Configuring Secure Erase

Information about Secure Erase

Beginning with Cisco Nexus 3550-T Release 10.2(3t), the Secure Erase feature is introduced to erase all customer information for Nexus 3550-T switches. Secure Erase is an operation to remove all the identifiable customer information on Cisco NX-OS devices in conditions of product removal due to Return Merchandise Authorization (RMA), or upgrade or replacement, or system end-of-life.

Cisco Nexus 3550-T switches consume storage to conserve system software images, switch configuration, software logs, and operational history. These areas can have customer-specific information such as details regarding network architecture, and design as well as a potential target for data thefts.

The Secure Erase process is used in the following two scenarios:

- Return Material Authorization (RMA) for a device - If you must 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 that are stored on a device is compromised, reset the device to factory configuration, and then reconfigure the device.

Note Secure Erase feature will not erase content in External storage.

The device reloads to perform a factory reset which results in the ToR chassis modules to enter the power down mode. After a factory reset, the device clears all configuration, logs, and storage information.

Prerequisites for Performing Secure Erase

- Ensure that all the software images, configurations, and personal data are backed up before performing the secure erase operation.

- Ensure that there is an uninterrupted power supply when the process is in progress.

Guidelines and Limitations for Secure Erase

- Software patches, if installed on the device, will not be restored after the Secure Erase operation.
- If the **factory-reset** command is issued through a session, the session is not restored after the completion of the factory reset process.

  The top of rack switches and supervisor modules returns to the loader prompt.

Configuring Secure Erase

To delete all necessary data before shipping to RMA, configure secure erase using the below command:

Command	Purpose
factory-reset module *mod* Example: `switch(config)# factory-reset [module <1>]`	Use the command with **all** options enabled. No system configuration is required to use the **factory reset** command. Use the option **mod** to reset the start-up configurations: • For top of rack switches, the command is **factory-reset** or **factory-reset module 1**. After the factory reset process is successfully completed, the switch reboots.

The factory-reset log is displayed below:

```
switch# factory-reset
!!!! WARNING !!!!
The factory reset operation will erase ALL persistent storage on the specified module.
This includes configuration, all log data, and the full contents of flash and SSDs.
Special steps are taken in an effort to render data non-recoverable. Please, proceed with
caution and understanding that this operation cannot be undone and will leave the system
in
a fresh-from-factory state.
!!!! WARNING !!!!
Continue? (y/n) [n] y
A module reload is required for the reset operation to proceed.
Please, wait...

Factory reset requested! Please, do not power off module!

Python 3.7.10
Python Version 3 ...

>>>> Wiping all storage devices ...
+++ Starting NVMe secure erase for /dev/nvme0n1p +++
Using secure format for /dev/nvme0n1p...)
\
---> SUCCESS
```

```
+++ Starting cmos secure erase +++
\
 ---> SUCCESS
+++ Starting nvram secure erase +++
\
 ---> SUCCESS
>>>> Done
>>>> Initializing system to factory defaults ...
+++ Starting init-system +++
\
 ---> SUCCESS
All operations complete! Exiting..
```

Configuring Secure Erase