Factory Reset

Factory Reset

A factory reset deletes all customer-specific data stored on a device and restores the device to its original configuration as it was at the time of shipping. This process erases configurations, log files, boot variables, core files, and credentials, including Federal Information Processing Standard (FIPS)-related keys. The data erasure performed during a factory reset aligns with the *clear* method defined in NIST Special Publication 800-88 Revision 1.

When do you need to do factory reset

You need to perform factory reset in the following scenarios

- Return Material Authorization (RMA) for a device

  If you need 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 are compromised, reset the device to the factory configuration, and then reconfigure the device.

What happens during a factory reset

1. During a factory reset, the device reloads and enters ROMMON mode.

   After the 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.

2. Perform a reset in ROMmon mode to automatically set the environment variables.

The BAUD rate environment variable returns to its default value after a factory reset. Make sure that the BAUD rate and the console speed are the same at all times. Otherwise, the console becomes unresponsive.

3. After the system reset in ROMmon mode is complete, add the Cisco IOS XE either through an 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 a factory reset

Data erased	Data retained
All Cisco IOS XE 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, and public key infrastructure (PKI) keys.
Onboard Failure Logging (OBFL) logs	—
ROMmon variables added by a user.	—
Licenses	—

Secure Data Wipe

The device storage is utilized to maintain software images, device configurations, software logs, and operational history. Customer-specific data may be present in any of these areas, and this information can include details about the network architecture and design implemented by customers.

How to do secure data wipe

To perform secure data wipe, use the **all secure** option in the **factory-reset** command. This performs data sanitization and securely resets the device. After data sanitization, the device reloads and boots with the software image present in flash.

Secure data wipe standards

Secure data wipe feature implements guidelines for media sanitization as described in NIST SP 800-88 Rev. 1. NIST 800-88 is a standard published by the National Institute of Standards and Technology (NIST) that provides guidelines for media sanitization.

The PURGE standard within NIST 800-88 specifies methods to render data on storage media unrecoverable using laboratory techniques. When a device is sanitized using NIST 800-88 PURGE method, data cannot be recovered through simple non-invasive data recovery techniques or advanced laboratory techniques.

Guidelines to perform 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) are not in progress before you begin the factory reset process.
- 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.
- The **config** keyword of the **factory-reset** command is not supported when the switch is in stacking or Stackwise Virtual Link (SVL) mode.
- For modular chassis devices configured in high-availability mode, factory reset must be applied on each supervisor module.

Perform a Factory Reset

Perform this procedure for a factory reset.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 Configure one of these commands based on the switch configuration:

- Switch

  factory-reset {**all** [**secure**] [**3-pass**] | **config** | **boot-vars**}
- Switch stack

  factory-reset {**all** [**secure 3-pass**] | **config** | **boot-vars** | **switch** {*switch-number* | **all** {**all** [**secure 3-pass**] | **config** | **boot-vars**}}

Example:

```
Device(config)# factory-reset all
OR
Device(config)# factory-reset all secure
```

Resets the device to its configuration at the time of its shipping.

Note
No system configuration is required to use the **factory reset** command.

- **all**: Erases all the content from the NVRAM, all the Cisco IOS XE images, including the current boot image, boot 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
  - 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.

- **secure 3-pass**: Erases all the content from the device with 3-pass overwrite.
  - Pass 1: Overwrites all addressable locations with binary zeroes.
  - Pass 2: Overwrites all addressable locations with binary ones.
  - Pass 3: Overwrites all addressable locations with a random bit pattern.

    Note
    This option takes approximately thrice the time taken to perform any other option.

  - **config**: Resets the startup configurations.
  - **boot-vars**: Resets the user-added boot variables.
  - **switch** {*switch-number* | **all**}:
    - *switch-number*: Specifies the switch number.
    - **all**: Selects all the switches in the stack.

After the factory reset process is successfully completed, the device reboots and enters ROMmon mode.