Introduction to Software Maintenance Upgrade

The 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 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.

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

- Controller SMU: Embedded Wireless Controller bug fixes or Cisco Product Security Incident Response information (PSIRT).
- AP bug fixes, PSIRTs, or minor features which do not require any embedded wireless 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 to a system after installing the SMU. SMUs can be non-traffic affecting or can result in device restart, reload, or switchover.

Controller hot patching support allows SMU to be effective immediately after activation without reloading the system. Other controller SMUs 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 currently). This reload ensures that all processes are started with the correct libraries and files that are installed as part of the SMU.

After the SMU is committed, the activation changes are persistent across reloads.

Overview of Controller SMUs

The following table describes the SMU types supported in the Cisco Embedded Wireless Controller:

Table 1: Supported SMU Types in the Embedded Wireless Controller

Package Type	Use Case	SMU Type	Supported on EWC
Controller SMU - Cold Patch	Replace impacted binaries, libraries, or subpackages.	Reload	Limited support (Patch size < 20 MB). No support for IOSD.
Controller SMU - Hot Patch	Replace impacted functions.	Nonreload	Yes
APSP	AP fix by replacing the AP image (does not impact the AP running the active controller).	Nonreload	Yes

Package Type	Use Case	SMU Type	Supported on EWC
APSP	AP fix by replacing the AP image (impacts the AP that is running the active controller).	Reload	Yes (EWC specific variation)
APDP	New AP model support without upgrading the controller.	Nonreload	Yes

Managing Controller Hot or Cold SMU Package

Procedure

	Command or Action	Purpose
Step 1	**install add file tftp:**//<server-ip>/<path>/<smu-filename> **Example:** `Device# install add file tftp://<server-ip>/<path>/<smu-filename>`	The `install add` command copies the file from the external server to the backup_image directory on the embedded wireless controller.
Step 2	**install activate file backup_image:** *smu-filename* **Example:** `Device# install activate file backup_image:<smu-filename>`	This command is used to activate the patch. The `install activate` causes the controller reload only for a cold patch. There is no reload for a hot patch.
Step 3	**install auto-abort-timer stop** **Example:** `Device# install auto-abort-timer stop`	(Optional) Stops the auto cancel timer in case of activated or deactivated SMUs.
Step 4	**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 patch is activated and not committed, the auto cancel timer automatically cancels the activation of the patch in six hours .
Step 5	**show install rollback** **Example:** `Device# show install rollback`	Displays the list of rollback IDs that are available.
Step 6	**install rollback to** {**base** | **committed** | **id** | **label** } *specific-rollback-point*	Rolls back a committed patch. The committed patch can be deactivated and the commit for

	Command or Action	Purpose
	Example: `Device# install rollback to base`	deactivation can be done using the single install rollback command.
Step 7	**install deactivate file backup_image:** *smu-filename* **Example:** `Device# install deactivate file backup_image:<Smu-Filename>`	Deactivates a comitted patch. The `install deactivate` command causes the reload of the controller in case of a cold patch. There is no reload of the controller in case of a hot patch.
Step 8	**install auto-abort-timer stop** **Example:** `Device# install auto-abort-timer stop`	(Optional) Stops the auto cancel timer in case of activated or deactivated SMUs.
Step 9	**install commit** **Example:** `Device# install commit`	Commits the deactivation changes to be persistent across reloads.
Step 10	**install remove file backup_image:** *smu-filename* **Example:** `Device# install remove file backup_image:<smu-filename>`	Removes a patch that is in the inactive state. This command also removes the file physically from `backup-image:`
Step 11	**install abort** **Example:** `Device# install abort`	Cancels the upgrade by resetting the APs in rolling fashion.
Step 12	**show install summary** **Example:** `Device# show install summary`	Displays information about the active package. The output of this command varies based on the packages, and the package states that are installed.
Step 13	**show install package backup_image:** *smu-filename* **Example:** `Device# show install package backup-image: <smu_filename>`	Displays information about the SMU package.

Creating SMU Files (GUI)

Follow the steps given below to create SMU files:

Procedure

Step 1 Choose **Administration** > **Software Management** > **Software Maintenance Upgrade (SMU)**.

Step 2 Click **Add**.
A dialog box is displayed.

Step 3 From the **Transport Type** drop-down list,

- **TFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **File Path**, **File Name**, and **File System**.
- **SFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **Port Number** (Default port number is 22), SFTP username and password, **File Path**, **File Name**, and **File System**.
- **FTP**: Specify the **Server IP Address (IPv4/IPv6)**, **Port Number** (Default port number is 22), FTP username and password, **File Path**, **File Name**, and **File System**.
- **Device**: Specify the **File System** and **File path**.
- **My Desktop**: Specify the **File System** and **Source File Path** .

Step 4 Click **Add File**.

Configuration Examples for SMU

The following is sample of the SMU configuration:

```
Device# install add file
tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-apsp1.bin
install_add: START Tue Jun 4 15:08:26 UTC 2019
Downloading file tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-smu.bin
Finished downloading file tftp://10.1.1.2/auto/tftpboot/user1/ewc/ewc-smu.bin to
backup_image:ewc-smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....
install_add: ap image predownload is allowed.

--- Starting initial file syncing ---
Info: Finished copying backup_image: ewc-smu.bin to the selected chassis
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on chassis 1
MEWLC response success sync_successCumulative SMU Size: 24 KB
Cumulative size of all SMU's will not exceed 20000 KB
Available Memory in /backup_image is 251480 KB
Available memory 251480 KB is greater than available memory required 2000 KB
[1] Finished SMU_ADD on chassis 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add
```

```
Device# install activate file backup_image:ewc-apsp1.bin
install_activate: START Tue Jun 4 15:18:58 UTC 2019
install_activate: Activating SMU
Cumulative SMU Size: 24 KB
Cumulative size of all SMU's will not exceed 20000 KB
```

```
Available Memory in /backup_image is 250984 KB
Available memory 250984 KB is greater than available memory required 2000 KB
MEWLC response success sync_successExecuting pre scripts....
Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
[1] SMU_ACTIVATE package(s) on chassis 1
valid
install_activate: FP fp error skipping. Platform to fix this in Fru List
[1] Finished SMU_ACTIVATE on chassis 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

Executing post scripts....
Executing post scripts done.
Executing post scripts....
Executing post scripts done.
SUCCESS: install_activate /backup_image/ewc-apsp1.bin
```

Device#install commit

```
install_commit: START Tue Jun 4 16:15:25 UTC 2019
install_commit: Committing SMU
Executing pre scripts....
install_commit:
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
[1] SMU_COMMIT package(s) on chassis 1
valid
[1] Finished SMU_COMMIT on chassis 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

Waiting for the platform to set the SMU sync timerSMU sync status is sync_successSMU sync
to AP's success
/tmp/rp/chasfs/wireless/wlc_notify
SUCCESS: install_commit /backup_image/ewc-apsp1.bin
```

Device#install rollback to base

```
install_rollback: START Tue Jun 4 16:42:24 UTC 2019
install_rollback: Rolling back SMU
Executing pre scripts....
install_rollback:
Executing pre sripts done.

--- Starting SMU Rollback operation ---
Performing SMU_ROLLBACK on all members
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
ls: cannot access '/tmp/sw/fp/*/*/*/mount/.pkginfo': No such file or directory
[1] SMU_ROLLBACK package(s) on chassis 1
[1] Finished SMU_ROLLBACK on chassis 1
Checking status of SMU_ROLLBACK on [1]
SMU_ROLLBACK: Passed on [1]
Finished SMU Rollback operation

Executing post scripts....
Executing post scripts done.
Waiting for the platform to set the SMU sync timerSMU sync status is sync_successSMU sync
```

```
to AP's success
/tmp/rp/chasfs/wireless/wlc_notifyExecuting post scripts....
Executing post scripts done.
SUCCESS: install_rollback /backup_image/ewc-apsp1.bin Tue Jun 4 16:43:01 UTC 2019
```

Device# install deactivate file backup_image: ewc-apsp1.bin

install remove file backup_image:ewc-apsp1.bin

Device#show install sum

```
[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
APSP C backup_image:ewc-apsp1.bin
IMG C 17.1.1.0.69043

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

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.

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 neighbouring AP information. For example, if you identify an AP for upgrade, a certain number (N) of its neighbours 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 neighbouring AP information, select candidates from indirect neighbours. 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 neighbour 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>
   ```

Verifying 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: 17.1.0.6
To version: 17.1.0.99

Started at: 06/04/2019 15:19:32 UTC
Configured percentage: 15
Percentage complete: 0
Expected time of completion: 06/04/2019 16:39:32 UTC

Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-----------------------------------------------------------------------------------------------------
0 06/04/2019 15:19:33 UTC 06/04/2019 15:19:33 UTC 1
1 06/04/2019 15:19:33 UTC ONGOING 1

Upgraded
--------
Number of APs: 1
AP Name Ethernet MAC Iteration Status Site
```

```
-------------------------------------------------------------------------------------------------
AP7069.5A74.7604 7069.5a78.5580 0 Not Impacted default-site-tag

In Progress
-----------
Number of APs: 1
AP Name Ethernet MAC
-----------------------------------------------
APB4DE.3169.7842 4c77.6dc4.a220

Remaining
---------
Number of APs: 0

AP Name Ethernet MAC
-----------------------------------------------

APs not handled by Rolling AP Upgrade
-------------------------------------
AP Name Ethernet MAC Status Reason for not handling by Rolling AP Upgrade
```

AP Device Pack (APDP) and AP Service Pack (APSP)

APSP and APDP

AP Service Pack (APSP) - APSP rolls out fixes to AP images for one or more AP models. Pre-download the AP images and activate (through rolling upgrade) these images to a subset of AP models.

- Patched APs run a different CAPWAP version than the rest of the APs. For e.g. 17.1.0.100 and 17.1.0.0.
- Per site APSP rollout is not supported. In embedded wireless controller APSP all APs must be in a single default site.

AP Device Pack (APDP) -

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

APDP allows you introduce the new AP model into your wireless network using the SMU infrastructure without the need to upgrade to the new embedded wireless controller version.

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 bundled with APDP SMU zip file. The corresponding metadata file is updated with the new AP model capability information including the AP image that it requires.

If a new AP model belongs to a new AP model family, a new image file would be bundled in the APDP SMU zip file. The corresponding metadata file is updated with the new AP model capability information including the AP image that it requires.

Information about APSP and APDP

SMU AP images are not part of the SMU binary, and the AP images are hosted outside the contoller.

- Only SFTP and TFTP methods are supported for SMU AP image download.
- HTTP, HTTP, and CCO methods are not supported for APSP or APDP.

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

Note All the zipped files are required in order to successfully proceed with the upgrade. All the contained files in the zip folder are made accessible through the download method.

Following are the pre-requisites for TFTP/SFTP software upgrade:

- A TFTP/SFTP server is reachable from the management IP address of the embedded wireless controller.
- The upgrade bundle with the AP images (ap1g6, ap1g6a, ap1g7, ap3g3, and so on) and the controller image (C9800-AP-iosxe-wlc.bin) that is downloaded from the website is unzipped and copied onto the TFTP/SFTP server.

Managing APSP and APDP

AP images are hosted outside the wireless controller. In the embedded wireless controller, only TFTP or SFTP is supported for SMU AP image download.

Configuring the APSP and APDP Files (GUI)

Follow the steps given below to add APSP or APDP files:

Procedure

Step 1 Choose **Administration** > **Software Management** > **AP Service Package (APSP)** or **AP Device Package (APDP)**.
The **Add an AP Device Package** or **Add an AP Service Package** window is displayed.

Step 2 From the **Transport Type** drop-down list,

- **TFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **File Path**, **File Name**, and **File System**.
- **SFTP**: Specify the **Server IP Address (IPv4/IPv6)**, **Port Number** (Default port number is 22), SFTP username and password, **File Path**, **File Name**, and **File System**.

Step 3 Click **Add File**.

Configuring the TFTP Server Directory

To set up the TFTP server directory, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enter the configuration mode.
Step 2	**wireless profile image-download default** **Example:** `Device(config)#wireless profile image-download default`	Configures EWC-AP image download parameters. Use only default as the image download profile name.
Step 3	**image-download-mode** { **tftp** | **sftp** } **Example:** `Device(config-wireless-image-download-profile)#image-download-mode tftp`	Configures image download using TFTP.
Step 4	**tftp-image-path** *tftp-image-path* **Example:** `Device(config-wireless-image-download-profile-tftp)#tftp-image-path /tftpboot/cisco/ewc/`	Configures the TFTP server root directory for the AP images.
Step 5	**tftp-image-server** { **A.B.C.D** | **X:X:X:X::X** } **Example:** `Device(config-wireless-image-download-profile-tftp)#tftp-image-server 5.5.5.5`	Configures the TFTP server address.

What to do next

- Set up the remote server directory: When you receive the complete bundle in a zip file, copy the zip file to a root directory, for example, `/tftpboot/user/ewc`. Example of the complete bundle - `/tftpboot/user/ewc/17.1.zip`.
- Unzip the file. The following are the examples of the files that will be present in the root directory: `ap3g3, ap1g4, C9800-AP-iosxe-wlc.bin`, and so on.

Note When there is an issue and you want to patch an APSP SMU based on the 17.1 patch file `C9800_AP.17_1.22.CSCvr11111.apsp.zip` is pasted in the same root folder, that is, `/tftproot/user/ewc/C9800_AP.17_1.22.CSCvr11111.apsp.zip`. When you unzip the file, a sub-directory, for example, `/tftpboot/user/ewc/17_1.22.CSCvr11111/` is created automatically. The AP images (for example, `ap3g3`) and SMU binary (`apsp_CSCvr11111.bin`) are present in that sub-directory.

Configuring the SFTP Server Directory

To set up the SFTP server directory, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enter the configuration mode.
Step 2	**wireless profile image-download default** **Example:** `Device(config)#wireless profile image-download default`	Configures EWC-AP image download parameters. Use only default as the image download profile name.
Step 3	**image-download-mode** {**tftp** | **sftp**} **Example:** `Device(config-wireless-image-download-profile)#image-download-mode sftp`	Configures image download using SFTP.
Step 4	**sftp-image-path** *sftp-image-path* **Example:** `Device(config-wireless-image-download-profile-sftp)#sftp-image-path /sftpboot/cisco/ewc/`	Configures the SFTP server root directory for the AP images.
Step 5	**sftp-image-server** {**A.B.C.D** | **X:X:X:X::X**} **Example:** `Device(config-wireless-image-download-profile-sftp)#sftp-image-server 5.5.5.5`	Configures the SFTP server address.
Step 6	**sftp-password** {**0** | **8**} *password re-enter password* **Example:** `Device(config-wireless-image-download-profile-sftp)#sftp-password 0 admin`	Configures the SFTP password.
Step 7	**sftp-username** *username* **Example:** `Device(config-wireless-image-download-profile-sftp)#sftp-username admin`	Configures the SFTP username.

What to do next

- Set up the remote server directory: When you receive the complete bundle in a zip file, copy the zip file to a root directory, for example, `/sftpboot/user/ewc`. Example of the complete bundle - `/sftpboot/user/ewc/17.1.zip`.
- Unzip the file. The following are the examples of the files that will be present in the root directory: `ap3g3, ap1g4, C9800-AP-iosxe-wlc.bin`, and so on.

Note When there is an issue and you want to patch an APSP SMU based on the 17.1 patch file `C9800_AP.17_1.22.CSCvr11111.apsp.zip` is pasted in the same root folder, that is, `/sftproot/user/ewc/C9800_AP.17_1.22.CSCvr11111.apsp.zip`. When you unzip the file, a sub-directory, for example, `/sftpboot/user/ewc/17_1.22.CSCvr11111/` is created automatically, and the AP images (for example, `ap3g3`) and SMU binary (`apsp_CSCvr11111.bin`) are present in that sub-directory.

Positive Workflow - APSP and APDP

Procedure

	Command or Action	Purpose

Step 1	**install add file** {**tftp:** | **sftp:** | **backup_image:**} `apsp.bin`
	Example:
	TFTP and Backup Image -
	`Device# install add file tftp://server_path/auto/tftpboot/user/ewc/17_1.22.CSCvr11111/apsp_CSCvr11111.bin`
	`Device#install add file backup-image:apsp_CSCvr11111.bin`
		The `install add` command copies the file from the external server to the backup_image directory on the embedded wireless controller.

Step 2	**ap image predownload** **Example:** `Device# ap image predownload`	This command is optional. The command predownloads the AP image. If the predownload has started, ensure that it completes before step 3 is initiated.
Step 3	**install activate file backup-image:** *apsp.bin* **Example:** `Device# install activate file backup-image:apsp.bin`	This command starts the rolling AP upgrade. **Note** For APDP, after activate, the EWC Controller allows APs of the new AP model to join, and get the newly installed SMU AP image.
Step 4	**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 one reload. If a patch is activated and not committed, the auto abort timer automatically cancels the activation of the patch in six hours .

Rollback and Cancel

One-Shot Rollback

Procedure

	Command or Action	Purpose
Step 1	**show install rollback** **Example:** `Device# show install rollback`	Displays the possible rollback points.
Step 2	**install rollback to** {**base** | **committed** | **id** | **label** } *specific-rollback-point* **Example:** `Device# install rollback to base`	This command triggers the Rolling AP upgrade. Rolling upgrade works for all APs that have the required image. Rest of the APs are rebooted together. Rolls back a committed patch. The committed patch can be deactivated and the commit for deactivation can be done using the single install rollback command.

Multi-Step Rollback

Procedure

	Command or Action	Purpose
Step 1	**show install profile** **Example:** `Device# show install profile`	The `show install profile` command displays the profiles corresponding to the rollback points.
Step 2	**install add profile** *profile-rollback-point* **Example:** `Device# install add profile profile-rollback-point`	This command prepares the wireless module for the predownload step corresponding to the rollback point.
Step 3	**install rollback to** {**base** | **committed** | **id** | **label** } *specific-rollback-point* **Example:** `Device# install rollback to base`	This command triggers the Rolling AP upgrade. Rolling upgrade works for all APs that have the required image. Rest of the APs are rebooted together. Rolls back a committed patch. The committed patch can be deactivated and the commit for deactivation can be done using the single install rollback command.

One-Shot Cancel

The following command is used for the One-Shot manual cancel:

Procedure

- **install abort**

  Example:

  ```
  Device# install abort
  ```

  This command triggers rolling AP upgrade. Cancel is allowed only if commit is not yet completed. With One-Shot Cancel there is no predownload step. Rolling AP upgrade works for all APs which have the required image. Rest are rebooted together.

Automatic Timer-Based One-Shot Cancel

After activation, a default 6-hour cancel timer is started. The cancel timer can be set to a different value when the **activate** command is issued, through the **auto-abort-timer** parameter. When the cancel timer expires, cancellation is performed the same way as the manual cancellation.

Configuring Rollback (GUI)

Follow the steps given below to configure rollback for APSP and APDP:

Procedure

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

Step 2 Select either **AP Service Pack (APSP)** or **AP Device Pack (APDP)**.

Step 3 From the **Rollback to** drop-down list, choose the Rollback type as *Base* or *Committed*.

Step 4 Click **Submit**.

Verifying APDP on the Embedded Wireless Controller

To verify the status of APDP packages on the embedded wireless 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.