Snort

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's GUI.

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 is set by default in Cisco Cyber Vision. You can enable Snort Subscriber Rules using the corresponding toggle button **(1)**. Note that this option requires the Advantage licensing and a specific IDS sensor license per 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.

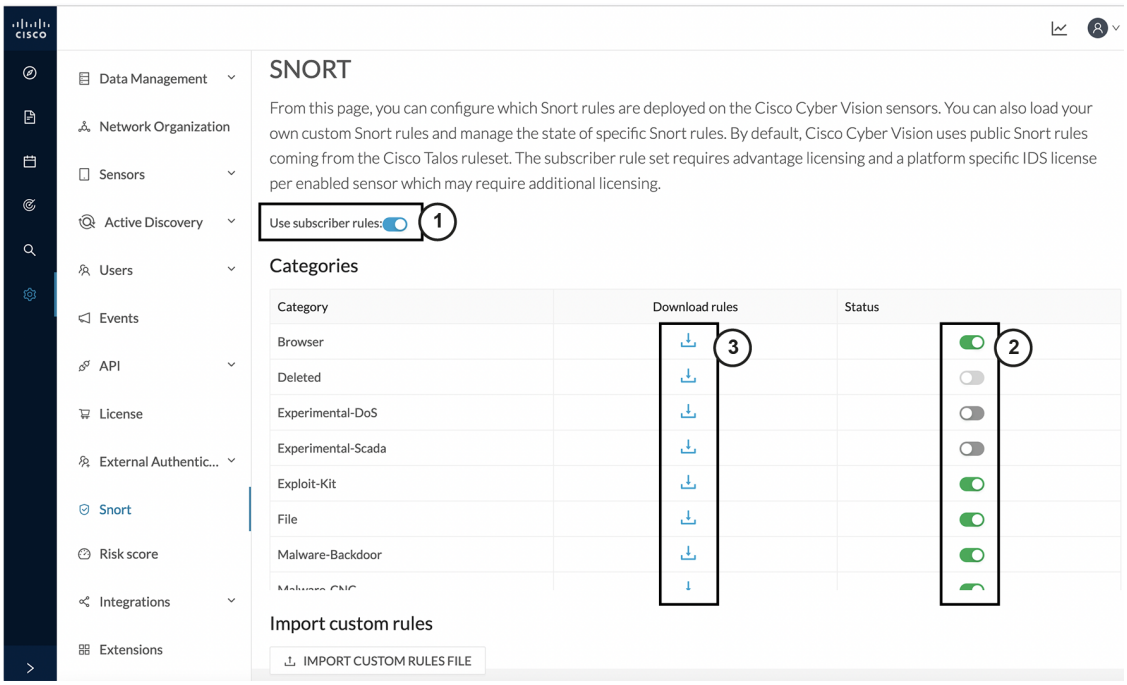
Subscriber ruleset

- 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.

In the Snort administration page, you can find Snort rules grouped into categories, and configure which set of rules to enable or not using the toggle status button **(2)**.

You can download each category rule file using the corresponding button **(3)**.



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/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.

Enable IDS on a sensor

To enable the Snort engine on a sensor:

Before you begin

To use Snort you need to enable IDS on sensors.

Snort is only compatible with sensors embedded in:

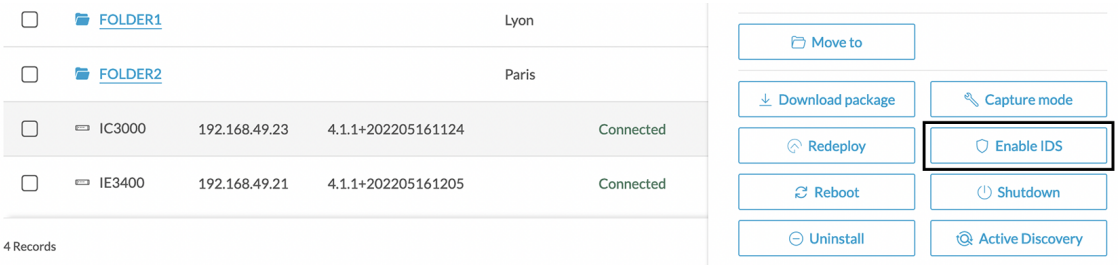
- The Cisco IC3000 Industrial Compute Gateway
- The Cisco Catalyst 9300 Series Switches
- The Cisco IR8340 Integrated Services Router Rugged

Step 1 In Cisco Cyber Vision, navigate to Admin > Sensor Explorer.

Step 2 Click a compatible sensor in the list.

The sensor's right side panel opens.

Step 3 Click **Enable IDS**.



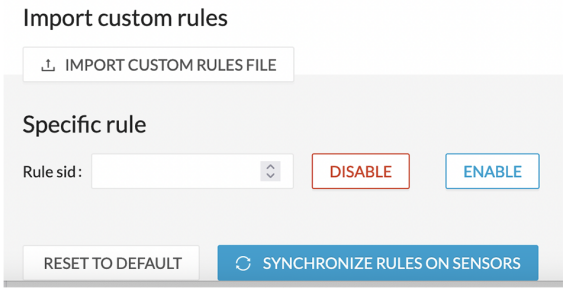
Import Snort custom rules

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.

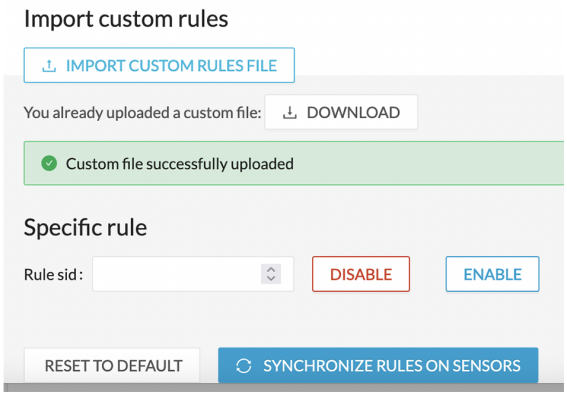
To import custom rules in the Center:

Step 1 Prepare your custom rules file.

Step 2 Click the **Import custom rules file** button.



Once a custom rules file is imported, it is stored in the Center, and a **Download** button appears to check its content.



Step 3 Click **Synchronize rules on sensors**.

What to do next

You can Enable/disable a rule.

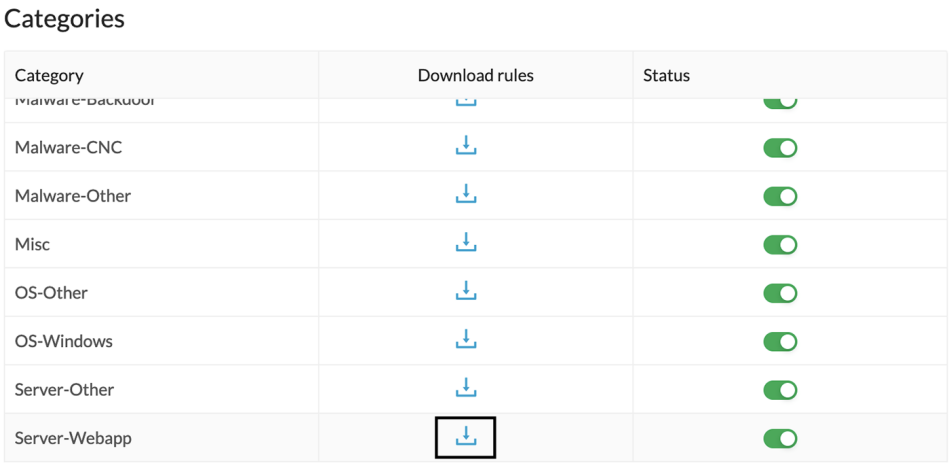
Enable/disable a rule

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.

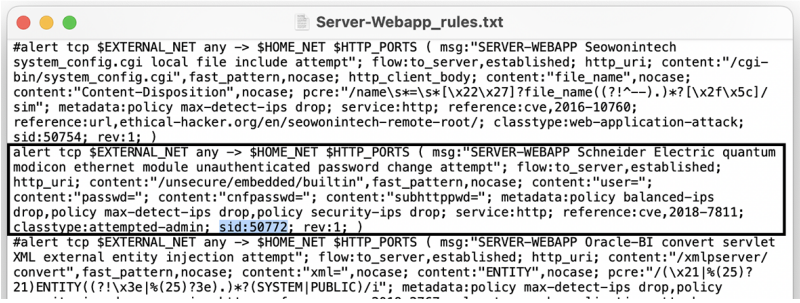
In the following procedure, we will disable Snort rule sid 50772 as example.

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.

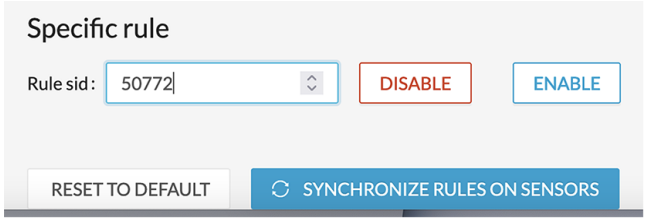
Step 1 Click the **download icon** button.



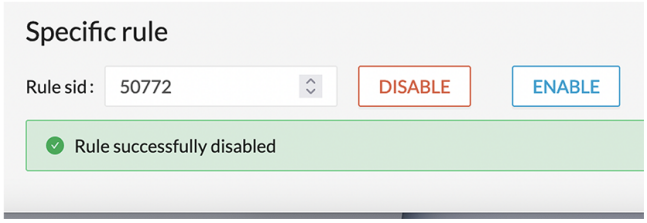
Step 2 In the rule files, look for the rule you want to enable/disable.



Step 3 Type the rule sid and click **Disable**.



A message indicating the rule is disabled appears.



If you download the rules file again you will find a "#" preceding the rule. This indicates the rule is disabled.

Step 4 Click **Synchronize rules on sensors** to save and push changes on the sensors.