ManageEngine
ADSelfService Plus

NPS configuration for Endpoint MFA

NPS configuration for Endpoint MFA

ADSelfService Plus adds an extra step of authentication for VPN and endpoint logins that use RADIUS authentication (like Microsoft Remote Desktop Gateway, VMware Horizon View, etc.) for enhanced security.

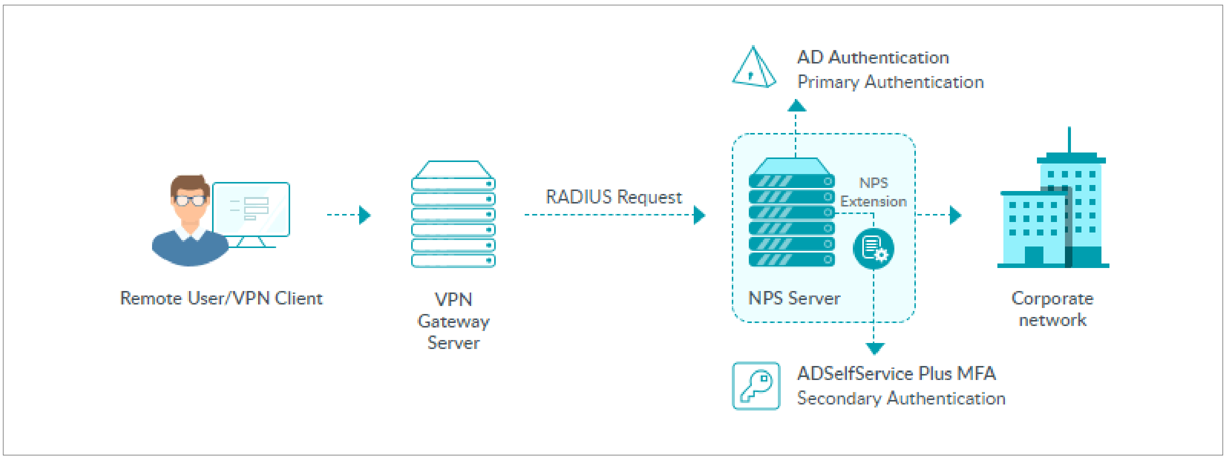
How it works

This process requires three entities that need to be configured to work with each other. They are:

1. ADSelfService Plus with Endpoint MFA is required to enable multi-factor authentication (MFA) for VPN and RADIUS-supported endpoint logins. Visit the store to purchase Endpoint MFA.
2. An NPS server.
3. A VPN gateway server (or any other RADIUS endpoints).

ADSelfService Plus comes bundled with an NPS extension, which should be installed in your NPS server. This extension facilitates communication between the NPS server and ADSelfService Plus for MFA during VPN logins. To achieve this, the VPN gateway or other endpoints will need to authenticate with the NPS via RADIUS protocol.

Once the VPN or endpoint (Microsoft RD Gateway, VMware Horizon View, etc.) server is configured to use RADIUS authentication and the NPS extension is installed in the RADIUS server, here is how the authentication process will work:



VPN MFA Authentication

1. A user tries to establish a connection by providing their username and password to the VPN or endpoint server.
2. The VPN server converts the request to a RADIUS Access-Request message and sends it to the NPS server where the ADSelfService Plus NPS extension is installed.
3. If the username and password combination is correct, the NPS extension triggers a request for second-factor authentication with the ADSelfService Plus server.
4. ADSelfService Plus performs the secondary authentication and sends the result to the NPS extension in the NPS server.
5. If the authentication is successful, the NPS server sends a RADIUS Access-Accept message to the VPN or endpoint server.
6. The user is granted access to the VPN or endpoint server and establishes an encrypted tunnel to the internal network.

Configuration steps

✓ **NPS installation and configuration:**

1. Installing the NPS service
2. Registering the NPS in Active Directory
3. Configuring the NPS service

✓ **Configuration at the VPN gateway (or other endpoints):**

1. Configuring the VPN server to use RADIUS authentication

✓ **ADSelfService Plus configuration:**

1. Enabling the required authenticators
2. Enabling MFA for VPN logins in ADSelfService Plus
3. Installing the NPS extension

NPS Installation and Configuration

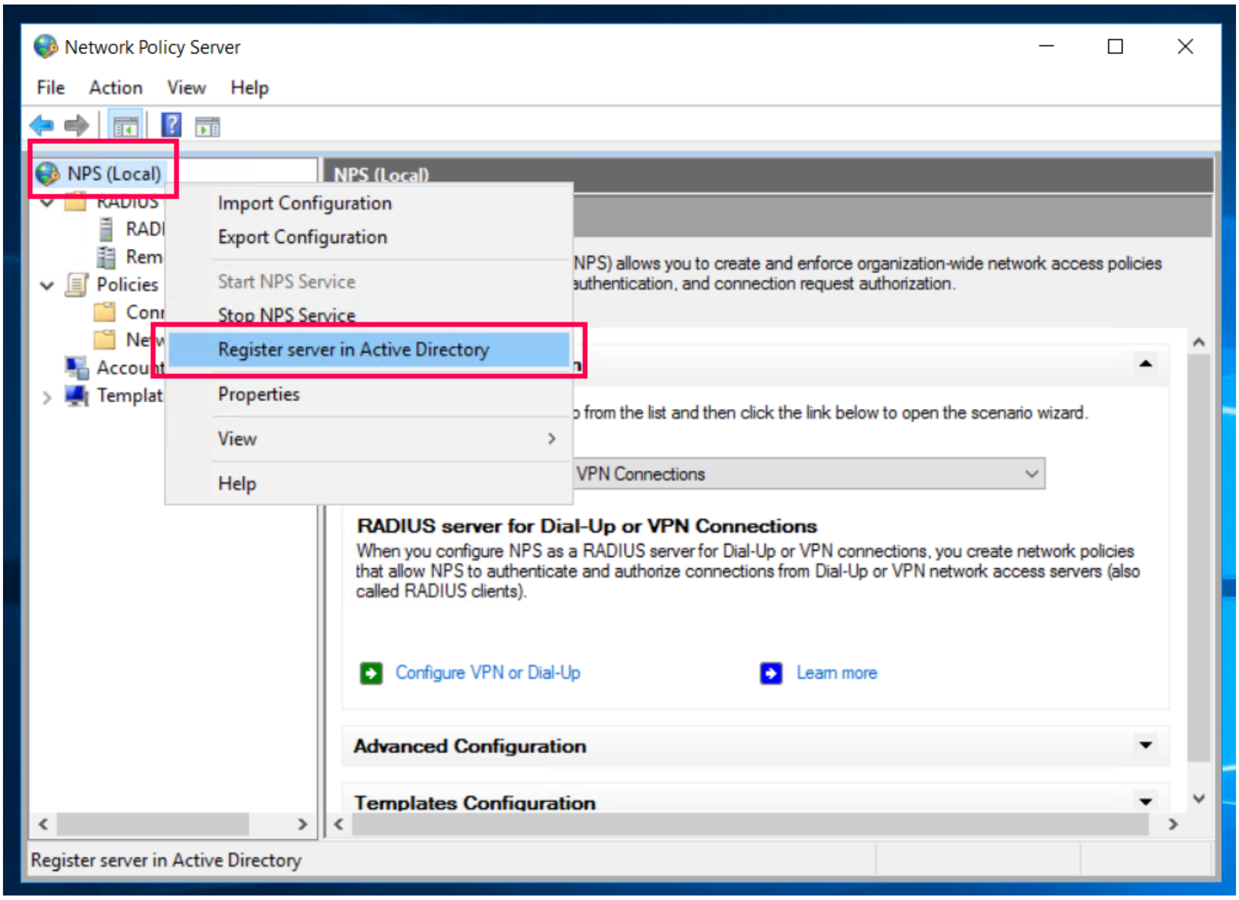
1. Installing the NPS service

You can follow the official Microsoft guide to install the NPS service on your server. This must be a Windows server (Windows Server 2008 R2 and above) with NPS role enabled.

2. Registering the NPS server in Active Directory

For the correct functionality of RADIUS authentication, the NPS server must be registered in Active Directory. Only then can it authenticate credentials.

Step 1: From the main NPS screen of NPS, right-click *NPS (local)* and select **Register server in Active Directory.**



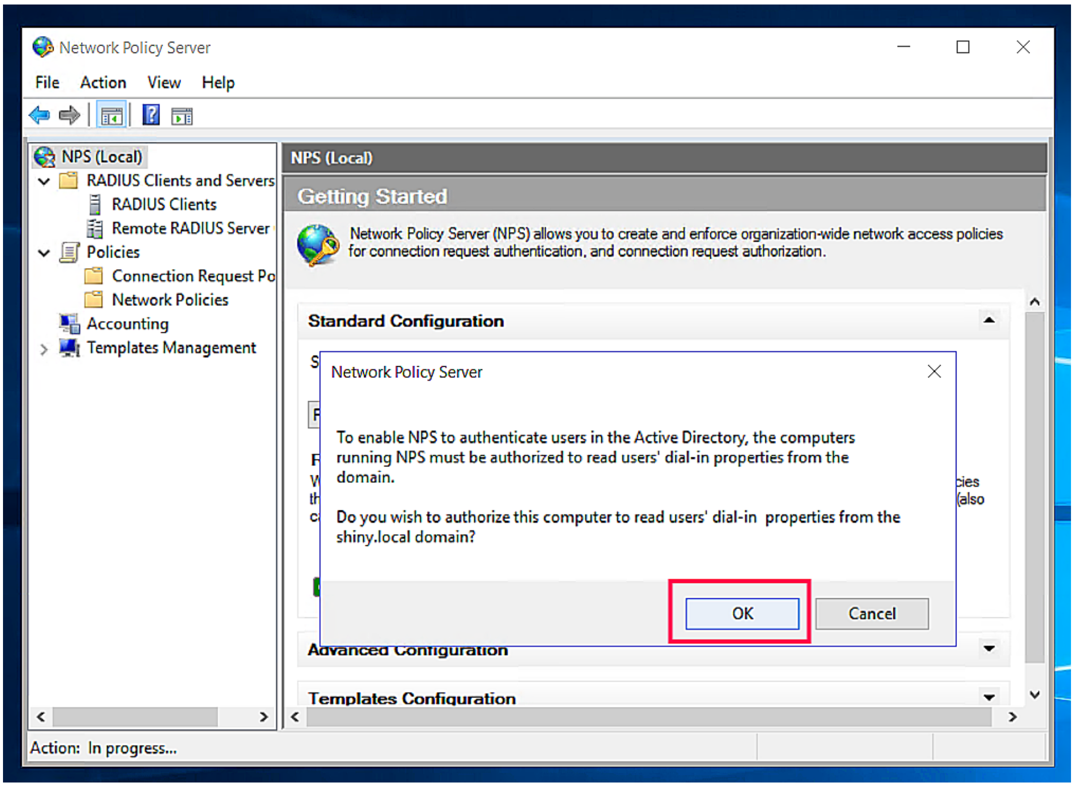
NPS) allows you to create and enforce organization-wide network access policies
authentication, and connection request authorization.

from the list and then click the link below to open the scenario wizard.

RADIUS server for Dial-Up or VPN Connections

When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).

Step 2: Click **OK** to authorize the local server in Active Directory.



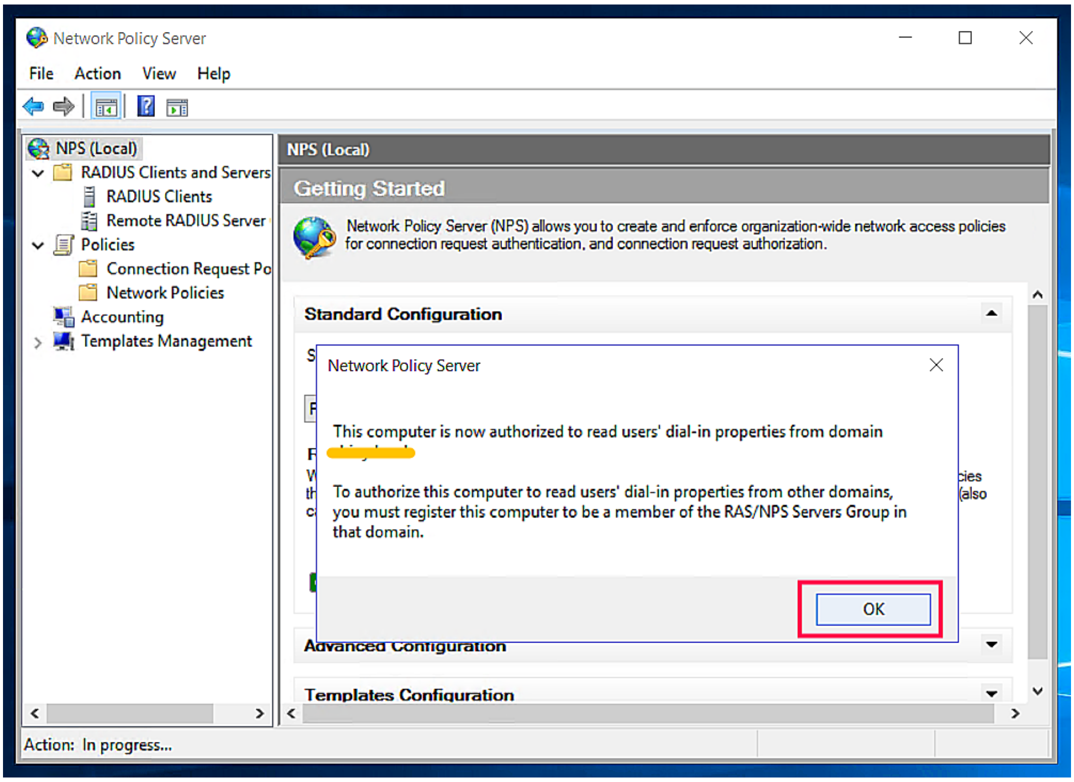
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.

Network Policy Server

To enable NPS to authenticate users in the Active Directory, the computers running NPS must be authorized to read users' dial-in properties from the domain.

Do you wish to authorize this computer to read users' dial-in properties from the shiny.local domain?

Step 3: Click **OK** again.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.

Network Policy Server

This computer is now authorized to read users' dial-in properties from domain [redacted]

To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/NPS Servers Group in that domain.

The NPS server will now be registered in Active Directory.

3. NPS Configuration

Configuring the NPS service involves three stages:

Stage 1: Registering your VPN Gateway server as a RADIUS client.

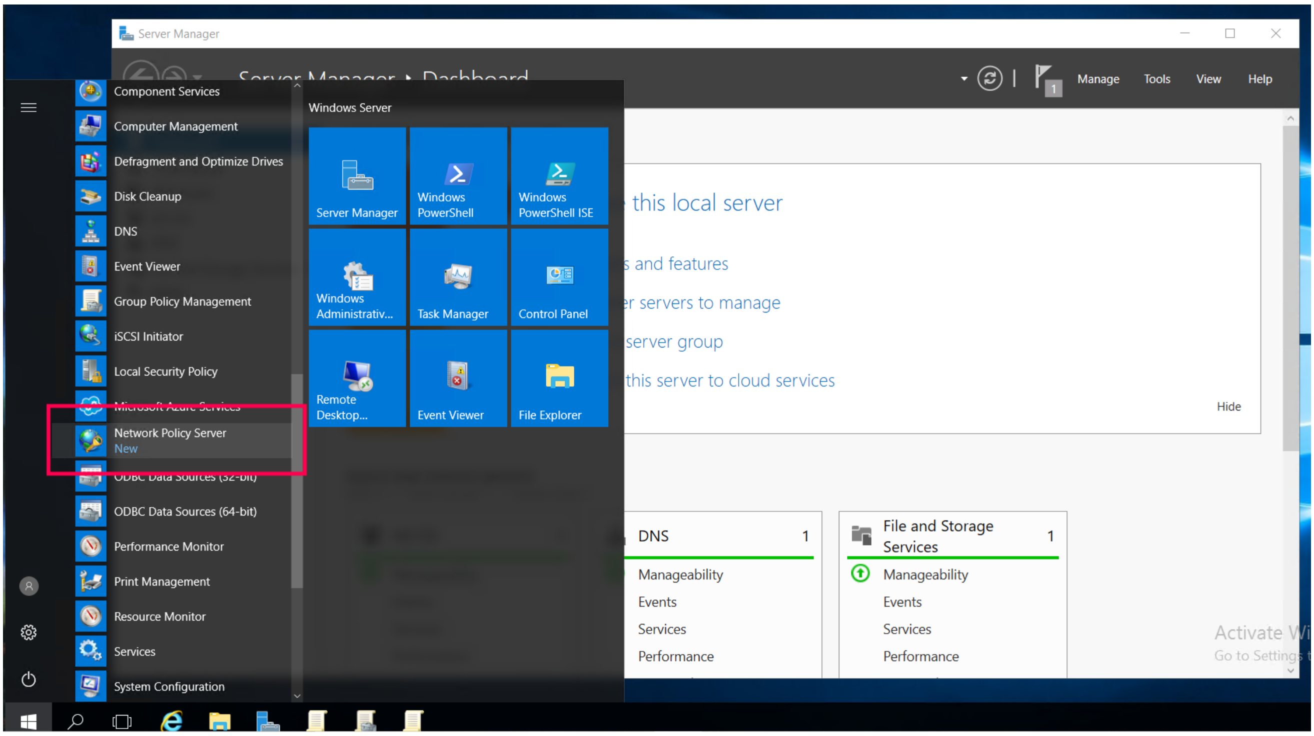
Stage 2: Configuring a Connection Request policy for your VPN Gateway server.

Stage 3: Configuring a Network policy to authorize the requests with conditions.

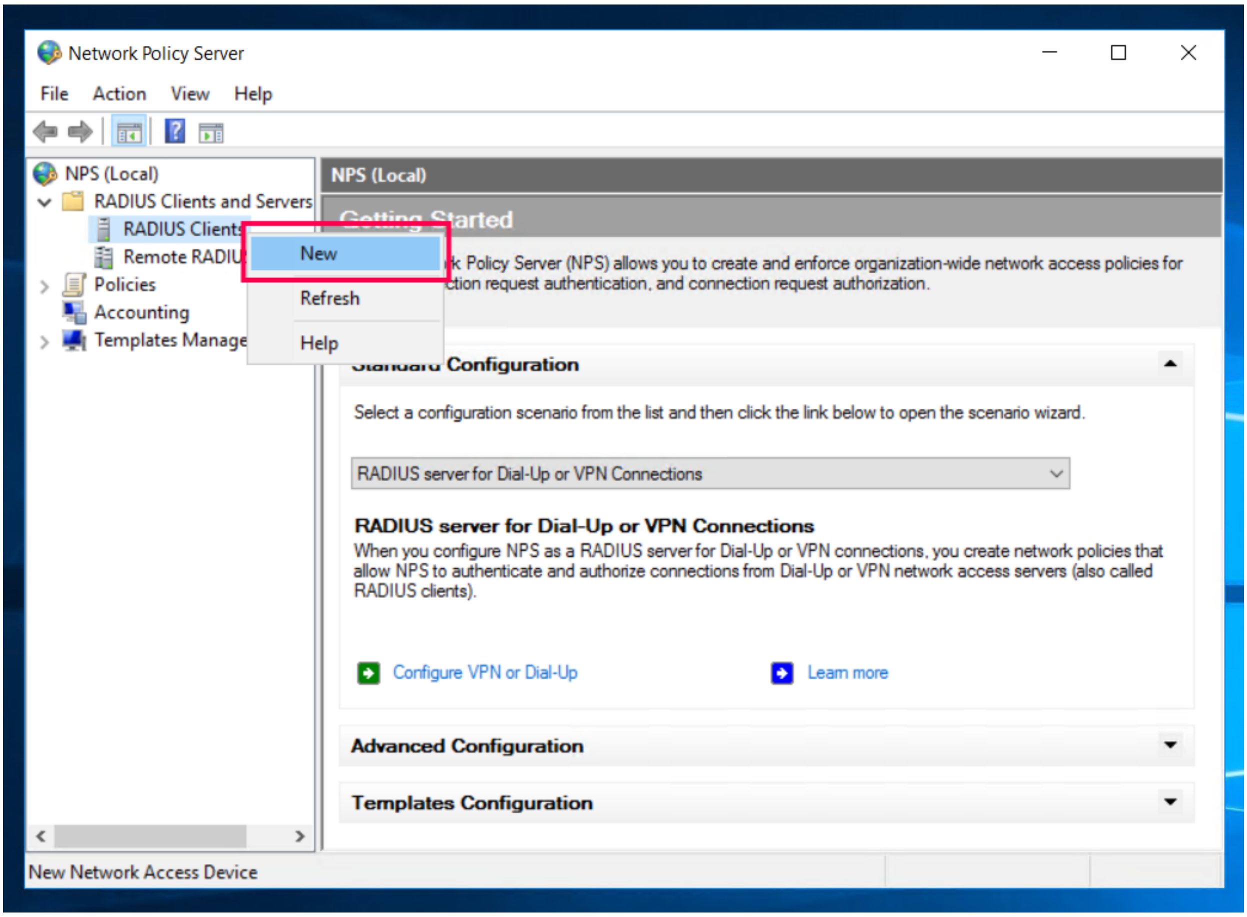
Stage 1: Registering your VPN gateway server as a RADIUS client

In this stage, you will configure the VPN gateway server as a RADIUS client such that the NPS receives the RADIUS access requests from the VPN gateway server.

Step 1: Go to **Start → Windows Administrative tools → Network Policy server.**



Step 2: In the *Network Policy Server* window that opens, expand **RADIUS Clients and Servers**, then right-click on **RADIUS Clients** and select **New.**



k Policy Server (NPS) allows you to create and enforce organization-wide network access policies for ction request authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

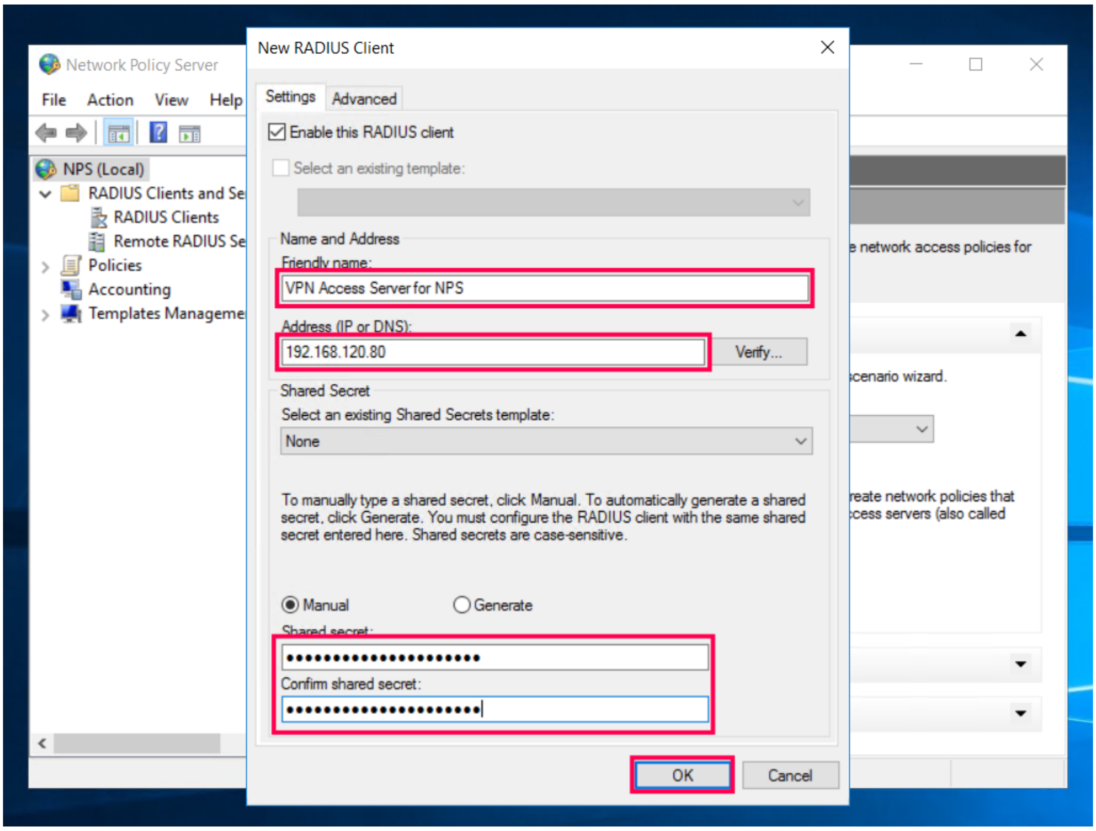
RADIUS server for Dial-Up or VPN Connections

RADIUS server for Dial-Up or VPN Connections

When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).

Step 3: In the *New RADIUS Client* window:

- Select **Enable this RADIUS client**. This is to ensure that authentication requests are processed on this NPS.
- Add a **Friendly name** that makes the intended use clear.
- Enter the **IP Address** or **DNS address** of the VPN gateway server.
- Choose to **Manual** or **Generate** for the **Shared Secret**, then copy it.
- Click **OK.**



New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: VPN Access Server for NPS

Address (IP or DNS): 192.168.120.80

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••••••••••••

Confirm shared secret: ••••••••••••••••••••

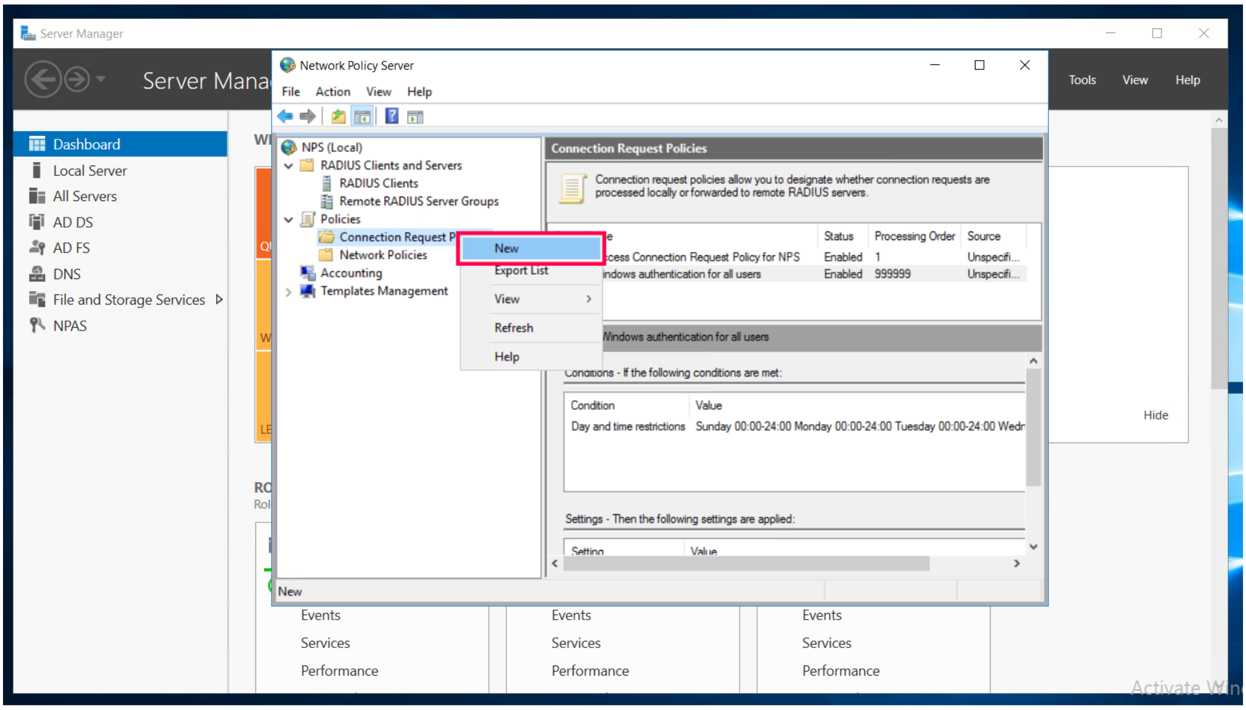
Now the VPN server has been configured as a RADIUS client. Next, you will need to edit the Connection Request Policy and the Network Policy.

Stage 2: Configuring a Connection Request policy for your VPN Gateway server

A Connection Request Policy defines how authentication should happen for the incoming RADIUS requests. Since you need the authentication to happen on the server you are configuring, you need to specify this in the Connection Request policy.

Step 1: In the *Network Policy Server* window, expand **Policies,** then right-click **Connection Request Policy → New.**

Note: You can also modify an existing policy if you require it to work with your VPN server.



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

…e	Status	Processing Order	Source
…cess Connection Request Policy for NPS	Enabled	1	Unspecifi…
…indows authentication for all users	Enabled	999999	Unspecifi…

…Windows authentication for all users

Conditions - If the following conditions are met:

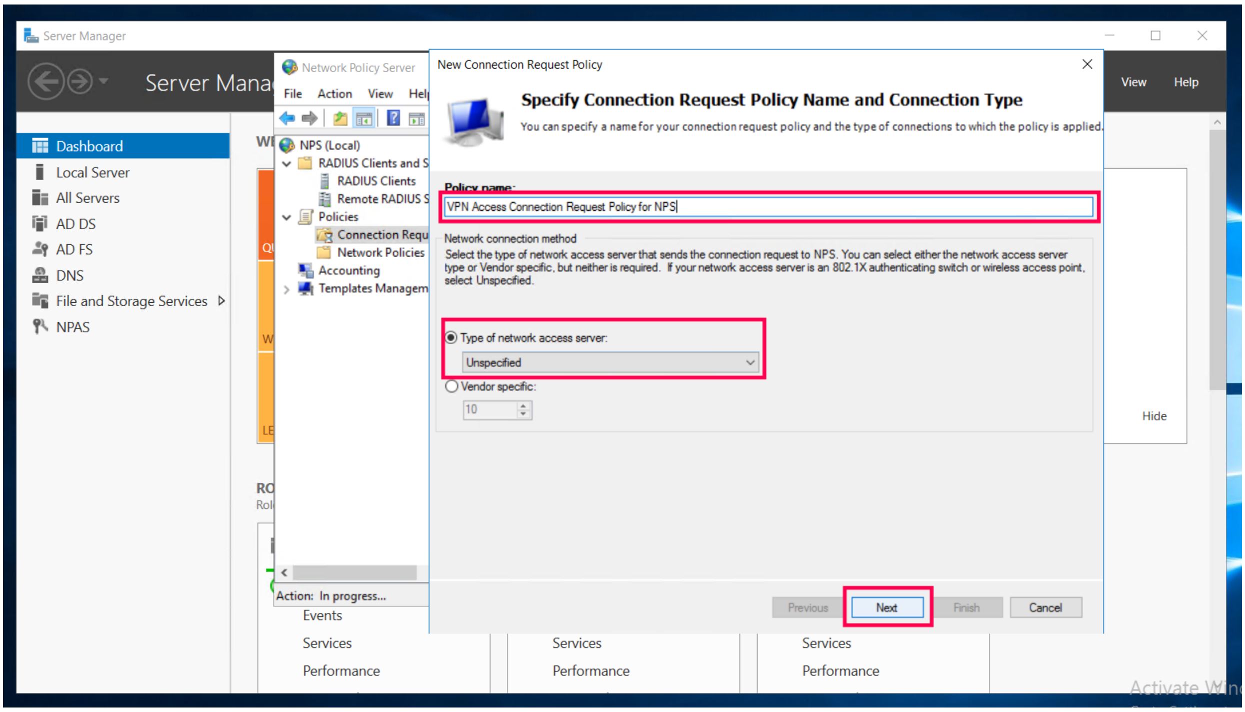
Condition	Value
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wedr…

Settings - Then the following settings are applied:

Setting	Value

New

Step 2: Leave the *Type* of network access server field **Unspecified.**



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:
VPN Access Connection Request Policy for NPS

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

○ Vendor specific:
10

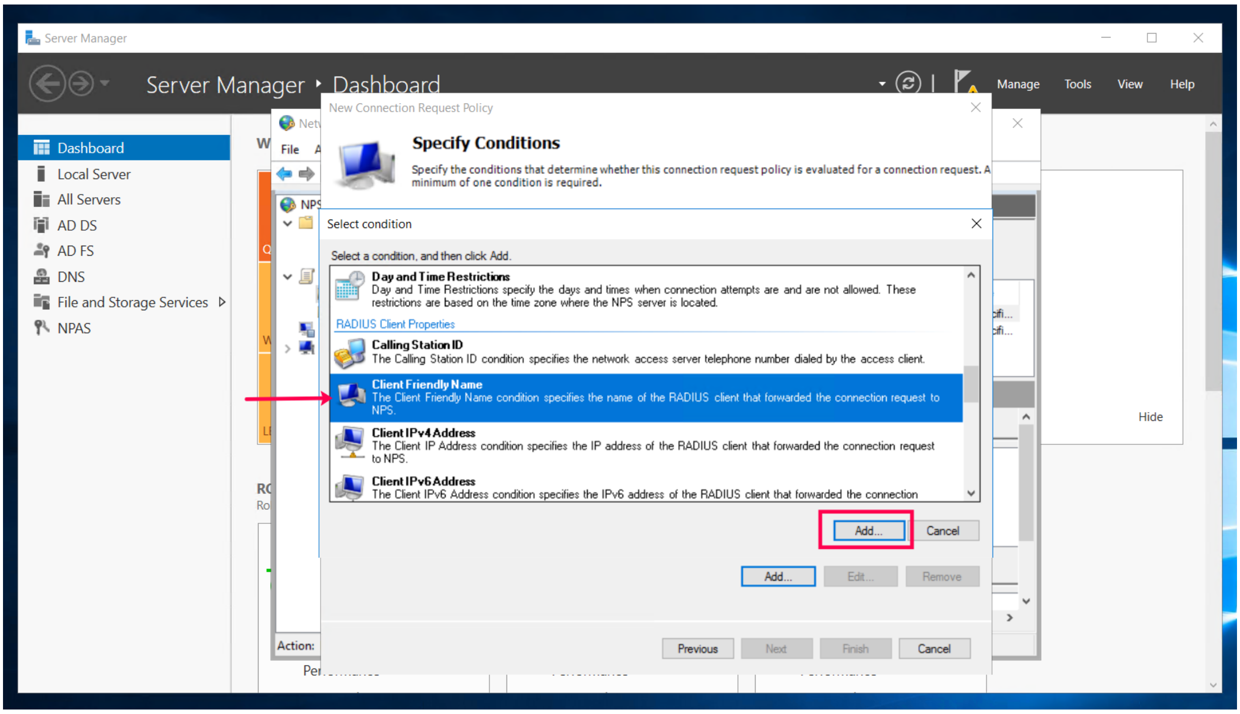
Action: In progress...

Step 3: Specify the conditions for when this connection request policy is evaluated for a connection request. These conditions depend on your organization's policies. A minimum of one condition is required.

For instance, you can add a friendly name for the RADIUS client for the RADIUS client configured during Stage 1.

Adding a friendly name:

Step 3a: Click on **Client Friendly Name** and click **Add.**



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.

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.

RADIUS Client Properties

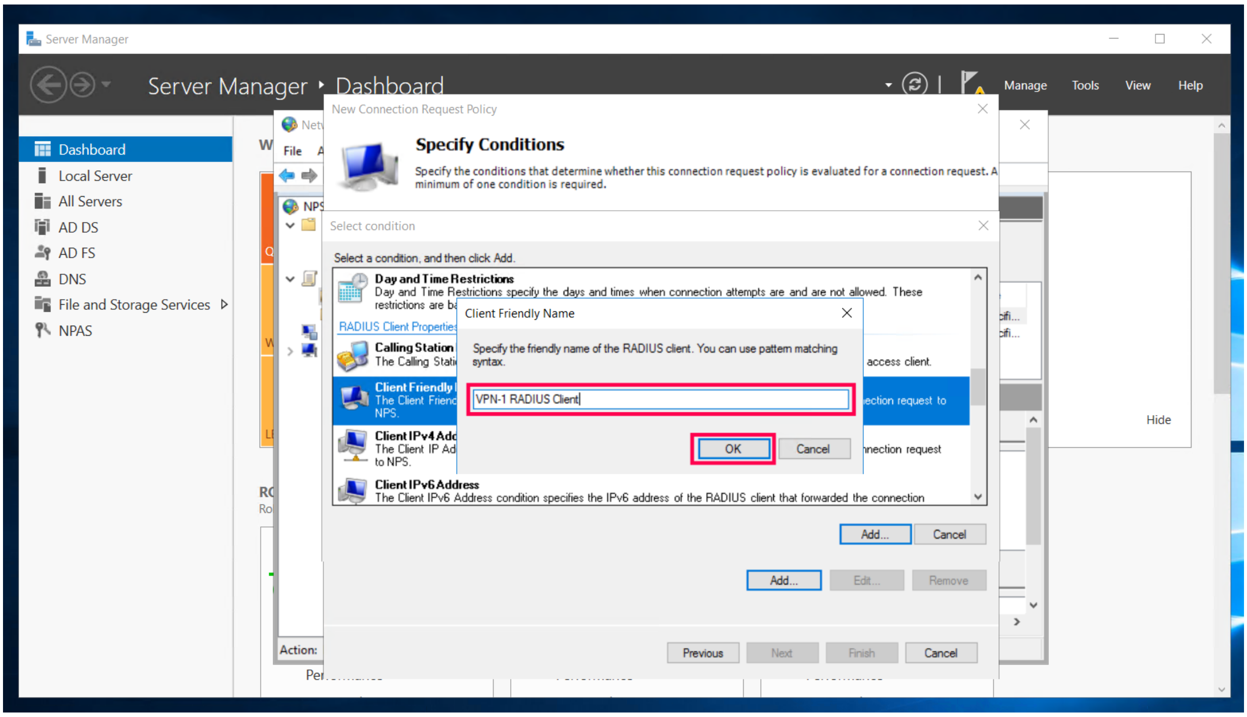
Calling Station ID
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.

Client Friendly Name
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.

Client IPv4 Address
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

Client IPv6 Address
The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the connection

Step 3b: Enter a relevant friendly name for the RADIUS client and click **OK**. This condition will be added to the policy.

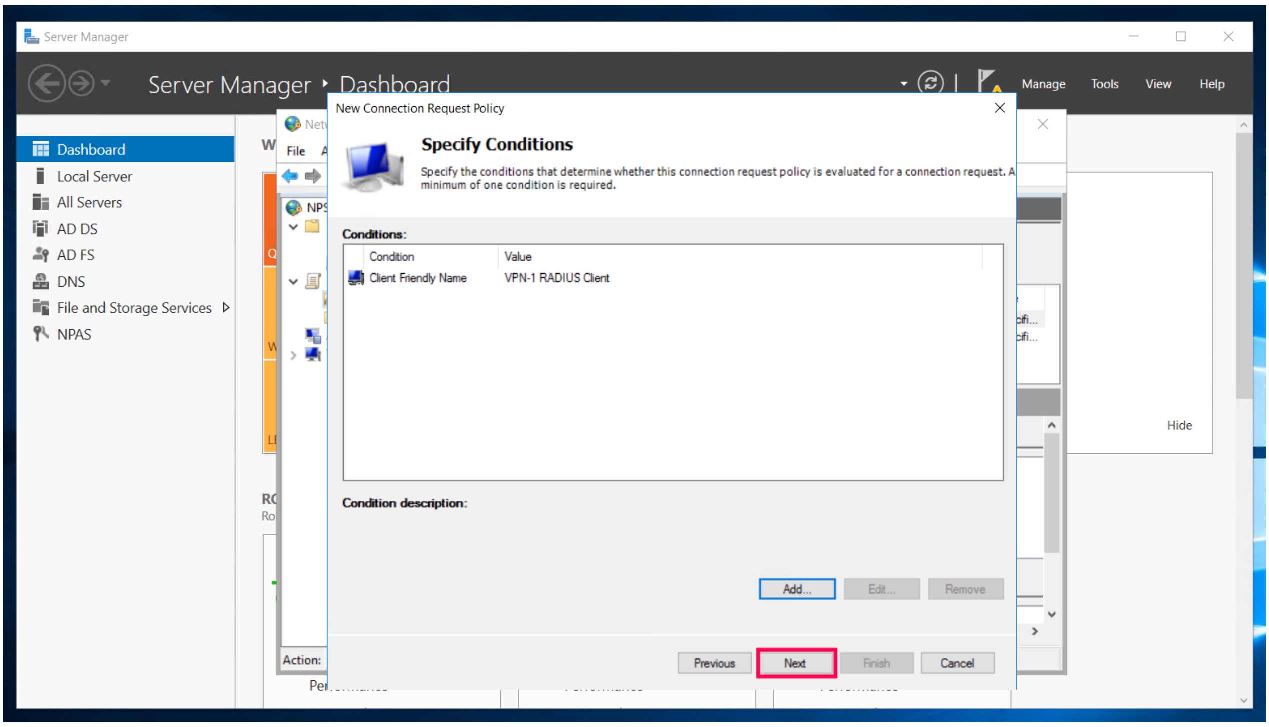


Client Friendly Name

Specify the friendly name of the RADIUS client. You can use pattern matching syntax.

VPN-1 RADIUS Client

Step 3c: You can add any other organization-specific conditions you might require. Once done, click **Next.**


New Connection Request Policy

Specify Conditions

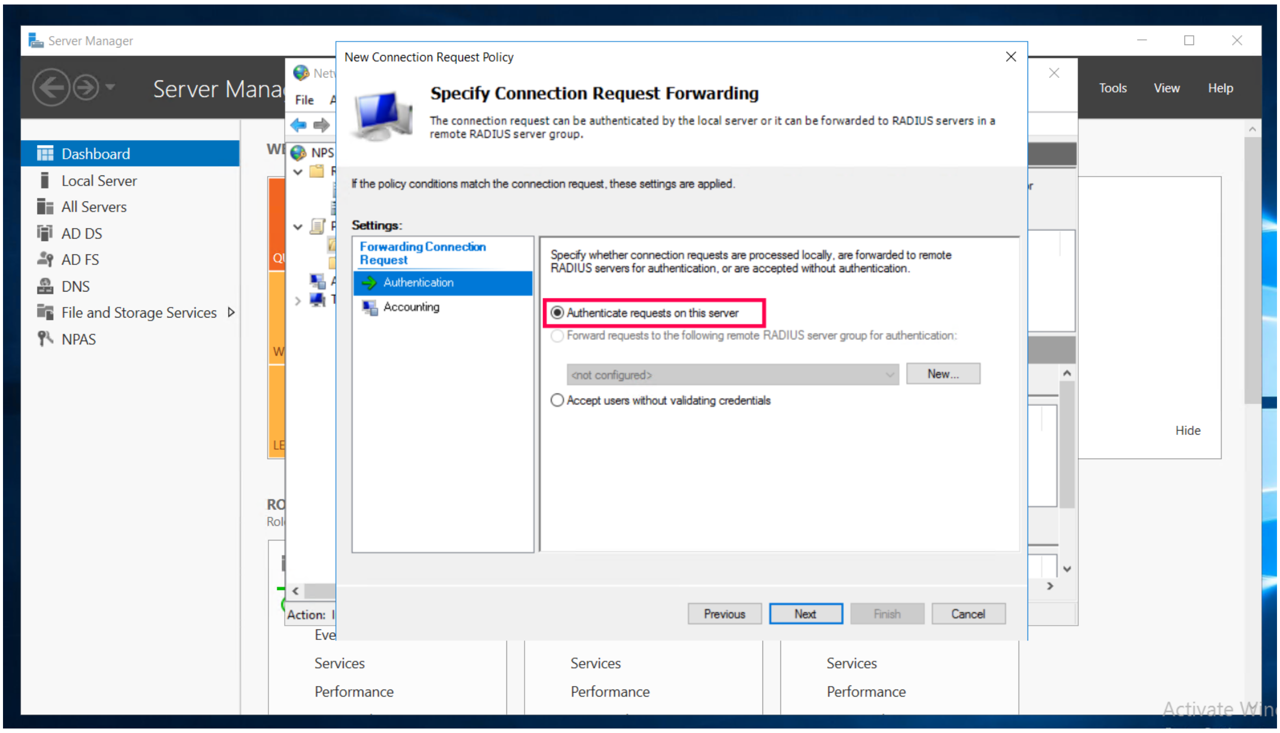
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
Client Friendly Name	VPN-1 RADIUS Client

Condition description:

Step 4: In the *Specify Connection Request Forwarding* section, choose the **Authenticate requests on this server** option. This ensures that the authentication process happens on the server that you are configuring. Then click **Next.**


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

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

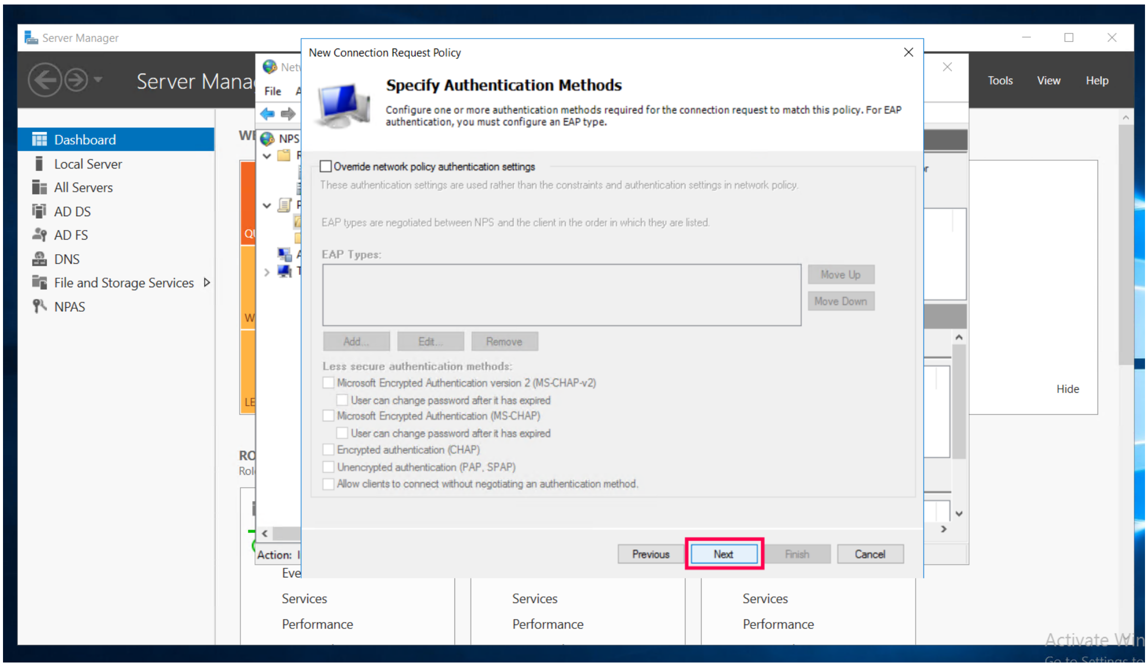
● Authenticate requests on this server

○ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

○ Accept users without validating credentials

Step 5: Leave the *Specify Authentication Methods* section untouched. Click **Next.**



New Connection Request Policy

Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

□ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

□ Encrypted authentication (CHAP)

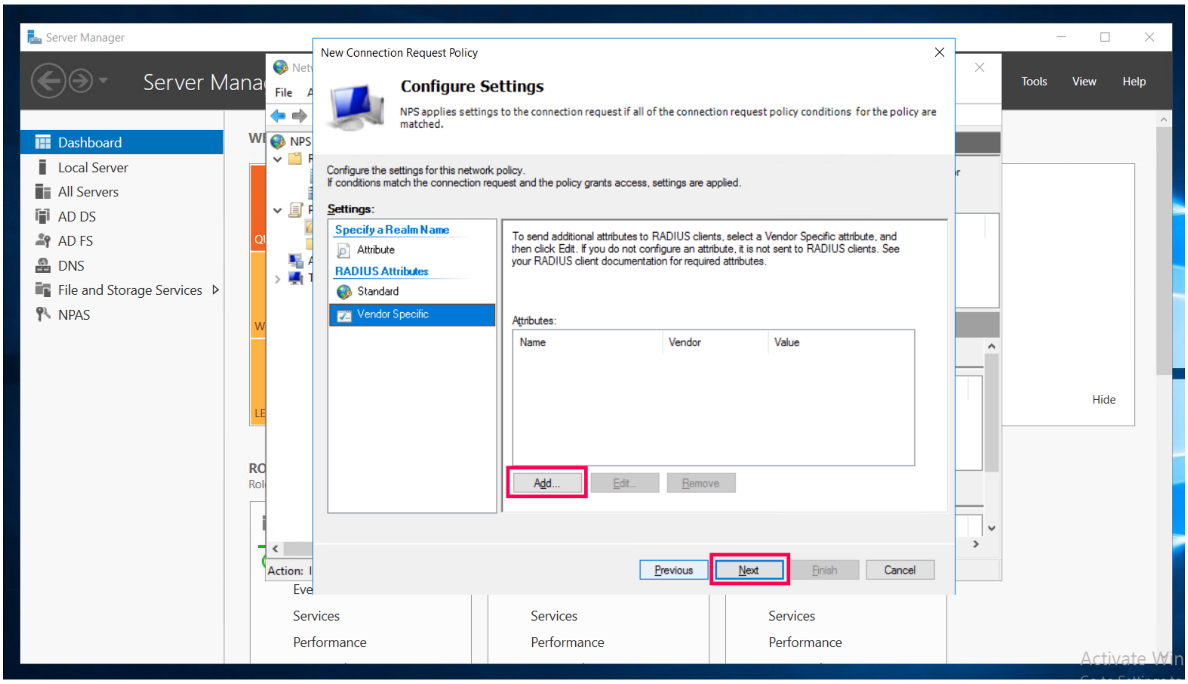
□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

Step 6: Add any vendor-specific conditions.

Note:

- Additional attributes can only be set for one-way MFA methods such as push notifications and biometrics.
- Additional attributes are incompatible with challenge-based MFA methods such as **Google Authenticator, Microsoft Authenticator, ZohoOneAuth, CustomTOTP, Yubikey,** etc. When challenge-based authenticators are used, the RADIUS attributes that are configured in the Network Policy won't be forwarded to the RADIUS client (VPN or endpoint server). As a result, the VPN client might either have more access than you want it to have, less access, or no access.



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.

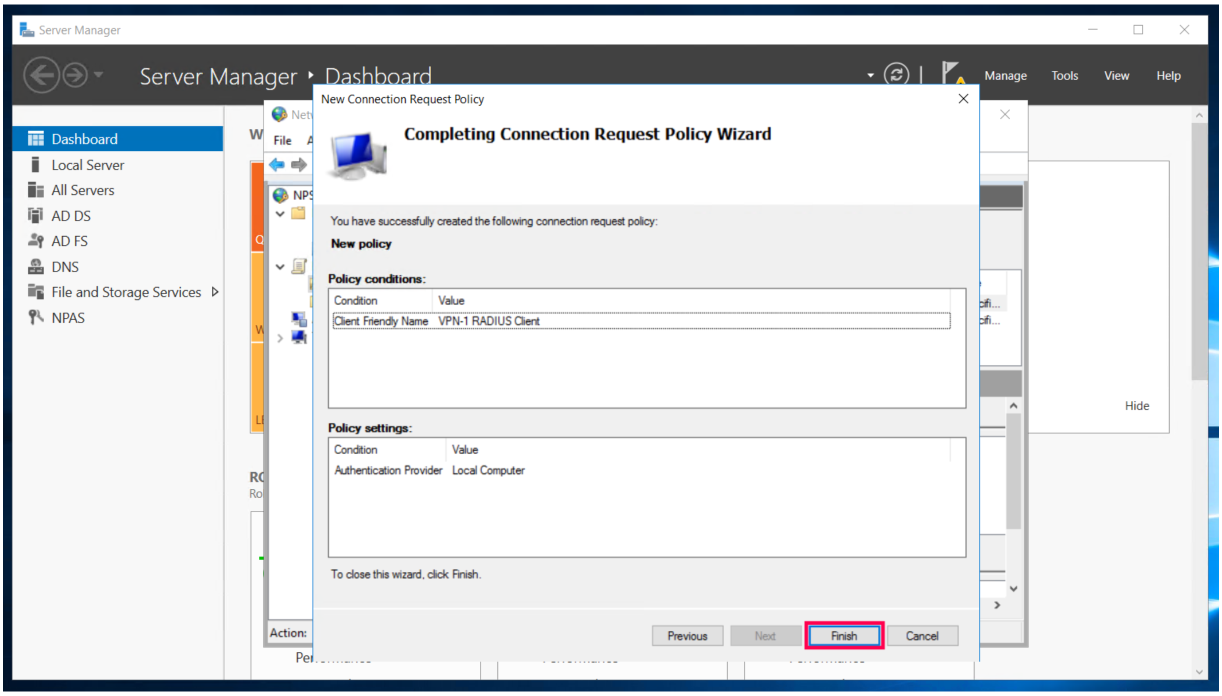
Settings:

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value

Step 7: Click **Finish.**



New Connection Request Policy

Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

New policy

Policy conditions:

Condition	Value
Client Friendly Name	VPN-1 RADIUS Client

Policy settings:

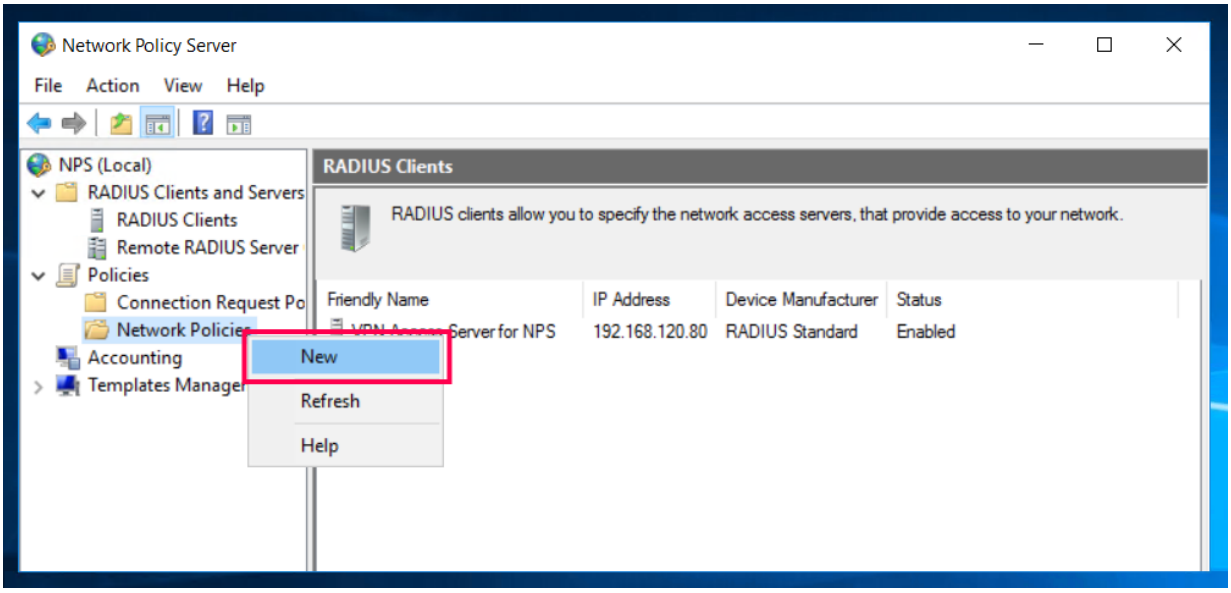
Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.

Stage 3: Configuring a Network policy to authorize the requests with conditions

Network Policies deal with authorization, meaning that these policies determine which parts of the network the user is authorized to access. Whenever a request meets and passes the conditions in the Connection Request policy, a user will be authenticated.

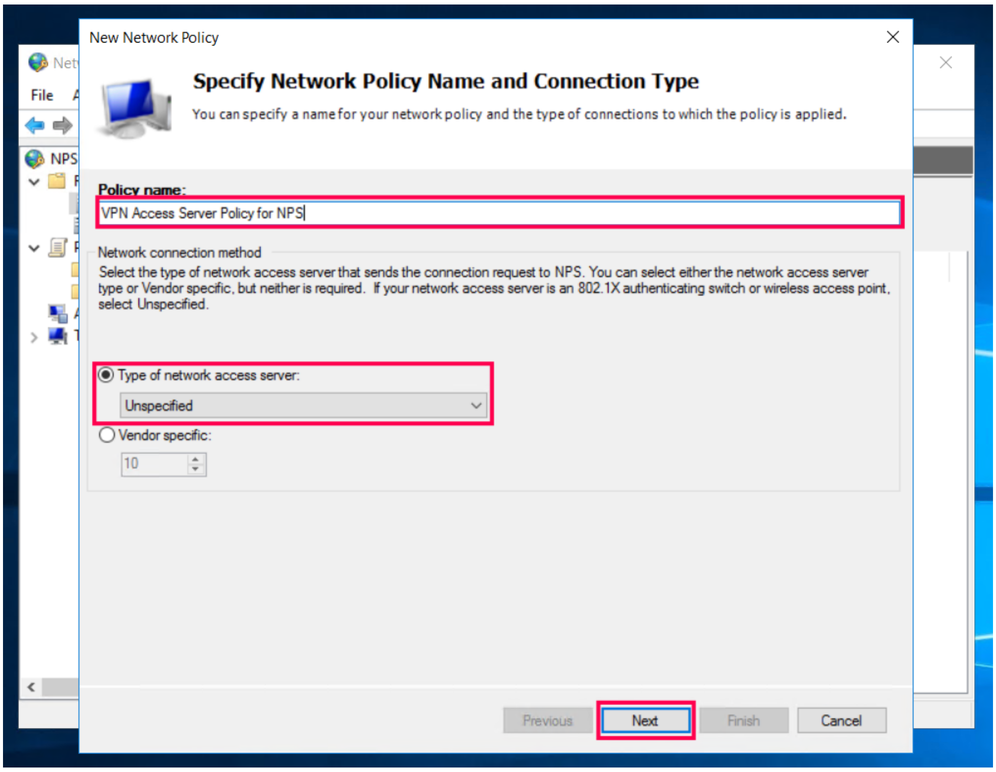
Step 1: Go to **Policies → Network Policies**. Right-click on **New.**



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	Status
VPN Access Server for NPS	192.168.120.80	RADIUS Standard	Enabled

Step 2: Specify the **Policy name**. Leave the connection type unspecified. Click **Next.**



New Network Policy

Specify Network Policy Name and Connection Type

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

Policy name:
VPN Access Server Policy for NPS

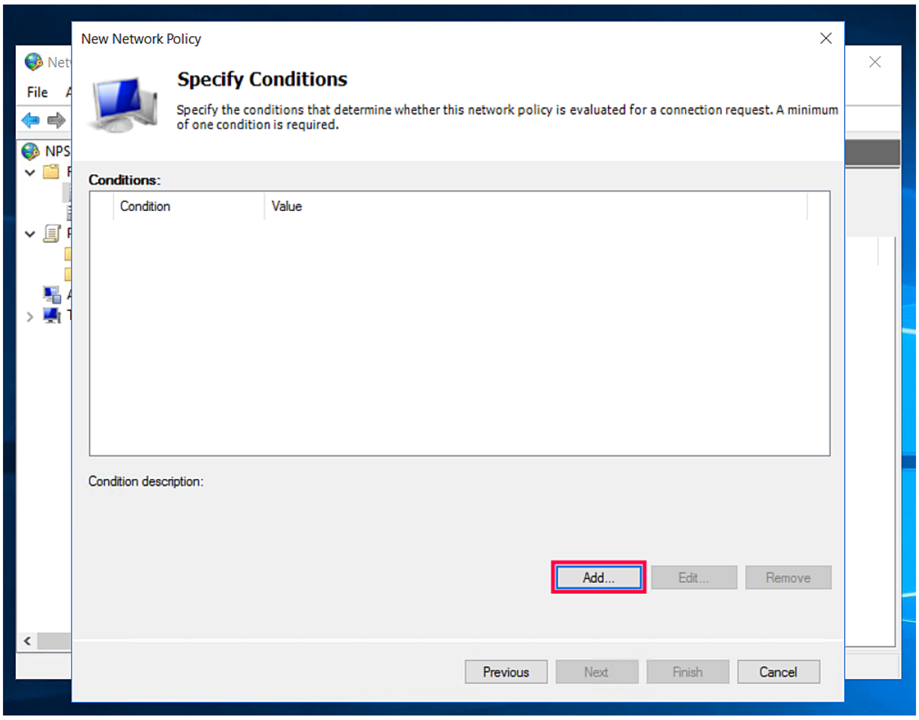
Network connection method

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

○ Vendor specific:
10

Step 3: On the *Specify Conditions* page, you can now configure access conditions based on your requirements. Click on **Add** to configure the access conditions. These conditions depend on your organizational policies.



New Network Policy

Specify Conditions

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

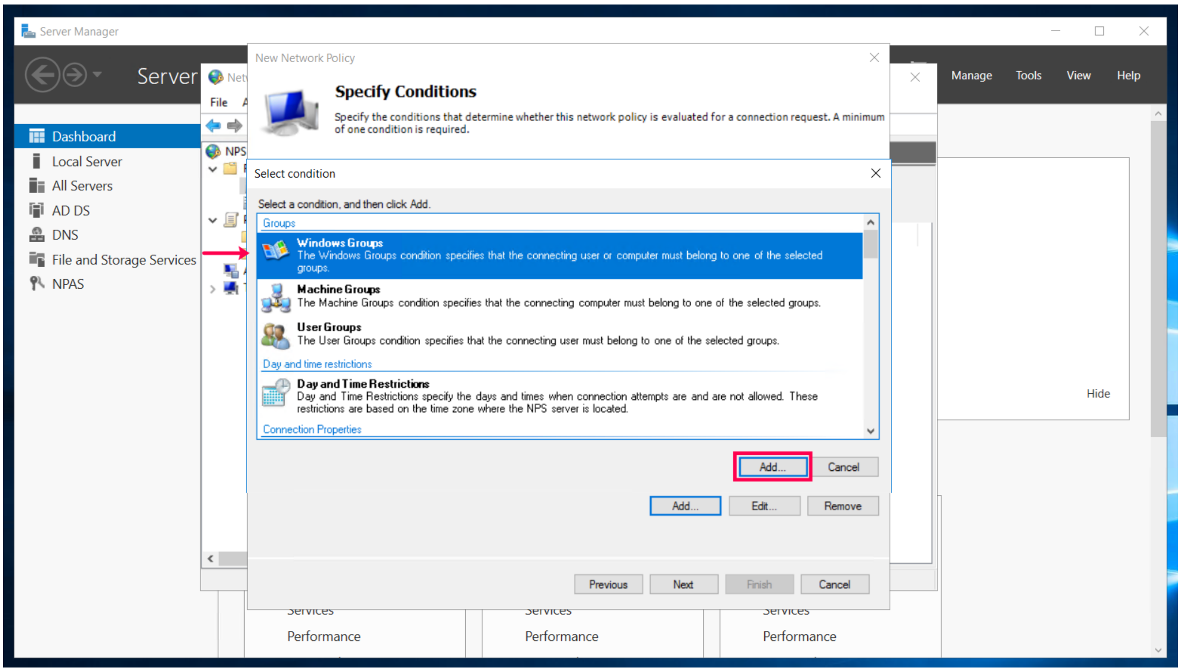
Conditions:

Condition	Value

Condition description:

For instance, if only members of a certain Active Directory group with VPN permissions need to be granted access:

Step 3a: Step 3a: Click on **Windows Groups → Add.**



Specify Conditions

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

Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

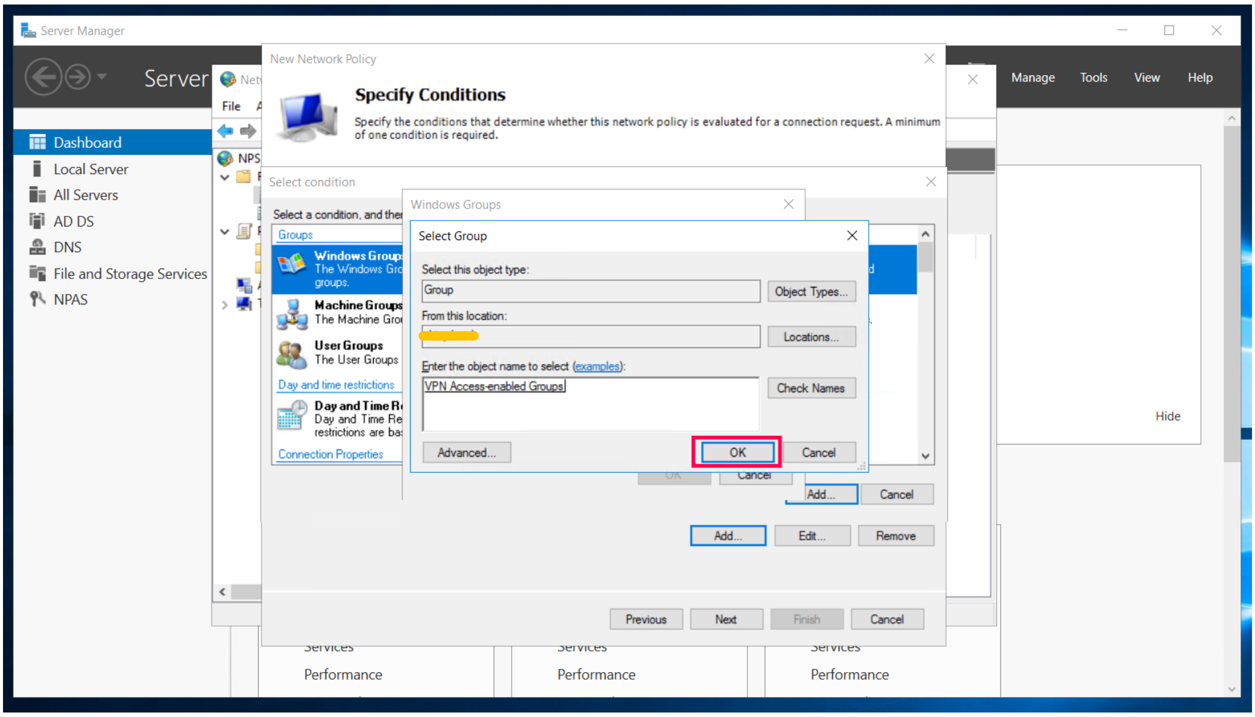
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

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.

Connection Properties

Step 3b: Specify the group to be granted access.



Specify Conditions

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

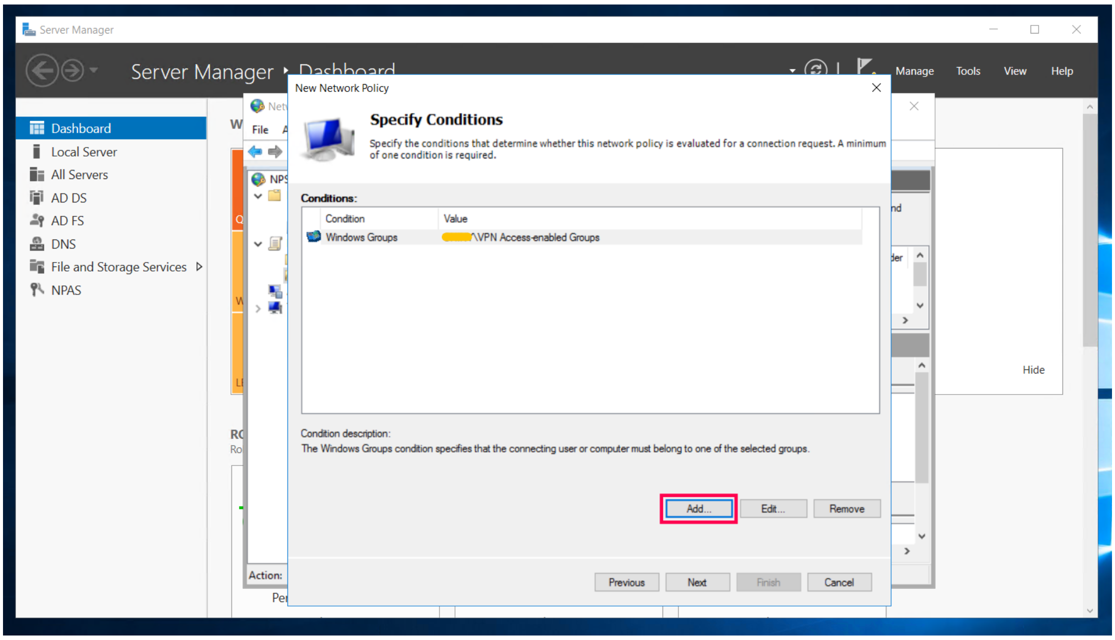
Select Group

Select this object type:
Group

From this location:
[redacted]

Enter the object name to select (examples):
VPN Access-enabled Groups

Step 3c: Click **OK**. Once all the access conditions you require are enabled, click **Next.**



New Network Policy

Specify Conditions

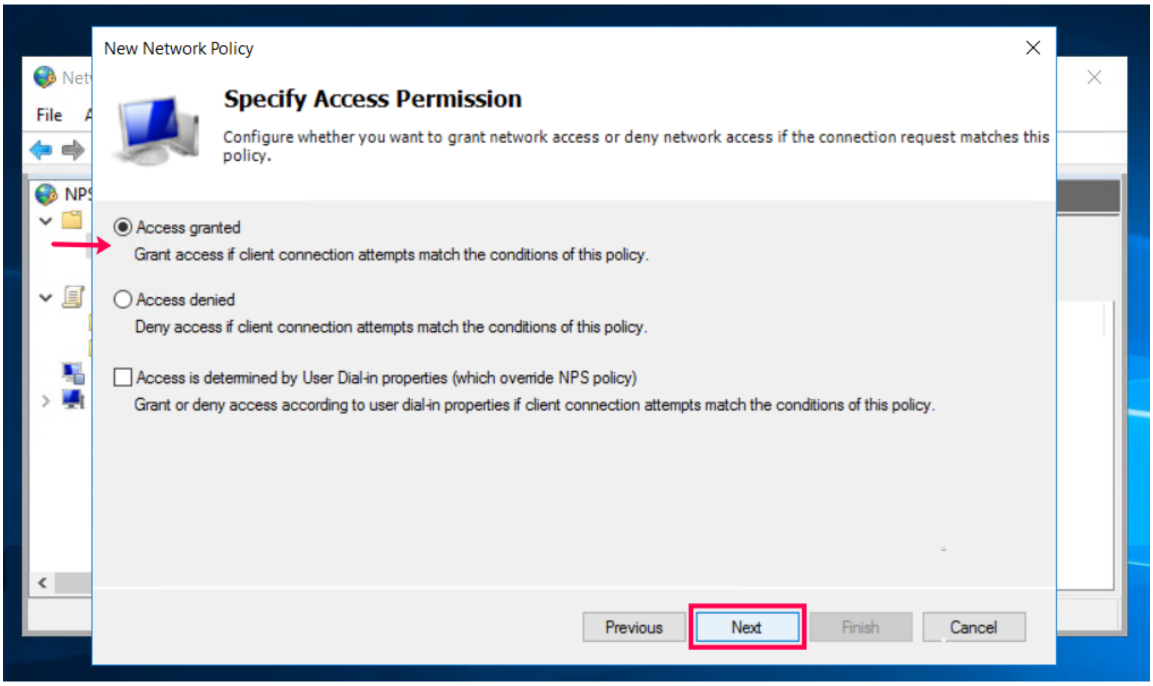
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
Windows Groups	[redacted]\VPN Access-enabled Groups

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Step 4: n the *Specify Access Permission* section, choose **Access Granted.** Click **Next.**



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● Access granted
Grant access if client connection attempts match the conditions of this policy.

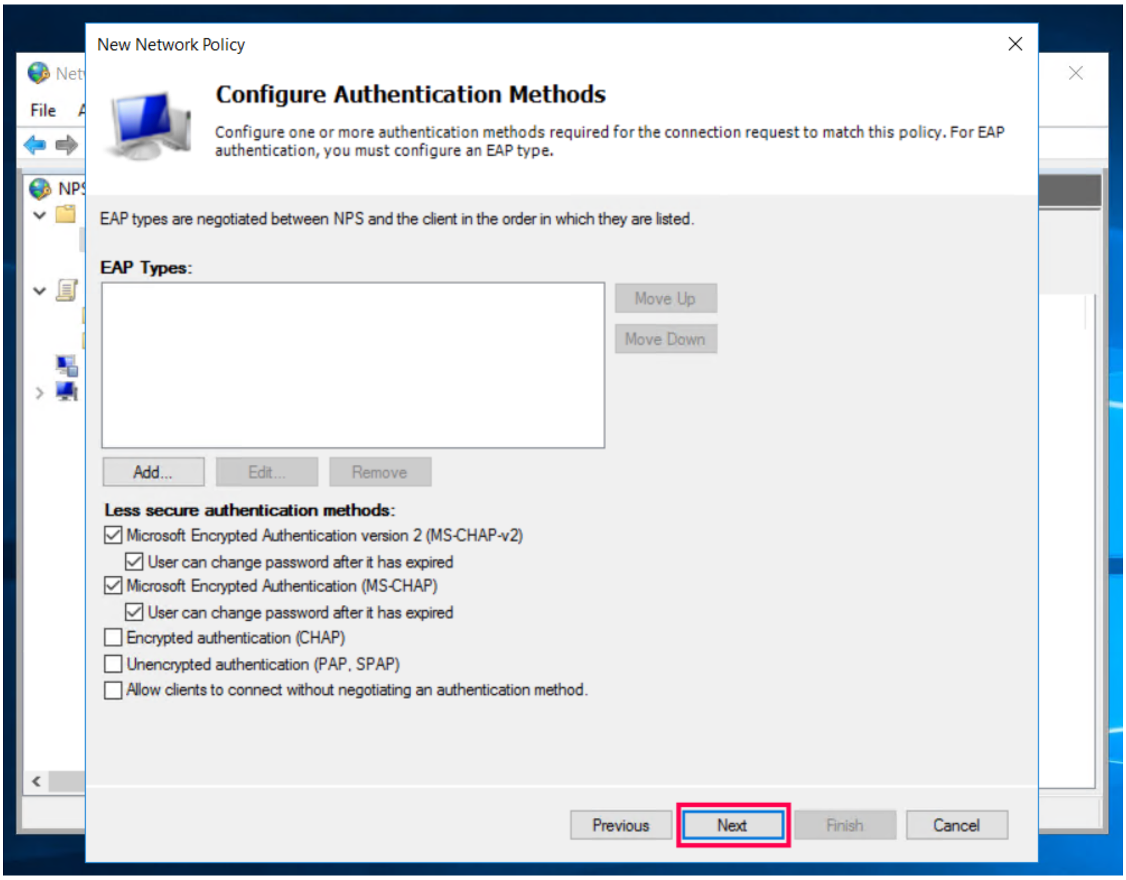
○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Step 5: Configure the protocols for your **Authentication Methods.**

- For one-way authenticators such as push notifications or biometrics, you can choose any method of authentication.

- For challenge-based MFA methods like **Google Authenticator, Microsoft Authenticator, ZohoOneAuth, CustomTOTP, Yubikey,** etc., you must enable the **PAP** protocol.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☑ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

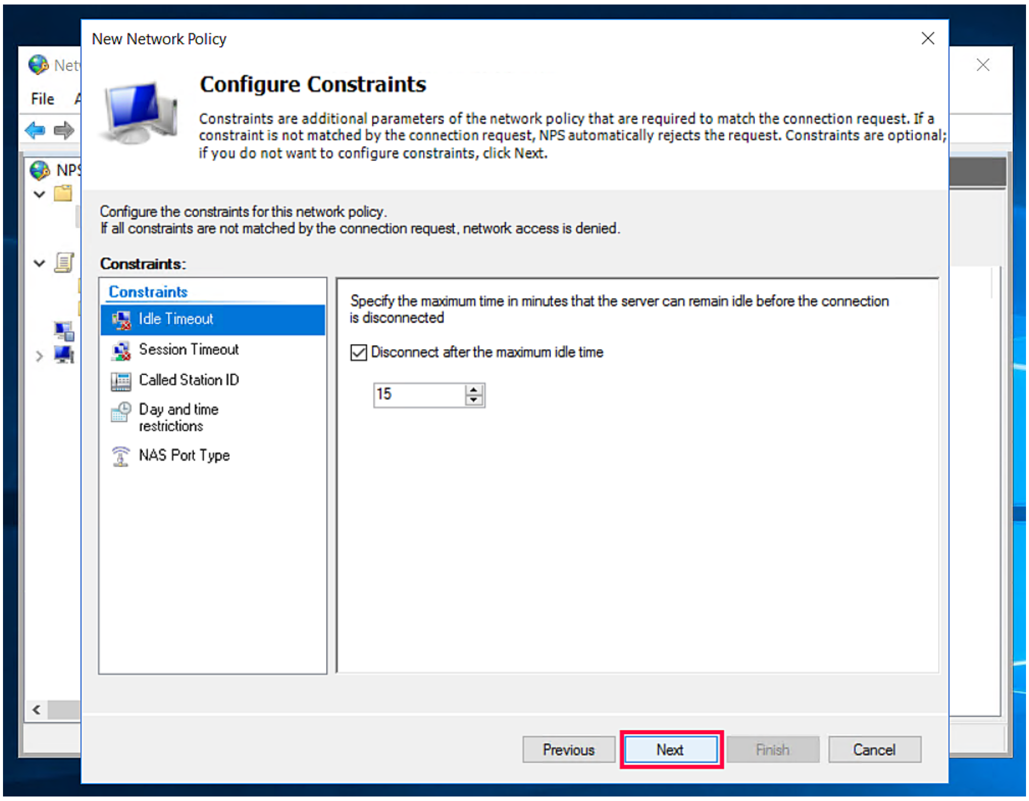
☑ User can change password after it has expired

□ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

Step 6: Configure any constraints you might have, then click **Next.**



New Network Policy

Configure 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. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☑ Disconnect after the maximum idle time

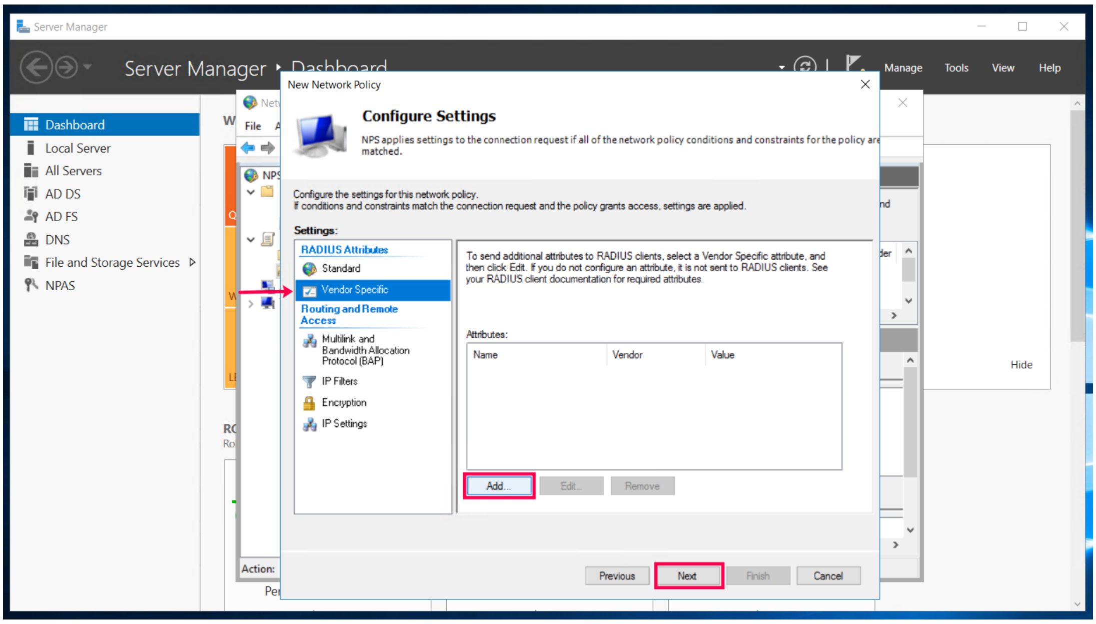
15

Step 7: In the *Configure Settings* window, set additional attributes requested by the VPN server.

Note:

- Additional attributes can only be set for one-way authentication methods such as push notifications and biometrics.

- Additional attributes are incompatible with challenge-based authentication methods such as **Google Authenticator, Microsoft Authenticator, ZohoOneAuth, CustomTOTP, Yubikey,** etc. When challenge-based authenticators are used, the RADIUS attributes that are configured in the Network Policy won't be forwarded to the RADIUS client (VPN or endpoint server). As a result, the VPN client might either have more access than you want it to have, less access, or no access.



New Network Policy

Configure Settings

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

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

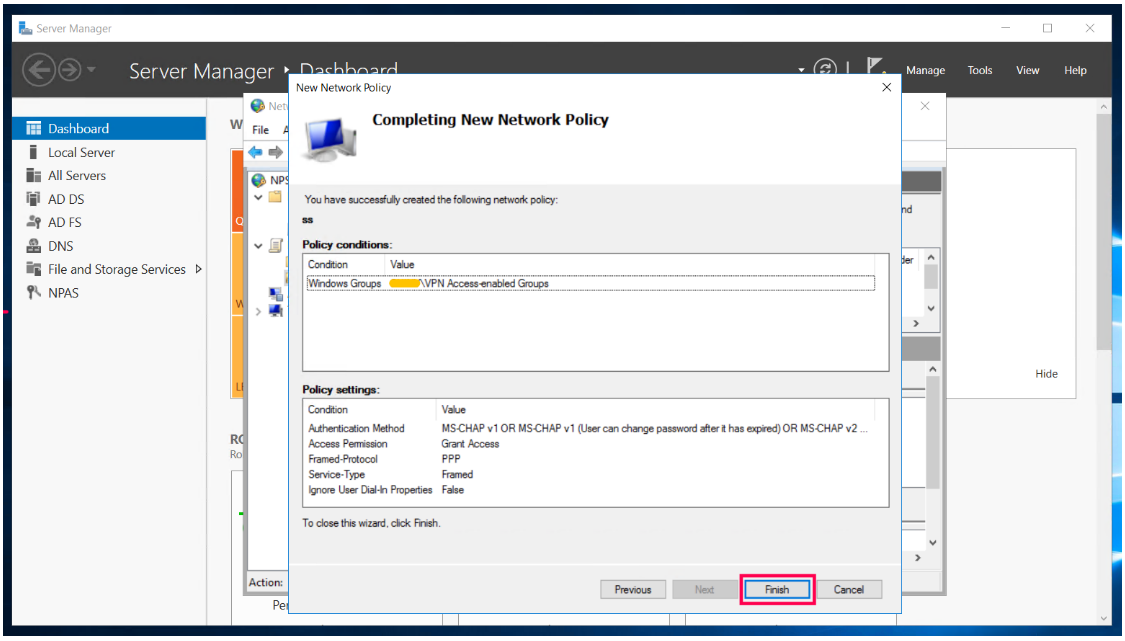
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value

Step 8: When all the settings have been configured, click **Finish.**



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

ss

Policy conditions:

Condition	Value
Windows Groups	[redacted]\VPN Access-enabled Groups

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False

To close this wizard, click Finish.

Now the NPS service has been installed, registered in Active Directory and configured.

Configuration at the VPN gateway (or other endpoints)

Configuring the VPN server to use RADIUS authentication

To authenticate VPN clients on this NPS, the RADIUS authentication type must be configured in the VPN server.

VPN server configuration is vendor-specific. The broad steps to perform are as follows:

Step 1: Log into the admin interface and navigate to the Authentication Servers section.
Step 2: Specify that the new server is a RADIUS server.
Step 3: Enter the IP Address and port number (the default port no. is 1812) of the RADIUS server (the NPS server in Stage 1). You will also have to enter the shared secret you used while registering the VPN gateway server as a RADIUS client.

Note: Once the VPN gateway has been pointed to the NPS for authentication, the admin will be able to verify the configuration by testing if primary authentication works.

ADSelfService Plus Configuration for MFA

1. Enabling the required authenticators

1. Log into ADSelfService Plus as an admin.
2. Go to **Configuration → Self-Service → Multi-Factor Authentication → Authenticators**

Authenticators supported for Endpoint VPN MFA can be classified into one-way authenticators and challenge-based authenticators

1. One-way authenticators

- Push notification Authentication
- Fingerprint/Face ID Authentication

These authenticators are applicable by default for all the endpoints providing RADIUS authentication.

Note:

- When you enable Push Notification or Fingerprint/Face ID Authentication, make sure the ADSelfService Plus server is reachable by the users through the internet from their mobile devices.

- RADIUS authentication timeout should be set to at least 60 seconds in the VPN server's RADIUS authentication configuration settings.

2. Challenge-based authenticators

- ADSelfService Plus TOTP Authentication
- Google Authenticator
- Microsoft Authenticator
- Yubico OTP (hardware key authentication)

Challenge-based authenticators are applicable only when:

- PAP is configured for the RADIUS authentication method.

- The RADIUS client (VPN or endpoint server) supports challenge-response, such that it has a way for prompting challenges (a verification code) from the users and sending back the entered challenge.

Note: When challenge-based authenticators are used, the RADIUS responses that are configured in the Network Policy won't be forwarded to the RADIUS client (VPN or endpoint server). As a result, the VPN client might either have more access than you want it to have, less access, or no access.

Click on the authenticators in the product UI to learn how to enable these authentication methods.

2. Enabling MFA for VPN Logins in ADSelfService Plus

Step 1: Go to **Configuration → Self-Service → Multi-Factor Authentication → MFA for Endpoints.**

Step 2: Select a policy from the Choose the Policy drop-down. This policy will determine the users for whom MFA for VPN and endpoint login will be enabled. To learn more about creating an OU or a group-based policy, click here.

Step 3: In the **MFA for VPN Login** section, select the checkbox next to Select the authenticators required. Choose the number of authentication factors to be enforced. Select the authentication methods to be used. The authentication methods listed can also be rearranged by dragging and dropping to the necessary position.

Step 4: Click **Save Settings.**

3. Installing the NPS extension

Step 1: Go to **Configuration → Self-Service → Multi-Factor Authentication → MFA for Endpoints → MFA for VPN Login.**

Step 2: Click on the tooltip next to MFA for VPN Login and download the NPS extension from the download link in the pop-up window.

Step 3: Copy the extension file (**ADSSPNPSExtension.zip**) to the Windows server which you have configured as the RADIUS server. Extract the ZIP file's contents and save it in a location of your choice.

Step 4: Open Windows PowerShell as administrator and navigate to the folder where the extension files are located.

Step 5: Execute the following command:

```
PS C:\> .\setupNpsExtension.ps1 Install
```

Note: If the NPS extension plugin has to be uninstalled or needs updated configuration data, replace "Install" with "Uninstall" or "Updated" respectively.

Step 6: After installation, you will be prompted to restart the NPS Windows service. Proceed with the restart.

Advanced settings

Refer to Advanced Settings to configure VPN MFA session limits and the options for bypassing MFA if ADSelfService Plus is not reachable or the user is not enrolled.

You can customize the MFA configuration based on organizational requirements. To do so:
Step 1: Open the **Registry Editor** (type regedit in the Run dialog box).

Step 2: Go to **HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfService Plus NPS Extension.**

Note:

- Take a backup of the registry key before editing it.
- Only the built-in administrator group in the computer will have the privilege to edit this key.

3. Installing the NPS extension

You can customize the parameters mentioned below according to your organizational requirements:

- **ServerName:** Mention the HostName or IP address of the ADSelfService Plus web server.

- **ServerPortNo:** Mention the TCP Port number for the ADSelfService Plus web server.

- **ServerContextPath:** Mention the web server context (if changed)

- **MfaStatus:** This can be set to true or false depending on whether you need MFA to be enforced or not.

- **ServerSSLValidation:** This can be set to true or false. If set to true, it verifies the SSL certificate and hostname when establishing an HTTPS connection from the NPS extension to the ADSelfService Plus server. It is recommended that the property always be set to true for security reasons.

- **BypassMFAOnConnectionError (Optional):** This property can be set to true or false, depending on whether you want MFA to be bypassed if any connection issues are present during authentication.

- **CRPolicies (Optional):** This property can be used to enforce MFA only for a user who falls under these connection request policies. Enter the connection request policy's names, then if more than one policy has to be mentioned, separate each policy name with a semicolon (;).

- **NetworkPolicies (Optional):** This property can be used to enforce MFA only for a user who falls under these network policies. Enter the network policy's names, then if more than one policy has to be mentioned, separate each policy name with a semicolon (;).

  Note: When both Connection Request Policies and Network Policies are configured, an authentication request will be considered for MFA only if both the Connection Request Policies and Network Policies of the RADIUS request match with the ones configured. If the policies are not configured, MFA will be enforced for all the successful RADIUS requests sent to the NPS server.

- **LogLevel (optional):** This property can be used to determine the intricacy of the logged information on the feature's functioning. The property will be set to **Normal** by default and can be changed to **Debug** to additionally log details that will aid with debugging. It is recommended that the property be set to **Normal.**

Step 3: Click OK.

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus, visit https://www.manageengine.com/products/self-service-password.

$ Get Quote   Download   Support