



In-Service Software Upgrade

- [In-service software upgrade \(ISSU\), on page 1](#)
- [Prerequisites for performing ISSU, on page 2](#)
- [Guidelines for ISSU, on page 2](#)
- [Upgrade software using ISSU \(CLI\), on page 3](#)
- [Upgrade software using ISSU \(GUI\), on page 5](#)
- [Upgrade software using ISSU with delayed commit \(CLI\), on page 5](#)
- [Monitor ISSU, on page 6](#)
- [Troubleshoot ISSU, on page 9](#)

In-service software upgrade (ISSU)

An In-Service Software upgrade (ISSU) is a wireless controller procedure that

- upgrades the controller software image to a later release while the network continues to forward packets
- enables administrators to avoid network outages during software upgrades, and
- allows cold patches to be applied without impacting the active network.

ISSU is supported only on these Cisco Catalyst 9800 Series Wireless Controllers. It supports only upgrade operations.

- 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)
- Cisco Wireless 9800M Wireless Controller
- Cisco Wireless 9800H1/H2 Wireless Controller

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.

Table 1: Feature history for In-Service Software Upgrade (ISSU)

Feature Name	Release Information	Feature Description
In-Service Software Upgrade (ISSU)	Cisco IOS XE 17.1.1s	This feature upgrades an image to another image on a device while the network continues to forward packets. ISSU helps network administrators avoid a network outage when performing a software upgrade.

Prerequisites for performing ISSU

- 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 that the system has an uninterrupted power supply. A power interruption during the upgrade procedure can corrupt the software image.

Guidelines for ISSU

- During ISSU upgrade, the system displays a warning message similar to:

```
found 46 disjoint TDL objects
```

The warning message does not impact system functionality.

- 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 Version 1 (V1) software on the active controller. Apply a SMU hot patch. Perform a commit. Upgrade to Version 2 using ISSU. Power cycle the active controller. The system now has a version mismatch (V1 and V2). After bulk synchronization, the active controller reloads. Both controllers have the same version (V1 and V1).
- 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.
- A stale rollback history can affect image rollback after the stack forms. We recommend running the **clear install state** command to clear stale information and boot the controller in bundle mode.
- After the image upgrade, when the new active controller starts up, it does not retain the old logs on the web GUI window as part of show logs.
- During a stateful switchover (SSO) or HA event, the rolling AP upgrade stops. Use the **ap image upgrade** command to restart the upgrade process.

- Use the clear **ap predownload statistics** running the **show ap image** command. This ensures you get accurate data after every pre-download.
- To avoid a software version mismatch between the active and standby controller, manually cancel the ISSU process by using the **install issu abort** command in the appropriate scenarios.
 - The system may disable an RP link after standby HOT during an ISSU procedure. The link stays down after the auto-abort timer expires.
 - An RP link is brought down before the standby controller reaches standby HOT during an ISSU procedure.
- The ISSU upgrade from version 17.12 to 17.15 fails if WPA3 suite-b-192, suite-b, gcmp128, gcmp256, or ccmp256 are already configured.

Restrictions for ISSU

- If you do not run the **install commit** command within six hours of the **install activate issu** command, the system reverts to the original commit position. Delay the commit by using the [Delayed Commit](#) procedure.
- You cannot use the **install abort** command during the AP rolling upgrade. You should use the **install abort issu** command, instead to cancel the upgrade.
- If configuration synchronization fails on the standby controller, the ISSU upgrade cancels and rolls back to software image V1. However, this information isn't available in the **show install** command log. Run the **show issu state detail** command to see the current ISSU state.
- The **clear install state** command doesn't delete the SMU file from flash or storage. To remove a SMU, use either the **install remove file** command or the **install remove inactive** command.
- If HA does not form after the ISSU procedure, reload one chassis.
- You cannot use Cisco TrustSec (CTS) on RMI interfaces.
- If a switchover occurs while performing an AP upgrade using ISSU, the upgrade process will restart automatically after the switchover.

Upgrade software using ISSU (CLI)

Use this procedure to upgrade the image from one version to another.



Note ISSU is supported only within and between major releases. For example, upgrades are supported from 17.3.x to 17.3.y or 17.6.x to 17.6.y (within a major release), as well as from 17.3.x to 17.6.x and from 17.3.x to 17.9.x (among major releases). For more information, check https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/tech-notes/b_issu_9800.html#id_129557. ISSU is not supported within or between minor releases or between minor and major releases. For example, upgrades such as 17.4.x to 17.4.y, 17.4.x to 17.5.x or 17.3.x to 17.4.x are not supported.

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



Note We recommend configuring the percentage of APs to be upgraded by using the *ap upgrade staggered* command.

Procedure

Step 1 Install the file to expand the wireless package file.

Example:

```
Device# install add file file-name
```

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 Perform predownload of the AP image.

Example:

```
Device# ap image predownload
```

To see the progress of the predownload, use the **show ap image** command.

Step 3 Run compatibility checks, install the package, and update the package status details.

Example:

```
Device# install activate issu [auto-abort-time timer]
```

Optionally, you can configure the time limit to cancel the addition of new software without committing the image. The valid values are from 30 to 1200 minutes.

Step 4 Run either of the following commands:

- Cancel the upgrade process and return to the device to the previous installation state.

```
Device# install abort issu
```

This is applicable for both controller and the AP.

- Commit the activation changes to be persistent across reloads.

```
Device# install commit
```

Note

If you do not run the **install commit** command within 6 hours of completing the previous step, the system will revert to the original commit position.

Upgrade software using ISSU (GUI)

Before you begin

1. The device should be in Install mode.
2. It should also have a high-availability (HA) pair. The standby controller should be online and in SSO mode.

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

Procedure

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

Step 2 Check the **ISSU Upgrade (HA Upgrade) (Beta)** check box under the **Software Upgrade** tab.

Step 3 Select the **AP Upgrade per Iteration** percentage option of APs to be upgraded from the drop-down list in the **AP Upgrade Configuration** section.

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.

Upgrade software using ISSU with delayed commit (CLI)

Use this procedure to upgrade the controller software with delayed commit. This lets you run and test the new software without committing the image.

Procedure

Step 1 Add and expand the controller software image to the flash.

Example:

```
Device# install add file file-name
```

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 Perform predownload of the AP image.

Example:

```
Device# ap image predownload
```

Step 3 Run compatibility checks, install the package, and update the package status details.

Example:

```
Device# install activate issu
```

The ISSU completes activation and a message that the **terminal state is reached** is displayed in the **show issue state detail** command output.

Step 4 Stop the termination timer.

Example:

```
Device# install auto-abort-timer stop
```

This ensures that the upgrade process is not terminated after the default termination time of six to eight hours.

Step 5 Commit the activation changes to be persistent across reloads.

Example:

```
Device# install commit
```

Step 6 (Optional) Abort ISSU and go back to the previous version.

Example:

```
Device# install abort issu
```

Monitor ISSU

To view the ISSU state after the install add ISSU and before the install activate ISSU, use the 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 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 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 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 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
-----
```

Troubleshoot ISSU

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

This scenario applies when you run the **install activate issu** command before AP pre-download is complete. In this situation, run the **ap image predownload** command and then activate the system.

```
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 for 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
```

