Secure Cisco Catalyst SD-WAN with Live Protect

Secure Cisco Catalyst SD-WAN with Live Protect

Secure Cisco Catalyst SD-WAN with Live Protect

Feature history for Live Protect

This table describes the developments of this feature, by release.

Feature name	Release information	Description
Live Protect for Cisco SD-WAN Control Components	Cisco Catalyst SD-WAN Control Components Release 20.18.3	Live Protect allows customers to deploy compensating controls (called “Vulnerability Shields”) that protect Cisco products from Common Vulnerabilities and Exposures (CVEs) disclosed in Cisco Security Advisories. An advisory may disclose one or more CVEs, and a Vulnerability Shield may protect against one or more of those CVEs without requiring a device reload or service interruption. Because Vulnerability Shields may not address all vulnerabilities present in a software release and are intended as a temporary measure in place of the software fix, upgrading to the latest release containing the relevant software fixes is the recommended approach to address vulnerabilities in the long term Customers can deploy Vulnerability Shields in Monitoring mode or Enforcing mode. Live Protect allows customers to monitor, enforce, and deactivate Vulnerability Shields until they are retired when a software upgrade or patch is applied, designed to help customers achieve a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risk until software upgrades or patches are deployed.

Live Protect for Cisco Catalyst SD-WAN

Live Protect is a security capability that

- enables compensating controls and vulnerability mitigation without software upgrades or reboots,
- allows you to manage Vulnerability Shields through Cisco SD-WAN Manager to protect against known vulnerabilities before patching.

Deployment modes

You can deploy Vulnerability Shields in two modes:

- Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action.
- Protecting (Enforce) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities.

Benefits of Live Protect

- Zero-downtime remediation: Provides temporary mitigation against vulnerabilities without requiring software upgrades or device reboots, designed to ensure continuous network availability until remediation.
- Dynamic security: Allows real-time enforcement of security policies.
- Flexible deployment: Allows you to deploy Vulnerability Shields in Monitoring mode to provide visibility into potential exploit attempts without enforcement, or in Enforce mode to actively apply mitigation policies and reduce exposure to known vulnerabilities.
- Centralized management: Allows you to manage Vulnerability Shields for supported Cisco Catalyst SD-WAN Control Components through Cisco SD-WAN Manager.
- Visibility: Provides hit statistics to help monitor Vulnerability Shield activity.

Vulnerability Shield lifecycle

Vulnerability Shields are designed to provide interim mitigation for vulnerabilities on Cisco Catalyst SD-WAN Control Components releases. You may temporarily use a Vulnerability Shield until you upgrade to a software release that contains the fix or install another applicable, supported Vulnerability Shield.

-
- Lifecycle policy scope
-
- Vulnerability Shield availability

Lifecycle policy scope

This lifecycle policy defines how Cisco publishes, supports, and retires Vulnerability Shields for supported Cisco Catalyst SD-WAN Control Components and Cisco IOS XE Catalyst SD-WAN devices .

This lifecycle applies to:

- Cisco Catalyst SD-WAN Manager
- Cisco Catalyst SD-WAN Validator
- Cisco Catalyst SD-WAN Controller
- The Live Protect Agent (Tetragon) integrated into the control-component software image
- Cloud-hosted and cloud-tethered Cisco Catalyst SD-WAN deployments

The lifecycle policy does not apply to:

- Cisco IOS XE Catalyst SD-WAN devices
- Air-gapped Cisco Catalyst SD-WAN deployments

Vulnerability Shield availability

Cisco associates each Vulnerability Shield with a Cisco security advisory. A Vulnerability Shield can address one or more Common Vulnerabilities and Exposures (CVEs) identified in the advisory. Cisco SD-WAN Manager displays High and Critical security advisories and identifies the applicable Vulnerability Shields for affected Cisco Catalyst SD-WAN Control Components .

Availability and support policy

Policy item	Rule
Version support	Cisco creates Vulnerability Shields for the SD-WAN release that is current when the shield is published and for the two immediately preceding releases in each supported release train that includes Live Protect. In most cases, the current release already contains the fix for the vulnerability, so shields are created only for the two preceding releases. However, if an actively exploited vulnerability is disclosed before fixed software is available, Cisco may also create a shield for the current release.
Availability period	Cisco announces the download and support period when it publishes a Vulnerability Shield. The six-month period begins when Cisco releases a software fix for the vulnerability.
End of support	At the end of the six-month period, Cisco removes the Vulnerability Shield from download and ends support. Although the installed Vulnerability Shield is no longer supported, if it remains installed it will continue to operate until you manually remove it.
Software upgrades	Upgrading the SD-WAN devices and control-component software removes installed Vulnerability Shields. If the vulnerability still applies after the upgrade, reinstall the appropriate Vulnerability Shield or deploy another applicable Vulnerability Shield.

Vulnerability Shield lifecycle

Stage	**Description**
Day 0 – Publication	Cisco publishes the Vulnerability Shield, makes it available for download, and announces its six-month download and support period.
Day 1 – Deployment	Deploy the Vulnerability Shield in Monitoring, Protecting (Enforce), or Disabled mode. Cisco SD-WAN Manager applies the selected mode to all applicable Cisco Catalyst SD-WAN Control Components.
Day 2 – Operation	Cisco SD-WAN Manager displays the installed Vulnerability Shield and its operating mode. The Vulnerability Shield continues protecting the applicable SD-WAN control components, even if it is no longer supported by Cisco, until you remove it or upgrade the software.
Day N – Upgrade or end of support	A software upgrade removes installed Vulnerability Shields. If the vulnerability still applies after the upgrade, deploy the appropriate, supported Vulnerability Shield again, if any. **Note** After the six-month download and support period ends, an installed Vulnerability Shield continues operating in its existing mode until you manually remove it. Although Cisco no longer provides support or downloads for the shield, it is not automatically removed from the control component.

Note

Live Protect and its Vulnerability Shields may not fully mitigate risks during the device boot process, during which systems may remain temporarily exposed until security policies are initialized. They also do not mitigate the risk of system instability, including boot loops, resulting from incompatible Vulnerability Shields. Although Cisco uses commercially reasonable efforts to develop effective security technologies, Cisco does not represent or warrant that its offerings will provide absolute security or protect all files, systems, networks, or endpoints against all malware, malicious attacks, or other threats.

Configure Live Protect for Cisco SD-WAN Control Components using Cisco SD-WAN Manager

Use these steps to deploy and configure Live Protect Vulnerability Shields in Cisco SD-WAN Manager.

Step 1 From the Cisco SD-WAN Manager menu, go to Monitor > Advisories > Security Advisories.

Step 2 Select Control Components or Devices to display the relevant information for your infrastructure.

Step 3 Select a specific security advisory to view its details.

Step 4 Select Affected Control Components.

Step 5 Choose Deploy Shield.

This shield is deployed to all applicable control components associated with the selected advisory. Individual control component selection for deployment is not supported.

Step 6 Choose the desired mode:

- Monitoring: Observes activity and logs events without blocking traffic.
- Protecting (Enforce): Enforces security policies to actively block exploit attempts.

Note

Shields provide temporary mitigation for identified vulnerabilities until affected components are upgraded to a software version that includes remediation.

Cisco strongly recommends upgrading to a software release containing the fix as soon as possible.

Disable Live Protect using Cisco SD-WAN Manager

Use these steps to disable a Live Protect shield.

Step 1 From the Cisco SD-WAN Manager menu, choose Monitor > Compliance > Advisories.

Step 2 Select the advisory for which you want to deactivate the shield.

Step 3 Select ... and choose Disable Shield.

Monitor Live Protect

You can monitor Live Protect through shield status and event statistics.

-
- View shield status for Live Protect
-
- View event statistics for Live Protect

View shield status for Live Protect

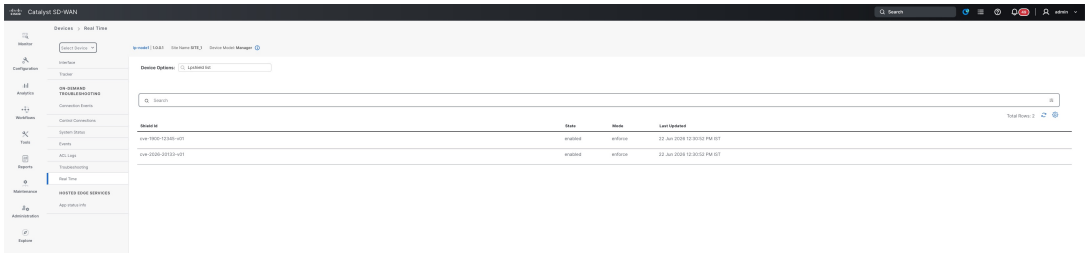
Step 1 From the Cisco SD-WAN Manager menu, go to Monitor > Devices.

Step 2 Select a device to open the Device360 page.

Step 3 Select real-time monitoring from the drop-down list and choose Lpshield List.

The Lpshield List view displays the installed shield status on the selected device.

View shield status



View event statistics for Live Protect

Step 1 From the Cisco SD-WAN Manager menu, go to Monitor > Advisory.

Step 2 Select Control Components.

The Hits field displays the event statistics for the deployed shields.

View event statistics

