

Remote Authentication Dial-In User Service (RADIUS) Settings on Sx500 Series Stackable Switches

Objective

Remote Authentication Dial-In User Service (RADIUS) is a client or server protocol. The RADIUS client is usually a Network Access Server (NAS) and the Radius server is a process that runs on UNIX or Windows NT machine. The Radius server responds to client's issues related to server availability, re-transmission, and timeouts. Radius server also handles user's connection requests, authenticates the user, and sends the necessary configuration information to client to deliver services to the user.

RADIUS server is a server that centralizes control of a network that is made of RADIUS enabled devices. RADIUS servers are based on either 802.1X or MAC addresses. This article explains how to configure RADIUS Settings on the Sx500 Series Stackable Switches.

Applicable Devices

- Sx500 Series Stackable Switches

Software Version

- v1.2.7.76

RADIUS Settings

Step 1. Log in to the web configuration utility and choose **Security > RADIUS**. The *Radius* page opens:

RADIUS

RADIUS Accounting:
☐ Port Based Access Control (802.1X, MAC Based)
☐ Management Access
☐ Both Port Based Access Control and Management Access
☒ None

Use Default Parameters

IP Version: Version 6 Version 4

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

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

⚙ Dead Time: 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	Accounting 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. Click the desired radio button for the RADIUS Accounting type in the RADIUS Accounting field.

- Port Based Access Control — This option has server/client interaction occur through a 802.1X port.
- Management Access — This option has the server/client interaction occur over an user account.
- Both Port Based Access Control and Management Access — This option has the server/client interaction occur over both a 802.1X port and a user account.
- None — This option does not permit accounting on the RADIUS Server.

RADIUS

RADIUS Accounting: ☐ Port Based Access Control (802.1X, MAC Based)
☐ Management Access
☐ Both Port Based Access Control and Management Access
☒ None

Use Default Parameters

IP Version: ☐ Version 6 ☐ Version 4

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

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

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

Key String: (7/128 ASCII Alphanumeric Characters Used)

Apply

Cancel

RADIUS Table

<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
--------------------------	--------	----------	------------	-------------------	---------------------	-----------------	---------	-----------	------------

0 results found.

Add...

Edit...

Delete

Step 3. In the Retries field, enter a number of retries that a request can be sent before a failure notice is given.

RADIUS

RADIUS Accounting: ☐ Port Based Access Control (802.1X, MAC Based)
☐ Management Access
☐ Both Port Based Access Control and Management Access
☒ None

Use Default Parameters

IP Version: ☐ Version 6 ☐ Version 4

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

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

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

Key String: (7/128 ASCII Alphanumeric Characters Used)

Apply

Cancel

RADIUS Table

<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
--------------------------	--------	----------	------------	-------------------	---------------------	-----------------	---------	-----------	------------

0 results found.

Add...

Edit...

Delete

Step 4. In the Timeout for Reply field, enter a time (in seconds) before an unanswered request is resent.

RADIUS

RADIUS Accounting: ☐ Port Based Access Control (802.1X, MAC Based)
☐ Management Access
☐ Both Port Based Access Control and Management Access
☒ None

Use Default Parameters

IP Version: ☐ Version 6 ☐ Version 4

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

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

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

Key String: (7/128 ASCII Alphanumeric Characters Used)

Apply

Cancel

RADIUS Table

<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
--------------------------	--------	----------	------------	-------------------	---------------------	-----------------	---------	-----------	------------

0 results found.

Add...

Edit...

Delete

Step 5. In the Dead Time field, enter a time (in minutes) before an unresponsive RADIUS server is bypassed. The authentication request then goes to the next configured RADIUS server. A value of 0 means that the RADIUS server is not bypassed.

RADIUS

RADIUS Accounting: ☐ Port Based Access Control (802.1X, MAC Based)
☐ Management Access
☐ Both Port Based Access Control and Management Access
☒ None

Use Default Parameters

IP Version: ☐ Version 6 ☐ Version 4

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

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

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

Key String: (7/128 ASCII Alphanumeric Characters Used)

RADIUS Table									
<input type="checkbox"/>	Server	Priority	Key String	Timeout for Reply	Authentication Port	Accounting 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 6. In the Key String field, enter a password that will help encrypt messages between the server and client. The key string must match the key string of the RADIUS server.

Step 7. Click **Apply**.

RADIUS Table

The RADIUS table allows an user to create a new RADIUS server. This procedure shows how to create a RADIUS server.

Step 1. In the RADIUS Table, click **Add**. A new window appears.

The screenshot shows a configuration window for a RADIUS server. It contains several fields and radio buttons for defining the server's properties. The 'Server Definition' field has 'By IP address' selected. The 'IP Version' field has 'Version 4' selected. The 'IPv6 Address Type' is set to 'Global'. The 'Server IP Address/Name' field is empty. The 'Priority' field is empty with a range of 0 to 65535. The 'Key String' field has 'Use Default' selected. The 'Timeout for Reply' field has 'Use Default' selected. The 'Authentication Port' field is set to 1812. The 'Accounting Port' field is set to 1813. The 'Retries' field has 'Use Default' selected. The 'Dead Time' field has 'Use Default' selected. The 'Usage Type' field has 'All' selected. At the bottom, there are 'Apply' and 'Close' buttons.

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)
* Timeout for Reply:	<input checked="" type="radio"/> Use Default	
	<input type="radio"/> User Defined	<input type="text" value="Default"/> sec. (Range: 1 - 60)
* Authentication Port:	<input type="text" value="1812"/>	(Range: 0 - 65535, Default: 1812)
* Accounting Port:	<input type="text" value="1813"/>	(Range: 0 - 65535, Default: 1813)
* Retries:	<input checked="" type="radio"/> Use Default	
	<input type="radio"/> User Defined	<input type="text" value="Default"/> (Range: 1 - 10)
* Dead Time:	<input checked="" type="radio"/> Use Default	
	<input type="radio"/> User Defined	<input type="text" value="Default"/> min. (Range: 0 - 60)
Usage Type:	<input type="radio"/> Login	
	<input type="radio"/> 802.1x	
	<input checked="" type="radio"/> All	

Step 2. In the Server Definition field, click the following radio buttons.

- By IP address — This option defines the RADIUS server by the IP address.
- By name — This option defines the RADIUS server by the name.

Step 3. In the IP Version field, click the following radio buttons.

- Version 6 — This option sets the IP address of the RADIUS server to IPv6.
- Version 4 — This option sets the IP address of the RADIUS server to IPv4.

Server Definition: ☐ By IP address ☒ By name

IP Version: ☐ Version 6 ☒ Version 4

IPv6 Address Type: Global

* Server IP Address/Name:

* Priority: (Range: 0 - 65535)

Key String: ☒ Use Default ☐ User Defined (0/128 ASCII Alphanumeric Characters Used)

* Timeout for Reply: ☒ Use Default ☐ User Defined sec. (Range: 1 - 30, Default: 3)

* Authentication Port: (Range: 0 - 65535, Default: 1812)

* Accounting Port: (Range: 0 - 65535, Default: 1813)

* Retries: ☒ Use Default ☐ User Defined (Range: 1 - 10, Default: 3)

* Dead Time: ☒ Use Default ☐ User Defined min. (Range: 0 - 2000, Default: 0)

Usage Type: ☐ Login ☐ 802.1x ☒ All

Step 4. In the Server IP Address/Name field, enter the name or IP address for the RADIUS server depending on your choice in Step 2.

Step 5. In the Priority field, enter a priority level for the RADIUS server. 0 is the top priority. This priority determines if the Radius server is primary or backup. Radius server with the lowest priority is considered the highest.

Step 6. To the right of Key String, choose an option.

- Use Default — Sets the key string of the RADIUS server to the default string.
- User Defined — Allows a user to enter the key string in the adjacent field.

Step 7. To the right of Timeout for Reply, choose an option for the time (in seconds) in which the switch waits for the RADIUS server to respond.

- Use Default — Sets the time to the default value.
- User Defined — Allows an user to enter the time in the adjacent field.

Step 8. In the Authentication Port field, enter a port number for authentication requests.

Step 9. In the Accounting Port field, enter a port number for accounting requests.

Step 10. To the right of Retries, choose an option for the number of requests that are sent to the RADIUS server before a failure notice occurs.

- Use Default — Uses the default number of retries.

- User Defined — Allows an user to enter the number of retries in the adjacent field.

Step 11. In the Dead Time field, choose an option for the time in minutes before a RADIUS server is bypassed for being unresponsive.

- Use Default — Uses the default time.
- User Defined — Allows an user to enter the time in the adjacent field.

Step 12. In the Usage Type field, choose an option for RADIUS server authentication type.

- Login — Authenticates the user for the RADIUS server.
- User Defined — Uses 802.1X authentication.
- All — Performs both authentications.

Step 13. Click **Apply**.