

Configure 802.1x Port Authentication Setting on a Switch

Objective

IEEE 802.1x is a standard which facilitates access control between a client and a server. Before services can be provided to a client by a Local Area Network (LAN) or switch, the client connected to the switch port has to be authenticated by the authentication server which runs Remote Authentication Dial-In User Service (RADIUS).

802.1x authentication restricts unauthorized clients from connecting to a LAN through publicly-accessible ports. 802.1x authentication is a client-server model. In this model, network devices have the following specific roles:

Client or supplicant — A client or supplicant is a network device that requests access to the LAN. The client is connected to an authenticator.

Authenticator — An authenticator is a network device that provides network services and to which supplicant ports are connected. The following authentication methods are supported:

802.1x-based — Supported in all authentication modes. In 802.1x-based authentication, the authenticator extracts the Extensible Authentication Protocol (EAP) messages from the 802.1x messages or EAP over LAN (EAPoL) packets, and passes them to the authentication server, using the RADIUS protocol.

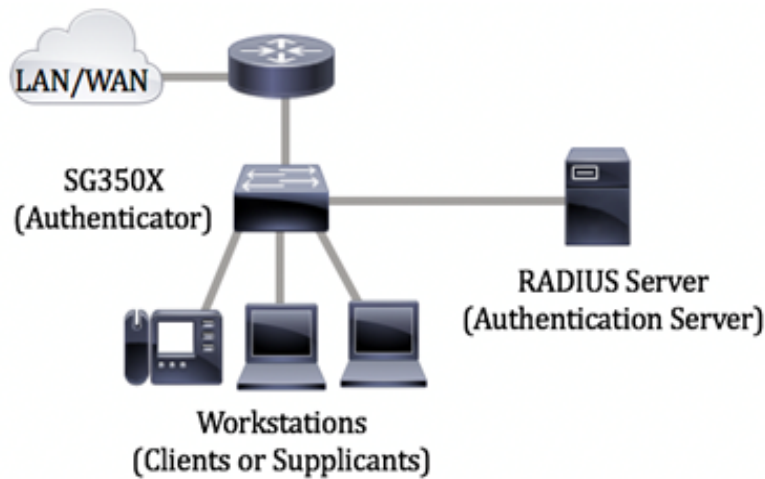
MAC-based — Supported in all authentication modes. With Media Access Control (MAC)-based, the authenticator itself executes the EAP client part of the software on behalf of the clients seeking network access.

Web-based — Supported only in multi-sessions modes. With web-based authentication, the authenticator itself executes the EAP client part of the software on behalf of the clients seeking network access.

Authentication server — An authentication server performs the actual authentication of the client. The authentication server for the device is a RADIUS authentication server with EAP extensions.

Note: A network device can be either a client or supplicant, authenticator, or both per port.

The image below displays a network that have configured the devices according to the specific roles. In this example, an SG350X switch is used.



Guidelines in configuring 802.1x:

Create a Virtual Access Network (VLAN). To create VLANs using the web-based utility of your switch, click [here](#). For CLI-based instructions, click [here](#).

Configure Port to VLAN settings on your switch. To configure using the web-based utility, click [here](#). To use the CLI, click [here](#).

Configure 802.1x properties on the switch. 802.1x should be globally enabled on the switch to enable 802.1x port-based authentication. For instructions, click [here](#).

(Optional) Configure Time Range on the switch. To learn how to configure time range settings on your switch, click [here](#).

Configure 802.1x Port Authentication. This article provides instructions on how to configure 802.1x port authentication settings on your switch.

To learn how to configure mac-based authentication on a switch, click [here](#).

Applicable Devices

Sx300 Series

Sx350 Series

SG350X Series

Sx500 Series

Sx550X Series

Software Version

1.4.7.06 — Sx300, Sx500

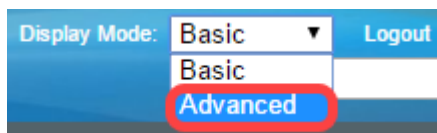
2.2.8.04 — Sx350, SG350X, Sx550X

Configure 802.1x Port Authentication Settings on a Switch

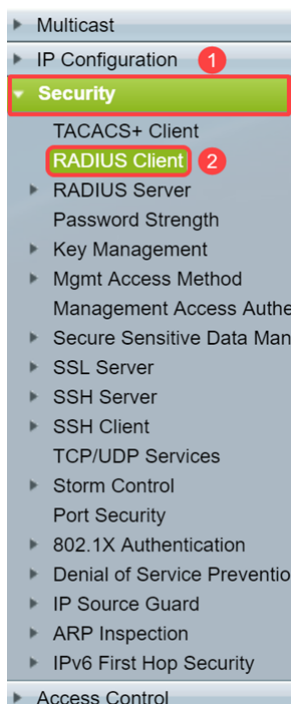
Configure RADIUS Client Settings

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

Note: The available menu options may vary depending on the device model. In this example, SG550X-24 is used.



Step 2. Navigate to **Security > RADIUS Client**.



Step 3. Scroll down to the *RADIUS Table* section and click **Add...** to add a RADIUS server.

Retries: 3 (Range: 1 - 15, Default: 3)

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

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

Key String: Encrypted Plaintext (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

Apply Cancel

Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.								

Add... Edit... Delete

An * indicates that the parameter is using the default global value.

Display Sensitive Data as Plaintext

Step 4. Select whether to specify the RADIUS server by IP address or name in the *Server Definition* field. Select the version of the IP address of the RADIUS server in the *IP Version* field.

Note: We will be using **By IP address** and **Version 4** in this example.

Add RADIUS Server - Google Chrome

Not secure | https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security_authen_radius_a_jq.htm

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name:

Priority: (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

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

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

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

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Step 5. Enter in the RADIUS server by IP address or name.

Note: We will be entering the IP address of **192.168.1.146** in the *Server IP Address/Name* field.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

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

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

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

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Step 6. Enter the priority of the server. The priority determines the order the device attempts to contact the servers to authenticate a user. The device starts with the highest priority RADIUS server first. 0 is the highest priority.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

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

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

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

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Step 7. Enter the key string used for authenticating and encrypting communication between the device and the RADIUS server. This key must match the key configured on the RADIUS server. It can be entered in **Encrypted** or **Plaintext** format. If **Use Default** is selected, the device attempts to authenticate to the RADIUS server by using the default key string.

Note: We will be using the **User Defined (Plaintext)** and entering in the key **example**.

To learn how to configure the RADIUS server settings on your switch, click [here](#).

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

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

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

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

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Step 8. In the *Timeout for Reply* field, select either **Use Default** or **User Defined**. If **User Defined** was selected, enter the number of seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server if the maximum number of retries made. If **Use Default** is selected, the device uses the default timeout value.

Note: In this example, **Use Default** was selected.

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

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

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

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

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Apply Close

Step 9. Enter the UDP port number of the RADIUS server port for authentication request in the *Authentication Port* field. Enter the UDP port number of the RADIUS server port for accounting requests in the *Accounting Port* field.

Note: In this example, we will be using the default value for both authentication port and accounting port.

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

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

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

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

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Apply Close

Step 10. If **User Defined** is selected for *Retries* field, enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. If **Use Default** was selected, the device uses the default value for the number of retries.

If **User Defined** is selected for *Dead Time*, enter the number of minutes that must pass before a non-responsive RADIUS server is bypassed for service requests. If **Use Default** was selected, the device uses the default value for the dead time. If you entered 0 minutes, there is no dead time.

Note: In this example, we will be selecting **Use Default** for both of these fields.

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

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

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

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

Retries: 1 Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: 2 Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

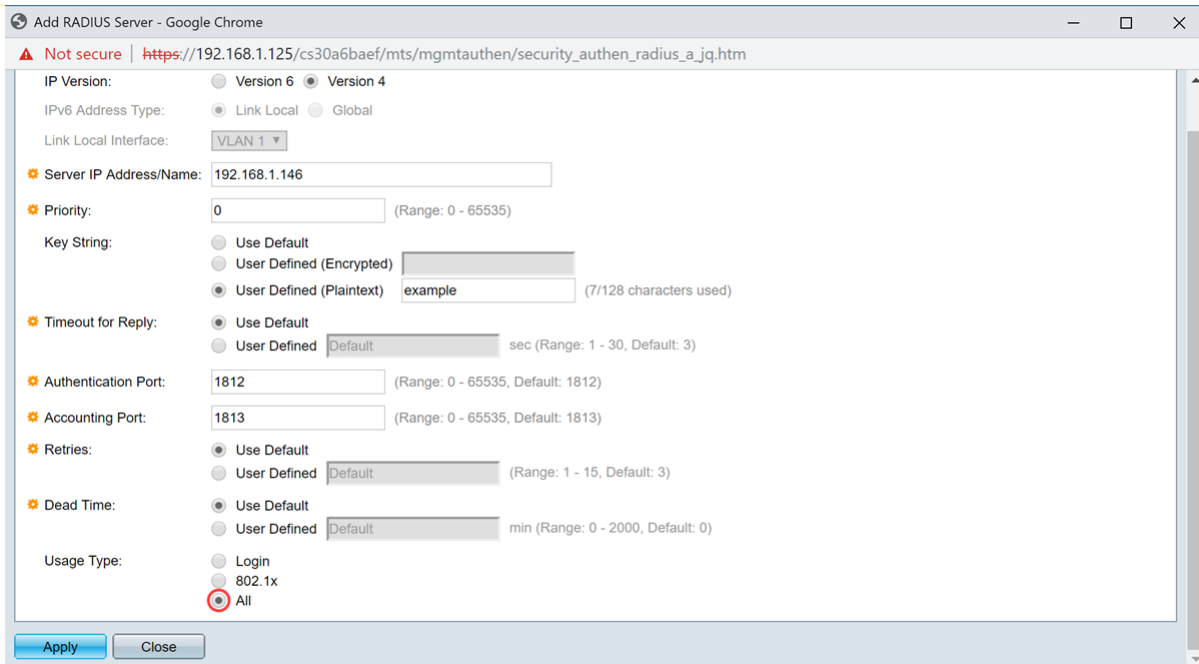
Apply Close

Step 11. In the *Usage Type* field, enter the RADIUS server authentication type. The options are:

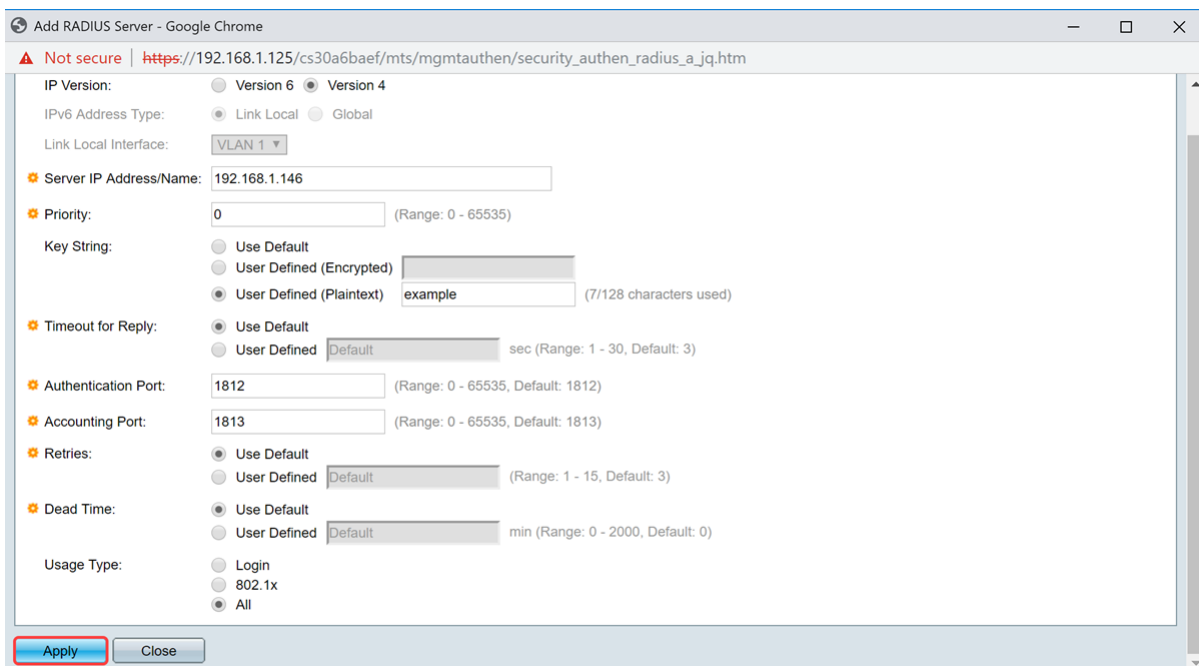
Login – RADIUS server is used for authenticating users that ask to administer the device.

802.1x – RADIUS server is used for 802.1x authentication.

All – RADIUS server is used for authenticating user that ask to administer the device and for 802.1x authentication.



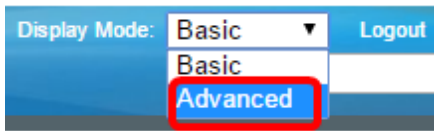
Step 12. Click Apply.



Configure 802.1x Port Authentication Settings

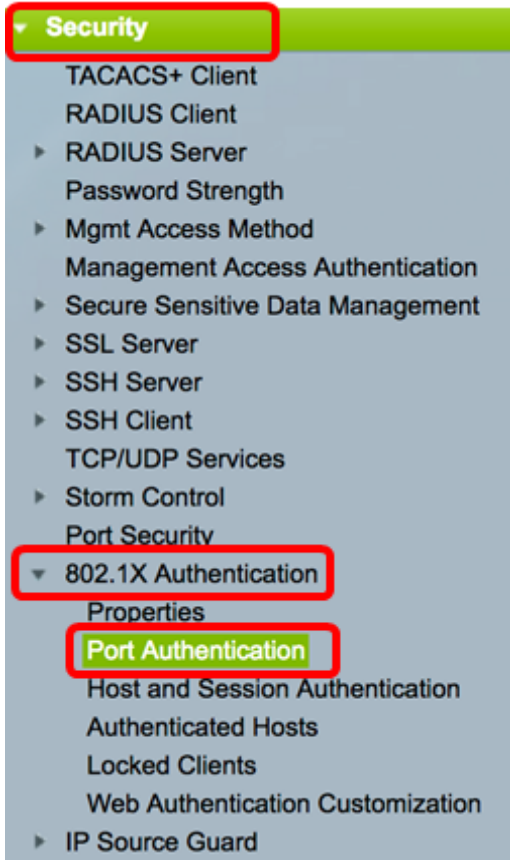
Step 1. Log in to the web-based utility of your switch then choose **Advanced** in the Display Mode drop-down list.

Note: The available menu options may vary depending on the device model. In this example, SG350X-48MP is used.



Note: If you have an Sx300 or Sx500 Series switch, skip to [Step 2](#).

Step 2. Choose **Security > 802.1X Authentication > Port Authentication**.

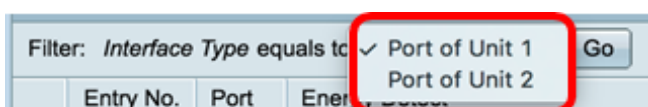


Step 3. Choose an interface from the *Interface Type* drop-down list.

Port — From the *Interface Type* drop-down list, choose **Port** if only a single port needs to be chosen.

LAG — From the *Interface Type* drop down list, choose the LAG to configure. This affects the group of ports defined in the LAG configuration.

Note: In this example, Port of Unit 1 is chosen.



Note: If you have a non-stackable switch such as a Sx300 Series switch, skip to [Step 5](#).

Step 4. Click **Go** to bring up a list of ports or LAGs on the interface.

Port Authentication

Port Authentication Table

Filter: *Interface Type* equals to Port of Unit 1

Step 5. Click the port that you want to configure.

Port Authentication

Port Authentication Table

Filter: *Interface Type* equals to Port of Unit 1

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication	Web Based Authentication
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input checked="" type="radio"/>	4	GE4	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled

Note: In this example, GE4 is chosen.

Step 6. Scroll down the page then click **Edit**.

<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	47	GE47	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	48	GE48	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled

Step 7. (Optional) If you want to edit another interface, choose from the Unit and Port drop-down lists.

Interface:
Current Port Control: Authorized

Note: In this example, port GE4 of unit 1 is chosen.

Step 8. Click the radio button that corresponds to the desired port control in the Administrative Port Control area. The options are:

Force Unauthorized — Denies the interface access by moving the port into the unauthorized state. The port will discard traffic.

Auto — The port moves between an authorized or unauthorized state based on authentication of the supplicant.

Force Authorized — Authorizes the port without authentication. The port will forward traffic.

Administrative Port Control:  Force Unauthorized
Auto
Force Authorized

Note: In this example, Auto is chosen.

Step 9. Click a RADIUS VLAN Assignment radio button to configure dynamic VLAN assignment on the selected port. The options are:

Disable — Feature is not enabled.

Reject — If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is rejected.

Static — If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted.

RADIUS VLAN Assignment: Disable
 Reject
 Static

Note: In this example, Static is chosen.

Step 10. Check **Enable** in the Guest VLAN check box to enable Guest VLAN for unauthorized ports. Guest VLAN makes the unauthorized port automatically join the VLAN chosen in the Guest VLAN ID area of the 802.1 properties.

Guest VLAN: Enable

Step 11. (Optional) Check the **Enable** Open Access check box to enable open access. Open Access helps you to understand the configuration problems of hosts connecting to the network, monitors bad situations and enables these problems to be fixed.

Note: When Open Access is enabled on an interface, the switch treats all failures received from a RADIUS server as successes and allows access to the network for stations connected to interfaces regardless of authentication results. In this example, Open Access is disabled.

Guest VLAN: Enable
Open Access: Enable

Step 12. Check the **Enable** 802.1x Based Authentication check box to enable 802.1X authentication on the port.

Guest VLAN: Enable
Open Access: Enable
802.1x Based Authentication: Enable

Step 13. Check the **Enable** MAC Based Authentication check box to enable port authentication based on the supplicant MAC address. Only eight MAC-based authentications

can be used on the port.

Note: For MAC authentication to succeed, the RADIUS server supplicant username and password must be the supplicant MAC address. The MAC address must be in lower case letters and entered without the . or – separators (such as 0020aa00bbcc).

802.1x Based Authentication: Enable
MAC Based Authentication: Enable

Note: In this example, MAC-based authentication is disabled.

Step 14. Check the **Enable** Web Based Authentication check box to enable web-based authentication on the switch. In this example, web-based authentication is disabled.

802.1x Based Authentication: Enable
MAC Based Authentication: Enable
Web Based Authentication: Enable

Note: In this example, web-based authentication is disabled.

Step 15. (Optional) Check the **Enable** Periodic Reauthentication check box to force the port to re-authenticate after a given time. This time is defined in the *Reauthentication Period* field.

Web Based Authentication: Enable
Periodic Reauthentication: Enable

Note: In this example, period re-authentication is enabled.

Step 16. (Optional) Enter a value in the *Reauthentication Period* field. This value represents the amount of seconds before the interface re-authenticates the port. The default value is 3600 seconds and the range is from 300 to 4294967295 seconds.

Periodic Reauthentication: Enable
Reauthentication Period: sec

Note: In this example, 6000 seconds is configured.

Step 17. (Optional) Check the **Enable** Reauthenticate Now check box to force an immediate port re-authentication. In this example, immediate re-authentication is disabled.

Periodic Reauthentication: Enable
Reauthentication Period: sec
Reauthenticate Now:
Authenticator State: Force Authorized

The Authenticator State area displays the authorization state of the port.

Step 18. (Optional) Check the **Enable** Time Range check box to enable a limit on the time that the port is authorized.

Time Range: Enable
Time Range Name: Dayshift

Note: In this example, Time Range is enabled. If you prefer to skip this feature, proceed to [Step 20](#).

Step 19. (Optional) From the Time Range Name drop-down list, choose a time range to use.

Time Range: Enable
Time Range Name: Dayshift
NightShift
Maximum WBA Login Attempts:

Note: In this example, Dayshift is chosen.

Step 20. In the Maximum WBA Login Attempts area, click either Infinite for no limit or User Defined to set a limit. If User Defined is chosen, enter the maximum number of login attempts allowed for web-based authentication.

Maximum WBA Login Attempts: Infinite
 User Defined

Note: In this example, Infinite is chosen.

Step 21. In the Maximum WBA Silence Period area, click either Infinite for no limit or User Defined to set a limit. If User Defined is chosen, enter the maximum length of the silent period for web-based authentication allowed on the interface.

Maximum WBA Silence Period: Infinite
 User Defined sec

Note: In this example, Infinite is chosen.

Step 22. In the Max Hosts area, click either Infinite for no limit or User Defined to set a limit. If User Defined is chosen, enter the maximum number of authorized hosts allowed on the interface.

Max Hosts: Infinite
 User Defined

Note: Set this value to 1 to simulate single-host mode for web-based authentication in multi-sessions mode. In this example, Infinite is chosen.

Step 23. In the *Quiet Period* field, enter the time the switch remains in quiet state after a failed authentication exchange. When the switch is in quiet state, it means the switch is not listening for new authentication requests from the client. The default value is 60 seconds and the range is from one to 65535 seconds.

Quiet Period:

Note: In this example, the quiet period is set to 120 seconds.

Step 24. In the *Resending EAP* field, enter the time the switch waits for a response message from the supplicant before resending a request. The default value is 30 seconds and the range is from one to 65535 seconds.

⚙ Quiet Period:

⚙ Resending EAP:

Note: In this example, resending EAP is set to 60 seconds.

Step 25. In the *Max EAP Requests* field, enter the maximum number of EAP requests that can be sent. EAP is an authentication method used in 802.1X that provides authentication information exchange between the switch and the client. In this case, EAP requests are sent to the client for authentication. The client then has to respond and match the authentication information. If the client does not respond, then another EAP request is set based on the Resending EAP value and the authentication process is restarted. The default value is 2 and the range is from one to 10.

⚙ Quiet Period:

⚙ Resending EAP:

⚙ Max EAP Requests:

Note: In this example, the default value of 2 is used.

Step 26. In the *Supplicant Timeout* field, enter the time before EAP requests are resent to the supplicant. The default value is 30 seconds and the range is from one to 65535 seconds.

⚙ Max EAP Requests: (Rar

⚙ Supplicant Timeout: sec |

Note: In this example, supplicant timeout is set to 60 seconds.

Step 27. In the *Server Timeout* field, enter the time that elapses before the switch sends a request again to the RADIUS server. The default value is 30 seconds and the range is from one to 65535 seconds.

⚙ Max EAP Requests: (Rar

⚙ Supplicant Timeout: sec |

⚙ Server Timeout: sec |

Note: In this example, server timeout is set to 60 seconds.

Step 28. Click **Apply** then click **Close**.

Interface:	Unit	1	Port	GE4
Current Port Control:	Unauthorized			
Administrative Port Control:	<input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized			
RADIUS VLAN Assignment:	<input type="radio"/> Disable <input type="radio"/> Reject <input checked="" type="radio"/> Static			
Guest VLAN:	<input checked="" type="checkbox"/> Enable			
Open Access:	<input type="checkbox"/> Enable			
802.1x Based Authentication:	<input checked="" type="checkbox"/> Enable			
MAC Based Authentication:	<input type="checkbox"/> Enable			
Web Based Authentication:	<input type="checkbox"/> Enable			
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable			
Reauthentication Period:	6000	sec (Range: 300 - 4294967295, Default: 3600)		
Reauthenticate Now:	<input type="checkbox"/>			
Authenticator State:	Connecting			
Time Range:	<input type="checkbox"/> Enable			
Time Range Name:	Dayshift	Edit		
Maximum WBA Login Attempts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> (Range: 3 - 10)			
Maximum WBA Silence Period:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 60 - 65535)			
Max Hosts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 1 - 4294967295)			
Quiet Period:	120	sec (Range: 10 - 65535, Default: 60)		
Resending EAP:	60	sec (Range: 30 - 65535, Default: 30)		
Max EAP Requests:	2	(Range: 1 - 10, Default: 2)		
Supplicant Timeout:	60	sec (Range: 1 - 65535, Default: 30)		
Server Timeout:	60	sec (Range: 1 - 65535, Default: 30)		
Apply <input type="button" value="Close"/>				

Step 29. (Optional) Click **Save** to save settings to the startup configuration file.

Save

8-Port Gigabit PoE Stackable Managed Switch

Port Authentication

Port Authentication Table

Filter: *Interface Type* equals to

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled

You should now have successfully configured the 802.1x port authentication settings on your switch.

Apply Interface Configuration Settings to Multiple Interfaces

Step 1. Click the radio button of the interface that you want to apply the authentication configuration to multiple interfaces.

Port Authentication Table

Filter: *Interface Type* equals to

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input checked="" type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled

Note: In this example, GE4 is chosen.

Step 2. Scroll down then click **Copy Settings**.

<input type="radio"/>	43	GE43	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	44	GE44	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	47	GE47	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	48	GE48	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled

Step 3. In the *to* field, enter the range of interfaces that you want to apply the configuration of

the chosen interface. You can use the interface numbers or the name of the interfaces as input. You can enter each interface separated by a comma (such as 1, 3, 5 or GE1, GE3, GE5) or you can enter a range of interfaces (such as 1-5 or GE1-GE5).

Copy configuration from entry 4 (GE4)

to: (Example: 1,3,5-10 or: GE1,GE3-XG4)

Note: In this example, the configuration settings will be applied to ports 47 to 48.

Step 4. Click **Apply** then click **Close**.

Copy configuration from entry 4 (GE4)

to: (Example: 1,3,5-10 or: GE1,GE3-XG4)

The image below depicts the changes after the configuration.

Port Authentication Table							
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1"/> <input type="button" value="Go"/>							
	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	47	GE47	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	48	GE48	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled	Disabled

You should now have successfully copied the 802.1x authentication settings of one port and applied to other port or ports on your switch.