802.1X Port Authentication Configuration on Cisco 200/300 Series Managed Switches

Objective

The objective of this document is to explain 801.1X port authentication on the 200/300 Series Managed Switches. 802.1X Port Authentication enables the configuration of 802.1X parameters for each port. A port that requests authentication is called the supplicant. The authenticator is a switch or an access point that acts as a network guard to supplicants. The authenticator forwards authentication messages to the RADIUS server so that a port can be authenticated and can send and receive information.

Applicable Devices

- SF/SG 200 and SF/SG 300 Series Managed Switches

Software Version

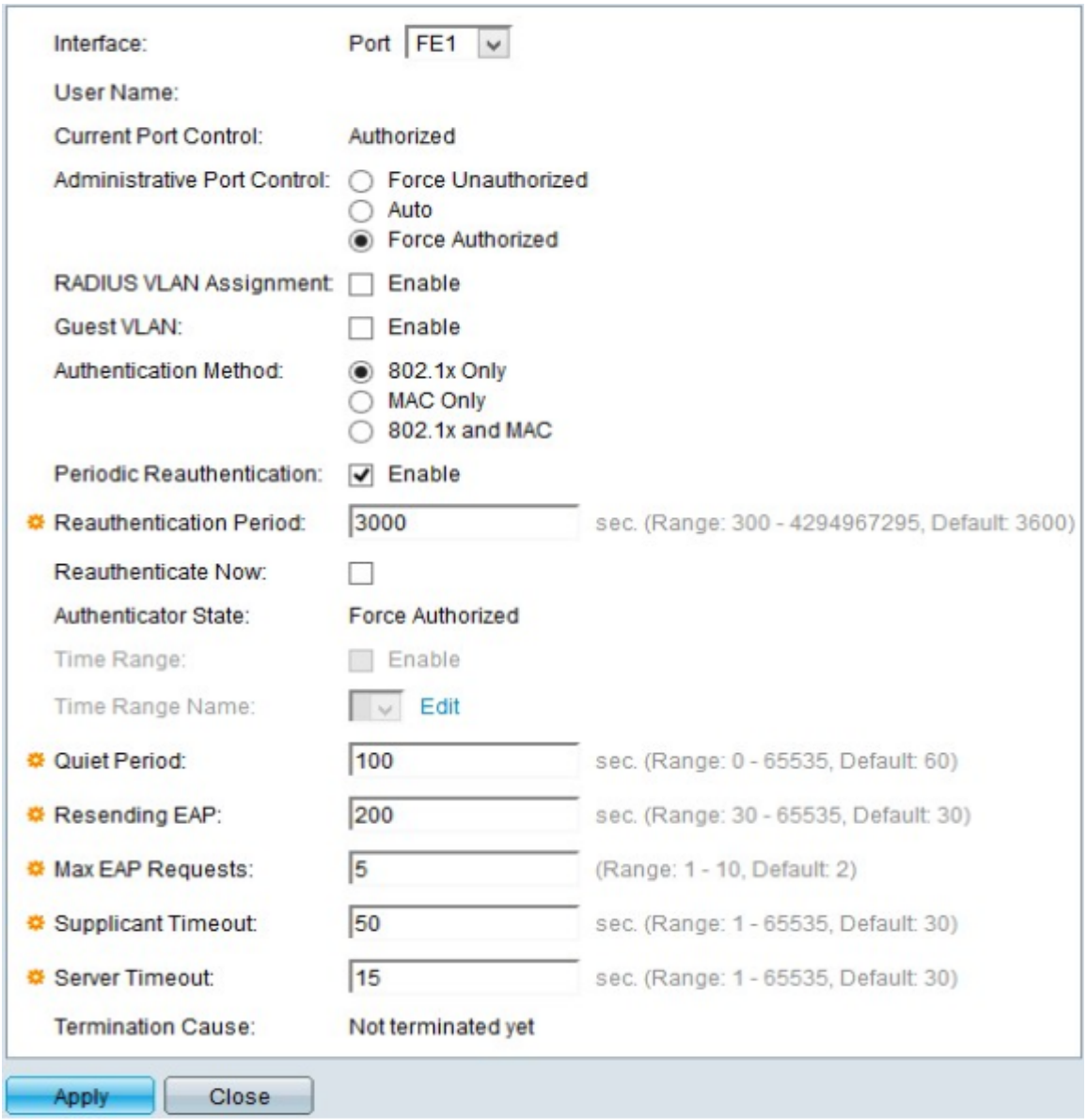
- 1.3.0.62

Port Authentication Configuration

Step 1. Log in to the web configuration utility and choose **Security > 802.1x > Port Authentication**. The *Port Authentication* page opens:

Step 2. Click the radio button that corresponds to the port you would like to edit.

Step 3. Click **Edit**. The *Edit Port Authentication* window appears.



The User Name field displays the user name of the port.

Note: The Current Port Control field displays the current port state. If the port is in Unauthorized state it means that the port is either not authenticated or the Administrative Port Control is set to Force Unauthorized. On the other hand, if the port is in Authorized state, it means that the port is either authenticated or the Administrative Port Control is set to Force authorized.

Step 4. In the Administrative Port Control field, click one of the available radio buttons to determine the port authorization state:

- Force Unauthorized — This option moves the chosen interface to Unauthorized state. In this state, the switch does not provide authentication to the client connected to the interface.

- Auto — This option enables authentication and authorization on the chosen interface. In this state, the switch provides 802.1X authentication to the clients connected to the interface and decides, based on the authentication information exchange with the client, if the client is authenticated or not, and moves the interface to Authorized or Unauthorized state.

- Force Authorized — This option set the interface to Authorized without client

authentication.

Step 5. (Optional) In the Guest VLAN field, check the **Enable** check box to use a guest VLAN for unauthorized ports.

Step 6. In the Authentication Method field, click one of the available radio buttons to authenticate the port. The options are:

- 802.1X Only — Only 802.1X authentication is performed on the port.
- MAC Only — Only MAC-based authentication is performed on the port. Only 8 MAC-based authentications can be performed on a single port.
- 802.1X and MAC — Both authentication methods are performed on the port.

Step 7. In the Periodic Reauthentication field, check the **Enable** check box to enable periodic authentication of the port based on the Reauthentication Period value.

Step 8. In the Reauthentication Period field, enter the time in seconds to reauthenticate the port.

Step 9. Check the **Reauthenticate Now** check box to immediately reauthenticate the port.

Note: The Authenticator State field displays the current state of authentication.

Step 10. (Optional) If Port Based Authentication is enabled on the switch, then the Time Range and Time Range Name fields are enabled. In the Time Range field, enter a time (in seconds) where the port is authorized for use if 802.1X authorization is enabled. In the Time Range Name drop-down list, choose the profile that identifies the time range.

Step 11. In the Quiet Period field, enter the time the switch remains in quite 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.

Step 12. In the Resending EAP (Extensible Authentication Protocol) field, enter the time the switch waits for a response message from supplicant before resending a request.

Step 13. 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 request 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.

Step 14. In the Supplicant Timeout field, enter the time before EAP requests are resent to the supplicant.

Step 15. In the Server Timeout field, enter the time that elapses before the switch sends a request again to the RADIUS server.

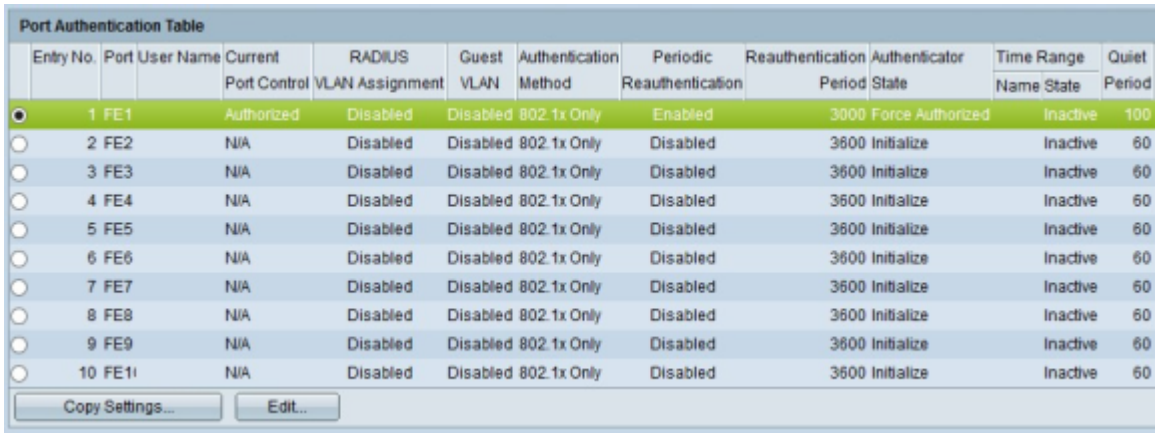
The Termination Cause field displays the reasons for port authentication failure.

Step 16. Click **Apply** to save your configuration.

Apply an Interface Configuration to Multiple Interfaces

This section explains how to apply the 802.1X authentication configuration of a port to multiple ports.

Step 1. Log in to the web configuration utility and choose **Security > 802.1x > Port Authentication**. The *Port Authentication* page opens:



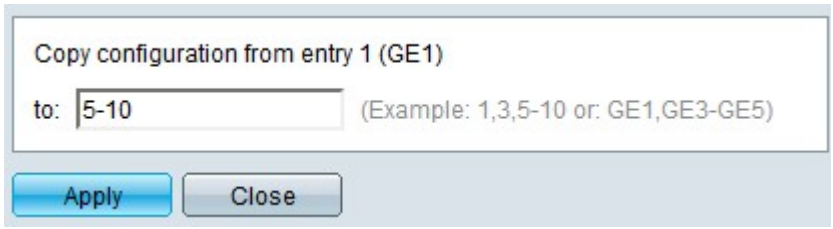
Port Authentication Table

Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period	Authenticator State	Time Range Name	Time Range State	Quiet Period
1	FE1		Authorized	Disabled	Disabled	802.1x Only	Enabled	3000	Force Authorized		Inactive	100
2	FE2		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
3	FE3		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
4	FE4		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
5	FE5		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
6	FE6		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
7	FE7		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
8	FE8		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
9	FE9		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
10	FE1		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60

Copy Settings... Edit...

Step 2. Click the radio button of the interface that you want to apply the authentication configuration to multiple interfaces.

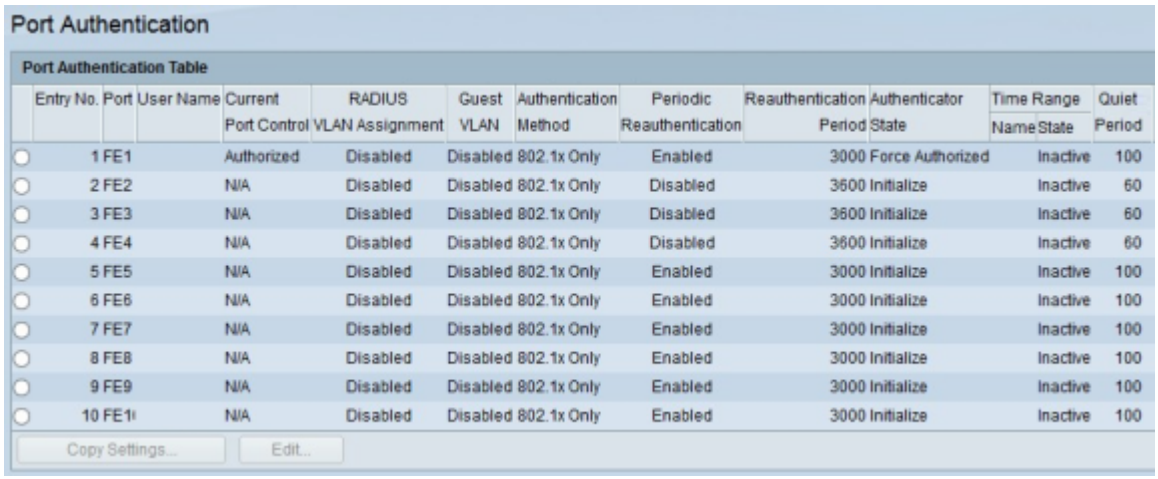
Step 3. Click **Copy Settings**. The *Copy Settings* window appears.



Step 4. In the **to** field, enter the range of interfaces that you want to apply the configuration of the interface chosen in Step 2. You can use the interface numbers or the name of the interfaces as input. You can enter each interface separated by a comma (For example: 1, 3, 5 or GE1, GE3, GE5) or you can enter a range of interfaces (For example: 1-5 or GE1-GE5).

Step 5. Click **Apply** to save your configuration.

The image below depicts the changes after the configuration.



Port Authentication

Port Authentication Table

Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period	Authenticator State	Time Range Name	Time Range State	Quiet Period
1	FE1		Authorized	Disabled	Disabled	802.1x Only	Enabled	3000	Force Authorized		Inactive	100
2	FE2		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
3	FE3		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
4	FE4		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
5	FE5		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
6	FE6		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
7	FE7		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
8	FE8		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
9	FE9		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
10	FE1		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100

Copy Settings... Edit...