Network Policy Server

Updated: March 29, 2012

Applies To: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2

Network Policy Server

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. In addition, you can use NPS as a Remote Authentication Dial-In User Service (RADIUS) proxy to forward connection requests to a server running NPS or other RADIUS servers that you configure in remote RADIUS server groups.

NPS allows you to centrally configure and manage network access authentication, authorization, and client health policies with the following three features:

- **RADIUS server** . NPS performs centralized authentication, authorization, and accounting for wireless, authenticating switch, remote access dial-up and virtual private network (VPN) connections. When you use NPS as a RADIUS server, you configure network access servers, such as wireless access points and VPN servers, as RADIUS clients in NPS. You also configure network policies that NPS uses to authorize connection requests, and you can configure RADIUS accounting so that NPS logs accounting information to log files on the local hard disk or in a Microsoft SQL Server database. For more information, see RADIUS Server.

- **RADIUS proxy** . When you use NPS as a RADIUS proxy, you configure connection request policies that tell the NPS server which connection requests to forward to other RADIUS servers and to which RADIUS servers you want to forward connection requests. You can also configure NPS to forward accounting data to be logged by one or more computers in a remote RADIUS server group. For more information, see RADIUS Proxy.

- **Network Access Protection (NAP) policy server** . When you configure NPS as a NAP policy server, NPS evaluates statements of health (SoH) sent by NAP-capable client computers that want to connect to the network. NPS also acts as a RADIUS server when configured with NAP, performing authentication and authorization for connection requests. You can configure NAP policies and settings in NPS, including system health validators (SHVs), health policy, and remediation server groups that allow client computers to update their configuration to become compliant with your organization's network policy. For more information, see Network Access Protection in NPS.

You can configure NPS with any combination of the preceding features. For example, you can configure one NPS server to act as a NAP policy server using one or more enforcement methods, while also configuring the same NPS server as a RADIUS server for dial-up connections and as a RADIUS proxy to forward some connection requests to members of a remote RADIUS server group for authentication and authorization in another domain.

Configuration

To configure NPS as a RADIUS server or a NAP policy server, you can use either standard configuration or advanced configuration in the NPS console or in Server Manager. To configure NPS as a RADIUS proxy, you must use advanced configuration.

Standard configuration

With standard configuration, wizards are provided to help you configure NPS for the following scenarios:

- NAP policy server

- RADIUS server for dial-up or VPN connections
- RADIUS server for 802.1X wireless or wired connections

To configure NPS using a wizard, open the NPS console, select one of the preceding scenarios, and then click the link that opens the wizard.

Advanced configuration
When you use advanced configuration, you manually configure NPS as a RADIUS server, NAP policy server, or RADIUS proxy. Some wizards are provided to assist you with policy and NAP configuration; however, these wizards are opened from the NPS folder tree in the NPS console rather than from the **Getting Started** section in the details pane of the console.

To configure NPS by using advanced configuration, open the NPS console, and then click the arrow next to **Advanced Configuration** to expand this section.

The following advanced configuration items are provided.

Configure RADIUS server

To configure NPS as a RADIUS server, you must configure RADIUS clients, network policy, and RADIUS accounting.

The following Help sections provide the information you need to deploy NPS as a RADIUS server:

- RADIUS Server
- Network Policies
- RADIUS Client
- RADIUS Accounting

Configure NAP policy server

To deploy NAP, you must configure NAP components in addition to configuring RADIUS clients and network policy.

The following Help sections provide the information you need to deploy NPS as a NAP policy server:

- Network Access Protection in NPS
- Network Policies
- Health Policies
- Connection Request Policies
- RADIUS Client

Configure RADIUS proxy

To configure NPS as a RADIUS proxy, you must configure RADIUS clients, remote RADIUS server groups, and connection request policies.

The following Help sections provide the information you need to deploy NPS as a RADIUS proxy:

- RADIUS Proxy
- RADIUS Client
- Connection Request Processing
- Remote RADIUS Server Groups

NPS logging

NPS logging is also called *RADIUS accounting* . Configure NPS logging to your requirements whether NPS is used as a RADIUS server, proxy, NAP policy server, or any combination of the three configurations.

To configure NPS logging, you must configure which events you want logged and viewed with Event Viewer, and then determine which other information you want to log. In addition, you must decide whether you want to log user authentication and accounting information to text log files stored on the local computer or to a SQL Server database on either the local computer or a remote computer.

The following Help sections provide the information you need to deploy RADIUS accounting:

- Configure Log File Properties
- Configure SQL Server Logging in NPS

Community Additions