



cisco Identify Network Security Advisories User Guide

[Home](#) » [Cisco](#) » cisco Identify Network Security Advisories User Guide 



Identify Network Security Advisories



User Guide

Contents

- [1 Security Advisories Overview](#)
- [2 Prerequisites](#)
- [3 View Security Advisories](#)
- [4 Schedule a Security Advisories Scan](#)
- [5 Hide and Unhide Devices from an Advisory](#)
- [6 Hide and Unhide Advisories from a Device](#)
- [7 Add Notification for a New Security Advisory KB](#)
- [8 View Security Advisories in Inventory Page](#)
- [9 Add a Match Pattern](#)
- [10 Define AND/OR for the Match Pattern](#)
- [11 Edit the Match Pattern](#)
- [12 Delete the Match Pattern](#)
- [13 Documents / Resources](#)
- [14 Related Posts](#)

Security Advisories Overview

The Cisco Product Security Incident Response Team (PSIRT) responds to Cisco product security incidents, regulates the Security Vulnerability Policy, and recommends [Cisco Security Advisories and Alerts](#). The Security Advisories tool uses these recommended advisories, scans the inventory within Cisco DNA Center, and finds the devices with known vulnerabilities.

Prerequisites

To use the Security Advisories tool, you must install the Machine Reasoning package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).

If you log in to Cisco DNA Center as an Observer, you cannot view the Security Advisories tool in the home page.

View Security Advisories


Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

If you are launching the Security Advisories page for the first time, click Scan Network.

Cisco DNA Center uses the knowledge base to identify security issues and improve automated analysis. We recommend that you update the knowledge base on a regular basis to view the latest security advisories.

- a) In the Cisco DNA Center GUI, click the Menu icon () and choose System > Settings > Machine Reasoning Knowledge Base.
- b) Click Import, or click Download to download the latest available knowledge base, and then click Import.
- c) Click the AUTO UPDATE toggle button to subscribe to automatic updates.

Note

- The security advisories dashboard shows security advisories published by Cisco that may affect devices on your network based on the software image currently installed. A further analysis of the configuration, platform details, or other criteria is required to determine if a vulnerability is actually present.
- The Overview tab with its security advisories graphic displays the distribution percentage of impact on the network, such as Critical, High, Medium, Low, or Informational.
- Security advisories scanning is only available for routers and switches that are running the minimum supported

software version. For more information, see [Cisco DNA Center Supported Devices](#).

- The security advisories displayed are subject to the [Cisco Security Vulnerability Policy](#).

The following table describes the information that is available.

Column	Description
Advisory ID	ID of the security advisories found in the topology. Click the ID to go to the respective advisory web page.
Advisory title	Name of the security vulnerability advisory applicable to the network devices.
CVSS score	Score evaluated based on the Common Vulnerability Scoring System (CVSS) model.
Impact	Impact of the vulnerability on the network.
CVE	Common Vulnerabilities and Exposures (CVE) identifier for the vulnerability.
Devices	The number of devices impacted by the vulnerability. Click the number to view the devices that may be vulnerable based on this specific advisory, and upgrade the devices as needed.
Match Type	Indicates whether the vulnerability was detected based on Image Version match or Configuration match.
Known since (days)	The number of days since the vulnerability was discovered.
Last updated	The date when the advisory was last updated.

Step 3

Click the Devices tab to view the number of advisories applicable to each device.

a) Click the number of advisories to view all that match the device.

b) Click the topology icon in the top-right corner to view the device topology. You can click a device in the topology to view all advisories that match the device.

A lock icon next to the device indicates that there are one or more advisories applicable to the device.

Step 4

Click Scan Network at any time to refresh the results displayed.

Schedule a Security Advisories Scan

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

Click Scan Network.

The Scan Network window appears.

Step 3

To scan the security advisories immediately, click the Now radio button and click Start.

Step 4

To schedule the scan for a later date and time, click the Later radio button and specify the date and time.

Step 5

Use the Time Zone drop-down list to schedule the scan according to a specific time zone.

Step 6

Choose the recurrence option: None (the default), Daily, or Weekly.

Step 7

In the Run at Interval field, enter the number of days or weeks for the recurrence of the scan.

Step 8

(Optional) Check the Set Schedule End check box to schedule an end date and number of occurrences.

a) To schedule a scan end date, click the End Date radio button and define the date and time.

b) To define the number of scan occurrences, click the End After radio button.

Step 9

Click Schedule.

Step 10

In the Cisco DNA Center GUI, click the Menu icon () and choose Activity > Tasks and confirm the schedule and recurrence of the scan.



Note

In Cisco DNA Center releases earlier than 2.1.1.x, you have the ability to opt in or out of telemetry that Cisco collects. When you opt in, we collect your cisco.com ID, system telemetry, feature usage telemetry, network device inventory, and license entitlement. Telemetry is not application or feature specific; the disclosure of telemetry is for all of Cisco DNA Center. In Cisco DNA Center 2.1.1.x and later, telemetry collection is mandatory. The telemetry is designed to help the development of features that you use. See the [Cisco DNA Center Data Sheet](#) for a more expansive list of data that we collect.

When a security advisory scan runs, the following telemetry data is collected:

- Whether automatic update of knowledge packages has been set up.
- Whether recurring scanning and recurring reports have been set up.
- The number of reports that have been run.
- The number of devices with a security advisory match based on software version and configuration.
- The number of thumbs up/thumbs down votes, per scan.
- The manual configurations entered as a search, and the associated advisory.
- The number of advisory matches by software version and configuration, including product family.
- The number of devices based on other categories (zero advisories, unknown, and unsupported).
- The number of successful, failed, and terminated scans.
- The average scan time.

Hide and Unhide Devices from an Advisory

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

If you are launching the Security Advisories page for the first time, click Scan Network.

Step 3

In the Scan Network window, choose Now, and then click Start.

Step 4

To hide the devices from an advisory, do the following:

a) From the Focus drop-down list, choose Advisories.

b) In the Devices column, click the devices count that corresponds to the advisory for which you want to hide the devices.

The Active tab shows the number of devices for which these advisories are issued.

c) Choose the devices that you want to hide and click Suppress Device.

The hidden devices can be viewed in the Suppressed tab.

d) Close the advisory window and view the change in the device count for this advisory.


Step 5

To restore the devices to an advisory, do the following:

- a) From the Focus drop-down list, choose Advisories.
 - b) In the Devices column, click the devices count that corresponds to the advisory for which you want to unhide the devices.
 - c) Click the Suppressed tab to view the hidden devices.
 - d) Choose the devices that you want to unhide and click Mark as Active.
- The restored devices can be viewed in the Active tab.
- e) Close the advisory window and view the change in the device count for this advisory.

Hide and Unhide Advisories from a Device

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

If you are launching the Security Advisories page for the first time, click Scan Network.

Step 3

In the Scan Network window, choose Now, and then click Start.

Step 4

To hide the advisories for a device, do the following:

- a) From the Focus drop-down list, choose Devices.
- b) In the Advisories column, click the advisories count that corresponds to device for which you want to hide the advisories.

The Active tab shows the number of advisories issued for this device.

- c) Choose the advisories that you want to hide and click Suppress Advisory.

The hidden advisories can be viewed in the Suppressed tab.

- d) Close the device window and view the change in the advisory count for this device.

Step 5

To restore the advisories for a device, do the following:

- a) From the Focus drop-down list, choose Devices.
- b) In the Advisories column, click the advisories count that corresponds to the device for which you want to unhide the advisories.
- c) Click the Suppressed tab to view the hidden advisories.
- d) Choose the advisories that you want to unhide and click Mark as Active.

The restored advisories can be viewed in the Active tab.

- e) Close the device window and view the change in the advisories count for this device.

Add Notification for a New Security Advisory KB

A security advisory Knowledge Bundle (KB) uses a Machine Reasoning Engine (MRE) to scan the network.

You can configure Cisco DNA Center to notify you when a new security advisory Knowledge Bundle (KB) is available. After you enable notifications, Cisco DNA Center displays a visual notification and actionable alert whenever a new security advisory Knowledge Bundle (KB) is available.

The following procedure explains how to add notifications for a new security advisory knowledge bundles:

Before you begin

- You must install the Cisco DNA Center core package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- You must install the Machine Reasoning (MRE) package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- The following containers must be present in your system:
 - cnsr-reasoner
 - cloud connectivity/download

Step 1

In the Cisco DNA Center GUI, click the notification icon located at the top-right corner. From the drop-down menu, select the gear icon to view the notification preferences.

Step 2

In the My Profile and Settings window, enable the security advisory notification by choosing the Security Advisories option.

Step 3

Click Save.

Step 4

In the Machine Reasoning Engine window, click the Download Latest link to download the latest knowledge bundle.

Step 5

Review and update the Knowledge Base settings.

Step 6

In the Security Advisory Settings section, choose the recurrence option: None (default), Daily, or Weekly.

Step 7

In the Cisco DNA Center GUI, choose Notification Center > Go to Security Advisories to view the Security Advisories tool page directly.

Step 8

Rescan the network with the newly downloaded security advisories. For more information, see Schedule a Security Advisories Scan, on page 3.

View Security Advisories in Inventory Page

The Cisco DNA Center security focus view allows you to view the list of security advisories for your devices, based on the data retrieved from the previous security scan. The device data that you retrieve from the Security Advisories tool is now displayed in the inventory page.

Use the following procedure to view the security advisories column in the inventory page:

Before you begin

- You must install the Cisco DNA Center core package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- You must install the Machine Reasoning package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2


Click Scan Network.

The Scan Network window appears.

Step 3

To scan the security advisories immediately, click the Now radio button and click Start. For more details, refer Schedule a Security Advisories Scan.

Step 4

In the Cisco DNA Center GUI, click the Menu icon () and choose Provision > Devices > Inventory.

Step 5

From the FOCUS: Inventory drop-down menu, select Security.

The Advisories column is displayed in the Inventory table.

Step 6


In the Device Details page, select a device and view the advisories data.

Step 7

Click Manage All to navigate to Security Advisories tool.

Add a Match Pattern

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

If you are launching the Security Advisories page for the first time, click Scan Network.

Step 3

In the Scan Network window, choose Now, and then click Start.

Step 4

Choose an advisory and in the Match Type column, click Add match pattern.

Step 5

In the Add Configuration Match Pattern window, enter the condition to match with devices in the CONDITIONS text box.

Step 6

Click Save.

The match pattern is added to the advisory.

Step 7

Click Scan Network to check the number of devices that match with the match pattern.

Define AND/OR for the Match Pattern

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

If you are launching the Security Advisories page for the first time, click Scan Network.

Step 3

In the Scan Network window, choose Now, and then click Start.

Step 4

Choose an advisory and in the Match Type column, click Add match pattern.

Step 5

In the Add Configuration Match Pattern window, do the following:

- a) In the CONDITIONS text box, enter a condition and then click the Add icon.
- b) From the drop-down list, choose AND or OR and then enter the next condition.
- c) If you want to delete a condition, click the Remove icon.
- d) Click Save.

The match pattern is added to the advisory.

Step 6

Click Scan Network to check the number of devices that match the match pattern.

Edit the Match Pattern

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

If you are launching the Security Advisories page for the first time, click Scan Network.

Step 3

In the Scan Network window, choose Now, and then click Start.

Step 4

Choose an advisory that already has a match pattern and in the Match Type column, click Edit match pattern.

Step 5

In the Edit Configuration Match Pattern window, enter the condition to match with devices in the CONDITIONS text box.

Step 6

Click Save.

The match pattern is changed.

Step 7

Click Scan Network to check the number of devices that match the match pattern.

Delete the Match Pattern

Step 1

In the Cisco DNA Center GUI, click the Menu icon () and choose Tools > Security Advisories.

Step 2

If you are launching the Security Advisories page for the first time, click Scan Network.

Step 3

In the Scan Network window, choose Now, and then click Start.

Step 4

Choose an advisory that already has a match pattern and in the Match Type column, click Edit match pattern.


Step 5

In the Edit Configuration Match Pattern window, click Delete.

The match pattern is deleted.

Identify Network Security Advisories

Documents / Resources

	<p>cisco Identify Network Security Advisories [pdf] User Guide</p> <p>Identify Network Security Advisories, Network Security Advisories, Identify Security Advisories, Security Advisories, Advisories</p>
---	--