Performing Factory Reset

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.

- 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, and core files.

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
Onboard Failure Logging(OBFL) logs	Credentials (Secure Unique Device Identifier [SUDI] certificates, public key infrastructure (PKI) keys, and FIPS-related keys)
ROMMON variables added by the user	Licenses

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 ISO image either through a a USB or TFTP.

The Factory Reset process can be used in the following 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.

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**[**secure**] | **config** | **boot-vars**}
	Example:
	`Device# factory-reset all`
	OR
	`Device# factory-reset all secure`
		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

	Command or Action	Purpose
		variables, startup and running configuration data, and user data. We recommend that you use this option. - **all secure**: Performs data sanitization and securely resets the device. **Note** • The keyword **secure** is only supported from the Cisco IOS XE Gibraltar 16.12.9 release. • You can use the **all secure** option only on standalone devices. • This option implements guidelines for media sanitization as described in NIST SP 800-88 Rev. 1. • The **factory-reset all secure** command initiates data sanitization. The booted image of the device is retained. • When data sanitization is completed, the device reloads, and the device image is retained in flash if it was booted with an image from the flash. - **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 on a standalone switch:

```
Device> enable
Device# factory-reset all secure

The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]
The following will be deleted as a part of factory reset: NIST SP-800-88r1
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, excluding the current boot image
4: OBFL logs
5: User added rommon variables
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/Flash from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
Chassis 1 reloading, reason - Factory Reset

Successfully removed non factory default boot variables in rommon
Protection key not found
Switch#reload fp action requested
                                 rp processes exit with reload switch code


Enabling factory reset for this reload cycle
Switch booted with flash:cat3k_caa-universalk9.S2C.SSA.bin
 Switch booted via cat3k_caa-universalk9.S2C.SSA.bin
FACTORY-RESET-RESTORE-IMAGE Taking backup of flash:cat3k_caa-universalk9.S2C.SSA.bin
FACTORY-RESET-RESTORE-IMAGE Searching for cat3k_caa-universalk9.S2C.SSA.bin on flash
factory-reset-restore-image copying /flash/cat3k_caa-universalk9.S2C.SSA.bin image to
/tmp/factory_reset

% FACTORYRESET - Backup lic0 Files
% FACTORYRESETSECURE - Started Cleaning Up...
% FACTORYRESETSECURE - Unmounting sd1
% FACTORYRESETSECURE - Unmounting sd3
% FACTORYRESETSECURE - Unmounting sd5
% FACTORYRESETSECURE - Unmounting sd6
% FACTORYRESETSECURE - Unmounting sd7
% FACTORYRESETSECURE - Starting ds_script
Executing Data Sanitization...
MTD Data Sanitization started ...
!!! Please, wait - Reading MTD Info !!!
!!! Please, wait - Validating Erase for/dev/mtd2 !!!
!!! Please, wait - Validating Erase for/dev/mtd4 !!!
!!! Please, wait - Validating Erase for/dev/mtd6 !!!
MTD Data Sanitization completed ...
CompactFlash Data Sanitization started ...
!!! Please, wait - Reading Flash !!!
!!! Please, wait - Reading CompactFlash !!!
!!! Please, wait - Reading Flash !!!
!!! Please, wait - Shredding !!!
!!! Please, wait - Validating Erase for/dev/sda1 !!!
!!! Please, wait - Reading Flash !!!
!!! Please, wait - Shredding !!!
!!! Please, wait - Validating Erase for/dev/sda3 !!!
!!! Please, wait - Reading Flash !!!
!!! Please, wait - Shredding !!!
!!! Please, wait - Validating Erase for/dev/sda5 !!!
!!! Please, wait - Reading Flash !!!
!!! Please, wait - Shredding !!!
!!! Please, wait - Validating Erase for/dev/sda6 !!!
!!! Please, wait - Reading Flash !!!
!!! Please, wait - Shredding !!!
!!! Please, wait - Validating Erase for/dev/sda7 !!!
CompactFlash Data Sanitization completed ...
Data Sanitization Success! Exiting...
% FACTORYRESET - Data Sanitization Success...
% FACTORYRESETSECURE - Finished ds_script
% FACTORYRESETSECURE - Making File System sd1
% FACTORYRESETSECURE - Mounting Back sd1
% FACTORYRESETSECURE - Handling Mounted sd1
% FACTORYRESETSECURE - Factory Reset Done for sd1
% FACTORYRESETSECURE - Making File System sd3
% FACTORYRESETSECURE - Mounting Back sd3
% FACTORYRESETSECURE - Handling Mounted sd3
% FACTORYRESETSECURE - Factory Reset Done for sd3
% FACTORYRESETSECURE - Making File System sd5
% FACTORYRESETSECURE - Mounting Back sd5
% FACTORYRESETSECURE - Handling Mounted sd5
% FACTORYRESETSECURE - Factory Reset Done for sd5
% FACTORYRESETSECURE - Making File System sd6
% FACTORYRESETSECURE - Mounting Back sd6
% FACTORYRESETSECURE - Handling Mounted sd6
% FACTORYRESETSECURE - Factory Reset Done for sd6
% FACTORYRESETSECURE - Making File System sd7
% FACTORYRESETSECURE - Mounting Back sd7
% FACTORYRESETSECURE - Handling Mounted sd7
% FACTORYRESETSECURE - Factory Reset Done for sd7
% act2 logging success
% FACTORYRESET - Restore lic0 Files
% FACTORYRESET - Setting VERSION_ID
Factory reset Secure Completed ...
ReloadReason=Factory Reset
FACTORY-RESET-RESTORE-IMAGE Copying back image from /tmp/factory_reset onto /bootflash/
FACTORY-RESET-RESTORE-IMAGE Copying image is successful.
% FACTORYRESET - Clean Up Successful...
watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system



Booting...(use SKIP_POST)Warning: primary VB has been corrupted!!, checking backup VB...
  Backup VB is also corrupted!!
Up 1000 Mbps Full duplex (port  0) (SGMII)
The "IP_ADDR" environment variable is not set.
file name too long

The system is unable to boot automatically. The
BOOT environment variable needs to be set to a
bootable image.
```

The following sample output from the **show platform software factory-reset secure log** command displays the data sanitization report:

```
Device#show plat software factory-reset secure log
Factory reset log:
#CISCO WS-C3850CF DATA SANITIZATION REPORT#
START : 16-03-2023, 20:44:46
```

```
  END : 16-03-2023, 20:58:12
-MTD-
PNM : nor
Status : SUCCESS
NIST : PURGE
-CompactFlash-
MNM : SGEFD2GHBATED211
SN : STP20391SGA
Status : SUCCESS
NIST : CLEAR
```

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 Everest 16.6.1	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 16.12.9	Enable Secure Data Wipe capabilities	A factory reset can be performed by using the **all secure** option in the **factory-reset** command. This option performs data sanitisation and securely resets the device. This option implements guidelines for media sanitization as described in NIST SP 800-88 Rev. 1.

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.