Factory Reset

Factory Reset

This chapter describes the Factory Reset feature and how it can be used to protect or restore a router to an earlier, clean state.

Table 1: Feature History

Feature Name	Release Information	Feature Description
Enhancements to Factory Reset	Cisco IOS XE Dublin 17.12.1	You can use the **factory-reset all secure** command to reset the router and securely clear the files that are stored in both bootflash and SSD. This command performs sanitization and clears all the user data from eUSB, SSD, ROMVAR, and ACT2. With this release, the **factory-reset all secure** command is more secure and performs better sanitization.
Secure Factory Reset	Cisco IOS XE Cupertino 17.9.1w	Use the **factory-reset all secure** command to reset the router and securely clear the files that are stored in both bootflash and SSD. This command performs sanitization and clears all the user data from eUSB, SSD, and ROMVAR and ACT2.

Feature Name	Release Information	Feature Description
Fast Factory Reset	Cisco IOS XE Everest 16.6.1	In this release we introduce the **factory-reset all** command. The following steps are performed while executing the **factory-reset all** command: **1.** Backing up of the image. **2.** Deletion of ROMMON variables. **3.** Resetting eUSB flash: • Overwriting each partition with 0's using the dd command. **4.** Resetting SSD: • Skipping the dd command to overwrite, and to save time. • Formatting harddisk partition. **5.** Copying image and debug log to bootflash.

Information About Factory Reset

Factory Reset is a process of clearing the current running and start-up configuration information and other private user information on a device, and resetting the device to an earlier clean state.

To perform a fast factory reset, use the **factory-reset all** command to erase existing configuration, and other user data and reset the router to a clean state. This command reformats the eUSB Flash, SSD, and clears ROMVAR. The duration of the factory reset process depends on the storage size of the router. It varies from 10–30 minutes.

Starting with Cisco IOS XE Cupertino 17.9.1w, you can use the **factory-reset all secure** command to reset the router and securely clear the files that are stored in both bootflash and SSD. This command performs sanitization and clears all the user data from eUSB, SSD, and ROMVAR and ACT2. Secure reset can take around 1.5 hours for SUP160 and around 2 hours for SUP250.

The Cisco CBR-8 has two Supervisor Modules, 8 Line Cards, 8 Line Card PIC slots, and two Supervisor PIC slots. There are two types of Supervisor Modules, with different SSD locations:

- Cisco cBR-8 Converged Cable Access Router Supervisor 160G (SUP-160)—SSD is present on the Supervisor Module's PIC Card.
- Cisco cBR-8 Converged Cable Access Router Supervisor 250G (SUP-250)—SSD is present on the Supervisor Module.

Only Supervisor Modules store sensitive user information. Factory reset can't be performed when booting with subpackages. To perform factory reset, you must boot with a single consolidated image.

There are several storage components in Cisco cBR-8 Supervisor Modules as listed below:

Table 2: Cisco cBR-8 Supervisor Modules Memory Components

Memory Component	Type	Memory Size(GB)	Volatility	Purpose	Data Sanitization
RP memory	DRAM	48GB	Volatile	DRAM for CPU	All data is lost when power is turned off. Sanitization measure is not required.
FP memory	DRAM	10GB	Volatile	DRAM for data engine (data-plane configuration and packet buffer)	All data is lost when power is turned off. Sanitization measure is not required.
ROM	SPI ROM Flash	56MB	Non-volatile	• FPGA images • BootRom images • ROMMON variables	Both fast and secure factory reset commands erase ROMMON variables.
TAM	ACT2	10-15KB	Non-volatile	• SUDI • Keys, including a private configure encryption key. • Secure storage	Both fast and secure factory reset commands erase ACT2 user content.
Bootdisk	eUSB Flash	8GB	Non-volatile	Four types of partitions store: • Bootflash: images • NVRAM and NVRAM backup: IOS CFG • OBFL: OBFL logs • CSL: Licensing-related information	• Fast factory reset reformats bootflash, OBFL, CSL partitions and overwrites NVRAM partitions with zeros. **Note** Reformat does not erase file content in the partition. • Secure factory reset overwrites the whole device twice with random data then overwrites with zeros.

Memory Component	Type	Memory Size(GB)	Volatility	Purpose	Data Sanitization
SSD Drive	SATA SSD	• SUP-160 and its PIC: 100GB or 120GB • SUP-250: 240GB	Non-volatile	One partition mount at /harddisk/ for • Images • Core files • Logs	• Fast factory reset reformats harddisk partitions. • Secure factory reset uses a device built-in secure erase command to erase all user data.
Front panel USB Ports	Type-A USB Flash drives		Non-volatile	Used for file transfer	Not covered by data sanitization. You can unplug them.

Factory Reset Commands

Note Before performing a factory reset:

- Use the **show usb-devices summary** command to view a summary of all the system USB devices (eUSB Flash). See show usb-devices summary.
- Use the **show hdd-devices summary** command to view a summary of all the system HDD/SSD devices. See show hdd-devices summary.

factory-reset all

Starting with Cisco IOS XE Cupertino 17.9.1w, the following steps are performed while executing the **factory-reset all** command. See factory-reset all.

1. Backing up of the image.
2. Deleting ROMMON variables and deleting user info in ACT2.
3. Formatting eUSB Flash device partitions.
4. Formatting SSD device partitions.
5. Copying the image and debugging log to bootflash.

factory-reset all secure

Starting with Cisco IOS XE Cupertino 17.9.1w, the following steps are performed while executing the **factory-reset all secure** command. See factory-reset all secure.

1. Backing up of the image.
2. Deleting ROMMON variables.
3. Sanitizing eUSB Flash

- Overwriting the device with random data multiple times and finally fill the device with zeros.
- Verifying that the device has all 0's.
- Recreating partitions.
- Formatting the partitions.

4. Sanitizing SSD
   - Sending secure erase command to SSD.
   - Verifying that the SSD has all 0's.
   - Recreating partitions.
   - Formatting a harddisk partition
5. Copying the image and debugging log to bootflash

Starting with Cisco IOS XE Cupertino 17.12.1, factory reset is enhanced and is more secure.

Prerequisites for Performing Factory Reset

- Ensure that all the software images, configurations, and personal data are backed up before performing a factory reset.
- Ensure that there is an uninterruptible power supply when the factory reset is in progress.

Restrictions for Performing a Factory Reset

- Any software patches that are installed on the router are not restored after the factory reset operation.
- If the factory reset command is issued through a Virtual Teletype (VTY) session, the session is not restored after the completion of the factory reset process.

When to Perform Factory Reset

- Return Material Authorization (RMA): If a router is returned back to Cisco for RMA, it is important that all sensitive information is removed.
- Router is compromised: If the router data is compromised due to a malicious attack, the router must be reset to factory configuration and then reconfigured once again for further use.
- Repurposing: The router must be moved to a new topology or market from the existing site to a different site.

Factory Reset