Identify Network Security Advisories

- Security Advisories Overview, on page 1
- Prerequisites, on page 1
- View Security Advisories, on page 2
- Schedule a Security Advisories Scan, on page 3
- CLI Commands Invoked for Security Advisories, on page 4
- Rescan the Network to Identify Security Advisories, on page 5
- Hide and Unhide Devices from an Advisory, on page 5
- Hide and Unhide Advisories from a Device, on page 6
- Add Notification for a New Security Advisory KB, on page 6
- View Security Advisories in the Inventory, on page 7
- Add a Match Pattern, on page 8
- Define AND/OR for the Match Pattern, on page 8
- Edit the Match Pattern, on page 9
- Delete the Match Pattern, on page 9

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 Catalyst 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 Catalyst Center Administrator Guide.

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

View Security Advisories

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Security Advisories**.

Step 2 If you are launching the **Security Advisories** window for the first time, click **Scan Network**.

Catalyst 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) From the top-left corner, click the menu icon and choose **System** > **Settings** > **Machine Reasoning Engine**.
b) Either click **Import** or click **Download Latest** to download the latest available knowledge base. After the download, click **Import**.
c) Click the **AUTO UPDATE** toggle button to subscribe to automatic updates.

Note Click the **here** link in the banner that appears at the top, to create new trial that provides access to customized field notices based on device configuration.

Step 3 The **ADVISORIES** area displays the distribution percentage of impact on the network, such as **Critical**, **High**, **Medium**, **Low**, **Informational**, or **Unknown**.

Step 4 Scans are performed on the devices based on the licenses associated against each device. In the **SCAN CRITERIA** area, you must follow the following order to match advisories against your devices:

- **Software Version**: Scans are performed on devices based on the software version with **Essentials** license.
- **Custom**: Scans are performed on devices based on the software version and the custom configuration entered for an advisory (if any) against the device running configuration with **Advantage** license.
- **Advanced**: Scans are performed on devices based on the software version, configuration, and operations data on devices with **Cisco CX Cloud Success Track** entitlements.

  The license entitlements are not enforced in trial period and all devices are scanned at the **Advanced** level.

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.
- Security advisories scanning is only available for routers and switches that are running the minimum supported software version. For more information, see the Catalyst Center Compatibility Matrix.
- 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 network. 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.

Column	Description
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 the **Image Version** match or the **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 5 The **FAILED DEVICES** area displays the information about the device scan scheduled for a later date and time.

Note The **FAILED DEVICES** area appears only when there is a failed device in a scan and system schedules a scan automatically.

Step 6 In the **Advisories** table click **All** tab to list all the advisories.

Step 7 In the **Advisories** table click **Affecting Devices** tab to view the advisories based on affecting devices.

The **Devices** table list the devices based on **Device Name**, **Device Family**, **Device Series**, **IP Address**, **Advisories**, **Advisories (Suppressed)**, **Platform**, **Image Version**, **Scan Status**, **Scan Criteria**, **Site**, and **Reachability**.

Step 8 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.

The **Fixed Version** column shows the version in which the advisories are fixed. You can remove the advisory on your device by upgrading to the version mentioned in this column.

Step 9 Click **Re-scan Network** to run the scan the network again.

To re-scan the network to identify security advisories based on automated config scan, see Rescan the Network to Identify Security Advisories, on page 5.

Schedule a Security Advisories Scan

Step 1 From the top-left corner, 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 From the top-left corner, click the menu icon and choose **Activities** > **Tasks** and confirm the schedule and recurrence of the scan.

Note In Catalyst 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 Catalyst Center. In Catalyst 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 Catalyst 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.

CLI Commands Invoked for Security Advisories

Catalyst Center collects network device configuration and operational data by running CLI commands on network devices, and then sends the information to the CX Cloud to be processed for exposure to potential security advisories or bugs. Catalyst Center invokes the following CLI commands for security advisories:

- **show inventory**
- **show running-config**

- **show version**

Rescan the Network to Identify Security Advisories

The following procedure describes how to rescan the network to identify security advisories based on automated configuration scan.

Before you begin

You must enable the Cisco CX Cloud service. For more information, see **Update the Machine Reasoning Knowledge Base** in the *Cisco Catalyst Center Administrator Guide*.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Security Advisories** > **Advisories**.

Step 2 Click **Re-Scan Network** to start the network scan again.

Step 3 To rescan the security advisories immediately, click the **Now** radio button and click **Start**.

Step 4 To schedule the rescan for a later date and time, click the **Later** radio button and specify the details. For information, see Schedule a Security Advisories Scan, on page 3.

In the **Device** table, the **Advisories** column is updated with the number of advisories.

- The Catalyst Center network rescan sends the running config of devices along with other details, such as platform details and the CX Cloud software version. The information is processed and sent back to Catalyst Center. The Machine Reasoning Engine (MRE) running on Catalyst Center maps the advisories against the devices provided by the Cisco CX Cloud.
- If Catalyst Center cannot determine the correct license level for a given device, the security advisory scan falls back to scan by software version.

Hide and Unhide Devices from an Advisory

Step 1 From the top-left corner, 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 From the top-left corner, 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 Catalyst Center to notify you when a new security advisory KB is available. After you

enable notifications, Catalyst Center displays a visual notification and actionable alert whenever a new security advisory KB is available.

The following procedure explains how to add notifications for new security advisory KBs:

Before you begin

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

Step 1 Click the notification icon in the top-right corner of the Catalyst Center GUI. 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 Choose **Notification Center** > **Go to Security Advisories** to view the Security Advisories tool window 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 the Inventory

The Catalyst Center security focus view lists the 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 displayed in the **Inventory** window.

Use the following procedure to view the security advisories:

Before you begin

- You must install the Catalyst Center core package. See Download and Install Packages and Updates in the *Cisco Catalyst Center Administrator Guide*.
- You must install the Machine Reasoning package. See Download and Install Packages and Updates in the *Cisco Catalyst Center Administrator Guide*.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Security Advisories**.

Step 2 Click **Scan Network**.

Step 3 To scan the security advisories immediately, click the **Now** radio button and click **Start**.

Step 4 From the top-left corner, click the menu icon and choose **Provision** > **Network Devices** > **Inventory**.

Step 5 From the **FOCUS: Inventory** drop-down menu, choose **Security**.
The **Advisories** column is displayed in the **Inventory** table.

Step 6 In the **Device Details** window, select a device and view the advisories data.

Step 7 Click **Manage All** to navigate to the **Security Advisories** tool.

Add a Match Pattern

Step 1 From the top-left corner, 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 From the top-left corner, 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 From the top-left corner, 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 From the top-left corner, 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.