Software Maintenance Upgrade

Software maintenance upgrade

A software maintenance upgrade (SMU) is a software package that

- is installed on a system to provide a patch or a security fix resolution to a released image, and
- is on a per component basis and is specific to the corresponding platform.

Feature history

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature history for Software maintenance upgrade

Feature Name	Release Information	Feature Description
Software maintenance upgrade	Cisco IOS XE Gibraltar 16.11.1b	This feature provides network administrators with targeted, platform-specific patches and security fixes for released images, applicable either on a per-component basis or for the entire corresponding platform.

A SMU offers significant benefits over classic Cisco IOS software. It lets you address network issues promptly and reduces required testing time and scope. The Cisco IOS XE platform validates SMU compatibility internally and prevents installation of non-compatible SMUs.

All SMUs are also integrated into subsequent Cisco IOS XE software maintenance releases. A SMU is an independent and self-sufficient package without prerequisites or dependencies. You can choose which SMUs to install or uninstall in any order.

Note SMUs are supported only on Extended Maintenance releases and throughout the full lifecycle of the underlying software release.

Note Activate the file using the **install add file** command only from the filesystems of the active device. If you use a file from the standby or member filesystems, the **install add file** command fails.

Note When the SMU file is deleted and the device is rebooted, the device may display an error message such as:

```
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
    FAILED: Improper State./bootflash/<previously-installed-smu-filename>.smu.bin not
present. Please restore file for stability.
Checking status of SMU_ADD on [1/R0]
SMU_ADD: Passed on []. Failed on [1/R0]
Finished SMU Add operation
FAILED: add_activate_commit /bootflash/<tobeinstalled-wlc-smu-filename>.smu.bin Wed Aug 02
 08:30:18 UTC 2023.
```

This error occurs because the previous SMU file was not properly removed from the controller. As a result, you may not be able to install new SMU or APSP files.

Use the **install remove file** command to remove previous instances of APSP or SMU files from the bootflash.

You can use SMU infrastructure to meet these requirements in wireless contexts:

- Controller SMU: Controller bug fixes or Cisco Product Security Incident Response information (PSIRT).
- APSP: APSP is used for AP bug fixes, PSIRTs, or minor features that do not require controller changes.
- APDP: APDP supports new AP models without introducing new hardware or software capabilities.

Note The **show ap image** command displays cumulative statistics for AP images in the controller. Clear the statistics using the **clear ap predownload statistics** command, before using the **show ap image** command, to ensure correct data is displayed.

SMU Workflow

Begin the SMU process by requesting approval from the SMU committee. Contact customer support to raise an SMU request. During the release, the SMU package is posted on the Cisco Software Download page. You can then download and install it.

Warning: Commit changes within six hours of activation or deactivation to avoid rollback

Always run the **install commit** command within 6 hours after executing either **install activate** or **install deactivate** .

If you do not commit changes within this window

- the system automatically reverts to the previous commit state
- this reversion can lead to service interruption, especially over low-bandwidth links where image transfers may not complete in time, and
- remote deployments with slow transfer rates are particularly vulnerable.

To reduce these risks

- run **install commit** after activation or deactivation
- monitor image transfer progress proactively, and
- plan for available bandwidth and duration at remote sites.

SMU Package

An SMU package contains the metadata and the fix for the reported issue that prompted the request.

SMU Reload

The SMU type describes the effect on a system after you install a SMU. SMUs can be non-traffic-affecting, or they can require a device restart, reload, or switchover.

A controller cold patch requires a cold reload of the system during activation. A cold reload means completely restarting the operating system.

This process affects traffic during two phases:

- the reload of the wireless controller, and
- the time needed for all APs to rejoin the controller, receive the new image, and upgrade to the new SMU patch. This reload ensures that all processes use the correct libraries and files installed as part of the SMU.

The reload ensures all processes use the correct libraries and files installed as part of the SMU.

With controller hot patching, a SMU is effective immediately after activation, without rebooting the system. After you commit the SMU, activation changes persist across reloads. Hot patching SMU packages contain metadata listing processes to restart for activation. During activation, each process is restarted one by one until activation completes.

Install a SMU (GUI)

Add and activate a SMU image on your device using the GUI.

Procedure

Step 1 Choose **Administration** > **Software Management** and click the **Software Maintenance Upgrade** tab.

Step 2 Click **Add** to add a SMU image.

Step 3 From the **Transport Type** drop-down list, select the transfer type, TFTP, SFTP, FTP, Device, or Desktop (HTTP) to transfer the software image to your device.

a) If you choose **TFTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **File path** and select a **File System** from the drop-down list. For example, if the SMU file is at the root of the TFTP server you can enter **`/C9800-universalk9_wlc.17.03.02a.CSCvw55275.SPA.smu.bin`** in the **File path** field.
b) If you choose **SFTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and select a **File System** from the drop-down list.
c) If you choose **FTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and select a **File System** from the drop-down list.
d) If you choose **Device** as the **Transport Type**, enter the **File path** and select a **File System** from the drop-down list. This is possible when the software is already present on the device due to an earlier download and activation, followed by a subsequent deactivation.

Note
Depending on your device, available file systems may vary. On physical controllers, store files on bootflash or hard disk. On virtual controllers, use bootflash.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, select a **File System** from the drop-down list and click **Select File** to navigate to the **Source File Path**.

Step 4 Enter the **File Name** and click **Add File**.

When you complete this step, the maintenance update package is copied to the device, platform and image versions are checked for compatibility, and the SMU package is added for all members. After adding a SMU, you see a message indicating success and letting you know the SMU can be activated. The message displays the name of the package (SMU) that is available for activation. It lists the SMU details: Name, Version, State (active or inactive), Type (reload, restart, or non-reload), and other compatibility details. If the SMU type is 'reload,' any operation (activate, deactivate, or rollback) causes the device to reload. The 'restart' type involves only a process restart. If it is 'non-reload,' no process changes occur.

Step 5 Select the SMU and click **Activate** to activate it on the system, install the package, and update the package status details.

Step 6 Select the SMU and click **Commit** to make these activation changes persistent across reloads.

The Commit operation creates commit points, which are similar to snapshots. Use commit points to decide which changes to activate or roll back if you have a problem with the SMU. You can commit after activation when the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.

Install SMU (CLI)

Update device software with a SMU using CLI.

Procedure

Step 1 Copy the maintenance update package from a remote location to the device, and perform a compatibility check for the platform and image versions.

Example:

```
Device# install add file bootflash filename
```

This command runs base compatibility checks on a file to verify that the SMU package is supported on the platform. The command also adds an entry to the package or SMU.sta file. This entry allows you to monitor and maintain the package's status.

Step 2 Run compatibility checks, install the package and update the package status details.

Example:

```
Device# install activate file bootflash filename
```

For a restartable package, the command triggers the appropriate post-install scripts to restart the necessary processes. For non-restartable packages it triggers a reload.

Step 3 Commit the activation changes to be persistent across reloads.

Example:

```
Device# install commit
```

You can perform the commit after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload; however, it is no longer active after the second reload.

Step 4 Display the image version on the device.

Example:

```
Device# show version
```

Step 5 Display information about the active package.

Example:

```
Device# show install summary
```

The output of this command varies according to the install commands that are configured.

Roll back an image (GUI)

Return the software image on the system to a previous stable state using the GUI.

Procedure

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

Step 2 Go to **SMU**, **APSP** or **APDP**.

Step 3 Click **Rollback**.

Step 4 In the **Rollback to** drop-down list, select **Base**, **Committed** or **Rollback Point**.

Step 5 Click **Add File**.

Roll back SMU (CLI)

Return the device to a previous software state by rolling back a SMU using CLI.

Procedure

Step 1 Return the device to the previous installation state.

Example:

```
Device(config)# install rollback to {base | committed | id | committed} committed ID id
1234
```

After the rollback, a reload is required.

Step 2 Commit the activation changes to be persistent across reloads.

Example:

```
Device# install commit
```

Deactivate SMU (CLI)

Deactivate an active SMU package on a network device using CLI.

Procedure

Step 1 Deactivate an active package, update the package status, and trigger a process to restart or reload.

Example:

```
Device# install deactivate file bootflash filename
```

Step 2 Commit the activation changes to be persistent across reloads.

Example:

```
Device# install commit
```

Configuration examples for SMU

This example shows the SMU configuration after the system completes the install add for the SMU.

```
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    16.8.1.0.39751

--------------------------------------------------------------------
```

```
Auto abort timer: inactive
----------------------------------------------------------------------
```

AP device package

An AP device package is a software module that

- allows new AP hardware models to connect to an existing wireless network
- uses the SMU infrastructure to deliver new AP images, and
- enables flexible, out-of-cycle support for new AP devices independent of controller major releases.

AP Service Pack (APSP)

When a new AP hardware model is introduced, it is shipped along with the corresponding controller related major software version. Subsequently, you must wait for the release of a controller version compatible with the new AP model before upgrading the entire network.

Starting with version 16.11.1, you can add new AP models to your wireless network using the SMU infrastructure, without upgrading the controller version. This solution is called AP Device Package (APDP).

SMU Process or Workflow

The SMU process builds APDP to detect code changes and to build APDP. You can add new AP image files to APDP and include AP images as needed.

The workflow is as follows:

- install add
- install activate
- install commit

For more details, see Managing AP Device Package.

Warning: Commit changes within six hours of activation or deactivation

To complete the APSP or APDP activation or deactivation process, always run the **install commit** command within six hours after executing either **install activate** or **install deactivate**.

If you do not commit the changes within this window, the system reverts to the previous commit state automatically. Potential issues include:

- service interruptions, especially over low bandwidth links where image transfers may not finish in time, and
- rollbacks for remote deployments with slow transfer rates.

To avoid these risks:

- Run the **install commit** command immediately after activation or deactivation.
- Monitor the progress of the image transfer.
- Plan to have sufficient time available at remote sites.

SMU package and AP image changes

SMU Package

A SMU package is a software metadata unit that:

- contains AP model and capability-related details
- is updated when new AP models are introduced, and
- is bundled into APDP packages for deployment.

AP Image Changes

When new AP models are introduced, there may or may not be corresponding new AP images. AP images are mapped to the AP model families. If a new AP model belongs to an existing AP model family there will be existing AP image entries (for example: ap3g3 and ap1g5). If an AP model belongs to either ap3g3 or ap1g5, update the respective image file with the correct AP image location. The corresponding metadata file is also updated with the new AP model capability information.

If a new AP model belongs to a new AP model family and requires a new image file, create a new image entry file in the correct AP image location. The corresponding metadata file is updated with the new AP model capability information.

Note The APDP images must not be renamed to prevent impact on its functionality.

Install AP device package (GUI)

Add or upgrade AP device support in your network.

Procedure

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

Step 2 Click **AP Device Package (APDP)** tab.

Step 3 Click **Add**.

Step 4 From the **Transport Type** drop-down list, select the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **File path** and select a **File System** from the drop-down list.

b) If you choose **SFTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and select a **File System** from the drop-down list.

c) If you choose **FTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and select a **File System** from the drop-down list.

d) If you choose **Device** as the **Transport Type**, enter the **File path** and select a **File System** from the drop-down list.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, select a **File System** from the drop-down list.

f) Click **Select File** to navigate to the **Source File Path**.

Step 5 Enter the **File Name** and click **Add File**.

Step 6 From the **AP Upgrade Configuration** section, select the percentage of APs to be included from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Install AP device package (CLI)

Install and activate new AP device packages on the controller using the CLI.

Procedure

Step 1 Extract AP images from APDP and place them in SMU or APDP specific mount location.

Example:

```
Device# install add file bootflash filename
```

Note
Here, the SMU does not trigger the Wireless module.

Step 2 Add the AP software in APDP to the existing current active AP image list.

Example:

```
Device# install activate file bootflash filename
```

Also, update the capability information for the new AP models in the controller .

Note
Even if the new AP module supports new hardware capabilities, the controller recognizes only the capability information that its base version supports.

At this point, the controller accepts the new connection from the new AP model. The new AP model then joins the controller .

Step 3 Commit the new AP software to be persistent across reloads.

Example:

```
Device# install commit
```

The commit occurs after activation when the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload but becomes inactive after the second reload.

Step 4 (Optional) Deactivate an active APDP, update the package status, and trigger a process to restart or reload.

Example:

```
Device# install deactivate file bootflash filename
```

Step 5 Display the image version on the device.

Example:

```
Device# show version
```

Verify APDP on the Controller

To verify the status of APDP packages on the controller , use the command:

```
Device# show install summary

[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted, C - Activated & Committed, D -
Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
APDP  I    bootflash:apdp_CSCvp12345.bin
IMG   C    17.1.0.0
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Note The output of this command varies based on the packages, and the package states that are installed.

Per site or per AP model service pack (APSP)

A per-site and per-AP model service pack is a software maintenance update option that:

- allows administrators to roll out critical AP updates and bug fixes to subsets of APs at specific sites or to particular AP models
- enables staggered and targeted deployment (by site or AP model) to control the propagation of a SMU in your network by selecting which sites to include in the SMU activation.
- integrates with FlexConnect, local mode, and SD-Access wireless deployments for selective upgrade strategies.

Ensure all sites are at the same SMU level before you roll out a new SMU to selected sites or start an image upgrade on the system.

With per-AP model SMU, you can update only specific AP models. The software downloads and activates only on chosen AP models at a site. If you include specific model images in a SMU, you must also include software images for those models in future updates.

Note After you apply the AP site filter for a per-site SMU upgrade, install a new image only if you have applied the site filter to all sites, or if you have removed the current site filter.

Restrictions and workflow

Restrictions for configuring APs to a primary controller

- If you do not configure APs to a primary controller, all APs receive the same discovery response from controllers with and without the APSP image. This causes your APs to switch repeatedly between two controllers.

Workflow of AP SMU Upgrade

- To upgrade the AP SMU, run a query to check for ongoing activities, such as AP image predownload or AP rolling upgrade.
- Identify the sites for SMU installation and set up a site filter.
- Trigger the SMU predownload for the sites in the site filter.
- Activate the SMU after the predownload completes.
- Commit the update.

Note After you set up the site filter, you can add more sites. To make your changes take effect, apply the filter again using the **ap image site-filter file** *file-name* **apply** command. If you clear the site filter, updates are applied to all remaining sites. When you deactivate or roll back images, the action is applied to all sites, not just filtered sites.

Rolling AP upgrade

A rolling AP upgrade is an upgrade method that

- updates APs in staggered batches such that some APs are always up in the network and provide seamless coverage to clients while the other APs are selected to be upgraded, and
- requires preloading the image in advance to ensure that all APs scheduled for upgrade have the new version.

Note The time needed to complete a rolling AP upgrade depends on several factors: the number of APs, the percentage in each iteration, the controller type, and the controller's connectivity to the APs. To estimate the upgrade time, multiply the number of iterations by the maximum iteration time. Each iteration can take up to 5 minutes multiplied by the expected number of iterations. You can view the end time by checking the **iteration expiry time** field in the **show ap upgrade** command.

Rolling AP upgrade process

Summary

Rolling AP upgrade is done on a per controller basis. The number of APs to be upgraded at a given time is a percentage of the total number of APs connected to the controller. The percentage is capped at a user configured value. The default percentage is 15. Upgrade all non-client APs before upgrading any client APs.

The key components involved in the process are:

- Controller
- APs
- Clients

Workflow

The process involves the following stages:

1. Candidate AP set selection:

   In this stage, a set of AP candidates is selected based on neighboring AP information. For example, if you identify an AP for upgrade, a certain number (N) of its neighbors are excluded from candidate selection. The N values are generated in the following manner:

   If the user configurable capped percentage is 25%, then N=6 (Expected number of iterations =5)

   If the user configurable capped percentage is 15%, then N=12 (Expected number of iterations=12)

   If the user configurable capped percentage is 5%, then N=24 (Expected number of iterations =22)

   If you cannot select candidates using neighboring AP information, select candidates from indirect neighbors. If this still fails, the AP is upgraded without failure.

Note If you have more candidate APs than the configured percentage allows, remove the extra candidates to maintain the percentage cap.

2. Client steering:

   Move clients connected to candidate APs to other APs before rebooting the candidate APs. Each AP sends a request to its associated clients, providing a list of the best available APs (excluding candidate APs). The system marks candidate APs as unavailable for neighbor lists and resets these markings during the AP rejoin and reload process.

3. AP rejoin and reload process:

   After steering clients, if any clients remain connected to the candidate AP, de-authorize those clients and reload the AP so it restarts with a new image. Set a three-minute timer for the APs to rejoin. When the timer expires, check if all candidate APs have joined the controller or mobility peer. If 90% have joined, end the iteration. If not, extend the timer by three minutes and check again. After three attempts, start the next iteration. Each iteration usually lasts about 10 minutes.

   You only need to configure the number of APs to upgrade at a time as a percentage of the total APs in the network. The default is 15 percent.

```
Device(config)# ap upgrade staggered {25 | 15 | 5}
```

Use the command to trigger the rolling AP upgrade:

```
Device# ap image upgrade [test]
```

Note Rolling AP upgrade does not resume after an SSO. To restart it, use the **ap image upgrade** command. This restarts the upgrade for all APs, including Mesh APs.

Install AP service package (GUI)

Use the GUI to install a new or updated AP service package on your device when needed.

Procedure

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

Step 2 Click the **AP Service Package (APSP)** tab.

Step 3 Click **Add**.

Step 4 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **File path**, and select **File System** from the drop-down list.

b) If you choose **SFTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path**, and select **File System** from the drop-down list.

c) If you choose **FTP** as the **Transport Type**, enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and select **File System** from the drop-down list.

d) If you choose **Device** as the **Transport Type**, enter the **File path** and select **File System** from the drop-down list.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, select **File System** from the drop-down list, and click **Select File** to navigate to the **Source File Path**.

Step 5 Enter the **File Name** and click **Add File**.

Step 6 From the **AP Upgrade Configuration** section, select the percentage of APs to include from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Install AP service package (CLI)

Use this procedure to selectively update APs with SMU. Apply image updates only to APs that are filtered by site tags using CLI.

Procedure

Step 1 Check for ongoing activities such as AP image predownload or AP rolling upgrade.

Example:

```
Device# install add file flash filename
```

If there are no such activities, populate the predownload directory to install a package file to the system.

Step 2 Add a site tag to a site filter.

Example:

```
Device# ap image site-filter file filename flash add site-tag bgl18
```

Step 3 (Optional) Remove a site tag from a site filter.

Example:

```
Device# ap image site-filter file filename flash remove site-tag bgl18
```

Step 4 (Optional) Perform predownload of an AP image.

Example:

```
Device# ap image predownload
```

This image predownload is filtered by the site filter, set up in the previous step.

Step 5 Trigger the AP upgrade in a rolling, staggered fashion for the APs added in the site filter.

Example:

```
Device# install activate file filename flash
```

Step 6 Commit the image update.

Example:

```
Device# install commit
```

During the commit, the mapping from file to site is saved in the persistent database. This ensures the mapping remains available after a reload.

Add a site to a filter (CLI)

Add a site tag to a site filter to control which APs receive image pre-downloads and upgrades.

Procedure

Step 1 Add a site tag to a site filter.

Example:

```
Device# ap image site-filter file filename flash add site-tag bgl18
```

Step 2 Predownload the image and upgrade the APs based on the site filter.

Example:

```
Device# ap image site-filter file filename flash apply
```

Step 3 Clear the site filter table, predownload the image, and perform a rolling AP upgrade to all sites where it is not active.

Example:

```
Device# ap image site-filter file flash filename clear
```

Deactivate an image (CLI)

Remove or deactivate a specific AP image from all sites using CLI.

Procedure

Perform rolling AP upgrade based on the AP models present in the prepare file.

Example:

```
Device# install deactivate file flash filename
```

Deactivation is not limited by site and applies to all sites.

Note
The system takes action only if the APs in a site are not running the SMU that is being deactivated.

Roll back APSP (CLI)

Revert AP images to a previous software state by using rollback profiles and image predownload support.

Procedure

Step 1 (Optional) Move to any rollback point using AP image predownload support.

Example:

```
Device# install add profile rollback_profile-name rollback_id1
```

Note
To get a list of available rollback profile names, use the **show install profile** command.

Step 2 (Optional) Perform predownload of an AP image.

Example:

```
Device# ap image predownload
```

This image predownload is filtered by the site filter, which you set up earlier.

Step 3 Perform rollback of the image for the affected AP models.

Example:

```
Device# install rollback to rollback_id rollback_id1
```

The roll back action is not filtered by site. Therefore, rollback applies to all the sites.

Note
APs that are in the base image, or at a point before the rollback action takes effect, are not affected.

Cancel the Upgrade (CLI)

Stop an in-progress or pending software upgrade on your device using CLI.

Procedure

Abort the upgrade by resetting the APs in a rolling fashion.

Example:

```
Device# install abort
```

Verify the upgrade

To see the summary of the AP software install files, enter the command:

```
Device# show ap image file summary

AP Image Active List
============================
Install File Name: base_image.bin
------------------------------
AP Image Type    Capwap Version  Size (KB)         Supported AP models
-------------    --------------
-----------------------------------------------------------------------
     ap1g1       17.3.0.30        13300   NA

     ap1g2       17.3.0.30        34324   NA

     ap1g3       17.3.0.30        98549   AP803

    ap1g4       17.3.0.30             34324   AP1852E, AP1852I, AP1832I, AP1830I, AP1810W,
 OEAP1810

    ap1g5      17.3.0.30            23492   AP1815W, AP1815T, OEAP1815, AP1815I, AP1800I,
 AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I

     ap1g6       17.3.0.30        93472               AP2900I, C9117AXI

   ap1g6a       17.3.0.30       247377             C9130AXI, C9130AXE, C9140AXI, C9140AXD,
```

```
 C9140AXT

     ap1g7       17.3.0.30        23988               AP1900I, C9115AXI, AP1900E, C9115AXE,
 C9120AXE, C9120AXP, C9120AXI

     ap1g8       17.3.0.30        23473   C9105AXI, C9105AXW, C9110AXI, C9110AXE

     ap3g1       17.3.0.30        23422   NA

     ap3g2       17.3.0.30        23411   AP1702I

     ap3g3       17.3.0.30        23090   AP3802E, AP3802I, AP3802P, AP4800, AP2802E,
AP2802I, AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC,
IW-6300H-DCW, ESW-6300

     c1570       17.3.0.30        13000   AP1572E, 1573E, AP1572I

     c3700       17.3.0.30        14032   AP3702E, AP3701E, AP3701I, AP3702I, AP3701P,
AP3702P, AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C

 virtApImg       17.3.0.30                   177056        APVIRTUAL


AP Image Prepare List**
============================
Install File Name: base_image.bin
------------------------------
============================
Install File Name: base_image.bin
------------------------------
AP Image Type    Capwap Version  Size (KB)         Supported AP models
-------------    --------------
-----------------------------------------------------------------------
     ap1g1       17.3.0.30     13300             NA

     ap1g2       17.3.0.30     34324             NA

     ap1g3       17.3.0.30     98549             AP803

     ap1g4       17.3.0.30           34324             AP1852E, AP1852I, AP1832I, AP1830I,
 AP1810W, OEAP1810

     ap1g5       17.3.0.30           23492             AP1815W, AP1815T, OEAP1815, AP1815I,
 AP1800I, AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I

     ap1g6       17.3.0.30     93472                         AP2900I, C9117AXI

    ap1g6a       17.3.0.30     247377                        C9130AXI, C9130AXE, C9140AXI,
 C9140AXD, C9140AXT

     ap1g7       17.3.0.30     23988                   AP1900I, C9115AXI, AP1900E, C9115AXE,
 C9120AXE, C9120AXP, C9120AXI

     ap1g8       17.3.0.30     23473             C9105AXI, C9105AXW, C9110AXI, C9110AXE

     ap3g1       17.3.0.30     23422             NA

     ap3g2       17.3.0.30     23411             AP1702I

     ap3g3       17.3.0.30     23090            AP3802E, AP3802I, AP3802P, AP4800, AP2802E,
 AP2802I, AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC,
IW-6300H-DCW, ESW-6300

     c1570       17.3.0.30     13000             AP1572E, 1573E, AP1572I
```

```
    c3700      17.3.0.30     14032            AP3702E, AP3701E, AP3701I, AP3702I, AP3701P,
 AP3702P, AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C

 virtApImg       17.3.0.30                 177056            APVIRTUAL

**The difference between the Active and Prepare lists identifies images being predownloaded
 to APs.
```

To see the summary of the AP site-filtered upgrades, enter the command:

```
Device# show ap image site summary

Install File Name: vwlc_apsp_16.11.1.0_74.bin

Site Tag                                    Prepared         Activated        Committed

-------------------------------------------------------------------------------------------
bgl-18-1                                    Yes              Yes              Yes

bgl-18-2                                    Yes              Yes              Yes

bgl-18-3                                    Yes              Yes              Yes

default-site-tag                            Yes              Yes              Yes
```

To see the summary of AP upgrades, enter the command:

```
Device# show ap upgrade summary
```

To check the status of an APSP, enter the command:

```
Device# show install summary

[ Chassis 1 ] Installed Package(s) Information:

State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated & Committed, D - Deactivated & Uncommitted

--------------------------------------------------------------------------------

Type St Filename/Version

--------------------------------------------------------------------------------

APSP I bootflash:vwlc_apsp_16.11.1.0_74.bin

IMG C 16.11.1.0.1249


--------------------------------------------------------------------------------

Auto abort timer: inactive

--------------------------------------------------------------------------------
```

Verify AP upgrade on the controller

Use the **show** command to verify the AP upgrade on the controller:

```
Device #show ap upgrade

AP upgrade is in progress
From version: 8 16.9.1.6
To version: 9 16.9.1.30
Started at: 03/09/2018 21:33:37 IST
Percentage complete: 0
Expected time of completion: 03/09/2018 22:33:37 IST
Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-------------------------------------------------------------------------
0 03/09/2018 21:33:37 IST 03/09/2018 21:33:37 IST 0
1 03/09/2018 21:33:37 IST ONGOING 0
Upgraded
--------
Number of APs: 0
AP Name Ethernet MAC Iteration Status
-------------------------------------------------------------------------
In Progress
-----------
Number of APs: 1
AP Name Ethernet MAC
-------------------------------------------------
APf07f.06a5.d78c f07f.06cf.b910
Remaining
---------
Number of APs: 3
AP Name Ethernet MAC
-------------------------------------------------
APCC16.7EDB.6FA6 0081.c458.ab30
AP38ED.18CA.2FD0 38ed.18cb.25a0
AP881d.fce7.5ee4 d46d.50ee.33a0
```