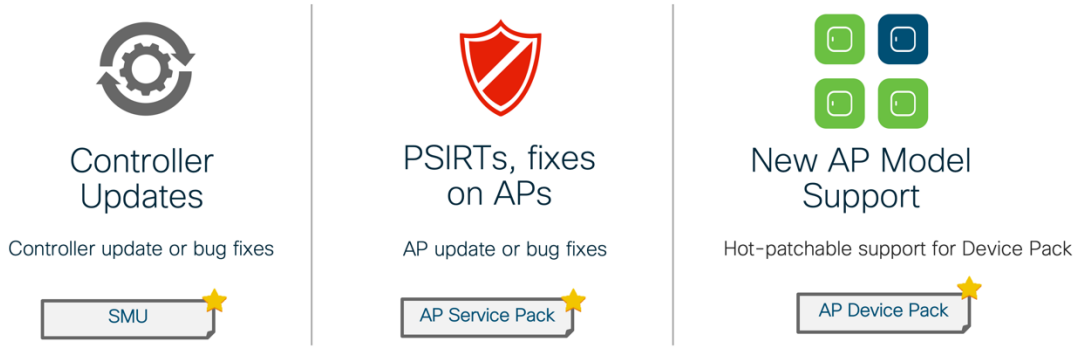
High Availability using Patching and Rolling AP Upgrade on Cisco Catalyst 9800 Wireless Controllers

Overview

Designing for high availability isn't just limited to box failures and network events. It is also about providing high availability in the entire lifecycle of deployment . A significant part of this is the need for updates and upgrades on the network . This is where the power of IOS-XE comes in to provide features that the wireless controllers can now leverage using capabilities that allow for timely fixes and updates to be put into the network. This helps contain impact within an already released image for defects and updates without the need to requalify a new release and helps with faster resolution to critical issues that are time-sensitive by providing fixes in a timely manner.

IOS-XE Release 16.10 and above are infrastructure-ready to support the following features:



1. Controller fixes and updates using Software Maintenance Updates (SMUs)
2. Access point fixes and updates using an AP Service Pack (APSP)
3. The capability to support new AP models using an AP device pack (APDP) .

Platform Support

Catalyst wireless platforms 9800-40, 9800-80, 9800-CL

11ac Wave 1 and Wave 2 Access Points: AP18xx, 2802, 3802, 4800, 1540, 1560, 1700, 2700, 3700, 1570

11ax Access Points: Catalyst 9115, 9117, 9120, 9130

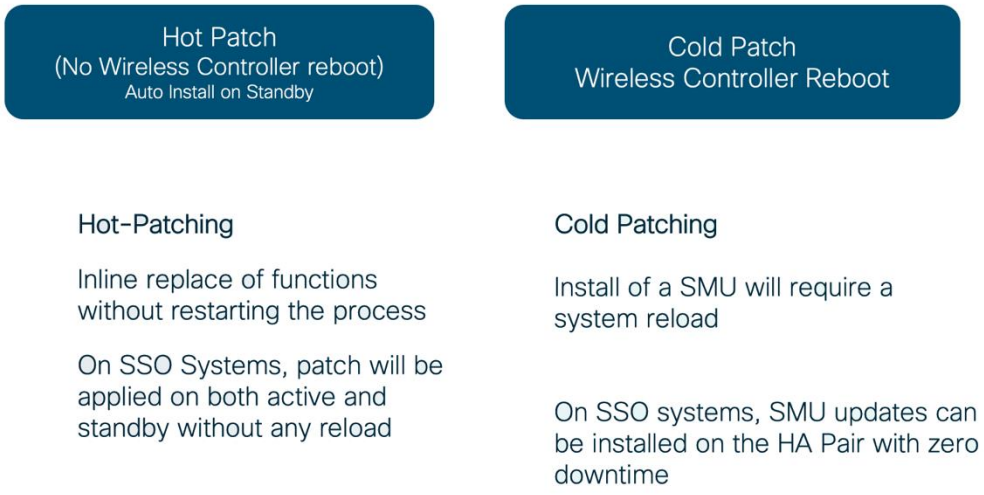
Supported releases

IOS-XE -16.10 and higher

Controller Patching using Software Maintenance Updates (SMU)

SMU is a package that can be installed on a system to provide a patch fix or security resolution to an already released image. An SMU package is provided on a per release and per component basis and is specific to the platform.

There are two types of SMUs – one that can be hot-patched and one that can only be cold-patched.



A hot patch does not need a system reload which means the clients and APs will not be affected. Also, the SMU activation applies to both active and hot-standby in case the controller is an HA pair.

A cold patch on the other hand requires a reload. However, Since we are looking for a seamless, zero-downtime update story, a cold patch can be installed without bringing the network down with an SSO pair. The figure shown below illustrates the process of installing a cold patch on an SSO pair.

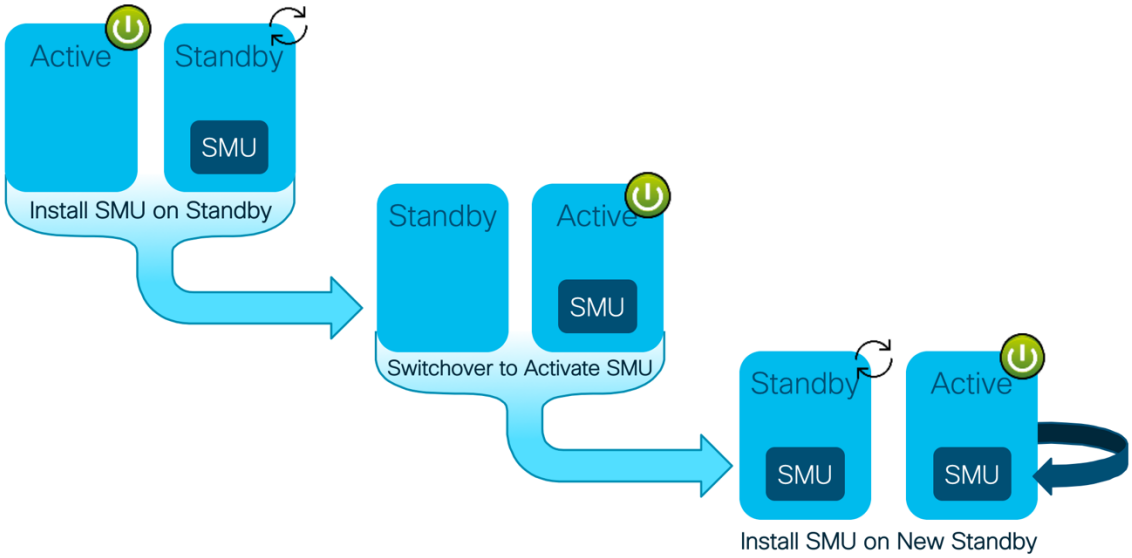


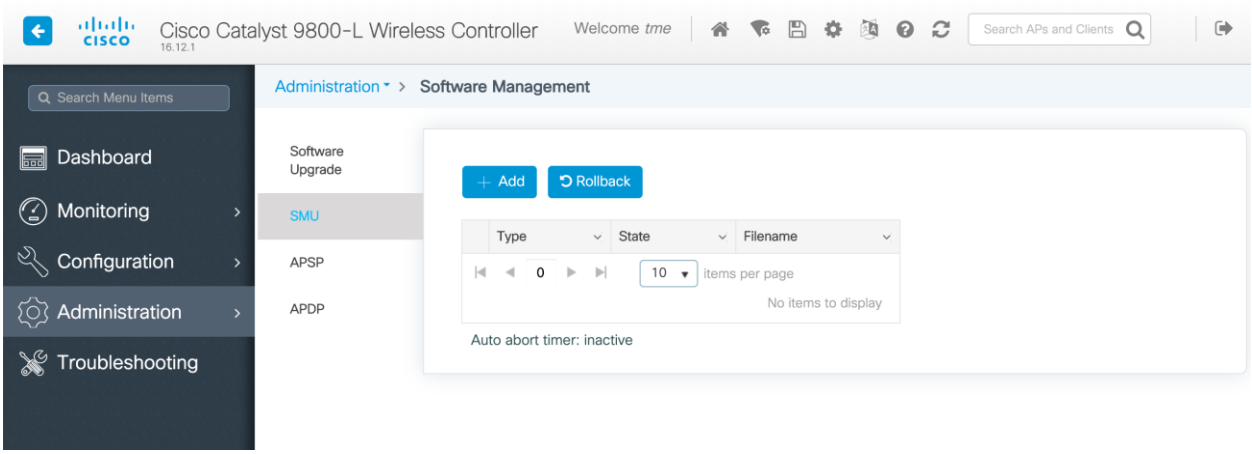
Figure 1: Active Standby Cold Patch Activation

The system will install the SMU on the Standby controller and reload the standby. The network is running because the APs and clients are on the Active. Once the standby is up, a switchover occurs pushing all AP and client sessions to the new active. At this point the SMU is installed on the new standby (which was the old active controller). Both controllers have not been updated with the SMU

Note: SMUs are only released on long-lived MD releases which means controller SMUs will be available starting the first MD release.

Software Maintenance Updates (SMU) installation using WebUI

SMUs can be installed using the workflow under Administration > Software Management > SMU. Add to begin the process followed by Activate and Commit. The option of Rollback is also provided to roll back to a previously created checkpoint.



The following CLIs can be used to install a SMU on the controller :

- Install add
- Install activate
- Install commit

AP Patching using AP Service Pack

Rolling AP Update Infrastructure

Cisco 9800 supports rolling out critical AP bug fixes using an AP Service pack (APSP). To activate the new AP images, APs need to be upgraded to the new image. Cisco 9800 supports doing this in a staggered fashion. The idea here is to upgrade access points in a wireless network in a staggered manner such that an appropriate number of APs are always up and running in the network and providing RF coverage to clients. This is referred to as “Rolling AP Upgrade”.

The AP service pack which is for AP specific fixes will be independent of SMU timeline and will be available on non-MD releases as well post 16.10.

Three main highlights to this feature are:

- Supported natively on the wireless controller using UI/CLI
- Supports Automatic Candidate selection using the RRM based AP neighbor information. The device auto-selects the candidate APs to be upgraded in each iteration based on the percentage of APs to be selected for upgrade in each iteration (5%, 15% or 25% with the default as 15%) and RRM AP neighbor information.
- Clients from candidate APs are actively steered away using 802.11v packet with dissociation imminent field set to make sure we have seamless network connectivity as APs are being upgraded . If clients do not honor this, they will be de-authenticated before AP reload.

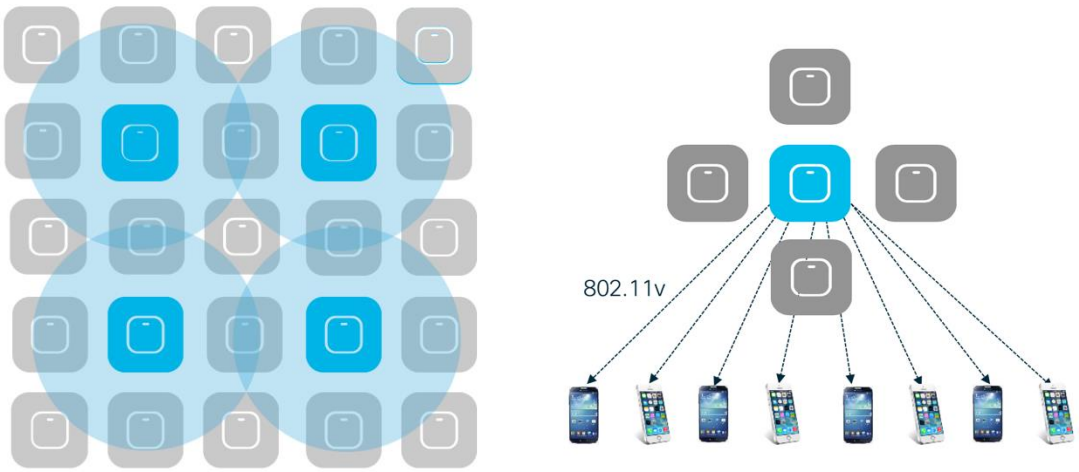


Figure 2: Candidate AP Selection and Client Steering

Release 16.11 provides us the ability to apply an AP fix on a per site and per AP model which means that a pack can be selectively applied on a particular site and specific AP models that are affected by the fix.

Per Site AP Service Pack Rollout

At the time of AP Service Pack (APSP) activation, user selects the sites where the AP service pack should be rolled out. All APs on this site will be updated with the designated service pack, including any new APs that join the site after the filter is applied. This provides an ability to the user to control the propagation of a Service Pack in the network.

It should be noted that this enhancement allows for activating Service Pack on sites incrementally but restricts that all sites should be brought to the same APSP level before a new APSP can be rolled out to a subset of sites.

Per AP Model Service Pack

AP Service pack can also be built with a subset of AP images. The same, when installed results in pre-download only to the affected AP models. Similarly, when activated, it is activated only on the AP models affected, also in conjunction with any site based filers as mentioned in above paragraph

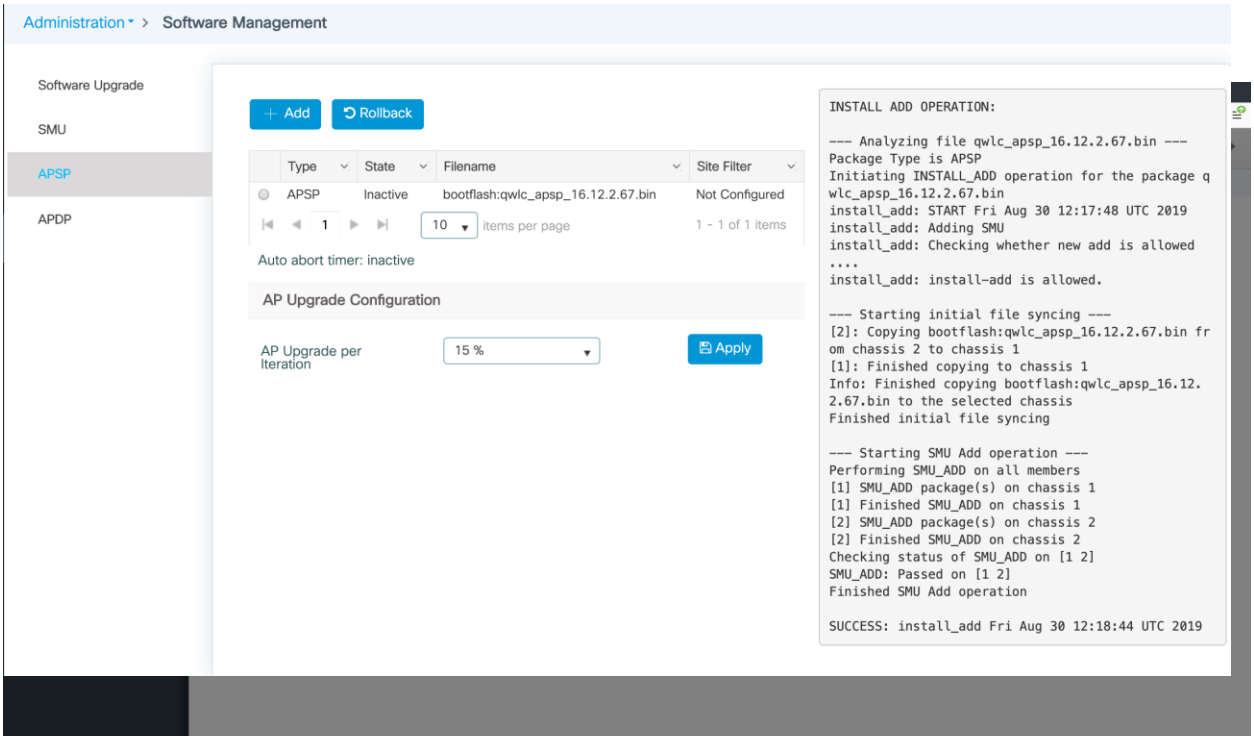
Again, it should be noted that if, for example, 3 model images were included in an APSP, then all future APSPs in that release for any of these 3 AP images will contain all 3 of them. This would help subsequent APSPs to supersede older ones.

Both of these work in conjunction with each other, meaning, you can select specific sites in a campus and then within those sites the fix will be applied to specific APs as designated by the service pack. This enables controlled propagation of the fix with minimum or n service disruption because the fix is pre-downloaded and rolled out only to affected AP models.

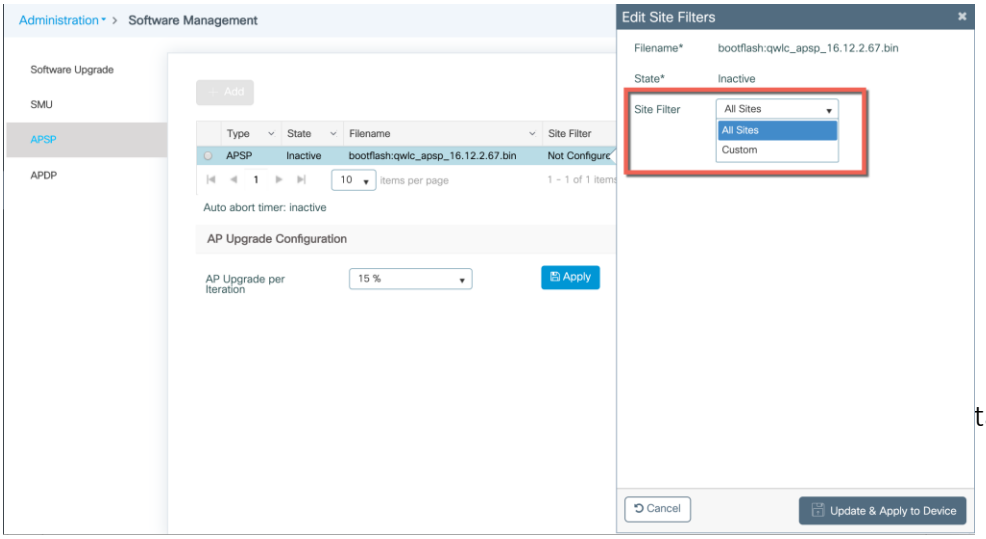
Web UI Configuration

The AP Service pack can be applied using a simple workflow on the controller UI. The process is described in the steps below:

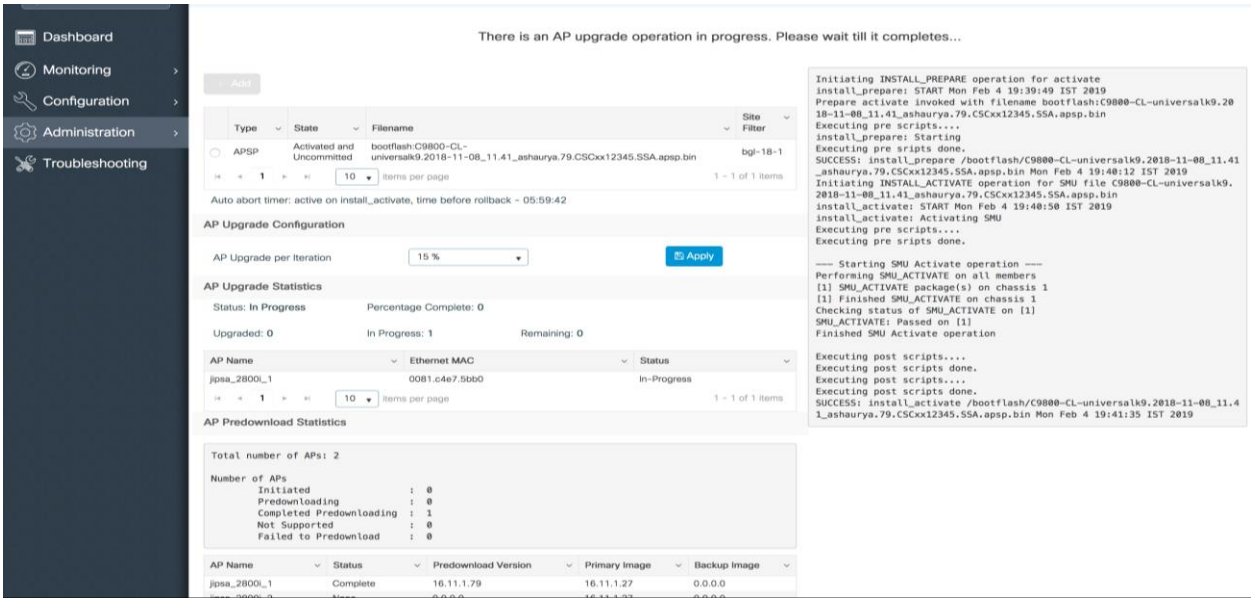
Step1: Add the AP Service pack under Administration > Software Management > APSP



Step 2: Select the Site-filters (Optional) and AP Upgrade per iteration percentage (the default is 15%) . Click on Update & Apply to Device

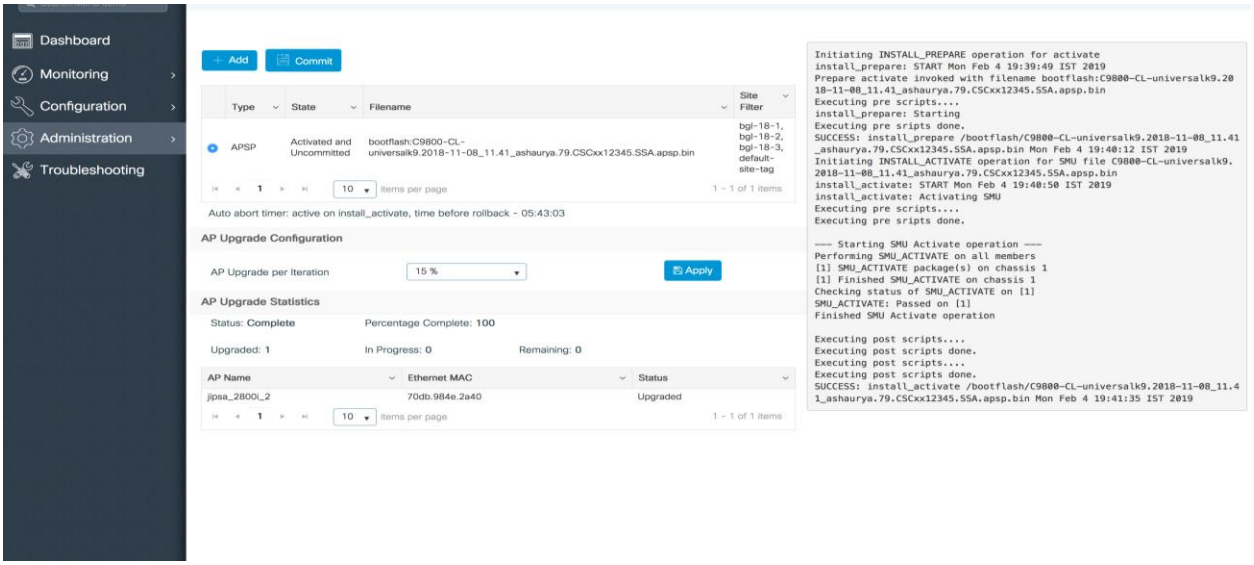


tatistics until all APs

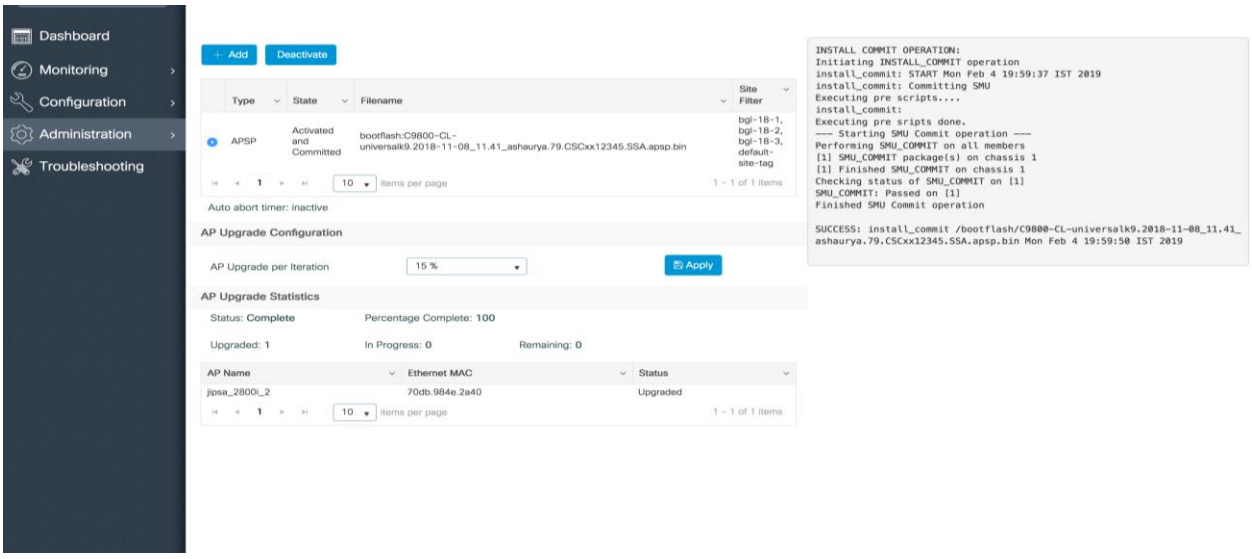


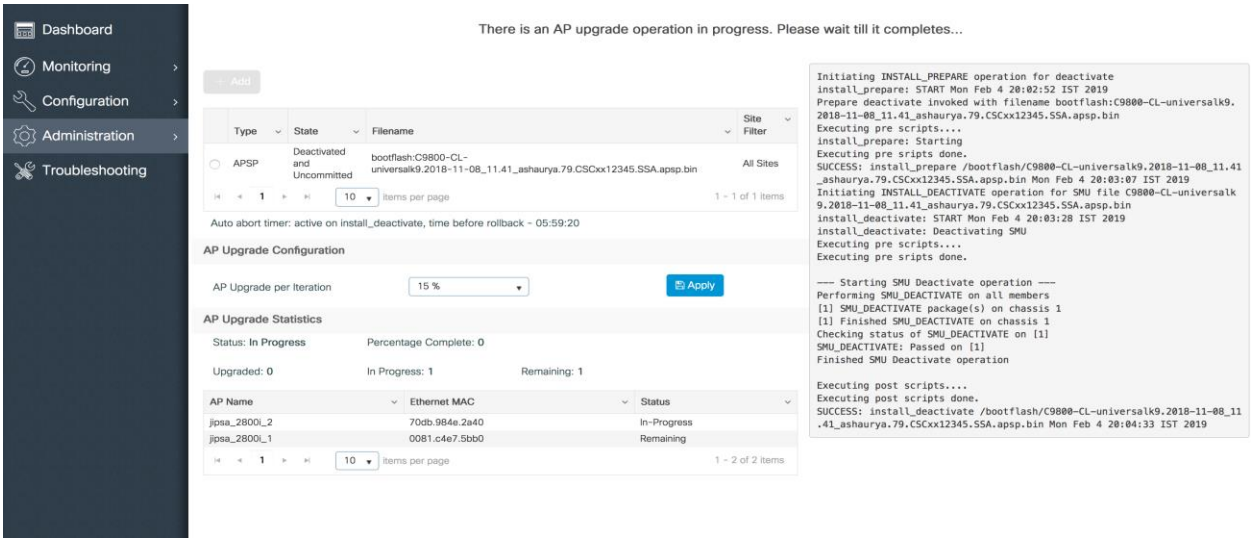
Site-filters can be edited or cleared in order to propagate the AP service pack to other/all sites using the “All Sites” option as shown below

Step 3: Commit the AP Service pack by clicking on the Commit button



The AP Service pack can be deactivated using the “Deactivate” option which will deactivate the AP Service pack from all sites where it was installed.





The CLI workflow of successful APSP activation is shown below

- Install add
- Install prepare activate
- Install activate
- Install commit

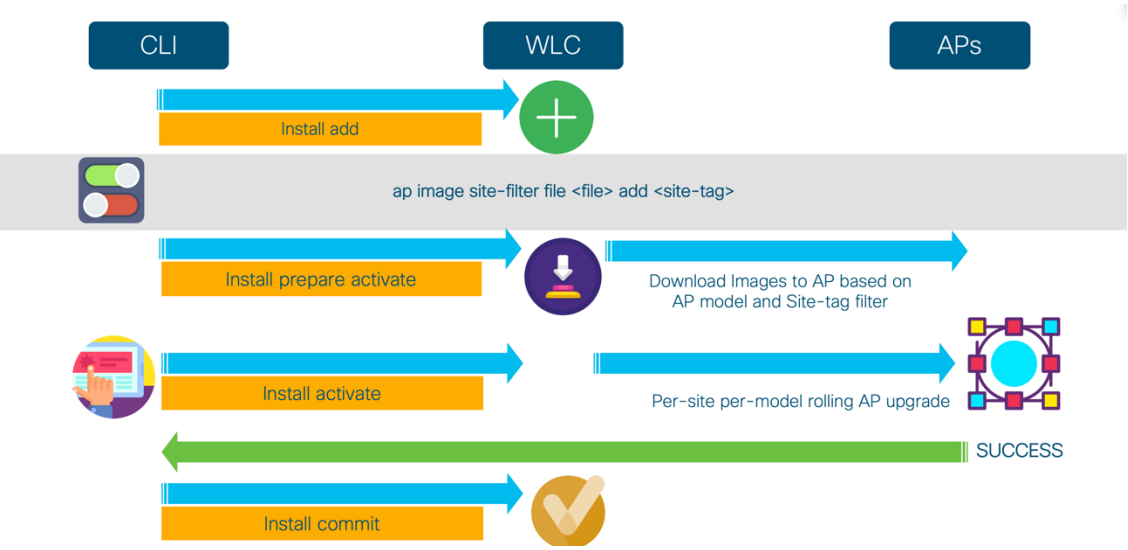


Figure 3: APSP Successful installation workflow

In case of a failure, the APSP can be rolled back and the system will return to the last stable checkpoint

- Install add
- Install prepare activate
- Install activate
- Install rollback

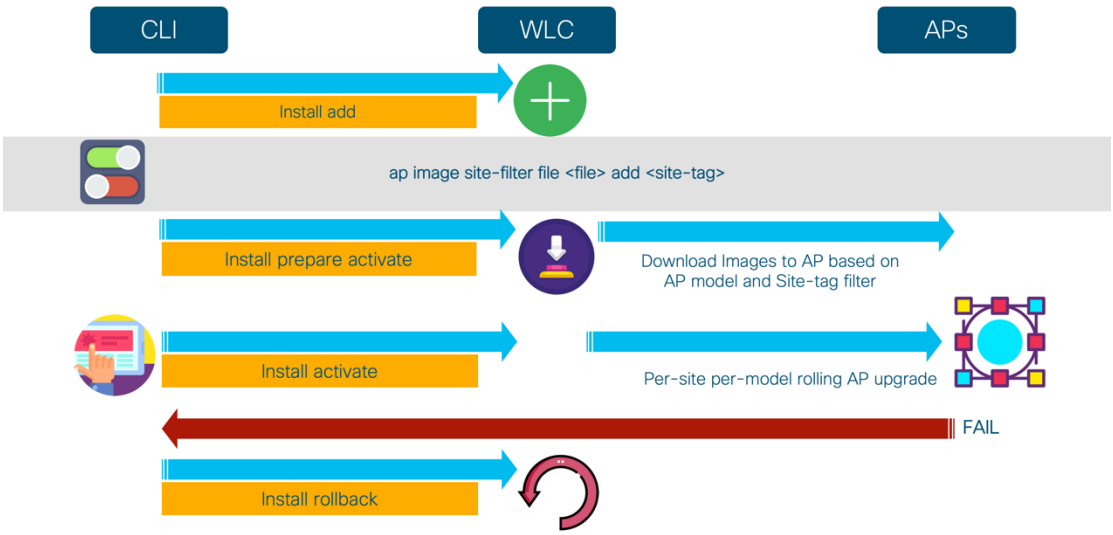


Figure 4: APSP Installation Failure workflow

Upgrade and Downgrade Scenarios with APSP

In an upgrade scenario if upgrading to the next major or minor release, the fix should be integrated into the next release. The controller can be upgraded using the N+1 rolling upgrade process described in the next section of this document. The target image is loaded on the N+1 controller, the APs are rolled over, the primary is upgraded and the APs are rolled back. There is no service disruption since N+1 rolling AP upgrade is used.

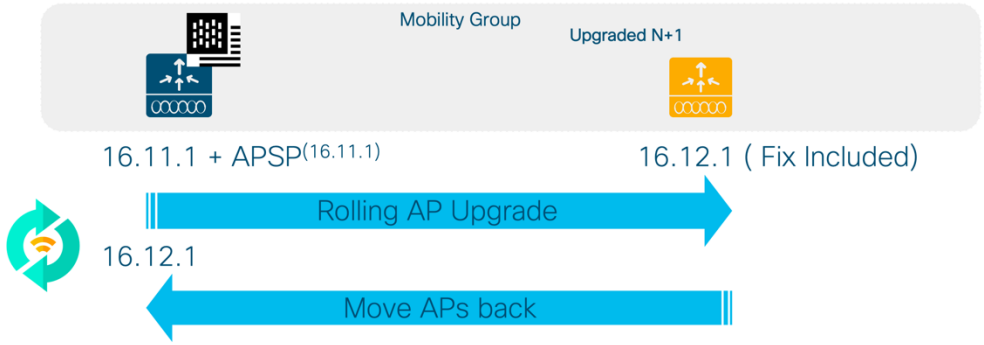


Figure 5: Upgrade Scenario with APSP

In the case of downgrade, the N+1 controller is installed with the target downgrade image and the corresponding APSP. The APs are rolled over back to the N+1 controller, the primary is reloaded with the downgraded image and the corresponding APSP. Any new APs that join part of the site where the fix is applicable will have the APSP pushed to them at the time of AP join, if the AP is of same AP model as the installed APSP

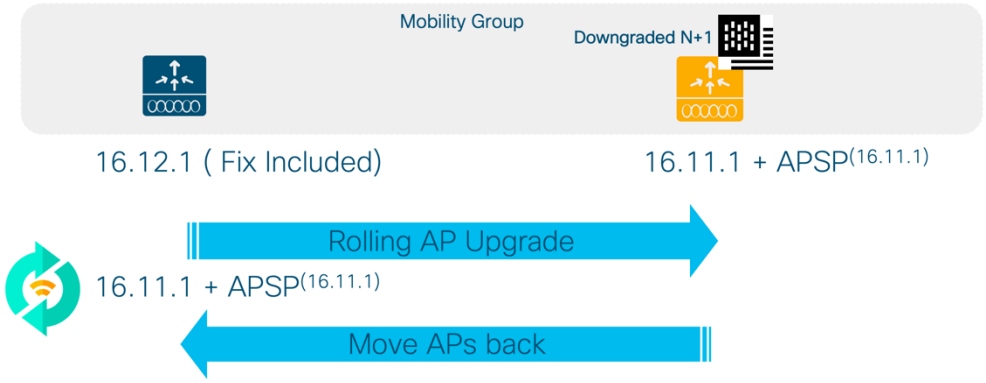


Figure 6: Downgrade Scenario with APSP

CLI Reference

Activating an AP Service Pack

1. install add file <file>

Populates pre-download directory, persistent

2. ap image site-filter file <file> add <site-tag>

Can be entered multiple times to set up a multi-site filter

3. ap image site-filter file <file> remove <site-tag>

Can be entered to remove site filter

4. install activate prepare file <file>

Does pre-download to some or all sites based on filter

5. install activate file <file>

Does rolling AP upgrade to some or all sites based on filter

6. install commit

Adding a Site Filter

ap image site-filter file <file> add <site-tag>

Above can be entered multiple times to set up a multi-site filter

ap image site-filter file <file> apply

Does pre-download and rolling AP upgrade to added sites based on filter

Removing a Site Filter

1. ap image site-filter file <file> clear

Does pre-download and rolling AP upgrade to all sites where it's not active

Deactivating AP service Pack

1. install deactivate prepare file <file>

Informs wireless about imminent deactivate, wireless does pre-download to affected APs

2. install deactivate file <file>

Does rolling AP upgrade based on which AP models were present in above file

Please note that during deactivate if no APs in any sites are currently running the AP images from the APSP being deactivated then above steps will be no-op in terms of pre-

download and rolling AP upgrade. Only internal tables will be updated to remove that APSP.

Rollback an AP Service Pack

1. install rollback to rollback_id1 prepare

Informs wireless about imminent rollback, wireless does pre-download to affected APs

2. install rollback to rollback_id1

Does rolling AP upgrade for all sites based on which AP models are affected

Please note that if there were some AP models on base image or a point before rollback point then they will not be affected by rollback.

Abort Activation of AP Service Pack

1. install abort prepare

Informs wireless about imminent abort, wireless does pre-download if needed

2. install abort

If needed, does the abort by resetting APs in rolling fashion

It is important to note here that if “install abort prepare” must be followed up with an “install abort”.
If the “install abort prepare” is called after “install deactivate file bootflash:abcd” was called but rolling AP upgrade is still running then the rolling AP upgrade is stopped and we mark the last upgrade report as “abort prepped”. We know that the APs which completed the upgrade will need to be moved back to their last image when “install abort” trigger comes so these APs are asked to pre-download the necessary image. The remaining APs are asked to pre-download if their active image is not in the flash. This completes the “install abort prepare” handling. When “install abort” trigger is received, we go through the report which was marked “abort prepped” and reset all the APs which were upgraded in there so that the abort is complete. Post this, the user is free to enter any commands.

Show commands to verify functionality

show ap image site summary

```
c9800# show ap image site summary

Image name: apsp1.bin
Site Tag          Prepared          Activated          Committed
```

```
---------------------------------------------------------------------------------------------------------------
BGL18           yes             ongoing         no
BGL17           yes             ongoing         no
c9800#
```

show ap image file <APSP file name>

```
c9800# show ap image file apsp1.bin

Image version: 16.10.1.25
AP image type: ap1g4, ap3g3
c9800#
```

The following show CLIs can be used to see rolling ap upgrade progress:

show ap upgrade summary

show ap upgrade detailed <report-name>

N+1 Rolling AP Image Upgrade

Zero downtime network upgrade is a challenge for Wireless Networks. The reason is that these networks are made up of a set of interlocked devices, WLCs and a set of APs, which all need to be up to keep the network operational.

The advent of Rolling AP Upgrade opens up new possibilities for upgrading the controller code in a network without bringing the network down using an N+1 controller. This can effectively achieve a Zero Downtime network upgrade in a N+1 deployment.

The idea here is to upgrade access points in a wireless network in a staggered manner, using the same Rolling AP update infrastructure as described earlier in this document, such that an appropriate number of APs are always up and running in the network and providing RF coverage to clients

The solution for N+1 Network Upgrade using Rolling AP Upgrade takes the form of three primitives which the administrator can use to achieve Zero Downtime Upgrade. Orchestration and visualization capabilities are available on the wireless controller and will be available in DNAC as well. The workflow for this solution is described in the following steps:

1. The target version is installed on WLC2 and WLC2 is added to the same mobility group as WLC1. The target image is downloaded to WLC1 and associated APs are pre-downloaded with the image.

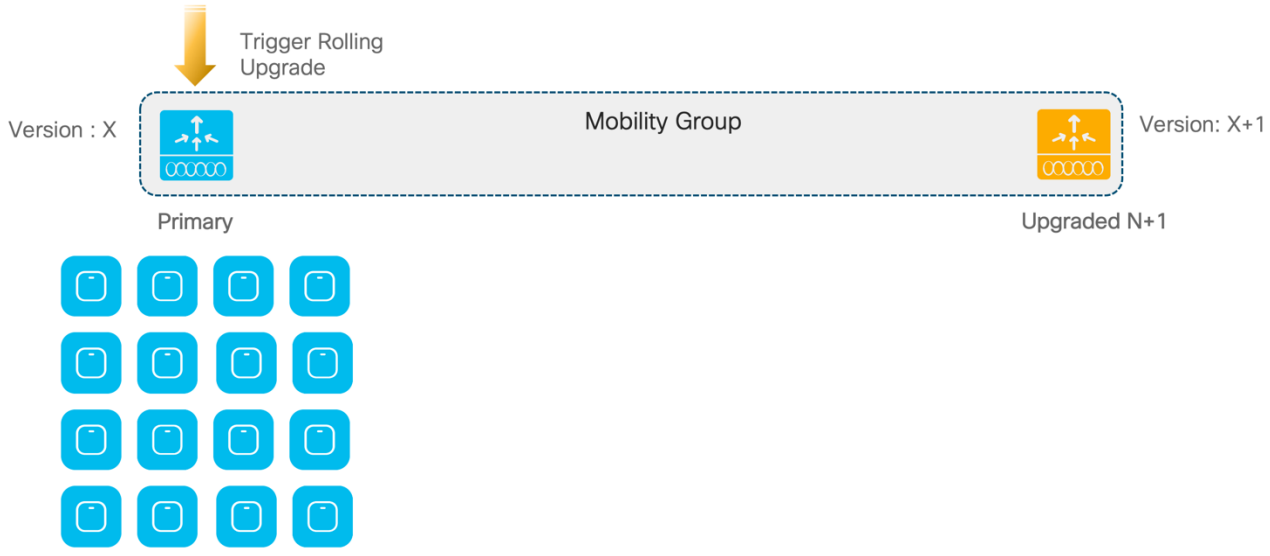


Figure 7: Image download to primary WLC and AP pre-download to APs

The user then triggers the exec command below using which all APs from a WLC (WLC1) can be moved to a mobility member (WLC2) whose identity (Hostname and Wireless Management IP) is provided by the user.

ap image upgrade destination <WLC Name> <WLC IP>

This CLI will move APs to the specified destination WLC with a swap and reset command. It is assumed that destination WLC is on the same version as APs backup image.

The device auto-selects the candidate APs to be upgraded in each iteration based on the percentage of APs to be selected for upgrade in each iteration (5%, 15% or 25% with the default as 15%) and RRM AP neighbor information.

- For 25%, expected number of iterations is ~ 5 and expected to take about an hour.
- For 15%, expected number of iterations is ~ 12 and expected to take about 2 hours.
- For 5%, expected number of iterations is ~ 22 and expected to take about 4 hours.

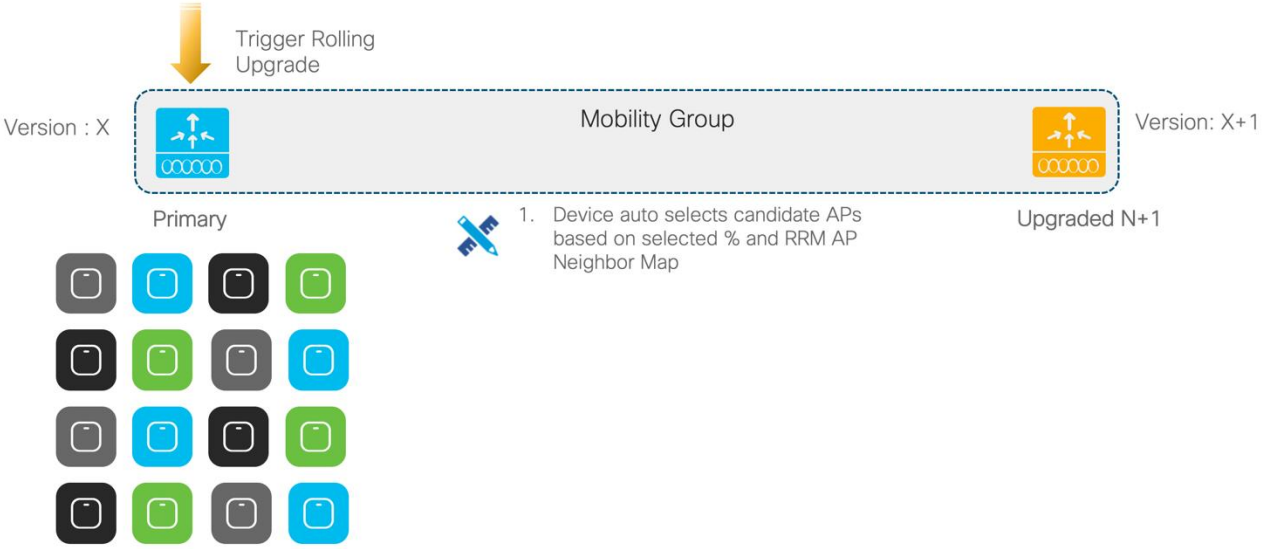


Figure 8: RRM Based Candidate AP Selection

On this exec command, the APs will be given a command that its primary WLC is WLC2. After this, APs will be asked to swap and reset themselves using Rolling AP Upgrade. As this AP upgrade happens, WLC2 will be informed about each iteration so that upgrade report for this activity is available on both WLC1 and WLC2. The upgrade report created contains an indication that this is an AP move report and notes the source and destination

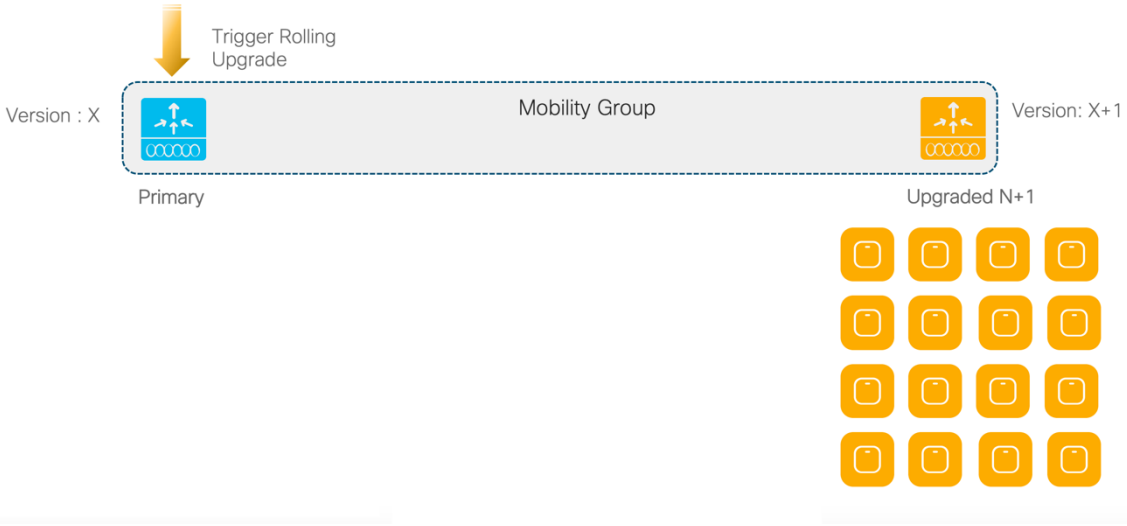


Figure 9: Staggered rolling AP Upgrade to N+1 WLC

2. Once this move is complete, the image downloaded beforehand on WLC1 is activated with a reload to bring it up with the new version.

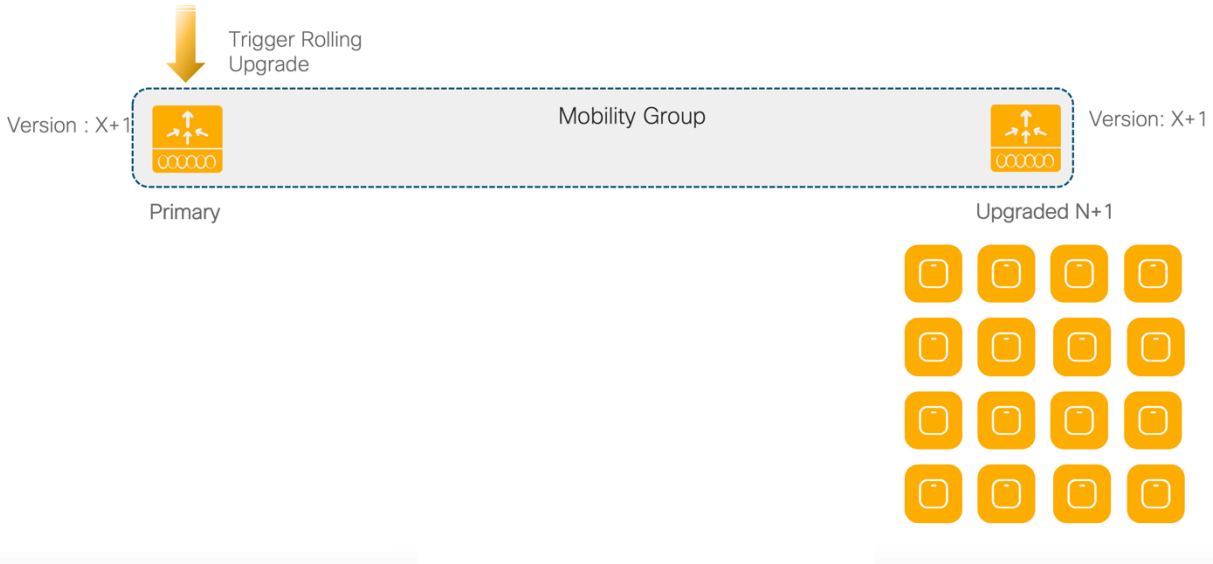


Figure 10: Reload on Primary WLC and upgrade to target image

3. After reload of WLC1 once the mobility tunnel comes up, WLC2 will run rolling AP upgrade to move the APs using the same algorithm back to WLC1.

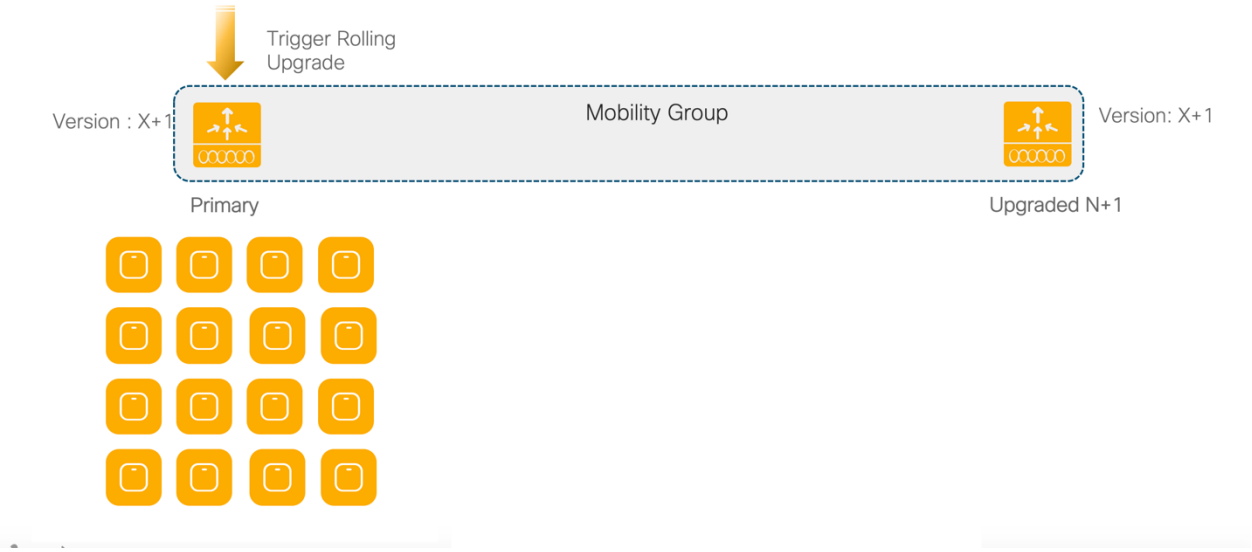


Figure 11: Optional fallback to Primary WLC

Here we provide a command using which APs contained in an upgrade report can be moved to another WLC without any version change. The command takes in a destination WLC identity (Hostname and Wireless Management IP) and optionally a report name.

On this CLI trigger, if an upgrade report name was provided, we go to that report and go through the APs iteration by iteration. For each iteration we change the primary WLC to the provided WLC for APs in this iteration. If no upgrade report file name was provided, we run rolling AP Upgrade candidate selection and come up with iterations afresh.

ap image move destination <WLC Name> <WLC IP> [<Upgrade report Name>]

This CLI will move APs to the specified destination WLC without a swap and reset command. It is assumed that destination WLC is on the same version as current WLC.

Starting Release 16.11, a single command to set the variables for the Rolling AP upgrade. User needs to trigger "install activate" command manually to activate and reload WLC1 with the new image. After reload, APs will move back to WLC1 automatically

ap image upgrade destination <WLC Name> <WLC IP> [fallback]

The following show commands are provided to support this feature

show ap upgrade summary

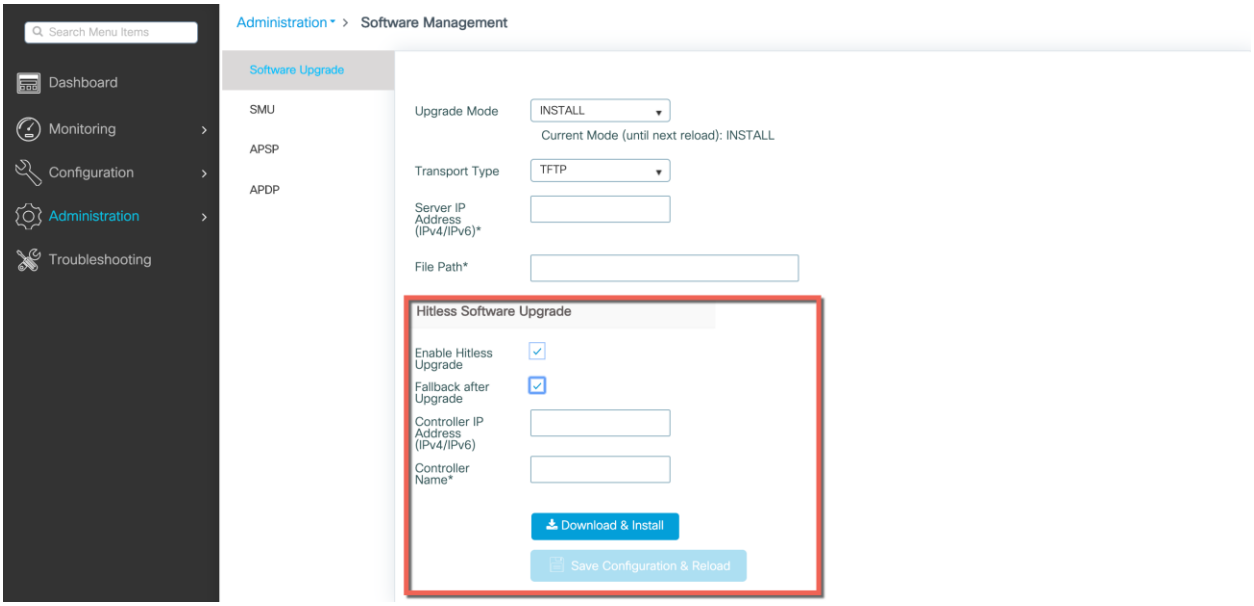
For displaying all the upgrade report names.

show ap upgrade name <report-name>

For displaying AP upgrade information based on upgrade report name

N+1 Rolling Image Upgrade using WebUI

- Download the target image to the primary controller using one of the supported transport options such as HTTP, TFTP or SFTP.
- Select the “Enable Hitess Upgrade” checkbox
- Select “Fallback after Upgrade” option if APs need to be automatically moved back to the primary controller after upgrade (This step is optional).
- Enter the IP address and name of the N+1 wireless controller.



New AP model support using AP Device Pack

Traditionally, if new AP Hardware models are introduced, those are shipped with corresponding WLC Major software version. So, the customer has to wait for a corresponding CCO version relative to the new AP model and has to upgrade their entire network. In release 16.11, the wireless controller provides a solution to introduce new AP models into customer networks using an AP Device pack (APDP) without the customer having to move to new WLC CCO version. This allows faster deployment of the APs, confining impact within the already validated image and effectively zero downtime for the controller since it is a hot patch that does not require a reload on the controller.

Since this feature is platform independent functionality, it is supported on all wireless platforms and all AP deployment modes (Flex, Local and Fabric).

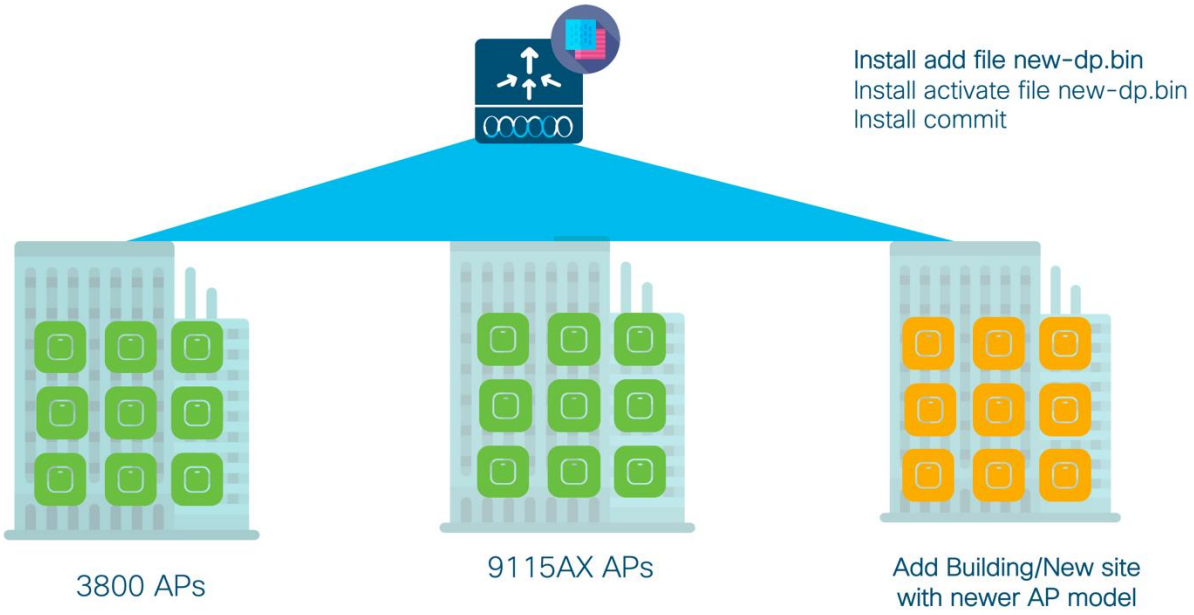


Figure 12: APDP enables new AP models to join existing WLC code

Note: the new AP module will support only those capabilities that are supported in the base CCO version of the controller.

The workflow to install and activate an AP Device Pack is as follows:

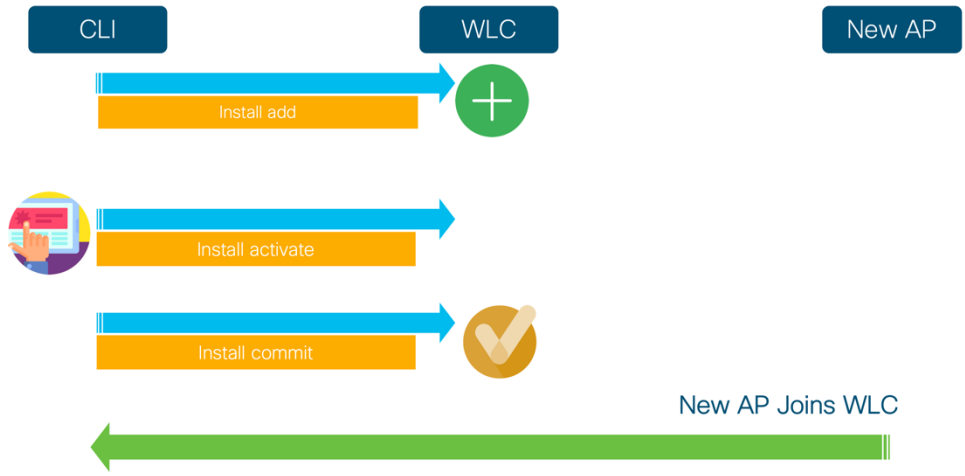


Figure 13: APDP installation workflow

1. Add the APDP file using Install add of APDP
2. Install activate of APDP
3. At this point, WLC should be in a position to accept new connection from new AP model.
4. Install commit will make this new AP software persistent

- Installation of APDP information is synced to Standby-WLC in HA system.
- Bug fixes will be provided for the new AP introduced with the installation of an AP service pack
- AP Device PACK will be supported up to previous maintenance release. E.g. if new AP model is introduced in 16.14.1, APDP will be supported in 16.12.x and 16.13.x

Upgrade and Downgrade Scenarios with APDP

If the upgrade is to the next major release, the support for the AP would be likely integrated into it. In the case of a maintenance release upgrade, an AP DP pack corresponding to the image would be available and needs to be loaded on the N+1 controller. The APs are rolled over using the rolling AP upgrade process, the primary controller then needs to be reloaded with the new image and corresponding APDP and the APs are rolled back. No disruption for existing or new model APs since the device pack is always available.

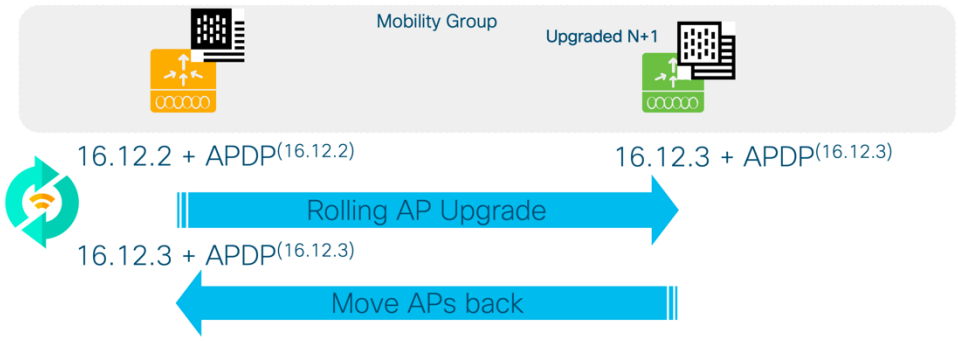


Figure 14: Upgrade Scenario with APDP

In the case of downgrade, the N+1 controller is installed with the target downgrade image and the corresponding APDP. The APs are rolled over back to the N+1 controller, the primary is reloaded with the downgraded image and the corresponding APDP.

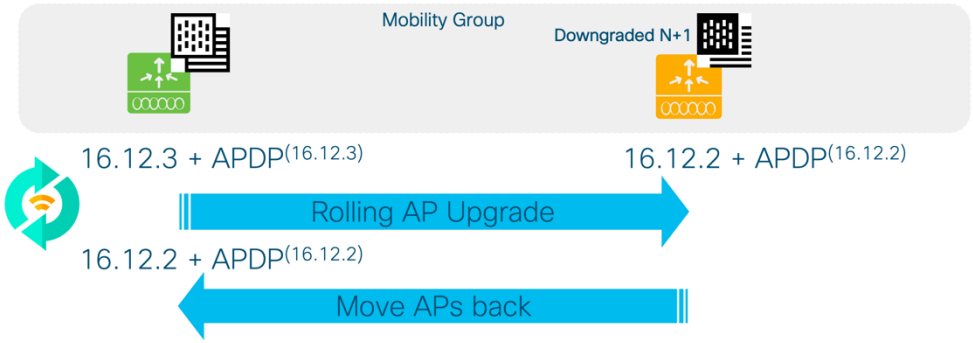
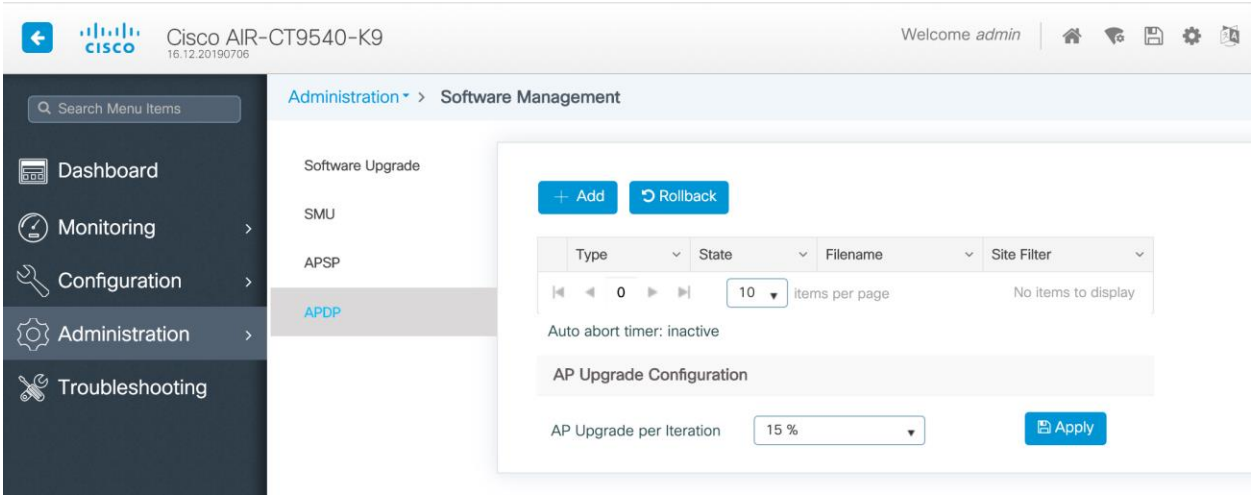


Figure 15: Downgrade Scenario with APDP

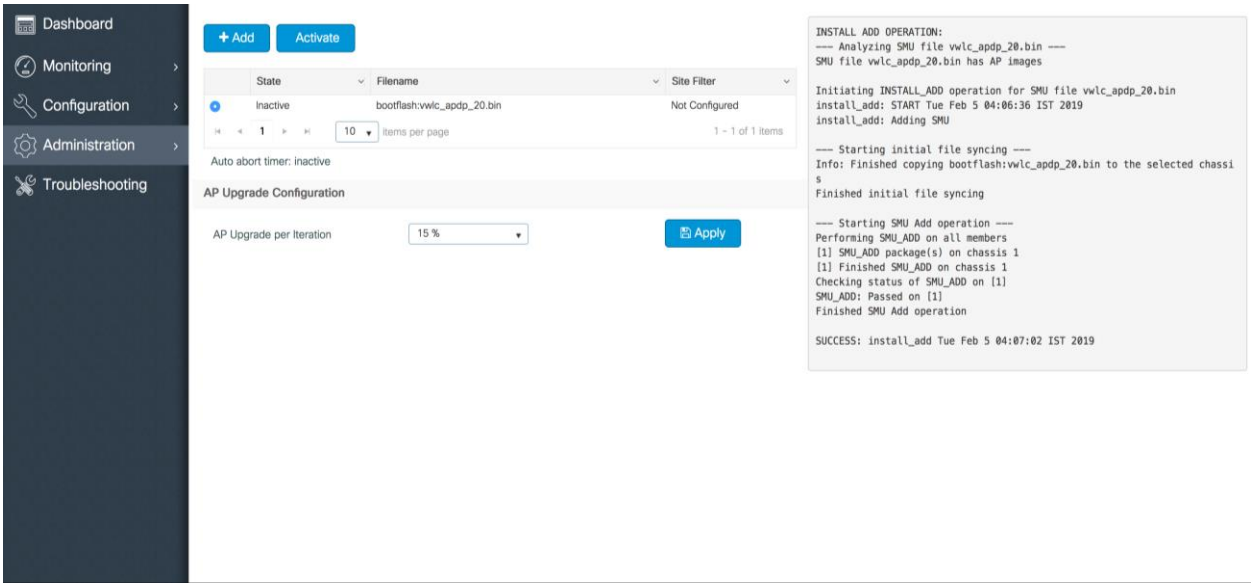
Web UI Configuration

Step 1: AP Device pack is downloaded and added to the controller Under Administration > Software Management > APDP

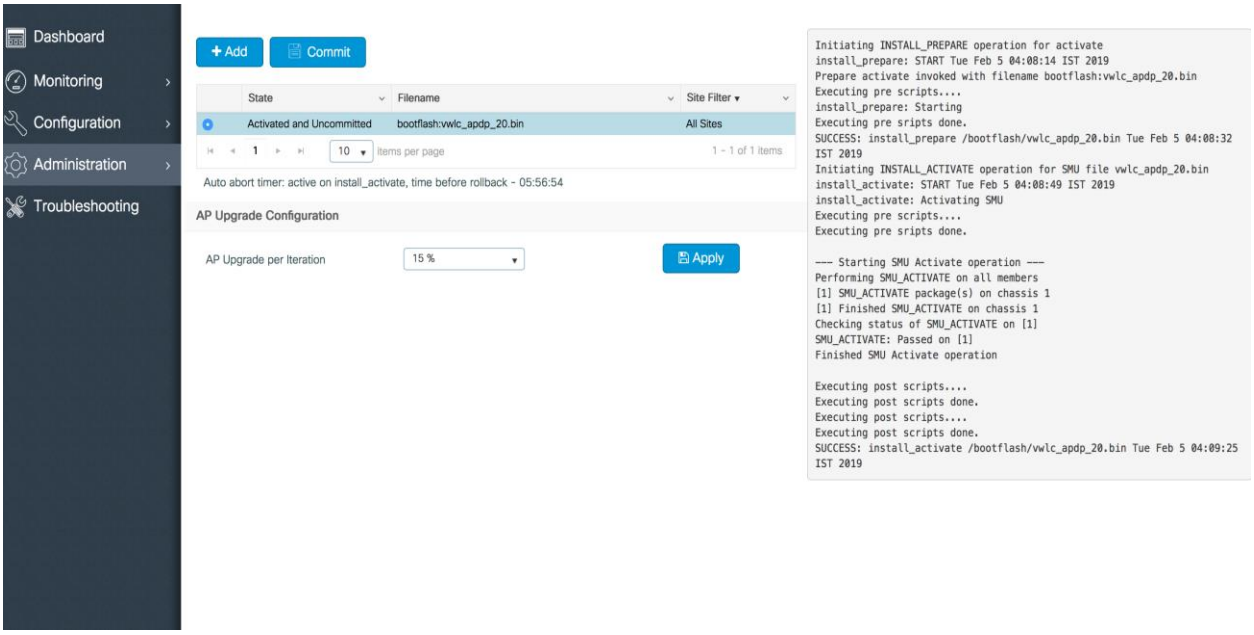


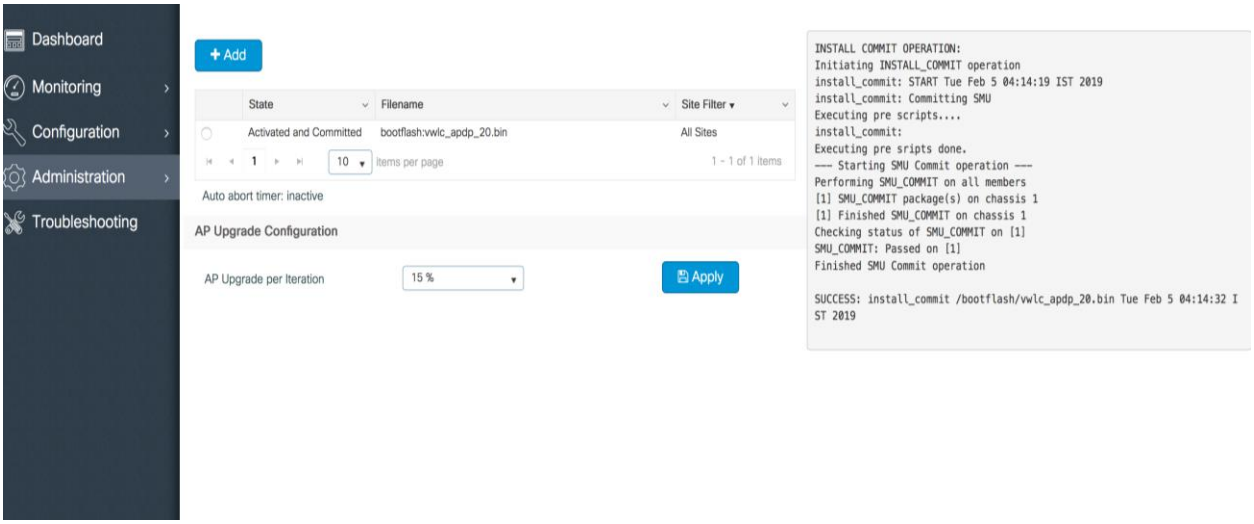
Note: If the new AP shares code with existing APs, the controller will roll out the new image to existing APs using Rolling AP upgrade. Hence, the AP Upgrade per Iteration option is shown on this page.

Step 2: Click on **Activate** to install AP Device pack on the controller as a hot patch



Step 3: Monitor logs on the right hand panel to verify that APDP has been successfully installed. Once APs join the WLC, the APDP can be committed by click on the **Commit** button.





CLI Reference

The following install commands are provided to support this feature

- install add file < tftp/ftp/flash/disk:*.bin>
- install activate file <disk:*.bin>
- install commit

In case, is user decides to deactivate already installed APDP, the following install CLIs can be used:

- install deactivate file <disk:*.bin>
- install commit

In-Service Software Upgrade (ISSU)

In Service Software Upgrade (ISSU) is a procedure to accomplish a wireless controller upgrade while packet forwarding continues uninterrupted which increases the network availability and reduces downtime. ISSU provides a complete image upgrade from one image to another without network downtime. All AP and client sessions are maintained and the procedure is carried out natively from the controller without the need for an external orchestrator or additional licenses.
The prerequisites ISSU are that the base image has to be IOS XE 17.3 and higher , the controllers have to be in SSO ready state and the boot mode has to be set to INSTALL.

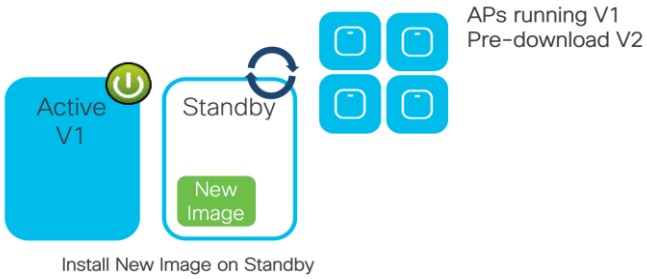
Note: ISSU is available on 17.1 and 17.2 in Beta mode.

Platforms Supported for ISSU:

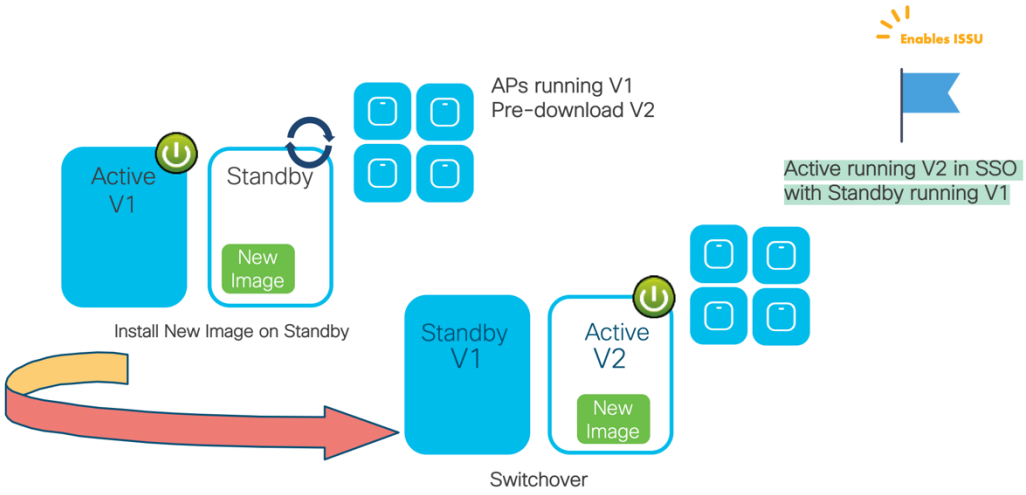
Cisco Catalyst Wireless 9800-L, 9800-40, 9800-80, 9800-CL for private cloud.

ISSU workflow

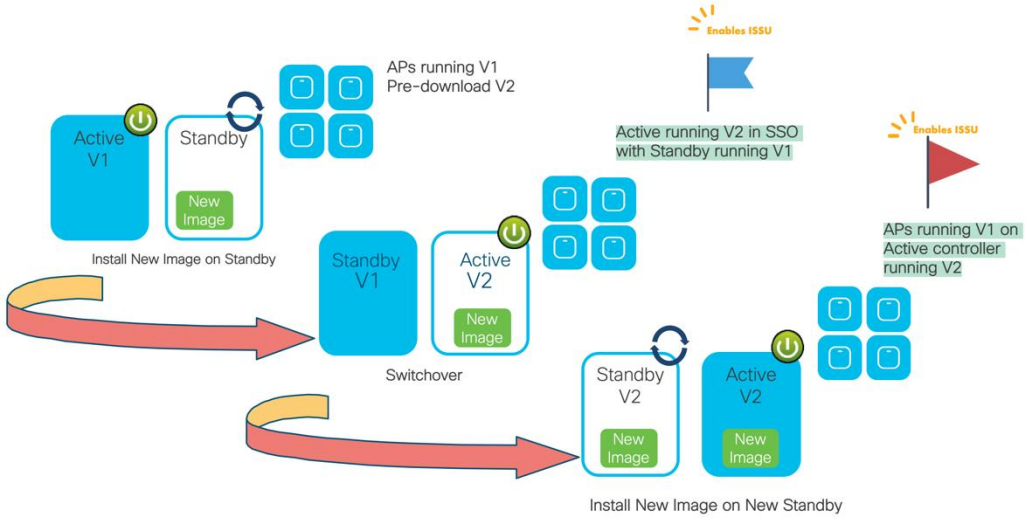
The ISSU workflow utilises the base SSO capability that has been enhanced in a couple of key ways to enable in-service software upgrades.
In the first step, the target image (v2) is downloaded to the primary controller running v1 and expanded into packages. The image is then synced to the Hot standby controller over the RP connection. AP images corresponding to v2 image are also pre-downloaded to APs running v1. The standby controller is reloaded and loads with image v2.



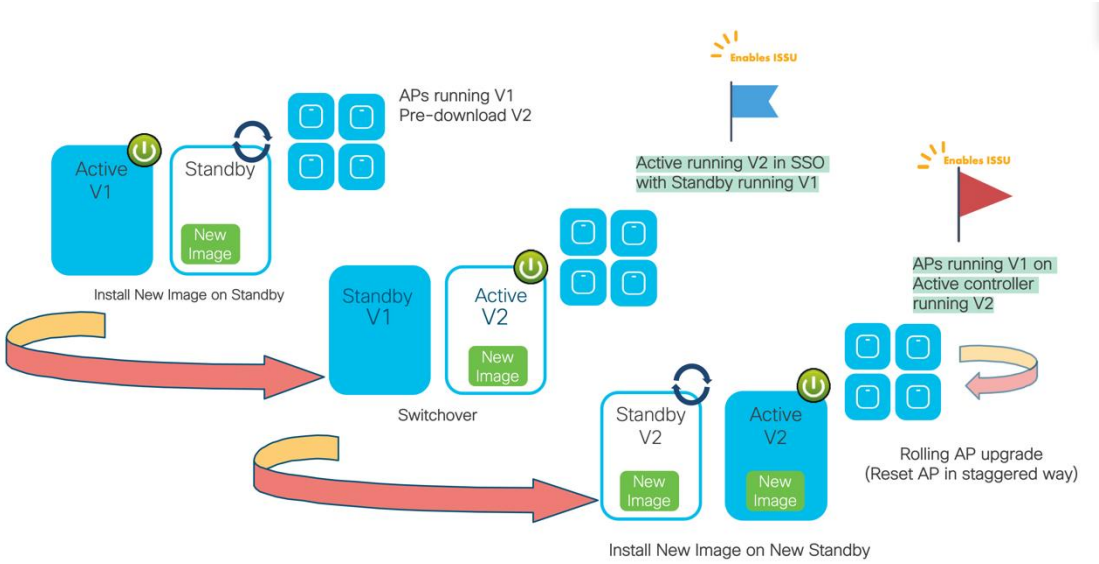
Active running V1 and standby running V2 form an SSO pair. This was earlier not possible and is one of the enhancements that makes ISSU possible. Once the HA pair is ready, a switchover is executed.



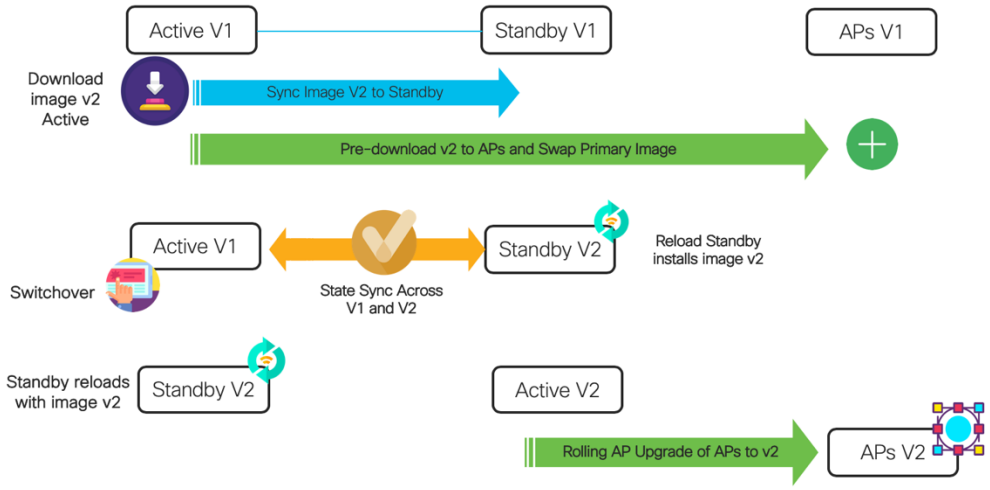
Standby running V2 now becomes the active and the old active reloads thus coming up as V2. At this point both controllers are on V2 and APs on V1.



APs are asked to switch images after the activate step and are upgraded in a rolling AP upgrade fashion. To minimize the data outage during ISSU the rolling upgrade of AP is done, so that clients can connect to the neighboring AP. The activate trigger does the AP reset in a staggered manner with a best-effort attempt to retain connectivity for clients. When APs rejoin, they rejoin with v2 AP images. The final step is commit which makes the changes permanent. Commit can be executed once SSO pair re-forms or after the rolling AP upgrade process completes



The overall workflow can also be depicted as follows :

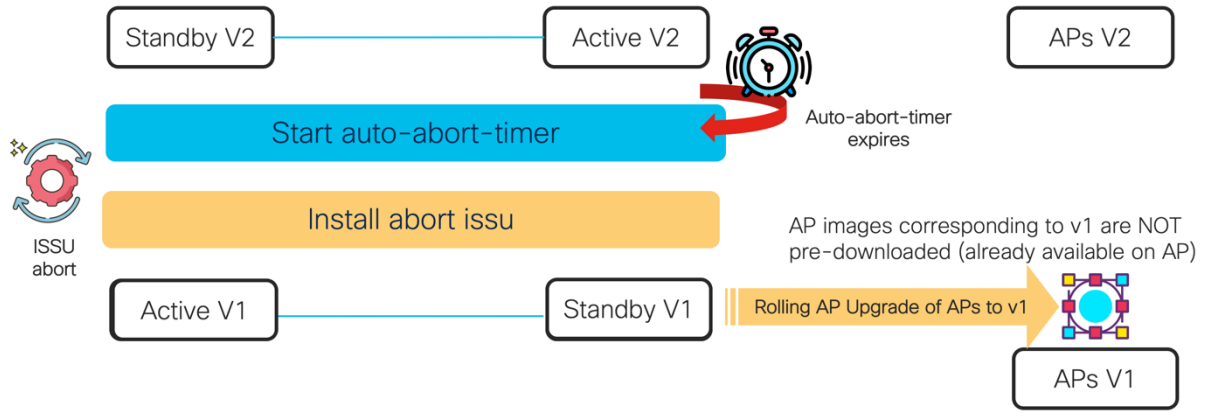


ISSU Success workflow

The commit operation makes the ISSU changes permanent. It can be issued any time after the controller is upgraded successfully even without waiting for the rolling APs upgrade procedure to complete. As part of install commit, a rollback point is created. The rollback point can be used to roll back to a specific rolled back point.

ISSU Abort with Auto Abort timer

If commit is not executed, an auto abort timer will be started and continuously run counting down from a default of 6 hours after which the controllers will be aborted in ISSU fashion back to image V1

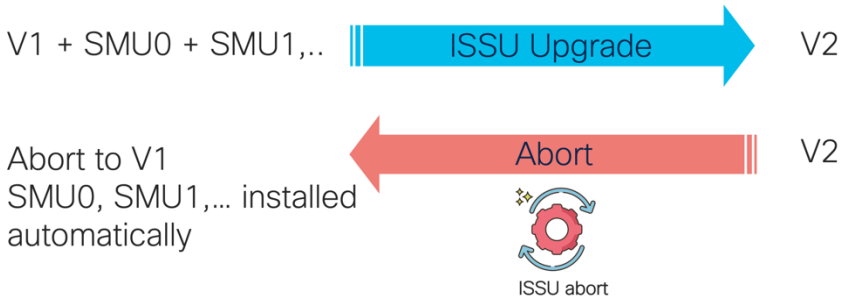


The “install auto-abort-timer stop” can be used to stop the auto-abort timer stop or install activate issu auto-abort-timer <30-1200> can be used to overwrite the default

The user can also manually initiate an abort using the command “install abort issu” which will abort both controllers to v1 in an ISSU manner.

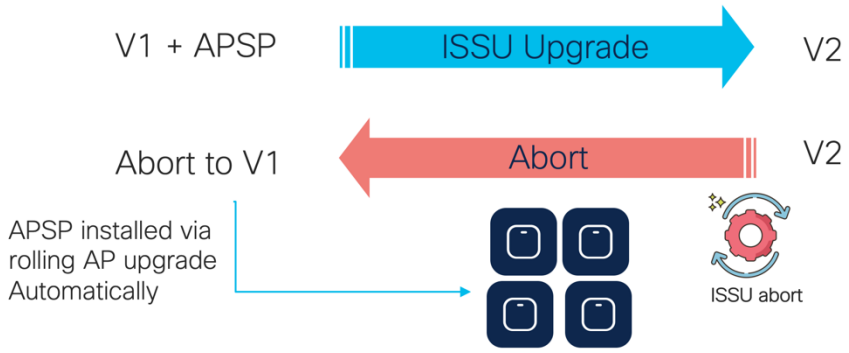
ISSU Abort with SMU installed

When a SMU is present with V1 and an abort operation is performed, the system will move to V1 and the SMUs will be automatically applied.
Initially system is running with v1 + SMU0 + SMU1 and so on. During ISSU from (v1+SMU0+ SMU1….) to v2 if ISSU operation is aborted, system will move to v1 first, at the same time AP upgrade operation will also be aborted. SMU0, SMU1 and other SMUs are available on the box and will be patched to v1 automatically.



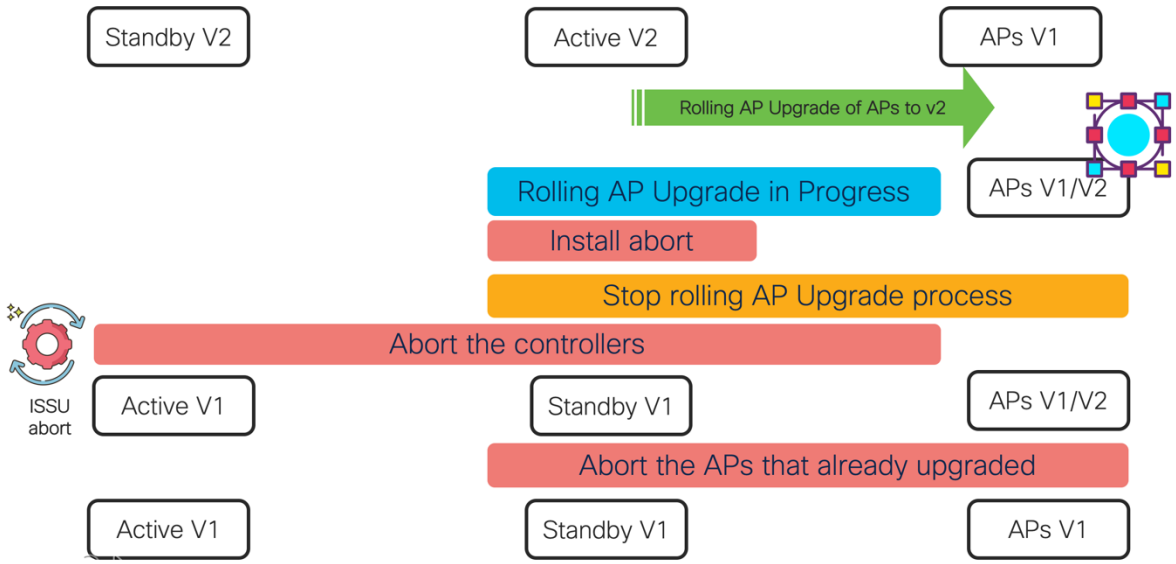
ISSU Abort with APSP installed

Similarly, when an APSP was present with V1 and an abort operation is performed, the system will move to v1 and the APSP automatically rolled out to the APs. When APSP is also present, after Abort, controller will fall back to the previously running image. Once controller is up, depending on the availability of APSP image at the AP, WLC will download APSP to the APs automatically.



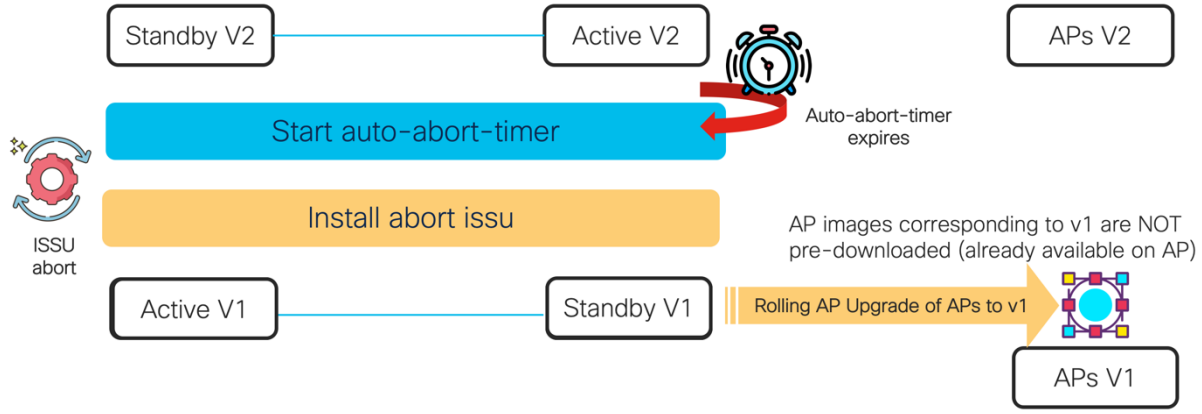
ISSU Abort when rolling AP upgrade is in progress

Aborting a system while the rolling AP upgrade is in process first stops the rolling AP upgrade process. An abort is then performed in ISSU fashion on the controllers bringing them back to the prior version V1. Once that is complete, the APs are rolled back in a staggered manner to image V1.



ISSU Rollback

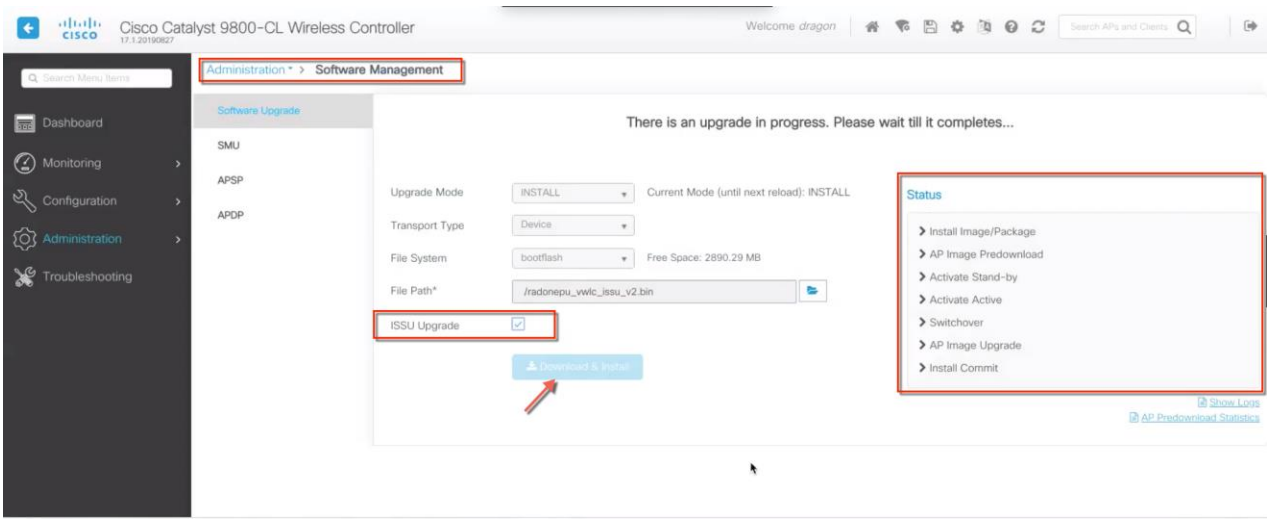
A rollback option is supported if the user chooses to rollback to a previous snap-shot or rollback point on the controller. Rollback is always in non-ISSU fashion and APs are reloaded in one-shot.



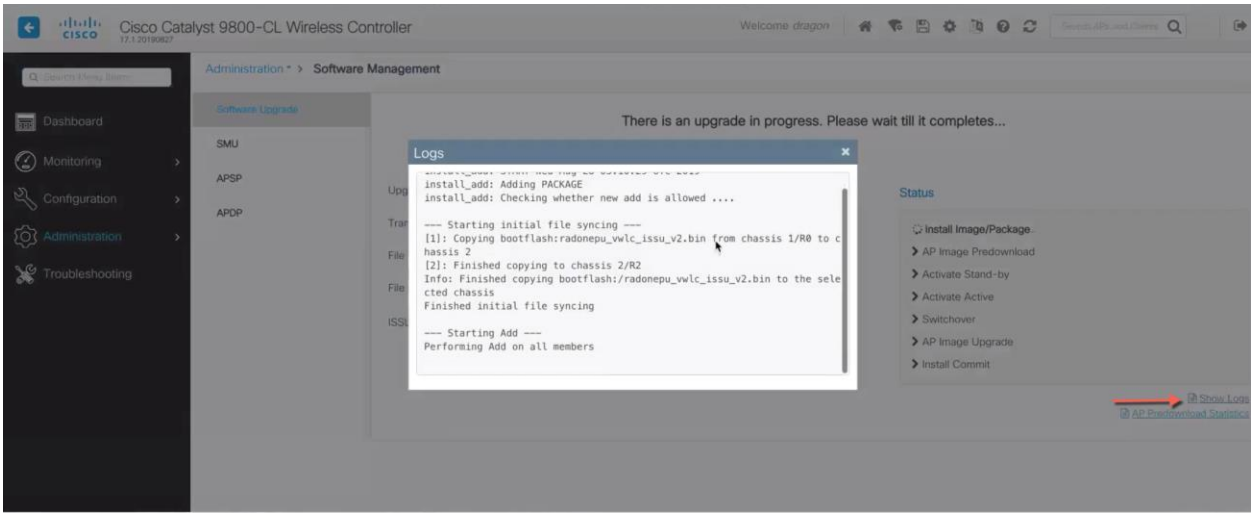
ISSU WebUI Workflow

Using the controller UI, ISSU is an automated workflow.

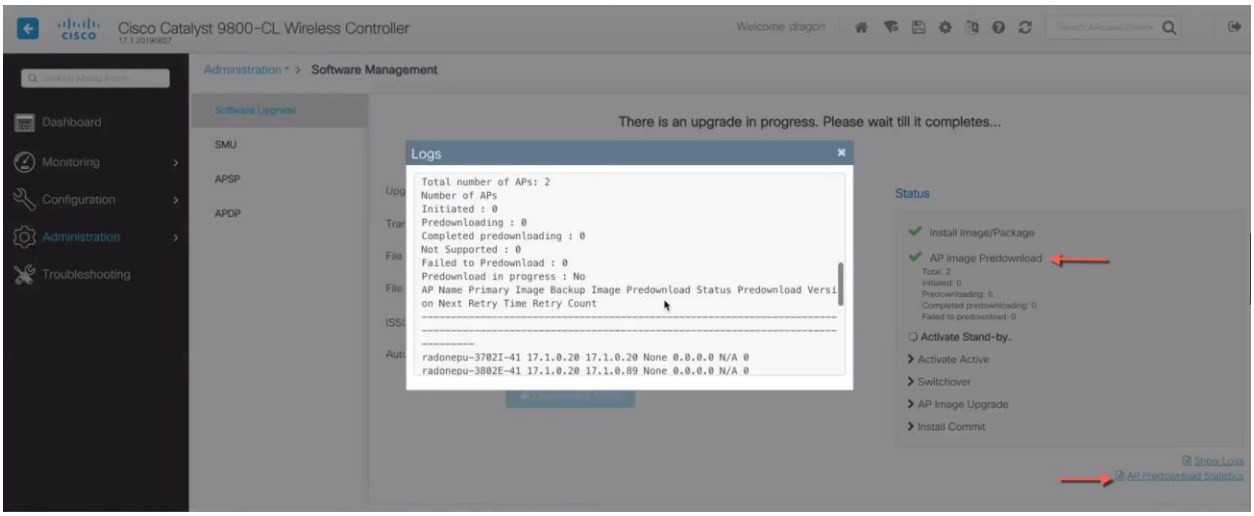
1. Select the target (V2) image to upgrade to, enable the **ISSU upgrade** checkbox and click on Download & Install . This kick starts the ISSU process and the status can be monitored in the panel on the right hand side.
   Note: The upgrade mode has to be set to INSTALL for ISSU to go through.



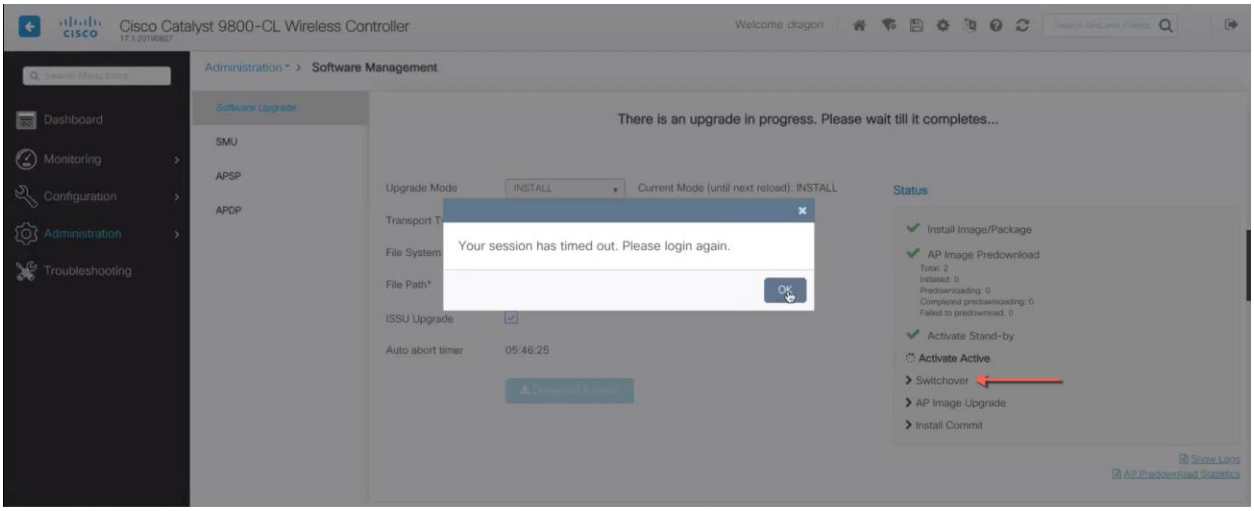
2. Monitor the logs to see the progress of the ISSU process. The first step involves adding the image on the Active and standby controller.



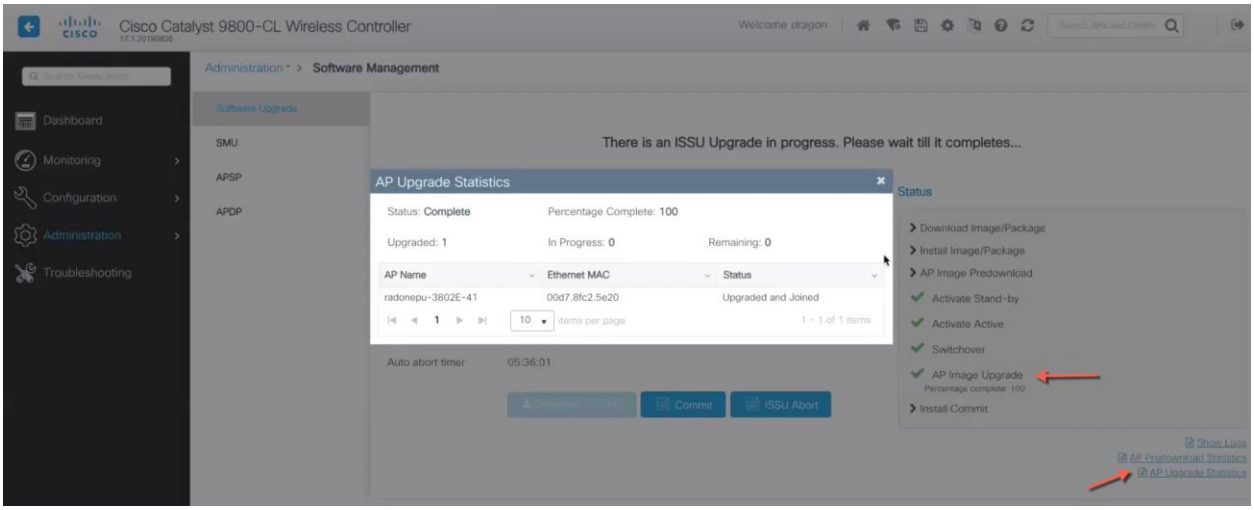
3. Once the image is synced to the standby, the V2 image is pre-downloaded to the access points and the logs can be monitored by clicking on "AP Predownload Statistics" as shown below. This shows the total number of AP, APs initiated or pre-download, APs undergoing pre-download currently and APs that completed pre-download. In addition to also shows any APs that failed to pre-download.



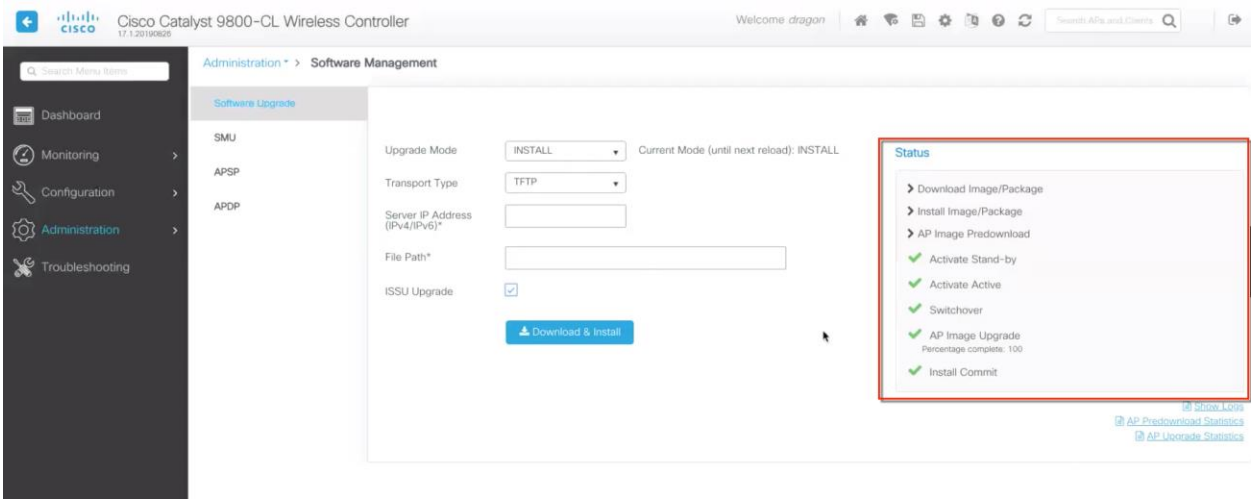
4. After AP predownload completes, the standby reloads with V2 and re-forms the HA SSO pair with active running V1. Once the standby is back to Hot-standby mode, a switchover takes place. Controller running V2 is now the active controller and the old active reloads with V2 and comes up as Hot standby. At this point, the webUI will show the following message. Log back into the controller.



5. The target image V2 is now installed on the APs using Rolling AP upgrade mechanism and the logs can be monitored by clicking on “AP Upgrade Statistics”. This should the percentage of APs completed and the AP name, MAC and status of each AP.



6. After all the steps are complete, execute Commit. This makes the changes permanent. If at any time before the completion, the process needs to be aborted, the ISSU Abort button can be used to abort the process. This reverts to image V1 in an ISSU fashion.



ISSU CLI workflow

Workflow Sequence	Description
install add file <file>	Image downloaded from CCO to the bootflash will be 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	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.
Install rollback	Rollback to previous commit point after the current ISSU operation is completed.

Show install profile	To see previous rollback points
Install abort issu	Abort the ISSU process before a commit is issued. This is done in ISSU fashion
install auto-abort-timer stop	To stop the auto-abort timer
install activate issu auto-abort-timer <30-1200>	To modify the auto-abort timer

ISSU Release support

Supported:

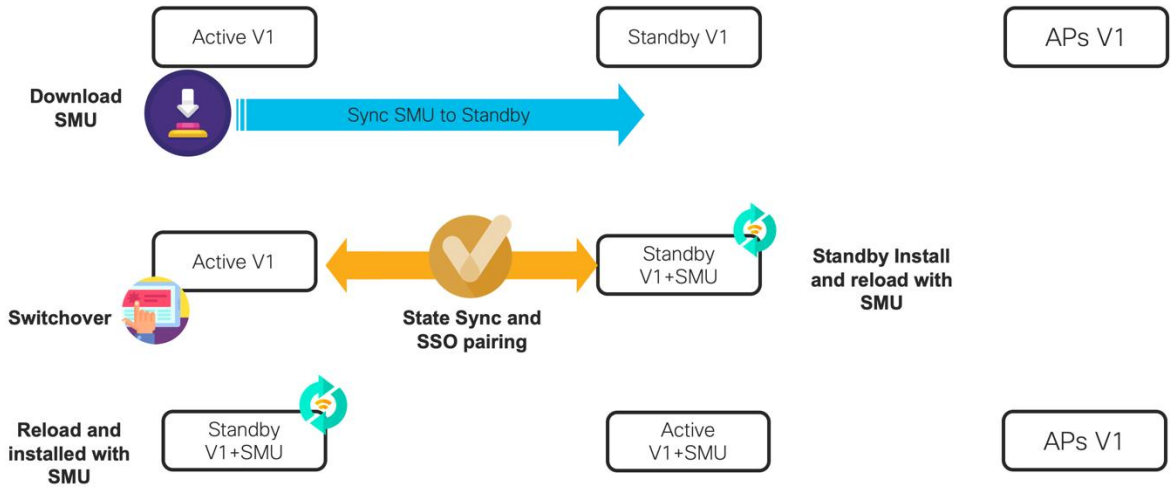
- ISSU works within a major Release train (16.x, 17.x, 18.x etc.) for 3 years
- Within a major release train (ex. 16.x or 17.x) – ISSU supported from Any Rebuild of EM1/EM2/EM3 to Any rebuild of EM1/EM2/EM3
    - Example: EM1 – 16.9.x to EM2 – 16.12.x
    - Example: EM1 – 17.3.x to EM2 – 17.6.x, EM3 – 17.9.x
    - Example: EM1 – 16.9.2 to EM1 – 16.9.3, 16.9.4, 16.9.x
    - Example: EM1 – 16.12.1 to EM1 – 16.12.2, 16.12.3, 16.12.x
- Wireless ISSU Recommendation:
    - **From Any EM /EM Rebuild** release on CCO to **Current EM Recommended** release on CCO
    - ISSU Best Practice guideline: For SM to EM or EM to SM, use N+1 image upgrade mechanism.

Unsupported:

- ISSU Downgrades
- Within a major release train (ex. 16.x) - SM to EM or EM to SM is not supported
    - For example 16.10.x or 16.11.x to 16.12.x is not supported
- No ISSU support on Engineering Special image or .s (or similar) images that are not posted on CCO publicly
- No ISSU support when switching to major release version
    - For example 16.x.x to 17.x.x or 17.x.x to 18.x.x is not supported

Cold Patch SMU activation using ISSU Workflows

The ISSU mechanism is also used to install a cold patch SMU with the SMU first being installed on the standby. After standby reloads and forms the HA pair, a switchover is initiated and the new standby reloads with SMU installed. The APs continue to be on the original image since the SMU only impacts the controller code. No pre-download is required.



Summary

Solutions described in this document enable controller and AP update and upgrade operations on the network without causing a service disruption on the wireless network. The Cisco Catalyst 9800 controller provides high availability across the lifecycle of deployment; from unplanned network events to planned upgrades in the network.

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Copyright