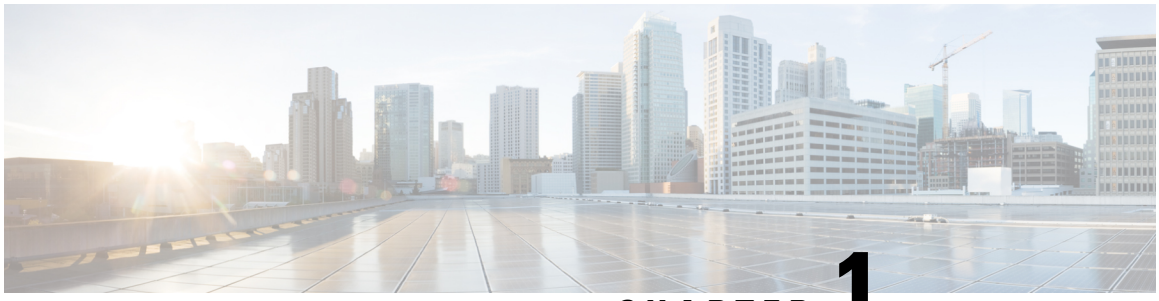
Cisco Catalyst SD-WAN Network Maintenance Guide, Releases 26.x and Later

First Published: 2026-05-25

Last Modified: 2026-06-18

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

Device Software Installation and Upgrade, Cisco IOS XE 17.2.1r and Later

Feature history for device software installation and upgrade

This table describes the history of features that relate to installing and upgrading the software of network devices.

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.
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.
Day 0 WAN Interface Automatic IP Detection using ARP	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 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.

Platform support

Describes the platforms that support the installation and upgrade procedures described here.

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

Describes which software image types to use for platforms operating in Cisco Catalyst SD-WAN.

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

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 2: 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 3: 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

Self-signed trustpoint

Describes the self-signed trustpoint that is generated and loaded to a device when it boots up.

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.

Autonomous and controller modes

Describes the two installation modes that are available on devices. Autonomous mode supports the functionality of Cisco IOS XE in a non-Cisco Catalyst SD-WAN deployment and Controller mode supports the Cisco Catalyst SD-WAN solution.

Table 4: Comparison of modes

Feature	Autonomous Mode	Controller Mode
Configuration method	• Command Line Interface (CLI) • NETCONF	YANG-based configuration • Cisco SD-WAN Manager • NETCONF
Onboarding modes	• Plug and Play • Config-Wizard • WebUI • Bootstrap (USB, bootflash, and so on) • Auto-Install (Python Script, TCL Script) • ZTP (Using DHCP Option 150 and Option 67)	• Plug and Play • 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

Restrictions for installing and upgrading device software

Describes restrictions relevant for installing and upgrading software on devices in a Cisco Catalyst SD-WAN environment.

Dual-IOSd

Dual-IOSd is supported only in autonomous mode.

Requirement of universalk9 images

Software 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.

Changing mode clears configuration

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

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, the WebUI is not supported, and an error message is displayed if used.

Keep existing image

When upgrading, do not delete the existing image. This provides a software rollback option.

If upgrade fails

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.

Upgrading a device to to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

When upgrading to Cisco IOS XE Catalyst SD-WAN Release 17.4.1a from Cisco IOS XE Releases 17.3.1a or earlier, do not make any changes to the device configuration using CLI commands 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 commands, the device can have inconsistent configuration and the upgrade fails. If you perform the upgrade 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, upgrade the device using Cisco Catalyst SD-WAN.

Firmware upgrade: primary and backup tunnel interfaces

From 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, refer to the **vmanage-connection-preference** command in the *Cisco Catalyst SD-WAN Command Reference Guide*. Configuring an interface with a higher preference value gives the interface a higher priority.

Downgrading devices to releases earlier than 17.1.x

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.

Software Installation for Cisco IOS XE Routers

Describes software installation for different platforms, in the context of Cisco Catalyst SD-WAN.

Software image type

Describes the software image type to download.

For devices operating with Cisco Catalyst SD-WAN, the software image to use has a filename in this pattern:

<router-model>-universalk9.<release-number>

Images are available on the Cisco Software Download site.

Installing software on select platforms

Provides links to documents for information about installing software on specific platforms.

Refer to these documents for installation instructions:

- 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 the Cisco Catalyst 8000V Edge Software platform

Provides information about installing software on the Cisco Catalyst 8000V Edge software platform.

From 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.

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.

Software image

Use 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

Controller mode

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.

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.

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.

Install software on the Cisco CSR 1000v platform

Provides links to detailed information about installing software on the Cisco CSR 1000v platform.

Based on the cloud service in which you are deploying the CSR 1000v instance, see this information about performing the bootstrap or the day 0 configurations:

- 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

Plug and Play onboarding

Provides information about onboarding devices through Cisco Plug and Play.

Plug and Play onboarding workflow

Note these considerations regarding Plug and Play:

- 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.
- 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.

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

Procedure

Step 1 Place an order for the device in Cisco Commerce with Smart Account and Virtual Account details of the customer.

Step 2 The device information from Cisco Commerce like Device serial number, Smart Account, and Virtual Account are added to the Plug and Play portal.

Step 3 Add a Cisco SD-WAN Validator controller profile into the Plug and Play (PnP) portal for the same Smart Account and Virtual Accounts.

Step 4 Associate the new device to the Cisco SD-WAN Validator controller profile manually.

Step 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).

Step 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.

Mode discovery with Plug and Play onboarding

Describes how the Plug and Play (PnP)-based discovery process determines the mode and changes it if necessary.

The PnP-based discovery process determines the mode in which the device operates, based on the controller discovery and initiates a mode change if necessary. The mode change causes the device to reboot. After the reboot, the device performs the appropriate discovery process.

When you upgrade to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r or later, on a Cisco device running an earlier verion of Cisco IOS XE or a Cisco Catalyst SD-WAN image, the device starts in Autonomous mode or Controller mode depending on the configured controller.

Deployment using Plug and Play (PnP) may include any of these discovery process scenarios:

Table 5: PnP discovery process scenarios

Bootup 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
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

Describes how a device can automatically learn about the available IP addresses and default gateway information by using Address Resolution Protocol (ARP) packets.

How a device receives IP address and gateway server information during PnP onboarding

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.

Automatic IP address detection applies only to day zero deployments and is enabled by default.

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.

IP address not preserved after reboot

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.

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.

Restrictions for automatic IP address detection

- Automatic IP address detection 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.
- Automatic IP address detection is supported only on devices that are in Controller mode, for configuration by Cisco Catalyst SD-WAN.
- Automatic IP address detection 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.
- Automatic IP address detection 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-Plug and Play onboarding

Describes how to onboard devices to Cisco Catalyst SD-WAN without using Plug and Play (PnP).

New installation: Mode change device day zero scenario

A prerequisite for this process is a bootstrap file.

For software devices such as Cisco Catalyst 8000V Edge Software, 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.

Summary

Describes the process by which a new device determines which mode to use (Autonomous or Controller) and boots up.

Workflow

1. If a 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 device determines if a mode change is required, based on the bootstrap file, and boots up.
   - If the ciscosdwan.cfg or ciscosdwan_cloud_init.cfg bootstrap files are available 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.

     The bootstrap file (ciscosdwan.cfg) is generated by Cisco SD-WAN Manager, and has a UUID, but no OTP.
   - If a ciscortr.cfg bootstrap file or config-wizard is discovered, mode change is not initiated and the boot up continues in Autonomous mode.

Change a device to Autonomous mode

Use the **controller-mode disable** command only to temporarily change the device to Autonomous mode. Return the device to Controller mode using the same image.

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.

Procedure

Step 1 Use the **controller-mode reset** command to take the device back to the day zero configuration.

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

Step 2 Use the **controller-mode disable** command to switch the device to Autonomous mode.

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

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.

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.

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, refer to Troubleshoot software image expansion failure due to lack of bootflash space.

Viewing the sdwaninstaller directory

Describes conditions in which you cannot view the contents of the sdwaninstaller directory.

You cannot view the contents of the bootflash:/.sdwaninstaller directory or .sdwanistallerfs file of a Cisco IOS XE Catalyst SD-WAN device in either of these 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 possible when the file and directory are hidden.

Mode discovery and mode change with a bootstrap file

Describes mode discovery and mode change using a bootstrap file.

Preventing a device from booting in Controller mode

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 Controller mode. To prevent the device from booting up in Controller mode, before performing the device upgrade, ensure that you remove the stale Cisco Catalyst SD-WAN configuration file from the bootflash, and delete all artifacts of Cisco Catalyst SD-WAN from the bootflash.

To delete all the artifacts:

- 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

Configuration file prerequisites for mode change

Table 6: Configuration file prerequisites

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 • Cisco Integrated Services Virtual Router, ISRv • Cisco Catalyst 8000V • Cisco ASR1002-X	ciscosdwan_cloud_init.cfg on bootflash, USB, CDROM0, or CDROM1

Current Mode	Mode change to	Platforms	Configuration file and location
Autonomous	Controller	• Cisco Aggregation Services Router, ASR 1000 Series • Cisco Integration Service Routers, ISR 4000 series and ISR 1000 series routers	ciscosdwan.cfg on bootflash or USB

Upgrading a device already running a Cisco Catalyst SD-WAN image

On a device that is already running 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.

Booting Cisco CSR 1000v and Cisco Catalyst 8000V devices in Controller mode

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

Reset a device to a Controller mode day zero configuration using CLI commands

Erase the Cisco Catalyst SD-WAN configuration of the current active image to a reset a device to a Controller mode day zero configuration.

Before you begin

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 performing the configuration reset operation.

Note Failure to follow save the bootstrap file in these environments causes loss of virtual machine connectivity.

Procedure

Step 1 To erase the Cisco Catalyst SD-WAN configuration of the current active image, use the **request platform software sdwan config reset** CLI command

```
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.
```

Step 2 Reload the router after running the CLI command.

Executing this CLI command ensures the configuration for the currently installed version is wiped, together with crypto keys. The device enters the day zero workflow after the reload.

One of these occurs next:

- If the device is set up to use PnP for onboarding, then PnP discovery begins.
- 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.

Configuration persistence during mode switch

Describes configuration retention and erasure when switching a device between Autonomous and Controller modes.

Table 7: Mode switch behavior

Current configuration mode	Switching to	Behavior
Autonomous	Controller	Erases the contents of NVRAM and the startup configuration. Device reverts to a day zero configuration. The previous running configuration is stored in bootflash. The configuration is not restored. **Note** 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 can manually restore the configuration from a backup.

Current configuration mode	Switching to	Behavior
Controller	Autonomous	Erases the ConfD configuration database (CDB) contents, for subsequent mode switches, and the Cisco IOS XE configuration is not restored, as the startup configuration is empty. You can manually restore the configuration from a backup.

Verifying Controller and Autonomous modes

Describes the **show** commands to use on a device to verify Controller or Autonomous mode.

Verifying 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 a device is in Controller mode, the **show sdwan running-config** command does not display this 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.

Verifying 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
```

Change the console port access after installation, in Controller mode

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.

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.

Procedure

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

```
Router> enable
```

Step 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.

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

```
Router> enable
```

Step 4 Enter global configuration mode.

```
Device# configure terminal
```

Step 5 Use one of these options to configure the type of access:

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

- 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 **platform console serial** command to the CLI add-on profile or CLI add-on template. This helps prevent Cisco SD-WAN Manager from 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.

Step 6 Exit configuration mode.

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

Step 7 Save the configuration.

```
Device# write memory
```

Step 8 Copy the running configuration to the startup configuration.

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

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

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

This step reboots the device in controller mode.

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 23
- Upgrade using CLI commands, on page 23

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
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 24
- Downgrade a Cisco IOS XE Catalyst SD-WAN device to an older software image, on page 25

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
```

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.

Restoring Smart Licensing after switching modes

Describes methods to restore Smart Licensing authorization lost when a device switches from Autonomous to Controller mode.

When a device swtiches from Autonomous mode to Controller mode and back to Autonomous mode again, it loses authorization for Smart Licensing.

Restore Smart License reservation

Procedure

Step 1 Enable the reservation mode using the **license smart reservation** command in global configuration mode.

Step 2 Set the required crypto throughput using **platform hardware throughput crypto** *crypto-value*.

Step 3 Save the configuration using **write memory**.

Step 4 Reload the device and verify that the new crypto throughput value is applied using the **show platform hardware throughput crypto** command.

Restore Smart Licensing

Procedure

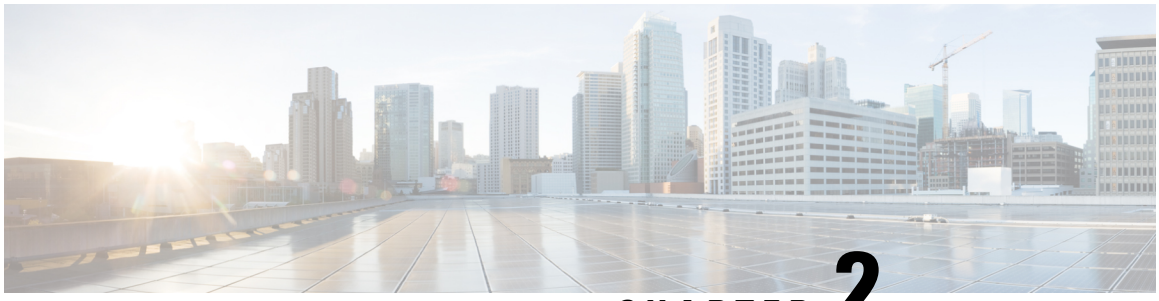
Step 1 Configure the device to reach Cisco Smart Software Manager (CSSM).

Step 2 Register the device using the **license smart register idtoken** *token* **force** command in privileged EXEC mode.

Step 3 Set the required crypto throughput using the **platform hardware throughput crypto** *crypto-value* command.

Step 4 Save the configuration using the **write memory** command in privileged EXEC mode.

Step 5 Reload the device and verify that the new crypto throughput value is applied using the **show platform hardware throughput crypto** command.



CHAPTER 2

Device Operations

Reboot devices

Use the Device Reboot screen to reboot one or more Cisco Catalyst SD-WAN devices.

Reboot devices

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Device Reboot**.
2. Click **WAN Edge**, **Control Components**, or **Manager** depending on the device type that you want to reboot..
3. Check the check boxes next to the device or devices that you want to reboot.
4. Click **Reboot**.

View active devices

To view a list of devices on which the reboot operation was performed:

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 a row to see 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.

Reload a security application

The **Reload Services** option in the **Maintenance** > **Device Reboot** window lets you to recover a security application from an inoperative state. Ensure that you use this service as an initial recovery option. See #unique_44 unique_44_Connect_42_section_r3p_5gc_yhb.

Ensure that a security application has already been installed on the device that you choose to reload services for. To reload one or more security applications:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Device Reboot**.
2. Under **WAN Edge**, check the check box for the Cisco Catalyst SD-WAN device you want to choose.
3. Click **Reload Services**.

   The **Reload Container** dialog box appears.
4. If the security application version is correct, check the check box against the version of the security application.
5. Click **Reload**.

   The security application stops, is uninstalled, reinstalled, and restarted.

Reset a security application

The **Reset Services** option in the **Maintenance** > **Device Reboot** window enables you to recover a security application from an inoperative state.

Use the **Reset Services** option when the virtual network configuration of a security application changes, such as, the virtual port group configuration on a device.

- Ensure that a security application is already been installed on the device that you choose to reset services for.
- Ensure that the chosen security application is in a running state.

To reset one or more security applications:

1. Click **WAN Edge** and check against a Cisco Catalyst SD-WAN device to reload the security application.
2. Click **Reset Services**.

   The **Reset Container** dialog box opens.
3. If the security application version is correct, check the check box against the version of the device.
4. Click **Reset**.

   The security application is stopped, and then restarted.

Determine security applications in inoperative state

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.
3. In the left pane, click **Real Time**.

   The real time device information appears in the right pane.
4. From the **Device Options** drop-down list, choose **App Hosting Details**.

A table appears with the device-specific application hosting information. In the table, if the state of the device is ACTIVATED, DEPLOYED, or STOPPED, perform a reload or reset operation on the security application.

If the state of the device is RUNNING, the security application is in an operative state.

5. From the **Device Options** drop-down list, choose **Security App Dataplane Global**.

   A table appears with the device-specific application data plane information. In the table, if the **SN Health** of the device is yellow or red, perform a reload or reset operation on the security application.

   If the **SN Health** of the device is green, the security application is in an operative state.

Reset interfaces

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation without having to modify the device's configuration.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. For the desired template, click **…** and choose **Reset Interface**.
3. In the **Interface Reset** dialog box, choose the desired interface.
4. Click **Reset**.

Invalidate a device

You can make your device invalid should your device go beyond its target location.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Make Device Invalid**.
3. Confirm that you want to make the device invalid and click **OK**.

Re-validate a device

1. From the Cisco Catalyst SD-WAN menu, choose **Configuration** > **Certificates**.
2. Choose the invalid device and look for the **Validate** column.
3. Click **Valid**.
4. Click **Send to Controllers** to complete the action.

Stop data traffic

You can stop data traffic to your device should your device exceed its target location.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Stop Traffic**.
3. Confirm that you want to stop data traffic to your device and click **OK**.

Perform a factory reset

If your device is outside its target boundary, you may need to perform a factory reset of your device.

Note The **Factory Reset** operational command is supported only for Cisco ISR 1000 series and Catalyst 8K devices.

For more information on geofencing, see the *Cisco IOS XE Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Factory Reset**.
3. Choose one of the following options:
   - **Retain License**: Wipes all the device settings and partitions except for licenses. **Retain License** is a sub option to the factory-reset option.
   - **Full Wipe** factory-reset: Wipes all the device settings and partitions.

Note After a full-wipe operation, the device can only be booted up using a USB or TFTP.

4. Click **Reset**.