System Logging Guide, Cisco IOS XE 17 (Cisco ASR 900 Series)

First Published: 2022-11-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

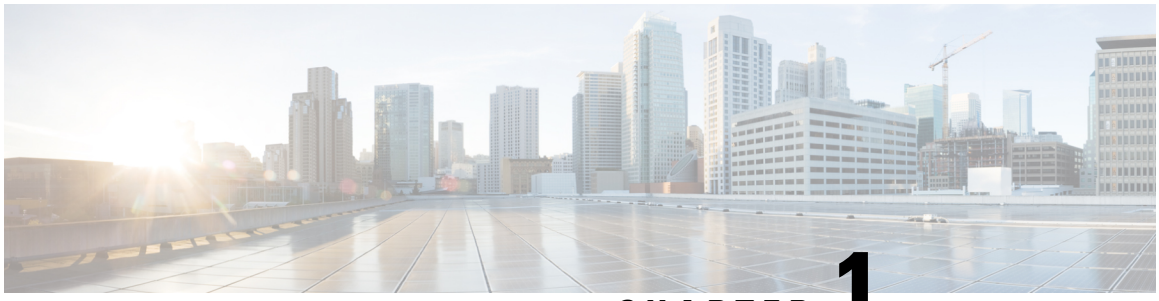
CHAPTER 1 **Feature History** 1

CHAPTER 2 **Configuration of Onboard Failure Logging** 3

- Restrictions for OBFL 3
- Overview of OBFL 3
- Data Collected by OBFL 3
  - Temperature 4
    - Example for Temperature 5
  - Voltage 6
    - Example for Voltage 6
  - Message Logging 7
    - Example for Error Message Log 7
- Enabling OBFL 8
- Disabling OBFL 8
- Displaying OBFL Information 9
  - Clearing OBFL Information 9

CHAPTER 3 **Cisco Secure Development Lifecycle—Factory Reset** 11

- Prerequisites for Performing Factory Reset 13
- Limitations for Performing Factory Reset 13
- Factory Reset Command Options 13
- Clear User Files from Bootflash on Factory Reset 15

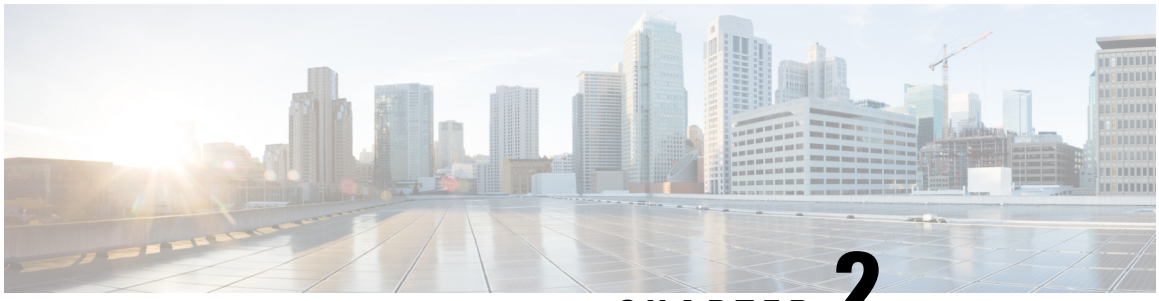


CHAPTER 1

Feature History

The following table lists the new and modified features supported in the System Logging Guide in Cisco IOS XE 17 releases.

Feature	Description
Cisco IOS XE Dublin 17.10.1	
Clear User Files from Bootflash on Factory Reset with "No Service Password Recovery" Configuration Enabled	This feature provides additional security by removing all user files from bootflash during factory reset. It prevents the malicious users from accessing configuration files that are stored in bootflash.
Cisco IOS XE Bengaluru 17.6.1	
Cisco Secure Development Lifecycle—Factory Reset	This feature removes all the customer-specific data that stored on the device since the time of its shipping. Data erased includes configurations, log files, boot variables, core files, and credentials like FIPS-related keys. Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable proces designed to increase Cisco product resiliency and trustworthiness. The following new commands are introduced: • **factory-reset all** • **factory reset keep-licensing-info** • **factory-reset all secure 3-pass DoD 5220.22-M**
Cisco IOS XE Bengaluru 17.5.1	
OBFL Enhancements	You can enable the **`show logging onboard slot ver_uptime`** command to view OBFL information on the Cisco router.



CHAPTER 2

Configuration of Onboard Failure Logging

This chapter describes how to configure Onboard Failure Logging (OBFL).

- Restrictions for OBFL, on page 3
- Overview of OBFL, on page 3
- Data Collected by OBFL, on page 3
- Enabling OBFL, on page 8
- Disabling OBFL, on page 8
- Displaying OBFL Information, on page 9

Restrictions for OBFL

- Software Restrictions—If a device (router or switch) intends to use *linear* flash memory as its OBFL storage media, Cisco IOS software must reserve a minimum of two physical sectors (or physical blocks) for the OBFL feature. Because an erase operation for a linear flash device is done on per-sector (or per-block) basis, one extra physical sector is needed. Otherwise, the minimum amount of space reserved for the OBFL feature on any device must be at least 8 KB.
- Hardware Restrictions—To support the OBFL feature, a device must have at least 8 KB of nonvolatile memory space reserved for OBFL data logging.

Overview of OBFL

The Onboard Failure Logging (OBFL) feature collects data such as operating temperatures, hardware uptime, interrupts, and other important events and messages from system hardware installed in a Cisco router or switch. The data is stored in nonvolatile memory and helps technical personnel diagnose hardware problems.

Data Collected by OBFL

The OBFL feature records operating temperatures, hardware uptime, interrupts, and other important events and messages that can assist with diagnosing problems with hardware cards (or modules)installed in a Cisco router or switch. Data is logged to files stored in nonvolatile memory. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records. The OBFL feature provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the system. Data is recorded in one of two formats: continuous information

that displays a snapshot of measurements and samples in a continuous file, and summary information that provides details about the data being collected. The data is displayed using the show logging onboard command. The message “No historical data to display” is seen when historical data is not available.

The following sections describe the type of data collected:

Temperature

Temperatures surrounding hardware modules can exceed recommended safe operating ranges and cause system problems such as packet drops. Higher than recommended operating temperatures can also accelerate component degradation and affect device reliability. Monitoring temperatures is important for maintaining environmental control and system reliability. Once a temperature sample is logged, the sample becomes the base value for the next record. From that point on, temperatures are recorded either when there are changes from the previous record or if the maximum storage time is exceeded. Temperatures are measured and recorded in degrees Celsius.

Note The following table with temperature description is only for your reference. The slots and sensors may vary based on your router.

Table 1: Temperature Description

Slot	Sensor	Description
P0	Temp 1	Power Module1 Sensor-1
	Temp 2	Power Module1 Sensor-2[1]
P1	Temp 1	Power Module2 Sensor-1
	Temp 2	Power Module2 Sensor-2
P2	FC PWM1	Fan Tray Sensor
	FC PWM1	Top Fan Tray Sensor
P3	Temp 1	Power Module3 Sensor-1
	Temp 2	Power Module3 Sensor-2
P4	FC PWM1	Bottom Fan tray Sensor
P5	FC PWM3	Power Module Fan Tray Sensor

Slot	Sensor	Description
R0	CPU	RP0 CPU Sensor
	C-Inlet	RP0 CPU Board inlet sensor
	C-Outlet	RP0 CPU Board outlet sensor
	PCIe Sw	RP0 PCIe Switch Sensor
	ARAD+0	RP0 NPU0 Sensor
	ARAD+1	RP0 NPU1 Sensor
	Inlet	RP0 Inlet Sensor
	N-Inlet	RP0 NPU Board Inlet Sensor
	N-Outlet	RP0 NPU Board Outlet Sensor
	Outlet	RP0 Outlet Sensor
R1	CPU	RP1 CPU Sensor
	C-Inlet	RP1 CPU Board inlet sensor
	C-Outlet	RP1 CPU Board outlet sensor
	PCIe Sw	RP1 PCIe Switch Sensor
	ARAD+0	RP1 NPU0 Sensor
	ARAD+1	RP1 NPU1 Sensor
	Inlet	RP1 Inlet Sensor
	N-Inlet	RP1 NPU Board Inlet Sensor
	N-Outlet	RP1 NPU Board Outlet Sensor
	Outlet	RP1 Outlet Sensor

[1] There are two sensors per power module.

Example for Temperature

```
Router# show logging onboard slot <R0/R1> temperature
Name               Id     Data (C)  Poll      Last Update
-------------------------------------------------------------------------
Temp: FC PWM1      80           24  1         01/31/12 14:36:30
Temp: FC PWM1      80           25  1         01/31/12 14:37:30
Temp: FC PWM1      80           23  1         01/31/12 14:38:30
Temp: FC PWM1      80           25  1         01/31/12 14:40:30
Temp: FC PWM1      80           24  1         01/31/12 14:41:30
Temp: FC PWM1      80           25  1         01/31/12 14:43:31
Temp: FC PWM1      80           23  1         01/31/12 14:46:31
Temp: FC PWM1      80           25  1         01/31/12 14:50:31
Temp: FC PWM1      80           24  1         01/31/12 14:54:31
```

```
Temp: FC PWM1     80           26  1         01/31/12 14:56:31
Temp: FC PWM1     80           24  1         01/31/12 14:57:31
Temp: FC PWM1     80           26  1         01/31/12 15:00:31
Temp: FC PWM1     80           24  1         01/31/12 15:02:31
Temp: FC PWM1     80           25  1         01/31/12 15:03:31
Temp: FC PWM1     80           24  1         01/31/12 15:04:32
Temp: FC PWM1     80           26  1         01/31/12 15:08:32
Temp: FC PWM1     80           24  1         01/31/12 15:11:32
```

To interpret this data:

- A column for each sensor is displayed with temperatures listed under the number of each sensor, as available.
- The ID column lists an assigned identifier for the sensor.
- Temp indicates a recorded temperature in degrees Celsius in the historical record. Columns following show the total time each sensor has recorded that temperature.
- Sensor ID is an assigned number, so that temperatures for the same sensor can be stored together.
- Poll indicates the number of times a given sensor has been polled.
- The Last Update column provides the most recent time that the data was updated.

Voltage

OBFL allows you to track the voltage of system components, as shown in the following example.

Example for Voltage

```
Router# show logging onboard slot R1 voltage
Name              Id    Data (mV)  Poll      Last Update
-------------------------------------------------------------------------
VNILE: VX1        20         1002  1         01/30/12 03:45:46
VNILE: VX2        21         1009  1         01/30/12 03:45:46
VNILE: VX3        22         1492  1         01/30/12 03:45:46
VNILE: VX4        23         1203  1         01/30/12 03:45:46
VNILE: VP1        24         1790  1         01/30/12 03:45:46
VNILE: VP2        25         2528  1         01/30/12 03:45:47
VNILE: VP3        26         3305  1         01/30/12 03:45:47
VNILE: VH         27        12076  1         01/30/12 03:45:47
VCPU : VX1        32          997  1         01/30/12 03:45:47
VCPU : VX2        33         1054  1         01/30/12 03:45:47
VCPU : VX3        34         1217  1         01/30/12 03:45:47
VCPU : VX4        35         1526  1         01/30/12 03:45:47
VCPU : VP1        36         4992  1         01/30/12 03:45:47
VCPU : VP2        37         3368  1         01/30/12 03:45:47
VCPU : VP3        38         2490  1         01/30/12 03:45:47
VCPU : VP4        39         1803  1         01/30/12 03:45:48
VCPU : VH         40        12034  1         01/30/12 03:45:48
VNILE: VX1        20         1001  1         01/30/12 03:48:11
VNILE: VX2        21         1008  1         01/30/12 03:48:11
VNILE: VX3        22         1492  1         01/30/12 03:48:11
VNILE: VX4        23         1200  1         01/30/12 03:48:11
VNILE: VP1        24         1790  1         01/30/12 03:48:11
VNILE: VP2        25         2530  1         01/30/12 03:48:11
VNILE: VP3        26         3305  1         01/30/12 03:48:11
VNILE: VH         27        12066  1         01/30/12 03:48:11
VCPU : VX1        32          997  1         01/30/12 03:48:11
```

```
VCPU : VX2        33         1054  1         01/30/12 03:48:11
VCPU : VX3        34         1218  1         01/30/12 03:48:11
VCPU : VX4        35         1526  1         01/30/12 03:48:11
```

To interpret this data:

- The Name and ID fields identify the system component.
- The Data (mV) indicates the component voltage
- The poll field indicates the number of times the component voltage has been polled.
- A timestamp shows the date and time the message was logged.

Message Logging

The OBFL feature logs standard system messages. Instead of displaying the message to a terminal, the message is written to and stored in a file, so the message can be accessed and read at a later time.

Example for Error Message Log

```
--------------------------------------------------------------------------------
ERROR MESSAGE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
ERROR MESSAGE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS Facility-Sev-Name
--------------------------------------------------------------------------------
03/06/2007 22:33:35  %GOLD_OBFL-3-GOLD : Diagnostic OBFL: Diagnostic OBFL testing
```

To interpret this data:

- A timestamp shows the date and time the message was logged.
- Facility-Sev-Name is a coded naming scheme for a system message, as follows:
  - The Facility code consists of two or more uppercase letters that indicate the hardware device (facility) to which the message refers.
  - Sev is a single-digit code from 1 to 7 that reflects the severity of the message.
  - Name is one or two code names separated by a hyphen that describe the part of the system from where the message is coming.
- The error message follows the Facility-Sev-Name codes. For more information about system messages, see the Cisco System Messages.
- Count indicates the number of instances of this message that is allowed in the history file. Once that number of instances has been recorded, the oldest instance will be removed from the history file to make room for new ones.
- The Persistence Flag gives a message priority over others that do not have the flag set.

Enabling OBFL

Note The OBFL feature is enabled by default. Because of the valuable information this feature offers technical personnel, it should not be disabled. If you find the feature has been disabled, use the following steps to reenable it.

Procedure

	Command or Action	Purpose
Step 1	Router# **enable**	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router(config)# **hw-module slot {R0 | R1} logging onboard enable** **Example:** `hw-module slot R0 logging onboard enable`	Enables OBFL on the specified hardware module.
Step 4	Router(config)# **end**	Ends global configuration mode.

Disabling OBFL

Procedure

	Command or Action	Purpose
Step 1	Router# **enable**	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router(config)# **hw-module slot {R0 | R1} logging onboard disable** **Example:** `hw-module slot R0 logging onboard disable`	Enables OBFL on the specified hardware module.
Step 4	Router(config)# **end**	Ends global configuration mode.

Displaying OBFL Information

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
OBFL Enhancements	Cisco IOS XE Bengaluru 17.5.1	You can enable the **show logging onboard slot ver_uptime** command to view OBFL information on the Cisco router.

You can use the following commands to display OBFL information:

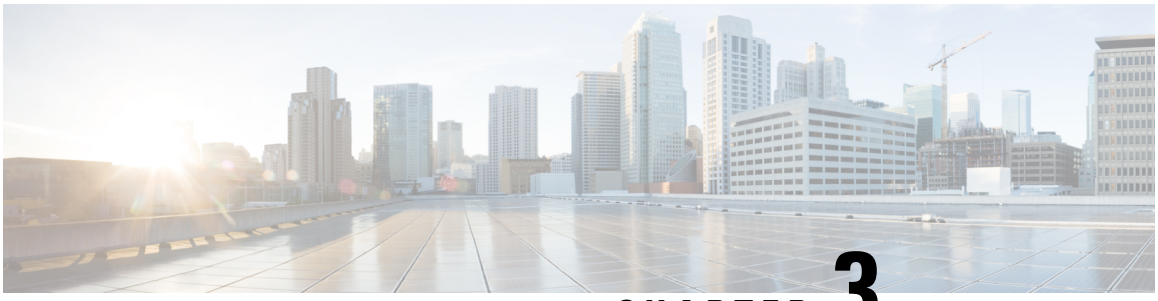
- show logging onboard slot status—To display the slot status.
- show logging onboard slot temperature—To display the slot temperature.
- show logging onboard slot voltage—To display the slot voltage.
- show logging onboard slot hw_errors—To display any hardware error in the setup.
- show logging onboard slot uptime— To display historical board bootup time.
- show logging onboard slot ver_uptime— To display historical board bootup time with version information.

Clearing OBFL Information

You can use the **clear logging onboard slot {R0 | R1} {temperature | voltage}** command to clear OBFL data:

Router#**clear logging onboard slot R1 voltage**

You can use the **show logging onboard temperature** or **show logging onboard voltage** command to verify that the OBFL data is cleared.



CHAPTER 3

Cisco Secure Development Lifecycle—Factory Reset

Table 3: Feature History

Feature Name	Release Information	Description
Cisco Secure Development Lifecycle—Factory Reset	Cisco IOS XE Bengaluru 17.6.1	This feature removes all the user-configured data that are stored on the device from the time of its shipping. Data erased includes configurations, log files, boot variables, core files, and credentials like FIPS-related keys. Cisco Secure Development Lifecycle (CSDL) is a repeatable and measurable process designed to increase Cisco product resiliency and trustworthiness. The following new commands are introduced: • **factory-reset all** • **factory-reset keep-licensing-info** • **factory-reset all secure 3-pass**

Starting with Cisco IOS XE Release 17.6.1, the Cisco Secure Development Lifecycle (CSDL) — Factory Reset feature removes the following customer-specific data that are stored on the device since the time of its shipping:

- Configurations
- Log files
- Boot variables

- Core files
- Credentials like FIPS-related keys

The following table provides details about the data that is erased and retained during the Factory Reset process:

Table 4: Data Erased and Retained During Factory Reset

Data Erased	Data Retained
All Cisco IOS images **Note** The factory reset process takes a backup of the boot image if the system is booted from an image stored locally (bootflash).	Data from Remote field-replaceable units (FRUs)
Crash information and logs	Value of the configuration register
User data, and startup and running configuration	Contents of USB
Credentials like FIPS-related keys	Credentials like Secure Unique Device Identifier (SUDI) certificates, Public key infrastructure (PKI) keys
On board Failure Logging (OBFL) logs	—
ROMMON variables added by the user	—
Licenses	—

Note After a factory reset, the device returns to its default license.

Factory reset securely purge all physical storage to enter a clean state and protect sensitive data. The following data are deleted as a part of factory reset:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

The Factory Reset process is used in the following two scenarios:

- Return Material Authorization (RMA) for a device—If you have to 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 the factory reset that results in the router entering the ROMMON mode. After a factory reset, the device clears all its environment variables including the MAC_ADDRESS and the IP_ADDRESS, which are required to locate and load the software. Perform a reset in ROMMON mode to automatically set the environment variables.

After the system reset in ROMMON mode is complete, you can add the Cisco IOS image either through a USB or TFTP.

- Prerequisites for Performing Factory Reset, on page 13
- Limitations for Performing Factory Reset, on page 13
- Factory Reset Command Options, on page 13
- Clear User Files from Bootflash on Factory Reset, on page 15

Prerequisites for Performing Factory Reset

- Ensure that all the software images, configurations, and personal data are backed up before performing the factory reset operation.
- Ensure that the device is not in the stacking mode as factory reset is supported only in the standalone mode. For Modular-chassis in high availability mode, factory reset is applied per supervisor.
- Ensure that there is uninterrupted power supply when the process is in progress.
- Ensure that you take a backup of the current image before you begin the factory reset process.
- Ensure that neither In-Service Software Upgrade (ISSU) nor In-Service Software Downgrade (ISSD) is in progress before starting the factory reset process.

Caution Removing OBFL logs may hamper failure analysis after RMA. Take precaution before deleting the log files.

Limitations for Performing Factory Reset

- Software patches, if installed on the device, will not be restored after the factory reset operation.
- If the **factory-reset** command is issued through a vty session, the session is not restored after completion of the factory reset process.

Factory Reset Command Options

1. **Erase All Data**:

   To erase all data:

   ```
   Router>enable
   Router#factory-reset all
   ```

   The **factory-reset all** command erases the following data:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

2. **Erase All Data Except License Information**:

   To erase all data except the license information:

   ```
   Router>enable
   Router#factory-reset keep-licensing-info
   ```

   The **factory-reset keep-licensing-info** command erases the following data:

   - All writable file systems and personal data
   - OBFL logs
   - User data and startup configuration
   - ROMMON variables
   - User credentials

3. **Erase All Data Using DoD 5220.22-M Wiping Standard**:

   To erase all data using the the National Industrial Security Program Operating Manual (DoD 5220.22-M) Wiping Standard:

   ```
   Router>enable
   Router#factory-reset all secure 3-pass
   DoD 5220.22-M
   ```

Use the following options for HA and standalone routers:

- Any factory reset option with image.bin is present on the subfolder of bootflash.
- For any factory reset option with packages.conf based boot, if packages.conf is present in any sub folder path under bootflash, the packages.conf and packages are copied back to bootflash root path after the factory reset.
- Check for prompt abort cases as "Monitor for confirmation prompt." The **factory-reset** command should not proceed when aborted before final confirmation.When the standby router is not reachable, a message must appear stating factory reset will be performed only on the active router.

Note

- If you boot the image from local storage, the image (.bin or packages.conf/packages) is retained after factory reset.
- If you boot the image from TFTP server, the booted image is not copied to bootflash.
- Only the config register value is retained. All other ROMMON variables are cleared.

Clear User Files from Bootflash on Factory Reset

Table 5: Feature History

Feature Name	Release Information	Description
Clear User Files from Bootflash on Factory Reset with "No Service Password Recovery" Configuration Enabled	Cisco IOS XE Dublin 17.10.1	This feature provides additional security by removing all user files from bootflash during factory reset. It prevents the malicious users from accessing configuration files that are stored in bootflash. This feature is applicable for Cisco ASR 900 series routers.

Starting with Cisco IOS XE Dublin Release 17.10.1, this feature removes all the user files from bootflash during factory reset associated with "no service password recovery" on the ASR 900 RSP3 and RSP2 modules. This feature is supported in ROMMON version 15.6(54r)S. Ensure that you upgrade to the Cisco IOS XE 17.10.1 Dublin release version to get autoupgraded to this specific ROMMON version.

During recovery mechanism from no-service password recovery configuration, when you attempt to boot with default configurations (Press CTRL+C and "yes"), this feature helps in removing the user files from bootflash along with the startup-configuration. It prevents the malicious users from accessing configuration files that are stored in the bootflash. All the required system files and software images are retained in the bootflash during the erase operation.