



Managing Security Advisories and Protecting Devices Using Nexus Dashboard, Release 4.2.1

Table of Contents

New and changed information	1
Device security overview	2
Security advisories	3
Topology	3
Live Protect overview	4
Prerequisites	4
Live Protect workflow	6
Deploy Live Protect	6
Copyright	9

New and changed information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
Nexus Dashboard 4.2.1	Live Protect	Beginning with Nexus Dashboard 4.2.1 you can protect your network from active threats by deploying compensating-control policies directly to switches, without requiring a maintenance window or immediate software upgrade. For more information, see Live Protect overview .

Device security overview

The **Device Security** page in Nexus Dashboard provides a unified interface for monitoring, evaluating, and responding to security advisories that affect your network devices. It allows you to efficiently manage vulnerabilities and enhance the protection of your Cisco Nexus environment.

You can view the security advisories that apply to your devices on the **Device Security** page by navigating to **Manage > Device Security**.

The screenshot shows the 'Device Security' page in the Nexus Dashboard. The page title is 'Device Security' with sub-tabs for 'Security advisories' and 'Topology'. A sidebar on the left contains navigation options: Home, Manage, Analyze, and Admin. The main content area features a table of advisories with columns for Advisory Id, Title, Advisory level, Status, CVSS, Nodes, Fabric, and actions. The table lists five advisories, all with a 'Warning' level and 'Active' status. The first four are related to Cisco APIC vulnerabilities (CSCwk18865, CSCwk18862, CSCwk18864, CSCwk18863), and the fifth is a Cisco NX-OS vulnerability (CSCwi48264). Buttons for 'Acknowledge advisory' and 'Live Protect Deploy' are visible above the table.

Advisory Id	Title	Advisory level	Status	CVSS	Nodes	Fabric	
cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18865: Cisco APIC Authenticated Local Denial of Service Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	J 0
cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18862: Cisco APIC Authenticated Command Injection Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	J 0
cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18864: Cisco APIC Authenticated Information Disclosure Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	J 0
cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18863: Cisco APIC Stored Cross-Site Scripting Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	J 0
cisco-sa-nxos-cmdinj-Lq6jsZhH	CSCwi48264: Cisco NX-OS Software Command Injection Vulnerability	Warning	Active	4.4	aci-spine1 View all (2 total)	aci130	J 0



You can also view the **Device Security** page from the Nexus Dashboard **Overview** page. Click the number of active advisories or the impacted devices from the **Advisory level** card.

The screenshot shows the 'Welcome, admin' Overview page in the Nexus Dashboard. The 'dual-14 at a glance' section contains four cards: 'Anomaly level' (Healthy, 0 total anomalies), 'Advisory level' (Warning, 23 total, 6 active, 18 impacted), 'Network infrastructure' (2 Fabrics, 0 Inter-fabric, 19 Switches, 2 Active Endpoints), and 'Recent activity' (Login successful, Login initiated). Below this is a 'Fabrics' section with a map of the United States and Europe.

The **Device Security** page includes the following tabs.

- **Security advisories**
- **Topology**

Security advisories

The **Security advisories** tab displays a comprehensive list of current advisories detected across your network. It allows you to assess potential risks and prioritize remediation efforts. You can search, filter, and sort advisories, as well as choose one or more advisories to deploy compensating controls such as Live Protect policies.

For more information, see [Live Protect overview](#).

The **Security advisories** table displays the following details.

Field	Description
Advisory Id	Specifies a unique identifier for the advisory
Title	Provides a brief summary of the advisory and affected vulnerability.
Advisory level	Indicates the severity or priority of the advisory.
Status	Indicates the current state of the advisory.
CVSS	Indicates the Common Vulnerability Scoring System (CVSS) value, that represents the severity of the vulnerability.
Nodes	Indicates the devices or endpoints affected by the advisory.
Fabric	Specifies the network fabric or logical domain impacted by the advisory.
Detection time	Indicates when the advisory was first detected.
Last scan time	Specifies the date and time when the system most recently scanned for this advisory.
Compensating control	Indicates if a compensating control (such as a Tetragon policy) is available or deployed to address the advisory.

Topology

The **Topology** tab provides a visual representation of the managed fabrics within your network. It allows you to quickly assess the security status of various fabrics and view details for specific devices to view their security status and Live Protect availability.

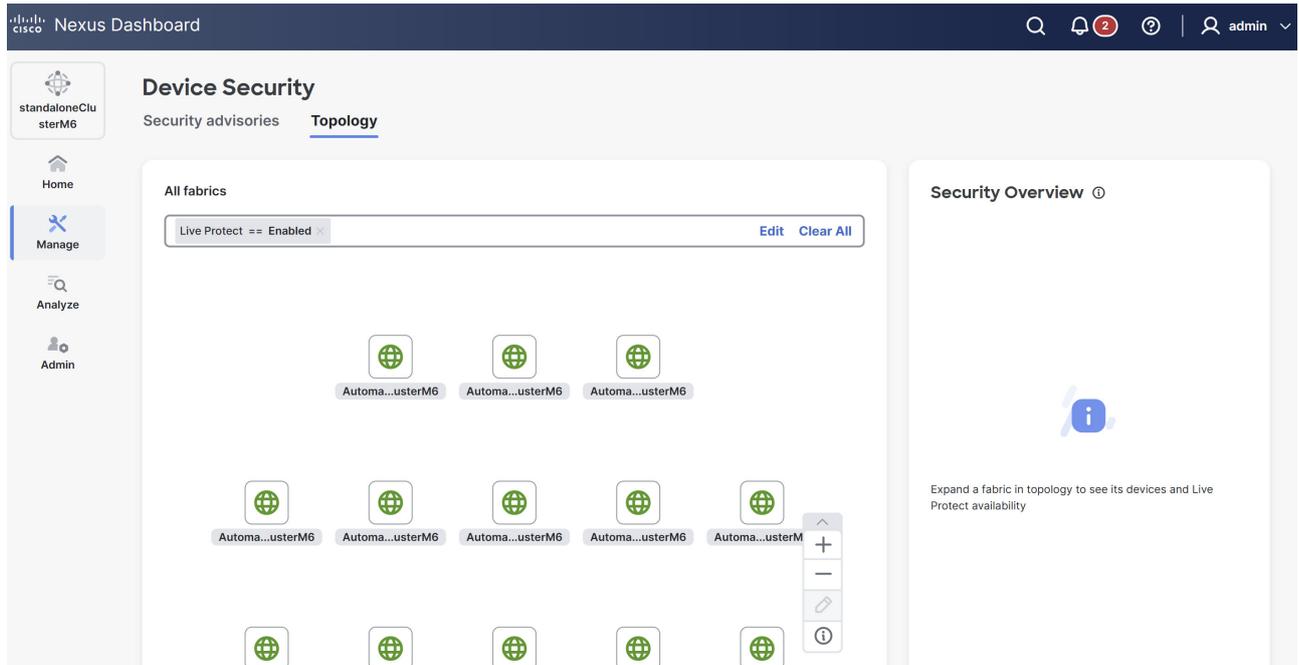
Follow these steps to view the **Topology** page.

1. Navigate to **Manage > Device Security**.

The **Device Security** page displays.

2. Click the **Topology** tab.

Nexus Dashboard displays the graphical view of all managed fabrics and their security status.



3. (Optional) To view specific device details within a fabric, click a fabric icon in the topology map.

The **Topology** page displays the following details.

- Fabric map—provides a high-level overview of the network hierarchy.
- Security Overview—provides details about specific devices and Live Protect availability.

Live Protect overview

Live Protect is a Cisco Nexus feature that enables rapid mitigation of certain security advisories on eligible Nexus 9000 Series switches. By deploying compensating-control policies directly to switches, you can protect your network from active threats without requiring a maintenance window or immediate software upgrade.

For more information, see [Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#).

Live Protect identifies security advisories affecting your devices. If an advisory can be mitigated, the system provides a signed compensating control (Tetragon policy) in the form of an RPM package. You can deploy these controls to eligible switches in either monitor or protect mode. Live Protect tracks the status and impact of each control, providing visibility through the Cisco Nexus user interface.

- **Protect mode**—Policy actively blocks threat attempts, enforcing protection on the device.
- **Monitor mode**—Policy logs exploit attempts but does not enforce protection.
- **Disable mode**—Disables specific policy on the switch without removing the policy.

Prerequisites

- Live Protect requires either connectivity from Nexus Dashboard to Cisco Intersight or a manual

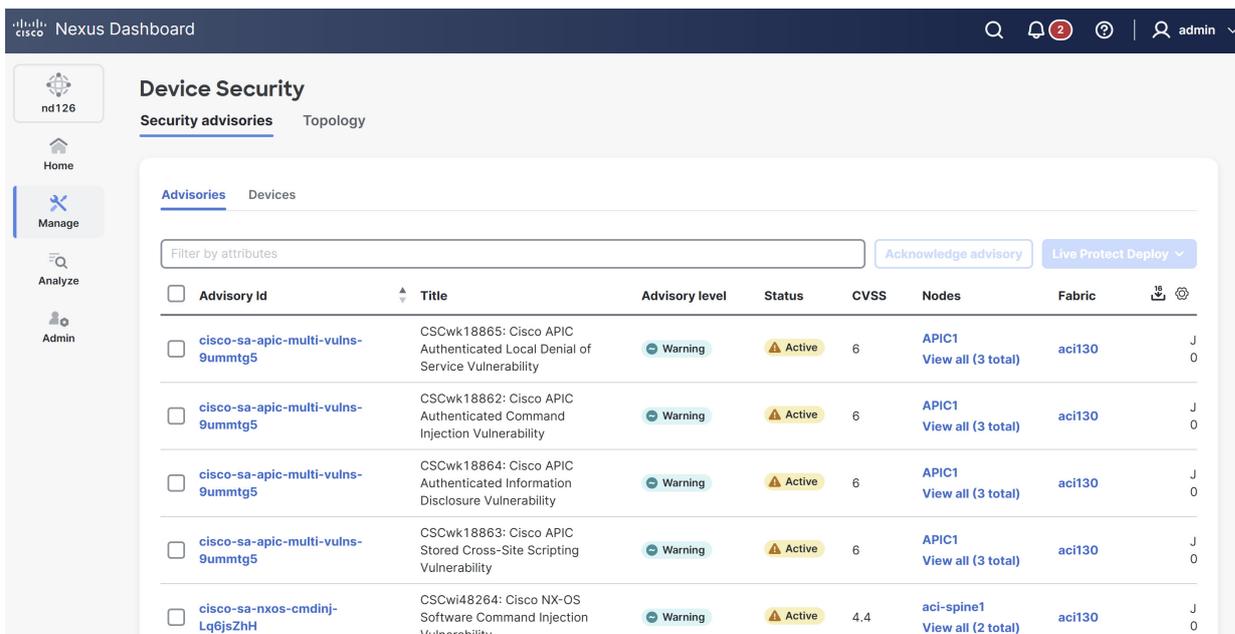
upload of the security advisory metadata using the air-gapped process. Ensure you provide one of these methods to fetch the latest security advisory metadata.

- Ensure that telemetry is enabled and operational on all relevant devices.
- Ensure that you enable **Live Protect** on devices.

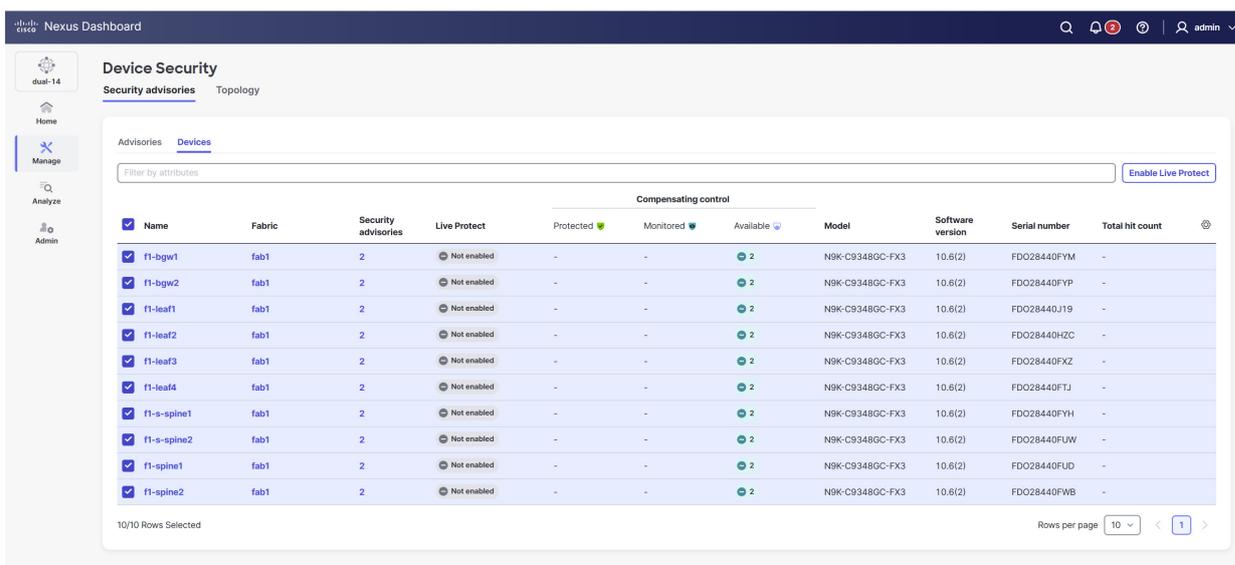
Follow these steps to enable Live Protect.

1. Navigate to **Manage > Device Security**.

The **Device Security** page displays.



2. Under the **Security advisories** tab, click the **Devices** tab.



3. Locate devices with a **Live Protect** status of **Not enabled**.

4. Choose device(s) you want to include.

5. Click **Enable Live Protect**.

Live Protect workflow

The Live Protect workflow guides you through mitigating security advisories on eligible Nexus 9000 Series switches. It includes detecting advisories, assessing device impact, deploying compensating controls, monitoring status, and clearing advisories after software updates. This process helps ensure your network remains protected from active threats with minimal operational disruption.

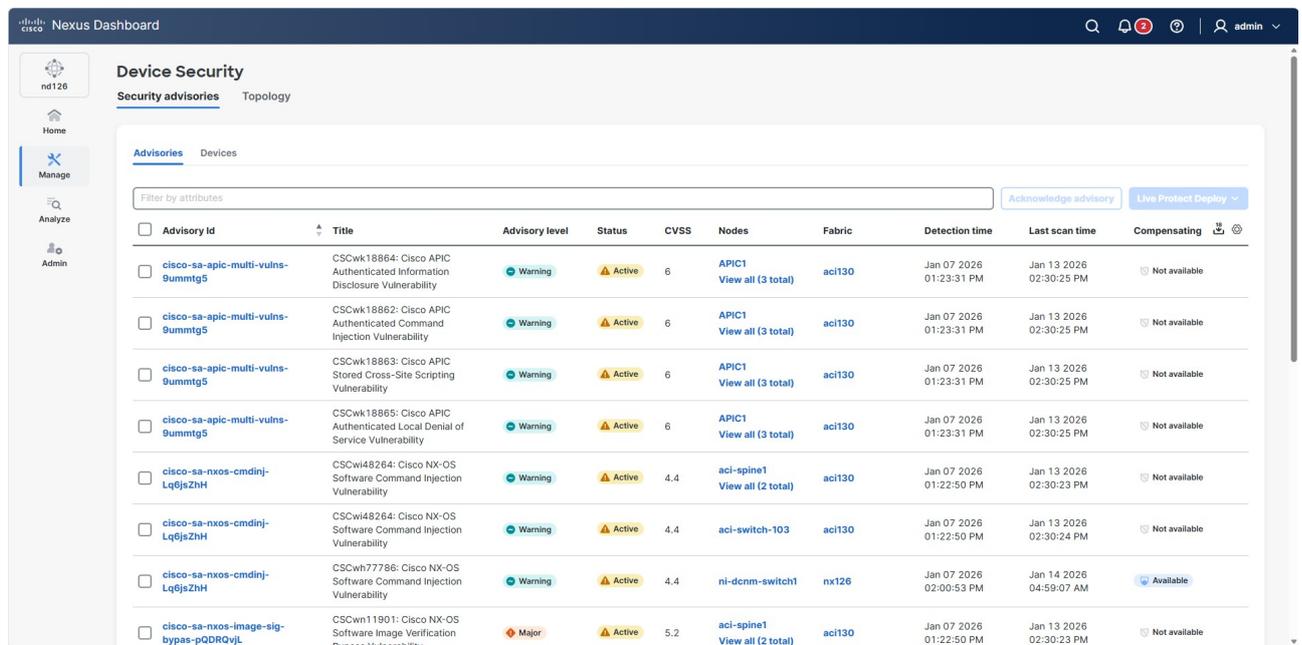
1. **Detect advisories:** Nexus Dashboard identifies active security advisories affecting your managed devices.
2. **Assess impact:** Review the devices impacted by advisories and eligible for Live Protect in the **Security advisories** table.
3. **Deploy compensating control:** Choose the advisory and impacted devices. Choose **Monitor** (observe only) or **Protect** (block exploits) mode, then deploy the control.
4. **Monitor status:** Track deployment progress, policy status, and exploit hit counts directly in Nexus Dashboard.
5. **Upgrade and clear:** When a software fix becomes available, upgrade your devices. Nexus Dashboard automatically clears the advisory and removes the compensating control.

Deploy Live Protect

Follow these steps to deploy the Live Protect.

1. Navigate to **Manage > Device Security** to view all the security advisories.

The **Device Security** page displays. For information, see [Advisories](#).



Advisory Id	Title	Advisory level	Status	CVSS	Nodes	Fabric	Detection time	Last scan time	Compensating
<input type="checkbox"/> cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18864: Cisco APIC Authenticated Information Disclosure Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	Jan 07 2026 01:23:31 PM	Jan 13 2026 02:30:25 PM	Not available
<input type="checkbox"/> cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18862: Cisco APIC Authenticated Command Injection Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	Jan 07 2026 01:23:31 PM	Jan 13 2026 02:30:25 PM	Not available
<input type="checkbox"/> cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18863: Cisco APIC Stored Cross-Site Scripting Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	Jan 07 2026 01:23:31 PM	Jan 13 2026 02:30:25 PM	Not available
<input type="checkbox"/> cisco-sa-apic-multi-vulns-9ummtg5	CSCwk18865: Cisco APIC Authenticated Local Denial of Service Vulnerability	Warning	Active	6	APIC1 View all (3 total)	aci130	Jan 07 2026 01:23:31 PM	Jan 13 2026 02:30:25 PM	Not available
<input type="checkbox"/> cisco-sa-nxos-cmdinj-Lq6jsZH	CSCwi48264: Cisco NX-OS Software Command Injection Vulnerability	Warning	Active	4.4	aci-spine1 View all (2 total)	aci130	Jan 07 2026 01:22:50 PM	Jan 13 2026 02:30:23 PM	Not available
<input type="checkbox"/> cisco-sa-nxos-cmdinj-Lq6jsZH	CSCwi48264: Cisco NX-OS Software Command Injection Vulnerability	Warning	Active	4.4	aci-switch-103	aci130	Jan 07 2026 01:22:50 PM	Jan 13 2026 02:30:24 PM	Not available
<input type="checkbox"/> cisco-sa-nxos-cmdinj-Lq6jsZH	CSCwh77786: Cisco NX-OS Software Command Injection Vulnerability	Warning	Active	4.4	ni-dcnm-switch1	nx126	Jan 07 2026 02:00:53 PM	Jan 14 2026 04:59:07 AM	Available
<input type="checkbox"/> cisco-sa-nxos-image-sig-bypass-pQDRQvJL	CSCwn11901: Cisco NX-OS Software Image Verification Bypass Vulnerability	Major	Active	5.2	aci-spine1 View all (2 total)	aci130	Jan 07 2026 01:22:50 PM	Jan 13 2026 02:30:23 PM	Not available

2. Under the **Advisories** tab, identify a security advisory that has the **Compensating control** status as **Available**.

Following are the **Compensating control** statuses.

- **Protected**—All impacted devices have control in protection mode.
- **Monitoring**—All impacted devices have control in monitoring mode.
- **Partially applied**—Some devices are protected, others are not.
- **Available**—Control exists but not deployed.
- **Not available**—No control exists.

3. Click the check box next to the **Advisory ID**.

4. From the **Live Protect Deploy** drop-down list, choose **Protect Mode**.

The advisory details page displays.

The screenshot shows the Cisco Nexus Dashboard interface for a security advisory. The main heading is "CSCwh77786: Cisco NX-OS Software Command Injection Vulnerability".

What's wrong?

Cisco NX-OS Software Command Injection Vulnerability. For more information, please visit <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh77786>

Advisory level: Warning (CVSS 4.4)

Status: Active (Last scan time: Jan 23, 2026, 07:09:48 PM)

Fabric	Category	Devices/Nodes	Detection time
nx126	Security	ni-dcnm-switch1	Jan 23 2026 07:09:48 PM

What's the impact? 1 device

Filter by attributes

<input checked="" type="checkbox"/> Name	Fabric	Device role	Software version	Live Protect	Compensating control
<input checked="" type="checkbox"/> ni-dcnm-switch1	nx126	leaf	10.6(2)	Enabled	Not available

Buttons: Cancel, Deploy Protect mode

5. Under **What's the impact**, click **Deploy Protect mode**.

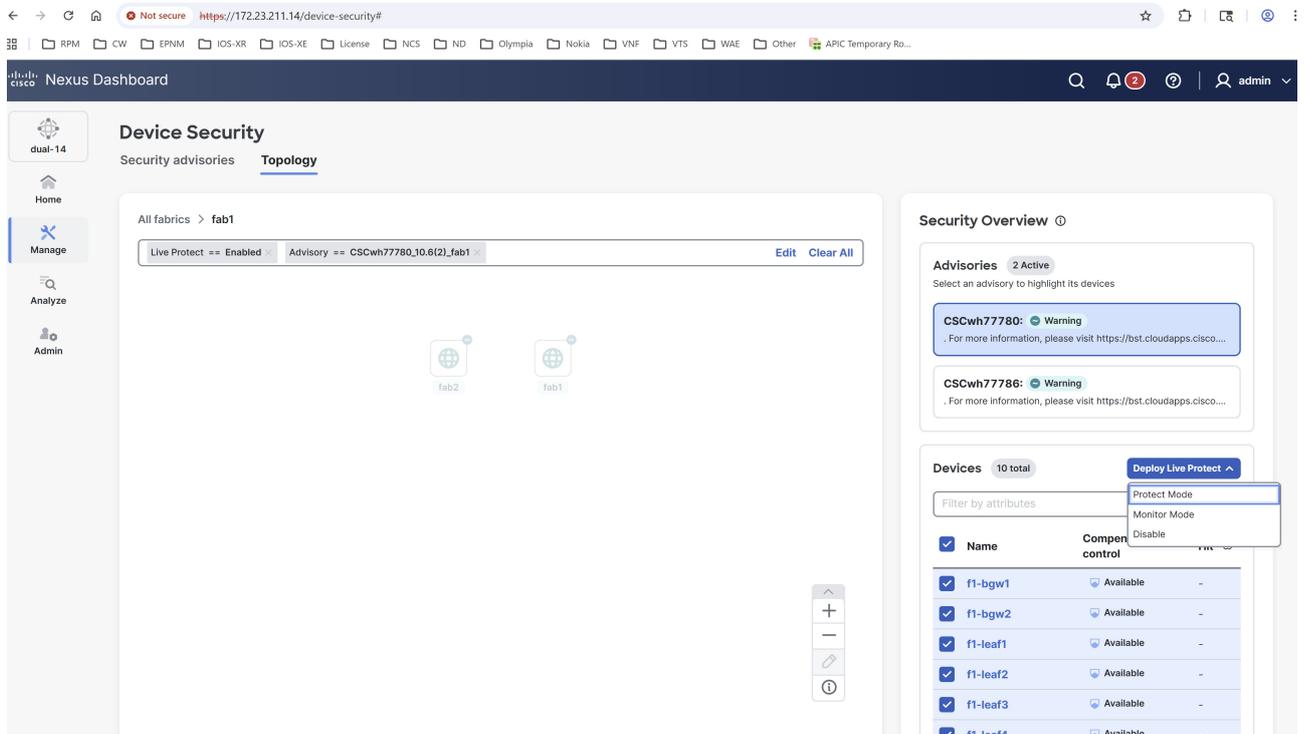
The status of the advisory changes to **Protected** in the **Security advisories** table.

You can view the following statuses for the security advisories.

- **Active**—No compensating control applied (Red).
- **Protected**—All impacted devices have a compensating control in protection mode (Green).
- **Partially protected**—Some devices protected, others monitoring or not deployed (Orange).
- **Monitoring**—Nexus Dashboard deploys a compensating control in monitor mode on all impacted devices, logging threat attempts without enforcing protection.
- **Cleared**—Displayed when advisory is cleared (SW version upgrade).

6. In the **Device Security** page, click the **Topology** tab.

7. Double-click the fabric to view the switches with security advisories.



8. In the **Security Overview** pane on the right, under **Advisories**, you can view the current advisories for the switch and under **Devices**, you can view the affected devices.
9. Choose the advisory.
10. Click the box next to **Name** to choose devices.
11. From the **Deploy Live Protect** drop-down list, choose **Protect Mode**.

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017–2026 Cisco Systems, Inc. All rights reserved.

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<https://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883