

Secure Data Wipe

- Enabling Secure Data Wipe, on page 1

Enabling Secure Data Wipe

Secure data wipe is a Cisco wide initiative to ensure storage devices on all IOS XE based platforms are properly purged using NIST SP 800-88r1 compliant secure erase commands.

This feature is supported in Cisco IOS XE 17.10.1 and later on the following IoT switches for all license levels:

- IE3200
- IE3300
- IE3400
- IE3400H
- ESS3300

When secure data wipe is enabled, everything in internal flash memory is erased, including:

- User configuration and passwords
- Cisco IOS XE image
- Embedded MultiMediaCard (eMMC)
- rommon variables
- ACT2 Secure Storage

Note Secure erase does not clear the SD card or USB device contents. You must manually erase or reformat external storage devices.

The switch will be in rommon prompt with default factory settings (baud rate 9600) after the command is executed. The internal flash memory will not get formatted until the IOS image is rebooted.

Note If an sdflash/usbflash with a valid image inserted, the device will boot with the image in the external media based on the boot precedence. The device will be in rommon only if no external media with an image is inserted in the device.

Performing a Secure Data Wipe

To enable secure data wipe, enter the **factory-reset all secure** command in priviledged exec mode, as shown in the following example:

```
Switch#factory-reset ?
  all                 All factory reset operations
  keep-licensing-info  Keep license usage info
Switch#factory-reset all ?
secure  Securely reset all
Switch#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]Y
```

factory-reset command options:

- **factory-reset all**—Remove everything from flash
- **factory-reset keep-licensing-info**—Keep the licensing information after factory reset and remove everything else from flash.
- **factory-reset all secure** —Remove everything from flash, and also unmount and sanitize the partitions before mounting back. This ensures that the data from those partitions cannot be recovered.

Important The **factory-reset all secure** operation may take hours. Please do not power cycle.

To check the log after the switch executes the command, boot up IOS XE and enter the following **show** command:

```
Switch#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IE3200
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```