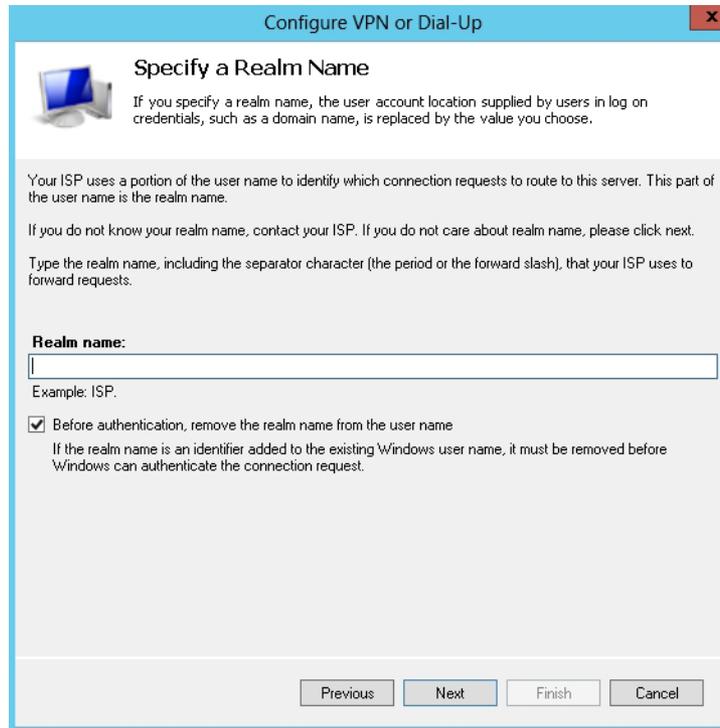
Configuring inbound filters

Configure NPS for RADIUS Server for VPN Connections



Specifying encryption settings

Configure NPS for RADIUS Server for VPN Connections



The screenshot shows a dialog box titled "Configure VPN or Dial-Up" with a close button (X) in the top right corner. The main heading is "Specify a Realm Name". Below the heading is a small icon of a computer monitor and keyboard. The text explains that specifying a realm name replaces the user account location in log-on credentials. It provides instructions on how to determine the realm name from an ISP and includes a text input field for the realm name. An example "ISP." is provided. A checked checkbox indicates that the realm name should be removed before authentication. At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Specify a Realm Name

If you specify a realm name, the user account location supplied by users in log on credentials, such as a domain name, is replaced by the value you choose.

Your ISP uses a portion of the user name to identify which connection requests to route to this server. This part of the user name is the realm name.

If you do not know your realm name, contact your ISP. If you do not care about realm name, please click next.

Type the realm name, including the separator character (the period or the forward slash), that your ISP uses to forward requests.

Realm name:

Example: ISP.

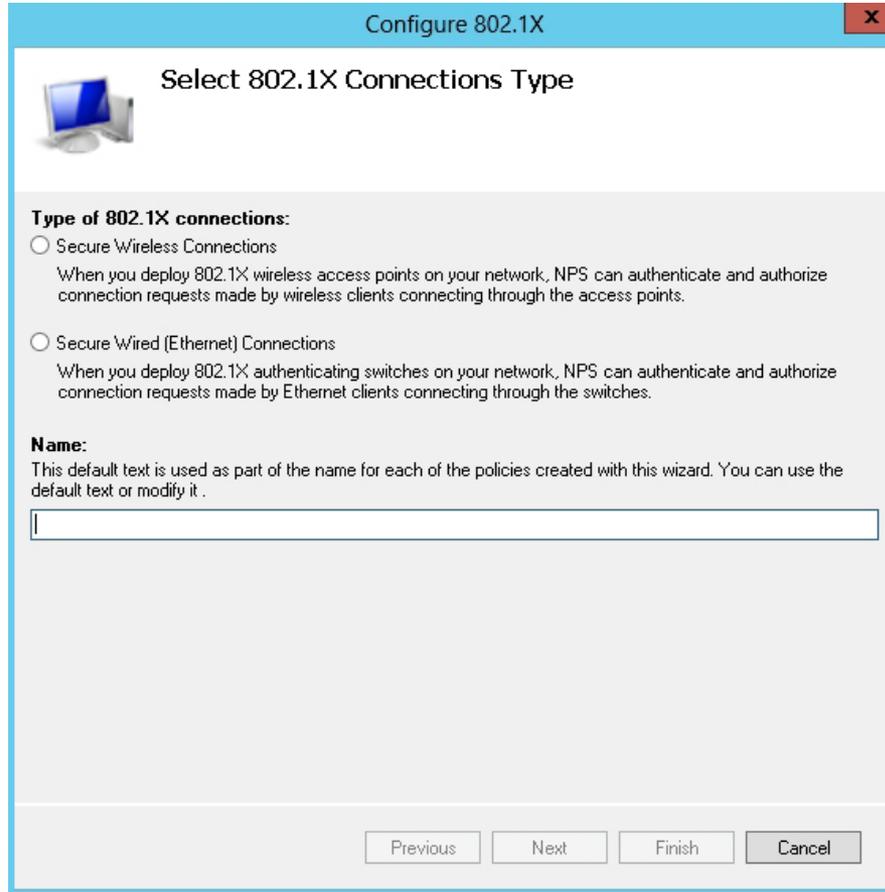
Before authentication, remove the realm name from the user name

If the realm name is an identifier added to the existing Windows user name, it must be removed before Windows can authenticate the connection request.

Previous Next Finish Cancel

Specifying a realm name

Configure NPS for 802.1X Wireless Connections



The screenshot shows a window titled "Configure 802.1X" with a close button in the top right corner. The main heading is "Select 802.1X Connections Type" next to a computer icon. Under the heading "Type of 802.1X connections:", there are two radio button options. The first is "Secure Wireless Connections" with a description: "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." The second is "Secure Wired (Ethernet) Connections" with a description: "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." Below this is a section labeled "Name:" with a text box and a description: "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." At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Configure 802.1X

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.

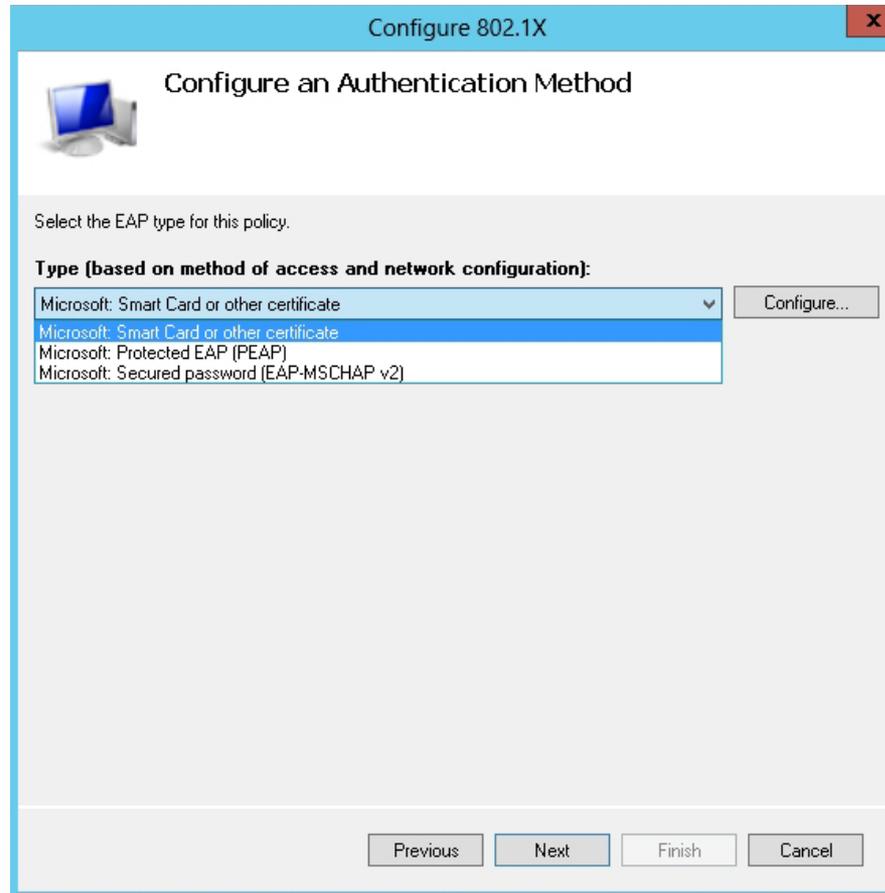
Secure Wired (Ethernet) Connections
When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

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

Selecting the 802.1X connections type

Configure NPS for 802.1X Wireless Connections



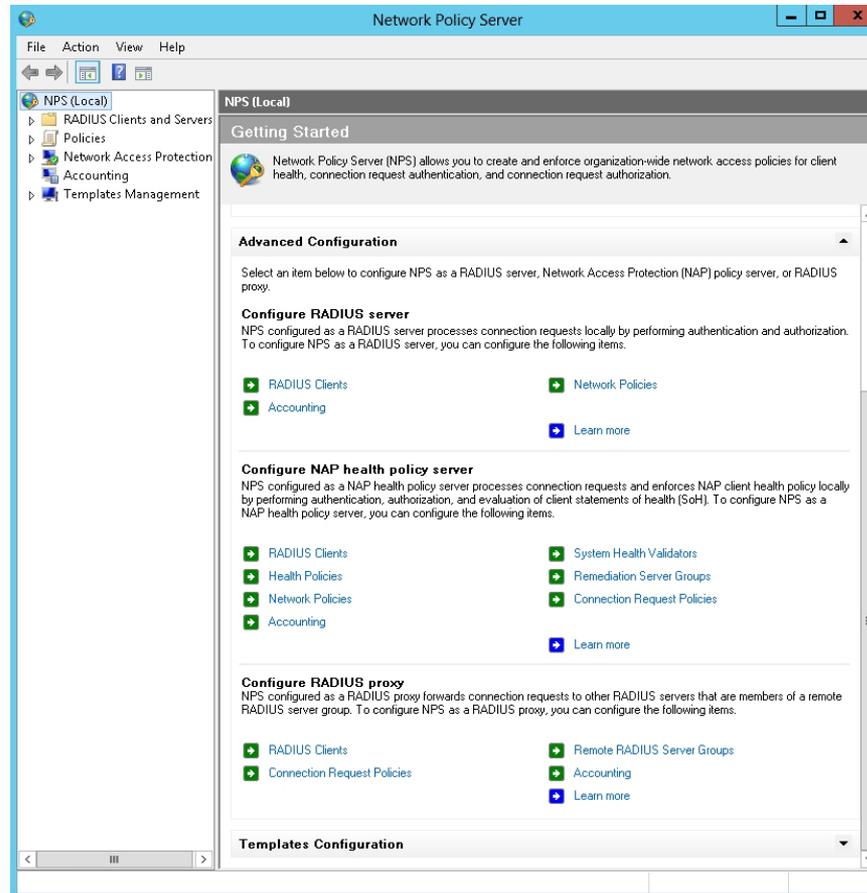
Configuring authentication methods for 802.1X

Configure NPS for 802.1X Wireless Connections



Configuring traffic controls

NPS Advanced Configuration



Network Policies

The screenshot shows the Network Policy Server console. The left pane displays the tree structure under 'NPS (Local)', with 'Network Policies' selected. The main pane shows a list of policies and the configuration for the selected 'Virtual Private Network (VPN) Connections' policy.

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified
Virtual Private Network (VPN) Connections	Enabled	2	Grant Access	Remote Ac...
Connections to Microsoft Routing and Remote Access server	Enabled	999999	Deny Access	Unspecified
Connections to other access servers	Enabled	1000000	Deny Access	Unspecified

Virtual Private Network (VPN) Connections

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Virtual (VPN)
Windows Groups	CONTOSO\Domain Users

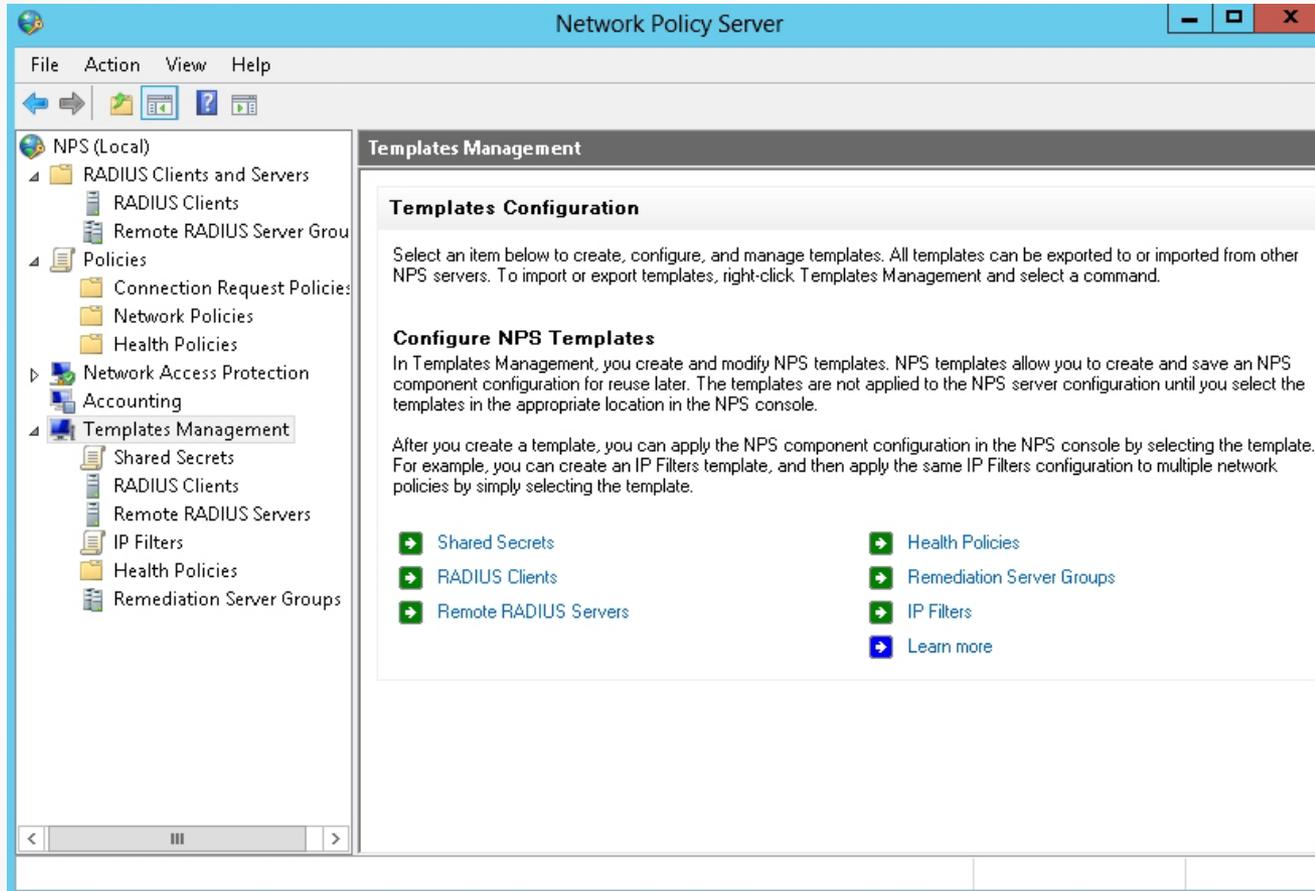
Settings - Then the following settings are applied:

Setting	Value
Authentication Method	MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired)
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed
Encryption	Basic encryption (MPPE 40-bit), Strong encryption (MPPE 56-bit), Strongest encryption (EAP-TLS)

Managing RADIUS Templates

- RADIUS templates:
 - Are designed to reduce the amount of time and cost that it takes to configure RADIUS on one or more servers
- Creating a RADIUS template does not affect the functionality of NPS.
- A RADIUS template affects only the NPS server when the template is selected and applied when configuring RADIUS.

Managing RADIUS Templates



Templates Configuration options
in the NPS console

Managing RADIUS Templates

The image shows a screenshot of a software dialog box titled "New RADIUS Client". The dialog has a blue header bar with a close button (X) in the top right corner. Below the header, there are two tabs: "Settings" and "Advanced", with "Advanced" being the active tab. The dialog is divided into several sections:

- Name and Address:** This section contains two text input fields. The first is labeled "Friendly name:" and is currently empty. The second is labeled "Address (IP or DNS):" and is also empty. To the right of the address field is a "Verify..." button.
- Shared Secret:** This section starts with a label "Select an existing Shared Secrets template:" followed by a dropdown menu that currently shows "None". Below this is a paragraph of text: "To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive." Below the text are two radio buttons: "Manual" (which is selected) and "Generate".
- Shared secret fields:** Below the radio buttons are two text input fields. The first is labeled "Shared secret:" and the second is labeled "Confirm shared secret:". Both are currently empty.

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Creating a RADIUS client template

Managing RADIUS Templates

The screenshot shows a dialog box titled "New RADIUS Client" with a close button (X) in the top right corner. The dialog is divided into two tabs: "Settings" and "Advanced", with "Advanced" currently selected. The "Advanced" tab contains the following fields and options:

- Enable this RADIUS client
- Select an existing template:
 - test
- Name and Address**
 - Friendly name:
 - test
 - Address (IP or DNS):
 - 192.168.3.122
 - Verify...
- Shared Secret**
 - Select an existing Shared Secrets template:
 - None
 - To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
 - Manual Generate
 - Shared secret:
 -
 - Confirm shared secret:
 -

At the bottom of the dialog are "OK" and "Cancel" buttons.

Using the RADIUS client template

Configuring RADIUS Accounting

- NPS can log accounting data to a text log file and/or a SQL Server database.
- NPS server generates an Accounting-Start message describing the type of service being delivered and the user it is being delivered to, which is sent to the RADIUS Accounting server.
- The RADIUS Accounting server sends back an acknowledgment to the RADIUS client.
- At the end of service delivery, the client generates an Accounting-Stop message that describes the type of service that was delivered, and optional statistics, such as elapsed time, input and output octets, or input and output packets. It then sends that data to the RADIUS Accounting server, which sends back an acknowledgment to the RADIUS client.

Configuring RADIUS Accounting

NPS Server

Generates an Accounting-Start message



RADIUS Accounting Server

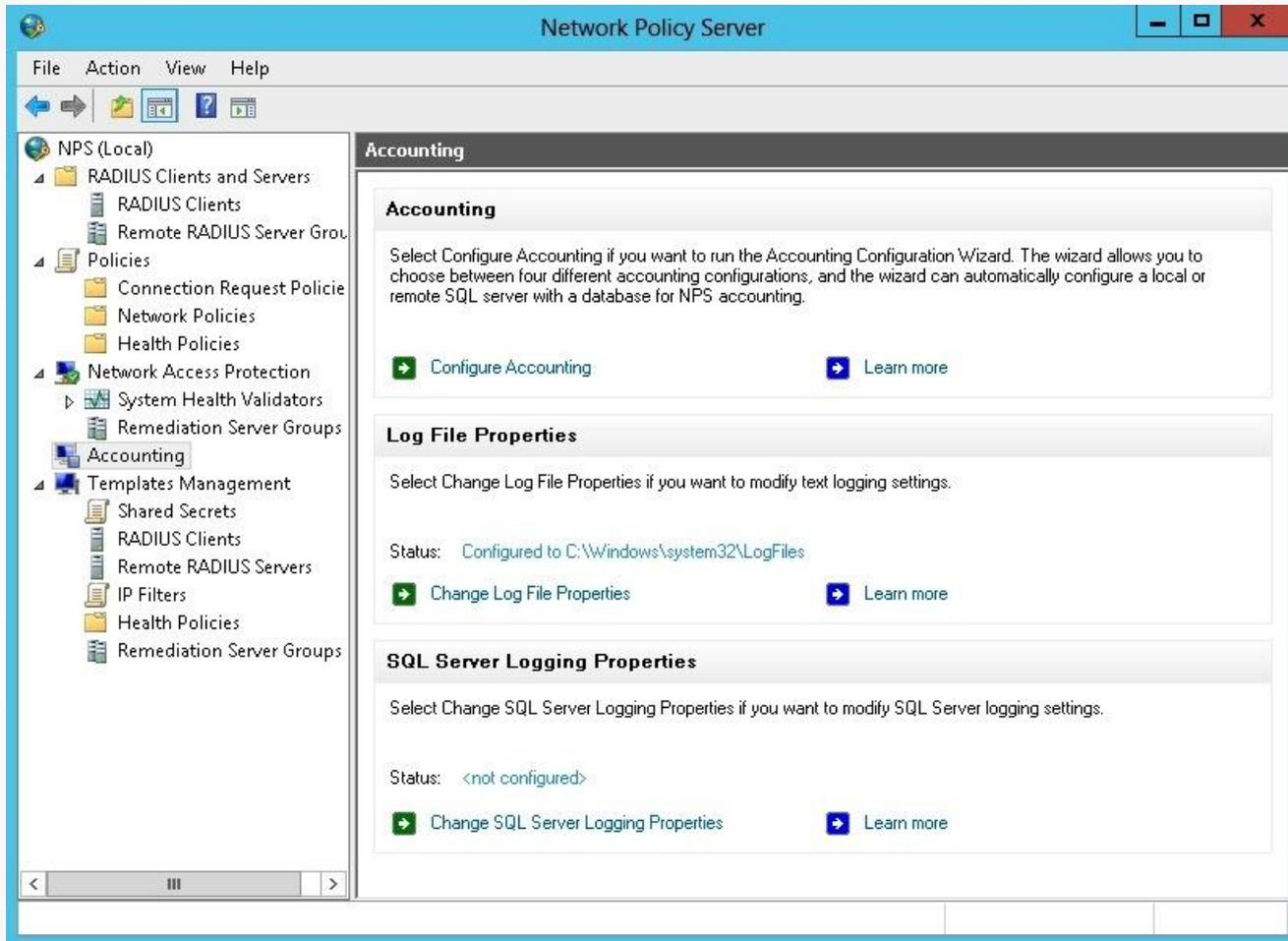
Sends an acknowledgment



RADIUS Client

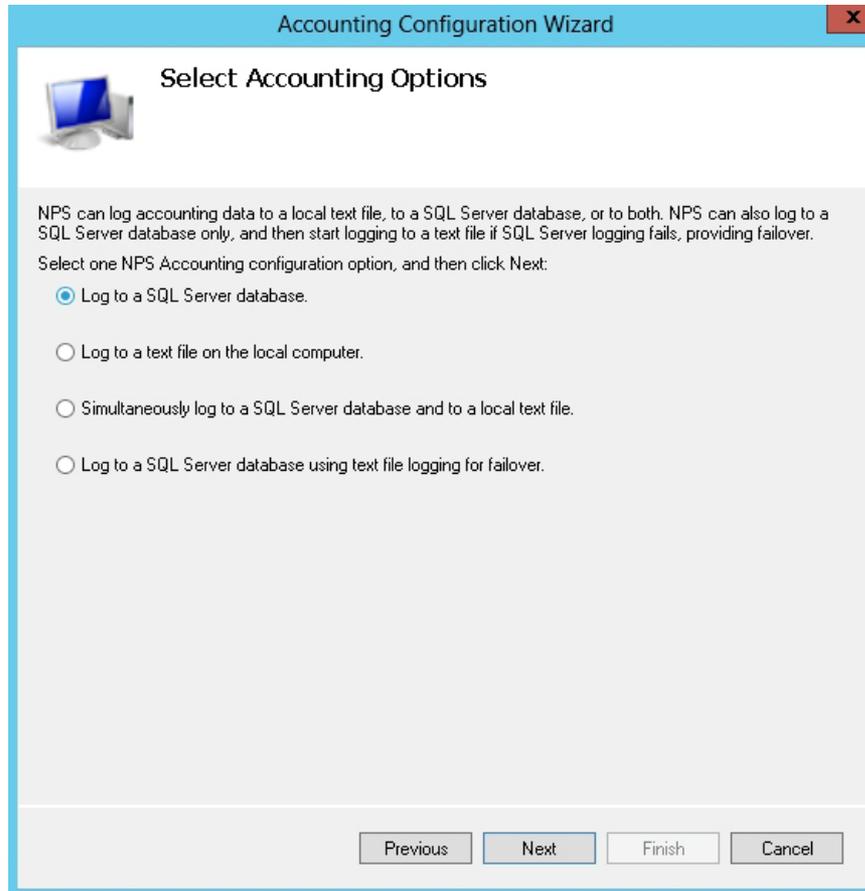
Generates an Accounting-Stop message

To Enable and Configure Accounting in NPS



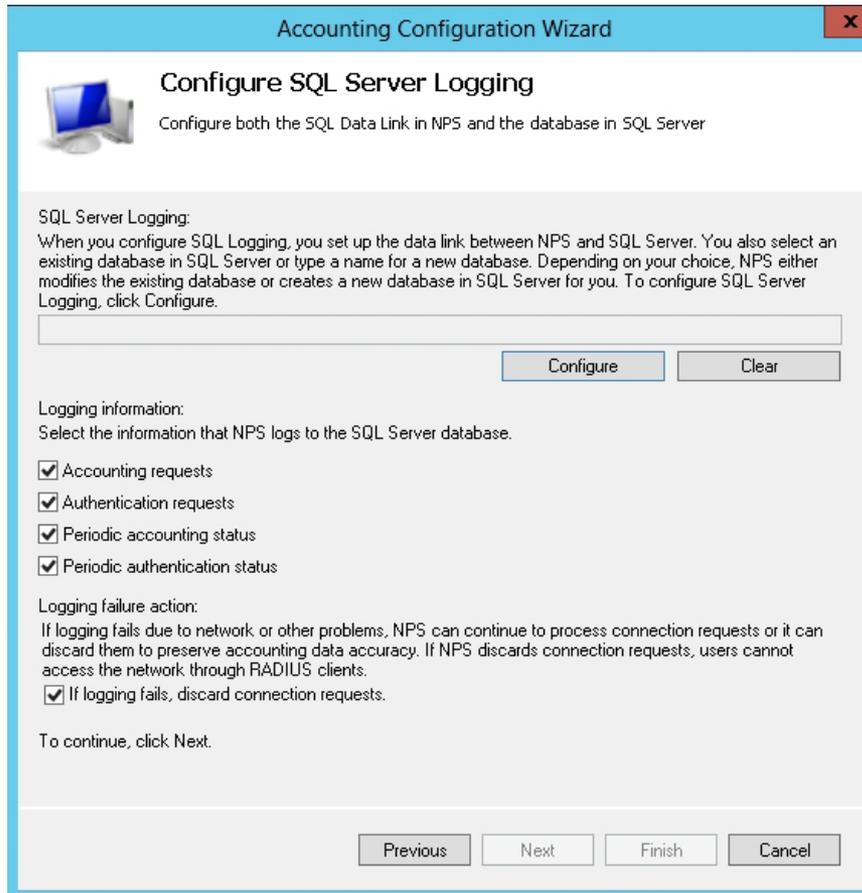
Accounting configuring options

To Enable and Configure Accounting in NPS



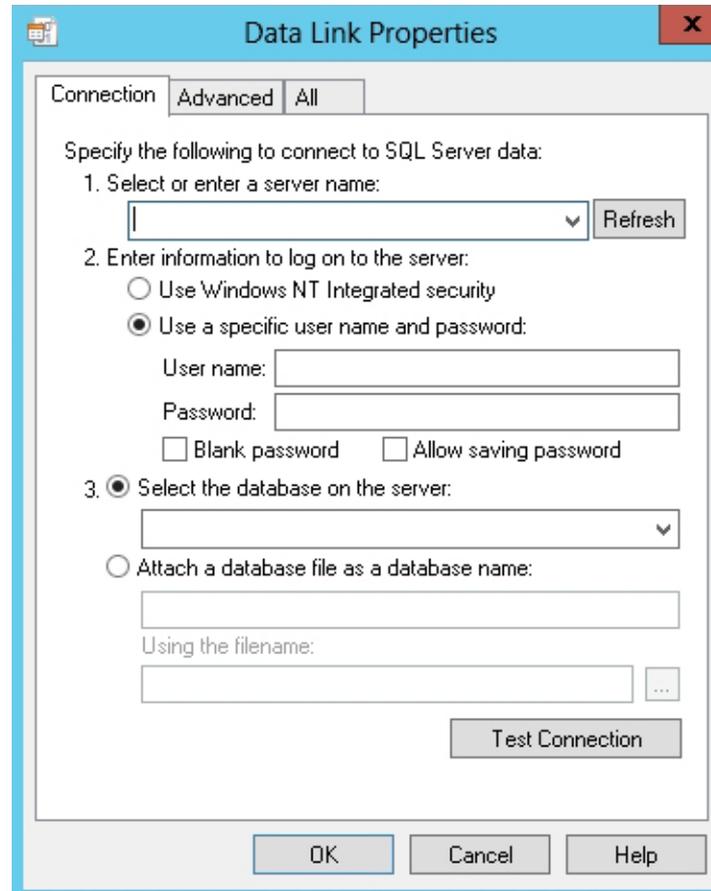
Selecting Accounting options

To Enable and Configure Accounting in NPS



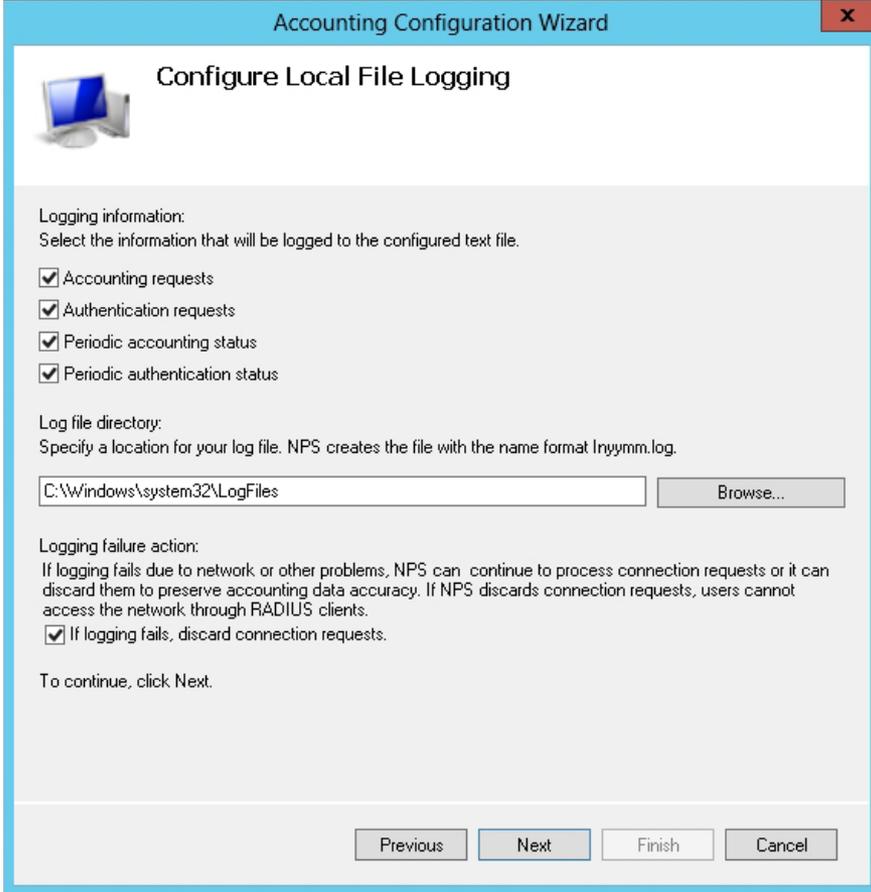
Configuring SQL Server logging

To Enable and Configure Accounting in NPS



Configuring the Data Link properties

To Enable and Configure Accounting in NPS



The screenshot shows a Windows dialog box titled "Accounting Configuration Wizard" with a close button (X) in the top right corner. The main heading is "Configure Local File Logging" next to a computer icon. The dialog is divided into three sections: "Logging information", "Log file directory", and "Logging failure action".

Logging information:
Select the information that will be logged to the configured text file.

- Accounting requests
- Authentication requests
- Periodic accounting status
- Periodic authentication status

Log file directory:
Specify a location for your log file. NPS creates the file with the name format Inyyymm.log.

Logging failure action:
If logging fails due to network or other problems, NPS can continue to process connection requests or it can discard them to preserve accounting data accuracy. If NPS discards connection requests, users cannot access the network through RADIUS clients.

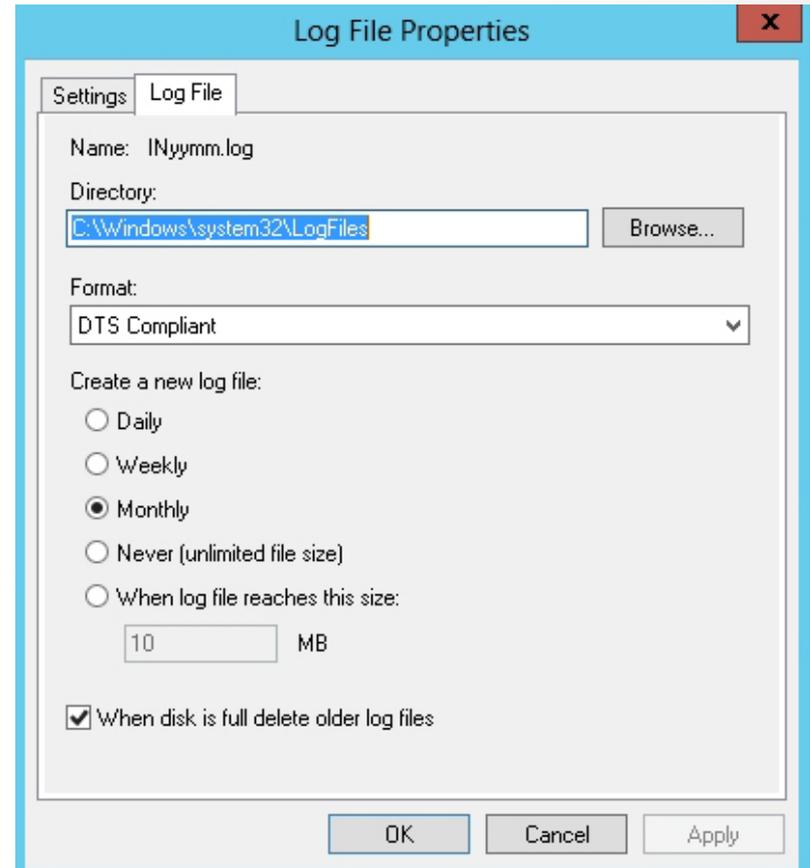
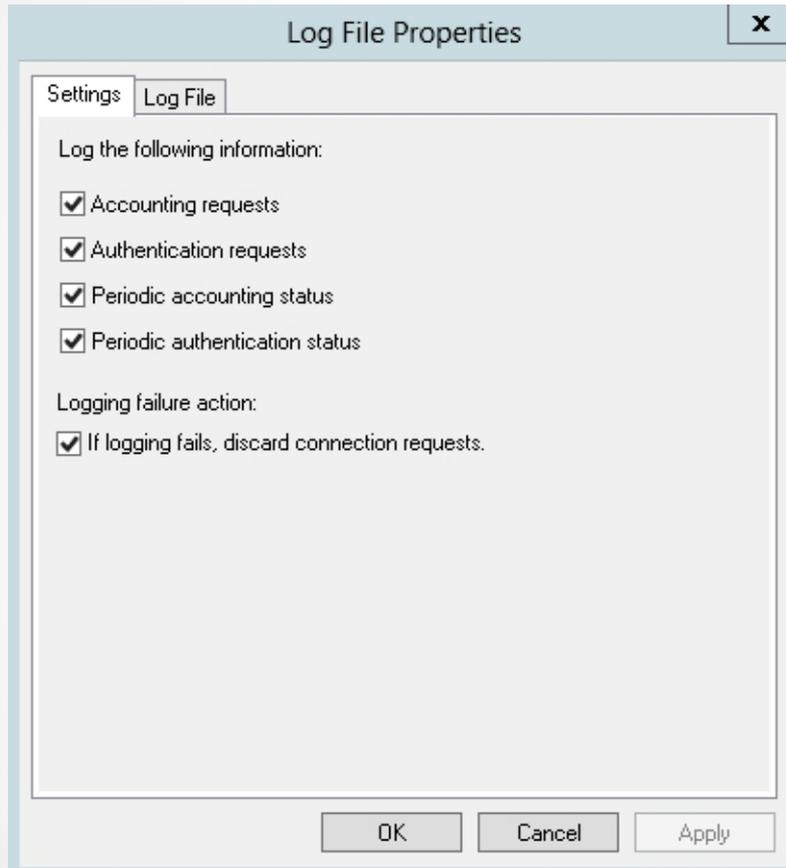
- If logging fails, discard connection requests.

To continue, click Next.

At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Configuring local file logging

Log File Properties



Configuring Log File properties

Understanding NPS Authentication Methods

Authentication is usually broken down into the following categories:

- Password-based credentials
- Certificate-based credentials

Using Password-Based Authentication

- The network access server passes the username and password to the NPS server.
- The NPS server verifies the credentials against the user account database.
 - Processed from the most secure (Microsoft Challenge-Handshake Authentication Protocol v2 or MS-CHAPv2) to the least secure (unauthenticated access) of those enabled options.
- For stronger security, use certificate authentication or multi-factor authentication.

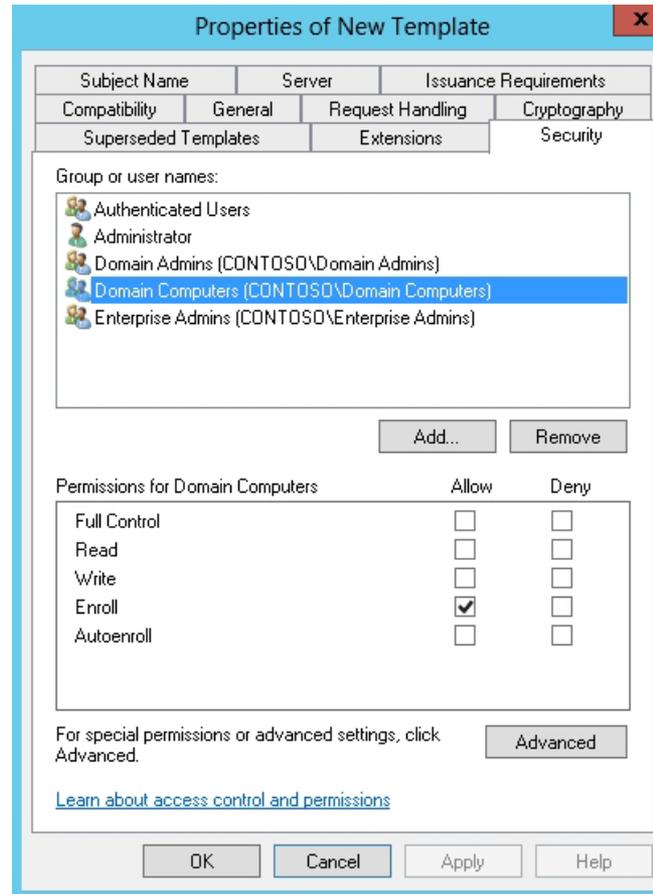
Using Certificates for Authentication

- Much stronger than password-based authentication methods
- Certificates are:
 - Customized using certificate templates
 - Issued using a Certificate Authority
- If smart cards are used, certificates must include:
 - Smart Card Logon purpose
 - Client Authentication purpose

Using Certificates for Authentication

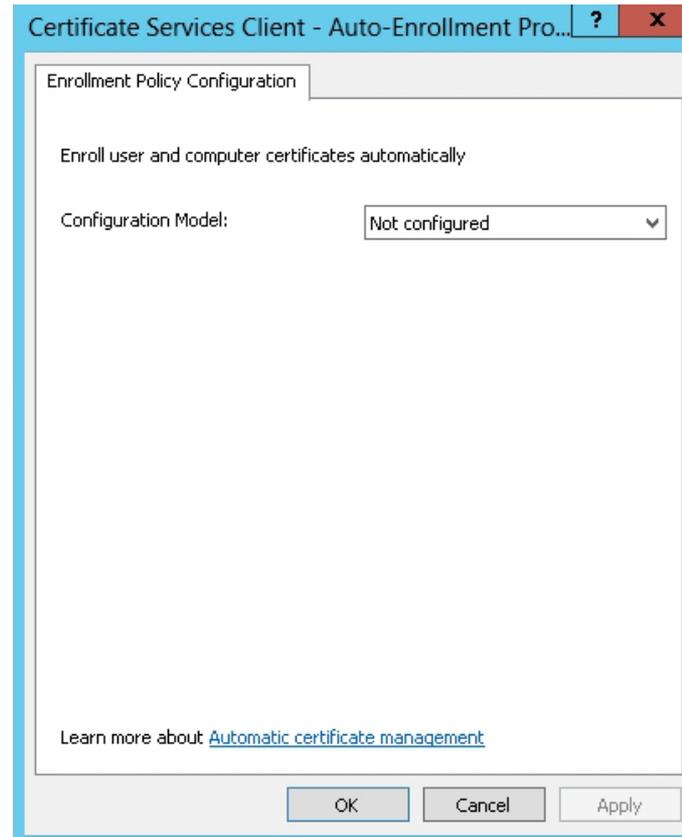
- Digital certificate required and NPS server must use a server certificate for:
 - Protected Extensible Authentication Protocol Microsoft Challenge-Handshake Authentication Protocol v2 (PEAP-MS-CHAP v2)
 - Protected Extensible Authentication Protocol Transport Layer Security (PEAP-TLS)
 - Extensible Authentication Protocol Transport Layer Security (EAP-TLS)

Automatically Add Workstation Authentication Certificates to All Workstations



Configuring security for a template

Automatically Add Workstation Authentication Certificates to All Workstations



Configuring user and computer certificate—
Auto-Enrollment

Lesson Summary

- Microsoft's RADIUS server is Network Policy Server (NPS).
- By installing and configuring RADIUS, you can create and enforce wide network access policies for client health, connection request authentication, and connection request authorization.
- When you implement RADIUS, Windows Server 2012 computers running Routing and Remote Access and/or wireless access points can forward access requests to a single RADIUS server.
- Installing NPS is a simple process, which is done with Server Manager. After NPS is installed, you use the Network Policy Server console to configure NPS.

Lesson Summary

- With multiple RADIUS servers, you can configure RADIUS clients to use a primary RADIUS server and alternate RADIUS servers. If the primary RADIUS server becomes unavailable, the request is sent to the alternate RADIUS server.
- Much like the use of other templates, RADIUS templates are designed to reduce the amount of time and cost that it takes to configure RADIUS on one or more servers.
- Creating a RADIUS template does not affect the functionality of NPS. It affects the RADIUS server only when the template is selected and applied when configuring NPS.
- NPS supports RADIUS accounting, which you can use to track network usage for auditing and billing purposes.
- Using certificates with the NPS provides strong security for authenticating users and computers and eliminates the need for less secure password-based authentication methods.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.