Configuring Authentication for Access Points

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Authentication for Access Points

- You can set a global username, password, and enable password for all access points that are currently joined to the device and any that join in the future inherit as they join the device. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.
- After an access point joins the device, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point's console port. When you log in, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.
- The global credentials that you configure on the device are retained across device and access point reboots. They are overwritten only if the access point joins a new device that is configured with a global username and password. If the new device is not configured with global credentials, the access point retains the global username and password configured for the first device.
- You must track the credentials used by the access points. Otherwise, you might not be able to log into an access point's console port. If you need to return the access points to the default *Cisco/Cisco* username

and password, you must clear the device's configuration and the access point's configuration to return them to factory-default settings. To reset the default access point configuration, enter the **ap name** *Cisco_AP* **mgmtuser username** *Cisco* **password** *Cisco* command. Entering the command does not clear the static IP address of the access point. Once the access point rejoins a device, it adopts the default *Cisco/Cisco* username and password.

- You can configure global authentication settings for all access points that are currently joined to the device and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

- This feature is supported on the following hardware:
  - All Cisco switches that support authentication.
  - Cisco Aironet 1140, 1260, 1310, 1520, 1600, 2600, 3500, and 3600 access points

Restrictions for Configuring Authentication for Access Points

- The device name in the AP configuration is case sensitive. Therefore, make sure to configure the exact system name on the AP configuration. Failure to do this results in the AP fallback not working.

Information about Configuring Authentication for Access Points

Cisco IOS access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the nonprivileged mode and enter the **show** and **debug** commands that pose a security threat to your network. You must change the default enable password to prevent unauthorized access and to enable users to enter configuration commands from the access point's console port.

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch where it uses EAP-FAST with anonymous PAC provisioning.

How to Configure Authentication for Access Points

Configuring Global Credentials for Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value*
4. **end**
5. **ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret*
6. **show ap summary**
7. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap mgmtuser username** *user_name* **password 0** *passsword* **secret 0** *secret_value* **Example:** `Device(config)# ap mgmtuser apusr1 password appass 0 secret 0 appass1`	Configures the global username and password and enables the password for all access points that are currently joined to the device and any access points that join the device in the future. In the command, the parameter 0 specifies that an unencrypted password will follow and 8 specifies that an AES encrypted password will follow.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **mgmtuser username** *user_name* **password** *password* **secret** *secret* **Example:** `Device(config)# ap name TSIM_AP-2 mgmtuser apusr1 password appass secret secret`	Overrides the global credentials for a specific access point and assigns a unique username and password and enables password to this access point. The credentials that you enter in this command are retained across device and access point reboots and if the access point joins a new device. **Note** If you want to force this access point to use the device's global credentials, enter the **ap name** *Cisco_AP* **no mgmtuser** command. The following message appears after you execute this command: "AP reverted to global username configuration."
Step 6	**show ap summary** **Example:** `Device# show ap summary`	Displays a summary of all connected Cisco APs.
Step 7	**show ap name** *Cisco_AP* **config general** **Example:** `Device# show ap name AP02 config general`	Displays the global credentials configuration for a specific access point. **Note** If this access point is configured for global credentials, the AP User Mode text boxes shows "Automatic." If the global credentials have been overwritten for this access point, the AP User Mode text box shows "Customized."

Configuring Global Credentials for Access Points (GUI)

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **Global AP Configuration**.

The **Global Configuration** page is displayed.

Step 2 In the **Login Credentials** area, enter the following parameters:

- **User Name**
- **Password**
- **Confirm Password**
- **Secret Password**
- **Confirm Secret Password**

The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters. No character in the password can be repeated more than three times consecutively. The password should not contain the management username or the reverse of the username. The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 3 Click **Apply**.

The global username and password are applied to all the access points that are associated with the devices

Step 4 Click **Save Configuration**.

Step 5 (Optional) You can override the global credentials for a specific access point and assign a unique username and password by following these steps:

a) Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page is displayed.

b) Click the name of an access point.

The **AP > Edit** page is displayed.

c) Click the **Credentials** tab.

d) In the **Login Credentials** area, select the **Over-ride Global Credentials** check box.

e) Enter the values for the following parameters:

- **Username**
- **Password**
- **Enable Password**

f) Click **Apply**.

g) Click **Save Configuration**.

Configuring Authentication for Access Points (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap dot1x username** *user_name_value* **password 0** *password_value*
4. **end**
5. **ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value*
6. **configure terminal**
7. **no ap dot1x username** *user_name_value* **password 0** *password_value*
8. **end**
9. **show ap summary**
10. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap dot1x username** *user_name_value* **password 0** *password_value* **Example:** `Device(config)# ap dot1x username AP3 password 0 password`	Configures the global authentication username and password for all access points that are currently joined to the device and any access points that join the device in the future. This command contains the following keywords and arguments: • **username**—Specifies an 802.1X username for all access points. • *user-id*—Username. • **password**—Specifies an 802.1X password for all access points. • **0**—Specifies an unencrypted password. • **8**—Specifies an AES encrypted password. • *passwd*—Password.

	Command or Action	Purpose
		Note You must enter a strong password for the password parameter. Strong passwords are at least eight characters long, contain a combination of uppercase and lowercase letters, numbers, and symbols, and are not a word in any language.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **dot1x-user username** *username_value* **password** *password_value* **Example:** `Device# ap name AP03 dot1x-user username apuser1 password appass`	Overrides the global authentication settings and assigns a unique username and password to a specific access point. This command contains the following keywords and arguments: • **username**—Specifies to add a username. • *user-id*—Username. • **password**—Specifies to add a password. • **0**—Specifies an unencrypted password. • **8**—Specifies an AES encrypted password. • *passwd*—Password. **Note** You must enter a strong password for the password parameter. See the note in Step 2 for the characteristics of strong passwords. The authentication settings that you enter in this command are retained across device and access point reboots and whenever the access point joins a new device.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**no ap dot1x username** *user_name_value* **password 0** *password_value* **Example:** `Device(config)# no ap dot1x username dot1xusr password 0 dot1xpass`	Disables 802.1X authentication for all access points or for a specific access point. The following message appears after you execute this command: “AP reverted to global username configuration.” **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.

	Command or Action	Purpose
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show ap summary** **Example:** `Device# show ap summary`	Displays the authentication settings for all access points that join the device. **Note** If global authentication settings are not configured, the Global AP Dot1x User Name text box shows "Not Configured."
Step 10	**show ap name** *Cisco_AP* **config general** **Example:** `Device# show ap name AP02 config general`	Displays the authentication settings for a specific access point. **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."

Related Topics

Displaying the Authentication Settings for Access Points: Examples, on page 10

Configuring Authentication for Access Points (GUI)

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **Global AP Configuration**.

The **Global Configuration** page is displayed.

Step 2 In the **802.1x Supplicant Credentials** area, select the **Credentials Required** check box.

Step 3 Enter the username and password details.

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 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 (Optional) You can override the global configuration and assign a unique username and password to a specific access point by following these steps:

a) Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.

The **All APs** page is displayed.

Step 7 Click the name of an access point.

The **AP > Edit** is displayed.

Step 8 Click the **Credentials** tab.

Step 9 In the **802.1x Supplicant Credentials** area, select the **Over-ride Global Credentials** check box.

Step 10 Enter the username and password details.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring the Switch for Authentication (CLI)

Note The procedure to perform this task using the device GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **aaa new-model**
5. **aaa authentication dot1x default group radius**
6. **radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key*
7. **interface TenGigabitEthernet1/0/1**
8. **switch mode access**
9. **dot1x pae authenticator**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables system authentication control.

	Command or Action	Purpose
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables new access control commands and functions.
Step 5	**aaa authentication dot1x default group radius** **Example:** `Device(config)# aaa authentication dot1x default group radius`	Sets the default authentications lists for IEEE 802.1X by using all the radius hosts in a server group.
Step 6	**radius-server host** *host_ip_adress* **acct-port** *port_number* **auth-port** *port_number* **key 0** *unencryptied_server_key* **Example:** `Device(config)# radius-server host 10.1.1.1 acct-port 1813 auth-port 6225 key 0 encryptkey`	Sets a clear text encryption key for the RADIUS authentication server.
Step 7	**interface TenGigabitEthernet1/0/1** **Example:** `Device(config)# interface TenGigabitEthernet1/0/1`	Sets the 10-Gigbit Ethernet interface. The command prompt changes from Controller(config)# to Controller(config-if)#.
Step 8	**switch mode access** **Example:** `Device(config-if)# switch mode access`	Sets the unconditional truncking mode access to the interface.
Step 9	**dot1x pae authenticator** **Example:** `Device(config-if)# dot1x pae authenticator`	Sets the 802.1X interface PAE type as the authenticator.
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Displaying the Authentication Settings for Access Points: Examples, on page 10

Configuration Examples for Configuring Authentication for Access Points

Displaying the Authentication Settings for Access Points: Examples

This example shows how to display the authentication settings for all access points that join the device:

```
Device# show ap summary
Number of APs..................................... 1
Global AP User Name............................... globalap
Global AP Dot1x User Name......................... globalDot1x
```

This example shows how to display the authentication settings for a specific access point:

```
Device# show ap name AP02 config dot11 24ghz general
Cisco AP Identifier............................... 0
Cisco AP Name..................................... TSIM_AP2
...
AP Dot1x User Mode................................ AUTOMATIC
AP Dot1x User Name............................... globalDot1x
```