Perform a Secure Factory Reset on SD-WAN cEdge Routers

Contents

Introduction

This document describes the secure factory reset procedure for Cisco Catalyst SD-WAN Edge Routers running Cisco IOS® XE.

Background

A factory reset returns the device to its original manufacturing state and is typically required as part of decommissioning, redeployment, or security remediation workflows.

⚠ **Caution**: This article recommends exclusively the `factory-reset all secure` option, which performs data sanitization aligned with NIST SP 800-88 Rev. 1. This method renders data on

---

storage media unrecoverable and provides the highest level of assurance that sensitive data has been permanently removed.

Applicability

The `factory-reset all secure` command is supported on these platforms running Cisco IOS XE:

- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 Series Edge Platforms
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco ISR 1000 Series Integrated Services Routers

Note: The `all secure` option can **only** be used on standalone devices. Verify your platform and Cisco IOS XE version supports the `secure` keyword by checking `factory-reset ?` in privileged EXEC mode before proceeding.

Prerequisites

Before performing the secure factory reset, ensure these prerequisites are met:

- **Backup Configuration:** Export and securely store all device configurations, templates, and policies from the SD-WAN Manager (vManage) prior to reset.
- **Backup Software Images:** Ensure you have a copy of the Cisco IOS XE software image loaded into bootflash **before** performing the reset. While the `secure` option retains the boot image in flash on most platforms, certain platforms sanitize bootflash entirely as part of the secure wipe. As a contingency, always have the Cisco IOS XE image available on a USB drive or accessible TFTP server to guarantee recovery regardless of platform behavior.
- **Uninterrupted Power:** Ensure the device has an uninterrupted power supply throughout the entire reset process. Power loss during sanitization can render the device unrecoverable.
- **Complete Any ISSU Procedures:** If any In-Service Software Upgrade (ISSU) operations are pending or in progress, complete them before initiating the factory reset.
- **Release HSEC License:** The HSEC license must be released from the device **before** performing the factory reset. Return the HSECK9 License as outlined in the "Return the HSECK9 License" section at: Configure HSECK9 License on Cisco Edge Routers
- **Remove from SD-WAN Fabric:** Invalidate the device certificate from vManage and remove the device from the controller overlay before performing the reset.
- **Console Access:** Ensure you have physical console access to the device. After the reset, the device enters ROMMON mode and VTY sessions are not available.

Tip: Confirm the Cisco IOS XE image is loaded into bootflash **and** that a recovery copy is available on USB or TFTP **before** executing the factory reset. While the `secure` option retains the boot image on most platforms, some platforms sanitize bootflash completely during the process.

What Gets Erased

The `factory-reset all secure` command permanently removes this data from the device:

Category	Data Erased
Software	All Cisco IOS XE software images (the current boot image is retained in flash on most platforms; however, on certain platforms bootflash is sanitized entirely)
Configuration	Startup configuration, running configuration
Logs & Diagnostics	Crash info, system logs, OBFL (On-Board Failure Logging)
Security Material	FIPS-related keys and credentials, user-configured PKI keys and certificates
Storage	All user data on removable storage (SATA, SSD, USB)
Licensing	All device licenses (requires re-registration)
ROMMON	User-added ROMMON environment variables

Note: These items are **retained** after the secure factory reset:

- SUDI (Secure Unique Device Identifier) certificates and associated PKI keys
- Configuration register value
- The current boot image (retained in flash on most platforms; on certain platforms bootflash is fully sanitized—always have USB/TFTP recovery staged)

Procedure: Secure Factory Reset

Warning: This procedure is irreversible. Once initiated, all data listed in the previous table is permanently destroyed. Ensure all backups have been verified before proceeding.

Step 1: Access the Device via Console

Connect to the device via a physical console connection. SSH/VTY access is lost during the reset process.

Step 2: Enter Privileged EXEC Mode

```
Device> enable
Device#
```

Step 3: Execute the Secure Factory Reset

Run this command to initiate the secure factory reset:

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

The system prompts for confirmation:

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

Check: At the confirmation prompt, verify one final time that:

- All configurations have been backed up
- The Cisco IOS XE recovery image is available on USB or TFTP
- The device has been removed from the SD-WAN overlay

Type `y` or press **Enter** to confirm and proceed.

Step 4: Wait for Sanitization to Complete

The device performs data sanitization on all storage media. This process can take an extended period depending on storage capacity. **Do not interrupt power during this operation.**

Upon completion, the device automatically reloads and enters ROMMON mode.

Step 5: Restore ROMMON Environment Variables

After the reset, environment variables including `MAC_ADDRESS` and `SERIAL_NUMBER` can be cleared. Perform a ROMMON reset to restore them:

```
rommon 1> reset
```

> **Note**: The BAUD rate environment variable returns to its default value (9600) after a factory reset. If your console session was configured at a different baud rate, you can adjust your terminal emulator settings to 9600 baud to regain console access.

Step 6: Boot the Cisco IOS XE Software Image

On most platforms, the `secure` option retains the boot image in flash. Verify its presence with `dir bootflash:` from ROMMON. If the image is available, boot directly:

```
rommon 2> boot bootflash:<image-filename>.bin
```

> **Platform-specific behavior:** On certain hardware platforms, the secure sanitization process wipes bootflash entirely, including the boot image. In these cases, recover via USB or TFTP.
>
> **Option A — USB recovery:**
>
> ```
> rommon 2> boot usbflash0:<image-filename>.bin
> ```
>
> **Option B — TFTP recovery:**
>
> Set the required ROMMON environment variables, then initiate the transfer:
>
> ```
> rommon 2> IP_ADDRESS=<device-mgmt-ip>
> rommon 3> IP_SUBNET_MASK=<subnet-mask>
> rommon 4> DEFAULT_GATEWAY=<gateway-ip>
> rommon 5> TFTP_SERVER=<tftp-server-ip>
> rommon 6> TFTP_FILE=<image-filename>.bin
> rommon 7> tftpboot
> ```
>
> Verify connectivity to the TFTP server is available through the management interface or a directly connected network segment. ROMMON does not support routing protocols, so the TFTP server must be reachable via the configured default gateway.
>
> Always have a recovery image staged on USB **or** an accessible TFTP server before initiating the factory reset to account for this behavior.

Post-Reset: Re-Onboarding to SD-WAN Fabric

After the device has been restored with a clean Cisco IOS XE image, use standard SD-WAN onboarding

procedures to bring the device back into the fabric:

1. **Bootstrap Configuration:** Apply initial bootstrap configuration (system IP, site ID, organization name, vBond address). Refer to Generate Bootstrap File Using CLI for the procedure.
2. **Certificate Installation:** Install the device certificate and root CA chain as required by your certificate authority (Symantec/DigiCert, Cisco PKI, or Enterprise CA).
3. **Control Connections:** Verify that DTLS/TLS control connections are established to vManage, vSmart, and vBond.
4. **Template Push:** From vManage, attach the appropriate device template or configuration group to the device.
5. **Validation:** Confirm BFD sessions, OMP routes, and data plane tunnels are operational.

Note: After re-onboarding, the HSEC (High Security) license must be manually re-applied via CLI to restore crypto throughput. As documented in Managing HSEC Licenses in Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) does **not** support re-installing an HSEC license on a device. A device reload is required on physical routers to activate the license. Refer to Configure HSECK9 License on Cisco Edge Routers for the manual CLI procedure.

Troubleshooting

Console Unresponsive After Reset

If the console appears unresponsive after the factory reset completes, the baud rate has likely reverted to the default (9600). Adjust your terminal emulator to 9600 baud and reconnect.

Device Does Not Enter ROMMON

If the device does not enter ROMMON after the reset completes, verify the configuration register is set correctly. In most cases, a power cycle forces the device into ROMMON when no bootable image is present.

Missing Environment Variables in ROMMON

If `MAC_ADDRESS` or `SERIAL_NUMBER` variables are missing after the reset, issue the `reset` command in ROMMON to restore factory-default environment variables from hardware storage.

Frequently Asked Questions

Q: Why is the “secure” option recommended over the standard “all” or “3-pass” options?

A: The `factory-reset all secure` option performs the most thorough data sanitization available, aligned with NIST SP 800-88 Rev. 1. It renders data unrecoverable and retains the current boot image in flash, simplifying recovery. By comparison, the `3-pass` option performs a three-pass overwrite pattern (zeroes, ones, random) which takes approximately **three times longer** and also erases the boot image, requiring a full image reload from USB or TFTP. The `secure` option is recommended as it provides the most thorough sanitization with the least operational overhead for recovery.

Q: How long does the secure factory reset take?

A: The duration varies based on the total storage capacity of the device. For devices with standard flash storage (8–32 GB), the process typically completes within 15–45 minutes. Devices with larger SSD or SATA storage can take longer. **Important:** Do not interrupt power during this process. Plan for a maintenance window that accounts for the reset plus image reload and re-onboarding time.

Q: Does the device retain its identity (serial number, SUDI) after the reset?

A: **Yes.** The Secure Unique Device Identifier (SUDI) certificate and its associated PKI keys are stored in hardware-protected storage (TAm/ACT2 chip) and are **not** erased by the factory reset. The device serial number is also preserved in hardware. This means the device can be re-onboarded to the SD-WAN fabric using its original identity after the reset.

Q: Do I need to remove the device from SD-WAN Manager before performing the reset?

A: **Yes.** It is strongly recommended to invalidate the device certificate and remove the device from the SD-WAN overlay **before** performing the factory reset. This ensures clean removal from the controller infrastructure, no stale entries in vManage device inventory, and no orphaned control connections or tunnel state. From vManage: Navigate to **Configuration** > **Certificates** > select the device > **Invalidate**, then **Send to Controllers**. Afterward, delete the device from the device list.

Q: What happens to the HSEC license after the factory reset?

A: The HSEC (High Security) license is removed during the factory reset. Without it, the device operates with restricted crypto throughput. The HSEC license must be **released before** the factory reset so it can be re-used afterward:

1. **Before reset:** Release the license via `license smart authorization return local online` and remove the product instance from Smart License Central.
2. **After re-onboarding:** Manually re-apply the HSEC license via CLI. As documented in Managing HSEC Licenses in Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) does **not** support re-installing the HSEC license.
3. **Reload:** A reload is required on physical routers to activate the license.
4. Verify via `show license summary` and `show license authorization`.

For the full procedure, refer to Configure HSECK9 License on Cisco Edge Routers and Managing HSEC Licenses in Cisco Catalyst SD-WAN.

Q: Can I perform the secure factory reset remotely (via SSH/VTY)?

A: While the command can technically be issued over an SSH/VTY session, it is **strongly discouraged**. The device immediately begins sanitization and the remote session is terminated. After the reset, the device enters ROMMON mode where no IP connectivity is available, no VTY access is possible, and console access is required for image recovery. **Always ensure physical console access is available before initiating the factory reset.**

Q: Is the secure factory reset appropriate for security remediation scenarios?

A: **Yes.** The secure factory reset is the recommended approach when a device must be returned to a known-good state after a suspected compromise. This ensures all attacker-planted keys, backdoors, or persistence mechanisms are permanently removed, no residual configuration or credential data remains, and the device is guaranteed clean for re-onboarding. For security-related factory resets, ensure that new credentials (passwords, keys, certificates) are generated during re-onboarding and that no pre-compromise backup configurations are restored to the device.

Q: Why not use "request platform software sdwan software reset" or "request platform software sdwan config reset" instead?

A: These commands serve a different purpose and do **not** provide the same level of sanitization as `factory-reset all secure`. The `request platform software sdwan software reset` command resets the SD-WAN software overlay but does not wipe underlying Cisco IOS XE configurations, keys, certificates, or storage — the device retains its base OS state. The `request platform software sdwan config reset` command resets only the SD-WAN configuration but leaves the Cisco IOS XE image, local credentials, SSH keys, and all other data intact on disk. Neither command performs data sanitization on the storage media. If the goal is to return the device to a fully clean state — particularly after a security incident — these commands are **insufficient** because residual data (keys, credentials, logs, attacker-planted files) can remain on flash or SSD. Use `factory-reset all secure` when the device must be guaranteed clean at the storage level.

References

- Cisco Trustworthy Systems — Factory Reset Guide
- Configure HSECK9 License on Cisco Edge Routers
- Managing HSEC Licenses in Cisco Catalyst SD-WAN
- Generate Bootstrap File Using CLI — SD-WAN Getting Started Guide
- Upgrade SD-WAN Controllers with the Use of vManage GUI or CLI