Configuration of 802.1x Properties on Sx500 Series Stackable Switches

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 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) in this case. To enable 802.1x port-based authentication, 802.1x should be enabled globally on the switch.

To fully configure 802.1x, the following configurations have to be done:

1. Create a VLAN, click here.
2. Assign Port to VLAN, continue the article referenced above. To configure in the CLI, click here.
3. Configure Port Authentication, click here.

This article explains how to configure 802.1x properties, which include authentication and guest VLAN properties. Please refer to the above articles for other configurations. Guest VLAN provides access to services that do not require the subscribing devices or ports to be authenticated and authorized via 802.1x or MAC-based authentication.

Applicable Devices

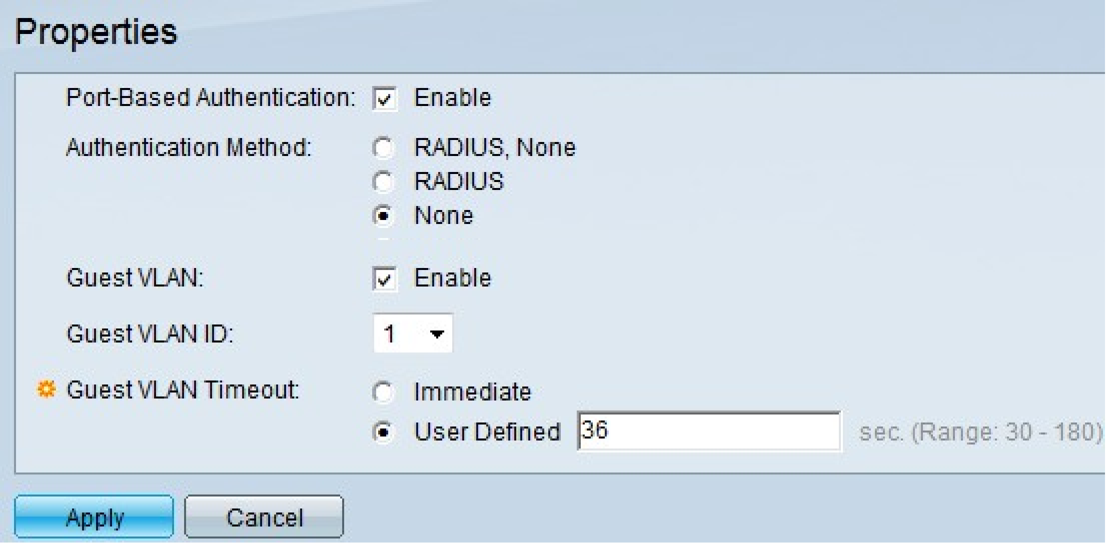
- Sx500 Series Stackable Switches

Software Version

- 1.3.0.62

Enable Port Based Authentication and Guest VLAN in 802.1x Properties

Step 1. Log in to the web configuration utility to choose **Security > 802.1X > Properties** . The *Properties* page opens:



Properties

Port-Based Authentication: ☑ Enable

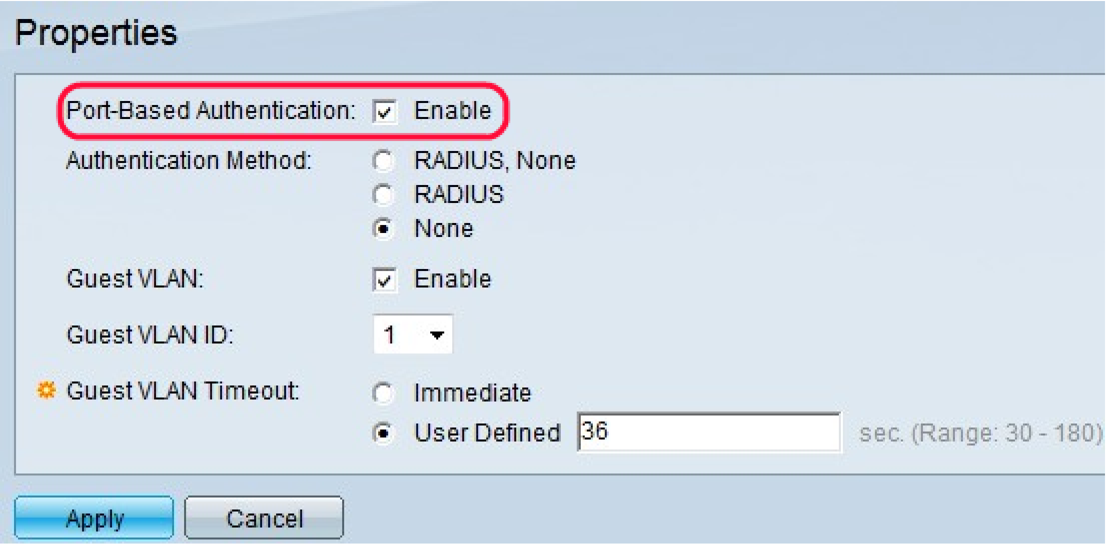
Authentication Method: ○ RADIUS, None ○ RADIUS ● None

Guest VLAN: ☑ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ○ Immediate ● User Defined 36 sec. (Range: 30 - 180)

Step 2. Check **Enable** in the Port-Based Authentication field to enable port-based 802.1x authentication.



Properties

Port-Based Authentication: ☑ Enable

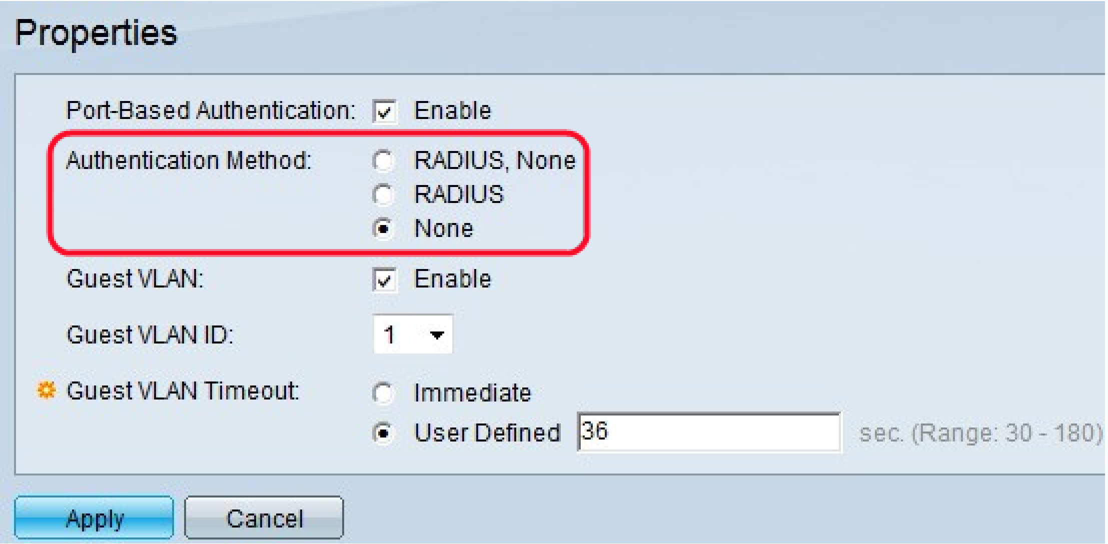
Authentication Method: ○ RADIUS, None ○ RADIUS ● None

Guest VLAN: ☑ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ○ Immediate ● User Defined 36 sec. (Range: 30 - 180)

Step 3. Click the desired radio button from the Authentication Method field. The RADIUS Server performs the authentication of the client. This server validates whether the user is authenticated or not and notifies the switch whether or not the client is allowed access to the LAN and other switch services. The switch acts as a proxy and the server is transparent to the client.



Properties

Port-Based Authentication: ☑ Enable

Authentication Method: ○ RADIUS, None ○ RADIUS ● None

Guest VLAN: ☑ Enable

Guest VLAN ID: 1

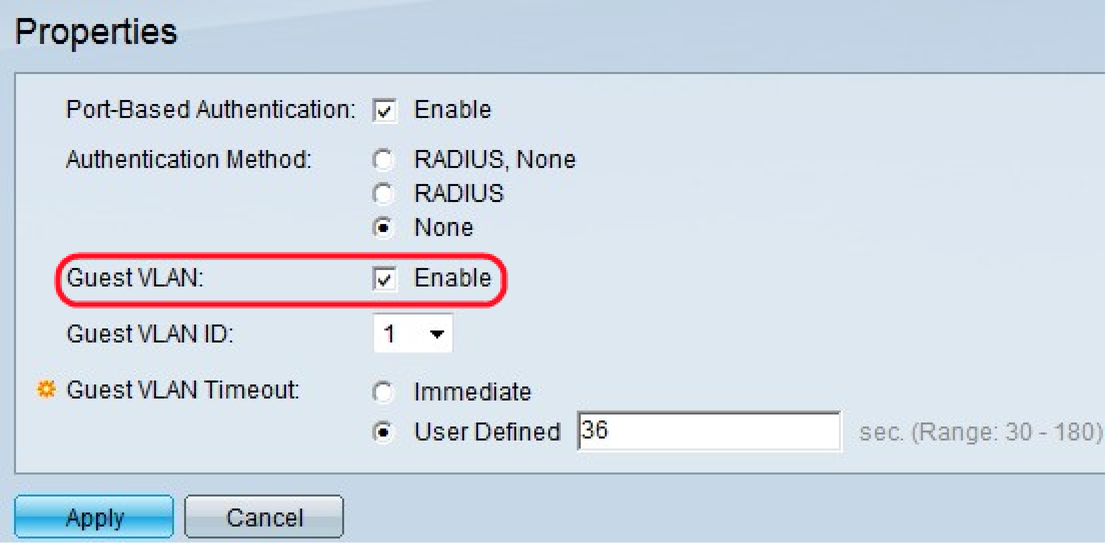
Guest VLAN Timeout: ○ Immediate ● User Defined 36 sec. (Range: 30 - 180)

- RADIUS, None — This performs the port authentication first with the help of the RADIUS Server. If there is no response from the server such as when the server is down, then no authentication is performed and the session is permitted. If the server is available and the user credentials are incorrect then access is denied and the session is ended.

- RADIUS — This performs the port authentication based on the RADIUS Server. If there is no authentication performed then the session is terminated.

- None — Does not authenticate the user and permits the session.

Step 4. (Optional) Check **Enable** to enable the use of a guest VLAN for unauthorized ports in the Guest VLAN field. If a Guest VLAN is enabled, all unauthorized ports automatically join the VLAN chosen in the Guest VLAN ID field. If a port is later authorized, it is removed from the Guest VLAN.



Properties

Port-Based Authentication: ☑ Enable

Authentication Method: ○ RADIUS, None
○ RADIUS
● None

Guest VLAN: ☑ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ○ Immediate
● User Defined 36 sec. (Range: 30 - 180)

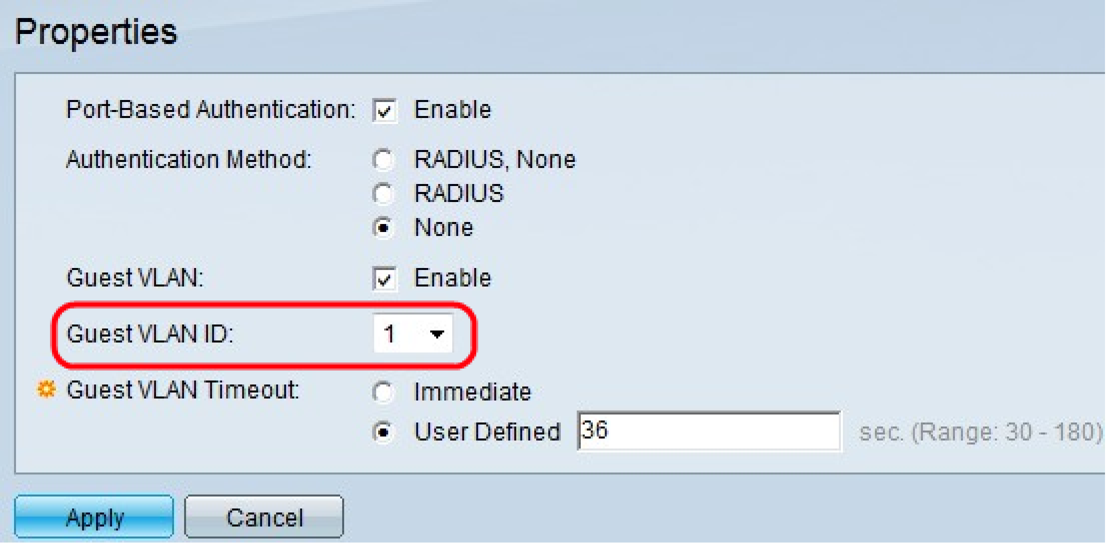
A Guest VLAN mode must be configured before you can use the MAC authentication mode. The 802.1x framework enables a device (the supplicant) to request port access from a remote device (authenticator) to which it is connected. Only when the supplicant that requests port access is authenticated and authorized is it permitted to send data to the port. Otherwise, the authenticator discards the supplicant data unless the data is sent to a Guest VLAN and/or unauthenticated VLANs.

Note: The Guest VLAN, if configured, is a static VLAN with the following characteristics:

- Must be manually defined from an existing static VLAN.
- Is automatically available only to unauthorized devices or ports of devices that are connected and Guest-VLAN-enabled.
- If a port is Guest-VLAN-enabled, the switch automatically adds the port as an untagged member of the Guest VLAN when the port is not authorized, and removes the port from the Guest VLAN when the first supplicant of the port is authorized.
- The Guest VLAN cannot be used as both the Voice VLAN and an unauthenticated VLAN.

Timesaver: If Guest VLAN is disabled, then skip to Step 7.

Step 5. Choose the guest VLAN ID from the list of VLANs in the Guest VLAN ID drop-down list.



Properties

Port-Based Authentication: ☑ Enable

Authentication Method: ○ RADIUS, None ○ RADIUS ● None

Guest VLAN: ☑ Enable

Guest VLAN ID: 1

Guest VLAN Timeout: ○ Immediate ● User Defined 36 sec. (Range: 30 - 180)

Step 6. Click the desired radio button in the Guest VLAN Timeout field. The options available are:

- Immediate — The Guest VLAN expires after a time period of 10 seconds.
- User Defined — Enter the time period manually in the User Defined field.

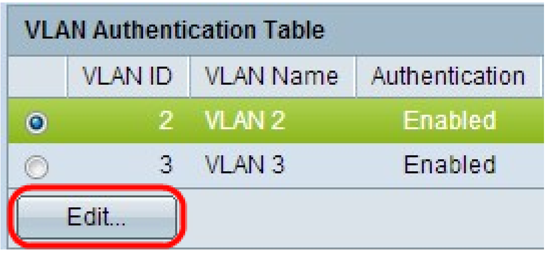
Note: After linkup, if the software does not detect a 802.1x supplicant or if the port authentication has failed, then the port is added to the guest VLAN only after the Guest VLAN Timeout period expires. If the port changes from Authorized to Not Authorized, the port is added to the Guest VLAN only after the Guest VLAN Timeout period expires. The VLAN Authentication Table displays all the VLANs and shows whether authentication is enabled on them or not.

Step 7. Click **Apply** to save the settings.

Unauthenticated VLAN Configuration

When 802.1x is enabled, unauthorized ports or devices are not allowed access to the VLAN unless they are a part of the Guest VLAN or an Unauthenticated VLAN. Ports need to be added manually to VLANs with the use of the *Port to VLAN* page.

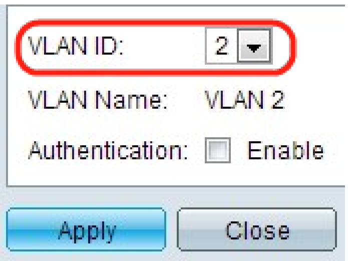
Step 1. Log in to the web configuration utility to choose **Security > 802.1X > Properties.** The *Properties* page opens.



VLAN Authentication Table

	VLAN ID	VLAN Name	Authentication
●	2	VLAN 2	Enabled
○	3	VLAN 3	Enabled

Step 2. Scroll down the page to the VLAN Authentication Table, click the radio button of the VLAN on which you want to disable authentication, and click **Edit**. The *Edit VLAN Authentication* page opens.

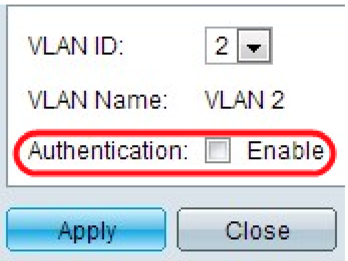


VLAN ID: 2

VLAN Name: VLAN 2

Authentication: □ Enable

Step 3. (Optional) Choose a VLAN ID from the VLAN ID drop-down list.



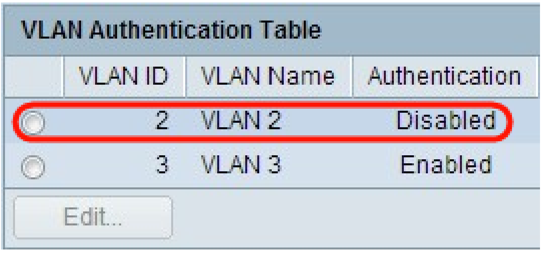
VLAN ID: 2

VLAN Name: VLAN 2

Authentication: □ Enable

Step 4. Uncheck **Enable** to disable authentication and make the VLAN an unauthenticated VLAN.

Step 5. Click **Apply** to apply the settings. The changes are made to the VLAN Authentication Table:



VLAN Authentication Table

	VLAN ID	VLAN Name	Authentication
○	2	VLAN 2	Disabled
○	3	VLAN 3	Enabled