

# NPS configuration for Endpoint MFA



# Table of Contents

Introduction	1
How it works	1
Configuration steps	2
NPS Installation and Configuration	3
Configuration at the VPN gateway (or other endpoints)	18
ADSelfService Plus Configuration for MFA	18

# Introduction

ADSelfService Plus introduces 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.

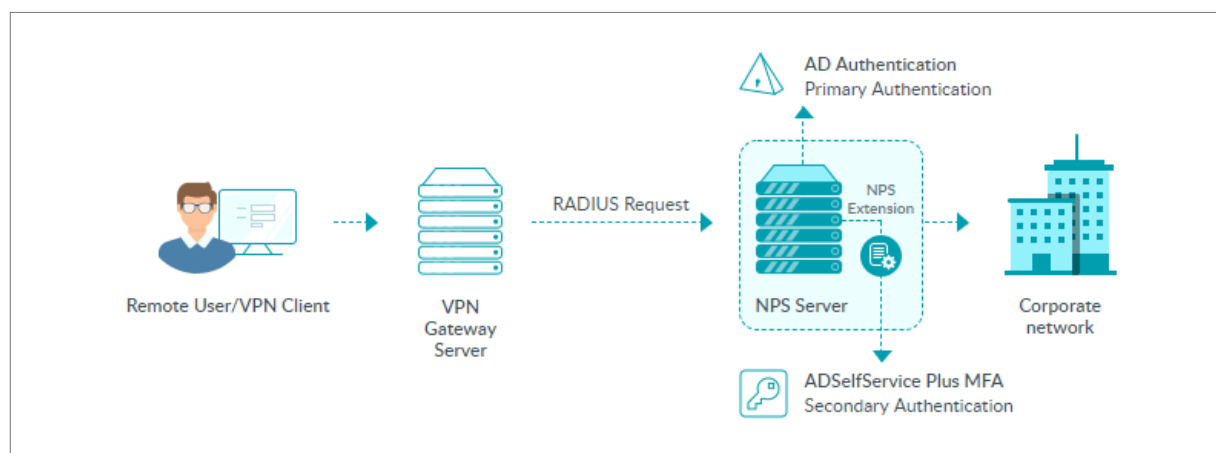
## How it works

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

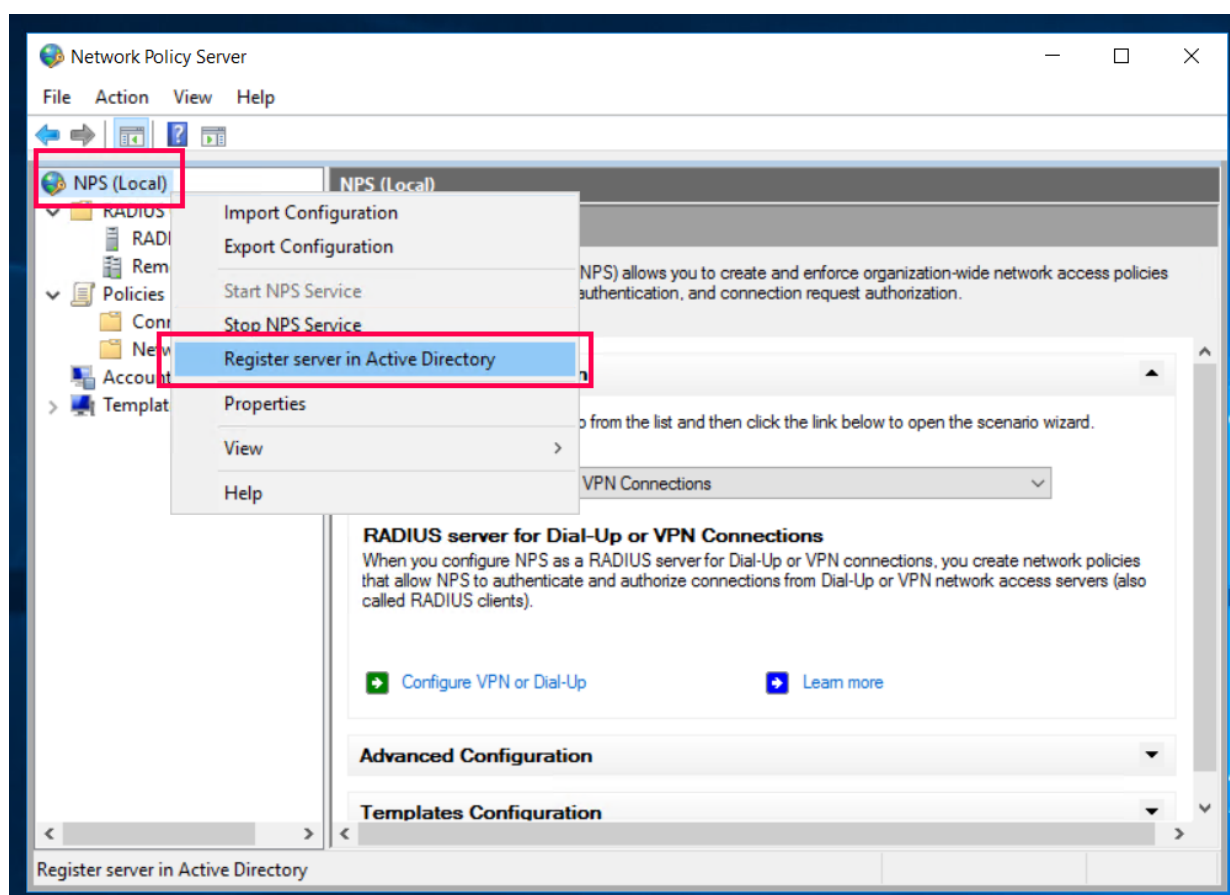
## 1. Installing the NPS service

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.

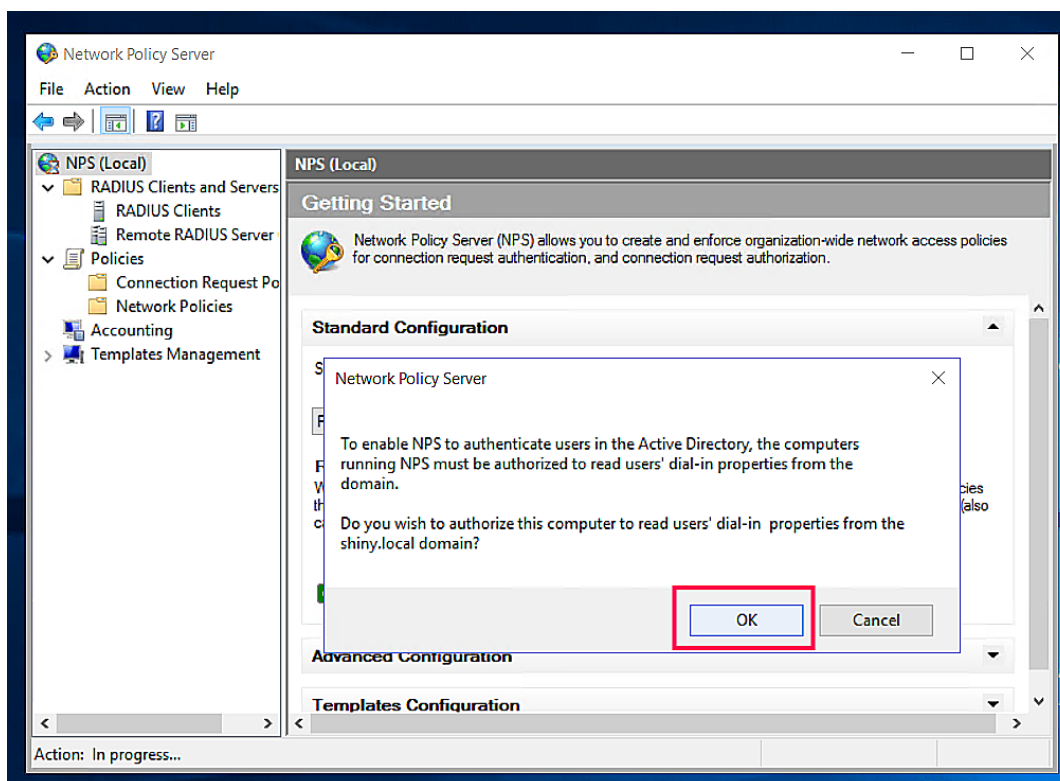
## 2. Registering the NPS server in Active Directory

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

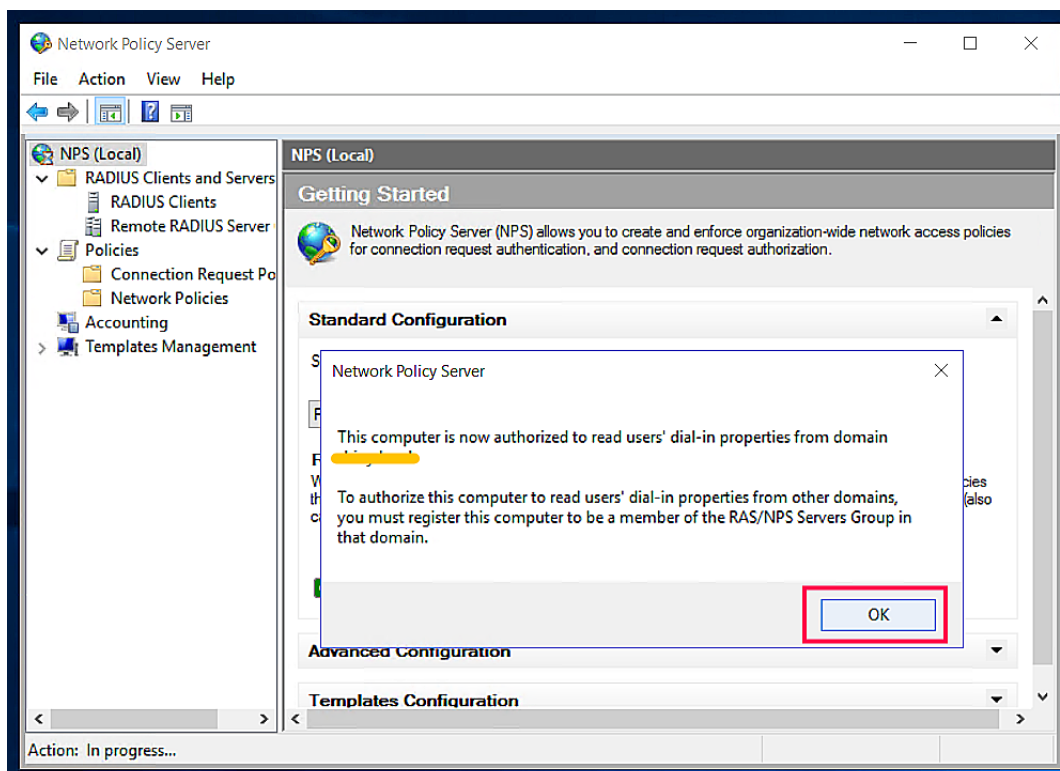
**Step 1:** From the main NPS screen of NPS, right-click *NPS (local)* and select **Register server in Active Directory**.



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



**Step 3:** Click **OK** again.



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.

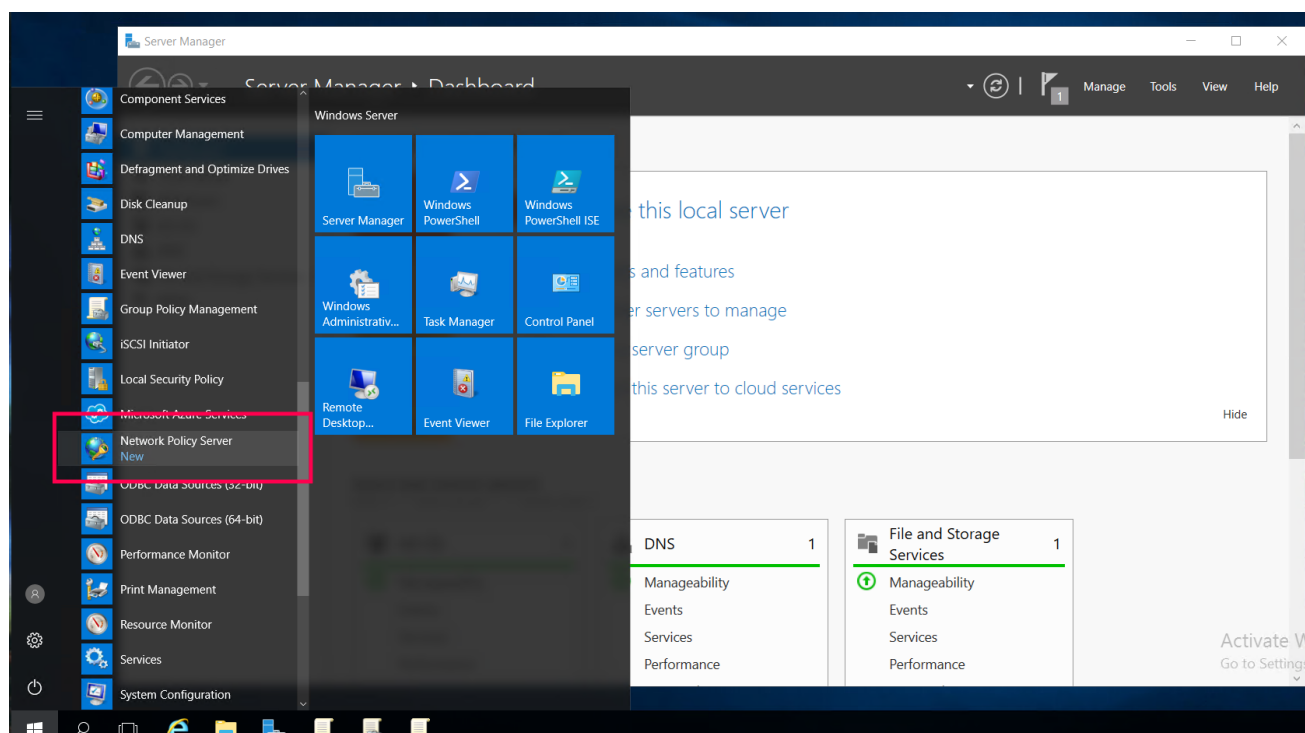
**Stage 2:** Configuring a Connection Request policy for your VPN Gateway server.

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

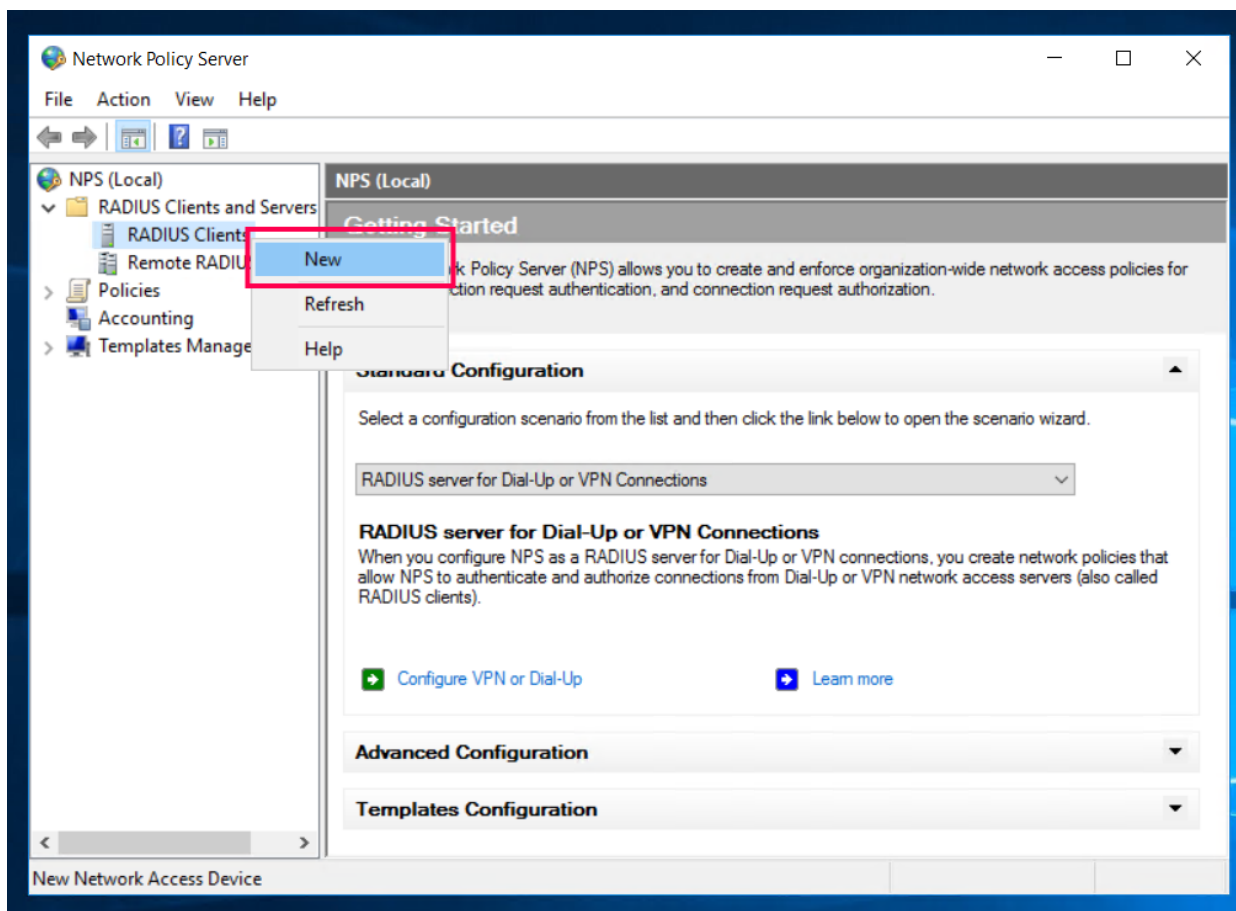
#### Stage 1: Registering your VPN gateway server as a RADIUS client

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.**



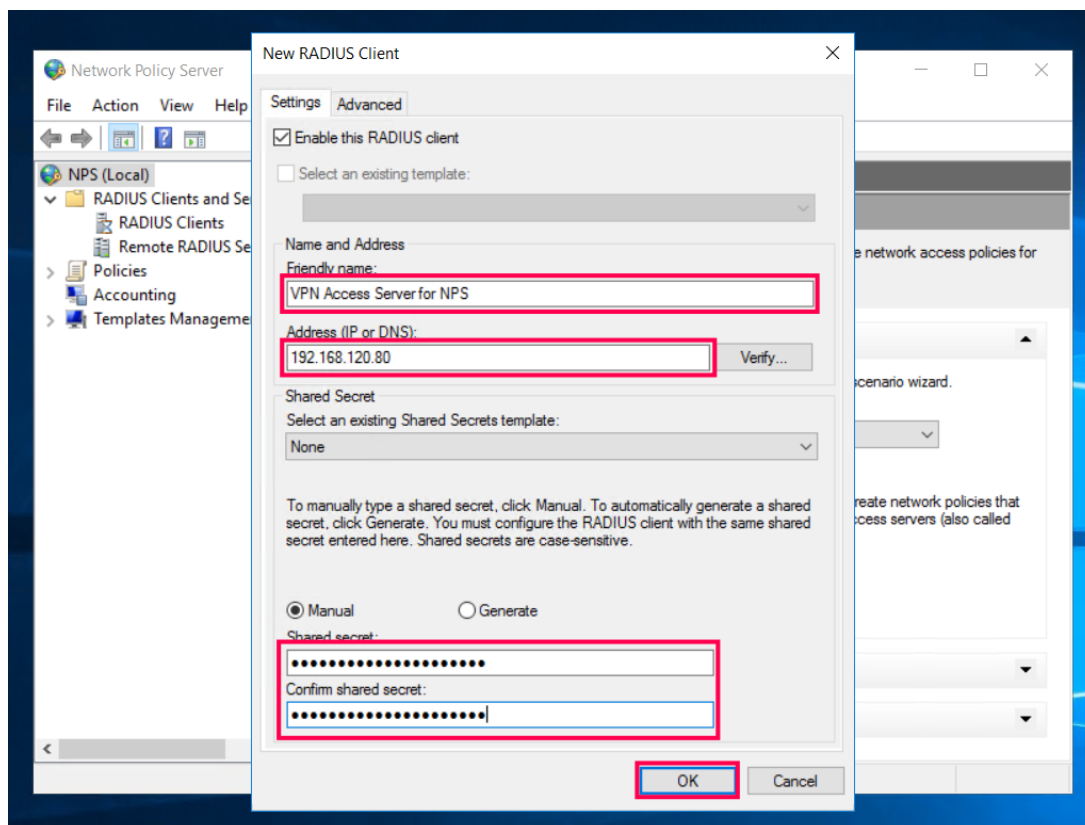
**Step 2:** In the *Network Policy Server* window that opens, expand **RADIUS Clients and Servers**, then right-click on **RADIUS Clients** and select **New**.



**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**.





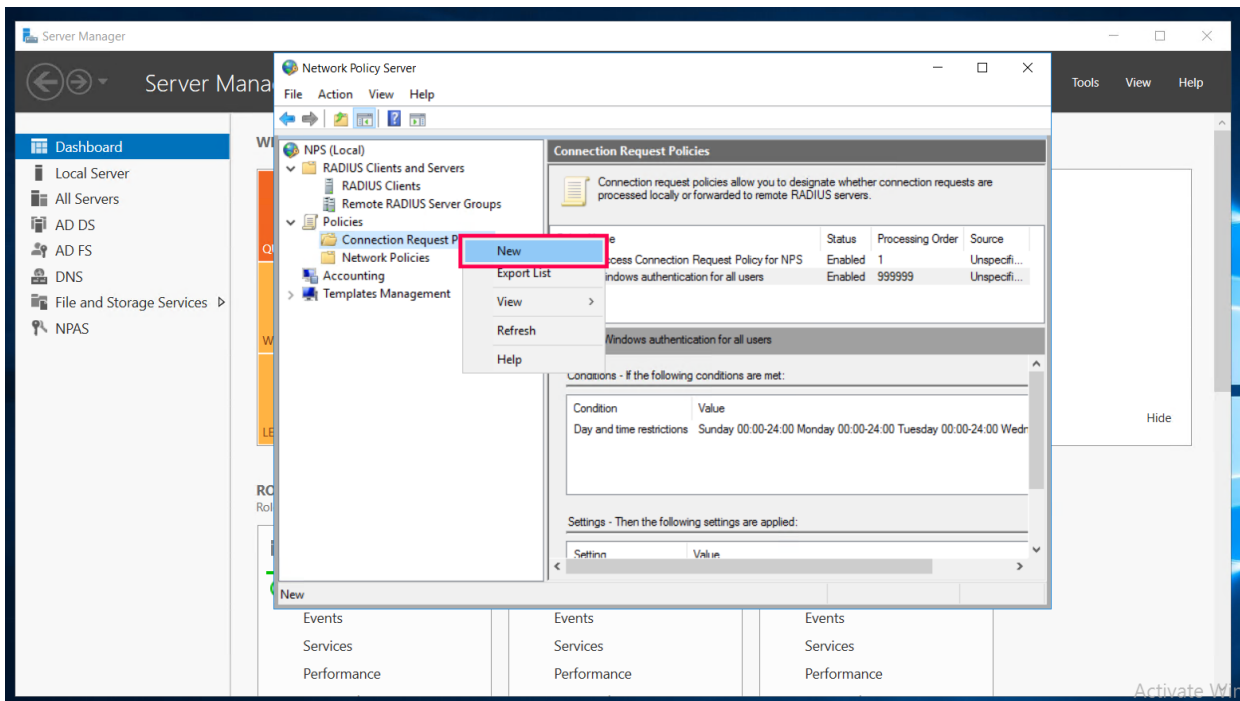
Now the VPN server has been configured as a RADIUS client. Next, you will need to edit the Connection Request Policy and the Network Policy.

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

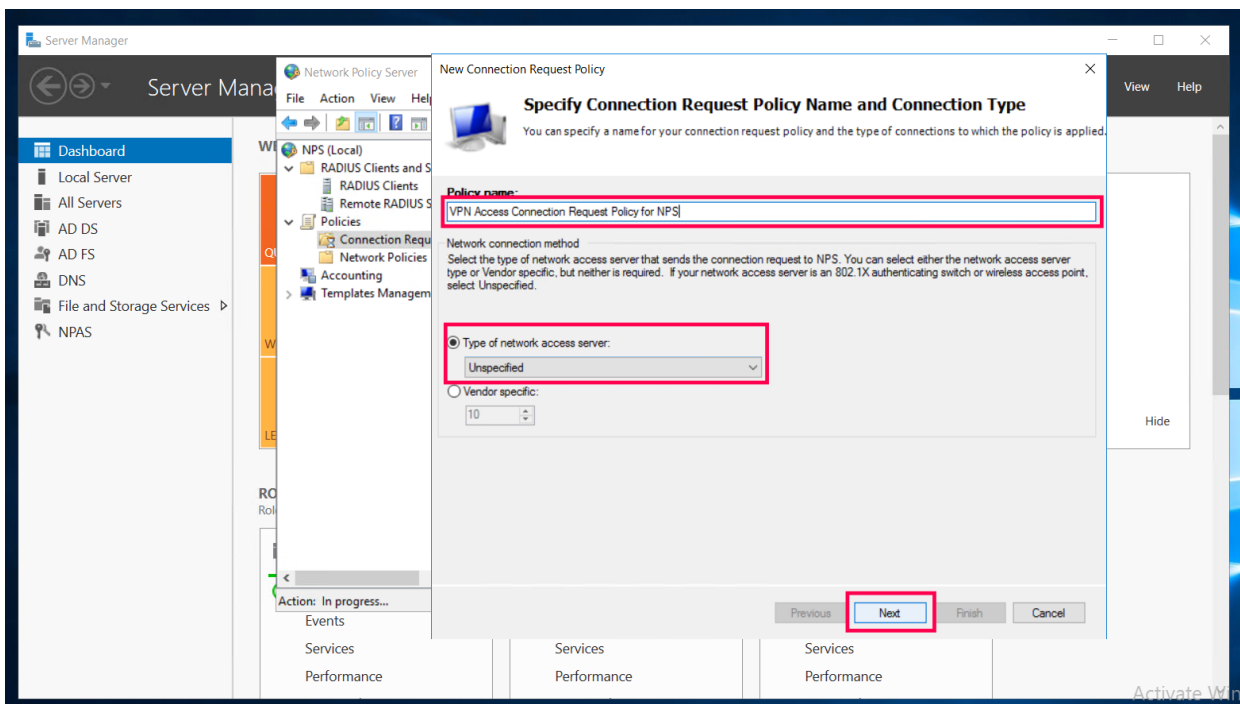
A Connection Request Policy defines how authentication should happen for the incoming RADIUS requests. Since you need the authentication to happen on the server you are configuring, you need to specify this in the Connection Request policy.

**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.



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

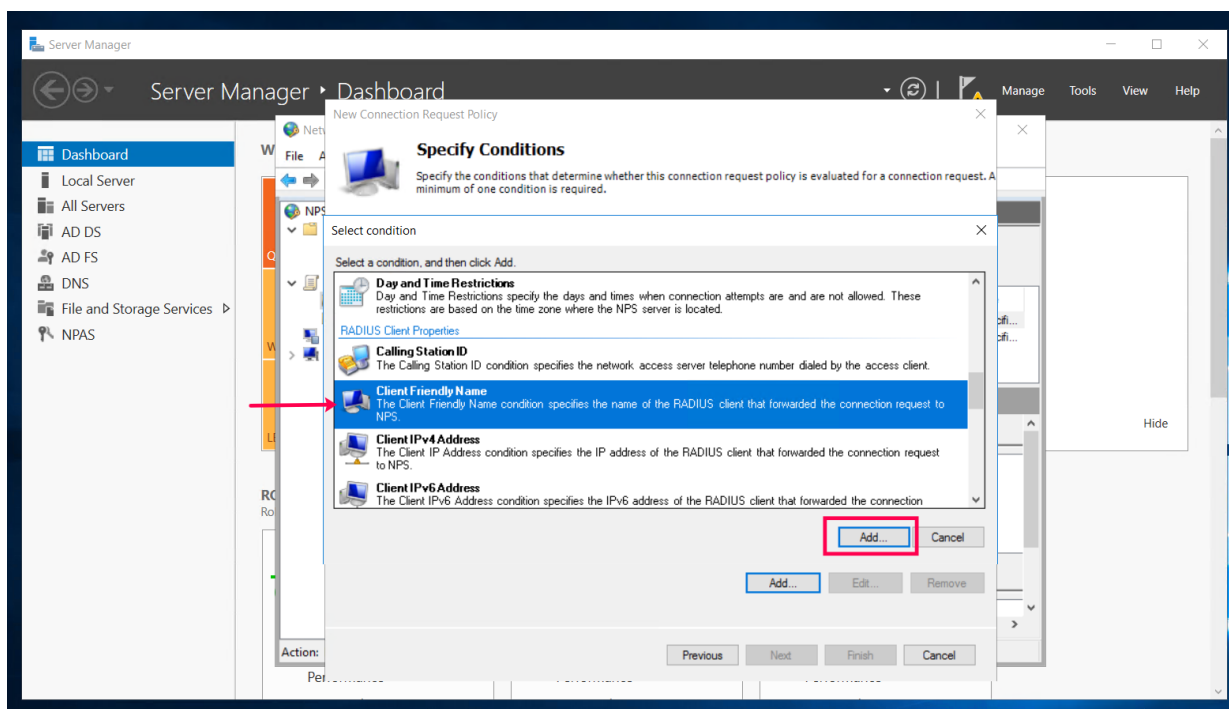


**Step 3:** Specify the conditions for when this connection request policy is evaluated for a connection request. These conditions depend on your organization's policies. A minimum of one condition is required.

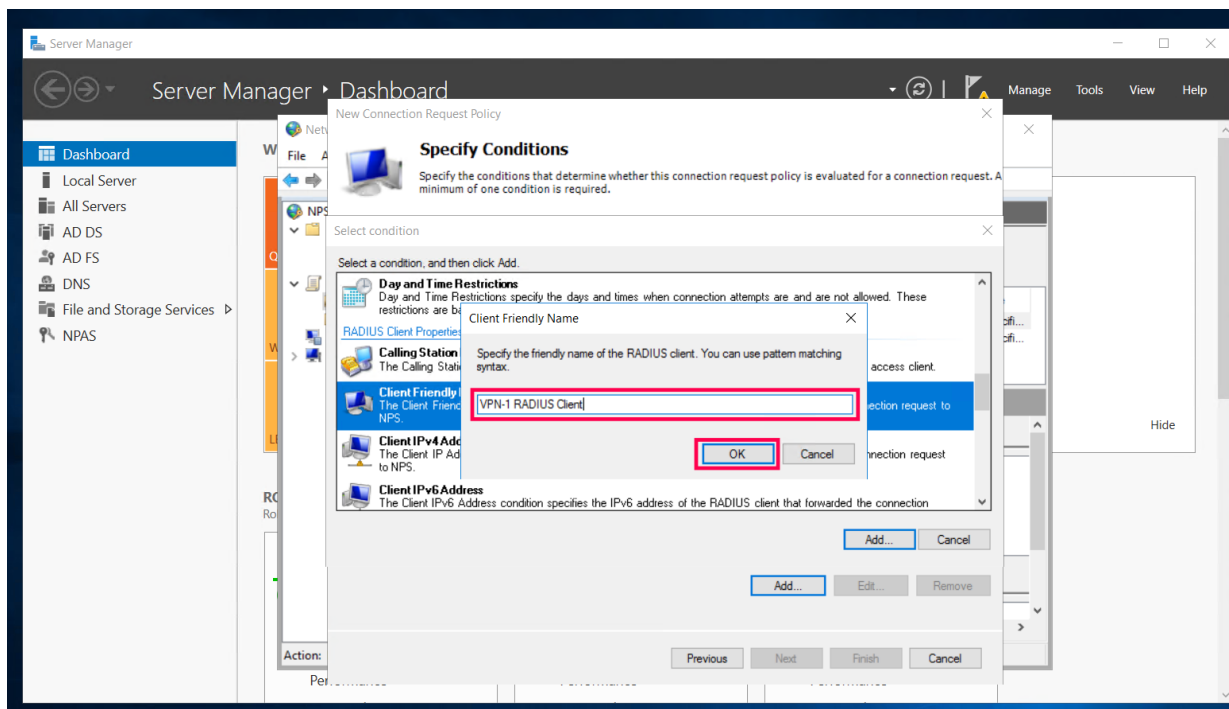
For instance, you can add a friendly name for the RADIUS client for the RADIUS client configured during Stage 1.

Adding a friendly name:

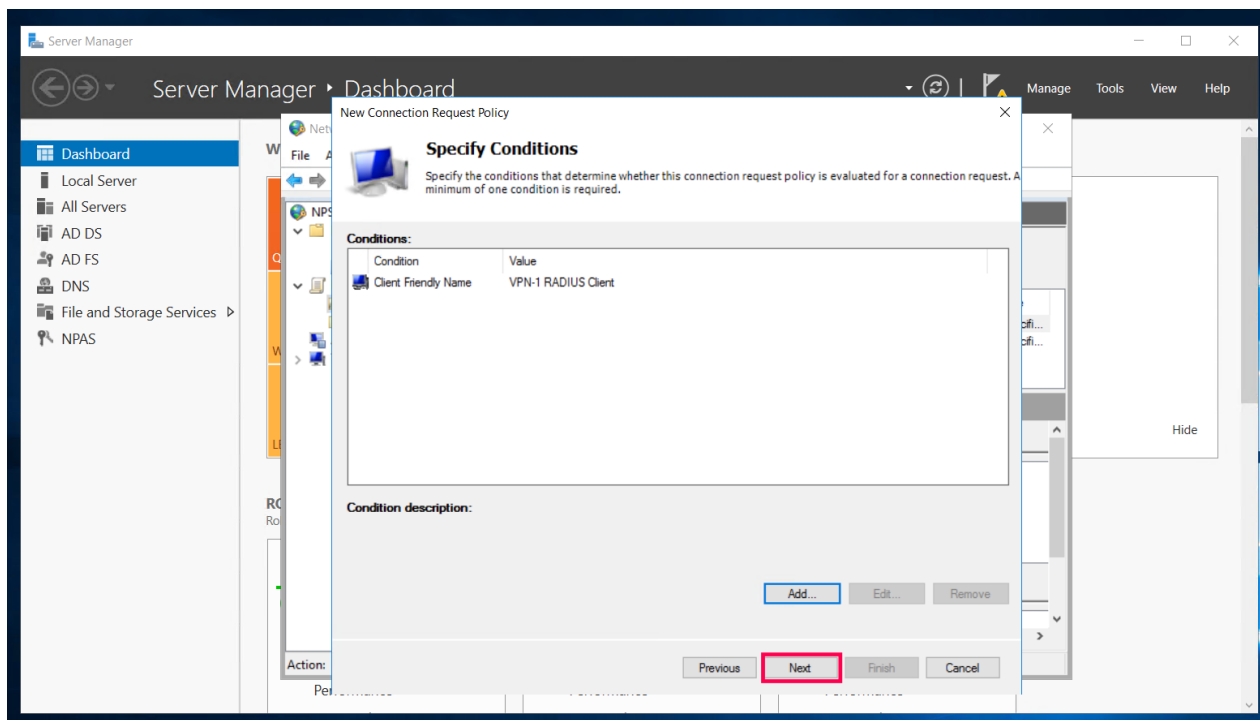
**Step 3a:** Click on **Client Friendly Name** and click **Add**.



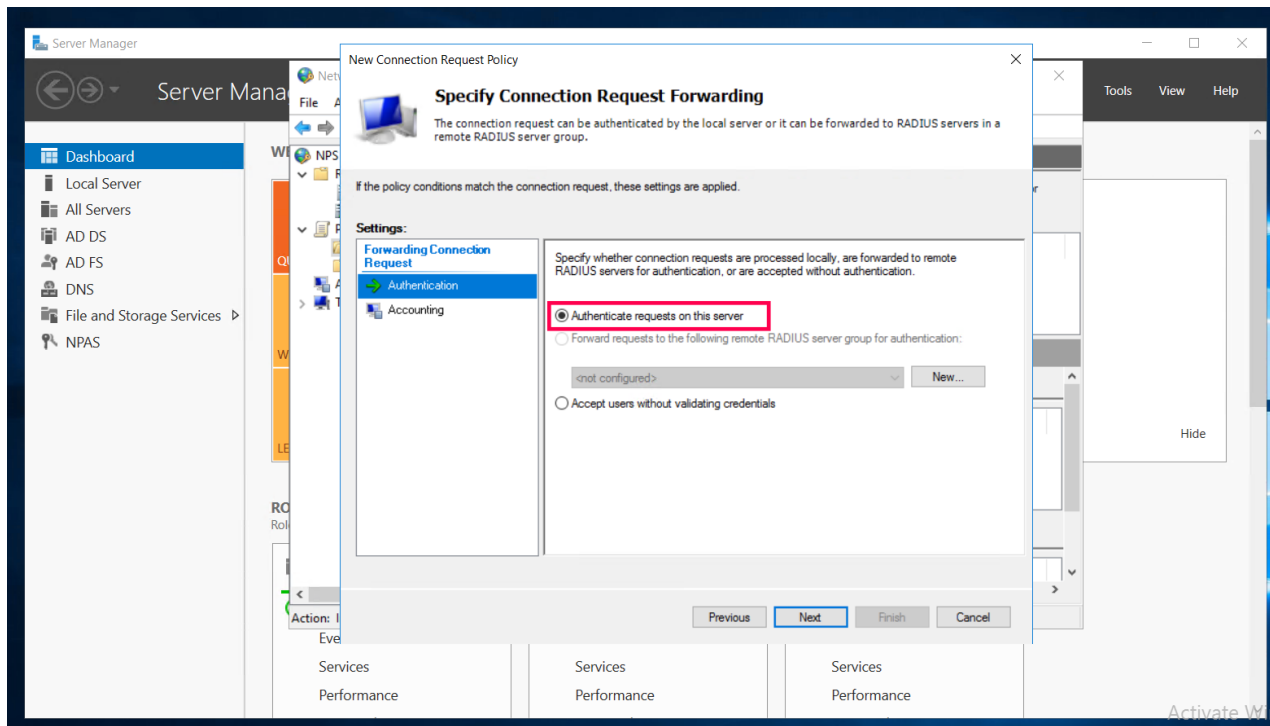
**Step 3b:** Enter a relevant friendly name for the RADIUS client and click **OK**. This condition will be added to the policy.



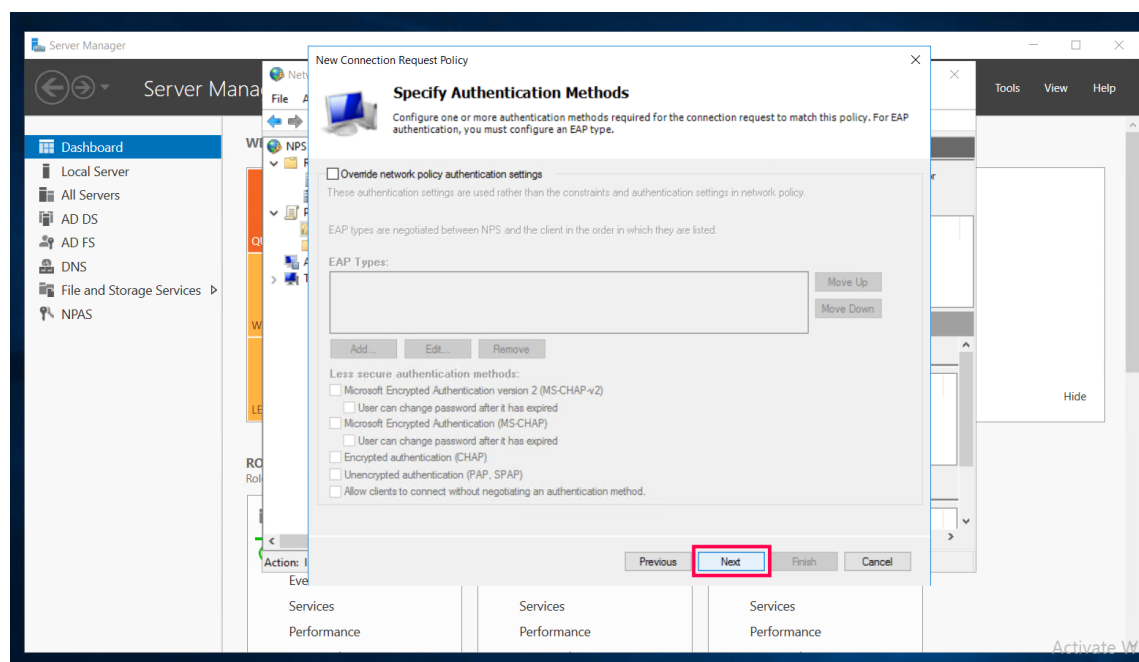
**Step 3c:** You can add any other organization-specific conditions you might require. Once done, click **Next**.



**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**.



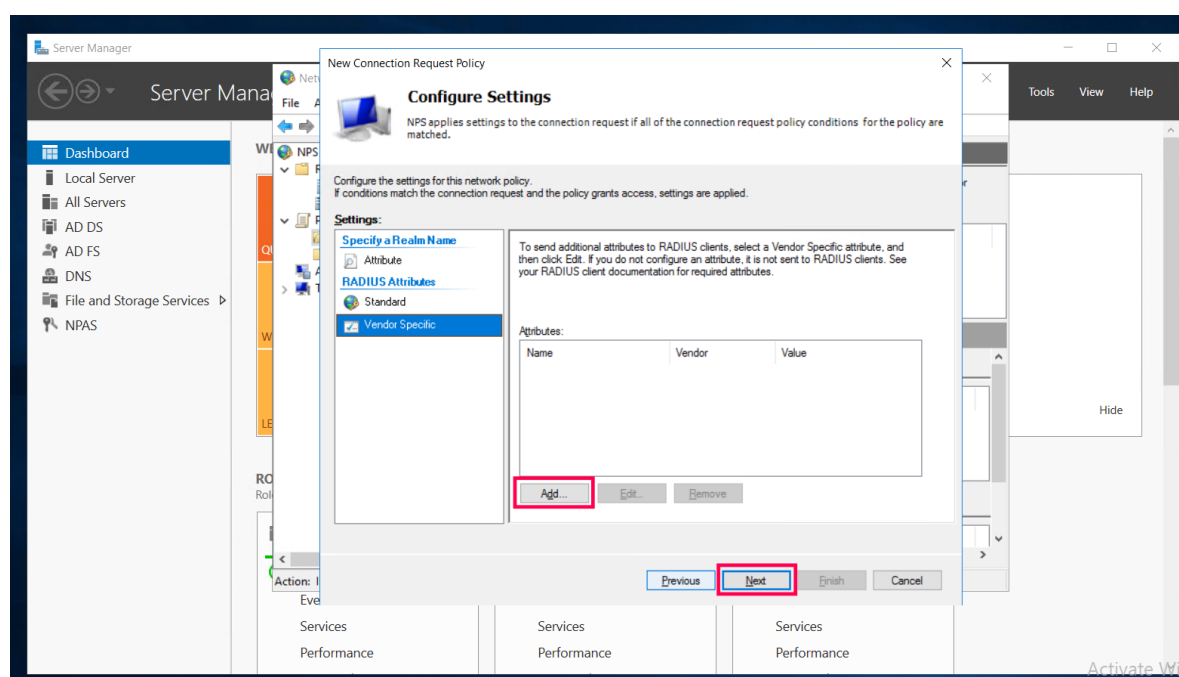
**Step 5:** Leave the *Specify Authentication Methods* section untouched. Click **Next**.



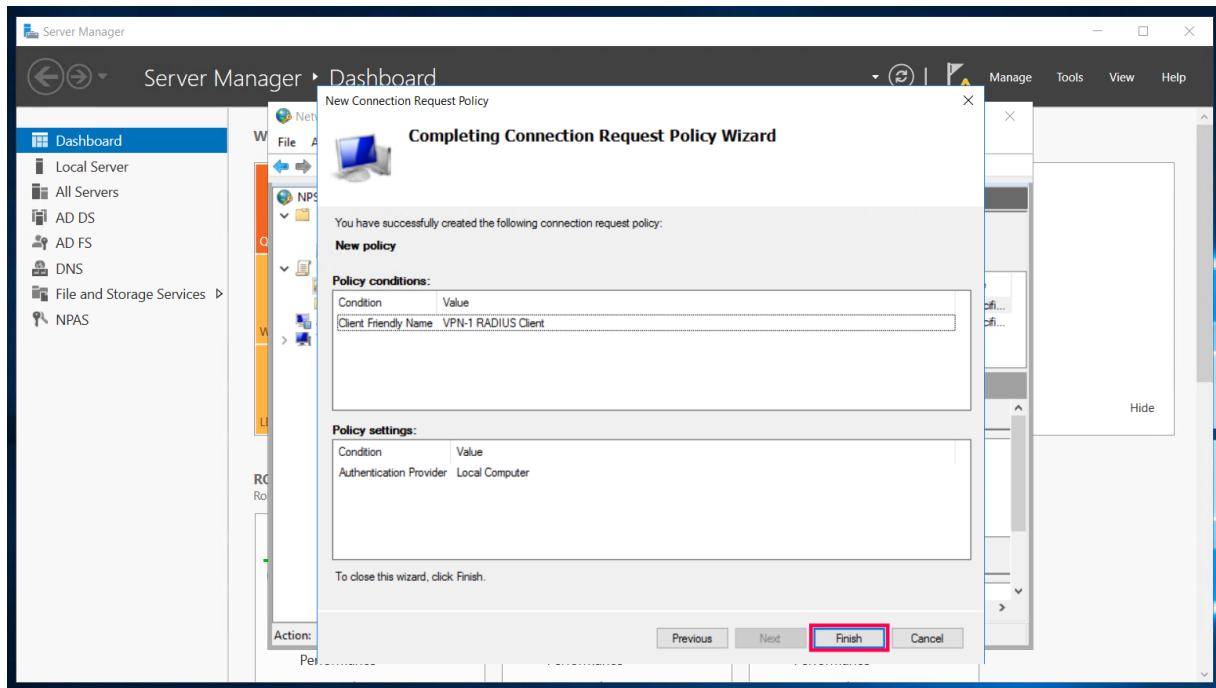
**Step 6:** Add any vendor-specific conditions.

**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.



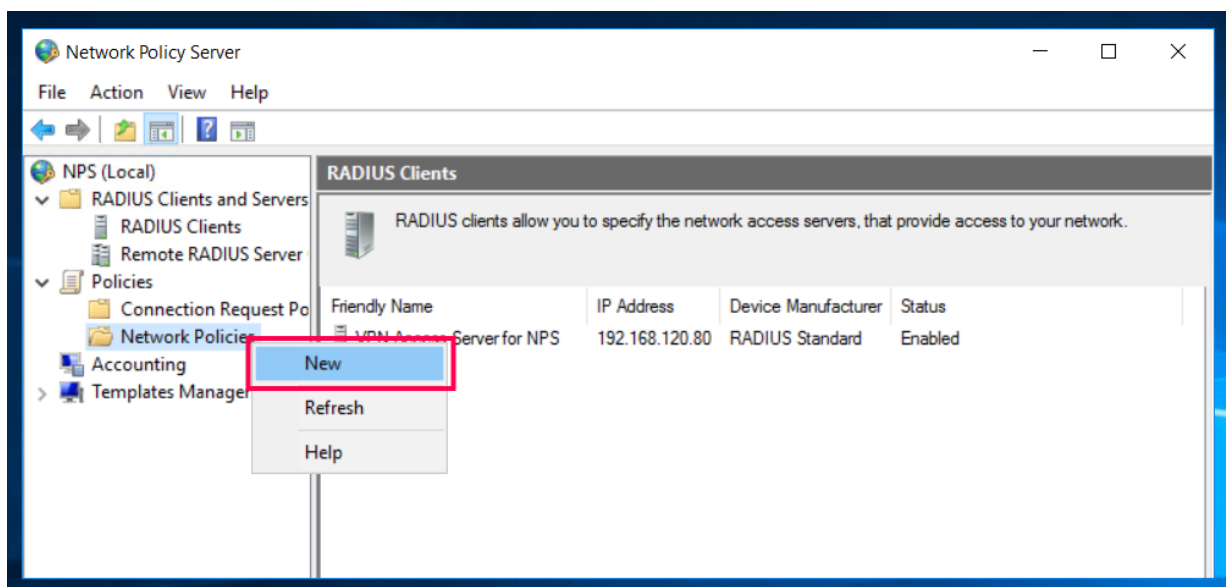
**Step 7: Click Finish.**



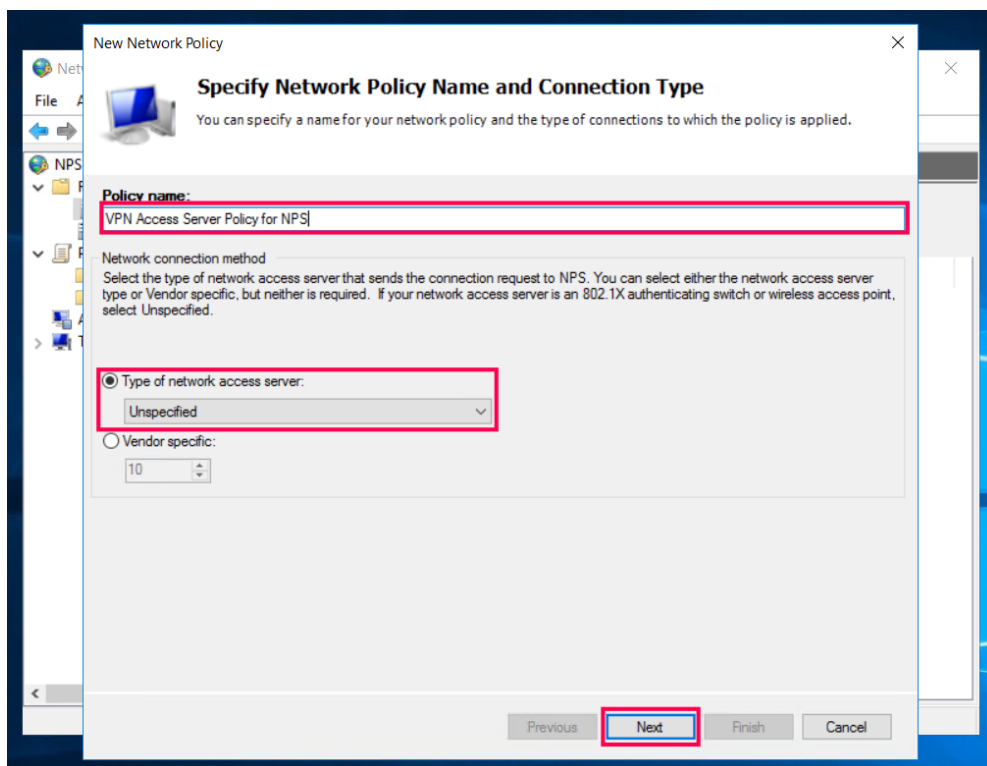
### Stage 3: Configuring a Network policy to authorize the requests with conditions

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.**



**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

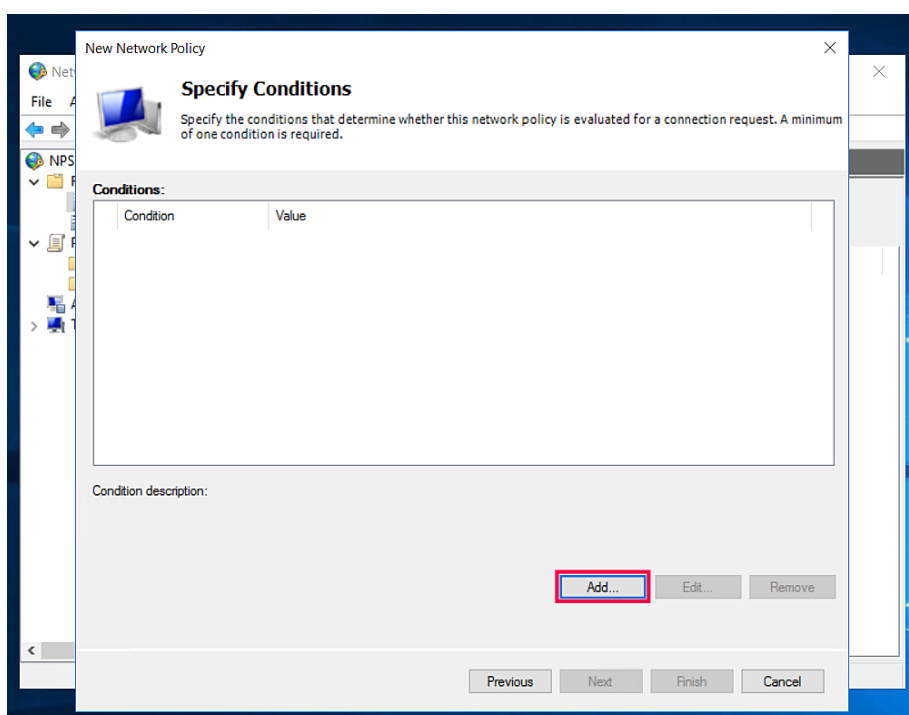
**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point,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

☒ Type of network access server:  
Unspecified

☐ Vendor specific:  
10

Previous **Next** Finish Cancel

**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.

Condition	Value
-----------	-------

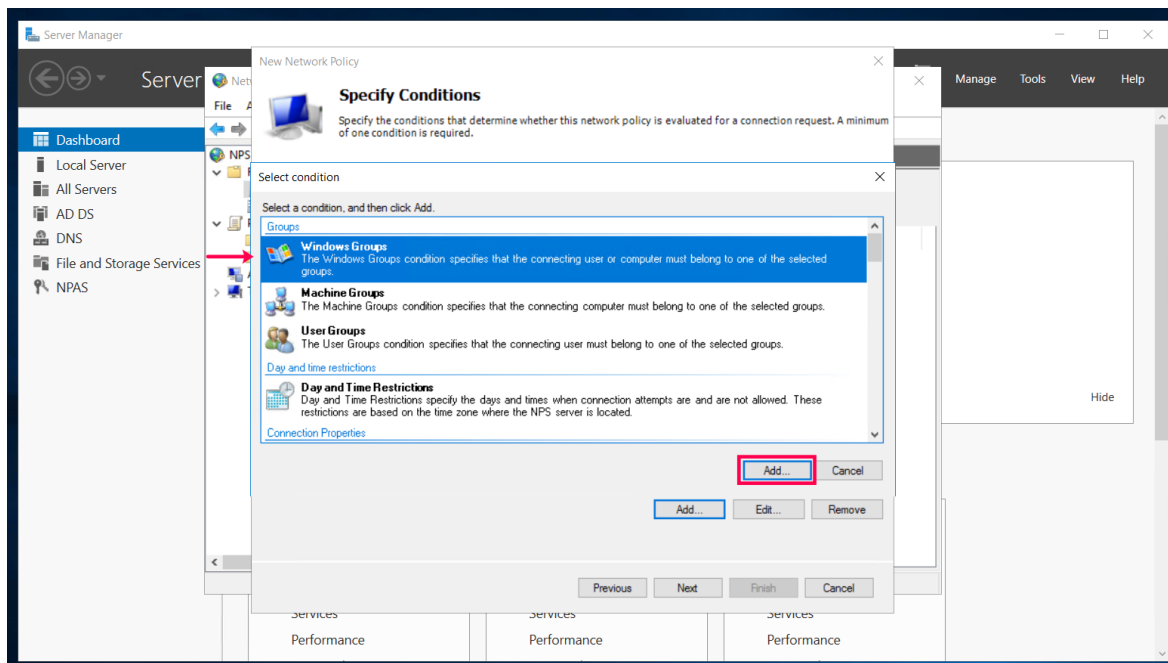
Condition description:

**Add...** Edit... Remove

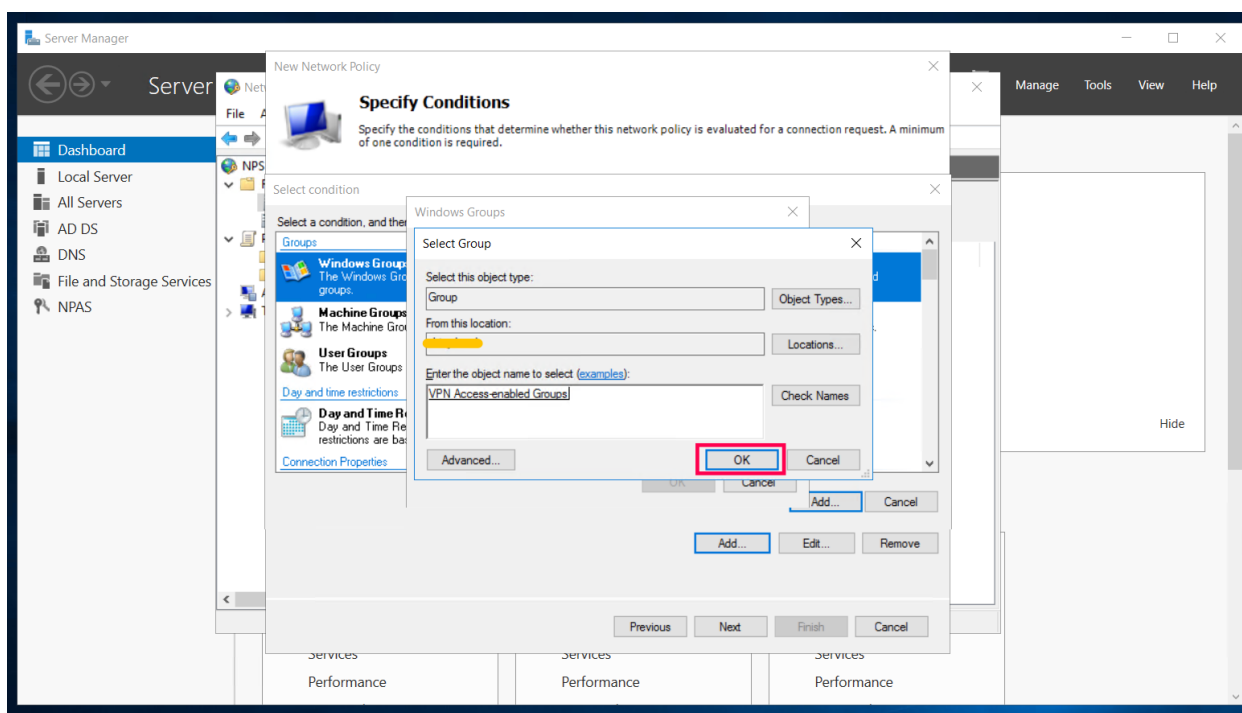
Previous Next **Finish** Cancel

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**.

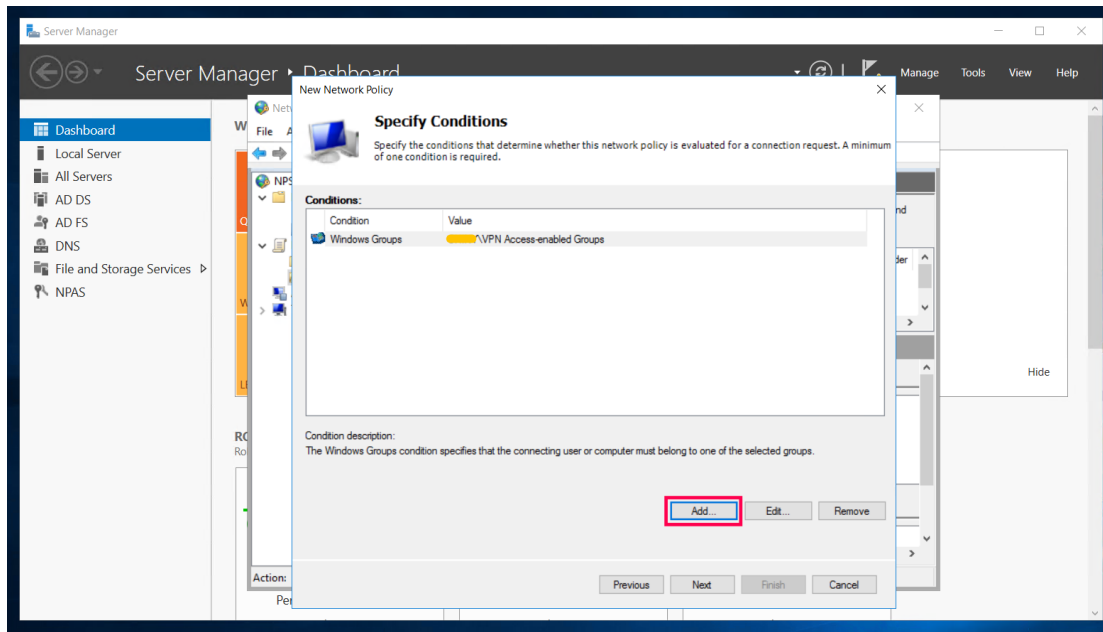


**Step 3b:** Specify the group to be granted access.

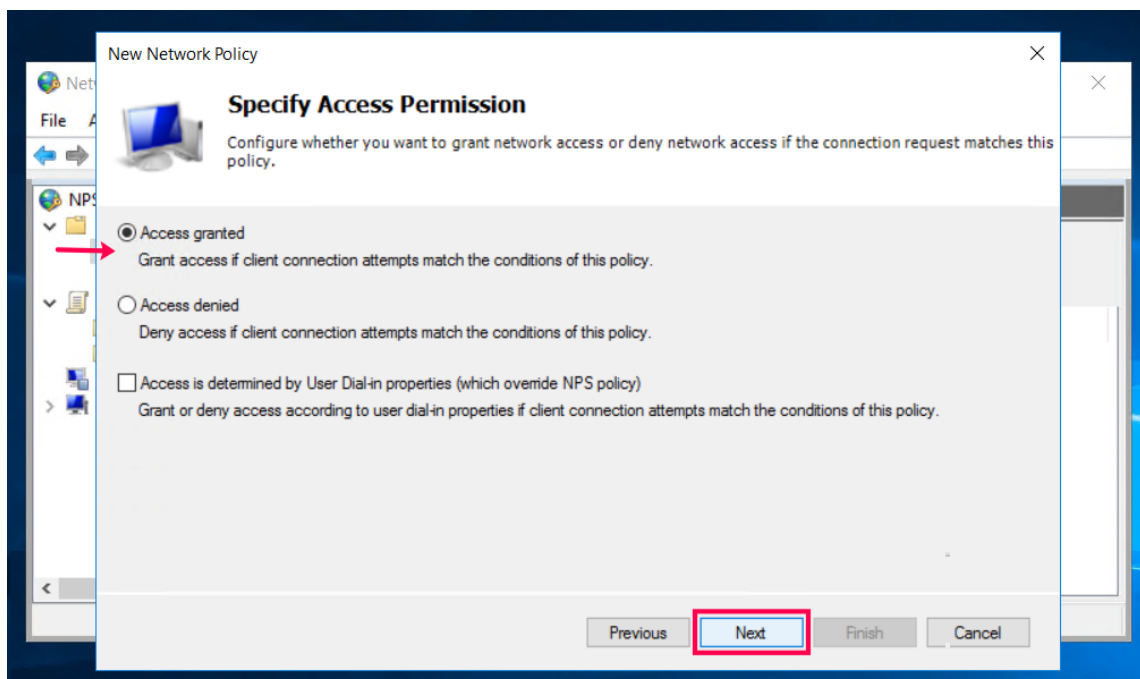




**Step 3c:** Click **OK**. Once all the access conditions you require are enabled, click **Next**.

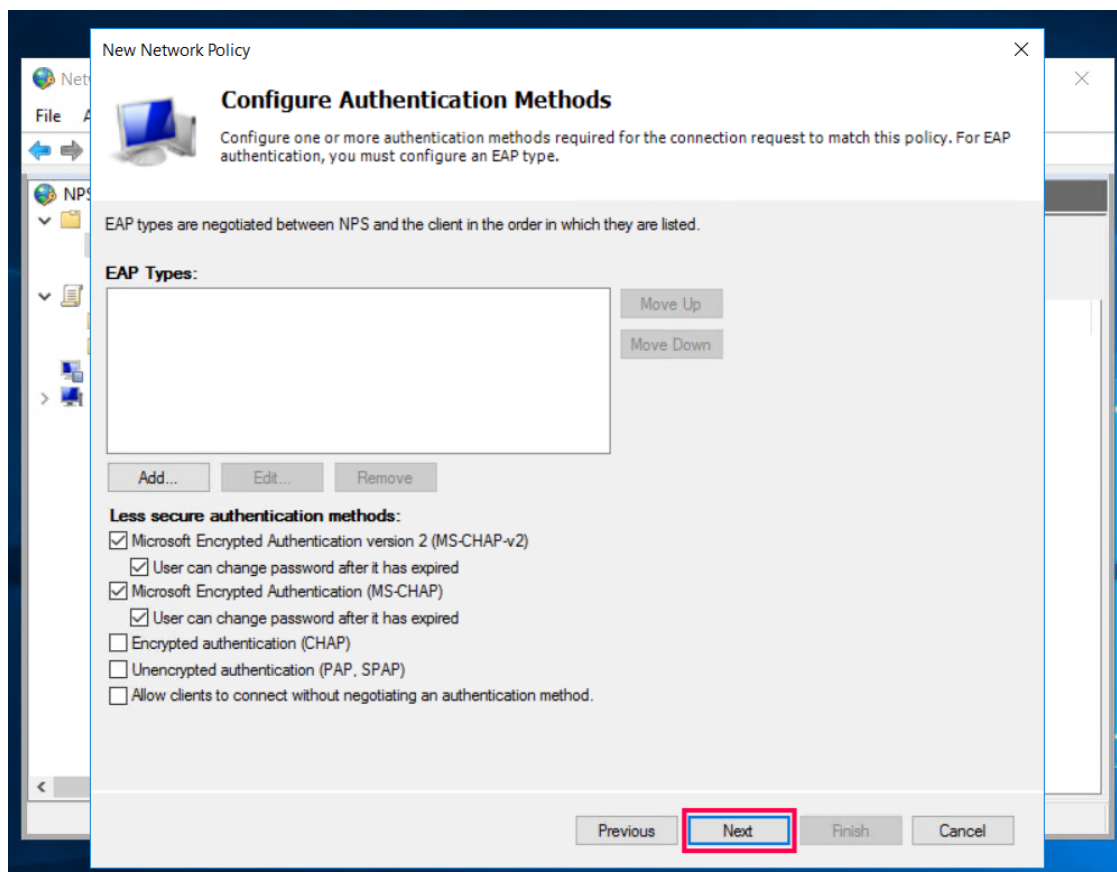


**Step 4:** In the *Specify Access Permission* section, choose **Access Granted**. Click **Next**.

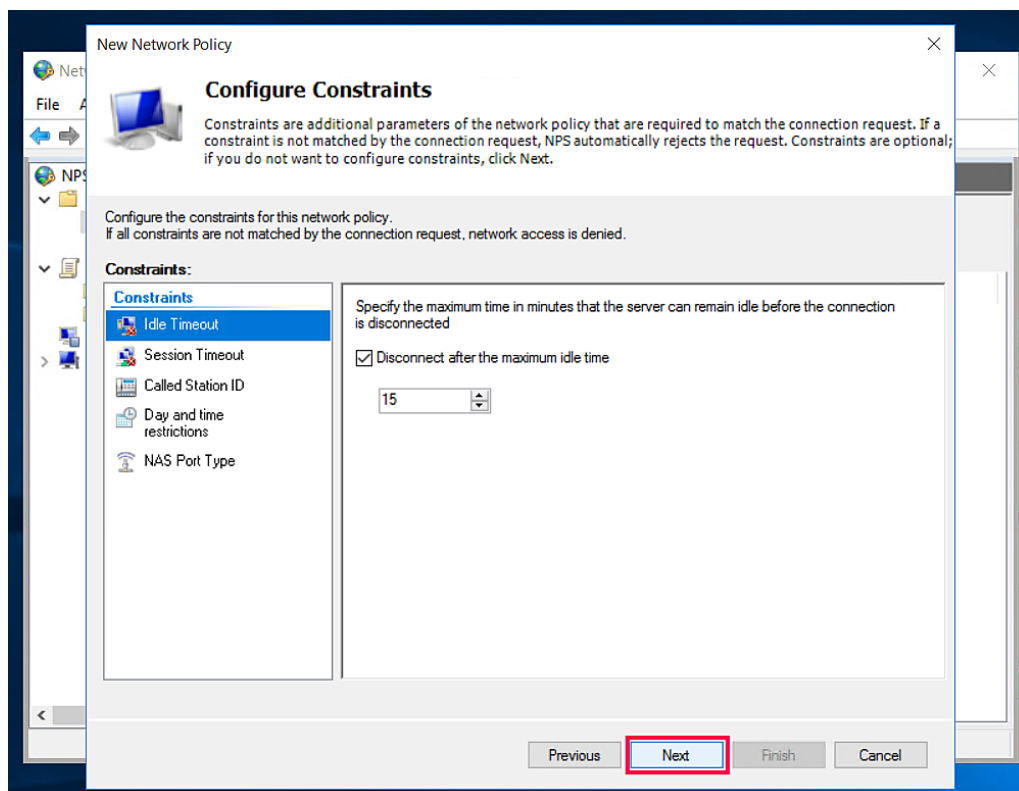


**Step 5:** Configure the protocols for your **Authentication Methods**.

- 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.



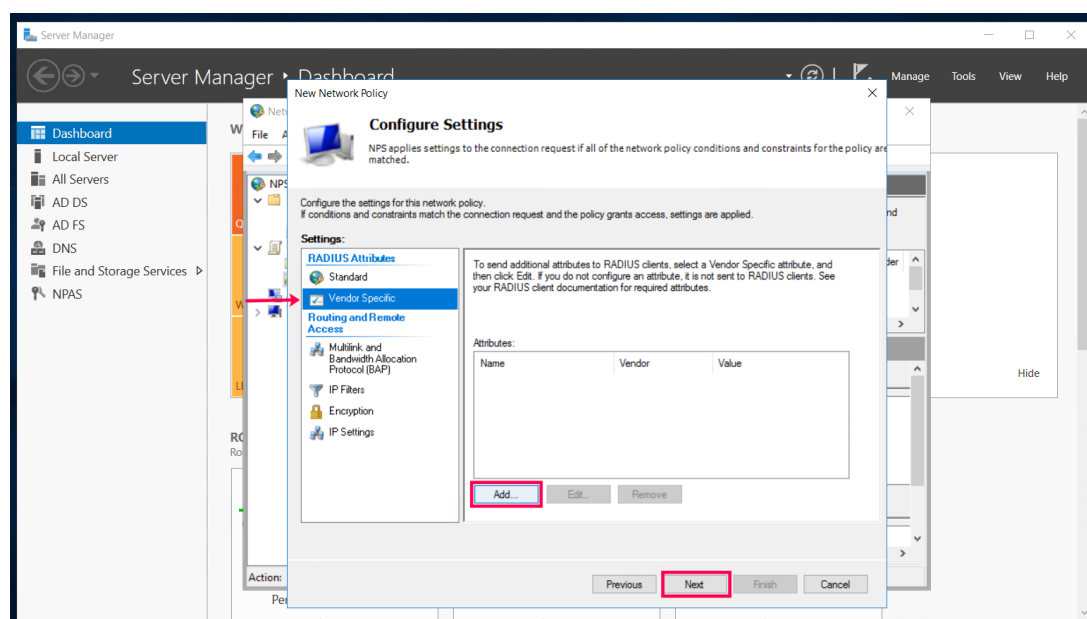
**Step 6:** Configure any constraints you might have, then click **Next**.



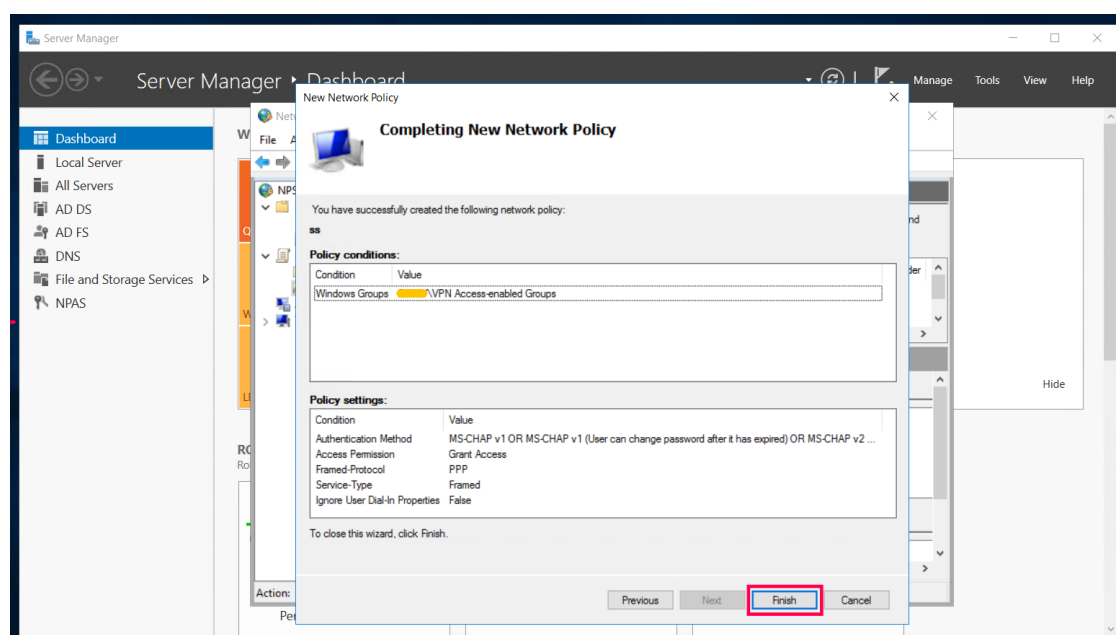
**Step 7:** In the *Configure Settings* window, set additional attributes requested by the VPN server.

**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.



**Step 8:** When all the settings have been configured, 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 "Update" 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\ZOHOCorp\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.

ManageEngine  
**ADSelfService Plus**

### Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus  
RecoveryManager Plus | M365 Manager Plus

## 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  
[www.manageengine.com/products/self-service-password](https://www.manageengine.com/products/self-service-password).

\$ Get Quote

Download

Support