



Maintain and Monitor Cisco Cyber Vision

- [Monitored presets, on page 1](#)
- [Center Shutdown/Reboot, on page 7](#)
- [Upgrade with a Combined Update File, on page 7](#)
- [Configure syslog, on page 9](#)
- [Import/Export, on page 10](#)
- [Knowledge DB, on page 10](#)
- [Certificate Fingerprint, on page 11](#)
- [Cisco Cyber Vision Telemetry, on page 11](#)
- [Reset to Factory Defaults, on page 11](#)
- [Snort, on page 12](#)
- [Risk Score, on page 16](#)
- [Extensions, on page 16](#)

Monitored presets

To monitor your network using Cisco Cyber Vision Center, you must set up monitored presets. A monitored preset is any preset that is monitored against a baseline.

To view the presets in your Center, from the main menu, choose **Explore**. Click a preset to view the network data that matches the preset definition. You can also export the data as a PDF file.

Presets

A preset is a customizable view that allow you to focus on specific subsets of network data. A preset filters network data based on defined criteria and gives you a focused view of an organizational network for quick, meaningful analysis.

The parameters that you can configure for a preset include:

- Time
- Risk score range
- Networks, by IP subnets or VLAN IDs
- Device tags
- Activity tags

- Groups
- Sensors

Baseline

A baseline is a snapshot of a preset. It is the reference point against which network behavior is periodically compared to detect network deviations or anomalies by identifying changes such as new devices, altered communications, or unusual activities that may indicate security issues or operational problems.

Multiple baselines for a preset

You can create multiple baselines for a preset to monitor in various known states of your network.

For example, network activity baselines may differ for weekdays and weekends. Create two baselines for these scenarios, and activate the baseline that would be an accurate monitor for your network on any given day.

To activate one of multiple baselines for a monitored preset, see [Configure monitored presets, on page 5](#)

Default presets

Some presets categories are available by default. You can make changes to the default presets and save the modified settings as new copies, but you cannot modify the default presets.

Table 1: Default presets available in Cisco Cyber Vision Center

Preset category	Presets available
Basics	<ul style="list-style-type: none"> • All data • Essential data • Active Discovery activities
Asset management	<ul style="list-style-type: none"> • OT devices • IT devices • IT infrastructure devices • All Microsoft Windows systems • All controllers
Control systems management	<ul style="list-style-type: none"> • OT activities • Control system activities • Process control activities

Preset category	Presets available
IT communication management	<ul style="list-style-type: none"> • IT activities • Web activities • Email activities • File activities • Microsoft activities
Security	<ul style="list-style-type: none"> • DNS activities • Remote procedure call activities • Remote access • Insecure activities • Encrypted activities • Authentication activities
Network management	<ul style="list-style-type: none"> • IT infrastructure activities • IT technical activities • IPv6 communications • Multicast traffic only • Broadcast traffic only

Create categories

The **Explore** page contains many default categories, including one named **My preset** in which you can place any preset that you create. You can create more categories to better organize your presets.

Procedure

-
- Step 1** From the main menu, choose **Explore**.
- Step 2** Click **New Category**.
- Step 3** Enter a name for the category.
- Step 4** (Optional) Select the presets you want to place in this category.
- Step 5** Click **Create**.
-

What to do next

After you create a category, you can add a preset to the category at any time. To add a preset to a category:

1. Click the edit button for the category.
2. In the **Presets** field, select the preset you want to add to the category.

Create presets

Procedure

- Step 1** From the main menu, choose **Explore**.
- Step 2** Click **New Preset**.
- Step 3** To create a preset:
- a) Enter a name for the preset.
 - b) (Optional) Enter a description for the preset.
 - c) Choose a category to place your preset in.
 - d) Click **Create**.
- Step 4** Select the newly created preset from the **Explore** page.
- Step 5** In the left pane, define each criteria category. For each criteria parameter:
- Click the check box once to include the parameter
 - Click the check box twice to exclude the parameter
- Step 6** Click **Save**.
-


What to do next

After you create a preset, you can edit it at any time and update any criteria setting. These criteria settings management options are also available to you in the **Criteria** section of a preset:

- **Select all:** Include all the criteria parameters available in your Center.
- **Reject all:** Exclude all the criteria parameters available in your Center.
- **Default:** Reset all the selections such that no parameter is included or excluded.

Create baselines

Procedure

- Step 1** From the main menu, choose **Explore**.
- Step 2** To create a baseline, you can create a baseline from a preset icon () from two paths:
- The preset dashlet listed on the **Explore** page.

- The preset details page that is displayed when you click a preset dashlet.

Step 3 Enter a name and description for the preset.

Step 4 Click **Create**.

To view the newly created baseline, from the main menu, choose **Monitor**. All the baselines that are available in your Center are displayed in this page, categorized by the preset for which they were created.

Configure monitored presets

Before you begin

A monitored preset is a preset with a baseline. See [Create baselines, on page 4](#).

In this task, you:

- Define the interval for checking the network against a monitored preset
- Choose the type of event differences you want to view alerts for

Any differences in the selected baseline and the current network status result in alerts that can review and acknowledge.

Procedure

Step 1 From the main menu, choose **Monitor**.

Step 2 For the monitored presets you want to configure, click the vertical ellipsis icon and choose **Monitored preset settings**.

Step 3 For the monitored preset:

- a) Enter a monitoring interval, in seconds.
 - b) If you have created more than one baseline for the preset, in the **Monitored baseline** field, choose the preset you want to activate.
 - c) In the **Events severity** section, choose the severity level for the alerts generated for each event type.
 - d) In the **Advanced settings** section, choose the component, property, and activity differences for which you want to view alerts.
 - e) Click **OK**.
-

Manage monitored preset differences

This task guides you through acknowledging or reporting a single difference entry.

- To mark a reported event as normal for the network, acknowledge the entry.
- To identify a reported event as an anomaly and create an event in Cisco Cyber Vision Center, report the entry.

After you select a baseline in the **Monitor** page, you have two bulk management options:

- To acknowledge all differences across the components and activities, click the blue tick icon in the left pane
- To acknowledge or report multiple, specific differences in the components or activities listings, select the entries and click **Acknowledge Selection** or **Report Selection**.

Procedure

Step 1 From the main menu, choose **Monitor**.

Step 2 In the **What changed** area, for a monitored preset, click the baseline you want to examine.

Step 3 You can view the differences reported based on:

- New components
- New activities

Step 4 To view the communication flows that may have caused the reported difference, click **Investigate with flows**.

Step 5 In the components list, click an entry to view the details. You can choose from four options:

Action	Definition
Acknowledge Component	<p>You can enter a message explaining your choice for reference. You have two acknowledgement options:</p> <ul style="list-style-type: none"> • Acknowledge and include: Retain this alert and receive new alerts if something new happens with this component or activity. • Acknowledge and keep warning: Delete this alert and receive new alerts if the same event repeats.
Ack. with related activities	<p>You can enter a message explaining your choice for reference.</p> <p>Click Acknowledge and include to retain the alert and receive alerts for any new events for the component and its activities.</p>
Report component	<p>You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again.</p> <p>Click Report component to create an event report for this anomaly.</p>
Show details	View device tags and properties.

Step 6 In the activities list, click an entry to view the details. You can choose from three options:

Action	Definition
Acknowledge activity	<p>Acknowledge the reported event as normal for the network.</p> <p>You can enter a message explaining your choice for</p>

Action	Definition
	<p>reference. Two acknowledgement options are available to you:</p> <ul style="list-style-type: none"> • Acknowledge and include: Retain this alert and receive alerts if something new happens with this component or activity. • Acknowledge and keep warning: Delete this alert and receive a new alert if the same event repeats.
Report activity	<p>You must enter a message explaining your choice for reference. You continue to receive alerts if the anomaly is detected again.</p> <p>Click Report activity to create an event report for this anomaly.</p>
Show details	View activity tags and variables.

Center Shutdown/Reboot

You can trigger a safe shutdown and reboot of the **Center**.

Use **Reboot** to fix a minor bug, such as a system overload.

To access the **Center shutdown/reboot** page, choose **Admin > System** from the main menu.

Upgrade with a Combined Update File

Version releases include a **Cisco Cyber Vision Manual Update Center** update file. To access this file, choose **Admin > System** from the main menu.



Important Rolling back to an older Cisco Cyber Version version is not supported.

Requirements

- A combined update to retrieve from cisco.com.

Use the SHA512 checksum provided by Cisco to verify that the file you just downloaded is healthy.

Windows users:

Procedure

Step 1 Retrieve the Cisco Cyber Vision combined update from cisco.com.

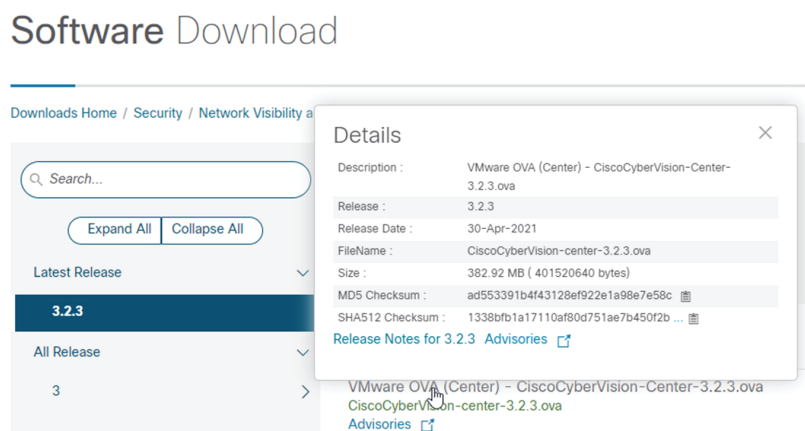
Step 2 Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List

```
PS C:\Users\ > Get-FileHash .\Downloads\CiscoCyberVision-center-3.2.3.ova -Algorithm SHA512 | Format-List

Algorithm : SHA512
Hash      : 1338BF81A17110AF80D751AE7B450F2B29CCB4C854F550F3888E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
          : 18622E48088E889E94DB16
Path      : C:\Users\ \Downloads\CiscoCyberVision-center-3.2.3.ova
```

Step 3 In cisco.com, hover over the file and copy the SHA512 checksum.



Step 4 Compare both checksums.

- If both checksums are identical, the file is healthy.
- If the checksums do not match, download the file again.
- If the checksums still don't match, please contact Cisco support.

To update the Center and all applicable sensors:

Step 5 Log in to Cisco Cyber Vision.

Step 6 From the main menu, choose **Admin > System**.

Step 7 Click **System update**.

Step 8 Select the update file CiscoCyberVision-update-combined-<VERSION>.dat

Step 9 Confirm the update.

As the Center and sensors update, a holding page appears. When done, click Center **Reboot**. You will be logged out.

Step 10 Log in.

If sensors were offline when the update occurred, repeat the procedure until all sensors update.

Configure syslog

Security Information and Event Management (SIEM):

It is an approach to security management that combines SIM (Security Information Management) and SEM (Security Event Management) into a single security management system.

CEF standard for syslog messages:

You must use the Common Event Format (CEF) standard for syslog configurations in the Cyber Vision Center. Update existing syslog configurations from non-CEF to CEF message formats.

Syslog messages from the Beta UI:

In Cyber Vision Center, the configured syslog server also receives messages from the Cyber Vision Center Beta UI. The syslog messages from the Beta UI contain the key-pair value 'Version Number = 2.0', and syslog notifications are generated for each alert type configured in the Beta UI of the Center.

For more information, see [Syslog notifications for alert types](#).

To add a syslog server:

Procedure

Step 1 From the main menu, choose **Admin > System**.

Step 2 Click **Configure** in the **Syslog configuration** menu.

Step 3 Select **UDP**, **TCP**, or **TCP + TLS** in the **Protocol** field.

Note

Select **TCP + TLS** to secure communications with a syslog collector using a p12 certificate file provided by your SIEM administrator. Use the **Set certificate** button to import it.

Step 4 Enter the **Host**.

Enter the IP address of the SIEM that is reachable from the Administration network interface (for example, eth0) of the Center.

Step 5 Enter the **Port** on the SIEM that receives syslogs.

Step 6 Select **Format**.

- **CEF**: Based on the Common Event Format (CEF) standard, this format sends event messages with a legacy timestamp of one-second precision.
- **CEF Extended Time Precision**: Based on the Common Event Format (CEF) and an extended syslog header, this format sends event messages with a legacy timestamp of microsecond precision.

Step 7 Click **Save configuration**.

Import/Export

Use the System interface to import and export the Cisco Cyber Vision database. To access the **Import/Export** page, choose **Admin > System** from the main menu.

Regularly export the database to back up the industrial network data on Cisco Cyber Vision or if you need to transfer the database to a different **Center**.

Exports database file limitation is up to 2 GB of data. This avoids side effects related to slow database exports. If the database is larger than 2 GB, you get an error message. In this case, connect to the Center using SSH and perform a data dump. Use the command: `sbs-db dump`.

Network data, events, and users are retained, as well as all customizations (e.g., groups, component names).

Only configurations created in Cisco Cyber Vision's GUI persist. If you change **Center**, perform a basic configuration of the Center and then configure Cisco Cyber Vision again. Refer to the corresponding [Center Installation Guide](#).



Note The **Import** process may take one hour for big databases. Refresh the page to check that the import remains active (i.e., no error message).

Knowledge DB

Cisco Cyber Vision uses an internal database which contains a list of recognized vulnerabilities, icons, and threats.



Important To remain protected against vulnerabilities, always update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version.

To update the Knowledge DB:

Procedure

-
- Step 1** Download the latest.db file available from cisco.com.
 - Step 2** From the main menu, choose **Admin > System**.
 - Step 3** Click **Import a Knowledge DB** under the **Knowledge DB** field.
 - Step 4** Select the file and click **Open** to upload the file.

Importing the new database rematches your existing components against any new vulnerabilities and updates the network data.

Certificate Fingerprint

Use the certificate fingerprint to register a **Global Center** with its synchronized centers and vice versa. To access the **Center Fingerprint**, choose **Admin > System** from the main menu. Click the copy icon to copy the **Fingerprint** and enroll your center with a global center.

For more information, refer [the Centers Installation Guides](#).

Cisco Cyber Vision Telemetry

Telemetry monitors your system to provide anonymous diagnostics and usage data, helps us to understand and enhance product usage. Cisco Cyber Vision telemetry data communication occurs as HTTPS traffic through Port 443 with <https://connectdna.cisco.com/>.

Telemetry is enabled by default. To disable this feature, follow these steps:

Procedure

-
- Step 1** From the main menu, choose **Admin > System**.
- Step 2** To disable telemetry, click the **ON** toggle button under the **Telemetry Collection** field. The switch turns **OFF**.
-

Reset to Factory Defaults

Only use **Reset to Factory Defaults** *as a last resort*, after all other troubleshooting attempts fail. Get help from product support.

To access the **Reset**, choose **Admin > System** from the main menu.

A **Reset to Factory Defaults** deletes the following:

- Some Center configuration data elements.
- The GUI configuration (such as user accounts, the setup of event severities, etc.).
- Data collected by the sensors.
- The configuration of all known sensors (such as IP addresses, capture modes, etc.).

Root password, certificates and configurations from the Basic Center configuration persist.

After a **Reset to Factory Defaults** occurs, the GUI refreshes with the installation wizard. See the corresponding [Center Installation Guide](#).

Snort

Snort is a Network Intrusion Detection System (NIDS) software which detects malicious network behavior based on a rule matching engine and a set of rules characterizing malicious network activity. Cisco Cyber Vision can run the Snort engine on both the Center and some sensors. The Center stores the configuration rule files, pushes rules on compatible sensors, and intercepts Snort alerts to display them as events in the Cisco Cyber Vision Center's GUI.

To access the **SNORT** page, choose **Admin > Snort** from the main menu.

Snort is not activated by default on sensors, so you must first [enable IDS in the Sensor Explorer page](#).

It is available on the following sensor devices:

- The Cisco IC3000 Industrial Compute Gateway
- The Cisco Catalyst 9300 Series Switches
- The Cisco IR8340 Integrated Services Router Rugged

It is also available on the Center DPI, and is enabled by default.

Snort Community Rules are set by default in the Cisco Cyber Vision Center. You can use the **Use Subscriber Rules** toggle button to enable snort subscriber rules. This option requires Advantage licensing and a specific IDS sensor license for each enabled sensor.

Community ruleset

- The community ruleset is a Talos certified ruleset that is distributed freely. It includes rules that have been submitted by the open-source community or by Snort integrators. This ruleset is a subset of the full ruleset available to the subscriber users. It does not contain the latest Snort rules and does not ensure coverage of the latest threats.

Subscriber ruleset

- The subscriber ruleset includes all the rules released by the Talos Security Intelligence and Research Team. The ruleset ensures fast access to the latest rules and early coverage of exploits. Compared to the Community ruleset, it contains more rules and remains in sync with the latest Talos research work on vulnerability detection.

On the **SNORT** Administration page, you can find Snort rules grouped into categories. Use the toggle buttons under the **Status** columns to enable or disable sets of rules.

Click the download buttons under the **Download Rules** column to download each category rule file.

Note that some rules are **not** enabled inside these categories. So, using the toggle button on a category won't necessarily have an effect on their rules. The ones that are considered the most useful are enabled by default, others have been disabled to avoid performance issues. Consequently, if you want to enable these rules you need to use the [specific rule field](#).

It is also possible to enable/disable a specific rule from a custom rule file.

Snort rules categories:

- Browser:

Rules for vulnerabilities present in several browsers including, but not restricted to, Chrome, Firefox, Internet Explorer and Webkit. This category also covers vulnerabilities related to browser plugins such as Active-x.

- Deleted:

When a rule has been deprecated or replaced it is moved to this category.

- Experimental-DoS:

Rules developed by the Cisco CyberVision team for various kinds of DoS activities (TCP SYN flooding, DNS/HTTP flooding, LOIC, etc.).

- Experimental-Scada:

Rules developed by the Cisco CyberVision team for attacks against industrial control system assets.

- Exploit-Kit:

Rules that are specifically tailored to detect exploit kit activity.

- File:

Rules for vulnerabilities found in numerous types of files including, but not restricted to, executable files, Microsoft Office files, flash files, image files, Java files, multimedia files and pdf files.

- Malware-Backdoor:

Rules for the detection of traffic destined to known listening backdoor command channels.

- Malware-CNC:

Known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and ex-filtration of data.

- Malware-Other:

Rules that deal with tools that can be considered malicious in nature as well as other malware-related rules.

- Misc:

Rules that do not fit in any other categories such as indicator rules (compromise, scan, obfuscation, etc.), protocol-related rules, policy violation rules (spam, social media, etc.), and rules for the detection of potentially unwanted applications (p2p, toolbars, etc.).

- OS-Other:

Rules that are looking for vulnerabilities in various operating systems such as Linux based OSes, Mobile based OSes, Solaris based OSes and others.

- OS-Windows

Rules that are looking for vulnerabilities in Windows based OSes.

- Server-Other:

Rules dealing with vulnerabilities found in numerous types of servers including, but not restricted to, web servers (Apache, IIS), SQL servers (Microsoft SQL server, MySQL server, Oracle DB server), mail servers (Exchange, Courier) and Samba servers.

- Server-Webapp:

Rules pertaining to vulnerabilities in or attacks against web based applications on servers.

In case of mistake, or to revert to the default configuration, you can use the **RESET TO DEFAULT** button. Note that all categories status and specific rules status will be reset and any added custom rules file will be deleted.

In addition, this page allows you to import custom rules, to enable or disable rules, and reset Snort's parameters to default.

Import Snort Custom Rules

Custom rules are useful if you want to define and use your own rules in addition to the rules provided in the Cyber Vision rulesets. To do this, a file must be created containing syntactically well-formed Snort rules and imported into Cisco Cyber Vision. Refer to Snort documentation for more information about creating rules.

To import custom rules in the Center, follow these steps:

Procedure

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Prepare your custom rules file. |
| Step 2 | From the main menu, choose Admin > Snort . |
| Step 3 | Click IMPORT CUSTOM RULES FILE under the Import custom rules field.

Once a custom rules file is imported, it is stored in the Center, and a "Download" button appears, allowing you to view its content. |
| Step 4 | Click Synchronize rules on sensors . |
-

What to do next

You can [enable/disable a specific rule](#).

Enable IDS on a Sensor

To enable the Snort engine on a sensor, follow these steps:

Before you begin

To use Snort you need to enable IDS on sensors.

Snort is only compatible with sensors embedded in:

- The Cisco IC3000 Industrial Compute Gateway
- The Cisco Catalyst 9300 Series Switches
- The Cisco IR8340 Integrated Services Router Rugged

Procedure

- Step 1** From the main menu, choose **Admin > Sensor Explorer**.
- Step 2** Click a compatible sensor in the list.
- The right side panel appears with sensor details.
- Step 3** Click **Enable IDS**.

Enable or Disable a Rule

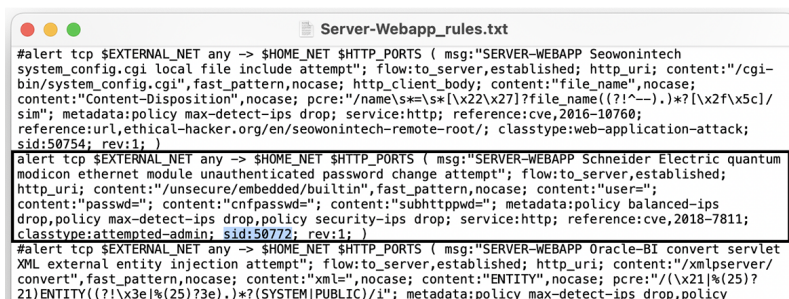
You can manually enable and disable any specific rule, whether it is a default or a custom one. To do so you need the sid (i.e. signature id) that you will find in the rules file.

In the following procedure, we will disable Snort rule sid 50772 as example.

sid 50772: An unverified password change vulnerability (CVE-2018-7811) exists in the embedded web servers of Schneider Electric Quantum Modicon Ethernet modules. This vulnerability could allow an unauthenticated remote user to access the “change password” functionality of the web server. Snort rule with sid 50772 detects such attempts. It monitors and analyzes HTTP flows coming from the external network and raises an alert when the HTTP URI fields contain specific keywords (ex. “passwd=“,”cnfpasswd=“,”subhttppwd=“) that indicate a password change attempt targeting the web server.

Procedure

- Step 1** From the main menu, choose **Admin > Snort**.
- Step 2** Click the **download icon** in the **Download rules** column.
- In the downloaded rule files, locate the rule you wish to enable or disable.



```
#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Seowonintech
system_config.cgi local file include attempt"; flow:to_server,established; http_uri; content:"cgi-
bin/system_config.cgi", fast_pattern,nocase; http_client_body; content:"file_name",nocase;
content:"Content-Disposition",nocase; pcre:"/name\s*=\s*[\x22\x27]?file_name(?:!~|.)*?[\x2f\x5c]/
sim"; metadata:policy max-detect-ips drop; service:http; reference:cve,2016-10760;
reference:url,ethical-hacker.org/en/seowonintech-remote-root/; classtype:web-application-attack;
sid:50754; rev:1; )

#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Schneider Electric quantum
modicon ethernet module unauthenticated password change attempt"; flow:to_server,established;
http_uri; content:"/unsecure/embedded/builtin",fast_pattern,nocase; content:"user=";
content:"passwd="; content:"cnfpasswd="; content:"subhttppwd="; metadata:policy balanced-ips
drop,policy max-detect-ips drop,policy security-ips drop; service:http; reference:cve,2018-7811;
classtype:attempted-admin; sid:50772; rev:1; )

#alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP Oracle-BI convert servlet
XML external entity injection attempt"; flow:to_server,established; http_uri; content:"/xmlpservlet/
convert",fast_pattern,nocase; content:"xml="; nocase; content:"ENTITY",nocase; pcre:"/(\x21|%(25)?
21)ENTITY(?:\?|\x3e|%(25)?3e).)*?(SYSTEM|PUBLIC)/1"; metadata:policy max-detect-ips drop,policy
```

- Step 3** Enter the **Rule sid** under the **Specific rule** field.
- Step 4** Click **Disable**.
- A success message appears.

Note

If you download the rules file again, you will find a "#" preceding the rule, indicating it is disabled.

Step 5 Click **Synchronize rules on sensors** to save and push changes to the sensors.

Risk Score

The **Risk score** page allows you to set up the time range used for risk score computation. To access the **Risk score** page, choose **Admin > Risk score** from the main menu. Computation occurs every hour but considers only the activities within the configured time period.

You can select a time range of 30 days (by default), 7 days, or set a custom one with a minimum of one day

For more information about risk scores, see the [Risk Score Concept](#).

Extensions

From this page, you can manage Cisco Cyber Vision extensions. Extensions are optional add-ons to the Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services. To access the **Extensions** page, choose **Admin > Extensions** from the main menu.

Currently, there are two extensions available:

- **Cyber Vision sensor management**

For more information about this extension and how to use it, see the [Sensors](#).

- **Cyber Vision Reports Management**

For more information about this extension and how to use it, see the [Reports](#).

To install an extension, retrieve the extension file on cisco.com and click **Import a new extension file** to import.