

Configure Remote Authentication Dial-In User Service (RADIUS) Server Settings on a Switch

Objective

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. A RADIUS server regulates access to the network by verifying the identity of the users through the login credentials entered. For example, a public Wi-Fi network is installed in a university campus. Only those students who have the password can access these networks. The RADIUS server checks the passwords entered by the users and permits or denies access as appropriate.

Setting up a RADIUS Server is useful in enhancing security since it authenticates before authorizing a client or a user to gain access to the network. The RADIUS Server responds to client issues related to server availability, re-transmission, and timeouts. The RADIUS Server also handles users connection requests, authenticates the user, and sends the necessary configuration information to client to deliver services to the user.

The RADIUS Server is a server that centralizes control of a network that is made of RADIUS-enabled devices. RADIUS servers based its forwarding decisions on either 802.1X or Media Access Control (MAC) addresses.

This article explains how to configure RADIUS settings on the Sx350, SG350X, and Sx550X Series Switches.

Applicable Devices

- Sx350 Series
- SG350X Series
- Sx550X Series

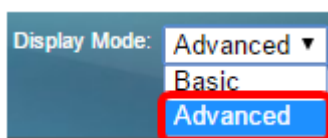
Software Version

- 2.2.5.68

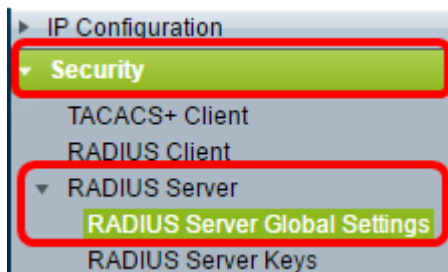
Configure RADIUS Server Settings

Configure RADIUS Server Global Settings

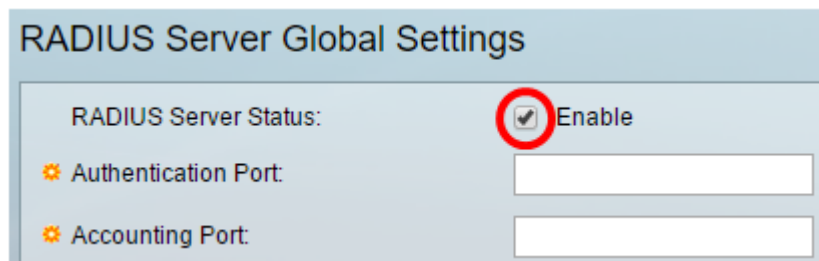
Step 1. Log in to the switch web-based utility and choose **Advanced** from the Display Mode drop-down list.



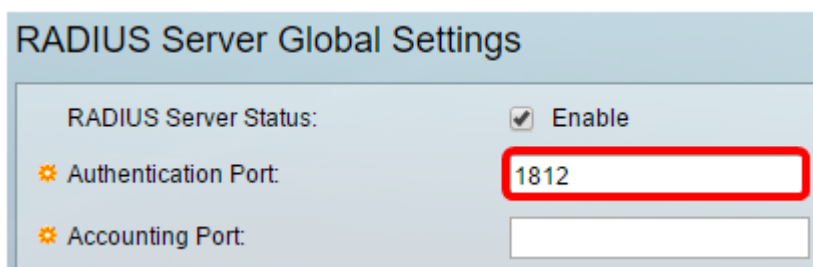
Step 2. Choose **Security > RADIUS Server > RADIUS Server Global Settings**.



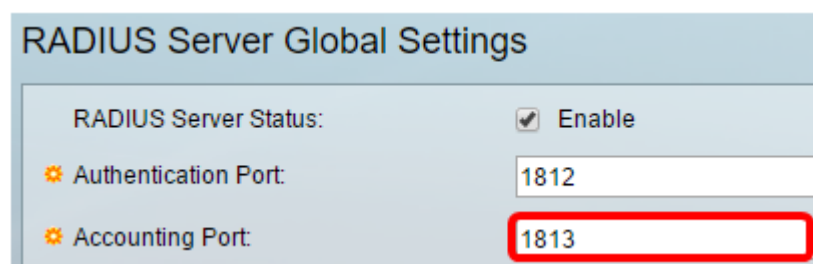
Step 3. Check the **Enable** check box for RADIUS Server Status.



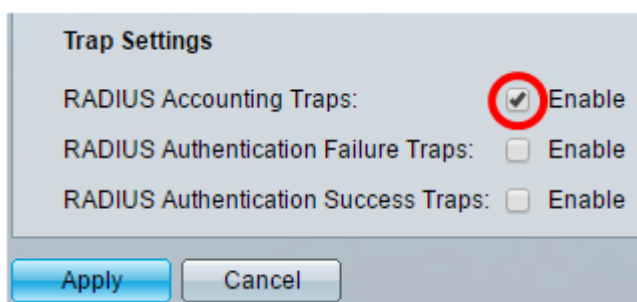
Step 4. Enter the User Datagram Protocol (UDP) port number of the RADIUS server port for authentication requests. The range is 1 to 65535 and the default is 1812.



Step 5. Enter the UDP port number of the RADIUS server port for accounting requests. The range is from 1 to 65535 and the default is 1813.



Step 6. (Optional) To generate traps for RADIUS accounting events, check the **Enable** check box for RADIUS Accounting Traps under Trap Settings.



Step 7. (Optional) To generate traps for logins that failed, check the **Enable** check box for RADIUS Authentication Failure Traps.

Trap Settings

RADIUS Accounting Traps: Enable

RADIUS Authentication Failure Traps: Enable

RADIUS Authentication Success Traps: Enable

Apply Cancel

Step 8. (Optional) To generate traps for logins that succeeded, check the **Enable** check box for RADIUS Authentication Success Traps.

Trap Settings



RADIUS Accounting Traps: Enable

RADIUS Authentication Failure Traps: Enable

RADIUS Authentication Success Traps: Enable

Apply Cancel

Step 9. Click **Apply**.

Step 10. A  icon indicates that the configuration has been saved successfully. To permanently save the configuration, go to the File Operations page or click the  icon at the top portion of the page. Otherwise, click **Close**.

Configure RADIUS Server Keys

Step 1. Choose **RADIUS Server Keys** under RADIUS Server.

- ▼ Security
 - TACACS+ Client
 - RADIUS Client
 - ▼ RADIUS Server
 - RADIUS Server Global Settings
 - RADIUS Server Keys**

Step 2. (Optional) Enter the default RADIUS key if required. Values entered in the Default Key are applied to all servers configured (in the Add RADIUS Server page) to use the default key.

RADIUS Server Keys

Default Key: Keep existing default key

Encrypted

Plaintext (0/128 characters used)

MD5 Digest: bed128365216c019988915ed3add75fb

Apply Cancel

Default Key— Choose the default key string that you want to be used for authenticating and



encrypting between the device and the RADIUS client. The options are:

- Keep existing default key — For specified servers, the device attempts to authenticate the RADIUS client by using the existing default Key String.
- Encrypted — To encrypt communications by using Message Digest 5 (MD5) algorithm, enter the key in encrypted form.
- Plaintext — Enter the key string in plaintext mode.

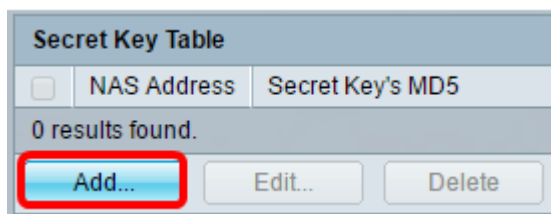
MD5 Digest— Displays the MD5 digest of the user-entered password.

Note: In this example, Keep existing default key under Default Key is chosen.

Step 3. Click **Apply**.

Step 4. A  icon indicates that the configuration has been saved successfully. To permanently save the configuration, go to the File Operations page or click the  icon at the top portion of the page.

Step 5. (Optional) Under the Secret Key Table area, click the **Add** button to add a secret key.



Step 6. Enter the IP Address of the NAS or the switch that contains the RADIUS Client in the *NAS Address* field.


Note: In the image below, 192.168.1.118 is used as an example of the IP Address.

 NAS Address:

Secret Key: Use default key
 Encrypted
 Plaintext

Step 7. Choose your preferred Secret Key.

Note: In the image below, Plaintext is chosen as an example.



 NAS Address:

Secret Key: Use default key
 Encrypted
 Plaintext

The options are:

- Use default key — For specified servers, the device attempts to authenticate the RADIUS client by using the existing default Key String.
- Encrypted — To encrypt communications by using MD5, enter the key in encrypted form.
- Plaintext — Enter the key string in plaintext mode. You can enter up to 128 characters.

Step 8. Click **Apply**.

Step 9. A  icon indicates that the configuration has been saved successfully. To permanently save the configuration, go to the File Operations page or click the  icon at the top portion of the page. Otherwise, click **Close**.

Configure RADIUS Server Groups

RADIUS Server Groups are a group of users that will be using the device as its RADIUS Server. To set up a group, follow the instructions below:

Step 1. Choose **RADIUS Server Groups** under RADIUS Server.

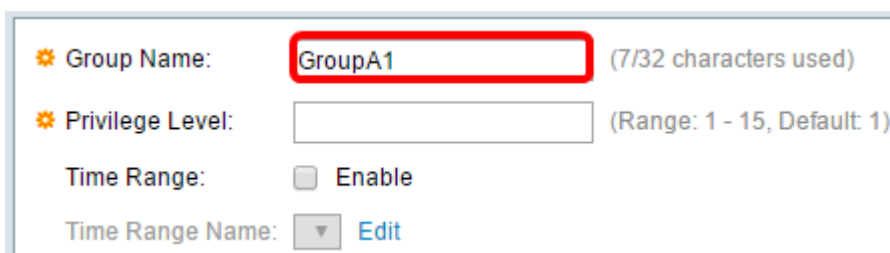


Step 2. Click the **Add** button under RADIUS Server Group table.



Step 3. In the popup window, enter a name for the group in the *Group Name* field. You can enter up to 32 characters.

Note: In the image below, GroupA1 is used as an example.



The image shows the configuration form for a RADIUS Server Group. The 'Group Name' field is highlighted with a red box and contains the text 'GroupA1' with '(7/32 characters used)' next to it. Below it, the 'Privilege Level' field is empty with '(Range: 1 - 15, Default 1)' next to it. The 'Time Range' section has an unchecked 'Enable' checkbox. The 'Time Range Name' field has a dropdown arrow and an 'Edit' button.

Step 4. Enter the privilege level that you want to assign to the group. The privilege level determines the level of access that you will assign to each group that you created. You can

set the levels from 1-15. The default value is 1.

Note: In this example, 7 is used.

Group Name: (7/32 characters used)
Privilege Level: (Range: 1 - 15, Default: 1)
Time Range: Enable
Time Range Name:

- 1 (Read-Only CLI Access) — Users in the group cannot access the GUI, and can only access CLI commands that do not change the device configuration.
- 7 (Read/Limited Write CLI Access) — Users in the group cannot access the GUI, and can only access some CLI commands that change the device configuration. See the [CLI Reference Guide](#) for more information.
- 15 (Read/Write Management Access) — Users in the group can access the GUI, and can configure the device.

Step 5. (Optional) If you want to apply a time range for this group, check the **Enable** check box for the Time Range. Otherwise, skip to [Step 15](#).

Group Name: (7/32 characters used)
Privilege Level: (Range: 1 - 15, Default: 1)
Time Range: Enable
Time Range Name:

Step 6. Click the **Edit** link beside Time Range Name to configure the Time settings.

Group Name: (7/32 characters used)
Privilege Level: (Range: 1 - 15, Default: 1)
Time Range: Enable
Time Range Name:

Step 7. A popup window will appear telling you that the current window will be closed so that you can continue with the Time Range settings. Click **OK**.

Confirm dialog closing - Google Chrome
Not Secure | <https://192.168.1.116/cs61cad552/kubrick/cor>
The navigation to the Time Range page will close the current window. Do you want to continue?

You will then be directed to the Time Range page.

Step 8. Click the **Add** button under the Time Range Table.

Time Range

Time Range Table			
<input type="checkbox"/>	Time Range Name	Absolute Starting Time	Absolute Ending Time
0 results found.			
<input type="button" value="Add..."/>	<input type="button" value="Edit..."/>	<input type="button" value="Delete"/>	

Step 9. Enter a name for the Time Range in the *Time Range Name* field.

Note: In the image below, Reconnect is used as an example.

(9/32 characters used)

Absolute Starting Time: Immediate
 Date 2010 Jan 01 Time 00 00 HH:MM

Absolute Ending Time: Infinite
 Date 2010 Jan 01 Time 00 00 HH:MM

Step 10. Choose your preferred Absolute Starting and Ending Time by clicking on the radio button.

(12/32 characters used)



Absolute Starting Time: Immediate
 Date 2016 Sep 15 Time 14 00 HH:MM

Absolute Ending Time: Infinite
 Date 2016 Sep 23 Time 13 59 HH:MM

- Absolute Starting Time — To define the start time, choose from the following:
- Immediate — Choose this if you want the time range to start immediately.
- Date, Time — Choose this if you want to specify the date and time that the Time Range begins.
- Absolute Ending Time — To define the start time, choose from the following:
- Infinite — Choose this if you want the time range to never end.
- Date, Time — Choose this if you want to specify the date and time that the Time Range ends.

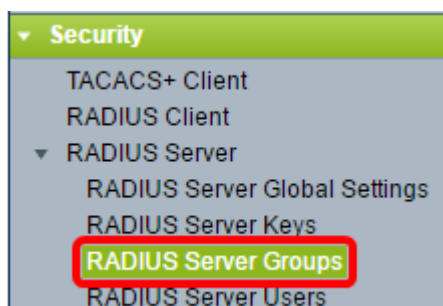
Note: In this example, Date and Time are chosen.

Step 11. Click **Apply**.

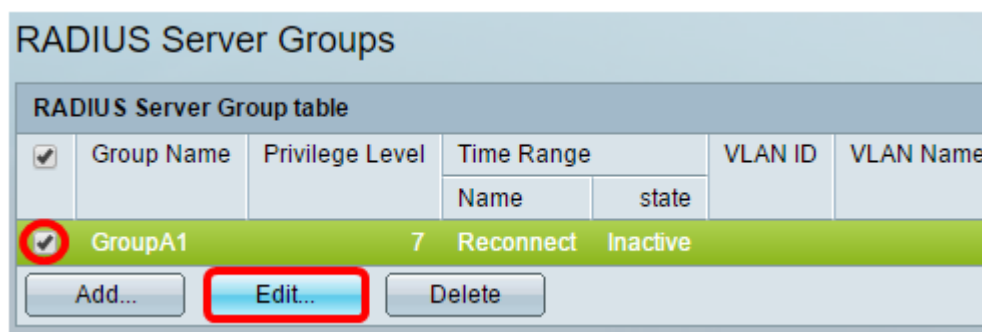
Step 12. A  icon indicates that the configuration has been saved successfully. To permanently save the configuration, go to the File Operations page or click the  icon at the top portion of the page. Otherwise, click **Close**.

You will then be directed to the main page.

Step 13. Click **RADIUS Server Groups** again under RADIUS Server.



Step 14. The newly created group will now appear under RADIUS Server Group table. Check the box beside the name of the group and then click **Edit**.





Step 15. (Optional) Choose the VLAN for the group. The options are:

- None — No VLAN specified.
- VLAN ID — Specify a VLAN ID.
- VLAN Name — Specify a VLAN name.

A screenshot of the configuration form for a RADIUS Server Group. The 'Group Name' is set to 'GroupA1'. The 'Privilege Level' is set to '7' (Range: 1 - 15, Default: 1). The 'Time Range' is set to 'Enable'. The 'Time Range Name' is set to 'Reconnect' with an 'Edit' link. The 'VLAN' section has three radio buttons: 'None', 'VLAN ID' (selected), and 'VLAN Name'. The 'VLAN ID' field contains the value '8' (Range: 1 - 4094). The 'VLAN Name' field is empty (0/32 characters used). At the bottom are 'Apply' and 'Close' buttons.

Note: In this example, VLAN ID 8 is used.

Step 16. Click **Apply**.

Step 17. A  icon indicates that the configuration has been saved successfully. To permanently save the configuration, go to the File Operations page or click the  icon at the top portion of the page. Otherwise, click **Close**.

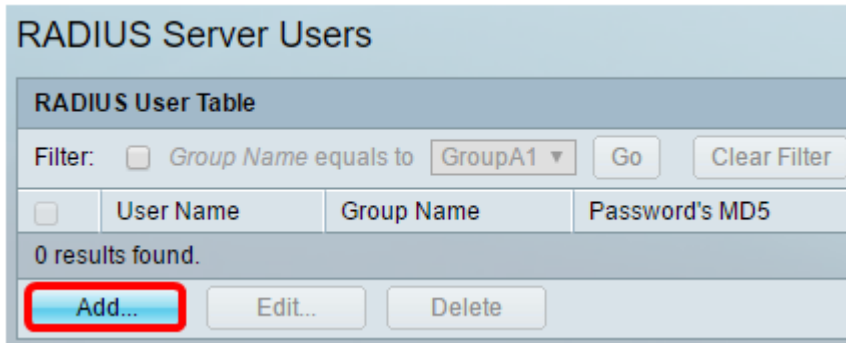
Configure RADIUS Server Users

To add users to the previously created group:

Step 1. Click **RADIUS Server Users** under RADIUS Server.

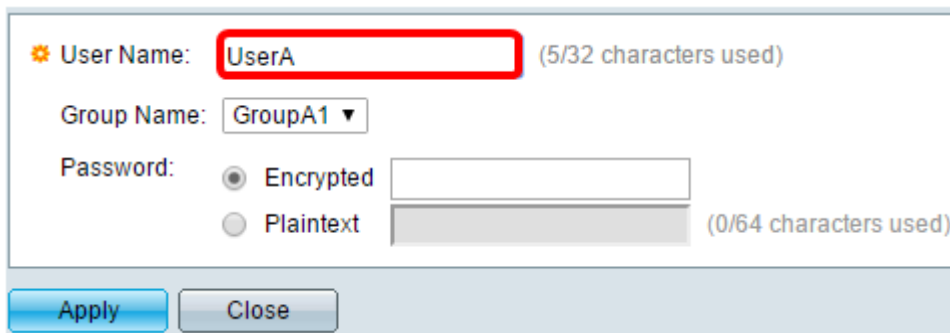


Step 2. Click the **Add** button under the RADIUS User Table.

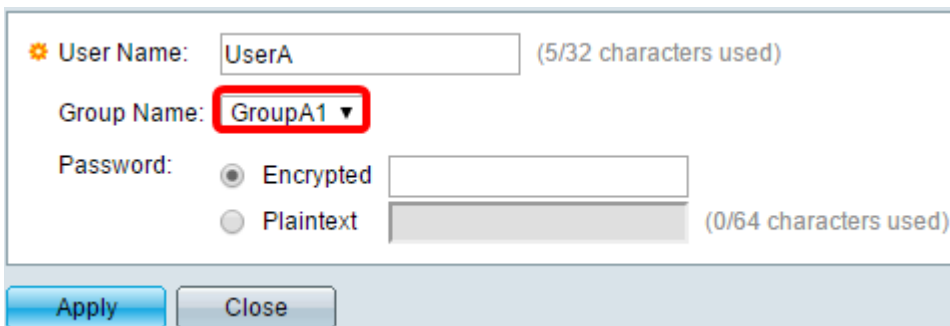


Step 3. Enter the name of the user in the *User Name* field.

Note: In this example, UserA is used.



Step 4. Choose the group where the user belongs from the Group Name drop-down list.



Step 5. Click a radio button in the Password area.

Step 6. Enter your preferred password.

User Name: (5/32 characters used)



Group Name:

Password: Encrypted
 Plaintext (9/64 characters used)

- Encrypted — A key string is used to encrypt communications by using MD5. To use encryption, enter the key in encrypted form.
- Plaintext — If you do not have an encrypted key string (from another device), enter the key string in plaintext mode. The encrypted key string is generated and displayed.

Note: In this example, Plaintext is chosen.

Step 6. Click **Apply**.

Step 7. A  icon indicates that the configuration has been saved successfully. To permanently save the configuration, go to the File Operations page or click the  icon at the top portion of the page. Otherwise, click **Close**.

You should now have successfully configured the RADIUS Server settings on your switch.

©2016 Cisco Systems, Inc. All rights reserved.