Configuring Authentication for Access Points

AP 802.1X Supplicant

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of an access point, depending on the fixed configuration or installed modules.

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The switch uses a RADIUS server (Cisco ISE) which uses EAP-FAST with anonymous PAC provisioning to authenticate the supplicant AP device.

You can configure global authentication settings that all access points that are currently associated with the controller and any that associate in the future. You can also override the global authentication settings and assign unique authentication settings for a specific access point.

After the 802.1x authentication is configured on the switch, it allows 802.1x authenticated device traffic only.

There are two modes of authentication models:

- Global authentication—authentication setup for all APs
- AP Level authentication—authentication setup for a particular AP

The switch by default authenticates one device per port. This limitation is not present in the Cisco Catalyst Switches. The host mode type configured on the switch determines the number and type of endpoints allowed on a port. The host mode options are:

- Single host mode-a single IP or MAC address is authenticated on a port. This is set as the default.
- Multi-host mode-authenticates the first MAC address and then allows an unlimited number of other MAC addresses. Enable the host mode on the switch ports if connected AP has been configured with local switching mode. It allows the client's traffic pass the switch port. If you want a secured traffic path, then enable dot1x on the WLAN to protect the client data.

The feature supports AP in local mode, FlexConnect mode, sniffer mode, and monitor mode. It also supports WLAN in central switching and local switching modes.

Note In FlexConnect mode, ensure that the VLAN support is enabled on the AP the correct native VLAN is configured on it.

Table 1: Deployment Options

802.1x on AP	Switch	Result
DISABLED	ENABLED	AP does not join the controller
ENABLED	DISABLED	AP joins the controller. After failing to receive EAP responses, fallbacks to non-dot1x CAPWAP discovery automatically
ENABLED	ENABLED	AP joins the controller, post port-Authentication

In a situation where the credentials on the AP need correction, disable the Switch port Dot1x Authentication, and re-enable the port authentication after updating the credentials.

This section contains the following subsections:

Prerequisites for Configuring Authentication for Access Points

Step 1 If the access point is new, do the following:

a) Boot the access point with the installed recovery image.

b) If you choose not to follow this suggested flow and instead enable 802.1X authentication on the switch port connected to the access point prior to the access point joining the controller, enter this command:

lwapp ap dot1x username *username* **password** *password*

Note If you choose to follow this suggested flow and enable 802.1X authentication on the switch port after the access point has joined the controller and received the configured 802.1X credentials, you do not need to enter this command.

Note This command is available only for access points that are running the applicable recovery image.

Connect the access point to the switch port.

Step 2 Install the required software image on the controller and reboot the controller.

Step 3 Allow all access points to join the controller.

Step 4 Configure authentication on the controller.

Step 5 Configure the switch to allow authentication.

Restrictions for Authenticating Access Points

- The OEAP 600 Series access points do not support LEAP.
- Always disable the Bridge Protocol Data Unit (BPDU) guard on the switch port connected to the AP. Enabling the BPDU guard is allowed only when the switch puts the port in port fast mode.

Configuring Authentication for Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 Under 802.1x Supplicant Credentials, select the **802.1x Authentication** check box.

Step 3 In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 4 In the Password and Confirm Password text boxes, enter the password that is to be inherited by all access points that join the controller.

Note You must enter a strong password in these text boxes. Strong passwords have the following characteristics:

- They are at least eight characters long
- They contain a combination of uppercase and lowercase letters, numbers, and symbols
- They are not a word in any language

Step 5 Click **Apply** to send the global authentication username and password to all access points that are currently joined to the controller and to any that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

Step 7 If desired, you can choose to override the global authentication settings and assign a unique username and password to a specific access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to override the authentication settings.
c) Click the **Credentials** tab to open the All APs > Details for (Credentials) page.
d) Under 802.1x Supplicant Credentials, select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global authentication username and password from the controller. The default value is unselected.
e) In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

f) Click **Apply** to commit your changes.
g) Click **Save Configuration** to save your changes.

Note If you want to force this access point to use the controller's global authentication settings, unselect the **Over-ride Global Credentials** check box.

Configuring Authentication for Access Points (CLI)

Step 1 Configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

config ap 802.1Xuser add username *ap-username* **password** *ap-password* **all**

Note You must enter a strong password for the *ap-password* parameter. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Step 2 (Optional) Override the global authentication settings and assign a unique username and password to a specific access point. To do so, enter this command:

config ap 802.1Xuser add username *ap-username* **password** *ap-password Cisco_AP*

Note You must enter a strong password for the *ap-password* parameter. See the note in Step 1 for the characteristics of strong passwords.

The authentication settings that you enter in this command are retained across controller and access point reboots and whenever the access point joins a new controller.

Note If you want to force this access point to use the controller's global authentication settings, enter the **config ap 802.1Xuser delete** *Cisco_AP* command. The following message appears after you execute this command: "`AP reverted to global username configuration.`"

Step 3 Enter the **save config** command to save your changes.

Step 4 (Optional) Disable 802.1X authentication for all access points or for a specific access point by entering this command:

config ap 802.1Xuser disable {**all** | *Cisco_AP*}

Note You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Step 5 See the authentication settings for all access points that join the controller by entering this command:

show ap summary

Information similar to the following appears:

```
Number of APs.................................. 1
Global AP User Name............................ globalap
```

```
Global AP Dot1x User Name..................... globalDot1x
```

Step 6 See the authentication settings for a specific access point by entering this command:

show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

Note If this access point is configured for global authentication, the AP Dot1x User Mode text boxes shows "Automatic." If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode text box shows "Customized."

Step 7 See the authentication status on the AP by entering this command:

show authentication interface wired-port status

Configuring the Switch for Authentication

To enable 802.1X authentication on a switch port, on the switch CLI, enter these commands:

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**
- Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**
- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**
- Switch(config-if)# **end**