



Cisco CSC SSM

The Cisco CSC SSM (Content Security and Control Security Services Module) integrates with Trend Micro InterScan to provide an all-in-one antivirus and spyware management solution for a network. It provides the following protections:

- Detects and takes action against viruses, worms, Trojans, and other threats in network traffic using the SMTP, POP3, HTTP, and FTP protocols
- Blocks compressed or very large files that exceed specified parameters
- Scans for and removes spyware, adware, and other types of grayware

CSC-SSM is a module that resides in a Cisco ASA appliance. Based on user-defined policies, the ASA forwards the specified traffic to the CSC SSM for inspection. The CSC SSM performs actions according to its policies and generates syslog messages about those actions. Cisco Secure MARS parses those messages, which can alert the system to potential and active network threats.



Note

MARS neither parses the configuration settings for the CSC SSM nor monitors the module for performance anomalies. Any anomalies in operation will be reported by the host ASA appliance. Also, while the host ASA appliance does appear in the topology path analysis diagram, the CSC SSM module does not.

This chapter contains the following topics:

- [Defining a CSC SSM in MARS, page 32-1](#)

Defining a CSC SSM in MARS

You can define a CSC SSM module in MARS by adding it manually. Because MARS does not parse (or discover) the configuration settings for the CSC SSM, you do not need to bootstrap the module to allow MARS administrative access to the module. However, you do need to define MARS as a syslog target of the module.

1. Bootstrap the CSC SSM module to send syslog message to the MARS appliances.
See ["Configuring System Log Message Settings"](#) to define the MARS appliances as a target syslog server on the CSC SSM.
2. Define the CSC SSM module under an existing ASA appliance.
See [Define a CSC SSM in MARS Manually, page 32-2](#).

Related Documents

Related Topics	Document Title
See " Configuring System Log Message Settings " to specify the MARS appliances as a target syslog server.	Cisco Content Security and Control SSM Administrator Guide

Define a CSC SSM in MARS Manually

To manually define a CSC SSM, you must have previously define the host ASA appliance in which the module is installed and configured. When the module is defined and the changes are activated, MARS normalizes the syslog message receive by the module against known event types.

To define a CSC SSM module on an ASA appliances in MARS, follow these steps:

- Step 1** From the list of devices, select the ASA appliances under which you want to define the CSC SSM module, and click **Edit**.



Tip You can filter the list of devices selectable devices by typing the device name in the Search field and clicking **Search**.

The ASA appliance settings page appears.

- Step 2** Click **Add Module** at the bottom of the page.

The Device Type page appears.

Device Type: Cisco CSC SSM 6.1

- Cisco ASA 7.0
- Cisco ASA 7.2
- Cisco ASA 8.0
- Cisco ASA 8.1
- Cisco CSC SSM 6.1
- Cisco CSC SSM 6.2
- Cisco IPS 5.x
- Cisco IPS 6.x

*Device

Reporting IP

Cancel Submit

- Step 3** Select **Cisco CSC SSM 6.1** or **Cisco CSC SSM 6.2** for the Device Type list.
- Step 4** Type the name of this module in the **Device Name** field.
- Step 5** Type the IP address of the CSC-SSM module in the **Reporting IP** field.
- Step 6** To save your changes, click **Submit**.

The module name appears under the Module Names list. The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

- Step 7** To enable MARS to start sessionizing events from this module, click **Activate**.

MARS begins to sessionize events generated by this module and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see [Activate the Reporting and Mitigation Devices, page 1-15](#).
