Configuring Microsoft NPS (Network Policy Server) / (Internet Authentication Service) IAS as Wireless LAN Controller (WLC) RADIUS Server

# Solution

This goes through client and user certificate generation via Cert Templates as well as client auto-enrollment of certs through group policy.  Also, cert template creation for the NPS server itself.

# 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

## RADIUS Server

80 out of 102 rated this helpful - Rate this topic

Updated: March 29, 2012

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

Network Policy Server (NPS) can be used as a Remote Authentication Dial-In User Service (RADIUS) server to perform authentication, authorization, and accounting for RADIUS clients. A RADIUS client can be an access server, such as a dial-up server or wireless access point, or a RADIUS proxy. When NPS is used as a RADIUS server, it provides the following:

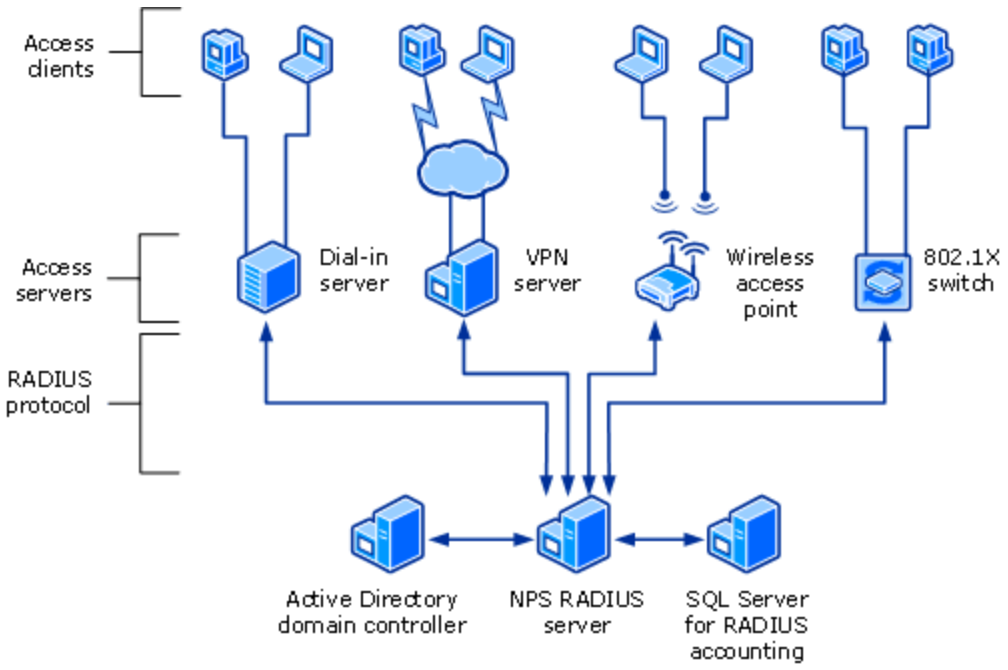
- A central authentication and authorization service for all access requests that are sent by RADIUS clients.

  NPS uses a Microsoft® Windows NT® Server 4.0 domain, an Active Directory® Domain Services (AD DS) domain, or the local Security Accounts Manager (SAM) user accounts database to authenticate user credentials for connection attempts. NPS uses the dial-in properties of the user account and network policies to authorize a connection.

- A central accounting recording service for all accounting requests that are sent by RADIUS clients.

  Accounting requests are stored in a local log file or a Microsoft® SQL Server™ database for analysis.

The following illustration shows NPS as a RADIUS server for a variety of access clients, and also shows a RADIUS proxy. NPS uses an AD DS domain for user credential authentication of incoming RADIUS Access-Request messages.




When NPS is used as a RADIUS server, RADIUS messages provide authentication, authorization, and accounting for network access connections in the following way:

1. Access servers, such as dial-up network access servers, VPN servers, and wireless access points, receive connection requests from access clients.

2. The access server, configured to use RADIUS as the authentication, authorization, and accounting protocol, creates an Access-Request message and sends it to the NPS server.

3. The NPS server evaluates the Access-Request message.

4. 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.

5. 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.

6. The connection attempt is authorized with both the dial-in properties of the user account and network policies.

7. If the connection attempt is both authenticated and authorized, 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.

8. 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.

9. The NPS server sends an Accounting-Response to the access server.

**Note**

The access server also sends Accounting-Request messages during the time in which the connection is established, when the access client connection is closed, and when the access server is started and stopped.

## You can use NPS as a RADIUS server when:

- You are using a Windows NT Server 4.0 domain, an AD DS domain, or the local SAM user accounts database as your user account database for access clients.

- You are using Routing and Remote Access on multiple dial-up servers, VPN servers, or demand-dial routers and you want to centralize both the configuration of network policies and connection logging for accounting.

- You are outsourcing your dial-up, VPN, or wireless access to a service provider. The access servers use RADIUS to authenticate and authorize connections that are made by members of your organization.

- You want to centralize authentication, authorization, and accounting for a heterogeneous set of access servers.

**Note**

In Internet Authentication Service (IAS) in the Windows Server® 2003 operating systems, network policies are referred to as remote access policies.

# Network Policies

17 out of 30 rated this helpful - Rate this topic

Updated: March 29, 2012

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

*Network policies* are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that Network Policy Server (NPS) performs client health checks during the authorization process.

When processing connection requests as a Remote Authentication Dial-In User Service (RADIUS) server, NPS performs both authentication and authorization for the connection request. During the authentication process, NPS verifies the identity of the user or computer that is connecting to the network. During the authorization process, NPS determines whether the user or computer is allowed to access the network.

To make this determination, NPS uses network policies that are configured in the NPS Microsoft Management Console (MMC) snap-in. NPS also examines the dial-in properties of the user account in Active Directory® Domain Services (AD DS) to perform authorization.

**Note**

In Internet Authentication Service (IAS) in the Windows Server® 2003 operating systems, network policies were called *remote access policies* .

Network policies can be viewed as rules. Each rule has a set of conditions and settings. NPS compares the conditions of the rule to the properties of connection requests. If a match occurs between the rule and the connection request, the settings defined in the rule are applied to the connection.

When multiple network policies are configured in NPS, they are an ordered set of rules. NPS checks each connection request against the first rule in the list, then the second, and so on, until a match is found.

Each network policy has a **Policy State** setting that allows you to enable or disable the policy. When you disable a network policy, NPS does not evaluate the policy when authorizing connection requests.

**Important**

If you want NPS to evaluate a network policy when performing authorization for connection requests,

you must configure the **Policy State** setting by selecting the **Policy enabled** check box.

# Network policy properties

There are four categories of properties for each network policy:

- Overview

  These properties allow you to specify whether the policy is enabled, whether the policy grants or denies access, and whether a specific network connection method, or type of network access server (NAS), is required for connection requests. Overview properties also allow you to specify whether the dial-in properties of user accounts in AD DS are ignored. If you select this option, only the settings in the network policy are used by NPS to determine whether the connection is authorized.

- Conditions

  These properties allow you to specify the conditions that the connection request must have in order to match the network policy; if the conditions configured in the policy match the connection request, NPS applies the settings designated in the network policy to the connection. For example, if you specify the NAS IPv4 address as a condition of the network policy and NPS receives a connection request from a NAS that has the specified IP address, the condition in the policy matches the connection request.

- Constraints

  Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Unlike the NPS response to unmatched conditions in the network policy, if a constraint is not matched, NPS denies the connection request without evaluating additional network policies.

- Settings

  These properties allow you to specify the settings that NPS applies to the connection request if all of the network policy conditions for the policy are matched.

When you add a new network policy by using the NPS snap-in, you must use the New Network Policy Wizard. After you have created a network policy by using the wizard, you can customize the policy by double-clicking the policy in the NPS snap-in to obtain the policy properties.

## RADIUS Client



Updated: March 29, 2012

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

A network access server (NAS) is a device that provides some level of access to a larger network. A NAS using a RADIUS infrastructure is also a RADIUS client, sending connection requests and accounting messages to a RADIUS server for authentication, authorization, and accounting.

**Important**

Client computers, such as wireless portable computers and other computers running client operating systems, are not RADIUS clients. RADIUS clients are network access servers—such as wireless access points, 802.1X-capable switches, virtual private network (VPN) servers, and dial-up servers—because they use the RADIUS protocol to communicate with RADIUS servers such as Network Policy Server (NPS) servers.

To deploy NPS as a RADIUS server, a RADIUS proxy, or a Network Access Protection (NAP) policy server, you must configure RADIUS clients in NPS.

# RADIUS client examples

Examples of network access servers are:

- Network access servers that provide remote access connectivity to an organization network or the Internet. An example is a computer running the Windows Server® 2008 operating system and the Routing and Remote Access service that provides either traditional dial-up or virtual private network (VPN) remote access services to an organization intranet.
- Wireless access points that provide physical layer access to an organization network using wireless-based transmission and reception technologies.
- Switches that provide physical layer access to an organization's network, using traditional LAN technologies, such as Ethernet.
- RADIUS proxies that forward connection requests to RADIUS servers that are members of a remote RADIUS server group that is configured on the RADIUS proxy.

# RADIUS Access-Request messages

RADIUS clients either create RADIUS Access-Request messages and forward them to a RADIUS proxy or RADIUS server, or they forward Access-Request messages to a RADIUS server that they have received from another RADIUS client but have not created themselves.

RADIUS clients do not process Access-Request messages by performing authentication, authorization, and accounting. Only RADIUS servers perform these functions.

NPS, however, can be configured as both a RADIUS proxy and a RADIUS server simultaneously, so that it processes some Access-Request messages and forwards other messages.

## NPS as a RADIUS client

NPS acts as a RADIUS client when you configure it as a RADIUS proxy to forward Access-Request messages to other RADIUS servers for processing. When you use NPS as a RADIUS proxy, the following general configuration steps are required:

1. Network access servers, such as wireless access points and VPN servers, are configured with the IP address of the NPS proxy as the designated RADIUS server or authenticating server. This allows the network access servers, which create Access-Request messages based on information they receive from access clients, to forward messages to the NPS proxy.

2. The NPS proxy is configured by adding each network access server as a RADIUS client. This configuration step allows the NPS proxy to receive messages from the network access servers and to communicate with them throughout authentication. In addition, connection request policies on the NPS proxy are configured to specify which Access-Request messages to forward to one or more RADIUS servers. These policies are also configured with a remote RADIUS server group, which tells NPS where to send the messages it receives from the network access servers.

3. The NPS or other RADIUS servers that are members of the remote RADIUS server group on the NPS proxy are configured to receive messages from the NPS proxy. This is accomplished by configuring the NPS proxy as a RADIUS client.

# RADIUS client properties

When you add a RADIUS client to the NPS configuration through the NPS snap-in or through the use of the netsh commands for NPS, you are configuring NPS to receive RADIUS Access-Request messages from either a network access server or a RADIUS proxy.

When you configure a RADIUS client in NPS, you can designate the following properties:

- Client name

  A friendly name for the RADIUS client, which makes it easier to identify when using the NPS snap-in or netsh commands for NPS.

- IP address

  The Internet Protocol version 4 (IPv4) address or the Domain Name System (DNS) name of the RADIUS client.

- Client-Vendor

The vendor of the RADIUS client. Otherwise, you can use the RADIUS standard value for Client-Vendor.

- Shared secret

  A text string that is used as a password between RADIUS clients, RADIUS servers, and RADIUS proxies. When the Message Authenticator attribute is used, the shared secret is also used as the key to encrypt RADIUS messages. This string must be configured on the RADIUS client and in the NPS snap-in.

- Message Authenticator attribute

  Described in RFC 2869, "RADIUS Extensions," a Message Digest 5 (MD5) hash of the entire RADIUS message. If the RADIUS Message Authenticator attribute is present, it is verified. If it fails verification, the RADIUS message is discarded. If the client settings require the Message Authenticator attribute and it is not present, the RADIUS message is discarded. Use of the Message Authenticator attribute is recommended.

  **Note**

  The Message Authenticator attribute is required and enabled by default when you use EAP authentication.

- Client is NAP-capable

  A designation that the RADIUS client is compatible with Network Access Protection (NAP), and NPS sends NAP attributes to the RADIUS client in the Access-Accept message.

## RADIUS Accounting

2 out of 3 rated this helpful - Rate this topic

Updated: March 29, 2012

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

There are three types of logging for Network Policy Server (NPS):

- Event logging.

  Used primarily for auditing and troubleshooting connection attempts. You can configure NPS event logging by obtaining the NPS server properties in the NPS console.

- Logging user authentication and accounting requests to a local file.

  Used primarily for connection analysis and billing purposes. Also useful as a security

investigation tool because it provides you with a method of tracking the activity of a malicious user after an attack. You can configure local file logging using the Accounting Configuration wizard.

- Logging user authentication and accounting requests to a Microsoft® SQL Server™ XML-compliant database.

  Used to allow multiple servers running NPS to have one data source. Also provides the advantages of using a relational database. You can configure SQL Server logging by using the Accounting Configuration wizard.

# Accounting Configuration wizard

By using the Accounting Configuration wizard in the NPS console, you can configure the following four accounting settings:

- **SQL logging only** . By using this setting, you can configure a data link to a SQL Server that allows NPS to connect to and send accounting data to the SQL server. In addition, the wizard can configure the database on the SQL Server to ensure that the database is compatible with NPS SQL server logging.

- **Text logging only** . By using this setting, you can configure NPS to log accounting data to a text file.

- **Parallel logging** . By using this setting, you can configure the SQL Server data link and database. You can also configure text file logging so that NPS logs simultaneously to the text file and the SQL Server database.

- **SQL logging with backup** . By using this setting, you can configure the SQL Server data link and database. In addition, you can configure text file logging that NPS uses if SQL Server logging fails.

In addition to these settings, both SQL Server logging and text logging allow you to specify whether NPS continues to process connection requests if logging fails. You can specify this in **Logging failure action** section in local file logging properties, in SQL Server logging properties, and while you are running the Accounting Configuration wizard.

To run the Accounting Configuration Wizard, complete the following steps:

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.

2. In the console tree, click **Accounting** .

3. In the details pane, in **Accounting** , click **Configure 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

## Network Access Protection in NPS

8 out of 12 rated this helpful - Rate this topic

Updated: March 29, 2012

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

Network Access Protection (NAP) is a client health policy creation, enforcement, and remediation technology that is included in Windows Vista®, Windows Server® 2008, Windows® 7, and Windows Server® 2008 R2. By using NAP, you can establish health policies that define such things as software requirements, security update requirements, and required configuration settings for computers that connect to your network.

NAP enforces health policies by inspecting and assessing the health of client computers, restricting network access when client computers are noncompliant with health policy, and remediating noncompliant client computers to bring them into compliance with health policy before they are granted full network access. NAP enforces health policies on client computers that are attempting to connect to a network. NAP also provides ongoing health compliance enforcement while a client computer is connected to a network.

NAP is an extensible platform that provides an infrastructure and an application programming interface (API) set. By using the NAP API set, you can add components to NAP clients and to servers running Network Policy Server (NPS) that check computer health, enforce network health policy, and remediate noncompliant computers to bring them into compliance with health policy.

By itself, NAP does not provide components to verify or remediate computer health. Other components, known as *system health agents (SHAs)* and *system health validators (SHVs)* , provide client computer health state inspection and reporting, validation of client computer health state compared to health policy, and configuration settings to help the client computer become compliant with health policy.

The Windows Security Health Agent (WSHA) is included in Windows Vista and Windows 7 as part of the operating system. The corresponding Windows Security Health Validator (WSHV) is included in Windows Server 2008 and Windows Server 2008 R2 as part of the operating system. By using the NAP API set, other products can also implement SHAs and SHVs to integrate with

NAP. For example, an antivirus software vendor can use the API set to create a custom SHA and SHV. These components can then be integrated into the NAP solutions deployed by customers of the software vendor.

If you are a network or system administrator planning to deploy NAP, you can deploy NAP with the WSHA and WSHV that are included with the operating system. You can also check with other software vendors to find out if they provide SHAs and SHVs for their products.

# NAP overview

Most organizations create network policies that dictate the type of hardware and software that can be deployed on the organization network. These policies frequently include rules for how client computers can be configured before connecting to the network. For example, many organizations require that client computers run antivirus software with recent antivirus updates installed, and that client computers have a software firewall installed and enabled before connecting to the organization network. A client computer that is configured according to the organization network policy can be viewed as compliant with policy, while a computer that is not configured according to the organization network policy can be viewed as noncompliant with policy.

NAP allows you to use NPS to create policies that define client computer health. NAP also allows you to enforce the client health policies you create, and to automatically update, or remediate, NAP-capable client computers to bring them into compliance with client health policy. NAP provides continuous detection of client computer health to guard against cases in which a client computer is compliant when it connects to the organization network but becomes noncompliant while connected.

NAP provides complementary client computer and organization network protection by ensuring that computers connecting to the network comply with organization network and client health policies. This protects the network from harmful elements introduced by client computers, such as computer viruses, and it also protects client computers from harmful elements that could be introduced by the network to which it is connecting.

In addition, NAP autoremediation reduces the amount of time that noncompliant client computers are prevented from accessing organization network resources. When autoremediation is configured and clients are in a noncompliant state, NAP client components can rapidly update the computer by using resources you supply on a remediation network, allowing the now-compliant client to be more quickly authorized by NPS to connect to the network.

# NPS and NAP

NPS can act as a NAP policy server for all NAP enforcement methods.

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. You can configure NAP

policies in NPS that allow client computers to update their configuration to become compliant with your organization network policy.

## Client computer health

*Health* is defined as information about a client computer that NAP uses to determine whether to allow or deny client access to a network. An assessment of client computer health status represents the configuration state of a client computer in comparison to the state that is required by health policy.

Example measurements of health include:

- The operational status of Windows Firewall. Is the firewall enabled or disabled?
- The update status of antivirus signatures. Are the antivirus signatures the most recent ones available?
- The installation status of security updates. Are the most recent security updates installed on the client?

The health status of the client computer is encapsulated in an SoH, which is issued by NAP client components. NAP client components send the SoH to NAP server components for evaluation to determine whether the client is compliant and can be granted full network access.

In NAP terminology, verifying that a computer meets your defined health requirements is called *health policy validation* . NPS performs health policy validation for NAP.

## How NAP enforcement works

NAP enforces health policies by using client-side components that inspect and assess the health of client computers, server-side components that restrict network access when client computers are deemed noncompliant, and both client-side and server-side components that assist in remediating noncompliant client computers for full network access.

# Key processes of NAP

To help protect network access, NAP relies on three processes: policy validation, NAP enforcement and network restriction, and remediation and ongoing compliance.

## Policy validation

By using NPS, you can create client health policies using SHVs that allow NAP to detect, enforce, and remediate client computer configurations.

WSHA and WSHV provide the following functionality for NAP-capable computers:

- The client computer has firewall software installed and enabled.
- The client computer has antivirus software installed and running.
- The client computer has current antivirus updates installed.
- The client computer has antispyware software installed and running.
- The client computer has current antispyware updates installed.
- Microsoft Update Services is enabled on the client computer.

In addition, if NAP-capable client computers are running Windows Update Agent and are registered with a Windows Server Update Service (WSUS) server, NAP can verify that the most recent software security updates are installed based on one of four possible values that match security severity ratings from the Microsoft Security Response Center (MSRC).

When you create policies that define the client computer health status, policies are validated by NPS. The NAP client-side components send a SoH to the NPS server during the network connection process. NPS examines the SoH and compares it to health policies.

# NAP enforcement and network restriction

NAP denies noncompliant client computers access to the network or allows them access only to a special restricted network called a *remediation network* . A remediation network provides client computers with access to remediation servers, which provide software updates, and other key NAP services, such as Health Registration Authority (HRA) servers, that are required to bring noncompliant NAP clients into compliance with health policy.

The NAP enforcement setting in NPS network policy allows you to use NAP to limit the network access or observe the state of NAP-capable client computers that do not comply with your network health policy.

You can choose to restrict access, defer restriction of access, or allow access with network policy settings.

# Remediation

Noncompliant client computers that are put into a restricted network might undergo remediation. *Remediation* is the process of automatically updating a client computer so that it meets current health policies. For example, a restricted network might contain a File Transfer Protocol (FTP) server that automatically updates the virus signatures of noncompliant client computers that have outdated signatures.

### *Ongoing compliance*

NAP can enforce health compliance on client computers that are already connected to the network. This functionality is useful for ensuring that a network is protected on an ongoing basis as health policies change and the health of client computers change. For example, NAP determines that the client computer is in a noncompliant state if a health policy requires that Windows Firewall is turned on and an administrator inadvertently turns the firewall off on a client computer. NAP will then disconnect the client computer from the organization network and connect the client computer to the remediation network until Windows Firewall is turned back on.

You can use NAP settings in NPS network policies to configure autoremediation so that NAP client components automatically attempt to update the client computer when it is not compliant. As with NAP enforcement settings, autoremediation is configured in network policy settings.

## Network Policies



Updated: March 29, 2012

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

*Network policies* are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that Network Policy Server (NPS) performs client health checks during the authorization process.

When processing connection requests as a Remote Authentication Dial-In User Service (RADIUS) server, NPS performs both authentication and authorization for the connection request. During the authentication process, NPS verifies the identity of the user or computer that is connecting to the network. During the authorization process, NPS determines whether the user or computer is allowed to access the network.

To make this determination, NPS uses network policies that are configured in the NPS Microsoft Management Console (MMC) snap-in. NPS also examines the dial-in properties of the user account in Active Directory® Domain Services (AD DS) to perform authorization.

**Note**

In Internet Authentication Service (IAS) in the Windows Server® 2003 operating systems, network policies were called *remote access policies* .

Network policies can be viewed as rules. Each rule has a set of conditions and settings. NPS compares the conditions of the rule to the properties of connection requests. If a match occurs between the rule and the connection request, the settings defined in the rule are applied to the connection.

When multiple network policies are configured in NPS, they are an ordered set of rules. NPS checks each connection request against the first rule in the list, then the second, and so on, until a match is found.

Each network policy has a **Policy State** setting that allows you to enable or disable the policy. When you disable a network policy, NPS does not evaluate the policy when authorizing connection requests.

**Important**

If you want NPS to evaluate a network policy when performing authorization for connection requests, you must configure the **Policy State** setting by selecting the **Policy enabled** check box.

# Network policy properties

There are four categories of properties for each network policy:

- Overview

  These properties allow you to specify whether the policy is enabled, whether the policy grants or denies access, and whether a specific network connection method, or type of network access server (NAS), is required for connection requests. Overview properties also allow you to specify whether the dial-in properties of user accounts in AD DS are ignored. If you select this option, only the settings in the network policy are used by NPS to determine whether the connection is authorized.

- Conditions

  These properties allow you to specify the conditions that the connection request must have in order to match the network policy; if the conditions configured in the policy match the connection request, NPS applies the settings designated in the network policy to the connection. For example, if you specify the NAS IPv4 address as a condition of the network policy and NPS receives a connection request from a NAS that has the specified IP address, the condition in the policy matches the connection request.

- Constraints

  Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Unlike the NPS response to unmatched conditions in the network policy, if a

constraint is not matched, NPS denies the connection request without evaluating additional network policies.

- Settings

  These properties allow you to specify the settings that NPS applies to the connection request if all of the network policy conditions for the policy are matched.

When you add a new network policy by using the NPS snap-in, you must use the New Network Policy Wizard. After you have created a network policy by using the wizard, you can customize the policy by double-clicking the policy in the NPS snap-in to obtain the policy properties

## Health Policies

2 out of 4 rated this helpful - Rate this topic

Updated: March 29, 2012

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

*Health policies* consist of one or more system health validators (SHVs) and other settings that allow you to define client computer configuration requirements for the Network Access Protection (NAP)-capable computers that attempt to connect to your network.

When NAP-capable clients attempt to connect to the network, the client computer sends a statement of health (SoH) to Network Policy Server (NPS). The SoH is a report of the client configuration state, and NPS compares the SoH to the requirements defined in health policy. If the client configuration state does not match the requirements defined in health policy, NPS takes one of the following actions, depending on how NAP is configured:

- The connection request by the NAP client is rejected.
- The NAP client is placed on a restricted network where it can receive updates from remediation servers that bring the client into compliance with health policy. After the client is compliant with health policy, it is allowed to connect.
- The NAP client is allowed to connect to the network despite being noncompliant with health policy.

You can define client health policies in NPS by adding one or more SHVs to the health policy.

After a health policy is configured with one or more SHVs, you can add the health policy to the Health Policies condition of a network policy that you want to use to enforce NAP when client computers connect to your network.

# Using multiple SHVs in a health policy

The Windows Security Health Validator (WSHV) is included by default in NPS. Other companies might also provide additional SHV and system health agent (SHA) pairs for their NAP-compatible products.

If you want to use a NAP-compatible product, you can follow the documentation for that product about how to install the SHA on NAP-capable client computers, and then install the SHV on the server running NPS. After you have installed the SHV on the NPS server, you can configure the SHV and then add the SHV to a health policy.

After your health policy is configured with the SHVs you want to use, you can add the health policy to the settings of a network policy.

## Connection Request Policies

5 out of 5 rated this helpful - Rate this topic

Updated: March 29, 2012

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

*Connection request policies* are sets of conditions and settings that allow network administrators to designate which Remote Authentication Dial-In User Service (RADIUS) servers perform the authentication and authorization of connection requests that the server running Network Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS servers are used for RADIUS accounting.

**Important**

When you deploy Network Access Protection (NAP) by using the virtual private network (VPN) or 802.1X enforcement methods with Protected Extensible Authentication Protocol (PEAP) authentication, you must configure PEAP authentication in the connection request policy even when connection requests are processed locally.

You can create connection request policies so that some RADIUS request messages sent from RADIUS clients are processed locally (NPS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (NPS is being used as a RADIUS proxy).

With connection request policies, you can use NPS as a RADIUS server or as a RADIUS proxy, based on factors such as the following:

- The time of day and day of the week
- The realm name in the connection request
- The type of connection being requested

- The IP address of the RADIUS client

RADIUS Access-Request messages are processed or forwarded by NPS only if the settings of the incoming message match at least one of the connection request policies configured on the NPS server. If the policy settings match and the policy requires that the NPS server process the message, NPS acts as a RADIUS server, authenticating and authorizing the connection request. If the policy settings match and the policy requires that the NPS server forwards the message, NPS acts as a RADIUS proxy and forwards the connection request to a remote RADIUS server for processing.

If the settings of an incoming RADIUS Access-Request message do not match at least one of the connection request policies, an Access-Reject message is sent to the RADIUS client and the user or computer attempting to connect to the network is denied access.

# Configuration examples

The following configuration examples demonstrate how connection request policies can be used:

- NPS as a RADIUS server

  The default connection request policy is the only configured policy. In this example, NPS is configured as a RADIUS server and all connection requests are processed by the local NPS server. The NPS server can authenticate and authorize users whose accounts are in the domain of the NPS server domain and in trusted domains.

- NPS as a RADIUS proxy

  The default connection request policy is deleted, and two new connection request policies are created to forward requests to two different domains. In this example, NPS is configured as a RADIUS proxy. NPS does not process any connection requests on the local server. Instead, it forwards connection requests to NPS or other RADIUS servers that are configured as members of remote RADIUS server groups.

- NPS as both RADIUS server and RADIUS proxy

  In addition to the default connection request policy, a new connection request policy is created that forwards connection requests to an NPS or other RADIUS server in an untrusted domain. In this example, the proxy policy appears first in the ordered list of policies. If the connection request matches the proxy policy, the connection request is forwarded to the RADIUS server in the remote RADIUS server group. If the connection request does not match the proxy policy but does match the default connection request policy, NPS processes the connection request on the local server. If the connection request does not match either policy, it is discarded.

- NPS as RADIUS server with remote accounting servers

  In this example, the local NPS server is not configured to perform accounting and the default connection request policy is revised so that RADIUS accounting messages are forwarded to an

NPS or other RADIUS server in a remote RADIUS server group. Although accounting messages are forwarded, authentication and authorization messages are not forwarded, and the local NPS server performs these functions for the local domain and all trusted domains.

- NPS with Remote RADIUS to Windows User Mapping

  In this example, NPS acts as both a RADIUS server and as a RADIUS proxy for each individual connection request by forwarding the authentication request to a remote RADIUS server while using a local Windows user account for authorization. This configuration is implemented by configuring the **Remote RADIUS to Windows User Mapping** attribute as a condition of the connection request policy. (In addition, a user account must be created locally that has the same name as the remote user account against which authentication is performed by the remote RADIUS server.)

# Conditions

*Connection request policy conditions* are one or more RADIUS attributes that are compared to the attributes of the incoming RADIUS Access-Request message. If there are multiple conditions, then all of the conditions in the connection request message and in the connection request policy must match in order for the policy to be enforced by NPS.

Following are the available condition attributes that you can configure in connection request policies.

The **Connection Properties** attribute group contains the following attributes.

- **Framed Protocol** . Used to designate the type of framing for incoming packets. Examples are Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Frame Relay, and X.25.

- **Service Type** . Used to designate the type of service being requested. Examples include framed (for example, PPP connections) and login (for example, Telnet connections). For more information about RADIUS service types, see RFC 2865, "Remote Authentication Dial-in User Service (RADIUS)."

- **Tunnel Type** . Used to designate the type of tunnel that is being created by the requesting client. Tunnel types include the Point-to-Point Tunneling Protocol (PPTP) and the Layer Two Tunneling Protocol (L2TP).

The **Day and Time Restrictions** attribute group contains the **Day and Time Restrictions** attribute. With this attribute, you can designate the day of the week and the time of day of the connection attempt. The day and time is relative to the day and time of the NPS server.

The **Gateway** attribute group contains the following attributes.

- **Called Station ID** . Used to designate the phone number of the network access server. This attribute is a character string. You can use pattern-matching syntax to specify area codes.

- **NAS Identifier** . Used to designate the name of the network access server. This attribute is a character string. You can use pattern-matching syntax to specify NAS identifiers.

- **NAS IPv4 Address** . Used to designate the Internet Protocol version 4 (IPv4) address of the network access server (the RADIUS client). This attribute is a character string. You can use pattern-matching syntax to specify IP networks.

- **NAS IPv6 Address** . Used to designate the Internet Protocol version 6 (IPv6) address of the network access server (the RADIUS client). This attribute is a character string. You can use pattern-matching syntax to specify IP networks.

- **NAS Port Type** . Used to designate the type of media used by the access client. Examples are analog phone lines (known as *async* ), Integrated Services Digital Network (ISDN), tunnels or virtual private networks (VPNs), IEEE 802.11 wireless, and Ethernet switches.

The **Machine Identity** attribute group contains the **Machine Identity** attribute. By using this attribute, you can specify the method with which clients are identified in the policy.

The **RADIUS Client Properties** attribute group contains the following attributes.

- **Calling Station ID** . Used to designate the phone number used by the caller (the access client). This attribute is a character string. You can use pattern-matching syntax to specify area codes.

- **Client Friendly Name** . Used to designate the name of the RADIUS client computer that is requesting authentication. This attribute is a character string. You can use pattern-matching syntax to specify client names.

- **Client IPv4 Address** . Used to designate the IPv4 address of the network access server (the RADIUS client). This attribute is a character string. You can use pattern-matching syntax to specify IP networks.

- **Client IPv6 Address** . Used to designate the IPv6 address of the network access server (the RADIUS client). This attribute is a character string. You can use pattern-matching syntax to specify IP networks.

- **Client Vendor** . Used to designate the vendor of the network access server that is requesting authentication. A computer running the Routing and Remote Access service is the Microsoft NAS manufacturer. You can use this attribute to configure separate policies for different NAS manufacturers. This attribute is a character string. You can use pattern-matching syntax.

The **User Name** attribute group contains the **User Name** attribute. By using this attribute, you can designate the user name, or a portion of the user name, that must match the user name supplied by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name. You can use pattern-matching syntax to specify user names.

# Settings

Connection request policy settings are a set of properties that are applied to an incoming RADIUS message. Settings consist of the following groups of properties:

- Authentication
- Accounting
- Attribute manipulation
- Advanced

# Authentication

By using this setting, you can override the authentication settings that are configured in all network policies and you can designate the authentication methods and types that are required to connect to your network.

**Important**

If you configure an authentication method in connection request policy that is less secure than the authentication method you configure in network policy, the more secure authentication method that you configure in network policy will be overridden. For example, if you have one network policy that requires the use of Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2), which is a password-based authentication method for secure wireless, and you also configure a connection request policy to allow unauthenticated access, no clients are required to authenticate by using PEAP-MS-CHAP v2. In this example, all clients connecting to your network are granted unauthenticated access.

# Accounting

By using this setting, you can configure connection request policy to forward accounting information to an NPS or other RADIUS server in a remote RADIUS server group so that the remote RADIUS server group performs accounting.

**Note**

If you have multiple RADIUS servers and you want accounting information for all servers stored in one central RADIUS accounting database, you can use the connection request policy accounting setting in a policy on each RADIUS server to forward accounting data from all of the servers to one NPS or other RADIUS server that is designated as an accounting server.

Connection request policy accounting settings function independent of the accounting configuration of the local NPS server. In other words, if you configure the local NPS server to

log RADIUS accounting information to a local file or to a Microsoft® SQL Server™ database, it will do so regardless of whether you configure a connection request policy to forward accounting messages to a remote RADIUS server group.

If you want accounting information logged remotely but not locally, you must configure the local NPS server to not perform accounting, while also configuring accounting in a connection request policy to forward accounting data to a remote RADIUS server group.

# Attribute manipulation

You can configure a set of find-and-replace rules that manipulate the text strings of one of the following attributes:

- User Name
- Called Station ID
- Calling Station ID

Find-and-replace rule processing occurs for one of the preceding attributes before the RADIUS message is subject to authentication and accounting settings. Attribute manipulation rules apply only to a single attribute. You cannot configure attribute manipulation rules for each attribute. In addition, the list of attributes that you can manipulate is a static list; you cannot add to the list of attributes available for manipulation.

**Note**

If you are using the MS-CHAP v2 authentication protocol, you cannot manipulate the **User Name** attribute if the connection request policy is used to forward the RADIUS message. The only exception occurs when a backslash (\) character is used and the manipulation only affects the information to the left of it. A backslash character is typically used to indicate a domain name (the information to the left of the backslash character) and a user account name within the domain (the information to the right of the backslash character). In this case, only attribute manipulation rules that modify or replace the domain name are allowed.

# Forwarding request

You can set the following forwarding request options that are used for RADIUS Access-Request messages:

**Authenticate requests on this server** . By using this setting, NPS uses a Windows NT 4.0 domain, Active Directory, or the local Security Accounts Manager (SAM) user accounts database to authenticate the connection request. This setting also specifies that the matching network policy configured in NPS, along with the dial-in properties of the user account, are used

by NPS to authorize the connection request. In this case, the NPS server is configured to perform as a RADIUS server.

**Forward requests to the following remote RADIUS server group** . By using this setting, NPS forwards connection requests to the remote RADIUS server group that you specify. If the NPS server receives a valid Access-Accept message that corresponds to the Access-Request message, the connection attempt is considered authenticated and authorized. In this case, the NPS server acts as a RADIUS proxy.

**Accept users without validating credentials** . By using this setting, NPS does not verify the identity of the user attempting to connect to the network and NPS does not attempt to verify that the user or computer has the right to connect to the network. When NPS is configured to allow unauthenticated access and it receives a connection request, NPS immediately sends an Access-Accept message to the RADIUS client and the user or computer is granted network access. This setting is used for some types of compulsory tunneling where the access client is tunneled before user credentials are authenticated.

**Note**

This authentication option cannot be used when the authentication protocol of the access client is MS-CHAP v2 or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), both of which provide mutual authentication. In mutual authentication, the access client proves that it is a valid access client to the authenticating server (the NPS server), and the authenticating server proves that it is a valid authenticating server to the access client. When this authentication option is used, the Access-Accept message is returned. However, the authenticating server does not provide validation to the access client and mutual authentication fails.

# Advanced

You can set advanced properties to specify the series of RADIUS attributes that are:

- Added to the RADIUS response message when the NPS server is being used as a RADIUS authentication or accounting server.

  When there are attributes specified on both a network policy and the connection request policy, the attributes that are sent in the RADIUS response message are the combination of the two sets of attributes.

- Added to the RADIUS message when the NPS server is being used as a RADIUS authentication or accounting proxy. If the attribute already exists in the message that is forwarded, it is replaced with the value of the attribute specified in the connection request policy.

In addition, some attributes that are available for configuration on the connection request policy **Settings** tab in the **Advanced** category provide specialized functionality. For example, you can configure the **Remote RADIUS to Windows User Mapping** attribute when you want to split

the authentication and authorization of a connection request between two user accounts databases.

The **Remote RADIUS to Windows User Mapping** attribute specifies that Windows authorization occurs for users who are authenticated by a remote RADIUS server. In other words, a remote RADIUS server performs authentication against a user account in a remote user accounts database, but the local NPS server authorizes the connection request against a user account in a local user accounts database. This is useful when you want to allow visitors access to your network.

For example, visitors from partner organizations can be authenticated by their own partner organization RADIUS server, and then use a Windows user account at your organization to access a guest local area network (LAN) on your network.

Other attributes that provide specialized functionality are:

- **MS-Quarantine-IPFilter and MS-Quarantine-Session-Timeout** . These attributes are used when you deploy Network Access Quarantine Control (NAQC) with your Routing and Remote Access VPN deployment.
- **Passport-User-Mapping-UPN-Suffix** . This attribute allows you to authenticate connection requests with Windows Live™ ID user account credentials.
- **Tunnel-Tag** . This attribute designates the VLAN ID number to which the connection should be assigned by the NAS when you deploy virtual local area networks (VLANs).

# Default connection request policy

A default connection request policy is created when you install NPS. This policy has the following configuration:

- **Authentication** is not configured.
- **Accounting** is not configured to forward accounting information to a remote RADIUS server group.
- **Attribute** is not configured with attribute manipulation rules that forward connection requests to remote RADIUS server groups.
- **Forwarding Request** is configured so that connection requests are authenticated and authorized on the local NPS server.
- **Advanced** attributes are not configured.

The default connection request policy uses NPS as a RADIUS server. To configure a server running NPS to act as a RADIUS proxy, you must also configure a remote RADIUS server group. You can create a new remote RADIUS server group while you are creating a new

connection request policy by using the New Connection Request Policy Wizard. You can either delete the default connection request policy or verify that the default connection request policy is the last policy processed.

**Note**

If NPS and the Routing and Remote Access service are installed on the same computer, and the Routing and Remote Access service is configured for Windows authentication and accounting, it is possible for Routing and Remote Access authentication and accounting requests to be forwarded to a RADIUS server. This can occur when Routing and Remote Access authentication and accounting requests match a connection request policy that is configured to forward them to a remote RADIUS server group.

## RADIUS Client

10 out of 15 rated this helpful - Rate this topic

Updated: March 29, 2012

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

A network access server (NAS) is a device that provides some level of access to a larger network. A NAS using a RADIUS infrastructure is also a RADIUS client, sending connection requests and accounting messages to a RADIUS server for authentication, authorization, and accounting.

**Important**

Client computers, such as wireless portable computers and other computers running client operating systems, are not RADIUS clients. RADIUS clients are network access servers—such as wireless access points, 802.1X-capable switches, virtual private network (VPN) servers, and dial-up servers—because they use the RADIUS protocol to communicate with RADIUS servers such as Network Policy Server (NPS) servers.

To deploy NPS as a RADIUS server, a RADIUS proxy, or a Network Access Protection (NAP) policy server, you must configure RADIUS clients in NPS.

# RADIUS client examples

Examples of network access servers are:

- Network access servers that provide remote access connectivity to an organization network or the Internet. An example is a computer running the Windows Server® 2008 operating system

and the Routing and Remote Access service that provides either traditional dial-up or virtual private network (VPN) remote access services to an organization intranet.

- Wireless access points that provide physical layer access to an organization network using wireless-based transmission and reception technologies.

- Switches that provide physical layer access to an organization's network, using traditional LAN technologies, such as Ethernet.

- RADIUS proxies that forward connection requests to RADIUS servers that are members of a remote RADIUS server group that is configured on the RADIUS proxy.

# RADIUS Access-Request messages

RADIUS clients either create RADIUS Access-Request messages and forward them to a RADIUS proxy or RADIUS server, or they forward Access-Request messages to a RADIUS server that they have received from another RADIUS client but have not created themselves.

RADIUS clients do not process Access-Request messages by performing authentication, authorization, and accounting. Only RADIUS servers perform these functions.

NPS, however, can be configured as both a RADIUS proxy and a RADIUS server simultaneously, so that it processes some Access-Request messages and forwards other messages.

# NPS as a RADIUS client

NPS acts as a RADIUS client when you configure it as a RADIUS proxy to forward Access-Request messages to other RADIUS servers for processing. When you use NPS as a RADIUS proxy, the following general configuration steps are required:

1. Network access servers, such as wireless access points and VPN servers, are configured with the IP address of the NPS proxy as the designated RADIUS server or authenticating server. This allows the network access servers, which create Access-Request messages based on information they receive from access clients, to forward messages to the NPS proxy.

2. The NPS proxy is configured by adding each network access server as a RADIUS client. This configuration step allows the NPS proxy to receive messages from the network access servers and to communicate with them throughout authentication. In addition, connection request policies on the NPS proxy are configured to specify which Access-Request messages to forward to one or more RADIUS servers. These policies are also configured with a remote RADIUS server group, which tells NPS where to send the messages it receives from the network access servers.

3. The NPS or other RADIUS servers that are members of the remote RADIUS server group on the NPS proxy are configured to receive messages from the NPS proxy. This is accomplished by configuring the NPS proxy as a RADIUS client.

# RADIUS client properties

When you add a RADIUS client to the NPS configuration through the NPS snap-in or through the use of the netsh commands for NPS, you are configuring NPS to receive RADIUS Access-Request messages from either a network access server or a RADIUS proxy.

When you configure a RADIUS client in NPS, you can designate the following properties:

- Client name

  A friendly name for the RADIUS client, which makes it easier to identify when using the NPS snap-in or netsh commands for NPS.

- IP address

  The Internet Protocol version 4 (IPv4) address or the Domain Name System (DNS) name of the RADIUS client.

- Client-Vendor

  The vendor of the RADIUS client. Otherwise, you can use the RADIUS standard value for Client-Vendor.

- Shared secret

  A text string that is used as a password between RADIUS clients, RADIUS servers, and RADIUS proxies. When the Message Authenticator attribute is used, the shared secret is also used as the key to encrypt RADIUS messages. This string must be configured on the RADIUS client and in the NPS snap-in.

- Message Authenticator attribute

  Described in RFC 2869, "RADIUS Extensions," a Message Digest 5 (MD5) hash of the entire RADIUS message. If the RADIUS Message Authenticator attribute is present, it is verified. If it fails verification, the RADIUS message is discarded. If the client settings require the Message Authenticator attribute and it is not present, the RADIUS message is discarded. Use of the Message Authenticator attribute is recommended.

  **Note**

  The Message Authenticator attribute is required and enabled by default when you use EAP authentication.

- Client is NAP-capable

A designation that the RADIUS client is compatible with Network Access Protection (NAP), and NPS sends NAP attributes to the RADIUS client in the Access-Accept message.

# 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

## RADIUS Proxy

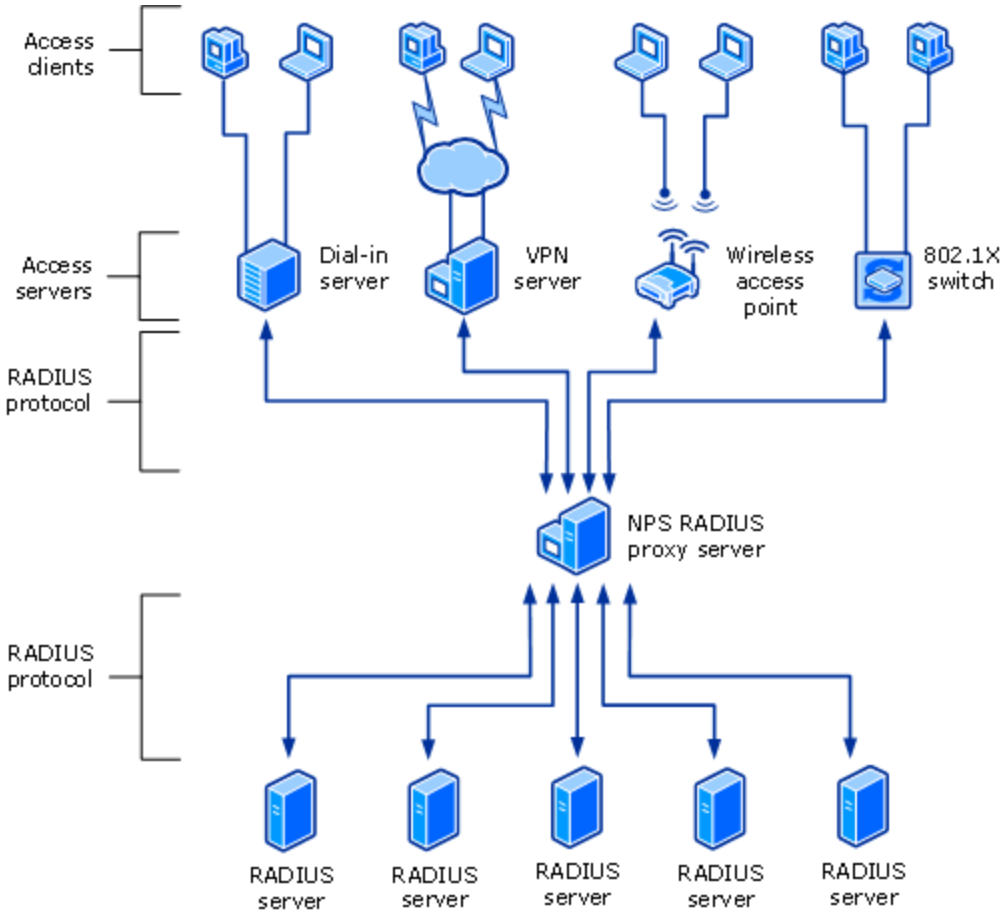
14 out of 18 rated this helpful - Rate this topic

Updated: March 29, 2012

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

Network Policy Server (NPS) can be used as a RADIUS proxy to provide the routing of RADIUS messages between RADIUS clients access servers and RADIUS servers that perform user authentication, authorization, and accounting for the connection attempt. When used as a RADIUS proxy, NPS is a central switching or routing point through which RADIUS access and accounting messages flow. NPS records information in an accounting log about the messages that are forwarded.

The following illustration shows NPS as a RADIUS proxy between RADIUS clients (access servers) and either RADIUS servers or another RADIUS proxy.




When NPS is used as a RADIUS proxy between a RADIUS client and a RADIUS server, RADIUS messages for network access connection attempts are forwarded in the following way:

1. Access servers, such as dial-up network access servers, virtual private network (VPN) servers, and wireless access points, receive connection requests from access clients.

2. The access server, configured to use RADIUS as the authentication, authorization, and accounting protocol, creates an Access-Request message and sends it to the NPS server that is being used as the NPS RADIUS proxy.

3. The NPS RADIUS proxy receives the Access-Request message and, based on the locally configured connection request policies, determines where to forward the Access-Request message.

4. The NPS RADIUS proxy forwards the Access-Request message to the appropriate RADIUS server.

5. The RADIUS server evaluates the Access-Request message.

6. If required, the RADIUS server sends an Access-Challenge message to the NPS RADIUS proxy, where it is forwarded to the access server. The access server processes the challenge with the access client and sends an updated Access-Request to the NPS RADIUS proxy, where it is forwarded to the RADIUS server.

7. The RADIUS server authenticates and authorizes the connection attempt.

8. If the connection attempt is both authenticated and authorized, the RADIUS server sends an Access-Accept message to the NPS RADIUS proxy, where it is forwarded to the access server.

   If the connection attempt is either not authenticated or not authorized, the RADIUS server sends an Access-Reject message to the NPS RADIUS proxy, where it is forwarded to the access server.

9. The access server completes the connection process with the access client and sends an Accounting-Request message to the NPS RADIUS proxy. The NPS RADIUS proxy logs the accounting data and forwards the message to the RADIUS server.

10. The RADIUS server sends an Accounting-Response to the NPS RADIUS proxy, where it is forwarded to the access server.

You can use NPS as a RADIUS proxy when:

- You are a service provider who offers outsourced dial-up, VPN, or wireless network access services to multiple customers. Your NASs send connection requests to the NPS RADIUS proxy. Based on the realm portion of the user name in the connection request, the NPS RADIUS proxy forwards the connection request to a RADIUS server that is maintained by the customer and can authenticate and authorize the connection attempt.

- You want to provide authentication and authorization for user accounts that are not members of either the domain in which the NPS server is a member or another domain that has a two-way trust with the domain in which the NPS server is a member. This includes accounts in untrusted domains, one-way trusted domains, and other forests. Instead of configuring your access servers to send their connection requests to an NPS RADIUS server, you can configure them to send their connection requests to an NPS RADIUS proxy. The NPS RADIUS proxy uses the realm name portion of the user name and forwards the request to an NPS server in the correct domain or forest. Connection attempts for user accounts in one domain or forest can be authenticated for NASs in another domain or forest.

- You want to perform authentication and authorization by using a database that is not a Windows account database. In this case, connection requests that match a specified realm name are forwarded to a RADIUS server, which has access to a different database of user accounts and authorization data. Examples of other user databases include Novell Directory Services (NDS) and Structured Query Language (SQL) databases.

- You want to process a large number of connection requests. In this case, instead of configuring your RADIUS clients to attempt to balance their connection and accounting requests across multiple RADIUS servers, you can configure them to send their connection and accounting requests to an NPS RADIUS proxy. The NPS RADIUS proxy dynamically balances the load of connection and accounting requests across multiple RADIUS servers and increases the processing of large numbers of RADIUS clients and authentications per second.

- You want to provide RADIUS authentication and authorization for outsourced service providers and minimize intranet firewall configuration. An intranet firewall is between your perimeter network (the network between your intranet and the Internet) and intranet. By placing an NPS server on your perimeter network, the firewall between your perimeter network and intranet must allow traffic to flow between the NPS server and multiple domain controllers. By replacing the NPS server with an NPS proxy, the firewall must allow only RADIUS traffic to flow between the NPS proxy and one or multiple NPS servers within your intranet.

## Connection Request Processing

This topic has not yet been rated - Rate this topic

Updated: March 29, 2012

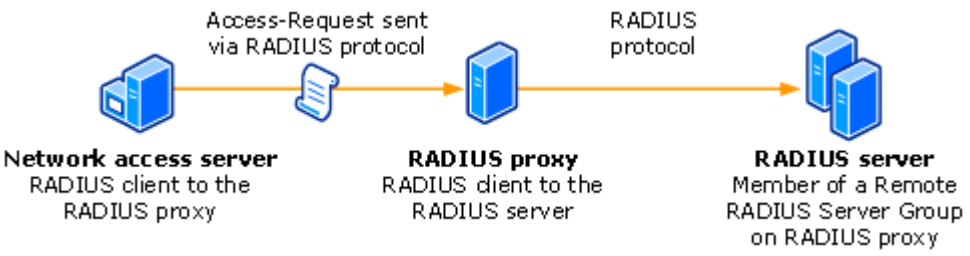
Applies To: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2

You can use connection request processing to specify where the authentication of connection requests is performed - on the local computer or at a remote RADIUS server that is a member of a remote RADIUS server group.

If you want the local server running Network Policy Server (NPS) to perform authentication for connection requests, you can use the default connection request policy without additional configuration. Based on the default policy, NPS authenticates users and computers that have an account in the local domain and in trusted domains.

If you want to forward connection requests to a remote NPS or other RADIUS server, create a remote RADIUS server group and then configure a connection request policy that forwards requests to that remote RADIUS server group. With this configuration, NPS can forward authentication requests to any RADIUS server, and users with accounts in untrusted domains can be authenticated.

The following illustration shows the path of an Access-Request message from a network access server to a RADIUS proxy, and then on to a RADIUS server in a remote RADIUS server group. On the RADIUS proxy, the network access server is configured as a RADIUS client; and on each RADIUS server, the RADIUS proxy is configured as a RADIUS client.



**Note**

The network access servers that you use with NPS can be gateway devices that are compliant with the RADIUS protocol, such as 802.1X wireless access points and authenticating switches, servers running Routing and Remote Access that are configured as VPN or dial-up servers, Remote Desktop Gateway (RD°Gateway) servers, and other devices.

If you want NPS to process some authentication requests locally while forwarding other requests to a remote RADIUS server group, configure more than one connection request policy.

To configure a connection request policy that specifies which NPS or RADIUS server group processes authentication requests, see Connection Request Policies.

To specify NPS or other RADIUS servers to which authentication requests are forwarded, see Remote RADIUS Server Groups

## Remote RADIUS Server Groups

6 out of 8 rated this helpful - Rate this topic

Updated: March 29, 2012

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

When you configure Network Policy Server (NPS) as a Remote Authentication Dial-In User Service (RADIUS) proxy, you use NPS to forward connection requests to RADIUS servers that are capable of processing the connection requests because they can perform authentication and authorization in the domain where the user or computer account is located. For example, if you want to forward connection requests to one or more RADIUS servers in untrusted domains, you can configure NPS as a RADIUS proxy to forward the requests to the remote RADIUS servers in the untrusted domain.

To configure NPS as a RADIUS proxy, you must create a connection request policy that contains all of the information required for NPS to evaluate which messages to forward and where to send the messages.

When you configure a remote RADIUS server group in NPS and you configure a connection request policy with the group, you are designating the location where NPS is to forward connection requests.

# Configuring RADIUS servers for a group

A *remote RADIUS server group* is a named group that contains one or more RADIUS servers. If you configure more than one server, you can specify load balancing settings to either determine

the order in which the servers are used by the proxy or to distribute the flow of RADIUS messages across all servers in the group to prevent overloading one or more servers with too many connection requests.

Each server in the group has the following settings:

- Name or address

  Each group member must have a unique name within the group. The name can be an IP address or a name that can be resolved to its IP address.

- Authentication and accounting

  You can forward authentication requests, accounting requests, or both to each remote RADIUS server group member.

- Load balancing

  A priority setting is used to indicate which member of the group is the primary server (the priority is set to 1). For group members that have the same priority, a weight setting is used to calculate how often RADIUS messages are sent to each server. You can use additional settings to configure the way in which the NPS server detects when a group member first becomes unavailable and when it becomes available after it has been determined to be unavailable.

After a remote RADIUS server group is configured, it can be specified in the authentication and accounting settings of a connection request policy. Because of this, you can configure a remote RADIUS server group first. Next, you can configure the connection request policy to use the newly configured remote RADIUS server group. Alternatively, you can use the New Connection Request Policy Wizard to create a new remote RADIUS server group while you are creating the connection request policy.

**Note**

Remote RADIUS server groups are unrelated to and separate from Windows groups and Network Access Protection (NAP) remediation server groups.