Windows Server

HOW TO CONFIGURE RADIUS/NPS SERVER ON WINDOWS SERVER?

written by Cyril Kardashevsky | May 31, 2023

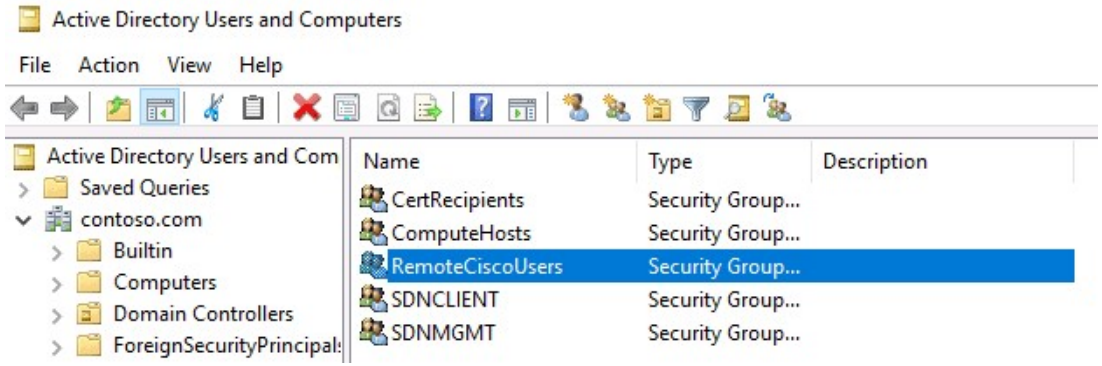
RADIUS (Remote Authentication in Dial-In User Service) is a network protocol implementing authentication, authorization, and the collection of information about the resources being used. It is designed to transfer information between the central platform and network clients/devices. Your remote access (RADIUS) server can communicate with a central server/service (for example, Active Directory domain controller) to authenticate remote dial-in clients and authorize them to access specific network services or resources. NPS allows you to authenticate remote users against Active Directory, allowing them to connect using different client devices and connection types (Wi-Fi access points, wireless controllers, VPN, Dial-up, 802.1x switches, routers, etc.)

In this article, we'll show how to configure a RADIUS server on Windows Server 2022, 2019, or 2016, and how to configure RADIUS authentication on Cisco and Mikrotik switches/routers (act as RADIUS clients)using the Network Policy Server (NPS) service.

Installing RADIUS (NPS) Role on Windows Server 2022/2019/2016

Assuming you have already deployed Active Directory Domain Services environment, because we are going to configure the authentication on the network devices under the AD user accounts.

First, create a new security group in the Active Directory domain (for example, RemoteCiscoUsers) and add all users who will be allowed to authenticate on Cisco routers and switches to this group.



So, you need to install the RADIUS server role on your Windows Server 2022/2019/2016. Open the **Server Manager** console and run the **Add Roles and Features** wizard. The Remote Authentication Dial-In User Service (RADIUS) protocol in Windows Server is a part of the Network Policy Server (NPS) role. NPS role allows you to authenticate remote clients against Active Directory using the Radius protocol.

In the wizard that appears, select the **Network Policy and Access Services** role in the role selection step.

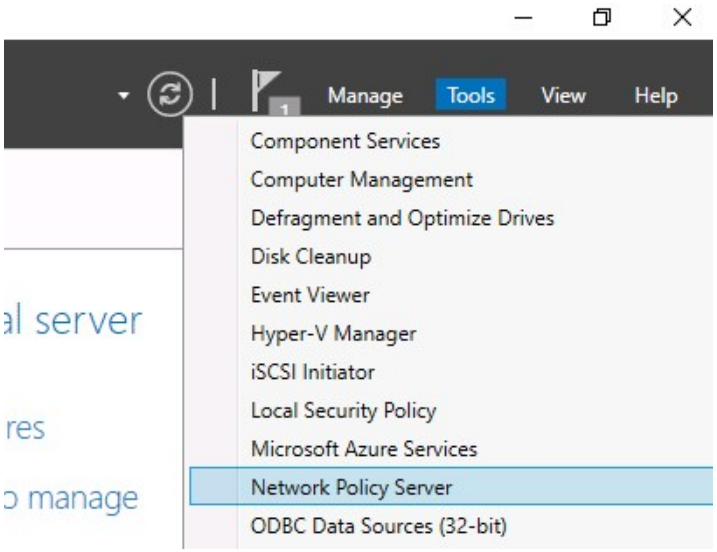
> **Note**. *Also, you can install NPS role and management tools from an elevated PowerShell console:*
>
> ```
> Install-WindowsFeature NPAS –IncludeManagementTools
> ```

Check if the NPAS role is installed on your Windows Server host:

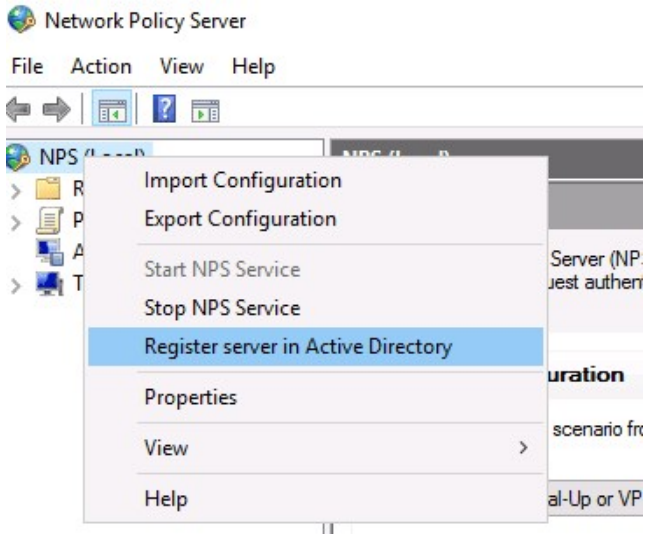
```
Get-WindowsFeature -Name NPAS
```

```
PS C:\Users\Administrator> Get-WindowsFeature -Name npas

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[X] Network Policy and Access Services                  NPAS                        Installed
```

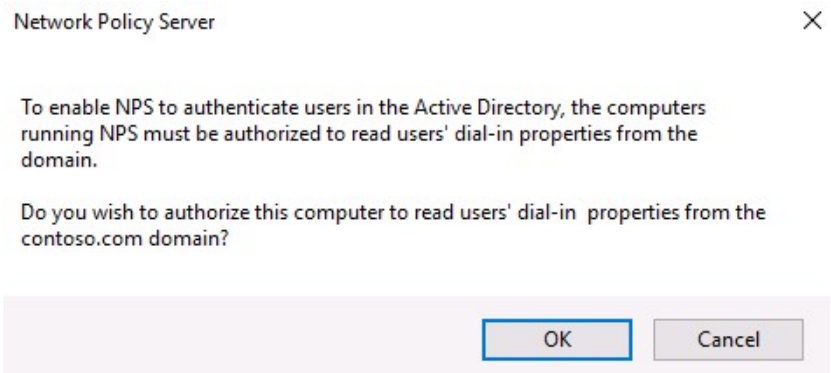
After the role installation is completed, open the Network Policy Server (nps.msc) in the Tools menu.



To use the NPS server in the domain, you must register it in the Active Directory. In the NPS snap-in, right-click on a root and select **Register server in Active Directory**.



Confirm the registration of the server in Active Directory.



Also, you can register your NPS server in Active Directory with a command:

```
netsh ras add registeredserver
```

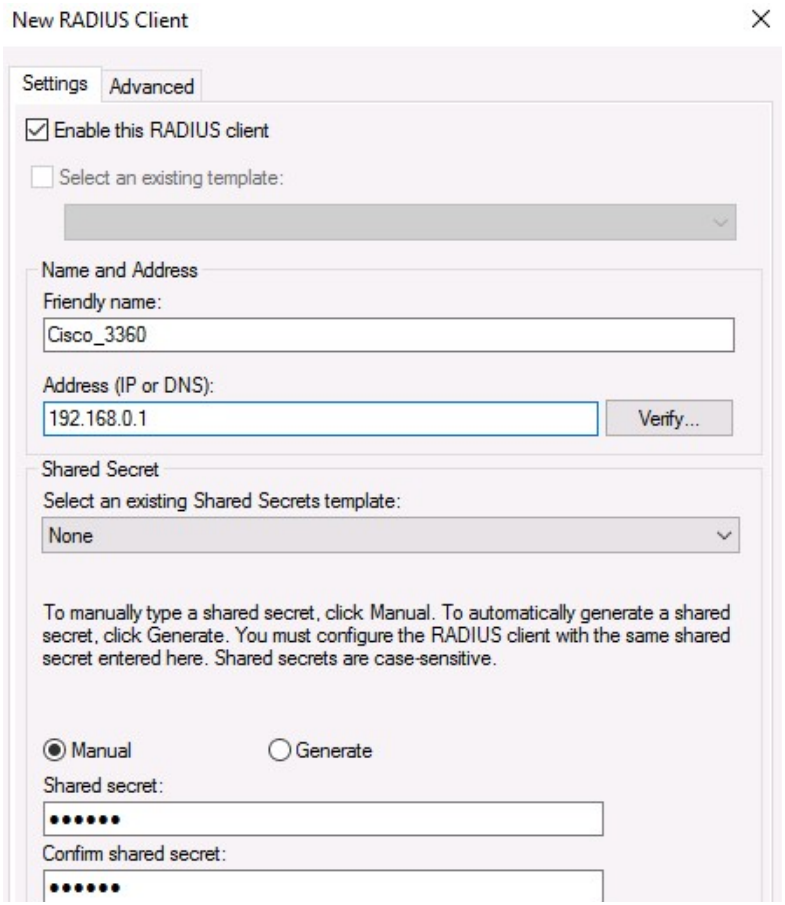
In this case, the server will be given permission to read the properties of Active Directory user accounts to authenticate users. Your NPS host computer account will be added to the built-in domain group **RAS and IAS Servers**.

Now you can add the Radius client. Radius client is the device from which your server will receive authentication requests. This could be a Cisco router, switch, Wi-Fi access point, etc.

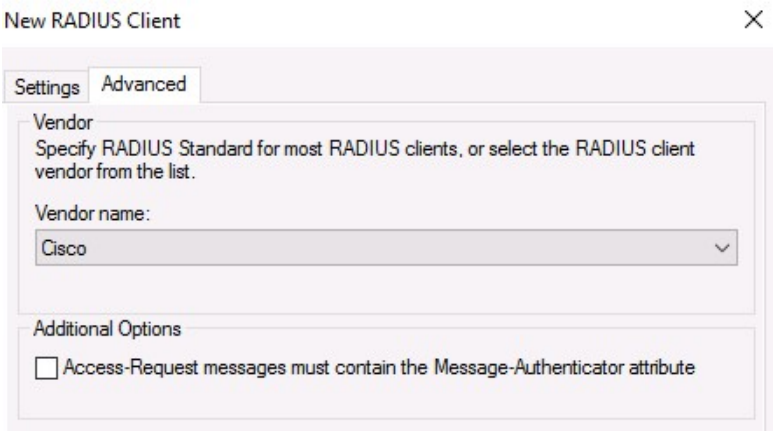
To add the new Radius client, expand the **RADIUS Clients and Servers** section in the NPS console tree and select **New** on the **RADIUS Clients** item.

On the Settings tab, fill the fields **Friendly name**, client **Address** (you can specify IP address or DNS name), and **Shared Secret** + **Confirm shared** password (you will use this password in the configuration of the Cisco switch/router).

> **Note**. *The shared secret password is rarely used in large corporate networks due to the problems with the distribution of shared secrets. Instead of shared passwords, it is recommended to use certificates. If you have a corporate Certification Authority (CA) deployed to implement PKI infrastructure, you can request a *.p12 certificate for the Radius/NPS server. Just import the certificate to the personal certification store of the Local Machine.*



In the Advanced tab, select Vendor name – Cisco.



You can use the PowerShell command instead of the NPS GUI to add a new RADIUS client. In this case, you can use the New-NpsRadiusClient PowerShell cmdlet:

```
New-NpsRadiusClient –Address "192.168.31.1" –Name "cisco2960" –SharedSecret "Zb+kp^JUy]v\ePb-h.Q*
d=weya2AY?hn+npRRp[/J7d"
```

> **Note**. *If you are running Datacenter Edition of Windows Server 2022/2019/2016 on the NPS host, you can configure RADIUS clients on NPS by IP address range. This allows you to quickly add a large number of generic RADIUS clients (such as wireless access points) to the NPS console, rather than adding them individually. Specify the IP address range instead of the IP address of the device, using the format* **10.1.0.0/22**.

By default, NPS uses the following UDP ports to send and receive RADIUS traffic: 1812, 1813, 1645, and 1646. When you install the NPS role on Windows Server, rules for these ports are automatically created and enabled for Windows Defender Firewall. You can list these Windows Firewall rules using PowerShell:

```
Get-NetFirewallRule -DisplayGroup "Network Policy Server"
```

If your RADIUS client is located in a DMZ network or an external security perimeter, you must create the appropriate firewall rules.

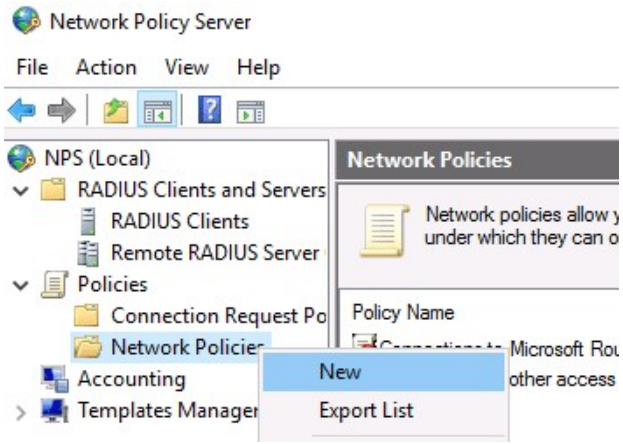
Configuring NPS Policies on the RADIUS Server

NPS policies allow you to authenticate remote users and grant them access permissions configured in the NPS role. Using NPS access policies, you link the RADIUS client to the domain security group that determines the user privileges on CISCO devices.

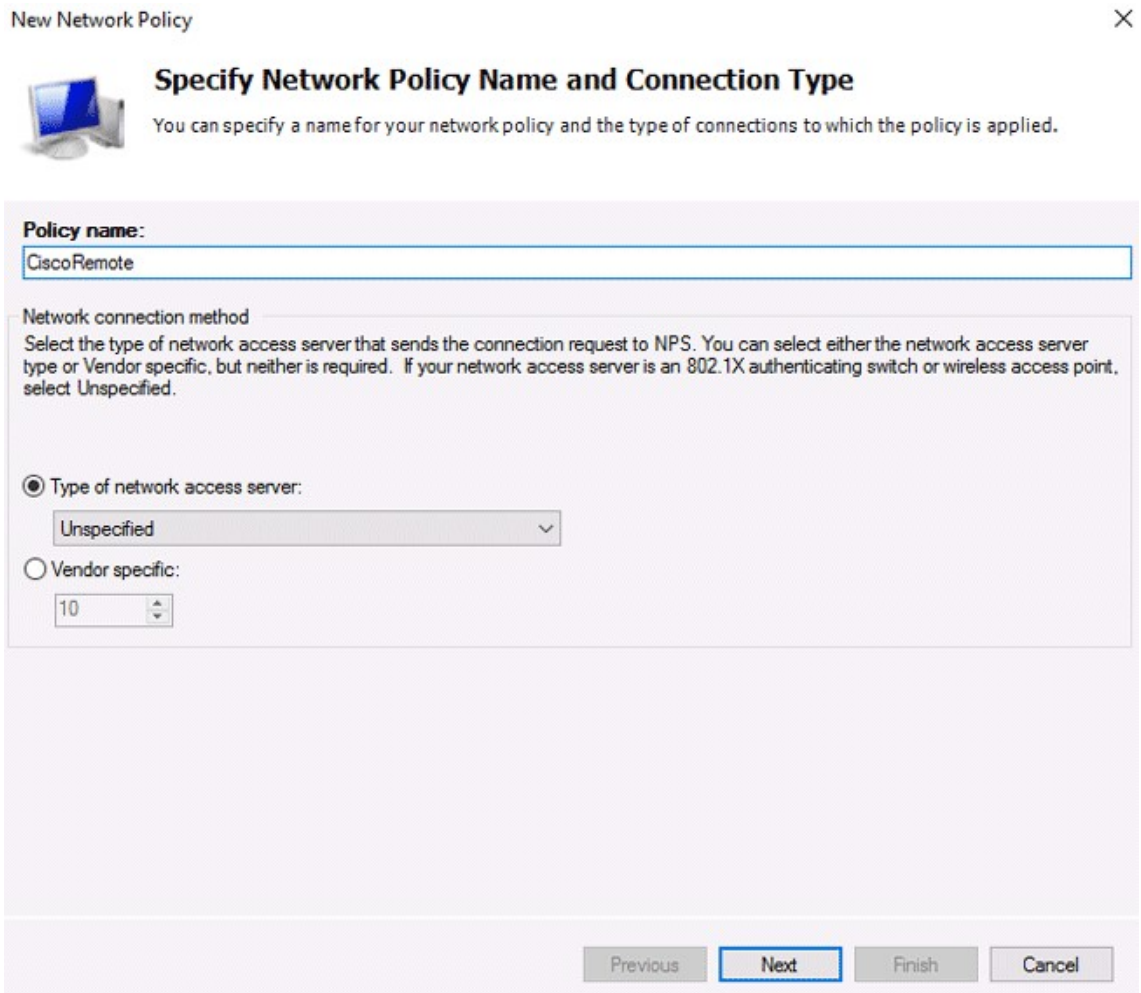
There are two types of policy on a RADIUS server:

- **Connection request policies** — these policies define a set of conditions that determine which RADIUS servers should authenticate and authorize connection requests received from RADIUS clients;
- **Network policies** — a set of conditions and settings that allow you to specify who is authorized to connect to your network and a list of assigned privileges. These policies are processed sequentially from top to bottom;

In our case, we will use only the NPS Network policies. Expand the **Policies** > **Network Policies** branch and select **New**:



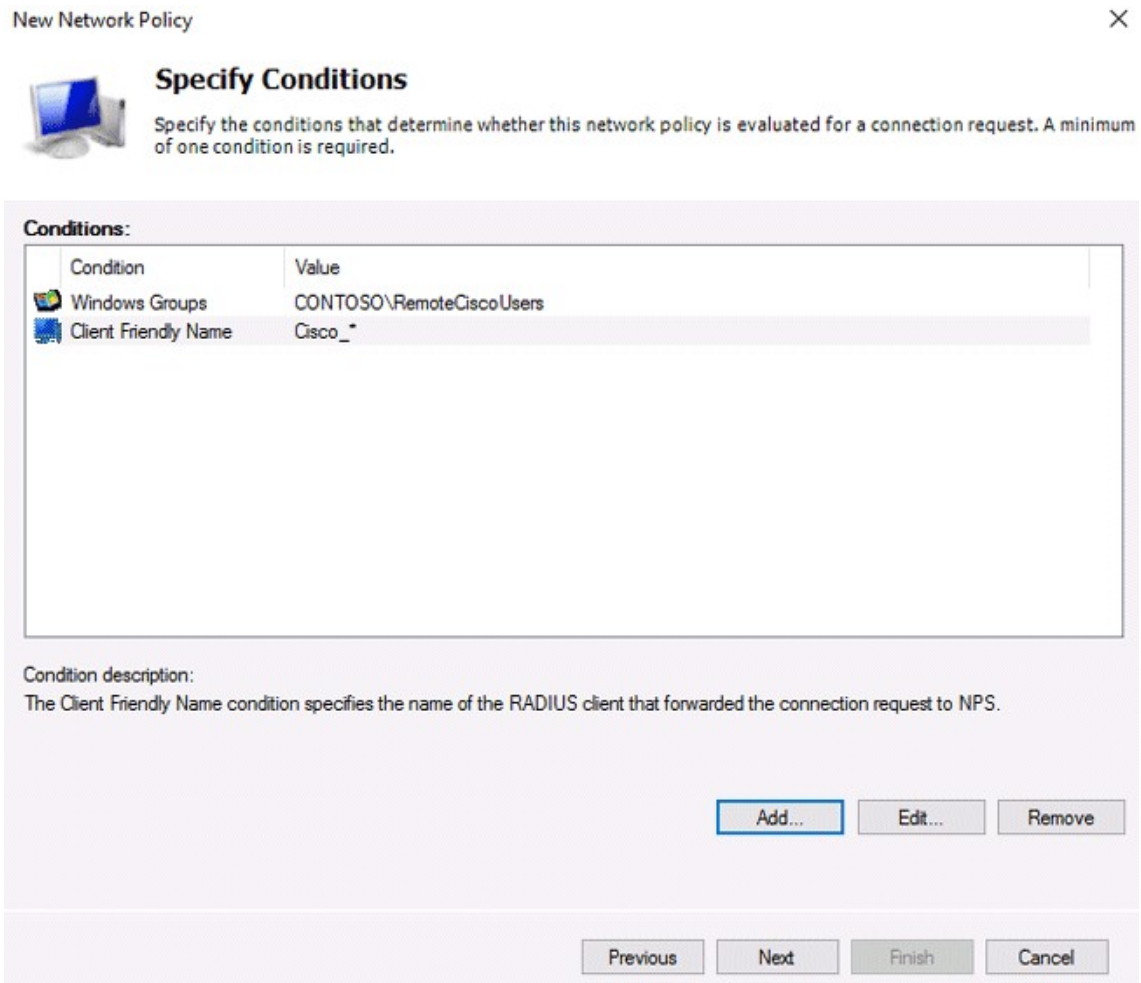
Specify the Policy name, the type of network access server should remain unchanged (Unspecified).



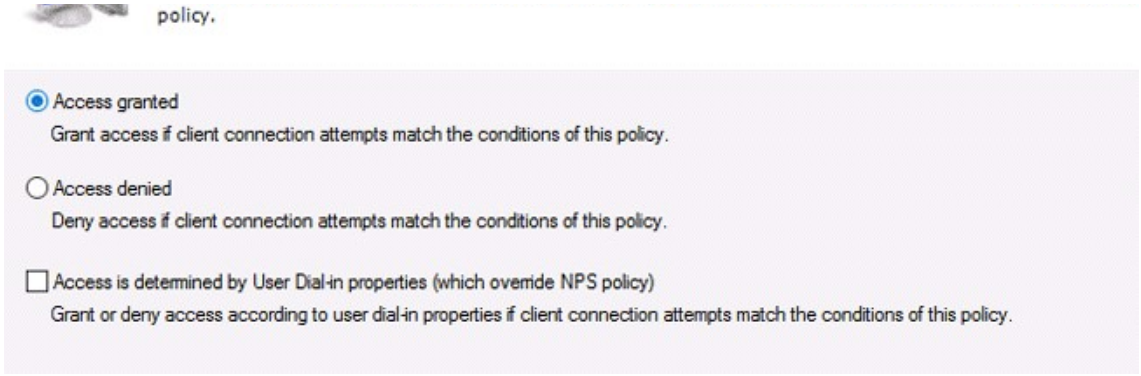
In the next step **Specify conditions**, you need to add the conditions under which this RADIUS policy will be applied. Let's add two conditions — the authorized user must be a member of a specific domain security group, and the device you want to access has a specific name. Use the **Add** option to create a new condition by selecting the **Windows Group** type (add the RemoteCiscoUsers group) and specifying the **Client Friendly Name** (Cisco_*).

> **Note**. *The Client Friendly Name field may differ from the DNS name of your device. We will need it in the*

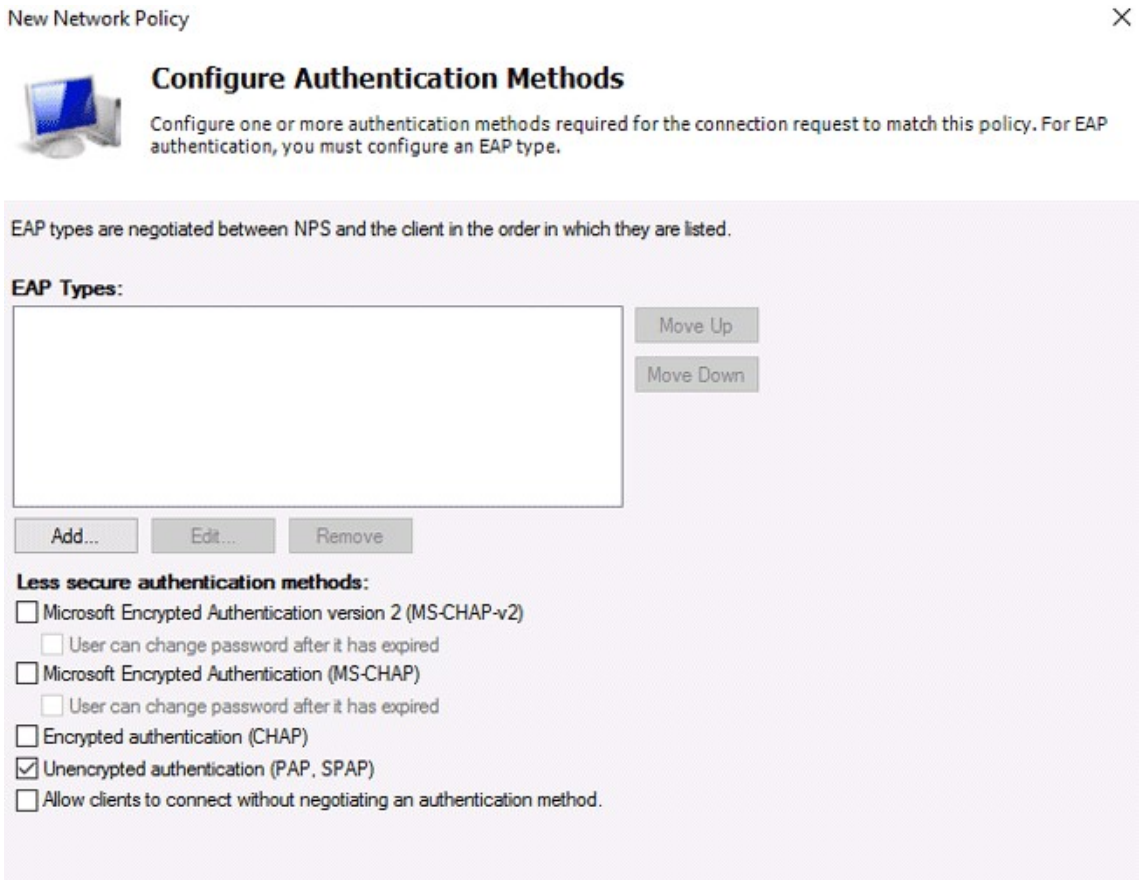
further steps to identify a specific network device when creating a Remote Access Policy. For example, you can use this name to specify a mask through which several different RADIUS clients are processed by a single access policy.

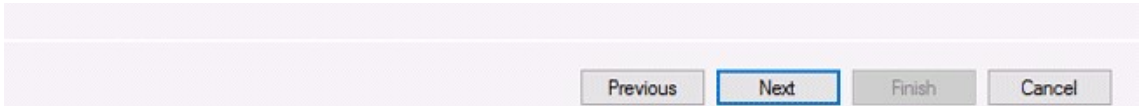


On the next screen, select **Access Granted**.



Our Cisco switch supports only the Unencrypted authentication method (PAP, SPAP), so that's why we'll uncheck all other options.

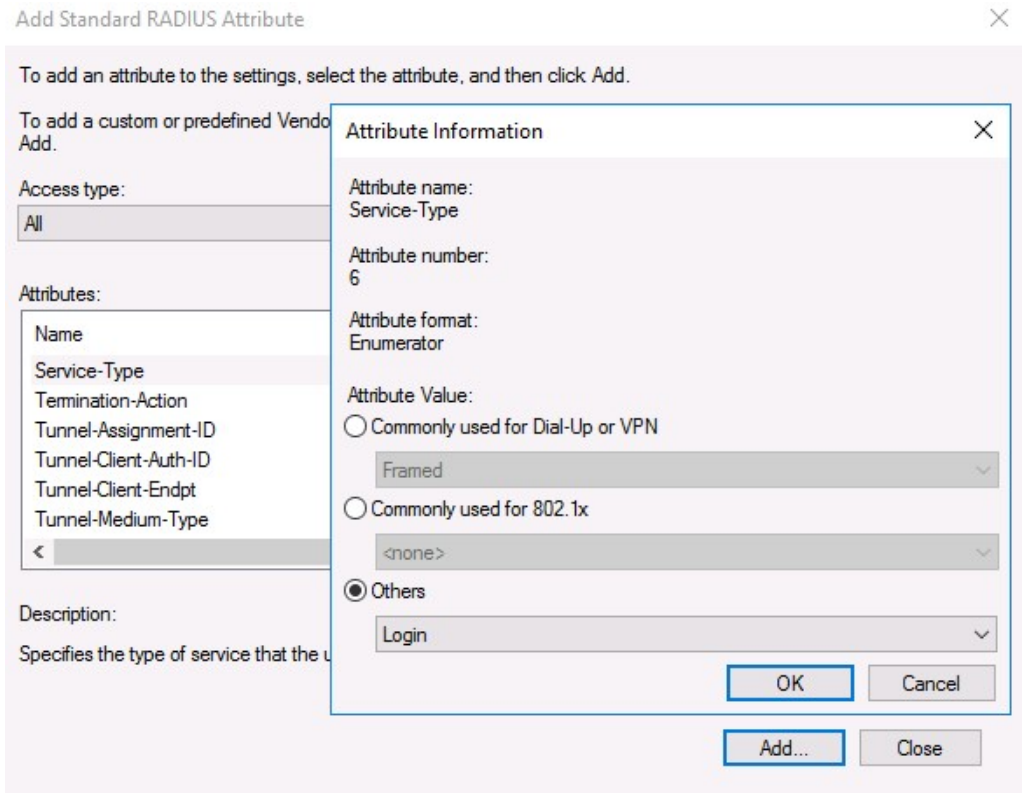




Skip the next configuration Constraints step.

In the Configure Settings section, go to the RADIUS Attributes > Standard section. Delete the existing attributes there and click the Add button.

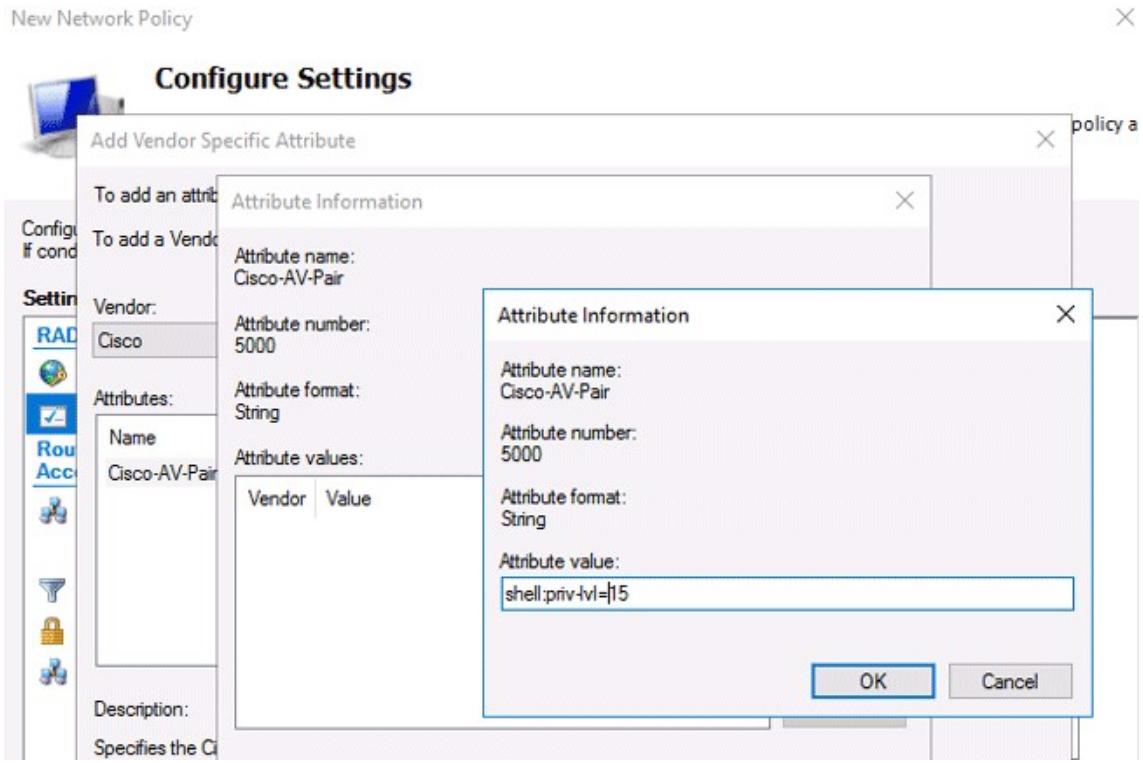
Select Access type > All, then Service-Type > Add. Specify Others = Login.



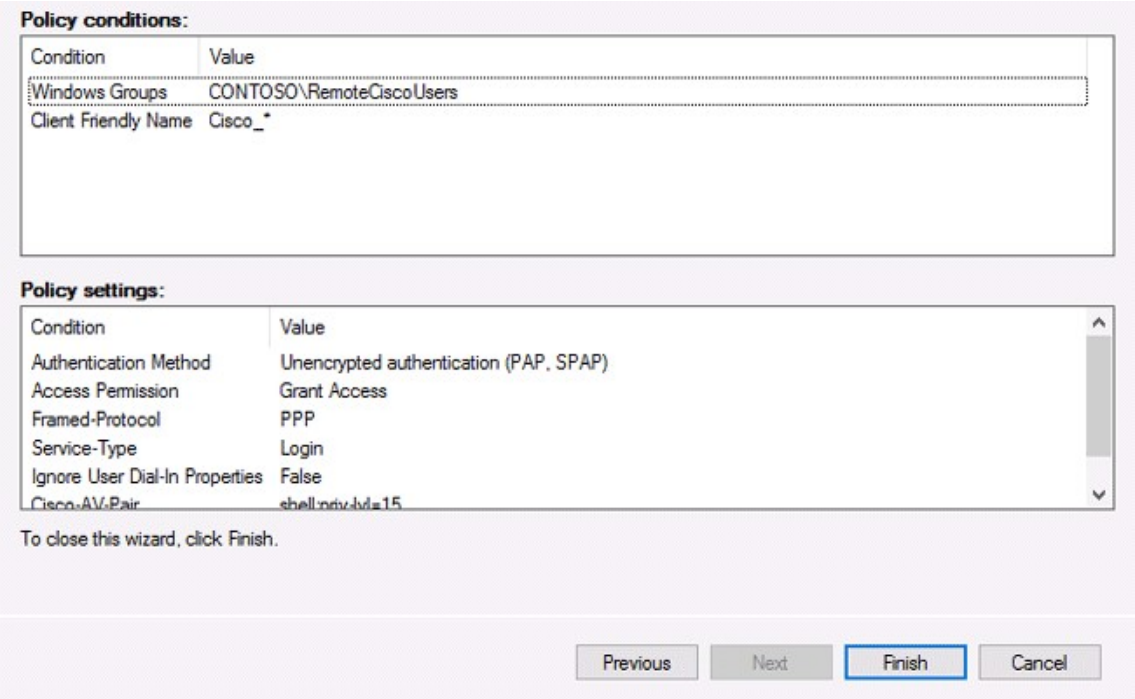
Now add a new attribute in the RADIUS Attributes > Vendor Specific section. Under Vendor, select Cisco, and click Add. Here you need to add information about the attribute. Click Add and specify the following value:

```
shell: priv-lvl = 15
```

This value means that the user authorized by this policy will be granted a maximum (15) administrative access privileges on the Cisco device.



The last screen displays all selected NPS policy settings. Click Finish.

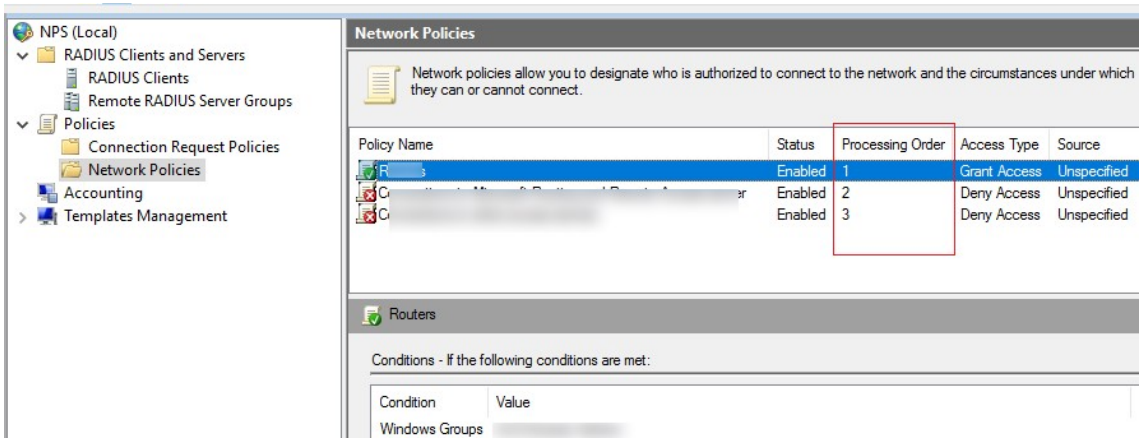


> **Hint**. *You can back up the current NPS server configuration to the XML file using the command:*
>
> ```
> Export-NpsConfiguration -Path c:\ps\backup_nps.xml
> ```

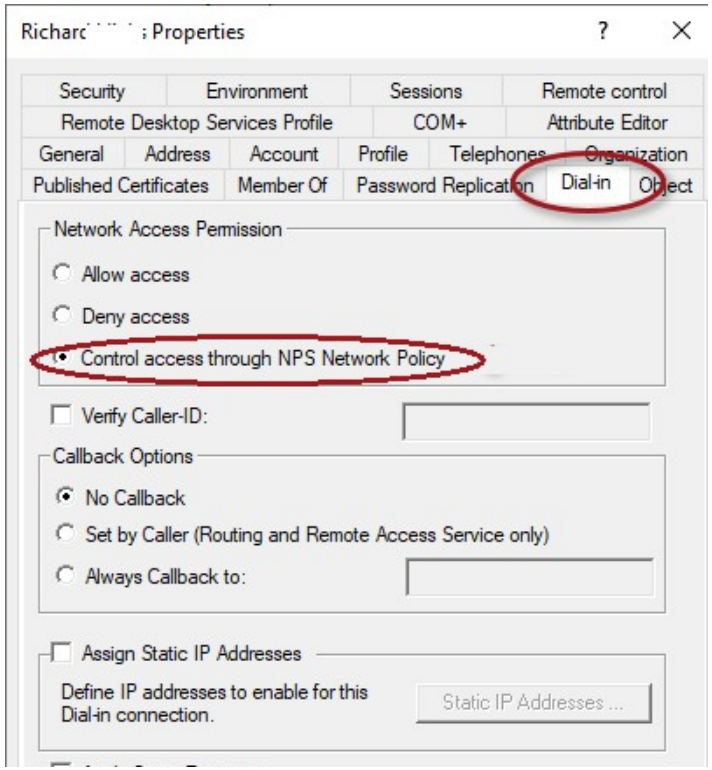
If you need to restore the NPS configuration from a previously created backup file, run:

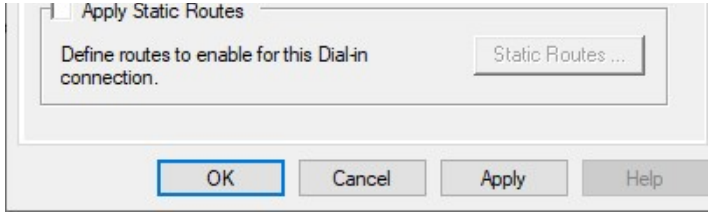
```
Import-NpsConfiguration -Path c:\ps\backup_nps.xml
```

When creating and planning RADIUS policies, pay attention to what matters in their order. NPS policies are processed from the top to down, and when it turns out that all the conditions in the next policy are met, their further processing is terminated. You can change the priority of policies in the NPS console using the Processing Order value.



To enable the user account to be used for Radius authentication, open the Active Directory Users and Computers snap-in (dsa.msc), find the user, open its properties, go to the **Dial-In** tab and select the **Control access through NPS Network Policy** option in the **Network Access Permission** section.





Also, you can check the current option value using PowerShell:

```
Get-ADUser richard.doe -Properties msNPAllowDialin -Server dc1.theitbros.com
```

If the above command did not return any result (empty), this means that the default value “Control access through NPS Network Policy” is used.

If you want to reset this user attribute to the default state, use the command:

```
Set-ADUser richard.doe -Clear msNPAllowDialin -Server dc1.theitbros.com
```

Or you can reset this attribute for all users in the specific Active Directory OU using the LDAP filter:

```
Get-ADUser -SearchBase "ou=Users,ou=Paris,dc=theitbros,dc=com" -LDAPFilter "(msNPAllowDialin=*)"
| % {Set-ADUser $_ -Clear msNPAllowDialin}
```

Configuring RADIUS Authentication on Cisco Devices

Once you have created the NFS policy, you can proceed to configure your Cisco routers or switches for authentication on the newly installed RADUIS server.

Because we use domain accounts for authorization, the user credentials must be transmitted over the network in an encrypted form. To do this, disable the telnet protocol on the switch and enable SSHv2 on Cisco device using the following commands in configuration mode:

```
configure terminal

crypto key generate rsa modulus 1024

ip ssh version 2
```

This is how the **Authentication, Authorization, and Accounting (AAA)** service works in Cisco IOS: if the response from the server is not received, the client assumes that the authentication has failed. Make sure you created a local user to access your Cisco device in case the RADIUS server is unavailable for any reason.

You can create a local user with the following command:

```
username cisco_local password $UPerrP@ssw0rd
```

To make the use of SSH mandatory and disable remote access using Telnet, execute the following commands:

```
line vty 5 15

transport input ssh
```

Below is an example of the configuration for authorizing a Radius server for the Cisco Catalyst Switch:

```
aaa new-model

aaa authentication login default group radius local

aaa authorization exec default group radius if-authenticated

radius-server host 192.168.1.16 key Sfs34e#sf

#Specify your RADIUS server IP address and key for encryption (the shared secret that we specifie
d on the RADIUS server)
```

```
service password-encryption

# Enable password encryption
```

If you have several Radius servers, add them to the group:

```
aaa group server radius radius_srv_group

server 192.168.1.16

server 192.168.101.16
```

This completes the minimum switch configuration and you can try to check Radius authentication on your Cisco device.

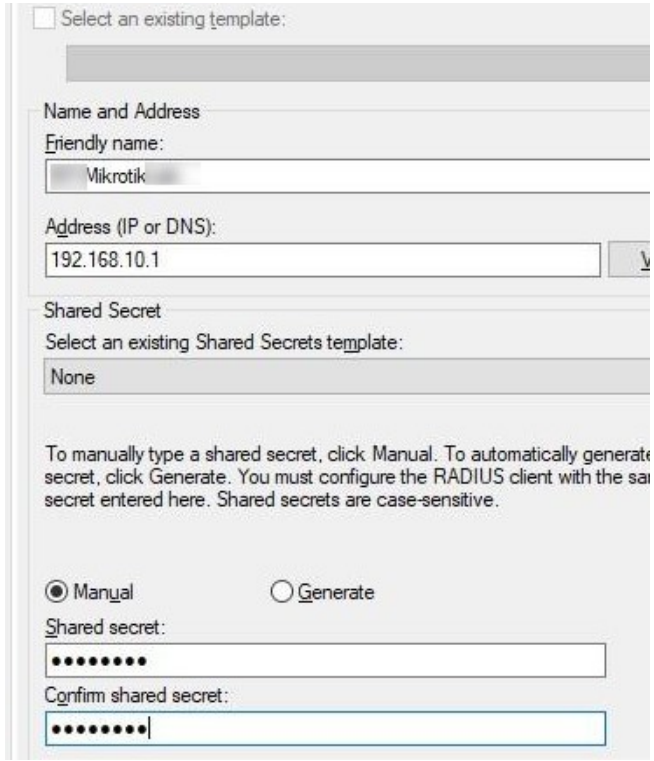
How to Enable Microtik (RouterOS) User Authentication via RADIUS?

In this part, we will show you how to configure RADIUS authentication for VPN user connections via a Mikrotik router (RouterOS based).

Open the Network Policy Server console (nps.msc) and create a new Radius client.

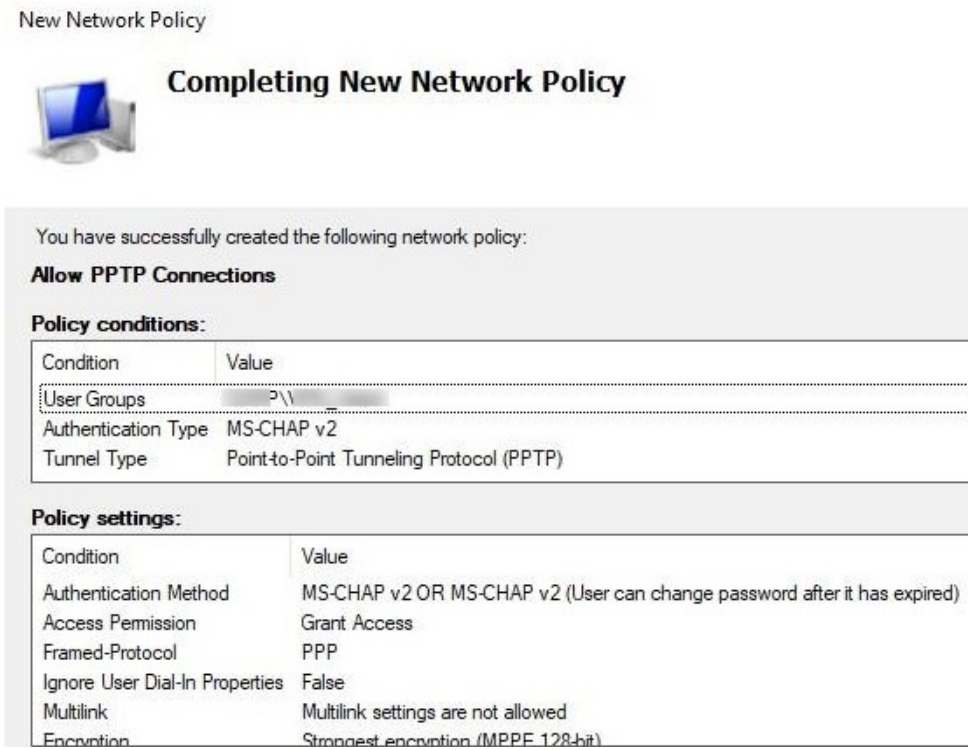
Select **New RADIUS Client** and configure the following settings:

- Enable this RADIUS Client;
- Friendly Name — enter the name of your Mikrotik router here;
- Address — specific the IP address of the Mikrotik router;
- Specify your Pre-shared secret key.



Create a new Network Policy with the following settings:

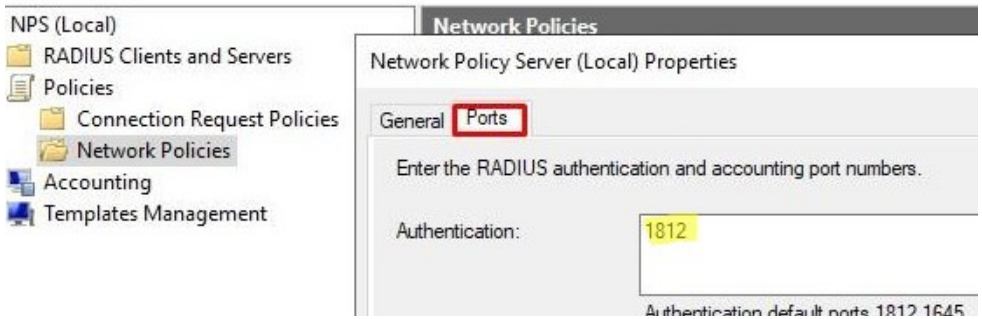
- **User Groups** — specify the name of the domain user group that is allowed to authenticate on your Mikrotik router;
- **Authentication Type** — MS-CHAPv2;
- **Tunnel Type** — Point-to-Point Tunneling Protocol (PPTP);
- **Access Permissions** — Access granted;
- In the **Configure Authentication Methods** window, leave only **MS-CHAPv2** and allow users to change expired passwords (**User can change password after it has expired** option);
- **Multilink and Bandwidth Allocation Protocol (BAP)** – Do not allow Multilink connections;
- In the **Standard** section, remove Service-Type – Framed and leave only Framed-Protocol **PPP**;
- **Encryptions** — leave only the strongest encryption (MPP 128-bit) method.

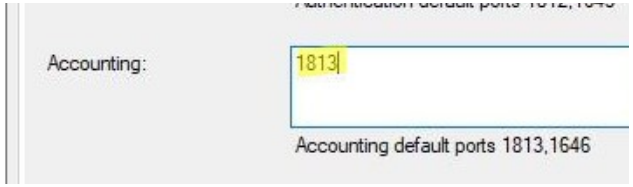


Once you have created a new policy, open the Network Policy Server settings.

Leave only the following UDP ports for the RADIUS server communications:

- Authentication — 1812;
- Accounting — 1813.

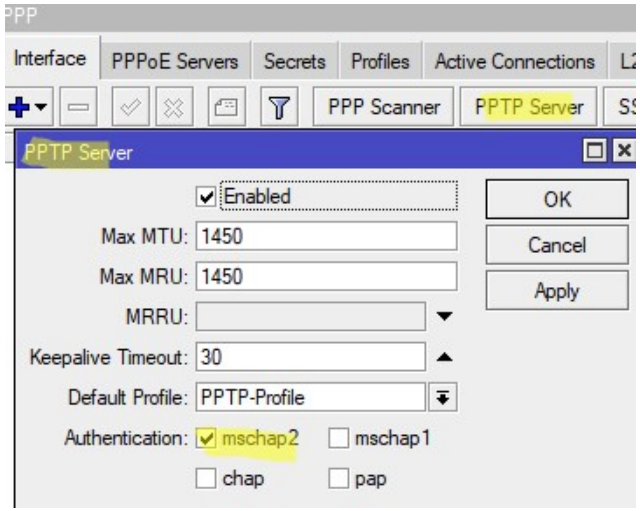




Check if these UDP ports are open in Microsoft Defender Firewall Rules. If not, open them manually.

Now you need to configure the connection settings for Windows Server RADIUS in the Mikrotik configuration (we assume that PPP VPN Server is already configured on RouterOS).

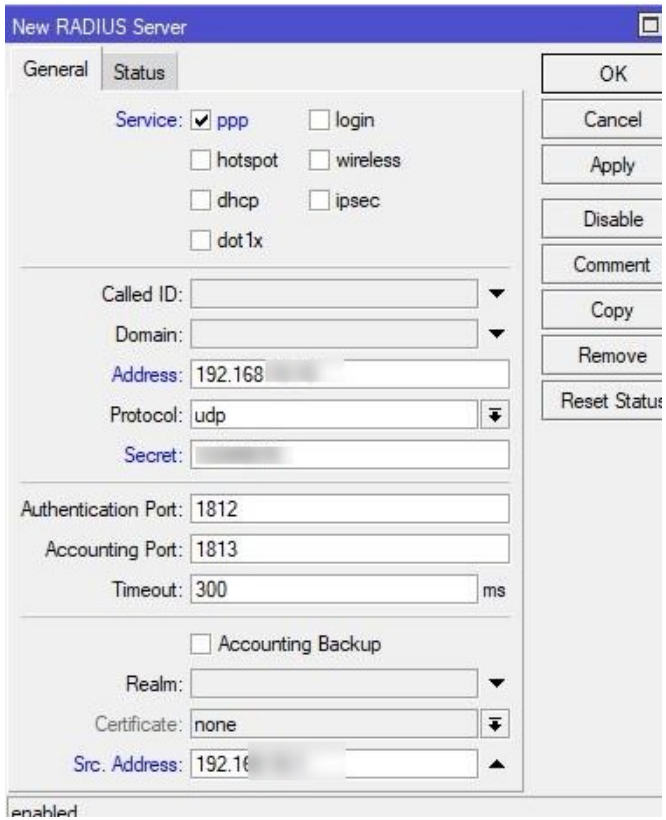
Check in the PPTP server settings that only **mschap2** is allowed to use for authentication.



Now we need to configure the connection to Radius NPS server. Select New Radius Server and specify the following options:

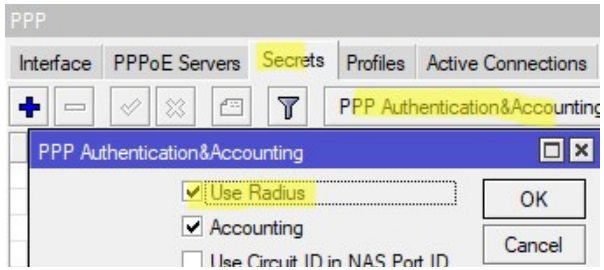
- Service: ppp;
- Address: IP address of the RADIUS server;
- Secret: pre-shared key that you specified in the network policy settings;
- Src/ Address: Mikrotik IP address from which traffic will be sent to NPS;

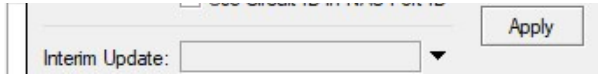
- Authentication Port: 1812;
- Accounting Port: 1813.



Add appropriate access rules to Mikrotik Firewall.

Then go to **Secrets** > **PPP Authentication and Accounting** and enable the **Use Radius** option.





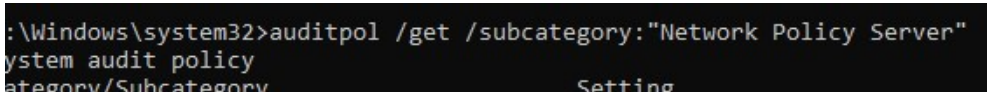
It remains to configure a PPTP VPN connection to your Mikrotik VPN on users' computers. Users can use their Active Directory account credentials to authenticate against Mikrotik (accounts must be added to the AD group that you have specified when creating the Miktotik Network Policy on NPS).

How to View the NPS/RADIUS Event Logs on Windows?

To enable NPS Server Radius Authentication logging, you need to enable the Network Policy Server audit policy. You can enable this policy via the local Group Policy Editor (gpedit.msc). Go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Advanced Audit Policy Configuration** > **Audit Policies** > **Logon/Logoff** > **Audit Network Policy Server** and check the option to audit both success and failure logon attempts.

Or you can enable this NPS audit policy with the following commands:

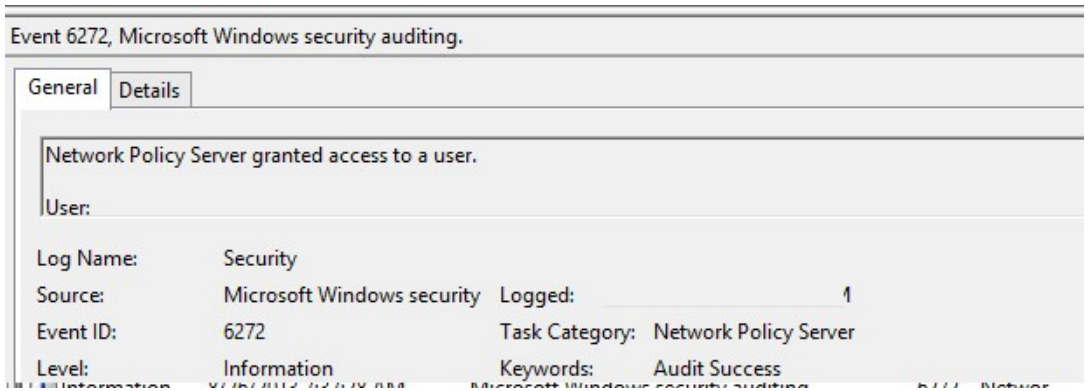
```
auditpol /get /subcategory:"Network Policy Server"

auditpol /set /subcategory:"Network Policy Server" /success:enable /failure:enable
```



```
ogon/Logoff
 Network Policy Server                    Success and Failure
```

Now you can open the Event Viewer console (eventvwr.msc), go to the Windows Logs > Security, and filter the event by the Event ID 6272.

Network Policy Server granted access to a user.



If the user has entered an incorrect password or is not authorized to log on through the RADIUS Client, Event ID 6272 is displayed:

> *Network Policy Server denied access to a user.*

If a user enters an incorrect password multiple times, their account will be locked out in accordance with your Account Lockout Policy in AD.

> *Event ID: 6279*
> *Network Policy Server locked the user account due to repeated failed authentication attempts.*

If you need to find all NPS authorizations events for the specific user (Richard.Doe in this example), use the next PowerShell script:

```
$Query = @"
```

```
<QueryList>

<Query Id="0" Path="Security">

<Select Path="Security">

*[EventData[Data[@Name='SubjectUserName'] and (Data=theitbros\richard.doe')]] and

*[System[(EventID='6272')]]

</Select>

</Query>

</QueryList>

"@

$events = Get-WinEvent -FilterXML $Query

$ipaddr = @{ label="IP"; Expression={$_.properties[9].value} }

$events | select $ipaddr | group "IP" | format-table Count, Name -autosize
```

CONF WINDOWS SERVER

1

Cyril Kardashevsky

I enjoy technology and developing websites. Since 2012 I'm running a few of my own websites, and share useful content on gadgets, PC administration and website promotion.

previous post
HOW TO FIX USER PROFILE SERVICE FAILED THE SIGN IN ON WINDOWS?

next post
POWERSHELL: MOVE COMPUTER TO OU

3 COMMENTS

CESAR REPLY

August 23, 2021 - 12:35 pm

Thank you for the guide! great work.

MM REPLY

January 23, 2022 - 7:40 pm

Hi Cyril,
Kudos! Thank you for making the time to share a very well-written and informative Radius Server on Windows tutorial blog.
MM

JASPER REPLY

April 6, 2022 - 8:20 am

Please help me understand how to set up vpn reconnect, I have specific directive to configure vpn reconnect on Radius VPN server (server 2019), and I cannot find this information.

LEAVE A COMMENT

Your Comment

Name*

Email*

Save my name, email, and website in this browser for the next time I comment.

SUBMIT

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Privacy Policy Contact Us