

Connection Request Policies



- NPS (Local)
 - RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Server Groups
 - Policies
 - Connection Request Policies**
 - Network Policies
 - Health Policies
 - Network Access Protection
 - Accounting
 - Templates Management
 - Shared Secrets
 - RADIUS Clients
 - Remote RADIUS Servers
 - IP Filters
 - Health Policies
 - Remediation Server Groups

Connection Request Policies



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Order	Source
Microsoft Routing and Remote Access Service Policy	Enabled	1	Remote Access Server(VPN-Dial up)
Secure Wireless Connections	Enabled	2	Unspecified
Virtual Private Network (VPN) Connections	Enabled	3	Remote Access Server(VPN-Dial up)
NAP DHCP	Enabled	4	DHCP Server
NAP DHCP 2	Enabled	5	DHCP Server

Conditions - If the following conditions are met:

Condition	Value

Settings - Then the following settings are applied:

Setting	Value



NPS (Local)

- └─ RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Server Groups
- └─ Policies
 - Connection Request Policies
 - Network Policies
 - Health Policies
- └─ Network Access Protection
- └─ Accounting
- └─ Templates Management
 - Shared Secrets
 - RADIUS Clients
 - Remote RADIUS Servers
 - IP Filters
 - Health Policies
 - Remediation Server Groups

New
Export List
View ▶
Refresh
Help



Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applied.

Policy name:

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

 Unspecified

File Action View Help

NPS (Local)

- RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Servers
- Policies
 - Connection Request Policies
 - Network Policies
 - Health Policies
- Network Access Protection
 - Accounting
- Templates Management
 - Shared Secrets
 - RADIUS Clients
 - Remote RADIUS Servers
 - IP Filters
 - Health Policies
 - Remediation Server Groups



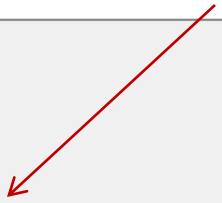
Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value	

Condition description:





Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

Select a condition, and then click Add.

HCAP



Location Groups

The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

User Name



User Name

The user name that is used 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.

Connection Properties



Access Client IPv4 Address

The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.



Access Client IPv4 Address

The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.



Access Client IPv6 Address

The Access Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access from the RADIUS client.



Framed Protocol

The Framed Protocol condition restricts the policy to only clients specifying a certain framing protocol for incoming packets, such as PPP or SLIP.



Service Type

The Service Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or Point to Point Protocol connections.

Select a condition, and then click Add.



Tunnel Type

The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.

Day and time restrictions



Day and Time Restrictions

Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

Identity Type



Identity Type

The Identity Type condition restricts the policy to only clients that can be identified through the specified mechanism, such as NAP statement of health (SoH).

RADIUS Client Properties



Calling Station ID

The Calling Station ID condition specifies the network access server telephone number dialed by the access client.

Gateway



Called Station ID

The Called Station ID condition specifies a character string that is the telephone number of the network access server (NAS). You can use pattern matching syntax to specify area codes.



NAS Identifier

The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.



NAS IPv4 Address

The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.



NAS IPv6 Address

The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.



NAS Port Type

The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

New Connection Request Policy



Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

Select a condition, and then click Add.



Tunnel Type

The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.

[Day and time restrictions](#)



Day and Time Restrictions

Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

[Identity Type](#)



Identity Type

The Identity Type condition restricts the policy to only clients that can be identified through the specified mechanism, such as NAP statement of health (SoH).

[RADIUS Client Properties](#)



Calling Station ID

The Calling Station ID condition specifies the network access server telephone number dialed by the access client.



Client Friendly Name

The Client Friendly Name condition restricts the policy to only clients that have a specific RADIUS Client Friendly Name or Client Name.

Day and time restrictions



12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12

All	12	2	4	6	8	10	12	2	4	6	8	10	12
Sunday													
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													

OK

Cancel

- Permitted
- Denied

Sunday through Saturday from 12:00 AM to 12:00 AM


New Connection Request Policy



Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
 Day and time restri...	Monday 04:00-19:00 Tuesday 04:00-19:00

Condition description:

Add...

Edit..

Remove

Previous

Next

Finish

Cancel



Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request

→ Authentication

Accounting

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

- Authenticate requests on this server
- Forward requests to the following remote RADIUS server group for authentication:

rgroup



New...

- Accept users without validating credentials

Previous

Next

Finish

Cancel

New Connection Request Policy



Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request

→ Authentication

Accounting

RADIUS accounting allows you to record user authentication and accounting requests in a log file or to a SQL Server database. To forward accounting requests to remote RADIUS servers, specify a remote RADIUS server group.

Forward accounting requests to this remote RADIUS server group

rgroup



New...

Previous

Next

Finish

Cancel

New Connection Request Policy



Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.

If conditions match the connection request and the policy grants access, settings are applied.

Settings:

Specify a Realm Name

Attribute

RADIUS Attributes

Standard

Vendor Specific

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute:

Rules:

Find	Replace With	
		<input type="button" value="Add"/>
		<input type="button" value="Edit"/>
		<input type="button" value="Remove"/>
		<input type="button" value="Move Up"/>
		<input type="button" value="Move Down"/>

Previous

Next

Finish

Cancel



Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

class connection request policy

Policy conditions:

Condition	Value
Day and time restrictions	Monday 04:00-19:00 Tuesday 04:00-19:00

Policy settings:

Condition	Value
Authentication Provider	Forwarding Request
Authentication Provider Name	rgroup
Accounting Provider Name	rgroup

To close this wizard, click Finish.

Previous

Next

Finish

Cancel