Lesson 12: Configuring a Network Policy Server

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

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

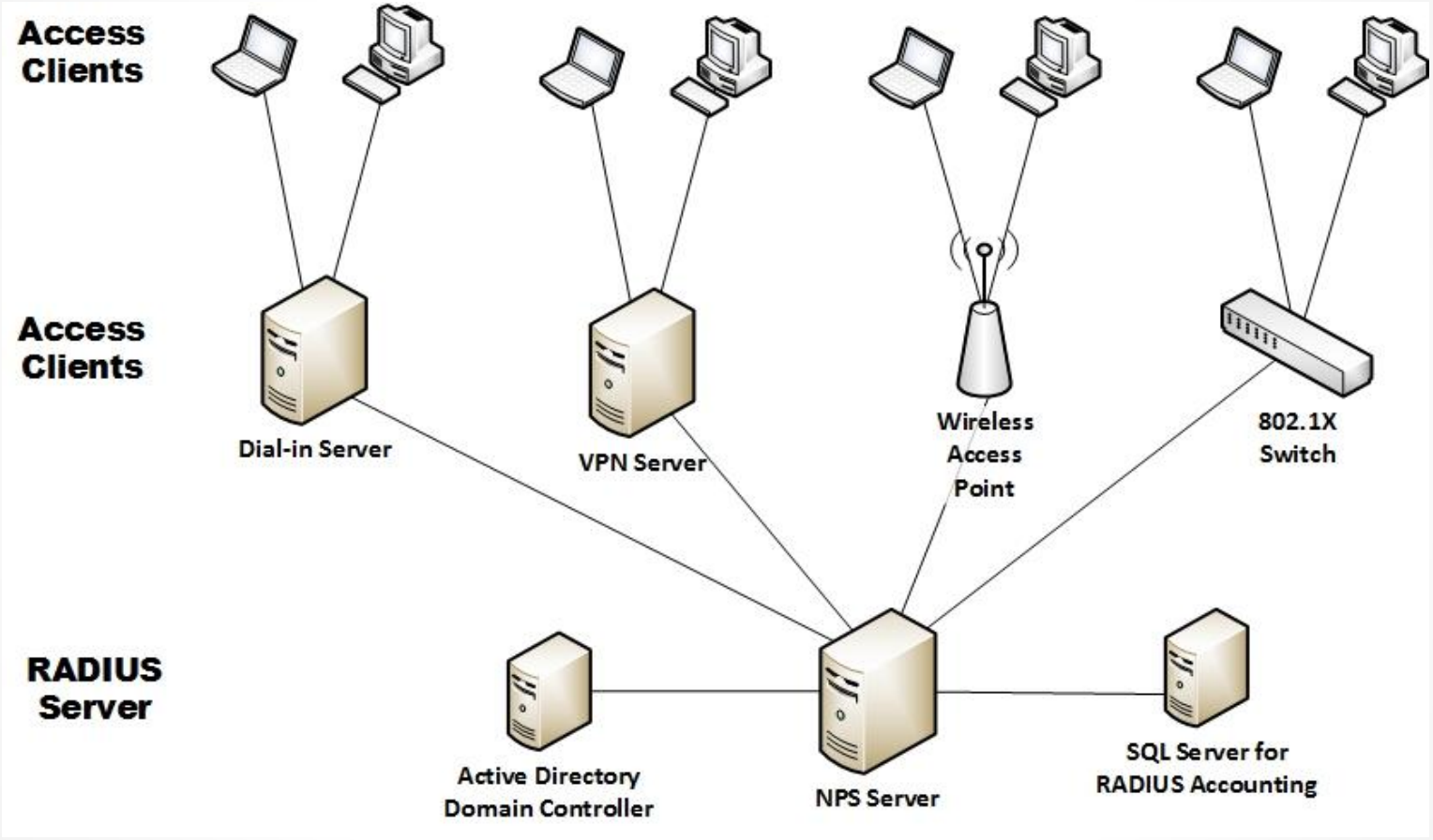
Network Policy Server (NPS): Microsoft's RADIUS server.

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:

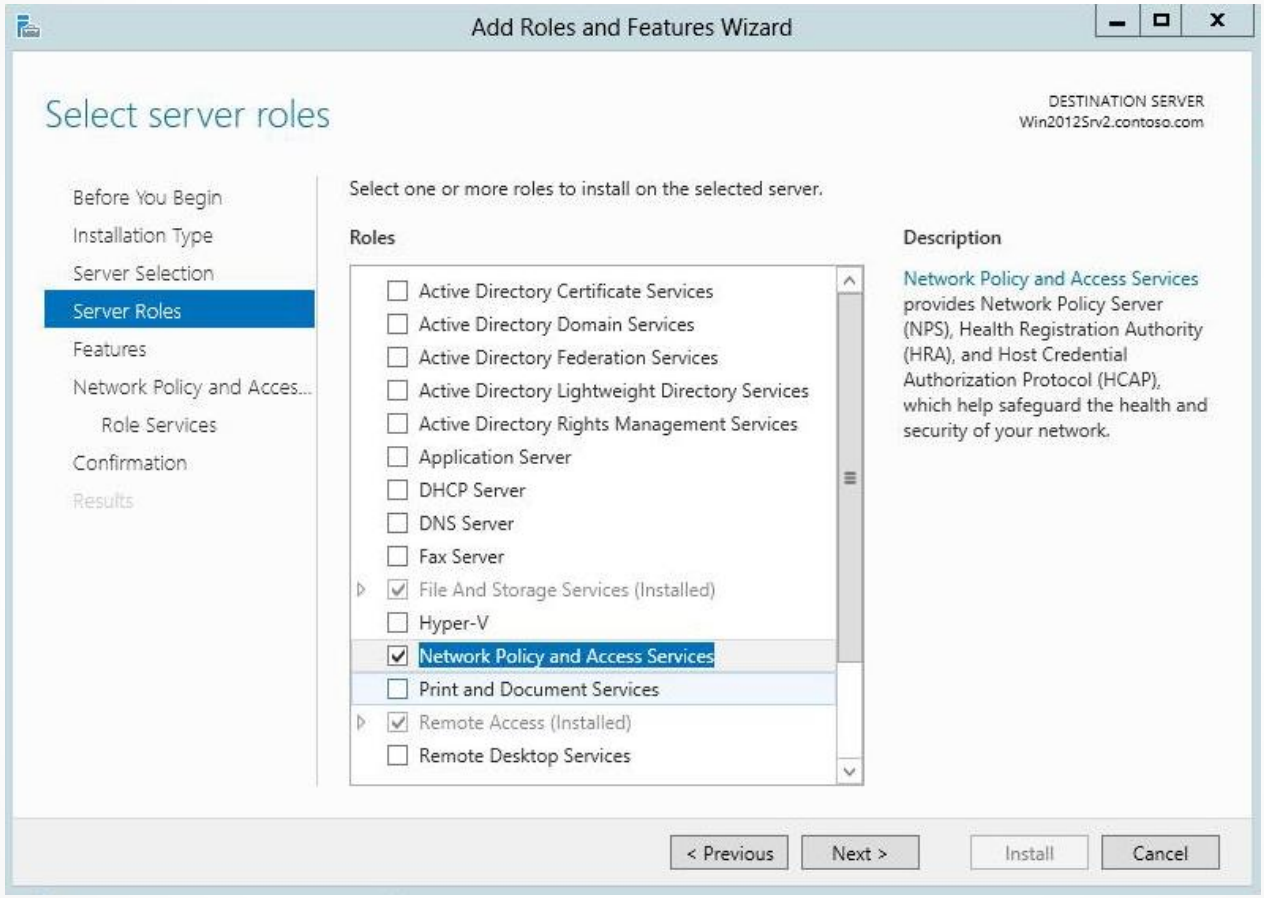
1. When an access client accesses a VPN server or wireless access point, a connection request is created that is sent to the NPS server.
2. The NPS server evaluates the Access-Request message.
3. If required, the NPS server sends an Access-Challenge message to the access server. The access server processes 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.):

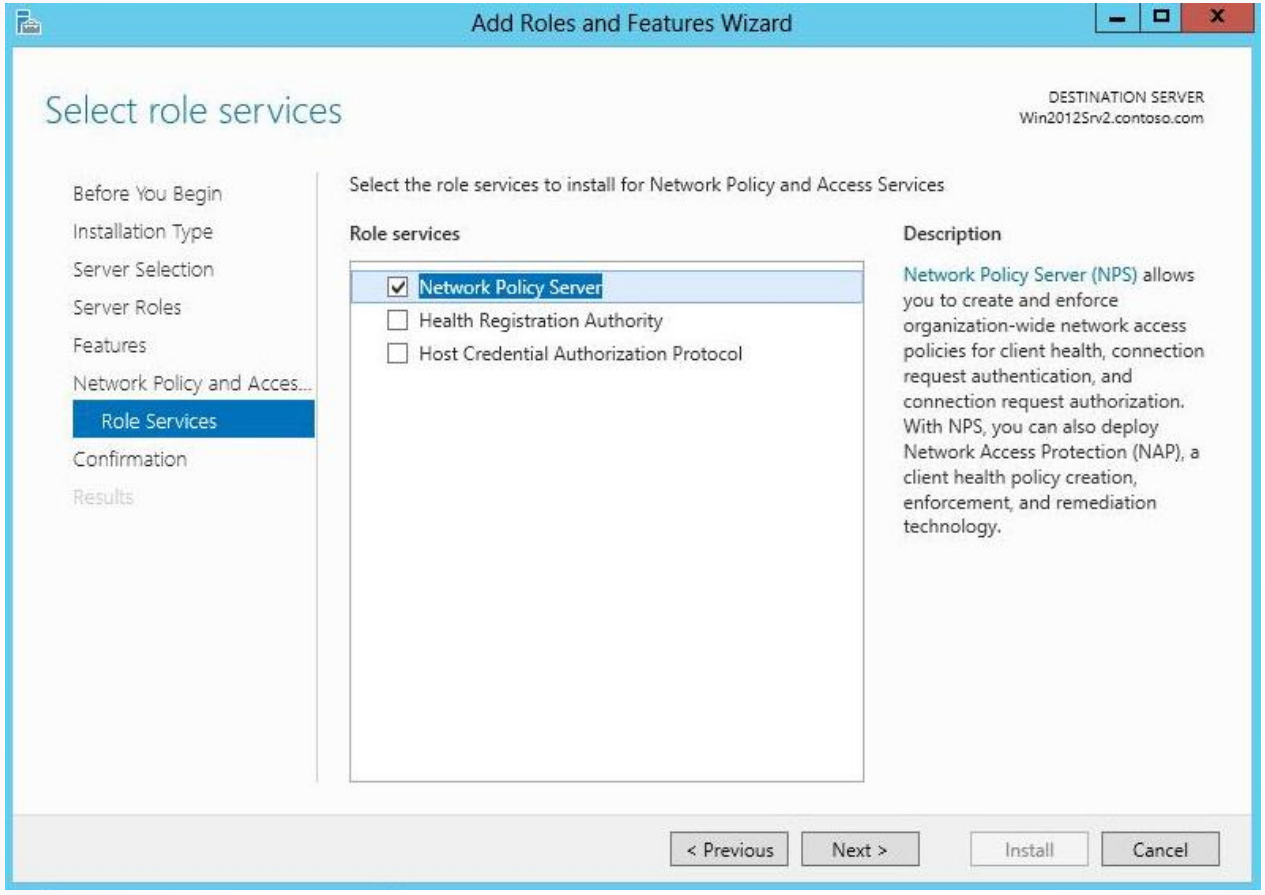
5. When the connection attempt is authorized with both the dial-in properties of the user account and network policies, the NPS server sends an Access-Accept message to the access server. If the connection attempt is either not authenticated or not authorized, the NPS server sends an Access-Reject message 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



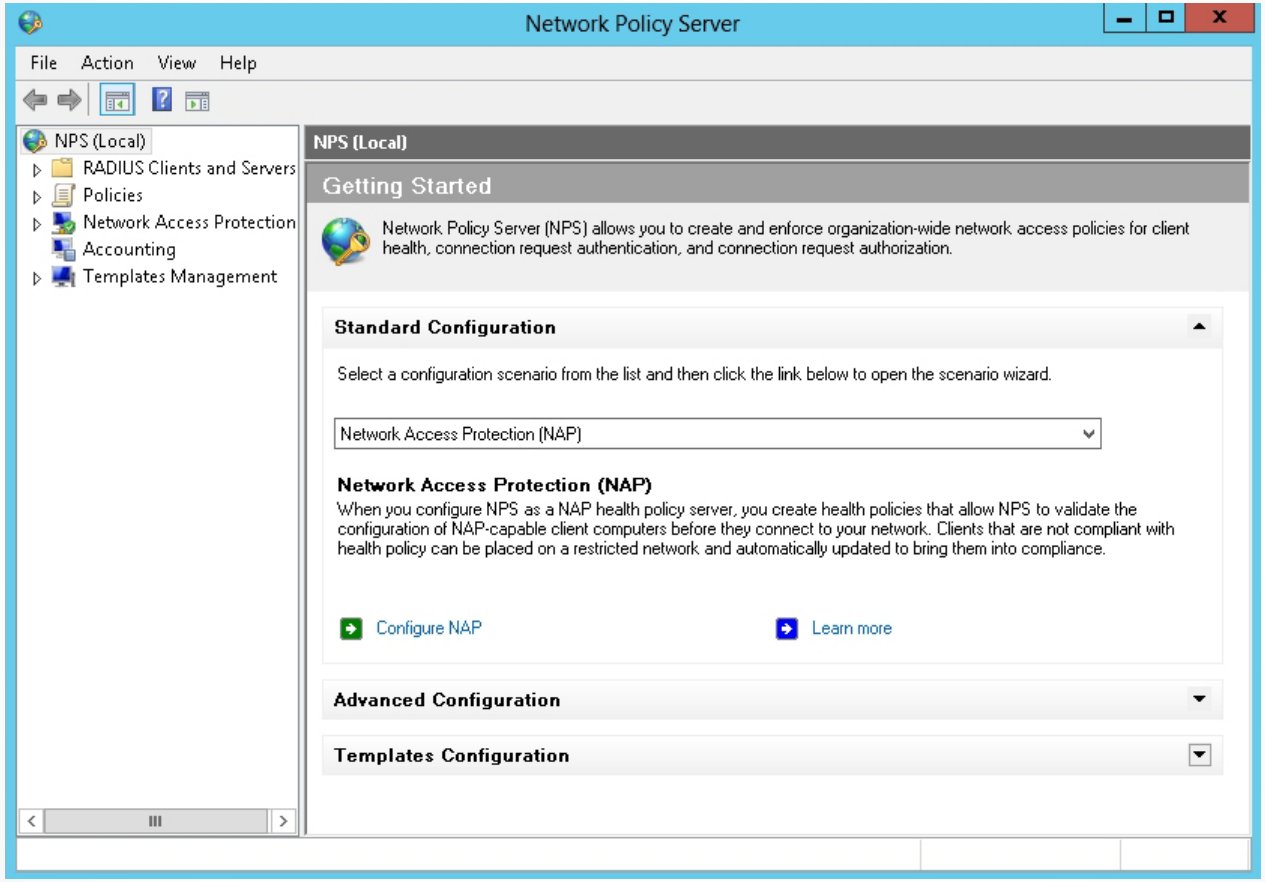
Installing Network Policy and Access Services

Installing Network Policy Server



Selecting Network Policy and Access Service Role Services

Installing Network Policy Server



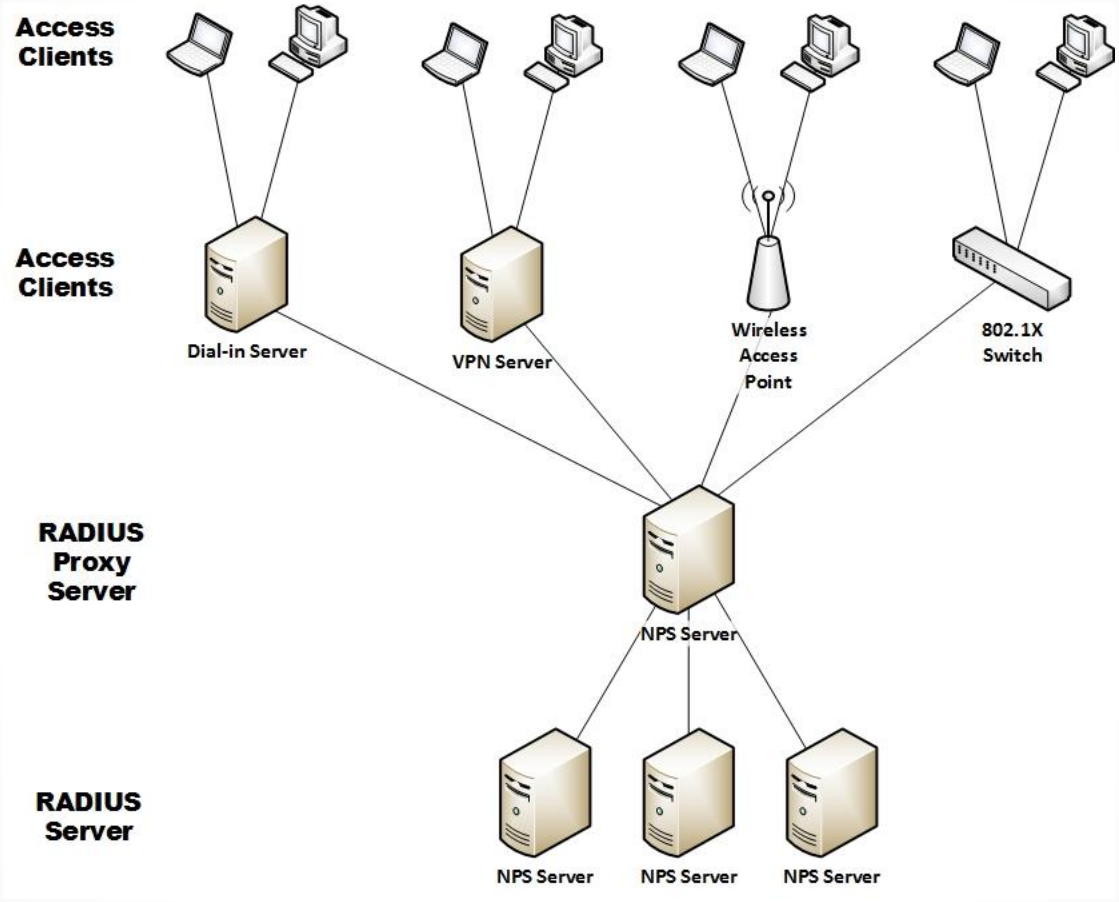
Opening the Network Policy Server console

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



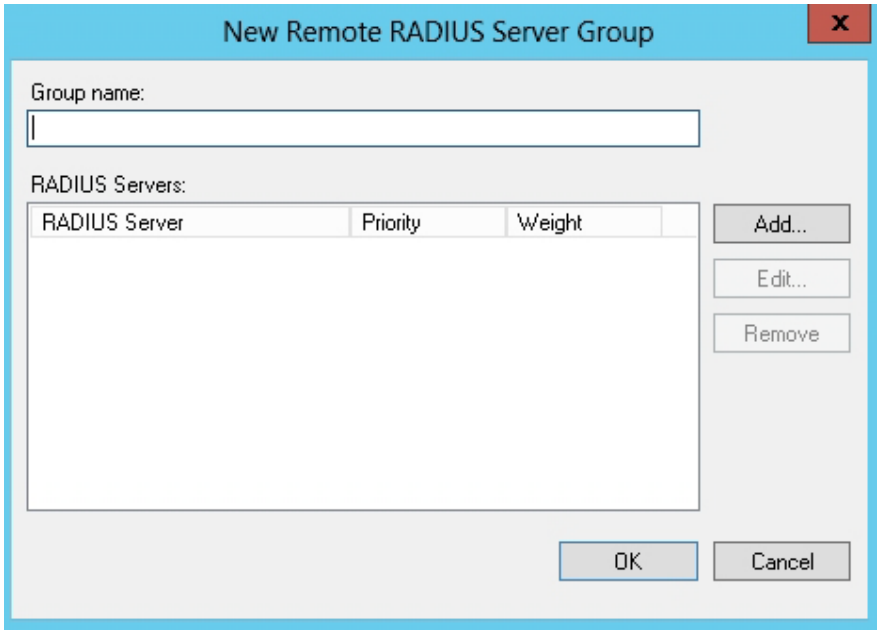
Using a RADIUS proxy server

Configuring RADIUS Server Infrastructures

Load balancing options:

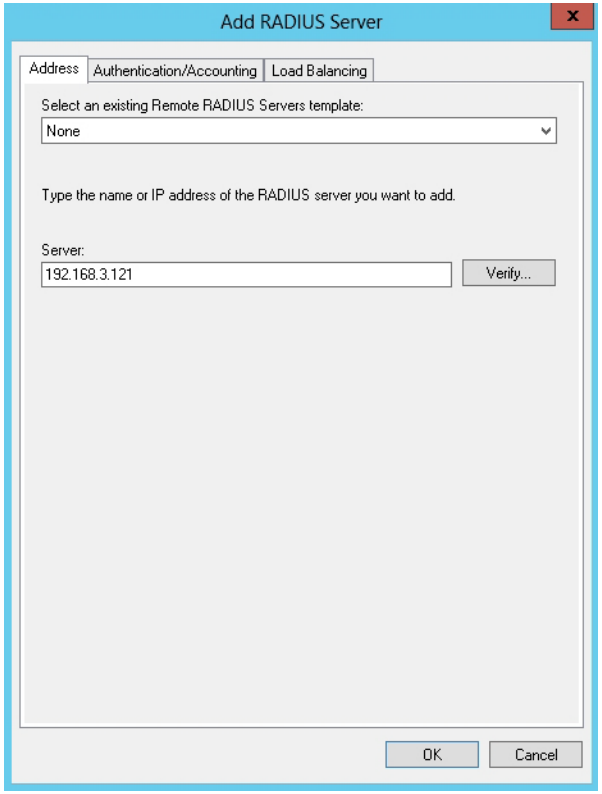
- Priority
- Weight
- Advanced settings

Add a Remote RADIUS Server Group



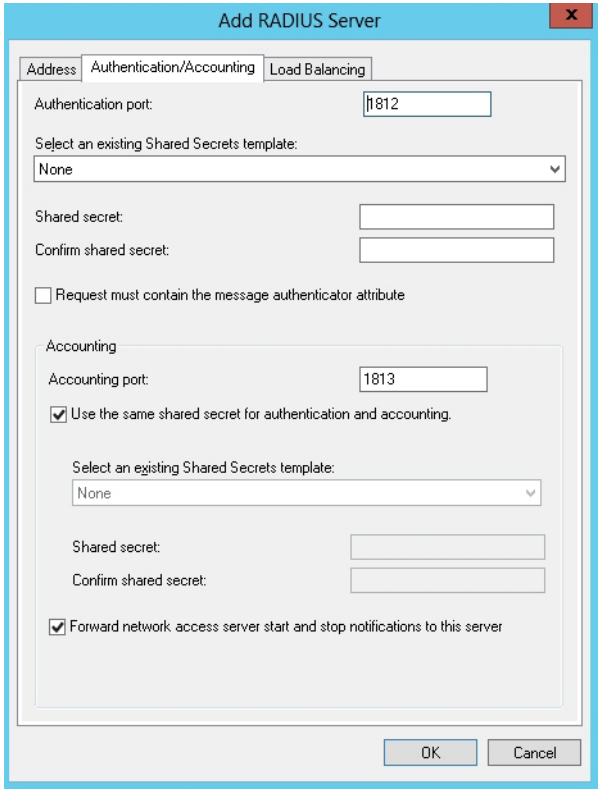
Creating a new RADIUS server group

Add a Remote RADIUS Server Group



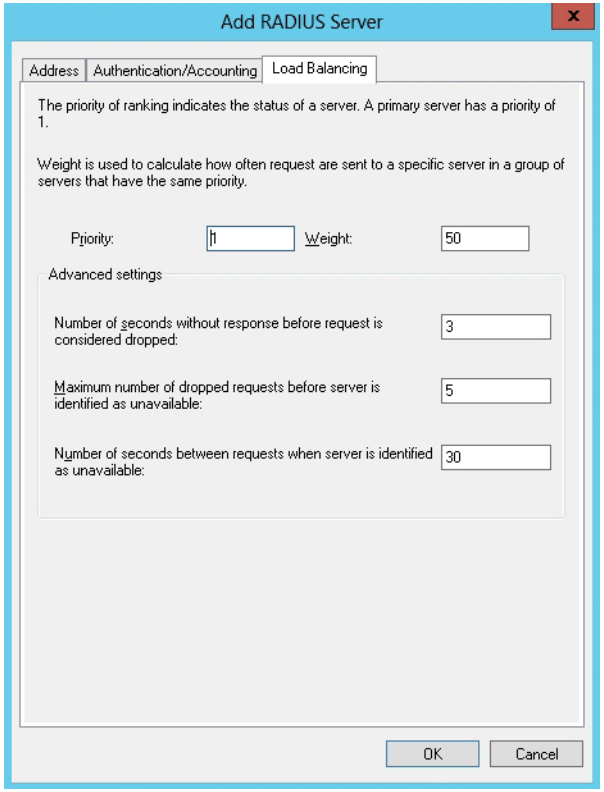
Adding a RADIUS server to the RADIUS server group

Add a Remote RADIUS Server Group



Configuring Authentication and Accounting RADIUS

Add a Remote RADIUS Server Group



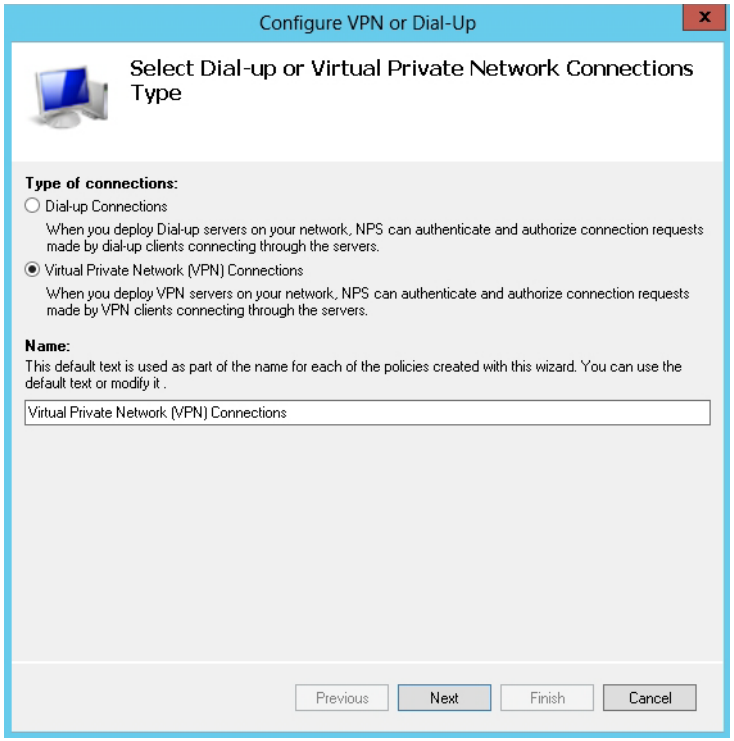
Configuring RADIUS load balancing

Configuring RADIUS Clients

The standard configuration includes:

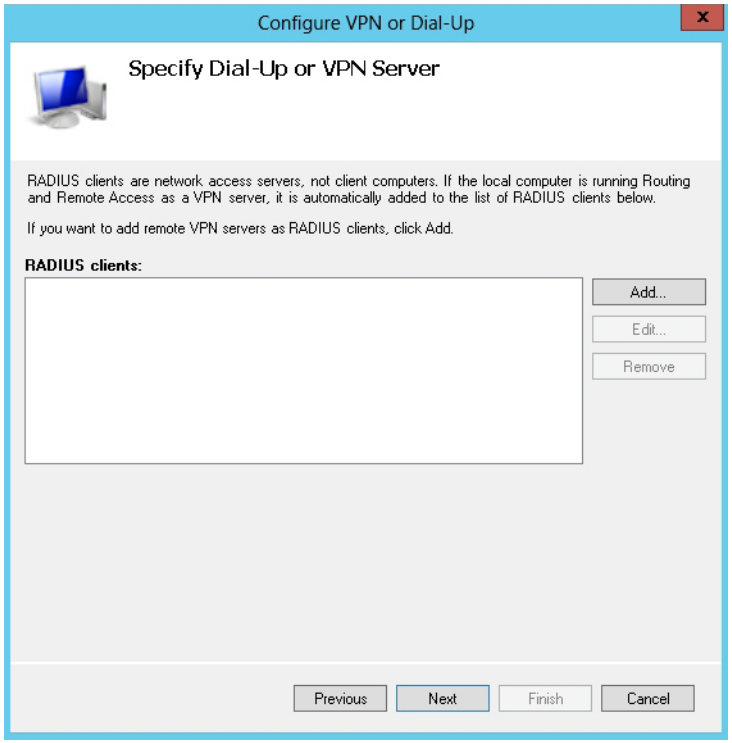
- RADIUS server for dial-up or VPN connections
- RADIUS server for 802.1X wireless or wired connections
- NAP policy server (discussed in Lesson 14)

Configure NPS for RADIUS Server for VPN Connections



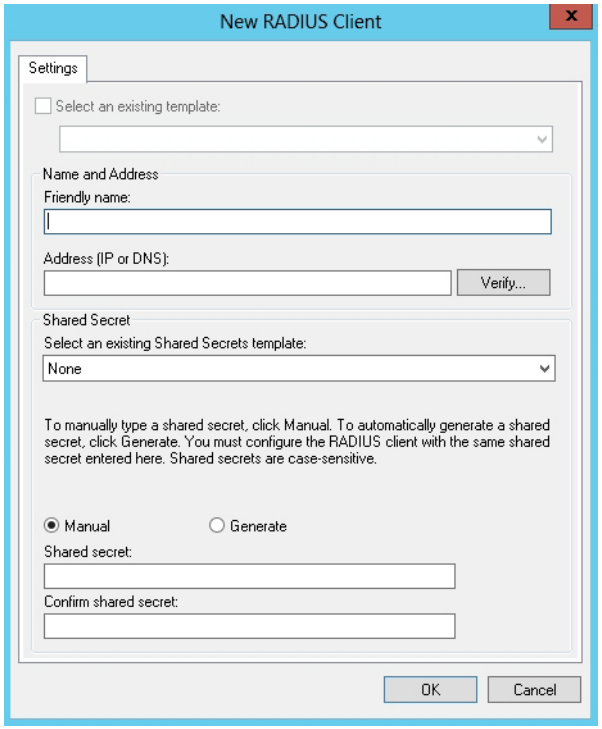
Specifying connections on the Dial-up or Virtual Private Network Connections Type page

Configure NPS for RADIUS Server for VPN Connections



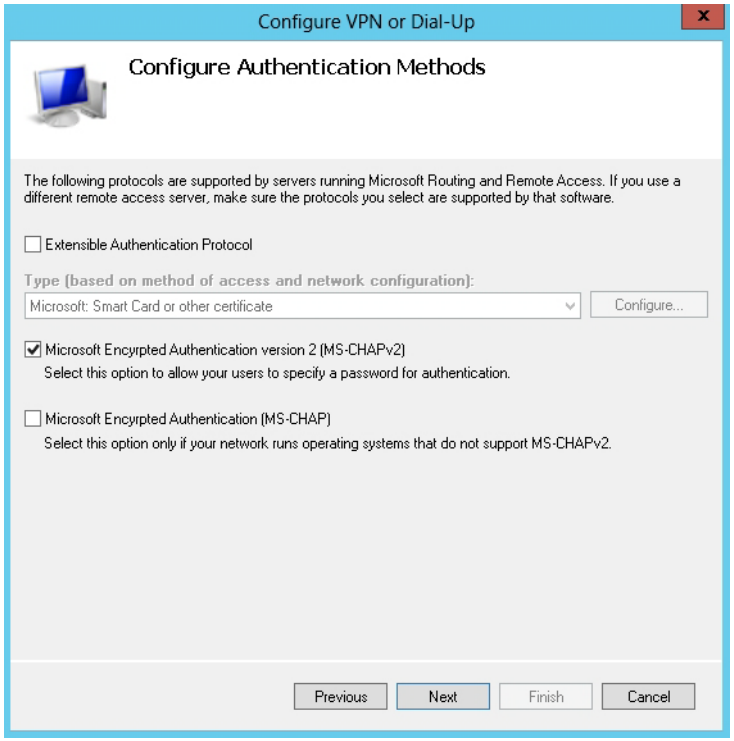
Showing the RADIUS clients page

Configure NPS for RADIUS Server for VPN Connections



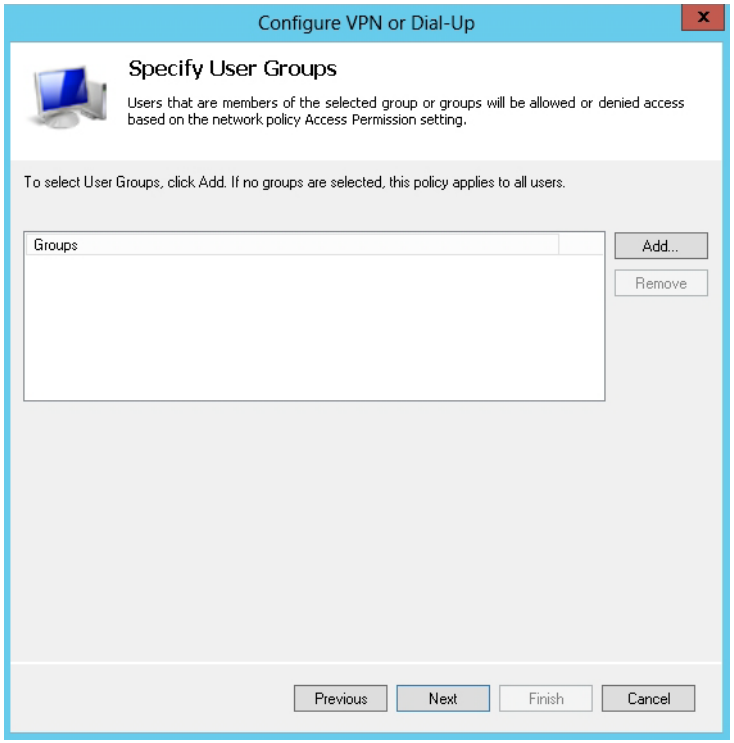
Adding RADIUS clients

Configure NPS for RADIUS Server for VPN Connections



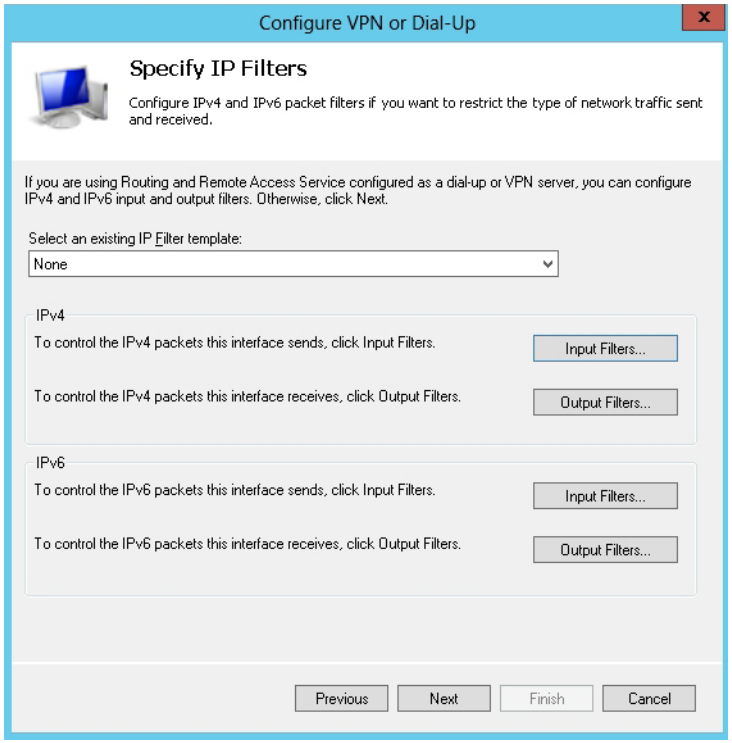
Specifying authentication methods

Configure NPS for RADIUS Server for VPN Connections



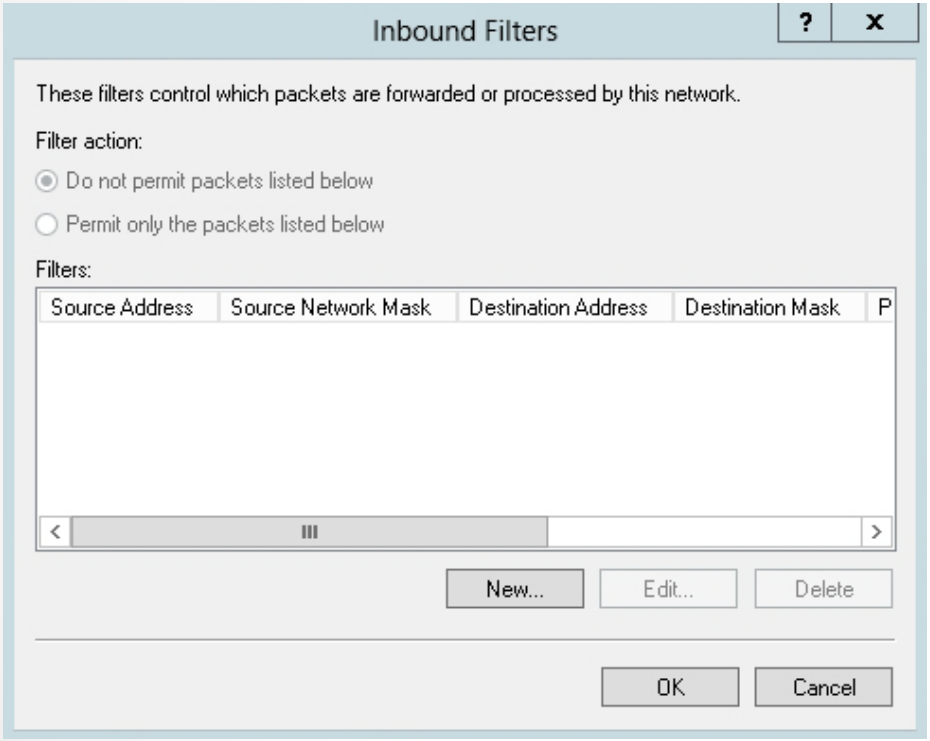
Specifying user groups

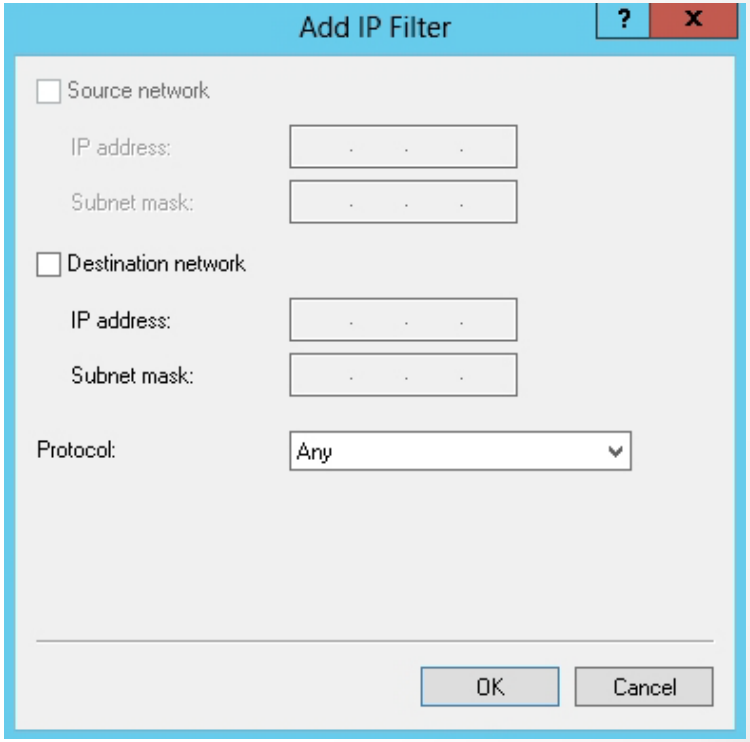
Configure NPS for RADIUS Server for VPN Connections



Specifying IP filters

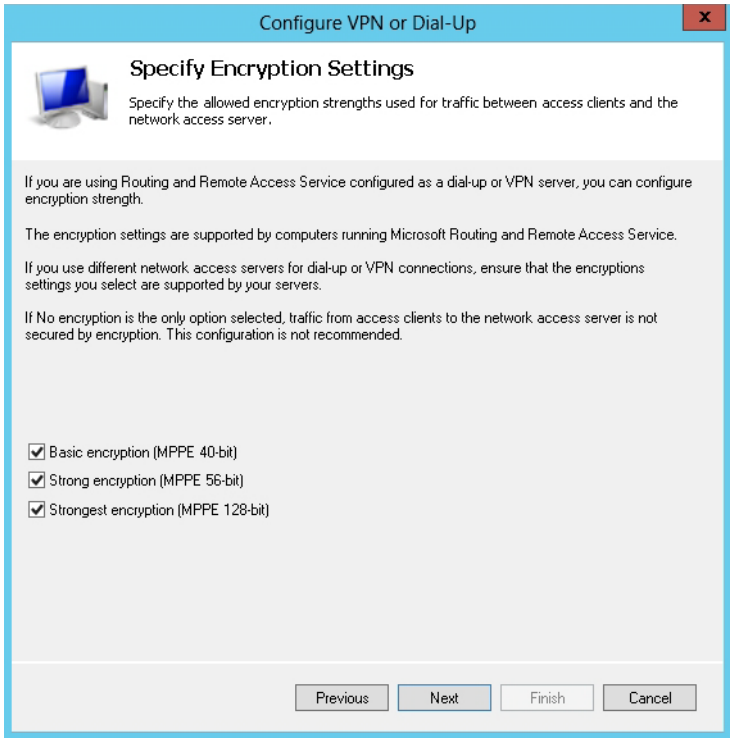
Configure NPS for RADIUS Server for VPN Connections





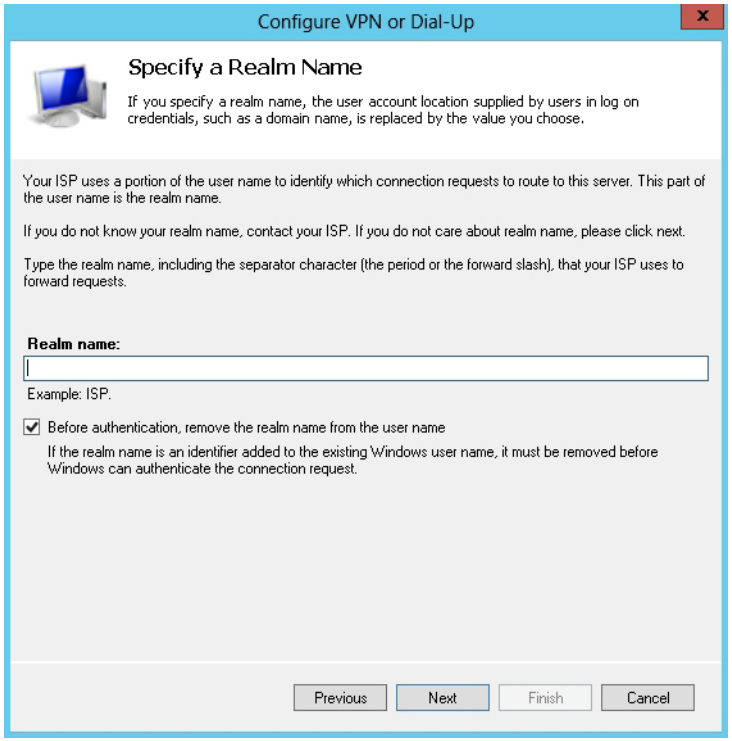
Configuring inbound filters

Configure NPS for RADIUS Server for VPN Connections



Specifying encryption settings

Configure NPS for RADIUS Server for VPN Connections

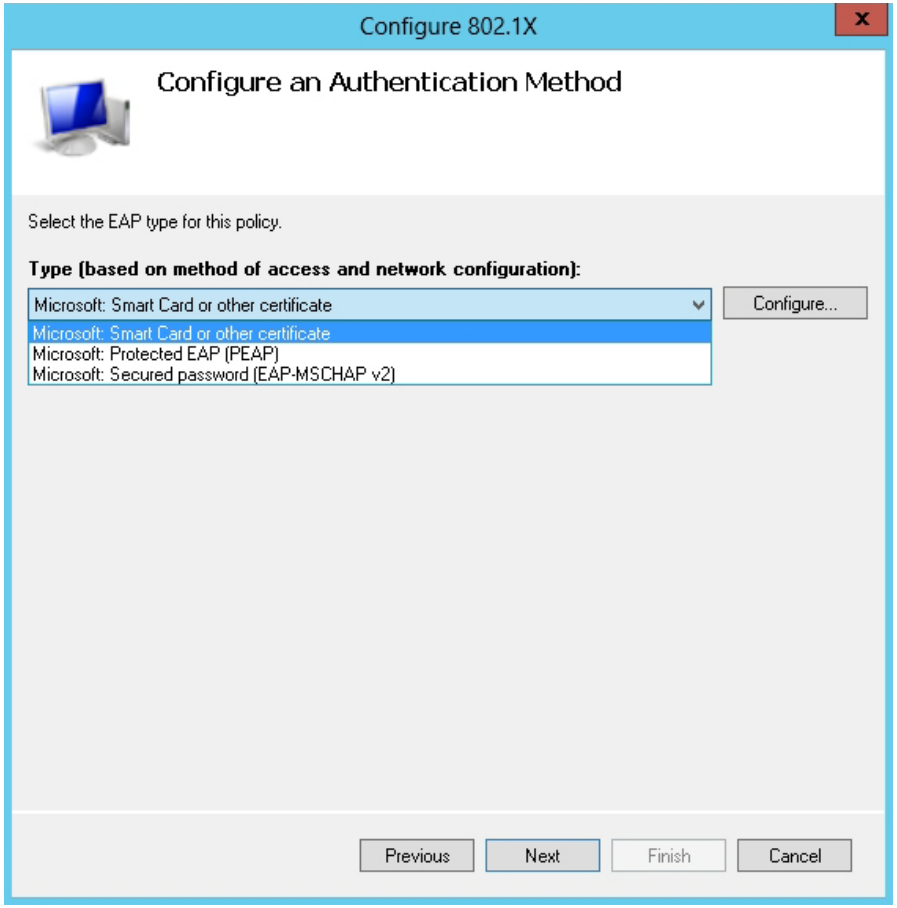


Specifying a realm name

Configure NPS for 802.1X Wireless Connections

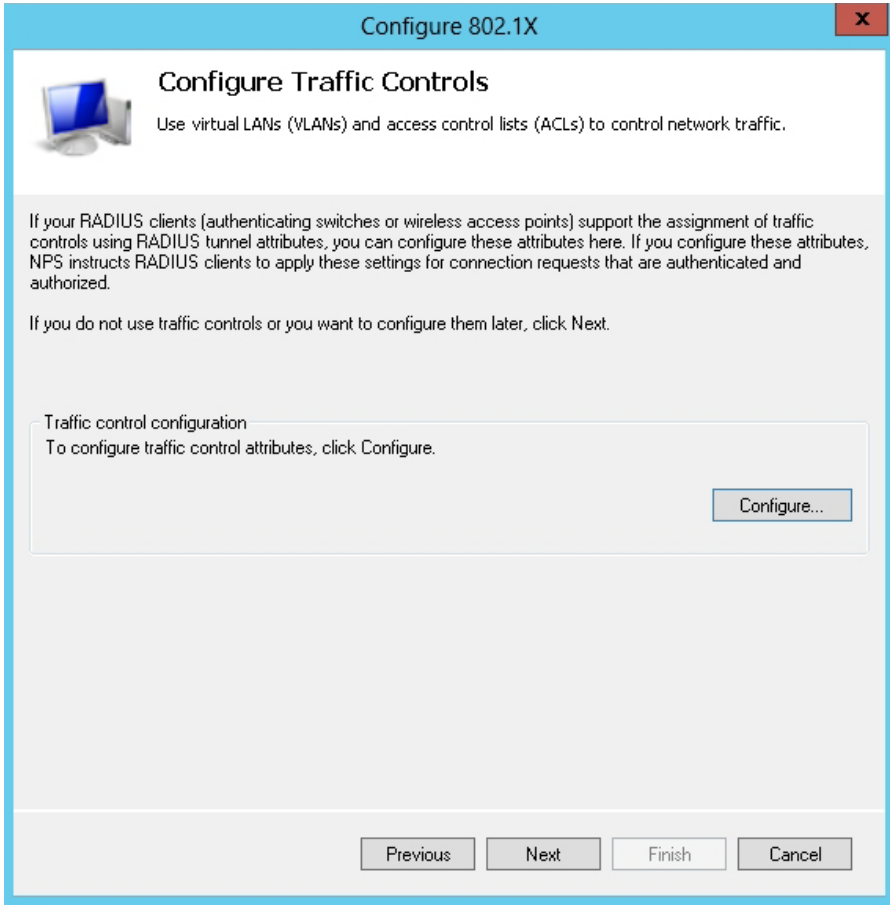
Selecting the 802.1X connections type

Configure NPS for 802.1X Wireless Connections



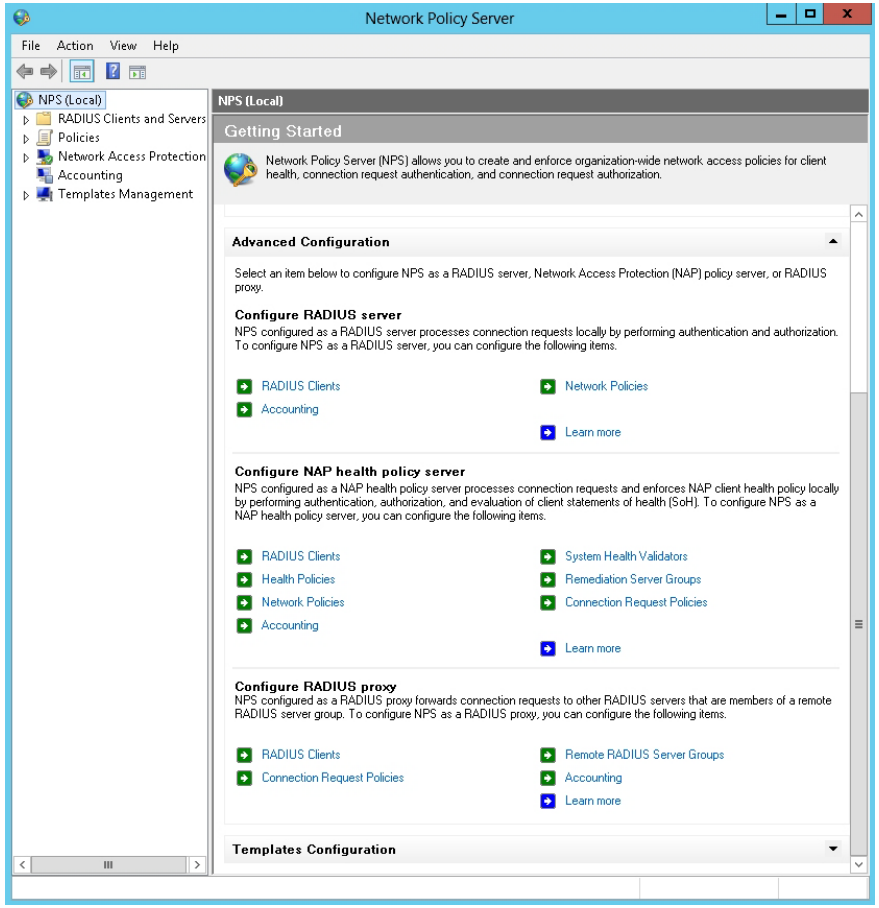
Configuring authentication methods for 802.1X

Configure NPS for 802.1X Wireless Connections

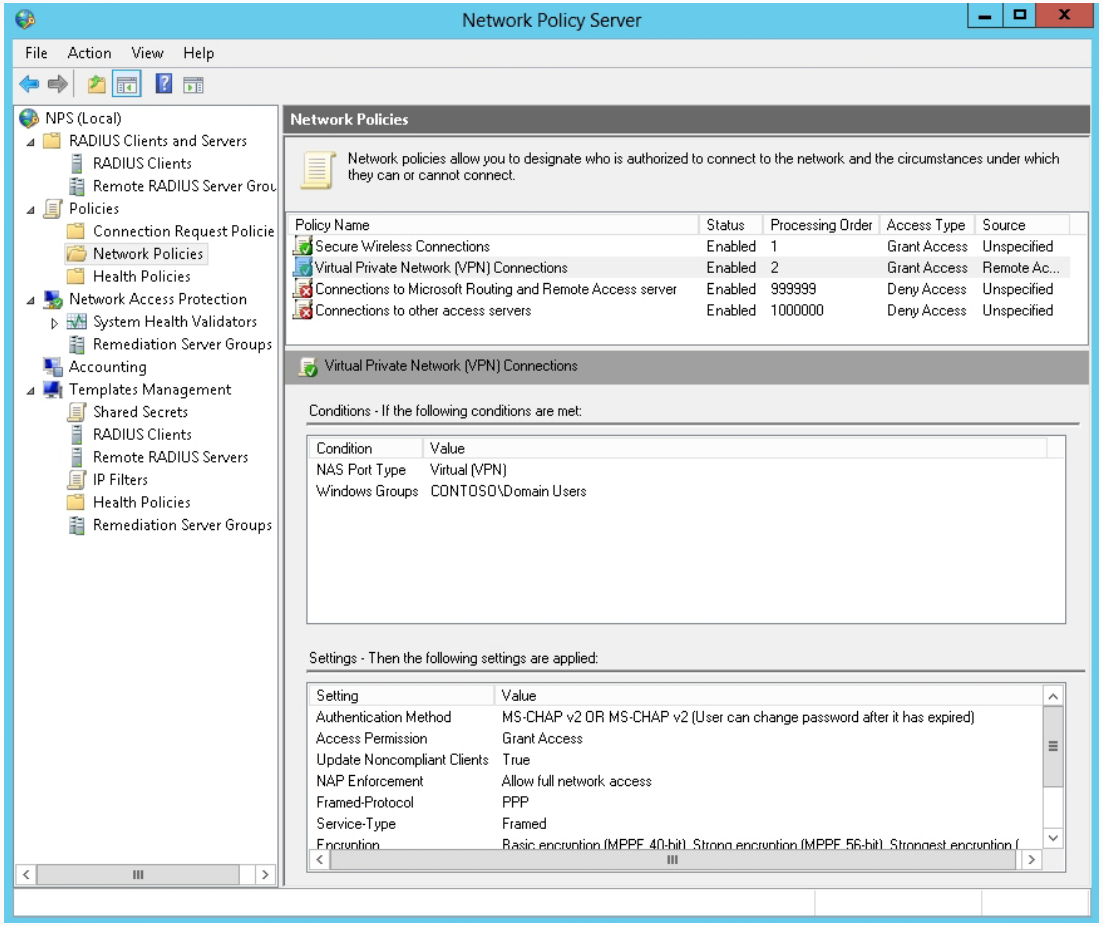


Configuring traffic controls

NPS Advanced Configuration



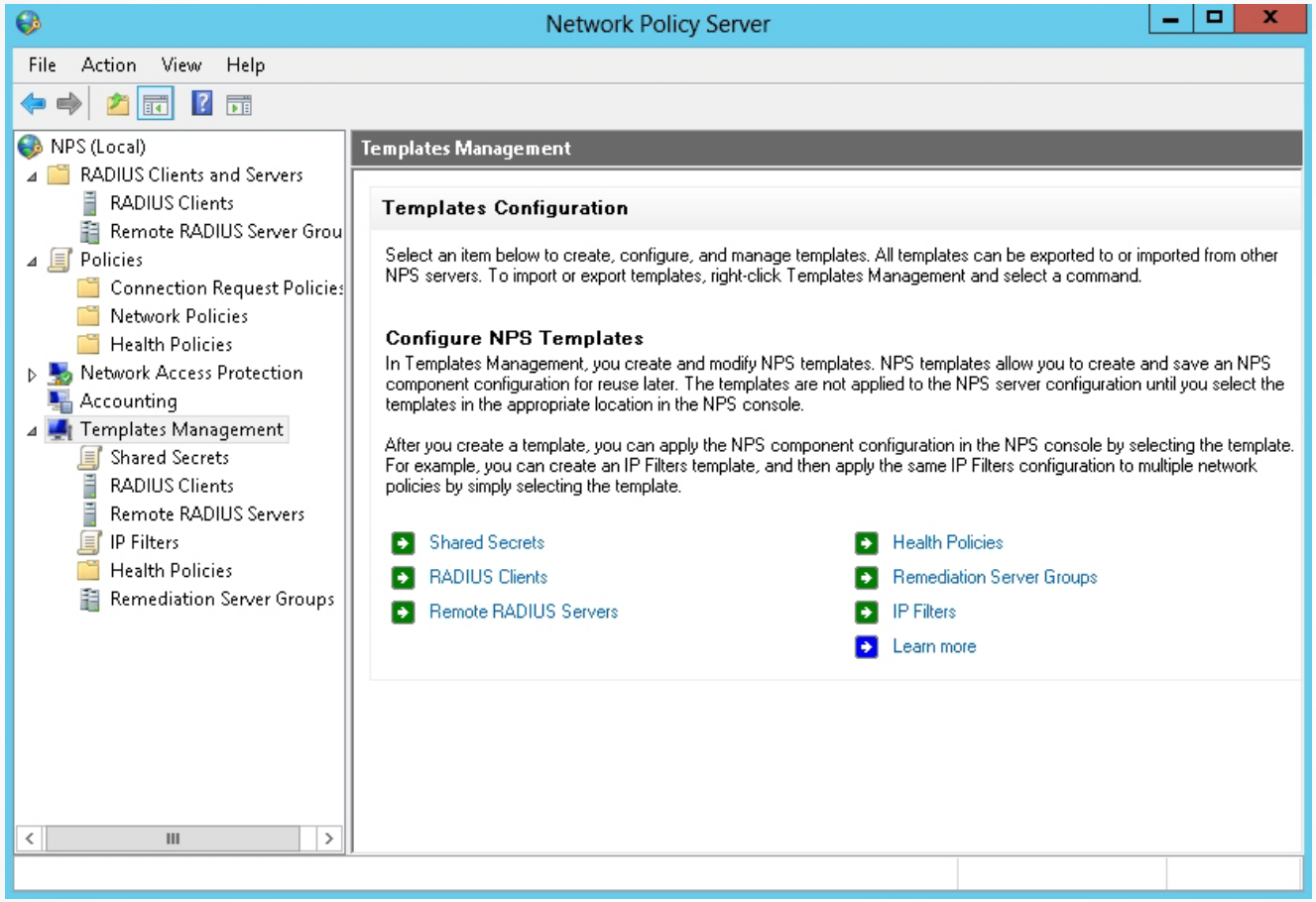
Network Policies



Managing RADIUS Templates

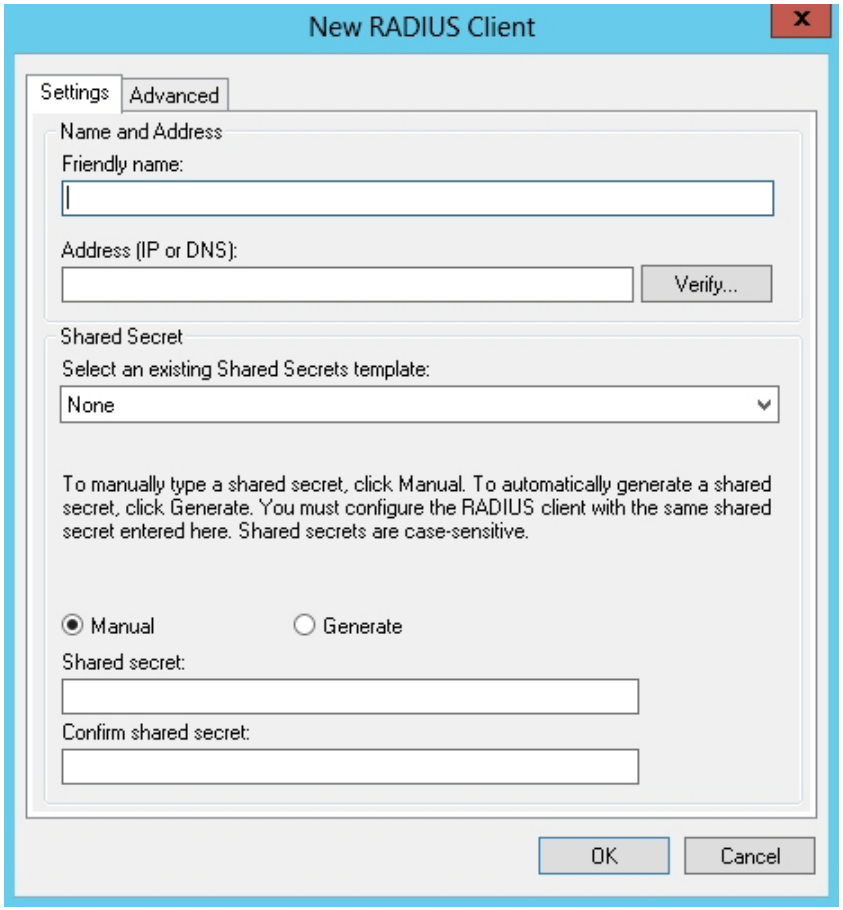
- RADIUS templates:
  - Are designed to reduce the amount of time and cost that it takes to configure RADIUS on one or more servers
- Creating a RADIUS template does not affect the functionality of NPS.
- A RADIUS template affects only the NPS server when the template is selected and applied when configuring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

Managing RADIUS Templates



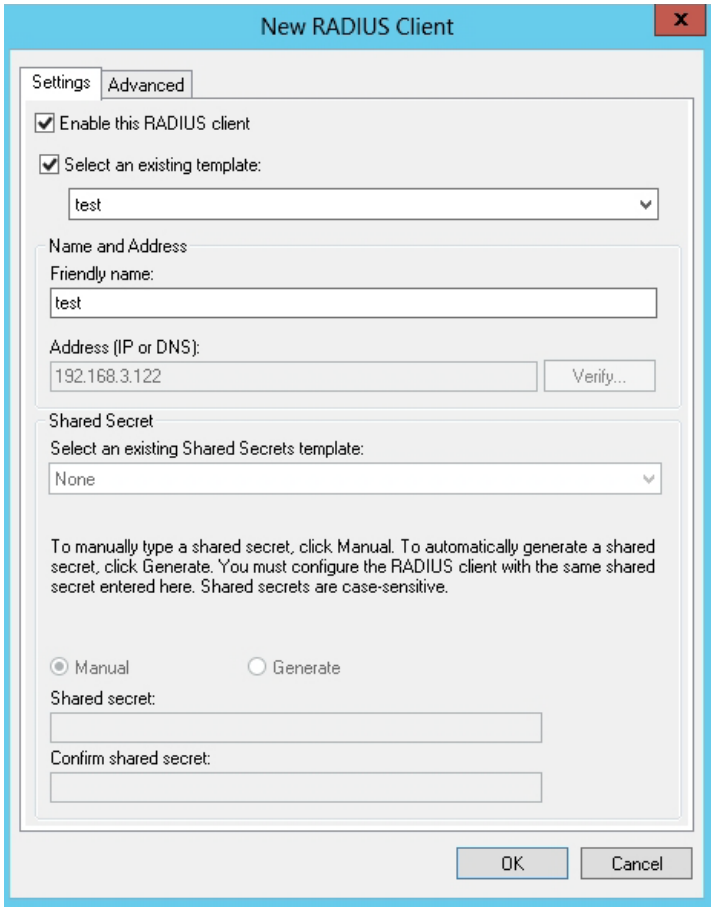
Templates Configuration options
in the NPS console

Managing RADIUS Templates



Creating a RADIUS client template

Managing RADIUS Templates

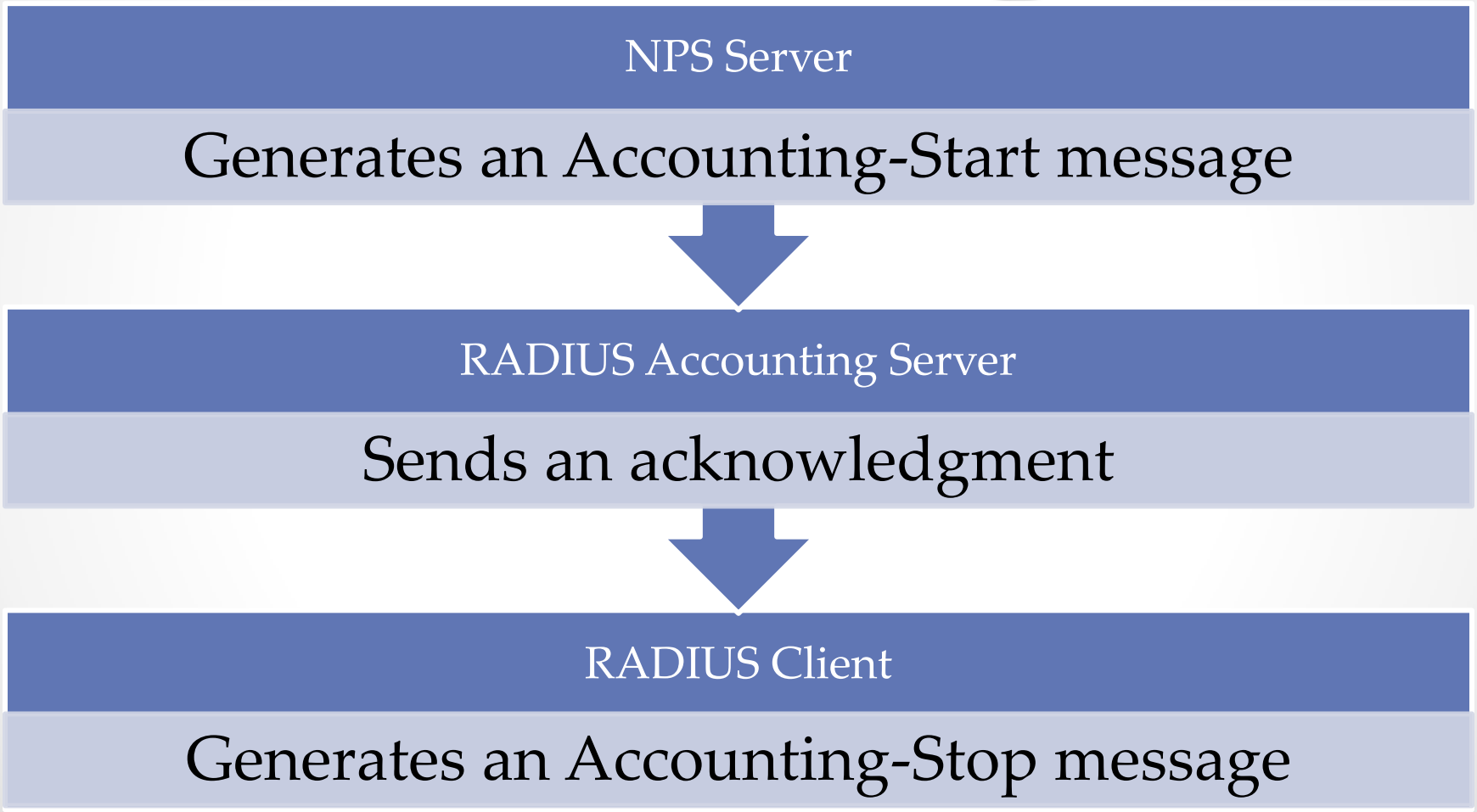


Using the RADIUS client template

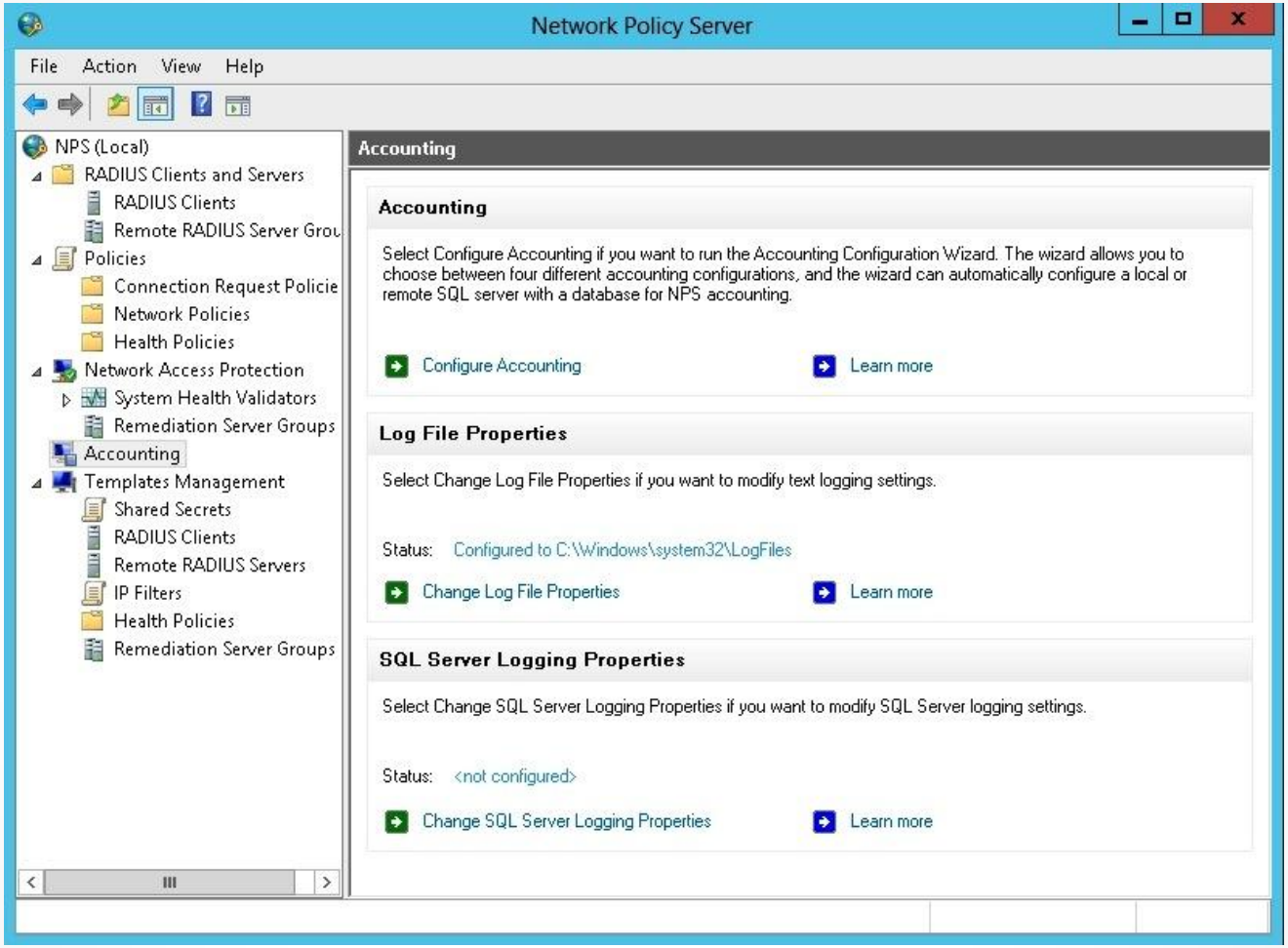
Configuring RADIUS Accounting

- 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

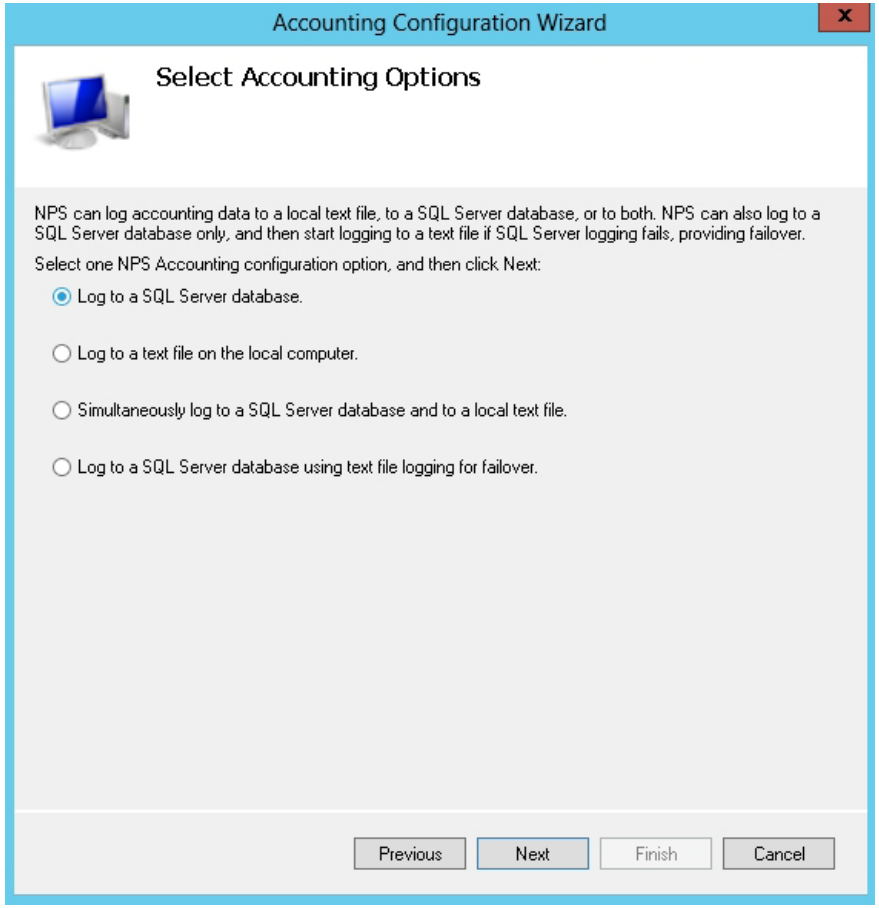


To Enable and Configure Accounting in NPS



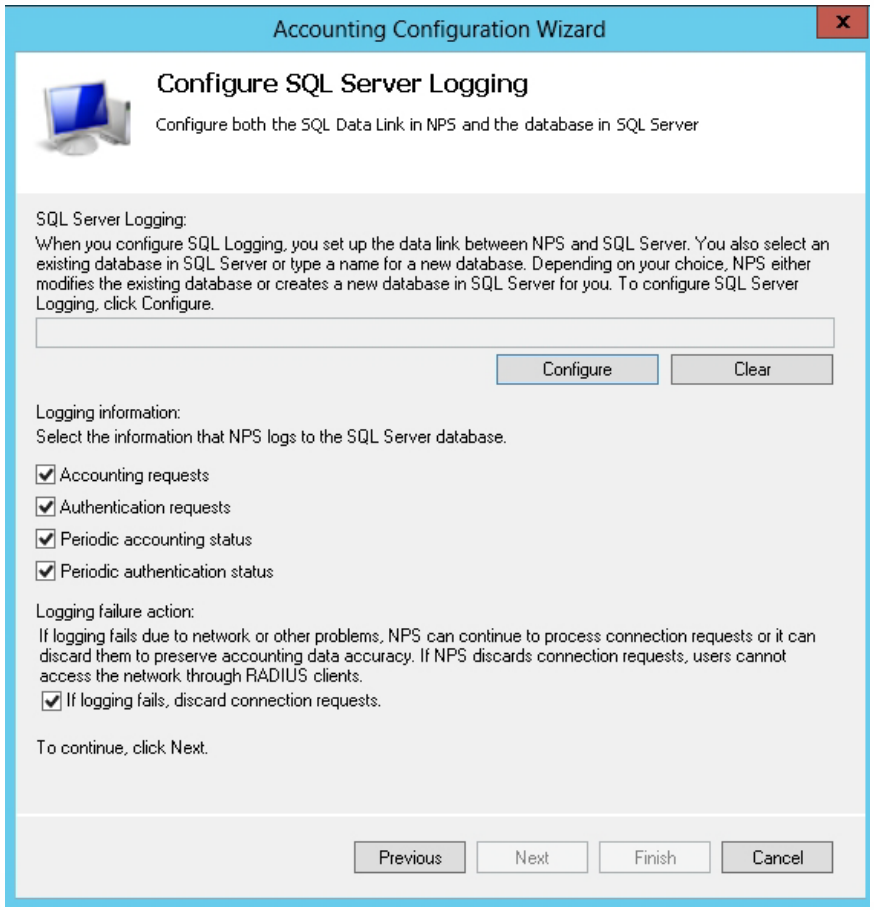
Accounting configuring options

To Enable and Configure Accounting in NPS



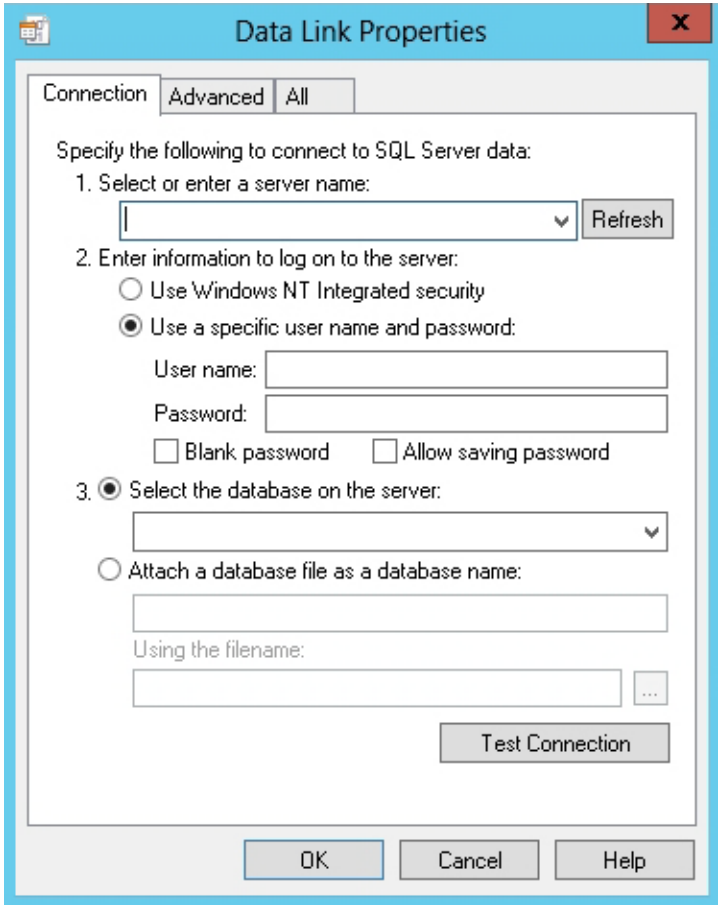
Selecting Accounting options

To Enable and Configure Accounting in NPS



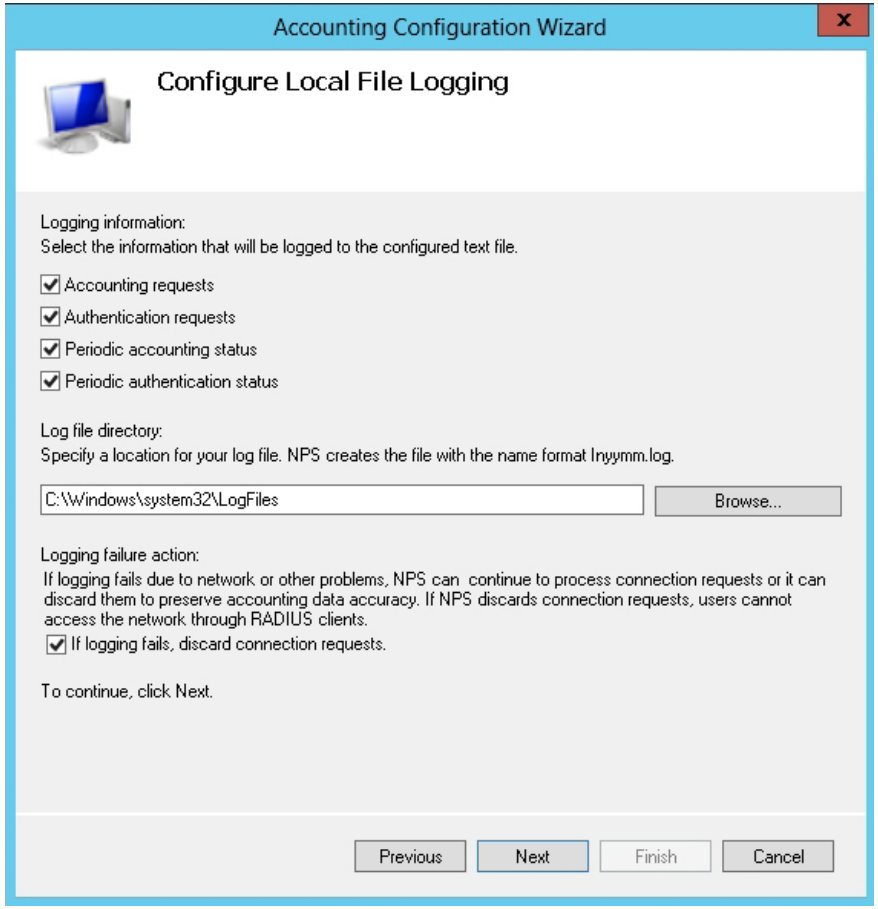
Configuring SQL Server logging

To Enable and Configure Accounting in NPS



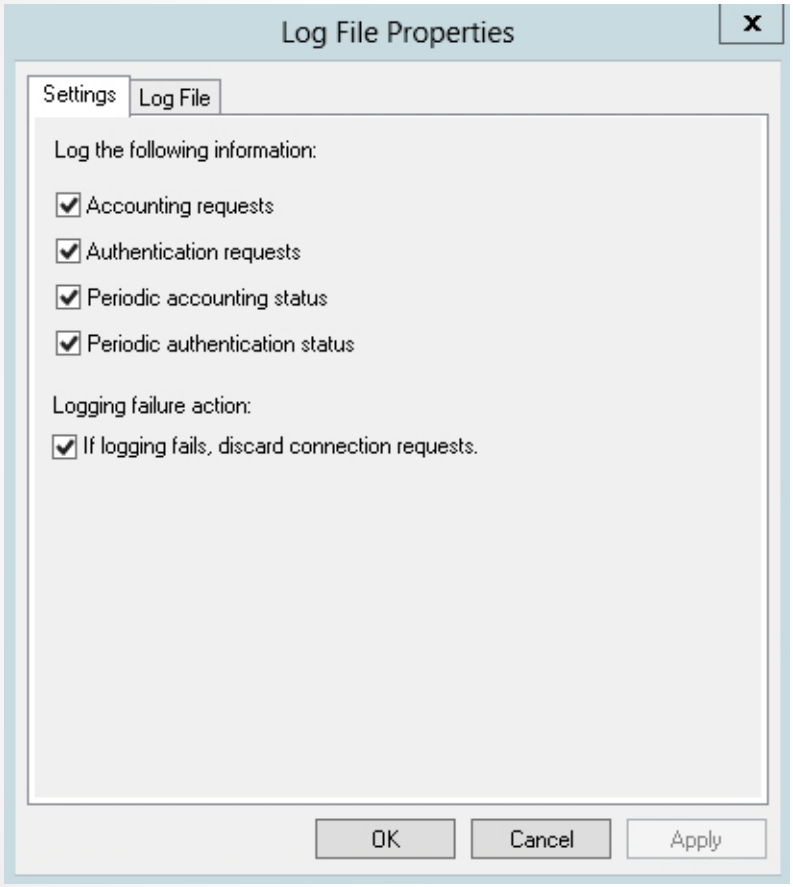
Configuring the Data Link properties

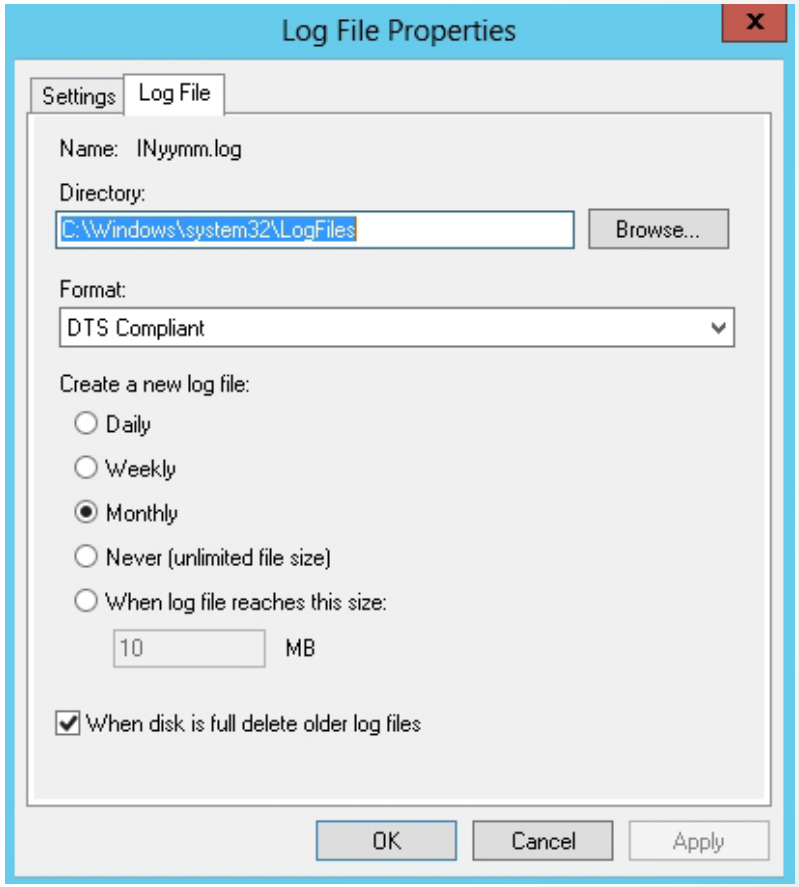
To Enable and Configure Accounting in NPS



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.

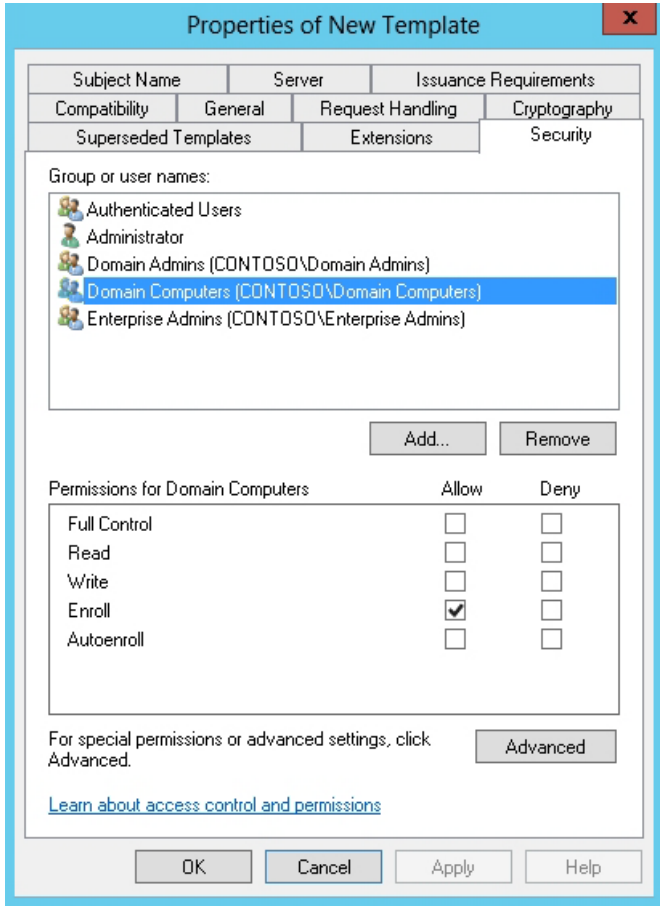
Using Certificates for Authentication

- 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

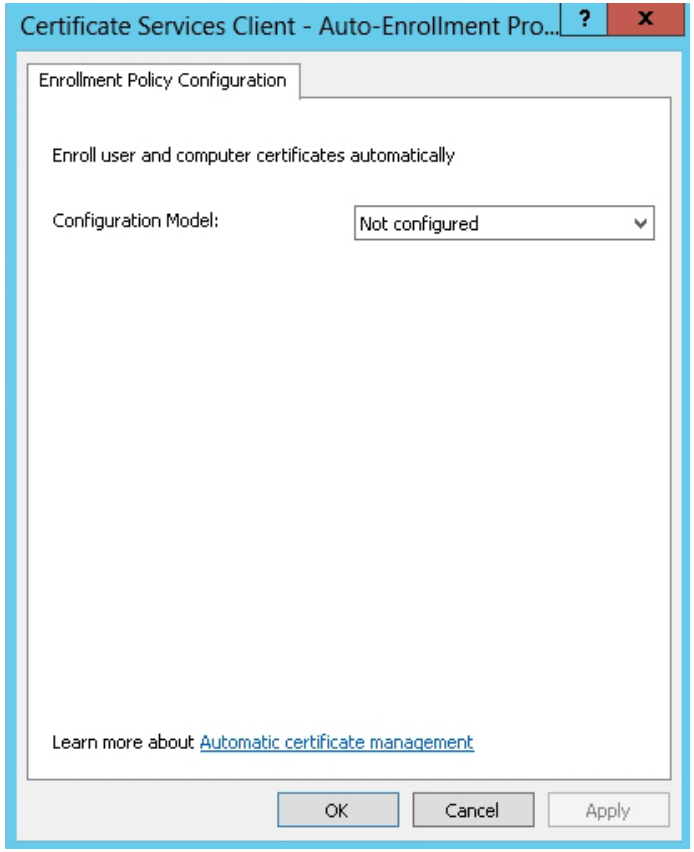
- Digital certificate required and NPS server must use a server certificate for:
  - Protected Extensible Authentication Protocol Microsoft Challenge-Handshake Authentication Protocol v2 (PEAP-MS-CHAP v2)
  - Protected Extensible Authentication Protocol Transport Layer Security (PEAP-TLS)
  - Extensible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