



Live Protect

- [Feature history for Live Protect, on page 1](#)
- [Live Protect, on page 1](#)
- [Install Live Protect Shield: 1-step process, on page 3](#)
- [Install Live Protect Shield: 3-step process, on page 4](#)
- [Verify Live Protect configuration, on page 6](#)

Feature history for Live Protect

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1	Live Protect: This feature provides real-time, kernel-level security using eBPF technology through the Tetragon agent embedded in the IOS XE software.	Cisco C9350 Series Smart Switches Cisco C9550 Series Smart Switches Cisco C9610 Series Smart Switches

Live Protect

Live Protect is a security feature that

- provides real-time, kernel-level security using extended Berkeley Packet Filter (eBPF) technology through the Tetragon agent embedded in IOS XE software,
- enables Common Vulnerabilities and Exposures (CVE) compensating controls without software upgrades or reboots, and
- configures Tetragon for monitoring, detection, and logging of security events for enhanced threat visibility and telemetry integration.

Benefits of Live Protect

- **Zero-downtime remediation:** Provides temporary protection against vulnerabilities without requiring software upgrades or device reboots, ensuring continuous network availability until remediation.
- **Dynamic security:** Allows for real-time enforcement of security policies using eBPF technology.
- **Flexible deployment:** You can deploy security shields in two modes. Monitoring mode to provide visibility into potential exploit attempts without enforcement and protecting (enforcing) mode to actively apply mitigation policies to reduce exposure to known vulnerabilities.
- **Visibility:** Provides hit statistics to help track the efficacy of deployed shields.

Key concepts of Live Protect

The Live Protect feature secures IOS XE and provides enhanced security and software integrity assurance for the IOS XE device control plane. A few key concepts of this feature are:

- **Extended Berkeley Packet Filter:** Also abbreviated as eBPF, is a powerful Linux kernel technology that enables programmable, safe, and efficient kernel extensions for networking, security, and observability, forming the foundation for advanced security and networking features.
- **Tetragon:** This is an agent developed by Isovalent and embedded in IOS XE software. It compiles CVE compensating controls/shields into eBPF policies that run in the kernel, enabling advanced monitoring and enforcement of security policies in real time. It provides protection and security through the Live Protect feature. Tetragon is automatically installed on Cisco IOS XE 26.2.1 release and manual installation of the agent is not needed.
- **Live Protect shields:** These shields are release signed artifacts with known good values used to verify the integrity of the software artifact. The Live Protect feature uses tracing policies to provide security observability. These policies are part of the live protect shield which can be downloaded and loaded on the device. Live protect policies are only triggered for control-plane packets and cannot protect downstream or upstream devices from vulnerabilities.
- **Modes:**
 - **Monitoring mode:** Based on the configured policies, the monitoring mode allows the system to detect and generate log files for each anomaly event. Monitoring hit counters are incremented when an event occurs. This mode is the default mode when a shield is activated.
 - **Enforcing mode:** In enforcing mode, Live Protect actively blocks or mitigates detected threats in real time. This mode provides proactive protection by enforcing security policies that prevent exploitation of vulnerabilities such as privilege escalation and control-plane DDoS attacks. Enforcement happens at the kernel level, allowing immediate mitigation without requiring software upgrades, reboots, or downtime. This mode enables continuous protection against emerging CVEs while maintaining operational stability and uptime.

**Note**

- Live Protect feature is supported on all license types unless specified otherwise.
- A reload of the device is not required when a shield is activated.
- If a shield file is deleted from the directory and a device bootup is performed, the device displays this error message. This will not lead to any functional error.

```
%BOOT-3-BOOTTIME_LPS_MISSING_DETECTED: R0/0: install_engine: LPS file
/bootflash/cisco9k_iosxe.26.02.01.CVE-2026-10000-v01.lps.SSA.bin missing and system
impact will be unknown.
```

Install Live Protect Shield: 1-step process

This task shows how to use the single **install add file activate commit** command for installing a Live Protect Shield.

Procedure

Step 1 **enable****Example:**

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password if prompted.

Step 2 **install add file flash: *filename* activate commit****Example:**

```
Device# install add file flash:cisco9k_iosxe.26.02.01.CVE-1900-99999.lps.SPA.bin activate
commit
```

Copies the live protect shield update package from flash to the device, performs a compatibility check for the platform and image versions, activates the package, and makes the package persistent across reloads.

This command extracts the individual components of the .bin file into the subpackages and packages.conf files.

You can also copy the package from a remote location (through FTP, HTTP, HTTPS, or TFTP).

Step 3 **show install summary****Example:**

```
Device# show install summary
```

Displays installed packages information of the software image and live protect shield.

Step 4 **show platform software live-protect shield****Example:**

```
Device# show platform software live-protect shield
```

Displays live protect shield IDs, modes, and the number of hits.

Step 5 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 6 **[no] platform security live-protect shield *lpshield-id* enforcing**

Example:

```
Device(config)# platform security live-protect shield CVE-2023-20190.01 enforcing
```

Sets the live protect shield to enforcing mode. By default, monitoring mode is enabled once the live protect shield package is installed.

Step 7 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Step 8 **show platform software live-protect shield *lpshield-id***

Example:

```
Device# show platform software live-protect shield
```

Displays live protect shield IDs, modes, and the number of hits.

Install Live Protect Shield: 3-step process

This task shows you the 3-step process for installing a Live Protect Shield.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password if prompted.

Step 2 **install add file flash: *filename***

Example:

```
Device# install add file flash:cisco9k_iosxe.26.02.01.CVE-1900-99999.lps.SPA.bin
```

Copies the live protect shield update package from flash to the device, performs a compatibility check for the platform and image versions.

This command extracts the individual components of the .bin file into the subpackages and packages.conf files.

You can also copy the package from a remote location (through FTP, HTTP, HTTPS, or TFTP).

Step 3 **install activate file flash:** *filename*

Example:

```
Device# install activate file flash:cisco9k_iosxe.26.02.01.CVE-1900-99999.lps.SPA.bin
```

Activates the package file that was added and updates the package status details.

Step 4 **install commit**

Example:

```
Device# install commit
```

Commits the activation changes to be persistent across reloads.

The commit can be done after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.

Step 5 **show install summary**

Example:

```
Device# show install summary
```

Displays installed packages information of the software image and live protect shield.

Step 6 **show platform software live-protect shield**

Example:

```
Device# show platform software live-protect shield
```

Displays live protect shield IDs, modes, and the number of hits.

Step 7 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 8 **[no] platform security live-protect shield *lpshield-id* enforcing**

Example:

```
Device(config)# platform security live-protect shield CVE-2023-20190.01 enforcing
```

Sets the live protect shield to enforcing mode. By default, monitoring mode is enabled once the live protect shield package is installed.

Step 9 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Step 10 **show platform software live-protect shield *lpshield-id***

Example:

```
Device# show platform software live-protect shield
```

Displays live protect shield IDs, modes, and the number of hits.

Verify Live Protect configuration

To verify the Live Protect feature configuration, use these show commands:

Command	Purpose
show install summary	Displays installed packages information, like software image and live protect shield filenames and versions.
show install package {bootflash: crashinfo: flash: webui:} <i>file-name</i>	Displays package details which are added for the shield.
show platform software live-protect shield	Displays live protect shield IDs, modes, and the number of hits.
show platform software live-protect slot switch {switch-number active standby}	Displays the switch number or type along with the aggregate live protect hit counters.

This is a sample output from the **show install summary** command:

```
Device# show install summary
```

```
[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St   Filename/Version
-----
```

```
IMG   C    26.02.01.0.237015
LPS   C    flash:cisco9k_iosxe.26.02.01lpseft3.CVE-1900-99999.lps.SPA.bin
```

This is a sample output from the **show install package flash:** command:

```
Device# sshow install package flash:cisco9k_iosxe.26.02.01.CVE-2026-10000-v01.lps.SSA.bin
```

```
Name: cisco9k_iosxe.26.02.01.CVE-2026-10000-v01.lps.SSA.bin
```

```
Version: 27.01.01.0.251074.1786667099..IOSXE
```

```
Platform: CISCO9K
```

```
Package Type: LPS
```

```
Defect ID: CSCaa15401
```

```
Package State: Activated & Committed
```

```
Supersedes List: {}
```

```
LPS Fixes List: CVE-2026-10000
```

```
LPS Build ID: 154
```

LPS Type: non-reload

LPS Compatible with Version: 26.02.01

LPS Impact: Dummy WebUI Vulnerability Shield. User will not be able to edit a file in nginx

LPS Supported Family: cisco9k

This is a sample output from the **show platform software live-protect shield** command:

Device# **show platform software live-protect shield**

Aggregate Live Protect Hit Counters

LP Shield ID	Mode	Enforcing Hits	Monitoring Hits	Total Hits
cve-2026-10000-v01	Enforcing	21	27	48
cve-2026-10011-v02	Monitoring	0	48	48

This is a sample output from the **show platform software live-protect slot switch 4 r0 shield** command:

Device# **show platform software live-protect slot switch 4 r0 shield**

Aggregate Live Protect Hit Counters

Member Switch	LP Shield ID	Mode	Enforcing Hits	Monitoring Hits	Total Hits
4	cve-2026-10000-v01	Enforcing	17	0	17
4	cve-2026-10011-v02	Monitoring	0	17	17
4	cve-2026-10111-v03	Enforcing	17	0	17
4	cve-2026-11111-v04	Monitoring	0	17	17
4	cve-2026-11110-v05	Enforcing	17	0	17

