Software Maintenance Upgrade

Introduction to Software Maintenance Upgrade

Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a patch fix or a security resolution to a released image. A SMU package is provided for each release and per component basis, and is specific to the corresponding platform.

A SMU provides a significant benefit over classic Cisco IOS software because it allows you to address the network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install noncompatible SMUs.

All the SMUs are integrated into the subsequent Cisco IOS XE software maintenance releases. A SMU is an independent and self-sufficient package and does not have any 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 for the full lifecycle of the underlying software release.

Note You can activate the file used in the **install add file** command only from the filesystems of the active device. You cannot use the file from the standby or member filesystems; the **install add file** command will fail in such instances.

Note When the SMU file is deleted and a reboot is performed, the device may display the following error message:

```
--- 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. It may lead to functional errors, such as the inability to install new SMU or APSP files.

We recommend that you use the install remove file command to remove previous instances of APSP or SMU files from the bootflash.

SMU infrastructure can be used to meet the following requirements in the wireless context:

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

Note The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the **show ap image** command, to ensure that correct data is displayed.

SMU Workflow

The SMU process should be initiated with a request to the SMU committee. Contact your customer support to raise an SMU request. During the release, the SMU package is posted on the Cisco Software Download page and can be downloaded and installed.

SMU Package

An SMU package contains the metadata and fix for the reported issue the SMU is requested for.

SMU Reload

The SMU type describes the effect on a system after installing the corresponding SMU. SMUs can be nontraffic-affecting or can result in device restart, reload, or switchover.

A controller cold patch require a cold reload of the system during activation. A cold reload is the complete reload of the operating system. This action affects the traffic flow for the duration of the reload (~5 min). This reload ensures that all the processes are started with the correct libraries and files that are installed as part of the corresponding SMU.

Controller hot patching support allows the SMU to be effective immediately after activation, without reloading the system. After the SMU is committed, the activation changes are persistent across reloads. Hot patching

SMU packages contain metadata that lists all processes that need to be restarted in order to activate the SMU. During SMU activation, each process in this list will be restarted one at a time until the SMU is fully applied.

Installing a SMU (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, 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**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose 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**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.

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

d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose 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 The File System depends upon the kind of device you are using. On physical controllers, you have the option to store the file to the bootflash or hard disk, whereas in case of virtual controllers, you can only store it in the bootflash.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose 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**.

This operation copies the maintenance update package from the location you selected above to the device and performs a compatibility check for the platform and image versions and adds the SMU package for all the members. After a SMU is successfully added to the system, a message is displayed about the successful operation and that the SMU can be activated on the device. The message displays the name of the package (SMU) that is now available to be activated. It lists the SMU Details - Name, Version, State (active or inactive), Type (reload, restart, or non-reload) and other compatibility details. If SMU is of the Type - reload, then any operation (activate, deactivate or rollback) will cause the device to reload; restart involves only a process restart and if it is non reload- no change in process takes place.

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

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

The Commit operation creates commit points. These commit points are similar to snapshots using which you can determine which specific change you want to be activated or rolled back to, in case there is any issue with

the SMU. The commit can be done 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.

Installing SMU

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:** *filename* **Example:** `Device# install add file bootflash:<Filename>`	Copies the maintenance update package from a remote location to the device, and performs a compatibility check for the platform and image versions. This command runs base compatibility checks on a file to ensure that the SMU package is supported on the platform. It also adds an entry in the package/SMU.sta file, so that its status can be monitored and maintained.
Step 2	**install activate file bootflash:** *filename* **Example:** `Device# install activate file bootflash:<Filename>`	Runs compatibility checks, installs the package, and updates the package status details. For a restartable package, the command triggers the appropriate post-install scripts to restart the necessary processes, and for non-restartable packages it triggers a reload.
Step 3	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads. The commit can be done 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, but not after the second reload.
Step 4	**show version** **Example:** `Device# show version`	Displays the image version on the device.
Step 5	**show install summary** **Example:** `Device# show install summary`	Displays information about the active package. The output of this command varies according to the install commands that are configured.

Roll Back an Image (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, choose **Base**, **Committed** or **Rollback Point**.
Step 5 Click **Add File**.

Rollback SMU

Procedure

	Command or Action	Purpose
Step 1	**install rollback to** {**base** | **committed** | **id** | **committed** } *committed ID* **Example:** `Device(config)# install rollback to id 1234`	Returns the device to the previous installation state. After the rollback, a reload is required.
Step 2	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Deactivate SMU

Procedure

	Command or Action	Purpose
Step 1	**install deactivate file bootflash:** *filename* **Example:** `Device# install deactivate file bootflash:<Filename>`	Deactivates an active package, updates the package status, and triggers a process to restart or reload.
Step 2	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Configuration Examples for SMU

The following is sample of the SMU configuration, after the install add for the SMU is done:

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

Information About AP Device Package

The controller supports rolling out critical bug fixes using Software Maintenance Upgrade (SMU). Similarly, if any new AP hardware model is introduced, the AP models need to be connected to the existing wireless network.

Currently, when a new AP hardware model is introduced, those get shipped along with the corresponding controller related major software version. Then you need to wait for the release of a corresponding controller version relative to the new AP model and upgrade the entire network.

From 16.11.1 onwards, you can introduce the new AP model into your wireless network using the SMU infrastructure without the need to upgrade to the new controller version. This solution is termed as AP Device Package (APDP).

SMU Process or Workflow

The SMU process builds APDP to detect code changes and build APDP. It also supports addition of a new file (AP image file) to APDP and inclusion of those AP images into APDP.

The workflow is as follows:

- install add
- install activate
- install commit

For more details, see *Managing AP Device Package*.

Note To ensure completion of the APSP or APDP activation or deactivation process, ensure that you run the **install commit** command after the **install activate** or **install deactivate** command. Failing to do so within 6 hours of the deactivate operation terminates the deactivate operation and moves it back to the original commit position.

SMU Package

A SMU package contains the metadata that carry AP model and its capability related details.

AP Image Changes

When new AP models are introduced, there may or may not be corresponding new AP images. This means that AP images are mapped to the AP model families. If a new AP model belongs to an existing AP model family then you will have existing AP image entries (Example: ap3g3, ap1g5, and so on). For instance, if an AP model belongs to either ap3g3 or ap1g5, the respective image file is updated with the right AP image location. Also, the corresponding metadata file is updated with the new AP model capability information.

If a new AP model belongs to a new AP model family and new image file, the new image entry file is created in the right AP image location. Also, the corresponding metadata file is updated with the new AP model capability information.

During AP image bundling and packaging of APDP, the new AP model images and metadata file are packaged into APDP.

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

Installing AP Device Package (GUI)

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, 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**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list.

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

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

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

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **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, choose the percentage of APs to be included from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Installing AP Device Package (CLI)

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:** *filename* **Example:** `Device# install add file bootflash:<Filename>`	Extracts AP images from APDP and places them in SMU or APDP specific mount location. **Note** Here, the SMU does not trigger the Wireless module.
Step 2	**install activate file bootflash:** *filename* **Example:** `Device# install activate file bootflash:<Filename>`	Adds the AP software in APDP to the existing current active AP image list. Also, updates 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	**install commit** **Example:** `Device# install commit`	Commits the new AP software to be persistent across reloads. The commit can be done 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, but not after the second reload.
Step 4	**install deactivate file bootflash:** *filename* **Example:** `Device# install deactivate file bootflash:<Filename>`	(Optional) Deactivates an active APDP, updates the package status, and triggers a process to restart or reload.
Step 5	**show version** **Example:** `Device# show version`	Displays the image version on the device.

Verifying APDP on the Controller

To verify the status of APDP packages on the controller , use the following 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.

Information About Per Site or Per AP Model Service Pack (APSP)

The controller supports critical updates to the access points (APs) using Software Maintenance Update (SMU). Using the Per Site or Per AP Model Service Pack feature, you can roll out critical AP bug fixes to a subset of APs, on a site or group of sites, using SMU in a staggered manner.

This feature allows to control the propagation of a SMU in your network by selecting the sites, to be included in the SMU activation, using Per Site AP SMU rollout. However, all sites should be brought to the same SMU level before a new SMU can be rolled out to a subset of sites or for a subsequent image upgrade to be initiated on the system..

Using Per AP model SMU, you can limit the update to only certain AP models. The software is predownloaded and is activated only to certain AP models, within a site. Note that if a certain number of model images are included in a SMU, all the future updates must contain software images for those models.

This feature is supported in the flex-connect mode, local mode, and Software-Defined Access (SD-Access) wireless scenarios.

Note After applying the AP site filter for per site SMU upgrade, a new image installation will not be allowed without applying the site filter to all the other sites, or removing the existing site filter.

Restrictions

- If APs are not configured to a primary controller, the APs will see the same discovery response from controllers with the APSP image and without the APSP image, causing the APs to flap between two controllers.

Workflow of AP SMU Upgrade

- Run a query to check whether there are ongoing activities, such as AP image predownload or AP rolling upgrade.
- Identify the site or sites to install the SMU in, and set up a site filter.
- Trigger the predownload of SMU to the sites in the site filter.

- Activate the SMU after the predownload is complete.
- Commit the update.

Note You can add more sites to a filter after setting up the filter. However, you have to apply the filter again using the **ap image site-filter file** *file-name* **apply** command. If you clear the site filter, the update is made on all the remaining sites. Deactivation and rollback of the images are not filtered per site, and are applicable to all the sites.

Rolling AP Upgrade

Rolling AP upgrade is a method of upgrading the APs in a staggered manner 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.

Note The AP images should be downloaded before the rolling upgrade is triggered, so that all the APs that are to be upgraded have the new image version.

Note The time required to complete Rolling AP upgrade depends on factors such as the number of APs, the percentage of APs in each iteration, the controller type, and the connectivity between the controller and the APs. In general, Rolling AP upgrade completion time is the max iteration time (where each iteration can take up to 5 minutes) * expected number of iterations. You use the *iteration expiry time* field of the **show ap upgrade** command output to see the end time.

Rolling AP Upgrade Process

Rolling AP upgrade is done on a per controller basis. The number of APs to be upgraded at a given time, is the percentage of the total number of APs that are connected to the controller. The percentage is capped at a user configured value. The default percentage is 15. The non-client APs will be upgraded before the actual upgrade of APs begin.

The upgrade process is as follows:

1. **Candidate AP Set Selection**

   In this stage, a set of AP candidates are 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 the candidates cannot be selected using the neighboring AP information, select candidates from indirect neighbors. If you still are not able to select candidates, the AP will be upgraded successfully without any failure.

Note After the candidates are selected, if the number of candidates are more than the configured percentage value, the extra candidates are removed to maintain the percentage cap.

2. **Client Steering**

   Clients that are connected to the candidate APs are steered to APs that are not there in the candidate AP list, prior to rebooting the candidate APs. The AP sends out a request to each of its associated clients with a list of APs that are best suited for them. This does not include the candidate APs. The candidate APs are marked as unavailable for neighbor lists. Later, the markings are reset in the AP rejoin and reload process.

3. **AP Rejoin and Reload Process**

   After the client steering process, if the clients are still connected to the candidate AP, the clients are sent a de-authorization and the AP is reloaded and comes up with a new image. A three-minute timer is set for the APs to rejoin. When this timer expires, all the candidates are checked and marked if they have either joined the controller or the mobility peer. If 90% of the candidate APs have joined, the iteration is concluded; if not, the timer is extended to three more minutes. The same check is repeated after three minutes. After checking thrice, the iteration ends and the next iteration begins. Each iteration may last for about 10 minutes.

   For rolling AP upgrade, there is only one configuration that is required. It is the number of APs to be upgraded at a time, as a percentage of the total number of APs in the network.

   Default value will be 15.

```
Device (config)#ap upgrade staggered <25 | 15 | 5>
```

Use the following command to trigger the rolling AP upgrade:

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

Note Rolling AP upgrade is not resumed after an SSO. You should run the **ap image upgrade** command to restart the rolling AP upgrade from the beginning and it affects all the APs, including the Mesh APs.

Installing AP Service Package (GUI)

Procedure

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

Step 2 Click **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**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list.

b) If you choose **SFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.
c) If you choose **FTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and choose a **File System** from the drop-down list.
d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose a **File System** from the drop-down list.
e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **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, choose the percentage of APs to be included from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Installing AP Service Package (CLI)

Use the following procedure to roll out critical bug fixes to a subset of APs using SMU.

Procedure

	Command or Action	Purpose
Step 1	**install add file** *file-name* **Example:** `Device# install add file flash:<file-name>`	Checks for ongoing activities, such as AP image predownload or AP rolling upgrade. If there are no such activities, populates the predownload directory to install a package file to the system.
Step 2	**ap image site-filter file** *file-name* **add** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> add bgl18`	Adds a site tag to a site filter.
Step 3	**ap image site-filter file** *file-name* **remove** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> remove bgl18`	(Optional) Removes a site tag from a site filter.
Step 4	**ap image predownload** **Example:** `Device# ap image predownload`	(Optional) Performs predownload of an AP image. This image predownload will be filtered by the site filter, set up in the previous step.
Step 5	**install activate file** *file-name* **Example:** `Device# install activate file flash:<file-name>`	Triggers the AP upgrade in rolling a staggered fashion for the APs added in site filter.
Step 6	**install commit**	Commits the image update.

	Command or Action	Purpose
	Example: `Device# install commit`	During the commit, the mapping from file to site is saved in the persistent database so that it is available even after a reload.

Adding a Site to a Filter

Procedure

	Command or Action	Purpose
Step 1	**ap image site-filter file** *file-name* **add** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> add bgl18`	Adds a site tag to a site filter. Repeat this step again to set up a multisite filter.
Step 2	**ap image site-filter file** *file-name* **apply** **Example:** `Device# ap image site-filter file flash:<file-name> apply`	Predownloads the image and upgrades the APs based on the site filter.
Step 3	**ap image site-filter file** *file-name* **clear** **Example:** `Device# ap image site-filter file flash:<file-name> clear`	Clears the site filter table and predownloads the image and does a rolling AP upgrade to all sites where it is not active.

Deactivating an Image

Procedure

	Command or Action	Purpose
Step 1	**install deactivate file flash** *file-name* **Example:** `Device# install deactivate file flash:<file-name>`	Performs rolling AP upgrade based on the AP models present in the prepare file. Deactivation is not filtered by site. Therefore, deactivation applies to all the sites. **Note** Action is taken if the APs in a site are not running the SMU that is being deactivated. Only internal tables are updated to remove the SMU.

Roll Back APSP

Procedure

	Command or Action	Purpose
Step 1	**install add profile** *rollback_profile-name* **Example:** `Device# install add profile rollback_id1`	(Optional) Moves back to any rollback points in a graceful way with AP image predownload support. **Note** To get a list of available rollback profile names, use **show install profile** command.
Step 2	**ap image predownload** **Example:** `Device# ap image predownload`	(Optional) Performs predownload of an AP image. This image predownload will be filtered by the site filter, set up in the previous step.
Step 3	**install rollback to** *rollback_id* **Example:** `Device# install rollback to rollback_id1`	Performs rollback of the image for the affected AP models. The roll back action is not filtered by site. Therefore, rollback applies to all the sites. **Note** The APs that are in the base image or in a point before the rollback action takes effect are not affected.

Canceling the Upgrade

Procedure

	Command or Action	Purpose
Step 1	**install abort** **Example:** `Device# install abort`	Aborts the upgrade by resetting the APs in rolling fashion.

Verifying the Upgrade

To see the summary of the AP software install files, use the following 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

**Difference of Active and Prepare list gives images being predownloaded to Access Points.
```

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

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

To check the status of an APSP, use the following 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

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

Verifying of AP Upgrade on the Controller

Use the following **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
```