Performing Factory Reset

- Prerequisites for Performing Factory Reset, on page 1
- Limitations for Performing Factory Reset, on page 1
- Information About Factory Reset, on page 1
- How to Perform Factory Reset, on page 2
- Feature History and Information for Factory Reset, on page 3

Prerequisites for Performing Factory Reset

- Ensure that all the software images, configurations, and personal data are backed up before performing the Factory Reset operation.
- Ensure that the device is not in the stacking mode as Factory Reset is supported only in the standalone mode. For Modular-chassis in high availability mode, Factory Reset is applied per supervisor.
- Ensure that there is uninterrupted power supply when the process is in progress.
- Ensure that you take a backup of the current image before you begin the Factory Reset process.
- Ensure that neither In-Service Software Upgrade (ISSU) nor In-Service Software Downgrade (ISSD) is in progress before starting the Factory Reset process.

Limitations for Performing Factory Reset

- Software patches, if any, that are installed on the switch will not be restored after the Factory Reset operation.
- If the Factory Reset command is issued through a vty session, the session is not restored after completion of the Factory Reset process.

Information About Factory Reset

Factory Reset removes all the customer specific data that has been added to the device since the time of its shipping. Data erased includes configurations, log files, boot variables, core files, and credentials like FIPS-related keys.

The following table provides details about the data that is erased and retained during the Factory Reset process:

Table 1: Data Erased and Retained During Factory Reset

Data Erased	Data Retained
All Cisco IOS images, including the current boot image	Data from Remote field-replaceable units (FRUs)
Crash information and logs	Value of the configuration register
User data, and startup and running configuration	Contents of USB
Credentials like FIPS-related keys	Credentials like Secure Unique Device Identifier (SUDI) certificates, Public key infrastrutcure (PKI) keys
Onboard Failure Logging (OBFL) logs	
ROMMON variables added by the user	

The Factory Reset process can be used in the following two scenarios:

- Return Material Authorization (RMA) for a device—If you have to return a device to Cisco for RMA, remove all the customer-specific data before obtaining an RMA certificate for the device.
- Recovering the compromised device— If the key material or credentials stored on a device is compromised, reset the device to factory configuration, and then reconfigure the device.

The device reloads to perform the Factory Reset task. Note that this reload results in a ROMMON mode.

After the Factory Reset operation is complete, you can load the Cisco IOS image either through a USB or TFTP.

How to Perform Factory Reset

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**factory-reset** {**all** | **config** | **boot-vars**} **Example:** `Device# factory-reset all`	Use the command with all options enabled. No system configuration is required to use the **factory reset** command. Erases all the content from the NVRAM, all the Cisco IOS images, including the current boot image, boot variables, startup and running configuration data, and user data.

	Command or Action	Purpose
		Use the option **config** to reset the start-up configurations. Use the option **boot-vars** to reset the user added boot variables. After the Factory Reset process is successfully completed, the device reboots and stops at ROMMON mode.

Feature History and Information for Factory Reset

Release	Feature Information
Cisco IOS XE Fuji 16.9.2	This feature was introduced.