RADIUS Configuration with Cisco 200/300 Series Managed Switches and Windows Server 2008

Objective

Remote Authorization Dial-in User Service (RADIUS) offers a robust way of authentication of users to allow access to a network service. Therefore, RADIUS servers offers a centralized access control, where the server administrator decides if a specific segment is authenticated or not using RADIUS. This article explains the general steps to establish RADIUS in a client/server environment, where the client is represented by the Cisco 200/300 Series Managed Switch and the server is running a Windows Server 2008 with RADIUS enabled.

Applicable Devices

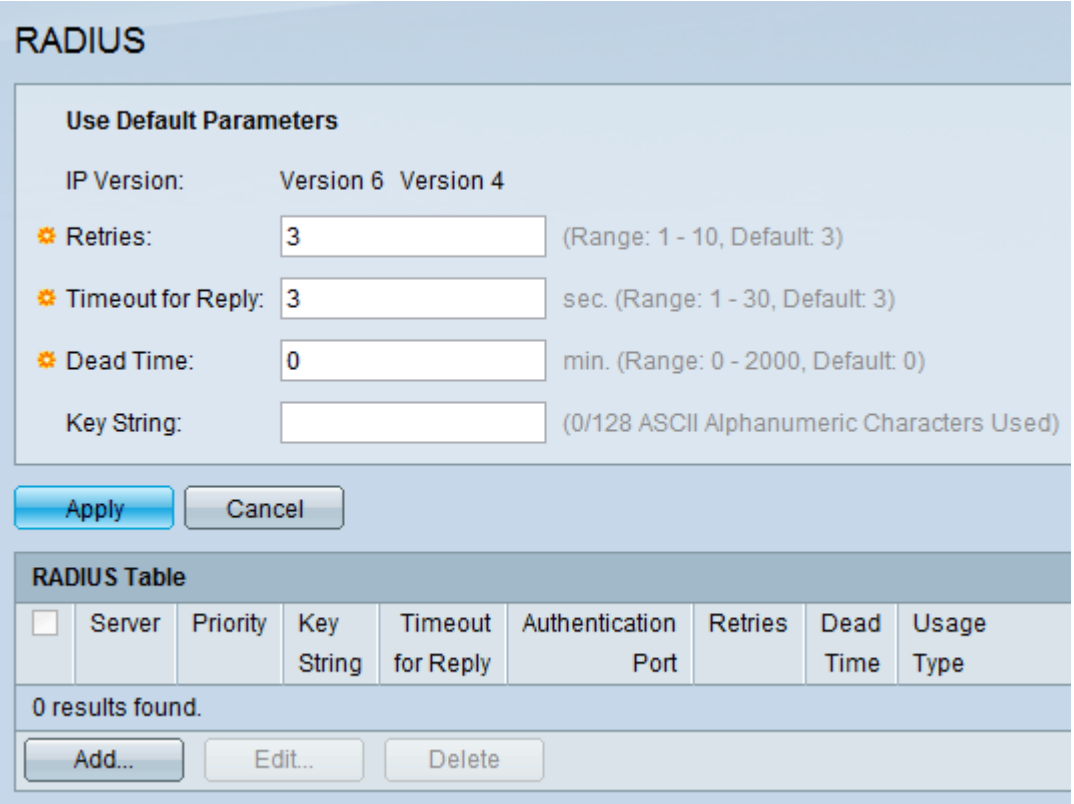
- Cisco 200/300 Series Managed Switches

Step-by-Step Procedure

The configuration takes place in two parts. First we have to set the switch as a RADIUS client, then we have to set the server properly for RADIUS.

Setting RADIUS on the switch

Step 1. In the SG200/300 Series configuration utility, choose **Security > RADIUS**. The *RADIUS* page opens:

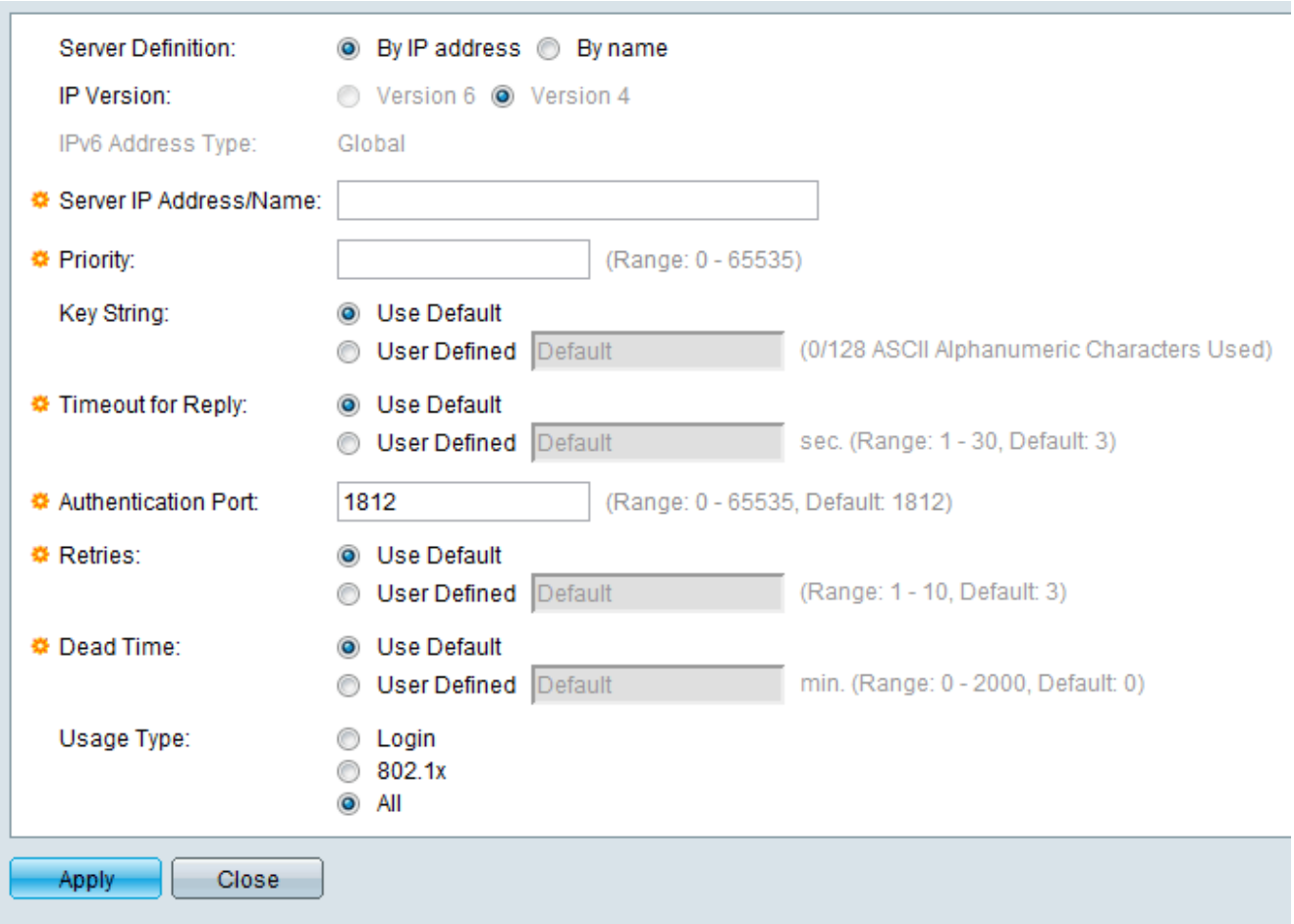


Step 2. Enter the default RADIUS settings.

- IP Version — Displays the supported IP version.
- Retries — In this field, enter the number of transmitted requests that are sent to the RADIUS server before a failure occurs.
- Timeout for Reply — In this field, enter the time, in seconds, the switch waits for an answer from the RADIUS server before it tries a query again.
- Dead Time — In this field, enter the time in minutes the switch waits before bypassing the RADIUS server.
- Key String — In this field, enter the default string used for authentication and encryption between the switch and the RADIUS server. The key must match the one configured at the RADIUS server.

Step 3. Click **Apply** to update the running configuration of the switch with the RADIUS settings.

Step 4. You need to add the RADIUS server to the switch. Click **Add**. The *Add RADIUS Server* page opens in a new window:



Step 5. Enter The values in the fields for the server. If you want to use the default values, select **Use Default** in the desired field.

- Server Definition — In this field, you specify how to connect to the server, either by IP address, or by the server name.
- IP Version — If the server is going to be identified by IP address, then select IPv4 or IPv6 address.
- IPv6 Address Type — This field display the type Global of the IPv6 address.
- Server IP Address/Name — In this field, enter the IP address or the domain name of the RADIUS server.
- Priority — In this field, enter the priority of the server. If more than one server is configured, the switch will attemp to connect to each server according to this priority value.
- Key String — In this field, enter the default string used for authentication and encryption between the switch and the RADIUS server. The key mmust match the one configured at the RADIUS server.
- Timeout for Reply — In this field, enter the time, in seconds, the switch waits for an answer from the RADIUS server before it tries a query again.
- Authentication Port — In this field, enter the UDP port number set for the RADIUS server for authentication requests.
- Retries — In this field, enter the number of transmitted requests that are sent to the RADIUS server before a failure occurs.
- Dead Time — In this field, enter the time in minutes the switch waits before bypassing the RADIUS server.
- Usage Type — In this field, enter the authentication type of the RADIUS server. There are three options:

- Login — RADIUS server authenticates users that wants to administer the switch.

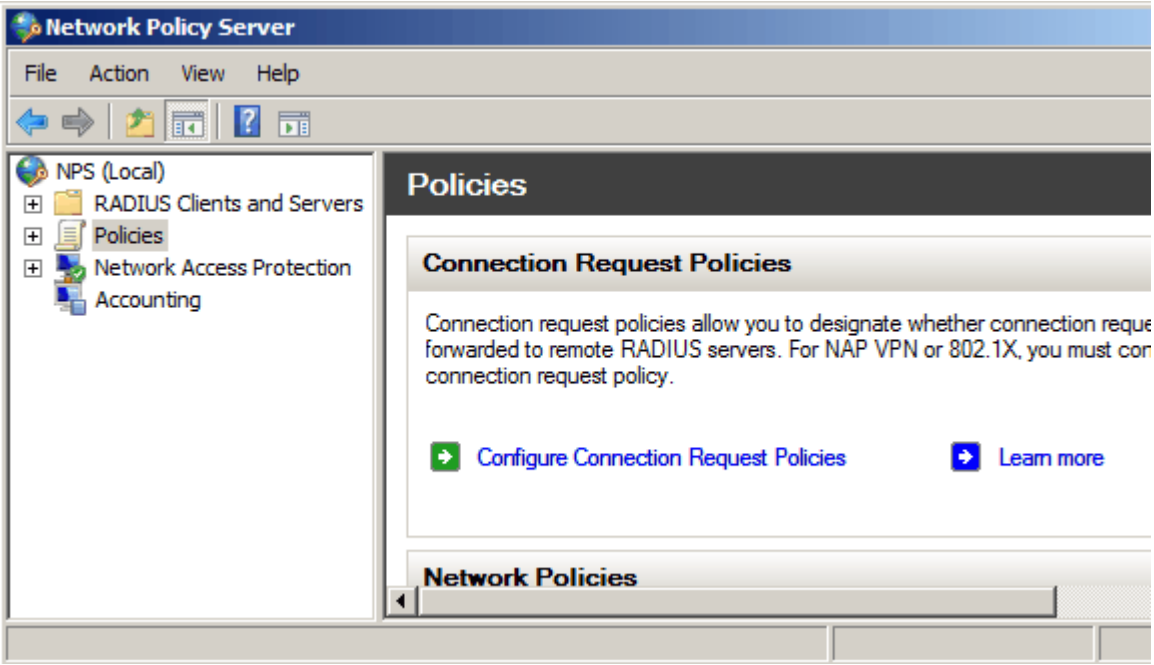
- 802.1X — RADIUS server is used for 802.1X authentication.

- All — RADIUS server is used for Login and 802.1X authentications.

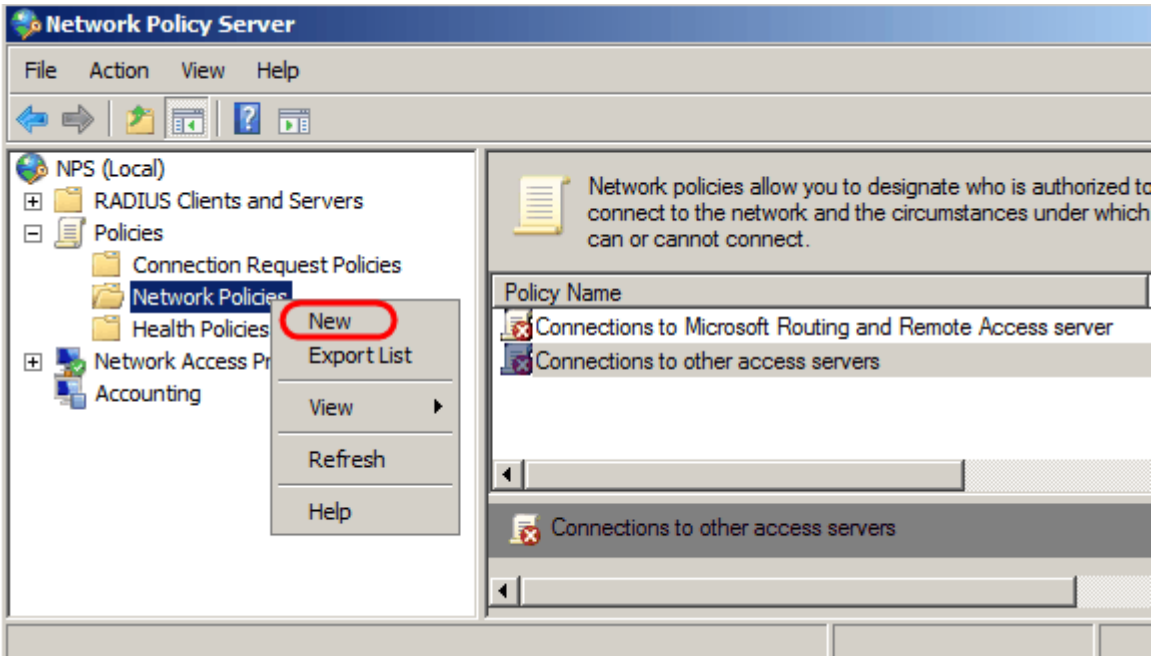
Step 6. Click **Apply** to add the server definition to the running configuration of the switch.

Configuring Windows Server 2008 for RADIUS

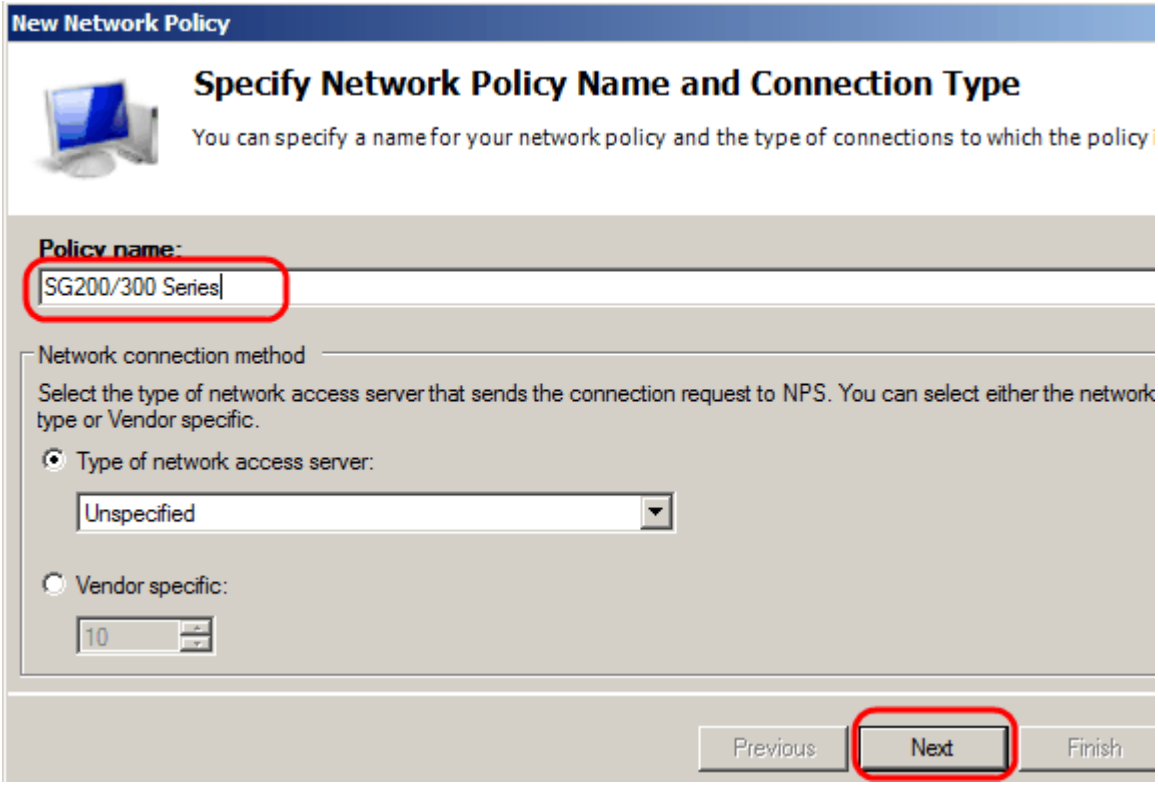
Step 1. In the Windows Server 2008 machine, choose **Start > Administrative tools > Network Policy Server**. The *Network Policy Server* window opens:



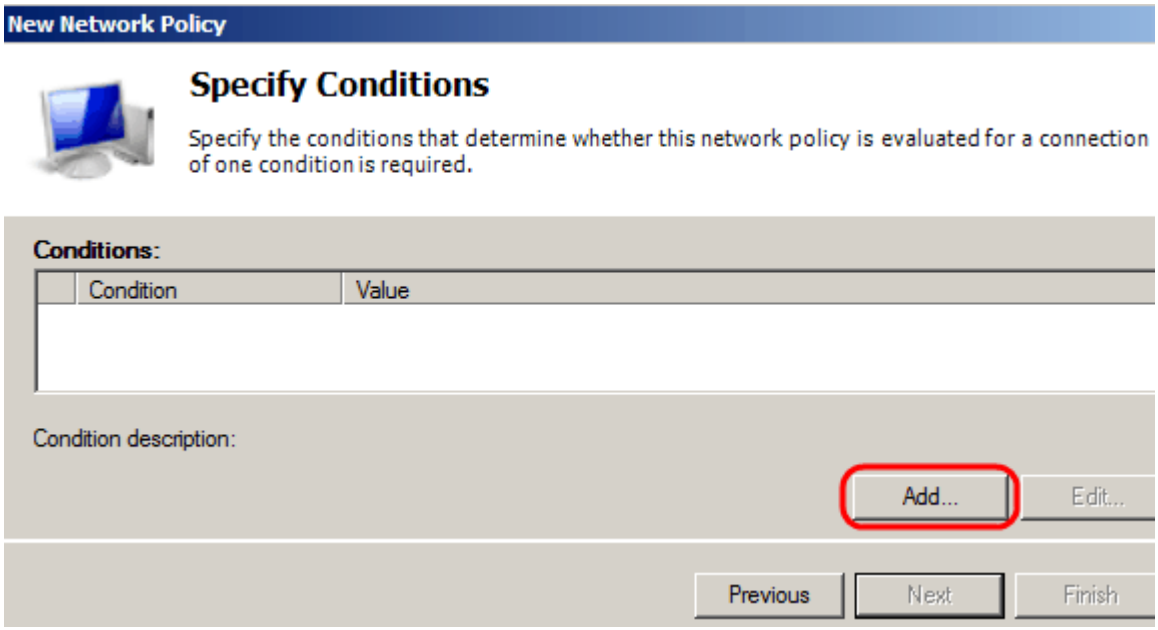
Step 2. To enable the RADIUS server for a specific segment of the network, you need to create a new network policy. To create a new Network Policy, choose **Policies > Network Policy**, then right click and select **New**. The *New Network Policy* windows opens:



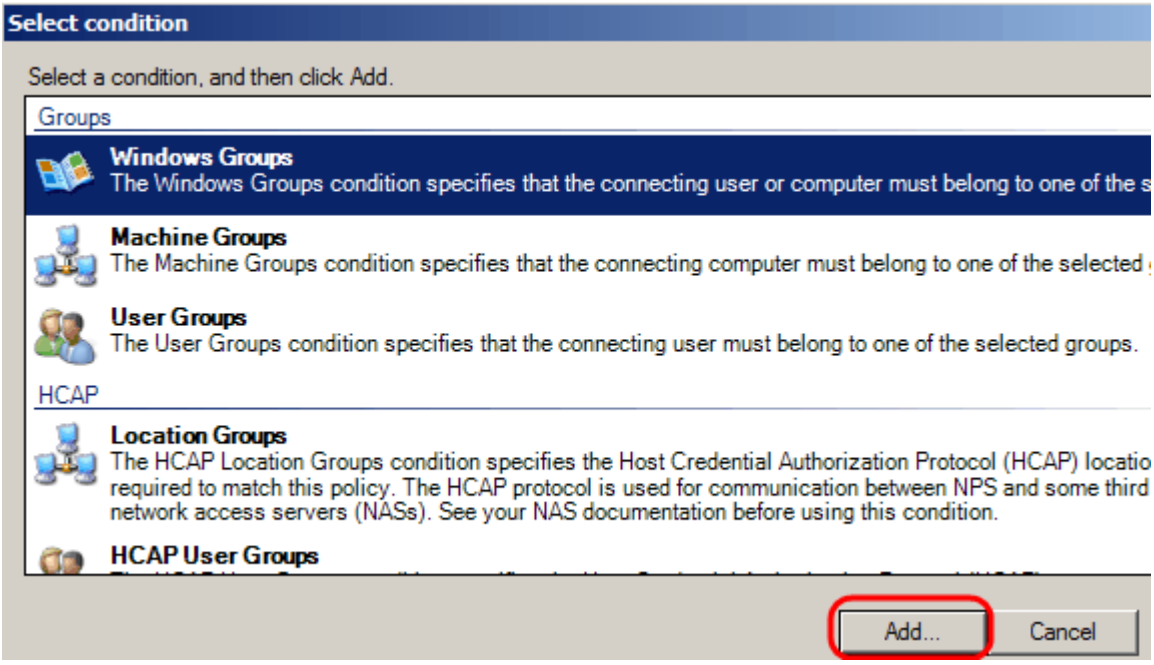
Step 3. In the Policy Name field, enter the name for the new policy. Click **Next**.



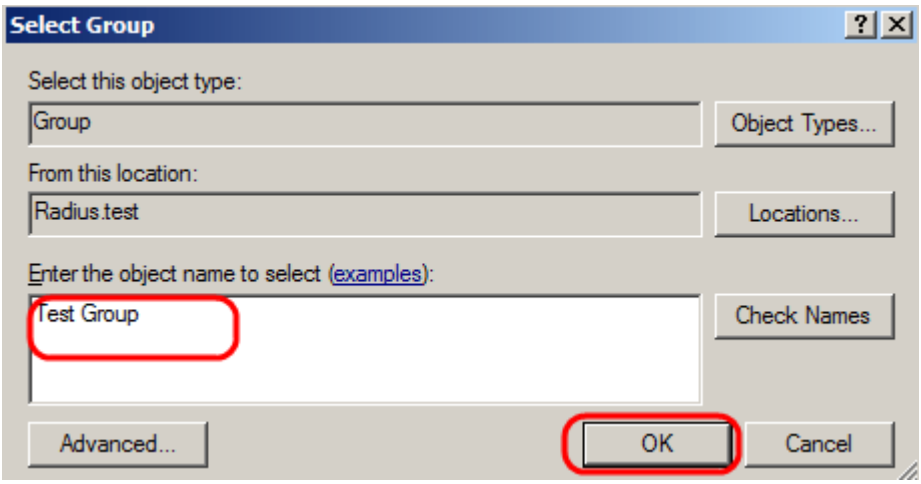
Step 4. You need to specify the conditions of this policy. There are two conditions needed: to which segment of users the RADIUS server is going to be implemented, and the method used to connect to this segment. Click **Add** to add these conditions.



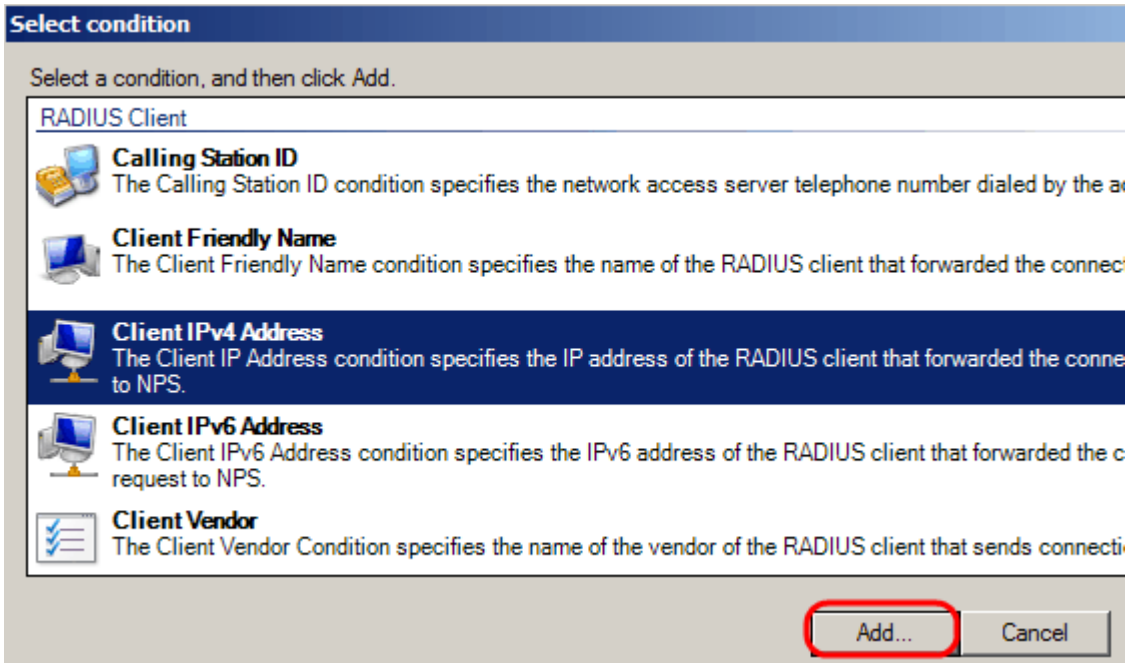
Step 5. Under Groups, there are three options: Windows Groups, Machine Groups, and User Groups. choose the group according to the setting of the network and click **Add**. A new window opens according to the group selected, click **Add Groups**.



Step 6. Select the object type, the location, and enter the name of the object. Click **Ok**, then click **Ok**. Click **Add** to add the next condition.

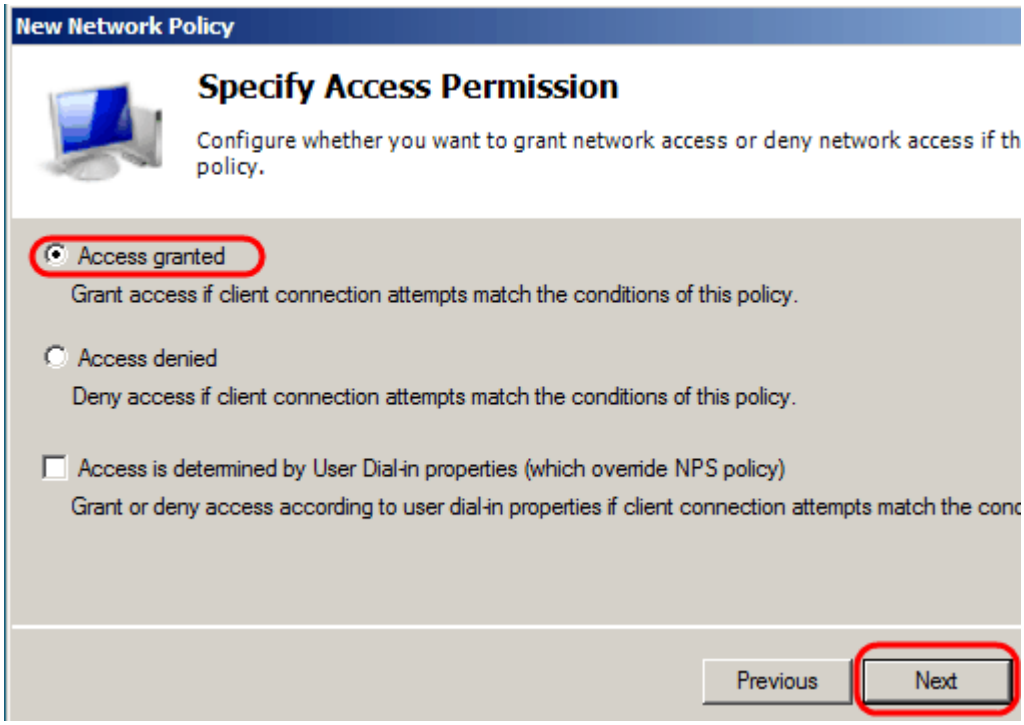


Step 7. Under RADIUS Client, select choose IPv4 Address as the method to connect the server to the RADIUS clients, which in this case, will be the switch IP address. Click **Add**.

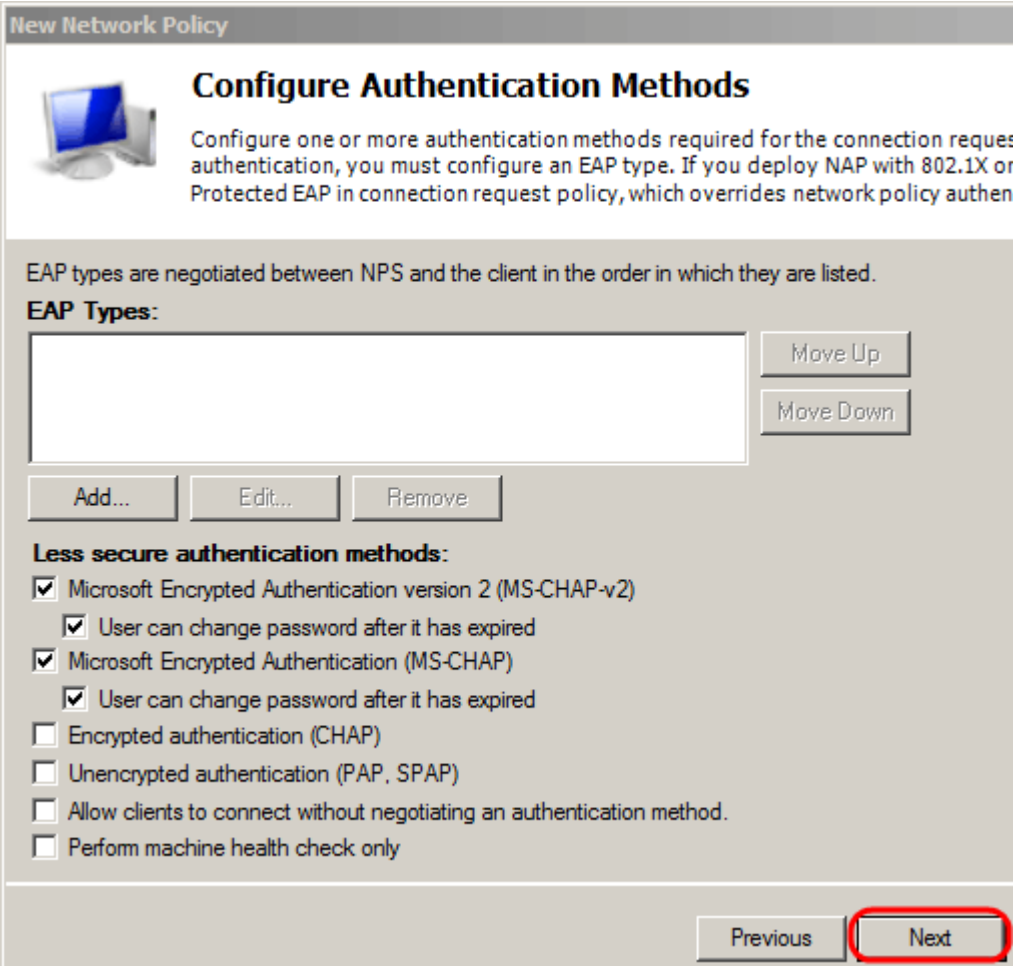


Step 8. Enter the corresponding IP address, then click **Ok**. A list with the added conditions is showed, click **Next**.

Step 9. In the Specify Access Permission page, select **Access Granted**. Click **Next**.



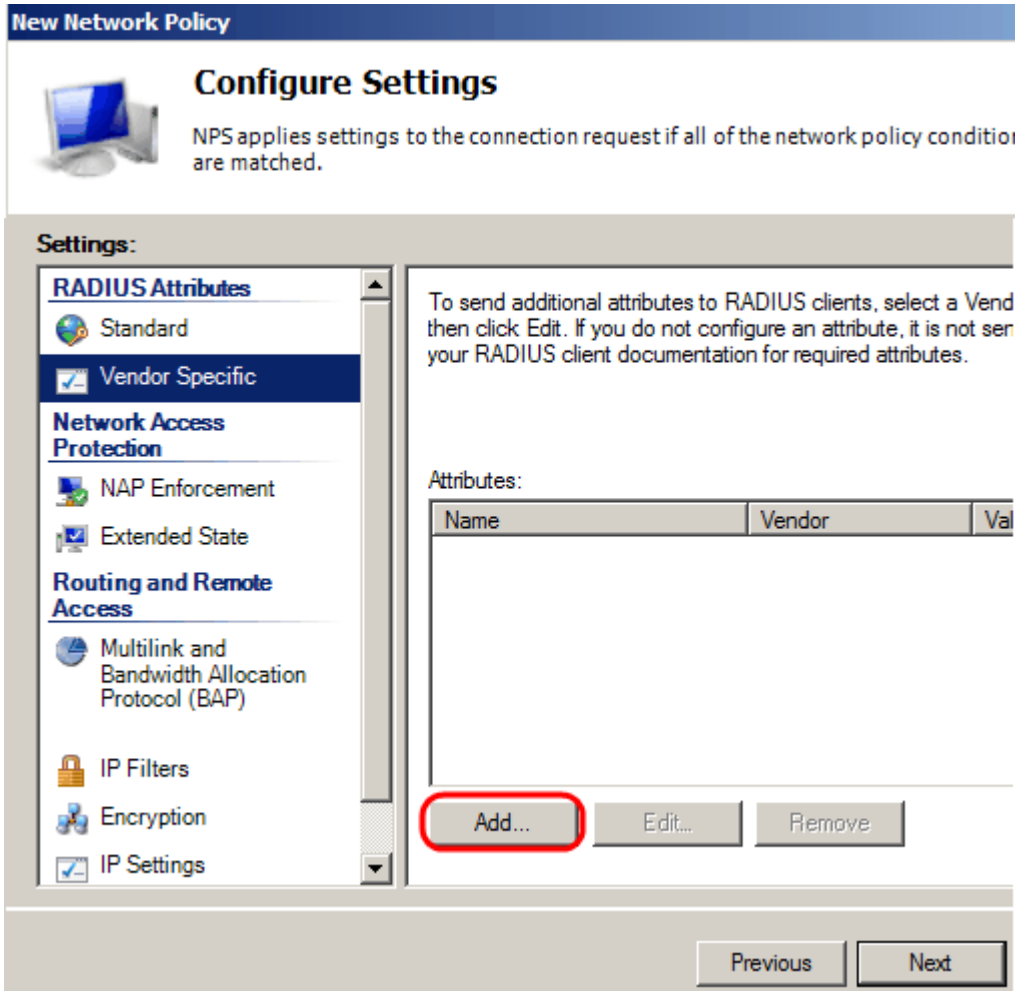
Step 10. In the authentication page, set the authentication method that best fit your network. Click **Next**.



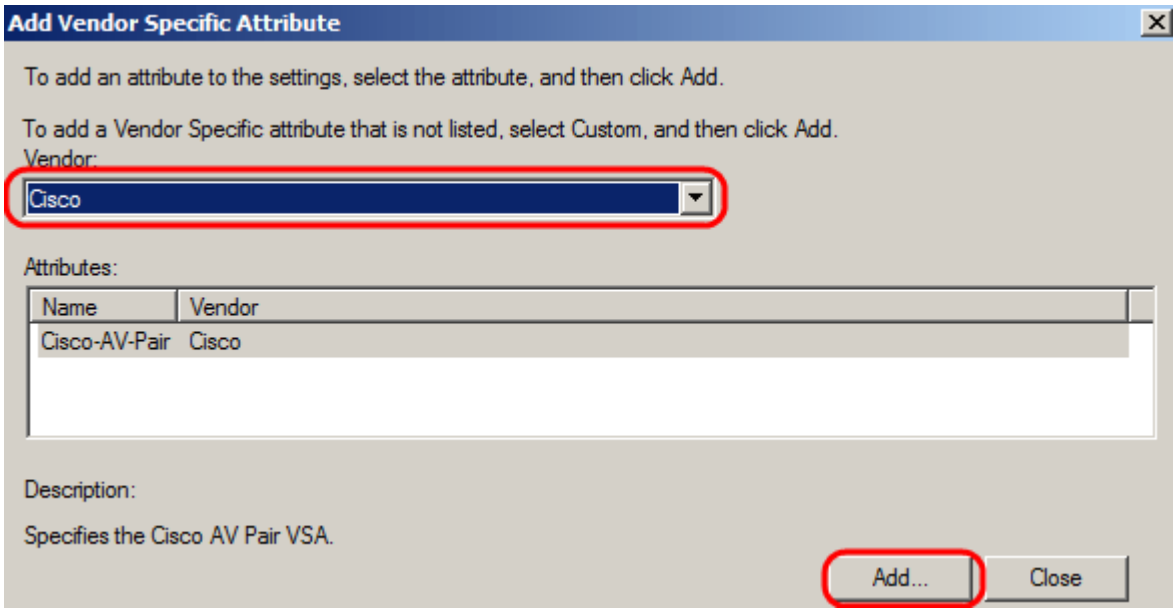
Step 11. In the Configure Constraints window, use the default values. Click **Next**.

Step 12. In the Configure Settings page, under RADIUS Attributes, click **Vendor Specific**, then click **Add**.

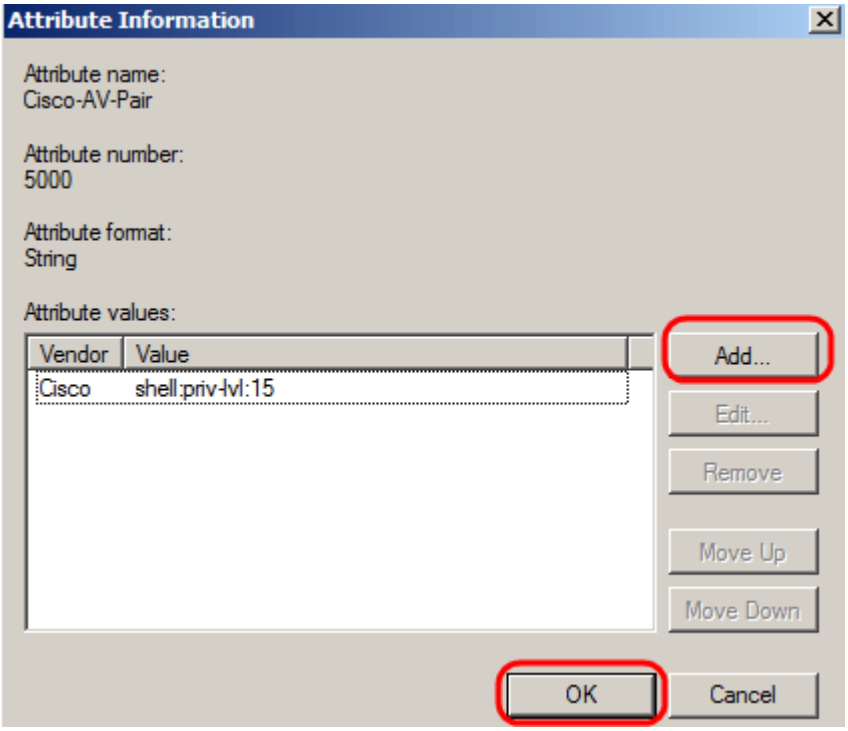
Note: The rest of the settings In this page are set to their default values. You only need to take care of the Vendor Specific settings.



Under Vendor, Select **Cisco**. Click **Add**. The *Attribute Information* window opens.



In the Attribute Information window, click **Add** and enter the value shell:priv-lvl:15. Click **Ok**.



Note: This is the value assigned by Cisco in order for the RADIUS server to grant access to the web-based switch configuration utility.

Click **Ok** to close the Attribute Information window, then click **Close** to close the Add Vendor Specific Attribute window. Click **Next**.

Step 13. A summary of the settings for this policy is showed, click **Finish**. The network policy is created.