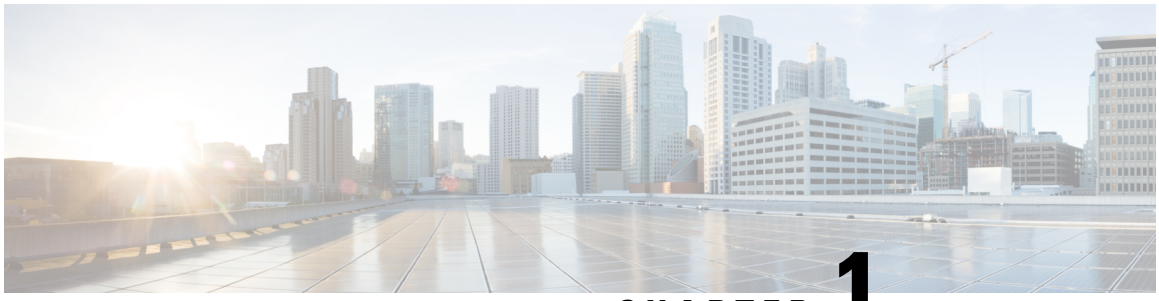
Cisco Catalyst SD-WAN Upgrade Guide

First Published: 2026-06-15

Last Modified: 2026-07-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Upgrade and Downgrade Device Software

Upgrade considerations

Describes the issues to consider when planning to upgrade the software of a device operating in a Cisco Catalyst SD-WAN network.

Software image to use from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

From Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, use the universalk9 image to deploy both Cisco IOS XE Catalyst SD-WAN and Cisco IOS XE on Cisco IOS XE Catalyst SD-WAN devices.

From Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, UCMK9 image is not available.

Upgrade considerations: Multirate interfaces

Describes the multirate interface issues to consider when planning to upgrade the software of a device operating in a Cisco Catalyst SD-WAN network.

The following Cisco IOS XE Catalyst SD-WAN devices support multirate interfaces and support the 1GE small form-factor pluggable (SFP) (optical and CU) and 10GE SFP+ (optical and CU) modules on their 10G interfaces ports:

- Cisco ASR 1001-HX Router
- Cisco Catalyst 8500-12X4QC
- Cisco Catalyst 8500-12X

Upgrade considerations: Autonegotiation

Describes autonegatiation issues to consider when planning to upgrade the software of a device operating in a Cisco Catalyst SD-WAN network.

These considerations apply to auto-negotiation in both Catalyst SD-WAN and non-SD-WAN modes of the router models that support multirate interfaces:

Before upgrading

Before upgrading to Cisco Catalyst SD-WAN Manager Release 20.12.1 or Cisco IOS XE Catalyst SD-WAN Release 17.12.1a or later releases, contact Cisco TAC to check and drop any non-compatible indexes. Non-compatible old index can impact successful upgrade to newer version.

CLI configuration

For releases before Cisco IOS XE 17.6.1a, auto-negotiation can be configured using the CLI.

10G interface with a 10GE SFP+ module

For releases before Cisco IOS XE 17.6.1a, if you use the CLI or Cisco Catalyst SD-WAN to reboot a device with a 10G interface that includes a 10GE SFP+ module, that interface will not come up. In this situation, use Cisco Catalyst SD-WAN or the CLI to configure **`no negotiation auto`** for the interface, then reboot the device.

Feature templates

From Cisco IOS XE Release 17.6.3a, **`auto neg`** values for auto-negotiation are pushed to 10G interfaces on supported devices through feature templates. Ensure that you know which SFP module is on which 10G interface on a device so that you can properly configure the feature template.

Restriction for the negotiation auto CLI command

On software releases up to Cisco IOS XE Release 17.6.3a, the **negotiation auto** command is not supported on a 10G interface that includes a 10GE SFP+ module.

Restriction for the no negotiation auto CLI command

On software releases up to Cisco IOS XE Release 17.6.3a, the **no negotiation auto** command with the default OFF option must be sent through a feature template to all 10G interfaces that include a 10GE SFP+ module. Otherwise, the template push fails.

Support for 10G interface with 10 GE SFP+ module

If you upgrade to Cisco IOS XE Release 17.6.3a from a release in which auto-negotiation was enabled on a 10G interface that includes a 10GE SFP+ module, that interface will not come up. In this situation, use the CLI to configure **no negotiation auto** for the interface after the upgrade completes.

From Cisco IOS XE Release 17.6.4 onwards, the **negotiation auto** command is supported on a 10G interface with 10 GE SFP+ module. In this scenario, in the output of **show interface Tengig** *x*/*y*/*z*, the link type is force-up regardless of **negotiation auto/no negotiation auto** configuration. The same is applicable when the configurations are pushed through Cisco SD-WAN Manager template.

Preparation for 10G interfaces with 10GE SFP+ module

Before upgrading to Cisco IOS XE Release 17.6.3a, use a feature template, a CLI add-on feature templates, or the CLI to apply the **no negotiation auto** command to all 10G interfaces that include a 10GE SFP+ module.

Support for 10G interface with 1GE Fiber and Copper SFP

From Cisco IOS XE Release 17.6.4 onwards, the **negotiation auto** command is supported on a 10G interface that includes a 1GE Fiber and Copper SFP.

ASR 1001-HX multirate support

For an ASR 1001-HX platform, multirate is supported only on the last four ports of bay1 8X10G/1G.

Redeploy configuration after upgrade

After upgrading a device, configurations for new features in the updated version are not applied automatically. To enable these new features, you must manually redeploy the configuration group or device template.

Upgrade considerations: Cisco 8000 Series Routers

Describes the issues to consider when planning to upgrade the software of C8300 and C8500L-8S4X routers operating in a Cisco Catalyst SD-WAN network.

10G interface with 10GE SFP+ module

- From Cisco IOS XE Release 17.15.1 and later, the **negotiation auto** command is supported on a 10G interface that includes a 10GE SFP+ module.
- From Cisco IOS XE Release 17.15.1 and later, on a 10G interface that includes a 10GE SFP+ module, the output of **show interface Tengig** *x*/*y*/*z* always shows the link type as force-up, regardless of **negotiation auto**/**no negotiation auto** configuration. The same is applicable when the configurations are pushed through Cisco SD-WAN Manager template.

Dual rate ports

The command **show running config** does not display **no neg auto** for dual rate ports in Controller mode. Where as **show sdwan running-config** shows **no neg auto**. In case of **neg auto** configuration, the command **show interfaces** *interface-num* always displays for dual rate ports with 10G optics.

Autonegotiation

Ensure that the negotiation configuration matches with the peer device interface settings. If there is a mismatch in the interface settings, the interface may go down.

Table 1: Cisco 8300 Series platforms: Autonegotiation defaults by platform and small form-factor pluggable (SFP) module type

SFP module type	Default autonegotiation	Default speed	Default duplex
1G Copper	On	1000 M	Full
1G Optical	On	1000 M	Full
10G Optical	On	10,000 M	Full

Table 2: Cisco 8500 Series platforms: Autonegotiation defaults by platform and small form-factor pluggable (SFP) module type

SFP module type	Default autonegotiation	Default speed	Default duplex
1G Copper	Off	1000 M	Full
1G Optical	Off	1000 M	Full
10G Optical	Off	10,000 M	Full

Upgrading devices

Provides information about upgrading devices using SD-WAN Manager or CLI commands.

Use these procedures to upgrade device software:

- Upgrade using SD-WAN Manager, on page 5
- Upgrade using CLI commands, on page 5

Supported device upgrades

Describes supported upgrade paths for various platforms.

Cisco CSR1000V and Cisco ISRv routers

You can upgrade to...	from these releases
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Cisco IOS XE SD-WAN 17.3.1a or later Cisco IOS XE SD-WAN 17.2.2 or later Cisco IOS XE SD-WAN 16.12.4a or later **Note** • To upgrade a Cisco CSR1000V or Cisco ISRv router to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a from a release not listed here requires first upgrading to one of these releases. • Upgrading a Cisco CSR1000V or Cisco ISRv router to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a includes upgrading to the Cisco Catalyst 8000V.
Cisco IOS XE 17.3.x	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco IOS XE Release 17.2.1v Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

You can upgrade to...	from these releases
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

All routers supported by Cisco Catalyst SD-WAN except Cisco CSR1000V, Cisco ISRv, and Cisco Catalyst 8000V

You can upgrade to...	from these releases
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Cisco IOS XE SD-WAN 17.3.1a or later Cisco IOS XE SD-WAN 17.2.1 or later Cisco IOS XE SD-WAN 16.12.4a or later
Cisco IOS XE 17.3.x	
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Cisco IOS XE SD-WAN 16.12.x Cisco IOS XE SD-WAN 16.11.x Cisco IOS XE SD-WAN 16.10.x Cisco IOS XE SD-WAN 16.9.x

Upgrade using SD-WAN Manager

Using SD-WAN Manager to upgrade devices keeps devices and the SD-WAN Control Components synchronized.

Procedure

From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.

Upgrade using CLI commands

We recommend using Cisco SD-WAN Manager to upgrade. This keeps devices and SD-WAN Manager synchronized. If it is necessary to upgrade using the CLI, use the procedure here.

Before you begin

Back up configuration files. Without first backing up, the device loses its configuration during the upgrade. You can use these commands to back up the Cisco IOS XE Catalyst SD-WAN configuration and running configuration:

```
show sdwan running-config | redirect bootflash:/sdwan/sdwan.cli
show running-config | redirect bootflash:/sdwan/ios.cli
```

Procedure

Step 1 Download the software image for your device from https://software.cisco.com .

Step 2 Upload the image to the device.

Step 3 Install the new software.

Example:

```
Device# request platform software sdwan software install bootflash:/isr4300-universalk9.17.2.1.SPA.bin
```

Step 4 Activate the software. The device reloads when the activation is complete.

Example:

```
Device# request platform software sdwan software activate 17.2.01r.9.3
```

Step 5 Verify that the software is activated.

Example:

```
Device# show sdwan software

VERSION      ACTIVE DEFAULT PREVIOUS CONFIRMED TIMESTAMP
--------------------------------------------------------------------------------
16.12.1d.0.48 false  true   true     auto     2020-03-04T10:43:45-00:00
17.2.01r.9.3   true  false  false    user     2020-03-04T11:15:20-00:00

Total Space:388M Used Space:100M Available Space:285M
```

Step 6 Optionally, to ensure that the new version is preserved if a software reset is required, use the **request platform software sdwan software set-default** command.

Example:

```
Device# request platform software sdwan software set-default 17.2.01r.9.3
```

Step 7 Verify the upgrade using **request platform software sdwan software upgrade-confirm**.

Example:

```
Device# request platform software sdwan software upgrade-confirm
```

Note
From the 17.6.1 release, you cannot perform another install, or activate or deactivate an operation for an image or a Software Maintenance Update (SMU), when the upgrade-confirm function is pending for an existing operation.

Downgrading a device from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later releases

Describes procedures for downgrading device software.

Use these procedures to downgrade device software:

- Downgrade a Cisco IOS XE Catalyst SD-WAN device to a previously installed software image, on page 7
- Downgrade a Cisco IOS XE Catalyst SD-WAN device to an older software image, on page 8

Supported device downgrades

Describes behavior in device downgrade scenarios.

Downgrade behavior

When you downgrade from...	to these releases	Behavior
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r(universalk9) in controller mode	Cisco IOS XE SD-WAN Release 16.12 and earlier (ucmk9)	Device boots up with ucmk9 image and configuration is restored if the uckm9 image was previously installed on the device. Downgrading to a fresh install of old image versions brings the device to Day 0 configuration. To proceed, use the **clean** option at activation.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r (universalk9) in autonomous mode	Cisco IOS XE Release 17.1.1 and earlier (universalk9)	Device boots up with universalk9 image and configuration is restored.

Downgrade a Cisco IOS XE Catalyst SD-WAN device to a previously installed software image

Downgrade a Cisco IOS XE Catalyst SD-WAN device to an earlier software image that is currently installed on the device, using CLI commands.

Procedure

Step 1 Display the currently installed images.

Example:

```
Device# show sdwan software

Example:
VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
16.10.400.0.0    false   true     true      auto       2019-11-20T04:40:05-00:00
17.3.1.0.102822  true    false    false     auto       2020-07-31T11:01:22-00:00
```

Step 2 Activate the image. This resets the device, deleting any existing configuration. The device starts in day zero configuration.

```
Device# request platform software software activate desired-build
```

Example:

```
Device# request platform software software activate 16.10.400.0.0
```

Downgrade a Cisco IOS XE Catalyst SD-WAN device to an older software image

Download an earlier software image and downgrade a Cisco IOS XE Catalyst SD-WAN device to an earlier software image, using CLI commands.

Procedure

Step 1 Display the currently installed images.

Example:

```
Device# show sdwan software

Example:
VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
16.10.400.0.0    false   true     true      auto       2019-11-20T04:40:05-00:00
17.3.1.0.102822  true    false    false     auto       2020-07-31T11:01:22-00:00
```

Step 2 If necessary, remove an existing software image to provide space for loading a new software image.

```
Device# request platform software sdwan software remove previous-installed-build
```

Example:

```
Device# request platform software sdwan software remove 16.10.400.0.0
```

Step 3 Download the software image for the downgrade and copy it to the device bootflash.

Step 4 Install the downloaded image.

```
Device# request platform software sdwan software install bootflash:/desired-build
```

Example:

```
Device# request platform software sdwan software install
bootflash:/isr1100be-universalk9.17.02.01a.SPA.bin
```

Step 5 Display the currently installed images, which now include the new image.

Example:

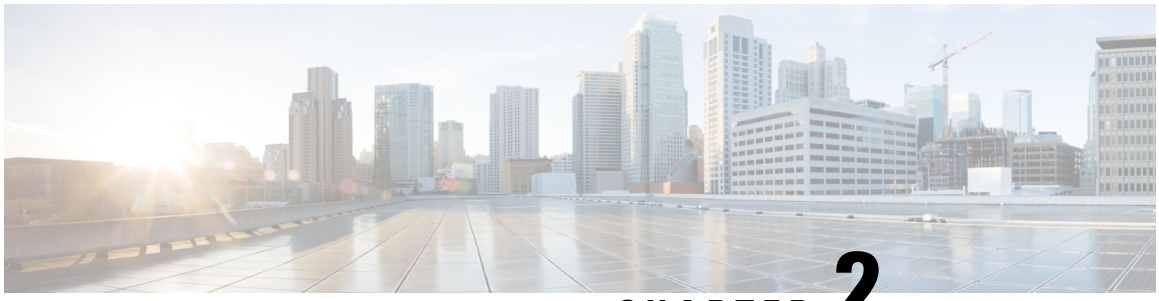
```
Device# show sdwan software
VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
17.02.01a.0.211  false    true     true      auto       2020-03-30T09:34:04-00:00
```

Step 6 Activate the new image. This resets the device, deleting any existing configuration. The device starts in day zero configuration.

```
Device# request platform software sdwan software activate desired-build clean
```

Example:

```
Device# request platform software sdwan software 17.02.01a.0.211 clean
```



CHAPTER 2

Manage Software Upgrade and Repository

Manage Software Upgrade and Repository

Table 3: Feature History

Feature Name	Release Information	Description
Software Upgrade Using a Remote Server	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enables you to upgrade device or controller software using software images stored on a remote server. The feature enables you to register a remote server with Cisco SD-WAN Manager, and add locations of software images on the remote server to the Cisco SD-WAN Manager software repository. When you upgrade device or controller software, the device or controller can download the new software image from the remote server. This feature also improves the listing of images available in the repository. When two or more images have the same version but different filenames, each image is listed as a separate entry.

Feature Name	Release Information	Description
Device version compliance in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.x Cisco Catalyst SD-WAN Manager Release 20.18.1	

Feature Name	Release Information	Description
		The Device Version Compliance feature in Cisco SD-WAN Manager ensures device compatibility when upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1. The Cisco Catalyst SD-WAN Manager Release 20.18.1 supports devices up to N-2 long-lived releases and does not support older versions in the Cisco Catalyst SD-WAN overlay. This feature implements the following key aspects: • Upgrade Blocking: Prevents Cisco SD-WAN Manager upgrades through the user interface if the overlay contains devices with software versions older than N-2. • Post-Upgrade Notification: After a Cisco SD-WAN Manager software upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager flags incompatible devices in the overlay through compliance banners and alarms. • Removal of End-of-Life (EOL) Platforms from ZTP Settings: Removes unsupported device families from the Zero Touch Provisioning settings page in Cisco SD-WAN Manager. • Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition: Changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system when they are added

Feature Name	Release Information	Description
		to and recognized by Cisco SD-WAN Manager. This change removes the Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers migration menu in Cisco SD-WAN Manager when Cisco IOS XE operating system is detected.

Information about software upgrade

Use the Software Upgrade window to download new software images and to upgrade the software image running on a Cisco Catalyst SD-WAN device.

From a centralized Cisco SD-WAN Manager, you can upgrade the software on Cisco Catalyst SD-WAN devices in the overlay network and reboot them with the new software. You can do this for a single device or for multiple devices simultaneously.

When you upgrade a group of Cisco Catalyst SD-WAN Validator, Cisco Catalyst SD-WAN Controllers, and Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices in either a standalone or Cisco SD-WAN Manager cluster deployment, the software upgrade and reboot is performed first on the Cisco Catalyst SD-WAN Validator, next on the Cisco Catalyst SD-WAN Controller, and finally on the Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices. Up to 40 Cisco IOS XE Catalyst SD-WAN devices or Cisco vEdge devices can be upgraded and rebooted in parallel, depending on CPU resources.

Introduced in the Cisco vManage Release 20.8.1, the software upgrade workflow feature simplifies the software upgrade process for the Cisco Catalyst SD-WAN edge devices through a guided workflow and displays the various device and software upgrade statuses. For more information on creating a Software Upgrade Workflow, see Software Upgrade Workflow.

Note

- You cannot include Cisco SD-WAN Manager in a group software upgrade operation. You must upgrade and reboot the Cisco SD-WAN Manager server by itself.
- You can create a software upgrade workflow only for upgrading the Cisco Catalyst SD-WAN edge devices.
- It is recommended that you perform all software upgrades from Cisco SD-WAN Manager rather than from the CLI.
- For software compatibility information, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, devices within the same site are upgraded sequentially. If a device fails, subsequent upgrades are skipped.

Prior to Cisco Catalyst SD-WAN Manager Release 20.18.1, devices within the same site are also upgraded sequentially. Even if a device fails, the remaining devices continue to upgrade.

The upgrade will proceed sequentially only if the certificate status of all devices with the same site ID is valid. If any device has an invalid certificate status, upgrades will occur in parallel.

Device version compliance

Device version compliance is a policy that

- ensures compatibility of network devices with Cisco SD-WAN Manager upgrades,
- supports devices in the overlay up to N-2 long-lived releases, and
- does not support devices older than this version in the overlay after an upgrade.

The release versions referenced in this policy are defined as follows:

- N: Represents the current Cisco SD-WAN Manager release (for example, Cisco Catalyst SD-WAN Manager Release 20.18.x).
- N-1: Refers to the prior long-lived release (for example, Cisco Catalyst SD-WAN Manager Release 20.15.x).
- N-2: Refers to the long-lived release two versions prior (for example, Cisco Catalyst SD-WAN Manager Release 20.12.x).

If you onboard a new device of any version, the device is still supported. However, after onboarding, this device will be flagged with a red banner in Cisco SD-WAN Manager, indicating that an upgrade is required.

Cisco ISR 4000 series devices (ISR4331, ISR4431, ISR4451-X, ISR4321, ISR4351, ISR4221 and ISR4221X) that are running version 17.12.x are marked as non-compliant in the device compliance dashboard and API responses as per N-2 supported version rule. However, starting from Cisco Catalyst SD-WAN Manager Release 26.1.1.1, if you are using Cisco ISR 4000 series devices version greater than or equal to SD-WAN Manager 17.12.6, it will not be marked as non-compliant. You can have greater than or equal to17.12.6 ISR 4000 devices in Cisco SD-WAN Manager version greater than or equal to SD-WAN Manager 26.1.x and later.

Upgrade behavior

This feature changes the upgrade process depending on how the upgrade is initiated:

When a user initiates an upgrade to a newer Cisco SD-WAN Manager version (e.g., Cisco Catalyst SD-WAN Manager Release 20.18.x) through the UI, the upgrade is blocked if the overlay contains devices with software versions older than N-2 (e.g., Cisco Catalyst SD-WAN Manager Release 20.12.x).

For instance, if Cisco SD-WAN Manager is on version Cisco Catalyst SD-WAN Manager Release 20.15.1 and devices are on Cisco IOS XE Catalyst SD-WAN Release 17.9.x, an upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.x will be blocked because the minimum supported device version for Cisco Catalyst SD-WAN Manager Release 20.18.x is Cisco Catalyst SD-WAN Manager Release 20.12.x. All devices in the

network must be on version Cisco IOS XE Catalyst SD-WAN Release 17.12.x or above for the upgrade to proceed.

If a user performs the upgrade via the CLI, the upgrade proceeds even if devices are older than N-2. However, Cisco SD-WAN Manager displays a banner indicating the presence of less than N-2 devices and recommends upgrading them.

Device compliance notifications

Cisco SD-WAN Manager uses two primary methods to flag incompatible devices. If a user performs any operations on devices running versions older than N-2, it may lead to unexpected errors or device operational failures.

Compliance messages

A message appears in Cisco SD-WAN Manager when incompatible devices are detected. This message recommends upgrading those devices. Clicking the message redirects the user to the **Compliance & Conflicts** page, which displays the device status and software version.

- Error: If devices are less than N-2 versions, an error message appears:

```
Incompatible software version detected. Click here for details.
```

- Error: If devices are on N-3 version, or if Cisco Catalyst SD-WAN Controller or Cisco Catalyst SD-WAN Validator are on N-1 or N-2 versions, an error message appears:
  - N-3 devices with N version of SD-WAN Controller or SD-WAN Validator:

```
Incompatible software versions between the Manager and WAN Edge have been
 detected. Upgrade the software immediately to avoid any disruptions.
```

  - N-3 devices with N-1 or lesser versions of SD-WAN Controller or SD-WAN Validator:

```
Incompatible software versions between the Manager and Controller, Validator
 and WAN Edge have been detected. Upgrade the software immediately to avoid
 any disruptions.
```

Out of compliance alarm

An alarm is raised in the **Alarm Details** page in Cisco SD-WAN Manager when devices running versions older than N-2 are detected in the overlay. Multiple alarms may be raised if device versions change.

If the list of out-of-compliance devices contains five or fewer entries, the **Probable Causes** section displays the device hostnames. For more than five devices, the **Probable Causes** section displays only the count of out-of-compliance devices.

Unsupported devices

Starting with the Cisco Catalyst SD-WAN Manager Release 20.18.x release, Cisco SD-WAN Manager removes unsupported device families from the Zero Touch Provisioning (ZTP) settings page. These platform families include:

- Cisco vEdge Cloud

- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ASR 1002-X Series Aggregation Services Routers
- Cisco vEdge devices

Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition

Cisco SD-WAN Manager changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system. As a result, Cisco SD-WAN Manager removes the Migration menu if it detects that a Cisco ISR 1100 and ISR 1100X Series Integrated Services Router is running Cisco IOS XE operating system. However, the Migration menu continues to be displayed for devices running Viptela operating system.

Restrictions for software upgrade

Upgrade only

The software upgrade process can only install a later release (upgrade) not an earlier release (downgrade). For example you can upgrade from 17.15.1 to 17.16.1.

Note When an edge device is upgraded to a newer SD-WAN release, new feature configurations introduced in the new release are not automatically applied to devices that were previously onboarded. The system preserves existing configuration intent, and new feature knobs become active only after an explicit template or after redeploying a configuration group.

Migration of the device configuration only when installing a release

A device migrates the current active configuration to another release only when installing the new release. If you have a release that is installed but out of sync with recent configuration changes, you can trigger a fresh migration of the current configuration. Uninstall the release that is out of sync, then re-install the release.

Reactivating an earlier release

A device can have more than one release installed, but only one release is active at a given time.

If a device is running release A (example: 17.15.1), you can install a later release B (example: 17.16.1). After you activate release B, the inactive release A keeps its configuration in the state when release A was last active. Configuration changes you make while release B is active do not affect the configuration stored with release A.

If you keep release A installed on the device and later reactivate release A, the device uses the stored configuration reflecting the state when release A was last active.

Device version compatibility

The following restrictions are the restrictions for device compatibility when upgrading Cisco SD-WAN Manager to Cisco Catalyst SD-WAN Manager Release 20.18.x:

Device software version support

Cisco Catalyst SD-WAN Manager Release 20.18.x supports devices running up to N-2 long-lived software releases. Devices running software versions older than N-2 are not supported in the Cisco Catalyst SD-WAN overlay. For more information, see Device version compliance, on page 16.

Upgrade blocking

Cisco SD-WAN Manager prevents upgrades through the user interface if the Cisco Catalyst SD-WAN overlay contains devices with software versions older than N-2. For more information, see the section Upgrade behavior in Device version compliance, on page 16.

Post-Upgrade notification

After a Cisco SD-WAN Manager software upgrade to Cisco Catalyst SD-WAN Manager Release 20.18.x, Cisco SD-WAN Manager flags incompatible devices in the overlay through compliance notifications and alarms. For more information, see the section Device compliance notifications in Device version compliance, on page 16.

Removal of End-of-Life platforms in Cisco SD-WAN Manager

Cisco SD-WAN Manager removes unsupported device families from the **Zero Touch Provisioning** settings page. For more information, see the section Unsupported devices in Device version compliance, on page 16.

Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition

Cisco SD-WAN Manager changes the default recognition of Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers from Viptela operating system to Cisco IOS XE operating system. This change helps prevent upgrade blocks for these devices and removes the migration menu when Cisco IOS XE operating system is detected. For more information, see the section Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers default operating system recognition in Device version compliance, on page 16.

Upgrade Virtual Image on a Device

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. To choose a device, check the check box for the desired device.
3. Click **Upgrade Virtual Image**.

   The **Virtual Image Upgrade** dialog box opens.
4. Choose **Manager** or **Remote Server - Manager**, as applicable.
5. From the **Upgrade to Version** drop-down list, choose the virtual image version to upgrade the device to.
6. Click **Upgrade**.

Upgrade the Software Image on a Device

Note

- This procedure does not enable downgrading to an older software version. If you need to downgrade, see Downgrade a Cisco vEdge Device to an Older Software Image in the Cisco Catalyst SD-WAN Getting Started Guide.
- If you want to perform a Cisco SD-WAN Manager cluster upgrade see, Upgrade Cisco SD-WAN Manager Cluster.
- Starting from Cisco vManage Release 20.11.1, before upgrading the configuration database, ensure that you verify the database size. We recommend that the database size is less than or equal to 5 GB. To verify the database size, use the following diagnostic command:

  request nms *configuration-db diagnostics*
- You may experience GUI upgrade failures due to incorrect database member count checks in single-node/cloud deployments. To resolve this, opt for the CLI upgrade method instead.

To upgrade the software image on a device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager** based on the type of device for which you wish to upgrade the software.
3. In the table of devices, select the devices to upgrade by selecting the check box on the far left.

Note While upgrading Cisco SD-WAN Manager clusters, select all the nodes of the cluster in the table.

4. Click **Upgrade**.
5. In the **Software Upgrade** slide-in pane, do as follows:
   a. Choose the server from which the device should download the image: **Manager**, **Remote Server**, or **Remote Server – Manager**.

Note

- The Remote Server option is introduced in Cisco vManage Release 20.7.1. If you chose **Remote Server**, ensure that the device can reach the remote server.
- Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:
  - User ID: a-z, 0-9, ., _, -
  - Password: a-z, A-Z, 0-9, _, *, ., +, =, %, -
  - URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -, :, /, @, ?, ~

Note Software images created before upgrading the Cisco SD-WAN Manager to version Cisco Catalyst SD-WAN Manager Release 20.18.1 lack platform family and version details. To use these images after the upgrade, edit them in **Maintenance** > **Software Repository** and add the required platform family and version information.

b. For **Manager**, choose the image version from the **Version** drop-down list.

c. For **Remote Server – Manager**, choose the **Manager OOB VPN** from the drop-down list and choose the image version from the **Version** drop-down list.

d. For **Remote Server**, configure the following:

Remote Server Name	Choose the remote server that has the image.
Image Filename	Choose the image filename from the drop-down list.

e. Check the **Activate and Reboot** check box.

If you do not check this check box, the software image is downloaded and installed on the device, but, the image is not activated, and the device is not rebooted. You must activate the image after the upgrade task is completed.

f. Click **Upgrade**.

The device restarts, using the new software version, preserving the current device configuration. The **Task View** page opens, showing the progress of the upgrade on the devices.

6. Wait for the upgrade process, which takes several minutes, to complete. When the **Status** column indicates Success, the upgrade is complete.

7. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** and view the devices.

8. Click **WAN Edge**, **Controller**, or **Manager** based on the type of device for which you wish to upgrade the software.

9. In the table of devices, confirm that the **Current Version** column for the upgraded devices shows the new version. Confirm that the **Reachability** column says reachable.

Note

- If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image. The configured time limit for all Cisco Catalyst SD-WAN devices to come up after a software upgrade is 5 minutes, except for Cisco vEdge devices, which have a default time of 12 minutes.
- If you upgrade the Cisco vEdge device software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first before upgrading the Cisco vEdge device software.
- When upgrading a Cisco CSR1000V or Cisco ISRv device to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a or later, the software upgrade also upgrades the device to a Cisco Catalyst 8000V. After the upgrade, on the Devices page, the **Chassis Number** and **Device Model** columns show the device as a Cisco CSR1000V or Cisco ISRv, but the device has actually been upgraded to a Cisco Catalyst 8000V. The reason for preserving the old name is to avoid invalidating licenses, and so on. To confirm that the device has been upgraded to a Cisco Catalyst 8000V, note that the **Current Version** column for the device indicates 17.4.1 or later.

Activate a New Software Image

Use this procedure to activate a software image that is currently loaded on a device. The software image may be a later release (upgrade) or earlier release (downgrade) than the current active release.

When you use Cisco SD-WAN Manager to upgrade the software image on a device, if you did not check the **Activate and Reboot** check box during the procedure, the device continues to use the existing configuration. Use this procedure to activate the upgraded software version.

Note To activate software for Cisco SD-WAN Manager while using a custom user group, you need read permission and read-write permissions to upgrade each software feature.

To activate a software image:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Choose **WAN Edge**, **Control Components**, or **Manager**.
3. For the desired device or devices, check the check box to choose the device or devices,
4. Click **Activate**. The **Activate Software** dialog box opens.
5. Choose the software version to activate on the device.
6. Click **Activate**. Cisco SD-WAN Manager reboots the device and activates the new software image.

If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image. The configured time limit for all Cisco Catalyst SD-WAN devices to come up after a software upgrade is 5 minutes, except for Cisco vEdge device, which have a default time of 12 minutes.

If the image activation fails, do not attempt to activate the image again. Remove the image from the device, then attempt to install and activate the image again.

Upgrade a CSP Device with a Cisco NFVIS Upgrade Image

Before you begin

Ensure that the Cisco NFVIS software versions are the files that have `.nfvispkg` extension.

Procedure

Step 1 From theCisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** > **WAN Edge**.

Step 2 Check one or more CSP device check boxes for the devices you want to choose.

Step 3 Click **Upgrade**. The **Software Upgrade** dialog box appears.

Step 4 Choose the Cisco NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.

Step 5 To automatically upgrade and activate with the new Cisco NFVIS software version and reboot the CSP device, check the **Activate and Reboot** check box.

If you don't check the **Activate and Reboot** check box, the CSP device downloads and verifies the software image. However, the CSP device continues to run the old or current version of the software image. To enable the CSP device to run the new software image, you must manually activate the new Cisco NFVIS software version by choosing the device again and clicking the **Activate** button in the **Software Upgrade** window.

Step 6 Click **Upgrade**.

The **Task View** window displays a list of all running tasks along with total number of successes and failures. The window periodically refreshes and displays messages to indicate the progress or status of the upgrade. You can easily access the software upgrade status window by clicking the **Task View** icon located in the Cisco SD-WAN Manager toolbar.

Note
If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happens in a sequence.

Note
The **Set the Default Software Version** option isn't available for the Cisco NFVIS images.

The CSP device reboots and the new NFVIS version is activated on the device. This reboot happens during the **Activate** phase. The activation can either happen immediately after upgrade if you check the **Activate and Reboot** check box, or by manually clicking **Activate** after choosing the CSP device again.

To verify if CSP device has rebooted and is running, use the task view window. Cisco SD-WAN Manager polls your entire network every 90 seconds up to 30 times and shows the status on th task view window.

Note You can delete a Cisco NFVIS software image from a CSP device if the image version isn't the active version that is running on the device.

Delete a Software Image

To delete a software image from a Cisco Catalyst SD-WAN device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
3. Choose one or more devices from which to delete a software image.
4. Click the **Delete Available Software**.

   The **Delete Available Software** dialog box opens.
5. Choose the software version to delete.
6. Click **Delete**.

Set the Default Software Version

You can set a software image to be the default image on a Cisco Catalyst SD-WAN device. Performing this operation overwrites the factory-default software image, replacing it with an image of your choosing. It is recommended that you set a software image to be the default only after verifying that the software is operating as desired on the device and in your network.

In case of error, see Error message during software upgrade or setting default software version.

To set a software image to be the default image on a device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
3. Choose one or more devices by checking the check box for the desired device or devices.
4. Click **Set Default Version**.

   The **Set Default Version** dialog box opens.
5. From the **Version** drop-down list, choose the software image to use as the default for the chosen device or devices.
6. Click **Set Default**.

Export Device Data in CSV Format

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Control Components**, or **Manager**.
3. Choose one or more devices by checking the checkbox for the desired device or devices.
4. Click the download icon.

Cisco SD-WAN Manager downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your brower's default download location and is named `Software_Upgrade.csv`

View Log of Software Upgrade Activities

1. From the Cisco SD-WAN Manager toolbar, click the **Tasks** icon.

   Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

2. Click the arrow to see details of a task. Cisco SD-WAN Manager opens a status window displaying the status of the task and details of the device on which the task was performed.

Manage Software Repository

Register Remote Server

Register a remote server with Cisco SD-WAN Manager so that you can add locations of software images on the remote server to the Cisco SD-WAN Manager software repository and upgrade device or controller software using these software images. In multitenant Cisco Catalyst SD-WAN deployment, only the provider can register a remote server and perform software upgrade using images on the remote server.

When Cisco Catalyst SD-WAN device is running on 17.15.1 release and if remote FTP server is configured with non-standard port, you cannot upgrade the device as you cannot download the image that is using non-standard ports. You must reconfigure FTP server to use standard ports to upgrade.

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Add Remote Server**.
3. In the **Add Remote Server** slide-in page, configure the following:

Server Info	• **Server Name**: Enter a name for the server. • **Server IP or DNS Name**: Enter the IP address or the DNS name of the server. • **Protocol**: Choose HTTP, FTP, or SCP. • **Port**: Enter the access port number.
Credentials	• **User ID**: Enter the user ID required to access the server. The username can contain only the following characters: a-z, 0-9, ., _, and -. • **Password**: Enter the password required to access the server. The password can contain only the following characters: a-z, A-Z, 0-9, _, *, ., +, =, %, and -. **Note** Special characters such as /, ?, :, @, and SPACE, which are used in URLs and are needed for proper parsing of fields so files can be fetched properly with the relevant protocol, are not supported in the username and the password. The use of the valid characters is supported starting from Cisco vManage Release 20.9.1.

Image Info	• **Image Location Prefix**: Enter the folder path where the uploaded images must be stored. For SCP, use the absolute directory path as the **Image Location Prefix**; for FTP or HTTP, use the relative path from the home directory. • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN

4. Click **Add** to add the remote server.

Enable devices to use a remote repository server

See Enable Software Updates by a Remote Repository Server.

Manage Remote Server

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. For the desired remote server, click **…**
3. To view the remote server settings, click **View Details**.
4. To edit the remote server settings, click **Edit**. Edit any of the following settings as necessary and click **Save**.

Note You cannot edit the remote server settings if you have added locations of any software images on the remote server to the Cisco SD-WAN Manager software repository. If you wish to edit the remote server settings, remove the software image entries from the software repository and then edit the settings.

Server Info	• **Server Name**: Enter a name for the server. • **Server IP or DNS Name**: Enter the IP address or the DNS name of the server. • **Protocol**: Choose HTTP, FTP, or SCP. • **Port**: Enter the access port number.
Credentials	• **User ID**: Enter the user ID required to access the server. The username can contain only the following characters: a-z, 0-9, ., _, and -. • **Password**: Enter the password required to access the server. The password can contain only the following characters: a-z, A-Z, 0-9, _, *, ., +, =, %, and -. **Note** Special characters such as /, ?, :, @, and SPACE, which are used in URLs and are needed for proper parsing of fields so files can be fetched properly with the relevant protocol, are not supported in the username and the password. The use of the valid characters is supported starting from Cisco vManage Release 20.9.1.

Image Info	• **Image Location Prefix**: Enter the folder path where the uploaded images must be stored. For SCP, use the absolute directory path as the **Image Location Prefix**; for FTP or HTTP, use the relative path from the home directory. • **VPN**: Enter the VPN ID, either the transport VPN, management VPN, or service VPN.

5. To delete the remote server, click **Remove**. Confirm that you wish to remove the remote server in the dialog box.

Note Before deleting a remote server, remove any entries for software images on the remote server that you have added to the Cisco SD-WAN Manager software repository.

Add Software Images to the Repository

Before you can upgrade the software on an edge device, Cisco Catalyst SD-WAN Controller, or Cisco SD-WAN Manager to a new software version, you need to add the software image to the Cisco SD-WAN Manager software repository. The repository allows you to store software images on the local Cisco SD-WAN Manager server or add locations of software images stored on a remote file server.

The Cisco SD-WAN Manager software repository allows you to store images in three ways:

- On the local Cisco SD-WAN Manager server, to be downloaded over a control plane connection: Here, the software images are stored on the local Cisco SD-WAN Manager server, and they are downloaded to the Cisco Catalyst SD-WAN devices over a control plane connection. The receiving device generally throttles the amount of data traffic it can receive over a control plane connection, so for large files, the Cisco SD-WAN Manager server might not be able to monitor the software installation on the device even though it is proceeding correctly.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, image uploads to the Cisco SD-WAN Manager repository fail when disk space limits are exceeded. In a cluster environment, the disk space is assessed on all nodes simultaneously. Even if one node is experiencing low disk space, the image upload will fail for all nodes.

When the total utilized space exceeds the limit, you may delete the existing image data on the local server. If this does not resolve the issue or if there is no existing image data to delete, please contact your network administrator for further assistance in freeing up disk space. The administrator can ensure that the total used space at /opt/data/ remains below 80%.

- On the local Cisco SD-WAN Manager server, to be downloaded over an out-of-band connection: Here, the software images are stored on the local Cisco SD-WAN Manager server, and they are downloaded to the Cisco Catalyst SD-WAN devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because

it bypasses any throttling that the device might perform and so the Cisco SD-WAN Manager server is able to monitor the software installation.

- On a remote server: From Cisco vManage Release 20.7.1, you can store software images on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the Cisco SD-WAN Manager server sends this URL to the Cisco Catalyst SD-WAN device, which establishes a connection to the file server to download the software images. In a multitenant Cisco Catalyst SD-WAN deployment, only the provider can register a remote server with Cisco SD-WAN Manager and add locations of software images on the remote server to the Cisco SD-WAN Manager repository.

Note Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:

- User ID: a-z, 0-9, ., _, -
- Password: a-z, A-Z, 0-9, _, *, ., +, =, %, -
- URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -, :, /, @, ?, ~

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Software Images**.
3. Click **Add New Software**.
4. Choose the location for the software image:

Note Store NFVIS upgrade images on the local Cisco SD-WAN Manager server.

   a. To store the software image on the local Cisco SD-WAN Manager server and have it be downloaded to Cisco Catalyst SD-WAN devices over a control plane connection, choose **Manager**. The **Upload Software to Manager** dialog box opens.
      1. Drag and drop the software image file to the dialog box or click **Browse** to select the software image from a directory on the local Cisco SD-WAN Manager server.
      2. Click **Upload** to add the image to the software repository.

   b. To store the image on a remote Cisco SD-WAN Manager server and have it be downloaded to Cisco Catalyst SD-WAN devices over an out-of-band management connection, choose **Remote Server - Manager**. The **Upload Software to Remote Server - Manager** dialog box opens.
      1. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on the Cisco SD-WAN Manager server that is in a management VPN (typically, VPN 512).
      2. Drag and drop the software image file to the dialog box, or click **Browse** to select the software image from a directory on the local Cisco SD-WAN Manager server.
      3. Click **Upload**.

c. If the software image is stored on a remote server, choose **Remote Server (preferred)**. The **Add New Software via Remote Server** slide-in pane appears. Before choosing this option, ensure that you have registered a remote server with Cisco SD-WAN Manager.

   1. Click **Image** to upload a new software image, or **SMU Image** to upload an SMU image. The default selection is **Image**.
   2. From the **Remote Server Name** drop-down list, choose the desired remote server.
   3. **Image Filename**: Enter the image filename, including the file extension. For an SMU image, the file extension must be `.smu.bin`.
   4. For an SMU image, enter the correct **SMU Defect ID** and choose the correct **SMU Type**. An incorrect defect ID or SMU type selection can cause the software upgrade to fail.
   5. Click **Save**.

View Software Images

From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Respository**.

The **Software Repository** window displays the images avaialable in the repository.

The **Software Version** column lists the version of the software image, and the **Controller Version** column lists the version of Cisco SD-WAN Control Components that is equivalent to the software version. The Cisco SD-WAN Control Components version is the minimum supported version. The software image can operate with the listed Cisco SD-WAN Control Components version or with a higher version.

The **Software Location** column indicates where the software images are stored, either in the repository on the Cisco SD-WAN Manager server, or in a repository in a remote location.

The **Available Files** column lists the names of the software image files.

The **Updated On** column shows when the software image was added to the repository.

The **...** option for a desired software version provides the option to delete the software image from the repository.

In Cisco vManage Release 20.6.1 and earlier releases, when two or more software images have the same software version but are uploaded with different filenames, the images are listed in a single row. The **Available Files** column lists the different filenames. This listing scheme is disadvantageous when deleting software images as the delete operation removes all the software images corresponding to a software version.

From Cisco vManage Release 20.7.1, when two or more software images have the same software version but are uploaded with different filenames, each software image is listed in a separate row. This enables you to choose and delete specific software images.

Add Virtual Images to the Repository

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. Click **Add New Virtual Image** and choose one of the following options:
   - **Remote Server (preferred)**: Choose this option to link to an image that has been uploaded to a remote server.

Note Before choosing this option, ensure that you have registered a remote server with Cisco SD-WAN Manager. For more information on how to register a remote server, see Register Remote Server.

The **Add Virtual Image with Remote Server Details** slide-in pane appears. (This option does not store the image on the local Cisco SD-WAN Manager server).

For Cisco vManage Release 20.11.1 and later, follow these steps:

a. Click **Add New Virtual Image** and choose **Remote Server (preferred)**.

b. In the **Image Name** field, enter the file name of the image.

c. In the **Image description** field, enter a description of the image.

d. (Optional) Click the **Add Tags** field and choose tags for the virtual image file.

e. In the **Select service type** field, choose **App-Hosting**.

The following applications are supported:

- **UTD-Snort-Feature**
- **DRE-Optimization-Feature**
- **ThousandEyes-Enterpeise-Agent**
- **Cybervision-Enterprise-Agent**

For standard filenames, Cisco SD-WAN Manager automatically displays the attributes of the image file.

For non-standard filenames, enter the following manually:

- **App type**: Choose an application type from the drop-down list.
- **Enter version**: Enter the version as free text.

  Cisco SD-WAN Manager automatically chooses the x86_64 architecture. You can choose a different architecture if necessary from the drop-down list.

f. Click the **Remote Server Name** field and choose a remote server.

g. In the **Image File Path** field, enter a path from the root directory of the remote server.

If you do not enter a path, Cisco SD-WAN Manager uses the root directory.

h. (Optional) To provide another server that contains the image, click **Add Remote Server**, and enter the details of the additional server.

i. Click **Add**.

- **Manager**: Choose this option to upload a file to the local Cisco SD-WAN Manager repository using a control-plane connection. This option is useful for uploading small files.

  The **Upload VNF's Package to Manager** dialog box opens.

a. Drag and drop the virtual image file to the dialog box or click **Browse** to select the virtual image file from a directory on the local Cisco SD-WAN Manager server.

b. In the **Description** field, enter the description.

c. In the drop-down list, choose **Image Package** or **Scaffold**.

d. Click the **Add Tags** field and choose tags for the virtual image file.

e. Click **Upload** to add the virtual image file to the repository.

- **Remote Server - Manager**: Choose this option to store the virtual image file on a remote Cisco SD-WAN Manager server and download the virtual image file to Cisco Catalyst SD-WAN devices over an out-of-band management connection.

  The **Upload VNF's Package to Remote Server - Manager** dialog box opens.

  a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on the Cisco SD-WAN Manager server that is in a management VPN (typically, VPN 512).

  b. Drag and drop the virtual image file to the dialog box or click **Browse** to select the virtual image file from a directory on the local Cisco SD-WAN Manager server.

  c. In the **Description** field, enter the description of the virtual image file.

  d. In the drop-down list, choose **Image Package** or **Scaffold**.

  e. Click the **Add Tags** field and choose tags for the virtual image file.

  f. Click **Upload**.

Note To upload virtual images using the **Manager** or **Remote Server - Manager** options, use files with extensions, .tar, .gz, .tar or .qcow2. For more information on the steps to upload virtual images with extensions .tar, gz, .tar or .qcow2, see Upload VNF Images, on page 31

Upload VNF Images

The VNF images are stored in the Cisco SD-WAN Manager software repository. These VNF images are referenced during service chain deployment, and then they are pushed to Cisco NFVIS during service chain attachment.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 To add a prepackaged VNF image, click **Virtual Images**, and then click **Upload Virtual Image**.

Step 3 Choose the location to store the virtual image.

- To store the virtual image on the local Cisco SD-WAN Manager server and download it to CSP devices over a control plane connection, click **Manager**. The **Upload VNF's Package to Manager** dialog box appears.

a. Drag and drop the virtual image file or the qcow2 image file to the dialog box or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server. For example, CSR.tar.gz, ASAv.tar.gz, or ABC.qcow2

b. If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

c. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

   - Description of the image
   - Version number of the image
   - Checksum
   - Hash algorithm

   You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

   Note
   - It is mandatory to upload a scaffold file if you choose a qcow2 image file.
   - The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

d. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it available for installing on the CSP devices.

- To store the image on a remote Cisco SD-WAN Manager server and then download it to CSP devices, click **Remote Server - Manager**. The **Upload VNF's Package to Remote Server-Manager** dialog box appears.

  a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on Cisco SD-WAN Manager server that is in the management VPN (typically, VPN 512).

  b. Drag and drop the virtual image file or the qcow2 image file to the dialog box, or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server.

  c. If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

  d. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

     - Description of the image
     - Version number of the image
     - Checksum
     - Hash algorithm

     You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

Note

- It is mandatory to upload a scaffold file if you choose a qcow2 image file.
- The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

e. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

You can have multiple VNF entries such as a firewall from same or from different vendors. Also, you can add different versions of VNF that are based on the release of the same VNF. However, ensure that the VNF name is unique.

Create Customized VNF Image

Before you begin

You can upload one or more qcow2 images in addition to a root disk image as an input file along with VM-specific properties, bootstrap configuration files (if any), and generate a compressed TAR file. Through custom packaging, you can:

- Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.
- Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

- Root disk image for a VNF–qcow2
- Day-0 configuration files–system and tokenized custom variables
- VM configuration–CPU, memory, disk, NICs
- HA mode–If a VNF supports HA, specify Day-0 primary and secondary files, NICs for a HA link.
- Additional Storage–If more storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .

Step 2 Click **Virtual Images** > **Add Custom VNF Package**.

Step 3 Configure the VNF with the following VNF package properties and click **Save**.

Table 4: VNF Package Properties

Field	Mandatory or Optional	Description
Package Name	Mandatory	The filename of the target VNF package. It's the Cisco NFVIS image name with .tar or .gz extensions.
App Vendor	Mandatory	Cisco VNFs or third-party VNFs.
Name	Mandatory	Name of the VNF image.
Version	Optional	Version number of a program.
Type	Mandatory	Type of VNF to choose. Supported VNF types are: Router, Firewall, Load Balancer, and Other.

Step 4 To package a VM qcow2 image, click **File Upload**, and browse to choose a qcow2 image file.

Step 5 To choose a bootstrap configuration file for VNF, if any, click **Day 0 Configuration** and click **File Upload** to browse and choose the file.

Include the following Day-0 configuration properties:

Table 5: Day-0 Configuration

Field	Mandatory or Optional	Description
Mount	Mandatory	The path where the bootstrap file gets mounted.
Parseable	Mandatory	A Day-0 configuration file can be parsed or not. Options are: **Enable** or **Disable**. By default, **Enable** is chosen.
High Availability	Mandatory	High availability for a Day-0 configuration file to choose. Supported values are: Standalone, HA Primary, HA Secondary.

Note
If any bootstrap configuration is required for a VNF, create a *bootstrap-config* or a *day0-config* file.

Step 6 To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize variables of a Day-0 configuration file, click **View Configuration File** next to the desired Day-0 configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

Note
The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. For a shared VNF, see the Custom Packaging Details for Shared VNF topic and additional references in Cisco SD-WAN

Cloud OnRamp for Colocation Solution Guide for the list of system variables that must be added for different VNF types..

a) To add a system variable, in the **CLI configuration** dialog box, select, and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.
b) Choose a system variable from the **Variable Name** drop-down list, and click **Done**. The highlighted property is replaced by the system variable name.
c) To add a custom variable, in the **CLI configuration** dialog box, choose and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.
d) Enter the custom variable name and choose a type from **Type** drop-down list.
e) To set the custom variable attribute, do the following:
   - To ensure that the custom variable is mandatory when creating a service chain, click **Type** next to **Mandatory**.
   - To ensure that a VNF includes both primary and secondary day-0 files, click **Type** next to **Common**.
f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

Step 7 To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an extra qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

Note
Ensure that you don't combine ephemeral disks and storage volumes when uploading extra VM images.

Step 8 To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

Table 6: Storage Properties

Field	Mandatory or Optional	Description
Size	Mandatory	The disk size that is required for the VM operation. If the size unit is GiB, the maximum disk size can be 256 GiB.
Size Unit	Mandatory	Choose size unit. The supported units are: MIB, GiB, TiB.
Device Type	Optional	Choose a disk or CD-ROM. By default, disk is chosen.
Location	Optional	The location of the disk or CD-ROM. By default, it's local.
Format	Optional	Choose a disk image format. The supported formats are: qcow2, raw, and vmdk. By default, it's raw.

Field	Mandatory or Optional	Description
Bus	Optional	Choose a value from the drop-down list. The supported values for a bus are: virtio, scsi, and ide. By default, it's virtio.

Step 9 To add VNF image properties, expand **Image Properties** and enter the following image information.

Table 7: VNF Image Properties

Field	Mandatory or Optional	Description
SR-IOV Mode	Mandatory	Enable or disable SR-IOV support. By default, it's enabled.
Monitored	Mandatory	VM health monitoring for those VMs that you can bootstrap. The options are: enable or disable. By default, it's enabled.
Bootup Time	Mandatory	The monitoring timeout period for a monitored VM. By default, it's 600 seconds.
Serial Console	Optional	The serial console that is supported or not. The options are: enable or disable. By default, it's disabled.
Privileged Mode	Optional	Allows special features like promiscuous mode and snooping. The options are: enable or disable. By default, it's disabled.
Dedicate Cores	Mandatory	Facilitates allocation of a dedicated resource (CPU) to supplement a VM's low latency (for example, router and firewall). Otherwise, shared resources are used. The options are: enable or disable. By default, it's enabled.

Step 10 To add VM resource requirements, expand **Resource Requirements** and enter the following information.

Table 8: VM Resource Requirements

Field	Mandatory or Optional	Description
Default CPU	Mandatory	The CPUs supported by a VM. The maximum numbers of CPUs supported are 8.
Default RAM	Mandatory	The RAM supported by a VM. The RAM can range 2–32.
Disk Size	Mandatory	The disk size in GB supported by a VM. The disk size can range 4–256.
Max number of VNICs	Optional	The maximum number of VNICs allowed for a VM. The number of VNICs can from range 8–32 and by default, the value is 8.
Management VNIC ID	Mandatory	The management VNIC ID corresponding to the management interface. The valid range is from 0 to maximum number of VNICs.
Number of Management VNICs ID	Mandatory	The number of VNICs.
High Availability VNIC ID	Mandatory	The VNIC IDs where high availability is enabled. The valid range is from 0–maximum number of VNICs. It shouldn't conflict with management VNIC Id. By default, the value is 1.
Number of High Availability VNICs ID	Mandatory	The maximum number of VNIC IDs where high availability is enabled. The valid range is 0–(maximum number of VNICs-number of management VNICs-2) and by default, the value is 1.

Step 11 To add day-0 configuration drive options, expand **Day 0 Configuration Drive options** and enter the following information.

Table 9: Day-0 Configuration Drive Options

Field	Mandatory or Optional	Description
Volume Label	Mandatory	The volume label of the Day-0 configuration drive. The options are: V1 or V2. By default, the option is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.

Field	Mandatory or Optional	Description
Init Drive	Optional	The Day-0 configuration file as a disk when mounted. The default drive is CD-ROM.
Init Bus	Optional	Choose an init bus. The supported values for a bus are: virtio, scsi, and ide. By default, it's ide.

The Software Repository table displays the customized VNF image, and image is available for choosing when creating a custom service chain.

View VNF Images

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**.

Step 3 To filter the search results, use the filter option in the search bar.

The Software Version column provides the version of the software image.

The Software Location column indicates where the software images are stored. Software images can be stored either in the repository on the Cisco SD-WAN Manager server or in a repository in a remote location.

The **Version Type Name** column provides the type of firewall.

The **Available Files** column lists the names of the VNF image files.

The **Update On** column displays when the software image was added to the repository.

Step 4 For the desired VNF image, click **...** and choose **Show Info**.

Delete a Software Image from the Repository

To delete a software image from the Cisco SD-WAN Manager software repository:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 For the desired software image, click **...** and choose **Delete**.

If a software image is being downloaded to a router, you cannot delete the image until the download process completes.

Delete VNF Images

Procedure

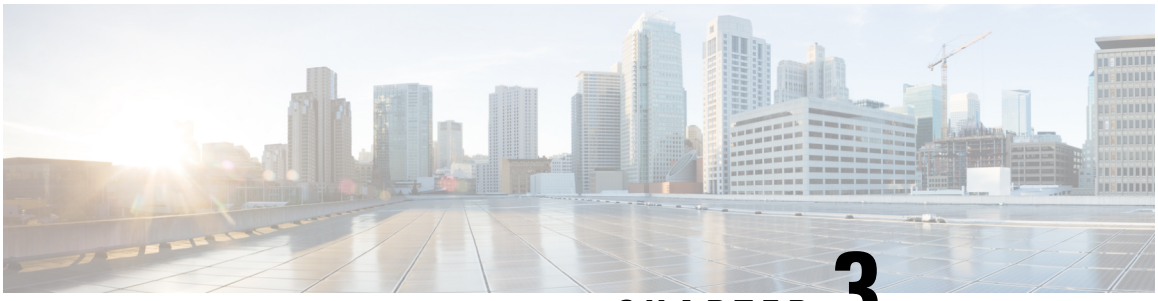
Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**. The images in the repository are displayed in a table.

Step 3 For the desired image, click **...** and choose **Delete**.

Note If you're downloading a VNF image to a device, you can’t delete the VNF image until the download process completes.

Note If the VNF image is referenced by a service chain, it can’t be deleted.



CHAPTER 3

Software Upgrade Workflow

Table 10: Feature History

Feature Name	Release Information	Description
Software Upgrade Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1 Cisco SD-WAN Release 20.8.1	This feature introduces a guided workflow through which you can upgrade the software image on your Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices and monitor the status of the software upgrade. With this workflow, you can choose to download, install, and activate the new software image in discrete steps or in a single step.
Schedule the Software Upgrade Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1 Cisco SD-WAN Release 20.9.1	This feature introduces an option to schedule software upgrades for edge devices using Cisco SD-WAN Manager.
Software Upgrade Workflow Support for Additional Platforms	Cisco vManage Release 20.9.1	Added support for Cisco Enterprise NFV Infrastructure Software (NFVIS) and Cisco Catalyst Cellular Gateways.
Software Upgrade Scheduling Support for Additional Platforms	Cisco vManage Release 20.10.1	Added support for software upgrade scheduling for Cisco Catalyst Cellular Gateways.

Feature Name	Release Information	Description
Device Software Upgrade Workflow Enhancements	Cisco Catalyst SD-WAN Manager Release 20.18.1	The new workflow for device software upgrade includes the following key enhancemnets: • Uploading software image from local drive. • Filtering devices for software upgrade using device tags and network hierarchy. • Scheduling a software upgrade based on a device's local time zone.

Information About Software Upgrade Workflow

Using this workflow, you can download and upgrade software images on the various supported Cisco devices with an option to schedule the upgrade process at your convenience. The workflow also shows the status of the software upgrade. This workflow provides you with two options to perform the software upgrade and they are: **Download and Upgrade** and **Download Only**.

Benefits of Software Upgrade Workflow

- The software upgrade workflow helps you prevent various device software upgrade failures by displaying device upgrade status. For example, if the upgrade process fails at any particular stage, the workflow flags it as **failed**.
- With this workflow, you can choose to download, install, and activate the new software image in discrete steps or in a single step. You can schedule the workflow at your convenience as well.

Information About Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later

From Cisco Catalyst SD-WAN Manager Release 20.18.1, the Software Upgrade Workflow is renamed to Device Software Upgrade Workflow. The new workflow is easy to manage and reduces the chances of upgrade failure.

This workflow includes the following enhancement in device software upgrade:

- Uploading software image from your local drive.
- Adding the platform details for each software image. It ensures you do not upload an incompatible software image for upgrade.

Note Starting Cisco Catalyst SD-WAN Manager Release 20.18.1, you cannot choose different software images for each device platform class. You can only choose one software image version that is compatible with all device platforms.

- Filtering devices for software upgrade using network hierarchies, device tags and software version.
- Scheduling the software upgrade in the device's local time zone.
- Additional preupgrade and postupgrade checks to reduce the chances of upgrade failures.

Supported Devices for the Software Upgrade Workflow

Devices	Minimum Supported Releases	Comments
Cisco IOS XE Catalyst SD-WAN devices	Cisco SD-WAN Manager: Cisco vManage Release 20.8.1 Devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Scheduled software upgrade supported from: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
Cisco vEdge devices	Cisco SD-WAN Manager: Cisco vManage Release 20.8.1 Devices: Cisco SD-WAN Release 20.8.1	Scheduled Software Upgrade feature supported from: Cisco SD-WAN Release 20.9.1
Cisco Catalyst 8200 uCPE Series Edge Platforms	Cisco SD-WAN Manager: Cisco vManage Release 20.9.1 Devices: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	None

Devices	Minimum Supported Releases	Comments
Cisco 5400 Series Enterprise Network Compute System (ENCS)	Cisco SD-WAN Manager: Cisco vManage Release 20.9.1 Devices: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	None
Cisco Catalyst Cellular Gateways	Cisco SD-WAN Manager: Cisco vManage Release 20.9.1 Devices: Cisco IOS CG Release 17.9.1	Scheduled software upgrade supported from: Cisco vManage Release 20.10.1 and Cisco IOS CG Release 17.9.1

Prerequisites for Using the Software Upgrade Workflow

- Ensure that the Cisco devices are running the required software versions for using the software upgrade workflow feature. For the respective device requirements, see Supported Devices for the Software Upgrade Workflow, on page 43.
- From Cisco Catalyst SD-WAN Control Components Release 20.18.1, if you want to filter devices for software upgrade using tags, ensure that you have already assigned tags to the devices. For more information about device tagging, see Device Tagging.
- You cannot use a software image from a remote repository directly in the workflow. Navigate to **Maintenance** > **Software Repository** and edit the software image to add the version and platform information.

Restrictions for software upgrade

TLOC extension configuration

If a device

- is using Cisco IOS XE Catalyst SD-WAN Release 17.9.x or earlier, and
- the device has a tunnel interface configuration includes a TLOC extension,

then you cannot upgrade to one of these:

- 17.12.1 through 17.12.4
- 17.15.1 through 17.15.2

Attempting such an upgrade causes the device to crash and enter a rollback state.

If you have a TLOC extension configured and need to perform such an upgrade, remove the TLOC extension configuration from the tunnel interface configuration before upgrading.

This issue was fixed and does not apply for upgrades to one of these releases:

- 17.12.5 and later releases of 17.12.x

- 17.15.3 and later releases of 17.15.x
- 17.18.1a and later

Access the Software Upgrade Workflow

Before You Begin

To check if there is an in-progress software upgrade workflow:

From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon. Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

Access the Software Upgrade Workflow

1. In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

Note In the Cisco vManage Release 20.8.1, the **Workflow Library** is titled **Launch Workflows**.

2. Start a new software upgrade workflow: **Library** > **Software Upgrade**.

   OR

   Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.

3. Follow the on-screen instructions to start a new software upgrade workflow.

Note Click **Exit** to exit from an in-progress software upgrade workflow. You can resume the in-progress workflow at your convenience.

Note In a multi-node cluster setup, if the control connection switches to a different node during a device upgrade from Cisco SD-WAN Manager, the upgrade may be impacted due to NetConf session timeout. The device then establishes control connection to a different node. You need to re-trigger the upgrade activity.

Verify the Status of the Software Upgrade Workflow

To check the software upgrade workflow status:

1. From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon.

   Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

2. Click the + icon to view the details of a task.

   Cisco SD-WAN Manager opens a pane displaying the status of the task and details of the device on which the task was performed.

Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 and Later

Before you begin

To filter devices for upgrade using tags, ensure the devices that you want to choose have tags. For more information, see Prerequisites for Using the Software Upgrade Workflow.

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

Step 2 Start a new software upgrade workflow: **Workflow Library** > **Device Software Upgrade**.

Step 3 Choose the devices using the network hierarchy panel.

Alternatively, use the filters **Search**, **Device tags**, and **Software version** options or a combination of these filters to search and choose devices.

Note
In the workflow, you can choose a specific software image version from a dropdown to upgrade devices. Before choosing the software image version, you must select the devices for upgrade. Software image versions only show up in the dropdown if all choosen devices in the workflow have the necessary images available in a local or remote repository. If the supported software image version is not available in the repository for one or more devices, then you cannot choose that software image version from the dropdown.

Note
In the upgrade workflow, do not choose different types of devices together. Specifically, avoid the combination of the following devices: Cisco IOS XE Catalyst SD-WAN devices together, Cisco Enterprise NFVIS (Cisco Enterprise Network Function Virtualization Infrastructure Software) devices, or Cisco Catalyst Cellular Gateway devices.

Step 4 Choose one for the following upgrade type:

a. **Upgrade**: To install and activate the software image.

b. **Patch**: To apply patch fixes on the existing software.

Step 5 Choose one of the following options to add a software image:

- **+ Add New Image** to upload an image from local drive.
- **+ Add New Remote Server** to add a remote server for upgrade and then add a software image.

Note
Software images created before upgrading the Cisco SD-WAN Manager to version Cisco Catalyst SD-WAN Manager Release 20.18.1 lack platform family and version details. To use these images after the upgrade, edit them in **Maintenance** > **Software Repository** and add the required platform family and version information.

Step 6 Follow the on-screen instructions to complete the software upgrade workflow.

Note
Click **Exit** to exit from an in-progress software upgrade workflow. You can resume the in-progress workflow at your convenience.

Note
For an error during device software upgrade, see Error message during software upgrade or setting default software version.

What to do next

To view the list of successful upgrades on the devices. Click the **Task log** in the task bar.

Schedule Software Upgrade Workflow

Introduced in Cisco vManage Release 20.9.1, the scheduler in the software upgrade workflow enables you to schedule workflows at your convenience and avoid any downtime due to the software upgrade process. A scheduler enables you to schedule the upgrade workflow either **Now** or **Later**. If you choose to schedule an upgrade for a later time, you can enter the **Start Date**, **Start time**, and **Select Timezone**.

Schedule Software Upgrade Workflow

Use the following steps to schedule a software upgrade workflow:

1. In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**

   OR

   Starting from Cisco vManage Release 20.9.1, click **Workflows** > **Popular Workflows** > **Software Upgrade.**.
2. Start a new software upgrade workflow: **Workflow Library** > **Software Upgrade**.

   OR

   Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.
3. In the **Scheduler** section, choose **Later**.

Note Use the **Now** option to perform the software upgrade for the selected devices immediately.

4. Choose the **Start Date**, **Start Time**, and **Select Timezone**.

Note Start date and time should always be greater than the Cisco SD-WAN Manager server date and time.

5. Click **Next**.
6. The software upgrade workflow is scheduled.

Schedule a Device Software Upgrade Workflow in Cisco Catalyst SD-WAN Manager Release 20.18.1 or Later

Before you begin

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

Step 2 Start a new software upgrade workflow: **Workflow Library** > **Device Software Upgrade**.

Step 3 After choosing the devices, in the **Action** section, choose **Download and Upgrade** to schedule upgrade.

Step 4 In the **Scheduler** section, choose **Later**.

Note
Choose the **Now** option to upgrade device software immediately after completing the workflow.

Step 5 Add a **Task Name** and choose the **Start Date**, **Start Time**, and **Select Timezone**.
Alternately, choose **Site Time** to perform the software upgrade in the device's local time zone.

Step 6 Follow the on-screen instructions to complete the workflow.

What to do next

To view the list of sucessful upgrades on the devices. click on the **Task log** in the task bar.

Cancel the Scheduled Software Upgrade Workflow

To cancel a scheduled software upgrade workflow,

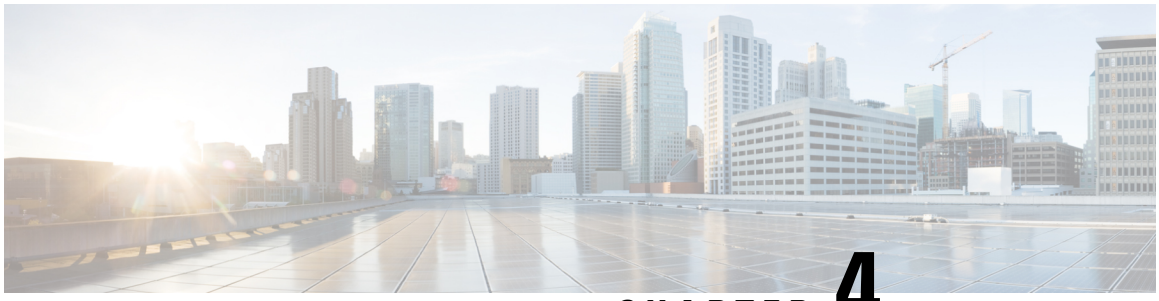
1. From the Cisco SD-WAN Manager menu, click **Maintenance** > **Software Upgrade**.
2. Choose the device that is scheduled for a software upgrade from the list of devices.
3. Click **Cancel Software Upgrade**.

Delete a Downloaded Software Image

To delete downloaded software images from WAN edge devices:

1. From the Cisco Catalyst SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**.
3. Click **Delete Downloaded Images**

4. In the **Delete Downloaded Images** pop-up window, choose the image or images to delete.
5. Click **Delete**.



CHAPTER 4

Software maintenance upgrade for Cisco IOS XE Catalyst SD-WAN Devices

Feature history of software maintenance upgrade

Feature history of software maintenance upgrade, release by release.

Table 11: Feature history

Feature Name	Release Information	Description
Support for Software Maintenance Upgrade Package	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables support for a Software Maintenance Upgrade (SMU) package that can be installed on Cisco IOS XE Catalyst SD-WAN devices. The SMU package provides a patch fix or a security resolution to a released Cisco IOS XE image. Developers can build this package that provides a fix for a reported issue without waiting for the fix to become available in the next release.
SMU Support for Cisco ISR1100 and ISR1100X Series Routers	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	Added support for Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers.

Information about software maintenance upgrade

A software maintenance upgrade (SMU) is a point fix to resolve a security issue in released software that attempts to minimize disruption to the router, if possible. An SMU is not designed to replace a maintenance release.

- SMUs are provided as package files for each release and component of Cisco Catalyst SD-WAN.
- Each SMU image filename includes a base image version and the defect ID related to the fix.
- The package contains metadata describing its content and the fix for a reported issue.
- Cisco can release a package that provides a fix for a reported issue without waiting for the fix to become available in the next release.

SMU types and benefits

SMU types determine how the installed package affects the device, and SMUs offer several operational benefits.

- Hot SMU (non-reload): Enables an SMU package to take effect after activation without rebooting the Cisco IOS XE Catalyst SD-WAN device .
- Cold SMU (reload): Enables an SMU package to take effect after rebooting the Cisco IOS XE Catalyst SD-WAN device.

SMUs provide operational advantages for network maintenance.

- Address network issues quickly while reducing testing time and scope. The Cisco IOS XE Catalyst SD-WAN device validates SMU image compatibility and prevents installation of non-compatible packages.
- Allow installation or activation of only one SMU package at a time to simplify implementation.
- Enable installation of SMU packages on multiple Cisco IOS XE Catalyst SD-WAN device s simultaneously using Cisco SD-WAN Manager. For CLI-based installation, repeat the process for each device.

Supported devices for software maintenance upgrade

This topic provides a reference table of Cisco router platforms and the minimum software releases that support software maintenance upgrade.

Table 12: Supported devices and minimum software releases for SMU

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.9.5a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.9.x Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and later	• Cisco ISR 1000 Series Integrated Services Routers • Cisco IR1101 Integrated Services Router Rugged • Cisco ISR 4000 series Integrated Services Routers • Cisco ASR 1000 Series Aggregation Services Routers • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8500L Series Edge Platforms • Cisco Catalyst 8000v Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x	• Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200L Series Edge Platforms
Cisco IOS XE Catalyst SD-WAN Release 17.12.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.12.x	Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers

Manage software maintenance upgrade images

Use Cisco SD-WAN Manager to add, upgrade and activate, or deactivate and remove an SMU image.

Note When you activate or deactivate an SMU image, the device may reboot, depending on the SMU image. A non-reload SMU type does not trigger a device reboot. A reload SMU type triggers a device reboot.

Procedure

Step 1 Add an SMU image using the Cisco SD-WAN Manager software repository.

See the Cisco SD-WAN Manager *Add Software Images to Repository* procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 2 View SMU images using the Cisco SD-WAN Manager software repository.

See the Cisco SD-WAN Manager *View Software Images* procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide* . Note the following points when viewing SMU images:

- The **Available SMU Versions** column displays the number of SMU images available for the current base image version (Cisco IOS XE image version).
- View the defects that are associated with an SMU image by clicking a desired entry in the **Available SMU Versions** column. In the **Available SMU Versions** dialog box, you can view the defect ID, the corresponding SMU version, and the SMU types, such as non-reload or reload.
- In the **Available SMU Versions** dialog box, delete an SMU version by clicking the delete icon next to an SMU version.

Step 3 Upgrade an SMU image using the Cisco SD-WAN Manager software upgrade window.

See the Cisco SD-WAN Manager *Upgrade the Software Image on a Device* procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide* . Note the following points about the SMU image that you choose to upgrade:

- In the devices table, the **Available SMUs** column displays the number of SMU images that are available for the current base image version.
- View a list of all available SMU versions and the upgrade images for a device by clicking a desired entry under the **Available SMUs** column. In the **Available SMUs** dialog box, you can view the SMU versions, SMU types, and the state of an SMU version.

  The SMU version is in the format *base_image_version* . *cdet_id*.
- In the **Upgrade** dialog box, optionally check **Activate and Reboot** to activate an SMU image and perform a reboot of the Cisco IOS XE Catalyst SD-WAN device automatically.

  After you check the **Activate and Reboot** check box, Cisco SD-WAN Manager installs and activates the SMU image on a device and triggers a reload based on the SMU type. For more Information about activating a software image, see the Cisco SD-WAN Manager *Activate a Software Image* procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

After a successful upgrade of an SMU image, the Cisco IOS XE Catalyst SD-WAN device sends a corresponding success message.

Step 4 Deactivate an SMU image and remove the image from a device using the *Delete a Software Image* procedure in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 5 Do not enable the Cisco IOS XE Catalyst SD-WAN device interface on the ISR1100 device.

Step 6 Add the serial.viptela file to Cisco SD-WAN Manager to add the device.

Step 7 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Migrate Device** to migrate from viptela operating system to Cisco IOS XE operating system.

Step 8 Enable the Cisco IOS XE Catalyst SD-WAN device interface to bring up the control connections.

Step 9 Verify the device sync up in Cisco SD-WAN Manager.

Manage software maintenance upgrade images using the CLI

Use CLI commands to install, activate, deactivate, and remove SMU images on the device.

These sections describe the CLI procedures:

- Install and activate an SMU image using the CLI, on page 55

- Deactivate and Remove an SMU Image Using the CLI

Note When an SMU image is activated and deactivated, the device reboot may be triggered based on non-reload or reload SMU types. A non-reload SMU type does not trigger a device reboot, but a reload SMU type triggers a device reboot.

Install and activate an SMU image using the CLI

Procedure

Step 1 Upload the SMU image from the file server to the bootflash of the device.

Use the `copy` command to upload an SMU image. For information about the copy command, see Step 2 of the Install the Cisco IOS XE Software topic.

Step 2 If not already configured, configure the time limit for confirming that a SMU image activation is successful.

The time limit can be 1 through 60 minutes. We recommend that you configure the time limit to be at least 15 minutes.

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm minutes
```

Step 3 Install an SMU image from the bootflash of your device and perform a compatibility check for the device and SMU package version.

```
Device# request platform software sdwan smu install file-path
```

Step 4 Activate the SMU image on a Cisco IOS XE Catalyst SD-WAN device .

```
Device# request platform software sdwan smu activate build-number.smu-defect-id
```

Step 5 Confirm the upgrade of the SMU image within the configured confirmation time limit.

```
Device# request platform software sdwan smu upgrade-confirm
```

Note
If you don't issue this command on the device within the time limit that is specified in the **upgrade-confirm** *minutes* command, the device automatically reverts to the state that it was in before the SMU image activation.

Deactivate and remove an SMU image using the CLI

Procedure

Step 1 If not already configured, configure the time limit for confirming that a SMU image deactivation is successful.

The time limit can be 1 through 60 minutes. We recommend that you configure the time limit to at least 15 minutes.

```
Device# config-transaction
Device(config)# system
Device(config-system)# upgrade-confirm minutes
```

Step 2 Deactivate an SMU image on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan smu deactivate build-number.smu-defect-id
Device# request platform software sdwan smu upgrade-confirm
```

Note
If you do not issue this command on the device within the time limit specified in the **upgrade-confirm** *minutes* command, the image deactivation fails and the device automatically reverts to the state that it was in before the SMU image deactivation.

Step 3 Remove an SMU image from a Cisco IOS XE Catalyst SD-WAN device .

```
Device# request platform software sdwan smu remove build-number.smu-defect-id
```

These examples show commands that you can use to manage the SMU image operations.

- Check the upgrade and confirm the configuration:

  ```
  show sdwan running system
  ```

- Add and upgrade the confirm timer:

  ```
  Device# config-transaction
  Device(config)# system
  Device(config-system)# upgrade-confirm 15
  Device(config-system)# commit
  ```

- Execution commands:

  - **request platform software sdwan smu install bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin**
  - **request platform software sdwan smu activate 17.09.01a.0.247.CSCvq24042**
  - **request platform software sdwan smu upgrade-confirm**
  - **request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042**
  - **request platform software sdwan smu upgrade-confirm**
  - **request platform software sdwan smu remove 17.09.01a.0.247.CSCvq24042**

Verify the status of SMU images using CLI

Use CLI commands to check the installation, activation, deactivation, and removal status of SMU images. Review command outputs to determine the current state and rollback timer for SMU images on the device.

SMU image status verification and output interpretation

The **show install summary** command displays the installed packages and their states, including SMU images. The state codes indicate whether an image is inactive, activated and uncommitted, activated and committed, or deactivated and uncommitted. The `Auto abort timer` value shows the time left before rollback.

Note State (St): I - Inactive, U - Activated & Uncommitted, C - Activated & Committed, D - Deactivated & Uncommitted

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01a.0.247
SMU   I    bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

SMU image deactivation and removal

The **request platform software sdwan smu deactivate** command deactivates an SMU image. The output confirms the deactivation process and result. After deactivation, the **show install summary** command reflects the new state and the auto abort timer status.

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042
smu_deactivate: START Mon Mar 5 21:54:06 PST 2021
smu_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on all members
[1] SMU_DEACTIVATE package(s) on switch 1
[1] Finished SMU_DEACTIVATE on switch 1
Checking status of SMU_DEACTIVATE on [1]
SMU_DEACTIVATE: Passed on [1]
Finished SMU Deactivate operation
SUCCESS: smu_deactivate 17.09.01a.0.247.CSCvq24042
```

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01a.0.247
SMU   D    bootflash: c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
--------------------------------------------------------------------------------
Auto abort timer: active , time before rollback - 00:04:57
--------------------------------------------------------------------------------
```

```
Device# request platform software sdwan smu deactivate 17.09.01a.0.247.CSCvq24042
install_deactivate: START Thu Aug 25 17:47:10 UTC 2022
install_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre sripts done.
```

```
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on Active/Standby
[1] SMU_DEACTIVATE package(s) on R0
[1] Finished SMU_DEACTIVATE on R0
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation
CSCvq24042:SUCCESS
SUCCESS: install_deactivate /bootflash/c8kv_hot.bin Thu Aug 25 17:47:33 UTC 2022
```

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01a.0.247
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

SMU image metadata inspection

The **show install package** command provides metadata for an SMU image, including name, version, platform, package type, defect ID, package state, SMU ID, SMU type, compatibility, and impact.

```
Device# show install package
bootflash:c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
Name: c8000v-universalk9.2022-08-17_23.44_mcpre.24042.CSCvq24042.SSA.smu.bin
Version: 17.09.01a.0.247.1660805065
Platform: C8000V
Package Type: SMU
Defect ID: CSCvq24042
Package State: Inactive
Supersedes List: {}
SMU Fixes List: {}
SMU ID: 24042
SMU Type: non-reload
SMU Compatible with Version: 17.09.01a.0.247
SMUImpact:
```

Monitor the SMU status using Cisco SD-WAN Manager

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** .

Step 2 For the desired Cisco IOS XE Catalyst SD-WAN device , click an SMU image link (hyperlink) under **Available SMUs**. In the **Available SMUs** dialog box, you can view the state of an SMU image.

If no SMU images are available for the current base image version (Cisco IOS XE image version), the SMU image link is not available under **Available SMUs** and Cisco SD-WAN Manager displays 0.

CHAPTER 5

Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Feature history for the Cisco Catalyst SD-WAN Control Components upgrade workflow

Table 13: Feature history

Feature Name	Release Information	Description
Cisco SD-WAN Control Components Upgrade Workflow	Cisco Catalyst SD-WAN Control Components Release 20.18.1	With the guided workflow you can upgrade the software image of all the Cisco SD-WAN Control Components. It also allows you to apply patch release upgrades to Cisco SD-WAN Control Components, for bug fixes and minor improvements. From Cisco Catalyst SD-WAN Control Components Release 20.18.1, you can schedule full OS and patch upgrades for Cisco SD-WAN control plane components (SD-WAN Manager, SD-WAN Validator, SD-WAN Controller) for a specific future date and time.

Information About Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

A Cisco SD-WAN Control Components upgrade workflow is a process that:

- integrates the software image upgrade of the Cisco SD-WAN Control Components—Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator, and
- reduces the complexity of upgrading each Cisco SD-WAN Control Component separately.

The workflow upgrades the Cisco SD-WAN Control Components in the following sequence:

1. Cisco SD-WAN Manager
2. Cisco SD-WAN Validator
3. Cisco SD-WAN Controller

In the workflow, you can download software images from the Cisco Software Download repository and upload software images from a local drive.

During the upgrade process, you can monitor the progress for each control component separately.

Information About Patch Release Upgrade For Control Components

A patch release upgrade is a targeted update that addresses specific bugs and introduces minor improvements to the software. It is designed to complement the existing software.

You can apply a patch release upgrade only to its compatible software release version. For example, if your software version is 20.18.1, you can apply patches designed only for 20.18.1. A patch release image is named as a 6-tuple, with the last digit indicating the patch number (e.g., 20.18.1.0.0.1). It is applied on a compatible base 5-tuple release version (e.g., 20.18.1.0.0)

Benefits of Using Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

- Streamlined upgrade process: All Cisco SD-WAN Control Components are upgraded in the correct sequence, reducing the risk of errors.
- Progress monitoring: With better visibility into the progress of each control component's upgrade, you can track and manage the upgrade process more efficiently.
- Pre-check and post-check tasks: The workflow includes a list of validation tasks that run before and after the upgrade. This flexibility ensures that the upgrade completes successfully.
- Flexibility in software image selection: You can either use the recommended image versions or choose a compatible custom image. For software compatibility information, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources
- Operational efficiency: Implementing patch release upgrades simplifies the process of fixing minor issues, thereby minimizing operational overhead in addressing minor problems.

Prerequisite for Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

You must ensure that the Cisco SD-WAN Control Components are running on the compatible software versions before using the Control Components Upgrade workflow.

Restrictions for Cisco Catalyst SD-WAN Control Components Upgrade Workflow

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

- You cannot select or deselect specific Cisco SD-WAN Control Components for upgrade.

- The workflow does not support older versions of Cisco SD-WAN Control Components.

Restrictions for Patch Release Upgrade

You cannot uninstall a patch release upgrade, after you apply it to the Cisco SD-WAN Control Components. We recommend taking a VM snapshot before upgrading.

Upgrade Cisco Catalyst SD-WAN Control Components Using a Workflow

Before you begin

Minimum Supported Version: Cisco Catalyst SD-WAN Control Components Release 20.18.1

If you are planning to upload software images from your local drive, ensure all the appropriate software image files for Cisco SD-WAN Control Components are available for upload. To ensure that the current device versions support the new software image verision, see Cisco SD-WAN Compatibility Matrix

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.

a) Start a **Control Components Upgrade** workflow.

Step 2 Choose the type of upgrade:

- Upgrade: To install and activate all Cisco SD-WAN Control Components.

  .
- Patch: To install and activate patch image to Cisco SD-WAN Control Components.

Step 3 Select Image Version.

- **Recommended Image** shows an image that is recommended based on compatibility, if logged into cisco.com.
- **Custom** allows you to select from a dropdown of images that include images already uploaded in the Software Repository. Or, if you are logged into cisco.com you can select images from software.cisco.com that aren't necessarily the recommend version, but are options to upgrade to.
- **+ Add New Image** allows you to select an image from software.cisco.com (either from the Recommended Image option or from the Custom dropdown). The image automatically downloads from CCO.

Step 4 Follow the on-screen instructions to continue with the Cisco SD-WAN Control Components upgrade.

Note

- Click **Exit** to exit from an in-progress upgrade workflow. You can resume the in-progress workflow at your convenience.
- You cannot cancel the Cisco SD-WAN Control Components upgrade process after initializing it.

Note
Click **View upgrade status** to monitor the progress of software upgrade for each control component during the upgrade process.

Alternatively, you can navigate to **Maintenance** > **Software Upgrade** > **Control Components** and click **View upgrade status** to monitor the progress of software upgrade.

What to do next

Verify the success or failure of the Cisco SD-WAN Control Components upgrade or patch upgrade by reviewing the task logs. For more information about viewing task logs, see View Log of Software Upgrade Activities.

Scheduling Cisco Catalyst SD-WAN Control Components Upgrade Using Workflow

Use the following steps to schedule a Cisco SD-WAN Control Components upgrade workflow.

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**

Step 2 Start a new software upgrade workflow: **Workflow Library** > **Software Upgrade**.

Step 3 In the **Scheduler** section, select **Later**.

Note
Use the **Now** option to perform the software upgrade for the selected devices immediately.

Step 4 Select the **Start Date**, **Start Time**, and **Select Timezone**.

Step 5 Click **Next**.

Note
If an upgrade fails, Cisco SD-WAN Manager initates a rollback.

Reschedule a Cisco Catalyst SD-WAN Control Components Upgrade

Use the following steps to reschedule a previously scheduled Cisco SD-WAN Control Components upgrade workflow that has not started yet.

Procedure

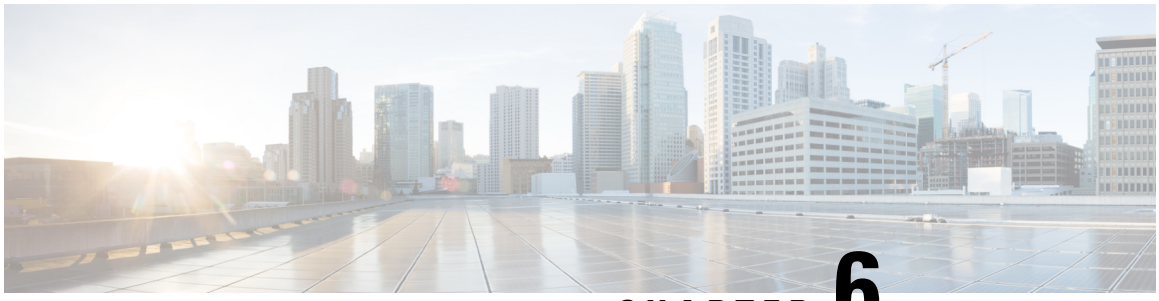
Step 1 In the Cisco SD-WAN Manager menu, click **Workflows** > **Workflow Library**.
Step 2 Go to your scheduled software upgrade workflow: **Workflow Library** > **Software Upgrade**.
Step 3 Click on the **Control Components** tab and click **Reschedule upgrade**.
Step 4 Select the **Start Date**, **Start Time**, and **Select Timezone**.

Cancel a Scheduled Cisco Catalyst SD-WAN Control Components Upgrade

Use the following steps to cancel a scheduled Cisco Catalyst SD-WAN Control Components upgrade that has not started yet:

Procedure

Step 1 In the Cisco SD-WAN Manager menu, click **Maintenance** > **Software Upgrade**.
Step 2 Choose the device that is scheduled for a software upgrade from the list of devices.
Step 3 Click **Cancel Software Upgrade**.



CHAPTER 6

Remote Server Support for ZTP Software Upgrade

Feature history for remote server support for ZTP software upgrade

Table 14: Feature History

Feature Name	Release Information	Description
Remote Server Support for ZTP Software Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	This features introduces remote server support for upgrading the software of Cisco IOS XE Catalyst SD-WAN devices at scale using Zero Touch Provisioning (ZTP). Upload the software upgrade images to Cisco SD-WAN Manager using a preferred remote server and then upgrade the respective devices.

Information About Remote Server Support for ZTP Upgrade

You can onboard and upgrade numerous Cisco IOS XE Catalyst SD-WAN devices together, using the software images hosted on a remote server. The physical WAN edge onboard and upgrade options include the following:

- Manual
- Bootstrap
- Automated deployment

In Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and earlier, the software upgrade images are hosted only on Cisco SD-WAN Manager. During the software upgrade process, the devices fetch the upgrade information from Cisco SD-WAN Manager to upgrade the devices with the latest software.

From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, remote server support for ZTP upgrades enables you to upgrade Cisco IOS XE Catalyst SD-WAN devices using the software images stored in a remote server. The remote server support for ZTP upgrade feature enables you to register a remote server with Cisco SD-WAN Manager and add locations of the software images that are present in the remote server to theCisco SD-WAN Manager software repository. When you upgrade a device, the device downloads the new software image from the remote server, without overwhelming the Cisco SD-WAN Manager server.

When using the Cisco Catalyst SD-WAN hosted service, it is possible to enforce a version of the Cisco SD-WAN software to run on a router as it joins the fabric for the first time. When you enable ZTP, you can see the platform version and status details of the devices running on a router. For example, ISR1101 Disabled, C8000AES Disabled, ISR4400 Disabled, C8000AEP Disabled, ASR1001-X Disabled and so on.

Benefits of Remote Server Support for ZTP Upgrade

- Enables you to upgrade Cisco IOS XE Catalyst SD-WAN devices using software images stored on a remote server, thus removing the dependency on the Cisco SD-WAN Manager software repository.
- Many software upgrade image file formats are supported.
- Cisco SD-WAN Manager provides the devices that are being upgraded with the information they require to download the necessary software images from the servers hosting the images. The devices retrieve the images directly from the servers. This minimizes performance demands on Cisco SD-WAN Manager, as compared to storing images in the Cisco SD-WAN Manager software repository.

Supported Devices for Remote Server Support for ZTP Upgrade

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	• ASR 1000 • ISR 1000 • ISR 4000 series router models (with exception of ISR1100-4G/6G) • IR 1001 • IR 8340 • IR 8100 • Ciso 8000 series router models • Cisco Catalyst Wireless Gateway CG113 Series • ASR 1001-X • Cisco 1100 • Ciso ESR6300

Prerequisites for Remote Server Support for ZTP Upgrade

- Ensure that a remote server is registered to the Cisco SD-WAN Manager Software Repository. For more information see, the section Register Remote Server.
- Ensure that you add a new software image using the **Remote Server (preferred)** option. For more information see, the section Add Software Images to the Repository.

Note Ensure that the **Image Filename** matches the **Image Filename** in the **Remote Server Name** field.

- Make sure the device can reach the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers.
- To be upgraded, a device must be in the **Valid** or the **Staging Certificate** state.

Restrictions for Remote Server Support for ZTP Upgrade

- You cannot upgrade Cisco SD-WAN Manager along with devices that are present in a group upgrade operation. You must upgrade and reboot the only the Cisco SD-WAN Manager server.

- The ZTP upgrade flow doesn't restart automatically when the devices are interrupted by an unforeseen manual device reload or a power failure.
- The **Enforce Software Version (ZTP)** option is available only for Cisco IOS XE Catalyst SD-WAN devices.
- We recommend that you perform all software upgrades from Cisco SD-WAN Manager rather than from the CLI.
- Remote server support for ZTP upgrades is available only through VPN-0.

Note For software compatibility information, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

Enable Enforce Software Version (ZTP)

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Enforce Software Version (ZTP)**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Enable the software version for the corresponding device.
4. In the **Image Location** window, click the **Remote Server** radio button.
5. From the **Remote Server Name** drop-down list, choose a remote server.
6. From the **Image Filename** drop-down list, choose an image.
7. Click **Save**.

Upload Device List

You can upload a list of devices that you want to upgrade, to Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Upload WAN Edge List**.
3. Upload the .CSV file that you have created from the Sample CSV.
4. Check the **Validate the uploaded vEdge List and send to controllers** checkbox.
5. Click **Upload**.

Note You can upload device lists to Cisco SD-WAN Manager using your Cisco Smart Account as well. For more information about enabling PnP Connect Sync see, Enable PnP Connect Sync.

Use Cisco Catalyst SD-WAN Manager to Configure and Upgrade a Device

Devices in the overlay network that are managed by Cisco SD-WAN Manager must be configured using Cisco SD-WAN Manager in order to be upgraded.

Use the following steps to configure and upgrade a device, using Cisco SD-WAN Manager:

1. Create feature templates:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and choose **Add Templates**.
2. Create device templates.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose **Create Templates**.
3. Attach device templates to individual devices.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose a template.
   c. Click **…**, and choose **Attach Devices**.
   d. You can see the added device in the list of **Available Devices** list. Send the particular device to the **Selected Devices** window using the **Right arrow** button.
   e. Click **Attach**.
4. In the **Device Template** window, click **...** to update the device template by entering the following parameters:

Field	Description
Status	Displays the current status of the device template.
Chassis Number	Displays the chassis number of the device.
System IP	Displays the system IP address, if applicable.
Host Name	Displays the host name, if applicable.
DNS Address (vpn_dns_primary)	Enter the DNS address.
Host Name	Enter the host name.
System IP	Enter the system IP address.
Site ID	Enter the site ID.

5. Click **Update**. and then click **Next**.

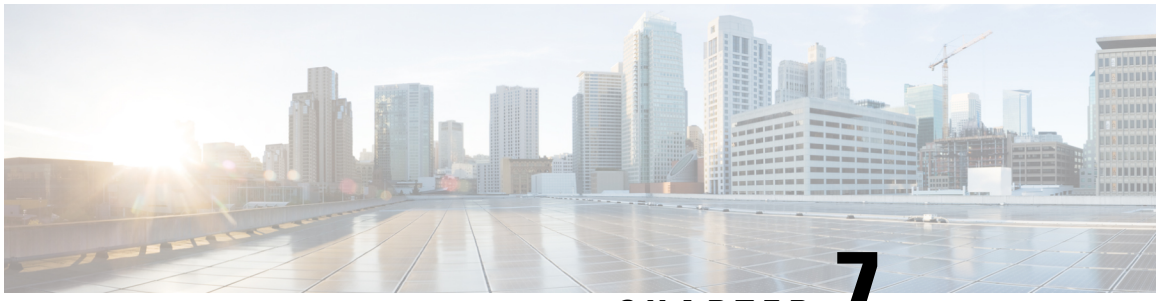
6. After the device template is added, select the device template and click **Configure Devices**.
7. The **Config Preview** is displayed.
8. Click **Configure Devices**.
9. You are routed to the **Task List** window, where you can see the status of the configuration.
10. The configuration is attached to the device once the device is online.
11. Cisco SD-WAN Manager creates a task for this software upgrade through the ZTP server, and you can monitor the status of the upgrade using the **Task List** window.

Monitor the ZTP Software Install

In Cisco SD-WAN Manager, click the task list icon at the top-right corner of the window.

The task list shows open software installation tasks, if any, and indicates the status of these tasks.

Note Cisco SD-WAN Manager pushes the device template to a device only after the software upgrade process is complete. You can monitor the status of the software upgrade using the **Tasks** window.



CHAPTER 7

Cellular Modem Firmware Upgrade

Cellular Modem Firmware Upgrade

Table 15: Feature History

Feature Name	Release Information	Feature Description
Cellular Modem Firmware Upgrade	Cisco IOS CG Release 17.12.1 Cisco Catalyst SD-WAN Control Components Release 20.12.1	Cisco SD-WAN Manager supports upgrading the cellular modem firmware of the following devices running Cisco IOS CG software: • Cisco Catalyst Wireless Gateways (CG113-4GW6) • Cisco Catalyst Cellular Gateways (CG522-E, CG418-E)

Feature Name	Release Information	Feature Description
Cellular Modem Firmware Upgrade for Cisco IOS XE Platforms	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Control Components Release 20.14.1	Extended support to the following platforms, when equipped with a cellular modem: • Cisco ISR1100 and ISR1100X Series Platforms • Cisco Catalyst 8200 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms
P-LTE-450 MHz Module Firmware Upgrade using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Cisco SD-WAN Manager supports upgrading the P-LTE-450 MHz module firmware on the following platforms: • Cisco IR1101 platform • Cisco IR1800 Series platforms See the Firmware upgrade for P-LTE-450 MHz modules section.
Wi-Fi Module Firmware Upgrade using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Cisco SD-WAN Manager supports upgrading the Wi-Fi module firmware on Cisco IR1800 platforms.

Information About Cellular Modem Firmware Upgrade

Using Cisco SD-WAN Manager, you can upgrade the cellular modem firmware of devices that include a cellular modem.

Notification of Available Firmware Upgrades

On the Cisco Software Download site, you can log in with your user account and set notifications to inform you of when a firmware upgrade is available for your devices.

Upgrade Process

After you download firmware upgrade files from the Cisco Software Download site, the overall process is as follows:

- Save the downloaded firmware upgrade files to a file server accessible by the devices in the network. For details, see **Before You Begin** in Upgrade the Cellular Modem Firmware of a Device, on page 76.

- Using the workflow described in Upgrade the Cellular Modem Firmware of a Device, on page 76, select the devices for which to upgrade the modem firmware using the downloaded files. In that workflow, you indicate the location of the file server and directory. If a firmware update file is available for a selected device, Cisco SD-WAN Manager automatically determines the correct file to use and upgrades the modem firmware on the device.

The workflow enables you to schedule the firmware upgrade for a specific time, such as to align with a maintenance window.

Example Illustrating Cellular Modem Firmware Upgrade

The following example scenario illustrates how the firmware upgrade affects only the active firmware on the device.

1. You begin with the following firmware versions on a cellular-enabled device:

```
Router#show cellular 0/2/0 firmware
 Idx Carrier              FwVersion        PriVersion   Status
 1   DOCOMO               02.24.05.06      001.007_000  Inactive
 2   GENERIC              02.24.05.06      002.026_000  Active
 3   KDDI                 02.24.05.06      001.005_000  Inactive

Firmware Activation mode  =  AUTO
```

   The command output indicates, for example, that the GENERIC firmware type has firmware version 02.24.05.06, and that the GENERIC firmware type is the active one.

2. You learn that there are two firmware upgrades available:
   - For GENERIC, you can download 02.24.05.07.
   - For DOCOMO, you can download 02.24.05.07.
3. You download both of the files and put them on the file server.
4. You run the firmware upgrade workflow, described in Upgrade the Cellular Modem Firmware of a Device, on page 76.
   - The device finds the GENERIC 02.24.05.07 firmware upgrade file and uses it to upgrade the GENERIC firmware type, which is the active firmware type.
   - The device does not upgrade the DOCOMO firmware type, even though there is a firmware upgrade file that could accomplish that. This is because DOCOMO is not an active firmware type on the device.
5. After the upgrade, check the firmware versions and note that the firmware upgrade occurred only for the GENERIC firmware type, which is the active one.

```
Router#show cellular 0/2/0 firmware
 Idx Carrier              FwVersion        PriVersion   Status
 1   DOCOMO               02.24.05.06      001.007_000  Inactive
 2   GENERIC              02.24.05.07      002.026_000  Active
 3   KDDI                 02.24.05.06      001.005_000  Inactive

Firmware Activation mode  =  AUTO
```

Benefits of Cellular Modem Firmware Upgrade

Cisco SD-WAN Manager provides an easy-to-use workflow for upgrading modem firmware on one or more devices, making it unnecessary to execute modem firmware upgrade using CLI commands on each device individually.

Supported Platforms for Cellular Modem Firmware Upgrade

- From Cisco Catalyst SD-WAN Control Components Release 20.12.1:
  - Cisco Catalyst Wireless Gateways (CG113-4GW6)
  - Cisco Catalyst Cellular Gateways (CG522-E, CG418-E)
- From Cisco Catalyst SD-WAN Control Components Release 20.14.1:
  - Cisco ISR1100 and ISR1100X Series Platforms
  - Cisco Catalyst 8200 Series Edge Platforms
  - Cisco Catalyst 8300 Series Edge Platforms
- From Cisco Catalyst SD-WAN Manager Release 20.18.1, for P-LTE-450 modules:
  - Cisco IR1101 Platform
  - Cisco IR1800 Series Platforms

Supported Platforms for Wi-Fi module firmware upgrade

Wi-Fi module firmware upgrade

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the Cisco IR1800 series supports Wi-Fi module firmware upgrade using Cisco SD-WAN Manager.

Prerequisites for Cellular Modem Firmware Upgrade

File Server Accessibility

Ensure that the file server storing the firmware upgrade files is accessible by the devices in the network.

Firmware Download

Download the required firmware updates from Cisco.com, for the cellular-modem-equipped devices you wish to upgrade.

Prerequisites for Wi-Fi module firmware upgrades

Minimum Firmware Version – Wi-Fi Module

The Wi-Fi module must be running a firmware version 17.17.1 or higher. If the module's firmware version is earlier than 17.17.1, you cannot upgrade to 17.18.x or later using Cisco SD-WAN Manager.

To verify the current firmware version of a Wi-Fi module, use the `show wireless-bridge status` CLI command.

Restrictions for Cellular Modem Firmware Upgrade

- After downloading a firmware upgrade file from Cisco.com, do not change the filename. A device uses the filename to determine which firmware upgrade files are relevant to it.
- Cisco SD-WAN Manager only supports upgrading the currently active firmware type. For example a device may have five different firmware types, such as generic and firmware for four specific carriers. Only one firmware type can be active at a given time and Cisco SD-WAN Manager upgrades only the the active one.
- Firmware downgrade is not supported by Cisco SD-WAN Manager.
- The P-LTE-450 firmware upgrade will not start if the device is turned off or unreachable.

Order of firmware upgrade

Upgrade Sequence

The firmware upgrade process follows a specific order of precedence based on the firmware files present on the remote server. Modules are upgraded in this order:

- Wi-Fi Module
- P-LTE-450 module
- LTE module

To ensure the correct module is upgraded, save only the relevant firmware files on the remote server.

For example, if you want to upgrade the firmware for LTE modules, make sure that no Wi-Fi firmware files are stored on the server. If firmware files for other modules, such as Wi-Fi or P-LTE-450 module are present, those modules will be upgraded first, following the precedence order, even if you do not intend to upgrade them.

Note For WI-FI modules, the upgrade process works only when the device is in Workgroup Bridge (WGB) mode.

If the Wi-Fi module is turned off or unreachable, Wi-Fi module firmware upgrade will be skipped and cellular modem firmware upgrade will continue.

Upgrade the Cellular Modem Firmware of a Device

Before You Begin

- See the prerequisites and restrictions sections of this documentation.
- Download firmware upgrade files from the Cisco Software Download site.
- Save the downloaded firmware upgrade files to a file server accessible by devices in the network. The file types of the downloaded files may differ, according to the different modem hardware used in your Cisco products. Example file types include .bin, .cwe, .nvu, and .spk.

  You can download firmware upgrade files for different types of cellular-enabled devices and in most cases, save them to the same directory on the file server. If the firmware upgrade for your device requires two files for two upgrade steps (a modem firmware upgrade file, and a separate OEM PRI file) save the two files to separate directories.

Upgrade the Cellular Modem Firmware of a Device

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Firmware Upgrade**.
2. In the workflow, follow the prompts to select the devices to upgrade, the server, and the firmware image path.

   When configuring a server for storing firmware upgrade images, enter the following fields:

Field	Description
Server Name	Enter a name for the file server with the firmware upgrade files.
Server IP or DNS Name	IP address or DNS name of the file server.
Protocol	Choose the SCP protocol.
Port	Enter the port that you have configured for the remote server. Default (for SCP): 22
User ID, Password	Enter the login credentials for the file server.
Image Location Prefix	Enter the path to the directory storing the firmware upgrade files.
VPN	Enter the VPN that you have configured for reaching the remote server interface.

Note For information about configuring a remote server for storing device software upgrade images, see Register Remote Server in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

If a relevant firmware upgrade file exists at the image path location, the device uses the file for the upgrade. If more than one relevant firmware upgrade file is available, the device uses the latest version. If no

relevant file exists at the image path location, the **Summary** page of the workflow indicates that no file is available, and no firmware upgrade occurs.

Cisco SD-WAN Manager upgrades only the currently active firmware type.

Note The workflow prompts you to configure a remote server. Alternatively, you can configure a file server as described in Configure a Remote File Server for Firmware Upgrade Images, on page 77.

3. Optionally, schedule the upgrade for a specific time, for example to coincide with a maintenance window.

Note To cancel a scheduled upgrade before it occurs, do the following:

   a. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.

   b. Click **Firmware**.

   c. Click **Cancel Firmware Upgrade** to cancel a scheduled upgrade.

4. On the **Summary** page, review the details and click **Next** to begin the upgrade task.

   The upgrade takes several minutes.

5. (Optional) Click **Check my upgrade task** to show the status of the upgrade or upgrades for each device.

View the Status of a Cellular Modem Firmware Upgrade

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **Firmware**.

   The table shows devices in the process of firmware upgrade or awaiting a scheduled upgrade. See the **CurrentVersion** column to view the firmware version of a device.
3. (Optional) Click **Cancel Firmware Upgrade** to cancel a scheduled upgrade.

Configure a Remote File Server for Firmware Upgrade Images

Before You Begin

This procedure addresses configuring a remote server for firmware upgrade images, for the firmware upgrade use case. For information about configuring a remote server for storing device software upgrade images, see Register Remote Server in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Configure a Remote File Server for Firmware Upgrade Images

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** and click **Remote Server**.
2. Click **Add Remote Server** and enter the following fields:

Field	Description
Server Name	Enter a name for the file server with the firmware upgrade files.
Server IP or DNS Name	IP address or DNS name of the file server.
Protocol	Choose the SCP protocol.
Port	Enter the port that you have configured for the remote server. Default (for SCP): 22
User ID, Password	Enter the login credentials for the file server.
Image Location Prefix	Enter the path to the directory storing the firmware upgrade files, or enter **/** by itself, which enables you to specify the path while executing the Firmware Upgrade workflow.
VPN	Enter the VPN that you have configured for reaching the remote server interface.

3. Click **Add**.

Firmware upgrade for P-LTE-450 MHz modules

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you can upgrade the firmware for P-LTE-450 MHz modules on Cisco IOS XE Catalyst SD-WAN devices from the Cisco SD-WAN Manager.

A P-LTE-450 module firmware upgrade is a process that:

- provides you a simplified workflow in Cisco SD-WAN Manager for upgrade,
- enables you to upgrade multiple devices at the same time, and
- allows you to track upgrade status and schedule tasks from a central interface.

Firmware upgrade for Wi-Fi modules

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you can upgrade the Wi-Fi modules (PID is WP-WIFI6) on Cisco IOS XE Catalyst SD-WAN devices directly from the Cisco SD-WAN Manager.

A Wi-Fi module firmware upgrade is a process that:

- provides you a simplified workflow in Cisco SD-WAN Manager for upgrade,
- enables you to upgrade multiple devices at the same time, and

- allows you to track upgrade status and schedule tasks from a central interface.

Upgrading module firmware using Cisco SD-WAN Manager

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1and Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the following module firmware upgrades are supported:

- P-LTE-450 MHz module
- Wi-Fi module

Summary

The module firmware upgrade process involves a sequence of actions between the SD-WAN Manager, remote server, and devices. Cisco SD-WAN Manager sends the necessary instructions to each device, which then performs pre-checks, downloads, validates, and installs the firmware. Throughout the process, Cisco SD-WAN Manager provides real-time status updates, allowing you to monitor and confirm the completion of the upgrade across all selected devices.

Workflow

These are the stages of upgrading firmware for P-LTE-450 MHz and Wi-Fi modules:

1. Identify device or module: Identify the device or module that requires a firmware upgrade. Cisco SD-WAN Manager displays the list of devices that are eligible for firmware upgrade. Each of these devices have either a Wi-Fi module, P-LTE-450 MHz module, or a cellular modem or a combination of these.

   Before you proceed with upgrading the firmware for the module, make a note of which devices to upgrade. This is an important step because firmware upgrade is done in a specific order. For more information, see Order of firmware upgrade, on page 75.

2. Download firmware files: Download the firmware files for the Wi-Fi module from Cisco Software Central. All the firmware files are hosted on Cisco Software Central. After identifying the device to be upgraded, search and download the specific firmware software.

   Download the firmware files for the P-LTE-450 MHz module from the Intelliport product website. For any assistance, contact the Intelliport representatives. You can download the Pluggable Interface Module (PIM) firmware or modem firmware or both.

   Save the downloaded firmware upgrade files to a file server accessible by devices in the network.

3. Configure a remote server to host the firmware image:

   The P-LTE-450 PIM has an integrated modem, which is a core component for establishing and managing the connection to the LTE 450 MHz mobile networks. The firmware upgrade of P-LTE-450 module includes upgrading the PIM firmware and the modem firmware.

   There are two phases in the P-LTE-450 firmware upgrade process, each using a separate firmware file. The sequence of upgrade is as follows:

   a. Modem firmware is upgraded first

b. PIM firmware is upgraded next

You can also upgrade the modem firmware and PIM firmware seperately. If the firmware upgrade fails either for PIM or modem, an error message with error details appears on Cisco SD-WAN Manager.

To configure remote file server for firmware upgrade, see Configure a Remote File Server for Firmware Upgrade Images, on page 77.

4. Understand the order of upgrading firmware:The firmware upgrade process follows a specific order of precedence based on the firmware files present on the remote server. For more information, see Order of firmware upgrade, on page 75

.

5. Start or Schedule the firmware upgrade: Use the firmware upgrade workflow in Cisco SD-WAN Manager. You can start the upgrade right away or schedule it for a specific time, for example to coincide with a maintenance window. For more information, see Upgrade the firmware for P-LTE-450 MHz or Wi-Fi modules, on page 80.
6. Processing upgrade: Cisco SD-WAN Manager sends an upgrade request, including server details and the firmware path, to each device for the modules requiring an upgrade. Each device verifies the files, then downloads and installs the firmware either at the scheduled time or immediately.
7. Track progress: Use Cisco SD-WAN Manager to monitor the status of your firmware upgrades.
8. Upgrade execution: After verification, the P-LTE-450 MHz or the Wi-Fi module firmware is upgraded.
9. Verify the firmware upgrade: After the upgrade, verify that the devices have successfully updated to the new firmware version. For more information, see View the Status of a Cellular Modem Firmware Upgrade, on page 77.

Upgrade the firmware for P-LTE-450 MHz or Wi-Fi modules

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 and Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

This section provides the steps to upgrade the firmware on your Cisco IOS XE Catalyst SD-WAN device.

Before you begin

- See the prerequisite and restrictions sections.
- See the Supported Platforms for Cellular Modem Firmware Upgrade, on page 74 section.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Firmware Upgrade**.

Step 2 In the workflow, follow the prompts to choose the devices to upgrade. Proceed with one of the methods in the following table based on your scenario.

If..	Then..
If you have configured the remote server for storing firmware image files.	Follow the prompts to choose the server, and the firmware image path.
If you want to configure a remote server in the firmware upgrade workflow.	After choosing the device or devices to upgrade, configure a remote file server for the firmware upgrade images. To configure a remote file server, click the **Select remote server** dropdown, then click **Create New**, and enter the following fields in the **Add Remote Server**. See the following table "Add Remote Server" to enter the fields.
If you want to configure a remote server from **Maintenance** > **Software Repository**.	Configure a file server as described in Configure a Remote File Server for Firmware Upgrade Images, on page 77.

Table 16: Add Remote Server

Field	Description
Server Name	Enter a name for the file server with the firmware upgrade files.
Server IP or DNS Name	IP address or DNS name of the file server.
Protocol	Choose the SCP protocol. **Note** For P-LTE-450 MHz and Wi-Fi modules, choose only SCP protocol.
Port	Enter the port that you have configured for the remote server. Default (for SCP): 22
User ID and Password	Enter the login credentials for the file server.
Image Location Prefix	Enter the path to the directory storing the firmware upgrade files.
VPN	Enter the VPN that you have configured for reaching the remote server interface.

The following table describes different scenarios when one, multiple, or no relevant firmware upgrade files are found at the specified location.

Table 17: Image Path Location

If..	Then..
If a relevant firmware upgrade file exists at the image path location.	The device uses the file for the upgrade.
If more than one relevant firmware upgrade file is available.	The device uses the latest version.
If no relevant file exists at the image path location.	The device checks the availability of files on the specified remote server. The firmware upgrade fails if no valid files are found on the remote server. This status is indicated in the **Summary** page of the workflow.

Cisco SD-WAN Manager upgrades only the currently active firmware type.

Step 3 If you have not configured a remote server, you can configure it after selecting a device. To configure a remote file server for firmware upgrade images, click the **Select remote server** dropdown, then click **Create New**, and enter the required fields.

Step 4 Optionally, schedule the upgrade for a specific time, for example to coincide with a maintenance window.

Step 5 On the **Summary** page, review the details and click **Next** to begin the upgrade task.

Step 6 (Optional) Click **Check my upgrade task** to see the status of the upgrade or upgrades for each device.

What to do next

View status of the firmware upgrade, View the Status of a Cellular Modem Firmware Upgrade

Upgrade the firmware for Cellular or Wi-Fi modules

This section provides the steps to upgrade the firmware on your Cisco IOS XE Catalyst SD-WAN device.

Before you begin

- See the prerequisite and restrictions sections.
- See the Supported Platforms for Cellular Modem Firmware Upgrade, on page 74 section.

Procedure

Step 1 From the SD-WAN Manager menu, choose **Workflows** > **Workflow Library** > **Firmware Upgrade**.

Step 2 In the workflow, follow the prompts to choose the devices to upgrade. To begin with, choose the type of module for firmware upgrade.

- Cellular module
- Wi-Fi
- Cellular LTE 450 MHz

Note
You can choose module type for firmware upgrade only on devices running SD-WAN Manager 26.1.1.1 or higher.

For devices running versions earlier than SD-WAN Manager 26.1.1.1, SD-WAN Manager performs the firmware upgrade based on the firmware image stored in the remote server.

For all device versions, modules are upgraded in this order:

a. Wi-Fi Module

b. P-LTE-450 module

c. Cellular module

Step 3 Choose the reachable device or devices for firmware upgrade.

Based on the module type you choose in Step 2, SD-WAN Manager will filter and display only devices that support that specific module type. For example, if you choose **Wi-Fi**, SD-WAN Manager will list only devices with Wi-Fi module support.

Note
SD-WAN Manager filters devies based on the supported module type but not based on the presence of the module on the device.

Step 4 Proceed with one of the methods in the following table based on your scenario.

If..	Then..
If you have configured the remote server for storing firmware image files.	Choose the remote server from the **Host server** dropdown, and the firmware **Image path**.
If you want to configure a remote server in the firmware upgrade workflow.	To configure a remote file server, click **+ Add new remote server**, and enter the required fields. See the following table "Add Remote Server" to enter the fields.
If you want to configure a remote server from **Maintenance** > **Software Repository**.	Configure a file server as described in Configure a Remote File Server for Firmware Upgrade Images, on page 77.

Table 18: Add Remote Server

Field	Description
Server Name	Enter a name for the file server with the firmware upgrade files.
Server IP or DNS Name	IP address or DNS name of the file server.
Protocol	Choose the SCP protocol. **Note** For P-LTE-450 MHz and Wi-Fi modules, choose only SCP protocol.
Port	Enter the port that you have configured for the remote server. Default (for SCP): 22
User ID and Password	Enter the login credentials for the file server.
Image Location Prefix	Enter the path to the directory storing the firmware upgrade files.
VPN	Enter the VPN that you have configured for reaching the remote server interface.

The following table describes different scenarios when one, multiple, or no relevant firmware upgrade files are found at the specified location.

Table 19: Image Path Location

If..	Then..
If a relevant firmware upgrade file exists at the image path location.	The device uses the file for the upgrade.

If..	Then..
If more than one relevant firmware upgrade file is available.	The device uses the latest version.
If no relevant file exists at the image path location.	The device checks the availability of files on the specified remote server. The firmware upgrade fails if no valid files are found on the remote server. This status is indicated in the **Summary** page of the workflow.

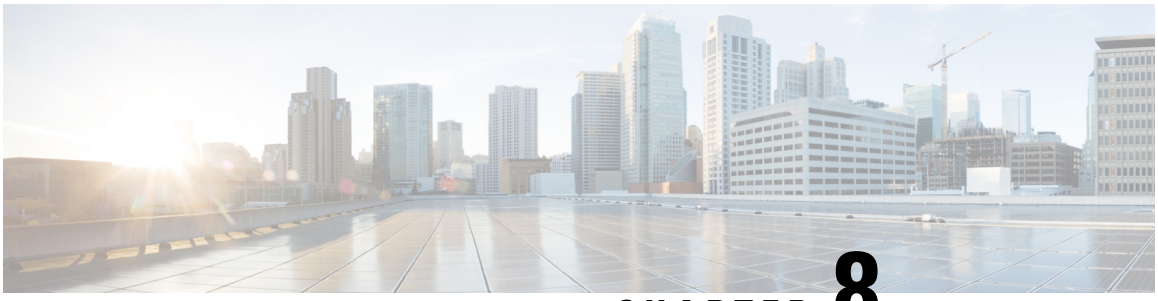
SD-WAN Manager upgrades only the currently active firmware type.

Step 5 (Optional) Schedule the upgrade for a specific time, for example to coincide with a maintenance window.

Step 6 On the **Summary** page, review the details and click **Schedule upgrade** to begin the upgrade task.

What to do next

View status of the firmware upgrade, View the Status of a Cellular Modem Firmware Upgrade



CHAPTER 8

Management of Virtual Machine Hosting an SD-WAN Control Component

Upgrade memory and vCPU resources on a virtual machine hosting Cisco Catalyst SD-WAN Manager

Only memory or vCPU increase is allowed. After the memory or vCPU is upgraded, you cannot downgrade.

Procedure

Step 1 Check the current configuration on Cisco SD-WAN Manager using the **show system status** command.

```
vManage# show system status
Viptela (tm) vmanage Operating System Software
Copyright (c) 2013-2021 by Viptela, Inc.
Controller Compatibility:
Version: 20.7.0-185
Build: 185
System logging to host  is disabled
System logging to disk is enabled
System state:            GREEN. All daemons up
System FIPS state:       Enabled
Testbed mode:            Enabled
Engineering Signed:      True
Last reboot:             Initiated by user.
CPU-reported reboot:     Not Applicable
Boot loader version:     Not applicable
System uptime:           1 days 02 hrs 44 min 52 sec
Current time:            Sat Oct 23 22:12:10 UTC 2021
Load average:            1 minute: 14.58, 5 minutes: 12.31, 15 minutes: 10.73
Processes:               5775 total
CPU allocation:          32 total
CPU states:              31.58% user,   4.36% system,   64.06% idle
Memory usage:            65741448K total,    38096172K used,   490324K free
```

```
                        4606444K buffers,  22548508K cache
Disk usage:             Filesystem      Size   Used  Avail   Use %  Mounted on
                        /dev/root       15230M  3496M  10898M   24%   /
vManage storage usage:  Filesystem      Size  Used  Avail  Use%  Mounted on
                        /dev/sdb        502942M  206906M  270435M   41%   /opt/data
Personality:            vmanage
Model name:             vmanage
Services:               None
vManaged:               false
Commit pending:         false
Configuration template: None
Chassis serial number:  None
```

Step 2 Power the device down to upgrade the memory.

Step 3 Upgrade the CPU and memory for the VM using the guidelines of the hosting platform. You can make the following upgrades:

Resources	Current	Upgrade
vCPU	16	32
Memory	32 G	64 G or 128 G
Memory	64 G	128 G

Step 4 Power on the device and verify the memory and CPU.

```
vManage1# show system status
Viptela (tm) vmanage Operating System Software
Copyright (c) 2013-2021 by Viptela, Inc.
Controller Compatibility:
Version: 20.7.0-139
Build: 139
System logging to host  is disabled
System logging to disk is enabled
System state:           GREEN. All daemons up
System FIPS state:      Enabled
Testbed mode:           Enabled
Engineering Signed:     True
Last reboot:            Initiated by user - activate 20.7.0-139.
CPU-reported reboot:    Not Applicable
Boot loader version:    Not applicable
System uptime:          16 days 17 hrs 43 min 28 sec
Current time:           Sat Oct 23 22:22:16 UTC 2021
Load average:           1 minute: 15.86, 5 minutes: 13.02, 15 minutes: 11.45
Processes:              6067 total
CPU allocation:         32 total
CPU states:             32.13% user,   4.34% system,   63.53% idle
Memory usage:           131703148K total,    88221488K used,   19285636K free
                        7022488K buffers,  17173536K cache
Disk usage:             Filesystem      Size   Used  Avail   Use %  Mounted on
                        /dev/root       15998M  10702M  4461M   71%   /
vManage storage usage:  Filesystem      Size  Used  Avail  Use%  Mounted on
                        /dev/sdb        10402115M  702212M  9175615M   6%   /opt/data
Personality:            vmanage
Model name:             vmanage
Services:               None
vManaged:               false
Commit pending:         false
```

```
Configuration template:  None
Chassis serial number:   None
```

Expand the secondary disk size, Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier

Before you begin

Ensure that you are on Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier.

Due to a known limitation, this procedure is not effective for Cisco Catalyst SD-WAN Manager Release 20.13.x, 20.14.x, or 20.15.x.

Perform these steps to increase the size of the secondary disk on the virtual machine hosting a Cisco SD-WAN Manager instance.

Procedure

Step 1 Shut down the virtual machine hosting Cisco SD-WAN Manager .

Step 2 Using the hypervisor (for example, ESXi, Azure, or AWS), provision additional space for the secondary disk of the virtual machine hosting Cisco SD-WAN Manager .

Step 3 Restart the VM that is hosting Cisco SD-WAN Manager .

Step 4 In Cisco SD-WAN Manager, enter the following to enable Cisco SD-WAN Manager to detect the additional disk space and extend the file system to use the space.

```
vm# request nms application-server resize-data-partition
```

Step 5 Enter the following commands to confirm that the /opt/data disk has been resized.

```
vm# vshell
vm:~$ df -hk | grep data
```

The output shows the new disk size.