Device Zeroization

This chapter contains the following sections:

Device Zeroization

Zeroization consists of erasing any and all potentially sensitive information in the router. This includes erasure of Main memory, cache memories, and other memories containing packet data, NVRAM, and Flash memory. The process of zeroization is launched upon the initiation of a user command and a subsequent trigger.

By default, the router will have the zeroization feature disabled. SPI: Flash, I2C, and ACT2 are not impacted by this feature.

When zeroization is functionally active, the SYS LED indicates blinking yellow until the router reloads.

Important In order to recover the device from a complete zeroization, it must be configured with a Cisco supported USB3.0 device.

Caution The ESR6300 does not support USB hot plug when it is in ROMMON mode.

Push Button

There is no actual button on the ESR6300, and the system integrator must configure their platform with a Push Button. Reset on an ESR6300 does not cause the device to reboot, but initiates the configured level of zeroization.

Zeroization can be triggered by the Push Button, or software-triggered by a privilege 15 user with console access. There is no remote access for security reasons.

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

Important Notice about Zeroization

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

"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".

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

Warning 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.

Warning 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.

Warning 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.

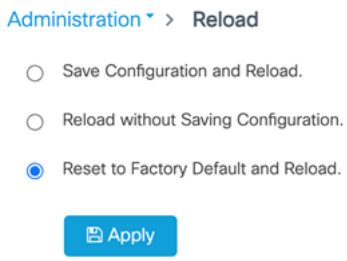
Warning Declassification procedures are unique to each Government organization. Cisco solely provides the technical detail of the erasure operation here, not the policy distinction or any specific recommendation per classification.

Warning 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.

Zeroization Details

These are the detailed steps the ESR6300 software performs after pressing the Push Button with **service declassify erase-all** enabled:

Zeroization is triggered after push button is pressed for 4 seconds:

1. Software will check if **service declassify erase-all** is enabled in the configuration. If not enabled, then nothing happens. If it is enabled, then will move on to the next step.
2. Software deletes vlan.dat, nvram_config, moncfg, and NVRAM partition. Then software sanitizes the eMMC which is the storage device permanently soldered to the ESR6300 module.
3. Software removes all rommon variables, but it will set one rommon variable to tell bootloader to finish the rest of zeroization process. Eventually that rommon variable will be removed by bootloader after it finishes zeroization.
4. A software trigger is set to soft reload the system. Control is passed to the bootloader.

Zeroization Performed on bootloader:

1. After display banner is in rommon, it will then read the rommon variable flag. If the flag exists, then it will finish the rest of zeroization by executing the erase and sanitize commands to the eMMC device. This results in the bootflash partition being removed.
2. Next, it removes the rommon variable flag if zeroization was successful and it will go back to the rommon CLI prompt.

Note If a power cycle happens during zeroization, the bootloader would start zeroization over again since the rommon variable for zeroize is still present.

The following message appears on the console when reset has been triggered:

```
System Bootstrap, Version 1.4(DEV) [vandvisw-vandvisw 113], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2019 by cisco Systems, Inc.
Compiled at Mon Jun 3 10:56:19 2019 by vandvisw
ESR-6300-CON-K9 platform with 4194304 Kbytes of main memory
MCU Version - Bootloader: 8, App: 10
MCU is in application mode.
Reset button push detected
```

Zeroization Trigger

Zeroization can be triggered by either software or by the Push Button. In either case, there are a series of commands that need to be entered.

```
Router#config terminal
Router(config)#service declassify {erase-nvram | erase-all}
```

To confirm if the option is enabled:

```
Router#show declassify
Declassify facility: Enabled=Yes  In Progress=No
  Erase flash=Yes  Erase nvram=Yes
  Declassify Console and Aux Ports
  Shutdown Interfaces
  Reload system
```

To remove the option, use the following command:

```
Router(config)#no service declassify
```

To Trigger Zeroization

To trigger the zeroization from the command line:

```
Router#declassify trigger
```

To trigger the zeroization from the Push Button, press and hold the button for 4+ seconds. When the system auto reloads, it will come up in ROMMON mode: "$$" with bootflash: wiped clean.

Command Line Interface

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

```
router(config)#service declassify ?
erase-nvram    Enable erasure of router 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
```

Microcontroller Unit (MCU)

The MCU is part of the ESR6300 hardware. It performs the following functions:

- Monitors the Push Button status at power up
- Monitors the system hardware watchdog output
- Maintains Reset Reason register
- Controls the SYS LED

The MCU versions are displayed using show version. Details on MCU version and upgrade status are also stored in Flash: as boothelper.log. The MCU is automatically upgraded by the software.

```
Router#show ver | i MCU
MCU bootloader version: 8
MCU application version: 10

Router#cat flash:boothelper.log
Logging at Fri Nov 15 05:00:54 Universal 2019
boot loader upgrade enabled
Bootloader is up-to-date
Current MCU App version is 10
MCU firmware is up-to-date
```

In the event the MCU Application is corrupt, or does not match the Release Notes version, this has to be repaired. Steps to recover from this state: Reload router, hit Ctrl+C to break into rommon mode.

```
Rommon>set MCU_UPGRADE=IGNORE<- Ignore MCU firmware upgrade errors.

Rommon>sync

Rommon>reset

Rommon>boot bootflash:<image>
```

Once the MCU successfully upgrades, you can disable/unset this IGNORE option in rommon. Details on other MCU setting rommon options follow: (there are no available IOS configuration options or linux shell mode troubleshooting measures)

```
set MCU_UPGRADE=SKIP <- Prevents MCU firmware upgrade from taking place.

set MCU_UPGRADE=FORCE <- Forces MCU firmware upgrade to take place.

unset MCU_UPGRADE <- Normal operation. Allows automatic upgrade.
```