Maintain and Monitor Cisco Cyber Vision

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.

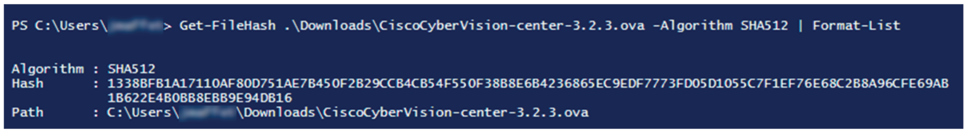
Windows users:

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:

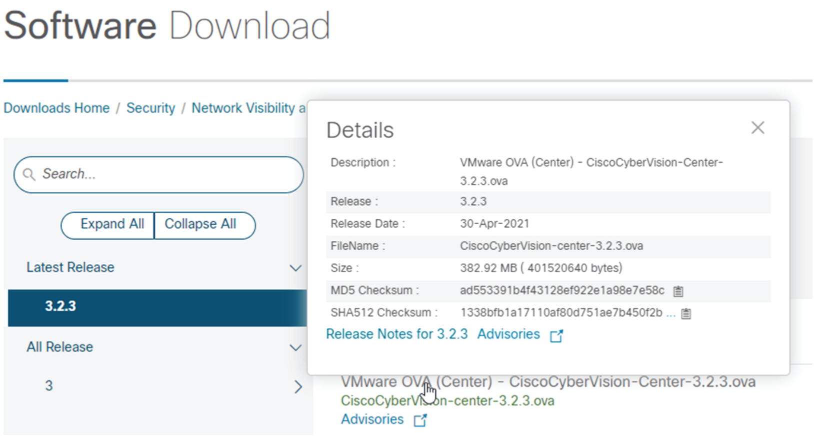
Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List



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

Algorithm : SHA512
Hash      : 1338BFB1A17110AF80D751AE7B450F2B29CCB4CB54F550F38B8E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
            1B622E4B0BB8EBB9E94DB16
Path      : C:\Users\[redacted]\Downloads\CiscoCyberVision-center-3.2.3.ova
```

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



Details

Description : VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova

Release : 3.2.3

Release Date : 30-Apr-2021

FileName : CiscoCyberVision-center-3.2.3.ova

Size : 382.92 MB (401520640 bytes)

MD5 Checksum : ad553391b4f43128ef922e1a98e7e58c

SHA512 Checksum : 1338bfb1a17110af80d751ae7b450f2b ...

Software Download
Downloads Home / Security / Network Visibility a
Search...
Expand All
Collapse All
Latest Release
3.2.3
All Release
3
Release Notes for 3.2.3
Advisories
VMware OVA (Center) - CiscoCyberVision-Center-3.2.3.ova
CiscoCyberVision-center-3.2.3.ova
Advisories

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 meu, 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.

Syslog Configuration

Cisco Cyber Vision provides syslog configuration so that events can be exported and used by a SIEM. The following procedure configures to which machine the syslogs will be sent.

Procedure

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

Step 2 Click **Configure** under **Syslog configuration**.

Step 3 Click the drop-down arrow for the Protocol field and select a protocol from the drop-down list.

If you select **TCP + TLS** connection, the **Set certificate** button displays to import a p12 file. The administrator of your SIEM solution provides this file to secure communications between the Center and the syslog collector.

Step 4 Enter the **Host**.

IP address of the SIEM reachable from the Administration network interface (i.e., eth0) of the Center.

Step 5 Enter the **Port** on the SIEM that will receive syslogs. Use the arrrows.

Step 6 Click the drop-down arrow of the **Format** field to select the variant of syslog.

- **Standard**: Event messages are sent in a format specific to Cisco Cyber Vision and with legacy timestamps (one-second precision).
- **CEF**: Industry standard **Common Event Format** which is understood by most SIEM solutions (no extra configuration is needed on the SIEM). This is the recommended option.
- **Standard/CEF**: Combination of both.
- **RFC3164**: Extended syslog header format with microsecond precision for timestamps.
- **RFC3164/CEF**: Combination of both.

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 on a Sensor.

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 avaible 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 Enable or Disable a Rule.

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 vulnerabilites 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 or Disable a 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 appers 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.

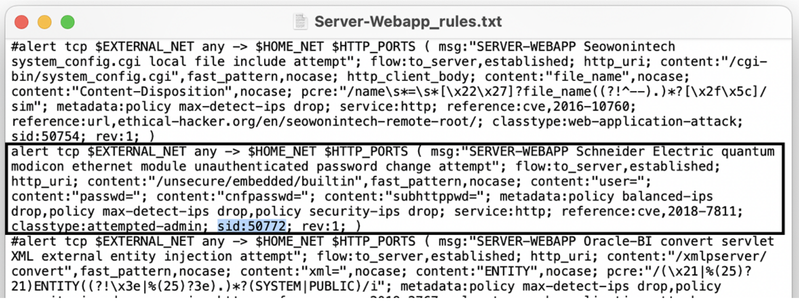
sid 50772: An unverified password change vulnerability (CVE-2018-7811) exists in the embedded web servers of Schneider Electric Quantum Modicon Ethernet modules. This vulnerability could allow an unauthenticated remote user to access the “change password” functionality of the web server. Snort rule with 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:"/xmlpserver/
convert",fast_pattern,nocase; content:"xml=",nocase; content:"ENTITY",nocase; pcre:"/(\x21|%(25)?
21)ENTITY((?!\x3e|%(25)?3e).)*?(SYSTEM|PUBLIC)/i"; 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.