Cisco-Practice-Book

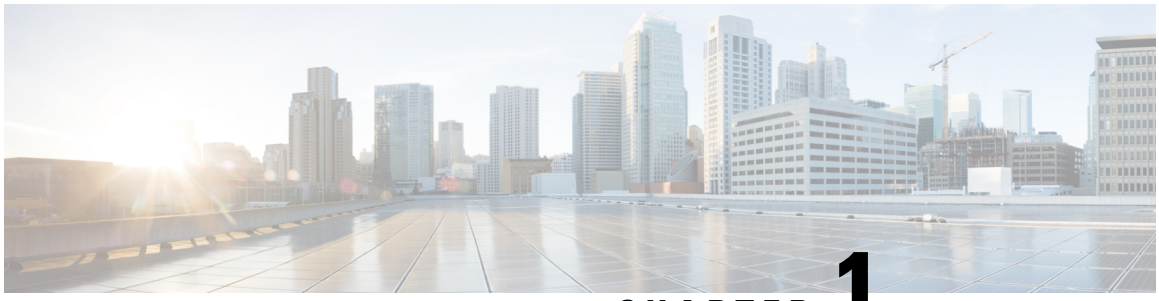
First Published: 2023-06-16

Last Modified: 2023-06-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS



CHAPTER 1

Optimized Roaming

Optimised Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. This feature disassociates clients based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. You can disable the data rate option so that only RSSI is used for disassociating clients.

Optimized roaming also prevents client association when the client's RSSI is low. This feature checks the RSSI of the incoming client against the RSSI threshold. This check prevents the clients from connecting to a Wi-Fi network unless the client has a viable connection. In many scenarios, even though clients can hear beacons and connect to a Wi-Fi network, the signal might not be strong enough to support a stable connection.

You can also configure the client coverage reporting interval for a radio by using optimized roaming. The client coverage statistics include data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) prealarm failures, retransmission requests, and current data rates.

Optimized roaming is useful in the following scenarios:

- Addresses the sticky client challenge by proactively disconnecting clients.
- Actively monitors data RSSI packets.
- Disassociates client when the RSSI is lower than the set threshold.

This section contains the following subsections:

Restrictions for Optimised Learning

- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.

- When basic service set (BSS) transition is sent to 802.11v-capable clients, and if the clients are not transitioned to other BSS before the disconnect timer expires, the corresponding client is disconnected forcefully. BSS transition is enabled by default for 802.11v-capable clients.
- The Cisco Catalyst 9800 controller increments the 80211v smart roam failed counter while disconnecting the client due to optimized roaming.
- We recommend that you do not use the optimized roaming feature with RSSI low check.

Configuring Optimized Roaming (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 On the **Advanced** window, click the relevant band's tab: either **5 GHz Band** or **2.4 GHz Band**.

Step 3 Check the **Optimized Roaming Mode** check box to enable the feature.

Step 4 Choose the required **Optimized Roaming Date Rate Threshold**. The threshold value options are different for 802.11a and 802.11b networks.

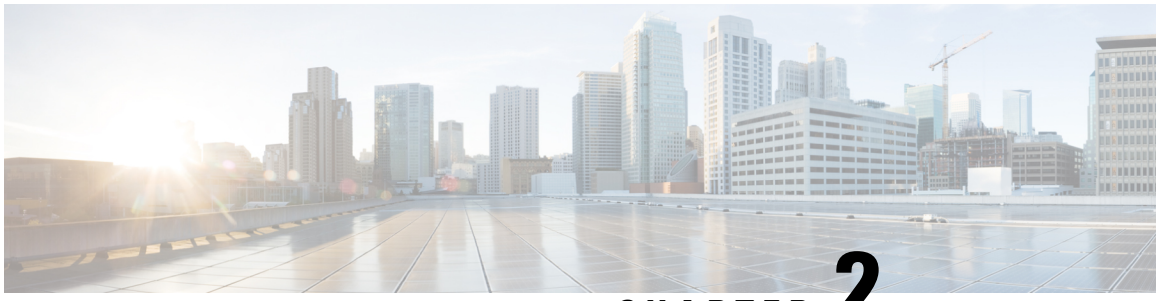
Step 5 Click **Apply** to save the configuration.

Configuring Optimized Roaming (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm optimized-roam** **Example:** `Device(config)# ap dot11 {24ghz|5ghz|6ghz|} rrm optimised-roam`	Configures 802.11a, 802.11b, or 802.11 6-GHz optimized roaming. By default, optimized roaming is disabled.
Step 3	**ap dot11 24ghz rrm monitor optimized-roam data-rate-threshold** {**1M** | **2M** | **5_5M** | **6M** | **9M** | **11M** | **12M** | **18M** | **24M** | **48M** | **54M** | **disable**} **Example:** `Device(configu)# ap dot11 24ghz rrm monitor optimized-roam 18 M`	Configure the data rate threshold for 802.11b for optimized roaming.

	Command or Action	Purpose
Step 4	**ap dot11** {**5ghz** | **6ghz**} **rrm monitor optimized-roam data-rate-threshold**{**6M** | **9M** | **12M** | **18M** | **24M** | **36M** | **48M** | **54M** | **disable**} **Example:** `Device(config)#ap dot11 6ghz rrm monitor optimized-roam 18`	Configure the data rate threshold for 802.11a or 802.11 6-GHz optimized roaming.
Step 5	**p dot11** {**24 ghz** | **6ghz**} **optimized-roaming statistics** **Example:** `Device#show ap dot11 24ghz optimized-roaming statistics`	Displays the 802.11a, 802.11b, or 802.11 6-GHz optimized roaming configurations.



CHAPTER 2

In-Service Software Upgrade

Information about In-Service Software Upgrade

In-Service Software Upgrade (ISSU) is a procedure to upgrade a wireless controller image to a later release while the network continues to forward packets. ISSU helps network administrators avoid a network outage when performing a software upgrade.

ISSU can also be used to apply cold patches without impacting the active network.

ISSU is supported only on the following Cisco Catalyst 9800 Series Wireless Controllers, and supports only upgrade.

- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Catalyst 9800-CL Wireless Controller (Private Cloud)

High-Level Workflow of ISSU

1. Onboard the controller software image to the flash memory.
2. Download the AP image to the AP.
3. Install the controller software image.
4. Commit the changes.

Prerequisites for Performing In-Service Software Upgrade

- Ensure that both Active and Standby controllers are in install mode and are booted from *bootflash:/packages.conf*.
- Ensure that the network or device is not being configured during the upgrade.
- Schedule the upgrade when your network is stable and steady.
- Ensure uninterrupted power supply. A power interruption during upgrade procedure might corrupt the software image.

Guidelines and Restrictions for In-Service Software Upgrade

- If you do not run the **install commit** command within 6 hours of the **install activate issu** command, the system will revert to the original commit position. You can choose to delay the commit using the Delayed Commit procedure.
- During ISSU upgrade, while AP rolling upgrade is in progress, the **install abort** command will not work. You should use the **install abort issu** command, instead to cancel the upgrade.
- During ISSU upgrade, the system displays a warning message similar to:

```
found 46 disjoint TDL objects
```

You can ignore the warning message because it does not have any functional impact.

- During ISSU upgrade, if both the controllers (active and standby) have different images after the power cycle, an auto cancel of ISSU is triggered to bring both the controllers to the same version. The following is a sample scenario: Install Version1 (V1) software on the active controller and then apply a SMU hot patch and perform a commit. Now, upgrade the software to Version2 using ISSU, and then power cycle the active controller. At this point, the system has a version mismatch (V1 and V2). The active controller reloads at this stage, after the completion of bulk synchronization. Now, both the controllers come up with the same version (V1 and V1).
- An ISSU upgrade that is canceled because of configuration synchronization failure on the standby controller rolls back to V1 of the software image. However, this information is not available in the **show install** command log. Run the **show issu state detail** command to see the current ISSU state.
- To enable the **clear install** command, you should first run the **service internal** command in global configuration mode, and then run the **clear install** command in privileged EXEC mode.
- Image rollback could be affected if the controller has a stale rollback history and the stack gets formed afterwards. We recommend that you run the **clear install state** command to clear stale information and boot the controller in bundle mode.
- The **clear install state** command doesn't clear an added SMU. To remove a SMU, use either the **install remove file** command or the **install remove inactive** command.
- When the new active controller comes up, after the image upgrade, it doesn't retain the old logs on web GUI window as part of show logs.

- If a stateful switchover (SSO) or a high-availability (HA) event occurs during the rolling AP upgrade procedure of the ISSU feature, the rolling AP upgrade stops. You should then use the **ap image upgrade** command to restart the upgrade process.
- If HA fails to form after the ISSU procedure, you should reload any one chassis again to form HA again.
- Use clear **ap predownload statistics** command before using the **show ap image** command. This ensures that you get the right data after every pre-download.
- Manually cancel the ISSU process using the **install issu abort** command in the scenarios given below, to avoid a software version mismatch between the active controller and the standby controller.
  - An RP link is brought down after standby HOT during an ISSU procedure and the links remains down even after the auto-abort timer expiry
  - An RP link is brought down before the standby controller reaches standby HOT during an ISSU procedure.
- Cisco TrustSec (CTS) is not supported on the RMI interfaces.
- If a switchover occurs while performing an AP upgrade using ISSU, the upgrade process will restart automatically after the switchover.

Upgrading Software Using In-Service Software Upgrade

Use the following procedure to perform a complete image upgrade, that is, from one image to another.

Note ISSU is supported only within and between major releases, for example, 17.3.*x* to 17.3.*y*, 17.6.*x* to 17.6.*y* (within a major release) and 17.3.*x* to 17.6.*x*, 17.3.*x* to 17.9.*x* (among major releases), that is, for two releases after the current supported release. ISSU is NOT supported within and between minor releases or between minor and major releases, for example 17.4.*x* to 17.4.*y* or 17.4.*x* to 17.5.*x* or 17.3.*x* to 17.4.*x*.

ISSU downgrade is not supported for Cisco Catalyst 9800 Series Wireless Controller platforms.

Procedure

	Command or Action	Purpose
Step 1	**install add file** *file-name* **Example:** `Device# install add file Richard`	The controller software image is added to the flash and expanded. **Note** In Cisco Catalyst 9800 Wireless Controller for Switch, run the **install add file** *sub-package-file-name* command to expand the wireless subpackage file.
Step 2	**ap image predownload** **Example:**	Performs predownload of the AP image.

	Command or Action	Purpose
	`Device# ap image predownload`	To see the progress of the predownload, use the **show ap image** command.
Step 3	**install activate issu [auto-abort-timer** *timer***]** **Example:** `Device# install activate issu`	Runs compatibility checks, installs the package, and updates the package status details. Optionally, you can configure the time limit to cancel the addition of new software without committing the image. Valid values are from 30 to 1200 minutes.

Step 4	Run either of the following commands:
	• **instal abort issu**
	`Device# install abort issu`
	Cancels the upgrade process and returns the device to the previous installation state. This is applicable for both controller and the AP.
	• **install commit**
	`Device# install commit`
	Commits the activation changes to be persistent across reloads.
	Note If you do not run the **install commit** command within six hours of completing the previous step, the system will revert to the original commit position.	

Upgrading Software Using ISSU (GUI)

Before you begin

1. The device should be in Install mode.
2. The device should have an HA pair. The standby controller should be online and is in SSO mode.

   You can verify the details using **show issu state detail** command.

Procedure

Step 1 Choose **Administration** > **Software Management**.

Step 2 Under the **Software Upgrade** tab, check the **ISSU Upgrade (HA Upgrade) (Beta)** check box.

Step 3 In the **AP Upgrade Configuration** section, from the **AP Upgrade per Iteration** drop-down list choose the percentage of APs to be upgraded.

Step 4 Click **Download & Install**.

This initiates the upgrade process and you can view the progress in the **Status** dialog box.

Click the **Show Logs** link to view the upgrade process details.

Note An SSO takes place while activating the image on the active controller. After the SSO, you should login again to the controller.

Step 5 The system enables the **Commit** and **ISSU Abort** buttons after the upgrade.

Click **Commit** to commit the activation changes, or **ISSU Abort** to terminate the upgrade process and return the device to the previous installation state.

Upgrading Software Using In-Service Software Upgrade with Delayed Commit

Use this procedure to upgrade the controller software with delayed commit, which will help you to run and test the new software without committing the image.

Procedure

	Command or Action	Purpose
Step 1	**install add file** *file-name* **Example:** `Device# install add file <file>`	Adds and expands the controller software image to the flash. **Note** In Cisco Catalyst 9800 Wireless Controller for Switch, run the **Install add file***sub-package-file-name*command to expand the wireless subpackage file.
Step 2	**ap image predownload** **Example:** `Device# ap image predownload`	Performs predownload of the AP image.
Step 3	**install auto-abort-timer stop** **Example:** `Device# install auto-abort-timer stop`	Stops the termination timer so that the upgrade process is not terminated after the default termination time of six-eight hours.
Step 4	**install activate issu** **Example:** `Device# install activate issu`	Runs compatibility checks, installs the package, and updates the package status details.

	Command or Action	Purpose
Step 5	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Monitoring In-Service Software Upgrade

To view the ISSU state after the install add ISSU and before the install activate ISSU, use the following command:

```
Device# show issu state detail

-- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1
Current ISSU Status: Enabled
Previous ISSU Operation: Abort Successful
====================================================
System Check Status
----------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
====================================================
No ISSU operation is in progress
show install summary
[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG I 17.1.1.0.432
IMG C 16.12.2.0.2707
--------------------------------------------------------------------------------
Auto abort timer: inactive
```

To view the ISSU state after activating ISSU, use the following command:

```
Device# show issu state detail

Current ISSU Status: In Progress
Previous ISSU Operation: Abort Successful
====================================================
System Check Status
----------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
====================================================
Operation type: Step-by-step ISSU
Install type : Image installation using ISSU
Current state : Activated state
Last operation: Switchover
```

```
Completed operations:
Operation Start time
-----------------------------------------------------
Activate location standby Chassis 2 2019-09-17:23:41:12
Activate location active Chassis 1 2019-09-17:23:50:06
Switchover 2019-09-17:23:52:03
State transition: Added -> Standby activated -> Active switched-over
Auto abort timer: automatic, remaining time before rollback: 05:41:53
Running image: bootflash:packages.conf
Operating mode: sso, terminal state reached
show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG U 17.1.1.0.432
--------------------------------------------------------------------------------
Auto abort timer: active on install_activate, time before rollback - 05:41:49
```

To view the ISSU state after installing the commit, use the following command:

```
Device# show issu state detail

--- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1
Current ISSU Status: Enabled
Previous ISSU Operation: Successful
=====================================================
System Check Status
-----------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
=====================================================
No ISSU operation is in progress
show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG C 17.1.1.0.432
--------------------------------------------------------------------------------
Auto abort timer: inactive
```

To view the ISSU state after terminating the ISSU process, use the following command:

```
Device# show issu state detail
Current ISSU Status: In Progress
Previous ISSU Operation: Abort Successful
=====================================================
System Check Status
-----------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
```

```
=====================================================
Operation type: Step-by-step ISSU
Install type : Image installation using ISSU
Current state : Timeout-error state
Last operation: Commit Chassis 1
Completed operations:
Operation Start time
-----------------------------------------------------
Activate location standby Chassis 2 2019-09-17:23:41:12
Activate location active Chassis 1 2019-09-17:23:50:06
Switchover 2019-09-17:23:52:03
Abort 2019-09-18:00:14:13
Commit Chassis 1 2019-09-18:00:28:23
State transition: Added -> Standby activated -> Active switched-over -> Activated ->
Timeout-error
Auto abort timer: inactive
Running image: bootflash:packages.conf
Operating mode: sso, terminal state reached

To view the summary of the active packages in a system, use the following command:
Device# show install summary

[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG C 16.12.2.0.2707
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Troubleshooting ISSU

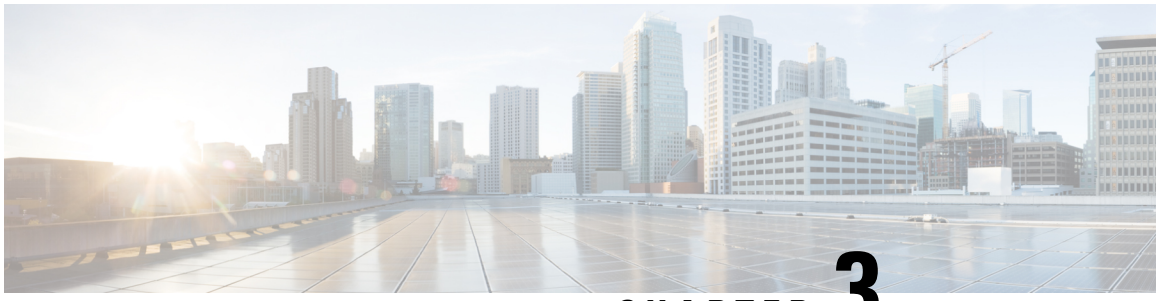
Using **install activate issu** command before completing AP pre-download.

The following scenario is applicable when you run the **install activate issu** command before completing AP pre-download. In such instances, you should run the **ap image predownload** command and then proceed with the activation.

```
Device# install activate issu

install_activate: START Wed Jan  8 04:48:04 UTC 2020
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]
y
Building configuration...
[OK]Modified configuration has been saved
install_activate: Activating ISSU
NOTE: Going to start Activate ISSU install process
STAGE 0: System Level Sanity Check
================================================
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
--- Verifying Platform specific ISSU admission criteria ---
CONSOLE: FAILED: Install operation is not allowed.
```

```
 Reason -> AP pre-image download is mandatory f
or hitless software upgrade.
 Action -> Trigger AP pre-image download.
FAILED: Platform specific ISSU admission criteria
ERROR: install_activate  exit(2 ) Wed Jan  8 04:48:37 UTC 2020
```



CHAPTER 3

Security

Information about Data Datagram Transport Layer Security

Data Datagram Transport Layer Security (DTLS) enables you to encrypt CAPWAP data packets that are sent between an access point and the controller using DTLS, which is a standards-track IETF protocol that can encrypt both control and data packets based on TLS. CAPWAP control packets are management packets that are exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data).

If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

If an access point supports Data DTLS, it enables data DTLS after receiving the new configuration from the controller . The access point performs a DTLS handshake on port 5247 and after successfully establishing the DTLS session. All the data traffic (from the access point to the controller and the controller to the access point) is encrypted.

Note The throughput is affected for some APs that have data encryption enabled.

The controller does not perform a DTLS handshake immediately after processing client-hello with a cookie, if the following incorrect settings are configured:

- ECDHE-ECDSA cipher in “ap dtls-cipher < >” and RSA-based certificate in “wireless management trustpoint”.
- RSA cipher in “ap dtls-cipher < >” and EC-based certificate in “wireless management trustpoint”.

Note This is applicable when you move from CC - > FIPS - > non-FIPS mode.

Note If the AP’s DHCP lease time is less and the DHCP pool is small, access point join failure or failure in establishing the Data Datagram Transport Layer Security (DTLS) session may occur. In such scenarios, associate the AP with a named site-tag and increase the DHCP lease time for at least 8 days.

Configuring Data DTLS (GUI)

Follow the procedure to enable DTLS data encryption for the access points on the controller :

Procedure

Step 1 Click **Configuration** > **Tags and Profile** > **AP Join**.

Step 2 Click **Add** to create a new **AP Join Profile** or click an existing profile to edit it.

Step 3 Click **CAPPWAP** > **Advanced**.

Step 4 Check **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.

Step 5 Click **Update & Apply to Device**.

Configuring Data DTLS (CLI)

Follow the procedure given below to enable DTLS data encryption for the access points on the controller :

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:**	Configures an AP profile and enters AP profile configuration mode.

	Command or Action	Purpose
	`Device(config)# ap profile test-ap-profile`	**Note** You can use the default AP profile (default-ap-profile) or create a named AP profile, as shown in the example.

Step 3	**link-encryption**
	Example:
	`Device(config-ap-profile)# link-encryption`
		Enables link encryption based on the profile. Answer yes, when the system prompts you with this message:
		Note If you set stats-timer as as zero (0) under the AP profile, then the AP will not send the link encryption statistics.
		`Enabling link-encryption will reboot the APs with link-encryption.`
		`Are you sure you want to continue? (y/n)[y]:`

Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.
Step 5	**show wireless dtls connections** **Example:** `Device# show wireless dtls connections`	(Optional) Displays the DTLS session established for the AP that has joined this controller.
Step 6	**show ap link-encryption** **Example:** `Device# show ap link-encryption`	(Optional) Displays the link encryption-related statistics (whether link encryption is enabled or disabled) counter received from the AP.

Introduction to the 802.1X Authentication

IEEE 802.1X port-based authentication is configure on a device to prevent unauthorized devices from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration. Any device connecting to a switch port where 802.1X authentication is enabled must go through relevant EAP authentication model to start exchanging traffic.

Currently, the Cisco Wave 2 and Wi-Fi 6 (802.11AX) APs support 802.1X authentication with switch port for EAP-FAST, EAP-TLS and EAP-PEAP methods. Now, you can enable configurations and provide credentials to the AP from the controller .

Note If the AP is dot1x EAP-FAST, when the AP reboots, it should perform an anonymous PAC provision. For performing PAC provision, the ADH cipher suites should be used to establish an authenticated tunnel. If the ADH cipher suites are not supported by radius servers, AP will fail to authenticate on reload.

- EAP-FAST Protocol
- EAP-TLS/EAP-PEAP Protocol

EAP-FAST Protocol

In the EAP-FAST protocol developed by Cisco, in order to establish a secured TLS tunnel with RADIUS, the AP requires a strong shared key (PAC), either provided via in-band provisioning (in a secured channel) or via out-band provisioning (manual).

Note The EAP-FAST type configuration requires 802.1x credentials configuration for AP, since AP will use EAP-FAST with MSCHAP Version 2 method.

Note Local EAP is not supported on the Cisco 7925 phones.

Note In Cisco Wave 2 APs, for 802.1x authentication using EAP-FAST after PAC provisioning (caused by the initial connection or after AP reload), ensure that you configure the switch port to trigger re-authentication using one of the following commands: **authentication timer restart***num* or **authentication timer reauthenticate***num*

Starting from Cisco IOS XE Amsterdam 17.1.1, TLS 1.2 is supported in EAP-FAST authentication protocol.

EAP-TLS/EAP-PEAP Protocol

The EAP-TLS protocol or EAP-PEAP protocol provides certificate based mutual EAP authentication.

In EAP-TLS, both the server and the client side certificates are required, where the secured shared key is derived for the particular session to encrypt or decrypt data. Whereas, in EAP-PEAP, only the server side certificate is required, where the client authenticates using password based protocol in a secured channel.

Note The EAP-PEAP type configuration requires Dot1x credentials configuration for AP; and the AP also needs to go through LSC provisioning. AP uses the PEAP protocol with MSCHAP Version 2 method.

Limitations of the 802.1X Authentication

- 802.1X is not supported on dynamic ports or Ethernet Channel ports.
- 802.1X is not supported in a mesh AP scenario.
- There is no recovery from the controller on credential mismatch or the expiry/invalidity of the certificate on AP. The 802.1X authentication has to be disabled on the switch port to connect the AP back to fix the configurations.

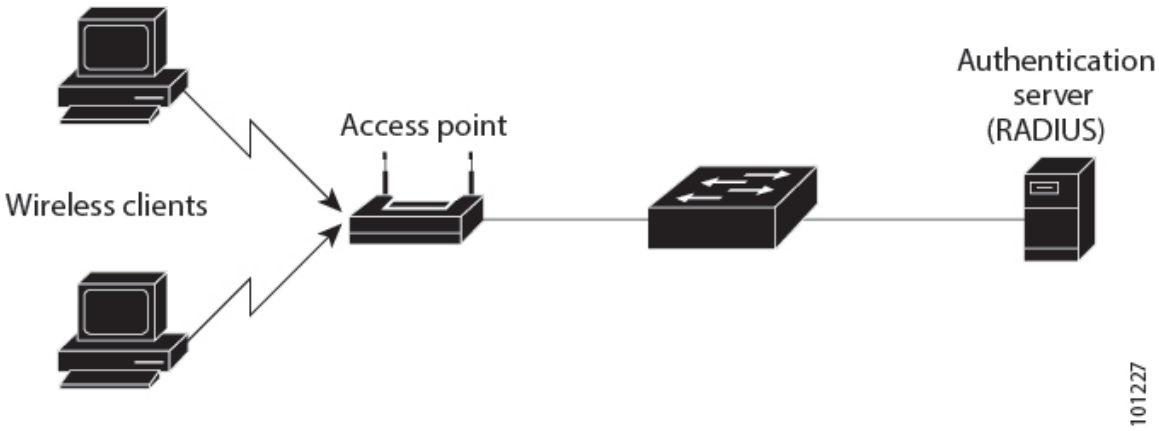
- There are no certificate revocation checks implemented on the certificates installed in AP.
- Only one Locally Significant Certificates (LSC) can be provisioned on the AP and the same certificate must be used for CAPWAP DTLS session establishment with controller and the 802.1X authentication with the switch. If global LSC configuration on the controller is disabled; AP deletes LSC which is already provisioned.
- If clear configurations are applied on the AP, then the AP will lose the 802.1X EAP type configuration and the LSC certificates. AP should again go through staging process if 802.1X is required.
- 802.1X for trunk port APs on multi-host authentication mode is supported. Network Edge Authentication Topology (NEAT) is not supported on COS APs.

Topology - Overview

The 802.1X authentication events are as follows:

1. The AP acts as the 802.1X supplicant and is authenticated by the switch against the RADIUS server which supports EAP-FAST along with EAP-TLS and EAP-PEAP. When dot1x authentication is enabled on a switch port, the device connected to it authenticates itself to receive and forward data other than 802.1X traffic.
2. In order to authenticate with EAP-FAST method, the AP requires the credentials of the RADIUS server. It can be configured at the controller , from where it will be passed on to the AP via configuration update request. For, EAP-TLS or EAP-PEAP the APs use the certificates (device/ID and CA) made significant by the local CA server.

Figure 1: Topology for 802.1X Authentication



Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click **Add**.

Step 3 In the **AP** > **General** tab, navigate to **AP EAP Auth Configuration** section.

Step 4 From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, or *EAP-PEAP* to configure the dot1x authentication type.

Step 5 From the **AP Authorization Type** drop-down list, choose the type as either CAPWAP DTLS + or CAPWAP DTLS.

Step 6 Click **Save & Apply to Device**.

Configuring 802.1X Authentication Type and LSC AP Authentication Type

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile new-profile`	Specify a profile name.
Step 4	**dot1x**{**max-sessions** | **username** | **eap-type** | **sc-ap-auth-state**} **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type. **max-sessions**: Configures the maximum 802.1X sessions initiated per AP. **username**: Configures the 802.1X username for all Aps.

	Command or Action	Purpose
		eap-type: Configures the dot1x authentication type with the switch port. **lsc-ap-auth-state**: Configures the LSC authentication state on the AP.
Step 5	**dot1x eap-type** {**EAP-FAST** | **EAP-TLS** | **EAP-PEAP**} **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type: EAP-FAST, EAP-TLS, or EAP-PEAP.
Step 6	**dot1x lsc-ap-auth-state** {**CAPWAP-DTLS** | **Dot1x-port-auth** | **Both**} **Example:** `Device(config-ap-profile)#dot1x lsc-ap-auth-state Dot1x-port-auth`	Configures the LSC authentication state on the AP. **CAPWAP-DTLS**: Uses LSC only for CAPWAP DTLS. **Dot1x-port-auth**: Uses LSC only for dot1x authentication with port. **Both**: Uses LSC for both CAPWAP-DTLS and Dot1x authentication with port.
Step 7	**end** **Example:** `Device(config-ap-profile)# end`	Exits the AP profile configuration mode and enters privileged EXEC mode.

Configuring the 802.1X Username and Password (GUI)

Procedure

Step 1 Click **Configuration** > **Tags & Profile** > **AP Join**

Step 2 On the **AP Join** page, click the name of the AP Join profile or click **Add** to create a new one.

Step 3 Click the **Management** tab and then click the **Credentials** tab.

Step 4 Enter the local username and password details.

Step 5 Choose the appropriate local password type.

Step 6 Enter 802.1X username and password details.

Step 7 Choose the appropriate 802.1X password type.

Step 8 Enter the time in seconds after which the session should expire.

Step 9 Enable local credentials and/or 802.1X credentials as required.

Step 10 Click **Update & Apply to Device**.

Configuring the 802.1X Username and Password (CLI)

The following procedure configures the 802.1X password for all the APs:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile new-profile`	Specify a profile name.
Step 4	**dot1x** {**max-sessions** | **username** | **eap-type** | **lsc-ap-auth-state**} **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type. **max-sessions**: Configures the maximum 802.1X sessions initiated per AP. **username**: Configures the 802.1X username for all Aps. **eap-type**: Configures the dot1x authentication type with the switch port. **lsc-ap-auth-state**: Configures the LSC authentication state on the AP.
Step 5	**dot1x username** *username***password** {**0** | **8**} *password* **Example:** `Device(config-ap-profile)#dot1x username username password 0 password`	Configures the dot1x password for all the APs. **0**: Specifies an unencrypted password will follow. **8**: Specifies an AES encrypted password will follow.

Enabling 802.1X on the Switch Port

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication dot1x** {**default** | **listname**} **method1**[**method2**…] **Example:** `Device(config)# aaa authentication dot1x default group radius`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
Step 5	**aaa authorization network group** **Example:** `aaa authourization network group`	Enables AAA authorization for network services on 802.1X.
Step 6	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 7	**interface type slot/port** **Example:** `Device(config)# interface fastethernet2/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 8	**authentication port-control** {**auto** | **force-authorized** | **force-unauthorized**} **Example:** `Device(config-if)# authentication port-control auto`	Enables 802.1X port-based authentication on the interface. **auto**—Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the Device by using the supplicant MAC address. **force-authorized**-—Disables IEEE 802.1X authentication and causes the port to change

	Command or Action	Purpose
		to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting. **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port.
Step 9	**dot1x pae** [**supplicant** | **authenticator** | **both**] **Example:** `Device(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters.
Step 10	**end** **Example:** `Device(config-if)# end`	Enters privileged EXEC mode.

Verifying 802.1X on the Switch Port

The following show command displays the authentication state of 802.1X on the switch port:

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version      2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Device#
```

Verifying the Authentication Type

The following show command displays the authentication state of an AP profile:

```
Device#show ap profile <profile-name> detailed ?
  chassis  Chassis
```

```
  |        Output modifiers
  <cr>

Device#show ap profile <profile-name> detailed

  AP Profile Name        : default-ap-profile
  Description            : default ap profile
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth
```