



Data Sanitization

This module provides information on how to sanitize data from devices.

- [Data Sanitization, on page 1](#)

Data Sanitization

Use the National Institute of Standards and Technology (NIST) purge method that renders the data unrecoverable through simple, non-invasive data recovery techniques or through state-of-the-art laboratory techniques.



Note Unless otherwise stated, the data sanitization instructions provide NIST 800-88 clear sanitization techniques in user-addressable storage locations for protection against simple non-invasive data recovery techniques and do not provide techniques that render data recovery infeasible using state of the art laboratory techniques.

Follow these steps to remove the files from a flash drive:

Procedure

Step 1 **factory-reset all secure**

Example:

```
Device> factory-reset all secure
```

Purges the data on the flash.

Step 2 Copy the image to the flash using TFTP.

For more information, see [Copying Image Files using TFTP](#).

Step 3 **reload**

Example:

```
Device> reload
```

Reloads the device.

Note If you have copied the image to the flash drive (Step 2), the switch reboots automatically.

Step 4 **show platform software factory-reset secure log**

Example:

```
Device> show platform software factory-reset secure log
```

Displays the data sanitization report.

Example: Data Sanitization

The following example shows how to reset all data from a device:

```
Device# factory-reset all secure
```

```
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
```

```
The following will be deleted as a part of factory reset: NIST-SP-800-88-R1
```

- 1: Crash info and logs
- 2: User data, startup and running configuration
- 3: All IOS images, including the current boot image
- 4: User added rommon variables
- 5: OBFL logs
- 6: License usage log files

Note:

1. You are advised to COPY an IOS image via TFTP after factory-reset and before reloading the box (OPTIONAL)
2. Then, Reload the box for factory-reset to complete

```
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
```

```
Are you sure you want to continue?
```

```
[confirm]
```

```
% factory-reset: started.
% Format of nvram start..
% Format of nvram end...
```

```
*Sep 20 11:36:14.980: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

```
% Erase of obfl0 start...
```

```
.....
```

```
% Erase of obfl0 end...
```

```
% Validating obfl0 partition...
```

```
00000000: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
.....
```

```
003FFFF0: **
```

```
.
```

```

% Format of obfl0 start
% Format of obfl0 complete
% Erase of rsvd start...

.....

% Erase of rsvd end...
% Validating rsvd partition...

00000000: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....

000DFFF0: **

.

% Erase of flash start...

.....

% Erase of flash end...
% Validating flash partition...

00000000: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
.....

0E9FFFF0: **

.

% Format of flash start
% Format of flash complete
% Format of vb: start...
% Format of vb: end...
% act2 erase started...

----- USER 1 -----

ObjectID  ObjectType  ObjectSize
=====

0xBA7E1F05  0x01      0x00DC

% act2 erase completed...

#CISCO C1000-48T-4G-L DATA SANITIZATION REPORT#

START : 2022-09-20 11:36:11
END   : 2022-09-20 11:37:28
PNM   : NAND
MNM   : IS34/35ML02G084
MID   : 0x00
DID   : 0xDAC8
NIST  : PURGE SUCCESS

% factory-reset: logging success...
% FACTORY-RESET - Secure Successfull...

```

1. You are advised to COPY an IOS image via TFTP before reloading the box (OPTIONAL)
2. Then, Reload the box for factory-reset to complete

The following is sample output from the show platform software factory-reset secure log command after a secure factory reset of the device:

```
Device# show platform software factory-reset secure log

#CISCO C1000-48T-4G-L DATA SANITIZATION REPORT#
START : 2022-07-13 10:50:29
END   : 2022-07-13 10:51:45
PNM   : NAND
MNM   : IS34/35ML02G084
MID   : 0x00
DID   : 0xDAC8
NIST  : PURGE SUCCESS
```