Upgrade Catalyst 9800 WLC HA SSO Using ISSU

Contents

Introduction

This document describes how to upgrade a pair of 9800 wireless controllers in HA SSO using the ISSU (In-Service Software Upgrade) method.

Requirements

The document covers the procedure, limitation, precautions to take and the upgrade instructions.

Cisco recommends that you have knowledge of these topics:

- Catalyst 9800 Wireless LAN Controller (WLC)
- High Availability Stateful Switchover (HA SSO)

Components used

This document is not restricted to specific software and hardware versions.

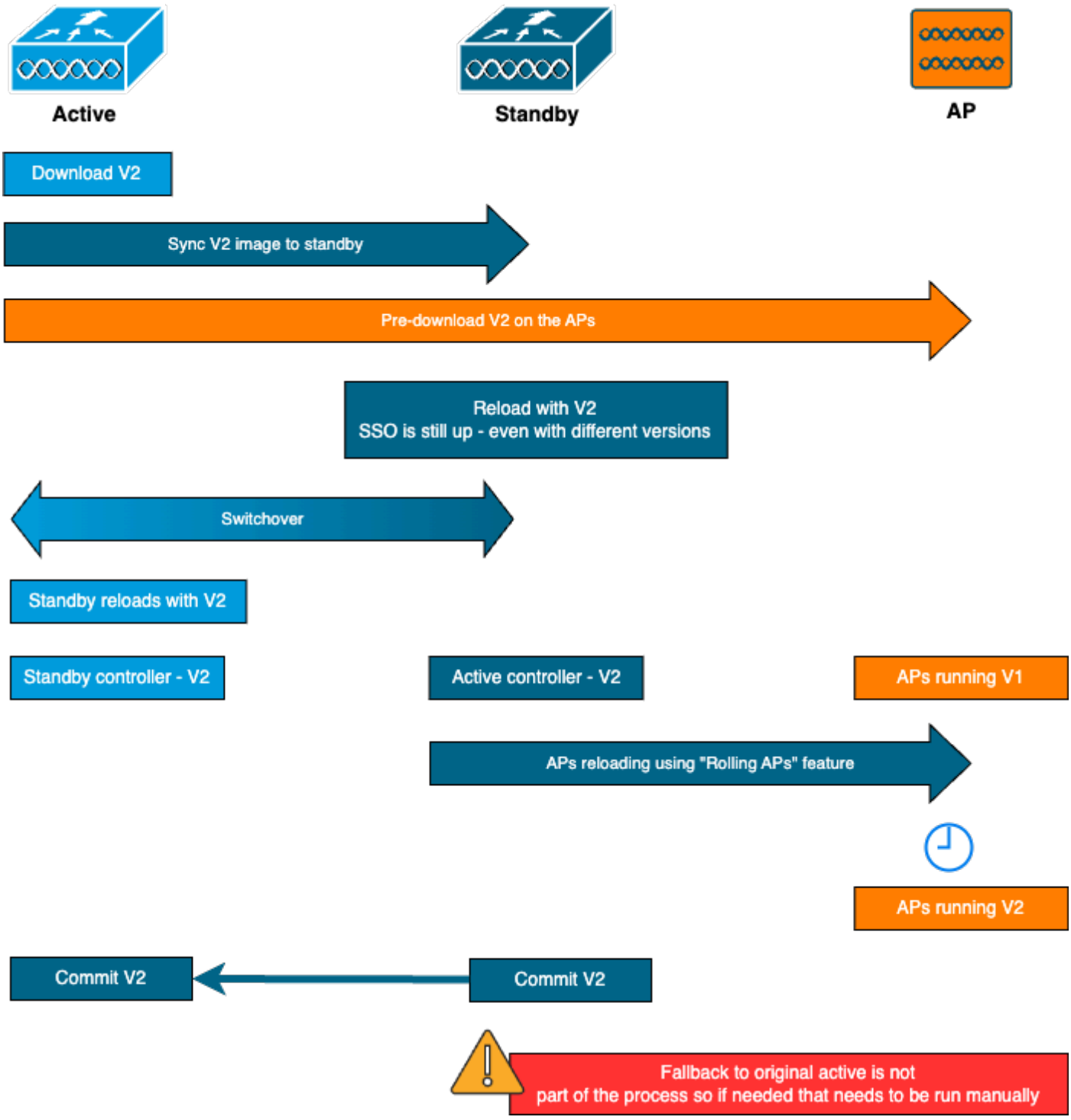
The information in this document was created from the devices in a specific lab environment. All devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

How ISSU works

ISSU is a feature that allows to upgrade the 9800 wireless controllers **with minimal downtime**. If you have enough coverage, then the upgrade is seamless, and the wireless clients must not observe any downtime. To make this possible, ISSU has a mechanism that upgrades one controller at a time and allows APs to upgrade in staggered manner.

Here is a brief overview of the different steps that occur during an ISSU upgrade:

1. The target image (V2) is downloaded to the primary controller running V1 and expanded into packages.
2. The image is then synced to the hot standby controller over the RP connection. That process is the same for every type of upgrade
3. The corresponding AP image (V2) is pre-downloaded to the APs. The pre-download of an image does not impact the service.
4. The standby controller is reloaded and loads with the new image (V2). At this point, the active controller runs V1 and standby run V2 and they form a SSO pair. This is possible only during ISSU upgrade.
5. Once the HA pair is ready (active/standby-hot state), a switchover is executed. The active controller is now running V2 and the standby is running V1. The standby controller reloads and comes up with V2. At this stage, both controllers are on V2, but APs are still running V1.
6. APs are asked to switch images to V2 after the activate step and are upgraded in a rolling AP upgrade fashion to minimize the downtime. This means that sub-groups of APs are reloaded per cycle, and the clients can connect to the neighbouring APs. When the APs rejoin, they rejoin with V2.
7. The final step is commit, which makes the changes permanent.



Limitations

These are the limitation you need to be aware of before proceeding to a ISSU upgrade:

- The base image has to be Cisco IOS XE 17.3 or higher
- ISSU is available only between major releases within the same train. For example, 16.x.x to 17.x.x or 17.x.x to the next major train is **not supported**
- ISSU downgrade is not supported for Cisco Catalyst 9800 Series Wireless Controller platforms
- ISSU upgrade is supported for controller in INSTALL mode only (BUNDLE mode not supported)
- an ISSU upgrade takes more time than a standard upgrade by design because one WLC upgrades itself in the HA pair at a given time, then AP upgrade in a rolling upgrade manner in order to minimize downtime. If you have APs behind a WAN link with some latency, it is important to minimize the AP

image download time as this can drastically increase the ISSU upgrade time through cascading effect. Look into efficient AP upgrade or HTTPS out of band upgrade methods in order to speed up the AP image download time and keep the ISSU total time to a minimum.

Requirements and verifications

Before proceeding to the upgrade of the 9800 wireless controllers using ISSU, there are a few requirements and verifications to make to ensure a smooth upgrade of the controllers and the access points.

Step 1: Verify there is no active or uncommitted version running

CLI command:

```
show install summary
```

Expected output:

You see only one version in "C" (for Activated & Committed) state:

```
WLC#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    17.09.04a.0.6
```

Step 2: Verify the controller is in INSTALL mode

Ensure that both Active and Standby controllers are in install mode and are booted from "bootflash:/packages.conf" (see step 3).

CLI command:

```
show version | i Installation mode
```

Expected output:

```
WLC#show version | i Installation mode
Installation mode is INSTALL
```

Step 3: Check the file used for boot ("packages.conf")

If the controller is in INSTALL mode, it must be booting from the "packages.conf" file.

CLI command:

```
show boot
```

Expected output:

```
WLC#show boot
BOOT variable = bootflash:packages.conf,12;
CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x102

Standby BOOT variable = bootflash:packages.conf,12;
Standby CONFIG_FILE variable =
Standby BOOTLDR variable does not exist
Standby Configuration register is 0x102
```

Step 4: Check redundancy states

The active controller must be in **ACTIVE** state and the standby controller must be in **STANDBY-HOT** state, meaning that the communication is **UP** and that they are communicating with each other.

CLI command:

```
show chassis rmi
show redundancy
```

Expected output:

```
WLC#show chassis rmi
Chassis/Stack Mac Address : 000c.29c4.caff - Local Mac Address
Mac persistency wait time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP                RMI-IP
-------------------------------------------------------------------------------------------------------
*1       Active   000c.29c4.caff     2      V02     Ready               169.254.10.9       198.19.10.9
 2       Standby  000c.29d2.4018     1      V02     Ready               169.254.10.10      198.19.10.1

WLC#show redundancy
Redundant System Information :
------------------------------
...
                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
```

```
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
...

Peer Processor Information :
-----------------------------
              Standby Location = slot 2
        Current Software state = STANDBY HOT
...
```

Step 5: Check if there is enough space in the bootflash to store the new image

A *.bin image size is around 1GB. Make sure that you have multiple GB of free space in the bootflash before proceeding.

CLI command:

```
dir bootflash:/ | in free
```

Expected output:

```
WLC#dir bootflash:/ | in free
14785671168 bytes total (11446026240 bytes free)
```

Step 6: Check that there is no other upgrade in progress

This is a crucial step, because if the controller is stuck in a previous upgrade, then the new upgrade fails.

CLI command:

```
show issu state detail
```

Expected output:

```
WLC#show issu state detail
Current ISSU Status: Enabled
Previous ISSU Operation: N/A
====================================================
System Check                       Status
----------------------------------------------------
Platform ISSU Support              Yes
Standby Online                     Yes
```

```
Autoboot Enabled                    Yes
SSO Mode                            Yes
Install Boot                        Yes
Valid Boot Media                    Yes
Operational Mode                    HA-REMOTE
=====================================================
No ISSU operation is in progress
```

Upgrade procedure

After all checks passed, we can now proceed to the upgrade of the wireless controllers. You can choose to either upgrade the controllers using the GUI or the CLI. There are advantages/disadvantages to both methods. CLI gives you more control since you can initiate each step individually, but this requires a bit more work than upgrading via the GUI. Upgrading the controller via the GUI can be done with a single press of button and all steps are done automatically. However, if something fails during the upgrade, you need to go into CLI to re-initiate the specific step that failed. This guide only shows the CLI upgrade procedure, as GUI procedure can be done simply by executing the GUI instructions.

ISSU CLI Workflow

This section shows a brief summary of the commands executed to upgrade the controllers. A complete explanation of each commands and all steps is provided:

Command	Description
install add file <file>	Image downloaded from CCO to the bootflash is loaded to the controller and expanded into packages
ap image predownload	AP images corresponding to v2 image are pre-downloaded to APs
install activate issu [auto-abort-timer <30-1200>]	ISSU orchestration of one WLC reload followed by the other. The activate trigger does the AP reset in a staggered manner with a best-effort attempt to retain connectivity for clients
install commit	The commit make the changes permanent

Complete procedure

Step 1: Clear AP pre-download statistics

It is best if you clear those statistics before upgrading so you can get a fresh output that only relates to the current upgrade. There must not be any pre-download in progress before starting the upgrade.

CLI command:

```
clear ap predownload statistics
show ap image
```

Expected output:

```
WLC#show ap image
Total number of APs  : 2
```

```
Number of APs
        Initiated                   : 0
        Downloading                 : 0
        Predownloading              : 0
        ...
        Predownload in progress     : No
```

Step 2: Remove the previous software image
In case of not enough space in bootflash, you can always consider to clean up the old installation files using the install remove inactive command.

CLI command:

```
install remove inactive
```

Step 3: Configure the value of AP rolling upgrade percentage

You can set this value up to 25% (max value). Note that if you choose 5% (min value), less APs are upgraded per iteration and the upgrade takes longer, but this helps reduce the global downtime as well. Choose this value according to your deployment and your AP coverage.

CLI command:

```
conf t
ap upgrade staggered {5 | 15 | 25 | one-shot}
end
write memory
```

Step 4: Download the .bin image on the controller

Yon can either upload this image via CLI or via the GUI. With the GUI, this is done when you launch the upgrade process.

CLI command:

```
dir bootflash:*.bin
[OPTIONAL] copy ftp://<username>:<password>@<SERVER_IP>/<IMAGE_FILE> bootflash:
```

Step 5: Install the image

This step initiates the first phase of the upgrade. The controller software image is added to the flash and expanded into packages. This must take a couple of minutes. Once the install add process is complete, check that the new image is seen as "Inactive" from the "show install summary" command.

CLI command:

```
install add file bootflash:<filename>
show install summary
```

Expected output:

```
WLC#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    17.09.04a.0.6
IMG   I    17.12.02.0.2739
```

Step 6: Pre-download the image to the APs

Before activating the image, we need to instruct the APs to pre-download the image that is currently inactive (V2). If the pre-download is not initiated, then the ISSU upgrade fails since this is a required step to minimise downtime. This operation can take several minutes depending on the number of APs that are joined to the controller and the link latency.

CLI command:

```
ap image predownload
show ap image
```

Expected output:

```
WLC#show ap image
Total number of APs  : 2

Number of APs
        Initiated                   : 0
        Downloading                 : 0
        Predownloading              : 2
        Completed downloading       : 0
        Completed predownloading    : 0
        Not Supported               : 0
        Failed to Predownload       : 0
        Predownload in progress     : Yes
```

Step 7: Activate the new image

Once the pre-download is finished, you can activate the new image. This is the longest step of the upgrade process. It 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. Default value is 360 minutes (6 hours). Once you launch the upgrade, the whole ISSU process takes place : standby upgrades, switchover, then new standby upgrades and then the AP staggered upgrade.

CLI command:

```
install activate issu [auto-abort-timer <30-1200 mins>]
```

Expected output:

```
WLC#install activate issu
install_activate: START Sun Jan 14 08:29:36 EST 2024
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 ---
--- Verifying Image ISSU Compatibility ---
Finished Initial System Level Sanity Check

STAGE 1: Installing software on Standby
================================================
--- Starting install_remote ---
[2] install_remote package(s) on chassis 2/R0
WARNING: Found 1545 disjoint TDL objects.
[2] Finished install_remote on chassis 2/R0
install_remote: Passed on [2/R0]
Finished install_remote

STAGE 2: Restarting Standby
================================================
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby to reach terminal redundancy state ---
Finished wait for Standby to reach terminal redundancy state

STAGE 3: Installing software on Active
================================================
--- Starting install_active ---
WARNING: Found 2969 disjoint TDL objects.
[1] install_active package(s) on chassis 1/R0
[1] Finished install_active on chassis 1/R0 install_active: Passed on [1/R0]
Finished install_active

STAGE 4: Restarting Active (switchover to standby)
================================================
--- Starting active reload ---
New software will load after reboot process is completed
```

It is a good idea to monitor the current status of the upgrade using the "show chassis rmi" and "show redundancy" commands periodically. This shows you once a controller is removed from the HA pair and when it comes back, and on which version. Note that the process can take around 20 to 30 minutes.

Once the upgrade is completed, you will see the image as active but "uncommitted" :

```
WLC#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    17.12.02.0.2739

--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 05:23:37
--------------------------------------------------------------------------------
```

Once the installation is over, the WLC will start to reload the APs in staggered manner. To monitor the AP staggered upgrade, you can use the GUI (under "AP Upgrade Statistics" in the "Software Upgrade" section) or the CLI command "show ap uptime", which will show the CAPWAP uptime of the APs. This gives an indication of which APs have already reloaded. You can also check that the AP upgrade is over by checking the logs, using the "show logging" command on the controller:

```
Jan 20 14:23:22.478: %UPGRADE-6-STAGGERED_UPGRADE_COMPLETE: Chassis 2 R0/0: wncmgrd: Staggered AP Upgra
```

Step 8: [OPTIONAL] Stop the "auto-abort" timer

In case you need more time than the default 6 hours for the upgrade (when you have a lot of APs to upgrade and want to make sure this is working fine before committing the image), you can stop this timer. This way the auto rollback will not take place.

CLI command:

```
install auto-abort-timer stop
```

Step 9: Make the new software persistent

Commit the activation changes to be persistent across reloads using the install commit command. This is the final step in a normal upgrade process. The install commit command makes software persistent across reboots.

CLI command:

```
install commit
```

Expected output:

```
WLC#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    17.12.02.0.2739
```

Once the version is committed and the APs have reloaded on the new version, the ISSU upgrade is finished.

Additional operations

You can find some other operations that you possibly need to do during or after the ISSU upgrade, such as aborting the upgrade or rollback to a previous version :

Abort ISSU

This step cancels the upgrade process done so far and returns the device to the previous installation state (V1)**in ISSU fashion**. This is applicable for both controllers and the APs. This can be done in case you notice a severe impact due to the upgrade and if you did not commit the image yet. This command and process **only works if "install commit" has not been issued yet**. Once the image has been committed you cannot rollback in ISSU manner.

CLI command:

```
install abort issu
```

Expected output:

```
STAGE 1: Rolling Back software on Standby
==================================================
--Starting Deactivation at the standby --
--- Starting abort_standby ---
[1] abort_standby package(s) on chassis 1/R0
WARNING: Found 1545 disjoint TDL objects.

[1] Finished abort_standby on chassis 1/R0
abort_standby: Passed on [1/R0]
Finished abort_standby

STAGE 2: Restarting Standby
==================================================
--- Starting standby reload ---
```

```
Finished standby reload

--- Starting wait for Standby to reach terminal redundancy state ---
Finished wait for Standby to reach terminal redundancy state

STAGE 3: Rolling Back software on Active
================================================
--Starting Deactivation at the active --
--- Starting abort_active ---
WARNING: Found 1545 disjoint TDL objects.
[2] abort_active package(s) on chassis 2/R0
[2] Finished abort_active on chassis 2/R0
abort_active: Passed on [2/R0]
Finished abort_active

STAGE 4: Restarting Active (switchover to standby)
================================================
--- Starting active reload ---
New software will load after reboot process is completed
SUCCESS: install_abort  Wed Jan 17 21:58:52 CET 2024
client_loop: send disconnect: Broken pipe
```

Switchover to the "primary" controller

In a production environment this step can be desired if you want to have the original controller being active again. Remember that once ISSU upgrade has completed, the "secondary" unit is the active controller. You can always return to the original state by performing a manual switchover. You need to make sure that the peer unit is in "Standby Hot" state before proceeding.

CLI command:

```
redundancy force-switchover
```

Rollback to previous state once ISSU Upgrade has been completed

Once the upgrade has been committed, ISSU downgrade is not supported for Cisco Catalyst 9800 Series Wireless Controller platforms. At this point a rollback will mean that both Wireless Controllers and APs will reload because of the code change and this will create downtime. You can start by checking the available rollback points and then decide to which one to rollback.

CLI command:

```
show install rollback
show install rollback id <id number>
install rollback to id <id number>
```

Expected output:

```
WLC#sh install rollback
```

```
ID      Label                           Description
-------------------------------------------------------
3       No Label                        No Description
2       No Label                        No Description
1       No Label                        No Description

WLC#sh install rollback id 2
Rollback id - 2 (Created on 2024-04-22 10:31:57.000000000 +0000)
Label: No Label
Description: No Description
Reload required: NO
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.04a.0.6

WLC#install rollback to id 2
install_rollback: START Thu May 30 09:44:38 UTC 2024
install_rollback: Rolling back to id 2

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Rollback ---
Performing Rollback on all members
 [2] Rollback package(s) on Chassis 2/R0
 [1] Rollback package(s) on Chassis 1/R0
 [2] Finished Rollback package(s) on Chassis 2/R0
Checking status of Rollback on [1/R0 2/R0]
Rollback: Passed on [1/R0 2/R0]
Finished Rollback operation

SUCCESS: install_rollback Thu May 30 09:45:40 UTC 2024
```

Troubleshoot

In case you are facing an issue before, during or after the upgrade of the 9800 wireless controllers using ISSU, we recommend that you go through this document that explains the common problems encountered and their solutions.

References

- High Availability using Patching and Rolling AP Upgrade on Cisco Catalyst 9800 Wireless Controllers
- 17.12.X configuration guide