



CISCO ASR 920 Series Secure Development Lifecycle Factory Reset User Guide

[Home](#) » [Cisco](#) » CISCO ASR 920 Series Secure Development Lifecycle Factory Reset User Guide 

Contents

- 1 CISCO ASR 920 Series Secure Development Lifecycle Factory Reset
- 2 Prerequisites for Performing Factory Reset
- 3 Limitations for Performing Factory Reset
- 4 Factory Reset Command Options
- 5 Clear User Files from Bootflash on Factory Reset
- 6 Documents / Resources
 - 6.1 References



CISCO ASR 920 Series Secure Development Lifecycle Factory Reset



Table 1: Feature History

Feature Name	Release Information	Description
Cisco Secure Development Lifecycle—Factory Reset	Cisco IOS XE Bengaluru 17.6.1	<p>This feature removes all the user-configured data that are stored on the device from the time of its shipping. Data erased includes</p> <p>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.</p> <p>The following new commands are introduced:</p> <ul style="list-style-type: none"> • 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 2: 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 purges all physical storage to enter a clean state and protect sensitive data. The following data are deleted as a part of the 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 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 which 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 3
- Limitations for Performing Factory Reset, on page 3
- Factory Reset Command Options, on page 3
- Clear User Files from Bootflash on Factory Reset,

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 an 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 precautions 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 the completion of the factory reset process.

Factory Reset Command Options

- 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

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

Erase All Data Using DoD 5220.22-M Wiping Standard:

- To erase all data using 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 in the subfolder of boot flash.
- For any factory reset option with packages.conf-based boot, if packages.conf is present in any subfolder 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 the 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 3: 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 Cupertino 17.9.1	This feature provides additional security by removing all user files from bootflash during factory reset. It prevents malicious users from accessing configuration files that are stored in bootflash on the ASR 920 series routers.
		<p>This feature is only supported on Cisco ASR 920-10SZ-PD, Cisco ASR-920-12CZ-A/D, Cisco ASR-920-4SZ-A/D, Cisco</p> <p>ASR-920-12SZ-IM,</p> <p>ASR-920U-12SZ-IM, Cisco ASR-920-24SZ-IM, Cisco</p> <p>ASR-920-24SZ-M, and Cisco ASR-920-24TZ-M routers.</p>

Starting with Cisco IOS XE Cupertino 17.9.1, this feature removes all the user files from bootflash during factory reset associated with “no service password recovery” on the ASR 920 series routers. This feature is supported in ROMMON version 15.6(53r)S onwards. Ensure that you upgrade to the Cisco IOS XE 17.9.1 Cupertino release version to get auto-upgraded to this specific ROMMON version. During the recovery mechanism from the 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 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.

Documents / Resources

	CISCO ASR 920 Series Secure Development Lifecycle Factory Reset [pdf] User Guide ASR 920 Series Secure Development Lifecycle Factory Reset, ASR 920 Series, Secure Development Lifecycle Factory Reset, Development Lifecycle Factory Reset, Lifecycle Factory Reset, Factory Reset, Reset
---	---

References

- [User Manual](#)

Manuals+.