Configuring Secure Erase

Beginning with Cisco NX-OS Release 7.3(11)N1(1), the Secure Erase feature is introduced to erase all customer information for 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.

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.

Note To remove all to erase the customer data on FEX, ensure that the FEX factory reset action is performed before performing factory-reset on switch. For more information, refer to Configure Secure Erase section.

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.
- The secure erase operation can take from 15 minutes to 2 hours.

Configuring Secure Erase

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

Note If fex is attached to the switch, to erase the customer data on the connected fex perform below operation before performing a factory reset on the switch:

- To erase customer data on a single fex - **factory reset fex <fex-id>**
- To erase customer data on all fex - **factory reset fex all**

Procedure

	Command or Action	Purpose
Step 1	**factory-reset** [**fex** [*all*]|[*fex id*]] **Example:** `switch# factory-reset`	Use the command with all options enabled. No system configuration is required to use the factory reset command. To initiate secure erase on switch only, use **factory-reset fex**. To initiate secure erase on fex only, use **factory-reset [fex {all|fex-id}]**.

Example

The following is an example output for secure erase on fex 102:

```
switch# factory-reset fex {all | fex-id}
switch# factory-reset fex 102
!!!! WARNING: This command will perform factory-reset of FEX module 102 !!!!
The factory reset operation will erase ALL persistent storage on the specified FEX 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

Initiating factory-reset for the FEX: 102 --- SUCCESS!!
------------------------------------------------------------------------------
FEX: 102 is reloading for the reset operation to proceed.
Factory reset may take time...
Please, wait and do not power off the FEX...

Trying to remove the FEX:102 config !!!
2022 Feb 10 10:57:26 UUT4 %$ VDC-1 %$ %NOHMS-2-NOHMS_ENV_FEX_OFFLINE: FEX-102 Off-line
(Serial Number SSI182005PM)
2022 Feb 10 10:57:26 UUT4 %$ VDC-1 %$ %PFMA-2-FEX_STATUS: Fex 102 is offline
Successfully removed FEX:102 config. !!!
```

Configuring Secure Erase