# Install and Upgrade for Cisco Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later


- Install and Upgrade Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later, on page 2
- Platforms Supported in Controller Mode, on page 2
- Cisco IOS XE Image Compatibility, on page 3
- Upgrade Considerations, on page 4
- Restrictions, on page 6
- Self-Signed Trustpoint, on page 6
- Introducing Autonomous and Controller Mode, on page 6
- Software Installation for Cisco IOS XE Routers, on page 7
- Plug and Play in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later Releases, on page 9
- Non-PnP Onboarding, on page 12
- Mode Discovery and Mode Change with Bootstrap Files, on page 15
- Reset Controller Mode Configuration, on page 17
- Mode Switching: Additional Information, on page 19
- Verify Controller and Autonomous Modes, on page 19
- Change the Console Port Access After Installation, in Controller Mode, on page 20
- Upgrade to Cisco IOS XE Release 17.2.1r or Later, on page 22
- Downgrade from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or Later Releases, on page 26
- Restore Smart Licensing and Smart License Reservation, on page 28
- Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing, on page 28
- Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices, on page 30
- Troubleshooting, on page 31

# Install and Upgrade Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later

*Table 1: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Install and Upgrade | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r | This feature supports the use of a single "universalk9" image to deploy Cisco IOS XE Catalyst SD-WAN and Cisco IOS XE functionality on all the supported devices. This universalk9 image supports two modes - Autonomous mode (for Cisco IOS XE features) and Controller mode (for Cisco Catalyst SD-WAN features) . |
| Cisco Catalyst 8000V Edge SoftwarePlatform | Cisco IOS XE Catalyst SD-WAN Release 17.4.1a | Support added for the Cisco Catalyst 8000V Edge Software platform. Upgrading Cisco CSR1000V or Cisco ISRv platforms to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a includes upgrading to the platform type to the Cisco Catalyst 8000V. |

Starting with 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.

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

This release helps in seamless upgrades of both the Cisco Catalyst SD-WAN and non Cisco Catalyst SD-WAN features and deployments.

Access the Cisco IOS XE and Cisco IOS XE Catalyst SD-WAN functionality through Autonomous and Controller execution modes, respectively. The Autonomous mode is the default mode for the routers and includes the Cisco IOS XE functionality. To access Cisco IOS XE Catalyst SD-WAN functionality, switch to the Controller mode. You can use the existing Plug and Play Workflow to determine the mode of the device.

# Platforms Supported in Controller Mode

### Platforms Supported in Controller Mode

- Cisco ASR 1000 Series Aggregation Services Routers
- Modular Cisco ASR 1006-X with ASR1000-RP3 module (Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or later, see Cisco ASR 1006-X with an RP3 Module.)

- Cisco ISR 1000 Series Integrated Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco 1101 Industrial Integrated Services Router
- Cisco CSR 1000v Series Cloud Services Routers
- Cisco Integrated Services Virtual Router (ISRv)
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 Series Edge Platforms
- Cisco Catalyst 8000V Edge Software (Cisco IOS XE Catalyst SD-WAN Release 17.4.1a or later)

### Platforms Not Supported in Controller Mode

Modular platforms based on the following ASR 1000 Series Routers are not supported in controller mode:

- ASR1000-RP2

### Crypto Modules Supported in Controller Mode

The following crypto modules are required for the ASR 1000 series routers:

- ASR1001HX-IPSECHW, for the ASR 1001-HX
- ASR1002HX-IPSECHW, for the ASR 1002-HX

# Cisco IOS XE Image Compatibility

| Deployment Image Version | Cisco Catalyst SD-WAN | Non Cisco Catalyst SD-WAN |
|---|---|---|
| Cisco IOS XE Releases 16.9.x, 16.10.x, 16.11.x, 16.12.x | ucmk9 | universalk9 |
| Cisco IOS XE Release 17.1.x | NA | universalk9 |
| Cisco IOS XE Release 17.2.x and later | universalk9* | universalk9** |

- * For Cisco Catalyst SD-WAN use case, non-LI and non-payload encryption image types are not supported.
- ** For non Cisco Catalyst SD-WAN use case, non-LI and non-payload encryption image types are supported (universalk9_noli, universalk9_npe, universalk9_npe_noli).

# Upgrade Considerations

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

These devices support auto-negotiation on 10G interfaces ports with 1GE SFP (optical and CU) modules. The following notes apply to auto-negotiation in both SD-WAN and non-SD-WAN modes of the above three router models only:

- For releases before Cisco IOS XE 17.6.1a, auto-negotiation can be configured using the CLI.
- 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.
- 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.
- On software releases upto Cisco IOS XE Release 17.6.3a, the **`negotiation auto`** command is not supported on a 10G interface that includes a 10GE SFP+ module.
- 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/x/x`**, 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.
- 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.
- On software releases upto 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.
- 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 no negotiation auto`** to all 10G interfaces that include a 10GE 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.
- 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.

- In ASR 1001-HX, multi-rate supported only on last 4 ports of bay1 8X10G/1G.
- After upgrading the device, configurations for new features in the updated version are not applied automatically. To enable these new features, you must manually redeploy the template or configuration group.
- When a Cisco IOS XE Catalyst SD-WAN 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.

Following notes are applicable for C8300, C8500L-8S4X models of routers:

- From Cisco IOS XE Release 17.15.1 onwards, the **`negotiation auto`** command is supported on a 10G interface that includes a 10GE SFP+ module.
- From Cisco IOS XE Release 17.15.1 onwards, on a 10G interface that includes a 10GE SFP+ module, in the output of **`show interface Tengig x/x/x`** the link type will show as force-up always regardless of **`negotiation auto/no negotiation auto`** configuration. The same is applicable when the configurations are pushed through Cisco SD-WAN Manager template.
- 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 display for dual rate ports with 10G optics.

***Table 2: Auto Negotiation Configurations***

| **C8500** | | | |
|---|---|---|---|
| SFPs | Default Auto Negotiation | Default Speed | Default Duplex |
| 1G Copper | OFF | 1000M | Full |
| 1G Optical | OFF | 1000M | Full |
| 10G Optical | OFF | 10000M | Full |
| **C8300** | | | |
| 1G Copper | ON | 1000M | Full |
| 1G Optical | ON | 1000M | Full |
| 10G Optical | ON | 10000M | Full |

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

# Restrictions

### Restrictions for single "universalk9" image

- Dual-IOSd is supported only in autonomous mode.
- Images without payload encryption and NO-LI (universalk9_npe, universalk9_noli, universalk9_npe_noli) images are not supported in controller mode. Only universalk9 images are supported.
- After onboarding and determining the mode of operation, changing from Controller mode to Autonomous mode or vice-versa, results in the loss of configuration.
- Reset button functionality is not supported in controller mode on Cisco ISR 1000 series Integrated Service Routers. The reset button does not function to restore a golden image or configuration in controller mode.
- Auto-install (Python and TCL scripts) and ZTP—Autoinstall and ZTP are not supported in controller mode. If DHCP discovers an attempt to install using either of these processes, a mode change to Autonomous mode is triggered.
- WebUI—In controller mode, WebUI is not supported and an error message is displayed, if used.

# Self-Signed Trustpoint

A self-signed trustpoint is generated and loaded to a Cisco IOS XE Catalyst SD-WAN device when the device boots up. If this trustpoint is deleted for any reason, you can generate and load a new trustpoint by rebooting the device. The new key may be different than the deleted one.

# Introducing Autonomous and Controller Mode

The Cisco IOS XE Catalyst SD-WAN Release 17.2.1r release introduces two installation modes – Autonomous and Controller modes. The autonomous mode supports the functionality of Cisco IOS XE non Cisco Catalyst SD-WAN deployment and the controller mode supports the Cisco Catalyst SD-WAN solution.

The following are the main differences between Autonomous mode and Controller mode:

***Table 3:***

| Feature | Autonomous Mode | Controller Mode |
|---|---|---|
| Configuration Method | • Command Line Interface (CLI)<br>• NETCONF | YANG-based configuration<br>• Cisco SD-WAN Manager<br>• NETCONF |

| Feature | Autonomous Mode | Controller Mode |
|---|---|---|
| Onboarding Modes | • Plug and Play<br>• Config-Wizard<br>• WebUI<br>• Bootstrap (USB, bootflash, and so on)<br>• Auto-Install (Python Script, TCL Script)<br>• ZTP (Using DHCP Option 150 and Option 67) | • Plug and Play<br>• Bootstrap (USB, bootflash, and so on) |
| Licensing | Cisco Smart Licensing | Cisco High Performance Security (HSEC) software licensing. No device licensing. |
| Image Type | Universalk9 | Universalk9 |
| Dual-IOSd redundancy model | Supported | Not Supported |
| High Availability | Supported | Not Supported |
| Global configuration mode | configure terminal | config-transaction |

# Software Installation for Cisco IOS XE Routers

## Download the Software for Cisco IOS XE Release 17.2.1r or Later

Download the *router-model*-universalk9.*release-number*. image for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later software from the Cisco site https://software.cisco.com .

## Install Software on Cisco ASR, Cisco ISR and Cisco ENCS Platforms

Refer to the following documents for installation instructions:

- Cisco ISR 1000 Series Integrated Services Router
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Installing Cisco Enterprise NFVIS on Cisco ENCS 5100 and ENCS 5400

# Install Software on Cisco CSR 1000v Platform

Based on the cloud in which you are deploying the CSR 1000v instance, see the following to perform the bootstrap and/or the day 0 configuration:

- Deploying the OVA to the VM
- Manually creating the Cisco CSR 1000v VM using the .iso file (Citrix XenServer)
- Creating a CSR 1000v VM using the self installing .run package
- Manually creating the VM using the .iso file (Microsoft Hyper-V)
- Booting the CSR 1000v Instance
- Deploying a CSR 1000v VM Using Custom Data
- Deploying a CSR 1000v VM on Microsoft Azure

# Install a Cisco Catalyst 8000V Edge Software Platform

***Table 4: Feature History***

| Feature Name | Release Information | Description |
|---|---|---|
| Support for the Cisco Catalyst 8000V Edge Software Platform on OpenStack Train | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a | This feature introduces support for managing a Cisco Catalyst 8000V Edge software platform hosted in the OpenStack cloud computing platform "Train" release. |

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco Catalyst SD-WAN supports the Cisco Catalyst 8000V virtual router platform, which replaces the Cisco CSR1000V and Cisco ISRv. Installing the Cisco Catalyst 8000V in an Cisco Catalyst SD-WAN environment requires Cisco vManage Release 20.4.1 or later.

Download the Cisco Catalyst 8000V software image that is appropriate for your method of deployment. For example, this can be an OVA file for ESXi, or a QCOW2 image for OpenStack or KVM. Do not choose an ISO image. Have the image ready to upload to the Cisco SD-WAN Manager software image repository. The file name begins with: c8000v-universalk9

**Note** To operate with Cisco Catalyst SD-WAN, the device must be in controller mode. When starting the device in controller mode, boot the device using the bootflash:packages.conf file.

For complete information about the platform, including installation in KVM, ESXi, and OpenStack environments, see the Cisco Catalyst 8000V Edge Software Installation and Configuration Guide. For information about creating a bootstrap file for onboarding the Cisco Catalyst 8000V into Cisco Catalyst SD-WAN, see Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices.

### Clean Install

We recommend a clean install of the Cisco Catalyst 8000V. This ensures support for all features, provides the most up-to-date licensing, and ensures that devices and the controller stay synchronized. For cases where upgrade is necessary, see the procedure in **Upgrade to Cisco IOS XE Release 17.2.1r or Later**.

**Note** After a clean install of the Cisco Catalyst 8000V, it is not possible to downgrade the device to a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.4.1a.

### Upgrading a Cisco CSR1000V to a Cisco Catalyst 8000V

Upgrading a Cisco CSR1000V or Cisco ISRv virtual router to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a includes upgrading to the Cisco Catalyst 8000V. Note the following:

- The Cisco Catalyst 8000V preserves all of the functionality available on Cisco CSR1000V or Cisco ISRv platforms.
- Performing the upgrade in Cisco SD-WAN Manager preserves the configuration of the device(s) being upgraded.

### OpenStack

Installing a Cisco Catalyst 8000V on the OpenStack Train release requires using a Cisco IOS XE Catalyst SD-WAN Release 17.7.1a or later image for the Cisco Catalyst 8000V.

Cisco does not support installing a Cisco Catalyst 8000V on OpenStack using an earlier image, or installing on OpenStack using an earlier image and upgrading to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

# Plug and Play in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and Later Releases

## Plug and Play Onboarding Workflow

1. Place an order for the device in Cisco Commerce with Smart Account and Virtual Account details of the customer.
2. The device information from Cisco Commerce like Device serial number, Smart Account, and Virtual Account are added to the Plug and Play portal.
3. Add a Cisco SD-WAN Validator controller profile into the Plug and Play (PnP) portal for the same Smart Account and Virtual Accounts.
4. Associate the new device to the Cisco SD-WAN Validator controller profile manually.
5. PnP sends all relevant information including Cisco SD-WAN Validator details, device serial number, organization name, and network ID to Zero Touch Provisioning (ZTP).
6. Download the device serial number file (provisioning file) from PnP and upload it to Cisco SD-WAN Manager. The devices are now available on Cisco SD-WAN Manager. You can also use the **Sync Smart**

**Account**option on Cisco SD-WAN Manager to sync the device with your virtual account and populate the device in Cisco SD-WAN Manager.

**Note** If you created and scheduled a device template on Cisco vManage Release 20.3.x and upgraded Cisco SD-WAN Manager to Cisco vManage Release 20.4.1 or later before onboarding the target device, when you onboard the device using PNP or ZTP, the template push fails. To avoid this failure, reschedule the template after upgrading the Cisco SD-WAN Manager software and then onboard the device.

**Note** If the ZTP process for a device is interrupted because the device reloads or power cycles, the ZTP process does not restart and the device comes online with the Cisco SD-WAN Manager image that was in its original configuration. In this situation, upgrade the device to the desired Cisco SD-WAN Manager release manually.

**Note** For more information, refer to the Plug and Play Support Guide.

# Mode Discovery with Plug and Play Onboarding

The PnP-based discovery process determines the mode in which the device operates, based on the controller discovery and initiates a mode change, if required. The mode change results in a reboot of the device. Once reboot is complete, the device performs appropriate discovery process.

When you upgrade to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later, on a Cisco device that already runs a Cisco IOS XE or Cisco Catalyst SD-WAN image, the device starts in autonomous mode or controller mode depending on the configured controller.

Plug and Play (PnP) deployment include the following discovery process scenarios:

***Table 5:***

| Boot up Mode | Deployment Mode | On-boarding agent | Cisco SD-WAN Validator | Discovery Process | Mode Change |
|---|---|---|---|---|---|
| Autonomous | Cisco Digital Network Architecture (DNA) | Plug and Play | No | Plug and Play Connect Discovery or on-premise plug and play server discovery | No Mode change |
| Autonomous | Cisco SD-WAN Manager | Plug and Play | Yes | Plug and Play Connect Discovery | Mode change to controller mode |

| Boot up Mode | Deployment Mode | On-boarding agent | Cisco SD-WAN Validator | Discovery Process | Mode Change |
|---|---|---|---|---|---|
| Controller | Cisco DNA | Plug and Play | No | Plug and Play Connect Discovery or on-premise plug and play server discovery | Mode change to autonomous mode |
| Controller | Cisco SD-WAN Manager | Plug and Play | Yes | Plug and Play Connect Discovery | No mode change |

# Automatic IP Address Detection

*Table 6: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Day 0 WAN Interface Automatic IP Detection using ARP | Cisco IOS XE Catalyst SD-WAN Release 17.7.1a<br>Cisco SD-WAN Release 20.7.1<br>Cisco vManage Release 20.7.1 | This feature enables a device to automatically learn about the available IP addresses and default gateway information when a DHCP server is not available. The device assigns an IP address to its WAN interface, and then contacts the PnP server and begins the PnP onboarding process. |

Typically, the WAN interface on a Cisco IOS XE Catalyst SD-WAN device or Cisco vEdge device is configured as a DHCP client, and this interface receives an IP address and gateway server information from the DHCP server during the plug-and-play (PnP) onboarding process.

If the DHCP server is not available, the device automatically learns about the available IP addresses and default gateway information by using Address Resolution Protocol (ARP) packets. If an IP address that the device learns allows a successful connection to the PnP server, the device continues with the PnP onboarding process.

**Note** This feature applies only to day zero deployments and is enabled by default.

**Prerequisites for Automatic IP Address Detection**

- To trigger ARP, configure the IP address of the device as the BGP neighbor on the provider edge (PE) router.

  This PE router is the first point of contact for the device in the WAN transport network. The PE router then sends ARP packets with this IP address to the device. The device receives the ARP packets, and then the Automatic IP Address Detection feature defines the ARP destination IP address as the device's WAN interface IP address.

- For Cisco IOS XE Catalyst SD-WAN devices, the network mask of this IP address must be 30 bits.

- For automatic IP address detection and redirection through an on-premises ZTP server, the A record of the ZTP server on the DNS server must be set to ztp.cisco.com. In addition, the DNS server must have an ip name-server value of 8.8.8.8 or 8.8.4.4.

For automatic IP address detection, a device uses 8.8.8.8 or 8.8.4.4 as the DNS server to resolve devicehelper.cisco.com or ztp.cisco.com. The PnP process then attempts to reach devicehelper.cisco.com or ztp.cisco.com to continue onboarding.

**Note** An IP address that a device automatically detects is not preserved during reboots of the device that occur before the PnP onboarding completes. In such cases, an IP address is assigned automatically when the PE router ARP cache expires.

**Limitations and Restrictions for Automatic IP Address Detection**

The following limitations and restrictions apply only to Cisco IOS XE Catalyst SD-WAN devices:

- This feature is supported only on Cisco 1000 Series Integrated Service Routers, Cisco 4000 Series Integrated Service Router, and Cisco Catalyst 8200 and 8300 Series Edge Platforms. On these devices, this features is supported only for Gigabit Ethernet Interface 0/0/0.
- The feature is supported only on devices that are in controller (SD-WAN configuration) mode. See https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/install-upgrade-17-2-later.html.
- This feature is supported only in a simple 30 bit network mask Layer 2 network in which one PE router and one customer edge router are in the same VLAN.
- This feature does not support VRRP, HSRP, or GLBP on the PE router.
- An ARP destination IP address is used as the WAN interface IP address on a device only after the device receives the same ARP request eight times within an interval of 150 seconds.

# Non-PnP Onboarding

## Creating a Cisco Catalyst SD-WAN Bootstrap Configuration File

See On-Site Bootstrap Process for Cisco Catalyst SD-WAN Devices and Generate a Bootstrap File For Cisco IOS XE Catalyst SD-WAN Devices Using the CLI for information about generating a bootstrap file.

## New Installation: Mode Change Device Day Zero Scenario

1. If the device is running a pre-17.2 universalk9 image on a new box, or for an existing box where you performed **write erase** and **reload** and loaded a Cisco IOS XE 17.2 or newer image, the device boots in day zero configuration and in autonomous mode.
2. The new device determines if a mode change is required based on the bootstrap file.

- If ciscosdwan.cfg or ciscosdwan_cloud_init.cfg bootstrap file in a plugged in the bootstrap location, mode change to controller mode is initiated. After the device boots up in controller mode, the configuration present in the configuration file is applied.
- If a ciscortr.cfg bootstrap file or config-wizard is discovered, mode change is not initiated and the boot up continues in the Autonomous mode.

**Note**

- The bootstrap file (ciscosdwan.cfg) is generated by Cisco SD-WAN Manager, and has UUID, but no OTP.
- For software devices (Cisco Catalyst 8000V Edge Software, Cisco Cloud Services Router 1000V Series, and Cisco ISRv), and for OTP-authenticated devices such as the Cisco ASR1002-X, use the bootstrap file ciscosdwan_cloud_init.cfg. This file has OTP but no UUID validation.

# Switch Modes Using Cisco CLI

Use the **controller-mode** command in privileged EXEC mode to switch between controller and autonomous modes.

### Autonomous Mode

The **controller-mode reset** command takes the device back to day zero configuration.

```
Device# controller-mode reset
```

The **controller-mode disable** command switches the device to autonomous mode.

```
Device# controller-mode disable
```

**Note** **controller-mode disable** should only be used for temporarily operating the device in autonomous mode. Ensure the device is returned to controller mode using the same image.

### Controller Mode

**Note** To switch the device to the controller-mode, boot the system using either the bootflash:/*.bin or bootflash:/packages.conf file.

**Note** If bootflash:core or harddisk:core contain core files (files containing information about process crashes), move the files to another location before changing the device to controller mode. If these files remain in the bootflash:core or harddisk:core directories, Cisco SD-WAN Manager displays an alarm after onboarding the device. You can move the files to any other directory on the device other than a core directory.

The **controller-mode enable** command switches the device to controller mode.

```
Device# controller-mode enable
```

### Notes

| Note | Description |
|---|---|
| Bundle mode | If device is booted with bundle mode (Super packages), after reboot, the image gets automatically expanded and activated to prepare the router for SDWAN operation. Devices with 4GB RAM may require an additional reboot to free up space in /bootflash. The following devices with 4GB RAM need reload:<br>• Cisco ISR 4451<br>• Cisco ISR 4431<br>• Cisco ISR 4461<br>• Cisco ISR 4351<br>• Cisco ISR 4331<br>• Cisco ISR 4321 |
| Viewing the contents of the bootflash:/.sdwaninstaller directory | You cannot view the contents of the bootflash:/.sdwaninstaller directory of a Cisco IOS XE Catalyst SD-WAN device in either of the following conditions:<br>• The device is in controller mode.<br>or<br>• The device is in autonomous mode and using Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later. |

# Change a device to Controller mode

Changing from Autonomous mode to Controller mode requires the device to perform an operation that expands the software package of the current running image. The expand operation requires bootflash space. When you execute the **controller-mode enable** command to change to Controller mode, there is a possibility that the router does not have enough bootflash space to expand the software package of the running image. The first step of the procedure addresses this.

### Procedure

**Step 1** Check the available space on the device bootflash. Ensure that there is space equal to the size of the software image .bin file plus 100 MB.

**Step 2** Use the **controller-mode enable** command on the device to change to Controller mode.

The device verifies that the bootflash has sufficient space to expand the software image file.

If there is sufficient bootflash space, the device reboots in Controller mode and expands the software image.

If the bootflash does not have sufficient space, the command output indicates the space required and the device does not change to Controller mode.

**Note**
The device verifies that the bootflash has sufficient space to expand the software image file, from these releases:

- Cisco IOS XE Catalyst SD-WAN Release 17.12.5a and later maintenance releases of 17.12.x
- Cisco IOS XE Catalyst SD-WAN Release 17.15.2 and later maintenance releases of 17.12.x
- Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and all later releases

In earlier releases, the **controller-mode enable** command does not first verify that the bootflash has sufficient space to expand the software image file. It first changes the device to Controller mode, then expands the file. To verify that the device expanded the image file and to troubleshoot if it did not, see Troubleshoot software image expansion failure due to lack of bootflash space.

# Mode Discovery and Mode Change with Bootstrap Files

**Note** If your Cisco IOS XE Catalyst SD-WAN device is already running an older Cisco Catalyst SD-WAN configuration version or file and when you upgrade your device from Cisco IOS XE Catalyst SD-WAN Release 16.x to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later, the device boots up in the controller mode. To prevent the device from booting up in the controller mode, before performing the device upgrade, ensure that you remove the stale Cisco Catalyst SD-WAN configuration file from the bootflash.

Detailed steps to delete all Cisco Catalyst SD-WAN artifacts from bootflash:

delete /force bootflash:/ciscosdwan*.cfg

delete /force /recursive bootflash:/.sdwaninstallerfs

delete /force /recursive bootflash:/.sdwaninstaller

delete /force /recursive bootflash:/.sdwaninternal

delete /force /recursive bootflash:/sdwan

delete /force /recursive bootflash:/vmanage-admin

delete /force /recursive bootflash:/.cdb_backup

delete /force /recursive bootflash:/.installer/active

delete /force /recursive bootflash:/.installer

On a device that already runs a Cisco Catalyst SD-WAN image, after upgrading to a Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later image, the device boots up in controller mode.

**Note** Installing the Cisco Catalyst 8000V on OpenStack requires using the Cisco Catalyst 8000V image for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a or later.

Use the **controller-mode enable** command to switch from autonomous to controller mode and the **controller-mode disable** command to switch from controller mode to autonomous mode.

To switch modes using CLI, ensure that the appropriate configuration files mentioned in the table below are present. After the device boots up, the configuration present in the configuration file is applied. The device reads the configuration file and uses the configuration information to come up on the network.

***Table 7: Configuration File Prerequisites for Mode Change***

| Current Mode | Mode change to | Platforms | Configuration file and location |
|---|---|---|---|
| Controller | Autonomous | All supported platforms | ciscortr.cfg in any file system available to the device |
| Autonomous | Controller | • Cisco Cloud Services Router, CSR1000v<br>• Cisco Integrated Services Virtual Router, ISRv<br>• Cisco Catalyst 8000V<br>• Cisco ASR1002-X | ciscosdwan_cloud_init.cfg on bootflash, USB, CDROM0, or CDROM1 |
| Autonomous | Controller | • Cisco Aggregation Services Router, ASR 1000 Series<br>• Cisco Integration Service Routers, ISR 4000 series and ISR 1000 series routers | ciscosdwan.cfg on bootflash or USB |

**Note** On a Cisco CSR1000v device (for Cisco IOS XE Release 17.2 or later) and a Cisco Catalyst 8000V (for Cisco IOS XE Release 17.4 or later) image deployment, if you want to boot up the device in controller mode, load the bootstrap file generated by Cisco SD-WAN Manager by bootstrap (ESXi, KVM, and OpenStack) or user-data (AWS) or custom-data (Azure and GCP).

The following fields must be present in the ciscosdwan_cloud_init.cfg bootstrap file:

- otp
- uuid
- vbond
- org

**Note** When the device mode is switched from autonomous to controller, the startup configuration and the information in NVRAM (certificates), are erased. This action is equivalent to running the **write erase** command.

**Note** When the device mode is switched from controller to autonomous, all Yang-based configuration is preserved and can be reused if you switch back to controller mode.

**Note** When the device is in Day N configuration and is reloaded, the presence of a bootstrap file does not impact the device operating mode.

**Note** You cannot view the contents of the bootflash:/.sdwaninstaller directory and .sdwanistallerfs file of a Cisco IOS XE Catalyst SD-WAN device in either of the following conditions:

- The device is in controller mode.

  or

- The device is in autonomous mode and using Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later.

Directory, more, copy and delete operations are not allowed when the file and directory are hidden in controller-mode.

# Reset Controller Mode Configuration

If you use **request platform software sdwan config reset** or **request platform software sdwan software reset** commands to bring the device back to controller-mode day-zero configuration, the device performs one of the following actions:

- Performs mode discovery. For more information on mode discovery, see Mode Discovery with Plug and Play Onboarding, on page 10.
- Uses the appropriate configuration file to perform bootstrap. For more information on the Cisco Catalyst SD-WAN bootstrap configuration file, see Creating a Cisco Catalyst SD-WAN Bootstrap Configuration File, on page 12.

To erase the Cisco Catalyst SD-WAN configuration of the current active image, use the following CLI:

```
Device# request platform software sdwan config reset
%WARNING: Bootstrap file doesn't exist and absence of it can cause loss of connectivity to
 the controller.
For saving bootstrap config, use:
request platform software sdwan bootstrap-config save
Proceed to reset anyway? [confirm]
Backup of running config is saved under /bootflash/sdwan/backup.cfg
WARNING: Reload is required for config-reset to become effective.
```

**Note** The warning listed in the above configuration is visible only on Cisco IOS XE Catalyst SD-WAN Release 17.3.1a and later images.

For the changes to take effect, you must reload the router after running the CLI. Running this CLI ensures the configuration for the currently installed version is wiped along with crypto keys and the device enters the day zero workflow after the reload.

If the device is not set up to use PnP for onboarding, then it reads the configuration file in the bootflash and uses the configuration information to come up on the network. If the device is setup to use PnP onboarding, then after reload, the PnP discovery will start again.

**Note** In the case of public clouds, just like a fresh install, additional bootstrap configuration is provisioned that allows you to login to the instance.

**Note** In public cloud and NFVIS environments, ensure that a latest day-zero bootstrap configuration file (exported from Cisco SD-WAN Manager) is available in a supported location and following standard file naming conventions (example: bootflash:/ciscosdwan_cloud_init.cfg file), before the configuration reset operation is performed.

**Warning** Failure to follow save the bootstrap file in these environments cause loss of virtual machine connectivity.

### Configuration Reset

When you do a configuration reset, the device performs the following:

- Erases only the configuration of the current running image.
- Erases the certificates.
- Reboots the router with the same image. At this point, the device repeats Day-0 boot up.

### Software Reset

When you do a software reset, the device performs the following:

- Erases all SD-WAN metadata saved in the `bootflash:/sdwan` folder including certificates.
- Erases configuration of all the images (running as well as previously activated).
- Removes all image files except the one marked as default.
- Reboots the router with the default version image. At this point, the device repeats Day-0 boot up.

# Mode Switching: Additional Information

## Configuration Persistence During Mode Switch

*Table 8:*

| Current Configuration Mode | Mode Switched to | Behavior |
|---|---|---|
| Autonomous | Controller | Contents of NVRAM and the startup configuration are erased. Configuration is not be restored. Device is reverted to Day zero configuration. Previous running configuration is stored in bootflash.<br>**Note**<br>When you switch from autonomous mode to controller mode, and switch back to autonomous mode, the Cisco IOS XE configuration is not restored because the startup configuration is empty. You have to manually restore configuration from the backup. |
| Controller | Autonomous | CDB contents are erased (for subsequent mode switches) and Cisco IOS configuration are not restored (as startup configuration is empty). You have to manually restore configuration from the backup. |

# Verify Controller and Autonomous Modes

## Show Command Output for Controller Mode

```
Device# show logging | include OPMODE_LOG
*Dec  8 16:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in CONTROLLER mode

Device# show version | inc operating

Router operating mode: Controller-Managed

Device# show platform software device-mode
Operating device-mode: Controller

Device-mode bootup status:
------------------------------------
 Success

Device# show platform software chasfs r0 brief | inc device_managed_mode

/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [controller]
  /tmp/fp/chasfs/etc/device_managed_mode : [controller]

Device# show version | inc Last reload
Last reload reason: Enabling controller-mode
```

# Show Command Output for Autonomous Mode

```
Device# show logging | include OPMODE_LOG
*Dec  8 17:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Device# show version | inc operating

Router operating mode: Autonomous

Device# show platform software device-mode

Operating device-mode: Autonomous

Device-mode bootup status:
------------------------------------

Device# show platform software chasfs r0 brief | inc device_managed_mode

/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [autonomous]
  /tmp/fp/chasfs/etc/device_managed_mode : [autonomous]

Device# show version | inc Last reload
Last reload reason: Enabling autonomous-mode
```

**Note** If the device is in controller mode, the **show sdwan running-config** command does not display the following information:

- All service commands under /native/service except tcp-small-servers, udp-small-servers, tcp-keepalives-in, and tcp-keepalives-out
- Configurations under line VTY except for transport, access-class, and ipv6 access-class
- IPv6 unicast routing configuration
- Commands in /native/enable

To verify these configuration use the **show running-config** command.

# Change the Console Port Access After Installation, in Controller Mode

### Before You Begin

Before beginning this procedure, ensure that you have access to the Cisco CSR1000V or Cisco Catalyst 8000V router through the currently configured console access method.

### Change the Console Port Access

This procedure changes the method for connecting to the console to access a Cisco CSR1000V or Cisco Catalyst 8000V software device.

The image used for deploying the Cisco CSR1000V or Cisco Catalyst 8000V software determines the default type of console access to use, which can be virtual or serial.

The procedure includes changing the mode from controller to autonomous, and then back to controller, which is required for operation with Cisco Catalyst SD-WAN. These mode changes cause the device to reload.

Perform the following steps to change the console port access.

1. In EXEC mode, enter **enable** to enter privileged EXEC mode.

   ```
   Router> enable
   ```

2. Disable controller mode. Enter the following command and follow the prompts to complete the command.

   ```
   Device# controller-mode disable
   ```

**Note** This reboots the device in autonomous mode.

3. After the device restarts, enter **enable** to enter privileged EXEC mode.

   ```
   Router> enable
   ```

4. Enter global configuration mode.

   ```
   Device# configure terminal
   ```

5. Use one of the following options to configure the type of access:

   - virtual: This option specifies that the device is accessed through the hypervisor virtual VGA console.

     ```
     Device(config)# platform console virtual
     ```

   - serial: This option specifies that the device is accessed through the serial port on the virtual machine (VM).

**Note**

- Use this option only if your hypervisor supports serial port console access.
- If the device configuration is stored as a Cisco SD-WAN Manager device template and is attached to the device using Cisco SD-WAN Manager, enter the command

  ```
  Device(config)# platform console serial
  ```

  to the CLI add-on feature template. For more information on CLI Add-On Feature Templates see, Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide. This helps in avoiding Cisco SD-WAN Manager removing the serial port when the device template is attached to the device.

```
Device(config)# platform console serial
```

   - auto: (This option has been deprecated and is not recommended.) This option specifies that the device console is detected automatically. This is the default setting during the initial installation boot process. For additional information, see Booting the Cisco CSR 1000v as the VM.

6. Exit configuration mode.

   ```
   Device(config)# end
   ```

7. Save the configuration.

```
Device# write memory
```

8. Copy the running configuration to the startup configuration.

```
Device# copy system:running-config nvram:startup-config
```

9. Change the device back to controller mode. Enter the following command and follow the prompts to complete the command.

```
Device# controller-mode enable
```

**Note** This step reboots the device in controller mode.

# Upgrade to Cisco IOS XE Release 17.2.1r or Later

## Supported Upgrades

***Table 9: 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<br>Cisco IOS XE SD-WAN 17.2.2 or later<br>Cisco IOS XE SD-WAN 16.12.4a or later<br>**Note**<br>• 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.<br>• 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<br>Cisco IOS XE Release 17.2.1v<br>Cisco IOS XE SD-WAN 16.12.x<br>Cisco IOS XE SD-WAN 16.11.x<br>Cisco IOS XE SD-WAN 16.10.x<br>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<br>Cisco IOS XE SD-WAN 16.11.x<br>Cisco IOS XE SD-WAN 16.10.x<br>Cisco IOS XE SD-WAN 16.9.x |

***Table 10: 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<br>Cisco IOS XE SD-WAN 17.2.1 or later<br>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<br>Cisco IOS XE SD-WAN 16.11.x<br>Cisco IOS XE SD-WAN 16.10.x<br>Cisco IOS XE SD-WAN 16.9.x |

Use the following procedures to upgrade your device to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later images.

**Note** Do not delete the existing image to ensure that you have a rollback option.

**Note** If an upgrade fails, do not attempt to reactivate the new software image. Instead, remove the new software image, identify and correct any configuration settings that might have caused the failure, and try the upgrade procedure again. If the issue persists, contact Cisco for assistance.

**Note** When upgrading to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a from Cisco IOS XE Releases 17.3.1a or earlier, we recommend that you do not make any changes to the device configuration using CLI, while a feature template is detached. Starting Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, we use Cisco Catalyst SD-WAN assisted upgrades. In this upgrade procedure, Cisco Catalyst SD-WAN saves the device configuration before the upgrade. If the configuration on the device, that is modified using CLI is not same as on Cisco Catalyst SD-WAN, then the device has inconsistent configuration after the upgrade.

For example, if you configure the BGP AS number of a device to a different value using CLI, the device can have inconsistent configuration and the upgrade fails. If the upgrade is performed when the device is in CLI mode, then you must revert the BGP AS number to the original value and then upgrade the device. Therefore, we recommend that you upgrade the device using Cisco Catalyst SD-WAN.

**Note** Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, if you are upgrading the firmware for a device on which the primary tunnel interface is a cellular interface and the backup tunnel interface is a gigabit interface, use the gigabit interface as the primary interface for the firmware upgrade.

For information about configuring the priority of a tunnel interface, see the vmanage-connection-preference command in *Cisco Catalyst SD-WAN Command Reference*. An interface that is configured with a higher preference value has a higher priority.

## Upgrade Using Cisco Catalyst SD-WAN

We recommend using Cisco SD-WAN Manager to upgrade. This keeps devices and the controller synchronized.

1. Use the Cisco SD-WAN Manager upgrade and activate procedure described in the *Cisco Catalyst SD-WAN Monitor and Maintain* guide.

## Upgrade Using CLI

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

### Back Up Configuration Files

Use these following steps to make configuration file copies before performing the manual upgrade process. Without these steps, the router will lose its configuration during the upgrade.

**Note** If the deployment is on a public cloud service, such as Amazon Web Services (AWS), failure to save the configuration before upgrading manually can cause an unrecoverable loss of connectivity with the device. In contrast to a hardware device, there may be no way to gain any type of console access to the virtual router.

1. Use the following command to make a backup copy of the Cisco IOS XE Catalyst SD-WAN configuration:

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

2. Use the following command to make a backup copy of the Cisco Catalyst SD-WAN running configuration:

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

### Upgrade Procedure

1. Download the Cisco IOS XE Release 17.2 image for your device from https://software.cisco.com
2. Upload the image to the device.
3. Install the new software. Example:

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

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
   ```

5. Verify that the software is activated.

   ```
   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
   ```

6. (Optional) To ensure that the new version is preserved if software reset required, use the following command. Example:

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

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

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

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

**Note** In controller mode, use the **config-transaction** command to enter global configuration mode. The **configuration terminal** command is not supported in Controller mode.

*Table 11: Configuration Persistence in Upgrade Scenarios*

| Existing Installation (image) | Upgraded to (image) | Behavior |
|---|---|---|
| Cisco IOS XE SD-WAN Release 16.12 and earlier (ucmk9) | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r (universalk9) | Device boots up in controller mode and configuration is preserved. |
| Cisco IOS XE Release 16.12 and earlier (universalk9) | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r (universalk9) | Device boots up in autonomous mode and configuration is preserved (via startup configuration). |

# Downgrade from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or Later Releases

## Downgrade a Cisco IOS XE Catalyst SD-WAN Device to a Previously Installed Software Image

To downgrade a Cisco IOS XE Catalyst SD-WAN device to an earlier software image that is currently installed on the device using the CLI, perform the following steps:

1. Display the currently installed images.

   ```
   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
   ```

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

To download an earlier software image and downgrade a Cisco IOS XE Catalyst SD-WAN device to an earlier software image using the CLI, perform the following steps:

1. Display the currently installed images.

   ```
   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
   ```

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
   ```

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

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

```
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
```

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
```

# Downgrade Scenarios for Cisco IOS XE Release 17.2.x

*Table 12: Configuration Persistence in Downgrade Scenarios*

| Existing Installation (image) | Downgrade to (image) | 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.<br>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. |

**Note**

- Downgrading directly from controller mode to Cisco IOS XE Amsterdam Release 17.1.x or earlier universalk9 or other non Cisco Catalyst SD-WAN images is not supported. To downgrade from controller mode to earlier IOS XE images, switch to autonomous mode and follow the downgrade process.
- Downgrading directly from autonomous mode to Cisco IOS XE SD-WAN 16.12 or earlier ucmk9 SD-WAN images is not supported. To downgrade from autonomous mode to earlier Cisco IOS XE Catalyst SD-WAN images, switch to controller mode and follow the downgrade process.

# Restore Smart Licensing and Smart License Reservation

The smart licensing authorization is lost when a device switches from autonomous to controller mode and back to autonomous mode again.

For more information about Smart Licensing, refer to Smart Licensing Guide for Access and Edge Routers.

## Restore Smart Licensing

1. Reconfigure device to reach Cisco Smart Software Manager (CSSM).
2. Register the device using **license smart register idtoken** *token* **force** command in privileged EXEC mode.
3. Set the required crypto throughput using **platform hardware throughput crypto** *crypto-value*.
4. Save the configuration using **write memory** in privileged EXEC mode.
5. Reload the device and verify that the new crypto throughput value is applied using the **show platform hardware throughput crypto** command.

## Restore Smart License Reservation

1. Enable the reservation mode using the **license smart reservation** command in global configuration mode.
2. Set the required crypto throughput using **platform hardware throughput crypto** *crypto-value*.
3. Save the configuration using **write memory**.
4. Reload the device and verify that the new crypto throughput value is applied using the **show platform hardware throughput crypto** command.

# Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing

To onboard a Cisco Catalyst 8000V platform hosted by a cloud service, using pay as you go (PAYG) licensing, perform these steps.

You can also use Cisco Cloud onRamp for Multi-Cloud to onboard a Cisco Catalyst 8000V platform using PAYG licensing. For information to integrate public cloud infrastructure into the Cisco Catalyst SD-WAN fabric, see Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x.

**Note** This procedure is applicable to Cisco Catalyst 8000V hosted by Amazon Web Services (AWS).

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**, and click **Add PAYG WAN Edges**.

2. In the **Add PAYG WAN Edges** dialog box, enter the number of PAYG devices to onboard into Cisco Catalyst SD-WAN, select the **Validate** check box, and click **Add**.

   The **Task View** page opens, showing the progress as Cisco SD-WAN Manager creates logical devices.

**Note** Validating causes Cisco SD-WAN Manager to publish the list of devices to the Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller controllers in the network.

3. After the **Task View** page shows the logical devices have been created successfully, choose **Configuration** > **Devices** to view the new logical devices on the **Devices** page.

**Note** The **Chassis Number** column shows the unique identifier for each logical device.

4. For the logical devices that you have created, click **…** and choose **Generate Bootstrap Configuration**.
5. (Optional) Attach a device template to the logical devices that you have created.
6. In the **Generate Bootstrap Configuration** dialog box, click **Cloud-Init** and then click **OK**.

   The **Generate Bootstrap Configuration** dialog box shows the content of the bootstrap configuration, which includes the UUID of the logical device, and includes the configuration details provided by the device template if you have attached one.

**Note** The UUID corresponds to the identifier in the **Chassis Number** column in the **Devices** table.

7. There are different methods for loading the bootstrap configuration onto a C8000V instance on a cloud service. The method you use depends on the cloud service. We recommend to click **Download** in the **Generate Bootstrap Configuration** dialog box to save a copy of the bootstrap configuration.
8. In the cloud services portal, create a PAYG instance of the Cisco Catalyst 8000V. When configuring the instance, use the bootstrap configuration that you created in Cisco SD-WAN Manager. The details of how to load the Cisco Catalyst SD-WAN bootstrap configuration onto the instance are specific to the cloud services provider.

**Note** On AWS, the workflow for bringing up an instance includes a user data step that enables loading the bootstrap configuration.

9. On the cloud service platform, start the Cisco Catalyst 8000V instance using the bootstrap configuration from an earlier step.

   When the Cisco Catalyst 8000V instance boots up, it joins the Cisco Catalyst SD-WAN overlay automatically. In Cisco SD-WAN Manager, on the **Devices** page, this Cisco Catalyst 8000V instance shows a green medal icon in the **State** column and **In Sync** in the **Device Status** column.

**Note** On the **Devices** page, for logical devices that have not joined the Cisco Catalyst SD-WAN overlay, the **State** column shows a dotted-circle icon.

# Bootstrap Process for Cisco Catalyst SD-WAN Cloud-Hosted Devices

### Before You Begin

The device template provides the configuration details that enable the device to connect to Cisco SD-WAN Manager.

If you create a logical device and then generate a bootstrap configuration without first attaching a device template, the resulting file will include a minimal configuration. If you attach a device template to the logical device before generating the bootstrap configuration, the resulting file will include a more complete configuration, which can be helpful in enabling the device to connect to the Cisco Catalyst SD-WAN overlay. We recommend that you attach a device template to the logical device before creating the bootstrap configuration.

This procedure is useful when onboarding a software device, such as the Cisco Catalyst 8000V, to a private cloud, such as KVM, ESXi, or OpenStack.

### Bootstrap Process for Cisco SD-WAN Cloud-Hosted Devices

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. For the logical device (includes the UUID) that you are using for a new cloud-hosted instance, click **…** and choose **Generate Bootstrap Configuration**.
3. In the **Generate Bootstrap Configuration** dialog box, choose **Cloud-Init** and click **OK**. The **Generate Bootstrap Configuration** dialog box displays the bootstrap configuration, including the OTP token for the license, Cisco SD-WAN Validator address, UUID, and organization information.

**Note** The UUID corresponds to the identifier in the **Chassis Number** column in the **Devices** table.

**Note** Ensure that the bootstrap configuration does not include more interfaces than the virtual device instance has in the cloud environment.

4. There are different methods for loading the bootstrap configuration onto a device instance on a cloud service. The method you use depends on the cloud service. We recommend that you click **Download** in the **Generate Bootstrap Configuration** dialog box to save a copy of the bootstrap configuration.

   You can use the bootstrap configuration when setting up a device instance in the cloud service. The configuration enables the device instance to connect to Cisco Catalyst SD-WAN.

For information about onboarding a Cisco Catalyst 8000V in a private cloud, see the following:

- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide, Installing in KVM Environments
- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide, Installing in VMware ESXi Environment
- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide, Installing in OpenStack

For example bootstrap configuration files for the Cisco Catalyst 8000V, see **Cisco Catalyst 8000V Cloud Initialization Files**.

# Troubleshooting

## Troubleshooting Software Installation

**Router Loads the Previous Software Version After Booting**

## Router Loads the Previous Software Version After Booting

### Problem

A router starts up using the previously installed software version.

### Conditions

A router using Cisco IOS XE has two or more software versions installed.

### Possible Causes

If the router begins booting up, and power cycles during the bootup, it may reboot using the previously installed software version.

**Note** Cisco IOS XE Catalyst SD-WAN devices have a mechanism that preserves the previously installed software version. As a safeguard against getting stuck during bootup with a corrupted software image, a device can fall back to the previously installed software version. This fallback can also occur if the device experiences a power cycle during bootup. In this case (power cycle during bootup), you can reboot the device to load the latest software.

### Solutions

1. Check the active and inactive system software versions for a device using one of the following procedures:
   - SD-WAN Manager procedure:
     a. From the SD-WAN Manager menu, choose **Monitor** > **Devices**.
     b. Click a device name in the **Hostname** column.

c. In the left pane, click **Real Time**.

d. In the **Device Options** field, enter **Software Versions**.

A table displays the installed software versions and indicates which version is active.

- CLI procedure:

a. Execute the **show sdwan software** command in privileged EXEC mode to view the current active software version and the previous version.

b. Execute the **show version** command on the device, in privileged EXEC mode.

If the device is using the latest installed software version, the command output shows bootflash:packages.conf.

If the device is using the previous software version, the command output shows bootflash:prev_packages.conf.

2. Reboot the device and check the loaded system software again.
3. If the device boots again with the previous software version (bootflash:prev_packages.conf), contact Cisco TAC for assistance.

**Note** The software update, such as Cisco IOS XE Catalyst SD-WAN Release 17.18.2, prevents unintended boot failures by ensuring the `previous_packages.conf` file is aligned with the specified default software version, configured either via CLI (request platform software sdwan software set-default) or SD-WAN Manager UI.

This change addresses a scenario where a power outage during the boot process could cause the device to revert to an older, potentially unsupported release, leading to isolation from the SD-WAN fabric.