

Device Zeroization and Recovery

This chapter contains the following sections:

- Device Zeroization, on page 1
- Important Notice about Zeroization, on page 2
- Command Line Interface, on page 3
- Zeroization Trigger, on page 3
- Recovery Procedures, on page 4

Device Zeroization

On the ESS-3300, the Push Button is used exclusively for triggering the Zeroization process which zeroize and erase switch configuration files or entire flash file system depending on the option provided under the CLI **service declassify**.

The Zeroization process starts as soon as the Push Button is pressed. The CLI command, **service declassify**, is used to set the desired action in response to the Push Button press. To prevent accidental erasure of the system configuration/image, the default setting is set to **no service declassify**.

eMMC is a managed NAND. This means that our embedded switch or router system does not interact with the flash memory directly. The flash controller presents a block-style interface to our system, and it handles the flash management (analogous to the Flash Translation Layer). Our embedded switch or router system cannot access the raw flash directly.

The JEDEC standard has commands that are supposed to remove data from the raw flash. In Cisco's implementation, the "Erase" and "Sanitize" commands are used. The eMMC standard JESD84-B51 defines "Sanitize" as follows:

Note The Sanitize operation is a feature that is used to remove data from the device according to Secure Removal Type. The use of the Sanitize operation requires the device to physically remove data from the unmapped user address space.

Note After the sanitize operation is completed, no data *should exist* in the unmapped host address space.

Important Zeroization does NOT erase removable media such as SD Card and USB Storage. This media must be removed from the system and erased or destroyed using procedures that are outside the scope of this document.

Important Notice about Zeroization

Caution Zeroize does a very thorough wipe of all non-protected parts of the eMMC flash using the best technology designed by the flash manufacturer today and can do so using the push of a button without the need for a console, ssh, or management session of any kind. It is the integrator's and end user's responsibility to determine the suitability regardless of the CLI keyword used to enable the feature.

Caution While Cisco IOS and Cisco IOS-XE use the command line text of "declassify" in the command line interface (CLI) to enable the zeroize feature, in no way does this represent any specific endorsement or acknowledgment of a Government approved flash erasure methodology.

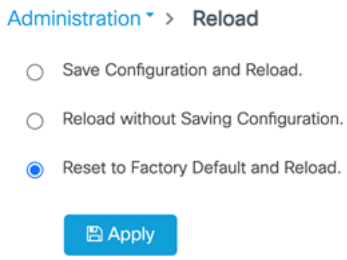
Caution Declassification procedures are unique to each Government organization. Cisco solely provides the technical detail of the erasure operation here, not the policy distinction or any specific recommendation per classification.

Caution Please refer to your respective Government Agency policies, procedures, and recommendations for the handling of sensitive data to see if this procedure meets with those requirements.

WARNING!

The CLI **service declassify erase-all** is literally a **software self-destruct mechanism** intended for defense and intelligence environments that attempts to wipe clean, all of the writable non-volatile storage on the device to clear the device configuration, other stored configurations and all security credentials including any additional license keys.

Please do not use this feature in lieu of doing a **write erase** from the CLI or from the Administration page, Reload option of the WebUI. Invoke the reload with the **Reset to Factory Default and Reload** option and click **Apply**. See the following figure.



If **service declassify erase-all** is invoked, after restoring the IOS-XE image and device configuration, you must re-license the device using the standard Cisco Smart Licensing procedures which ultimately require a Cisco Smart Account and access to the internet or a satellite license server.

Command Line Interface

There are two levels of Zeroization actions, erase-nvram and erase-all. The following CLI shows the options:

```
Switch(config)#service declassify ?
erase-nvram    Enable erasure of switch configuration as declassification action. Default
is no erasure.
erase-all      Enable erasure of both flash and nvram file systems as part of
declassification. Default is no erasure
```

The “erase-nvram” level of declassification process searches for the following files, and erases the ones found.

- flash:/nvram_config
- flash:/vlan.dat

This also erases the complete NVRAM filesystem, therefore, all configurations, including startup and running configurations will get deleted.

The perma-locked bootable image(s) in the flash file system will still be available and can be used for booting the device. See Recovery Procedures, on page 4

The “erase-all” level of Zeroization process erases the entire flash file system. This also wipes out all files and perma-locked bootable image(s). All interfaces are shut down before this process. Here, erasure of individual files in the flash file system is not possible and the only option is to erase the entire flash file system. This also erases packet data, ASIC data and processors related caches along with scrubbing Main memory.

With any level of Zeroization, the switch always fall back to the ROMMON prompt on the console after the erasure of configuration files or flash file system.

Zeroization Trigger

The user needs to press the Push Button after configuring the level of erasure required by the above CLI commands. To make sure that the Push Button press has been identified by underlying software, the user needs to press and hold it for ONE second, or at least till the zero LED starts blinking.

Recovery Procedures

Complete these steps in order to perform an emergency recovery:

Procedure

Step 1 Boot the emergency install image.

Example:

```
switch: boot emgy0:<image-name>.SPA.bin
Booting golden bootloader...
Initializing disk drivers...
Initializing file systems...
**********************************************************
* Rom Monitor for ESS3300                                *
* Copyright (c) 2017-2018 by Cisco Systems, Inc.         *
* All rights reserved.                                   *
**********************************************************
* Version:  1.1.1
* Compiled: Sun 01-Jul-18 22:17 [RELEASE SOFTWARE]
* Boot Partition: qspi-golden-bootloader
* Reset Reason: Soft Reset
Loading "emgy0:ess3x00-universalk9.16.09.01.SPA.bin" to memory...
Verifying image "emgy0:ess3x00-universalk9.16.09.01.SPA.bin"...
Image passed digital signature verification
Checking for Bootloader upgrade...
Bootloader upgrade not required
SUP PL (profile: 1) configuration done successfully
<...>
Press RETURN to get started!
Switch>
```

Step 2 Configure an IP address on the switch. Additional details on IP configuration can be found here .

Example:

```
switch(config-if)#ip address <ip-address> <subnet-mask>
```

Step 3 Ping the terminal that contains the TFTP server in order to test the connectivity:

Example:

```
switch# ping 192.0.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.0.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Step 4 Copy the image via tftp

Example:

```
switch# copy tftp://location/directory/bundle_name flash:<...>
```

Step 5 Restart the system.

Example:

```
switch#reload
Proceed with reload? [confirm]Enter
```