

# 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:

## RADIUS

**Use Default Parameters**

IP Version:      Version 6   Version 4

Retries:      3      (Range: 1 - 10, Default: 3)

Timeout for Reply:      3      sec. (Range: 1 - 30, Default: 3)

Dead Time:      0      min. (Range: 0 - 2000, Default: 0)

Key String:      (0/128 ASCII Alphanumeric Characters Used)

RADIUS Table								
<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Retries	Dead Time	Usage Type
0 results found.								
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>								

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:

Server Definition:	<input checked="" type="radio"/> By IP address	<input type="radio"/> By name
IP Version:	<input type="radio"/> Version 6	<input checked="" type="radio"/> Version 4
IPv6 Address Type:	Global	
Server IP Address/Name:	<input type="text"/>	
Priority:	<input type="text"/>	(Range: 0 - 65535)
Key String:	<input checked="" type="radio"/> Use Default	
	<input type="radio"/> User Defined	<input type="text" value="Default"/> (0/128 ASCII Alphanumeric Characters Used)
Timeout for Reply:	<input checked="" type="radio"/> Use Default	
	<input type="radio"/> User Defined	<input type="text" value="Default"/> sec. (Range: 1 - 30, Default: 3)
Authentication Port:	<input type="text" value="1812"/>	(Range: 0 - 65535, Default: 1812)
Retries:	<input checked="" type="radio"/> Use Default	
	<input type="radio"/> User Defined	<input type="text" value="Default"/> (Range: 1 - 10, Default: 3)
Dead Time:	<input checked="" type="radio"/> Use Default	
	<input type="radio"/> User Defined	<input type="text" value="Default"/> min. (Range: 0 - 2000, Default: 0)
Usage Type:	<input type="radio"/> Login	
	<input type="radio"/> 802.1x	
	<input checked="" type="radio"/> All	

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.

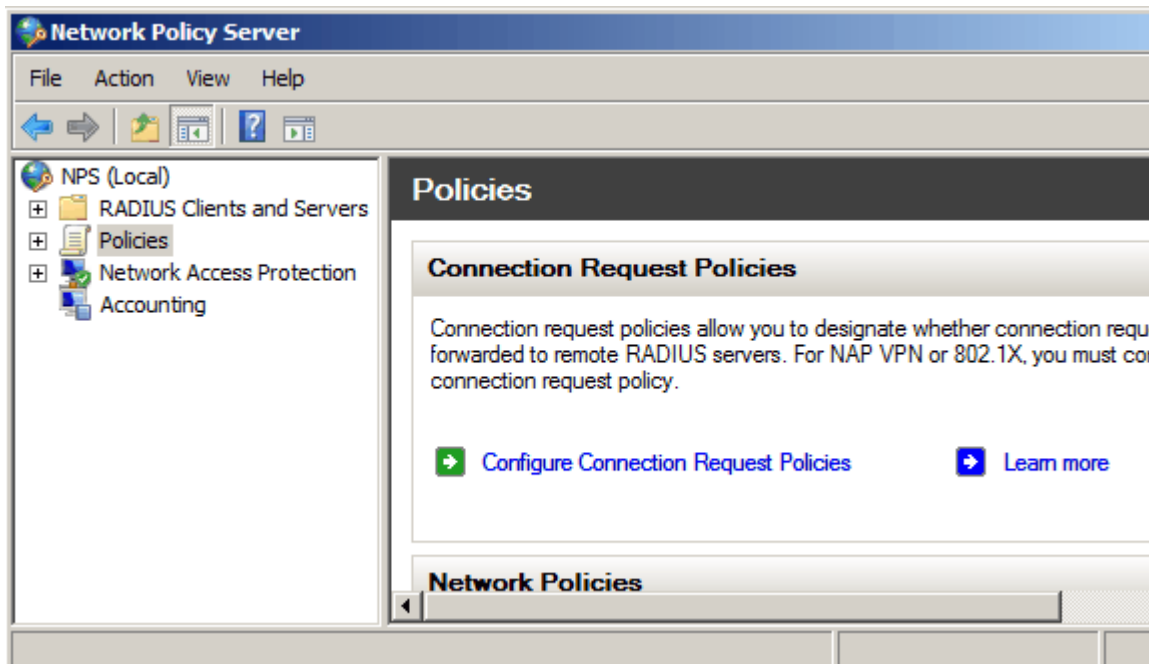
- **Server Definition** — In this field, you specify how to connect to the server, either by IP address, or by the server name.
- **IP Version** — If the server is going to be identified by IP address, then select IPv4 or IPv6 address.
- **IPv6 Address Type** — This field display the type Global of the 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 attempt 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.

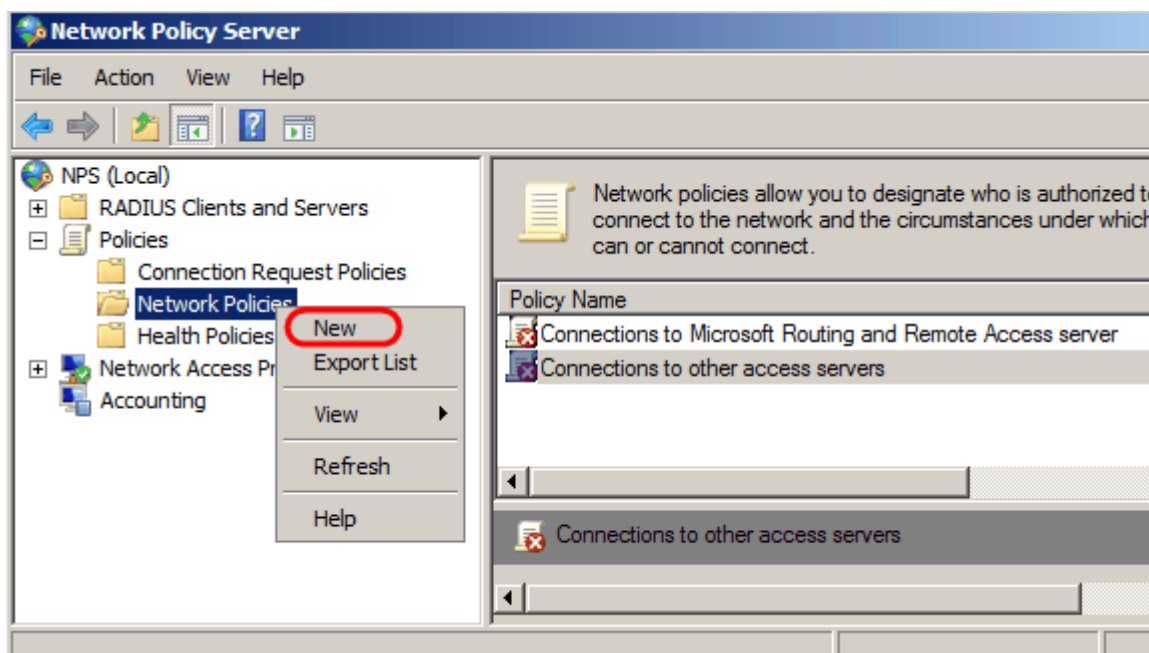
Step 6. Click **Apply** to add the server definition to the running configuration of the switch.

## 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**.

**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:**

**Network connection method**

Select the type of network access server that sends the connection request to NPS. You can select either the network type or Vendor specific.

☒ Type of network access server:

☐ Vendor specific:

Previous **Next** Finish

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.

**New Network Policy**

**Specify Conditions**

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

**Conditions:**

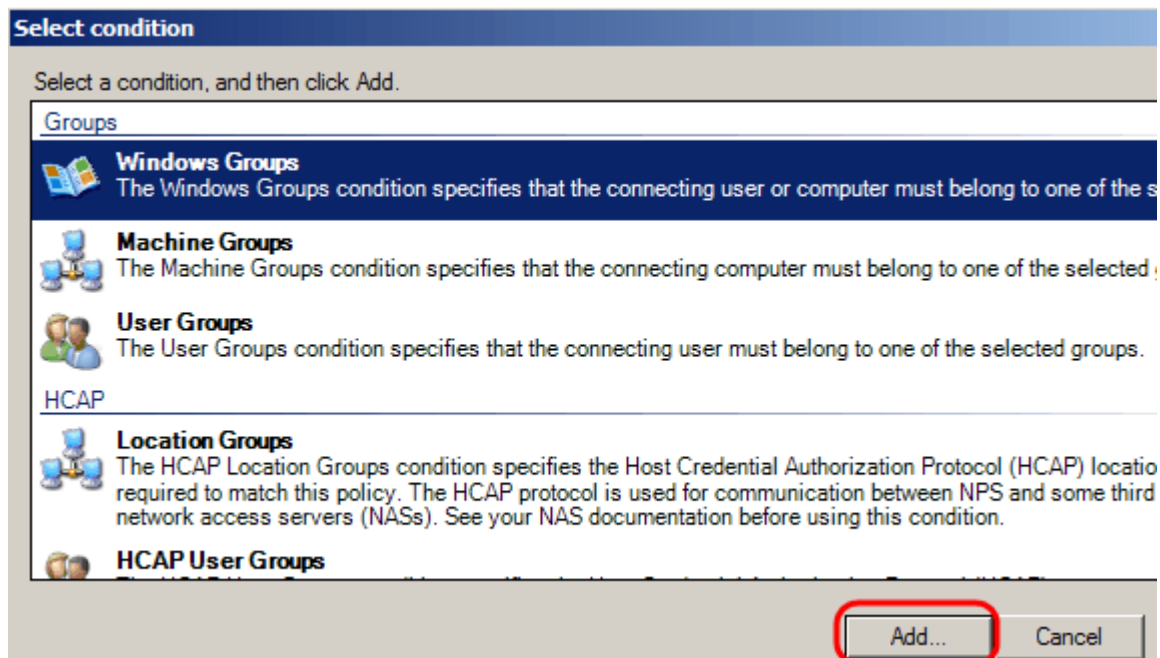
Condition	Value

Condition description:

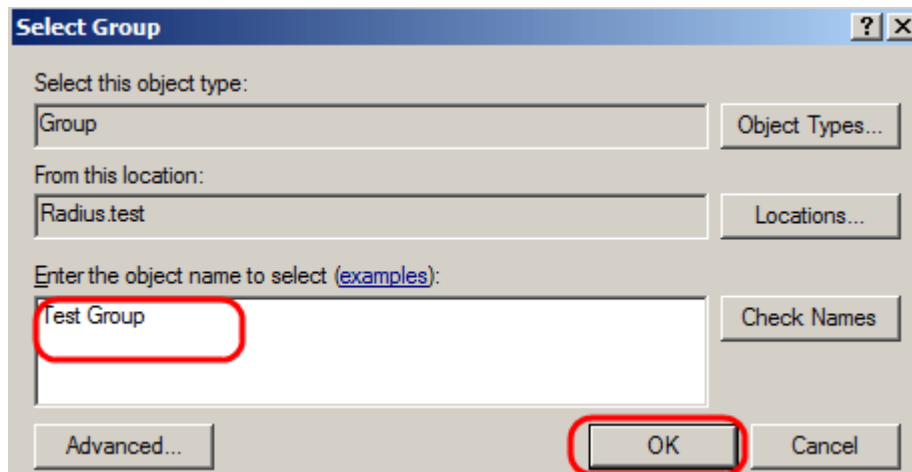
Add... Edit...

Previous Next Finish

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**.

**Select condition**

Select a condition, and then click Add.

RADIUS Client

- Calling Station ID**  
The Calling Station ID condition specifies the network access server telephone number dialed by the a
- Client Friendly Name**  
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connect
- Client IPv4 Address**  
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connecti  
to NPS.
- Client IPv6 Address**  
The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the c  
request to NPS.
- Client Vendor**  
The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connecti

**Add...** **Cancel**

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**.

**New Network Policy**

**Specify Access Permission**

Configure whether you want to grant network access or deny network access if th 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 conc

**Previous** **Next**

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

New Network Policy

## Configure Authentication Methods

Configure one or more authentication methods required for the connection request authentication, you must configure an EAP type. If you deploy NAP with 802.1X or Protected EAP in connection request policy, which overrides network policy authentication.

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

**EAP Types:**

Move Up

Move Down

Add...

Edit...

Remove

**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.
- ☐ Perform machine health check only

Previous

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.



**New Network Policy**

## Configure Settings

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

**Settings:**

- RADIUS Attributes**
  - Standard
  - Vendor Specific**
- Network Access Protection**
  - NAP Enforcement
  - Extended State
- 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 then click Edit. If you do not configure an attribute, it is not sent to your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
------	--------	-------

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

Previous Next

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

**Add Vendor Specific Attribute**

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

**Cisco**

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

**Add...** Close

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

**Attribute Information** [X]

Attribute name:  
Cisco-AV-Pair

Attribute number:  
5000

Attribute format:  
String

Attribute values:

Vendor	Value
Cisco	shell:priv-lvl:15

Buttons: Add... Edit... Remove Move Up Move Down OK Cancel

**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.

## New Network Policy



### Completing New Network Policy

You have successfully created the following network policy:

#### SG200/300 Series

##### Policy conditions:

Condition	Value
Windows Groups	RADIUS\Test Group
Client IPv4 Address	192.168.1.10

##### Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OF
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous

Next

Finish