Performing Factory Reset

- Prerequisites for Performing a Factory Reset, on page 1
- Restrictions for Performing a Factory Reset, on page 1
- Information About Factory Reset, on page 1
- How to Perform a Factory Reset, on page 2
- Configuration Example for Performing a Factory Reset, on page 3
- Additional References for Factory Reset, on page 4
- Feature History for Performing a Factory Reset, on page 4

Prerequisites for Performing a Factory Reset

- Ensure that all the software images, including the current image, configurations, and personal data are backed up before you begin the factory reset process.
- Ensure that there is uninterrupted power supply when the factory reset process is in progress.
- Ensure that In-Service Software Upgrade (ISSU) or In-Service Software Downgrade (ISSD) are not in progress before you begin the factory reset process.

Restrictions for Performing a Factory Reset

- Software patches, if installed on the device, will not be restored after the factory reset process.
- If the **factory-reset** command is issued through a VTY session, the session is not restored after completion of the factory reset process.
- Factory reset is supported only in standalone mode and not in stacking mode. For modular chassis devices configured in high-availability (HA) mode, factory reset is applied for each supervisor module.

Information About Factory Reset

Factory reset erases all the customer-specific data stored in a device and restores the device to its original configuration at the time of shipping. Data erased includes configurations, log files, boot variables, core files, and credentials like Federal Information Processing Standard-related (FIPS-related) keys.

After a factory reset is completed, the device returns to its default license configuration.

The factory reset process is 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 a compromised device: If the key material or credentials that are stored on a device is compromised, reset the device to factory configuration, and then reconfigure the device.

During the factory reset, the device reloads and enters ROMmon mode. After a factory reset, the device removes all its environment variables, including the **MAC_ADDRESS** and the **SERIAL_NUMBER** variables, which are required to locate and load the software. Perform a reset in ROMmon mode to automatically set the environment variables.

After the system reset in ROMmon mode is complete, add the Cisco IOS image either through a USB or TFTP.

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, startup and running configuration, and contents of removable storage devices such as Serial Advanced Technology Attachment (SATA), Solid State Drive (SSD), or USB	—
Credentials such as FIPS-related keys	Credentials such as Secure Unique Device Identifier (SUDI) certificates, public key infrastructure (PKI) keys.
Onboard Failure Logging (OBFL) logs	
ROMmon variables added by the user.	—
Licenses	—

How to Perform a Factory Reset

To perform a factory reset, complete this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password, if prompted.
Step 2	**factory-reset** {**all** | **config** | **boot-vars**} **Example:** `Device# factory-reset all`	Resets the device to its configuration at the time of its shipping. No system configuration is required to use the **factory reset** command. The following options are available: • **all**: 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. Cisco recommends using the option **all**. • **config**: Resets the startup configurations. • **boot-vars**: Resets the user-added boot variables. After the factory reset process is successfully completed, the device reboots and enters ROMmon mode.

Configuration Example for Performing a Factory Reset

The following example shows how to perform a factory reset:

```
Device> enable
Device# factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
```

Additional References for Factory Reset

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	Command Reference

Feature History for Performing a Factory Reset

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	Factory Reset	Factory reset erases all the customer-specific data stored in a device and restores the device to its original configuration at the time of shipping
Cisco IOS XE Gibraltar 16.12.1	Factory Reset for Removable Storage Devices	Performing a factory reset erases the contents of removable storage devices, such as SATA, SSD, or USB.
Cisco IOS XE Amsterdam 17.2.1	Factory Reset with 3-pass Overwrite	A factory reset can be performed to erase all the content from the device securely with 3-pass overwrite. The **secure 3-pass** keyword was introduced.
	Enhanced Factory Reset Option for Stack and Cisco StackWise Virtual	Support for factory reset on stacked devices and for Cisco StackWise Virtual enabled devices is introduced.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.