Upgrading the Cisco Catalyst 9800 Wireless Controller Software

Software upgrade for Cisco Catalyst 9800 Series Wireless Controller

A software upgrade for Cisco Catalyst 9800 Series Wireless Controllers is a series of improvements and maintenance updates that:

- introduce new features and enhancements with each major release,
- offer various upgrade methods including full image upgrades and bug patch applications, and
- support upgrading through either GUI or CLI interfaces for user convenience.

This section describes the upgrade process and the methods to upgrade the Cisco Catalyst 9800 Series Wireless Controller Software.

Newer versions of the controller software are released at regular intervals. This includes major releases as well as rebuild releases that focuses on bug fixes. The version of the AP software is also tied to the controller software release. Every major Cisco IOS XE software release contains new sets of features that are essential for the enterprise-class customers.

Based on your requirement, such as upgrading the full image or applying a software patch for bugs, you can go for an appropriate software upgrade, using either GUI or CLI.

- Upgrade the Controller Software (GUI)
- Upgrade the Controller Software (CLI)

Software Upgrade Options

- **Software Maintenance Upgrade**: This method installs a software package on the system to provide a patch fix or a security resolution to a released image. This upgrade package is provided on a per release and per component basis, and is specific to the platform.
- **Hitless Upgrade**: This method allows the APs to be upgraded in a staggered manner, while still being connected to the same controller. This avoids upgrade downtime even for N+1 networks.
- **In-Service Software Upgrade**: This method upgrades a wireless controller image to a later release while the network forwards packets. This feature is supported only within and between major releases.

Note We recommend In-Service Software Upgrade if you are upgrading the entire image or cold controller SMU. Use Software Maintenance Upgrade for software patches or bug fixes.

The software upgrade time is estimated to be less than 6 hours for a large network. However, the upgrade time depends on factors such as the number of APs, the percentage of APs to upgrade in each iteration, the controller type (9800-80, 9800-L, and so on), and the connectivity between the controller and the APs.

Device Upgrade Options

The following device upgrade options are available:

- NBAR Dynamic Protocol Pack Upgrade: Protocol packs are software packages that update the Network-Based Application Recognition (NBAR) engine protocol support on a device without replacing the Cisco software on the device. A protocol pack contains information on applications that are officially supported by NBAR, and are compiled and packed together.
- Field Programmable Upgrade: These are hardware programmable packages released by Cisco to upgrade the hardware programmable firmware. Hardware programmable package upgrade is necessary only when a system message indicates that one of the field programmable devices needs an upgrade or when a Cisco technical support representative suggests an upgrade.

Upgrade the controller software using GUI

The purpose of this task is to guide users through the process of upgrading the controller software via the graphical user interface (GUI), ensuring a seamless transition to the latest version.

- Ensure device configurations remain intact during the upgrade process.
- Provide an option for users to select their preferred upgrade and transport modes.

Before you begin

Clean up the old installation files using the **Remove Inactive Files** link.

- Software Maintenance Upgrade
- AP Service Package
- AP Device Package

Procedure

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

Step 2 Choose an option from the **Upgrade Mode** drop-down list:

- **INSTALL**: The Install mode uses a package-provisioning file named *packages.conf* in order to boot a device.
- **BUNDLE**: The Bundle mode uses monolithic Cisco IOS images to boot a device. The Bundle mode consumes more memory than the Install mode because the packages are extracted from the bundle and copied to RAM.

Note
You get to view the **Destination** field only for BUNDLE upgrade mode.

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)**.

Table 1: Transport Type Options

If...	Then...
You choose **TFTP** as the **Transport Type**	Enter the **Server IP Address** of the TFTP server that you want to use. Also, enter the complete **File Path**. In controllers, the IP TFTP source is mapped to the service port by default.
You choose **SFTP** as the **Transport Type**	Enter the **Server IP Address** of the SFTP server that you want to use. Also, enter the **SFTP Username**, **SFTP Password**, and the complete **File Path**.
You choose **FTP** as the **Transport Type**	Enter the **Server IP Address** of the FTP server that you want to use. Also, enter the **FTP Username**, **FTP Password**, and the complete **File Path**.
You choose **Device** as the **Transport Type**	Choose the **File System** from the drop-down list. In the **File Path** field, browse through the available images or packages from the device and select one of the options, and click **Select**.
You choose **Desktop (HTTPS)** as the **Transport Type**	Choose the **File System** from the drop-down list. In the **Source File Path** field, click **Select File** to select the file, and click **Open**.

Step 4 Click **Download & Install**.

Step 5 To boot your device with the new software image, click **Save Configuration & Activate**.

Step 6 Click **Commit** after the device reboots to make the activation changes persistent across reloads.

Note

For 17.4 and later releases, this step is mandatory for the upgrade to be persistent. If you do not click **Commit**, the auto-timer terminates the upgrade operation after 6 hours, and the controller reverts back to the previous image.

After completing the upgrade, the controller runs the latest version of the software, maintaining continuity and performance enhancements brought by the new update.

Upgrade the controller software (CLI)

The purpose of this task is to update the controller software to the latest version using CLI to ensure optimal performance and security.

Before you begin

- Determine the Cisco IOS release that is currently running on your controller, and the filename of the system image using the **show version** command in user EXEC or privileged EXEC mode.
- Clean up the old installation files using the **install remove inactive** command.
- Use the **show version | include Installation mode** to verify the boot mode.

Note We recommend that you use install mode for the software upgrade.

For steps on converting the device from bundle-mode to install-mode, see Converting from Bundle-Mode to Install-Mode.

Procedure

Step 1 Download the software from Cisco.com: https://software.cisco.com/download/home/286322524

- Click IOS XE Software link.
- Select the release number you want to install, for example Gibraltar-16.12.3.

  Note
  Cisco recommended release is selected by default. For release designation information, see: https://software.cisco.com/download/static/assets/i18n/reldesignation.html?context=sds

- Click **Download**.

Step 2 Copy the new image to flash using the command: **copy tftp:***image* **flash:**

Step 3 Verify that the image has been successfully copied to flash using the command: **dir flash:**

Step 4 Upgrade the software by choosing an upgrade process from the options that are currently supported.

For a list of upgrade options, see Software Upgrade Options, on page 2.

Upon completing this task, the controller software will be successfully upgraded to the latest version, enhancing device functionality and security.

Convert from bundle-mode to install-mode

Use the procedure given below to boot in install-mode:

Before you begin

- Clean up the old installation files using the command **install remove inactive**
- Verify the boot mode using the command: **show version | include Installation mode**
- Download the software image from Cisco.com.

  For steps on how to download the software, see *Upgrading the Controller Software (CLI)*

Procedure

Step 1 Copy the new image to flash using the command: **copy tftp:***image* **flash:**

```
Device# copy tftp://xx.x.x.x//C9800-universalk9_wlc.xx.xx.xx.SSA.bin flash:

Destination filename [C9800-universalk9_wlc..xx.xx.xx..SSA.bin]?
Accessing tftp://xx.x.x.x//C9800-universalk9_wlc.xx.xx.xx.SSA.bin...
Loading /C9800-universalk9_wlc.xx.xx.xx.SSA.bin from xx.x.x.x (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]
601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

Step 2 Verify that the image has been successfully copied to flash using the command: **dir flash:**

```
Device# dir flash:*.bin

Directory of bootflash:/*.bin

On Active

Directory of bootflash:/

   12  -rw-  1231746613  Jun 11 2020 23:15:49 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200611_101837.SSA.bin
   17  -rw-  1232457039   Jun 9 2020 21:14:40 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200609_031801.SSA.bin
   21  -rw-  1219332990  Jun 10 2020 02:06:14 +00:00
C9800-universalk9_wlc.BLD_V173_THROTTLE_LATEST_20200608_003622_V17_3_0_183.SSA.bin
   18  -rw-  1232167230   Jun 8 2020 02:42:22 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200607_002322.SSA.bin
24811823104 bytes total (16032391168 bytes free)


On Standby
Directory of stby-bootflash:/*.bin

Directory of stby-bootflash:/

   18  -rw-  1232167230   Jun 8 2020 02:42:22 +00:00
```

```
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200607_002322.SSA.bin
   20  -rw-  1231746613  Jun 11 2020 23:15:49 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200611_101837.SSA.bin
   17  -rw-  1232457039   Jun 9 2020 21:14:40 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200609_031801.SSA.bin
   16  -rw-  1219332990  Jun 10 2020 02:06:14 +00:00
C9800-universalk9_wlc.BLD_V173_THROTTLE_LATEST_20200608_003622_V17_3_0_183.SSA.bin
26462998528 bytes total (17686335488 bytes free)
```

Step 3 Set the boot variable to **bootflash:packages.conf**.

```
Device(config)# boot sys flash bootflash:packages.conf
```

Step 4 Save your changes by entering this command: **write memory**.

```
Device(config)# write memory
```

Note
For this configuration, the mode changes from enable to config mode.

Step 5 Verify whether the boot variable is set to bootflash:packages.conf using the command: **show boot**

```
Device# show boot

BOOT variable = bootflash:packages.conf,12;
CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x2102

Standby BOOT variable = bootflash:packages.conf,12;
Standby CONFIG_FILE variable =
Standby BOOTLDR variable does not exist
Standby Configuration register is 0x2102
```

Step 6 Move the device from bundle-mode to install-mode using the command: **install add file** *image.bin location* **activate commit**

```
Device# install add file bootflash:C9800-universalk9_wlc.xx.xx.xx.SPA.bin activate commit

install_add_activate_commit: START Thu Dec 6 15:43:57 UTC 2018
Dec 6 15:43:58.669 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin to the selected
chassis
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
[1] Add package(s) on chassis 1
[1] Finished Add on chassis 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: xx.xx.xx.216
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/C9800-xx-rpboot.xx.xx.xx.SPA.pkg
```

```
/bootflash/C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg
This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on chassis 1
--- Starting list of software package changes ---
Old files list:
Removed C9800-xx-mono-universalk9.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
Removed C9800-xx-rpboot.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
New files list:

Added C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg
Added C9800-xx-rpboot.xx.xx.xx.SPA.pkg
Finished list of software package changes
[1] Finished Activate on chassis 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
[1] Commit package(s) on chassis 1
[1] Finished Commit on chassis 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Thu Dec 6 15:49:21 UTC 2018
Dec 6 15:49:21.294 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
```

Note

The system reloads automatically after executing the **install add file activate commit** command. You do not have to manually reload the system.

If upgrade fails, cleanup is required before attempting the upgrade procedure again. An upgrade failure may occur due lack of disk space, validation failure of extracted image, system crashes, and so on. Should a system failure occurs during upgrade process, wait till the system is back in service and check the system image version.

- If it is a new image, check for the stability and functionality of the system, and decide whether to commit and complete the upgrade procedure or discard the upgrade procedure.
- If it is a new image, use the cleanup procedure and reattempt the upgrade procedure.

Step 7 Click **yes** to all the prompts.

Step 8 Verify the boot mode using the command: **show version**

```
Device# show version | in Installation mode is

Installation mode is INSTALL
```

Copy a WebAuth tar bundle to the standby controller (GUI)

Ensure the standby controller receives the WebAuth tar bundle to maintain seamless high-availability functionality.

Copy a WebAuth tar bundle to the standby controller in a high-availability configuration.

Procedure

Step 1 Go to **Administration** , select **Management** , and then select **Backup and Restore**.

Step 2 Select **To Device** from the **Copy** drop-down list.

Step 3 Select **WebAuth Bundle** from the **File Type** drop-down list.

Step 4 Select **TFTP** , **SFTP** , **FTP** , or **HTTP** from the **Transfer Mode** drop-down list.

The required values for the **Server IP Address** and **File Path** fields depend on the selected transfer mode.

- **TFTP**
  - **IP Address (IPv4/IPv6)** : Enter the server IP address (IPv4 or IPv6) of the TFTP server you want to use.
  - **File Path**: Enter the file path. Start the file path with a slash, such as */path*.
  - **File Name**: Enter a file name.

    Do not use spaces in the file name. Use underscores and hyphens. Make sure the file name ends with .tar, for example, webauthbundle.tar.

- **SFTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the SFTP server that you want to use.
  - **File Path**: Enter the file path. Start the file path with a slash, such as */path*.
  - **File Name**: Enter a file name.

    Do not use spaces in the file name. Only underscores and hyphens are allowed. Make sure the file name ends with .tar, for example, webauthbundle.tar.
  - **Server Login Username**: Enter the SFTP server login user name.
  - **Server Login Password**: Enter the SFTP server login passphrase.

- **FTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the FTP server that you want to use.
  - **File Path**: Enter the file path. Start the file path with a slash, such as */path* .
  - **File Name**: Enter a file name.

Do not use spaces in the file name. Only underscores and hyphens are allowed. Make sure the file name ends with .tar, for example, webauthbundle.tar.

- **Logon Type**: Choose **Anonymous** or **Authenticated** . If you choose **Authenticated**, these fields are activated:
  - **Server Login Username**: Enter the FTP server login user name.
  - **Server Login Password**: Enter the FTP server login passphrase.

- **HTTP**
  - **Source File Path**: Click **Select File** to select the configuration file, and click **Open**.

Step 5 Click the **Yes** or **No** radio button to back up the existing startup configuration to Flash.

Save the configuration to Flash to propagate the WebAuth bundle to other members, including the standby controller.

Step 6 Click **Download File**.

The WebAuth tar bundle is successfully copied to the standby controller, ensuring high-availability readiness.