Configuring Secure Erase

Information about Secure Erase

Beginning with Cisco NX-OS Release 8.2(8), the Secure Erase feature is introduced to erase all customer information for Nexus 7000 series 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 7000 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.

The device reloads to perform a factory reset which results in the switch entering the power-down mode. After a factory reset, the device clears all its environment variables including the MAC_ADDRESS and the SERIAL_NUMBER which are required to locate and load the software.

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 the device is not in stacking mode as factory reset is supported only in the standalone mode.
- Ensure that there is an uninterrupted power supply when the process is in progress.

- Ensure that you take a backup before you begin the secure erase process.
- Ensure that neither In-Service Software Upgrade (ISSU) nor In-Service Software Downgrade (ISSD) is in progress before starting the secure erase process.

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 standby supervisor will be powered down after erasing it.
- If you configure secure erase of fex, the factory reset is initiated and fex configuration will be removed.
- After a successful factory reset, the switch will be powered down.
- You can erase information in order of modules, stand by supervisor, and active supervisor.
- The active supervisor and FEX modules will not be powered down. Only standby supervisor and line card modules will be powered down.

Configuring Secure Erase

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

Procedure

	Command or Action	Purpose
Step 1	**factory-reset** [**fex** | **module** *mod*] **Example:** `Switch (config)# factory-reset [module <3>]`	Use the command with all options enabled. No system configuration is required to use the factory reset command. To initiate secure erase on fex, use **factory-reset fex**. To initiate secure erase on module, use **factory-reset mod**. After the factory reset process is successfully completed, the switch reboots and is powered down.

The erase procedure will be in the order of line card, standby supervisor, the active supervisor. It informs the target module of the erase request through the platform removes the module from the service and then reboots the card, which in turn triggers secure erase on the subsequent boot. Multiple modules can be done in parallel with each card responsible for notifying the active sup of success/failure upon completion.

In the absence of an NX-OS image supporting these commands, a stand-alone image supporting erase will be provided. The user can then boot that secure erase image to trigger the data wipe.

Example

The following is an example output for configuring secure erase factory reset command for fex as follows:

```
switch# factory-reset fex {all | fex-id}
switch# factory-reset [fex <101>]

!!!! 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) y

A module reload is required for the reset operation to proceed.
Please, wait...
reloading fex 101 ...
Waiting for fex: 101 to complete factory-reset !!
.....................................................................................................................
All detected storage devices on fex 101 have been wiped and reinitialized!
```

Feature History for Secure Erase

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 1: Feature History for Secure Erase

Feature Name	Releases	Feature Information
Secure Erase	8.4(6)	Added support for 8.4(x) release.
Secure Erase	8.2(8)	This feature was introduced.